ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

Σχολή Τεχνολογίας

Τμήμα Ψηφιακών Συστημάτων

Ανίχνευση Ευπαθειών σε Ψηφιακά Συστήματα με τεχνικές Ethical Hacking

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ουστάς Αναστάσιος (ΑΜ: 3119263)

Ρεντζιλάς Νικόλαος (ΑΜ: 3119041)

Επιβλέπων: ***Απόστολος Ξενάκης, Επίκουρος Καθηγητής***

ΛΑΡΙΣΑ, Μάρτιος 2024

UNIVERSITY OF THESSALY

School of Technology

Digital Systems Department

Vulnerabilities Detection in Digital Systems with Ethical Hacking techniques

BACHELOR THESIS

Oustas Anastasios (RN: 3119263)

Rentzilas Nikolaos (RN: 3119041)

Supervisor: ***Apostolos Xenakis, Assistant Professor***

LARISSA, March 3 2024

Υπεύθυνη Δήλωση περί Ακαδημαϊκής Δεοντολογίας και Πνευματικών Δικαιωμάτων

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα πτυχιακή εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον, και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο Δηλών

Ονοματεπώνυμο Φοιτητή
ΟΥΣΤΑΣ ΑΝΑΣΤΑΣΙΟΣ
ΜΑΡΤΙΟΣ 2024

Ο Δηλών

Ονοματεπώνυμο Φοιτητή
ΡΕΝΤΖΙΛΑΣ ΝΙΚΟΛΑΟΣ
ΜΑΡΤΙΟΣ 2024

Εγκρίνεται από την Επιτροπή Εξέτασης:

Επιβλέπων/πουσα	**Ονοματεπώνυμο Επιβλέποντα** Βαθμίδα/ιδιότητα επιβλέποντα, Τμήμα Ψηφιακών Συστημάτων, Πανεπιστήμιο Θεσσαλίας
Μέλος	**Ονοματεπώνυμο Μέλους 1** Βαθμίδα/ιδιότητα μέλους 1, Τμήμα/Ίδρυμα μέλους 1
Μέλος	**Ονοματεπώνυμο Μέλους 2** Βαθμίδα/ιδιότητα μέλους 2, Τμήμα/Ίδρυμα μέλους 2

Ημερομηνία έγκρισης: dd-mm-yyyy

Περίληψη

Η παρούσα εργασία πραγματεύεται το <<ηθικό>> χακαρισμα ή οπως αναφέρεται στην αγγλική βιβλιογραφία Ethical Hacking.Στόχος της πτυχιάκης αυτής είναι η εξοικείωση και μελέτη του Ethical Hacking με την χρηση πολλών εργαλείων και τεχνικών μεσά απο την χρήση Εικονικών Εργαστηρίων.Εξετάζεται επίσης ο ορισμός του Hacking ως προς την ιστορία του και την σημασία του. Παρουσιάζονται και αναλύονται τα βασικά στάδια του χάκινγκ. Επιπλέον, διακρίνονται διάφορες μορφές χάκερ που υπάρχουν, ηλεκτρονικές επιθέσεις, καθως και τα εργαλεία που χρειάζονται για να γίνει μια σωστή αναπαράσταση χακινγκ. Η αναπαράσταση παραδειγμάτων που θα εξεταστεί θα γίνει απο την μεριά ενος Ethical Hacker και δίνεται έμφαση κυρίως στο ηθικό κομμάτι ενος Penetration testing.

Abstract

The following thesis deals with "moral" hacking known as Ethical Hacking. The aim of this thesis is to get familiar with and study Ethical Hacking using many tools and techniques throughout the use of Virtual Machines. The definition, background, and significance of the term "hacking" are also explored. It outlines and examines the fundamental stages of hacking. Additionally, it distinguishes between different types of hackers that are out there, cyberattacks, and the software tools needed to carry them out. Finally, utilizing some of these technologies, a Virtual Laboratory is developed to mimic potential assault situations. The scenarios analyzed are viewed through the lens of an ethical hacker, with a focus on adhering to the approved Penetration Testing Standard.

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε μέσα απο τα βάθη της καρδιάς μας τους συγγενείς μας για την συνεχή στηριξή τους μέχρι και την ολοκλήρωση των σπουδών μας, τους φίλους μας και τον καθηγητή μας Κο Απόστολο Ξενάκη, Επίκουρο Καθηγητή στα Ασύρματα Δίκτυα Αισθητήρων με Εφαρμογές στην Πρωτογενή Παραγωγή, για το ενδιαφέρον του και τη βοήθεια του στην ολοκλήρωση της πτυχιακής μας εργασίας.

Ρεντζιλάς Νικόλαος

Ουστάς Αναστάσιος

ημερομηνία

Περιεχόμενα

1 Εισαγωγή

1.1 Τι είναι το Hacking

Ο ορισμός του Hacking είναι η προσπάθεια εκμετάλλευσης ενός συστήματος υπολογιστή ή ενός ιδιωτικού δικτύου στο εσωτερικό ενός υπολογιστή. Με λιγα λόγια, είναι η μη εξουσιοδοτημένη πρόσβαση ή ο έλεγχος των συστημάτων ασφαλείας δικτύων υπολογιστών για κάποιο παράνομο σκοπό. Οι δραστηριότητες hacking μπορούν να περιλαμβάνουν την ανεπιθύμητη πρόσβαση σε προσωπικές πληροφορίες, την κλοπή δεδομένων, την προκάλυψη ζημιάς σε συστήματα, ή την παραβίαση της ιδιωτικότητας χρηστών.

Είναι αξιοσημειωτο να πουμε ότι το hacking μπορεί να είναι τόσο νόμιμο όσο και παράνομο, ανάλογα με τον σκοπό και την άδεια του χάκερ. Το ηθικο χακινγκ (ethical hacking), που γίνεται για νομικούς σκοπούς όπως η βελτίωση της κυβερνοασφάλειας, είναι νόμιμη και πρατκικά χρήσιμη στον τομέα της ασφάλειας των υπολογιστών. Αντίθετα, το μη εξουσιοδοτημένο hacking με κακόβουλες προδιαθέσεις είναι παράνομο και μπορεί να οδηγήθει σε σοβαρές κυρώσεις.

1.2.1 Ιστορική αναδρομή επιθέσεων

- 1960s - Phone Phreaking: Στην δεκαετία του 60, οι πρώτοι χακερς ήταν γνωστοί ως "phone phreaks". Χρησιμοποιούσαν σφυρίγματα και άλλες τεχνικές για να "παρακάμψουν" τα τηλεφωνικά δίκτυα και να κάνουν κλήσεις χωρίς χρέωση. Ο πιο γνωστός από αυτούς ήταν ο John Draper, γνωστός ως Captain Crunch.

- 1970s - Εμφάνιση των Προσωπικών Υπολογιστών: Με την εμφάνιση των πρώτων προσωπικών υπολογιστών, οι χακερς αρχισαν την ερευνα τους προς τα λειτουργικά συστήματα και το λογισμικό. Οι πρώτες ομάδες χακερ όπως οι

"Homebrew Computer Club", αντάλλασσαν πληροφορίες και τεχνικές.

- 1980s - Εμφάνιση των Ιών: Στην δεκαετια του 80, οι πρώτοι υπολογιστικοί ιοί άρχισαν να εμφανίζονται. Ο "Brain", ο πρώτος ιός για PCs, γεννηθηκε το 1986. Επίσης, οι χακερς άρχισαν να οργανωνουν ομάδες και να δημιουργούν πιο οργανωμένες κοινότητες.

- 1990s - Εποχή του Διαδικτύου: Με την ραγδαια αναπτυξη του Διαδικτύου, το χακινγκ έγινε πιο δημοφιλές. Οι επιθέσεις άρχισαν να γίνονται πιο συχνές και ορατές. Οι πρώτοι ιοί που εξαπλώνονται μέσω email, όπως ο "ILOVEYOU", προκάλεσαν τεράστιες ζημιές.

- 2000s - Η Εποχή των Διαρροών Δεδομένων: Κατά το ξεκινημα του 2000, μεγάλες εταιρείες όπως η Sony, η Target και η Home Depot ειχαν μεγάλες διαρροές δεδομένων. παραλληλα, οι κυβερνοεπιθέσεις έγιναν πιο πολύπλοκες, με τη χρήση τεχνικών όπως τα botnets.

- 2010s-και μετά - Κυβερνοεπιθέσεις και Ransomware: Οι επιθέσεις έγιναν πιο εξειδικευμένες. Οι hackers στόχευσαν σε κρίσιμες υποδομές, όπως ηλεκτρικές εταιρείες και νοσοκομεία. Το ransomware, όπως ο WannaCry και ο NotPetya, προκάλεσε τεράστιες ζημιές σε εταιρείες και οργανισμούς σε όλο τον κόσμο.

1.2.2 Οι πιο γνωστοί χακερ όλων των εποχών

- **Kevin Mitnick**: Ο Mitnick ισως ειναι και το συνώνυμο του Hacker. Το Υπουργείο Δικαιοσύνης της Αμερικής ακόμα αναφέρεται σε αυτόν χαρακτηρίζοντας τον ως «τον νούμερο ένα καταζητούμενο για ηλεκτρονικά εγκλήματα στην ιστορία της Αμερικής.». Ο Mitnick εκανε τα πρωτα του βηματα από το σύστημα καρτών λεωφορείων του Los Angeles όπου μπορούσε να εκτυπώνει κάρτες για δωρεάν κουρσες. Μετά από εκεί αρχισε να ενδιαφερεατι στα κινητά τηλέφωνα και μπήκε στο σύστημα της Digital Equipment Corporation κλέβοντας πολύτιμο λογισμικο. Από εκεί και μετά ξεκίνησε μια διαδρομή 2.5 χρόνων περίπου με τον Mitnick να παραβιάζει υπολογιστές, δίκτυα τηλεφώνων, κυβερνητικά έγγραφα και δημόσια συστήματα. Το τέλος στο ταξιδι του ήταν η προσπάθεια του να χακαρει τον προσωπικό υπολογιστή ενός άλλου χακερ, του Tsutomu Shimomura. Πλεον ο Mitnick εργάζεται ως υπεύθυνος Cyber security, σχολιαστής και σύμβουλος.

- **Adrian Lamo**: Ο Lamo ήταν ένας διάσημος χάκερ που έγινε γνωστός επειδή εισέβαλε στα συστήματα υπολογιστών μεγάλων εταιρειών όπως η Microsoft και οι New York Times. Αυτό το έκανε χρησιμοποιώντας δημόσιες συνδέσεις στο Διαδίκτυο σε μέρη όπως καφετέριες, έτσι ώστε να ήταν πιο δύσκολο για τους ανθρώπους να τον βρουν. Εξαιτίας αυτού, ονομάστηκε άστεγος χάκερ. Ο Lamo εισέβαλε επίσης σε άλλες εταιρείες όπως το Yahoo η Citigroup, η Bank of America και η Cingular, αλλά το έκανε νόμιμα ως μέλος μιας ομάδας καλών χάκερ που βοηθούν τις εταιρείες να βρουν και να διορθώσουν προβλήματα στην ασφάλειά τους. Ωστόσο, παραβίασε το νόμο όταν εισέβαλε στο σύστημα ιδιωτικής ασφάλειας των New York Times. Συνελήφθη και καταδικάστηκε σε δύο χρόνια φυλάκιση, αλλά τώρα είναι έξω και εργάζεται ως βραβευμένος δημοσιογράφος.

- **Jonathan James**: Όταν ο Τζέιμς ήταν 16 ετών, έκανε κάτι πολύ "λάθος" με τους υπολογιστές και μπήκε σε μπελάδες. Παραδέχτηκε ότι το έκανε γιατί πίστευε ότι ήταν διασκεδαστικό και του άρεσαν οι προκλήσεις. Ο Τζέιμς εισέβαλε σε σημαντικά μέρη όπως το Υπουργείο Δικαιοσύνης και πήρε μυστικούς κωδικούς πρόσβασης για να διαβάσει σημαντικά μηνύματα ηλεκτρονικού ταχυδρομείου. Μπήκε επίσης στους υπολογιστές της NASA και πήρε ειδικό λογισμικό που άξιζε πολλά χρήματα.

- **Robert Tappan Morris**: Ο Morris είναι γιος κάποιου που εργάζεται για τη NASA και δημιούργησε έναν ιό που ονομάζεται σκουλήκι Morris το οποιο ηταν το πρωτο που διαδοθηκε μεσω του διαδικτυου και μαλσιτα όταν ήταν μολις φοιτητής. Το σκουλήκι εξαπλώθηκε γρήγορα σε πολλούς υπολογιστές στο διαδίκτυο, προκαλώντας πολλά προβλήματα. Ο Μόρις μπήκε σε μπελάδες που έφτιαξε το σκουλήκι και έπρεπε να πληρώσει πρόστιμο, να κάνει κοινωφελή εργασία και να κάνει ένα διάλειμμα από το σχολείο. Τώρα, διδάσκει σε ένα πανεπιστήμιο και μελετά πώς συνδέονται οι υπολογιστές μεταξύ τους.

- **Kevin Poulsen**: Ο Kevin Poulsen, γνωστός και ως Dark Dante, έγινε διάσημος κάνοντας ¨ατακτα¨ πράγματα. Μπήκε κρυφά σε έναν ραδιοφωνικό σταθμό και μπέρδεψε με τους διαγωνισμούς τους, κερδίζοντας όμορφα βραβεία σαν ένα φανταχτερό αυτοκίνητο. Η αστυνομία ενεπλάκη γιατί μπήκε και σε μυστικά αρχεία υπολογιστή και πήρε σημαντικές πληροφορίες. Ήταν πολύ καλός στο να μπλέκει με τις τηλεφωνικές γραμμές και προκάλεσε πολλά προβλήματα στα μεγάλα ραδιοφωνικά δίκτυα. Τον έπιασαν σε ένα μπακάλικο και έπρεπε να πάει φυλακή για πέντε χρόνια. Αλλά ενώ ήταν στη φυλακή, έγινε συγγραφέας για έναν ειδησεογραφικό ιστότοπο που ονομάζεται Wired News.

1.3 Τυποι χακερ

1. Λευκό Καπέλο (White Hat Hackers): Είναι οι ethical hackers που δουλεύουν για να βελτιώσουν την ασφάλεια. Συνήθως είναι επαγγελματίες που έχουν πιστοποιηθεί και εργάζονται για εταιρείες ή οργανισμούς.

2. Μαύρο Καπέλο (Black Hat Hackers): Είναι άτομα που προσπαθούν να παραβιάσουν τα συστήματα ασφαλείας με παράνομους τρόπους, συχνά με κακές προθέσεις, όπως η κλοπή δεδομένων ή η πρόκληση ζημιάς.

3. Γκρι Καπέλο (Grey Hat Hackers): Είναι κάπου ανάμεσα στα δύο προηγούμενα. Μπορεί να παραβιάζουν συστήματα χωρίς άδεια, αλλά χωρίς να έχουν κακές προθέσεις. Συχνά ανακαλύπτουν ευπάθειες και στη συνέχεια ενημερώνουν τους ιδιοκτήτες των συστημάτων.

4. Κόκκινο Καπέλο (Red Hat Hackers): Αυτοί είναι σαν τους "εκδικητές" του χώρου του hacking. Όταν ανακαλύπτουν έναν κακόβουλο hacker, αντί να αναφέρουν την επίθεση, προσπαθούν να "καταστρέψουν" τον υπολογιστή του ή το δίκτυό του.

5. Πράσινο Καπέλο (Green Hat Hackers): Είναι οι "νέοι" στο χώρο του hacking. Έχουν περιορισμένες γνώσεις, αλλά έναν μεγάλο περιστασιακό ενθουσιασμό για τον τομέα.

6. Μπλε Καπέλο (Blue Hat Hackers): Αυτοί είναι ειδικοί που δοκιμάζουν την ασφάλεια πριν από την επίσημη δοκιμή. Συχνά, οι Blue Hat Hackers είναι εξωτερικοί εργολάβοι που έρχονται για να εντοπίσουν ευπάθειες σε

συστήματα που έχουν ήδη ελεγχθεί από τους εσωτερικούς ομάδες ασφαλείας (White Hat Hackers). Το όνομα "Blue Hat" προέρχεται συχνά από τις παρουσιάσεις που κάνουν στις εταιρείες για τις ευπάθειες που ανακαλύπτουν.

Εικονα 1.3 Οι 6 τύποι ομάδων χάκερ

1.4 Οι 5 Φάσεις του Ethical Hacking

Εικόνα 1.4 Οι 5 φάσεις του ηθικού χάκινγκ

1.4.1 Αναγνώριση (Reconnaissance)

Η αναγνώριση, που συχνά αναφέρεται ως η πρώτη φάση του hacking, είναι η διαδικασία συλλογής πληροφοριών σχετικά με ένα σύστημα με ενα δίκτυο ή εναν οργανισμό. Παίζει σημαντικό ρόλο στη στρατηγική και σκεψη του χάκερ, επειδή οι πληροφορίες που συλλέγονται κατά τη φάση αυτή τον βοηθούν να σχεδιάσει και να εκτελέσει αποτελεσματικότερα τις επόμενες ενεργειες του.

Παθητική και ενεργητική αναγνώρισή

Η αρχική φάση του hacking, μπορεί να χωριστεί σε δύο σταδια, την παθητική και ενεργητική αναγνώριση. Η παθητική αναγνώριση περιλαμβάνει τη συλλογή διαθέσιμων πληροφοριών χωρίς άμεση αλληλεπίδραση με τον στόχο. Οι πληροφορίες αυτές μπορεί να περιλαμβάνουν λεπτομέρειες μεσα απο προφίλ στα social media, δημόσιες βάσεις δεδομένων και διαδικτυακά φόρουμ. Αυτα με την σειρα τους μπορούν να χρησιμοποιηθούν ως βάση για την κατανόηση του περιβάλλοντος του στόχου. Αντιθέτος η ενεργητική αναγνώριση περιλαμβάνει μια πιο άμεση αλληλεπίδραση με τον στόχο για τη συλλογή πιο συγκεκριμένων και λεπτομερών πληροφοριών. Χρησιμοποιούνται διαφορες τεχνικές όπως η σάρωση δικτύου και η ερευνα για την ανακάλυψη ανοικτών θυρών, υπηρεσιών και ευπαθειών.

Συλλογή Πληροφοριών κατά την αναγνώριση

Κατά τη φάση της αναγνώρισης, οι χάκερ συλλέγουν ένα ευρύ φάσμα πληροφοριών σχετικά με τον στόχο. Αυτό περιλαμβάνει τον εντοπισμό διευθύνσεων IP, ονόματα domain, τοπολογίες δικτύων, εκδόσεις συστημάτων, στοιχεία εργαζομένων, διευθύνσεις ηλεκτρονικού ταχυδρομείου, ακόμη και πληροφορίες σχετικά με τις πολιτικές ασφαλείας. Οι πληροφορίες αυτές αποτελούν τη βάση για τις επόμενες φάσεις hacking, καθώς βοηθούν τους επιτιθέμενους να εντοπίσουν πιθανές αδυναμίες και σημεία εισόδου στον στόχο.

1.4.2 Σάρωση (Scanning)

Η διαδικασία της σάρωσης αποτελεί την δεύτερη φάση της διαδικασίας και συνδέεται στενά με την πρωτη. Κατά τη διάρκεια αυτής της φάσης, οι δραστες χρησιμοποιουν εργαλεία και διενεργούν πολυ προσεκτικα ετσι ωστε να γινει η σάρωση στα συστήματα, τα δίκτυα ή τις εφαρμογές του στόχου προκειμένου να εντοπίσουν ευπάθειες και αδυναμίες που ενδέχεται να εκμεταλλευτούν. Κύριος στόχος αυτής της διαδικασίας είναι η πλήρης εξέταση και η κατανόηση του συστήματος του στόχου.Η σάρωση παιζει κρίσιμο ρόλο στη στρατηγική του εισβολέα, παρέχοντας λεπτομερή κατανόηση του περιβάλλοντος του στόχου και των πιθανών σημείων εισόδου.

1.4.3 Απόκτηση Πρόσβασης (Gaining Access)

Η απόκτηση πρόσβασης γνωστή και ως φάση εκμετάλλευσης, είναι ένα κρίσιμο βήμα στη διαδικασία, όπου οι δραστες προσπαθούν να αξιοποιήσουν ευπάθειες και αδυναμίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Σε αυτή τη φάση οι χάκερς εκτελούν τις εντολες για να εκθέσουν τον στόχο σε κίνδυνο. Τα πράγματα που θέλει να πετύχει κάποιος σε αυτή τη φάση μπορεί να είναι διαφορετικά ανάλογα με το γιατί το κάνει. Σε ορισμένες περιπτώσεις, ο στόχος μπορεί να είναι η παραβίαση λογαριασμών χρηστών για την κλοπή ευαίσθητων πληροφοριών ή τη εξαπατηση αλλων ενργειων. Άλλοι δραστες μπορεί να επιδιώκουν να εκμεταλλευτούν ευαλωτα σημεία στο σύστημα ή το δίκτυο για να αποκτήσουν τον έλεγχο.

