ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διπλωματική Εργασία

ΑΠΕΙΛΕΣ ΚΑΙ ΑΝΙΧΝΕΥΣΗ/ΠΡΟΒΛΕΨΗ ΕΙΣΒΟΛΩΝ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

ΑΡΓΥΡΟΥ-ΚΟΛΟΤΟΥΡΟΥ ΝΙΚΗ

Επιβλέπων Καθηγητής: Μαλιάτσος Κωνσταντίνος

Επιτροπή: Καρύδα Μαρία, Διαμαντοπούλου Βασιλική

Περίληψη

Η εργασία αφορά την κυβερνοασφάλεια και συγκεκριμένα την ανίχνευση και πρόληψη των επιθέσεων μέσω δικτύου. Η ασφάλεια στον κυβερνοχώρο αποσκοπεί στην προστασία των συστημάτων από επιθέσεις και τη διατήρηση της ακεραιότητάς τους. Η κυβερνοτρομοκρατία στην οποία εντάσσονται αυτές οι επιθέσεις είναι η χρήση του διαδικτύου, των μέσων πληροφόρησης και των πλατφορμών επικοινωνίας για τη διεξαγωγή τρομοκρατικών επιθέσεων ή την προώθηση τρομοκρατικών σκοπών. Αυτές οι επιθέσεις περιλαμβάνουν ένα μεγάλο εύρος περιπτώσεων που αναφέρονται εντός του θεωρητικού τμήματος της εργασίας. Στη διπλωματική εργασία αναλύεται το Διαδίκτυο των Πραγμάτων, ως σύστημα συνδεδεμένων υπολογιστικών συσκευών, ψηφιακών μηχανών, αντικειμένων ή ακόμα και ανθρώπων, τα οποία διαθέτουν μοναδικά αναγνωριστικά και μπορούν να ανταλλάσσουν δεδομένα μέσω δικτύου χωρίς την ανάγκη για ανθρώπινη επέμβαση. Παρουσιάζεται επίσης η έννοια του επαγγελματικού/ηθικού χάκινγκ, μια νόμιμη διαδικασία με στόχο τον εντοπισμό αδυναμιών σε ένα σύστημα πληροφορικής, προσομοιώνοντας μια πραγματική κυβερνοεπίθεση. Σε αυτά τα πλαίσια η εργασία είναι μια μελέτη περίπτωσης για την ανίχνευση εισβολών με σύστημα Intrusion Detection/Protecton Systems IDPS - που αυτοματοποιεί τη διαδικασία ανίχνευσης εισβολής. Η διαδικασία περιλάμβανε την εγκατάσταση του Snort (ανοικτό λογισμικό ανίχνευσης επιθέσεων) και τη διαμόρφωση κανόνων ανίχνευσης που σχεδιάστηκαν για να εντοπίζουν συγκεκριμένες επιθέσεις, όπως επιθέσεις DDoS, SQL injection, και ARP spoofing. Η χρήση του Snort σε συνδυασμό με το Raspberry Pi αποδείχθηκε ιδιαίτερα αποτελεσματική, καθώς οι επιθέσεις ανιχνεύθηκαν με ακρίβεια και τα δεδομένα των ανιχνεύσεων αναλύθηκαν σε πραγματικό χρόνο. Η ενσωμάτωση του Grafana (λογισμικό οπτικοποίησης) για την παρακολούθηση των επιθέσεων παρείχε μια διαισθητική και οπτική αναπαράσταση των δεδομένων ασφαλείας. Με τη δημιουργία διαδραστικών πινάκων και γραφημάτων, διευκόλυνε την ανάλυση των ανιχνευόμενων δραστηριοτήτων και την αξιολόγηση της απόδοσης του συστήματος ασφαλείας. Η μελέτη έδειξε ότι είναι εφικτό να αναπτυχθούν αποδοτικά συστήματα ανίχνευσης και πρόληψης εισβολών ακόμα και με περιορισμένους πόρους σε υλικό όπως τα Raspberry Pi που έχουν περιορισμένες δυνατότητες, είναι όμως αποτελεσματικά για μικρές και μεσαίες επιχειρήσεις. Τα αποτελέσματα έδειξαν ότι η σωστή διαμόρφωση και χρήση εργαλείων μπορούν να προσφέρουν υψηλό επίπεδο προστασίας, ανιχνεύοντας και καταγράφοντας κακόβουλες δραστηριότητες.

Λέξεις – κλειδιά: Κυβερνοασφάλεια, Διαδίκτυο των Πραγμάτων, Επιθέσεις, Πρόβλεψη και Ανίχνευση Επιθέσεων, Raspberry Pi

Abstract

The present study concerns cyber security and specifically the detection and prevention of internet attacks. Cyber security aims to protect systems from attacks and maintain their integrity. Cyberterrorism, which these attacks fall under, is the use of the internet, information media and communication platforms to carry out terrorist attacks or promote terrorist aims. These attacks include a wide range of cases reported within the theoretical part of the paper. In diplomacy, the Internet of Things is analyzed as a system of connected computing devices, digital machines, objects or even people, which have unique identifiers and can exchange data over a network without the need for human intervention. Also introduced is the concept of professional, ethical hacking, a legal process aimed at identifying weaknesses in an IT system by simulating a real cyber-attack. In this context the dissertation is a case study of intrusion detection with an IDPS system - which automates the intrusion detection process. The process involved installing Snort (IDPS software) and configuring detection rules designed to detect specific attacks, such as DDoS attacks, SQL injection, and ARP spoofing. Using Snort in conjunction with the Raspberry Pi proved to be particularly effective, as attacks were accurately detected, and detection data analyzed in real-time. Integration of Grafana (visualization software) was performed to monitor attacks provided an intuitive and visual representation of security data. By creating interactive charts and graphs, it facilitated the analysis of detected activities and the evaluation of security system performance. The study showed that it is possible to develop efficient intrusion detection and prevention systems even with limited resources with hardware such as Raspberry Pi which has limited capabilities, but it is effective for small and medium enterprises. The results of the study showed that the right configuration and use of tools can provide a high level of protection by detecting and recording malicious activities.

Keywords: Cybersecurity, Internet of Things, Hacking, Raspberry Pi

Πίνακας περιεχομένων

Κατάλογος Εικόνων

Εισαγωγή

Η κυβερνοασφάλεια αναδεικνύεται ως κρίσιμος τομέας στην εποχή της ψηφιακής επανάστασης, καθώς οι απειλές στον διαδικτυακό χώρο αυξάνονται και προκαλούν διάφορες μορφές ζημίας σε επιχειρήσεις, οργανισμούς, ακόμα και ιδιώτες. Στο πλαίσιο αυτό, η προστασία των υποδομών, των δεδομένων και των ευαίσθητων πληροφοριών απαιτεί στρατηγικές και λύσεις που προσαρμόζονται διαρκώς στις νέες απειλές και τεχνολογικές εξελίξεις.

Μια από τις βασικές πτυχές της κυβερνοασφάλειας είναι η ανίχνευση και πρόληψη επιθέσεων. Σε αυτό το πλαίσιο, η εργασία αυτή εστιάζεται στη χρήση του Raspberry Pi ως εργαλείου για επιθέσεις και την υλοποίηση μιας προστατευτικής υποδομής στο δίκτυο. Αναλύονται οι διάφορες φάσεις της εργασίας, περιλαμβανομένης της εγκατάστασης του Snort IDS/IPS (Intrusion Detection/Prevention System) και του Grafana, καθώς και της διαμόρφωσης του Snort για το δίκτυο και την εγκατάσταση των συνόλων κανόνων. Η υλοποίηση αυτής της πρακτικής πλευράς αναδεικνύει τη σημασία της κυβερνοασφάλειας στην προστασία των ψηφιακών περιουσιών και την ανάγκη για σταθερές και αποτελεσματικές λύσεις ανίχνευσης και πρόληψης επιθέσεων.

Η υλοποίηση του πρακτικού μέρους της εργασίας αφορά την χρήση Raspberry Pi για επιθέσεις και τα βήματα που πραγματοποιήθηκαν στο πρακτικό κομμάτι είναι η εγκατάσταση Snort IDS/IPS και Grafana, η υλοποίηση μιας διαμόρφωσης (setup) προστασίας στο Raspberry Pi, στο ίδιο δίκτυο με το Snort, θεωρώντας ότι στο ίδιο δίκτυο θα είναι και ο επιτιθέμενος. Στη συνέχεια πραγματοποιήθηκε παραμετροποίηση του Snort για το δίκτυο και εγκατάσταση των rules sets. Τέλος μέσω του Kali linux ενεργοποιήθηκε η αντίδραση του συστήματος στις ανιχνευόμενες επιθέσεις.

1 Εισαγωγή στην Κυβερνοασφάλεια

Η ασφάλεια στον κυβερνοχώρο περιλαμβάνει τις διάφορες προσεγγίσεις που αποσκοπούν στην προστασία των συστημάτων από επιθέσεις και τη διατήρηση της ακεραιότητάς τους. Προβλέπεται ότι η εργασία/ενασχόληση με την ασφάλεια στον τομέα της πληροφορικής θα αυξηθεί σημαντικά στο μέλλον, με εκτιμήσεις να δείχνουν ότι θα ανέλθει στο 10% του συνολικού μεριδίου αγοράς πληροφορικής το 2025. Αυτό σημαίνει μια αύξηση από τα σημερινά 4 τρισεκατομμύρια δολάρια (Shandilya, 2020).

Η ασφάλεια στον κυβερνοχώρο έχει γίνει πρωταρχική προτεραιότητα τόσο για επιχειρήσεις όσο και για κυβερνήσεις παγκοσμίως. Συγκεκριμένα, η προστασία των δεδομένων παίζει καθοριστικό ρόλο σε αυτή την προσπάθεια, είτε πρόκειται για την προστασία από κακόβουλους επιτιθέμενους που επιδιώκουν την καταστροφή ή την κλοπή δεδομένων, είτε για την προστασία από εταιρίες που διαχειρίζονται δεδομένα χρηστών. Στην πρώτη περίπτωση, απαιτείται η ανάλυση των απειλών και η αξιολόγηση των ύποπτων ενεργειών στον κυβερνοχώρο. Μια επίθεση στον κυβερνοχώρο μπορεί να έχει καταστροφικές συνέπειες λόγω της μη εξουσιοδοτημένης πρόσβασης σε δεδομένα. Στη δεύτερη περίπτωση, που αφορά την προστασία της ιδιωτικότητας των δεδομένων των χρηστών από εταιρίες, η ασφάλεια επιτυγχάνεται μέσω πολιτικών όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). Μέσω αυτού του κανονισμού, οι προμηθευτές λογισμικού υποχρεούνται να συμμορφώνονται με τις απαιτήσεις των νόμων και να διασφαλίζουν την ποιότητα του λογισμικού όσον αφορά την ασφάλεια και ιδιωτικότητα (Shandilya, 2020).

Η ασφάλεια στον κυβερνοχώρο είναι ζωτικής σημασίας, καθώς οποιοσδήποτε μπορεί να είναι δυνητικός στόχος επίθεσης. Από επιχειρηματικούς οργανισμούς μέχρι κυβερνητικούς φορείς και άτομα με μικρότερη “σημασία” στο διαδίκτυο, όλοι είναι εκτεθειμένοι στον κίνδυνο επίθεσης. Αυτό οδηγεί στην ανάγκη για εφαρμογή προληπτικών μέτρων. Οι κυβερνοεπιθέσεις μπορούν να περιλαμβάνουν επιθέσεις Denial of Service -DoS, κακόβουλο λογισμικό, ιούς και ηλεκτρονικό "ψάρεμα" (phishing), επηρεάζοντας τους χρήστες και τις υπηρεσίες που χρησιμοποιούν (Deepa, 2014).

Κατά το σχεδιασμό ενός σχεδίου ασφάλειας, ορισμένοι βασικοί τομείς αξίζουν ιδιαίτερη προσοχή. Αυτοί περιλαμβάνουν την ασφάλεια εφαρμογών, την ασφάλεια έναντι καταστροφών, την ασφάλεια πληροφοριών και την ασφάλεια δικτύου. Η ασφάλεια εφαρμογών αφορά την ανάπτυξη μέτρων για την προστασία των εφαρμογών από απειλές

κατά τη διάρκεια σχεδίασης, ανάπτυξης, εγκατάστασης και συντήρησης. Η ασφάλεια έναντι καταστροφών αφορά την ανάπτυξη διαδικασιών αντιμετώπισης κρίσεων στον κυβερνοχώρο, συμπεριλαμβανομένης της αξιολόγησης κινδύνου και της καθορισμένης στρατηγικής ανάκαμψης. Η ασφάλεια πληροφοριών επικεντρώνεται στην προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση. Τέλος, η ασφάλεια δικτύου αποσκοπεί στην εξασφάλιση της προστασίας, ακεραιότητας και αξιοπιστίας του δικτύου. Περιλαμβάνει λογισμικό προστασίας, τείχη προστασίας, εικονικά ιδιωτικά δίκτυα και συστήματα πρόληψης εισβολών (Deepa, 2014).

1.1 Πληροφοριακά Συστήματα - Information Systems

Ένα Πληροφοριακό Σύστημα (Information System – IS) είναι μια συλλογή υλικού, λογισμικού, δεδομένων και ανθρώπων που συνεργάζονται για τη συλλογή, επεξεργασία, αποθήκευση και διάδοση πληροφοριών. Ένα IS μπορεί να χρησιμοποιηθεί για διάφορους σκοπούς, όπως η υποστήριξη επιχειρηματικών λειτουργιών, η λήψη αποφάσεων και η επικοινωνία (Rainer et al., 2020).

Η ασφάλεια των πληροφοριών αναφέρεται στην προστασία των πληροφοριών και των πληροφοριακών συστημάτων από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση ή καταστροφή. Αποσκοπεί στην προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των πληροφοριακών συστημάτων.

Τα πληροφοριακά συστήματα είναι ευάλωτα σε ποικίλες απειλές ασφάλειας, όπως οι χάκερ, οι ιοί και οι φυσικές καταστροφές. Ως εκ τούτου, είναι σημαντικό για τους οργανισμούς να εφαρμόζουν κατάλληλα μέτρα ασφαλείας για την προστασία των πληροφοριακών τους συστημάτων (Rainer et al., 2020).

Υπάρχουν πολλά διαφορετικά μέτρα ασφαλείας που μπορούν να εφαρμόσουν οι οργανισμοί για την προστασία των πληροφοριακών τους συστημάτων, όπως (Rainer et al., 2020):

- **Τείχη προστασίας:** Τα τείχη προστασίας χρησιμοποιούνται για τον περιορισμό της πρόσβασης στο δίκτυο ενός οργανισμού και για την προστασία από μη εξουσιοδοτημένη πρόσβαση.

- **Συστήματα ανίχνευσης εισβολών:** Τα συστήματα αυτά χρησιμοποιούνται για την ανίχνευση και την ειδοποίηση των οργανισμών για πιθανές παραβιάσεις της ασφάλειας.
- **Κρυπτογράφηση:** Η κρυπτογράφηση χρησιμοποιείται για την προστασία ευαίσθητων πληροφοριών με τη μετατροπή τους σε μη αναγνώσιμο «κείμενο».
- **Έλεγχοι πρόσβασης:** Οι έλεγχοι πρόσβασης χρησιμοποιούνται για τον περιορισμό της πρόσβασης σε πληροφορίες και πληροφοριακά συστήματα μόνο σε εξουσιοδοτημένα άτομα.
- **Πολιτικές ασφαλείας:** Οι οργανισμοί μπορούν να εφαρμόσουν πολιτικές ασφαλείας για να διασφαλίσουν ότι οι υπάλληλοί τους κατανοούν τις ευθύνες τους στον τομέα της ασφάλειας και τις τηρούν.
- **Έλεγχος ασφάλειας:** Τακτική παρακολούθηση του συστήματος για πιθανές κακόβουλες δραστηριότητες και ευπάθειες.

Με την εφαρμογή αυτών των μέτρων ασφαλείας, οι οργανισμοί μπορούν να προστατεύσουν τα πληροφοριακά τους συστήματα από μη εξουσιοδοτημένη πρόσβαση και χρήση και να διασφαλίσουν ότι οι ευαίσθητες πληροφορίες τους διατηρούνται εμπιστευτικές και ασφαλείς.

Το Πληροφοριακό Σύστημα είναι ένα ολοκληρωμένο σύνολο στοιχείων για τη συλλογή, την αποθήκευση, την επεξεργασία και την διακίνηση πληροφοριών. Επιχειρήσεις και άλλοι οργανισμοί βασίζονται στο πληροφοριακό σύστημα για να διαχειρίζονται τη λειτουργία τους στην αγορά, να παρέχουν υπηρεσίες και να αυξάνουν την ποιότητας ζωής των χρηστών τους (Rainer et al., 2020).

1.1.1 Τύποι πληροφοριακών συστημάτων

Τα πληροφοριακά συστήματα κατηγοριοποιούνται με βάση το πεδίο εφαρμογής, τον σκοπό και τη λειτουργικότητά τους. Ακολουθούν οι κύριοι τύποι πληροφοριακών συστημάτων (Stair & Reynolds, 2018):

- **Συστήματα επεξεργασίας συναλλαγών (Transaction Processing Systems - TPS):** Τα TPS χρησιμοποιούνται για την επεξεργασία και την καταγραφή συναλλαγών, όπως πωλήσεις, αγορές και πληρωμές. Έχουν σχεδιαστεί για να διαχειρίζονται

μεγάλο όγκο συναλλαγών και είναι ζωτικής σημασίας για τις καθημερινές λειτουργίες των επιχειρήσεων.

- **Συστήματα διαχείρισης πληροφοριών (Management Information Systems - MIS):** Τα MIS χρησιμοποιούνται για να παρέχουν στους διαχειριστές τις πληροφορίες που χρειάζονται για τη λήψη αποφάσεων. Συνήθως παρέχουν αναφορές και αναλύσεις σχετικά με την απόδοση του οργανισμού, συμπεριλαμβανομένων οικονομικών, λειτουργικών και εμπορικών δεδομένων.
- **Συστήματα υποστήριξης αποφάσεων (Decision Support System - DSS):** Τα DSS χρησιμοποιούνται για την υποστήριξη της λήψης αποφάσεων με την παροχή πληροφοριών και αναλύσεων στους χρήστες. Χρησιμοποιούν μοντέλα και αναλυτικά εργαλεία για την ανάλυση δεδομένων και την παροχή συστάσεων με βάση την ανάλυση αυτή.
- **Συστήματα υποστήριξης στελεχών (Executive Support Systems - ESS):** Τα ESS χρησιμοποιούνται για την υποστήριξη της λήψης στρατηγικών αποφάσεων από ανώτερα στελέχη. Παρέχουν υψηλού επιπέδου περιλήψεις δεδομένων και αναλύσεων, συνήθως με τη μορφή πινάκων ελέγχου και άλλων οπτικοποιήσεων.
- **Συστήματα προγραμματισμού επιχειρησιακών πόρων (Enterprise Resource Planning Systems - ERPS):** Τα συστήματα ERPS χρησιμοποιούνται για τη διαχείριση και ολοκλήρωση όλων των επιχειρηματικών διαδικασιών και δεδομένων ενός οργανισμού. Συνήθως περιλαμβάνουν ενότητες για τα οικονομικά, το ανθρώπινο δυναμικό, τη διαχείριση αποθεμάτων και άλλους τομείς της επιχείρησης.
- **Συστήματα διαχείρισης πελατειακών σχέσεων (Customer Relationship Management Systems - CRMS):** Τα συστήματα CRMS χρησιμοποιούνται για τη διαχείριση των αλληλεπιδράσεων και των σχέσεων με τους πελάτες. Παρέχουν μια εικόνα 360 μοιρών για τον πελάτη, συμπεριλαμβανομένου του ιστορικού αγορών, των προτιμήσεων και των ανατροφοδοτήσεών του.
- **Συστήματα διαχείρισης εφοδιαστικής αλυσίδας (Supply Chain Management Systems - SCMS):** Τα συστήματα SCMS χρησιμοποιούνται για τη διαχείριση της ροής αγαθών και υπηρεσιών από τους προμηθευτές στους πελάτες. Περιλαμβάνουν ενότητες για τη διαχείριση αποθεμάτων, την εφοδιαστική και τις προμήθειες.
- **Συστήματα διαχείρισης γνώσης (Knowledge Management Systems - KMS):** Τα KMS χρησιμοποιούνται για τη σύλληψη, την αποθήκευση και την ανταλλαγή

γνώσεων και τεχνογνωσίας εντός ενός οργανισμού. Περιλαμβάνουν εργαλεία για συνεργασία, διαχείριση περιεχομένου και αναζήτηση.

- **Συστήματα γεωγραφικών πληροφοριών (Geographic Information Systems - GIS):** Τα GIS χρησιμοποιούνται για τη διαχείριση και ανάλυση χωρικών δεδομένων. Χρησιμοποιούνται σε τομείς όπως ο αστικός σχεδιασμός, η περιβαλλοντική διαχείριση και η διαχείριση των φυσικών πόρων.
- **Συστήματα εμπειρογνωμόνων (Expert Systems - ES):** Τα ES χρησιμοποιούνται για την παροχή συμβουλών και τη λήψη αποφάσεων σε επίπεδο εμπειρογνωμόνων σε συγκεκριμένους τομείς. Συνήθως βασίζονται σε συστήματα βασισμένα σε κανόνες ή σε συστήματα βασισμένα στη γνώση.

1.1.2 Πλεονεκτήματα και Μειονεκτήματα

Τα πλεονεκτήματα της εφαρμογής των πληροφοριακών συστημάτων και των μέτρων ασφάλειας τους περιλαμβάνουν (Pearlson, Saunders & Galletta, 2024):

- **Προστασία των ευαίσθητων πληροφοριών:** Με την εφαρμογή μέτρων ασφαλείας, οι οργανισμοί μπορούν να προστατεύσουν τις ευαίσθητες πληροφορίες τους από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διατάραξη, τροποποίηση ή καταστροφή.
- **Συμμόρφωση:** Η εφαρμογή της ασφάλειας πληροφοριών μπορεί να βοηθήσει τους οργανισμούς να ανταποκριθούν στις απαιτήσεις συμμόρφωσης, όπως οι HIPAA(Healthcare Insurance Portability and Accountability), PCI-DSS (Payment Card Industry Data Security Standard), GDPR, και SOX (Sarbanes – Oxley Act).
- **Διαχείριση κινδύνων:** Με την εφαρμογή μέτρων ασφαλείας, οι οργανισμοί μπορούν να διαχειριστούν καλύτερα τους κινδύνους που σχετίζονται με τα πληροφοριακά τους συστήματα.
- **Επιχειρησιακή συνέχεια:** Προστατεύοντας τα συστήματα πληροφοριών από φυσικές καταστροφές, διακοπές ρεύματος και άλλες διαταραχές, οι οργανισμοί μπορούν να διασφαλίσουν ότι οι επιχειρηματικές τους δραστηριότητες μπορούν να συνεχιστούν απρόσκοπτα.

- **Εξοικονόμηση κόστους:** Η εφαρμογή μέτρων ασφαλείας μπορεί να βοηθήσει τους οργανισμούς να αποφύγουν δαπανηρές παραβιάσεις δεδομένων και άλλα περιστατικά ασφαλείας.

Τα μειονεκτήματα της εφαρμογής του συστήματος πληροφοριών και της ασφάλειας περιλαμβάνουν (Pearlson, Saunders & Galletta, 2024):

- **Κόστος:** Η εφαρμογή μέτρων ασφαλείας μπορεί να είναι δαπανηρή, καθώς μπορεί να απαιτεί πρόσθετους πόρους, όπως εμπειρογνώμονες ασφαλείας, για τη διαχείριση της διαδικασίας.
- **Καθυστέρηση:** Η εφαρμογή μέτρων ασφαλείας μπορεί να είναι χρονοβόρα, ιδίως για οργανισμούς που δεν έχουν χρησιμοποιήσει προηγουμένως αυτό το πλαίσιο.
- **Πολυπλοκότητα:** Η εφαρμογή μέτρων ασφαλείας μπορεί να είναι πολύπλοκη, ιδίως για οργανισμούς που έχουν να προστατεύσουν πολλά δεδομένα και συστήματα.
- **Ευκαμψία:** Τα μέτρα ασφαλείας μπορεί να είναι άκαμπτα, καθιστώντας δύσκολο για τους οργανισμούς να ανταποκριθούν γρήγορα στις μεταβαλλόμενες ανάγκες ασφαλείας.
- **Περιορισμένη προσαρμοστικότητα:** Τα μέτρα ασφαλείας είναι προκαθορισμένα, τα οποία αν δεν μπορούν να προσαρμοστούν στις νέες τεχνολογίες, μπορεί να απαιτούν ενημέρωση ή αναθεώρηση για να προσαρμοστούν στη νέα τεχνολογία.

1.2 Κυβερνοτρομοκρατία

Η κυβερνοτρομοκρατία αναφέρεται στη χρήση του διαδικτύου, των μέσων πληροφόρησης και των πλατφορμών επικοινωνίας για τη διεξαγωγή τρομοκρατικών επιθέσεων ή την προώθηση τρομοκρατικών σκοπών. Οι επιθέσεις αυτές μπορεί να λάβουν πολλές μορφές, όπως η διάδοση προπαγάνδας, η κλοπή ή η χειραγώγηση δεδομένων ή η διατάραξη κρίσιμων υποδομών. Είναι επίσης δυνατόν να αναφερθούν ως πράξη μη εξουσιοδοτημένων επιθέσεων και απειλών κατά υπολογιστών, δικτύων και των δεδομένων που φιλοξενούν και διαδίδουν (Theohary & Rollins, 2015).

Για την επίτευξη ενός πολιτικού ή κοινωνικού στόχου, αυτό γίνεται μέσω του εκφοβισμού ή της απειλής μιας κυβέρνησης ή των πολιτών της. Οι κυβερνοεπιθέσεις υψηλής έντασης μπορούν επίσης να προκαλέσουν βία κατά προσώπων ή περιουσίας, ή τουλάχιστον αρκετές

ζημιές ώστε να εμπνεύσουν φόβο. Τις περισσότερες φορές, η κυβερνοτρομοκρατία μπορεί να οδηγήσει σε θάνατο ή σωματική βλάβη (π.χ., έκρηξη, αεροπορικό ατύχημα, ρύπανση των υδάτων) ή μεγάλη οικονομική ή πολιτική απώλεια. Για να έχει μεγάλο αποτέλεσμα, η κυβερνοτρομοκρατία μπορεί να διεξαχθεί κατά βασικών υποδομών. Οι επιθέσεις που παρεμβαίνουν σε περιττές υπηρεσίες ή αποτελούν απλώς ενόχληση δεν χρειάζεται να αναφέρονται. Η κυβερνοτρομοκρατία είναι η σκόπιμη χρήση των δυνατοτήτων του κυβερνοχώρου, συχνά από μη κρατικούς φορείς, με πρωταρχική πρόθεση την πρόκληση ευρέως φόβου, πανικού ή διαταραχής σε έναν πληθυσμό, μια κυβέρνηση ή έναν οργανισμό. Οι πράξεις κυβερνοτρομοκρατίας περιλαμβάνουν συνήθως επιθέσεις με πολιτικά, ιδεολογικά ή κοινωνικά κίνητρα που στοχεύουν κρίσιμες υποδομές, έχουν ως αποτέλεσμα σημαντική ζημία ή συνιστούν σοβαρή απειλή για την εθνική ασφάλεια. Αυτό που διακρίνει την κυβερνοτρομοκρατία από άλλες κυβερνοεπιθέσεις, όπως το κυβερνοέγκλημα ή ο χακτιβισμός, είναι η ρητή πρόθεση υποκίνησης του τρόμου ή αποσταθεροποίησης των κοινωνιών, συχνά για την επιδίωξη πολιτικών ή ιδεολογικών στόχων και όχι καθαρά οικονομικού κέρδους ή επιδίωξης κοινωνικών ή ηθικών στόχων. Η κυβερνοτρομοκρατία επιδιώκει να δημιουργήσει φόβο, χάος και δυσπιστία σε μεγαλύτερη κλίμακα, συχνά με τη δυνατότητα να προκαλέσει βλάβη ή καταστροφή στον πραγματικό κόσμο (Theohary & Rollins, 2015).

Η έννοια της κυβερνοτρομοκρατίας μπορεί να μην είναι επαρκώς κατανοητή. Οι πρόσφατες προσπάθειες να διευρυνθεί ο ορισμός της κυβερνοτρομοκρατίας ώστε να συμπεριλάβει τον χακτιβισμό και τη χρήση του Διαδικτύου από τους τρομοκράτες για την προώθηση της συμβατικής τρομοκρατίας ευθύνονται κυρίως για την αβεβαιότητα γύρω από τον όρο. Η μεγαλύτερη διαδικτυακή απειλή που θέτει μια μη κρατική τρομοκρατική ομάδα προέρχεται από την ικανότητά της να χρησιμοποιεί το Διαδίκτυο για σκοπούς άλλους από την κυβερνοτρομοκρατία, όπως η συγκέντρωση κεφαλαίων, η έρευνα στόχων και η στρατολόγηση υποστηρικτών. Αν και η κυβερνοτρομοκρατία μπορεί να προκύψει στο μέλλον, το διαδικτυακό έγκλημα, ο χακτιβισμός και ο κυβερνοπόλεμος αποτελούν πιο άμεσες απειλές (Kenney, 2015).

Ένα εντυπωσιακό χαρακτηριστικό της κατανόησής μας για το έγκλημα στον κυβερνοχώρο είναι η ποικιλία των όρων που χρησιμοποιούνται για την περιγραφή του. Παρά το ευρύ φάσμα της ορολογίας που χρησιμοποιείται, υπάρχει ένα κοινό νήμα που ξεχωρίζει. Σε παλαιότερους τρόπους σκέψης σχετικά με την κατάχρηση της τεχνολογίας των

πληροφοριών, αυτή ονομαζόταν «έγκλημα μέσω υπολογιστή». Πριν από το Διαδίκτυο, οι υπολογιστές ήταν ο πρωταρχικός στόχος του εγκλήματος, οπότε αυτή η ονομασία φαινόταν κατάλληλη. Παρόλο που η δικτυωμένη πληροφορική διαδόθηκε ευρέως τη δεκαετία του 1990, ο όρος αυτός συνέχισε να χρησιμοποιείται. Μέχρι το 2000, ήταν ο πιο συχνά χρησιμοποιούμενος όρος για τα εγκλήματα που σχετίζονται με την τεχνολογία των πληροφοριών. Άλλες λέξεις, όπως e-crime, online crime, digital crime, net crime, techno-crime, Internet crime, ή ακόμη και hi-tech crime, έχουν χρησιμοποιηθεί σε διάφορες χρονικές στιγμές. Στο παρελθόν, η φράση που χρησιμοποιούνταν για να χαρακτηρίσει το έγκλημα ήταν το έγκλημα ηλεκτρονικών υπολογιστών. Η ακαδημαϊκή βιβλιογραφία για το έγκλημα στον κυβερνοχώρο περιέχει δύο φορές περισσότερες αναφορές στον όρο αυτό. Ωστόσο, μέχρι το 2018, η κατάσταση είχε αλλάξει σημαντικά. Στις επιστημονικές πηγές μεταξύ του 2001 και του 2018, υπήρχαν διπλάσιες αναφορές στο έγκλημα στον κυβερνοχώρο από ότι στο «έγκλημα των υπολογιστών», καθιστώντας το έγκλημα στον κυβερνοχώρο τον προτιμώμενο όρο (Kapto, 2013).

Το πρόβλημα εγκλήματος στον κυβερνοχώρο υπάρχει για περισσότερες από τρεις δεκαετίες με διάφορες μορφές. Καθώς η τεχνολογία χρησιμοποιείται ευρύτερα και οι εγκληματικές δυνατότητές της αναγνωρίζονται ευρύτερα, ορισμένες μορφές κυβερνοεπιθέσεων που αναφέρονται από τη βιομηχανία φαίνεται να αυξάνονται σε κλίμακα και εύρος. Η ευαισθητοποίηση του κοινού έχει επίσης αυξηθεί, όπως και η αναγνώριση από τις κυβερνήσεις, τις επιχειρήσεις και τα νομικά συστήματα. Γενικά ήταν εξαιρετικά δύσκολο να μετρηθεί με ακρίβεια η κλίμακα και οι τάσεις του εγκλήματος στον κυβερνοχώρο (όχι μόνο οι επιθέσεις) ή να εκτιμηθούν οι ζημίες και οι επιπτώσεις που προκαλούνται από επιτυχημένες επιθέσεις (Furnell & Dowling, 2019).

Ο κυβερνοπόλεμος είναι η λέξη-ομπρέλα για τις επιθέσεις σε δίκτυα υπολογιστών και τις άμυνες εναντίον τους, καθώς και για μοναδικές τεχνολογικές δραστηριότητες. Ο κυβερνοπόλεμος είναι ο όρος που χρησιμοποιείται για να περιγράψει όταν μια χώρα χρησιμοποιεί ψηφιακές επιθέσεις, όπως ιούς υπολογιστών και hacking, για να βλάψει, να σκοτώσει και να καταστρέψει τα κρίσιμα συστήματα υπολογιστών μιας άλλης χώρας. Στο μέλλον, οι χάκερς θα πολεμούν παράλληλα με τα παραδοσιακά όπλα, όπως τα όπλα και οι πύραυλοι, επιτιθέμενοι στις υποδομές του αντιπάλου χρησιμοποιώντας κώδικα υπολογιστή. Ο κυβερνοπόλεμος έχει αναδειχθεί σε μια τακτική και θανατηφόρα πτυχή των διεθνών συγκρούσεων σε έναν κόσμο που εξακολουθεί να είναι γεμάτος με κατασκόπους, χάκερ και

άκρως απόρρητα προγράμματα ψηφιακών όπλων. Ωστόσο, τώρα υπάρχει πραγματικός κίνδυνος οι καταστάσεις να ξεφύγουν γρήγορα από τον έλεγχο λόγω του συνεχούς ανταγωνισμού των όπλων στον κυβερνοπόλεμο και της απουσίας καθορισμένων κατευθυντήριων γραμμών που διέπουν τις διαδικτυακές μάχες (Furnell & Dowling, 2019).

Η κυβερνοτρομοκρατία προκαλλεί αυξανόμενη ανησυχία λόγω της αυξανόμενης εξάρτησης από την τεχνολογία πληροφοριών σε πολλές πτυχές της κοινωνίας και της πιθανότητας σημαντικής διακοπής ή βλάβης που προκαλείται από κυβερνοεπιθέσεις. Είχε σημαντικό αντίκτυπο παγκοσμίως και συνεχίζει να απειλεί τις διάφορες πτυχές της σταθερότητας ενός έθνους. Μία από τις μεγαλύτερες επιπτώσεις των κυβερνοεπιθέσεων είναι η διακοπή ζωτικής σημασίας υποδομής, όπως τα δίκτυα μεταφορών, τα δίκτυα ηλεκτρικής ενέργειας και τα τραπεζικά δίκτυα. Οι κατευθυνόμενες επιθέσεις σε αυτά τα συστήματα μπορεί να έχουν εκτεταμένες συνέπειες, όπως διακοπές ρεύματος, καθυστερήσεις στη μεταφορά και οικονομικές απώλειες (Caplan, 2013).

