
Τμήμα
Μηχανικών
Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Δυτικής Ελλάδας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σύγκριση μεθοδολογιών ελέγχου διήθησης για δικτυακές υποδομές

Βασίλειος Παπαθανασίου

Αριθμός Μητρώου
0819

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ
ΠΑΕΑΣΚΕΥΑΣ ΚΙΤΣΟΣ

ΑΝΤΙΡΡΙΟ, 2016

Περιεχόμενα

Ευρετήριο Πινάκων

Ευρετήριο Σχημάτων

1. Εισαγωγή

Τα τελευταία χρόνια με την εξέλιξη της τεχνολογίας και τη μετάβαση στην «Εποχή της Πληροφορίας», η πληροφορική έχει παρεισφρήσει σε όλες τις διαστάσεις της σημερινής κοινωνίας. Η παρείσφρηση αυτή έχει οδηγήσει στην ολοένα και μεγαλύτερη ανάπτυξη πληροφοριακών και δικτυακών συστημάτων υποδομών. Τα συστήματα αυτά διαχειρίζονται ποσά πληροφορίας ανάλογα του μεγέθους και του σκοπού τους.

Σε αυτό το σημείο, εισέρχεται η έννοια της Ασφάλειας. Η εξέλιξη της τεχνολογίας έδωσε τα τεχνολογικά εργαλεία και δημιούργησε τις κατάλληλες συνθήκες ώστε να υπάρξει μία σειρά επιθέσεων στα εν λόγω πληροφοριακά συστήματα. Οι επιθέσεις αυτές συνήθως αφορούν προσπάθειες υποκλοπής, τροποποίησης, αλλοίωσης πληροφοριών, μη εξουσιοδοτημένης πρόσβασης σε υπολογιστικούς πόρους, και άρνησης παροχής υπηρεσιών.

Γίνεται έτσι ιδιαίτερα σημαντική η έννοια της προστασίας των πληροφοριακών συστημάτων από τέτοιου είδους επιθέσεις. Είναι γνωστό ότι κανένας δεν μπορεί να επιτύχει πλήρη ασφάλεια σε ένα σύστημα. Το γεγονός αυτό έχει οδηγήσει τους επιστήμονες αυτής της γνωστικής περιοχής στη δημιουργία ενός νέου μέτρου ασφάλειας, τον έλεγχο διείσδυσης (penetration testing). Με τον όρο έλεγχος διείσδυσης εννοούμε μία δυναμική και εξουσιοδοτημένη προσπάθεια αξιολόγησης της ασφάλειας ενός πληροφοριακού συστήματος προσπαθώντας να εκμεταλλευτούμε τα τρωτά σημεία του συστήματος συμπεριλαμβανομένων των λειτουργικών του συστημάτων, των υπηρεσιών, των ενδεχομένων ατελειών στις ρυθμίσεις, ακόμα και μίας επικίνδυνης συμπεριφοράς του τελικού χρήστη.

Πιο συγκεκριμένα, οι έλεγχοι διείσδυσης πραγματοποιούνται συνήθως χρησιμοποιώντας χειροκίνητες η αυτοματοποιημένες τεχνολογίες ώστε να θέσουν σε κίνδυνο διακομιστές, τελικά τερματικά συστήματα, εφαρμογές δικτύου, δικτυακές υποδομές, κινητές συσκευές και άλλα πιθανά σημεία έκθεσης. Οι πληροφορίες που προκύπτουν από τους ελέγχους που πραγματοποιήθηκαν σχετικά με τρωτότητες που έγιναν αντικείμενο εκμετάλλευσης, συλλέγονται, ταξινομούνται και παρουσιάζονται στον υπεύθυνο ή στο υπεύθυνο τμήμα του οργανισμού. Έτσι, δημιουργούνται σημαντικά στρατηγικά συμπεράσματα και λίστες με τις ενέργειες αποκατάστασης των τρωτοτήτων.

1.1 Αντικείμενο πτυχιακής εργασίας

Η παρούσα πτυχιακή εργασία ασχολείται με την παρουσίαση και ανάλυση των δημοφιλέστερων μεθοδολογιών ελέγχου διείσδυσης, τη σύγκριση τους πάνω σε συγκεκριμένους άξονες, και την πρόταση μίας συνδυαστικής ενοποιημένης μεθοδολογίας. Επιπλέον, παρουσιάζονται και περιγράφονται τα τεχνολογικά εργαλεία που απαιτούνται για έναν επιτυχημένο έλεγχο. Ειδικότερα, για το τεχνολογικό εργαλείο Nessus παρουσιάζεται ένας Java parser που αναλαμβάνει την ανάγνωση αρχείων csv με τα αποτελέσματα από σάρωση του εργαλείου Nessus και την απόδοση τους σε αρχεία κειμένου docx. Τέλος, προτείνεται ένα πρότυπο αναφοράς και παρουσιάζεται ένα παράδειγμα μετά από τη διενέργεια ελέγχου σε εργαστηριακές συνθήκες.

Πιο αναλυτικά, περιγράφονται αναλυτικά οι μεθοδολογίες ISSAF, NIST, OSSTMM, PTES και PTF και παρουσιάζονται οι φάσεις της κάθε μεθόδου, οι τεχνικές, η προσέγγιση που η κάθε μεθοδολογία ακολουθεί και οι ιδιαιτερότητες τους [PTES, 2014] . Στη συνέχεια, οι μεθοδολογίες συγκρίνονται βάση πέντε (5) κριτηρίων: «Χαρακτήρας της μεθοδολογίας», «Φάσεις της μεθοδολογίας», «Γνωσιακό Επίπεδο», «Τεχνολογικός ή Θεωρητικός Χαρακτήρας» και «Ιδιαίτερα χαρακτηριστικά». Η σύγκριση αυτή οδηγεί σε χρήσιμα πορίσματα. Κατόπιν, παρουσιάζεται η προτεινόμενη μεθοδολογία με την αναλυτική περιγραφή της κάθε φάσης της. Οι φάσεις που αναλύονται είναι: «Σχεδιασμός – Προετοιμασία», «Συλλογή Πληροφοριών», «Αναγνώριση Τρωτοτήτων», «Εκμετάλλευση», «Διατήρηση Πρόσβασης» και «Δημιουργία Αναφοράς». Παραθέτονται επίσης όλες οι εξελίξεις στον κλάδο τον τελευταίο καιρό, αναφέροντας σημαντικές εργασίες στην ενότητα Σχετική Έρευνα. Επιπροσθέτως, η εργασία περιγράφει αναλυτικά μία σειρά τεχνολογικών εργαλείων συνοδευτικών της μεθοδολογίας κατά τη διενέργεια του ελέγχου διείσδυσης ανά φάση. Τέλος, αναφέρεται το πρότυπο αναφοράς και παρουσιάζεται εκτενώς μέσα από παράδειγμα εκτέλεσης ελέγχου σε εργαστηριακό περιβάλλον.

1.2 Αφορμή για την έρευνα

Καθώς η πληροφορική έχει παρεισφρήσει στις περισσότερες πτυχές της σημερινής κοινωνίας, η πλειοψηφία των οργανισμών και των εταιρειών χρησιμοποιούν πληροφοριακά συστήματα και δικτυακές υποδομές για την υποστήριξη των λειτουργιών τους. Μία επίθεση σε αυτές τις υποδομές μπορεί να έχει καταστροφικά αποτελέσματα όχι μόνο στον οργανισμό αλλά και στο χρήστη/πελάτη/καταναλωτή/συνεργάτη που εμπλέκεται στις διαδικασίες και στις υπηρεσίες που παρέχει ο οργανισμός. Επιπλέον, κάθε μέρα προστίθενται επιπλέον τρωτότητες σε ένα ήδη μακρύ κατάλογο και καθώς η τεχνολογία αναπτύσσεται και η γνώση σήμερα είναι πιο ανοιχτή από ποτέ, οι επιτιθέμενοι και οι ειδικοί της Ασφάλειας βρίσκονται σε ένα διαρκές παιχνίδι «ποντικού και γάτας».

Όσον αφορά στο τομέα του ελέγχου διείσδυσης, η διενέργεια των ελέγχων τείνει να γίνεται εμπειρικά και όχι βάσει κάποιας μεθοδολογίας. Επιπλέον, έκπληξη παρουσιάζει το γεγονός ότι στην πράξη κάποιες φάσεις του ελέγχου εκλείπουν ή ακόμα χειρότερα πραγματοποιείται μόνο η φάση της Αναγνώριση Τρωτοτήτων. Είναι ανάγκη λοιπόν

για έρευνα γύρω από τις μεθοδολογίες που υπάρχουν και της προσπάθειας ενοποίησης τους σε μία μεθοδολογία κατανοητή, αναλυτική και όσο το δυνατόν πιο συμβατή στις ανάγκες ενός ελεγκτή. Το ίδιο φαινόμενο παρουσιάζεται και στο πεδίο των τεχνολογικών εργαλείων. Παρατηρείται η ύπαρξη μίας πληθώρας εργαλείων για τη διενέργεια ελέγχου διείσδυσης. Αυτό δημιουργεί σύγχυση καθώς ένας (άπειρος ή μέτριας εμπειρίας) ελεγκτής «χάνεται» μέσα σε μία αμέτρητη λίστα εργαλείων, χωρίς να αναγνωρίζει ποια εργαλεία είναι αποτελεσματικά ή ποια εργαλεία θα τον βοηθήσουν στη διενέργεια των επόμενων φάσεων. Τέλος, είναι σημαντικό για έναν οργανισμό η εικόνα του ελέγχου διείσδυσης να αποτυπωθεί σε μία αναφορά η οποία θα είναι κατανοητή από τη διοίκηση και όχι μόνο από ανθρώπους του χώρου της Πληροφορικής, οι τρωτότητες να συνοδεύονται από επιπτώσεις και οι επιπτώσεις από κόστος. Το κόστος είναι μία έννοια που κάθε διοίκηση αναγνωρίζει.

2. Θεωρία Ελέγχου Διείσδυσης

2.1 Περιγραφή των διαθέσιμων πλαισίων

2.1.1 NIST

Η μεθοδολογία NIST [NIST, 2008] όπως διασαφηνίζεται στις πρώτες σελίδες του εγχειριδίου της, αποτελεί μια μεθοδολογία αξιολόγησης και εκτίμησης κινδύνου (risk assessment), ελέγχου διείσδυσης και άμβλυνσης των συνεπειών από επιθέσεις. Επομένως, η μεθοδολογία σχετικά με τον έλεγχο διείσδυσης είναι υποσύνολο της συνολικής μεθόδου NIST και η ίδια κρατάει αποστάσεις από το να χαρακτηριστεί ως αμιγώς μεθοδολογία ελέγχου διείσδυσης. Πιο συγκεκριμένα, η οπτική της μεθοδολογίας NIST είναι αφαιρετική. Λείπουν οι τεχνικές ιδιαιτερότητες και οι αναφορές σε συγκεκριμένα εργαλεία ή προτιμήσεις αυτών. Το χαρακτηριστικό αυτό, προσφέρει μεγάλη ευελιξία στον ελεγκτή (ή αξιολογητή) που θα τη χρησιμοποιήσει. Σύμφωνα με το εγχειρίδιο της, δεν υπάρχει εργαλείο που ταιριάζει απόλυτα σε έναν οργανισμό ή σε κάποιο είδος ελέγχου. Από την άλλη μεριά, αυτό το χαρακτηριστικό θα πρέπει να αποτρέψει ελεγκτές με λίγη εμπειρία από το να τη χρησιμοποιήσουν. Το πεδίο δράσης της μεθοδολογίας βρίσκεται σε επίπεδο οργανισμού παρά σε επίπεδο χρήστη. Επομένως, η χρήση της μεθοδολογίας NIST ενδείκνυται για (μεγάλους) οργανισμούς.

Αρχικά, η μεθοδολογία ορίζει τέσσερις βασικούς πυλώνες. Αυτοί είναι:

- **Δημιουργία πολιτικής** (Policy establishment)
- **Επαναληψιμότητα και τεκμηρίωση** (Implementation of a repeatable and documented methodology)
- **Καθορισμός των στόχων** (Determination of the objectives)
- **Ανάλυση των ευρημάτων** (Analysis of findings)

Η διαμόρφωση αυτών των πυλώνων αποτελεί βασικό βήμα για οποιαδήποτε υλοποίηση της μεθόδου. Μετά τη διαμόρφωση αυτών των πυλώνων, η μεθοδολογία ορίζει τις φάσεις της. Αυτές είναι οι:

- **Σχεδιασμός** (Planning)
- **Ανεύρεση** (Discovery)

- **Επίθεση** (Attack)
- **Δημιουργία Αναφοράς** (Reporting)

Από τον ορισμό των φάσεων και τον αριθμό τους διαφαίνεται ο αφαιρετικός χαρακτήρας αλλά και η ενσωμάτωση άλλων φάσεων σε μία, όπως έχει προαναφερθεί. Παρακάτω, ακολουθεί η ανάλυση των φάσεων της μεθόδου.

2.1.1.1 Μεθοδολογία Αξιολόγησης Ασφάλειας

Η μεθοδολογία αξιολόγησης της Ασφάλειας NIST δεν είναι συγκεκριμένη. Η μεθοδολογία αναφέρει τα πλεονεκτήματα που μπορούν να προκύψουν για έναν οργανισμό αν ακολουθηθούν κάποιες συγκεκριμένες κατευθυντήριες γραμμές. Μεταξύ των οδηγιών που δίνονται είναι η διατήρηση της **συνέπειας** και η διαμόρφωση **δομής.** Η διατήρηση των δύο προσφέρει την ικανότητα στον οργανισμό που χρησιμοποιεί μία τέτοια μεθοδολογία να επαναχρησιμοποιήσει πόρους που έχει χρησιμοποιήσει στο παρελθόν. Το γεγονός αυτό εξυπηρετεί τη μείωση του κόστους χρήματος αλλά και του χρόνου [NIST, 2008].

Οι φάσεις της μεθόδου αξιολόγησης της ασφάλειας πρέπει να είναι διακριτές μεταξύ τους και να εμπεριέχουν τα εξής βήματα: Σχεδιασμός **(Planning)**, Εκτέλεση **(Execution)**, Ενέργειες μετά την Εκτέλεση **(Post-Execution Actions)**. Πέρα από αυτά τα βήματα, τα αποτελέσματα των ελέγχων και οι αξιολογήσεις πρέπει να είναι αρκετές σε αριθμό, ώστε να συγκριθούν μεταξύ τους για την καλύτερη εξαγωγή συμπερασμάτων.

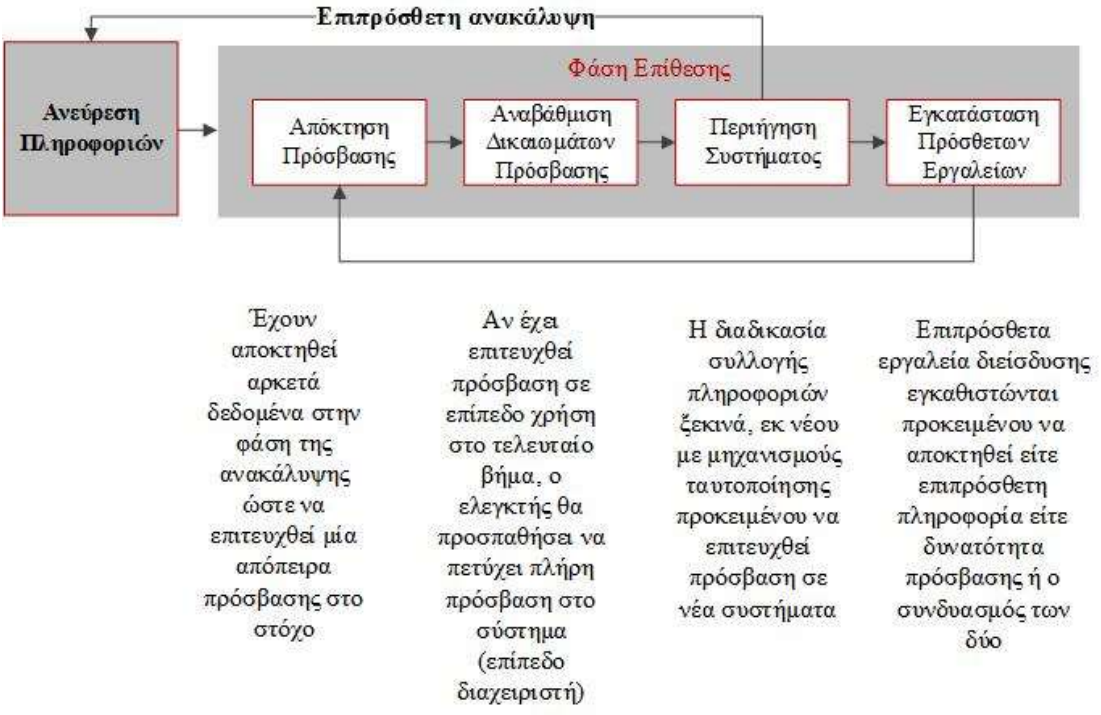
Η μεθοδολογία NIST χρησιμοποιεί συγκεκριμένες τεχνικές αξιολόγησης. Σε αυτή την ενότητα, αναλύονται αυτές οι τεχνικές. Αρχικά, η μεθοδολογία χρησιμοποιεί **Τεχνικές Αναθεώρησης** (Review techniques). Αυτές, χρησιμοποιούνται για να αξιολογηθούν συστήματα, εφαρμογές, δίκτυα, πολιτικές διαδικασίες και να ανακαλύψουν τρωτά σημεία. Πέρα από τις Τεχνικές Αναθεώρησης, χρησιμοποιούνται **Τεχνικές Αναγνώρισης και Ανάλυσης Στόχων** (Target Identification and Analysis Techniques). Τέλος, χρησιμοποιούνται **Τεχνικές Επαλήθευσης και Επικύρωσης Τρωτοτήτων** (Target Vulnerability Validation Techniques). Για τη NIST, υπάρχει διάκριση των τεχνικών των ελέγχων. Ο έλεγχος μπορεί να διακριθεί σε **εσωτερικό ή**

εξωτερικό. Πιο πρακτικά, η οπτική αυτή διακρίνει τις επιθέσεις οι οποίες λαμβάνουν χώρα εκτός της περιμέτρου του συστήματος του οργανισμού με εκείνες που λαμβάνουν χώρα εντός της περιμέτρου (insider attack).

Επίσης, οι επιθέσεις διακρίνονται σε επιθέσεις **λευκού κουτιού** και **μαύρου κουτιού** (overt and covert attacks). Επιθέσεις λευκού κουτιού ονομάζονται εκείνες κατά τις οποίες ο ελεγκτής διεξάγει τον έλεγχο στο σύστημα, με τις προδιαγραφές και τις τεχνικές λεπτομέρειες να είναι γνωστές εξαρχής σε αυτόν. Επιθέσεις μαύρου κουτιού ονομάζονται εκείνες οι επιθέσεις σε σύστημα του οποίου οι λεπτομέρειες δεν είναι γνωστές και ο ελεγκτής πρέπει να μαζέψει πληροφορίες για αυτό χωρίς καμία βοήθεια.

2.1.1.2 Μεθοδολογία Ελέγχου Διείσδυσης

Ο έλεγχος διείσδυσης για τη μεθοδολογία είναι ένα βήμα της επιβεβαίωσης τρωτοτήτων. Στη φάση αυτή, η μεθοδολογία ορίζει τέσσερις εσωτερικές υπο-φάσεις. Όπως έχει προαναφερθεί, οι φάσεις είναι:



Σχήμα 1. Οι φάσεις της μεθοδολογίας.

Planning (Σχεδιασμός): Στη φάση αυτή γίνεται η ανεύρεση των ονομάτων διακομιστών, διευθύνσεων IP, ανεύρεση DNS διακομιστών, κάνοντας χρήση

διάφορων εργαλείων. Η φάση του Σχεδιασμού είναι επίσης υπεύθυνη για την απόκτηση πληροφοριών σχετικές με τους υπάλληλους του οργανισμού, την εύρεση πληροφοριών του συστήματος και των εφαρμογών που αυτό χρησιμοποιεί, όπως είναι τα ονόματα των εφαρμογών και οι εκδόσεις αυτών.

- **Discovery (Ανεύρεση Πληροφοριών)**, στη φάση αυτή ανακαλύπτονται τρωτότητες, ικανές να πλήξουν το σύστημα κατά την εκμετάλλευση τους στην επόμενη φάση. Η ανεύρεση γίνεται μέσα από σάρωση των θυρών, των υπηρεσιών και αντιστοίχιση τους σε βάσεις δεδομένων τρωτοτήτων (vulnerability databases).
- **Attack (Επίθεση)**, αποτελεί τον πυρήνα του ελέγχου διείσδυσης. Η Επίθεση πραγματοποιείται τμηματικά σε στάδια, τα οποία είναι : **Απόκτηση Πρόσβασης** (Gaining Access), **Αναβάθμιση Δικαιωμάτων Πρόσβασης** (Escalating Privileges), **Περιήγηση Συστήματος** (System Browsing) και **Εγκατάσταση Πρόσθετων Εργαλείων** (Install Additional Tools). Στο στάδιο Περιήγηση Συστήματος, υπάρχει η πιθανότητα ο ελεγκτής να αποκτήσει πληροφορίες τέτοιες που θα τον οδηγήσουν στο προηγούμενο βήμα, εκείνο της Ανεύρεσης Πληροφοριών. Οι φάσεις με τα βήματα και τις συνδέσεις αυτών φαίνονται στον πίνακα. Στις παρακάτω κατηγορίες ανήκουν οι τρωτότητες, όπου η φάση της επίθεσης συμβαίνει λόγω ελλιπούς προστασίας: misconfigurations, kernel flaws, buffer overflows, insufficient input validation, symbolic links, file descriptor attacks , race conditions , incorrect file and directory permissions.
- **Reporting (Δημιουργία Αναφοράς)**, αποτελεί την φάση εκείνη κατά την οποία δημιουργείται η αναφορά προς παράδοση. Πρακτικά πραγματοποιείται παράλληλα με τις τρεις προηγούμενες φάσεις. Σε όλες τις φάσεις χρησιμοποιούνται αρχεία καταγραφών και περιοδικών αναφορών που τελικά συμπεριλαμβάνονται στη τελική παραδοτέα αναφορά.

2.1.1.3 Εκτέλεση και Τεχνικές Αξιολόγησης

Όπως προαναφέρθηκε, η μεθοδολογία ορίζει **Τεχνικές Αναθεώρησης** (review techniques). Σύμφωνα με αυτές, θα πρέπει να εξετάζονται όλα τα έγγραφα ώστε να εξασφαλίζεται αν οι πολιτικές και οι διαδικασίες είναι σύγχρονες και ολοκληρωμένες. Τα έγγραφα αυτά αφορούν:

- πολιτικές ασφάλειας
- αρχιτεκτονικές
- απαιτήσεις
- τυποποιημένες διαδικασίες λειτουργίας
- σχέδια ασφαλείας του συστήματος και των συμφωνιών αδειοδότησης
- μνημόνια συνεννόησης και συμφωνίας για τις διασυνδέσεις του συστήματος
- σχέδια για την αντιμετώπιση συμβάντων
- αρχεία καταγραφής (log files), σύμφωνα με τη μεθοδολογία

Τα αρχεία καταγραφής χρησιμοποιούνται στην επικύρωση της σωστής λειτουργίας του συστήματος, δηλαδή αν λειτουργεί σύμφωνα με τις καθιερωμένες πολιτικές. Η επανεξέταση αυτή μπορεί να αποκαλύψει προβλήματα, όπως λανθασμένη διαμόρφωση υπηρεσιών και ελέγχων ασφάλειας, παράνομης πρόσβασης, και προσπάθειες εισβολών. Στο πλαίσιο αυτό κατανοούμε, πως από τις τεχνικές αυτές δεν λείπουν οι κανόνες δικτύου που έχουν οριστεί, δηλαδή οι υπογραφές και τα μοτίβα των router, firewall, IDS, IPS και η αναθεώρηση της διαμόρφωσης του συστήματος. Με τον όρο αυτό εννοούμε, τη διαδικασία εντοπισμού των αδυναμιών στις ρυθμίσεις ασφάλειας του συστήματος. Πιο συγκεκριμένα, αυτό το είδος ελέγχου θα αποκαλύψει περιττές υπηρεσίες και εφαρμογές, ακατάλληλες ρυθμίσεις λογαριασμών χρήστη και κωδικών πρόσβασης, ακατάλληλες καταγραφές και λανθασμένες ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας.

Ακόμα, η μεθοδολογία αναφέρει τεχνικές ανίχνευσης διαδικτυακής κίνησης για απόκτηση πληροφοριών πάνω σε ασύρματα δίκτυα αλλά και τεχνικές ελέγχων ακεραιότητας αρχείων. Στη συνέχεια, αναφέρονται οι **Τεχνικές Αναγνώρισης και Ανάλυσης Στόχων**, μέσω του Εντοπισμού Δικτύων (Network Discovery) που χρησιμοποιεί μια σειρά από μεθόδους για να ανακαλύψει ενεργούς κεντρικούς υπολογιστές σε ένα δίκτυο, και να εντοπίσει αδυναμίες. Υπάρχουν τόσο παθητικές όσο και ενεργητικές τεχνικές για την ανακάλυψη συσκευών σε ένα δίκτυο. Οι παθητικές τεχνικές:

- παρακολουθούν την κίνηση του δικτύου
- καταγράφουν τις διευθύνσεις IP των ενεργών υπολογιστών,
- αναφέρουν ποιες θύρες είναι σε χρήση

- ανακαλύπτουν τα λειτουργικά συστήματα που είναι εγκατεστημένα σε μηχανήματα στο δίκτυο.

Μπορούν επίσης να προσδιορίσουν τρωτότητες που ενδεχομένως αυτές οι υπηρεσίες παρουσιάζουν.

Στο σημείο αυτό, γίνεται ξεχωριστή αναφορά στη σάρωση ασύρματων δικτύων με παθητικές αλλά και ενεργητικές τεχνικές. Ειδικότερα, γίνονται αναφορές για ασύρματα δίκτυα Bluetooth τεχνολογίας καθώς πολλοί οργανισμοί επιζητούν τη συμμόρφωση με προδιαγραφές ασφάλειας τέτοιου τύπου.

Η επόμενη κατηγορία τεχνικών μετά την ενότητα αναγνώρισης και ανάλυσης στόχων είναι εκείνη των **Τεχνικών Επαλήθευσης και Επικύρωσης Τρωτοτήτων** (Target Vulnerability Validation Techniques), δηλαδή των τεχνικών εκείνων που θα επιβεβαιώσουν ότι μία τρωτότητα υπάρχει αλλά και θα την αποκαλύψουν. Η αποκάλυψη ύπαρξης μίας τρωτότητας γίνεται μέσω προσπάθειας εκμετάλλευσης της (exploitation of vulnerability). Για το λόγο αυτό, η φάση αυτή θεωρείται και η πιο επικίνδυνη, καθώς αυτές οι τεχνικές μπορούν να προκαλέσουν επίπτωση στον οργανισμό πολύ μεγαλύτερη από κάθε άλλο βήμα. Σε αυτή τη φάση της επιβεβαίωσης των τρωτοτήτων, πραγματοποιείται ο έλεγχος διείσδυσης στο σύστημα, όπως εκείνος περιγράφεται στην ενότητα Μεθοδολογία Ελέγχου Διείσδυσης.

2.1.2 ISAAF

Η μεθοδολογία ISSAF [ISSAF, 2006] αποτελεί μία μεθοδολογία ελέγχου διείσδυσης η οποία εστιάζει στο δίκτυο (τοπολογία), το σύστημα και τις εφαρμογές αυτού. Αυτή τη στιγμή η μεθοδολογία βρίσκεται στην έκδοση 0.2.1b. Είναι φανερό από την έκδοση της μεθοδολογίας ότι βρίσκεται σε πρώιμη φάση. Ο χαρακτήρας της είναι ιδιαίτερα τεχνικός και λεπτομερής παρά θεωρητικός. Αυτό αποτελεί τόσο δυνατό όσο και αδύνατο σημείο της μεθόδου. Τεχνικές, εργαλεία και προσεγγίσεις αναλύονται σε μεγάλο βαθμό αλλά ταυτόχρονα δεν γίνεται ιδιαίτερη αναφορά στις φάσεις πριν και μετά τον έλεγχο, οι οποίες είναι εξίσου σημαντικές. Σε κάθε βήμα του ελέγχου, η μεθοδολογία προτείνει τα αντίστοιχα εργαλεία αλλά και τις αντίστοιχες μεθόδους. Η μεθοδολογία ISSAF δεν ασχολείται με τη μετάδοση κάποιας ιδιαίτερης κουλτούρας σχετική με τον έλεγχο διείσδυσης. Η μεθοδολογία απαρτίζεται από τρεις φάσεις (phases): **Σχεδιασμός και Προετοιμασία** (Planning and Preparation) - Phase 1, **Αξιολόγηση** (Assessment) - Phase 2, **Δημιουργία Αναφοράς, Εκκαθάριση και Καταστροφή Αντικειμένων** (Reporting, Clean up and Destroy Artefacts) - Phase 3.

Η Φάση 1 περιγράφεται λιτά και θεωρητικά, η Φάση 2 αναλύεται εκτενώς και επαρκώς και η Φάση 3 αναφέρεται επιγραμματικά. Πέρα από τις τρεις βασικές φάσεις, η μεθοδολογία κάνει αναφορά σε τρία ακόμα σημεία. Τα σημεία αυτά είναι : Ασφάλεια Δικτύου (Network Security), Ασφάλεια Υπολογιστών (Host Security), Ασφάλεια Εφαρμογών (Application Security) και Ασφάλεια Βάσεων Δεδομένων (Database Security).

2.1.2.1 Μεθοδολογία ISSAF - Φάση 1

Η φάση 1 της μεθοδολογίας ISSAF σχετίζεται με το σχεδιασμό και την προετοιμασία που αφορούν στον έλεγχο διείσδυσης και είναι εκείνη που αναλύεται λιγότερο από κάθε άλλη [ISSAF, 2006]. Δυστυχώς, η μεθοδολογία αναφέρει επιγραμματικά τα βασικά σημεία του σχεδιασμού και της προετοιμασίας του ελέγχου όπως είναι το εύρος, οι ημερομηνίες, ο ορισμός της ομάδας ελέγχου, καθώς και το επίπεδο διείσδυσης που θα προσεγγιστεί από την ομάδα. Η μεθοδολογία τονίζει ιδιαίτερα ότι τα δύο μέρη (ελεγκτής και ελεγχόμενος) πρέπει να έρθουν σε συμφωνία πριν τον έλεγχο και ότι αυτή η συμφωνία πρέπει να υπογραφεί για την εξασφάλιση και των δύο ενδιαφερομένων.

