ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
& ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

Διπλωματική Εργασία

Μελέτη και κατηγοριοποίηση κυβερνοεπιθέσεων σε δημοφιλή λειτουργικά συστήματα και υπηρεσίες με τη χρήση Honeypots

Βογιατζής Μανώλης

Επιβλέπων καθηγητής: Δασυγένης Μηνάς

Εργαστήριο Ρομποτικής, Ενσωματωμένων και Ολοκληρωμένων Συστημάτων

Κοζάνη, Ιούλιος 2022

Περίληψη

Στην σύγχρονη εποχή, οι άνθρωποι κάνουν εκτενή χρήση του διαδικτύου μέσα από το οποίο μεταφέρουν πολλά προσωπικά δεδομένα και πληροφορίες, χωρίς να γνωρίζουν ακόμα και οι ίδιοι τον όγκο των ευαίσθητων στοιχείων, που διαρρέονται. Αυτή την διάδοση των πληροφοριών προσπαθούν να εκμεταλλευτούν κακόβουλοι χρήστες, προκειμένου να αποσπάσουν κωδικούς λογαριασμών, πληροφορίες συναλλαγών και οτιδήποτε μπορούν να χρησιμοποιήσουν προς όφελος τους. Τα δεδομένα είναι ο σημαντικότερος παράγοντας για την ιδιοτικότητα του ανθρώπου και η προστασία τους συσχετίζονται με τον όρο της κυβερνοασφάλειας. Πιο συγκεκριμένα, η κυβερνοασφάλεια είναι ο ορισμός της προστασίας των δεδομένων και πρέπει να αναβαθμίζεται συνεχώς καθώς οι τρόποι επιθέσεων αναπτύσσονται, ποικίλουν και διαφοροποιούνται. Ένας τρόπος για την αναβάθμιση της κυβερνοασφάλειας είναι τα honeypot.

Πιο συγκεκριμένα, τα Honeypot είναι ένας μηχανισμός ασφάλειας υπολογιστών για την ανίχνευση, την εκτροπή και την εξουδετέρωση των προσπαθειών μη εξουσιοδοτημένης χρήσης συστημάτων πληροφοριών. Διαθέτουν αναπτυγμένες δυνατότητες για συλλογή και ανάλυση των επιθέσεων, που κάνουν οι κακόβουλοι χρήστες. Με αυτόν τον τρόπο συμβάλουν στην αναγνώριση καινούργιων διαδικτυακών επιθέσεων, στην κατηγοριοποίηση ομάδων επιθέσεων, στην συγκέντρωση και στην ανάλυση των εργαλείων που χρησιμοποιούνται. Τα honeypot ελκύουν τους επιτιθέμενους, καθώς παρουσιάζονται ως αληθινά πληροφοριακά συστήματα και εκθέτουν διαδικτυακές πόρτες στον παγκόσμιο ιστό.

Σκοπός αυτής της εργασίας είναι η δημιουργία ενός υψηλού αλληλεπίδρασης honeypot για να μελετηθούν οι διαδικτυακές απειλές που υπάρχουν στο διαδίκτυο και η κατηγοριοποίηση των επιθέσεων αυτών. Πιο συγκεκριμένα το honeypot που θα δημιουργηθεί θα είναι μία σουίτα από υπάρχοντα honeypots και θα συνδυάζονται μέσω της εφαρμογής docker. Στο υψηλού αλληλεπίδρασης honeypot που θα δημιουργηθεί θα γίνεται καταγραφή, επεξεργασία, παρακολούθηση δικτυακής κίνησης, αποτροπή των επιθέσεων, απομακρυσμένη διαχείριση και οπτικοποίηση των δεδομένων. Οι πληροφορίες από τις επιθέσεις που θα δέχονται τα honeypots θα απεικονίζονται στο χρήστη μέσω του “Kibana” και του “Elastic Search”. Ο χρήστης θα έχει πρόσβαση σε αυτά τα συστήματα μέσα από το περιηγητή ιστού που χρησιμοποιεί και θα μπορεί να βλέπει τις επιθέσεις σε πραγματικό χρόνο. Επιπρόσθετα θα γίνεται κατηγοριοποίηση των επιθέσεων με κριτήρια την υπηρεσία που θα χρησιμοποιεί το honeypot, την διεύθυνση διαδικτυακού πρωτοκόλλου του κακόβουλου χρήστη και την χώρα από την οποία προέρχεται η επίθεση.

Λέξεις-Κλειδιά: Honeypot, Διεύθυνση Διαδικτυακού Πρωτοκόλλου, Ασφάλεια Πληροφοριακών Συστημάτων, Κυβερνοεπιθέσεις, Ασφάλεια δικτύων, Honeynet, Ανάλυση Επιθέσεων, Κυβερνοασφάλεια.

Title

Study and categorization of cyberattacks on popular operating systems and services using Honeypots

Abstract

In modern times, people use the Internet extensively and transfer a lot of personal data and information without even knowing the volume of personal data leaking. This information is being exploited by malicious users to extract account codes, transaction information and anything they can use to their advantage. Data is the most important factor and its protection is related to the term cybersecurity. More specifically, cybersecurity is the definition of data protection and needs to be constantly upgraded as the ways of attacks are developed, varied and diversified. One way to upgrade cybersecurity is a honeypot.

Honeypot is a computer security mechanism for detecting, diverting, and neutralizing the attempts of unauthorized use of information systems. They have advanced capabilities for collecting and analyzing attacks made by malicious users. They contribute to the recognition of new online attacks, to the categorization of attack groups, to the collection and analysis of the tools used in this way. Honeypot attracts attackers as they present themselves as real information systems and expose ports to the internet.

The purpose of this work is to create a high interaction honeypot to study the online threats that exist on the internet and to categorize these attacks. More specifically, the honeypot that will be created will be a suite of existing honeypots and will be combined through the Docker application. The high-interaction honeypot that will be created will record, process, monitor network traffic, prevent attacks, remote management, and visualize data. The information from the attacks that honeypots will receive will be displayed to the user through Kibana and Elastic Search. The user will have access to these systems through the web browser he or she will use and will be able to see the attacks in real time. In addition, the attacks will be categorized based on the service that the honeypot will use, the IP address of the malicious user and the country of origin of the attack.

Keywords: Honeypot, IP Address, Information Systems Security, Cyber Attacks , Network Security, Honeynet, Attack Analysis, Cybersecurity.

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν.1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο "Μελέτη και κατηγοριοποίηση κυβερνοεπιθέσεων σε δημοφιλή λειτουργικά συστήματα και υπηρεσίες με τη χρήση Honeypots" καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν και η οποία έχει εκπονηθεί στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Μηνά Δασυγένη αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο. Copyright (C) Ονοματεπώνυμο Φοιτητή & Επιβλέποντα, Έτος, Πόλη Copyright (C) Βογιατζής Μανώλης, Δασυγένης Μηνάς, 2020 , Κοζάνη.

Υπογραφή Φοιτητή

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1 – Εισαγωγή

1.1 Εισαγωγή

Στην σύγχρονη εποχή, η τεχνολογία αποτελεί αναπόσπαστο κομμάτι στην καθημερινότητα των ανθρώπων, αφού τα κινητά, τα tablet, οι υπολογιστές και κάθε είδος τεχνολογίας αποτελούν εργαλεία διευκόλυνσης εργασιών, επικοινωνίας και ψυχαγωγίας. Η συνεχής τεχνολογική πρόοδος, η εξέλιξη των συσκευών, η απανταχού συνδεσιμότητα στο διαδίκτυο και το χαμηλό κόστος των συσκευών αυτών δίνει την δυνατότητα σε κάθε άνθρωπο να αλληλοεπιδρά με τον παγκόσμιο ιστό. Η αύξηση των χρηστών στο παγκόσμιο ιστό είναι ραγδαία καθώς επίσης οι χρήστες μπορούν να χρησιμοποιήσουν περισσότερες από μία συσκευές για την περιήγηση τους στο διαδίκτυο. Συνήθως οι χρήστες χρησιμοποιούν τον παγκόσμιο ιστό για να πραγματοποιήσουν ηλεκτρονικές συναλλαγές, να επιμορφωθούν, να υλοποιήσουν δουλείες εξ αποστάσεως και να ψυχαγωγηθούν. Για όλες αυτές τις ανάγκες το διαδίκτυο και οι εταιρίες πληροφορικής αναπτύσσονται με κεντρικό τους στόχο να προσφέρουν εύχρηστα και οπτικοποιημένα, όμορφα στον χρήστη, προγράμματα. Συνεπώς οι χρήστες βλέπουν το τελικό αποτέλεσμα και δεν συνειδητοποιούν τον μεγάλο όγκο πληροφοριών που διανέμουν και τον τρόπο διανομής αυτών. Σε αυτό το σημείο εμπλέκεται ο ορισμός της κυβερνοασφάλειας, ο οποίος ταυτίζεται με την ασφαλή διανομή των πληροφοριών στο διαδίκτυο και διασφαλίζει, ότι πρόσβαση σε αυτές τις πληροφορίες θα έχουν όσοι ορίσει ο αποστολέας.

Η διαφορετικότητα των συσκευών, που στέλνουν τα δεδομένα, η πολυπλοκότητα των πληροφοριακών συστημάτων τα οποία μεσολαβούν για να σταλθούν τα δεδομένα, οι δικτυακές πόρτες και τα διαδικτυακά πρωτόκολλα ,που χρησιμοποιούνται για την διανομή των πληροφοριών και η διασφάλιση όλων των προηγουμένων αποτελεί παράγοντας της κυβερνοασφάλειας. Συνεπώς η ασφάλεια των δεδομένων στο διαδίκτυο επιτυγχάνεται λαμβάνοντας πολλούς διαφορετικούς παράγοντες. Αυτό αποτελεί πρόκληση για τους ερευνητές και τις εταιρίες πληροφορικής, που ασχολούνται με την ασφάλεια δικτυακών συστημάτων, αφού τα πληροφοριακά συστήματα και τα δικτυακά πρωτόκολλα αναβαθμίζονται ραγδαία και δημιουργούνται καινούργια. Οι ερευνητές, προκειμένου να συνυπάρχει η κυβερνοασφάλεια με την ραγδαία ανάπτυξη, χρησιμοποιούν παλιές μεθόδους και αναπτύσσουν νέες τεχνικές για να αντιληφθούν την κακόβουλη κίνηση από τους επιτιθέμενους.

1.2 Κακόβουλοι Χρήστες

Όλες οι συσκευές που συνδέονται στο διαδίκτυο, αποτελούν υποψήφιο στόχο για τους κακόβουλους χρήστες. Γνωρίζουμε ότι στο διαδίκτυο, κυβερνοεπιθέσεις συμβαίνουν συνεχώς και ασταμάτητα. Οι επιθέσεις αυτές μπορούν να πραγματοποιηθούν από μεμονωμένους χρήστες, από ειδικευμένα πληροφοριακά συστήματα, τα οποία έχουν ρυθμιστεί να κάνουν αυτόματα τυφλές επιθέσεις σε συσκευές και από συστήματα Botnet[1], τα οποία είναι πολλές συσκευές που τρέχουν κακόβουλο κώδικα στις συσκευές των χρηστών χωρίς αυτοί να το

γνωρίζουν. Στόχος αυτών των επιθέσεων είναι η υποκλοπή προσωπικών δεδομένων, η βιομηχανική κατασκοπεία, η δυσλειτουργία ή καταστροφή υπολογιστικών συστημάτων, η υποδούλωση και χρήση αυτών των συσκευών για κακόβουλες ενέργειες και ο διαδικτυακός πόλεμος μεταξύ κρατών. Οι επιτιθέμενοι μπορεί να είναι μέρος σε εγκληματικές οργανώσεις ή ακτιβιστές και το όφελος τους πίσω από τις επιθέσεις συνήθως είναι οικονομικό.

Οι μεμονωμένοι κακόβουλοι χρήστες συνήθως είναι Hackers[2] ακτιβιστές οι οποίοι κάνουν επιλεκτικές επιθέσεις σε εταιρίες και κυβερνήσεις. Σε αυτήν την περίπτωση ο στόχος είναι μια εταιρία και αφορά μία κατηγορία επιθέσεων. Σκοπός των ακτιβιστών είναι να κάνουν πειράματα για να ανακαλύψουν καινούργιες ευπάθειες στα συστήματα, να αξιολογήσουν τα μέτρα ασφαλείας της εταιρίας, να αξιολογήσουν τις δυνατότητες τους. Οι εγκληματικές οργανώσεις πραγματοποιούν και τυφλές επιθέσεις αλλά και επιλεκτικές. Με τον όρο τυφλές επιθέσεις εννοούμε την προώθηση κακόβουλων προγραμμάτων σε πολλά συστήματα χωρίς να έχουν στοιχεία γι' αυτά με την προοπτική οποία συσκευή το εκτελέσει να γίνει μέρος της μαζικής επίθεσής. Αντίθετά, οι επιλεκτικές επιθέσεις στοχεύουν στην εκβίαση μίας εταιρίας, καθώς πρώτα οι οργανώσεις έχουν υποκλέψει ή αλλοιώσει τα δεδομένα της και ζητάνε λύτρα για την ανάκτηση αυτών των πληροφοριών.

1.3 Τεχνικές Επίθεσης

Οι τεχνικές που χρησιμοποιούν οι επιτιθέμενοι κατατάσσονται σε πολλές κατηγορίες και καθημερινά δημιουργούνται πολλοί νέες επιθέσεις. Σύμφωνα με την παγκόσμια βάση γνώσεων για κυβερνοεπιθέσεις που βασίζεται σε πραγματικά δεδομένα MITRE ATTACK[3], καθημερινά δημιουργούνται 350.000 κακόβουλα προγράμματα. Τα κακόβουλα προγράμματα δεν έχουν όλα τα ίδιο στόχο επίθεσης αφού κατηγοριοποιούνται ανάλογα με την κρισιμότητα τους και την επιρροή τους σε χαμηλή κρισιμότητα, μέτρια κρισιμότητα και υψηλή κρισιμότητα. Συγκεκριμένα με βάση τον στόχο του κακόβουλού προγράμματος, τις ενέργειες που κάνει στο σύστημα του θύματος, την κρισιμότητα του και την γλώσσα προγραμματισμού που φτιάχτηκε, κατηγοριοποιούνται σε παγκόσμιες βάσεις δεδομένων. Ένα παράδειγμα είναι ο ιός "JS Trojan.Crysos.3367" όπου ο όρος JS αναφέρεται ότι το κακόβουλο πρόγραμμα δημιουργήθηκε με βάση την γλώσσα προγραμματισμού JavaScript[4], ο όρος Trojan[5] δείχνει σε ποια οικογένεια κακόβουλων προγραμμάτων ανήκει, ο όρος Crysos είναι το γένος του δηλαδή τι ενέργειες κάνει και ο αριθμός 3367 είναι ο αριθμός που είναι καταχωρημένος στις παγκόσμιες βάσεις δεδομένων. Το κάθε κακόβουλο λογισμικό προγραμματίζεται με διαφορετικές τεχνικές επίθεσης και διαφέρει από τα υπόλοιπα κακόβουλα προγράμματα.

Μία επίθεση ανεξάρτητά σε ποια κατηγορία επίθεσης ανήκει, έχει δώδεκα στάδια μέχρι να ολοκληρωθεί επιτυχώς. Το κάθε στάδιο αναφέρεται που έχει πρόσβαση ο επιτιθέμενος στο σύστημα της εταιρίας ή του οργανισμού. Το κάθε στάδιο είναι σημαντικό για την ανάκτηση πληροφοριών αλλά όσο φτάνουμε στο τελευταίο στάδιο τόσο ποιο επικίνδυνος και περισσότερη πρόσβαση έχει ο Hacker[2]. Τα

στάδια μιας κυβερνοεπίθεσης σύμφωνα με την παγκόσμια βάση γνώσεων για κυβερνοεπιθέσεις MITRE ATT&CK[3] είναι:

- Αρχική πρόσβαση
- Εκτέλεση του κακόβουλου προγράμματος
- Συνεχόμενη εκτέλεση του κακόβουλου προγράμματος
- Απόκτηση δικαιωμάτων για περισσότερες ενέργειες (Privilege Escalation)
- Αποφυγή Άμυνας, Αντιμέτρων Ασφαλείας
- Πρόσβαση
- Ανακάλυψη, διερεύνηση του συστήματος
- Εκμετάλλευση των ευπαθειών του συστήματος
- Πρόσβαση στα ευαίσθητα δεδομένα
- Έλεγχος και εκτέλεση εντολών στις υπηρεσίες του συστήματος
- Εξαγωγή ή κρυπτογράφηση των δεδομένων
- Επίπτωση που θα προκαλέσουν στην εταιρία

Πίνακας 1 Δημοφιλέστερες Κατηγορίες Επιθέσεων

Αριθμός	Όνομα Επίθεσης	Περιγραφή	Πρωτόκολλο
1	Brute Force Attack	Προσπάθεια απόκτησης κωδικού πρόσβασης ή όνομα χρήστη ή του κλειδιού κρυπτογράφησης ενός μηνύματος, χρησιμοποιώντας μια προσέγγιση δοκιμής και σφάλματος και ελπίζοντας, τελικά, να μαντέψει σωστά ο επιτιθέμενος.	SSH, HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Email)
2	Denial-of-service (DoS)	Οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας, οι οποίες έχουν ως σκοπό την δυσλειτουργία ή τον τερματισμό αυτής, στέλνοντας μεγάλο όγκο δικτυακών πακέτων.	HTTP (Hypertext Transfer Protocol), SSH, DNS (Domain Name System)
3	Man-in-the-middle attack	Ο επιτιθέμενος ακούει την διαδικτυακή συνομιλία μεταξύ δύο πληροφοριακών συστημάτων και υποκλέπτει πληροφορίες.	TCP/ UDP
4	Phishing Attack	Ο χρήστης τοποθετεί το όνομα χρήστη και τον κωδικό του σε ένα ψεύτικο περιβάλλον και τα στοιχεία στέλνονται στον επιτιθέμενο μέσω διαδικτύου.	TCP/UDP, SMTP

5	SQL injection	Ο επιτιθέμενος στέλνει κακόβουλα ερωτήματα στην βάση δεδομένων της εταιρίας προκειμένου να υποκλέψει τα στοιχεία σύνδεσης των χρηστών.	SQL (Structured Query Language), HTTP
6	Suspicious Activity	Κακόβουλα προγράμματα προσπαθούν να αλλάξουν μεταβλητές στο λειτουργικό σύστημα για να αποκτήσουν περισσότερη πρόσβαση	Operating System, Sys Logs
7	Communication with C&C Site	Ο χρήστης συνδέεται σε μία κακόβουλη ιστοσελίδα και κατεβάζει κακόβουλο πρόγραμμα χωρίς να έχει επίγνωση.	HTTP (Hypertext Transfer Protocol), TCP/ UDP
8	Communication with Command-and-Control Server	Αφού έχει εκτελεστεί το κακόβουλο πρόγραμμα, η συσκευή επικοινωνεί με έναν malicious server που του δίνει εντολές πως θα ενεργήσει κακόβουλα.	TCP/UDP
9	Suspicious Successful Login	Η είσοδος σε λογαριασμό του χρήστη από άλλη χώρα ή από διαφορετική συσκευή, που δεν έχει εξουσιοδοτημένη πρόσβαση.	SMTP, SSH, HTTP
10	Spam Emails	Ο χρήστης δέχεται email χωρίς να γνωρίζει τον αποστολέα με την προοπτική να πατήσει το σύνδεσμο και να συνδεθεί στον malicious server.	SMTP
11	Exploit's Execution	Ο hacker με συγκεκριμένα προγράμματα και συγκεκριμένες ευπάθειες προσπαθεί να δημιουργήσει σύνδεση με την υπηρεσία που προσφέρει η εταιρία	TCP/UDP, HTTP, SAMBA (SMB networking protocol), FTP, SQL, SSH

1.4 Αντίμετρα ασφαλείας διαδικτυακών συστημάτων

Η ασφάλεια πληροφοριακών συστημάτων και δικτύων είναι ένας πολύ σημαντικός τομέας για τις βιομηχανίες και τις κυβερνήσεις οι οποίες προκειμένου να διασφαλίσουν τα ευαίσθητα δεδομένα τους χρησιμοποιούν διάφορα αμυντικά πληροφορικά συστήματα όπως Firewall[6], Security Email Gateway[7], Antivirus[8], Cloud Monitor Analysis[9], User Behavior Analysis[10] κτλ. Όλα τα συστήματα που αναφέραμε ανήκουν σε μεγάλες εταιρίες παγκόσμιου βεληνεκούς και έχουν πρόσβαση σε πολλές παγκόσμιες βάσεις δεδομένων προκειμένου να είναι ενημερωμένες για τους καθημερινούς διαδικτυακούς κινδύνους. Οι παγκόσμιες βάσεις δεδομένων όπως MITRE ATT&CK[3], Virus Total(Google)[11], Cisco[12], Checkpoint[13] αποθηκεύουν καθημερινά εκατομμύρια κακόβουλα προγράμματα.

