ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ
ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Σχεδιασμός, ανάπτυξη και υλοποίηση μεθοδολογιών ανοικτού κώδικα για εφαρμογή δοκιμών διείσδυσης σε πληροφοριακά συστήματα.

Δαμιανός Χαραλάμπους

Επιβλέπων Καθηγητής
Δρ. Νικόλαος Σκλάβος

Μάϊος 2019

ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

Σχεδιασμός, ανάπτυξη και υλοποίηση μεθοδολογιών ανοικτού κώδικα για εφαρμογή δοκιμών διείσδυσης σε πληροφοριακά συστήματα.

Δαμιανός Χαραλάμπους

Επιβλέπων Καθηγητής
Δρ. Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των
απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάϊος 2019

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Οι πληροφορίες, και ειδικότερα ο τομέας της ασφάλειας πληροφοριών, είναι πιο ευάλωτες από ποτέ καθώς κάθε τεχνολογική πρόοδος, δημιουργεί μια καινούρια απειλή. Οι επίδοξοι εγκληματίες, δοκιμάζουν καθημερινά νέες μορφές αλλά και καινοτόμες μεθοδολογίες επιθέσεων, με σκοπό την παραβίαση και την εξασφάλιση παράνομης πρόσβασης, σε πληροφορικά συστήματα. Η ανάγκη για καλύτερη προστασία και ασφάλεια των δικτύων και υπολογιστών είναι επιτακτική. Οι λύσεις, οφείλουν να είναι σύγχρονες, δραστικές, λειτουργικές και εφαρμόσιμες. Πρέπει να μπορούν να αναγνωρίζουν και να διορθώνουν έγκαιρα ευπάθειες και αδυναμίες. [40] Έτσι, έξυπνα, μικρά σε μέγεθος και απαιτήσεις εργαλεία, απλά και κατανοητά, επιβάλλεται να αναπτύσσονται και να εφαρμόζονται. Συστήματα και εφαρμογές, που λειτουργούν ως εργαλεία δοκιμών διείσδυσης, φιλικά, πρακτικά και εύκολα, πρέπει να χρησιμοποιούνται. Σκοπός της διατριβής που ακολουθεί, είναι η διενέργεια μιας εκτενούς ανασκόπησης στις υπάρχουσες διανομές ανοικτού κώδικα οι οποίες έχουν σχεδιαστεί κατά τρόπο ώστε να υποστηρίζουν εργαλεία δοκιμών διείσδυσης. Αυτό αποτελεί και το πλαίσιο της βιβλιογραφικής ανασκόπησης. Στην παρούσα έρευνα, επεξηγείται ο ρόλος και η σημαντικότητα των δοκιμών διείσδυσης και παρουσιάζεται ο τρόπος με τον οποίο οι δοκιμές βοηθούν στην αξιολόγηση της αποτελεσματικότητας του αμυντικού μηχανισμού και της πολιτικής των οργανισμών. Η σημασία, οι παράγοντες και τα συστατικά των δοκιμών ως επίσης τα εργαλεία, οι διαδικασίες και το κόστος υλοποίησης τους, είναι μεταξύ των θεμάτων που ερευνήθηκαν. Στόχος, ο σχεδιασμός και η ανάπτυξη μεθοδολογιών ανοικτού κώδικα για την δημιουργία μιας ειδικά προσαρμοσμένης διανομής για εκτέλεση δοκιμών διείσδυσης. Η διανομή αυτή, ονομάστηκε LFS και αποτελείται από πυρήνα που βασίζεται στην διανομή Debian Linux, όπου και οφείλει τις κύριες λειτουργίες της. Διαθέτει, ένα απλό γραφικό περιβάλλον, γρήγορο προσαρμοστικό διαχειριστή παραθύρων, με δυνατότητα προσθαφαίρεσης διάφορων πρακτικών εφαρμογών. Ως αποτέλεσμα, η έρευνα κατάφερε να απαντήσει στα ερευνητικά ερωτήματα που έθεσε καταδεικνύοντας ότι, παρόλη την απλοϊκότητα του συστήματος, που αναπτύχθηκε, εντούτοις ο χειριστής επιβάλλεται να κατέχει στοιχειώδεις γνώσεις, στον ευρύτερο τομέα της ασφάλειας πληροφοριών και τον τομέα των λειτουργικών συστημάτων Linux. Φαντάζει πολύ δύσκολο να μπορεί να κατανοεί τα εξαγόμενα αποτελέσματα και να καθορίζει τις λειτουργίες για εκμετάλλευση τους. Έτσι, η μίσθωση επαγγελματιών καθίσταται απαραίτητη για όσους επιθυμούν να διενεργήσουν δοκιμές διείσδυσες στα πληροφοριακά τους συστήματα.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: αναγνώριση, δίκτυα, εκμετάλλευση, σάρωση ευπάθειας, συλλογή πληροφοριών

Summary

Information, and in particular information security, is more vulnerable than ever as any technological progress creates a new threat. The aspiring criminals are testing new forms every day, as well as innovative methodologies of attacks aimed at infringing and securing unauthorized access to information systems. The need for better network and computer security and security is imperative. The solutions must be modern, effective, functional and workable. They must be able to recognize and correct in time vulnerabilities and weaknesses. [40] Thus, smart, small-sized and demanding tools, simple and comprehensible, need to be developed and implemented. Systems and applications that act as penetration testing tools, friendly, practical and easy to use, should be used. The purpose of the dissertation is to perform a comprehensive review of existing open source distributions that are designed to support penetration testing tools. This is the framework of the bibliographic review. In the present study, the role and importance of penetration tests is explained. It also shows how testing helps to assess the effectiveness of the defense mechanism and agency policy. The importance, factors and components of the tests as well as the tools and processes and the cost of their implementation are among the issues explored. Objective, design and development of open source methodologies to create a customized distribution for conducting penetration tests. The distribution was named LFS. It consists of a Debian Linux-based kernel where it owes its main functions. It has a simple graphical environment, a fast adaptive window manager, with the ability to add various practical applications. As a result, the research has succeeded in answering the research questions raised by demonstrating that, despite the simplicity of the system that has developed, the operator needs to have elementary knowledge in the broader area of information security and the Linux operating system. It seems very difficult to be able to understand the exported results and to define the functions for exploitation. Thus, the hiring of professionals becomes necessary for those who wish to conduct penetration tests on their information systems.

KEYWORDS: reconnaissance, networks, exploitation, vulnerability scanning, information gathering

Ευχαριστίες

Ευχαριστίες στον επιβλέποντα καθηγητή μου, Δρ. Νικόλαο Σκλάβο για την βοήθεια και καθοδήγηση για την εκπόνηση της μεταπτυχιακής διατριβής. Ευχαριστώ, επίσης την οικογένεια μου, τα παιδιά μου και ιδιαίτερα την σύζυγο μου, για την υπομονή που υπέδειξαν και την υποστήριξη που μου παρείχαν σε όλο αυτό το χρονικό διάστημα.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ασφάλεια των πληροφοριακών συστημάτων, θεωρείται ένας από τους κυριότερους αλλά και ουσιαστικότερους παράγοντες κάθε επιχείρησης. Οι απειλές για την ασφάλεια, αποτελούν ένα διαρκώς αυξανόμενο πρόβλημα στις σύγχρονες υποδομές των πληροφοριακών συστημάτων. [41] Υπάρχουν όμως δυστυχώς, αρκετοί τρόποι με τους οποίους ένα σύστημα μπορεί να παραβιαστεί. Είναι για αυτό το λόγο που πρέπει να διασφαλιστεί, με την εφαρμογή σύγχρονων, μοντέρνων και αξιόπιστων τεχνολογιών, υψηλής ποιότητας. Λύσεις, αποτελούν διάφορες μεθοδολογίες αλλά και τα πιστοποιητικά αυθεντικότητας, τα τείχη προστασίας, η προστασία με φυσικά μηχανήματα ανίχνευσης και αναγνώρισης επιθέσεων και άλλα. Για να διατηρείται η ασφάλεια των συστημάτων, από πιθανές επιθέσεις, θα χρειαστεί να γίνεται συστηματική παρακολούθηση επιδόσεων και ασφάλειας. Στο τομέα αυτό, οι δοκιμές διείσδυσης έχουν αποδειχθεί ότι αποτελούν την καλύτερη μέθοδο ανίχνευσης παραβιάσεων ασφαλείας. Στην έρευνα που ακολουθεί, θα περιγράψουμε λεπτομερώς τα πλεονεκτήματα και τα μειονεκτήματα των ελέγχων διείσδυσης καθώς και το κόστος εφαρμογής τους. Θα συμπεριληφθούν επίσης συστάσεις, όσο και σχετικές επεξηγήσεις που παρουσιάζουν τα οφέλη που έχουν αυτοί που επιλέγουν να προχωρήσουν σε εφαρμογή των δοκιμών αυτών, ως μέτρο αντιμετώπισης των κενών ασφάλειας. [38]

1.1 Τι είναι οι δοκιμές διείσδυσης

Δοκιμές διείσδυσης, «Penetration Testings» ή σε συντομογραφία «PenTests», ονομάζουμε τις δοκιμές ασφάλειας που μιμούνται επιθέσεις σε πραγματικό περιβάλλον, με σκοπό τον εντοπισμό μεθόδων για καταστρατήγηση των χαρακτηριστικών ασφάλειας. Σε αυτές, περιλαμβάνονται οι διαδικασίες για εντοπισμό ευπαθειών ασφαλείας σε εφαρμογές ή σε συστήματα. Όσον αφορά τα τρωτά σημεία ενός συστήματος, αυτά αξιοποιούνται με διαδικασίες μέσω της εξουσιοδοτημένης και προσομοιωμένης επίθεσης. Με τον όρο ευπάθεια, ορίζεται το ελάττωμα ασφαλείας, το οποίο προκύπτει από το σχεδιασμό, την υλοποίηση, τη συντήρηση και τη λειτουργία του συστήματος υπολογιστών. [42] Πρωταρχικός σκοπός των δοκιμών, είναι να προστατεύσουν το σύστημα από μη εξουσιοδοτημένη πρόσβαση και τις πιθανές αδυναμίες που δυνατόν να παρουσιάζονται στην ευρύτερη υποδομή του δικτύου. Κατά δεύτερον, ευελπιστούν να εξασφαλίζουν σημαντικά δεδομένα από τους επιτιθέμενους, που κατάφεραν να αποκτήσουν πρόσβαση στο σύστημα. Ακόμα, μέσω των δοκιμών γίνεται αναφορά εάν τα υφιστάμενα αμυντικά μέτρα που χρησιμοποιούνται στο σύστημα, είναι αρκετά ισχυρά ώστε να μπορούν να αποτρέπουν τυχόν παραβιάσεις της ασφάλειας. Τέλος, αφού ολοκληρωθούν οι διαδικασίες, παραδίδονται αναφορές που υποδεικνύουν τα αντίμετρα, για βελτίωση και διαμόρφωση των εφαρμογών, τα οποία πρέπει να ληφθούν για να μειωθεί ο κίνδυνος παραβίασης του συστήματος. Δεν είναι λίγες οι φορές φυσικά, που οι δοκιμές διείσδυσης αναφέρονται με τον ορισμό «Ethical Hacking», για το οποίο θα γίνει αναφορά σε κατοπινό στάδιο. [23]

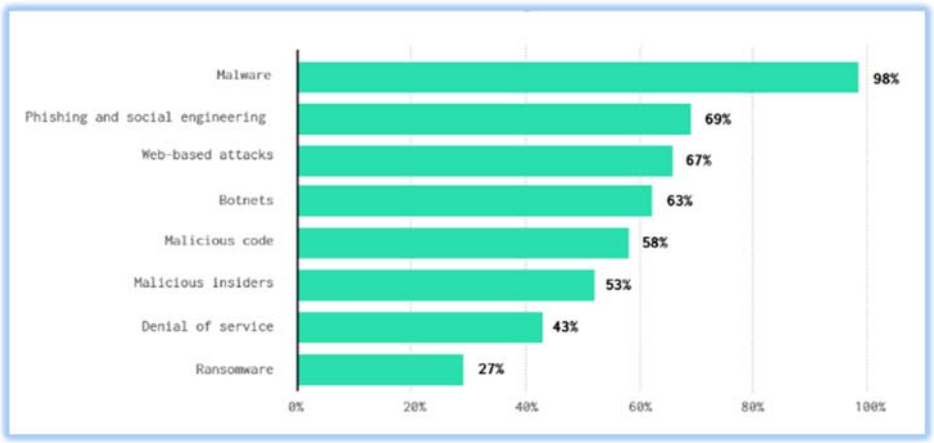
Στην πραγματικότητα, όταν μια εταιρεία δεν προστατεύεται αποτελεσματικά, αφήνει μια κωδικοποιητή ευπάθεια. Η ευπάθεια αυτή, τις πλείστες φορές οδηγεί στην σκόπιμη ή τυχαία, καταστροφή, αλλοίωση ή ακόμα και σε ανεξέλεγκτη έκθεση ευαίσθητων δεδομένων. Έρευνα, κατέδειξε ότι περίπου το 69%, των οργανώσεων στις Η.Π.Α., δεν προστατεύονται από παραβιάσεις στον κυβερνοχώρο, μόνο επειδή έχουν λάβει μέτρα κατά των κακόβουλων λογισμικών ή επειδή χρησιμοποιούν μέτρα που προσφέρονται από τους τοίχους προστασίας. Όπως αναφέρει η έρευνα, οι οργανισμοί έχουν την πεποίθηση ότι είναι πιο πιθανόν ένας εξειδικευμένος επαγγελματίας, που εκτελεί δοκιμές διείσδυσης, να εντοπίσει τα τρωτά σημεία ενός συστήματος, πολύ καλύτερα από οποιοδήποτε εξειδικευμένο λογισμικό. Η άποψη τους θεωρείται ορθολογιστική καθώς στηρίζεται στο γεγονός, ότι ο άνθρωπος σε αντίθεση με την μηχανή, μπορεί να διεξαγάγει έρευνα με βάση τις προηγούμενες του εμπειρίες. [32]

1.2 Σημαντικότητα της εκτέλεσης ελέγχων

Σήμερα, οι εταιρείες είναι αντιμέτωπες με τεράστιες και επικίνδυνες επιθέσεις στον κυβερνοχώρο. Ενδεικτικές είναι οι επιθέσεις Ransomware WannaCry, Locky και Jaff, που «κλειδώνουν», δεδομένα σε συστήματα κυρίως μεγάλων εταιρειών. Οι επιθέσεις αυτές, αφού επιτύχουν να κωδικοποιήσουν όλα τα δεδομένα που περιέχονται σε αυτά, απαιτούν λύτρα σε κρυπτονομίσματα «Bitcoin», για να αποστείλουν τα κλειδιά που τα αποκωδικοποιούν. Στις περισσότερες περιπτώσεις, παρόλο που καταβάλλονται τα λύτρα, τα κλειδιά δεν αποστέλλονται. Έχοντας αυτό υπόψη, δεν αφήνουν άλλη επιλογή παρά να λαμβάνονται προληπτικά μέτρα αλλά και έλεγχοι σε τακτά χρονικά διαστήματα. Μια αρκετά καλή πρακτική είναι η συστηματική φύλαξη των δεδομένων του οργανισμού σε αποθηκευτικά μέσα, με δυνατότητα ανάκτησης. Φυσικά μια ακόμη καλύτερη πρακτική που αφορά την πρόληψη, ίσως πιο σημαντική, από την προηγούμενη είναι η εκτέλεση της διαδικασίας των δοκιμών διείσδυσης. Οι δοκιμές αυτές, έχουν ως σκοπό, την έγκυρη διάγνωση και ενημέρωση, για ευπάθειες που παρουσιάζουν τα διάφορα συστήματα καθώς και την προστασία των συστημάτων πληροφοριών από παραβιάσεις που αφορούν την ασφάλεια. [23]

Είναι γεγονός, ότι ένα αδύναμο σύστημα ασφαλείας το οποίο είναι ευάλωτο στις διάφορες μορφές παραβιάσεων να είναι αντιμέτωπο με τις τεράστιες απώλειες σε διάφορους τομείς. Σίγουρα οι κυριότερες απώλειες, αφορούν και επηρεάζουν, τα έσοδα της εταιρείας, την φήμη της όσο και την εμπιστοσύνη της, απέναντι στους πελάτες και συνεργάτες της. Σύμφωνα με τα αποτελέσματα του ινστιτούτου Ponemon που έγινε το 2017, σε πάνω από 400 εταιρείες σε παγκόσμιο επίπεδο, αποδείχθηκε ότι το 43% των παραβιάσεων και επιθέσεων, είχαν ως στόχο, τις μικρές επιχειρήσεις. Οι κυριότερες μορφές επιθέσεων, αφορούσαν επιθέσεις «phishing» και επιθέσεις κοινωνικής μηχανικής. [17] Βασίζονταν δε, κατά μεγάλο ποσοστό, πέραν του 60%, σε επιθέσεις κακόβουλων λογισμικών που αποκτούν προσβάσεις σε συστήματα, μέσω του διαδικτύου (σχήμα 1.1). Σύμφωνα με τα αποτελέσματα της ίδια έρευνας, το μέσο κόστος των αρχείων που κλάπηκαν είχε μειωθεί. Οι επιθέσεις που γίνονται όμως τώρα, είναι μεγαλύτερες σε έκταση και βλάπτουν περισσότερο τα οικονομικά των εταιρειών. Ενδεικτικά, το μέσο κόστος μιας εταιρείας ανά παραβίαση έφθασε στις Η.Π.Α., σχεδόν τα 7,5 εκατομμύρια δολάρια και σχεδόν τα 5 εκατομμύρια δολάρια, στη Μέση Ανατολή. Το ίδιο συμβαίνει με τον αριθμό των επιθέσεων σε όλη την υφήλιο, ο οποίος αυξάνεται χρόνο με το χρόνο. Σημειώνεται ότι το 2017, καταγράφηκαν επιθέσεις στον κυβερνοχώρο κάθε 40 δευτερόλεπτα, με αποτέλεσμα συνολικές απώλειες ύψους 5 δισεκατομμυρίων δολαρίων. Η αντίστοιχες απώλειες το 2015 ήταν, 325 εκατομμύρια δολάρια.

Μέχρι το τέλος του 2019, ο αριθμός που αφορά την συχνότητα των επιθέσεων αναμένεται να κυμανθεί στα 14 δευτερόλεπτα ανά επίθεση, επιφέροντας 21,5 δισεκατομμύρια δολάρια, ως έσοδα σε κυβερνο-εγκληματίες. [17]



Σχήμα 1.1: Καταγραμμένες μορφές και τύποι επιθέσεων σε παγκόσμια κλίμακα

Είναι πολύ σημαντικό λοιπόν, για οποιονδήποτε οργανισμό να εντοπίσει έγκαιρα πριν να είναι πολύ αργά, τα ζητήματα ασφάλειας που υπάρχουν στο εσωτερικό δίκτυο και τους υπολογιστές του. Αφού εκμεταλλευτεί, την πληροφόρηση και την καθοδήγηση των αναφορών από τις δοκιμές διείσδυσης, θα πρέπει να σχεδιάσει την άμυνα του ενάντια σε οποιαδήποτε απόπειρα παραβίασης. Το απόρρητο των προσωπικών δεδομένων των χρηστών του συστήματος και η γενικότερη ασφάλεια των δεδομένων που εμπεριέχονται σε αυτό, αποτελούν σήμερα τις μεγαλύτερες ανησυχίες τους. [23]

1.3 Χαρακτηριστικά της έρευνας

Σκοπός της έρευνας

Σκοπός της διατριβής που ακολουθεί, είναι η διενέργεια μιας εκτενούς ανασκόπησης στις υπάρχουσες διανομές ανοικτού κώδικα, οι οποίες έχουν σχεδιαστεί κατά τρόπο ώστε να υποστηρίζουν εργαλεία, δοκιμών διείσδυσης. Σε αυτή, επεξηγείται ο ρόλος που διαδραματίζουν οι δοκιμές διείσδυσης, στο τομέα της ασφάλειας των πληροφοριακών συστημάτων. Παράλληλα, παρουσιάζεται ο τρόπος με τον οποίο οι δοκιμές, βοηθούν στην αξιολόγηση της αποτελεσματικότητας του αμυντικού μηχανισμού και της πολιτικής που εφαρμόζεται σε ένα οργανισμό. [03]

Βασικά ερευνητικά ερωτήματα

Τα βασικά ερωτήματα διατήρησαν την ισορροπία της έρευνας και δεν επέτρεψαν σε κανένα σημείο να ξεφεύγει από τον σκοπό της. Τα ερωτήματα, απαντώνται από την ανάπτυξη των ενοτήτων στα διάφορα κεφάλαια. Τα ερευνητικά ερωτήματα που τέθηκαν είναι τα ακόλουθα:-

1. Ποιο είναι το πεδίο εφαρμογής των δοκιμών διείσδυσης;
2. Τι διαδικασίες ακολουθούνται για εκτέλεση δοκιμών διείσδυσης; Ποια άτομα πρέπει να τις εκτελούν;
3. Πότε και γιατί τα πληροφοριακά συστήματα παρουσιάζουν ευπάθειες;
4. Γιατί πρέπει να επενδύσει κάποιος σε δοκιμές διείσδυσης. Ποιοι παράγοντες καθορίζουν την απόφαση; Ποιο το κόστος τους;
5. Ποιες είναι οι βέλτιστες πρακτικές για την επιλογή ομάδας που θα εκτελέσει τις δοκιμές; Ποια τα κριτήρια επιλογής εργαλείων;

Σπουδαιότητα και αναγκαιότητα της έρευνας

Ο τομέας της ασφάλειας πληροφοριών, δοκιμάζεται καθημερινά καθώς διανύει την περίοδο της νέας πραγματικότητας και των νέων προκλήσεων, της τέταρτης βιομηχανικής επανάστασης όπως την αποκαλούν αρκετοί. Η ψηφιακοί ασφάλεια, η οποία περιλαμβάνει την ασφάλεια πληροφοριών, δικτύων και υποδομών, θεωρείται ο πιο κρίσιμος τομέας της νέας εποχής. Ο τομέας της τεχνολογίας όμως, δεν είναι ο μόνος τομέας που εξελίχθηκε. Ανάλογες ίσως και πιο προηγμένες τεχνολογικές εξελίξεις, υπήρξαν και στο στρατόπεδο των επίδοξων εγκληματιών. Ως εκ τούτου, η ανάγκη για καλύτερη προστασία και ασφάλεια των δικτύων και υπολογιστών, θεωρείται επιτακτική. Εξίσου αναγκαία, είναι και η εφαρμογή νέων καινοτόμων εργαλείων διάγνωσης, αναγνώρισης και καταστολής των απειλών. Έτσι, μελετόντας τις τάσεις και τις στρατηγικές των εισβολέων, πρέπει να κατασκευάζονται ανάλογα αντίμετρα, συστήματα και εφαρμογές. Τέτοια εργαλεία είναι τα εργαλεία δοκιμών διείσδυσης, τα οποία μπορούν να προστατεύσουν το σύστημα από μη εξουσιοδοτημένη πρόσβαση και να προβάλουν τις πιθανές αδυναμίες που δυνατόν να παρουσιάζονται στην ευρύτερη υποδομή του δικτύου. Η διατριβή που ακολουθεί, εστιάζει ακριβώς στην ανάγκη αυτή για δημιουργία διανομής ανοικτού κώδικα με σκοπό την εφαρμογή δοκιμών διείσδυσης. Ο κάθε χρήστης, δηλαδή θα μπορεί να εκτελεί μόνος του δοκιμές διείσδυσης, αποκτώντας έτσι το πρώτο επίπεδο γνώσης, για την κατάσταση της υποδομής του. [03]

Μεθοδολογία που ακολουθήθηκε

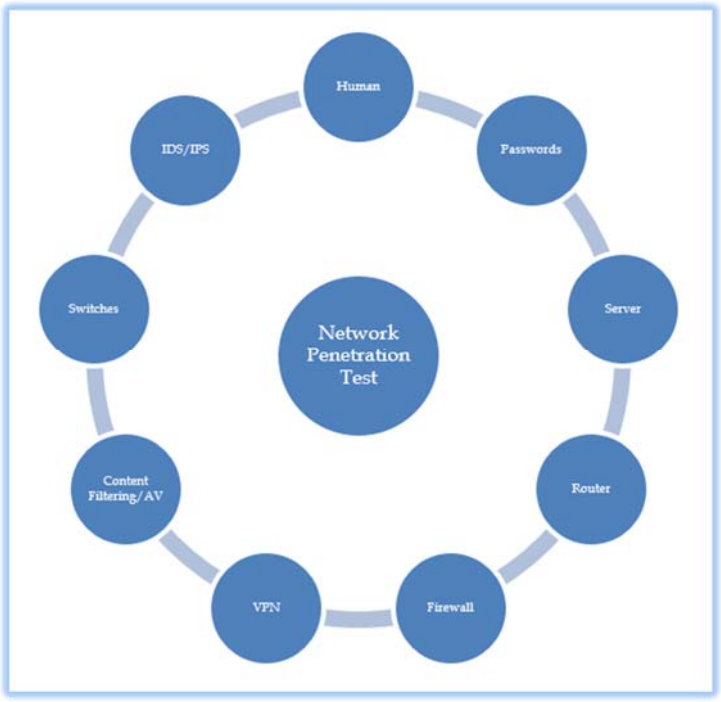
Η βιβλιογραφική ανασκόπηση, εφαρμόστηκε στις υπάρχουσες αυτόνομες εφαρμογές και διανομές λειτουργικών συστημάτων που εμπεριέχουν εφαρμογές για δοκιμές διείσδυσης. Οι πληροφορίες αντλήθηκαν μέσα από την μελέτη ηλεκτρονικών και μη βιβλίων, επιστημονικών περιοδικών και ακαδημαϊκών άρθρων. Πιο συγκεκριμένα, η ηλεκτρονική πληροφόρηση αντλήθηκε με την χρήση της ιστοσελίδας της βιβλιοθήκης του Ανοικτού Πανεπιστημίου Κύπρου, «MyAthens», της ενοποιημένης αναζήτησης «Τεύκρος» καθώς και άλλων ελεύθερων μηχανών αναζήτησης. Το κύριο μέρος της έρευνας αποτελείται από τέσσερα κεφάλαια. Στο κεφάλαιο 2, γίνεται αναφορά στις διανομές ελεύθερου κώδικα καθώς και τους τομείς εφαρμογής των δοκιμών. Παράλληλα, αναπτύσσονται οι τεχνικές που χρησιμοποιούνται ως επίσης και οι τύποι των δοκιμών. Ακόμα παρουσιάζονται οι διάφορες ομάδες ελέγχου και εκτέλεσης δοκιμών διείσδυσης. Στο κεφάλαιο 3, παρουσιάζονται οι διάφορες φάσεις, μεθοδολογίες επίθεσης και διείσδυσης, οι διαδικασίες, οι κατηγορίες και τα απαιτούμενα εργαλεία για εφαρμογή των δοκιμών. Στο επόμενο κεφάλαιο, αναλύονται τα αίτια των ευπαθειών που παρουσιάσουν τα πληροφοριακά συστήματα, η επιλογή των δοκιμών που θα χρησιμοποιηθούν καθώς και το κόστος υλοποίησης των δοκιμών. Στο τελευταίο κεφάλαιο, γίνεται η δημιουργία της νέας διανομής με την χρήση ανοικτού κώδικα. Παράλληλα, γίνεται παρουσίαση των χαρακτηριστικών της διανομής και η αρχιτεκτονική που χρησιμοποιήθηκε. Τέλος, αναφορά γίνεται και στα εργαλεία που έχουν προστεθεί στην διανομή για να ικανοποιηθεί η μελέτη περίπτωσης «case study» σε μια δοκιμή διείσδυσης. [17]

Κεφάλαιο 2
Πεδίο Εφαρμογής, Ομάδες και Τεχνικές

Οι διανομές ελεύθερου κώδικα καθώς και τα εργαλεία που συμπεριλαμβάνονται σε αυτά, ίσως να είναι ένας από τους λόγους για τους οποίους έγιναν γνωστές οι δοκιμές διείσδυσης. Βάση των διανομών αυτών, έχουν σχεδιαστεί εργαλεία τα οποία είναι ικανά στην διάγνωση ευπαθειών και την διεξαγωγή ελέγχων προστατεύοντας το σύστημα από μη εξουσιοδοτημένες προσβάσεις. Βάζοντας σε εφαρμογή τον στόχο τους, εφαρμόζουν τεχνικές, διαδικασίες και ακολουθούν μεθοδολογίες σε εφαρμογές και δικτυακές υποδομές. Η ομάδα που θα εκτελέσει τις δοκιμές καθώς και ο τύπος της δοκιμής, επιλέγεται ανάλογα με τα δεδομένα που έχουν συλλεχθεί. [08]

2.1 Εφαρμογή δοκιμών διείσδυσης

Το δίκτυο, θεωρείται το νευρικό σύστημα ενός οργανισμού αφού αποτελεί ένα σύνολο υπολογιστικών συσκευών που συνδέονται μεταξύ τους. Αυτός είναι και ο λόγος της ύπαρξης του αφού έχει δημιουργήσει το δικό του οικοσύστημα (σχήμα 2.1), στο οποίο εμπεριέχονται οι συσκευές, οι διαδικασίες και ο άνθρωπος που αποτελεί και το αδύναμο του συνεργάτη. Το δίκτυο, χρησιμοποιεί, συνδεσμολογία και τοπολογία, μοντέλα αλληλεπίδρασης χρηστών, διακομιστών και εξυπηρετητών. Τοπικά, ως επίσης και ευρυζωνικά , εξυπηρετεί τις λειτουργίες που καθορίζει ο οργανισμός όπου ανήκει, ενώ διαδικτυακά, έχει την δυνατότητα είτε να παρέχει υπηρεσίες, είτε να χρησιμοποιεί υπηρεσίες από άλλα δίκτυα. Επιπρόσθετα, μπορεί να χαρακτηρισθεί και ως ο οδηγός του οργανισμού, καθώς μέσω των επικοινωνιακών του διαύλων, τον οδηγεί. Το γεγονός όμως, ότι είναι συνάμα υπεύθυνο, να καθορίζει όλες προσβάσεις των χρηστών στο οικοσύστημα του, το καταστούν ευάλωτο και αναγκαίο να διασφαλιστεί. Είναι σε αυτό το σημείο, που οι δοκιμές διείσδυσης δικτύου μπορούν να βοηθήσουν, εφαρμόζοντας, τον πρωταρχικό τους στόχο, για εντοπισμό των ευπαθειών και των τρωτών σημείων που δυνατό να παρουσιάζονται στο δίκτυο. Οι δοκιμές διείσδυσης που εφαρμόζονται σε δίκτυα, χωρίζονται σε τρις κύριες κατηγορίες, τις δοκιμές για ενσύρματα δίκτυα, δοκιμές για ασύρματα δίκτυα και τις δοκιμές σε εφαρμογές και λογισμικά. [13]



Σχήμα 2.1: Προσέγγιση δοκιμών διείσδυσης σε δίκτυα

Δοκιμές σε ενσύρματα δίκτυα

Η δοκιμή διείσδυσης στην δικτυακή υποδομή ενός οργανισμού, μπορεί να περιλαμβάνει σάρωση όλων των ηλεκτρονικών συσκευών, των θυρών, των διακομιστών, των δρομολογιτών, των συστημάτων ανίχνευσης και προστασίας από εισβολείς, τις βάσεις δεδομένων κλπ. Στις δοκιμές δικτύου εμπεριέχονται επίσης και οι δοκιμές παράκαμψης τείχους προστασίας, όπως και οι δοκιμές επιθέσεων DNS. Οι δοκιμές δικτύου, ονομάζονται και δοκιμές σύγκρουσης του συστήματος. Ανάλογα με την πολυπλοκότητα του δικτύου, οι δοκιμές αυτές μπορεί να διαφέρουν σε διάρκεια και κόστος. Ορισμένες ομάδες που εκτελούν δοκιμές διείσδυσης σε δίκτυα, προσφέρουν μια σταθερή τιμή, η οποία συνήθως περιλαμβάνει έναν καθορισμένο κατάλογο με τις διαθέσιμες υπηρεσίες. Εκτενέστερη αναφορά για το κόστος των δοκιμών γενικότερα θα γίνει στο κεφάλαιο 4. Κάθε υπεύθυνος ασφαλείας, μπορεί να προτείνει τον τρόπο με τον οποίο επιθυμεί να εκτελούνται οι διαδικασίες σάρωσης για ευπάθειες. Παράλληλα, οι τεχνικές διενέργειας διείσδυσης μπορεί να διαφέρουν ανάλογα με τον αριθμό και τους τύπους δοκιμών, ως επίσης τα εργαλεία και τις υπηρεσίες που χρησιμοποιούνται στη διαδικασία. Ο έλεγχος αυτός, χωρίζεται σε εσωτερικά και εξωτερικά τμήματα (componets) καθώς μπορεί να χρησιμοποιούν διαφορετικά εργαλεία. Διαφορετικά εργαλεία αλλά και χαρακτηριστικά είναι βέβαιο να χρησιμοποιούνται όταν το σύστημα είναι αρκετά περίπλοκο. [38]

Δοκιμές σε ασύρματα δίκτυα

Οι δοκιμές διείσδυσης σε ασύρματα δίκτυα, στοχεύουν στην εξεύρεση κενών εντός των σημείων πρόσβασης του δικτύου, κλειδιών, αδύναμων πρωτοκόλλων και άλλων πιθανών σημείων παραβίασης. Σημειώνεται ότι, κάθε διαδικασία σάρωσης ευπάθειας είναι μια δοκιμή διείσδυσης, η οποία μας επιτρέπει να κατανοήσουμε τον πραγματικό κίνδυνο ύπαρξης των διαφόρων ευπαθειών. Ενδεικτικά, εργαλεία ανοικτού κώδικα τα οποία μπορούν να διενεργούν δοκιμές διείσδυσης σε ασύρματα δίκτυα είναι: το kismet, το reaver, το wifite, το cowpatty κλπ. [23]

Δοκιμές σε εφαρμογές και λογισμικά

Οι δοκιμές διείσδυσης σε εφαρμογές, εκτελούνται κυρίως σε εφαρμογές ιστού και είναι αρκετά περίπλοκες. Ως εκ τούτου, έχουν πολλές δυνατότητες διερεύνησης όσον αφορά τον τομέα των ευπαθειών, συμπεριλαμβανομένων εσωτερικών και εξωτερικών δοκιμών. Η διαφορά από μια δοκιμή συνήθους τύπου ευπάθειας (vulnerability test), είναι η εκμετάλλευση των πιθανών

αδύναμων σημείων στο σύστημα. Χρησιμοποιώντας μεθόδους με την χρήση λογισμικού, μπορεί να γίνει έλεγχος εάν μια εφαρμογή εκτίθεται σε ευπάθειες ασφαλείας ή αποτελεί στόχο. Με τον τρόπο αυτό ελέγχονται δηλαδή οι ευπάθειες ως προς την ασφάλεια των εφαρμογών ιστού και των λογισμικών του προγραμμάτων. [08]

2.2 Τεχνικές δοκιμών διείσδυσης

Όλες οι τεχνικές που εφαρμόζονται κατά την εκτέλεση των δοκιμών διείσδυσης, έχουν κοινό στόχο. Αυτός, δεν είναι άλλος από την αναζήτηση και τον εντοπισμό των ευπαθειών που δυνατόν να παρουσιάζονται στα πληροφοριακά τους συστήματα. Σε σύγκριση με τις σαρώσεις ευπάθειας, οι δοκιμές διείσδυσης είναι πολύ πιο εκτεταμένες. Ενώ οι δοκιμές ευπάθειας εξετάζουν μόνο τις πιθανές ευπάθειες στο σύστημα, οι δοκιμές διείσδυσης εκμεταλλεύονται τις αδυναμίες στην αρχιτεκτονική του συστήματος. [23]