2.1.2.2. Μεθοδολογία ISSAF - Φάση 2

Η φάση 2 της μεθοδολογίας ISSAF αφορά στη διενέργεια του ίδιου του ελέγχου διείσδυσης και αναλύεται περισσότερο από κάθε άλλη. Αναφέρονται εκτενώς όλα τα βήματα της φάσης αυτής και παρουσιάζονται εργαλεία, προσεγγίσεις και τακτικές. Μετά την ανάλυση των φάσεων ακολουθεί περαιτέρω ανάλυση των βημάτων σε υπο-βήματα. Η μεθοδολογία τονίζει ιδιαίτερα τις τεχνικές ιδιαιτερότητες που παρουσιάζει αυτή η φάση. Για το λόγο αυτό αφιερώνει ένα πολύ μεγάλο κομμάτι στην επεξήγηση του κάθε βήματος. Πρόκειται για τα εξής βήματα:

- **Συλλογή Πληροφοριών (Information Gathering)**, το οποίο βρίσκεται εντός της φάσης αυτής καθώς άλλες μέθοδοι το τοποθετούν στη φάση της προετοιμασίας. Αναφέρονται οι στόχοι που απαιτείται να ικανοποιηθούν κατά τη φάση, αλλά και ο στόχος της. Η μεθοδολογία διαχωρίζει το βήμα αυτό σε παθητικό (passive) και ενεργητικό (active).
- **Χαρτογράφηση του Δικτύου (Network Mapping)**, δηλαδή η λειτουργία κατά την οποία εντοπίζονται πληροφορίες απαραίτητες για την επίθεση στο σύστημα. Πιο συγκεκριμένα, κατά τη διάρκεια του βήματος αυτού, εντοπίζεται η πιθανή τοπολογία του δικτύου του στόχου. Έπειτα, ανιχνεύονται με ποικίλες τεχνικές οι θύρες, οι υπηρεσίες, τα λειτουργικά συστήματα, και τα firewalls που ενδεχομένως χρησιμοποιούνται. Η επιτυχημένη χαρτογράφηση του δικτύου εγγυάται τα καλά αποτελέσματα της επόμενης φάσης, εκείνης της αναγνώρισης ευπαθειών.
- **Αναγνώριση Τρωτοτήτων (Vulnerability Identification)**, το βήμα αυτό είναι υπεύθυνο για την αναζήτηση τρωτοτήτων στο σύστημα. Στο βήμα αυτό, ο ελεγκτής χρησιμοποιεί όλες τις πληροφορίες που συλλέχθηκαν στα δύο προηγούμενα βήματα. Η ενοποίηση των πληροφοριών οδηγεί σε ένα κατάλογο με τις πιθανές αδυναμίες. Με τον τρόπο αυτό, ο ελεγκτής θα αποφύγει περιπτώσεις λανθασμένων ενδείξεων και την προοπτική μιας «τυφλής» (blind scanning).
- **Επίθεση Διείσδυσης (Penetration)**, η διαδικασία εκείνη κατά την οποία επιχειρείται η απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα. Η μεθοδολογία ορίζει το βήμα αυτό αλλά παράλληλα αναφέρει τον προαιρετικό του χαρακτήρα. Ο ελεγκτής εκτελεί επίθεση διείσδυσης μόνο αν ο οργανισμός-

πελάτης επιθυμεί κάποιου είδους επίδειξη. Ο ελεγκτής θα πραγματοποιήσει την επίθεση εκμεταλλευόμενος μία τρωτότητα όπως αυτή αναδείχθηκε στο προηγούμενο βήμα. Τέλος, θα χρησιμοποιήσει είτε κάποιο εργαλείο από τα αναφερθέντα είτε κάποιο εργαλείο που ο ίδιος θα δημιουργήσει.

- **Απόκτηση Πρόσβασης και Αναβάθμιση Δικαιωμάτων (Gaining Access and Privilege Escalation)**, στο βήμα αυτό αναλύεται η απόκτηση πρόσβασης στο σύστημα μέσω χαμηλής κλίμακας δικαιωμάτων (user) και η μετέπειτα εξέλιξη αυτών σε δικαιώματα διαχειριστή (admin).
- **Κλιμακώνοντας την Επίθεση (Enumerating Further)**, στο βήμα αυτό επεκτείνεται το προηγούμενο βήμα για την απόκτηση περαιτέρω πληροφοριών και πόρων του συστήματος μέσω ανάλυσης κίνησης, απόκτησης κωδικών, απόκτηση cookies, υποκλοπή διευθύνσεων ηλεκτρονικού ταχυδρομείου, αναγνώριση μονοπατιών και δικτύων.
- **«Μολύνοντας» απομακρυσμένους χρήστες/ιστότοπους (Compromising remote users/sites)**, αποτελεί το βήμα εκείνο κατά το οποίο υλοποιείται η έκθεση απομακρυσμένων χρηστών και ιστοσελίδων σε απειλές και η έμμεση απόκτηση πρόσβασης στο στόχο μέσω αυτών.
- **Διατηρώντας την πρόσβαση (Maintaining Access),** αποτελεί το βήμα εκείνο κατά το οποίο πραγματοποιούνται ενέργειες σχετικές με τη διατήρηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα στόχους. Το βήμα αυτό σχετίζεται με την εγκαθίδρυση «κερκοπορτών» (backdoors), την αξιοποίηση και την επιλογή κατάλληλων εργαλείων για την εκμετάλλευση τους.
- **Κάλυψη Ιχνών (Cover the tracks)**, η διαδικασία που είναι υπεύθυνη για την κάλυψη των ιχνών που ενδεχομένως να παραμείνουν μετά τη διείσδυση. Πιο αναλυτικά, στο βήμα αυτό ο ελεγκτής πραγματοποιεί συγκεκριμένες ενέργειες για την απόκρυψη και διαγραφή αρχείων που έχουν προκύψει κατά τα προηγούμενα βήματα. Επιπλέον, ο ελεγκτής προχωρά σε απόκρυψη των τρωτοτήτων που έγιναν αντικείμενο εκμετάλλευσης και των εργαλείων που χρησιμοποιήθηκαν.

Η μεθοδολογία ISSAF διαχωρίζει τα βήματα της δεύτερης φάσης με ένα κοινότυπο τρόπο, αλλά επιτρέπει στον ελεγκτή χωρίς ιδιαίτερη εμπειρία (ή στην ομάδα ελέγχου) να ακολουθήσει μία συγκεκριμένη διαδρομή χωρίς να υποπέσει σε σφάλματα [ISSAF, 2006]. Αυτή η διαδρομή σε συνδυασμό με τα εργαλεία και τις τακτικές που

προτείνονται, εγγυώνται ένα καλό αποτέλεσμα από τον έλεγχο διείσδυσης. Κάποια βήματα αναλύονται σε δυσανάλογα μεγάλο βαθμό σε σχέση με άλλα και αυτό έχει σαν αποτέλεσμα τη δημιουργία απορίων/ερωτημάτων στον αξιολογητή (ελεγκτή) ως προς την εκτέλεση των τελευταίων.

2.1.2.3 Μεθοδολογία ISSAF - Φάση 3

Η φάση 3 της μεθοδολογίας ISSAF αφορά στις ενέργειες εκείνες που ακολουθούν τη Φάση 2 και είναι σχετικές με τη δημιουργία αναφοράς, την απομάκρυνση πληροφοριών που ενδεχομένως να έχουν παραμείνει στα συστήματα/μηχανήματα που δοκιμάστηκαν κατά τον έλεγχο [ISSAF, 2006]. Η Φάση 3, όπως και η Φάση 1 περιγράφεται συνοπτικά και ο βαθμός ανάλυσης της δεν είναι ο επιθυμητός. Ενώ στη Φάση 2, το κάθε βήμα αναλύεται σε υπέρτατο βαθμό και το γεγονός αυτό βοηθά τον ελεγκτή, καθώς ένας άπειρος ελεγκτής θα συναντήσει δυσκολία στη διαχείριση της συγκεκριμένης φάσης.

2.1.2.4 Μεθοδολογία ISSAF - Ασφάλεια Δικτύου, Υπολογιστών, Διαδικτυακών Εφαρμογών και Βάσεων Δεδομένων.

Η μεθοδολογία ISSAF σε αυτό το σημείο αναφέρει διάφορες πτυχές Ασφάλειας [ISSAF, 2006]. Από τις πιο βασικές πτυχές που αναλύονται είναι ο **Έλεγχος Ασφάλειας Κωδικών (Password Security Checking).** Στο σημείο αυτό η μεθοδολογία αναλύει τεχνικές επιλογής σωστών κωδικών, τεχνικές κρυπτογράφησης, τεχνικές κατακερματισμού και παρουσιάζει διάφορα σενάρια επιθέσεων. Τα σενάρια επιθέσεων συνοδεύονται από μία πληθώρα εργαλείων και παραδείγματα αυτών. Ο βασικός χαρακτήρας των σεναρίων είναι εκείνος της αυθεντικοποίησης σε ένα δίκτυο. Επιπλέον, αναφέρονται **διάφορα αντίμετρα** που μπορούν να ληφθούν για την προστασία από τέτοιου είδους επιθέσεις.

Στη συνέχεια, η μεθοδολογία αναφέρει διάφορα στοιχεία σχετικά με την **ασφάλεια** σε επίπεδο **υπολογιστών**. Αναφέρονται τεχνικά χαρακτηριστικά για λειτουργικά συστήματα UNIX και WINDOWS και επεξηγείται μεθοδολογία για την αποκάλυψη διακομιστών, θυρών και υπηρεσιών. Επιπροσθέτως, η μεθοδολογία αναφέρει τρωτότητες των συστημάτων και αντίστοιχες απειλές.

Συμπληρωματικά, η μεθοδολογία αναφέρει διάφορα στοιχεία που αφορούν στην **Ασφάλεια Διαδικτυακών Εφαρμογών**. Ειδικότερα, αναφέρονται οι τρόποι εκείνοι με τους οποίους ένας επιτιθέμενος μπορεί να εκμεταλλευτεί διαδικτυακές εφαρμογές. Για τη μεθοδολογία ISSAF η ασφάλεια διαδικτυακών εφαρμογών επιτυγχάνεται μέσω της συνολικής ασφάλειας σε όλα τα κομμάτια που απαρτίζουν μία τέτοια εφαρμογή. Δυστυχώς, δεν γίνεται κάποια πιο συγκεκριμένη αναφορά [ISSAF, 2006]. Έπειτα, ακολουθεί μεθοδολογία που αφορά επίθεση σε διαδικτυακές εφαρμογές όπως και στα προηγούμενα όπως έγινε και στις προηγούμενες μεθοδολογίες. Η μεθοδολογία ορίζει πως με αυτό τον τρόπο, διάφορες ατέλειες του συστήματος θα φανερωθούν.

Τέλος, αναλύεται η **Ασφάλεια Βάσεων Δεδομένων**. Η μεθοδολογία αναφέρει τα πιο δημοφιλή Συστήματα Βάσεων Δεδομένων. Αυτά είναι τα: Oracle, MS SQL και MySQL. Αρχικά, αναφέρονται εκτενώς τρόποι και εργαλεία με τα οποία μπορεί να επιτευχθεί απομακρυσμένη απαρίθμηση βάσεων δεδομένων. Πέρα από αυτό, η μεθοδολογία συνεχίζει αναλύοντας τεχνικές επιθέσεων brute force. Τέλος, αναλύεται η διαδικασία και η μέθοδος ελέγχου (audit).

2.1.3 OSSTMM

Η μεθοδολογία OSSTMM [OSSTMM, 2008] (Open Source Security Testing Methodology Manual) αποτελεί μεθοδολογία Ασφάλειας Ελέγχου και Αξιολόγησης. Βρίσκεται στην τρίτη έκδοση της και είναι «ανοιχτή» (open-source). Σύμφωνα με τη μεθοδολογία, η πλειοψηφία των ελέγχων που αφορούν στην ασφάλεια, μπορούν να βασιστούν στη μεθοδολογία OSSTMM. Ο σκοπός της μεθοδολογίας είναι να δώσει οδηγίες ώστε:

- να εξασφαλίζεται η συμμόρφωση του ελέγχου με το νόμο
- να ορίζονται οι ευθύνες του αξιολογητή ως προς τον έλεγχο
- να δημιουργείται μία αναφορά της οποίας τα αποτελέσματα και τα πορίσματα είναι ξεκάθαρα και κατανοητά από τον πελάτη
- να παρέχει μία ολοκληρωμένη ανασκόπηση παρά μία σύνοψη του συστήματος
- να παρέχει κατανοητές σε όλους μετρικές

Ο στόχος της μεθοδολογίας δεν είναι να ορίσει κανόνες και πολιτικές για τις μονάδες ενός συστήματος αλλά να ελέγξει κατά πόσο αυτές οι μονάδες λειτουργούν όπως έχει οριστεί κατά τη διαμόρφωση απαιτήσεων. Για το λόγο αυτό, αναφέρονται και ορίζονται οι όροι: επιφάνεια της επίθεσης (attack surface), διάνυσμα επίθεσης (attack vector), τέλεια ασφάλεια (perfect security), έλεγχοι (controls), λειτουργίες (operations), διαπεραστικότητα (porosity), μετρική ραβ (rav), στόχος και τρωτότητα. Η ασφάλεια ορίζεται διαφορετικά, όπως αναλύεται και στη συνέχεια, και είναι μία εφαρμογή απομόνωσης (separation).

2.1.3.1 Μεθοδολογία OSSTMM- Ορισμοί εννοιών

Η μεθοδολογία OSSTMM ορίζει νέες έννοιες καθώς όπως αναφέρεται στο εγχειρίδιο της, είναι μία αναγκαία διαδικασία ώστε η έννοια της Ασφάλειας να γίνει αντιληπτή με διαφορετικό τρόπο. Στον πίνακα 1, ακολουθούν οι ορισμοί των εννοιών με την ερμηνεία τους [OSSTMM, 2008].

Έννοια	Ορισμός
Επιφάνεια Επίθεσης	Η έλλειψη απομόνωσης/διαχωρισμού και λειτουργικών ελέγχων.
Διάνυσμα Επίθεσης	Ένα υπο-πεδίο εφαρμογής που δημιουργήθηκε με σκοπό να προσεγγίσει την ασφάλεια ενός πιο σύνθετου πεδίου. Βασίζεται στον αλγόριθμο διαίρει και βασίλευε.
Μέτρα/Ελεγχοι (Controls)	Έλεγχοι μείωσης των απειλών και των επιπτώσεων. Η βεβαιότητα πως τα αγαθά φυσικής και πληροφοριακής υπόστασης, καθώς και τα ίδια τα κανάλια προστατεύονται από διάφορες επιδράσεις.
Περιορισμοί	Η τρέχουσα κατάσταση των αντιληπτών και γνωστών ορίων για τα κανάλια, τις λειτουργίες και τους ελέγχους που έχουν επαληθευτεί μέσα από τον έλεγχο του συστήματος (audit).
Λειτουργίες	Είναι η έλλειψη ασφάλειας που πρέπει κανείς να έχει για να είναι διαδραστική, χρήσιμη, ανοιχτή, ή διαθέσιμη. Για παράδειγμα, περιορίζοντας το πώς ένα άτομο αγοράζει αγαθά ή υπηρεσίες από ένα κατάστημα σε ένα συγκεκριμένο κανάλι, όπως μια πόρτα για να πάει μέσα και έξω, είναι μια μέθοδος ασφάλειας κατά των λειτουργιών του καταστήματος.
Τέλεια Ασφάλεια	η ακριβής εξισορρόπηση της ασφάλειας και των ελέγχων με τις λειτουργίες και τους περιορισμούς.
Διαπεραστικότητα	Όλα τα διαδραστικά σημεία, οι λειτουργίες, οι οποίες κατηγοριοποιούνται ως ορατότητα (visibility), πρόσβαση (access), ή εμπιστοσύνη (trust).
Ασφάλεια (Safety)	Μια μορφή προστασίας, όπου η απειλή ή τα αποτελέσματά της ελέγχονται. Για να υπάρχει ασφάλεια, οι έλεγχοι πρέπει να είναι σε θέση να εξασφαλίσουν ότι η ίδια η απειλή ή οι συνέπειες της έχουν ελαχιστοποιηθεί σε αποδεκτό επίπεδο από τον ιδιοκτήτη των αγαθών ή το διαχειριστή.
Ασφάλεια (Security)	Μια μορφή προστασίας όπου γίνεται διαχωρισμός μεταξύ των αγαθών και της απειλών. Αυτό περιλαμβάνει αλλά δεν περιορίζεται στην εξάλειψη του αγαθού ή της απειλής. Για να είναι ασφαλές, το αγαθό αφαιρείται από την απειλή ή η απειλή απομακρύνεται από το αγαθό. Αυτό το εγχειρίδιο καλύπτει την ασφάλεια από επιχειρησιακή άποψη, επιβεβαιώνοντας τον έλεγχο των μέτρων ασφάλειας σε ένα λειτουργικό περιβάλλον.

Έννοια	Ορισμός
RAV	Το RAV είναι μία κλίμακα μέτρησης στην επιφάνειας επίθεσης, το ποσό των ανεξέλεγκτων αλληλεπιδράσεων με ένα στόχο, η οποία υπολογίζεται από την ποσοτική ισορροπία μεταξύ της διαπεραστικότητας, των περιορισμών, και των ελέγχων. Σε αυτή την κλίμακα, 100 RAV (επίσης μερικές φορές εμφανίζεται ως 100% RAV) σημαίνει τέλεια ισορροπία και οτιδήποτε λιγότερο σημαίνει ελάχιστοι έλεγχοι και ως εκ τούτου μεγαλύτερη επιφάνεια επίθεσης. Περισσότερα από 100 rav σημαίνει περισσότεροι έλεγχοι από ό,τι είναι απαραίτητο πράγμα που μπορεί να είναι πρόβλημα, καθώς οι έλεγχοι προσθέτουν συχνά αλληλεπιδράσεις μέσα σε ένα πεδίο, καθώς και πολυπλοκότητα.
Vulnerability	Μια ταξινόμηση Περιορισμών όπου ένα άτομο ή διαδικασία μπορεί να έχει πρόσβαση, να αρνηθεί πρόσβαση σε τρίτους, ή να κρύψει αγαθά εντός του πεδίου εφαρμογής.

Πίνακας 1.Οι έννοιες και οι ορισμοί τους σύμφωνα με τη OSSTMM

Μέσω των ορισμών αυτών, η μεθοδολογία αναλύει και εκφράζει τη διαφορετική αντίληψη που έχει για την Ασφάλεια. Εκφράζεται η άποψη της απομόνωσης της απειλής από το αγαθό. Σε ένα σύστημα, υπάρχουν διάφορα σημεία αλληλεπίδρασης, τοποθετημένα έτσι ώστε να προσφέρουν μία υπηρεσία. Η μέθοδος αναφέρεται στο γεγονός αυτό με τον όρο διαπεραστικότητα (porosity). Σε αυτή την περίπτωση, τα αγαθά μπορούν να διαπεραστούν και είναι αναγκαία η ύπαρξη ελέγχων (controls). Με τη χρήση των ελέγχων, ορίζει η OSSTMM, μπορούν να μετριαστούν οι επιπτώσεις από την εκμετάλλευση μίας απειλής.

2.1.3.2 Φάσεις και Μονάδες της ενοποιημένης μεθοδολογίας OSSTMM

Τα χαρακτηριστικά της μεθοδολογίας OSSTMM είναι ιδιαίτερου χαρακτήρα και απαιτούν εμπειρία από το άτομο (ή ομάδα) που θα τη χρησιμοποιήσει. Η μεθοδολογία που προτείνεται αποτελείται από τέσσερις φάσεις. Κάθε φάση έχει τις δικές της μονάδες. Σε αυτή την ενότητα, αναλύονται οι φάσεις, οι μονάδες των φάσεων αλλά και η ενοποιημένη μεθοδολογία αυτών. Κάθε φάση προσδίδει ένα διαφορετικό βάθος στον έλεγχο, αλλά καμία φάση δεν είναι λιγότερο σημαντική από κάποια άλλη. Οι φάσεις είναι οι εξής [OSSTMM, 2008]:

- **Επαγωγική Φάση** (Induction Phase), ο αναλυτής αρχίζει τον έλεγχο κατανοώντας τις απαιτήσεις του ελέγχου, το πεδίο εφαρμογής και τους περιορισμούς στον έλεγχο αυτής της εμβέλειας. Τις περισσότερες φορές, ο τύπος του ελέγχου προσδιορίζεται καλύτερα μετά από αυτή τη φάση.
- **Φάση Αλληλεπιδράσεων** (Interaction Phase), αποτελεί το πυρήνα του ελέγχου για τη μεθοδολογία και απαιτεί την κατανόηση του εύρους του ελέγχου σε σχέση με τις αλληλεπιδράσεις των στόχων και των αγαθών. Στη φάση αυτή συντελείται ο τελικός καθορισμός του εύρους.
- **Ανακριτική Φάση** (Inquest Phase), η φάση αυτή είναι σχετική με τις πληροφορίες που ο αναλυτής αποκαλύπτει. Σε αυτή τη φάση, οι διάφοροι τύποι αξίας ή ζημίας από αστοχία και κακοδιαχείριση πληροφορίων έρχονται στο φως.
- **Φάση Παρεμβάσεων** (Intervention Phase), η φάση αυτή επικεντρώνεται στους πόρους που οι στόχοι χρησιμοποιούν. Οι πόροι αυτοί μπορεί να έχουν αλλάξει, υπερφορτωθεί, πεθάνει και έτσι να προκληθεί αναστάτωση στον οργανισμό. Αυτή είναι συχνά η τελική φάση μιας δοκιμής ασφάλειας.

Κάθε φάση από αυτές που αναλύθηκαν εμπεριέχουν διάφορες μονάδες (modules). Κάθε μονάδα εκτελεί διαφορετικές λειτουργίες. Ακολουθούν οι φάσεις με τις αντίστοιχες μονάδες τους. Η **Επαγωγική Φάση** (Induction Phase) εμπεριέχει τρεις μονάδες.

- **Αξιολόγηση Κουλτούρας** (Posture Review), η αξιολόγηση δηλαδή του πολιτισμού, των αρχών, των κανόνων, των κανονισμών, της νομοθεσίας και τις πολιτικών που εφαρμόζονται στο στόχο.
- **Διοικητική Υποστήριξη** (Logistics), η μέτρηση των περιορισμών αλληλεπίδρασης, όπως η απόσταση, η ταχύτητα και η σφαλερότητα να καθοριστούν τα περιθώρια της ακρίβειας. Η διαδικασία αυτή ελαχιστοποιεί το σφάλμα και να βελτιώνει την αποδοτικότητα.

- **Ενεργός έλεγχος ανίχνευσης** (Active Detection Verification), ο έλεγχος και το εύρος της ανίχνευσης αλληλεπιδράσεων.

Η **Φάση Αλληλεπιδράσεων** (Interaction Phase) εμπεριέχει τέσσερις μονάδες.

- **Ορατότητα Ελέγχου** (Visibility Audit), ο προσδιορισμός των στόχων που πρέπει να ελέγχονται εντός του πεδίου εφαρμογής/εύρους. Ορατότητα θεωρείται ως «παρουσία» και δεν περιορίζεται μόνο στην ανθρώπινη όραση.
- **Έλεγχος Πρόσβασης** (Access Verification), η μέτρηση του εύρους και του βάθους των διαδραστικών σημείων πρόσβασης εντός του στόχου και η απαίτηση ελέγχων ταυτότητας. Το σημείο πρόσβασης είναι το σημείο οποιασδήποτε αλληλεπίδρασης του αγαθού. Ο πλήρης έλεγχος απαιτεί ο ελεγκτής να γνωρίζει όλες τις πληροφορίες για το σημείο πρόσβασης.
- **Επαλήθευση Εμπιστοσύνης** (Trust Verification), ο προσδιορισμός των σχέσεων εμπιστοσύνης από και μεταξύ των στόχων. Μια σχέση εμπιστοσύνης υπάρχει οπουδήποτε ο στόχος αποδέχεται αλληλεπίδραση με άλλους στόχους στο πεδίο εφαρμογής.

- **Επαλήθευση Ελέγχου** (Control Verification), η μέτρηση της χρήσης και της αποτελεσματικότητας των διεργασιών που βασίζονται σε έλεγχούς απώλειας: αποποίηση ευθύνης, απώλεια εμπιστευτικότητας, απώλεια ιδιωτικότητας και ακεραιότητας.

Η **Ανακριτική Φάση** (Inquest Phase) εμπεριέχει έξι μονάδες.

- **Διαδικασίας επαλήθευσης** (Process Verification), ο καθορισμός της ύπαρξης και της αποτελεσματικότητας των αρχείων και η συντήρηση των υφιστάμενων πραγματικών επιπέδων ασφαλείας ή η επιμέλεια που ορίζεται από τη μονάδα αξιολόγησης κουλτούρας.

- **Επαλήθευση Ρύθμισης Παραμέτρων** (Configuration Verification), η έρευνα για τη κανονική λειτουργία των στόχων υπό κανονικές συνθήκες ώστε να καθοριστούν τυχόν προβλήματα.

- **Επικύρωση Περιουσίας** (Property Validation), η μέτρηση του βαθμού χρήσης παράνομων ή χωρίς άδεια αντικειμένων πνευματικής ιδιοκτησίας ή των υπολογιστικών εφαρμογών του στόχου.

- **Αξιολόγηση Διαχωρισμού** (Segregation Review), ο προσδιορισμός των επιπέδων των προσωπικών πληροφοριών, όπως ορίστηκαν στην Αξιολόγηση Κουλτούρας.

- **Επαλήθευση Έκθεσης** (Exposure Verification), η αναζήτηση για ελεύθερα διακινούμενη πληροφορία η οποία περιγράφει την έμμεση προβολή των στόχων ή των αγαθών εντός του πεδίου εφαρμογής.

- **Ανταγωνιστική Αναζήτηση Πληροφοριών** (Competitive Intelligence Scouting), η αναζήτηση για ελεύθερες διαθέσιμες πληροφορίες, άμεσα ή έμμεσα, που θα μπορούσαν να βλάψουν ή να επηρεάσουν δυσμενώς τον ιδιοκτήτη του στόχου.

Τέλος, η **Φάση Παρεμβάσεων** (Intervention Phase) εμπεριέχει τέσσερις μονάδες.

- **Επαλήθευση Καραντίνας** (Quarantine Verification), ο προσδιορισμός και η μέτρηση της αποτελεσματικής χρήσης καραντίνας για κάθε πρόσβαση προς και εντός του στόχου.

- **Έλεγχος Δικαιωμάτων** (Privileges Audit), η χαρτογράφηση και η μέτρηση των επιπτώσεων της κατάχρησης των ελέγχων ταυτοποίησης, των διαπιστευτηρίων, των δικαιωμάτων και της μη εξουσιοδοτημένης κλιμάκωση τους.
- **Επικύρωση Επιβίωσης** (Survivability Validation), ο προσδιορισμός και η μέτρηση της αντοχής του στόχου σε υπερβολικές ή δυσμενείς αλλαγές και η προσαρμοστικότητα των ελέγχων.

- **Αξιολόγηση Προειδοποιήσεων και Καταγραφών** (Alert and Log Review), επανεξέταση των δραστηριοτήτων ελέγχου που διενεργήθηκε με το αληθινό βάθος των δραστηριοτήτων αυτών όπως καταγράφονται από το στόχο ή από τρίτους.

Γίνεται, επομένως, εύκολα αντιληπτό ότι το σύνολο αυτών των μονάδων οδηγούν στη συγκρότηση μίας ενοποιημένης μεθοδολογίας. Η μεθοδολογία αυτή είναι εφαρμόσιμη σε όλους τους τύπους ελέγχων, είτε πρόκειται για πληροφοριακό σύστημα, έναν άνθρωπο, μία διαδικασία, κ.ά.

2.1.3.3 Τομείς Ελέγχου

Η μεθοδολογία OSSTMM, ορίζει τη διενέργεια ελέγχων Ασφάλειας σε διάφορους τομείς. Σε αυτή την ενότητα, περιγράφονται οι τομείς και αναλύονται συνοπτικά οι βασικοί στόχοι του εκάστοτε ελέγχου. Οι τομείς είναι οι :

- **Έλεγχος Ασφάλειας Ανθρώπινου Δυναμικού** (Human Security Testing), είναι μια υποδιαίρεση της PHYSSEC και περιλαμβάνει Ψυχολογικούς Ελέγχους (PSYOPS). Οι δοκιμές σε αυτό το κανάλι απαιτούν την αλληλεπίδραση με τους ανθρώπους που βρίσκονται σε θέσεις φύλακα των αγαθών. Αυτό το κανάλι καλύπτει τη συμμετοχή των ανθρώπων, κατά κύριο λόγο το προσωπικό λειτουργίας. Πολλοί θεωρούν αυτό ως «κοινωνική μηχανική», ο πραγματικός στόχος είναι ο έλεγχος του προσωπικού και η ευαισθητοποίηση του σε θέματα ασφάλειας στο απαιτούμενο επίπεδο ασφάλειας που επισημαίνονται στην πολιτική της εταιρείας, τους κανονισμούς της βιομηχανίας ή της περιφερειακής νομοθεσίας.

- **Έλεγχος Ασφάλειας Φυσικών Εγκαταστάσεων** (Physical Security Testing), είναι μια ταξινόμηση για την ασφάλεια υλικού μέσα από τη φυσική σφαίρα που βρίσκεται στα όρια της ανθρώπινου - διαδραστικού 3D χώρου. Οι δοκιμές αυτές απαιτούν μη επικοινωνιακή αλληλεπίδραση με τα φυσικά εμπόδια και τους ανθρώπους που βρίσκονται σε καίριες θέσεις φύλακα. Ο πραγματικός στόχος των δοκιμών ασφάλειας σε αυτό το κανάλι είναι η φυσική και λογική δοκιμή και μέτρηση στα απαιτούμενα επίπεδα ασφάλειας, όπως περιγράφεται στην πολιτική της εταιρείας, τους κανονισμούς της βιομηχανίας ή της νομοθεσίας.

- **Έλεγχος Ασφάλειας Ασυρμάτων Δικτύων** (Wireless Security Testing), είναι η διαβάθμιση ασφαλείας που περιλαμβάνει την ασφάλεια των ηλεκτρονικών συστημάτων (ELSEC). Ο έλεγχος ELSEC είναι τα μέτρα για την άρνηση μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες που προέρχονται από την παρακολούθηση και την ανάλυση των μη-επικοινωνιακών ηλεκτρομαγνητικών ακτινοβολιών. Ο έλεγχος SIGSEC αφορά τα μέτρα για την προστασία των ασύρματων επικοινωνιών από μη εξουσιοδοτημένη πρόσβαση. Οι δοκιμές σε αυτό το κανάλι απαιτούν την αλληλεπίδραση των εμπόδιων εισόδου με τα αγαθά πάνω από της ηλεκτρομαγνητικές (EM) και συχνότητες μικροκυμάτων (MW).

- **Έλεγχος Ασφάλειας Τηλεπικοινωνιών** (Telecommunications Security Testing), είναι μια ταξινόμηση για την ασφάλεια υλικού εντός του ELSEC σφαίρα η οποία είναι εντός των ορίων των τηλεπικοινωνιών πέρα από το φυσικό επίπεδο (π.χ. καλώδια). Ο πραγματικός στόχος των δοκιμών ασφάλειας είναι ο λογικός έλεγχος και η μέτρηση της απόστασης που υπάρχει από το απαιτούμενο επίπεδο ασφάλειας, όπως περιγράφεται στην πολιτική της εταιρείας, τους κανονισμούς της βιομηχανίας ή της νομοθεσίας.

- **Έλεγχος Ασφάλειας Δικτύων Δεδομένων** (Data Networks Security Testing), αυτός ο έλεγχος καλύπτει τη συμμετοχή των συστημάτων πληροφορικής, κυρίως τα δίκτυα λειτουργίας εντός του πεδίου στόχου. Ο πραγματικός στόχος των δοκιμών ασφάλειας είναι η αλληλεπίδραση του συστήματος με τον έλεγχο λειτουργίας της ποιότητας και οι μετρήσεις της απόστασης που υπάρχει με το απαιτούμενο πρότυπο ασφαλείας έτσι όπως περιγράφονται στην πολιτική της εταιρείας, τους κανονισμούς της βιομηχανίας ή της νομοθεσίας.