Το τείχος προστασίας ή αλλιώς firewall αποτελεί το πρώτο και πιο σημαντικό μηχανισμό ασφάλειας που πρέπει να έχει κάθε εταιρία. Σκοπός του είναι να ελέγχει ποια δικτυακή κίνηση πρέπει να επιτρέπεται και να αποτρέπει τις ύποπτες συνδέσεις. Ως το πιο βασικό επίπεδο, τα τείχη προστασίας μπορούν να αποκλείσουν την δικτυακή κυκλοφορία από και προς συγκεκριμένες διευθύνσεις δικτυακού πρωτοκόλλου ή πόρτες και υπηρεσίες διακομιστή. Επίσης περιέχουν δυνατότητες, που καθιστούν το firewall τον απόλυτο μηχανισμό ασφαλείας και περιγράφονται στο παρακάτω πίνακα. Τα δεδομένα σε αυτόν τον πίνακα έχουν παρθεί από την εταιρία Checkpoint η οποία είναι από τις καλύτερες στο τομέα των Firewalls.

Πίνακας 2 Δυνατότητες ενός τείχους προστασίας (Checkpoint Firewall)

Όνομα	Περιγραφή
IPsec VPN	Το VPN Software Blade ενσωματώνει τον έλεγχο πρόσβασης, τον έλεγχο ταυτότητας και την κρυπτογράφηση για να εγγυηθεί την ασφαλή σύνδεση με εταιρικά δίκτυα για απομακρυσμένους και κινητούς χρήστες, μέσω του Διαδικτύου
Identity Awareness	Το Identity Awareness Blade παρέχει λεπτομερή ορατότητα χρηστών, ομάδων και μηχανών, παρέχοντας έλεγχο πρόσβασης το που συνδέεται ο χρήστης και τον τρόπο που θα συνδεθεί πχ. One-Time-Password. Επίσης αποθηκεύει την ιστορικότητα του χρήστη.
Application Control	Το Application Control Blade επιτρέπει τον εντοπισμό, τον αποκλεισμό ή τον περιορισμό χρήσης προγραμμάτων και ιστοσελίδων, τα οποία θεωρούνται κακόβουλα προγράμματα με βάση τις παγκόσμιες βάσεις δεδομένων για κυβερνοεπιθέσεις.
Data Loss Prevention	Το DLP blade απαγορεύει την διαρροή δεδομένων έξω από την εταιρία.
Intrusion Prevention System	Το IPS blade συγκρίνει τις ενέργειες του χρήστη στο διαδίκτυο με τις παγκόσμιες βάσεις δεδομένων για κακόβουλα προγράμματα, ύποπτα πληροφοριακά συστήματα και αποφασίζει αν θα εγκαταστήσει ή αποκλείσει την επικοινωνία των δύο πληροφοριακών συστημάτων.
Anti-Bot	Το Anti-Bot αποτρέπει τις ζημιές από μαζικά κακόβουλα συστήματα που κάνουν τυφλές επιθέσεις και ελέγχουν την συσκευή(botnets, C&C Site), αποκλείοντας τις επικοινωνίες. Τα δεδομένα για αυτά τα συστήματα τα αντλεί από τις παγκόσμιες βάσεις δεδομένων.
Anti-Spam and Email Security	Το Anti-Spam αποτρέπει την επίθεση SPAM
Antivirus	Το Antivirus αντλεί δεδομένα από τις βάσεις και αποκλείει κάθε κακόβουλο πρόγραμμα.

Threat Emulation	Το Threat Emulation αποτρέπει τα συστήματα από απειλές μηδενικής ημέρας (Zero-Day Threats), νέο κακόβουλο λογισμικό και στοχευμένες επιθέσεις. Συγκεκριμένα τα αρχεία αναλύονται πρώτα σε ψεύτικα μηχανήματα της εταιρίας και μόλις επιβεβαιωθεί η εγκυρότητα του προγράμματος επιτρέπεται η σύνδεση με τον διακομιστή.

Εκτός από τα Antivirus και Firewall υπάρχουν και μηχανισμοί ασφάλειας που λειτουργούν με τεχνητή νοημοσύνη είναι περισσότερο αποδοτικά. Συγκεκριμένα τα περισσότερα προηγμένα προγράμματα ενσωματώνουν τον μηχανισμό ανάλυσης συμπεριφοράς χρήστη (User Behavior Analysis), ο οποίος είναι μία διαδικασία συλλογής πληροφοριών για τα συμβάντα του δικτύου που δημιουργούν οι χρήστες καθημερινά. Αφού συλλεχθούν και αναλυθούν τα δεδομένα των χρηστών από το προηγούμενο χρονικό διάστημα, ο μηχανισμός αυτός μπορεί να ανιχνεύσει την κακόβουλη και την μη φυσιολογική συμπεριφορά των χρηστών και να την αποτρέψει.

1.5 Τεχνικές Ανάλυσης Κακόβουλων Προγραμμάτων

Προτού αποθηκευτούν στις παγκόσμιες βάσεις δεδομένων οι ιοί, γίνεται ανάλυση συμπεριφοράς πολλών προγραμμάτων και ιστοσελίδων σε ειδικά διαμορφωμένα συστήματα και διεκπεραιώνεται αν είναι κακόβουλο το πρόγραμμα ή η ιστοσελίδα. Η ανάλυση συμπεριφοράς ενός προγράμματος πραγματοποιείται με πολλές τεχνικές. Μια σημαντική τεχνική ανάλυσης συμπεριφοράς είναι η εγκατάσταση και η εκτέλεση του προγράμματος σε εικονικά μηχανήματα τα οποία έχουν φτιαχτεί για αυτόν τον σκοπό και δεν υπάρχει κανένας κίνδυνος να εξαπλώσουν το ιό ή όπως αλλιώς ονομάζονται Sandbox. Επίσης, σημαντική τεχνική είναι τα antivirus στις συσκευές τα οποία αναλύουν ασταμάτητα την συμπεριφορά των προγραμμάτων στις τοπικές πληροφοριακές συσκευές και στέλνουν δεδομένα στις παγκόσμιες βάσεις δεδομένων. Τρίτον, ειδικά εικονικά συστήματα χρησιμοποιώντας συγκεκριμένα εργαλεία επικοινωνούν με ιστοσελίδες, DNS διακομιστές και αναλύεται η δικτυακή κίνηση αν είναι κακόβουλη. Τέλος σημαντική τεχνική ανάλυσης δεδομένων είναι τα Honeypots, τα οποία πραγματοποιούν όλα τα παραπάνω σε ένα πληροφοριακό σύστημα. Αφού πρώτα ελκύουν με μηχανισμούς τους επιτιθέμενους και παρουσιάζονται σαν αληθινά συστήματα, τα honeypots έχουν πολλές δυνατότητες όπως η ανάλυση της συμπεριφοράς ενός κακόβουλου προγράμματος, η ανάλυση της δικτυακής συμπεριφοράς όταν συνδεθεί σε έναν κακόβουλο διακομιστή, η αποστολή των δεδομένων σε παγκόσμιες βάσεις δεδομένων. Οι λίστες αναφοράς και αποτροπής κακόβουλων διακομιστών και κακόβουλων προγραμμάτων (Blacklists[14]) του παγκόσμιου ιστού δημιουργούνται κυρίως από τα Honeypots, τα οποία μαζεύουν όλα τα στοιχεία του κακόβουλου διακομιστή και των διακομιστών που επικοινωνεί για να συντονίσουν την επίθεση.

1.6 Ορισμός Honeypots

Τα honeypot είναι συστήματα που έχουν στόχο την ανίχνευση, την ανάλυση και την εξουδετέρωση των κακόβουλων προσπαθειών. Με τις υπηρεσίες που προσφέρουν όπως SSH, SMTP, HTTP, SAMBA, κτλ., με τις διαδικτυακές πόρτες που εκθέτουν στο διαδίκτυο και με τους μηχανισμούς επικοινωνίας, έλκουν τους επιτιθέμενους. Επίσης αποτελούν πραγματικού χρόνου εργαλεία ανάλυσης καθώς την στιγμή της επίθεσης συλλέγουν και καταγράφουν δεδομένα αυτής και υπάρχει οπτική παρακολούθηση για τις ενέργειες του επιτιθέμενου. Συμβάλουν έτσι, στην αναγνώριση νέων διαδικτυακών επιθέσεων, την κατηγοριοποίηση των επιτιθέμενων και την συγκέντρωση και ανάλυση των εργαλείων που χρησιμοποιούνται στην επίθεση.

1.7 Κατηγορίες Honeypots

Τα Honeypots κατηγοριοποιούνται ανάλογα με το βαθμό αλληλεπίδρασης τους στην ανάλυση σε τρεις κατηγορίες low-interaction, medium-interaction, high-interaction. Τα χαμηλής αλληλεπίδρασης ή αλλιώς low-interaction honeypots είναι εργαλεία που δίνουν στον επιτιθέμενο περιορισμένη πρόσβαση στο λειτουργικό σύστημα καθώς έχει στατικό περιβάλλον. Ένα Honeypot χαμηλής αλληλεπίδρασης συνήθως μιμείται ένα μικρό αριθμό πρωτοκόλλων διαδικτύου και υπηρεσιών δικτύου Σε γενικές γραμμές, προσομοιώνουν πρωτόκολλα όπως TCP και IP, τα οποία επιτρέπουν στον εισβολέα να πιστεύει ότι συνδέονται με ένα πραγματικό σύστημα και όχι με ένα περιβάλλον Honeypot. Ωστόσο, ένα Honeypot χαμηλής αλληλεπίδρασης μπορεί να μην ξεγελάσει τους επιτιθέμενους να εμπλακούν και σίγουρα δεν είναι αρκετά σε βάθος για να συλλάβει πολύπλοκες απειλές.

Τα honeypot μεσαίας αλληλεπίδρασης αποτελούν την καλύτερη λύση, παρέχοντας μικρότερο κίνδυνο από τη δημιουργία ενός πλήρους φυσικού ή εικονικοποιημένου συστήματος για την εκτροπή των εισβολέων, αλλά με περισσότερη λειτουργικότητα. Αυτά εξακολουθούν να μην είναι κατάλληλα για σύνθετες απειλές, όπως 0-day επιθέσεις[15] οι οποίες είναι πολύ επικίνδυνες γιατί δεν αναγνωρίζονται ως κακόβουλες από τα αντίμετρα ασφαλείας ενός συστήματος, αλλά θα μπορούσαν να στοχεύουν επιτιθέμενους που αναζητούν συγκεκριμένες ευπάθειες. Τέλος τα honeypot υψηλής αλληλεπίδρασης παρέχουν μια πολύ πιο λεπτομερή εικόνα για το πώς εξελίσσεται μια επίθεση ή εισβολή ή πώς εκτελείται ένα συγκεκριμένο κακόβουλο λογισμικό σε πραγματικό χρόνο. Επειδή δεν υπάρχει προσομοιωμένη υπηρεσία, το υψηλής αλληλεπίδρασης Honeypots βοηθά στον εντοπισμό άγνωστων ευπαθειών. Παρόλα αυτά τα Honeypots υψηλής αλληλεπίδρασης είναι πιο επιρρεπή σε μολύνσεις αφού οι επιτιθέμενοι έχουν την δυνατότητα να αποκτήσουν πρόσβαση στο λειτουργικό σύστημα.

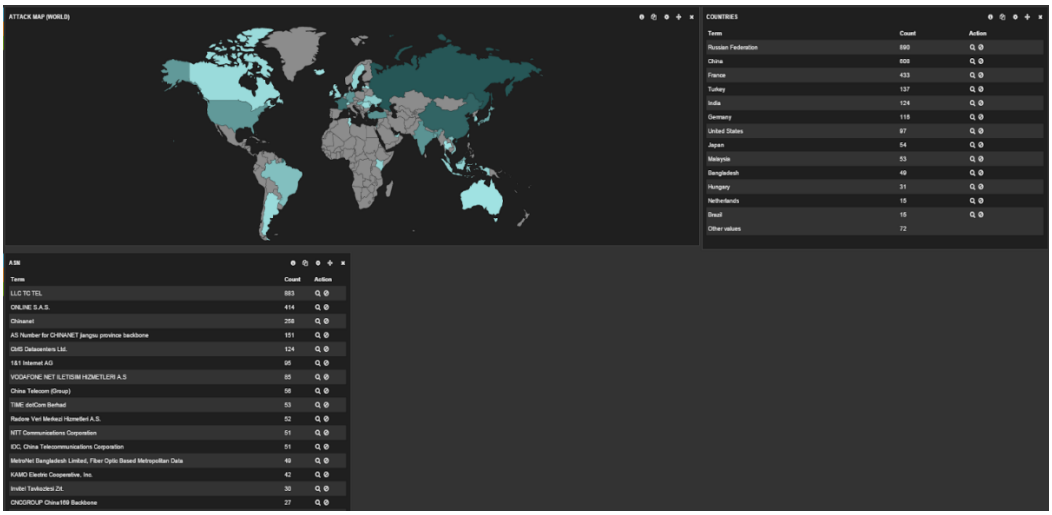
1.8 Ιστορική Εξέλιξη των honeypots

Με την έναρξη των ιών ή αλλιώς malwares που διαμορφώθηκαν στη δεκαετία του 1960, το πρώτο Honeypot εμφανίστηκε αργότερα, περίπου το 1986 που γράφτηκε από τον Clifford Stoll. Αυτή τη στιγμή, ο όρος "Honeypot" δεν χρησιμοποιήθηκε, αλλά ο Stoll χρησιμοποίησε μια πρώιμη έκδοση ενός σύγχρονου Honeypot για να αιχμαλωτίσει έναν δυτικογερμανικό χάκερ και τελικά να γράψει ένα βιβλίο για την εμπειρία του με το όνομα TheCuckoo's Egg. Η επόμενη πρόοδος στα Honeypot προήλθε από έναν αξιοσημείωτο εμπειρογνώμονα τείχους προστασίας Bill Cheswick, ο οποίος έγραψε μια σειρά από ψεύτικες υπηρεσίες, αρχεία κωδικού πρόσβασης, ακόμη και σενάρια για να κάνει δραστηριότητα υπηρεσίας σε αυτό που τώρα θεωρείται ως ένα σύγχρονο Honeypot. Τέλος, το πρωτοφανές, διακριτό Honeypot δημιουργήθηκε από τον Fred Cohen το 1997 με την ονομασία Deception ToolKit (DTK). Αυτό κατασκευάστηκε με σκοπό να υλοποιήσουν επιθέσεις εκείνης της εποχής και δημιουργήσαν σε αυτό κακόβουλά εκτελέσιμα προγράμματα τα οποία φτιάχτηκαν με την γλώσσα προγραμματισμού C. Έτσι ανακάλυψαν ευπάθειες και αδυναμίες των τότε συστημάτων. Το Honeynet Project ήταν ένα πρόγραμμα που ιδρύθηκε από τον Lance Spitzer το 1999. Αυτό το έργο ήταν η αφετηρία για την έρευνα και δημιουργία Honeypot. Με τα μέλη του The Honeynet Project που αποτελούσαν ως επί το πλείστον επαγγελματίες της ασφάλειας των πληροφοριών, παρήγαγαν πολλά έγγραφα και σχέδια σχετικά με τον τρόπο δημιουργίας αποτελεσματικών Honeypots. Το πρώτο πρόγραμμα σχεδιασμού και εμπορικού ανοιχτού κώδικα κυκλοφόρησε το 2001 με το όνομα the Genen Model. Τα σχέδια Sincethen, honeypot και άλλα έργα ανοιχτού κώδικα συνέχισαν να επεκτείνονται εκτός του The Honeynet Project. Σήμερα, όλα τα είδη honeypots χαμηλής, μεσαίας και υψηλής αλληλεπίδρασης στηρίζονται στην λογική των πρώτων honeypot και ενσωματώνουν καινούργιες τεχνικές.