Επιπλέον, η κυβερνοτρομοκρατία έχει χρησιμοποιηθεί για τη διάδοση προπαγάνδας και τη χειραγώγηση της κοινής γνώμης, καθώς και για την κλοπή ευαίσθητων πληροφοριών, όπως πνευματική ιδιοκτησία ή προσωπικά δεδομένα. Ο φόβος της κυβερνοτρομοκρατίας έχει επίσης οδηγήσει σε αυξημένες δαπάνες για μέτρα κυβερνοασφάλειας από τις κυβερνήσεις και τις ιδιωτικές εταιρείες. Ο κόσμος έχει επηρεαστεί με διάφορους τρόπους από την πράξη των επιθέσεων στον κυβερνοχώρο, όπως ζημιές σε υποδομές, νομισματική κρίση, οικονομική κρίση, διάδοση προπαγάνδας ή παραπληροφόρησης, απώλεια ευαίσθητων πληροφοριών και παραβίαση της ιδιωτικής ζωής κ.λπ. Η κυβερνοτρομοκρατία μπορεί να οδηγήσει σε σημαντικές οικονομικές απώλειες για επιχειρήσεις και κυβερνήσεις, καθώς και βλάβη στη φήμη και την οικονομική σταθερότητα μιας χώρας. Μπορεί να χρησιμοποιηθεί για τη διάδοση προπαγάνδας και τη χειραγώγηση της κοινής γνώμης, η οποία μπορεί να οδηγήσει σε κοινωνική και πολιτική αστάθεια. Οι επιθέσεις στον κυβερνοχώρο μπορεί να οδηγήσουν σε κλοπή ευαίσθητων πληροφοριών, όπως πνευματικής ιδιοκτησίας ή προσωπικών δεδομένων, που μπορεί να έχει βαθιές συνέπειες για άτομα και οργανισμούς. Ο φόβος της εμπλοκής στη μοχθηρή πράξη της κυβερνοεισβολής έχει οδηγήσει σε αυξημένες δαπάνες για μέτρα κυβερνοασφάλειας από τις κυβερνήσεις και τις ιδιωτικές εταιρείες. Οι κυβερνοεπιθέσεις μπορεί να οδηγήσουν σε απώλεια της ιδιωτικής ζωής, καθώς τα προσωπικά δεδομένα κλέβονται ή δημοσιοποιούνται (Bryan Foltz, 2004).

Συνολικά, η κυβερνοτρομοκρατία μπορεί να προκαλέσει σημαντική αναστάτωση και βλάβη, τόσο στα άτομα όσο και στην κοινωνία. Τα αναφερόμενα ερευνητικά έργα προορίζονται για ένα ευρύ φάσμα κοινού, συμπεριλαμβανομένων επιχειρήσεων, εταιρειών, κυβερνητικών φορέων και ιδιωτών για να αποκτήσουν ποικίλη ευαισθητοποίηση σχετικά με όλες αυτές τις απειλές που τους απειλούν (Bryan Foltz, 2004).

1.3 Απειλές και Ευπάθειες

Οι απειλές και οι ευπάθειες στην κυβερνοασφάλεια αποτελούν ένα σημαντικό ζήτημα που αντιμετωπίζουν οργανισμοί και άτομα παγκοσμίως. Αυτές οι απειλές μπορούν να προέλθουν από διάφορες πηγές και να προκαλέσουν σοβαρές επιπτώσεις στην ασφάλεια και τη λειτουργία των πληροφοριακών συστημάτων (Humayun et al., 2020).

Οι κύριες απειλές περιλαμβάνουν επιθέσεις όπως οι διάφοροι τύποι κακόβουλου λογισμικού (malware), όπως ιοί, τρωτά άλογα (Trojans), και κακόβουλα προγράμματα, που στοχεύουν στην παραβίαση της ασφάλειας των συστημάτων. Επιπλέον, οι επιθέσεις DoS (Denial of Service) και DDoS (Distributed Denial of Service) επιβαρύνουν τα δίκτυα με την υπερφόρτωσή τους, εμποδίζοντας ή περιορίζοντας την πρόσβαση σε υπηρεσίες.

Επιπλέον, οι απειλές μπορούν να προέλθουν είτε από εξωτερικές πηγές, όπως κυβερνοεπιθέσεις από κρατικούς οργανισμούς ή εγκληματικές ομάδες, είτε από εσωτερικές πηγές, όπως οι εσφαλμένες δράσεις των χρηστών ή οι αδυναμίες στη διαχείριση των πληροφοριακών συστημάτων.

Για να αντιμετωπιστούν αυτές οι απειλές, είναι σημαντικό να λαμβάνονται μέτρα για την πρόληψη και την αντιμετώπισή τους, συμπεριλαμβανομένης της ενίσχυσης των μέτρων ασφαλείας, της εκπαίδευσης των χρηστών και της συνεχούς επίβλεψης και ενημέρωσης για τις τρέχουσες απειλές και τις βέλτιστες πρακτικές ασφαλείας (Humayun et al., 2020).

Η κυβερνοασφάλεια αντιμετωπίζει μια σειρά από απειλές, οι οποίες μπορούν να έχουν σοβαρές επιπτώσεις στη λειτουργία των κρατικών συστημάτων και υποδομών. Ορισμένες από τις κύριες κατηγορίες εκφάνσεις περιστατικών στην κυβερνοασφάλεια περιλαμβάνουν (Abomhara & Køien, 2015):

- **Κυβερνοεπιθέσεις:** Αυτές οι επιθέσεις μπορούν να προέλθουν από κράτη ή μη κρατικούς φορείς και να έχουν ως στόχο τη διατάραξη της λειτουργίας των κρατικών συστημάτων, την παρακολούθηση των επικοινωνιών ή την κλοπή ευαίσθητων πληροφοριών.
- **Κυβερνοπόλεμος:** Οι κυβερνοεπιθέσεις μπορούν να εξελιχθούν σε μια μορφή κυβερνοπολέμου, όπου ένα κράτος χρησιμοποιεί κυβερνοεπιθέσεις για να απειλήσει ή να επιτεθεί σε άλλα κράτη.

- **Κυβερνοτρομοκρατία:** Οι τρομοκρατικές οργανώσεις μπορούν να χρησιμοποιήσουν κυβερνοεπιθέσεις για να προκαλέσουν πανικό ή να προκαλέσουν ζημιές στις υποδομές και τα συστήματα ενός κράτους.
- **Κυβερνοκατασκοπεία:** Ορισμένες κυβερνοεπιθέσεις έχουν ως στόχο την παρακολούθηση ή την κλοπή ευαίσθητων πληροφοριών από κυβερνητικά συστήματα ή οργανισμούς.
- **Διακινδύνευση της εθνικής ασφάλειας:** Οι επιθέσεις στην κυβερνοασφάλεια μπορούν να διακινδυνεύσουν την εθνική ασφάλεια ενός κράτους, προκαλώντας σοβαρές οικονομικές, κοινωνικές ή πολιτικές επιπτώσεις.

Για την αντιμετώπιση αυτών των απειλών, η κυβέρνηση, οι οργανισμοί και οι επιχειρήσεις χρειάζεται να επενδύσουν σε προληπτικά μέτρα ασφάλειας, να αναπτύξουν ικανότητες στην ανίχνευση και απόκριση σε επιθέσεις και να συνεργαστούν με άλλα κράτη και οργανισμούς για την αντιμετώπιση κοινών κυβερνοασφαλειακών απειλών (Abomhara & Køien, 2015).

Οι ευπάθειες στην κυβερνοασφάλεια αναφέρονται στα σημεία που είναι ευάλωτα στις κυβερνοεπιθέσεις και τις παραβιάσεις ασφάλειας στα συστήματα και τις υποδομές της κυβέρνησης, του οργανισμού ή της επιχείρησης. Η αντιμετώπισή τους απαιτεί την εφαρμογή ισχυρών πολιτικών ασφαλείας, την αναβάθμιση των συστημάτων, τη διαχείριση αποτελεσματικών μέτρων ταυτοποίησης και πρόσβασης, καθώς και την εκπαίδευση του προσωπικού για την αναγνώριση και αντιμετώπιση κυβερνοεπιθέσεων (Abomhara & Køien, 2015).

1.4 Ρίσκο και Επιπτώσεις σε Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα

Η κυβερνοασφάλεια αποτελεί ένα σημαντικό θέμα λόγω των πολλαπλών κινδύνων και επιπτώσεων που ενέχει στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των πληροφοριακών συστημάτων (Aminzade, 2018).

Η εμπιστευτικότητα είναι ένας θεμελιώδης πυλώνας της κυβερνοασφάλειας, ο οποίος αφορά την προστασία των ευαίσθητων πληροφοριών από τη μη εξουσιοδοτημένη πρόσβαση, χρήση ή αποκάλυψη. Η διατήρηση της εμπιστευτικότητας είναι ζωτικής σημασίας για την προστασία της ιδιωτικότητας και των συμφερόντων των ατόμων και των οργανισμών.

Όταν μια πληροφορία θεωρείται εμπιστευτική, αυτό σημαίνει ότι μόνο εξουσιοδοτημένα άτομα έχουν το δικαίωμα να έχουν πρόσβαση σε αυτήν. Οι ευαίσθητες πληροφορίες μπορεί να περιλαμβάνουν προσωπικά δεδομένα, εμπιστευτικές συνομιλίες, εμπιστευτικά έγγραφα ή εμπορικά μυστικά (Aminzade, 2018).

Ένα παράδειγμα έλλειψης εμπιστευτικότητας είναι όταν ένας χρήστης αποκτά πρόσβαση σε προσωπικά δεδομένα ενός άλλου χρήστη χωρίς την εξουσιοδοτημένη άδεια. Αυτό μπορεί να συμβεί μέσω διαρροών δεδομένων, ευπάθειας στο λογισμικό ή την υποκλοπή διαπραγματεύσεων. Η μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες μπορεί να έχει σοβαρές επιπτώσεις, συμπεριλαμβανομένων της κατάχρησης των δεδομένων, της παραβίασης της ιδιωτικότητας και της απώλειας εμπιστοσύνης στον οργανισμό ή το σύστημα που παραβιάστηκε.

Η ακεραιότητα αποτελεί έναν ακόμα σημαντικό πυλώνα της κυβερνοασφάλειας και αφορά τη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή και αναλλοίωτη κατάσταση. Σε άλλα λόγια, η ακεραιότητα εξασφαλίζει ότι τα δεδομένα παραμένουν ανέπαφα από μη εξουσιοδοτημένες τροποποιήσεις (Yee & Zolkipli, 2021).

Η απώλεια της ακεραιότητας μπορεί να προκληθεί από διάφορες απειλές και επιθέσεις, όπως η εισβολή σε ένα σύστημα ή η ανεπιθύμητη τροποποίηση δεδομένων από εξουσιοδοτημένους χρήστες. Μια τέτοια παραβίαση μπορεί να προκαλέσει σοβαρές επιπτώσεις, όπως οικονομικές απώλειες, παραβίαση της εμπιστευτικότητας, απώλεια εμπιστοσύνης των χρηστών, ή ακόμα και παραβίαση της ασφάλειας.

Ένα παράδειγμα απώλειας ακεραιότητας είναι όταν ένας χρήστης τροποποιεί τα δεδομένα των τραπεζικών λογαριασμών που αποθηκεύονται σε ένα πληροφοριακό σύστημα. Αυτό μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, καθώς μπορεί να δημιουργήσει χρηματοοικονομικά προβλήματα για τους κατόχους των λογαριασμών, νομικές συνέπειες για τις τράπεζες και απώλεια εμπιστοσύνης από το κοινό (Yee & Zolkipli, 2021).

Για την αντιμετώπιση αυτών των κινδύνων, είναι σημαντικό να λαμβάνονται μέτρα για την ενίσχυση της ακεραιότητας των δεδομένων, όπως η χρήση τεχνικών ασφαλείας, η παρακολούθηση των δεδομένων για ανιχνευση παραβιάσεων και η υιοθέτηση πρακτικών για τον έλεγχο της πρόσβασης και των δικαιωμάτων των χρηστών.

Η διαθεσιμότητα αποτελεί έναν ακόμα βασικό πυλώνα της κυβερνοασφάλειας και αφορά την εξασφάλιση ότι τα συστήματα, τα δίκτυα, τα δεδομένα και οι υπηρεσίες είναι διαθέσιμα όταν τα χρειάζονται οι χρήστες. Σε άλλα λόγια, η διαθεσιμότητα εξασφαλίζει ότι οι χρήστες μπορούν να έχουν πρόσβαση στις υπηρεσίες και τα δεδομένα όποτε τα χρειάζονται, χωρίς καθυστερήσεις ή διακοπές (Kure, Islam & Razzaque, 2018).

Η απώλεια διαθεσιμότητας μπορεί να προκληθεί από διάφορους λόγους, όπως η καταστροφή ενός διακομιστή ή η διακοπή του δικτύου. Αυτό μπορεί να οδηγήσει σε αδυναμία πρόσβασης στις εφαρμογές ή τα δεδομένα που αποθηκεύονται σε αυτόν, με αποτέλεσμα να παρεμποδίζεται η κανονική λειτουργία της οργάνωσης ή της υπηρεσίας.

Ένα παράδειγμα απώλειας διαθεσιμότητας είναι η υποστολή λειτουργίας ενός διακομιστή λόγω ζημιάς στον εξοπλισμό ή λόγω επιθέσεων κακόβουλου λογισμικού. Κατά τη διάρκεια αυτής της περιόδου αδιαθεσίας, οι χρήστες δεν θα μπορούν να αποκτήσουν πρόσβαση σε εφαρμογές ή δεδομένα που εξυπηρετούνται από αυτόν το διακομιστή, με αναμενόμενες σοβαρές επιπτώσεις στην εταιρική λειτουργία, την εξυπηρέτηση πελατών και την αξιοπιστία της οργάνωσης (Kure, Islam & Razzaque, 2018).

Για την αντιμετώπιση αυτού του κινδύνου, είναι σημαντικό να λαμβάνονται μέτρα για την προστασία και την αποκατάσταση της διαθεσιμότητας, όπως η χρήση εφεδρικών συστημάτων και δικτύων, η εφαρμογή μεθόδων επισκευής και αναγέννησης, καθώς και η ανάπτυξη σχεδίων επαναφοράς καταστάσεων.

Συνολικά, οι απειλές στην κυβερνοασφάλεια αποτελούν σοβαρό κίνδυνο για την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών και των πληροφοριακών συστημάτων της κυβέρνησης. Για να αντιμετωπιστούν αυτές οι απειλές, απαιτούνται ισχυρά μέτρα ασφαλείας, εκπαίδευση του προσωπικού και συνεχής παρακολούθηση του κυβερνοασφαλειακού τοπίου (Kure, Islam & Razzaque, 2018).

2 Διαδίκτυο των Πραγμάτων (IoT)

Το Διαδίκτυο των Πραγμάτων, ή IoT (Internet of Things), αποτελεί ένα σύστημα συνδεδεμένων υπολογιστικών συσκευών, ψηφιακών μηχανών, αντικειμένων ή ακόμα και ανθρώπων, τα οποία διαθέτουν μοναδικά αναγνωριστικά (unique identifiers / UIDs) και μπορούν να ανταλλάσσουν δεδομένα μέσω δικτύου χωρίς την ανάγκη για ανθρώπινη επέμβαση. Για παράδειγμα, ένα αντικείμενο στο IoT μπορεί να είναι ένα αυτοκίνητο με ενσωματωμένους αισθητήρες που ειδοποιούν τον οδηγό για χαμηλή πίεση ελαστικών ή οποιαδήποτε άλλη πληροφορία που αφορά την κατάσταση του οχήματος (Rose, Eldridge & Chapin, 2015).

Το IoT επιτρέπει την εκχώρηση διευθύνσεων Πρωτοκόλλου Διαδικτύου (Internet Protocol / IP) σε φυσικά αντικείμενα, επιτρέποντάς τους να επικοινωνούν δεδομένα μέσω δικτύου. Ολοένα και περισσότερες επιχειρήσεις και οργανισμοί σε διάφορους κλάδους χρησιμοποιούν το IoT για να λειτουργούν πιο αποτελεσματικά, να κατανοούν καλύτερα τις ανάγκες των πελατών τους, να παρέχουν βελτιωμένη εξυπηρέτηση πελατών, να λαμβάνουν καλύτερες αποφάσεις και να αυξάνουν την αξία της επιχείρησής τους (Rose, Eldridge & Chapin, 2015).

2.1. Εισαγωγή στις περιπτώσεις χρήσης (use cases-components)

Το Διαδίκτυο των Πραγμάτων (IoT) έχει φέρει επανάσταση στον τρόπο με τον οποίο αλληλοεπιδρούμε με την τεχνολογία συνδέοντας διάφορες συσκευές στο διαδίκτυο, δίνοντάς τους τη δυνατότητα να επικοινωνούν και να μοιράζονται δεδομένα. Αυτό το διασυνδεδεμένο δίκτυο συσκευών έχει βρει εφαρμογή σε πολλούς τομείς, ο καθένας με τις δικές του μοναδικές περιπτώσεις χρήσης και εξαρτήματα (Bhattacharjee, 2018).

Περιπτώσεις χρήσης IoT

- **Έξυπνος αυτοματισμός σπιτιού:** Οι συσκευές IoT όπως οι έξυπνοι θερμοστάτες, τα συστήματα φωτισμού και οι κάμερες ασφαλείας επιτρέπουν στους ιδιοκτήτες σπιτιού να ελέγχουν και να παρακολουθούν εξ αποστάσεως τα σπίτια τους. Για παράδειγμα, οι χρήστες μπορούν να προσαρμόσουν τις ρυθμίσεις θερμοκρασίας, να

ανάψουν/σβήσουν τα φώτα και να λαμβάνουν ειδοποιήσεις για ύποπτη δραστηριότητα.

- **Παρακολούθηση υγειονομικής περίθαλψης:** Οι συσκευές IoT, όπως φορετοί ιχνηλάτες γυμναστικής και ιατρικά εμφυτεύματα επιτρέπουν τη συνεχή παρακολούθηση της υγείας. Συλλέγουν δεδομένα σχετικά με τα ζωτικά σημεία, τα επίπεδα δραστηριότητας και την τήρηση των φαρμάκων, παρέχοντας πολύτιμες γνώσεις στους επαγγελματίες υγείας και βελτιώνοντας τα αποτελέσματα των ασθενών.
- **Βιομηχανικό IoT (IIoT):** Σε κατασκευαστικές και βιομηχανικές ρυθμίσεις, οι αισθητήρες και οι ενεργοποιητές IoT παρακολουθούν την απόδοση του εξοπλισμού, εντοπίζουν σφάλματα και βελτιστοποιούν τις διαδικασίες παραγωγής. Το IIoT ενισχύει την αποδοτικότητα, μειώνει το χρόνο διακοπής λειτουργίας και διευκολύνει την προγνωστική συντήρηση.
- **Έξυπνες πόλεις:** Οι τεχνολογίες IoT χρησιμοποιούνται για την αποτελεσματική διαχείριση των αστικών υποδομών και υπηρεσιών. Τα έξυπνα συστήματα διαχείρισης της κυκλοφορίας, οι λύσεις διαχείρισης απορριμμάτων και οι αισθητήρες περιβαλλοντικής παρακολούθησης βοηθούν τις πόλεις να ελαχιστοποιήσουν τη συμφόρηση, να βελτιώσουν τη δημόσια ασφάλεια και να ενισχύσουν τη βιωσιμότητα.
- **Γεωργία ακριβείας:** Οι αισθητήρες IoT που αναπτύσσονται σε γεωργικά χωράφια συλλέγουν δεδομένα για την υγρασία του εδάφους, τη θερμοκρασία και την υγεία των καλλιεργειών. Αυτές οι πληροφορίες επιτρέπουν στους αγρότες να λαμβάνουν αποφάσεις βάσει δεδομένων σχετικά με την άρδευση, τη λίπανση και τον έλεγχο των παρασίτων, οδηγώντας σε αυξημένες αποδόσεις και αποδοτικότητα των πόρων.

Συστατικά του IoT

- **Αισθητήρες και ενεργοποιητές:** Αυτές οι συσκευές συλλέγουν δεδομένα από το περιβάλλον (αισθητήρες) ή εκτελούν φυσικές ενέργειες με βάση την είσοδο (ενεργοποιητές). Οι αισθητήρες μετρούν παραμέτρους όπως η θερμοκρασία, η υγρασία και η κίνηση, ενώ οι ενεργοποιητές ελέγχουν διαδικασίες όπως το άνοιγμα/κλείσιμο βαλβίδων ή το γύρισμα των κινητήρων.
- **Συνδεσιμότητα:** Οι συσκευές IoT βασίζονται σε διάφορα πρωτόκολλα επικοινωνίας για τη μετάδοση δεδομένων μέσω του Διαδικτύου ή των τοπικών δικτύων. Οι κοινές

επιλογές συνδεσιμότητας περιλαμβάνουν Wi-Fi, Bluetooth, Zigbee και δίκτυα κινητής τηλεφωνίας (3G, 4G, 5G).

- **Edge Computing:** Οι συσκευές Edge επεξεργάζονται δεδομένα τοπικά, κοντά στην πηγή παραγωγής δεδομένων, πριν τα μεταδώσουν σε κεντρικούς διακομιστές ή στο cloud. Το Edge computing μειώνει τον λανθάνοντα χρόνο, τη χρήση εύρους ζώνης και την εξάρτηση από την υποδομή cloud, καθιστώντας τα συστήματα IoT πιο αποκριτικά και επεκτάσιμα.
- **Πλατφόρμες Cloud:** Τα δεδομένα IoT συνήθως αποθηκεύονται, αναλύονται και διαχειρίζονται σε πλατφόρμες cloud. Οι υπηρεσίες Cloud προσφέρουν επεκτάσιμη αποθήκευση, υπολογιστική ισχύ και εργαλεία ανάλυσης, επιτρέποντας πληροφορίες σε πραγματικό χρόνο, προγνωστικά αναλυτικά στοιχεία και απομακρυσμένη διαχείριση συσκευών.
- **Μέτρα ασφαλείας:** Με τον πολλαπλασιασμό των συσκευών IoT, η διασφάλιση της ασφάλειας των δεδομένων και του απορρήτου είναι πρωταρχικής σημασίας. Τα μέτρα ασφαλείας περιλαμβάνουν κρυπτογράφηση, μηχανισμούς ελέγχου ταυτότητας, έλεγχο ταυτότητας συσκευής, ασφαλή εκκίνηση και τακτικές ενημερώσεις λογισμικού για τον μετριασμό των τρωτών σημείων.

Συνοπτικά, το Διαδίκτυο των Πραγμάτων περιλαμβάνει ένα ευρύ φάσμα εφαρμογών και στοιχείων, από έξυπνα σπίτια και υγειονομική περίθαλψη έως βιομηχανικούς αυτοματισμούς και έξυπνες πόλεις. Αξιοποιώντας τις τεχνολογίες IoT, οι οργανισμοί μπορούν να ξεκλειδώσουν νέες ευκαιρίες για αποτελεσματικότητα, καινοτομία και βελτιωμένες εμπειρίες χρηστών (Bhattacharjee, 2018).

Εικόνα 1 - Internet of Things components

2.2. Δίκτυο

Το Δίκτυο IoT αναφέρεται στις τεχνολογίες επικοινωνίας που χρησιμοποιούν οι συσκευές Internet of Things (IoT) για την κοινή χρήση ή τη διάδοση δεδομένων σε άλλες συσκευές ή διεπαφές που είναι διαθέσιμες σε προσβάσιμη απόσταση. Διάφοροι τύποι δικτύων IoT είναι διαθέσιμοι για την επικοινωνία συσκευών/αισθητήρων IoT. Η επιλογή του κατάλληλου πρωτοκόλλου δικτύωσης για συγκεκριμένες απαιτήσεις είναι κρίσιμη για τη συλλογή δεδομένων σε πραγματικό χρόνο και την πρόσβαση σε πληροφορίες μέσω εφαρμογών IoT (Srinidhi, Kumar & Venugopal, 2019).

Καθώς ο κλάδος έρχεται επανάσταση με την αλλαγή των εποχών, η τρέχουσα βιομηχανία - Indusrty 4.0 είναι αποδέκτης της προόδου στην τεχνολογία των τηλεπικοινωνιών που έχει καινοτομήσει το IoT (Internet of Things). Το IIoT (Industrial Internet of Things), μια υποπροδιαγραφή του IoT, έχει σχεδιαστεί για να διευκολύνει την αυτοματοποίηση του κλάδου και να επιτρέπει την Έξυπνη κατασκευή.

Το IIoT εστιάζει σε παραμέτρους αποκλειστικά για τη μεταποιητική βιομηχανία και παρουσιάζει πιθανή ανάπτυξη, παραγωγή, βελτιστοποίηση και συντήρηση βιομηχανικών εκροών και εξοπλισμού, αντίστοιχα. Στην καρδιά της τεχνολογίας IoT για τις βιομηχανίες, η επιλογή του δικτύου διαδραματίζει ζωτικό ρόλο στην επιτυχία του IIoT στην Έξυπνη Παραγωγή (Srinidhi, Kumar & Venugopal, 2019).

Για να γίνει επιλογή της σύνδεσης ποιο δίκτυο υποστηρίζει κατάλληλα τις ανάγκες μιας βιομηχανίας, συνιστάται να ενημερώνεστε για τα επίπεδα δικτύου στον χώρο του IoT. Το IoT περιλαμβάνει πολλή επικοινωνία μηχανών, αναγνώριση συσκευών και επικοινωνία, μαζί με ενεργά εργαλεία μηχανικής μάθησης για ανάλυση δεδομένων. Επομένως, απαιτείται ένα ισχυρό δίκτυο για την υποστήριξη του ίδιου (Gulati et al., 2022).

Μια δομή που απεικονίζει τη στρώση δικτύου στην τεχνολογία IoT είναι η εξής:

- Επίπεδο δικτύου / συνδέσμων
- Επίπεδο Διαδικτύου
- Στρώμα μεταφοράς

- Επίπεδο Εφαρμογής

Το πρώτο επίπεδο συνδέσεων ευθυγραμμίζεται με τα πρότυπα ασύρματης δικτύωσης όπως αυτά των IEEE 802 MAC και IEEE 802 PHY, τα οποία ασχολούνται με τοπικά και μητροπολιτικά δίκτυα. Το επόμενο επίπεδο είναι το επίπεδο Διαδικτύου (IPv4/IPv6/IP Routing), το αφορά συνδεδεμένες συσκευές/συστήματα έτοιμες για Διαδίκτυο που επικοινωνούν εντός τομέων συνδεδεμένων στο Διαδίκτυο με τη βοήθεια μιας μοναδικής αναγνώρισης συσκευής (Gulati et al., 2022).

Μετά το επίπεδο διαδικτύου ακολουθεί το επίπεδο μεταφοράς που αποτελείται από τα πρωτόκολλα TCP/UDP/DTLS/HTTP συνήθως στο ενσύρματο τμήμα του δικτύου, το οποίο βοηθά στην επικοινωνία μεταξύ των συστημάτων ως μέρος των αρχών και των πρωτοκόλλων μεταφοράς. Το επίπεδο εφαρμογής στο apex δέχεται βιομηχανικές τυπικές προσεγγίσεις όπως MQTT, CoAP και API για επικοινωνία εφαρμογών μεταξύ συσκευών/συστημάτων (Bera, Misra & Vasilakos, 2017).

Τα ασύρματα δίκτυα δεν είναι νέες λύσεις στον τομέα της τεχνολογίας, αλλά έχουν υποστεί εξέλιξη και καινοτομία κατά καιρούς για την αντιμετώπιση των αυξανόμενων προκλήσεων με την συνεχή αύξηση σε συσκευές/συστήματα επικοινωνίας. Ακολουθούν οι κύριοι τύποι ασύρματων δικτύων που μπορούν να διευκολύνουν τις εφαρμογές IoT και την ανάπτυξη αισθητήρων IoT σε βιομηχανίες.

- RFID
- BLE / NFC
- WIFI / LoFI
- Πρωτόκολλα MESH
- LPWAN (LoRa, Sigfox)
- Κινητό (3G / 4G /5G)

Εισάγονται προοδευτικά πρότυπα για την μείωση της λειτουργικής πολυπλοκότητας, από τη σάρωση και την επικοινωνία RFID έως την επικοινωνία δεδομένων Bluetooth (BLE/NFC). Παρόλο που το BLE/NFC είναι ενσωματωμένο στη λειτουργία των κινητών τηλεφώνων,

άλλα πρωτόκολλα δικτύου εξυπηρετούν αποκλειστικά τον σκοπό της ανάπτυξης του IoT σύμφωνα με τις απαιτήσεις του κλάδου (Bera, Misra & Vasilakos, 2017).

Η ανάπτυξη του IoT υποστηρίζεται από τα πρωτόκολλα δικτύου κινητής τηλεφωνίας (2G, 3 G, 4G & 5G) παρότι τα συμβατικά πρωτόκολλα δεν είναι κατάλληλα για IoT, και WiFi / LoFI παρέχοντας αποτελεσματική τοπική δικτύωση συσκευών μικρής εμβέλειας και πρόσβαση στο διαδίκτυο.

Τα πρωτόκολλα MESH αποτελούνται από ραδιοκόμβους οργανωμένους σε μια τοπολογία πλέγματος για την κατανεμημένη σύνδεση συσκευών και κόμβων, την μεταφορά δεδομένων και επικοινωνία που μπορούν να επιλεγούν στην ανάπτυξη IoT με βάση τις ανάγκες των πελατών.

Τα LPWAN (LoRa, Sigfox) είναι σύγχρονα πρότυπα που αναφέρονται σε ένα δίκτυο ευρείας περιοχής χαμηλής κατανάλωσης που στόχο έχει να μειώνει την κατανάλωση ενέργειας ενώ προσφέρει ένα προηγμένο και ευρείας κλίμακας δίκτυο για συνδεσιμότητα. Έχει σχεδιαστεί για να διευκολύνει τις ασύρματες επικοινωνίες μεγάλης εμβέλειας με χαμηλό ρυθμό μετάδοσης bit μεταξύ συνδεδεμένων συσκευών/συστημάτων (Bera, Misra & Vasilakos, 2017).

2.3. Κυβερνοασφάλεια σε IoT

Με την ταχεία ανάπτυξη του IoT, νέες απειλές και προκλήσεις για την ασφάλεια εμφανίζονται σε όλους τους κλάδους. Το IoT αλλάζει την αλληλεπίδραση των επιχειρήσεων και των πελατών με τον κόσμο. Η ανάπτυξη συσκευών IoT ήταν από 10 δισεκατομμύρια το 2016 σε 24 δισεκατομμύρια το 2020 – με συνεχόμενα αυξανόμενες τάσεις. Η κοινή χρήση πληροφοριών μεταξύ ετερογενών συσκευών και πηγών είναι μια τεράστια πρόκληση για την ασφάλεια στον κυβερνοχώρο. Όταν δισεκατομμύρια συσκευές IoT συνδεθούν με άλλα δίκτυα, οι κακόβουλες επιθέσεις θα αυξηθούν. Οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν συσκευές IoT ως πόρτα για να εισέλθουν σε επιχειρηματικά δίκτυα και περιβάλλον cloud (Karlov, 2017).

Η κυβερνοασφάλεια είναι η κύρια πρόκληση των εφαρμογών του IoT. Οι επιθέσεις στον κυβερνοχώρο έχουν ήδη ξεκινήσει σε συνδεδεμένες συσκευές, όπως η δυνατότητα

πειρατείας συνδεδεμένου οχήματος. Σήμερα, οι πελάτες έχουν συνειδητοποιήσει ότι οι επιλογές τους μπορούν να αναλυθούν από τις πληροφορίες τους και έχουν αρχίσει να σκέφτονται ποιος έχει πρόσβαση στα δεδομένα τους και ποιος είναι υπεύθυνος για την ασφάλειά τους. Όταν θα αλληλεπιδράσουν διαφορετικά συστήματα, θα υπάρξει μάχη μεταξύ τους για την ανταγωνιστική νοημοσύνη. Καθώς θα δημιουργήσει νέες προκλήσεις στον κυβερνοχώρο και αυτές οι προκλήσεις θα αυξήσουν τη σημασία της ασφάλειας. Επίσης, η ασφάλεια των δεδομένων είναι μια σημαντική ανησυχία για τις συσκευές IoT και θα πρέπει να ληφθεί σοβαρά υπόψη. Κάθε δεύτερη μέρα, υπάρχουν ειδήσεις για παραβιάσεις δεδομένων (Karlov, 2017).

Κάθε συνδεδεμένο αντικείμενο δημιουργεί δεδομένα και ο όγκος των δεδομένων που δημιουργούνται είναι σε zeta byte. Οι κακόβουλοι παράγοντες μπορούν να έχουν πρόσβαση σε αυτά τα ευαίσθητα δεδομένα. Ένα παράδειγμα δεδομένων θερμοστάτη. μπορεί να χρησιμοποιηθεί για την καταμέτρηση του συνολικού αριθμού ατόμων και της διαθεσιμότητάς τους. Το GPS μπορεί να χρησιμοποιηθεί για την παρακολούθηση της θέσης ενός προσώπου και της διαθεσιμότητάς του σε μια συγκεκριμένη θέση.

Αυτές οι πληροφορίες δεν φαίνονται πολύ κρίσιμες, αλλά αρκούν σε εγκληματίες για να τις χρησιμοποιήσουν για κατάχρηση εναντίον οποιουδήποτε. Τα επιχειρηματικά δεδομένα μπορούν να χρησιμοποιηθούν με τον ίδιο τρόπο. Σήμερα, αρκετές εταιρείες συλλέγουν δεδομένα κοινωνικής δικτύωσης, όπως η Google, η Yahoo και το Facebook κ.λπ. και αυτά τα δεδομένα μπορούν να παραβιαστούν από χάκερ. Στις 14 Δεκεμβρίου 2016, η Yahoo αποδέχτηκε ότι 1 δισεκατομμύριο λογαριασμοί της είχαν παραβιαστεί. Οι κατασκευαστές συσκευών IoT πρέπει να κατανοήσουν ότι το απόρρητο των δεδομένων ξεκινά από την πηγή. Οι πληροφορίες δεν πρέπει να αφήνουν τον αισθητήρα χωρίς προστασία. Τα δεδομένα πρέπει να κρυπτογραφηθούν πριν μεταφερθούν στο cloud για επεξεργασία και αποθήκευση (Sani et al., 2019).

Η κυβερνοασφάλεια στο IoT (Internet of Things) είναι υψίστης σημασίας λόγω της διασυνδεδεμένης φύσης των συσκευών IoT και των ευαίσθητων δεδομένων που χειρίζονται (Sani et al., 2019).

Ασφάλεια συσκευής (Karlov, 2017):

- **Έλεγχος ταυτότητας και εξουσιοδότηση:** Η διασφάλιση ότι οι συσκευές IoT είναι πιστοποιημένες και εξουσιοδοτημένες για πρόσβαση σε δίκτυα και υπηρεσίες είναι ζωτικής σημασίας. Ισχυροί μηχανισμοί ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων και τα ψηφιακά πιστοποιητικά, συμβάλλουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης.

- **Ασφαλής εκκίνηση:** Η εφαρμογή διαδικασιών ασφαλούς εκκίνησης διασφαλίζει ότι οι συσκευές IoT εκτελούν μόνο αξιόπιστο υλικολογισμικό και λογισμικό, μετριάζοντας τον κίνδυνο εκτέλεσης κακόβουλου κώδικα κατά την εκκίνηση.

- **Διαχείριση ταυτότητας συσκευής:** Κάθε συσκευή IoT θα πρέπει να έχει ένα μοναδικό αναγνωριστικό και κατάλληλα στοιχεία ελέγχου πρόσβασης για την αποφυγή πλαστοπροσωπίας ή μη εξουσιοδοτημένων συνδέσεων συσκευής.