2.1.4 PTF

Η μεθοδολογία PTF [PTF, 2014] παίρνει το όνομα της από τα αρχικά του Penetration Testing Framework. Αυτή τη στιγμή βρίσκεται στην έκδοση 0.59. Η μεθοδολογία βρίσκεται σε δοκιμαστική φάση (beta). Αυτό φαίνεται τυπικά, τόσο από την έκδοση της αλλά και ουσιαστικά από τις φάσεις, τα βήματα και τα χαρακτηριστικά της. Η μεθοδολογία PTF δεν αναφέρει καθόλου υπόβαθρο στον αναγνώστη του εγχειριδίου της και κατ' επέκταση στον ελεγκτή (ή αξιολογητή) που θα επιλέξει να την χρησιμοποιήσει. Αυτό δυσχεραίνει τη χρήση της και μειώνει αισθητά τις πιθανότητες να επιλεχθεί ανάμεσα σε άλλες μεθοδολογίες ελέγχου διείσδυσης. Παρόλα αυτά, το τεχνικό κομμάτι της μεθοδολογίας είναι ιδιαίτερα ενδιαφέρον καθώς παρέχει αρκετά εργαλεία, παραδείγματα εντολών, ιστοσελίδες και τακτικές επιθέσεων. Οι φάσεις της μεθοδολογίας PTF είναι εφτά, αν και δεν γίνεται ξεκάθαρο πως διαχωρίζονται τα στάδια της. Δυστυχώς, η μεθοδολογία δεν περιγράφει όλες τις φάσεις σε ικανοποιητικό βαθμό. Αυτό δημιουργεί προβλήματα τόσο στην κατανόηση της μεθόδου όσο και στην πρακτική της εφαρμογή. Οι φάσεις είναι οι εξής:

- **Αποτύπωση Δικτύου** (Network Footprinting)
- **Ανακάλυψη και Ανίχνευση** (Discovery & Probing)
- **Κλιμάκωση Ενεργειών** (Enumeration)
- **Σπάσιμο Κωδικών** (Password Cracking)
- **Ανάλυση Τρωτοτήτων** (Vulnerability Assessment)
- **Φάση Διείσδυσης Ελέγχου** (Penetration)
- **Δημιουργία Τελικής Αναφοράς** (Final Report)

Πέρα από τα στάδια αυτά, η μεθοδολογία κάνει ιδιαίτερη αναφορά στον ειδικότερο έλεγχο των συσκευών Bluetooth, των συσκευών cisco και citrix. Επιπλέον, προτείνονται συγκεκριμένοι έλεγχοι για τους διακομιστές, για τα κανάλια φωνής και ειδικότερα τεχνολογίας VoIP. Τέλος, η μεθοδολογία προτείνει βήματα ελέγχου για φυσική προστασία. Στις επόμενες ενότητες, αναλύονται οι κυριότερες φάσεις της μεθοδολογίας όπως αυτές παρουσιάζονται στο εγχειρίδιο της.

2.1.4.1 Οι φάσεις της μεθοδολογίας PTF

Οι κυριότερες φάσεις της PTF έτσι όπως αναλύονται από τη μεθοδολογία είναι οι: **Αποτύπωση Δικτύου** (Network Footprinting), **Ανακάλυψη και Ανίχνευση** (Discovery & Probing) **Κλιμάκωση Ενεργειών** (Enumeration), **Σπάσιμο Κωδικών** (Password Cracking), **Ανάλυση Τρωτοτήτων** (Vulnerability Assessment) [PTF, 2014].

Στη φάση με όνομα **Αποτύπωση Δικτύου** (Network Footprinting), ο ελεγκτής προσπαθεί να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με το επιλεγμένο δίκτυο. Η αναγνώριση μπορεί να πάρει δύο μορφές, ενεργητική ή παθητική. Η μεθοδολογία ορίζει την παθητική επίθεση ως την καλύτερη επιλογή εκκίνησης. Αυτό περιλαμβάνει συνήθως προσπάθειες ανακάλυψης πληροφοριών διαθέσιμες στο κοινό με τη χρήση web browser και επισκέψεις σε newsgroups κλπ. Μια ενεργητική μορφή είναι πιο ενοχλητική και μπορεί να εμφανιστεί στα αρχεία καταγραφής ελέγχου. Στο σημείο αυτό δίνονται διάφορες ιστοσελίδες που μπορούν να βοηθήσουν αλλά και μία λίστα από εργαλεία. Επίσης, η μεθοδολογία αναφέρει την αναζήτηση στοιχείων μέσω του διαδικτύου, την αναζήτηση για μεταδεδομένα, την επίσκεψη σε κοινωνικά δίκτυα, την απόκτηση πληροφοριών από δημόσιους DNS διακομιστές αλλά και την κοινωνική μηχανική αναπόσπαστα κομμάτια της φάσης αυτής.

Η επόμενη φάση **Ανακάλυψη και Ανίχνευση** (Discovery and Probing) είναι εκείνη που είναι υπεύθυνη για την ανάλυση των πακέτων που λαμβάνονται από τους κεντρικούς υπολογιστές (hosts). Υπάρχουν δύο διαφορετικοί τρόποι για ανίχνευση του λειτουργικού συστήματος, ενεργά ή παθητικά. Η παθητική ανίχνευση του λειτουργικού καθορίζεται απομακρυσμένα χρησιμοποιώντας τα πακέτα που λαμβάνονται μόνο και δεν απαιτεί πακέτα που πρέπει να σταλούν. Η Ενεργή ανίχνευση είναι πολύ «θορυβώδης» και απαιτεί τα πακέτα να αποστέλλονται στον απομακρυσμένο υπολογιστή. Δεν κάνει εντύπωση το γεγονός πως και σε αυτή τη φάση η μεθοδολογία προτείνει μία μεγάλη λίστα από εργαλεία μαζί με ένα σύνολο εντολών και παραδειγμάτων.

Η τρίτη φάση είναι εκείνη της **Κλιμάκωσης Ενεργειών** (Enumeration). Η μεθοδολογία δεν εξηγεί πραγματικά ποιες ενέργειες υπόκεινται σε αυτή τη φάση. Από τα εργαλεία που παραθέτει η μέθοδος εξάγεται το συμπέρασμα πως ενέργειες όπως η

ανίχνευση διακομιστών, η προσπάθεια ανεύρεσης κωδικών με υπόθεση, με επιθέσεις ωμής βίας (brute force attack) αλλά και ποικίλες επιθέσεις στις θύρες σημαντικών υπηρεσιών πρέπει να θεωρούνται κομμάτια αυτής της φάσης.

Στη συνέχεια ακολουθεί η φάση **Σπάσιμο Κωδικών** (Password Cracking). Σε αυτή την ενότητα όπως και στην προηγούμενη, αναφέρεται ένας εκτεταμένος κατάλογος εργαλείων και εντολές για τα εργαλεία αυτά χωρίς όμως τη συνοδεία από κάποιο θεωρητικό υπόβαθρο ή κάποια πιο συγκεκριμένη τεχνική.

Η τελευταία φάση της μεθοδολογίας είναι η **Ανάλυση Τρωτοτήτων** (Vulnerability Assessment). Η φάση αυτή υποδεικνύει τη χρήση σαρωτών τρωτοτήτων σε όλους τους κεντρικούς υπολογιστές που βρέθηκαν κατά τη φάση της Ανίχνευσης και στη συνέχεια πραγματοποιείται έλεγχος για τρωτά σημεία. Το αποτέλεσμα αναλύεται προκειμένου να καθοριστεί εάν υπάρχουν τυχόν αδυναμίες που θα μπορούσαν να αξιοποιηθούν και να αποκτηθεί η πρόσβαση στο στόχο.

2.1.4.2 Δημιουργία Αναφοράς

Η δημιουργία αναφοράς είναι ένα από τα σημεία που η μεθοδολογία περιγράφει σε ικανοποιητικό βαθμό. Σύμφωνα με τις οδηγίες που δίνονται η τελική αναφορά πρέπει να εμπεριέχει τα εξής στοιχεία:

- ημερομηνία ελέγχου
- ονόματα των εμπλεκομένων, δηλαδή τα πλήρη ονόματα ελεγκτή και ομάδας και πληροφορίες επικοινωνίας
- πληροφορίες δικτύου, πληροφορίες σχετικές με τον αριθμό των διακομιστών, τις διευθύνσεις δικτύου, τα λειτουργικά συστήματα που χρησιμοποιούν τα μηχανήματα και άλλες τεχνολογικές λεπτομέρειες
- εύρος του ελέγχου, δηλαδή τα όρια εκείνα που οριοθετήθηκε ο έλεγχος
- ο σκοπός του ελέγχου
- οι τύποι του ελέγχου που έγιναν (π.χ. άσπρο κουτί, μαύρο κουτί)
- θέματα ασφάλειας στο τομέα των εφαρμογών
- θέματα ασφάλειας στο τομέα της φυσικής ασφάλειας
- θέματα ασφάλειας στο τομέα της ασφάλειας του προσωπικού
- θέματα ασφάλειας στο τομέα της γενικότερης ασφάλειας, όπως ορίζει η μεθοδολογία

- τεχνική ανάλυση πολιτικών ασφάλειας, σχετικά με τους κωδικούς, της ενημερώσεις του συστήματος, τα λογισμικά προστασίας ιών, στους διακομιστές διαδικτύου (web servers) και δεδομένων (data servers),
- παραρτήματα, με επεξηγήσεις τεχνικών όρων, με αναφορά των μεθόδων που έχουν χρησιμοποιηθεί και ανάλυση αυτών.

2.1.5 PTES

Η μεθοδολογία PTES [PTES, 2014] αποτελεί όπως αναφέρει το όνομα της, μία μεθοδολογία για ελέγχους διείσδυσης. Το πρότυπο αναπτύσσεται από το 2010 και βρίσκεται σε δοκιμαστική φάση (beta stage) μέχρι και σήμερα. Αυτό δείχνει ότι ακόμα η μέθοδος δεν έχει φτάσει σε μία σταθερή μορφή πόσο μάλλον σε κάποια ωριμότητα. Όπως ενημερώνει ο ιστότοπος του προτύπου, το πρότυπο έχει δεχθεί μέχρι τώρα πάνω από 1800 αναθεωρήσεις και νέα στοιχεία προστίθενται συνέχεια. Οι φάσεις της μεθόδου δεν παρουσιάζουν κάποια ιδιαιτερότητα σε σχέση με άλλες μεθοδολογίες αλλά περιγράφονται σε μεγάλο βαθμό εξαιτίας του μεγάλου αριθμού αναθεωρήσεων και προσθηκών στη μέθοδο. Οι βασικές φάσεις της μεθόδου είναι:

- **Προ-Εμπλοκής Αλληλεπιδράσεις** (Pre-Engagement Interactions)
- **Συλλογή Πληροφοριών** (Intelligence Gathering)
- **Μοντελοποίηση Απειλών** (Threat Modeling)
- **Ανάλυση Τρωτοτήτων** (Vulnerability Analysis)
- **Εκμετάλλευση** (Exploitation)
- **Ενέργειες μετά την Εκμετάλλευση** (Post Exploitation)
- **Δημιουργία Αναφοράς** (Reporting)

Παρακάτω, αναλύονται οι φάσεις με τα υπο-βήματα τους.

2.1.5.1 Οι φάσεις της μεθοδολογίας

Η πρώτη φάση της μεθοδολογίας είναι η φάση με όνομα **προ-εμπλοκής αλληλεπιδράσεις**. Στο βήμα αυτό, ορίζεται το εύρος του ελέγχου, όπως συνήθως. Η PTES δίνει διάφορες οδηγίες για τον ορισμό του εύρους. Επίσης, προτείνονται μετρικές για το χρόνο που απαιτείται για τον εκάστοτε έλεγχο [PTES, 2014]. Η μεθοδολογία παρέχει ερωτηματολόγια για τη φάση αυτή, δίνοντας ένα βασικό κορμό αλλά και την ευελιξία στον αξιολογητή να προσθέσει δικές του επιπλέον ερωτήσεις. Η φάση αυτή είναι υπεύθυνη επίσης για τη διευκρίνιση του εύρους των διευθύνσεων IP και των domain names που θα ελεγχθούν. Επίσης, στη συγκεκριμένη φάση, ιδιαίτερη προσοχή πρέπει να δοθεί στη συνεργασία με τρίτους φορείς (συνεργάτες του οργανισμού). Για αυτό το λόγο, δίνονται διάφορες οδηγίες για τους πιο συχνά συνεργαζόμενους

οργανισμούς. Ενώ, στη φάση αυτή η μεθοδολογία δίνει οδηγίες σχετικά με τις επιθέσεις κοινωνικής μηχανικής (social engineering), αλλά και οδηγίες για την πληρωμή του αξιολογητή από τον πελάτη-οργανισμό. Έτσι, σε αυτό το επίπεδο, η μεθοδολογία επεξηγεί διάφορες πτυχές της επικοινωνίας μεταξύ αξιολογητή και πελάτη. Τέλος, σε αυτήν την φάση η μεθοδολογία καταλήγει με τον ορισμό μερικών κανόνων εμπλοκής. Οι κανόνες αυτοί αφορούν το χρόνο και την τοποθεσία που θα λάβουν χώρα οι έλεγχοι, πληροφορίες που θα χρειαστεί να προσπελαστούν καθώς και νομικές πτυχές.

Η δεύτερη φάση είναι υπεύθυνη για τη **Συλλογή Πληροφοριών.** Συνοπτικά αλλά περιεκτικά διασαφηνίζεται ο στόχος της. Αναφέρεται η χρησιμότητα της και η σύνδεση της με τις επόμενες φάσεις της μεθοδολογίας. Η Συλλογή Πληροφοριών αποσκοπεί στην ανεύρεση πληροφοριών σχετικά με σημεία εισόδου είτε αυτά είναι φυσικά, ηλεκτρονικά ή ανθρώπινα. Η συλλογή μπορεί να γίνει παθητικά (passive gathering), ημι-παθητικά (semi-passive gathering) ή ενεργητικά (active gathering). Για τη μεθοδολογία, ο κατάλογος πληροφοριών που αναζητούνται είναι σχεδόν ανεξάντλητος. Πιο αναλυτικά, οι πληροφορίες που αναζητούνται αφορούν τοποθεσίες και χώρους του οργανισμού και λίστα με τα μέτρα ασφάλειας και τις τοποθεσίες αυτών, του οργανισμού. Πληροφορίες όπως φορολογικά αρχεία, αρχεία ιδιοκτησίας, γεωγραφικές συντεταγμένες θεωρούνται απαραίτητα. Επίσης, η συλλογή αφορά πληροφορίες που αφορούν συνεργάτες, ανταγωνιστές, οικονομικά στοιχεία του οργανισμού, τη γραμμή παραγωγής του, την καθετοποίηση της αγοράς στην οποία δραστηριοποιείται καθώς και πληροφορίες σχετικές με τις συναντήσεις των στελεχών του. Από τη Συλλογή Πληροφοριών δε λείπει η αναζήτηση για ανοιχτές θέσεις εργασίας, η απόκτηση του οργανογράμματος της εταιρείας, τα διάφορα αγαθά και οι τεχνολογίες που χρησιμοποιούνται.

Μετά τη Συλλογή Πληροφοριών, η μεθοδολογία συνεχίζει ορίζοντας τη **Φάση Μοντελοποίηση Απειλών.** Όπως φαίνεται και από το όνομα της φάσης, σε αυτή την ενότητα επιχειρείται να δοθεί ένας τρόπος μοντελοποίησης των απειλών. Το πρότυπο PTES δεν χρησιμοποιεί ένα συγκεκριμένο μοντέλο, αλλά, προϋποθέτει ότι το μοντέλο που χρησιμοποιήθηκε είναι συνεπές όσον αφορά στην παρουσίαση των απειλών, των δυνατοτήτων τους, των χαρακτηριστικών τους, σύμφωνα με τον οργανισμό που εξετάζεται, και την ικανότητα να επαναληφθεί σε μελλοντικές δοκιμές με τα ίδια αποτελέσματα [PTES, 2014]. Το πρότυπο εστιάζει σε δύο βασικά στοιχεία της

παραδοσιακής μοντελοποίησης απειλών τα αγαθά και τον επιτιθέμενο (απειλή). Είναι αξιοπρόσεκτο πως στη φάση αυτή, η πραγματική λειτουργία που επιτελείται είναι η ανάλυση και ο ορισμός των αγαθών με την αξία τους και την πιθανή επίπτωση που θα υποστεί το σύστημα μετά από κάποια απειλή. Οι απειλές κατηγοριοποιούνται σε επιχειρησιακές, ανθρώπινες και διαδικασίας. Τέλος, στο βήμα αυτό, γίνεται προσπάθεια αναγνώρισης της πιθανότητας εμφάνισης της απειλής μέσα από την ανάλυση των εργαλείων που υπάρχουν διαθέσιμα και μοντελοποιείται το κίνητρο που έχει κάποιος να επιτεθεί στο σύστημα.

Στη συνέχεια, η φάση που ακολουθεί εκείνη της Μοντελοποίησης Απειλών, είναι η Φάση της **Ανάλυσης Τρωτοτήτων**. Η Ανάλυση Τρωτοτήτων είναι η διαδικασία της ανακάλυψης αδυναμιών στα συστήματα και τις εφαρμογές που μπορούν να γίνουν αντικείμενα εκμετάλλευσης από έναν εισβολέα. Παρά το γεγονός ότι η διαδικασία που χρησιμοποιείται για να βρεθούν ελαττώματα ποικίλλει και εξαρτάται σε μεγάλο βαθμό από τη συγκεκριμένη μονάδα που εξετάζεται, ορισμένες βασικές αρχές ισχύουν για τη διαδικασία. Κατά τη διεξαγωγή ανάλυση τρωτοτήτων οποιουδήποτε τύπου ο ελεγκτής θα πρέπει να ορίσει σωστά στο πεδίο δοκιμών το εφαρμοστέο βάθος και το εύρος για την επίτευξη των στόχων ή / και τις απαιτήσεις του επιθυμητού αποτελέσματος. Η Ανάλυση Τρωτοτήτων, σύμφωνα με τη μεθοδολογία εκτελείται με τους εξής τρόπους:

- **Αυτοματοποιημένα εργαλεία αναζήτησης τρωτοτήτων**
- **Δικτυακοί Σαρωτές Τρωτοτήτων** (Network Vulnerability Scanners), οι οποίοι χωρίζονται σε σαρωτές θυρών (ports), υπηρεσιών (service), και υποκλοπής πακέτων (banner grabbing).
- **Δικτυακοί Σαρωτές Εφαρμογών** (Web Application Scanners), όπως είναι εργαλεία σάρωσης τρωτοτήτων, λίστες καταλόγου, και επιθέσεις ωμής βίας (brute forcing attack).
- **Δικτυακοί Σαρωτές Ήχου** (Voice Network Scanners), εργαλεία που ψάχνουν τρωτότητες και λανθασμένες ρυθμίσεις στις υποδομές VoIP και στις κλασσικού τύπου υποδομές τηλεφωνικής επικοινωνίας του στόχου.
- **Εργαλεία παθητικού χαρακτήρα** (Passive tools), όπως είναι εργαλεία ανάλυσης μέτα-δεδομένων και εργαλεία ανίχνευσης/ανάλυσης δικτυακής κίνησης.

Το αποτέλεσμα της παραπάνω διαδικασίας και εκτέλεσης των εργαλείων οδηγεί τη φάση της Ανάλυσης Τρωτοτήτων, στην επαλήθευση και επικύρωση των

αποτελεσμάτων. Έτσι, γίνεται προσπάθεια μέσα από λίστες και βάσεις δεδομένων να επαληθευτεί η ύπαρξη της τρωτότητας αλλά και η πιθανότητα εκμετάλλευσης της.

Από τη μεθοδολογία δεν θα μπορούσε να λείπει η φάση της **Εκμετάλλευσης** (Exploitation). Η φάση εκμετάλλευσης ενός ελέγχου διείσδυσης επικεντρώνεται αποκλειστικά και μόνο στην καθιέρωση της πρόσβασης σε ένα σύστημα ή στους πόρους αυτού μέσω της παράκαμψης των περιορισμών ασφαλείας. Η θετική έκβαση αυτής της φάσης εξαρτάται από την αρτιότητα με την οποία εκτελέστηκε η προηγούμενη φάση. Η κύρια εστίαση της φάσης είναι ο εντοπισμός των κύριων σημείων εισόδου και ο εντοπισμός αγαθών υψηλής αξίας και αναλύονται τα εξής στοιχεία:

- **Αντίμετρα (Countermeasures),** τα μέτρα εκείνα συνήθως τεχνολογικού χαρακτήρα που παίρνει κάποιος για να ενισχύσει τους ελέγχους στο σύστημα του. Η ύπαρξη αντιμέτρων είναι ικανή να αποτρέψει μία επιτυχημένη διαδικασία εκμετάλλευσης. Αντίμετρα θεωρούνται τα λογισμικά προστασίας από ιούς, ο συσκοτισμός δεδομένων (obfuscating data), η κρυπτογράφηση δεδομένων και η εισχώρηση σε διεργασίες (process injection).

- **Ανθρώπινος Παράγοντας (Human Factor),** μερικές φορές ο ανθρώπινος παράγοντας είναι ο καλύτερος τρόπος για να επιτεθείς σε ένα οργανισμό.
- **Τείχος Προστασίας διαδικτυακών εφαρμογών (web application firewall),** είναι μορφή λογισμικού που βρίσκεται μέσα σε μία εφαρμογή και την προστατεύει από διαδικτυακές επιθέσεις.
- **Διάφοροι τύποι Εκμετάλλευσης**, όπως είναι οι επιθέσεις υπερχείλισης (buffer overflows), η φυσική προσέγγιση του στόχου, η προσέγγιση του στόχου μέσω δικτύου wifi και άλλες επιθέσεις.

Είναι λογικό ότι μετά την Εκμετάλλευση ακολουθούν ένα σύνολο από ενέργειες. Είναι κατανοητό πως η φάση αυτή ονομάζεται **Ενέργειες μετά την Εκμετάλλευση.** Ο σκοπός της φάσης είναι να προσδιοριστεί η αξία του μηχανήματος σε κίνδυνο και να διατηρηθεί ο έλεγχος του μηχανήματος για μελλοντική χρήση. Οι μέθοδοι που περιγράφονται σε αυτή τη φάση έχουν ως στόχο να βοηθήσουν τον ελεγκτή να προσδιορίσει και να τεκμηριώσει τα ευαίσθητα δεδομένα, να εντοπίσει τις ρυθμίσεις διαμόρφωσης, τα κανάλια επικοινωνίας, και τις σχέσεις με άλλες συσκευές του δικτύου

που μπορούν να χρησιμοποιηθούν για να υπάρχει πρόσβαση στο δίκτυο, καθώς και την εγκατάσταση μία ή περισσότερων μεθόδων πρόσβασης του μηχανήματος.

Τελευταία φάση της μεθοδολογίας αλλά ιδιαίτερα σημαντική είναι εκείνη της **Δημιουργία Αναφοράς** (Reporting). Η Δημιουργία Αναφοράς έχει ως στόχο να καθορίσει τα κριτήρια βάσης για την υποβολή εκθέσεων ελέγχων διείσδυσης. Ενώ ενθαρρύνεται να χρησιμοποιείται η προσαρμοσμένη και επώνυμα μορφή του ελεγκτή, κάποια στοιχεία απαιτούνται μέσα σε μια έκθεση, καθώς και προτείνεται μια δομή για την έκθεση με σκοπό την παροχή αξίας προς τον αναγνώστη. Αρχικά, ορίζεται μία ενότητα με υπόβαθρο για να εξηγήσει στον αναγνώστη κάποιες σημαντικές πληροφορίες. Έπειτα, ακολουθεί μία αναφορά με την αποτελεσματικότητα του ελέγχου και τις ικανότητες των ελεγκτών να επιτύχουν τους συγκεκριμένους στόχους. Στη συνέχεια, παρατίθεται το ρίσκο σε κάποια μετρική. Η μεθοδολογία προτείνει τη δικιά της μετρική και τις αντίστοιχες κλίμακες. Από την αναφορά δε λείπει η ενότητα με τις συστάσεις που γίνονται σε κατανοητή γλώσσα και τις προσπάθειες που πρέπει να γίνουν από εδώ και στο εξής. Μετά από όλες αυτές τις λεπτομέρειες, ο αναγνώστης καταλήγει στο τεχνικό τμήμα της αναφοράς. Εκεί αναφέρονται όλα τα τεχνικά στοιχεία των ελέγχων από κάθε φάση ξεχωριστά και κατηγοριοποιημένα.

2.2 Σύγκριση μεθοδολογιών

Η ενότητα αυτή, αφιερώνεται στη σύγκριση μεθοδολογιών ελέγχου διείσδυσης. Οι μεθοδολογίες που γίνονται αντικείμενο σύγκρισης είναι: η μέθοδος ISSAF (Information Systems Security Assessment Framework), η μεθοδολογία του ινστιτούτου NIST (National Institute of Standards and Technology), η «ανοιχτή» (open-source) μεθοδολογία OSSTMM (Open Source Security Testing Methodology Manual), η μεθοδολογία PTF από τα αρχικά Penetration Testing Framework και τέλος, η μεθοδολογία PTES (Penetration Testing Execution Standard) [OSSTMM, 2008].

Ένα από τα μεγαλύτερα προβλήματα στη σύγκριση μεθοδολογιών είναι ο αριθμός των διαφορετικών προσεγγίσεων και ιδιαίτερων χαρακτηριστικών που εμπεριέχει η κάθε μέθοδος. Το γεγονός αυτό μειώνει τον αριθμό των κριτηρίων σε τέτοιο βαθμό που καθιστά το χαρακτήρα της σύγκρισης ανώφελο. Από την άλλη, η προσπάθεια αύξησης των κριτηρίων σύγκρισης μπορεί να οδηγήσει σε μεγάλο βαθμό εξειδίκευσης, με αποτέλεσμα να δημιουργηθεί πολύ μεγάλος αριθμός κριτηρίων.

Με αφετηρία τη θέση αυτή, η σύγκριση των μεθοδολογιών κινείται στους εξής άξονες:

- **ο γενικός χαρακτήρας της μεθοδολογίας**, το κριτήριο αυτό ουσιαστικά διαχωρίζει τις μεθοδολογίες σε μεθοδολογίες ελέγχου διείσδυσης ή σε μεθοδολογίες αξιολόγησης ασφάλειας που είναι υπερσύνολο των μεθοδολογιών ελέγχου διείσδυσης,
- **οι φάσεις της μεθοδολογίας**, η σύγκριση που αφορά δηλαδή τα διακριτά βήματα της εκάστοτε μεθοδολογίας καθώς υπάρχουν ομοιότητες στις περισσότερες μεθοδολογίες ελέγχου διείσδυσης,
- **το γνωστικό επίπεδο που απαιτείται**, η σύγκριση αυτή διαχωρίζει τις μεθοδολογίες εκείνες που μπορούν να χρησιμοποιηθούν από κάποιο αξιολογητή (ελεγκτή) με χαμηλή ή καθόλου εμπειρία και εκείνες που απευθύνονται σε αξιολογητές με πλούσια εμπειρία,
- **ο τεχνολογικός ή μη χαρακτήρας της μεθοδολογίας**, σύμφωνα με αυτό το κριτήριο διαχωρίζονται οι τεχνολογικές μεθοδολογίες από τις μη-τεχνολογικές,
- **ιδιαίτερα χαρακτηριστικά**, δηλαδή εκείνα τα χαρακτηριστικά που δεν μπορούν να κατηγοριοποιηθούν ή ενσωματωθούν σε κάποιο άλλο κριτήριο.

2.2.1 Κριτήριο 1. Χαρακτήρας της μεθοδολογίας

Κατά κοινή ομολογία, η πλειοψηφία των προαναφερθεισών μεθοδολογιών δεν αποτελούν μόνο μεθόδους ελέγχου διείσδυσης. Πιο συγκεκριμένα στην περίπτωση της **μεθοδολογίας ISSAF**, η μεθοδολογία ελέγχου διείσδυσης είναι ένα μικρό υποσύνολο της συνολικής μεθοδολογίας. Η ίδια η μεθοδολογία αναφέρει ότι είναι μέθοδος αξιολόγησης ασφάλειας. Όσον αφορά στη **μεθοδολογία του ινστιτούτου NIST**, ο έλεγχος διείσδυσης αποτελεί ένα μικρό κομμάτι. Η μεθοδολογία NIST είναι και εκείνη μία μέθοδος αξιολόγησης ασφάλειας. Παράλληλα με το χαρακτήρα των δύο προηγούμενων μεθοδολογιών κινείται η **μεθοδολογία OSSTMM**. Η μεθοδολογία αποτελεί σύμφωνα με το εγχειρίδιο της, μεθοδολογία αξιολόγησης ασφάλειας. Σε αντίθεση με τις προηγούμενες τρεις, **οι PTES και PTF** είναι αμιγώς μεθοδολογίες ελέγχου διείσδυσης. Για την ευκολότερη κατανόηση του χαρακτήρα των μεθοδολογιών, η σύγκριση απεικονίζεται συνοπτικά στον Πίνακα 2.

Μεθοδολογία Αξιολόγησης Ασφάλειας[1]	Μεθοδολογία Ελέγχου Διείσδυσης
ISSAF methodology*	PTES
NIST methodology*	PTF
OSSTMM methodology*	

Πίνακας 2. Μεθοδολογίες ομαδοποιημένες ανά χαρακτήρα.

Ο διαχωρισμός αυτός είναι ιδιαίτερα σημαντικός, καθώς μία μεθοδολογία αξιολόγησης ασφάλειας μπορεί να ανταποκρίνεται καλύτερα στις ανάγκες ενός οργανισμού, που πέρα από έναν έλεγχο διείσδυσης αποσκοπεί στη συμμόρφωση με κανονισμούς και νομοθεσίες ή σε μία ολοκληρωμένη αναφορά σχετικά με τις πολιτικές και τους κανόνες που πρέπει να ακολουθούνται. Από την άλλη, είναι πιθανό μία μεθοδολογία ελέγχου διείσδυσης να είναι πιο κατάλληλη για τις ανάγκες κάποιου άλλου οργανισμού που ενδιαφέρεται μόνο για αυτού του είδους τον έλεγχο. Αυτό δεν πρέπει να κάνει εντύπωση, καθώς τα βήματα ενός ελέγχου διείσδυσης είναι λιγότερα από εκείνα μεθοδολογιών αξιολόγησης ασφάλειας.

[1] Η μεθοδολογία αποτελεί και μεθοδολογία ελέγχου διείσδυσης.