Μη αυτοματοποιημένη διαδικασία

Είναι γεγονός, ότι τα άτομα που εκτελούν δοκιμές διείσδυσης, μπορούν να επιτελέσουν καλύτερες επιθέσεις κατά των εφαρμογών με βάση τις ικανότητές τους, ως επίσης και βάση της εμπειρίας τους στα εργαλεία διείσδυσης. Μέθοδοι όπως είναι η κοινωνική μηχανική, μπορούν να εφαρμόζονται μόνο από τους ανθρώπους, ενώ είναι πολύ δύσκολο να εντοπίζονται όλες οι ευπάθειες των συστημάτων, χρησιμοποιώντας αυτοματοποιημένα εργαλεία. Ορισμένες δε ευπάθειες, μπορούν να εντοπίζονται μόνο μέσω χειροκίνητης σάρωσης. Τα αυτοματοποιημένα εργαλεία, αδυνατούν να εκτελούν εργασίες που προϋποθέτουν χειρωνακτικούς ελέγχους, σχεδιασμό, επιχειρησιακή λογική καθώς και επαληθεύσεις κάποιου κώδικα. [36]

Αυτοματοποιημένη διαδικασία

Τα αυτοματοποιημένα εργαλεία από την άλλη, μπορούν να χρησιμοποιηθούν για τον εντοπισμό μερικών βασικών τύπων ευπάθειας που υπάρχει σε μια εφαρμογή. Τα εργαλεία, έχουν την δυνατότητα πολύ γρήγορης σάρωσης του περιεχομένου ενός συστήματος, με σκοπό την αναζήτηση κακόβουλου κώδικα που μπορεί να οδηγήσει σε πιθανή παραβίαση της ασφάλειας. Μπορούν επίσης, να αναζητήσουν και να βεβαιώσουν την ύπαρξη κενών ασφάλειας σε ένα σύστημα και να εξετάσουν τεχνικές κρυπτογράφησης δεδομένων. Επιπρόσθετα έχουν την

ικανότητα να προσδιορίζουν, δύσκολες κωδικοποιημένες τιμές, όπως είναι το όνομα χρήστη και ο κωδικός πρόσβασης. [43]

Συνδυασμός χειροκίνητης και αυτοματοποιημένης διαδικασίας

Είναι η πιο συνηθισμένη τεχνική που εφαρμόζεται κατά την διαδικασία των δοκιμών διείσδυσης και χρησιμοποιείται για τον εντοπισμό κάθε είδους ευπάθειας. Η συνεργασία του ανθρώπινου παράγοντα, με την αυτοματοποιημένη διαδικασία, εξασφαλίζει γρήγορα και με ακρίβεια αποτελέσματα. Ο συνδυασμός χειροκίνητης και αυτόματης διαδικασίας, καθιερώνεται ως συνταγή επιτυχίας στον τομέα των δοκιμών διείσδυσης. [36]

2.3 Διανομές ελεύθερου κώδικα

Οι ειδικά προσαρμοσμένες διανομές ελεύθερου κώδικα που ακολουθούν, αποτελούν τις πιο ολοκληρωμένες λύσεις επί του παρόντος στον τομέα των δοκιμών διείσδυσης και όχι μόνο. Στηρίζονται σε κορυφαίες διανομές συστημάτων Linux, όπως είναι η Ubuntu, η OpenSUSE, η Fedora, το Arch Linux, η Linux Mint κλπ. Εστιάζουν, πέραν του τομέα των δοκιμών διείσδυσης και σε άλλους σχετικούς τομείς όπως είναι, η δικανική ανάλυση, η ανάλυση συστημάτων και δικτύων, οι δοκιμές επίθεσης σε ιστότοπους και οι διεισδύεις σε ζωντανά συστήματα. Επιπρόσθετα, καλύπτουν επάξια των τομέα της εκπαίδευσης, κυρίως με θέματα που εμπίπτουν στο τομέα της ασφάλειας και των εφαρμογών ιστού. Κάθε διανομή, αναλόγως και του υπαρξιακού της σκοπού, έχει αναπτύξει τα δικά της ξεχωριστά εργαλεία. Σχετική αναφορά, για τα εργαλεία αυτά, γίνεται στο παράρτημα Β1. [26]

Διανομή Kali Linux

Το Kali Linux, είναι η πιο διαδεδομένη διανομή Linux που υπάρχει σήμερα και είναι σχεδιασμένη αποκλειστικά για σκοπούς δοκιμών διείσδυσης και δικανικής ανάλυσης. Η αρχική απαίτηση ελεύθερου χώρου στον σκληρό δίσκο για εγκατάσταση του, είναι 2.8Gb. Το Kali, είναι βασισμένο στη διανομή Debian και αναπτύχθηκε από την Offensive Security, η οποία είναι υπεύθυνη για την συνεχή αναβάθμιση της. Στο Kali, περιλαμβάνεται ένας μεγάλος αριθμός εργαλείων, με πάνω από 600 προεγκατεστημένα προγράμματα ελέγχου διείσδυσης. Αποτελεί την πιο προηγμένη πλατφόρμα δοκιμών διείσδυσης που υπάρχει, είναι ανοικτού τύπου λογισμικό και μπορεί να χρησιμοποιηθεί από οποιοδήποτε δωρεάν. Ακόμα είναι, πλήρως προσαρμόσιμη στον χρήστη και

διαθέτει πολυγλωσσική υποστήριξη. Υποστηρίζει, ένα ευρύ φάσμα συσκευών και συστημάτων υλικού και μπορεί να εγκατασταθεί ως λειτουργικό σύστημα σε υπολογιστές γραφείου, σε laptops ή ακόμα σε εικονικές μηχανές: Hyper-V manager, Oracle VM Virtual Box, VmWare κλπ. Το Kali, είναι διανομή που παρέχει λεπτομερείς οδηγίες και ενημερωμένα εγχειρίδια για τα εργαλεία που χρησιμοποιεί. Το πιο σημαντικό όμως, είναι ότι υποστηρίζεται από μια ενεργή κοινότητα η οποία προσφέρει βοήθεια σε θέματα του ευρύτερου τομέα της ασφάλειας. [10]

Διανομή BackBox

Το BackBox, όπως φαίνεται στο σχήμα 2.2, είναι μια καινούρια διανομή που βασίζεται στην διανομή Ubuntu. Αναπτύχθηκε με σκοπό την αξιολόγηση της ασφάλειας, με την χρήση των δοκιμών διείσδυσης. Χρειάζεται, 2.2Gb, ελεύθερο χώρο στον σκληρό δίσκο για να γίνει η αρχική εγκατάσταση της διανομής. Είναι μια από τις καλύτερες διανομές στον τομέα της και διαθέτει το δικό της αποθετήριο λογισμικού. Παρέχει δε, τις πιο πρόσφατες σταθερές εκδόσεις διαφόρων εργαλείων ανάλυσης συστημάτων και δικτύων ως επίσης και τα πιο γνωστά εργαλεία, για Ethical Hacking. Χρησιμοποιεί περιβάλλον εργασίας XFCE, το οποίο είναι ελαφρύ, γρήγορο, ελκυστικό και φιλικό στο χρήστη. Το BackBox, διαθέτει και αυτό μια πολύ καλή και υποστηρικτική κοινότητα. [29]

Σχήμα 2.2: Επιφάνεια εργασίας διανομής BackBox Linux

Διανομή Parrot Security

Το Parrot Security, είναι σχετικά μια νέα διανομή που αναπτύχθηκε από το δίκτυο Frozenbox. Απαιτεί 3.6Gb, ελεύθερο χώρο στον σκληρό δίσκο για να γίνει η αρχική του εγκατάσταση. Χρήστες της διανομής αυτής είναι άτομα που ασχολούνται με δοκιμές διείσδυσης σε cloud περιβάλλοντα που βασίζονται στην ηλεκτρονική ανωνυμία και σε κρυπτογραφημένα συστήματα. Η διανομή Parrot, βασίζεται στο Debian και χρησιμοποιεί το MATE που αποτελεί την συνέχεια του GNOME 2, ως περιβάλλον επιφάνειας εργασίας του. Σχεδόν κάθε αναγνωρισμένο εργαλείο δοκιμών διείσδυσης, περιλαμβάνεται στο Pattor Security, μαζί με μερικά αποκλειστικά προσαρμοσμένα εργαλεία από το Frozenbox Network. [19]

Διανομή Samurai Web Testing Framework

Το Samurai Web Testing Framework, αναπτύχθηκε με μοναδικό σκοπό τη διενέργεια δοκιμών διείσδυσης στο ιστό. Λειτουργεί μόνο σε εικονικές μηχανές, Virtualbox και VMWare. Η διανομή, βασίζεται στην διανομή Ubuntu και περιέχει τα καλύτερα εργαλεία ελεύθερου και ανοιχτού κώδικα που εστιάζουν στη δοκιμή και την επίθεση ιστότοπων. Περιλαμβάνει επίσης ένα προεγκατεστημένο Wiki, που έχει ρυθμιστεί για την αποθήκευση πληροφοριών κατά τη διάρκεια των δοκιμών διείσδυσης.[29]

Διανομή DEFT Linux

Το DEFT, αποτελεί το ακρωνύμιο των λέξεων Digital Evidence & Forensics Toolkit. Η διανομή αυτή, μπορεί να χρησιμοποιηθεί τόσο για συλλογή και ανάλυση ψηφιακών αποδεικτικών στοιχείων όσο και για την δικανική εξέταση τεκμηρίων, μέσω της μεγάλης γκάμας των εργαλείων που διαθέτει. Οι απαιτήσεις σε ελεύθερο χώρο στο σκληρό δίσκο είναι περίπου οι ίδιες με τις προαναφερόμενες διαμονές, περίπου 3.1 Gb. Στόχος του, είναι να διεισδύει σε ζωντανά συστήματα και να λαμβάνει τα δεδομένα που περιέχονται σε αυτό, αυτούσια χωρίς να τα αλλοιώνει ή να τα παραποιεί. Η διανομή DEFT, μπορεί να συνδυαστεί με το εργαλείο DART (Digital Advanced Response Toolkit), το οποίο αποτελεί επίσης ένα πολύ δυνατό εργαλείο δικανικής εξέτασης συστημάτων, που λειτουργεί σε περιβάλλοντα Windows. [26]

Άλλες διανομές Linux

Υπάρχουν φυσικά, αρκετές άλλες διανομές που μπορούν να συναγωνιστούν στις διανομές για τις οποίες έγινε ήδη αναφορά. Μια από αυτές είναι, το BlackArch η οποία είναι σχεδιασμένη για να εκτελεί δοκιμές διείσδυσης και βασίζεται στην διανομή Arch Linux. Διαθέτει, το δικό της αποθετήριο που περιέχει χιλιάδες εργαλεία, οργανωμένα σε διάφορες ομάδες. Είναι η πιο απαιτητική στην εγκατάσταση διανομή από όλες καθώς χρειάζεται 11Gb, ελεύθερου χώρου στο σκληρό δίσκο. Παρόμοια και σχεδόν ίδια με την BlackArch είναι η διανομή ArchStrike, η οποία είναι ελαφρώς λιγότερο φιλική για το χρήστη διανομή, ιδιαίτερα όμως βολική για προγραμματιστές. Ακόμα μια διανομή που εστιάζει σε δοκιμές διείσδυσης, είναι η διανομή Pentoo που βασίζεται στο Gentoo Linux. Τα εργαλεία της, είναι προσαρμοσμένα για να ικανοποιούν τόσο το επίπεδο των εφαρμογών όσο και το επίπεδο του πυρήνα. Το Network Security Toolkit, είναι μια διανομή με βάση το Fedora που διαθέτει μια πολύ προηγμένη προσέγγιση σχετικά με την διαχείριση, παρακολούθηση και ανάλυση συστημάτων και δικτύων. Ακόμη μια αξιόλογη διανομή είναι η διανομή CAINE, που πηγάζει από το ακρωνύμιο των λέξεων Computer Aided Investigative Environment και περιλαμβάνει μεγάλη ποικιλία εργαλείων που αναπτύσσονται για την δικανική διερεύνηση και ανάλυση ενός συστήματος. Ακόμα, το Bugtraq είναι μια διανομή Linux με ένα τεράστιο εύρος εργαλείων διείσδυσης, δικανικής και εργαστηριακών εργαλείων για κακόβουλα λογισμικά. Τέλος, η πιο ξεχωριστή διανομή από τις υπόλοιπες διανομές είναι η Fedora Security Spin, η οποία ουσιαστικά είναι μια παραλλαγή της διανομής Fedora και έχει σχεδιαστεί τόσο για τον έλεγχο και τις δοκιμές ασφαλείας, όσο και για σκοπούς εκπαίδευσης και διδασκαλίας. Υποστηρίζει ουσιαστικά την ακαδημαϊκή κοινότητα, καθηγητές και φοιτητές, σε θέματα άσκησης και εκπαίδευσης σε μεθοδολογίες ασφαλείας αλλά και την ασφάλεια των πληροφοριών γενικότερα. Μέσω της διανομής αυτής, μπορούν να γίνουν εκπαιδεύσεις σχετικές με την ασφάλεια των εφαρμογών ιστού και την δικανική ανάλυση. [19]

2.4 Τύποι δοκιμών διείσδυσης

Δοκιμές διείσδυσης, μπορούν να χαρακτηρίζονται έτσι οι δοκιμές ασφαλείας, οι οποίες μιμούνται ουσιαστικά επιθέσεις σε πραγματικό περιβάλλον, με σκοπό τον εντοπισμό μεθόδων για καταστρατήγηση των χαρακτηριστικών ασφαλείας μιας εφαρμογής, ενός συστήματος ή και ολόκληρου του δικτύου. Οι επιθέσεις, πραγματοποιούνται συνήθως σε συστήματα παραγωγής σε πραγματικά δεδομένα και χρησιμοποιούν, εργαλεία και τεχνικές, ανάλογες με αυτές που

χρησιμοποιούνται από τους κακόβουλους εισβολείς. Οι δοκιμές διείσδυσης χωρίζονται σε δύο κατηγορίες, τις εσωτερικές και τις εξωτερικές. [06]

Εσωτερικές δοκιμές

Αυτές οι δοκιμές εκτελούνται από το εσωτερικό μέρος ενός δικτύου και μιμούνται έναν πιθανό εσωτερικό εισβολέα. Ο εισβολέας μπορεί να είναι επισκέπτης, είτε εξουσιοδοτημένος είτε όχι, ικανός να συνδεθεί με το δίκτυο ή ένας οποιοσδήποτε υπάλληλος που είναι ήδη συνδεδεμένος με το δίκτυο. Είναι σημαντικό να πούμε, ότι οι στόχοι των δοκιμών διείσδυσης μπορεί να διαφέρουν μεταξύ τους αφού, υπάρχουν αυτοί που θέλουν να ελέγξουν τις ευπάθειές του δικτύου τους και άλλοι που θέλουν να δοκιμάσουν την αποτελεσματικότητα του. Οι δοκιμές διείσδυσης αυτού του τύπου ταξινομούνται σε τρεις ομάδες, την ομάδα White Hat, Grey Hat και Black Hat. Συνοπτικά στην πρώτη ομάδα, αυτός που θα εκτελέσει τις δοκιμές έχει στην κατοχή του ή του παραχωρούνται όλες οι πληροφορίες που χρειάζεται. Επιπρόσθετα, μπορεί να ζητήσει από τον πελάτη, πρόσθετες πληροφορίες κατά τη διάρκεια της διαδικασίας δοκιμής. Στην δεύτερη ομάδα, υπάρχουν, κάποιες βασικές πληροφορίες σχετικά με την υποδομή στόχου, ενώ στην τελευταία ομάδα, δεν διατίθεται καμία πληροφορία σχετικά με τους στόχους, πριν από τη δοκιμή. [37]

Εξωτερικές δοκιμές

Είναι δοκιμές, που εκτελούνται εκτός δικτύου και μιμούνται πιθανές εξωτερικές απειλές. Τέτοιου είδους δοκιμές διείσδυσης κατηγοριοποιούνται σε διάφορους τύπους με ανάλογα κριτήρια και σύμφωνα πάντοτε με τους στόχους που έχουν να αντιμετωπίσουν. Τέτοιες, δοκιμές μπορεί να είναι οι δοκιμές VPN, δοκιμές σε εφαρμογές Ιστού και ασύρματες δοκιμές. [35]

2.5 Έλεγχος και εκτέλεση δοκιμών διείσδυσης

Μια δοκιμή διείσδυσης πρέπει να γίνεται από πιστοποιημένο ειδικό με εμπειρία στον τομέα. Αυτό είναι εξαιρετικά σημαντικό καθώς ο ειδικός μπορεί να επηρεάσει όχι μόνο τα αποτελέσματα μιας δοκιμής αλλά και τα μελλοντικά ενδεχόμενα παραβιάσεων του συστήματος. Σίγουρα, ένας εξειδικευμένος προγραμματιστής μπορεί να εκτελεί δοκιμές οι οποίες τις πλύστες φορές, είναι δυνατό να βοηθούν στη διάγνωση των αδυναμιών καθώς και στην αποκατάσταση ή και την πλήρη διόρθωση τους. Παρόλα αυτά όμως, ακόμη και στην παρουσία ειδικών υπάρχει ο κίνδυνος

βλάβης του συστήματος κατά τη διάρκεια μιας δοκιμής, όμως αυτό είναι λιγότερο πιθανό να συμβεί κατά την διάρκεια που εκτελούνται δοκιμές από έναν ειδικό. [03]

Μπλε και κόκκινες ομάδες δοκιμών διείσδυσης

Κατά την εκτέλεση των δοκιμών διείσδυσης, εφαρμόζονται οι μεθοδολογίες, η διεργασίες και οι διαδικασίες, από τα άτομα που τις εκτελούν, μετά από συγκεκριμένες και εγκεκριμένες οδηγίες. Η εξασφάλιση έγκρισης, είναι πάρα πολύ σημαντική καθώς κατά την διάρκεια της δοκιμής, θα γίνει προσπάθεια για παράκαμψη των επιπέδων προστασίας των πληροφοριακών συστημάτων, συμπεριλαμβανομένης της κατάργησης των ολοκληρωμένων χαρακτηριστικών ασφαλείας. Οι ομάδες εκτέλεσης δοκιμών διείσδυσης χωρίζονται σε δύο βασικές ομάδες, τις μπλε και τις κόκκινές ομάδες. [34]

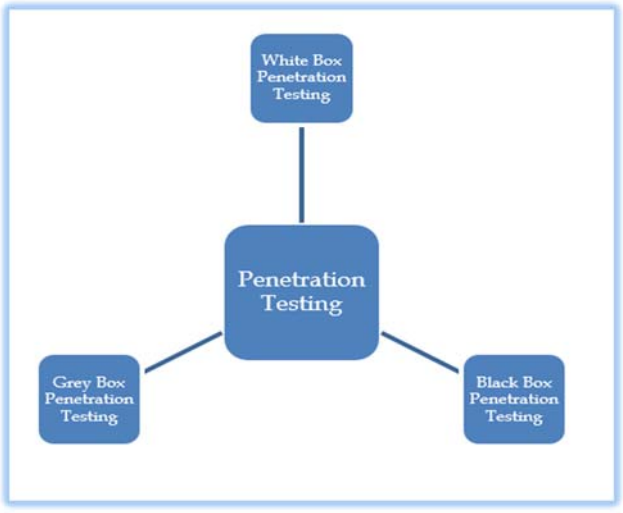
1. Blue Teaming. Οι μπλε ομάδες, αξιολογούν την ασφάλεια του δικτύου και εντοπίζουν τυχόν ευπάθειες στο σύστημα. Ο ρόλος τους είναι να αποτρέψουν κάθε είδους παραβιάσεις βρίσκοντας τρόπους για να υπερασπίζονται, να αλλάζουν και να αναπτύσσουν αμυντικούς μηχανισμούς, έτσι ώστε να καταστήσουν την αντίδραση των περιστατικών πολύ πιο ισχυρή. Οι μπλε ομάδες, είναι παρόμοιες με τις κόκκινες ομάδες οι οποίες μιμούνται ένα επιτιθέμενο και εκτελούν επιθέσεις με συγκεκριμένες τεχνικές και τακτικές. Όπως και οι κόκκινες ομάδες, οι μπλε ομάδες πρέπει να γνωρίζουν τις ίδιες κακόβουλες τακτικές που κατέχει ένα εισβολέας. Οι τακτικές αυτές όπως και άλλες τεχνικές και διαδικασίες, πρέπει να χρησιμοποιούνται ώστε να δημιουργούν στρατηγικές απόκρισης γύρω τους. Οι δραστηριότητες των μπλε ομάδων, δεν είναι αποκλειστικές για επιθέσεις καθώς ασχολούνται συνεχώς με την ενίσχυση ολόκληρης την υποδομή της ψηφιακής ασφάλειας. Για να το επιτύχουν αυτό, χρησιμοποιούν λογισμικά σύστημα ανίχνευσης εισβολών (IDS) τα οποίο τους παρέχουν μια συνεχή ανάλυση ασυνήθιστης και ύποπτης δραστηριότητας. Μερικές εργασίες των μπλε ομάδων είναι, οι έλεγχοι ασφαλείας (DNS), η καταγραφή και η ανάλυση μνήμης, η δέσμευση πακέτων (PCAP), η ανάλυση δεδομένων κινδύνου πληροφοριών, η ανάλυση ψηφιακού αποτυπώματος, η αντίστροφη μηχανική, οι δοκιμές (DDoS), η ανάπτυξη σεναρίων κινδύνου κλπ. [30]

2. Red Teaming. Οι κόκκινες ομάδες, προσομοιώνουν έναν δυνητικό αντίπαλο στη μεθοδολογία και τις τεχνικές. Οι ομάδες αυτές, είναι συνήθως μεγαλύτερες αριθμητικά από τις ομάδες δοκιμών διείσδυσης και έχουν πολύ πιο μεγάλο πεδίο δράσης. Οι κόκκινες

ομάδες, κάνουν επιθέσεις και προσβάλλουν συχνά έναν οργανισμό στόχο, μέσω τεχνικών, κοινωνικών και φυσικών μέσων. Αρκετά συχνά, χρησιμοποιούν ίδιες τεχνικές, όπως αυτές που χρησιμοποιούνται από τις ομάδες Black Hat, με σκοπό να δοκιμάσουν την προστασία των οργανισμών ή των πληροφοριακών συστημάτων. Επιπρόσθετα, οι κόκκινες ομάδες εκτελούν επιθέσεις κοινωνικής μηχανικής, συμπεριλαμβανομένων των τεχνικών «phishing» και «spear phishing», ως επίσης και φυσικές επιθέσεις με σκοπό να αποκτήσουν πληροφορίες και πρόσβαση. Για να είναι πραγματικά αποτελεσματικές, οι κόκκινες ομάδες πρέπει να γνωρίζουν όλες τις τακτικές, τις τεχνικές και τις διαδικασίες που χρησιμοποιεί ένας εισβολέας. Εφαρμόζοντας τες, προσπαθούν να εκμεταλλευτούν τα τρωτά σημεία της ασφάλειας, αλλά χωρίς να γνωρίζουν τίποτα σχετικά με την άμυνα που υπάρχει στην υποδομή του οργανισμού. Ο τύπος των δοκιμών των κόκκινων ομάδων, σχετίζεται με την αξιολόγηση των τεχνικών, των διοικητικών και λειτουργικών ρυθμίσεων και των ελέγχων ενός συστήματος. [03] Οι διαχειριστές του δικτύου στόχου και το προσωπικό του, ενδέχεται να γνωρίζουν ή να μην γνωρίζουν, ότι διεξάγεται άσκηση από μια κόκκινη ομάδα. Έτσι, μια προσομοίωση επίθεσης από τέτοιες ομάδες, που εκτελούνται εν άγνοια του προσωπικού και που έχουν αναχαιτισθεί, θεωρούνται μεγάλη υπόθεση και επιτυχία του τομέα της ασφάλειας του οργανισμού. [22]

Τύποι ομάδων εκτέλεσης δοκιμών διείσδυσης

Ο τύπος των δοκιμών διείσδυσης, εξαρτάται συνήθως από το πεδίο εφαρμογής και τις οργανωτικές επιθυμίες και απαιτήσεις. Ακολουθεί, σύντομη ανάλυση των διαφορετικών τύπων δοκιμών Διείσδυσης. Οι τύπου των ομάδων εκτέλεσης δοκιμών αναφέρονται στο σχήμα 2.3. [10]



Σχήμα 2.3: Τύποι δοκιμών διείσδυσης

1. Ομάδα White Hat. Ονομάζουμε έτσι την ομάδα από επαγγελματίες ασφάλειας υπολογιστών, που ειδικεύονται σε μεθοδολογίες που βελτιώνουν την ασφάλεια των πληροφοριακών συστημάτων. Με αυτήν την προσέγγιση, αυτοί που διεξάγουν την δοκιμή διείσδυσης, είναι εφοδιασμένοι με πλήρεις λεπτομέρειες σχετικά με το περιβάλλον στόχο, όπως είναι συστήματα, δίκτυο, λειτουργικό σύστημα, διευθύνσεις IP, πηγαίο κώδικα, σχήμα, κλπ. Οι ομάδες αυτές, εξετάζουν τον κώδικα και εντοπίζουν σφάλματα στο σχεδιασμό και την ανάπτυξη. Είναι μια προσομοίωση επίθεσης εσωτερικής ασφάλειας. [04]

2. Ομάδα Grey Hat. Η ομάδα αυτή αναφέρεται σε τεχνικούς εμπειρογνώμονες, που βρίσκονται μεταξύ της γραμμής που καθορίζει ο ρόλος μιας ομάδας White Hat και μιας ομάδας Black Hat. Αυτά τα άτομα, προσπαθούν συχνά να παρακάμψουν τα χαρακτηριστικά ασφαλείας ενός πληροφοριακού συστήματος χωρίς άδεια. Δεν έχουν ως στόχο τους το κέρδος, αλλά θέλουν να ενημερώσουν τους διαχειριστές του συστήματος για τις αδυναμίες που ενδέχεται να ανακαλύψουν. Έχουν περιορισμένες λεπτομέρειες σχετικά με το περιβάλλον στόχου. Πρόκειται για μια προσομοίωση, επίθεσης εξωτερικής ασφάλειας. [03]

3. Ομάδα Black Hat. Ονομάζουμε τα άτομα ομάδας που χρησιμοποιούν τις τεχνικές τους ικανότητες, για να παρακάμψουν την ασφάλεια συστημάτων χωρίς την εξασφάλιση άδειας από τους ιδιοκτήτες. Ενεργούν δηλαδή παράνομα, με σκοπό την διάπραξη εγκλημάτων σε ηλεκτρονικούς υπολογιστές. Με αυτήν την προσέγγιση, αξιολογούν το σύστημα «στόχο», το δίκτυο ή τη διαδικασία, χωρίς να γνωρίζουν λεπτομέρειες. Η ομάδα Black Hat, λαμβάνει, πολύ μεγάλο όγκο δεδομένων τα οποία χρησιμοποιούν για να διεισδύουν στο περιβάλλον του στόχου. Κανένας κώδικας, δεν εξετάζεται σε αυτή τη μέθοδο.[23] Τα άτομα της ομάδας αυτής, εκτελούν δοκιμές διείσδυσης και αρκετά συχνά χρησιμοποιούν ανάλογες τεχνικές, με εκείνες που χρησιμοποιούν τα μέλη της κόκκινης ομάδας. Οι τεχνικές αυτές, εφαρμόζονται φυσικά κατά την διεξαγωγή εγκεκριμένων ασκήσεων ή δοκιμών. [04]

Ομάδες Ethical Hacking

Η ομάδα Ethical Hacking, εκτελεί δοκιμές διείσδυσης με σκοπό να επιτεθεί σε συστήματα για λογαριασμό του ιδιοκτήτη ή του οργανισμού που κατέχει τα συστήματα αυτά. Δεν είναι λίγοι, αυτοί που τους θεωρούν, ως τα άτομα που διενεργούν δοκιμές διείσδυσης. Αυτό φυσικά είναι λάθος καθώς στον ορισμό του Ethical Hacking, περιλαμβάνονται όλες οι μέθοδοι παραβίασης συστημάτων με σχετικά εργαλεία κυβερνοεπιθέσεων. Σημειώνεται ότι η δοκιμή διείσδυσης, είναι μόνο ένα χαρακτηριστικό γνώρισμα του Ethical Hacking. Η ομάδα αυτή, σε αντίθεση με όσους εκτελούν δοκιμές διείσδυσης, πρέπει να διαθέτει ολοκληρωμένες γνώσεις από διάφορες τεχνικές προγραμματισμού, ως επίσης και τεχνικές γνώσεις υλικού. Συνήθως, απαιτείται υποχρεωτική πιστοποίηση. Ακόμα, θεωρείται απαραίτητη η πρόσβαση, σε ολόκληρη την υποδομή του πληροφοριακού συστήματος καθώς και των συστημάτων που το περιβάλλουν. [18]

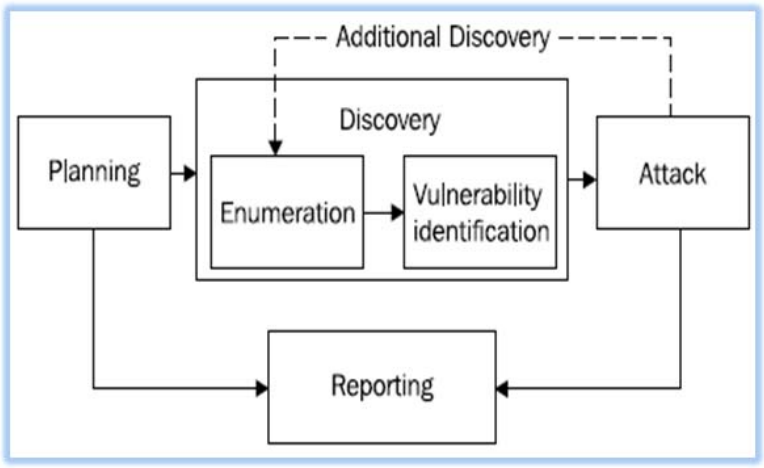
Κεφάλαιο 3

Διαδικασίες, Απαιτούμενα Εργαλεία

Η πιο σημαντική πτυχή των δοκιμών διείσδυσης, θεωρείται η δοκιμή ασφαλείας. Η δοκιμή ασφαλείας, δεν πρέπει να θεωρείται ως προϊόν αλλά ως μια διαδικασία. Ειδικότερα, οι δοκιμές αυτές λαμβάνουν υπόψη τους κύριους τομείς ενός μοντέλου ασφάλειας, τον τομέα δηλαδή της Αυθεντικοποίησης, της Εξουσιοδότησης, της Εμπιστευτικότητας, της Ακεραιότητας και της Διαθεσιμότητας. Κάθε μία από αυτές τις συνιστώσες, πρέπει να εφαρμόζεται πιστά όταν ένας οργανισμός βρίσκεται στη διαδικασία, οικοδόμησης μιας ασφαλούς αρχιτεκτονικής. Το ζήτημα φυσικά είναι, ότι όταν δοκιμάζουμε την ασφάλεια, πρέπει να αντιμετωπίσουμε πάντοτε κάθε μία από αυτές τις συνιστώσες. Η έλλειψη τάξης και δομής, σε μια δοκιμή διείσδυσης συχνά οδηγεί σε απογοήτευση και αποτυχία. Οι δοκιμές διείσδυσης είναι κάτι περισσότερο από μια απλή εκμετάλλευση. [33]

3.1 Μεθοδολογία, φάσεις και βήματα δοκιμών

Η μεθοδολογία των δοκιμών διείσδυσης, όπως φαίνεται στο σχήμα 3.1, ακολουθεί μια σειρά από βήματα-φάσεις. Η πρώτη φάση, είναι η φάση του προγραμματισμού (Planning) και δεύτερη είναι η φάση της ανακάλυψης (Discovery). Η επόμενη είναι η φάση της επίθεσης (Attack) και τελευταία η φάση της Αναφοράς (Reporting). Οι φάσεις προγραμματισμού και αναφοράς, γίνονται συνήθως μία φορά κατά τη διάρκεια του έργου σε αντίθεση με τις φάσεις της ανακάλυψης και της επίθεσης που μπορούν να επαναλαμβάνονται πολλές φορές, ανάλογα με τα αποτελέσματά τους. Η φάση της ανακάλυψης, περιλαμβάνει δύο άλλες υποκατηγορίες-βήματα, την μη επιθετική αναζήτηση στόχων (enumeration) και την παρεμβατική αναζήτηση στόχων (vulnerability identification). [15] Όλες οι φάσεις αναλύονται πιο κάτω.