Ασφάλεια δεδομένων (Karlov, 2017):

- **Κρυπτογράφηση:** Η κρυπτογράφηση δεδομένων τόσο κατά τη μεταφορά όσο και σε κατάσταση ηρεμίας προστατεύει ευαίσθητες πληροφορίες από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή. Τα πρωτόκολλα ασφαλούς επικοινωνίας όπως το TLS (Transport Layer Security) ή το HTTPS (Hypertext Transfer Protocol Secure) είναι απαραίτητα για την προστασία των δεδομένων κατά τη μετάδοση.

- **Ακεραιότητα δεδομένων:** Η εφαρμογή μέτρων για τη διατήρηση της ακεραιότητας των δεδομένων διασφαλίζει ότι τα δεδομένα παραμένουν αμετάβλητα και αξιόπιστα καθ' όλη τη διάρκεια του κύκλου ζωής τους. Οι λειτουργίες κατακερματισμού και οι ψηφιακές υπογραφές μπορούν να επαληθεύσουν την ακεραιότητα των δεδομένων και να ανιχνεύσουν μη εξουσιοδοτημένες τροποποιήσεις.

- **Έλεγχος πρόσβασης:** Η εφαρμογή λεπτομερών ελέγχων πρόσβασης διασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες ή συσκευές μπορούν να έχουν πρόσβαση σε συγκεκριμένα δεδομένα, μειώνοντας τον κίνδυνο παραβιάσεων ή διαρροών δεδομένων.

Ασφάλεια δικτύου (Karlov, 2017):

- **Τμηματοποίηση:** Η τμηματοποίηση δικτύων IoT από κρίσιμες υποδομές ή ευαίσθητα συστήματα μειώνει την επιφάνεια επίθεσης και περιορίζει τον πιθανό αντίκτυπο των παραβιάσεων της ασφάλειας.

- **Συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS):** Η ανάπτυξη λύσεων IDPS βοηθά στον εντοπισμό και τον μετριασμό ύποπτης δραστηριότητας δικτύου ή μη εξουσιοδοτημένων προσπαθειών πρόσβασης σε πραγματικό χρόνο.

- **Τείχη προστασίας:** Τα τείχη προστασίας φιλτράρουν την κυκλοφορία του δικτύου και επιβάλλουν πολιτικές ασφαλείας για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και την προστασία των συσκευών IoT από κακόβουλες απειλές.

Ενημερώσεις υλικολογισμικού και λογισμικού (Sani et al., 2019):

- **Διαχείριση ενημερώσεων κώδικα:** Η τακτική ενημέρωση υλικολογισμικού και λογισμικού σε συσκευές IoT βοηθά στην αντιμετώπιση γνωστών τρωτών σημείων και στην προστασία από αναδυόμενες απειλές. Τα αυτοματοποιημένα συστήματα διαχείρισης ενημερώσεων κώδικα εκσυγχρονίζουν τη διαδικασία ενημέρωσης και διασφαλίζουν ότι οι συσκευές παραμένουν ασφαλείς έναντι των εξελισσόμενων απειλών στον κυβερνοχώρο.

- **Υποστήριξη προμηθευτών:** Η επιλογή συσκευών IoT από αξιόπιστους προμηθευτές που παρέχουν συνεχή υποστήριξη και έγκαιρες ενημερώσεις ασφαλείας είναι απαραίτητη για τη διατήρηση της στάσης ασφαλείας των αναπτύξεων IoT.

Φυσική ασφάλεια (Sani et al., 2019):

- **Αντοχή σε παραβίαση:** Η εφαρμογή μέτρων φυσικής ασφάλειας, όπως περιβλήματα με προστασία από παραβίαση ή μηχανισμοί κατά της παραβίασης, αποτρέπει τη μη

εξουσιοδοτημένη πρόσβαση σε συσκευές IoT και προστατεύει από φυσικές επιθέσεις ή παραβιάσεις.

- **Διαχείριση assets:** Η διατήρηση αποθέματος συσκευών IoT, η παρακολούθηση των τοποθεσιών τους και η διασφάλιση της σωστής απόρριψης παροπλισμένων συσκευών συμβάλλει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και παραβιάσεων δεδομένων.

Θέματα απορρήτου (Sani et al., 2019):

- **Ελαχιστοποίηση δεδομένων:** Η συλλογή και αποθήκευση μόνο των απαραίτητων δεδομένων ελαχιστοποιεί τον κίνδυνο παραβιάσεων απορρήτου και παραβιάσεων δεδομένων. Η εφαρμογή τεχνολογιών που βελτιώνουν το απόρρητο, όπως η ανωνυμοποίηση ή η ψευδωνυμοποίηση, προστατεύει το απόρρητο των χρηστών, ενώ παράλληλα επιτρέπει πολύτιμες πληροφορίες από τα δεδομένα IoT.

Συνοπτικά, τα ισχυρά μέτρα κυβερνοασφάλειας είναι απαραίτητα για τον μετριασμό των κινδύνων που σχετίζονται με την ανάπτυξη του IoT. Εφαρμόζοντας ολοκληρωμένες πρακτικές ασφάλειας σε συσκευές, δίκτυα και δεδομένα, οι οργανισμοί μπορούν να ενισχύσουν την ανθεκτικότητα και την ακεραιότητα των οικοσυστημάτων IoT τους, προστατεύοντας παράλληλα ευαίσθητες πληροφορίες από απειλές στον κυβερνοχώρο και κακόβουλους παράγοντες (Sani et al., 2019).

2.4. Κυβερνοτρομοκρατία σε IoT

Η κυβερνοτρομοκρατία στο IoT (Διαδίκτυο των πραγμάτων) παρουσιάζει σημαντικές προκλήσεις και απειλές λόγω της διασυνδεδεμένης φύσης των συσκευών IoT και των πιθανών επιπτώσεών τους σε ζωτικής σημασίας υποδομές, τη δημόσια ασφάλεια και την κοινωνία στο σύνολό της (Tzezana, 2016).

Ορισμός της κυβερνοτρομοκρατίας στο IoT

Η κυβερνοτρομοκρατία περιλαμβάνει τη χρήση ψηφιακών τεχνολογιών, συμπεριλαμβανομένων των συσκευών IoT, για τη διεξαγωγή τρομοκρατικών δραστηριοτήτων ή επιθέσεων με στόχο την πρόκληση διακοπής, καταστροφής ή βλάβης σε άτομα, οργανισμούς ή κυβερνήσεις (Tzezana, 2016).

Στο πλαίσιο του IoT, η κυβερνοτρομοκρατία μπορεί να περιλαμβάνει την εκμετάλλευση τρωτών σημείων σε διασυνδεδεμένες συσκευές για διακοπή βασικών υπηρεσιών, παραβίαση υποδομών ή πρόκληση σωματικής βλάβης (Tzezana, 2016).

Πιθανοί στόχοι και επιπτώσεις (Tzezana, 2016):

- **Υποδομή ζωτικής σημασίας:** Οι συσκευές IoT ενσωματώνονται ολοένα και περισσότερο σε συστήματα υποδομής ζωτικής σημασίας, όπως δίκτυα ενέργειας, δίκτυα μεταφορών και εγκαταστάσεις υγειονομικής περίθαλψης. Οι κυβερνοτρομοκράτες μπορεί να στοχεύουν αυτά τα συστήματα για να διαταράξουν βασικές υπηρεσίες, να προκαλέσουν εκτεταμένες διακοπές λειτουργίας ή να δημιουργήσουν χάος.
- **Δημόσια ασφάλεια:** Οι συσκευές IoT που αναπτύσσονται σε συστήματα δημόσιας ασφάλειας, συμπεριλαμβανομένων των καμερών παρακολούθησης, των φωτεινών σηματοδοτών και των συστημάτων απόκρισης έκτακτης ανάγκης, αποτελούν πιθανούς στόχους για την κυβερνοτρομοκρατία. Η παραβίαση αυτών των συσκευών θα μπορούσε να εμποδίσει τις προσπάθειες αντίδρασης έκτακτης ανάγκης ή να διευκολύνει τις φυσικές επιθέσεις.
- **Οικονομική διαταραχή:** Οι επιθέσεις σε αλυσίδες εφοδιασμού με δυνατότητα IoT, χρηματοοικονομικά συστήματα ή εμπορικές επιχειρήσεις μπορεί να έχουν εκτεταμένες οικονομικές συνέπειες, οδηγώντας σε οικονομικές απώλειες, αστάθεια της αγοράς και διακοπή των επιχειρηματικών λειτουργιών.

Μέθοδοι και τεχνικές (Tzezana, 2016)

- **Εκμετάλλευση τρωτών σημείων:** Οι κυβερνοτρομοκράτες ενδέχεται να εκμεταλλευτούν ευπάθειες σε συσκευές IoT, όπως προεπιλεγμένους κωδικούς πρόσβασης, μη ασφαλή πρωτόκολλα επικοινωνίας ή ξεπερασμένο υλικολογισμικό, για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και έλεγχο σε αυτές τις συσκευές.

- **Κακόβουλο λογισμικό και Botnets:** Η ανάπτυξη κακόβουλου λογισμικού ή η δημιουργία botnets χρησιμοποιώντας παραβιασμένες συσκευές IoT επιτρέπει στους τρομοκράτες του κυβερνοχώρου να εξαπολύουν επιθέσεις μεγάλης κλίμακας κατανεμημένης άρνησης υπηρεσίας (DDoS), να διακόπτουν τις επικοινωνίες δικτύου ή να διεξάγουν συντονισμένες επιθέσεις στον κυβερνοχώρο.
- **Κοινωνική μηχανική:** Τεχνικές κοινωνικής μηχανικής, όπως μηνύματα ηλεκτρονικού ψαρέματος (phishing) ή παραπλανητικά μηνύματα, μπορούν να χρησιμοποιηθούν για τη χειραγώγηση χρηστών ή διαχειριστών συσκευών IoT ώστε να διευκολύνουν άθελά τους κυβερνοτρομοκρατικές δραστηριότητες, όπως η παραχώρηση μη εξουσιοδοτημένης πρόσβασης ή η αποκάλυψη ευαίσθητων πληροφοριών.

Προκλήσεις και προβληματισμοί (Henschke, 2021):

- **Αναφορά:** Ο εντοπισμός των δραστών κυβερνοτρομοκρατικών επιθέσεων σε περιβάλλοντα IoT μπορεί να είναι δύσκολος λόγω της ανωνυμίας που παρέχεται από το Διαδίκτυο και της πολυπλοκότητας της ανίχνευσης των επιθέσεων στην προέλευσή τους.
- **Διασυνοριακή δικαιοδοσία:** Οι κυβερνοτρομοκρατικές επιθέσεις συχνά υπερβαίνουν τα εθνικά σύνορα, θέτοντας προκλήσεις για τις υπηρεσίες επιβολής του νόμου και τη διεθνή συνεργασία για τη διερεύνηση και τη δίωξη κυβερνοτρομοκρατικών δραστηριοτήτων.
- **Ταχεία εξέλιξη του τοπίου απειλών:** Η δυναμική και εξελισσόμενη φύση των τεχνολογιών IoT, σε συνδυασμό με τον πολλαπλασιασμό νέων φορέων και τεχνικών επιθέσεων, απαιτεί συνεχή επαγρύπνηση, συνεργασία και προσαρμογή των μέτρων κυβερνοασφάλειας για την αντιμετώπιση αναδυόμενων απειλών κυβερνοτρομοκρατίας.

Αντίμετρα και στρατηγικές μετριασμού (Henschke, 2021):

- **Ενίσχυση της ασφάλειας του IoT:** Η εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας, όπως κρυπτογράφηση, έλεγχοι πρόσβασης, συστήματα ανίχνευσης εισβολών και

τακτικές ενημερώσεις ασφαλείας, συμβάλλει στον μετριασμό του κινδύνου κυβερνοτρομοκρατίας σε περιβάλλοντα IoT.

- **Ευαισθητοποίηση και εκπαίδευση του κοινού:** Η ευαισθητοποίηση των χρηστών συσκευών IoT, των διαχειριστών και των υπευθύνων χάραξης πολιτικής σχετικά με τις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο, η ευαισθητοποίηση σχετικά με τις απειλές και τα πρωτόκολλα αντιμετώπισης συμβάντων είναι απαραίτητες για την ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο και τη μείωση του αντίκτυπου των επιθέσεων κυβερνοτρομοκρατίας.
- **Διεθνής Συνεργασία:** Ενίσχυση της συνεργασίας και της ανταλλαγής πληροφοριών μεταξύ των κυβερνήσεων, των υπηρεσιών επιβολής του νόμου, των ενδιαφερόμενων μερών του κλάδου και των οργανισμών κυβερνοασφάλειας για την αποτελεσματική αντιμετώπιση των διασυνοριακών απειλών κυβερνοτρομοκρατίας.

Συμπερασματικά, η κυβερνοτρομοκρατία στο IoT θέτει σημαντικές προκλήσεις για την παγκόσμια ασφάλεια και απαιτεί μια συντονισμένη προσέγγιση πολλαπλών ενδιαφερομένων για τον μετριασμό των κινδύνων, την ενίσχυση της ανθεκτικότητας και την προστασία των ζωτικών υποδομών, της δημόσιας ασφάλειας και της κοινωνίας από απειλές και επιθέσεις στον κυβερνοχώρο (Henschke, 2021).

3 Penetration testing - Ethical Hacking

3.1. Ορισμός – Εννοιολογική προσέγγιση

Η διαδικασία του Έλεγχου Διείσδυσης, επίσης γνωστή ως Επαγγελματικό ή Ηθικό Χάκινγκ, αποτελεί μια νόμιμη διαδικασία με στόχο τον εντοπισμό αδυναμιών σε ένα σύστημα πληροφορικής και την είσοδο σε αυτό, προσομοιώνοντας μια πραγματική κυβερνοεπίθεση. Κατά τη διάρκεια αυτών των ελέγχων, χρησιμοποιούνται τεχνικές και εργαλεία που αντιστοιχούν στις μεθόδους που θα χρησιμοποιούσε ένας πραγματικός εισβολέας, καθιστώντας τους ιδιαίτερα αποτελεσματικούς (Baloch, 2017).

Οι δοκιμές αυτές μπορούν να περιλαμβάνουν όχι μόνο τα πληροφοριακά συστήματα, αλλά και κτίρια ή ακόμη και το προσωπικό ενός οργανισμού. Είναι ένα διαδεδομένο μέσο για τη διασφάλιση της ασφάλειας, καθώς πολλοί οργανισμοί το χρησιμοποιούν συστηματικά και τακτικά (Baloch, 2017).

3.1.1 Είδη Ελέγχου Διείσδυσης

Υπάρχουν πολλά είδη Ελέγχου Διείσδυσης, καθένα με διαφορετική προσέγγιση, τα οποία παρουσιάζονται παρακάτω (Yaacoub et al., 2021):

- **Έλεγχος Διείσδυσης Δικτύου (Network Penetration Testing):** Ο έλεγχος αυτός είναι ο πιο κοινός και περιλαμβάνει τον έλεγχο ανοιχτών πορτών, ευπαθειών στο δίκτυο, των routers, παράκαμψη των Firewalls, ανίχνευση ιχνών από DNS, διαμεσολαβητές, επιθέσεις σε SSH, SQL Server, αποφυγή IDS/IPS, FTP, SMTP κ.ά.

- **Έλεγχος Διείσδυσης Διαδικτυακών Εφαρμογών (Web Application Penetration Testing):** Αυτός ο έλεγχος είναι εξειδικευμένος και εστιάζει στην ανακάλυψη ευπαθειών σε διαδικτυακές εφαρμογές, συμπεριλαμβανομένων των φυλλομετρητών, προσθέτων, ActiveX, Silverlight, Scriptlets και Applets.

- **Έλεγχος από την πλευρά του τελικού χρήστη (Client-Side Penetration Testing):** Στον έλεγχο αυτόν ελέγχονται τα προγράμματα περιήγησης, τα email και άλλες εφαρμογές τελικού χρήστη για ανακάλυψη ευπαθειών όπως Clickjacking, Cross-Site

Scripting, Form Hijacking, HTML Injection, Open Redirection, μόλυνση από ιούς κ.ά.

- **Έλεγχος Διείσδυσης Ασύρματου Δικτύου (Wireless Penetration Testing):** Ο έλεγχος αυτός εξετάζει τις συνδέσεις σε ασύρματα δίκτυα και ελέγχει την ασφάλειά τους και την προστασία των δεδομένων.

- **Φυσικός Έλεγχος Διείσδυσης (Physical Penetration Testing**): Σε αυτόν τον έλεγχο προσπαθείται να παραβιαστεί η φυσική ασφάλεια των εγκαταστάσεων του οργανισμού, αναζητώντας ευπάθειες σε κλειδαριές, κάμερες, αισθητήρες κ.ά. Η αναγνώριση αυτών των ευπαθειών επιτρέπει την λήψη κατάλληλων μέτρων για την ενίσχυση της φυσικής ασφάλειας.

3.1.2 Προσεγγίσεις του Ελέγχου Διείσδυσης (Penetration Testing)

Οι προσεγγίσεις του Ελέγχου Διείσδυσης (Penetration Testing) διαφέρουν στον τρόπο που προσεγγίζουν τον στόχο τους και στο επίπεδο πληροφοριών που διαθέτουν οι ελεγκτές. Η προσέγγιση καθορίζεται από το πόσο οι ελεγκτές έχουν πρόσβαση σε πληροφορίες σχετικά με το σύστημα και το περιβάλλον που ελέγχουν. Οι τρεις βασικές προσεγγίσεις είναι (Pradeep & Sakthivel, 2021):

- **Black Box Έλεγχος Διείσδυσης (Black Box Penetration Testing):** Σε αυτήν την προσέγγιση, οι ελεγκτές δεν έχουν προηγούμενη γνώση για το σύστημα που ελέγχουν. Προσομοιώνουν μια αληθινή επίθεση, αναλαμβάνοντας το ρόλο του εισβολέα χωρίς καμία πληροφόρηση εκ των προτέρων. Αυτό σημαίνει ότι πρέπει να ανακαλύψουν τις ευπάθειες χωρίς καμία βοήθεια.

- **White Box Έλεγχος Διείσδυσης (White Box Penetration Testing):** Σε αυτήν την προσέγγιση, οι ελεγκτές έχουν πλήρη πρόσβαση στις πληροφορίες σχετικά με το σύστημα που ελέγχουν. Αυτό συμπεριλαμβάνει τον πηγαίο κώδικα των εφαρμογών και άλλες λεπτομέρειες για το δίκτυο και το περιβάλλον του οργανισμού.

- **Gray Box Έλεγχος Διείσδυσης (Gray Box Penetration Testing):** Αυτή η προσέγγιση συνδυάζει τα χαρακτηριστικά των δύο προηγούμενων προσεγγίσεων. Οι ελεγκτές έχουν κάποιες πληροφορίες για το σύστημα, αλλά όχι την πλήρη γνώση που

έχουν στον White Box έλεγχο. Αυτό τους επιτρέπει να προσεγγίσουν το σύστημα με περισσότερη γνώση από ό,τι στο Black Box, αλλά χωρίς την πλήρη πρόσβαση που έχουν στον White Box έλεγχο.

3.1.3 Φάσεις του Ελέγχου Διείσδυσης

Ο Έλεγχος Διείσδυσης χωρίζεται σε διάφορα στάδια, τα οποία διαφέρουν ανάλογα με τη μέθοδολογία που χρησιμοποιείται (Pradeep & Sakthivel, 2021):

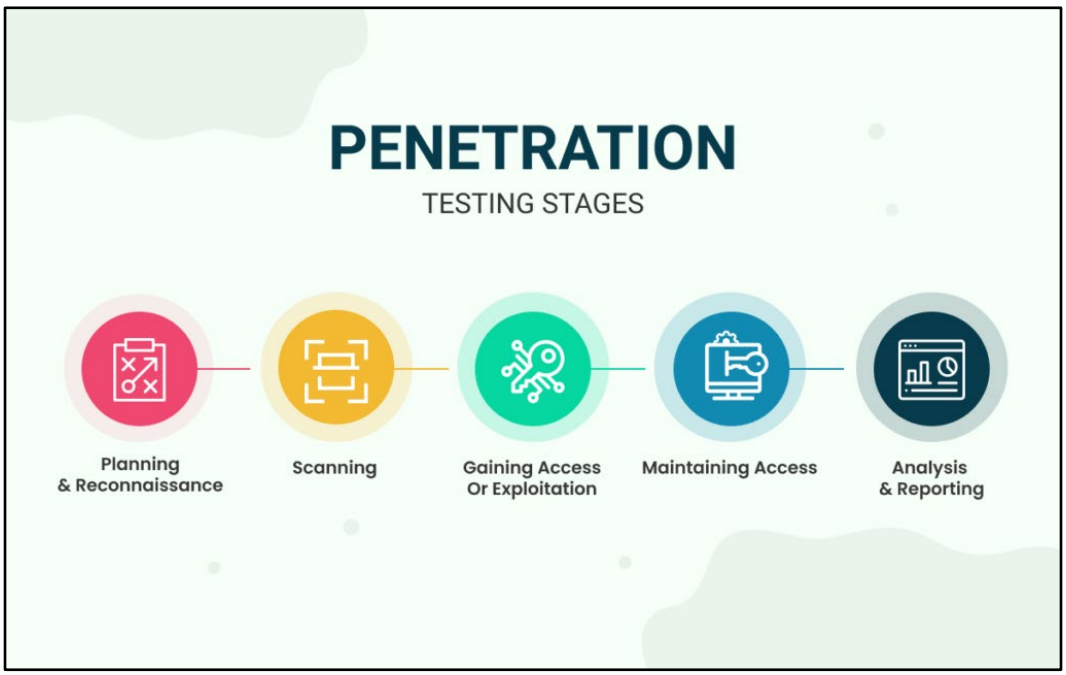
- **Σχεδιασμός και Αναγνώριση (Planning and Reconnaissance):** Η αναγνώριση αποτελεί το πρώτο βήμα σε έναν έλεγχο διείσδυσης, κατά τη διάρκεια του οποίου ο ελεγκτής συλλέγει όσο το δυνατόν περισσότερες πληροφορίες για τον στόχο. Αυτό περιλαμβάνει λογαριασμούς χρηστών, λειτουργικά συστήματα, εφαρμογές και την τοπολογία του δικτύου. Η αναγνώριση μπορεί να είναι είτε ενεργητική, με άμεση πρόσβαση στο σύστημα του στόχου, είτε παθητική, αποσπώντας πληροφορίες από ευρέως προσβάσιμες πηγές. Συνήθως, και οι δύο τεχνικές απαιτούνται για μία ολοκληρωμένη απεικόνιση των ευπαθειών του στόχου.

- **Σάρωση (Scanning):** Στη φάση της σάρωσης, ο ελεγκτής χρησιμοποιεί διάφορα εργαλεία για να εντοπίσει ανοιχτές πόρτες και να εξετάσει τη δραστηριότητα του δικτύου στα συστήματα του στόχου. Αυτό του επιτρέπει να προετοιμαστεί για την επόμενη φάση, καθώς οι ανοιχτές πόρτες αποτελούν πιθανά σημεία πρόσβασης για επιτιθέμενους. Η σάρωση μπορεί να εκτελείται είτε αυτόνομα, είτε ως μέρος του ελέγχου διείσδυσης. Παρόλο που η σάρωση μπορεί να αναγνωρίσει πιθανούς κινδύνους, χρειάζεται πάντα παρέμβαση από ελεγκτές διείσδυσης για την πλήρη λειτουργία της.

- **Απόκτηση Πρόσβασης (Gaining Access or Exploration):** Στη φάση αυτή, ο ελεγκτής εκτελεί επιθέσεις εφαρμογών ιστού όπως SQL Injection και Cross Site Scripting (XSS) για να εντοπίσει ευπάθειες στο στόχο. Στη συνέχεια, εκμεταλλεύεται αυτές τις ευπάθειες για να αναβαθμίσει δικαιώματα, να αποκτήσει δεδομένα και να υποκλέψει κίνηση.

- **Διατήρηση Πρόσβασης (Maintaining Access):** Στη φάση αυτή, ο ελεγκτής προσπαθεί να διατηρήσει την πρόσβαση στο σύστημα του στόχου και να εκμεταλλευτεί τις ευπάθειες που έχουν ανακαλυφθεί. Αυτό γίνεται προσομοιώνοντας πραγματικές επιθέσεις και αποφεύγοντας τα συστήματα προστασίας.

- **Ανάλυση (Analysis):** Ο ελεγκτής δημιουργεί μια αναφορά κατηγοριοποιώντας τα αποτελέσματα του ελέγχου διείσδυσης. Αυτή η αναφορά χρησιμοποιείται για να κλείσουν όλες οι τρύπες ασφαλείας στο σύστημα και να βελτιωθεί η ασφάλεια του οργανισμού. Περιέχει λεπτομερή ανάλυση των ευπαθειών και προτάσεις για βελτίωση της στρατηγικής ασφάλειας.



Εικόνα 2 - Φάσεις penetration testing

3.2. Penetration test in IoT

Η δοκιμή διείσδυσης σε περιβάλλοντα IoT (Internet of Things) παρουσιάζει μοναδικές προκλήσεις λόγω της κατανεμημένης φύσης των συστημάτων IoT, της ποικιλίας των συσκευών που εμπλέκονται και των πιθανών επιπτώσεων των παραβιάσεων της ασφάλειας. Ακολουθούν ορισμένες βασικές σκέψεις και προσεγγίσεις για τη διεξαγωγή δοκιμών διείσδυσης στο IoT (Johari et al., 2020):

- **Κατανόηση του οικοσυστήματος IoT:** Πριν από τη διεξαγωγή δοκιμών διείσδυσης, είναι σημαντικό να υπάρχει μια βαθιά κατανόηση του οικοσυστήματος IoT που δοκιμάζεται, συμπεριλαμβανομένων των τύπων συσκευών, πρωτοκόλλων επικοινωνίας, ροών δεδομένων και πιθανών τρωτών σημείων.

- **Εντοπισμός επιφανειών επίθεσης:** Απαιτείται προσδιορισμός τις επιφάνειες επίθεσης εντός του οικοσυστήματος IoT, συμπεριλαμβανομένων συσκευών, επικοινωνιών δικτύου, υπηρεσιών cloud, εφαρμογών για κινητά και διεπαφών Ιστού. Αυτό περιλαμβάνει τον εντοπισμό πιθανών σημείων εισόδου για εισβολείς.

- **Δοκιμή φυσικής πρόσβασης:** Σε περιβάλλοντα IoT, η φυσική πρόσβαση σε συσκευές μπορεί να αποτελεί σημαντικό πρόβλημα ασφάλειας. Οι ελεγκτές διείσδυσης μπορεί να χρειαστεί να αξιολογήσουν μέτρα φυσικής ασφάλειας και να ελέγξουν για τρωτά σημεία που θα μπορούσαν να εκμεταλλευτούν εάν ένας εισβολέας αποκτήσει φυσική πρόσβαση σε μια συσκευή.

- **Δοκιμή ασύρματης ασφάλειας:** Πολλές συσκευές IoT επικοινωνούν ασύρματα, καθιστώντας τις ευάλωτες σε επιθέσεις όπως η υποκλοπή, η πλαστογράφηση και η μη εξουσιοδοτημένη πρόσβαση. Οι ελεγκτές διείσδυσης θα πρέπει να αξιολογούν την ασφάλεια των πρωτοκόλλων ασύρματης επικοινωνίας και των μηχανισμών κρυπτογράφησης που χρησιμοποιούνται από συσκευές IoT.

- **Ανάλυση υλικολογισμικού:** Οι συσκευές IoT συχνά εκτελούν υλικολογισμικό που μπορεί να περιέχει ευπάθειες. Οι ελεγκτές διείσδυσης ενδέχεται να αναλύσουν images υλικολογισμικού για ελαττώματα ασφαλείας, όπως διαπιστευτήρια με σκληρό κώδικα, υπερχειλίσεις buffer ή μη ασφαλείς μηχανισμούς ενημέρωσης.

- **Δοκιμή ασφαλείας Cloud:** Οι λύσεις IoT συχνά αξιοποιούν υπηρεσίες cloud για αποθήκευση, επεξεργασία και διαχείριση δεδομένων. Οι ελεγκτές διείσδυσης θα πρέπει να αξιολογούν την ασφάλεια της υποδομής cloud, των Application Programming Interfaces API και των μηχανισμών ελέγχου ταυτότητας που χρησιμοποιούνται από εφαρμογές IoT.

- **Δοκιμή απορρήτου και ακεραιότητας δεδομένων:** Οι συσκευές IoT συλλέγουν και μεταδίδουν ευαίσθητα δεδομένα, καθιστώντας κρίσιμα ζητήματα για το απόρρητο και την ακεραιότητα των δεδομένων. Οι ελεγκτές διείσδυσης θα πρέπει να αξιολογούν

τον τρόπο με τον οποίο τα συστήματα IoT χειρίζονται δεδομένα χρήστη, συμπεριλαμβανομένης της κρυπτογράφησης, των ελέγχων πρόσβασης και των μέτρων πρόληψης διαρροής δεδομένων.

- **Δοκιμή άρνησης υπηρεσίας (Denial of Service - DoS):** Οι συσκευές IoT μπορεί να είναι ευάλωτες σε επιθέσεις άρνησης υπηρεσίας που διαταράσσουν την κανονική τους λειτουργία. Οι ελεγκτές διείσδυσης θα πρέπει να αξιολογούν την ανθεκτικότητα των συστημάτων IoT σε επιθέσεις DoS και να αξιολογούν τις στρατηγικές μετριασμού.

- **Συμμόρφωση και Πρότυπα:** Πρέπει να λαμβάνονται υπόψη οι απαιτήσεις συμμόρφωσης και τα βιομηχανικά πρότυπα που σχετίζονται με την ασφάλεια του IoT, όπως οι οδηγίες του IoT Security Foundation ή τα ρυθμιστικά πλαίσια όπως ο GDPR. Η δοκιμή διείσδυσης πρέπει να ευθυγραμμίζεται με αυτές τις απαιτήσεις.

- **Αναφορά και αποκατάσταση:** Μετά τη διεξαγωγή δοκιμών διείσδυσης, παρέχονται εκτενείς αναφορές που περιγράφουν λεπτομερώς τις ευπάθειες που εντοπίστηκαν, τη σοβαρότητά τους και συστάσεις για αποκατάσταση. Απαιτείται στενή συνεργασία με τα ενδιαφερόμενα μέρη για την ιεράρχηση και την αντιμετώπιση των εντοπισμένων ζητημάτων ασφάλειας.

Η δοκιμή διείσδυσης σε περιβάλλοντα IoT απαιτεί ενδελεχή κατανόηση του οικοσυστήματος IoT, αναγνώριση επιφανειών επίθεσης και δοκιμές σε διάφορα επίπεδα της στοίβας IoT, συμπεριλαμβανομένων συσκευών, δικτύων, υπηρεσιών cloud και εφαρμογών. Εφαρμόζοντας μια ολοκληρωμένη προσέγγιση, οι οργανισμοί μπορούν να εντοπίσουν και να αντιμετωπίσουν τις ευπάθειες ασφαλείας στις αναπτύξεις τους στο IoT (Johari et al., 2020).

3.3. Εργαλεία - Kali Linux

Το Kali Linux είναι μια διανομή Linux που βασίζεται στο Debian, ειδικά σχεδιασμένη για ψηφιακή εγκληματολογία και δοκιμές διείσδυσης. Έρχεται προεγκατεστημένο με πολλά εργαλεία δοκιμών διείσδυσης, καθιστώντας το μια δημοφιλή επιλογή μεταξύ των επαγγελματιών της κυβερνοασφάλειας, των ηθικών χάκερ και των ερευνητών ασφάλειας (Najera-Gutierrez & Ansari, 2018).

Ακολουθούν ορισμένα βασικά χαρακτηριστικά του Kali Linux:

- **Εργαλεία δοκιμής διείσδυσης:** Το Kali Linux περιλαμβάνει μια τεράστια γκάμα εργαλείων για διάφορα στάδια δοκιμής διείσδυσης, όπως συλλογή πληροφοριών, αξιολόγηση ευπάθειας, εκμετάλλευση, κλιμάκωση προνομίων και διατήρηση της πρόσβασης.

- **Ανοιχτού κώδικα:** Το Kali Linux είναι ένα έργο ανοιχτού κώδικα που διατηρείται και χρηματοδοτείται από την Offensive Security. Αυτό σημαίνει ότι ολόκληρο το λειτουργικό σύστημα και τα εργαλεία του είναι ελεύθερα διαθέσιμα για λήψη, διανομή και τροποποίηση.

- **Τακτικές ενημερώσεις:** Το Kali Linux ενημερώνεται τακτικά για να διασφαλιστεί ότι περιλαμβάνει τις πιο πρόσφατες εκδόσεις εργαλείων ασφαλείας και ενημερώσεις κώδικα για γνωστά τρωτά σημεία. Οι χρήστες μπορούν εύκολα να ενημερώσουν τα συστήματά τους χρησιμοποιώντας τα ενσωματωμένα εργαλεία διαχείρισης πακέτων.

- **Προσαρμογή:** Το Kali Linux επιτρέπει στους χρήστες να προσαρμόζουν τις εγκαταστάσεις τους εγκαθιστώντας πρόσθετα εργαλεία, τροποποιώντας διαμορφώσεις και δημιουργώντας προσαρμοσμένα σενάρια. Αυτή η ευελιξία το καθιστά κατάλληλο για διάφορα σενάρια δοκιμών ασφαλείας.

- **Δυνατότητα Live Boot:** Το Kali Linux μπορεί να εκκινηθεί απευθείας από μονάδα USB ή DVD χωρίς να το εγκαταστήσετε σε σύστημα. Αυτή η "ζωντανή" λειτουργία επιτρέπει στους χρήστες να χρησιμοποιούν το λειτουργικό σύστημα και τα εργαλεία του σε οποιοδήποτε συμβατό υλικό χωρίς να τροποποιούν το κεντρικό σύστημα.

- **Υποστήριξη για πολλαπλές πλατφόρμες:** Το Kali Linux υποστηρίζει ένα ευρύ φάσμα αρχιτεκτονικών υλικού, συμπεριλαμβανομένων συστημάτων x86 32-bit και 64-bit, συσκευών που βασίζονται σε ARM και πλατφορμών εικονικοποίησης όπως το VMware και το VirtualBox.

- **Τεκμηρίωση και υποστήριξη κοινότητας:** Το Kali Linux παρέχει εκτενή τεκμηρίωση, σεμινάρια και φόρουμ για να βοηθήσει τους χρήστες να ξεκινήσουν με τη δοκιμή διείσδυσης και την αντιμετώπιση προβλημάτων. Η ζωντανή κοινότητα

χρηστών και προγραμματιστών συμβάλλει στη συνεχή ανάπτυξη και βελτίωση της διανομής.

Συνολικά, το Kali Linux είναι μια ισχυρή και ευέλικτη πλατφόρμα για τη διεξαγωγή αξιολογήσεων ασφαλείας, δοκιμών ευπάθειας και ηθικών δραστηριοτήτων hacking. Το ολοκληρωμένο σύνολο εργαλείων, οι τακτικές ενημερώσεις και η ισχυρή υποστήριξη της κοινότητας το καθιστούν απαραίτητο πόρο για τους επαγγελματίες της κυβερνοασφάλειας παγκοσμίως (Najera-Gutierrez & Ansari, 2018).