2.2.2 Κριτήριο 2. Φάσεις της μεθοδολογίας

Ίσως το πιο ενδιαφέρον κομμάτι της σύγκρισης των μεθοδολογιών, είναι εκείνο των φάσεων. Αυτό προκύπτει από τον απαραίτητο χαρακτήρα κάποιων βημάτων και τις απαραίτητες ενέργειες του ελέγχου διείσδυσης. Συνοπτικά, ενέργειες όπως σχεδιασμός και προετοιμασία, συλλογή πληροφοριών, ανάλυση τρωτοτήτων και εκμετάλλευση ή επίθεση θεωρούνται απαραίτητες για τη διενέργεια ενός ελέγχου διείσδυσης και δε λείπουν από σχεδόν καμία μεθοδολογία. Σε αντίθεση με το γεγονός αυτό, υπάρχουν αρκετές φάσεις που απουσιάζουν από μεθοδολογίες και εμφανίζονται σε άλλες διαφοροποιημένες στον πυρήνα τους από ονομαστικά παρόμοιες. Από το μοτίβο αυτό, λείπει η μεθοδολογία OSSTMM. Όπως έχει αναφερθεί στην αντίστοιχη ενότητα περιγραφής της, η μεθοδολογία OSSTMM παρουσιάζει μία εντελώς διαφορετική προσέγγιση ασφάλειας και οι φάσεις της είναι κατά κύριο λόγο διαφοροποιημένες των άλλων τεσσάρων μεθοδολογιών [OSSTMM, 2008]. Ο Πίνακας 3 εμπεριέχει τις φάσεις και τις μεθοδολογίες που υλοποιούν την κάθε μία. Για τις ανάγκες της σύγκρισης, θεωρήθηκαν ως βασικές φάσεις οι εξής: Σχεδιασμός ή Προετοιμασία, Συλλογή Πληροφοριών, Χαρτογράφηση, Σπάσιμο Κωδικών, Αναγνώριση Τρωτοτήτων, Μοντελοποίηση Απειλών, Επίθεση η οποία αναφέρεται και ως Εκμετάλλευση ή και Επίθεση Διείσδυσης, Απόκτηση Πρόσβασης ή Αναβάθμιση Δικαιωμάτων, Κλιμάκωση Επίθεσης, Διατήρηση Πρόσβασης, Κάλυψη Ιχνών, Δημιουργία Αναφοράς. Συνοπτικά στον πίνακα, εξάγονται τα εξής πορίσματα:

1. Οι φάσεις Σχεδιασμός-Προετοιμασία, Συλλογή Πληροφοριών, Χαρτογράφηση, Αναγνώριση Τρωτοτήτων, Επίθεση, Απόκτηση Πρόσβασης, Δημιουργία Αναφοράς θεωρούνται βασικές φάσεις ή έστω βήματα για σχεδόν κάθε μεθοδολογία.
2. Η διαδικασία Σπάσιμο Κωδικών έχει ιδιαίτερη σημασία για τη μεθοδολογία PTF και παρουσιάζεται σαν φάση ενώ στις άλλες μεθοδολογίες αναφέρεται σαν βήμα ή καθόλου.
3. Η φάση Μολύνοντας Χρήστες ανήκει μόνο στη μεθοδολογία ISSAF.
4. Η Δημιουργία Αναφοράς είναι το πιο κοινό σημείο των πέντε μεθοδολογιών.

Τα πορίσματα αυτά έχουν ιδιαίτερη σημασία τόσο για τα επόμενα κριτήρια της σύγκρισης και ειδικά για το κριτήριο των ιδιαιτεροτήτων, όσο και για τη συνέχεια της εργασίας.

Φάσεις	ISSAF	NIST	OSSTMM	PTES	PTF
Σχεδιασμός/ Προετοιμασία	☑ ναι	☑ ναι	☐ όχι και δεν αναφέρεται στο εγχειρίδιο	☑ ναι, ως προ-εμπλοκής αλληλεπιδράσεις	☐ όχι
Συλλογή Πληροφοριών	☑ ναι	☑ ναι, με ελάχιστες αλλαγές	~αναφέρεται ως Αξιολόγηση Κουλτούρας και Διοικητική Υποστήριξη	☑ ναι	~αναφέρεται ως Αποτύπωση Δικτύου μόνο ως υποσύνολο
Χαρτογράφηση	☑ ναι	☑ ναι	☐ όχι	~αναφέρεται στο Συλλογή Πληροφοριών	☑ ναι, ως Ανακάλυψη Ανίχνευση
Σπάσιμο Κωδικών	~όχι, υπάρχει ενότητα όμως	~όχι σαν βήμα, αναφέρεται όμως	~όχι σαν βήμα, αναφέρεται όμως	~όχι σαν βήμα, αναφέρεται όμως	☑ ναι
Μοντελοποίηση Απειλών	☐ όχι	☐ όχι	~όχι σαν βήμα, αναφέρεται σε διάφορα σημεία	☑ ναι	☐ όχι
Αναγνώριση Τρωτοτήτων	☑ ναι	~όχι σαν βήμα, αναφέρεται όμως	~όχι σαν βήμα, αναφέρεται σε ένα σημείο	☑ ναι, ως Ανάλυση Τρωτοτήτων	☑ ναι
Επίθεση/ Εκμετάλλευση	☑ ναι	☑ ναι	☐ όχι	☑ ναι	☑ ναι
Απόκτηση Πρόσβασης/ Αναβάθμιση Δικαιωμάτων	☑ ναι	☑ ναι, μαζί με το βήμα Περιήγηση Συσ/τος	~αναφέρεται το βήμα έλεγχος δικαιωμάτων	☑ ναι, ως ενέργειες μετά την Εκμετάλ-λευση	~αναφορές στο Σπάσιμο Κωδικών
Μολύνοντας Χρήστες	☑ ναι	☐ όχι	☐ όχι	☐ όχι	☐ όχι
Κλιμάκωση Επίθεσης	☑ ναι	~όχι σαν βήμα, αναφέρεται όμως	☐ όχι	☑ ναι, ως ενέργειες μετά την Εκμετάλ-λευση	~όχι σαν βήμα, αναφέρεται σε ένα σημείο
Διατήρηση Πρόσβασης	☑ ναι	~αναφέρεται σαν Εγκ/ση εργαλείων	☐ όχι	☑ ναι, ως ενέργειες μετά την Εκμετάλ-λευση	~όχι σαν βήμα, αναφέρεται σε ένα σημείο
Κάλυψη Ιχνών	☑ ναι	~όχι σαν βήμα, αναφέρεται όμως	☐ όχι	☑ ναι, ως ενέργειες μετά την Εκμετάλ-λευση	☐ όχι
Δημιουργία Αναφοράς	☑ ναι	☑ ναι	☑ ναι	☑ ναι	☑ ναι

Πίνακας 3. Συνοπτικός πίνακας σύγκρισης μεθοδολογιών ανά φάση.

2.2.3 Κριτήριο 3. Γνωστικό επίπεδο

Η ενότητα αυτή έχει σαν σκοπό τη σύγκριση των μεθοδολογιών με κριτήριο το γνωστικό επίπεδο που απαιτείται για τη χρήση τους. Πρακτικά, διαχωρίζει τις μεθοδολογίες σε εκείνες που μπορούν να χρησιμοποιηθούν από οποιονδήποτε αξιολογητή (μικρή ή καθόλου εμπειρία) και σε εκείνες που μπορούν να

χρησιμοποιηθούν μόνο από έμπειρους αξιολογητές. Η σύγκριση πραγματοποιήθηκε με γνώμονα τις απαιτήσεις που υπάρχουν από τη μεθοδολογία σε:

1. αριθμό βημάτων, ο μεγάλος αριθμός βημάτων σημαίνει αναλυτικότερη μεθοδολογία, ο μικρός σημαίνει πολυπλοκότερη
2. επεξήγηση βημάτων, δηλαδή ο βαθμός ανάλυσης του κάθε βήματος
3. παρουσίαση και επεξήγηση εργαλείων και τεχνικών, δηλαδή ο βαθμός επεξήγησης και παρουσίασης εργαλείων προς βοήθεια του ελεγκτή
4. αναγνωσιμότητα και κατανόηση μεθοδολογίας, ο βαθμός ευκολίας σύλληψης του νοήματος και ανάγνωσης του εγχειριδίου της μεθοδολογίας, ο αριθμός σελίδων του εγχειριδίου της μεθοδολογίας, η ομοιογένεια έκτασης των φάσεων.

Τα κριτήρια έχουν αξιολογηθεί σε μία κλίμακα πέντε βαθμίδων:

- Πολύ Κακός
- Κακός
- Μέτριος
- Καλός
- Πολύ Καλός

Γνωσιακό επίπεδο	Μεθοδολογίες				
Κριτήρια	**ISSAF**	**NIST**	**OSSTMM**	**PTES**	**PTF**
Αριθμός Βημάτων	Πολύ Καλός	Μέτριος	Πολύ Καλός	Καλός	Καλός
Επεξήγηση Βημάτων	Πολύ Καλή	Μέτρια	Πολύ Κακή	Πολύ Καλή	Κακή
Παρουσίαση - Επεξήγηση Εργαλείων	Πολύ Καλή	Κακή	Πολύ Κακή	Μέτρια	Καλή
Αναγνωσιμότητα και Κατανόηση	Κακή	Πολύ Καλή	Καλή	Καλή	Πολύ Κακή

Πίνακας 4. Μεθοδολογίες ομαδοποιημένες ανά γνωστικό επίπεδο.

Ο Πίνακας 4 παρουσιάζει τις μεθοδολογίες και τις αξιολογήσεις αυτών σε κάθε κριτήριο γνωστικού επιπέδου. Βαθμολογώντας τις μεθοδολογίες για κάθε κριτήριο και

αθροίζοντας τις αξιολογήσεις σε μία συνολική, προκύπτει το συμπέρασμα πως η μεθοδολογία ISSAF είναι η εκείνη που απευθύνεται σε όλους τους αξιολογητές και δεν απαιτεί κάποιο ιδιαίτερο γνωστικό επίπεδο και οι μεθοδολογίες OSSTMM και PTF είναι εκείνες που απευθύνονται σε έμπειρους αξιολογητές και η χρήση τους δεν συνίσταται εύκολα.

2.2.4 Κριτήριο 4. Τεχνολογικός ή Θεωρητικός Χαρακτήρας

Το κριτήριο του τεχνολογικού ή θεωρητικού χαρακτήρα χρησιμοποιείται για να διαχωρίσει τις μεθοδολογίες που περιγράφουν τις διαδικασίες του ελέγχου διείσδυσης. Με το κριτήριο αυτό διαχωρίζονται εκείνες οι μεθοδολογίες που προτείνουν τεχνολογικά εργαλεία και πρακτικές προσεγγίσεις από εκείνες που κάνουν απλή αναφορά των φάσεων σε θεωρητικό επίπεδο.

Οι μεθοδολογίες **θεωρητικού χαρακτήρα** είναι οι:

1. NIST
2. OSSTMM

και οι μεθοδολογίες **τεχνολογικού χαρακτήρα** είναι οι:

1. ISSAF
2. PTES
3. PTF

2.2.5 Κριτήριο 5. Ιδιαίτερα Χαρακτηριστικά

Πριν οποιαδήποτε ανάλυση της σύγκρισης που πραγματοποιείται σε αυτή την ενότητα, είναι σημαντικό να επεξηγηθεί τι περιλαμβάνει ο όρος Ιδιαίτερα Χαρακτηριστικά. Στον όρο αυτό, αποδίδονται όλα εκείνα τα γνωρίσματα μίας μεθοδολογίας που αναφέρονται είτε σε μεγάλη έκταση και η μεθοδολογία κάνει ιδιαίτερη αναφορά σε αυτά, είτε δεν ομοιάζουν με γνωρίσματα άλλης μεθοδολογίας. Αυτά τα χαρακτηριστικά, όπως αναφέρθηκε στην ενότητα που περιγράφει τις μεθοδολογίες, είναι αρκετά και ποικίλα. Για το λόγο αυτό, κρίθηκε απαραίτητη η σύγκριση των μεθοδολογιών με κριτήριο αυτά τα χαρακτηριστικά. Πιο αναλυτικά, παρακάτω ακολουθεί η κάθε μεθοδολογία με τα ιδιαίτερα χαρακτηριστικά της.

ISSAF

1. Χειρισμός ψευδών ενδείξεων, η μεθοδολογία ISSAF αφιερώνει ένα κεφάλαιο σε αυτή την ενότητα βάζοντας ιδιαίτερη βαρύτητα στο πως μπορεί να επηρεαστούν τα αποτελέσματα του ελέγχου από μία κακή διαχείριση,
2. Έλεγχος Ασφάλειας Κωδικών, αναφέρεται και εδώ σε ξεχωριστό κεφάλαιο μαζί με την Κωδικοποίηση (Encryption) και Κατακερματισμό (Hashing),
3. Έλεγχος Ασφάλειας Μεταγωγών (Switches), Δρομολογητών (Routers), Τειχών Προστασίας, αναφέρονται σε αντίστοιχα κεφάλαια πληροφορίες και συμβουλές για τη ρύθμιση ασφάλειας των προαναφερθέντων στοιχείων δικτύου [ISSAF, 2006].

NIST

1. Κοινωνική Μηχανική, γίνεται ιδιαίτερη αναφορά στο εγχειρίδιο της μεθοδολογίας για αυτή τη τεχνική [NIST, 2008].

OSSTMM

1. Έννοιες και Ορισμοί, η μεθοδολογία εισάγει και ορίζει νέες έννοιες σχετικά με την ασφάλεια, τις απειλές, τους ελέγχους, μετρικές,
2. Κανόνες Εμπλοκής, αναλύονται σε ένα ολόκληρο κεφάλαιο οι κανόνες κάτω από τους οποίους θα πραγματοποιηθεί ο έλεγχος, η συμφωνία που θα γίνει από τα δύο μέρη και η σημαντικότητα της για τη διασφάλιση τους.
3. Χειρισμός ψευδών ενδείξεων, αφιερώνεται μεγάλη έκταση και σε αυτό το γνώρισμα όπως στη μεθοδολογία ISSAF,
4. Μετρικές, η μεθοδολογία εισάγει μετρικές. Αυτές ορίζονται και αναλύονται επαρκώς [OSSTMM, 2008].

PTES

1. Κανόνες Εμπλοκής, αποτελεί σημαντικό γνώρισμα για τη μεθοδολογία και αναλύεται σε μεγάλο βαθμό, αναλύοντας το τρόπο με τον οποίο θα οριστούν
2. Συλλογή Πληροφοριών, αναφέρεται σε όλες σχεδόν τις μεθοδολογίες, αλλά η φάση της PTF είναι αναλυτική σε τέτοιο βαθμό που οι φάσεις των άλλων μοιάζουν με συνοπτικές αναφορές [PTF, 2014],

3. Ανάλυση των Επιχειρησιακών Αγαθών και Διαδικασιών, το βήμα αυτό δεν υπάρχει σε κάποια άλλη μεθοδολογία. Η PTF το αναλύει και περιγράφει εκτενώς [PTES, 2014].

PTF

1. Μεγάλη πληθώρα εργαλείων, ιδιαίτερο χαρακτηριστικό της μεθόδου αυτό η περιγραφή και έκθεση εργαλείων για κάθε φάση. Σε ορισμένα σημεία, μάλιστα, μοιάζει με κατάλογο εργαλείων παρά με μεθοδολογία ελέγχου διείσδυσης [PTF, 2014].

2.3 Προτεινόμενη μεθοδολογία

Η ενότητα αυτή έχει σαν σκοπό την παρουσίαση μίας ενοποιημένης μεθοδολογίας ελέγχου διείσδυσης για υποδομές (infrastructure penetration testing methodology). Στο πλαίσιο αυτό γίνεται κατανοητό, πως οι φάσεις της μεθοδολογίας αυτής προκύπτουν από τη μελέτη υφιστάμενων μεθοδολογιών όπως αυτές αναλύθηκαν, περιεγράφηκαν και έγιναν αντικείμενο σύγκρισης στις προηγούμενες ενότητες. Επομένως, μετά από την ανάλυση των μεθοδολογιών ISSAF, NIST, OSSTMM, PTES και PTF, τα χαρακτηριστικά εκείνα που αφορούν τους ελέγχους διείσδυσης υποδομών απομονώθηκαν, μελετήθηκαν και αξιολογήθηκαν. Πιο συγκεκριμένα, τα ουσιώδη χαρακτηριστικά διαχωρίστηκαν από τα επουσιώδη και διατηρήθηκαν για τη διαμόρφωση μίας ενοποιημένης μεθοδολογίας.

Κατά κοινή ομολογία, είναι σημαντικό για μία μεθοδολογία Ελέγχου Διείσδυσης να παρουσιάζει κάποια συγκεκριμένα στοιχεία, να εκτελεί δηλαδή τις ενέργειες εκείνες που διασφαλίζουν τα καλά αποτελέσματα των υπόλοιπων βημάτων και ένα συνολικό αποτέλεσμα που είναι κοντά στην πραγματική εικόνα του οργανισμού. Παρακάτω, ακολουθούν οι φάσεις που θεωρούνται απαραίτητες καθώς και οι πίνακες 1 και 2 με μία σχηματική μορφή της ακολουθίας αυτών.

1. **Σχεδιασμός - Προετοιμασία (Planning - Preparation),** σε αυτή τη φάση εκτελούνται εκείνες οι ενέργειες που αφορούν τον ορισμό της ομάδας, τον ορισμό ρόλων μεταξύ των μελών. Είναι ιδιαίτερα σημαντικό στη φάση αυτή να πραγματοποιηθεί μία συνετή κατανομή ρόλων. Αυτό εξασφαλίζει τη τήρηση των χρονικών ορίων που θα τεθούν στη συνέχεια και αποτρέπει τη σπατάλη πόρων με επαναλαμβανόμενες διεργασίες. Επιπροσθέτως, ορίζονται οι ημερομηνίες ελέγχου και ο συνολικός χρόνος που απαιτείται για τη διενέργεια του ελέγχου διείσδυσης. Επίσης, κατά το Σχεδιασμό και την Προετοιμασία πραγματοποιείται μία σειρά από συναντήσεις με τα ελεγχόμενα μέρη όπου φτάνουν σε συμφωνία γύρω από τους κανόνες εμπλοκής (engagement rules), τους ελέγχους που θα πραγματοποιηθούν και τον ορισμό του πεδίου ελέγχου (scope). Ο ορισμός των παραπάνω επιτυγχάνεται ευκολότερα μέσω της διενέργειας ερωτηματολογίων στα διάφορα μέρη του οργανισμού. Τέλος, στη φάση αυτή οριστικοποιούνται τα εύρη των IP διευθύνσεων και γίνεται ξεκάθαρο το είδος του ελέγχου που θα πραγματοποιηθεί στους τομείς που

εμπλέκονται με συνεργαζόμενες εταιρείες [ISSAF,2014; NIST, 2008; OSSTMM, 2008; PTES, 2014; PTF, 2014].

2. **Ενεργητική και Παθητική Συλλογή Πληροφοριών (Passive and Active Information Gathering),** σε αυτή τη φάση βρίσκονται οι ενέργειες που αποσκοπούν στην εύρεση πληροφοριών σχετικές με το στόχο. Η φάση αυτή διαχωρίζεται σε δύο λειτουργίες, την παθητική και την ενεργητική. Η Παθητική Συλλογή Πληροφοριών, αφορά τη συλλογή πληροφοριών που επιτυγχάνεται χωρίς τη δημιουργία ιχνών και γενικότερα χωρίς να γίνει αντιληπτή η αναζήτηση πληροφοριών από τον οργανισμό. Ειδικότερα, η παθητική συλλογή πληροφοριών αφορά την αναζήτηση σε καταλόγους και ευρετήρια με πληροφορίες σχετικές με τους υπάλληλους του οργανισμού, με τα περιουσιακά στοιχεία αυτού, την εύρεση πληροφοριών από φορολογικά αρχεία, ιστοσελίδων, κοινωνικών δικτύων, ομάδων ενημέρωσης, φυλλάδια και επαγγελματικές κάρτες. Δεν αποτελεί έκπληξη για τη φάση αυτή, η αναζήτηση για επαγγελματικές συναντήσεις των υπαλλήλων, τις τοποθεσίες των γραφείων και διάφορες αγγελίες για δουλειά στον οργανισμό. Από τη παθητική συλλογή πληροφοριών δεν λείπει η ανίχνευση πακέτων δικτύου και η επεξεργασία αυτών για την ανακάλυψη ενεργών συσκευών. Η παθητική συλλογή μπορεί να ανακαλύψει μη κρυπτογραφημένους κωδικούς και ονόματα χρηστών καθώς και τα λειτουργικά συστήματα που χρησιμοποιούνται. Η **Ενεργητική Συλλογή Πληροφοριών** ή και **Χαρτογράφηση Δικτύου** είναι η λειτουργία κατά την οποία συλλέγονται πληροφορίες σχετικές με το στόχο, όπως οι διευθύνσεις κεντρικών υπολογιστών, το λειτουργικό σύστημα που χρησιμοποιούν τα μηχανήματα και τις κρίσιμες υπηρεσίες που τρέχουν στις ανάλογες θύρες. Αυτή η διαδικασία επιτυγχάνεται "ενεργητικά" καθώς γίνεται χρήση εργαλείων που αποστέλλουν πακέτα και θεωρείται "θορυβώδης" έναντι της παθητικής συλλογής. Επίσης, συλλέγονται πληροφορίες για τις διαδικασίες που ακολουθούνται όπως είναι οι φυσικές τοποθεσίες μηχανημάτων, τα φυσικά μέσα προστασίας μέσω τεχνικών κοινωνικής μηχανικής ώστε να πραγματοποιηθεί ανάλυση στην επόμενη φάση[ISSAF, 2006; NIST, 2008; OSSTMM, 2008; PTES, 2014; PTF, 2014].

3. **Αναγνώριση Τρωτοτήτων (Vulnerability Identification),** αφορά την αναζήτηση των τρωτοτήτων του στόχου χρησιμοποιώντας τις πληροφορίες που συλλέχθηκαν στα προηγούμενα βήματα. Αυτές οι τρωτότητες αφορούν είτε τα συστήματα υπολογιστών, είτε εσφαλμένες ρυθμίσεις στις υπηρεσίες που τρέχουν, είτε σε κακό σχεδιασμό ασφάλειας των εφαρμογών που χρησιμοποιούνται. Η αναγνώριση τρωτοτήτων μπορεί να επιτευχθεί με διάφορους τρόπους. Αρχικά, η αναγνώριση μπορεί να επιτευχθεί ενεργητικά, δηλαδή με την άμεση αλληλεπίδραση του ελεγκτή με το στοιχείο υπό έλεγχο. Τα εν λόγω στοιχεία μπορεί να είναι μία στοίβα TCP ή κάποιο άλλο στοιχείο σε ανώτερη ιεραρχία, όπως είναι μία διεπαφή για τον έλεγχο μίας συσκευής. Η δεύτερη μορφή αναγνώρισης είναι η αυτοματοποιημένη. Εργαλεία σάρωσης εμπορίου είτε εργαλεία που δημιουργούνται κατά τη διάρκεια του ελέγχου, αλληλοεπιδρούν με το στόχο λαμβάνοντας τα μηνύματα που θα επιστρέψει και προσδιορίζουν με αυτό το τρόπο τις τρωτότητες που υπάρχουν. Ο τρίτος τρόπος αναγνώρισης πραγματοποιείται μέσω σαρωτών δικτύου ή γενικών σαρωτών (network/general vulnerability scanners). Οι σαρωτές αυτού του τύπου ανιχνεύουν είτε τις θύρες, είτε τις υπηρεσίες που τρέχουν σε αυτές και τα πρωτόκολλα που χρησιμοποιούνται. Με τους τρόπους αυτούς αναγράφονται οι τρόποι απόκτησης (μη εξουσιοδοτημένης) πρόσβασης στο σύστημα και χρησιμοποιούνται στη φάση της Επίθεσης. Κατά τη διάρκεια της φάσης της Αναγνώρισης Τρωτοτήτων, πραγματοποιείται επίσης η ταξινόμηση αυτών βάση της επίπτωσης τους και διαμορφώνονται σενάρια επίθεσης για τη Φάση 5 (Εκμετάλλευση)[ISSAF, 2006; PTES, 2014; PTF, 2014].

4. **Χειροκίνητη Επαλήθευση Τρωτοτήτων (Manual Vulnerability Verification)** , αποτελεί τη φάση που ακολουθεί την Αναγνώριση Τρωτοτήτων και αφορά Τεχνικές Επαλήθευσης και Επικύρωσης αυτών. Είναι κατανοητό πως κατά τη φάση της Αναγνώρισης Τρωτοτήτων διάφορες τρωτότητες μπορεί να εντοπιστούν ή και όχι ανάλογα με τα εργαλεία που χρησιμοποιούνται. Πιο πρακτικά, ένα εργαλείο μπορεί να εντοπίσει μία τρωτότητα ενώ κάποιο άλλο όχι. Αυτές οι εσφαλμένες ενδείξεις ή ασυνέπειες των αποτελεσμάτων δυσχεραίνουν την επόμενη φάση του ελέγχου (Εκμετάλλευση) και για αυτό το λόγο πρέπει να εξαλειφθούν. Στην πραγματικότητα μετά τη φάση αυτή, η διαδικασία επιστρέφει πίσω στη Φάση 3 όπου γίνεται επαναπροσδιορισμός των

τρωτοτήτων και δεν αποκλείεται η διαδικασία αυτή να επαναληφθεί αρκετές φορές μέχρι να φτάσει στη φάση της Εκμετάλλευσης. Η φάση της Χειροκίνητης Επαλήθευσης μοιάζει αρκετά με εκείνη της Εκμετάλλευσης. Πιο συγκεκριμένα, στη φάση αυτή χρησιμοποιούνται παρόμοιες τεχνικές για να επαληθευθεί η ύπαρξη τρωτοτήτων. Επίσης, χρησιμοποιούνται τεχνικές παραβίασης κωδικών πρόσβασης για τον προσδιορισμό αδύναμων κωδικών και των πολιτικών δημιουργίας αυτών. Τέλος, η μεθοδολογία χρησιμοποιεί τεχνικές κοινωνικής μηχανικής για τον προσδιορισμό των τρωτοτήτων. Με αυτό το τρόπο, πραγματοποιείται η επαλήθευση σε επίπεδο διαδικασιών και ανθρώπινου παράγοντα. Στον Πίνακα 2 φαίνεται η ανατροφοδότηση των φάσεων Αναγνώρισης Τρωτοτήτων και Χειροκίνητης Επαλήθευσης[ISSAF, 2006; PTF, 2014].

5. **Εκμετάλλευση (Exploitation),** με την ονομασία αυτή εννοούμε τη διαδικασία απόκτησης μη εξουσιοδοτημένης πρόσβασης στο σύστημα μέσα από την εκμετάλλευση των τρωτοτήτων που βρέθηκαν στο προηγούμενο βήμα. Αυτό επιτυγχάνεται με τη χρήση εργαλείων είτε έτοιμων είτε σχεδιασμένων από την ομάδα ελέγχου τα οποία εκμεταλλεύονται λανθασμένες ρυθμίσεις, αδυναμίες του πυρήνα (kernel) και υπερχειλίσεις μνήμης (stack overflow). Ένας από τους στόχους της Εκμετάλλευσης είναι η τελική επαλήθευση της ύπαρξης των τρωτοτήτων. Όταν μία τρωτότητα γίνει αντικείμενο εκμετάλλευσης, η ύπαρξη της θα σημειωθεί και θα προσδιοριστούν οι τρόποι με τους οποίους οι επιπτώσεις της θα μετριαστούν. Η διαφορά της φάσης αυτής από τη φάση της Χειροκίνητης Επαλήθευσης Τρωτοτήτων διαφέρει στο εξής. Είναι δυνατόν μία τρωτότητα να υπάρχει αλλά να μην επιτρέπει στον ελεγκτή την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο στόχο. Αυτού του είδους τρωτότητες, ενδεχομένως να προσφέρουν περαιτέρω πληροφορίες στον ελεγκτή αλλά δεν κρίνονται ως αξιόλογες και δεν καταγράφονται. Όσον αφορά στην Εκμετάλλευση, στόχο επίσης αποτελεί η εύρεση του "μονοπάτι ενεργειών" που παρουσιάζει την μικρότερη αντίσταση ως προς την απόκτηση πρόσβασης. Το βήμα αυτό, όσο περίεργο και αν φαίνεται μπορεί να θεωρηθεί και προαιρετικό ανάλογα με τη συμφωνία που έχει πραγματοποιηθεί μεταξύ της ομάδας ελέγχου και τον οργανισμό κατά τη φάση του Σχεδιασμού. Αν η φάση της Αναγνώρισης έχει διεξαχθεί σωστά, η Επίθεση του στόχου θεωρείται ένα χτύπημα ακριβείας.

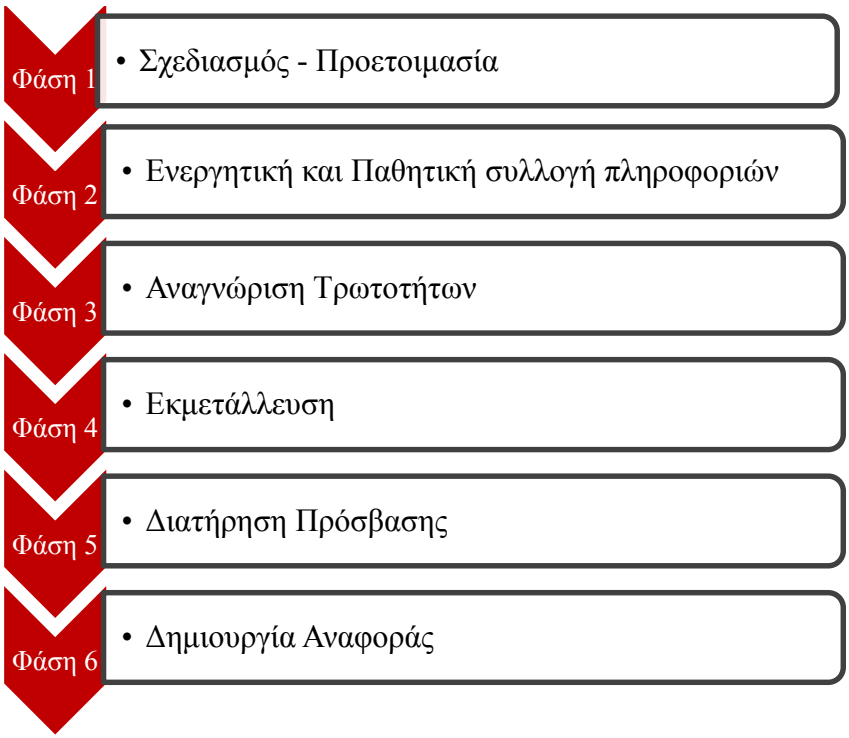
Η φάση της Εκμετάλλευσης είναι εκείνη που θα βοηθήσει στη διαμόρφωση μίας λίστας από μέτρα προστασίας αναγκαίων για τον οργανισμό και θα αναδείξει στην πράξη κακές ρυθμίσεις υφιστάμενων τέτοιων μέτρων. Είναι αναγκαίο να αναφερθεί ότι σε αυτή τη φάση εκτελούνται παράλληλα και βήματα της φάσης της Δημιουργίας Αναφοράς καθώς δεν είναι δυνατή η δημιουργία της αναφοράς στο τέλος και αυτόνομα των άλλων φάσεων [NIST, 2008; PTES, 2014; PTF, 2014].

