Πανεπιστήμιο Πελοποννήσου
Σχολή Θετικών Επιστημών και Τεχνολογίας
Τμήμα Επιστήμης και Τεχνολογίας Υπολογιστών

Μεταπτυχιακή Εργασία

<Μέθοδοι αξιολόγησης της ασφάλειας λογισμικού εφαρμογών>

Ονοματεπώνυμο Φοιτητή: Αλεξανδροπούλου Μαρία

ΑΜ: 2009002

Επιβλέπων Καθηγητής: Βασιλάκης Κωνσταντίνος

Τρίπολη, Φεβρουάριος 2011

…αφιερώνεται στη μνήμη του αδελφού μου…

Ευχαριστίες

Τελειώνοντας τη μεταπτυχιακή εργασία, οφείλω να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Βασιλάκη Κωνσταντίνο για την πολύτιμη και απαραίτητη καθοδήγησή του, καθώς και για την ευκαιρία που μου έδωσε ώστε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα. Τέλος, ευχαριστώ τους γονείς μου για την συμπαράστασή τους στη διάρκεια αυτής της προσπάθειάς μου.

Μαρία

Περίληψη

Μια βασική ιδιότητα του λογισμικού είναι η ασφάλεια. Η ασφάλεια αποτελεί επιτακτική ανάγκη, ιδιαίτερα εξαιτίας της διασύνδεσης των υπολογιστών στο Διαδίκτυο, το οποίο αυξάνει τις πιθανές επιθέσεις από κακόβουλους επιτιθέμενους που βασίζονται σε ευπάθειες στο λογισμικό. Οι υπεύθυνοι της ασφάλειας πρέπει να ανιχνεύσουν τις απειλές που δεν μπορούν να δουν οι υπόλοιποι, να ποσοτικοποιήσουν τους κινδύνους που οι άλλοι δεν μπορούν κατανοήσουν, καθώς και να ανακαλύψουν τις ευπάθειες που κρύβονται στις εφαρμογές, στα δίκτυα και τα συστήματα του οργανισμού. Μια σημαντική πτυχή της διασφάλισης της ασφάλειας του λογισμικού είναι η αξιολόγησή της, ώστε να αναδειχθούν ευπάθειες και να ληφθούν κατάλληλα διορθωτικά μέτρα. Πρόκειται για μια μεγάλη διαδικασία που απαιτεί ένα διεξοδικό σχέδιο, λεπτομερείς οδηγίες, αυξημένες δεξιότητες και ένα καλό σύνολο εργαλείων. Ο απαραίτητος χρόνος και οι δεξιότητες για την αποτελεσματική αξιολόγηση της ασφάλειας δεν θα είναι ποτέ ελεύθερα διαθέσιμα, αλλά μια κατάλληλη μεθοδολογία και τα αντίστοιχα εργαλεία είναι εύκολα στη χρήση και ελεύθερα διαθέσιμα, χάρη στην κοινότητα ανοικτού κώδικα.

Υπάρχουν πολλές μεθοδολογίες ανοικτού κώδικα που χρησιμοποιούνται σήμερα από τους ελεγκτές ασφάλειας για την αξιολόγηση της ασφάλειας λογισμικού εφαρμογών. Όλες αυτές οι μεθοδολογίες παρέχουν ένα σύνολο από λεπτομερείς οδηγίες ώστε να διεξαχθεί ένας έλεγχος ασφάλειας και κάθε μια μπορεί να έχει τα θετικά της σημεία αλλά και τις αδυναμίες της. Τα συμπεράσματα που προκύπτουν μετά τη διενέργεια ενός ελέγχου ασφάλειας χρησιμοποιώντας κάποια μεθοδολογία, μπορούν διασφαλίσουν τον οργανισμό από πολλές κακόβουλες επιθέσεις.

Αντικείμενο της παρούσας μεταπτυχιακής εργασίας αποτελεί η διερεύνηση και η μελέτη των πιο δημοφιλών μεθοδολογιών αξιολόγησης της ασφάλειας λογισμικού ανοικτού κώδικα. Πραγματοποιείται, διεξοδική αναφορά σε αυτές τις μεθοδολογίες, καθώς και στο πλαίσιο που τις διέπει και παράλληλα, μελετώνται τα αντίστοιχα εργαλεία λογισμικού ανοικτού κώδικα που τις υποστηρίζουν.

Η διάρθρωση της εργασίας έχει ως εξής: Το Κεφάλαιο 1 εισάγει τον αναγνώστη στις βασικές έννοιες που σχετίζονται με την ασφάλεια λογισμικού εφαρμογών και αναλύει τον όρο της αξιολόγησης της ασφάλειας. Στο Κεφάλαιο 2 περιγράφεται η μεθοδολογία OSSTMM (Open Source Security Testing Methodology) v2.2. Το Κεφάλαιο 3 ασχολείται με τη μεθοδολογία OWASP (Open Web Application Security Project) και συγκεκριμένα, στο υποκεφάλαιο 3.2 γίνεται αναφορά στον οδηγό OWASP Testing Guide v3 και στο υποκεφάλαιο 3.3 στο πρότυπο OWASP ASVS (Application Security Verification Standard). Στο Κεφάλαιο 4 περιγράφεται η μεθοδολογία Technical Guide to Information Security Testing and Assessment του NIST-SP 800-115 και στο Κεφάλαιο 5 αναλύεται η μεθοδολογία ISSAF (Information System Security Assessment Framework) 0.2. Στο Κεφάλαιο 6 πραγματοποιείται συγκριτική αξιολόγηση και εξάγονται συμπεράσματα σχετικά με τις μεθοδολογίες που αναλύθηκαν. Τέλος, επισημαίνεται ότι έχει ακολουθηθεί μία τυποποιημένη δομή για όλες τις μεθοδολογίες, ώστε να διευκολύνεται η σύγκριση των χαρακτηριστικών τους. Συγκεκριμένα, η δομή για κάθε μεθοδολογία (κεφάλαιο) είναι η ακόλουθη:

- Γενικά - Βασικοί στόχοι της μεθοδολογίας.
- Εμβέλεια.
- Επίπεδα ασφάλειας, εφόσον υπάρχουν.
- Βασική μεθοδολογία ασφάλειας.

- Εργαλεία για την υποστήριξη της μεθοδολογίας.

Abstract

A basic attribute of software is security. Security is of vital importance, especially because of the interconnection of computers in the Internet, which increases the possible attacks based on software vulnerabilities from malicious hackers. Those responsible for security should detect threats that others can't see, quantify risks that others can't understand, as well as reveal hidden vulnerabilities in the applications, networks and systems of the organization. An important aspect of software security assurance is its assessment, in order vulnerabilities to be detected and appropriate corrective countermeasures to be taken. This is a big process that requires a comprehensive plan, detailed instructions, strong skills, and a good set of tools. The time and skills necessary for effective security assessment will never be free, but an appropriate methodology and the corresponding tools are easy, freely available due to the open source community.

There are many open source security methodologies which are used today by security auditors for the security assessment of the application software. All of these methodologies provide a set of detailed instructions in order a security testing to be conducted, and each one has its strong points and weaknesses. The conclusions resulting from the realisation of a security testing after using some methodology protect the organization from many malicious attacks.

The purpose of the present master thesis constitutes the investigation and study of the most popular open source methodologies in software security assessment. An extensive report in these methodologies is made, as well as in their framework, and at the same time, the corresponding open source software tools that support them are under consideration.

The structure of thesis is as follows: Chapter 1 introduces the basic notions that are related to the application software security and it analyzes the term of security assessment. In Chapter 2, OSSTMM (Open Source Security Testing Methodology) v2.2 methodology is described. Chapter 3 deals with OWASP (Open Web Application Security Project) methodology. More specifically, subchapter 3.2 refers to the guide of OWASP Testing Guide v3 and subchapter 3.3 refers to the standard of OWASP ASVS (Application Security Verification Standard). In Chapter 4, the Technical Guide to Information Security Testing and Assessment of NIST - SP 800-115 methodology is described and in Chapter 5, ISSAF (Information System Security Assessment Framework) 0.2 methodology is analyzed. In Chapter 6, a comparative assessment is made and conclusions are drawn from the methodologies that were analyzed. Finally, it is pointed out that a standardised structure for all methodologies has been followed in order to facilitate the comparison of their characteristics. Particularly, the structure for each methodology (chapter) is, as follows:

- Overview - Basic objectives of methodology.
- Scope.
- Security levels, if they exist.
- Basic security methodology.
- Tools for the support of methodology.

Περιεχόμενα

Κεφάλαιο 1:

Εισαγωγή

Η ασφάλεια του λογισμικού είναι ένα από τα βασικά ποιοτικά χαρακτηριστικά του, το οποίο αποκτά ιδιαίτερη σημασία καθώς η αξία των πληροφοριών αυξάνεται και τα πληροφοριακά συστήματα συνδέονται στο Διαδίκτυο, για να προσφέρουν υπηρεσίες στους χρήστες σύμφωνα με την αρχή «οπουδήποτε/οποτεδήποτε». Υπάρχει ένα πλήθος διαφορετικών πτυχών για το πώς μπορεί να αντιληφθεί κάποιος την έννοια της ασφάλειας, στο πλαίσιο των πληροφοριακών συστημάτων, αλλά όλες πηγάζουν από τη βασική έννοια της ασφάλειας.

Η ραγδαία εξέλιξη των νέων τεχνολογιών έχει καταστήσει ευκολότερη τη διαδικασία καταγραφής, αποθήκευσης μεταφοράς και διαμοιρασμού οποιουδήποτε είδους ηλεκτρονικού δεδομένου ή πληροφορίας. Έτσι, η διενέργεια εμπορικών

συναλλαγών από τους διάφορους οργανισμούς ή επιχειρήσεις γίνεται ακόμη ευκολότερη. Αυτό όμως έχει σαν αποτέλεσμα να προκύπτουν σοβαρά ζητήματα ασφάλειας σχετικά με το ποιος έχει πρόσβαση στις πληροφορίες του συστήματος και πώς αυτές θα μπορέσουν να προστατευθούν από επίδοξους κακόβουλους επιτιθέμενους.

Η σημασία της ασφάλειας έγινε περισσότερο εμφανής, τα τελευταία χρόνια. Πλέον δεν είναι αναγκαίο να έχει κανείς φυσική πρόσβαση σε έναν υπολογιστή για να μπορέσει να προσπελάσει και να επεξεργαστεί τα δεδομένα του. Αυτό έχει ως συνέπεια να αυξάνονται οι πιθανότητες επίθεσης και οι απειλές στα συστήματα και μερικές φορές να είναι πολύ δύσκολο να εντοπιστούν αυτοί που πραγματοποιούν την επίθεση. Το παραπάνω ενισχύεται από το γεγονός ότι, το κόστος μιας επίθεσης στην ασφάλεια ενός συστήματος μπορεί να είναι πολύ χαμηλό. Υπάρχουν τεχνικές επιθέσεων που πραγματοποιούνται εξ αποστάσεως και

βασίζονται είτε σε επιθέσεις εκμετάλλευσης αδυναμιών του συστήματος, είτε σε επιθέσεις μέσω ιών, είτε σε επιθέσεις στο δίκτυο ή επιθέσεις στο λογισμικό ενός υπολογιστή με στόχο την παράνομη προσπέλαση σε αυτόν και την αλλοίωση ή υποκλοπή των δεδομένων του. Οι συνέπειες αυτών των επιθέσεων, που περιλαμβάνουν τη μειωμένη πλέον εμπιστοσύνη του κοινού στον συγκεκριμένο οργανισμό που δέχθηκε την επίθεση, μεγιστοποιούν κατά πολύ τις αρνητικές επιπτώσεις που προκαλούνται στον οργανισμό.

Ο αδύναμος κρίκος στην αλυσίδα της ασφάλειας των συστημάτων, είναι η ύπαρξη ευπαθειών (vulnerabilities) στις εφαρμογές και το λογισμικό γενικότερα (συμπεριλαμβάνοντας τα λειτουργικά συστήματα, τις βάσεις δεδομένων, τους εξυπηρέτες διαδικτύου κ.λπ.), οι οποίες επιτρέπουν εισβολές από κακόβουλους χρήστες (hackers). Οι ευπάθειες που πιθανότητα υπάρχουν σε κάποια εφαρμογή, μπορεί να προκαλέσουν σημαντική ζημιά στην εφαρμογή και στα δεδομένα της. Για να αποφευχθεί κάτι τέτοιο, οι υπεύθυνοι ανάπτυξης των εφαρμογών θα πρέπει να μπορούν να ανιχνεύσουν αυτές τις αδυναμίες και να προτείνουν κατάλληλους τρόπους αντιμετώπισής τους. Κι εδώ είναι η στιγμή που εμφανίζεται ένας νέος τομέας στη διασφάλιση της ασφάλειας του λογισμικού. Αυτός ο νέος τομέας είναι η αξιολόγηση της ασφάλειας, έτσι ώστε να ανακαλυφθούν αδυναμίες και να ληφθούν σχετικά διορθωτικά μέτρα. Οι υπεύθυνοι ανάπτυξης του λογισμικού οφείλουν, λοιπόν, να πραγματοποιούν αξιολόγηση της ασφάλειας του λογισμικού που παράγουν, δηλαδή να μπορούν να ανιχνεύουν τις ευπάθειες, αλλά και να διεξάγουν τους απαραίτητους ελέγχους γρήγορα και σωστά. Για να το επιτύχουν αυτό,

χρησιμοποιούν μεθοδολογίες αξιολόγησης της ασφάλειας (ανοικτού κώδικα ή όχι), καθώς και τα αντίστοιχα εργαλεία λογισμικού που υποστηρίζουν οι μεθοδολογίες αυτές.

1.1 Ασφάλεια (Security)

Ο αγγλικός όρος «security», φέρεται να είναι λατινικής προέλευσης, αφού προέρχεται από τις αντίστοιχες λατινικές λέξεις «se» που σημαίνει «χωρίς» και «cura» που σημαίνει «φροντίδα». Δηλαδή, η έννοια της ασφάλειας σε ένα σύστημα μπορεί και να θεωρηθεί ως μια επιθυμητή ιδιότητα - κατάστασή του, κατά την οποία οι χρήστες του απαλλάσσονται κάθε έγνοιας και φροντίδας, ως προς τη σωστή λειτουργία του. Παρόλο που ο όρος ασφάλεια φαίνεται να έχει μια προφανή σημασία, χρειάζεται να καταβληθεί σημαντική προσπάθεια προκειμένου να καταγραφεί το ακριβές της νόημα.

Ας θεωρήσουμε τον εξής ορισμό της ασφάλειας: «Ως ασφάλεια αποδίδεται η διαδικασία αναγνώρισης των γεγονότων που έχουν τη δυνατότητα να προκαλέσουν ζημιά (ή σενάρια απειλής) και η εφαρμογή μέτρων προστασίας (safeguards) για να μειωθεί ή να απομακρυνθεί αυτή η δυνατότητα» [Landwerh, C., (2001)] [Gollmann, D., (2002)]. Στην απλούστερη μορφή της, είναι η διαδικασία για την προστασία από ζημίες ή απώλειες. Η ασφάλεια επίσης περιγράφει τα μέτρα προστασίας, δηλαδή τα αντίμετρα (countermeasures) που τίθενται από την διαδικασία ασφάλειας.

Μπορούμε να κατανοήσουμε καλύτερα την έννοια της ασφάλειας αν διακρίνουμε τις τρεις συνεχείς και διαφορετικές μεταξύ τους δράσεις που αυτή απαιτεί:

- Πρόληψη (prevention): Λήψη μέτρων που μας επιτρέπουν να προλαβαίνουμε τη δημιουργία επικίνδυνων καταστάσεων.
- Ανίχνευση (detection): Λήψη μέτρων που μας επιτρέπουν να αντιληφθούμε πως, πότε και από ποιόν έχει προκληθεί κάποια ζημιά.
- Αντίδραση (reaction): Λήψη μέτρων που μας επιτρέπουν να αποκαταστήσουμε τις ζημιές που έχουν προκληθεί.

Η πρόληψη αποτελεί το θεμέλιο λίθο, καθώς χρησιμεύει ως μονάδα ποσοτικής μέτρησης έναντι της ανίχνευσης και αντίδρασης. Η ανίχνευση συνεπικουρεί στην ανίχνευση τυχόν κενών και προβλημάτων ασφάλειας, μόλις τα προληπτικά μέτρα τεθούν σε εφαρμογή και τέλος, η αντίδραση ανταποκρίνεται με τους κατάλληλους μηχανισμούς στις διαρροές ασφάλειας (security breach) [Canavan, J., (2001)]. Ασφάλεια σε ένα σύστημα λοιπόν, κατά κύριο λόγο, συνεπάγεται εξέταση των ευπαθειών, απειλών, αντιμέτρων και του αποδεκτού ρίσκου.

Εννοείται πως χρειάζεται να γίνει περισσότερο σαφής η εικόνα των «επικίνδυνων καταστάσεων» ή «ζημιών». Θα πρέπει λοιπόν να απαντήσουμε στην ερώτηση: «Τι ακριβώς διακυβεύεται;» Οι επικρατούσες απόψεις διακρίνουν τις τρεις ακόλουθες βασικές έννοιες σε σχέση με τη διαχείριση ενός ασφαλούς συστήματος:

- Εμπιστευτικότητα (confidentiality): Καλείται η προστασία των αποθηκευμένων ή μεταδιδόμενων πληροφοριών από κοινοποίηση σε ένα πρόσωπο ή μια οντότητα και κατά επέκταση, η αποτροπή της μη εξουσιοδοτημένης ανάγνωσης. Στην υπηρεσία της εμπιστευτικότητας διακρίνουμε και δύο επιπλέον όψεις της. Την ιδιωτικότητα (privacy), δηλαδή

την προστασία των προσωπικών δεδομένων και τη μυστικότητα (secrecy), δηλαδή την προστασία των δεδομένων, που ανήκουν σε ένα οργανισμό. Η εμπιστευτικότητα καλείται να παρέχει ασφάλεια από μη εξουσιοδοτημένη ανάγνωση, αντιγραφή, μετατροπή πληροφοριών. Ειδικότερα για την ανταλλαγή πληροφοριών πρέπει επιπρόσθετα να διασφαλίζεται ότι η ανταλλαγή πληροφοριών είναι αδιάλειπτη.

- Ακεραιότητα (integrity): Η ετυμολογική ανάλυση της λέξης προσδίδει και το επακριβές της νόημα. Ο έλεγχος της ακεραιότητας γίνεται προκειμένου να αποτραπεί εσφαλμένη ενδεχόμενη τροποποίηση (π.χ. εγγραφή, διαγραφή ή μεταβολή) των πληροφοριών που μπορεί να πραγματοποιηθεί με ή δίχως δόλο. Το σύστημα πρέπει να επιτρέπει τέτοιου είδους ενέργειες μόνο σε κατάλληλα εξουσιοδοτημένους χρήστες. Αναφορικά με τη μετάδοση πληροφοριών, η ακεραιότητα σημαίνει ότι διασφαλίζεται η ακρίβεια και η πληρότητα των διακινούμενων πληροφοριών, ώστε οι πληροφορίες που αποστέλλονται να καταλήγουν στον τελικό τους αποδέκτη όπως ακριβώς στάλθηκαν.
- Διαθεσιμότητα (availability): Η έννοια της διαθεσιμότητας καθορίζεται ως εκείνη η υπηρεσία ασφάλειας που επιτρέπει στην πληροφορία να είναι συνεχώς παρεχόμενη, προσβάσιμη και ικανή προς χρήση όταν ζητείται από μια εξουσιοδοτημένη οντότητα, δίχως αδικαιολόγητη καθυστέρηση και σύμφωνα πάντα με τις προδιαγραφές του συστήματος.

Σε αρκετές ερευνητικές εργασίες υποστηρίζεται πως οι παραπάνω τρεις ιδιότητες δεν επαρκούν, για να οριστεί η ασφάλεια πληροφοριών. Πρόσθετες ιδιότητες που συναντώνται είναι οι παρακάτω:

- Μη αποποίηση ευθύνης (no-repudiation): Η μη αποποίηση ευθύνης αποτρέπει τόσο τον αποστολέα όσο και τον παραλήπτη μίας πληροφορίας να αρνηθούν την πράξη της συμμετοχής τους σε μία συναλλαγή. Αυτός ο έλεγχος συνίσταται όταν αποστέλλεται ένα μήνυμα, ότι αυτό έχει αποσταλεί και έχει παραληφθεί δίχως καμία πλευρά να αμφισβητεί τη πράξη της συναλλαγής.
- Έλεγχος πρόσβασης (access control): Καλείται η ικανότητα να προσδιορίζεται και να ελέγχεται η πρόσβαση σε διακομιστές (servers) και στις εφαρμογές, συμπεριλαμβάνοντας και την πρόσβαση μέσω των επικοινωνιακών συνδέσμων. Ο έλεγχος πρόσβασης, αυθεντικοποιεί και εξουσιοδοτεί την ταυτότητα της οντότητας (ανθρώπινης ή υπολογιστικής) που επιχειρεί να έχει πρόσβαση σε ένα υπολογιστικό πόρο (computing resource) και ελέγχει τη χρήση του υπολογιστικού πόρου στα προκαθορισμένα επίπεδα δικαιοδοσίας. Περιλαμβάνει τις έννοιες της Αυθεντικοποίησης (authentication) και της Εξουσιοδότησης (authorization).
  Η αυθεντικοποίηση ελέγχει και επικυρώνει την ταυτότητα της οντότητας που επιζητεί πρόσβαση και χρήση, ώστε να καθίσταται πρακτικά αδύνατο να παρουσιαστεί ένα άλλο αντικείμενο ως ένα άλλο (impersonation). Η οντότητα αυτή μπορεί να είναι ένας άνθρωπος, μια εφαρμογή δικτύου, μία συσκευή (δρομολογητής - router).
  Η εξουσιοδότηση αναφέρεται στα δικαιώματα πρόσβασης μιας οντότητας σε ένα σύστημα (κατανεμημένο, πληροφοριακό). Ουσιαστικά ο ρόλος της είναι να καθορίζει τις ενέργειες ή τις λειτουργίες που οι εξουσιοδοτημένες οντότητες μπορούν να πραγματοποιήσουν στο σύστημα, όπως ανάλογα με το επίπεδο και το δικαίωμα πρόσβασης να αναγνώσουν πληροφορίες, να δημιουργούν ή να καταστρέφουν δεδομένα κ.λπ. Θα πρέπει να επισημανθεί

ότι η εξουσιοδότηση διαφέρει από την πιστοποίηση. Η πιστοποίηση (verification) ελέγχει εάν ο χρήστης είναι μέλος του συστήματος και από την στιγμή που αυτό πιστοποιείται, εξουσιοδοτείται με τα ανάλογα δικαιώματα που έχουν δοθεί από το σύστημα.

1.2 Ασφάλεια Λογισμικού

Η ασφάλεια λογισμικού (software security) είναι ένα πεδίο που ασχολείται με τον τρόπο που πρέπει να αναπτύσσεται και να σχεδιάζεται το λογισμικό, ώστε να είναι όσο το δυνατόν λιγότερο ευάλωτο σε κακόβουλες επιθέσεις. Αυτό το πεδίο της ασφάλειας αναπτύχθηκε κυρίως κατά τα τελευταία χρόνια. Η Microsoft, το 2002, έθεσε ως μια από τις πρώτες προτεραιότητές της, την ασφάλεια λογισμικού. Τα προηγούμενα χρόνια, είτε δε δινόταν και τόση σημασία στην ασφάλεια λογισμικού, αφού υπερίσχυε η λειτουργικότητα των εφαρμογών, ή η ασφάλεια συμπεριλαμβανόταν στο σύστημα εκ των υστέρων. Η επιτυχής ανάπτυξη ασφαλούς λογισμικού απαιτεί από την αρχή προσεγμένη σχεδίαση και υλοποίηση με όσο το δυνατό λιγότερα προγραμματιστικά σφάλματα.

Το σημαντικότερο πρόβλημα της ασφάλειας αναφέρεται στο λογισμικό το οποίο δεν έχει υλοποιηθεί σωστά. Κάτι τέτοιο θα έχει σαν αποτέλεσμα, να διακυβεύονται οι έννοιες που αναφέραμε προηγουμένως (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, κ.λπ.). Είναι λογικό ότι τα προηγούμενα χρόνια, όπου οι υπολογιστές παρέμεναν αυτόνομοι, τα προβλήματα ασφάλειας περιοριζόταν στις επιθέσεις από χρήστες που είχαν φυσική πρόσβαση στο σύστημα. Όταν όμως έγινε επιτακτική ανάγκη η σύνδεσή τους σε δίκτυα και κυρίως στο Διαδίκτυο, τότε τα προβλήματα ασφάλειας αυξήθηκαν σημαντικά, αφού υπήρχε η δυνατότητα οποιοσδήποτε να μπορεί να αποκτήσει πρόσβαση σε οποιονδήποτε συνδεδεμένο υπολογιστή. Οι ευπάθειες (vulnerabilities) ασφάλειας στο λογισμικό, υπήρχαν πάντα, όμως απέκτησαν μεγαλύτερη σημασία με τη δικτύωση των υπολογιστών.

Η ευπάθεια είναι μια αδυναμία που μπορεί κάποιος να εκμεταλλευθεί με σκοπό να υποκλέψει πληροφορίες, να προκαλέσει ζημιά ή με οποιονδήποτε τρόπο να υποβαθμίσει μία από τις προαναφερθείσες διαστάσεις της ασφάλειας. Στην πραγματικότητα, οι εισβολείς δεν δημιουργούν ευπάθειες στο λογισμικό, το μόνο που κάνουν είναι να ανιχνεύουν τις ευπάθειες που πιθανόν υπάρχουν και στη συνέχεια να τις εκμεταλλεύονται για να επιτεθούν στο σύστημα. Σε αυτή την περίπτωση, το σύστημα ονομάζεται σύστημα-στόχος. Επομένως, είναι πολύ σημαντική η ανάπτυξη ασφαλούς κώδικα, δηλαδή κώδικα που δεν περιλαμβάνει προγραμματιστικά σφάλματα, τα οποία μπορεί να αποτελέσουν ευπάθειες. Η ανάπτυξη ασφαλούς κώδικα σημαίνει κατασκευή ασφαλών προϊόντων λογισμικού, τα οποία αντέχουν σε κακόβουλες επιθέσεις ή ακόμη και σε ατυχείς ενέργειες που δεν περιλαμβάνουν δόλο.

Οι περισσότεροι κατασκευαστές λογισμικού, θεωρούν ότι η ασφάλεια είναι ένα χαρακτηριστικό το οποίο μπορεί να προστεθεί στο τέλος της ανάπτυξης του λογισμικού, ενώ θα έπρεπε να δίνουν ιδιαίτερη σημασία ήδη από τη φάση της σχεδίασης και της ανάπτυξης του προϊόντος. Η απόδοση ασφάλειας σε ένα σύστημα λογισμικού εκ των υστέρων, δεν είναι και πολύ καλή ιδέα και επιπλέον, απαιτεί μεγαλύτερη προσπάθεια και περισσότερο κόστος.

Οι ευπάθειες λογισμικού είναι κάτι συνηθισμένο, όμως και οι εφαρμογές ιστού (web applications) ειδικότερα εμφανίζουν επίσης μεγάλο κίνδυνο ασφάλειας. Τα προηγούμενα σε συνδυασμό με την πολυπλοκότητα και επεκτασιμότητα του

λογισμικού, έχουν ως αποτέλεσμα το πρόβλημα της ασφάλειας να γίνεται ακόμη πιο σύνθετο.

Η ασφάλεια εφαρμογών (application security) αναφέρεται στην προστασία του λογισμικού αφού αυτό κατασκευαστεί. Σε μία αναφορά από τη Symantec, σημειώθηκε μια σημαντική αύξηση των επιθέσεων ενάντια στις εφαρμογές. Η αναφορά δηλώνει ότι περίπου 48% από τις 1.403 νέες ευπάθειες που τεκμηριώθηκαν μεταξύ της 1ης Ιουλίου και 31 Δεκεμβρίου, του 2004, ενέπεσαν στην κατηγορία των εφαρμογών. Ακόμη και οι εταιρίες με την ισχυρότερη δικτυακή ασφάλεια, θα πρέπει να κατανοήσουν ότι υπάρχει άλλο ένα στρώμα ανοικτό στις επιθέσεις: οι εφαρμογές.

Από τη μια πλευρά, η ασφάλεια λογισμικού αναφέρεται στη δημιουργία ασφαλούς λογισμικού, δηλαδή στη σχεδίαση του λογισμικού ώστε να είναι ασφαλές. Σημαντικό είναι να εκπαιδεύονται οι προγραμματιστές, οι σχεδιαστές λογισμικού και οι χρήστες σχετικά με το πώς μπορούν να αναπτύξουν ένα ασφαλές προϊόν. Από την άλλη πλευρά, η ασφάλεια εφαρμογών αναφέρεται στην προστασία των εφαρμογών αφού έχει ολοκληρωθεί η ανάπτυξή τους. Η ασφάλεια εφαρμογών ασχολείται με την αναζήτηση, ανίχνευση και διόρθωση γνωστών προβλημάτων ασφάλειας, αφού αυτά τα έχει εκμεταλλευτεί κάποιος στα υπό εξέταση συστήματα.

Δίνοντας λίγο περισσότερη έμφαση στις εφαρμογές ιστού (web), θα πρέπει να επισημάνουμε η ασφάλειά τους πρέπει να είναι ιδιαίτερο μέλημα για τους κατασκευαστές και τους οργανισμούς που τις λειτουργούν, αφού σχετίζονται άμεσα με το Διαδίκτυο. Άλλωστε για τη δημιουργία και τη λειτουργία ενός ιστοτόπου (website) στο οποίο «τρέχουν» εφαρμογές ιστού, χρησιμοποιείται ένας μεγάλος αριθμός διαφορετικών τεχνολογιών και προϊόντων. Η αλληλεπίδραση μεταξύ αυτών, προκαλεί ένα μεγάλο πλήθος πιθανών προβλημάτων ασφάλειας. Από την ύπαρξη και την εκμετάλλευση αυτών των αδυναμιών, ένας επιτιθέμενος μπορεί να προκαλέσει μεγάλη ζημιά.

Οι αδυναμίες αυτές, επομένως, καθιστούν τις εφαρμογές ιστού πολύ ευάλωτες σε επιθέσεις από hackers. Άλλωστε, οι hackers, πλέον, δεν αποτελούν μια μικρή εξειδικευμένη κοινότητα. Υπάρχουν πίνακες ανακοινώσεων και ομάδες συζητήσεων, όπου ο καθένας μπορεί να βρει κατάλληλο υλικό και πληροφορίες για την πραγματοποίηση διαφόρων ειδών επιθέσεων. Η πλειοψηφία των επιθέσεων προέρχεται από αυτήν την κατηγορία. Για τον λόγο αυτό, θα πρέπει να γίνονται τακτικοί έλεγχοι στο σύνολο των εφαρμογών, να επαναλαμβάνονται σε κάθε νέα εγκατάσταση και κάθε φορά που γίνεται μια επέκταση, προσθήκη ή αναβάθμιση.

Σχετικά με το πρόβλημα της ασφάλειας, μια μορφή βέλτιστων πρακτικών (best practices) περιλαμβάνει την εκπαίδευση των προγραμματιστών σε θέματα ασφάλειας λογισμικού. Μια αποτελεσματική μορφή εκπαίδευσης θα πρέπει να περιλαμβάνει τα εξής: την περιγραφή του προβλήματος, την τεχνολογία ασφάλειας (security engineering), τις αρχές και οδηγίες σχεδίασης, τους κινδύνους που πρέπει να λαμβάνονται υπ' όψιν στην υλοποίηση, τα πιθανά ελαττώματα στη σχεδίαση και το πώς να αποφεύγονται, τις τεχνικές ανάλυσης, την εκμετάλλευση σφαλμάτων στο λογισμικό (software exploits) και τον έλεγχο ασφάλειας (security testing).

1.2.1 Κίνδυνος και ασφάλεια

Ο καθορισμός των απαιτήσεων ασφάλειας για ένα δεδομένο σύστημα, καθώς και η επιλογή των κατάλληλων μηχανισμών ασφάλειας αποτελούν μέρος της διαχείρισης κινδύνου (risk management). Τα βασικά βήματα είναι η ανάλυση της αξίας και της κριτικής διάθεσης, η ανάλυση της ευπάθειας, ο προσδιορισμός της

απειλής, η ανάλυση κινδύνου (risk analysis), η αξιολόγηση κινδύνου (risk assessment), η επιλογή των μέτρων ασφάλειας, η ανάπτυξη και η εφαρμογή των σχεδίων για απρόοπτα γεγονότα και η επισκόπηση της αποτελεσματικότητας [Turn R., (1986)]. Αυτά τα βήματα μπορεί να είναι δύσκολο να εφαρμοστούν στην πράξη.

Η διαχείριση κινδύνου χρησιμοποιεί την ανάλυση κινδύνου, την ανάλυση απειλής και άλλες τεχνικές για να ελεγχθεί ο κίνδυνος για τα αγαθά. Αναπτύσσει πολιτικές ασφαλείας, διαδικασιών, προτύπων και οδηγιών. Η αποτελεσματική διαχείριση ασφάλειας εξαρτάται από την ορθή διαχείριση κινδύνου, η οποία βασίζεται σε μία αξιόπιστη αξιολόγηση-αποτίμηση κινδύνου (risk assessment), που περιλαμβάνει τη συλλογή δεδομένων που επηρεάζουν τον κίνδυνο των υπολογιστικών συστημάτων.

Παρατηρούμε λοιπόν ότι ο περιορισμός του κινδύνου πληροφοριών εστιάζεται στην ασφάλεια πληροφοριών με κατάλληλες πολιτικές ασφάλειας. Η πολιτική ασφάλειας (security policy) καθορίζει σε γενικές γραμμές, τι επιτρέπεται και τι απαγορεύεται σε μία εγκατάσταση, ένα σύστημα, μία εφαρμογή κ.τ.λ. Οι πολιτικές υπαγορεύουν μέτρα ασφάλειας και στη συνέχεια, τα μέτρα ασφάλειας υλοποιούνται με μηχανισμούς ασφάλειας. Πρόκειται για ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μία επιχείρηση ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του. Μόλις καθοριστεί η πολιτική ασφάλειας που θα εξυπηρετήσει τις ανάγκες για τις οποίες κλήθηκε, το επακόλουθο στάδιο είναι να επιβληθεί. Για να πραγματοποιηθεί αυτό, η επιχείρηση αναπτύσσει ένα μίγμα διαδικασιών και τεχνικών μηχανισμών.

Ο καταληκτικός στόχος της ασφάλειας πληροφοριών είναι να καθορίσει την αποτελεσματικότητα των μέτρων που λαμβάνονται, προκειμένου να προστατεύσουν τις πληροφορίες από τον κίνδυνο. Όσο πληρέστερο και καλύτερο είναι το μοντέλο κινδύνου, τόσο καλύτερες αποφάσεις ασφάλειας μπορούν να λαμβάνονται χρησιμοποιώντας τις προβλέψεις της.

1.2.2 Βασικοί όροι στο πλαίσιο της ασφάλειας λογισμικού εφαρμογών

Ως αγαθό (asset) ορίζεται κάθε αντικείμενο ή πόρος το οποίο αξίζει να προστατευθεί. Διακρίνονται σε: 1. Φυσικά Αγαθά (Physical Assets): όπως κτίρια, υπολογιστές, δικτυακή υποδομή, έπιπλα, κ.τ.λ., 2. Αγαθά Δεδομένων (Data Assets): όπως αρχεία (ηλεκτρονικά, έντυπα) και 3. Αγαθά Λογισμικού (Software Assets): όπως λογισμικό εφαρμογών, λειτουργικά συστήματα, κ.τ.λ.

Ως *συνέπεια* (impact) ή αντίκτυπος ή επίπτωση ορίζεται η απώλεια που θα προκληθεί από την προσβολή ενός αγαθού. Οι συνέπειες διακρίνονται σε: Άμεσες Συνέπειες (π.χ. κόστος επαναγοράς και διαμόρφωσης) και Έμμεσες Συνέπειες (π.χ. πρόκληση δυσφήμησης, νομικές συνέπειες, απώλειες από διακοπή ή παρεμπόδιση λειτουργιών, κοινωνικές συνέπειες κ.ά.).

Απειλή (threat) είναι η ένδειξη του ότι επίκειται κάποιος κίνδυνος ή κάποιο κακό για την εφαρμογή ή το σύστημα γενικότερα. Είναι ο πιθανός κίνδυνος μιας επικείμενης επίθεσης που μπορεί να βλάψει την εφαρμογή. Πιο συγκεκριμένα είναι οποιαδήποτε περίπτωση ή γεγονός με δυνατότητα πρόκλησης ζημιάς σε ένα σύστημα υπό μορφή καταστροφής, κοινοποίησης, τροποποίησης των στοιχείων του, ή/και άρνησης της υπηρεσίας. Απειλή είναι το ενδεχόμενο ότι το σύστημα δεν θα είναι σε

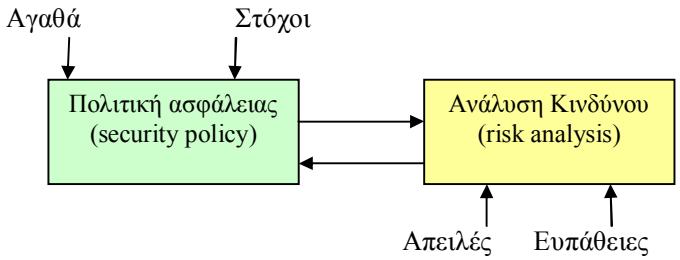
θέση να επιβάλει την πολιτική ασφαλείας του (συμπεριλαμβανομένης της συνέχειας των κρίσιμων διαδικασιών) σε μια επίθεση.

*Ε*υπάθεια (vulnerability) ονομάζεται μια «τρύπα» ή μια αδυναμία της εφαρμογής, η οποία μπορεί να οφείλεται σε μια ατέλεια στη σχεδίαση ή ένα σφάλμα υλοποίησης. Αυτή επιτρέπει σε έναν επιτιθέμενο να βλάψει τους ιδιοκτήτες και τους νόμιμους χρήστες της εφαρμογής, ή άλλες οντότητες, που βασίζονται στην εφαρμογή. Ο όρος της ευπάθειας πολύ συχνά χρησιμοποιείται εσφαλμένα. Οι ευπάθειες ενός συστήματος χωρίζονται σε σφάλματα (bugs) και ελαττώματα (flaws). Τα σφάλματα είναι ευπάθειες που εντοπίζονται αποκλειστικά στον κώδικα, ενώ τα ελαττώματα είναι ευπάθειες που είναι πιο εγγενείς, καθώς προέρχονται από κακή σχεδίαση. Σύμφωνα με τη Microsoft, περίπου το 50% των ευπαθειών είναι ελαττώματα. Η ευπάθεια πρέπει να διακρίνεται από τους όρους: απειλή (threat), επίθεση (attack) και αντίμετρα (countermeasures). Οι απειλές είναι αναγκαίο να εκμεταλλευτούν συγκεκριμένες ευπάθειες, προκειμένου να προκαλέσουν ένα περιστατικό ασφάλειας. Επιπλέον, οι απειλές, οι ευπάθειες, και οι επιδράσεις τους πρέπει να συνδυαστούν ώστε να παράσχουν μια μονάδα μέτρησης του κινδύνου.

Εκμετάλλευση (exploit) ή αλλιώς «αδυναμίες - κενά - τρύπες». Αυτές αποτελούν ένα μικρό μέρος του λογισμικού, στο οποίο εντοπίζονται προγραμματιστικά σφάλματα. Τα σφάλματα αυτά οδηγούν συνήθως σε μη εξουσιοδοτημένη πρόσβαση στο σύστημα ή/και σε κατάρρευση τύπου άρνησης παροχής υπηρεσιών του δικτύου του πληροφοριακού συστήματος. Οι εκμεταλλεύσεις προσδιορίζουν έναν προκαθορισμένο τρόπο παραβίασης της ασφάλειας ενός πληροφοριακού συστήματος σε μια ευπάθεια. Κατηγοριοποιούνται σε εκείνα που εκμεταλλεύονται αδυναμίες του συστήματος με σκοπό την πρόσβαση σε αυτό και σε εκείνα που στοχεύουν στην απόκτηση περισσότερων δικαιωμάτων μέσα στο σύστημα. Οι αναλυτές με την χρήση κατάλληλων εργαλείων προσπαθούν να εντοπίσουν «κενά» που βασίζονται στη λανθασμένη ή μη παραμετροποίηση του λειτουργικού συστήματος, του δικτύου και των προεγκατεστημένων εφαρμογών του συστήματος. Η εύρεση τέτοιων «κενών» ασφάλειας και η διόρθωση τους, μπορούν να αποτρέψουν μια πιθανή επίθεση στο σύστημα ή δίκτυο-στόχο.

Τα αντίμετρα - μέτρα προστασίας (ή έλεγχοι ασφάλειας) (safeguards, countermeasures) είναι οι ενέργειες οι οποίες περιορίζουν τον κίνδυνο να υποστεί ζημιά ένα αγαθό. Περιλαμβάνουν τεχνολογίες ή μοντέλα άμυνας, που χρησιμοποιούνται με σκοπό να ανιχνεύσουν ή να αποτρέψουν επιθέσεις. Τα αναγκαία αντίμετρα σε μια εφαρμογή πρέπει να αναγνωρισθούν με τη χρήση της ανάλυσης κινδύνου, έτσι ώστε να διασφαλιστεί ότι η εφαρμογή προστατεύεται από κοινούς τύπους επιθέσεων. Μια αδυναμία ή μια ατέλεια στη σχεδίαση ενός αντιμέτρου ή η έλλειψη του αναγκαίου αντιμέτρου, έχει ως αποτέλεσμα μια ευπάθεια, η οποία μπορεί να είναι σε θέση να καταστήσει την εφαρμογή ευάλωτη σε επιθέσεις.

Για να εξεταστούν αυτά τα προβλήματα, χρησιμοποιείται ο έλεγχος (control, testing) ως προστατευτικό μέτρο. Ο έλεγχος αποτελεί μια δράση, μια διαδικασία ή μια τεχνική που εξαλείφει ή μειώνει σε επίπεδο διαβαθμίσεων την ευπάθεια. Ο [Turn R., (1986)] περιγράφει τη συσχέτιση μεταξύ των απειλών, των ελέγχων και των ευπαθειών με τον εξής τρόπο: «Μια απειλή εμποδίζεται από τον έλεγχο μιας ευπάθειας».



Σχήμα 1. Πολιτική Ασφάλειας και Ανάλυση Κινδύνου.

1.2.3 Αρχιτεκτονική και υποδομή ασφάλειας

Με τον όρο αρχιτεκτονική ασφάλειας (security architecture) εννοούμε τη θεώρηση για το πώς τα συστήματα (με την ευρεία έννοια) μίας επιχείρησης πρέπει να σχεδιαστούν προκειμένου να εξασφαλίζουν ότι η επιχείρηση ικανοποιεί τους στόχους της ασφάλειας.

Η υποδομή ασφάλειας (security infrastructure) είναι η πραγματοποίηση της αρχιτεκτονικής ασφάλειας σε απτή και λειτουργική μορφή. Ο στόχος της ασφάλειας (security objective) συνίσταται στη διατήρηση των ιδιοτήτων της ασφάλειας σε αποδεκτό επίπεδο. Ο όρος *στόχος ασφάλειας* δεν πρέπει να συγχέεται με τις υπηρεσίες ασφάλειας, οι οποίες αποτελούν τη διαδικαστική ή επικοινωνιακή υπηρεσία που παρέχεται από το σύστημα προκειμένου να προσδώσει συγκεκριμένα είδη προστασίας στους πόρους του. Συνεπώς, οι στόχοι ασφάλειας είναι οι τελικοί στόχοι που πρέπει να επιτευχθούν, ενώ οι υπηρεσίες ασφάλειας είναι τα μέσα επίτευξης των στόχων αυτών. Έτσι, προκύπτουν τα ακόλουθα:

- Προσδιορισμός (identification) του συστήματος και των συνιστωσών του.
- Προσδιορισμός των αγαθών του συστήματος και της αξίας τους στο σύστημα.
- Στόχοι ασφάλειας για τα αγαθά.
- Οι απειλές και οι ευπάθειες τις οποίες αντιμετωπίζουν ή θα αντιμετωπίσουν τα αγαθά.
- Αξιολόγηση της διαδικασίας ασφάλειας μέσω της διαχείρισης κινδύνου.
- Σχεδιασμός και καθιέρωση των αρχών ασφάλειας, που θα εφαρμοστούν στο επιχειρησιακό σύστημα.

1.3 Αξιολόγηση ασφάλειας (security assessment)

Ο ορισμός της αξιολόγησης της ασφάλειας είναι ένας σχετικά νέος όρος στον τομέα της ασφάλειας της πληροφορικής. Ο όρος αυτός χρησιμοποιείται και ερμηνεύεται λανθασμένα πολλές φορές από τις εταιρείες που θέλουν να εμπλακούν στο χώρο της ασφάλειας της πληροφορικής. Οι λόγοι που οδηγούν στην παρερμηνεία είναι είτε επειδή χρησιμοποιούν την δική τους εταιρική ορολογία, είτε λόγω άγνοιας του αντικειμένου.

Η αξιολόγηση της ασφάλειας στην τεχνολογία πληροφοριών (IT security assessment) είναι μια μελέτη για να ευρεθούν οι ευπάθειες και οι κίνδυνοι ασφάλειας. Στόχος μιας αξιολόγησης της ασφάλειας (επίσης γνωστής και ως έλεγχος ασφάλειας-security audit ή επισκόπηση ασφάλειας-security review), είναι να εξασφαλιστεί ότι οι απαραίτητοι έλεγχοι ασφάλειας είναι ενσωματωμένοι στον σχεδιασμό και την εφαρμογή ενός έργου (project).

Επομένως, η αξιολόγηση της ασφάλειας είναι η διαδικασία ελέγχου της τρωτότητας ως προς της ασφάλεια του συστήματος και δικτύου μιας εταιρείας ή ενός

οργανισμού. Η αξιολόγηση αυτή εστιάζει στις τρέχουσες διαδικασίες του συστήματος παρά σε θεωρητικά ζητήματα ασφάλειας του συστήματος. Η διαδικασία αυτή μπορεί να είναι αρκετά αναλυτική, χρονοβόρα και να ενσωματώνει πολλούς επιμέρους εσωτερικούς ελέγχους. Το πόσο αναλυτική θα είναι αφορά τόσο τη δομή και τις διαδικασίες της εταιρείας, όσο και μέχρι ποιο βαθμό αξιολόγησης θέλει η εταιρεία να προχωρήσει. Στο τέλος, τα αποτελέσματα της αξιολόγησης συνήθως καταγράφονται σε μια αναφορά. Στην αναφορά αυτή παρουσιάζεται μια σύνοψη των αποτελεσμάτων του ελέγχου ανά κριτήριο, καθώς επίσης και των προτεινόμενων λύσεων και στρατηγικών που καλείται να ακολουθήσει η εταιρεία για την βελτίωση της ασφάλειάς της.

Η ασφάλεια δεν αποτελεί μια απλή στατική διαδικασία που μια εταιρεία πρέπει να την λαμβάνει υπόψη της μόνο στην αρχή υλοποίησης του δικτύου της και του συστήματός της και ύστερα να την παραμελεί. Η ασφάλεια είναι σημαντικό να γίνει ένα αναπόσπαστο μέρος του σχεδιασμού ενός οργανισμού. Η συνεχόμενη ανάπτυξη νέων τεχνολογικών επιτευγμάτων και προγραμμάτων, μας αναγκάζουν να θεωρούμε την ασφάλεια σαν μια δυναμική διαδικασία ώστε να καταφέρνουμε να είμαστε πάντα προετοιμασμένοι έναντι νέων απειλών.

Ένα επιπλέον στοιχείο το οποίο θα πρέπει να σκεφτούμε για την σημασία της αξιολόγησης ασφάλειας, είναι το γεγονός ότι μαζί με την βελτίωση των τεχνολογικών εφαρμογών, βελτιώνονται και τα εργαλεία που χρησιμοποιούν οι διάφοροι επίδοξοι εισβολείς. Άρα, είναι επακόλουθο να αυξάνονται και οι ηλεκτρονικές απειλές.

Ο μόνος τρόπος ώστε να μπορέσουμε να ελαχιστοποιήσουμε τις πιθανότητες απειλής στα συστήματά μας είναι η πρόληψη. Σε αυτή την φάση, μπορεί να μας βοηθήσει ένας αξιολογητής ασφάλειας (security tester). Το άτομο αυτό είναι ένας «ηθικός» (ethical) hacker και αμείβεται για να μπορέσει να εισβάλει στο σύστημα του οργανισμού με σκοπό να αξιολογήσει το επίπεδο ασφάλειάς του. Το συγκεκριμένο άτομο θα προσπαθήσει να ανιχνεύσει τις ευπάθειες-τρωτά σημεία στο σύστημα και θα φθάσει σε κάποια συμπεράσματα σχετικά με την ασφάλεια. Η αξιολόγηση ασφάλειας που θα πραγματοποιηθεί από ένα τέτοιο άτομο, θα παρουσιάσει μια συνολική εικόνα για την αξιοπιστία των συστημάτων μας. Οι διαδικασίες που πρέπει να ακολουθήσει σε μια τέτοιου είδους αξιολόγηση, συνήθως εξαρτάται από τη μεθοδολογία αξιολόγησης (καθώς και τα εργαλεία που την υποστηρίζουν) την οποία θα επιλέξει ο οργανισμός.

1.3.1 Βασικές μέθοδοι ελέγχου ασφάλειας των εφαρμογών ιστού

Για τη διατήρηση της ασφάλειας ενός συστήματος, το οποίο συνδέεται στο Διαδίκτυο, είναι σημαντικό να πραγματοποιούνται συνεχείς έλεγχοι της ασφάλειας των διαδικτυακών εφαρμογών. Άλλωστε για τη λειτουργία ενός ιστοτόπου, «τρέχουν» πολλές και διαφορετικές εφαρμογές ιστού. Υπάρχουν διάφοροι τρόποι με τους οποίους μπορεί να διεξαχθεί ένας έλεγχος ασφάλειας. Οι βασικές μέθοδοι ελέγχου ασφάλειας των εφαρμογών ιστού είναι:

- Επιθεώρηση Ασφάλειας (security audit): Είναι μία συστηματική, ανεξάρτητη επανεξέταση για την επαλήθευση της ύπαρξης και εφαρμογής των στοιχείων της επιχειρησιακής ασφάλειας. Εφαρμόζει μία καλώς ορισμένη διαδικασία επανεξέτασης που επιβεβαιώνει τη συνοχή και επιτρέπει στον ελεγκτή να βγάλει ασφαλή συμπεράσματα. Το σύστημα ελέγχεται με βάση ένα σύνολο από λίστες ή ερωτηματολόγια ελέγχου (checklists), που διαμορφώνονται σύμφωνα με διεθνή πρότυπα ασφάλειας, καθώς και κατάλληλες πολιτικές

ασφάλειας του οργανισμού, που χρησιμοποιεί την εφαρμογή ιστού. Οι ελεγκτές πραγματοποιούν προσωπικές συνεντεύξεις, ανιχνεύσεις αδυναμιών, εξετάσεις των ρυθμίσεων, αναλύσεις των διαμοιρασμένων πόρων δικτύου και μελέτες των αρχείων καταγραφής (log files).

- Αυτοαξιολόγηση Ασφάλειας (security self-assessment): Σε αυτήν τη μέθοδο δεν χρησιμοποιούνται συγκεκριμένα πρότυπα με βάση τα οποία θα αξιολογηθεί το σύστημα αλλά ούτε και λίστες ελέγχου (checklists). Είναι ένας λεπτομερής έλεγχος για τον εντοπισμό ευπαθειών, ο οποίος προχωρά και σε προτάσεις για επιδιορθώσεις και βελτιώσεις. Το πλεονέκτημα αυτού του ελέγχου είναι το γεγονός ότι μπορεί να καθορίζει επίπεδα προτεραιότητας σε κάθε συστατικό της περιοχής που αξιολογείται. Επομένως, αφού ολοκληρωθεί ο έλεγχος μπορεί να δοθεί μια σειρά προτεραιότητας σε ότι αφορά την επιδιόρθωση των ευπαθειών που βρέθηκαν.
- Έλεγχος Διείσδυσης (penetration testing ή "ethical hacking"): Επίσης γνωστή και ως εσωτερική επιθεώρηση ασφάλειας (internal security auditing). Αποτελεί μια προσομοίωση επίθεσης (attack simulation), η οποία είναι ελεγχόμενη και χρησιμοποιεί παρόμοια εργαλεία και τεχνικές που χρησιμοποιούνται από κακόβουλους εισβολείς. Σκοπός είναι να εντοπιστούν και να απομονωθούν οι ευπάθειες του συστήματος ή του δικτύου για την ασφάλειά του, καθώς και διερευνηθεί κατά πόσο είναι δυνατόν ένας εξωτερικός προς το σύστημα χρήστης, κάνοντας χρήση αυτών των αδυναμιών, να είναι σε θέση να δημιουργήσει προβλήματα. Κατά τη διάρκεια του ελέγχου διείσδυσης διασφαλίζεται η σωστή λειτουργία όλων των συστημάτων, έτσι ώστε να μην μπορούν να παραβιαστούν και να μην επηρεαστούν τα δεδομένα τους. Αυτό που προσπαθεί ο αμυνόμενος να πετύχει με τον έλεγχο διείσδυσης, είναι να κατανοήσει ο ίδιος τους κινδύνους του συστήματός του, δηλαδή τις απειλές που υπάρχει περίπτωση να συναντήσει, καθώς και να βρει τρόπο ώστε να μειώσει τα τρωτά σημεία. Ο έλεγχος μπορεί να πραγματοποιηθεί στη βάση μηδενικής γνώσης (zero knowledge) ή με πλήρη γνώση (full knowledge) του συστήματος, που ελέγχεται.

  Ο έλεγχος διείσδυσης συχνά αποτελεί την καλύτερη μέθοδο διότι συγκεντρώνει τα εξής στοιχεία: απαιτεί ελάχιστο προσωπικό και δεν είναι αναγκαία η μετακίνησή αυτού, είναι πιο οικονομικός από τις δύο άλλες μεθόδους, παρέχει τη δυνατότητα πλήρους αυτοματοποίησης, είναι λιγότερο χρονοβόρος και επαναλαμβάνεται εύκολα, δεν απαιτεί τη σε βάθος γνώση της ελεγχόμενης εφαρμογής και δε διαταράσσει τη λειτουργία της. Ο έλεγχος διείσδυσης χρησιμοποιεί δυο διαφορετικές προσεγγίσεις τεχνικών ελέγχου:

  I. Χειροκίνητος (manual) έλεγχος, όπου ο έλεγχος πραγματοποιείται βήμα προς βήμα χωρίς να υπάρχουν αυτοματισμοί για την επανάληψη παρόμοιων βημάτων.
  II. Αυτοματοποιημένος (automated) έλεγχος, όπου γίνεται χρήση εργαλείων ώστε οι έλεγχοι να εκτελούνται αυτόματα. Η συγκεκριμένη προσέγγιση περιλαμβάνει τις παρακάτω τεχνικές:
      - Black box: Σκοπός είναι η απόκτηση πρόσβασης σε κρίσιμες πληροφορίες χωρίς γνώση και χωρίς να υπάρχει φυσική πρόσβαση στις εγκαταστάσεις του οργανισμού-στόχου. Το χαρακτηριστικό της είναι ότι προσομοιάζει την κατάσταση στην οποία ο κακόβουλος ή επιτιθέμενος χρήστης δεν έχει πρόσβαση και γνώση για τον οργανισμό.

- White box: Ο ελεγκτής έχει πλήρη ή μερική γνώση -ανάλογα με το εύρος του έργου- και στόχο τη δημοσίευση κρίσιμων πληροφοριών του οργανισμού πελάτη. Γνωρίζει τις εφαρμογές που τρέχουν και τα διαγράμματα της αρχιτεκτονικής του συστήματος.
- Gray box: ο ελεγκτής εκτελεί την επίθεση έχοντας περιορισμένη γνώση της υποδομής και των μηχανισμών άμυνας του οργανισμού-στόχου. Είναι μια προσομοίωση μιας συστηματικής επίθεσης από καλά προετοιμασμένους εξωτερικούς επιτιθεμένους ή από άτομα στο εσωτερικό του οργανισμού με περιορισμένη πρόσβαση και προνόμια.

Στα επόμενα κεφάλαια, περιγράφονται οι βασικές μεθοδολογίες αξιολόγησης της ασφάλειας λογισμικού εφαρμογών ανοικτού κώδικα, καθώς και οι βασικοί στόχοι, η εμβέλεια, οι μέθοδοι ελέγχου που χρησιμοποιούν και τα αντίστοιχα εργαλεία που τις υποστηρίζουν, ενώ στη συνέχεια παρατίθεται μία συγκριτική αξιολόγηση των μεθοδολογιών αναδεικνύοντας τα ισχυρά σημεία και τις αδυναμίες της κάθε μίας.

Κεφάλαιο 2: OSSTMM - Open Source Security Testing Methodology (έκδοση 2.2)

2.1 Γενικά

Το OSSTMM είναι ένα εγχειρίδιο για τον έλεγχο (testing) και την ανάλυση της ασφάλειας, το οποίο δημιουργήθηκε από τον Pete Herzog το 2001 και παρέχεται από την ISECOM, ένα μη κερδοσκοπικό ίδρυμα για την ασφάλεια και τις ανοικτές μεθοδολογίες (Institute for Security & Open Methodologies). Η συγκεκριμένη μεθοδολογία, η οποία καλύπτει το τι, το πότε και το που σε ό,τι αφορά τον έλεγχο, είναι ελεύθερη να χρησιμοποιηθεί και διανέμεται υπό την Open Methodology License (OML) - Άδεια Ανοικτής Μεθοδολογίας. Το εγχειρίδιο του OSSTMM συνολικά, είναι επίσης ελεύθερο, απελευθερωμένο υπό την άδεια Creative Commons 3.0 Attribution-NonCommercial-NoDerivs. Η έκδοση 2.2 (Version 2.2) της μεθοδολογίας ελέγχου είναι σήμερα διαθέσιμη και η πλήρως αναθεωρημένη έκδοση 3.0 (version 3.0) πρόκειται να δημοσιευθεί σύντομα. Αξίζει να σημειωθεί ότι στην έκδοση 2.2, το OSSTMM περιλαμβάνει αρκετές πληροφορίες από την έκδοση 3.0 της μεθοδολογίας.

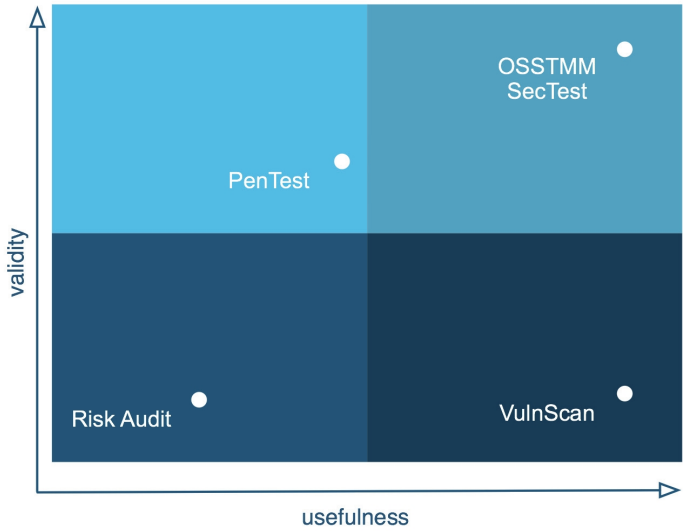
Ο στόχος αυτού του εγχειριδίου είναι να δημιουργηθεί μια αποδεκτή μέθοδος για έναν λεπτομερή έλεγχο ασφάλειας. Λεπτομέρειες όπως τα πιστοποιητικά του ελεγκτή (tester) ασφάλειας, το μέγεθος της εταιρίας ασφάλειας, η χρηματοδότηση ή υποστήριξη προμηθευτών, θα έχουν επίπτωση στην κλίμακα και στην πολυπλοκότητα του ελέγχου. Κάθε ειδικός δικτύων ή ασφάλειας που καλύπτει τις απαιτήσεις που σκιαγραφούνται σε αυτό το εγχειρίδιο, θα έχει κατορθώσει να δημιουργήσει ένα ολοκληρωμένο προφίλ ασφάλειας του συστήματος. Πρέπει να σημειωθεί ότι σε καμία περίπτωση δεν συστήνεται να ακολουθηθεί η μεθοδολογία ως ένα διάγραμμα ροής. Είναι μια σειρά από βήματα που πρέπει να θεωρηθούν, πιθανότατα πολλαπλές φορές, κατά τη διάρκεια της εκτέλεσης ενός λεπτομερούς ελέγχου. Το διάγραμμα μεθοδολογίας που παρέχεται αφορά στον βέλτιστο τρόπο να διενεργηθεί ο έλεγχος με δύο ελεγκτές, εντούτοις οποιοσδήποτε αριθμός ελεγκτών μπορεί να χρησιμοποιηθεί. Το πιο σημαντικό σε αυτήν την μεθοδολογία είναι ότι οι διάφοροι επιμέρους έλεγχοι αξιολογούνται και εκτελούνται όπου είναι εφαρμόσιμο μέχρι να προκύψουν τα αναμενόμενα αποτελέσματα μέσα σε ένα δεδομένο χρονικό πλαίσιο. Μόνο τότε ο ελεγκτής θα έχει εξετάσει τον έλεγχο σύμφωνα με το πρότυπο OSSTMM. Μόνο τότε η έκθεση, θα θεωρηθεί επαρκώς λεπτομερής.

Μερικοί ελεγκτές ασφάλειας θεωρούν ότι ένας έλεγχος ασφάλειας είναι απλά "ένα σημείο στο χρόνο" (μια άποψη αμυντικής στάσης) και παρουσιάζουν την έξοδο (output) από τους ελέγχους ως "στιγμιότυπο ασφάλειας". Το καλούν στιγμιότυπο επειδή εκείνη την στιγμή οι γνωστές ευπάθειες, αδυναμίες και διαμορφώσεις δεν έχουν αλλάξει. Είναι όμως επαρκές αυτό το στιγμιότυπο; Η μεθοδολογία που προτείνεται στο εγχειρίδιο του OSSTMM οδηγεί σε αποτύπωση περισσοτέρων στιγμιοτύπων. Οι Τιμές Αξιολόγησης Κινδύνου (Risk Assessment Values - RAVs) θα ενισχύσουν αυτά τα στιγμιότυπα με τις διαστάσεις της συχνότητας και ενός πλαισίου συγχρονισμού στους ελέγχους ασφάλειας. Επομένως, το στιγμιότυπο αναβαθμίζεται σε ένα προφίλ, το οποίο περιλαμβάνει μια σειρά μεταβλητών που αφορούν μια χρονική περίοδο, πριν η εκτίμηση κινδύνου υποβιβασθεί κάτω από ένα αποδεκτό επίπεδο. Στην έκδοση 2.5 του OSSTMM έχει εξελιχθεί ο ορισμός και η εφαρμογή των RAVs προκειμένου να μετρηθεί ακριβέστερα αυτό το επίπεδο κινδύνου. Τα RAVs παρέχουν συγκεκριμένους ελέγχους σε συγκεκριμένα χρονικά διαστήματα, τα

οποία είναι κυκλικής φύσεως και ελαχιστοποιούν τον κίνδυνο που διατρέχει κάποιος σε οποιαδήποτε αμυντική στάση.

Κάποιοι μπορεί να αναρωτηθούν: "Αξίζει να έχουμε μια τυποποιημένη μεθοδολογία για τους ελέγχους ασφάλειας;" Η απάντηση είναι ότι η ποιότητα της εξόδου (output) και τα αποτελέσματα ενός ελέγχου ασφάλειας είναι δύσκολο να μετρηθούν χωρίς μια τέτοια μεθοδολογία. Πολλές μεταβλητές έχουν επίπτωση στην έκβαση ενός ελέγχου, συμπεριλαμβανομένου του προσωπικού ύφους και της προκατάληψης του ελεγκτή. Εξαιτίας όλων αυτών των μεταβλητών είναι σημαντικό να καθοριστεί ο σωστός τρόπος για έναν έλεγχο, ο οποίος να βασίζεται σε βέλτιστες πρακτικές (best practices) και σε μια γενικότερη συναίνεση. Εάν μπορούμε να μειώσουμε το ποσό της προκατάληψης στον έλεγχο, θα καταφέρουμε να μειώσουμε πολλές ψευδείς υποθέσεις και παραδοχές και θα αποφύγουμε τα αποτελέσματα μέτριας ποιότητας. Ο περιορισμός και η καθοδήγηση των προκαταλήψεων, καθιστά τους καλούς ελεγκτές ασφάλειας καλύτερους και παρέχει στους αρχαρίους την κατάλληλη μεθοδολογία ώστε να διεξάγουν τους σωστούς ελέγχους στις σωστές περιοχές.

Συνοψίζοντας, το OSSTMM είναι μια ανοικτή μεθοδολογία για τον έλεγχο και την εξαγωγή μετρικών ασφάλειας που έχει ελεγχθεί από πολλούς ειδικούς χωρίς να περιορίζεται σε κάποιο συγκεκριμένο κατασκευαστή ή τεχνολογία. Ολόκληρη η μεθοδολογία εστιάζει κυρίως στο ποιες ακριβώς είναι οι τεχνικές λεπτομέρειες που πρόκειται να εξεταστούν, στο τι πρέπει να προσεχθεί κατά τη διαδικασία του ελέγχου από την προετοιμασία μέχρι την αξιολόγηση (μετά τον έλεγχο) και προ πάντων, στο πώς τα αποτελέσματα πρέπει να αξιολογηθούν και να μετρηθούν. Οι έλεγχοι για βέλτιστες πρακτικές (best practices) και πρότυπα (standards) όπως BSI, ISO κ.λπ., καθώς επίσης, οι κανονισμοί και η νομοθεσία ενημερώνονται τακτικά. Το OSSTMM αποδίδει μεγάλη σημασία στον έλεγχο κατά ένα λεπτομερή, συνεπή, διαφανή και, κυρίως, σταθερό τρόπο. Επομένως η μεθοδολογία, όταν χρησιμοποιείται με συνέπεια, παρέχει αποτελέσματα υψηλής ποιότητας. Λαμβάνοντας υπόψη τα παραπάνω, το OSSTMM οριοθετεί τους ελέγχους με έναν σημασιολογικό τρόπο (βλ. Σχήμα 2).

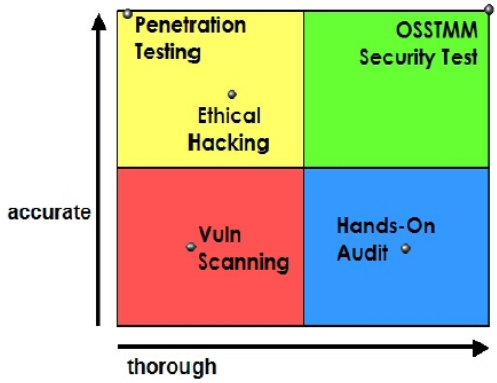


Σχήμα 2. Κατηγοριοποίηση των ελέγχων ως προς τη χρησιμότητα και την ισχύ

2.1.1 Βασικοί στόχοι

2.1.1.1 Εμβέλεια της μεθοδολογίας

Η εμβέλεια της μεθοδολογίας περιλαμβάνει όλα τα συστατικά ενός πλήρους και λεπτομερούς ελέγχου ασφάλειας, τις υπολογισμένες μετρικές από τους ελέγχους, τις έννοιες για τον σχεδιασμό του έργου αποτίμησης της ασφάλειας και τους κανόνες δέσμευσης (rules of engagement) που καλύπτουν τα θέματα επαγγελματικής πρακτικής και δεοντολογίας για την αγορά, εκτέλεση και παράδοση αυτού του ελέγχου κατάλληλα και νόμιμα. Το εγχειρίδιο αυτό δεν πραγματοποιεί καμία υπόθεση βασισμένη στο μέγεθος ή τη θέση του στόχου. Μπορεί να εφαρμοστεί σε οτιδήποτε που πρέπει να εξεταστεί ως προς τη λειτουργική ασφάλεια.



Σχήμα 3. Κατηγοριοποίηση των ελέγχων με βάση το πόσο λεπτομερείς και ακριβείς είναι

2.1.1.2 Σκοπός

Ο κύριος σκοπός της μεθοδολογίας και της τεκμηρίωσης που τη συνοδεύει είναι να παρέχει μια επιστημονική μεθοδολογία για τον ακριβή χαρακτηρισμό της ασφάλειας μέσω της εξέτασης και του συσχετισμού με έναν συνεπή και αξιόπιστο τρόπο. Η μεθοδολογία μπορεί να εφαρμοστεί για τους περισσότερους τύπους ελέγχου πληροφοριακών συστημάτων (Information Systems – IS), συμπεριλαμβάνοντας τους: έλεγχος διείσδυσης (penetration tests), ethical hacking, αξιολογήσεις ασφάλειας (security assessments), αξιολογήσεις ευπάθειας (vulnerability assessments), red-teaming[1], blue-teaming[2], posture assessments[3] και ελέγχους ασφάλειας. Έχει γραφεί ως ερευνητικό έγγραφο ασφάλειας και έχει σχεδιαστεί για την πραγματική επαλήθευση της ασφάλειας και την παρουσίαση μετρικών σε επαγγελματικό επίπεδο.

Ο δευτερεύων σκοπός είναι να παρέχει οδηγίες, οι οποίες όταν ακολουθούνται θα επιτρέψουν στον ελεγκτή να εκτελέσει έναν επικυρωμένο έλεγχο OSSTMM. Αυτές οι οδηγίες υπάρχουν για να διασφαλίσουν τα παρακάτω:

- Ο έλεγχος έχει διεξαχθεί διεξοδικά.
- Ο έλεγχος περιλαμβάνει όλα τα απαραίτητα κανάλια [2.2.1].

[1] Το red-teaming είναι η διαδικασία ανάλυσης ευπαθειών σε ένα δεδομένο σύστημα ή δίκτυο με την εκτέλεση των επιθετικών ενεργειών που εκτιμάται ότι θα εκτελέσει ένας επίδοξος εισβολέας.
[2] Το blue-teaming έχει τους ίδιους στόχους με το red-teaming αλλά η «μπλε ομάδα» δρα ως υπερασπιστής που συνεργάζεται με τους υπεύθυνους για τη λειτουργία των δικτύων ή συστημάτων ώστε να μετριάσει τον κίνδυνο.
[3] Το Security Posture Assessment (SPA) είναι ένα εργαλείο που περιέχει πάνω από 850 μετρήσιμα ανεξάρτητα σημεία δεδομένων, που χρησιμοποιούνται για να μετρήσουν αντικειμενικά την τρέχουσα κατάσταση των κινδύνων ασφάλειας μιας επιχείρησης.

- Όλες οι φάσεις του ελέγχου συμμορφώνονται με τον νόμο.
- Τα αποτελέσματα είναι μετρήσιμα και μπορούν να ποσοτικοποιηθούν.
- Τα αποτελέσματα που λαμβάνονται είναι συνεπή και με δυνατότητα επανάληψης, με την έννοια του ότι αν εκτελέσουμε ξανά τους ίδιους ελέγχους στο ίδιο σύστημα θα λάβουμε τα ίδια αποτελέσματα.
- Τα αποτελέσματα περιέχουν μόνο γεγονότα όπως προέρχονται από τους ίδιους τους ελέγχους.

Ο τελευταίος στόχος είναι να καθοριστεί ένα πρότυπο για μια μεθοδολογία ελέγχου ασφάλειας όπου τα αποτελέσματα να καλύπτουν τις πραγματικές, πρακτικές και λειτουργικές απαιτήσεις ασφάλειας. Ως έμμεσο αποτέλεσμα, δημιουργείται ένας τομέας γνώσης που μπορεί να ενεργήσει ως σημείο αναφοράς σε όλους τους ελέγχους ασφάλειας ανεξάρτητα από το μέγεθος του οργανισμού, της τεχνολογίας ή της προστασίας.

2.1.1.3 Διαπίστευση

Για να παραχθεί ένας έλεγχος πιστοποιημένος κατά OSSTMM, ο οποίος να υπέχει θέση διαπίστευσης για τη λειτουργική ασφάλεια του στόχου, πρέπει να υπογραφεί μια έκθεση ελέγχου OSSTMM (OSSTMM Audit Report) από τον ελεγκτή ή αναλυτή. Η συγκεκριμένη έκθεση υποβάλλεται στην ISECOM για έλεγχο και έκδοση της επίσημης πιστοποίησης OSSTMM. Επομένως, ένας πιστοποιημένος έλεγχος και μια διαπιστευμένη έκθεση δε χρειάζονται για να δείξουν ότι ακολουθήθηκε κάποιο συγκεκριμένο εγχειρίδιο ή οποιεσδήποτε συγκεκριμένες υποενότητες. Χρειάζονται μόνο για να παρουσιάσουν το τι εξετάστηκε και τι δεν εξετάστηκε ώστε να είναι δυνατή η πιστοποίηση.

Ένας πιστοποιημένος έλεγχος OSSTMM παρέχει τα ακόλουθα οφέλη:

- Χρησιμεύει ως απόδειξη ενός πραγματικού ελέγχου.
- Καθιστά τους ελεγκτές υπεύθυνους για τον έλεγχο.
- Παρέχει μια σαφή δήλωση στον πελάτη.
- Παρέχει μια εκτενέστερη επισκόπηση σε σχέση με μια επιτελική σύνοψη.
- Παρέχει μια έγκυρη λίστα ελέγχου (checklist) για τον ελεγκτή.
- Παρέχει σαφώς υπολογισμένες και κατανοητές μετρικές.

2.1.1.4 Πιστοποίηση

Καμία συγκεκριμένη πιστοποίηση δεν απαιτείται προκειμένου να πραγματοποιήσει κανείς έναν έλεγχο OSSTMM. Η πιστοποίηση παρέχεται ως μέσο ανεξάρτητης επικύρωσης και όχι ως απαίτηση για την εφαρμογή του εγχειριδίου. Ο καθένας που χρησιμοποιεί αυτήν τη μεθοδολογία για έλεγχο και ανάλυση ασφάλειας θεωρείται ότι εκτελεί έναν έλεγχο OSSTMM και αναφέρεται ως ελεγκτής OSSTMM (OSSTMM Auditor) με την προϋπόθεση ότι ο έλεγχος και η ανάλυση βασίζονται στη μεθοδολογία σύμφωνα με τα διαθέσιμα εγχειρίδια και τις συστάσεις.

Υπάρχει διαθέσιμη μεμονωμένη πιστοποίηση μέσω ISECOM για δεξιότητες που αναγνωρίζονται σε δυνατότητες επαγγελματικού ελέγχου και ανάλυσης της ασφάλειας. Το OPST (OSSTMM Professional Security Tester), το OPSA (OSSTMM Professional Security Analyst), το OSSTMM Professional Security Expert (OPSE) και το OSSTMM Wireless Security Expert είναι οι επίσημες πιστοποιήσεις για τους ελεγκτές OSSTMM, παρέχοντας τη γνώση ως δεξιότητες που απαιτούνται για να

εφαρμοστεί κατάλληλα το OSSTMM ή οποιοσδήποτε έλεγχος ασφάλειας με επιστημονικό τρόπο.

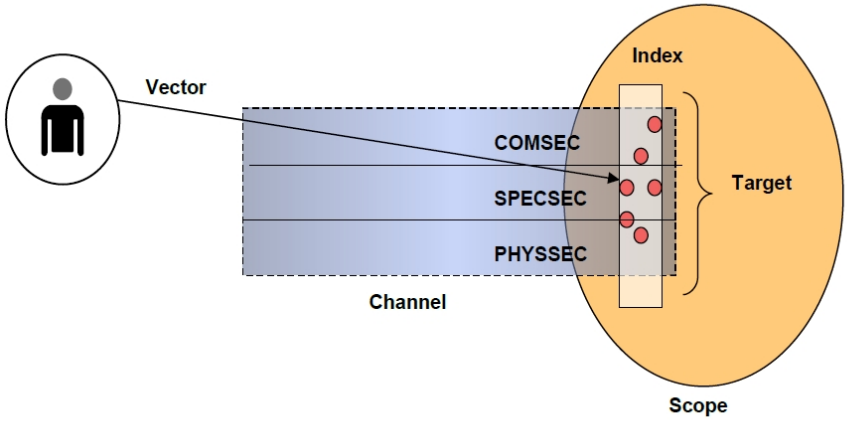
Το εγχειρίδιο της OSSTMM έχει γραφεί ως ερευνητικό έγγραφο ασφάλειας. Έχει σχεδιαστεί για την πιο βέλτιστη και πρακτική μέθοδο επαλήθευσης και μέτρησης της πραγματικής ασφάλειας σε ένα επαγγελματικό επίπεδο. Το πεδίο του εγγράφου δεν περιλαμβάνει άμεση ανάλυση, εντούτοις υπονοείται η ανάλυση κάποιας μορφής με τη χρήση των «αναμενόμενων αποτελεσμάτων- Expected Results» μέσα στη μεθοδολογία. Θα πρέπει να πραγματοποιηθεί κάποια ανάλυση για να βεβαιώσει ότι τουλάχιστον αυτά τα αναμενόμενα αποτελέσματα επιτυγχάνονται.

2.2 Εμβέλεια

2.2.1 Εμβέλεια (The Scope)

Η εμβέλεια είναι το συνολικό πιθανό περιβάλλον λειτουργικής ασφάλειας για οποιαδήποτε αλληλεπίδραση με οποιοδήποτε αγαθό (asset), που μπορεί να περιλαμβάνει επίσης τα φυσικά συστατικά των μέτρων ασφάλειας. Το πεδίο αποτελείται από τρία κανάλια (channels): COMSEC (ασφάλεια επικοινωνιών), PHYSSEC (φυσική ασφάλεια) και SPECSEC (ασφάλεια φάσματος). Τα κανάλια είναι τα μέσα αλληλεπίδρασης με τα αγαθά. Ένα αγαθό είναι αυτό που έχει αξία για τον ιδιοκτήτη. Τα αγαθά μπορεί να είναι φυσική περιουσία όπως χρυσό, άνθρωποι, σχεδιαγράμματα, laptops, το τυπικό τηλεφωνικό σήμα συχνότητας 900 MHz και χρήματα, ή μπορεί να είναι πνευματική περιουσία όπως τα προσωπικά δεδομένα, μια σχέση, ένα εμπορικό σήμα, οι επιχειρησιακές διαδικασίες, οι κωδικοί πρόσβασης και κάτι που λέγεται πάνω από το τηλεφωνικό σήμα των 900 MHz. Η εμβέλεια είναι το σημείο όπου μπορεί να υπάρξει αλληλεπίδραση με ένα κανάλι Η αλληλεπίδραση μπορεί να είναι είτε παθητική (π.χ. snooping[4]), είτε ενεργητική (π.χ. κλοπή). Συχνά, η εμβέλεια εκτείνεται αρκετά πέρα από τα όρια ευθύνης και παρέμβασης του ιδιοκτήτη αγαθών. Στον ορισμό της εμβέλειας απαιτείται να θεωρούνται όλες οι απειλές δυνατές, ακόμα κι αν δεν είναι ιδιαίτερα πιθανές. Αν και πρέπει να καταστεί σαφές ότι ένας έλεγχος ασφάλειας περιορίζει συχνά τις παραμέτρους σε αυτές που είναι εντός ενός ορισμένου εύρους κινδύνου και αγνοεί τους πιο απίθανους κινδύνους, όπως μια έκρηξη ηφαιστείου εκεί όπου κανένα ηφαίστειο δεν υπάρχει.

[4] Το Snooping (κατασκόπευση) είναι η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα ενός άλλου ατόμου ή επιχείρησης. Η πρακτική είναι παρόμοια με τον «ωτακουσμό» (eavesdropping) αλλά δεν περιορίζεται απαραιτήτως στο να αποκτήσει πρόσβαση στα δεδομένα κατά τη διάρκεια της μετάδοσής τους. Το Snooping μπορεί να περιλαμβάνει την περιστασιακή παρατήρηση ενός e-mail που εμφανίζεται στην οθόνη ενός άλλου υπολογιστή ή την παρακολούθηση του τι κάποιος πληκτρολογεί.



Σχήμα 4. Η εμβέλεια και τα κανάλια

Κανάλι	OSSTMM Τμήμα	Περιγραφή
PHYSSEC	Ανθρώπινο	Περιλαμβάνει το ανθρώπινο στοιχείο της επικοινωνίας, όπου η αλληλεπίδραση είναι είτε φυσική ή ψυχολογική.
	Φυσικό	Ο έλεγχος φυσικής ασφάλειας όπου το κανάλι είναι και φυσικής και μη-ηλεκτρονικής φύσης. Περιλαμβάνει το αισθητό στοιχείο της ασφάλειας, όπου η αλληλεπίδραση απαιτεί φυσική προσπάθεια ή ένα πομπό ενέργειας.
SPECSEC	Ασύρματες Επικοινωνίες	Περιλαμβάνει όλες τις ηλεκτρονικές επικοινωνίες, σήματα και εκπομπές που πραγματοποιούνται στο γνωστό ηλεκτρομαγνητικό φάσμα. Περιλαμβάνει το ELSEC για τις ηλεκτρονικές επικοινωνίες, SIGSEC για τα σήματα και EMSEC για τις ασύρματες εκπομπές.
COMSEC	Δίκτυα Δεδομένων	Περιλαμβάνει όλα τα δίκτυα ηλεκτρονικών συστημάτων και δεδομένων όπου η αλληλεπίδραση πραγματοποιείται μέσω καλωδίου και γραμμών ενσύρματου δικτύου.
	Τηλεπικοι-νωνίες	Περιλαμβάνει όλα τα δίκτυα τηλεπικοινωνιών, ψηφιακά ή αναλογικά, όπου η αλληλεπίδραση πραγματοποιείται από το καθιερωμένο τηλέφωνο ή γραμμές δικτύου τύπου τηλεφώνου.

Πίνακας 1 Περιγραφή των καναλιών και τμημάτων κατά OSSTMM

Ενώ ένας λεπτομερής έλεγχος ασφάλειας απαιτεί έλεγχο και στα τρία κανάλια, στην πραγματικότητα, οι έλεγχοι διεξάγονται και ταξινομούνται από την απαιτούμενη πείρα του ελεγκτή και τον απαιτούμενο εξοπλισμό για τον έλεγχο. Τα τρία κανάλια διαχωρίζονται σε πέντε λογικά τμήματα, όπως παρουσιάζει ο Πίνακας 1.

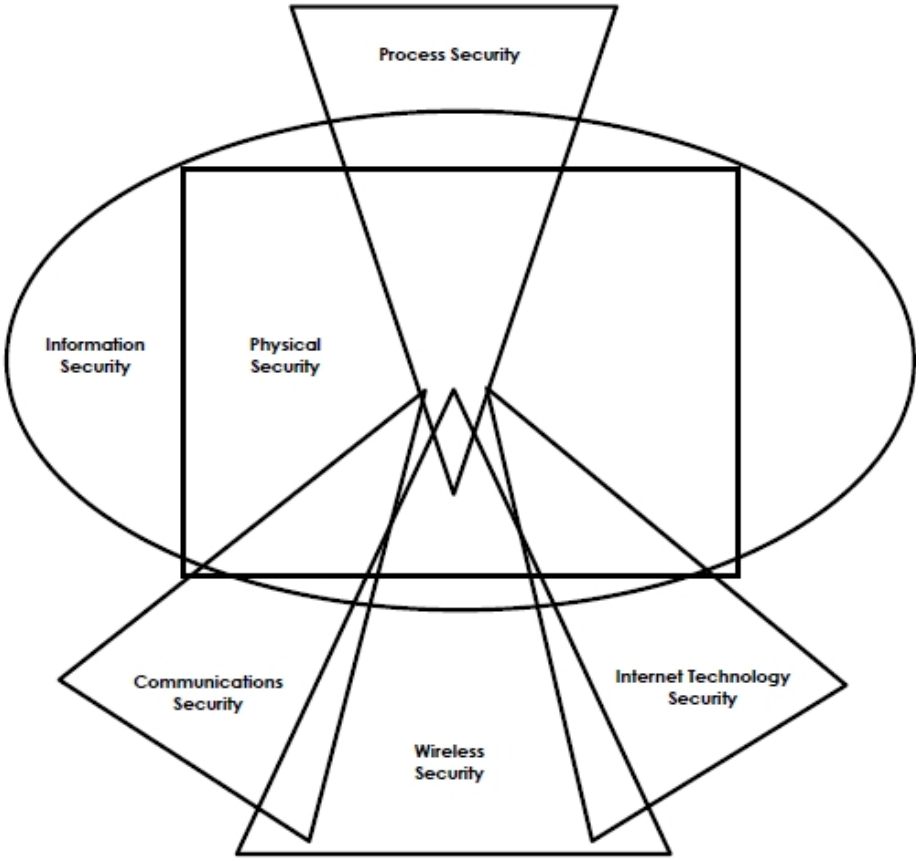
2.2.2 Ο χάρτης ασφάλειας

Ο χάρτης ασφάλειας (security map) είναι μια οπτική απεικόνιση της παρουσίας της ασφάλειας. Η παρουσία της ασφάλειας είναι το περιβάλλον ενός ελέγχου ασφάλειας και αποτελείται από έξι τμήματα (sections), που ουσιαστικά είναι

οι ενότητες του εγχειριδίου της OSSTMM. Τα τμήματα επικαλύπτονται και κάθε τμήμα περιλαμβάνει στοιχεία από όλα τα άλλα τμήματα. Ο κατάλληλος έλεγχος για οποιοδήποτε τμήμα θα πρέπει να περιλαμβάνει, άμεσα ή έμμεσα, τα στοιχεία όλων των άλλων τμημάτων.

Τα τμήματα (sections) στο εγχειρίδιο της OSSTMM είναι:

1. Ασφάλεια Πληροφοριών - Information Security
2. Ασφάλεια Διαδικασιών - Process Security
3. Ασφάλεια Τεχνολογίας Διαδικτύου - Internet Technology Security
4. Ασφάλεια Επικοινωνιών - Communications Security
5. Ασφάλεια Ασύρματων επικοινωνιών - Wireless Security
6. Φυσική Ασφάλεια - Physical Security



Σχήμα 5. Τα τμήματα (sections) του εγχειριδίου της OSSTMM

2.2.2.1 Κατάλογος συνιστωσών του χάρτη ασφάλειας

Ο κατάλογος συνιστωσών του χάρτη ασφάλειας είναι τα πρωτεύοντα στοιχεία της κάθε ενότητας του εγχειριδίου. Κάθε συνιστώσα πρέπει περαιτέρω να περιλαμβάνει όλες τις διαστάσεις ασφάλειας που είναι ενσωματωμένες σε εργασίες που πρέπει να ολοκληρωθούν. Για να θεωρηθεί ότι εκτελούμε έναν έλεγχο ασφάλειας OSSTMM ενός συγκεκριμένου τμήματος, όλες οι συνιστώσες αυτού του τμήματος θα πρέπει να εξεταστούν. Για τις συνιστώσες που η υποδομή ελέγχου δεν υπάρχει, θα πρέπει να χαρακτηριστούν ως «μη εφαρμόσιμες» (non-applicable) στο φύλλο δεδομένων OSSTMM (OSSTMM Data Sheet) συμπεριλαμβανομένης και της τελικής έκθεσης. Οι ενότητες που αντιστοιχούν σε κάθε τμήμα είναι οι παρακάτω:

1. **Έλεγχος Ασφάλειας Πληροφοριών - Information Security Testing**

- Αξιολόγηση Στάσης (Posture Assessment)
- Επισκόπηση Ακεραιότητας Πληροφοριών (Information Integrity Review)
- Έρευνα Συλλογής Πληροφοριών (Intelligence Survey)
- Συλλογή και Ανάλυση Εγγράφων Διαδικτύου (Internet Document Grinding)
- Επισκόπηση Ανθρώπινων Πόρων (Human Resources Review)
- Διερεύνηση Ανταγωνιστικής Συλλογής Πληροφοριών (Competitive Intelligence Scouting)
- Επισκόπηση Ελέγχων Ιδιωτικότητας (Privacy Controls Review)
- Επισκόπηση Ελέγχων Πληροφοριών (Information Controls Review)

2. **Έλεγχος Ασφάλειας Διαδικασιών - Process Security Testing**
    - Επισκόπηση Στάσης (Posture Review[5])
    - Έλεγχος Αιτήματος (Request Testing)
    - Έλεγχος Αντίστροφου Αιτήματος (Reverse Request Testing)
    - Έλεγχος Καθοδηγούμενης Πρότασης (Guided Suggestion Testing)
    - Έλεγχος Έμπιστων Προσώπων (Trusted Persons Testing)

3. **Έλεγχος Ασφάλειας Τεχνολογίας Διαδικτύου - Internet Technology Security Testing**
    - Εφοδιαστικές και Έλεγχοι (Logistics[6] and Controls)
    - Επισκόπηση Στάσης (Posture Review)
    - Επισκόπηση Ανίχνευσης Εισβολής (Intrusion Detection Review)
    - Έρευνα Δικτύων (Network Surveying)
    - Προσδιορισμός Υπηρεσιών Συστήματος (System Services Identification)
    - Διερεύνηση Ανταγωνιστικής Συλλογής Πληροφοριών (Competitive Intelligence Scouting)
    - Επισκόπηση Ιδιωτικότητας (Privacy Review)
    - Συλλογή και Ανάλυση Εγγράφων (Document Grinding)
    - Έλεγχος Εφαρμογών Διαδικτύου (Internet Application Testing)
    - Έρευνα Εκμεταλλεύσεων-αδυναμιών και Επαλήθευση (Exploit Research and Verification)
    - Δρομολόγηση (Routing)
    - Έλεγχος Έμπιστων Συστημάτων (Trusted Systems Testing)
    - Δοκιμή Ελέγχου Πρόσβασης (Access Control Testing)
    - Παραβίαση Κωδικού Πρόσβασης (Password Cracking)
    - Έλεγχος Μέτρων Περιορισμού (Containment Measures Testing)
    - Επισκόπηση Ικανότητας Επιβίωσης (Survivability Review)
    - Έλεγχος Άρνησης Υπηρεσιών (Denial of Service Testing)
    - Επισκόπηση Πολιτικής Ασφάλειας (Security Policy Review)

[5] Posture Review-είναι βέλτιστες πρακτικές, οι κανονισμοί της επιχείρησης του πελάτη, η πολιτική ασφάλειας του πελάτη και τα νομικά ζητήματα για τον πελάτη.