1.9 Σχετικές Εργασίες

Τα Honeypot άρχισαν αναπτύσσονται ραγδαία στις αρχές του 20ου αιώνα και συνεχίζουν να αναπτύσσονται με τα πιο δημοφιλή να είναι το T-Pot, το Cowrie, το Dionaea, το glastopf και το Google Hack Honeypot. Ανάλογα τις πόρτες που εξυπηρετεί το κάθε ένα προσπαθεί να ανιχνεύσει και ένα συγκεκριμένο εύρος επιθέσεων. Αρχικά το Cowrie είναι ένα μεσαίας αλληλεπίδρασης honeypot το οποίο έχει σχεδιαστεί για να καταγράφει επιθέσεις ωμής βίας και εξυπηρετεί την πόρτα SSH και Telnet. Το Cowrie είναι γραμμένο στη γλώσσα Python και μιμείται ένα σύστημα Linux Debian 5[16] καθώς περιέχει πλήρως όλα τα αρχεία του λειτουργικού συστήματος, δίνοντας την αίσθηση ότι επιτιθέμενος βρίσκεται σε αληθινό σύστημα. Εκτός από τις τεχνικές επίθεσης ωμής βίας γίνεται καταγραφή και ανάλυση των τεχνικών που χρησιμοποιεί ο επιτιθέμενος προκειμένου να πάρει δικαιώματα διαχειριστή. Επίσης μπορεί να ανιχνεύσει τις εξωτερικές συνδέσεις που κάνει ο επιτιθέμενος και καταγράφει την όλη συμπεριφορά του. Πρόκειται για την εξέλιξη του Honeypot Kippo καθώς η εταιρεία Rapid7 που το εφηύρε συνέχισε στην αναβάθμιση του συγκεκριμένου μετά ονομάζοντας το σε Cowrie. Οι εφευρέτες του δημιούργησαν και μία δυνατότητα εικονοποίησης των δεδομένων του συγκεκριμένου, η οποία ονομάζεται Kippo-Graph και δίνει τη δυνατότητα να

αποθηκευτούν τα δεδομένα σε μία βάση δεδομένων για την ανάλυσή τους σε μετέπειτα χρόνο.



Εικόνα 1. Τα δεδομένα του Cowrie στην βάση δεδομένων Kippo-Graph

Μία σημαντική αναφορά είναι το honeypot T-pot της εταιρείας Deutsche telekom Security[17], το οποίο είναι μία σουίτα που συνδυάζει τις καλύτερες τεχνολογίες Honeypot σε ένα σύστημα. Συγκεκριμένα χρησιμοποιεί τα καλύτερα ανοιχτού κώδικα Honeypot όπως adbhoney, dionaea, cowrie, snare, suricata κτλ, έχοντας ως στόχο να καλύψει όλο το εύρος των υπηρεσιών σε tcp και udp επικοινωνίες. Το σύστημα αναλύει τις προσπάθειες μη εξουσιοδοτημένης πρόσβασης και αποτρέπουν τις παρατεταμένες επιθέσεις με συγκεκριμένους μηχανισμούς όπως το fail2ban. Το T-Pot είναι εύκολο στον χρήστη αφού οπτικοποιεί τα δεδομένα που έχει και τα ταξινομεί σε κατηγορίες κατανοητές από τον χρήστη με την βοήθεια του ELK stack[18]. Το ELK stack[18] αποτελείται από τρία διαφορετικά honeypots Elastic Search, Logtrash και Kibana και ο χρήστης έχει πρόσβαση σε αυτό μέσω του περιηγητή. Τέλος το T-Pot αποτελεί την ιδανικότερη επιλογή για να αναγνώριση νέων επιθέσεων και καταγραφή κατηγοριών κυβερνοεπιθέσεων και χρησιμοποιείται σε πολλές κυβερνήσεις και βιομηχανίες παγκοσμίως.

Εικόνα 1 TPOT

Επίσης ένα από τα καλύτερα Honeypot που χρησιμοποιείται συχνά από τους ερευνητές είναι το Glastopf. Πρόκειται για ένα δυναμικό χαμηλής αλληλεπίδρασης ψεύτικο σύστημα διαδικτυακών εφαρμογών και έχει την ικανότητα προσομοίωση χιλιάδων αδυναμιών με σκοπό τη συγκέντρωση δεδομένων από τις επιθέσεις ενάντια στις ευπάθειες αυτές. Το Glastopf υποστηρίζει την καταγραφή επιθέσεων πολλαπλών επιπέδων (multi-stage) και περιέχει έναν προσομοιωτή ευπαθειών με τις πιο σημαντικές και επικίνδυνες ευπάθειες σε διαδικτυακές εφαρμογές. Στόχος του είναι να βρεθούν απαντήσεις και να καλυφθούν τα κενά ασφαλείας στις αδυναμίες αυτές. Αποτελείται από τρία κύρια τμήματα τα οποία και σχηματίζουν τον πυρήνα του προγράμματος.

- Web Server: τον διακομιστή που περιέχει τις διαδικτυακές εφαρμογές και απαντάει σε αιτήματα πρωτόκολλου HTTP. Το τμήμα αυτό είναι υπεύθυνο για την υλοποίηση της διασύνδεσης μέσω της οποίας θα καταστεί δυνατόν να δεχθεί επιθέσεις.
- Βάση δεδομένων: στη βάση δεδομένων αποθηκεύονται οι σημαντικότερες ευπάθειες οι οποίες είναι μεγάλης κρισιμότητας για τις διαδικτυακές αυτές εφαρμογές και το τμήμα αυτό είναι υπεύθυνο για την εκτέλεση ενεργειών και καταγραφής δεδομένων.
- Pattern matching: αυτό το τμήμα είναι υπεύθυνο για να αντιστοιχίσει τις επιθέσεις σε συγκεκριμένες αδυναμίες και λειτουργεί με αλγόριθμους Regex. Όλα τα τμήματα είναι σημαντικά αλλά το συγκεκριμένο χρησιμοποιεί στην τεχνητή νοημοσύνη, μπορεί να κατηγοριοποιήσει τις επιθέσεις σε κατηγορίες και να καταλάβει κάθε επίθεση πόσο ζημιά μπορεί να κάνει στο σύστημα.

Τέλος ο Farouk Samu από το πανεπιστήμιο St. Cloud State της Αμερικής διπλωματική εργασία με τίτλο "Design and Implementation of a Real-Time Honeypot System for the Detection and Prevention of Systems Attacks" δημιούργησε ένα χρήσιμο Honeypot που εξυπηρετεί πολλές υπηρεσίες. Το σύστημα που δημιούργησε πρόκειται για μια σουίτα Honeypot παρόμοιο με το T-Pot Project και περιέχει τέσσερα δημοφιλή ψεύτικα συστήματα τα οποία είναι το Con-SshHoenypot, FTP trap, Pot και Apache Server. Μαζεύοντας τα δεδομένα από τα ψεύτικα συστήματα τα οπτικοποιεί με το πρόγραμμα Elasticsearch και στη συνέχεια με το πρόγραμμα Kibana δημιουργεί τα γραφήματα και τα στατιστικά των επιθέσεων. Ο συγκεκριμένος ερευνητής έχει δημοσιεύσει τον κώδικα και τα στατιστικά των δεδομένων του στην προσωπική του σελίδα στο διαδίκτυο.

1.10 Σκοπός της διπλωματικής

Στην παρούσα εργασία αναπτύχθηκε ένα υψηλής αλληλεπίδρασης honeypot το οποίο ενσωματώνει πολλά δημοφιλή honeypot. Τα honeypot αυτά θα στοχεύουν σε συγκεκριμένες υπηρεσίες όπως ssh, http, samba, mail, ftp. Η ενσωμάτωση των honeypots σε ένα σύστημα θα υλοποιείται μέσω της εφαρμογής Docker, η οποία δημιουργεί ένα εικονικό server Hyper vision[19] και τα συγχωνεύει με τέτοιο τρόπο ώστε να γνωρίζουν το καθένα ποιες διεργασίες χρησιμοποιεί τα άλλα παρόλα αυτά το καθένα να τρέχει τις δικές του διεργασίες. Τα δεδομένα από αυτές τις κυβερνοεπιθέσεις θα συλλέγονται και θα οπτικοποιούνται μέσω του ELK stack και

θα κατηγοριοποιούνται με βάση την κατηγορία της επίθεσης, την μέθοδο της επίθεσης, τα εργαλεία που χρησιμοποιήθηκαν. Θα υπάρχει ένας οπτικός παγκόσμιος χάρτης που θα δείχνει την συχνότητα και τις χώρες που προήλθαν οι επιθέσεις. Επίσης θα ενσωματωθεί εργαλείο για την παρακολούθηση σε πραγματικό χρόνο όταν θα εισέρχεται ο επιτιθέμενος στο λειτουργικό σύστημα. Με αυτό τον τρόπο επιτυγχάνεται η συγκέντρωση των εντολών και των τεχνικών που χρησιμοποιεί ο κακόβουλος χρήστης για να παραβιάσει το σύστημα στο τελικό στάδιο της επίθεσης. Το fail2ban[20] και το Iptables[21] θα αποτελούν τα εργαλεία αποτροπής των επιθέσεων αφού ανάλογα με την επιμονή και την συχνότητα της επίθεσης θα απαγορεύεται η επικοινωνία με την συγκεκριμένη διεύθυνση διαδικτυακού πρωτοκόλλου. Το Iptables[21] θα μπλοκάρει τις συνδέσεις με συγκεκριμένα υποδίκτυα τα οποία θεωρούνται κακόβουλα από πολλές παγκόσμιες βάσεις δεδομένων. Με αυτό επιτυγχάνουμε την έλξη επιτιθέμενων που δεν θα κάνουν τυφλές επιθέσεις αλλά στοχευμένες.

Στόχος αυτής της διπλωματικής είναι να παραχθεί ένα ισχυρό εργαλείο ανίχνευσης, ανάλυσης και αποτροπής κυβερνοεπιθέσεων. Οι διαδικασίες εγκατάστασης και ρύθμισης του αναλύονται στο παρακάτω τμήμα αυτής της εργασίας. Επιπρόσθετα το εργαλείο αυτό θα δημοσιευτεί στον προσωπικό λογαριασμό στο Github[22] προκειμένου να χρησιμοποιηθεί και από άλλους ερευνητές. Τα αποτελέσματα αυτής της εργασίας θα παρουσιαστούν και θα αναλυθούν στο 4 κεφάλαιο αυτής της εργασίας.

1.11 Διάρθρωσή εργασίας

Στο πρώτο κεφάλαιο γίνεται μία εισαγωγή στα ζητήματα που διαπραγματεύονται σε αυτήν την διπλωματική εργασία. Αναφέρονται και αναλύονται όροι ασφάλειας πληροφοριακών ζητημάτων και δικτύων. Συγκεκριμένα αναλύεται η έννοια του επιτιθέμενου, των αντιμέτρων ασφάλειας για τις κυβερνήσεις και τις εταιρίες, οι τεχνικές επίθεσης που θα συναντήσουμε στο σύστημα και ο όρος honeypot και οι ιδιότητες τους. Γίνεται αναφορά στο υπάρχουσα κατάσταση στο χώρο της ασφάλειας, οι προκλήσεις που υπάρχουν, στοιχειοθετείτε το πρόβλημα και αναφέρονται υλοποιήσεις από άλλους ερευνητές.

Στο δεύτερο κεφάλαιο δίνεται το θεωρητικό υπόβαθρο του έργου, για την πληρέστερη κατανόησή της εργασίας. Γίνεται αναφορά στην τεχνική παρουσίαση και ανάπτυξη του έργου, στο οποίο τοποθετούνται και περιγράφονται όλα τα εργαλεία λογισμικού που χρησιμοποιήθηκαν.

Στο τρίτο κεφάλαιο γίνεται παρουσιάζονται τα βήματα και η μεθοδολογία εγκατάστασης του εργαλείου. Δίνονται αναλυτικά οι εντολές για την ρύθμιση του εργαλείου και επεξηγεί τους τρόπους που ο κάθε χρήστης μπορεί να διαμορφώσει το περιβάλλον και τις πλατφόρμες απεικόνισης δεδομένων.

Στο τέταρτο παρατίθενται τα αποτελέσματα της μελέτης σε κατηγορίες και σε πίνακες. Αναφέρονται στατιστικά των επιθέσεων και γίνεται μελέτη ποιες κατηγορίες επιθέσεων παρατηρούνται πιο συχνά, την χώρα που προέρχονται οι περισσότερες επιθέσεις και τα δημοφιλέστερα εργαλεία επιθέσεων χρησιμοποιούνται.

Στο τελευταίο κεφάλαιο αναφέρεται η σύνοψη του έργου που έχει γίνει, τα συμπεράσματα και οι προτάσεις για την επέκταση της εργασίας. Προτείνονται μελλοντικές επεκτάσεις για την ανάπτυξη του Honeypot.

Κεφάλαιο 2 – Θεωρητικό υπόβαθρο

2.1 Εισαγωγή

Στο συγκεκριμένο κεφάλαιο περιγράφονται τεχνικές λεπτομέρειες καθώς και το θεωρητικό υπόβαθρο, με βάση το οποίο έχει δημιουργηθεί το υψηλής αλληλεπίδρασης Honeypot. Σκοπός αυτής της διπλωματικής εργασίας, είναι να κατανοήσει ο αναγνώστης την αρχιτεκτονική στην οποία έχει δημιουργηθεί το Honeypot, τον τρόπο κατηγοριοποίησης και συλλογής των επιθέσεων και τον λόγο που κάνει αυτό το σύστημα καινοτόμο.

Το συγκεκριμένο Honeypot αποτελείται από μια πληθώρα παραπλανητικών συστημάτων τα οποία καταγράφουν, αναλύουν και εξουδετερώνουν απειλές από το διαδίκτυο. Τα παραπλανητικά αυτά συστήματα έχουν διαμορφωθεί καταλλήλως, ώστε να είναι προσβάσιμα από τον κάθε χρήστη στο διαδίκτυο, με σκοπό να προσελκύουν και παγιδεύουν τους επιτιθέμενους. Οι κακόβουλοι χρήστες πραγματοποιούν επιθέσεις ωμής βίας και οριζόντιας σάρωσης θυρών και προσπαθούν να ανιχνεύσουν ανοιχτές υπηρεσίες και ευπάθειες στα παραπλανητικά μας συστήματα.

Στην προσπάθεια των χρηστών να εισβάλλουν στα ψεύτικα συστήματα, το Honeypot υποκλέπτει τις τεχνικές που εφαρμοστήκαν, τα αυτοματοποιημένα εργαλεία που χρησιμοποιήθηκαν και στοιχεία για τον επιτιθέμενο όπως η διεύθυνση διαδικτυακού πρωτοκόλλου, η τοποθεσία, ο ξεχωριστός αριθμός (ASN[24]) της διεύθυνσης διαδικτυακού πρωτοκόλλου και από ποια εταιρία προήλθε η επίθεση. Αυτά τα στοιχεία συλλέγονται και με τα προγράμματα “Filebeat” και “Logstash” μεταφέρονται στο “Kibana” , στο οποίο αναλύονται με διαγράμματα και πίνακες τα δεδομένα των επιθέσεων. Ο τρόπος μεταφοράς δεδομένων και περισσότερες τεχνικές λεπτομέρειες αναλύονται στην υποενότητα «Συλλογή Δεδομένων».

Τέλος, ο ρόλος του honeypot και όλα τα δεδομένα που συγκεντρώνονται θα αποστέλλονται σε παγκόσμιες βάσεις δεδομένων προκειμένου οι ειδικοί στο τομέα της ασφάλειας να έχουν την γνώση για τους κακόβουλους χρήστες και τις τοποθεσίες τους. Αυτό επιφέρει την εξόπλιση των οργανισμών να μην δέχονται πολλές επιθέσεις καθώς τα τείχη προστασίας θα αποτρέπουν τις επιθέσεις που προέρχονται από διευθύνσεις διαδικτυακού πρωτοκόλλου που έχουν χαρακτηριστεί ως κακόβουλες.

2.2 Τοποθέτηση των honeypots

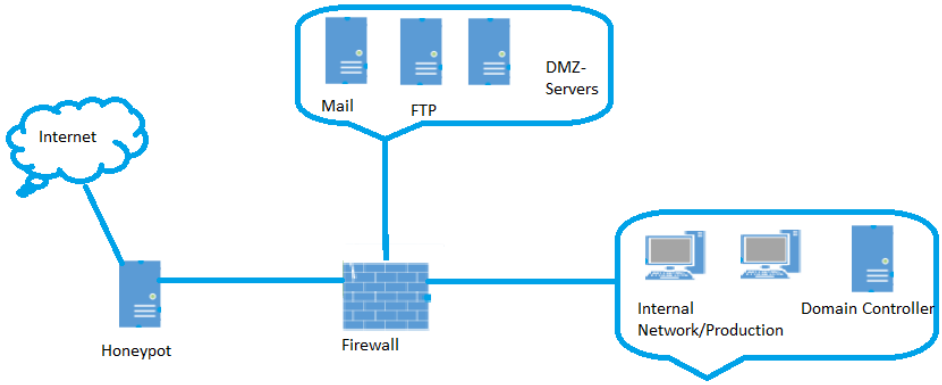
Ο κύριος στόχος των honeypots είναι η αναγνώριση και ανάλυση των επιθέσεων σε μία εταιρία ή έναν οργανισμό. Επίσης ανάλογα με τον τρόπο που έχουν διαμορφωθεί, αποτρέπουν τις εσωτερικές ή τις εξωτερικές επιθέσεις. Η διαφορά μεταξύ αυτών των δύο υποδεικνύεται από τα ονόματα τους, οι εσωτερικές επιθέσεις γίνονται μέσα στο κτήριο του οργανισμού όπως το ασύρματο δίκτυο των επισκεπτών και το δίκτυο θα είναι της μορφής 192.168.x.x. Αντίθετα, οι εξωτερικές επιθέσεις είναι χαμηλότερης κρισιμότητας, πολυπληθέστερες και η επίθεση έρχεται από το διαδίκτυο.

Η τοποθέτηση των honeypots αλλάζει σε κάθε οργανισμό καθώς αλλάζουν και οι ανάγκες τους για ποιες επιθέσεις θέλουν να αναγνωρίζουν και να αποτρέψουν. Με

βάση το παραπάνω υπάρχουν τρείς διαφορετικές προσεγγίσεις για την τοποθέτηση των honeypots στο δίκτυο του οργανισμού.