Τεχνικές και Μέθοδοι

Οι χάκερ χρησιμοποιούν ένα ευρύ φάσμα τεχνικών και μεθόδων σε αυτη τη φαση για να επιτύχουν τους στόχους τους. Μια συνηθισμενη προσέγγιση είναι η εκμετάλλευση γνωστών ευπαθειων σε λογισμικό, λειτουργικά συστήματα,εφαρμογές κτλπ. Οι δραστες μπορούν να αξιοποιήσουν διαθέσιμα exploits ή να αναπτύξουν exploits προσαρμοσμένα στον συγκεκριμένο στόχο. Επιπλέον, κακόβουλα λογισμικα, όπως ιοί, δούρειοι ίπποι ή backdoors, μπορουν να εισαχθούν για να παραβιάσουν συστήματα και να αποκτήσουν τον έλεγχο. Μέθοδοι κλοπής στοιχείων πρόσβασης οπως οι επιθέσεις phishing,keyloggers ή επιθέσεις brute force, χρησιμοποιούνται συχνά για την απόκτηση πρόσβασης.

1.4.4 Διατήρηση Πρόσβασης (Maintaining Access)

Η διατήρηση της πρόσβασης είναι μια κρίσιμη φάση στη διαδικασία, όπου οι επιτιθέμενοι επιδιώκουν να διασφαλίσουν τον συνεχή έλεγχό τους σε ένα παραβιασμένο σύστημα. Μετά την επιτυχή απόκτηση αρχικής πρόσβασης, η διατήρηση της πρόσβασης επιτρέπει στους επιτιθέμενους να ελέγχουν συνεχώς τον στόχο τους, να εκτελούν κακόβουλες δραστηριότητες και να επιτυγχάνουν τους στόχους τους. Σε αυτό το στάδιο, οι φορείς απειλών ενδιαφέρονται κυρίως να διασφαλίσουν ότι έχουν τη δυνατότητα να επανακτήσουν πρόσβαση στα συστήματα, ακόμη και αν τα μετρα ασφαλειας εξαλείψουν το αρχικό σημείο εισόδου τους.

Μηχανισμοί διατήρησης πρόσβασης

Για να επιτευχθεί η συνεχης διατήρηση, οι φορείς αναπτύσσουν ένα πολύπλευρο οπλοστάσιο τεχνικών και μηχανισμών που τους επιτρέπει να διατηρουν την πρόσβαση και τον έλεγχο του παραβιασμένου συστήματος ή. Αυτοί οι μηχανισμοί περιλαμβάνουν την οργάνωση backdoors, μυστικών ή κρυφών σημείων πρόσβασης με διαφορετικές μεθόδους εισόδου σε συνδυασμό με την αρχικά εκμεταλλευόμενη ευπάθεια. Οι δραστες μπορούν επίσης να δημιουργησουν νέους λογαριασμους χρηστών ή να προσαρμώσουν τους ήδη υπαρχον, προσδίδοντας αυξημένα προνόμια για να εξασφαλίσουν συνεχή

πρόσβαση. Η εμφύτευση μόνιμου κακόβουλου λογισμικού, όπως τα rootkits ή τα Trojans, αποτελεί μια συνηθισμένη τακτική για τη διατήρηση συνεχούς πρόσβασης.

1.4.5 Κάλυψη Ιχνών (Covering Tracks)

Η φάση της κάλυψης των ιχνών αποτελεί ένα κομβικό σημειο στη διαδικασία του hacking, απαιτώντας τις συντονισμένες προσπάθειες των δραστων να αποκρύψουν την παρουσία τους, τις δραστηριότητές τους και κάθε ίχνος εισβολής. Η φάση αυτή αποκτά κρίσιμη σημασία για τους χάκερ, καθώς είναι καθοριστική για τη διατήρηση της ανωνυμίας, την αποφυγή της ανίχνευσης και τη διασφάλιση ότι η μη εξουσιοδοτημένη πρόσβασή τους θα παραμείνει κρυφή για όσο το δυνατόν γίνεται. Βασικός στόχος της φάσης της κάλυψης των ιχνών στο hacking είναι η σχολαστική εξάλειψη ή η απόκρυψη κάθε ψηφιακού αποτυπώματος ή ίχνους που θα μπορούσε να προδώσει την παρουσία του επιτιθέμενου στο παραβιασμένο σύστημα ή δίκτυο. Σε αυτό το σημείο, οι απειλητικοί φορείς προσπαθούν οσο περισσοτερο μπορουν να ματαιώσουν τις προσπάθειες των ομάδων ασφαλείας , με απώτερο στόχο να αποκλείσουν οποιαδήποτε γνώση της επίθεσης.

Τεχνικές και μέθοδοι

Οι δράστες κινούνται επιδέξια στο ψηφιακό τοπίο, συμμετέχοντας σε δραστηριότητες όπως η χειραγώγηση αρχείων καταγραφής. Αυτό περιλαμβάνει την ικανότητα αλλοίωσης ή διαγραφής των αρχείων καταγραφής συστήματος, των αρχείων(system logs), των αρχείων καταγραφής συμβάντων (event logs) και των διαδρομών ελέγχου (audit trails), εξαλείφοντας αποτελεσματικά κάθε ίχνος των ανονυμων ενεργειών τους. Οι δραστες χειρίζονται επιδέξια τα timelogs σε αρχεία ή αρχεία καταγραφής συστήματος για να δημιουργήσουν μια ψευδαίσθηση, αποκρύπτοντας έτσι τις μη εξουσιοδοτημένες δραστηριότητές τους. Για να προκαλέσουν περαιτέρω σύγχυση στους ερευνητές, οι επιτιθέμενοι μπορεί να εισάγουν αντιπερισπασμούς με τη μορφή ψευδών πληροφοριών αποσπώντας την προσοχή από τον πραγματικό φορέα της επίθεσης.

1.5 ΣΥΝΟΨΗ

Σε αυτό το κεφάλαιο έγινε η πρώτη επαφή και εξοικείωση με τους τύπους χακερς και με τον ορισμο του χακινγκ καθως και η ιστορική αναδρομή του hacking με την αναφορά κάποιων πολύ σημαντικών ατόμων γύρω από το χώρο του.

Τέλος, εγιναν κατανοητές οι 5 φάσεις εκτέλεσης μιας διείσδυσης, οι οποίες είναι τα βασικά πρώτα βήματα που ακολουθούμε, ώστε να γίνει η διείσδυση με οργάνωση, επιτυχία και μυστικότητα.

Στο επόμενο κεφάλαιο θα γίνει αναφορά σε αρκετές κατηγορίες επιθέσεων, με σαφή περιγραφή κάθε επίθεσης, καθώς θα δωθούν και αρκετές συμβουλές για την προστασία των συστημάτων.

2 Περιγραφές Επιθέσεων

2.1 Επίθεση σε Διαδικτυακές Εφαρμογές

2.1.1 Server attack

SQL INJECTION

Το SQL injection είναι ένας τύπος επίθεσης κυβερνοασφάλειας που στοχεύει στις ευπάθειες του λογισμικού που αλληλεπιδρά με ένα σύστημα διαχείρισης βάσεων δεδομένων (DataBaseManagentSystem). Εκτελείται με την εισαγωγή ή κάνοντας " ένεση " κακόβουλων εντολών SQL σε ένα πεδίο εισαγωγής με σκοπό την παραβίαση των μέτρων ασφαλείας και τη χειραγώγηση της βάσης δεδομένων. Η τεχνική αυτή εκμεταλλεύεται τα τρωτά σημεία στο λογισμικό της εφαρμογής, ιδίως στον τρόπο με τον οποίο επεξεργάζονται και ενσωματώνονται τα δεδομένα εισόδου του χρήστη στα ερωτήματα(queries) SQL. Όταν ένα πρόγραμμα αποτυγχάνει να καθαρίσει σωστά τις εισόδους του χρήστη, οι εισβολεις μπορούν να εισάγουν εντολές SQL που ερμηνεύονται ως μέρη ενός ερωτήματος SQL από το DBMS. Αυτή η παραβίαση συμβαίνει λόγω ανεπαρκούς επικύρωσης εισόδου και παραμετροποιημένων queries, επιτρέποντας σε έναν επιτιθέμενο να αλλάξει την κατασκευή μιας backend SQL. Οι συνέπειες μιας επιτυχημένης επίθεσης SQL ένεσης μπορεί να είναι σοβαρές και ξεκινούν από τη μη εξουσιοδοτημένη προβολή δεδομένων, τη χειραγώγηση δεδομένων έως τον πλήρη έλεγχο της λειτουργικότητας της βάσης δεδομένων. Η επίθεση μπορεί να οδηγήσει σε

παραβιάσεις δεδομένων, απώλεια δεδομένων, ακόμη και σε παραβίαση της ακεραιότητας του διακομιστή.

Remote Code Execution (RCE)

Μια κυβερνοεπίθεση γνωστή ως "απομακρυσμένη εκτέλεση κώδικα" συμβαίνει όταν ένας εισβολέας αποκτά τη δυνατότητα να εκτελέσει αυθαίρετο κώδικα σε έναν υπολογιστή ή διακομιστή στόχο μέσω δικτύου. Αυτός ο τύπος επίθεσης χρησιμοποιεί ελαττώματα στο υλικό ή το λογισμικό για τη μετάδοση ειδικά κατασκευασμένων αιτημάτων ή δεδομένων σε ένα σύστημα. Αυτά τα αιτήματα ενεργοποιούν τον κακόβουλο κώδικα του επιτιθέμενου για να εκτελεστεί από το σύστημα. Το λογισμικό που χειρίζεται μη αξιόπιστες εισόδους χωρίς επαρκή επικύρωση ή εξυγίανση συχνά διαπιστώνεται ότι έχει ευπάθειες RCE.
Συνήθως, στις επιθέσεις RCE χρησιμοποιούνται υπερχειλίσεις buffer, σφάλματα αποδιαταγής ή άλλες ευπάθειες επικύρωσης εισόδου. Αυτές οι επιθέσεις έχουν τη δυνατότητα να παραβιάσουν πλήρως το στοχευμένο σύστημα, δίνοντας στους χάκερ πρόσβαση για να κλέψουν εμπιστευτικά δεδομένα, να παρεμβαίνουν στις λειτουργίες ή να χρησιμοποιήσουν το παραβιασμένο σύστημα ως εφαλτήριο για πρόσθετες επιθέσεις.

Directory Traversal

Ένα διαδικτυακό ελάττωμα ασφαλείας που ονομάζεται Directory Traversal, μερικές φορές αναφέρεται ως Path Traversal, επιτρέπει σε έναν εισβολέα να έχει πρόσβαση σε αρχεία και καταλόγους που διατηρούνται εκτός του ριζικού φακέλου του ιστού. Μέσω της χειραγώγησης μεταβλητών που αναφέρονται σε αρχεία ('../' σε συστήματα που βασίζονται στο Unix), ένας εισβολέας μπορεί να αποκτήσει πρόσβαση σε αρχεία ή καταλόγους που δεν προορίζονται να είναι προσβάσιμα μέσω της εφαρμογής ιστού με πλοήγηση στο σύστημα αρχείων.

Όταν μια web εφαρμογή χρησιμοποιεί είσοδο χρήστη για τη δημιουργία αρχείων χωρίς να καθαρίζει σωστά την είσοδο, δημιουργεί ευπάθεια, καθώς δεν υπάρχουν επαρκή μέτρα ασφαλείας. Εάν μια ευπάθεια διάσχισης καταλόγου αξιοποιηθεί επιτυχώς, ο εισβολέας μπορεί να είναι σε θέση να αποκτήσει πρόσβαση και να εκτελέσει αρχεία στο διακομιστή, γεγονός που μπορεί να οδηγήσει σε διαρροή πληροφοριών, μη εξουσιοδοτημένη πρόσβαση και περιστασιακά σε απομακρυσμένη εκτέλεση κώδικα.

Ευπαθειες Σε Αρχεια (File Upload Vulnerabilities)

Όταν μια web εφαρμογή επιτρέπει στους χρήστες να ανεβάζουν αρχεία στο διακομιστή χωρίς να εκτελεί αρκετούς ελέγχους ασφαλείας, δημιουργούνται ευπάθειες στο ανέβασμα αρχείων. Ανάλογα με το είδος της ευπάθειας και τους στόχους του επιτιθέμενου, αυτό μπορεί να οδηγήσει σε μια ποικιλία επιθέσεων. Ο κύριος κίνδυνος είναι ότι ένα κακόβουλο αρχείο, όπως μια δέσμη ενεργειών, θα μπορούσε να μεταφορτωθεί από έναν δράστη και να εκτελεστεί στο διακομιστή ή στα προγράμματα περιήγησης άλλων ατόμων, προκαλώντας ενδεχομένως cross-site scripting, απομακρυσμένη εκτέλεση κώδικα ή κλοπή δεδομένων.

Password Mismanagement(κακη διαχειρηση κωδικων προσβασης)

Ο ακατάλληλος χειρισμός και η προστασία των κωδικών πρόσβασης, οι οποίοι είναι απαραίτητοι για τη διασφάλιση των λογαριασμών χρηστών και των προσωπικών δεδομένων, αναφέρεται ως κακή διαχείριση των κωδικών πρόσβασης. Περιλαμβάνει μια ποικιλία ενεργειών που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια και την ακεραιότητα των δεδομένων, με πιθανό αποτέλεσμα την παραβίαση δεδομένων και τη μη εξουσιοδοτημένη πρόσβαση.

Αδύναμοι κωδικοί πρόσβασης

Χρήση κωδικών πρόσβασης που είναι εύκολο να μαντέψουν ή να σπάσουν, όπως κοινές λέξεις, φράσεις ή ακολουθίες (π.χ. "password", "123456"). Οι αδύναμοι κωδικοί πρόσβασης μπορούν να σπάσουν γρήγορα με επιθέσεις ωμής βίας ή λεξικού.

Επαναχρησιμοποίηση κωδικών πρόσβασης

Χρήση του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς ή συστήματα. Αυτή η πρακτική ενισχύει τον κίνδυνο, διότι εάν ένας λογαριασμός παραβιαστεί, όλοι οι άλλοι λογαριασμοί που χρησιμοποιούν τον ίδιο κωδικό πρόσβασης καθίστανται ευάλωτοι.

Ανεπαρκείς πρακτικές αποθήκευσης

Αποθήκευση κωδικών πρόσβασης σε απλό κείμενο ή χρήση αδύναμων κρυπτογραφικών μεθόδων. Οι κωδικοί πρόσβασης θα πρέπει να αποθηκεύονται με τη χρήση ισχυρών αλγορίθμων ανάλυσης (hashing algorithms), ιδανικά με salt (τυχαία δεδομένα που προστίθενται στον κωδικό πρόσβασης πριν από την ανάλυση) για την αποτροπή επιθέσεων όπως οι επιθέσεις με rainbow table attacks.

Έλλειψη ασφαλούς μετάδοσης

Μετάδοση κωδικών πρόσβασης μέσω μη κρυπτογραφημένων καναλιών. Οι κωδικοί πρόσβασης θα πρέπει πάντα να μεταδίδονται μέσω ασφαλών, κρυπτογραφημένων συνδέσεων (όπως το HTTPS) για την αποφυγή υποκλοπής από μη εξουσιοδοτημένα μέρη.

Ανεπαρκείς πολιτικές κωδικών πρόσβασης

Αποτυχία εφαρμογής ή επιβολής ισχυρών πολιτικών κωδικών πρόσβασης. Οι φορείς θα πρέπει να επιβάλλουν πολιτικές που απαιτούν σύνθετους κωδικούς πρόσβασης (συμπεριλαμβανομένου ενός συνδυασμού γραμμάτων, αριθμών και ειδικών χαρακτήρων) και να επιβάλλουν την τακτική αλλαγή κωδικών πρόσβασης.

Παραμέληση του ελέγχου ταυτότητας δύο παραγόντων (2FA)

Βασίζεται αποκλειστικά σε κωδικούς πρόσβασης για τον έλεγχο ταυτότητας των χρηστών. Η εφαρμογή 2FA προσθέτει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας πιο δύσκολο για τους μη εξουσιοδοτημένους χρήστες να αποκτήσουν πρόσβαση, ακόμη και αν έχουν τον κωδικό πρόσβασης.

2.1.2 Client attack

Προσδιορισμός των τρωτών σημείων (Identification of Vulnerabilities)

Οι επιθέσεις από την πλευρά του πελάτη συχνά ξεκινούν με τον εντοπισμό ευπαθειών στο λογισμικό από την πλευρά του πελάτη. Αυτό περιλαμβάνει την εκμετάλλευση αδυναμιών σε εφαρμογές που επεξεργάζονται εξωτερικές εισόδους, όπως προγράμματα

περιήγησης στο διαδίκτυο, προγράμματα ανάγνωσης εγγράφων, προγράμματα ηλεκτρονικού ταχυδρομείου και διάφορα άλλα διαδραστικά εργαλεία. Οι δράστες σαρώνουν σχολαστικά για ελαττώματα ασφαλείας, όπως υπερχειλίσεις buffer, ευπάθειες cross-site scripting (XSS), ανασφαλής αποδιαταγή και άλλα ελαττώματα λογισμικού που μπορούν να ενεργοποιηθούν από ειδικά διαμορφωμένες εισόδους. Αυτές οι ευπάθειες καταγράφονται συνήθως σε βάσεις δεδομένων, όπως ο κατάλογος Common Vulnerabilities and Exposures (CVE), παρέχοντας στους δράστες πληροφορίες για πιθανούς στόχους.

Οι επιθέσεις Cross-Site Scripting (XSS) είναι ένας διαδεδομένος τύπος ευπάθειας ασφαλείας σε εφαρμογές ιστού. Οι επιθέσεις XSS συμβαίνουν όταν ένας εισβολέας καταφέρνει να εισάγει κακόβουλα scripts σε ιστοσελίδες που προβάλλονται από άλλους χρήστες. Αυτά τα scripts μπορούν να εκτελεστούν στο πλαίσιο της συνεδρίας του θύματος, επιτρέποντας στον επιτιθέμενο να κλέψει tokens συνεδρίας, διαπιστευτήρια σύνδεσης ή άλλες ευαίσθητες πληροφορίες.

Stored XSS (Persistent XSS)

Το αποθηκευμένο XSS, επίσης γνωστό ως Persistent XSS, είναι μια σοβαρή μορφή XSS, όπου ο δράστης εισάγει ένα κακόβουλο script (συχνά JavaScript) απευθείας στις βάσεις δεδομένων μιας web εφαρμογής-στόχου. Αυτός ο τύπος επίθεσης συνήθως αξιοποιεί ανεπαρκείς μηχανισμούς επικύρωσης εισόδου στην πλευρά του διακομιστή. Το payload του εισβολέα μπορεί να εισαχθεί μέσω εισόδων φόρμας, σχολίων ή οποιουδήποτε άλλου μηχανισμού εισόδου που δέχεται και αποθηκεύει δεδομένα χρήστη. Μόλις το κακόβουλο σενάριο αποθηκευτεί, γίνεται μέρος του περιεχομένου της εφαρμογής ιστού. Στη συνέχεια, κάθε φορά που ένας χρήστης αποκτά πρόσβαση στην παραβιασμένη σελίδα ή λειτουργία, το κακόβουλο σενάριο παραδίδεται και εκτελείται στο πλαίσιο του προγράμματος περιήγησης του χρήστη. Αυτός ο επίμονος χαρακτήρας της επίθεσης

επιτρέπει να επηρεάσει πολλούς χρήστες με την πάροδο του χρόνου και μπορεί να οδηγήσει σε εκτεταμένες παραβιάσεις δεδομένων, πειρατεία συνόδου και άλλες εκμεταλλεύσεις. Η αντιμετώπιση του Stored XSS συνήθως περιλαμβάνει την εφαρμογή αυστηρής επικύρωσης εισόδου, την απολύμανση περιεχομένου και τη χρήση ασφαλών πρακτικών κωδικοποίησης για να διασφαλίσει τον κατάλληλο χειρισμό των δεδομένων που παρέχονται από τον χρήστη.

Reflected XSS (Non-Persistent XSS)

Το αντανακλώμενο XSS, ή μη μόνιμο XSS, συμβαίνει όταν το σενάριο ενός επιτιθέμενου αντανακλάται από έναν διακομιστή ιστού, όπως εσφαλμένο μήνυμα, σε ένα αποτέλεσμα αναζήτησης ή σε οποιαδήποτε απάντηση που περιλαμβάνει μέρος ή το σύνολο της εισόδου που αποστέλλεται στον διακομιστή. Σε αντίθεση με το αποθηκευμένο XSS, το κακόβουλο σενάριο στο Reflected XSS δεν αποθηκεύεται στο διακομιστή. Αντ' αυτού, συνήθως ενσωματώνεται σε μια διεύθυνση URL ή διαμορφώνεται σε μια αίτηση HTTP (όπως μια υποβολή φόρμας), η οποία στη συνέχεια αποστέλλεται στο θύμα, συνήθως μέσω ενός συνδέσμου σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μια ιστοσελίδα. Όταν το θύμα κάνει κλικ στο σύνδεσμο, το ενέσιμο σενάριο(injected script) μεταβαίνει στον ευάλωτο ιστότοπο, ο οποίος επιστρέφει την επίθεση πίσω στο browser (πρόγραμμα περιήγησης). Στη συνέχεια, το πρόγραμμα περιήγησης θα εκτελέσει το σενάριο, θεωρώντας το ως νόμιμο μέρος της αντίδρασης από τον αξιόπιστο ιστότοπο. Αυτός ο τύπος XSS απαιτεί συχνά social engineering για να πείσει το θύμα να κάνει κλικ στον κακόβουλο σύνδεσμο. Για την αποτροπή του αντανακλώμενου XSS, οι προγραμματιστές θα πρέπει να χρησιμοποιούν κατάλληλη κωδικοποίηση και επικύρωση εξόδου, διασφαλίζοντας ότι η είσοδος του χρήστη που αντανακλάται στις ιστοσελίδες καθίσταται ακίνδυνη.