[6] Logistics-είναι η προετοιμασία του περιβάλλοντος ελέγχου καναλιών που απαιτείται, για να αποτραπούν false positives και false negatives τα οποία θα οδηγήσουν τον έλεγχο σε ανακριβή αποτελέσματα.

- Επισκόπηση Καταγραφής και Προειδοποίησης (Alert and Log Review)

4. **Έλεγχος Ασφάλειας Επικοινωνιών - Communications Security Testing**
   - Επισκόπηση Στάσης (Posture Review)
   - Επισκόπηση Ιδιωτικού Τηλεφωνικού Κέντρου-PBX (Private branch exchange-PBX Review)
   - Έλεγχος Φωνητικού Ταχυδρομείο (Voicemail Testing)
   - Έλεγχος FAX (FAX Testing)
   - Έρευνα Διαποδιαμορφωτών (Modem Survey)
   - Δοκιμή Ελέγχου Απομακρυσμένης Πρόσβασης (Remote Access Control Testing)
   - Έλεγχος Τηλεφωνίας πάνω από IP (Voice over IP Testing)
   - Έλεγχος Δικτύων Μεταγωγής X.25 Πακέτων (X.25 Packet Switched Networks Testing)

5. **Έλεγχος Ασφάλειας Ασύρματων επικοινωνιών - Wireless Security Testing**
   - Επισκόπηση Στάσης (Posture Review)
   - Έλεγχος Ηλεκτρομαγνητικής Ακτινοβολίας (Electromagnetic Radiation (EMR) Testing)
   - Έλεγχος Δικτύων 802.11 Ασύρματων επικοινωνιών (802.11 Wireless Networks Testing)
   - Έλεγχος Δικτύων Bluetooth (Bluetooth Networks Testing)
   - Έλεγχος Ασύρματων Συσκευών Εισόδου (Wireless Input Device Testing)
   - Έλεγχος Ασύρματων Φορητών (Wireless Handheld Testing)
   - Έλεγχος Ασύρματων Επικοινωνιών (Cordless Communications Testing)
   - Έλεγχος Συσκευών Επιτήρησης Ασύρματων επικοινωνιών (Wireless Surveillance Device Testing)
   - Έλεγχος Συσκευών Συναλλαγής Ασύρματων επικοινωνιών (Wireless Transaction Device Testing)
   - Έλεγχος Προσδιορισμού Ραδιοσυχνότητας-RFID (Radio Frequency Identification-RFID Testing)
   - Έλεγχος Υπερύθρων (Infrared Testing)
   - Επισκόπηση Ιδιωτικότητας (Privacy Review)

6. **Έλεγχος Φυσικής Ασφάλειας - Physical Security Testing**
   - Επισκόπηση Στάσης (Posture Review)
   - Δοκιμή Ελέγχου Πρόσβασης (Access Controls Testing)
   - Επισκόπηση Περιμέτρου (Perimeter Review)
   - Επισκόπηση Ελέγχου-παρακολούθησης (Monitoring Review)
   - Επισκόπηση Απόκρισης Προειδοποιήσεων (Alarm Response Review)
   - Επισκόπηση Τοποθεσίας (Location Review)
   - Επισκόπηση Περιβάλλοντος (Environment Review)

2.2.3 Μετρικές Ασφάλειας (Security Metrics)

Η ολοκλήρωση ενός λεπτομερούς ελέγχου ασφάλειας έχει το πλεονέκτημα να μας παρέχει ακριβείς μετρικές για την κατάσταση της ασφάλειας. Όσο λιγότερο λεπτομερής είναι ο έλεγχος, τόσο λιγότερο ακριβής θα είναι η μετρική. Αντίστοιχα, οι λιγότερο ειδικευμένοι ελεγκτές και λιγότερο πεπειραμένοι αναλυτές, επίσης έχουν επιπτώσεις στην ποιότητα της μετρικής. Επομένως, μια επιτυχής μετρική ασφάλειας απαιτεί έναν έλεγχο που μπορεί να περιγραφεί ως έλεγχος (μέτρηση) από τα κατάλληλα διανύσματα (vectors) που απαιτούνται, συμπεριλαμβάνοντας τον υπολογισμό για ανακρίβειες και στρεβλώσεις στα δεδομένα του ελέγχου και τις δεξιότητες ή την εμπειρία των επαγγελματιών ασφάλειας που εκτελούν τον έλεγχο. Σφάλματα σε αυτές τις απαιτήσεις θα οδηγήσουν σε μετρήσεις χαμηλότερης ποιότητας και αναληθείς προσδιορισμούς ασφάλειας. Αυτή η μεθοδολογία αναφέρεται στις μετρικές ως Τιμές Αξιολόγησης Κινδύνου (Risk Assessment Values - RAVs). Έτσι, ένας έλεγχος με αυτήν την μεθοδολογία και τις RAVs, θα παρέχουν την πραγματική βάση για μια ακριβής και πληρέστερη αξιολόγηση του κινδύνου.

2.2.4 Εφαρμόζοντας Τιμές Αξιολόγησης Κινδύνου - Risk Assessment Values

Αυτή η μεθοδολογία θα καθορίσει και θα ποσοτικοποιήσει τρεις περιοχές στην εμβέλεια (scope), οι οποίες συνθέτουν τη «μεγάλη εικόνα» (big picture) που ορίζεται ως Πραγματική Ασφάλεια (Actual Security), ως τη σχέση της με την τρέχουσα και πραγματική κατάσταση της ασφάλειας. Η «προσέγγιση της συνολικής εικόνας»[7] (big picture approach) είναι να υπολογίσει ξεχωριστά τιμές επιτομής (hash values), για κάθε μια από τις εξής περιοχές: Λειτουργίες - Operations, Έλεγχοι - Controls και Περιορισμοί - Limitations. Οι τρεις τιμές συνδυάζονται για να διαμορφώσουν την τέταρτη τιμή επιτομής, την Πραγματική Ασφάλεια, ώστε να παρέχουν τη «συνολική εικόνα» και μια τελική μετρική για συγκρίσεις. Δεδομένου ότι τα RAVs είναι η επιτομή των πληροφοριών που είναι σχετικές με την ασφάλεια, έχει σαν αποτέλεσμα να μπορούν να κλιμακώνονται χωρίς όριο. Αυτό επιτρέπει να έχουμε συγκρίσιμες τιμές ανάμεσα σε δύο ή περισσότερες εμβέλειες (scopes) ανεξάρτητα από τον στόχο, το διάνυσμα (vector), τον τύπο του ελέγχου, ή το δείκτη (index), όπου δείκτης είναι η μέθοδος υπολογισμού μεμονωμένων στόχων. Αυτό σημαίνει ότι με τα RAVs η ασφάλεια στόχου μπορεί να συγκριθεί αποτελεσματικά με 10.000 στόχους.

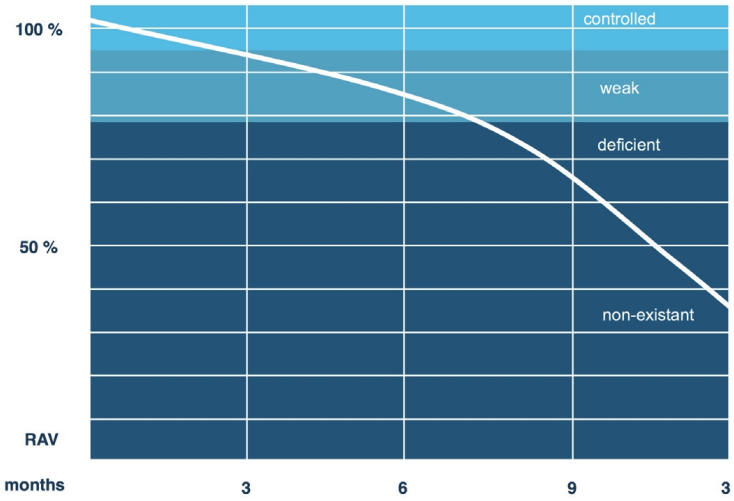
Ένας σημαντικός κανόνας για την εφαρμογή αυτών των μετρικών είναι ότι η πραγματική ασφάλεια μπορεί να υπολογιστεί μόνο ανά εμβέλεια. Μια αλλαγή στο κανάλι (channel), το διάνυσμα, ή το δείκτη είναι ένα νέο πεδίο και καθιστά αναγκαίο έναν νέο υπολογισμό για την πραγματική ασφάλεια. Εντούτοις, πολλαπλές εμβέλειες μπορούν να συνυπολογιστούν για να δημιουργήσουν μια πραγματική ασφάλεια που αντιπροσωπεύει ένα πληρέστερο φάσμα της λειτουργικής ασφάλειας. Παραδείγματος χάριν, ο έλεγχος σε internet-facing[8] servers θα έπρεπε να πραγματοποιηθεί και από την πλευρά του Διαδικτύου και μέσα από την περίμετρο του δικτύου που βρίσκονται.

[7] Η προσέγγιση «Big picture» είναι μια ολιστική προσέγγιση, που «βλέπει» πέρα από τα συμπτώματα και μεταχειρίζεται το όλο σύνολο. Είναι πάρα πολύ διαδεδομένη σε αυτούς που θέλουν στοχοθετημένες (και γρήγορες) διορθώσεις για υψηλού επιπέδου προβλήματα.

[8] Internet facing είναι ένα σύστημα με μια θύρα, συνήθως Ethernet, που συνδέεται απευθείας σε ένα internet modem ή ένα network interface unit

Αυτά είναι 2 διανύσματα. Το πρώτο διάνυσμα δεικτοδοτείται βάσει IP address και περιέχει 50 στόχους. Το δεύτερο διάνυσμα δεικτοδοτείται βάσει MAC address και είναι 100 στόχοι. Μόλις ολοκληρωθεί κάθε έλεγχος και οι μετρικές υπολογίζονται για κάθε μια από τις 3 εμβέλειες, μπορούν να συνδυαστούν σε έναν υπολογισμό 150 στόχων και περιλήψεων-αθροισμάτων κάθε περιοχής. Αυτό θα δώσει μια τελική μετρική πραγματικής ασφάλειας, η οποία είναι πληρέστερη για το συγκεκριμένο δίκτυο περιμέτρου.

Αρχίζοντας από μια προσέγγιση "τέλειας ασφάλειας" βασισμένη σε βέλτιστες πρακτικές, το RAV καθορίζει το μεμονωμένο επίπεδο ασφάλειας από το οποίο μια καμπύλη υποβάθμισης (βλ. την παρακάτω γραφική παράσταση) παράγεται, επεξηγώντας τη δυνατότητα του συστήματος να αντιδράσει με ασφάλεια και κατάλληλα σε απροσδόκητα γεγονότα.



Σχήμα 6. Διάγραμμα με τη καμπύλη που παράγεται από το RAV

Συνδεδεμένο με αυτό, είναι το γεγονός ότι ο έλεγχος ασφάλειας (σύμφωνα με το OSSTMM) που βασίζεται σε τεχνικές λεπτομέρειες, δεν αποτελεί έναν έλεγχο (risk audit) κινδύνου - βασισμένο σε χαρτί, ο οποίος αξιολογεί την πιθανότητα της εμφάνισης κινδύνων. Το RAV είναι βασισμένο σε μια τεχνικώς αδιαμφισβήτητη, επαληθεύσιμη πραγματική κατάσταση. Επομένως, το OSSTMM διαφοροποιείται σαφώς από τους εναλλακτικούς συμβατικούς ελέγχους κινδύνου και τοποθετείται ως έλεγχος λειτουργικής ασφάλειας. Συγχρόνως, εξασφαλίζει ότι ο έλεγχος ασφάλειας μπορεί να πραγματοποιηθεί κατά ένα συγκρίσιμο τρόπο.

2.2.4.1 Πραγματική Ασφάλεια (Actual Security)

Για την αποτύπωση της αποτίμησης της πραγματικής ασφάλειας χρησιμοποιούνται οι κάτωθι *τύποι τιμών* (value types):

- Λειτουργίες (Operations)

Η ανάγκη για ασφάλεια που έχει κάποιος, θα πρέπει να είναι διαλογική, χρήσιμη, δημόσια, ανοικτή, ή διαθέσιμη. Παραδείγματος χάριν, ας σκεφτούμε ένα κατάστημα. Έχει πόρτες, μερικές φορές παράθυρα, ρολόγια στους τοίχους, διαδρόμους που μας επιτρέπουν να κινούμαστε, καθώς και μια πόρτα με ένα σήμα που μας ενημερώνει ότι είναι ανοικτό. Το κατάστημα λοιπόν, πρέπει να είναι επαρκώς εξασφαλισμένο προκειμένου ο πελάτης να το επισκεφθεί και να αφήσει χρήματα. Άρα, πριν θεωρήσουμε οποιαδήποτε άλλη απαίτηση, το κατάστημα αρχικά οφείλει να είναι σε

λειτουργία. Τα παραπάνω, αποτελούν μια μέθοδο ασφάλειας για τις λειτουργίες του καταστήματος. Οι λειτουργίες καθορίζονται από διαφάνεια (visibility), εμπιστοσύνη (trust) και πρόσβαση (access).

Επομένως, η μέτρηση της ασφάλειας των λειτουργιών (OPSEC), απαιτεί τις μετρήσεις της διαφάνειας, της εμπιστοσύνης, και της πρόσβασης στα πλαίσια της εμβέλειας. Διαφάνεια είναι ο αριθμός των στόχων οι οποίοι προσδιορίζεται ότι αλληλεπιδρούν είτε άμεσα, είτε έμμεσα με την περιοχή της εμβέλειας ή ακόμη και αυτοί που αποτελούν παθητικές προελεύσεις, Καθώς η διαφάνεια καθορίζεται, η τιμή της αντιπροσωπεύει τον αριθμό των στόχων στην εμβέλεια. Η εμπιστοσύνη είναι οποιαδήποτε μη-επικυρωμένη αλληλεπίδραση σε οποιονδήποτε από τους στόχους. Η πρόσβαση είναι ο αριθμός των σημείων αλληλεπίδρασης με κάθε στόχο. Το άθροισμα και των τριών, είναι το OPSEC Delta (Διαφάνεια + Εμπιστοσύνη + Πρόσβαση), το οποίο είναι ο συνολικός αριθμός ενάρξεων μέσα στις λειτουργίες και αντιπροσωπεύει το συνολικό ποσό της λειτουργικής ασφάλειας που μειώνεται μέσα στο στόχο.

- Έλεγχοι (Controls)

Έλεγχοι επίπτωσης και μείωσης απώλειας. Είναι η διαβεβαίωση ότι τα φυσικά και πληροφοριακά αγαθά, καθώς επίσης και τα ίδια τα κανάλια, προστατεύονται από διάφορους τύπους άκυρων αλληλεπιδράσεων, όπως καθορίζονται από το κανάλι. Παραδείγματος χάριν, η ασφάλιση του καταστήματος σε περίπτωση πυρκαγιάς είναι ένας έλεγχος που δεν αποτρέπει το απόθεμα εμπορευμάτων από το να καταστραφεί ή να κλαπεί, παρόλα αυτά όμως θα πληρώσει την ισοδύναμη τιμή για την απώλεια. Υπάρχουν 10 έλεγχοι. Οι πρώτοι πέντε έλεγχοι είναι Κατηγορίας Α που ελέγχουν αλληλεπιδράσεις, ενώ, οι πέντε έλεγχοι Κατηγορίας Β είναι σχετικοί με τον έλεγχο των διαδικασιών.

Κατηγορία Α - έλεγχοι αλληλεπίδρασης (interactive):

- Αυθεντικοποίηση (Authentication) - είναι ο έλεγχος της αλληλεπίδρασης όπου απαιτείται να υπάρχουν τόσο διαπιστευτήρια (credentials) όσο και έγκριση, όπου απαιτείται διακρίβωση ταυτότητας (ταυτοποίηση - identification) για τη λήψη και των δύο.
- Αποζημίωση (Indemnification) - είναι ο έλεγχος της τιμής των αγαθών από το νόμο ή/ και η ασφάλεια για την αποζημίωση της πραγματικής και τρέχουσας τιμής της απώλειας.
- Υποταγή (Subjugation) - είναι ο τοπικός έλεγχος της προστασίας και των περιορισμών των αλληλεπιδράσεων από το αρμόδιο αγαθό.
- Συνέχεια (Continuity) - είναι ο έλεγχος των διαδικασιών για να διατηρηθεί η πρόσβαση στα αγαθά σε περιπτώσεις φθοράς ή αποτυχίας.
- Ανθεκτικότητα (Resilience) - είναι ο έλεγχος των μηχανισμών ασφάλειας για να παρασχεθεί προστασία στα αγαθά σε περιπτώσεις φθοράς ή αποτυχίας.

Κατηγορία Β - έλεγχοι διαδικασίας (process):

- Μη αποποίηση ευθύνης (Non-repudiation) - αποτρέπει την πηγή από την άρνηση του ρόλου της σε οποιαδήποτε αλληλεπίδραση, άσχετα από το εάν επιτεύχθηκε η πρόσβαση ή όχι.
- Εμπιστευτικότητα (Confidentiality) - είναι ο περιορισμός για τη διασφάλιση ότι ένα αγαθό που παρουσιάζεται ή ανταλλάσσεται

μεταξύ συμβαλλόμενων μερών παραμένει γνωστό μόνο μεταξύ αυτών των συμβαλλόμενων μερών.

- Ιδιωτικότητα (Privacy) - είναι ο περιορισμός για τη μέθοδο του πώς ένα αγαθό που εκτίθεται ή ανταλλάσσεται μεταξύ συμβαλλόμενων μερών, παραμένει γνωστό μόνο μεταξύ αυτών των συμβαλλόμενων μερών.
- Ακεραιότητα (Integrity) - είναι ο περιορισμός σε εφαρμογή άγνωστων αλλαγών σε μεθόδους και αγαθά.
- Προειδοποίηση (Alarm) - είναι ο έλεγχος προειδοποίησης ότι το OPSEC ή οποιοιδήποτε έλεγχοι έχουν αποτύχει, έχουν παραβιαστεί, ή έχουν παρακαμφθεί.

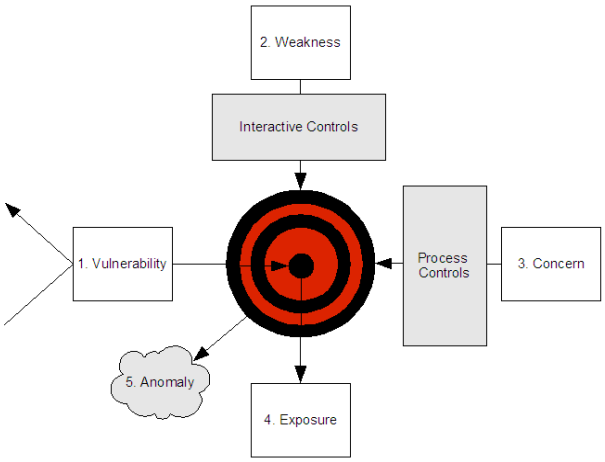
➢ Περιορισμοί (Limitations)

Αυτό αποτυπώνει την τρέχουσα κατάσταση των αντιληπτών και γνωστών ορίων για τα κανάλια, τις λειτουργίες και τους ελέγχους, όπως τα στοιχεία αυτά επαληθεύονται από τον έλεγχο. Για παράδειγμα, μια παλαιά κλειδαριά που είναι σκουριασμένη και θρυμματισμένη χρησιμοποιείται για να εξασφαλίσει τις εισόδους του καταστήματος κατά το κλείσιμό του, εισάγει έναν περιορισμό ασφάλειας ο οποίος αντιστοιχεί σε ένα μικρό κλάσμα της ισχύος προστασίας που είναι απαραίτητη για να καθυστερήσει την εξέλιξη μιας επίθεσης ή να αντισταθεί σ' αυτή. Καθορίζοντας ότι η κλειδαριά είναι παλαιά και αδύναμη μέσω οπτικής επαλήθευσης, τότε σε αυτήν την περίπτωση έχουμε έναν «προσδιορισμένο περιορισμό». Καθορίζοντας ότι είναι παλαιά και αδύναμη, σπάζοντάς τη, χρησιμοποιώντας 100 kg δύναμης όταν ένας επιτυχής αποτρεπτικός παράγοντας (δηλ. μία κλειδαριά που θεωρείται επαρκής) απαιτεί 1000 kg δύναμης, τότε έχουμε έναν «επιβεβαιωμένο περιορισμό».

Η κατάσταση της ασφάλειας όσον αφορά τις γνωστές ατέλειες και τους περιορισμούς προστασίας εντός της εμβέλειας, λογίζονται ως Περιορισμοί. Για να δοθούν κατάλληλες τιμές σε κάθε τύπο περιορισμού, θα πρέπει να είναι ταξινομημένοι και κατηγοριοποιημένοι. Φυσικά είναι δυνατόν να χρησιμοποιηθεί οποιοδήποτε όνομα ή αριθμός ταξινόμησης, αυτή η μεθοδολογία ωστόσο προσπαθεί να τους ορίσει σύμφωνα με τις επιπτώσεις τους στα OPSEC και Controls, αποφεύγοντας να τους εντάξει σε ένα αυστηρά ιεραρχικό σχήμα. Πέντε ταξινομήσεις έχουν οριστεί για να αντιπροσωπεύσουν όλους τους τύπους περιορισμών.

- Ευπάθεια (Vulnerability) - είναι μία ατέλεια ή σφάλμα που αρνείται την πρόσβαση σε αγαθά για τους εξουσιοδοτημένους χρήστες ή διαδικασίες, επιτρέπει την πρόσβαση σε αγαθά σε μη εξουσιοδοτημένους χρήστες ή διαδικασίες, ή επιτρέπει σε μη εξουσιοδοτημένους χρήστες ή διαδικασίες να αποκρύψουν τα αγαθά ή τους εαυτούς τους εντός της εμβέλειας.
- Αδυναμία (Weakness) - είναι μία ατέλεια ή σφάλμα που διαταράσσει, μειώνει, κάνει κακή χρήση, ή ακυρώνει συγκεκριμένα τα αποτελέσματα των ελέγχων αλληλεπίδρασης (αυθεντικοποίησης, αποζημίωσης, υποταγής, συνέχειας και ανθεκτικότητας).
- Ανησυχία (Concern) - είναι μία ατέλεια ή σφάλμα που διαταράσσει, μειώνει, κάνει κακή χρήση, ή ακυρώνει τα αποτελέσματα της ροής ή της εκτέλεσης των ελέγχων διαδικασίας (μη αποποίησης ευθύνης, εμπιστευτικότητας, ιδιωτικότητας, ακεραιότητας και προειδοποίησης).

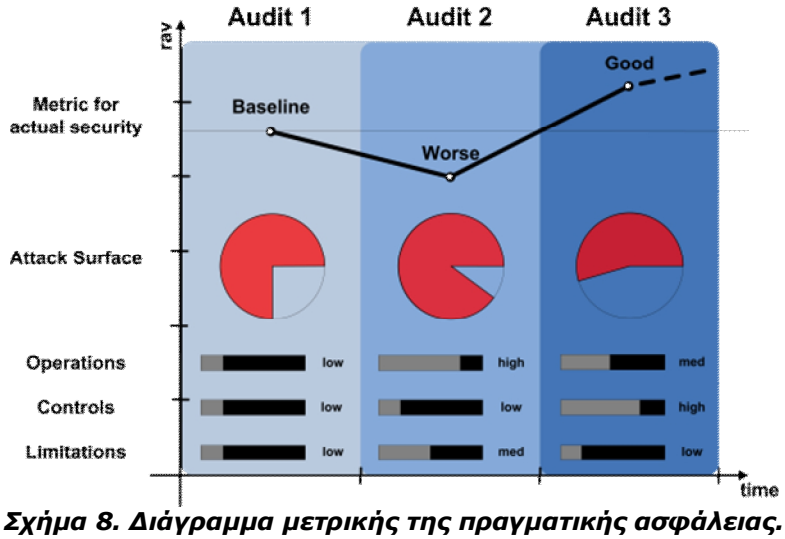
- Έκθεση (Exposure) - είναι μια αδικαιολόγητη δράση, ατέλεια ή σφάλμα που παρέχει άμεση ή έμμεση ορατότητα των στόχων ή των αγαθών εντός του επιλεγμένου καναλιού της εμβέλειας.
- Ανωμαλία (Anomaly) - είναι οποιοδήποτε μη αναγνωρίσιμο ή άγνωστο στοιχείο που δεν μπορεί να λογισθεί σε κανονικές λειτουργίες.



Σχήμα 7. Περιορισμοί.

2.2.4.1.1 Υπολογισμός της Πραγματικής Ασφάλειας (Actual Security)

Για να μετρηθεί η τρέχουσα κατάσταση των λειτουργιών με εφαρμογή των ελέγχων και τους περιορισμούς που αναγνωρίστηκαν, απαιτείται ένας τελικός υπολογισμός που θα καθορίσει την *Πραγματική ασφάλεια*. Όπως υπονοείται και από το όνομά της, είναι μία τιμή για το σύνολο της ασφάλειας, η οποία συνδυάζει τις τρεις τιμές της λειτουργικής ασφάλειας, των ελέγχων και των περιορισμών, για να παρουσιάσει την πραγματική κατάσταση της ασφάλειας. Ο σκοπός της πραγματικής ασφάλειας είναι να συνοψιστούν οι τρεις συνδυασμένες τιμές σε ένα εκατοστημόριο τιμής μίας μοναδικής μετρικής που μπορεί να χρησιμοποιηθεί για να εκτιμήσει την αποτελεσματικότητα της λειτουργικής ασφάλειας και να παρέχει μια μέθοδο σύγκρισης, βαθμολόγησης και εκτίμησης. Αυτή η προσέγγιση "συνολικής εικόνας" είναι αποτελεσματική επειδή δεν επιδεικνύει απλά το πώς κάποιος προετοιμάζεται για απειλές αλλά το πόσο αποτελεσματικές είναι οι προετοιμασίες του ενάντια στις απειλές.



Σχήμα 8. Διάγραμμα μετρικής της πραγματικής ασφάλειας.

2.2.4.2 Παράδειγμα μέτρησης RAV

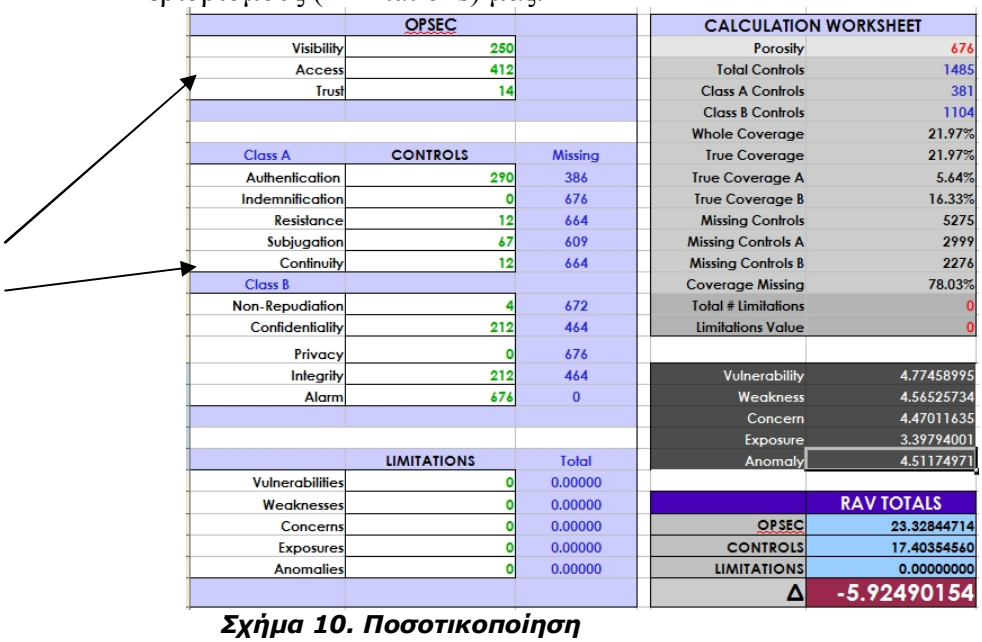
Στη συνέχεια, θα περιγραφεί ένα παράδειγμα. Η Τιμή Αξιολόγησης Κινδύνου (RAV), όπως, αναφέραμε και προηγουμένως, προσδιορίζεται από τρεις κατηγορίες που καθορίζονται εντός της εμβέλειας: Λειτουργική ασφάλεια (Operational Security), Έλεγχοι απώλειας (Loss Controls) και Περιορισμοί ασφάλειας (Security Limitations).

- Αρχικά, θα συγκεντρώσουμε και θα συνδέσουμε όλες τις πληροφορίες εισαγωγής (input) μας στις αντίστοιχες κατηγορίες για κάθε μεταβλητή εισόδου.

Category		Input
Operational Security		Visibility
		Access
		Trust
Loss Controls	Class A	
		Authentication
		Indemnification
		Resistance
		Subjugation
		Continuity
	Class B	
		Non-Repudiation
		Confidentiality
		Privacy
		Integrity
		Alarm
Security Limitations		Vulnerability
		Weakness
		Concern
		Exposure
		Anomaly

Σχήμα 9. Η μέθοδος RAV

- Προσδιορισμός ποσότητας - ποσοτικοποίηση (Quantification): Στη συνέχεια, μετράμε το OPSEC, καθώς και τους Ελέγχους (Controls) και τους Περιορισμούς (Limitations) μας.

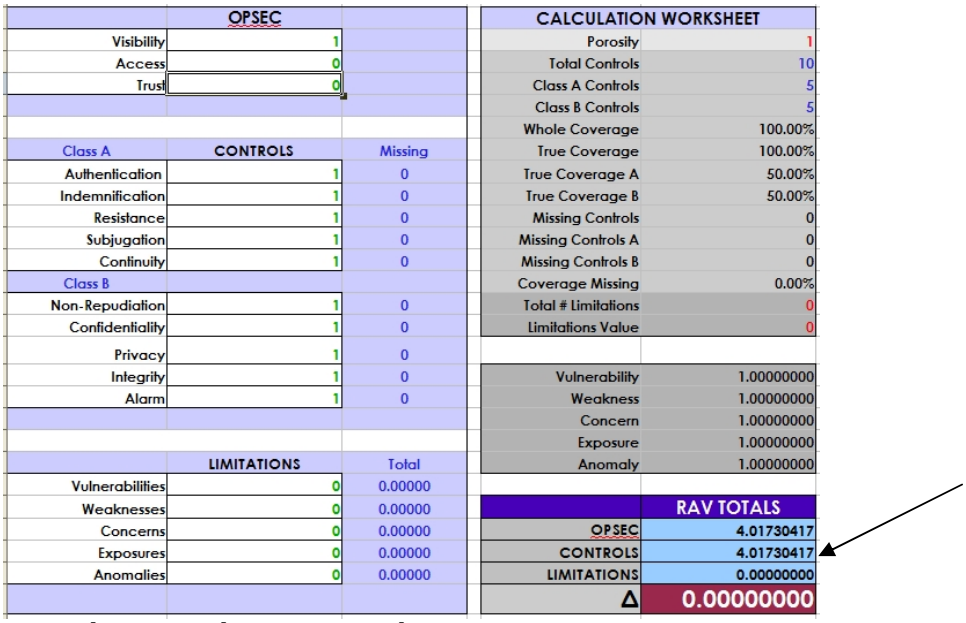


	OPSEC	
Visibility	250	
Access	412	
Trust	14	
Class A	CONTROLS	Missing
Authentication	290	386
Indemnification	0	676
Resistance	12	664
Subjugation	67	609
Continuity	12	664
Class B		
Non-Repudiation	4	672
Confidentiality	212	464
Privacy	0	676
Integrity	212	464
Alarm	676	0
	LIMITATIONS	Total
Vulnerabilities	0	0.00000
Weaknesses	0	0.00000
Concerns	0	0.00000
Exposures	0	0.00000
Anomalies	0	0.00000

CALCULATION WORKSHEET	
Porosity	676
Total Controls	1485
Class A Controls	381
Class B Controls	1104
Whole Coverage	21.97%
True Coverage	21.97%
True Coverage A	5.64%
True Coverage B	16.33%
Missing Controls	5275
Missing Controls A	2999
Missing Controls B	2276
Coverage Missing	78.03%
Total # Limitations	0
Limitations Value	0
Vulnerability	4.77458995
Weakness	4.56525734
Concern	4.47011635
Exposure	3.39794001
Anomaly	4.51174971
	RAV TOTALS
OPSEC	23.32844714
CONTROLS	17.40354560
LIMITATIONS	0.00000000
Δ	-5.92490154

Σχήμα 10. Ποσοτικοποίηση

- Νόμος Ισορροπίας: Ισχύει ότι 10 έλεγχοι μπορούν να ακυρώσουν 1 OPSEC.

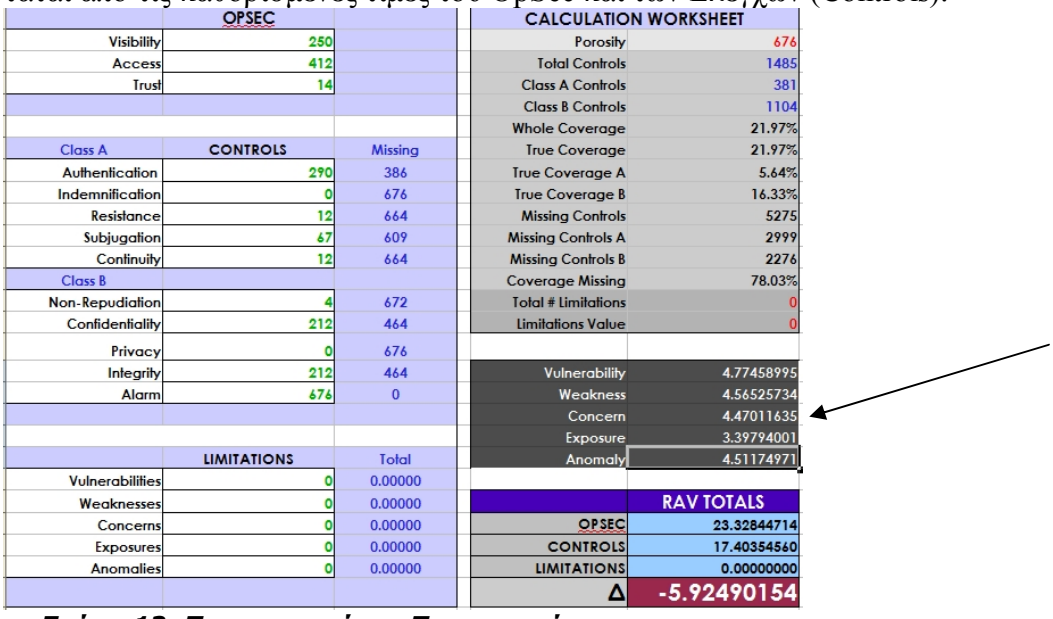


OPSEC		
Visibility	1	
Access	0	
Trust	0	
Class A	CONTROLS	Missing
Authentication	1	0
Indemnification	1	0
Resistance	1	0
Subjugation	1	0
Continuity	1	0
Class B		
Non-Repudiation	1	0
Confidentiality	1	0
Privacy	1	0
Integrity	1	0
Alarm	1	0
	LIMITATIONS	Total
Vulnerabilities	0	0.00000
Weaknesses	0	0.00000
Concerns	0	0.00000
Exposures	0	0.00000
Anomalies	0	0.00000

CALCULATION WORKSHEET	
Porosity	1
Total Controls	10
Class A Controls	5
Class B Controls	5
Whole Coverage	100.00%
True Coverage	100.00%
True Coverage A	50.00%
True Coverage B	50.00%
Missing Controls	0
Missing Controls A	0
Missing Controls B	0
Coverage Missing	0.00%
Total # Limitations	0
Limitations Value	0
Vulnerability	1.00000000
Weakness	1.00000000
Concern	1.00000000
Exposure	1.00000000
Anomaly	1.00000000
	RAV TOTALS
OPSEC	4.01730417
CONTROLS	4.01730417
LIMITATIONS	0.00000000
Δ	0.00000000

Σχήμα 11. Νόμος ισορροπίας.

- Ποσοτικοποίηση Περιορισμών: Η τιμή του κάθε Περιορισμού (Limitation) εξαρτάται από τις καθορισμένες τιμές του OpSec και των Ελέγχων (Controls).



OPSEC		
Visibility	250	
Access	412	
Trust	14	
Class A	CONTROLS	Missing
Authentication	290	386
Indemnification	0	676
Resistance	12	664
Subjugation	67	609
Continuity	12	664
Class B		
Non-Repudiation	4	672
Confidentiality	212	464
Privacy	0	676
Integrity	212	464
Alarm	676	0
	LIMITATIONS	Total
Vulnerabilities	0	0.00000
Weaknesses	0	0.00000
Concerns	0	0.00000
Exposures	0	0.00000
Anomalies	0	0.00000

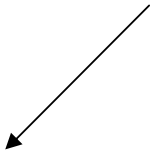
CALCULATION WORKSHEET	
Porosity	676
Total Controls	1485
Class A Controls	381
Class B Controls	1104
Whole Coverage	21.97%
True Coverage	21.97%
True Coverage A	5.64%
True Coverage B	16.33%
Missing Controls	5275
Missing Controls A	2999
Missing Controls B	2276
Coverage Missing	78.03%
Total # Limitations	0
Limitations Value	0
Vulnerability	4.77458995
Weakness	4.56525734
Concern	4.47011635
Exposure	3.39794001
Anomaly	4.51174971
	RAV TOTALS
OPSEC	23.32844714
CONTROLS	17.40354560
LIMITATIONS	0.00000000
Δ	-5.92490154

Σχήμα 12. Ποσοτικοποίηση Περιορισμών

- Έλεγχος αλλαγής: Μέτρηση για να ευρεθεί το Δέλτα (Δ=Controls-Opsec-Limitations). Αυτό θα μας υποδείξει την αλλαγή που θα προέκυπτε εάν τοποθετούσαμε αυτό το δίκτυο σε ένα άλλο δίκτυο.

	OPSEC	
Visibility	250	
Access	412	
Trust	14	
Class A	CONTROLS	Missing
Authentication	290	386
Indemnification	0	676
Resistance	12	664
Subjugation	67	609
Continuity	12	664
Class B		
Non-Repudiation	4	672
Confidentiality	212	464
Privacy	0	676
Integrity	212	464
Alarm	676	0
	LIMITATIONS	Total
Vulnerabilities	0	0.00000
Weaknesses	0	0.00000
Concerns	0	0.00000
Exposures	0	0.00000
Anomalies	0	0.00000

CALCULATION WORKSHEET	
Porosity	676
Total Controls	1485
Class A Controls	381
Class B Controls	1104
Whole Coverage	21.97%
True Coverage	21.97%
True Coverage A	5.64%
True Coverage B	16.33%
Missing Controls	5275
Missing Controls A	2999
Missing Controls B	2276
Coverage Missing	78.03%
Total # Limitations	0
Limitations Value	0
Vulnerability	4.77458995
Weakness	4.56525734
Concern	4.47011635
Exposure	3.39794001
Anomaly	4.51174971
	RAV TOTALS
OPSEC	23.32844714
CONTROLS	17.40354560
LIMITATIONS	0.00000000
Δ	-5.92490154



Σχήμα 13. Έλεγχος αλλαγής

2.2.5 Κανόνες Δέσμευσης (Rules Of Engagement)

Αυτοί οι κανόνες καθορίζουν τις λειτουργικές οδηγίες για τις αποδεκτές, δεοντολογικές και σύμφωνες με την ηθική πρακτικές που αφορούν στην εμπορική προώθηση και πώληση των ελέγχων, στην εκτέλεση του ελέγχου και στον χειρισμό των αποτελεσμάτων του ελέγχου. Παρά το γεγονός ότι, θυγατρικές, συνεργάτες, μέλη ομάδων ή συνέταιροι της ISECOM πρέπει βάσει του νόμου να υποστηρίξουν τους ακόλουθους κανόνες δέσμευσης, η κατάλληλη χρήση του OSSTMM επίσης απαιτεί προσήλωση σε αυτούς τους κανόνες. Η αποτυχία οποιουδήποτε προσώπου ή οργανισμού να ακολουθήσει αυτούς τους κανόνες μπορεί να αναφερθεί άμεσα στο ISECOM. Τα παρακάτω είναι ένα απόσπασμα από τους "Rules of Engagement" του OSSTMM που παρουσιάζει αυτά που απαιτούνται, προτού ένα έργο μπορέσει να αρχίσει [Herzog P, (2006)]:

- Sales and Marketing (Πωλήσεις και Μάρκετινγκ)
- Assessment / Estimate Delivery (Παράδοση Αξιολόγησης-Εκτίμησης)
- Contracts and Negotiations (Συμβάσεις και Διαπραγματεύσεις)
- Scope Definition (Καθορισμός Εμβέλειας)
- Test Plan (Σχέδιο Ελέγχου)
- Test Process (Διαδικασία Ελέγχου)
- Reporting (Υποβολή Έκθεσης)

2.2.6 Διαδικασία (Process)

Η διαδικασία ελέγχου ασφάλειας είναι ένας έλεγχος διακριτών γεγονότων που λαμβάνουν χώρα σε ένα δυναμικό, στοχαστικό σύστημα. Ο στόχος του ελέγχου είναι ένα σύστημα, μια συλλογή από αλληλεπιδρούσες και αλληλεξαρτώμενες διαδικασίες, ο οποίος επηρεάζεται επίσης από το στοχαστικό περιβάλλον στο οποίο υπάρχει. Το γεγονός ότι το σύστημα είναι στοχαστικό σημαίνει ότι η συμπεριφορά των γεγονότων σε ένα σύστημα δεν μπορεί να καθοριστεί επειδή η επόμενη κατάσταση περιβάλλοντος, μπορεί μόνο να καθοριστεί μερικώς αλλά όχι πλήρως από την προηγούμενη κατάσταση. Το σύστημα περιέχει έναν πεπερασμένο, ενδεχομένως εξαιρετικά μεγάλο, αριθμό μεταβλητών και κάθε αλλαγή σε κάποια μεταβλητή

αντιστοιχεί σε ένα γεγονός και μια αλλαγή στην κατάσταση. Δεδομένου ότι το περιβάλλον είναι στοχαστικό, υπάρχει ένα στοιχείο τυχαιότητας και δεν υπάρχει κανένας τρόπος που να προκαθορίζει με βεβαιότητα το πώς όλες οι μεταβλητές θα επηρεάσουν την κατάσταση του συστήματος. Ένας διακριτός έλεγχος εξετάζει αυτές τις καταστάσεις μέσα στο δυναμικό σύστημα σε συγκεκριμένα χρονικά διαστήματα. Η παρακολούθηση διαδικασιών κατά τρόπο συνεχή, σε αντιδιαστολή με έναν διακριτό, θα παρείχε πολύ περισσότερες πληροφορίες για ανάλυση. Αλλά, επιπλέον, δε θα μπορούσε να είναι εφικτή. Ακόμη και οι συνεχείς έλεγχοι εντούτοις, απαιτούν τον εντοπισμό κάθε κατάστασης σε σχέση με το χρόνο προκειμένου να αναλυθούν σωστά.

Κάτι που πρέπει να σημειωθεί είναι η εκτενής έρευνα που είναι διαθέσιμη για τον έλεγχο αλλαγής για διαδικασίες ώστε να περιοριστεί το ποσό των ακαθόριστων γεγονότων σε ένα στοχαστικό σύστημα. Ο ελεγκτής συχνά θα προσπαθήσει να υπερβεί τους περιορισμούς του ελέγχου αλλαγής και να παρουσιάσει σενάρια «τι θα συμβεί εάν» ("what if"), τα οποία οι υπεύθυνοι για την εφαρμογή του ελέγχου αλλαγών μπορεί να μην έχουν εξετάσει. Μια λεπτομερής κατανόηση του ελέγχου αλλαγών είναι ουσιαστική για οποιοδήποτε ελεγκτή.

Δυστυχώς, οι ελεγκτές υποθέτουν ότι ο έλεγχος ασφάλειας είναι απλός και συχνά πραγματοποιούν τον έλεγχο σύμφωνα με τη γνωστή ως «διαδικασία αντήχησης» ("echo process") που απαιτεί ανατάραξη (agitating) και έπειτα παρακολούθηση εκπομπών από τον στόχο για τους δείκτες μιας συγκεκριμένης κατάστασης (ασφαλής ή επισφαλής, τρωτής ή προστατευμένης, ενεργής ή ανενεργής, left ή right). Η «διαδικασία αντήχησης» ακολουθεί το πρότυπο αιτίας και αποτελέσματος. Ο ελεγκτής επιφέρει την αιτία και αναλύει το αποτέλεσμα στον στόχο. Αυτός ο τρόπος ελέγχου είναι πολύ γρήγορος αλλά είναι επίσης ιδιαίτερα επιρρεπής σε σφάλματα, μερικά εκ των οποίων μπορεί να είναι καταστρεπτικά για τον στόχο. Ενώ οι κανόνες δέσμευσης μπορεί να βοηθήσουν ώστε να ελαχιστοποιήσουμε τη ζημία στον στόχο στη διαδικασία αντήχησης, δεν μπορεί όμως να βοηθήσουν ώστε να ελαχιστοποιήσουμε τα σφάλματα. Τα σφάλματα ταξινομούνται ως εξής:

2.2.6.1 Τύποι Σφάλματος (Error Types)

- Ψευδώς θετικό (False Positive): Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση ως αληθή ενώ στην πραγματικότητα η κατάσταση δεν είναι αληθής. Ένα ψευδώς θετικό αποτέλεσμα εμφανίζεται συχνά όταν οι προσδοκίες ή παραδοχές του ελεγκτή για αυτό που υποδεικνύει μια συγκεκριμένη κατάσταση, δεν ισχύει σε πραγματικές συνθήκες.
- Ψευδώς αρνητικό (false negative): Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση ως μη αληθή ενώ στην πραγματικότητα η κατάσταση είναι αληθής. Ένα ψευδώς αρνητικό αποτέλεσμα εμφανίζεται συχνά όταν οι προσδοκίες ή παραδοχές του ελεγκτή για το στόχο δεν ισχύουν σε πραγματικές συνθήκες, όταν τα εργαλεία που χρησιμοποιούνται για τον έλεγχο δεν είναι του κατάλληλου τύπου, όταν τα εργαλεία χρησιμοποιούνται με ακατάλληλο τρόπο ή όταν ο ελεγκτής δεν έχει εμπειρία. Ένα ψευδώς αρνητικό αποτέλεσμα μπορεί να είναι επικίνδυνο, δεδομένου ότι αποτελεί μια κακή διάγνωση μιας ασφαλούς κατάστασης, όταν στην πραγματικότητα η κατάσταση δεν είναι ασφαλής.

- Gray Positive: Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση ως αληθή, εντούτοις ο στόχος έχει σχεδιαστεί ώστε να αποκριθεί σε οποιαδήποτε αιτία με αυτήν την κατάσταση, είτε είναι αληθής είτε όχι. Αυτός ο τύπος ασφάλειας μέσω της συσκότισης (security through obscurity) μπορεί να είναι επικίνδυνος, δεδομένου ότι δεν μπορεί να είναι εγγυημένο ότι η ψευδαίσθηση θα λειτουργήσει το ίδιο για όλα τα ερεθίσματα.
- Gray Negative: Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση ως μη αληθή, εντούτοις ο στόχος σχεδιάζεται ώστε να αποκριθεί σε οποιαδήποτε αιτία με αυτήν την κατάσταση είτε είναι αληθής είτε όχι. Αυτός ο τύπος ασφάλειας μέσω της συσκότισης (security through obscurity) μπορεί να είναι επικίνδυνος, δεδομένου ότι δεν μπορεί να είναι εγγυημένο ότι η ψευδαίσθηση θα λειτουργήσει το ίδιο για όλα τα ερεθίσματα.
- Αντικατοπτρισμός (Specter): Η απόκριση από τον στόχο υποδεικνύει μια συγκεκριμένη κατάσταση ως είτε αληθή είτε ψευδή ενώ στην πραγματικότητα η κατάσταση δεν μπορεί να είναι γνωστή. Ένας αντικατοπτρισμός εμφανίζεται συχνά όταν λαμβάνει ο ελεγκτής μια απόκριση από ένα εξωτερικό ερέθισμα, το οποίο όμως θεωρείται ότι προέρχεται από τον στόχο. Ένας αντικατοπτρισμός μπορεί όντως να προέρχεται από τον στόχο, αλλά μπορεί να προέρχεται και από μια ανωμαλία στο κανάλι, είτε να είναι το αποτέλεσμα της απροσεξίας ή/και της απειρίας του ελεγκτή. Ένα από τα πιο συνηθισμένα προβλήματα στη διαδικασία αντήχησης είναι η υπόθεση ότι η απόκριση είναι ένα αποτέλεσμα του ελέγχου. Ο έλεγχος τύπου αιτίας-αποτελέσματος στον πραγματικό κόσμο δεν μπορεί να επιτύχει με συνέπεια αξιόπιστα αποτελέσματα, δεδομένου ότι ούτε η αιτία ούτε το αποτέλεσμα δεν μπορούν να απομονωθούν κατάλληλα.
- Έλλειψη εμβάθυνσης (Indiscretion): Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση είτε ως αληθή είτε ως ψευδή αλλά αυτό ισχύει μόνο σε μια συγκεκριμένη χρονική στιγμή. Οι στιγμές που εμφανίζεται η συγκεκριμένη απόκριση μπορεί να ακολουθούν ή όχι ένα μοτίβο (pattern) και εάν δεν μπορεί να ελεγχθεί το σύστημα σε στιγμή όπου η κατάσταση είναι διαφορετική, τότε αυτό ίσως έχει σαν αποτέλεσμα ο ελεγκτής να μην κατανοήσει την άλλη κατάσταση. Ένας ελεγκτής μπορεί επίσης να καθορίσει ότι αυτό είναι μια ανωμαλία ή ένα πρόβλημα με τον εξοπλισμό του ελέγχου, ειδικά εάν ο ελεγκτής δεν προνόησε να ρυθμίσει τον εξοπλισμό πριν από τον έλεγχο και να εκτελέσει τους κατάλληλους ελέγχους. Ένα σφάλμα από έλλειψη εμβάθυνσης μπορεί να είναι επικίνδυνο, δεδομένου ότι μπορεί να οδηγήσει σε μια εσφαλμένη έκθεση της κατάστασης της ασφάλειας.
- Σφάλμα Εντροπίας (Entropy Error): Η απόκριση στόχου δεν μπορεί να υποδείξει με ακρίβεια μια συγκεκριμένη κατάσταση είτε ως αληθή είτε ως ψευδή, λόγω υψηλού θορύβου, δηλαδή εξωτερικών παρεμβολών που είναι άσχετες προς τον έλεγχο. Ο ελεγκτής δεν μπορεί να καθορίσει κατάλληλα την κατάσταση έως ότου μειωθεί ο θόρυβος. Αυτός ο τύπος σφάλματος που προκαλείται από το περιβάλλον, σπάνια υπάρχει στο εργαστήριο εντούτοις είναι ένα σύνηθες περιστατικό εκτός εργαστηρίου σε ένα μη ελεγχόμενο περιβάλλον. Η εντροπία μπορεί να είναι επικίνδυνη, εάν τα αποτελέσματά της δεν μπορούν να αντιμετωπιστούν.
- Παραποίηση (Falsification): Η απόκριση στόχου υποδεικνύει μια συγκεκριμένη κατάσταση είτε ως αληθή είτε ως ψευδή λόγω προκαταλήψεων

σε ό,τι αφορά τον στόχο ή εσφαλμένης στόχευσης των ελέγχων, ενώ στην πραγματικότητα η κατάσταση εξαρτάται κατά ένα μεγάλο μέρος από τις άγνωστες μεταβλητές. Αυτός ο τύπος ασφάλειας μέσω της συσκότισης μπορεί να είναι επικίνδυνος, δεδομένου ότι η στόχευση των ελέγχων θα μετατοπιστεί όταν οι έλεγχοι προέρχονται από διαφορετικά διανύσματα ή χρησιμοποιούν διαφορετικές τεχνικές.

- Σφάλμα Δειγματοληψίας (Sampling Error): Ο στόχος είναι ένα πολωμένο δείγμα ενός μεγαλύτερου συστήματος ή ενός μεγαλύτερου αριθμού πιθανών καταστάσεων. Αυτό το σφάλμα εμφανίζεται συνήθως όταν μια αρχή (authority) επηρεάζει τη λειτουργική κατάσταση του στόχου κατά τη διάρκεια του ελέγχου. Αυτό μπορεί να συμβαίνει θέτοντας περιορισμούς που ορίζουν ότι ο έλεγχος θα γίνει σε συγκεκριμένο χρόνο ή μιας προκατάληψης που υποδεικνύει ότι θα πρέπει να ελέγχεται μόνο ό,τι θεωρείται "σημαντικό" μέσα σε ένα σύστημα. Αυτός ο τύπος σφάλματος θα προκαλέσει μια στρέβλωση της ερμηνείας της γενικής λειτουργικής ασφάλειας.
- Περιορισμός (Constraint): Οι περιορισμοί των ανθρώπινων αισθήσεων ή ικανοτήτων εξοπλισμού υποδεικνύουν μια συγκεκριμένη κατάσταση ως είτε αληθή είτε ως ψευδή, αν και η πραγματική κατάσταση είναι άγνωστη. Αυτό το σφάλμα δεν προκαλείται από κακές αξιολογήσεις ή από λανθασμένες επιλογές εξοπλισμού, αλλά μάλλον από την αποτυχία να αναγνωριστούν οι επιβληθέντες περιορισμοί.
- Διάδοση (Propagation): Ο ελεγκτής δεν πραγματοποιεί έναν συγκεκριμένο έλεγχο ή είναι προκατειλημμένος, με συνέπεια να αγνοήσει ένα συγκεκριμένο αποτέλεσμα λόγω μιας εκ των προτέρων θεώρησης ότι θα υπάρξει συγκεκριμένο αποτέλεσμα. Ο έλεγχος μπορεί να επαναληφθεί πολλές φορές ή τα εργαλεία και ο εξοπλισμός μπορεί να τροποποιηθεί για να οδηγηθούμε στην επιθυμητή έκβαση. Όπως υπονοείται και από το όνομα, μια διαδικασία που δεν λαμβάνει καμία ανατροφοδότηση και στην οποία τα σφάλματα παραμένουν άγνωστα ή αγνοούνται, θα διαδώσει περαιτέρω σφάλματα καθώς συνεχίζεται ο έλεγχος. Τα σφάλματα διάδοσης μπορεί να είναι επικίνδυνα επειδή τα σφάλματα που διαδίδονται από νωρίς στον έλεγχο, μπορεί να μην είναι ορατά κατά τη διάρκεια μιας ανάλυσης συμπερασμάτων. Επιπλέον, απαιτείται μελέτη ολόκληρης της διαδικασίας του ελέγχου, για να αποκαλύψει τα σφάλματα διάδοσης.
- Ανθρώπινο σφάλμα (Human Error): Τα λάθη που προκαλούνται από την έλλειψη ικανότητας, εμπειρίας, ή κατανόησης, δεν αποδίδονται σε προκατάληψη και είναι ένας παράγοντας που πάντοτε υπάρχει, ανεξάρτητα από τη μεθοδολογία ή την τεχνική. Όταν ένας πεπειραμένος ελεγκτής ίσως να κάνει λάθη τύπου διάδοσης, ένας ελεγκτής χωρίς εμπειρία είναι πιθανότερο να μην αναγνωρίσει το ανθρώπινο λάθος. Οι έμπειροι ελεγκτές έχουν την ικανότητα να αναγνωρίσουν και να διορθώσουν τα ανθρώπινα σφάλματα. Στατιστικά, υπάρχει μια έμμεση σχέση μεταξύ της εμπειρίας και του ανθρώπινου σφάλματος. Όσο λιγότερη εμπειρία έχει ένας ελεγκτής, τόσο μεγαλύτερο είναι το πλήθος των ανθρωπίνων σφαλμάτων που περιέχει ένας έλεγχος.

2.3 Βασική μεθοδολογία ασφάλειας

2.3.1 Ορίζοντας έναν έλεγχο ασφάλειας

Τα παρακάτω 7 βήματα θα μας βοηθήσουν να φθάσουμε στην αρχή ενός κατάλληλα ορισμένου ελέγχου ασφάλειας.

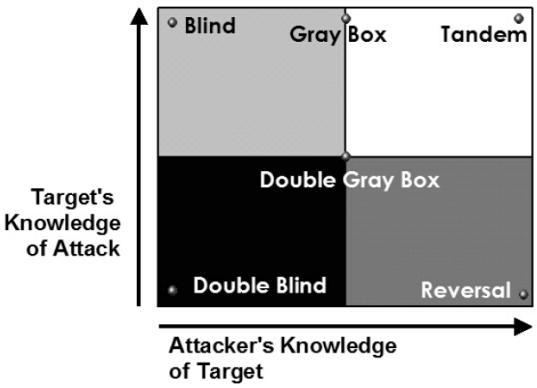
1. Ορίζουμε αυτό που θέλουμε να προστατεύσουμε. Αυτά είναι τα αγαθά (assets). Οι μηχανισμοί προστασίας για αυτά τα αγαθά είναι οι Έλεγχοι (Controls) που θα εξετάσουμε για να προσδιορίσουμε τους Περιορισμούς (Limitations).
2. Προσδιορίζουμε την περιοχή γύρω από τα αγαθά που περιλαμβάνει τους μηχανισμούς προστασίας και τις διαδικασίες ή τις υπηρεσίες που δημιουργούνται γύρω από τα αγαθά. Εντός αυτής της περιοχής θα πραγματοποιηθεί η αλληλεπίδραση με τα αγαθά. Αυτή είναι η ζώνη δέσμευσης (engagement zone).
3. Ορίζουμε οτιδήποτε έξω από τη ζώνη δέσμευσης που είναι απαραίτητο για να διατηρηθούν τα αγαθά λειτουργικά. Αυτό μπορεί να περιλάβει πράγματα, τα οποία μπορεί να μην είμαστε σε θέση να επηρεάσουμε άμεσα, όπως ηλεκτρική ενέργεια, τρόφιμα, ύδρευση, αέρας, σταθερό έδαφος, πληροφορίες, νομοθεσία, κανονισμούς αλλά και πράγματα τα οποία μπορούμε να ρυθμίσουμε όπως ξηρότητα, θερμοκρασία, ψυχραιμία, σαφήνεια, ανάδοχοι, συνάδελφοι, συνεργασίες, και τα λοιπά. Επίσης, συμπεριλαμβάνουμε οτιδήποτε είναι απαραίτητο για να διατηρείται η υποδομή λειτουργική, όπως οι διαδικασίες και τα πρωτόκολλα. Αυτή είναι η εμβέλεια του ελέγχου (test scope).
4. Ορίζουμε τις αλληλεπιδράσεις εντός της εμβέλειας που έχουμε καθορίσει καθώς και τις αλληλεπιδράσεις της εμβέλειας με τον εξωτερικό κόσμο. Εκτελούμε έναν λογικό διαχωρισμό των αγαθών του πεδίου ανάλογα με την κατεύθυνση των αλληλεπιδράσεων όπως: εσωτερικό προς εξωτερικό, εξωτερικό προς εσωτερικό, εσωτερικό προς εσωτερικό, τμήμα Α προς τμήμα Β, κ.λπ. Αυτά είναι τα διανύσματά που θα χρησιμοποιήσουμε στη συνέχεια. Κάθε διάνυσμα θα πρέπει ιδανικά να είναι ένας ξεχωριστός έλεγχος, για να είναι σύντομη η διάρκεια του ελέγχου σε κάθε ξεχωριστή αλληλεπίδραση, έτσι ώστε να ολοκληρώνονται οι έλεγχοι πριν γίνουν πολύ μεγάλες αλλαγές στο περιβάλλον.
5. Προσδιορίζουμε τι εξοπλισμός θα απαιτηθεί για κάθε έλεγχο. Μέσα σε κάθε διάνυσμα, μπορεί να εμφανιστούν αλληλεπιδράσεις σε διάφορα επίπεδα. Αυτά τα επίπεδα μπορούν να ταξινομηθούν με πολλούς τρόπους: ένας δόκιμος τρόπος ταξινόμησης ορίζει σε πέντε κανάλια (channels). Τα κανάλια είναι Human (ανθρώπινο), Physical (φυσικό), Wireless (ασύρματο), Telecommunications (τηλεπικοινωνίες) και Data Networks (δίκτυα δεδομένων). Κάθε κανάλι πρέπει να εξεταστεί χωριστά για κάθε διάνυσμα.
6. Καθορίζουμε ποιες πληροφορίες θέλουμε να μάθουμε από τον έλεγχο. Θα καθορίσουμε αν θα εξετάζουμε τις αλληλεπιδράσεις με τα αγαθά μόνον ή επιπρόσθετα και την απόκριση από τα ενεργά μέτρα ασφάλειας; Ο τύπος ελέγχου πρέπει να καθοριστεί χωριστά για κάθε έλεγχο, εντούτοις υπάρχουν έξι κοινοί τύποι που προσδιορίζονται ως εξής: Blind, Double Blind, Gray Box, Double Gray Box, Tandem, και Reversal (βλ. υποενότητα 2.3.2).

7. Βεβαιωνόμαστε ότι οι έλεγχοι ασφάλειας που έχουμε ορίσει είναι σύμφωνοι με τους κανόνες δέσμευσης (Rules of Engagement). Η επιβεβαίωση αυτή προσπαθεί να διασφαλίσει ότι η διαδικασία για τον έλεγχο ασφάλειας είναι κατάλληλη και δεν δημιουργεί παρανοήσεις, παρερμηνείες ή ψεύτικες προσδοκίες.

Το τελικό αποτέλεσμα θα είναι μια μέτρηση της *επιφάνειας επίθεσης* (attack surface) του συστήματός μας. Η επιφάνεια επίθεσης είναι το μη προστατευμένο μέρος της εμβέλειας (Scope) από ένα καθορισμένο διάνυσμα (Vector).

2.3.2 Τύποι Ελέγχου Ασφάλειας

Ο «Έλεγχος Ασφάλειας» είναι ένας όρος-ομπρέλα που χρησιμοποιείται προκειμένου να καλύψει όλες τις μορφές και τα είδη των ελέγχων ασφάλειας από την παρείσφρηση (intrusion) μέχρι τον hands-on έλεγχο. Η εφαρμογή της μεθοδολογίας δεν αποκλείει κάποιον τύπο ελέγχου.



Σχήμα 14. Διάγραμμα των τύπων ελέγχων ασφάλειας με άξονες τη γνώση επιτιθεμένου στόχου και τη γνώση στόχου επίθεσης

Εντούτοις αυτή η μεθοδολογία, ως πρότυπο, δεν έχει σχεδιαστεί για να ακολουθηθεί με αυστηρά προκαθορισμένα μέσα. Η πρακτική εφαρμογή αυτής της μεθοδολογίας απαιτεί μεμονωμένες πρακτικές ελέγχων ώστε να καλυφθούν οι απαιτήσεις που καθορίζονται κάθε φορά. Αυτό σημαίνει ότι ακόμα και όταν ακολουθηθεί αυτή η μεθοδολογία, η εφαρμογή της -ή ακόμη καλύτερα- η τεχνική μας, θα απεικονίσει τον τύπο του ελέγχου που έχουμε επιλέξει να κάνουμε. Οι βασικοί τύποι ελέγχων είναι οι έξι ακόλουθοι, αλλά δεν υπάρχει κανένας περιορισμός στο να συμπεριληφθεί οποιοσδήποτε άλλος.

1. Τυφλός (Blind): Ο ελεγκτής αναλύει τον στόχο χωρίς προγενέστερη γνώση των αμυνών, των αγαθών ή των καναλιών του. Ο στόχος προετοιμάζεται για τον έλεγχο γνωρίζοντας εκ των προτέρων όλες τις λεπτομέρειες του ελέγχου. Ένας τυφλός έλεγχος εξετάζει πρώτιστα τις δεξιότητες του ελεγκτή. Το εύρος και το βάθος ενός τυφλού ελέγχου μπορούν να είναι τόσο αχανείς όσο επιτρέπει η σχετιζόμενη γνώση και η αποδοτικότητα του ελεγκτή.
2. Διπλά τυφλός (Double Blind): Επίσης γνωστός και ως έλεγχος μαύρου κουτιού (black box audit). Ο ελεγκτής αναλύει τον στόχο χωρίς καμία προγενέστερη γνώση των αμυνών, των αγαθών ή των καναλιών του. Ο στόχος δεν ενημερώνεται εκ των προτέρων σχετικά με την εμβέλεια του ελέγχου, για τα κανάλια που θα ελεγχθούν, ή για τα διανύσματα του ελέγχου. Ένας διπλά τυφλός έλεγχος εξετάζει τις δεξιότητες του ελεγκτή και την ετοιμότητα του στόχου σε άγνωστες μεταβλητές αναταραχής (agitation). Το εύρος και το

βάθος ενός διπλά τυφλού ελέγχου μπορούν να είναι τόσο αχανείς όσο επιτρέπει η εφαρμόσιμη γνώση και η αποδοτικότητα του ελεγκτή.

3. Γκρίζο κουτί (Gray Box): Ο ελεγκτής αναλύει τον στόχο με περιορισμένη γνώση των αμυνών και των αγαθών του και πλήρη γνώση των καναλιών. Ο στόχος προετοιμάζεται για τον έλεγχο γνωρίζοντας εκ των προτέρων όλες τις λεπτομέρειες του ελέγχου. Ένας έλεγχος γκρίζου κουτιού δοκιμάζει τις δεξιότητες του ελεγκτή και την ετοιμότητα του στόχου σε άγνωστες μεταβλητές αναταραχής. Το χαρακτηριστικό του συγκεκριμένου τύπου ελέγχου είναι η αποδοτικότητα. Το εύρος και το βάθος εξαρτώνται από την ποιότητα των πληροφοριών που παρέχονται στον ελεγκτή πριν από τον έλεγχο, καθώς επίσης και από τη σχετιζόμενη γνώση του ελεγκτή.
4. Διπλά γκρίζο κουτί (Double Gray Box): Ο τύπος αυτός του ελέγχου είναι επίσης γνωστός και ως έλεγχος λευκού κουτιού (white box test). Ο ελεγκτής αναλύει τον στόχο με περιορισμένη γνώση των αμυνών και των αγαθών του και με την πλήρη γνώση των καναλιών. Ο στόχος ενημερώνεται εκ των προτέρων για την εμβέλεια και το χρονικό πλαίσιο του ελέγχου αλλά όχι για τα κανάλια που θα ελεγχθούν ή τα διανύσματα του ελέγχου. Ένας έλεγχος διπλά γκρίζου κουτιού δοκιμάζει τις δεξιότητες του ελεγκτή και την ετοιμότητα του στόχου σε άγνωστες μεταβλητές αναταραχής. Το χαρακτηριστικό του ελέγχου είναι η αποδοτικότητα. Το εύρος και το βάθος του ελέγχου εξαρτώνται από την ποιότητα των πληροφοριών που παρέχονται στον ελεγκτή και τον στόχο πριν από τον έλεγχο, καθώς επίσης και τη σχετιζόμενη γνώση του ελεγκτή.
5. Διαδοχικός (tandem): Επίσης γνωστός και ως έλεγχος κρυστάλλινου κουτιού (crystal box). Ο ελεγκτής και ο στόχος είναι έτοιμοι για τον έλεγχο, γνωρίζοντας και οι δύο εκ των προτέρων όλες τις λεπτομέρειες του ελέγχου. Ένας διαδοχικός έλεγχος εξετάζει την προστασία και τους ελέγχους του στόχου. Εντούτοις, δεν μπορεί να εξετάσει την ετοιμότητα του στόχου σε άγνωστες μεταβλητές αναταραχής. Το χαρακτηριστικό του ελέγχου είναι η πληρότητα, δεδομένου ότι ο ελεγκτής έχει την πλήρη άποψη όλων των ελέγχων και των αποκρίσεων τους συμπεριλαμβανομένων και των περιπτώσεων εκείνων που δεν κάνουν καμία επιστροφή. Το εύρος και το βάθος εξαρτώνται από την ποιότητα των πληροφοριών που παρέχονται στον ελεγκτή πριν από τον έλεγχο, καθώς επίσης και από τη σχετιζόμενη γνώση του ελεγκτή.
6. Αντιστροφή (Reversal): Ο ελεγκτής αναλύει τον στόχο με πλήρη γνώση του στόχου, τις διαδικασίες του και τη λειτουργική ασφάλεια αλλά ο στόχος δεν ξέρει τίποτα σχετικά με το που, πώς, ή πότε ο ελεγκτής θα διενεργήσει τους ελέγχους. Το χαρακτηριστικό αυτού του ελέγχου είναι να ελεγχθεί η ετοιμότητα του στόχου σε άγνωστες μεταβλητές και διανύσματα αναταραχής. Το εύρος και το βάθος εξαρτώνται από την ποιότητα των πληροφοριών που παρέχονται στον ελεγκτή και τη σχετιζόμενη γνώση αλλά και τη δημιουργικότητα του ελεγκτή.

Σε περίπτωση υποβολής έκθεσης του ελέγχου, θα πρέπει να προσδιοριστεί ακριβώς ο τύπος ελέγχου που διενεργήθηκε. Πάρα πολύ συχνά, οι έλεγχοι διαφορετικών τύπων test συγκρίνονται για να ανιχνεύσουν το delta (αποκλίσεις) από μια καθιερωμένη αρχική τιμή της παρουσίας της ασφάλειας. Εάν ο ακριβής τύπος test δεν είναι διαθέσιμος σε έναν τρίτο (third-party) αναθεωρητή ή ρυθμιστή, ο ίδιος ο

έλεγχος θα πρέπει να θεωρηθεί ως Blind test, που είναι αυτός με τη λιγότερη αξία σε ένα λεπτομερές έλεγχο ασφάλειας.

2.3.3 Τμήματα και ενότητες

Η μεθοδολογία χωρίζεται σε: τμήματα (sections), ενότητες (modules) και εργασίες (tasks). Τα τμήματα είναι συγκεκριμένα σημεία στο χάρτη ασφάλειας, τα οποία επικαλύπτονται το ένα με το άλλο και αρχίζουν να τεμαχίζουν ένα σύνολο που είναι πολύ λιγότερο από το άθροισμα των μερών του. Οι ενότητες αφορούν τη ροή της μεθοδολογίας από το ένα σημείο της παρουσίας ασφάλειας στο άλλο. Κάθε ενότητα έχει μια είσοδο (input) και μια έξοδο (output). Η είσοδος είναι οι πληροφορίες που χρησιμοποιούνται για την εκτέλεση κάθε εργασίας. Η έξοδος είναι το αποτέλεσμα των ολοκληρωμένων εργασιών. Η έξοδος μπορεί να είναι ή να μην είναι δεδομένα τα οποία έχουν αναλυθεί ώστε να χρησιμεύσουν ως είσοδος για μία άλλη ενότητα. Μπορεί ακόμη να υπάρχει η περίπτωση όπου, η ίδια έξοδος χρησιμεύει ως είσοδος για περισσότερες από μία ενότητες ή εργασίες.

Μερικές εργασίες δεν παράγουν καμία έξοδο: αυτό σημαίνει ότι θα υπάρχουν και συνιστώσες χωρίς είσοδο, και οι ενότητες αυτές μπορούν να αγνοηθούν κατά τη διάρκεια του ελέγχου. Το γεγονός ότι θα αγνοηθούν ενότητες δεν υποδηλώνει απαραιτήτως υποβάθμιση της ποιότητας του ελέγχου, αντιθέτως μπορεί να υποδηλώνει ανώτερη ασφάλεια.

Η ύπαρξη ενοτήτων που δεν έχουν καμία έξοδο ως αποτέλεσμα, μπορεί να σημαίνει ένα από τα παρακάτω:

- Το κανάλι παρεμποδίστηκε με κάποιο τρόπο κατά τη διάρκεια της εκτέλεσης των εργασιών.
- Οι εργασίες δεν εκτελέσθηκαν κατάλληλα.
- Οι εργασίες δεν είχαν έδαφος εφαρμογής (not applicable).
- Τα δεδομένα αποτελέσματος της εργασίας έχουν αναλυθεί εσφαλμένα.
- Η εργασία καταδεικνύει ύπαρξη ανώτερης ασφάλειας.

Είναι ζωτικής σημασίας να υπάρχει αμεροληψία στην εκτέλεση των εργασιών κάθε ενότητας. Η έρευνα για κάτι που δεν έχουμε καμία πρόθεση να βρούμε, μπορεί να μας οδηγήσει ακριβώς σε αυτό που θέλουμε. Σε αυτή την μεθοδολογία, κάθε ενότητα αρχίζει με το να θεωρείται ως μια είσοδος και έξοδος, ακριβώς για να διατηρήσει την προκατάληψη στο ελάχιστο. Κάθε ενότητα δίνει μια κατεύθυνση για το τι θα πρέπει να αποκαλυφθεί ώστε να προχωρήσει περαιτέρω η ροή του ελέγχου.

Ο χρόνος είναι σχετικός. Μεγαλύτερα περιβάλλοντα ελέγχου απαιτούν να δαπανάται περισσότερος χρόνος σε κάθε τμήμα, ενότητα και εργασία. Το χρονικό διάστημα που ορίζεται να περιμένουμε έως ότου να έχουμε δεδομένα εξόδου, εξαρτάται από τον ελεγκτή, το περιβάλλον του ελέγχου και την εμβέλεια του έργου. Για τον καθορισμό του κατάλληλου ελέγχου πρέπει να επιτευχθεί μια ισορροπία ανάμεσα στο χρόνο και την ενέργεια, όπου ο χρόνος είναι χρήμα και η ενέργεια είναι το όριο της προσπάθειας των ανθρώπων και της ισχύος των μηχανών που θα αφιερώσουμε στον έλεγχο.

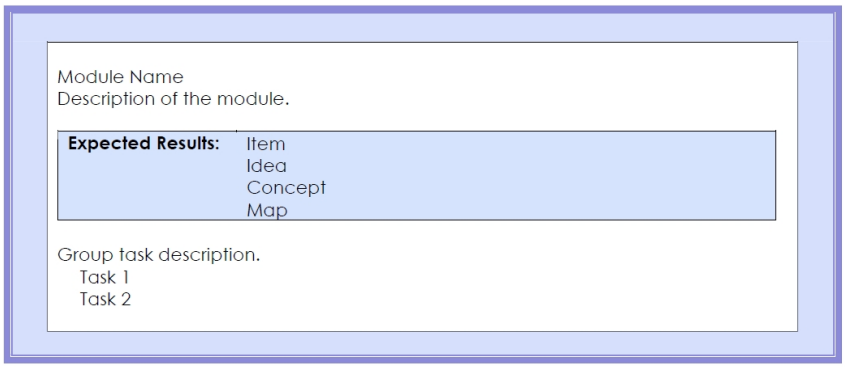
Ο προσδιορισμός εργασιών που μπορεί να θεωρηθούν ως "λιγότερο σημαντικές" και άρα μπορούν να αφαιρεθούν από τον έλεγχο χωρίς να αυξάνεται υπέρμετρα η επισφάλεια, είναι ζωτικής σημασίας όταν γίνεται καθορισμός των ενοτήτων ελέγχου για ένα σύστημα στόχων, όπου είτε η εμβέλεια του έργου είτε οι περιορισμοί του έργου το απαιτούν. Για τις εργασίες που παραλείπονται, θα πρέπει να

τεκμηριωθεί σαφώς ο λόγος παράλειψής τους και να συμφωνηθεί η παράλειψή τους πριν από τον έλεγχο.

Μια και ο έλεγχος παρέχεται με τη μορφή υπηρεσίας, είναι ιδιαίτερα σημαντικό να προσδιοριστεί από το αναθέτων συμβαλλόμενο μέρος το τι ακριβώς δεν έχει εξεταστεί και τι δε θα εξεταστεί. Με αυτόν τον τρόπο γίνεται διαχείριση των προσδοκιών και ενδεχομένως της μη τεκμηριωμένης εικόνας για την ασφάλεια ενός συστήματος.

2.3.4 Ενότητες και εργασίες ελέγχου

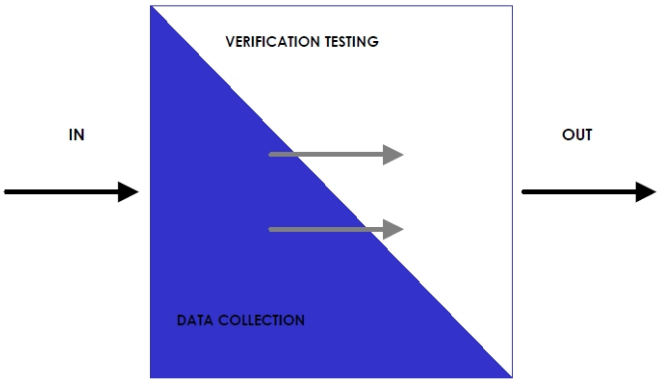
Στο Σχήμα 15 φαίνεται ένα παράδειγμα περιγραφής μιας ενότητας και των εργασιών που περιλαμβάνει.



Σχήμα 15. Παράδειγμα ενότητας

2.3.5 Μεθοδολογία

Η μεθοδολογία ρέει από την αρχική ενότητα προς την ολοκλήρωση της τελικής ενότητας. Η μεθοδολογία επιτρέπει έναν διαχωρισμό μεταξύ της συλλογής των δεδομένων (data collection) και του ελέγχου επαλήθευσης (verification testing) σε αυτά τα δεδομένα που συλλέχθηκαν. Η ροή μπορεί επίσης να καθορίσει τα ακριβή σημεία για το πότε να εξαγάγει και πότε να εισάγει αυτά τα δεδομένα.



Σχήμα 16. Μεθοδολογία

Κατά τον καθορισμό της μεθοδολογίας ελέγχου, είναι σημαντικό να μην περιοριστεί η δημιουργικότητα του ελεγκτή (tester) με την εισαγωγή προτύπων τόσο τυπικών και άκαμπτων που μπορεί να οδηγήσουν στην υποβάθμιση της ποιότητας του ελέγχου. Επιπλέον, είναι σημαντικό να αφεθούν οι εργασίες (tasks) ανοικτές σε

μία διαδικασία ερμηνείας των αποτελεσμάτων τους, διότι ο ακριβής καθορισμός τους θα οδηγήσει σε ακαταλληλότητα των συμπερασμάτων όταν εισάγεται νέα τεχνολογία.

Κάθε ενότητα έχει σχέση με την προηγούμενή της και την επόμενή της. Κάθε τμήμα (section) έχει τις σχετικές πτυχές με άλλες ενότητες και μερικά συσχετίζονται με όλα τα άλλα τμήματα. Συνολικά, ο έλεγχος ασφάλειας αρχίζει με μια είσοδο (input), η οποία συνίσταται τελικά στις διευθύνσεις των συστημάτων που εξετάζονται. Ο έλεγχος ασφάλειας τελειώνει με την έναρξη της φάσης ανάλυσης και τη σύνταξη της τελικής έκθεσης (report). Αυτή η μεθοδολογία δεν έχει επιπτώσεις στη μορφή, το μέγεθος, το ύφος ή το περιεχόμενο της τελικής έκθεσης, ούτε διευκρινίζει το πώς τα δεδομένα πρόκειται να αναλυθούν. Αυτό αφήνεται στον ελεγκτή ή τον οργανισμό ασφάλειας.

Ο ρόλος των τμημάτων είναι να διαιρέσει το σύνολο του πρότυπου ασφάλειας σε εύχρηστες, ελέγξιμες κατατμήσεις. Οι ενότητες είναι οι μεταβλητές ελέγχου εντός των τμημάτων. Η ενότητα απαιτεί μια είσοδο (input) για να εκτελέσει τις εργασίες (tasks) εντός της ίδιας της ενότητας καθώς και σε ενότητες άλλων τμημάτων. Οι εργασίες είναι οι έλεγχοι ασφάλειας που πρέπει να εκτελεστούν ανάλογα με την είσοδο της ενότητας. Τα αποτελέσματα των στόχων μπορεί να αναλυθούν αμέσως για να αποτελέσουν ένα επεξεργασμένο αποτέλεσμα ή να αφεθούν ακατέργαστα. Σε κάθε περίπτωση, θεωρούνται ως η έξοδος (output) της ενότητας. Αυτή η έξοδος είναι συχνά η είσοδος για μία επόμενη ενότητα ή σε ορισμένες περιπτώσεις, όπως π.χ. όταν ανακαλύπτονται νέοι υπολογιστές, μπορεί να αποτελέσουν είσοδο για μία προηγούμενη ενότητα. Ολόκληρο το πρότυπο ασφάλειας μπορεί να χωριστεί σε διαχειρίσιμα τμήματα για να ελεγχθεί. Κάθε τμήμα μπορεί στη συνέχεια να αντιμετωπισθεί ως μια συλλογή από ενότητες ελέγχου, με κάθε ενότητα να χωρίζεται σε σύνολα από εργασίες.

2.3.6 Παραδείγματα

Στη συνέχεια, θα γίνει αναφορά σε τρία παραδείγματα ενοτήτων και των αντίστοιχων εργασιών τους. Θα αναφερθεί η περιγραφή της ενότητας, τα αναμενόμενα αποτελέσματα και τα βήματα που εφαρμόζονται για κάθε έλεγχο. Συγκεκριμένα, παρουσιάζονται ο Έλεγχος Καθοδηγούμενης Πρότασης του τμήματος 2 (Έλεγχος Ασφάλειας Διαδικασιών) και οι Έλεγχος Άρνησης Υπηρεσιών και Παραβίαση Κωδικού Πρόσβασης του τμήματος 3 (Έλεγχος Ασφάλειας Τεχνολογίας Διαδικτύου).

2.3.6.1 Έλεγχος Καθοδηγούμενης Πρότασης (Guided Suggestion Testing)

Περιγραφή

Είναι μια μέθοδος απαρίθμησης, καθώς και απαρίθμησης σημείων πρόσβασης (με προνόμια) σε έναν οργανισμό και στα αγαθά του, προσκαλώντας το εσωτερικό προσωπικό με χρήση μέσων επικοινωνίας όπως το τηλέφωνο, το ηλεκτρονικό ταχυδρομείο, το chat, οι πίνακες ανακοινώσεων, κ.λπ. σε μια εξωτερική τοποθεσία από μια ψευδώς «προνομιούχο» θέση. Αυτή η τεχνική πρόσκλησης απαιτεί μια «τοποθεσία» για το πρόσωπο που καλείται σε αυτήν, όπως μια ιστοσελίδα ή ένας λογαριασμός ηλεκτρονικού ταχυδρομείου.

Αναμενόμενα αποτελέσματα:

- Λίστα των σημείων πρόσβασης.
- Λίστα των εσωτερικών διευθύνσεων IP.
- Μέθοδοι απόκτησης αυτών των πληροφοριών.

- Λίστα των πληροφοριών που λαμβάνονται

Βήματα που εφαρμόζονται για έναν έλεγχο Καθοδηγούμενης Πρότασης:

- Επιλογή ενός πρόσωπου ή περισσοτέρων από τις πληροφορίες που έχουν ήδη ληφθεί σχετικά με το προσωπικό.
- Εξέταση των μεθόδων επαφής για τους χρήστες από τον οργανισμό στόχου.
- Πρόσκληση των χρηστών να χρησιμοποιήσουν ή να επισκεφθούν την τοποθεσία.
- Συγκέντρωση πληροφοριών από τους επισκέπτες.
- Απαρίθμηση του τύπου και της ποσότητας των πληροφοριών που αποκαλύφθηκαν.

2.3.6.2 Έλεγχος Άρνησης Υπηρεσιών - Denial of Service Testing

Περιγραφή

Το Denial of Service-Άρνηση υπηρεσίας (DoS) είναι μια κατάσταση όπου μια περίσταση, είτε σκόπιμα είτε τυχαία, αποτρέπει το σύστημα από την κανονική λειτουργία του. Σε ορισμένες περιπτώσεις, το σύστημα μπορεί να λειτουργεί ακριβώς όπως είχε σχεδιαστεί, εντούτοις, ποτέ δεν είχε την πρόθεση να χειρίζεται το φορτίο, την εμβέλεια της εφαρμογής, είτε τις παραμέτρους που επιβάλλει. Είναι πολύ σημαντικό ότι το DoS λαμβάνει πρόσθετη υποστήριξη από τον οργανισμό και παρακολουθείται στενά. Οι επιθέσεις Flood και Distributed (DDoS) συγκεκριμένα δεν εξετάζονται και απαγορεύεται να εξεταστούν σύμφωνα με αυτό το εγχειρίδιο. Αυτές οι επιθέσεις πάντα θα προκαλούν ορισμένα προβλήματα και συχνά όχι μόνο στο στόχο αλλά και σε όλους τους δρομολογητές και στα συστήματα που υπάρχουν ανάμεσα στον ελεγκτή και τον στόχο.

Αναμενόμενα αποτελέσματα:

- Λίστα των αδύναμων σημείων στη διαδικτυακή παρουσία του οργανισμού συμπεριλαμβανομένων των σημείων συνολικής αποτυχίας.
- Καθιέρωση μιας βασικής γραμμής (baseline) για κανονική χρήση.
- Αποτύπωση των συμπεριφορών του συστήματος σε βαριά χρήση.
- Λίστα των συστημάτων που είναι τρωτά σε επιθέσεις τύπου DoS.

Βήματα που εφαρμόζονται για έναν έλεγχο DoS:

- Έλεγχος για το εάν εξασφαλίζονται κατάλληλα οι λογαριασμοί των διαχειριστών και τα αρχεία και οι πόροι των συστημάτων, καθώς και αν όλη η πρόσβαση παρέχεται με «Ελάχιστα Προνόμια (Least Privilege)».
- Έλεγχος των περιορισμών έκθεσης των συστημάτων σε μη-έμπιστα δίκτυα.
- Έλεγχος για το ότι οι βασικές γραμμές έχουν καθιερωθεί για την κανονική δραστηριότητα των συστημάτων.
- Έλεγχος για το ποιες διαδικασίες είναι σε θέση να ανταποκριθούν σε μη κανονική δραστηριότητα.
- Έλεγχος των αποκρίσεων στις επιθέσεις προσομοίωσης αρνητικών πληροφοριών (προπαγάνδα).
- Έλεγχος ιδιαίτερα αυξημένων φορτίων δικτύου και εξυπηρέτη.