Σχήμα 3.1: Διάγραμμα της ροής μιας εργασίας δοκιμής διείσδυσης

Φάση Προγραμματισμού

Η φάση του προγραμματισμού, παρόλο που αποτελεί το πιο κρίσιμο βήμα για τις επαγγελματικές δοκιμές διείσδυσης, δυστυχώς, είναι ένα από τα βήματα που σπάνια του δίνεται ο απαιτούμενος χρόνος, κυρίως λόγο προϋπολογισμού. Έτσι, καταλαμβάνει ένα πολύ μικρό μέρος του χρόνου της σύμβασης. Η ροή της εργασίας σε μια δοκιμή διείσδυσης, ξεκινά από την φάση του προγραμματισμού, όπου διαπραγματεύονται όλα τα ερωτήματα. Στη φάση αυτή, λαμβάνονται όλες οι εγκρίσεις, ρυθμίζεται ο χρόνος εργασίας και οι καθορίζονται οι ημερομηνίες υλοποίησης. Παράλληλα εκτελούνται και άλλες εργασίες διαχείρισης που μαζί με τις πληροφορίες που συλλέγονται, χρησιμοποιούνται για την δημιουργία της αναφοράς στη τελευταία φάση. [06]

Φάση Ανακάλυψης - Μη επιθετική αναζήτηση στόχων

Η μη επιθετική αναζήτηση στόχων, αποτελεί το βήμα αναζήτησης δημόσιων πληροφοριών, είτε μέσω των εργαλείων ανοικτού κώδικα, είτε μέσω άλλων εμπορικών εργαλείων. Ουσιαστικά, όλα τα εργαλεία καταλήγουν να εξάγουν πληροφορίες για το θύμα-στόχο. Μερικά από αυτά είναι το nslookup, το traceroute κλπ. Η μη επιθετική αναζήτηση στόχων αποτελεί υποκατηγορία της δεύτερης φάσης της εργασίας, την φάση της ανακάλυψης. Στην φάση αυτή γίνεται και η αναγνώριση των ευπαθειών από τις πληροφορίες που αποκτήθηκαν. Επίσης, αποτελεί την διαδικασία για αναγνώριση των δικτύων στόχων και την εξόρυξη των δεδομένων. Σε αυτή, περιλαμβάνονται διευθύνσεις IP των ανοιχτών θυρών, των υπηρεσιών δικτύου και των εκδόσεων, των λειτουργικών συστημάτων κλπ. [02]

Η εξόρυξη δεδομένων από ένα στόχο, γίνεται με ανάλυση των αντιδράσεων και των απαντήσεων του στόχου με μια εξωτερική αλληλεπίδραση. Αυτή η αλληλεπίδραση, ονομάζεται απαρίθμηση και μπορεί να πραγματοποιηθεί μέσω αυτοματοποιημένων εργαλείων, μέσω της σάρωσης ή με το χέρι. Όπως συμβαίνει με τη διαδικασία της απαρίθμησης, οι εργασίες στην φάση της ανακάλυψης, μπορούν να είναι, αυτοματοποιημένες, μη αυτοματοποιημένες ή μικτές. Φυσικά, η αυτοματοποιημένη προσέγγιση, προϋποθέτει τη χρήση εξειδικευμένων εργαλείων λογισμικού. Η μη αυτοματοποιημένη προσέγγιση, από την άλλη, χρησιμοποιεί μέσα σύγκρισης των εκδόσεων του λογισμικού ενός στόχου. Οι πληροφορίες, μπορεί να αποκτούνται κατά τη διάρκεια της διαδικασίας απαρίθμησης ή μέσω της χρήσης βάσεων δεδομένων ευπάθειας, την ανάλυση της συμπεριφοράς των στόχων ή μετά από την εισαγωγή δεδομένων. Γενικά, οι διάφοροι τύποι σάρωσης μπορούν να χρησιμοποιούνται ταυτόχρονα στη φάση ανακάλυψης εάν δεν υπάρχει τρόπος για αποφυγή του συστήματος IDS. [03]

Φάση Ανακάλυψης - Παρεμβατική αναζήτηση στόχων

Η παρεμβατική αναζήτηση στόχων, αποτελεί και αυτή υποκατηγορία της φάσης ανακάλυψης. Είναι το βήμα που ξεκινά την πραγματική δραστηριότητα ενός εισβολέα, αφού μέσω της, γίνονται διάφορες δοκιμές και εκτελέσεις ελέγχων προς την εξερεύνηση του δικτύου που βρίσκεται ο στόχος. Απαραίτητη προϋπόθεση όμως πριν την πραγματοποίηση της δραστηριότητας αυτής, είναι η εξασφάλιση της ρητής συγκατάθεσης του ιδιοκτήτη συνήθως μετά από γραπτή άδεια. Στο πλαίσιο αυτού του βήματος, υπάρχουν πέντε στοιχεία που καθορίζουν περαιτέρω την μεθοδολογία. Τα στοιχεία αυτά αναλύονται πιο κάτω. [02]

1. Η Αναζήτηση ζωντανών συστημάτων αποτελεί το πρώτο στοιχείο, εναντίων των οποίων θα γίνει η επίθεση. Ένα ισχυρό εργαλείο ανοικτού κώδικα, που μπορεί να χρησιμοποιηθεί για το σκοπό αυτό είναι το nmap. Ανάλογα εργαλεία, για σάρωση δικτύων και εύρεση ζωντανών συστημάτων, είναι το Netdiscover, το Arp-Scan το Arping κλπ. [02]

2. Η Αναζήτηση των ανοικτών Θυρών του συστήματος, αποτελεί το δεύτερο στοιχείο της μεθοδολογίας. Η παραμετροποίηση του εργαλείου nmap, ικανοποιεί και το δεύτερο στοιχείο της μεθοδολογίας. Οι ανοικτές πόρτες, καταδεικνύουν ότι υπάρχει το ενδεχόμενο προσβασιμότητας. Άλλα εργαλεία που χρησιμοποιούνται ως σαρωτές αναζήτησης ανοικτών θυρών σε συστήματα είναι, το Unicornscan, Hping3 κλπ. [02]

3. Το τρίτο στοιχείο, είναι η καταγραφή του λειτουργικού συστήματος. Το στοιχείο αυτό αναζητείται αφού εξασφαλιστούν τα ζωντανά συστήματα και οι ανοικτές πόρτες στο σύστημα στόχο. Εκτός από την καταγραφή των λειτουργικών συστημάτων, καταγράφονται και άλλα προγράμματα ή υπηρεσίες που τρέχουν σε αυτό. Η απαρίθμηση (Enumeration), αποτελεί τη διαδικασία εξαγωγής περισσότερων πληροφοριών σχετικά με τον πιθανό στόχο, με σκοπό να συμπεριληφθεί το λειτουργικό σύστημα, τα ονόματα των χρηστών, τα ονόματα των μηχανών και άλλες λεπτομέρειες που μπορεί να ανακαλυφθούν. Οι πληροφορίες που συγκεντρώνονται χρησιμοποιούνται για τον εντοπισμό των τρωτών σημείων ή των αδύναμων σημείων στην ασφάλεια του συστήματος και στη συνέχεια προσπαθούν να την εκμεταλλευτούν. Υπάρχουν πολλοί τρόποι συλλογής δεδομένων. Μπορούν να συλλεγούν από τους χρήστες του δικτύου, από τους πίνακες δρομολόγησης και πληροφορίες SNMP. Για την εκτέλεση της διαδικασίας απαρίθμησης, χρησιμοποιείται και πάλι το εργαλείο nmap. [20]

4. Ο Προσδιορισμός τρωτότητας συστήματος αποτελεί το τέταρτο στοιχείο της μεθοδολογίας. Πέραν του προσδιορισμού των τρωτών σημείων του συστήματος γίνεται εκ νέου επεξεργασία όλων των προηγούμενων βημάτων. Στον προσδιορισμό τρωτότητα του συστήματος περιλαμβάνεται και η λήψη πληροφοριών για ευπάθειες και αδυναμίες, είτε από το διαδίκτυο, σχετικά με τις υπηρεσίες και τις εκδόσεις του λογισμικού που εκτελούνται στο μηχάνημα, είτε με την χρήση εργαλείων σάρωσης ευπαθειών. Υπάρχουν αρκετοί σαρωτές ευπάθειας στην αγορά, που προσφέρονται μέσω εμπορικών εργαλείων ή εργαλείων ανοικτού κώδικα. Τα εμπορικά εργαλεία φυσικά, περιέχουν πολύ περισσότερες λειτουργίες από ότι τα εργαλεία ανοιχτού κώδικα, αλλά έχουν ένα αρκετά

υψηλό κόστος. Ένα αρκετά καλό αλλά εμπορικό εργαλείο για σάρωση ευπαθειών, είναι το Nexpose. [02]

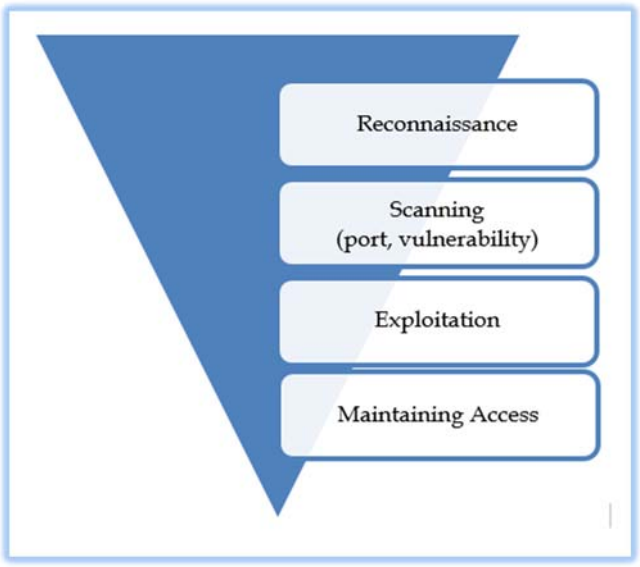
5. Η επικύρωση των ευπαθειών που ανακαλύφθηκαν είναι το τελευταίο στοιχείο της μεθοδολογίας. Με την εφαρμογή της επικύρωσης ολοκληρώνεται και η παρεμβατική αναζήτηση των στόχων, η διαδικασία δηλαδή της εκμετάλλευσης (Exploitation) του συστήματος στόχου. Στην ουσία με την επικύρωση γίνεται εκτέλεση μέρους ενός κώδικα, στο μηχάνημα στόχο, ο οποίος ενδέχεται να προκαλέσει ζημιά στο μηχάνημα. Το πιο δημοφιλές δωρεάν εργαλείο εκμετάλλευσης, είναι το Metasploit. Περισσότερες πληροφορίες για την διαδικασία εκμετάλλευσης γίνεται στην επόμενη παράγραφο. [43]

Φάση επίθεσης και τεχνικές

Η επόμενη φάση αποτελεί την ίδια την διείσδυση και εφαρμόζεται εναντίον γνωστών τρωτών σημείων, με τη διεξαγωγή διαφορετικών επιθέσεων. Οι επιθέσεις γίνονται ενάντια στα συστήματα στόχων και ονομάζονται εκμεταλλεύσεις (exploitations) των ευπαθειών. Μετά από μια επιτυχημένη εκμετάλλευση, είναι στην ευχέρεια αυτού που εκτελεί την διείσδυση, να ακολουθήσει όποια διαδρομή επιθυμεί για να φτάσει σε άλλα συστήματα, τα οποία ήταν αρχικά μη προσβάσιμα. Σε τέτοια περίπτωση, αυτός που διενήργησε την διείσδυση, επιστρέφει στη φάση ανακάλυψης και το επαναλαμβάνει για νέους στόχους. Έτσι, οι φάσεις ανακάλυψης και επίθεσης θα μπορούσαν να επαναληφθούν αρκετές φορές, ανάλογα με το πεδίο εφαρμογής και τις συμφωνίες τους με τον πελάτη. Σύμφωνα με το πεδίο εφαρμογής, ενδέχεται να υπάρξει ανάγκη συλλογής τεράστιου όγκου πληροφορίων, όπως είναι τα δεδομένα των χρηστών του δικτύου, οι πίνακες δρομολόγησης, οι πληροφορίες SNMP κλπ. [43]

Τα βήματα μιας επίθεσης, είτε αυτά προέρχονται από την πλευρά των επιτιθέμενων είτε από την πλευρά αυτών που υπερασπίζονται συστήματα, είναι τα ίδια. Πηγάζουν από την μεθοδολογία, των φάσεων και των βήματα δοκιμών διείσδυσης όπως φαίνονται στο σχήμα 3.1. Διακρίνονται δε, σε τέσσερις τεχνικές, την τεχνική της αναγνώρισης (Reconnaissance), της σάρωσης (Scanning), της εκμετάλλευσης (Exploitation) και της διατήρηση της πρόσβασης (Maintaining Access). Μερικές φορές, η κατανόηση των τεχνικών βημάτων γίνεται καλύτερα αντιληπτή, όταν παρουσιάζεται σε μορφή απεικόνισης, όπως φαίνεται στο σχήμα 3.2 που ακολουθεί. Η απεικόνιση, αναδεικνύει την προσέγγιση αυτή και το λόγο που έχει χρησιμοποιηθεί το ανεστραμμένο τρίγωνο. Η επεξήγηση είναι απλή. Από την εκτέλεση των βημάτων της πρώτης

φάσης μαζεύονται αρκετές πληροφορίες για το σύστημα στόχο, οι οποίες είναι πολύ δύσκολο να αναλυθούν. Κάθε φορά όμως, που εκτελείται το επόμενο βήμα της μεθοδολογίας, τα αποτελέσματα γίνονται ολοένα και πιο συγκεκριμένα, με αποτέλεσμα στο τέλος της διαδικασίας η ανάλυση τους να είναι αρκετά πιο εύκολη. [43]

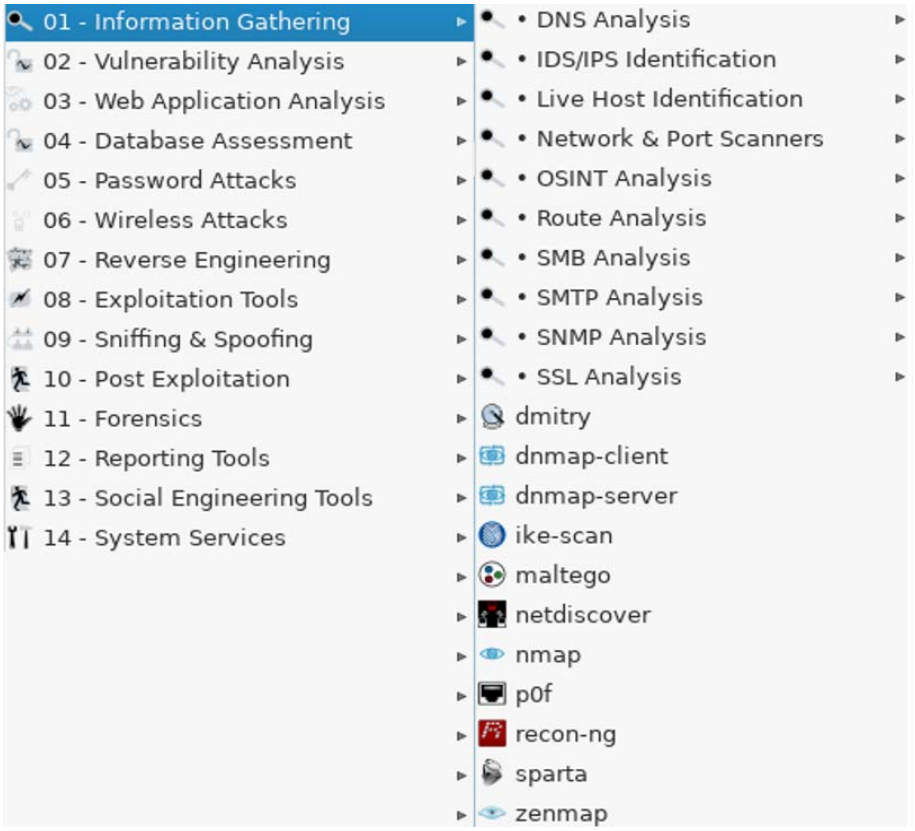


Σχήμα 3.2: Βήματα επίθεσης ανεστραμμένου τριγώνου

Οι πληροφορίες αυτές που συγκεντρώνονται στην αρχική φάση αξιολογούνται ανάλογα. Ενδέχεται να αποδειχθούν κρίσιμες για την επιτυχή ολοκλήρωση μιας εκμετάλλευσης και την απόκτηση πρόσβασης στο σύστημα. Είναι για αυτόν ακριβώς το λόγο που σε κάθε μεταγενέστερη φάση-βήμα, οι τεχνικές έναντι του στόχου, γίνονται πιο συγκεκριμένες και πιο λεπτομερείς. Σε αυτό, βοηθούν τα ερωτήματα όπως, πού βρίσκεται ο στόχος; ποια είναι η IP διεύθυνση του; ποιο λειτουργικό σύστημα τρέχει σε αυτό; ποιες είναι οι εκδόσεις του λογισμικού του; Τι υπηρεσίες υπάρχουν σε αυτό; [36]

Εξίσου σημαντικό, είναι και το γεγονός ότι τα βήματα πρέπει να εκτελούνται κατά σειρά. Κάθε επόμενο βήμα δηλαδή, εξαρτάται από το αποτέλεσμα του προηγούμενου. Έτσι, η κατανόηση της σωστής σειράς στην οποία εκτελούνται τα βήματα, οδηγεί σε μια περιεκτική και πιο ρεαλιστική δοκιμή διείσδυσης. Αρκετοί νεοεισερχόμενοι στο χώρο, παραλείπουν τη φάση της αναγνώρισης και πηγαίνουν κατ 'ευθείαν στην φάση της εκμετάλλευσης του στόχου τους. Η μη ολοκλήρωση των πρώτων δύο βημάτων, τους αφήνει με ένα σημαντικά μικρότερο κατάλογο στόχων και μικρότερο εύρος τεχνικών επίθεσης. [36] Πιο κάτω ακολουθεί η ανάλυση των τεχνικών επίθεσης.

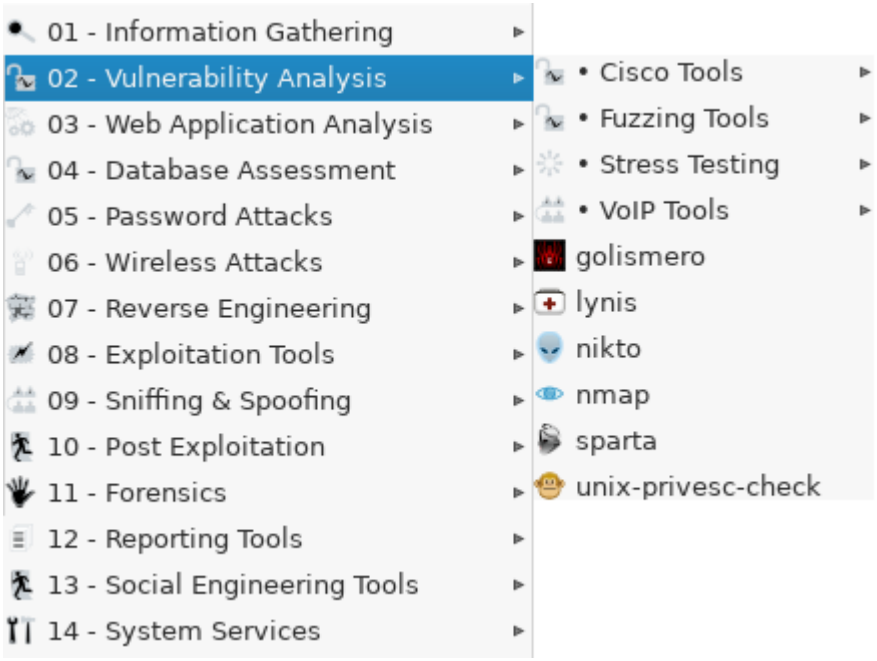
1. Τεχνική Αναγνώρισης. Η τεχνική της αναγνώρισης, αποτελεί το πρώτο βήμα σε κάθε δοκιμή διείσδυσης. Σε αρκετές διανομές, όπως για παράδειγμα στην διανομή kali Linux (σχήμα 3.3), χρησιμοποιείται με την ονομασία συγκέντρωση πληροφοριών (Information Gathering). Άλλες διανομές, χρησιμοποιούν την ονομασία αναγνώριση (Reconnaissance). Το βήμα αυτό, ασχολείται με τη συλλογή πληροφοριών σχετικά με το στόχο. Όπως αναφέρθηκε προηγουμένως, όσο περισσότερες πληροφορίες συγκεντρώνονται για τον στόχο, τόσο πιο πιθανό είναι να πετύχουν τα επόμενα βήματα. Αφού συμπληρωθεί η διαδικασία της αναγνώρισης, πρέπει να έχει εξασφαλισθεί η σχετική λίστα διευθύνσεων IP, με τους προορισμούς που μπορούν να σαρωθούν. Μερικά εργαλεία που χρησιμοποιούνται στο βήμα αυτό είναι: Arping, Arp-scan, Automater, Knock, Zenmap, Regon-ng κλπ. Αρκετά από αυτά τα εργαλεία επεξηγούνται στο Παράρτημα Β1. [05]



Σχήμα 3.3: Εργαλεία αναγνώρισης για διανομή Kali Linux

2. Τεχνική Σάρωσης. Το δεύτερο βήμα της μεθοδολογίας, μπορεί να διαχωριστεί σε δύο ξεχωριστές δραστηριότητες. Η πρώτη δραστηριότητα που πραγματοποιούμε είναι η σάρωση στις θύρες των συστημάτων του δικτύου. Αφού τελειώσει η σάρωση των θυρών, θα εξασφαλιστεί μια λίστα με όσες από αυτές είναι ανοιχτές. Έτσι, θα μπορεί να συνεχιστεί ο έλεγχος ως προς την κατεύθυνση, οι πόρτες να οδηγούν σε υπηρεσίες που τρέχουν ή

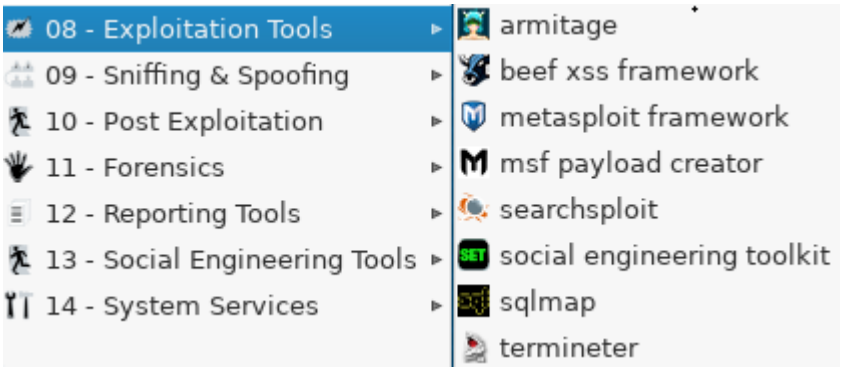
είναι απαραίτητες για το σύστημα στόχο. Η δεύτερη δραστηριότητα στη φάση σάρωσης είναι σάρωση ευπάθειας (Vulnerability scanning), η διαδικασία εντοπισμού και αναγνώρισης συγκεκριμένων αδυναμιών στο λογισμικό και τις υπηρεσίες που τρέχουν ή εκτελούνται στο σύστημα στόχο. Στο βήμα αυτό, γίνεται προσπάθεια ταυτοποίησης συστημάτων που βρίσκονται σε λειτουργία και των υπηρεσιών τους που υπάρχουν σε αυτά. Δίκτυα που βρίσκονται σε πλήρη απομόνωση, χωρίς σύνδεση στο διαδίκτυο και χωρίς υπηρεσίες όπως, το ηλεκτρονικό ταχυδρομείο είναι πολύ σπάνια να υπάρχουν σήμερα. Έτσι κάθε υπηρεσία, σύνδεση ή δυνατότητα σύνδεσης σε άλλο δίκτυο, είναι λογικό να παρέχει μια πιθανή ευκαιρία εκμετάλλευσης για έναν εισβολέα. Συνοψίζοντας, στο βήμα της σάρωσης εκτελούνται , τρεις ξεχωριστές φάσεις. Στην πρώτη φάση, γίνεται προσδιορισμός εάν ένα σύστημα βρίσκεται σε λειτουργία, στην δεύτερη, γίνεται η σάρωση των πιθανών θυρών που είναι ανοικτές στο σύστημα και στη τρίτη γίνεται η σάρωση του συστήματος για ευπάθειες. Στο σχήμα 3.4, που ακολουθεί, φαίνεται η γκάμα με τα εργαλεία που χρησιμοποιεί η διανομή Kali Linux, για να εκτελέσει το βήμα της σάρωσης. Μερικά εργαλεία που χρησιμοποιούνται στο βήμα αυτό είναι: Cvechecker, RIPS, OpenVAS, Nikto, SkipFish, ZAP. Αρκετά από αυτά, επεξηγούνται στο Παράρτημα Β1. [11]



Σχήμα 3.4: Εργαλεία σάρωσης, για διανομή Kali Linux

3. Τεχνική Εκμετάλλευσης. Το βήμα της εκμετάλλευσης (Exploitation), ακολουθεί το βήμα της σάρωσης και τροφοδοτείτε με την λίστα των ανοικτών θυρών και τις υπηρεσίες που τρέχουν σε αυτές. Το βήμα της εκμετάλλευσης, αποτελεί την διαδικασία απόκτησης ελέγχου ενός συστήματος και μπορεί να περιλαμβάνει πολλές διαφορετικές τεχνικές,

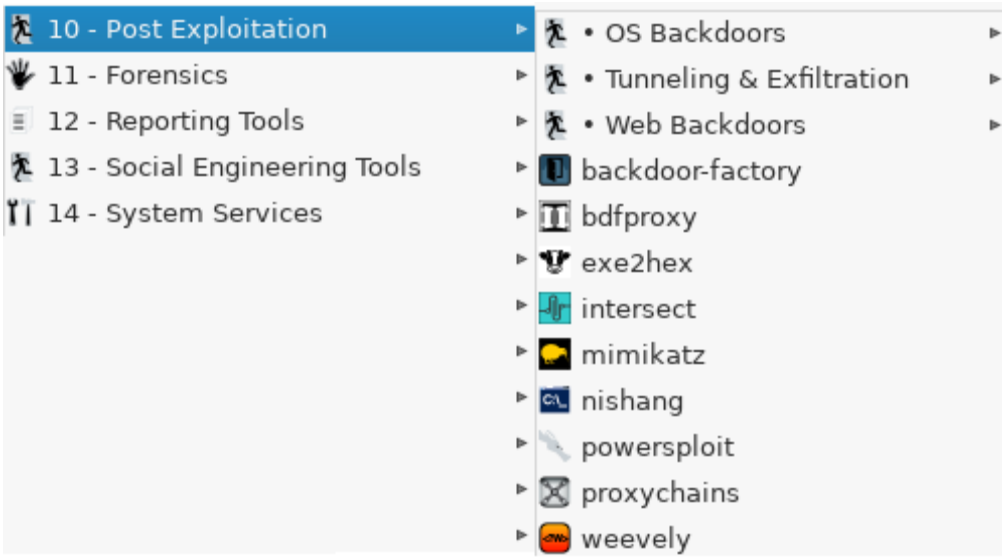
εργαλεία και κώδικα. Ο απώτερος στόχος της είναι η εξασφάλισης διαχειριστικής πρόσβασης (administrative access). Μέσω του βήματος αυτού, γίνεται προσπάθεια να μετατραπεί ο υπολογιστής-στόχος σε μαριονέτα, που θα εκτελεί εντολές. Ουσιαστικά η τεχνική της εκμετάλλευσης είναι η διαδικασία αποστολής, μιας εκμετάλλευσης (exploit). Η εκμετάλλευση είναι προβλήματα ή σφάλματα στον κώδικα λογισμικού που επιτρέπουν σε έναν εισβολέα να αλλάξει την αρχική λειτουργικότητα του λογισμικού. Η πραγματοποίηση δηλαδή μιας ευπάθειας. Η έλλειψη τάξης και δομής, σε μια δοκιμή διείσδυσης συχνά οδηγεί σε λανθασμένα συμπεράσματα και αποτυχία. Οι δοκιμές διείσδυσης είναι κάτι περισσότερο από απλή εκμετάλλευση. Η διανομή Kali Linux, όπως φαίνονται στο σχήμα 3.5, χρησιμοποιεί αρκετά προεγκατεστημένα εργαλεία όπως είναι το Armitage, το Metasploit, το Beef κλπ. , για να εκτελέσει το βήμα της εκμετάλλευσης. Άλλα εργαλεία που χρησιμοποιούνται στο βήμα αυτό είναι: Sqlmap, MSF, Armitage, Fimap, Weaf, Wpscan, κλπ. Αρκετά από αυτά επεξηγούνται στο Παράρτημα Β1. [05]



Σχήμα 3.5: Εργαλεία εκμετάλλευσης, για διανομή Kali Linux

4. Τεχνική Διατήρησης της Πρόσβασης. Το τελευταίο βήμα, είναι η διατήρηση της πρόσβασης, (Maintaining Access). Πολλές φορές, τα φορτία πληροφοριών (payloads) που χρησιμοποιούνται στη φάση εκμετάλλευσης, παρέχουν μόνο προσωρινή πρόσβαση. Τα περισσότερα φορτία πληροφοριών, δεν είναι επιθετικά. Έτσι, πρέπει να γίνεται προσπάθεια για δημιουργία μιας πιο μόνιμης σύνδεσης με το σύστημα στόχο. Τα φορτία πληροφοριών, είναι είτε εντολές, είτε κείμενο με οδηγίες που έχει την ιδιότητα να μετατρέπεται σε κώδικα, ο οποίος εκτελείται στο υπολογιστή στόχο. Στο βήμα της διατήρησης πρόσβασης, γίνεται προσπάθεια η συνδεσιμότητα με το σύστημα στόχο, να παραμένει ζωντανή, ακόμα και όταν το πρόγραμμα κλείνει ή επανεκκινά. Αυτό επιτυγχάνεται φυσικά, εάν έχει προηγούμενα εξασφαλίσει η διαχειριστική πρόσβαση του συστήματος, έτσι επιβάλλεται να γίνονται πολύ προσεκτικοί χειρισμοί. Η διανομή Kali

Linux, όπως φαίνεται στο σχήμα 3.6, περιλαμβάνει στα εργαλεία της το βήμα αυτό, με την ονομασία «μετά την εκμετάλλευση» (Post Exploitation). Εργαλεία που χρησιμοποιούνται στο βήμα της διατήρησης της πρόσβασης είναι: Iodine, Ptunnel, Weevely, κλπ. Αρκετά από αυτά επεξηγούνται στο Παράρτημα Β1. [05]



Σχήμα 3.6: Εργαλεία για διατήρηση της πρόσβασης, στη διανομή Kali Linux

Φάση Δημιουργίας Αναφορών

Η δημιουργία αναφορών, είναι συνήθως ένας τομέας που συχνά παραβλέπετε. Παρόλο που δεν περιλαμβάνεται ως επίσημο βήμα στη μεθοδολογία των δοκιμών διείσδυσης, η τελική και αναμφίβολα η πιο σημαντική δραστηριότητα των δοκιμών διείσδυσης, είναι η δημιουργία της αναφοράς. Η φάση της αναφοράς, αποτελεί τον τρόπο παρουσίασης των ευρημάτων στον πελάτη, ο οποίος καθορίζει το χρόνο και τον προγραμματισμό για την διεξαγωγή της δοκιμής διείσδυσης. Είναι γεγονός ότι ο πελάτης είναι αυτός που κρίνει συχνά την εργασία και την αποτελεσματικότητά των δοκιμών, με βάση την ποιότητα της αναφοράς. Η τελική έκθεση, πρέπει να περιλαμβάνει όλες τις σχετικές πληροφορίες που αποκαλύπτονται στη δοκιμή διείσδυσης. Πρέπει να εξηγεί, λεπτομερώς τον τρόπο με τον οποίο διεξήχθη η δοκιμασία, καθώς και τι έγινε κατά τη διάρκεια της δοκιμής. Σκοπός της, είναι να παράσχει μια απλή μη-τεχνική επισκόπηση των αποτελεσμάτων, πολύ συνοπτικά. Η έκθεση, πρέπει να επισημαίνει και να συνοψίζει τα περισσότερα κρίσιμα ζητήματα της δοκιμής. Είναι ύψιστης σημασίας και πρέπει να είναι ευανάγνωστη και κατανοητή τόσο από τεχνικό και μη τεχνικό προσωπικό. Αυτός είναι και ο λόγος που πρέπει να μην περιλαμβάνει πάρα πολλές τεχνικές λεπτομέρειες. Επίσης, αρκετά σημαντικό είναι και το γεγονός, ότι η βελτίωση της στάσης ασφαλείας, βασίζεται στα ευρήματα που αναφέρονται στην έκθεση. Στα ευρήματα, γίνονται οι διάφορες συστάσεις, ως προς την λήψη

μέτρων που θα συμβάλουν στον μετριασμό του κινδύνου ως επίσης και για οποιαδήποτε άλλα ζητήματα ασφάλειας αποκαλύφθηκαν. [06]

Τα δύο κύρια συστατικά που χρησιμοποιούνται κατά την δημιουργία αναφορών, είναι η περίληψη των ευρημάτων σε μορφή πίνακα και το τμήμα λεπτομερών ευρημάτων. Η περίληψη των ευρημάτων σε μορφή πίνακα, γίνεται κατά τρόπο ώστε εξάγονται εύκολα και κατανοητά συμπεράσματα. Στο τμήμα λεπτομερών ευρημάτων, πέραν των σχετικών πληροφοριών για τα ευρήματα, περιλαμβάνεται μια βαθμολογία, σύμφωνα με τη σοβαρότητα τους. Στις πληροφορίες, συμπεριλαμβάνεται, η περιγραφή της ευπάθειας και οι παράγοντες που επηρεάζονται από αυτή. Ακόμα περιλαμβάνεται η παρουσίαση της έρευνας που έγινε, αναφορά στους πόρους που χρησιμοποιήθηκαν και ανάλυση της ευπάθειας ως προς τον τρόπο που επίδρασε στην εταιρεία. Η μορφή της έκθεσης ευπάθειας, προσαρμόζεται σε διάφορες μορφές, HTML, XML, MS Word ή PDF, σύμφωνα με τις ανάγκες αυτού για τον οποίο διεξάγεται. [11]

3.2 Κατηγορίες, Κριτήρια και Χρήση εργαλείων

Κατηγορίες εργαλείων δοκιμών διείσδυσης

Τα εργαλεία που χρησιμοποιούν οι ομάδες που εκτελούν δοκιμές διείσδυσης, χωρίζονται σε τρείς κύριες κατηγορίες, τα στατικά εργαλεία, τα δυναμικά εργαλεία και τα εργαλεία διαδραστικής ανάλυσης. Τα στατικά εργαλεία εκμεταλλεύονται τα πρότυπα γνωστών τρωτών σημείων στον πηγαίο κώδικα ενώ τα δυναμικά εργαλεία, εκτελούν δοκιμές σύγκρουσης με το σύστημα. Αυτό γίνεται χρησιμοποιώντας τα πρότυπα γνωστών επιθέσεων. Τέλος, τα εργαλεία διαδραστικής ανάλυσης, κάνουν εγκατάσταση ενός πράκτορα (agent) σε έναν διακομιστή ή σε μια ενσωματωμένη βιβλιοθήκη κωδικών. Δημιουργείται έτσι, μια έκδοση ελέγχου και οργάνωσης του λογισμικού για ευκολότερη ανίχνευση των αδυναμιών. Τα εργαλεία γενικά, εάν χρησιμοποιηθούν από ένα εξειδικευμένο επαγγελματία, μπορούν να δημιουργήσουν πολλά δεδομένα για επεξεργασία αφού έχουν δυνατότητα να προσαρμόζονται κατά τρόπο ώστε να ταιριάζουν σε κάθε σύστημα, βάση των απαιτήσεων. [17]

Κριτήρια για την επιλογή του καλύτερου εργαλείου διείσδυσης

Πριν την επιλογή ενός εργαλείου, με το οποίο θα εκτελεστεί η δοκιμή διείσδυσης πρέπει να λαμβάνονται υπόψη, αρκετοί παράγοντες. Μερικοί από αυτούς είναι η ευκολία στην ανάπτυξη, στη διαμόρφωση και στην χρήση του. Πρέπει να μπορεί να σαρώνει εύκολα διάφορα συστήματα και να βάζει σε κατηγορίες τα τρωτά σημεία του συστήματος, ανάλογα με την σοβαρότητα του καθενός. Παράλληλα, πρέπει να θέτει προτεραιότητες για την άμεση επιδιόρθωση τους, να είναι σε θέση να αυτοματοποιεί την επαλήθευση των τρωτών σημείων και να μπορεί να επαληθεύει εκ νέου τις προηγούμενες παραβιάσεις. Σημαντικότερο των όλων, είναι να δημιουργεί λεπτομερείς αναφορές ευπάθειας και αρχεία καταγραφής (log files). Μερικές φορές, αυτά τα εργαλεία μπορούν να εξάγουν λανθασμένα συμπεράσματα (false positive), με αποτέλεσμα να δαπανείται περισσότερος χρόνος κατά την ανάλυση των τρωτών σημείων, που στην πραγματικότητα δεν υπάρχουν. Αφού γίνουν γνωστές οι δοκιμές που πρέπει να εκτελεστούν, μπορούν είτε να εκπαιδευτούν οι πόροι των εσωτερικών δοκιμών, είτε να μισθωθούν εμπειρογνώμονες που θα ενεργούν ως σύμβουλοι για να εκτελέσουν το έργο της διείσδυσης. Παραδείγματα δωρεάν εργαλείων, τα χαρακτηριστικά των οποίων εμφανίζονται στο παράρτημα Β1, είναι το Nmap, το Nessus, το Metasploit, το Wireshark, το OpenSSL, το Cain & Abel το THC Hydra και το w3af. Παραδείγματα εμπορικών εργαλείων είναι, το Pure Hacking, το Torrid Networks, το SecPoint και το Veracode. [23]