DOM-based XSS

Οι επιθέσεις XSS που βασίζονται στο DOM στοχεύουν στο Μοντέλο Αντικειμένου Εγγράφου ("Document Object Model", DOM) μιας ιστοσελίδας, το οποίο είναι μια προγραμματιστική διεπαφή για έγγραφα HTML και XML. Σε αυτές τις επιθέσεις, η ευπάθεια βρίσκεται στον κώδικα της πλευράς του πελάτη (όπως η JavaScript) και όχι στον κώδικα της πλευράς του διακομιστή. Ο επιτιθέμενος χειρίζεται το περιβάλλον DOM στο πρόγραμμα περιήγησης του θύματος, αναγκάζοντας το script από την πλευρά του πελάτη να συμπεριλάβει μη αξιόπιστα δεδομένα στο DOM. Αυτό το είδος επίθεσης XSS συμβαίνει όταν μια δέσμη εντολών λαμβάνει δεδομένα από μια ελεγχόμενη από τον επιτιθέμενο πηγή, όπως η διεύθυνση URL, και τα μεταβιβάζει εσφαλμένα σε μια απορροή(sink) εντός του DOM που υποστηρίζει τη δυναμική εκτέλεση κώδικα (όπως το 'innerHTML' ή το 'document.write'). Δεδομένου ότι το payload δεν πηγαίνει στον διακομιστή αλλά εκτελείται απευθείας στο πρόγραμμα περιήγησης, οι συνήθεις άμυνες από την πλευρά του διακομιστή, όπως η επικύρωση εισόδου, είναι λιγότερο αποτελεσματικές. Στα πλαίσια των μεθόδων μετριασμού του DOM-based XSS περιλαμβάνεται η διασφάλιση ότι τα scripts στην πλευρά του πελάτη αντιμετωπίζουν όλα τα δεδομένα ως μη αξιόπιστα και χρησιμοποιούν λειτουργίες που χειρίζονται ρητά τα δεδομένα με ασφάλεια, παράλληλα με την υιοθέτηση πλαισίων που χειρίζονται αυτόματα αυτές τις ανησυχίες.

Μηχανισμοί Παράδοσης

Ηλεκτρονικά μηνύματα phishing(ψαρέματος)

Οι επιτιθέμενοι χρησιμοποιούν εξελιγμένες τεχνικές κοινωνικής μηχανικής για να δημιουργήσουν μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνονται νόμιμα, δελεάζοντας τους χρήστες να κάνουν κλικ σε κακόβουλους συνδέσμους ή να κατεβάσουν μολυσμένα συνημμένα αρχεία. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να εκμεταλλεύονται γνωστές ευπάθειες σε προγράμματα ηλεκτρονικού ταχυδρομείου ή να χρησιμοποιούν κακόβουλες μακροεντολές σε συνημμένα έγγραφα.

Παραβιασμένοι ιστότοποι (Compromised Websites)

Ιστοσελίδες με τρωτά σημεία ασφαλείας μπορούν να υποκλαπούν και να χρησιμοποιηθούν για την αποστολή κακόβουλου λογισμικού. Αυτό περιλαμβάνει νόμιμους ιστότοπους στους οποίους έχουν διεισδύσει δράστες, οι οποίοι στη συνέχεια ενσωματώνουν κακόβουλα σενάρια ή exploit kits στις σελίδες του ιστότοπου.

Κακόβουλη διαφήμιση (Malvertising)

Περιλαμβάνει την εισαγωγή κακόβουλου κώδικα σε διαδικτυακά διαφημιστικά δίκτυα. Όταν τα θύματα κάνουν κλικ σε αυτές τις διαφημίσεις, ο κώδικας τους ανακατευθύνει σε κακόβουλους ιστότοπους ή κατεβάζει απευθείας κακόβουλο λογισμικό στο σύστημά τους.

Drive By Downloads

Αναφέρεται στην ακούσια λήψη κακόβουλου λογισμικού όταν ένας χρήστης επισκέπτεται έναν μολυσμένο ιστότοπο. Το κακόβουλο λογισμικό παραδίδεται συνήθως μέσω exploit kits που εντοπίζουν ευπάθειες στο πρόγραμμα περιήγησης ή στα πρόσθετά του και εκτελούν τον κώδικα χωρίς τη συγκατάθεση του χρήστη.

Λειτουργία κακόβουλων scripts (Running Malicious Scripts)

Στην περίπτωση των ευπαθειών XSS ή των ευπαθειών που βασίζονται σε JavaScript, το κακόβουλο σενάριο εκτελείται εντός του προγράμματος περιήγησης του χρήστη, επιτρέποντας ενέργειες όπως η πειρατεία, η κλοπή δεδομένων ή η επανακατεύθυνση σε επικίνδυνους ιστότοπους.

Εγκατάσταση κακόβουλου λογισμικού (Installing Malware)

Το payload μπορεί να εγκαταστήσει κακόβουλο λογισμικό, όπως trojans, ransomware ή spyware, το οποίο μπορεί να εκτελέσει μια σειρά ενεργειών από την κρυπτογράφηση αρχείων για λύτρα έως την κατασκοπεία των δραστηριοτήτων του χρήστη και την κλοπή ευαίσθητων δεδομένων.

2.2 Επίθεση σε Operating System

2.2.1 Malicious Software

Το κακόβουλο λογισμικό ,που συχνά αναφέρεται ως malware Είναι ένας τύπος λογισμικού, ειδικά σχεδιασμένος για να διαταράξει, να βλάψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα ,δίκτυα ή συσκευές υπολογιστών. Το κακόβουλο λογισμικό περιλαμβάνει ένα ευρύ φάσμα κακόβουλων προγραμμάτων, συμπεριλαμβανομένωνιών,worms,Trojans,ransomware,spyware,adware,rootkits,keylog gers,botnets,polymorphic malware και fileless malware. Αυτές οι απειλές διαφέρουν ως προς τις μεθόδους μόλυνσης, τις δυνατότητες και τους στόχους τους. Για παράδειγμα, οι ιοί προσκολλώνται σε νόμιμα προγράμματα και αναπαράγονται όταν εκτελούνται, ενώ τα worms εξαπλώνονται ανεξάρτητα σε δίκτυα. Οι Δούρειοι Ίπποι(Trojans) μεταμφιέζονται σε νόμιμο λογισμικό για να εξαπατήσουν τους χρήστες έτσι ώστε να τους κατεβάσουν. Ενώ το ransomware κρυπτογραφεί αρχεία απαιτώντας πληρωμή για την αποκρυπτογράφηση.Το Spyware παρακολουθεί τις δραστηριότητες των χρηστών χωρίς τη συγκατάθεσή τους, το adware κατακλύζει τους χρήστες με ανεπιθύμητες διαφημίσεις και τα rootkits αποκρύπτουν την παρουσία τους για να διατηρήσουν την πρόσβαση των επιτιθέμενων. Τα keyloggers καταγράφουν τις πληκτρολογήσεις για να κλέψουν ευαίσθητες πληροφορίες, τα botnets εκμεταλλεύονται παραβιασμένες συσκευές για κακόβουλες δραστηριότητες και το πολυμορφικό κακόβουλο λογισμικό αλλάζει τον κώδικά του για να αποφύγει την ανίχνευση. Το κακόβουλο λογισμικό χωρίς αρχεία λειτουργεί στη μνήμη του συστήματος χωρίς να αφήνει ίχνη στο δίσκο. Για να μετριάσουν τους κινδύνους που ενέχει το κακόβουλο λογισμικό, τα άτομα και οι οργανισμοί πρέπει να εφαρμόζουν προληπτικά μέτρα, όπως η χρήση αξιόπιστου λογισμικού ασφαλείας, η ενημέρωση των συστημάτων, η άσκηση ασφαλούς διαδικτυακής συμπεριφοράς και η εφαρμογή προηγμένων τεχνικών ασφαλείας, όπως η ανίχνευση βάσει συμπεριφοράς και η τμηματοποίηση του δικτύου.

2.2.2 Ευπαθή Σημεία Σε Μη Ενημερωμένο Λογισμικό

Τι είναι μια ευπάθεια Λογισμικού

Μια "ευπάθεια" στο λογισμικό αναφέρεται σε μια αδυναμία ή ένα ελάττωμα στο σχεδιασμό, την υλοποίηση ή τη διαμόρφωση ενός συστήματος λογισμικού που μπορεί να χρησιμοποιηθεί από επιτιθέμενους για να θέσει σε κίνδυνο την ακεραιότητα, τη διαθεσιμότητα ή την εμπιστευτικότητα του συστήματος ή των δεδομένων του. Αυτές οι ευπάθειες μπορεί να προκύψουν λόγω ποικίλων παραγόντων, συμπεριλαμβανομένων σφαλμάτων προγραμματισμού, εσφαλμένων παραδοχών σχετικά με την ασφάλεια, ανεπαρκών δοκιμών ή αποτυχίας αντιμετώπισης γνωστών ζητημάτων ασφάλειας. Παραδείγματα κοινών ευπαθειών περιλαμβάνουν υπερχειλίσεις buffer, έγχυση SQL, cross-site scripting (XSS).

Οι ευπάθειες συχνά προέρχονται από σφάλματα προγραμματισμού που γίνονται κατά την ανάπτυξη του λογισμικού. Τα σφάλματα αυτά μπορεί να περιλαμβάνουν ακατάλληλη επικύρωση εισόδου(validation input), ανεπαρκή έλεγχο ορίων ή λανθασμένη διαχείριση μνήμης, τα οποία μπορούν να οδηγήσουν σε εκμεταλλεύσιμες αδυναμίες στον κώδικα του λογισμικού. Η ανεπαρκής δοκιμή του λογισμικού μπορεί επίσης να οδηγήσει σε αδυναμίες που περνούν απαρατήρητες. Χωρίς ολοκληρωμένες διαδικασίες δοκιμών, οι προγραμματιστές μπορεί να παραβλέψουν πιθανές αδυναμίες ασφαλείας, αφήνοντας το λογισμικό ευάλωτο στην εκμετάλλευση από επιτιθέμενους. Ορισμένες φορές, τα ευπαθή σημεία δεν αντιμετωπίζονται ακόμη και όταν είναι γνωστά στους προγραμματιστές ή τους προμηθευτές. Αυτό μπορεί να συμβαίνει λόγω ανταγωνιστικών προτεραιοτήτων, περιορισμών πόρων ή έλλειψης κατανόησης της σοβαρότητας της ευπάθειας.

Τι είναι ενα exploit

Ένα exploit είναι ένα κομμάτι λογισμικού ή μια ακολουθία εντολών που προσπαθεί να εκμεταλλευτεί μια ευπάθεια στο λογισμικό ή το υλικό για να εκτελέσει ακούσιες ενέργειες ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Τα exploits συνήθως σχεδιάζονται για να χειραγωγήσουν ή να κάνουν κατάχρηση των ευπαθειών προκειμένου να θέσουν σε κίνδυνο την ασφάλεια ενός συστήματος υπολογιστή, δικτύου ή εφαρμογής λογισμικού. Σε αρκετές περιπτώσεις, ενα exploit μπορεί να χρησιμοποιηθεί ως ενα κομμάτι επίθεσης πολλών στοιχείων. Αντ 'αυτού, με την χρήση ενός κακοβουλού αρχείου, το exploit μπορεί να ρίξει ένα άλλο κακόβουλο λογισμικό, το οποίο να αποτελείται απο trojans και spyware backdoor που μπορούν να υποκλέψουν πληροφορίες χρηστών από τα μολυσμένα συστήματα.

Εικόνα 2.2 Exploit:πρόγραμμα εκμετάλευσης ευπάθειας

Η εξέλιξη τους στο πέρασμα των χρόνων

Από τη δεκαετία του 1980, τα exploits έχουν εξελιχθεί σημαντικά, ακολουθώντας στενά την πορεία των τεχνολογικών εξελίξεων και του μεταβαλλόμενου τοπίου απειλών στον κυβερνοχώρο. Αρχικά, τα exploits ήταν υποτυπώδη, εστιάζοντας σε ευπάθειες σε αυτόνομες εφαρμογές λογισμικού ή λειτουργικά συστήματα. Ωστόσο, στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000, εμφανίστηκε μια νέα εποχή δικτυακών exploits, που στόχευαν ευπάθειες σε διακομιστές ιστού, προγράμματα περιήγησης και πρωτόκολλα δικτύου. Στην εποχή αυτή παρατηρήθηκε επίσης η άνοδος των σκουληκιών και των ιών, με παραδείγματα τον ιό Melissa το 1999 και το σκουλήκι Code Red το 2001, τα οποία εκμεταλλεύονταν ευπάθειες σε συστήματα που ήταν συνδεδεμένα στο διαδίκτυο. Επιπλέον, στη δεκαετία του 2010 παρατηρήθηκε η άνοδος των προηγμένων επίμονων απειλών (Advanced Persistent Threats - APTs), οι οποίες χαρακτηρίζονται από εξελιγμένες, στοχευμένες επιθέσεις με στόχο συγκεκριμένους οργανισμούς ή άτομα. Στα αξιοσημείωτα παραδείγματα περιλαμβάνονται το σκουλήκι Stuxnet, που ανακαλύφθηκε το 2010 και είχε ως στόχο τις πυρηνικές εγκαταστάσεις του Ιράν, και η ομάδα Equation, μια APT που πιστεύεται ότι συνδέεται με την Εθνική Υπηρεσία Ασφαλείας (NSA) των Ηνωμένων Πολιτειών.Τελος τα exploits είναι έτοιμα να συνεχίσουν να εξελίσσονται σε πολυπλοκοτητα ,τροφοδοτούμενα απο την ανάπτυξη της τεχνολογίας και την αυξανόμενη επαγγελματοποίηση του εγκλήματος στον χώρο του κυβερνοχώρου.

Τι είναι τα security updates

Οι ενημερώσεις ασφαλείας είναι επιδιορθώσεις ή βελτιώσεις που κυκλοφορούν από τους προμηθευτές λογισμικού για την αντιμετώπιση γνωστών ευπαθειών, αδυναμιών ή σφαλμάτων στα προϊόντα τους. Αυτές οι ενημερώσεις είναι απαραίτητες για τη διατήρηση της ασφάλειας και της ακεραιότητας των συστημάτων λογισμικού, καθώς συμβάλλουν στην πρόληψη της εκμετάλλευσης από κακόβουλους φορείς και στην προστασία από πιθανές παραβιάσεις ή επιθέσεις ασφαλείας.

Και ο σημαντικός ρόλος τους

Η τακτική εφαρμογή ενημερώσεων ασφαλείας είναι άκρως σημαντική για τη διατήρηση της ασφάλειας και της ακεραιότητας των συστημάτων λογισμικού. Αυτές οι ενημερώσεις, που κυκλοφορούν από τους προμηθευτές λογισμικού, περιέχουν διορθώσεις που αντιμετωπίζουν γνωστές ευπάθειες, αδυναμίες ή σφάλματα στα προϊόντα τους. Με την εφαρμογή αυτών των ενημερώσεων, οι οργανισμοί και οι ιδιώτες μπορούν να μετριάσουν τον κίνδυνο εκμετάλλευσης από εγκληματίες του κυβερνοχώρου και άλλους κακόβουλους φορείς, μειώνοντας την έκθεση σε κινδύνους ασφαλείας και ελαχιστοποιώντας την πιθανότητα επιτυχών επιθέσεων. Επιπλέον, οι ενημερώσεις ασφαλείας συμβάλλουν στην προστασία ευαίσθητων δεδομένων, πνευματικής ιδιοκτησίας και άλλων πολύτιμων περιουσιακών στοιχείων από μη εξουσιοδοτημένη πρόσβαση ή χειραγώγηση, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ψηφιακών περιουσιακών στοιχείων. Τέλος, οι ενημερώσεις ασφαλείας μπορεί επίσης να περιλαμβάνουν βελτιώσεις επιδόσεων και βελτιώσεις σταθερότητας, βελτιστοποιώντας την απόδοση και την αξιοπιστία των συστημάτων λογισμικού και ελαχιστοποιώντας παράλληλα τον χρόνο διακοπής λειτουργίας. Συνολικά, η τακτική εφαρμογή ενημερώσεων ασφαλείας είναι ζωτικής σημασίας για την προστασία από τις εξελισσόμενες απειλές στον κυβερνοχώρο και τη διατήρηση μιας ισχυρής στάσης ασφαλείας.

Τρόποι για να μείνουμε προστατευμένοι απο exploits

Η εξασφάλιση ισχυρής άμυνας κατά των exploits απαιτεί την εφαρμογή πολύπλευρων μέτρων ασφαλείας και την κατανόηση των τεχνικών εννοιών. Κεντρικό ρόλο σε αυτή την άμυνα παίζει η συνεπής εφαρμογή ενημερώσεων λογισμικού σε όλα τα συστήματα και στοιχεία, που περιλαμβάνουν λειτουργικά συστήματα, εφαρμογές, plugins και firmware. Η έγκαιρη εγκατάσταση των διορθωτικών εκδόσεων ασφαλείας είναι ζωτικής σημασίας για τον μετριασμό των γνωστών ευπαθειών, αποτρέποντας έτσι τις πιθανές οδούς εκμετάλλευσης από τους επιτιθέμενους στον κυβερνοχώρο. Αυτή η

προληπτική στάση συμπληρώνεται από την ανάπτυξη αξιόπιστων λύσεων antivirus/antimalware, ενισχυμένων με συμπληρωματικά εργαλεία ασφαλείας, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών (IDS) και αποκλειστές διαφημίσεων. Αυτοί οι μηχανισμοί οχυρώνουν συλλογικά την ψηφιακή περίμετρο, εντοπίζοντας και αναχαιτίζοντας ενεργά τα κακόβουλα φορτία προτού μπορέσουν να θέσουν σε κίνδυνο την ακεραιότητα του συστήματος.

2.2.3 Τι είναι τα APTs (Advanced Persistent Threats)

Τα APTs(εξελιγμενες επιμονες απειλες) είναι νεες και μυστικές επιθέσεις στον κυβερνοχώρο που διεξάγονται από αντιπάλους με επαρκείς πόρους, όπως εθνικούς-κρατικούς παράγοντες, οργανωμένες ομάδες κυβερνοεγκληματιών ή κρατικά χρηματοδοτούμενες συλλογικότητες χάκερ. Σε αντίθεση με τις παραδοσιακές επιθέσεις στον κυβερνοχώρο, οι οποίες μπορεί να έχουν ευκαιριακό ή αδιάκριτο χαρακτήρα, οι APTs χαρακτηρίζονται από τη μεθοδική και στοχευμένη προσέγγισή τους, που συχνά διαρκεί εβδομάδες, μήνες ή ακόμη και χρόνια.

Αντιμετώπιση

Η αντιμετώπιση των προηγμένων επίμονων απειλών (APTs) απαιτεί μια ολοκληρωμένη και πολυεπίπεδη προσέγγιση που αντιμετωπίζει τόσο τις τεχνικές ευπάθειες όσο και τους ανθρώπινους παράγοντες. Για να μετριάσουν τον κίνδυνο διείσδυσης APTs, οι οργανισμοί θα πρέπει να δώσουν προτεραιότητα σε αρκετά μέτρα. Αρχικά, η εφαρμογή ισχυρής άμυνας κυβερνοασφάλειας, συμπεριλαμβανομένων των firewalls επόμενης γενιάς, των συστημάτων ανίχνευσης εισβολών και των πλατφορμών προστασίας τελικών σημείων, μπορεί να συμβάλει στον εντοπισμό και τον αποκλεισμό δραστηριοτήτων που σχετίζονται με APTs. Επιπλέον, οι τακτικές αξιολογήσεις ασφαλείας και οι δοκιμές διείσδυσης μπορούν να εντοπίσουν και να αποκαταστήσουν τα τρωτά σημεία πριν αυτά αξιοποιηθούν από τους φορείς APT. Επίσης, η ανάπτυξη προηγμένων λύσεων πληροφοριών απειλών μπορεί να παρέχει πολύτιμες πληροφορίες σχετικά με τις αναδυόμενες απειλές και τις τακτικές APT, επιτρέποντας το προληπτικό κυνήγι απειλών και την αντιμετώπιση περιστατικών. Παράλληλα με τις τεχνικές άμυνες, η επένδυση σε προγράμματα εκπαίδευσης και

ευαισθητοποίησης των εργαζομένων μπορεί να ενισχύσει την ανθεκτικότητα έναντι επιθέσεων κοινωνικής μηχανικής που σχετίζονται με APTs, όπως το spear phishing.

2.2.4 Pass the Hass

Το "Pass the hash" (PtH) αποτελεί μια εξελιγμένη τεχνική κυβερνοεπίθεσης που χρησιμοποιείται από αντιπάλους για τη διείσδυση σε συστήματα υπολογιστών, κυρίως σε περιβάλλοντα που βασίζονται στα Windows. Η μέθοδος αυτή αξιοποιεί εγγενείς ευπάθειες στο πρωτόκολλο ελέγχου ταυτότητας των Windows για την παράκαμψη των παραδοσιακών μηχανισμών ελέγχου ταυτότητας με κωδικό πρόσβασης, παρέχοντας μη εξουσιοδοτημένη πρόσβαση και αυξημένα προνόμια. Αρχικά, οι επιτιθέμενοι συλλέγουν κατακερματισμούς(hashes) κωδικών πρόσβασης προνομιούχων χρηστών με διάφορα μέσα, όπως η απόσπαση μνήμης, η υποκλοπή δικτύου ή η εκμετάλλευση ευπαθειών του συστήματος. Αυτές οι κατακερματισμένες αναπαραστάσεις των κωδικών πρόσβασης χρησιμεύουν ως κρυπτογραφικές αναπαραστάσεις που αποθηκεύονται στις βάσεις δεδομένων ασφαλείας του συστήματος. Αντί να αυθεντικοποιούνται με τον κωδικό πρόσβασης απλού κειμένου, οι αντίπαλοι εκμεταλλεύονται αδυναμίες στη διαδικασία αυθεντικοποίησης μεταδίδοντας απευθείας τον κλεμμένο κατακερματισμένο κωδικό πρόσβασης. Με τον τρόπο αυτό παρακάμπτεται η ανάγκη γνώσης του πραγματικού κωδικού πρόσβασης, επιτρέποντας τη μη εξουσιοδοτημένη πρόσβαση στο σύστημα-στόχο με τα προνόμια του σχετικού χρήστη. Μόλις αποκτήσουν πρόσβαση, οι αντίπαλοι μπορούν να εκτελέσουν μια πληθώρα κακόβουλων δραστηριοτήτων, από την ανάπτυξη κακόβουλου λογισμικού έως τη διαρροή ευαίσθητων δεδομένων ή την περαιτέρω κλιμάκωση των προνομίων εντός της υποδομής δικτύου.