2.2.1 Τοποθέτηση του Honeypot μπροστά από το τείχος προστασίας για την καλύτερη ανίχνευση των επιθέσεων

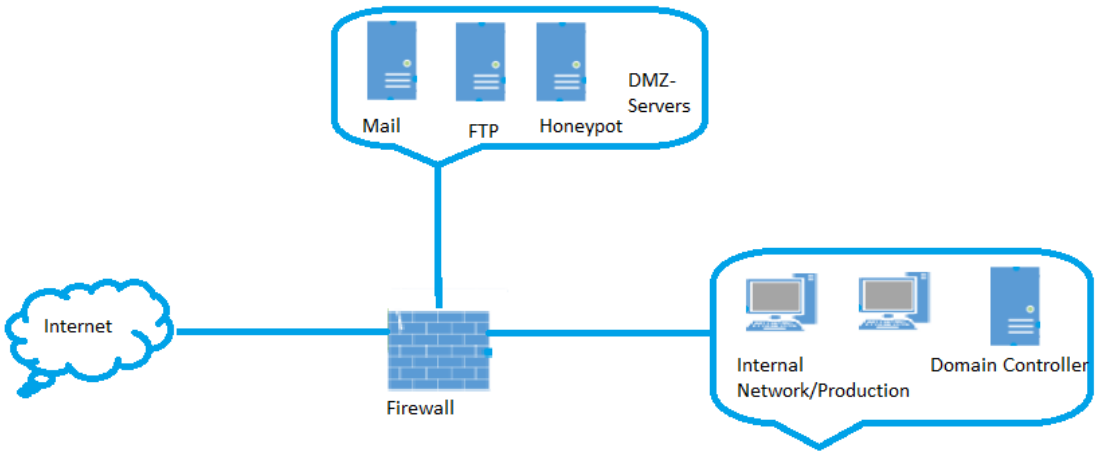
Η μέθοδος αυτή εφαρμόζεται κυρίως για ερευνητικούς σκοπούς προκειμένου να αναγνωρίσουν τις επιθέσεις που δέχεται ο οργανισμός από το διαδίκτυο. Πρόκειται για την καλύτερη μέθοδο, όταν ο σκοπός είναι η ανίχνευση και αναγνώριση των κυβερνοεπιθέσεων. Στην εξωτερική τοποθέτηση δεν υπάρχει τείχος προστασίας δηλαδή η επικοινωνία μεταξύ honeypot και διαδικτύου γίνεται χωρίς ασφάλεια. Το τείχος προστασίας δεν φιλτράρει αυτή την επικοινωνία και συνεπώς δεν το προστατεύει από τους κακόβουλους χρήστες. Για αυτήν την τοποθέτηση, χρειάζεται να δεσμευτεί μια δημόσια διεύθυνση διαδικτυακού πρωτοκόλλου στο μηχάνημα. Το σημαντικό σε αυτήν την μέθοδο είναι να μην υπάρχει επικοινωνία του honeypot με το εσωτερικό δίκτυο, καθώς αν ο host έχει παραβιαστεί και μολυνθεί, δεν θα διαδώσει τον ιό στον οργανισμό.



Εικόνα 2 Τοποθέτηση του Honeypot μπροστά από το τείχος προστασίας για την καλύτερη ανίχνευση των επιθέσεων

2.2.2 Τοποθέτηση του Honeypot πίσω από το τείχος προστασίας για την ανίχνευση των επιθέσεων που δεν αποτρέπει το τείχος προστασίας

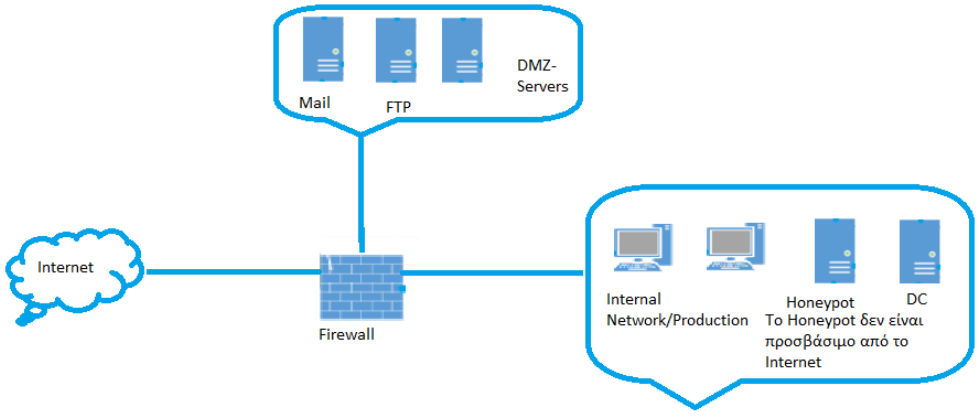
Η τοποθέτηση του honeypot πίσω από το τείχος προστασίας έχει στόχο την αναγνώριση των επιθέσεων, που δεν αντιλαμβάνεται το τείχος προστασίας ή δεν μπορεί να τις αποτρέψει. Σε αυτήν την μέθοδο το honeypot βρίσκεται στην αποστασιοποιημένη ζώνη DMZ[25], η οποία δεν έχει επικοινωνία με το εσωτερικό δίκτυο και του υπολογιστές της παραγωγής. Συνεπώς, η επίθεση ή κάποιο ιός (trojan[5]) θα περιοριστεί στην ζώνη αυτή και δεν θα επηρεάσει σημαντικά τον οργανισμό. Σε αυτήν την μέθοδο πρέπει να δεσμευτεί στο honeypot μία εσωτερική και μία εξωτερική διεύθυνση διαδικτυακού πρωτοκόλλου. Τέλος, με την συγκεκριμένη τοποθέτηση η ασφάλεια μίας εταιρίας βελτιώνεται καθώς αναλύοντας τις επιθέσεις, μπορούν να οργανώσουν καλύτερα την αρχιτεκτονική της ασφάλειας του δικτύου και να καλύψουν τα κενά ασφαλείας στο τείχος προστασίας της υποδομής τους.



Εικόνα 3 Τοποθέτηση του Honeypot πίσω από το τείχος προστασίας για την ανίχνευση των επιθέσεων που δεν αποτρέπει το τείχος προστασίας

2.2.3 Τοποθέτηση του Honeypot στο εσωτερικό δίκτυο για την ανίχνευση των σοβαρών επιθέσεων που θα πλήξουν την παραγωγή του οργανισμού

Ως τρίτη επιλογή, το Honeypot μπορεί να τοποθετηθεί στο εσωτερικό δίκτυο και σε αυτήν την περίπτωση να ανιχνεύσει τις επιθέσεις που θα προκαλέσουν μεγάλη ζημία στον οργανισμό. Το μεγάλης αλληλεπίδρασης honeypot βρίσκεται στο ίδιο δίκτυο με τα συστήματα παραγωγής και λειτουργεί σαν παγίδα καθώς ούτε οι επιτιθέμενοι ούτε οι χρήστες της εταιρίας θα γνωρίζουν την ύπαρξη του. Σε αυτό το σημείο θα μπορεί να αναγνωρίσει την διάδοση κάποιου ιού (worm[26]), την οριζόντια σάρωση θυρών, την σάρωση απαρίθμησης χρηστών στο πρωτόκολλο SMB και τις επιθέσεις ωμής βίας. Όπως έχουμε αναφέρει νωρίτερα, το Honeypot θα κρατάει στοιχεία για τη εσωτερική διεύθυνση διαδικτυακού πρωτόκολλου που ξεκίνησε η επίθεση, τον χρήστη που την πραγματοποίησε και το είδος της επίθεσης. Με αυτόν τον τρόπο μπορούμε να προλαμβάνουμε εγκαίρως, ποιος χρήστης ή υπολογιστής έχει μολυνθεί και παραβιαστεί. Το ψεύτικο σύστημα χρειάζεται μια εσωτερική διεύθυνση διαδικτυακού πρωτόκολλου και όχι εξωτερική καθώς δεν θα είναι προσβάσιμο από το διαδίκτυο.



Εικόνα 4 Τοποθέτηση του Honeypot στο εσωτερικό δίκτυο για την ανίχνευση των σοβαρών επιθέσεων που θα πλήξουν την παραγωγή του οργανισμού

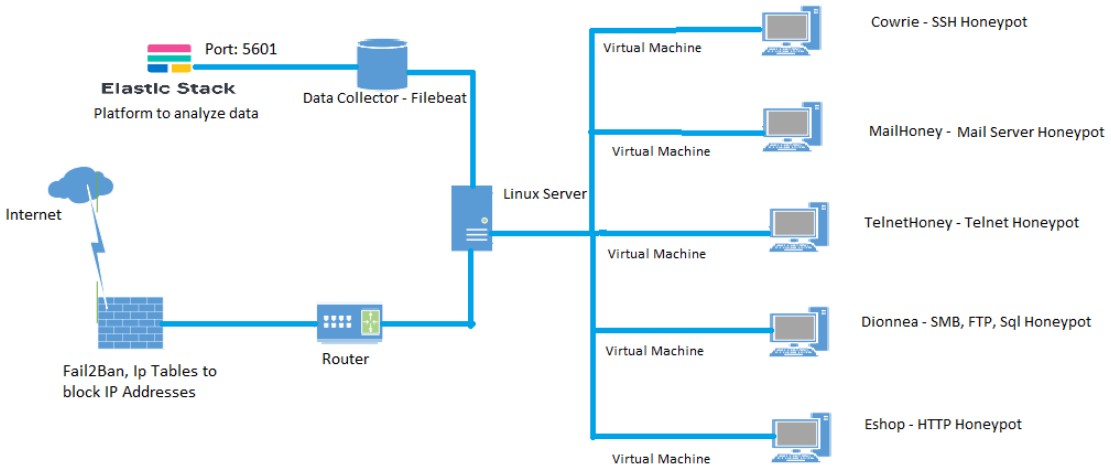
2.3 Αρχιτεκτονική του Honeypot

Στην παρούσα εργασία το υψηλής αλληλεπίδρασης honeypot που δημιουργήθηκε, αποτελείται από ένα δίκτυο Honeypots “Honeynet[27]”, τα οποία το καθένα ξεχωριστά συλλέγει πληροφορίες για την υπηρεσία-πόρτα που εξυπηρετεί. Τα παραπλανητικά συστήματα είναι απομονωμένα και δεν υπάρχει κανάλι επικοινωνίας μεταξύ τους. Το γεγονός ότι κάθε σύστημα έχει μια ανεξάρτητα στοίβα δικτύωσης και λειτουργεί αυτόνομα εξασφαλίζει περισσότερη ασφάλεια, καθώς αν παραβιαστεί ένα σύστημα από τον κακόβουλο χρήστη, δεν θα μπορεί να προχωρήσει την επίθεση σε άλλα συστήματα. Για την απομόνωση των συστημάτων χρησιμοποιήθηκε το λογισμικό Docker το οποίο υλοποιεί εικονοποίηση σε επίπεδο λειτουργικού συστήματος. Περισσότερες πληροφορίες για το λογισμικό Docker[28] και για την έκδοση που χρησιμοποιήθηκε αναλύονται στην επόμενη υποενότητα του κεφαλαίου.

Αρχικά, η τοποθέτηση του Honeypot είναι μπροστά από το τείχος προστασίας καθώς αποσκοπεί στην μελέτη και στην έρευνα των κυβερνοεπιθέσεων που λαμβάνουν χώρα στο διαδίκτυο. Όπως αναφέραμε και παραπάνω, στην τοποθέτηση αυτή δεν υπάρχει τείχος προστασίας που να φιλτράρει τις επιθέσεις που δέχεται. Για αυτό το λόγο είναι πολύ σημαντικό να οριστούν καταλλήλως τα δικαιώματα των χρηστών, σε ποια αρχεία του Server[29] έχουν πρόσβαση οι χρήστες και αν μπορούν να τα μορφοποιήσουν.

Στη συνέχεια λόγω της συγκεκριμένης τοποθέτησης, ο διακομιστής δέχεται πάρα πολλές επιθέσεις από το διαδίκτυο όπου αυτό αυξάνει τις απαιτήσεις του σε χωρητικότητα, σε μνήμη και σε επεξεργαστή. Για τις ανάγκες καταγραφής όλων αυτών των επιθέσεων και ανάλυση αυτών μέσω της πλατφόρμας ELK Stack, έχει νοικιαστεί από μία εταιρεία παροχής υπολογιστικών συστημάτων, ένας φυσικός Server[29] με υψηλές προδιαγραφές οι οποίες αναφέρονται στο επόμενο υποκεφάλαιο 2.4.

Για λόγους ασφάλειας, ο συγκεκριμένος διακομιστής επικοινωνεί μόνο με το router για να έχει πρόσβαση στο διαδίκτυο. Έχουν παρθεί μέτρα για την καλύτερη ασφάλεια του συστήματος όπως ο περιορισμός των δικαιωμάτων των χρηστών, η μεγάλη πολυπλοκότητα των κωδικών των χρηστών και η τεχνική απομόνωσης (containers[30]) προκειμένου να περιοριστεί ο κίνδυνος.



Εικόνα 5 Στην αρχιτεκτονική Honeypot που προτείνουμε, χρησιμοποιούνται virtual machines containers για παραπλάνηση των επιτηθέμενων, μία βάση δεδομένων για την αποθήκευση των στατιστικών στοιχείων (Filebeat- ElasticSearch) και ένα εργαλείο ανάλυσης των δεδομένων (Kibana)

Όπως φαίνεται στο διάγραμμα υπάρχουν πέντε ψεύτικα συστήματα, τα οποία το καθένα εξυπηρετεί διαφορετική υπηρεσία/ πόρτα. Το κάθε honeypot έχει μία ψεύτικη IP address[31] στο εσωτερικό δίκτυο και η πρόσβαση από το ίντερνετ γίνεται αν πληκτρολογήσει ο επιτιθέμενος την εξωτερική IP του server μαζί με την πόρτα του ψεύτικου συστήματος. Η εφαρμογή Docker που πραγματοποιεί την εικονοποίηση του λειτουργικού συστήματος, δημιουργεί ένα εικονικό δίκτυο το οποίο είναι το "172.16.0.0/16". Το κάθε κοντέινερ έχει μία εσωτερική IP address όπως "172.16.0.x". Το ψεύτικο αυτό εσωτερικό δίκτυο χρησιμοποιείται για την επικοινωνία της εφαρμογής Docker με το κοντέινερ, ωστόσο όπως έχουμε ξανά αναφέρει δεν υπάρχει επικοινωνία μεταξύ των ψεύτικων συστημάτων. Το εσωτερικό αυτό δίκτυο, που δημιουργεί η εφαρμογή Docker, δημιουργεί ένα κανάλι επικοινωνίας του συστήματος με τα κοντέινερ με σκοπό να δίνουμε εντολές στα ψεύτικα συστήματα, να συλλέγουμε τα δεδομένα και τις πληροφορίες που μας παρέχουν.

Αφού έχουμε συλλέξει τα δεδομένα, που βρίσκονται στην διαδρομή "/var/lib/docker/containers/…/…[dot]log", μεταφέρονται στο “elk stack” με το πρόγραμμα “Filebeat”. Το “Filebeat” είναι μία υπηρεσία που μεταφέρει τα δεδομένα σε μορφή που μπορούν να αποκωδικοποιηθούν από το “Logstash”. Ο ρόλος του είναι πολύ σημαντικός, γιατί συλλέγει τα δεδομένα από πολλά αρχεία, συμπυκνώνει αρχεία πολλών GB και απελευθερώνει χώρο από το server. Αναλυτικότερα, για τη λειτουργία του και περισσότερες τεχνικές λεπτομέρειες αναγράφονται παρακάτω.

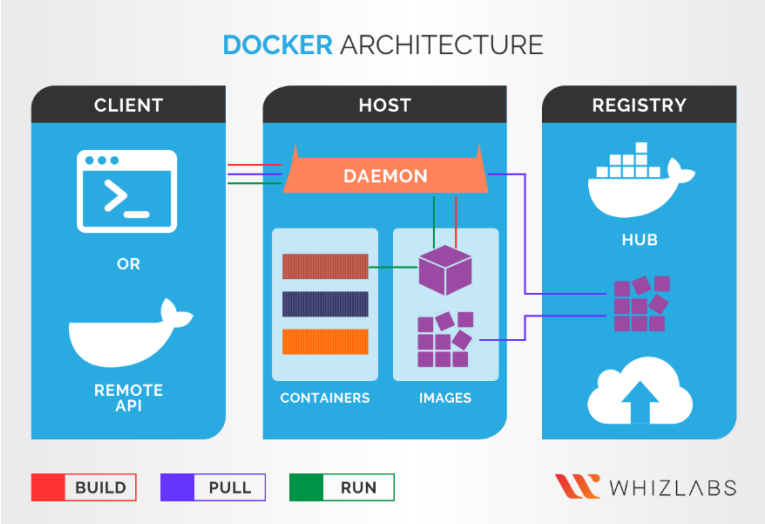
Στη συνέχεια, κάνουμε ανάλυση των επιθέσεων στην πλατφόρμα “Elasticsearch” και καταλαβαίνουμε ποιοι είναι οι επιτιθέμενοι, από ποιες χώρες έχουν πραγματοποιήσει την επίθεση, τι αποσκοπεί η επίθεση κι αν οι μέθοδοι που χρησιμοποιεί μπορούν να βλάψουν και να παραβιάζουν το σύστημά μας. Επίσης, το πρόγραμμα Kibana μας βοηθάει να δούμε την ευρύτερη εικόνα των κυβερνοεπιθέσεων καθώς δημιουργεί διαγράμματα για τα δεδομένα που έχουν αναληφθεί. Κατά κύριο λόγο το διάγραμμα των IP διευθύνσεων πού προήλθαν οι επιθέσεις, τα προγράμματα που

χρησιμοποιήθηκαν και οι κωδικοί που πληκτρολογήθηκαν είναι τα πιο σημαντικά για να βγάλουμε συμπεράσματα.

Τέλος η πρόσβαση από το διαδίκτυο στον διακομιστή ή σε κάποιο ψεύτικο σύστημα φιλτράρεται από το "fail2ban[32]", ένα πρόγραμμα το οποίο είναι δωρεάν και με τις πολιτικές που έχουμε ορίσει μπλοκάρει τις IP διευθύνσεις που έχουνε κάνει παραπάνω από εκατό αποτυχημένες αυθεντικοποιήσεις. Με αυτό τον τρόπο θέλουμε να πιάσουμε και να αναλύσουμε τις επιθέσεις, οι οποίες είναι έξυπνες και αποτελεσματικές και περιορίζουμε τον αριθμό των επιθέσεων που χρησιμοποιούν τον αλγόριθμο ωμής βίας (Brute Force Attack). Μέχρι εκατό κακόβουλες προσπάθειες μπορούμε να αντιληφθούμε αν μία IP διεύθυνση κατηγοριοποιείται ως επικίνδυνη και την μπλοκάρουμε για να μην επιβαρύνει περισσότερο τον διακομιστή καθώς θέλουμε να εστιάσουμε στις άλλες έξυπνες επιθέσεις. Επιπρόσθετα, χρησιμοποιείται η υπηρεσία του "Linux Iptables[21]" στο οποίο χειροκίνητα προσθέτουμε IP διευθύνσεις, οι οποίες έχουν χαρακτηριστεί ως κακόβουλες.