Το Kali Linux είναι μια δημοφιλής διανομή δοκιμών διείσδυσης που παρέχεται προεγκατεστημένη με ένα ευρύ φάσμα εργαλείων για τη διεξαγωγή αξιολογήσεων ασφαλείας και δοκιμών διείσδυσης. Μερικά από τα αξιοσημείωτα εργαλεία που είναι διαθέσιμα στο Kali Linux είναι τα εξής (Asaad, 2021):

- **Nmap:** Ένας ισχυρός σαρωτής δικτύου που χρησιμοποιείται για την ανακάλυψη συσκευών/τοπολογίας δικτύου και τον έλεγχο ασφάλειας. Το Nmap μπορεί να χρησιμοποιηθεί για τον εντοπισμό ανοιχτών θυρών, τον εντοπισμό λειτουργικών συστημάτων και την εκτέλεση σάρωσης ευπάθειας.

- **Metasploit Framework:** Ένα ολοκληρωμένο εργαλείο για την ανάπτυξη και την εκτέλεση κώδικα εκμετάλλευσης έναντι απομακρυσμένων στόχων. Το Metasploit περιλαμβάνει μια μεγάλη βάση δεδομένων με εκμεταλλεύσεις, ωφέλιμα φορτία και βοηθητικές μονάδες για δοκιμές διείσδυσης.

- **Wireshark:** Αναλυτής πρωτοκόλλου δικτύου που επιτρέπει στους χρήστες να καταγράφουν και να επιθεωρούν την κυκλοφορία του δικτύου σε πραγματικό χρόνο. Το Wireshark είναι χρήσιμο για την ανάλυση της συμπεριφοράς του δικτύου και τον εντοπισμό τρωτών σημείων ασφαλείας.

- **Aircrack-ng:** Μια σουίτα εργαλείων για έλεγχο ασύρματων δικτύων. Το Aircrack-ng μπορεί να χρησιμοποιηθεί για την εκτέλεση καταγραφής πακέτων, την παρακολούθηση της κυκλοφορίας δικτύου και τη διάρρηξη των κλειδιών κρυπτογράφησης WEP και WPA/WPA2.

- **John the Ripper:** Ένα εργαλείο διάρρηξης κωδικού πρόσβασης που χρησιμοποιείται για τον εντοπισμό αδύναμων κωδικών πρόσβασης εκτελώντας επιθέσεις λεξικών, επιθέσεις brute force και άλλες τεχνικές διάρρηξης κωδικών πρόσβασης.

- **Burp Suite:** Μια πλατφόρμα δοκιμών ασφάλειας διαδικτυακών εφαρμογών που χρησιμοποιείται για τη διενέργεια χειροκίνητων και αυτοματοποιημένων δοκιμών ασφαλείας εφαρμογών ιστού. Το Burp Suite περιλαμβάνει εργαλεία για σάρωση, ανίχνευση και εκμετάλλευση ευπαθειών ιστού.

- **Hydra:** Ένα γρήγορο και ευέλικτο εργαλείο διάρρηξης κωδικού πρόσβασης που υποστηρίζει διάφορα πρωτόκολλα και υπηρεσίες, συμπεριλαμβανομένων των HTTP, FTP, SSH και άλλων.

- **SQLMap:** Ένα αυτοματοποιημένο εργαλείο για τον εντοπισμό και την εκμετάλλευση ευπαθειών SQL injection σε εφαρμογές web. Το SQLMap μπορεί να χρησιμοποιηθεί για τον εντοπισμό τρωτών σημείων της βάσης δεδομένων και την εξαγωγή ευαίσθητων πληροφοριών από βάσεις δεδομένων.

- **OpenVAS:** Ένας σαρωτής ευπάθειας ανοιχτού κώδικα που εκτελεί ολοκληρωμένες αξιολογήσεις ευπάθειας συστημάτων και δικτύων. Το OpenVAS μπορεί να εντοπίσει ένα ευρύ φάσμα ζητημάτων ασφαλείας, συμπεριλαμβανομένων εσφαλμένων διαμορφώσεων, απαρχαιωμένου λογισμικού και γνωστών τρωτών σημείων.

- **Hashcat:** Ένα εργαλείο ανάκτησης κωδικού πρόσβασης που υποστηρίζει διάφορους αλγόριθμους και τρόπους επίθεσης για το σπάσιμο κατακερματισμένων κωδικών πρόσβασης.

Αυτά είναι μερικά μόνο παραδείγματα από τα πολλά εργαλεία που είναι διαθέσιμα στο Kali Linux για τη διεξαγωγή δοκιμών διείσδυσης και αξιολογήσεων ασφάλειας. Ανάλογα με τις ειδικές απαιτήσεις της αξιολόγησης, οι ελεγκτές διείσδυσης μπορούν να χρησιμοποιήσουν έναν συνδυασμό αυτών των εργαλείων για τον εντοπισμό και την εκμετάλλευση των τρωτών σημείων ασφαλείας σε συστήματα και δίκτυα-στόχους (Asaad, 2021).

3.4. Επιθέσεις

Τα τεστ διείσδυσης συχνά αντιμετωπίζουν διάφορους τύπους επιθέσεων στον κυβερνοχώρο, με το καθένα να έχει ως στόχο την εκμετάλλευση αδυναμιών σε συστήματα ή δίκτυα. Ακολουθούν ορισμένοι συνήθεις τύποι (Denis, Zena & Hayajneh, 2016):

- **SQL Injection (SQLi):** Οι εισβολείς εισάγουν κακόβουλα ερωτήματα SQL σε πεδία εισόδου για να χειριστούν βάσεις δεδομένων, να εξαγάγουν ευαίσθητες πληροφορίες ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση.

- **Σενάρια μεταξύ ιστότοπων (XSS):** Οι εισβολείς εισάγουν κακόβουλα σενάρια σε ιστοσελίδες που προβάλλονται από άλλους χρήστες, οδηγώντας ενδεχομένως σε παραβίαση συνεδρίας, κλοπή cookie ή παραμόρφωση ιστότοπου.

- **Denial-of-Service (DoS) και Distributed Denial-of-Service (DDoS):** Οι εισβολείς πλημμυρίζουν συστήματα ή δίκτυα-στόχους με υπερβολική κίνηση, με αποτέλεσμα να μην είναι διαθέσιμα σε νόμιμους χρήστες.

- **Man-in-the-Middle (MitM):** Οι επιτιθέμενοι παρεμποδίζουν και πιθανώς αλλάζουν τις επικοινωνίες μεταξύ δύο μερών, δίνοντάς τους τη δυνατότητα να κρυφακούουν ευαίσθητες πληροφορίες ή να χειραγωγούν δεδομένα.

- **Ηλεκτρονικό Ψάρεμα (phishing):** Οι εισβολείς υποδύονται νόμιμες οντότητες για να εξαπατήσουν τους χρήστες να αποκαλύψουν εμπιστευτικές πληροφορίες, όπως διαπιστευτήρια σύνδεσης ή οικονομικές λεπτομέρειες.

- **Επιθέσεις brute force:** Οι εισβολείς προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή λογαριασμούς δοκιμάζοντας συστηματικά όλους τους πιθανούς κωδικούς πρόσβασης ή τα κλειδιά κρυπτογράφησης.

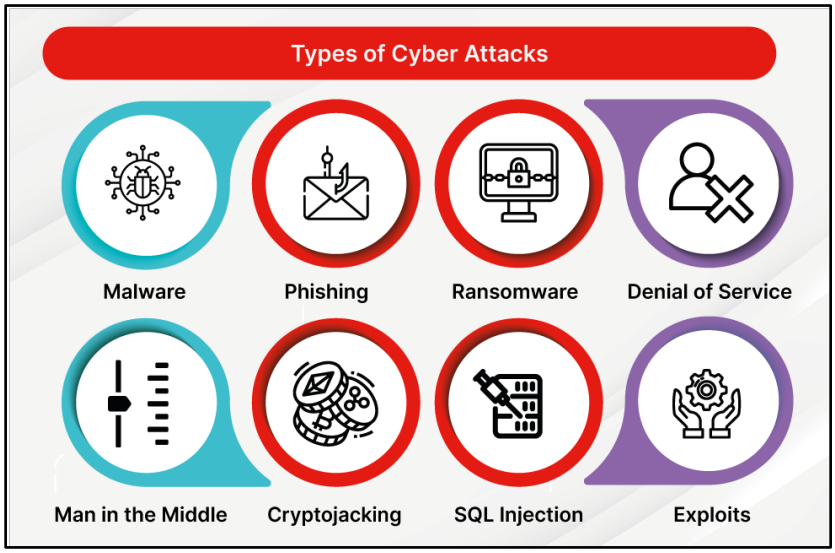
- **Υπερχείλιση buffer:** Οι εισβολείς εκμεταλλεύονται τρωτά σημεία στο λογισμικό για να υπερχειλίσουν buffer με υπερβολικά δεδομένα, επιτρέποντάς τους ενδεχομένως να εκτελέσουν αυθαίρετο κώδικα ή να καταρρεύσει το σύστημα.

- **Κλιμάκωση προνομίων:** Οι εισβολείς εκμεταλλεύονται ευπάθειες για να αυξήσουν τα προνόμιά τους σε ένα σύστημα ή δίκτυο, αποκτώντας πρόσβαση σε περιορισμένους πόρους ή εκτελώντας μη εξουσιοδοτημένες εντολές.

- **Κακόβουλο λογισμικό:** Οι εισβολείς αναπτύσσουν κακόβουλο λογισμικό για να παραβιάσουν συστήματα, να κλέψουν δεδομένα ή να διακόψουν τις λειτουργίες. Αυτό περιλαμβάνει ιούς, σκουλήκια (worms), Trojans, ransomware και spyware.

- **Εσωτερικές απειλές:** Επιτιθέμενοι με νόμιμη πρόσβαση κάνουν κατάχρηση των προνομίων τους για να κλέψουν δεδομένα, να υπονομεύσουν συστήματα ή να διευκολύνουν εξωτερικές επιθέσεις.

Αυτές οι επιθέσεις προσομοιώνονται κατά τη διάρκεια δοκιμών διείσδυσης για τον εντοπισμό τρωτών σημείων και την αξιολόγηση της αποτελεσματικότητας των ελέγχων ασφαλείας, βοηθώντας τους οργανισμούς να βελτιώσουν τη συνολική στάση ασφαλείας τους (Denis, Zena & Hayajneh, 2016).



Εικόνα 3 - Τύποι κυβερνηεπιθέσεων.

4 Intrusion Detection Prevention Systems

Η ανίχνευση εισβολής είναι η διαδικασία παρακολούθησης των γεγονότων που συμβαίνουν σε ένα σύστημα ή δίκτυο υπολογιστών και η ανάλυσή τους για ενδείξεις πιθανών συμβάντων, τα οποία είναι παραβιάσεις ή επικείμενες απειλές παραβίασης πολιτικών ασφάλειας υπολογιστών, αποδεκτών πολιτικών χρήσης ή τυπικών πρακτικών ασφαλείας. Ένα σύστημα ανίχνευσης εισβολής (IDS) είναι λογισμικό που αυτοματοποιεί τη διαδικασία ανίχνευσης εισβολής. Ένα σύστημα πρόληψης εισβολής (IPS) είναι λογισμικό που έχει όλες τις δυνατότητες ενός συστήματος ανίχνευσης εισβολής και μπορεί επίσης να προσπαθήσει να σταματήσει πιθανά περιστατικά. Οι τεχνολογίες IDS και IPS προσφέρουν πολλές από τις ίδιες δυνατότητες και οι διαχειριστές μπορούν συνήθως να απενεργοποιήσουν τις λειτουργίες πρόληψης σε προϊόντα IPS, με αποτέλεσμα να λειτουργούν ως IDS. Συνεπώς, για συντομία, ο όρος συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS) χρησιμοποιείται σε όλο το υπόλοιπο αυτού του κεφαλαίου για να αναφέρεται τόσο στις τεχνολογίες IDS όσο και στις τεχνολογίες IPS (Kenkre, Pai & Colaco, 2015).

Οι IDPS επικεντρώνονται κυρίως στον εντοπισμό πιθανών περιστατικών. Για παράδειγμα, ένα IDPS θα μπορούσε να εντοπίσει πότε ένας εισβολέας έχει παραβιάσει με επιτυχία ένα σύστημα εκμεταλλευόμενος μια ευπάθεια στο σύστημα. Το IDPS θα καταγράφει πληροφορίες για τη δραστηριότητα και θα αναφέρει το περιστατικό στους διαχειριστές ασφαλείας, ώστε να μπορούν να ξεκινήσουν ενέργειες αντιμετώπισης περιστατικών για την ελαχιστοποίηση της ζημιάς. Πολλά IDPS μπορούν επίσης να ρυθμιστούν ώστε να αναγνωρίζουν παραβιάσεις αποδεκτών πολιτικών χρήσης και άλλων πολιτικών ασφάλειας—παραδείγματα περιλαμβάνουν τη χρήση απαγορευμένων εφαρμογών κοινής χρήσης αρχείων peer-to-peer και τη μεταφορά μεγάλων αρχείων βάσης δεδομένων σε αφαιρούμενα μέσα ή φορητές συσκευές. Επιπλέον, πολλοί IDPS μπορούν να προσδιορίσουν αναγνωριστική δραστηριότητα, η οποία μπορεί να υποδεικνύει ότι μια επίθεση είναι επικείμενη ή ότι ένα συγκεκριμένο σύστημα ή χαρακτηριστικό συστήματος ενδιαφέρει ιδιαίτερα τους επιτιθέμενους. Μια άλλη χρήση των IDPS είναι η καλύτερη κατανόηση των απειλών που εντοπίζουν, ιδιαίτερα της συχνότητας και των χαρακτηριστικών των επιθέσεων, ώστε να μπορούν να εντοπιστούν τα κατάλληλα μέτρα ασφαλείας. Ορισμένοι IDPS μπορούν επίσης να αλλάξουν το προφίλ ασφαλείας τους όταν εντοπίζεται μια νέα απειλή. Για παράδειγμα, ένα IDPS μπορεί να συλλέξει πιο λεπτομερείς πληροφορίες για μια συγκεκριμένη συνεδρία

μετά τον εντοπισμό κακόβουλης δραστηριότητας σε αυτήν τη συνεδρία (Kenkre, Pai & Colaco, 2015).

Οι τεχνολογίες IPS διαφέρουν από τις τεχνολογίες IDS κατά ένα χαρακτηριστικό (Quincozes et al., 2021):

- Οι τεχνολογίες IPS μπορούν να ανταποκριθούν σε μια απειλή που έχει εντοπιστεί προσπαθώντας να την αποτρέψουν από το να πετύχει. Χρησιμοποιούν διάφορες τεχνικές απόκρισης, οι οποίες μπορούν να χωριστούν στις ακόλουθες ομάδες:
    - Το IPS σταματά την ίδια την επίθεση. Παραδείγματα για το πώς θα μπορούσε να γίνει αυτό περιλαμβάνουν το IPS που τερματίζει τη σύνδεση δικτύου που χρησιμοποιείται για την επίθεση και το IPS που αποκλείει την πρόσβαση στον στόχο από τον παραβατικό λογαριασμό χρήστη, τη διεύθυνση IP ή άλλο χαρακτηριστικό του εισβολέα.
    - Το IPS αλλάζει το περιβάλλον ασφαλείας. Το IPS θα μπορούσε να αλλάξει τη διαμόρφωση άλλων στοιχείων ελέγχου ασφαλείας για να διακόψει μια επίθεση. Συνήθη παραδείγματα είναι το IPS που αναδιαρθρώνει ένα τείχος προστασίας δικτύου για να εμποδίζει την πρόσβαση από τον εισβολέα ή τον στόχο και το IPS που τροποποιεί ένα τείχος προστασίας που βασίζεται σε κεντρικό υπολογιστή σε έναν στόχο για να εμποδίζει τις εισερχόμενες επιθέσεις. Ορισμένα IPS μπορούν ακόμη και να προκαλέσουν την εφαρμογή ενημερώσεων κώδικα σε έναν κεντρικό υπολογιστή, εάν το IPS εντοπίσει ότι ο κεντρικός υπολογιστής έχει ευπάθειες.
    - Το IPS αλλάζει το περιεχόμενο της επίθεσης. Ορισμένες τεχνολογίες IPS μπορούν να αφαιρέσουν ή να αντικαταστήσουν κακόβουλα τμήματα μιας επίθεσης για να την καταστήσουν καλοήθη. Ένα απλό παράδειγμα είναι ένα IPS που αφαιρεί ένα μολυσμένο συνημμένο αρχείο από ένα email και στη συνέχεια επιτρέπει στο καθαρισμένο email να φτάσει στον παραλήπτη του. Ένα πιο περίπλοκο παράδειγμα είναι ένα IPS που λειτουργεί ως διακομιστής μεσολάβησης και κανονικοποιεί τα εισερχόμενα αιτήματα, πράγμα που σημαίνει ότι ο διακομιστής μεσολάβησης συσκευάζει εκ νέου τα ωφέλιμα φορτία των αιτημάτων, απορρίπτοντας τις πληροφορίες κεφαλίδας. Αυτό μπορεί να προκαλέσει την απόρριψη ορισμένων επιθέσεων ως μέρος της διαδικασίας κανονικοποίησης.

Ορισμένοι αισθητήρες IPS διαθέτουν λειτουργία εκμάθησης ή προσομοίωσης που καταστέλλει όλες τις ενέργειες πρόληψης και αντ' αυτού υποδεικνύει πότε θα είχε πραγματοποιηθεί μια ενέργεια πρόληψης. Αυτό επιτρέπει στους διαχειριστές να παρακολουθούν και να ρυθμίζουν με ακρίβεια τη διαμόρφωση των δυνατοτήτων πρόληψης πριν ενεργοποιήσουν τις ενέργειες πρόληψης, γεγονός που μειώνει τον κίνδυνο ακούσιου αποκλεισμού της καλοήθους δραστηριότητας (Quincozes et al., 2021).

Ένα κοινό χαρακτηριστικό όλων των τεχνολογιών IDPS είναι ότι δεν μπορούν να παρέχουν απόλυτα ακριβή εντοπισμό. Ο εσφαλμένος προσδιορισμός της καλοήθους δραστηριότητας ως κακόβουλης είναι γνωστός ως ψευδώς θετικός. η αντίθετη περίπτωση, η αποτυχία εντοπισμού κακόβουλης δραστηριότητας, είναι ψευδώς αρνητική. Δεν είναι δυνατό να εξαλειφθούν όλα τα ψευδώς θετικά και αρνητικά. Στις περισσότερες περιπτώσεις, η μείωση των εμφανίσεων του ενός αυξάνει τα περιστατικά του άλλου. Πολλοί οργανισμοί επιλέγουν να μειώσουν τα ψευδώς αρνητικά με το κόστος της αύξησης των ψευδώς θετικών, πράγμα που σημαίνει ότι εντοπίζονται περισσότερα κακόβουλα συμβάντα, αλλά χρειάζονται περισσότεροι πόροι ανάλυσης για να διαφοροποιηθούν τα ψευδώς θετικά από τα αληθινά κακόβουλα συμβάντα. Η αλλαγή της διαμόρφωσης ενός IDPS για τη βελτίωση της ακρίβειας ανίχνευσης είναι γνωστή ως συντονισμός.

Οι περισσότερες τεχνολογίες IDPS αντισταθμίζουν επίσης τη χρήση κοινών τεχνικών αποφυγής. Το Evasion είναι η τροποποίηση της μορφής ή του χρονισμού της κακόβουλης δραστηριότητας έτσι ώστε η εμφάνισή της να αλλάζει αλλά η επίδρασή της να είναι η ίδια. Οι επιτιθέμενοι χρησιμοποιούν τεχνικές αποφυγής για να προσπαθήσουν να αποτρέψουν τις τεχνολογίες IDPS από τον εντοπισμό επιθέσεων. Για παράδειγμα, ένας εισβολέας θα μπορούσε να κωδικοποιήσει χαρακτήρες κειμένου με συγκεκριμένο τρόπο που θα κατανοήσει ο στόχος, ελπίζοντας ότι οι IDPS που παρακολουθούν τη δραστηριότητα δεν θα το κάνουν. Οι περισσότερες τεχνολογίες IDPS μπορούν να ξεπεράσουν τις τεχνικές αποφυγής αντιγράφοντας την ειδική επεξεργασία που εκτελείται από τους στόχους (Quincozes et al., 2021).

4.1. Signature-based Detection

Η υπογραφή είναι ένα μοτίβο που αντιστοιχεί σε μια γνωστή επίθεση ή τύπο επίθεσης. Η ανίχνευση βάσει υπογραφών είναι η διαδικασία σύγκρισης υπογραφών με παρατηρούμενα συμβάντα για τον εντοπισμό πιθανών επιθέσεων. Παραδείγματα ανίχνευσης μέσω υπογραφών είναι (Kwon et al., 2022):

- Μια απόπειρα telnet με όνομα χρήστη "root", η οποία αποτελεί παραβίαση της πολιτικής ασφαλείας ενός οργανισμού.

- Ένα email με θέμα "Δωρεάν φωτογραφίες!" και ένα όνομα αρχείου συνημμένου "freepics.exe", τα οποία είναι χαρακτηριστικά μιας γνωστής μορφής κακόβουλου λογισμικού.

- Μια καταχώρηση αρχείου καταγραφής λειτουργικού συστήματος με τιμή κωδικού κατάστασης 645, η οποία υποδεικνύει ότι ο έλεγχος του κεντρικού υπολογιστή έχει απενεργοποιηθεί.

Η ανίχνευση βάσει υπογραφών είναι πολύ αποτελεσματική στον εντοπισμό γνωστών επιθέσεων, αλλά σε μεγάλο βαθμό αναποτελεσματική στην ανίχνευση προηγουμένως άγνωστων επιθέσεων, επιθέσεων που συγκαλύπτονται από τη χρήση τεχνικών αποφυγής και πολλών παραλλαγών γνωστών επιθέσεων. Για παράδειγμα, εάν ένας εισβολέας τροποποίησε το κακόβουλο λογισμικό στο προηγούμενο παράδειγμα για να χρησιμοποιήσει ένα όνομα αρχείου "freepics2.exe", μια υπογραφή που αναζητά "freepics.exe" δεν θα ταιριάζει με αυτό (Kwon et al., 2022).

Η ανίχνευση βάσει υπογραφών είναι η απλούστερη μέθοδος ανίχνευσης, επειδή απλώς συγκρίνει την τρέχουσα μονάδα δραστηριότητας, όπως ένα πακέτο ή μια καταχώρηση αρχείου καταγραφής, με μια λίστα υπογραφών χρησιμοποιώντας λειτουργίες σύγκρισης συμβολοσειρών. Οι τεχνολογίες ανίχνευσης που βασίζονται αποκλειστικά σε υπογραφές έχουν ελάχιστη κατανόηση πολλών πρωτοκόλλων δικτύου ή εφαρμογών και δεν μπορούν να παρακολουθήσουν και να κατανοήσουν την κατάσταση των επικοινωνιών - για παράδειγμα, δεν μπορούν να αντιστοιχίσουν ένα αίτημα με την αντίστοιχη απόκριση, ούτε μπορούν να θυμηθούν προηγούμενα αιτήματα κατά την επεξεργασία του τρέχοντος αιτήματος. Αυτό εμποδίζει τις μεθόδους που βασίζονται σε υπογραφές από τον εντοπισμό επιθέσεων που

περιλαμβάνουν πολλαπλά συμβάντα εάν κανένα μεμονωμένο συμβάν δεν περιέχει σαφή ένδειξη επίθεσης (Kwon et al., 2022).

4.2. Anomaly-based Detection

Η ανίχνευση με βάση την ανωμαλία είναι η διαδικασία σύγκρισης των ορισμών για το ποια δραστηριότητα θεωρείται φυσιολογική έναντι των παρατηρούμενων γεγονότων για τον εντοπισμό σημαντικών αποκλίσεων. Ένα IDPS που χρησιμοποιεί ανίχνευση βάσει ανωμαλιών έχει προφίλ που αντιπροσωπεύουν την κανονική συμπεριφορά τέτοιων πραγμάτων όπως χρήστες, κεντρικοί υπολογιστές, συνδέσεις δικτύου ή εφαρμογές. Τα προφίλ αναπτύσσονται παρακολουθώντας τα χαρακτηριστικά της τυπικής δραστηριότητας σε μια χρονική περίοδο. Για παράδειγμα, ένα προφίλ για ένα δίκτυο μπορεί να δείχνει ότι η δραστηριότητα Ιστού περιλαμβάνει κατά μέσο όρο το 13% του εύρους ζώνης δικτύου κατά τις τυπικές ώρες εργασίας. Στη συνέχεια, το IDPS χρησιμοποιεί στατιστικές μεθόδους για να συγκρίνει τα χαρακτηριστικά της τρέχουσας δραστηριότητας με τα κατώφλια που σχετίζονται με το προφίλ, όπως η ανίχνευση πότε η δραστηριότητα Ιστού περιλαμβάνει σημαντικά μεγαλύτερο εύρος ζώνης από το αναμενόμενο και η ειδοποίηση ενός διαχειριστή για την ανωμαλία. Τα προφίλ μπορούν να αναπτυχθούν για πολλά χαρακτηριστικά συμπεριφοράς, όπως ο αριθμός των email που αποστέλλονται από έναν χρήστη, ο αριθμός των αποτυχημένων προσπαθειών σύνδεσης για έναν κεντρικό υπολογιστή και το επίπεδο χρήσης του επεξεργαστή για έναν κεντρικό υπολογιστή σε μια δεδομένη χρονική περίοδο (Yang et al., 2022).

Το κύριο πλεονέκτημα των μεθόδων ανίχνευσης που βασίζονται σε ανωμαλίες είναι ότι μπορούν να είναι πολύ αποτελεσματικές στον εντοπισμό προηγουμένως άγνωστων επιθέσεων. Για παράδειγμα, ας υποθέσουμε ότι ένας υπολογιστής μολυνθεί από έναν νέο τύπο κακόβουλου λογισμικού. Το κακόβουλο λογισμικό θα μπορούσε να καταναλώσει τους πόρους επεξεργασίας του υπολογιστή, να στείλει πολλά email, να ξεκινήσει μεγάλους αριθμούς συνδέσεων δικτύου και να εκτελέσει άλλη συμπεριφορά που θα ήταν σημαντικά διαφορετική από τα καθιερωμένα προφίλ για τον υπολογιστή.

Ένα αρχικό προφίλ δημιουργείται σε μια χρονική περίοδο που μερικές φορές ονομάζεται περίοδος εκπαίδευσης. Τα προφίλ μπορεί να είναι είτε στατικά είτε δυναμικά. Μόλις

δημιουργηθεί, ένα στατικό προφίλ παραμένει αμετάβλητο, εκτός εάν το IDPS χρησιμοποιείται ειδικά για τη δημιουργία ενός νέου προφίλ. Ένα δυναμικό προφίλ προσαρμόζεται συνεχώς καθώς παρατηρούνται πρόσθετα συμβάντα. Επειδή τα συστήματα και τα δίκτυα αλλάζουν με την πάροδο του χρόνου, αλλάζουν και τα αντίστοιχα μέτρα κανονικής συμπεριφοράς. Ένα στατικό προφίλ θα γίνει τελικά ανακριβές, επομένως πρέπει να ανανεώνεται περιοδικά. Τα δυναμικά προφίλ δεν έχουν αυτό το πρόβλημα, αλλά είναι επιρρεπή σε απόπειρες υπεκφυγής από επιτιθέμενους. Για παράδειγμα, ένας εισβολέας μπορεί να εκτελεί μικρές ποσότητες κακόβουλης δραστηριότητας περιστασιακά και στη συνέχεια να αυξάνει σταδιακά τη συχνότητα και την ποσότητα της δραστηριότητας. Εάν ο ρυθμός αλλαγής είναι αρκετά αργός, το IDPS μπορεί να θεωρήσει ότι η κακόβουλη δραστηριότητα είναι φυσιολογική συμπεριφορά και να την συμπεριλάβει στο προφίλ του (Yang et al., 2022).

Ένα άλλο πρόβλημα με τη δημιουργία προφίλ είναι ότι μπορεί να είναι πολύ δύσκολο σε ορισμένες περιπτώσεις να γίνουν ακριβή, επειδή η υπολογιστική δραστηριότητα είναι εξαιρετικά περίπλοκη. Για παράδειγμα, εάν μια συγκεκριμένη δραστηριότητα συντήρησης που εκτελεί μεγάλες μεταφορές αρχείων πραγματοποιείται μόνο μία φορά το μήνα, ενδέχεται να μην παρατηρηθεί κατά τη διάρκεια της περιόδου εκπαίδευσης. Όταν γίνει η συντήρηση, είναι πιθανό να θεωρηθεί σημαντική απόκλιση από το προφίλ. Τα προϊόντα IDPS που βασίζονται σε ανωμαλίες συχνά παράγουν πολλά ψευδώς θετικά αποτελέσματα λόγω της καλοήθους δραστηριότητας που αποκλίνει σημαντικά από τα προφίλ, ειδικά σε πιο διαφορετικά ή δυναμικά περιβάλλοντα. Ένα άλλο αξιοσημείωτο πρόβλημα με τη χρήση τεχνικών ανίχνευσης που βασίζονται σε ανωμαλίες είναι ότι είναι συχνά δύσκολο για τους αναλυτές να προσδιορίσουν τι πυροδότησε μια συγκεκριμένη ειδοποίηση (Yang et al., 2022).

4.3. Rule-based Platforms: Snort

Οι πλατφόρμες που βασίζονται σε κανόνες είναι συστήματα ή λογισμικό που λειτουργούν εφαρμόζοντας προκαθορισμένους κανόνες ή συνθήκες σε εισερχόμενα δεδομένα ή συμβάντα προκειμένου να λάβουν αποφάσεις ή να αναλάβουν ενέργειες. Αυτές οι πλατφόρμες χρησιμοποιούνται ευρέως σε διάφορους τομείς, συμπεριλαμβανομένης της κυβερνοασφάλειας, του αυτοματισμού και της επεξεργασίας δεδομένων. Στην κυβερνοασφάλεια, οι πλατφόρμες που βασίζονται σε κανόνες χρησιμοποιούνται συχνά για

τον εντοπισμό και την πρόληψη εισβολών, την ανάλυση της κυκλοφορίας δικτύου και την επιβολή της πολιτικής ασφαλείας (Fallahi, Sami & Tajbakhsh, 2016).

Οι πλατφόρμες που βασίζονται σε κανόνες χρησιμοποιούνται επίσης σε διάφορους κλάδους για την αυτοματοποίηση διαδικασιών και τη λήψη αποφάσεων. Για παράδειγμα, στην κατασκευή, συστήματα που βασίζονται σε κανόνες μπορούν να χρησιμοποιηθούν για την παρακολούθηση των διαδικασιών παραγωγής και την ενεργοποίηση ειδοποιήσεων ή διορθωτικών ενεργειών εάν εντοπιστούν αποκλίσεις από προκαθορισμένα πρότυπα ποιότητας. Στα χρηματοοικονομικά, οι πλατφόρμες που βασίζονται σε κανόνες μπορούν να χρησιμοποιηθούν για αλγοριθμικές συναλλαγές, διαχείριση κινδύνου και ανίχνευση απάτης, όπου εφαρμόζονται προκαθορισμένοι κανόνες σε οικονομικά δεδομένα για τον εντοπισμό ευκαιριών συναλλαγών ή την επισήμανση ύποπτων συναλλαγών.

Οι πλατφόρμες που βασίζονται σε κανόνες παρέχουν ένα ευέλικτο και αποτελεσματικό μέσο για την αυτοματοποίηση της λήψης αποφάσεων και την επιβολή πολιτικών σε ένα ευρύ φάσμα εφαρμογών και βιομηχανιών. Αξιοποιώντας προκαθορισμένους κανόνες και συνθήκες, αυτές οι πλατφόρμες επιτρέπουν στους οργανισμούς να εξορθολογίσουν τις λειτουργίες, να βελτιώσουν την αποτελεσματικότητα και να βελτιώσουν τη στάση ασφαλείας (Fallahi, Sami & Tajbakhsh, 2016).

Το Snort είναι μια πλατφόρμα βασισμένη σε κανόνες που χρησιμοποιείται για συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS). Λειτουργεί αναλύοντας την κίνηση του δικτύου σε πραγματικό χρόνο και εντοπίζοντας ύποπτη ή κακόβουλη δραστηριότητα βάσει προκαθορισμένων κανόνων. Αυτοί οι κανόνες, που συχνά αναφέρονται ως υπογραφές, δημιουργούνται από ειδικούς σε θέματα ασφάλειας και ερευνητές για τον εντοπισμό συγκεκριμένων μοτίβων ή συμπεριφορών που σχετίζονται με γνωστές απειλές ή τεχνικές επιθέσεων (Tasneem, Kumar & Sharma, 2018).

- **Επιθεώρηση πακέτων:** Το Snort παρακολουθεί την κυκλοφορία του δικτύου καταγράφοντας και αναλύοντας πακέτα καθώς περνούν μέσα από μια διεπαφή δικτύου. Εξετάζει τις κεφαλίδες πακέτων και τα ωφέλιμα φορτία για να εξάγει σχετικές πληροφορίες για ανάλυση.

- **Αντιστοιχία κανόνων:** Το Snort συγκρίνει τα περιεχόμενα κάθε πακέτου με τη βάση δεδομένων κανόνων του. Αυτοί οι κανόνες ορίζουν διάφορα χαρακτηριστικά της

κίνησης δικτύου που μπορεί να υποδηλώνουν κακόβουλη δραστηριότητα, όπως συγκεκριμένα μοτίβα, υπογραφές ή ανωμαλίες συμπεριφοράς.

- **Δημιουργία ειδοποιήσεων:** Όταν το Snort προσδιορίζει ένα πακέτο που ταιριάζει με έναν από τους κανόνες του, δημιουργεί μια ειδοποίηση ή καταχώρηση αρχείου καταγραφής για να ειδοποιεί τους διαχειριστές για πιθανά συμβάντα ασφαλείας. Αυτές οι ειδοποιήσεις συνήθως περιλαμβάνουν λεπτομέρειες σχετικά με την απειλή που εντοπίστηκε, όπως τον τύπο της επίθεσης, τις διευθύνσεις IP προέλευσης και προορισμού και τη χρονική σήμανση.

- **Ενέργειες απόκρισης:** Ανάλογα με τη διαμόρφωση, το Snort μπορεί να πραγματοποιήσει προκαθορισμένες ενέργειες απόκρισης όταν εντοπίζονται συγκεκριμένοι τύποι απειλών. Αυτές οι ενέργειες μπορεί να περιλαμβάνουν αποκλεισμό ή απόρριψη πακέτων που σχετίζονται με την απειλή που εντοπίστηκε, καταγραφή πρόσθετων πληροφοριών για εγκληματολογική ανάλυση ή ενεργοποίηση αυτοματοποιημένης απόκρισης από άλλα συστήματα ασφαλείας.

- **Προσαρμογή και συντονισμός:** Το Snort επιτρέπει στους διαχειριστές να προσαρμόζουν και να συντονίζουν τα σύνολα κανόνων του για να ανταποκρίνονται στις συγκεκριμένες απαιτήσεις ασφαλείας του περιβάλλοντός τους. Αυτό περιλαμβάνει την ενεργοποίηση ή απενεργοποίηση συγκεκριμένων κανόνων, την προσαρμογή ορίων ή παραμέτρων κανόνων και τη δημιουργία προσαρμοσμένων κανόνων στη συγκεκριμένη αρχιτεκτονική δικτύου και το τοπίο απειλών του οργανισμού.