6. **Διατήρηση Πρόσβασης (Maintaining Access),** συνήθως κατά το βήμα αυτό χρησιμοποιούνται τεχνικές και εργαλεία που έχουν σκοπό την αναβάθμιση δικαιωμάτων και την εγκατάσταση κερκοπορτών (backdoors), την εγκατάσταση κάποιας ανοιχτής θύρας στο σύστημα ώστε μετά την Εκμετάλλευση του συστήματος να διατηρηθεί η δυνατότητα πρόσβασης ακόμα και αν χρησιμοποιηθούν αντίμετρα. Αυτό επιτυγχάνεται με την εγκατάσταση προγραμμάτων όπως είναι τα προγράμματα καταγραφής πληκτρολόγησης (keyloggers), προγράμματα καταγραφής κίνησης τερματικών (screen capture programs) αλλά και με την αλλοίωση συστημάτων ασφάλειας, διακίνησης ηλεκτρονικών μηνυμάτων και περιηγητών διαδικτύου. Πέρα από αυτού του είδους του λογισμικού, προτείνεται η εγκατάσταση rootkit στο στόχο ώστε ο ελεγκτής να έχει τον πλήρη έλεγχο του συστήματος χωρίς αυτό να γίνεται αντιληπτό από κάποιο λογισμικό προστασίας από ιούς. Είναι δυνατόν κατά τη διάρκεια της φάσης Διατήρηση Πρόσβασης να επιτυγχάνονται και περαιτέρω στόχοι. Ανάμεσα σε αυτούς είναι η δημιουργία συνθηκών για πρόκληση επίθεσης άρνηση υπηρεσιών (denial of service attack), η αποκάλυψη μίας σειράς από στοιχεία του συστήματος όπως είναι οι διεπαφές, οι ρυθμίσεις των δρομολογητών, οι DNS διακομιστές και οι εγγραφές αυτών, οι διακομιστές μεσολάβησης (proxy servers), οι εγγραφές του ARP πρωτοκόλλου, οι VPN συνδέσεις. Επιπλέον, καταγράφονται δευτερεύοντα στοιχεία όπως τα δικαιώματα αρχείων και εκτύπωσης, οι βάσεις δεδομένων και οι λίστες με τα αρχεία που περιέχουν και οι αρχές έκδοσης πιστοποιητικών. Πρέπει να σημειωθεί ότι, όπως και στη φάση της Εκμετάλλευσης όλες οι διαδικασίες πρέπει να σημειώνονται καθώς πραγματοποιούνται στη αναφορά καθώς αυτό δεν μπορεί να γίνει αυτοτελώς[ISSAF, 2006; PTES, 2014].

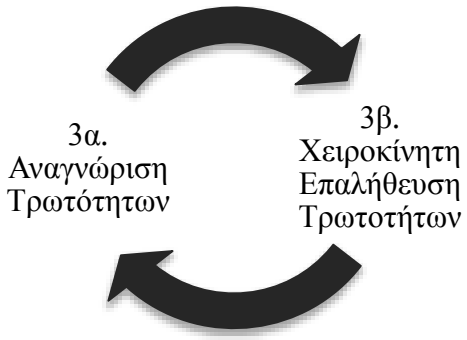
7. **Δημιουργία Αναφοράς**, η οποία έχει σαν σκοπό τη σύνταξη ενός κειμένου με στόχο την πληροφόρηση των ενδιαφερομένων. Για το λόγο αυτό, το κείμενο που συντάσσεται πρέπει να είναι ελεύθερο τεχνικών όρων όσο αυτό είναι δυνατό και να έχει την μικρότερη δυνατή έκταση. Πρέπει να γίνει κατανοητό το γεγονός ότι η αναφορά θα διαβαστεί από τη διοίκηση του οργανισμού τις περισσότερες φορές. Για το λόγο αυτό, πρέπει να μεταφραστούν τα αποτελέσματα του ελέγχου σε επικινδυνότητα ή επιχειρησιακά "ρίσκο" που μετριόνται σε χρηματικά ποσά. Επιπλέον, είναι σημαντικό ο βαθμός περιεκτικότητας να είναι ο μέγιστος επιτρεπτός. Εκεί αναφέρονται διάφορα σημαντικά στοιχεία. Αυτά είναι:

    - οι ημερομηνίες ελέγχου
    - η ομάδα αξιολόγησης, τα ονόματα των μελών και οι ρόλοι τους καθώς και πληροφορίες επικοινωνίας
    - όλοι οι διακομιστές που σχετίζονται με τον οργανισμό, διακομιστές DNS, διακομιστές βάσεων δεδομένων, διακομιστές μεσολάβησης (proxy servers), καθώς και όλες οι τυχόν εγγραφές που υπάρχουν
    - κεντρικοί υπολογιστές με όλες τις διευθύνσεις IP, τις τροποποιήσεις που έγιναν στο σύστημα, μαζί με μία λεπτομερή λίστα από τις ενέργειες που εκτελέστηκαν κατά τον έλεγχο
    - τα λειτουργικά συστήματα που είναι εγκατεστημένα στους κεντρικούς υπολογιστές
    - το υπόλοιπο υλικό και ρυθμίσεις αυτού, όπως είναι οι εκτυπωτές
    - τα εργαλεία που χρησιμοποιήθηκαν είτε αυτό αφορά εργαλεία εμπορίου, είτε εργαλεία που χρησιμοποιήθηκαν
    - το εύρος του ελέγχου μαζί με τους κανόνες εμπλοκής
    - ο σκοπός του ελέγχου δηλαδή για ποιο λόγο πραγματοποιήθηκε ο έλεγχος (π.χ. πιστοποίηση ή νομικές υποχρεώσεις)
    - οι τύποι ελέγχου που χρησιμοποιήθηκαν
    - όλα τα αρχεία που παράχθηκαν κατά την εκτέλεση των εργαλείων
    - μία λίστα με όλες τις τρωτότητες που βρεθήκαν κατά τη φάση της Αναγνώρισης ανά τομέα (Εφαρμογής, Φυσικές, Προσωπικού, Γενικές)
    - μία λίστα με τα πιθανά αντίμετρα

Στην αναφορά επίσης, αναφέρονται οι επιπτώσεις κάθε απειλής στο στόχο (οργανισμό) και ο συνολικός βαθμός επικινδυνότητας.



Σχήμα 2. Οι φάσεις της προτεινόμενης μεθοδολογίας.



Σχήμα 3. Η φάση τρία της μεθοδολογίας.

2.4 Related work για μεθοδολογίες

Στο κεφάλαιο αυτό αναφέρονται και περιγράφονται συναφείς έρευνες που έχουν πραγματοποιηθεί τα τελευταία χρόνια σχετικά με μεθοδολογίες ελέγχου διείσδυσης και τα αντίστοιχα τεχνολογικά εργαλεία που χρησιμοποιούνται κατά τον έλεγχο διείσδυσης. Επιπλέον, αναφέρονται οι τάσεις που παρουσιάζονται στην ερευνητική περιοχή των ελέγχων διείσδυσης.

Πιο συγκεκριμένα, αναφέρονται νέες θεωρητικές προσεγγίσεις γύρω από τον έλεγχο διείσδυσης, όπως είναι μεθοδολογίες διενέργειας ελέγχου διείσδυσης και μία προτεινόμενη ταξινομία. Στη θεωρητική προσέγγιση βρίσκεται επίσης έρευνα σχετικά με τη στατική και δυναμική ανάλυση εκτελέσιμου κώδικα. Σε αυτή την ενότητα, χωρίς να αποτελεί ένα καθαρά θεωρητικό αντικείμενο, αναφέρονται οι εξελίξεις και οι τάσεις της έρευνας γύρω από το φυσικό έλεγχο διείσδυσης.

Αντίστοιχα, όσον αφορά στην τεχνολογική προσέγγιση, αναφέρονται και περιγράφονται έρευνες που αφορούν έλεγχο διείσδυσης σε εφαρμογές ιστού (web penetration testing) και σε υπηρεσίες αυτού (web services penetration testing). Επίσης, στην ενότητα αυτή βρίσκονται έρευνες σχετικές με έλεγχο διείσδυσης σε συστήματα SCADA, στο λογισμικό έξυπνων κινητών (και όχι μόνο) Android και σε συσκευές που χρησιμοποιούν τεχνολογία NFC. Τέλος, αναφέρονται έρευνες σύγκρισης αποτελεσματικότητας σε εμπορικά, επί των πλείστων, εργαλεία.

2.4.1 Έρευνα Θεωρητικής Προσέγγισης

Στο επίπεδο των μεθοδολογιών ελέγχου διείσδυσης, πέρα από τις ήδη αναφερθέντες, οι Alisherov & Sattarova αναφέρουν μία μεθοδολογία από μία διαφορετική οπτική γωνία. Η μεθοδολογία που προτείνουν αποτελείται από τρεις βασικές οντότητες. Αυτές είναι η πληροφορία, η ομάδα που διεξάγει τον έλεγχο και τα εργαλεία που χρησιμοποιούνται για τον έλεγχο. Σχετικά με την οντότητα πληροφορία, εκείνη ακολουθεί ενέργειες αντίστοιχες με τη φάση Συλλογή Πληροφοριών, όπως αυτή αναφέρεται στις περισσότερες μεθοδολογίες. Εντύπωση προκαλεί το γεγονός ότι οι άλλες φάσεις δεν αναφέρονται τουλάχιστον τυπικά. Οι Alisherov & Sattarova εμμένουν χαρακτηριστικά σε αυτή τη φάση, καθώς θεωρούν πως αν αυτή επιτύχει τότε

τα άλλα βήματα (φάσεις) θα διεξαχθούν με επιτυχία. Στη συνέχεια της εργασίας τους, επεξηγούνται οι άλλες δύο ενότητες. Τα μέλη της ομάδας που θα διεξάγει τον έλεγχο θα πρέπει να έχουν συγκεκριμένους ρόλους και καθήκοντα. Επιπλέον, η μεθοδολογία αναφέρει το σαφές πλαίσιο μέσα στο οποίο θα κινηθεί ο έλεγχος διείσδυσης, συμφωνημένο μεταξύ των δύο μερών, το οποίο ορίζει τυχόν ευθύνες, κανόνες και κατευθυντήριες γραμμές στις οποίες ο έλεγχος θα κινηθεί [Alisherov & Sattarova, 2009].

Στο ίδιο επίπεδο, οι Nor Fatimah Awang και Azizah Abd Manaf, προτείνουν μία μεθοδολογία με σκοπό τη μείωση των ψευδώς θετικών αποτελεσμάτων που εμφανίζονται κατά τη φάση της Αναγνώρισης Τρωτοτήτων ενός ελέγχου σε μία εφαρμογή ιστού. Η μεθοδολογία τους απαρτίζεται από τέσσερις φάσεις. Κατά την πρώτη φάση, επιλέγεται η ιστοσελίδα που θα ελεγχθεί και ένα αυτοματοποιημένο εργαλείο σάρωσης τρωτοτήτων. Στη δεύτερη φάση, η εφαρμογή ιστού σαρώνεται από το εργαλείο. Στη τρίτη φάση, επιχειρείται η Χειροκίνητη Επαλήθευση Τρωτοτήτων μέσω της εκμετάλλευσης τους. Με αυτό τον τρόπο επιχειρείται η μείωση των ψευδώς θετικών αποτελεσμάτων. Τέλος, οι ερευνητές αναφέρουν την ανάλυση που πρέπει να συντελεστεί κατά την τέταρτη φάση μεταξύ των αποτελεσμάτων της δεύτερης και τρίτης φάσης [Ismail et al, 2013].

Τα προβλήματα ασφάλειας των υπηρεσιών ιστού δεν είναι δυνατό να αντιμετωπιστούν μόνο μετά από τη δημιουργία αυτών. Για το λόγο αυτό, οι Xiong και Peyton στην εργασία τους “A model-driven penetration test framework for Web Applications”, περιγράφουν ένα νέο μοντέλο ανάπτυξης εφαρμογών ιστού εισάγοντας την έννοια της ασφάλειας στους κύκλους ζωής και στην αρχιτεκτονική της εφαρμογής. [Xiong & Peyton, 2010].

Μία ακόμα σημαντική μεθοδολογία κινούμενη στη λογική της αποτελεσματικότητας και της αποδοτικότητας είναι εκείνη των Haubris και Pauli, όπως περιγράφεται στην έρευνα τους. Η μεθοδολογία που προτείνουν απαρτίζεται από εργαλεία και φάσεις. Αρχικά, αναζητούνται συγκεκριμένες πληροφορίες που είναι απαραίτητες για το σχεδιασμό και έπειτα πληροφορίες σχετικές με το δίκτυο τις θύρες και τις υπηρεσίες που είναι απαραίτητες για τη φάση της Αναγνώρισης Τρωτοτήτων με τη βοήθεια των εργαλείων. Έπειτα, ανακαλύπτονται οι όποιες τρωτότητες και τέλος γίνονται

αντικείμενο εκμετάλλευσης. Οι συγγραφείς δημιούργησαν ένα εργαλείο το οποίο ενσωματώνει υπάρχοντα εργαλεία και με αυτό τον τρόπο η εκτέλεση γίνεται γρήγορα και αποτελεσματικά, αφού η σειρά εκτέλεσης των εργαλείων γίνεται με τέτοιο τρόπο ώστε να επιτυγχάνεται η αξιοπιστία των αποτελεσμάτων, όπως αναφέρουν οι ερευνητές [Haubris & Pauli, 2013].

Εξίσου σημαντική, είναι η έρευνα των hudic et al, περί ταξινομιών. Ο hudic και η ομάδα του δημιούργησαν και ανέπτυξαν ένα εννοιολογικό πλαίσιο με στόχο να καλύψουν τις περισσότερες πτυχές ενός ελέγχου διείσδυσης. Έτσι, το μοντέλο τους απαρτίζεται από έξι υποτάξεις. Οι τάξεις αφορούν τη τεχνολογία, τη συμμόρφωση, τη χρησιμότητα, το τομέα εφαρμογών, τη φυσική ασφάλεια και τη συλλογή πληροφοριών. Σύμφωνα με τους ερευνητές, η ταξινομία αυτή βοηθάει στην οργάνωση και στην κατανόηση τόσο των θεωρητικών όσο και των τεχνολογικών πτυχών ενός ελέγχου διείσδυσης [Hudic et al, 2012].

Αναφορικά με τη στατική και δυναμική ανάλυση, οι Halfond et al, παρουσίασαν μία νέα προσέγγιση ελέγχου διείσδυσης η οποία έχει σαν στόχο τη βελτίωση της Συλλογής Πληροφοριών και την ανάλυση των απαντήσεων. Η έρευνα τους προσεγγίζεται στο συνδυασμό στατικής και δυναμικής ανάλυσης. Η στατική ανάλυση του κώδικα είναι ικανή να εντοπίσει τα IV των εφαρμογών ιστού και η δυναμική να αυτοματοποιήσει την ανάλυση των απαντήσεων. Η έρευνα τους έδειξε ότι η νέα προσέγγιση συνδυαστικής ανάλυσης απέφερε καλύτερα αποτελέσματα με πιο αποτελεσματικό τρόπο από ένα παραδοσιακό έλεγχο διείσδυσης [Halfond et al, 2011]. Στα ίδια αποτελέσματα μέσω εμπορικών εργαλείων κατέληξαν και οι Antunes & Vieira στη σύγκριση που διενέργησαν μεταξύ ελέγχου διείσδυσης και στατικής ανάλυσης κώδικα για την ανεύρεση τρωτοτήτων σε υπηρεσίες ιστού. Η έρευνα τους αν και περιορισμένη σε SQLi τρωτότητες ανέδειξε τη χρήση στατικής ανάλυσης ως προτιμητέα σε σχέση με ένα παραδοσιακό έλεγχο διείσδυσης [Antunes et al, 2009].

Τέλος, μεγάλο ενδιαφέρον παρουσιάζει το βιβλίο με τίτλο Unauthorized Access [Wil Allsopp, 2009] το οποίο συνοψίζει μεθοδολογίες και τεχνικές για τη διενέργεια ενός φυσικού ελέγχου διείσδυσης. Ο φυσικός έλεγχος διείσδυσης είναι ένα είδος ελέγχου που σπάνια διενεργείται. Ο συγγραφέας πέρα από τεχνικές κοινωνικές μάθησης, παραπλάνησης και παραβίασης χώρων εκθέτει πληροφορίες γύρω από το κανονιστικό

πλαίσιο, συμβουλές σχετικά με τον έλεγχο αλλά και μεθόδους για επίθεση σε ασύρματα δίκτυα.

2.4.2 Έρευνα τεχνολογικής προσέγγισης

Στην ενότητα αυτή, αναφέρονται τεχνολογικά εργαλεία και προσπάθειες που έχουν πραγματοποιηθεί για αναγνώριση τρωτοτήτων, επαλήθευση και εκμετάλλευση αυτών. Οι προσπάθειες των ερευνητών τη τελευταία πενταετία έχουν προσανατολιστεί σε εφαρμογές και υπηρεσίες ιστού, καθώς η δημοτικότητα των τελευταίων έχει αυξηθεί δραματικά το τελευταίο καιρό. Το γεγονός αυτό έχει τις ρίζες του στη διαθεσιμότητα των εφαρμογών μέσω ενός περιηγητή διαδικτύου και την ευκολία που αυτού του είδους η χρήση παρουσιάζει. Επίσης, αναφέρονται έρευνες που παρουσιάζουν συγκρίσεις εργαλείων και δοκιμαστικές εκτελέσεις αναγνώρισης τρωτοτήτων καθώς η επαλήθευση τρωτοτήτων παρουσιάζει πολλές ιδιαιτερότητες. Εκτός αυτών αναφέρεται η έρευνα γύρω από τα συστήματα SCADA, το λογισμικό Android και τη τεχνολογία NFC.

Σε αυτό το επίπεδο, ο Falkenberg του δημιούργησε ένα εργαλείο για την εκτέλεση επιθέσεων άρνησης υπηρεσιών. Το εργαλείο πραγματοποιεί επιτυχημένες επιθέσεις άρνησης υπηρεσιών με μέθοδο μαύρου κουτιού και χρησιμοποιήθηκε σε συστήματα Axis2Java, Apache CXF και Metro [Falkenberg, 2013]. Αυτό επιτυγχάνεται μέσα από την εκμετάλλευση διάφορων τρωτοτήτων που παρουσιάζουν οι εφαρμογές ιστού και τα μηνύματα XML που ανταλλάσσονται κατά τη χρήση τους.

Σχετικά με την επαλήθευση των τρωτοτήτων, έχουν πραγματοποιηθεί αρκετές έρευνες. Ανάμεσα τους εκείνη των [Awad & Hassanien, 2013], στην οποία πραγματοποιείται σύγκριση των αποτελεσμάτων σάρωσης τριών εμπορικών εργαλείων αναγνώρισης τρωτοτήτων. Η έρευνα τους καταδεικνύει το μεγάλο αριθμό ψευδώς θετικών αποτελεσμάτων. Οι ίδιοι παρουσιάζουν έναν αλγόριθμο μείωσης των ψευδώς θετικών αποτελεσμάτων και αναφέρουν την αποτελεσματικότητα του. Σε μία παρόμοια έρευνα ο Vieira και οι συνεργάτες του, χρησιμοποίησαν 3 εμπορικά εργαλεία σάρωσης τρωτοτήτων και συνέκριναν τα αποτελέσματα σάρωσης. Τα ευρήματα τους κατέληξαν στο γεγονός ότι το κάθε εργαλείο αναγνωρίζει διαφορετικά είδη τρωτοτήτων ενώ αγνοεί κάποια άλλα. Εκτός από αυτό, αναγνώρισαν το μεγάλο αριθμό ψευδώς θετικών

αποτελεσμάτων και την ανάγκη για επαλήθευση των αποτελεσμάτων [Vieira et al, 2009]. Ιδιαίτερα ανησυχητικά είναι τα συμπεράσματα της έρευνας του David Shelly [David Shelly, 2009] σχετικά με την ύπαρξη ψευδώς θετικών αλλά και ψευδώς αρνητικών αποτελεσμάτων των εργαλείων σάρωσης και αναγνώρισης τρωτοτήτων. Στην έρευνα του σχετικά με τα εργαλεία αναγνώρισης τρωτοτήτων για εφαρμογές ιστού, υπογραμμίζει την ανάγκη για βελτίωση τους, καθώς όπως αναφέρει ο αριθμός ψευδώς θετικών και αρνητικών αποτελεσμάτων στις τρωτότητες SQLi, XSS, διαχείρισης συνόδου και υπερχείλισης στοίβας είναι ιδιαίτερα μεγάλος.

Σχετικά με τα συστήματα SCADA, μία από τις πιο σημαντικές έρευνες είναι το άρθρο με τίτλο "Security issues in SCADA networks", το οποίο περιγράφει τις νέες προκλήσεις που παρουσιάζονται στα δίκτυα SCADA. Οι συγγραφείς αναφέρουν σαν βασική αιτία προβλημάτων τη διασυνδεσιμότητα των δικτύων με αποτέλεσμα την έκθεση τους σε μία σειρά από απειλές. Το άρθρο αναφέρει ως προβληματική την ύπαρξη μίας πληθώρας πρωτοκόλλων (150-200) σχετικά με αυτά τα δίκτυα και ως επικίνδυνη την αντίληψη που έχουν πολλοί διαχειριστές περί δικτυακής απομόνωσης τους. Τα δίκτυα SCADA δεν είναι απομονωμένα και ο συνδυασμός υλικού και λογισμικού τύπου COTS τα καθιστά ιδιαίτερα ευάλωτα σε επιθέσεις. Το γεγονός αυτό δε δημιουργεί εντύπωση, καθώς την εποχή που άρχισαν να χρησιμοποιούνται, έμφαση δινόταν στην απρόσκοπτη λειτουργία και την αποτελεσματικότητα τους. Στην προσπάθεια ενίσχυσης της ασφάλειας των δικτύων SCADA, έχουν εκδοθεί διάφοροι οδηγοί με κατευθυντήριες γραμμές με πιο σημαντικούς εκείνους του Συμβουλίου Προστασίας Κρίσιμων Υποδομών του Προέδρου των ΗΠΑ, του Υπουργείου Ενέργειας των ΗΠΑ και του Εθνικού Κέντρου Ασφάλειας Υποδομών και Συντονισμού του Ηνωμένου Βασιλείου [Ralstona & Graham, 2011]. Πιο συγκεκριμένα, ο οργανισμός SANDIA έχει εκδώσει ένα μικρό οδηγό με βήματα για τον έλεγχο των δικτύων SCADA, δίνοντας ένα λεπτομερή αλλά λιτό οδηγό [Duggan, 2005].

Μία από τις ερευνητικές τάσεις των τελευταίων χρόνων είναι ο έλεγχος διείσδυσης στο λογισμικό των έξυπνων κινητών όπως είναι το iOS και το Android το οποίο είναι ανοιχτού κώδικα. Έρευνα που πραγματοποιήθηκε σε διάφορες εκδόσεις του λειτουργικού συστήματος Android κατέδειξε τις αδυναμίες και τις επιθέσεις εκείνες που το σύστημα είναι επιρρεπές. Η μεθοδολογία και τα εργαλεία που χρησιμοποιήθηκαν είναι ανάλογα με εκείνα που χρησιμοποιούνται σε ένα συμβατικό

έλεγχο διείσδυσης τερματικών (π.χ. ηλεκτρονικών υπολογιστών). Σύμφωνα με την έρευνα, το λειτουργικό παρουσιάζει ιδιαιτέρως μεγάλα προβλήματα σε σχέση με τις επιθέσεις άρνησης υπηρεσιών, τις επιθέσεις ενδιάμεσου (man-in-the-middle attack) και παραβίασης συνόδου (session hijacking). Πρέπει να σημειωθεί ότι το λειτουργικό Android ανανεώνεται συχνά και μία τέτοια έρευνα σύντομα μπορεί να θεωρηθεί αναχρονιστική [Ehtsam, 2011].

Μία άλλη τάση στην έρευνα των ελέγχων διείσδυσης είναι εκείνη σε συσκευές (και ειδικότερα έξυπνα τηλέφωνα) που χρησιμοποιούν τεχνολογία NFC. Η τεχνολογία NFC χρησιμοποιείται αρκετά στο τομέα των (ηλεκτρονικών) εισιτηρίων και των (ηλεκτρονικών) πληρωμών. Έρευνα γύρω από τη τεχνολογία NFC, έδειξε ότι υπάρχει ένας μεγάλος αριθμός τρωτοτήτων σε συσκευές που χρησιμοποιούν τη τεχνολογία, ικανές να γίνουν αντικείμενο εκμετάλλευσης μέσω επιθέσεων ηλεκτρονικού ψαρέματος (phishing attacks), επιθέσεων άρνησης υπηρεσιών. Οι επιθέσεις αυτές γίνονται μέσω fuzzing δηλαδή που περιλαμβάνει την παροχή άκυρων, έγκυρων, ή τυχαίων δεδομένων σαν είσοδο ενός προγράμματος ηλεκτρονικού υπολογιστή. [Mulliner, 2009]

3. Διαθέσιμα εργαλεία

3.1 Ανάλυση και περιγραφή (ανά κατηγορία / βήμα)

Ακολουθεί η περιγραφή διάφορων εργαλείων ικανά να συνοδεύσουν τις μεθοδολογίες ελέγχου διείσδυσης στη διενέργεια του ελέγχου. Τα εργαλεία έχουν διαχωριστεί ανά φάση. Αναφέρεται η περιγραφή της λειτουργίας τους, τα χαρακτηριστικά τους και η βασική φάση στα οποία χρησιμοποιούνται. Κάποια εργαλεία χρησιμοποιούνται σε παραπάνω από μία φάσεις και για αυτό το λόγο στο τέλος της ενότητας ακολουθεί πίνακας με αντιστοίχηση μεταξύ εργαλείων και φάσεων ελέγχου.

3.1.1 Συλλογή Πληροφοριών (Information Gathering)

Wireshark

Το εργαλείο wireshark αποτελεί εργαλείο ανάλυσης πρωτοκόλλων στην κίνηση δικτύου. Αυτό επιτρέπει στο χρήστη να δει τι συμβαίνει στο δίκτυο σε μικροσκοπικό επίπεδο. Αποτελεί το de facto πρωτόκολλο σε πολλές βιομηχανίες και εκπαιδευτικά ιδρύματα. Υπάρχουν εκδόσεις του εργαλείου για πολλά λειτουργικά συστήματα. Το εργαλείο επιτρέπει στο χρήστη να επιθεωρεί την κίνηση μέσα από εκατοντάδες πρωτόκολλα, να καταγράφει εντός σύνδεσης την κίνηση και έπειτα να την αναλύει εκτός σύνδεσης. Προσφέρει στο χρήστη μία πολύ φιλική και χρηστική διεπαφή και μία μεγάλη πληθώρα από φίλτρα αποτελεσμάτων. Επιπλέον, μπορεί να διαβάσει από πολλά μέσα, δηλαδή Ethernet, IEEE 802.11, PPP/HDLC, bluetooth, usb, token ring, frame relay και να εγγράψει σε πολλούς διαφορετικούς τύπους καταγραφής. Τέλος, το εργαλείο υποστηρίζει αποκρυπτογράφηση για αρκετά πρωτόκολλα όπως είναι τα: IPsec, ISAKMP, Kerberos, SSL, WEP, WPA/WPA2. Ο στόχος του εργαλείου είναι να βοηθήσει τον ελεγκτή να συλλέξει όσο το δυνατόν περισσότερες πληροφορίες σχετικά με το δίκτυο και την κίνηση σε αυτό. Για το λόγο αυτό, το εργαλείο συγκαταλέγεται στα εργαλεία εκείνα που βρίσκονται στη φάση της Συλλογής Πληροφοριών. [Wireshark, 2014]

Nmap

Το εργαλείο nmap είναι ένα δωρεάν και ανοιχτού κωδικά λογισμικό που χρησιμοποιείται για την ανακάλυψη δικτύων και τον έλεγχο της ασφάλειας τους. Πολλοί διαχειριστές δικτύων και πληροφοριακών συστημάτων χρησιμοποιούν το εργαλείο για εργασίες όπως είναι η διαχείριση αναβάθμισης των υπηρεσιών και η παρακολούθηση των κεντρικών υπολογιστών και των χρόνων λειτουργίας των υπηρεσιών. Το nmap χρησιμοποιεί πακέτα IP με διάφορους τρόπους ώστε να καθοριστεί αν και ποια μηχανήματα είναι διαθέσιμα στο δίκτυο, ποιες υπηρεσίες προσφέρει το κάθε μηχάνημα, ποια λειτουργικά συστήματα, ποιο τύπο φίλτρων και τείχη προστασίας χρησιμοποιεί. Αρχικά, το εργαλείο σχεδιάστηκε για να σαρώνει μεγάλα δίκτυα αλλά μπορεί να χρησιμοποιηθεί εξίσου καλά απέναντι σε μοναδικούς στόχους. Το εργαλείο μπορεί να εγκατασταθεί σε όλα τα γνωστά λειτουργικά συστήματα. Πέρα από την κλασσική μορφή του εργαλείου μέσω της γραμμής εντολών, παρέχεται μια γραφική διεπαφή, καθώς και μία ειδική λειτουργία για θέαση των αποτελεσμάτων, το Zenmap.[Nmap,2014] Τέλος, το εργαλείο προσφέρει ευέλικτη μεταφορά δεδομένων, λειτουργία ανακατεύθυνσης, εργαλείο εντοπισμού σφαλμάτων, ένα βοηθητικό πρόγραμμα για τη σύγκριση των αποτελεσμάτων σάρωσης, ένα εργαλείο δημιουργίας πακέτων και λειτουργία ανάλυσης απαντήσεων. Ο στόχος του εργαλείου είναι να βοηθήσει το χρήστη να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες γίνεται ώστε να πραγματοποιήσει τις επόμενες φάσεις με σιγουριά. Το εργαλείο χρησιμοποιείται στη φάση της Συλλογής Πληροφοριών αλλά και τις Αναγνώρισης Τρωτοτήτων χάρη στη δυνατότητα του να χρησιμοποιεί διάφορες προσθήκες λογισμικού (extensions, plugins). Το nmap παρουσιάζει αρκετά χαρακτηριστικά. Αυτά είναι:

- Ευελιξία- υποστηρίζει δεκάδες προηγμένες τεχνικές για τη χαρτογράφηση των δικτύων σε συνεργασία με πολλά φίλτρα. Αυτό περιλαμβάνει πολλούς μηχανισμούς ανίχνευσης λειτουργικών, εκδόσεων λογισμικού κ.ά.
- Δύναμη- έχει χρησιμοποιηθεί με μεγάλη επιτυχία για τη σάρωση πολύ μεγάλων δικτύων, με εκατοντάδες χιλιάδες μηχανήματα
- Φορητότητα- εγκαθίσταται στα πιο γνωστά λειτουργικά συστήματα

- Ευκολία χρήσης- ενώ το εργαλείο παρέχει μία λίστα από παραμετροποιήσιμες εντολές για τους προχωρημένους χρήστες, προσφέρει διεπαφή και για τους λιγότερο έμπειρους
- Διαθεσιμότητα- Χαρακτηριστικό είναι πως διατίθεται δωρεάν
- Καλή τεκμηρίωση- έχει γίνει μία πολύ καλή προσπάθεια τεκμηρίωσης του εργαλείου, παρέχεται ένα ολόκληρο βιβλίο με τις λειτουργίες του εργαλείου καθώς και μαθήματα εκμάθησης είτε σε γραπτή μορφή είτε σε μορφή βίντεο

Maltego

Το εργαλείο maltego δημιουργήθηκε με στόχο να παραδώσει μία σαφή εικόνα του περιβάλλοντος στον οργανισμό κάτω υπό το πρίσμα των απειλών. Το ιδιαίτερο πλεονέκτημα που παρέχει το εργαλείο είναι η ικανότητα του να καταδείξει την πολυπλοκότητα και τη σοβαρότητα της αποτυχίας που μπορεί να παρουσιάζονται σε διάφορα σημεία, καθώς και τις σχέσεις εμπιστοσύνης που υπάρχουν την τρέχουσα περίοδο διεξαγωγής του ελέγχου στις υποδομές του οργανισμού. Το maltego προσφέρει μία μοναδική προοπτική τόσο σχετικά με το δίκτυο όσο και με τις διάφορες οντότητες που βασίζονται στους πόρους του, όπως είναι η συγκέντρωση των πληροφοριών που δημοσιεύονται σε όλο το Διαδίκτυο. Αυτές οι πληροφορίες, για παράδειγμα, μπορεί να αφορούν την τρέχουσα διαμόρφωση του δρομολογητή που επικοινωνεί με το διαδίκτυο. Το maltego μπορεί να εντοπίσει και να απεικονίσει συνολικά αυτές τις πληροφορίες. Πιο συγκεκριμένα, μπορεί να χρησιμοποιηθεί για να προσδιορίσει τις σχέσεις και τους δεσμούς στην πραγματική ζωή μεταξύ ανθρώπων, ομάδων ανθρώπων, εταιρειών, οργανισμών, ιστοσελίδων, και πληροφορίες διαδικτύου όπως είναι οι περιοχές (domains), διευθύνσεις IP, συνεργασίες, έγγραφα και αρχεία.[Maltego,2014] Είναι σαφές από τη περιγραφή του εργαλείου ότι αυτό χρησιμοποιείται κατά τη φάση του Σχεδιασμού και της Προετοιμασίας αλλά και της Συλλογής Πληροφοριών (παθητική).