2.3.6.3 Παραβίαση Συνθηματικού - Password Cracking

Περιγραφή

Το password cracking είναι μια διαδικασία επικύρωσης της «ισχύος» ενός συνθηματικού-κωδικού πρόσβασης μέσω της χρήσης αυτοματοποιημένων εργαλείων ανάκτησης συνθηματικών, τα οποία αποκαλύπτουν είτε τις εφαρμογές με αδύναμους

αλγόριθμους κρυπτογράφησης, είτε τη λανθασμένη εφαρμογή αυτών, ή και τους αδύναμους κωδικούς πρόσβασης λόγω ανθρώπινων παραγόντων. Αυτή η ενότητα δεν θα πρέπει να συγχέεται με την ανάκτηση κωδικών μέσω υποκλοπής (sniffing) μη κρυπτογραφημένων καναλιών, η οποία μπορεί να είναι μία πολύ απλούστερη προσέγγιση για την υπονόμευση της ασφάλειας των συστημάτων, εξαιτίας των μη κρυπτογραφημένων μηχανισμών αυθεντικοποίησης και όχι της ίδιας της αδυναμίας του συνθηματικού. Θα πρέπει να σημειωθεί ότι αυτή η ενότητα μπορεί να περιέχει χειροκίνητες (manual) τεχνικές εύρεσης συνθηματικών, οι οποίες εκμεταλλεύονται προεπιλεγμένους συνδυασμούς ονομάτων χρήστη και συνθηματικών σε εφαρμογές ή λειτουργικά συστήματα (π.χ. Username: System Password: Test) ή εύκολα στην εύρεση συνθηματικά από σφάλμα του χρήστη (π.χ. Username: joe, Password: joe). Αυτός μπορεί να είναι ένας τρόπος ώστε να γίνει εφικτή η απόκτηση πρόσβασης σε ένα σύστημα, ίσως και πρόσβαση με προνόμια διαχειριστή.

Έχοντας αποκτήσει δικαιώματα διαχειριστή σε ένα υπολογιστικό σύστημα, το password cracking μπορεί να συμβάλλει στην απόκτηση πρόσβασης και σε επιπρόσθετα συστήματα ή εφαρμογές και αποτελεί μια έγκυρη τεχνική που μπορεί να χρησιμοποιηθεί σε συστήματα που διερευνώνται διαμέσου ενός ελέγχου ασφάλειας. Ένα λεπτομερές password cracking μπορεί επίσης να εφαρμοστεί ως μια απλή μεταγενέστερη άσκηση και μπορεί να επισημάνει την ανάγκη για ισχυρότερους αλγόριθμους κρυπτογράφησης για την αποθήκευση των συνθηματικών σε βασικά συστήματα, καθώς και να προβάλλει την ανάγκη για την ενίσχυση της χρήσης ισχυρότερων συνθηματικών μέσω αυστηρότερης πολιτικής, αυτόματης παραγωγής, ή ενότητες ενσωματωμένης αυθεντικοποίησης (pluggable authentication modules-PAMs).

Αναμενόμενα αποτελέσματα:

- Το αρχείο των συνθηματικών να είναι «σπασμένο» ή «μη σπασμένο».
- Λίστα των ταυτοτήτων σύνδεσης (login IDs) με συνθηματικά χρήστη ή συστήματος.
- Λίστα των συστημάτων που είναι ευαίσθητα σε επιθέσεις τύπου παραβίασης συνθηματικού.
- Λίστα από έγγραφα ή αρχεία που είναι ευαίσθητα σε επιθέσεις τύπου παραβίασης συνθηματικού.
- Λίστα συστημάτων με ταυτότητες χρήστη ή συστήματος που χρησιμοποιούν τους ίδιους κωδικούς πρόσβασης.

Βήματα που εφαρμόζονται για την ανάκτηση των συνθηματικών:

- Αναζήτηση του αρχείου των συνθηματικών από το σύστημα που αποθηκεύει τα ονόματα των χρηστών (usernames) και τους αντίστοιχους κωδικούς πρόσβασης (passwords).
  - Σε συστήματα UNIX, το αρχείο μπορεί να είναι είτε το /etc/passwd είτε το /etc/shadow.
  - Σε συστήματα UNIX, τα οποία εκτελούν αυθεντικοποίηση SMB, τα συνθηματικά NT μπορούν να βρεθούν στο /etc/smbpasswd.
  - Σε συστήματα Windows (NT, 2000 κ.λπ.), το αρχείο μπορεί να είναι στο /winnt/repair/Sam. (ή και σε άλλο, όμως σε αυτήν την περίπτωση θα είναι δυσκολότερη η ανάκτηση των συνθηματικών)
- Υλοποίηση μιας επίθεσης της μορφής automated dictionary στο αρχείο με τα συνθηματικά.

- Υλοποίηση μιας επίθεσης της μορφής εξαντλητικής δοκιμής (brute-force) στο αρχείο με τα συνθηματικά, για όσο ο χρόνος και οι κύκλοι της επεξεργασίας το επιτρέπουν.
- Χρήση των ανακτημένων συνθηματικών ή των παραλλαγών τους, για την πρόσβαση σε επιπλέον συστήματα ή εφαρμογές.
- Χρήση αυτοματοποιημένων προγραμμάτων (password crackers) σε κρυπτογραφημένα αρχεία τα οποία μπορούν να αντιμετωπιστούν (αρχεία όπως PDF ή Word) σε μια προσπάθεια να αποκτηθούν περισσότερες πληροφορίες και να επισημανθεί η ανάγκη για ισχυρότερη κρυπτογράφηση σε αρχεία και σε συστήματα αρχείων.

2.3.7 Πρότυπα Απαιτήσεων Έκθεσης - Report Requirements Templates

Τα ακόλουθα πρότυπα είναι ένα μικρό παράδειγμα των απαιτήσεων της έκθεσης σύμφωνα με αυτό που θα πρέπει να επιδειχθεί σε μια έκθεση ώστε να χαρακτηριστεί ως πιστοποιημένη σύμφωνα με το OSSTMM. Ισχύουν οι περιορισμοί δυνατότητας εφαρμογής (applicability) και εμβέλειας.

- Network Profile Template - Πρότυπο Σχεδιαγράμματος Δικτύων
- Server Information Template - Πρότυπο Πληροφοριών εξυπηρέτη (server)
- Firewall Analysis Template - Πρότυπο Ανάλυσης Τείχους Προστασίας
- Advanced Firewall Testing Template - Πρότυπο Προηγμένου Ελέγχου Τείχους Προστασίας
- IDS Test Template - Πρότυπο Ελέγχου IDS
- Social Engineering Target Template - Πρότυπο Στόχου Κοινωνικής Μηχανικής
- Social Engineering Telephone Attack Template - Πρότυπο Τηλεφωνικής Επίθεσης Κοινωνικής Μηχανικής
- Social Engineering E-mail Attack Template - Πρότυπο Επίθεσης Κοινωνικής Μηχανικής μέσω η-ταχυδρομείου
- Trust Analysis Template - Πρότυπο Ανάλυσης Εμπιστοσύνης
- Privacy Review Template – Πρότυπο Επισκόπησης Προστασίας Προσωπικών Δεδομένων
- Containment Measures Review Template - Πρότυπο Επισκόπησης Μέτρων Συνοχής
- E-Mail Spoofing Template - Πρότυπο αντιποίησης η-ταχυδρομείου
- Competitive Intelligence Template - Πρότυπο Ανταγωνιστικής Συλλογής Πληροφοριών
- Password Cracking Template - Πρότυπο Cracking Κωδικού Πρόσβασης
- Denial of Service Template - Πρότυπο Άρνησης Παροχής Υπηρεσιών
- Document Grinding Template - Πρότυπο Συλλογής και Ανάλυσης Εγγράφων
- Social Engineering Template - Πρότυπο Κοινωνικής Μηχανικής
- Legal Penetration Testing Checklist - Πίνακας Νόμιμου Έλεγχου Διείσδυσης

Σύμφωνα με το ISECOM, ο έλεγχος που είναι σύμφωνος με OSSTMM θα πρέπει να διαθέτει τα ακόλουθα ποιοτικά χαρακτηριστικά. Πρέπει να είναι:

- ποσοτικά προσδιορίσιμος
- συνεπές και με δυνατότητα επανάληψης
- βασισμένος σε ένα ευρύ χρονικό πλαίσιο

- βασισμένος στη συμβολή του ελεγκτή
- λεπτομερής
- συμβατός με τους μεμονωμένους και τοπικούς νόμους, καθώς και τη νομοθεσία περί προστασίας των δεδομένων

Αυτό που έλειπε για πολύ μεγάλο διάστημα, στον έλεγχο ασφάλειας, ήταν ένα εγχειρίδιο λίστας ελέγχου (checklist) με σαφείς ορισμούς που να δηλώνει το πώς θα πρέπει να πραγματοποιηθούν συγκεκριμένοι έλεγχοι. Επιπλέον, το OSSTMM απαιτεί να ενσωματωθούν οι βασικές πτυχές ασφάλειας της επιχείρησης, σε σχέση με το υπάρχον επιχειρησιακό πρότυπο. Μόνο τότε μπορεί να γίνουν δηλώσεις σχετικές με τη σφαιρική εταιρική ασφάλεια.

2.4 Εργαλεία για την υποστήριξη της μεθοδολογίας

2.4.1 Εργαλεία υπό ανάπτυξη για το OSSTMM

2.4.1.1 PWDM (http://www.pwdm.net/)

Το PWDM (Πρακτική Μεθοδολογία Εγκατάστασης Ασύρματης Δικτύωσης - Practical Wireless Deployment Methodology) είναι ένα πρακτικό, ανεξάρτητο από τον προμηθευτή, υψηλού επιπέδου πλαίσιο-μεθοδολογία που προορίζεται ώστε να βοηθήσει τα άτομα που επιφορτίζονται με την ανάπτυξη, την αναβάθμιση, τη διατήρηση και την εξασφάλιση των βασισμένων στο 802.11 WLANs, ανεξάρτητα από εάν είναι ιδιωτικά (SOHO, επιχείρηση, σπίτι) ή δημόσια (hotspots).

Η μεθοδολογία περιλαμβάνει τα ακόλουθα βήματα:

- Ανάλυση εγκατάστασης
- Διαπραγμάτευση συμβολαίων και συμφωνητικών
- Προγραμματισμός εγκατάστασης σε τακτικό επίπεδο
- Διαδικασίες εγκατάστασης εξοπλισμού
- Εγκατάσταση ενισχυτικής υποδομής
- Ζητήματα ασφάλειας σημείων πρόσβασης (access points)
- Στρατηγικές αντιμετώπισης ζητημάτων επιπέδου 3
- Διαχείριση του συνόλου της υποδομής
- Ασφάλεια πυλών
- UAT (User Acceptance Testing - Έλεγχος Αποδοχής Χρήστη) & Ανάθεση

2.4.1.2 UnicornScan (http://www.unicornscan.org/)

Πρόκειται για έναν ανιχνευτή (scanner) θυρών και πρωτοκόλλων. Πραγματικά πρόκειται για έναν ανιχνευτή που χαρακτηρίζεται «ειλικρινής», και χρησιμοποιείται σε πολύ μεγάλα δίκτυα παραμένοντας εξίσου γρήγορος. Ο ανιχνευτής χαρακτηρίζεται «ειλικρινής», δεδομένου ότι αναφέρει στον ελεγκτή ακριβώς τι επιστρέφεται με ένα σαφές σχήμα χωρίς περιπλοκές που μπορεί να ξεγελάσουν τον ελεγκτή. Τα αποτελέσματα μπορούν να πηγαίνουν σε μια βάση δεδομένων SQL ώστε να είναι δυνατή η επανεξέτασή τους στα πλαίσια μιας πλήρους χαρτογράφησης.

Το Unicornscan είναι μια νέα μηχανή συλλογής και συσχετισμού πληροφοριών που δημιουργείται από μέλη της έρευνας της ασφάλειας και των κοινοτήτων που ασχολούνται με τον έλεγχο. Έχει ως σκοπό να παρέχει μια μηχανή που είναι εξελικτική, ακριβής, ευέλικτη και αποδοτική. Χρησιμοποιείται υπό τους όρους της GPL άδειας.

2.4.1.2.1 ***Χαρακτηριστικά***

Το Unicornscan λειτουργεί σε επίπεδο διεργασίας χρήστη, με κατανεμημένο τρόπο και αφορά τη στοίβα πρωτοκόλλων TCP/IP. Ο στόχος του είναι να παρέχει στον ερευνητή-ελεγκτή μία διεπαφή για την εισαγωγή ερεθισμάτων σε μία συσκευή ή ένα δίκτυο που βασίζεται στο TCP/IP και να μετρά τις αντιδράσεις τους. Το κύριο σύνολο των δυνατοτήτων του περιλαμβάνει τα παρακάτω (χωρίς να περιορίζεται σ' αυτά):

- Ασύγχρονη ανίχνευση TCP χωρίς κατάσταση (stateless) με όλες τις παραλλαγές από TCP Flags.
- Ασύγχρονο TCP banner grabbing[9].
- Ασύγχρονη ανίχνευση UDP, με εξειδίκευση στα διάφορα πρωτόκολλα (τα μηνύματα που στέλνονται περιλαμβάνουν επαρκή δεδομένα ώστε να επιστραφεί μια σχετική απάντηση)
- Ενεργός και παθητικός προσδιορισμός απομακρυσμένου λειτουργικού συστήματος, εφαρμογής και συστατικών από την ανάλυση αποκρίσεων.
- Καταγραφή σε αρχεία PCAP και δυνατότητα φιλτραρίσματός τους.
- Έξοδος σε σχεσιακές βάσεις δεδομένων.
- Υποστήριξη προσαρμοσμένων-εξειδικευμένων ενοτήτων.
- Προσαρμοσμένες απόψεις συνόλου δεδομένων.

2.4.1.3 AFD (http://www.purehacking.com/news/afd-technical-details)

Το Active Filter Detection (Ενεργή Ανίχνευση Φίλτρου) είναι ένα βήμα, σύμφωνα με το OSSTMM, το οποίο οι ελεγκτές ασφάλειας θα πρέπει να εκτελέσουν για να προσδιορίσουν την παρουσία των Intrusion Prevention Systems (Συστημάτων Πρόληψης Εισβολών) και άλλων τεχνολογιών που θα επηρέαζαν άμεσα την ποιότητα μιας αξιολόγησης της ασφάλειας. Το πρόγραμμα λειτουργεί χρησιμοποιώντας μία λίστα από γνωστές υπογραφές επιθέσεων, τις οποίες αποστέλλει στον στόχο και παρατηρώντας αν θα κλειδωθεί – αν όντως κλειδωθεί, αυτό σημαίνει ότι υπάρχει ενεργό φίλτρο.

2.4.1.4 DNS Scan (http://www.isecom.org/mirror/scandns.zip)

Ένα PERL script που συμπληρώνει την εργασία της ανίχνευσης σύνδεσης DNS που λειτουργεί κάτω από την ενότητα ανίχνευσης θυρών. Χρησιμοποιεί DNS συνδέσεις σε μια κατηγορία C για να βρει ενεργούς υπολογιστές πίσω από firewalls.

2.4.1.5 MUTATEv2 (http://www.isecom.org/mirror/mutate2.tgz)

Ένα IDS εργαλείο παράκαμψης συστημάτων ανίχνευσης εισβολέων για ενίσχυση στην απαρίθμηση συστημάτων, στην ανίχνευση θυρών και στον έλεγχο ευπαθειών.

[9] Το banner grabbing μπορεί να οριστεί απλά ως η σύνδεση με απομακρυσμένες εφαρμογές και παρατήρηση της εξόδου (output) και μπορεί να είναι εκπληκτικά πληροφοριακή στους απομακρυσμένους επιτιθεμένους. Κατ' ελάχιστο, μπορεί να έχουν προσδιορίσει τον τύπο και το πρότυπο της υπηρεσίας που τρέχει, το οποίο είναι σε πολλές περιπτώσεις αρκετό ώστε να θέσει σε εφαρμογή τη διαδικασία έρευνας για ευπάθειες.

2.4.1.6 Assessment Scanner (http://www.isecom.org/mirror/asstool.zip)

Ένα εργαλείο JAVA που συμπληρώνει την ενότητα Συλλογής και Ανάλυσης Εγγράφων για το ηλεκτρονικό dumpster diving[10]. Υποστηρίζει τις αιτήσεις τύπου GET και POST του HTTP.

2.4.1.7 NWRAP (http://www.isecom.org/mirror/nwrap.zip)

Ένα εργαλείο που σχεδιάστηκε για να προσθέσει την Open Protocol Resource Database, ως πρόσθετη λειτουργία του NMAP. Αυτό θα παρουσιάσει όλα τα γνωστά πρωτόκολλα για τις θύρες που έχουν ανακαλυφθεί, κάτι που θα επεκτείνει σε μεγάλο βαθμό το αρχείο nmap_services που ορίζει μόνο μία υπηρεσία ανά θύρα. Για να λειτουργήσει, θα πρέπει να εγκατασταθεί το NMAP και θα πρέπει να συμπεριληφθεί η τρέχουσα έκδοση του oprp.dump το οποίο πρέπει να είναι στον ίδιο κατάλογο.

2.4.1.8 Metis v. 2.1. (http://www.severus.org/sacha/metis/)

Είναι ένα βασισμένο σε Java εργαλείο για την εκτίμηση του βαθμού στον οποίο μπορούν να συλλεχθούν πληροφορίες για έναν εξυπηρέτη διαδικτύου (web server) από πιθανούς επιτιθέμενους και βοηθά στην ολοκλήρωση του ελέγχου συλλογής πληροφοριών που περιλαμβάνεται στο OSSTMM. Το εργαλείο διανέμεται υπό την δημόσια άδεια GNU.

2.4.1.9 WMAP v. 1.2. (http://www.isecom.org/mirror/wmap1.2.tar.gz)

Ένας λιγότερο απλοϊκός ανιχνευτής ιστού. Αναζητά με εξαντλητική μέθοδο (brute-force[11]) τους γνωστούς καταλόγους για να αποκαλύψει παραλλαγές στη δομή για καλύτερη ανίχνευση ευπάθειας. Επίσης, περιλαμβάνει στην αναζήτηση ονόματα αρχείων και καταλόγων στα Ισπανικά.

2.4.1.10 Firewall tester (Ftester) (http://www.inversepath.com/ftester.html)

Ένα εργαλείο που αναπτύχθηκε σε PERL για τον έλεγχο των λιστών ελέγχου πρόσβασης (ACLs) σε δρομολογητές και firewalls. Ειδικά scripts επιτρέπουν να ικανοποιήσουμε τις απαιτήσεις του ελέγχου κατά το OSSTMM, είτε έχοντας είτε όχι πρόσβαση και στις δύο πλευρές του firewall.

2.4.1.10.1 Χαρακτηριστικά:

- έλεγχος firewall
- έλεγχος συστημάτων ανίχνευσης εισβολών (IDS testing)
- Προσομοίωση πραγματικών TCP συνδέσεων για επιθεώρηση firewalls και IDS λαμβάνοντας υπ' όψιν την κατάσταση του πρωτοκόλλου (statefull)
- αντιποίηση (spoofing) TCP connection
- κατάτμηση (fragmentation) IP / TCP segmentation

---

[10] Το dumpster diving «βουτιά στα σκουπίδια» αποτελεί βασική πηγή συγκέντρωσης πληροφοριών για τους χάκερς. Σε αρκετές χώρες του εξωτερικού θεωρείται «ένοχο» για σειρά τραπεζικών απατών και την υποκλοπή ευαίσθητων προσωπικών στοιχείων πολιτών.

[11] Η brute-force attack (επίθεση *ωμής βίας*) αναφέρεται στην εξαντλητική δοκιμή πιθανών κλειδιών που παράγουν ένα κρυπτογράφημα, ώστε να αποκαλυφθεί το αρχικό μήνυμα. Τέτοιου είδους επιθέσεις, οι οποίες χρησιμοποιούν όλα τα δυνατά κλειδιά, μπορούν πάντοτε να πραγματοποιηθούν. Κατ' αναλογία ο όρος εφαρμόζεται σε οποιοδήποτε πεδίο έχει εφαρμογή η εξαντλητική αναζήτηση.

- τεχνικές παράκαμψης συστημάτων ανίχνευσης εισβολών (IDS evasion techniques)

Πρέπει να σημειωθεί ότι αυτό το εργαλείο είναι πλέον ξεπερασμένο και παρουσιάζεται εδώ για ιστορικούς λόγους, ένα πιο πλήρες με νέα χαρακτηριστικά γνωρίσματα και υποστήριξη IPv6, σχεδιάζεται σύντομα για το μέλλον.

2.4.1.11 nmap 3.48 patch (http://www.isecom.org/mirror/nmap-3.48-random-size.diff)

Αυτό το patch χρησιμοποιείται για να παρέχει ένα τυχαίο μέγεθος φορτίου (payload) στο NMAP για τυχαία Intrusion Detection Systems.

2.4.1.12 Jack of All Trades (http://www.isecom.org/mirror/Jack_of_All_Trades.v2.pdf)

Το JAT είναι ένα εργαλείο για να βελτιώσει τη διαδικασία διαλογής των υπαλλήλων ασφάλειας. Η ασφάλεια είναι ένα γρήγορα μεταβαλλόμενο πεδίο με έναν ευρύ τομέα γνώσης, έτσι απαιτεί υποψηφίους που είναι πολυμήχανοι και στοχαστές με ισχυρή κρίση. Το τμήμα ανθρώπινων πόρων θα πρέπει να βρει τους ανθρώπους αυτού του προφίλ που επίσης ταιριάζουν στο επιχειρησιακό περιβάλλον τους. Αυτό το εργαλείο θα βοηθήσει να γίνει κάτι τέτοιο.

Ο οδηγός JAT Q&A παρέχει πολλαπλά σενάρια ώστε να εξεταστεί λεπτομερώς ο υποψήφιος. Οι τύποι αποτελεσμάτων που έδωσε ο υποψήφιος, είναι ενδεικτικοί του τύπου επαγγελματία ασφάλειας που θα ήταν. Για παράδειγμα, οι υποψήφιοι επέλεξαν μόνο τις προφανείς απαντήσεις και σταμάτησαν ή σκέφτηκαν περισσότερο; Ήξεραν τις τεχνικές λεπτομέρειες ή κόλλησαν σε πεζές περιγραφές; Επίσης, αποκρίθηκαν αποτελεσματικά ανεξάρτητα από το εάν ήξεραν τις απαντήσεις ή όχι;

Το JAT μπορεί επίσης να είναι ένα συμπληρωματικό εγχειρίδιο κατάρτισης για τον έλεγχο και την εκπαίδευση νέων υπαλλήλων ώστε να γίνουν επαγγελματίες ασφάλειας. Είναι βασισμένο στο OSSTMM και χρησιμοποιείται αυτήν την περίοδο ως άσκηση κριτικής σκέψης σχετικής με την ασφάλεια στο OPST και OPSA. Ως εργαλείο κατάρτισης γραφείου, έχει το πλεονέκτημα να εκπαιδεύει το προσωπικό ώστε να σκέφτεται έξω από την πεπατημένη και να μάθει να χρησιμοποιεί τη γνώση του με διαφορετικούς τρόπους.

2.4.2 Εργαλεία για τις ενότητες του OSSTMM

Στον παρακάτω πίνακα παραθέτουμε κάποια εργαλεία (μαζί με τα προηγούμενα), τα οποία μπορούν να χρησιμοποιηθούν για τις διάφορες ενότητες του OSSTMM. Τα εργαλεία καλύπτουν κάποιες ενότητες των τμημάτων: Ασφάλεια Πληροφοριών (Information Security), Ασφάλεια Τεχνολογίας Διαδικτύου (Internet Technology Security) και Ασφάλεια Ασύρματων επικοινωνιών (Wireless Security) του OSSTMM.

Ενότητα που αντιστοιχεί σε κάθε έλεγχο	Εργαλεία
Έλεγχος Ασφάλειας Πληροφοριών - Information Security Testing	
όλες οι ενότητες	Google and Google Hacking Database[1]
Έρευνα Συλλογής Πληροφοριών (Intelligence Survey)	Metis v. 2.1 [2.4.1.8]
Έλεγχος Ασφάλειας Τεχνολογίας Διαδικτύου - Internet Technology Security Testing	
Επισκόπηση Ανίχνευσης Εισβολής (Intrusion Detection Review)	MUTATEv2 [2.4.1.5]

Έρευνα Δικτύων (Network Surveying)	Whireshark[3], TCPDump[4], NetCat[5], Wikto[9]
Ανίχνευση Θυρών (Port Scanning)	Unicornscan[2.4.1.2], DNS Scan[2.4.1.4], Ping Tester, Superscan, Scanline
Προσδιορισμός Υπηρεσιών Συστήματος (System Services Identification)	Nmap, NWRAP[2.4.1.7], WMAP v.1.2 [2.4.1.9]
Συλλογή και Ανάλυση Εγγράφων (Document Grinding)	Assessment Scanner[2.4.1.6]
Έρευνα ευπαθειών/εκμεταλλεύσεων και Επαλήθευση (Vulnerability/Exploit Research and Verification)	Nessus[2], Retina, CoreImpact, Sara Metasploit Framework[10], Canvas
Δρομολόγηση (Routing)	Ftester [2.4.1.10]
Παραβίαση Κωδικού Πρόσβασης (Password Cracking)	PDF Password Cracker Pro, Cain & Abel (windows)[8], John the Ripper (unix), Aircrack[7]
Έλεγχος Άρνησης Υπηρεσιών (Denial of Service Testing)	Udp Flood, DoS HTTP
Έλεγχος Ασφάλειας Ασύρματων επικοινωνιών - Wireless Security Testing	
Έλεγχος Δικτύων 802.11 Ασύρματων επικοινωνιών (802.11 Wireless Networks Testing)	PWDM [2.4.1.1], Kismet[6]

Πίνακας 2. Εργαλεία για τις ενότητες του OSSTMM.

2.5 Συμπεράσματα

2.5.1 Αναβάθμιση από παλαιότερες εκδόσεις

Εάν κάποιος έχει εξοικειωθεί με τη σειρά 2.x του OSSTMM, θα πρέπει να σημειώσουμε ότι η μεθοδολογία έχει αλλάξει σε κάποια σημεία στην έκδοση 3. Συγκεκριμένα, τα RAVs παρέχουν μια πραγματική μετρική επιφάνειας επιθέσεων (Attack Surface) αντί μιας εκτίμησης κινδύνου.

2.5.2 Μια εισαγωγή στην OSSTMM έκδοση 3

Τι είναι το OSSTMM;

Εν ολίγοις, το OSSTMM είναι ένας μηχανισμός που χρησιμοποιείται για να καθορίσει τη λειτουργική ασφάλεια ("OpSec-Operational Security") μια εμβέλειας στόχων. Το OpSec ορίζεται ως ο συνδυασμός "διαχωρισμού και ελέγχων χωρίς περιορισμούς". Είναι ουσιαστικά μια μέτρηση της προστασίας μεταξύ των αγαθών, χρησιμοποιώντας μια φόρμουλα με μια μέθοδο και μια προσέγγιση, προκειμένου να προσδιορίσει και ταξινομήσει ελέγχους (μέτρα ασφάλειας) και περιορισμούς (αδυναμίες ή ευπάθειες). Αυτό που μετριέται πραγματικά είναι η "Attack Surface-επιφάνεια επίθεσης" ενός δεδομένου στόχου, δίνοντας έμφαση στον προσδιορισμό πιθανών ανεπαρκειών στα μέτρα προστασίας που ισχύουν.

Τι δεν είναι το OSSTMM; Δεν είναι μια μεθοδολογία αξιολόγησης κινδύνου (Risk Assessment). Είναι μάλλον ένας τρόπος για συλλογή και ανάλυση δεδομένων ώστε να παραχθούν επαρκή αποτελέσματα που θα βοηθήσουν σε αποφάσεις σχετικές με κινδύνους. Δεδομένου ότι "κίνδυνος" είναι μια υποκειμενική έννοια (όπου η άποψη ενός ατόμου σχετικά με αυτό, διαφέρει από τους άλλους), το OSSTMM είναι ένας τρόπος για να καθοριστεί και να μετρηθεί με συνέπεια η κατάσταση της λειτουργικής ασφάλειας έτσι ώστε οι αποφάσεις για τον κίνδυνο να μπορούν να παρθούν βασισμένες σε επιστημονικά δεδομένα και όχι σε προηγούμενες εμπειρίες, προτιμήσεις προϊόντων ή άλλες προκατειλημμένες ανθρώπινες εισόδους (inputs).

Το OSSTMM δεν είναι μια μεθοδολογία "ανάλυσης απειλής-Threat Analysis". Μάλλον, θα μπορούσαμε να πούμε ότι, δεν υποθέτει τίποτα για συγκεκριμένες απειλές, μόνο για την επιφάνεια επιθέσεων (Attack Surface) και προσπαθεί να προσδιορίσει και να μετρήσει τις ανεπάρκειες (περιορισμούς) στην προστασία των αγαθών. Είναι επίσης επαναλαμβανόμενη και μπορεί να χρησιμοποιηθεί για να μετρήσει την πρόοδο (ή την έλλειψη της ασφάλειας) στις λειτουργίες οποιουδήποτε οργανισμού.

Χρησιμοποιώντας τις ISECOM Risk Assessment Values, είναι πιθανό να επιλύσουμε απλά και εύκολα το πρόβλημα των κύκλων του ελέγχου, χρησιμοποιώντας προκαθορισμένα διαστήματα ελέγχου. Με τη χρησιμοποίηση του ISECOM “Business Security Testing & Analysis Workbook” σε συνδυασμό με τις φόρμες (forms) και τις λίστες ελέγχου (checklists) του OSSTMM, ο έλεγχος μπορεί να πραγματοποιηθεί με τον ίδιο τρόπο κάθε φορά, ανεξάρτητα από το ποιος τον κάνει. Οι φόρμες και οι λίστες ελέγχου του OSSTMM ενεργούν επίσης και ως βασικό πλαίσιο για τις εκθέσεις και βοηθούν πολύ τις επιχειρήσεις στην επίτευξη της συνέπειας υποβολής εκθέσεων από έτος σε έτος.

Κεφάλαιο 3: OWASP - Open Web Application Security Project

3.1 Εισαγωγή

"Ανοικτή και συλλογική γνώση: είναι η προσέγγιση του OWASP." *Matteo Meucci*

Το Έργο Ασφάλειας Εφαρμογών Ιστού Ανοικτού κώδικα (Open Web Application Security Project-OWASP) δημιουργήθηκε ώστε να βοηθάει τους οργανισμούς να κατανοήσουν και να βελτιώσουν την ασφάλεια των δικτυακών τους εφαρμογών και υπηρεσιών. Αποτελεί μια πρωτοβουλία που αποσκοπεί στον εντοπισμό και στην καταπολέμηση των τρωτών σημείων του λογισμικού τέτοιων εφαρμογών.

Στο OWASP θα βρείτε ελεύθερα:

- Εργαλεία και πρότυπα ασφάλειας εφαρμογών.
- Πλήρη βιβλία για τον έλεγχο ασφάλειας εφαρμογών, την ανάπτυξη ασφαλούς κώδικα και την επισκόπηση κώδικα ασφάλειας.
- Τυποποιημένους έλεγχους και βιβλιοθήκες ασφάλειας.
- Local chapters (Τοπικές ομάδες εργασίας) παγκοσμίως.
- Έρευνα αιχμής (Cutting edge research).
- Εκτενείς διασκέψεις παγκοσμίως.
- Mailing lists (Λίστες ηλεκτρονικού ταχυδρομείου).
- Και ακόμη περισσότερα …στο http://www.owasp.org

Σχήμα 17. Συστατικά μέρη του OWASP.

Όλα τα εργαλεία, έγγραφα, forums και κεφάλαια του OWASP είναι ελεύθερα και ανοικτά σε καθέναν που ενδιαφέρεται να βελτιώσει την ασφάλεια των εφαρμογών. Το πρόβλημα της ασφάλειας εφαρμογών αφορά ανθρώπους, διαδικασίες και τεχνολογία και ως εκ τούτου μια αποτελεσματική προσέγγιση επίλυσής του, θα πρέπει να περιλαμβάνει βελτιώσεις σε όλους αυτούς τους τομείς.

Το OWASP είναι ένα νέο είδος οργανισμού. Η ανεξαρτησία του από εμπορικές πιέσεις έχει σαν αποτέλεσμα την παροχή αμερόληπτων, πρακτικών και οικονομικώς αποδοτικών πληροφοριών για την ασφάλεια εφαρμογών. Το OWASP δεν συνδέεται με κάποια επιχείρηση τεχνολογίας, αν και υποστηρίζει την ενημερωμένη χρήση της εμπορικής τεχνολογίας ασφάλειας. Όμοια με πολλά προγράμματα ελεύθερου ή ανοικτού κώδικα (open source) λογισμικού, το OWASP παράγει πολλά είδη υλικών με ένα συλλογικό και ανοικτό τρόπο.

Το OWASP Foundation είναι μια μη κερδοσκοπική οντότητα που εξασφαλίζει τη μακροπρόθεσμη επιτυχία του προγράμματος. Σχεδόν ο καθένας που συνδέεται με το OWASP είναι εθελοντής, συμπεριλαμβανομένων των: Ομάδα Συμβούλων του

OWASP (OWASP Board), Παγκόσμιες Επιτροπές (Global Committees), Επικεφαλείς των Ομάδων εργασίας (Chapter Leaders), Επικεφαλείς Έργων (Project Leaders) και τα μέλη του προγράμματος. Το OWASP αριθμεί μέλη σε όλο τον πλανήτη, συμπεριλαμβανομένων μεγάλων οργανισμών και εταιρειών του χώρου όπως οι VISA, Deloitte, Unisys, Foundstone και άλλες.

3.1.1 Ελληνική ομάδα εργασίας του OWASP

Η ελληνική ομάδα εργασίας του OWASP δημιουργήθηκε το 2005, με κύριο στόχο την ενημέρωση και την αφύπνιση της ελληνικής κοινότητας αναφορικά με τους κινδύνους ασφάλειας στις διαδικτυακές εφαρμογές. Αφορμή για τη δημιουργία της, αποτέλεσαν ουσιαστικά τα ολοένα αυξανόμενα περιστατικά ασφαλείας στο Διαδίκτυο, όπως τα κρούσματα phishing[77] σε ελληνικές τράπεζες.

Σήμερα, η ελληνική ομάδα του OWASP δραστηριοποιείται σε προγράμματα Ελεύθερου ή Ανοικτού λογισμικού καθώς και μεταφράσεις κειμένων του OWASP στα ελληνικά, προωθώντας την ιδέα του OWASP σε τοπικό επίπεδο. Παράλληλα, μέσα από τη mailing list της, ενημερώνει και προκαλεί συζητήσεις σχετικά με επίκαιρα θέματα ασφάλειας στο Διαδίκτυο, ενώ εκδίδει και μηνιαίο newsletter. Επιπλέον, διοργανώνει συναντήσεις και συμμετέχει σε συνέδρια, με στόχο κυρίως την ενημέρωση και την ευαισθητοποίηση γύρω από τα θέματα ασφαλείας.

3.2 Οδηγός ελέγχου του OWASP (OWASP Testing Guide)

3.2.1 Γενικά

3.2.1.1 Εισαγωγή

"Είναι αδύνατο να υποτιμηθεί η σημασία του γεγονότος ότι υπάρχει διαθέσιμος αυτός ο οδηγός με έναν απολύτως ελεύθερο και ανοικτό τρόπο." Jeff Williams (OWASP Chair)

Η δημιουργία ενός οδηγού όπως αυτού, είναι ένα ογκώδες σχέδιο, που αντιπροσωπεύει την εμπειρία εκατοντάδων ανθρώπων σε όλο τον κόσμο. Υπάρχουν πολλοί διαφορετικοί τρόποι οι οποίοι εξετάζουν για ατέλειες ασφάλειας. Αυτός όμως ο οδηγός αποτελεί τη συναίνεση των βασικών εμπειρογνωμόνων στο πώς να εκτελεστεί ένας τέτοιος έλεγχος γρήγορα, με ακρίβεια και αποτελεσματικά. Η ασφάλεια δεν πρέπει να αποτελεί «μαύρη τέχνη (black art)» όπου μόνο μερικοί μπορούν να την ασκήσουν. Ένα μεγάλο μέρος της διαθέσιμης καθοδήγησης της ασφάλειας είναι επαρκές ώστε να καταστήσει τους ανθρώπους ανήσυχους για ένα πρόβλημα, χωρίς να τους παρέχει αρκετές πληροφορίες για να βρουν, να εντοπίσουν και να λύσουν προβλήματα ασφάλειας. Το έργο (project) προκειμένου να δημιουργηθεί αυτός ο οδηγός, διατηρεί την πείρα στα χέρια των ανθρώπων που τη χρειάζονται.

Αυτός ο οδηγός χρειάζεται να κάνει τη διαδρομή του, περνώντας από τους υπεύθυνους ανάπτυξης και τους ελεγκτές λογισμικού. Δεν υπάρχουν αρκετοί εμπειρογνώμονες ασφάλειας εφαρμογών στον κόσμο που μπορούν να κάνουν οποιαδήποτε σημαντική τομή στο γενικό πρόβλημα. Η αρχική ευθύνη για την ασφάλεια εφαρμογών πρέπει να πέσει στους ώμους των υπεύθυνων ανάπτυξης. Δεν θα πρέπει να αποτελεί έκπληξη ότι οι υπεύθυνοι ανάπτυξης δεν παράγουν ασφαλή κώδικα εάν δεν τον εξετάσουν.

Η διατήρηση αυτών των πληροφοριών ώστε να παραμένουν ενημερωμένες, είναι μια κρίσιμη πτυχή αυτού του έργου οδηγού (guide project). Με την υιοθέτηση της προσέγγισης wiki, η κοινότητα OWASP μπορεί να εξελίξει και να επεκτείνει τις πληροφορίες σε αυτόν τον οδηγό ώστε να συμβαδίσει με το -γρήγορα κινούμενο- πεδίο απειλής της ασφάλειας εφαρμογών. Αυτός ο οδηγός αντιμετωπίζεται καλύτερα ως σύνολο τεχνικών που μπορούμε να χρησιμοποιήσουμε για να βρούμε τους διαφορετικούς τύπους τρυπών (ατελειών) ασφάλειας. Δεν είναι, όμως, όλες οι τεχνικές εξίσου σημαντικές. Θα ήταν καλό να αποφευχθεί η χρησιμοποίηση του οδηγού ως λίστα ελέγχου (checklist).

Υπάρχουν αρκετά άτομα με διαφορετικούς ρόλους σε έναν οργανισμό, που μπορούν να χρησιμοποιήσουν αυτόν τον οδηγό.

- Οι υπεύθυνοι ανάπτυξης-προγραμματιστές (developers): πρέπει να χρησιμοποιήσουν αυτόν τον οδηγό για να εξασφαλίσουν ότι παράγουν ασφαλή κώδικα. Αυτοί οι έλεγχοι θα πρέπει να είναι ένα μέρος του κανονικού κώδικα και των διαδικασιών ελέγχου μονάδας.
- Οι ελεγκτές λογισμικού (software testers): πρέπει να χρησιμοποιήσουν αυτόν τον οδηγό για να επεκτείνουν το σύνολο περιπτώσεων του ελέγχου που εφαρμόζουν για τις εφαρμογές. Όσο νωρίτερα ανιχνεύονται οι ευπάθειες, τόσο περισσότερο κερδίζουμε σε χρόνο και προσπάθεια.
- Οι ειδικοί ασφάλειας (security specialists): πρέπει να χρησιμοποιήσουν αυτόν τον οδηγό σε συνδυασμό με άλλες τεχνικές, ως έναν τρόπο ώστε να ελεγχθεί ότι καμία τρύπα ασφάλειας δεν έχει παραβλεφθεί σε μια εφαρμογή.

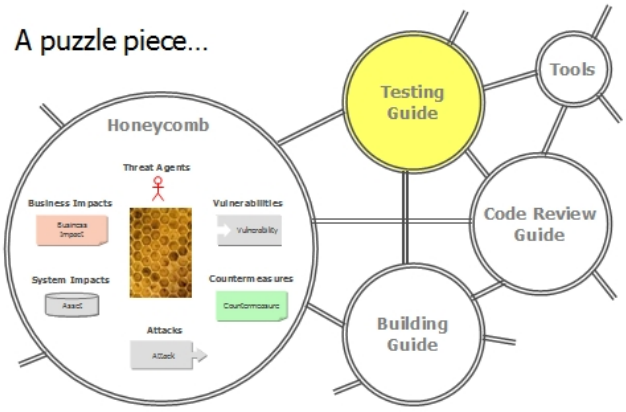
Πιθανώς η σημαντικότερη πτυχή του ελέγχου ασφάλειας εφαρμογών που πρέπει να ληφθεί υπόψη, είναι το γεγονός ότι θα έχουμε περιορίσει το χρόνο και θα πρέπει να παρέχουμε όσο το δυνατόν περισσότερη κάλυψη. Συστήνεται να μην ανοίξει κάποιος απλά το βιβλίο και να αρχίζει τον έλεγχο. Το ιδανικό θα ήταν, να γίνει κάποια διαμόρφωση απειλών για να καθοριστεί ποια είναι τα σημαντικότερα θέματα ασφάλειας που αφορούν την συγκεκριμένη επιχείρηση. Στο τέλος, θα πρέπει να προκύψει ένας πρωτεύων κατάλογος απαιτήσεων ασφάλειας που θα ελεγχθεί.

Το επόμενο βήμα είναι να αποφασιστεί πως να ελεγχθούν αυτές οι απαιτήσεις. Υπάρχουν αρκετές διαφορετικές επιλογές. Μπορούμε να χρησιμοποιήσουμε το εγχειρίδιο ελέγχου ασφάλειας ή εγχειρίδιο επισκόπησης κώδικα (code review). Μπορούμε επίσης να χρησιμοποιήσουμε αυτοματοποιημένη ανίχνευση (scanning) ευπαθειών ή αυτοματοποιημένη ανίχνευση κώδικα (στατική ανάλυση-static analysis). Ή ακόμη να χρησιμοποιήσουμε επισκόπηση αρχιτεκτονικής της ασφάλειας ή συζητήσεις με τους υπεύθυνους ανάπτυξης και τους αρχιτέκτονες ώστε να ελέγξουμε αυτές τις απαιτήσεις. Το σημαντικό είναι να αποφασιστεί ποιες από αυτές τις τεχνικές, θα είναι οι πιο ακριβείς και αποδοτικές για την συγκεκριμένη εφαρμογή.

3.2.1.2 Τι είναι ο οδηγός ελέγχου OWASP (OWASP Testing Guide);

Ο οδηγός ελέγχου OWASP περιλαμβάνει ένα πλαίσιο ελέγχου διείσδυσης (penetration testing) βασισμένο σε βέλτιστες πρακτικές, το οποίο μπορούν να χρησιμοποιούν οι χρήστες στους οργανισμούς τους, και έναν οδηγό ελέγχου διείσδυσης «χαμηλού επιπέδου» που περιγράφει τεχνικές για τον έλεγχο των πιο συνηθισμένων ζητημάτων ασφάλειας σε διαδικτυακές εφαρμογές και υπηρεσίες διαδικτύου.

Είναι ένα κομμάτι... από ένα πείραμα... για τη δημιουργία μιας βάσης γνώσης της ασφάλειας εφαρμογών... (Σχήμα 18) Είναι πολύ σημαντικό για την επίτευξη αξιόπιστων εφαρμογών.



Σχήμα 18. OWASP Testing Guide-ένα κομμάτι παζλ...

Το Έργο Ελέγχου του OWASP (OWASP Testing Project) ήταν υπό ανάπτυξη για πολλά έτη. Το συγκεκριμένο έργο, βοηθά τους ανθρώπους να κατανοήσουν το τι, γιατί, πότε, που και πως να εκτελούν έλεγχο στις εφαρμογές ιστού (web) και δεν παρέχει μόνο μια απλή λίστα ελέγχου (checklist) ή μια λίστα θεμάτων που πρέπει να εξεταστούν. Το εξαγόμενο αυτού του έργου είναι ένα πλήρες Πλαίσιο Ελέγχου (Testing Framework), από το οποίο κάποιοι μπορούν να δημιουργήσουν τα δικά τους προγράμματα ελέγχου ή να τροποποιήσουν τις διαδικασίες άλλων. Ο Οδηγός Ελέγχου (Testing Guide) περιγράφει διεξοδικά και το γενικό Πλαίσιο Ελέγχου (Testing Framework) αλλά και τις τεχνικές που απαιτούνται για να εφαρμοστεί στην πράξη αυτό το πλαίσιο.

3.2.1.2.1 Έκδοση 3

Η έκδοση 3 του Οδηγού Ελέγχου του OWASP (OWASP Testing Guide Version 3) βελτιώνει αρκετά την έκδοση 2 και δημιουργεί νέα τμήματα και ελέγχους. Η νέα έκδοση έχει προσθέσει τα εξής:

- Τμήματα Διαχείρισης Διαμόρφωσης (Configuration Management) και Έγκρισης (Authorization) Ελέγχου, καθώς και Παράρτημα Κωδικοποιημένης Έγχυσης (Encoded Injection Appendix).
- 36 νέα άρθρα (1 εκ των οποίων λαμβάνεται από το OWASP BSP[12]).

Η έκδοση 3 βελτίωσε 9 άρθρα, για συνολικά 10 κατηγορίες ελέγχου και 66 ελέγχους. Το έγγραφο του Οδηγού Ελέγχου δημοσιεύεται υπό την Creative Commons Attribution-Share Alike 3.0 άδεια.

3.2.1.3 Βασικοί στόχοι

Η συγγραφή του Οδηγού Ελέγχου (Testing Guide) αποδείχθηκε ένας δύσκολος στόχος. Η απόκτηση συναίνεσης και η ανάπτυξη του περιεχομένου που θα επέτρεπε στους ανθρώπους να εφαρμόσουν τις έννοιες που περιγράφονται στον Οδηγό Ελέγχου, ενώ παράλληλα θα τους επέτρεπε να τις υλοποιήσουν στο περιβάλλον τους, αποτελούσε μεγάλη πρόκληση. Επίσης πρόκληση αποτελούσε, και η αλλαγή εστίασης του ελέγχου εφαρμογών ιστού από τον έλεγχο διείσδυσης

[12] BSP - Σελίδες Επιχειρησιακών Εξυπηρετών (Business Server Pages)

(penetration testing), στον έλεγχο που ενσωματώνεται στον κύκλο ζωής ανάπτυξης του λογισμικού.

Εντούτοις, τα αποτελέσματα είναι πολύ ικανοποιητικά. Αρκετοί εμπειρογνώμονες βιομηχανίας και άτομα υπεύθυνα για την ασφάλεια λογισμικού σε μερικές από τις μεγαλύτερες επιχειρήσεις στον κόσμο, επικυρώνουν το Πλαίσιο Ελέγχου (Testing Framework). Το συγκεκριμένο πλαίσιο βοηθά τους οργανισμούς να εξετάσουν τις εφαρμογές ιστού προκειμένου να δημιουργήσουν αξιόπιστο και ασφαλές λογισμικό και δε δίνει απλά έμφαση σε τομείς αδυναμίας, αν και το τελευταίο αποτελεί ένα υποσύνολο για πολλούς από τους οδηγούς και τις λίστες ελέγχου (checklists) του OWASP. Επομένως, έχουν ληφθεί μερικές σημαντικές αποφάσεις για την καταλληλότητα ορισμένων τεχνικών και τεχνολογιών ελέγχου, που είναι πλήρως κατανοητό ότι δεν θα υποστηριχθούν από όλους. Εντούτοις, το OWASP είναι σε θέση να αλλάξει τη νοοτροπία κατά τη διάρκεια του χρόνου μέσω της συνειδητοποίησης και της εκπαίδευσης που βασίζεται σε συναίνεση και εμπειρία. Ο οδηγός οργανώνεται ως εξής: Περιλαμβάνει μια εισαγωγή, η οποία καλύπτει τις προϋποθέσεις του ελέγχου των εφαρμογών ιστού: την εμβέλεια του ελέγχου, τις αρχές του επιτυχούς ελέγχου και τις τεχνικές ελέγχου. Το κεφάλαιο 3 παρουσιάζει το Πλαίσιο Ελέγχου του OWASP και εξηγεί τις τεχνικές και τους στόχους του, σε σχέση με τις διάφορες φάσεις του κύκλου ζωής ανάπτυξης του λογισμικού. Τέλος, το κεφάλαιο 4 καλύπτει τον τρόπο εξέτασης για συγκεκριμένες ευπάθειες (π.χ. έγχυση SQL-SQL Injection) με έλεγχο επιθεώρησης κώδικα (code inspection) και έλεγχο διείσδυσης (penetration testing).

Το Πλαίσιο που περιγράφεται στο έγγραφο ενθαρρύνει τους υπεύθυνους να μετρήσουν την ασφάλεια των συστημάτων καθ' όλη τη διαδικασία ανάπτυξής τους. Μπορούν έπειτα να συσχετίσουν το κόστος του επισφαλούς λογισμικού, με τον αντίκτυπο που έχει στην επιχείρησή τους και να αναπτύξουν, συνεπώς, τις σωστές επιχειρησιακές αποφάσεις (πόρους) για να ρυθμίσουν τον κίνδυνο. Θα πρέπει να επισημάνουμε ότι η μέτρηση και ο έλεγχος των εφαρμογών ιστού είναι πιο κρίσιμες από οποιοδήποτε άλλο λογισμικό, δεδομένου ότι οι εφαρμογές ιστού εκτίθενται σε εκατομμύρια χρήστες μέσω του Διαδικτύου.

Για τους σκοπούς του συγκεκριμένου εγγράφου, ο έλεγχος αποτελεί μια διαδικασία σύγκρισης της κατάστασης ενός συστήματος ή μιας εφαρμογής ενάντια σε ένα σύνολο κριτηρίων. Στη βιομηχανία ασφάλειας, οι υπεύθυνοι εξετάζουν συχνά με βάση ένα σύνολο ιδεολογικών κριτηρίων, τα οποία ούτε καθορίζονται σωστά, ούτε είναι ολοκληρωμένα. Για αυτόν τον λόγο, πολλοί θεωρούν τον έλεγχο ως «μαύρη τέχνη». Ο στόχος του εγγράφου είναι να ξεπεραστεί αυτή η αντίληψη και να διευκολύνει τους υπεύθυνους να διαφέρουν χωρίς να κατέχουν πολλές γνώσεις σχετικά με την ασφάλεια.

Το συγκεκριμένο έγγραφο σχεδιάστηκε για να βοηθήσει τους οργανισμούς να κατανοήσουν τι περιλαμβάνει ένα πρόγραμμα ελέγχου και για να τους βοηθήσει να προσδιορίσουν τα βήματα που θα πρέπει να ακολουθήσουν για να δημιουργήσουν και να εφαρμόσουν αυτό το πρόγραμμα ελέγχου στις εφαρμογές ιστού τους. Πρόκειται να δώσει μια ευρεία πτυχή των απαιτούμενων στοιχείων ώστε να γίνει ένα διεξοδικό πρόγραμμα ασφάλειας εφαρμογών ιστού. Αυτός ο οδηγός μπορεί να χρησιμοποιηθεί ως αναφορά και ως μεθοδολογία ώστε να βοηθήσει να καθοριστεί το χάσμα μεταξύ των υπαρχουσών πρακτικών και των βέλτιστων πρακτικών (best practices) της

βιομηχανίας. Ο οδηγός επιτρέπει στους οργανισμούς να συγκριθούν με άλλους, καθώς και να κατανοήσουν το μέγεθος των πόρων που απαιτούνται ώστε να εξετάσουν και να διατηρήσουν το λογισμικό τους, ή να προετοιμαστούν για έναν έλεγχο.

Οι περισσότεροι υπεύθυνοι σήμερα εξετάζουν το λογισμικό μόνο εφόσον έχει δημιουργηθεί ήδη και είναι στη φάση επέκτασης του κύκλου ζωής του (δηλ., ο κώδικας έχει δημιουργηθεί και αρχικοποιηθεί σε μια εφαρμογή ιστού που «τρέχει»). Αυτό γενικά αποτελεί μια πολύ ατελέσφορη και απαγορευτική -λόγω κόστους- πρακτική. Μια από τις καλύτερες μεθόδους για να αποτραπούν τα σφάλματα (bugs) ασφάλειας από την εμφάνισή τους στις εφαρμογές, είναι να βελτιωθεί ο κύκλος ζωής ανάπτυξης λογισμικού (Software Development Life Cycle-SDLC), συμπεριλαμβάνοντας την ασφάλεια σε κάθε μια από τις φάσεις της.

Εν κατακλείδι, ο βασικός σκοπός του Οδηγού Ελέγχου του OWASP είναι ότι περιλαμβάνει: μια «βέλτιστη πρακτική» ελέγχου διείσδυσης την οποία οι χρήστες μπορούν να εφαρμόσουν στους οργανισμούς τους, καθώς και ένα «χαμηλού επιπέδου» οδηγό ελέγχου διείσδυσης που περιγράφει τις τεχνικές για τον έλεγχο των πιο κοινών ζητημάτων ασφάλειας των εφαρμογών και υπηρεσιών ιστού.

3.2.1.4 OWASP Top 10

Η OWASP Top Ten είναι μια ολοκληρωμένη λίστα των 10 πιο κρίσιμων κινδύνων ασφάλειας εφαρμογών Διαδικτύου που απαιτούν άμεση αντιμετώπιση. Ο ήδη υπάρχων κώδικας πρέπει να ελεγχθεί για αυτά τα προβλήματα ασφάλειας άμεσα, καθώς τα σημεία αυτά αποτελούν πρωτεύοντες στόχους για τους επιτιθέμενους. Τα προγράμματα ανάπτυξης λογισμικού πρέπει να αναφέρουν τα προβλήματα αυτά στα συνοδευτικά τους έγγραφα, να σχεδιάζονται, να υλοποιούνται και να ελέγχουν τις εφαρμογές τους για να επιβεβαιώσουν ότι δεν κινδυνεύουν από κάποιο από αυτά. Οι διευθυντές των προγραμμάτων αυτών πρέπει να αφιερώνουν χρόνο και χρήμα για δραστηριότητες σχετικά με την ασφάλεια των εφαρμογών συμπεριλαμβάνοντας εκπαίδευση των προγραμματιστών, ανάπτυξη πολιτικής ασφαλείας για τις εφαρμογές, σχεδιασμό μηχανισμού ασφάλειας, έλεγχο κατά των επιθέσεων και εξέταση του κώδικα.

Ο αρχικός στόχος του OWASP Top 10 είναι να εκπαιδευτούν οι υπεύθυνοι ανάπτυξης, οι σχεδιαστές, οι αρχιτέκτονες, οι διευθυντές και οι οργανισμοί σχετικά με τις συνέπειες των σημαντικότερων αδυναμιών ασφάλειας των εφαρμογών ιστού. Το Top 10 παρέχει τις βασικές τεχνικές που προστατεύουν από αυτές τις προβληματικές περιοχές υψηλού κινδύνου, καθώς επίσης και τις οδηγίες για το τι θα πρέπει να γίνει στη συνέχεια. Ο στόχος του Top 10 είναι κυρίως η ευαισθητοποίηση για την ασφάλεια εφαρμογών, εντοπίζοντας τους κυριότερους κινδύνους που αντιμετωπίζουν οι οργανισμοί. Υπάρχουν πολλές αναφορές στο Top 10 μέσα σε πρότυπα, βιβλία, εργαλεία και οργανισμούς όπως τα MITRE, PCI DSS, DISA, FTC, και πολλά ακόμα. Αυτή η έκδοση του OWASP Top 10 σηματοδοτεί τον $8^{ο}$ χρόνο του έργου αυτού αλλά και της προσπάθειας για την ευαισθητοποίηση σχετικά με τη σημασία των κινδύνων στην ασφάλεια εφαρμογών. Το OWASP Top 10 εκδόθηκε πρώτη φορά το 2003, ενώ μικρές ενημερώσεις έγιναν το 2004 και 2007. Στη συνέχεια παρουσιάζεται η έκδοση του 2010.

Ας δούμε, όμως, ποιες είναι, σύμφωνα με το OWASP, οι 10 κυριότερες ευπάθειες για το 2010 από τις οποίες κινδυνεύουν οι εφαρμογές που «τρέχουν» στο Διαδίκτυο.

- **A1: Έγχυση (Injection)** - Οι injection flaws (επιθέσεις με εγχυόμενο κώδικα), όπως SQL, OS και LDAP injection (έγχυση), εμφανίζονται όταν μη έγκυρα δεδομένα στέλνονται σε έναν διερμηνέα (interpreter) όπου χρησιμοποιούνται ως τμήμα μιας εντολής ή μιας επερώτησης (query). Τα εχθρικά δεδομένα του επιτιθεμένου μπορούν να εξαπατήσουν τον διερμηνέα στην εκτέλεση εντολών για τις οποίες δεν υπήρχε σχετική πρόθεση ή στην πρόσβαση δεδομένων για τα οποία δεν υπήρχε κατάλληλη εξουσιοδότηση.
- **A2: Cross-Site Scripting (XSS)** - Οι ατέλειες τύπου XSS εμφανίζονται όταν μια εφαρμογή λαμβάνει μη έγκυρα δεδομένα και τα στέλνει σε ένα φυλλομετρητή ιστού (web browser) χωρίς την κατάλληλη επικύρωση και κωδικοποίηση. Οι επιθέσεις τύπου XSS επιτρέπουν στους επιτιθεμένους να εκτελέσουν scripts στον browser του θύματος, όπου ο επιτιθέμενος μπορεί να πάρει τον έλεγχο των συνόδων (sessions) του χρήστη, να μεταβάλλει το περιεχόμενο (deface) των ιστοσελίδων (web sites), ή να ανακατευθύνει το χρήστη σε κακόβουλα sites.
- **A3: Ατελής Αυθεντικοποίηση και Διαχείριση Συνόδων (Broken Authentication and Session Management)** - Οι λειτουργίες εφαρμογών που σχετίζονται με την αυθεντικοποίηση και τη διαχείριση συνόδων (sessions) συχνά δεν εφαρμόζονται σωστά, επιτρέποντας σε επιτιθεμένους να υποκλέψουν κωδικούς πρόσβασης (passwords), κλειδιά, στοιχεία-τεκμήρια συνόδου (session tokens), ή να εκμεταλλευτούν άλλες ατέλειες εφαρμογών για να υιοθετήσουν ταυτότητες άλλων χρηστών.
- **A4: Ανασφαλής Απευθείας Αναφορά σε Αντικείμενα (Insecure Direct Object References)** - Μια άμεση αναφορά αντικειμένου εμφανίζεται όταν ένας υπεύθυνος ανάπτυξης (προγραμματιστής) καθιστά δημόσια μια αναφορά σε ένα εσωτερικό αντικείμενο εφαρμογής, όπως ένα αρχείο, ένας κατάλογος, ή ένα κλειδί μιας βάσης δεδομένων. Χωρίς κατάλληλο έλεγχο πρόσβασης ή κατάλληλη προστασία, οι επιτιθέμενοι μπορούν να διαχειριστούν αυτές τις αναφορές ώστε να αποκτούν πρόσβαση σε δεδομένα για τα οποία δεν υπήρχε κατάλληλη εξουσιοδότηση.
- **A5: Πλαστογράφηση Αίτησης μεταξύ Θέσεων (Cross-Site Request Forgery-CSRF)** - Μια επίθεση CSRF αναγκάζει το φυλλομετρητή (browser) ενός θύματος να στείλει μια πλαστή http αίτηση (request), συμπεριλαμβάνοντας το cookie της συνόδου του θύματος καθώς και οποιαδήποτε άλλη πληροφορία αυθεντικοποίησης, σε μια τρωτή-ευάλωτη εφαρμογή ιστού. Έτσι, αυτό επιτρέπει στον επιτιθέμενο να αναγκάσει τον browser του θύματος να παράγει αιτήσεις για τις οποίες η ευπαθής εφαρμογή θεωρεί ότι είναι νόμιμες αιτήσεις από το θύμα.
- **A6: Λανθασμένες Ρυθμίσεις Ασφάλειας (Security Misconfiguration)** - Οι καλές πρακτικές ασφάλειας απαιτούν την ύπαρξη μιας ασφαλούς διαμόρφωσης (δηλαδή, ρυθμίσεων) που καθορίζεται και αναπτύσσεται για τις εφαρμογές, τα πλαίσια (frameworks), τους εξυπηρέτες (servers) εφαρμογών, τους εξυπηρέτες ιστού (web servers) και τους εξυπηρέτες βάσεων δεδομένων. Όλες αυτές οι ρυθμίσεις πρέπει να καθοριστούν, να εφαρμοστούν και να διατηρηθούν δεδομένου ότι οι περισσότερες δεν διατίθενται ως προεπιλογές. Στα παραπάνω περιλαμβάνεται η ενημέρωση του ήδη υπάρχοντος λογισμικού, καθώς και όλων των βιβλιοθηκών κώδικα που χρησιμοποιούνται από την εφαρμογή.
- **A7: Ανασφαλής Κρυπτογραφική Αποθήκευση (Insecure Cryptographic Storage)** - Πολλές εφαρμογές ιστού δεν προστατεύουν κατάλληλα τα

ευαίσθητα δεδομένα, όπως αριθμοί πιστωτικών καρτών, ΑΦΜ/ΑΜΚΑ και πιστοποιητικά αυθεντικοποίησης, με κατάλληλη κρυπτογράφηση ή hashing (συνάρτηση κερματισμού). Οι επιτιθέμενοι μπορούν να υποκλέψουν ή να τροποποιήσουν τέτοια μη-προστατευμένα δεδομένα ώστε να πραγματοποιήσουν επιθέσεις κλοπής ταυτότητας, απάτες με πιστωτικές κάρτες, ή άλλα εγκλήματα.

- **A8: Αποτυχία Περιορισμού της Πρόσβασης URL (Failure to Restrict URL Access)** - Πολλές εφαρμογές ιστού ελέγχουν τα δικαιώματα πρόσβασης ενός URL πριν προχωρήσουν στη διαμόρφωση των διαφόρων υπερσυνδέσμων και κουμπιών που θα έπρεπε να είναι προστατευμένα. Εντούτοις, οι εφαρμογές πρέπει να εκτελέσουν παρόμοιους ελέγχους πρόσβασης κάθε φορά που κάποιος επισκέπτεται αυτές τις σελίδες, διαφορετικά οι επιτιθέμενοι θα είναι σε θέση να αποκτήσουν πρόσβαση σε αυτές τις κρυφές σελίδες.
- **A9: Ανεπαρκής Προστασία Επιπέδου Μεταφοράς (Insufficient Transport Layer Protection)** - Οι εφαρμογές συχνά αποτυγχάνουν να επικυρώσουν, να κρυπτογραφήσουν και να προστατεύσουν την εμπιστευτικότητα και την ακεραιότητα της δικτυακής κυκλοφορίας. Αυτό συμβαίνει διότι μερικές φορές υποστηρίζουν αδύναμους αλγορίθμους, χρησιμοποιούν ληγμένα ή ανίσχυρα πιστοποιητικά, ή δεν τα χρησιμοποιούν σωστά.
- **A10: Μη Επαληθευμένες Ανακατευθύνσιες και Προωθήσεις (Unvalidated Redirects and Forwards)** - Οι εφαρμογές ιστού συχνά ανακατευθύνουν και προωθούν τους χρήστες σε άλλες σελίδες και ιστοχώρους και χρησιμοποιούν μη ελεγμένα/επαληθευμένα δεδομένα για να καθορίσουν τις σελίδες προορισμού. Χωρίς την κατάλληλη επικύρωση, οι επιτιθέμενοι μπορούν να ανακατευθύνουν τα θύματά τους σε ιστοσελίδες phishing[77] ή ιστοσελίδες που περιέχουν κακόβουλο λογισμικό, ή μπορούν να χρησιμοποιήσουν προωθήσεις (forwards) για να αποκτήσουν πρόσβαση σε σελίδες για τις οποίες δεν υπάρχει η κατάλληλη εξουσιοδότηση.

Η ενημερωμένη έκδοση του 2010 βασίζεται σε περισσότερες πηγές πληροφόρησης για ευπάθειες διαδικτυακών εφαρμογών σε σχέση με την προηγούμενη. Επιπλέον, παρουσιάζει τις πληροφορίες με πιο συνοπτικό τρόπο, ώστε να μπορούν εύκολα να τεθούν σε εφαρμογή αφού περιλαμβάνουν πολλές αναφορές σε νέο, πλούσιο υλικό που μπορεί να χρησιμοποιηθεί για να αντιμετωπίσει το κάθε θέμα.

3.2.2 Εμβέλεια (Scope)

3.2.2.1 Οι Τεχνικές Ελέγχου που Εξηγούνται

Αυτό το τμήμα παρουσιάζει μια υψηλού επιπέδου επισκόπηση των διάφορων τεχνικών ελέγχου που μπορούν να υιοθετηθούν κατά τη δημιουργία ενός προγράμματος ελέγχου σύμφωνα με το OWASP. Αυτό το τμήμα παρέχει το υπόβαθρο για το πλαίσιο (framework) που θα παρουσιαστεί στη συνέχεια και δίνει έμφαση στα πλεονεκτήματα και μειονεκτήματα μερικών από των τεχνικών που πρέπει να εξεταστούν. Συγκεκριμένα, έχουμε τις παρακάτω τεχνικές:

- **Χειροκίνητες Επιθεωρήσεις και Επισκοπήσεις (Manual Inspections & Reviews)**

Οι χειροκίνητες επιθεωρήσεις είναι επισκοπήσεις καθοδηγούμενες από ανθρώπους, οι οποίες τυπικά εξετάζουν τις επιπτώσεις της ασφάλειας των χρηστών,

των πολιτικών και των διαδικασιών, αλλά επίσης συμπεριλαμβάνουν την επιθεώρηση των αποφάσεων τεχνολογίας όπως ο αρχιτεκτονικός σχεδιασμός. Διεξάγονται συνήθως με την ανάλυση τεκμηρίωσης ή την εκτέλεση συνεντεύξεων με τους σχεδιαστές ή τους ιδιοκτήτες του συστήματος. Αν και η έννοια των χειροκίνητων επιθεωρήσεων και επισκοπήσεων είναι απλή, εντούτοις θεωρούνται μεταξύ των ισχυρότερων και πιο αποτελεσματικών διαθέσιμων τεχνικών. Ρωτώντας κάποιον για το πως λειτουργεί κάτι και γιατί εφαρμόστηκε με έναν συγκεκριμένο τρόπο, επιτρέπει στον ελεγκτή να καθορίσει γρήγορα εάν οποιεσδήποτε υποψίες προβλημάτων ασφάλειας μπορεί να είναι εμφανείς. Οι χειροκίνητες επιθεωρήσεις και επισκοπήσεις είναι ένας από τους λίγους τρόπους ώστε να εξεταστεί η ίδια η διαδικασία του κύκλου ζωής ανάπτυξης λογισμικού και να εξασφαλισθεί ότι υπάρχει μια επαρκής πολιτική που τίθεται σε ισχύ.

Πλεονεκτήματα:	Μειονεκτήματα:
▪ Δεν απαιτεί καμία τεχνολογία για υποστήριξη.	▪ Μπορεί να είναι εξαιρετικά απαιτητική ως προς το χρόνο.
▪ Μπορεί να εφαρμοστεί σε ποικίλες καταστάσεις.	▪ Δεν υπάρχει πάντα διαθέσιμο υλικό υποστήριξης.
▪ Ευέλικτη.	▪ Απαιτεί στελέχη με αυξημένα προσόντα και αναλυτική σκέψη για να είναι αποτελεσματική!
▪ Προωθεί την ομαδική εργασία.	
▪ Εισάγεται νωρίς στον κύκλο ζωής του συστήματος.	

Πίνακας 3. Πλεονεκτήματα και μειονεκτήματα της τεχνικής Manual Inspections & Reviews.

- **Μοντελοποίηση Απειλής (Threat Modeling)**

Η μοντελοποίηση απειλής έχει γίνει μια δημοφιλής τεχνική που ενισχύει τους σχεδιαστές συστήματος να σκεφτούν για τις απειλές ασφάλειας όπου τα συστήματα ή οι εφαρμογές τους μπορεί να αντιμετωπίσουν. Επομένως, η μοντελοποίηση απειλής μπορεί να θεωρηθεί ως αξιολόγηση κινδύνου για εφαρμογές. Στην πραγματικότητα, επιτρέπει στο σχεδιαστή να αναπτύξει στρατηγικές μετριασμού για τις πιθανές ευπάθειες και τους βοηθά να εστιάσουν στους αναπόφευκτα περιορισμένους πόρους και στα μέρη του συστήματος τα οποία το απαιτούν περισσότερο. Συνιστάται ότι όλες οι εφαρμογές θα πρέπει να έχουν ανεπτυγμένο και τεκμηριωμένο, ένα μοντέλο απειλής (threat model). Τα πρότυπα απειλής πρέπει να δημιουργηθούν όσο το δυνατόν νωρίτερα στον κύκλο ζωής του συστήματος και πρέπει να επανεξετασθούν καθώς η εφαρμογή εξελίσσεται και η ανάπτυξη προχωρά. Για να αναπτύξουμε ένα μοντέλο απειλής, συστήνεται μια απλή προσέγγιση που ακολουθεί το NIST 800-30 [Gary Stoneburner, Alice Goguen, and Alexis Feringa, (2002)] πρότυπο για την αξιολόγηση κινδύνου. Αυτή η προσέγγιση περιλαμβάνει:

- Αποσύνθεση της εφαρμογής, για την κατανόηση του πώς λειτουργεί η εφαρμογή, τα αγαθά της, τη λειτουργικότητά της και τη συνδεσιμότητά της.
- Προσδιορισμός και ταξινόμηση των αγαθών σε υλικές και άυλες και κατάταξή τους ανάλογα με το πόσο σημαντικές είναι.
- Έρευνα πιθανών ευπαθειών – τεχνικές, λειτουργικές ή διαχειριστικές.
- Έρευνα πιθανών απειλών – ανάπτυξη μιας ρεαλιστικής άποψης των πιθανών διανυσμάτων επίθεσης από την προοπτική του επιτιθέμενου, χρησιμοποιώντας σενάρια απειλών ή δένδρα επιθέσεων.
- Δημιουργία στρατηγικών μετριασμού. Οι στρατηγικές αναπτύσσονται για τις απειλές που θεωρούνται ρεαλιστικές.

Πλεονεκτήματα:	Μειονεκτήματα:
▪ Πρακτική άποψη του επιτιθεμένου στο σύστημα.	▪ Σχετικά νέα τεχνική.
▪ Ευέλικτη.	▪ Καλά πρότυπα απειλής δεν σημαίνει αυτόματα και καλό λογισμικό.
▪ Εισάγεται νωρίς στον κύκλο ζωής του συστήματος..	

Πίνακας 4. Πλεονεκτήματα και μειονεκτήματα της τεχνικής Threat Modeling.

- **Επισκόπηση Κώδικα (Code Review)**

Η επισκόπηση πηγαίου κώδικα είναι η διαδικασία ελέγχου του πηγαίου κώδικα μιας εφαρμογής ιστού για ζητήματα ασφάλειας. Υπάρχουν αρκετές σοβαρές ευπάθειες ασφάλειας, που δεν είναι δυνατό να ανιχνευθούν με οποιαδήποτε άλλη μορφή ανάλυσης ή ελέγχου. Ένα γνωστό ρητό αναφέρει: «εάν θέλουμε να μάθουμε τι πραγματικά συμβαίνει, πηγαίνουμε κατ' ευθείαν στην πηγή». Σχεδόν όλοι οι εμπειρογνώμονες ασφάλειας συμφωνούν ότι δεν υπάρχει κανένα υποκατάστατο που να εξετάζει πραγματικά τον κώδικα. Όλες οι πληροφορίες για τον προσδιορισμό των προβλημάτων ασφάλειας είναι κάπου εκεί, στον κώδικα. Αντίθετα με τον έλεγχο κλειστού λογισμικού που προμηθευόμαστε από τρίτους (third party) όπως τα λειτουργικά συστήματα, όταν εξετάζονται εφαρμογές ιστού (ειδικά εάν έχουν αναπτυχθεί στο εσωτερικό του οργανισμού) ο πηγαίος κώδικας πρέπει να είναι διαθέσιμος για λόγους ελέγχου. Πολλά ακούσια αλλά σημαντικά προβλήματα ασφάλειας είναι επίσης εξαιρετικά δύσκολο να ανακαλυφθούν με άλλες μορφές ανάλυσης ή ελέγχου, όπως ο έλεγχος διείσδυσης (penetration testing), έτσι η ανάλυση του πηγαίου κώδικα αποτελεί την τεχνική επιλογής για τον έλεγχο. Με τον πηγαίο κώδικα, ένας ελεγκτής μπορεί ακριβώς να καθορίσει αυτό που συμβαίνει (ή υποτίθεται ότι θα συμβεί) και επιπλέον χωρίς να χρειάζεται τον έλεγχο μαύρου κουτιού (black box testing). Παραδείγματα ζητημάτων που είναι ιδιαίτερα σημαντικά και μπορούμε να βρούμε με την επισκόπηση πηγαίου κώδικα, είναι τα προβλήματα συγχρονισμού, εσφαλμένης επιχειρησιακής λογικής, προβλήματα ελέγχου πρόσβασης και οι αδυναμίες κρυπτογράφησης, καθώς επίσης και τα backdoors[13], Trojans[14], Easter eggs[15], time bombs[16], logic bombs[17] και άλλες μορφές κακόβουλου κώδικα.

[13] Backdoors (Κερκόπορτες): Σε πολλές περιπτώσεις επιθέσεων σε συστήματα υπολογιστών, οι επίδοξοι hackers φροντίζουν να δημιουργήσουν μια κρυφή είσοδο ή κερκόπορτα (backdoor) στον υπολογιστή στόχο, από την οποία θα μπορούν να εισβάλουν σ' αυτό χωρίς να χρειασθεί να προσπελάσουν κάποιο σύστημα ασφαλείας.

[14] Trojan Horses (Δούρειοι Ίπποι): είναι προγράμματα με κρυφές λειτουργίες που δεν περιλαμβάνονται στην τεκμηρίωση που τα συνοδεύει. Δηλαδή, ενώ ισχυρίζονται ότι επιτελούν κάποια εργασία, στην πραγματικότητα εκτελούν ή/και μια διαφορετική λειτουργία. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών.

[15] Easter eggs (Πασχαλινά αυγά): είναι αρχεία κινούμενης εικόνας ή παιχνιδιού που οι σχεδιαστές λογισμικού κρύβουν σ' ένα πρόγραμμα. Η πρόσβαση στο πασχαλινό αυγό γίνεται με κωδικό.

[16] Time Bombs (Ωρολογιακές Βόμβες): κακόβουλα προγράμματα που ενεργοποιούνται όταν έρθει η κατάλληλη χρονική στιγμή ή μέρα.

[17] Logic Bombs (Λογικές Βόμβες): κακόβουλα προγράμματα που «εκρήγνυνται» όταν ικανοποιηθεί μια λογική συνθήκη.

Πλεονεκτήματα:	Μειονεκτήματα:
▪ Πληρότητα και αποτελεσματικότητα.	▪ Απαιτεί πολύ καλά καταρτισμένους προγραμματιστές ασφάλειας
▪ Ακρίβεια.	▪ Μπορεί να μην ανιχνεύσει προβλήματα σε μεταγλωττισμένες (compiled) βιβλιοθήκες.
▪ Γρήγορη (για ικανούς αξιολογητές).	▪ Δεν μπορεί να ανιχνεύσει εύκολα σφάλματα χρόνου εκτέλεσης (run-time).
	▪ Ο πηγαίος κώδικας (source code) που τελικά βρίσκεται σε λειτουργία μπορεί να διαφέρει από αυτόν που αναλύεται (λόγω τροποποιήσεων που επήλθαν στο μεσοδιάστημα).

Πίνακας 5. Πλεονεκτήματα και μειονεκτήματα της τεχνικής Code Review.

- **Έλεγχος Διείσδυσης (Penetration Testing)**

Ο έλεγχος διείσδυσης είναι μια κοινή τεχνική που χρησιμοποιείται για να εξετάσει την ασφάλεια δικτύων, εδώ και πολλά έτη. Είναι επίσης συνήθως γνωστός ως *έλεγχος μαύρου κουτιού* (black box testing) ή *ηθική διείσδυση* (ethical hacking). Ο έλεγχος διείσδυσης είναι ουσιαστικά η τεχνική εξέτασης μιας εφαρμογής που «τρέχει» από μακριά, χωρίς τη γνώση των εσωτερικών διεργασιών της ίδιας της εφαρμογής, για να ευρεθούν ευπάθειες ασφάλειας. Στην ουσία, η ομάδα του έλεγχου διείσδυσης θα έχει πρόσβαση σε μια εφαρμογή σαν να ήταν χρήστες. Ο ελεγκτής ενεργεί όπως ένας επιτιθέμενος και προσπαθεί να εντοπίσει και να εκμεταλλευτεί τις ευπάθειες. Σε πολλές περιπτώσεις, θα δοθεί στον ελεγκτή ένας έγκυρος λογαριασμός (account) στο σύστημα. Αν και ο έλεγχος διείσδυσης έχει αποδειχθεί αποτελεσματικός στην ασφάλεια δικτύων, η τεχνική δε μεταγλωττίζεται φυσικά σε εφαρμογές. Όταν ο έλεγχος διείσδυσης εκτελείται σε δίκτυα και λειτουργικά συστήματα, το μεγαλύτερο μέρος της δουλειάς συμπεριλαμβάνεται στην εύρεση των γνωστών ευπαθειών και έπειτα στην εκμετάλλευσή τους σε συγκεκριμένες τεχνολογίες. Ο έλεγχος διείσδυσης στο χώρο των εφαρμογών ιστού είναι πιο κοντά στην απλή έρευνα. Έχουν αναπτυχθεί κάποια εργαλεία έλεγχου διείσδυσης τα οποία αυτοματοποιούν τη διαδικασία, αλλά πάλι, εξαιτίας της φύσης των εφαρμογών ιστού η αποτελεσματικότητά τους είναι συνήθως περιορισμένη.

Πλεονεκτήματα:	Μειονεκτήματα:
▪ Μπορεί να είναι γρήγορη (και επομένως φθηνή).	▪ Εισάγεται πάρα πολύ αργά στον κύκλο ζωής του συστήματος.
▪ Απαιτεί ένα -σχετικά- χαμηλότερης ικανότητας στελεχιακό δυναμικό από την επισκόπηση του πηγαίου κώδικα.	▪ Μόνο έλεγχος αρχικής επίπτωσης (front impact)!
▪ Εξετάζει τον κώδικα που πραγματικά εκτίθεται.	

Πίνακας 6. Πλεονεκτήματα και μειονεκτήματα της τεχνικής Penetration Testing.

Με τόσες πολλές τεχνικές και τόσες πολλές προσεγγίσεις στον έλεγχο της ασφάλειας των εφαρμογών ιστού, μπορεί να είναι δύσκολο τελικά να κατανοηθεί ποιες τεχνικές θα πρέπει να χρησιμοποιηθούν και πότε. Η εμπειρία δείχνει ότι δεν υπάρχει καμία σωστή ή λανθασμένη απάντηση για το ποιες ακριβώς τεχνικές πρέπει να χρησιμοποιηθούν για να δημιουργηθεί ένα πλαίσιο ελέγχου. Γενικά αυτό που ισχύει είναι ότι όλες οι τεχνικές πρέπει πιθανώς να χρησιμοποιηθούν ώστε να εξασφαλισθεί ότι όλες οι περιοχές που πρέπει να εξεταστούν, πράγματι εξετάζονται. Εντούτοις, είναι σαφές, ότι δεν υπάρχει καμία τεχνική που καλύπτει αποτελεσματικά τον έλεγχο ασφάλειας που πρέπει να εκτελεσθεί για να εξασφαλίσει ότι όλα τα θέματα έχουν αντιμετωπιστεί. Πολλές επιχειρήσεις υιοθετούν μία μόνο προσέγγιση, η οποία είναι ο έλεγχος διείσδυσης (penetration testing). Ο έλεγχος διείσδυσης, ενώ είναι χρήσιμος, δεν μπορεί να αντιμετωπίσει αποτελεσματικά πολλά από τα ζητήματα που πρέπει να εξεταστούν και επιπλέον, εισέρχεται ελάχιστα αλλά και πάρα πολύ

αργά στον κύκλο ζωής της ανάπτυξης του συστήματος (SDLC). Είναι πιο σωστό να υιοθετηθεί μία ισορροπημένη προσέγγιση, η οποία περιλαμβάνει διάφορες τεχνικές, ξεκινώντας από χειροκίνητες συνεντεύξεις μέχρι και τεχνικό έλεγχο. Η ισορροπημένη προσέγγιση είναι σίγουρο ότι θα καλύψει τον έλεγχο σε όλες τις φάσεις του κύκλου ζωής της ανάπτυξης του συστήματος. Αυτή η προσέγγιση αξιοποιεί τις πιο κατάλληλες τεχνικές ώστε να είναι διαθέσιμες ανάλογα με την τρέχουσα φάση του κύκλου ζωής της ανάπτυξης του συστήματος. Φυσικά υπάρχουν στιγμές και περιστάσεις όπου μόνο μια τεχνική είναι αρκετή, για παράδειγμα, ένας έλεγχος σε μια εφαρμογή ιστού που έχει ήδη δημιουργηθεί και όπου το συμβαλλόμενο μέρος του ελέγχου δεν έχει πρόσβαση στον πηγαίο κώδικα. Σε αυτήν την περίπτωση, ο έλεγχος διείσδυσης είναι σαφώς ο κατάλληλος έλεγχος. Εντούτοις, συστήνεται τα μέρη που ενέχονται στον έλεγχο να υιοθετούν παραδοχές, όπως το να μην υπάρχει καμία πρόσβαση στον πηγαίο κώδικα και να διερευνούν τη δυνατότητα του πιο πλήρους ελέγχου.

3.2.2.2 Πλαίσιο Ελέγχου του OWASP (OWASP Testing Framework)

Το πλαίσιο ελέγχου θα μπορούσε να θεωρηθεί ως πλαίσιο αναφοράς που περιλαμβάνει τις τεχνικές και τους στόχους που είναι κατάλληλοι για τις διάφορες φάσεις του κύκλου ζωής της ανάπτυξης συστήματος (SDLC). Οι επιχειρήσεις και οι ομάδες έργου μπορούν να χρησιμοποιήσουν αυτό το πρότυπο για να αναπτύξουν το δικό τους πλαίσιο ελέγχου και για να εφαρμόσουν υπηρεσίες ελέγχου από προμηθευτές. Το συγκεκριμένο πλαίσιο δεν πρέπει να θεωρηθεί ως καθοδηγητικό, αλλά περισσότερο ως μια ευέλικτη προσέγγιση που μπορεί να επεκταθεί και να διαμορφωθεί για να ταιριάξει στη διαδικασία ανάπτυξης και στην κουλτούρα ενός οργανισμού. Στοχεύει στο να βοηθήσει τους οργανισμούς να δημιουργήσουν μια πλήρη στρατηγική διαδικασία ελέγχου και δεν αναφέρεται σε συμβούλους ή αναδόχους που τείνουν προς τους πιο τακτικούς και συγκεκριμένους τομείς του ελέγχου. Το πλαίσιο ελέγχου αποτελείται από τις ακόλουθες δραστηριότητες που πρέπει να πραγματοποιηθούν:

1. **Φάση 1: Πριν Αρχίσει η Ανάπτυξη (Before Development Begins).**

Πριν αρχίσει η ανάπτυξη εφαρμογών:

- ✓ Πρέπει να γίνει έλεγχος ώστε να εξασφαλιστεί ότι υπάρχει ένας κατάλληλος κύκλος ζωής της ανάπτυξης συστήματος, στον οποίο η ασφάλεια έχει ολοκληρωθεί ως αναπόσπαστο τμήμα.
- ✓ Πρέπει να γίνει έλεγχος ώστε να εξασφαλιστεί ότι υπάρχει τόσο η κατάλληλη πολιτική ασφάλειας, όσο και τα σχετικά πρότυπα, για να μπορεί να ανατρέξει σ' αυτά η ομάδα ανάπτυξης.
- ✓ Πρέπει να γίνει ανάπτυξη μετρικών και των κριτηρίων μέτρησης.
    - Φάση 1A: Επισκόπηση πολιτικών και προτύπων (Review Policies and Standards). - Εξασφαλίζεται ότι υπάρχουν κατάλληλες πολιτικές, πρότυπα, καθώς και τεκμηρίωση. Η τεκμηρίωση είναι εξαιρετικά σημαντική δεδομένου ότι παρέχει οδηγίες και πολιτικές στις ομάδες ανάπτυξης, τις οποίες μπορούν να ακολουθήσουν. Μπορούμε να εφαρμόσουμε το σωστό, μόνο εάν γνωρίζουμε ποιο ακριβώς είναι το σωστό. Εάν η εφαρμογή πρόκειται να αναπτυχθεί σε Java, είναι σημαντικό ότι υπάρχει πρότυπο ασφαλούς κωδικοποίησης σε Java. Εάν η εφαρμογή πρόκειται να χρησιμοποιήσει κρυπτογράφηση, είναι σημαντικό ότι υπάρχει πρότυπο κρυπτογράφησης. Καμία πολιτική ή πρότυπο δεν μπορεί να καλύψει κάθε κατάσταση που ίσως θα

αντιμετωπίσει η ομάδα ανάπτυξης. Με την τεκμηρίωση κοινών και προβλέψιμων ζητημάτων, θα υπάρξουν λιγότερες αποφάσεις που πρέπει να ληφθούν κατά τη διάρκεια της διαδικασίας ανάπτυξης.

- Φάση 1B: Ανάπτυξη Κριτηρίων Μέτρησης και Μετρικών (Εξασφάλιση Ανιχνευσιμότητας) (Develop Measurement and Metrics Criteria (Ensure Traceability) - Πριν αρχίσει η ανάπτυξη, σχεδιάζουμε το πρόγραμμα μέτρησης. Με τον καθορισμό των κριτηρίων που θα πρέπει να μετρηθούν, διασφαλίζεται ότι θα υπάρχει ορατότητα για τις ατέλειες, τόσο γι' αυτές της διαδικασίας όσο και γι' αυτές του προϊόντος. Είναι σημαντικό να καθοριστούν οι μετρικές πριν αρχίσει η ανάπτυξη, διότι μπορεί να υπάρξει ανάγκη να τροποποιηθεί η διαδικασία προκειμένου να συλλεχθούν δεδομένα.

2. **Φάση 2: Κατά τη Διάρκεια του Καθορισμού και του Σχεδιασμού (During Definition and Design).**

    - Φάση 2A: Επισκόπηση Απαιτήσεων Ασφάλειας (Review Security Requirements). - Οι απαιτήσεις ασφάλειας καθορίζουν το πως μια εφαρμογή λειτουργεί από μια πτυχή της ασφάλειας. Είναι σημαντικό να εξετάζονται οι απαιτήσεις ασφάλειας. Ο έλεγχος σε αυτήν την περίπτωση σημαίνει να ελέγχονται οι υποθέσεις που γίνονται στις απαιτήσεις και να ελέγχεται το εάν υπάρχουν κενά στους ορισμούς των απαιτήσεων. Θα πρέπει να εξασφαλισθεί ότι οι απαιτήσεις είναι όσο το δυνατόν πιο σαφείς. Κατά τον έλεγχο για κενά απαιτήσεων, ερευνούμε σε μηχανισμούς ασφάλειας όπως: Διαχείριση Χρηστών (User Management) (επαναφορά κωδικού πρόσβασης κ.λπ.), Αυθεντικοποίηση (Authentication), Εξουσιοδότηση (Authorization), Εμπιστευτικότητα Δεδομένων (Data Confidentiality), Ακεραιότητα (Integrity), Υπευθυνότητα (Accountability), Διαχείριση Συνόδου (Session Management), Ασφάλεια Μεταφοράς (Transport Security), Στρωματοποιημένος Διαχωρισμός Συστήματος (Tiered System Segregation), Ιδιωτικότητα (Privacy).
    - Φάση 2B: Επισκόπηση Σχεδιασμού και Αρχιτεκτονικής (Review Design and Architecture). - Οι εφαρμογές θα πρέπει να έχουν ένα τεκμηριωμένο σχεδιασμό και αρχιτεκτονική. Η τεκμηρίωση αναφέρεται στα πρότυπα, στα έγγραφα κειμένου, καθώς και σε άλλα παρόμοια αντικείμενα. Είναι σημαντικό να ελεγχθούν αυτά τα αντικείμενα για να εξασφαλιστεί ότι ο σχεδιασμός και η αρχιτεκτονική επιβάλλουν το κατάλληλο επίπεδο ασφάλειας, όπως καθορίζεται από τις απαιτήσεις. Ο προσδιορισμός των ατελειών της ασφάλειας στη φάση του σχεδιασμού, εκτός του ότι διασφαλίζει την καλύτερη σχέση κόστους-απόδοσης σχετικά με το χρονικό σημείο εντοπισμού των σφαλμάτων, αποτελεί επιπλέον και την αποτελεσματικότερη στιγμή για να γίνουν αλλαγές. Παραδείγματος χάριν, εάν προσδιορίζεται ότι ο σχεδιασμός απαιτεί αποφάσεις εξουσιοδότησης που πρέπει να ληφθούν σε πολλαπλές θέσεις, ίσως θα είναι σωστό να θεωρηθεί μια κεντρική συνιστώσα εξουσιοδότησης. Εάν η εφαρμογή εκτελεί επικύρωση δεδομένων σε πολλαπλές θέσεις, ίσως θα είναι σωστό να αναπτυχθεί ένα κεντρικό πλαίσιο επικύρωσης (η διόρθωση της επικύρωσης εισόδου (input) σε ένα μόνο σημείο και όχι σε εκατοντάδες σημεία (αν αυτή είναι διάσπαρτη στον κώδικα),

είναι πολύ φτηνότερη). Εάν ανακαλυφθούν αδυναμίες, θα πρέπει να επισημανθούν στον αρχιτέκτονα συστήματος για να διαμορφωθούν εναλλακτικές προσεγγίσεις.