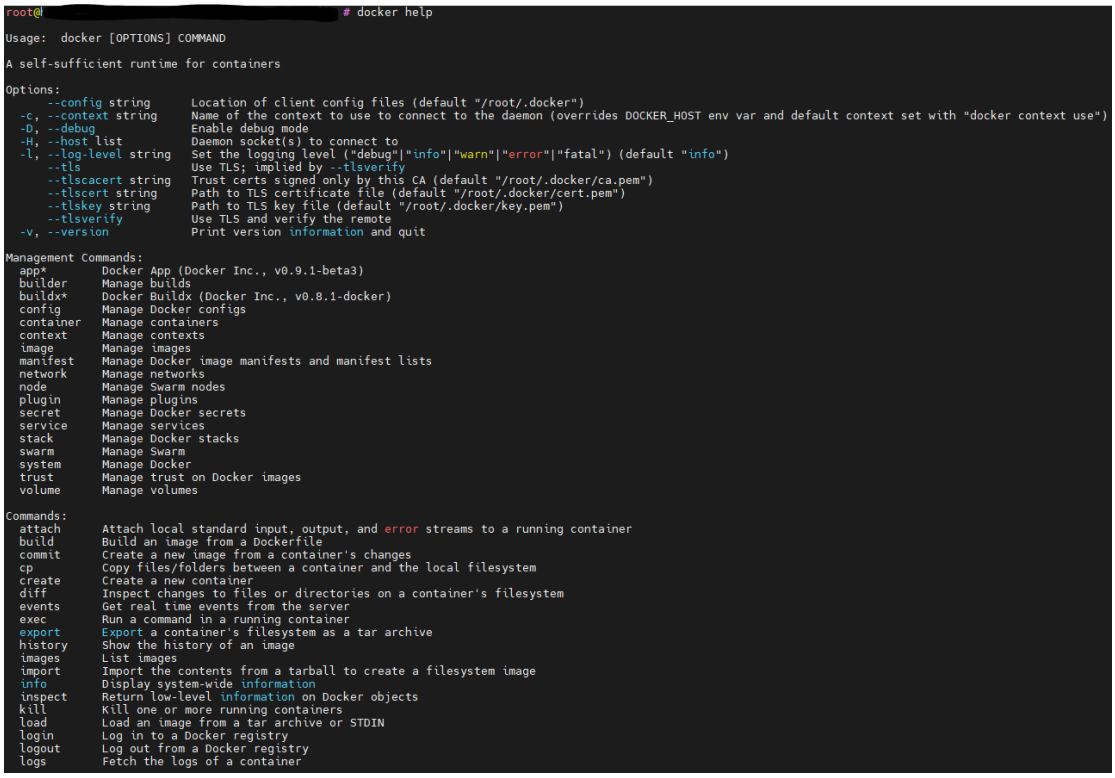
2.3.1 Ανάλυση του προγράμματος Docker

Το Docker είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα, που υλοποιεί εικονικοποίηση (Virtualization) σε επίπεδο λειτουργικού Συστήματος. Το Docker προσφέρει αυτοματοποιημένες διαδικασίες για την ανάπτυξη εφαρμογών σε απομονωμένες περιοχές χρήστη που ονομάζονται Software Containers. Το λογισμικό χρησιμοποιεί τεχνολογίες του πυρήνα του Linux όπως τα "cgroups[32]" και οι χώροι ονομάτων πυρήνα, για να επιτρέπει σε ανεξάρτητα "Software containers" να εκτελούνται στο ίδιο λειτουργικό σύστημα. Έτσι αποφεύγεται η χρήση επιπλέον υπολογιστικών πόρων που θα απαιτούσε μια εικονική μηχανή "virtual machine[33]".



Εικόνα 6 Αρχιτεκτονική Docker

Η έκδοση του Docker που χρησιμοποιήθηκε για την παρούσα εργασία είναι η "20.10.6" και για να δούμε την έκδοση χρησιμοποιήθηκε η εντολή "docker version". Η εφαρμογή έχει δικιά της γλώσσα προγραμματισμού είναι ευκολονόητη για τους χρήστες της καθώς οι εντολές που χρησιμοποιεί είναι απλές λέξεις του αγγλικού λεξιλογίου που αντικατοπτρίζουν τις ενέργειες που θέλουμε να κάνουμε.



Εικόνα 7 Μενού εντολών του προγράμματος docker

Όπως φαίνεται στην παραπάνω φωτογραφία με την εντολή "*docker help*" βλέπουμε όλες τις διαθέσιμες εντολές που μπορούμε να πληκτρολογήσουμε μετά την λέξη docker. Οι εντολές που χρησιμοποιούνται πιο συχνά είναι οι "*docker pull*", "*docker run*", "*docker build*" οι οποίες ανάλογα με τις ενέργειες, που πρέπει να κάνει ο χρήστης ακολουθούνται από τις κατάλληλες παραμέτρους. Η εντολή "*docker pull*" χρησιμοποιείται για να κατεβάσουν οι χρήστες ένα έτοιμο docker container από τη βάση δεδομένων του docker hub, στο οποίο η κοινότητα του Docker ανεβάζει διάφορες εφαρμογές, σε μορφή containers. Η εντολή "*docker Run*" χρησιμοποιείται για να τρέξει ένα container και η σημαντικότερη παράμετρος του είναι "-p" η οποία ορίζει την πόρτα που θα ακούει το container. Τέλος, η εντολή "*docker build*" χρησιμοποιείται για να φτιάξουμε ένα καινούργιο κοντέινερ.

2.3.2 Ανάλυση του SSH Honeypot

Το ssh-honeypot δημιουργήθηκε το 2016 και αποτελεί την εξελιγμένη εκδοχή του πολύ γνωστού Honeypot Kippo[34]. Η αρχιτεκτονική του και οι μέθοδοι που χρησιμοποιεί για να πιάσει τους επιτιθέμενους βασίζονται κατά κύριο λόγο στο Kippo αλλά με περισσότερες και πιο προηγμένες τεχνικές. Εξυπηρετεί στην πόρτα 22/SSH και είναι ένα από τα πιο σημαντικά Honeypot που έχουν δημιουργηθεί καθώς οι επιτιθέμενοι χρησιμοποιούν την υπηρεσία SSH, για να μπούν στο υπολογιστικό μηχάνημα με δικαιώματα χρήστη ή διαχειριστή. Την υπηρεσία αυτήν, την χρησιμοποιούν συνήθως υπολογιστικά συστήματα που έχουν λογισμικό Unix/Linux και συνήθως είναι Server's. Το να παραβιάσει ο επιτιθέμενος τον κωδικό ενός χρήστη στην υπηρεσία SSH και με διάφορες εντολές να αποκτήσει δικαιώματα ιδιοκτήτη, είναι από τις πιο συνήθεις επιθέσεις και θα παρατηρηθεί αυτό και στα δεδομένα που παρατίθενται στο τέταρτο

κεφάλαιο. Όπως φαίνεται στην εικόνα 4, το πλήθος των επιθέσεων στο συγκεκριμένο κοντέινερ είναι πολύ μεγαλύτερο από ότι τα υπόλοιπα λόγω της κρισιμότητας αν παραβιαστεί.

Εικόνα 8 Χάρτης με τις επιθέσεις που δέχεται το SSH Honeypot

Όταν κάποιος επιτιθέμενος πληκτρολογήσει την IP Address του δικού μας Honeypot και την πόρτα 22 θα εμφανιστεί να πληκτρολογήσει το όνομα χρήστη και τον κωδικό του. Αφού έχουμε ορίσει εμείς στο αρχείο ρυθμίσεων (configuration file) τους κωδικούς και τους χρήστες που είναι επιτρεπτά για να εισέλθουν στο κοντέινερ και πληκτρολογήσουν κάποιους από αυτούς εισέρχονται σε ένα ψεύτικο σύστημα. Αυτό το σύστημα είναι διαμορφωμένο με τέτοιο τρόπο, ώστε οι επιτιθέμενοι να νομίζουν ότι πρόκειται για αληθινό σύστημα. Ωστόσο το σύστημα δεν μπορεί να παρέχει πληροφορίες και ευαίσθητα δεδομένα στον επιτιθέμενο και από αυτό δεν έχει πρόσβαση στο αληθινό σύστημα.

Σημαντικές πληροφορίες για το τι μας παρέχει ssh-honeypot είναι:

1) Ποιοι είναι οι πιο συχνοί κωδικοί που χρησιμοποιούνται σε επιθέσεις ωμής βίας
2) Τα πιο συχνά ονόματα χρηστών που χρησιμοποιούνται σε επιθέσεις της βίας
3) Ποιες είναι οι χώρες με τις περισσότερες επιθέσεις προς το σύστημά μας

```
Command found: crontab -l
Command found: ls -lh /bin/ls
Command found: cat /proc/cpuinfo
Command found: rm -rf .ssh\n
Command found: mkdir .ssh\n","stream":"stdout","time":"2021-01-29T15:12:47.246040397Z"}
Command found: echo ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEArDp4cun2lhr4KUhBGE7VvAcwdli2a8dbnrTOrbMz1+5O73fcBOx8NVbUT0bUa
nUV9tJ2/9p7+vD0EpZ3Tz/+0kX34uAx1RV/75GVOmNx+9EuWOnvNoaJe0QXxziIg9eLBHpgLMuakb5+BgTFB+rKJAw9u9FSTDengvS8hX1kNFS4Mjux0hJOK8rvcEmP
ecjdySYMb66nylAKGwCEE6WEQHmdlmUPgHwGQ0hWCwsQk13yCGPK5w6hYp5zYkFnvlC8hGmd4Ww+u97k6pfTGTUbJk14ujvcD9iUKQTTWYYjIIu5PmUux5bsZ0R4WFw
dIe6+i6rBLAsPKgAySVKPRK+oRw== mdrfckr \u003e\u003e .ssh/authorized_keys
Command found: echo root:DJdFscFslnh6
login attempt [b'nproc'/b'nproc'] failed
login attempt b'root' failed auth b'password123!@#'\ failed
login attempt b'root' failed auth b'password!@#'\ failed
login attempt b'root' failed auth b'qwerty!'\ failed
login attempt b'root' failed auth b'james'\ failed
login attempt b'root' failed auth b'james123'\ failed
```

Εικόνα 9 Εντολές που πληκτρολογούνται από τους επιτηθέμενους στο SSH Honeypot

2.3.3 Ανάλυση του Mailoney Honeypot

Το Mailoney Honeypot εξυπηρετείται στην πόρτα 25 δηλαδή στο πρωτόκολλο SMTP και αποτελεί ένα από τα πιο σημαντικά honeypot καθώς μας προσφέρει πληροφορίες για τις επιθέσεις ψαρέματος. Ουσιαστικά, είναι ένας mail διακομιστής και οι επιτιθέμενοι μπορούν να έχουν πρόσβαση σε αυτόν χωρίς να πληκτρολογήσουν όνομα χρήστη και κωδικό. Σε αυτό το σημείο, οι επιτιθέμενοι καταλαβαίνουν ότι έχουν πρόσβαση και μπορούν να στείλουν κακόβουλα e-mails σε διάφορους αποστολείς.

Ο Mail server περιέχει δικές του εντολές που αναγράφονται παρακάτω οι οποίες χρησιμοποιούνται από τους χάκερς για να στείλουν ύποπτα e-mails που περιέχουν κακόβουλα αρχεία προκειμένου να αποσπάσουν πληροφορίες και να εξαπατήσουν χρήστες άλλων οργανισμών.

Οι πληροφορίες που μας παρέχει το Mailoney είναι:

1. οι IP διευθύνσεις που προσπαθούν να στείλουν κακόβουλα e-mails
2. τα κακόβουλα αρχεία που στέλνουνε ως συνημμένα
3. το email του κακόβουλου αποστολέα
4. το subject του e-mail
5. το κείμενο του email προκειμένου να δελεάσει τον παραλήπτη

Έχοντας όλα αυτά τα δεδομένα βγάζουμε συμπεράσματα για τις πιο δημοφιλείς και συχνότερες τεχνικές της επίθεσης κοινωνικής μηχανικής (Social Engineering[35]). Η επίθεση αυτή είναι με βάση στατιστικών πάνω από το 80% των κυβερνοεπιθέσεων που δέχονται οι οργανισμοί και οι εταιρείες. Γνωρίζοντας λοιπόν όλα αυτά τα δεδομένα βγάζουμε συμπεράσματα για τις μεθόδους που προσπαθούν να προσελκύσουν οι χάκερς άλλους χρήστες προκειμένου να τους δώσουν τους κωδικούς τους και τα προσωπικά δεδομένα τους.

Παρακάτω αναγράφονται οι εντολές που πληκτρολογούνται στο mail honeypot:

1. HELO/EHLO || απάντηση του server καταχωρώντας την IP Address και το domain που είναι εγγεγραμμένος.
2. MAIL FROM “το email του αποστολέα”
3. RCPT TO “το email του παραλήπτη”
4. DATA || τα δεδομένα που δέχεται ο server για να στείλει το email.
5. NOOP || επιστρέφει το server status response

6. HELP || εμφανίζει το μενού των εντολών
7. VRFY “username” || ελέγχει αν ο χρήστης υπάρχει στην βάση δεδομένων
8. RSET || reset τον mail server (δεν έχουν πρόσβαση οι επιτιθέμενοι)
9. QUIT || έξοδος από τον mail server

2.3.4 Ανάλυση του Dionaea Honeypot

Το συγκεκριμένο honeypot είναι ένα υψηλής αλληλεπίδρασης honeypot καθώς εξυπηρετεί πολλά πρωτόκολλα και υπηρεσίες, ωστόσο για την παρούσα εργασία έχουν χρησιμοποιηθεί το πρωτόκολλο ftp, tftp, mysql και smb. Ο σκοπός αυτού είναι να μας παρέχει δεδομένα και πληροφορίες για κακόβουλα αρχεία που τοποθετούνται στη βάση δεδομένων του honeypot. Εκτός από την υπηρεσία mysql όλες οι υπόλοιπες δελεάζουν τους κακόβουλους χρήστες να αποθηκεύσουν κακόβουλα αρχεία στη βάση δεδομένων με σκοπό να εκτελεστούν από άλλους χρήστες και να μολυνθεί το δίκτυο.

Επίσης η υπηρεσία smb είναι η πιο ενδιαφέρουσα καθώς σχετίζεται με τις επιθέσεις ransomware σε οργανισμούς. Το αρχείο ransomware έχει προγραμματιστεί ώστε να μολύνει κατά την εκτέλεση του το παρόν σύστημα να υποκλέψει τα στοιχεία των χρηστών που είναι συνδεδεμένοι στο σύστημα και στη συνέχεια να διαδίδει το τον ιό trojan στο δίκτυο. Στη συνέχεια κρυπτογραφεί τα δεδομένα του συστήματος, τα στέλνει σε εξωτερικούς servers και οι εγκληματίες ζητούν χρηματικό ποσό προκειμένου να αποκρυπτογραφήσουν τα δεδομένα. Σε αυτήν την επίθεση πού έχει επηρεάσει πάρα πολλούς οργανισμούς ανά όλο τον κόσμο μπορούμε τα δεδομένα μας βλέποντας τις IP διευθύνσεις, τις χώρες και όλα τα δεδομένα που μας παρέχονται από το Dionaea να συνεισφέρουμε στην αντιμετώπιση του ransomware attack κατά την δημοσιοποίηση των δεδομένων που σχετίζονται με αυτές τις επιθέσεις.

2.4 Τεχνικά Χαρακτηριστικά του Server

Όπως είπαμε και προηγουμένως για να ικανοποιηθούν όλες αυτές οι ανάγκες που αναφέρεται στο προηγούμενο κεφάλαιο έχει ενοικιαστεί από μία εταιρεία παροχής υπολογιστικών συστημάτων, ένας διακομιστής με πολλή μνήμη RAM προκειμένου να καλύψει όλες τις ανάγκες χωρίς προβλήματα. Διαθέτει λειτουργικό σύστημα Linux Debian και συγκεκριμένα η έκδοση του είναι "Linux 4.19.0-16-amd64 SMP Debian 4.19.181-1 x86_64 GNU/Linux".

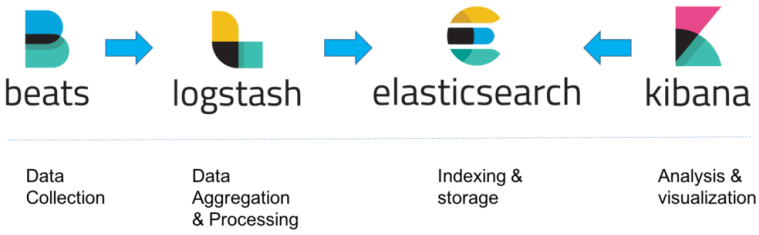
Τα τεχνικά του χαρακτηριστικά είναι:

1) Επεξεργαστής: Intel Core i7-920, Core:8, Threads pre Core:2
2) Σκληρός Δίσκος: 618 GB
3) Μνήμη RAM: 12 GB

Τα προγράμματα της συλλογής των δεδομένων όπως Filebeat, Logstash, Kibana και Elasticsearch καταναλώνουν τους περισσότερους πόρους του συστήματος καθώς χρησιμοποιούν το 50% της μνήμης RAM του συστήματος και ακόμη ένα 20% της μνήμης RAM χρησιμοποιεί εφαρμογή Docker για την ενεργοποίηση των Honeypots.