ArpScan

Το arpscan αποτελεί εργαλείο σάρωσης (συχνά εμφανίζεται ως ARP sweep ή MAC scanner) και είναι ένας πολύ γρήγορος σαρωτής πακέτων ARP. Ο σκοπός του

εργαλείου είναι να υποδείξει κάθε ενεργό μηχάνημα (συσκευή) στο υποδίκτυο. Βέβαια, από τη στιγμή που το πρωτόκολλο ARP δεν έχει δυνατότητα δρομολόγησης, αυτό το είδος σάρωσης χρησιμοποιείται μόνο εντός υποδικτύου. Στα πλεονεκτήματα του εργαλείου συγκαταλέγεται η δυνατότητα του να ανακαλύπτει τις ενεργές συσκευές ακόμα και αν βρίσκονται πίσω από κάποιο τείχος προστασίας. Οι συσκευές δεν μπορούν να αρνηθούν την ύπαρξη τους στα ARP πακέτα, όπως μπορούν να κάνουν σε μία εντολή ping.[Arpscan,2014] Το εργαλείο αυτό χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών ή Αναγνώριση Δικτύου.

Social Engineer Tool SET

Το εργαλείο Social Engineer Tool είναι ειδικά σχεδιασμένο για να εκτελεί προηγμένες επιθέσεις εναντίον του ανθρώπινου στοιχείου. Το SET γρήγορα έγινε ένα αναπόσπαστο εργαλείο για τους επαγγελματίες ελεγκτές ασφάλειας. Οι επιθέσεις που είναι ενσωματωμένες στην εργαλειοθήκη του SET είναι σχεδιασμένες να στοχεύουν σε ένα πρόσωπο κάθε φορά ή και στον οργανισμό σαν ολότητα. Ο σκοπός του εργαλείου είναι η συλλογή πληροφοριών μέσω επιθέσεων κοινωνικής μηχανικής.[Social Engineer Tool, 2014] Το εργαλείο συνήθως χρησιμοποιείται από κοινού με το εργαλείο Maltego. Είναι προφανές ότι η χρήση του εργαλείου συμβαίνει κατά τη φάση του Σχεδιασμού και της Συλλογής Πληροφοριών.

DnsDict6

Το συγκεκριμένο εργαλείο είναι ιδανικό για τη συγκέντρωση πληροφοριών σχετικές με το διακομιστή DNS. Το dnsdict6 μπορεί να απαριθμήσει διάφορες πληροφορίες, οι οποίες είναι μη ορατές στον απλό χρήστη. Το εργαλείο βρίσκεται όπως και πολλά άλλα στη σουίτα kali linux και σκοπός του είναι η ανεύρεση πληροφοριών όπως: πληροφορίες για υποτομείς(subdomains), τις διευθύνσεις IPv4 και IPv6, λεπτομέρειες σχετικές με srv αρχεία και λεπτομέρειες για τους διακομιστές.[DNSDict6,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

DnsEnum

Το dnsenum δημιουργήθηκε για να πραγματοποιεί απαρίθμηση πληροφοριών σχετικές με το διακομιστή DNS και τους τομείς αυτού (domains). Ο σκοπός του εργαλείου είναι να συγκεντρώσει όσο το δυνατόν περισσότερες πληροφορίες για ένα τομέα. Το πρόγραμμα επί του παρόντος εκτελεί τις εξής λειτουργίες: απόκτηση ονόματος διακομιστή, απόκτηση διεύθυνσης ενεργών συσκευών (μηχανημάτων, κεντρικών υπολογιστών), απόκτηση του αρχείου MX, πραγματοποίηση axfr ερωτημάτων στους διακομιστές, απόκτηση επιπλέον ονομάτων μέσω της μηχανής αναζήτησης Google, υπολογισμός του εύρους της τάξης C στους τομείς των δικτύων και αντίστροφες αναζητήσεις (reverse lookups) στα εύρη των δικτύων.[DnsEnum,2014] Χρησιμοποιείται στη φάση της Αναγνώρισης Δικτύου.

DnsMap

Ο σκοπός του εργαλείου dnsmap είναι η ανακάλυψη τμημάτων (μπλοκ) από διευθύνσεις συσκευών στο δίκτυο. Το dnsmap κυρίως προορίζεται για να χρησιμοποιηθεί από τους ελεγκτές κατά τη διάρκεια της συλλογής πληροφοριών ή της απαρίθμησης σχετικά με την αξιολόγηση της ασφάλειας των υποδομών. Κατά το στάδιο αυτό, ο ελεγκτής θα προσπαθήσει να βρει τα εύρη των διευθύνσεων στο υποδίκτυο, τα ονόματα των τομέων, νούμερα τηλεφώνων. Επιπλέον, το εργαλείο έχει τη δυνατότητα να ανακαλύψει και τους υπο-τομείς από συγκεκριμένους τομείς (για παράδειγμα από το google.com είναι δυνατό να ανακαλύψει το mail.google.com, earth.google.com κλπ). Η ανακάλυψη των υποτομέων πραγματοποιείται με τη βοήθεια επιθέσεων ωμής βίας (brute force attack).[DNSMap,2014] Οι επιθέσεις αυτές είναι ιδιαίτερα χρήσιμες όταν τα άλλα είδη επιθέσεων δε λειτουργούν.

DnsTracer

Το dnstracer είναι ένα εργαλείο που χρησιμοποιείται στη φάση της συλλογής πληροφοριών για τον εξής λόγο. Είναι ικανό να καθορίσει από που ένας συγκεκριμένος διακομιστής DNS παίρνει τις πληροφορίες του και να ακολουθήσει την αλυσίδα των διακομιστών DNS πίσω σε εκείνους που γνωρίζουν τις

πληροφορίες.[DNSTracer,2014] Το εργαλείο βρίσκεται στη σουίτα εργαλείων του kali linux.

Fierce

Το fierce είναι και αυτό ένα εργαλείο που βρίσκεται στο kali linux. Ο στόχος του εργαλείου είναι να συγκεντρώσει πληροφορίες σχετικές με το διακομιστή DNS. Χρησιμοποιείται ιδιαίτερα σε περιπτώσεις τέτοιες που οι διευθύνσεις του οργανισμού δεν είναι συνεχόμενες. Μία από τις βασικές λειτουργίες του εργαλείου είναι η δημιουργία DNS ερωτημάτων με σκοπό την εύρεση των διακομιστών του στόχου. Το εργαλείο αφού βρει το διακομιστή, μπορεί να το χρησιμοποιήσει και να διαγράψει τα αρχεία SOA του κάτω υπό το πρίσμα ότι ο διακομιστής μπορεί να μην έχει σωστές ρυθμίσεις. Αν αυτό αποτύχει, το εργαλείο χρησιμοποιεί μέσω επίθεσης ωμής βίας (brute force attack) να μαντέψει ονόματα τα οποία εμφανίζονται συχνά σε εταιρείες και οργανισμούς. Στη συνέχεια, αν το εργαλείο βρει κάτι σε κάποια IP διεύθυνση, θα σαρώσει πάνω και κάτω από αυτή τη διεύθυνση σε ένα προκαθορισμένο εύρος χρησιμοποιώντας αντίστροφη αναζήτηση. Αν βρει κάτι στη δευτερεύουσα αναζήτηση, θα επιχειρήσει ξανά αναζήτηση στο προκαθορισμένο εύρος γύρω από αυτήν. Η λειτουργία αυτή μπορεί να παρουσιάζει μία καθυστέρηση αλλά όσο μεγαλύτερη η καθυστέρηση τόσο μεγαλύτερη η έκταση των αποτελεσμάτων.[Fierce,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

TcpFlow

Το εργαλείο αυτό καταγράφει τα δεδομένα που διαβιβάζονται στο πλαίσιο των TCP συνδέσεων, και αποθηκεύει τα δεδομένα κατά τρόπο τέτοιο που είναι κατάλληλος για την ανάλυση των πρωτοκόλλων ή τον εντοπισμό σφαλμάτων. Το tcpflow έχει την ικανότητα να παρουσιάζει μία περίληψη των πακέτων που ανταλάσσονται στην επικοινωνία. Επιπλέον, το tcpflow, ανακατασκευάζει τις πραγματικές ροές δεδομένων και αποθηκεύει κάθε ροή σε ξεχωριστό αρχείο για μετέπειτα ανάλυση. Αυτό συμβαίνει επειδή το tcpflow αντιλαμβάνεται τους αριθμούς ακολουθίας και έτσι μπορεί και ανακατασκευάζει σωστά τις ροές δεδομένων, ανεξάρτητα από αναμεταδόσεις ή

παραδόσεις πακέτων με λάθος σειρά.[TcpFlow,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Δικτύου.

Creepy

Το Creepy είναι μία απλή εφαρμογή που λαμβάνει τα ονόματα των χρηστών στο Twitter και το Flickr και εξάγει δεδομένα geolocation που περιέχουν πληροφορίες που έχουν δημοσιεύσει αυτοί οι χρήστες σε αυτές τις υπηρεσίες. Το ποσό της πληροφορίας που δημοσιεύεται με την ανάρτηση μίας φωτογραφίας με γεωγραφικό προσδιορισμό σε υπηρεσίες όπως το foursquare είναι τεράστιο. Το creepy επιτρέπει στο χρήστη να δει τις τοποθεσίες που άλλοι χρήστες με δημοσιευμένες φωτογραφίες ή πληροφορίες έχουν βρεθεί και να δημιουργήσει μία αλυσίδα με αυτές τις τοποθεσίες. Το εργαλείο είναι εξαιρετικά εύκολο στη χρήση. Ο χρήστης πληκτρολογεί το όνομα χρήστη στο Twitter η το Flickr και αφήνει το εργαλείο να αναζητήσει και να εξάγει αποτελέσματα. Μόλις η αναζήτηση ολοκληρωθεί, ο χρήστης θα λάβει ένα χάρτη με όλες τις τοποθεσίες που το εργαλείο. Εκτός από το χάρτη, τα αποτελέσματα συνθέτονται από μία λίστα με τις τοποθεσίες σε χρονολογική σειρά. Σε αυτή τη λίστα, ο χρήστης του Creepy μπορεί να κάνει δεξί κλικ και να περιηγηθεί μέσω του λογισμικού Google Maps στην ακριβή τοποθεσία.[Creepy,2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών.

Metagoofil

Το metagoofil είναι ένα εργαλείο που χρησιμοποιείται κατά τη συλλογή πληροφοριών. Πιο συγκεκριμένα, το εργαλείο χρησιμοποιείται για την εξαγωγή πληροφοριών από δημόσια έγγραφα (pdf, doc, xls, ppt) που ανήκουν σε μία εταιρεία στόχο. Αρχικά, το εργαλείο εκτελεί μία αναζήτηση στη μηχανή αναζήτησης Google, για να εντοπίσει και να κατεβάσει τα έγγραφα στο τοπικό δίσκο και στη συνέχεια, θα εξάγει μεταδεδομένα, με διαφορετικές βιβλιοθήκες, όπως HACHOIR, PdfMiner και άλλες. Τέλος, θα συγκεντρώσει τα αποτελέσματα σε μία αναφορά, με τα ονόματα, τις εκδόσεις του λογισμικού και των διακομιστών ή ακόμα και ονόματα μηχανημάτων για να βοηθήσει τους ελεγκτές μετέπειτα στις επόμενες φάσεις. [Metagoofil,2014] Στόχος του εργαλείο

είναι η εκμετάλλευση δημόσια δημοσιευμένων πληροφοριών προς όφελος του ελεγκτή.

theharvester

Το συγκεκριμένο εργαλείο έχει σαν στόχο να βοηθήσει τον ελεγκτή στα αρχικά στάδια του ελέγχου διείσδυσης να κατανοήσει το ηλεκτρονικό αποτύπωμα του (πελάτη) στόχου στο διαδίκτυο. Το εργαλείο είναι χρήσιμο στην οπτικοποίηση των πληροφοριών που υπάρχει στο διαδίκτυο για έναν οργανισμό και ενδεχομένως αυτές οι πληροφορίες να μπορούν να χρησιμοποιηθούν κακόβουλα.[theharvester, 2014] Ανήκει και αυτό όπως και τα προηγούμενα εργαλεία στη φάση της Συλλογής Πληροφοριών.

twofi

Το όνομα του εργαλείου twofi προέρχεται από τις λέξεις Twitter Words Of Interest και όπως φαίνεται από το όνομα του επιχειρεί αναζητήσεις μέσω Twitter για λέξεις με ιδιαίτερο ενδιαφέρον. Πιο συγκεκριμένα, χρησιμοποιεί την υπηρεσία κοινωνικής δικτύωσης Twitter για να δημιουργήσει λίστες βασισμένες σε αναζητήσεις πάνω σε ένα χρήστη, εντοπίζοντας λέξεις κλειδιά. Το αποτέλεσμα της αναζήτησης αυτής είναι μία λίστα από λέξεις-κλειδιά στοιχισμένες σε φθίνουσα σειρά και ακολουθούμενες με τη συχνότητα εμφάνισης της λέξης. Στόχος του εργαλείου είναι να συλλέξει και να οργανώσει τη δομή των πληροφοριών για ένα χρήστη και να τις προβάλλει με τρόπο κατανοητό.[twofi, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών.

DMitry

Το εργαλείο αυτό παίρνει το όνομα του από τα αρχικά των λέξεων Deepmagic Information Gathering Tool. Χρησιμοποιείται όπως φανερώνει και το όνομα του στη φάση της Συλλογής Πληροφοριών και έχει τη δυνατότητα να συλλέξει όσο το δυνατόν περισσότερες πληροφορίες για ένα κεντρικό υπολογιστή (host). Το εργαλείο είναι γραμμένο σε C, δίνοντας στο χρήστη μία γραμμή εντολών από την οποία εκτελεί

εντολές[Dmitry, 2014]. Η βασική λειτουργία του εργαλείου είναι οι αναζητήσεις whois, η εύρεση του χρόνου που μία υπηρεσία είναι ενεργή και να εκτελεί σαρωσεις TCP.

NetDiscover

Το netdiscover είναι ένα εργαλείο ενεργητικής και παθητικής συλλογής πληροφοριών δικτύων, κυρίως προορισμένο για σάρωση ασύρματων δικτύων χωρίς τη παρουσία dhcp διακομιστή. Ο στόχος του εργαλείου είναι να βοηθήσει τον ελεγκτή να συλλέξει πληροφορίες σχετικές με τα δίκτυα στη φάση της Συλλογής Πληροφοριών. Το εργαλείο μπορεί να χρησιμοποιηθεί και σε δίκτυα με μεταγωγέα (switch) ή με κόμβο (hub). Είναι κατασκευασμένο πάνω στο libnet και libcap και μπορεί με χρήση παθητικής αναζήτησης να ανευρίσκει συνδεδεμένα μηχανήματα ή να τα αναζητήσει ενεργά με την αποστολή ARP πακέτων. Επιπλέον, το εργαλείο μπορεί να χρησιμοποιηθεί για την επιθεώρηση της κυκλοφορίας του arp δικτύου του χρήστη ή για να βρει διευθύνσεις στο δίκτυο χρησιμοποιώντας τη λειτουργία αυτόματης σάρωσης [NetDiscover, 2014].

arping

Το arping είναι ένα εργαλείο λογισμικού που χρησιμοποιείται για να ανακαλύψει υπολογιστές (μηχανήματα) σε ένα δίκτυο υπολογιστών. Το λογισμικό ελέγχει αν μία διεύθυνση είναι ήδη σε χρήση στο τοπικό δίκτυο και μπορεί να λάβει επιπλέον πληροφορίες σχετικά με τον υπολογιστή που χρησιμοποιεί τη διεύθυνση. Το εργαλείο arping λειτουργεί με τρόπο που είναι ανάλογος με την εντολή ping, το οποίο ανιχνεύει υπολογιστές μέσω του πρωτοκόλλου ICMP. Η διαφορά εδώ είναι ότι ενώ το ICMP πρωτόκολλο έχει δυνατότητα δρομολόγησης καθώς λειτουργεί στο τρίτο επίπεδο της διασύνδεσης των συστημάτων OSI, το ARP δεν έχει αυτή τη δυνατότητα καθώς λειτουργεί στο δεύτερο επίπεδο. Έτσι, το εργαλείο λειτουργεί μόνο στο τοπικό δίκτυο. Υπάρχουν δύο βασικές υλοποιήσεις του εργαλείου, η μία είναι εκείνη που βρίσκεται κάτω από το πακέτο προγραμμάτων iputils και δεν έχει τη δυνατότητα ανεύρεσης MAC διευθύνσεων και εκείνη που είναι γραμμένη από τον Thomas Habets και έχει την

προηγούμενη δυνατότητα[arping, 2014]. Ο στόχος του εργαλείου είναι η αναγνώριση του δικτύου και η ανεύρεση πληροφοριών σχετικά με αυτό.

fping

Το εργαλείο fping μοιάζει στη λειτουργία του με την εντολή ping το οποίο χρησιμοποιεί μηνύματα πρωτοκόλλου ICMP για να ανιχνεύσει μηχανήματα, μόνο που το fping διαφέρει στη δυνατότητα καθορισμού οποιουδήποτε αριθμού στόχων μέσω της γραμμής εντολών. Επιπλέον, δίνεται η δυνατότητα ο καθορισμός στόχων να γίνει μέσω καθορισμού αρχείου που τους περιέχει σε λίστα. Στην προεπιλεγμένη λειτουργία του, το εργαλείο θα στείλει ένα πακέτο και θα συνεχίσει να στείλει στον επόμενο ακολουθώντας τον αλγόριθμο round robin. Εάν κάποιος στόχος απαντήσει, τότε σημειώνεται και αφαιρείται από τη λίστα των στόχων προς έλεγχο. Εάν ένας στόχος δεν απαντήσει μέσα σε ένα προκαθορισμένο χρονικό διάστημα, τότε σημειώνεται σαν απρόσιτος.[fping, 2014] Το εργαλείο μοιάζει με το εργαλείο arping όσον αφορά στη βασική λειτουργία και μοιράζονται τον ίδιο στόχο, την αναγνώριση του δικτύου.

hping

Το hping είναι ένας αναλυτής και εργαλείο συναρμολόγησης πακέτων TCP/IP. Παρέχει στο χρήστη μια γραμμή εντολών και όχι μία γραφική διεπαφή και είναι εμπνευσμένο από την εντολή ping των unix συστημάτων όπως και τα προηγούμενα εργαλεία. Το εργαλείο διαφέρει στο ότι δεν είναι μόνο σε θέση να στείλει ICMP μηνύματα αλλά και να υποστηρίξει επιπλέον τα πρωτόκολλα TCP, UDP, RAW-IP, παρέχει δυνατότητα ανίχνευσης διαδρομής πακέτων (traceroute) και δυνατότητα αποστολής αρχείων μεταξύ κρυφών καναλιών.[hping, 2014] Ο στόχος του εργαλείου είναι η αναγνώριση του δικτύου και η συλλογή πληροφοριών για αυτό.

ncat

Το ncat είναι ένα εργαλείο που χρησιμοποιείται για ανάγνωση, γραφή, ανακατεύθυνση και κρυπτογράφηση των δεδομένων μέσα στο δίκτυο. Είναι άλλο ένα εργαλείο με γραμμή εντολών και όχι με γραφική διεπαφή όπως τα περισσότερα εργαλεία σε αυτές

τις φάσεις. Στόχος του εργαλείου είναι να λειτουργεί σαν ένας ελβετικός σουγιάς για τους ελεγκτές ασφάλειας ή τους διαχειριστές συστημάτων. Το ncat είναι κατάλληλο για διαδραστική χρήση ή για βοηθητικό εργαλείο ως προς άλλα εργαλεία. Το ncat λειτουργεί ως εξής: σαν ένας απλός TCP/UDP/SCTP/SSL εξυπηρετητής ο οποίος αλληλεπιδρά με διακομιστές διαδικτύου, telnet, εξυπηρετητής ηλεκτρονικής αλληλογραφίας, και άλλες υπηρεσίες του πρωτοκόλλου TCP/IP. Επίσης, το εργαλείο μπορεί να χρησιμοποιηθεί σαν δρομολογητής ανακατεύθυνσης ή μεσολάβησης της κυκλοφορίας των δεδομένων σε άλλες θύρες ή κεντρικούς υπολογιστές. Υποστηρίζει τεχνικές κρυπτογράφησης των πληροφοριών και τη μεταφορά τους στα πρωτόκολλα IPv4 και IPv6. Ακόμα, το ncat μπορεί να δράσει ως ενδιάμεσος σε σύνδεση δύο η περισσοτέρων εξυπηρετητών. Αυτό επιτρέπει πολλαπλά μηχανήματα που κρύβονται πίσω από NAT να επικοινωνούν μεταξύ τους.[ncat, 2014] Τέλος, το εργαλείο μπορεί να εγκατασταθεί σε όλα τα γνωστά λειτουργικά συστήματα. Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών και της Αναγνώρισης Δικτύου.

dnschef

Το dnschef είναι ένα ιδιαίτερα διαμορφώσιμο εργαλείο που λειτουργεί σαν ένας DNS διακομιστής μεσολάβησης που απευθύνεται σε ελεγκτές ασφάλειας και διαχειριστές συστημάτων. Ένας DNS διακομιστής μεσολάβησης ή αλλιώς και ψεύτικος DNS διακομιστής χρησιμοποιείται για την ανάλυση κίνησης τους δικτύου σε επίπεδο εφαρμογής. Για παράδειγμα, μπορεί να χρησιμοποιηθεί με σκοπό την αποστολή ψευδών αιτημάτων προς μία τρίτη ιστοσελίδα ώστε να οδηγήσει ένα μηχάνημα σε τερματισμό ή να υποκλέψει την κίνηση του. Η διαφορά του dnschef σε σχέση με άλλα παρόμοια εργαλεία, είναι ο μεγάλος βαθμός παραμετροποίησης του. Το γεγονός αυτό πηγάζει από το σκοπό τον οποίο υπηρετεί το εργαλείο αυτό, ο οποίος είναι η διενέργεια ενός ελέγχου διείσδυσης. Υποστηρίζεται σε πολλά λειτουργικά συστήματα, μπορεί να χρησιμοποιήσει λίστες αποκλεισμού, υποστηρίζει διάφορους τύπους αρχείων DNS, την αντιστοιχία διακομιστών με τη χρήση wildcards και τη ανακατεύθυνση μηνυμάτων σε διακομιστές που δεν έχουν αντιστοιχισθεί.[dnschef, 2014] Η χρήση του εργαλείου συνίσταται όταν δεν είναι δυνατή η αλλαγή του διακομιστή που χρησιμοποιεί μία εφαρμογή με άμεσο τρόπο.

dsniff

Το dsniff δεν αποτελεί από μόνο του ένα εργαλείο αλλά μία συλλογή από εργαλεία για τον έλεγχο του δικτύου και των ελέγχων διείσδυσης. Τα εργαλεία που βρίσκονται στο dsniff είναι τα filesnarf, msgsnarf, urlsnarf, webspy. Αυτά χρησιμοποιούνται για την παθητική παρακολούθηση ενός δικτύου για ενδιαφέρονται στοιχεία, όπως είναι: κωδικοί πρόσβασης, διευθύνσεις email, αρχεία κ.ά. Επίσης, υπάρχουν τα arpspoof, dsnsspoof, macof που χρησιμοποιούνται για την υποκλοπή πληροφοριών που κανονικά δεν είναι διαθέσιμες στον επιτιθέμενο.[dsniff, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Συλλογής Πληροφοριών και Αναγνώρισης Δικτύου.

3.1.2 Αναγνώριση Τρωτοτήτων (Vulnerability Identification)

Nessus

Το εργαλείο Nessus είναι αυτή τη στιγμή το πιο δημοφιλές εργαλείο σάρωσης, ανίχνευσης και αναγνώρισης τρωτοτήτων παγκοσμίως. Δίνει τη δυνατότητα στον ελεγκτή να αξιολογήσει απομακρυσμένα την ασφάλεια ενός συστήματος και να εξακριβώσει εάν αυτό παραβιάστηκε ή έγινε αντικείμενο κατάχρησης. Οι λειτουργίες του Nessus είναι πολλές. Μεταξύ αυτών, οι πιο σημαντικές είναι:

- Αρθρωτός χαρακτήρας, η αρχιτεκτονική εξυπηρετητή/διακομιστή παρέχει την ευελιξία στον ελεγκτή να αναπτύξει το εργαλείο με τρόπο που τον εξυπηρετεί και να συνδεθεί στο GUI από οποιοδήποτε μηχάνημα με ένα απλό πρόγραμμα περιήγησης, μειώνοντας τα κόστη διαχείρισης.
- Έξυπνη Σάρωση, σε αντίθεση με πολλούς σαρωτές ασφάλειας το Nessus δε θεωρεί τίποτα δεδομένο. Δηλαδή, δεν πραγματοποιεί υποθέσεις περί της ύπαρξης μίας υπηρεσίας σε μία θύρα. Αυτό σημαίνει ότι αν ο διακομιστής του διαδικτύου λειτουργεί στη θύρα 1234, το Nessus θα το βρει και θα δοκιμάσει τα επίπεδα ασφάλειας του κατάλληλα.
- Συμβατότητα με CVE, τα περισσότερα plugins του εργαλείου είναι συνδεδεμένα με τα αντίστοιχα CVE, έτσι ώστε οι ελεγκτές ή διαχειριστές του συστήματος να ανατρέχουν εκεί για περισσότερες πληροφορίες.
- Αρχιτεκτονική Plugin, κάθε έλεγχος ασφάλειας είναι συσχετισμένος με ένα plugin και ομαδοποιημένος σε μία από 42 οικογένειες ελέγχων. Με αυτό τον τρόπο ο χρήστης μπορεί να εισάγει τους δικούς του ελέγχους να διαλέξει με

κριτήριο την οικογένεια αυτών, χωρίς να χρειαστεί να γνωρίζει τι κάνει ο κάθε ένας ξεχωριστά.

- Υποστηρίζει τη γλώσσα NASL, μία γλώσσα η οποία γράφτηκε με σκοπό τη συγγραφή ελέγχων ασφαλείας εύκολα και γρήγορα.
- Συχνές αναβαθμίσεις, η βάση τρωτοτήτων ενημερώνεται σε καθημερινή βάση.
- Έλεγχος σε πολλαπλούς στόχους, υποστηρίζεται ο πολλαπλός και ταυτόχρονος έλεγχος.
- Συνεργασία plugin, το εργαλείο επιτρέπει συνεργασία των plugins του με τέτοιο τρόπο έτσι ώστε αν κάποιος έλεγχος έχει πραγματοποιηθεί ήδη από κάποιο plugin και ζητηθεί από κάποιο άλλο να αγνοηθεί. Με αυτό τον τρόπο περιττοί έλεγχοι δεν εκτελούνται.
- Πλήρης Αναφορές, το εργαλείο δεν προσφέρει μόνο αναγνώριση τρωτοτήτων αλλά και αναγνώριση της απειλής που εμπεριέχεται με κατηγοριοποίηση. Πέρα από αυτή τη λειτουργία, προσφέρει μέτρα για μετριασμό των απειλών.
- Πλήρης υποστήριξη SSL, το Nessus επιτρέπει τον έλεγχο υπηρεσιών που χρησιμοποιούν το SSL πρωτόκολλο.

Σκοπός του εργαλείου όσον αφορά στον έλεγχο διείσδυσης είναι η αναγνώριση των τρωτοτήτων ώστε να επιλεχθούν οι αντίστοιχες επιθέσεις στην επόμενη φάση.[Nessus, 2014] Πέρα από αυτό, δίνει τη δυνατότητα σύνταξης εκείνου του μέρους της αναφοράς σχετικά με την αντιμετώπιση των απειλών.

Core Impact

Το Core Impact αποτελεί λογισμικό για τη διενέργεια κυβερνο-επιθέσεων (cyber attacks) σε απομακρυσμένους στόχους. Σκοπός του είναι η αξιολόγηση της ασφάλειας διαδικτυακών εφαρμογών, δικτυακών συστημάτων, κινητών συσκευών, χρηστών και ασύρματων δικτύων. Το εργαλείο είναι ικανό να:

- Σαρώσει διακομιστές του δικτύου, σταθμούς εργασίας (workstations), τείχη προστασίας (firewalls), δρομολογητές και διάφορες εφαρμογές για τρωτά σημεία.
- Προσδιορίσει ποιες τρωτότητες υπάρχουν και ποιες αποτελούν πραγματικό κίνδυνο για το σύστημα.

- Προσδιορίσει τις πιθανές επιπτώσεις από την εκμετάλλευση των τρωτοτήτων.
- Ιεραρχήσει και να εκτελέσει προσπάθειες αποκατάστασης της ασφάλειας του συστήματος.

Το εργαλείο είναι ένα ολοκληρωμένο λογισμικό ελέγχου διείσδυσης. Όπως φαίνεται και από τις λειτουργίες του, μπορεί να υποστηρίξει όλες τις σημαντικές φάσεις ενός ελέγχου διείσδυσης.[Core Impact, 2014] Για το λόγο αυτό, θα μπορούσε να συμπεριληφθεί σε οποιοδήποτε φάση. Αναφέρεται στη φάση της Εκμετάλλευσης διότι η εταιρεία που το παρέχει ρίχνει μεγαλύτερο βάρος στις αντίστοιχες λειτουργίες.

OpenVas

Το OpenVas αποτελεί ένα ολοκληρωμένο λογισμικό που συνίσταται από διάφορες υπηρεσίες και εργαλεία. Προσφέρει ένα ολοκληρωμένο σύστημα αναγνώρισης τρωτοτήτων αλλά και διαχείρισης αυτών. Ο σαρωτής τρωτοτήτων είναι συνδεδεμένος με μία βάση ελέγχων που ανανεώνεται καθημερινά και περιέχει 35,000 ελέγχους (Απρίλιος 2014). Το εργαλείο δίνεται δωρεάν και βρίσκεται υπό την εποπτεία του General Public License (GNU GPL). [OpenVas, 2014] Σκοπός του εργαλείου είναι να υποστηρίξει τη φάση της Αναγνώρισης Τρωτοτήτων σε έναν έλεγχο διείσδυσης με το καλύτερο δυνατό τρόπο ή να ενημερώσει το διαχειριστή του συστήματος για τους πιθανούς κινδύνους.