- Φάση 2C: Δημιουργία και Επισκόπηση Προτύπων UML (Create and Review UML Models). - Μόλις ο σχεδιασμός και η αρχιτεκτονική είναι πλήρεις, δημιουργούμε πρότυπα σε UML (Unified Modeling Language), τα οποία περιγράφουν το πως λειτουργεί η εφαρμογή. Σε μερικές περιπτώσεις, αυτά μπορεί ήδη να είναι διαθέσιμα. Χρησιμοποιούμε αυτά τα πρότυπα, για να κατανοήσουμε με ακρίβεια μαζί με τους σχεδιαστές συστήματος το πως λειτουργεί η εφαρμογή. Εάν ανακαλυφθούν αδυναμίες, θα πρέπει να επισημανθούν στον αρχιτέκτονα συστήματος για να διαμορφωθούν εναλλακτικές προσεγγίσεις.
- Φάση 2D: Δημιουργία και Επισκόπηση Προτύπων Απειλής (Create and Review Threat Models). - Έχοντας εφοδιαστεί με τις επισκοπήσεις του σχεδιασμού και της αρχιτεκτονικής, καθώς και με τα πρότυπα UML που εξηγούν πως ακριβώς λειτουργεί το σύστημα, επιχειρούμε μια άσκηση μοντελοποίησης απειλής. Θα πρέπει να αναπτύξουμε ρεαλιστικά σενάρια απειλής. Να αναλύσουμε τον σχεδιασμό και την αρχιτεκτονική, ώστε να εξασφαλίσουμε ότι αυτές οι απειλές έχουν μετριαστεί, έχουν γίνει αποδεκτές από την επιχείρηση, ή έχουν εκχωρηθεί σε μια τρίτη οντότητα (third party), όπως μια ασφαλιστική εταιρία. Όταν οι προσδιορισμένες απειλές δεν έχουν καμία στρατηγική μετριασμού, θα πρέπει να εξετάσουμε εκ νέου τον σχεδιασμό και την αρχιτεκτονική, μαζί με τον αρχιτέκτονα συστήματος, ώστε να τροποποιήσουμε το σχεδιασμό.

3. Φάση 3: Κατά τη Διάρκεια της Ανάπτυξης (During Development).

Θεωρητικά, η ανάπτυξη είναι η εφαρμογή ενός σχεδιασμού. Εντούτοις, στην πραγματικότητα, πολλές αποφάσεις σχεδιασμού λαμβάνονται κατά τη διάρκεια της ανάπτυξης κώδικα. Συχνά είναι μικρότερες αποφάσεις, που ήταν είτε πάρα πολύ λεπτομερείς για να περιγραφούν στο σχεδιασμό, ή σε άλλες περιπτώσεις, ήταν ζητήματα όπου καμία καθοδήγηση πολιτικής ή προτύπου δεν προσφερόταν.

- Φάση 3A: Περιηγήσεις Κώδικα (Code Walkthroughs). - Η ομάδα ασφάλειας θα πρέπει να εκτελέσει μια περιήγηση κώδικα με τους υπεύθυνους ανάπτυξης και σε μερικές περιπτώσεις, τους αρχιτέκτονες συστήματος. Μια περιήγηση κώδικα είναι μια υψηλού επιπέδου περιήγηση του κώδικα όπου οι υπεύθυνοι ανάπτυξης μπορούν να εξηγήσουν τη λογική και τη ροή του εφαρμοσμένου κώδικα. Επιτρέπει στην ομάδα επισκόπησης κώδικα να αποκτήσει μια γενική κατανόηση του κώδικα και επιτρέπει στους υπεύθυνους ανάπτυξης να εξηγήσουν γιατί ορισμένα πράγματα αναπτύχθηκαν με τον τρόπο που αναπτύχθηκαν.
- Φάση 3B: Επισκοπήσεις Κώδικα (Code Reviews). - Έχοντας εφοδιαστεί με μια καλή κατανόηση για το πως είναι δομημένος ο κώδικας και γιατί ορισμένα πράγματα κωδικοποιήθηκαν με τον τρόπο που έγιναν, ο ελεγκτής (tester) μπορεί πλέον να εξετάσει τον πραγματικό κώδικα για ατέλειες ασφάλειας. Οι στατικές επισκοπήσεις

κώδικα επικυρώνουν τον κώδικα ενάντια σε ένα σύνολο από λίστες ελέγχου (checklists), που περιλαμβάνουν:

- Απαιτήσεις επιχείρησης για τη διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα.
- λίστες ελέγχου για τις ευπάθειες που περιλαμβάνονται στο OWASP Guide ή Top 10 για τα τεχνικά σημεία που είναι εκτεθειμένα..
- Συγκεκριμένα ζητήματα σχετικά με τη γλώσσα ή το πλαίσιο που χρησιμοποιείται, όπως το Scarlet paper για την PHP ή τις λίστες ελέγχου ασφαλούς κωδικοποίησης (Secure Coding checklists) της Microsoft για την ASP.NET.
- Οποιεσδήποτε συγκεκριμένες απαιτήσεις βιομηχανίας, όπως Sarbanes-Oxley 404, COPPA, ISO 17799, APRA, HIPAA, Visa Merchant guidelines.

4. **Φάση 4: Κατά τη Διάρκεια της Επέκτασης (During Deployment).**

- Φάση 4A: Έλεγχος Διείσδυσης Εφαρμογών (Application Penetration Testing). - Έχοντας ελέγξει τις απαιτήσεις, αναλύσει το σχεδιασμό και εκτελέσει την επισκόπηση κώδικα, υποτίθεται ότι όλα τα ζητήματα έχουν ευρεθεί. Ενδεχομένως, να συμβαίνει αυτό, όμως ο έλεγχος διείσδυσης σε μια εφαρμογή αφού έχει επεκταθεί, παρέχει έναν τελευταίο έλεγχο για να εξασφαλιστεί ότι όντως τίποτα δεν έχει ξεφύγει.
- Φάση 4B: Έλεγχος Διαχείρισης Διαμόρφωσης (Configuration Management Testing). - Ο έλεγχος διείσδυσης εφαρμογών θα πρέπει να περιλαμβάνει τον έλεγχο για το πως επεκτάθηκε και εξασφαλίσθηκε, η υποδομή. Αν και η εφαρμογή μπορεί να είναι ασφαλής, μια μικρή πτυχή της διαμόρφωσης θα μπορούσε να ακολουθεί τις προεπιλεγμένες ρυθμίσεις της εγκατάστασης και συνεπώς να είναι τρωτή.

5. **Φάση 5: Συντήρηση και Λειτουργίες (Maintenance and Operations).**

- Φάση 5A: Διενέργεια επισκοπήσεων διαχείρισης λειτουργίας (Conduct Operational Management Reviews). - Θα πρέπει να υπάρχει μια διαδικασία που να εξηγεί λεπτομερώς το πως ρυθμίζεται η λειτουργική πλευρά και της εφαρμογής αλλά και της υποδομής.
- Φάση 5B: Περιοδικοί Έλεγχοι Κατάστασης (Conduct Periodic Health Checks). - Μηνιαίοι ή τριμηνιαίοι έλεγχοι θα πρέπει να εκτελεσθούν και στην εφαρμογή και στην υποδομή για να εξασφαλιστεί ότι κανένας νέος κίνδυνος ασφάλειας δεν έχει εισαχθεί και ότι το επίπεδο ασφάλειας είναι ακόμα άθικτο.
- Φάση 5C: Εξασφάλιση Επαλήθευσης Αλλαγών (Ensure Change Verification). - Αφού έχει εγκριθεί και έχει ελεγχθεί κάθε αλλαγή στο περιβάλλον QA[18] και έχει εγκατασταθεί στο περιβάλλον παραγωγικής λειτουργίας, είναι ζωτικής σημασίας ότι, ως μέρος της διαδικασίας διαχείρισης αλλαγής, η αλλαγή θα πρέπει να ελεγχθεί για να εξασφαλισθεί ότι το επίπεδο ασφάλειας δεν έχει επηρεαστεί από αυτήν την αλλαγή.

[18] QA (Quality Assurance) - Διασφάλιση ποιότητας.

3.2.3 Βασική μεθοδολογία ασφάλειας

3.2.3.1 Έλεγχος Διείσδυσης Εφαρμογών Ιστού (Web Application Penetration Testing)

Σε αυτήν την ενότητα περιγράφεται η μεθοδολογία του ελέγχου διείσδυσης εφαρμογών ιστού του OWASP και εξηγείται πως μπορεί να ελεγχθεί η κάθε ευπάθεια.

Ένας έλεγχος διείσδυσης είναι μια μέθοδος αξιολόγησης της ασφάλεια ενός συστήματος ηλεκτρονικών υπολογιστών ή ενός δικτύου με την προσομοίωση μιας επίθεσης. Ένας Έλεγχος Διείσδυσης Εφαρμογών Ιστού (Web Application Penetration Test) εστιάζει μόνο στην αξιολόγηση της ασφάλειας μιας εφαρμογής ιστού. Η διαδικασία περιλαμβάνει μια ενεργή ανάλυση της εφαρμογής για οποιεσδήποτε αδυναμίες, τεχνικές ατέλειες, ή ευπάθειες. Οποιαδήποτε ζητήματα ασφάλειας ανιχνεύονται, θα πρέπει να επισημανθούν στον ιδιοκτήτη συστήματος μαζί με μια αξιολόγηση της επίπτωσής τους και συχνά με μια πρόταση για το μετριασμό ή μια τεχνική λύση.

Μια ευπάθεια είναι μια ατέλεια ή μια αδυναμία στο σχεδιασμό, στην υλοποίηση, ή λειτουργία και στη διαχείριση ενός συστήματος που θα μπορούσε να χρησιμοποιηθεί για να παραβιαστεί η πολιτική ασφάλειας του συστήματος. Μια απειλή είναι μια πιθανή επίθεση όπου, με την εκμετάλλευση μιας ευπάθειας, μπορεί να βλάψει τα αγαθά μιας εφαρμογής (πόροι αξίας, όπως τα δεδομένα σε μια βάση δεδομένων ή στο σύστημα αρχείων). Ένας έλεγχος (test) είναι μια ενέργεια που προσπαθεί να αναδείξει μια ευπάθεια στην εφαρμογή. Ο έλεγχος διείσδυσης δε θα είναι ποτέ μια ακριβής επιστήμη όπου μια πλήρης λίστα όλων των πιθανών ζητημάτων που θα πρέπει να ελεγχθούν, μπορεί να καθοριστεί. Πράγματι, ο έλεγχος διείσδυσης είναι μια κατάλληλη τεχνική για το έλεγχο της ασφάλειας εφαρμογών ιστού, μόνο υπό ορισμένες συνθήκες. Στόχος είναι να συλλεχθούν όλες οι πιθανές τεχνικές έλεγχου, να εξηγηθούν και να κρατηθεί ενημερωμένος ο οδηγός.

Η μέθοδος Έλεγχος Διείσδυσης Εφαρμογών Ιστού του OWASP βασίζεται στην προσέγγιση black box (μαύρου κουτιού). Ο ελεγκτής δεν γνωρίζει τίποτα ή γνωρίζει ελάχιστες πληροφορίες για την εφαρμογή, την οποία εξετάζει. Ο έλεγχος περιλαμβάνει τα εξής στοιχεία::

- τον ελεγκτή, ο οποίος εκτελεί τις δραστηριότητες του ελέγχου.
- τα εργαλεία και τη μεθοδολογία: τα οποία αποτελούν τον πυρήνα του Οδηγού Ελέγχου (Testing Guide).
- την εφαρμογή, η οποία είναι το μαύρο κουτί (black box) που θα ελεγχθεί.

Ο έλεγχος διαιρείται σε 2 φάσεις:

- Παθητικός τρόπος (Passive mode): στον παθητικό τρόπο, ο ελεγκτής προσπαθεί να καταλάβει τη λογική της εφαρμογής, δηλαδή «παίζει» με την εφαρμογή. Μπορούν να χρησιμοποιηθούν εργαλεία για τη συλλογή πληροφοριών, παραδείγματος χάριν, ένας HTTP proxy για να παρατηρεί όλες τις αιτήσεις (HTTP requests) και αποκρίσεις (responses) HTTP. Στο τέλος αυτής της φάσης, ο ελεγκτής θα πρέπει να καταλάβει όλα τα σημεία πρόσβασης (πύλες-gates) της εφαρμογής (π.χ., επικεφαλίδες HTTP (HTTP headers), παράμετροι και cookies). Το τμήμα της συλλογής πληροφοριών (Information Gathering) εξηγεί το πως να εκτελεστεί ένας έλεγχος με

παθητικό τρόπο. Παραδείγματος χάριν, ο ελεγκτής θα μπορούσε να βρει το εξής: https://www.example.com/login/Authentic_Form.html

Αυτό υποδεικνύει μια φόρμα (form) αυθεντικοποίησης, στην οποία η εφαρμογή αιτείται ένα όνομα χρήστη (username) και έναν κωδικό πρόσβασης (password). Οι ακόλουθες παράμετροι αντιπροσωπεύουν δύο σημεία πρόσβασης (gates) στην εφαρμογή:

http://www.example.com/Appx.jsp?a=1&b=1

Σε αυτήν την περίπτωση, η εφαρμογή παρουσιάζει δύο πύλες (παράμετροι a και b). Όλες οι πύλες, που βρίσκονται σε αυτήν την φάση, αντιπροσωπεύουν ένα σημείο του ελέγχου. Ένα spreadsheet (υπολογισμός με λογιστικό φύλλο) για το δέντρο καταλόγου της εφαρμογής και όλα τα σημεία πρόσβασής της, θα ήταν πολύ χρήσιμος για τη δεύτερη φάση.

- Ενεργός τρόπος (Active mode): σε αυτήν την φάση, ο ελεγκτής αρχίζει να ελέγχει χρησιμοποιώντας τη μεθοδολογία η οποία περιγράφεται στις επόμενες παραγράφους.

3.2.3.2 Πρότυπο της Παραγράφου του Ελέγχου (Testing paragraph template)

Παρακάτω εμφανίζεται το πρότυπο (βασικά τμήματα) που πρέπει να ακολουθεί η παράγραφος που αναφέρεται σε κάθε έλεγχο.

- Συνοπτική Περίληψη (Brief Summary**)** - Περιγράφει σε «φυσική γλώσσα» αυτό που θέλουμε να εξετάσουμε. Το τμήμα αυτό απευθύνεται κυρίως στους ανθρώπους που δεν είναι τεχνικοί (π.χ.: διευθυντής πελατών).
- Περιγραφή του Ζητήματος (Description of the Issue) - Σύντομη περιγραφή του ζητήματος: Θέμα και επεξήγηση.
- Έλεγχος μαύρου κουτιού και παράδειγμα (Black Box testing and example)
  - Πώς θα γίνει ο έλεγχος για ευπάθειες.
  - Αναμενόμενο Αποτέλεσμα.
- Έλεγχος γκρίζου κουτιού και παράδειγμα (Gray Box testing and example)
  - Πώς θα γίνει ο έλεγχος για ευπάθειες.
  - Αναμενόμενο Αποτέλεσμα.
- Αναφορές (References)
  - Whitepapers
  - Εργαλεία (Tools)

Black Box έναντι Gray Box

- Black Box: είναι η εφαρμογή δοκιμαστικών δεδομένων που έχουν προέλθει από καθορισμένες λειτουργικές απαιτήσεις, χωρίς να λαμβάνουν υπόψη τη δομή της εφαρμογής στην οποία εφαρμόζονται. Η εφαρμογή εξετάζεται χρησιμοποιώντας την εξωτερική της διεπαφή, αυτή που χρησιμοποιούν οι απλοί χρήστες. Μιμούνται την ακολουθία αλληλεπιδράσεων χρήστη-εφαρμογής και κάθε αποτυχία δείχνει ότι ο χρήστης έλαβε ανεπαρκή υπηρεσία.
- Gray Box: Ο ελεγκτής διείσδυσης έχει μερικές πληροφορίες σχετικά με την εσωτερική δομή της εφαρμογής. π.χ.: προμηθευτής πλατφόρμας (platform vendor), αλγόριθμος παραγωγής συνόδου ID (session ID generation algorithm). Εξετάζεται η δομή της εφαρμογής και βάση αυτής καθορίζονται τα δεδομένα του ελέγχου.

Ο έλεγχος λευκού κουτιού (White box testing), που ορίζεται ως πλήρης γνώση του εσωτερικού της εφαρμογής, είναι πέρα από το πεδίο εφαρμογής του Οδηγού Ελέγχου (Testing Guide) και καλύπτεται από το έργο επισκόπησης κώδικα του OWASP (OWASP Code Review Project).

3.2.3.3 Πρότυπο Ελέγχου (Testing Model)

Το σύνολο των ενεργών ελέγχων έχει χωριστεί σε 9 υποκατηγορίες που καλύπτουν συνολικά 66 ελέγχους και περιγράφονται συνοπτικά στις επόμενες παραγράφους:

3.2.3.3.1 Συλλογή Πληροφοριών (Information Gathering)

Η πρώτη φάση στην αξιολόγηση της ασφάλειας εστιάζει στη συλλογή όσο το δυνατόν περισσότερων πληροφοριών σχετικά με μια εφαρμογή-στόχο. Η Συλλογή Πληροφοριών είναι απαραίτητο βήμα ενός ελέγχου διείσδυσης (penetration test). Αυτή η εργασία μπορεί να εκτελεσθεί με πολλούς διαφορετικούς τρόπους. Χρησιμοποιώντας κοινά εργαλεία (π.χ. μηχανές αναζήτησης), ανιχνευτές (scanners), στέλνοντας απλές αιτήσεις http (http requests), ή ειδικά επεξεργασμένες αιτήσεις, είναι δυνατό να οδηγηθεί η εφαρμογή στη διαρροή πληροφοριών, όπως η αποκάλυψη μηνυμάτων σφάλματος που στέλνει ως απάντηση στις αιτήσεις μας ή η αποκάλυψη των εκδόσεων και τεχνολογιών που χρησιμοποιούνται από την εφαρμογή. Οι έλεγχοι που περιλαμβάνει είναι οι ακόλουθοι:

- Αράχνες, ρομπότ και ιχνηλάτες - Spiders, Robots, and Crawlers[19] (OWASP-IG-001): Αυτή η φάση της διαδικασίας συλλογής πληροφοριών αποτελείται από την πλοήγηση (browsing) σε πόρους που είναι σχετικοί με την εφαρμογή που ελέγχεται με συνακόλουθη επεξεργασία τους.
- Ανακάλυψη / Αναγνώριση Μηχανών Αναζήτησης - Search Engine Discovery / Reconnaissance (OWASP-IG-002): Οι μηχανές αναζήτησης, όπως το Google, μπορούν να χρησιμοποιηθούν για να ανακαλύψουν ζητήματα σχετικά με τη δομή μιας εφαρμογής ιστού ή τις σελίδες σφάλματος που παράγονται από την εφαρμογή και έχουν εκτεθεί δημόσια.
- Ταυτοποίηση των σημείων εισόδου εφαρμογής - Identify application entry points (OWASP-IG-003): Η εξέταση της εφαρμογής και της «επιφάνειας επίθεσής της» (δηλαδή των τμημάτων που είναι ορατά και επομένως διαθέσιμα στον επιτιθέμενο), προηγείται πριν αρχίσει οποιαδήποτε επίθεση. Αυτό το τμήμα θα βοηθήσει να ταυτοποιηθεί και να προσδιορισθεί κάθε περιοχή μέσα στην εφαρμογή που θα πρέπει να ερευνηθεί, μόλις ολοκληρωθεί η φάση της απαρίθμησης και χαρτογράφησης.
- Έλεγχος Αποτυπώματος Εφαρμογής Ιστού - Testing Web Application Fingerprint (OWASP-IG-004): Το αποτύπωμα εφαρμογής ιστού είναι το πρώτο βήμα της διαδικασίας συλλογής πληροφοριών. Η γνώση της έκδοσης και του τύπου ενός εξυπηρέτη ιστού (web server), επιτρέπει στους ελεγκτές να προσδιορίσουν τις γνωστές ευπάθειες και τις κατάλληλες εκμεταλλεύσεις

[19] Οι spiders ή αλλιώς crawlers ή robots είναι προγράμματα υπεύθυνα για τον εντοπισμό ιστοσελίδων στο Ίντερνετ για δεικτοδότηση. Μέσω αυτών των προγραμμάτων, η μηχανή αναζήτησης πληροφορείται για την ύπαρξη ενός δικτυακού τόπου ο οποίος, αν δεν είχε εντοπιστεί από τους spiders, θα έμενε στην αφάνεια, κάπου σε κάποιον server στο αόρατο Ίντερνετ.

(exploits[20]), τις οποίες μπορούν να χρησιμοποιήσουν κατά τη διάρκεια του ελέγχου.

- Ανακάλυψη Εφαρμογής - Application Discovery (OWASP-IG-005): Η ανακάλυψη εφαρμογής είναι μια δραστηριότητα που προσανατολίζεται στον προσδιορισμό των εφαρμογών ιστού που φιλοξενούνται σε έναν εξυπηρέτη ιστού/εφαρμογής (web server/application server). Αυτή η ανάλυση είναι σημαντική επειδή συχνά δεν υπάρχει άμεσος σύνδεσμος που να οδηγεί στο παρασκήνιο (backend) της κύριας εφαρμογής. Η ανάλυση ανακάλυψης μπορεί να είναι χρήσιμη για να εμφανίσει λεπτομέρειες όπως εφαρμογές ιστού που χρησιμοποιούνται για λόγους διαχείρισης. Επιπλέον, μπορεί να αποκαλύψει παλαιές εκδόσεις αρχείων ή αντικειμένων όπως, μη διαγραμμένα και παρωχημένα scripts, που προέκυψαν κατά τη διάρκεια της φάσης της δοκιμής/ανάπτυξης ή ως αποτέλεσμα της συντήρησης.
- Ανάλυση των Κωδικών Σφάλματος - Analysis of Error Codes (OWASP-IG-006): Κατά τη διάρκεια ενός ελέγχου διείσδυσης, οι εφαρμογές ιστού μπορούν να αποκαλύψουν πληροφορίες που δεν προορίζεται να φανούν σ' έναν τελικό χρήστη. Πληροφορίες όπως κωδικοί σφάλματος (μηνύματα λάθους) μπορούν να ενημερώσουν τον ελεγκτή για τις τεχνολογίες και τα προϊόντα που χρησιμοποιούνται από την εφαρμογή.

3.2.3.3.2 Έλεγχος Διαχείρισης Διαμόρφωσης (Configuration Management Testing)

Συχνά η ανάλυση της αρχιτεκτονικής της υποδομής και της τοπολογίας μπορεί να αποκαλύψει πολλά στοιχεία σχετικά με μια εφαρμογή ιστού. Οι πληροφορίες όπως πηγαίος κώδικας, λειτουργία διαχείρισης, μέθοδοι αυθεντικοποίησης και διαμορφώσεις υποδομής, μπορούν να ληφθούν υπόψη. Οι έλεγχοι που περιλαμβάνει είναι οι ακόλουθοι:

- Έλεγχος SSL/TLS - SSL/TLS Testing (OWASP-CM-001): Τα SSL και TLS είναι δύο πρωτόκολλα που παρέχουν, με την υποστήριξη της κρυπτογράφησης, ασφαλή κανάλια για προστασία, εμπιστευτικότητα και αυθεντικοποίηση της διαβίβασης των πληροφοριών. Εξετάζοντας την κρισιμότητα αυτών των εφαρμογών ασφάλειας, είναι σημαντικό να ελεγχθεί η χρήση ενός ισχυρού κρυπτογραφικού αλγορίθμου (cipher[21]) και της κατάλληλης εκτέλεσής του.
- Έλεγχος Ακροατή βάσης δεδομένων - DB Listener Testing (OWASP-CM-002): Κατά τη διάρκεια της διαμόρφωσης ενός εξυπηρέτη βάσεων δεδομένων, πολλοί διαχειριστές DB δεν εξετάζουν επαρκώς την ασφάλεια του τμήματος ακροατή βάσης δεδομένων. Ο ακροατής θα μπορούσε να αποκαλύψει ευαίσθητα δεδομένα, καθώς επίσης και ρυθμίσεις διαμόρφωσης ή στιγμιότυπα (instances) βάσεων δεδομένων που «τρέχουν», εάν διαμορφώνονται χωρίς ασφάλεια και εξετάζονται με χειροκίνητες ή αυτοματοποιημένες τεχνικές. Οι

[20] Exploit αποκαλείται ένα κακόβουλο και επιθετικό πρόγραμμα το οποίο εκμεταλλεύεται τα κενά ασφαλείας σε κάποιον υπολογιστή για να αποκτηθεί πρόσβαση σε αυτόν. Για παράδειγμα, κάποιο κενό στο λειτουργικό σύστημα, ή ένα κακορυθμισμένο firewall.

[21] Κρυπτογραφικός αλγόριθμος (cipher) είναι η μέθοδος μετασχηματισμού δεδομένων σε μια μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα, είναι μια πολύπλοκη μαθηματική συνάρτηση.

πληροφορίες που εμφανίζονται, θα είναι συχνά χρήσιμες σε έναν ελεγκτή και θα χρησιμοποιηθούν ως είσοδος σε επόμενους ελέγχους.

- Έλεγχος Διαχείρισης Διαμόρφωσης Υποδομής - Infrastructure Configuration Management Testing (OWASP-CM-003): Η εγγενής πολυπλοκότητα της διασυνδεόμενης και ετερογενούς υποδομής ενός εξυπηρέτη ιστού (web server), που μπορεί να περιλαμβάνει εκατοντάδες εφαρμογές ιστού, καθιστά τη διαχείριση και επισκόπηση της διαμόρφωσης ως ένα θεμελιώδες βήμα στον έλεγχο και στην ανάπτυξη κάθε ξεχωριστής εφαρμογής. Στην πραγματικότητα, αρκεί μόνο μια απλή ευπάθεια για να υπονομεύσει την ασφάλεια ολόκληρης της υποδομής και έτσι, τα διάφορα μικρά και σχεδόν ασήμαντα προβλήματα μπορούν να εξελιχθούν σε σοβαρούς κινδύνους για τυχόν άλλες εφαρμογές στον ίδιο εξυπηρέτη (server). Προκειμένου να ελεγχθούν αυτά τα προβλήματα, είναι εξαιρετικά σημαντικό να εκτελεστεί μια σε βάθος επισκόπηση της διαμόρφωσης και των γνωστών ζητημάτων ασφάλειας των συστημάτων.
- Έλεγχος Διαχείρισης Διαμόρφωσης Εφαρμογής - Application Configuration Management Testing (OWASP-CM-004): Οι εφαρμογές ιστού κρύβουν κάποιες πληροφορίες που συνήθως δεν εξετάζονται κατά τη διάρκεια της ανάπτυξης ή της διαμόρφωσης της ίδιας της εφαρμογής. Αυτά τα δεδομένα μπορεί να ανακαλυφθούν στον πηγαίο κώδικα, στα αρχεία καταγραφής (log files) ή στους προεπιλεγμένους κωδικούς σφάλματος των εξυπηρετών ιστού. Μια σωστή προσέγγιση σε αυτό το θέμα είναι θεμελιώδης, κατά τη διάρκεια μιας αξιολόγησης της ασφάλειας.
- Έλεγχος για Χειρισμό Επεκτάσεων Αρχείων - Testing for File Extensions Handling (OWASP-CM-005): Όταν οι επεκτάσεις των αρχείων είναι παρούσες σε έναν εξυπηρέτη ιστού ή μια εφαρμογή ιστού, καθιστούν δυνατό τον προσδιορισμό των τεχνολογιών που συνθέτουν την εφαρμογή-στόχο, π.χ. επεκτάσεις jsp και asp. Οι επεκτάσεις αρχείων μπορούν επίσης να αποκαλύψουν πρόσθετα συστήματα που συνδέονται με την εφαρμογή.
- Παλιά, Εφεδρικά και Μη-αναφερόμενα Αρχεία - Old, Backup and Unreferenced Files (OWASP-CM-006): Τα περιττά, αναγνώσιμα και μεταφορτώσιμα (downloadable) αρχεία σε έναν εξυπηρέτη ιστού, όπως τα παλαιά, εφεδρικά και μετονομασμένα αρχεία, αποτελούν μια σημαντική πηγή διαρροής πληροφοριών. Είναι απαραίτητο να ελεγχθεί η παρουσία αυτών των αρχείων διότι ίσως να περιέχουν μέρος του πηγαίου κώδικα, διαδρομές (paths) εγκατάστασης, καθώς επίσης και κωδικούς πρόσβασης για εφαρμογές ή/και βάσεις δεδομένων.
- Διαχειριστικές Διεπαφές Υποδομής και Εφαρμογής - Infrastructure and Application Admin Interfaces (OWASP-CM-007): Πολλές εφαρμογές χρησιμοποιούν μια κοινή πορεία για τις διαχειριστικές διεπαφές (interfaces), την οποία μπορεί να χρησιμοποιήσουν μη εξουσιοδοτημένοι χρήστες για να υποθέσουν ή αναζητήσουν (ακόμη και με ωμή βία) διαχειριστικούς κωδικούς πρόσβασης. Αυτός ο έλεγχος έχει σκοπό να ανακαλύψει τις διεπαφές διαχείρισης και να κατανοήσει εάν είναι δυνατό να τις εκμεταλλευτεί κάποιος για να έχει πρόσβαση στη λειτουργικότητα του διαχειριστή.
- Έλεγχος για Μεθόδους HTTP και XST - Testing for HTTP Methods and XST (OWASP-CM-008): Σε αυτόν τον έλεγχο, εξετάζεται το γεγονός ότι ο εξυπηρέτης ιστού δεν διαμορφώνεται για να επιτρέψει κάποιες ενδεχομένως

επικίνδυνες εντολές (μέθοδοι) http, καθώς και ότι δεν είναι δυνατό το Cross Site Tracing (XST)[22].

3.2.3.3.3 Έλεγχος Επιχειρησιακής Λογικής (Business Logic Testing)

Έλεγχος επιχειρησιακής λογικής - Business logic testing (OWASP-BL-001): Ο έλεγχος για ατέλειες επιχειρησιακής λογικής σε μια πολυσύνθετη δυναμική εφαρμογή ιστού, απαιτεί σκέψη με μη συμβατικούς τρόπους. Αυτός ο τύπος ευπάθειας δεν μπορεί να ανιχνευθεί από έναν ανιχνευτή (scanner) ευπάθειας και στηρίζεται στις δεξιότητες και τη δημιουργικότητα του ελεγκτή διείσδυσης. Επιπλέον, αυτός ο τύπος ευπάθειας είναι συνήθως ένας από τους πιο δύσκολους να ανιχνευθεί, αλλά, συγχρόνως, είναι και ένας από τους πιο καταστρεπτικούς, εάν χρησιμοποιηθεί, σε μια εφαρμογή. Η επιχειρησιακή λογική μπορεί να συμπεριλαμβάνει:

- Επιχειρησιακούς κανόνες που εκφράζουν την πολιτική της επιχείρησης (όπως κανάλια, τοποθεσία, διοικητικές μέριμνες, τιμές και προϊόντα) και
- Ροές εργασίας (workflows) που βασίζονται στις οργανωμένες σε βήματα εργασίες διαβίβασης των εγγράφων ή δεδομένων από έναν συμμετέχοντα (ένα πρόσωπο ή ένα σύστημα λογισμικού) σε ένα άλλο.

3.2.3.3.4 Έλεγχος Αυθεντικοποίησης (Authentication Testing)

Η αυθεντικοποίηση είναι η ενέργεια της καθιέρωσης ή της επιβεβαίωσης κάποιου ως αυθεντικού, δηλαδή ότι οι αξιώσεις που γίνονται από κάποιον, ή για ένα συγκεκριμένο πράγμα είναι αληθινές. Η αυθεντικοποίηση ενός αντικειμένου μπορεί να αφορά την προέλευσή του, ενώ η αυθεντικοποίηση ενός πρόσωπου συνίσταται συχνά στην επαλήθευση της ταυτότητάς του. Η αυθεντικοποίηση εξαρτάται από έναν ή περισσότερους παράγοντες αυθεντικοποίησης. Στην ασφάλεια υπολογιστών, η αυθεντικοποίηση είναι η διαδικασία του ελέγχου της ψηφιακής ταυτότητας του αποστολέα σε μια επικοινωνία. Ένα κοινό παράδειγμα μιας τέτοιας διαδικασίας είναι η διαδικασία σύνδεσης (logon). Ο έλεγχος του σχήματος αυθεντικοποίησης σημαίνει την κατανόηση για το πώς η διαδικασία αυθεντικοποίησης λειτουργεί και το πώς χρησιμοποιώντας αυτές τις πληροφορίες θα μπορέσουμε να παρακάμψουμε το μηχανισμό αυθεντικοποίησης. Οι έλεγχοι που περιλαμβάνει είναι οι ακόλουθοι:

- Μεταφορά Πιστοποιητικών δια μέσου ενός Κρυπτογραφημένου Καναλιού - Credentials transport over an encrypted channel (OWASP-AT-001): Ο ελεγκτής θα προσπαθήσει ακριβώς να καταλάβει εάν τα δεδομένα που καταχωρούν οι χρήστες στη διαδικτυακή φόρμα (form), προκειμένου να εισέλθουν σε έναν ιστοχώρο (web site), διαβιβάζονται χρησιμοποιώντας ασφαλή πρωτόκολλα που τους προστατεύουν από έναν επιτιθέμενο ή όχι.
- Έλεγχος για απαρίθμηση χρηστών - Testing for user enumeration (OWASP-AT-002): Ο σκοπός αυτού του ελέγχου είναι να επαληθεύσει εάν είναι δυνατό να συλλεχθεί ένα σύνολο έγκυρων χρηστών, αλληλεπιδρώντας με το

[22] Cross Site Tracing (XST) είναι μια ευπάθεια ασφάλειας δικτύου που εκμεταλλεύεται τη μέθοδο HTTP TRACE. Τα XST scripts εκμεταλλεύονται ActiveX, Flash, Java ή οποιουσδήποτε άλλους ελέγχους που επιτρέπουν την εκτέλεση μιας αίτησης (request) HTTP TRACE. Η απόκριση (response) HTTP TRACE περιλαμβάνει όλες τις επικεφαλίδες HTTP, συμπεριλαμβανομένων των δεδομένων πιστοποίησης και του περιεχομένου των HTTP cookies, τα οποία είναι έπειτα διαθέσιμα στο script. Σε συνδυασμό με ατέλειες cross domain access στους web browsers, το exploit είναι σε θέση να συλλέξει τα εναποθηκευμένα (cached) πιστοποιητικά οποιουδήποτε web site, συμπεριλαμβανομένων εκείνων που χρησιμοποιούν SSL.

μηχανισμό αυθεντικοποίησης της εφαρμογής. Αυτός ο έλεγχος θα είναι χρήσιμος για τον έλεγχο «ωμής βίας» (brute force testing), στον οποίο ελέγχεται εάν, έχοντας διαθέσιμο ένα έγκυρο όνομα χρήστη (username), είναι δυνατό να ευρεθεί ο αντίστοιχος κωδικός πρόσβασης (password).

- Έλεγχος για Εικάσιμο (με Λεξικό) Λογαριασμό Χρηστών - Testing for Guessable (Dictionary) User Account (OWASP-AT-003): Εδώ εξετάζεται εάν υπάρχουν προκαθορισμένοι λογαριασμοί χρηστών ή εικάσιμοι συνδυασμοί ονόματος χρήστη-κωδικού πρόσβασης (έλεγχος βάσει λεξικού).
- Έλεγχος «Ωμής Βίας» - Brute Force Testing (OWASP-AT-004): Όταν μια επίθεση τύπου λεξικού αποτυγχάνει, ένας ελεγκτής μπορεί να προσπαθήσει να χρησιμοποιήσει τις μεθόδους «ωμής Βίας», προκειμένου να επιτύχει την αυθεντικοποίηση. Ο έλεγχος «ωμής Βίας» δεν είναι εύκολο να ολοκληρωθεί για τους ελεγκτές, λόγω του χρόνου που απαιτείται και του πιθανού αποκλεισμού του ελεγκτή από περαιτέρω προσβάσεις (π.χ. κλείδωμα του ονόματος χρήστη μετά από 3 αποτυχημένες προσπάθειες σύνδεσης ή αποκλεισμός ΄για κάποιο χρονικό διάστημα της δικτυακής διεύθυνσης από την οποία προέρχονται συνεχόμενες αποτυχημένες αιτήσεις σύνδεσης).
- Έλεγχος για την παράκαμψη του σχήματος αυθεντικοποίησης - Testing for bypassing authentication schema (OWASP-AT-005): Κάποιες παθητικοί μέθοδοι ελέγχου προσπαθούν να παρακάμψουν το σχήμα αυθεντικοποίησης, αναγνωρίζοντας ότι δεν προστατεύονται επαρκώς όλοι οι πόροι της εφαρμογής. Ο ελεγκτής μπορεί να έχει πρόσβαση σε αυτούς τους πόρους χωρίς να απαιτείται η αυθεντικοποίησή του.
- Έλεγχος για ευπαθείς λειτουργίες υπενθύμισης και επαναφοράς κωδικού πρόσβασης - Testing for vulnerable remember password and pwd reset (OWASP-AT-006): Εδώ εξετάζεται το πώς η εφαρμογή διαχειρίζεται τις περιπτώσεις που ένας νομότυπος χρήστης έχει ξεχάσει τον κωδικό πρόσβασης. Επίσης, ελέγχεται εάν η εφαρμογή επιτρέπει στο χρήστη να αποθηκεύσει τον κωδικό πρόσβασης στον φυλλομετρητή (browser) (λειτουργία «απομνημόνευση του κωδικού πρόσβασης»).
- Έλεγχος Αποσύνδεσης και Διαχείρισης Μνήμης του Φυλλομετρητή - Testing for Logout and Browser Cache Management (OWASP-AT-007): Εδώ ελέγχεται, εάν οι λειτουργίες αποσύνδεσης (logout) και προσωρινής αποθήκευσης-απομνημόνευσης (caching) εφαρμόζονται κατάλληλα.
- Έλεγχος για CAPTCHA - Testing for CAPTCHA (OWASP-AT-008): Το CAPTCHA ("Εντελώς Αυτοματοποιημένος Έλεγχος Turing Κοινού για διαχωρισμό Υπολογιστών και Ανθρώπων -Completely Automated Public Turing test to tell Computers and Humans Apart") είναι ένας τύπος έλεγχου πρόκλησης-απόκρισης που χρησιμοποιείται από πολλές εφαρμογές ιστού για να εξασφαλίσει ότι η απόκριση δεν παράγεται από έναν υπολογιστή. Οι υλοποιήσεις είναι συχνά ευπαθείς σε διάφορα είδη επιθέσεων, ακόμα κι αν το παραγόμενο CAPTCHA είναι απαραβίαστο.
- Έλεγχος Αυθεντικοποίησης Πολλαπλών Παραγόντων - Testing Multiple Factors Authentication (OWASP-AT-009): Αυθεντικοποίηση πολλαπλών παραγόντων σημαίνει ότι πρέπει να εξετασθούν τα ακόλουθα σενάρια: λεκτικές μονάδες-συσκευές παραγωγής (generator tokens) κωδικού πρόσβασης μιας χρήσης (One-time password-OTP[23]), συσκευές Crypto όπως

[23] Ένας κωδικός πρόσβασης μίας χρήσης (OTP) είναι ένας κωδικός πρόσβασης που ισχύει για μόνο μια σύνοδο ή συναλλαγή σύνδεσης (login). Τα OTPs αποφεύγουν διάφορες ατέλειες που συνδέονται

USB tokens ή έξυπνες κάρτες, εφοδιασμένες με πιστοποιητικά X.509, τυχαίο OTP που στέλνεται μέσω SMS, προσωπικές πληροφορίες τις οποίες μόνο ο νόμιμος χρήστης υποτίθεται ότι γνωρίζει [OUTOFWALLET[24]].

- Έλεγχος για Συνθήκες Ανταγωνισμού - Testing for Race Conditions (OWASP-AT-010): Μια συνθήκη ανταγωνισμού (race condition) είναι μια ατέλεια που παράγει ένα απροσδόκητο αποτέλεσμα όταν η εκτέλεση με συγκεκριμένο χρονισμό δύο κατά τα λοιπά ανεξάρτητων ενεργειών οδηγεί στο να επηρεαστούν τα αποτελέσματα της μίας από την άλλη. Ένα τέτοιο παράδειγμα μπορεί να εμφανιστεί σε μια πολυνηματική εφαρμογή, όπου οι ενέργειες εκτελούνται στα ίδια δεδομένα. Οι συνθήκες ανταγωνισμού, από τη φύση τους, είναι δύσκολο να ελεγχθούν.

3.2.3.3.5 Έλεγχος Εξουσιοδότησης (Authorization testing)

Η εξουσιοδότηση έχει την έννοια του να επιτρέπεται πρόσβαση σε πόρους μόνο σε εκείνους, που απορρέει σχετικό δικαίωμα χρήσης από την πολιτική ασφάλειας. Ο έλεγχος εξουσιοδότησης που θα διενεργήσει ο ελεγκτής σημαίνει κατανόηση για το πώς λειτουργεί η διαδικασία εξουσιοδότησης και χρησιμοποίηση αυτών των πληροφοριών ώστε να παρακάμψει το μηχανισμό εξουσιοδότησης. Η εξουσιοδότηση είναι μια διαδικασία που επακολουθεί μετά από μια επιτυχή αυθεντικοποίηση, έτσι ο ελεγκτής θα επαληθεύσει αυτό το σημείο αφού πρώτα έχει αποκτήσει έγκυρα πιστοποιητικά, που συνδέονται με ένα καθορισμένο σύνολο ρόλων και δικαιωμάτων. Κατά τη διάρκεια αυτού του είδους αξιολόγησης, πρέπει να ελεγχθεί εάν είναι δυνατό να παρακαμφθεί το σχήμα εξουσιοδότησης, να βρεθεί μια ευπάθεια διάσχισης μονοπατιού, ή να βρεθούν τρόποι για να κλιμακωθούν (escalate) τα δικαιώματα που ορίζονται στον ελεγκτή. Οι έλεγχοι που περιλαμβάνει είναι οι ακόλουθοι:

- Έλεγχος για Διάσχιση Μονοπατιού - Testing for Path Traversal (OWASP-AZ-001): Αρχικά, εξετάζεται εάν είναι δυνατό να βρεθεί ένας τρόπος για να εκτελεστεί μια επίθεση διάσχισης μονοπατιού (path traversal) και να υπάρχει πρόσβαση σε προστατευμένες πληροφορίες.
- Έλεγχος για παράκαμψη του σχήματος εξουσιοδότησης - Testing for bypassing authorization schema (OWASP-AZ-002): Αυτό το είδος έλεγχου εστιάζει στην επαλήθευση για το πώς το σχήμα εξουσιοδότησης έχει εφαρμοστεί για κάθε ρόλο ή δικαίωμα ώστε να επιτρέψει πρόσβαση σε προστατευμένες λειτουργίες ή πόρους.

με τους παραδοσιακούς (στατικούς) κωδικούς πρόσβασης. Η σημαντικότερη ατέλεια που εξετάζεται από τα OTPs είναι ότι, σε αντίθεση με τους στατικούς κωδικούς πρόσβασης, δεν είναι ευπαθείς σε επιθέσεις επανάληψης. Αυτό σημαίνει ότι, εάν ένας πιθανός εισβολέας κατορθώσει να καταγράψει ένα OTP που χρησιμοποιήθηκε ήδη για να συνδεθεί (log into) σε μια υπηρεσία ή για να πραγματοποιήσει μια συναλλαγή, αυτός δε θα είναι σε θέση να το χρησιμοποιήσει κακόβουλα δεδομένου ότι δεν θα ισχύει πλέον.

[24] Out of Wallet (Εκτός πορτοφολιού): αναφέρεται στα ιδιωτικά δεδομένα που χρησιμοποιούνται για πιστοποίηση σε δραστηριότητες όπως telephone banking ή internet banking προκειμένου να αποτραπεί η κλοπή ταυτότητας. τα δεδομένα επιλέγονται ώστε να αποτελούν δεδομένα τα οποία δεν είναι εύκολα διαθέσιμα σε πρόσωπα εκτός από το χρήστη που θα γνώριζε αυτές τις πληροφορίες αλλά δεν είναι πιθανό να φέρει τέτοιες πληροφορίες στο πορτοφόλι του (οπότε η απώλεια-κλοπή του πορτοφολιού θα καθιστούσε τα δεδομένα αυτά διαθέσιμα σε τρίτους). Τυπικές ερωτήσεις θα ήταν «σε ποιο δημοτικό σχολείο πήγατε», «ποιο ήταν το όνομα του πρώτου σας κατοικιδίου» κ.λπ.. Αυτά τα δεδομένα παράγονται πλέον αυτόματα μέσω της επικάλυψης βάσεων δεδομένων.

- Έλεγχος για Κλιμάκωση Δικαιωμάτων - Testing for Privilege Escalation (OWASP-AZ-003): Κατά τη διάρκεια αυτής της φάσης, ο ελεγκτής πρέπει να επαληθεύσει ότι δεν είναι δυνατό για έναν χρήστη, να τροποποιήσει τα δικαιώματα ή τους ρόλους του μέσα στην εφαρμογή με τρόπους, οι οποίοι θα μπορούσαν να επιτρέψουν επιθέσεις κλιμάκωσης δικαιωμάτων.

3.2.3.3.6 Έλεγχος Διαχείρισης Συνόδου (Session Management Testing)

Στον πυρήνα οποιασδήποτε εφαρμογής ιστού υπάρχει ο τρόπος με τον οποίο, η εφαρμογή διατηρεί την κατάσταση της συνόδου του χρήστη και με αυτόν τον τρόπο ελέγχει την αλληλεπίδραση του χρήστη με τον ιστότοπο (site). Η διαχείριση συνόδου καλύπτει ευρέως όλους τους ελέγχους που γίνονται σε έναν χρήστη από την αυθεντικοποίηση μέχρι και το κλείσιμο της εφαρμογής. Το HTTP είναι ένα πρωτόκολλο χωρίς κατάσταση (stateless), που σημαίνει ότι οι εξυπηρέτες ιστού (web servers) αποκρίνονται στις αιτήσεις των πελατών (clients) χωρίς να συνδέουν τις αιτήσεις αυτές μεταξύ τους. Ωστόσο, η λογική ακόμη και των απλών εφαρμογών απαιτεί πολλαπλές αιτήσεις ενός χρήστη να συνδέονται η μια με την άλλη σε μια σύνοδο. Αυτό απαιτεί να χρησιμοποιηθούν λύσεις τρίτων κατασκευαστών (third party), είτε μέσω έτοιμου (Off-The-Shelf-OTS) ενδιάμεσου λογισμικού (middleware) και εξυπηρετών HTTP, είτε μέσω κατά περίπτωση υλοποιήσεων από τους υπεύθυνους ανάπτυξης εφαρμογών. Τα πλέον πιο δημοφιλή περιβάλλοντα εφαρμογών ιστού, όπως ASP και PHP, παρέχουν στους υπεύθυνους ανάπτυξης έτοιμες ενσωματωμένες ρουτίνες (routines) διαχείρισης συνόδου. Τυπικά, εκδίδεται κάποιο είδος τεκμηρίου (token) ταυτοποίησης, το οποίο αναφέρεται ως «ταυτότητα συνόδου» (Session ID) ή Cookie.

Υπάρχουν διάφοροι τρόποι με τους οποίους μια εφαρμογή ιστού μπορεί να αλληλεπιδράσει με ένα χρήστη. Κάθε ένας εξαρτάται από τη φύση του ιστοτόπου (site), την ασφάλεια και τις απαιτήσεις διαθεσιμότητας της εφαρμογής. Ενώ υπάρχουν αποδεκτές βέλτιστες πρακτικές (best practices) για την ανάπτυξη εφαρμογών, είναι σημαντικό να επισημανθεί ότι η ασφάλεια εφαρμογής εξετάζεται μέσα στα πλαίσια των απαιτήσεων και των προσδοκιών του προμηθευτή της. Οι έλεγχοι που περιλαμβάνει είναι οι ακόλουθοι:

- Έλεγχος για το Σχήμα Διαχείρισης Συνόδου - Testing for Session Management Schema (OWASP-SM-001): Αυτός ο έλεγχος περιγράφει τον τρόπο με τον οποίο θα πρέπει να γίνει η ανάλυση ενός σχήματος διαχείρισης συνόδου, με στόχο να καταλάβουμε το πώς έχει αναπτυχθεί ο μηχανισμός διαχείρισης συνόδου και εάν είναι δυνατόν κάποιος επιτιθέμενος να μπορεί να τον «σπάσει» για να παρακάμψει τη σύνοδο χρήστη. Εξηγεί το πώς να εξετάσουμε την ασφάλεια των τεκμηρίων (tokens) συνόδου, που διανέμονται στον browser του πελάτη: δηλαδή, πώς να πραγματοποιήσουμε έναν αντίστροφο μηχανισμό παραγωγής ενός cookie (cookie reverse engineering) και πώς να χειριστούμε τα cookies, έτσι ώστε να αναγκάσουμε μια «κλεμμένη» σύνοδο (hijack a session) να λειτουργήσει.
- Έλεγχος για ιδιότητες Cookies - Testing for Cookies attributes (OWASP-SM-002): Τα cookies είναι συχνά ένα βασικό διάνυσμα επίθεσης για κακόβουλους χρήστες (τυπικά, στοχεύοντας σε άλλους χρήστες) και, γι' αυτό, η εφαρμογή θα πρέπει πάντα να λάβει τα μέτρα που οφείλει, προκειμένου να προστατεύσει τα cookies. Σε αυτόν τον έλεγχο, εξετάζεται το πώς μια εφαρμογή μπορεί να λάβει τις απαραίτητες προφυλάξεις κατά την ανάθεση των cookies και το πώς να εξετάσει ότι αυτές οι ιδιότητες έχουν διαμορφωθεί σωστά.

- Έλεγχος για Προσήλωση Συνόδου - Testing for Session Fixation (OWASP-SM-003): Όταν μια εφαρμογή δεν ανανεώνει το cookie μετά από μια επιτυχή αυθεντικοποίηση χρήστη, θα μπορούσε να είναι δυνατό να βρεθεί μια ευπάθεια προσήλωσης συνόδου και να αναγκαστεί ένας χρήστης να χρησιμοποιήσει ένα cookie που ήταν γνωστό στον επιτιθέμενο.
- Έλεγχος για Εκτεθειμένες Μεταβλητές Συνόδου - Testing for Exposed Session Variables (OWASP-SM-004): Τα τεκμήρια (tokens) συνόδου αντιπροσωπεύουν εμπιστευτικές πληροφορίες διότι συνδέουν την ταυτότητα χρηστών με τη σύνοδό τους. Είναι δυνατό να εξεταστεί, εάν το τεκμήριο συνόδου εκτίθεται σε αυτήν την ευπάθεια και να δοκιμαστεί η προσπάθεια δημιουργίας μιας επίθεσης επανάληψης συνόδου.
- Έλεγχος για CSRF - Testing for CSRF (OWASP-SM-005): Η παραποίηση αιτήματος ιστοτόπου (Cross Site Request Forgery-CSRF) περιγράφει έναν τρόπο, με τον οποίο μπορούμε να αναγκάσουμε έναν χρήστη να εκτελέσει ανεπιθύμητες ενέργειες σε μια εφαρμογή ιστού, στην οποία ο ίδιος είναι ήδη αυθεντικοποιημένος, χωρίς ο ίδιος ο χρήστης να έχει γνώση της εκτέλεσης των ενεργειών αυτών. Αυτός ο έλεγχος περιγράφει το πώς να εξεταστεί μια εφαρμογή για να βρεθεί αυτό το είδος ευπάθειας.

3.2.3.3.7 Έλεγχος Επικύρωσης Δεδομένων (Data Validation Testing)

Η πιο κοινή αδυναμία ασφάλειας εφαρμογών ιστού είναι η αποτυχία κατάλληλης επικύρωσης δεδομένων (data validation), τα οποία εισάγονται από τον χρήστη ή το περιβάλλον. Αυτή η αδυναμία οδηγεί σχεδόν σε όλες τις σημαντικές ευπάθειες στις εφαρμογές ιστού, όπως cross site scripting, η έγχυση SQL (SQL injection), η έγχυση διερμηνείας (interpreter injection), οι επιθέσεις locale/Unicode, οι επιθέσεις στο σύστημα αρχείων και η υπερχείλιση ενδιάμεσης μνήμης (buffer overflows).

Τα δεδομένα από μια εξωτερική οντότητα ή έναν πελάτη (client) δεν πρέπει ποτέ να θεωρούνται έμπιστα, δεδομένου ότι μπορεί να έχουν πλαστογραφηθεί από έναν επιτιθέμενο. Στο δημοφιλές βιβλίο «Writing Secure Code» του Michael Howard, αναφέρεται ότι «Όλη η είσοδος είναι κακόβουλη» («All Input is Evil»), με την έννοια ότι πρέπει να ελέγχεται διεξοδικά. Αυτός είναι ο νούμερο ένα κανόνας. Δυστυχώς, οι σύνθετες εφαρμογές έχουν συχνά έναν μεγάλο αριθμό σημείων πρόσβασης (εισόδου), πράγμα το οποίο καθιστά εξαιρετικά δύσκολο για έναν υπεύθυνο ανάπτυξης να εφαρμόσει τον παραπάνω κανόνα. Σε αυτήν την ενότητα, περιγράφεται ο έλεγχος όλων των πιθανών φορμών επικύρωσης δεδομένων εισαγωγής, ώστε να κατανοηθεί εάν η εφαρμογή επικυρώνει επαρκώς τα δεδομένα εισαγωγής πριν τα χρησιμοποιήσει. Ο έλεγχος επικύρωσης δεδομένων περιλαμβάνει τις ακόλουθες κατηγορίες:

- Έλεγχος για Cross site scripting - Testing for Cross site scripting: Στον έλεγχο Cross Site Scripting (XSS), εξετάζεται εάν είναι δυνατό να γίνει χειρισμός των παραμέτρων εισόδου (input) της εφαρμογής έτσι ώστε να παράγει κακόβουλη έξοδο (output). Μια ευπάθεια XSS μπορεί να ευρεθεί, όταν η εφαρμογή δεν επικυρώνει την είσοδό μας και δημιουργεί μια έξοδο (αποτέλεσμα), η οποία είναι υπό τον έλεγχό μας. Αυτή η ευπάθεια οδηγεί σε διάφορες επιθέσεις, παραδείγματος χάριν, υποκλοπή εμπιστευτικών πληροφοριών (όπως cookies συνόδου (session)) ή έλεγχος του browser του θύματος. Μια επίθεση XSS παραβιάζει το ακόλουθο μοτίβο:
  Είσοδος → Έξοδος == cross-site scripting
  (Input → Output == cross-site scripting)

Σε αυτόν τον οδηγό, συμπεριλαμβάνονται οι επόμενοι τύποι ελέγχων XSS:

- Έλεγχος για Reflected Cross Site Scripting - Testing for Reflected Cross Site Scripting (OWASP-DV-001): Το Reflected Cross Site Scripting είναι ο πιο συνηθισμένος και γνωστός τύπος ευπάθειας. Αυτές οι ατέλειες (τρύπες) εμφανίζονται, όταν τα δεδομένα, που παρέχονται από κάποιο χρήστη, χρησιμοποιούνται άμεσα από scripts στην πλευρά του εξυπηρέτη, για να παρέχουν μια σελίδα αποτελεσμάτων σε αυτόν το χρήστη.
- Έλεγχος για Αποθηκευμένο Cross Site Scripting - Testing for Stored Cross Site Scripting (OWASP-DV-002): Η ευπάθεια Stored Cross Site Scripting είναι ο πιο ισχυρός τύπος XSS επιθέσεων. Η ευπάθεια Stored XSS υφίσταται όταν τα δεδομένα που παρέχονται από το χρήστη στην εφαρμογή, αποθηκεύονται πρώτα μόνιμα σε μια βάση δεδομένων, σύστημα αρχείων ή σε άλλη τοποθεσία στον εξυπηρέτη και μετά παρουσιάζονται στους χρήστες σε μια σελίδα, χωρίς να κωδικοποιούνται με τη χρήση οντοτήτων HTML.
- Έλεγχος για DOM based Cross Site Scripting - Testing for DOM based Cross Site Scripting (OWASP-DV-003): Το πρόβλημα του DOM based Cross Site Scripting (όπου το Document Object Model καθορίζει το πώς αντικείμενα όπως κείμενα, εικόνες, επικεφαλίδες, links, κλπ εμφανίζονται σε μια σελίδα ιστού), υπάρχει μέσα σε ένα script μιας σελίδας ενός πελάτη. Αν η JavaScript έχει πρόσβαση σε μια παράμετρο αίτησης URL, της οποίας ένα παράδειγμα θα ήταν μια τροφοδοσία RSS[25] και χρησιμοποιεί αυτήν την πληροφορία για να παράξει κώδικα HTML στην ίδια σελίδα και επιπλέον, αυτή η πληροφορία δεν είναι κωδικοποιημένη με τη χρήση οντοτήτων HTML, πιθανώς θα υπάρξει μια XSS ευπάθεια, αφού αυτή η πληροφορία θα επαναμεταφραστεί από τους browsers ως HTML, το οποίο θα περιλαμβάνει πρόσθετο script από την πλευρά του πελάτη.
- Έλεγχος για Cross Site Flashing - Testing for Cross Site Flashing (OWASP-DV004): Η ActionScript είναι η γλώσσα, που βασίζεται σε ECMAScript και χρησιμοποιείται από εφαρμογές Flash για την κάλυψη διαδραστικών αναγκών. Η ActionScript, όπως κάθε άλλη γλώσσα, έχει κάποια πρότυπα υλοποίησης που θα μπορούσαν να οδηγήσουν σε ζητήματα ασφάλειας. Ειδικότερα, δεδομένου ότι οι εφαρμογές Flash ενσωματώνονται συχνά σε browsers, οι ευπάθειες όπως DOM based Cross Site Scripting μπορεί να είναι παρούσες σε ελαττωματικές εφαρμογές Flash.

- Έγχυση SQL - SQL Injection (OWASP-DV-005): Στην Έγχυση SQL, εξετάζεται εάν είναι δυνατό να γίνει έγχυση δεδομένων στην εφαρμογή, έτσι ώστε να εκτελεστεί μια επερώτηση SQL (SQL query) που ελέγχεται από τον χρήστη, στην βάση δεδομένων (back-end DB). Μια ευπάθεια έγχυσης SQL μπορεί να ευρεθεί, εάν η εφαρμογή χρησιμοποιεί την είσοδο (input) του χρήστη για να δημιουργήσει επερωτήσεις χωρίς να κάνει την κατάλληλη επικύρωση εισόδου. Μια επιτυχής εκμετάλλευση αυτής της κατηγορίας ευπαθειών, επιτρέπει σε έναν μη εξουσιοδοτημένο χρήστη να έχει πρόσβαση και να χειριστεί τα δεδομένα στη βάση δεδομένων. Πρέπει να σημειωθεί ότι τα δεδομένα των εφαρμογών αντιπροσωπεύουν συχνά το πυρήνα των αγαθών

[25] Το RSS είναι ένα αρχείο σε μορφή XML, που χρησιμοποιείται με διάφορους τρόπους για διαμοιρασμό περιεχομένου και κυρίως για διαμοιρασμό επικεφαλίδων ειδήσεων στο Διαδίκτυο.

(assets) μιας επιχείρησης. Μια επίθεση έγχυσης SQL παραβιάζει το ακόλουθο μοτίβο:
Είσοδος → Επερώτηση SQL == έγχυση SQL
(Input → Query SQL == SQL injection).

Ο έλεγχος Έγχυσης SQL χωρίζεται περαιτέρω σε:

- Έλεγχος Oracle - Oracle Testing
- Έλεγχος MySQL - MySQL Testing
- Έλεγχος SQL Server - SQL Server Testing
- Έλεγχος MS Access - MS Access Testing
- Έλεγχος PostgreSQL - Testing PostgreSQL

- Έγχυση LDAP - LDAP Injection (OWASP-DV-006): Ο έλεγχος για Έγχυση LDAP είναι παρόμοιος με τον έλεγχο Έγχυσης SQL. Οι διαφορές είναι ότι χρησιμοποιούμε το πρωτόκολλο LDAP αντί για την SQL και ότι ο στόχος είναι ένας εξυπηρέτης (Server) LDAP αντί ενός SQL Server. Μια επίθεση Έγχυσης LDAP παραβιάζει το ακόλουθο μοτίβο:
Είσοδος → Επερώτηση LDAP == έγχυση LDAP
(Input → Query LDAP == LDAP injection).
- Έγχυση ORM - ORM Injection (OWASP-DV-007): Ο έλεγχος έγχυσης ORM (Object Role Modeling) είναι παρόμοιος με τον έλεγχο έγχυσης SQL. Σε αυτήν την περίπτωση, χρησιμοποιούμε Έγχυση SQL για να επιτεθούμε σε ένα μοντέλο αντικειμένων (object model) πρόσβασης δεδομένων ORM. Από την πλευρά του ελεγκτή, αυτή η επίθεση είναι ουσιαστικά ίδια με μια επίθεση Έγχυσης SQL. Εντούτοις, η ευπάθεια της έγχυσης υπάρχει σε μορφή κώδικα που παράγεται από ένα ORM εργαλείο.
- Έγχυση XML - XML Injection (OWASP-DV-008): Στον έλεγχο Έγχυσης XML, εξετάζεται εάν είναι πιθανό να γίνει έγχυση ενός συγκεκριμένου εγγράφου XML στην εφαρμογή. Μια ευπάθεια έγχυσης XML μπορεί να ευρεθεί (δηλαδή, ο έλεγχος να έχει θετικό αποτέλεσμα), εάν ο XML parser (γραμματικός αναλυτής XML) αποτύχει να κάνει κατάλληλη επικύρωση δεδομένων. Μια επίθεση έγχυσης XML παραβιάζει το ακόλουθο μοτίβο:
Είσοδος → έγγραφο XML == έγχυση XML
(Input → XML doc == XML injection).
- Έγχυση SSI - SSI Injection (OWASP-DV-009): Οι εξυπηρέτες ιστού (web servers) δίνουν συνήθως στους υπεύθυνους ανάπτυξης, τη δυνατότητα να προσθέσουν μικρά κομμάτια δυναμικού κώδικα μέσα σε στατικές σελίδες HTML, χωρίς να πρέπει να ασχοληθούν με ειδικές γλώσσες προγραμματισμού από την πλευρά του εξυπηρετητή (server-side) ή του πελάτη (client-side). Αυτό το χαρακτηριστικό γνώρισμα είναι ενσωματωμένο στην έγχυση Server-Side Includes (SSI). Στον έλεγχο έγχυσης SSI, εξετάζεται εάν είναι δυνατό να γίνει έγχυση δεδομένων στην εφαρμογή, τα οποία θα ερμηνευθούν από SSI μηχανισμούς. Μια επιτυχής εκμετάλλευση αυτής της ευπάθειας επιτρέπει σε έναν επιτιθέμενο να εγχύσει κώδικα σε σελίδες HTML ή ακόμα και να προκαλέσει απομακρυσμένη εκτέλεση κώδικα.
- Έγχυση XPath - XPath Injection (OWASP-DV-010): Η XPath είναι μια γλώσσα που έχει σχεδιαστεί και αναπτυχθεί κυρίως για να διαχειρίζεται μέρη ενός εγγράφου XML. Στον έλεγχο έγχυσης XPath, εξετάζεται εάν είναι δυνατό να γίνει έγχυση δεδομένων σε μια εφαρμογή έτσι ώστε να εκτελεί επερωτήσεις Xpath, που ελέγχονται από το χρήστη. Όταν χρησιμοποιείται επιτυχώς, αυτή η ευπάθεια μπορεί να επιτρέψει σε έναν επιτιθέμενο να

παρακάμψει τους μηχανισμούς αυθεντικοποίησης ή να έχει πρόσβαση σε πληροφορίες χωρίς κατάλληλη εξουσιοδότηση.

- Έγχυση IMAP/SMTP - IMAP/SMTP Injection (OWASP-DV-011)**:** Αυτή η απειλή έχει επιπτώσεις σε όλες τις εφαρμογές, που επικοινωνούν με εξυπηρέτες ηλεκτρονικού ταχυδρομείου (mail servers) (πρωτόκολλο IMAP/SMTP) και γενικά webmail εφαρμογές. Στον έλεγχο έγχυσης IMAP/SMTP, εξετάζεται εάν είναι πιθανό να γίνει αυθαίρετα έγχυση εντολών IMAP/SMTP σε εξυπηρέτες ηλεκτρονικού ταχυδρομείου, λόγω των δεδομένων εισόδου που δεν ελέγχονται κατάλληλα. Μια επίθεση έγχυσης IMAP/SMTP παραβιάζει το ακόλουθο μοτίβο:
  Είσοδος → εντολή IMAP/SMTP == Έγχυση IMAP/SMTP
  (Input → IMAP/SMTP command == IMAP/SMTP Injection).
- Έγχυση Κώδικα - Code Injection (OWASP-DV-012): Στον έλεγχο έγχυσης κώδικα, ελέγχεται εάν είναι δυνατή η έγχυση σε μια εφαρμογή, δεδομένων τα οποία θα εκτελεσθούν αργότερα από τον εξυπηρέτη ιστού (web server) ως εκτελέσιμες εντολές. Μια επίθεση έγχυσης κώδικα παραβιάζει το ακόλουθο μοτίβο:
  Είσοδος → κακόβουλος Κώδικας == Έγχυση Κώδικα
  (Input → malicious Code == Code Injection).
- Εντολές Λειτουργικού Συστήματος - OS (operating system) Commanding (OWASP-DV-013): Στον έλεγχο έγχυσης εντολών (command injection), προσπαθούμε να εγχύσουμε μια εντολή OS (λειτουργικού συστήματος) μέσω μιας αίτησης HTTP στην εφαρμογή. Μια επίθεση έγχυσης εντολών OS παραβιάζει το ακόλουθο μοτίβο:
  Είσοδος → Εντολή OS == Έγχυση Εντολών OS
  (Input → OS Command == OS Command Injection).
- Υπερχείλιση Προσωρινής μνήμης - Buffer overflow (OWASP-DV-014): Σε αυτούς τους ελέγχους, εξετάζουμε για διάφορους τύπους ευπάθειας υπερχείλισης προσωρινής μνήμης. Οι μέθοδοι έλεγχου για τους κοινούς τύπους ευπαθειών υπερχείλισης προσωρινής μνήμηςείναι οι εξής:
  - Heap overflow
  - Stack overflow
  - Format string.

  Γενικά η υπερχείλιση προσωρινής μνήμης παραβιάζει το ακόλουθο μοτίβο:
  Είσοδος → Σταθερό buffer ή format string == υπερχείλιση
  (Input → Fixed buffer or format string == overflow).
- Έλεγχος «κυοφορίας» ευπάθειας - Incubated vulnerability Testing (OWASP-DV-015): Ο έλεγχος «κυοφορίας» είναι ένας σύνθετος έλεγχος, που απαιτεί περισσότερες από μια ευπάθειες επικύρωσης δεδομένων, για να λειτουργήσει.
- Έλεγχος για διαχωρισμό/λαθραία εισαγωγή HTTP HTTP Splitting/Smuggling - Testing for HTTP Splitting/Smuggling (OWASP-DV-016): Περιγράφει το πώς να γίνει έλεγχος για μια εκμετάλλευση HTTP (HTTP Exploit), όπως HTTP Verb, HTTP Splitting, HTTP Smuggling. Γίνεται ανάλυση δύο διαφορετικών επιθέσεων που στοχεύουν σε συγκεκριμένες επικεφαλίδες HTTP: HTTP splitting (διαχωρισμός) και HTTP smuggling (λαθραία εισαγωγή). Η πρώτη επίθεση εκμεταλλεύεται την έλλειψη λογικής εισαγωγής δεδομένων (input), που επιτρέπει σε έναν εισβολέα να εισάγει τους χαρακτήρες CR και LF στις επικεφαλίδες της απόκρισης της εφαρμογής και να «διαχωρίσει» αυτήν την απόκριση σε δύο διαφορετικά μηνύματα HTTP. Στη δεύτερη επίθεση, ο επιτιθέμενος εκμεταλλεύεται το γεγονός ότι μερικά

ειδικά επεξεργασμένα μηνύματα HTTP μπορούν να αναλυθούν και να ερμηνευθούν με διαφορετικούς τρόπους, ανάλογα με τον πράκτορα (agent) που τα λαμβάνει. Το HTTP smuggling απαιτεί κάποιο επίπεδο γνώσης για τους διαφορετικούς πράκτορες που χειρίζονται τα μηνύματα HTTP (web server, proxy, firewall).

Τέλος, θα πρέπει να επισημανθεί ότι σε κάθε μοτίβο που παρουσιάστηκε παραπάνω, τα δεδομένα πρέπει πρώτα να επικυρωθούν από την εφαρμογή, πριν θεωρηθούν έμπιστα και υποβληθούν σε επεξεργασία. Στόχος του ελέγχου είναι να ελεγχθεί εάν η εφαρμογή εκτελεί πραγματικά την επικύρωση και ότι δεν εμπιστεύεται έτσι απλά την είσοδό της.

3.2.3.3.8 Έλεγχος Άρνησης Παροχής Υπηρεσιών (Denial of Service Testing)

Ο πιο κοινός τύπος επίθεσης άρνησης υπηρεσιών (DoS) είναι το είδος της επίθεσης που χρησιμοποιείται σε ένα δίκτυο για να καταστήσει έναν εξυπηρέτη (server) αδύνατο να χρησιμοποιηθεί από άλλους νομότυπους χρήστες. Η θεμελιώδης έννοια μιας επίθεσης DoS αφορά έναν κακόβουλο χρήστη που πλημμυρίζει με αιτήσεις ένα απλό μηχάνημα (server)-στόχο, γεγονός το οποίο καθιστά τον στόχο ανίκανο να διαχειριστεί όλο αυτόν τον όγκο των αιτήσεων που λαμβάνει. Όταν ο κακόβουλος χρήστης χρησιμοποιεί έναν μεγάλο αριθμό μηχανημάτων, προκειμένου να κατακλύζει με αιτήσεις το μηχάνημα-στόχο, αυτή η επίθεση είναι γενικά γνωστή ως κατανεμημένη επίθεση άρνησης υπηρεσιών (Distributed DoS). Αυτοί οι τύποι επιθέσεων είναι γενικά πέρα από την εμβέλεια του τι ο υπεύθυνος ανάπτυξης της εφαρμογής μπορεί να αποτρέψει δια μέσου του κώδικά του. Ο συγκεκριμένος τύπος επιθέσεων μετριάζεται καλύτερα μέσω λύσεων αρχιτεκτονικής δικτύου. Υπάρχουν, εντούτοις, τύποι ευπαθειών μέσα στις εφαρμογές που μπορούν να επιτρέψουν σε έναν κακόβουλο χρήστη να προκαλέσει τη μη διαθεσιμότητα συγκεκριμένης λειτουργικότητας στην εφαρμογή, ή μερικές φορές να καταστήσει μη διαθέσιμο ολόκληρο τον ιστότοπο. Αυτά τα προβλήματα προκαλούνται από τα σφάλματα (bugs) των εφαρμογών, τα οποία συχνά ενεργοποιούνται ως αποτέλεσμα της κακόβουλης ή απροσδόκητης εισαγωγής δεδομένων από τους χρήστες. Αυτή η ενότητα θα εστιάσει στις επιθέσεις επιπέδου εφαρμογής ενάντια στη διαθεσιμότητα, η οποία μπορεί να προωθηθεί από έναν κακόβουλο χρήστη σε ένα απλό μηχάνημα. Οι έλεγχοι DoS, είναι οι ακόλουθοι:

- Έλεγχος για Επιθέσεις Μεταχαρακτήρων SQL - Testing for SQL Wildcard Attacks (OWASP-DS-001): Οι επιθέσεις Μεταχαρακτήρων SQL αναφέρονται στον εξαναγκασμό της υποκείμενης βάσης δεδομένων ώστε να πραγματοποιήσει επερωτήσεις, χρησιμοποιώντας διάφορους μεταχαρακτήρες (%, _), κάτι που μπορεί να έχει ως αποτέλεσμα την επεξεργασία τεράστιου όγκου δεδομένων. Αυτή η ευπάθεια γενικά υπάρχει σε λειτουργίες αναζήτησης των εφαρμογών ιστού.
- Κλείδωμα των λογαριασμών χρηστών - Locking Customer Accounts (OWASP-DS-002): Σε αυτόν τον έλεγχο ο ελεγκτής εξετάζει, εάν ένας επιτιθέμενος μπορεί να κλειδώσει τους λογαριασμούς νόμιμων χρηστών, κάνοντας διαδοχικές προσπάθειες σύνδεσης στην εφαρμογή με λανθασμένο κωδικό πρόσβασης.
- Υπερχειλίσεις ενδιάμεσης μνήμης - Buffer Overflows (OWASP-DS-003): Σε αυτόν τον έλεγχο εξετάζουμε εάν είναι δυνατό να προκαλέσουμε μια κατάσταση άρνησης υπηρεσιών με την υπερχείλιση μιας ή περισσοτέρων δομών δεδομένων στην υπό έλεγχο εφαρμογή.

- Κατανομή Αντικειμένου που προσδιορίζεται από το Χρήστη - User Specified Object Allocation (OWASP-DS-004): Σε αυτόν τον έλεγχο εξετάζουμε, εάν είναι δυνατό να εξαντλήσουμε τους πόρους του εξυπηρέτη (server) με το να αποθηκεύσουμε μεγάλο αριθμό αντικειμένων.
- Καθορισμός Μετρητή Βρόχου από το Χρήστη - User Input as a Loop Counter (OWASP-DS-005): Σε αυτόν τον έλεγχο εξετάζουμε, εάν είναι δυνατό να εξαναγκάσουμε την εφαρμογή να εκτελέσει εντός βρόχου ένα τμήμα κώδικα, που απαιτεί αρκετούς υπολογιστικούς πόρους, με σκοπό να μειώσουμε τη συνολική απόδοση του συστήματος.
- Εγγραφή Δεδομένων Χρήστη στο Δίσκο - Writing User Provided Data to Disk (OWASP-DS-006): Σε αυτόν τον έλεγχο εξετάζουμε, εάν είναι δυνατό να προκληθεί μια κατάσταση άρνησης υπηρεσιών, με την κατανάλωση του αποθηκευτικού χώρου των δίσκων του συστήματος από δεδομένα καταγραφής (log data).
- Αποτυχία Αποδέσμευσης Πόρων - Failure to Release Resources (OWASP-DS-007): Σε αυτόν τον έλεγχο εξετάζουμε, εάν η εφαρμογή αποδεσμεύει κανονικά τους πόρους, (δηλαδή αρχεία ή και μνήμη) που είχε δεσμεύσει για τη διεκπεραίωση διαφόρων αιτημάτων.
- Αποθήκευση Υπερβολικά Πολλών Δεδομένων σε Αντικείμενο Συνόδου - Storing too Much Data in Session (OWASP-DS-008): Σε αυτόν τον έλεγχο εξετάζουμε, εάν είναι δυνατό να αποθηκεύσουμε μεγάλο αριθμό δεδομένων σε ένα αντικείμενο συνόδου χρήστη, με σκοπό να εξαντλήσουμε τους πόρους μνήμης του εξυπηρέτη (server).

3.2.3.3.9 Έλεγχος Υπηρεσιών Ιστού (Web Services Testing)

Οι εφαρμογές υπηρεσιών ιστού / SOA (Αρχιτεκτονική Προσανατολισμένη στις Υπηρεσίες-Service Orientated Architecture), είναι ανερχόμενα συστήματα που δίνουν τη δυνατότητα στις επιχειρήσεις να διαλειτουργούν μεταξύ τους και αναπτύσσονται με πρωτοφανή τρόπο. Οι πελάτες (clients) των υπηρεσιών ιστού γενικά δεν είναι απλοί χρήστες εφαρμογών αλλά backend servers. Οι υπηρεσίες ιστού εκτίθενται στο δίκτυο όπως οποιαδήποτε άλλη υπηρεσία, αλλά μπορούν να χρησιμοποιηθούν με τα HTTP, FTP, SMTP, MQ μεταξύ άλλων πρωτοκόλλων μεταφοράς. Το πλαίσιο υπηρεσιών ιστού χρησιμοποιεί το πρωτόκολλο HTTP (ως τυποποιημένη εφαρμογή ιστού) μαζί με τις τεχνολογίες XML, SOAP[26], WSDL[27] και UDDI[28]. Οι ευπάθειες στις υπηρεσίες ιστού είναι παρόμοιες με άλλες ευπάθειες, όπως η έγχυση SQL, η κοινοποίηση πληροφοριών και διαρροή, αλλά περιλαμβάνουν επίσης και ευπάθειες XML. Οι υπηρεσίες ιστού που εξετάζονται είναι οι ακόλουθες:

- Συλλογή πληροφοριών WS - WS Information Gathering (OWASP-WS-001): Το πρώτο βήμα για να εκτελεστεί ένας έλεγχος υπηρεσίας ιστού (Web Service-WS) είναι να καθοριστούν τα σημεία εισόδων της WS και το σχήμα επικοινωνίας: αυτό περιγράφεται στο WSDL που συνδέεται με τη WS.

[26] Το SOAP (Πρωτόκολλο Απλής Πρόσβασης Αντικειμένου- Simple Object Access Protocol) παρέχει τα μέσα για την επικοινωνία μεταξύ των εφαρμογών υπηρεσιών ιστού και πελατών με XML και HTTP.

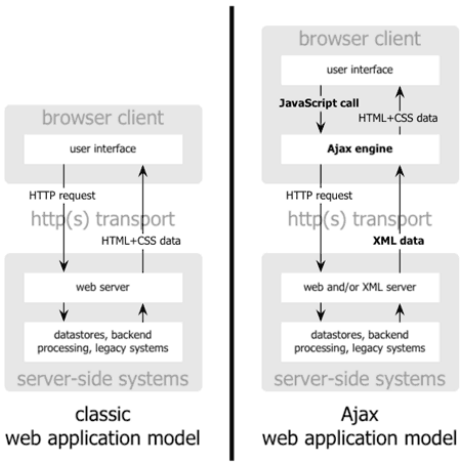
[27] Το WSDL (Γλώσσα Περιγραφής Υπηρεσιών Ιστού-Web Services Description Language) χρησιμοποιείται για να περιγράψει τις διεπαφές μιας υπηρεσίας.

[28] Το UDDI (Καθολική Περιγραφή, Ανακάλυψη και Ολοκλήρωση -Universal Description, Discovery and Integration) χρησιμοποιείται για καταχωρήσει και να δημοσιεύσει πληροφορίες για υπηρεσίες ιστού, καθώς και τα χαρακτηριστικά τους, έτσι ώστε να μπορούν να βρεθούν από πιθανούς πελάτες.

- Έλεγχος WSDL - Testing WSDL (OWASP-WS-002): Μόλις προσδιοριστεί το WSDL, μπορούμε να εξετάσουμε αυτό το σημείο εισόδου.
- Δομικός Έλεγχος XML - XML Structural Testing (OWASP-WS-003): Κάθε μήνυμα ή αρχείο σε γλώσσα XML (Extensible Markup Language), για να χρησιμοποιηθεί χωρίς πρόβλημα θα πρέπει να είναι καλά δομημένο, αλλιώς θα υπάρξει πρόβλημα, όταν θα περάσει από το μεταφραστή στην πλευρά του server. Ο μεταφραστής διατρέχει το μήνυμα με σειριακό τρόπο και ελέγχει τη σωστή δομή του.
- Έλεγχος επιπέδου περιεχομένου της XML - XML Content-level Testing (OWASP-WS-004): Οι επιθέσεις επιπέδου περιεχομένου της XML (XML Content Level) έχουν ως στόχο τον εξυπηρέτη (server), που προσφέρει μια υπηρεσία ιστού και κάθε εφαρμογή, η οποία χρησιμοποιείται από την υπηρεσία αυτή συμπεριλαμβανομένων άλλων servers, όπως ιστού, βάσεων δεδομένων, εφαρμογών, λειτουργικά συστήματα κ.λπ.
- Έλεγχος παραμέτρων HTTP GET/REST - HTTP GET parameters/REST Testing (OWASP-WS-005): Πολλές εφαρμογές XML καλούνται με μεταβίβαση σε αυτές παραμέτρων μέσω αιτήσεων HTTP GET. Αυτές είναι γνωστές ως «REST-style» υπηρεσίες ιστού (REST-Representational State Transfer) και μπορεί να γίνουν στόχοι επίθεσης, διαβιβάζοντας κακόβουλο περιεχόμενο στο HTTP GET string (π.χ. υπερβολικά μεγάλες παράμετροι – π.χ. 2048 χαρακτήρες- δηλώσεις ή έγχυση SQL, κ.λπ.).
- Κακόβουλα συνημμένα σε μηνύματα SOAP - Naughty SOAP attachments (OWASP-WS-006): Αυτός ο έλεγχος αναφέρεται σε διανύσματα επιθέσεων (attack vectors) προς υπηρεσίες που επιδέχονται συνημμένα σε μηνύματα SOAP (SOAP attachments). Ο κίνδυνος παρουσιάζεται στην επεξεργασία του συνημμένου από το εξυπηρέτη (server), καθώς και στη διανομή του αρχείου στους πελάτες.
- Έλεγχος Αναπαραγωγής - Replay Testing (OWASP-WS-007): Ο έλεγχος αναπαραγωγής είναι ένας έλεγχος για την ύπαρξη της ευπάθειας επανάληψης σε μια υπηρεσία ιστού. Ο επιτιθέμενος μπορεί να προσποιηθεί ένα νόμιμο χρήστη και να πραγματοποιήσει κακόβουλες ενέργειες χωρίς να ελεγχθεί.

3.2.3.3.10 Έλεγχος Ajax (Ajax Testing)

Η AJAX (Ασύγχρονο JavaScript και XML- Asynchronous JavaScript and XML) είναι μια τεχνική ανάπτυξης ιστού που χρησιμοποιείται για να δημιουργήσει περισσότερο αποκριτικές (responsive) εφαρμογές ιστού. Χρησιμοποιεί έναν συνδυασμό τεχνολογιών προκειμένου να αποκτηθεί εμπειρία που θα μοιάζει περισσότερο με τη χρησιμοποίηση μιας desktop εφαρμογής. Ολοκληρώνεται με τη χρησιμοποίηση του XMLHttpRequest αντικειμένου και της JavaScript για να υποβάλει ασύγχρονες αιτήσεις στον εξυπηρέτη ιστού (web server), αναλύοντας τις αποκρίσεις και έπειτα ενημερώνοντας το DOM της σελίδας HTML όπως και το CSS. Η χρησιμοποίηση τεχνικών AJAX μπορεί να έχει



Σχήμα 19. Μοντέλο κλασσικών εφαρμογών ιστού και εφαρμογών ιστού μορφής Ajax.

τεράστια οφέλη χρησιμότητας για τις εφαρμογές ιστού. Εντούτοις, από την πλευρά της ασφάλειας, οι εφαρμογές AJAX έχουν μια μεγαλύτερη επιφάνεια επίθεσης από τις κανονικές εφαρμογές ιστού και αναπτύσσονται συχνά εστιάζοντας σε αυτό που μπορεί να *γίνει* και όχι σε αυτό που θα *έπρεπε να γίνει*. Οι εφαρμογές AJAX είναι τρωτές σε αρκετές παραδοσιακές ευπάθειες εφαρμογών ιστού. Οι έλεγχοι που πραγματοποιούνται είναι οι ακόλουθοι:

- Ευπάθειες AJAX - AJAX Vulnerabilities (OWASP-AJ-001): Δεδομένου ότι η AJAX είναι σχετικά νέα τεχνολογία, υπάρχουν πολλά ζητήματα ασφάλειας που δεν έχουν ακόμη ερευνηθεί, όπως:
  - Αυξημένη επιφάνεια επίθεσης (attack surface) με πολλές περισσότερες εισαγωγές δεδομένων που πρέπει να εξασφαλισθούν.
  - Εκτεθειμένες εσωτερικές λειτουργίες της εφαρμογής.
  - Πρόσβαση πελατών σε πόρους τρίτων οντοτήτων χωρίς ενσωματωμένη ασφάλεια και μηχανισμούς κωδικοποίησης.
  - Αποτυχία να προστατευθεί η πιστοποίηση των πληροφοριών και των συνόδων.
  - Ανεπαρκής διαχωρισμός μεταξύ του client-side και server-side κώδικα, με συνέπεια λάθη ασφάλειας.
- Πώς γίνεται ο έλεγχος AJAX - How to test AJAX (OWASP-AJ-002): Επειδή οι περισσότερες επιθέσεις ενάντια σε εφαρμογές AJAX είναι ανάλογες με τις επιθέσεις ενάντια στις παραδοσιακές εφαρμογές ιστού, οι ελεγκτές πρέπει να αναφερθούν σε άλλα τμήματα του οδηγού ελέγχου για να αναζητήσουν συγκεκριμένους χειρισμούς παραμέτρων που θα χρησιμοποιηθούν προκειμένου να ανακαλυφθούν οι ευπάθειες. Η πρόκληση με τις εφαρμογές AJAX είναι το να ευρεθούν τα σημεία τέλους (endpoints) όπου είναι οι στόχοι για τις ασύγχρονες κλήσεις και έπειτα να καθοριστεί το κατάλληλο σχήμα (format) για τις αιτήσεις.

3.2.3.4 Εκθέσεις (Reports): εκτίμηση του πραγματικού κινδύνου

Αυτή η ενότητα περιγράφει το πώς να εκτιμηθεί ο πραγματικός κίνδυνο ως αποτέλεσμα μιας αξιολόγησης της ασφάλειας. Η ιδέα είναι να δημιουργηθεί μια γενική μεθοδολογία ώστε να διαχωρίσει τα συμπεράσματα ασφάλειας και να αξιολογήσει τους κινδύνους, με το στόχο να τους διαχειριστεί. Παρουσιάζεται ένας πίνακας που μπορεί εύκολα να αντιπροσωπεύσει ένα στιγμιότυπο της αξιολόγησης. Αυτός ο πίνακας αντιπροσωπεύει τις τεχνικές πληροφορίες που παραδίδονται στον πελάτη. Στη συνέχεια, είναι σημαντικό να παρουσιαστεί μια εκτενής περίληψη για τη διαχείριση.

*3.2.3.4.1 **Πώς γίνεται η εκτίμηση του πραγματικού κινδύνου***

Η Μεθοδολογία Εκτίμησης Κινδύνου του OWASP - The OWASP Risk Rating Methodology: Έχοντας ένα σύστημα σε ισχύ για την εκτίμηση του κινδύνου, θα κερδίσουμε και θα χρόνο και θα εξοικονομήσουμε πόρους, καταγράφοντας τις προτεραιότητες των κινδύνων. Ένα τέτοιο σύστημα θα βοηθήσει να εξασφαλισθεί ότι δεν αποπροσανατολιζόμαστε από δευτερεύοντες κινδύνους, αγνοώντας τους σοβαρότερους κινδύνους οι οποίοι γίνονται λιγότερο κατανοητοί. Ιδανικά, θα υπήρχε ένα καθολικό σύστημα εκτίμησης κινδύνου που θα εκτιμούσε ακριβώς όλους τους κινδύνους για ολόκληρο τον οργανισμό. Όμως, μια ευπάθεια που είναι κρίσιμη για έναν οργανισμό μπορεί να μην είναι πολύ σημαντική για έναν άλλο. Στη συνέχεια

παρουσιάζεται ένα βασικό πλαίσιο που θα μπορούσε να προσαρμοστεί σε έναν οργανισμό.