2.2.5 Hash Collection

Η συλλογή hashes περιλαμβάνει την απόκτηση hashes κωδικών πρόσβασης από συστήματα υπολογιστών ή δίκτυα, συνήθως στο πλαίσιο μιας επίθεσης στον κυβερνοχώρο ή μιας ανάλυσης ασφάλειας. Οι κατακερματισμοί κωδικών πρόσβασης, κρυπτογραφικές αναπαραστάσεις των κωδικών πρόσβασης των χρηστών, αποθηκεύονται συνήθως σε βάσεις δεδομένων ελέγχου ταυτότητας ή αρχεία συστήματος. Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους για τη συλλογή κατακερματισμών, όπως η παρακολούθηση δικτύων για την υποκλοπή πακέτων ελέγχου ταυτότητας, οι επιθέσεις pass-the-hash για την εξαγωγή κατακερματισμών από τη μνήμη ή τα αρχεία συστήματος, η απόρριψη τοπικών κατακερματισμών κωδικών

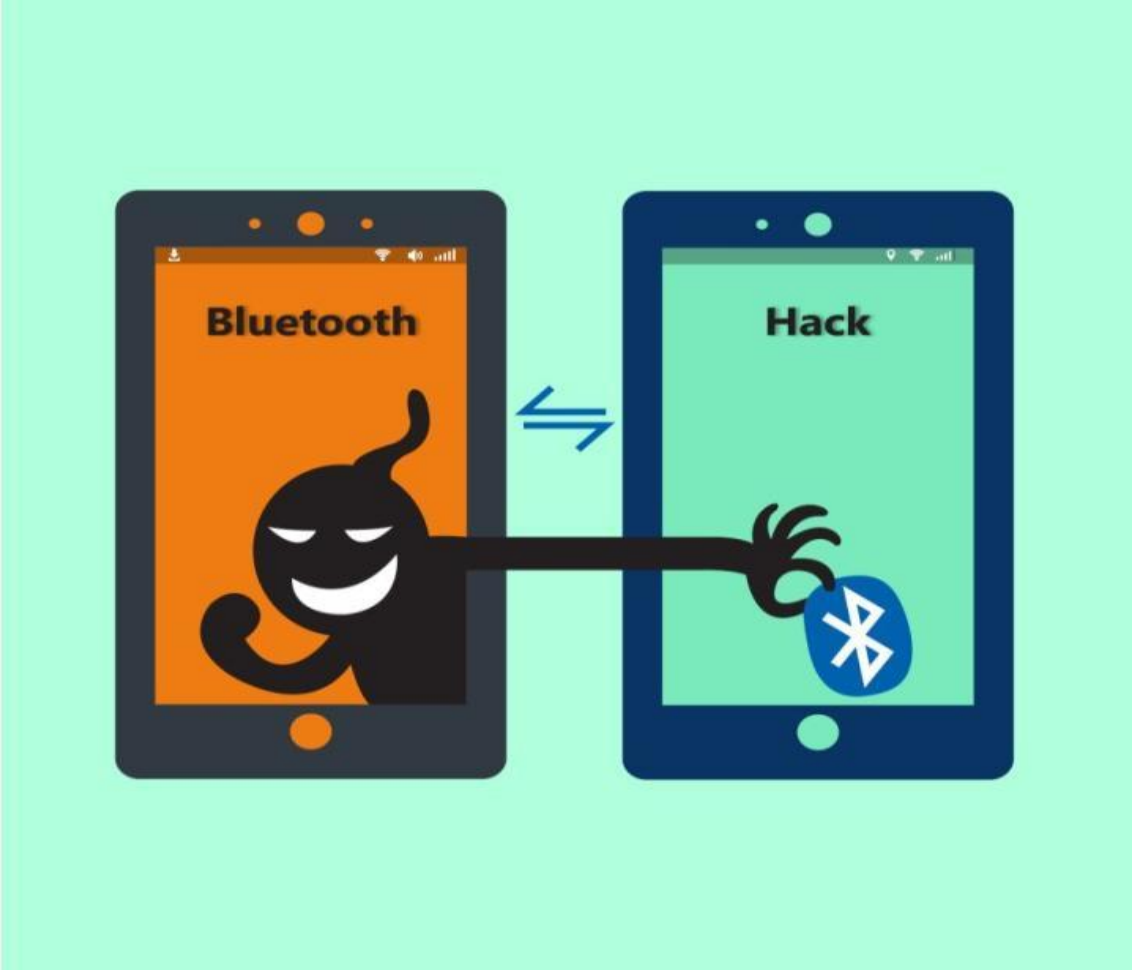
πρόσβασης από αποθήκες ελέγχου ταυτότητας, η εκμετάλλευση ευπαθειών λογισμικού ή η χρήση τακτικών κοινωνικής μηχανικής για να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν τα διαπιστευτήριά τους. Μόλις αποκτηθούν, οι επιτιθέμενοι μπορούν να προσπαθήσουν να σπάσουν τους κατακερματισμούς για να ανακτήσουν κωδικούς πρόσβασης απλού κειμένου ή να τους χρησιμοποιήσουν απευθείας σε επιθέσεις pass-the-hash για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα

2.3 Επίθεση Σε Κινητές Συσκευές

Η συλλογή hashes περιλαμβάνει την απόκτηση hashes κωδικών πρόσβασης από συστήματα υπολογιστών ή δίκτυα, συνήθως στο πλαίσιο μιας επίθεσης στον κυβερνοχώρο ή μιας ανάλυσης ασφάλειας. Οι κατακερματισμοί κωδικών πρόσβασης, κρυπτογραφικές αναπαραστάσεις των κωδικών πρόσβασης των χρηστών, αποθηκεύονται συνήθως σε βάσεις δεδομένων ελέγχου ταυτότητας ή αρχεία συστήματος. Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους για τη συλλογή κατακερματισμών, όπως η παρακολούθηση δικτύων για την υποκλοπή πακέτων ελέγχου ταυτότητας, οι επιθέσεις pass-the-hash για την εξαγωγή κατακερματισμών από τη μνήμη ή τα αρχεία συστήματος, η απόρριψη τοπικών κατακερματισμών κωδικών πρόσβασης από αποθήκες ελέγχου ταυτότητας, η εκμετάλλευση ευπαθειών λογισμικού ή η χρήση τακτικών κοινωνικής μηχανικής για να εξαπατήσουν τους χρήστες ώστε να αποκαλύψουν τα διαπιστευτήριά τους. Μόλις αποκτηθούν, οι επιτιθέμενοι μπορούν να προσπαθήσουν να σπάσουν τους κατακερματισμούς για να ανακτήσουν κωδικούς πρόσβασης απλού κειμένου ή να τους χρησιμοποιήσουν απευθείας σε επιθέσεις pass-the-hash για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα

2.3.1 Bluetooth Attacks

Το Bluetooth είναι η γνωστότερη ασύρματη τεχνολογία που τροφοδοτεί τα ακουστικά hands-free και συνδέει το τηλέφωνό με τον ήχο, την πλοήγηση και τα ηλεκτρονικά μέσα από το Διαδίκτυο των πραγμάτων (IoT). Όσο βολικό και αν είναι το Bluetooth για την παραγωγικότητα και την άνεση, μπορεί επίσης να παρουσιάζει σημαντικούς κινδύνους για την ασφάλεια. Παρά τους ήδη παρών αμυντικούς μηχανισμούς, η χρήση του Bluetooth μπορεί να προκαλέσει επιθέσεις στη συσκευή μέσω αρκετών τεχνικ΄χν και μεθόδων.



Εικόνα 2.3 Οι κίνδυνοι που κρύβει η χρήση του Bluetooth

Bluejacking (¨Μπλε γρύλλος¨)

Το Bluejacking είναι μια σχετικά αγαθή μορφή αλληλεπίδρασης στον κυβερνοχώρο που περιλαμβάνει την αποστολή ανεπιθύμητων μηνυμάτων ή επαγγελματικών καρτών σε συσκευές με δυνατότητα Bluetooth που βρίσκονται σε κοντινή απόσταση. Συνήθως, το bluejacking δεν περιλαμβάνει κακόβουλη πρόθεση, αλλά χρησιμοποιείται συχνά για παιχνιδιάρικους ή εμπορικούς σκοπούς. Η πρακτική αυτή απέκτησε δημοτικότητα στις

αρχές της δεκαετίας του 2000 ως ένας τρόπος για να στέλνουν άτομα ανώνυμα μηνύματα σε τηλέφωνα αγνώστων που βρίσκονται σε κοντινή απόσταση ως μια μορφή ακίνδυνης διασκέδασης. Ωστόσο, ενώ το bluejacking από μόνο του μπορεί να μην είναι εκ φύσεως επιβλαβές, αλλα ενδεχομένως μπορεί να χρησιμοποιηθεί ως πρόδρομος για πιο κακόβουλες επιθέσεις με βάση το Bluetooth, όπως το bluesnarfing ή η αλλοίωση δικτύου. Ως εκ τούτου, είναι σημαντικό για τους χρήστες να γνωρίζουν τις ρυθμίσεις Bluetooth και να είναι προσεκτικοί όταν λαμβάνουν απροσδόκητα μηνύματα από άγνωστες πηγές για να αποτρέψουν τυχόν κινδύνους για την ασφάλεια.

Bluesnarfing

Το Bluesnarfing αντιπροσωπεύει μια πιο κακόβουλη μορφή κυβερνοεπίθεσης που στοχεύει συσκευές με δυνατότητα Bluetooth, επιτρέποντας μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες όπως επαφές, μηνύματα κειμένου, ακόμη και μηνύματα ηλεκτρονικού ταχυδρομείου. Σε αντίθεση με το bluejacking, το οποίο είναι συνήθως ακίνδυνο και περιλαμβάνει την αποστολή μη ζητηθέντων μηνυμάτων, το bluesnarfing περιλαμβάνει την εκμετάλλευση ευπαθειών στις συνδέσεις Bluetooth για την κλοπή δεδομένων χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Οι κυβερνοεγκληματίες μπορούν να χρησιμοποιούν εξειδικευμένο λογισμικό και εργαλεία για να υποκλέπτουν και να εξάγουν δεδομένα από ευάλωτες συσκευές εντός εμβέλειας, συχνά χωρίς να αφήνουν ίχνη των δραστηριοτήτων τους. Αυτή η μορφή επίθεσης θέτει σε σημαντικούς κινδύνους την ιδιωτικότητα και την ασφάλεια, ιδίως καθώς πολλοί άνθρωποι χρησιμοποιούν το Bluetooth για κοινή χρήση αρχείων, ασύρματα ακουστικά και άλλες βολικές λειτουργίες.

Bluebugging

Σε αντίθεση με το bluejacking ή το bluesnarfing, τα οποία περιλαμβάνουν παθητική υποκλοπή ή κλοπή δεδομένων, το bluebagging επιτρέπει στους επιτιθέμενους να αναλάβουν τον πλήρη έλεγχο της συσκευής ενός θύματος, συχνά εν αγνοία του. Εκμεταλλευόμενοι αδυναμίες στα πρωτόκολλα ζεύξης Bluetooth, οι επιτιθέμενοι μπορούν να εξαπατήσουν τους χρήστες ώστε να συνδεθούν σε κακόβουλες συσκευές που εμφανίζονται ως νόμιμα αξεσουάρ ή δίκτυα. Μόλις συνδεθούν, ο επιτιθέμενος μπορεί να εκτελέσει εξ αποστάσεως εντολές, να εγκαταστήσει κακόβουλο λογισμικό ή να υποκλέψει ευαίσθητα δεδομένα από την παραβιασμένη συσκευή. Οι επιθέσεις

Bluebagging μπορεί να έχουν σοβαρές συνέπειες, που κυμαίνονται από κλοπή ταυτότητας και οικονομική απάτη έως κατασκοπεία και δολιοφθορά.

Bluesmack

Αυτή η επίθεση αξιοποιεί την ευαισθησία του πρωτοκόλλου Bluetooth στον κατακερματισμό πακέτων και την ασύγχρονη επικοινωνία, επιτρέποντας στους επιτιθέμενους να στέλνουν μια ροή ειδικά διαμορφωμένων πακέτων στη συσκευή στόχο. Ως αποτέλεσμα, η στοχευόμενη συσκευή υπερφορτώνεται, οδηγώντας σε κατάσταση άρνησης παροχής υπηρεσιών (DoS), όπου δεν ανταποκρίνεται ή καταρρέει. Οι επιθέσεις Bluesmack μπορούν να προκαλέσουν σημαντική διακοπή της παραγωγικότητας και της επικοινωνίας, ιδιαίτερα σε περιβάλλοντα όπου χρησιμοποιούνται εκτενώς συσκευές Bluetooth, όπως γραφεία, αεροδρόμια ή δημόσιοι χώροι.

2.3.2 Wi-Fi Attacks

Οι επιθέσεις WiFi περιλαμβάνουν ένα ευρύ φάσμα κακόβουλων δραστηριοτήτων που στοχεύουν ασύρματα δίκτυα, εκμεταλλευόμενες ευπάθειες σε πρωτόκολλα ή διαμορφώσεις δικτύου. Αυτές οι επιθέσεις, συμπεριλαμβανομένων των επιθέσεων Man-in-the-Middle, WiFi eavesdropping, Evil Twin, cracking κωδικού πρόσβασης, Denial of Service, packet injection, WiFi phishing και WPS PIN, ενέχουν σημαντικούς κινδύνους για τους χρήστες και τους οργανισμούς. Μπορούν να οδηγήσουν σε κλοπή δεδομένων, διακοπή του δικτύου και μη εξουσιοδοτημένη πρόσβαση.

Evil Twin (¨Σατανικό Δίδυμο¨)

Η επίθεση Evil Twin είναι μια παραπλανητική και κακόβουλη τακτική που στοχεύει σε δίκτυα WiFi, όπου ένας επιτιθέμενος εγκαθιστά ένα αθέμιτο ασύρματο σημείο πρόσβασης με όνομα παρόμοιο με ένα νόμιμο δίκτυο. Μιμούμενος το όνομα του

νόμιμου δικτύου (SSID), ο επιτιθέμενος εξαπατά τους ανυποψίαστους χρήστες ώστε να συνδεθούν αντί αυτού στο απατηλό σημείο πρόσβασης. Μόλις συνδεθεί, ο επιτιθέμενος μπορεί να υποκλέψει ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης και οικονομικά δεδομένα, που μεταδίδονται μέσω του δικτύου. Αυτός ο τύπος επίθεσης μπορεί να οδηγήσει σε κλοπή ταυτότητας, παραβιάσεις δεδομένων και οικονομικές απώλειες.

Wifi eavesdropping

Η υποκλοπή WiFi είναι μια μυστική μέθοδος επίθεσης στον κυβερνοχώρο, όπου κακόβουλοι φορείς παρακολουθούν παθητικά την κυκλοφορία ασύρματων δικτύων για να υποκλέψουν ευαίσθητες πληροφορίες που μεταδίδονται μέσω μη κρυπτογραφημένων συνδέσεων. Εκμεταλλευόμενοι ευπάθειες σε πρωτόκολλα WiFi, οι επιτιθέμενοι μπορούν να υποκλέψουν πακέτα δεδομένων που περιέχουν διαπιστευτήρια σύνδεσης, οικονομικές πληροφορίες ή άλλα εμπιστευτικά δεδομένα. Αυτή η μορφή επίθεσης είναι ιδιαίτερα ανησυχητική στα δημόσια WiFi hotspots, όπου οι χρήστες μπορεί να μεταδίδουν άθελά τους ευαίσθητα δεδομένα χωρίς κρυπτογράφηση, αφήνοντάς τα ευάλωτα σε υποκλοπή. Η υποκλοπή WiFi μπορεί να οδηγήσει σε κλοπή ταυτότητας, οικονομική απάτη και μη εξουσιοδοτημένη πρόσβαση σε προσωπικά ή εταιρικά δίκτυα

Μεσολαβητής (Man in the middle)

Μια επίθεση Man in the Middle (MitM) είναι μια εξελιγμένη απειλή στον κυβερνοχώρο που στοχεύει σε δίκτυα WiFi, όπου ένας εισβολέας υποκλέπτει την επικοινωνία μεταξύ δύο μερών εν αγνοία τους. Σε αυτόν τον τύπο επίθεσης, ο επιτιθέμενος τοποθετείται μεταξύ της συσκευής του θύματος και του προοριζόμενου προορισμού, ενεργώντας ως αναμεταδότης για τη σύλληψη και τη δυνητική χειραγώγηση των δεδομένων που μεταδίδονται μέσω του δικτύου. Αξιοποιώντας ευπάθειες σε πρωτόκολλα κρυπτογράφησης WiFi ή παραβιάζοντας συσκευές δικτύου, ο επιτιθέμενος μπορεί να υποκλέψει ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, οικονομικά δεδομένα ή προσωπικές επικοινωνίες. Οι επιθέσεις MitM μπορούν να συμβούν σε διάφορα σενάρια, συμπεριλαμβανομένων των δημόσιων δικτύων WiFi, όπου οι χρήστες εν αγνοία τους συνδέονται σε μη ασφαλή δίκτυα, καθιστώντας τα ευάλωτα σε υποκλοπές.

2.3.3 Tracking Services

Η χρήση των υπηρεσιών παρακολούθησης, ενώ συχνά είναι επωφελής για προσωπικούς ή οργανωτικούς σκοπούς, μπορεί επίσης να επιφέρει ευπάθειες και κινδύνους για την προστασία της ιδιωτικής ζωής, εάν αξιοποιηθεί κακόβουλα. Οι επιτιθέμενοι μπορούν να αξιοποιήσουν τις υπηρεσίες εντοπισμού για να παρακολουθούν τις κινήσεις των ατόμων, να συλλέγουν ευαίσθητα δεδομένα θέσης ή ακόμη και να διευκολύνουν τη φυσική παρακολούθηση ή παρενόχληση. Αξιοποιώντας ευπάθειες σε εφαρμογές εντοπισμού ή παραβιάζοντας λογαριασμούς χρηστών, οι επιτιθέμενοι μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε δεδομένα θέσης και να παρακολουθούν άτομα χωρίς τη συγκατάθεσή τους. Αυτό μπορεί να οδηγήσει σε παραβίαση της ιδιωτικής ζωής, παρενόχληση, ή ακόμη και σε σωματική βλάβη σε ακραίες περιπτώσεις. Επιπλέον, η συλλογή και η κατάχρηση δεδομένων θέσης από κακόβουλους φορείς μπορεί να έχει εκτεταμένες συνέπειες, όπως κλοπή ταυτότητας,εκβιασμό ή στοχευμένη διαφήμιση.

2.4 Distributed Denial Of Service attack(Επίθεση Αρνησης Υπηρεσίας)

Μια επίθεση κατανεμημένης άρνησης εξυπηρέτησης (Distributed Denial of Service,DDOS), είναι ένας τύπος κυβερνοεπίθεσης όπου πολλαπλά συστήματα που έχουν παραβιαστεί, τα οποία συχνά είναι μολυσμένα με κακόβουλο λογισμικό, χρησιμοποιούνται για να στοχεύσουν ένα μόνο σύστημα ή δίκτυο. Ο στόχος μιας επίθεσης DDoS είναι να υπερφορτώσει το στοχευμένο σύστημα με μια πλημμύρα διαδικτυακής κίνησης, καθιστώντας το ανίκανο να ανταποκριθεί σε νόμιμα αιτήματα. Αυτό μπορεί να οδηγήσει σε άρνηση παροχής υπηρεσιών για τους χρήστες που προσπαθούν να αποκτήσουν πρόσβαση στο στοχευμένο σύστημα ή δίκτυο. Οι επιθέσεις DDoS μπορούν να ποικίλουν σε κλίμακα και πολυπλοκότητα, από σχετικά απλές επιθέσεις που εξαπολύονται από μεμονωμένα άτομα έως εξαιρετικά συντονισμένες επιθέσεις που οργανώνονται από εξειδικευμένους χάκερ ή ομάδες κυβερνοεγκληματιών.

Εικόνα 2.4 DDOS Επιθέσεις

2.4.1 Επιθέσεις Μεγάλου Ογκου

Οι επιθέσεις όγκου είναι μια κατηγορία κυβερνοεπιθέσεων που αποσκοπούν στην υπερφόρτωση ενός συστήματος ή δικτύου-στόχου με τεράστιο όγκο κίνησης ή δεδομένων.