2.5 Συλλογή Δεδομένων

Σε αυτήν την ενότητα του υποκεφαλαίου θα μιλήσουμε για τον τρόπο κωδικοποίησης, μετατροπής και εμφάνισης των δεδομένων από τα honeypots στην πλατφόρμα Elastic Search. Όπως φαίνεται στην εικόνα παρακάτω τα τέσσερα αυτά εργαλεία παίζουν διαφορετικό ρόλο, ξεκινώντας από το Filebeat το οποίο είναι υπεύθυνο για τη συλλογή δεδομένων από τα κοντείνερ. Στο αρχείο ρύθμισης ορίζουμε τις διαδρομές των αρχείων των containers για να πάρουμε τα δεδομένα, τα οποία βρίσκονται στην εξής θέση "/data/nameofcontainer/nameofcontainer.log", τον χρόνο που θα ανανεώνει τα δεδομένα και τέλος τα στοιχεία πρόσβασης στην πλατφόρμα του “ELK stack”.

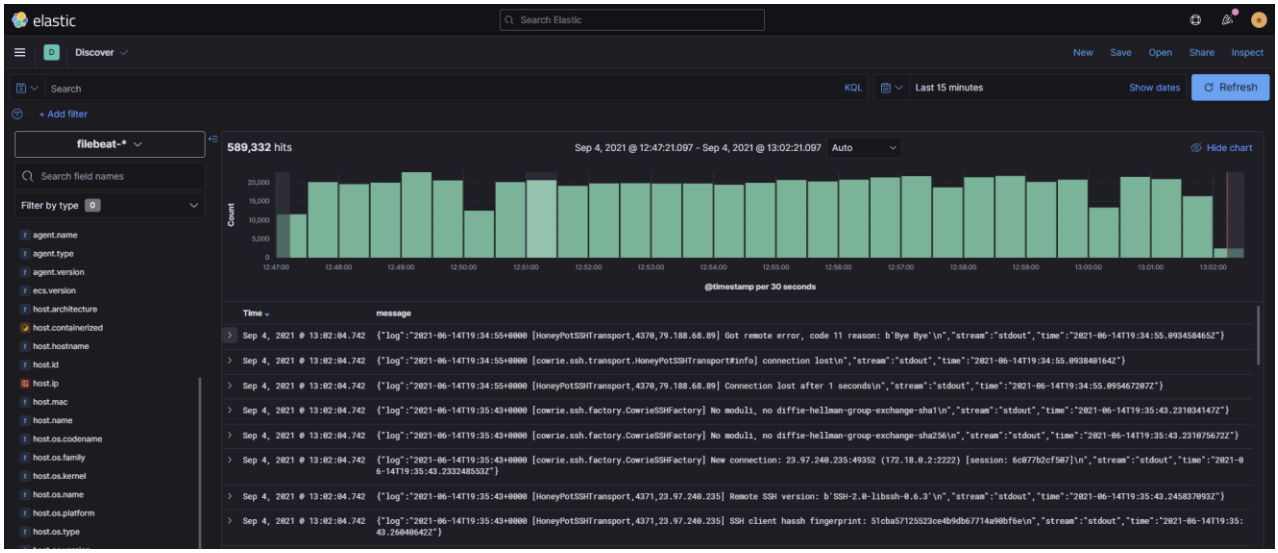


Εικόνα 10 Αρχιτεκτονική Συλλογής Δεδομένων

Στη συνέχεια τα δεδομένα μεταφέρονται στο Logstash το οποίο φιλτράρει τα δεδομένα και τα επεξεργάζεται σε τέτοια μορφή πού να την καταλαβαίνει το Elasticsearch. Σε αυτό το σημείο να σημειωθεί πως έχουν δημιουργηθεί φίλτρα προκειμένου τα δεδομένα από τα containers να απεικονίζονται σωστά στην πλατφόρμα. Τα αρχεία logs που παίρνουμε βρίσκονται σε μορφή json. Τα φίλτρα έχουν σχεδιαστεί έτσι ώστε να κρατάμε από την πληροφορία μόνο την source IP, την χώρα πού προήλθε η επίθεση, την Mac Address[36] του επιτιθέμενου και το payload[37] της επίθεσης το οποίο διαφέρει σε κάθε honeypot.

Αφού φιλτραριστεί η πληροφορία μεταφέρεται στο Elastic Search όπου αποθηκεύεται στην τοπική βάση δεδομένων. Το Elastic Search είναι μια μηχανή αναζήτησης και ανάλυσης που έχει αναπτυχθεί στην γλώσσα προγραμματισμού Java. Μας επιτρέπει να αποθηκεύσουμε, να αναζητούμε και να αναλύουμε τεράστιους όγκους δεδομένων γρήγορα και σε σχεδόν πραγματικό χρόνο. Με συγκεκριμένους όρους αναζήτησης μπορούμε να βρούμε σε πολύ μικρό χρόνο πόσες επιθέσεις έχουν πραγματοποιηθεί από μία χώρα, από μία IP address, πόσες φορές έχει χρησιμοποιηθεί ένας κωδικός σε επιθέσεις ωμής βίας και άλλα πολλά τα οποία απεικονίζονται με διαγράμματα στην πλατφόρμα Elasticsearch μέσω του προγράμματος Kibana.

Το Kibana είναι ένα εργαλείο απεικόνισης και διαχείρισης δεδομένων για το Elasticsearch που παρέχει ιστογράμματα σε πραγματικό χρόνο, γραφήματα γραμμών, διαγράμματα πίτας και χάρτες. Επίσης μπορούμε να οπτικοποιήσουμε τα δεδομένα Elasticsearch, μπορούμε να επιλέξουμε τα φίλτρα και την ερώτηση με βάση το οποίο θα φτιαχτεί το διάγραμμα. Με την δια δραστική απεικόνιση μπορούμε να έχουμε έλεγχο του συστήματος εύκολα και γρήγορα και βλέπουμε συγκεντρωτικά τα δεδομένα των κυβερνοεπιθέσεων.



Εικόνα 11 Πλατφόρμα του Elasticsearch

Κεφάλαιο 3. Σχεδίαση, Ρύθμιση και Υλοποίηση του Honeypot

3.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζονται λεπτομέρειες για την ανάπτυξη ενός υψηλού αλληλεπίδρασης Honeypot. Περιγράφονται οι απαιτήσεις του συστήματος για την υλοποίηση του, αναλύεται η αρχιτεκτονική του εφαρμοζόμενου λογισμικού και εξηγούνται σημαντικές σχεδιαστικές αποφάσεις. Παρέχονται βήματα εγκατάστασης και διαμόρφωσης των προγραμμάτων στον διακομιστή, στα παραπλανητικά συστήματα που υλοποιήθηκαν μέσω του προγράμματος docker και της πλατφόρμας "ELK Stack" που είναι υπεύθυνη για την διάδοση και οπτικοποίηση των δεδομένων.

3.2 Προ απαιτούμενες ρυθμίσεις του διακομιστή

Το πρώτο βήμα στην υλοποίηση και στη σχεδίαση του καινούργιου Honeypot είναι η ρύθμιση του λειτουργικού συστήματος του διακομιστή μας, ώστε να έχει τις κατάλληλες απαιτήσεις για να υποστηρίξει τα παραπλανητικά συστήματα αλλά και την πλατφόρμα ELK Stack η οποία θα δει τα δεδομένα. Για την παρούσα διπλωματική επιλέχθηκε το λειτουργικό σύστημα "Linux Debian 10" γιατί το συγκεκριμένο λειτουργικό είναι ανοιχτού κώδικα και μπορεί να γίνει αλλαγή των ρυθμίσεων του συστήματος. Επίσης μας προσφέρει ασφάλεια, σταθερότητα και ευελιξία στο σύστημα μας. Εκτελώντας την εντολή *"uname -a"* βλέπουμε την έκδοση του λειτουργικού η οποία είναι " Linux XXX 5.10.0-9-amd64 #1 SMP Debian 5.10.70-1 (2021-09-30) x86_64 GNU/Linux".

Αρχικά για την υλοποίηση του συστήματος, έγινε ενημέρωση και εγκατάσταση πολλών προγραμμάτων/βιβλιοθηκών από το αποθετήριο λογισμικού των "Linux Debian". Οι εντολές που εκτελέστηκαν είναι:

- *apt-get update* || Ενημέρωση αποθετηρίου λογισμικού του λογισμικού Debian
- *apt-get upgrade*
- *apt-get install -y python* || Εγκατάσταση της γλώσσας προγραμματισμού python
- *apt install python-virtualenv* || Εγκατάσταση του ψεύτικου περιβάλλοντος της γλώσσας python
- *apt-get install -y –force-yes php7.0 php7.0-dev* || Εγκατάσταση της γλώσσας προγραμματισμού php
- *pip install flask* || Εγκατάσταση της βιβλιοθήκης flask για την εκτέλεση του hpfeeds 3.0, το οποίο χρησιμοποιείται για την λειτουργία του open_relay Email Server
- *apt install telnet* || Εγκατάσταση της υπηρεσίας telnet
- *apt install fail2ban* || Εγκατάσταση της υπηρεσίας fail2ban για την αποτροπή των επιθέσεων
- *apt install cockpit* || Εγκατάσταση της υπηρεσίας cockpit η οποία είναι διαχειριστικό εργαλείο για linux διακομιστές
- *apt install git* || Εγκατάσταση της υπηρεσίας git για να εύκολη πρόσβαση σε κώδικες από την ιστοσελίδα "GitHub.com"

3.2.1 Εγκατάσταση της υπηρεσίας Fail2ban

Το Fail2ban είναι ένα αμυντικό εργαλείο, το οποίο σαρώνει αρχεία καταγραφής του διακομιστή και αποκλείει IP διευθύνσεις που εμφανίζουν κακόβουλες ενδείξεις όπως πάρα πολλές αποτυχίες κωδικών πρόσβασης, αναζήτηση εκμεταλλεύσεων κ.λπ. Το Fail2Ban χρησιμοποιείται για την ενημέρωση των κανόνων του τείχους προστασίας για την απόρριψη των διευθύνσεων IP για συγκεκριμένο χρονικό διάστημα. Η εγκατάσταση του σε συστήματα Linux γίνεται με την "*apt install fail2ban*" και για την ενεργοποίηση της υπηρεσίας εκτελείται η εντολή "*service fail2ban start*". Όπως φαίνεται στην Εικόνα 11 ο χρήστης μπορεί να ρυθμίσει, από το αρχείο που συνήθως βρίσκεται στην διαδρομή " /etc/fail2ban/jail.conf", την διάρκεια που θα είναι μπλοκαρισμένη η IP διεύθυνση, τον αριθμό των αποτυχημένων προσπαθειών πριν μπλοκαριστεί και σε ποιες υπηρεσίες/πόρτες θα λειτουργεί το τείχος προστασίας.

Στην παρούσα εργασία, οι χρόνοι αποκλεισμού αυξήθηκαν από ότι οι προεπιλεγμένες ρυθμίσεις γιατί μας ενδιαφέρουν οι έξυπνες επιθέσεις και όχι οι επιθέσεις ωμής βίας:

- Η διάρκεια που γίνεται μπλοκ η IP είναι: 1 day
- Ο μέγιστος αριθμός αποτυχημένων προσπαθειών είναι: 5
- Ο χρόνος μέχρι ο αριθμός αποτυχημένων προσπαθειών να μηδενιστεί είναι: 1day
- Υπηρεσίες: SSH, HTML, Telnet, Mail, κτλ..

```
# "bantime" is the number of seconds that a host is banned.
bantime  = 1d

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 1d

# "maxretry" is the number of failures before a host get banned.
maxretry = 5
```

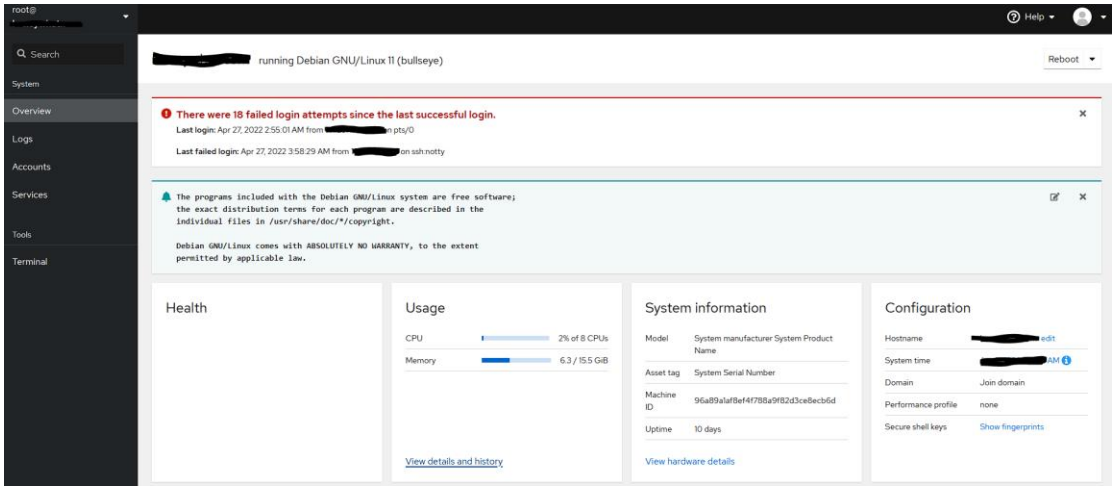
Εικόνα 11. Ρυθμίσεις στο τείχος προστασίας Fail2ban

3.2.2 Εγκατάσταση της υπηρεσίας Cockpit

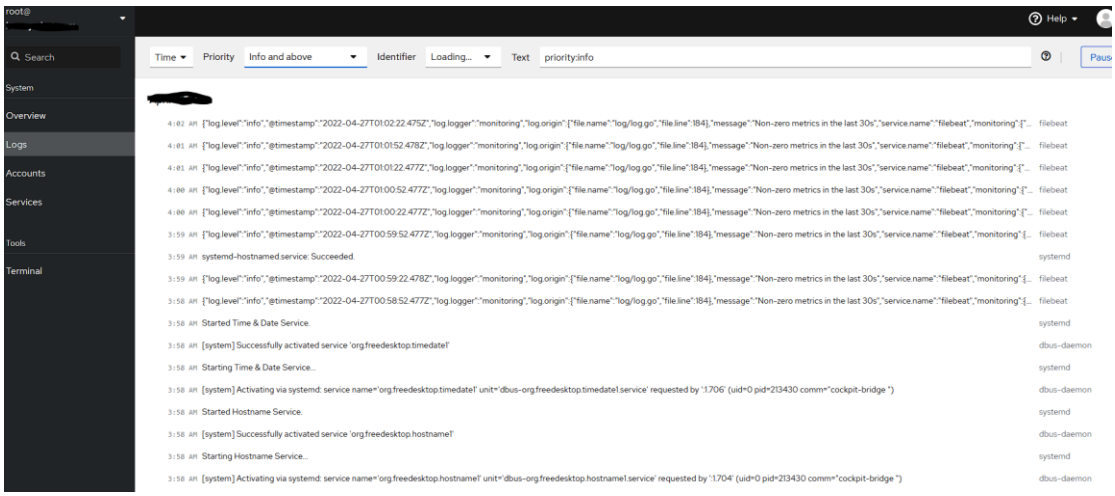
Το Cockpit είναι διαχειριστικό εργαλείο το οποίο είναι εύκολο για τον χρήστη και πιο κατανοητό σε σύγκριση από την γραμμή εντολών του Linux "Bash". Συγκεκριμένα το Cockpit προσφέρει:

1. Έλεγχο και τροποποίηση των ρυθμίσεων του δικτύου.
2. Διαμόρφωση ενός τείχους προστασίας.
3. Διαχείριση αποθηκευτικού χώρου.
4. Δημιουργία και διαχείριση εικονικών μηχανών/κοντέινερ.
5. Περιήγηση και αναζήτηση σε αρχεία καταγραφής συστήματος
6. Αναβάθμιση Λογισμικού
7. Παρακολούθηση και έλεγχος της απόδοσης της μνήμης RAM, επεξεργαστή.
8. Εκτέλεση απομακρυσμένης γραμμής εντολών "Bash".

Για την εγκατάσταση του εκτελέστηκε η εντολή "*apt install cockpit*" και να τρέξει η υπηρεσία, η εντολή "*service cockpit start*". Σε περίπτωση αποτυχίας της υπηρεσίας να ξεκινήσει, ο χρήστης με την εντολή "*service cockpit status*" βλέπει το πρόβλημα και προχωράει στην αποσφαλμάτωση (Troubleshoot) του. Στην εικόνα 12 και 13 εμφανίζονται οι δυνατότητες του λογισμικού.



Εικόνα 12 Η διαχειριστική πλατφόρμα Cockpit



Εικόνα 13 Περιήγηση και αναζήτηση σε αρχεία καταγραφής συστήματος

3.2.3 Εγκατάσταση της υπηρεσίας Filebeat

Το Filebeat είναι ένας ελαφρύς πράκτορας για προώθηση και συγκέντρωση δεδομένων καταγραφής. Είναι εγκατεστημένο ως υπηρεσία στον διακομιστή και παρακολουθεί τα αρχεία καταγραφής, συλλέγει συμβάντα καταγραφής και τα προωθεί είτε στο Elasticsearch, είτε στο Logstash για ευρετηρίαση. Σε αντίθεση με το ELK Stack (Elasticsearch/Logstash/Kibana) που υλοποιήθηκαν σε κοντέινερ, το Filebeat εγκαταστάθηκε ως υπηρεσία καθώς η συνεργασία του με το πρόγραμμα Docker δεν είναι εφικτή και βρίσκεται σε πειραματικό στάδιο.

Για την εγκατάσταση και την ρύθμιση του Filebeat εκτελέστηκαν οι εντολές:

- *curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-Version-amd64.deb* ||
- *sudo dpkg -i filebeat-8.1.3-amd64.deb* || εγκατάσταση του πακέτου.
- *filebeat modules list* || λίστα με τις έξτρα λειτουργείες που θα χρησιμοποιήσουμε
- *filebeat modules enable kibana logstash elasticsearch* || ενεργοποίηση δυνατοτήτων
- *nano /etc/filebeat/filebeat.yml* || ρύθμιση της υπηρεσίας, ορίζοντας τα στοιχεία πρόσβασης προς το ELK Stack και τις διαδρομές των αρχείων που στέλνουμε για ανάλυση
- *filebeat setup -e* || εγκατάσταση στο Elasticsearch προεπιλεγμένων γραφημάτων, πινάκων κτλ.
- *sudo service filebeat start* || εκκίνηση υπηρεσίας.

3.2.4 Εγκατάσταση του προγράμματος Docker

Το Docker είναι μια πλατφόρμα λογισμικού ανοιχτού κώδικα που υλοποιεί εικονικοποίηση σε επίπεδο Λειτουργικού Συστήματος. Ουσιαστικά το Docker προσφέρει αυτοματοποιημένες διαδικασίες για την ανάπτυξη εφαρμογών σε απομονωμένες περιοχές Χρήστη που ονομάζονται Software Containers.