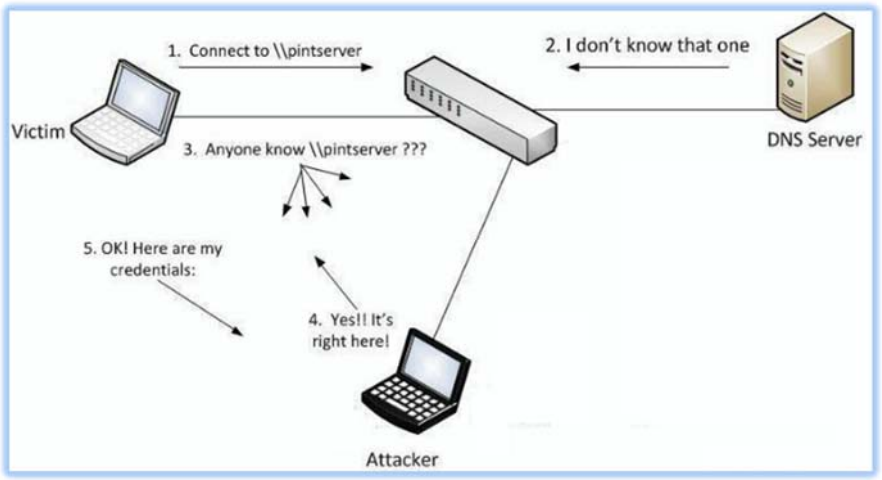
3.3 Χρήση εργαλείων για δοκιμές διείσδυσης

Απαραίτητη προϋπόθεση, πριν να επιχειρήσει κάποιος να διενεργήσει μια δοκιμή διείσδυσης, πρέπει να γνωρίσει τα εργαλεία που θα χρησιμοποιήσει. Τα εργαλεία επιτρέπουν στο άτομο που θα εκτελέσει τις δοκιμές διείσδυσης, να εφαρμόζει σωστά τις διάφορες τεχνικές, όπως είναι οι τεχνικές αναγνώρισης, οι τεχνικές απαρίθμησης και οι υπόλοιπες τεχνικές, στα συστήματα του δικτύου. Στις πλύστες περιπτώσεις, δεν είναι απαραίτητη η φυσική επαφή με τα διάφορα συστήματα, για να κατανοήσει την γενικότερη υποδομή του δικτύου. Μερικά από αυτά τα εργαλεία αναλύονται πιο κάτω. [17]

Responder

Αυτό το εργαλείο, είναι πιθανόν να αποτελεί το πρώτο εργαλείο με το οποίο θα ξεκινήσει ένας pentester τις δοκιμές του. Λειτουργεί σε περιβάλλον Linux και περιλαμβάνεται στα εργαλεία του

Kali linux. Το εργαλείο αυτό, λειτουργεί ως ακροατής (listener) και ακολούθως δηλητηριάζει (poisoning) τις αποκρίσεις από πρωτόκολλα, όπως είναι , το NBT-NS, το LLMNR και το WPAD. Το NBT-NS, είναι ένα πολύ παλιό πρωτόκολλο, το οποίο έχει αφεθεί ενεργοποιημένο από τη Microsoft για λόγους κυρίως συμβατότητας και επιτρέπει, σε εφαρμογές που βασίζονται στο NetBIOS να λειτουργούν μέσω δικτύων TCP / IP. Το LLMNR, είναι ένα πρωτόκολλο, το οποίο έχει σχεδιαστεί με τον ίδιο τρόπο όπως το DNS και βασίζεται στις επικοινωνίες πολυεκπομπής και peer-to-peer, για την επίλυση ονομάτων. Έχει εμφανιστεί, από την εποχή των Microsoft Windows Vista και το πιο πιθανόν δεν χρησιμοποιείται από κανένα πέραν αυτών που γνωρίζουν για την ύπαρξη του. Φυσικά, το χρησιμοποιούν προς όφελος τους όσοι επιθυμούν να επιτεθούν σε συστήματα, δηλητηριάζοντας διάφορα πακέτα στο δίκτυο. Το WPAD, από την άλλη, εξυπηρετεί έναν πολύ πιο λειτουργικό σκοπό στο δίκτυο. Τα περισσότερα δίκτυα που χρησιμοποιούν οι εταιρείες, χρησιμοποιούν ένα αρχείο μεσολάβησης (proxy), με αυτορρύθμιση (PAC) για τον έλεγχο του τρόπου με τον οποίο οι υπολογιστές επικοινωνούν στο διαδίκτυο. Το WPAD, το κάνει αυτό με ιδιαίτερη ευκολία. Τα μηχανήματα διαφημίζονται(broadcast) στο δίκτυο αναζητώντας ένα αρχείο WPAD και λαμβάνουν το PAC που τους δίνεται. Εκεί συμβαίνει η δηλητηρίαση. [27]



Σχήμα 3.7: Παράδειγμα δηλητηρίασης LLMNR /NBT-NS

Στο παράδειγμα του σχήματος 3.7 , ένας εισβολέας μπορεί να ακούσει σε ένα δίκτυο της εκπομπές LLMNR στην θύρα 5355 ή NBT-NS στην θύρα 137 και να απαντήσει σε αυτές, προσποιώντας ότι γνωρίζει τη θέση κάποιου αιτούμενου διακομιστή. Το μηχάνημα του θύματος, προσπαθεί να επικοινωνήσει με τον διακομιστή \\printserver αλλά κάνει λανθασμένο αίτημα στον κεντρικό διακομιστή DNS. Αναζητώντας λανθασμένα τον διακομιστή \\pintsrvr ο οποίος δεν υπάρχει. Το DNS, με την σειρά του αποκρίνεται ότι δεν γνωρίζει κάτι σχετικά με αυτό το αίτημα. Έτσι, το θύμα ρωτά στο δίκτυο εάν υπάρχει κάποιος που γνωρίζει την θέση του. Ο εισβολέας αποκρίνεται στο θύμα ότι αυτός είναι ο διακομιστής που γυρεύει. Το θύμα πιστεύει τον εισβολέα και του στέλνει το

όνομα χρήστη και την hash τιμή του NTLMv2. Ο εισβολέας αποκωδικοποιεί την τιμή αυτή και αποκαλύπτει τον κωδικό πρόσβασης. [20]

Όσοι ασχολούνται με την ασφάλεια στον κυβερνοχώρο γνωρίζουν ότι τα περισσότερα πρωτόκολλα που βασίζονται σε οποιαδήποτε μορφή εκπομπής και μετάδοσης μπορούν εύκολα να τύχουν παραβίασης. Κλασσική τακτική ενός εισβολέα είναι να εμποδίσει τα πιστοποιητικά ενός δικτύου προκαλώντας ρήγματα στα hashes που λαμβάνονται από τα handshakes των αρχικών πρωτοκόλλων. [25]

PowerShell

Πριν να εμφανιστεί το Powershell, τα άτομα που εκτελούσαν δοκιμές διείσδυσης, βασίζονταν στην τεχνική «Command and Control». Μέσω της τεχνικής αυτής, εξασφάλιζαν πρώτα πρόσβαση στο δίσκο του συστήματος στόχου και ακολούθως έκαναν σε αυτόν εγκατάσταση ενός (agent). Ως φυσικό επακόλουθο, ο (agent) γινόταν εύκολα αντιληπτός από το antivirus, ο οποίος τον τοποθετούσε σε μη ενεργή κατάσταση. Φυσικά υπήρχαν τρόποι να ξεγελαστεί ο antivirus, πάντα όμως ως ένα επιπλέον βήμα. Σήμερα, τόσο τα εργαλεία, όσο και ολόκληρο το πλαίσιο εργασίας των ατόμων που εκτελούν τέτοιου είδους δοκιμές έχει μετατοπιστεί σε εντολές μέσω του PowerShell. Το γεγονός αυτό τους δίνει αμέτρητες δυνατότητες κατά την εκτέλεση των δοκιμών διείσδυσης. Φυσικά δεν ήταν αφύσικο, την μεθοδολογία αυτή, να την χρησιμοποιήσουν πολύ γρήγορα και όσοι εκτελούσαν επιθέσεις σε συστήματα. Παρόλο που οι έλεγχοι ασφαλείας, σχεδιάζονται και εφαρμόζονται από καταρτισμένους διαχειριστές ασφάλειας συστημάτων, εντούτοις μπορούν να παρακάμπτονται σχετικά εύκολα. Το PowerShell ουσιαστικά, δίνει την δυνατότητα ανάπτυξης κακόβουλων λογισμικών τα οποία φορτώνονται απευθείας στην μνήμη των συστημάτων, καθιστώντας τα antivirus, λιγότερο αποτελεσματικά. [27]

Hashcat

Το Hashcat, είναι ένα από τα πιο γρήγορα εργαλεία παραβίασης κωδικών πρόσβασης. Χρησιμοποιεί εργαλεία ανάκτησης κωδικών πρόσβασης GPU. Υποστηρίζει διάφορες μορφές αποκωδικοποίησης από μια μεγάλη ποικιλία από hash αλγόριθμους, συμπεριλαμβανομένων των LM hash, NT hash, MD4, MD5, SHA-1, SHA-2, Unix Crypt formats κλπ. Συνήθως χρησιμοποιείται όταν ανακτώνται διάφορα hashes, που μαζεύονται από το εργαλείο Responder. Επιπλέον, είναι

απαραίτητη προϋπόθεση η χρήση εξωτερικών μέσων αποθήκευσης μεγάλης χωρητικότητας που θα περιέχον λίστες με κωδικούς. Στόχος, η κατά το δυνατό γρηγορότερη ανάκτηση των κωδικών. [07]

Nessus, Nexpose και Retina

Είναι σημαντικό να σημειωθεί ότι ένα εργαλείο δοκιμής διείσδυσης στο διαδίκτυο δεν είναι το ίδιο με ένα εργαλείο για σάρωση ευπάθειας. Τα εργαλεία που βασίζονται στο διαδίκτυο έχουν σίγουρα δυνατότητες σάρωσης. Εστιάζονται όμως, στο επίπεδο εφαρμογής (application layer) μιας ιστοσελίδας, σε σχέση με το επίπεδο υπηρεσίας ή πρωτοκόλλου (service or protocol level). Τα εργαλεία Nessus, Nexpose και Retina, χρησιμοποιούνται κυρίως ως σαρωτές ευπάθειας με δυνατότητες σάρωσης εφαρμογών ιστού. Ακόμα, μερικά άλλα εργαλεία, άξια προς αναφορά, τα οποία χρησιμοποιούνται για να επιδεικνύουν σημαντικά ζητήματα, είναι τα Stored Cross-site Scripting (XSS), τα SQL Injection, τα Authentication bypass, τα Directory traversal abuse και τα Unrestricted file upload. [27]

Επιπρόσθετα, όσοι είναι διαχειριστές συστημάτων και αναπτύσσουν ή συντηρούν εσωτερικές εφαρμογές ιστού, πρέπει να εξετάζουν συστηματικά, εάν ο κώδικας περιλαμβάνει άγνωστες πηγές, ελαττώματα ασφαλείας ή δυνητικά κακόβουλες λειτουργίες. Ένα πολύ χρήσιμο εργαλείο είναι το OWASP, το οποίο εστιάζεται στην ασφαλή ανάπτυξη εφαρμογών την οποία οφείλουν να υιοθετούν ως κόρη οφθαλμού οι διαχειριστές συστημάτων. Πέραν του OWASP, για την εξέταση εφαρμογών, μπορούν αν εφαρμόζονται οι μεθοδολογίες SAST και DAST. Η πρώτη, η στατική εφαρμογή δοκιμής ασφάλειας, επιτρέπει σε αυτούς που εκτελούν τις δοκιμές διείσδυσης να διαβάζουν και αναλύουν το πηγαίο κώδικα, ψάχνοντας για λογικές αδυναμίες τις οποίες ένας εισβολέας θα μπορούσε να εκμεταλλευτεί. Στην δυναμική εφαρμογή δοκιμής ασφάλειας, αντί να τρέχουν την εφαρμογή και να αναζητούν ευπάθειες, εκτελούν δοκιμές συμπεριφοράς. Αναλύουν, δηλαδή τις εφαρμογές κατά την διάρκεια που αυτές βρίσκονται σε λειτουργία. Επιπλέον, μια αρκετά καλή τακτική είναι η σάρωση των εφαρμογών ιστού τουλάχιστον ανά τρίμηνο. Υπάρχει πληθώρα επιλογών από εργαλεία, κάποια από τα οποία είναι ανοικτού κώδικα, όπως το Burp Suite Pro, το Proxy Zed Attack OWASP, το Acunetix ή το Trustwave. Οι λειτουργίες σάρωσης αυτών των εργαλείων, μπορούν να ανιχνεύσουν και να προσομοιώνουν επιθέσεις κατά των διαφόρων εφαρμογών στο διαδίκτυο. [07]

Arpspoof

Το Arpspoof, είναι ένα εργαλείο που επιτρέπει την εισαγωγή του ατόμου που κάνει την δοκιμή, μεταξύ ενός στόχου (target) και της πύλης (gateway) του ή απευθείας μεταξύ δύο στόχων. Κατά την διάρκεια μιας δοκιμής διείσδυσης, μπορεί να ανακατευθυνθεί η κίνηση από έναν τυχαίο στόχο, όπως έναν σταθμό εργασίας ενός υπαλλήλου και να παρακολουθηθούν οι κινήσεις του. Ίσως, η πρώτη θεωρητική επίθεση που παρουσιάστηκε σε όσους ασχολούνται με την ασφάλεια του κυβερνοχώρου, να είναι η επίθεση MITM. Η επίθεση αυτή, εξακολουθεί ακόμα και σήμερα να είναι αποτελεσματική, στα σύγχρονα δίκτυα. Είναι γεγονός, ότι σχεδόν όλος ο κόσμος εξακολουθεί να στηρίζεται στο IPv4 για εσωτερική δικτύωση και πιθανόν για μεγάλο χρονικό διάστημα ακόμα. Αυτό, σε συνδυασμό με τον τρόπο με τον οποίο σχεδιάστηκε το πρωτόκολλο επίλυσης διευθύνσεων ARP, μια παραδοσιακή επίθεση MITM εξακολουθεί να είναι αρκετά πιθανή. [07]

Κεφάλαιο 4

Εφαρμογή και Κόστος Υλοποίησης

Τα αίτια που προκαλούν τις ευπάθειες σε συστήματα, οφείλονται σε διάφορα σφάλματα αλλά και σε ανθρώπινα λάθη. Τα αίτια, σε συνδυασμό με την εξέλιξη των εγκλημάτων διογκώνουν καθημερινά το πρόβλημα. Ένα από τα πιο σημαντικά εργαλεία που μπορούν να χρησιμοποιήσουν οι εταιρείες για να υπερασπιστούν τον εαυτό τους, είναι τα εργαλεία των δοκιμών διείσδυσης. Οι κύριοι λόγοι, για τους οποίους πρέπει να επενδύσει μια εταιρεία σε δοκιμές διείσδυσης είναι, η εξασφάλιση της καλύτερης ασφάλειας στον τομέα της άμυνας και η μείωση του επιπέδου του κινδύνου. Οι δοκιμές απαραίτητα, πρέπει να εκτελούνται από άτομα που είναι πιστοποιημένα να εκτελούν διεισδύσεις και να έχουν εμπειρία σε όλες τις μορφές δοκιμών. Για την εκτέλεση των δοκιμών απαιτούνται διαφορετικά είδη εργαλείων, γνώσεων και εμπειρογνωμοσύνης και όλα μαζί θα καθορίσουν το κόστος των δοκιμών. Πέραν από τα εργαλεία, το κόστος καθορίζεται από την πολυπλοκότητα του συστήματος και το μέγεθος του. [16]

4.1 Αίτια ευπαθειών

Τα αίτια, που προκαλούν τις ευπάθειες, είναι αρκετά περίπλοκα και πολυδιάστατα. Οφείλονται σε σφάλματα ανάπτυξης, σε θέματα ρυθμίσεων, σε ανθρώπινα λάθη, στην συνδεσιμότητα και την πολυπλοκότητα των συστημάτων, σε κωδικούς πρόσβασης, στην έλλειψη επικοινωνίας και στη κοινωνικής μηχανική. Συνοπτική ανάλυση των αιτιών ακολουθεί πιο κάτω. [02]

Σφάλματα Ανάπτυξης, Ρυθμίσεων και Διαμόρφωσης

Αρκετές ευπάθειες σε πληροφορικά συστήματα, οφείλονται σε σφάλματα σχεδιασμού και ανάπτυξης. Παρουσιάζονται δηλαδή, ελαττώματα στο σχεδιασμό του υλικού ή και του λογισμικού. Τα σφάλματα αυτά, σε αρκετές περιπτώσεις θέτουν σε κίνδυνο, τα κρίσιμα δεδομένα του οργανισμού. Η κακή διαμόρφωση ενός συστήματος, είναι ακόμα ένα αίτιο. Εάν το σύστημα δεν είναι σωστά ρυθμισμένο, τότε μπορεί να παρουσιάζει κενά τα οποία ενδέχεται να εκμεταλλεύονται οι εισβολείς, με σκοπό να εξασφαλίζουν πρόσβαση σε αυτά για να υποκλέψουν σημαντικές πληροφορίες. [02]

Ανθρώπινα λάθη και κατάρτιση

Μια ακόμα μεγάλη κατηγορία αιτιών ευπάθειας, ίσως και η συχνότερη σε εμφάνιση, είναι τα ανθρώπινα σφάλματα. Ο άνθρωπος, εκ φύσεως υποπίπτει σε σφάλματα. Τα ανθρώπινα σφάλματα μπορεί να είναι, η ακατάλληλη διάθεση των εγγράφων, η έκθεση των εγγράφων χωρίς επίβλεψη, τα λάθη στην κωδικοποίησης, οι αθέμιτες απειλές εκ των έσω, η χρήση κωδικών πρόσβασης μέσω δικτύου ηλεκτρονικού "ψαρέματος" και άλλα. Όλα τα σφάλματα, μπορούν να οδηγήσουν σε παραβιάσεις της ασφάλειας ή κενά ασφάλειας σε συστήματα. Επιπρόσθετα, παρόλο που δεν λαμβάνεται αρκετά σοβαρά υπόψη από τους οργανισμούς, είναι η έλλειψη της κατάρτισης του προσωπικού η οποία οφείλεται κυρίως σε οικονομικούς λόγους, καθώς θεωρείται πρόσθετο έξοδο. Το φαινόμενο όμως της έλλειψης κατάρτισης του προσωπικού επηρεάζει αρνητικά τους ορθούς χειρισμούς τους, με αποτέλεσμα να γίνονται συχνά σφάλματα. [03]

Συνδεσιμότητα και πολυπλοκότητα

Ευπάθειες, υπάρχουν ακόμα και στον τομέα της συνδεσιμότητας. Στις περιπτώσεις δηλαδή, που το σύστημα στόχος είναι συνδεδεμένο σε ένα μη ασφαλές δίκτυο το οποίο χρησιμοποιεί ανοιχτές

συνδέσεις. Το γεγονός αυτό δημιουργεί σίγουρα ευκαιρία πρόσβασης σε εισβολείς, να επιχειρούν επιθέσεις. Ανάλογο κενό ασφάλειας και συνάμα πρόβλημα ευπάθειας, όμοιας σημαντικότητας με την συνδεσιμότητα, υπάρχει όταν παρουσιάζονται θέματα σχετικά με την πολυπλοκότητα των συστημάτων. Η πολυπλοκότητα των συστημάτων, αυξάνει τα επίπεδα ευπάθειας, αφού όσο περισσότερα σύνθετα χαρακτηριστικά διαθέτει ένα σύστημα, τόσο περισσότερες πιθανότητες θα έχει να δεχθεί επιθέσεις. [31]

Κωδικοί πρόσβασης

Μια πολύ σημαντική ενότητα, στη οποία παρουσιάζονται ευπάθειες, είναι οι κωδικοί πρόσβασης οι οποίοι χρησιμοποιούνται για την αποτροπή μη εξουσιοδοτημένης πρόσβασης. Θα πρέπει όμως να είναι αρκετά μεγάλοι σε μέγεθος και περίπλοκοι, ώστε κανείς να μην μπορεί κάποιος να μαντεύει τον κωδικό πρόσβασής. Έτσι η διατήρηση απλών κωδικών, που μπορεί κάποιος εύκολα να μαντέψει, πρέπει ρητά να αποφεύγεται. Το ίδιο πρέπει να γίνεται όμως και με όσους μοιράζονται τους κωδικούς τους με άλλους, καθώς αυτό και πάλι απαγορεύεται. Παρά τις οδηγίες όμως, δεν είναι λίγοι αυτοί που όχι μόνο δεν αλλάζουν τους κωδικούς τους περιοδικά, αλλά τους αποκαλύπτουν και σε άλλους. Άλλοτε, τους αναγράφουν σε χαρτί για να μην χρειάζεται να τους θυμούνται και τους αποθηκεύουν σε σημεία που δεν έχουν μόνο αυτοί, εύκολη πρόσβαση. [37]

Έλλειψη επικοινωνίας

Ακόμα ένα αίτιο για πρόκληση ευπαθειών, είναι ο τομέας της επικοινωνίας. Κανάλια, όπως το ασύρματο δίκτυο, το διαδίκτυο ή ακόμα και η χρήση των έξυπνων τηλέφωνων ή άλλων συσκευών, όπως είναι το διαδίκτυο των πραγμάτων (IoT), ανοίγουν την πόρτα σε βέβαιες παραβιάσεις της ασφάλειας των συστημάτων. [03]

Κοινωνική μηχανική

Η κοινωνική μηχανική, θεωρείται το πιο εξειδικευμένο αίτιο πρόκλησης ευπάθειας, από όλα όσα έχουν αναφερθεί. Με την μέθοδο της κοινωνικής μηχανικής γίνεται συλλογή ηλεκτρονικών πληροφοριών, η οποίες αφορούν χρήστες ή διαχειριστές συστημάτων. Το ανησυχητικό και το πιο επικίνδυνο, είναι όταν αυτές δεν γίνονται τυχαία αλλά μετά από στοχευμένες επιθέσεις. Οι στοχευμένες επιθέσεις καταφέρουν να εξασφαλίσουν σχετικές πληροφορίες για τα συστήματα και γενικότερα προκαλούν τον τομέα της ασφάλειας, δημιουργώντας του κενά ασφάλειας. Στόχος

των επιθέσεων αυτού του είδους είναι να δημιουργούν τέτοια προβλήματα στην ασφάλεια των συστημάτων που θα κάνουν ακόμα πιο δαπανηρή τη διαχείριση της. [23]

4.2 Εφαρμογή και Έλεγχος δοκιμών

Η ανάγκη να εφαρμόζονται οι δοκιμές διείσδυσης, παρουσιάζεται όταν τα οικονομικά ή κρίσιμα δεδομένα, πρέπει να διασφαλίζονται κατά τη μεταφορά τους μεταξύ διαφορετικών συστημάτων ή μέσω του δικτύου. Ακόμα, απαιτείται η εφαρμογή τους όταν το ζητήσουν οι πελάτες ως μέρος του κύκλου προώθησης ενός λογισμικού, για να διασφαλιστούν τα δεδομένα των χρηστών ή για να εντοπιστούν ευπάθειες ασφαλείας σε μια εφαρμογή. Ως επί το πλείστο όμως, εκτελούνται δοκιμές, για να ανακαλυφθούν τυχόν κενά σε συστήματα ή για αξιολόγηση των επιπτώσεων επιτυχημένων επιθέσεων ή γιατί πρέπει να ικανοποιηθεί η πολιτική συμμόρφωσης της ασφάλειας των πληροφοριών της εταιρείας και να εφαρμόσει αποτελεσματική στρατηγική ασφαλείας. Κατά την διάρκεια των δοκιμών διείσδυσης πρέπει να ελέγχονται, αρχικά το λογισμικό, στο οποίο περιλαμβάνεται το λειτουργικό σύστημα, οι διάφορες υπηρεσίες που τρέχουν σε αυτό καθώς και οι εφαρμογές του. [08]

4.3 Επένδυση σε δοκιμές διείσδυσης

Καθώς οι εγκληματίες στον κυβερνοχώρο, γίνονται πιο εξειδικευμένοι και εξελιγμένοι, το βάρος μεταφέρεται στους ιδιοκτήτες των επιχειρήσεων για να διασφαλίσουν ότι τα συστήματα τους στον κυβερνοχώρο μπορούν να προστατεύονται από απειλές. Ένα από τα πιο σημαντικά εργαλεία που μπορούν να χρησιμοποιήσουν οι εταιρείες για να υπερασπιστούν τον εαυτό τους, είναι αυτό των δοκιμών διείσδυσης. Ένας επαγγελματίας που εκτελεί δοκιμές διείσδυσης, χρησιμοποιεί τις ίδιες τεχνικές με έναν εγκληματία, για να αποκτήσει παράνομα πρόσβαση στα διάφορα συστήματα του οργανισμού, με σκοπό να αναδείξει τις ευπάθειες, εάν υπάρχουν. Χρησιμοποιεί, ακόμα τις ίδιες μεθοδολογίες που μπορεί να χρησιμοποιήσει ένας εγκληματίας, όπως είναι το σπάσιμο κωδικών πρόσβασης, η τοποθέτηση κακόβουλων λογισμικών ή ακόμα η χρήση της κοινωνικής μηχανικής. [21]

Γενικότερα, οι δοκιμές πρέπει να εκτελούνται από άτομα που είναι πιστοποιημένα να εκτελούν διεισδύσεις και να έχουν εμπειρία σε όλες τις μορφές δοκιμών. Τα άτομα αυτά, θα προσπαθήσουν να εισέλθουν στα διάφορα συστήματα συγκεντρώνοντας πληροφορίες, προβάλλοντας τα κενά

ασφάλειας και τις τρωτότητες που υπάρχουν. Ακολούθως θα προτείνουν, μέτρα που πρέπει να ληφθούν έτσι ώστε τα συστήματα να μπορούν να προστατευθούν από ανάλογα είδη επιθέσεων όταν θα έχουν να αντιμετωπίσουν επιθέσεις από πραγματικούς εισβολείς. Ακολουθούν έξι λόγοι για τους οποίους μια εταιρεία πρέπει να επενδύει, σε δοκιμές διείσδυσης. [39]

Εκθέτει αδυναμίες

Αναμφισβήτητα, η πολυτιμότερη πτυχή των δοκιμών διείσδυσης, είναι να δοκιμάζει την ασφάλεια του οργανισμού, μέσα από τις ίδιες συνθήκες, όπως θα γινόταν με μια πραγματική απόπειρα επίθεσης. Με αυτό τον τρόπο, εκθέτει τις αδυναμίες του συστήματος κάτω από την ελεγχόμενη έκθεση της ασφάλειας του συστήματος στο κυβερνοχώρο. Είναι σίγουρα, καλύτερο από το να γνωστοποιείται στην εταιρεία, μέσω μιας δαπανηρής πραγματικής επίθεσης. Τυχόν λάθη και παραλείψεις, μπορούν να διορθώνονται αντιμετωπίζοντας έτσι τις όποιες κακόβουλες προσπάθειες παραβίασης επιχειρούνται. Είναι πάρα πολύ σημαντικό λοιπόν, οι αναφορές που εξάγονται από τις δοκιμές διείσδυσης να παρέχουν όλες τις λεπτομέρειες, για το πώς και ποια μέτρα πρέπει να παρθούν για να διορθώνονται τα τρωτά σημεία του συστήματος. Δεν υπάρχει καμία αμφιβολία, ότι οι επιχειρήσεις μπορούν να μάθουν από τα λάθη τους, αλλά σίγουρα καλύτερα είναι να μαθαίνουμε από μια προσομοιωμένη επίθεση, παρά από μια πραγματική. [16]

Περιοχές ασφαλείας

Οι ανησυχητικές στατιστικές, δείχνουν ότι πάνω από το 43% των μικρών επιχειρήσεων έπεσαν θύματα κυβερνοεπιθέσεων. Από αυτές που δέχθηκαν την επίθεση, το 60% τερματίζουν τις δραστηριότητες τους μέσα σε διάρκεια έξι μηνών. [16] Είναι ξεκάθαρο λοιπόν, ότι δεν είναι πλέον αρκετό να λαμβάνονται επιδερμικά μέτρα στο τομέα της ασφάλειας, ελπίζοντας ότι με τον τρόπο αυτό ο οργανισμός δεν θα αποτελεί στόχο των κυβερνοεγκλημάτιών. Πρέπει επιτέλους, να ξεφύγουν όλοι από τοποθετήσεις του τύπου, «μια επιχείρηση είναι ασφαλής εάν εγκατασταθούν λογισμικά προστασίας από κακόβουλα λογισμικά και ισχυροί τοίχοι προστασίας». Η επένδυση στην αναβάθμιση της ασφάλειας του κυβερνοχώρου και της άμυνας, επιβάλλεται να είναι άμεση. Σίγουρα, πρέπει να γίνεται σε συνδυασμό με τα αποτελέσματα μιας δοκιμής διείσδυσης, η οποία θα αποκαλύψει τις αδυναμίες του τομέα άμυνας ενός συστήματος. Υπάρχουν βέβαια περιπτώσεις, που η ασφάλεια του συστήματος είναι επαρκής για να υπερασπιστεί τις απειλές και αυτό περιλαμβάνεται στα αποτελέσματα το δοκιμών που διεξάγονται. Άλλοτε, τα αποτελέσματα των δοκιμών αναφέρουν κενά ασφάλειας που προέρχονται κυρίως από το προσωπικό, το οποίο για

παράδειγμα ανοίγει μηνύματα ηλεκτρονικού ψαρέματος (phishing) ή χρησιμοποιεί πολύ απλούς κωδικούς πρόσβασης. Όταν οι οργανισμοί έχουν να αντιμετωπίσουν τέτοιες περιπτώσεις, δεν χρειάζονται να γίνονται επενδύσεις σε συστήματα ασφαλείας αλλά πρέπει να γίνονται ενέργειες για ενίσχυση της κατάρτισης του προσωπικού. Το προσωπικό, πρέπει να είναι σε θέση να κατανοήσει το πρόβλημα, για να μπορεί να αντιμετωπίσει τους διαφόρους κινδύνους και τις μεθοδολογίες παραβίασης συστημάτων. [39]

Προοπτική ασφάλειας

Είναι πολύ συχνό φαινόμενο, οι εταιρείες που διαχειρίζονται από μόνες τους εσωτερικά, την ασφάλεια των πληροφοριακών τους συστημάτων, να μην δέχονται σχεδόν ποτέ μια δεύτερη γνώμη. Πολλοί ιδιοκτήτες επιχειρήσεων ή διευθυντές οργανισμών, εμπιστεύονται επαγγελματίες του τομέα της τεχνολογίας και της πληροφορικής. Σε αυτούς αναθέτουν την εφαρμογή ενός ισχυρού συστήματος, το οποίο δεν πρέπει να παρουσιάζει σχεδόν καθόλου αδυναμίες. Το πρόβλημα όμως, της μη απόκτησης δεύτερης γνώμης εμπειρογνωμοσύνης, είναι η πιθανότητα μη αντίληψης των «τυφλών σημείων». Τα τυφλά σημεία, αποτελούν τα κενά ασφάλειας, τα οποία μπορεί να υπάρχουν αλλά να μην φαίνονται. Για το λόγο αυτό, αλλά και για να παρουσιαστεί πιο σφαιρικά η πραγματική εικόνα του συστήματος, είναι σημαντικό να γίνονται συστηματικά δοκιμές διείσδυσης. Είναι φυσικό να υπάρχει ο υπεύθυνος για την άμυνα κυβερνοεπιθέσεων, αλλά και αυτός μπορεί να κάνει λάθη, όπως οποιοσδήποτε άλλος. [09]

Εξοικονόμηση χρημάτων

Αρχικά ακούγεται αντιφατικό, καθώς είναι πιο εύκολο να κατανοήσει κάποιος ότι, κέρδος αποφέρει οτιδήποτε μπορεί να θεωρηθεί επένδυση. Να δαπανάς χρήματα για ένα έξοδο, όπως είναι η αγορά υπηρεσιών και αυτό να σου αποφέρει κέρδος, μάλλον θεωρείται παράλογο. Αυτό ακριβώς συμβαίνει, εάν η δαπάνη γίνεται για την χρήση υπηρεσιών δοκιμών διείσδυσης. Οι δοκιμές διείσδυσης, έχουν την δυνατότητα να προβάλλουν τις περιοχές με τις μεγαλύτερες αδυναμίες, να ενημερώνουν και να κατευθύνουν της εταιρείες ως προς τα πού πρέπει να ξοδεύουν τον προϋπολογισμό τους για τα θέματα της κυβερνοασφάλειας. Έτσι δεν θα είναι πλέον απαραίτητο να γίνονται άσκοπες δαπάνες χρημάτων, σε ένα ευρύτερο φάσμα πτυχών. Η μακροπρόθεσμη εξοικονόμηση χρήματων, είναι ακόμα ένα πλεονέκτημα που ενάγεται από την χρήση των δοκιμών αυτών. Μέσω των δοκιμών ο οργανισμός, μπορεί να αντιμετωπίζει, απειλές πρόστιμων από τα διοικητικά όργανα, σε περιπτώσεις αποτυχίας για προστασία των δεδομένων

των πελατών. Είναι σχεδόν βέβαιο, ότι με την χρήση των δοκιμών διείσδυσης και την διόρθωση πιθανών προβλημάτων του συστήματος, προστατεύεται η απώλεια εμπιστοσύνης των πελάτων, που σε άλλη περίπτωση θα μπορούσε να συμβεί μετά από μια παραβίαση. [31]

Αντιμετώπιση επίθεσης

Αν έχουν γίνει επενδύσεις σε συστήματα που προσφέρουν ισχυρή ασφάλεια στο τομέα των κυβερνοεπιθέσεων, τότε ο οργανισμός μπορεί σχεδόν με βεβαιότητα να μην ανησυχεί για παραβιάσεις που προέρχονται από κυβερνοεπιθέσεις. Ο εφησυχασμός όμως και η υπερβολική αυτοπεποίθηση, ότι υπάρχει και λειτουργεί ένα ισχυρό μηχάνημα άμυνας, τις περισσότερες φορές οδηγεί σε εσφαλμένα συμπεράσματα. Εάν μια εταιρεία δεν θέλει να ξοδέψει χρήματα σε δοκιμές διείσδυσης, πως θα ξέρει αν η άμυνα που εγκατέστησε μπορεί να αντέξει σε μια κυβερνοεπίθεση. Στην πραγματικότητα, είναι εξαιρετικά σπάνιο ένα σύστημα να είναι αλάνθαστο, γνωρίζοντας ότι εξειδικευμένοι εγκληματίες, αναζητούν συνεχώς τρόπους να σπάσουν τις άμυνες τέτοιων συστημάτων. Επιπρόσθετα, δεν είναι λίγοι αυτοί που νομίζουν ότι τα συστήματα τους μπορούν να αντιμετωπίσουν οποιαδήποτε απειλή, παραβλέποντας σοβαρές ευπάθειες και προβλήματα. Ο έλεγχος διείσδυσης από την άλλη, μέσω της προσομοίωσης, γνωρίζει ακριβώς τι θα συμβεί σε μια πραγματική, εξειδικευμένη επίθεση στο σύστημα. [16]

Συμμόρφωση με GDPR

Ο Κανονισμός Γενικής Προστασίας Δεδομένων (GDPR) έχει τεθεί σε ισχύ τον Μάιο του 2018. Πρόκειται για κανονισμό, που επηρεάζει κάθε οργανισμό που δραστηριοποιείται εντός της Ευρωπαϊκής Ένωσης ή επηρεάζει τις δραστηριότητες των πολιτών της Ευρωπαϊκής Ένωσης. Μία από τις σημαντικότερες πτυχές του GDPR, είναι το γεγονός ότι επηρεάζει τις επιχειρήσεις που δέχονται παραβιάσεις και που έχουν ως σκοπό τους την κλοπή των προσωπικών δεδομένων από τα αρχεία που διατηρούν για τους πελάτες τους, ως αποτέλεσμα της φτωχής ασφάλειας που διαθέτουν στα συστήματα τους. Αντιμετωπίζουν δε, πολύ μεγάλες κυρώσεις και πρόστιμα που σε αρκετές περιπτώσεις οδηγούν στην διακοπή των δραστηριοτήτων τους. Η διενέργεια δοκιμών διείσδυσης, δίνει την δυνατότητα να εκθέτει τις αδυναμίες των συστημάτων κατά τρόπο ώστε να δώσει ευκαιρίες διόρθωσης, εναρμόνισης και συμμόρφωσης του οργανισμού, με τον κανονισμό GDPR καθώς και με άλλους κανονισμούς προστασίας δεδομένων ή απορρήτου. [09]