2.4.2 Protocol Attack

Η επίθεση πρωτοκόλλου, γνωστή και ως επίθεση βάσει πρωτοκόλλου, είναι ένας τύπος κυβερνοεπίθεσης που εκμεταλλεύεται ευπάθειες ή αδυναμίες σε πρωτόκολλα δικτύου για να διαταράξει ή να θέσει σε κίνδυνο τις επικοινωνίες δικτύου. Σε αντίθεση με τις ογκομετρικές επιθέσεις, οι οποίες αποσκοπούν στην υπερφόρτωση ενός στόχου με

μεγάλο όγκο κίνησης, οι επιθέσεις πρωτοκόλλου στοχεύουν στα πρωτόκολλα που χρησιμοποιούνται για τη μετάδοση δεδομένων σε δίκτυα.

2.4.3 Application Layer Attacks

Οι επιθέσεις DDoS σε επίπεδο εφαρμογής αποτελούν μια εξελιγμένη κυβερνοαπειλή που στοχεύει το ανώτερο επίπεδο του μοντέλου OSI, με σκοπό να διακόψει την παροχή υπηρεσιών ιστού και εφαρμογών. Αντίθετα από τις παραδοσιακές επιθέσεις DDoS που κατακλύζουν τα δίκτυα με κίνηση, αυτές είναι πιο κακόβουλες, επιδιώκοντας να εξαντλήσουν τους πόρους του διακομιστή και τη λειτουργικότητα των εφαρμογών, συχνά αφήνοντας τα συστήματα υπερφορτωμένα και τις υπηρεσίες μη διαθέσιμες.

2.4.4 UDP/ICMP Flood

Οι επιθέσεις UDP (User Datagram Protocol) και οι επιθέσεις ICMP (Internet Control Message Protocol) είναι τακτικές που χρησιμοποιούνται συνήθως στις επιθέσεις DDoS (Distributed Denial of Service). Στις επιθέσεις UDP, οι δράστες κατακλύζουν το δίκτυο-στόχο με σημαντικό όγκο πακέτων UDP, εκμεταλλευόμενοι τη φύση του πρωτοκόλλου χωρίς σύνδεση και συχνά παραποιώντας τις διευθύνσεις IP προέλευσης για να ενισχύσουν τον αντίκτυπο της επίθεσης. Αυτή η πλημμύρα πακέτων υπερκαλύπτει τους πόρους του δικτύου του θύματος, οδηγώντας σε διακοπή των υπηρεσιών για τους νόμιμους χρήστες. Εν τω μεταξύ, οι επιθέσεις ICMP περιλαμβάνουν τη μετάδοση μεγάλου όγκου πακέτων ICMP, κοινώς γνωστών ως " ping packets ", τα οποία μπορούν να καταναλώσουν εύρος ζώνης δικτύου και να υπερφορτώσουν τις συσκευές δικτύου.

Και οι δύο τύποι επιθέσεων έχουν ως στόχο να καταστήσουν τον στόχο μη προσβάσιμο στους νόμιμους χρήστες.

2.4.5 SYN/Ping of Death Flood

Οι επιθέσεις βάσει πρωτοκόλλου, όπως οι πλημμύρες SYN, οι επιθέσεις Smurf και οι επιθέσεις Ping of Death, αντιπροσωπεύουν διαφορετικές μεθόδους στο οπλοστάσιο των εισβολέων DDoS. Στις πλημμύρες SYN, ο επιτιθέμενος στέλνει έναν καταιγισμό αιτήσεων TCP SYN στον διακομιστή του θύματος, αλλά δεν ολοκληρώνει τη διαδικασία χειραψίας, εξαντλώντας τους πόρους του διακομιστή και εμποδίζοντας τη δημιουργία νόμιμων συνδέσεων. Οι επιθέσεις Smurf κάνουν κατάχρηση του ICMP, στέλνοντας μεγάλο αριθμό πακέτων ICMP echo request (pings) σε διευθύνσεις εκπομπής IP, με τη διεύθυνση πηγής παραποιημένη ώστε να εμφανίζεται ως η διεύθυνση του θύματος. Αυτό αναγκάζει όλες τις συσκευές στο δίκτυο να απαντήσουν στην IP του θύματος, υπερφορτώνοντας τους πόρους του. Το Ping of Death εκμεταλλεύεται ευπάθειες στο πρωτόκολλο ICMP στέλνοντας κακοσχηματισμένα ή υπερμεγέθη πακέτα στο θύμα, οδηγώντας σε υπερχειλίσεις buffer και καταρρεύσεις.

2.4.6 Slowloris

Το Slowloris είναι ένα ύπουλο και έξυπνο εργαλείο επίθεσης DDoS σε επίπεδο εφαρμογής, σχεδιασμένο να εξαντλεί τους πόρους ενός στοχευμένου διακομιστή ιστού. Σε αντίθεση με τις παραδοσιακές επιθέσεις πλημμύρας που κατακλύζουν τον διακομιστή με μεγάλο όγκο αιτημάτων, το Slowloris λειτουργεί εγκαθιστώντας και διατηρώντας μεγάλο αριθμό συνδέσεων HTTP στον διακομιστή, αλλά στέλνοντας κεφαλίδες HTTP

πολύ αργά, σε μικροσκοπικά βήματα. Με τον τρόπο αυτό, διατηρεί τις συνδέσεις ανοιχτές για όσο το δυνατόν περισσότερο χρόνο, δεσμεύοντας διαθέσιμους πόρους του διακομιστή, όπως υποδοχές και νήματα. Το Slowloris δεν απαιτεί τεράστιο αριθμό επιτιθέμενων μηχανών αντίθετα, μπορεί να ξεκινήσει από μία μόνο μηχανή, καθιστώντας δύσκολη την ανίχνευση και τον μετριασμό του.

2.4.7 Enhanced NTP

Οι επιθέσεις ενίσχυσης NTP (Network Time Protocol) εκμεταλλεύονται ευπάθειες στην υπηρεσία NTP για την εξαπόλυση ισχυρών επιθέσεων κατανεμημένης άρνησης παροχής υπηρεσιών (DDoS). Σε μια επίθεση ενίσχυσης NTP, ο επιτιθέμενος στέλνει ένα μικρό πακέτο αίτησης με πλαστή διεύθυνση IP πηγής σε πολλούς διακομιστές NTP με δημόσια πρόσβαση. Αυτοί οι διακομιστές, οι οποίοι είναι ρυθμισμένοι να απαντούν με ένα πολύ μεγαλύτερο πακέτο απάντησης, ενισχύουν ακούσια τον όγκο της κίνησης που κατευθύνεται προς το θύμα, υπερφορτώνοντας τους πόρους του δικτύου του. Αυτή η μέθοδος επίθεσης εκμεταλλεύεται τον μεγάλο παράγοντα ενίσχυσης των απαντήσεων NTP, με αποτέλεσμα συχνά να αυξάνεται σημαντικά η κίνηση που κατευθύνεται στο θύμα σε σύγκριση με το αρχικό αίτημα.

2.4.8 HTTP Flood

Η κατάκλυση HTTP είναι ένας τύπος κατανεμημένης επίθεσης άρνησης παροχής υπηρεσιών (DDoS) που στοχεύει σε διακομιστές ιστού κατακλύζοντάς τους με μεγάλο όγκο αιτημάτων HTTP. Αυτός ο κατακλυσμός αιτημάτων υπερκαλύπτει τους πόρους του διακομιστή, όπως η CPU, η μνήμη και το εύρος ζώνης δικτύου, με αποτέλεσμα να γίνεται

αργός ή να μην ανταποκρίνεται και να αρνείται την εξυπηρέτηση των νόμιμων χρηστών. Οι κατακλύσεις HTTP μπορούν να εξαπολυθούν χρησιμοποιώντας botnets ή δίκτυα παραβιασμένων συσκευών που ελέγχονται από τον επιτιθέμενο. Αυτές οι επιθέσεις μπορούν να στοχεύουν συγκεκριμένες διευθύνσεις URL ή ολόκληρο το διακομιστή ιστού, ανάλογα με τους στόχους του επιτιθέμενου. Οι κατακλύσεις HTTP χαρακτηρίζονται συχνά από την ικανότητά τους να παράγουν τεράστιο όγκο κίνησης από ένα ευρύ φάσμα πηγών, γεγονός που καθιστά δύσκολο τον μετριασμό τους. Για την άμυνα κατά των πλημμυρών HTTP, οι διαχειριστές διακομιστών ιστού μπορούν να εφαρμόσουν μέτρα όπως ο περιορισμός του ρυθμού, η επικύρωση αιτήσεων, η προσωρινή αποθήκευση και η χρήση δικτύων παράδοσης περιεχομένου (CDN) για τη διανομή και την απορρόφηση της κυκλοφορίας.

2.4.9 Zero-Day Attack

Η επίθεση zero-day αναφέρεται σε μια κυβερνοεπίθεση που εκμεταλλεύεται μια μέχρι πρότινος άγνωστη ευπάθεια ή ευπάθεια " zero-day " σε software ή hardware. Αυτές οι ευπάθειες ονομάζονται " zero-day " επειδή αξιοποιούνται από τους επιτιθέμενους πριν οι προγραμματιστές του επηρεαζόμενου λογισμικού ή υλικού προλάβουν να κυκλοφορήσουν ένα patch ή μια διόρθωση. Οι ευπάθειες zero-day μπορεί να υπάρχουν σε λειτουργικά συστήματα, προγράμματα περιήγησης στο διαδίκτυο, εφαρμογές ή ακόμη και σε υλικολογισμικό.

2.5 Συμπεράσματα

Σε αυτό το κεφάλαιο οι επιθέσεις που αναφέρθηκαν είναι πολλές αλλά είναι μόνο τα βασικά στον κόσμο του hacking. Αυτό αποδεικνύεται καθώς άμα κάποιος κάνει μια έρευνα πάνω στην κάθε μια υποκατηγορία που αναλύθηκε, θα βρει ολόκληρα βιβλία αναλύοντας σχολαστικά τις επιθέσεις. Επιπλέον ένα θέμα σχολιασμού είναι ότι χρονο με τον χρόνο βγαίνουν στο ¨φώς¨ νέες τεχνολογίες και νέες μέθοδοι για επιθέσεις καθώς η τεχνολογία κάθε μέρα εξελίσσεται.

Στο επόμενο κεφάλαιο θα γίνει χρήση και αναφορά αρκετών εργαλειών που χρησιμοποιεί ένας χακερ, προκειμένου να εκτελέσει πολλές απο τις περιπτώσεις επιθέσεων που αναφερθηκαν σε αυτο το κεφάλαιο μεσα απο την χρήση ενος lab.

3 Παραδείγματα Επιθέσεων(attack scenarios)

3.1 Χρήσιμα Εργαλεία

Εισαγωγή στα Εργαλεία Δοκιμών Διείσδυσης

Στον τομέα του ηθικού χάκινγκ, ένα κρίσιμο στοιχείο βρίσκεται στο οπλοστάσιο των εργαλείων που χρησιμοποιούν οι ηθικοί χάκερ για την αξιολόγηση και βελτίωση της ασφάλειας των συστημάτων. Αυτά τα εργαλεία, γνωστά ως εργαλεία δοκιμών διείσδυσης ή εργαλεία pentesting, λειτουργούν ως τα μέσα μέσω των οποίων ανακαλύπτονται, αναλύονται και μετριάζονται οι ευπάθειες. Η δοκιμή διείσδυσης αποτελεί μια προσομοιωμένη κυβερνοεπίθεση ενάντια στο σύστημα υπολογιστών σας για τον έλεγχο ευπαθειών που μπορούν να εκμεταλλευτούν, στο πλαίσιο της ασφάλειας διαδικτυακών εφαρμογών, για παράδειγμα.

Αυτά τα εργαλεία είναι ουσιαστικά στην "εργαλειοθήκη" του ηθικού χάκερ για πολλούς λόγους. Καταρχάς, παρέχουν έναν τρόπο για την αξιολόγηση της ασφαλιστικής στάσης των δικτύων, συστημάτων και "Ψηφιακών Συστημάτων", στην δικία μας περίπτωση, με έναν ελεγχόμενο και ασφαλή τρόπο. Αυτή η αξιολόγηση είναι κρίσιμη για τον εντοπισμό αδυναμιών και ευπαθειών που θα μπορούσαν να εκμεταλλευτούν οι κακόβουλοι χάκερς. Δεύτερον, τα εργαλεία pen-testing βοηθούν στην κατανόηση του πώς διαμορφώνονται και εκτελούνται οι στρατηγικές επίθεσης, επιτρέποντας έτσι την ανάπτυξη ισχυρών μηχανισμών άμυνας.

Το ευρως τον εργαλείων δοκιμών διείσδυσης είναι ποικίλο, περιλαμβάνοντας μια ευρεία γκάμα λειτουργικοτήτων - από τον καταλογισμό δικτύων και την σάρωση ευπαθειών έως την παραβίαση κωδικών πρόσβασης και την εκμετάλλευση διαδικτυακών εφαρμογών. Κάθε εργαλείο έχει τα δικά του μοναδικά χαρακτηριστικά και ειδικεύεται σε διαφορετικούς τομείς της κυβερνοασφάλειας. Για παράδειγμα, εργαλεία όπως το Nmap και το Wireshark είναι κρίσιμα για την ανάλυση δικτύων, ενώ το Metasploit και το Burp Suite επικεντρώνονται περισσότερο στην εκμετάλλευση ευπαθειών και στις δοκιμές διαδικτυακών εφαρμογών, αντίστοιχα. (Υπάρχουν πρακτικά παραδείγματα παρακάτω.)

Είναι σημαντικό να σημειωθεί ότι η χρήση αυτών των εργαλείων απαιτεί όχι μόνο τεχνική επάρκεια αλλά και την τήρηση των ηθικών προτύπων και των νομικών ορίων. Οι ηθικοί χάκερ πρέπει να διασφαλίσουν ότι οι δραστηριότητές τους έχουν εξουσιοδοτηθεί και ότι σέβονται την ιδιωτικότητα και την ακεραιότητα των δεδομένων και των συστημάτων.

Στις ακόλουθες ενότητες, θα εμβαθύνουμε σε μερικά από τα πιο δημοφιλή και ευρέως χρησιμοποιούμενα εργαλεία δοκιμών διείσδυσης στον τομέα του “Cyber Security”. "Αυτά τα εργαλεία αποτελούν τον "κορμό" του ηθικού χάκινγκ, επιτρέποντας στους επαγγελματίες να προστατεύσουν τα συστήματα και τα δίκτυα από πιθανές απειλές και παραβιάσεις.

Επισκόπηση Δημοφιλών Εργαλείων Δοκιμής Διείσδυσης

3.1.1 Metasploitable Linux

Μια έκδοση του Metasploit Framework που δημιουργήθηκε ειδικά για να τρέχει σε λειτουργικά συστήματα Linux ονομάζεται Metasploit for Linux. Παρέχει στους ειδικούς σε θέματα ασφάλειας και στους ερευνητές μια πλήρη εργαλειοθήκη για δοκιμές διείσδυσης και αξιολόγηση ευπαθειών σε συστήματα που βασίζονται σε Linux, με τις ίδιες ισχυρές δυνατότητες με το κανονικό Metasploit Framework. Λόγω της μεγάλης ποικιλίας ωφέλιμων φορτίων, βοηθητικών ενοτήτων, exploits και δυνατοτήτων post-

exploitation, το Metasploit for Linux διευκολύνει την εύρεση και εκμετάλλευση κενών ασφαλείας, γεγονός που συμβάλλει στη βελτίωση της άμυνας κυβερνοασφάλειας για περιβάλλοντα Linux.

3.1.2 Kali Linux

Το Kali Linux είναι μια εξειδικευμένη κατανομή (Distribution) Linux που έχει αναπτυχθεί με επίκεντρο την ασφάλεια πληροφορικής και το ηθικό χάκινγκ. Δημιουργήθηκε από την Offensive Security και αποτελεί τη διάδοχο κατάσταση του BackTrack, μιας προηγούμενης διανομής με παρόμοιο στόχο. Σχεδιασμένο κυρίως για επαγγελματίες στον τομέα του ηθικού χάκινγκ και τις δοκιμές διείσδυσης, το Kali Linux περιλαμβάνει εκατοντάδες εργαλεία ασφαλείας που καλύπτουν μια πληθώρα λειτουργιών, όπως είναι η δοκιμή διείσδυσης, η κρυπτογραφία, η διαχείριση και ανάλυση δεδομένων, καθώς και επιθέσεις σε παθητικά και ενεργά συστήματα.

Χρησιμοποιείται ευρέως στον τομέα της εκπαίδευσης και της επαγγελματικής ανάπτυξης στην ασφάλεια πληροφορικής, καθώς και για την διενέργεια δοκιμών διείσδυσης σε δίκτυα και συστήματα. Επίσης, αποτελεί ένα βασικό εργαλείο στην έρευνα ασφαλείας. Υπάρχει μια ενεργή κοινότητα γύρω από το Kali Linux, η οποία παρέχει τακτικές ενημερώσεις και υποστήριξη, καθώς και εκτεταμένη τεκμηρίωση και εκπαιδευτικό υλικό για τους χρήστες του.

Η σημασία του Kali Linux στον χώρο της ασφάλειας πληροφορικής δεν μπορεί να υποτιμηθεί. Αναγνωρίζεται ως ένα από τα πιο σημαντικά εργαλεία για τους επαγγελματίες ασφάλειας, χάρη στην ευελιξία του, την πληθώρα δυνατοτήτων που προσφέρει και την ευρεία υποστήριξη που διαθέτει. Στις επόμενες ενότητες, θα εξετάσουμε πιο λεπτομερώς μερικά από τα βασικά εργαλεία που προσφέρει το Kali Linux και τις εφαρμογές τους στον τομέα της ασφάλειας πληροφορικής.

3.1.3 Metasploit

Ερευνητές και ειδικοί σε θέματα ασφάλειας χρησιμοποιούν το πρόγραμμα δοκιμών διείσδυσης Metasploit Framework ανοιχτού κώδικα για να εντοπίζουν και να εκμεταλλεύονται τις αδυναμίες των συστημάτων υπολογιστών. Εκτός από τα payloads, τις βοηθητικές ενότητες, τα post-exploitation modules και τα exploits, προσφέρει μια εκτεταμένη συλλογή modules για την ανακάλυψη δραστηριοτήτων, την εκμετάλλευση και την παρακολούθηση. Παρέχοντας μια ενιαία πλατφόρμα για αναγνώριση, επίθεση και ανάλυση, το Metasploit απλοποιεί τη διαδικασία δοκιμής και επαλήθευσης των μέτρων ασφαλείας, συμβάλλοντας τελικά στην ενίσχυση της άμυνας του συστήματος και της συνολικής στάσης ασφαλείας.

3.1.4 SQLmap

Το SQLMap είναι ένα ανοικτού κώδικα εργαλείο εκμετάλλευσης ευπαθειών SQL σε ιστοσελίδες και εφαρμογές βάσεων δεδομένων. Χρησιμοποιείται συχνά από επαγγελματίες Ethical Hacking για να διαπιστώσουν την ασφάλεια ιστοσελίδων και εφαρμογών και να εντοπίσουν ευπαθείς σημεία που μπορούν να εκμεταλλευτούν κακόβουλοι χακερς. Λειτουργεί εξερευνώντας αυτόματα μια ιστοσελίδα ή μια εφαρμογή για ευπαθειες στις βασεις δεδομένων. Μπορεί να εντοπίσει, να εκμεταλλευτεί και να εξαγάγει δεδομένα από τις βάσεις δεδομένων, συμπεριλαμβανομένων ονομάτων πινάκων, στηλών, καταχωρήσεων και πολλών άλλων.

3.1.5 Nmap

Το Nmap είναι ένα από τα πιο δημοφιλή εργαλεία σάρωσης δικτύου που χρησιμοποιούνται στον κόσμο του Ethical Hacking. Αρχικά κυκλοφόρησε το 1997 και από τότε έχει γίνει ένα από τα πιο ισχυρά και ευέλικτα εργαλεία για ανάλυση δικτύου. Ο βασικός στόχος του Nmap είναι να εντοπίζει συσκευές σε ένα δίκτυο και να αναλύει τις υπηρεσίες που παρέχουν αυτές οι συσκευές. Αυτό μπορεί να γίνει μέσω διαφόρων τεχνικών όπως η σάρωση πόρτας, η αναγνώριση λειτουργικού συστήματος, η αναγνώριση των εκδόσεων των υπηρεσιών και πολλά άλλα. Έχει επίσης τη δυνατότητα να εκτελεί αυτοματοποιημένες επιθέσεις όπως η σύντομη σάρωση θυρών (Port Scanning) και η εκτέλεση επιθέσεων DOS. Το Nmap είναι διαθέσιμο για χρήση σε διάφορα λειτουργικά συστήματα και είναι ανοικτού κώδικα, προσφέροντας ένα ευέλικτο και προσαρμόσιμο περιβάλλον για ερευνητές ασφαλείας και επαγγελματίες Ethical Hacking. (Υπάρχει και πρακτικό παράδειγμα)

3.1.6 Wireshark

Το Wireshark είναι ένα εργαλείο ανάλυσης πακέτων δικτύου που χρησιμοποιείται ευρέως στον χώρο του Ethical Hacking. Ξεκίνησε ως ένα πρόγραμμα με το όνομα Ethereal το 1998, αλλά μετονομάστηκε σε Wireshark το 2006. Το Wireshark επιτρέπει

στους χρήστες να αναλύσουν την κίνηση δικτύου σε πραγματικό χρόνο ή από καταγεγραμμένα αρχεία πακέτων. Μπορεί να αναγνωρίσει και να ερμηνεύσει ποικίλα πρωτόκολλα δικτύου και να παρουσιάσει τα δεδομένα με διάφορους τρόπους, συμπεριλαμβανομένων γραφικών και διαγραμμάτων. Το Wireshark επιτρέπει στους "ερευνητές ασφαλείας" και τους επαγγελματίες Ethical Hacking να εντοπίζουν προβλήματα ασφαλείας, να ανιχνεύουν επιθέσεις και να ανακαλύπτουν αδυναμίες στο δίκτυο. Επιπλέον, το Wireshark είναι ανοικτού κώδικα και διατίθεται δωρεάν για χρήση, κάτι που το καθιστά προσιτό σε ερευνητές και επαγγελματίες ασφαλείας σε όλο τον κόσμο.