Συνολικά, το Snort χρησιμεύει ως πολύτιμο εργαλείο για τη βελτίωση της ασφάλειας του δικτύου παρέχοντας εντοπισμό και πρόληψη σε πραγματικό χρόνο ενός ευρέος φάσματος απειλών στον κυβερνοχώρο, συμπεριλαμβανομένων των μολύνσεων από κακόβουλο λογισμικό, των εισβολών στο δίκτυο και των προσπαθειών μη εξουσιοδοτημένης πρόσβασης. Η βασισμένη σε κανόνες προσέγγισή του, επιτρέπει στους οργανισμούς να εντοπίζουν αποτελεσματικά και να ανταποκρίνονται σε συμβάντα ασφαλείας, συμβάλλοντας στην προστασία κρίσιμων περιουσιακών στοιχείων και στη διατήρηση της ακεραιότητας της υποδομής του δικτύου τους (Tasneem, Kumar & Sharma, 2018).

4.4. Προκλήσεις

Οι συνεχιζόμενες μελέτες επικεντρώνονται στην ανάπτυξη νέων συστημάτων για τον αυτόματο εντοπισμό μη φυσιολογικής χρήσης του συστήματος. Ο Denning εισήγαγε ένα μοντέλο ανίχνευσης εισβολής, προτείνοντάς το ως πλαίσιο για ένα IDS γενικής χρήσης. Έκτοτε, οι ειδικοί έχουν αναπτύξει και εφαρμόζουν διάφορους αλγόριθμους για την αυτοματοποίηση της ανίχνευσης εισβολών στο δίκτυο, με στόχο την αυξημένη ακρίβεια, ταχύτητα και επεκτασιμότητα. Στην εποχή «IoT» και Big Data, ο αριθμός των συνδεδεμένων συσκευών έχει ξεπεράσει τα 26 δισεκατομμύρια, οδηγώντας σε αύξηση των ζητημάτων κυβερνοασφάλειας. Οι προκλήσεις στο IDS περιλαμβάνουν τα ποσοστά ψευδών συναγερμών, τα χαμηλά ποσοστά ανίχνευσης, τα μη ισορροπημένα σύνολα δεδομένων και τους χρόνους απόκρισης (Khraisat et al., 2019).

Ορισμένοι ερευνητές υποστηρίζουν την επέκταση των κατηγοριών IDS, προτείνοντας πέντε υποκατηγορίες: IDS που βασίζεται σε μοτίβο, βάσει κανόνων, βάσει στατιστικών, βάσει κατάστασης και ευρετικής βάσης. Ωστόσο, αυτή η ταξινόμηση μπορεί να προκαλέσει σύγχυση λόγω ομοιοτήτων μεταξύ τεχνικών και έλλειψης σαφών κριτηρίων. Τα IDS που βασίζονται σε κανόνες, για παράδειγμα, συχνά εμφανίζουν ψευδώς θετικά στοιχεία και παλεύουν με νέες επιθέσεις. Τα συστήματα αναγνώρισης που βασίζονται στην ανάλυση πρωτοκόλλων κατάστασης αντιμετωπίζουν προκλήσεις στη διατήρηση ενημερωμένων προφίλ καθώς τα πρωτόκολλα εξελίσσονται (Khraisat et al., 2019).

Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS) είναι απαραίτητα για την ασφάλεια του δικτύου και του συστήματος, αλλά αντιμετωπίζουν πολλές προκλήσεις (Khraisat et al., 2019):

- **Εσφαλμένοι θετικοί και αρνητικοί συναγερμοί:** Η εξισορρόπηση της ακρίβειας ανίχνευσης με τα ποσοστά ψευδών συναγερμών είναι ζωτικής σημασίας.

- **Όγκος και ποικιλία επισκεψιμότητας:** Η ανάλυση διαφορετικών τύπων κίνησης, συμπεριλαμβανομένων των κρυπτογραφημένων και του IoT, με παράλληλη διατήρηση της απόδοσης είναι πρόκληση.

- **Κρυπτογραφημένη κυκλοφορία:** Η επιθεώρηση κρυπτογραφημένων ωφέλιμων φορτίων χωρίς να διακυβεύεται το απόρρητο ή η απόδοση δημιουργεί δυσκολίες.

- **Προηγμένες απειλές:** Η προσαρμογή για τον εντοπισμό εξελιγμένων επιθέσεων, συμπεριλαμβανομένων των εκμεταλλεύσεων μηδενικής ημέρας, είναι απαραίτητη.

- **Εσωτερικές απειλές:** Η παρακολούθηση και η διάκριση μεταξύ νόμιμης και κακόβουλης συμπεριφοράς χρηστών είναι πρόκληση.

- **Πολυπλοκότητα δικτύου:** Η προστασία σύνθετων περιβαλλόντων χωρίς διακοπές είναι απαραίτητη.

- **Τεχνικές αποφυγής:** Η ανθεκτικότητα σε τακτικές αποφυγής όπως η κρυπτογράφηση ή η συσκότιση (obfuscation) είναι ζωτικής σημασίας.

- **Περιορισμοί πόρων:** Η εξισορρόπηση της ακρίβειας ανίχνευσης με την αποδοτικότητα των πόρων είναι απαραίτητη.

- **Κανονιστική συμμόρφωση:** Η ικανοποίηση των απαιτήσεων συμμόρφωσης με παράλληλη διατήρηση της αποτελεσματικής παρακολούθησης ασφάλειας αποτελεί πρόκληση.

- **Ενοποίηση με το Οικοσύστημα Ασφαλείας:** Η επίτευξη διαλειτουργικότητας με άλλα εργαλεία ασφαλείας είναι πολύπλοκη.

Η αντιμετώπιση αυτών των προκλήσεων απαιτεί προηγμένες τεχνολογίες όπως η μηχανική μάθηση, μαζί με ισχυρές πολιτικές και συνεχή εκπαίδευση για το προσωπικό ασφαλείας. Η τακτική αξιολόγηση και ενημέρωση του IDPS είναι ουσιαστικής σημασίας για την προσαρμογή στις εξελισσόμενες απειλές και τεχνολογίες (Khraisat et al., 2019).

5 Μελέτη περίπτωσης

5.1. Το Raspberry Pi

Το Raspberry Pi είναι μια σειρά μικρών, προσιτών υπολογιστών με μία πλακέτα που αναπτύχθηκε από το Raspberry Pi Foundation, έναν μη-κερδοσκοπικό οργανισμό με έδρα το Ηνωμένο Βασίλειο. Αυτοί οι υπολογιστές έχουν σχεδιαστεί για να προάγουν τη διδασκαλία της βασικής επιστήμης των υπολογιστών και των δεξιοτήτων προγραμματισμού σε σχολεία και αναπτυσσόμενες χώρες. Το Raspberry Pi διαθέτει διάφορα μοντέλα, καθένα από τα οποία προσφέρει διαφορετικές προδιαγραφές και δυνατότητες, αλλά όλα μοιράζονται κοινά χαρακτηριστικά όπως σύστημα Broadcom-on-chip (SoC), RAM, θύρες USB, έξοδος HDMI και GPIO (Είσοδος/Εξοδος Γενικού Σκοπού). ακίδες για διασύνδεση με εξωτερικές συσκευές και αισθητήρες. Οι υπολογιστές Raspberry Pi τρέχουν σε λειτουργικά συστήματα που βασίζονται σε Linux όπως το Raspbian (τώρα γνωστό ως Raspberry Pi OS) και μπορούν να χρησιμοποιηθούν για ένα ευρύ φάσμα εφαρμογών, όπως εκπαίδευση, οικιακός αυτοματισμός, κέντρα πολυμέσων, ρομποτική και έργα DIY (Ghael, Solanki & Sahu, 2020).

5.2. Αρχιτεκτονική

Η αρχιτεκτονική ενός Raspberry Pi βασίζεται σε ένα σχέδιο System-on-Chip (SoC), ενσωματώνοντας πολλαπλά στοιχεία σε ένα μόνο τσιπ. Ακολουθεί μια ανάλυση των βασικών αρχιτεκτονικών στοιχείων (Ghael, Solanki & Sahu, 2020):

- **Κεντρική Μονάδα Επεξεργασίας (Central Processing Unit - CPU):** Οι πλακέτες Raspberry Pi διαθέτουν επεξεργαστές βασισμένους σε ARM, οι οποίοι είναι χαμηλής κατανάλωσης και ενεργειακά αποδοτικοί. Η CPU χειρίζεται υπολογιστικές εργασίες γενικής χρήσης, όπως η εκτέλεση εφαρμογών, η εκτέλεση εντολών και η διαχείριση των πόρων του συστήματος.

- **Μονάδα Επεξεργασίας Γραφικών (Graphics Processing Unit - GPU):** Η GPU είναι υπεύθυνη για το χειρισμό εργασιών που σχετίζονται με γραφικά, συμπεριλαμβανομένης της απόδοσης εικόνων, βίντεο και διεπαφών χρήστη.

Λειτουργεί σε συνδυασμό με την CPU για να προσφέρει ομαλή απόδοση γραφικών και δυνατότητες πολυμέσων.

- **Μνήμη τυχαίας πρόσβασης (Random Access Memory - RAM):** Τα μοντέλα Raspberry Pi διαθέτουν διάφορα μεγέθη μνήμης RAM, παρέχοντας προσωρινή αποθήκευση για δεδομένα και οδηγίες προγράμματος στα οποία χρειάζεται η CPU να έχει γρήγορη πρόσβαση. Η περισσότερη μνήμη RAM γενικά οδηγεί σε βελτιωμένη απόδοση και δυνατότητες πολλαπλών ταυτόχρονων διεργασιών.

- **Διεπαφές εισόδου/εξόδου (Input/Output - I/O):** Οι πλακέτες Raspberry Pi διαθέτουν μια ποικιλία διεπαφών I/O για τη σύνδεση περιφερειακών και εξωτερικών συσκευών. Αυτές περιλαμβάνουν θύρες USB για πληκτρολόγια, ποντίκια και άλλα αξεσουάρ, θύρες HDMI για οθόνες, υποδοχές ήχου για έξοδο ήχου, θύρες Ethernet για δικτύωση και ακίδες GPIO (Γενικής Είσοδος/Έξοδος) για διασύνδεση με αισθητήρες, ενεργοποιητές και άλλα ηλεκτρονικά εξαρτήματα .

- **Αποθήκευση:** Οι υπολογιστές Raspberry Pi χρησιμοποιούν κάρτες microSD ή εξωτερικές συσκευές αποθήκευσης για την αποθήκευση του λειτουργικού συστήματος, των προγραμμάτων και των δεδομένων χρήστη. Η υποδοχή κάρτας microSD είναι η κύρια διεπαφή αποθήκευσης στα περισσότερα μοντέλα Raspberry Pi.

- **Τροφοδοσία:** Οι πλακέτες Raspberry Pi απαιτούν μια πηγή τροφοδοσίας για να λειτουργήσουν, που συνήθως παρέχεται μέσω υποδοχής τροφοδοσίας micro USB ή USB-C. Οι απαιτήσεις ισχύος ποικίλλουν ανάλογα με το μοντέλο και τα συνδεδεμένα περιφερειακά.

- **Δίκτυο:** Ορισμένα μοντέλα Raspberry Pi περιλαμβάνουν ενσωματωμένες δυνατότητες Wi-Fi και Bluetooth, επιτρέποντας ασύρματη συνδεσιμότητα για εφαρμογές δικτύωσης, επικοινωνίας και IoT. Διαφορετικά κάτι τέτοιο επιτυγχάνεται μέσω USB περιφερειακών

- **Έξοδος βίντεο:** Οι πλακέτες Raspberry Pi υποστηρίζουν έξοδο βίντεο μέσω θυρών HDMI, επιτρέποντας στους χρήστες να συνδέουν οθόνες και τηλεοράσεις για προβολή γραφικών διεπαφών χρήστη, βίντεο και άλλου περιεχομένου πολυμέσων.

- **Έξοδος ήχου:** Οι πλακέτες Raspberry Pi διαθέτουν δυνατότητες εξόδου ήχου, συνήθως μέσω υποδοχής ήχου 3,5 mm ή θύρας HDMI, δίνοντας τη δυνατότητα στους χρήστες να συνδέσουν ηχεία, ακουστικά ή εξοπλισμό ήχου για αναπαραγωγή ήχου.

Η αρχιτεκτονική ενός Raspberry Pi έχει σχεδιαστεί για να παρέχει μια συμπαγή, προσιτή και ευέλικτη πλατφόρμα για διάφορα έργα υπολογιστών και ηλεκτρονικών, που κυμαίνονται από εκπαιδευτικές δραστηριότητες έως συστήματα οικιακού αυτοματισμού DIY (Ghael, Solanki & Sahu, 2020).

5.3. Βασικά στοιχεία

Το Raspberry Pi αποτελείται από πολλά βασικά στοιχεία που συνεργάζονται για να σχηματίσουν μια πλήρη υπολογιστική πλατφόρμα. Εδώ είναι τα κύρια συστατικά ενός τυπικού Raspberry Pi (Zhao, Jegatheesan & Loon, 2015):

- **System-on-Chip (SoC):** Η καρδιά του Raspberry Pi, το SoC ενσωματώνει διάφορα βασικά στοιχεία σε ένα μόνο τσιπ. Αυτό περιλαμβάνει την CPU, την GPU, τη RAM και άλλα βασικά κυκλώματα.

- **Κεντρική Μονάδα Επεξεργασίας (CPU):** Η CPU είναι υπεύθυνη για την εκτέλεση εντολών και την εκτέλεση υπολογισμών. Τα μοντέλα Raspberry Pi χρησιμοποιούν συνήθως CPU που βασίζονται σε αρχιτεκτονική ARM, οι οποίες προσφέρουν ισορροπία απόδοσης και ενεργειακής απόδοσης.

- **Μονάδα Επεξεργασίας Γραφικών (GPU):** Η GPU χειρίζεται εργασίες που σχετίζονται με γραφικά, όπως η απόδοση εικόνων, βίντεο και διεπαφών χρήστη. Λειτουργεί παράλληλα με την CPU για να προσφέρει ομαλή απόδοση γραφικών.

- **Μνήμη τυχαίας πρόσβασης (RAM):** Η RAM παρέχει προσωρινή αποθήκευση για δεδομένα και εντολές προγράμματος στα οποία χρειάζεται η CPU να έχει γρήγορη πρόσβαση. Η περισσότερη μνήμη RAM επιτρέπει την καλύτερη εκτέλεση πολλαπλών εργασιών και απόδοση.

- **Αποθήκευση:** Οι υπολογιστές Raspberry Pi χρησιμοποιούν κάρτες microSD ή εξωτερικές συσκευές αποθήκευσης για την αποθήκευση του λειτουργικού

συστήματος, των προγραμμάτων και των δεδομένων χρήστη. Η υποδοχή κάρτας microSD είναι η κύρια διεπαφή αποθήκευσης στα περισσότερα μοντέλα Raspberry Pi.

- **Διεπαφές εισόδου/εξόδου (I/O):** Οι πλακέτες Raspberry Pi διαθέτουν διάφορες διεπαφές I/O για τη σύνδεση περιφερειακών και εξωτερικών συσκευών. Αυτές περιλαμβάνουν θύρες USB, θύρες HDMI, υποδοχές ήχου, θύρες Ethernet και ακίδες GPIO για διασύνδεση με αισθητήρες και άλλα ηλεκτρονικά εξαρτήματα.

- **Τροφοδοτικό:** Οι πλακέτες Raspberry Pi απαιτούν μια πηγή τροφοδοσίας για να λειτουργήσουν, που συνήθως παρέχεται μέσω υποδοχής τροφοδοσίας micro USB ή USB-C. Οι απαιτήσεις ισχύος ποικίλλουν ανάλογα με το μοντέλο και τα συνδεδεμένα περιφερειακά.

- **Δικτύωση:** Ορισμένα μοντέλα Raspberry Pi περιλαμβάνουν ενσωματωμένες δυνατότητες Wi-Fi και Bluetooth, επιτρέποντας ασύρματη σύνδεση και δικτύωση. Για ενσύρματη δικτύωση υπάρχει θύρα Ethernet.

- **Έξοδος βίντεο:** Οι πλακέτες Raspberry Pi υποστηρίζουν έξοδο βίντεο μέσω θυρών HDMI, επιτρέποντας στους χρήστες να συνδέουν οθόνες και τηλεοράσεις για προβολή γραφικών διεπαφών χρήστη και περιεχομένου πολυμέσων.

- **Έξοδος ήχου:** Οι πλακέτες Raspberry Pi διαθέτουν δυνατότητες εξόδου ήχου, συνήθως μέσω υποδοχής ήχου 3,5 mm ή θύρας HDMI, επιτρέποντας στους χρήστες να συνδέσουν ηχεία, ακουστικά ή εξοπλισμό ήχου για αναπαραγωγή ήχου.

Αυτά τα στοιχεία συνδυάζονται για να δημιουργήσουν μια ευέλικτη και προσιτή υπολογιστική πλατφόρμα που μπορεί να χρησιμοποιηθεί για ένα ευρύ φάσμα εφαρμογών, συμπεριλαμβανομένης της εκπαίδευσης, του οικιακού αυτοματισμού, των κέντρων πολυμέσων και των έργων IoT (Zhao, Jegatheesan & Loon, 2015):

5.4. Τύποι Επιθέσεων

Οι συσκευές Raspberry Pi, όπως κάθε άλλος υπολογιστής που είναι συνδεδεμένος σε δίκτυο, μπορεί να είναι ευάλωτες σε διάφορους τύπους επιθέσεων. Οι συνήθεις τύποι επιθέσεων που

μπορούν να στοχεύουν συσκευές Raspberry Pi περιλαμβάνουν επιθέσεις άρνησης υπηρεσίας (DoS), επιθέσεις man-in-the-middle (MitM), επιθέσεις brute force, απομακρυσμένη εκτέλεση κώδικα (RCE), δέσμες ενεργειών μεταξύ τοποθεσιών (XSS).), έγχυση SQL (SQLi), φυσικές επιθέσεις, πλαστογράφηση DNS, επιθέσεις phishing, επιθέσεις botnet IoT, κ.α. (Oh et al., 2020).

Οι επιθέσεις Denial-of-Service (DoS) στοχεύουν να κατακλύσουν τους πόρους του Raspberry Pi, όπως η CPU, η μνήμη ή το εύρος ζώνης δικτύου, καθιστώντας το απρόσιτο για τους νόμιμους χρήστες. Στις επιθέσεις MitM, οι εισβολείς υποκλέπτουν την επικοινωνία μεταξύ του Raspberry Pi και άλλων συσκευών στο δίκτυο για να παρακολουθούν ή να τροποποιούν τα δεδομένα που μεταδίδονται.

Οι επιθέσεις brute force περιλαμβάνουν τη συστηματική δοκιμή διαφορετικών συνδυασμών ονομάτων χρήστη και κωδικών πρόσβασης μέχρι να βρεθούν τα σωστά διαπιστευτήρια για να αποκτηθεί μη εξουσιοδοτημένη πρόσβαση σε ένα Raspberry Pi. Οι επιθέσεις απομακρυσμένης εκτέλεσης κώδικα (Remote Code Execution - RCE) εκμεταλλεύονται τρωτά σημεία σε λογισμικό που εκτελείται στο Raspberry Pi για την εκτέλεση αυθαίρετου κώδικα εξ αποστάσεως, επιτρέποντας ενδεχομένως στους εισβολείς να αναλάβουν τον έλεγχο της συσκευής (Oh et al., 2020).

Το Cross-site scripting (XSS) επιτίθεται σε πιθανές εφαρμογές ιστού που εκτελούνται στο Raspberry Pi, επιτρέποντας στους εισβολείς να εισάγουν κακόβουλα σενάρια σε ιστοσελίδες που βλέπουν οι χρήστες. Οι επιθέσεις SQL injection (SQLi) εκμεταλλεύονται τρωτά σημεία σε εφαρμογές web που χρησιμοποιούν βάσεις δεδομένων SQL για εξαγωγή ή χειρισμό αποθηκευμένων δεδομένων.

Οι φυσικές επιθέσεις περιλαμβάνουν την απόκτηση φυσικής πρόσβασης στη συσκευή Raspberry Pi για παραβίαση στοιχείων υλικού ή εξαγωγή ευαίσθητων πληροφοριών. Οι επιθέσεις πλαστογράφησης DNS χειραγωγούν τον Εξυπηρετητή Ονομάτων Τομέα (Domain Name Server - DNS) για να ανακατευθύνουν την κυκλοφορία δικτύου σε κακόβουλους διακομιστές που ελέγχονται από τον εισβολέα (Oh et al., 2020).

Οι επιθέσεις ηλεκτρονικού ψαρέματος χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα για να εξαπατήσουν τους χρήστες να αποκαλύψουν ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, τα οποία μπορούν να χρησιμοποιηθούν για να παραβιάσουν συσκευές Raspberry Pi ή άλλα συστήματα στο δίκτυο. Οι επιθέσεις botnet IoT στοχεύουν

συσκευές Raspberry Pi που αποτελούν κόμβους στο Internet of Things (IoT) για να τις «στρατολογήσουν» σε ένα δίκτυο παραβιασμένων συσκευών που χρησιμοποιούνται για την έναρξη κακόβουλων δραστηριοτήτων.

Για τον μετριασμό αυτών των κινδύνων, οι χρήστες του Raspberry Pi θα πρέπει να ακολουθούν τις βέλτιστες πρακτικές για την ασφάλεια των συσκευών τους, όπως η τακτική ενημέρωση λογισμικού, η χρήση ισχυρών κωδικών πρόσβασης, η ενεργοποίηση του τείχους προστασίας, η εφαρμογή ελέγχων πρόσβασης, η παρακολούθηση της κυκλοφορίας του δικτύου και η ενημέρωση σχετικά με τις συμβουλές ασφαλείας για τον εντοπισμό και την απόκριση σε πιθανές απειλές άμεσα (Oh et al., 2020).

5.1.1 UDP floods

Οι πλημμύρες UDP είναι ένας τύπος επίθεσης άρνησης υπηρεσίας (DoS) που στοχεύει το Πρωτόκολλο Δεδομένων Χρήστη (UDP), το οποίο είναι ένα πρωτόκολλο χωρίς σύνδεση που χρησιμοποιείται για τη μετάδοση δεδομένων μέσω του Διαδικτύου. Σε μια επίθεση πλημμύρας UDP, ο εισβολέας στέλνει μεγάλο όγκο πακέτων UDP σε έναν διακομιστή ή ένα δίκτυο-στόχο με σκοπό να συντρίψει τους πόρους του και να τον κάνει να μην είναι προσβάσιμος ή να μην ανταποκρίνεται στους νόμιμους χρήστες (Nagy & Coleşa, 2019).

Σε αντίθεση με το TCP (Transmission Control Protocol), το UDP δεν απαιτεί διαδικασία χειραψίας για τη δημιουργία μιας σύνδεσης, καθιστώντας ευκολότερη την παραπλάνηση των διευθύνσεων IP προέλευσης των πακέτων. Αυτό το χαρακτηριστικό του UDP επιτρέπει στους εισβολείς να εξαπολύσουν επιθέσεις πλημμύρας UDP χρησιμοποιώντας πλαστές διευθύνσεις IP, καθιστώντας δύσκολο τον εντοπισμό της προέλευσης της επίθεσης.

Οι επιθέσεις πλημμύρας UDP μπορούν να εκμεταλλευτούν τρωτά σημεία σε υποδομή δικτύου, τείχη προστασίας ή διακομιστές που δεν έχουν ρυθμιστεί σωστά για να χειρίζονται υπερβολική κίνηση UDP. Η επίθεση μπορεί να καταναλώσει το εύρος ζώνης του δικτύου, να εξαντλήσει τους πόρους του διακομιστή όπως η CPU και η μνήμη και να προκαλέσει συμφόρηση δικτύου, οδηγώντας σε υποβαθμισμένη απόδοση ή πλήρη διακοπή λειτουργίας για το στοχευόμενο σύστημα ή δίκτυο (Nagy & Coleşa, 2019).

Για τον μετριασμό των επιθέσεων πλημμύρας UDP, οι οργανισμοί μπορούν να εφαρμόσουν διάφορους αμυντικούς μηχανισμούς, όπως περιορισμό ρυθμού, φιλτράρισμα κυκλοφορίας,

συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS), τείχη προστασίας με δυνατότητες προστασίας από πλημμύρες UDP και κατανεμημένες υπηρεσίες μετριασμού άρνησης υπηρεσίας (DDoS). Επιπλέον, οι διαχειριστές δικτύου μπορούν να διαμορφώσουν δρομολογητές και switches για να μπλοκάρουν ή να φιλτράρουν ύποπτη κίνηση UDP και να παρακολουθούν την κυκλοφορία δικτύου για ενδείξεις ασυνήθιστης δραστηριότητας που μπορεί να υποδηλώνουν μια συνεχιζόμενη επίθεση πλημμύρας UDP (Nagy & Coleşa, 2019).

5.1.2 SYN floods

Η πλημμύρα SYN είναι ένας τύπος επίθεσης άρνησης υπηρεσίας (DoS) που εκμεταλλεύεται τη διαδικασία τριπλής χειραψίας του Πρωτοκόλλου Ελέγχου Μετάδοσης (Transport Control Protocol - TCP) για να κατακλύσει τους πόρους ενός διακομιστή-στόχου και να διαταράξει την ικανότητά του να ανταποκρίνεται σε νόμιμα αιτήματα. Σε μια επίθεση πλημμύρας SYN, ο εισβολέας στέλνει μεγάλο αριθμό πακέτων TCP SYN (συγχρονισμός) στον διακομιστή στόχο, αλλά δεν ολοκληρώνει τη διαδικασία χειραψίας στέλνοντας το τελικό πακέτο ACK (επιβεβαίωση). Αυτό προκαλεί τον διακομιστή να διατηρεί μισάνοιχτες συνδέσεις, δεσμεύοντας τους πόρους του και εμποδίζοντάς τον να δέχεται νέες συνδέσεις από νόμιμους χρήστες (Coşar & Kiran, 2018).

Οι επιθέσεις πλημμύρας SYN εκμεταλλεύονται τη διαδικασία χειραψίας TCP, η οποία περιλαμβάνει τρία βήματα:

- **SYN:** Ο πελάτης στέλνει ένα πακέτο SYN στον διακομιστή, ζητώντας τη δημιουργία σύνδεσης.
- **SYN-ACK:** Ο διακομιστής απαντά με ένα πακέτο SYN-ACK, αναγνωρίζοντας το αίτημα του πελάτη και δηλώνοντας την ετοιμότητά του να δημιουργήσει μια σύνδεση.
- **ACK:** Ο πελάτης στέλνει ένα πακέτο ACK για να αναγνωρίσει την απόκριση του διακομιστή, ολοκληρώνοντας την τριπλή χειραψία και δημιουργώντας τη σύνδεση.

Σε μια επίθεση πλημμύρας SYN, ο εισβολέας πλημμυρίζει τον διακομιστή στόχο με μεγάλο όγκο πακέτων SYN, αλλά είτε δεν ανταποκρίνεται στα πακέτα SYN-ACK από τον διακομιστή είτε πλαστογραφεί τις διευθύνσεις IP προέλευσης για να δυσκολέψει τον

διακομιστή να διακρίνει τα νόμιμα αιτήματα από κακόβουλα. Ως αποτέλεσμα, ο διακομιστής παρακολουθεί πολυάριθμες μισάνοιχτες συνδέσεις, εξαντλώντας τελικά τους πόρους του, όπως η μνήμη, η CPU και το εύρος ζώνης δικτύου (Coşar & Kiran, 2018).

Για τον μετριασμό των επιθέσεων πλημμύρας SYN, οι οργανισμοί μπορούν να εφαρμόσουν διάφορα αντίμετρα, όπως:

- **Cookies SYN:** Πρόκειται για τεχνική που χρησιμοποιείται από ορισμένα λειτουργικά συστήματα για τον χειρισμό επιθέσεων SYN flood δημιουργώντας μια κρυπτογραφική τιμή κατακερματισμού (hash check) που βασίζεται στο αρχικό πακέτο SYN, επιτρέποντας στον διακομιστή να επικυρώνει τα επόμενα πακέτα ACK χωρίς να διατηρεί πληροφορίες κατάστασης για μισάνοιχτες συνδέσεις.

- **Περιορισμός ρυθμού:** Εφαρμογή μέτρων περιορισμού ρυθμού για τον έλεγχο του αριθμού των εισερχόμενων πακέτων SYN ανά δευτερόλεπτο, αποτρέποντας τον κατακλυσμό του διακομιστή από υπερβολικά αιτήματα σύνδεσης.

- **Διακομιστής μεσολάβησης SYN:** Χρήση διακομιστή μεσολάβησης SYN ή εξισορρόπησης φορτίου για την αναχαίτιση εισερχόμενων πακέτων SYN και την επικύρωση της νομιμότητάς τους πριν από την προώθηση τους στον διακομιστή προορισμού, προστατεύοντας έτσι τον διακομιστή από επιθέσεις πλημμύρας SYN.

- **Κανόνες τείχους προστασίας:** Διαμόρφωση τείχους προστασίας για φιλτράρισμα και αποκλεισμό ύποπτων πακέτων SYN με βάση προκαθορισμένους κανόνες ή ευριστικές μεθόδους, συμβάλλοντας στον μετριασμό του αντίκτυπου των επιθέσεων πλημμύρας SYN στον διακομιστή-στόχο.

Συνολικά, οι επιθέσεις πλημμύρας SYN αποτελούν σημαντική απειλή για τη διαθεσιμότητα και την απόδοση των διαδικτυακών υπηρεσιών και οι οργανισμοί θα πρέπει να λαμβάνουν προληπτικά μέτρα για την προστασία των διακομιστών και των δικτύων τους από τέτοιες επιθέσεις (Coşar & Kiran, 2018).

5.1.3 ARP spoofing

Η πλαστογράφηση Address Resolution Protocol - ARP, γνωστή και ως δηλητηρίαση προσωρινής μνήμης ARP ή δηλητηρίαση ARP, είναι ένας τύπος επίθεσης κατά την οποία ένας εισβολέας στέλνει παραποιημένα μηνύματα πρωτοκόλλου ανάλυσης διευθύνσεων (ARP) μέσω ενός τοπικού δικτύου (LAN). Ο σκοπός της πλαστογράφησης ARP είναι να συσχετίσει τη διεύθυνση MAC του εισβολέα με τη διεύθυνση IP μιας άλλης συσκευής (όπως ένας δρομολογητής ή ένας διακομιστής) στο δίκτυο. Αυτό επιτρέπει στον εισβολέα να υποκλέψει, να τροποποιήσει ή να ανακατευθύνει την κυκλοφορία δικτύου που προορίζεται για τη στοχευμένη συσκευή, οδηγώντας σε διάφορους κινδύνους ασφαλείας και πιθανές επιθέσεις (Nasser & Hussain, 2022).

- **Πρωτόκολλο ARP:** Το ARP είναι ένα πρωτόκολλο που χρησιμοποιείται για την αντιστοίχιση διευθύνσεων IP σε διευθύνσεις MAC σε ένα τοπικό δίκτυο. Όταν μια συσκευή χρειάζεται να επικοινωνήσει με μια άλλη συσκευή στο ίδιο δίκτυο, χρησιμοποιεί ARP για να επιλύσει τη διεύθυνση MAC που σχετίζεται με τη διεύθυνση IP προορισμού.

- **Παραποιημένα μηνύματα ARP:** Σε μια επίθεση πλαστογράφησης ARP, ο εισβολέας στέλνει παραποιημένα μηνύματα ARP σε άλλες συσκευές του δικτύου. Αυτά τα μηνύματα περιέχουν πλαστές πληροφορίες, που συσχετίζουν τη διεύθυνση MAC του εισβολέα με τη διεύθυνση IP μιας άλλης νόμιμης συσκευής στο δίκτυο.

- **Δηλητηρίαση προσωρινής μνήμης ARP:** Όταν οι συσκευές στο δίκτυο λαμβάνουν τα παραποιημένα μηνύματα ARP, ενημερώνουν τις κρυφές μνήμες ARP με τις πλαστές πληροφορίες. Ως αποτέλεσμα, πιστεύουν ότι η διεύθυνση MAC του εισβολέα σχετίζεται με τη διεύθυνση IP της στοχευμένης συσκευής.

- **Ανακατεύθυνση επισκεψιμότητας:** Με δηλητηριασμένη την προσωρινή μνήμη ARP, η κίνηση δικτύου που προορίζεται για τη στοχευμένη συσκευή αποστέλλεται στη διεύθυνση MAC του εισβολέα. Ο εισβολέας μπορεί στη συνέχεια να παρεμποδίσει, να τροποποιήσει ή να ανακατευθύνει την κίνηση όπως επιθυμεί.

- **Πιθανές επιθέσεις:** Η πλαστογράφηση ARP μπορεί να χρησιμοποιηθεί για διάφορους κακόβουλους σκοπούς, όπως:

- **Επιθέσεις Man-in-the-Middle (MITM):** Ο εισβολέας παρεμποδίζει και παρακολουθεί την επικοινωνία μεταξύ δύο μερών, υποκλέπτοντας ενδεχομένως ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης ή οικονομικά δεδομένα.

- **Παραβίαση συνεδρίας:** Ο εισβολέας αναλαμβάνει τον έλεγχο μιας υπάρχουσας περιόδου σύνδεσης μεταξύ δύο μερών, επιτρέποντάς τους να μιμηθούν ένα από τα μέρη και να εκτελέσουν μη εξουσιοδοτημένες ενέργειες.

- **Επιθέσεις άρνησης υπηρεσίας (DoS):** Ανακατευθύνοντας την κυκλοφορία μακριά από νόμιμες συσκευές, ο εισβολέας μπορεί να διακόψει την επικοινωνία του δικτύου και να προκαλέσει διακοπές στην υπηρεσία.

Για τον μετριασμό των επιθέσεων πλαστογράφησης ARP, οι διαχειριστές δικτύου μπορούν να εφαρμόσουν διάφορα αντίμετρα, όπως (Nasser & Hussain, 2022):

- **ARP Spoofing Detection:** Παρακολούθηση της κυκλοφορίας ARP και ανίχνευση ανωμαλιών όπως πολλαπλές διευθύνσεις MAC που σχετίζονται με την ίδια διεύθυνση IP.

- **ARP Spoofing Prevention:** Εφαρμογή μηχανισμών όπως στατικές καταχωρήσεις ARP, ρυθμίσεις χρονικού ορίου λήξης της προσωρινής μνήμης ARP ή εργαλεία ανίχνευσης πλαστογράφησης ARP για την πρόληψη ή τον μετριασμό των επιπτώσεων των επιθέσεων πλαστογράφησης ARP.

- **Τμηματοποίηση δικτύου:** Διαμερισμός του δικτύου σε ξεχωριστά τμήματα ή VLAN για τον περιορισμό του εύρους των επιθέσεων πλαστογράφησης ARP και τη μείωση του πιθανού αντίκτυπου στην ασφάλεια του δικτύου.

- **Κρυπτογράφηση και έλεγχος ταυτότητας:** Χρήση πρωτοκόλλων κρυπτογράφησης όπως HTTPS ή IPsec για την προστασία ευαίσθητων δεδομένων κατά τη μεταφορά και εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας για την επαλήθευση της ταυτότητας των συσκευών δικτύου.