Nexpose

Το Nexpose δεν αποτελεί εργαλείο αλλά σουίτα εργαλείων με βασική λειτουργία την αναγνώριση τρωτοτήτων. Στόχος του εργαλείου είναι να υποστηρίξει όλες τις φάσεις του κύκλου ζωής της διαχείρισης τρωτοτήτων. Αυτό πρακτικά σημαίνει ότι το εργαλείο υποστηρίζει την αναγνώριση, επαλήθευση, ταξινόμηση (σε τάξεις επικινδυνότητας) ανάλυση επιπτώσεων, υποβολή έκθεσης και μετριασμό των τρωτοτήτων ενός συστήματος. Επιπλέον, μπορεί να χρησιμοποιηθεί σε συνεργασία με το Metasploit καθώς οι λειτουργίες του μπορούν να ενσωματωθούν με αυτό. Η άδεια χρήσης του δεν είναι δωρεάν καθώς αποτελεί εμπορικό προϊόν (αν και υπάρχει μία με ιδιαίτερα περιορισμένες δυνατότητες). Πιο συγκεκριμένα, το εργαλείο έχει δυνατότητα εκτέλεσης των παρακάτω λειτουργιών:

- Αναγνώριση αγαθών, αυτόματη λειτουργία αναγνώρισης αγαθών και απογραφής αυτών. Εύκολη οργάνωση αυτών σε λογικές ομάδες για τη καλύτερη διαχείριση τους
- Αναγνώριση τρωτοτήτων και σύνδεση αυτών με λανθασμένες ρυθμίσεις
- παραβιάσεις πολιτικών, έκθεση σε ιομορφικό λογισμικό
- Ιεράρχηση απειλών, η οποία γίνεται όχι μόνο με τη βοήθεια της βαθμολογίας CVSS αλλά και με τη συνεργασία άλλων παραγόντων
- Επαλήθευση Τρωτοτήτων, η οποία επιτυγχάνεται από τη συνέργεια του Nexpose με το Metasploit
- Δημιουργία Αναφοράς με σαφή βήματα μετριασμού Απειλών, το εργαλείο έχει τη δυνατότητα δημιουργίας αναφοράς ώστε να ρυθμιστούν κατάλληλα οι έλεγχοι και την αποστολή εκθέσεων αποκατάσταση στην ομάδα με οδηγίες για μετριασμό της επικινδυνότητας. [Nexpose, 2014]

Tripwire IP360

Το Tripwire IP360 είναι ένα ολοκληρωμένο σύστημα αναγνώρισης τρωτοτήτων και μετριασμού επικινδυνότητας. Το εργαλείο απευθύνεται σε μεγάλες εταιρείες και οργανισμούς. Η άδεια χρήσης του είναι εμπορική. Το εργαλείο παρέχει πλήρη ορατότητα στο εταιρικό δίκτυο, συμπεριλαμβανομένων των λειτουργικών τους συστημάτων. Το εργαλείο διατηρείται ενημερωμένο καθώς υπάρχουν συνεχείς καθημερινές αναβαθμίσεις με ακριβείς, μη-παρεμβατικές υπογραφές που είναι συναφείς με μεγάλες επιχειρήσεις. Το tripwire χρησιμοποιεί προηγμένες τεχνικές ανάλυσης και ένα ποσοτικό αλγόριθμο βασισμένο σε διάφορους παράγοντες όπως είναι ο βαθμός τρωτότητας και η επιχειρησιακή σχετική αξία του αγαθού. Το αποτέλεσμα της ανάλυσης που πραγματοποιείται είναι αξιοποιήσιμα δεδομένα που επιτρέπουν στην ομάδα ελέγχου να επικεντρωθούν στην επίλυση των προβλημάτων μειώνοντας τη συνολική επικινδυνότητα χρησιμοποιώντας τους ελάχιστους δυνατούς πόρους. [Tripwire IP360, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Αναγνώρισης Τρωτοτήτων.

BeyondTrust Retina

Το εργαλείο Retina της BeyondTrust είναι άλλο ένα εργαλείο για την αναγνώριση Τρωτοτήτων και την αντιμετώπιση της επικινδυνότητας. Το εργαλείο έχει εμπορική άδεια και δε διατίθεται δωρεάν. Είναι εστιασμένο σε μεγάλες εταιρείες και τα προβλήματα ασφάλειας που εμφανίζονται σε επιχειρησιακό επίπεδο. Το εργαλείο πραγματοποιεί αναγνώριση δικτύου, αναγνώριση λειτουργικών συστημάτων, εφαρμογών και βάσεων δεδομένων. Στη συνέχεια, πραγματοποιεί εκτίμηση της επικινδυνότητας και ιεράρχηση των ενεργειών αποκατάστασης βασισμένη σε ενέργειες εκμετάλλευσης που έχουν προηγηθεί σε συνεργασία με άλλα εργαλεία. Το Retina συνεργάζεται πολύ καλά με τα Core Impact, Metasploit, Exploit-db. Τέλος, το εργαλείο εμφανίζει μία αναφορά για διαχείριση και έλεγχο των απειλών. Τέλος, το εργαλείο Retina υποστηρίζει πλήρως περιβάλλοντα εικονικών μηχανών.[BeyondTrust Retina, 2014] Το εργαλείο χρησιμοποιείται στη φάση της Συλλογής Πληροφοριών και Αναγνώρισης Τρωτοτήτων.

3.1.3 Vulnerability Exploitation

Metasploit

Το Metasploit είναι μία προηγμένη πλατφόρμα λογισμικού ανοιχτού κώδικα για την ανάπτυξη, δοκιμή και χρήση κώδικα προς εκμετάλλευση συστημάτων. Το εργαλείο χρησιμοποιεί ένα επεκτάσιμο μοντέλο του οποίου στοιχεία είναι το ωφέλιμο φορτίο (payload), κωδικοποιητές (encoders), γεννήτριες no-op και ο κώδικας εκμετάλλευσης. Αυτό το μοντέλο έχει καταστήσει το metasploit, το καλύτερο εργαλείο για διενέργεια ελέγχου διείσδυσης στη φάση της Εκμετάλλευσης. Το εργαλείο παρέχει εκατοντάδες έτοιμες μονάδες κώδικα εκμετάλλευσης επιτρέποντας στο χρήστη να δει τα μέρη αυτών. Με αυτό τον τρόπο, δίνεται η δυνατότητα στο χρήστη να γράψει τις δικές του μονάδες. Τέλος, παρέχεται μαζί και το εργαλείο Metasploitable το οποίο είναι μία εικονική μηχανή Linux σκόπιμα κατασκευασμένη να έχει ανασφαλείς ρυθμίσεις, ώστε ο χρήστης να χρησιμοποιήσει λειτουργίες εκμετάλλευσης χωρίς να πλήξει πραγματικούς στόχους.[Metasploit, 2014] Το εργαλείο είχε δωρεάν άδεια χρήσης αλλά αγοράστηκε από τη Rapid7 και σήμερα υπάρχουν επί των πλείστων εμπορικές άδειες με τη δωρεάν έκδοση να είναι περιορισμένων δυνατοτήτων.

Immunity Canvas

Το εργαλείο Immunity Canvas καθιστά διαθέσιμες εκατοντάδες μονάδες κώδικα εκμετάλλευσης, ένα αυτοματοποιημένο σύστημα εκμετάλλευσης στόχων και ένα ολοκληρωμένο, αξιόπιστο πλαίσιο ανάπτυξης μονάδων κώδικα εκμετάλλευσης. Όπως φαίνεται από τις λειτουργίες του, σκοπός του εργαλείου είναι να πλήξει απομακρυσμένους στόχους με τη χρήση μονάδων κώδικα. Η χρήση του εργαλείου πραγματοποιείται κατά τη φάση της Εκμετάλλευσης. Το εργαλείο παρουσιάζει τα εξής χαρακτηριστικά:

- Υποστήριξη των περισσότερων λειτουργικών συστημάτων, Windows, Linux, MacOSX, όλα τα Python περιβάλλοντα.
- Υποστήριξη εκατοντάδων μονάδων κώδικα εκμετάλλευσης, επί του παρόντος περιέχονται 490 μονάδες με μηνιαίες αναβαθμίσεις – ανανεώσεις της βάσης.
- Υποστήριξη πολλών επιλογών στο ωφέλιμο φορτίο.
- Υποστήριξη δημιουργίας μονάδων κώδικα εκμετάλλευσης από το χρήστη.
- Υποστήριξη προϊόντος και υπηρεσίες συντήρησης μέσω συνδρομής.

Το εργαλείο χρησιμοποιείται κατά τη φάση της Εκμετάλλευσης. [Immunity Canvas, 2014]

3.1.4 Maintaining Access

Cymothoa

Το Cymothoa αποτελεί εργαλείο για δημιουργία κερκοπορτών στο σύστημα. Το εργαλείο χρησιμοποιεί κρυφή λειτουργία (stealth mode) για τις λειτουργίες του με αποτέλεσμα να μη γίνεται αντιληπτή η παρουσία του ή οι αλλαγές που προξενεί στο σύστημα. Η βασική λειτουργία του εργαλείου Cymothoa είναι η έγχυση κώδικα εκμετάλλευσης σε μία υπάρχουσα διαδικασία. Χρησιμοποιεί τη βιβλιοθήκη ptrace (διατίθεται σε όλα τα *nix συστήματα) για να χειριστεί διαδικασίες και να τις μολύνει. Μία ενδιαφέρουσα καινοτομία της τελευταίας έκδοσης είναι η προσομοίωση ενός χρονο-προγραμματιστή στο εσωτερικό μίας διαδικασίας. Αυτό κάνει δυνατό να γραφτεί μία μονάδα κώδικα και δεν απαιτείται η ύπαρξη ανεξάρτητης διαδικασίας ή νήματος (thread) για να τρέξει. Η καινοτομία αυτή ενισχύει ιδιαίτερα την κρυφή

λειτουργία του εργαλείου.[Cymothoa, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση της Διατήρησης Πρόσβασης.

John the Ripper

Το εργαλείο John the Ripper είναι ένα γρήγορο εργαλείο για σπάσιμο κωδικών χρηστών, που διατίθεται σε πολλές εκδόσεις λειτουργικών συστημάτων, Unix, DOS, BeOS, OpenVMS. Ο πρωταρχικός σκοπός του εργαλείου είναι η ανίχνευση αδύναμων κωδικών πρόσβασης. Το εργαλείο υποστηρίζει τα περισσότερα αρχεία κατακερματισμένων κωδικών εκτός από κάποιες ειδικές περιπτώσεις κρυπτογραφημένων κωδικών Unix συστημάτων (crypt3). [John The Ripper, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση Διατήρηση Πρόσβασης.

Hydra

Στην περίπτωση που ο ελεγκτής χρειαστεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα μέσω επίθεσης ωμής βίας (brute force attack), το εργαλείο Hydra προκρίνεται ως το καλύτερο. Το εργαλείο αυτό μπορεί να εκτελέσει μέσα σε πολύ λίγο χρόνο επιθέσεις λεξικού (dictionary attacks) εναντίον σε παραπάνω από 30 πρωτόκολλα, συμπεριλαμβανομένου του telnet, ftp, http, https, smb και αρκετές βάσεις δεδομένων.[Hydra, 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση Διατήρηση Πρόσβασης.

Cain and Abel

Το Cain and Abel είναι ένα εργαλείο ανάκτησης κωδικών πρόσβασης για λειτουργικά συστήματα της Microsoft. Μπορεί εύκολα να επαναφέρει διάφορα είδη κωδικών πρόσβασης μέσω της ανίχνευσης πακέτων από το δίκτυο, σπάσιμο κρυπτογραφημένων κωδικών, επιθέσεων κρυπτανάλυσης, επιθέσεων καταγραφής VoIP συνομιλιών, αποκωδικοποίησης «μπερδεμένων» κωδικών (scrambled passwords) και επιθέσεων ανάκτησης κλειδιών ασύρματων δικτύων. Το πρόγραμμα δεν εκμεταλλεύεται αδυναμίες του συστήματος ή σφάλματα σε ρυθμίσεις αυτού. Το εργαλείο καλύπτει κάποιες πτυχές ασφάλειας και εκμεταλλεύεται κάποιες αδυναμίες που υπάρχουν στα

πρότυπα των πρωτοκόλλων ή στις μεθόδους αυθεντικοποίησης. Ο βασικός του σκοπός είναι η ανάκτηση κωδικών πρόσβασης από διάφορες πηγές.[Cain and Abel , 2014] Το εργαλείο χρησιμοποιείται κατά τη φάση Διατήρηση Πρόσβασης.

3.2 Σύγκριση

Όνομα Εργαλείου	Συλλογή Πληροφοριών-Αναγνώριση Δικτύου	Αναγνώριση Τρωτοτήτων	Εκμετάλλευση	Διατήρηση Πρόσβασης
Arping	✓			
ArpScan	✓			
Cain and Abel				✓
CoreImpact	✓	✓	✓	✓
Creepy	✓			
Cymothoa				✓
DMitry	✓			
DNSChef	✓			
DNSDict6	✓			
DNSEnum	✓			
DNSMap	✓			
DNSTracer	✓			
Dsniff	✓			
Fierce	✓			
Fping	✓			
Hping	✓			
Hydra				✓
Immunity Canvas			✓	

John The Ripper				✓
Maltego	✓			
Metagoofil	✓			
Metasploit		✓	✓	✓
Ncat	✓			
Nessus	✓	✓		
NetDiscover	✓			
Nexpose		✓		
Nmap	✓	✓		
OpenVas		✓		
SET	✓			
TCPflow	✓			
TheHarvester	✓			
Twofi	✓			
Wireshark	✓			

Πίνακας 5. Τα εργαλεία σε αλφαβητική σειρά και οι φάσεις του ελέγχου διείσδυσης που υποστηρίζουν.

4. Δημιουργία Προτύπου Αναφοράς

4.1 Σενάριο Προτύπου Αναφοράς

4.1.1 Εισαγωγή

Use Case Scenario – Company X

Το σενάριο αφορά την εταιρεία Χ. Η εταιρεία Χ είναι μία μικρή εταιρεία που δραστηριοποιείται στο τομέα των πωλήσεων. Για τους επιχειρηματικούς σκοπούς της, χρησιμοποιεί 5 (ή 6) μηχανήματα (ηλεκτρονικούς υπολογιστές). Η διαμόρφωση των μηχανημάτων περιγράφεται στην Ενότητα 3. Η εταιρεία Χ ζητά τη διενέργεια ελέγχου διείσδυσης από την εταιρεία Παπαθανασίου (Πτυχιακή Α.Ε.). Ο έλεγχος διείσδυσης ακολουθεί έλεγχο άσπρο κουτιού και περιλαμβάνει δραστηριότητες Συλλογής Πληροφοριών (Information Gathering) και Αναγνώρισης Τρωτοτήτων (Vulnerability Identification). Προαιρετικά, θα πραγματοποιηθεί και Επαλήθευση Τρωτοτήτων (Vulnerability Verification) για την εξάλειψη των false positives.

4.1.2 Συλλογή Πληροφοριών, Αναγνώριση Τρωτοτήτων και Επαλήθευση Τρωτοτήτων

Η Συλλογή Πληροφοριών διαχωρίζεται σε δύο μέρη. Το πρώτο μέρος είναι η Παθητική Συλλογή Πληροφοριών και το δεύτερο, η Ενεργητική Συλλογή Πληροφοριών. Η Ενεργητική Συλλογή Πληροφοριών θα πραγματοποιηθεί στα ψηφιακά μηχανήματα όπως αυτά περιγράφονται στην Ενότητα 3.

Σχετικά με την Παθητική Συλλογή Πληροφορίων, θα χρησιμοποιηθούν τα έξης εργαλεία:

- Maltego, μαζεύει πληροφορίες και περιγράφει τις σχέσεις μεταξύ ανθρώπων και οργανισμών,
- Creepy, μαζεύει πληροφορίες geolocation μέσω του Twitter και Flickr,
- Metagoofil, μαζεύει πληροφορίες αναζητώντας μεταδομένα από δημόσια έγγραφα που ανήκουν στην εταιρεία στόχο,
- Theharvester, πραγματοποιεί οπτικοποίηση πληροφοριών σχετικά με το αποτύπωμα του στόχου,
- Twofi, προβάλλει και μαζεύει πληροφορίες από το Twitter

Σχετικά με την Ενεργητική Συλλογή Πληροφοριών και την Αναγνώριση Τρωτοτήτων, θα χρησιμοποιηθούν τα εξής εργαλεία:

- Nmap,
- Nessus.

Σχετικά με την Επαλήθευση Τρωτοτήτων, θα χρησιμοποιηθούν (προαιρετικά) τα εξής εργαλεία:

- OpenVas ή
- Nexpose

4.1.3 Διαμόρφωση Μηχανημάτων

Η εταιρεία Χ για την εκπλήρωση των επιχειρηματικών σκοπών της, έχει τα εξής μηχανήματα στην κατοχή της, συνδεδεμένα σε ένα δρομολογητή.

- Windows XP SP3
- Windows 7 sp1
- Windows 7 sp3
- Windows 2008 Server
- Windows 2012 Server
- Linux Server, Metasploitable

Επίσης, σε ένα μηχάνημα είναι εγκατεστημένη μία βάση δεδομένων SQL, σε SQL server 2008.

Το report του ελέγχου βρίσκεται ολοκληρωμένο σε παράρτημα στο τέλος της εργασίας.

5. Επίλογος

Στην παρούσα πτυχιακή εργασία μελετήθηκαν οι τεχνικές ελέγχου διείσδυσης, τόσο σε επίπεδο μεθοδολογιών όσο και σε επίπεδο τεχνολογικών εργαλείων. Οι πιο γνωστές μεθοδολογίες αναλύθηκαν ανά φάση με σκοπό τον εντοπισμό τυχόν ιδιαιτεροτήτων και διαφοροποιήσεων από μεθοδολογία σε μεθοδολογία. Έγινε μία προσπάθεια εντοπισμού των κοινών γραμμών κάθε μεθοδολογίας και προτάθηκε μία ενοποιημένη μεθοδολογία με τις αντίστοιχες φάσεις.

Όσον αφορά το τεχνολογικό κομμάτι του ελέγχου διείσδυσης, προτάθηκε μία σειρά από τεχνολογικά εργαλεία ικανά να συνοδεύσουν τη μεθοδολογία που προτείνεται, σε κάθε φάση της. Τα εργαλεία αναλύθηκαν επαρκώς και ένας πίνακας με όλα τα εργαλεία ανά φάση παρουσιάστηκε συνοπτικά.

Επιπλέον, δημιουργήθηκε ένα εργαστηριακό περιβάλλον βάσει ενός σεναρίου στο οποίο πραγματοποιήθηκε έλεγχος διείσδυσης, χρησιμοποιώντας τη προτεινόμενη μεθοδολογία καθώς και ένα υποσύνολο των προτεινόμενων εργαλείων. Βάσει αυτού του ελέγχου, δημιουργήθηκε μία αναφορά προτείνοντας ουσιαστικά και ένα πρότυπο για μελλοντική χρήση.

Τέλος, κατά την εκπόνηση της εργασίας δημιουργήθηκε ένας Nessus parser για τη διευκόλυνση του ελεγκτή να διαμορφώσει ένα ευανάγνωστο κείμενο ικανό να εξηγήσει τις ιδιότητες της τρωτότητας, όπως είναι η περιγραφή της, οι ενέργειες για την εξάλειψη της και άλλες απαραίτητες αναφορές.

Η εργασία απευθύνεται σε όλους τους ερευνητές, επαγγελματίες του χώρου και οποιονδήποτε θα ήθελε να ασχοληθεί με το αντικείμενο της διενέργειας ελέγχου διείσδυσης σε δικτυακές υποδομές. Η εργασία είναι χρήσιμη ακόμα και για εκείνους που ψάχνουν έναν οδηγό για να υλοποιήσουν ελέγχους διείσδυσης γενικότερα.

5.1 Σχόλια και παρατηρήσεις

Όσον αφορά στις μεθοδολογίες, κατά την ανάλυση και περιγραφή των μεθοδολογιών, γίνονται γρήγορα αντιληπτά τα εξής:

1. Ο έλεγχος διείσδυσης είναι μία πολύπλοκη και απαιτητική διαδικασία, η οποία πρέπει να διενεργείται από ειδικούς του χώρου με εμπειρία και εξοικείωση σε θέματα ασφάλειας και όχι μόνο.
2. Δεν υπάρχει καλή ή κακή μεθοδολογία.
3. Δεν υπάρχει μεθοδολογία που να ταιριάζει σε κάθε περίπτωση. Η προτεινόμενη μεθοδολογία αποτελεί μία πρόταση που ενδεχομένως να εξυπηρετήσει ένα μεγάλο αριθμό ελέγχων αλλά σε καμία περίπτωση δεν αποτελεί πανάκεια.
4. Οι φάσεις της μεθοδολογίας είναι εξίσου σημαντικές.
5. Οι φάσεις της μεθοδολογίας εκτελούνται σειριακά. Η εκτέλεση των φάσεων με οποιαδήποτε άλλη σειρά θα οδηγήσει σε λανθασμένα αποτελέσματα.
6. Η φάση Σχεδιασμός - Προετοιμασία είναι η φάση εκείνη που συνήθως εκτελείται πλημμελώς ή και καθόλου από την ομάδα ελέγχου. Η φάση αυτή είναι η πρώτη φάση της μεθοδολογίας και μία κακή εκτέλεση εγγυάται λανθασμένα αποτελέσματα στις επόμενες φάσεις.
7. Η φάση Συλλογή Πληροφοριών είναι η φάση γεννήτορας για την επόμενη, την Αναγνώριση Τρωτοτήτων.
8. Η φάση της Αναγνώρισης Τρωτοτήτων ενδεχομένως να παράγει αποτελέσματα που είναι λανθασμένα. Η επαλήθευση των αποτελεσμάτων θα πρέπει να γίνεται απαραίτητα από την ομάδα ελέγχου ώστε να επιτυγχάνεται εγκυρότητα.
9. Η φάση της Εκμετάλλευσης είναι προαιρετική και αντικείμενο διαπραγμάτευσης κατά το Σχεδιασμό – Προετοιμασία. Αυτό δε σημαίνει ότι η σημαντικότητα της φάσης είναι ελάσσονος σημασίας.
10. Η δημιουργία μίας κατανοητής και συνοπτικής αναφοράς με τα αποτελέσματα του ελέγχου συνδεδεμένα με τις επιπτώσεις αποτελεί ένα στοίχημα για την ομάδα ελέγχου.

Βιβλιογραφία

[Antunes, 2009] Nuno Antunes, Marco Vieira, "Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services", 2009

[Duggan, 2009] David P. Duggan, "Penetration Testing of Industrial Control Systems ", 2009

[Alisherov & Sattarova, 2009] Farkhod Alisherov A., and Feruza Sattarova Y. , "Methodology for Penetration Testing ", 2009

[Alsopp, 2009] Wil Allsopp, "Unauthorized Access", 2009

[Xiong & Peyton, 2010] Pulei Xiong, Liam Peyton, "A Model-Driven Penetration Test Framework for Web Applications", 2010

[UI Haq, 2011] Muhammad Ehtsham Ul Haq, "Penetration Testing of Android-based Smartphones", 2011

[Van der Loo, 2011] Frank van der Loo, "Comparison of penetration testing tools for web applications", 2011

[Bau et al, 2010] Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell, "State of the Art: Automated Black-Box Web Application Vulnerability Testing", 2010

[Falkenberg, 2013] Andreas Falkenberg, "A new Approach towards DoS Penetration Testing on Web Services", 2013

[Mulliner, 2009] Collin Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", 2009

[Awad & Hassanien, 2013] Ali Ismail Awad Aboul Ella Hassanien, "Advances in Security of Information and Communication Networks", 2013

[Haubris & Pauli, 2013] *Kevin P. Haubris Joshua J. Pauli, "*Improving the Efficiency and Effectiveness of Penetration Test Automation", 2013

[Vieira & Madeira, 2009] José Fonseca Marco Vieira, Henrique Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks", 2009

[Igure et al, 2006] Vinay M. Igure, Sean A. Laughter, Ronald D. Williams, "Security issues in SCADA", 2006

[Vieira et al, 2009] Marco Vieira, Nuno Antunes, and Henrique Madeira, "Using web security scanners to detect vulnerabilities in web services", 2009

[Doupe et al, 2010] Adam Doup´e, Marco Cova, and Giovanni Vigna, "Why Johnny Can't Pentest: An Analysis of Black-Box Web Vulnerability Scanners",2010

[Shelly, 2010] David A. Shelly, "Using a web server test bed to analyze the limitations of web app vulnerability scanners", 2010

[Antunes et al, 2009] Nuno Antunes, Nuno Laranjeiro, Marco Vieira, Henrique Madeira, "Effective detection of SQL/ Xpath Injection vulnerabilities in web services", 2009

[Kiezun et al, 2009] Adam Kiezun, Phili Guo, Karthick Jayaraman, Michael D. Ernst, "Automatic creation of SQLi and XSS attacks", 2009

[Hudic et al, 2012] Aleksandar Hudic, Lorenz Zechner, Shareeful Islam, Christian Krieg, Edgar Weippl, Severin Winkler, Richard Habble, "towards a unified penetration testing taxonomy" , 2012

[Ralstona et al, 2011] P.A.S. Ralstona, J.H. Grahamb, J.L. Hiebb, "cyber security risk assessment for SCADA and DCS networks", 2011

[Halfond et al, 2011] William G. J. Halfond, Shauvik Roy Choudhary and Alessandro Orso, "improving penetration testing through static and dynamic analysis", 2011

[Austin & Williams, 2011] Andrew Austin and Laurie Williams, "one technique is not enough", 2011

[ISSAF et al, 2006] Rathore, Brunner, Dilaj, Herrera, Brunati, Subramaniam, Raman, Chavan, "Information Systems Security Assessment Framework", 2006

[NIST, 2008] Karen Scarfone, Murugiah Souppaya, Amanda Cody, Angela Orebaugh, "NIST Technical Guide to Information Security Testing and Assessment", 2008

[OSSTMM, 2008] Pete Herzog, "OSSTMM Open Source Security Testing Methodology Manual", 2008

[PTF, 2014] Kev Orrey, Lee J Lawson, 2014 "Penetration Testing Framework", διαθέσιμο στην ιστοσελίδα http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

[PTES, 2014] Chris Nickerson,Dave Kennedy, Chris John Riley, Eric Smith, Partner Iftach Ian Amit Andrew Rabie Stefan Friedli Justin Searle, Brandon Knight, Chris Gates, Joe McCray Carlos Perez John Strand Steve Tornio Nick PercocoDave ShackelfordVal SmithRobin Wood,WimRemes Rick Hayes, "Penetration Testing Execution Standard, διαθέσιμο στην ιστοσελίδα http://www.pentest-standard.org/index.php/Main_Page

[Wireshark, 2014] Wireshark tool, διαθέσιμο στην ιστοσελίδα https://www.wireshark.org/

[Nmap, 2014] Nmap tool, διαθέσιμο στην ιστοσελίδα www.nmap.org

[Maltego, 2014] Maltego tool, διαθέσιμο στην ιστοσελίδα https://www.paterva.com/web6/

[ArpScan, 2014] Arpscan tool, διαθέσιμο στην ιστοσελίδα http://www.nta-monitor.com/tools-resources/security-tools/arp-scan

[SET, 2014] Social Engineer Tool SET, διαθέσιμο στην ιστοσελίδα https://www.trustedsec.com/downloads/social-engineer-toolkit/

[DNSDict6, 2014] DNSDict6, διαθέσιμο στην ιστοσελίδα http://www.hackingloops.com/2013/03/dnsdict6-hack-tool-tutorial-know-your-backtrack.html#axzz3FIqtTZpx

[DNSEnum, 2014] DnsEnum, διαθέσιμο στην ιστοσελίδα http://www.netpro.me/dnsenum.html

[DNSMap, 2014] DnsMap tool, διαθέσιμο στην ιστοσελίδα http://www.aldeid.com/wiki/Dnsmap

[DNSTracer, 2014] DnsTracer, διαθέσιμο στην ιστοσελίδα http://www.mavetju.org/unix/dnstracer.php

[Fierce, 2014] Fierce tool, διαθέσιμο στην ιστοσελίδα http://ha.ckers.org/fierce/

[TcpFlow, 2014] TcpFlow tool, διαθέσιμο στην ιστοσελίδα http://www.circlemud.org/jelson/software/tcpflow/

[Creepy, 2014] Creepy tool, διαθέσιμο στην ιστοσελίδα http://creepy.en.softonic.com/

[Metagoofil, 2014] Metagoofil tool, διαθέσιμο στην ιστοσελίδα http://www.edge-security.com/metagoofil.php

[TheHarvester, 2014] TheHarvester tool, διαθέσιμο στην ιστοσελίδα https://code.google.com/p/theharvester/

[Twofi, 2014] Twofi tool, διαθέσιμο στην ιστοσελίδα http://www.raviramesh.net/2014/09/twofi.html

[Dmitry, 2014] Dmitry tool, διαθέσιμο στην ιστοσελίδα http://linux.die.net/man/1/dmitry

[NetDiscover, 2014] NetDiscover tool, διαθέσιμο στην ιστοσελίδα http://nixgeneration.com/~jaime/netdiscover/

[Arping, 2014] arping tool, διαθέσιμο στην ιστοσελίδα http://en.wikipedia.org/wiki/Arping

[Fping, 2014] fping tool, διαθέσιμο στην ιστοσελίδα http://fping.org

[Hping, 2014] hping tool, διαθέσιμο στην ιστοσελίδα http://www.hping.org/

[Ncat, 2014] ncat tool, διαθέσιμο στην ιστοσελίδα https://www.trustedsec.com/downloads/social-engineer-toolkit/

[DNSChef, 2014] Dnschef tool, διαθέσιμο στην ιστοσελίδα https://thesprawl.org/projects/dnschef/

[Dsniff, 2014] dsniff tool, διαθέσιμο στην ιστοσελίδα http://www.monkey.org/~dugsong/dsniff/

[Nessus, 2014] Nessus tool, διαθέσιμο στην ιστοσελίδα http://sectools.org/tool/nessus/

[CoreImpact, 2014] Core Impact Penetration tool, διαθέσιμο στην ιστοσελίδα http://sectools.org/tool/impact/

[OpenVas, 2014] OpenVas tool, διαθέσιμο στην ιστοσελίδα http://www.openvas.org/about.html

[Nexpose, 2014] Nexpose tool, διαθέσιμο στην ιστοσελίδα http://sectools.org/tool/nexpose/

[Metasploit, 2014] Metasploit tool, διαθέσιμο στην ιστοσελίδα http://help.metasploit.com/

[ImmunityCanvas, 2014] Immunity Canvas tool, διαθέσιμο στην ιστοσελίδα http://www.immunitysec.com/products-documentation.shtml

[Cymothoa, 2014] Cymothoa tool, διαθέσιμο στην ιστοσελίδα http://cymothoa.sourceforge.net/

[JohnTheRipper, 2014] John The Ripper tool, διαθέσιμο στην ιστοσελίδα http://www.openwall.com/john/

[Hydra, 2014] Hydra tool, διαθέσιμο στην ιστοσελίδα https://www.thc.org/thc-hydra/

[CainAndAbel, 2014] Cain and Abel tool, διαθέσιμο στην ιστοσελίδα http://www.oxid.it/cain.html

[TripwireIP360, 2014] Tripwire IP360 tool, διαθέσιμο στην ιστοσελίδα http://www.tripwire.com/it-security-software/enterprise-vulnerability-management/tripwire-ip360/

[BeyondTrust Retina, 2014] BeyondTrust Retina tool, διαθέσιμο στην ιστοσελίδα http://www.beyondtrust.com/Products/RetinaCSThreatManagementConsole/Τελευταία επίσκεψη 5/10/14

ΠΡΑΚΤΙΚΟ ΤΜΗΜΑ ΠΤΥΧΙΑΚΗΣ

1. Εισαγωγή

Το έγγραφο αυτό αποδίδει τα αποτελέσματα του ελέγχου διείσδυσης όπως αυτός πραγματοποιήθηκε από την Εταιρεία Παπαθανασίου στις δικτυακές υποδομές της Εταιρείας Χ. Όλοι οι έλεγχοι πραγματοποιήθηκαν εκτός της περιμέτρου της Εταιρείας Χ / εντός της περιμέτρου της Εταιρείας Χ.