3.1.7 John the Ripper

Το εργαλείο John the Ripper είναι ένα κορυφαίο εργαλείο διάρρηξης κωδικών πρόσβασης, το οποίο χρησιμοποιείται ευρέως στους τομείς της κυβερνοασφάλειας και του ηθικού χάκινγκ. Αναπτύχθηκε από την Openwall Project και έχει γίνει ένα βασικό εργαλείο για τους επαγγελματίες ασφάλειας και τους ηθικούς χάκερς. Η κύρια λειτουργία του είναι η ανίχνευση αδύναμων κωδικών πρόσβασης, χρησιμοποιώντας διάφορες στρατηγικές διάρρηξης. Αυτή η ικανότητα το καθιστά ένα ανεκτίμητο εργαλείο για τον έλεγχο της ασφάλειας των κωδικών και την ενίσχυση των πολιτικών για τους "ισχυρούς κωδικούς".

Το λογισμικό λειτουργεί λαμβάνοντας λίστες γνωστών ή υποψήφιων κωδικών και χρησιμοποιώντας διάφορους αλγόριθμους για να προσπαθήσει να τους διαρρήξει. Υποστηρίζει πολλούς αλγορίθμους κρυπτογράφησης, γεγονός που το καθιστά ευέλικτο στην ικανότητά του να διαρρήξει κωδικούς που αποθηκεύονται σε διάφορες μορφές και συστήματα. Το εργαλείο John the Ripper είναι γνωστο για την ταχύτητα και την αποδοτικότητά του, ιδιαίτερα όταν χρησιμοποιείται με ισχυρό υλικό.

Ένα βασικό χαρακτηριστικό του John the Ripper είναι η δυνατότητά του για προσαρμοστικότητα και επέκταση. Οι πιο προχωρημένοι χρήστες μπορούν να τροποποιήσουν τη συμπεριφορά του επεξεργαζόμενοι τα αρχεία διαμόρφωσής του. Αυτή η προσαρμοστικότητα επιτρέπει να προσαρμοστεί σε συγκεκριμένα περιβάλλοντα ή απαιτήσεις. Επιπλέον, μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλα εργαλεία για να σχηματίσει ένα πιο πλήρες σύνολο δοκιμών ασφαλείας.

Το John the Ripper διατίθεται σε αρκετές εκδόσεις, συμπεριλαμβανομένης μιας δωρεάν, κοινοτικής έκδοσης με πρόσθετα χαρακτηριστικά και μιας πιο προχωρημένης επαγγελματικής έκδοσης, η οποία προσφέρει επιπλέον δυνατότητες για εμπορική χρήση. Η αποτελεσματικότητα του εργαλείου είναι εμφανής στην ευρεία χρήση του σε διάφορα σενάρια, από τακτικούς ελέγχους ασφάλειας συστημάτων έως περίπλοκες ασκήσεις δοκιμών διείσδυσης.

Ωστόσο, η ισχύς του John the Ripper φέρει μαζί της και την ανάγκη για ηθική χρήση. Είναι απαραίτητο να χρησιμοποιείται με νόμιμο και ηθικό τρόπο, συνήθως στα πλαίσια ενός ελέγχου ασφάλειας ή μιας δοκιμής διείσδυσης με ρητή άδεια. Η ανεξουσιοδότητη χρήση αυτού του εργαλείου για τη διάρρηξη κωδικών μπορεί να θεωρηθεί παράνομη και ανήθικη.

Συνοψίζοντας, το John the Ripper ξεχωρίζει ως ένα ισχυρό και ευέλικτο εργαλείο στο σετ εργαλείων της κυβερνοασφάλειας. Η ικανότητά του να διαρρήξει σύνθετους κωδικούς πρόσβασης γρήγορα και αποτελεσματικά, σε συνδυασμό με την προσαρμοστικότητά του και την υποστήριξη μιας ισχυρής κοινότητας χρηστών, το καθιστούν μια προτιμώμενη λύση για την αξιολόγηση και τη δοκιμή της ασφάλειας των κωδικών πρόσβασης.

3.1.8 Shodan

Το Shodan είναι μια μηχανή αναζήτησης που επικεντρώνεται στον εντοπισμό και την ανάλυση αντικειμένων και συστημάτων που είναι συνδεδεμένα στο διαδίκτυο. Το Shodan, σε αντίθεση με τις συμβατικές μηχανές αναζήτησης, επιτρέπει στους χρήστες να αναζητούν συσκευές με βάση διάφορους παράγοντες, όπως η τοποθεσία, το λειτουργικό σύστημα, το είδος της συσκευής, ακόμη και συγκεκριμένες ευπάθειες. Προσφέρει σημαντικές πληροφορίες σχετικά με την κατάσταση ασφαλείας των συσκευών που συνδέονται με το διαδίκτυο σε εμπειρογνώμονες ασφαλείας, ερευνητές και χάκερ, επιτρέποντάς τους να αξιολογήσουν ολόκληρο το περιβάλλον ασφαλείας ή να ανακαλύψουν πιθανούς στόχους για εκμετάλλευση. Το Shodan είναι ένα αποτελεσματικό εργαλείο τόσο για την αξιολόγηση της ασφάλειας όσο και για την αναγνώριση, λόγω των ικανοτήτων του να βρίσκει ανοιχτές θύρες, να ανακτά πληροφορίες για banner και ακόμη και να παρέχει πρόσβαση σε webcams, συστήματα βιομηχανικού ελέγχου και άλλες συσκευές που είναι συνδεδεμένες στο διαδίκτυο.

3.2 Πρακτικά Παραδείγματα Μεμονομένων Επιθέσεων

3.2.1 Παράδειγμα 1 Nmap - Metasploit

ΕΠΙΘΕΣΗ ΜΕ METASPLOIT FRAMEWORK ΚΑΙ ΧΡΗΣΗ NMAP ΓΙΑ PORT SCANNING

Σε αυτό το παράδειγμα θα γίνει εκτέλεση δοκιμής διείσδυσης(pentest) σε ένα σύστημα Linux με σκοπό να προσδιορίσουμε τις ευπάθειες στο σύστημα.Το παράδειγμα θα περιλαμβάνει την εκμετάλλευση διαφόρων ευπαθειών στο σύστημα Metasploitable.

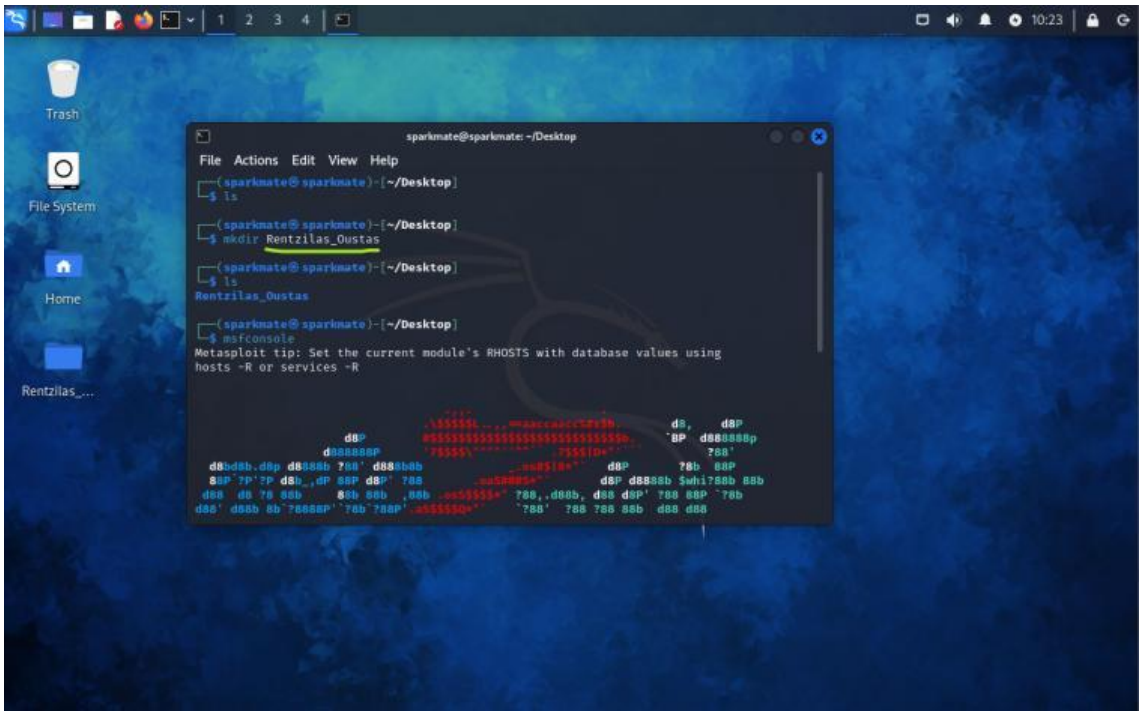
Για την υλοποίηση αυτού του παραδείγματος θα χρησιμοποιήσουμε 2 VirtualBox

1) Kali linux & metasploit framework

2) Metasploitable2

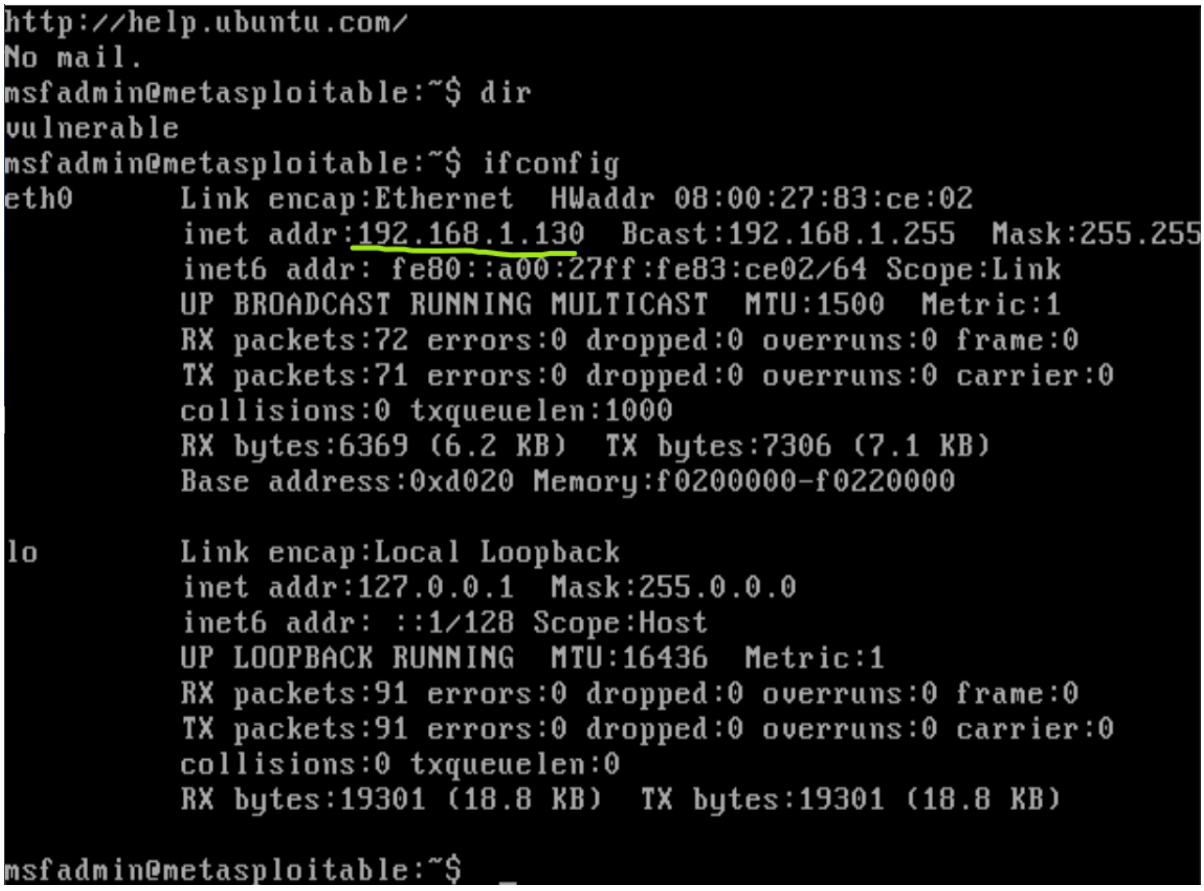
Το metasploitable2 (VirtualBox2) θα λειτουργήσει ως το θύμα στο οποίο θα προσπαθήσουμε να πάρουμε πρόσβαση.

Ανοιγουμε το metasploit framework χρησιμοποιώντας το command ~msfconsole



Εικόνα 3.1 terminal

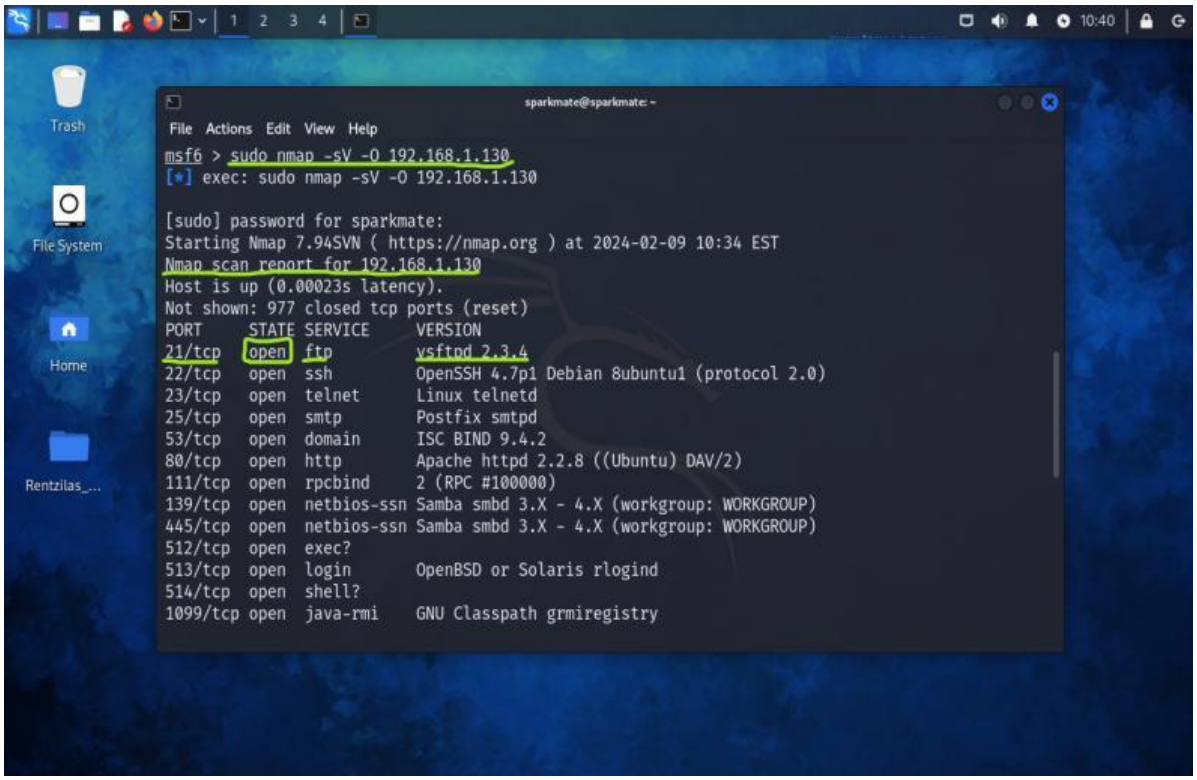
Για να αποκτήσουμε πρόσβαση στον υπολογιστή του θύματος, αρχικά πρέπει να έχουμε την IP του. Σε αυτή την περίπτωση θα χρησιμοποιήσουμε ένα απλό command ~"Ifconfig" για να πάρουμε την IP απο το Virtual box 2.Μπορουμε επίσης να κανουμε host discovery με nmap ετσι ωστε να βρουμε ποιες ip ειναι alive



Εικόνα 3.2 Metasploitable

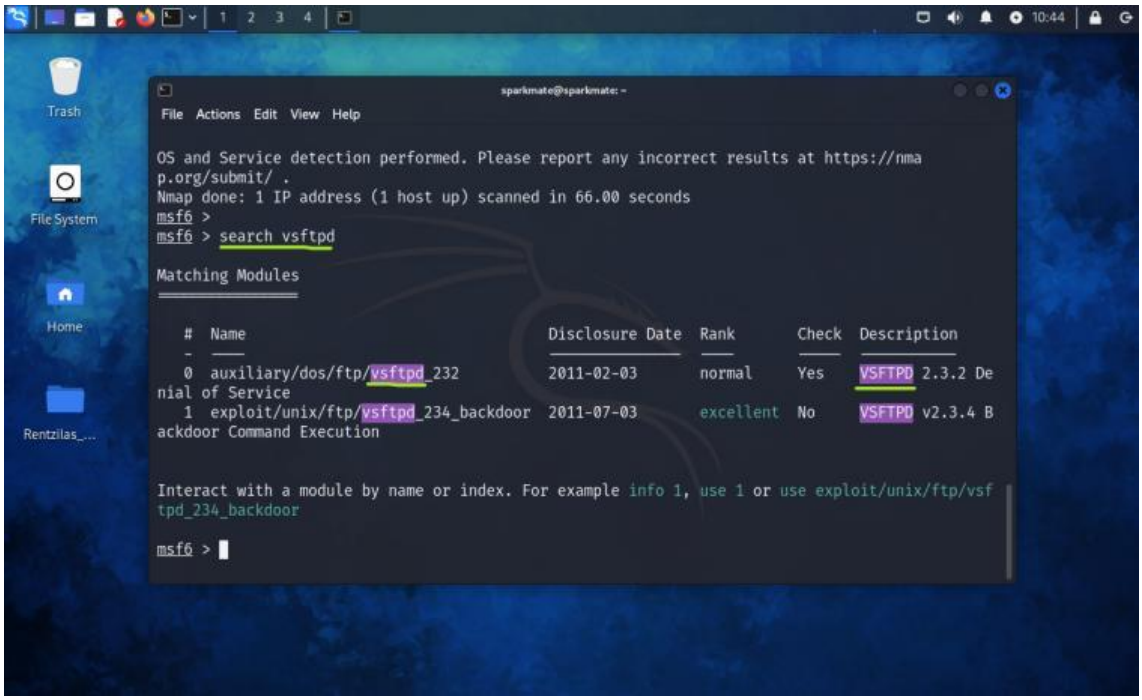
Στην συγκεκριμένη περίπτωση, η IP του θύματος είναι : 192.168.1.130

θα χρησιμοποιήσουμε το nmap για την λειτουργεία του Port scanning, εκτελώντας το ~command : sudo nmap -sV -O (Victim ip:192.168.1.130)



Εικόνα 3.3 terminal

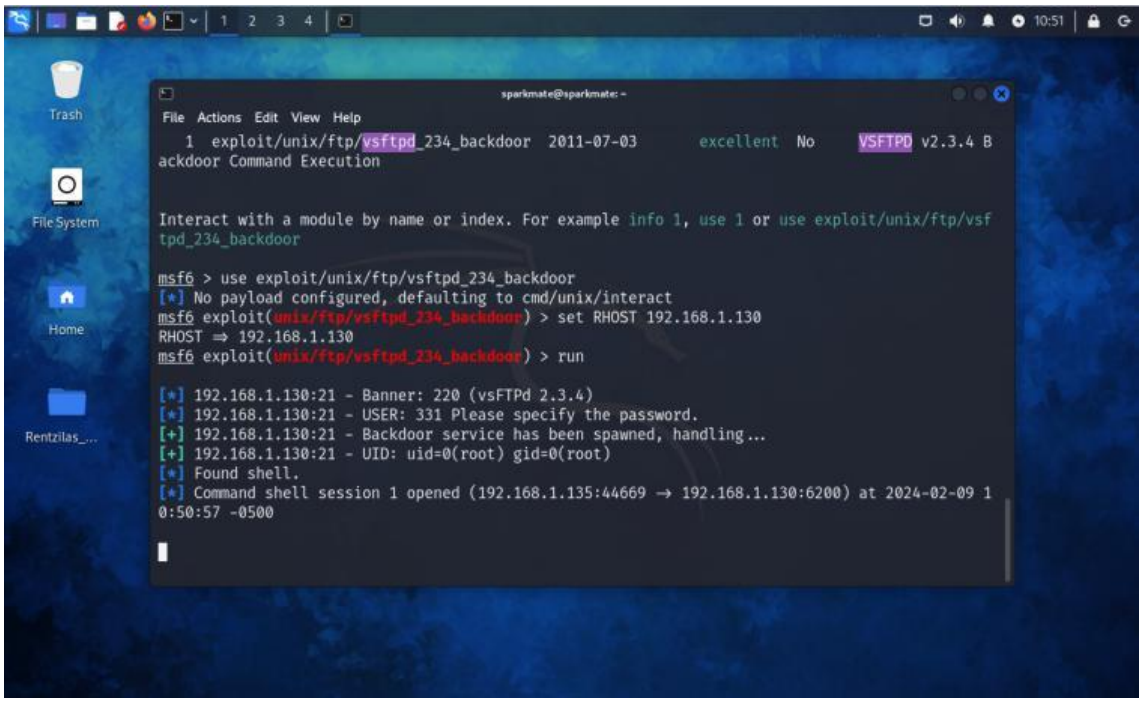
Οπως βλέπουμε στην εικόνα (3.3), το Port 21 είναι ανοιχτό και το FTP στο port 21 θα είναι ο πρώτος στόχος μας για exploit . Επομένως στο port 21 θα αναζητήσουμε για το exploit vsftpd 2.3.4. Με την χρήση του command~ search vsftpd.