Συνολικά, η πλαστογράφηση ARP ενέχει σημαντικό κίνδυνο ασφάλειας για τα τοπικά δίκτυα και οι οργανισμοί θα πρέπει να λαμβάνουν προληπτικά μέτρα για τον εντοπισμό, την

πρόληψη και τον μετριασμό των επιπτώσεων των επιθέσεων πλαστογράφησης ARP στην υποδομή του δικτύου τους (Nasser & Hussain, 2022).

5.1.4 SQL injection

Η έγχυση SQL είναι ένας τύπος επίθεσης στον κυβερνοχώρο που στοχεύει τα τρωτά σημεία ασφαλείας της βάσης δεδομένων μιας εφαρμογής Ιστού. Στις επιθέσεις SQL injection, κακόβουλοι παράγοντες εκμεταλλεύονται πεδία εισαγωγής χρηστών ή παραμέτρους URL για να εισάγουν κώδικα SQL σε ερωτήματα βάσης δεδομένων. Αυτός ο κώδικας SQL που εισάγεται μπορεί να χειραγωγήσει τη συμπεριφορά της βάσης δεδομένων, οδηγώντας ενδεχομένως σε μη εξουσιοδοτημένη πρόσβαση, κλοπή δεδομένων, χειραγώγηση δεδομένων ή ακόμα και πλήρη παραβίαση της βάσης δεδομένων (Singh & Aksanli, 2019):

- **Εισαγωγή χρήστη:** Μια εφαρμογή Ιστού περιλαμβάνει φόρμες ή παραμέτρους διεύθυνσης URL που δέχονται εισαγωγές χρήστη, όπως φόρμες σύνδεσης, πεδία αναζήτησης ή φόρμες υποβολής δεδομένων.

- **Σημείο έγχυσης:** Η εφαρμογή Ιστού αποτυγχάνει να επικυρώσει ή να ελέγξει σωστά την είσοδο του χρήστη, επιτρέποντας στους εισβολείς να εισάγουν εντολές SQL απευθείας στα ερωτήματα SQL της εφαρμογής.

- **Κακόβουλο ωφέλιμο φορτίο:** Ο εισβολέας υποβάλλει ειδικά διαμορφωμένη είσοδο που περιέχει κώδικα SQL ως μέρος της εισαγωγής χρήστη. Αυτός ο κώδικας SQL έχει σχεδιαστεί για να χειρίζεται τη συμπεριφορά της βάσης δεδομένων προς όφελος του εισβολέα.

- **Εκτέλεση:** Όταν η εφαρμογή Ιστού επεξεργάζεται την είσοδο του χρήστη χωρίς την κατάλληλη επικύρωση, κατασκευάζει ερωτήματα SQL χρησιμοποιώντας τον κώδικα SQL που έχει εισαχθεί και τα στέλνει στη βάση δεδομένων για εκτέλεση.

- **Χειρισμός βάσης δεδομένων:** Οι εντολές SQL που εισάγονται εκτελούνται στο πλαίσιο της βάσης δεδομένων, επιτρέποντας δυνητικά στον εισβολέα να παρακάμψει τον έλεγχο ταυτότητας, να ανακτήσει ευαίσθητα δεδομένα, να τροποποιήσει ή να διαγράψει εγγραφές βάσης δεδομένων ή να εκτελέσει άλλες κακόβουλες ενέργειες.

Οι επιθέσεις SQL injection μπορεί να έχουν σοβαρές συνέπειες, όπως (Singh & Aksanli, 2019):

- **Διαρροή δεδομένων:** Οι εισβολείς μπορούν να εξαγάγουν ευαίσθητες πληροφορίες από τη βάση δεδομένων, όπως διαπιστευτήρια χρήστη, προσωπικά δεδομένα ή οικονομικά αρχεία.

- **Χειρισμός δεδομένων:** Οι εισβολείς μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία βάσης δεδομένων, να αλλάξουν τη συμπεριφορά της εφαρμογής ή να παραβιάσουν κρίσιμα δεδομένα.

- **Μη εξουσιοδοτημένη πρόσβαση:** Οι εισβολείς μπορούν να παρακάμψουν μηχανισμούς ελέγχου ταυτότητας, να αποκτήσουν δικαιώματα διαχειριστή ή να κλιμακώσουν την πρόσβασή τους εντός της εφαρμογής ή της βάσης δεδομένων.

- **Συμβιβασμός εφαρμογής:** Τα τρωτά σημεία έγχυσης SQL μπορούν να αξιοποιηθούν για να παραβιάσουν ολόκληρη την εφαρμογή Ιστού, οδηγώντας ενδεχομένως σε περαιτέρω επιθέσεις ή εκμετάλλευση άλλων στοιχείων του συστήματος.

Για την αποτροπή επιθέσεων SQL injection, οι προγραμματιστές και οι διαχειριστές μπορούν να εφαρμόσουν πολλές βέλτιστες πρακτικές, όπως (Singh & Aksanli, 2019):

- **Επικύρωση και απολύμανση εισόδου:** Επικύρωση και καθαρισμός όλων των στοιχείων εισόδου του χρήστη για τη διασφάλιση ότι συμμορφώνονται με τις αναμενόμενες μορφές και δεν περιέχουν κακόβουλο κώδικα.

- **Παραμετροποιημένα ερωτήματα:** Χρήση παραμετροποιημένων ερωτημάτων ή προετοιμασμένων δηλώσεων με δεσμευμένες παραμέτρους για το διαχωρισμό του κώδικα SQL από την είσοδο του χρήστη και την αποτροπή επιθέσεων έγχυσης.

- **Αρχή ελάχιστου προνομίου:** Περιορισμός των δικαιωμάτων του χρήστη της βάσης δεδομένων μόνο σε εκείνα που είναι απαραίτητα για τη λειτουργικότητα της εφαρμογής, μειώνοντας τον πιθανό αντίκτυπο των επιτυχημένων επιθέσεων SQL injection.

- **Τείχη προστασίας εφαρμογών Ιστού (WAF):** Ανάπτυξη WAF για την επιθεώρηση και το φιλτράρισμα της εισερχόμενης κυκλοφορίας ιστού, αποκλείοντας αιτήματα που περιέχουν ύποπτα μοτίβα έγχυσης SQL.

- **Τακτικοί έλεγχοι ασφαλείας:** Διεξαγωγή τακτικών ελέγχων ασφαλείας και αξιολογήσεων τρωτών εφαρμογών και βάσεων δεδομένων Ιστού για τον εντοπισμό και την αποκατάσταση των τρωτών σημείων του SQL injection προληπτικά.

Εφαρμόζοντας αυτά τα προληπτικά μέτρα και υιοθετώντας μια νοοτροπία για την ασφάλεια στην ανάπτυξη εφαρμογών Ιστού, οι οργανισμοί μπορούν να μειώσουν σημαντικά τον κίνδυνο επιθέσεων SQL injection και να προστατεύσουν τις βάσεις δεδομένων τους από κακόβουλες ενέργειες (Singh & Aksanli, 2019).

5.1.5 Port scanning

Η σάρωση θυρών είναι ένας τύπος τεχνικής αναγνώρισης δικτύου που χρησιμοποιείται από τους εισβολείς για τον εντοπισμό ανοιχτών θυρών σε ένα σύστημα ή δίκτυο στόχου. Οι ανοιχτές θύρες αντιπροσωπεύουν υπηρεσίες δικτύου που ακούν ενεργά για εισερχόμενες συνδέσεις, όπως διακομιστές web (θύρα 80), διακομιστές email (θύρα 25) ή διακομιστές SSH (θύρα 22). Με σάρωση για ανοιχτές θύρες, οι εισβολείς μπορούν να συλλέξουν πληροφορίες σχετικά με την αρχιτεκτονική δικτύου, τις υπηρεσίες και τις πιθανές ευπάθειες του στόχου (Oh et al., 2020).

- **Επιλογή στόχου:** Οι εισβολείς προσδιορίζουν μία ή περισσότερες διευθύνσεις IP-στόχους ή εύρη προς σάρωση. Αυτοί οι στόχοι θα μπορούσαν να είναι συγκεκριμένοι κεντρικοί υπολογιστές, ολόκληρα υποδίκτυα ή εύρη διευθύνσεων IP που σχετίζονται με έναν συγκεκριμένο οργανισμό ή δίκτυο.
- **Τεχνικές σάρωσης θυρών:** Οι εισβολείς χρησιμοποιούν διάφορες τεχνικές σάρωσης θυρών για να διερευνήσουν το δίκτυο του στόχου και να αναγνωρίσουν τις ανοιχτές θύρες. Οι κοινές τεχνικές σάρωσης θυρών περιλαμβάνουν:
- **Σάρωση σύνδεσης TCP:** Αυτή η μέθοδος επιχειρεί να δημιουργήσει μια πλήρη σύνδεση TCP με κάθε θύρα στο στόχο. Εάν μια σύνδεση είναι επιτυχής, η θύρα θεωρείται ανοιχτή.
- **SYN Scan (Half-Open Scan):** Γνωστή και ως SYN stealth scanning, αυτή η τεχνική στέλνει πακέτα SYN στις θύρες του στόχου και αναλύει τις αποκρίσεις. Εάν ο στόχος αποκριθεί με ένα πακέτο SYN/ACK, η θύρα θεωρείται ανοιχτή.

- **Σάρωση UDP:** Η σάρωση UDP περιλαμβάνει την αποστολή πακέτων UDP σε διάφορες θύρες και την ανάλυση των απαντήσεων. Οι ανοιχτές θύρες UDP συνήθως δεν αποκρίνονται με μήνυμα σφάλματος ICMP, το οποίο υποδεικνύει ότι η θύρα είναι ανοιχτή.
- **FIN Scan:** Αυτή η μέθοδος στέλνει πακέτα FIN στις θύρες του στόχου και αναλύει τις απαντήσεις. Εάν η θύρα ανταποκρίνεται με ένα πακέτο RST, η θύρα θεωρείται κλειστή. διαφορετικά, θεωρείται ανοιχτή ή φιλτραρισμένη.
- **Ανάλυση και απαρίθμηση:** Μόλις ολοκληρωθεί η σάρωση της θύρας, οι εισβολείς αναλύουν τα αποτελέσματα για να εντοπίσουν τις ανοιχτές θύρες και τις αντίστοιχες υπηρεσίες που εκτελούνται σε αυτές τις θύρες. Αυτές οι πληροφορίες βοηθούν τους εισβολείς να κατανοήσουν την τοπολογία δικτύου του στόχου και να εντοπίσουν πιθανά σημεία εισόδου για περαιτέρω εκμετάλλευση.
- **Εκτίμηση ευπάθειας:** Αφού εντοπίσουν ανοιχτές θύρες και υπηρεσίες, οι εισβολείς ενδέχεται να πραγματοποιήσουν πρόσθετες αναγνωρίσεις για να συγκεντρώσουν πληροφορίες σχετικά με τις εκδόσεις λογισμικού, τις διαμορφώσεις και τα πιθανά τρωτά σημεία του στόχου. Αυτές οι πληροφορίες βοηθούν τους επιτιθέμενους να δώσουν προτεραιότητα στους φορείς επίθεσης και να προσαρμόσουν ανάλογα τις τεχνικές εκμετάλλευσής τους.

Η σάρωση θύρας μπορεί να χρησιμοποιηθεί τόσο για νόμιμους σκοπούς, όπως για την αντιμετώπιση προβλημάτων δικτύου και τον έλεγχο ασφαλείας, όσο και για κακόβουλες δραστηριότητες, όπως η αναγνώριση για επιθέσεις στον κυβερνοχώρο. Για την άμυνα έναντι των σαρώσεων θυρών και τον μετριασμό του κινδύνου μη εξουσιοδοτημένης πρόσβασης, οι οργανισμοί μπορούν να εφαρμόσουν μέτρα ασφαλείας όπως (Oh et al., 2020):

- Κανόνες τείχους προστασίας για περιορισμό της πρόσβασης σε περιττές θύρες και πρωτόκολλα.
- Συστήματα ανίχνευσης και πρόληψης εισβολής (IDPS) για τον εντοπισμό και τον αποκλεισμό ύποπτης δραστηριότητας σάρωσης θυρών.
- Εργαλεία παρακολούθησης δικτύου για την καταγραφή και ανάλυση της κυκλοφορίας δικτύου για ενδείξεις σάρωσης κακόβουλης θύρας.
- Τακτικές αξιολογήσεις ασφαλείας και σαρώσεις ευπάθειας για τον εντοπισμό και την αποκατάσταση ανοιχτών θυρών και υπηρεσιών.

5.5. Configuration του Snort

Η διαμόρφωση του Snort περιλαμβάνει πολλά βήματα που πρέπει να γίνουν για τη ρύθμιση του συστήματος ανίχνευσης και πρόληψης εισβολής (IDPS) σύμφωνα με το περιβάλλον του δικτύου και τις απαιτήσεις ασφαλείας. Το Snort μπορεί να εγκατασταθεί στο σύστημα, είτε μέσω διαχειριστών πακέτων, όπως το apt, είτε με τη μη αυτόματη μεταγλώττιση του πηγαίου κώδικα. Μόλις εγκατασταθεί, το κύριο αρχείο διαμόρφωσης, που συνήθως ονομάζεται `snort.conf`, θα πρέπει να ελεγχθεί και να τροποποιηθεί για να προσαρμόσει τη συμπεριφορά, τα σύνολα κανόνων, τους προεπεξεργαστές και τις εξόδους του Snort με βάση τη ρύθμιση του δικτύου σας και τις πολιτικές ασφαλείας (Saâdaoui et al., 2015).

Στη συνέχεια, οι επιθυμητές διεπαφές δικτύου θα πρέπει να ρυθμιστούν ώστε να παρακολουθούνται από το Snort και θα πρέπει να οριστούν τα υποδίκτυα που πρέπει να προστατευθούν. Στη συνέχεια, το σύνολο κανόνων μπορεί να προσαρμοστεί ενεργοποιώντας ή απενεργοποιώντας συγκεκριμένους κανόνες, τροποποιώντας τις επιλογές κανόνων και προσθέτοντας προσαρμοσμένους κανόνες στο περιβάλλον εργασίας. Οι προεπεξεργαστές που περιλαμβάνονται στο Snort μπορούν να ενεργοποιηθούν ή να απενεργοποιηθούν όπως απαιτείται για την ανάλυση της κυκλοφορίας δικτύου για ανωμαλίες, όπως η κανονικοποίηση HTTP και η ανίχνευση σάρωσης θυρών.

Το Snort θα πρέπει να ρυθμιστεί ώστε να δημιουργεί αρχεία καταγραφής και ειδοποιήσεις για συμβάντα που έχουν εντοπιστεί, με καθορισμένες επιλογές καταγραφής και προορισμούς εξόδου, όπως αρχεία καταγραφής ή εξωτερικά συστήματα όπως λύσεις SIEM. Η συμπεριφορά του χρόνου εκτέλεσης του Snort μπορεί να προσαρμοστεί ορίζοντας επιλογές όπως κατώφλια ανίχνευσης και παραμέτρους συντονισμού απόδοσης με βάση τους πόρους του υλικού σας και το επιθυμητό επίπεδο ευαισθησίας ανίχνευσης εισβολής (Saâdaoui et al., 2015).

Αφού ρυθμιστεί, η υπηρεσία Snort μπορεί να ξεκινήσει για να αρχίσει να παρακολουθεί την κυκλοφορία του δικτύου και να ανιχνεύει πιθανές εισβολές. Τα αρχεία καταγραφής και οι ειδοποιήσεις του Snort θα πρέπει να παρακολουθούνται για να διασφαλιστεί ότι λειτουργεί σωστά και ότι η διαμόρφωσή του μπορεί να ρυθμιστεί με ακρίβεια ανάλογα με τις ανάγκες με βάση τα εντοπισμένα συμβάντα και τα ψευδώς θετικά αποτελέσματα. Λεπτομερείς οδηγίες, βέλτιστες πρακτικές και συμβουλές αντιμετώπισης προβλημάτων μπορούν να

βρεθούν στην τεκμηρίωση του Snort, στους οδηγούς χρήσης και στους πόρους της κοινότητας σε όλη τη διαδικασία διαμόρφωσης. Επιπλέον, το σύνολο κανόνων και η έκδοση λογισμικού του Snort θα πρέπει να ενημερώνονται τακτικά για να διασφαλίζεται ότι παραμένει αποτελεσματικό έναντι των εξελισσόμενων απειλών και τρωτών σημείων (Saâdaoui et al., 2015).

5.6. Επίδοση

Η απόδοση του Raspberry Pi μπορεί να ποικίλλει ανάλογα με το μοντέλο και τις προδιαγραφές του. Γενικά, το Raspberry Pi προσφέρει αξιοπρεπή απόδοση για τις περιπτώσεις χρήσης που προορίζεται, οι οποίες περιλαμβάνουν εκπαιδευτικούς σκοπούς, έργα DIY, εφαρμογές IoT και βασικές εργασίες υπολογιστών (Zhao Jegatheesan & Loon, 2015).

Τα τελευταία μοντέλα, όπως το Raspberry Pi 4, παρουσιάζουν σημαντικές βελτιώσεις όσον αφορά την ισχύ επεξεργασίας, τη μνήμη και τη συνδεσιμότητα σε σύγκριση με προηγούμενες εκδόσεις. Αυτές οι βελτιώσεις συμβάλλουν σε καλύτερη συνολική απόδοση, επιτρέποντας στο Raspberry Pi 4 να χειρίζεται πιο απαιτητικές εργασίες και να εκτελεί ομαλά ένα ευρύτερο φάσμα εφαρμογών.

Ωστόσο, το Raspberry Pi εξακολουθεί να θεωρείται ένας χαμηλού κόστους υπολογιστής με μία πλακέτα και η απόδοσή του μπορεί να μην ταιριάζει με εκείνη των επιτραπέζιων ή φορητών υπολογιστών υψηλότερης ποιότητας. Μπορεί να δυσκολεύεται με εργασίες που απαιτούν πόρους, όπως παιχνίδια, επεξεργασία βίντεο ή εκτέλεση σύνθετων εφαρμογών λογισμικού (Zhao Jegatheesan & Loon, 2015).

Για βέλτιστη απόδοση, είναι απαραίτητο να λάβετε υπόψη παράγοντες όπως η ψύξη, η παροχή ρεύματος και τα περιφερειακά υλικού όταν χρησιμοποιείτε το Raspberry Pi. Επιπλέον, η βελτιστοποίηση των διαμορφώσεων λογισμικού και η επιλογή ελαφρών εφαρμογών μπορούν να βοηθήσουν στη βελτίωση της απόδοσης στις συσκευές Raspberry Pi.

6 Αποτελέσματα

Τα Συστήματα ανίχνευσης εισβολών (IDS) και τα Συστήματα πρόληψης εισβολών (IPS) είναι ζωτικής σημασίας στοιχεία αυτής της αμυντικής στρατηγικής. Αυτό το κεφάλαιο επικεντρώνεται στην πρακτική εφαρμογή του Snort, ενός ευρέως χρησιμοποιούμενου IDS/IPS ανοικτού κώδικα, και στην ενσωμάτωσή του με το Grafana για βελτιωμένη οπτικοποίηση και παρακολούθηση.

Ο πρωταρχικός στόχος της εργασίας είναι να επιδείξει τις δυνατότητες ανίχνευσης του Snort όταν υποβάλλεται σε διάφορες κοινές επιθέσεις δικτύου. Χρησιμοποιώντας εικονικές μηχανές (VM) για την προσομοίωση ενός περιβάλλοντος δικτύου, το Snort θα αναπτυχθεί για την παρακολούθηση και την προστασία μιας μηχανής-στόχου από προσομοιωμένες επιθέσεις που πραγματοποιούνται από μια μηχανή επιτιθέμενου Kali Linux. Το έργο περιλαμβάνει τη δημιουργία ενός εικονικού περιβάλλοντος, τη διαμόρφωση του Snort με σχετικά σύνολα κανόνων και την έναρξη επιθέσεων όπως UDP floods, SYN floods, ARP spoofing, SQL injection και σάρωση θυρών.

Μέσω αυτής της εγκατάστασης, στόχος μας είναι να αναδείξουμε την αποτελεσματικότητα του Snort στον εντοπισμό και την αντιμετώπιση απειλών δικτύου. Η ενσωμάτωση με το Grafana θα καταδείξει περαιτέρω τον τρόπο με τον οποίο μπορεί να βελτιωθεί η παρακολούθηση και η ανάλυση σε πραγματικό χρόνο, παρέχοντας μια ολοκληρωμένη εικόνα των συμβάντων ασφάλειας δικτύου. Η εργασία δεν χρησιμεύει μόνο ως πρακτικός οδηγός για την εγκατάσταση και τη διαμόρφωση του Snort, αλλά υπογραμμίζει επίσης τη σημασία των προληπτικών μηχανισμών άμυνας δικτύου στις σύγχρονες πρακτικές κυβερνοασφάλειας.

6.1 Εγκατάσταση Snort IDS/IPS

Τι είναι το Snort? Το Snort είναι ένα σύστημα ανίχνευσης εισβολών δικτύου (NIDS) και σύστημα πρόληψης εισβολών (IPS) ανοικτού κώδικα. Έχει σχεδιαστεί για να αναλύει την κυκλοφορία του δικτύου σε πραγματικό χρόνο, ώστε να ανιχνεύει και να ανταποκρίνεται σε κακόβουλες δραστηριότητες. Το Snort μπορεί να ρυθμιστεί ώστε να εκτελεί διάφορες λειτουργίες, όπως καταγραφή πακέτων, ανάλυση πρωτοκόλλων και αναζήτηση/αντιστοίχιση περιεχομένου. Αυτές οι δυνατότητες επιτρέπουν στο Snort να εντοπίζει και να αντιδρά σε ένα ευρύ φάσμα πιθανών απειλών ασφαλείας.

Βασική Ορολογία:

- **Network Intrusion Detection System (NIDS):** Σύστημα που παρακολουθεί την κυκλοφορία του δικτύου για ύποπτη δραστηριότητα και εκδίδει ειδοποιήσεις όταν εντοπίζεται τέτοια δραστηριότητα. Σε αντίθεση με τα συστήματα ανίχνευσης εισβολών που βασίζονται σε κεντρικούς υπολογιστές (HIDS), τα οποία παρακολουθούν έναν μεμονωμένο κεντρικό υπολογιστή ή συσκευή, τα NIDS εξετάζουν την κυκλοφορία ενός ολόκληρου τμήματος δικτύου.
- **Intrusion Prevention System (IPS):** Παρόμοια με ένα IDS, ένα IPS όχι μόνο ανιχνεύει αλλά και αποτρέπει τις απειλές που ανιχνεύονται, μπλοκάροντας ενεργά την ύποπτη κυκλοφορία.
- **Real-time Analysis:** Η δυνατότητα ανάλυσης των δεδομένων κατά την καταγραφή τους, χωρίς σημαντικές καθυστερήσεις, επιτρέποντας την άμεση ανίχνευση και αντιμετώπιση των απειλών
- **Rules:** Το Snort χρησιμοποιεί μια γλώσσα βασισμένη σε κανόνες για να ορίσει τις συνθήκες υπό τις οποίες θα πρέπει να παράγει ειδοποιήσεις ή να αναλαμβάνει δράση. Αυτοί οι κανόνες μπορούν να ανιχνεύσουν ένα ευρύ φάσμα απειλών εξετάζοντας τις επικεφαλίδες και τα ωφέλιμα φορτία πακέτων για γνωστά μοτίβα επιθέσεων.

Community Rules: Οι community rules του Snort είναι ένα σύνολο προκαθορισμένων κανόνων ανίχνευσης που συντηρούνται και ενημερώνονται από την κοινότητα του Snort. Αυτοί οι κανόνες παρέχουν μια ολοκληρωμένη βάση για τον εντοπισμό κοινών απειλών και είναι ελεύθερα διαθέσιμοι σε όλους τους χρήστες του Snort. Καλύπτουν ένα ευρύ φάσμα φορέων επιθέσεων και αποτελούν ένα καλό σημείο εκκίνησης για τη ρύθμιση του Snort.

Snort Detection for UDP Flood Attack: Το Snort μπορεί να ανιχνεύσει πλημμύρες UDP παρακολουθώντας έναν ασυνήθιστα υψηλό όγκο κυκλοφορίας UDP που κατευθύνεται σε έναν μόνο στόχο ή θύρα. Μπορούν να γραφτούν ειδικοί κανόνες για να ειδοποιούν για αυτά τα μοτίβα

Snort Detection for SYN Flood Attack: Το Snort μπορεί να ανιχνεύσει πλημμύρες SYN εντοπίζοντας μεγάλο αριθμό ατελών χειραψιών TCP. Μπορούν να οριστούν κανόνες για να επισημαίνουν επαναλαμβανόμενα πακέτα SYN χωρίς αντίστοιχες απαντήσεις ACK.

Snort Detection for ARP Spoofing: Το Snort μπορεί να ανιχνεύσει την παραποίηση ARP παρακολουθώντας για πακέτα ARP που έχουν ύποπτους ή μη αναμενόμενους συνδυασμούς

διευθύνσεων IP/MAC πηγής. Μπορούν να οριστούν κανόνες για την καταγραφή αυτών των ανωμαλιών.

Snort Detection for SQL Injection: Το Snort μπορεί να ανιχνεύσει απόπειρες SQL Injection αναζητώντας μοτίβα στην κίνηση του διαδικτύου που ταιριάζουν με γνωστές τεχνικές SQL Injection. Οι κανόνες μπορούν να αναζητήσουν λέξεις-κλειδιά όπως "SELECT", "INSERT", "DROP", κ.λπ., σε συνδυασμό με ύποπτα μοτίβα εισόδου.

Snort Detection for Port Scanning: Το Snort μπορεί να ανιχνεύσει σάρωση θύρας αναγνωρίζοντας μοτίβα πολλαπλών προσπαθειών σύνδεσης σε διαφορετικές θύρες σε έναν κεντρικό υπολογιστή μέσα σε σύντομο χρονικό διάστημα. Μπορούν να γραφτούν ειδικοί κανόνες για να ειδοποιούν για αυτές τις δραστηριότητες.

```
      @Ubuntu:~$ sudo snort -T -i enp3s0 -c /etc/snort/snort.conf
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741
 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014
8 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 944
0 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
```

Εικόνα 4 – Snort παρακολούθηση σάρωσης θυρών

6.2 Εγκατάσταση Grafana

Τι είναι το Grafana? Το Grafana είναι μια πλατφόρμα ανοικτού κώδικα που έχει σχεδιαστεί για την παρακολούθηση και την παρατηρησιμότητα. Επιτρέπει στους χρήστες να πραγματοποιούν ερωτήματα, να οπτικοποιούν και να ειδοποιούν για μετρήσεις που συλλέγονται από διάφορες πηγές δεδομένων. Το Grafana χρησιμοποιείται ευρέως στην υποδομή πληροφορικής, την παρακολούθηση εφαρμογών και την ανάλυση επιδόσεων για την παροχή πληροφοριών σε πραγματικό χρόνο μέσω διαδραστικών ταμπλό και ειδοποιήσεων.

Βασική Ορολογία:

- **Monitoring:** Η συνεχής παρατήρηση ενός συστήματος για την παρακολούθηση της απόδοσης, τον εντοπισμό προβλημάτων και τη διασφάλιση ότι όλα λειτουργούν εντός των αναμενόμενων παραμέτρων.

- **Observability:** Ένα μέτρο του πόσο καλά μπορούν να συναχθούν οι εσωτερικές καταστάσεις ενός συστήματος από τη γνώση των εξωτερικών εξόδων του. Συχνά περιλαμβάνει τη συλλογή αρχείων καταγραφής, μετρήσεων και ιχνών.

- **Metrics:** Ποσοτικά δεδομένα που συλλέγονται από διάφορες πηγές και αντιπροσωπεύουν την απόδοση και τη συμπεριφορά ενός συστήματος (π.χ. χρήση CPU, κατανάλωση μνήμης, ρυθμός αιτημάτων).

- **Alerts:** Ειδοποιήσεις που ενεργοποιούνται από συγκεκριμένες συνθήκες στις μετρήσεις, οι οποίες χρησιμοποιούνται για την ενημέρωση των χρηστών σχετικά με κρίσιμα συμβάντα ή προβλήματα επιδόσεων.

Βασικά χαρακτηρηστικά Grafana:

1. **Data Source Integration:** Η Grafana μπορεί να συνδεθεί σε ένα ευρύ φάσμα πηγών δεδομένων, όπως Prometheus, InfluxDB, Graphite, Elasticsearch, MySQL, PostgreSQL και πολλές άλλες. Αυτή η ευελιξία του επιτρέπει τη συγκέντρωση και οπτικοποίηση δεδομένων από διαφορετικά συστήματα.
2. **Querying:** Η Grafana παρέχει ισχυρές δυνατότητες αναζήτησης που επιτρέπουν στους χρήστες να εξάγουν σημαντικές πληροφορίες από τις πηγές δεδομένων τους. Υποστηρίζει διάφορες γλώσσες ερωτημάτων και προσφέρει έναν φιλικό προς το χρήστη επεξεργαστή ερωτημάτων.
3. **Visualization:** Η Grafana υπερέχει στη δημιουργία οπτικά ελκυστικών και κατατοπιστικών ταμπλό. Οι χρήστες μπορούν να επιλέξουν από πολυάριθμες επιλογές οπτικοποίησης, όπως γραμμικά γραφήματα, ραβδογράμματα, heatmaps και μετρητές. Οι προσαρμοσμένοι πίνακες και τα πρόσθετα επεκτείνουν περαιτέρω τις δυνατότητες οπτικοποίησής του.

4. **Alerting:** Η Grafana περιλαμβάνει ισχυρές λειτουργίες ειδοποίησης. Οι χρήστες μπορούν να ορίσουν κανόνες ειδοποιήσεων με βάση συνθήκες μέτρησης και να ρυθμίσουν ειδοποιήσεις μέσω email, Slack, PagerDuty και άλλων καναλιών. Αυτό συμβάλλει στη διασφάλιση έγκαιρης ανταπόκρισης σε κρίσιμα συμβάντα.
5. **Templating:** Η Grafana υποστηρίζει την πρότυπη σχεδίαση ταμπλό, επιτρέποντας στους χρήστες να δημιουργούν επαναχρησιμοποιήσιμα και δυναμικά ταμπλό που μπορούν να προσαρμόζονται σε διαφορετικές μεταβλητές και συνθήκες.
6. **Plugins:** Η αρχιτεκτονική των πρόσθετων της Grafana επιτρέπει στους χρήστες να επεκτείνουν τη λειτουργικότητά της. Διατίθενται πρόσθετα για πρόσθετες πηγές δεδομένων, πάνελ απεικόνισης και ενσωματώσεις εφαρμογών.

Εγκατάσταση και ρύθμιση Grafana:

1. **Λήψη και εγκατάσταση του Grafana**: Το Grafana μπορεί να εγκατασταθεί σε διάφορα λειτουργικά συστήματα (Linux, Windows, macOS) ή να εκτελεστεί ως Docker container. Για παράδειγμα, για να εγκατασταθεί το Grafana σε ένα σύστημα Linux βασισμένο στο Debian εκτελείται η σειρά εντολών:

   sudo apt-get install -y apt-transport-https

   sudo apt-get install -y software-properties-common wget

   wget -q -O - https://packages.grafana.com/gpg.key | sudo apt-key add -

   sudo add-apt-repository "deb https://packages.grafana.com/oss/deb stable main"

   sudo apt-get update

   sudo apt-get install grafana

   sudo systemctl start grafana-server

   sudo systemctl enable grafana-server

2. **Πρόσβαση στο Grafana:** Μετά την εγκατάσταση, η διαδικτυακή διεπαφή του

Grafana είναι προσβάσιμη μέσω http://localhost:3000. Τα προεπιλεγμένα στοιχεία σύνδεσης είναι admin τόσο για το όνομα χρήστη όσο και για τον κωδικό πρόσβασης..

3. **Προσθήκη πηγών δεδομένων:** Μεταβαίνουμε στο Configuration > Data Sources και προσθέτουμε τις πηγές δεδομένων που θέλουμε να χρησιμοποιήσουμε. Κάθε τύπος πηγής δεδομένων θα έχει τις δικές του συγκεκριμένες επιλογές διαμόρφωσης.

4. **Δημιουργία Dashboards:** Μεταβαίνουμε στο Create > Dashboard και ξεκινούμε να δημιουργούμε τον πίνακα ελέγχου προσθέτοντας πάνελ. Επιλέγουμε τον κατάλληλο τύπο οπτικοποίησης και διαμορφώνουμε τα ερωτήματα για κάθε πάνελ.

5. **Set Up Alerts:** Διαμορφώνουμε κανόνες ειδοποιήσεων μέσα στους πίνακες ελέγχου μας. Ορίζουμε τις συνθήκες που ενεργοποιούν τις ειδοποιήσεις και καθορίζουμε τα κανάλια ειδοποίησης.

Δοκιμή των δυνατοτήτων του Grafana:

Για να δοκιμαστεί η λειτουργικότητα της Grafana, μπορούμε να προσομοιώσουμε διάφορα σενάρια παρακολούθησης χρησιμοποιώντας δειγματικά δεδομένα ή ενσωματώνοντας με υπάρχοντα συστήματα. Ακολουθούν ορισμένες κοινές περιπτώσεις χρήσης και πώς μπορεί να χρησιμοποιηθεί η Grafana:

1. Παρακολούθηση συστήματος:

Μετρικές: Χρήση CPU, κατανάλωση μνήμης, εισόδου/εξόδου δίσκου, απόδοση δικτύου. Οπτικοποίηση: Γραμμικά γραφήματα που δείχνουν σε πραγματικό χρόνο τη χρήση της CPU και της μνήμης, κυκλικά διαγράμματα για την κατανομή της χρήσης του δίσκου. Ειδοποιήσεις: Ειδοποιήσεις για υψηλή χρήση CPU (π.χ. πάνω από 90% για περισσότερα από 5 λεπτά), χαμηλή διαθεσιμότητα μνήμης.

2. Παρακολούθηση επιδόσεων εφαρμογών:

Μετρικές: Χρόνοι απόκρισης, ποσοστά αιτήσεων, ποσοστά σφαλμάτων.

Οπτικοποίηση: Heatmaps για τους χρόνους απόκρισης, ραβδογράμματα για τα ποσοστά αιτήσεων.
Ειδοποιήσεις: Ειδοποιήσεις για αυξημένα ποσοστά σφαλμάτων (π.χ. περισσότερα από 5% σφάλματα τα τελευταία 10 λεπτά).

3. Παρακολούθηση βάσης δεδομένων:

Μετρικές: Απόδοση ερωτημάτων, αριθμός συνδέσεων, κατάσταση αντιγραφής.
Οπτικοποίηση: Πίνακες για αργές αναζητήσεις, πίνακες μετρητών για μετρήσεις συνδέσεων.
Ειδοποιήσεις: Ειδοποιήσεις για μακράς διάρκειας ερωτήματα (π.χ. ερωτήματα που διαρκούν περισσότερο από 10 δευτερόλεπτα).

4. Παρακολούθηση δικτύου:

Μετρήσεις: Απώλεια πακέτων, καθυστέρηση, χρήση εύρους ζώνης.
Οπτικοποίηση: Γραμμικά γραφήματα για τις τάσεις της καθυστέρησης, πίνακες μεμονωμένων στατιστικών στοιχείων για την τρέχουσα χρήση εύρους ζώνης.
Ειδοποιήσεις: Ειδοποιήσεις για υψηλή απώλεια πακέτων (π.χ. απώλεια πακέτων άνω του 1% σε διάστημα 5 λεπτών).