Προσέγγιση: Υπάρχουν πολλές διαφορετικές προσεγγίσεις για την ανάλυση κινδύνου. Η προσέγγιση του OWASP βασίζεται σε κάποιες τυποποιημένες μεθοδολογίες και προσαρμόζεται για την ασφάλεια εφαρμογών. Το τυποποιημένο μοντέλο κινδύνου που χρησιμοποιείται, είναι το εξής:

Κίνδυνος = Πιθανότητα * Επίπτωση (Risk = Likelihood * Impact)

Στη συνέχεια, διαχωρίζονται οι παράγοντες που αποτελούν την «πιθανότητα» και «επίπτωση» για την ασφάλεια εφαρμογών και φαίνεται το πώς πρέπει να συνδυαστούν για να καθορίσουν τη γενική σοβαρότητα για τον κίνδυνο.

1. Ταυτοποίηση ενός Κινδύνου (Βήμα 1): Το πρώτο βήμα είναι να ταυτοποιηθεί ένας κίνδυνος ασφάλειας, που πρέπει να εκτιμηθεί. Θα πρέπει να συγκεντρωθούν πληροφορίες: για τον πράκτορα (agent) απειλής που εμπλέκεται, για την επίθεση που χρησιμοποιεί, για την ευπάθεια που εμπλέκεται και την επίπτωση μιας επιτυχούς εκμετάλλευσής (exploit) της στην επιχείρησή μας. Μπορεί να υπάρξουν πολλαπλές πιθανές ομάδες επιτιθεμένων, ή ακόμα και πολλαπλές πιθανές επιπτώσεις στην επιχείρηση. Γενικά, είναι καλύτερο να γίνονται σφάλματα χρησιμοποιώντας την επιλογή της χειρότερης περίπτωσης (worst-case), αφού αυτό θα οδηγήσει στον υψηλότερο γενικό κίνδυνο.
2. Παράγοντες για τον Υπολογισμό της Πιθανότητας (Βήμα 2): Μόλις ταυτοποιηθεί ένας πιθανός κίνδυνος και θέλουμε να υπολογίσουμε το πόσο σοβαρός είναι, το πρώτο βήμα είναι να υπολογιστεί η «πιθανότητα». Γενικά, ο προσδιορισμός, για το εάν η πιθανότητα είναι χαμηλή (low), μεσαία (medium) ή υψηλή (high), είναι αρκετά ικανοποιητικός. Πρέπει να επισημανθεί ότι κάθε παράγοντας έχει ένα σύνολο επιλογών και κάθε επιλογή έχει μια εκτίμηση πιθανότητας από 0 έως 9, με την οποία συνδέεται. Οι αριθμοί αυτοί θα χρησιμοποιηθούν, για να υπολογίσουμε αργότερα τη γενική πιθανότητα.
    - Παράγοντες Πράκτορα Απειλής (Threat Agent Factors): Στόχος είναι να υπολογιστεί η πιθανότητα μιας επιτυχούς επίθεσης από αυτήν την ομάδα επιτιθεμένων. Χρησιμοποιούμε τον πράκτορα απειλής της χειρότερης περίπτωσης.
        - Επίπεδο ικανότητας - Skill level (0-9)
        - Κίνητρο - Motive (0-9)
        - Ευκαιρία - Opportunity (0-9)
        - Μέγεθος - Size (0-9)
    - Παράγοντες Ευπάθειας (Vulnerability Factors): Στόχος είναι να υπολογιστεί η πιθανότητα της συγκεκριμένης ευπάθειας σχετικά με την ανακάλυψη και εκμετάλλευσή της. Θεωρούμε τον πράκτορα απειλής που επιλέχθηκε παραπάνω.
        - Ευκολία ανακάλυψης - Ease of discovery (0-9)
        - Ευκολία εκμετάλλευσης - Ease of exploit (0-9)
        - Συνειδητοποίηση - Awareness (0-9)
        - Ανίχνευση εισβολής - Intrusion detection (0-9)

3. Βήμα 3 - Παράγοντες για τον Υπολογισμό των Επιχειρησιακών Επιπτώσεων: Κατά την εξέταση των επιπτώσεων μιας επιτυχούς επίθεσης, είναι σημαντικό να συνειδητοποιηθεί ότι υπάρχουν δύο είδη επιπτώσεων. Το πρώτο είδος είναι οι «τεχνικές επιπτώσεις» στην εφαρμογή, τα δεδομένα που χρησιμοποιεί και οι λειτουργίες που παρέχει. Το δεύτερο είδος είναι οι «επιχειρησιακές επιπτώσεις» στην επιχείρηση που λειτουργεί την εφαρμογή. Τελικά, οι επιχειρησιακές επιπτώσεις είναι σημαντικότερες. Και εδώ, πρέπει να επισημανθεί ότι κάθε παράγοντας έχει ένα σύνολο επιλογών και κάθε επιλογή έχει μια εκτίμηση επίπτωσης από 0 έως 9, με την οποία συνδέεται. Οι αριθμοί αυτοί θα χρησιμοποιηθούν, για να υπολογίσουμε αργότερα τη γενική επίπτωση.

    - Παράγοντες Τεχνικών Επιπτώσεων (Technical Impact Factors): Στόχος είναι να υπολογισθεί το μέγεθος της επίπτωσης στο σύστημα εάν η ευπάθεια επρόκειτο να χρησιμοποιηθεί.
        - Απώλεια εμπιστευτικότητας - Loss of confidentiality (0-9)
        - Απώλεια ακεραιότητας - Loss of integrity (0-9)
        - Απώλεια διαθεσιμότητας - Loss of availability (0-9)
        - Απώλεια υπευθυνότητας - Loss of accountability (0-9)
    - Παράγοντες Επιχειρησιακών Επιπτώσεων (Business Impact Factors): Οι επιχειρησιακές επιπτώσεις προέρχονται από τις τεχνικές επιπτώσεις, αλλά απαιτούν επιπρίσθετα μια επαρκή κατανόηση για το τι είναι σημαντικό για την επιχείρηση που «τρέχει» την εφαρμογή. Οι παρακάτω παράγοντες είναι κοινές περιοχές για πολλές επιχειρήσεις, αλλά η συγκεκριμένη περιοχή είναι περισσότερο σημαντική σε μια επιχείρηση από τους παράγοντες που σχετίζονται με τον πράκτορα απειλής, την ευπάθεια και τις τεχνικές επιπτώσεις.
        - Οικονομική ζημία - Financial damage (0-9)
        - Ζημία φήμης - Reputation damage (0-9)
        - Μη συμμόρφωση - Non-compliance (0-9)
        - Παραβίαση ιδιωτικότητας - Privacy violation (0-9)

4. Βήμα 4 - Καθορισμός της Σοβαρότητας του Κινδύνου: Σε αυτό το βήμα πρόκειται να χρησιμοποιήσουμε μαζί την εκτίμηση πιθανότητας και την εκτίμηση επίπτωσης για να υπολογίσουμε μια γενική σοβαρότητα (severity) για αυτόν τον κίνδυνο. Πρέπει να υπολογιστεί, λοιπόν, εάν η πιθανότητα είναι χαμηλή-low (0 έως < 3), μεσαία-medium (3 έως < 6) ή υψηλή-high (6 έως 9) και να γίνει έπειτα το ίδιο πράγμα για την επίπτωση. Η κλίμακα από 0 έως 9, χωρίζεται σε τρία μέρη.

   Παρακάτω παραθέτουμε ένα παράδειγμα:

Threat agent factors				**Vulnerability factors**			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Πίνακας 7. Παράγοντες πράκτορα απειλής και ευπάθειας. Ο μέσος όρος των αποτελεσμάτων υπολογίζει τη συνολική πιθανότητα.

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Πίνακας 8. Παράγοντες τεχνικών και επιχειρησιακών επιπτώσεων. Ο μέσος όρος των αποτελεσμάτων υπολογίζει τη συνολική επίπτωση.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Πίνακας 9. Καθορισμός συνολικής σοβαρότητας.

Στο παράδειγμα, η πιθανότητα είναι μεσαία και οι τεχνικές επιπτώσεις είναι υψηλές, έτσι από μια καθαρά τεχνική προοπτική, φαίνεται ότι η γενική σοβαρότητα είναι υψηλή. Εντούτοις, οι επιχειρησιακές επιπτώσεις είναι πραγματικά χαμηλές, έτσι η συνολική σοβαρότητα είναι επίσης χαμηλή.

5. Βήμα 5 - Απόφαση για το Τι να Διορθωθεί: Αφού έχουμε ταξινομήσει τους κινδύνους για την εφαρμογή μας, έχουμε πλέον μια λίστα προτεραιότητας σχετικά με το τι θα πρέπει να διορθωθεί. Κατά γενικό κανόνα, πρέπει να διορθωθούν πρώτα οι πιο σοβαρή κίνδυνοι. Δε βοηθά το γενικό προφίλ (profile) του κινδύνου μια επιχείρησης, το να γίνει διόρθωση των λιγότερο σημαντικών κινδύνων, ακόμα κι αν είναι εύκολο ή φθηνό να αντιμετωπιστούν.

6. Βήμα 6 - Προσαρμογή του Μοντέλου Εκτίμησης Κινδύνου: Ένα προσαρμοσμένο μοντέλο είναι πιθανότερο να παράγει αποτελέσματα που ταιριάζουν με τις αντιλήψεις των περισσοτέρων σχετικά με το τι θεωρείται σοβαρός κίνδυνος. Υπάρχουν διάφοροι τρόποι για να προσαρμοστεί αυτό το μοντέλο για έναν οργανισμό.

    - Προσθήκη παραγόντων: Μπορεί να γίνει επιλογή διαφορετικών παραγόντων, οι οποίοι αντιπροσωπεύουν καλύτερα το τι είναι σημαντικό για τον οργανισμό.
    - Προσαρμογή επιλογών: Υπάρχουν μερικές επιλογές δειγμάτων που συνδέονται με κάθε παράγοντα, αλλά το μοντέλο θα είναι αποτελεσματικότερο εάν γίνει προσαρμογή αυτών των επιλογών στην επιχείρηση.
    - Στάθμιση παραγόντων: Μπορεί να γίνει στάθμιση των παραγόντων ώστε να δοθεί έμφαση στους παράγοντες που είναι σημαντικότεροι για την επιχείρηση. Αυτό καθιστά το μοντέλο λίγο πιο σύνθετο, δεδομένου ότι θα πρέπει να χρησιμοποιηθεί ένας σταθμισμένος μέσος όρος.

3.2.3.4.2 Τρόπος συγγραφής της έκθεσης ελέγχου

Η εκτέλεση της τεχνικής πλευράς της αξιολόγησης είναι μόνο η μισή από τη συνολική διαδικασία της αξιολόγησης. Το τελικό προϊόν είναι η παραγωγή μιας καλά

γραμμένης και πληροφοριακής έκθεσης. Η έκθεση πρέπει να είναι εύκολο να κατανοηθεί και να δίνει έμφαση σε όλους τους κινδύνους που εντοπίζονται κατά τη διάρκεια της φάσης της αξιολόγησης, καθώς και να απευθύνεται και στο προσωπικό διαχείρισης αλλά και στο τεχνικό προσωπικό. Τα τμήματα που συστήνονται είναι τα εξής:

- Επιτελική Σύνοψη (Executive Summary): Η επιτελική σύνοψη παραθέτει τα γενικά συμπεράσματα της αξιολόγησης και δίνει στους διευθυντές ή ιδιοκτήτες συστημάτων, μια ιδέα του γενικού κινδύνου που αντιμετωπίζουν.
- Επισκόπηση Τεχνικής Διαχείρισης (Technical Management Overview): Αυτό το τμήμα απευθύνεται στους τεχνικούς διευθυντές που απαιτούν περισσότερες τεχνικές λεπτομέρειες από αυτές που παρατέθηκαν στην επιτελική σύνοψη. Αυτό το τμήμα θα πρέπει να περιλαμβάνει λεπτομέρειες για την εμβέλεια της αξιολόγησης, τους στόχους που συμπεριλαμβάνονται και οποιεσδήποτε προειδοποιήσεις, όπως διαθεσιμότητα συστήματος κ.λπ.
- Συμπεράσματα Αξιολόγησης (Assessment Findings): Αυτό το τμήμα περιλαμβάνει τεχνικές λεπτομέρειες σχετικά με τις ευπάθειες που εντοπίζονται και τις προσεγγίσεις που απαιτούνται, για να εξασφαλισθεί ότι επιλύονται.
- Εργαλεία (Toolbox): Αυτό το τμήμα χρησιμοποιείται για να περιγράψει εμπορικά εργαλεία και εργαλεία ανοικτού κώδικα, που χρησιμοποιήθηκαν στη διενέργεια της αξιολόγησης.

3.2.4 Εργαλεία για την υποστήριξη της μεθοδολογίας

3.2.4.1 Εργαλεία του OWASP

3.2.4.1.1 JbroFuzz

"Εάν δεν μπορούμε να κάνουμε fuzz με το JBroFuzz, τότε πιθανώς δεν θέλουμε να κάνουμε fuzz!" Παλαιό Ρητό για το JBroFuzz

3.2.4.1.1.1 Γενικά

Το JBroFuzz είναι ένας fuzzer διαδικτυακών εφαρμογών για αιτήσεις (requests) που υποβάλλονται μέσω HTTP ή HTTPS. Ο σκοπός του είναι να παραχθεί μια ενιαία, φορητή εφαρμογή που προσφέρει σταθερές ικανότητες fuzzing[29] πρωτοκόλλου ιστού. Το JBroFuzz παράγει αιτήσεις, τις αποστέλλει και καταγράφει τις αντίστοιχες αποκρίσεις (responses) που λαμβάνονται. Δεν προσπαθεί να προσδιορίσει εάν ένα συγκεκριμένο site είναι τρωτό ή όχι, αυτό απαιτεί περαιτέρω ανάλυση. Εντούτοις, ορισμένα δεδομένα-ωφέλιμα φορτία (payloads) που περιλαμβάνονται στους fuzzers και που μπορούν να χρησιμοποιηθούν για να παράγουν αιτήσεις (π.χ. XSS), επεξεργάζονται για να προσπαθήσουν να εκμεταλλευτούν επιτυχώς ατέλειες. Τέτοιες ατέλειες αντιπροσωπεύουν τις γνωστές ευπάθειες των εφαρμογών ιστού. Το JBroFuzz

[29] Το Web Fuzzing σε ελεύθερη μετάφραση σημαίνει «χνουδιάζω τον ιστό» και απέχει πολύ από το χνούδιασμα του βαμβακιού. Το Web Fuzzing είναι ένας από τους πλέον αποτελεσματικούς τρόπους ανακάλυψης bugs που προκαλούν DoS attacks κυρίως, XSS αλλά και SQL Injections. Ο έλεγχος Fuzz ή fuzzing είναι μια τεχνική ελέγχου λογισμικού που παρέχει τυχαία δεδομένα ("fuzz") ως είσοδο σε κάποιο πρόγραμμα. Εάν το πρόγραμμα αποτύχει (π.χ. αποτύχουν οι (assertions) που έχουν ενσωματωθεί στον κώδικα), τότε οι ατέλειες μπορούν να καταγραφούν.

ομαδοποιεί τους fuzzers με τα αντίστοιχα ωφέλιμα φορτία (payload) τους σε διάφορες κατηγορίες, ανάλογα με τις γνωστές ευπάθειες. Κατά συνέπεια, ο αναλυτής θα πρέπει να επιλέξει τους fuzzers που θα χρησιμοποιήσει, προκειμένου να εξετάσει για ένα συγκεκριμένο σύνολο ευπαθειών και να επισκοπήσει τα αποτελέσματα προκειμένου να αναγνωρίσει εάν η εκμετάλλευση πέτυχε ή όχι.

3.2.4.1.1.2 Χαρακτηριστικά

Τα συστατικά του JBroFuzz παρουσιάζονται σε καρτέλες (tabs), με περισσότερες επιλογές (κωδικοποιήσεις, hash calculator, επικεφαλίδες (headers) από δημοφιλείς browsers) που είναι διαθέσιμες στην επιλογή «Εργαλεία-Tools». Τα βασικά συστατικά είναι:

- **Fuzzing:** Η καρτέλα fuzzing είναι η κύρια καρτέλα του JBroFuzz και είναι αρμόδια για όλες τις λειτουργίες fuzzing που εκτελούνται στο δίκτυο. Ανάλογα με τα δεδομένα-ωφέλιμα φορτία (payloads) του fuzzer που επιλέγονται, δημιουργεί μη καλά δομημένα δεδομένα για κάθε αίτηση, τα στέλνει και γράφει την απόκριση σε ένα αρχείο.
- **Graphing:** Η καρτέλα graphing είναι αρμόδια για να δώσει με γραφική παράσταση (σε ποικίλες μορφές) τις αποκρίσεις που λαμβάνονται από το fuzzing. Αυτή η καρτέλα μπορεί να προσφέρει μια σαφή ένδειξη μιας απόκρισης που όταν λαμβάνεται είναι διαφορετική - αυτή η ένδειξη απαιτεί περαιτέρω εξέταση.
- **Payloads:** Η καρτέλα payloads είναι μια συλλογή από fuzzers με τα αντίστοιχα δεδομένα-ωφέλιμα φορτία (payloads) τους, που μπορούν να χρησιμοποιηθούν στο fuzzing. Τα payloads προστίθενται στην αίτηση στην καρτέλα fuzzing. Μια σαφέστερη εικόνα για το ποια payloads είναι διαθέσιμα, πώς ομαδοποιούνται και ποιες ιδιότητες έχει κάθε fuzzer, μπορούν να φανούν σε αυτήν την καρτέλα.
- **Headers:** Το παράθυρο headers είναι μια συλλογή επικεφαλίδων browser που μπορεί να χρησιμοποιηθούν κατά το fuzzing. Οι επικεφαλίδες λαμβάνονται από διαφορετικούς browsers σε διαφορετικές πλατφόρμες και λειτουργικά συστήματα. Αυτή η καρτέλα παρέχεται, όπως και πολλές εφαρμογές ιστού αποκρίνονται διαφορετικά σε διαφορετικές επιθέσεις προσωποποίησης browser.
- **System:** Η καρτέλα system αντιπροσωπεύει την κονσόλα καταγραφής (logging) του JBroFuzz στο χρόνο εκτέλεσης. Επιτρέπει την πρόσβαση σε πληροφορίες χρόνου εκτέλεσης Java, την εμφάνιση οποιονδήποτε σφαλμάτων που μπορεί να συμβούν και την πορεία της λειτουργίας σχετικά με τα γεγονότα που καταγράφονται.

3.2.4.1.2 DirBuster

3.2.4.1.2.1 Γενικά

Το DirBuster είναι μια πολύ-νηματική εφαρμογή java που σχεδιάστηκε για να δοκιμάζει εξαντλητικά (brute force) ονόματα καταλόγων και αρχείων σε εξυπηρέτες ιστού /εφαρμογών. Συχνά συμβαίνει η περίπτωση όπου ένας εξυπηρέτης Web που αρχικά φαίνεται να απλώς να έχει εγκατασταθεί, στην πραγματικότητα φιλοξενεί σελίδες και εφαρμογές που δεν είναι άμεσα ορατές. Το DirBuster προσπαθεί να τις ανιχνεύσει.

Τα εργαλεία ανίχνευσης συνήθως συνοδεύονται με μία λίστα καταλόγων και αρχείων τα οποία προσπαθούν να εντοπίσουν, και είναι αποτελεσματικά μόνο για αντικείμενα που περιλαμβάνονται στη λίστα αυτή. Το DirBuster ακολούθησε μία διαφορετική προσέγγιση όμως για την παραγωγή της λίστας αυτής: Η λίστα παράχθηκε από την αρχή, ανιχνεύοντας το Διαδίκτυο και συλλέγοντας τους καταλόγους και τα αρχεία που χρησιμοποιούνται πραγματικά από τους υπεύθυνους ανάπτυξης! Το DirBuster είναι εφοδιασμένο με συνολικά 9 διαφορετικές λίστες, οπότε θεωρείται εξαιρετικά αποτελεσματικό στην εύρεση αυτών των κρυμμένων αρχείων και καταλόγων. Έχει επίσης την επιλογή να εκτελεί έναν καθαρά εξαντλητικό έλεγχος (ωμής βίας-brute force), ο οποίος εντοπίζει οποιονδήποτε κρυμμένο κατάλογο ή αρχείο. Επομένως, το DirBuster προσπαθεί να βρει κρυμμένες σελίδες/ καταλόγους και καταλόγους με μια εφαρμογή ιστού, δίνοντας κατά συνέπεια ένα άλλο διάνυσμα επίθεσης (attack vector) (π.χ. ανιχνεύοντας κάτι αποσυνδεμένο στη σελίδα διαχείρισης). Όμως, το DirBuster δεν θα εκμεταλλευτεί τίποτα από αυτά που θα βρει. Δεν είναι αυτός ο σκοπός του. Η μόνη εργασία του είναι να ανακαλύπτει άλλα πιθανά διανύσματα επίθεσης. Το DirBuster βοηθά στη δημιουργία ασφαλών εφαρμογών: βρίσκοντας περιεχόμενο στον εξυπηρέτη ιστού (web server) ή μέσα στην εφαρμογή που δεν απαιτείται και βοηθώντας τους υπεύθυνους ανάπτυξης ώστε να κατανοήσουν ότι με το απλώς να μην παρέχουν σύνδεσμο προς μια σελίδα, δε σημαίνει ότι η σελίδα δεν μπορεί να προσπελαστεί. Οι στόχοι του έργου ανάπτυξης του εργαλείου DirBuster είναι οι ακόλουθοι:

- Παράγει ένα εργαλείο, το οποίο θα βοηθήσει στον έλεγχο μαύρου κουτιού (black box) εφαρμογών, προσπαθώντας να ανιχνεύσει κρυμμένο περιεχόμενο.
- Εξασφαλίζει ότι το εργαλείο που παράχθηκε, παρέχει πληροφορίες με τρόπο ώστε οποιεσδήποτε ψευδώς θετικές αναφορές (false positives) μπορούν να προσδιοριστούν γρήγορα.
- Παράγει λίστες ελέγχου σε μορφή κειμένου, που μπορούν να χρησιμοποιηθούν από το προαναφερθέν εργαλείο.

Το εργαλείο DirBuster έχει αναπτυχθεί σε Java και διανέμεται υπό την άδεια LGPL. Οι λίστες των καταλόγων διανέμονται υπό την άδεια Creative Commons Attribution-Share Alike 3.0.

3.2.4.1.2.2 Χαρακτηριστικά

Το DirBuster παρέχει τα ακόλουθα χαρακτηριστικά γνωρίσματα:

- Είναι πολύ-νηματικό με ικανότητα εκτέλεσης πάνω από 6000 αιτήσεις/sec.
- Δουλεύει σε http και https.
- Μπορεί να ανιχνεύσει τόσο καταλόγους όσο και αρχεία.
- Μπορεί να εκτελέσει αναδρομική ανίχνευση στους καταλόγους που βρίσκει.
- Είναι ικανό να εκτελέσει ανίχνευση βασισμένη σε λίστα ή ανίχνευση «ωμής βίας» (brute force).
- Το DirBuster μπορεί να αρχίσει σε οποιοδήποτε κατάλογο.
- Κοινές επικεφαλίδες HTTP, μπορούν να προστεθούν.
- Υποστήριξη proxy.
- Αυτόματη μεταγωγή (switching) μεταξύ αιτήσεων HEAD και GET.
- Περιλαμβάνει προηγμένο τρόπος ανάλυσης περιεχομένου για την περίπτωση όπου αποτυχημένες προσπάθειες (δηλ. αιτήσεις για σελίδες που δεν υπάρχουν) επιστρέφονται από τον εξυπηρέτη με κωδικό επιτυχίας (HTTP status 200). Οι

περιπτώσεις αυτές αναγνωρίζονται και έτσι δεν θεωρούνται ως επιτυχίες εύρεσης σελίδας.
- Κοινές επεκτάσεις αρχείων μπορούν να χρησιμοποιηθούν.
- Η απόδοση μπορεί να ρυθμιστεί ενώ το πρόγραμμα «τρέχει».
- Υποστηρίζει αυθεντικοποίηση Basic, Digest και NTLM.
- Γραμμή εντολών και διεπαφή GUI.

3.2.4.1.3 WSFuzzer

3.2.4.1.3.1 Γενικά

Το WSFuzzer είναι ένα πρόγραμμα LGPL'd, που έχει γραφεί σε Python, το οποίο στοχεύει αυτήν την περίοδο σε υπηρεσίες ιστού. Στην τρέχουσα έκδοση ο κύριος στόχος του είναι οι υπηρεσίες SOAP βασισμένες σε HTTP. Το συγκεκριμένο εργαλείο δημιουργήθηκε για να αυτοματοποιήσει, κάποιες διαδικασίες χειροκίνητου (manual) ελέγχου διείσδυσης με μηνύματα SOAP. Αυτό το εργαλείο δεν προορίζεται να αντικαταστήσει τη χειροκίνητη ανάλυση. Θα πρέπει να δούμε το WSFuzzer ως ένα εργαλείο προκειμένου να επαυξήσουμε την ανάλυση που εκτελείται από ικανούς και έμπειρους επαγγελματίες. Οι στόχοι είναι:

- Να αυτοματοποιήσει μερικές από τις πιο πολύπλοκες SOAP fuzzing διαδικασίες που θα κατανάλωναν αρκετό χρόνο εάν πραγματοποιούνταν χειροκίνητα.
- Να πραγματοποιήσει παραγωγή διανύσματος επίθεσης (attack vector) με ένα δυναμικό και ευφυή τρόπο που βασίζεται σε συγκεκριμένο στόχο.
- Να παρέχει τη λειτουργικότητά του και τα αποτελέσματα των δεδομένων του σε άλλα εργαλεία με όσο το δυνατόν μεγαλύτερο βαθμό ολοκλήρωσης.
- Να διευκολύνει την επαναλαμβανόμενη χρήση των γνωστών επιτυχών διανυσμάτων επίθεσης, ειδικά ενάντια σε συγκεκριμένους στόχους.
- Να αποτελέσει μέρος μιας εργαλειοθήκης (toolkit) για έλεγχο διείσδυσης εφαρμογών ιστού.
- Να είναι εύκολο να χρησιμοποιηθεί, να κατανοηθεί και να λειτουργήσει με υπηρεσίες SOAP.

Όπως αναφέρθηκε και προηγουμένως, δεν είναι στόχος του WSFuzzer να αντικαταστήσει την χειροκίνητη ανάλυση. Στην πραγματικότητα, το WSFuzzer δεν κάνει στην παρούσα έκδοσή του επαρκή ανάλυση των αποτελεσμάτων που συλλέγονται. Η διαδικασία της ανάλυσης αφήνεται για τον αναλυτή ή μηχανικό που εκτελεί ένα δεδομένο έλεγχο διείσδυσης.

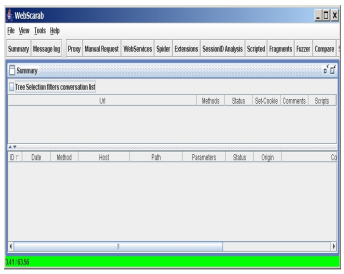
3.2.4.1.3.2 Χαρακτηριστικά

- Πραγματοποιεί έλεγχο διείσδυσης σε μια HTTP SOAP υπηρεσία ιστού που βασίζεται είτε στο έγκυρο WSDL, σε γνωστό έγκυρο ωφέλιμο φορτίο (payload) XML, είτε σ' ένα έγκυρο άκρο (endpoint) και περιοχή ονοματολογίας (namespace)[30].

[30] Η περιοχή ονοματολογίας (namespace) επιτρέπει να αποφεύγονται οι συγκρούσεις μεταξύ ονομάτων στοιχείων (element names) κυρίως όταν σε ένα αντικείμενο μπορούν ενσωματώνονται ή να χρησιμοποιούνται αρχεία και πόροι που έχουν αναπτυχθεί από διαφορετικές ομάδες. Το πλήρες όνομα ενός στοιχείου συναποτελείται από την ταυτότητα της περιοχής ονοματολογίας και το όνομα στοιχείου, οπότε ακόμη και αν δύο ομάδες έχουν χρησιμοποιήσει το ίδιο όνομα στοιχείου (π.χ. id) τα τελικά πλήρη ονόματα είναι διαφορετικά (π.χ. CryptographyAlgorithm::id και BankCustomer::id).

- Μπορεί να προσπαθήσει έξυπνα να ανιχνεύσει την περιγραφή WSDL για έναν δεδομένο στόχο.
- Περιλαμβάνει έναν απλό ανιχνευτή θυρών TCP (port scanner).
- Έχει τη δυνατότητα να πραγματοποιεί μεθόδους fuzz με πολλαπλές παραμέτρους. Υπάρχουν 2 τρόποι επίθεσης / fuzzing: «μεμονωμένος» και «ταυτόχρονος». Κάθε παράμετρος είτε αντιμετωπίζεται ως μοναδική οντότητα (μεμονωμένος τρόπος) και μπορεί είτε να επιχειρηθεί επίθεση με βάση τη συγκεκριμένη παράμετρο, είτε η παράμετρος να αγνοηθεί, είτε να επιχειρηθεί επίθεση με συνδυασμό πολλαπλών παραμέτρων (ταυτόχρονος τρόπος) με ένα δοθέν σύνολο δεδομένων.
- Η παραγωγή fuzz (attack strings) αποτελείται από έναν συνδυασμό ενός αρχείου-λεξικού, μερικά προαιρετικά δυναμικά πρότυπα έγχυσης μεγάλου μεγέθους και κάποιες προαιρετικές επιθέσεις που εξαρτώνται από τη μέθοδο, συμπεριλαμβανομένης της παραγωγής αυτοματοποιημένης επίθεσης XXE και WSSE.
- Καταγράφει με έξυπνο τρόπο, τα διανύσματα επίθεσης που μπορούν να προκαλέσουν καταστάσεις XDoS και έπειτα τα χρησιμοποιεί με βάση την απόκρισή μας για να εκτελέσει μια επίθεση XDoS.
- Το εργαλείο παρέχει επίσης την επιλογή της χρήσης μερικών τεχνικών διαφυγής IDS (IDS Evasion) που βοηθούν στην εκτέλεση ελέγχου υποδομής ισχυρής ασφάλειας (IDS/IPS).
- Το εργαλείο χρονομετρά το διάστημα μεταξύ της αίτησης και της απόκρισης, για να βοηθήσει ενδεχομένως στην ανάλυση αποτελεσμάτων.
- Για οποιοδήποτε δεδομένο πρόγραμμα που «τρέχει», τα παραγόμενα διανύσματα επίθεσης αποθηκεύονται σε ένα αρχείο XML. Το αρχείο XML ονομάζεται XXX και βρίσκεται στον ίδιο κατάλογο όπου είναι αποθηκευμένο το αρχείο HTML των αποτελεσμάτων.
- Η έξοδος (output) περιλαμβάνει αρχεία CSV και PDF.
- Ένα προηγούμενο παραγόμενο αρχείο XML των διανυσμάτων επίθεσης μπορεί να χρησιμοποιηθεί αντί του λεξικού. Αυτό γίνεται εξαιτίας της επανάληψης όπου τα ίδια διανύσματα πρέπει να χρησιμοποιηθούν επανειλημμένως.

3.2.4.1.4 WebScarab



3.2.4.1.4.1 Γενικά

Το WebScarab είναι ένα επιχειρησιακού επιπέδου, ανοικτού κώδικα εργαλείο ελέγχου ασφάλειας. Αποτελεί ένα πλαίσιο (framework), για την ανάλυση εφαρμογών ιστού που επικοινωνούν με χρήση των πρωτοκόλλων HTTP και HTTPS. Είναι γραμμένο σε γλώσσα Java και για αυτό το λόγο μπορεί να λειτουργήσει σε πολλές πλατφόρμες. Το WebScarab έχει διάφορους τρόπους λειτουργίας και λειτουργεί με τη χρήση διαφόρων plugins. Τα plugins ή αλλιώς extensions είναι προγράμματα που αλληλεπιδρούν με εφαρμογές (π.χ. ένα web browser ή ένα email client), παρέχοντας συγκεκριμένες συνήθως λειτουργίες. Στην πιο συνηθισμένη χρήση του, το WebScarab λειτουργεί ως ένας «αντιπρόσωπος παρεμβολής» (intercepting proxy), που επιτρέπει στο χρήστη να επισκοπήσει και να τροποποιήσει τις αιτήσεις που δημιουργούνται από τον browser του χρήστη, πριν σταλούν στον εξυπηρέτη (server), καθώς και να επισκοπήσει και να τροποποιήσει τις

επιστρεφόμενες αποκρίσεις του εξυπηρέτη, πριν αυτές παραληφθούν από τον browser. Το WebScarab είναι ένα εργαλείο που σχεδιάστηκε με σκοπό, πρώτιστα, να χρησιμοποιηθεί από εκείνους που μπορούν να γράψουν κώδικα οι ίδιοι ή έχουν τουλάχιστον μια αρκετά καλή κατανόηση του πρωτοκόλλου HTTP. Το WebScarab έχει ως σκοπό να αποκαλύψει τον τρόπο λειτουργίας μιας εφαρμογής HTTP(S), ή να επιτρέψει στον υπεύθυνο ανάπτυξης να διορθώσει τα δύσκολα προβλήματα, ή να επιτρέψει σε έναν ειδικό ασφάλειας να προσδιορίσει τις ευπάθειες μιας εφαρμογής, ανάλογα με τον τρόπο που αυτή έχει σχεδιαστεί ή εφαρμοσθεί.

3.2.4.1.4.2 Χαρακτηριστικά

Ένα πλαίσιο χωρίς λειτουργίες θα ήταν ελάχιστα χρήσιμο, γι' αυτό το WebScarab παρέχει διάφορα plugins, που στοχεύουν στη λειτουργία της επιθεώρησης ασφάλειας των εφαρμογών ιστού. Αυτά τα plugins περιλαμβάνουν:

- **Fragments:** εξάγει scripts και σχόλια από HTML σελίδες, όπως αυτά φαίνονται μέσω του proxy ή άλλων plugins.
- **Proxy:** παρατηρεί την κυκλοφορία μεταξύ browser και web server. Το WebScarab μπορεί να παρατηρεί και την HTTP αλλά και την κρυπτογραφημένη HTTPS κυκλοφορία, με τη δημιουργία μιας σύνδεσης SSL (SSL tunnel) μεταξύ του WebScarab και του browser, αντί απλά να συνδέσει τον browser στον εξυπηρέτη, επιτρέποντας έτσι σε κρυπτογραφημένα δεδομένα να περάσουν μέσω αυτού.
- **Manual intercept:** επιτρέπει στο χρήστη να τροποποιήσει άμεσα τις αιτήσεις HTTP/HTTPS και τις αποκρίσεις, πριν φθάσουν στον εξυπηρέτη ή στον browser.
- **Beanshell:** επιτρέπει την εκτέλεση αυθαίρετων σύνθετων λειτουργιών στις αιτήσεις και αποκρίσεις. Οτιδήποτε που μπορεί να εκφραστεί σε Java, μπορεί να εκτελεστεί.
- **Reveal hidden fields:** αλλάζει όλα τα κρυμμένα πεδία που βρίσκονται στις σελίδες HTML σε πεδία απλού κειμένου (text), καθιστώντας τα έτσι ορατά και επεξεργάσιμα.
- **Bandwidth simulator:** επιτρέπει στο χρήστη να μιμηθεί ένα αργό δίκτυο, με σκοπό να παρατηρήσει πώς θα εκτελεστεί ο δικτυακός του τόπος όταν προσπελαύνεται από ένα γραμμή χαμηλής ταχύτητας.
- **Spider:** προσδιορίζει νέα URLs στην περιοχή της σελίδας (site)-στόχου.
- **Manual request:** επιτρέπει την επεξεργασία και επανάληψη προηγούμενων αιτήσεων, ή δημιουργία νέων αιτήσεων.
- **SessionID analysis:** συλλέγει και αναλύει τα διάφορα cookies (καθώς επίσης και παραμέτρους που μεταβιβάζονται μέσω URL), ώστε να προσδιορίσει ο ελεγκτής το βαθμό τυχαιότητας και μη προβλεψιμότητας, των cookies που δημιουργούνται από την εφαρμογή.
- **Scripted:** μπορούμε γράψουμε scripts, τα οποία θα δημιουργήσουν τις αιτήσεις προς τον εξυπηρέτη. Το script μπορεί έπειτα να εκτελέσει μερική ανάλυση στις αποκρίσεις.
- **Parameter fuzzer:** εκτελεί την αυτοματοποιημένη αντικατάσταση των τιμών παραμέτρων, πράγμα το οποίο είναι πιθανό να αποκαλύψει την ελλειπή επικύρωση παραμέτρων, οδηγώντας έτσι σε ευπάθειες όπως είναι οι Cross Site Scripting (XSS) και Έγχυση SQL.
- **Search:** επιτρέπει στον χρήστη να εκτελεί αυθαίρετες BeanShell εκφράσεις για να προσδιορίσει διαλόγους που θα έπρεπε να εμφανισθούν στη λίστα.

- **Compare:** υπολογίζει την απόσταση επεξεργασίας ανάμεσα στα σώματα (bodies) απόκρισης των συνομιλιών που παρατηρήθηκαν και σε μια επιλεγμένη αρχική συνομιλία. Η απόσταση επεξεργασίας είναι ο αριθμός των επεξεργασιών που απαιτούνται για την μετατροπή ενός εγγράφου σε ένα άλλο.
- **SOAP:** αναλύει το έγγραφο WSDL και παρουσιάζει τις διάφορες λειτουργίες και τις απαραίτητες παραμέτρους, επιτρέποντας έτσι την επεξεργασία τους πριν σταλούν στον εξυπηρέτη (server).
- **Extensions:** αυτοματοποιεί ελέγχους για αρχεία που έχουν εσφαλμένα αφεθεί στον κατάλογο-ρίζα του web server. Οι έλεγχοι εκτελούνται και για αρχεία και για καταλόγους. Οι επεκτάσεις για αρχεία και καταλόγους μπορούν να επεξεργαστούν από το χρήστη.
- **XSS/CRLF:** παθητική ανάλυση plugin που αναζητά για δεδομένα ελεγχόμενα από το χρήστη σε επικεφαλίδες (headers) και στο σώμα (body) των HTTP αποκρίσεων, για να προσδιορίσει ενδεχόμενες ευπάθειες CRLF έγχυσης και cross-site scripting (XSS).

3.2.4.1.5 OWASP Live CD

3.2.4.1.5.1 Γενικά

Ο πρωταρχικός στόχος αυτού του έργου (project) είναι να καταστήσει τα εργαλεία και την τεκμηρίωση της ασφάλειας εφαρμογών ώστε να είναι εύκολα διαθέσιμα. Θεωρείται ως μια σημαντική προσθήκη στο στόχο του OWASP ώστε να γίνει ορατή η ασφάλεια εφαρμογών. Συγκεκριμένα, πρόκειται για ένα live CD, το οποίο είναι:

- εύκολο για τους χρήστες να το διατηρήσουν ενημερωμένο,
- εύκολο για τον υπεύθυνο έργου να το διατηρήσει ενημερωμένο,
- εύκολο να παράγει νέες εκδόσεις (τριμηνιαίες εκδόσεις),
- εστιάζει ακριβώς στον έλεγχο εφαρμογών ιστού και όχι σε γενικό έλεγχο διείσδυσης (Pen Testing).

3.2.4.1.5.2 Χαρακτηριστικά

Κάποια βασικά χαρακτηριστικά του έργου συνοψίζονται ως εξής:

- Παρέχει μια προθήκη για σημαντικά εργαλεία και τεκμηρίωση του OWASP.
- Παρέχει τα βέλτιστα, ελεύθερα διανεμούμενα εργαλεία ασφάλειας εφαρμογών σε μια εύχρηστη συσκευασία.
- Εξασφαλίζει ότι τα εργαλεία που παρέχονται, είναι όσο το δυνατόν πιο εύχρηστα.
- Συνεχίζει να προσθέτει τεκμηρίωση και εργαλεία στο OWASP Live CD.
- Συνεχίζει να τεκμηριώνει το πώς να χρησιμοποιηθούν τα εργαλεία και πώς δημιουργήθηκαν οι ενότητες (modules) εργαλείων.
- Ευθυγραμμίζει τα εργαλεία που παρέχονται με τον Οδηγό Ελέγχου έκδοσης 3 του OWASP (OWASP Testing Guide v3) ώστε να παρέχουν τη μέγιστη κάλυψη.

Μερικά από τα εργαλεία που υπάρχουν στο CD είναι: OWASP's WebScarab[3.2.4.1.4], OWASP's WebGoat, OWASP's JbroFuzz[3.2.4.1.1], Paros Proxy[11], Nmap, tcpdump[4], OWASP DirBuster[3.2.4.1.2], Nikto 2.0, Sqlmap, HTTP Print, OWASP WSFuzzer[3.2.4.1.3], OWASP Skavenger και άλλα.

3.2.4.2 Εργαλεία για τους ελέγχους του OWASP Testing Guide

Στον πίνακα που ακολουθεί παραθέτουμε κάποια εργαλεία, τα οποία μπορούν να χρησιμοποιηθούν για τους διάφορους ελέγχους του OWASP Testing Guide.

Κατηγορία	Ονομασία ελέγχου	Εργαλεία
Συλλογή Πληροφοριών (Information Gathering)	Ταυτοποίηση των σημείων εισόδου εφαρμογής - Identify application entry points (OWASP-IG-003)	Webscarab[3.2.4.1.4], Burp proxy, Paros Proxy[11]
	Έλεγχος Αποτυπώματος Εφαρμογής Ιστού - Testing Web Application Fingerprint (OWASP-IG-004)	httprint, Netcraft, httprecon, WebRecon
	Ανακάλυψη Εφαρμογής - Application Discovery (OWASP-IG-005)	Εργαλεία αναζήτησης DNS (nslookup, dig), Ανιχνευτές θυρών (nmap) και ανιχνευτές ευπάθειας (Nessus[2], wikto[9]), Μηχανές αναζήτησης (Google[1])
Έλεγχος Διαχείρισης Διαμόρφωσης (Configuration Management Testing)	Έλεγχος SSL/TLS - SSL/TLS Testing (OWASP-CM-001)	Nessus[2], SSL Digger, nmap, stunnel, OpenSSL
	Έλεγχος Ακροατή DB - DB Listener Testing (OWASP-CM-002)	TNS Listener tool (Perl), Toad για Oracle
	Έλεγχος για Χειρισμό Επεκτάσεων Αρχείων - Testing for File Extensions Handling (OWASP-CM-005)	Ανιχνευτές ευπάθειας (Nessus[2], Nikto), wget, curl, Google[1] για «web mirroring tools».
	Παλιά, Εφεδρικά και Μη-αναφερόμενα Αρχεία - Old, Backup and Unreferenced Files (OWASP-CM-006)	Ανιχνευτές ευπάθειας (Nessus[2], Nikto, Wikto[9]), Εργαλεία ανίχνευσης ιστού (wget, Sam Spade, Spike proxy, Xenu, curl).
	Έλεγχος για Μεθόδους HTTP και XST - Testing for HTTP Methods and XST (OWASP-CM-008)	NetCat[5]
Έλεγχος Επιχειρησιακής Λογικής (Business Logic Testing)	Έλεγχος επιχειρησιακής λογικής - Business logic testing (OWASP-BL-001)	Τα αυτοματοποιημένα εργαλεία είναι ανίκανα να ανιχνεύσουν λογικές ευπάθειες.
Έλεγχος Αυθεντικοποίησης (Authentication Testing)	Μεταφορά διαπιστευτηρίων σ' ένα Κρυπτογραφημένο Κανάλι - Credentials transport over an encrypted channel (OWASP-AT-001)	WebScarab[3.2.4.1.4]
	Έλεγχος για απαρίθμηση χρηστών - Testing for user enumeration (OWASP-AT-002)	WebScarab[3.2.4.1.4], CURL, PERL, εργαλείο απαρίθμησης χρηστών Sun Java Access & Identity Manager
	Έλεγχος για Εικάσιμο (με Λεξικό) Λογαριασμό Χρηστών - Testing for Guessable (Dictionary) User Account (OWASP-AT-003)	Burp Intruder, THC Hydra, Brutus
	Έλεγχος «Ωμής Βίας» - Brute Force Testing (OWASP-AT-004)	THC Hydra, John the Ripper, Brutus, Burp Intruder, Ophcrack
	Έλεγχος για την παράκαμψη του σχήματος αυθεντικοποίησης - Testing for bypassing authentication schema (OWASP-AT-005)	WebScarab[3.2.4.1.4], WebGoat
	Έλεγχος Αποσύνδεσης και Διαχείρισης Μνήμης του Φυλλομετρητή - Testing for Logout and Browser Cache Management (OWASP-AT-007)	Add N Edit Cookies (πρόσθετο του Firefox).

Κατηγορία	Ονομασία ελέγχου	Εργαλεία
Έλεγχος Εξουσιοδότησης (Authorization testing)	Έλεγχος για Διάσχιση Μονοπατιού - Testing for Path Traversal (OWASP-AZ-001)	Web Proxy (Burp Suite, Paros[11], WebScarab[3.2.4.1.4]), εργαλεία κωδικοποίησης / αποκωδικοποίησης, ερευνητής συμβολοσειράς (grep)
	Έλεγχος για παράκαμψη του σχήματος εξουσιοδότησης - Testing for bypassing authorization schema (OWASP-AZ-002)	WebScarab[3.2.4.1.4]
	Έλεγχος για Κλιμάκωση Δικαιωμάτων - Testing for Privilege Escalation (OWASP-AZ-003)	WebScarab[3.2.4.1.4]
Έλεγχος Διαχείρισης Συνόδου (Session Management Testing)	Έλεγχος για το Σχήμα Διαχείρισης Συνόδου - Testing for Session Management Schema (OWASP-SM-001)	WebScarab[3.2.4.1.4], Foundstone CookieDigger
	Έλεγχος για ιδιότητες Cookies - Testing for Cookies attributes (OWASP-SM-002)	Webscarab[3.2.4.1.4], Burp proxy, Paros Proxy[11]
	Έλεγχος για Προσήλωση Συνόδου - Testing for Session Fixation (OWASP-SM-003)	WebScarab[3.2.4.1.4]
	Έλεγχος για CSRF - Testing for CSRF (OWASP-SM-005)	εργαλεία spider/crawler
Έλεγχος Επικύρωσης Δεδομένων (Data Validation Testing)	Έλεγχος για Reflected Cross Site Scripting - Testing for Reflected Cross Site Scripting (OWASP-DV-001)	OWASP CAL9000, PHP Charset Encoder(PCE), WebScarab[3.2.4.1.4], XSS-Proxy, ratproxy, Burp Proxy
	Έλεγχος για Αποθηκευμένο Cross Site Scripting - Testing for Stored Cross Site Scripting (OWASP-DV-002)	OWASP CAL9000, PHP Charset Encoder(PCE), Hackvertor, BeEF, XSS-Proxy, Backframe, WebScarab[3.2.4.1.4], Burp, XSS Assistant
	Έλεγχος για Cross Site Flashing - Testing for Cross Site Flashing (OWASP-DV004)	SWFIntruder, Decompiler (Flare), Compiler (MTASC), Disassembler (Flasm), Swfmill, Debugger Version of Flash Plugin/Player
	Έγχυση SQL - SQL Injection (OWASP-DV-005)	SQLInjector, Orascan, sqlmap, SqlDumper, sqlninja, SQL Power Injector
	Έγχυση LDAP - LDAP Injection (OWASP-DV-006)	Softerra LDAP Browser
	Έγχυση ORM - ORM Injection (OWASP-DV-007)	Hibernate, NHibernate, Ruby On Rails
	Έγχυση SSI - SSI Injection (OWASP-DV-009)	Web Proxy Burp Suite, Paros[11], WebScarab[3.2.4.1.4], ερευνητής συμβολοσειράς (grep)
	Εντολές Λειτουργικού Συστήματος - OS (operating system) Commanding (OWASP-DV-013)	OWASP WebScarab[3.2.4.1.4], WebGoat
	Υπερχείλιση Προσωρινής μνήμης - Buffer overflow (OWASP-DV-014)	OllyDbg, Spike, Brute Force Binary Tester (BFB), Metasploit[10], Stack, ITS4
	Έλεγχος «κυοφορίας» ευπάθειας - Incubated vulnerability Testing (OWASP-DV-015)	XSS-proxy, Paros[11], Burp Suite, Metasploit[10]

Κατηγορία	Ονομασία ελέγχου	Εργαλεία
Έλεγχος Άρνησης Παροχής Υπηρεσιών (Denial of Service Testing)	Έλεγχος για Επιθέσεις Μπαλαντέρ SQL - Testing for SQL Wildcard Attacks (OWASP-DS-001)	Ο έλεγχος μπορεί να γίνει χειροκίνητα. Επίσης, ένας fuzzer θα μπορούσε να αυτοματοποιήσει τη διαδικασία.
Έλεγχος Υπηρεσιών Ιστού (Web Services Testing)	Συλλογή πληροφοριών WS - WS Information Gathering (OWASP-WS-001)	OWASP WebScarab[3.2.4.1.4], Mac OSX Soap Client, Foundstone WSDigger, Soaplite, Perl, SOAPClient4XG, CURL, Web Services Directory, Seekda, UDDI Browser, Xmethods, WSIndex
	Έλεγχος WSDL - Testing WSDL (OWASP-WS-002)	OWASP WebScarab[3.2.4.1.4], Foundstone WSDigger
	Δομικός Έλεγχος XML - XML Structural Testing (OWASP-WS-003)	OWASP WebScarab[3.2.4.1.4]
	Έλεγχος επιπέδου περιεχομένου της XML - XML Content-level Testing (OWASP-WS-004)	OWASP WebScarab[3.2.4.1.4], MetaSploit[10]
	Κακόβουλα συνημμένα σε μηνύματα SOAP - Naughty SOAP attachments (OWASP-WS-006)	EICAR, OWASP WebScarab[3.2.4.1.4]
	Έλεγχος Αναπαραγωγής - Replay Testing (OWASP-WS-007)	OWASP WebScarab[3.2.4.1.4], Ethereal, Wireshark[3], TCPReplay
Έλεγχος Ajax (Ajax Testing)	How to test AJAX (OWASP-AJ-002)	OWASP Sprajax, Venkman, Scriptaculous's Ghost Train, Squish, JsUnit, FireBug

Πίνακας 10. Εργαλεία για τους ελέγχους του OWASP Testing Guide

3.2.5 Συμπεράσματα

Συνοψίζοντας ο Οδηγός (Guide) θα βοηθήσει τη βιομηχανία ασφάλειας ως ακολούθως:

- στους ελεγκτές διείσδυσης (Pen-testers) παρέχει:
  - Μια δομημένη προσέγγιση για τις δραστηριότητες έλεγχου.
  - Μια λίστα ελέγχου (checklist) που θα πρέπει να ακολουθηθεί.
  - Ένα εργαλείο εκμάθησης και κατάρτισης.
- στους πελάτες (clients) παρέχει:
  - Ένα εργαλείο για να κατανοήσουν τις ευπάθειες ιστού και τις επιπτώσεις τους.
  - Έναν τρόπο για να ελεγχθεί η ποιότητα των ελέγχων διείσδυσης (penetration tests) που αγοράζουν.

Πιο γενικά, ο Οδηγός στοχεύει στην παροχή ενός προτύπου ελέγχου διείσδυσης (pen-testing) που δημιουργεί ένα «κοινό έδαφος» μεταξύ της βιομηχανίας ελέγχου διείσδυσης και του πελάτη της. Αυτό θα αυξήσει τη συνολική ποιότητα και κατανόηση αυτού του είδους δραστηριότητας και επομένως, το γενικό επίπεδο ασφάλειας στις υποδομές.

3.3 OWASP Application Security Verification Standard (ASVS)

3.3.1 Γενικά

3.3.1.1 Τι είναι το ASVS;

Εφόσον το OWASP Top Ten είναι ένα εργαλείο που παρέχει την επίγνωση της ασφάλειας των εφαρμογών ιστού, το Πρότυπο Επαλήθευσης της Ασφάλειας Εφαρμογών του OWASP (OWASP Application Security Verification Standard-ASVS) είναι ένα εμπορικά-εφαρμόσιμο ανοικτό (open) πρότυπο που ορίζει την εμβέλεια της κάλυψης και τα επίπεδα αυστηρότητας τα οποία μπορούν να χρησιμοποιηθούν για να εκτελέσουν επαληθεύσεις στην ασφάλεια εφαρμογών. Είναι το πρώτο πρότυπο που έχει δημοσιεύσει το OWASP..Το ASVS:

- Προορίζεται ως ένα πρότυπο που μας βοηθά στο πώς να ελέγξουμε την ασφάλεια των εφαρμογών ιστού.
- Πρέπει να είναι ανεξάρτητο από την εφαρμογή.
- Πρέπει να είναι ανεξάρτητο από τον κύκλο ζωής της ανάπτυξης.
- Πρέπει να καθορίζει τις απαιτήσεις που μπορούν να εφαρμοστούν στις εφαρμογές ιστού, χωρίς ειδική ερμηνεία.

3.3.1.2 Βασικοί στόχοι

Ο κύριος στόχος του έργου του Προτύπου Επαλήθευσης της Ασφάλειας Εφαρμογών (Application Security Verification Standard Project) είναι να κανονικοποιήσει την εμβέλεια της κάλυψης και τα επίπεδα αυστηρότητας που είναι διαθέσιμα στην αγορά, όταν πρόκειται να γίνει εκτέλεση επαλήθευσης της ασφάλειας εφαρμογών ιστού, χρησιμοποιώντας ένα εμπορικά-εφαρμόσιμο ανοικτό πρότυπο. Το συγκεκριμένο πρότυπο παρέχει μια βάση για την εξέταση των τεχνικών ελέγχων ασφάλειας των εφαρμογών, καθώς επίσης και οποιωνδήποτε τεχνικών ελέγχων ασφάλειας στο περιβάλλον, οι οποίες χρησιμοποιούνται για να προστατεύσουν από ευπάθειες όπως Cross-Site Scripting (XSS) και έγχυσης SQL (SQL injection). Αυτό το πρότυπο μπορεί να χρησιμοποιηθεί για να καθιερωθεί ένα επίπεδο εμπιστοσύνης στην ασφάλεια των εφαρμογών ιστού. Οι απαιτήσεις αναπτύχθηκαν με βάση τους ακόλουθους στόχους:

- Χρήση ως μετρικής - Παρέχει στους υπεύθυνους ανάπτυξης εφαρμογών και στους ιδιοκτήτες εφαρμογών, ένα κριτήριο με το οποίο να μπορούν να αξιολογήσουν το βαθμό εμπιστοσύνης που μπορεί να έχει ο οργανισμός στις εφαρμογές ιστού του,
- Χρήση ως καθοδήγηση - Παρέχει καθοδήγηση στους υπεύθυνους ανάπτυξης ελέγχων ασφάλειας ως προς το τι να εφαρμόσουν στους ελέγχους ασφάλειας προκειμένου να ικανοποιηθούν οι απαιτήσεις ασφάλειας εφαρμογών, και
- Χρήση κατά τη διάρκεια της προμήθειας - Παρέχει μια βάση για τον προσδιορισμό των απαιτήσεων επαλήθευσης της ασφάλειας εφαρμογών σύμφωνα με τους κανονισμούς.

Οι απαιτήσεις σχεδιάστηκαν για να επιτύχουν τους ανωτέρω στόχους εξασφαλίζοντας την επικύρωση για το πώς οι έλεγχοι ασφάλειας σχεδιάζονται, εφαρμόζονται και χρησιμοποιούνται από μια εφαρμογή. Οι απαιτήσεις εξασφαλίζουν ότι οι έλεγχοι ασφάλειας, που χρησιμοποιούνται από μια εφαρμογή, λειτουργούν χρησιμοποιώντας μια στρατηγική «άρνησης ως προεπιλογή» (deny-by-default), συγκεντρώνονται, εφαρμόζονται από την πλευρά του εξυπηρέτη (server) και χρησιμοποιούνται, όπου είναι απαραίτητο.

3.3.1.3 Στόχοι σχεδιασμού του ASVS

Οι στόχοι σχεδιασμού του ASVS είναι οι παρακάτω:

- Το πρότυπο πρέπει να καθορίζει τις λειτουργικές απαιτήσεις επαλήθευσης που ακολουθούν μια προσέγγιση λευκής λίστας (white-list[31]) (δηλ. θετικών, πλεονεκτημάτων).
- Το πρότυπο πρέπει να καθορίζει τα αυξανόμενα επίπεδα επαλήθευσης ασφάλειας εφαρμογών.
- Η διαφορά στην κάλυψη και τα επίπεδα διεξοδικότητας και αυστηρότητας ελέγχων (rigor) μεταξύ των επιπέδων, πρέπει να είναι σχετικά γραμμική.
- Το πρότυπο πρέπει επίσης να είναι ανεξάρτητο από εργαλεία και τεχνικές επαλήθευσης!

3.3.1.4 Από που προήλθε το ASVS;

Τα πρότυπα επαλήθευσης της ασφάλειας εφαρμογών (Application Security Verification Standards) είναι προδιαγραφές που παράγονται από το OWASP σε συνεργασία με υπεύθυνους ανάπτυξης και ελεγκτές ασφαλών εφαρμογών παγκοσμίως και έχουν σκοπό την επιτάχυνση της επέκτασης των ασφαλών εφαρμογών ιστού. Πρώτη φορά, δημοσιεύτηκε το 2008 ως αποτέλεσμα μιας επιχορήγησης OWASP Summer of Code και έπειτα από συνεδριάσεις με μια μικρή ομάδα από early adopters[32]. Πλέον τα έγγραφα του ASVS έχουν γίνει ευρέως γνωστά και έχουν υλοποιηθεί. Το πρόγραμμα ASVS του OWASP διευθύνεται από τον Mike Boberski (Booz Allen Hamilton). Οι αρχικοί συντάκτες του, είναι οι Mike, Jeff Williams (Aspect Security) και Dave Wichers (Aspect Security). Το ASVS είναι το αποτέλεσμα της συλλογής και ενοποίησης της -επί δεκαετιών- εμπειρίας συλλογικών θεμάτων στην ασφάλεια εφαρμογών.

3.3.2 Εμβέλεια (Scope)

3.3.2.1 ASVS - το κατάλληλο πρότυπο

Το ASVS είναι το πρότυπο που θα πρέπει να χρησιμοποιήσουμε, εάν στην επιχείρησή μας πραγματοποιούμε τα ακόλουθα:

- Ανίχνευση ευπαθειών (Vulnerability scanning)
- Στατική ανάλυση κώδικα (Static code analysis)
- Χειροκίνητο έλεγχο διείσδυσης (Manual penetration testing)
- Χειροκίνητη επισκόπηση κώδικα (Manual code review)
- Μοντελοποίηση απειλών (Threat modeling)
- Επισκόπηση αρχιτεκτονικής ασφάλειας (Security architecture review)

3.3.2.2 Γιατί μπορεί να χρησιμοποιηθεί το ASVS του OWASP;

Αυτό που γίνεται γρήγορα σαφές, όταν πραγματοποιείται προσπάθεια ώστε να συλλεχθούν οι συμβατικοί όροι και προϋποθέσεις που είναι σχετικές με την ασφάλεια των εφαρμογών και υπηρεσιών ιστού, είναι ότι ο προσδιορισμός των απαιτήσεων ελέγχου και ανάλυσης της ασφάλειας είναι πολύ δύσκολος. Γίνεται επίσης γρήγορα προφανές, κατά την επισκόπηση των αναφορών επαλήθευσης της ασφάλειας των εφαρμογών και υπηρεσιών ιστού, ότι δεν υπάρχει κανένας τρόπος για να διαχωρισθεί η περίπτωση μεταξύ κάποιου που διενεργεί έλεγχο ασφάλειας απλώς «τρέχοντας» ένα

[31] White-list - Μία λίστα επιτρεπόμενων δεδομένων ή λειτουργιών, παραδείγματος χάριν μια λίστα χαρακτήρων που επιτρέπονται για να εκτελεστεί επικύρωση εισαγωγής.
[32] Ένας πρόωρος (early) adopter είναι ένα άτομο που αγκαλιάζει ή υιοθετεί τη νέα τεχνολογία πριν το κάνουν οι περισσότεροι.

εργαλείο grep[33] και κάποιου που κάνει προσεκτική επισκόπηση κώδικα και χειροκίνητο έλεγχο.

Και τα δύο προβλήματα έχουν μια ενιαία πρωταρχική αιτία: την έλλειψη ενός προτύπου που να εκτελεί επαλήθευση ασφάλειας επιπέδου εφαρμογών, το οποίο να είναι ανεξάρτητο από τις εφαρμογές και υπηρεσίες ιστού, να είναι ανεξάρτητο του Κύκλου Ζωής Ανάπτυξης Λογισμικού (Software Development Life Cycle-SDLC) και που να μπορεί να χρησιμοποιηθεί για οποιαδήποτε εφαρμογή χωρίς ειδική ερμηνεία. Το Πρότυπο Επαλήθευσης της Ασφάλειας Εφαρμογών του OWASP (OWASP ASVS) σχεδιάστηκε με σκοπό να εξομαλύνει (κανονικοποιήσει) την εμβέλεια στην κάλυψη και τα επίπεδα αυστηρότητας τα οποία είναι διαθέσιμα στην αγορά, όταν εκτελείται επαλήθευση της ασφάλειας εφαρμογών.

3.3.2.3 Οι ερωτήσεις που απαντά το ASVS

- Ποια χαρακτηριστικά γνωρίσματα ασφάλειας, θα πρέπει να καλύπτονται από το απαιτούμενο σύνολο ελέγχων της ασφάλειας;
- Τι σημαίνουν οι λογικές αυξήσεις στην κάλυψη και το επίπεδο αυστηρότητας κατά την επαλήθευση της ασφάλειας μιας εφαρμογής ιστού;
- Πώς μπορούμε να συγκρίνουμε τα αποτελέσματα προσπαθειών επαλήθευσης;
- Τι βαθμός εμπιστοσύνης μπορεί να πλαισιωθεί σε μια εφαρμογή ιστού;

Το ASVS μπορεί να απαντήσει σε αυτές τις ερωτήσεις και για εφαρμογές ελάχιστου κινδύνου αλλά και για εφαρμογές κρίσιμης υποδομής.

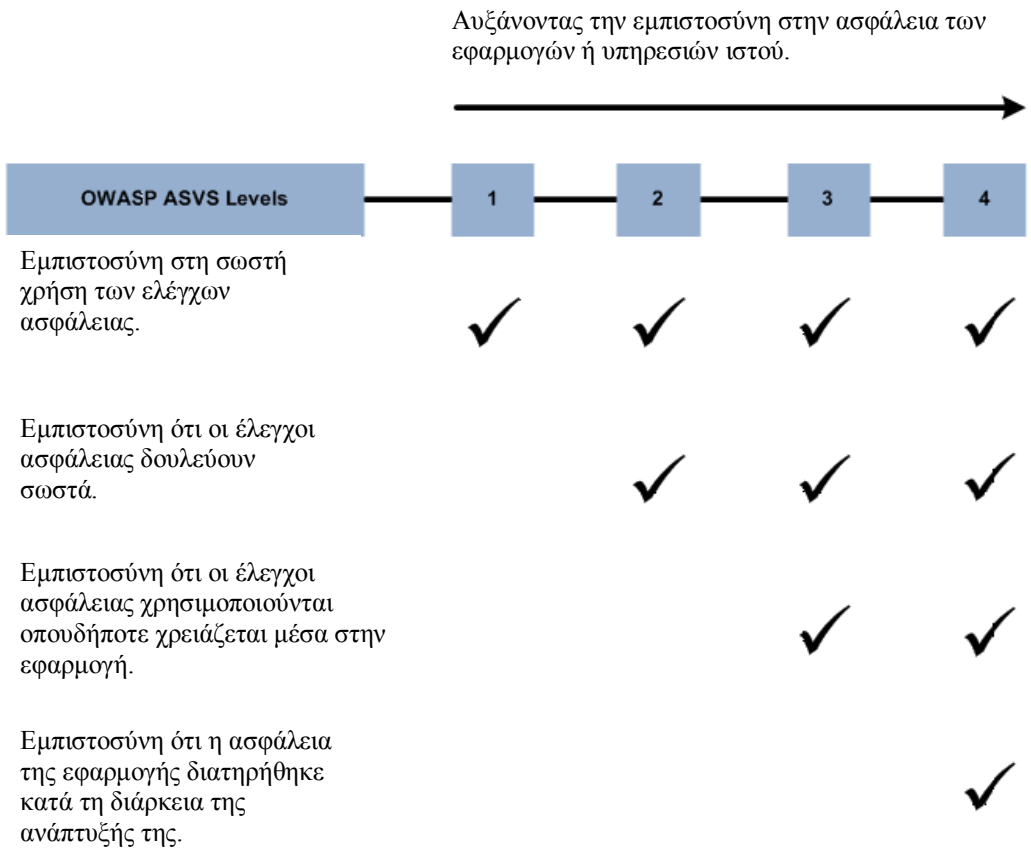
3.3.3 Επίπεδα ασφάλειας

3.3.3.1 Γενικά

Το πρότυπο ASVS του OWASP χρησιμοποιεί τον όρο «ελεγκτής» (verifier) για να υποδείξει το πρόσωπο ή την ομάδα που θα επισκοπήσει την εφαρμογή ενάντια σε αυτές τις απαιτήσεις. Ευθύνη ενός ελεγκτή είναι να καθορίσει, εάν μια εφαρμογή καλύπτει όλες τις απαιτήσεις για το επίπεδο που στοχεύει, με μια επισκόπηση. Εάν η εφαρμογή καλύπτει όλες τις απαιτήσεις για αυτό το επίπεδο, τότε μπορεί να θεωρηθεί ως μια εφαρμογή Επιπέδου N βάσει του OWASP ASVS, όπου N είναι το επίπεδο επαλήθευσης με το οποίο συμμορφώθηκε η εφαρμογή. Εάν η εφαρμογή δεν καλύπτει όλες τις απαιτήσεις για ένα συγκεκριμένο επίπεδο, αλλά καλύπτει όλες τις απαιτήσεις για ένα χαμηλότερο επίπεδο αυτού του προτύπου, τότε μπορεί να θεωρηθεί ότι έχει περάσει το χαμηλότερο επίπεδο επαλήθευσης.

Το ASVS του OWASP καθορίζει τις απαιτήσεις επαλήθευσης και τεκμηρίωσης που ομαδοποιούνται βάσει της σχετικής κάλυψης και του επιπέδου αυστηρότητας. Η επαλήθευση ασφάλειας των εφαρμογών ιστού, εκτελείται από μια λογική πτυχή, ακολουθώντας (ή προσπαθώντας να ακολουθήσει) μονοπάτια (paths) μέσα και έξω από την εφαρμογή και εκτελώντας ανάλυση κατά μήκος αυτών των μονοπατιών. Το πρότυπο καθορίζει τέσσερα ιεραρχικά επίπεδα (π.χ. το Επίπεδο 2 απαιτεί περισσότερη κάλυψη και αυστηρότητα από το Επίπεδο 1) όπως απεικονίζεται στο Σχήμα 20.

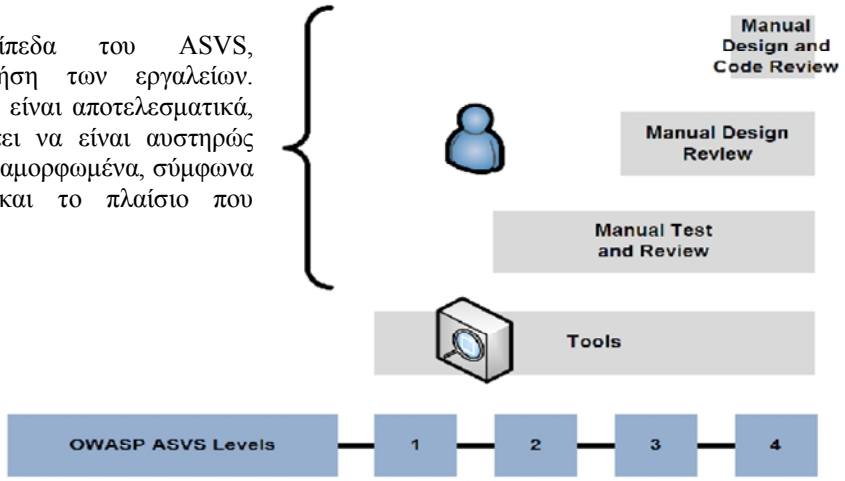
[33] grep είναι ένα εργαλείο που προέρχεται από το Unix. Μπορεί να ψάξει μέσα σε αρχεία και φακέλους (καταλόγους στο Unix) και να ελέγξει ποιες γραμμές σε αυτά τα αρχεία ταιριάζουν με μια δοθείσα κανονική έκφραση.



Σχήμα 20. Τα Επίπεδα (Levels) του OWASP ASVS.

Το Πρότυπο (Standard) επιπλέον καθορίζει τα συστατικά μέρη για τα Επίπεδα 1 και 2 (π.χ. η επαλήθευση στο Επίπεδο 1 απαιτεί την κάλυψη των απαιτήσεων και του επιπέδου 1Α και 1Β). Οι εφαρμογές μπορούν να απαιτήσουν συμμόρφωση είτε στο Επίπεδο 1Α, είτε στο 1Β αντί του Επιπέδου 1, αλλά η παραγωγή τέτοιων απαιτήσεων είναι λιγότερο ισχυρή από τους απαιτήσεις του Επιπέδου 1. Ομοίως, οι εφαρμογές μπορούν να απαιτήσουν συμμόρφωση είτε στο Επίπεδο 2Α, είτε στο 2Β αντί του Επιπέδου 2, αλλά κι εδώ ισχύει ότι, η παραγωγή τέτοιων απαιτήσεων είναι λιγότερο ισχυρή από τους απαιτήσεις του Επιπέδου 2.

Στα ανώτερα επίπεδα του ASVS, ενθαρρύνεται η χρήση των εργαλείων. Προκειμένου όμως να είναι αποτελεσματικά, τα εργαλεία θα πρέπει να είναι αυστηρώς προσαρμοσμένα και διαμορφωμένα, σύμφωνα με την εφαρμογή και το πλαίσιο που χρησιμοποιείται.

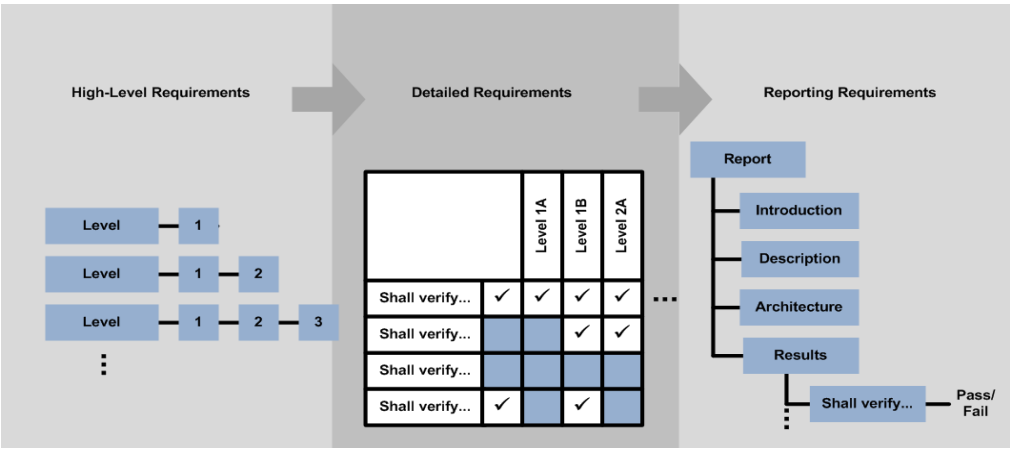


Σχήμα 21. Τα Επίπεδα Επαλήθευσης του ASVS.

Οι απαιτήσεις επαλήθευσης και τεκμηρίωσης καθορίζονται σε αυτό το πρότυπο, χρησιμοποιώντας τρεις τύπους απαιτήσεων:

- Απαιτήσεις επιπέδων,
- Απαιτήσεις Παραγόμενης Επαλήθευσης και
- Απαιτήσεις Παραγόμενων Εκθέσεων.

Οι απαιτήσεις επιπέδων καθορίζουν τις απαιτήσεις υψηλού επιπέδου υλοποίησης και επαλήθευσης των εφαρμογών ιστού, σύμφωνα με το ASVS του OWASP. Οι απαιτήσεις παραγόμενης επαλήθευσης καθορίζουν τις απαιτήσεις χαμηλού επιπέδου υλοποίησης και επαλήθευσης των εφαρμογών ιστού (δηλαδή, να επαληθευθούν συγκεκριμένα δεδομένα). Οι απαιτήσεις των παραγόμενων εκθέσεων καθορίζουν το πώς τα αποτελέσματα της εκτέλεσης μιας επαλήθευσης εφαρμογής ιστού, σύμφωνα με το OWASP ASVS, πρέπει να τεκμηριωθούν. Η σχέση μεταξύ αυτών των τύπων απαιτήσεων απεικονίζεται στο επόμενο Σχήμα 22.



Σχήμα 22. Σχέση μεταξύ των Απαιτήσεων του OWASP ASVS.

3.3.3.2 Επίπεδα Επαλήθευσης Ασφάλειας Εφαρμογών

Το ASVS καθορίζει τέσσερα επίπεδα επαλήθευσης που αυξάνονται και σε εύρος και σε βάθος, καθώς κινούμαστε επάνω στα επίπεδα. Το εύρος καθορίζεται σε κάθε επίπεδο από ένα σύνολο απαιτήσεων ασφάλειας που πρέπει να εξεταστεί. Το

βάθος της επαλήθευσης καθορίζεται από την προσέγγιση και το επίπεδο αυστηρότητας που απαιτείται στην επαλήθευση κάθε απαίτησης ασφάλειας.

Είναι ευθύνη ενός ελεγκτή να καθορίσει εάν ένας TOV[34] καλύπτει όλες τις απαιτήσεις για το επίπεδο που στοχεύει, με μια επισκόπηση. Εάν η εφαρμογή καλύπτει όλες τις απαιτήσεις για αυτό το επίπεδο, τότε μπορεί να θεωρηθεί ως μια εφαρμογή Επιπέδου N, όπου N είναι το επίπεδο επαλήθευσης με το οποίο συμμορφώθηκε η εφαρμογή. Εάν η εφαρμογή δεν καλύπτει όλες τις απαιτήσεις για ένα συγκεκριμένο επίπεδο, αλλά καλύπτει όλες τις απαιτήσεις για ένα χαμηλότερο επίπεδο αυτού του προτύπου, τότε μπορεί να θεωρηθεί ότι έχει περάσει το χαμηλότερο επίπεδο επαλήθευσης. Το συγκεκριμένο πρότυπο χρησιμοποιεί τον όρο «ελεγκτής» για να υποδείξει το πρόσωπο ή την ομάδα που θα επισκοπήσει την εφαρμογή ενάντια σε αυτές τις απαιτήσεις. Δεν υπάρχει κανένα επίπεδο επαλήθευσης 0. Επίσης, για να κερδίσουμε ένα επίπεδο, οι ευπάθειες πρέπει να έχουν ανιχνευθεί (ή μετρηθεί) και η εφαρμογή να επαληθευθεί ξανά.

1. Επίπεδο 1 - Αυτοματοποιημένη Επαλήθευση (Automated Verification)

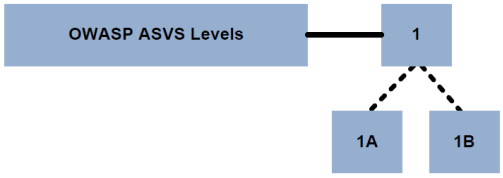
Το Επίπεδο 1 (Level 1) είναι τυπικά κατάλληλο για εφαρμογές όπου απαιτείται μερική εμπιστοσύνη στη σωστή χρήση των ελέγχων ασφάλειας. Οι απειλές στην ασφάλεια[35] θα είναι συνήθως κάποιοι ιοί (viruses) και σκουλήκια (worms) (οι στόχοι επιλέγονται ανεξάρτητα μέσω διαφόρων ανιχνεύσεων και καταγράφουν τον πιο τρωτό). Η εμβέλεια της επαλήθευσης περιλαμβάνει τον κώδικα που αναπτύχθηκε ή τροποποιήθηκε προκειμένου να δημιουργηθεί η εφαρμογή.

Στο Επίπεδο 1, η επαλήθευση περιλαμβάνει τη χρήση των αυτοματοποιημένων εργαλείων, και η επαλήθευση επαυξάνεται με τη χειροκίνητη (manual) επαλήθευση. Αυτό το επίπεδο παρέχει μόνο μερική κάλυψη της επαλήθευσης της ασφάλειας εφαρμογών. Η χειροκίνητη επαλήθευση δεν προορίζεται να διενεργήσει πλήρη επαλήθευση της ασφάλειας εφαρμογών σε αυτό το επίπεδο, αλλά μόνο να επαληθεύσει ότι κάθε αυτοματοποιημένη εύρεση είναι σωστή και όχι μία ψευδώς θετική αναφορά (false positive).

Υπάρχουν δύο τμήματα για το Επίπεδο 1. Το Επίπεδο 1Α είναι για τη χρήση των αυτοματοποιημένων εργαλείων ανίχνευσης (δυναμική ανάλυση) ευπάθειας των εφαρμογών και το Επίπεδο 1Β είναι για τη χρήση των αυτοματοποιημένων εργαλείων ανίχνευσης (στατική ανάλυση) πηγαίου κώδικα. Κατά την επαλήθευση μπορεί να χρησιμοποιηθεί, είτε καθένα από αυτά τα τμήματα χωριστά, είτε μπορεί να εκτελεσθεί ένας συνδυασμός αυτών των προσεγγίσεων για να επιτευχθεί πλήρης εκτίμηση Επιπέδου 1. Η δομή αυτών των επιπέδων απεικονίζεται στο επόμενο Σχήμα 23**Error! Reference source not found.**.

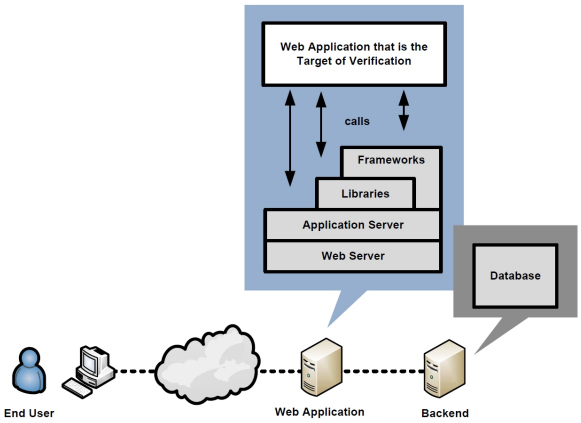
[34] Target of Verification (TOV). - Εάν εκτελούμε μια επαλήθευση ασφάλειας εφαρμογών σύμφωνα με τις απαιτήσεις του OWASP ASVS, η επαλήθευση θα είναι μιας συγκεκριμένης εφαρμογής. Αυτή η εφαρμογή καλείται "Στόχος της Επαλήθευσης- Target of Verification " ή απλά του TOV.

[35] Για περισσότερες πληροφορίες σχετικά με τον προσδιορισμό των κινδύνων και την εκτίμηση των κινδύνων που συνδέονται με τις ευπάθειες, ανατρέξτε στο Κεφάλαιο 3.2 OWASP Testing Guide (OWASP, 2008).



Σχήμα 23. Επίπεδα 1, 1Α και 1Β του OWASP ASVS.

Στο Επίπεδο 1, τα τμήματα της εφαρμογής μπορούν να καθοριστούν είτε από μεμονωμένα αρχεία πηγής, είτε από ομάδες αρχείων πηγής, βιβλιοθήκες ή/και εκτελέσιμα αρχεία, όπως απεικονίζονται στο Σχήμα 24. Στο Επίπεδο 1, η λίστα δεν χρειάζεται να ταξινομηθεί ή να οργανωθεί αλλιώς, όμως χρειάζεται να προσδιοριστεί ποια συστατικά είναι μέρος της εφαρμογής και ποια συστατικά είναι μέρος του περιβάλλοντος πληροφοριακής τεχνολογίας (IT). Η εφαρμογή μπορεί έπειτα να αντιμετωπιστεί ως ομάδες συστατικών μέσα σε μια ενιαία μονολιθική οντότητα. Το μονοπάτι (path) ή τα μονοπάτια, που η αίτηση ενός τελικού χρήστη ίσως ακολουθήσει μέσα στην εφαρμογή, δεν χρειάζεται να προσδιορισθεί και να τεκμηριωθεί.



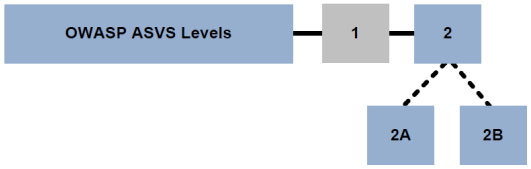
Σχήμα 24. Παράδειγμα Αρχιτεκτονικής Ασφάλειας Επίπεδο 1 OWASP ASVS.

- **Επίπεδο 1Α - Δυναμική Ανίχνευση (Μερικώς Αυτοματοποιημένη Επαλήθευση)**
  Απαιτήσεις Επαλήθευσης Ελέγχου Ασφάλειας Δυναμικής Ανίχνευσης: Η δυναμική ανίχνευση (επίσης γνωστή ως «ανίχνευση ευπάθειας εφαρμογών») αποτελείται από τη χρήση αυτοματοποιημένων εργαλείων τα οποία προσπελαύνουν τις διεπαφές εφαρμογής, ενώ η εφαρμογή «τρέχει», προκειμένου να ανιχνευθούν ευπάθειες στους ελέγχους ασφάλειας της εφαρμογής. Πρέπει να επισημανθεί ότι γενικώς δεν είναι αρκετό να επαληθευθεί ο σωστός σχεδιασμός, η υλοποίηση και η χρήση ενός ελέγχου ασφάλειας, αλλά αυτός ο έλεγχος αποτελεί αποδεκτή επαλήθευση για το Επίπεδο 1. Η εμβέλεια της επαλήθευσης καθορίζεται από τις απαιτήσεις της αρχιτεκτονικής της ασφάλειας αυτού του Επιπέδου. Πολλαπλά στιγμιότυπα ενός συγκεκριμένου τύπου ευπάθειας, τα οποία μπορεί να εντοπισθούν σε μια ενιαία πρωταρχική αιτία, θα πρέπει να συνδυαστούν με μια συγκεκριμένη εύρεση εάν το εργαλείο ανίχνευσης δεν το έχει κάνει ήδη.
- **Επίπεδο 1Β - Ανίχνευση Πηγαίου Κώδικα (Μερικώς Αυτοματοποιημένη Επαλήθευση)**
  Απαιτήσεις Επαλήθευσης Ελέγχου Ασφάλειας Επιθεώρησης Πηγαίου Κώδικα: Η επιθεώρηση πηγαίου κώδικα (επίσης γνωστή ως «στατική ανάλυση») αποτελείται από τη χρήση αυτοματοποιημένων εργαλείων τα

οποία αναζητούν μέσα στον πηγαίο κώδικα της εφαρμογής για να βρουν τα μοτίβα (patterns) που αντιπροσωπεύουν ευπάθειες. Πρέπει να επισημανθεί ότι γενικώς δεν είναι αρκετό να επαληθευθεί ο σωστός σχεδιασμός, η υλοποίηση και η χρήση ενός ελέγχου ασφάλειας, αλλά αυτός ο έλεγχος αποτελεί αποδεκτή επαλήθευση για το Επίπεδο 1. Η εμβέλεια της επαλήθευσης καθορίζεται από τις απαιτήσεις της αρχιτεκτονικής της ασφάλειας αυτού του Επιπέδου. Πολλαπλά στιγμιότυπα ενός συγκεκριμένου τύπου ευπάθειας τα οποία μπορεί να εντοπισθούν σε μια ενιαία πρωταρχική αιτία, θα πρέπει να συνδυαστούν με μια συγκεκριμένη εύρεση εάν το εργαλείο ανάλυσης κώδικα δεν το έχει κάνει ήδη.

2. **Επίπεδο 2 - Χειροκίνητη Επαλήθευση (Manual Verification)**

Το Επίπεδο 2 είναι κατάλληλο για εφαρμογές που χειρίζονται προσωπικές συναλλαγές, διεξάγουν ενδοεπιχειρησιακές συναλλαγές, προσπελαύνουν πληροφορίες πιστωτικών καρτών, ή επεξεργάζονται προσωπικές πληροφορίες. Το Επίπεδο 2 παρέχει μερική εμπιστοσύνη στη σωστή χρήση των ελέγχων ασφάλειας, καθώς και εμπιστοσύνη ότι οι έλεγχοι ασφάλειας λειτουργούν σωστά. Οι απειλές στην ασφάλεια θα είναι συνήθως κάποιοι ιοί, σκουλήκια, αλλά και επιτιθέμενοι με επαγγελματικά ή ανοικτού κώδικα εργαλεία επίθεσης. Η εμβέλεια της επαλήθευσης περιλαμβάνει όλο τον κώδικα που αναπτύσσεται ή τροποποιείται για την εφαρμογή, εξετάζοντας παράλληλα την ασφάλεια όλων των τμημάτων τρίτων οντοτήτων που παρέχουν λειτουργικότητα ασφάλειας για την εφαρμογή. Υπάρχουν δύο τμήματα για το Επίπεδο 2, όπως απεικονίζονται στο Σχήμα 25.

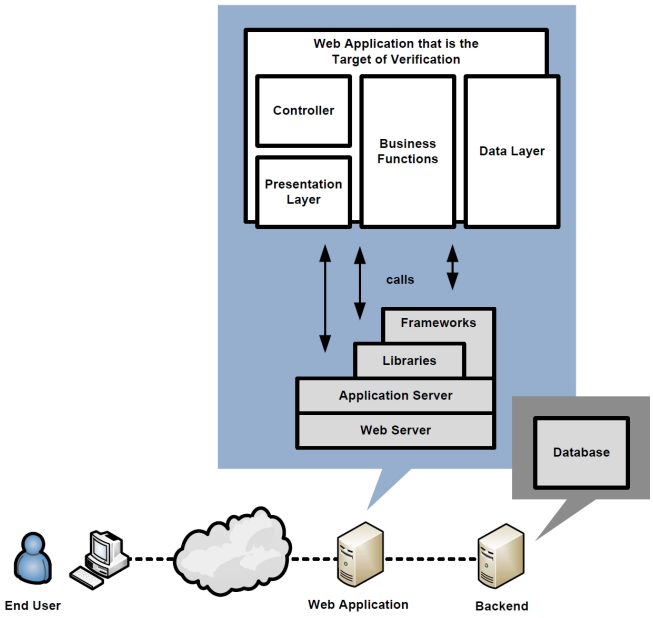


Σχήμα 25. Επίπεδα 2, 2A και 2B του OWASP ASVS.

Ενώ μπορεί να καθοριστεί ότι μια εφαρμογή καλύπτει τις απαιτήσεις είτε του Επιπέδου 2A είτε του 2B, κανένα όμως από αυτά τα επίπεδα δεν παρέχει από μόνο του, το ίδιο επίπεδο αυστηρότητας ή κάλυψης όπως το Επίπεδο 2. Επιπλέον, ενώ το Επίπεδο 2 είναι υπερσύνολο του Επιπέδου 1, δεν υπάρχει απαίτηση να χρησιμοποιηθεί ένα αυτοματοποιημένο εργαλείο για να καλύψει τις απαιτήσεις του Επίπεδου 2. Αντί αυτού, ο ελεγκτής έχει την επιλογή να χρησιμοποιήσει χειροκίνητες τεχνικές για όλες τις απαιτήσεις. Εάν τα αποτελέσματα των αυτοματοποιημένων εργαλείων είναι διαθέσιμα, ο ελεγκτής μπορεί να τα χρησιμοποιήσει για να υποστηρίξει την ανάλυση. Εντούτοις, ακόμη και όταν καλυφθεί μια απαίτηση στο Επίπεδο 1, δεν υποδεικνύει αυτόματα την κάλυψη της ίδιας απαίτησης στο Επίπεδο 2. Αυτό συμβαίνει διότι τα αυτοματοποιημένα εργαλεία δεν παρέχουν επαρκή στοιχεία που να αποδεικνύουν ότι η επιθυμητή απαίτηση έχει καλυφθεί. Οι χειροκίνητες τεχνικές υποτίθεται ότι χρησιμοποιούν εργαλεία. Αυτό μπορεί να περιλαμβάνει τη χρήση οποιουδήποτε είδους εργαλείου ανάλυσης ή ελέγχου ασφάλειας, συμπεριλαμβανομένων των αυτοματοποιημένων εργαλείων που χρησιμοποιούνται για τις επαληθεύσεις Επιπέδου 1. Εντούτοις, αυτά τα εργαλεία απλά υποστηρίζουν τον αναλυτή ώστε να βρει και να αξιολογήσει τους ελέγχους ασφάλειας που επαληθεύονται. Τέτοια εργαλεία μπορεί να περιέχουν ή να μην περιέχουν, λογική στην αυτόματη ανίχνευση ευπαθειών της εφαρμογής.