Εικόνα 3.4 terminal

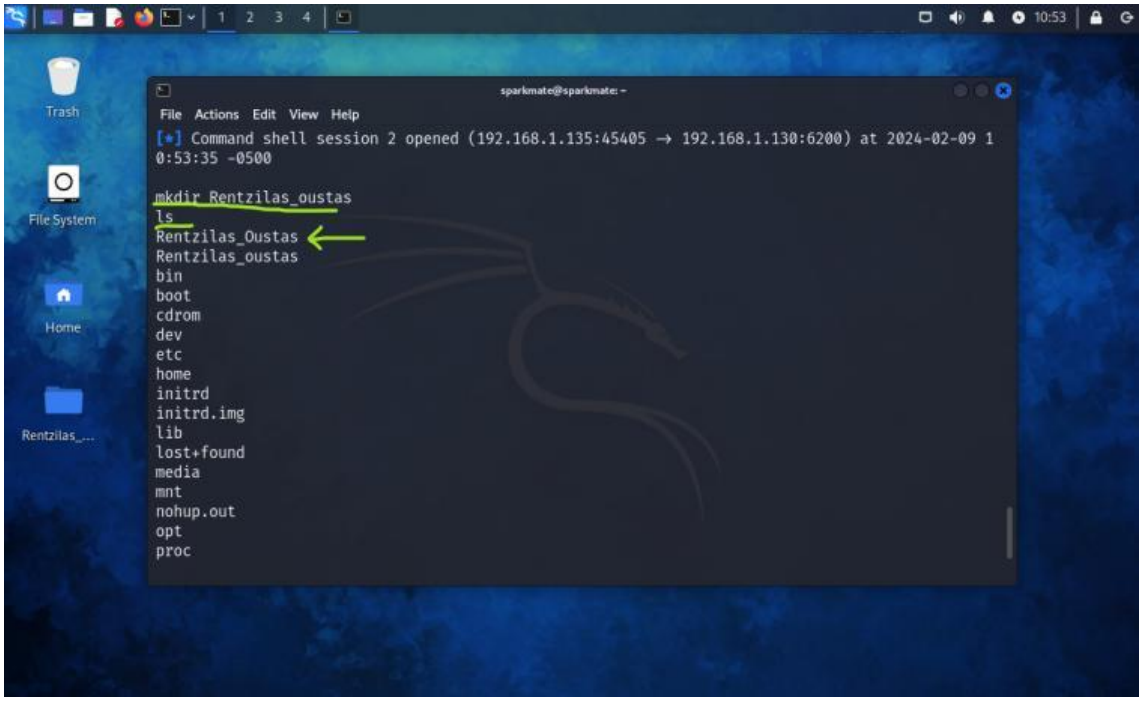
Τωρα θα γίνει η χρήση του exploit για κάνουμε ”επίθεση” στο σύστημα του θύματος με το command: use exploit/unix/ftp/vsftpd_234_backdoor

Αργοτερα θα γίνει η χρήση του command: set RHOST 192.168.1.130 για να ορίσουμε remote host στην ip του θύματος(victim). Μετά τρέχουμε το ~command run και έχουμε πρόσβαση στο shell του χρήστη.



Εικόνα 3.5 terminal

Αφού αποκτήσουμε πρόσβαση στο shell του θύματος μπορούμε να κάνουμε browsing στα αρχεία του και να χρησιμοποιήσουμε αλλα commands όπως να δημιουργήσουμε καινούριους φακέλους και να στείλουμε αρχεία όπως και να τα διαγράψουμε για να καλύψουμε τα ίχνη μας.



Εικόνα 3.6 terminal

Report: για να αποτρέψουμε το συγκεκριμένο ftp η λύση είναι να κάνουμε update service το sftp στο latest version

3.2.2 Παράδειγμα 2 Zphisher

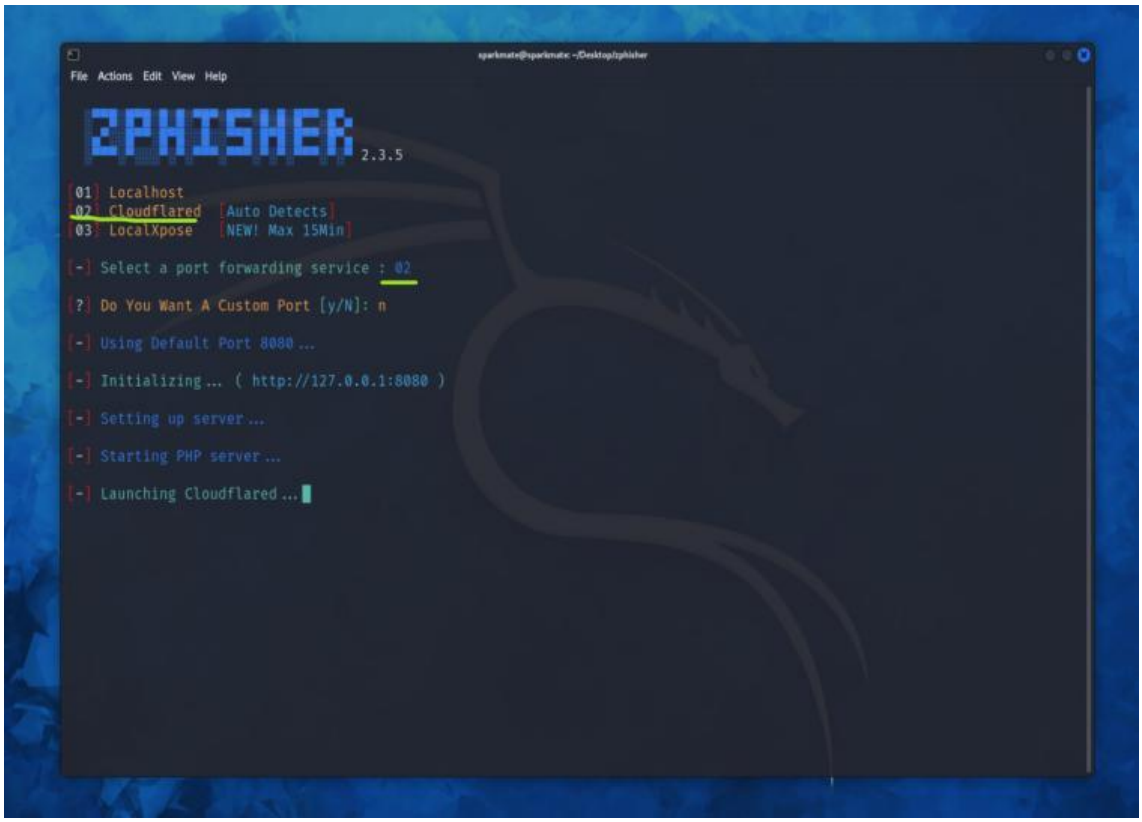
PHISHING "ΨΑΡΕΜΑ" ΚΩΔΙΚΩΝ ΜΕ ΧΡΗΣΗ ZPHISHER.

Σε αυτό το παράδειγμα θα αποκοτήσουμε τα στοιχεία πρόσβασης σε ενα απο τα μέσα κοινωνικής δικτύωσης της δικής μας επιλογής με την τεχνική του "ψαρέματος" phising.

Για την υλοποίηση αυτού του παραδείγματος θα χρησιμοποιήσουμε το tool Zphisher
Το Zphisher, χρησιμοποιείται για να κάνουμε υποκλοπή των στοιχείων σύνδεσης του χρήστη κάνοντας clone την σελίδα σύνδεσης απο δημοφιλή σελίδες κοινωνικής δικτύωσης

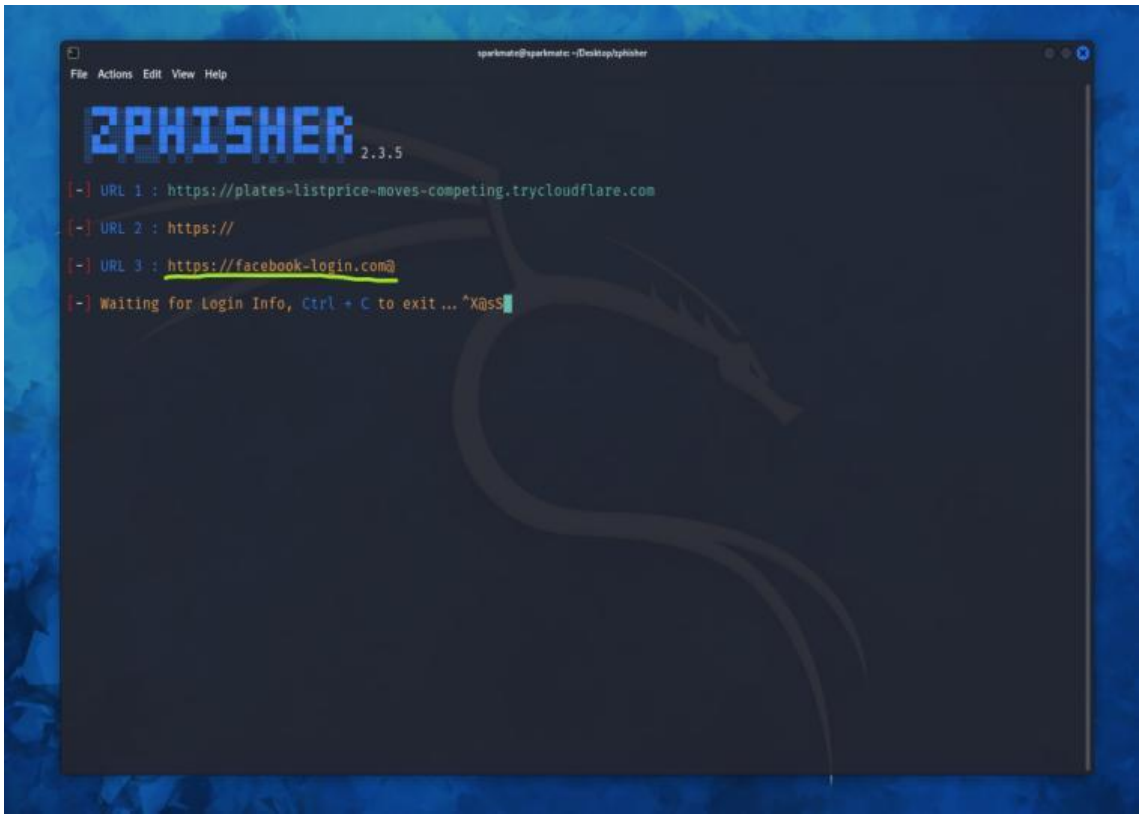
Εικόνα 3.7 Zphiser

Διαλέγουμε την εφαρμογή στην οποία θέλουμε να αποκτήσουμε πρόσβαση. Στην περιπτωσή μας θα διαλέξουμε το Facebook.



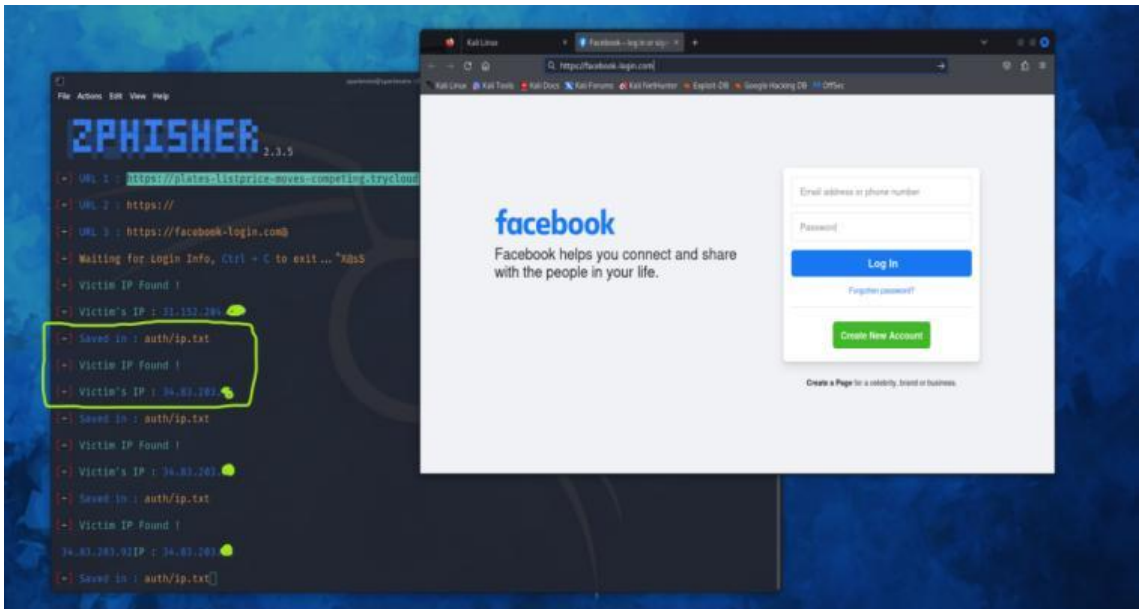
Εικόνα 3.8 Zphiser

Το Zphisher μας δίνει την επιλογή να κάνουμε host το link μας η να το έχουμε ως localhosted . Στην συγκεκριμένη περίπτωση μας θα διαλέξουμε την επιλογή cloudflare και θα δώσουμε mask https://facebook-login.com/ στο link μας έτσι ώστε να φαίνεται αληθοφανές.



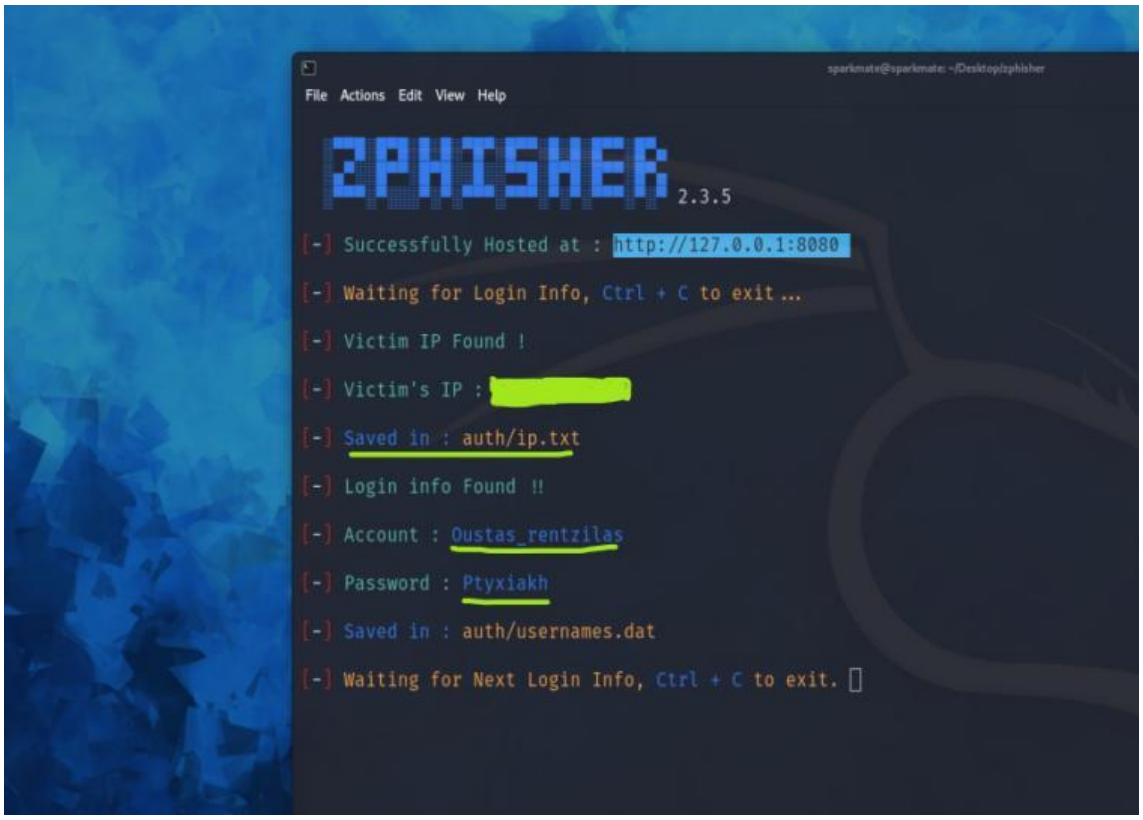
Εικόνα 3.9 Zphiser

Αφού ανοίξει ο χρήστης το link, έχουμε ήδη κλέψει την IP του.



Εικόνα 3.10 Zphiser και χρήση του cloudflare

Και μόλις γίνει εισαγωγή των στοιχείων το phising έχει ολοκληρωθεί εφόσον έχουμε κλέψει τα στοιχεία του.

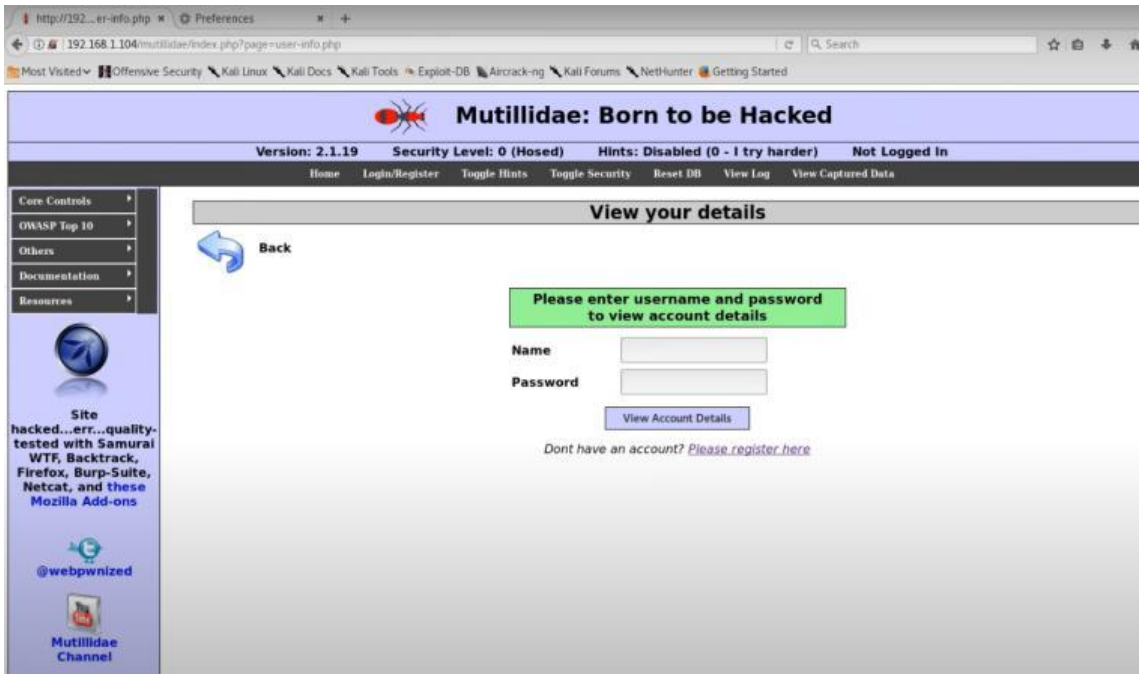


Εικόνα 3.11 Zphiser

Τέλος για να μην καταλάβει το θύμα ότι έχει γίνει υποκλοπή στοιχείων το tool κάνει redirect το θύμα στην επίσημη ιστοσελίδα του προγράμματος που διαλέξαμε.

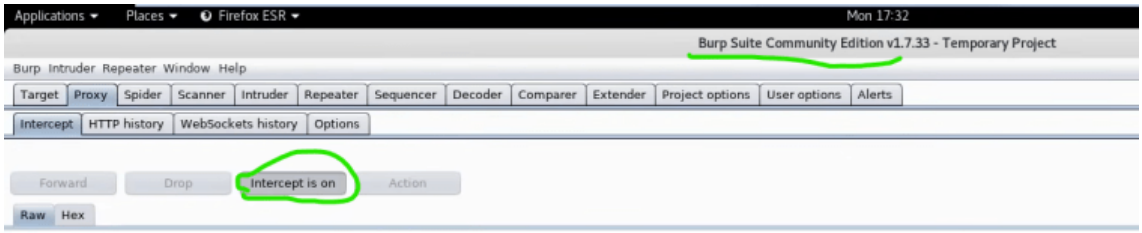
3.2.3 Παράδειγμα 3 BurpSuite και SQLMap

Για αυτό το παράδειγμα του SQL MAP θα χρησιμοποιήσουμε το mutillidae το οποίο είναι προεγκατεστημένο στο metasploitable2.



Εικόνα 3.12 Mutillidae

Θα χρησιμοποιήσουμε το BURP SUITE με την επιλογή intecept , για να κάνουμε capture το request που προκύπτει όταν ο χρήστης χρησιμοποιεί την φόρμα.