5. Ανάλυση αρχείων καταγραφής:

Μετρικές: Μετρήσεις καταγραφής, επίπεδα σφαλμάτων, συγκεκριμένα μοτίβα καταγραφής.
Οπτικοποίηση: Ιστογράμματα για τις καταγραφές, πίνακες κειμένου για τις πρόσφατες καταγραφές.

Ειδοποιήσεις: Ειδοποιήσεις για συγκεκριμένα μοτίβα καταγραφής (π.χ. πολλαπλές καταχωρίσεις σφάλματος σε σύντομο χρονικό διάστημα).

Απόδοση Grafana:

Η Grafana είναι ικανή να χειρίζεται μεγάλο όγκο μετρήσεων και να παρέχει οπτικοποιήσεις και ειδοποιήσεις σε πραγματικό χρόνο. Η απόδοσή της εξαρτάται από την αποδοτικότητα των πηγών δεδομένων, την πολυπλοκότητα των ερωτημάτων και τους διαθέσιμους πόρους υλικού.
Επεκτασιμότητα: Η Grafana μπορεί να κλιμακωθεί οριζόντια με την προσθήκη περισσότερων

περιπτώσεων πίσω από έναν εξισορροπιστή φορτίου, εξασφαλίζοντας ότι μπορεί να χειριστεί αυξανόμενα φορτία.

Ευελιξία: Με την υποστήριξη πολυάριθμων πηγών δεδομένων και επιλογών οπτικοποίησης, η Grafana μπορεί να προσαρμοστεί ώστε να καλύπτει διάφορες ανάγκες παρακολούθησης.

Κοινότητα και υποστήριξη: Η Grafana διαθέτει ισχυρή κοινότητα και εμπορικές επιλογές υποστήριξης, παρέχοντας εκτεταμένους πόρους για τη βελτιστοποίηση και την αντιμετώπιση προβλημάτων.
Με την εγκατάσταση του Grafana και τη διαμόρφωσή του με τις κατάλληλες πηγές δεδομένων και οπτικοποιήσεις, μπορείτε να επιτύχετε ολοκληρωμένη παρακολούθηση και παρατηρησιμότητα για τα συστήματα, τις εφαρμογές και τις υποδομές σας.

Βήμα 2: Ρύθμιση δικτύου

Διαμόρφωση δικτύου:Για την αποτελεσματική παρακολούθηση και τον εντοπισμό επιθέσεων που βασίζονται στο δίκτυο, είναι ζωτικής σημασίας να διασφαλιστεί ότι όλες οι συσκευές που εμπλέκονται στη ρύθμιση βρίσκονται στο ίδιο τοπικό δίκτυο. Αυτή η διαμόρφωση επιτρέπει την απρόσκοπτη επικοινωνία μεταξύ των συσκευών, επιτρέποντας στο σύστημα IDS/IPS να ανιχνεύει και να αναλύει με ακρίβεια την κυκλοφορία του δικτύου.

Επεξήγηση: Πρέπει να ρυθμιστεί το δίκτυό έτσι ώστε όλες οι συσκευές, συμπεριλαμβανομένου του Raspberry Pi που εκτελεί το Snort, του μηχανήματος-στόχου και του μηχανήματος του επιτιθέμενου, να βρίσκονται στο ίδιο τοπικό δίκτυο. Αυτό μπορεί να επιτευχθεί με τη σύνδεσή τους στον ίδιο δρομολογητή ή μεταγωγέα. Αυτή η ρύθμιση εξασφαλίζει ότι όλες οι συσκευές μπορούν να επικοινωνούν μεταξύ τους και ότι η κυκλοφορία του δικτύου μπορεί να παρακολουθείται κεντρικά από το Snort.

1. Εκχωρούνται στατικές IP ή χρησιμοποιείται DHCP για να διασφαλίστεί ότι όλες οι συσκευές βρίσκονται στο ίδιο υποδίκτυο.
Επεξήγηση: Έτσι διασφαλίζεται ότι όλες οι συσκευές μπορούν να επικοινωνούν μεταξύ τους. Μπορούμε να διαμορφώσουμε στατικές IP στις ρυθμίσεις δικτύου κάθε συσκευής ή να αφήσουμε το δρομολογητή να εκχωρήσει IP χρησιμοποιώντας DHCP.

Οι διευθύνσεις IP (Internet Protocol) είναι μοναδικά αναγνωριστικά που εκχωρούνται σε κάθε συσκευή σε ένα δίκτυο, επιτρέποντάς τους να επικοινωνούν μεταξύ τους. Υπάρχουν δύο κύριες μέθοδοι για την εκχώρηση διευθύνσεων IP: στατική εκχώρηση IP και Δυναμικό πρωτόκολλο διαμόρφωσης κεντρικού υπολογιστή (DHCP).

Στατική εκχώρηση IP: Περιλαμβάνει τη χειροκίνητη διαμόρφωση κάθε συσκευής με μια συγκεκριμένη διεύθυνση IP. Οι στατικές IP είναι συνεπείς και δεν αλλάζουν με την πάροδο του χρόνου, γεγονός που τις καθιστά ιδανικές για διακομιστές και συσκευές δικτύου που απαιτούν σταθερή διεύθυνση IP.

DHCP (Dynamic Host Configuration Protocol): Το DHCP είναι ένα πρωτόκολλο διαχείρισης δικτύου που χρησιμοποιείται για την αυτόματη εκχώρηση διευθύνσεων IP σε συσκευές σε ένα δίκτυο. Όταν μια συσκευή συνδέεται στο δίκτυο, ο διακομιστής DHCP της αναθέτει μια διαθέσιμη διεύθυνση IP από ένα προκαθορισμένο εύρος. Το DHCP απλοποιεί τη διαχείριση του δικτύου μειώνοντας την ανάγκη για χειροκίνητη διαμόρφωση IP.

Η διασφάλιση ότι όλες οι συσκευές βρίσκονται στο ίδιο υποδίκτυο είναι ζωτικής σημασίας. Ένα υποδίκτυο είναι ένα τμήμα ενός δικτύου που μοιράζεται ένα κοινό πρόθεμα διεύθυνσης IP. Οι συσκευές στο ίδιο υποδίκτυο μπορούν να επικοινωνούν απευθείας μεταξύ τους χωρίς να απαιτείται δρομολογητής για την αναμετάδοση της κυκλοφορίας. Η μάσκα υποδικτύου καθορίζει το μέγεθος του υποδικτύου. Για παράδειγμα, μια κοινή μάσκα υποδικτύου για μικρά δίκτυα είναι η 255.255.255.0, η οποία επιτρέπει 254 χρήσιμες διευθύνσεις IP εντός του υποδικτύου.

Βήματα για την Ανάθεση Διευθύνσεων IP:

1. **Χρήση Στατικών IPs**:
    - Σε κάθε συσκευή (**Raspberry Pi, μηχανή-στόχος, μηχανή επιτιθέμενου**), αποκτούμε πρόσβαση στις ρυθμίσεις δικτύου.
    - Ορίζουμε μια μοναδική **στατική διεύθυνση IP** εντός του ίδιου υποδικτύου. Για παράδειγμα:
        - **Raspberry Pi (Snort) & Μηχανή-Στόχος**: 192.168.1.10
        - **Μηχανή Επιτιθέμενου**: 192.168.1.20

- Ορίζουμε τη **μάσκα υποδικτύου** σε **255.255.255.0** (ή άλλη κατάλληλη για το δίκτυο).
- Ορίζουμε την **προεπιλεγμένη πύλη (default gateway)** στη διεύθυνση IP του δρομολογητή (π.χ. **192.168.1.1**).

2. **Χρήση DHCP:**
   - Βεβαιώνεται ότι ο διακομιστής DHCP του δρομολογητή είναι ενεργοποιημένος.
   - Συνδέεται κάθε συσκευή στο δίκτυο και ρυθμίστε τις ώστε να λαμβάνουν αυτόματα (μέσω DHCP) μια διεύθυνση IP.
   - Ελέγχεται η διεπαφή διαχείρισης του δρομολογητή ή χρησιμοποιούνται εργαλεία γραμμής εντολών (π.χ. `ifconfig` στο Linux, `ipconfig` στα Windows) για να επαληθευθούν οι εκχωρημένες διευθύνσεις IP. Βεβαιώνεται ότι σε όλες τις συσκευές έχουν εκχωρηθεί διευθύνσεις εντός του ίδιου υποδικτύου.

Διαδικασία λεπτομερούς ρύθμισης δικτύου:

Φυσική ρύθμιση:

1. Σύνδεση συσκευών στο δίκτυο:

- Βεβαιώνεται ότι όλες οι συσκευές (Raspberry Pi, μηχανή στόχος, μηχανή επιτιθέμενου) είναι φυσικά συνδεδεμένες στο ίδιο δίκτυο. Αυτό μπορεί να γίνει μέσω καλωδίων Ethernet συνδεδεμένων σε έναν κοινό μεταγωγέα ή δρομολογητή ή μέσω Wi-Fi αν χρησιμοποιείται ασύρματο δίκτυο.

- Βεβαιώνεται ότι ο δρομολογητής ή ο διακόπτης είναι ενεργοποιημένος και σωστά ρυθμισμένος για την υποστήριξη του δικτύου μας.

Ρύθμιση IP διευθύνσεων:

1. Raspberry Pi (με εγκατάσταση Snort):

- Αποκτούμε πρόσβαση στις ρυθμίσεις δικτύου στο Raspberry Pi.

- Επεξεργαζόμαστε το αρχείο διαμόρφωσης δικτύου (π.χ. /etc/dhcpcd.conf ή /etc/network/interfaces):

interface eth0
static ip_address=192.168.1.10/24
static routers=192.168.1.1
static domain_name_servers=192.168.1.1

- Επανεκκίνηση του network interface:

sudo service dhcpcd restart

2. Μηχάνημα επιτιθέμενου (Kali Linux):

- Αποκτούμε πρόσβαση στις ρυθμίσεις δικτύου στο μηχάνημα επιτιθέμενου.
- Ρυθμίζουμε στατική IP address:

sudo nano /etc/network/interfaces

Προστίθενται οι ακόλουθες γραμμές:

auto eth0
iface eth0 inet static
address 192.168.1.20
netmask 255.255.255.0
gateway 192.168.1.1

Επανεκκίνηση του network interface::

sudo ifdown eth0 && sudo ifup eth0

3. Επιβεβαίωση:

Χρησιμοποιούμε την εντολή ping από κάθε συσκευή για να βεβαιωθούμε ότι τα συστήματα μπορούν να επικοινωνούν μεταξύ τους:

ping 192.168.1.10 # From the target machine or attacker machine to Raspberry Pi
ping 192.168.1.20 # From Raspberry Pi or target machine to attacker machine

Διασφαλίζοντας ότι όλες οι συσκευές βρίσκονται στο ίδιο υποδίκτυο και έχουν ρυθμιστεί σωστά με στατικές διευθύνσεις IP ή μέσω DHCP, δημιουργείται ένα συνεκτικό περιβάλλον δικτύου όπου το Snort μπορεί να παρακολουθεί την κυκλοφορία και να ανιχνεύει πιθανές επιθέσεις. Αυτή η ρύθμιση θέτει τα θεμέλια για την αποτελεσματική παρακολούθηση και δοκιμή της ασφάλειας του δικτύου.

6.3 Χρήση Kali Linux για διεξαγωγή επιθέσεων σε ένα Ubuntu VM που φιλοξενεί Snort IDS/IPS.

UDP Flood Attack

Η επίθεση πλημμύρας UDP (User Datagram Protocol) είναι ένας τύπος επίθεσης άρνησης παροχής υπηρεσιών (DoS) που αποσκοπεί στην υπερφόρτωση των πόρων δικτύου ενός στόχου με τον κατακλυσμό του με μεγάλο αριθμό πακέτων UDP. Το UDP είναι ένα από τα βασικά πρωτόκολλα της σουίτας Internet Protocol (IP), το οποίο χαρακτηρίζεται από τη φύση του χωρίς σύνδεση και την έλλειψη μηχανισμών ελέγχου σφαλμάτων, γεγονός που το καθιστά αποτελεσματικό για εφαρμογές όπου η ταχύτητα είναι ζωτικής σημασίας και η αξιοπιστία δευτερεύουσα.

Μηχανισμός της επίθεσης πλημμύρας UDP:

1. Αποστολή μεγάλου όγκου πακέτων UDP: Σε μια επίθεση πλημμύρας UDP, ο επιτιθέμενος στέλνει έναν τεράστιο αριθμό πακέτων UDP σε τυχαίες ή συγκεκριμένες θύρες στο μηχάνημα-στόχο. Αυτά τα πακέτα συνήθως αποστέλλονται με υψηλό ρυθμό για να μεγιστοποιηθεί ο αντίκτυπος της επίθεσης.

2. Έλλειψη διαδικασίας χειραψίας: Σε αντίθεση με το TCP (Πρωτόκολλο ελέγχου

μετάδοσης), το UDP δεν απαιτεί διαδικασία χειραψίας για τη δημιουργία σύνδεσης. Αυτό σημαίνει ότι τα πακέτα UDP μπορούν να αποστέλλονται ταχύτατα χωρίς την ανάγκη δημιουργίας σύνδεσης, καθιστώντας ευκολότερο για τους επιτιθέμενους να κατακλύσουν τον στόχο με μεγάλο όγκο πακέτων.

3. Μηχανισμός αντίδρασης του στόχου: Όταν το μηχάνημα-στόχος λαμβάνει αυτά τα πακέτα UDP, συνήθως ελέγχει αν κάποια εφαρμογή ακούει στις καθορισμένες θύρες. Εάν καμία εφαρμογή δεν ακούει, το σύστημα-στόχος απαντά με ένα πακέτο ICMP (Internet Control Message Protocol), συγκεκριμένα με ένα μήνυμα "Destination Unreachable" (Μη προσβάσιμος προορισμός). Αυτός ο μηχανισμός απάντησης επιβαρύνει περαιτέρω τους πόρους του στόχου.

4. Υπερφόρτωση πόρων: Η συνεχής ροή πακέτων UDP και η επακόλουθη δημιουργία απαντήσεων ICMP μπορεί να υπερφορτώσει τη στοίβα δικτύου του στόχου. Αυτό οδηγεί σε εξάντληση του εύρους ζώνης δικτύου, αυξημένη χρήση της CPU και εξάντληση των πόρων μνήμης, με αποτέλεσμα να καθυστερεί ή να απορρίπτεται η νόμιμη κυκλοφορία δικτύου. Σε σοβαρές περιπτώσεις, το σύστημα-στόχος μπορεί να μην ανταποκρίνεται καθόλου.

Επιπτώσεις της επίθεσης πλημμύρας UDP

1. Συμφόρηση δικτύου: Η εισροή πακέτων UDP μπορεί να φέρει σε κορεσμό το εύρος ζώνης του δικτύου του στόχου, προκαλώντας σημαντική συμφόρηση. Αυτή η συμφόρηση επηρεάζει όχι μόνο τον στόχο αλλά και άλλες συσκευές στο ίδιο δίκτυο, οδηγώντας σε εκτεταμένη υποβάθμιση του δικτύου.

2. Αυξημένη καθυστέρηση και απώλεια πακέτων: Το υπερβολικό φορτίο στη στοίβα δικτύου αυξάνει την καθυστέρηση, καθιστώντας τις νόμιμες επικοινωνίες δικτύου αργές και αναξιόπιστες. Η απώλεια πακέτων εμφανίζεται καθώς το σύστημα-στόχος αγωνίζεται να διαχειριστεί τον υπερβολικό αριθμό εισερχόμενων πακέτων.

3. Διακοπή υπηρεσιών: Καταναλώνοντας κρίσιμους πόρους του συστήματος, μια επίθεση πλημμύρας UDP μπορεί να διαταράξει τις υπηρεσίες που εκτελούνται στο μηχάνημα-στόχο. Εφαρμογές που βασίζονται στη συνδεσιμότητα δικτύου ενδέχεται να μην είναι διαθέσιμες, με αποτέλεσμα τη διακοπή λειτουργίας και την απώλεια παραγωγικότητας.

4. Καταρρεύσεις του συστήματος: Σε ακραίες περιπτώσεις, η συνεχής καταπόνηση των πόρων του στόχου μπορεί να οδηγήσει σε κατάρρευση του συστήματος. Το μηχάνημα-στόχος μπορεί να παγώσει, να επανεκκινήσει ή να περιέλθει σε κατάσταση αποτυχίας, απαιτώντας χειροκίνητη παρέμβαση για την αποκατάσταση της κανονικής λειτουργίας.

Στρατηγικές μετριασμού:

1. Περιορισμός ποσοστού: Η εφαρμογή περιορισμού του ρυθμού στις συσκευές δικτύου μπορεί να συμβάλει στον μετριασμό των επιπτώσεων μιας επίθεσης πλημμύρας UDP, ελέγχοντας τον ρυθμό με τον οποίο γίνονται αποδεκτά και επεξεργάζονται τα πακέτα UDP.

2. Φιλτράρισμα κυκλοφορίας: Η χρήση τειχών προστασίας και συστημάτων ανίχνευσης/πρόληψης εισβολών (IDS/IPS) όπως το Snort μπορεί να φιλτράρει την κακόβουλη κυκλοφορία UDP με βάση προκαθορισμένους κανόνες και μοτίβα, μειώνοντας την αποτελεσματικότητα της επίθεσης.

3. Τμηματοποίηση δικτύου: Η τμηματοποίηση του δικτύου μπορεί να απομονώσει τα κρίσιμα συστήματα από το υπόλοιπο δίκτυο, περιορίζοντας το εύρος της επίθεσης και προστατεύοντας τις βασικές υπηρεσίες από την υπερφόρτωση.

Βήματα:

1. Άνοιγμα του τερματικού στο Kali Linux:

2. Εγκατάσταση του hping3 αν δεν είναι ήδη εγκατεστημένο:

```
sudo apt update
sudo apt install hping3
```

3. Εκτέλεση της UDP Flood επίθεσης:

```
sudo hping3 --flood --rand-source --udp -p 80 <target_IP>
```

- --flood: Στέλνει πακέτα όσο το δυνατόν γρηγορότερα, χωρίς να περιμένει απαντήσεις.
- --rand-source: Παραποιεί τυχαίες διευθύνσεις IP πηγής.
- --udp: Καθορίζει τη χρήση του πρωτοκόλλου UDP.
- -p 80: Στοχεύει τη θύρα 80.
- <target_IP>: Αντικαθίσταται με τη διεύθυνση IP της μηχανής-στόχου.

SYN Flood Attack

Η επίθεση SYN flood είναι ένας τύπος επίθεσης άρνησης παροχής υπηρεσιών (DoS) που εκμεταλλεύεται τον μηχανισμό δημιουργίας σύνδεσης TCP (Transmission Control Protocol) για να κατακλύσει ένα σύστημα-στόχο. Αυτή η επίθεση αξιοποιεί τη διαδικασία χειραψίας τριών κατευθύνσεων που χρησιμοποιεί το TCP για την εγκαθίδρυση μιας σύνδεσης, αναγκάζοντας τον στόχο να διαθέσει πόρους για μισάνοιχτες συνδέσεις που δεν ολοκληρώνονται ποτέ, εξαντλώντας τελικά τους διαθέσιμους πόρους του και καθιστώντας τις υπηρεσίες μη διαθέσιμες.

Μηχανισμός επίθεσης SYN Flood:

Διαδικασία τριπλής χειραψίας: Για να κατανοήσουμε μια επίθεση πλημμύρας SYN, είναι απαραίτητο να κατανοήσουμε τη διαδικασία χειραψίας τριών κατευθύνσεων του TCP, η οποία περιλαμβάνει τρία βήματα:

- SYN: Ο πελάτης στέλνει ένα πακέτο SYN (συγχρονισμού) στον διακομιστή για να ξεκινήσει μια σύνδεση.
- SYN-ACK: Ο διακομιστής απαντά με ένα πακέτο SYN-ACK (synchronize-acknowledge) για να επιβεβαιώσει το αίτημα σύνδεσης.
- ACK: Ο πελάτης στέλνει ένα πακέτο ACK (επιβεβαίωση) πίσω στον διακομιστή, ολοκληρώνοντας τη χειραψία και εγκαθιδρύοντας τη σύνδεση.

Αποστολή μεγάλου αριθμού πακέτων SYN: Σε μια επίθεση πλημμύρας SYN, ο επιτιθέμενος στέλνει τεράστιο αριθμό πακέτων SYN στη θύρα TCP του στόχου. Αυτά τα πακέτα έχουν συνήθως παραποιημένες διευθύνσεις IP, καθιστώντας δύσκολο για τον στόχο να εντοπίσει την πηγή της επίθεσης.

Κατανομή πόρων από τον στόχο: Μετά τη λήψη των πακέτων SYN, το σύστημα-στόχος απαντά με πακέτα SYN-ACK και κατανέμει πόρους για να χειριστεί τις αναμενόμενες εισερχόμενες συνδέσεις. Αυτοί οι πόροι περιλαμβάνουν μνήμη και θέσεις σύνδεσης στον πίνακα συνδέσεων TCP.

Ημι-ανοικτές συνδέσεις: Ο επιτιθέμενος δεν ολοκληρώνει τη χειραψία με την αποστολή του τελικού πακέτου ACK. Κατά συνέπεια, το σύστημα-στόχος διατηρεί τις υποδοχές σύνδεσης ανοιχτές, περιμένοντας το πακέτο ACK που δεν φτάνει ποτέ. Αυτές οι συνδέσεις αναφέρονται ως μισάνοιχτες συνδέσεις.

Εξάντληση πόρων: Καθώς ο πίνακας συνδέσεων TCP του συστήματος-στόχου γεμίζει με αυτές τις μισάνοιχτες συνδέσεις, φτάνει στη μέγιστη χωρητικότητά του. Αυτό εμποδίζει την επεξεργασία κανονικών προσπαθειών σύνδεσης, καθώς το σύστημα δεν μπορεί πλέον να διαθέσει πόρους για νέες συνδέσεις.

Επιπτώσεις μιας επίθεσης πλημμύρας SYN:

1. Συμφόρηση του δικτύου: Ο μεγάλος όγκος πακέτων SYN μπορεί να προκαλέσει συμφόρηση στο δίκτυο του στόχου, προκαλώντας καθυστερήσεις και διακοπές στην επικοινωνία του δικτύου για τους νόμιμους χρήστες.

2. Αυξημένη καθυστέρηση και αποτυχίες σύνδεσης: Η αδυναμία του συστήματος-στόχου να χειριστεί νέα αιτήματα σύνδεσης έχει ως αποτέλεσμα αυξημένη καθυστέρηση και συχνές αποτυχίες σύνδεσης για τους νόμιμους χρήστες, υποβαθμίζοντας σημαντικά την ποιότητα των υπηρεσιών.

3. Μη διαθεσιμότητα υπηρεσιών: Η εξάντληση των πόρων του πίνακα συνδέσεων TCP του στόχου μπορεί να οδηγήσει σε πλήρη μη διαθεσιμότητα των υπηρεσιών που φιλοξενούνται στο σύστημα-στόχο. Αυτό περιλαμβάνει διακομιστές ιστού, διακομιστές ηλεκτρονικού ταχυδρομείου και άλλες υπηρεσίες που βασίζονται στο TCP.

4. Καταρρεύσεις του συστήματος: Σε σοβαρές περιπτώσεις, η συνεχής καταπόνηση των πόρων του στόχου μπορεί να προκαλέσει μη ανταπόκριση ή κατάρρευση του συστήματος, με

αποτέλεσμα να απαιτείται επανεκκίνηση ή χειροκίνητη παρέμβαση για την αποκατάσταση της κανονικής λειτουργίας.

Στρατηγικές μετριασμού:

1. SYN Cookies: Η εφαρμογή των SYN cookies είναι μια αποτελεσματική τεχνική για τον μετριασμό των επιθέσεων πλημμύρας SYN. Τα SYN cookies είναι μια μέθοδος χειρισμού των αιτήσεων SYN χωρίς να κατανέμονται πόροι μέχρι να ολοκληρωθεί η χειραψία. Αυτό αποτρέπει το γέμισμα του πίνακα συνδέσεων με μισάνοιχτες συνδέσεις.

2. Περιορισμός ρυθμού: Η εφαρμογή περιορισμού ρυθμού στα πακέτα SYN βοηθά στον έλεγχο του ρυθμού με τον οποίο γίνονται δεκτά και επεξεργάζονται τα πακέτα SYN, μειώνοντας την πιθανότητα εξάντλησης των πόρων.

3. Τείχη προστασίας και συστήματα ανίχνευσης/πρόληψης εισβολών (IDS/IPS): Η διαμόρφωση τειχών προστασίας και IDS/IPS όπως το Snort για την ανίχνευση και τον αποκλεισμό ύποπτης κυκλοφορίας SYN μπορεί να μετριάσει τις επιπτώσεις των επιθέσεων SYN flood. Αυτά τα συστήματα μπορούν να φιλτράρουν την κακόβουλη κυκλοφορία με βάση προκαθορισμένους κανόνες και μοτίβα.

4. Ρύθμιση χρονικού ορίου: Η μείωση της περιόδου χρονικού ορίου για τις μισάνοιχτες συνδέσεις μπορεί να βοηθήσει στην ταχύτερη απελευθέρωση πόρων, αποτρέποντας τη συμπλήρωση του πίνακα συνδέσεων TCP.

5. Παρακολούθηση δικτύου και ειδοποιήσεις: Η συνεχής παρακολούθηση της κυκλοφορίας δικτύου και η ρύθμιση ειδοποιήσεων για μη φυσιολογικά μοτίβα μπορεί να βοηθήσει στην έγκαιρη ανίχνευση επιθέσεων SYN flood, επιτρέποντας την άμεση αντίδραση και τον μετριασμό.

Βήματα:

1. Άνοιγμα του τερματικού στο Kali Linux:

2. Εγκατάσταση του hping3 αν δεν είναι ήδη εγκατεστημένο:

```
sudo apt update
sudo apt install hping3
```

3. Εκτέλεση της SYN Flood επίθεσης:

```
sudo hping3 --flood --rand-source -S -p 80 <target_IP>
```

- --flood: Στέλνει πακέτα όσο το δυνατόν γρηγορότερα, χωρίς να περιμένει απαντήσεις.
- --rand-source: Παραποιεί τυχαίες διευθύνσεις IP πηγής.
- -S: Στέλνει SYN πακέτα (χρησιμοποιείται για επιθέσεις SYN flood).
- -p 80: Στοχεύει τη θύρα 80 (HTTP).
- <target_IP>: Αντικαθίσταται με τη διεύθυνση IP της μηχανής-στόχου.

ARP Spoofing

Το ARP spoofing, επίσης γνωστό ως ARP poisoning, είναι ένας τύπος επίθεσης στον κυβερνοχώρο κατά τον οποίο ο επιτιθέμενος στέλνει πλαστά μηνύματα ARP (Address Resolution Protocol) μέσω ενός τοπικού δικτύου. Στόχος αυτής της επίθεσης είναι να συσχετίσει τη διεύθυνση MAC (Media Access Control) του επιτιθέμενου με τη διεύθυνση IP (Internet Protocol) ενός νόμιμου κεντρικού υπολογιστή, όπως η πύλη δικτύου, υποκλέπτοντας ή αλλοιώνοντας έτσι την κυκλοφορία του δικτύου. Μηχανισμός της επίθεσης ARP Spoofing

1. Κατανόηση του ARP: Το ARP είναι ένα πρωτόκολλο που χρησιμοποιείται για την αντιστοίχιση διευθύνσεων IP σε διευθύνσεις MAC, επιτρέποντας στις συσκευές ενός τοπικού δικτύου να επικοινωνούν μεταξύ τους. Όταν μια συσκευή θέλει να επικοινωνήσει με μια άλλη συσκευή, εκπέμπει ένα αίτημα ARP ζητώντας τη διεύθυνση MAC που σχετίζεται με τη διεύθυνση IP του στόχου. Η συσκευή με αυτή τη διεύθυνση IP απαντά με τη διεύθυνση MAC της.

2. Αποστολή ψεύτικων μηνυμάτων ARP: Σε μια επίθεση ARP spoofing, ο επιτιθέμενος στέλνει ψεύτικα μηνύματα ARP στο δίκτυο. Αυτά τα μηνύματα συσχετίζουν τη διεύθυνση MAC του επιτιθέμενου με τη διεύθυνση IP μιας νόμιμης συσκευής, όπως η πύλη ή ένας άλλος κεντρικός υπολογιστής στο δίκτυο.

3. Υποκλοπή της κίνησης δικτύου: Ως αποτέλεσμα των πλαστών μηνυμάτων ARP, άλλες συσκευές στο δίκτυο ενημερώνουν τους πίνακές τους ARP με την εσφαλμένη αντιστοίχιση. Κατά συνέπεια, η κυκλοφορία δικτύου που προοριζόταν για τη νόμιμη συσκευή αποστέλλεται αντ' αυτού στον επιτιθέμενο. Ο επιτιθέμενος μπορεί στη συνέχεια να υποκλέψει, να τροποποιήσει ή να ανακατευθύνει αυτή την κυκλοφορία.

4. Διατήρηση της απομίμησης: Για να διατηρήσει την παραποίηση ARP, ο επιτιθέμενος στέλνει συνεχώς ψεύτικες απαντήσεις ARP για να διασφαλίσει ότι οι πίνακες ARP των συσκευών του δικτύου παραμένουν δηλητηριασμένοι με την εσφαλμένη αντιστοίχιση MAC-IP.

Επιπτώσεις της επίθεσης ARP Spoofing:

1. Υποκλοπή ευαίσθητων πληροφοριών: Με την υποκλοπή της κίνησης δικτύου, ο επιτιθέμενος μπορεί να συλλάβει ευαίσθητες πληροφορίες, όπως διαπιστευτήρια σύνδεσης, προσωπικά δεδομένα και εμπιστευτικές επικοινωνίες. Αυτό μπορεί να οδηγήσει σε παραβιάσεις δεδομένων και μη εξουσιοδοτημένη πρόσβαση σε πόρους δικτύου.

2. Παραβίαση συνόδου: Ο επιτιθέμενος μπορεί να καταλάβει ενεργές συνεδρίες, καταλαμβάνοντας λογαριασμούς χρηστών ή αποκτώντας πρόσβαση σε περιορισμένους πόρους χωρίς εξουσιοδότηση. Αυτό είναι ιδιαίτερα επικίνδυνο για τις οικονομικές συναλλαγές και άλλες κρίσιμες λειτουργίες

3. Επιθέσεις Man-in-the-Middle: όπου ο επιτιθέμενος μπορεί να υποκλέψει και ενδεχομένως να αλλάξει την επικοινωνία μεταξύ δύο μερών εν αγνοία τους. Αυτό επιτρέπει την υποκλοπή, τη χειραγώγηση δεδομένων και την εισαγωγή κακόβουλου περιεχομένου.

4. Άρνηση παροχής υπηρεσιών (DoS): Ο επιτιθέμενος μπορεί να διαταράξει την επικοινωνία

του δικτύου αλλοιώνοντας τους πίνακες ARP, προκαλώντας την αδυναμία επικοινωνίας των νόμιμων συσκευών μεταξύ τους. Αυτό μπορεί να οδηγήσει σε διακοπή λειτουργίας του δικτύου και απώλεια παραγωγικότητας.

5. Σάρωση και αναγνώριση δικτύου: Το ARP spoofing μπορεί επίσης να χρησιμοποιηθεί για τη σάρωση του δικτύου και τη συλλογή πληροφοριών σχετικά με τις συνδεδεμένες συσκευές, όπως οι διευθύνσεις IP και οι διευθύνσεις MAC τους. Αυτή η αναγνώριση μπορεί να χρησιμοποιηθεί για τον σχεδιασμό περαιτέρω επιθέσεων.

Στρατηγικές μετριασμού:

1. Στατικές καταχωρίσεις ARP: Η διαμόρφωση στατικών καταχωρίσεων ARP σε κρίσιμες συσκευές, όπως διακομιστές και πύλες δικτύου, αποτρέπει την παραποίηση ARP διασφαλίζοντας ότι οι αντιστοιχίσεις MAC-IP δεν μπορούν να αλλάξουν. Ωστόσο, αυτό δεν είναι επεκτάσιμο για μεγάλα δίκτυα.

2. Επιθεώρηση ARP: Η εφαρμογή της Δυναμικής Επιθεώρησης ARP (DAI) στους μεταγωγείς δικτύου βοηθά στον εντοπισμό και την αποτροπή επιθέσεων ARP spoofing. Η DAI επαληθεύει τα μηνύματα ARP σε σχέση με μια αξιόπιστη βάση δεδομένων προτού τους επιτρέψει να διαδοθούν στο δίκτυο.

3. Κρυπτογράφηση: Η χρήση κρυπτογραφημένων πρωτοκόλλων επικοινωνίας, όπως το HTTPS, το SSH και τα VPN, διασφαλίζει ότι ακόμη και αν ένας επιτιθέμενος υποκλέψει την κυκλοφορία, δεν μπορεί εύκολα να διαβάσει ή να τροποποιήσει το περιεχόμενο.
4. Τμηματοποίηση του δικτύου: Η τμηματοποίηση του δικτύου με τη χρήση VLANs (Virtual Local Area Networks) μπορεί να περιορίσει το πεδίο εφαρμογής μιας επίθεσης ARP spoofing, περιορίζοντάς την σε ένα συγκεκριμένο τμήμα και προστατεύοντας άλλα τμήματα του δικτύου.

5. Συνεχής παρακολούθηση: Η χρήση εργαλείων παρακολούθησης δικτύου για τη συνεχή παρακολούθηση της κυκλοφορίας ARP και τον εντοπισμό ύποπτης δραστηριότητας ARP μπορεί να παρέχει έγκαιρη προειδοποίηση για πιθανές επιθέσεις ARP spoofing, επιτρέποντας την άμεση αντίδραση και τον μετριασμό.

Βήματα:

1. Άνοιγμα του τερματικού Kali Linux:

2. Εγκατάσταση του dsniff αν δεν έχει ήδη εγκατασταθεί:

sudo apt update
sudo apt install dsniff

3. Εκτέλεση της ARP Spoofing επίθεσης:

sudo arpspoof -i <interface> -t <target_IP> <gateway_IP>

- `-i <interface>`: Καθορίζει τη διεπαφή δικτύου (π.χ. `eth0`, `wlan0`).
- `-t <target_IP>`: Η διεύθυνση IP της μηχανής-στόχου.
- `<gateway_IP>`: Η διεύθυνση IP της προεπιλεγμένης πύλης (gateway).

SQL Injection

Η έγχυση SQL είναι ένας τύπος επίθεσης κατά την οποία ένας επιτιθέμενος εισάγει ή "εγχέει" κακόβουλο κώδικα SQL (Structured Query Language) σε ένα πεδίο εισόδου μιας διαδικτυακής εφαρμογής. Αυτός ο κώδικας εκτελείται στη συνέχεια από την back-end βάση δεδομένων, επιτρέποντας δυνητικά στον επιτιθέμενο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων και στα περιεχόμενά της, να χειριστεί δεδομένα ή ακόμη και να αναλάβει τον έλεγχο ολόκληρου του συστήματος βάσεων δεδομένων.