Στο Επίπεδο 2, τα τμήματα της εφαρμογής μπορούν να καθοριστούν είτε από μεμονωμένα, είτε από ομάδες πηγαίων αρχείων, βιβλιοθήκες ή/και εκτελέσιμα

αρχεία, τα οποία οργανώνονται με μια υψηλού επιπέδου αρχιτεκτονική (όπως, τμήματα Μοντέλο - Όψη - Ελεγκτής (MVC[36]), τμήματα επιχειρησιακής λειτουργίας και τμήματα επιπέδου δεδομένων). Παραδείγματος χάριν, το Σχήμα 26 παρακάτω απεικονίζει μια εφαρμογή που αποτελείται από μια εφαρμογή εξυπηρέτη, μια εφαρμογή της εφαρμογής εξυπηρέτη, έναν κοινό κώδικα, τις βιβλιοθήκες και μια εφαρμογή βάσεων δεδομένων που ομαδοποιούνται σύμφωνα με μια αρχιτεκτονική MVC. Στο Επίπεδο 2, το μονοπάτι (path) ή μονοπάτια, που η αίτηση ενός τελικού χρήστη ίσως ακολουθήσει μέσα στην εφαρμογή, πρέπει να τεκμηριωθεί. Εντούτοις, δεν είναι απαραίτητο να εξεταστούν όλα αυτά τα μονοπάτια.



Σχήμα 26. Παράδειγμα Αρχιτεκτονικής Ασφάλειας Επίπεδο 2 OWASP ASVS.

- **Επίπεδο 2A - Έλεγχος Ασφάλειας (Μερικώς Χειροκίνητη Επαλήθευση)** Απαιτήσεις Επαλήθευσης Ελέγχου Ασφάλειας Χειροκίνητου Ελέγχου Διείσδυσης Εφαρμογών: Ο χειροκίνητος έλεγχος ασφάλειας εφαρμογών αποτελείται από τη δημιουργία δυναμικών ελέγχων προκειμένου να ελεγχθεί ο σχεδιασμός, η υλοποίηση και η χρήση ελέγχων ασφάλειας που είναι κατάλληλα για μια εφαρμογή. Η εμβέλεια της επαλήθευσης καθορίζεται από τις απαιτήσεις της αρχιτεκτονικής της ασφάλειας αυτού του Επιπέδου. Όπου είναι απαραίτητο, ο ελεγκτής μπορεί να χρησιμοποιήσει δειγματοληψία ώστε να καθιερώσει την αποτελεσματική χρήση ενός ελέγχου ασφάλειας. Ο ελεγκτής μπορεί να επιλέξει να τεκμηριώσει ένα μοτίβο ευπάθειας που θα επιτρέψει στους υπεύθυνους ανάπτυξης να βρουν με βεβαιότητα και να διορθώσουν όλα τα στιγμιότυπα του μοτίβου στο λογισμικό. Τα πολλαπλά στιγμιότυπα ενός μοτίβου ευπάθειας, τα οποία μπορεί να εντοπισθούν σε μια ενιαία πρωταρχική αιτία, θα πρέπει να συνδυαστούν με μια συγκεκριμένη εύρεση.
- **Επίπεδο 2B - Επισκόπηση Κώδικα (Μερικώς Χειροκίνητη Επαλήθευση)** Απαιτήσεις Επαλήθευσης Ελέγχου Ασφάλειας Χειροκίνητης Επισκόπησης Κώδικα: Η χειροκίνητη επισκόπηση κώδικα αποτελείται από την έρευνα και την ανάλυση του πηγαίου κώδικα της εφαρμογής προκειμένου να επαληθευθεί

[36] MVC (Model-View-Controller): Κύριο χαρακτηριστικό του συγκεκριμένου μοντέλου, είναι ότι χωρίζεται η εφαρμογή σε τρία διαφορετικά υποσυστήματα. Το Μοντέλο, την Όψη και τον Ελεγκτή. Κάθε ένα από αυτά, λειτουργεί αυτόνομα αλλά επικοινωνεί με τα υπόλοιπα δυο υποσυστήματα.

ο σχεδιασμός, η υλοποίηση και η κατάλληλη χρήση των ελέγχων ασφάλειας της εφαρμογής. Μια τέτοια ανάλυση αναμένεται ότι θα πρέπει να υποστηριχθεί από εργαλεία, όμως θα μπορούσε απλά να περιλαμβάνει τα κοινώς διαθέσιμα εργαλεία όπως ένας συντάκτης πηγαίου κώδικα ή ένα IDE[37]. Η εμβέλεια της επαλήθευσης καθορίζεται από τις απαιτήσεις της αρχιτεκτονικής της ασφάλειας αυτού του Επιπέδου. Όπου είναι απαραίτητο, ο ελεγκτής μπορεί να χρησιμοποιήσει μια κατάλληλη δειγματοληπτική μέθοδο για να καθιερώσει την αποτελεσματική χρήση ενός ελέγχου ασφάλειας. Ο ελεγκτής μπορεί να επιλέξει να τεκμηριώσει ένα μοτίβο ευπάθειας που θα επιτρέψει στους υπεύθυνους ανάπτυξης να βρουν με βεβαιότητα και να διορθώσουν όλα τα στιγμιότυπα του μοτίβου ευπάθειας στο λογισμικό. Τα πολλαπλά στιγμιότυπα ενός μοτίβου ευπάθειας, τα οποία μπορεί να εντοπισθούν σε μια ενιαία πρωταρχική αιτία, θα πρέπει να συνδυαστούν με μια συγκεκριμένη εύρεση.

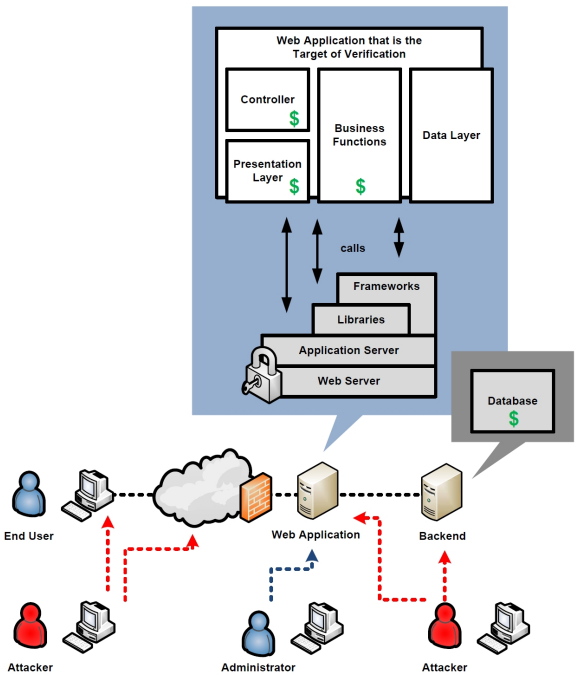
3. **Επίπεδο 3 - Επαλήθευση Σχεδιασμού (Design Verification)**

Το Επίπεδο 3 είναι κατάλληλο για εφαρμογές που χειρίζονται σημαντικές ενδοεπιχειρησιακές συναλλαγές, συμπεριλαμβανομένων εκείνων που επεξεργάζονται πληροφορίες υγειονομικής περίθαλψης, εφαρμόζουν λειτουργίες κρίσιμες για την επιχείρηση, ή επεξεργάζονται άλλα ευαίσθητα αγαθά. Οι απειλές στην ασφάλεια θα είναι συνήθως κάποιοι ιοί, σκουλήκια και ενδεχομένως προσδιορισμένοι επιτιθέμενοι (δηλαδή, ειδικευμένοι επιτιθέμενοι που εστιάζουν σε συγκεκριμένους στόχους χρησιμοποιώντας εργαλεία, συμπεριλαμβανομένων των εργαλείων ανίχνευσης που έχουν κατασκευαστεί γι' αυτό το λόγο). Η εμβέλεια της επαλήθευσης περιλαμβάνει όλο τον κώδικα που αναπτύσσεται ή τροποποιείται για την εφαρμογή, εξετάζοντας παράλληλα την ασφάλεια όλων των τμημάτων τρίτων οντοτήτων που παρέχουν λειτουργικότητα ασφάλειας για την εφαρμογή. Το Επίπεδο 3 εξασφαλίζει ότι οι ίδιοι οι έλεγχοι ασφάλειας λειτουργούν σωστά και ότι χρησιμοποιούνται οπουδήποτε χρειάζεται να εφαρμοσθούν μέσα στην εφαρμογή για να επιβάλουν συγκεκριμένες πολιτικές. Το Επίπεδο 3 δεν χωρίζεται σε πολλαπλά τμήματα, όπως απεικονίζεται στο επόμενο Σχήμα 27.

Σχήμα 27. Επίπεδο 3 του OWASP ASVS.

Στο Επίπεδο 3, τα τμήματα της εφαρμογής μπορεί να καθοριστούν είτε από μεμονωμένα, είτε από ομάδες πηγαίων αρχείων, βιβλιοθήκες ή/και εκτελέσιμα αρχεία, τα οποία ομαδοποιούνται με μια υψηλού επιπέδου αρχιτεκτονική (όπως, τμήματα MVC, τμήματα επιχειρησιακής λειτουργίας και τμήματα επιπέδου δεδομένων). Στο Επίπεδο 3, οι πληροφορίες που ενισχύουν τη διαμόρφωσης της απειλής σχετικά με πράκτορες και αγαθά απειλής, πρέπει επιπλέον να παρασχεθούν. Το μονοπάτι (path) ή μονοπάτια, που η αίτηση ενός τελικού χρήστη ίσως ακολουθήσει μέσω μιας υψηλού επιπέδου μοντελοποίησης της εφαρμογής, πρέπει να τεκμηριωθεί, όπως απεικονίζεται στο Σχήμα 28[38]. Στο Επίπεδο 3, όλα τα πιθανά μονοπάτια μέσω της υψηλού επιπέδου μοντελοποίησης της εφαρμογής πρέπει να εξεταστούν.

[37] Ένα ολοκληρωμένο περιβάλλον ανάπτυξης (integrated development environment, IDE) είναι μία σουίτα λογισμικού που βοηθάει στην ανάπτυξη προγραμμάτων υπολογιστή.
[38] Τα σύμβολα του δολαρίου δείχνουν τα αγαθά στο διάγραμμα.



Σχήμα 28. Παράδειγμα Αρχιτεκτονικής Ασφάλειας Επίπεδο 3 OWASP ASVS.

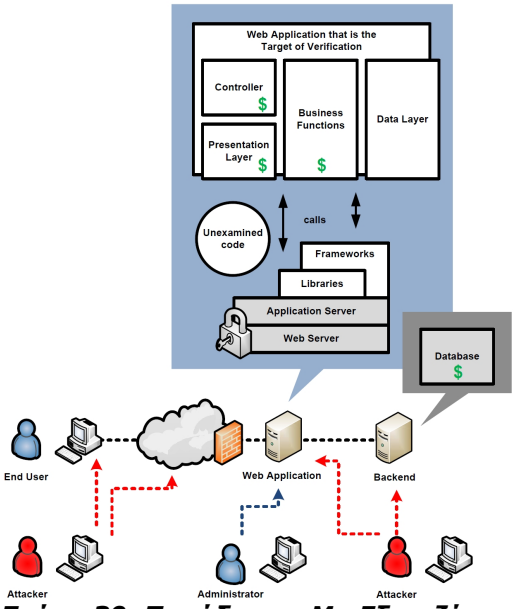
4. Επίπεδο 4 - Εσωτερική Επαλήθευση (Internal Verification)

Το Επίπεδο 4 είναι κατάλληλο για κρίσιμες εφαρμογές που προστατεύουν τη ζωή και την ασφάλεια, την κρίσιμη υποδομή, ή τις λειτουργίες άμυνας. Αυτό το επίπεδο μπορεί επίσης να είναι κατάλληλο για εφαρμογές που επεξεργάζονται ευαίσθητα αγαθά. Το Επίπεδο 4 εξασφαλίζει ότι οι ίδιοι οι έλεγχοι ασφάλειας λειτουργούν σωστά, ότι χρησιμοποιούνται οπουδήποτε χρειάζεται να εφαρμοσθούν μέσα στην εφαρμογή για να επιβάλουν συγκεκριμένες πολιτικές και ότι ακολουθήθηκαν οι πρακτικές ασφαλούς κωδικοποίησης. Οι απειλές στην ασφάλεια θα είναι συνήθως από κάποιους προσδιορισμένους επιτιθέμενους (δηλαδή, ειδικευμένοι επιτιθέμενοι που εστιάζουν σε συγκεκριμένους στόχους χρησιμοποιώντας εργαλεία συμπεριλαμβανομένων των εργαλείων ανίχνευσης που έχουν κατασκευαστεί γι' αυτό το λόγο). Η εμβέλεια της επαλήθευσης επεκτείνεται πέρα από την εμβέλεια του Επιπέδου 3, ώστε να περιλαμβάνει όλο τον κώδικα που χρησιμοποιείται από την εφαρμογή. Το Επίπεδο 4 δεν χωρίζεται σε τμήματα, όπως απεικονίζεται στο επόμενο Σχήμα 29.

Σχήμα 29. Επίπεδο 4 του OWASP ASVS.

Στο Επίπεδο 4, η αρχιτεκτονική της εφαρμογής θα καλυφθεί όπως και στο Επίπεδο 3. Επιπλέον, το Επίπεδο 4 απαιτεί ότι όλος ο κώδικας εφαρμογής, συμπεριλαμβανομένου του κώδικα που δεν εξετάζεται ρητά, προσδιορίζεται ως τμήμα του καθορισμού της εφαρμογής, όπως απεικονίζεται και στο Σχήμα 30. Αυτός ο κώδικας πρέπει να περιλαμβάνει όλες τις βιβλιοθήκες, τα πλαίσια και τον κώδικα που χρησιμοποιεί η εφαρμογή. Οι προηγούμενες επαληθεύσεις αυτών των τμημάτων μπορούν να επαναχρησιμοποιηθούν ως μέρος μιας άλλης προσπάθειας επαλήθευσης. Ο κώδικας πλατφόρμων, όπως το λειτουργικό σύστημα, η εικονική μηχανή, ή οι βιβλιοθήκες πυρήνα που συνοδεύουν έναν περιβάλλον εικονικής μηχανής, ένας εξυπηρέτης Ιστού, ή ένας εξυπηρέτης εφαρμογών, δεν συμπεριλαμβάνονται στο

Επίπεδο 4. Παραδείγματος χάριν, οι βιβλιοθήκες που συνδέονται με το χρόνο εκτέλεσης Java δεν θα πρέπει να αξιολογηθούν στο Επίπεδο 4.

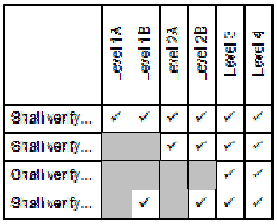


Σχήμα 30. Παράδειγμα Μη Εξεταζόμενου Κώδικα στο Επίπεδο 4 OWASP ASVS.

3.3.4 Βασική μεθοδολογία ασφάλειας

3.3.4.1 Λεπτομερείς Απαιτήσεις Επαλήθευσης

Αυτό το τμήμα του προτύπου ASVS του OWASP καθορίζει τις λεπτομερείς απαιτήσεις της επαλήθευσης, οι οποίες προέκυψαν από τις υψηλού επιπέδου απαιτήσεις που ίσχυαν για κάθε ένα από τα επίπεδα επαλήθευσης που καθορίστηκαν σε αυτό το πρότυπο. Κάθε τμήμα καθορίζει ένα σύνολο λεπτομερών απαιτήσεων επαλήθευσης που ομαδοποιούνται σε σχετικές περιοχές.



Σχήμα 31. Παράδειγμα πίνακα που καθορίζει τις αντίστοιχες απαιτήσεις επαλήθευσης που ισχύουν για κάθε ένα από τα 4 επίπεδα επαλήθευσης

Το ASVS προσδιορίζει τις ακόλουθες περιοχές απαιτήσεων για την ασφάλεια:

- V1 - Απαιτήσεις Τεκμηρίωσης Αρχιτεκτονικής Ασφάλειας[39] (Security Architecture Documentation Requirements): Για όλα τα επίπεδα του ASVS, η τεκμηρίωση κάποιων βασικών πληροφοριών της αρχιτεκτονικής της ασφάλειας είναι απαραίτητη για να εξασφαλισθεί και η πληρότητα και η ακρίβεια (αλλά και η επανάληψη των ελέγχων όταν απαιτείται επανόρθωση) της επαλήθευσης της ασφάλειας της εφαρμογής που εκτελείται. Η ανάλυση μπορεί να κατευθυνθεί και τα αποτελέσματα μπορούν να εντοπιστούν στην

[39] Αρχιτεκτονική ασφάλειας (Security Architecture) - Μια αφαίρεση του σχεδιασμού μιας εφαρμογής Ιστού που προσδιορίζει και περιγράφει που και πώς χρησιμοποιούνται οι έλεγχοι ασφάλειας, καθώς επίσης προσδιορίζει και περιγράφει τη θέση και την ευαισθησία και του χρήστη και των δεδομένων της εφαρμογής.

υψηλού επιπέδου αρχιτεκτονική ασφάλειας της εφαρμογής. Αυτές οι απαιτήσεις αρχίζουν με ένα βασικό επίπεδο λεπτομέρειας της αρχιτεκτονικής της ασφάλειας που πρέπει να καλυφθεί. Το συγκεκριμένο επίπεδο λεπτομέρειας αυξάνεται σε κάθε επίπεδο.

- V2 - Απαιτήσεις Επαλήθευσης Αυθεντικοποίησης (Authentication Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Αυθεντικοποίησης καθορίζουν ένα σύνολο απαιτήσεων για την παραγωγή και τον χειρισμό πιστοποιητικών λογαριασμού με ασφάλεια.
- V3 - Απαιτήσεις Επαλήθευσης Διαχείρισης Συνόδου (Session Management Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Διαχείρισης Συνόδου καθορίζουν ένα σύνολο απαιτήσεων για την ασφαλή χρησιμοποίηση αιτήσεων, αποκρίσεων, συνόδων, cookies και επικεφαλίδων HTTP αλλά και για την καταγραφή ώστε να γίνεται κατάλληλη διαχείριση των συνόδων.
- V4 - Απαιτήσεις Επαλήθευσης Ελέγχου Πρόσβασης (Access Control Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Ελέγχου Πρόσβασης καθορίζουν το πώς μια εφαρμογή μπορεί με ασφάλεια να ενεργοποιήσει τον έλεγχο πρόσβασης[40]. Στις περισσότερες εφαρμογές, ο έλεγχος πρόσβασης πρέπει να εκτελεσθεί σε πολλές διαφορετικές θέσεις στα διάφορα επίπεδα της εφαρμογής. Αυτές οι απαιτήσεις καθορίζουν τις απαιτήσεις επαλήθευσης που πρέπει να ισχύουν για ελέγχους πρόσβασης σε URLs, επιχειρησιακές λειτουργίες, δεδομένα, υπηρεσίες και αρχεία.
- V5 - Απαιτήσεις Επαλήθευσης Επικύρωσης Εισόδου (Input Validation Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Επικύρωσης Εισόδου καθορίζουν ένα σύνολο απαιτήσεων για την επικύρωση της εισόδου δεδομένων έτσι ώστε να είναι ασφαλές να χρησιμοποιηθούν μέσα σε μια εφαρμογή.
- V6 - Απαιτήσεις Επαλήθευσης Κωδικοποίησης ή Κατάλληλης Χρήσης Σημειώσεων Διαφυγής στην Έξοδο (Output Encoding/Escaping Verification Requirements): Η Απαιτήσεις Επαλήθευσης Κωδικοποίησης ή Κατάλληλης Χρήσης Σημειώσεων Διαφυγής στην Έξοδο καθορίζουν ένα σύνολο απαιτήσεων που χρησιμοποιείται για να επαληθεύσει ότι η έξοδος δεδομένων κωδικοποιείται κατάλληλα έτσι ώστε να είναι ασφαλής για εξωτερικές εφαρμογές.
- V7 - Απαιτήσεις Επαλήθευσης Κρυπτογράφησης (Cryptography Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Κρυπτογράφησης καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει την κρυπτογράφηση, τη διαχείριση κλειδιού, την παραγωγή τυχαίων αριθμών και τις διαδικασίες hashing μιας εφαρμογής. Οι εφαρμογές πρέπει πάντα να

[40] Έλεγχος Πρόσβασης (Access Control) - Ένα μέσο περιορισμού της πρόσβασης σε αρχεία, λειτουργίες, URLs και δεδομένα που βασίζονται στην ταυτότητα των χρηστών ή/και των ομάδων στην οποία ανήκουν.

χρησιμοποιήσουν ενότητες (modules) κρυπτογράφησης[41] επικυρωμένες σύμφωνα με το πρότυπο FIPS 140-2[42].

- V8 - Απαιτήσεις Επαλήθευσης Καταγραφής και Χειρισμού Σφαλμάτων (Error Handling and Logging Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Καταγραφής και Χειρισμού Σφαλμάτων καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει την ανίχνευση γεγονότων που σχετίζονται με την ασφάλεια και την αναγνώριση της συμπεριφοράς της επίθεσης.
- V9 - Απαιτήσεις Επαλήθευσης Προστασίας Δεδομένων (Data Protection Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Προστασίας των Δεδομένων καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει την προστασία των ευαίσθητων δεδομένων (π.χ., αριθμός πιστωτικής κάρτας, αριθμός διαβατηρίου, πληροφορίες προσωπικών δεδομένων).
- V10 - Απαιτήσεις Επαλήθευσης Ασφάλειας Επικοινωνιών (Communication Security Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Ασφάλειας Επικοινωνιών καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει ότι όλες οι επικοινωνίες με μια εφαρμογή είναι ασφαλείς.
- V11 - Απαιτήσεις Επαλήθευσης Ασφάλειας HTTP (HTTP Security Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Ασφάλειας HTTP καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει την ασφάλεια που σχετίζεται με τις HTTP αιτήσεις, τις αποκρίσεις, τις συνόδους, τα cookies, τις επικεφαλίδες και την καταγραφή.
- V12 - Απαιτήσεις Επαλήθευσης Διαμόρφωσης Ασφάλειας (Security Configuration Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Διαμόρφωσης της Ασφάλειας καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να χρησιμοποιηθεί για να επαληθεύσει την ασφαλή αποθήκευση όλων των πληροφοριών διαμόρφωσης που κατευθύνουν την ασφαλή συμπεριφορά της εφαρμογής. Η προστασία αυτών των πληροφοριών διαμόρφωσης είναι κρίσιμη για την ασφαλή λειτουργία της εφαρμογής.
- V13 - Απαιτήσεις Επαλήθευσης Αναζήτησης Κακόβουλου Κώδικα (Malicious Code Search Verification Requirements): Για το Επίπεδο 4, απαιτείται η αναζήτηση για κακόβουλο κώδικα[43] σε οποιοδήποτε κώδικα δεν έχει εξετασθεί ακόμα, αφού έχει εκτελεσθεί μια επαλήθευση εφαρμογής Επιπέδου 3.
- V14 - Απαιτήσεις Επαλήθευσης Εσωτερικής Ασφάλειας (Internal Security Verification Requirements): Οι Απαιτήσεις Επαλήθευσης Εσωτερικής Ασφάλειας καθορίζουν ένα σύνολο απαιτήσεων που μπορεί να

[41] Ενότητα κρυπτογράφησης - υλικό, λογισμικό ή/και firmware (λογισμικό συσκευών) που εφαρμόζει αλγόριθμους κρυπτογράφησης ή/και παράγει κλειδιά κρυπτογράφησης.
[42] Το Ομοσπονδιακό Πρότυπο Επεξεργασίας Πληροφοριών (Federal Information Processing Standard-FIPS) έκδοση 140-2, είναι ένα πρότυπο ασφάλειας υπολογιστών της κυβέρνησης των ΗΠΑ, που χρησιμοποιείται για να προσδιορίσει ενότητες κρυπτογράφησης.
(http://csrc.nist.gov/groups/STM/cmvp/validation.html).
[43] Κακόβουλος κώδικας (malicious code) - Πηγαίος κώδικας που εισάγεται σε μια εφαρμογή Ιστού κατά τη διάρκεια της ανάπτυξής της, χωρίς τη γνώση του ιδιοκτήτη της εφαρμογής Ιστού.

χρησιμοποιηθεί για να επαληθεύσει ότι η εφαρμογή προστατεύεται ως έναν βαθμό ενάντια στις ατέλειες της υλοποίησης.

Ο παρακάτω πίνακας παρουσιάζει συνολικά τον αριθμό των απαιτήσεων επαλήθευσης που ισχύουν για κάθε ένα από τα τέσσερα επίπεδα επαλήθευσης.

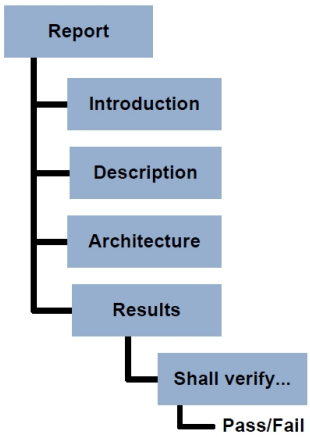
Security Area	Level 1A	Level 1B	Level 2A	Level 2B	Level 3	Level 4
V1 – Security Architecture Verification Requirements	1	1	2	2	4	5
V2 – Authentication Verification Requirements	3	2	9	13	13	14
V3 – Session Management Verification Requirements	4	1	6	7	8	9
V4 – Access Control Verification Requirements	5	1	12	13	14	15
V5 – Input Validation Verification Requirements	3	1	5	7	8	9
V6 – Output Encoding/Escaping Verification Requirements	0	1	2	8	9	10
V7 – Cryptography Verification Requirements	0	0	2	8	9	10
V8 – Error Handling and Logging Verification Requirements	1	1	2	8	8	9
V9 – Data Protection Verification Requirements	1	1	2	3	4	4
V10 – Communication Security Verification Requirements	1	0	3	6	8	8
V11 – HTTP Security Verification Requirements	3	3	6	6	7	7
V12 – Security Configuration Verification Requirements	0	0	0	2	3	4
V13 – Malicious Code Search Verification Requirements	0	0	0	0	0	5
V14 – Internal Security Verification Requirements	0	0	0	0	1	3
Totals	22	12	51	83	96	112

Πίνακας 11. Περίληψη απαιτήσεων

3.3.4.2 Απαιτήσεις Έκθεσης Επαλήθευσης

Μια έκθεση του ASVS του OWASP περιέχει μια περιγραφή της εφαρμογής που αναλύθηκε ως προς τις απαιτήσεις του OWASP ASVS για ένα δεδομένο επίπεδο. Η έκθεση τεκμηριώνει επίσης τα αποτελέσματα της ανάλυσης, συμπεριλαμβάνοντας οποιαδήποτε επανόρθωση ευπαθειών που πιθανώς απαιτήθηκε. Οι απαιτήσεις για την υποβολή έκθεσης του ASVS καθορίζουν το είδος των πληροφοριών που χρειάζεται να υπάρχουν στην έκθεση. Οι συγκεκριμένες απαιτήσεις δεν καθορίζουν τη δομή, την οργάνωση ή τη μορφή της έκθεσης. Επιπλέον, οι απαιτήσεις αυτές δεν αποκλείουν κάποιες πρόσθετες πληροφορίες που ίσως συμπεριληφθούν στην έκθεση.

Το είδος πληροφοριών που απαιτείται από κάθε σύνολο απαιτήσεων για την υποβολή έκθεσης του ASVS μπορεί να κατονομαστεί, να σχηματοποιηθεί και να οργανωθεί σύμφωνα με τις απαιτήσεις ενός ελεγκτή. Οι απαιτήσεις της έκθεσης του ASVS καλύπτονται, εφ' όσον υπάρχουν οι απαραίτητες πληροφορίες. Μια έκθεση πρέπει να περιλαμβάνει όλο το απαραίτητο υλικό για έναν αναγνώστη, το οποίο θα τον βοηθήσει να κατανοήσει την ανάλυση που εκτελέσθηκε και τα αποτελέσματα της ανάλυσης, συμπεριλαμβάνοντας τις πληροφορίες διαμόρφωσης και κομμάτια κώδικα (code snippets), που ίσως να χρησιμοποιηθούν κατά την κατασκευή της περίληψης της έκθεσης.



Σχήμα 32. Περιεχόμενο της Έκθεσης.

Οι απαιτήσεις παρουσιάζονται στη συνέχεια:

1. R1 - Εισαγωγή Έκθεσης (Report Introduction)
    - R1.1 - Η εισαγωγή της έκθεσης θα παρέχει ικανοποιητικές πληροφορίες για να προσδιορίσει και την έκθεση και την εφαρμογή, που αποτελεί το αντικείμενο της έκθεσης.
    - R1.2 - Η εισαγωγή της έκθεσης θα συνοψίσει τη συνολική εμπιστοσύνη στην ασφάλεια της εφαρμογής.
    - R1.3 - Η εισαγωγή της έκθεσης θα προσδιορίσει τους βασικούς επιχειρησιακούς κινδύνους που συνδέονται με τη λειτουργία της εφαρμογής.
    - R1.4 - Η εισαγωγή της έκθεσης θα προσδιορίσει τους κανόνες δέσμευσης που συνδέονται με την εκτέλεση της επαλήθευσης ή αυτούς που μπορεί να έχουν περιορίσει την εμβέλεια της επαλήθευσης.
2. R2 - Περιγραφή Εφαρμογής (Application Description)
    - R2.1 - Η περιγραφή εφαρμογής θα παρέχει μια ικανοποιητική περιγραφή της εφαρμογής, προκειμένου να βοηθήσει στην κατανόηση της λειτουργίας της και του περιβάλλοντος στο οποίο λειτουργεί.
3. R3 - Αρχιτεκτονική Ασφάλειας Εφαρμογής (Application Security Architecture)
    - R3.1 - Η αρχιτεκτονική ασφάλειας της εφαρμογής θα παρέχει πρόσθετη λεπτομέρεια κατά την περιγραφή της εφαρμογής και επιπλέον θα παρέχει στον αναγνώστη της έκθεσης την βεβαιότητα ότι η ανάλυση που εκτελέσθηκε ήταν και πλήρης, αλλά και ακριβής. Αυτό το μέρος της έκθεσης παρέχει το πλαίσιο για την ανάλυση. Οι πληροφορίες που παρουσιάζονται σε αυτό το τμήμα, θα χρησιμοποιηθούν κατά τη διάρκεια της ανάλυσης για να προσδιορίσουν τις ασυνέπειες. Αυτό το μέρος της έκθεσης θα ενσωματώνει διαφορετικά επίπεδα λεπτομέρειας, ανάλογα με το Επίπεδο του ASVS του OWASP και θα επικυρώνει ότι η ανάλυση εκτελέσθηκε. Οι λεπτομέρειες θα ποικίλουν ανάλογα με το Επίπεδο.
4. R4 - Αποτελέσματα Επαλήθευσης (Verification Results)

- R4.1 - Τα αποτελέσματα της επαλήθευσης θα παρουσιάσουν τα αποτελέσματα της ανάλυσης που εκτελέσθηκε, σύμφωνα με την ενότητα «Απαιτήσεις Επαλήθευσης» αυτού του προτύπου, συμπεριλαμβάνοντας την περιγραφή οποιασδήποτε επανόρθωσης ευπαθειών που απαιτήθηκε.

3.3.4.3 Πώς ξεκινάμε να χρησιμοποιήσουμε το ASVS;

Παρακάτω, αναφέρονται τα βασικά σημεία που πρέπει να ακολουθηθούν όταν χρησιμοποιήσουμε το πρότυπο ASVS:

- Αγοραστής και πωλητής: συμφωνούν για το πώς οι τεχνικές απαιτήσεις της ασφάλειας θα επαληθευθούν με τον προσδιορισμό ενός επιπέδου από το 1 έως το 4.
- Εκτέλεση μιας αρχικής επισκόπησης της εφαρμογής που επαληθεύεται,
  - Ελάχιστο: Θα πρέπει τουλάχιστον να εκτελεσθεί μια επισκόπηση αρχιτεκτονικής ασφάλειας Επιπέδου 1 του ASVS.
- Ανάπτυξη ενός σχεδίου επαλήθευσης και ενός χρονοδιαγράμματος έργου,
- Εκτέλεση μιας επαλήθευσης σύμφωνα με τις απαιτήσεις του επιλεγμένου επιπέδου ASVS,
- Παρουσίαση των συμπερασμάτων.
- Ανάπτυξη και εκτέλεση μιας στρατηγικής επανόρθωσης.
- Επαν-επαλήθευση αφού γίνουν οι διορθώσεις (επανάληψη όπου είναι αναγκαίο).
- Ανάπτυξη μιας στρατηγικής που προσθέτει επαληθεύσεις στο SDLC ως κανονικές δραστηριότητες.

3.3.5 Συμπεράσματα

Εάν θεωρήσουμε ότι είμαστε έτοιμοι να σταματήσουμε τις ευπάθειες και να εστιάσουμε στην καθιέρωση ισχυρών ελέγχων για την ασφάλεια εφαρμογών, το OWASP έχει παράγει το Πρότυπο Επαλήθευσης Ασφάλειας Εφαρμογής (ASVS) που λειτουργεί σαν οδηγός για τους υπεύθυνους των οργανισμών και τους εφοδιάζει ώστε να κατανοήσουν το τι θα πρέπει να επαληθεύσουν. Το ASVS δημιουργήθηκε για να καθορίσει μια ορολογία προτύπου στη βιομηχανία που θα μετρά το επίπεδο ασφάλειας για τις εφαρμογές ή τα προϊόντα. Μόλις εξοικειωθεί ο καθένας με αυτήν την ορολογία, οι οργανισμοί θα μπορούν να αγοράζουν λογισμικό και να ξέρουν ότι συμμορφώνεται με ένα συγκεκριμένο προκαθορισμένο επίπεδο ασφάλειας. Επιπλέον, το λογισμικό θα μπορεί να είναι βέβαιο ότι συμμορφώνεται με αυτό το επίπεδο, επειδή επαληθεύθηκε σύμφωνα με τις απαιτήσεις του προτύπου.

Κεφάλαιο 4: Technical Guide to Information Security Testing and Assessment του NIST - SP 800-115

4.1 Εισαγωγή

4.1.1 Γενικά

Το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας των ΗΠΑ (NIST- National Institute of Standards and Technology) είναι γνωστό για την παραγωγή ενός ευρέως φάσματος καλογραμμένων και διεξοδικών τεχνικών προτύπων, τα οποία (αντίθετα από τα πρότυπα της σειράς ISO27k) είναι διαθέσιμα σε όλους ελεύθερα. Τα πρότυπα προορίζονται αρχικά για κυβερνητική (US), στρατιωτική και εμπορική χρήση, αλλά αξίζει τον κόπο να τα «κατεβάσει» κανείς και να τα υιοθετήσει ή να τα δοκιμάσει σε άλλα πλαίσια. Υπάρχει μια συλλογή με τα άριστα παγκοσμίως πρότυπα της SP[44] 800-σειράς του NIST, τα οποία είναι σχετικά με τη διαχείριση της ασφάλειας των πληροφοριών.

Το Εργαστήριο Τεχνολογίας Πληροφοριών (Information Technology Laboratory) του NIST δημοσίευσε ένα νέο οδηγό για να βοηθήσει τους οργανισμούς να διαχειριστούν τις αξιολογήσεις της ασφάλειας των πληροφοριών τους. Τον Σεπτέμβριο του 2008, ο οδηγός παρουσίασε τα βασικά στοιχεία του ελέγχου και των αξιολογήσεων της ασφάλειας, εξήγησε συγκεκριμένες τεχνικές που μπορούν να εφαρμοστούν και πρότεινε αποτελεσματικές μεθόδους για την υλοποίηση πρακτικών ελέγχου και αξιολόγησης. Το NIST ανέπτυξε αυτό το έγγραφο ως συνέχεια των νομικών ευθυνών του στο πλαίσιο του Νόμου Διαχείρισης Ασφάλειας Ομοσπονδιακών Πληροφοριών (FISMA-Federal Information Security Management Act[45]) του 2002, Δημόσιος Νόμος 107-347.

Το NIST SP 800-115, Τεχνικός Οδηγός για τον Έλεγχο και την Αξιολόγηση της Ασφάλειας Πληροφοριών (Technical Guide to Information Security Testing and Assessment), γράφτηκε από τους Karen Scarfone και Murugiah Souppaya του NIST, και τους Amanda Cody και Angela Orebaugh του Booz Allen Hamilton. Ο νέος οδηγός αντικαθιστά το NIST SP 800-42, το οποίο είναι ένας οδηγός που ασχολείται με τον έλεγχο της ασφάλειας δικτύων.

Επομένως, το έγγραφο του NIST SP 800-115 είναι ένας οδηγός που αναφέρεται στις βασικές τεχνικές πτυχές στη διαχείριση των αξιολογήσεων της ασφάλειας πληροφοριών. Παρουσιάζει μεθόδους τεχνικού ελέγχου και τεχνικές όπου ένας οργανισμός μπορεί να χρησιμοποιήσει ως μέρος μιας αξιολόγησης και προσφέρει επιπλέον ιδέες στους αξιολογητές, σχετικά με την εκτέλεση αυτών των τεχνικών και τον πιθανό αντίκτυπο που μπορεί να έχουν στα συστήματα και τα δίκτυα. Προκειμένου μια αξιολόγηση να είναι επιτυχής και να έχει θετική επίδραση στην ασφάλεια ενός συστήματος (και τελικά ολόκληρου του οργανισμού), θα πρέπει να υποστηρίζουν την τεχνική διαδικασία πρόσθετα στοιχεία πέρα από την εκτέλεση του ελέγχου. Επίσης, σε αυτόν τον οδηγό παρουσιάζονται διάφορες προτάσεις για

[44] SP (Special Publication) - ειδική δημοσίευση

[45] Η παράγραφος 3544 απαιτεί «περιοδικό έλεγχο και αξιολόγηση της αποτελεσματικότητας των πολιτικών ασφάλειας πληροφοριών, διαδικασιών και πρακτικών, που να εκτελείται με μια συχνότητα ανάλογα με τον κίνδυνο, αλλά τουλάχιστον να εκτελείται ετησίως.» Το FISMA είναι διαθέσιμο http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

αυτές τις δραστηριότητες, όπως η εύρωστη διαδικασία προγραμματισμού, η ανάλυση πρωταρχικών αιτιών και η προσαρμοσμένη έκθεση.

4.1.2 Βασικοί στόχοι

Οι διαδικασίες και η τεχνική καθοδήγηση που παρουσιάζονται στο έγγραφο του NIST SP 800-115 επιτρέπουν στους οργανισμούς:

- Να αναπτύξουν την πολιτική αξιολόγησης της ασφάλειας πληροφοριών, τη μεθοδολογία και τους μεμονωμένους ρόλους και τις ευθύνες που σχετίζονται με τις τεχνικές πτυχές της αξιολόγησης.
- Να σχεδιάσουν με ακρίβεια την αξιολόγηση της ασφάλειας τεχνικών πληροφοριών, παρέχοντας οδηγίες που καθορίζουν ποια συστήματα πρέπει να αξιολογηθούν, καθώς και να σχεδιάσουν την προσέγγιση για την αξιολόγηση, εξετάζοντας λογιστικές μελέτες, αναπτύσσοντας ένα σχέδιο αξιολόγησης και εξασφαλίζοντας ότι εξετάζονται νομικές και πολιτικές υποθέσεις.
- Να εκτελέσουν με ασφάλεια και αποτελεσματικά, μια αξιολόγηση της ασφάλειας τεχνικών πληροφοριών, χρησιμοποιώντας τις μεθόδους και τις τεχνικές που παρουσιάζει το NIST SP 800-115, αλλά και να ανταποκριθούν σε οποιαδήποτε γεγονότα που ίσως εμφανισθούν κατά τη διάρκεια της αξιολόγησης.
- Να χειριστούν κατάλληλα τα τεχνικά δεδομένα (συλλογή, αποθήκευση, μετάδοση και καταστροφή) σε όλη τη διαδικασία της αξιολόγησης.
- Να διεξάγουν ανάλυση και έκθεση για να «μεταφράσουν» τα τεχνικά συμπεράσματα σε ενέργειες μετριασμού του κινδύνου, οι οποίες θα βελτιώσουν την ασφάλεια του οργανισμού.

Οι πληροφορίες που παρουσιάζονται στο NIST SP 800-115, προορίζονται να χρησιμοποιηθούν για ποικίλους λόγους αξιολόγησης. Παραδείγματος χάριν, κάποιες αξιολογήσεις εστιάζουν στο να επαληθεύσουν ότι ένας συγκεκριμένος έλεγχος ασφάλειας (ή έλεγχοι) καλύπτει τις απαιτήσεις, ενώ άλλες προορίζονται για να προσδιορίσουν, να επικυρώσουν και να αξιολογήσουν τις εκμεταλλεύσιμες αδυναμίες της ασφάλειας ενός συστήματος. Οι αξιολογήσεις εκτελούνται επίσης για να αυξήσουν την ικανότητα ενός οργανισμού, προκειμένου να διατηρήσει μια δυναμική άμυνα του δικτύου υπολογιστών. Οι αξιολογήσεις δεν προορίζονται να αντικαταστήσουν την υλοποίηση των ελέγχων ασφάλειας και την διατήρηση της ασφάλειας των συστημάτων.

4.2 Εμβέλεια

Όπως αναφέρθηκε προηγουμένως, ο σκοπός του εγγράφου NIST SP 800-115 είναι να παρέχει οδηγίες στους οργανισμούς για τον σχεδιασμό και τη διαχείριση αξιολογήσεων και ελέγχων της ασφάλειας τεχνικών πληροφοριών, για την ανάλυση των συμπερασμάτων και για την ανάπτυξη στρατηγικών μετριασμού. Προβαίνει σε πρακτικές συστάσεις για το σχεδιασμό, την υλοποίηση και τη διατήρηση των τεχνικών πληροφοριών που σχετίζονται με τον έλεγχο της ασφάλειας και τις διαδικασίες αξιολόγησης, οι οποίες μπορούν να χρησιμοποιηθούν για διάφορους λόγους - όπως η εύρεση ευπαθειών σε ένα σύστημα ή ένα δίκτυο και η επαλήθευση συμμόρφωσης με μια πολιτική ή άλλες απαιτήσεις. Ο οδηγός NIST SP 800-115 δεν σκοπεύει να παρουσιάσει ένα διεξοδικό πρόγραμμα αξιολόγησης ή ελέγχου της ασφάλειας των πληροφοριών, αλλά μάλλον πρόκειται για μια επισκόπηση των βασικών στοιχείων του τεχνικού ελέγχου και της αξιολόγησης της ασφάλειας,

δίνοντας έμφαση σε συγκεκριμένες τεχνικές, στα οφέλη και στους περιορισμούς τους, καθώς και στις συστάσεις για τη χρήση τους.

Ο συγκεκριμένος οδηγός προορίζεται να χρησιμοποιηθεί από το προσωπικό ασφάλειας των υπολογιστών και τους διευθυντές προγράμματος, τους διαχειριστές συστημάτων και δικτύων, αλλά και οποιοδήποτε άλλο τεχνικό προσωπικό που είναι αρμόδιο για τις τεχνικές πτυχές της προετοιμασίας, της λειτουργίας και της εξασφάλισης των υποδομών των συστημάτων και δικτύων. Οι διευθυντές μπορούν επίσης να χρησιμοποιήσουν τις πληροφορίες που παρουσιάζονται, για να διευκολύνουν τις τεχνικές διαδικασίες λήψης αποφάσεων που συνδέονται με τους ελέγχους και τις αξιολογήσεις της ασφάλειας. Το υλικό στο NIST SP 800-115 είναι τεχνικά προσανατολισμένο και θεωρεί ότι οι αναγνώστες του έχουν τουλάχιστον μια βασική γνώση στην ασφάλεια συστημάτων και δικτύων.

4.3 Βασική μεθοδολογία ασφάλειας

4.3.1 Αξιολογήσεις της Ασφάλειας Πληροφοριών: Μεθοδολογίες και Τεχνικές

Η διαδικασία αξιολόγησης επιτρέπει στους οργανισμούς να καθορίσουν το πόσο αποτελεσματικά, τα τμήματα των συστημάτων πληροφοριών, επιτυγχάνουν τους συγκεκριμένους σκοπούς και στόχους της ασφάλειάς τους. Τα στοιχεία που μπορούν να αξιολογηθούν, γνωστά ως αντικείμενα αξιολόγησης, περιλαμβάνουν τον ξενιστή υπολογιστή (host), ολόκληρο το σύστημα, το δίκτυο, μια συγκεκριμένη διαδικασία, ή ένα πρόσωπο. Οι μέθοδοι αξιολόγησης που μπορούν να χρησιμοποιηθούν περιλαμβάνουν:

- **Έλεγχος (Testing):** δοκιμή ενός ή περισσότερων αντικειμένων αξιολόγησης υπό διευκρινισμένες συνθήκες ώστε να συγκριθούν οι πραγματικές και αναμενόμενες συμπεριφορές,
- **Εξέταση (Examination):** έλεγχος, επιθεώρηση, επισκόπηση, παρατήρηση, μελέτη, ή ανάλυση ενός ή περισσότερων αντικειμένων αξιολόγησης, για να διευκολυνθεί η κατανόηση, να επιτευχθεί η διευκρίνιση, ή να αποκτηθούν αποδεικτικά στοιχεία και
- **Συνέντευξη (Interviewing):** διαχείριση συζητήσεων με άτομα ή ομάδες μέσα σε έναν οργανισμό ώστε να διευκολυνθεί η κατανόηση, να επιτευχθεί η διευκρίνιση, ή να προσδιορισθεί η εύρεση των αποδεικτικών στοιχείων.

Οι οργανισμοί μπορεί να θελήσουν να χρησιμοποιήσουν περισσότερες από μια μεθοδολογίες στη διαχείριση των αξιολογήσεών τους. Κάποιες αποδεκτές μεθοδολογίες για τη διαχείριση των διαφορετικών τύπων αξιολογήσεων της ασφάλειας πληροφοριών παρατίθενται στο παράρτημα Ε[46] του οδηγού του NIST SP 800-115. Παραδείγματος χάριν, το NIST έχει δημιουργήσει μια μεθοδολογία - που τεκμηριώνεται στην Ειδική Δημοσίευση (SP-Special Publication) 800-53A, Οδηγός για την Αξιολόγηση των Ελέγχων Ασφάλειας σε Ομοσπονδιακά Συστήματα Πληροφοριών - ο οποίος προσφέρει προτάσεις για την αξιολόγηση της αποτελεσματικότητας των ελέγχων ασφάλειας που περιγράφονται στο NIST SP 800-

[46] Το NIST δεν προκρίνει κάποια μεθοδολογία σε σχέση με μια άλλη. Ο σκοπός είναι να παρέχει στους οργανισμούς τις κατάλληλες επιλογές που θα τους επιτρέψει να λάβουν ενημερωμένες αποφάσεις, προκειμένου να υιοθετήσουν μια υπάρχουσα μεθοδολογία ή να συνδυάσουν διάφορες, για να αναπτύξουν μια μοναδική μεθοδολογία που θα ταιριάζει στον οργανισμό.

53[47]. Μια άλλη ευρέως χρησιμοποιούμενη μεθοδολογία αξιολόγησης που παραπέμπεται στο παράρτημα Ε είναι το Εγχειρίδιο Μεθοδολογίας Ελέγχου Ασφάλειας Ανοικτού Κώδικα (OSSTMM), που αναπτύσσεται από το ISECOM, ίδρυμα για την ασφάλεια και τις ανοικτές μεθοδολογίες.

4.3.2 Σχεδιασμός, Διαχείριση και Εκτίμηση των Αξιολογήσεων της Ασφάλειας

Το NIST SP 800-115 χρησιμοποιεί μια σταδιακή μεθοδολογία αξιολόγησης της ασφάλειας πληροφοριών προκειμένου να επιτύχει πιο αποδοτική χρήση του προσωπικού και των πόρων του οργανισμού κατά την πραγματοποίηση των αξιολογήσεων της ασφάλειας πληροφοριών. Περιλαμβάνει τις ακόλουθες φάσεις:

- Στη φάση σχεδιασμού (planning phase), οι οργανισμοί συγκεντρώνουν τις πληροφορίες που απαιτούνται για να διαχειριστούν την αξιολόγηση και να καθιερώσουν την προσέγγιση της αξιολόγησης. Ένα σχέδιο διαχείρισης έργου πρέπει να αναπτυχθεί για να εξετάσει τους σκοπούς και τους στόχους, την εμβέλεια, τις απαιτήσεις, τους ρόλους και τις ευθύνες της ομάδας, τους περιορισμούς, τους παράγοντες επιτυχίας, τις υποθέσεις, τους πόρους, το χρονοδιάγραμμα και τα παραδοτέα.
  Σε αυτήν τη φάση, οι οργανισμοί αναπτύσσουν μια πολιτική αξιολόγησης της ασφάλειας για να παρέχουν καθοδήγηση στις δραστηριότητες αξιολόγησής τους. Ο σχεδιασμός θα πρέπει επίσης να περιλαμβάνει την απόφαση σχετικά με το ποια συστήματα πρέπει να αξιολογηθούν και σχετικά με τη συχνότητα των αξιολογήσεων. Αυτές οι αποφάσεις πρέπει να βασίζονται στις εκτιμήσεις κινδύνου, στα αναμενόμενα οφέλη, στις απαιτήσεις προγραμματισμού και στη διαθεσιμότητα των πόρων. Οι τεχνικές ελέγχου και εξέτασης πρέπει να επιλεχθούν σύμφωνα με τις απαιτήσεις και επιπλέον, πρέπει να αναπτυχθεί ένα σχέδιο που να τεκμηριώνει όλες τις δραστηριότητες και τους πόρους.
- Στη φάση εκτέλεσης (execution phase), οι οργανισμοί προσδιορίζουν τις ευπάθειες και τις επικυρώνουν, όπου χρειάζεται. Αυτή η φάση εξετάζει τις δραστηριότητες που συνδέονται με τις μεθόδους και τις τεχνικές αξιολόγησης που αποφασίστηκαν προηγουμένως, στη φάση σχεδιασμού και προσδιορίζονται στο σχέδιο αξιολόγησης ή ROE[48]. Οι δραστηριότητες μπορεί να διαφέρουν ανάλογα με τον τύπο αξιολόγησης, αλλά με την ολοκλήρωση αυτής της φάσης, οι αξιολογητές θα έχουν προσδιορίσει το σύστημα, το δίκτυο και τις ευπάθειες διαδικασίας.
  Ο κατάλληλος συντονισμός μέσα στον οργανισμό είναι ένας κυρίαρχος παράγοντας σε αυτήν την φάση που θα διευκολύνει τη διαδικασία αξιολόγησης και θα μειώσει τους κινδύνους. Εάν ένα γεγονός ασφάλειας ανιχνεύεται κατά τη διάρκεια της διαδικασίας αξιολόγησης, οι αξιολογητές πρέπει να ακολουθήσουν τις διαδικασίες της έκθεσης του οργανισμού για

[47] NIST SP 800-53A (Guide for Assessing the Security Controls in Federal Information Systems) - συζητά το πλαίσιο για την ανάπτυξη διαδικασιών αξιολόγησης, περιγράφει τη διαδικασία αξιολόγησης ελέγχων ασφάλειας και προσφέρει διαδικασίες αξιολόγησης για κάθε έλεγχο. Το NIST SP 800-53A αναπτύχθηκε για να χρησιμοποιηθεί από κοινού με το NIST SP 800-37, *Οδηγός για την Πιστοποίηση και την Διαπίστευση της Ασφάλειας των Ομοσπονδιακών Συστημάτων Πληροφοριών*. Τα NIST SPs 800-53, 800-53A και 800-37 είναι διαθέσιμα http://csrc.nist.gov/publications/PubsSPs.html

[48] Κανόνες δέσμευσης (Rules of Engagement-ROE): Λεπτομερείς οδηγίες και περιορισμοί σχετικά με την εκτέλεση του ελέγχου ασφάλειας πληροφοριών. Το ROE καθιερώνεται πριν από την έναρξη ενός ελέγχου ασφάλειας και δίνει στην ομάδα ελέγχου την εξουσιοδότηση να διαχειρίζεται τις καθορισμένες δραστηριότητες χωρίς την ανάγκη πρόσθετων δικαιωμάτων.

τέτοιες δραστηριότητες. Η ανάλυση των ευπαθειών πρέπει να πραγματοποιηθεί κατά τη διάρκεια της διαδικασίας αξιολόγησης και αφού έχει ολοκληρωθεί η αξιολόγηση. Αυτό επιτρέπει σε μεμονωμένες ευπάθειες να εξεταστούν αμέσως και επιτρέπει στον οργανισμό να αναλύσει τις πρωταρχικές αιτίες των ευπαθειών. Οι υπεύθυνοι μπορούν έπειτα να εξετάσουν τις αδυναμίες του προγράμματος, όπως η ανεπαρκής διαχείριση των patches λογισμικού, οι αδυναμίες αρχιτεκτονικής και πολιτικής, και οι διαδικασίες ανεπαρκής κατάρτισης.
Κατά τη διάρκεια αυτής της φάσης, οι οργανισμοί πρέπει να σιγουρευτούν ότι όλα τα δεδομένα που συνδέονται με τις αξιολογήσεις έχουν προστατευθεί. Οι πληροφορίες για τις ευπάθειες των συστημάτων είναι ευαίσθητες και πρέπει να συλλεχθούν, να αποθηκευθούν και, εάν είναι απαραίτητο, να διαβιβασθούν με ασφάλεια. Μετά από την ολοκλήρωση της αξιολόγησης, τα δεδομένα που δε χρειάζονται πλέον στον οργανισμό πρέπει να καταστραφούν σύμφωνα με τις ορθές πρακτικές ασφάλειας.

- Στη φάση μετα-εκτέλεσης (post-execution phase), οι οργανισμοί εφαρμόζουν τις πληροφορίες που παρέχονται από την αξιολόγηση ώστε να βελτιώσουν τη γενική ασφάλεια των πληροφοριών τους. Θα πρέπει να προταθούν κατάλληλες ενέργειες που θα μετριάσουν τις ευπάθειες και να προετοιμαστεί μια έκθεση που θα ενσωματώσει αυτές τις προτάσεις. Το σημαντικότερο είναι ότι οι προτεινόμενες ενέργειες θα πρέπει να επιτευχθούν.

4.3.3 Τεχνικές Ελέγχου και Εξέτασης

Πολλές τεχνικές ελέγχου και εξέτασης τεχνικής ασφάλειας μπορούν να χρησιμοποιηθούν για να αξιολογήσουν την ασφάλεια των συστημάτων και των δικτύων. Στην πραγματικότητα, καμία τεχνική δεν μπορεί να παρέχει μια πλήρη εικόνα της ασφάλειας ενός συστήματος ή ενός δικτύου. Οι τεχνικές μπορούν να συνδυαστούν για να εξασφαλίσουν εύρωστες αξιολογήσεις της ασφάλειας.

- Οι τεχνικές επισκόπησης (Review techniques) χρησιμοποιούνται για να αξιολογήσουν συστήματα, εφαρμογές, δίκτυα, πολιτικές και διαδικασίες προκειμένου να ανακαλύψουν ευπάθειες. Συγκεντρώνουν επίσης πληροφορίες για να διευκολύνουν και να βελτιστοποιήσουν άλλες τεχνικές αξιολόγησης. Περιλαμβάνουν τις εξής τεχνικές: Επισκόπηση Τεκμηρίωσης-Documentation Review, Επισκόπηση Καταγραφής-Log Review, Επισκόπηση Συνόλου Κανόνων-Ruleset Review (μια συλλογή κανόνων που διέπουν την κυκλοφορία των δικτύων ή τη δραστηριότητα των συστημάτων), καθώς και Επισκόπηση Διαμόρφωσης Συστημάτων-System Configuration Review, Παρακολούθηση Δικτύου-Network Sniffing και Έλεγχο Ακεραιότητας Αρχείων-File Integrity Checking. Ο Πίνακας 12 συνοψίζει τα σημαντικότερα χαρακτηριστικά των τεχνικών επισκόπησης.

Τεχνική	Χαρακτηριστικά
Επισκόπηση Τεκμηρίωσης	• Αξιολογεί τις πολιτικές και τις διαδικασίες για τεχνική ακρίβεια και πληρότητα.
Επισκόπηση Καταγραφής	• Παρέχει ιστορικές πληροφορίες για τη χρήση, διαμόρφωση και τροποποίηση συστημάτων. • Θα μπορούσε να αποκαλύψει πιθανά προβλήματα και αποκλίσεις πολιτικής.
Επισκόπηση Συνόλου Κανόνων	• Αποκαλύπτει κενά σε ελέγχους ασφάλειας που βασίζονται σε σύνολο κανόνων.
Επισκόπηση Διαμόρφωσης Συστημάτων	• Αξιολογεί την ισχύ της διαμόρφωσης συστημάτων. • Επικυρώνει ότι τα συστήματα διαμορφώνονται σύμφωνα με την πολιτική.
Παρακολούθηση Δικτύου	• Ελέγχει την κυκλοφορία του δικτύου στο τοπικό τμήμα ώστε να αποκτήσει πληροφορίες όπως ενεργά συστήματα, λειτουργικά συστήματα, πρωτόκολλα επικοινωνίας, υπηρεσίες και εφαρμογές. • Επαληθεύει την κρυπτογράφηση των επικοινωνιών.
Έλεγχος Ακεραιότητας Αρχείων	• Προσδιορίζει αλλαγές σε σημαντικά αρχεία και επιπλέον μπορεί να προσδιορίσει ορισμένες μορφές ανεπιθύμητων αρχείων, όπως τα γνωστά εργαλεία επιτιθεμένων.

Πίνακας 12. Τεχνικές επισκόπησης.

- Οι τεχνικές ανάλυσης και προσδιορισμού στόχου (Target identification and analysis techniques) μπορούν να προσδιορίσουν συστήματα, θύρες, υπηρεσίες και πιθανές ευπάθειες. Αυτές οι τεχνικές μπορούν να εκτελεσθούν χειροκίνητα, αλλά γενικά εκτελούνται χρησιμοποιώντας αυτοματοποιημένα εργαλεία. Περιλαμβάνουν τις εξής τεχνικές: Ανακάλυψη Δικτύου (Network Discovery), Προσδιορισμό Υπηρεσιών και Θυρών Δικτύου (Network Port and Service Identification), Ανίχνευση Ευπαθειών (Vulnerability Scanning), Ανίχνευση Ασύρματων Επικοινωνιών (Wireless Scanning) και εξέταση της ασφάλειας των εφαρμογών. Ο Πίνακας 13 συνοψίζει τα σημαντικότερα χαρακτηριστικά των τεχνικών ανάλυσης και προσδιορισμού στόχων.

Τεχνική	Χαρακτηριστικά
Ανακάλυψη Δικτύου	• Ανακαλύπτει ενεργές συσκευές. • Προσδιορίζει τις διαδρομές επικοινωνίας και διευκολύνει τον προσδιορισμό των αρχιτεκτονικών δικτύου.
Προσδιορισμός Υπηρεσιών και Θυρών Δικτύου	• Ανακαλύπτει ενεργές συσκευές • Ανακαλύπτει ανοικτές θύρες και τις σχετικές υπηρεσίες ή εφαρμογές.
Ανίχνευση Ευπαθειών	• Προσδιορίζει τους ξενιστές (hosts) και τις ανοικτές θύρες. • Προσδιορίζει τις γνωστές ευπάθειες (έχει υψηλά ποσοστά σε false positives[49]) • Παρέχει συχνά συμβουλές για να μετριάσει τις ευπάθειες που ανακαλύπτονται.
Ανίχνευση Ασύρματων Επικοινωνιών	• Περιλαμβάνει τις εξής τεχνικές: Παθητική Ανίχνευση Ασύρματων Επικοινωνιών (Passive Wireless Scanning), Ενεργή Ανίχνευση Ασύρματων Επικοινωνιών (Active Wireless Scanning), Εντοπισμός Θέσης Συσκευών Ασύρματων Επικοινωνιών (Wireless Device Location Tracking), Ανίχνευση Bluetooth (Bluetooth Scanning). • Προσδιορίζει μη εξουσιοδοτημένες συσκευές ασύρματων επικοινωνιών μέσω ανιχνευτών. • Ανακαλύπτει ασύρματα σήματα έξω από την περίμετρο ενός οργανισμού. • Ανιχνεύει πιθανά backdoors[50] και άλλες παραβιάσεις ασφάλειας.

Πίνακας 13. Τεχνικές ανάλυσης και προσδιορισμού στόχου

- Οι τεχνικές επικύρωσης ευπάθειας στόχου (Target vulnerability validation techniques) επιβεβαιώνουν την ύπαρξη των ευπαθειών και μπορούν να

[49] False Positive: Μια ενημέρωση που δείχνει λανθασμένα ότι μια ευπάθεια είναι παρούσα.
[50] Back Doors: Ένας τύπος κακόβουλου κώδικα που επιτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε μια εφαρμογή ή ένα σύστημα.

εκτελεσθούν χειροκίνητα ή με τη χρησιμοποίηση των αυτόματων εργαλείων, ανάλογα με τη συγκεκριμένη τεχνική που χρησιμοποιείται και την ικανότητα της ομάδας ελέγχου. Περιλαμβάνουν τις εξής τεχνικές: Παραβίαση Κωδικού Πρόσβασης (Password Cracking), Έλεγχο Διείσδυσης (Penetration Testing), Κοινωνική Μηχανική (Social Engineering) και έλεγχο της ασφάλειας των εφαρμογών. Ο Πίνακας 14. Τεχνικές επικύρωσης ευπάθειας στόχου.

- συγκρίνει την εμβέλεια των τεχνικών επικύρωσης ευπάθειας στόχου.

Τεχνική	Χαρακτηριστικά
Παραβίαση Κωδικού Πρόσβασης	• Προσδιορίζει μη ισχυρούς κωδικούς πρόσβασης και πολιτικές κωδικού πρόσβασης.
Έλεγχος Διείσδυσης	• Ελέγχει την ασφάλεια χρησιμοποιώντας τις ίδιες μεθοδολογίες και τα εργαλεία που χρησιμοποιούν οι επιτιθέμενοι. • Επαληθεύει τις ευπάθειες. • Καταδεικνύει πώς οι ευπάθειες μπορούν να χρησιμοποιηθούν επαναληπτικά για να αποκτήσουν μεγαλύτερη πρόσβαση. • •Περιλαμβάνει τις εξής τεχνικές: Φάσεις Ελέγχου Διείσδυσης (Penetration Testing Phases), Εφοδιαστική Ελέγχου Διείσδυσης (Penetration Testing Logistics)[51].
Κοινωνική Μηχανική	• Επιτρέπει τον έλεγχο και των διαδικασιών και των ανθρώπινων στοιχείων (συνειδητοποίηση χρήστη).

Πίνακας 14. Τεχνικές επικύρωσης ευπάθειας στόχου.

4.3.4 Σύγκριση Ελέγχων και Εξετάσεων

Οι εξετάσεις αρχικά περιλαμβάνουν την επισκόπηση εγγράφων όπως οι πολιτικές, οι διαδικασίες, τα σχέδια ασφάλειας, οι απαιτήσεις ασφάλειας, οι τυποποιημένες λειτουργικές διαδικασίες, τα διαγράμματα αρχιτεκτονικής, η τεκμηρίωση εφαρμοσμένης μηχανικής, οι κατάλογοι αγαθών, οι διαμορφώσεις συστήματος, τα σύνολα κανόνων και οι καταγραφές συστήματος. Οι εξετάσεις διεξάγονται για να καθορίσουν εάν ένα σύστημα είναι κατάλληλα τεκμηριωμένο και για να αποκτήσουν επίγνωση των πτυχών της ασφάλειας που είναι διαθέσιμες μόνο μέσω τεκμηρίωσης. Αυτή η τεκμηρίωση προσδιορίζει το προτεινόμενο σχεδιασμό, την εγκατάσταση, τη διαμόρφωση, τη λειτουργία και τη συντήρηση των συστημάτων και του δικτύου.

Οι εξετάσεις δεν ασκούν καμία επίδραση στα πραγματικά συστήματα ή στα δίκτυα στο περιβάλλον στόχου, επηρεάζουν όμως την πρόσβαση στην απαραίτητη τεκμηρίωση, τις καταγραφές ή τα σύνολα κανόνων[52]. Εντούτοις, εάν τα αρχεία διαμόρφωσης συστήματος ή οι καταγραφές πρόκειται να ανακτηθούν από ένα δεδομένο σύστημα όπως ένας δρομολογητής (router) ή ένα τείχος προστασίας (firewall), μόνο οι διαχειριστές συστήματος και άλλα εκπαιδευμένα άτομα θα πρέπει να αναλάβουν αυτήν την εργασία για να εξασφαλισθεί ότι οι ρυθμίσεις δεν τροποποιούνται ή διαγράφονται ακούσια.

[51] Ο όρος logistics (εφοδιαστική) αποτελεί πολυσήμαντη και πολυσύνθετη έννοια, καλύπτοντας μια τεράστια γκάμα διαδικασιών σχεδιασμού, υλοποίησης και ελέγχου στο επιχειρηματικό πεδίο. Τα βασικά στοιχεία που συνυφαίνουν την «εφοδιαστική» είναι η διοίκηση και ο στρατηγικός σχεδιασμός της επιχείρησης, η βέλτιστη αξιοποίηση των έμψυχων (ανθρώπινων) και των άψυχων (υλικών) πόρων της, η παραγωγή, η αποθήκευση και η διανομή των αγαθών, από την πρώτη ύλη μέχρι το έτοιμο προϊόν και από την παραγωγή στο ράφι.

[52] Μια παθητική τεχνική ελέγχου που μπορεί ενδεχομένως να επηρεάσει τα δίκτυα είναι η παρακολούθηση δικτύων (network sniffing), η οποία περιλαμβάνει τη σύνδεση ενός sniffer με μία θύρα ενός hub στο δίκτυο. Σε μερικές περιπτώσεις, η απαιτείται η σύνδεση μιας συσκευή δικτύου, και κατά τη διάρκεια της σύνδεσης θα μπορούσε να διακοπεί η λειτουργία του δικτύου.

Ο έλεγχος περιλαμβάνει την άμεση εργασία με τα συστήματα και τα δίκτυα προκειμένου να προσδιορίσει τις ευπάθειες ασφάλειας και μπορεί να εκτελεσθεί σε μια επιχείρηση ή σε επιλεγμένα συστήματα. Η χρήση των τεχνικών ανίχνευσης και διείσδυσης μπορεί να παρέχει πολύτιμες πληροφορίες για τις πιθανές ευπάθειες και να προβλέψει την πιθανότητα όπου ένας αντίπαλος ή εισβολέας θα είναι σε θέση να τις εκμεταλλευτεί. Ο έλεγχος επιτρέπει επίσης στους οργανισμούς να μετρήσουν τα επίπεδα συμμόρφωσης σε περιοχές, όπως η διαχείριση επιδιορθώσεων (patch), η πολιτική κωδικών πρόσβασης και η διαχείριση διαμόρφωσης.

Ο έλεγχος μπορεί να παρέχει μια πιο ακριβή εικόνα της ασφάλειας ενός οργανισμού σε σύγκριση με τις εξετάσεις, εντούτοις, είναι πιο παρεμβατικός και μπορεί να επηρεάσει τα συστήματα ή τα δίκτυα στο περιβάλλον-στόχο. Το επίπεδο πιθανής επίδρασης εξαρτάται από τους συγκεκριμένους τύπους των τεχνικών ελέγχου που χρησιμοποιούνται, οι οποίοι μπορούν να αλληλεπιδράσουν με τα συστήματα και τα δίκτυα στόχου με διάφορους τρόπους - όπως η αποστολή κανονικών πακέτων δικτύου για να καθορίσουν ανοικτές και κλειστές θύρες ή η αποστολή ειδικά επεξεργασμένων πακέτων για να ελέγξουν για ευπάθειες. Οποτεδήποτε ένας έλεγχος ή ελεγκτής αλληλεπιδρά άμεσα με ένα σύστημα ή δίκτυο, υπάρχει το ενδεχόμενο για απροσδόκητες συμπεριφορές του συστήματος και καταστάσεις άρνησης υπηρεσιών (denial of service). Οι οργανισμοί πρέπει να καθορίσουν τα αποδεκτά επίπεδα παρέμβασής τους, όταν αποφασίζουν ποιες τεχνικές θα χρησιμοποιήσουν. Ο αποκλεισμός ελέγχων που δημιουργούν καταστάσεις άρνησης υπηρεσιών και άλλες διαταραχές, μπορεί να βοηθήσει να μειωθούν αυτές οι αρνητικές επιδράσεις.

Ο έλεγχος δεν παρέχει μια διεξοδική αξιολόγηση της ασφάλειας ενός οργανισμού και έχει συχνά μια συγκεκριμένη εμβέλεια λόγω των περιορισμών των πόρων - ιδιαίτερα στον τομέα του χρόνου. Επιπλέον, οι κακόβουλοι επιτιθέμενοι μπορούν να έχουν όσο χρόνο χρειάζονται για να εκμεταλλευτούν και να διαπεράσουν ένα σύστημα ή δίκτυο. Επίσης, ενώ οι οργανισμοί τείνουν να αποφύγουν τη χρήση τεχνικών ελέγχου που επηρεάζουν τα συστήματα ή δίκτυα, οι επιτιθέμενοι δεν δεσμεύονται από αυτούς τους περιορισμούς και χρησιμοποιούν οποιεσδήποτε τεχνικές θεωρούν απαραίτητες. Κατά συνέπεια, ο έλεγχος είναι λιγότερο πιθανό, σε σύγκριση με τις εξετάσεις, να προσδιορίσει τις αδυναμίες που είναι σχετικές με την πολιτική και τη διαμόρφωση ασφάλειας. Σε πολλές περιπτώσεις, ο συνδυασμός των τεχνικών ελέγχου και εξέτασης μπορεί να παρέχει μια πιο ακριβή πτυχή της ασφάλειας.

4.3.5 Προσεγγίσεις για Έλεγχο

Οι έλεγχοι μπορούν να εκτελεσθούν από διάφορες πτυχές - παραδείγματος χάριν, το πόσο εύκολα θα μπορούσε ένας εξωτερικός ή κακόβουλος επιτιθέμενος να επιτεθεί επιτυχώς σε ένα σύστημα; Παρακάτω γίνεται αναφορά στον έλεγχο που εκτελείται από την εξωτερική και εσωτερική πτυχή. Επίσης, γίνεται αναφορά και στον έλεγχο που εκτελείται από μια άλλη πτυχή απόψεων - συγκεκριμένα, την προηγούμενη γνώση που έχουν οι αξιολογητές για τον στόχο ή το περιβάλλον του στόχου.

- Ο εξωτερικός (external) έλεγχος ασφάλειας διεξάγεται έξω από την περίμετρο της ασφάλειας του οργανισμού, επιτρέποντας στην ασφάλεια του περιβάλλοντος να εξεταστεί με στόχο την εύρεση ευπαθειών που θα μπορούσαν να χρησιμοποιηθούν από έναν εξωτερικό επιτιθέμενο.

Ο εξωτερικός έλεγχος αρχίζει συχνά με τεχνικές αναγνώρισης που ψάχνουν σε δημόσια δεδομένα καταχώρησης, σε πληροφορίες εξυπηρέτη Domain Name System (DNS)[53], σε ανακοινώσεις ομάδων συζητήσεων[54] και σε άλλες δημόσια διαθέσιμες πληροφορίες για να συλλέξουν πληροφορίες που μπορούν να βοηθήσουν τον αξιολογητή ώστε να προσδιορίσει ευπάθειες. Ο αξιολογητής χρησιμοποιεί τις τεχνικές ανακάλυψης και ανίχνευσης δικτύων για να καθορίσει τους ξενιστές (hosts) που είναι εξωτερικά ορατοί και τις υπηρεσίες που εκτελούνται σε αυτούς και είναι εξωτερικά προσβάσιμες. Οι αρχικές επιθέσεις στρέφονται γενικά σε πρωτόκολλα εφαρμογής που χρησιμοποιούνται συνήθως, όπως FTP, HTTP, SMTP, και POP[55]. Οι εξυπηρέτες (servers) που είναι εξωτερικά προσβάσιμοι, ελέγχονται για ευπάθειες που μπορεί να επιτρέψουν την πρόσβαση σε εσωτερικούς εξυπηρέτες και ιδιωτικές πληροφορίες. Ο εξωτερικός έλεγχος ασφάλειας επικεντρώνεται επίσης στην ανακάλυψη της μεθόδου προσπέλασης ευπαθειών, όπως τα σημεία πρόσβασης ασύρματων επικοινωνιών, modems και πύλες (portals) σε εσωτερικούς εξυπηρέτες.

- Ο εσωτερικός (internal) έλεγχος ασφάλειας διεξάγεται από το εσωτερικό δίκτυο και ο αξιολογητής υποθέτει την ταυτότητα ενός έμπιστου μέλους ή ενός επιτιθεμένου που έχει διαπεράσει την άμυνα της περιμέτρου. Αυτό το είδος ελέγχου μπορεί να αποκαλύψει ευπάθειες που θα μπορούσαν να χρησιμοποιηθούν και καταδεικνύει την πιθανή ζημία που θα μπορούσε να προκληθεί. Ο εσωτερικός έλεγχος ασφάλειας εστιάζει επίσης στην ασφάλεια και τη διαμόρφωση στο επίπεδο του συστήματος.
  Στους αξιολογητές που εκτελούν τον εσωτερικό έλεγχο δίνεται συχνά κάποιο επίπεδο πρόσβασης στο δίκτυο, κανονικά ως γενικοί χρήστες και τους παρέχονται πληροφορίες όπου μόνο οι χρήστες με παρόμοια προνόμια θα είχαν. Αυτό το επίπεδο προσωρινής πρόσβασης εξαρτάται από τους στόχους του ελέγχου και μπορεί να συμπεριλαμβάνει μέχρι και τα προνομία ενός διαχειριστή συστήματος ή δικτύου. Λειτουργώντας από το επίπεδο πρόσβασης που τους έχει επιτραπεί, οι αξιολογητές προσπαθούν να αποκτήσουν πρόσθετη πρόσβαση στο δίκτυο και τα συστήματα, αυξάνοντας τα προνομία πρόσβασής τους, από το επίπεδο του χρήστη προς το επίπεδο του διαχειριστή.

Ο εσωτερικός έλεγχος είναι λιγότερο περιορισμένος από τον εξωτερικό έλεγχο επειδή πραγματοποιείται πίσω από την άμυνα της περιμέτρου ασφάλειας, ακόμα κι αν μπορεί να υπάρχουν σε ισχύ εσωτερικά τείχη προστασίας (firewalls), δρομολογητές (routers) και μεταγωγείς (switches) που θέτουν περιορισμούς. Οι τεχνικές εξέτασης όπως η παρακολούθηση δικτύου (network sniffing) μπορούν να χρησιμοποιηθούν μαζί με τις τεχνικές ελέγχου. Όταν και ο εσωτερικός και ο εξωτερικός έλεγχος εκτελούνται από τους ίδιους αξιολογητές, ο εξωτερικός έλεγχος πραγματοποιείται συνήθως πρώτα. Αυτή η προσέγγιση δεν επιτρέπει στους

[53] Το Domain Name System ή DNS (Σύστημα Ονομάτων Τομέα) είναι ένα σύστημα με το οποίο αντιστοιχίζονται οι διευθύνσεις IP σε ονόματα τομέων (Domain Names). Τα ονόματα τομέων όπως και οι διευθύνσεις IP που αναπαριστούν είναι μοναδικά, έχουν μια ιεραρχία και διαβάζονται από αριστερά προς τα δεξιά.

[54] Ένα Newsgroup είναι μια ομάδα συζήτησης που επιτρέπει σε ανθρώπους με κοινά ενδιαφέροντα να επικοινωνούν μεταξύ τους.

[55] File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), και Post Office Protocol (POP).

αξιολογητές να διαθέτουν κατά τη φάση του εξωτερικού ελέγχου πληροφορίες που ίσως να μην είναι διαθέσιμες σε έναν επιτιθέμενο.

- Ο προφανής (overt) έλεγχος ασφάλειας, επίσης γνωστός και ως έλεγχος white hat (λευκού καπέλου), περιλαμβάνει την εκτέλεση του εξωτερικού ή/και εσωτερικού ελέγχου με τη γνώση και τη συναίνεση του προσωπικού πληροφορικής (IT) του οργανισμού, επιτρέποντας την διεξοδική αξιολόγηση της ασφάλειας δικτύων ή συστημάτων. Το προσωπικό πληροφορικής μπορεί να παρέχει καθοδήγηση για να περιορίσει την επίπτωση του ελέγχου και επιπλέον, δημιουργούνται χρήσιμες ευκαιρίες κατάρτισης για τα μέλη του προσωπικού.
- Ο κρυφός (covert) έλεγχος ασφάλειας, επίσης γνωστός ως έλεγχος black hat (μαύρου καπέλου), υιοθετεί μια επιθετική προσέγγιση στον έλεγχο, με το προσωπικό πληροφορικής να μην έχει γνώση της επίθεσης που διενεργείται, αλλά με την επίθεση να είναι εν γνώσει και με εξουσιοδότηση από την ανώτερη διοίκηση. Μερικοί οργανισμοί υποδεικνύουν μια έμπιστη τρίτη οντότητα η οποία διασφαλίζει ότι ο οργανισμός-στόχος δεν εισάγει μέτρα αντίδρασης που συνδέονται με την επίθεση, χωρίς πρώτα να επαληθεύσει ότι η επίθεση είναι πράγματι σε εξέλιξη. Αυτός ο τύπος ελέγχου είναι χρήσιμος για τον έλεγχο των τεχνικών ασφάλειας, της απόκρισης του προσωπικού πληροφορικής στα περιστατικά ασφάλειας που ανιχνεύονται, καθώς και της γνώσης του προσωπικού και την υλοποίηση της πολιτικής ασφάλειας του οργανισμού. Ο έλεγχος μπορεί να διεξαχθεί με ή χωρίς προειδοποίηση και επιτρέπει στον οργανισμό να εξετάσει τη ζημία ή την επίπτωση που θα μπορούσε να προκαλέσει ένας επιτιθέμενος, αλλά δεν προσδιορίζει κάθε ευπάθεια ή δεν ελέγχει κάθε έλεγχο ασφάλειας.

Ο προφανής έλεγχος είναι λιγότερο δαπανηρός και λιγότερο επικίνδυνος από τον κρυφό έλεγχο, ο οποίος συχνά είναι χρονοβόρος και δαπανηρός εξαιτίας των απαιτήσεων μυστικότητας. Εντούτοις, ο κρυφός έλεγχος παρέχει μια καλύτερη ένδειξη της καθημερινής ασφάλειας του οργανισμού στόχου.

4.4 Εργαλεία για την υποστήριξη της μεθοδολογίας

4.4.1 Διανομές Live CD για Έλεγχο Ασφάλειας

Μια διανομή Live CD που αναφέρεται στον έλεγχο ασφάλειας είναι διαθέσιμη στο κοινό χωρίς κόστος και παρέχει στους ελεγκτές ασφάλειας μια live διανομή OS που περιέχει εργαλεία για τον έλεγχο ασφάλειας[56]. Η διανομή OS φορτώνεται σε ένα CD-ROM, σε έναν οδηγό Universal Serial Bus (USB), ή σε κάποια άλλη περιφερειακή συσκευή. Δεν εγκαθίσταται σε ένα σύστημα, αλλά «τρέχει» κατευθείαν από τη συσκευή στην οποία φορτώνεται - συνεπώς και ο προσδιορισμός της ως «live» διανομή. Δύο τέτοιες διανομές είναι το BackTrack και το Knoppix Security Tool Distribution (STD).

4.4.1.1 BackTrack

[56] Αυτά τα κουτιά εργαλείων (toolkits) δεν περιλαμβάνουν απαραιτήτως όλα τα εργαλεία που απαιτούνται για έναν συγκεκριμένο έλεγχο - σε πολλές περιπτώσεις, τα toolkits θα πρέπει να συμπληρωθούν με πρόσθετα εργαλεία.

4.4.1.1.1 Γενικά

Το BackTrack[57] αποτελεί μια συλλογή με περισσότερα από 300 εργαλεία ασφάλειας για ανακάλυψη δικτύου (network discovery), ανίχνευση και παρακολούθηση δικτύου (scanning and sniffing), παραβίαση κωδικού πρόσβασης (password cracking), έλεγχο απομακρυσμένης πρόσβασης (remote access testing), έλεγχο Bluetooth (Bluetooth testing), εγκληματολογία υπολογιστών (computer forensics[58]) και έλεγχο διείσδυσης (penetration testing).

4.4.1.1.2 Χαρακτηριστικά

Προσφέρει τμηματικότητα (modularity) στον χρήστη, κάτι που σημαίνει ότι ο χρήστης μπορεί να προσαρμόσει την έκδοση για να συμπεριλαμβάνει προσωπικά scripts ή πρόσθετα εργαλεία. Το BackTrack περιλαμβάνει επίσης εργαλεία για να αναλύει πρωτόκολλα Voice over Internet (Φωνής μέσω Πρωτοκόλλου Ίντερνετ-VoIP), όπως το Πρωτόκολλο Έναρξης Συνόδου (Session Initiation Protocol-SIP), περιλαμβάνει εργαλεία όπως το Cisco Global Exploiter (CGE) και Cisco Torch που στοχεύουν συγκεκριμένα σε συστήματα Cisco, καθώς και το Metasploit, ένα εργαλείο αξιολόγησης ευπαθειών. Αναγνωρίζοντας την αυξανόμενη σημασία του ελέγχου ασφάλειας εφαρμογών, το BackTrack περιλαμβάνει επίσης εργαλεία όπως Peach, Fuzzer και το Java εργαλείο, Paros Proxy. Ο Πίνακας 15. Δείγμα εργαλείων του BackTrack.

παρέχει ένα δείγμα των εργαλείων που είναι διαθέσιμα στο BackTrack.

[57] Το BackTrack προέρχεται από δύο ξεχωριστές Linux live διανομές που βασίζονται στην ασφάλεια, την WHAX και Auditor Security Collection. Και οι δύο ήταν δημοφιλείς για την αφθονία των εργαλείων ασφάλειας και την ευκολία της χρήσης τους. Όταν οι δημιουργοί κάθε διανομής άρχισαν να συνεργάζονται, κυκλοφόρησαν την πρώτη non-beta έκδοση, με όνομα BackTrack, το Μάιο του 2006. Το BackTrack πολύ γρήγορα έγινε και παρέμεινε, ένα αγαπημένο σύνολο εργαλείων για τους επαγγελματίες ασφάλειας. Το BackTrack 3.0 είναι η έκδοση στην οποία αναφερόμαστε.

[58] Computer forensics (μερικές φορές γνωστή και ως computer forensic science) είναι ένας κλάδος της ψηφιακής δικανικής επιστήμης που αφορά τα νομικά αποδεικτικά στοιχεία που βρίσκονται στους υπολογιστές και στα μέσα ψηφιακής αποθήκευσης. Ο στόχος της δικανικής υπολογιστών είναι να εξεταστούν τα ψηφιακά μέσα κατά τρόπο που είναι νομικά αποδεκτός με στόχο την αναγνώριση, συλλογή, διαφύλαξη, ανάλυση και παρουσίαση γεγονότων και απόψεων σχετικά με τις πληροφορίες.

Τεχνική Ελέγχου Ασφάλειας	Εργαλείο Ελέγχου Ασφάλειας
Επισκόπηση (Review)	
Παρακολούθηση Δικτύου (Network Sniffing)	Dsniff, Ettercap, Kismet[6], Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer και Wireshark[3]
Έλεγχος Ακεραιότητας Αρχείων (File Integrity Checking)	Autopsy, Foremost, RootkitHunter και Sleuthkit
Προσδιορισμός και Ανάλυση Στόχου (Target Identification and Analysis)	
Έλεγχος Ασφάλειας Εφαρμογών (Application Security Testing)	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy[11] και Peach
Ανακάλυψη Δικτύου (Network Discovery)	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace και Umit
Προσδιορισμός Υπηρεσιών και Θυρών Δικτύου (Network Port and Service Identification)	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit και UnicornScan[2.4.1.2]
Ανίχνευση Ευπαθειών (Vulnerability Scanning)	Firewalk, GFI LANguard, Hydra, Metasploit[10], Nmap, Paros Proxy[11], Snort και SuperScan
Ανίχνευση Ασύρματων Επικοινωνιών (Wireless Scanning)	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet[6] και WifiTAP
Επικύρωση Ευπάθειας Στόχου (Target Vulnerability Validation)	
Παραβίαση Κωδικού Πρόσβασης (Password Cracking)	Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack και WebCrack
Έλεγχος Απομακρυσμένης Πρόσβασης (Remote Access Testing)	IKEProbe, IKE-Scan, PSK-Crack και VNC_bypauth
Έλεγχος Διείσδυσης (Penetration Testing)	Driftnet, Dsniff, Ettercap, Kismet[6], Metasploit[10], Nmap, Ntop, SinFP, SMB Sniffer και Wireshark[3]

Πίνακας 15. Δείγμα εργαλείων του BackTrack.

4.4.1.2 Knoppix STD

4.4.1.2.1 Γενικά

Το Knoppix STD είναι ένα σύνολο εργαλείων ασφάλειας, παλαιότερης διανομής Linux live OS και ανοικτού κώδικα, το οποίο βασίζεται σε Knoppix Linux. Δημιουργήθηκε από έναν επαγγελματία ασφάλειας για να βοηθήσει με τη διδασκαλία τεχνικών ασφάλειας σε άλλους. Το Knoppix STD εκδόθηκε αρχικά τον Μάιο του 2004 ως Knoppix-STD 0.1 και δεν έχει ενημερωθεί από τότε. Πριν από το BackTrack, το Knoppix STD ήταν το σύνολο εργαλείων αναφοράς της ασφάλειας και παραμένει ευρέως χρησιμοποιούμενο. Το STD, επομένως, είναι ένα εργαλείο ασφάλειας. Στην πραγματικότητα, είναι μια συλλογή από εκατοντάδες ή και χιλιάδες εργαλεία ασφάλειας ανοικτού κώδικα. Όπως αναφέρθηκε και προηγουμένως, πρόκειται για μια Live Linux διανομή (δηλ. «τρέχει» από το bootable CD στη μνήμη χωρίς να χρειάζεται αλλαγή του λειτουργικού συστήματος στο PC μας).

4.4.1.2.2 Χαρακτηριστικά

Όμοια με το BackTrack, το Knoppix STD επιτρέπει ανακάλυψη δικτύου (network discovery), προσδιορισμό υπηρεσιών και θυρών (port and service identification), παρακολούθηση δικτύου (network sniffing), παραβίαση κωδικού πρόσβασης (password cracking), εγκληματολογία υπολογιστών (computer forensics) και έλεγχο απομακρυσμένης πρόσβασης (remote access testing). Υπάρχει μερική

επικάλυψη μεταξύ των διανομών Knoppix και BackTrack, υπάρχουν όμως και μερικές διαφορές. Το Knoppix περιέχει μερικά εργαλεία που δεν περιέχει το BackTrack, όπως το Netcat και Nessus. Επιπλέον, ασχολείται με τομείς τεχνολογίας όπως η κρυπτογράφηση και προσφέρει περισσότερα εργαλεία για εγκληματολογία και παρακολούθηση υπολογιστών. Δεν παρέχει το Metasploit και σε σύγκριση με το BackTrack είναι αδύναμο σε εργαλεία ασφάλειας ασύρματων επικοινωνιών. Ο Πίνακας 16. Δείγμα εργαλείων του Knoppix STD.

παρέχει ένα δείγμα των εργαλείων που είναι διαθέσιμα στη διανομή Knoppix STD.