4.4 Δοκιμές σε μικρές επιχειρήσεις

Τα τελευταία δύο χρόνια, αποτέλεσαν την κλήση αφύπνισης για τους αυξανόμενους κινδύνους του κυβερνοεγκλήματος και των διαφόρων ηλεκτρονικών μορφών παραβίασης στον κυβερνοχώρο. Οι κυβερνοεγκληματίες εξελίσσονται τεχνολογικά αφού έχουν στην κατοχή τους προηγμένα δίκτυα που μπορούν να δημιουργούν με ευκολία κακόβουλα προγράμματα και εργαλεία. Αυτό, τους επιτρέπει δυστυχώς να εξαπολύουν επιθέσεις στον κυβερνοχώρο προς όλες τις κατευθύνεις. Καθώς η τεχνολογία συνεχίζει να εξελίσσεται και να εξαπλώνεται σε όλα τα μήκη και πλάτη του πλανήτη μας, οι εγκληματίες στον κυβερνοχώρο γίνονται ακόμη πιο αδίστακτοι. Το ανησυχητικό βέβαια, είναι ότι επιθέσεις στρέφονται εξίσου και σε μικρότερες εταιρείες, οι οποίες είναι πολύ πιο ευάλωτες από τις μεγαλύτερες. Για να αντισταθμιστεί και να αντιμετωπιστεί η απειλή μιας επικείμενης επίθεσης, είναι πολύ σημαντικό οι μικρές επιχειρήσεις να λαμβάνουν προληπτικά μέτρα για να καταστήσουν την υποδομή τους ασφαλή. Για το λόγω αυτό, η υιοθέτηση των βέλτιστων πρακτικών για την ασφάλεια στον κυβερνοχώρο, συμβάλει σε μεγάλο βαθμό. Οι βέλτιστες πρακτικές, μπορούν να δουλεύουν αποτρεπτικά αντιμετωπίζοντας τους κινδύνους, της οικονομικής απώλειας, της ζημιάς λόγω της κακής φήμης και όλων των άλλων προβλημάτων που προκύπτουν από επιθέσεις στον κυβερνοχώρο. Πιο συγκεκριμένα, η τεχνική που πρέπει να εφαρμόζεται απαραίτητα από κάθε μικρή επιχείρηση, είναι η δοκιμή διείσδυσης. Μέσω των δοκιμών, μπορούν να εντοπίζονται στρατηγικά κενά και τρωτά σημεία ασφάλειας, που μπορεί να υπάρχουν στην υποδομή της επιχείρησης. Έτσι, δίνεται η ευκαιρία δημιουργίας διορθωτικών μέτρων και συστάσεων σε σχέση με το επίπεδο ασφάλειας του συστήματος. [28]

4.5 Επιλογή δοκιμών

Οι δοκιμές διείσδυσης, έχουν γίνει οι πιο κοινές δεσμεύσεις για τις σημερινές επιχειρήσεις που έχουν επίγνωση του τομέα της ασφάλειας. Υπάρχουν πολλοί λόγοι για τη διεξαγωγή δοκιμών διείσδυσης, συμπεριλαμβανομένης της καλύτερης ασφάλειας στον τομέα της άμυνας, της μείωσης του επιπέδου κινδύνου και της τήρησης αυστηρών απαιτήσεων συμμόρφωσης. Οι ακόλουθες βέλτιστες πρακτικές, μπορεί να φανούν χρήσιμες κατά την επιλογή, του ατόμου ή της ομάδας που θα εκτελέσει τις δοκιμές. [08]

Καθορισμός τύπου

Πριν την επιλογή θα πρέπει να καθοριστεί ο τύπος των τεχνικών δοκιμών που χρειάζεται να εκτελεστεί. Πρέπει δηλαδή, να υπάρξει μια ξεκάθαρη εικόνα, εάν οι δοκιμές διείσδυσης θα εκτελεστούν σε εφαρμογές, σε ένα συγκεκριμένο δίκτυο, για ενσύρματα δίκτυα ή ασύρματα δίκτυα ή γενικά για υποδομές δικτύων. Διαφορετικοί τύποι δοκιμών διείσδυσης, απαιτούν διαφορετικά είδη εργαλείων, γνώσεων και εμπειρογνωμοσύνης και όλα μαζί θα καθορίσουν το κόστος των δοκιμών. Αφού οριστεί το πεδίο εφαρμογής της δοκιμής, θα πρέπει να υποδειχθεί ένας εκ των τριών τρόπων, με τον οποίο θα εκτελεστούν οι δοκιμές. Ο πρώτος τρόπος εκτέλεσης δοκιμών διείσδυσης, αναφέρεται σε δοκιμές που πραγματοποιούνται με γνώση της εσωτερικής δομής, το γενικότερο σχεδιασμό και το πως έχει υλοποιηθεί το υπό εξέταση περιβάλλον. Ο δεύτερος τρόπος, αναφέρεται σε δοκιμές που πραγματοποιούνται με απλές προσβάσεις ή με περιορισμένες γνώσεις του περιβάλλοντος που εξετάζεται. Έτσι, μπορεί να εκτιμηθεί το επίπεδο ασφάλειας, όπως το βλέπει ο εξουσιοδοτημένος χρήστης, σε συνδυασμό με τις γενικότερες πληροφορίες του υπό εξέταση περιβάλλοντος. Ο τελευταίος τρόπος εκτέλεσης δοκιμών, αφορά τις δοκιμές που εκτελούνται χωρίς να είναι γνωστό το περιβάλλον που εξετάζεται. Ο στόχος, είναι η εκτίμηση του επιπέδου ασφάλειας του συστήματος, όπως την βλέπει κάποιος τρίτος που συνδέεται με το εσωτερικό δίκτυο ή το διαδίκτυο, χωρίς προηγούμενη γνώση του περιβάλλοντος. [06]

Αξιολόγηση δεξιοτήτων

Εκτός από την αξιολόγηση της εταιρείας που εκτελεί δοκιμές διείσδυσης στο σύνολό της, θα πρέπει επίσης να εξετάζονται προσεκτικά τα άτομα που θα διεξάγουν τις δοκιμές. Είναι πολύ σημαντικό τα άτομα αυτά, να είναι καλά καταρτισμένα και να κατέχουν δεξιότητες, γνώσεις και εμπειρίες από άλλες δοκιμές διείσδυσης. Από άποψη εμπειρογνωμοσύνης, η ομάδα που θα αναλάβει, θα πρέπει να είναι σε θέση να αποδείξει τις τεχνικές γνώσεις της. Για παράδειγμα, ένα πτυχίο πανεπιστημίου στην ασφάλεια πληροφοριών σε συνδυασμό με διάφορες πιστοποιήσεις στο τομέα του «Ethical Hacking» ή σε μαθήματα συνεχιζόμενης εκπαίδευσης, βεβαιώνουν ότι τα άτομα έχουν λάβει τις απαραίτητες θεωρητικές και πρακτικές δεξιότητες για να ολοκληρώσουν τις δοκιμές. Ιδανικότερη περίπτωση αποτελεί το γεγονός, ότι τα άτομα που θα αναλάβουν να εκτελέσουν τις δοκιμές θα έχουν εμπειρία σε διάφορους τομείς, για διαφορετικούς τύπους εταιρειών και σε διάφορα είδη προγραμμάτων δοκιμών διείσδυσης. Είναι σύνηθες επίσης, τα άτομα αυτά να συμπεριλαμβάνουν μια περίληψη των πιο πρόσφατων εργασιών που εκτέλεσαν στο τέλος του βιογραφικού τους. [09]

Παραχώρηση αναφορών

Πριν ξεκινήσουν οι δοκιμές, πρέπει να ζητούνται παρόμοιες αναφορές δοκιμών διείσδυσης που πραγματοποιήθηκαν για οργανισμούς ανάλογου μεγέθους, σε παρόμοιο πεδίο εφαρμογής ή που ανήκουν στον ίδιο κλάδο. Έτσι επιβεβαιώνεται και η καταλληλόλητα των ατόμων για το συγκεκριμένο επιχειρηματικό πλαίσιο.[12]

Διασφάλιση των δεδομένων

Τα άτομα που εκτελούν τις δοκιμές διείσδυσης, σίγουρα γνωρίζουν πώς να αποκτήσουν πρόσβαση στα εμπιστευτικά δεδομένα. Παράλληλα όμως, πρέπει να είναι σε θέση να υποδείξουν, τους τρόπους με τους οποίους θα διαχειριστούν τα δεδομένα αυτά με ασφάλεια, πριν, κατά τη διάρκεια των δοκιμών και μετά την ολοκλήρωση των δοκιμών διείσδυσης. Η λήψη διευκρινίσεων, σχετικά με την ασφάλεια των δεδομένων, μπορεί να είναι αποφασιστικός παράγοντας κατά την επιλογή μιας εταιρείας για να διεξάγει τις εν λόγω δοκιμές. [09]

Δείγμα αναφοράς

Το μοναδικό παραδοτέο σε μια δοκιμή διείσδυσης, είναι μια λεπτομερής έκθεση, που περιλαμβάνει όλα τα ευρήματα των δοκιμών, καθώς και τα απαραίτητα μέτρα και συστάσεις σε σχέση με το επίπεδο ασφάλειας του υπό εξέταση συστήματος. Η έκθεση, αποτελεί μια συνοπτική παρουσίαση που περιγράφει τη γενική στάση ασφαλείας του συστήματος και υποδεικνύει στοιχεία που απαιτούν άμεση προσοχή.[32] Πρέπει απαραίτητα, να περιέχει τα σωστά στοιχεία για όποιον την διαβάσει.

Η τεχνική ομάδα του Τμήματος πληροφορικής για παράδειγμα, ενδιαφέρεται ιδιαίτερα για τον λεπτομερή κατάλογο ευπαθειών και εκμεταλλεύσεων, νοουμένου ότι θα τους παραχωρούνται, βήμα προς βήμα οι προτάσεις για αποκατάσταση. Ο υπεύθυνος πληροφορικής ή τα ανώτερα στελέχη ενός οργανισμού από την άλλη, εξετάζουν συνοπτικά τα κυριότερα σημεία της έκθεσης. Έτσι, κατανοούν καλύτερα την γενικότερη εικόνα της κυβερνοασφάλειας και την έκθεση τους στους διάφορους κινδύνους, με αποτέλεσμα να λαμβάνουν πιο εύκολα αποφάσεις. [09]

Μια καλή έκθεση δοκιμής διείσδυσης, η οποία θα διευκολύνει τη διαδικασία λήψης αποφάσεων, πρέπει να περιλαμβάνει, την τεχνική επισκόπηση, την λίστα των ευπαθειών, συστάσεις, παραρτήματα και σύνοψη τακτικής. [12]

Η τεχνική επισκόπηση, περιγράφει τις δραστηριότητες που εκτελούνται για τον προσδιορισμό των τρωτών σημείων και των αποτελεσμάτων των δραστηριοτήτων που διεξάγονται για την επίθεση σε συστήματα στόχων. Στα αποτελέσματα συμπεριλαμβάνονται και οι μεθοδολογίες που χρησιμοποιήθηκαν. [12] Στην έκθεση επίσης περιλαμβάνεται, μια λεπτομερής λίστα που παρουσιάζει κατά σειρά κρισιμότητας, τις ευπάθειες που ανακαλύφθηκαν και τον τρόπο με τον οποίο έγινε η εκμετάλλευση τους. [09] Επιπρόσθετα στα όσα προσδιορίζει η έκθεση, γίνονται ανάλογες και εκτενείς συστάσεις, με σκοπό τη βελτιστοποίηση του δείκτη ασφάλειας και προστασίας των περιουσιακών στοιχείων. Σε αυτές τις συστάσεις, λαμβάνεται υπόψη το κόστος υλοποίησης των βελτιώσεων που θα προκύψει, η λειτουργία, η συντήρηση, το χρονικό πλαίσιο των εργασιών και το προσωπικό που θα χρειαστεί να λάβει μέρος σε αυτές. [32] Όσον αφορά τα παραρτήματα της έκθεσης, σε αυτά γίνεται αναφορά στα εργαλεία που χρησιμοποιούνται. Τα εργαλεία καταγράφουν, τα αποτελέσματα, τα στιγμιότυπα οθόνης και άλλα δεδομένα, που βοηθούν στο να δώσουν ακριβέστερα στοιχεία ή διευκρινίσεις σχετικά με τις ευπάθειες που εντοπίζονται. [09] Σε κάθε έκθεση, ενδέχεται να παρουσιαστεί μια προαιρετική σύνοψη τακτικής, που περιγράφει τα πιθανά βήματα που θα ακολουθηθούν. Τα βήματα αυτά είτε θα δώσουν προσωρινές λύσεις ή ακόμα και πιο μακροπρόθεσμες. Τέτοιες λύσεις, δυνατό να χρειάζεται να ενσωματώνονται σε μεγαλύτερα έργα ή σε έργα που χρήζουν περαιτέρω διερεύνησης.[09]

Διαχείριση έργου

Είναι γεγονός ότι ένα μέρος της επιτυχίας του έργου, εξαρτάται από τις δυνατότητες διαχείρισης του έργου. Η ομάδα που θα αναλάβει να εκτελέσει τις δοκιμές διείσδυσης πρέπει να είναι σε θέση να δίνει πληροφόρηση για το είδος της διαδικασίας και την μεθοδολογία που θα ακολουθήσει. Έτσι, διασφαλίζεται ότι το έργο των δοκιμών εκτελείται ομαλά και σύμφωνα με το χρονοδιάγραμμα με βάση τις τεχνικές που έχουν καθοριστεί. Εκτός από το ερώτημα για τα βιογραφικά της ομάδας που θα εκτελέσει τις δοκιμές, πρέπει να εξακριβώνονται τα προσόντα και η εμπειρία του διαχειριστή του έργου. Πρέπει να διευκρινίζεται, κατά πόσον έχει ασχοληθεί με παρόμοια προγράμματα στο παρελθόν και εάν κατέχει τις κατάλληλες πιστοποιήσεις με απώτερο στόχο την εξασφάλιση ποιοτικών παραδοτέων προϊόντων στο τέλος του έργου. [12]

Μεθοδολογία

Πριν επιλεγεί η κατάλληλη ομάδα, για να εκτελέσει τις δοκιμές διείσδυσης, πρέπει να διαβεβαιώνεται ότι οι υποψήφιοι ακολουθούν αναγνωρισμένες στην ευρύτερη αγορά μεθοδολογίες και διαδικασίες. Απαραίτητα, πρέπει να καταγράφεται επακριβώς ο τρόπος

εκτέλεσης των δοκιμών, τα βήματα που θα ακολουθηθούν, τα εργαλεία θα χρησιμοποιηθούν και μεθοδολογία αξιολόγησης των αποτελεσμάτων. Συνήθως, τέτοιου είδους λεπτομέρειες, περιλαμβάνονται στη δήλωση εργασίας ή όταν περιλαμβάνεται στους όρους ανάθεσης, στις προτάσεις πώλησης. [39]

Επανεξέταση

Η επανεξέταση, είναι ένα κρίσιμο στοιχείο σε μια πρακτική συνεχούς δοκιμής διείσδυσης. Μέσω της επανεξέτασης, επικυρώνονται τα μέτρα αποκατάστασης που προτάθηκαν από την ομάδα που εκτελεί τις δοκιμές και βεβαιώνεται, ότι έχουν πράγματι τεθεί σε εφαρμογή από την τεχνική ομάδα πληροφορικής. Με αυτό τον τρόπο, βοήθα την ενίσχυση της άμυνας του τομέα της ασφάλειας, έναντι των κυβερνοεπιθέσεων. [09]

4.6 Κόστος δοκιμών

Καθορισμός τιμών

Όπως προαναφέρθηκε, μια δοκιμή διείσδυσης μπορεί να περιλαμβάνει πολλές επιλογές. Κάθε επαγγελματίας που παρέχει την υπηρεσία αυτή, προσαρμόζει τις τιμές των δοκιμών ανάλογα. Οι κύριοι παράγοντες καθορισμού του κόστους είναι η πολυπλοκότητα του συστήματος, το μέγεθος του δικτύου και ο αριθμός των συστημάτων, τα εργαλεία που θα χρησιμοποιηθούν κλπ. [21]

1. Η πολυπλοκότητα του συστήματός σε μια δοκιμή διείσδυσης, είναι ένα ουσιαστικό μέρος της διαδικασίας τόσο για τις μικρές νεοσύστατες επιχειρήσεις όσο και τις πιο μεγάλες εταιρείες. Τέτοιου είδους συστήματα, χρειάζονται αρκετές εργατοώρες να αναλυθούν αλλά και να σχεδιαστούν κατάλληλα καθώς επηρεάζουν ή επηρεάζονται από άλλα επιμέρους συστήματα ή διαδικασίες. Ακόμα, ένας παράγοντας που επηρεάζει το καθορισμό του κόστους είναι το μέγεθος της εφαρμογής ή του δικτύου αφού είναι συνυφασμένο με το ποσό της απαιτούμενης εργασίας. Οι μεγάλες εταιρείες παροχής δοκιμών διείσδυσης, έχουν την δυνατότητα να παρέχουν συμβουλευτικές εξετάσεις, οι οποίες συμβάλλουν στη διάκριση μεταξύ της απαιτούμενης εργασίας και της τιμολόγησης. Πέραν της έκτασης του δικτύου, το κόστος μιας δοκιμής διείσδυσης επηρεάζεται από τον αριθμό των συστημάτων που υπάρχουν σε αυτό, το επίπεδο πρόσβασης, τον ρόλο και το

τύπο της δοκιμής. Ανάλογα με τον τύπο της δοκιμής θα καθοριστούν και οι μέθοδοι που θα ακολουθηθούν.[35]

2. Τα εργαλεία που θα χρησιμοποιηθούν για τις δοκιμές, αποτελούν επίσης ουσιαστικό μέρος της διαδικασίας. Βάση τούτου, το κόστος των δοκιμών διείσδυσης μπορεί να αυξηθεί εάν απαιτούνται πρόσθετα ή ειδικά εργαλεία. Υπάρχουν περιπτώσεις, όπου ενώ κάποια από τα εργαλεία μπορεί να είναι δωρεάν, το άτομο που τα χρησιμοποιεί ίσως χρειαστεί ειδική πιστοποίηση. Ορισμένα από τα εργαλεία, μπορεί να είναι αρκετά ακριβά ή να χρειάζονται να πληρωθεί κάποια άδεια για την χρήση τους. Ακόμα, είναι βέβαιο ότι το κόστος επηρεάζεται από την συχνότητα εκτέλεσης των δοκιμών διείσδυσης, καθώς και από άλλες αξιολογήσεις που θεωρούνται απαραίτητες να εκτελούνται σε τακτική βάση. Για παράδειγμα, η διασφάλιση ότι υπάρχει συμμόρφωση με όλα τα πρότυπα και το γεγονός ότι δεν θα εμφανίζονται νέα ζητήματα. [12]

3. Ένας ακόμα παράγοντας αλλοίωσης του κόστους που πρέπει να λαμβάνεται υπόψη, είναι τα διάφορα εμπόδια κατά την προετοιμασία ενός καλού συστήματος δοκιμής. Σε αυτά, πρέπει να προστίθεται η επίγνωση, που πρέπει να έχει ένας ειδικός σε πιθανές επιθέσεις που ενδέχεται να δεχθεί ένα σύστημα. Βάση αυτής της επίγνωσης, καθορίζονται και οι διαφορετικές μεθοδολογίες που πιθανόν να χρησιμοποιηθούν ή οι συμβουλές που θα πρέπει να δοθούν σχετικά με τον τρόπο με τον οποίο θα εξαλειφθούν αυτές οι απειλές αποτελεσματικά. [35]

Πιστοποιήσεις δοκιμών

Παρόλο που οι πιστοποιήσεις δεν επηρεάζουν το κόστος δοκιμής διείσδυσης κατά μέσο όρο, εντούτοις διαδραματίζουν σημαντικό ρόλο στην εξεύρεση του σωστού επαγγελματία. Οι τιμές των πιστοποιήσεων είναι αρκετά ψηλές και κάθε εταιρεία παροχής δοκιμών διείσδυσης φροντίζει να εκπαιδεύει τους ειδικούς της μόνη της. Ακόμα, η κατάρτιση μπορεί να διαρκέσει από μερικές εβδομάδες έως και αρκετούς μήνες. Σε κάθε περίπτωση, ένας πιστοποιημένος ειδικός, οφείλει να χρησιμοποιεί τα κατάλληλα εργαλεία, εξασφαλίζοντας έτσι την υψηλότερη απόδοση σε εκάστη διαδικασία. [17]

Σύσταση ομάδας και όροι

Οι τιμές για την προσφορά υπηρεσιών για εκτέλεση δοκιμών διείσδυσης, ποικίλλουν. Οι ελεύθεροι επαγγελματίες, προσφέρουν τις εκδουλεύσεις τους, ανά ώρα σε πολύ λογικές τιμές σε αντίθεση, με τις υπηρεσίες που προσφέρουν ομάδες ατόμων μέλη μεγάλων εταιρειών οι οποίοι σίγουρα μισθώνονται με αρκετά πιο μεγάλα ποσά. Το ποσό φυσικά αυξάνεται ακόμη περισσότερο, εάν οι δοκιμές θα εκτελεστούν σε συστήματα, εταιρείας ή οργανισμού με μεγάλο αριθμό δικτυακών υποδομών. Εναλλακτικά, υπάρχουν περιπτώσεις όπου μπορεί να εκτιμηθεί και να τιμολογηθεί μια εργασία με ένα συμφωνημένο από την αρχή ποσό, σε μορφή συμβολαίου. Σε αυτή την περίπτωση η τιμή, θα εξαρτηθεί αναλόγως των παραμέτρων και των εργασιών που θα εκτελεστούν συμπεριλαμβανομένων και των αυτοματοποιημένων ελέγχων στις επιδόσεις του λογισμικού. Το κόστος, μιας τέτοιας δοκιμής διείσδυσης, μπορεί να κυμαίνεται από τέσσερις χιλιάδες ευρώ έως και εκατό χιλιάδες ευρώ. [12]

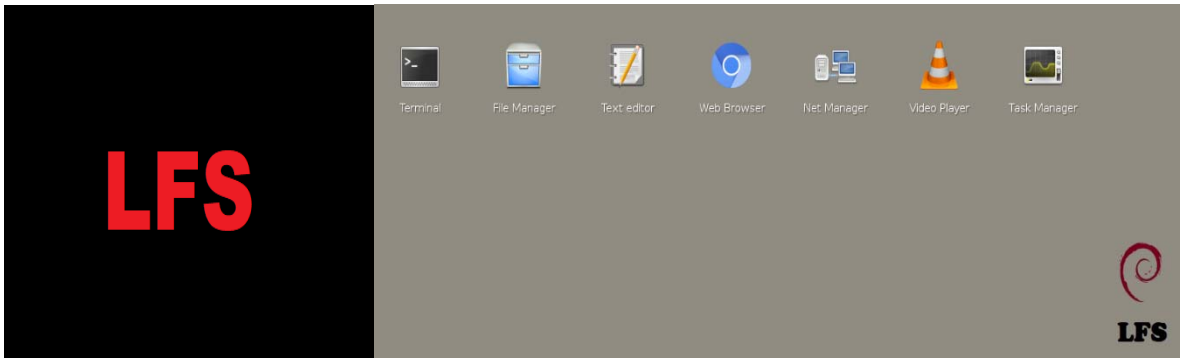
Κεφάλαιο 5
Δημιουργία Συστήματος LFS

Σχεδιασμός και ανάπτυξη των μεθοδολογιών ανοικτού κώδικα για δημιουργία μιας διανομής, με πυρήνα βασισμένο στην διανομή Debian Linux, όπου και οφείλει τις κύριες λειτουργίες του. Η διανομή έχει ως σκοπό την ενσωμάτωση εργαλείων δοκιμών διείσδυσης κατανοητά και εύκολα στην χρήση τους. Η διανομή που έχει ονομαστεί LFS, διαθέτει ένα απλό γραφικό περιβάλλον, γρήγορο διαχειριστή παραθύρων και δυνατότητα προσθαφαίρεσης εφαρμογών. Το LFS, δεν χρειάζεται εγκατάσταση και μπορεί να ξεκινήσει σε οποιοδήποτε Η.Υ. που υποστηρίζει συσκευές USB. Τόσο η αρχιτεκτονική όσο και η δομή του συστήματος, αναλύονται συνοπτικά. Η διανομή προσαρμόζεται ανάλογα με τους τύπους των ομάδων εκτέλεσης δοκιμών διείσδυσης όπως αυτές αναφέρονται στο κεφαλαίου 2. Όπως έχει επεξηγηθεί στην έρευνα, οι δοκιμές διείσδυσης χαρακτηρίζονται από την ποικιλία και την πολυπλοκότητα τόσο του τύπου όσο και του εύρους των εργαλείων που χρησιμοποιούν. Ως εκ τούτου, για σκοπούς της παρούσας έρευνας η διανομή LFS, έχει προσαρμοστεί κατά τρόπο ώστε, τα εργαλεία που εγκαταστάθηκαν σε αυτή, να μπορούν να χρησιμοποιηθούν από ομάδες White Hat και να εκτελούν δοκιμές διείσδυσης του τύπου αυτού ορίζοντας έτσι και το πεδίο εφαρμογής τους. Το πεδίο εφαρμογής της ομάδας, περιλαμβάνει δοκιμές που πραγματοποιούνται με γνώση της εσωτερικής δομής, το γενικότερο σχεδιασμό και το πως έχει υλοποιηθεί το υπό εξέταση περιβάλλον. Είναι μια προσομοίωση, επίθεσης εσωτερικής ασφάλειας. [03]

5.1 Πληροφορίες συστήματος

Λειτουργικό συστήματα

Όλα τα λειτουργικά συστήματα ανοικτού κώδικα, έχουν μοναδικές και ελαφρές αποκλίσεις, οι οποίες εμφανίζονται στα στάδια της αρχικής εγκατάστασης και ρύθμισης. Ωστόσο, οι περισσότερες πλατφόρμες που βασίζονται σε συστήματα Linux / Unix είναι σχετικά παρόμοιες. Κατά την εγκατάσταση ενός λειτουργικού συστήματος Linux, ο προγραμματισμός πριν από την εγκατάσταση είναι κρίσιμος. Έτσι, κατά την διάρκεια της φάσης του προγραμματισμού θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα ερωτήματα. Πόσο ρόλο παίζει η υπολογιστική δύναμη του Η.Υ.; Είναι αναγκαία η ύπαρξη ελεύθερου χώρου στον υπολογιστή, μετά την εγκατάσταση του συστήματος; Σε πόσα μέρη πρέπει να διαχωρίζεται ο σκληρός δίσκος, ώστε το σύστημα να είναι λειτουργικό; Η διαχείριση του μητρώου αρχείων (log files), ενδιαφέρει τον χρήστη; Η ασφάλεια είναι θέμα που προκαλεί ανησυχία για το χρήση; κλπ. [01]



Σχήμα 5.1: Ο διαχειριστής παραθύρων «FluxBox»

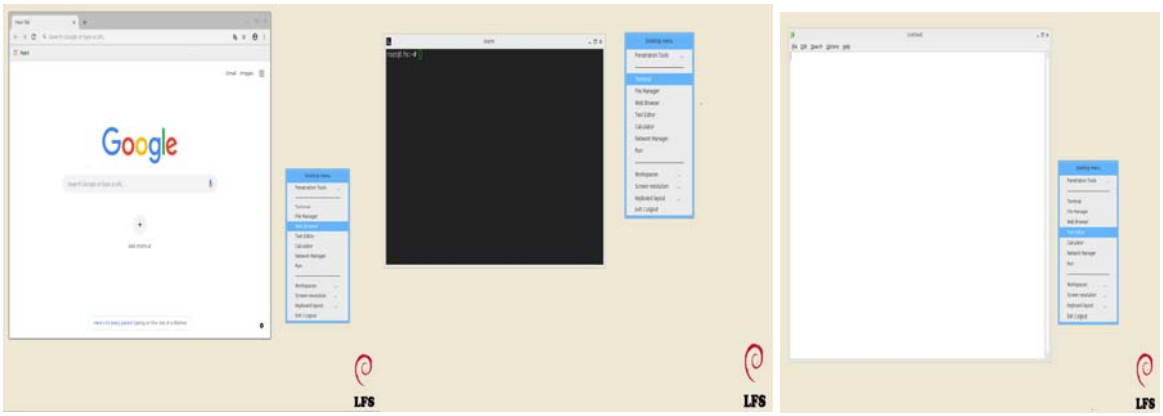
Επιλογή χαρακτηριστικών συστήματος

Το σύστημα LFS, είναι μια σύγχρονη, φορητή, μικρή σε μέγεθος και γρήγορη διανομή Linux με δυνατότητα πρόσθετης επέκτασης και απλοϊκό σχεδιασμό. Βασίζεται στη διανομή Slax Debian, η οποίο του δίνει τη δυνατότητα να εκμεταλλεύεται ολόκληρο το οικοσύστημα της, χρησιμοποιώντας την εντολή «apt». Η διανομή Debian, αποτελεί μια από τις κορυφαίες Linux διανομές που υπάρχουν σήμερα στην αγορά. Διανομές ανάλογου εκτοπίσματος, είναι η Fedora, το OpenSUSE, το Ubuntu κλπ. Το LFS, τρέχει απευθείας από οποιαδήποτε συσκευή USB. Στο σύστημα που θα τοποθετηθεί το USB, γίνονται οι ανάλογες ρυθμίσεις στο BIOS του, για να το αναγνωρίζει ως λειτουργικό μέσω εκκίνησης. Για το LFS, έχει χρησιμοποιηθεί συσκευή USB με χωρητικότητα 16GB παρόλο που το βασικό μέγεθος του λειτουργικού, πριν την τοποθέτηση των προγραμμάτων

ήταν περίπου 250Mb. Το εν λόγω λειτουργικό, δεν χρειάζεται να εγκατασταθεί στο σύστημα που θα τρέξει, έτσι μπορεί εύκολα να μεταφέρεται παντού. Επιπρόσθετα, αφού το λειτουργικό σύστημα έχει ξεκινήσει από το USB Flash Drive, όλες οι αλλαγές, οι διαμορφώσεις και οι τροποποιήσεις που γίνονται σε αυτό, αποθηκεύονται στο USB. Οι αλλαγές αυτές, διατηρούνται και κατά την επόμενη εκκίνηση, ακόμα και σε περιπτώσεις που η εκκίνηση μπορεί να γίνει από διαφορετικό υπολογιστή. [14]

Περιγραφή του LFS

Παρά το μικρό του μέγεθος, το LFS παρέχει ένα απλό και αρκετά γρήγορο γραφικό περιβάλλον, με δυνατότητα να προσαρμόζεται ανάλογα με τις ανάγκες του χρήστη. Μπορεί να προσθαφαιρεί διάφορες εφαρμογές, όπως είναι οι φυλλομετρητές περιήγησης στο διαδίκτυο, το πρόγραμμα σύνταξης κειμένου, τα εργαλεία διαχείρισης κλπ .Το LFS, έχει ως διαχειριστή για το περιβάλλον του το «FluxBox» (σχήμα 5.1), το οποίο είναι βασισμένο στο ανοικτό κώδικα του «BlackBox» γραμμένο στην γλώσσα προγραμματισμού C ++ και έχει ελεύθερη άδεια χρήσης. Ο τελευταίος αποτελεί ένα από τους πιο γνωστούς διαχειριστές παραθύρων (window managers). Χρησιμοποιεί, περιορισμένους πόρους και είναι πολύ εύκολο στο χειρισμό. Ακόμα σε αυτό, περιλαμβάνεται ένας φυλλομετρητής Chrome, το «Chromium», ένα Terminal emulator, το «xterm» και το πρόγραμμα σύνταξης κειμένου, «leafpad» (σχήμα 5.2). [14]

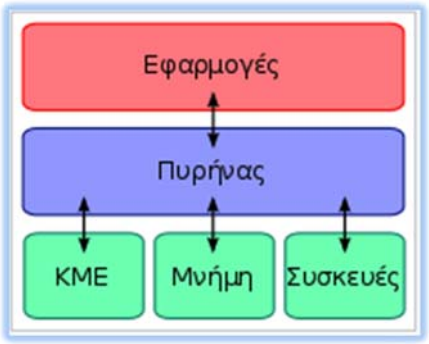


Σχήμα 5.2: Εφαρμογές που περιλαμβάνονται στο σύστημα LFS.

Επιλογή αρχιτεκτονικής

Ο πρωταρχικός στόχος, όσο αφορά την αρχιτεκτονική του λειτουργικού συστήματος LFS (σχήμα 5.3), είναι η συμβατότητα με τους επεξεργαστές AMD / Intel x86 (32-bit) και x86_64 (64-bit). Για το συγκεκριμένο σύστημα έχει επιλεγεί να χρησιμοποιηθεί ο πυρήνας (kernel)32bit . Ο πυρήνας,

είναι κώδικας χαμηλού επιπέδου, που χρησιμοποιείται αποκλειστικά για την αρχιτεκτονική του επεξεργαστή στην οποία στοχεύει το λειτουργικό σύστημα και είναι γραμμένος, σε γλώσσα προγραμματισμού C. Σε κάθε λογισμικό σύστημα, ο πυρήνας αποτελεί το πιο χαμηλό επίπεδο αφαίρεσης υλικού, ειδικά των επεξεργαστών, της μνήμης και των μονάδων εισόδου/ εξόδου. Ο πυρήνας, έχει σχεδιαστεί για να εξυπηρετεί χωρίς περιορισμούς ακόμα και υπολογιστές παλαιότερης εποχής και τεχνολογίας. Μοναδικό μειονέκτημα του, είναι ότι χρησιμοποιεί μόνο μέχρι 4GB μνήμης RAM, ανεξάρτητα εάν στον υπολογιστή είναι εγκατεστημένη πολύ περισσότερη μνήμη. [01]



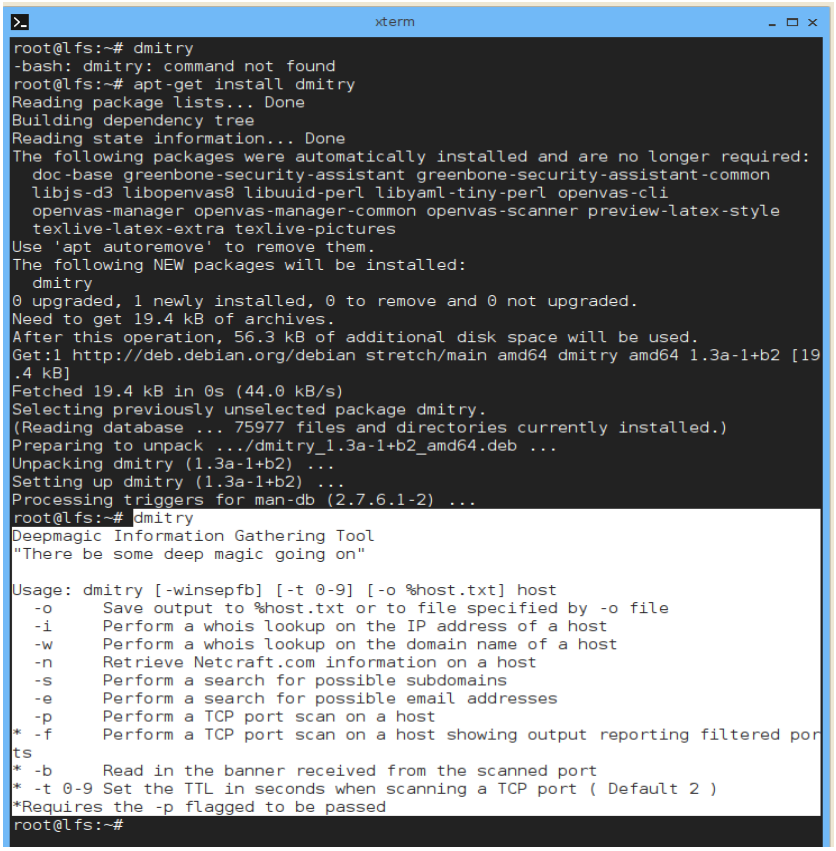
Σχήμα 5.3: Πυρήνας (kernel) συνδέει το λογισμικό εφαρμογών με το υλικό του υπολογιστή.