Μηχανισμός της επίθεσης SQL Injection

1. Κατανόηση της SQL και των βάσεων δεδομένων: Η SQL είναι μια γλώσσα που χρησιμοποιείται για την επικοινωνία με βάσεις δεδομένων και τον χειρισμό τους. Οι διαδικτυακές εφαρμογές χρησιμοποιούν συχνά ερωτήματα SQL για την αλληλεπίδραση με μια βάση δεδομένων, για εργασίες όπως η ανάκτηση δεδομένων χρήστη, η αποθήκευση των δεδομένων του χρήστη και η διαχείριση των δεδομένων της εφαρμογής.

2. Εισαγωγή κακόβουλου κώδικα SQL: Σε μια επίθεση έγχυσης SQL, ο επιτιθέμενος εντοπίζει ένα πεδίο εισόδου σε μια εφαρμογή ιστού (όπως μια φόρμα σύνδεσης, ένα πλαίσιο αναζήτησης ή μια παράμετρος URL) που είναι ευάλωτο σε έγχυση SQL. Στη συνέχεια, ο επιτιθέμενος εισάγει ειδικά διαμορφωμένο κώδικα SQL σε αυτό το πεδίο.

3. Εκτέλεση κακόβουλου κώδικα: Η διαδικτυακή εφαρμογή στέλνει τον εισαγόμενο κώδικα SQL στην back-end βάση δεδομένων ως μέρος ενός ερωτήματος. Εάν η είσοδος δεν έχει καθαριστεί ή επικυρωθεί σωστά, η βάση δεδομένων εκτελεί τον εγχυμένο κώδικα μαζί με το προβλεπόμενο ερώτημα.

4. Εκμετάλλευση της βάσης δεδομένων: Με την εκμετάλλευση αυτής της ευπάθειας, ο εισβολέας μπορεί να εκτελέσει διάφορες κακόβουλες ενέργειες, όπως:
   - Ανάκτηση ευαίσθητων δεδομένων: Πρόσβαση σε εμπιστευτικές πληροφορίες, όπως ονόματα χρήστη, κωδικούς πρόσβασης και προσωπικά στοιχεία.
   - Χειραγώγηση δεδομένων: Εισαγωγή, ενημέρωση ή διαγραφή δεδομένων στη βάση δεδομένων.

5. Απόκτηση διαχειριστικής πρόσβασης: Κλιμάκωση προνομίων για την απόκτηση διοικητικού ελέγχου της βάσης δεδομένων.

6. Εκτέλεση απομακρυσμένων εντολών: Εκτέλεση αυθαίρετων εντολών στο διακομιστή βάσης δεδομένων, με πιθανή παραβίαση ολόκληρου του συστήματος.

Επιπτώσεις της επίθεσης SQL Injection:

1. Παραβίαση δεδομένων: Μια επίθεση έγχυσης SQL μπορεί να οδηγήσει σε μη εξουσιοδοτημένη έκθεση ευαίσθητων δεδομένων που είναι αποθηκευμένα στη βάση δεδομένων. Αυτά περιλαμβάνουν προσωπικές πληροφορίες, οικονομικά αρχεία και άλλα εμπιστευτικά δεδομένα, με αποτέλεσμα την παραβίαση δεδομένων και την παραβίαση της ιδιωτικής ζωής.

2. Χειραγώγηση και απώλεια δεδομένων: Οι επιτιθέμενοι μπορούν να τροποποιήσουν ή να διαγράψουν δεδομένα, προκαλώντας προβλήματα ακεραιότητας δεδομένων και πιθανή

απώλεια δεδομένων. Αυτό μπορεί να διαταράξει τις επιχειρηματικές λειτουργίες και να οδηγήσει σε σημαντική οικονομική ζημία και ζημία φήμης.

3. Μη εξουσιοδοτημένη πρόσβαση: Οι επιτιθέμενοι μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς χρηστών και διαχειριστικές λειτουργίες. Αυτό μπορεί να οδηγήσει σε περαιτέρω εκμετάλλευση και κακή χρήση των παραβιασμένων συστημάτων.

4. Παραβίαση συστήματος: Σε ορισμένες περιπτώσεις, η έγχυση SQL μπορεί να χρησιμοποιηθεί για την εκτέλεση εντολών στον υποκείμενο διακομιστή, οδηγώντας σε πλήρη παραβίαση του διακομιστή και άλλων συνδεδεμένων συστημάτων.

5. Οικονομική ζημία και ζημία φήμης: Οι συνέπειες μιας επίθεσης SQL injection μπορεί να οδηγήσουν σε σημαντικές οικονομικές απώλειες λόγω παραβίασης δεδομένων, νομικές ευθύνες και απώλεια της εμπιστοσύνης των πελατών. Η βλάβη της φήμης μπορεί να είναι μακροχρόνια και δύσκολο να ανακάμψει κανείς.

Στρατηγικές μετριασμού:

1. Επικύρωση εισόδου: Η εφαρμογή ισχυρών τεχνικών επικύρωσης εισόδου διασφαλίζει ότι γίνονται δεκτά μόνο σωστά διαμορφωμένα δεδομένα. Αυτό περιλαμβάνει τον έλεγχο της εισόδου σε σχέση με ένα σύνολο κανόνων για να αποτραπεί η επεξεργασία κακόβουλου κώδικα.

2. Παραμετροποιημένα ερωτήματα: Η χρήση παραμετροποιημένων ερωτημάτων (γνωστών και ως prepared statements) συμβάλλει στην αποτροπή της έγχυσης SQL διαχωρίζοντας τον κώδικα SQL από την είσοδο του χρήστη. Αυτό διασφαλίζει ότι η είσοδος του χρήστη αντιμετωπίζεται ως δεδομένα και όχι ως εκτελέσιμος κώδικας.

3. Αποθηκευμένες διαδικασίες: Οι αποθηκευμένες διαδικασίες είναι προμεταγλωττισμένος κώδικας SQL αποθηκευμένος στη βάση δεδομένων. Η χρήση αποθηκευμένων διαδικασιών

μπορεί να μειώσει τον κίνδυνο έγχυσης SQL διασφαλίζοντας ότι οι εντολές SQL εκτελούνται όπως προβλέπεται χωρίς άμεση είσοδο από τους χρήστες.

4. Τείχη προστασίας εφαρμογών ιστού (WAF): Η ανάπτυξη ενός WAF μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό κακόβουλων προσπαθειών έγχυσης SQL. Τα WAF αναλύουν την εισερχόμενη κυκλοφορία και φιλτράρουν τις δυνητικά επιβλαβείς αιτήσεις με βάση προκαθορισμένους κανόνες ασφαλείας.

5. Τακτικοί έλεγχοι ασφαλείας: Η διενέργεια τακτικών ελέγχων ασφαλείας και αναθεωρήσεων κώδικα βοηθά στον εντοπισμό και την αποκατάσταση των ευπαθειών SQL injection στον κώδικα της εφαρμογής. Μπορούν να χρησιμοποιηθούν αυτοματοποιημένα εργαλεία και χειροκίνητες δοκιμές για να διασφαλιστεί η ολοκληρωμένη κάλυψη.

6. Αρχή των ελαχίστων προνομίων: Η εφαρμογή της αρχής των λιγότερων προνομίων διασφαλίζει ότι οι λογαριασμοί βάσεων δεδομένων έχουν μόνο τα ελάχιστα δικαιώματα που απαιτούνται για την εκτέλεση των καθηκόντων τους. Αυτό περιορίζει τη δυνητική ζημιά που μπορεί να προκληθεί σε περίπτωση παραβίασης ενός λογαριασμού.

Steps:

1. Άνοιγμα του τερματικού Kali Linux:

2. Εγκατάσταση του sqlmap αν δεν έχει ήδη εγκατασταθεί:

sudo apt update
sudo apt install sqlmap

3. Αναγνώριση μιας ευπαθούς Web εφαρμογής:

Ας υποθέσουμε ότι υπάρχει μια εφαρμογή web που εκτελείται στην εικονική μηχανή-στόχο (VM) και περιέχει μια ευπάθεια SQL Injection

4. Εκτέλεση της επίθεσης SQL Injection:

sqlmap -u "http://<target_IP>/vulnerablepage?param=value" --dbs

- -u "http://<target_IP>/vulnerablepage?param=value": Η διεύθυνση URL της ευάλωτης εφαρμογής, με μια παράμετρο ερωτήματος (query parameter).
- --dbs: Εμφανίζει τις διαθέσιμες βάσεις δεδομένων.

Port Scanning

Η σάρωση θυρών είναι μια τεχνική που χρησιμοποιείται για τον εντοπισμό ανοικτών θυρών και των υπηρεσιών που εκτελούνται σε αυτές σε ένα σύστημα-στόχο. Με τη διερεύνηση κάθε θύρας, ένας επιτιθέμενος μπορεί να προσδιορίσει ποιες θύρες είναι ανοικτές, κλειστές ή φιλτραρισμένες και να συλλέξει πληροφορίες σχετικά με τις υπηρεσίες που εκτελούνται σε αυτές τις θύρες. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για νόμιμους σκοπούς διαχείρισης δικτύου ή ως προκαταρκτικό βήμα για τον σχεδιασμό μιας επίθεσης στον κυβερνοχώρο.

Μηχανισμός σάρωσης θυρών:

1. Κατανόηση των θυρών: Οι θύρες είναι λογικά τελικά σημεία επικοινωνίας σε δικτυωμένα συστήματα. Κάθε θύρα συνδέεται με μια συγκεκριμένη υπηρεσία ή εφαρμογή. Για παράδειγμα, το HTTP χρησιμοποιεί συνήθως τη θύρα 80 και το HTTPS χρησιμοποιεί τη θύρα 443. Οι θύρες αριθμούνται από το 0 έως το 65535, με τις θύρες 0-1023 να λογίζονται ως γνωστές θύρες.

2. Τύποι Σαρώσεων Θυρών (Port Scans). Διάφοροι τύποι σαρώσεων θυρών μπορούν να χρησιμοποιηθούν για την ανίχνευση ενός συστήματος-στόχου:

- TCP Connect Scan: Δημιουργεί πλήρη σύνδεση με την θύρα-στόχο χρησιμοποιώντας τη διαδικασία TCP three-way handshake (SYN, SYN-ACK, ACK). Αυτή η σάρωση είναι εύκολο να εντοπιστεί, και παρέχει αξιόπιστα αποτελέσματα.
- SYN Scan (Half-Open Scan): Στέλνει SYN πακέτο και περιμένει για SYN-ACK απόκριση, χωρίς να ολοκληρώνει τη χειραψία. Αυτή η μέθοδος είναι πιο διακριτική

από τη TCP Connect Scan.

- UDP Scan: Στέλνει UDP πακέτα σε θύρες-στόχους και περιμένει για απόκριση. Επειδή το UDP δεν περιλαμβάνει διαδικασία χειραψίας, αυτή η σάρωση μπορεί να είναι πιο αργή και λιγότερο αξιόπιστη.
- Xmas Scan: Στέλνει πακέτα με τα FIN, URG και PUSH flags ενεργοποιημένα. Μπορεί να χρησιμοποιηθεί για την ανίχνευση firewalls και συστημάτων φιλτραρίσματος.
- FIN Scan: Στέλνει ένα FIN πακέτο στη θύρα-στόχο. Αν δεν ληφθεί απόκριση, η θύρα θεωρείται ανοιχτή.

3. Ανίχνευση Κατάστασης Θυρών (Probing Ports). Κατά τη διάρκεια μιας σάρωσης θυρών, ο επιτιθέμενος στέλνει πακέτα σε κάθε θύρα του συστήματος-στόχου. Η απόκριση (ή η απουσία της) βοηθά στον προσδιορισμό της κατάστασης της θύρας:

- Ανοιχτή Θύρα (Open Port): Η θύρα δέχεται συνδέσεις και η υπηρεσία που εκτελείται σε αυτήν απαντά στο probe.
- Κλειστή Θύρα (Closed Port): Η θύρα δεν είναι ανοιχτή, και το σύστημα-στόχος στέλνει πακέτο RST (reset) ως απόκριση.
- Φιλτραρισμένη Θύρα (Filtered Port): Η θύρα προστατεύεται από firewall ή φίλτρο, με αποτέλεσμα το probe να μην φτάνει στον στόχο. Αυτό οδηγεί είτε σε καμία απόκριση είτε σε μήνυμα ICMP unreachable.

4. Συλλογή πληροφοριών: Ο επιτιθέμενος μπορεί να συλλέξει πολύτιμες πληροφορίες σχετικά με τις υπηρεσίες που εκτελούνται σε ανοικτές θύρες. Αυτές περιλαμβάνουν τον τύπο της υπηρεσίας, την έκδοση και τις πιθανές ευπάθειες που θα μπορούσαν να αξιοποιηθούν.

Επιπτώσεις της σάρωσης θυρών:

1. Αναγνώριση: Η σάρωση θυρών χρησιμοποιείται συχνά ως τεχνική αναγνώρισης από τους επιτιθέμενους για τη χαρτογράφηση του δικτύου-στόχου. Παρέχει ένα σχέδιο της δομής του δικτύου του στόχου, αποκαλύπτοντας ποιες υπηρεσίες είναι διαθέσιμες και δυνητικά ευάλωτες.

2. Προσδιορισμός ευπαθειών: Εντοπίζοντας τις ανοικτές θύρες και τις υπηρεσίες που εκτελούνται σε αυτές, οι επιτιθέμενοι μπορούν να προσδιορίσουν πιθανά σημεία εισόδου για εκμετάλλευση. Οι γνωστές ευπάθειες σε συγκεκριμένες υπηρεσίες μπορούν να αποτελέσουν στόχο για την απόκτηση μη εξουσιοδοτημένης πρόσβασης ή τη διακοπή των λειτουργιών.

3. Ανίχνευση εισβολών: Ενώ η σάρωση θυρών από μόνη της δεν είναι εγγενώς κακόβουλη, μπορεί να αποτελέσει προάγγελο πιο σοβαρών επιθέσεων. Η ανίχνευση σαρώσεων θυρών μπορεί να παρέχει έγκαιρη προειδοποίηση για μια πιθανή επίθεση, επιτρέποντας στους υπερασπιστές του δικτύου να λάβουν προληπτικά μέτρα.

4. Συμφόρηση δικτύου και επιδόσεις: Η εκτεταμένη σάρωση θυρών μπορεί να δημιουργήσει σημαντικό όγκο δικτυακής κίνησης, οδηγώντας ενδεχομένως σε συμφόρηση και υποβαθμισμένες επιδόσεις για τους νόμιμους χρήστες. Αυτό ισχύει ιδιαίτερα σε μεγάλης κλίμακας ή κατανεμημένες προσπάθειες σάρωσης.

Στρατηγικές μετριασμού:

1. Διαμόρφωση τείχους προστασίας: Η σωστή διαμόρφωση των τειχών προστασίας για τον αποκλεισμό ή το φιλτράρισμα περιττών θυρών μπορεί να μειώσει την επιφάνεια επίθεσης και να περιορίσει την αποτελεσματικότητα των σαρώσεων θυρών. Μόνο οι απαραίτητες θύρες θα πρέπει να είναι ανοιχτές και προσβάσιμες από το εξωτερικό.

2. Συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS): Η ανάπτυξη IDS/IPS όπως το Snort μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό δραστηριοτήτων σάρωσης θυρών. Αυτά τα συστήματα μπορούν να αναλύουν μοτίβα κίνησης δικτύου και να δημιουργούν ειδοποιήσεις όταν ανιχνεύεται ύποπτη συμπεριφορά σάρωσης.

3. Περιορισμός ρυθμού: Η εφαρμογή περιορισμού ρυθμού στις συσκευές δικτύου μπορεί να επιβραδύνει τις προσπάθειες σάρωσης θυρών, καθιστώντας πιο δύσκολο για τους επιτιθέμενους να συλλέξουν γρήγορα πληροφορίες σχετικά με τις ανοικτές θύρες.

4. Honeypots: Η χρήση honeypots (συστήματα δόλωμα) μπορεί να παρασύρει τους επιτιθέμενους μακριά από κρίσιμα συστήματα και να επιτρέψει στους διαχειριστές δικτύου να παρακολουθούν και να αναλύουν τις δραστηριότητες σάρωσης θυρών χωρίς να εκθέτουν πραγματικές υπηρεσίες.

5. Τακτικοί έλεγχοι δικτύου: Η διενέργεια τακτικών ελέγχων δικτύου και αξιολογήσεων τρωτότητας μπορεί να βοηθήσει στον εντοπισμό και το κλείσιμο περιττών ανοικτών θυρών, μειώνοντας τον κίνδυνο εκμετάλλευσης μέσω σάρωσης θυρών.

Steps:

1. Άνοιγμα του τερματικού Kali Linux:

2. Εγκατάσταση του nmap αν δεν είναι ήδη εγκατεστημένο:

sudo apt update

sudo apt install nmap

3. Εκτέλεση Port Scanning:

nmap -sS <target_IP>

- -sS: Εκτελεί TCP SYN Scan (Half-Open Scan).
- <target_IP>: Αντικαθίσταται με τη διεύθυνση IP της μηχανής-στόχου.

7 Συμπεράσματα

Η παρούσα εργασία ασχολήθηκε με τις πολλαπλές πτυχές της κυβερνοασφάλειας, εστιάζοντας ειδικά στην εφαρμογή της στο Διαδίκτυο των Πραγμάτων (IoT) και την αξιοποίηση εργαλείων όπως το Raspberry Pi και το Snort IDS/IPS. Σκοπός της έρευνας ήταν να αναδείξει τις προκλήσεις, τις απειλές, και τις δυνατότητες των σύγχρονων τεχνολογιών ασφάλειας, προκειμένου να προστατευθούν οι ευαίσθητες πληροφορίες και οι κρίσιμες υποδομές. Οι παρακάτω παράγραφοι συνοψίζουν τα κύρια ευρήματα και τα συμπεράσματα που προέκυψαν από αυτήν την έρευνα.

Η ανίχνευση και η πρόληψη των κυβερνοεπιθέσεων αποτελούν κρίσιμες πτυχές της κυβερνοασφάλειας. Η εργασία ανέδειξε τη σημασία των συστημάτων ανίχνευσης και πρόληψης εισβολών (IDS/IPS) όπως το Snort, τα οποία είναι απαραίτητα για την προστασία των δικτύων από κακόβουλες δραστηριότητες. Η εγκατάσταση και παραμετροποίηση του Snort στο Raspberry Pi επιβεβαίωσε την αποδοτικότητα και την ευελιξία αυτών των εργαλείων σε περιβάλλοντα χαμηλού κόστους και περιορισμένων πόρων. Ειδικότερα, η χρήση του Snort IDS/IPS απέδειξε πως είναι δυνατό να αναπτυχθούν ισχυρές άμυνες ακόμη και με οικονομικά προσιτές συσκευές, κάνοντας την κυβερνοασφάλεια πιο προσιτή και αποτελεσματική.

Το IoT, παρά τις τεράστιες δυνατότητες που προσφέρει, εισάγει νέες προκλήσεις στην κυβερνοασφάλεια. Η μεγάλη ποικιλία και ο αριθμός των συνδεδεμένων συσκευών δημιουργούν πολυάριθμα σημεία ευπάθειας. Η έρευνα κατέδειξε την ανάγκη για ισχυρούς μηχανισμούς ασφαλείας, όπως η κρυπτογράφηση των δεδομένων και η αυστηρή ταυτοποίηση και εξουσιοδότηση των συσκευών, προκειμένου να προστατευθούν οι ευαίσθητες πληροφορίες και οι κρίσιμες υποδομές. Επιπλέον, αναδείχθηκε η σημασία της συνεχούς ενημέρωσης και αναβάθμισης των συστημάτων ασφαλείας για την αντιμετώπιση νέων και εξελισσόμενων απειλών.

Η εργασία ανέδειξε επίσης τη σημασία των ελέγχων διείσδυσης και του ethical hacking ως απαραίτητα εργαλεία για την αξιολόγηση και τη βελτίωση της ασφάλειας των συστημάτων. Μέσω της προσομοίωσης επιθέσεων σε ένα περιβάλλον IoT, αποδείχθηκε πως αυτές οι τεχνικές μπορούν να αποκαλύψουν κενά ασφαλείας και να ενισχύσουν τις άμυνες ενός

συστήματος. Η χρήση εργαλείων όπως το Kali Linux για την εκτέλεση των επιθέσεων ενίσχυσε την κατανόηση των πρακτικών πλευρών της ασφάλειας. Συγκεκριμένα, οι δοκιμές διείσδυσης σε ένα δίκτυο IoT έδειξαν την ανάγκη για συνεχείς αξιολογήσεις και προσαρμογές των αμυντικών μηχανισμών.

Η μελέτη περίπτωσης που αφορούσε το Raspberry Pi και την υλοποίηση του Snort IDS/IPS αποτέλεσε έναν θεμελιώδη πυλώνα της παρούσας έρευνας, καταδεικνύοντας την πρακτική εφαρμοσιμότητα αυτών των τεχνολογιών σε ένα πραγματικό περιβάλλον. Αρχικά, η επιλογή του Raspberry Pi ως πλατφόρμας βασίστηκε στο χαμηλό κόστος και στην ευελιξία του, χαρακτηριστικά που το καθιστούν ιδανικό για δοκιμαστικές εφαρμογές κυβερνοασφάλειας. Η επιτυχής εγκατάσταση και παραμετροποίηση του Snort IDS/IPS στο Raspberry Pi ανέδειξε τη δυνατότητα χρήσης προσιτών οικονομικά συσκευών για την ανάπτυξη ισχυρών συστημάτων ανίχνευσης και πρόληψης εισβολών.

Η διαδικασία περιλάμβανε την εγκατάσταση του Snort, την οποία ακολούθησε η διαμόρφωση κανόνων ανίχνευσης που σχεδιάστηκαν για να εντοπίζουν συγκεκριμένες επιθέσεις, όπως επιθέσεις DDoS, SQL injection, και ARP spoofing. Η χρήση του Snort σε συνδυασμό με το Raspberry Pi αποδείχθηκε ιδιαίτερα αποτελεσματική, καθώς οι επιθέσεις ανιχνεύθηκαν με ακρίβεια και τα δεδομένα των ανιχνεύσεων αναλύθηκαν σε πραγματικό χρόνο.

Επιπλέον, η ενσωμάτωση του Grafana για την παρακολούθηση των επιθέσεων παρείχε μια διαισθητική και οπτική αναπαράσταση των δεδομένων ασφαλείας. Το Grafana επέτρεψε τη δημιουργία διαδραστικών πινάκων και γραφημάτων, διευκολύνοντας έτσι την ανάλυση των ανιχνευόμενων δραστηριοτήτων και την αξιολόγηση της απόδοσης του συστήματος ασφαλείας. Η χρήση τέτοιων εργαλείων αναδεικνύει τη σημασία της οπτικοποίησης των δεδομένων στην αποτελεσματική διαχείριση της ασφάλειας των δικτύων.

Μέσα από τη μελέτη αυτή, αποδείχθηκε ότι είναι εφικτό να αναπτυχθούν αποδοτικά συστήματα ανίχνευσης και πρόληψης εισβολών ακόμα και με περιορισμένους πόρους. Τα ευρήματα της πρακτικής εφαρμογής έδειξαν ότι το Raspberry Pi, παρά τις περιορισμένες δυνατότητες του σε σχέση με πιο εξειδικευμένο εξοπλισμό, μπορεί να υποστηρίξει αποτελεσματικά την ανίχνευση κυβερνοεπιθέσεων σε μικρές και μεσαίες επιχειρήσεις. Αυτό προσφέρει μια οικονομικά προσιτή λύση για οργανισμούς που ίσως να μην έχουν τη δυνατότητα να επενδύσουν σε ακριβό εξοπλισμό κυβερνοασφάλειας.

Επιπλέον, η πρακτική αυτή προσέγγιση έδωσε τη δυνατότητα για δοκιμές σε ένα ελεγχόμενο περιβάλλον, όπου οι επιθέσεις μπορούσαν να εκτελεστούν και να αναλυθούν με ασφάλεια. Τα αποτελέσματα έδειξαν ότι η σωστή διαμόρφωση και χρήση εργαλείων όπως το Snort και το Grafana μπορούν να προσφέρουν υψηλό επίπεδο προστασίας, ανιχνεύοντας και καταγράφοντας κακόβουλες δραστηριότητες με ακρίβεια. Η αποτελεσματικότητα του συστήματος ανίχνευσης επαληθεύτηκε μέσω της προσομοίωσης πραγματικών επιθέσεων, οι οποίες αντιμετωπίστηκαν επιτυχώς, αναδεικνύοντας τη χρησιμότητα της προτεινόμενης λύσης σε πραγματικά σενάρια.

Τέλος, η εμπειρία και τα συμπεράσματα που αντλήθηκαν από την πρακτική αυτή εφαρμογή υπογραμμίζουν την αξία της καινοτομίας και της δημιουργικότητας στην ανάπτυξη λύσεων κυβερνοασφάλειας. Παρά τις προκλήσεις και τους περιορισμούς, η χρήση προσιτών και ευέλικτων τεχνολογιών όπως το Raspberry Pi μπορεί να προσφέρει σημαντικά οφέλη και να συμβάλλει στην ενίσχυση της προστασίας των πληροφοριακών συστημάτων.

Η συνεχής εξέλιξη της τεχνολογίας και η αυξανόμενη συνδεσιμότητα μέσω του IoT επιβάλλουν τη συνεχή αναβάθμιση των στρατηγικών και των εργαλείων κυβερνοασφάλειας. Η έρευνα αυτή ενισχύει την ανάγκη για συνεχή εκπαίδευση, καινοτομία και προσαρμογή στις νέες απειλές. Η διεπιστημονική προσέγγιση, που συνδυάζει την τεχνολογία με την ανάλυση ρίσκου και τη διαχείριση κρίσεων, θα είναι καθοριστική για την αντιμετώπιση των μελλοντικών προκλήσεων στην κυβερνοασφάλεια.

Επιπλέον, η υιοθέτηση νέων τεχνολογιών όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση μπορεί να βελτιώσει σημαντικά τις δυνατότητες ανίχνευσης και απόκρισης σε κυβερνοεπιθέσεις. Η ενσωμάτωση αυτών των τεχνολογιών σε συστήματα όπως το Snort θα μπορούσε να επιτρέψει την αυτοματοποίηση της ανάλυσης απειλών και την ανάπτυξη προγνωστικών μοντέλων που θα βελτιώσουν την προληπτική ασφάλεια.

Είναι επίσης σημαντικό να αναγνωριστεί η ανάγκη για κατάλληλες πολιτικές και ρυθμιστικά πλαίσια που θα ενισχύσουν την κυβερνοασφάλεια. Οι κυβερνήσεις και οι διεθνείς οργανισμοί πρέπει να συνεργαστούν για την ανάπτυξη κανονισμών που θα διασφαλίζουν την προστασία των δεδομένων και των συστημάτων. Η συμμόρφωση με πρότυπα όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) είναι κρίσιμη για την προστασία της ιδιωτικότητας και την αύξηση της εμπιστοσύνης των χρηστών στις τεχνολογίες IoT.

Η εκπαίδευση και η ευαισθητοποίηση των χρηστών σχετικά με τις πρακτικές ασφάλειας είναι εξίσου σημαντικές. Η κατάρτιση του προσωπικού στις αρχές της κυβερνοασφάλειας και η καλλιέργεια μιας κουλτούρας ασφάλειας μπορούν να μειώσουν σημαντικά τον κίνδυνο ανθρώπινων λαθών που μπορεί να οδηγήσουν σε παραβιάσεις ασφαλείας. Επιπλέον, η εκπαίδευση των χρηστών για την αναγνώριση των απειλών και την υιοθέτηση ασφαλών πρακτικών μπορεί να ενισχύσει την προστασία των πληροφοριακών συστημάτων.

Η εργασία αυτή επιβεβαίωσε την κρίσιμη σημασία της κυβερνοασφάλειας στην προστασία των σύγχρονων δικτύων και των συνδεδεμένων συσκευών. Η πρακτική εφαρμογή των τεχνολογιών και των στρατηγικών που εξετάστηκαν παρέχει μια ισχυρή βάση για περαιτέρω έρευνα και ανάπτυξη στον τομέα της κυβερνοασφάλειας. Η συνεχής εξέλιξη των απειλών και των τεχνολογιών απαιτεί διαρκή επαγρύπνηση και προσαρμογή από τους οργανισμούς και τα άτομα που είναι υπεύθυνα για την προστασία των ψηφιακών υποδομών.

Καταλήγει ότι με την κατάλληλη χρήση τεχνολογιών, τη συνεχή εκπαίδευση, και την υποστήριξη από τις ρυθμιστικές αρχές, οι οργανισμοί μπορούν να επιτύχουν ένα υψηλό επίπεδο ασφάλειας που θα τους επιτρέπει να αντιμετωπίσουν αποτελεσματικά τις προκλήσεις του μέλλοντος.

8 Βιβλιογραφία

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *J. Cyber Secur. Mobil.*, *4*(1), 65-88.

Alsakran, F., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2019, December). Intrusion detection systems for smart home iot devices: experimental comparison study. In *International Symposium on Security in Computing and Communication* (pp. 87-98). Singapore: Springer Singapore.

Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security*, *2018*(5), 9-11.

Asaad, R. R. (2021). Penetration testing: Wireless network attacks method on Kali Linux OS. *Academic Journal of Nawroz University*, *10*(1), 7-12.

Baloch, R. (2017). *Ethical hacking and penetration testing guide*. Auerbach Publications.

Bera, S., Misra, S., & Vasilakos, A. V. (2017). Software-defined networking for internet of things: A survey. *IEEE Internet of Things Journal*, *4*(6), 1994-2008.

Bhattacharjee, S. (2018). *Practical Industrial Internet of Things security: A practitioner's guide to securing connected industries*. Packt Publishing Ltd.

Bryan Foltz, C. (2004). Cyberterrorism, computer crime, and reality. *Information Management & Computer Security*, *12*(2), 154-166.

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press.

Caplan, N. (2013). Cyber War: the Challenge to National Security. *Global Security Studies*, *4*(1).

Coşar, M., & Kiran, H. E. (2018, May). Measurement of Raspberry Pi performance in network traffic analysis. In *2018 26th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.

Deepa, T. (2014). Survey on need for cyber security in India. *Unpublished manuscript, Acharya Institute of Technology, Bangalore, Karnataka, India. doi*, *10*(13140), 2-1.

Denis, M., Zena, C., & Hayajneh, T. (2016, April). Penetration testing: Concepts, attack methods, and defense strategies. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1-6). IEEE.

Fallahi, N., Sami, A., & Tajbakhsh, M. (2016, May). Automated flow-based rule generation for network intrusion detection systems. In *2016 24th Iranian Conference on Electrical Engineering (ICEE)* (pp. 1948-1953). IEEE.

Furnell, S., & Dowling, S. (2019). Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, *5*(1), 13-26.

Ghael, H. D., Solanki, L., & Sahu, G. (2020). A review paper on raspberry pi and its applications. *International Journal of Advances in Engineering and Management (IJAEM)*, *2*(12), 4.

Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., & Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). *Materials Today: Proceedings*, *51*, 161-165.

Henschke, A. (2021). Terrorism and the internet of things: cyber-terrorism as an emergent threat. In *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism* (pp. 71-87). Cham: Springer International Publishing.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189.

Johari, R., Kaur, I., Tripathi, R., & Gupta, K. (2020, October). Penetration testing in IoT network. In *2020 5th International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-7). IEEE.

Kapto, A. S. (2013). Cyberwarfare: Genesis and doctrinal outlines. *Herald of the Russian Academy of Sciences*, *83*(4), 357-364.

Karlov, A. A. (2017, September). Cybersecurity of internet of things—Risks and opportunities. In *Proceedings of the XXVI International Symposium on Nuclear Electronics & Computing (NEC'2017)* (pp. 182-187).

Kenkre, P. S., Pai, A., & Colaco, L. (2015). Real time intrusion detection and prevention system. In *Proceedings of the 3rd international conference on Frontiers of intelligent computing: theory and applications (FICTA) 2014: volume 1* (pp. 405-411). Springer International Publishing.

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, *59*(1), 111-128.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 1-22.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898.

Kwon, H. Y., Kim, T., & Lee, M. K. (2022). Advanced intrusion detection combining signature-based and behavior-based detection methods. *Electronics*, *11*(6), 867.

Nagy, L., & Coleşa, A. (2019, October). Router-based IoT Security using Raspberry Pi. In *2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

Najera-Gutierrez, G., & Ansari, J. A. (2018). *Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux*. Packt Publishing Ltd.

Nasser, H. I., & Hussain, M. A. (2022). Defending a wireless LAN against ARP spoofing attacks using a Raspberry Pi. *J. Basrah Res.(Sci.)*, *48*(2), 123-135.

Oh, S. K., Stickney, N., Hawthorne, D., & Matthews, S. J. (2020, October). Teaching web-attacks on a raspberry pi cyber range. In *Proceedings of the 21st Annual Conference on Information Technology Education* (pp. 324-329).

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2024). *Managing and using information systems: A strategic approach*. John Wiley & Sons.

Pradeep, I., & Sakthivel, G. (2021, March). Ethical hacking and penetration testing for securing us form Hackers. In *Journal of Physics: Conference Series* (Vol. 1831, No. 1, p. 012004). IOP Publishing.

Quincozes, S. E., Albuquerque, C., Passos, D., & Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, *184*, 107679.

Rainer, R. K., Prince, B., Sánchez-Rodríguez, C., Splettstoesser-Hogeterp, I., & Ebrahimi, S. (2020). *Introduction to information systems*. John Wiley & Sons.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The internet society (ISOC)*, *80*(15), 1-53.

Saâdaoui, A., Benmoussa, H., Bouhoula, A., & Kalam, A. A. E. (2015). Automatic classification and detection of snort configuration anomalies-a formal approach. In *International Joint Conference: CISIS'15 and ICEUTE'15* (pp. 27-39). Springer International Publishing.

Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, *93*, 849-859.

Scarfone, K., & Mell, P. (2010). Intrusion detection and prevention systems. In *Handbook of Information and Communication Security* (pp. 177-192). Berlin, Heidelberg: Springer Berlin Heidelberg.

Shandilya, S. K., Wagner, N., & Nagar, A. K. (Eds.). (2020). *Advances in Cyber Security Analytics and Decision Systems*. Springer International Publishing.

Singh, T., & Aksanli, B. (2019, November). Real-time traffic monitoring and SQL injection attack detection for edge networks. In *Proceedings of the 15th ACM International Symposium on QoS and Security for Wireless and Mobile Networks* (pp. 29-36).

Srinidhi, N. N., Kumar, S. D., & Venugopal, K. R. (2019). Network optimizations in the Internet of Things: A review. *Engineering Science and Technology, an International Journal*, *22*(1), 1-21.

Stair, R. M., & Reynolds, G. W. (2018). *Fundamentals of information systems*. Cengage Learning.

Tasneem, A., Kumar, A., & Sharma, S. (2018). Intrusion detection prevention system using SNORT. *International Journal of Computer Applications*, *181*(32), 21-24.

Theohary, C. A., & Rollins, J. W. (2015). *Cyberwarfare and cyberterrorism: In brief* (pp. p-2). Washington, DC: Congressional Research Service.

Tzezana, R. (2016). Scenarios for crime and terrorist attacks using the internet of things. *European Journal of Futures Research*, *4*(1), 18.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: issues and challenges. *arXiv preprint arXiv:2103.15072*.

Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., & Han, H. (2022). A systematic literature review of methods and datasets for anomaly-based network intrusion detection. *Computers & Security*, *116*, 102675.

Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, *8*(2), 34-42.

Zhao, C. W., Jegatheesan, J., & Loon, S. C. (2015). Exploring iot application using raspberry pi. *International Journal of Computer Networks and Applications*, *2*(1), 27-34.