Τα βασικά του τμήματα είναι:

1. το dockerfile: εκτελέσιμο αρχείο που παρέχει πληροφορίες για το κοντέινερ που θα δημιουργηθεί
2. το image: αρχείο που χρησιμοποιείται για να εκτελεστεί ο κώδικας του κοντέινερ
3. το κοντέινερ: το κοντέινερ μέσα στην οποία τρέχουν οι εφαρμογές
4. το network: συνδέει τα κοντέινερ μεταξύ τους

Όπως έχουμε αναφέρει στα προηγούμενα κεφάλαια το πρόγραμμα Docker μας προσφέρει ασφάλεια, με την τεχνική της απομόνωσης, σε επίπεδο εφαρμογών καθώς αν παραβιαστεί ένα κοντέινερ η διάδοση του ιού δεν θα συνεχιστεί στο επόμενο σύστημα. Για την εγκατάσταση του προγράμματος πρέπει ο χρήστης να επιλέξει την έκδοση που του ταιριάζει καθώς υπάρχουν διαφοροποιήσεις στο εικονικό δίκτυο των

κοντέινερ, στα "configuration" αρχεία του προγράμματος και στα προγράμματα τρίτων που είναι συμβατά με τη συγκεκριμένη έκδοση. Ο ιστότοπος "*https://docs.docker.com/release-notes/*" περιέχει αναλυτικά τις δυνατότητες, τα προβλήματα (bugs) και τα προγράμματα που είναι συμβατά της κάθε έκδοσης. Στην παρούσα εργασία, όπως φαίνεται στην εικόνα 14, η έκδοση του λογισμικού είναι "20.10.14". Αρχικά για την εγκατάσταση του προγράμματος πρέπει να γίνει απεγκατάσταση των παλαιότερων εκδόσεων από το υπολογιστικό σύστημα μας. Αυτό πραγματοποιείται με την εντολή "*sudo apt-get remove docker docker-engine docker.io containerd runc*".

Οι εντολές που πληκτρολόγηθηκαν για την εγκατάσταση του Docker σε λειτουργικό Debian είναι οι παρακάτω:

1. *sudo apt-get update*
2. *sudo apt-get install *
   *ca-certificates *
   *curl *
   *gnupg *
   lsb-release
3. *curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg*
4. *echo *
   *"deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian *
   $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
5. *sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin*

```
[redacted] ~ # docker version
Client: Docker Engine - Community
 Version:           20.10.14
 API version:       1.41
 Go version:        go1.16.15
 Git commit:        a224086
 Built:             Thu Mar 24 01:48:21 2022
 OS/Arch:           linux/amd64
 Context:           default
 Experimental:      true

Server: Docker Engine - Community
 Engine:
  Version:          20.10.14
  API version:      1.41 (minimum version 1.12)
  Go version:       go1.16.15
  Git commit:       87a90dc
  Built:            Thu Mar 24 01:46:14 2022
  OS/Arch:          linux/amd64
  Experimental:     false
 containerd:
  Version:          1.5.11
  GitCommit:        3df54a852345ae127d1fa3092b95168e4a88e2f8
 runc:
  Version:          1.0.3
  GitCommit:        v1.0.3-0-gf46b6ba
 docker-init:
  Version:          0.19.0
  GitCommit:        de40ad0
```

Εικόνα 14 Η έκδοση του προγράμματος Docker που χρησιμοποιήθηκε για την παρούσα εργασία

3.3 Εγκατάσταση των παραπλανητικών συστημάτων

Όπως έχει αναφερθεί και σε προηγούμενο κεφάλαιο, το υψηλής αλληλεπίδρασης Honeypot της παρούσας εργασίας αποτελείται από παραπλανητικά συστήματα τα οποία δελεάζουν τους επιτιθέμενους, συγκεντρώνουν τα δεδομένα των επιθέσεων και το καθένα από αυτά εξυπηρετεί μία διαφορετική υπηρεσία. Το δικό μας Honeypot καλύπτει μεγάλο εύρος των πιο σημαντικών υπηρεσιών διαθέτοντας πέντε παραπλανητικά ζητήματα. Τα τέσσερα από αυτά είναι ευρέως διαδεδομένα Honeypots όπως, "Ssh-Honeypot", "Wordpot", "Dionaea" και "Mailhoney" και το πέμπτο δημιουργήθηκε για να καλύψει τις ανάγκες της διπλωματικής αυτής. Οι υπηρεσίες που εξυπηρετούν φαίνονται στον πίνακα παρακάτω (Πίνακας 3).

Πίνακας 3 Υπηρεσίες που εξυπηρετεί το υψηλής αλληλεπίδρασης Honeypot

Honeypot	Πόρτα	Υπηρεσία
Dionaea	21	FTP
Ssh-Honeypot	22	SSH
Mailhoney	25	SMTP
Dionaea	42	WINS (Windows Internet Naming Service)
Dionaea	69	TFTP
Wordpot	80	HTTP
Dionaea	135	RPC (Remote Procedure Call)
Wordpot	443	HTTPS
Dionaea	445	RPC (Remote Procedure Call)
Dionaea	1433	Microsoft SQL Server

Dionaea	1723	PPTP VPN (Point-to-Point Tunneling Protocol Virtual Private Networking)
Dionaea	1883	MQTT (Message Queuing Telemetry Transport Protocol)
Dionaea	1900	UPnP, SSDP (Simple Service Discovery Protocol)
Ssh-Honeypot	2222	SSH
Mailhoney	2525	SMTP
Dionaea	3306	MySQL database server
Dionaea	5060	SIP (Session Initiation Protocol), VoIP Phones
Dionaea	5061	SIP (Session Initiation Protocol), VoIP Phones
Printer Honeypot	9100	Internet Printing Protocol
Dionaea	11211	Memcachedb

3.3.1 Εγκατάσταση Ssh-Honeypot

Το συγκεκριμένο Honeypot εξυπηρετεί την υπηρεσία SSH στην πόρτα 22 και έχει δημιουργηθεί από τον "drobertson" για να αναλύει τις επιθέσεις ωμής βίας. Πιο συγκεκριμένα βλέπουμε τις αποτυχημένες προσπάθειες σύνδεσης στο παραπλανητικό σύστημα, καταγράφοντας τους χρήστες και τους κωδικούς που παρατίθενται από τους επιτιθέμενους. Πρόκειται για ένα διαδεδομένο και χρήσιμο σύστημα ασφαλείας και ο ιστότοπος με τον κώδικα του συγκεκριμένου είναι "https://github.com/droberson/ssh-honeypot". Όπως και τα υπόλοιπα παραπλανητικά συστήματα έχει δημιουργηθεί ένα κοντέινερ για την ανάπτυξη αυτής της εφαρμογής.

Έχοντας κατεβάσει τον κώδικα από τον παραπάνω ιστότοπο, αρχικά δημιουργήθηκε ένα κοντέινερ με το όνομα είσαι "ssh-honeypot", τροποποιήθηκαν οι ρυθμίσεις του για να εξυπηρετεί την πόρτα είκοσι δύο ενώ η προεπιλεγμένη επιλογή είναι δύο χιλιάδες είκοσι δύο. Για να γίνει η ρύθμιση του συστήματος πρέπει να εισέλθουμε πρώτα στο κοντέινερ και να γίνει τροποποίηση του αρχείου entrypoint.sh. Στη συνέχεια πριν γίνει η εκτέλεση της εφαρμογής, είναι υποχρεωτικό να γίνει αλλαγή στα αρχεία του λειτουργικού συστήματος Debian ώστε η πραγματική SSH υπηρεσία του διακομιστή να μην είναι η πόρτα είκοσι δύο. Οι εντολές που πληκτρολογήθηκαν είναι οι εξής:

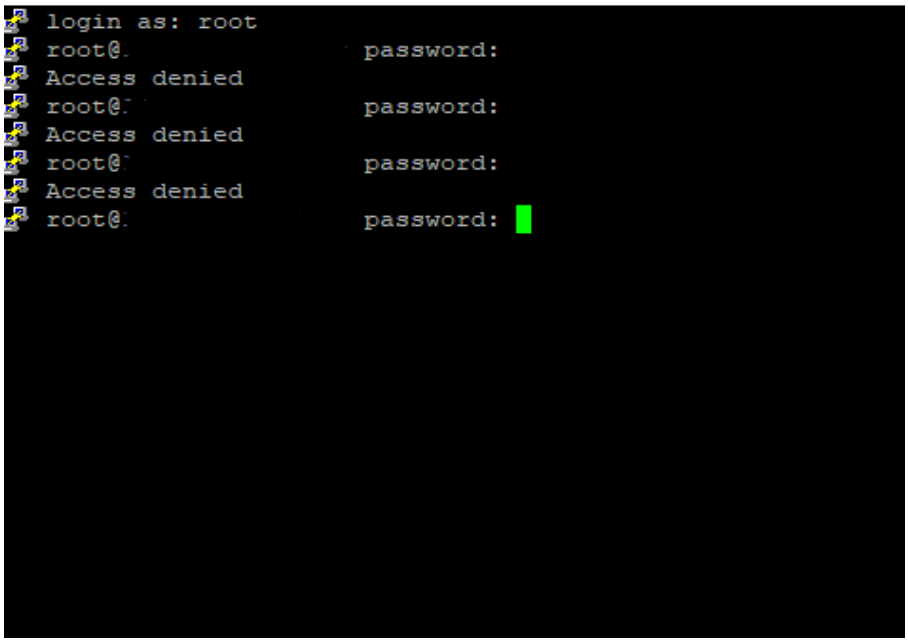
- *git clone https://github.com/random-robbie/docker-ssh-honey.git*
- *docker build –tag ssh-honeypot .*
- *docker run -p 22:22 ssh-honeypot* || η παράμετρος -p καθορίζει την πόρτα που εξυπηρετεί.
- *docker exec -it ssh-honeypot bash* || πρόσβαση στα αρχεία του ψεύτικου συστήματος
- *ssh-keygen -t rsa -f ./ssh-honeypot.rsa* || δημιουργία ssh κλειδιού για την SSH επικοινωνία
- *bin/ssh-honeypot -r ./ssh-honeypot.rsa*
- *nano entrypoint.sh* || ρύθμιση της πόρτας 22

- *nano /etc/ssh/sshd_config* || ρύθμιση της πραγματικής SSH υπηρεσίας του διακομιστή

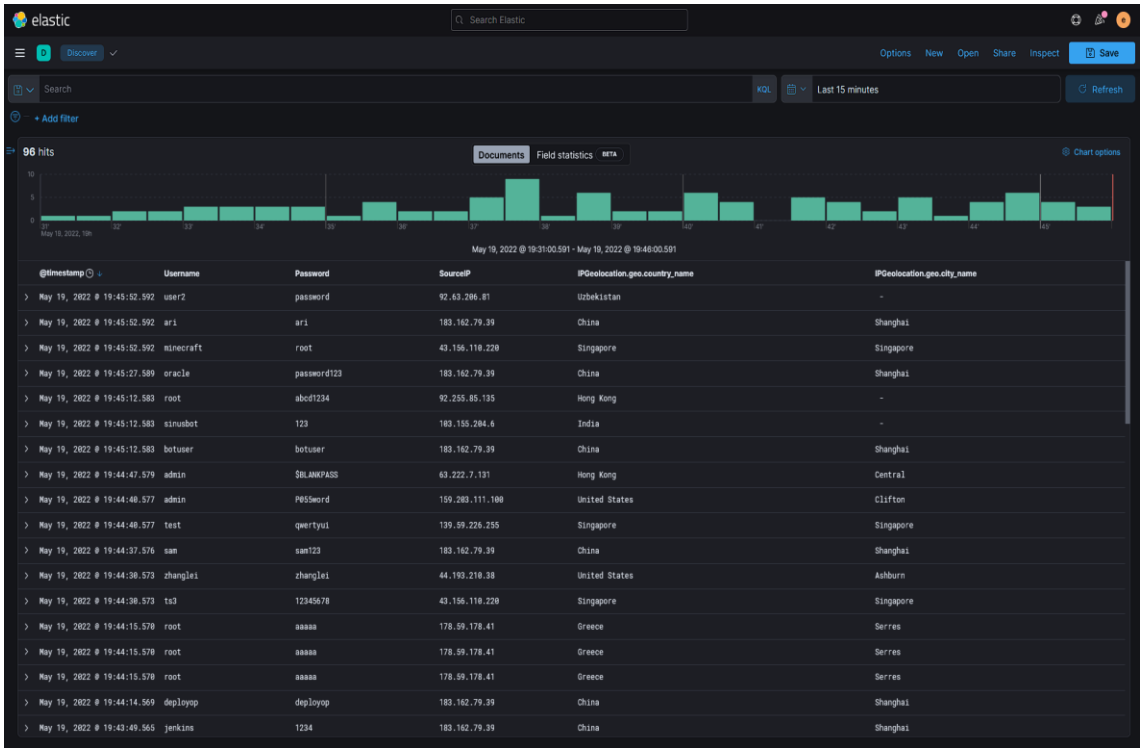
```
#!/bin/ash

SA=/etc/ssh-honeypot/ssh-honeypot.rsa

ssh-honeypot:
        $(CC) $(CFLAGS) -o bin/ssh-honeypot src/ssh-honeypot.c $(LIBS)

clean:
        rm -f *~ src/*~ bin/ssh-honeypot src/*.o

install: ssh-honeypot install-etc $(RSA)

install-etc:
        install -m 755 bin/ssh-honeypot /usr/local/bin/
        install -d /etc/ssh-honeypot
        install -m 644 ssh-honeypot.service /etc/ssh-honeypot/
        ln -sf /etc/ssh-honeypot/ssh-honeypot.service /etc/systemd/system/
        @echo
        @echo "You can enable ssh-honeypot at startup with: systemctl enable --now ssh-honeypot"

$(RSA):
        ssh-keygen -t rsa -f $(RSA) -N ''


ssh-honeypot -r /ssh-honeypot/ssh-honeypot.rsa -p 2222 -u nobody
echo "SSH Honeypot is Running..."
exec "$@"
```

Εικόνα 15 Το αρχείο ρυθμίσεως του Ssh-Honeypot “entrypoint.sh”

Όπως αναφέρεται στην εικόνα 17 οι κακόβουλοι χρήστες πληκτρολογούν τον χρήστη και τον κωδικό προσπαθώντας να μπουν στο σύστημα και τους εμφανίζεται μήνυμα αποτυχημένη σύνδεσης. Τις κακόβουλες προσπάθειες τις αναλύουμε στο Elasticsearch αφού πρώτα έχει δημιουργηθεί ειδικό φίλτρο για το συγκεκριμένο παραπλανητικό σύστημα. Η εικόνα 18 δείχνει πως στο Elasticsearch κατηγοριοποιούνται οι σημαντικότερες πληροφορίες της επίθεσης σε στήλες όπως όνομα χρήστη, κωδικός, IPaddress του επιτιθέμενου και χώρα/ πόλη προέλευσης της επίθεσης.



Εικόνα 16 Αποτυχημένες προσπάθειες σύνδεσης στο ssh-honeypot



Εικόνα 17 Ανάλυση των δεδομένων των επιθέσεων του ssh-honeypot στο Elasticsearch

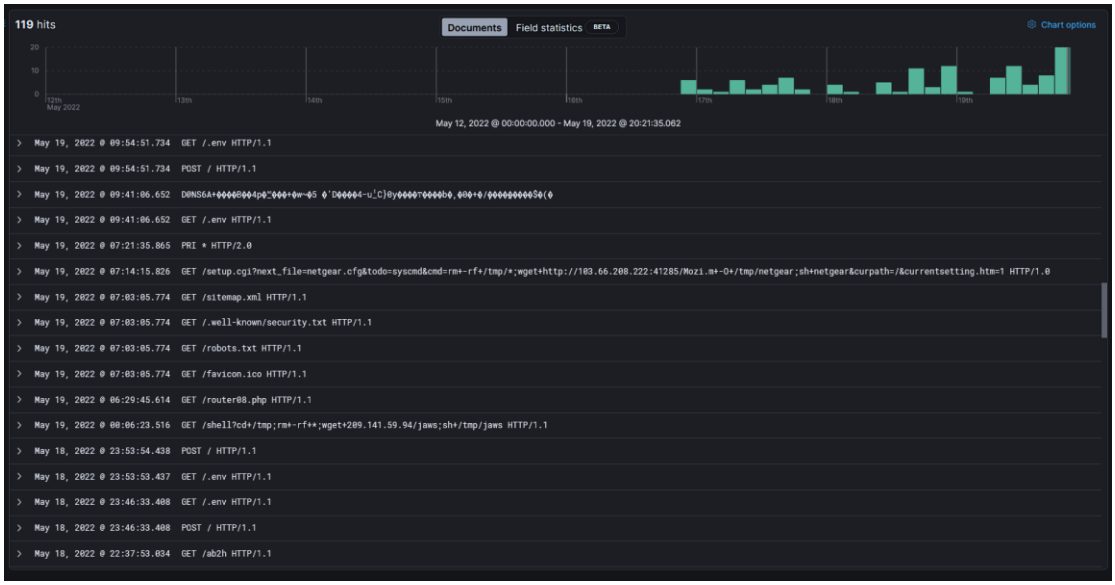
3.3.2 Εγκατάσταση Wordpot Honeypot

Το Wordpod Honeypot είναι ένα διαδικτυακό παραπλανητικό σύστημα το οποίο εξυπηρετείται στην υπηρεσία “HTTP” και “HTTPS” και ρόλος του είναι να ανιχνεύει τις κακόβουλες επιθέσεις ιστότοπους. Διαθέτει την έκδοση “Wordpress 2.8” και έχει εγκατασταθεί πάνω στον εικονικό διακομιστή που έχει έκδοση “Apache/2.2.22 (Ubuntu)”. Το συγκεκριμένο Honeypot καλύπτει τις ανάγκες της Παρούσης εργασίας

για τον αυξημένο αριθμό σε Wordpress συστήματα και ο κώδικας του είναι διαθέσιμος στον ιστότοπο "https://github.com/gbrindisi/wordpot". Η εντολή για την εκτέλεση του είναι η "*docker run -d --name wordpot -p 80:80 garland/wordpot:latest python /opt/wordport/wordpot.py --host=0.0.0.0 --port=80*".