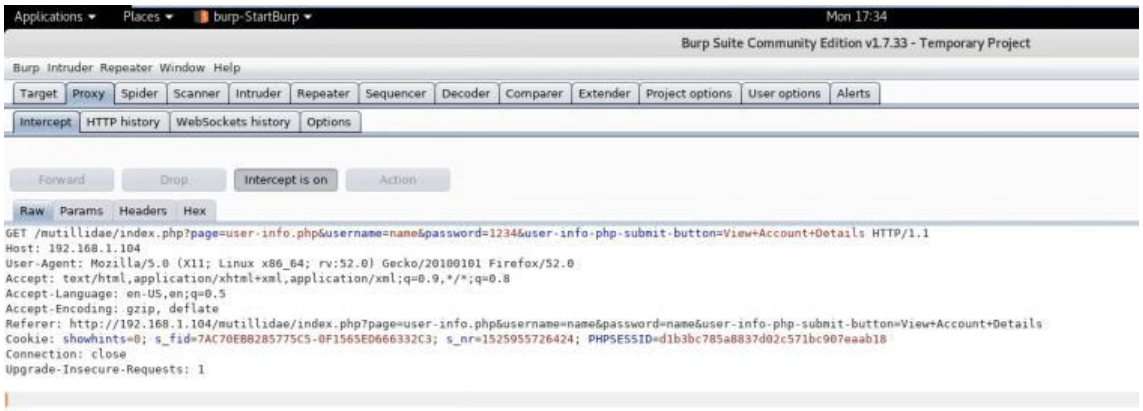


Εικόνα 3.13 Mutillidae

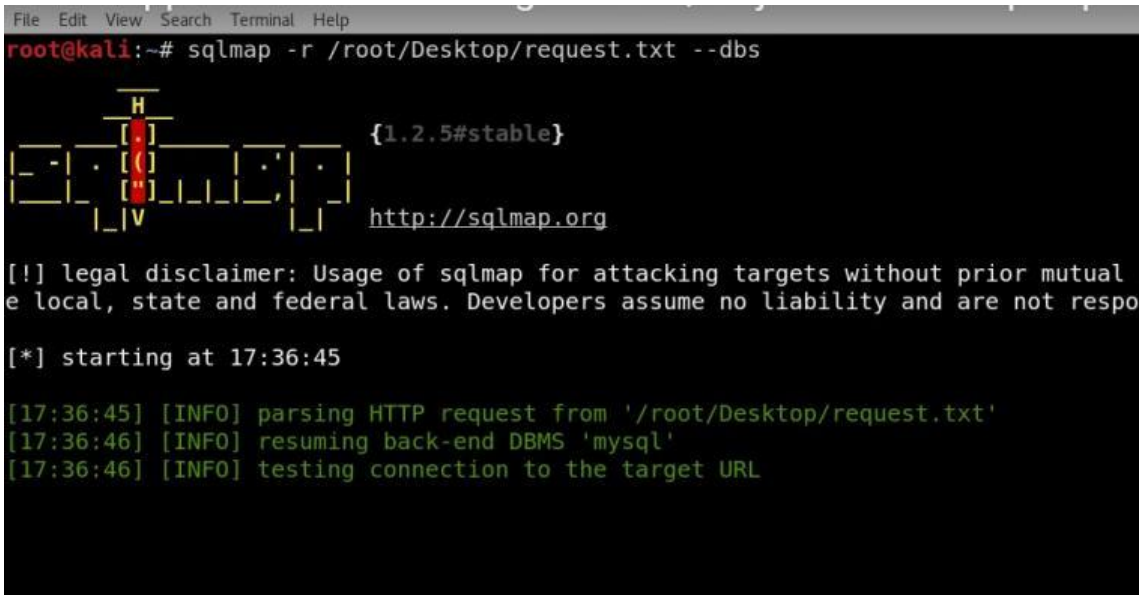
Αφού χρησιμοποιηθεί το form, το burpsuite κάνει “Capture” το request απο το browser στον server.

Εικόνα 3.14 Mutillidae

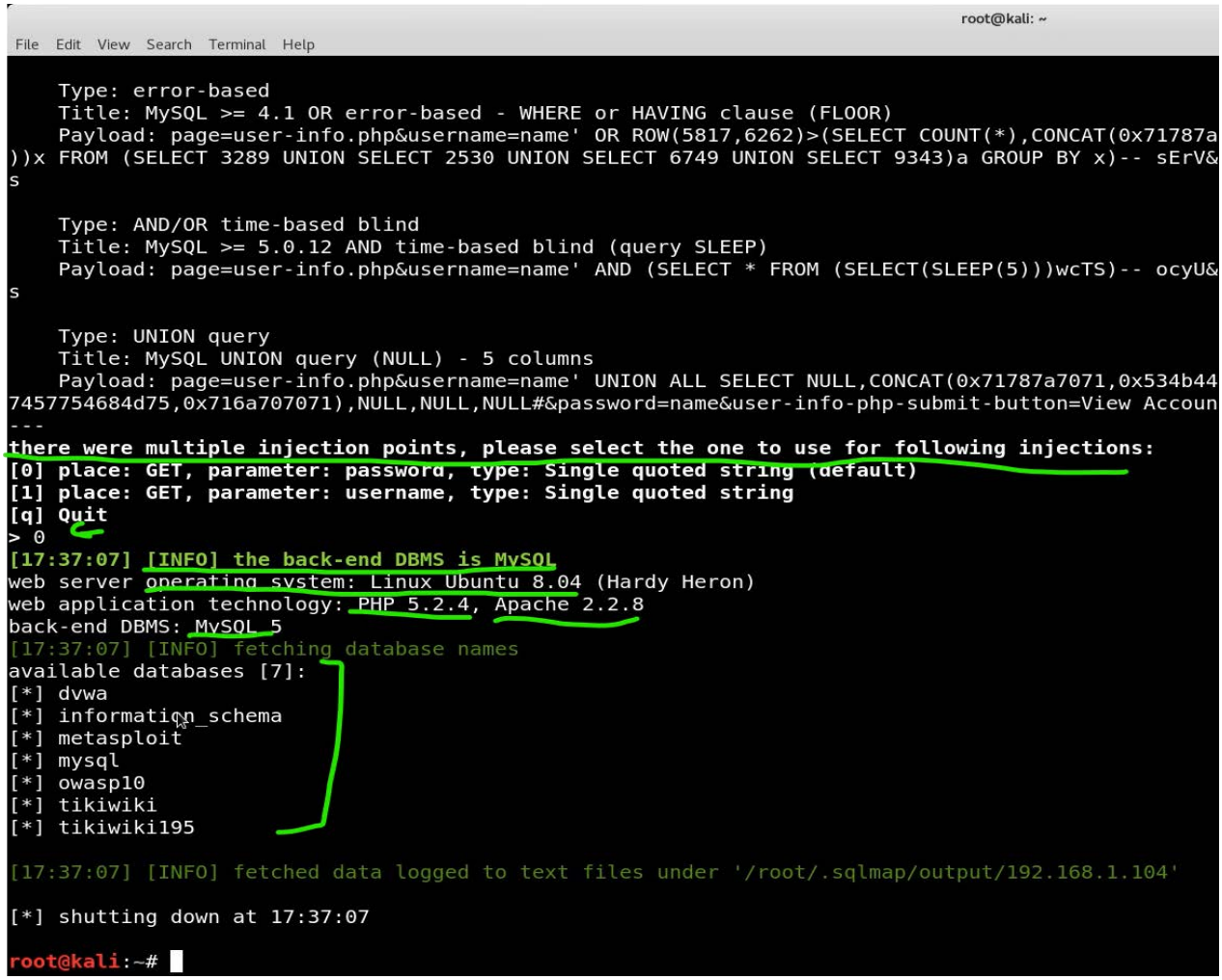
Το request που προκύπτει όταν συμπληρωθεί η φόρμα είναι το παρακάτω. Το αποθηκεύουμε για να το χρησιμοποιήσουμε στο sqlmap.



Εικόνα 3.15 Mutillidae



Εικόνα 3.16 SQLMAP



Εικόνα 3.17 SQLMAP

Με το command: sqlmap –r (request save location) --dbs απαριθμούμε τις βάσεις δεδομένων, που προκύπτουν απο το request που κάναμε capture προηγουμένως.

Με την χρήση του command του sqlmap, καταφέραμε να λάβουμε μερικές πληροφορίες για τον σέρβερ της βάσης δεδομένων όπως:

Web server operation system: Linux Ubuntu 8.04

Web application technology: PHP 5.2.4, Apache 2.2.8, MySQL 5

Και τα ονόματα των βάσεων δεδομένων.

1 dvwa

2 information_schema

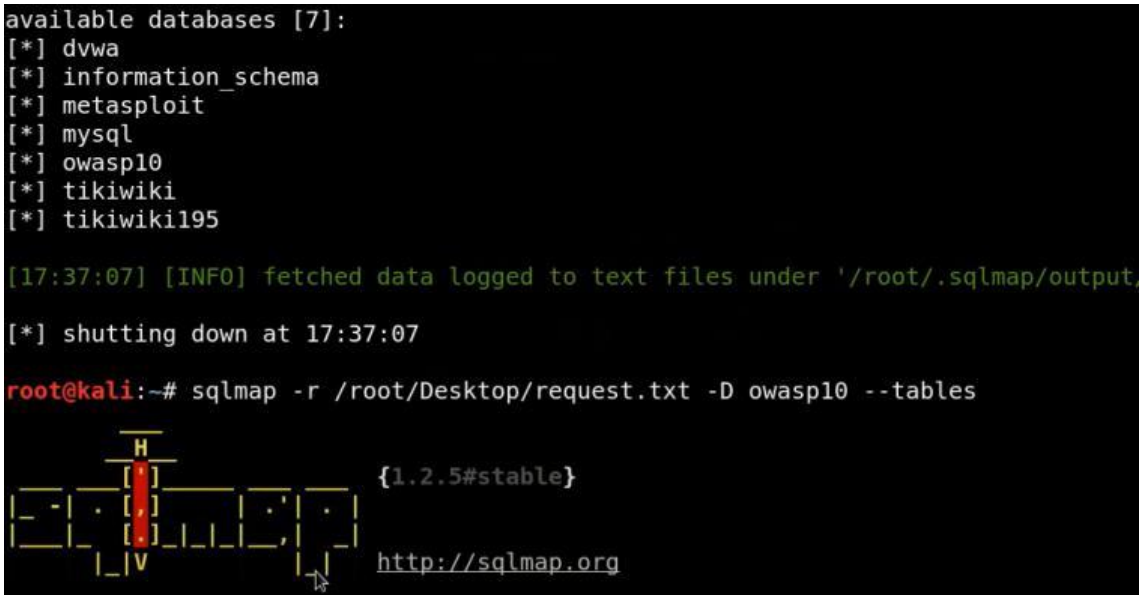
3 metasploit

4 mysql

5 owasp10

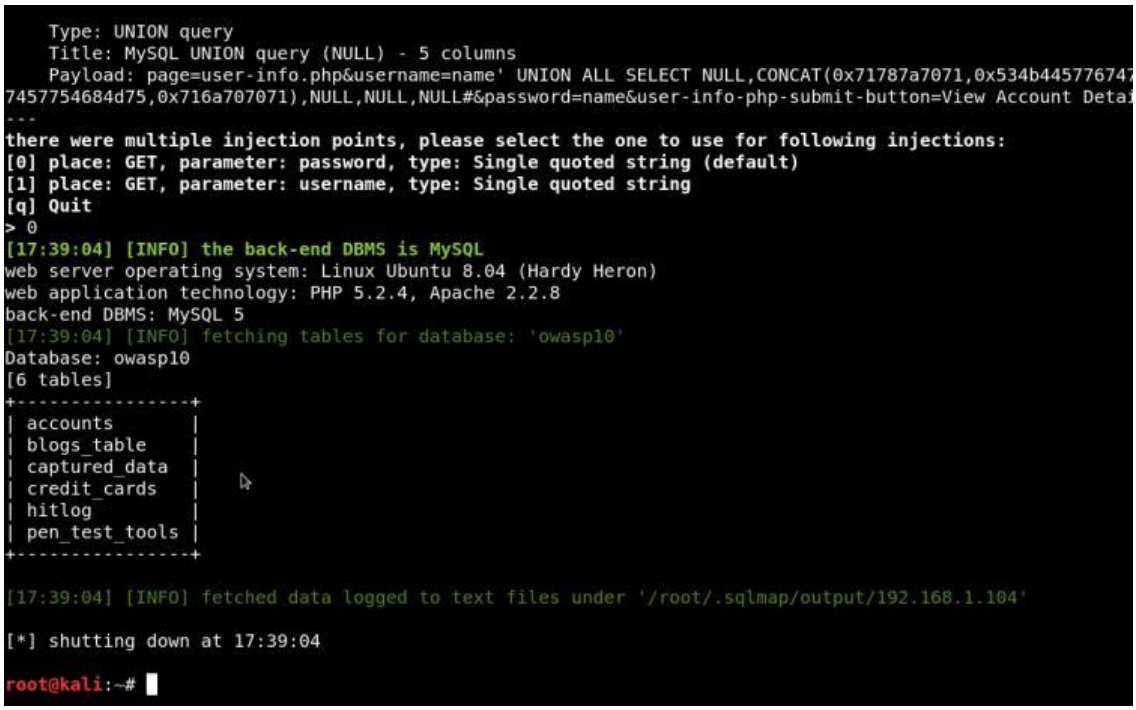
6 tikiwiki

7 tikiwiki195



Εικόνα 3.18 SQLMAP

Χρησιμοποιούμε το παραπάνω command για να απαριθμήσουμε τα tables της βάσης δεδομένων ”owasp10”



Εικόνα 3.19 SQLMAP

Προκύπτουν 6 tables:

accounts

blogs_table

captured_data

credit_cards

hitlog

pen_test_tools

Προσπαθουμε για παράδειγμα να δούμε τα στοιχεία που είναι αποθηκευμένα στο table accounts, χρησιμοποιώντας τοcommand:

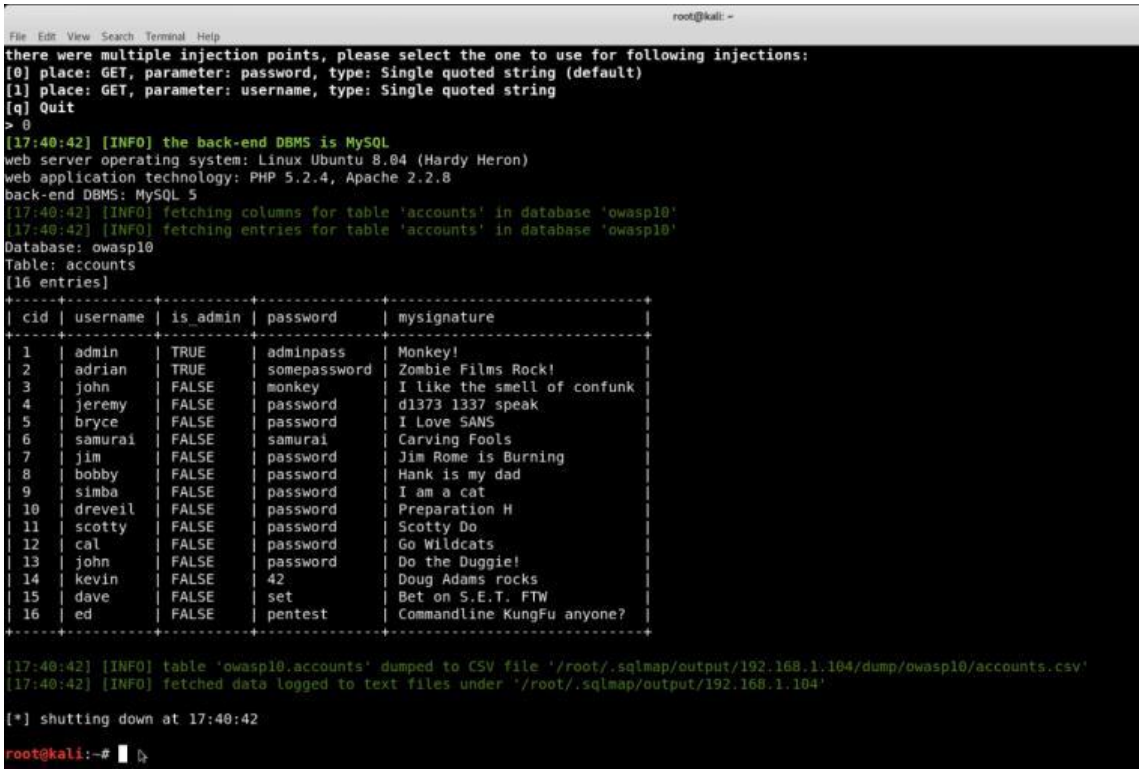
sqlmap -r (τοποθεσία request.txt) -D owasp10 -T accounts –dump

-D ονομα βασης δεδομένων

-T ονομα table

Και έτσι, με την χρήση του burp suite και sqlmap, έχουμε καταφέρει να απαριθμήσουμε της βάσεις δεδομένων μια ιστοσελίδας αλλά και να δούμε το περιεχόμενο της.

(Σε ένα φυσιολογικό περιβάλλον παράμετροι όπως το password, δεν θα αποθηκευόταν σε βάση δεδομένων ως plain text αλλά θα ήταν encrypted.)



Εικόνα 3.20 SQLMAP

4 Σύνοψη

Συνοψίζοντας, στην παρούσα εργασία, προσφέραμε μια εκτενή ιστορική αναδρομή στον κόσμο του χάκινγκ, καταπιαστήκαμε με τα στάδια που πρέπει να περάσουμε για να εκτελέσουμε με επιτυχία ένα Penetration Test σε ηθικά πλαισια παντα, εξετάζοντας πώς η θεωρία μεταφέρεται στην πράξη.Επιπλέον, εξετάσαμε ποικίλες επιθέσεις και τους τρόπους προστασίας από αυτές, προσφέροντας μια σφαιρική εικόνα των προκλήσεων και των λύσεων στον ψηφιακό κόσμο. Τέλος, παρουσιάσαμε τρία παραδείγματα από γνωστά είδη επιθέσεων, επισημαίνοντας τα εργαλεία που χρησιμοποιούνται για την εκτέλεσή τους.Τέλος, αναδείξαμε την ανάγκη για συνεχή εκπαίδευση και ενημέρωση στον τομέα του χάκινγκ, καθώς και τη σημασία της διατήρησης υψηλών προτύπων ηθικής για την προστασία του ασφαλούς ψηφιακού κόσμο.

Βιβλιογραφία

[1] International Council Of E-Commerce Consultants, and Ec-Council Press. *Ethical Hacking and Countermeasures. Book 2 of 4, Threats and Defense Mechanisms*. Boston, Massachusetts, Cengage Learning, 2017.

[2] Rowland, Andy. "Ethical Hacking: Protecting Connected Vehicles." *Engineering & Technology Reference*, vol. 1, no. 1, 1 Jan. 2012,

[3] Dominik Landwehr, et al. *Hacking*. Basel, Merian, 2014.

[4] Rowland, Andy. "Ethical Hacking: Protecting Connected Vehicles." *Engineering & Technology Reference*, vol. 1, no. 1, 1 Jan. 2012

[5] Erickson, Jon. *Hacking : The Art of Exploitation*. Erscheinungsort Nicht Ermittelbar, No Starch Press, Us, 2007.

[6] ---. *Hacking: The Art of Exploitation, 2nd Edition*. No Starch Press, 1 Feb. 2008.

[7] Scambray, Joel, et al. *Hacking Exposed Web Applications, Second Edition*. McGraw Hill Professional, 27 June 2010.

[8]. Thomas, Stephen. *Using Automated Fix Generation to Mitigate SQL Injection Vulnerabilities a Detailed Approach*. Saarbrücken Vdm Verlag Dr. Müller, 2008.

[9] Grossman, Jeremiah. *XSS Attacks : Cross-Site Scripting Exploits and Defense ; [Learn to Identify, Exploit, and Protect against XSS Attacks ; See Real XSS Attacks That Steal E-Mails, Own Web Surfers, and Trojanize Backend ; Leverage XSS Vulnerabilities to Allow Remote Proxy Attacks into External and Internal Networks]*. Burlington, Mass Syngress, 2007.

[10] Dunham, Ken. *Mobile Malware Attacks and Defense*. Syngress, 12 Nov. 2008.

[11] Barrett, Daniel J. *Linux Pocket Guide*. Beijing ; Sebastopol, Ca, O'reilly, 2004.

[12] *Web Hacking : Attacks and Defense*. Boston Etc., Addison-Wesley, 2005.

[13] https://ieeexplore.ieee.org/courses/details/EDP459 EthicalHacking:Scanning,Sen-Oriyano

[14] https://ieeexplore.ieee.org/courses/details/EDP467 Ethical Hacking: SQL Injections

[15] https://ieeexplore.ieee.org/courses/details/EDP464 Ethical Hacking: Scanning

[16] https://ieeexplore.ieee.org/courses/details/EDP466 Ethical Hacking: Session Hijacking

[17] https://ieeexplore.ieee.org/document/9740860 Ethical Hacking: Importance, Controversies and Scope in the Future

[18] https://ieeexplore.ieee.org/document/10342914 Penetration Testing and Ethical Hacking: Risk Assessments and Student Learning

[19] https://usa.kaspersky.com/resource-center/definitions/what-is-hacking kaspersky what is hacking

[20] https://www.proofpoint.com/us/threat-reference/hacking What Is Hacking?

[21] https://ieeexplore.ieee.org/abstract/document/5386933 Ethical hacking Published in: IBM Systems Journal (Volume: 40, Issue: 3, 2001)