Συνεχιζόμενες αλλαγές

Όπως αναφέρθηκε πιο πάνω, το LFS χρησιμοποιεί USB Flash Drive το οποίο έχει μορφοποιηθεί ανάλογα για να υποστηρίζει συστήματα αρχείων FAT32. Όλες οι αλλαγές που γίνονται στο σύστημα συμπεριλαμβανομένων εγκαταστάσεων εφαρμογών και δημιουργία αρχείων, αποθηκεύονται στο αρχείο «changes.dat», το οποίο δημιουργείται στη συσκευή εκκίνησης. Έτσι κάθε φορά που γίνεται επανεκκίνηση του συστήματος στο οποίο βρίσκεται το USB, κρατά τις αλλαγές που έγιναν σε αυτό. Σημειώνεται ότι οι αλλαγές είναι συνεχιζόμενες και δεν επηρεάζονται, εάν το USB λειτουργεί σε διαφορετικά συστήματα κάθε φορά. Κατά την εκκίνηση του το LFS, δεσμεύει το USB αφού διαβάζει δεδομένα συστήματος από αυτό. Παρόλο που η αποσύνδεση ή η εξαγωγή του από το σύστημα δεν θα κατέστρεφε το λειτουργικό του σύστημα, εντούτοις είναι πιο ορθό να αποσυνδέεται το USB, μετά την απενεργοποίηση του υπολογιστή χρησιμοποιώντας την λειτουργία Shutdown. Το ίδιο συμβαίνει, εάν υπάρχει πρόσβαση στους σκληρούς δίσκους του υπολογιστή στον οποίο γίνεται η σύνδεση, καθώς παραμένουν σε κατάσταση χρήσης. [14]

Προσθήκη πακέτων με αυτοματοποιημένο ή μη τρόπο

Το σύστημα, υποστηρίζει πλήρως την εντολή «apt» (σχήμα 5.4), η οποία αποτελεί ένα ισχυρό εργαλείο γραμμής εντολών, κατάλληλο για εργασίες όπως είναι η εγκατάσταση νέων πακέτων λογισμικού ή αναβάθμιση πακέτων που είδη υπάρχουν. Για να εγκατασταθεί ένα πακέτο συμπεριλαμβανομένων όλων των βιβλιοθηκών και άλλων εξαρτήσεων που είναι απαραίτητες για την εκτέλεση του, απλά εκτελείται το, «apt install» και η ονομασία του πακέτου. Επιπλέον, παρέχεται η δυνατότητα αναζήτησης πακέτων για τα οποία ο χρήστης δεν είναι σίγουρος πως αναγράφεται το όνομα του πακέτου που θα εγκατασταθεί. Σε περιπτώσεις όπου η προσθήκη πακέτων με αυτόματο τρόπο είναι αδύνατη, μπορεί να γίνει χειροκίνητα, κάνοντας λήψη και σύνταξη πηγαίων κωδικών από το διαδίκτυο. Σε κάποιες περιπτώσεις, θα χρειαστεί να γίνει εγκατάσταση κάποιων απαραίτητων δομικών στοιχείων, τα οποία θα δίνουν την δυνατότητα τα πακέτα να γίνονται compile. Για πακέτα που ενδέχεται να χρειάζονται να κατεβούν από τον ιστότοπο «github» υπάρχει ήδη εγκατεστημένη και μπορεί να χρησιμοποιηθεί άμεσα η εφαρμογή «git». [10]



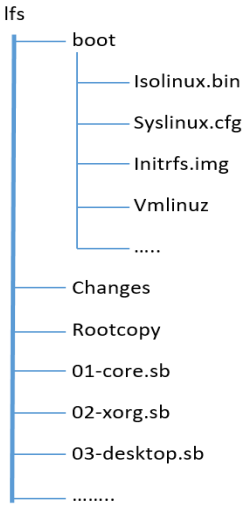
Σχήμα 5.4: Αναζήτηση και εγκατάσταση της εφαρμογής "dmitry" με την εντολή «apt»

Βοηθητικά προγράμματα λειτουργίας

Στο LFS έχουν συμπεριληφθεί αρκετά πακέτα που αφορούν, υπηρεσίες αρχειοθέτησης όπως είναι τα (gzip/gunzip, xz/unxz, cpio/tar), προγράμματα για σκληρούς δίσκους (fdisk, mdadm), εργαλεία παρακολούθησης υλικού (dmidecode, smartctl), βοηθητικά προγράμματα συστήματος αρχείων (mkfs, fsck), εργαλεία συστήματος (lsof, htop), εργαλεία ανάκτησης δεδομένων (ddrescue, rsync), εργαλεία δικτύωσης (ip, nc, networkctl, πακέτα υποστήριξης για Windows (mount –t cifs) κλπ.

5.2 Αρχιτεκτονική συστήματος

Δομή συστήματος LFS



Σχήμα 5.5: Ο Πυρήνας συνδέει το λογισμικό εφαρμογών με το υλικό του υπολογιστή.

Όλα τα αρχεία δεδομένων, βρίσκονται στο USB, σε μόνο μια ρίζα (σχήμα 5.5). Κατά την εκκίνηση του υπολογιστή στον οποίο έχει τοποθετηθεί το LFS-USB, στην πραγματικότητα φορτώνεται μόνο το αρχείο εκκίνησης «syslinux». Το αρχείο εκκίνησης, είναι αποθηκευμένο στο "ldlinux.sys" . Μόλις εκτελεστεί το αρχείο εκκίνησης «syslinux», ακολουθεί ότι περιλαμβάνεται στο αρχείο ρύθμισης παραμέτρων «syslinux.cfg». Σε αυτό το αρχείο περιλαμβάνονται οδηγίες για να φορτωθούν δύο αρχεία στη μνήμη. Το αρχείο «vmlinuz», το οποίο είναι στην πραγματικότητα ο πυρήνας του λειτουργικού συστήματος και το αρχείο «initrfs.img», το οποίο αποτελεί το σύστημα αρχείων ρίζας.

Ξεκινώντας το σύστημα

Είναι κοινή πρακτική σε όλες σχεδόν τις διανομές Linux, όταν αυτές ξεκινούν από έναν σκληρό δίσκο, ο πυρήνας τους συνδέεται (mount) με το σύστημα αρχείων ρίζας (root filesystem), στο σκληρό δίσκο. Το /sbin/init, εκτελείται ως η κύρια διαδικασία εκκίνησης του συστήματος. Στην περίπτωση του LFS και κυρίως στην απουσία σκληρού δίσκου από αυτό, εξακολουθεί να υπάρχει ανάγκη από τον πυρήνα για κάποια διαδικασία «init» για να ξεκινήσει. Για να επιτευχθεί αυτό, μεταφέρει ένα βασικό σύστημα αρχείων στο αρχείο «initrfs.img», σε συμπιεσμένη μορφή. Το συμπιεσμένο αρχείο, περιλαμβάνει ευρετήρια, διάφορα άλλα αρχεία και βασικά εργαλεία Linux με εντολές ως επίσης και το αρχείο «init».

Έτσι, αφού ο πυρήνας ξεκινήσει με επιτυχία και έχει τον πλήρη έλεγχο του υπολογιστή στον οποίο τρέχει, βρίσκει το συμπιεσμένο αρχείο στη μνήμη. Το συμπιεσμένο αρχείο, έχει φορτωθεί από το αρχείο «initrfs.img» με την βοήθεια του αρχείου εκκίνησης «syslinux», σε μια προσωρινή περιοχή μνήμης. Η προσωρινή μνήμη, λειτουργεί ως ένα σύστημα αρχείων ρίζας, και ονομάζεται «initramfs». Πριν η διαδικασία «init» μπορέσει να αρχίσει να αναζητά δεδομένα, από στις συσκευές που είναι διαθέσιμες, ρυθμίζεται το περιβάλλον εργασίας. Τα συστήματα αρχείων, «proc» και «sysfs», συνδέονται στα /proc και /sys αντίστοιχα. Ορισμένοι, σημαντικοί οδηγοί του πυρήνα, όπως είναι οι «aufs», «squashfs» και «loop», φορτώνονται στον πυρήνα, χρησιμοποιώντας το πρόγραμμα «modprobe», το οποίο βοηθά να γίνει η φόρτωση αυτή. Τέλος, τα αρχεία των συσκευών δημιουργούνται στο ευρετήριο, / dev μέσω της εντολής «mdev». [10]

5.3 Αρχεία λειτουργικού συστήματος

Όπως σε κάθε διανομή Linux που υπάρχει, έτσι και στο σύστημα LFS, έχει χρησιμοποιηθεί το πρότυπο ιεραρχίας του συστήματος αρχείων FHS. Το εν λόγο σύστημα αρχείων, ορίζει τη δομή του καταλόγου και τα περιεχόμενα του. Στο σχήμα 5.6, που ακολουθεί, παρουσιάζεται η εικόνα της ρίζας αρχείων του LFS. Στην ρίζα αρχείων, αναγράφεται σχετική ονομασία η οποία επεξηγείται σε πίνακα στο παράρτημα Α.

Σχήμα 5.6: Αρχεία ρίζας συστήματος LFS

5.4 Παρουσίαση συστήματος LFS μέσω σεναρίου

Η διανομή LFS όπως αναφέρθηκε πιο πάνω, μπορεί να προσαρμοστεί ανάλογα με το περιστατικό που έχει να χειριστεί. Για παράδειγμα, η διανομή και κατ' επέκταση τα εργαλεία που θα εκτελέσουν στις δοκιμές διείσδυσης, εάν είχαν να αντιμετωπίσουν συστήματα που δραστηριοποιούνται στο διαδίκτυο, θα περιλάμβανε συγκεκριμένα εργαλεία για το σκοπό αυτό, ώστε να μπορεί να χειρίζεται διακομιστές DNS, Web και Email, τα Firewalls, τα συστήματα IPS και IDS, τους δρομολογητές και άλλες συσκευές. Το παράδειγμα που θα ακολουθήσει, αφορά ένα πολύ απλό δίκτυο, σε ένα γραφείο με λιγοστούς πόρους και μικρή δικτυακή υποδομή. Το γραφείο αυτό, θα αποτελέσει το σενάριο (case study) και το πεδίο εφαρμογής της έρευνας, προσαρμόζοντας και χρησιμοποιώντας την διανομή LFS, ως το μοναδικό εργαλείο για εκτέλεση προκαταρκτικών δοκιμών διείσδυσης. Ο χειριστής του συστήματος θα είναι ένα νεαρό άτομο, το οποίο δεν έχει ιδιαίτερες γνώσεις σε πληροφορικά συστήματα, αλλά φαντάζει το καταλληλότερο υπό τις περιστάσεις πρόσωπο για να εκτελέσει τις δοκιμές διείσδυσης.

Περιγραφή του δικτύου βάση σεναρίου

Το πληροφοριακό σύστημα είναι εγκατεστημένο στο μικρό γραφείο στο οποίο θα γίνουν οι δοκιμές διείσδυσης. Μετά από συζήτηση που έγινε με τον ιδιοκτήτη, έχει διαφανεί ότι σε αυτό περιλαμβάνεται ένας μικρός αριθμό ηλεκτρονικών υπολογιστών και άλλων συσκευών. Υπάρχουν ουσιαστικά, δύο επιτραπέζιοι υπολογιστές, ένας κινητός υπολογιστής, ένας εκτυπωτής δικτύου μια έξυπνη τηλεόραση, ένας κεντρικός δρομολογητής και ακόμα δύο δρομολογητές σε άλλα

γραφεία. Τα προαναφερθέντα είναι ενωμένα μεταξύ τους χωρίς διακομιστή και έχουν όλα σύνδεση στο διαδίκτυο. Επιπρόσθετα στο ίδιο δίκτυο, με σύνδεση στο διαδίκτυο είναι η έξυπνη τηλεόραση και η συσκευή φωνητικών καλεσμάτων "Alexa". Ο ιδιοκτήτης δεν ήταν σε θέση να δώσει οποιεσδήποτε άλλες πληροφορίες πέραν της ρητής του συγκατάθεσης για να προχωρήσει η διαδικασία των δοκιμών, κατανοώντας τις επιπτώσεις που επιφέρει ο έλεγχος όταν διεξάγεται σε ζωντανά συστήματα και πραγματικά δεδομένα.

Μεθοδολογία σεναρίου

Η μεθοδολογία που επιλέγηκε να ακολουθηθεί, βασίζεται σε τέσσερα βασικά βήματα τα οποία αναλύονται στην παράγραφο "παρεμβατική αναζήτηση στόχων" στο κεφάλαιο 3. Τα βήματα, αποτελούν υποκατηγορία της φάσης ανακάλυψης και μέσω των βημάτων αυτών γίνονται οι διάφορες δοκιμές και εκτελούνται οι έλεγχοι προς την εξερεύνηση του δικτύου στόχου. Απαραίτητη προϋπόθεση όμως πριν την πραγματοποίηση της δραστηριότητας αυτής είναι η εξασφάλιση της συγκατάθεσης του ιδιοκτήτη. Παρόλο που στο πλαίσιο αυτού του βήματος, υπάρχουν πέντε στοιχεία που καθορίζουν περαιτέρω τη μεθοδολογία, για σκοπούς του σεναρίου θα γίνει αναφορά στα πρώτα τέσσερα. Τα βήματα που περιλαμβάνονται στο σενάριο είναι, τα βήματα της αναζήτησης των ζωντανών συστημάτων και των ανοικτών θυρών, η καταγραφή των λειτουργικών συστημάτων και ο προσδιορισμός τρωτότητας συστήματος. Επιπρόσθετα, για την ομαλότερη εξέλιξη της παρουσίασης της διανομής, έχει προστεθεί η φάση της τεχνικής αναγνώρισης. Στη φάση αυτή γίνεται η συγκέντρωση όσο το δυνατό περισσοτέρων πληροφοριών, που έχουν σχέση με το πληροφοριακό σύστημα. Για την ολοκλήρωση των ελέγχων του σεναρίου αυτού, έχουν χρησιμοποιηθεί διάφορα εργαλεία ανοικτού κώδικα. Μερικά από αυτά είναι, το Ip Route, το ArpScan, το Netdiscover, το Whois, το Nmap, το Zenmap, το knocker, το masscan κλπ. Η ανάλυση για κάθε εργαλείο υπάρχει στο παράρτημα Β1.

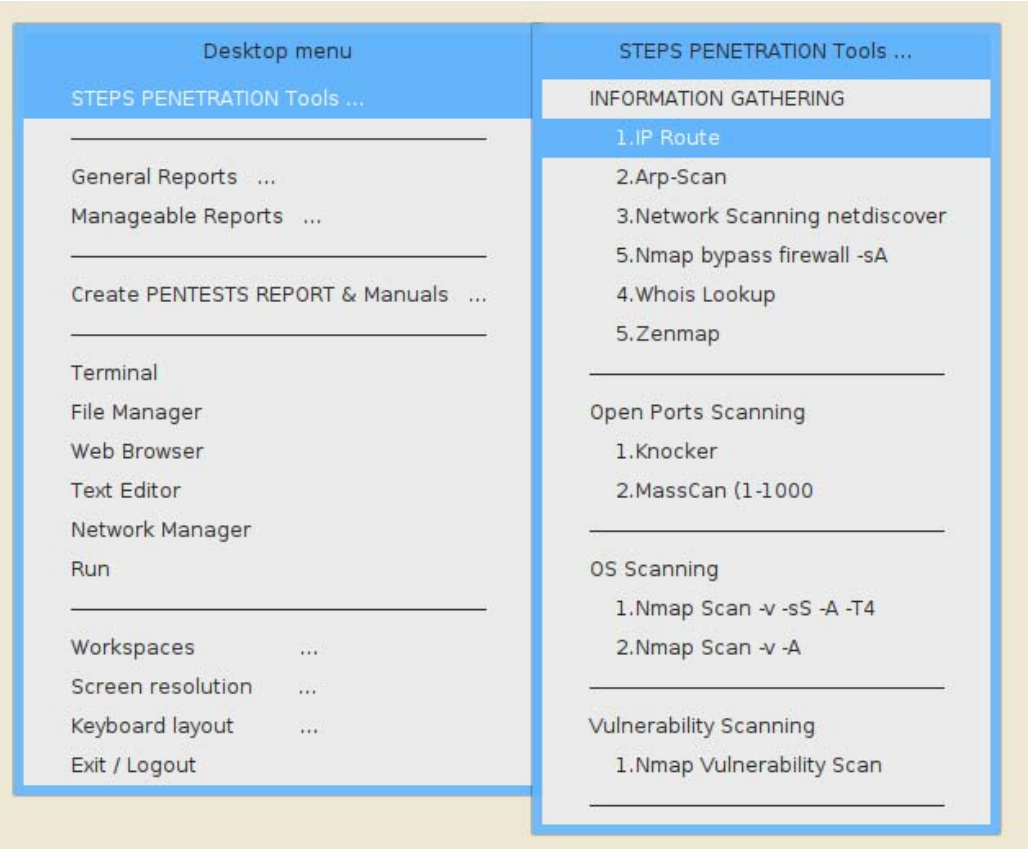
Συγκέντρωση πληροφοριών

Το LFS USB, τοποθετείται σε κινητό ηλεκτρονικό υπολογιστή από το άτομο που θα εκτελέσει τις δοκιμές διείσδυσης. Ο υπολογιστής ανήκει στον ιδιοκτήτη του γραφείου. Από πληροφορίες που δόθηκαν, είναι πιθανό ο υπολογιστής να τρέχει λειτουργικό σύστημα Windows 10 ή Windows 8.1. Ο υπολογιστής, προστατεύεται σίγουρα από κωδικό χρήστη. Ξεκινώντας τον υπολογιστή, φορτώνεται το λειτουργικό σύστημα του LFS (σχήμα 5.1). Παράλληλα, κάνει αυτόματα mount τους σκληρούς του δίσκους και τα partitions του, κατά τρόπο ώστε να επιτρέπει στον χειριστή

παρόλο που δεν έχει εξουσιοδότηση στον υπολογιστή, να μπορεί να κινείται σε όλα τα αρχεία του, ξεπερνώντας την πρώτη γραμμή ασφάλειας του συστήματος. Μέχρι τη δεδομένη στιγμή, το πρώτο επίπεδο ασφάλειας ήταν ο κωδικός χρήστη στο υπολογιστή. Αυτό καταγράφεται στον πίνακα του σχήματος 5.8, ως η ευπάθεια 1. Η δυνατότητα του χειριστή να αλλοιώνει αρχεία, να τα διαγράφει, να τα αντιγράφει και να τα μετακινεί, δημιουργεί την ευπάθεια 2. Η ευπάθεια 3, αποτελεί την δυνατότητα αφαίρεσης του κωδικού χρήσης από τον νόμιμο χρήστη ή ακόμα και τον διαχειριστή (Administrator) του Η.Υ. Αυτό επιτυγχάνεται με το εργαλείο chntpw και τις εντολές "chntpw -l" , "chntpw -i". Τα σχήματα Α2-1α και Α2-1β του παραρτήματος Α2, είναι σχετικά.

Το εργαλείο chntpw, εκτελείται στην τοποθεσία που βρίσκεται το αρχείο SAM, το οποίο είναι υπεύθυνο να διατηρεί και να διαχειρίζεται τα ονόματα των νόμιμων χρηστών του συστήματος. Η ακριβής τοποθεσία του αρχείου SAM στο λειτουργικό σύστημα Windows, είναι "/system32 /config/". Έτσι, έχοντας ο χειριστής τον πλήρη έλεγχο του υπολογιστή, τον επανεκκινά και επιτυγχάνει είσοδο σε αυτόν αφού δεν υπάρχει πλέον κωδικός χρήστη που να του απαγορεύει την είσοδο. Από το σημείο αυτό και έπειτα, τα οποιαδήποτε αρχεία και πληροφορίες, συμπεριλαμβανομένων των προσωπικών δεδομένων του νόμιμου ιδιοκτήτη, βρίσκονται στα χέρια του χειριστή.

Ακολούθως ο χειριστής, συνεχίζει να εφαρμόζει βάση του σεναρίου τα βήματα για να εκτελέσει τις δοκιμές διείσδυσης σε ολόκληρο το δίκτυο. Όπως είδη αναφέρθηκε, απαραίτητη προϋπόθεση για να λειτουργήσει το LFS πρέπει πριν την έναρξη του υπολογιστή, να τοποθετηθεί σε αυτόν το LFS USB. Αυτό έπραξε ο χειριστής αφού πρώτα απενεργοποίησε τον υπολογιστή από το περιβάλλον Windows. Ο υπολογιστής αφού αντιληφθεί την ύπαρξη του LFS-USB το διαβάζει ως το λειτουργικό σύστημα έναρξης και εισέρχεται στην κεντρική σελίδα του συστήματος. Στην σελίδα αυτή βρίσκεται το κεντρικό μενού διαχείρισης των δοκιμών διείσδυσης, όπου υπάρχουν οι κύριες επιλογές των εργαλείων χρήσης, όπως φαίνεται στο σχήμα 5.7 πιο κάτω. Η πρώτη επιλογή που πρέπει να εκτελείται, είναι η επιλογή με όνομα «STEPS PENETRATION Tools» στην οποία εμφανίζεται η υποκατηγορία «Information Gathering». Σε αυτή την επιλογή, έχουν δημιουργηθεί πέντε βήματα-επιλογές που χρησιμοποιούνται για να μαζέψουν όσο το δυνατό περισσότερες πληροφορίες για τις συσκευές που βρίσκονται στο δίκτυο.



Σχήμα 5.7: Κεντρικό μενού λειτουργειών για δοκιμές διείσδυσης

Μέσω του πρώτου εργαλείου, "IP Route" (σχήμα Α2-2 του παραρτήματος Α2), μαζεύεται πληροφόρηση σχετικά με την διεύθυνση IP της συσκευής στην οποία τρέχει το LFS, την μάσκα του δικτύου, π.χ. εάν είναι /24,/20,/16 κλπ., ως επίσης και η διεύθυνση IP του δρομολογητή. Αμέσως μετά, μέσω του εργαλείου Arp-Scan (σχήμα Α2-3 του παραρτήματος Α2), μαζεύονται οι διευθύνσεις IP και οι διευθύνσεις MAC των συσκευών που είναι ενωμένες με το δίκτυο, καθώς και τα ονόματα των συσκευών αυτών. Το επόμενο εργαλείο, χρησιμοποιείται για να συμπληρώσει τα όσα άγνωστα στοιχεία αφορούσαν τις εν λόγω συσκευές. Ακόμα ένα εργαλείο συλλογής πληροφοριών που μπορεί να χρησιμοποιηθεί είναι το Zenmap (σχήμα Α2-6 του παραρτήματος Α2). Το ZENMAP, αποτελεί την γραφική έκδοση του εργαλείου Nmap για το οποίο γίνεται επεξήγηση στον πίνακα του παραρτήματος Α2. Το άτομο βάση του σεναρίου που εκτέλεσε τις δοκιμές διείσδυσης, χρησιμοποίησε το εργαλείο Zenmap, γιατί θεωρείται πιο φιλικό και πιο εύχρηστο. Παρ' όλα αυτά, για να εκτελέσει εντολές σε αυτό, ζήτησε τηλεφωνική βοήθεια. Τα αποτελέσματα του Zenmap, φαίνονται στον πίνακα αναφοράς ευπαθειών (σχήμα 5.8), από τον αύξοντα αριθμό 4 έως και τον αύξοντα αριθμό 8. Τα επόμενα τρία βήματα που εκτελέστηκαν κατά την διαδικασία των δοκιμών, αφορούσαν την σάρωση των θυρών και των λειτουργικών προγραμμάτων, τον προσδιορισμό της τρωτότητας του συστήματος και τέλος την αναφορά των ευπαθειών. Τα βήματα αναλύονται πιο κάτω.

1. Σάρωση συστημάτων, θυρών και λειτουργικών προγραμμάτων. Οι τρεις λειτουργίες που εκτελούνται στο πρώτο βήμα, χρησιμοποιούν ανάλογες μεθοδολογίες με τα εργαλεία που είδη χρησιμοποιήθηκαν στην προηγούμενη παράγραφο για την συγκέντρωση των πληροφοριών. Συγκεκριμένα, το Netdiscover (σχήμα Α2-4 του παραρτήματος Α2) και το Arp-scan, όταν έτρεξαν επέστρεψαν όμοια αποτελέσματα. Το γεγονός ότι υπήρξαν αποτελέσματα, καταδεικνύει ότι τα συστήματα είναι ζωντανά. Το ίδιο συμβαίνει και με τα εργαλεία σάρωσης ανοικτών θυρών. Κατά την εκτέλεση του Zenmap, εμφανίστηκαν οι συσκευές των οποίων οι θύρες ήταν ανοικτές. Αρκετά από αυτά τα συστήματα παρουσίαζαν ευπάθειες (σχήμα Α2-7 του παραρτήματος Α2) οι οποίες απεικονίζονται στο σχήμα Α2-8 του παραρτήματος Α2, όπου το γράφημα παρουσιάζει πιο απλά τις συσκευές που παρουσιάζουν ευπάθειες με κόκκινο χρώμα. Επίσης, αυτό συνέβη και όταν έτρεξαν τα εργαλεία knocker και masscan (σχήμα Α2-9 του παραρτήματος Α2). Παρενθετικά, και στα δύο εργαλεία σάρωσης για ανεύρεση ανοικτών θυρών, ζητείται από τον χρήστη να καταχωρήσει καθορίζοντας την διεύθυνση IP της συσκευής που επιθυμεί να σαρώσει και μετά ξεκινά η σάρωση. Τέλος, οι εντολές “Nmap -v sS -A -T4”, (σχήμα Α2-10 του παραρτήματος Α2), είναι υπεύθυνες να τρέχουν σε όλο το δίκτυο και μαζεύουν τα πραγματικό λειτουργικά συστήματα των σαρωμένων συστημάτων ή άλλα προγράμματα που τρέχουν σε αυτά.

2. Προσδιορισμός τρωτότητας συστήματος. Ακολουθώντας πάντοτε την μεθοδολογία διείσδυσης, ο χειριστής προχώρησε με τον προσδιορισμό των τρωτών σημείων του συστήματος αφού παράλληλα προσπαθούσε να επεξεργαστεί και να εξηγήσει τα ευρήματα όλων των προηγούμενων βημάτων. Η αναζήτηση για ευπάθειες και τρωτά σημεία στο σύστημα γίνονται από το εργαλείο Nmap . Η παραμετροποίηση του Nmap σε συνδυασμό με τα προεγκατεστημένα –scrip, που περιλαμβάνονται στις βιβλιοθήκες του, καταφέρνουν να εκτελούν σχετικά γρήγορες και με ακρίβεια δοκιμές. Στο σενάριο που τέθηκε από την αρχή, δεν περιλαμβάνονται εμπορικά εργαλεία τα οποία περιέχουν πολύ περισσότερες λειτουργίες από ότι τα εργαλεία ανοιχτού κώδικα. Οι εντολή Nmap, που χρησιμοποιήθηκε για τις δοκιμές προς αναζήτηση ευπαθειών στα συστήματα του δικτύου ήταν, “nmap -Pn –script vuln” συνοδευόμενη με το IP της συσκευής για την οποία θα εκτελεστεί η αναζήτηση ευπάθειας (σχήμα Α2-11 του παραρτήματος Α2).

3. Αναφορά ευπαθειών.

Αρ. Ευπάθειας	Περιγραφή	Ευπάθεια
1	Δυνατότητα χειριστή να κυκλοφορά ελεύθερα στα αρχεία του υπολογιστή **192.168.10.18**	Πολύ κρίσιμη
2	Δυνατότητα χειριστή για αλλοίωση των αρχείων περιλαμβανομένης της διαγραφής, αντιγραφής και μετακίνησης **192.168.10.18**	Πολύ κρίσιμη
3	Δυνατότητα αφαίρεσης του κωδικού χρήσης από νόμιμούς χρήστες ή ακόμα και τον Admin του Η.Υ. Απόκτηση πλήρους ελέγχου του υπολογιστή επανεκκινώντας τον. Εκποίηση προσωπικών δεδομένων του νόμιμου ιδιοκτήτη. **192.168.10.18**	Πολύ κρίσιμη
Αποτελέσματα ZENMAP 192.168.10.0/24		
4	**MasterPC 192.168.10.6** – open ports 10 (21,80,135,139,443,445,902,912,3389,5357)	Κρίσιμη
5	**192.168.10.13** – open ports 11 (80,139,443,445,515,631,6839,7435,8080,9100,9220)	Κρίσιμη
6	**192.168.10.20** – open ports 23 (21-23,53,80,111,139,445,512,513,514,1099,1524, 2049,2121,3306,5432,5900,6000,6667,8009,8180)	Πολύ Κρίσιμη
7	192.168.10.10 – open ports 3 (23,80,333)	κρίσιμη
8	192.168.10.100 – open ports 3 (53,80,333)	λιγότερο κρίσιμη

Σχήμα 5.8: Πίνακας «Αναφορά Ευπαθειών» βάση του σεναρίου

Όπως διαφαίνεται στον πίνακα του σχήματος 5.8 πιο πάνω, τα συστήματα του εν λόγο δικτύου παρουσίαζαν αρκετές ευπάθειες και αναμένονται να γίνουν διορθωτικά μέτρα προς επίλυση τους. Οι πιο σημαντικές ευπάθειες, που πρέπει να τύχουν άμεσης διόρθωσης είναι στα συστήματα των συσκευών με διεύθυνση IP, 192.168.10.6 και 192.168.10.20. Πέραν τούτου, καταγράφηκε και το γεγονός, πάντα στο πλαίσιο του σεναρίου, ότι το άτομο που εκτελούσε τις δοκιμές χρειάστηκε να ζητήσει αρκετές φορές βοήθεια, κυρίως για θέματα παραμετροποίησης των εντολών που έτρεχε αλλά και για θέματα που άτονται τις επεξήγησης των ευρημάτων.

Ως εκ των αποτελεσμάτων, η δοκιμή διείσδυσης που εκτελέστηκε θεωρείται επιτυχής καθώς έχει εξάγει αρκετά αποτελέσματα που χρήζουν ανάλυσης. Παρόλο που δεν μπορεί να θεωρηθεί ως σοβαρή επαγγελματική εργασία εντούτοις εκτελέστηκε μια αρκετά καλή προκαταρτική δοκιμή.