Τεχνική Ελέγχου Ασφάλειας	Εργαλείο Ελέγχου Ασφάλειας
Επισκόπηση (Review)	
Παρακολούθηση Δικτύου (Network Sniffing)	Dsniff, Ettercap, Ethereal, Filesnarf, Kismet[6], Mailsnarf, Msgsnarf, Ngrep, Ntop, TCPdump[4] και Webspy
Έλεγχος Ακεραιότητας Αρχείων (File Integrity Checking)	Autopsy, Biew, Bsed, Coreography, Foremost, Hashdig, Rifiuti και Sleuthkit
Ανάλυση και Προσδιορισμός Στόχου (Target Identification and Analysis)	
Έλεγχος Ασφάλειας Εφαρμογών (Application Security Testing)	NetSed
Ανακάλυψη Δικτύου (Network Discovery)	Cryptcat, Ettercap, Firewalk, Netcat[5], Nmap και P0f
Προσδιορισμός Υπηρεσιών και Θυρών Δικτύου (Network Port and Service Identification)	Amap, Netcat[5], Nmap και P0f
Ανίχνευση Ευπαθειών (Vulnerability Scanning)	Exodus, Firewalk, Nmap και Snort
Ανίχνευση Ασύρματων Επικοινωνιών (Wireless Scanning)	Airsnarf, Airsnort, GPSdrive, Kismet[6] και MACchanger
Επικύρωση Ευπάθειας Στόχου (Target Vulnerability Validation)	
Παραβίαση Κωδικού Πρόσβασης (Password Cracking)	Allwords2, chntpw, Cisilia, Djohn, Hydra, John the Ripper και Rcrack
Έλεγχος Απομακρυσμένης Πρόσβασης (Remote Access Testing)	Apache Server, IKE-Scan, Net-SNMP, SSHD, TFTPD και VNC Server
Έλεγχο Διείσδυσης (Penetration Testing)	Driftnet, Dsniff, Ethereal, Ettercap, Kismet[6], Nessus[2], Netcat[5], Ngrep, Nmap, Ntop και TCPdump[4]

Πίνακας 16. Δείγμα εργαλείων του Knoppix STD.

4.5 Συμπέρασμα

Για να ολοκληρωθούν οι αξιολογήσεις της τεχνικής ασφάλειας και να εξασφαλιστεί ότι οι τεχνικοί έλεγχοι και οι εξετάσεις ασφάλειας παρέχουν τη μέγιστη ωφέλεια, το NIST συστήνει στους οργανισμούς να εφαρμόζουν τις ακόλουθες πολιτικές στον σχεδιασμό και στην υλοποίηση των δραστηριοτήτων για την αξιολόγηση της ασφάλειάς τους:

- Καθιέρωση μιας πολιτικής αξιολόγησης της ασφάλειας πληροφοριών: προκειμένου να προσδιοριστούν οι απαιτήσεις του οργανισμού για την εφαρμογή αξιολογήσεων και προκειμένου να προσδιοριστούν τα κατάλληλα άτομα που θα εξασφαλίσουν ότι οι αξιολογήσεις θα διεξάγονται σύμφωνα με τις απαιτήσεις. Οι οργανωτικές απαιτήσεις για τις αξιολογήσεις πρέπει να

διευκρινιστούν, παρέχοντας τους ρόλους και τις ευθύνες των ατόμων, την ανάγκη για επιμονή σε μια καθιερωμένη μεθοδολογία αξιολόγησης, τη συχνότητα αξιολόγησης και τις απαιτήσεις τεκμηρίωσης.

- Εφαρμογή μιας επαναλαμβανόμενης και τεκμηριωμένης μεθοδολογίας αξιολόγησης: για να επιτραπεί συνέπεια και δομή στη διαδικασία αξιολόγησης, για να επισπευσθεί η μετάβαση των νέων μελών του προσωπικού αξιολόγησης και για να εξετασθούν οι περιορισμοί των πόρων που συνδέονται με τις αξιολογήσεις. Η χρησιμοποίηση μιας επαναλαμβανόμενης και τεκμηριωμένης μεθοδολογίας επιτρέπει στους οργανισμούς να μεγιστοποιήσουν την αξία των αξιολογήσεων, ελαχιστοποιώντας τους πιθανούς κινδύνους που εισάγονται από ορισμένες τεχνικές αξιολόγησης. Τέτοιοι κίνδυνοι μπορεί να είναι: η μη συγκέντρωση ικανοποιητικών πληροφοριών για την ασφάλεια του οργανισμού εξαιτίας του φόβου για την επίπτωσή τους στην λειτουργικότητα του συστήματος, καθώς και η επιρροή της διαθεσιμότητας του συστήματος ή δικτύου όταν εκτελούνται τεχνικές χωρίς να βρίσκονται σε ισχύ τα κατάλληλα μέτρα προστασίας. Οι οργανισμοί μπορούν να ελαχιστοποιήσουν τον κίνδυνο που προκαλείται από ορισμένες τεχνικές αξιολόγησης με τη χρησιμοποίηση ειδικευμένων αξιολογητών, την ανάπτυξη διεξοδικών σχεδίων αξιολόγησης, την καταγραφή των δραστηριοτήτων των αξιολογητών, την εκτέλεση πολύωρων ελέγχων και τη διεξαγωγή ελέγχων σε αντίγραφα των συστημάτων παραγωγής, όπως τα συστήματα ανάπτυξης. Οι οργανισμοί πρέπει να καθορίσουν το επίπεδο κινδύνου, το οποίο είναι πρόθυμοι να δεχτούν για κάθε αξιολόγηση και να προσαρμόσουν ανάλογα τις προσεγγίσεις τους.
- Καθορισμός των στόχων κάθε αξιολόγησης της ασφάλειας και προσαρμογή της προσέγγισης που υιοθετείται. Οι αξιολογήσεις της ασφάλειας έχουν συγκεκριμένους στόχους, αποδεκτά επίπεδα κινδύνου και διαθέσιμους πόρους. Καμία τεχνική δεν μπορεί να παρέχει μια διεξοδική εικόνα της ασφάλειας ενός οργανισμού. Επομένως, οι οργανισμοί πρέπει να χρησιμοποιήσουν έναν συνδυασμό τεχνικών. Αυτό αποτελεί μια πρακτική που βοηθά τους οργανισμούς να περιορίσουν τους κινδύνους τους και τη χρήση των πόρων τους.
- Ανάλυση συμπερασμάτων και ανάπτυξη τεχνικών μετριασμού του κινδύνου: προκειμένου να εξεταστούν οι αδυναμίες. Για να εξασφαλιστεί ότι η διαδικασία αξιολόγησης της ασφάλειας παρέχει τη μέγιστη τιμή, οι οργανισμοί πρέπει να διεξάγουν την ανάλυση πρωταρχικών αιτιών μετά την ολοκλήρωση μιας αξιολόγησης για να διαβεβαιώσουν ότι τα συμπεράσματα αξιολόγησης προκύπτουν κατόπιν και υλοποιούνται στην εφαρμογή με πρακτικές τεχνικές που θα βελτιώσουν τη γενική ασφάλεια. Τα αποτελέσματα μπορούν να υποδείξουν ότι οι οργανισμοί πρέπει να εξετάσουν όχι μόνο τις τεχνικές αδυναμίες, αλλά και τις αδυναμίες στις οργανωτικές διαδικασίες επίσης.

Κεφάλαιο 5: Information System Security Assessment Framework - ISSAF 0.2

5.1 Γενικά

5.1.1 Εισαγωγή

Το ISSAF είναι μια από τις εκτενέστερες ελεύθερες μεθοδολογίες αξιολόγησης που υπάρχουν διαθέσιμες. Περιλαμβάνει 1200 σελίδες και παρέχει κλιμακωτό επίπεδο λεπτομέρειας. Οι συντάκτες της θεωρούν ότι είναι καλύτερο να παρέχει όλες τις πιθανές πληροφορίες που ένας ελεγκτής μπορεί να χρειαστεί, παρά να περιοριστεί σε στόχους υψηλού επιπέδου. Κάθε δοκιμή ελέγχου περιλαμβάνει λεπτομερείς οδηγίες για τα λειτουργικά εργαλεία ελέγχου και για τα αποτελέσματα που πρέπει να ευρεθούν. Είναι διαχωρισμένο σε δύο αρχικά έγγραφα. Το ένα (ISSAF Draft 0.2.1A) εστιάζει στην επιχειρησιακή πτυχή της ασφάλειας και το άλλο (ISSAF Draft 0.2.1B) σχεδιάζεται ως ένα πλαίσιο ελέγχου διείσδυσης. Το πλαίσιο δεν έχει ενημερωθεί από το 2006, αλλά είναι ακόμα χρήσιμο ως βασικό υλικό για τη δοκιμή ελέγχων και ως μεθοδολογία πλήρους αξιολόγησης. Το επίπεδο λεπτομερούς εξήγησης των υπηρεσιών, των εργαλείων ασφάλειας που χρησιμοποιούνται και των πιθανών εκμεταλλεύσεων (exploits[59]), είναι υψηλό και μπορεί να βοηθήσει έναν πεπειραμένο ελεγκτή ασφάλειας αλλά και κάποιον που κάνει τα πρώτα του βήματα στον έλεγχο.

Το Πλαίσιο Αξιολόγησης της Ασφάλειας Συστημάτων Πληροφοριών (Information System Security Assessment Framework-ISSAF) είναι ένα αξιολογημένο από ομότιμους[60] και δομημένο πλαίσιο που ταξινομεί την αξιολόγηση της ασφάλειας συστημάτων πληροφοριών σε διάφορες περιοχές και απαριθμεί συγκεκριμένα κριτήρια αξιολόγησης ή ελέγχου για κάθε μια από αυτές τις περιοχές. Στόχος του είναι να παρέχει την είσοδο τομέων στην αξιολόγηση της ασφάλειας, οι οποίοι απεικονίζουν πραγματικά σενάρια. Το ISSAF πρέπει αρχικά να χρησιμοποιηθεί για να ικανοποιήσει τις απαιτήσεις αξιολόγησης της ασφάλειας ενός οργανισμού και στη συνέχεια, μπορεί να χρησιμοποιηθεί ως αναφορά για την ικανοποίηση άλλων αναγκών ασφάλειας πληροφοριών. Το ISSAF περιλαμβάνει την κρίσιμη πτυχή των διαδικασιών ασφάλειας και της αξιολόγησή τους, και προσπαθεί ώστε να λάβει μια πλήρη εικόνα των ευπαθειών που μπορεί να υπάρχουν. Οι πληροφορίες του ISSAF οργανώνονται σε καλά καθορισμένα κριτήρια αξιολόγησης, κάθε ένα από τα οποία έχει επισκοπηθεί από εμπειρογνώμονες σε αυτήν την περιοχή. Αυτά τα κριτήρια αξιολόγησης περιλαμβάνουν τα παρακάτω:

- Μια περιγραφή των κριτηρίων αξιολόγησης.
- Τους στόχους και τους σκοπούς του.
- Τις προϋποθέσεις για τη διεξαγωγή των αξιολογήσεων.
- Τη διαδικασία για την αξιολόγηση.
- Την περιγραφή των αναμενόμενων αποτελεσμάτων.

[59] exploits - δηλαδή, οι τρόποι εκμετάλλευσης των ευπαθειών.

[60] αξιολογημένο από ομότιμους (peer reviewed) - είναι ένας γενικός όρος για μια διαδικασία αυτορύθμισης ή μια διαδικασία αξιολόγησης που πραγματοποιείται από καταρτισμένα άτομα για τον σχετικό τομέα. Οι μέθοδοι ομότιμης επισκόπησης υιοθετούνται για να υποστηρίξουν πρότυπα, να βελτιώσουν την απόδοση και να παρέχουν αξιοπιστία.

- Τα συνιστώμενα αντίμετρα.
- Τις αναφορές σε εξωτερικά έγγραφα.

5.1.2 Βασικοί στόχοι

5.1.2.1 Οι στόχοι του ISSAF

Οι βασικοί στόχοι του ISSAF έχουν ως ακολούθως:

- Να ενεργεί ως έγγραφο αναφοράς για την αξιολόγηση της ασφάλειας που καλύπτει τη διαδικασία από την αρχή έως το τέλος.
- Να τυποποιήσει τη διαδικασία αξιολόγησης της ασφάλειας συστημάτων πληροφοριών.
- Να θέσει το ελάχιστο επίπεδο αποδεκτής διαδικασίας.
- Να παρέχει ένα βασικό τρόπο σύμφωνα με τον οποίο μια αξιολόγηση μπορεί (ή πρέπει) να εκτελεσθεί.
- Να αξιολογεί τα μέτρα προστασίας που αναπτύχθηκαν ενάντια στη μη εξουσιοδοτημένη πρόσβαση.
- Να ενεργεί ως αναφορά για την υλοποίηση της ασφάλειας πληροφοριών.
- Να ενισχύσει τις υπάρχουσες διαδικασίες και την τεχνολογία ασφάλειας.

5.1.2.2 Οι σκοποί του ISSAF

Ο σκοπός του ISSAF είναι να παρέχει ένα ενιαίο σημείο αναφοράς για την αξιολόγηση της ασφάλειας. Πρόκειται για μια αναφορά που ευθυγραμμίζεται με τα πραγματικά ζητήματα αξιολόγησης της ασφάλειας και αποτελεί μια σημαντική πρόταση για τις επιχειρήσεις. Για την επίτευξη αυτού του στόχου, το ISSAF ακολουθεί τα παρακάτω:

- Αξιολόγηση των πολιτικών και των διαδικασιών της ασφάλειας πληροφοριών των οργανισμών και εξασφάλιση ότι καλύπτουν τις απαιτήσεις της βιομηχανίας και ότι δεν παραβιάζουν οποιουσδήποτε νόμους και κανονισμούς που εφαρμόζονται.
- Προσδιορισμός της υποδομής συστημάτων των κρίσιμων πληροφοριών που απαιτείται για τις επιχειρησιακές διαδικασίες των οργανισμών και αξιολόγηση της ασφάλειά τους.
- Διεξαγωγή αξιολογήσεων ευπάθειας και ελέγχων διείσδυσης, προκειμένου να δοθεί έμφαση στο σύστημα με τις ευπάθειες και με αυτόν τον τρόπο να προσδιοριστούν οι αδυναμίες στα συστήματα, τα δίκτυα και τις εφαρμογές.
- Αξιολόγηση των ελέγχων που εφαρμόζονται σε διάφορες περιοχές ασφάλειας με τους εξής τρόπους: (α) Εύρεση των εσφαλμένων ρυθμίσεων και αποκατάσταση αυτών. (β) Προσδιορισμός των κινδύνων που αφορούν τις τεχνολογίες και εξέταση αυτών. (γ) Προσδιορισμός των κινδύνων που σχετίζονται με τις επιχειρησιακές διαδικασίες ή/και τους ανθρώπους και εξέταση αυτών. (δ) Ενίσχυση των υπαρχουσών διαδικασιών και τεχνολογιών.
- Παραχώρηση προτεραιότητας σε δραστηριότητες αξιολόγησης σύμφωνα με την κρισιμότητα των συστημάτων, τις δαπάνες του ελέγχου και τα πιθανά οφέλη.
- Εκπαίδευση ανθρώπων στην εκτέλεση των αξιολογήσεων της ασφάλειας.
- Εκπαίδευση ανθρώπων στην εξασφάλιση των συστημάτων, των δικτύων και των εφαρμογών.

- Παροχή πληροφοριών σχετικά με την: Επισκόπηση των διαδικασιών καταγραφής, παρακολούθησης και ελέγχου. Δόμηση και επισκόπηση του σχεδίου ανάκτησης καταστροφής (Disaster Recovery Plan). Επισκόπηση των υποθέσεων εξωγενούς ασφάλειας.
- Συμμόρφωση σε νομικά και ρυθμιστικά πρότυπα.
- Δημιουργία συνειδητοποίησης της ασφάλειας.
- Αποτελεσματική διαχείριση των προγραμμάτων αξιολόγησης της ασφάλειας.
- Προστασία ενάντια στην εκμετάλλευση κοινωνικής μηχανικής.
- Επισκόπηση ελέγχου της φυσικής ασφάλειας.

5.2 Εμβέλεια

5.2.1 Το πλαίσιο

Βάσει των ανωτέρω, αυτό που απαιτείται είναι μια συστηματική προσέγγιση που θα βοηθήσει ένα ενδιαφερόμενο μέρος (έναν οργανισμό) να θεωρήσει την ασφάλεια ως μια πρωτοβουλία, να παραθέσει πειστικά επιχειρησιακά επιχειρήματα (εάν είναι απαραίτητο) για να επενδύσει σε αυτήν την πρωτοβουλία, να συνεχίσει με τον προσδιορισμό του ποιες δραστηριότητες πρέπει να πραγματοποιηθούν βήμα προς βήμα και έπειτα, να διαχειριστεί μια προς μια αυτές τις δραστηριότητες έως ότου να μπορεί να παραχθεί ένα λογικό επίπεδο διαβεβαίωσης σχετικά με την ασφάλεια των αγαθών πληροφοριών τους. Το ISSAF παρέχει ένα μοντέλο πέντε φάσεων που δομεί τη διαχείριση των πρωτοβουλιών ασφάλειας και εξασφαλίζει τη βιωσιμότητα της δέσμευσης με την παροχή της απαραίτητης τεχνογνωσίας υπό μορφή πακέτων εργασίας με κατάλληλο μέγεθος (που καλούνται δραστηριότητες), τα οποία μπορούν να ανατεθούν σε κάποια άτομα μέσα στην ομάδα έργου.

Οι πέντε φάσεις αντίστοιχα είναι: Σχεδιασμός, Αξιολόγηση, Αντιμετώπιση, Διαπίστευση και Συντήρηση. Κάθε μια από αυτές τις φάσεις έχει συγκεκριμένα πακέτα εργασίας που είναι γενικά και μπορούν να εφαρμοστούν σε όλους τους οργανισμούς, ανεξάρτητα από το μέγεθός τους, τις συγκεκριμένες περιοχές δραστηριότητάς τους και τη γεωγραφική τοποθεσία τους. Μέσω της αλληλουχίας των αντίστοιχων πακέτων εργασίας τους, αυτές οι φάσεις εστιάζουν στην παράδοση συγκεκριμένων αποτελεσμάτων, είτε πρόκειται για ένα παραδοτέο, είτε για μια επιθυμητή κατάσταση των υποθέσεων. Τα αποτελέσματα αυτών των φάσεων έπειτα ακολουθούνται από τις λειτουργικές δραστηριότητες που σχεδιάζονται με σκοπό να ενσωματώσουν το παραδοτέο ή να διατηρήσουν αποτελεσματικά την επιτευχθείσα κατάσταση.

5.2.1.1 Φάση I - Σχεδιασμός (Planning)

Η Φάση I - Σχεδιασμός περιλαμβάνει τις εξής δραστηριότητες:

- Συλλογή Πληροφοριών (Information Gathering): Όποια και να είναι η αφορμή, αυτό που έχει σημασία είναι ότι οι πληροφορίες πρέπει να συγκεντρωθούν για να τεκμηριώσουν την υποκείμενη υπόθεση (ανησυχία).
- Καταστατικό Έργου (Project Chartering): Συστήνεται ο προσδιορισμός των κρίσιμων παραγόντων επιτυχίας (επιθυμητά αποτελέσματα) και στη συνέχεια η απεικόνιση αυτών σε όλες τις βασικές εσωτερικές επιχειρησιακές διαδικασίες, συμπεριλαμβάνοντας τα έσοδα και τις δαπάνες, ως αρχικό βήμα.
- Προσδιορισμός Πόρων (Resource Identification): Οι πόροι μπορεί να αναφέρονται σε ανθρώπους, προϊόντα, διαδικασίες, εργαλεία, γνώση και υποστήριξη πολιτικής. Ο στόχος αυτής της δραστηριότητας είναι να ερευνηθεί

ο τύπος και τα πιθανά κόστη των πόρων που θα απαιτηθούν για να εκτελεστεί αυτό το έργο (project).

- Σύνταξη Προϋπολογισμού (Budgeting): Στη συνέχεια, προετοιμάζεται ένας προϋπολογισμός που προσδιορίζει τις επενδύσεις και τις επόμενες λειτουργικές δαπάνες, προκείμενου να αποσαφηνιστεί εάν η απαραίτητη χρηματοδότηση είναι πιθανό να γίνει εφικτή από μια γενική επιχειρησιακή προοπτική.
- Προετοιμασία Αιτήσεων-Ταμειακών Ροών (Cash flow[61] - pro forma[62] preparation): Είναι σημαντικό να προετοιμαστούν τα εξής: Εισοδηματική δήλωση (κέρδος και απώλεια), Ισολογισμός.
- Δομή κατάτμησης εργασιών (Work breakdown structure): Μια δομή κατάτμησης εργασιών (WBS) ουσιαστικά δημιουργεί ένα πλαίσιο που ομαδοποιεί και ενσωματώνει τα μεμονωμένα πακέτα εργασίας που θα λειτουργήσουν για να παραδώσουν τα αποτελέσματα του έργου.
- Έναρξη Έργου (Project kick-off): Ο αρχικός σκοπός του Project kick-off είναι να οριστεί τυπικά ένας διαχειριστής έργου. Αυτό εξασφαλίζει ότι ο διαχειριστής έργου έχει την απαραίτητη διαφάνεια και τη λειτουργική εξουσιοδότηση για να λάβει τις απαιτούμενες αποφάσεις προκειμένου να παραδώσει τα καθορισμένα αποτελέσματα του έργου.
- Σχέδιο Έργου - Εξόδου (Output - Project Plan): Με βάση τα ανωτέρω αποτελέσματα, προετοιμάζεται το τελικό σχέδιο του έργου, ενσωματώνοντας χρονοδιαγράμματα και πόρους στις δομές κατάτμησης εργασιών. Αυτό το αρχικό σχέδιο του έργου θα χρησιμεύσει έπειτα ως η βασική γραμμή που πρέπει να ακολουθηθεί, για να επιτηρηθεί και να ελεγχθεί η πραγματική εκτέλεση των προβαλλόμενων αποτελεσμάτων.

5.2.1.2 Φάση ΙΙ - Αξιολόγηση (Assessment)

Η φάση της αξιολόγησης παρέχει μια ολιστική προσέγγιση στην αξιολόγηση των κινδύνων ασφάλειας πληροφοριών για μια επιχείρηση. Αυτή η φάση υποστηρίζει την προσέγγιση των αξιολογήσεων του κινδύνου της ασφάλειας πληροφοριών από την προοπτική των επιχειρηματικών στόχων και των σχετικών κινδύνων. Το πλαίσιο αρχίζει με μια αξιολόγηση του επιχειρηματικού κινδύνου (Enterprise Risk Assessment) της επιχείρησης, η οποία βοηθά στον προσδιορισμό του εγγενούς κινδύνου συνολικά για την επιχείρηση. Οι εγγενείς κίνδυνοι[63] που προσδιορίζονται κατά τη διάρκεια της αξιολόγησης χρησιμοποιούνται περαιτέρω για να προσδιορίσουν συγκεκριμένους κινδύνους που προέρχονται από τη φύση και την έκταση της χρήσης της τεχνολογίας πληροφοριών (Information Technology) στην επιχείρηση. Στη συνέχεια, οι προσδιορισμένοι κίνδυνοι της τεχνολογίας πληροφοριών χρησιμοποιούνται, για να διατυπώσουν τις απαιτήσεις ελέγχου και ασφάλειας της επιχείρησης.

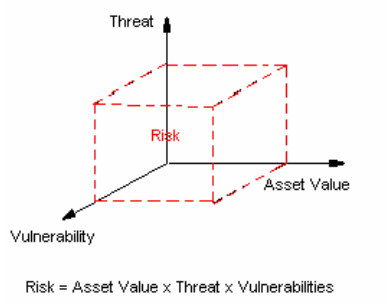
[61] Στην οικονομική λογιστική, μια δήλωση ταμειακών ροών (cash flow) είναι μια οικονομική δήλωση που επιδεικνύει το πώς οι αλλαγές στους λογαριασμούς ισολογισμών και τα έσοδα, έχουν επιπτώσεις στα μετρητά και τα ισοδύναμα μετρητών (cash equivalents) και διασπά την ανάλυση σε δραστηριότητες χρηματοδότησης, επένδυσης και λειτουργίας.

[62] pro forma - αίτηση, που παρέχεται εκ των προτέρων σε μια ορισμένη μορφή ή περιγράφει ένα στοιχείο, π.χ. για τον τύπο της οικονομικής δήλωσης ή για τον τύπο του τιμολογίου.

[63] Εγγενής κίνδυνος (inherent risk). Ο κίνδυνος αυτός έχει να κάνει με τα ιδιαίτερα χαρακτηριστικά της επιχείρησης (κλάδος, μέγεθος, κ.ά.) που ελέγχεται.

Επομένως, ο κίνδυνος είναι μια συνάρτηση της αξίας του αγαθού, των απειλών και των ευπαθειών και μπορεί να είναι υπολογιστεί ως εξής:

Κίνδυνος (Risk) = Αξία Αγαθού (Asset Value) x Απειλές (Threats) x Ευπάθειες (Vulnerabilities)



Σχήμα 33: Υπολογισμός κινδύνου.

Έχοντας ως δεδομένα τα κόστη της υλοποίησης και διατήρησης της ασφάλειας και τους ελέγχους στο περιβάλλον τεχνολογίας πληροφοριών (IT), μια επιχείρηση θα εξέταζε το όφελος του κόστους οποιασδήποτε υλοποίησης της ασφάλειας, μετρώντας το κόστος του ελέγχου σε σχέση με την επίπτωση της μη διενέργειας ενός τέτοιου ελέγχου. Στις περιπτώσεις όπου το κόστος του ελέγχου υπερβαίνει την επίπτωση του κινδύνου και από την πλευρά της προσπάθειας και της αξίας, τότε η επιχείρηση μπορεί να επιλέξει να μην εφαρμόσει τέτοιους μηχανισμούς ασφάλειας ή ελέγχου. Εναλλακτικά, η χαμηλή σημασία της επίπτωσης των κινδύνων μπορεί επίσης να προτρέψει μια επιχείρηση ώστε να μην υλοποιήσει οποιουσδήποτε συγκεκριμένους ελέγχους για να μετριάσει αυτούς τους κινδύνους. Τέτοιοι κίνδυνοι θεωρούνται ως «υπολειμματικοί κίνδυνοι - Residual Risks[64]».

Η φάση της αξιολόγησης χωρίζεται σε δύο κατηγορίες:

1. Αξιολόγηση Εγγενούς Κινδύνου (Inherent Risk Assessment):
   - Προετοιμασία Αξιολόγησης (Assessment Preparation): Εκτελούνται οι ακόλουθες δραστηριότητες:
     - Προσδιορισμός των οντοτήτων Αξιολόγησης (Identification of Assessment entities): Αυτές θα μπορούσε να είναι διαδικασίες, αγαθά, εγκαταστάσεις κ.λπ. Οι οντότητες αξιολόγησης αποτελούν τη βάση για τον προσδιορισμό των εφαρμόσιμων παραμέτρων αξιολόγησης, απειλών, κ.λπ. στις οντότητες.
     - Προσδιορισμός απειλών και ευπαθειών (Identify threats and Vulnerabilities): Οι διάφορες ευπάθειες των επιλεγμένων ή προσδιορισμένων οντοτήτων για την αξιολόγηση είναι τεκμηριωμένες. Στη συνέχεια, προσδιορίζονται και απαριθμούνται οι απειλές που θα μπορούσαν να εκμεταλλευτούν τις ευπάθειες. Αυτές οι απειλές αποτελούν τους κινδύνους για τις οντότητες. Οι κίνδυνοι αυτοί μπορούν να είναι επαναλαμβανόμενοι σε μια οντότητα.
   - Αξιολόγηση Απειλών (Threat Assessment): Εκτελούνται οι ακόλουθες δραστηριότητες:
     - Αξιολόγηση της Επίπτωσης (Impact Assessment): Η επίπτωση μιας απειλής, στην επιχείρηση ενός οργανισμού, η οποία πραγματοποιείται ενάντια σε ένα αγαθό, μετριέται ή υπολογίζεται. Αυτό γίνεται χωριστά για κάθε οντότητα αγαθών και δεν εξετάζει τους παράγοντες μετριασμού του κινδύνου. Είναι μια μέτρηση του ακατέργαστου κινδύνου. Ο αξιολογητής μπορεί να επιλέξει

[64] Residual Risks - υπολειμματικός ή εναπομένων κίνδυνος. Ένας αρκετά μικρότερος κίνδυνος. Γενικά, είναι ο κίνδυνος που παραμένει και είναι αδύνατο να προσδιορισθεί με περισσότερες λεπτομέρειες παρά την εφαρμογή όλων των επιστημονικών μεθόδων ανίχνευσης και εξουδετέρωσης. Στα πληροφοριακά συστήματα σημαίνει τον κίνδυνο που εξακολουθεί να υφίσταται παρά την εφαρμογή όλων των εσωτερικών ποσοτικών ελέγχων. Σε μερικές περιπτώσεις, ο residual risk αφορά κυρίως την παράνομη είσοδο μη εξουσιοδοτημένων προσώπων στο σύστημα παρά τα εξαντλητικά μέτρα ασφαλείας που έχουν ληφθεί.

να υπολογίσει το μέσο όρο ή το άθροισμα των τιμών παραμέτρου αξιολόγησης για μαθηματικούς ή λογικούς λόγους.

- Αξιολόγηση της Πιθανότητας (Likelihood Assessment): Εδώ, μετριέται ή υπολογίζεται η πιθανότητα του περιστατικού της απειλής για την επιλεγμένη οντότητα αξιολόγησης.

Τα σύνολα που προκύπτουν από τις δύο παραπάνω διεργασίες αποτελούν τον εγγενή κίνδυνος για την οντότητα που αξιολογείται.

2. Αξιολόγηση Ελέγχων (Controls Assessment):

Οι αντισταθμιστικοί έλεγχοι μπορεί να τίθενται σε ισχύ ώστε να μειώσουν ή να μετριάσουν τους κινδύνους. Αυτοί οι παράγοντες πρέπει να αντιπροσωπεύονται σε μια καλή αξιολόγηση του κινδύνου. Μετά την απόκτηση του εγγενούς κινδύνου μιας οντότητας αξιολόγησης, η αξιολόγηση των ελέγχων εκτελείται για να προσδιορίσει το ποσό μείωσης του κινδύνου που προσφέρουν και τον υπολειμματικό κίνδυνο (residual risk) που απομένει για την οντότητα αξιολόγησης. Κατά τη διάρκεια αυτής της φάσης, ο αξιολογητής μπορεί να επιλέξει τους ελέγχους από το ISSAF ή άλλους ελέγχους. Το σημαντικό είναι να προσδιοριστεί ότι η επιλογή του ελέγχου είναι επαρκής και ότι η ύπαρξη και η συμβολή του ελέγχου είναι αποδεκτή για την απόφαση του κινδύνου. Η σημαντικότερη πτυχή της αξιολόγησης ελέγχου είναι να αξιολογηθεί ο έλεγχος ενάντια στην παράμετρο αξιολόγησης ώστε να επαληθεύσει ότι η επίπτωση μιας δεδομένης παραμέτρου αξιολόγησης πρέπει να μειωθεί σε ένα αποδεκτό επίπεδο. Το αποτέλεσμα αυτού του στόχου είναι ο υπολειμματικός κίνδυνος (residual risk) για την οντότητα αξιολόγησης. Οι διαθέσιμες περιοχές ελέγχου για τις οντότητες αξιολόγησης που μπορεί να επιλέξει ο αξιολογητής από το ISSAF δίνονται κατωτέρω.

- Αξιολόγηση Νομικής και Ρυθμιστικής Συμμόρφωσης (Evaluation of Legal and Regulatory Compliance): Είναι ουσιαστική μια επισκόπηση των νομικών και ρυθμιστικών απαιτήσεων που έχουν επίπτωση στην επιχείρηση, προκειμένου να εξασφαλιστεί ότι η επιχείρηση είναι σύμφωνη με τους νόμους και κανονισμούς που ισχύουν στην υποδομή τεχνολογίας πληροφοριών (IT) της επιχείρησης.
- Αξιολόγηση της Πολιτικής Ασφάλειας Επιχειρηματικών Πληροφοριών (Evaluation of Enterprise Information Security Policy): Κατά την έναρξη μιας αξιολόγησης της επιχειρηματικής ασφάλειας, ένας από τους πρώτους στόχους θα ήταν να γίνει κατανοητή και να αξιολογηθεί η πολιτική ασφάλειας πληροφοριών της επιχείρησης. Η πολιτική ασφάλειας πληροφοριών είναι μια αντανάκλαση της πρόθεσης και της προσέγγισης της διαχείρισης στην ασφάλεια πληροφοριών και συνοψίζει την έκταση και τη φύση της ασφάλειας πληροφοριών που εφαρμόζεται μέσα στην επιχείρηση. Μια επισκόπηση της πολιτικής ασφάλειας των επιχειρηματικών πληροφοριών είναι απαραίτητη για να αποκτηθεί μια διεξοδική κατανόηση της προσέγγισης που χρησιμοποιείται για την υλοποίηση και διατήρηση της ασφάλειας των πληροφοριών του οργανισμού.
- Αξιολόγηση της Οργάνωσης και της Διαχείρισης Ασφάλειας Επιχειρηματικών Πληροφοριών (Evaluation of Enterprise Information Security Organization and Management): Μετά από την αξιολόγηση του επιχειρηματικού κινδύνου και την επισκόπηση της πολιτικής ασφάλειας των πληροφοριών, εκτελείται μια επισκόπηση της οργάνωσης και της διαχείρισης της ασφάλειας πληροφοριών. Αυτό περιλαμβάνει μια επισκόπηση της οργάνωσης των

λειτουργιών της ασφάλειας, των σχετικών ρόλων και των ευθυνών, καθώς και των ευθυνών διαχείρισης, μεταξύ άλλων περιοχών. Έχοντας κατανοήσει τους κινδύνους που εφαρμόζονται στην υποδομή της τεχνολογίας της επιχείρησης, την προσέγγιση της επιχείρησης στη διαχείριση της ασφάλειας όπως δηλώνεται στην πολιτική της ασφάλειας πληροφοριών (IT) της και την κατανομή των ρόλων και των ευθυνών ασφάλειας, θα ήταν λογικό να αξιολογηθεί η συγκεκριμένη υποδομή ασφάλειας και οι λειτουργικοί έλεγχοι που εφαρμόζονται μέσα στην επιχείρηση, προκειμένου να μετριασθούν οι προσδιορισμένοι κίνδυνοι της τεχνολογίας πληροφοριών (IT). Αυτή η φάση του πλαισίου αξιολόγησης του κινδύνου ασφάλειας αποτελείται από:

- Αξιολόγηση Επιχειρηματικής Ασφάλειας και Ελέγχων (Enterprise Security and Controls Assessment): Αυτή η φάση περιλαμβάνει μια επισκόπηση των παρακάτω (Πίνακας 17. Αξιολόγηση Επιχειρηματικής Ασφάλειας και Ελέγχων
-):

Αξιολόγηση Επιχειρηματικής Ασφάλειας και Ελέγχων	
• Φυσική και Περιβαλλοντική Ασφάλεια (Physical and Environmental Security)	
• Τεχνικοί Έλεγχοι (Technical Controls)	- Ασφάλεια Δικτύων (Network Security) - Ασφάλεια Ξενιστών (Host[65] Security) - Ασφάλεια Εφαρμογών (Application Security) - Ασφάλεια Βάσεων Δεδομένων (Database security)
• Αξιολόγηση της Συνειδητοποίησης της Ασφάλειας (Evaluation of Security Awareness) χρησιμοποιώντας:	- Συνεντεύξεις (Interviews) - Παρατήρηση (Observation) - Δομημένη συστηματική εξέταση (Structured walk through[66]) - Κοινωνική Μηχανική (Social Engineering)

Πίνακας 17. Αξιολόγηση Επιχειρηματικής Ασφάλειας και Ελέγχων

- Αξιολόγηση Διαχείρισης Λειτουργιών (Operations Management Assessment): Αυτή η επισκόπηση εκτελείται από κοινού με την Αξιολόγηση Επιχειρηματικής Ασφάλειας και Ελέγχων, για να αποκτηθεί μια κατανόηση των κινδύνων και των ελέγχων των λειτουργιών ασφάλειας. Αυτό αποτελείται από την αξιολόγηση των ακόλουθων λειτουργικών περιοχών (Πίνακας 18. Αξιολόγηση Διαχείρισης Λειτουργιών):

[65] host - Ένας οικοδεσπότης ή ξενιστής υπολογιστής (έμμεσα αυτός που φιλοξενεί) είναι μια προσπελάσιμη οντότητα μέσα σε ένα δίκτυο υπολογιστών. Κάθε οικοδεσπότης έχει μια μοναδική διεύθυνση μέσα σε ένα δίκτυο.

[66] Μια επίσημη μέθοδος αποσφαλμάτωσης ενός προγράμματος ή συστήματος υπολογιστών, που περιλαμβάνει μια συστηματική επισκόπηση για αναζήτηση λαθών και ανεπαρκειών.

Αξιολόγηση Διαχείρισης Λειτουργιών	
• Διαχείριση Χωρητικότητας (Capacity Management[67])	
• Διαχείριση Ευπαθειών (Vulnerability Management)	
• Διαχείριση απελευθέρωσης (Release Management)	- Διαχείριση επιδιορθώσεων (Patch Management[68]) - Διαχείριση διαμορφώσεων (Configuration Management[69]) - Διαχείριση Αλλαγών (Change Management[70])
• Διαχείριση Επιχειρηματικών Συμβάντων (Enterprise Incident Management[71])	- Καταγραφή (Logging) - Έλεγχος (Monitoring) - Διαχείριση Συμβάντων Ασφάλειας (Security Incident Management) - Διαχείριση Γεγονότων Λειτουργίας (Operation Event Management)
• Διαχείριση Χρηστών (User Management)	
• Πιστοποίηση και Διαπίστευση (Certification and Accreditation)	

Πίνακας 18. Αξιολόγηση Διαχείρισης Λειτουργιών

- Αξιολόγηση της Διαχείρισης Επιχειρηματικής Συνέχειας (Evaluation of Enterprise Business Continuity Management): Μια αξιολόγηση των ικανοτήτων της διαχείρισης της συνέχειας της επιχείρησης είναι ουσιαστική ώστε να αξιολογηθεί η επάρκεια της ετοιμότητας της επιχείρησης όσον αφορά την εξασφάλιση της διαθεσιμότητας της υποδομής τεχνολογίας πληροφοριών (IT). Αυτή η επισκόπηση συμπληρώνεται με μια επισκόπηση των διαδικασιών επιχειρησιακής συνέχειας της επιχείρησης για να εξασφαλιστεί ότι σε περίπτωση καταστροφής η επιχείρηση είναι επαρκώς έτοιμη να συνεχίσει τις βασικές επιχειρησιακές λειτουργίες μέχρι ότου να αποκατασταθούν εντελώς οι κανονικές λειτουργίες.
- Διαχείριση υπολειμματικών κινδύνων (Manage Residual Risks): Όπως αναφέρθηκε νωρίτερα, οι κίνδυνοι που δεν καλύπτονται από την επιχειρηματική ασφάλεια και τις υλοποιήσεις των ελέγχων ταξινομούνται στην κατηγορία των υπολειμματικών κινδύνων (Residual Risks). Δεδομένης της ασταθούς φύσης της επιχείρησης και των πάντα μεταβαλλόμενων κινδύνων που εφαρμόζονται γενικά στη βιομηχανία και στην τεχνολογία πληροφοριών, είναι σημαντικό τακτικά να διεξάγεται επισκόπηση των υπολειμματικών κινδύνων που δεν εξετάζονται από το πλαίσιο διαχείρισης της ασφάλειας πληροφοριών (Information Security Management Framework) μιας επιχείρησης. Αυτό απαιτείται για να εξασφαλιστεί ότι οι κίνδυνοι που ήταν

[67] Capacity management: εξασφαλίζει ότι οι πόροι IT χρησιμοποιούνται με αποδοτικό τρόπο όσον αφορά τη διαθεσιμότητα. Εξασφαλίζει το κατάλληλο όριο χρήσης του δίσκου (disk quota), τους χρόνους απάντησης, την επεξεργασία και την χωρητικότητα των δικτύων και συστημάτων.

[68] Patch management: καλύπτει τα εργαλεία ή βοηθήματα, τις πολιτικές και τις διαδικασίες που χρησιμοποιούνται για να διατηρηθούν τα συστήματα με νέες ενημερώσεις (updates) λογισμικού, που εκδίδονται αφού αναπτυχθεί το λογισμικό.

[69] Configuration Management: Η ασφάλεια εφαρμογών εξασφαλίζει ότι οι λειτουργικές εφαρμογές που υποστηρίζουν μια επιχειρησιακή διαδικασία, έχουν αναπτυχθεί, επεκταθεί και διατηρηθεί με ασφαλή τρόπο.

[70] Η διαδικασία Change management εξασφαλίζει ότι η ακεραιότητα των δεδομένων, τα προγράμματα εφαρμογής και οι ρυθμίσεις της ασφάλειας συστημάτων διατηρούνται σύμφωνα με τα πρότυπα και συναντούν τα αποδεκτά επίπεδα.

[71] Enterprise Incident Management: αφορά τον προσδιορισμό, την έρευνα και την ανάλυση των συμβάντων ασφάλειας που σχετίζονται με την υποδομή των συστημάτων πληροφοριών μιας επιχείρησης.

προηγουμένως ταξινομημένοι στην κατηγορία των υπολειμματικών κινδύνων, κλιμακώνονται και διαχειρίζονται κατάλληλα, καθώς αλλάζει η σχέση και η σημασία τους για την επιχείρηση. Εκτελείται μια επισκόπηση της διαδικασίας για τη διαχείριση των υπολειμματικών κινδύνων για να εξασφαλιστεί ότι οι υπολειμματικοί κίνδυνοι επισκοπούνται και επαναξιολογούνται τακτικά, ώστε να εξασφαλιστεί ότι δεν έχει αλλάξει η κρισιμότητα της κατάστασής τους και ότι δεν έχει αυξηθεί η ανάγκη για ελέγχους σε αυτές τις περιοχές.

5.2.1.3 Φάση III - Αντιμετώπιση (Treatment)

Η επεξεργασία κινδύνου παρέχει μια πλατφόρμα για τη λήψη μιας απόφασης σχετικά με τους υπόλοιπους κινδύνους, μέσω της επιλογής των μέτρων προστασίας, της ανάπτυξης των σχεδίων υλοποίησης, της παροχής της λεπτομερούς τεκμηρίωσης για την υλοποίηση και της διαδικασίας λήψης αποφάσεων.

5.2.1.4 Φάση IV - Διαπίστευση (Accreditation)

Η διαδικασία της διαπίστευσης περιλαμβάνει την αξιολόγηση των ελέγχων που έχουν επιλεχθεί για υλοποίηση σύμφωνα με την εμβέλεια της πιστοποίησης. Τα αποτελέσματα της αξιολόγησης αποδεικνύουν την διαπίστευση της πιστοποίησης ISSAF σε έναν οργανισμό. Η φάση αυτή περιλαμβάνει: Καθιέρωση πλαισίου (Context Establishment), Αξιολόγηση (Evaluation), Υποβολή έκθεσης (Reporting), Πιστοποίηση (Certification).

5.2.1.5 Φάση V - Συντήρηση (Maintenance)

Οι οργανισμοί που έχουν πιστοποιηθεί από το ISSAF, οφείλουν να αποδεικνύουν συμμόρφωση στην πιστοποίηση του ISSAF σε συνεχή βάση. Για να εξασφαλισθεί κάτι τέτοιο, το Open Information System Security Group (OISSG) θα διεξάγει τακτικά σχεδιασμένες αξιολογήσεις ή επιθεωρήσεις συμμόρφωσης. Η συχνότητα για αυτήν την επιθεώρηση θα βασιστεί στο μέγεθος του οργανισμού και της εμβέλειας της πιστοποίησης.

5.2.2 Διαχείριση Δέσμευσης

Μια δέσμευση ομαδοποιεί τις δραστηριότητες οι οποίες, όταν χρησιμοποιούνται συνολικά, επιτυγχάνουν έναν στόχο. Μια δέσμευση έχει πάντα μια αναγνωρίσιμη έναρξη και ένα τέλος. Η δέσμευση της αξιολόγησης της ασφάλειας συνεπάγεται τους πολυάριθμους στόχους και περιλαμβάνει διάφορα συμβαλλόμενα μέρη. Μια τέτοια δέσμευση απαιτεί το σχεδιασμό της από την αρχή και τη δραστηριότητα διαχείρισης κατά τη διάρκεια της ανάπτυξή της. Σε αυτήν την παράγραφο περιγράφονται συνοπτικά οι πτυχές διαχείρισης της δέσμευσης για μια δέσμευση αξιολόγησης της ασφάλειας. Οι ακόλουθες οδηγίες[72] [OISSG, (April 18, 2006)] μπορούν να χρησιμοποιηθούν άμεσα για την παροχή του σχεδίου διαχείρισης της δέσμευσης στον πελάτη (Πίνακας 19. Οδηγίες για Διαχείριση Δέσμευσης.).

[72] Περισσότερες πληροφορίες αναφέρονται στο Information Systems Security Assessment Framework (ISSAF) Draft 0.2, κεφάλαιο 4, σελίδα 39.

Οδηγίες για Διαχείριση Δέσμευσης.	
1. Επιτελική επισκόπηση δέσμευσης (Engagement executive Overview)	11. Καθορισμός ορόσημων και χρονοδιαγραμμάτων (Set Milestones and Timelines)
2. Στόχος (Objective)	12. Χρονοδιάγραμμα δέσμευσης (Engagement Schedule)
3. Προσέγγιση (Approach)	13. Παραδοτέα που παράγονται (Deliverables produced)
4. Εμβέλεια δέσμευσης (Engagement scope)	14. Εκτίμηση δέσμευσης για την προσπάθεια/κόστος/διάρκεια - το κόστος είναι προαιρετικό (Engagement estimated effort/cost/duration-Cost Optional)
5. Εναρκτήρια συνάντηση δέσμευσης - εσωτερική (Engagement kickoff meeting-Internal)	15. Παραδοχές δέσμευσης (Engagement assumptions)
6. Σχέδιο επικοινωνιών (Communications plan)	16. Κίνδυνοι δέσμευσης (Engagement risks)
7. Εναρκτήρια συζήτηση δέσμευσης με τον πελάτη (Engagement kickoff Discussion with client)	17. Προσέγγιση δέσμευσης (Engagement approach)
8. Δείγμα Έκθεσης Κατάστασης (Sample Status Report)	18. Οργάνωση δέσμευσης-ομάδα αξιολόγησης & πελάτης (Engagement organization-Assessment Team & Client)
9. Σχέδιο Κλιμάκωσης Ζητημάτων (Issue Escalation Plan)	19. Πίνακας ευθυνών (Responsibility Matrix)
10. Ανάπτυξη ενός σχεδίου δέσμευσης και αποστολή αυτού στον πελάτη για ενημέρωση. (Develop a Engagement Plan and Send it to Customer for update)	20. SIGN-OFF Sheet
	21. Παράρτημα - Χάρτης πορείας διαχείρισης αξιολόγησης (Annexure - Assessment Administration Roadmap)

Πίνακας 19. Οδηγίες για Διαχείριση Δέσμευσης.

5.2.3 Βέλτιστες Πρακτικές: Προ-Αξιολόγηση, Αξιολόγηση και Μετά-Αξιολόγηση

Αυτό το τμήμα του ISSAF, παρέχει όλες τις βέλτιστες πρακτικές ή οδηγίες[73] [OISSG, (April 18, 2006)] που απαιτούνται για να εκτελεστεί η αξιολόγηση της ασφάλειας. Τα μέλη της διαχείρισης που ασχολούνται με την αξιολόγηση και όλοι οι υπόλοιποι που ανήκουν στην ομάδα αξιολόγησης, πρέπει να το διαβάσουν και να το ακολουθήσουν. Τόσο ο οργανισμός για λογαριασμό του οποίου διενεργείται η αξιολόγηση όσο και οι διενεργούντες την αξιολόγηση πρέπει να το υπογράψουν πριν αρχίσει μια αξιολόγηση.

Η φάση - Ι: Πριν την Αξιολόγηση (Pre-Assessment) περιλαμβάνει τα παρακάτω:

- Αίτηση για Προτάσεις (Request for Proposal-RFP)
- Αξιολόγηση των Συμβάσεων Τρίτων (Evaluation of Third Party Contracts)
- Πωλήσεις και Μάρκετινγκ (Sales and Marketing)
- Απόκτηση Εξουσιοδότησης και Επιβεβαίωση ότι παρέχεται από τα σωστά άτομα (Obtain Authorization and Make sure Right People has given it)
- Καθορισμός της εμβέλειας της εργασίας (Define the scope of work)
- Καθορισμός των Περιοχών "εκτός Εμβέλειας" (Define the “Out of Scope” Areas)
- Υπογραφή Συμφωνίας (Sign Agreement)
- Σύνθεση Ομάδας (Team Composition)
- Αντιπρόσωποι (Commercials)

[73] Περισσότερες πληροφορίες αναφέρονται στο Information Systems Security Assessment Framework (ISSAF) Draft 0.2, κεφάλαιο 5, σελίδα 61.

- Διατήρηση της εμπιστευτικότητα των δεδομένων του πελάτη - πριν την έναρξη του έργου (Maintain confidentiality of client data - before start of Project)
- Προσδιορισμός σημείου πρόσβασης (Access Point Identification)

Η φάση - ΙΙ: Αξιολόγηση (Assessment) περιλαμβάνει τα παρακάτω:

- Κανόνες Δέσμευσης (Rules of Engagement)
- Χρόνος της Αξιολόγησης και Διαθεσιμότητα του Προσωπικού (Time of Assessment and Availability of Staff)
- Ένας μηχανισμός που ασχολείται με ψευδώς θετικές αναφορές (false positivew) ώστε να αποφευχθεί η άσκοπη κλήση των αρχών. (A mechanism for dealing with false positive to avoid calling law enforcement unnecessarily)
- Καταγραφή των Διευθύνσεων IP που πρέπει να αξιολογηθούν (Obtain IP Addresses or ranges that needs to be assessed)
- Αξιολόγηση Κεντρικών IP Διευθύνσεων (Assessment Centre IP Addresses)

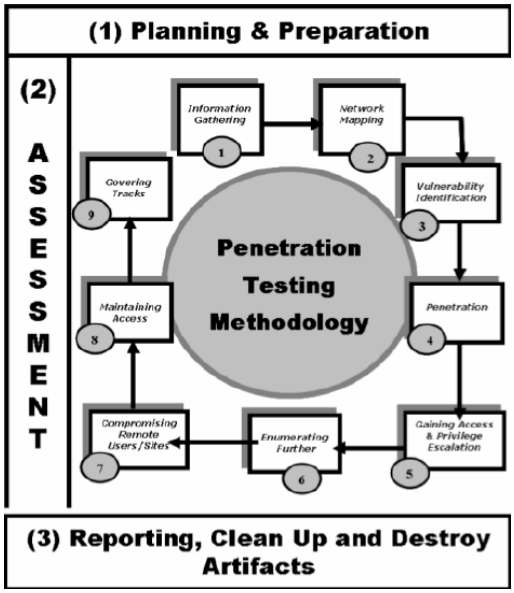
Η φάση - ΙΙΙ: Μετά την Αξιολόγηση (Post Assessment): Μετά από τη φάση της αξιολόγησης, αρχίζει η δραστηριότητα υποβολής της ανάλυσης και των εκθέσεων. Περιλαμβάνει τα παρακάτω:

- Υποβολή έκθεσης (Reporting)
- Παρουσίαση (Presentation)
- Μετά την παρουσίαση (After Presentation)

5.3 Βασική μεθοδολογία ασφάλειας

5.3.1 Μεθοδολογία Ελέγχου Διείσδυσης

Η μεθοδολογία ελέγχου διείσδυσης (Penetration testing) του ISSAF έχει ως σκοπό να αξιολογήσει τους ελέγχους των δικτύων, των συστημάτων και εφαρμογών. Αποτελείται από μια προσέγγιση τριών φάσεων και μια αξιολόγηση εννέα βημάτων [**Error! Reference source not found.**]. Η προσέγγιση περιλαμβάνει τις ακόλουθες τρεις φάσεις:



Σχήμα 34. Μεθοδολογία Ελέγχου Διείσδυσης

5.3.1.1 Φάση Ι: Σχεδιασμός και Προετοιμασία (Planning and Preparation)

Το ISSAF προσπαθεί να παρέχει στους χρήστες καθοδήγηση στον τομέα του σχεδιασμού και της προετοιμασίας - μια περιοχή που είναι πραγματικά κρίσιμη για έναν επιτυχή έλεγχο διείσδυσης.

Αυτή η φάση περιλαμβάνει τα βήματα που χρειάζονται για την ανταλλαγή των αρχικών πληροφοριών, τον σχεδιασμό και την προετοιμασία σχετικά με τον έλεγχο. Πριν τον έλεγχο, μια επίσημη Συμφωνία Αξιολόγησης (Assessment Agreement) θα πρέπει να υπογραφεί

από αμφότερα τα συμβαλλόμενα μέρη. Θα αποτελέσει τη βάση για την συγκεκριμένη ανάθεση αλλά και την αμοιβαία νομική προστασία. Επιπλέον, θα προσδιορίσει τη συγκεκριμένη ομάδα δέσμευσης, τις ακριβείς ημερομηνίες, τους χρόνους του ελέγχου, την πορεία κλιμάκωσης, καθώς και άλλες ρυθμίσεις. Σε αυτήν τη φάση προβλέπονται οι ακόλουθες δραστηριότητες:

- Προσδιορισμός των ατόμων επαφής και από τις δύο πλευρές,
- Εναρκτήρια συνάντηση για να επιβεβαιωθεί η εμβέλεια, η προσέγγιση και η μεθοδολογία και
- Συμφωνία σε συγκεκριμένες περιπτώσεις ελέγχου και πορείες κλιμάκωσης.

Γενικά υποστηρίζεται η άποψη ότι αυτή η φάση είναι σχετικά ανώφελη για ένα διαχειριστή επαγγελματικού έργου ελέγχου διείσδυσης. Αν και η μεθοδολογία βρίσκεται μόνο στην έκδοση 0.2B, πιθανολογείται ότι στο μέλλον είναι πιθανό αυτή η φάση της μεθοδολογίας ελέγχου διείσδυσης θα είναι πιο εύρωστη - μέχρι τότε όμως, θεωρούν ότι θα πρέπει να χρησιμοποιείται μια διαφορετική μεθοδολογία για τον σχεδιασμό και την προετοιμασία ενός επαγγελματικού έργου ελέγχου διείσδυσης.

5.3.1.2 Φάση - II: Αξιολόγηση (Assessment)

Ακριβώς επειδή το ISSAF δεν ορίζει το σχεδιασμό και την προετοιμασία μιας διείσδυσης αποτελεσματικά (όπως αναφέρθηκε προηγουμένως), δεν σημαίνει ότι το υπόλοιπο της μεθοδολογίας θα πρέπει να απορριφθεί. Ένα από τα ισχυρά σημεία του ISSAF είναι το επίπεδο λεπτομέρειας που παρέχεται στη σχετική τεκμηρίωση, η οποία περιλαμβάνει ακόμη και βαθμιαία παραδείγματα των εργαλείων λογισμικού και των εντολών που απαιτούνται για να τα «τρέξουν». Χρησιμοποιώντας το ISSAF, κάποιος που δεν έχει σχέση με τα εργαλεία ελέγχου διείσδυσης μπορεί να επαναλάβει τα παραδείγματα του εγγράφου και να αποκτήσει κάποια γνώση σχετικά με το τι κάνουν τα εργαλεία και τι σημαίνουν τα αποτελέσματά τους. Γενικά, δεν είναι η καλύτερη μέθοδος για τη διεξαγωγή ενός ελέγχου διείσδυσης, αλλά αποτελεί ένα αποτελεσματικό εργαλείο εκμάθησης για αυτούς που είναι νέοι στο επάγγελμα.

Κατά την φάση της αξιολόγησης, το ISSAF αναφέρεται στα βήματα που πρέπει να ακολουθηθούν κατά τη διάρκεια ενός ελέγχου διείσδυσης, γνωστά και ως «επίπεδα[74]». Αυτή είναι η φάση στην οποία πραγματοποιείται ο έλεγχος διείσδυσης. Όπως, αναφέραμε και πριν, η φάση της αξιολόγησης βασίζεται σε μια προσέγγιση επιπέδων που θα πρέπει να ακολουθηθεί, όπως φαίνεται στο **Error! Reference source not found.**. Κάθε επίπεδο αντιπροσωπεύει ένα μεγαλύτερο επίπεδο πρόσβασης στα αγαθά πληροφοριών της επιχείρησης. Αυτά τα επίπεδα, καθώς και η σημασία τους σύμφωνα με το ISSAF είναι τα ακόλουθα [OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B]:

- Συλλογή Πληροφοριών (Information Gathering): Χρήση του Διαδικτύου για να ευρεθούν όλες οι σχετικές πληροφορίες με τον στόχο, χρησιμοποιώντας και τεχνικές και μη τεχνικές μεθόδους.
- Χαρτογράφηση Δικτύων (Network Mapping): Προσδιορισμός όλων των συστημάτων και των πόρων μέσα στο δίκτυο-στόχο.
- Προσδιορισμός Ευπαθειών (Vulnerability Identification): Οι δραστηριότητες που εκτελούνται από τον αξιολογητή, προκειμένου να ανιχνεύσει τις ευπάθειες στον στόχο.

[74] layers - στρώματα, επίπεδα

- Διείσδυση (Penetration): Απόκτηση μη εξουσιοδοτημένης πρόσβασης θέτοντας τα μέτρα ασφάλειας σε ισχύ και προσπαθώντας να επιτευχθεί ένα - όσο το δυνατόν πιο αυξημένο - επίπεδο πρόσβασης.
- Απόκτηση πρόσβασης και Κλιμάκωση προνομίων (Gaining Access and Privilege Escalation): Μετά από την επιτυχή διείσδυση σε ένα σύστημα ή ένα δίκτυο-στόχο, ο αξιολογητής θα προσπαθήσει να αποκτήσει προνόμια υψηλότερου επιπέδου.
- Περαιτέρω απαρίθμηση (Enumerating Further): Απόκτηση πρόσθετων πληροφοριών σχετικά με τις διαδικασίες στο σύστημα, με στόχο την περαιτέρω εκμετάλλευση ενός παραβιασμένου δικτύου ή συστήματος.
- Παραβίαση απομακρυσμένων χρηστών ή ιστοσελίδων (Compromise Remote Users/Sites): Εκμετάλλευση των σχέσεων εμπιστοσύνης και της επικοινωνίας μεταξύ των απομακρυσμένων χρηστών και δικτύων επιχείρησης.
- Διατήρηση πρόσβασης (Maintaining Access): Χρησιμοποίηση κρυφών καναλιών, back doors[50] και rootkits[75] για να μη είναι ορατή η παρουσία του αξιολογητή στο σύστημα ή για να εξασφαλιστεί συνεχής πρόσβαση στο παραβιασμένο σύστημα.
- Κάλυψη των ιχνών (Covering Tracks): Εξάλειψη όλων των ιχνών της παραβίασης με την απόκρυψη αρχείων, τον καθαρισμό καταγραφών (logs), την παύση των ελέγχων ακεραιότητας και την αφαίρεση του αντιϊκού λογισμικού (antivirus).

Τα βήματα εκτέλεσης είναι κυκλικά και επαναληπτικά, έτσι ώστε να αντιπροσωπεύονται από τα κυκλικά βέλη στη φάση αξιολόγησης, όπως αυτά φαίνονται στο **Error! Reference source not found.**.

Τα επίπεδα ενός ελέγχου διείσδυσης μπορούν να εφαρμοστούν στους ακόλουθους στόχους: Δίκτυα, Ξενιστές, Εφαρμογές και Βάσεις Δεδομένων. Στη συνέχεια, θα αναφέρουμε ποιοι τύποι αξιολογήσεων πραγματοποιούνται σε κάθε κατηγορία, σύμφωνα με το ISSAF 0.2.

5.3.1.2.1 Ασφάλεια Δικτύων (Network Security)

Το ISSAF παρέχει αναλυτικές πληροφορίες για τους διάφορους τύπους αξιολόγησης της ασφάλειας δικτύων, με κυμαινόμενο βαθμό λεπτομέρειας. Οι πληροφορίες που παρέχονται περιλαμβάνουν βασικές πληροφορίες σχετικά με τα θέματα, τα παραδείγματα των τυποποιημένων διαμορφώσεων, μια λίστα εργαλείων επίθεσης που μπορεί να χρησιμοποιηθούν, καθώς και τα αναμενόμενα αποτελέσματα. Το ISSAF είναι πολύτιμο υπό την έννοια ότι παρέχει αρκετές πληροφορίες για ένα θέμα, έτσι κάποιος αρχάριος στην έννοια του ελέγχου διείσδυσης μπορεί να διαβάσει και να κατανοήσει τα βασικά. Στη συνέχεια αναφέρεται η λίστα των διαφορετικών θεμάτων, τα οποία περιλαμβάνει το ISSAF για την Ασφάλεια Δικτύων [OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B]:

[75] Τα rootkits είναι εργαλεία τα οποία ο επιτιθέμενος εγκαθιστά σε ένα σύστημα-θύμα και εκτελούν διάφορες λειτουργίες προς όφελός του. Ο επιτιθέμενος πρέπει προηγουμένως να έχει αποκτήσει πρόσβαση στο σύστημα-θύμα έτσι ώστε να μπορέσει να εγκαταστήσει ένα rootkit. Ένα rootkit είναι ένα σύνολο προγραμμάτων τα οποία επιτρέπουν στον επιτιθέμενο να συλλέγει κωδικούς από το θύμα, να βλέπει τα πακέτα που κινούνται από και προς το θύμα , να αφήσει ένα backdoor το οποίο θα του επιτρέπει μελλοντική πρόσβαση στο σύστημα-θύμα διατηρώντας έτσι τα δικαιώματα που είχε προηγουμένως αποκτήσει, να διατηρεί κρυφή την παρουσία του.

- Έλεγχος της Ασφάλειας Κωδικών Πρόσβασης (Password Security Testing)
- Αξιολόγηση της Ασφάλειας Μεταγωγέων (Switch Security Assessment)
- Αξιολόγηση της Ασφάλειας Δρομολογητών (Router Security Assessment)
- Αξιολόγηση της Ασφάλειας Τειχών Προστασίας (Firewall Security Assessment)
- Αξιολόγηση της Ασφάλειας Συστημάτων Ανίχνευσης Εισβολής (Intrusion Detection System Security Assessment)
- Αξιολόγηση της Ασφάλειας Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network Security Assessment)
- Στρατηγική Αξιολόγησης και Διαχείρισης της Ασφάλειας Αντιϊκών Συστημάτων (Antivirus System Security Assessment and Management Strategy)
- Ασφάλεια Δικτύων Περιοχών Αποθήκευσης (Storage Area Network (SAN) Security)
- Αξιολόγηση της Ασφάλειας Ασύρματων Δικτύων Τοπικής Περιοχής (Wireless Local Area Network Security Assessment)
- Ασφάλεια Χρηστών Διαδικτύου (Internet User Security)
- Ασφάλεια AS 400 (AS 400 Security)
- Ασφάλεια Lotus Notes (Lotus Notes Security)

Σε πολλές περιπτώσεις, δεν θα χρειαστεί να διαβάσει κάποιος ολόκληρο το ISSAF: θα ήταν πιο εύκολο να ασχοληθεί με εκείνα τα τμήματα που σχετίζονται με το τρέχον έργο (project) ελέγχου διείσδυσης (για παράδειγμα, ίσως να μη χρειαστεί να ασχοληθεί κάποιος με την Ασφάλεια Lotus Notes). Εντούτοις, το ISSAF είναι μια καλή αφετηρία για τον έλεγχο διείσδυσης.

5.3.1.2.2 Ασφάλεια Ξενιστών (Host Security)

Το ISSAF περιλαμβάνει, τα πιο ευρέως χρησιμοποιημένα λειτουργικά συστήματα, στη λίστα των πλατφόρμων της Ασφάλειας Ξενιστών. Και σε αυτήν την περίπτωση, το ISSAF παρέχει στους αναγνώστες του τις βασικές πληροφορίες σχετικά με κάθε πλατφόρμα, μια λίστα με τα αναμενόμενα αποτελέσματα, εργαλεία, καθώς και παραδείγματα σχετικά με το πώς μπορεί να μοιάζει ένας έλεγχος διείσδυσης (PenTest) σε ένα σύστημα. Οι ακόλουθες αξιολογήσεις συμπεριλαμβάνονται:

- Αξιολόγηση της Ασφάλειας Συστημάτων Unix/Linux (Unix/Linux System Security Assessment)
- Αξιολόγηση της Ασφάλειας Συστημάτων Windows (Windows System Security Assessment)
- Αξιολόγηση της Ασφάλειας Netware Novell (Novell Netware Security Assessment)
- Αξιολόγηση της Ασφάλειας Εξυπηρέτη Ιστού (Web Server Security Assessment)

Θα πρέπει να επισημανθεί για τους μηχανικούς (engineers) ότι το ISSAF, έκδοση 0.2.1B, γράφτηκε όταν τα συστήματα Windows NT ήταν το κυρίαρχο λειτουργικό σύστημα από τη Microsoft. Τα πράγματα από τότε όμως έχουν αλλάξει, έτσι δε θα πρέπει να περιμένει κανείς ότι τα παραδείγματα του ISSAF θα ισχύσουν σε όλες τις πλατφόρμες της Microsoft. Επιπλέον, εφιστάται η προσοχή στους διαχειριστές (managers), να διασφαλίσουν ότι η ομάδα του ελέγχου διείσδυσης

(PenTest) έχει εκπαιδευτεί στις πιο πρόσφατες εκδόσεις των λειτουργικών συστημάτων του στόχου, έτσι ώστε να είναι σε θέση να προσδιορίσει και να εκμεταλλευτεί κατάλληλα τις ευπάθειες. Η υποκείμενη αρχιτεκτονική των λειτουργικών συστημάτων έχει αλλάξει ριζικά κατά τη διάρκεια των ετών, συνεπώς δεν μπορεί να αναμένεται από ένα μηχανικό, ο οποίος είναι εξοικειωμένος με τα Windows NT, να είναι σε θέση να επιτεθεί σε συστήματα με λειτουργικό σύστημς Windows Server 2008 ή άλλα.

Το προηγούμενο σχόλιο σχετικά με το ότι ίσως να μη χρειάζεται να διαβαστούν όλα τα θέματα της Ασφάλειας Δικτύων (Network Security), δεν ευσταθεί στην συγκεκριμένη περίπτωση. Υπάρχουν τόσα πολλά διαφορετικά συστήματα, τα οποία «τρέχουν» τροποποιημένες εκδόσεις, των ξενιστών (hosts) που αναφέρθηκαν παραπάνω, όπου ένας επαγγελματίας μηχανικός ελέγχου διείσδυσης που διεξάγει αξιολογήσεις ξενιστών, θα πρέπει να έχει κατανοήσει και τα τέσσερα λειτουργικά συστήματα που μπορεί να εκτελούν οι ξενιστές. Υπάρχουν λειτουργικά συστήματα σε όλα τα είδη συσκευών δικτύου, πολλά εκ των οποίων μας εκπλήσσουν όταν ανακαλύπτουμε το τι «έτρεχαν». Οι εξυπηρέτες ιστού (web servers) περιλαμβάνονται επίσης σε έναν μεγάλο αριθμό συσκευών, συμπεριλαμβάνοντας δρομολογητές (routers), μεταγωγείς (switches), τείχη προστασίας (firewalls), καθώς και άλλα. Οι εξυπηρέτες ιστού δεν είναι πλέον μόνο για το Διαδίκτυο, αλλά χρησιμοποιούνται συχνά και ως ένα γραφικό περιβάλλον του χρήστη (GUI) για λόγους διαχείρισης.

5.3.1.2.3 Ασφάλεια Εφαρμογών (Application Security)

Η διαχωριστική γραμμή μεταξύ της εφαρμογής και της βάσης δεδομένων είναι μια γραμμή που δύσκολα ορίζεται. Αυτό συμβαίνει επειδή πολλές εφαρμογές απαιτούν πρόσβαση σε μια βάση δεδομένων, προκειμένου να λειτουργήσουν. Υπάρχουν απόψεις που υποστηρίζουν ότι το ISSAF δεν ορίζει και πολύ σωστά την συγκεκριμένη γραμμή και αυτό διότι περιλαμβάνει δραστηριότητες στην ασφάλεια εφαρμογών, οι οποίες είναι επιθέσεις των βάσεων δεδομένων (όπως οι επιθέσεις δομημένης γλώσσας επερωτήσεων (Structured Query Language-SQL) με σκοπό να λάβουν τον έλεγχο της βάσης δεδομένων). Οι αξιολογήσεις που περιλαμβάνονται στην ασφάλεια εφαρμογών σύμφωνα με το ISSAF είναι οι ακόλουθες [OISSG, 2006]:

- Αξιολόγηση της Ασφάλειας Εφαρμογών Ιστού (Web Application Security Assessment)
- Εγχύσεις SQL (SQL Injections)
- Έλεγχος Πηγαίου Κώδικα (Source Code Auditing)
- Δυαδικός Έλεγχος (Binary Auditing)

Η ασφάλεια εφαρμογών Ιστού είναι ένα μεγάλο θέμα. Όμως γενικά επικρατεί ότι οι ενέργειες που πραγματοποιούμε για τις επιθέσεις εφαρμογών Ιστού είναι πολύ παρόμοιες με τη μεθοδολογία που χρησιμοποιούμε για να επιτεθούμε σε όλες τις εφαρμογές. Συχνά, μόνο τα θέματα που έχουν σχέση με το χρόνο, είναι διαφορετικά στις εφαρμογές Ιστού και αυτό συμβαίνει όταν εμπλέκεται μια βάση δεδομένων.

5.3.1.2.4 Ασφάλεια Βάσεων Δεδομένων (Database Security)

Το ISSAF παρέχει στον αξιολογητή τέσσερα διαφορετικά επίπεδα αξιολόγησης, τα οποία είτε μπορούν να συμπεριλάβουν, είτε όχι, τις εφαρμογές και υπηρεσίες Ιστού [OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B]:

- Απομακρυσμένη απαρίθμηση των βάσεων δεδομένων (Remote Enumeration of Databases)
- Επίθεση «ωμής βίας» - εξαντλητική αναζήτηση βάσεων δεδομένων (Brute-forcing databases)
- Επίθεση χειραγώγησης διεργασιών[76] (Process manipulation attack)
- Διεξοδική επιθεώρηση των βάσεων δεδομένων (End-to-end audit of databases)

5.3.1.2.5 Κοινωνική Μηχανική (Social Engineering)

Το τμήμα της κοινωνικής μηχανικής του ISSAF ασχολείται με πολλές από τις παλαιότερες και γνωστές τεχνικές κοινωνικής μηχανικής, που χρησιμοποιούνται για να αποκτηθούν πληροφορίες από τους χρήστες των συστημάτων. Το αξιοπερίεργο είναι ότι όλες αυτές οι παλαιότερες τεχνικές είναι ακόμα αρκετά αποτελεσματικές. Εντούτοις, από το τμήμα αυτό απουσιάζουν και μερικές από τις πιο δημοφιλής τεχνικές που χρησιμοποιούνται σήμερα, συμπεριλαμβάνοντας το phishing[77] (και όλα του υποσύνολά του), καθώς και τις επιθέσεις Cross Site Scripting. Αυτό αποτελεί ένας επιπλέον λόγος για τον οποίο το ISSAF είναι καλό να χρησιμοποιηθεί ως αφετηρία για μια ομάδα ελέγχου διείσδυσης (PenTest) ώστε να κατανοήσει τις πιθανές απειλές, αλλά όχι ως ολόκληρο πλαίσιο για το πρόγραμμα (project) ελέγχου διείσδυσης.

5.3.1.3 Φάση - III: Υποβολή έκθεσης, Καθαρισμός και Καταστροφή (Reporting, Clean-up and Destroy)

Η τελευταία φάση στο ISSAF 0.2 ασχολείται με την παροχή των απαραίτητων εκθέσεων στους κατάλληλους ενδιαφερόμενους και την εξασφάλιση οποιωνδήποτε δεδομένων που παρήχθησαν κατά τη διάρκεια του ελέγχου διείσδυσης. Το ISSAF δεν προχωρά σε πάρα πολλή λεπτομέρεια για το πώς να εκτελεστούν οι στόχοι σε αυτήν την φάση, αλλά περιέχει κάποιες γενικές έννοιες.

- Υποβολή έκθεσης

Υπάρχουν δύο τύποι έκθεσης που μπορεί να εμφανιστούν σε έναν επαγγελματικό έλεγχο διείσδυσης, η προφορική και η γραπτή. Σύμφωνα με το ISSAF, οι προφορικές εκθέσεις χρησιμοποιούνται για εκείνα τα στιγμιότυπα όπου ανακαλύπτονται κρίσιμα ζητήματα και πρέπει να αναφερθούν σχεδόν αμέσως. Μπορεί να είναι θετικό να συμπεριλαμβάνεται στην τελική έκθεση και η αναφορά σε οποιαδήποτε συμπεράσματα που ειπώθηκαν προφορικώς, ακόμα κι αν το ISSAF δεν αναφέρει κάτι τέτοιο. Η προφορική αναφορά καταγράφεται επισήμως, ακόμα κι αν το κρίσιμο ζήτημα αποκατασταθεί πριν διανεμηθεί η τελική έκθεση στους ενδιαφερόμενους.

---

[76] Η επίθεση χειραγώγησης διεργασιών είναι μία μορφή επίθεσης όπου εκτελούμενες διεργασίες καθοδηγούνται ώστε είτε να εκτελέσουν ενέργειες που υποβαθμίζουν την ασφάλεια είτε να αποκαλύψουν πληροφορίες που μπορούν στη συνέχεια να αξιοποιηθούν στα πλαίσια επιθέσεων.

[77] Το phishing, όπως υπονοεί η λέξη (ψάρεμα), περιγράφεται ως μια προσπάθεια απόσπασης ή υποκλοπής προσωπικών στοιχείων αξιοποιήσιμων για μη εξουσιοδοτημένες ή παράνομες οικονομικές συναλλαγές. Το ιδιότυπο αυτό «ψάρεμα», το οποίο πρωτοεμφανίστηκε πριν από λίγα χρόνια, επιχειρείται όλο και συχνότερα με τη χρήση συνδυασμού spam mail και «πλαστών» ιστοσελίδων, που μιμούνται όσο πειστικότερα μπορούν τα αντίστοιχα των νόμιμων επιχειρήσεων ή χρηματοπιστωτικών οργανισμών.

Θα πρέπει να επισημανθεί ότι οποιεσδήποτε προφορικές εκθέσεις σχετικά με κρίσιμα ζητήματα ή ανακαλύψεις νομικής φύσεως, θα πρέπει να αντιμετωπιστούν προσεκτικά. Εάν ένας νόμος έχει παραβιαστεί, οι αρμόδιες αρχές θα πρέπει να ενημερωθούν και οι ενδιαφερόμενοι θα πρέπει να αποκλειστούν από οποιοδήποτε είδος προφορικών εκθέσεων. Πριν αρχίσει ένας έλεγχος διείσδυσης, οι νομικοί και οι αρχές επιβολής του νόμου θα πρέπει να προσδιοριστούν και να ενημερωθούν, όπου απαιτείται.

Εντός της τελικής γραπτής έκθεση, το ISSAF απαιτεί να περιλαμβάνονται τα εξής [OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B]:

- Περίληψη διαχείρισης(Management summary)
- Εμβέλεια έργου (Project scope)
- Εργαλεία ελέγχου διείσδυσης που χρησιμοποιήθηκαν (Penetration test tools used)
- Εκμεταλλεύσεις που χρησιμοποιήθηκαν (Exploits used)
- Ημερομηνία και χρόνος των ελέγχων (Date and time of the tests)
- Όλα τα αποτελέσματα των εργαλείων και των εκμεταλλεύσεων (All outputs of the tools and exploits)
- Μια λίστα των προσδιορισμένων ευπαθειών (A list of identified vulnerabilities)
- Συστάσεις για το μετριασμό των προσδιορισμένων ευπαθειών, που οργανώνονται με προτεραιότητα (Recommendations to mitigate identified vulnerabilities, organized into priorities)

Αυτές οι απαιτήσεις υποτίθεται ότι πρέπει να βρίσκονται στο σώμα του τελικού εγγράφου και μην περιλαμβάνονται σε συνημμένα. Γενικώς θεωρείται ότι κάτι τέτοιο μπορεί να παράγει ένα έγγραφο που είναι δύσκολο να διαβαστεί.

- Καθαρισμός και Καταστροφή Αντικειμένων

Όλες οι πληροφορίες που δημιουργούνται ή/ και αποθηκεύονται στα συστήματα που ελέγχονται, θα πρέπει να διαγραφούν από αυτά. Εάν για κάποιους λόγους, δεν είναι εφικτό κάτι τέτοιο από ένα απομακρυσμένο σύστημα, όλα αυτά τα αρχεία (με τη θέση τους) θα πρέπει να αναφερθούν στην τεχνική έκθεση, έτσι ώστε το τεχνικό προσωπικό του πελάτη να είναι σε θέση να τα αφαιρέσει αφού έχει πλέον ληφθεί η έκθεση.

Το ISSAF δεν αναφέρει αυτό το βήμα εντός της φάσης ΙΙΙ ενός ελέγχου διείσδυσης με μεγάλη λεπτομέρεια. Είναι πιθανό ότι σε μελλοντικές εκδόσεις του ISSAF, ίσως θα παρέχεται περισσότερη λεπτομέρεια σχετικά με το πώς να γίνει η κρυπτογράφηση, ο καθαρισμός και η καταστροφή των δεδομένων που δημιουργούνται κατά τη διάρκεια ενός ελέγχου διείσδυσης και τα οποία διατηρούνται στη συνέχεια.

5.4 Εργαλεία για την υποστήριξη της μεθοδολογίας

Στον παρακάτω πίνακα παρουσιάζονται μερικά παραδείγματα εργαλείων που χρησιμοποιούνται για κάθε επίπεδο (layer) της Φάσης - ΙΙ: Αξιολόγηση.

Επίπεδα	Παράδειγμα εργαλείων	
Συλλογή Πληροφοριών (Information Gathering)	παλαιά εργαλεία (old):	Google[1], whois, zone-transfers, reverse DNS lookups
	εξαιρετικά εργαλεία (shiny):	Maltego, Metagoofil, CentralOps.net, DigitalPoint.com, DomainTools.com
Χαρτογράφηση Δικτύων (Network Mapping)	βασικά εργαλεία (basic):	nmap, Hping3, p0f, Xprobe2, amap
	εξαιρετικά εργαλεία (shiny):	trigger SMTP bounces, Brute force HTTP vhosts, watch outbound DNS, just email the users
Προσδιορισμός Ευπαθειών (Vulnerability Identification)	βασικά εργαλεία (basic):	Nessus[2], commercial tools
	εργαλεία Ιστού (web):	hackvertor, Nikto, WFuzz, w3af, HttpRecon, WebScarab[3.2.4.1.4]
Διείσδυση (Penetration)	βασικά εργαλεία (basic):	milw0rm, bugtraq, exploit databases
	εξαιρετικά εργαλεία (shiny):	Metasploit[10], FastTrack, Inguma, Karma, wesside-ng
Κλιμάκωση προνομίων (Privilege Escalation)	βασικά εργαλεία (basic):	john, Hydra, Medusa, Ettercap, tcpdump[4]
	καλά εργαλεία (nice):	Scapy/Scruby, FPGAs (WPA2), Rainbowcrack, NTLM relays, social engineering, dhcpcd -h WPAD -i eth0
Διατήρηση πρόσβασης (Maintaining Access)	βασικά εργαλεία (basic):	VNC, BO2k, hxdef, Adore-ng, netcat cronjob
	εργαλεία διόδου (tunneling):	CryptCat, nstx, socat, vstt, ht[sc], icmptx

Πίνακας 20. Παραδείγματα εργαλείων για κάθε επίπεδο (layer) της φάσης ΙΙ.

5.5 Συμπέρασμα

Η Ομάδα Ασφάλειας Ανοικτών Συστημάτων Πληροφοριών (Open Information Systems Security Group-OISSG) δημιουργήθηκε με στόχο την εξέλιξη ενός συνόλου προτύπων ανοικτού κώδικα, οδηγιών και μιας συλλογής βέλτιστων πρακτικών στον τομέα της ασφάλειας πληροφοριών. Το ISSAF 0.2 επιδιώκει να ενσωματώσει τα ακόλουθα εργαλεία διαχείρισης και τις λίστες ελέγχου (checklists) εσωτερικού ελέγχου:

- Αξιολόγηση των πολιτικών και των διαδικασιών ασφάλειας πληροφοριών των οργανισμών, προκειμένου να υποβληθεί μια έκθεση σχετικά με τη συμμόρφωσή τους με τα πρότυπα βιομηχανίας τεχνολογίας πληροφορικής και τις απαιτήσεις των νόμων.
- Προσδιορισμός και αξιολόγηση των εξαρτήσεων της επιχείρησης σε υπηρεσίες υποδομής που παρέχονται από την τεχνολογία πληροφορικής.
- Διεξαγωγή αξιολογήσεων ευπάθειας και ελέγχων διείσδυσης, προκειμένου να δοθεί έμφαση στις ευπάθειες του συστήματος που θα μπορούσαν να οδηγήσουν σε πιθανούς κινδύνους για τα αγαθά πληροφοριών.
- Καθορισμός προτύπων αξιολόγησης από περιοχές ασφάλειας ώστε:
  - Να εντοπίσουν λανθασμένες ρυθμίσεις (misconfigurations) και να τις αποκαταστήσουν.
  - Να προσδιορίσουν τους κινδύνους που σχετίζονται με τις τεχνολογίες και να τους αντιμετωπίσουν.
  - Να προσδιορίσουν τους κινδύνους εντός των διαδικασιών της επιχείρησης και να τους αντιμετωπίσουν.
  - Να ενισχύσουν τις υπάρχουσες διαδικασίες και τεχνολογίες.

- Να παρέχουν βέλτιστες πρακτικές και διαδικασίες για να υποστηρίξουν τις πρωτοβουλίες της επιχειρησιακής συνέχειας.

Με την υποστήριξη της OISSG, το ISSAF αποτελεί μια αξιολογημένη από ομοτίμους διαδικασία που παρέχει πληροφορίες σχετικά με το πώς να διεξαχθεί ένας έλεγχος διείσδυσης. Ένα από τα πλεονεκτήματα του ISSAF 0.2 είναι ότι δημιουργεί μια ευδιάκριτη σύνδεση μεταξύ των στόχων ενός ελέγχου διείσδυσης και των εργαλείων αυτού του ελέγχου (PenTest).

Κεφάλαιο 6: Συμπεράσματα

Η ασφάλεια είναι ένα σημαντικό χαρακτηριστικό του λογισμικού εφαρμογών. Δεν είναι μια απλή και εύκολη διαδικασία και επιπλέον, απαιτεί οι ελεγκτές που διεξάγουν τους ελέγχους ασφάλειας να έχουν το κατάλληλο γνωστικό υπόβαθρο καθώς και να ενημερώνονται συχνά. Μια σημαντική πτυχή της διασφάλισης της ασφάλειας λογισμικού είναι η αξιολόγησή της, ώστε να αναδειχθούν αδυναμίες και να ληφθούν τα σχετικά διορθωτικά μέτρα. Η αξιολόγηση των ελέγχων ασφάλειας περιλαμβάνει περισσότερα από την απλή ανίχνευση ενός τείχους ασφάλειας (firewall) για να ανακαλυφθεί ποιες θύρες είναι ανοικτές και έπειτα, την παραγωγή μιας αντίστοιχης έκθεσης.

Ο έλεγχος ασφάλειας είναι μια σημαντική διαδικασία και σε αυτήν τη διαδικασία καθοριστικό ρόλο έχει η συλλογή εκείνων των στοιχείων που είναι χρήσιμα για τον έλεγχο. Πιο συγκεκριμένα, η αξιολόγηση ελέγχων ασφάλειας είναι ζωτικής σημασίας για να καθοριστεί εάν μια επιχείρηση συμμορφώνεται ή όχι με τις πολιτικές, τις διαδικασίες και τα πρότυπά της. Μέσω των αξιολόγησης των ελέγχων ασφάλειας, μπορούμε να επιβεβαιώσουμε εάν ο οργανισμός επιτυγχάνει τους στόχους του σχετικά με τη μείωση του κινδύνου και την αποφυγή της πρόσβασης κακόβουλων επιτιθέμενων στο δίκτυο και στα συστήματά του. Οι ελεγκτές θα πρέπει να έχουν μια βάση γνώσεων σχετικά με τις μεθοδολογίες και τα εργαλεία ελέγχου ασφάλειας. Η χρησιμοποίηση μεθοδολογιών - πλαισίων ελέγχου είναι ένας χρήσιμος τρόπος ώστε να αναπτυχθεί ένας καλός σχεδιασμός τεχνικού ελέγχου.

Υπάρχουν πολλές μεθοδολογίες ελέγχου ασφάλειας ανοικτού κώδικα που χρησιμοποιούνται σήμερα από τους ελεγκτές ασφάλειας για την τεχνική αξιολόγηση του ελέγχου. Οι τέσσερις πιο δημοφιλείς, με τις οποίες ασχοληθήκαμε και στην παρούσα μεταπτυχιακή εργασία είναι οι εξής:

- Εγχειρίδιο Μεθοδολογίας Ελέγχου Ασφάλειας Ανοικτού κώδικα - Open Source Security Testing Methodology Manual (OSSTMM).
- Έργο Ασφάλειας Εφαρμογών Ιστού Ανοικτού κώδικα - Open Web Application Security Project (OWASP).
- Τεχνικός Οδηγός για τον Έλεγχο και την Αξιολόγηση της Ασφάλειας Πληροφοριών (Technical Guide to Information Security Testing and Assessment) NIST 800-115.
- Πλαίσιο Αξιολόγησης της Ασφάλειας Συστημάτων Πληροφοριών - Information Systems Security Assessment Framework (ISSAF).

Όλες αυτές οι μεθοδολογίες - πλαίσια παρέχουν ένα λεπτομερή, διαδικαστικό τρόπο με τον οποίο διεξάγεται ένας έλεγχος ασφάλειας και κάθε μια έχει τα θετικά σημεία της αλλά και τις αδυναμίες της. Οι περισσότεροι ελεγκτές διείσδυσης χρησιμοποιούν αυτές τις μεθοδολογίες ως αφετηρία για να διεξάγουν τη διαδικασία ελέγχου τους και κατά τη διάρκεια της διαδικασίας, αποκομίζουν σημαντικά οφέλη όταν παραπέμπουν σε αυτές.

6.1 OSSTMM

Το OSSTMM αναπτύχθηκε υπό την άδεια της Creative Commons License ως μια μεθοδολογία ανοικτού κώδικα για τη διεξαγωγή ελέγχων ασφάλειας κατά λεπτομερή και επαναλαμβανόμενο τρόπο. Είναι ένας οδηγός που αξιολογεί πόσο ασφαλή είναι τα συστήματα. Περιέχει διεξοδικές οδηγίες για το πώς να ελέγξουμε τα

συστήματα με μεθοδολογικό τρόπο, καθώς και πώς να αξιολογήσουμε και να υποβάλουμε εκθέσεις σχετικά με τα αποτελέσματα.

Το OSSTMM δεν είναι απλά μια προσέγγιση ελέγχου διείσδυσης (penetration testing) αλλά αποτελεί ένα μεθοδολογικό πλαίσιο. Η μεθοδολογία βοηθά στην καθοδήγηση του σχεδιασμού του ελέγχου ασφάλειας, στην κατάλληλη ποσοτικοποίηση των αποτελεσμάτων και επιπλέον, παρέχει τους κανόνες δέσμευσης (rules of engagement) για εκείνους που εκτελούν τον έλεγχο. Στηρίζεται σε βέλτιστες πρακτικές και μια βάση δεδομένων απειλών, καθώς επίσης και στη γνώση του οργανισμού-στόχου ώστε να παρέχει μια ευρεία ανασκόπηση των κινδύνων που τίθενται στην υποδομή της επιχείρησης. Τα περισσότερα πλαίσια ελέγχου, όπως ISO 27001, OCTAVE, COBIT και ISM3, υιοθετούν μια οργανωτική προσέγγιση στην αξιολόγηση και εκτίμηση. Το OSSTMM αναφέρεται στη λειτουργική πτυχή του επιχειρηματικού κινδύνου.

Ένα όφελος του OSSTMM έναντι άλλων μεθοδολογιών είναι ότι εστιάζει στις τεχνικές λεπτομέρειες σχετικά με το ποια αντικείμενα πρέπει να ελεγχθούν, τι να γίνει πριν τον έλεγχο, κατά τη διάρκεια του ελέγχου, μετά τον έλεγχο και πώς να μετρηθούν τα αποτελέσματα. Αυτή η προσέγγιση εξασφαλίζει ότι η συνολική κάλυψη ελέγχου επιτυγχάνεται κατά τη διάρκεια μιας αξιολόγησης της ασφάλειας.