1.1 Σκοπός

Ο βασικός σκοπός των δοκιμών που πραγματοποιήθηκαν είναι η αξιολόγηση του επιπέδου ασφάλειας της Εταιρείας Χ και η εναρμόνιση της, με τις πολιτικές ασφάλειας της και το ισχύον κανονιστικό πλαίσιο. Ο κύριος στόχος είναι η αναγνώριση τρωτοτήτων και η αναγνώριση της συνολικής επίπτωσης αυτών, στην Εταιρεία. -Εδώ αναφέρονται και οι άλλοι ενδεχομένως στόχοι που έχει η εταιρεία Χ και περιμένει από έναν έλεγχο διείσδυσης.- Είναι αποδεκτό το ενδεχόμενο μη εύρεσης τρωτοτήτων εξαιτίας του τύπου ελέγχου που επιλέχθηκε (αναφέρεται σε περιπτώσεις μαύρου ή γκρι κουτιού). Στο έγγραφο καταγράφονται τα ευρήματα τρωτοτήτων όπως ανακαλύφθηκαν από τον έλεγχο, καθώς και λύσεις για την αντιμετώπιση τους.

1.2 Εύρος Εφαρμογής

Τα συστήματα τα οποία βρίσκονται εντός του πεδίου εφαρμογής του ελέγχου διείσδυσης είναι τα εξής:

- Windows 7 sp3
- Windows Xp sp3
- Windows 7 sp1
- Windows Server 2008
- Mac OSX

Τα συστήματα βρίσκονται κάτω από τις εξής IP διευθύνσεις:

- 192.168.56.101
- 192.168.1.105
- 192.168.1.103
- 192.168.1.109
- 192.168.1.102

Όπως αυτά σαρωθήκαν από το σύνολο διευθύνσεων 192.168.1.1/24

2. Περίληψη των κυριότερων σημείων

Η Εταιρεία Χ προσφέρει διαφημιστικές υπηρεσίες στους πελάτες της μέσα από διαδικτυακές εφαρμογές. Για το λόγο αυτό, χρησιμοποιεί τα συστήματα Siebel CRM και SAP ERP. Εκτός από τα δύο προαναφερθέντα συστήματα η εταιρεία χρησιμοποιεί τη σουίτα εφαρμογών Microsoft Office, Microsoft Project, Adobe Photoshop καθώς και μία σειρά από καθημερινής χρήσης εφαρμογές (π.χ. Skype) καθώς και browsers. Επιθέσεις πάνω σε αυτά τα συστήματα, μπορούν να οδηγήσουν σε απώλεια του πελατολογίου της εταιρείας, των διαδικασιών και των workflows. Επιπλέον, μπορεί να οδηγήσουν σε διαρροή πληροφοριών που αφορούν επιχειρηματικές εργασίες της εταιρείας, λογιστικές πληροφορίες, επιχειρηματικά σχέδια, μεθόδους αγοράς και μεθόδους προώθησης, λίστες προμηθευτών και στρατηγικές διαφήμισης.

2.1 Φάσεις μεθοδολογίας Ελέγχου Διείσδυσης

Οι φάσεις της μεθοδολογίας είναι συνυφασμένες με τον τύπο ελέγχου που συμφωνήθηκε μεταξύ των δύο ενδιαφερομένων μελών και περιεγράφηκε στην προηγούμενη παράγραφο. Οι φάσεις μαζί με μία σύντομη επεξήγηση τους περιγράφονται παρακάτω.

Η φάση **Σχεδιασμός – Προετοιμασία** αφορά τις ενέργειες εκείνες που πραγματοποιούνται πριν τον έλεγχο Διείσδυσης, όπως είναι ο ορισμός ομάδας, ορισμός ρόλων, τήρηση ημερομηνιών και ορισμός εύρους εφαρμογής.

Η φάση **Συλλογή Πληροφοριών** αφορά τις ενέργειες εκείνες που δίνουν στοιχεία για το στόχο. Το βήμα αυτό εξαιρείται της διαδικασίας, εάν ο έλεγχος διείσδυσης ακολουθεί έλεγχο τύπου άσπρου κουτιού.

Η φάση **Αναγνώριση Τρωτοτήτων** αφορά τη σάρωση των μηχανημάτων του στόχου με διάφορα τεχνολογικά εργαλεία. Στόχος της είναι η εύρεση τρωτοτήτων και η αντιστοιχία τους με τις επιπτώσεις και τα αντίμετρα για το μετριασμό τους.

Η φάση **Επαλήθευση Τρωτοτήτων** χρησιμοποιεί τεχνικές απαλοιφής των λανθασμένων ευρημάτων μέσω της σύγκρισης αυτών από διαφορετικά εργαλεία.

Η **Δημιουργία Αναφοράς** αφορά τις ενέργειες που απαιτούνται για τη δημιουργία του παρόντος

2.2 Λίστα Τεχνολογικών Εργαλείων

Για την πραγματοποίηση του ελέγχου διείσδυσης, χρησιμοποιήθηκαν τα εξής τεχνολογικά εργαλεία.

1. Nmap, εργαλείο ανοιχτού κώδικα
2. Nessus Vulnerability Scanner, εργαλείο εμπορικής άδειας
3. Metasploit, εργαλείο ανοιχτού κώδικα
4. OpenVas, εργαλείο ανοιχτού κώδικα

3. Σύνοψη Συλλογής Πληροφοριών

Για την εκτέλεση της φάσης Συλλογή Πληροφοριών, χρησιμοποιήθηκε το εργαλείο nmap. Ακολουθούν πίνακες με τις πληροφορίες της σάρωσης από το εργαλείο. Οι πίνακες περιέχουν πληροφορίες.

3.1 Σύνοψη ανά Διεύθυνση

Ακολουθούν οι πίνακες με τις top 5 τρωτότητες όπως αυτές εμφανίζονται στην αναλυτική περιγραφή τους. (Ενότητα 3.2)

Όνομα Εξυπηρετητή	192.168.56.101
Ανοιχτές Θύρες	135/tcp, 445/tcp, 139/tcp
Ενεργές Υπηρεσίες	Microsoft Windows RPC139/tcp open netbios-ssn, microsoft-ds Microsoft Windows XP
OS Detection	Windows XP (Windows 2000 LAN Manager)
Computer Name	WXPPx86BE-6244

Όνομα Εξυπηρετητή	192.168.1.109
Ανοιχτές Θύρες	135/tcp, 445/tcp, 139/tcp, 2869/tcp, 5357/tcp, 49152/tcp, 49153/tcp, 49155/tcp, 49165/tcp, 49154/tcp, 49156/tcp,
Ενεργές Υπηρεσίες	Microsoft Windows RPC139/tcp open netbios-ssn, Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) open msrpc open msrpc open msrpc open msrpc open msrpc open msrpc
OS Detection	Windows 7 Home Premium 7601 Service Pack 1
Computer Name	ILIASBOUD2B8

Όνομα Εξυπηρετητή	192.168.56.102
Ανοιχτές Θύρες	-
Ενεργές Υπηρεσίες	-
OS Detection	OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Computer Name	-

Όνομα Εξυπηρετητή	192.168.1.105
Ανοιχτές Θύρες	88/tcp, 631/tcp, 548/tcp,
Ενεργές Υπηρεσίες	open kerberos-sec Heimdal Kerberos, open afp? open ipp CUPS 2.0
OS Detection	-
Computer Name	-

Όνομα Εξυπηρετητή	192.168.1.103
Ανοιχτές Θύρες	-

Ενεργές Υπηρεσίες	open kerberos-sec Heimdal Kerberos, open afp? open ipp CUPS 2.0
OS Detection	-
Computer Name	-

4. Σύνοψη Αναγνώρισης Τρωτοτήτων

Για την εκτέλεση της φάσης Συλλογή Πληροφοριών, χρησιμοποιήθηκε το εργαλείο nmap. Ακολουθούν πίνακες με τις πληροφορίες της σάρωσης από το εργαλείο. Οι πίνακες περιέχουν τις αντίστοιχες πληροφορίες.

4.1 Σύνοψη ανά Τρωτότητα

Ακολουθούν οι πίνακες με τις top 5 τρωτότητες όπως αυτές εμφανίζονται στην αναλυτική περιγραφή τους. (Ενότητα 3.2)

Τρωτότητα νο1

Όνομα Εξυπηρετητή	Windows XP sp3
IP Διεύθυνση	192.168.56.101
CVSS	10
Κόστος Διόρθωσης	Cost of Windows
Ευκολία Εντοπισμού	Πολύ Εύκολο
Συνέπειες	
Αντιμετώπιση	Upgrade to a version of Windows that is currently supported.

Τρωτότητα νο2

Όνομα Εξυπηρετητή	Mac OSX Yosemite
IP Διεύθυνση	192.168.1.105
CVSS	9.3

Κόστος Διόρθωσης	Μηδενικό
Ευκολία Εντοπισμού	Πολύ Εύκολο
Συνέπειες	Το μηχάνημα μπορεί να γίνει αντικείμενο πλήρης εκμετάλλευσης.
Αντιμετώπιση	Microsoft has released a set of patches for Office for Mac 2011, Office 2008 for Mac, and Open XML File Format Converter for Mac.

Τρωτότητα νο3

Όνομα Εξυπηρετητή	Mac OSX Yosemite
IP Διεύθυνση	192.68.56.101
CVSS	9.3
Κόστος Διόρθωσης	Μηδενικό
Ευκολία Εντοπισμού	Πολύ Εύκολο
Συνέπειες	
Αντιμετώπιση	Upgrade to Firefox 33.0 or later.

Τρωτότητα νο4

Όνομα Εξυπηρετητή	Mac OSX Yosemite
IP Διεύθυνση	192.68.56.101
	MS14-014: Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677) (Mac OS X)
CVSS	6.8
Κόστος Διόρθωσης	Μηδενικό
Ευκολία Εντοπισμού	Πολύ Εύκολο
Συνέπειες	
Αντιμετώπιση	Microsoft has released a patch for Silverlight 5.

Τρωτότητα νο5

Όνομα Εξυπηρετητή	Windows Server 2012r5
IP Διεύθυνση	192.168.56.102
	SMB Signing Required
CVSS	5.0

Κόστος Διόρθωσης	Μηδενικό
Ευκολία Εντοπισμού	Μέτριο
Συνέπειες	
Αντιμετώπιση	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'

4.2 Σύνοψη Αναγνώρισης Τρωτοτήτων ανά Όνομα Εξυπηρετητή

Host:192.168.1.109

Windows 7sp3

Όνομα ευπάθειας	Σημαντικότητα	Αξιολόγηση ευπάθειας	Κόστος Διόρθωσης	Ευκολία Εντοπισμού	Συνέπειες	Αντιμετώπιση	Αναφορά
SMB Signing Required	Medium	5.0			Signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	

Windows NetBIOS SMB Remote Host Information Disclosure	Informational	0			It is possible to obtain the network name of the remote host.	n/a	
Microsoft Windows SMB Log In Possible	Informational	0			It is possible to log into the remote host.	n/a	
Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Informational	0			It is possible to obtain network information.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	

DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
Microsoft Windows SMB NativeLan Manager	Informational	0			It is possible to obtain information about the remote	n/a	

Remote System Information Disclosure					operating system.		
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
OS Identification	Informational	0			It is possible to guess the remote operating system.	n/a	
Host Fully Qualified Domain Name (FQDN) Resolution	Informational	0			It was possible to resolve the name of the remote host.	n/a	
Authenticated Check: OS Name and	Informational	0			This plugin gathers information about the remote	n/a	

Installed Package Enumeration					host via an authenticated session.		
Nessus Scan Information	Informational	0			Information about the Nessus scan.	n/a	
Nessus Windows Scan Not Performed with Admin Privileges	Informational	0			The Nessus scan of this host may be incomplete due to insufficient privileges provided.	Reconfigure your scanner to use credentials with administrative privileges.	
Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Informational	0			Nessus is not able to access the remote Windows Registry.	n/a	
Ethernet Card Manufacturer Detection	Informational	0			The manufacturer can be deduced from the Ethernet OUI.	n/a	

Common Platform Enumeration (CPE)	Informational	0			It is possible to enumerate CPE names that matched on the remote system.	n/a	
Device Type	Informational	0			It is possible to guess the remote device type.	n/a	

Host:192.168.1.105

MacBook Pro. OSX Yosemite

Όνομα ευπάθειας	Σημαντικότητα	Αξιολόγηση ευπάθειας	Κόστος Διόρθωσης	Ευκολία Εντοπισμού	Συνέπειες	Αντιμετώπιση	Αναφορά
MS10-087: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930) (Mac OS X)	High	9.3			Arbitrary code can be executed on the remote host through Microsoft Office.	Microsoft has released a set of patches for Office for Mac 2011, Office 2008 for Mac, and Open XML File Format Converter for Mac.	CVE-2010-3333 , CVE-2010-3334 , CVE-2010-3335 , CVE-2010-3336
MS11-021 MS11-022 MS11-023: Vulnerabilities in Microsoft Office	High	9.3			Arbitrary code can be executed on the remote host through Microsoft Office.	Microsoft has released a set of patches for Office for Mac 2011, Office 2008 for	CVE-2011-0097 , CVE-2011-0098 , CVE-2011-0101 , CVE-2011-0103

Could Allow Remote Code Execution (2489279 2489283 2489293) (Mac OS X)						Mac, Office 2004 for Mac, and Open XML File Format Converter for Mac.	, CVE-2011-0104 , CVE-2011-0105 , CVE-2011-0655 , CVE-2011-0656 , CVE-2011-0976 , CVE-2011-0977 , CVE-2011-0978 , CVE-2011-0979 , CVE-2011-0980
MS11-036 MS11-045: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2545814 2537146) (Mac OS X)	High	9.3			Arbitrary code can be executed on the remote host through Microsoft Office.	Microsoft has released a set of patches for Office for Mac 2011, Office 2008 for Mac, Office 2004 for Mac, and Open XML File Format Converter for Mac.	CVE-2011-1269 , CVE-2011-1270 , CVE-2011-1272 , CVE-2011-1273 , CVE-2011-1274 , CVE-2011-1275 , CVE-2011-1276 , CVE-2011-1277 , CVE-2011-1278 , CVE-2011-1279
MS11-072: Vulnerabilities in Microsoft Excel Could Allow	High	9.3			Arbitrary code can be executed on the remote	Microsoft has released a set of patches for Office 2004 for Mac,	CVE-2011-1987 , CVE-2011-1988 , CVE-2011-1989

Remote Code Execution (2587505) (Mac OS X)					host through Microsoft Excel.	Office 2008 for Mac, Office for Mac 2011, and Open XML File Format Converter for Mac.	
MS11-089 MS11-094 MS11-096 : Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2590602 2639142 2640241) (Mac OS X)	High	9.3			Arbitrary code can be executed on the remote host through Microsoft Office.	Microsoft has released a patch for Office for Mac 2011, Office 2008 for Mac, and Office 2004 for Mac.	CVE-2011-1983 , CVE-2011-3403 , CVE-2011-3413
MS12-029 MS12-030: Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2680352 2663830) (Mac OS X)	High	9.3			Arbitrary code can be executed on the remote host through Microsoft Office.	Microsoft has released patches for Office for Mac 2011 and Office 2008 for Mac.	CVE-2012-0141 , CVE-2012-0142 , CVE-2012-0143 , CVE-2012-0183 , CVE-2012-0184 , CVE-2012-1847

MS12-076: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2720184) (Mac OS X)	High	9.3			It is possible to execute arbitrary code on the remote host through Microsoft Excel.	Microsoft has released a set of patches for Office for Mac 2011 and Office 2008 for Mac.	CVE-2012-1885 , CVE-2012-1886 , CVE-2012-1887 , CVE-2012-2543
MS13-051: Vulnerability in Microsoft Office Could Allow Remote Code Execution (2839571) (Mac OS X)	High	9.3			The remote Office for Mac install has a buffer overflow vulnerability.	Microsoft has released a patch for Office for Mac 2011.	CVE-2013-1331
MS13-052: Vulnerability in Silverlight Could Allow Remote Code Execution (2861561) (Mac OS X)	High	9.3			A browser enhancement on the remote Mac OS X host could allow arbitrary code execution.	Microsoft has released a patch for Silverlight 5.	CVE-2013-3178
MS13-073: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution	High	9.3			It is possible to execute arbitrary code on the remote host through Microsoft Excel.	Microsoft has released a patch for Office for Mac 2011.	CVE-2013-1315 , CVE-2013-3158 , CVE-2013-3159

(2858300) (Mac OS X)							
MS13-085: Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2885080) (Mac OS X)	High	9.3			It is possible to execute arbitrary code on the remote host through Microsoft Excel.	Microsoft has released a patch for Office for Mac 2011.	CVE-2013-3889 , CVE-2013-3890
Firefox < 27.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is potentially affected by multiple vulnerabilities.	Upgrade to Firefox 27.0 or later.	CVE-2014-1477 , CVE-2014-1478 , CVE-2014-1479 , CVE-2014-1480 , CVE-2014-1481 , CVE-2014-1482 , CVE-2014-1483 , CVE-2014-1485 , CVE-2014-1486 , CVE-2014-1487 , CVE-2014-1488 , CVE-2014-1489 , CVE-2014-1490 , CVE-2014-1491

Firefox < 28.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is potentially affected by multiple vulnerabilities.	Upgrade to Firefox 28.0 or later.	CVE-2014-1493 , CVE-2014-1494 , CVE-2014-1496 , CVE-2014-1497 , CVE-2014-1498 , CVE-2014-1499 , CVE-2014-1500 , CVE-2014-1502 , CVE-2014-1504 , CVE-2014-1505 , CVE-2014-1508 , CVE-2014-1509 , CVE-2014-1510 , CVE-2014-1511 , CVE-2014-1512 , CVE-2014-1513 , CVE-2014-1514
MS14-017: Vulnerabilities in Microsoft Word and Office Web Apps Could Allow Remote	High	9.3			The remote host is affected by a remote code execution vulnerability.	Microsoft has released a patch for Office for Mac 2011.	CVE-2014-1761

Code Execution (2949660) (Mac OS X)							
Firefox < 29.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is potentially affected by multiple vulnerabilities.	Upgrade to Firefox 29.0 or later.	CVE-2014-1492 , CVE-2014-1518 , CVE-2014-1519 , CVE-2014-1522 , CVE-2014-1523 , CVE-2014-1524 , CVE-2014-1525 , CVE-2014-1526 , CVE-2014-1529 , CVE-2014-1530 , CVE-2014-1531 , CVE-2014-1532
Firefox < 30.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is affected by multiple vulnerabilities.	Upgrade to Firefox 30.0 or later.	CVE-2014-1533 , CVE-2014-1534 , CVE-2014-1536 , CVE-2014-1537 , CVE-2014-1538 , CVE-2014-1539 , CVE-2014-1540 , CVE-2014-

							1541 , CVE-2014-1542
Firefox < 31.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is affected by multiple vulnerabilities.	Upgrade to Firefox 31.0 or later.	CVE-2014-1544 , CVE-2014-1547 , CVE-2014-1548 , CVE-2014-1549 , CVE-2014-1550 , CVE-2014-1552 , CVE-2014-1555 , CVE-2014-1557 , CVE-2014-1558 , CVE-2014-1559 , CVE-2014-1560 , CVE-2014-1561
Firefox < 32.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is affected by multiple vulnerabilities.	Upgrade to Firefox 32.0 or later.	CVE-2014-1553 , CVE-2014-1554 , CVE-2014-1562 , CVE-2014-1563 , CVE-2014-1564 , CVE-2014-1565 , CVE-2014-1567
MS14-061: Vulnerability in	High	9.3			The remote host is affected by a	Microsoft has released a patch	CVE-2014-4117

Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)					remote code execution vulnerability.	for Office for Mac 2011.	
Firefox < 33.0 Multiple Vulnerabilities (Mac OS X)	High	9.3			The remote Mac OS X host contains a web browser that is affected by multiple vulnerabilities.	Upgrade to Firefox 33.0 or later.	CVE-2014-1574 , CVE-2014-1575 , CVE-2014-1576 , CVE-2014-1577 , CVE-2014-1578 , CVE-2014-1580 , CVE-2014-1581 , CVE-2014-1582 , CVE-2014-1583 , CVE-2014-1584 , CVE-2014-1585 , CVE-2014-1586
Firefox < 32.0.3 NSS Signature Verification Vulnerability (Mac OS X)	High	8.8			The remote Mac OS X host contains a web browser that is affected by a signature forgery vulnerability.	Upgrade to Firefox 32.0.3 or later.	CVE-2014-1568

MS14-014: Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677) (Mac OS X)	Medium	6.8			A browser enhancement on the remote Mac OS X host is affected by a security feature bypass vulnerability.	Microsoft has released a patch for Silverlight 5.	CVE-2014-0319
MS12-051: Vulnerability in Microsoft Office for Mac Could Allow Elevation of Privilege (2721015)(Mac OS X)	Medium	4.4			It is possible to elevate privileges on the remote host through Microsoft Office.	Microsoft has released a patch for Office for Mac 2011.	CVE-2012-1894
MS13-026: Vulnerability in Office Outlook for Mac Could Allow Information Disclosure (2813682) (Mac OS X)	Medium	4.3			The remote Outlook for Mac install has an information disclosure vulnerability.	Microsoft has released patches for Office for Mac 2011 and Office 2008 for Mac.	CVE-2013-0095
MS13-087: Vulnerability in Silverlight Could Allow	Medium	4.3			A browser enhancement on the remote Mac OS X host is	Microsoft has released a patch for Silverlight 5.	CVE-2013-3896

Information Disclosure (2890788) (Mac OS X)					affected by an information disclosure vulnerability.		
Apple Filing Protocol Server Detection	Informational	0			An Apple file sharing service is listening on the remote port.	n/a	
Network Time Protocol (NTP) Server Detection	Informational	0			An NTP server is listening on the remote host.	n/a	
OS Identification	Informational	0			It is possible to guess the remote operating system.	n/a	
Authenticated Check: OS Name and Installed Package Enumeration	Informational	0			This plugin gathers information about the remote host via an authenticated session.	n/a	
Nessus Scan Information	Informational	0			Information about the Nessus scan.	n/a	
Software Enumeration (SSH)	Informational	0			It is possible to enumerate installed software on the remote host, via SSH.	Remove any software that is not in compliance with your organization's	

						acceptable use and security policies.	
Enumerate IPv6 Interfaces via SSH	Informational	0			This plugin enumerates IPv6 interfaces on a remote host.	Disable IPv6 if you do not actually using it. Otherwise, disable any unused IPv6 interfaces.	
Enumerate IPv4 Interfaces via SSH	Informational	0			This plugin enumerates IPv4 interfaces on a remote host.	Disable any unused IPv4 interfaces.	
iTunes Version Detection (Mac OS X)	Informational	0			The remote Mac OS X host has a copy of iTunes installed.	Make sure use of this program agrees with your organization's acceptable use and security policies.	
Enumerate MAC Addresses via SSH	Informational	0			This plugin enumerates MAC addresses on a remote host.	Disable any unused interfaces.	
Ethernet Card Manufacturer Detection	Informational	0			The manufacturer can be deduced from the Ethernet OUI.	n/a	

Kerberos Information Disclosure	Informational	0			The remote Kerberos server is leaking information.	n/a	
Common Platform Enumeration (CPE)	Informational	0			It is possible to enumerate CPE names that matched on the remote system.	n/a	
Skype for Mac Installed (credentialed check)	Informational	0			Skype is installed on the remote Mac OS X host.	Make sure that use of this program agrees with your organization's acceptable use and security policies.	
Device Type	Informational	0			It is possible to guess the remote device type.	n/a	
Firefox Installed (Mac OS X)	Informational	0			The remote Mac OS X host contains an alternative web browser.	n/a	
Dropbox Installed (Mac OS X)	Informational	0			There is a file synchronization application on the remote host.	Ensure that use of this software agrees with your organization's	

						acceptable use and security policies.	
Device Hostname	Informational	0			It is possible to determine the remote system hostname.	n/a	
Firewall Rule Enumeration	Informational	0			A firewall is configured on the remote host.	n/a	
Time of Last System Startup	Informational	0			The system has been started.	n/a	
Microsoft Silverlight Installed (Mac OS X)	Informational	0			The remote host has Microsoft Silverlight installed.	n/a	
Mac OS X DNS Server Enumeration	Informational	0			Nessus enumerated the DNS servers being used by the remote Mac OS X host.	n/a	
Mac OS X Admin Group User List	Informational	0			There is at least one user in the 'Admin' group.	Verify that each member of the group should have this type of access.	

Apple Xcode IDE Detection (Mac OS X)	Informational	0			The remote host has an integrated development environment installed.	n/a	
Google Picasa Installed (Mac OS X)	Informational	0			Google Picasa is installed on the remote Mac OS X host.	n/a	
Patch Report	Informational	0			The remote host is missing several patches.	Install the patches listed below.	
Apple Keynote Detection (Mac OS X)	Informational	0			A presentation software application is installed on the remote Mac OS X host.	n/a	
Google Chrome Installed (Mac OS X)	Informational	0			The remote Mac OS X host contains an alternative web browser.	n/a	
Apple Pages Installed (Mac OS X)	Informational	0			The remote host has an application for word processing and desktop publishing.	n/a	

Host:192.168.56.102

Windows Server 2012r5

Όνομα ευπάθειας	Σημαντικότητα	Αξιολόγηση ευπάθειας	Κόστος Διόρθωσης	Ευκολία Εντοπισμού	Συνέπειες	Αντιμετώπιση	Αναφορά
SMB Signing Required	Medium	5.0			Signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	
Windows NetBIOS SMB Remote Host Information Disclosure	Informational	0			It is possible to obtain the network name	n/a	

					of the remote host.		
Microsoft Windows SMB Log In Possible	Informational	0			It is possible to log into the remote host.	n/a	
Microsoft Windows SMB Shares Enumeration	Informational	0			It is possible to enumerate remote network shares.	n/a	
Microsoft Windows SMB Shares Access	Informational	0			It is possible to access a network share.	To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.	
Microsoft Windows SMB Service Enumeration	Informational	0			It is possible to enumerate remote services.	To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter	

						incoming traffic to this port.	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
DCE Services Enumeration	Informational	0			A DCE/RPC service is	n/a	

					running on the remote host.		
DCE Services Enumeration	Informational	0			A DCE/RPC service is running on the remote host.	n/a	
Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Informational	0			It is possible to obtain information about the remote operating system.	n/a	
Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration	Informational	0			It is possible to obtain the host SID for the remote host.	You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value. Refer to the 'See also' section for guidance.	
SMB Use Host SID to Enumerate Local Users	Informational	0			It is possible to enumerate local users.	n/a	
Microsoft Windows 'Administrators' Group User List	Informational	0			There is at least one user in the	Verify that each member of the	

					'Administrators ' group.	group should have this type of access.	
Microsoft Windows - Local Users Information : Disabled accounts	Informational	0			At least one local user account has been disabled.	Delete accounts that are no longer needed.	
Microsoft Windows - Local Users Information : Never changed passwords	Informational	0			At least one local user has never changed his / her password.	Allow / require users to change their passwords regularly.	
Microsoft Windows - Local Users Information : User has never logged on	Informational	0			At least one local user has never logged in to his / her account.	Delete accounts that are not needed.	
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
OS Identification	Informational	0			It is possible to guess the remote	n/a	

					operating system.		
Host Fully Qualified Domain Name (FQDN) Resolution	Informational	0			It was possible to resolve the name of the remote host.	n/a	
Authenticated Check: OS Name and Installed Package Enumeration	Informational	0			This plugin gathers information about the remote host via an authenticated session.	n/a	
Microsoft Windows SMB : Obtains the Password Policy	Informational	0			It is possible to retrieve the remote host's password policy using the supplied credentials.	n/a	
Nessus Scan Information	Informational	0			Information about the Nessus scan.	n/a	
Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Informational	0			Nessus is not able to access the remote Windows Registry.	n/a	

Ethernet Card Manufacturer Detection	Informational	0			The manufacturer can be deduced from the Ethernet OUI.	n/a	
Microsoft Windows SMB Service Config Enumeration	Informational	0			It is possible to enumerate configuration parameters of remote services.	Ensure that each service is configured properly.	
Common Platform Enumeration (CPE)	Informational	0			It is possible to enumerate CPE names that matched on the remote system.	n/a	
Device Type	Informational	0			It is possible to guess the remote device type.	n/a	

Host:192.168.56.101

Windows XP sp3

Όνομα ευπάθειας	Σημαντικότητα	Αξιολόγηση ευπάθειας	Κόστος Διόρθωσης	Ευκολία Εντοπισμού	Συνέπειες	Αντιμετώπιση	Αναφορά
Microsoft Windows XP Unsupported Installation Detection	Critical	10			The remote operating system is no longer supported.	Upgrade to a version of Windows that is currently supported.	
Microsoft Windows SMB NULL Session Authentication	Medium	5			It is possible to log into the remote Windows host with a NULL session.	Apply the following registry changes per the referenced Technet advisories : Set : - HKLM\SYSTEM\ CurrentControlSet\ Control\LSA\Restri ctAnonymous=1 - HKLM\SYSTEM\ CurrentControlSet\ Services\lanmanser ver\parameters\rest rictnullsessaccess= 1 Remove BROWSER from : - HKLM\SYSTEM\ CurrentControlSet\ Services\lanmanser ver\parameters\Nul	CVE-1999-0519 , CVE-1999-0520 , CVE-2002-1117

						lSessionPipes Reboot once the registry changes are complete.	
SMB Signing Required	Medium	5			Signing is not required on the remote SMB server.	Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.	
Windows NetBIOS SMB Remote Host Information Disclosure	Informational	0			It is possible to obtain the network name of the remote host.	n/a	
Microsoft Windows SMB Log In Possible	Informational	0			It is possible to log into the remote host.	n/a	
Microsoft Windows SMB LanMan Pipe	Informational	0			It is possible to obtain	n/a	

Server Listing Disclosure					network information.		
Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Informational	0			It is possible to obtain information about the remote operating system.	n/a	
Network Time Protocol (NTP) Server Detection	Informational	0			An NTP server is listening on the remote host.	n/a	
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
Microsoft Windows SMB Service Detection	Informational	0			A file / print sharing service is listening on the remote host.	n/a	
OS Identification	Informational	0			It is possible to guess the remote	n/a	

					operating system.		
Authenticated Check: OS Name and Installed Package Enumeration	Informational	0			This plugin gathers information about the remote host via an authenticated session.	n/a	
Nessus Scan Information	Informational	0			Information about the Nessus scan.	n/a	
Nessus Windows Scan Not Performed with Admin Privileges	Informational	0			The Nessus scan of this host may be incomplete due to insufficient privileges provided.	Reconfigure your scanner to use credentials with administrative privileges.	
Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	Informational	0			Nessus is not able to access the remote Windows Registry.	n/a	
Ethernet Card Manufacturer Detection	Informational	0			The manufacturer can be	n/a	

					deduced from the Ethernet OUI.		
Common Platform Enumeration (CPE)	Informational	0			It is possible to enumerate CPE names that matched on the remote system.	n/a	
Device Type	Informational	0			It is possible to guess the remote device type.	n/a	

Εξυπηρετητές 1-5