Κεφάλαιο 6
Επίλογος

Στο τελευταίο μέρος της διατριβής, εξάγονται συμπεράσματα και προτάσεις που βασίστηκαν σε ερευνητικά ερωτήματα που τέθηκαν στην αρχή της έρευνας. Τα βασικά ερωτήματα που τέθηκαν από την αρχή έχουν απαντηθεί με επιχειρήματα τα οποία ενισχύθηκαν μέσα από την εκτενή βιβλιογραφική ανασκόπηση, πληροφορίες που αντλήθηκαν από ηλεκτρονικά και άλλα βιβλία σχετικά με το θέμα της έρευνας, καθώς και από επιστημονικά περιοδικά και ακαδημαϊκά άρθρα. Επιπρόσθετα, γίνονται συγκεκριμένες προτάσεις σχετικές με τις γενικές αρχές ασφάλειας, οι οποίες μπορούν να φανούν αρκετά χρήσιμες για όσους επιθυμούν να διενεργήσουν δοκιμές διείσδυσης. Οι προτάσεις κατά την εφαρμογή τους, μπορούν να περιορίσουν τις απειλές και να μειώσουν το επίπεδο των κινδύνων. [03]

6.1 Συμπεράσματα

Οι δοκιμές διείσδυσης, όπως έχει αναφερθεί αρκετές φορές στην έρευνα, είναι διαδικασίες, φάσεις βήματα και μεθοδολογίες που εκτελούνται από εξιδεικευμένους επαγγελματίες με σκοπό το εντοπισμό ευπαθειών ασφαλείας σε εφαρμογές, συστήματα ή δικτυακές υποδομές. Πρωταρχικός σκοπός των δοκιμών είναι να προστατεύσουν το σύστημα από μη εξουσιοδοτημένες προσβάσεις αλλά και από πιθανές αδυναμίες που παρουσιάζονται στην ευρύτερη υποδομή του δικτύου. Παράλληλα, όπου είναι εφικτό θα πρέπει να εξασφαλίζουν σημαντικά δεδομένα από τους επιτιθέμενους, που κατάφεραν να αποκτήσουν πρόσβαση στο σύστημα. Αφού επιτευχθεί ο στόχος, πρέπει να λαμβάνονται ισχυρά αντίμετρα έτσι ώστε να μπορούν να αποτρέπουν επαναλήψεις των παραβιάσεων της ασφάλειας. Τα αντίμετρα, πρέπει να περιλαμβάνονται στην τελική αναφορά και πρέπει απαραίτητα να λαμβάνονται υπόψη, ώστε να μειώνεται ανάλογα ο κίνδυνος. [23]

Όπως έχει διαφανεί στην έρευνα, τα αίτια που προκαλούν τις ευπάθειες, είναι αρκετά περίπλοκα και πολυδιάστατα. Οφείλονται , σε σφάλματα ανάπτυξης, ρυθμίσεων, ανθρώπινα λάθη, σχετικά με την συνδεσιμότητα και την πολυπλοκότητα, τους κωδικούς πρόσβασης, την έλλειψη επικοινωνίας και τις περιπτώσεις που άπτονται της κοινωνικής μηχανικής. Το πεδίο εφαρμογής των δοκιμών, εστιάζεται στις υποδομές των δικτύων, συμπεριλαμβανομένων της συνδεσμολογίας και της τοπολογίας καθώς και στα μοντέλα αλληλεπίδρασης τους με τους χειριστές , τους διακομιστές, εξυπηρετητές κλπ. Ο κύριος λόγος επένδυσης σε δοκιμές διείσδυσης είναι η εξασφάλιση της καλύτερης ασφάλειας στον τομέα της άμυνας και η μείωση του επιπέδου του κινδύνου. [02]

Η δοκιμή ασφάλειας θεωρείται ως η πιο σημαντική πτυχή των δοκιμών διείσδυσης, η οποία δεν αποτελεί το προϊόν αλλά την διαδικασία. Ειδικότερα, οι δοκιμές αυτές λαμβάνουν υπόψη τους κύριους τομείς ενός μοντέλου ασφάλειας. Η μεθοδολογία που ακολουθείται κατά την εκτέλεση των δοκιμών βασίζεται, σε τέσσερεις φάσεις: το προγραμματισμό, την ανακάλυψη, την επίθεση και την αναφορά. [15] Η παρεμβατική αναζήτηση παρόλο που είναι υποκατηγορία της φάσης ανακάλυψης, εντούτοις αποτελεί το πιο σημαντικό κομμάτι της μεθοδολογίας, καθώς είναι το βήμα που ξεκινά την πραγματική δραστηριότητα ενός εισβολέα. Βασική προϋπόθεση, είναι όπως πριν την πραγματοποίηση της δραστηριότητας αυτής, να εξασφαλίζεται η ρητή συγκατάθεση του ιδιοκτήτη. Συνήθως δίδεται γραπτή άδεια. [02]

Υπάρχουν αρκετοί οι οποίοι γνωρίζουν ότι οι παραβιάσεις είναι δαπανηρές, αλλά αγνοούν επιλεκτικά το γεγονός ότι σε περίπτωση που υπάρξει μια παραβίαση, ίσως να χρειαστεί να καταβληθούν αρκετά μεγάλα ποσά για νομικές αμοιβές, για πρόστιμα, για επιπρόσθετες εργατοώρες σε ειδικούς για εγκατάσταση νέων συστημάτων ασφαλείας κλπ. Ακόμα, δεν πρέπει να μη ληφθεί υπόψη το ενδεχόμενο η εταιρεία να βρεθεί αντιμέτωπη με την αντίδραση των πελατών πράγμα που μπορεί να καταλήξει να πλήξει τη φήμη και την αξιοπιστία της. [33] Φυσικά, δεν υπάρχει μία απάντηση που να καθορίζει πόσο κοστίζει η δοκιμή διείσδυσης καθώς ο αριθμός των μεταβλητών σε κάθε κατάσταση είναι διαφορετικός. [17] Είναι πολύ λογικό ότι κανένας δεν πρόκειται να ξοδέψει ποσά που είναι περισσότερα της αξίας των περιουσιακών του στοιχείων. Η επένδυση στο τομέα των δοκιμών διείσδυσης οφείλει να είναι πάντοτε ανάλογη με το αντικείμενο που πρόκειται να προστατευθεί. Έτσι, πριν γίνει η ανάθεση, πρέπει απαραίτητα να γνωστοποιείται την πραγματική αξία των περιουσιακών στοιχείων της εταιρείας. Πιο συγκεκριμένα, τα κέντρα λήψης αποφάσεων πρέπει να κατανοήσουν ότι οι δοκιμές διείσδυσης είναι μια επένδυση και όχι μόνο μια ακόμη περιττή δαπάνη. [03]

Μια δοκιμή διείσδυσης που εκτελείται από πιστοποιημένο ειδικό με εμπειρία στον τομέα των δοκιμών, μπορεί εφαρμόζοντας τις γνώσεις και την ειδικότητα του, να επηρεάσει όχι μόνο τα αποτελέσματα μιας δοκιμής αλλά και τα μελλοντικά ενδεχόμενα παραβιάσεων του συστήματος. Εξίσου μεγάλης σημασίας είναι και η επιλογή του εργαλείου, με το οποίο θα εκτελεστούν οι δοκιμές διείσδυσης το οποίο οφείλει να είναι εύκολο στην ανάπτυξη, στην διαμόρφωση και στην χρήση του. Πρέπει να μπορεί να σαρώνει γρήγορα τα διάφορα συστήματα και να βάζει σε κατηγορίες τα τρωτά σημεία του συστήματος, ανάλογα με την σοβαρότητα του καθενός. Κάποιες φορές όμως τα εργαλεία μπορούν να εξάγουν λανθασμένα συμπεράσματα (false positive). Αφού γίνουν γνωστές οι δοκιμές που πρέπει να εκτελεστούν, μπορούν είτε να εκπαιδευτούν οι πόροι των εσωτερικών δοκιμών, είτε να μισθωθούν εμπειρογνώμονες ως σύμβουλους για να εκτελέσουν το έργο της διείσδυσης. [02]

Συνοψίζοντας, έχει διαφανεί από την έρευνα ότι, μπορούν να δημιουργούνται αρκετά ενδιαφέρουσες διανομές, στις οποίες συμπεριλαμβάνονται δοκιμές διείσδυσης με ισχυρά εργαλεία που ικανοποιούν σχεδόν κάθε προσδοκία, βάση της ανάγκης που υπάρχει. Πέραν τούτου όμως, ο χειριστής απαιτείται να κατέχει αρκετές γνώσεις, τόσο στο τομέα των διανομών, αφού αυτές βασίζονται σε λειτουργικά συστήματα Linux, όσο και τεχνικές γνώσεις στον τομέα των δικτυακών υποδομών. Επιπλέον, πρέπει να κατέχει ανάλογη κατάρτιση και στο τομέα της ασφάλειας των πληροφοριακών συστημάτων. Πρέπει να μπορεί να χρησιμοποιεί τα συστήματα και τις

εφαρμογές δοκιμών διείσδυσης, αλλά κυρίως να γνωρίζει τα εργαλεία που εμπεριέχονται σε αυτές. Εν κατακλείδι, πρέπει να μπορεί να σκέφτεται σαν να είναι ο ίδιος εισβολέας και προσπαθεί χωρίς εξουσιοδότηση να εκμεταλλεύεται τις όποιες αδυναμίες παρουσιάζουν τα διάφορα συστήματα, ακολουθώντας τις υπάρχουσες μεθοδολογίες και διαδικασίες επιθέσεων. Βάση, των πιο πάνω, φτάνουμε στο συμπέρασμα ότι οι δοκιμές διείσδυσης οφείλουν να εκτελούνται από επαγγελματίες, οι οποίοι έχουν τόσο την εμπειρία, όσο και την γνώση αλλά και το ανάλογο προσωπικό, που θα μπορεί να ανταγωνιστεί και να περιορίσει τις απειλές και τους κινδύνους από τις διάφορες επιθέσεις. [08]

6.2 Προτάσεις

Είναι αυτονόητο, ότι η δουλειά του ατόμου που εκτελεί δοκιμές διείσδυσης, είναι να προσομοιώνει νόμιμες απειλές, με γνώμονα τις γενικές αρχές ασφάλειας. Για να μπορεί να καθορίζει αποτελεσματικά το επίπεδο του κινδύνου που υπάρχει σε ένα οργανισμό, πρέπει να λαμβάνει υπόψη τόσο τις αρχές όσο και τις πολιτικές ασφαλείας που εφαρμόζονται στον οργανισμό. Πώς μπορεί όμως να το επιτύχει αυτό, χωρίς την ύπαρξη κάποιας μορφής εξοικείωσης; Σχετικά με την ερώτηση αυτή, ο Sun Tzu κάποτε είπε ότι: "*Αν δεν γνωρίζουμε ούτε τον εχθρό αλλά ούτε τον εαυτό μας, θα υποκύπτουμε σε κάθε μάχη".* Βάση τούτου, η πραγματική διασφάλιση ενός δικτύου, για αυτούς που εκτελούν καθήκοντα ασφάλειας στον κυβερνοχώρο, πρέπει να βασίζεται όχι μόνο σε αυτά που κατανοούν και υπάρχουν στον οργανισμό, αλλά και να γνωρίζουν από τι απειλούνται, τουλάχιστον σε πληροφοριακό επίπεδο. [20]

Οι δοκιμές απαραίτητα, πρέπει να εκτελούνται από άτομα που είναι πιστοποιημένα να εκτελούν διεισδύσεις και να έχουν εμπειρία για όλες τις μορφές δοκιμών. Για την εκτέλεση των δοκιμών απαιτούνται διαφορετικά είδη εργαλείων, γνώσεων και εμπειρογνωμοσύνης και όλα μαζί θα καθορίζουν το κόστος των δοκιμών. Πέραν των εργαλείων, το κόστος καθορίζεται από την πολυπλοκότητα του συστήματος και το μέγεθος του. Δεν είναι λίγοι αυτοί που εσφαλμένα πιστεύουν ότι επειδή μπορούν να παρακολουθούν (monitor) τις κινήσεις που εμφανίζονται μέσα στα δικά τους δίκτυα, είναι ασφαλείς από ενδεχόμενα παραβιάσεων. Επομένως, πιστεύουν ότι δεν χρειάζεται να παίρνουν, αυστηρά μέτρα, όπως αυτά της κρυπτογράφησης των επικοινωνιών, στα δικά τους επιμέρους δίκτυα. Τέτοιες προσεγγίσεις σίγουρα δεν πρέπει να τις συμμερίζεται κανείς. [08]

Αντ' αυτού, κάθε πληροφοριακό σύστημα πρέπει να διαιρείται σε μικρότερα τμηματικά εικονικά δίκτυα (VLAN's), προσεκτικά προσαρμοσμένα για ευκολότερη διαχείριση και έλεγχο. Παράλληλα, πρέπει να γίνεται συστηματικός έλεγχος στο δίκτυο για τις μη αυθεντικές ή μη εξουσιοδοτημένες από το διαχειριστή του συστήματος συσκευές. Ακόμα μπορούν να εφαρμόζονται καλές πρακτικές όπως αναφέρονται στα σενάρια δοκιμών διείσδυσης, στο Παράρτημα Β.2. Η εφαρμογή ενός συστήματος ελέγχου πρόσβασης δικτύου NAC, προσθέτει περισσότερη αξία στον τομέα της ασφάλειας, όπως και η εφαρμογή του πρωτοκόλλου 802.1X στα δίκτυα, σε συνδυασμό με την απενεργοποίηση των αχρησιμοποίητων θυρών, θεωρείται ακόμη καλύτερη λύση. Επιπρόσθετα, μπορεί να εγκατασταθεί ένα σύστημα IDS/IPS, όπως είναι το Security Onion και το οποίο μπορεί να εστιάζει στον εντοπισμό ανώμαλης δραστηριότητας δικτύου η οποία μπορεί να υποδηλώνει μια απόπειρα δηλητηρίασης των διευθύνσεων του ARP. Τέλος μια ακόμη καλή τακτική, είναι η εγκατάσταση συστημάτων Honeypot ή Sandbox. [39]

Βιβλιογραφία

Βιβλία: -

[01] G. Beekmans, Linux From Scratch, Ver 8.3, 2018

[02] R. W. Beggs, Mastering Kali Linux for Advanced Penetration Testing. Birmingham, UK: Packt Publishing, 2014.

[03] J. Broad and A. Bindner, Hacking with Kali : Practical Penetration Testing Techniques, vol. 1st ed. Amsterdam: Syngress, 2014.

[04] K. Cardwell, Building Virtual Pentesting Labs for Advanced Penetration Testing. Birmingham: Packt Publishing, 2014.

[05] P. Engebretson, The Basics of Hacking and Penetration Testing : Ethical Hacking and Penetration Testing Made Easy, vol. 2nd ed. Amsterdam: Syngress, 2013.

[06] V. Fadyushin, Instant Penetration Testing : Setting up a Test Lab How-to: Set up Your Own Penetration Testing Lab Using Practical and Precise Recipes. Birmingham: Packt Publishing, 2013.

[07] V.V.Kumar, Penetration Testing: A Complete Pentesting Guide Facilitating Smooth Backtracking for Working Hackers : A Course in Three Modules., 2016.

[08] R. Messier, Penetration Testing Basics : A Quick-Start Guide to Breaking Into Systems. [Berkeley, CA]: Apress, 2016.

[09] S.P. Oriyano, Penetration Testing Essentials. Indianapolis, UNITED STATES: John Wiley & Sons, Incorporated, 2016.

[10] A.Singh, Metasploit Penetration Testing Cookbook. Olton, UNITED KINGDOM: Packt Publishing, Limited, 2012.

[11] S. U. Uygur, Penetration Testing with BackBox. Birmingham, UK: Packt Publishing, 2014.

[12] T. Wilhelm, Professional Penetration Testing : Creating and Learning in a Hacking Lab. Burlington: Syngress, 2013.

Διαδίκτυο:-

[13] RedTeamSecure, (n.d.). “Network Penetration Testing”. Retrieve February 20, 2019, from https://www.redteamsecure.com/network-penetration-testing/

[14] S. Yegulalp, (2017). “Start with Scratch: Learn Linux by rolling your own distro,” InfoWorld.com, 2017. Retrieve February 18, 2019, from

https://www.infoworld.com/article/3174523/start-with-scratch-learn-linux-by-rolling-your-own-distro.html

[15] CyperX. (n.d.). Seven Penetration Testing Phases to Achieve Amazing Results. Retrieve January 18, 2019, from https://cyberx.tech/penetration-testing-phases/

[16] GlobalSing. (2017). Six Reasons You Need to Invest in Penetration Testing. Retrieve November 27, 2018, from https://www.globalsign.com/en/blog/six-reasons-to-invest-in-penetration-testing/

[17] Hacken Hub. (n.d.). How much does Penetration Test Cost, or Price of your Security. Retrieved November 18, 2018, from https://hub.hacken.io/blog/how-much-does-penetration-test-cost-or-price-of-your-security

[18] Hudson. (n.d.). Ethical Hacler or Penetration Tester: What's the difference?.Retrieve November 27, 2018, from https://www.hudsoncourses.com/ethical-hacker-vs-penetration-tester/

[19] INFOSEC. (2018). Top 10 Linux Distro for Ethical Hacing and Penetration Testing. Retrieve Januaty 20, 2019, from https://resources.infosecinstitute.com/top-10-linux-distro-ethical-hacking-penetration-testing/#gref

[20] INFOSEC. (n.d). Process: Scanning and Enumeration. Retrieve Januaty 20, 2019, from https://resources.infosecinstitute.com/process-scanning-and-enumeration/#gref

[21] Nopsec. (2017). The True Cost of A Great Penetration Test. Retrieved November 20, 2018, from https://www.nopsec.com/blog/true-cost-great-penetration-test/

[22] Securitytrails.(2018). Cybersecurity Red Team Versus Blue Team — Main Differences Explained. Retrieve January 15, 2019, from https://securitytrails.com/blog/cybersecurity-red-blue-team

[23] SoftwareTestingHelp. (2019). Penetration Testing – Complete Guide with Sample Test Cases. Retrieve November 25, 2018, from https://www.softwaretestinghelp.com/penetration-testing-guide/

[24] SoftwareTestingHelp.(2019). Powerful Penetration Testing Tools in 2019 (Security Testing Tools). Retrieve January 12, 2019, from https://www.softwaretestinghelp.com/penetration-testing-tools/

[25] Sternstein, J. (n.d.). Local Network Attacks: LLMNR and NBT-NS Poisoning. Retrieve January 15, 2019, from

https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning

[26] Tamjim, M. (2019). Best Linux Distributions for Hacking and Penetration Testing. Retrieve January 10, 2019, from https://itsfoss.com/linux-hacking-penetration-testing/

[27] Trinaka, J. (2018). Five Pentesting Tools and Techniques (That Every Sysadmin Should Know). Retrieve November 21, 2018, from https://medium.com/@jeremy.trinka/five-pentesting-tools-and-techniques-that-sysadmins-should-know-about-4ceca1488bff

[28] Walker. J. (2017). Why your small business needs penetration testing. Retrieve November 25, 2018, from https://www.monitis.com/blog/why-your-small-business-needs-penetration-testing/

[29] Williams, A. (2018). Best Linux distros. Retrieve February 2, 2019, from https://www.techradar.com/news/best-linux-distro

Άρθρα:-

[30] Buczak, Anna L., Paul A. Hanke, George J. Cancro, Michael K. Toma, Lanier A. Watkins, and Jeffrey S. Chavis. "Detection of Tunnels in PCAP Data by Random Forests." In Proceedings of the 11th Annual Cyber and Information Security Research Conference, 16:1–16:4. CISRC '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2897795.2897804.

[31] Ceccato, Mariano, and Riccardo Scandariato. "Static Analysis and Penetration Testing from the Perspective of Maintenance Teams." In Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, 25:1–25:6. ESEM '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2961111.2962611.

[32] Chung, Sam, Sky Moon, and Barbara Endicott-Popovsky. "Architecture-Driven Penetration Testing Against an Identity Access Management (IAM) System." In Proceedings of the 5th Annual Conference on Research in Information Technology, 13–18. RIIT '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2978178.2978183.

[33] Cunha, Sarah, Whitney Winders, Dale C. Rowe, and Cara Cornel. "The Untrustables: How Underclassmen Evolved Our Approach to Student Red-Teaming." In Proceedings of the 17th Annual Conference on Information Technology Education, 26–30. SIGITE '16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/2978192.2978213.

[34] Epling, Lee, Brandon Hinkel, and Yi Hu. “Penetration Testing in a Box.” In Proceedings of the 2015 Information Security Curriculum Development Conference, 6:1–6:4. InfoSec ’15. New York, NY, USA: ACM, 2015. https://doi.org/10.1145/2885990.2885996.

[35] Falah, Ahmed, Lei Pan, and Mohamed Abdelrazek. “Visual Representation of Penetration Testing Actions and Skills in a Technical Tree Model.” In Proceedings of the Australasian Computer Science Week Multiconference, 8:1–8:10. ACSW ’17. New York, NY, USA: ACM, 2017. https://doi.org/10.1145/3014812.3014820.

[36] Guarda, Teresa, Walter Orozco, Maria Fernanda Augusto, Giovanna Morillo, Silvia Arévalo Navarrete, and Filipe Mota Pinto. “Penetration Testing on Virtual Environments.” In Proceedings of the 4th International Conference on Information and Network Security, 9–12. ICINS ’16. New York, NY, USA: ACM, 2016. https://doi.org/10.1145/3026724.3026728.

[37] Hussain, Muhammad Zunnurain, Muhammad Zulkifl Hasan, and Muhammad Taimoor Aamer Chughtai. “Penetration Testing In System Administration” , International Journal of Scientific & Technology Research, Vol 06, Iss 06, Pp 275-278 (2017), no. 06, p. 275, 2017

[38] Küçüksille, Ecir Uğur, Mehmet Ali Yalçınkaya, and Samet Ganal. “Developing a Penetration Test Methodology in Ensuring Router Security and Testing It in a Virtual Laboratory.” In Proceedings of the 8th International Conference on Security of Information and Networks, 189–195. SIN ’15. New York, NY, USA: ACM, 2015. https://doi.org/10.1145/2799979.2799989.

[39] Li, Richard, Dallin Abendroth, Xing Lin, Yuankai Guo, Hyun-Wook Baek, Eric Eide, Robert Ricci, and Jacobus Van der Merwe. “Potassium: Penetration Testing As a Service.” In Proceedings of the Sixth ACM Symposium on Cloud Computing, 30–42. SoCC ’15. New York, NY, USA: ACM, 2015. https://doi.org/10.1145/2806777.2806935.

[40] Shebli, H. M. Z. A., and B. D. Beheshti. “A Study on Penetration Testing Process and Tools.” In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 1–7, 2018. https://doi.org/10.1109/LISAT.2018.8378035.

[41] Singh, Sankalp, James Lyons, and David M. Nicol. “Fast Model-Based Penetration Testing.” In Proceedings of the 36th Conference on Winter Simulation, 309–317. WSC ’04. Winter Simulation Conference, 2004. http://dl.acm.org/citation.cfm?id=1161734.1161797.

[42] Stepanova, Taiana, Alexander Pechenkin, and Daria Lavrova. “Ontology-Based Big Data Approach to Automated Penetration Testing of Large-Scale Heterogeneous Systems.” In Proceedings of the 8th International Conference on Security of Information and Networks, 142–149. SIN ’15. New York, NY, USA: ACM, 2015. https://doi.org/10.1145/2799979.2799995.

[43] Wang, Yan, Chao Zhang, Xiaobo Xiang, Zixuan Zhao, Wenjie Li, Xiaorui Gong, Bingchang Liu, Kaixiang Chen, and Wei Zou. “Revery: From Proof-of-Concept to Exploitable.” In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 1914–1927. CCS ’18. New York, NY, USA: ACM, 2018. https://doi.org/10.1145/3243734.3243847.

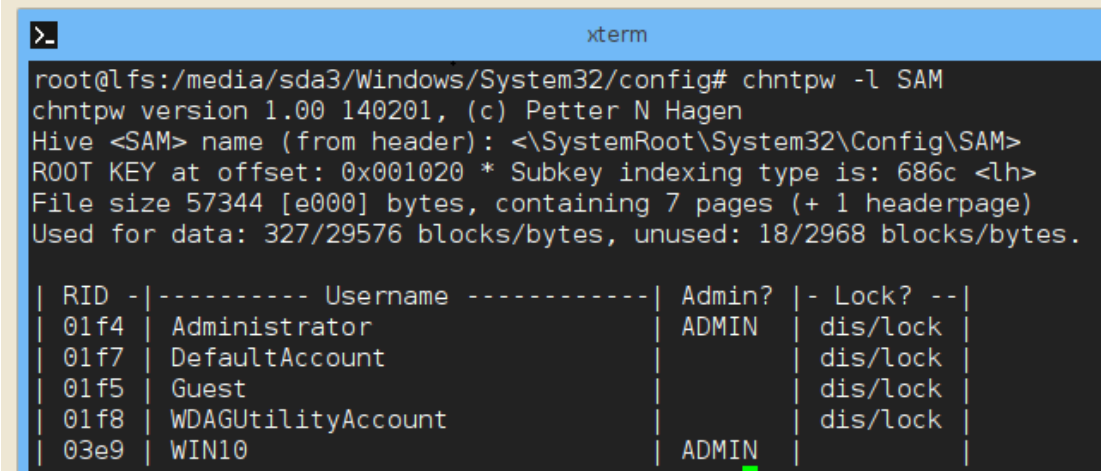
Παράρτημα Α
Διανομή LFS

Α1. Επεξηγηματικός πίνακας αρχείων ρίζας LFS

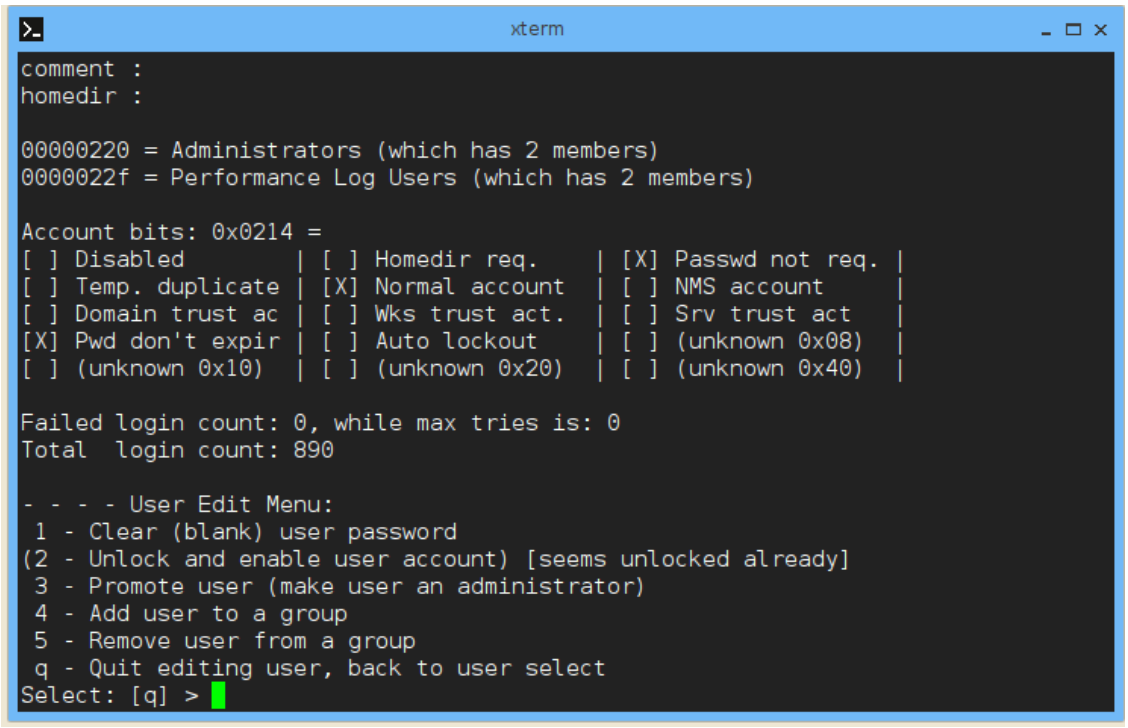
/	Είναι γνωστό ως "root" . Είναι η αρχή της δομής του συστήματος αρχείων Linux. Κάθε διαδρομή αρχείου στο Linux αρχίζει από τη ρίζα.
/ bin	Εδώ βρίσκονται τα περισσότερα από τα δυαδικά αρχεία του συστήματος, συνήθως για τις εντολές τερματικού Linux και βοηθητικά προγράμματα πυρήνα.
/ dev	Εδώ βρίσκονται οι φυσικές συσκευές: σκληροί δίσκοι, μονάδες USB, μονάδες οπτικών δίσκων. Τυπικά, ο σκληρός δίσκος του συστήματός, βρίσκεται στο / dev / sda, ενώ ο δίσκος USB στο / dev / sde.
/ etc	Εδώ αποθηκεύονται τα αρχεία ρυθμίσεων. Οι ρυθμίσεις στο / etc επηρεάζουν όλους τους χρήστες του συστήματος. Οι χρήστες που αποθηκεύουν τα αρχεία ρυθμίσεων κάτω από τους δικούς τους φακέλους, επηρεάζουν μόνο τους συγκεκριμένους χρήστες.
/ home	Εδώ διατηρούνται όλα τα προσωπικά αρχεία: φάκελοι Επιφάνεια εργασίας, Έγγραφα, Λήψεις, Φωτογραφίες και Βίντεο αποθηκεύονται.

/ lib (lib64)	Εδώ αποθηκεύονται οι βιβλιοθήκες. Πολλές φορές κατά την εγκατάσταση πακέτων λογισμικού Linux, οι βιβλιοθήκες μεταφορτώνονται αυτόματα να ξεκινούν με lib-*. Αυτά είναι αρχεία που χρειάζονται για να λειτουργούν τα προγράμματα στο Linux.
/ media	Χώρος όπου μπορούν να τοποθετηθούν οι εξωτερικές συσκευές, CD, USB κλπ
/ mnt	είναι ένας φάκελος που διατηρεί την θέση για την τοποθέτηση άλλων φακέλων ή μονάδων δίσκου. Χρησιμοποιείται ως σημείο αναφοράς για τις διάφορες συσκευές.
/ opt	Προαιρετικό λογισμικό για το σύστημά, δεν χρησιμοποιείται ιδιαίτερα.
/ proc	Ο φάκελος " processes " όπου πολλές πληροφορίες συστήματος φαίνονται ως αρχεία. Αποτελεί το τρόπο όπου ο πυρήνα του λειτουργικού συστήματος στέλνει και λαμβάνει πληροφορίες από διάφορες διεργασίες που εκτελούνται στο περιβάλλον του Linux.
/ root	Είναι ίδιο με το φάκελο / home για τον χρήστη root.
/ sbin	είναι παρόμοιο με το / bin, . Αναφέρεται σε συγκεκριμένες εντολές που μπορούν να εκτελεστούν μόνο από τον χρήστη root ή τον superuser.
/ tmp	Εδώ αποθηκεύονται τα προσωρινά αρχεία που συνήθως διαγράφονται μετά το κλείσιμο.
/ usr	Περιέχει αρχεία και βοηθητικά προγράμματα τα οποία μοιράζονται μεταξύ τους οι χρήστες.
/ var	χώρος όπου διατηρούνται τα μεταβλητά δεδομένα, συνήθως αρχεία καταγραφής του συστήματος. Μπορούν επίσης να περιλαμβάνονται και άλλοι τύποι δεδομένων.

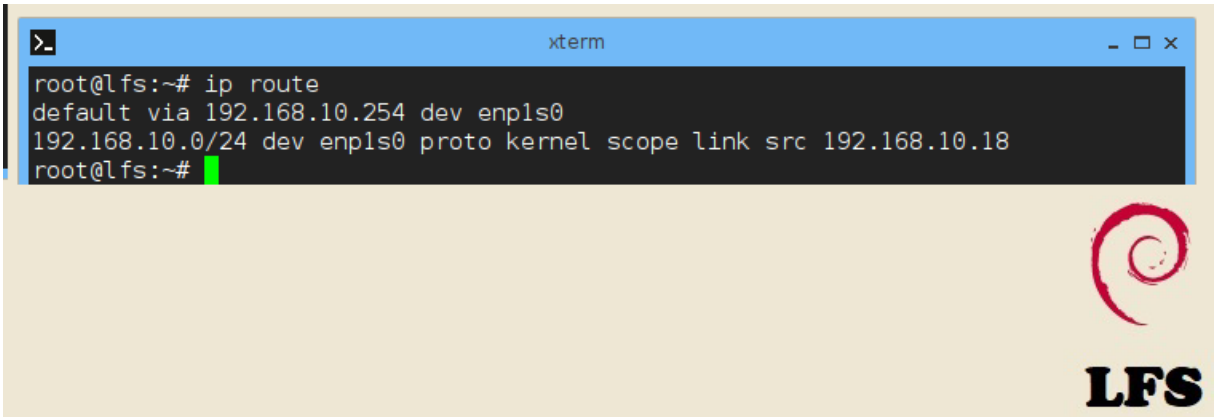
A.2 Εργαλεία δοκιμών διείσδυσης



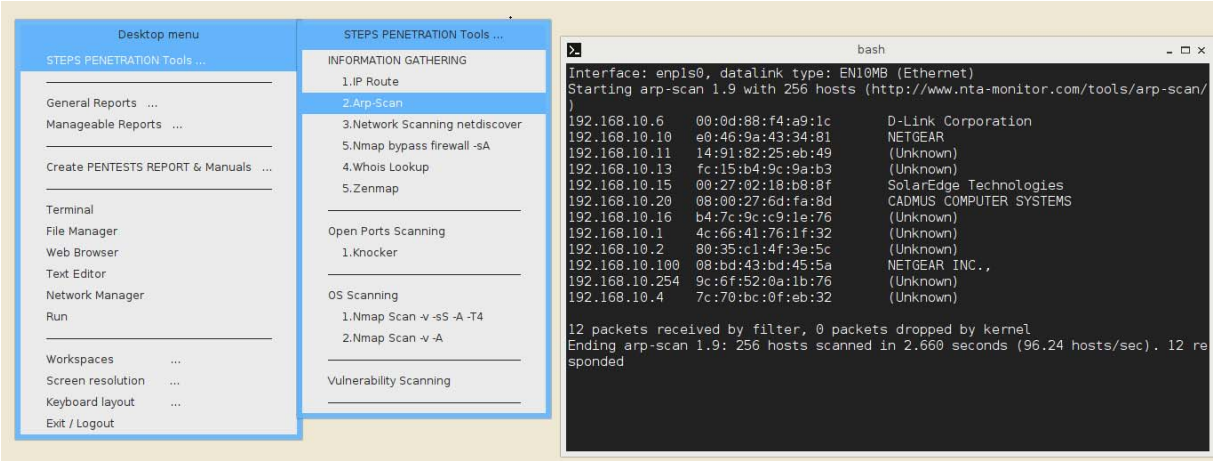
Σχήμα Α2-1α: Εργαλείο chntpw (Windows User Account cracking)



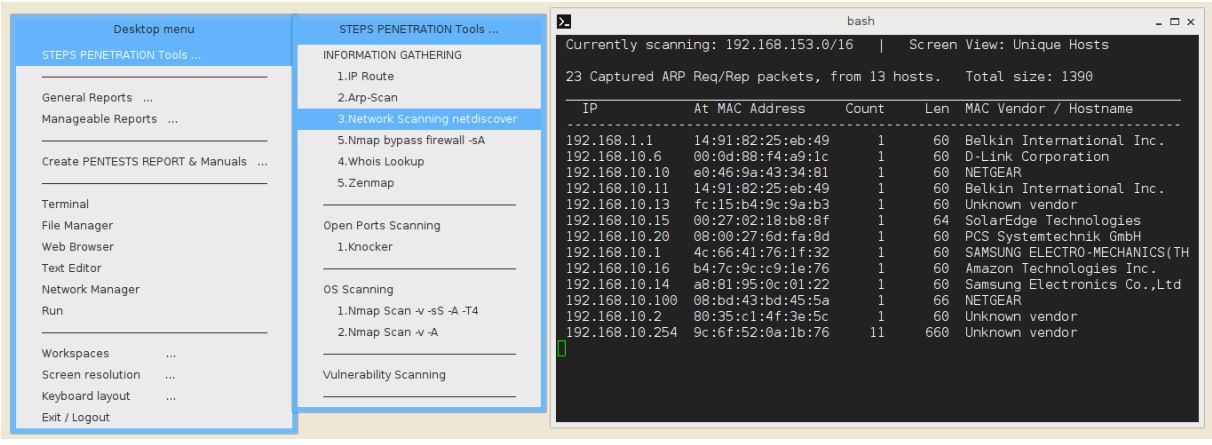
Σχήμα Α2-1β: Λειτουργίες εργαλείου chntpw (Windows User Account cracking)



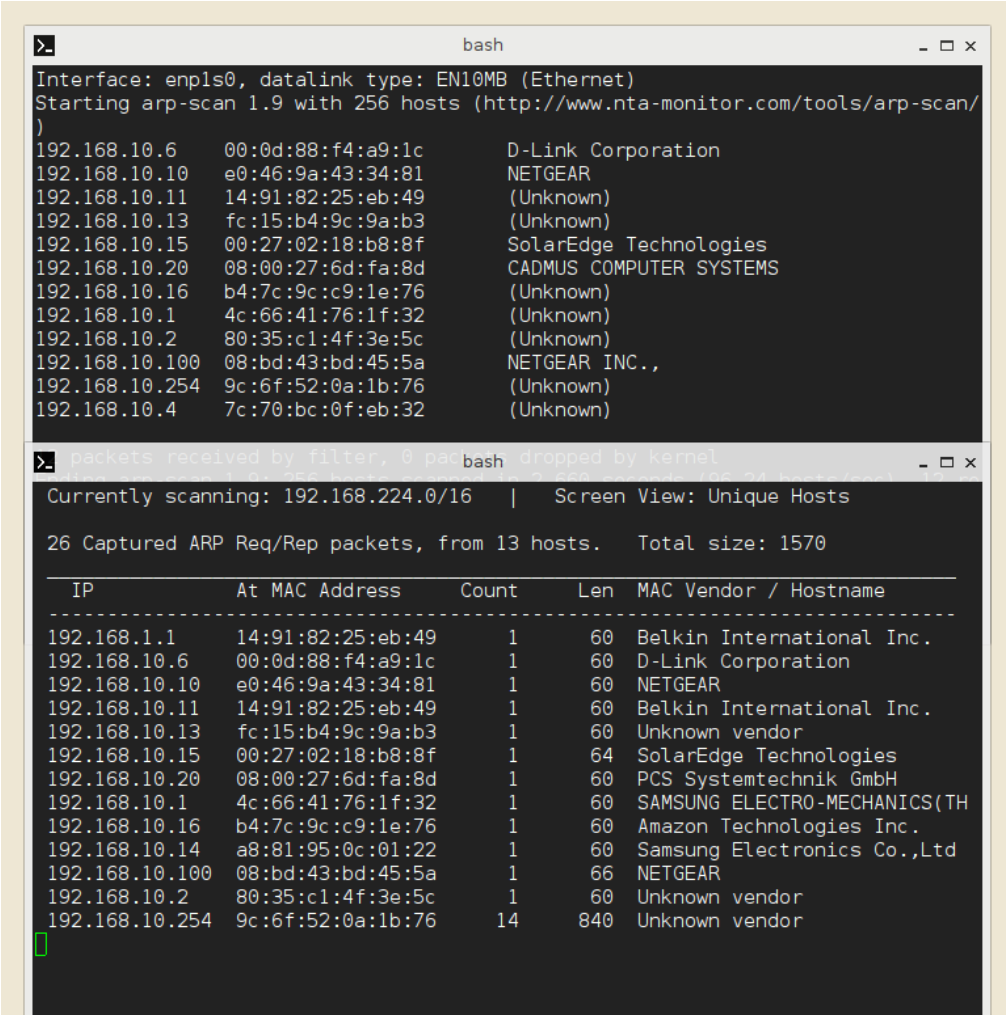
Σχήμα Α2-2: Εργαλείο Iproute ((Information Gathering)