Η τρέχουσα έκδοση 2.2 του εγχειριδίου δίνει έμφαση στον έλεγχο ασφάλειας διαιρώντας τις περιοχές αξιολόγησης σε έξι διασυνδεμένα τμήματα, με τις αντίστοιχες ενότητες:

- Ασφάλεια Πληροφοριών - Information Security: Έρευνα συλλογής πληροφοριών, συλλογή και ανάλυση εγγράφων Διαδικτύου, επισκόπηση ελέγχων ιδιωτικότητας, κ.ά.
- Ασφάλεια Διαδικασιών - Process Security: Διαδικασίες παραχώρησης πρόσβασης, έλεγχος κοινωνικής μηχανικής, κ.ά.
- Ασφάλεια Τεχνολογίας Διαδικτύου - Internet Technology Security: Έρευνα δικτύων, ανίχνευση θυρών, προσδιορισμός υπηρεσιών και λειτουργικού συστήματος, ανίχνευση ευπαθειών, έλεγχος εφαρμογών Διαδικτύου, έλεγχος δρομολογητή/ τείχους προστασίας (router/firewall), έλεγχος ανίχνευσης εισβολής (IDS), ανίχνευση κακόβουλου κώδικα, παραβίαση κωδικού πρόσβασης, έλεγχος άρνησης υπηρεσιών, επισκόπηση πολιτικής, κ.ά.
- Ασφάλεια Επικοινωνιών - Communications Security: Έλεγχος ιδιωτικού τηλεφωνικού κέντρου (PBX), φωνητικού ταχυδρομείου (voicemail), fax, διαποδιαμορφωτή (modem), φωνής μέσω πρωτοκόλλου IP (Voice over IP), κ.α.
- Ασφάλεια Ασύρματων επικοινωνιών - Wireless Security: Έλεγχος δικτύων 802.11, bluetooth, ηλεκτρομαγνητικής ακτινοβολίας (EMR), ανίχνευσης φορητών, συσκευών επιτήρησης, προσδιορισμού ραδιοσυχνότητας (RFID), υπερύθρων, κ.α.
- Φυσική Ασφάλεια - Physical Security: Έλεγχος πρόσβασης και επισκόπηση περιμέτρου, ελέγχου, απόκρισης προειδοποιήσεων, περιβάλλοντος, κ.α.

Το εγχειρίδιο του OSSTMM παρέχει ένα ευρύ φάσμα από πρότυπα έγγραφα για τη διεξαγωγή των ελέγχων που περιλαμβάνονται σε κάθε μια από τις έξι ενότητες. Αυτό το σύνολο των προτύπων δεν απαιτεί την ανάγκη υποστήριξης από λογισμικό. Εντούτοις, μπορεί να χρειαστεί η κατάρτιση από την ISECOM για την καλύτερη χρήση των προτύπων και ενοτήτων.

Το μεγάλο πλεονέκτημα της μεθοδολογίας OSSTMM είναι το spreadsheet (υπολογισμός με λογιστικό φύλλο) με τις Τιμές Αξιολόγησης Κινδύνου (Risk Assessment Values - RAVs) που παρέχεται. Το spreadsheet διαιρείται σε έξι λειτουργικές περιοχές και χαρακτηρίζει τον κίνδυνο σε κάθε μια από αυτές τις περιοχές με μια αριθμητική τιμή. Όλες αυτές οι τιμές κινδύνου αθροίζονται για να παρέχουν ένα γενικό προφίλ κινδύνου για τον οργανισμό. Κατά συνέπεια το OSSTMM παρέχει μια εύχρηστη, συνεπή και αξιόπιστη διαδικασία που μας οδηγεί σε σημαντικά αποτελέσματα, τα οποία μπορούν να συγκριθούν κατά τη διάρκεια του χρόνου.

Πιο συγκεκριμένα, το OSSTMM χρησιμοποιεί τρεις πτυχές μέσα σε ένα σύστημα για να εξακριβώσει το γενικό κίνδυνο στην ασφάλεια πληροφοριών:

- Λειτουργίες (Operations): Διαφάνεια (visibility), Εμπιστοσύνη (trust), Πρόσβαση (access).
- Έλεγχοι (Controls):
  - Κατηγορία Α: Αυθεντικοποίηση (Authentication), Αποζημίωση (Indemnification), Υποταγή (Subjugation), Συνέχεια (Continuity), Ανθεκτικότητα (Resilience).
  - Κατηγορία Β: Μη αποποίηση ευθύνης (Non-repudiation), Εμπιστευτικότητα (Confidentiality), Ιδιωτικότητα (Privacy), Ακεραιότητα (Integrity), Προειδοποίηση (Alarm).
- Περιορισμοί (Limitations): Ευπάθεια (Vulnerability), Αδυναμία (Weakness), Ανησυχία (Concern), Έκθεση (Exposure), Ανωμαλία (Anomaly).

Κάθε πτυχή είναι καθορισμένη χρησιμοποιώντας διαφορετικές εισόδους (inputs), κατάλληλες για την πτυχή. Σε κάθε τμήμα πτυχής ορίζεται μια τιμή που υπολογίζεται με βάση διάφορα κριτήρια, που καθορίζονται από το OSSTMM, όπως ο αριθμός των στόχων, η ποσότητα μεθόδων αυθεντικοποίησης στο κάθε σύστημα και ο αριθμός ευπαθειών. Πρόσθετοι μαθηματικοί τύποι χρησιμοποιούνται για να λάβουμε τελικά τη μετρική κινδύνου για το σύστημα-στόχο ή δίκτυο-στόχο, η οποία απεικονίζει το γενικό κίνδυνο ασφάλειας της επιχείρησης.

Το πλεονέκτημα της χρησιμοποίησης της μεθοδολογίας OSSTMM για την απόκτηση μετρικών κινδύνου είναι το γεγονός ότι όλες οι πτυχές της ασφάλειας ενός συστήματος απεικονίζονται στην τιμή κινδύνου. Το μειονέκτημα της χρησιμοποίησης της μεθοδολογίας OSSTMM είναι η μαθηματική πολυπλοκότητα που είναι δύσκολο να εξηγηθεί στους ενδιαφερόμενους, οι οποίοι συχνά πρέπει να κατανοήσουν τον υποκείμενο αλγόριθμο που χρησιμοποιείται για να προσδιορίσει τον κίνδυνο. Η πρόσθετη πολυπλοκότητα μπορεί να είναι εξίσου καταστρεπτική με την ελάχιστη πολυπλοκότητα, κατά την παρουσίαση του κινδύνου στους πελάτες.

Το OSSTMM παρέχει επίσης και ένα σύνολο εργαλείων ασφάλειας, τα οποία έχει αναπτύξει. Για τους ελέγχους στις ενότητες του OSSTMM, εκτός από αυτά τα εργαλεία μπορούν να χρησιμοποιηθούν και πολλά άλλα εργαλεία ανοικτού κώδικα, τα οποία είναι διαθέσιμα.

Το OSSTMM είναι ένα σημαντικό εφόδιο για τους διαχειριστές συστημάτων που θέλουν να αξιολογήσουν την ασφάλεια ενός ευρέως φάσματος συστημάτων με έναν καθορισμένο και λεπτομερή τρόπο. Περιέχει τις οδηγίες για τον έλεγχο των συστημάτων αλλά ελάχιστες λεπτομέρειες για τον τρόπο προστασίας των συστημάτων.

Ένα άλλο σημαντικό όφελος του OSSTMM είναι ότι είναι υπό συνεχή ομότιμη-επισκόπηση (peer-review). Η αξιολόγηση από ομοτίμους αποτρέπει το OSSTMM από το να γίνει πεπαλαιωμένο όπως πολλές άλλες μεθοδολογίες, αλλά επίσης εξασφαλίζει ότι το OSSTMM παραμένει σύγχρονο σύμφωνα με τις διεθνείς βέλτιστες πρακτικές, τους νόμους και τους κανονισμούς. Η ομότιμη-επισκόπηση είναι ένα σημαντικό πλεονέκτημα που έχει το OSSTMM σε σχέση με τις περισσότερες, εάν όχι όλες τις άλλες μεθοδολογίες ελέγχου ασφάλειας.

Συνοψίζοντας, το OSSTMM έχει μια ισχυρή συνέχεια στην κοινότητα και παρέχει μια καλή αναφορά για το ποιες περιοχές πρέπει να εξετασθούν και ποιοι τύποι αποτελεσμάτων να αναμένονται. Δεν αποτελεί ένα έγγραφο του τύπου «κάνε κλικ εδώ και έπειτα κάνε αυτό», αλλά απαιτεί ένα υπόβαθρο γνώσεων των διάφορων εργαλείων και τεχνικών για να εκπληρωθούν οι στόχοι των ελέγχων.

6.2 OWASP

Ο οδηγός ελέγχου του OWASP δημιουργήθηκε για να βοηθήσει τους υπεύθυνους ανάπτυξης Ιστού και τους επαγγελματίες ασφάλειας ώστε να εξασφαλίσουν καλύτερα τις εφαρμογές Ιστού. Η ανάπτυξη κακώς σχεδιασμένων και υλοποιημένων εφαρμογών Ιστού έχει οδηγήσει σε πολυάριθμες και εύκολα εκμεταλλεύσιμες ευπάθειες που καθιστούν την κοινότητα του Διαδικτύου ευάλωτη σε κίνδυνους από επιθέσεις κακόβουλου λογισμικού (malware), υποκλοπής ταυτότητας και άλλες. Ως μη κερδοσκοπικός οργανισμός, το OWASP έχει αναπτύξει διάφορα εργαλεία, οδηγούς και μεθοδολογίες ελέγχου που είναι ελεύθεροι προς χρήση για οποιονδήποτε.

Το Έργο Ασφάλειας Εφαρμογών Ιστού Ανοικτού κώδικα (Open Web Application Security Project-OWASP) διατηρείται και αναπτύσσεται από την κοινότητα του OWASP. Το OWASP είναι μια συλλογή πληροφοριών, προγραμμάτων και προτύπων που έχουν σχέση με την ασφάλεια εφαρμογών. Το πλεονέκτημα του OWASP έγκειται στη διεθνώς ευρεία αποδοχή του και στην ευρεία συλλογή συγκεκριμένων πληροφοριών που απεικονίζεται στον Οδηγό Ελέγχου του OWASP (OWASP Testing Guide) και στην OWASP Top Ten λίστα με τις ατέλειες της ασφάλειας των εφαρμογών Ιστού.

Η OWASP Top Ten είναι μια ενημερωμένη λίστα των 10 πιο κρίσιμων και συνηθισμένων διανυσμάτων επίθεσης στις εφαρμογές Ιστού που απαιτούν άμεση αντιμετώπιση. Ο αρχικός στόχος του OWASP Top 10 είναι να εκπαιδευτούν οι υπεύθυνοι ανάπτυξης και οι οργανισμοί, σχετικά με τις συνέπειες των σημαντικότερων αδυναμιών ασφάλειας των εφαρμογών ιστού. Παρέχει τις βασικές τεχνικές που προστατεύουν από αυτές τις προβληματικές περιοχές υψηλού κινδύνου, καθώς επίσης και τις οδηγίες για το τι θα πρέπει να γίνει στη συνέχεια.

Ο Οδηγός Ελέγχου του OWASP (OWASP Testing Guide) αποτελεί ένα πρότυπο για τον έλεγχο εφαρμογών Ιστού. Η έκδοση 3 κυκλοφόρησε το Δεκέμβριο του 2008 και έχει συντελέσει στην αύξηση της συνειδητοποίησης των ζητημάτων ασφάλειας στις εφαρμογές Ιστού μέσω πρακτικών ελέγχου και βέλτιστης κωδικοποίησης.

Αυτός ο οδηγός μπορεί να χρησιμοποιηθεί ως αναφορά και ως μεθοδολογία για να βοηθήσει ώστε να καθοριστεί το χάσμα μεταξύ των τρεχουσών πρακτικών μας και των βέλτιστων πρακτικών της βιομηχανίας. Επιτρέπει στους οργανισμούς να συγκριθούν με άλλους, να κατανοήσουν το μέγεθος των πόρων που απαιτούνται για

να ελέγξουν και να διατηρήσουν το λογισμικό τους, ή να προετοιμαστούν για έναν έλεγχο ασφάλειας. Ο συγκεκριμένος οδηγός, βοηθά τους ελεγκτές να κατανοήσουν το τι, γιατί, πότε, που και πως να εκτελούν έλεγχο στις εφαρμογές ιστού (web) και δεν παρέχει μόνο μια απλή λίστα ελέγχου (checklist) ή μια λίστα θεμάτων που πρέπει να εξεταστούν.

Στη μεθοδολογία ελέγχου του OWASP, το σύνολο των ενεργών ελέγχων έχει χωριστεί στις 10 ακόλουθες υποκατηγορίες, οι οποίες καλύπτουν συνολικά 66 ελέγχους:

- Συλλογή Πληροφοριών (Information Gathering)
- Έλεγχος Διαχείρισης Διαμόρφωσης (Configuration Management Testing)
- Έλεγχος Επιχειρησιακής Λογικής (Business Logic Testing)
- Έλεγχος Αυθεντικοποίησης (Authentication Testing)
- Έλεγχος Εξουσιοδότησης (Authorization testing)
- Έλεγχος Διαχείρισης Συνόδου (Session Management Testing)
- Έλεγχος Επικύρωσης Δεδομένων (Data Validation Testing)
- Έλεγχος Άρνησης Παροχής Υπηρεσιών (Denial of Service Testing)
- Έλεγχος Υπηρεσιών Ιστού (Web Services Testing)
- Έλεγχος Ajax (Ajax Testing)

Κάθε έλεγχος παρέχει μια περιγραφή των ζητημάτων, διάφορα εργαλεία που μπορούν να χρησιμοποιηθούν για να αξιολογήσουν την υπηρεσία, καθώς και παραδείγματα των αναμενόμενων αποτελεσμάτων. Οι πληροφορίες και τα παραδείγματα που δίνονται είναι λεπτομερείς και επιπλέον, στο τέλος κάθε μεμονωμένου ελέγχου συμπεριλαμβάνονται αναφορές για τα εργαλεία που χρησιμοποιήθηκαν ή τα ζητήματα που συζητήθηκαν.

Το OWASP έχει αναπτύξει ένα σύνολο από σημαντικά εργαλεία που χρησιμοποιούνται για να ανακαλύπτουν ατέλειες, στην υλοποίηση και στο σχεδιασμό, σχετικές με την ασφάλεια (WebScarab, WSFuzzer, DirBuster, JbroFuzz, κ.ά.). Στους διάφορους ελέγχους του OWASP Testing Guide, εκτός από αυτά τα εργαλεία του OWASP, χρησιμοποιούνται και άλλα κατάλληλα εργαλεία ανοικτού κώδικα που είναι ελεύθερα διαθέσιμα. Παρατηρήθηκε ότι σε αρκετούς ελέγχους ένα εργαλείο που φάνηκε επαρκές για τους συγκεκριμένους ελέγχους είναι το OWASP WebScarab. Το WebScarab έχει ως σκοπό να αποκαλύψει τον τρόπο λειτουργίας μιας εφαρμογής HTTP(S), να επιτρέψει στον υπεύθυνο ανάπτυξης να διορθώσει τα δύσκολα προβλήματα, ή να επιτρέψει σε έναν ειδικό ασφάλειας να προσδιορίσει τις ευπάθειες μιας εφαρμογής. Παρέχει καλή τεκμηρίωση, βασικές οδηγίες και λειτουργεί με τη χρήση διαφόρων plugins, τα οποία παρέχουν συγκεκριμένες συνήθως λειτουργίες. Το μειονέκτημά του, θα μπορούσε να είναι ότι σχεδιάστηκε με σκοπό να χρησιμοποιηθεί από εκείνους που μπορούν να γράψουν κώδικα ή έχουν μια αρκετά καλή κατανόηση του πρωτοκόλλου HTTP.

Το OWASP επίσης έχει δημοσιεύσει το πρότυπο ASVS. Το Πρότυπο Επαλήθευσης της Ασφάλειας Εφαρμογών του OWASP (OWASP Application Security Verification Standard-ASVS) είναι ένα πρότυπο ανοικτού κώδικα που ορίζει την εμβέλεια της κάλυψης και τα επίπεδα αυστηρότητας, τα οποία μπορούν να χρησιμοποιηθούν για να εκτελέσουμε επαληθεύσεις στην ασφάλεια εφαρμογών.

Δημιουργήθηκε για να καθορίσει μια τυποποιημένη ορολογία στη βιομηχανία που θα μετρά το επίπεδο ασφάλειας για τις εφαρμογές ή τα προϊόντα. Όταν όλοι συγχρονιστούν με τη συγκεκριμένη ορολογία, οι οργανισμοί θα μπορούν να

αγοράζουν λογισμικό και να γνωρίζουν ότι είναι συμβατό με ένα συγκεκριμένο προκαθορισμένο επίπεδο ασφάλειας και θα μπορεί να είναι βέβαιο ότι είναι συμβατό με αυτό το επίπεδο επειδή ελέγχθηκε σύμφωνα με τις κοινές ή τυποποιημένες απαιτήσεις. Σε περίπτωση που κάτι τέτοιο εκτελείται από έναν εξωτερικό προμηθευτή και δεδομένου ότι το ASVS είναι ένα πρότυπο καθορισμένο με σαφήνεια, η αναφορά της απόδοσης μεταξύ διαφορετικών προμηθευτών, θα είναι αρκετά εύκολο να αξιολογηθεί.

Το ASVS περιλαμβάνει τέσσερα επίπεδα επαλήθευσης ασφάλειας, όπου το κάθε ένα θα πρέπει να καλύπτει συγκεκριμένες απαιτήσεις. Σύμφωνα με το ASVS, το επίπεδο επαλήθευσης ξεκινά από ένα πολύ βασικό επίπεδο (επίπεδο 1), χρησιμοποιώντας απλά ένα αυτοματοποιημένο εργαλείο για την επαλήθευση και συνεχίζει σε ένα πιο υψηλό επίπεδο χειροκίνητης επισκόπησης σχεδιασμού και επισκόπησης κώδικα ασφάλειας. Προχωράει έπειτα στο επίπεδο 4, το οποίο περιλαμβάνει αναζήτηση για κακόβουλο κώδικα χειροκίνητα.

Γενικά, το ASVS είναι μια νέα πρωτοβουλία, δεδομένου ότι οι περισσότεροι οργανισμοί δεν έχουν αρχίσει να το εφαρμόζουν ακόμα, όμως μπορεί να αποτελέσει έναν άριστο επιχειρησιακό οδηγό για αυτούς, επειδή στοχεύει στο να θέσει ένα πιο υψηλό επίπεδο ασφάλειας, το οποίο θα βοηθήσει τους οργανισμούς να επικοινωνήσουν κατά ομοιόμορφο τρόπο (μεταξύ των τμημάτων), αλλά και με εξωτερικούς οργανισμούς. Επιπλέον, το ASVS απαιτεί την επισκόπηση κώδικα ασφάλειας, αρχίζοντας από ένα πλήρως αυτοματοποιημένο (βασικό επίπεδο) και έπειτα προχωρώντας σε ανώτερα επίπεδα που συνδυάζουν αυτοματοποιημένη και χειροκίνητη επαλήθευση. Αυτό θα συντελέσει ώστε να εξασφαλισθεί η ασφάλεια του λογισμικού.

Συνοψίζοντας, το OWASP αποτελεί μια προσπάθεια ανοικτού κώδικα. Σύμφωνα με το OWASP Foundation, είναι σε θέση να παρέχει σημαντικές πληροφορίες, πλήρως ανεξάρτητες από οποιαδήποτε εμπορική επιχείρηση. Η διαδικασία είναι συλλογική, εστιάζοντας κυρίως στη βελτίωση της ασφάλειας των εφαρμογών και των υπηρεσιών Ιστού. Μέσω των προσπαθειών της κοινότητας του OWASP έχουν αναπτυχθεί σημαντικοί οδηγοί, προγράμματα, πρότυπα και εργαλεία, ώστε οι υπεύθυνοι ανάπτυξης, οι προμηθευτές και οι καταναλωτές να ελέγχουν το λογισμικό εφαρμογών αλλά επιπλέον, να σχεδιάζουν και να επεκτείνουν ασφαλές λογισμικό εφαρμογών.

6.3 NIST 800-115

Το NIST 800-115, Τεχνικός Οδηγός για τον Έλεγχο και την Αξιολόγηση Ασφάλειας Πληροφοριών, παρέχει οδηγίες και μια μεθοδολογία που βοηθά τους οργανισμούς να διαχειριστούν τις αξιολογήσεις της ασφάλειας των πληροφοριών τους. Όπως όλα τα έγγραφα που έχουν δημιουργηθεί από το NIST, έτσι και το 800-115 είναι διαθέσιμο σε όλους ελεύθερα για χρήση. Περιλαμβάνει πρότυπα, τεχνικές και εργαλεία που μπορούν να χρησιμοποιηθούν για την αξιολόγηση διαφόρων τύπων συστημάτων και σεναρίων. Δεν είναι τόσο λεπτομερές όσο το ISSAF ή το OSSTMM, αλλά παρέχει μια επαναλαμβανόμενη διαδικασία για τη διεξαγωγή των επισκοπήσεων ασφάλειας. Το έγγραφο περιλαμβάνει καθοδήγηση σχετικά με τα ακόλουθα:

- Πολιτικές ελέγχου ασφάλειας
- Το ρόλο της διαχείρισης στον έλεγχο ασφάλειας
- Μέθοδοι ελέγχου

- Τεχνικές επισκόπησης ασφάλειας (Review techniques)
- Τεχνικές ανάλυσης και προσδιορισμού στόχου (Target identification and analysis techniques)
- Ανίχνευση και αξιολόγηση ευπαθειών
- Τεχνικές επικύρωσης ευπάθειας στόχου (Target vulnerability validation techniques)
- Σχεδιασμός ελέγχου ασφάλειας πληροφοριών (φάση σχεδιασμού)
- Εκτέλεση ελέγχου ασφάλειας (φάση εκτέλεσης)
- Ενέργειες μετά τον έλεγχο (φάση μετα την εκτέλεση)

Το NIST 800-115 παρέχει, επίσης, 2 εργαλεία, το BackTrack και Knoppix Security Tool Distribution (STD). Το Knoppix STD δεν έχει ενημερωθεί τα τελευταία χρόνια με αποτέλεσμα το BackTrack να έχει κερδίσει έδαφος. Το BackTrack είναι ο ευκολότερος τρόπος να αποκτηθεί πρόσβαση σε πολλά από τα εργαλεία που είναι κατάλληλα για διάφορους ελέγχους ασφάλειας, όπως ανακάλυψη δικτύου (network discovery), ανίχνευση και παρακολούθηση δικτύου (scanning and sniffing), παραβίαση κωδικού πρόσβασης (password cracking), έλεγχος απομακρυσμένης πρόσβασης (remote access testing), έλεγχος bluetooth (bluetooth testing), εγκληματολογία υπολογιστών (computer forensics) και έλεγχος διείσδυσης (penetration testing). Το πλεονέκτημά του είναι ότι μας απαλλάσσει από αρκετές ώρες εγκατάστασης και επιπλέον, μας παρέχει μια ισχυρή σουίτα (suite) εργαλείων με την υποστήριξη της κοινότητας.

Συνοψίζοντας, το NIST 800-115 συντελεί στο σχεδιασμό και στην εκτέλεση των τεχνικών ελέγχων ασφάλειας πληροφοριών, στην ανάλυση συμπερασμάτων και στην ανάπτυξη στρατηγικών μετριασμού. Προβαίνει σε πρακτικές συστάσεις για το σχεδιασμό, την υλοποίηση και τη διατήρηση των διαδικασιών ελέγχου. Τέλος, επισκοπεί τα σημαντικότερα στοιχεία για τον έλεγχο ασφάλειας, δίνοντας έμφαση στις τεχνικές ελέγχου, στα οφέλη και στους περιορισμούς κάθε τεχνικής, καθώς και στις συστάσεις για τη χρήση τους.

6.4 ISSAF 0.2

Το Πλαίσιο Αξιολόγησης της Ασφάλειας Συστημάτων Πληροφοριών (Information System Security Assessment Framework-ISSAF) είναι ένα αξιολογημένο από ομότιμους (peer reviewed) δομημένο πλαίσιο της ομάδας ασφάλειας ανοικτών συστημάτων πληροφοριών (Open Information Systems Security Group), το οποίο κατηγοριοποιεί την αξιολόγηση της ασφάλειας συστημάτων πληροφοριών σε διάφορες περιοχές και απαριθμεί συγκεκριμένη αξιολόγηση ή κριτήρια ελέγχου για κάθε μια από αυτές τις περιοχές. Στοχεύει στο να παρέχει πληροφορίες σχετικές με την αξιολόγηση της ασφάλειας, που απεικονίζουν πραγματικά σενάρια. Το ISSAF θα πρέπει αρχικά να χρησιμοποιηθεί για να ικανοποιήσει τις απαιτήσεις αξιολόγησης της ασφάλειας ενός οργανισμού και μπορεί επιπλέον, να χρησιμοποιηθεί ως αναφορά για την ικανοποίηση άλλων αναγκών στην ασφάλεια πληροφοριών. Περιλαμβάνει την κρίσιμη πτυχή των διαδικασιών ασφάλειας και της αξιολόγησής τους, με στόχο να λάβει πλήρη εικόνα των ευπαθειών που πιθανόν υπάρχουν.

Αποτελείται από δύο αρχικά έγγραφα. Το ένα εστιάζει στην επιχειρησιακή πτυχή της ασφάλειας και το άλλο σχεδιάζεται ως ένα πλαίσιο ελέγχου διείσδυσης. Το πλαίσιο δεν έχει ενημερωθεί από 2006, αλλά είναι ακόμα χρήσιμο ως βασικό υλικό για τη δοκιμή ελέγχων και ως μεθοδολογία πλήρης αξιολόγησης. Το επίπεδο

λεπτομερούς εξήγησης των υπηρεσιών, των εργαλείων ασφάλειας που χρησιμοποιούνται και των πιθανών εκμεταλλεύσεων (exploits), είναι υψηλό και μπορεί να βοηθήσει έναν πεπειραμένο ελεγκτή ασφάλειας αλλά και κάποιον που κάνει τα πρώτα του βήματα στον έλεγχο.

Το ISSAF παρέχει λεπτομερείς πληροφορίες για το πώς να διεξαχθεί ένας έλεγχος διείσδυσης. Ένα από τα πλεονεκτήματά του είναι ότι δημιουργεί μια διακριτή σύνδεση μεταξύ των εργασιών ενός ελέγχου διείσδυσης και των εργαλείων του ελέγχου (PenTest). Αν και το OSSTMM δεν προτείνει τη χρήση κάποιου συγκεκριμένου εργαλείου κατά τη διάρκεια μιας αξιολόγησης, ένας επαγγελματίας ελεγκτής διείσδυσης θα χρησιμοποιήσει τα περισσότερα, εάν όχι όλα, τα εργαλεία που χρησιμοποιούνται στο ISSAF, όταν επιλέξει να χρησιμοποιήσει το OSSTMM ως τη μεθοδολογία του ελέγχου διείσδυσης.

Με το ISSAF λαμβάνεται υπόψη και ο τεχνικός και ο επιχειρησιακός κίνδυνος, με αποτέλεσμα ο ελεγκτής του PenTest να έχει περισσότερη ευελιξία στην ανάθεση ενός γενικού κινδύνου για μια ευπάθεια που ανακαλύπτεται. Κάτι τέτοιο καθιστά τους ενδιαφερόμενους πιο δεκτικούς στις μετρικές κινδύνου. Επιπλέον, οι ελεγκτές θα είναι ικανοποιημένοι ότι η τεχνική πτυχή του προβλήματος έχει εξεταστεί αλλά επιπλέον, η διαχείριση θα πειστεί ότι τα γενικά επιχειρησιακά συμφέροντα της επιχείρησης ενσωματώθηκαν στην ανάθεση κινδύνου.

Επισημαίνεται ότι η φάση σχεδιασμού και επεξεργασίας του ISSAF, ίσως να μην παρέχει αρκετή υποστήριξη για έναν επιτυχές έλεγχο διείσδυσης. Έτσι, απαιτείται η ενσωμάτωση διαδικασιών από άλλες μεθοδολογίες. Επιπλέον, μπορεί τα παραδείγματα που παρέχονται μέσα στο ISSAF να χρησιμοποιούν εργαλεία PenTest, όμως τα παραδείγματα αυτά δεν καλύπτουν όλες τις περιπτώσεις. Οι ελεγκτές ελέγχου διείσδυσης πρέπει να επεκταθούν σε όλες τις πληροφορίες που παρέχονται στο ISSAF, για διεξάγουν έναν έλεγχο ασφάλειας με επιτυχία.

Δυστυχώς, είναι συχνά δύσκολο να χρησιμοποιήσουμε τις μεθοδολογίες σε πραγματικά παραδείγματα. Το ISSAF παρέχει διάφορους τρόπους για τη μέτρηση του κινδύνου αλλά είναι πολύ απλοϊκό στις προσεγγίσεις του. Αντιθέτως, το OSSTMM υιοθετεί μια διαφορετική μέθοδο και ποσοτικοποιεί όλες τις πτυχές ασφάλειας σε έναν στόχο, εντούτοις, ο υπολογισμός που απαιτείται για λάβουμε ένα αποτέλεσμα κινδύνου είναι σύνθετος και ίσως να αποθαρρύνει κάποιους. Το OSSTMM είναι μια άριστη μεθοδολογία ελέγχου ασφάλειας που εστιάζει κυρίως στον έλεγχο διείσδυσης. ενώ το ISSAF θεωρείται πλέον πεπαλαιωμένο. Σε μερικές περιοχές οι δυο μεθοδολογίες επικαλύπτονται, αλλά υπάρχουν και σημαντικές διαφορές που επιτρέπουν στα ISSAF και OSSTMM να συμπληρώνουν το ένα το άλλο.

Υπό κάποια έννοια, το ISSAF φαίνεται να είναι ευρύτερο και πιο λεπτομερές, π.χ. περιλαμβάνει ένα τμήμα σχετικά με την αξιολόγηση συστημάτων AS400, συσκευών δικτύων, κ.λπ. Όμως, υπάρχουν πλεονεκτήματα και μειονεκτήματα σε αυτήν τη μεθοδολογία. Το πλεονέκτημα είναι ότι μας παρέχει μια «Wikipedia» ασφάλειας με πληροφορίες για το πώς να διεξάγονται αξιολογήσεις ασφάλειας για έναν ευρύ φάσμα διαδικασιών και συστημάτων. Κάτι τέτοιο όμως σημαίνει ότι απαιτούνται συχνές ενημερώσεις και προσπάθεια για να διατηρηθεί.

Η μεθοδολογία του OSSTMM, θα επηρεαστεί λιγότερο από πεπαλαιωμένα ζητήματα, επειδή μπορούμε να εφαρμόσουμε την ίδια μεθοδολογία σε αρκετές δεσμεύσεις αξιολόγησης, χρησιμοποιώντας διαφορετικές τεχνικές και εργαλεία. Από την άλλη πλευρά, το ISSAF είναι ένα πλαίσιο το οποίο μας παρέχει πληροφορίες για

τις τεχνικές, τα εργαλεία, τις βέλτιστες πρακτικές και τα ζητήματα κανονισμού προκειμένου να συμπληρώσει τη δέσμευση της αξιολόγησής μας, είτε χρησιμοποιούμε το OSSTMM ως μεθοδολογία αξιολόγησης είτε οποιαδήποτε άλλη.

6.5 Επίλογος

Όπως έχει αναφερθεί αρκετές φορές σε αυτήν την εργασία, η ασφάλεια του λογισμικού εφαρμογών είναι ένα πολυσύνθετο ζήτημα που δεν μπορεί να αντιμετωπιστεί μεμονωμένα και έπειτα να ξεχαστεί. Οι υπεύθυνοι της ασφάλειας λογισμικού εφαρμογών οφείλουν να έχουν συνεχή ενημέρωση, εγρήγορση και εκπαίδευση, προκειμένου να είναι δυνατό να αντιμετωπίζουν έγκαιρα τις νέες απειλές που πιθανόν εμφανίζονται κατά διαστήματα.

Οποιαδήποτε κι αν είναι η μεθοδολογία-προσέγγιση που χρησιμοποιούμε για τον έλεγχο ασφάλειας, θα πρέπει να εξασφαλίσουμε ότι είναι συνεπής, επαναλαμβανόμενη και βασισμένη σε βέλτιστες πρακτικές. Έτσι, οι έλεγχοί μας θα είναι περισσότερο λεπτομερείς και θα εξαλειφθεί η πιθανότητα να χάσουμε σημαντικά ζητήματα που μπορεί να μας ξεφύγουν κατά τη διάρκεια του ελέγχου. Χρησιμοποιώντας, κάποια από αυτές τις μεθοδολογίες (καθώς και τα αντίστοιχα εργαλεία) που είναι ελεύθερα διαθέσιμες από την κοινότητα ασφάλειας, μπορούμε να αξιολογήσουμε με το καλύτερο δυνατό τρόπο την ασφάλεια του λογισμικού εφαρμογών του οργανισμού μας.

Όλες οι μεθοδολογίες έχουν θετικά και αρνητικά σημεία - οι μεθοδολογίες που ερευνήθηκαν σε αυτήν την εργασία δεν αποτελούν εξαίρεση. Η απόφαση για το ποια μεθοδολογία θα πρέπει να χρησιμοποιήσουμε σε έναν έλεγχο ασφάλειας ποικίλει, ανάλογα με την εμβέλεια του έργου, τις δυνατότητες και αδυναμίες των μελών της ομάδας του έργου, καθώς και την πολυπλοκότητα του δικτύου ή των συστημάτων του πελάτη.

ΑΝΑΦΟΡΕΣ

Κεφάλαιο 1 - Εισαγωγή

1. Gollmann, D., (2002). Computer Security, Wiley,
2. Landwerh, C., (2001). Computer Security, IJIS 1, Sringer-Verlag, pp. 3 - 13.
3. Turn R., (1986). Security and Privacy requirements in computing, Proceedings of 1986 ACM Fall joint computer conference, pp. 1106 - 1114.
4. Canavan, J., (2001). The Fundamentals of Network Security, Publisher: Artech House Publishers; 1st edition
5. Gunter Ollmann. Assessing Your Security, Advice on Assessing your IT Security Posture, http://www.technicalinfo.net/papers/AssessingYourSecurity.html

Κεφάλαιο 2 - OSSTMM

6. OSSTMM - http://www.isecom.org/osstmm/
7. Herzog P, (2006). OSSTMM 2.2, Open-Source Security Testing Methodology Manual, http://isecom.securenetltd.com/osstmm.en.2.2.pdf
8. Dreamlab Technologies AG, OSSTMM - measurable security - https://www.dreamlab.net/files/documents/dlt_OSSTMM_engl.pdf
9. Herzog P, (2008). OSSTMM 3 LITE - Introduction and Sample to the Open Source Security Testing Methodology Manual - http://www.idpnow.net/Documents/OSSTMM_3.0_LITE.pdf
10. Herzog P, (2010). OSSTMM 3: The Open Source Security Testing Methodology Manual-Contemporary Secutiy Testing and Analysis – http://www.isecom.org/mirror/OSSTMM.3.pdf
11. Menefee Michael, (Tuesday, September 14, 2010). An Introduction to OSSTMM Version 3 - https://www.infosecisland.com/blogview/7797-An-Introduction-to-OSSTMM-Version-3.html
12. Herzog P, (2000). Open-Source Security Testing Methodology Manual - http://www.selfsecurity.org/unclassified/mgmt/osstmm.pdf
13. OSSTMM - http://en.wikipedia.org/wiki/Open_Source_Security_Testing_Methodology_Manual
14. Security Tools - http://www.isecom.org/research/toolsandtemplates.shtml

Κεφάλαιο 3 - OWASP

14. OWASP - http://www.owasp.org/index.php/Main_Page
15. Yvan Boily, (March, 2005). OWASP: An Introduction - http://www.owasp.org/images/a/a9/Introduction_to_OWASP.ppt
16. Jeff Williams and Dave Wichers, (2010). OWASP Top 10 - 2010: The Ten Most Critical Web Application Security Risks - http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
    http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
17. OWASP Greek Chapter - http://owasp.wordpress.com/2010/04/20/owasp-top10-2010-released/
    http://www.owasp.org/index.php/Greece
    Οι 10 πιο σημαντικοί κίνδυνοι OWASP Top 10 2010 - http://www.zero.gr/images/OWASP-T10-2010_greek_brochure.pdf

18. Παπαπαναγιώτου Κ, (2008). OWASP: Ασφάλεια στις Web εφαρμογές - http://www.saka.gr/apofoitoistamme/8/file/
19. Papapanagiotou K, Committee Member, OWASP Greek Chapter, (2008). Detecting Web Application Vulnerabilities Using Open Source Means - http://www.owasp.org/images/e/e5/OWASP_ellak-Greece.ppt

OWASP Testing Guide

20. OWASP Testing Guide - http://www.owasp.org/index.php/Category:OWASP_Testing_Project
21. Matteo Meucci, (2008). OWASP Testing Guide 2008 V3.0 - http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
22. Jeff Williams, (2007). Overview of the OWASP Testing Guide - http://www.owasp.org/images/a/af/OWASP_Testing_Guide_Presentation.zip
23. Matteo Meucci, Alberto Revelli, (2007). The new OWASP Testing Guide http://www.owasp.org/images/e/e9/OWASP_Testing_Guide_Presentation_EUSecWest07.zip
24. Gary Stoneburner, Alice Goguen, and Alexis Feringa, (2002). NIST Special Publication 800-30, Risk management guide for information technology systems - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Tools

25. Tools - http://www.owasp.org/index.php/Category:OWASP_Project
26. OWASP JbroFuzz Project - http://www.owasp.org/index.php/JBroFuzz http://www.owasp.org/index.php/OWASP_JBroFuzz_Tutorial#Performing_User_Enumeration_with_a_Valid_Set_of_Credentials
27. Pavlosoglou Yiannis, (2008). JbroFuzz 0.1 to 1.1 - Building a Java Fuzzer - http://video.google.com/videoplay?docid=-1551704659206071145#
28. OWASP DirBuster Project - http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project#tab=Overview
29. OWASP WSFuzzer Project - http://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project http://www.neurofuzz.com/modules/software/vidz.php (θα δω αν το βάλω)
30. OWASP WebScarab Project - http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project http://www.owasp.org/index.php/WebScarab_Getting_Started
31. OWASP Live CD Project - http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project#tab=Main http://mtesauro.com/files/owasp-austin_live-cd_2008-08-26.pdf
32. Penetration Testing Tools - http://www.owasp.org/index.php/Category:Penetration_Testing_Tools

OWASP Application Security Verification Standard Project

33. OWASP Application Security Verification Standard Project - http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project http://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project_Proposal
34. Boberski Mike, (2008). OWASP Application Security Verification Standard 2008 - Web Application Edition Beta -

http://www.owasp.org/images/b/b4/OWASP_ASVS_Web_Edition_2008_Beta.pdf
35. Boberski Mike, (2009). OWASP Application Security Verification Standard 2009 - Web Application Standard Release - http://www.owasp.org/images/4/4e/OWASP_ASVS_2009_Web_App_Std_Release.pdf
36. Mike Boberski (Booz Allen Hamilton), Jeff Williams (Aspect Security), Dave Wichers (Aspect Security), (2009). OWASP Application Security Verification Standard (ASVS) - Web Application Edition - https://www.owasp.org/images/5/52/About_OWASP_ASVS_Web_Edition.ppt#1
37. The ASVS team, (2009). OWASP Application Security Verification Standard 2009 - Web Application Standard - http://www.owasp.org/images/7/71/About_OWASP_ASVS.ppt

Κεφάλαιο 4 - NIST - SP 800-115
38. NIST - SP 800-115 - http://csrc.nist.gov/publications/index.html
39. Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh, (September 2008). NIST Special Publication (SP) 800-115, Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Tools
40. BackTrack - http://www.remote-exploit.org/?page_id=160 http://www.BackTrack-linux.org/
41. Knoppix STD - http://s-t-d.org/index.html

Κεφάλαιο 5 - ISSAF 0.2
42. ISSAF 0.2 - http://www.oissg.org/downloads/issaf-0.2/index.php
43. OISSG, (April 18, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2, http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2/view.html
44. OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1A, http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1a/view.html
45. OISSG, (May 01, 2006). Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B- Penetration Testing Framework (PTF), http://www.oissg.org/downloads/issaf-0.2/information-systems-security-assessment-framework-issaf-draft-0.2.1b/view.html
46. ISSAF - People, Process & Technology - http://www.oissg.org/wiki/index.php?title=ISSAF-PEOPLE%2CPROCESS_%26_TECHNOLOGY
47. ISAAF - Penetration Testing Framework - http://www.oissg.org/wiki/index.php?title=ISAAF-PENETRATION_TESTING_FRAMEWORK

Παράρτημα-Tools
48. Top 100 Network Security Tools provided by Insecure.org, http://sectools.org/

ΠΑΡΑΡΤΗΜΑ Ι

Απόδοση Ξενόγλωσσων Όρων Στα Ελληνικά

Ξενόγλωσσος Όρος	Απόδοση στα Ελληνικά
agitating	ανατάραξη
assets	αγαθά
attack simulation	προσομοίωση επίθεσης
audit	έλεγχος
authentication	αυθεντικοποίηση
computing resource	υπολογιστικός πόρος
conducted	διεξάγονται
continuity	συνέχεια
decoder	αποκωδικοποιητής
defense	άμυνα
document grinding	συλλογή και ανάλυση εγγράφων
echo process	διαδικασία αντήχησης
error code	κωδικός σφάλματος, (μήνυμα λάθους)
exploit	εκμετάλλευση, αδυναμίες, κενά, τρύπες
flaws	ατέλειες
fuzzy risk analysis	ασαφής ανάλυση κινδύνου
hash values	τιμές επιτομής
host computer	ξενιστής υπολογιστής
impact	επίπτωση, επίδραση, αντίκτυπος, συνέπεια
indentification	ταυτοποίηση (διακρίβωση ταυτότητας), προσδιορισμός
inherent risk	εγγενής κίνδυνος
instance	στιγμιότυπο
intelligence	συλλογή πληροφοριών
Intrusion Detection System	Σύστημα Ανίχνευσης Παρείσφρησης
IT-Information Technology	Τεχνολογία Πληροφοριών
logistics	εφοδιαστική, η διαδικασία στρατηγικής διοίκησης του εφοδιασμού
manual	χειροκίνητος
mis-configurations	λανθασμένες ρυθμίσεις
mitigation	μετριασμός, μείωση
model	πρότυπο
module	συνιστώσα, ενότητα
network packets	πακέτα δικτύου
pattern	μοτίβο
privacy	ιδιωτικότητα
process	διαδικασία
project	έργο
request	αίτηση, αίτημα
response	απόκριση, απάντηση
review	επισκόπηση

root causes analysis	ανάλυση πρωταρχικών/γενεσιουργών αιτιών
scouting	διερεύνηση
security through obscurity	συσκότιση
server	εξυπηρέτης
software assets	αγαθά λογισμικού
spoofing	αντιποίηση
stream	ροή
task	εργασία, διεργασία
testing	έλεγχος
third party	τρίτες οντότητες
threat	απειλή
token	τεκμήριο, στοιχείο
user awareness	συνειδητοποίηση χρήστη
user input	εισαγωγή δεδομένων από τον χρήστη
vulnerability	αδυναμία, ευπάθεια
web server	εξυπηρέτης ιστού
wizard	οδηγός

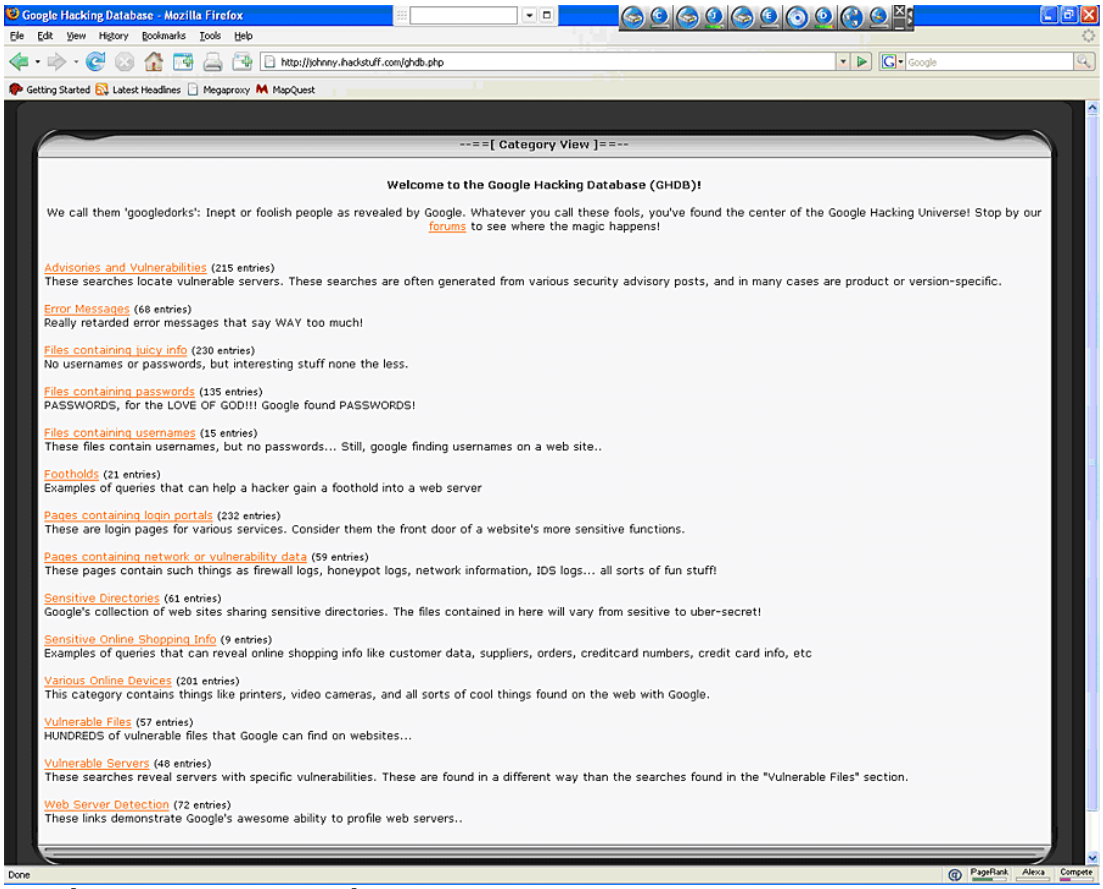
ΠΑΡΑΡΤΗΜΑ ΙΙ

Σε αυτό το παράρτημα, παραθέτουμε περισσότερες λεπτομέρειες για κάποια εργαλεία που κατά την αναζήτηση πληροφοριών σχετικά με τη συγκεκριμένη εργασία, φάνηκαν να είναι σημαντικά αλλά και κατάλληλα για τους διάφορους ελέγχους των περισσότερων μεθοδολογιών αξιολόγησης της ασφάλειας λογισμικού εφαρμογών. Θα μπορούσαμε να πούμε ότι αποτελούν ένα δείγμα των πιο δημοφιλών εργαλείων τα οποία ένας ελεγκτής θα έβρισκε χρήσιμα για τους ελέγχους ασφάλειας.

1. Google and Google Hacking Database

http://www.google.com, http://www.hackersforcharity.org/ghdb/

Το Google είναι ένα σημαντικό εργαλείο για την εύρεση όλων των ειδών πληροφορίας στον Ιστό, συμπεριλαμβανομένων ακόμη και των πληροφοριών που δεν θα έπρεπε να βρίσκονται εκεί. Το Google χρησιμοποιείται για ανιχνεύσεις και ανταγωνιστικής συλλογής πληροφοριών και ιδιωτικότητας των αγαθών. Ο Johnny Long κατέστησε αυτήν την μέθοδο διάσημη με την Google Hacking Database (GHD).



Σχήμα 35. Χρησιμοποιούμε το Google και την Google Hacking Database για να βρούμε στοιχεία με προστασία πνευματικής ιδιοκτησίας, ιδιωτικές πληροφορίες και συστήματα που εκτίθενται στον Ιστό ενώ δεν θα έπρεπε.

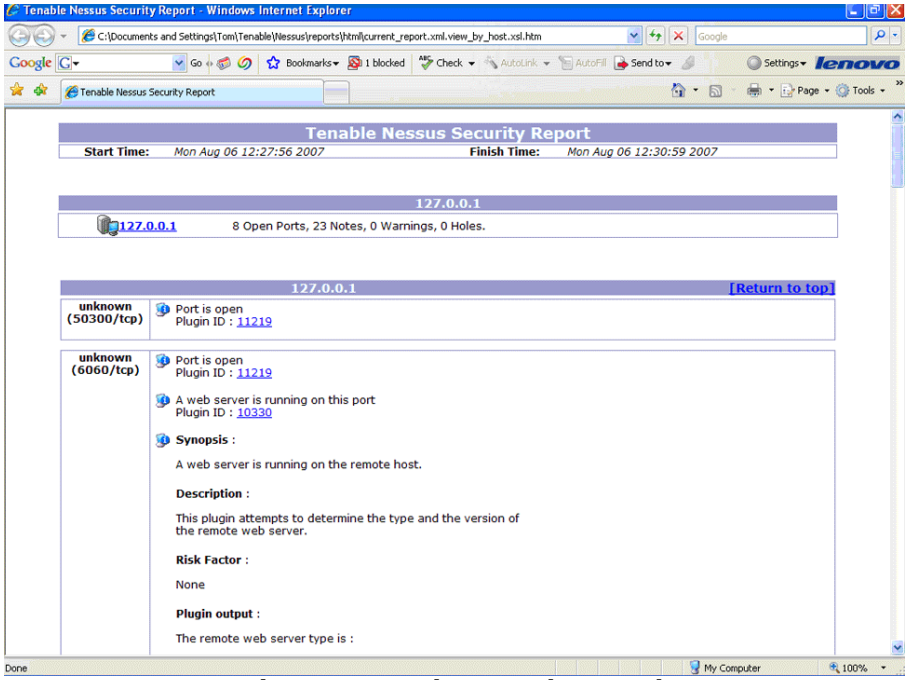
Η χρησιμοποίηση του Google για την εύρεση ευπαθών συστημάτων που συνδέονται με το δίκτυό μας είναι πάντα μια πολύ καλή εμπειρία. Ας υποθέσουμε ότι βρίσκουμε έναν εκτυπωτή που είναι συνδεμένος άμεσα μέσω του τείχους προστασίας (firewall) με το Διαδίκτυο. Κάτι τέτοιο συμβαίνει πολύ πιο συχνά από όσο νομίζουμε.

Ο ιστότοπος του Johnny Long είναι ένας εύκολος τρόπος για να μάθει κανείς πώς γίνεται αυτή η διαδικασία. Απλά επανακατευθύνουμε τις επερωτήσεις της GHD στο εύρος των IP διευθύνσεών μας. Κατόπιν, επεξεργαζόμαστε τις επερωτήσεις ώστε να ταιριάξουν με τους συγκεκριμένους δρομολογητές, μεταγωγείς (switches), εκτυπωτές και εξυπηρέτες ιστού μας. Οι ίδιες τεχνικές χρησιμοποιούνται για να ανακαλύψουμε τα δεδομένα ιδιωτικότητας των υπαλλήλων μας, που μπορεί να έχουν διαρρεύσει στο Διαδίκτυο από το δίκτυό μας. Αυτή η διαδικασία διευκρινίζεται καλά για οποιαδήποτε υποδομή δικτύου και συστήματα που συνδέονται στο Διαδίκτυο.

2. Nessus - ανιχνευτής ασφάλειας

http://www.nessus.org/

Μετά τη χρησιμοποίηση του Google για τον καθορισμό των τύπων των ξενιστών (hosts) στο δίκτυό μας, θα πρέπει να ξεκινήσουμε τον έλεγχο με μια γενική αξιολόγηση ευπαθειών. Το ιδανικό εργαλείο είναι το Nessus. Θα χρησιμοποιήσουμε τα αποτελέσματα από τις ανιχνεύσεις του Nessus ώστε να καθοδηγήσουμε τον υπόλοιπο έλεγχο. Παραδείγματος χάριν, εάν ανακαλύψουμε έναν εξυπηρέτη ιστού ή μια εφαρμογή που τρέχει σε έναν host, θα πρέπει να χρησιμοποιήσουμε τις πιθανές ευπάθειες που απαριθμούνται στην αναφορά του Nessus ως διανύσματα επίθεσης για εξερεύνηση ή εκμετάλλευση, χρησιμοποιώντας άλλα εργαλεία όπως: Wikto[9] ή Metasploit[10].



Σχήμα 36. Το Nessus είναι το βασικό εργαλείο αξιολόγησης που προσφέρει πληροφορίες σχετικά με το ποιες θύρες, πρωτόκολλα, εφαρμογές και υπηρεσίες υπάρχουν στο σύστημα υπό επισκόπηση.

Χαρακτηριστικά, το Nessus παρέχει μια ολοκληρωμένη μηχανή για «ανίχνευση θυρών-port scanning» και αναγνώριση υπηρεσιών, καθώς και ένα ημιαυτοματοποιημένο μηχανισμό για την ενημέρωση για νέου είδους επιθέσεις. Το Nessus αρχικά ξεκινά μια επίθεση ανίχνευσης θυρών, ελέγχοντας για ανοικτές θύρες στον υπολογιστή στόχο. Αφού εντοπίσει τις θύρες, προσπαθεί να βρει το λειτουργικό σύστημα που χρησιμοποιεί ο υπολογιστής, καθώς και πιθανές επιδιορθώσεις ασφάλειας (patches), πακέτα επιδιόρθωσης (service packs) και ενημερώσεις ασφάλειας (security updates). Στη συνέχεια, δοκιμάζει να χρησιμοποιήσει exploits

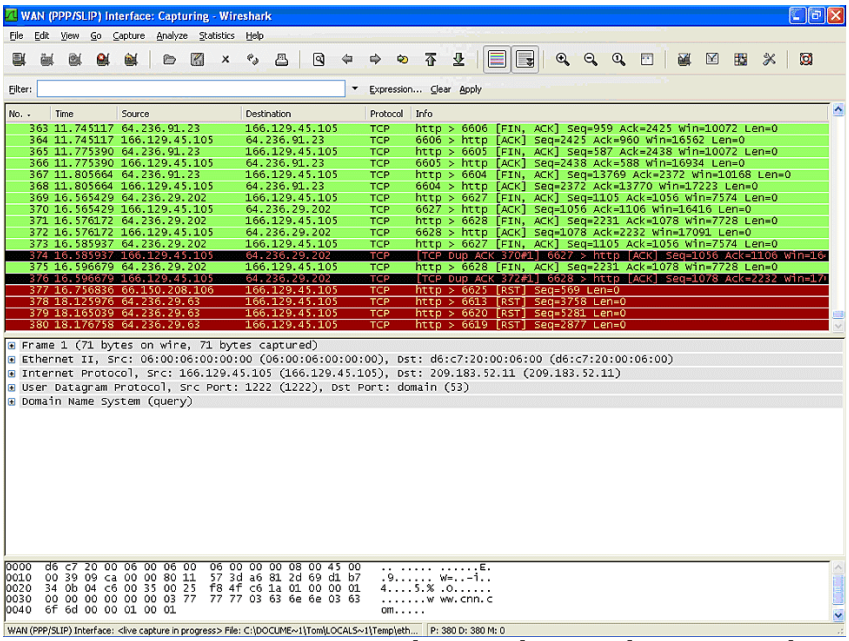
στις ανοικτές θύρες για να δει αν είναι εφικτό να αποκτήσει πρόσβαση. Τέλος, δημιουργεί εύκολες και ευανάγνωστες αναφορές για την κατάσταση των υπό εξέταση μηχανημάτων, καθώς και μια εξειδικευμένη γλώσσα για τη συγγραφή «σεναρίων» επίθεσης. Κατ' επιλογή του χρήστη, μπορεί να δοκιμάσει το ίδιο πρόγραμμα να επιτεθεί στο σύστημα, ώσπου αυτό να καταλήξει σε άρνηση παροχής υπηρεσιών (DoS) ή κατάρρευση (crash). Τέλος, επιτρέπει τον έλεγχο οποιασδήποτε διεύθυνσης IP χωρίς την ανάγκη κάποιας ειδικής αδείας χρήσης, αφού παρέχεται κάτω από την GNU GPL.

Το Nessus έχει μια έκδοση για Linux/Unix και μια έκδοση για Windows. Το σύστημα Nessus αποτελείται από έναν Nessus server, έναν client, Nessus plug-ins και τη βάση γνώσης. Εξετάζει όλες τις πτυχές ενός στόχου, συμπεριλαμβάνοντας τα εξής: λειτουργικό σύστημα, θύρες, υπηρεσίες και εφαρμογές. Κατά συνέπεια, οι αναφορές μπορεί να είναι εκτενείς αλλά είναι περιεκτικές. Θα πρέπει να επικυρώσουμε τα συμπεράσματα δεδομένου ότι το Nessus, όπως και άλλοι ανιχνευτές δικτύων, είναι επιρρεπές σε ψευδώς θετικά (false positives).

3. Wireshark - αναλυτής πακέτων

http://www.wireshark.org/

Στο παρελθόν γνωστό και ως Ethereal, το Wireshark είναι ένας εξαιρετικά ισχυρός αναλυτής πρωτοκόλλων. Τρέχει σε ένα ευρύ φάσμα λειτουργικών συστημάτων και επιτρέπει την live σύλληψη της κίνησης (traffic) δικτύων και την ανάλυση της κίνησης που συλλαμβάνεται από εξωτερικές πηγές. Προσφέρει ένα ευρύ φάσμα προεπιλεγμένων αποκωδικοποιητών (decoders) πρωτοκόλλων και μπορεί να αναλύσει τις διακριτές ροές κίνησης με ευκολία. Η οθόνη περιέχει τέσσερα κύρια τμήματα: τη γραμμή επιλογών (menu bar), τη λίστα πακέτων, λεπτομέρειες πακέτων (πρωτόκολλα και τομείς πρωτοκόλλου) και τέλος, τα bytes πακέτων που παρουσιάζουν την ακατέργαστη ροή δεδομένων σε δεκαεξαδικές και ASCII μορφές (formats). Τα εργαλεία γραφικής ανάλυσης του Wireshark παρέχουν μια σαφή εικόνα, όταν εξετάζονται προβλήματα ανίχνευσης λαθών ή ερευνώνται αδυναμίες κατά τη διάρκεια ενός ελέγχου διείσδυσης.



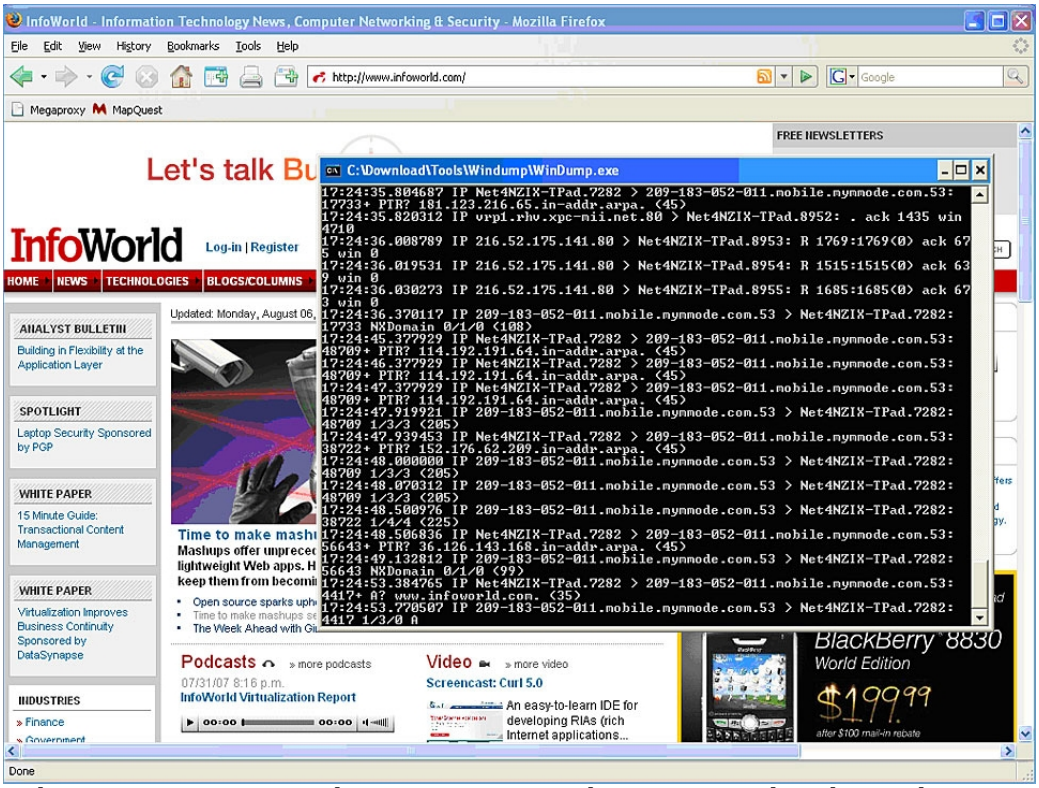
Σχήμα 37. Το Wireshark παρακολουθεί τα πακέτα δικτύων και παρέχει ονόματα χρηστών και κωδικούς πρόσβασης

Το πρόγραμμα αυτό, όπως αναφέρθηκε και προηγουμένως, είναι ένας αναλυτής πακέτων (packet analyzer), με κύριο στόχο την εύρεση μηνυμάτων, τα οποία είναι χρήσιμα για το χρήστη. Μπορεί να διαβάζει πακέτα είτε online σε ένα δίκτυο, είτε αποθηκευμένα σε κάποιο αρχείο αργότερα. Τα online δεδομένα, μπορούν να συγκεντρώνονται από Ethernet, Wireless, PPP και loopback επικοινωνίες. Τα δεδομένα που συλλέγονται μπορούν να υποβληθούν σε επεξεργασία ή να μετατραπούν ώστε να αναγνωρίζονται από διαφορετικά προγράμματα καθώς είναι εφικτή και η αναβάθμιση με plugins για την εγκατάσταση νέων πρωτοκόλλων.

4. TCPDump - αναλυτής δικτύων

http://www.tcpdump.org/

Το TCPDump, αλλά και το WinDump (που βασίζεται σε Windows) είναι βοηθήματα σύλληψης των αρχικών πακέτων. Είναι παρόμοια σε δυνατότητες και υποστηρίζονται ενεργά και τα δύο. Και τα δύο εργαλεία επιτρέπουν τη δημιουργία, την έγχυση και τη σύλληψη πακέτων κατά τη διάρκεια ενός ελέγχου ασφάλειας. Και τα δύο καθοδηγούνται από γραμμή εντολών. Οι πληροφορίες που παρέχονται είναι παρόμοιες με αυτές του Wireshark[3] και στην πραγματικότητα μπορούν να χρησιμοποιηθούν και τα δύο εναλλάξ (δεδομένα του TCPDump στο Wireshark ή αντιστρόφως).



Σχήμα 38. Το Windump, όπως και το κλασικό TCPDump, είναι ένα γρήγορο και ευέλικτο εργαλείο για τη σύλληψη μεγάλης ποσότητας δεδομένων για ανάλυση πρωτοκόλλων. Είναι χρήσιμο για παραβίαση (cracking) ασύρματης πρόσβασης, κωδικού πρόσβασης ή συνόδου.

Αυτό το εργαλείο χρησιμοποιείται ευρέως για να γίνει αποσφαλμάτωση (debugging) σε εφαρμογές που χρησιμοποιούν επικοινωνιακά πρωτόκολλα με άλλα συστήματα ή δίκτυα, προκειμένου να βρεθεί κάποιο πρόβλημα και να απομονωθεί. Επιπλέον, μπορεί να χρησιμοποιηθεί για να παρακολουθεί συνδέσεις με μη ασφαλή πρωτόκολλα και μεθόδους επικοινωνίας, όπως HTTP και Telnet, υποκλέπτοντας ονόματα χρήστη, κωδικούς πρόσβασης και διάφορα άλλα ευαίσθητα δεδομένα. Το

TCPDump παρέχεται ως προεπιλεγμένη εγκατάσταση μαζί με τα περισσότερα λειτουργικά συστήματα Unix. Το WinDump απαιτεί τη χρήση του λογισμικού Winpcap για τα Windows ώστε να επιτραπεί η σύλληψη πακέτων.

5. Netcat - εξερευνητής δικτύων
http://netcat.sourceforge.net/

Αφού ανακαλύψουμε τις ευπάθειες με Nessus[2] ή Wikto[9], θα πρέπει να τις ελέγξουμε μέσω της εκμετάλλευσης. Το Netcat είναι γνωστό ως «ελβετικός σουγιάς για δίκτυα» των εργαλείων ελέγχου. Είναι ένα εργαλείο γραμμής εντολών για την ανάγνωση και εγγραφή δεδομένων στις συνδέσεις TCP και UDP. Μπορεί να δημιουργήσει σχεδόν οποιαδήποτε σύνδεση που απαιτείται σε κάθε κατεύθυνση, αυτό το καθιστά ανεκτίμητο για την διερεύνηση δικτύων και εξυπηρετών κατά τη διάρκεια του ελέγχου διείσδυσης. Είναι ένα τέλειο εργαλείο για τη διαχείριση back doors[13] και μπορεί να κληθεί από άλλα προγράμματα. Κατά συνέπεια η χρήση αυτού του εργαλείου μπορεί να αυτοματοποιηθεί ή προκαθορισθεί. Ένα ευρύ φάσμα των παραγώγων του Netcat υπάρχει πλέον για εξειδικευμένες εφαρμογές όπως SSL.

6. Kismet - παρακολούθηση ασύρματων επικοινωνιών
http://www.kismetwireless.net/

Το Kismet, ένα ισχυρό πρόγραμμα ανίχνευσης ασύρματων επικοινωνιών 802.11 (στρώματος 2), χρησιμεύει ως εργαλείο αναγνώρισης για ασύρματους ξενιστές (hosts). Το Kismet προσδιορίζει τους πιθανούς ασύρματους στόχους για εκμετάλλευση. Κατά την εξέταση των καταγραφών του, συστήνεται να ασχοληθούμε αρχικά με τα σημεία πρόσβασης που δεν κρυπτογραφούνται, και έπειτα με εκείνα που χρησιμοποιούν προεπιλεγμένες διαμορφώσεις.

Είναι ένα πρόγραμμα το οποίο κατά κύριο λόγο παρακολουθεί ασύρματα δίκτυα ταυτόχρονα. Συνδέεται κατά σειρά σε όλα τα διαθέσιμα δίκτυα, ακόμη και όταν αυτά δεν εκπέμπουν, παρακολουθώντας τα πακέτα που αυτά ανταλλάσσουν και αποθηκεύοντάς τα για περαιτέρω επεξεργασία. Αλλάζει συνέχώς δίκτυα, χρησιμοποιώντας κατά σειρά διαφορετικά κανάλια για να επιτύχει τη μεγαλύτερη δυνατή συλλογή πακέτων. Επίσης, έχει τη δυνατότητα να ανακαλύπτει προγράμματα παρακολούθησης (sniffers) που λειτουργούν σε κάποιο δίκτυο και επιπλέον, είναι εφικτό να συγκεντρώσει και πληροφορίες σχετικά με τη γεωγραφική θέση των δικτύων, αν σε αυτά υπάρχει εκπομπή δεδομένων μέσω πρωτοκόλλων GPS[78].

7. Aircrack - WLAN cracker
http://www.aircrack-ng.org/

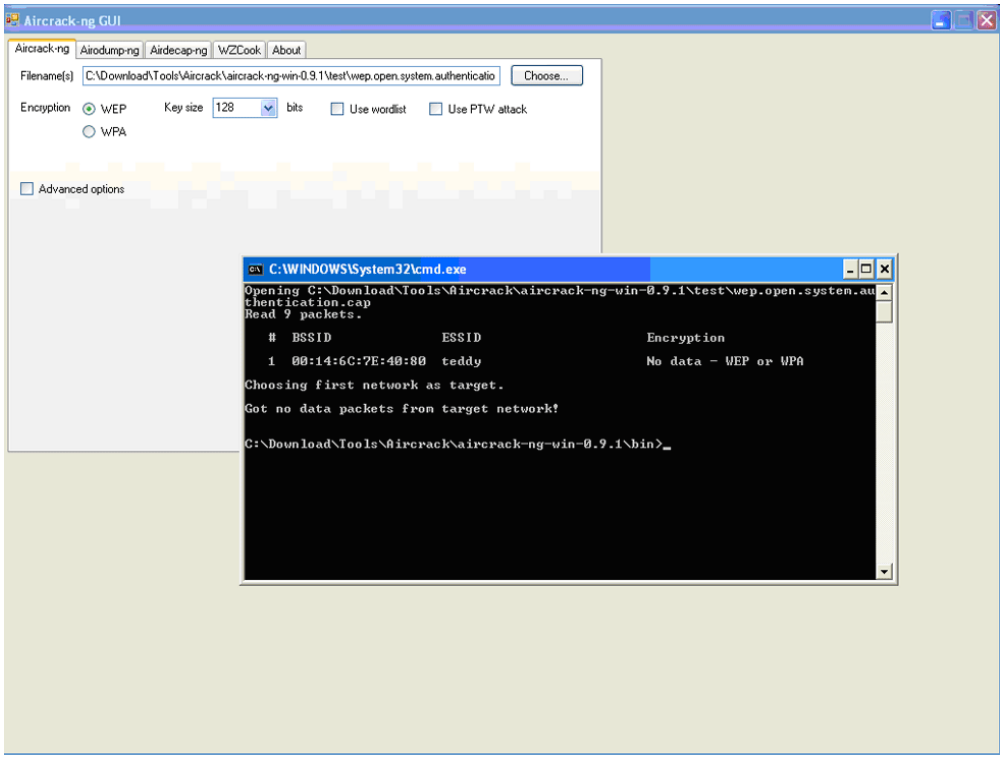
Ας υποθέσουμε ότι όλα τα ασύρματα συστήματά μας χρησιμοποιούν κάποιο τύπο κρυπτογράφησης, τότε θα χρειαστούμε κάποιο τρόπο για να τα παραβιάσουμε. Η καλύτερη μέθοδος είναι να χρησιμοποιηθεί το TCPDump[4] ή WinDump για να συλλάβει τα μεγάλα ποσά της κίνησης στο σημείο πρόσβασης του ελέγχου. Έπειτα, μπορούμε να χρησιμοποιήσουμε το σύνολο δεδομένων που προέκυψε στο Aircrack, ώστε να επιχειρήσουμε την αποκρυπτογράφηση των επικοινωνιών στο σημείο πρόσβασης.

Το Aircrack είναι ένα πρόγραμμα παραβίασης (cracking) 802.11.WEP και WPA-PSK κλειδιών που μπορεί να ανακτήσει τα κλειδιά μόλις συλληφθούν αρκετά πακέτα που χρησιμοποιούνται για τη σύνδεση συστημάτων στο ασύρματο δίκτυο που παρακολουθεί. Εφαρμόζει την πρότυπη επίθεση FMS μαζί με μερικές

[78] GPS (Global Positioning System) - Παγκόσμιο Σύστημα Θεσιθεσίας

βελτιστοποιήσεις όπως επιθέσεις KoreK, καθώς επίσης και την επίθεση PTW, καθιστώντας κατά συνέπεια την επίθεση πολύ γρήγορη σε σχέση με άλλα εργαλεία WEP cracking.

Χρειάζεται μια αρκετά μεγάλη βάση δεδομένων πακέτων από το δίκτυο στόχου για να αρχίσει η παραβίαση των κωδικών πρόσβασης. Οι τέσσερις ενότητες αυτής της σουίτας περιλαμβάνουν: το airodump - ένα βοήθημα σύλληψης πακέτων ασύρματων επικοινωνιών, το aireply - το οποίο εκτελεί έγχυση πακέτων για τον έλεγχο ασφάλειας, το aircrack - το οποίο παραβιάζει τον κωδικό πρόσβασης χρησιμοποιώντας επίθεση «ωμής βίας» (brute force) και κρυπτογραφικές μεθόδους και το airdecap - το οποίο αποκρυπτογραφεί τις ροές (streams) πακέτων WEP και WPA, μόλις παραβιαστούν οι κωδικοί πρόσβασης.

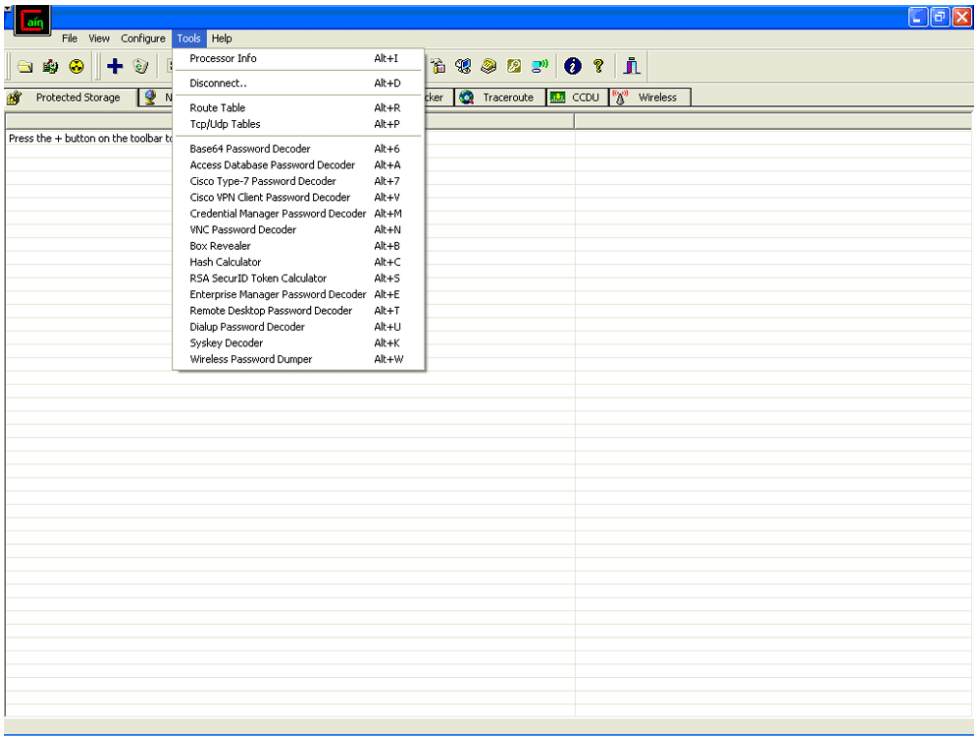


Σχήμα 39. Το Aircrack είναι ο μηχανισμός για την απόκτηση πρόσβασης σε κρυπτογραφημένα ασύρματα κανάλια, χρησιμοποιώντας ένα σύνολο δεδομένων που παρέχεται από το Windump.

8. Cain and Abel - cracker κωδικών πρόσβασης

http://www.oxid.it/cain.html

Αφού έχουμε ανακαλύψει έναν εξυπηρέτη μέσω του Nessus[2] και τον έχουμε παραβιάσει μέσω του Metasploit[10] ή Netcat[5], θα μπορούσαμε να χρησιμοποιήσουμε το Cain & Abel για να παραβιάσουμε τους κωδικούς πρόσβασης στο λειτουργικό σύστημα και τις εφαρμογές. Είναι ένα ελεύθερο εργαλείο ανάκτησης κωδικών πρόσβασης για τα λειτουργικά συστήματα της Microsoft. Επιτρέπει την εύκολη ανάκτηση των διάφορων κωδικών πρόσβασης με την καταγραφή (sniffing) του δικτύου, το σπάσιμο των κρυπτογραφημένων κωδικών πρόσβασης χρησιμοποιώντας επιθέσεις με χρήση λεξικού, «ωμής βίας», κρυπτολογικής ανάλυσης κ.ά., την αποκωδικοποίηση ανακατωμένων κωδικών πρόσβασης, την ανάκτηση κλειδιών ασύρματου δικτύου, την αποκάλυψη παραθύρων κωδικού πρόσβασης, την αποκάλυψη των εναποθηκευμένων κωδικών πρόσβασης και την ανάλυση των πρωτοκόλλων δρομολόγησης.



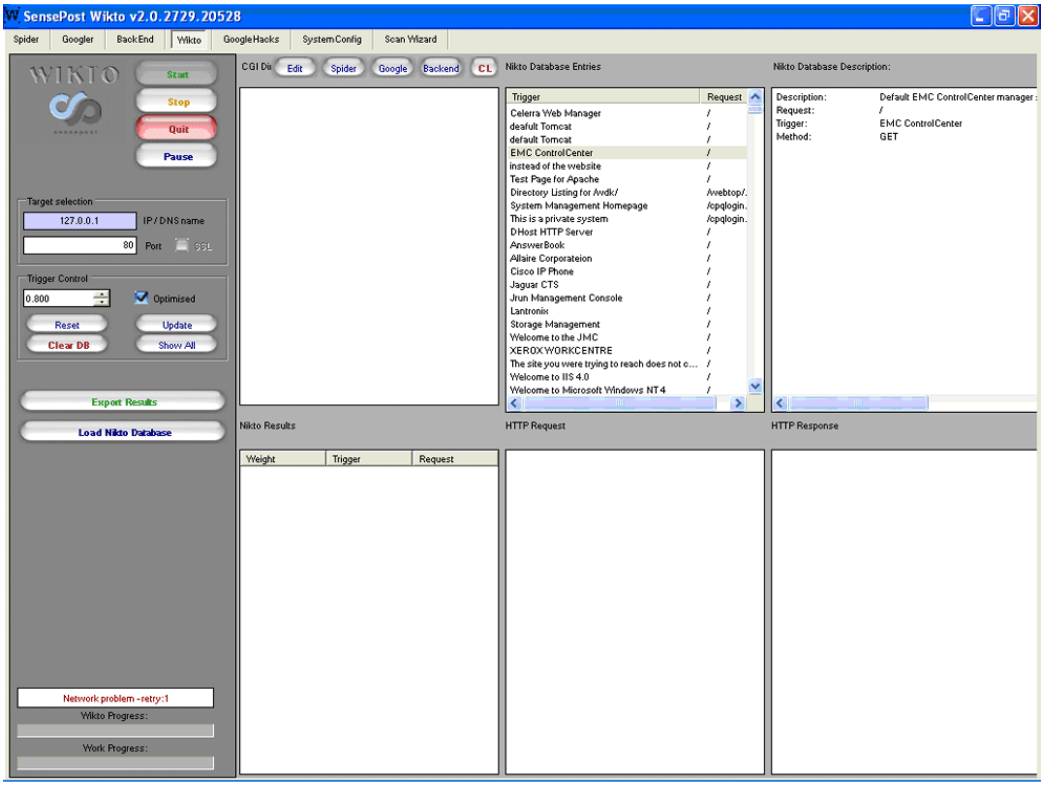
Σχήμα 40. Ένα βασικό συστατικό του ελέγχου συστημάτων που αξιολογεί τη δύναμη των πιστοποιητικών του χρήστη. Το Cain & Abel παραβιάζει τα πιστοποιητικά σε ένα μεγάλο εύρος συστημάτων και παρέχει μια εύχρηστη διεπαφή.

Το Cain & Abel αρχικά, σαρώνει το δίκτυο στο οποίο βρίσκεται το σύστημα και παρουσιάζει όλους τους διαθέσιμους κόμβους. Στη συνέχεια, χρησιμοποιεί ARP Poisoning, για να κάνει εκτροπή όλης της κίνησης μέσα από αυτό το σύστημα. Έτσι έχει τη δυνατότητα να καταγράφει κάθε πακέτο που περνά στο δίκτυο, όταν χρησιμοποιείται κάποιος δρομολογητής. Μετά από μικρό χρόνο παραμονής στο δίκτυο, μπορεί να παρουσιάσει ονόματα ομάδων (user groups) και ονόματα χρηστών (usernames), καθώς και τους συγκεντρωμένους κωδικούς πρόσβασης. Εάν οι κωδικοί πρόσβασης είναι κρυπτογραφημένοι, ή υπάρχει κρυπτογράφηση σε δεδομένα που μεταφέρονται, ή τέλος είναι κρυπτογραφημένα τα URLs που χρησιμοποιούνται στην εσωτερική και εξωτερική επικοινωνία του δικτύου, το εργαλείο είναι εφοδιασμένο με cracker κωδικού πρόσβασης δυνατοτήτων επίθεσης λεξικού, «ωμής βίας» και πολλών άλλων αλγορίθμων.

9. Wikto - ανιχνευτής εξυπηρέτη Ιστού

http://www.sensepost.com/labs/tools/pentest/wikto

Αφού ανακαλύψουμε ένα εξυπηρέτη ιστού χρησιμοποιώντας το Nessus[2], θα πρέπει να τρέξουμε ένα εργαλείο αξιολόγησης εξυπηρετών ιστού στο σύστημα για να βρούμε πιο συγκεκριμένα κενά ασφάλειας. Ένα επαγγελματικό εργαλείο για εξυπηρέτες ιστού είναι το Wikto, το οποίο είναι παρόμοιο με το γνωστό εργαλείο αξιολόγησης εξυπηρετών ιστού, το Nikto. Και τα δύο υποστηρίζονται από την κοινότητα ανοικτού κώδικα με το Wikto να παρέχει πρόσθετη λειτουργικότητα. Παραδείγματος χάριν, το Wikto αρχίζει πάντα με έναν οδηγό (wizard) ανίχνευσης Ιστού (Σχήμα 41).



Σχήμα 41. Αφότου έχουμε ανακαλύψει έναν εξυπηρέτη ιστού ανιχνεύοντας με το Nessus, θα χρησιμοποιήσουμε το Wikto για την έρευνα ευπαθειών συγκεκριμένα για http ή https

Το Wikto διαπερνά μια βάση δεδομένων ευπάθειας συγκεκριμένα για εξυπηρέτες ιστού και σχετικά στοιχεία (συμπεριλαμβάνοντας εφαρμογές Java, βάσεις δεδομένων, φόρμες και εικόνες), και επίσης αξιοποιεί πλήρως τη Google Hacking Database. Η αράχνη Wikto ανιχνεύει τον ιστότοπο στόχου και χαρτογραφεί τη δομή καταλόγων του, ενώ ο ανιχνευτής ευπάθειας επισκοπεί τις πιθανές αδυναμίες ασφάλειας. Για την αξιολόγηση της ευπάθειας, το Wikto χρησιμοποιεί τη βάση δεδομένων ευπάθειας του Nikto. Μια δευτερεύουσα αδυναμία του είναι η χρήση της CSV μορφής (format) για την εξαγωγή των εκθέσεων. Το CSV δεν ήταν ποτέ γνωστό ως ένας εύκολος τρόπος για να παρουσιασθούν τα δεδομένα εκθέσεων.

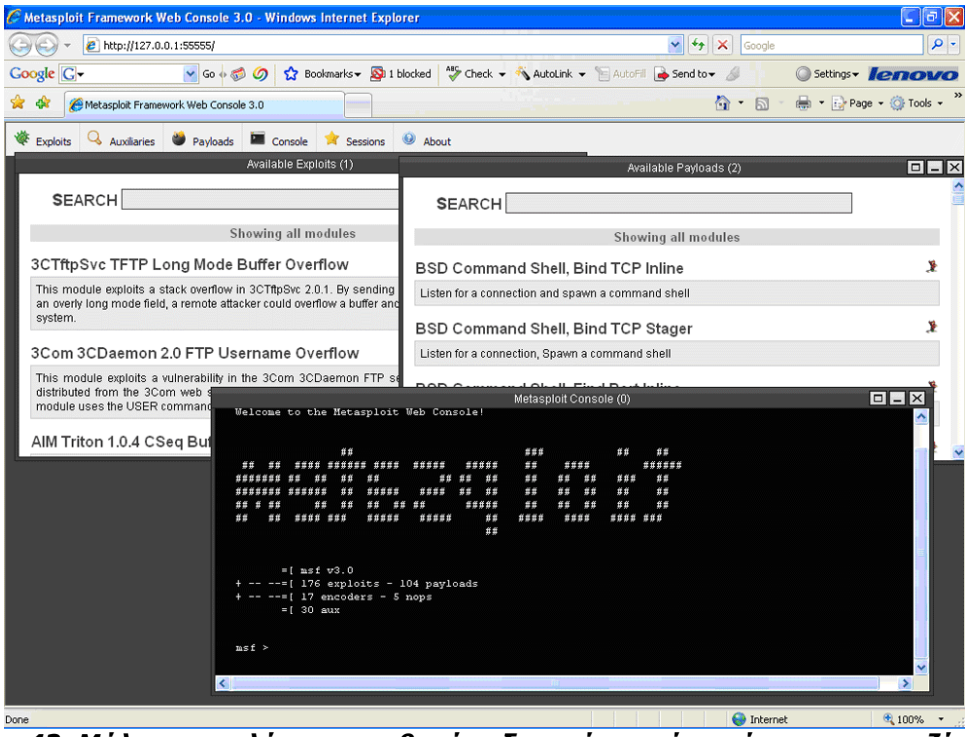
10. Metasploit - πλαίσιο εκμετάλλευσης

http://www.metasploit.com/

Το Metasploit, το οποίο εμφανίστηκε το 2004, είναι άλλο ένα εργαλείο που θα πρέπει να έχουμε στην εργαλειοθήκη μας. Το Metasploit είναι ο ευκολότερος τρόπος για να ελεγχθεί ότι μια ευπάθεια που προσδιορίζεται από το Nessus[2] ή Wikto[9], είναι πραγματικά ένα κενό ασφάλειας. Περιέχει έναν εκκινητή ενοτήτων (module launcher) για να προσαρμόσει και το exploit και το ωφέλιμο φορτίο (payload) που προορίζονται για έναν συγκεκριμένο στόχο. Εάν η διείσδυση είναι επιτυχής, ο ελεγκτής προμηθεύεται ένα φλοιό (shell) για να αλληλεπιδράσει με το ωφέλιμο φορτίο στο σύστημα στόχου. Υπάρχουν περίπου 350 διαφορετικές ενότητες (modules) για την κάλυψη ενός ευρέως φάσματος ξενιστών (hosts) και λειτουργικών συστημάτων. Εάν η αποθήκη του Metasploit δεν έχει ήδη ένα συγκεκριμένο exploit για την συγκεκριμένη ευπάθεια, μπορούμε να δημιουργήσουμε ένα εμείς.

Πιο αναλυτικά, το συγκεκριμένο πρόγραμμα, έχει ως κύριο στόχο την εκτέλεση κακόβουλου κώδικα σε συστήματα. Δίνει τη δυνατότητα στο χρήστη να παραμετροποιήσει το πρόγραμμα για να εκμεταλλευτεί το exploit που θέλει

(παρέχοντας βάση δεδομένων πολλών γνωστών bugs για όλα τα λειτουργικά συστήματα) και να δει αν ο στόχος είναι ευάλωτος στο επιλεγμένο exploit. Στη συνέχεια, ο χρήστης μπορεί να δημιουργήσει τον κώδικα που θέλει να εκτελέσει στο μηχάνημα-στόχο, κατόπιν επιτυχούς πρόσβασης σε αυτό και του δίνει τη δυνατότητα να τον κωδικοποιήσει με διάφορες μορφές κωδικοποίησης, για να μη γίνει αντιληπτός από προγράμματα IDS. Τέλος, το εργαλείο Metasploit εκτελεί τον κώδικα στον στόχο από τον οποίο ο χρήστης περιμένει τα αποτελέσματα.



Σχήμα 42. Μόλις ανακαλύψουμε πιθανές αδυναμίες σε ένα σύστημα, χρειαζόμαστε ένα εργαλείο για να προσπαθήσουμε να τις εκμεταλλευτούμε. Το Metasploit παρέχει και τις εκμεταλλεύσεις (exploits) και ένα πλαίσιο για τη δημιουργία νέων διανυσμάτων επίθεσης.

11. Paros Proxy - proxy αξιολόγησης ευπάθειας των εφαρμογών ιστού

http://www.parosproxy.org/

Το Paros Proxy είναι ένας proxy ιστού, βασισμένος σε Java, που δημιουργήθηκε για την αξιολόγηση ευπάθειας των εφαρμογών ιστού. Λειτουργεί ως διαμεσολαβητής, επιτρέποντας σε κάθε χρήστη να επεξεργάζεται και να παρακολουθεί τα μηνύματα HTTP και HTTPS μεταξύ του εξυπηρέτη (server) και πελάτη (client), προκειμένου να τροποποιήσει δεδομένα/αντικείμενα όπως cookies και φόρμες (forms). Περιλαμβάνει έναν αναγνώστη κίνησης ιστού (web traffic recorder), αράχνη ιστού (web spider), υπολογιστή κερματισμού (hash calculator), καθώς και έναν ανιχνευτή για τον έλεγχο κοινών επιθέσεων σε εφαρμογές ιστού όπως έγχυση SQL και cross-site scripting.