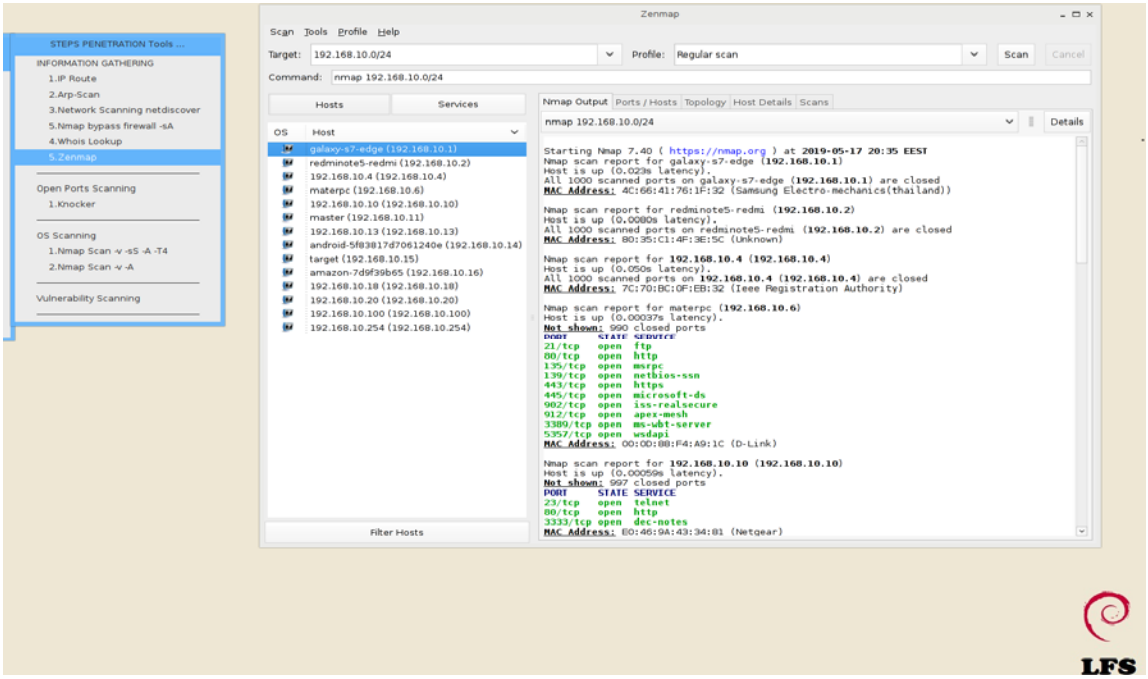
Σχήμα Α2-3: Εργαλείο Arp-Scan (Information Gathering)



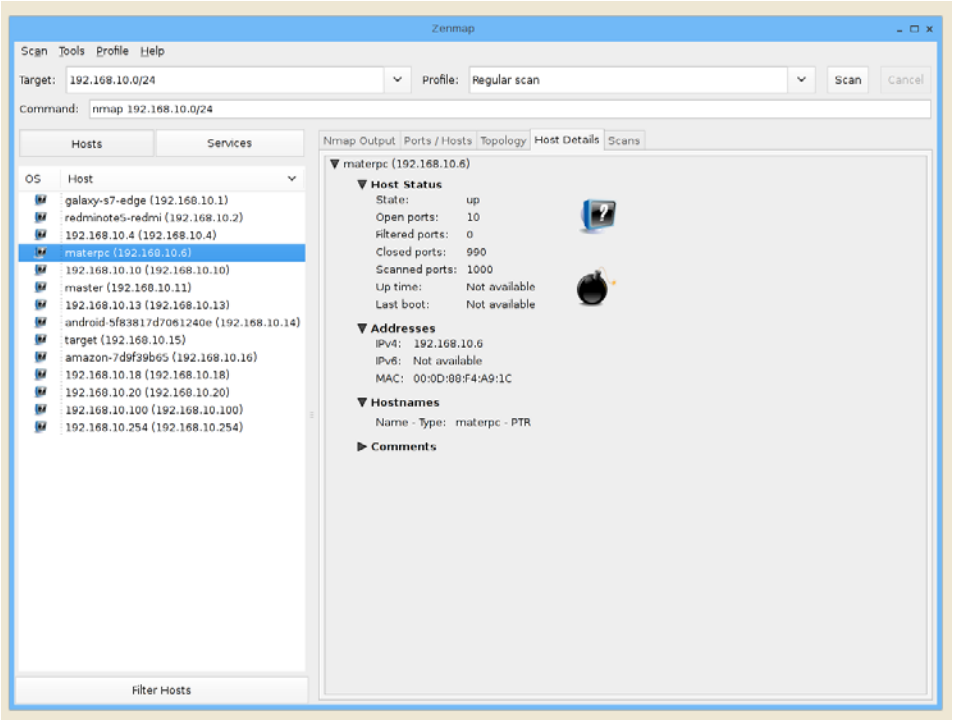
Σχήμα Α2-4: Εργαλείο Netdiscover (Information Gathering)



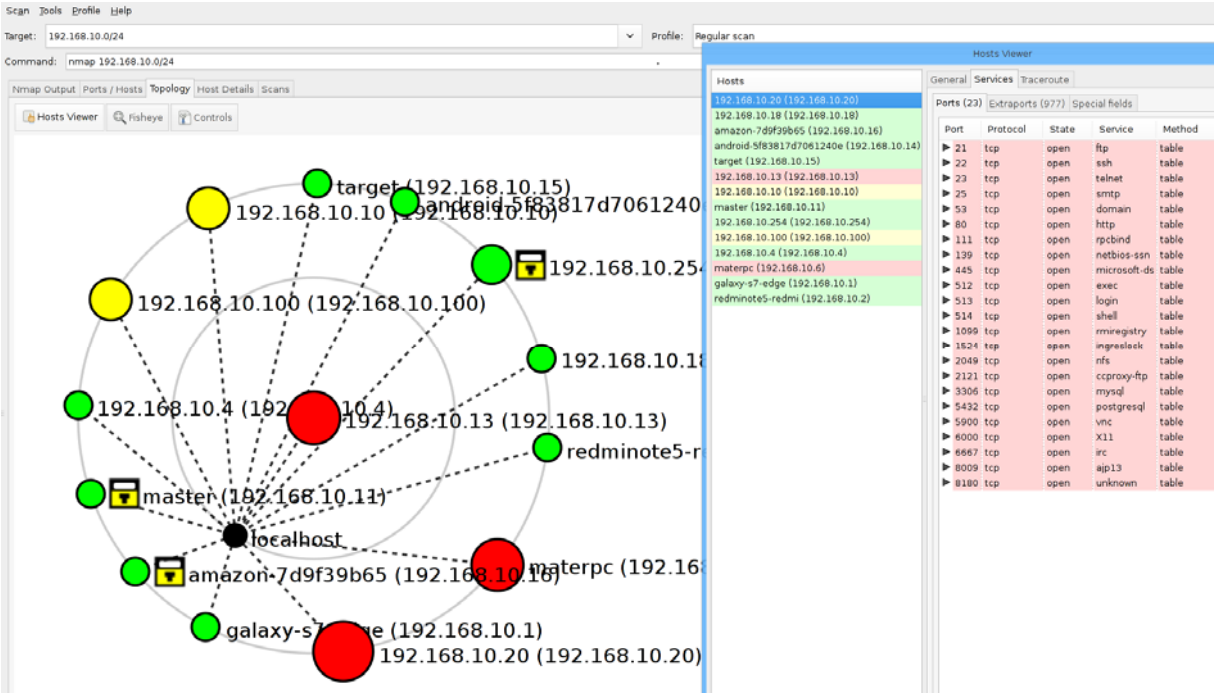
Σχήμα A2-5: Σύγκριση εργαλείου Arp-Scan Netdiscover (Information Gathering)



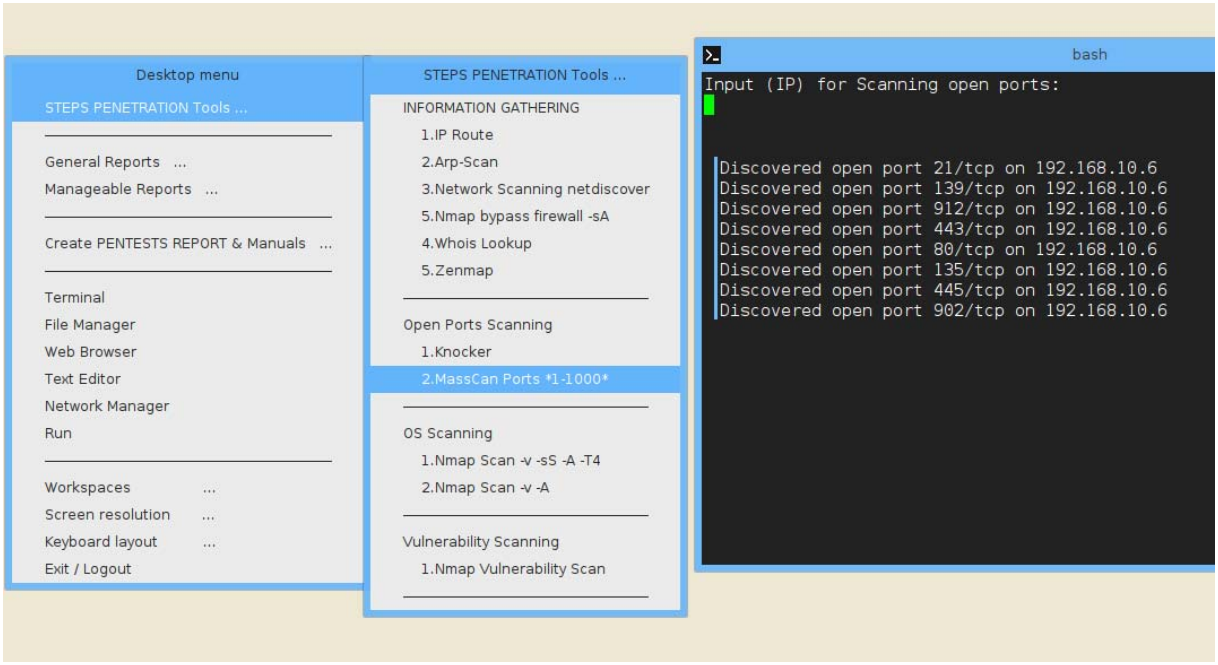
Σχήμα A2-6: Γραφικό εργαλείου Zenmap (Information Gathering)



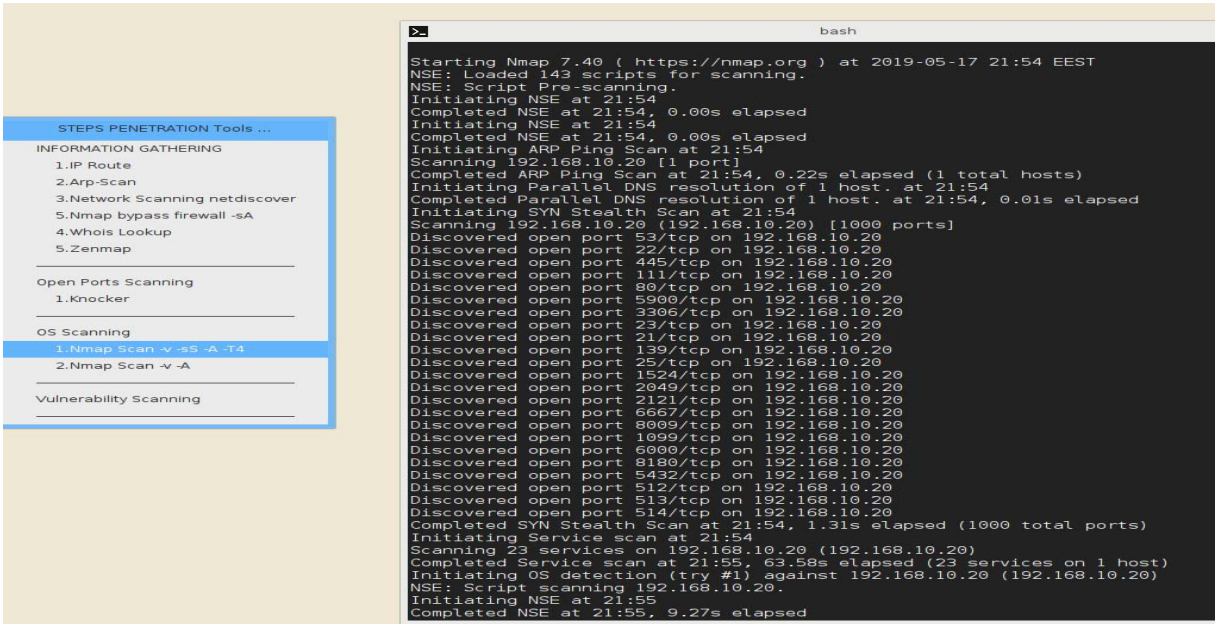
Σχήμα Α2-7: Σύστημα με ευπάθεια σε γραφικό εργαλείου Zenmap (Information Gathering)



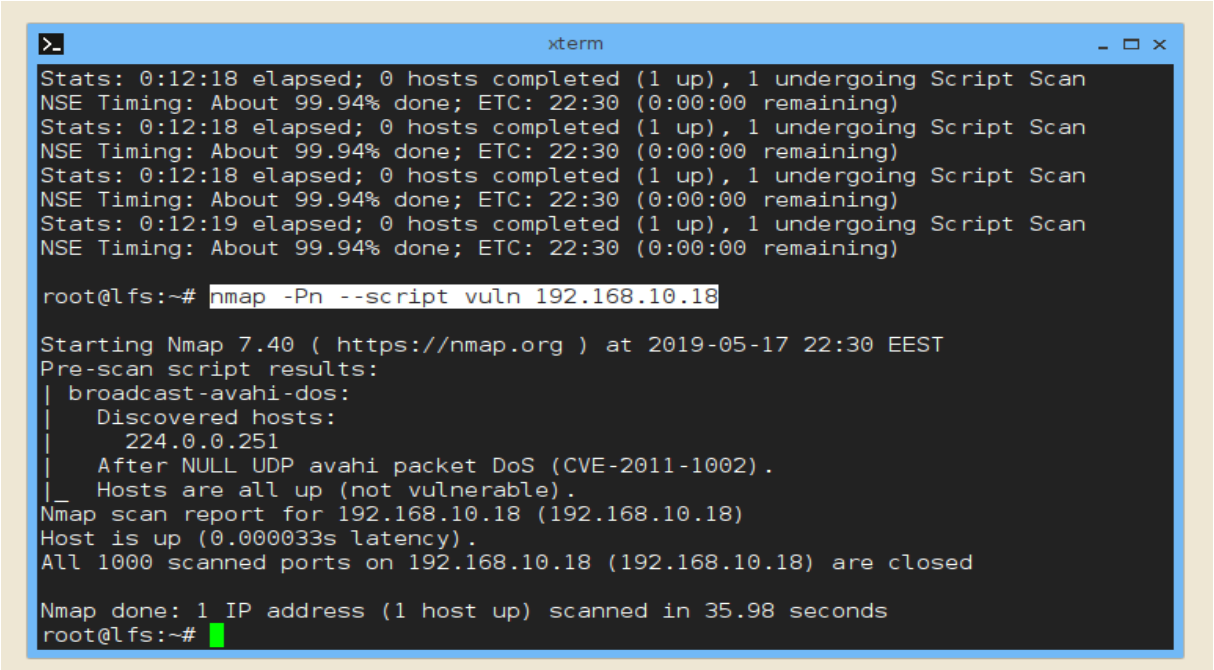
Σχήμα Α2-8: Γραφική απεικόνιση συστημάτων με ευπάθεια στο Zenmap (Information Gathering)



Σχήμα A2-9: Σάρωση με εργαλείο Masscan για ανοικτές θύρες από 1-1000(Port Scanning)



Σχήμα A2-10: Σάρωση για ανεύρεση λειτουργικών συστημάτων (OS Scanning)



Σχήμα Α2-11: Σάρωση για ανεύρεση συστημάτων με ευπάθειες (Vulnerability Scanning)

Παράρτημα Β
Σημαντικά εργαλεία και σενάρια δοκιμών διείσδυσης

Β.1 Σημαντικά εργαλεία δοκιμών διείσδυσης. [24]

Acunetix:	Είναι ένας πλήρως αυτοματοποιημένος σαρωτής ευπάθειας ιστού ο οποίος ανιχνεύει και αναφέρει πάνω από 4500 ευπάθειες εφαρμογών ιστού. Υποστηρίζει πλήρως HTML5, JavaScript και συστήματα CMS.
Aircrack-ng:	Συλλαμβάνει πακέτα δεδομένων που περιλαμβάνουν κωδικούς για ασύρματα δίκτυα
Arachni:	Βοηθά στην ανάλυση της ασφάλειας εφαρμογών στο διαδίκτυο.
Armitage:	Είναι το γραφικό προσωπείο του Metasploit Framework
Arping:	Είναι ένα βοηθητικό πρόγραμμα που στέλνει αιτήσεις ARP, σε κεντρικούς υπολογιστές σε ένα συγκεκριμένο υποδίκτυο
Arp-scan:	Είναι ένα εργαλείο γραμμής εντολών, που έχει σχεδιαστεί για την ανακάλυψη συστημάτων και fingerprinting. Συγκεντρώνει και στέλνει αιτήσεις ARP σε συγκεκριμένες διευθύνσεις IP, εμφανίζοντας τις απαντήσεις που λήφθηκαν.
Automater:	Είναι ένα αυτοματοποιημένο εργαλείο ανάλυσης εισβολής που βασίζεται σε διεύθυνση URL, διεύθυνση IP ή hash.

BeEF:	The Browser Exploitation Framework: Είναι εάν εργαλείο δοκιμών διείσδυσης που εστιάζει στις αδυναμίες και τα ρήγματα των φυλλομετριτών.
Burpsuite Burp suite:	Είναι ένας ουσιαστικός σαρωτής ανεύρεσης ευπαθειών. Αρκετοί ειδικοί σε θέματα ασφαλείας, αναφέρουν ότι είναι αδιανόητη η ολοκλήρωση της διαδικασίας δοκιμών διείσδυσης χωρίς τη χρήση αυτού του εργαλείου.
Cain & Abel:	Χρησιμοποιείται για κρυπτογραφημένους κωδικούς πρόσβασης ή κλειδιά δικτύου.
Core Impact:	Από τα παλαιότερα εργαλεία στην αγορά. Αποτελεί τη μεγαλύτερη γκάμα εκμεταλλεύσεων (exploits) που διατίθενται στην αγορά. Αυτοματοποιούν πολλές διαδικασίες με οδηγούς, έχουν πλήρη διαδρομή ελέγχου, συμπεριλαμβανομένων των εντολών PowerShell, και μπορούν να δοκιμάσουν εκ νέου έναν πελάτη απλώς επαναλαμβάνοντας το ίχνος ελέγχου
Cvechecker:	Δημιουργεί μια αναφορά σχετικά με πιθανές ευπάθειες στο σύστημά στόχο, συγκρίνοντας το αποτέλεσμα με τις πληροφορίες στη βάση δεδομένων του κοινού περιβάλλοντος ευπάθειας (CVE).
Dradis:	Είναι μια εφαρμογή στο διαδίκτυο ανοικτού κώδικα που βοηθά στη διατήρηση των πληροφοριών που μοιράζονται μεταξύ τους όσοι συμμετέχουν στην δοκιμή διείσδυσης ενός συγκεκριμένου οργανισμού.
Ettercap:	Είναι ένα εργαλείο ασφάλειας δικτύων για επιθέσεις Man-In-The-Middle
Fimap:	Είναι ένα εργαλείο ελέγχου εφαρμογών ιστού, για σφάλματα σε ενσωματωμένα αρχεία
HconSTF:	Εργαλείο που επιτρέπει την δημιουργία κώδικα επίθεσης στο διαδίκτυο για εκμετάλλευση ευπαθειών, σε τομείς όπως είναι η υποκλοπή κωδικών πρόσβασης, των βάσεων δεδομένων, του δικτύου κ.λπ.
IBM AppScan:	Είναι ένας σαρωτής που αναγνωρίζει προβληματικούς τομείς και προτείνει διορθωτικές ενέργειες.
Iodine:	Πρόκειται για μια δωρεάν εφαρμογή για προώθηση των δεδομένων IPv4, μέσω διακομιστών DNS
IronWASP:	Αποτελεί σαρωτή για εφαρμογές ιστού που χρησιμοποιεί κώδικα python ή ruby.
John the Ripper:	Θεωρείται ως ένα από τα ταχύτερα εργαλεία αποκωδικοποίησης κωδικών πρόσβασης.
Knock:	Είναι ένα script Python που έχει σχεδιαστεί για να απαριθμεί υποτομείς σε έναν τομέα-στόχο μέσω μιας λίστας λέξεων.
Maltego:	Εργαλείο που εστιάζει στην προβολή των σχέσεων μεταξύ ανθρώπων, ιστότοπων, υποδομών κλπ. Στόχος του ο εντοπισμός ευπαθειών και λανθασμένων συνδέσεων.
Metasploit:	Είναι το πιο προηγμένο και το πιο δημοφιλές εργαλείο, για δοκιμές διείσδυσης. Βασίζεται, σε μεθόδους εκμετέλευσης, που έχουν την δυνατότητα να ξεπερνούν τα μέτρα ασφαλείας και να εισέρχονται σε συστήματα. Αφού καταφέρουν να εισέλθουν σε αυτά εκτελούν συγκεκριμένους κώδικες που τρέχουν εργασίες σε μηχανές στόχους (payloads).

MSF:	Είναι ένα χρήσιμο εργαλείο ελέγχου που περιέχει πολλές εκμεταλλεύσεις (exploits) και περιβάλλον ανάπτυξης με δυνατότητα τροποποίησης ή δημιουργίας
Nagios:	Λογισμικό, για παρακολούθηση ολόκληρης της δικτυακής δομής, συμπεριλαμβανομένων των διακομιστών, των εφαρμογών. Προειδοποιεί, όταν εντοπίσει πιθανό πρόβλημα.
Nessus:	Είναι ένα από τα πιο ισχυρά εργαλεία ταυτοποίησης ευπάθειας. Ειδικεύεται σε ελέγχους συμμόρφωσης, αναζήτηση σε ευαίσθητα δεδομένων, σάρωση διευθύνσεων IP, σάρωση ιστότοπων κ.λπ. και βοηθά στην εξεύρεση των «αδύναμων σημείων».
Netsparker:	Είναι ένας αυτοματοποιημένος σαρωτής που ανιχνεύει και εντοπίζει τρωτά σημεία πληροφοριακά συστήματα. Εντοπίζει τις ευπάθειες που αποδεικνύονται ως πραγματικές αποφεύγοντας ψεύτικες ενδείξεις.
Nikto:	Είναι ένας διακομιστής σάρωσης ιστού ο οποίος εξετάζει επικίνδυνα αρχεία CGI και παλιά λογισμικά διακομιστών
Nmap:	"Network Mapper": Βοηθά κατά κύριο λόγο στην κατανόηση των χαρακτηριστικών κάθε δικτύου-στόχου.
OpenVAS:	Πρόγραμμα που αποτελείται από πολλές υπηρεσίες και εργαλεία για την παροχή ολοκληρωμένης, διαχείρισης σάρωσης για τρωτά σημεία.
Ptunnel:	Είναι εφαρμογή που επιτρέπει την προώθηση συνδέσεων TCP, σε έναν απομακρυσμένο κεντρικό υπολογιστή που χρησιμοποιεί πακέτα αιτημάτων και απάντησης (icmp echo_request)
Recon-ng:	Πρόκειται για ένα πλήρως εξοπλισμένο πλαίσιο Αναγνώρισης Ιστού
Retina:	Αποτελεί ένα εργαλείο διαχείρισης ευπάθειας που στοχεύει σε ολόκληρο το περιβάλλον του δικτύου που εξετάζει.
RIPS:	Είναι ένας στατικός αναλυτής πηγαίου κώδικα, για ευπάθειες σε εφαρμογές ιστού PHP.
Secunia PSI:	Είναι ένα λογισμικό επιθεώρησης που αφού εγκατασταθεί, κρατά ένα σύστημα ασφαλή κατάσταση.
Skipfish:	Είναι ένα ενεργό εργαλείο αναγνώρισης ασφάλειας εφαρμογών ιστού. Προετοιμάζει ένα διαδραστικό χάρτη ιστότοπου τοποθετώντας ανιχνευτές
Social Engineer Toolkit (SET):	Το εργαλείο κοινωνικής μηχανικής, είναι ένα μοναδικό στο είδος του εργαλείο, αφού οι επιθέσεις στοχεύουν στο ανθρώπινο παράγοντα αντί σε αυτοματοποιημένα συστήματα. Επιτρέπει την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, applets Java, κλπ τα οποία περιέχουν κώδικες επίθεσης.
Sqlmap:	Είναι ένα καλό εργαλείο δοκιμών διείσδυσης ανοιχτού κώδικα. Αυτό το εργαλείο χρησιμοποιείται κυρίως για την ανίχνευση και την αξιοποίηση των SQL injection σε εφαρμογές και βάσεις δεδομένων.
Sqlninja:	Χρησιμοποιείται για διείσδυση σε διακομιστές βάσεων δεδομένων μέσω SQL injection.
W3af:	Είναι ένα πρόγραμμα επίθεσης σε εφαρμογές ιστού και ελέγχου.
WebScarabNG:	Χρησιμοποιείται για τα request HTTP / https μεταξύ του προγράμματος περιήγησης και του διακομιστή, κατά τρόπο ώστε να κατανοήσει, να καταγράψει και μερικές φορές να

	τροποποιήσει τις παραμέτρους που αποτελούν μέρος της επικοινωνίας μεταξύ των δύο μερών
Weevely:	Πρόκειται για ένα κρυφό web php shell, που μιμείται μια σύνδεση τύπου telnet
Wireshark:	Είναι ένα από τα διασημότερα προγράμματα, ανάλυσης δικτύων στον κόσμο. Το εργαλείο αυτό παρέχει πληροφορίες για το δίκτυο και τα διάφορα πρωτοκόλλα σχετικά με τα δεδομένα που διακινούνται σ' αυτό. Για την συλλογή και την ανάλυση των πακέτων χρησιμοποιεί τη δικτυακή βιβλιοθήκη pcap.
ZAP:	Πρόκειται για μια εφαρμογή για εντοπισμό ευπάθειας για εφαρμογές ιστού (Zed Attack Proxy από το OWASP).
Zenmap:	Είναι το επίσημο GUI του Nmap.

Β.2 Σενάρια δοκιμών διείσδυσης.

1. Έλεγχος κατά πόσο η εφαρμογή Ιστού είναι σε θέση να εντοπίσει τις επιθέσεις spam στις φόρμες επικοινωνίας που χρησιμοποιούνται στον ιστότοπο.
2. Σε δίκτυα όπου υπάρχει διακομιστής μεσολάβησης (Proxy Server) πρέπει να γίνεται έλεγχος, εάν η κίνηση του δικτύου παρακολουθείται από συσκευές μεσολάβησης. Είναι γεγονός ότι ένας διακομιστής μεσολάβησης, δυσκολεύει τους εισβολείς να αποκτήσουν εσωτερικές λεπτομέρειες ενός δικτύου, προστατεύοντας έτσι το σύστημα από εξωτερικές επιθέσεις.
3. Όπου εφαρμόζονται φίλτρα, ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας πρέπει να γίνεται επαλήθευση εάν η εισερχόμενη και εξερχόμενη αλληλογραφία που κυκλοφορεί στο ηλεκτρονικού ταχυδρομείου είναι φιλτραρισμένη και τα μηνύματα που πιθανόν κακόβουλα επικολλιούνται σε αυτά, εμποδίζονται. Αρκετά λογισμικά ηλεκτρονικού ταχυδρομείου έρχονται με ενσωματωμένα φίλτρα ανεπιθύμητης αλληλογραφίας τα οποία ρυθμίζονται σύμφωνα με τις ανάγκες του καθενός. Αυτοί οι κανόνες ρύθμισης μπορούν να εφαρμόζονται στις κεφαλίδες ηλεκτρονικού ταχυδρομείου, στο θέμα ή στο κυρίως μέρος του μηνύματος.
4. Βεβαίωση ότι ολόκληρο το δίκτυο ή οι υπολογιστές προστατεύονται με το τείχος προστασίας. Το τείχος προστασίας μπορεί να είναι ένα λογισμικό ή μια μηχανή που εμποδίζει την μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Ένα τείχος προστασίας μπορεί να αποτρέψει την αποστολή δεδομένων εκτός δικτύου χωρίς την απαραίτητη άδεια.
5. Προσπάθεια εκμετάλλευσης όλων των διακομιστών, των υπολογιστών και των συστημάτων γραφείου, των εκτυπωτών καθώς και των συσκευών δικτύου.
6. Βεβαίωση, ότι όλα τα ονόματα χρηστών και οι κωδικοί πρόσβασης κρυπτογραφούνται και μεταφέρονται μέσω ασφαλούς σύνδεσης https.
7. Έλεγχος ότι οι πληροφορίες που αποθηκεύονται στα cookie του ιστότοπου δεν πρέπει να είναι σε αναγνώσιμη μορφή.
8. Εξέταση παλαιότερων ευρημάτων και έλεγχος ότι η διόρθωση λειτουργεί.
9. Βεβαίωση ότι δεν υπάρχει ανοιχτή θύρα στο δίκτυο.
10. Πιστοποίηση όλων των συσκευών τηλεφώνου.
11. Πιστοποίηση της ασφάλειας του ασύρματου δικτύου WIFI.

12. Πιστοποίηση των μεθόδων HTTP. Οι μέθοδοι «Put» και «Delete» δεν πρέπει να είναι ενεργοποιημένες σε ένα διακομιστή ιστού.
13. Βεβαίωση ότι οι κωδικοί πρόσβασης πληρούν τα απαιτούμενα πρότυπα. Ο κωδικός πρόσβασης πρέπει να έχει μήκος τουλάχιστον 8 χαρακτήρων και να περιέχει τουλάχιστον έναν αριθμό και έναν ειδικό χαρακτήρα.
14. Η σελίδα σύνδεσης της εφαρμογής πρέπει να κλειδώνεται μετά από μερικές ανεπιτυχείς προσπάθειες σύνδεσης.
15. Τα μηνύματα σφάλματος, πρέπει να είναι γενικά χωρίς να αναφέρουν συγκεκριμένες λεπτομέρειες όταν παρουσιάζεται σφάλμα, όπως "Μη έγκυρο όνομα χρήστη" ή "Μη έγκυρος κωδικός πρόσβασης".
16. Τα μηνύματα σφάλματος που έχουν προσαρμοστεί, ανάλογα με το σφάλμα, πρέπει να εμφανίζονται στον τελικό χρήστη σε περίπτωση που η ιστοσελίδα δεν είναι διαθέσιμη.
17. Στο μητρώο καταχωρήσεων, δεν πρέπει να τηρούνται ευαίσθητες πληροφορίες.
18. Όλα τα αρχεία πρέπει να σαρώνονται πριν μεταφορτωθούν στο διακομιστή.
19. Τα ευαίσθητα δεδομένα δεν πρέπει να διαβιβάζονται σε διευθύνσεις URL ενώ επικοινωνούν με διαφορετικές εσωτερικές ενότητες της εφαρμογής ιστού.
20. Πιστοποίηση ότι η λειτουργία επαναφοράς κωδικού πρόσβασης είναι ασφαλής.
21. Πιστοποίηση για αντιμετώπιση επίθεσης SQL Injection σε εφαρμογές.
22. Οι κρίσιμοι πόροι στο σύστημα πρέπει να είναι διαθέσιμοι μόνο σε εξουσιοδοτημένα άτομα και υπηρεσίες.
23. Όλα τα αρχεία καταγραφής πρόσβασης πρέπει να διατηρούνται με τα κατάλληλα δικαιώματα πρόσβασης.
24. Βεβαίωση ότι η περίοδος σύνδεσης χρήστη τελειώνει κατά την αποσύνδεση.
25. Πιστοποίηση ότι η περιήγηση είναι απενεργοποιημένη στο διακομιστή.
26. Βεβαίωση, ότι όλες οι εκδόσεις εφαρμογών και βάσεων δεδομένων είναι ενημερωμένες.
27. Έλεγχος των διευθύνσεων URL και βεβαίωση ότι οι εφαρμογές ιστού δεν εμφανίζουν ανεπιθύμητες πληροφορίες.
28. Έλεγχος για διαρροή μνήμης και την υπερχείλιση του buffer.
29. Πιστοποίηση ότι γίνεται σάρωση της εισερχόμενης κίνησης δικτύου για εντοπισμό επιθέσεων Trojan.
30. Βεβαίωση ότι το σύστημα είναι ασφαλές από Brute Force Attacks . Χρήση μεθόδων δοκιμής και σφάλματος για την εύρεση ευαίσθητων πληροφοριών, όπως κωδικών πρόσβασης.

31. Βεβαίωση ότι το σύστημα ή το δίκτυο είναι ασφαλές από επιθέσεις DoS. Ο επιτιθέμενος μπορεί να στοχεύσει σε δίκτυο ή ακόμα σε έναν μόνο υπολογιστή με συνεχείς αιτήσεις. Λόγω των πολλαπλών αιτήσεων οι πόροι στο σύστημα στόχου υπερφορτώνονται, με αποτέλεσμα την άρνηση παροχής υπηρεσίας για νόμιμες αιτήσεις.
32. Έλεγχος στις εφαρμογές για επιθέσεις σε κώδικα HTML.
33. Έλεγχος για επιθέσεις COM & ActiveX.
34. Έλεγχος για επιθέσεις πλαστογράφησης. Το Spoofing μπορεί να είναι πολλαπλών τύπων: πλαστογράφηση διεύθυνσης IP, ηλεκτρονικού ταχυδρομείου, ARP, του Referrer, έναντι της ταυτότητας αυτού που καλεί, δηλητηρίαση δικτύων κοινής χρήσης αρχείων και GPS.
35. Έλεγχος για ανεξέλεγκτη επίθεση string, επίθεση δηλαδή κατά της ασφαλείας, που μπορεί να προκαλέσει την κατάρρευση ή την εκτέλεση κακόβουλου κώδικα με ενέργειες.
36. Έλεγχος για επίθεση εισαγωγής XML η οποία χρησιμοποιείται για να αλλάξει την προγραμματισμένη λογική των εφαρμογών.
37. Πιστοποίηση ότι οι σελίδες σφαλμάτων δεν εμφανίζουν πληροφορίες που μπορούν να βοηθήσουν έναν εισβολέα να εισέλθει στο σύστημα.
38. Βεβαίωση ότι τα κρίσιμα δεδομένα όπως ο κωδικός πρόσβασης αποθηκεύονται σε μυστικά αρχεία στο σύστημα.
39. Βεβαίωση ότι η εφαρμογή δεν επιστρέφει περισσότερα δεδομένα από ό, τι απαιτείται.

Παράρτημα Γ
Ακρωνύμια

ARP	Address Resolution Protocol
DART	Digital Advanced Response Toolkit
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial-of-Service
DNS	Domain Name Server
DSS	Standard Card Security Data Security Standard
FHS	Filesystem Hierarchy Standard
GPU	Graphic processing Unit
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
LFS	Linux from Scratch
LLMNR	Link-Local Multicast Name Resolution
MITM	Man In The Middle
NAC	Network Access Control
NBT-NS	NetBIOS Name Service
OWASP	Open Web Application Security Project
PAC	Proxy Auto Configuration
PCAP	Packet Capture
PCI	Payment Card Industry
SAST	Static Application Security Testing
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
WPAD	Web Proxy Auto-Discovery