Όπως φαίνεται στην εικόνα 19 η πλατφόρμα εισόδου στον ιστότοπο είναι ψεύτικη καθώς κανένας χρήστης δεν είναι εγγεγραμμένος σε αυτήν. Παρατηρούνται επιθέσεις ωμής βίας, επιθέσεις εκμετάλλευσης των κενών ασφαλείας που έχει η έκδοση του Wordpress, κακόβουλες σαρώσεις των αρχείων που περιέχει και απόπειρες εκμετάλλευσης ευπαθειών όπως SQL injection. Η εικόνα 20 μας δείχνει την ανάλυση των δεδομένων από το συγκεκριμένο σύστημα στο Elasticsearch.

Εικόνα 18 Πλατφόρμα εισόδου στο Worppot Honeypot



Εικόνα 19 Ανάλυση δεδομένων του Wordpot Honeypot στο Elasticsearch

3.3.3 Εγκατάσταση Mailhoney

Το Mailhoney honeypot εξυπηρετείται στην πόρτα 2525 και αναγνωρίζει επιθέσεις στους Mail διακομιστές, τα κακόβουλα email και τα ύποπτα αρχεία που στέλνουν οι επιτιθέμενοι. Ο κώδικας του είναι διαθέσιμος στον ιστότοπο "https://github.com/phin3has/mailoney" και περιέχει τη δυνατότητα του Docker container ενσωματωμένη. Πριν την εκτέλεση του container ρυθμίζουμε το αρχείο dockerfile χρησιμοποιώντας την εικονική διεύθυνση του κοντέινερ και την πόρτα 25. Υπάρχουν τρεις δυνατότητες για την εκτέλεση του και Στην παρούσα εργασία χρησιμοποιήθηκε η δυνατότητα “open_relay” για την καταγραφή των κακόβουλων email που στέλνονται. Τέλος γίνεται προώθηση της πόρτας 25 στην 2525 μέσω της εντολής "*sudo iptables -t nat -A PREROUTING -p tcp --dport 25 -j REDIRECT --to-port 2525*" και αυτό γιατί η πόρτα 25 θεωρείται ευαίσθητη από το λειτουργικό σύστημα Debian και απορρίπτει τα πακέτα. Η έκδοση του mail server είναι "Python SMTP proxy version 0.3" και οι εντολές που μπορούν να εκτελεστούν από τους επιτιθέμενους είναι οι παρακάτω:

1. EHLO
2. HELO
3. MAIL
4. RCPT
5. DATA
6. RSET
7. NOOP
8. QUIT
9. VRFY

```
220 74c9b618fac6 Python SMTP proxy version 0.3
HELP
250 Supported commands: EHLO HELO MAIL RCPT DATA RSET NOOP QUIT VRFY
EHLO google.gr250-74c9b618fac6
250-SIZE 33554432
250-8BITMIME
250 HELP
MAIL FROM:<test@uowm.gr>250 OK
RCPT TO:<test2@uowm.gr>250 OK
DATA354 End data with <CR><LF>.<CR><LF>
THIS IS A TEST OF A ATTACK ON MAILHONEY HONEYPOT
```

Εικόνα 20 Επίθεση στο Mailhoney Honeypot

Στην εικόνα 21 παρατηρούμε μία επίδειξη επίθεσης στο παραπλανητικό σύστημα και στην εικόνα 22 βλέπουμε τις ρυθμίσεις που γίνονται στο αρχείο Dockerfile.

```
FROM ubuntu

RUN apt update && apt install -y python3 python3-pip

RUN mkdir -p /opt/mailoney
COPY . /opt/mailoney

WORKDIR /opt/mailoney

RUN /usr/bin/pip3 install -r requirements.txt

RUN mkdir -p /var/log/mailoney
RUN touch /var/log/mailoney/commands.log


VOLUME /var/log/mailoney

ENTRYPOINT ["/usr/bin/python3","mailoney.py","-i","IPAddress","-p","25","-t", "open_relay", "-logpath", "/var/log/mailoney", "-s","MailSRV.local"]
```

Εικόνα 21 Αρχείο ρυθμίσεως Dockerfile του Mailhoney Honeypot

3.3.3 Εγκατάσταση Dionaea

Το συγκεκριμένο honeypot προσφέρει μεγάλο εύρος υπηρεσιών και είναι ένα από τα σημαντικότερα για την ανάλυση δεδομένων. Διαθέτει ενσωματωμένο το Dockerfile αρχείο και η εγκατάσταση του είναι εύκολο νοητή προς τους χρήστες. Ο κώδικας του είναι διαθέσιμος στον ιστότοπο "https://github.com/DinoTools/dionaea-docker". Και την εκτέλεση της εφαρμογής χρησιμοποιήθηκαν παρακάτω εντολές:

- *Docker build –tag dionaea .*
- *Docker run --rm -it -p 21:21 -p 42:42 -p 69:69/udp -p 80:80 -p 135:135 -p 443:443 -p 445:445 -p 1433:1433 -p 1723:1723 -p 1883:1883 -p 1900:1900/udp -p 3306:3306 -p 5060:5060 -p 5060:5060/udp -p 5061:5061 -p 11211:11211 dionaea*

Όπως φαίνεται στην εικόνα 23 για την εξαγωγή των δεδομένων του “Dionaea” σε στήλες στο “Elasticsearch”, χρησιμοποιείται συγκεκριμένο φίλτρο το οποίο διαχωρίζει τα ονόματα χρηστών, τους κωδικούς και το μήνυμα της επίθεσης. Το φίλτρο αυτό αναγράφεται στο αρχείο του "Logstash" και ονομάζεται "pipeline.yml", το οποίο

ευθύνεται για την αποκωδικοποίηση του μηνύματος της επίθεσης σε μορφή ευκολονόητη προς το χρήστη.

```
# Dionaea
  if [type] == "Dionaea" {
    date {
      match => [ "timestamp", "ISO8601" ]
    }
    mutate {
      rename => {
        "dst_port" => "dest_port"
        "dst_ip" => "dest_ip"
      }
      gsub => [
        "src_ip", "::ffff:", "",
        "dest_ip", "::ffff:", ""
      ]
    }
    mutate {
    if != [request]
        add_field => {
         "malicious_request" => "%{[request][maliciou_request]}"
        }

    }
    if [credentials] {
      mutate {
        add_field => {
          "username" => "%{[credentials][username]}"
          "password" => "%{[credentials][password]}"
        }
        remove_field => "[credentials]"
      }
    }
  }
```

Εικόνα 22 Το φίλτρο για την αποκωδικοποίηση των επιθέσεων στο Dionaea Honeypot

3.3.4 Υλοποίηση και Εγκατάσταση του Printer Honeypot

Το Printer Honeypot δημιουργήθηκε από εμάς για να καλύψει τις επιθέσεις που αφορούν τους εκτυπωτές. Τις περισσότερες φορές στους οργανισμούς οι εκτυπωτές είναι εκτεθειμένοι χωρίς κάποια ασφάλεια για αυτό το λόγο οι επιτιθέμενοι στρέφονται πρώτα προς τους εκτυπωτές. Με το συγκεκριμένο παραπλανητικό σύστημα καταχωρείται η διεύθυνση διαδικτυακού πρωτοκόλλου, που πραγματοποίησε είτε TCP είτε UDP κίνηση προς τον εκτυπωτή, η πόρτα πού προήλθε η κίνηση και το "User agent" του επιτιθέμενου που φανερώνει τη συσκευή που χρησιμοποιήθηκε. Για την δημιουργία του χρησιμοποιήθηκε η γλώσσα προγραμματισμού "Python 3" και χρησιμοποιήθηκαν πολλές βιβλιοθήκες της Python. Συγκεκριμένα χρησιμοποιήθηκαν οι βιβλιοθήκες "sys", "logging", "argparse", "pkipplib" και "gevent". Το "pkipplib" είναι μια βιβλιοθήκη της Python που μπορεί να μετατρέπει τα αιτήματα IPP(Internet Printing Protocol) σε μορφή τέτοια ώστε στη συνέχεια να σταλούν στον διακομιστή εκτύπωσης και η βιβλιοθήκη "gevent" χρησιμοποιείται για την γρήγορη επεξεργασία και τον συγχρονισμό των αιτημάτων προς το διακομιστή. Όπως και τα υπόλοιπα παραπλανητικά συστήματα, έτσι και το printer honeypot υλοποιήθηκε σε docker κοντέινερ.

Η εικόνα 23 μας δείχνει τον κώδικα του Dockerfile που δημιουργήθηκε για να υλοποιηθεί το παραπλανητικό σύστημα σε κοντέινερ. Το "FROM" φανερώνει την γλώσσα προγραμματισμού, το "ADD" και το "WORKDIR" φανερώνουν τον φάκελο που θα περιέχει τα αρχεία του συστήματος στο ψεύτικο περιβάλλον, το "RUN" εκτελεί το συγκεκριμένο αρχείο για να είναι συμβατή η βιβλιοθήκη της Python, το "EXPOSE" δηλώνει την πόρτα που θα εξυπηρετεί και τέλος το

"CMD" ορίζει την εντολή που θα τρέχει το παραπλανητικό σύστημα ορίζοντας ως διεύθυνση διαδικτυακού πρωτοκόλλου την εικονική IP Address του κοντέινερ για να είναι προσβάσιμο από το διαδίκτυο.

```
FROM python

ADD . /honeyprint

WORKDIR /honeyprint

RUN cd /usr/local/lib/python*/site-packages/pkipplib/ -w pkipplib.py

EXPOSE 9100

CMD ["python3","server.py", "-i", "172.17.0.4", "-p", "9100"]
```

Εικόνα 23 Το αρχείο Dockerfile που δημιουργήθηκε για την υλοποίηση του παραπλανητικού συστήματος σε κοντέινερ

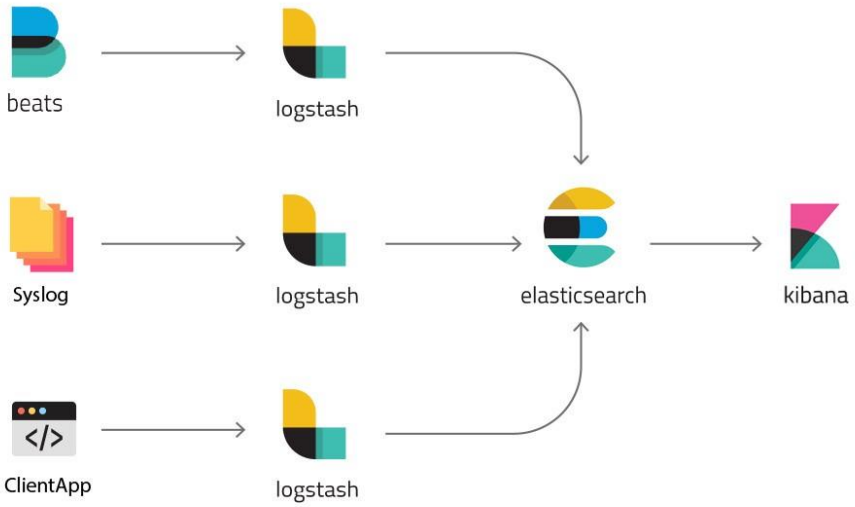
Ο κώδικας του παραπλανητικού συστήματος φαίνεται στην εικόνα 24 και επεξηγήσεις για τη χρήση της κάθε εντολής βρίσκονται δίπλα σε μορφή σχόλιου. Στα αιτήματα που δέχεται το σύστημα εμφανίζεται η διεύθυνση διαδικτυακού πρωτοκόλλου, η πόρτα από την οποία προέρχεται η κίνηση και το μοντέλο του περιηγητή που χρησιμοποιεί ο επιτιθέμενος. Στο υποκεφάλαιο 3.4.1 αναφέρεται το φίλτρο που δημιουργήθηκε για την εξαγωγή των δεδομένων στο “ELK stack”.

```
import sys # Εισαγωγή βιβλιοθηκών
import logging
import argparse
from pkipplib import pkipplib # Εισαγωγή βιβλιοθηκών

from gevent.server import StreamServer # Εισαγωγή βιβλιοθηκών

class PrintServer(object):

    def __init__(self):
        pass

    def handle(self, sock, address): # function για την διαχείρηση των αιτημάτων
        print(address) #εκτύπωση IP Address
        data = sock.recv(8192) # το μέγιστο μέγεθος που μπορεί να επεξεργαστεί το συστημα είναι 8192 bytes
        print(repr(data)) #εντολή για την ωραία εμφάνιση των δεδομένων
        try:
            body = data.split('\r\n\r\n', 1)[1] # εντολή για να μην είναι τα δεδομένα σε μία γραμμή
        except IndexError:
            body = data
        request = pkipplib.IPPRequest(body) #μετατροπη του αιτήματος σε μορφή ικανή για να κατανοήσει ο διακομιστής εκτυπωτής
        request.parse()
        print(request) #εκτύπωση αιτήματος
        request = pkipplib.IPPRequest #μετατροπη του αιτήματος σε μορφή ικανή για να κατανοήσει ο διακομιστής εκτυπωτής
        request.operation["attributes-charset"] = ("charset", "utf-8") #ορίζεται η μορφή του αιτήματος που είναι utf-8
        request.operation["attributes-natural-language"] = ("naturalLanguage", "en-us") #ορίζεται η γλώσσα του αιτήματος
        sock.send(request.dump())

    def get_server(self, host, port):
        connection = (host, port) #IP Address και πόρτα
        server = StreamServer(connection, self.handle)
        return server

if __name__ == "__main__": # για να εκτελεστούν τα modules "pkipplib" και "gevent"
    print_address="172.17.0.4" # IP Address του συστήματος
    print_port=9100 # Πόρτα του συστήματος
    parser.add_argument('-i','--serveraddress', const='172.17.0.4', required=False) #ορισμός της παραμέτρου "-i"
    parser.add_argument('-p','--port', const=9100, required=False) #ορισμός της παραμέτρου "-p"
    args = vars(parser.parse_args()) #παραδρέι τις νέες παραμέτρους αν πληκτρολογηθούν αλλιώς συνεχίζει με τα δεδομένα που έχει ως μεταβλητές στο "print_address" και στο "print_port"
    if args['serveraddress']:
            print_address=args['serveraddress']
    if args['port']:
            print_port=int(args['port'])

    # Start print server
    ps = PrintServer()
    print_server = ps.get_server(print_address, print_port)
    print(f'Network Printer')
    try:
        print_server.serve_forever() # module απο την βιβλιοθήκη gevent
    except KeyboardInterrupt as e: #να σταματάει το σύστημα οταν πατηθεί κάτι απο το πληκτρολόγιο
        print('Corrupted')
        sys.exit(0) #έξοδος απο το σύστημα.
```

Εικόνα 24 Ο κώδικας του Printer Honeypot

3.4 Εγκατάσταση και Ρύθμιση του ELK Stack

Στο υποκεφάλαιο αυτό θα δοθούν λεπτομέρειες για την εγκατάσταση την ρύθμιση και τρόπο λειτουργίας της στοίβας ELK stack. Η στοίβα αυτή αποτελείται από τρία προγράμματα όπως δείχνει το όνομα του, με το E να συμβολίζει το Elasticsearch, το L να συμβολίζει το Logstash και το K να συμβολίζει το Kibana. Κάθε ένα από αυτά τα προγράμματα είναι υπεύθυνο για διαφορετική λειτουργία και είναι αλληλεξάρτητα καθώς η μη εύρυθμη λειτουργία στο ένα θα επηρεάσει και τη λειτουργία των άλλων. Όπως φαίνεται στην εικόνα 25, το Logstah ευθύνεται για τη μεταφορά των δεδομένων και την αποκωδικοποίηση τους σε ευκολονόητη μορφής τους προς τους χρήστες. Ο ρόλος του Elasticsearch είναι η αποθήκευση, η αναζήτηση και η ανάλυση τεράστιων όγκων δεδομένων γρήγορα και σε πραγματικό χρόνο. Το Elasticsearch διαθέτει μία μηχανή αναζήτησης, η οποία είναι γραμμένη στη γλώσσα προγραμματισμού Java, και με τα κατάλληλα φίλτρα μας δίνει αποτελέσματα σε κλάσματα δευτερολέπτου. Τέλος το Kibana οπτικοποιεί τις πληροφορίες των επιθέσεων και με τη βοήθεια διαγραμμάτων συγκεντρώνει στατιστικά στοιχεία. Η εφαρμογή των τριών προγραμμάτων σε ένα έχει δημιουργηθεί από την εταιρεία “Elasticsearch”, η οποία έχει δημιουργήσει επεκτάσεις και δυνατότητες για τη βελτίωση της στοίβας.



Εικόνα 25 Αρχιτεκτονική της εφαρμογής ELK stack. Το Logstash συλλέγει και αποκωδικοποιεί τα δεδομένα, το Elasticsearch τα αποθηκεύει και το Kibana τα οπτικοποιεί σε διαγράμματα.

Μία σημαντική επέκταση της εταιρείας “Elasticsearch” χρησιμοποιηθεί στην παρούσα εργασία είναι το πρόγραμμα “Filebeat” που έχει αναλυθεί στο υποκεφάλαιο 3.2.3. Ο ρόλος της υπηρεσίας αυτής είναι να συλλέγει τα δεδομένα και να τα διανέμει στο “Logstash”. Παρόλο που το “Logstash” μπορεί να κάνει την ίδια δουλειά, στο “Filebeat” ο χρήστης έχει τη δυνατότητα να καθορίσει την συχνότητα, τον τρόπο που διαδίδονται τα δεδομένα και περιέχει περισσότερη ασφάλεια κατά τη διάδοση. Σε αντίθεση με την στοίβα “ELK Stack”, το “filebeat” εκτελείται ως υπηρεσία

και όχι ως κοντέινερ προκειμένου να αντλεί τα δεδομένα των παραπλανητικών συστημάτων.

3.4.1 Εγκατάσταση και ρύθμιση του Logstash

Το “Logstash” είναι εργαλείο συλλογής επεξεργασίας και προώθηση μηνυμάτων καταγραφής. Η συλλογή επιτυγχάνεται μέσω φίλτρο εισόδου στο αρχείο "pipeline.yml" το οποίο εξάγει τα δεδομένα σε στήλες είσαι μορφή κατανοητή προς το χρήστη. Η εφαρμογή του “Logstash” εκτελείται σε κοντέινερ μέσω του αρχείου “dockerfile”, όπου εκεί ρυθμίζουμε τη μνήμη Ram, τον επεξεργαστή και την εικονική IP διεύθυνση που θα έχει κατά την εκτέλεση του. Επίσης στο αρχείο αυτό έχουμε εγκαταστήσει το φίλτρο “Logstash Json” χρησιμοποιώντας την εντολή "*RUN logstash-plugin install logstash-filter-json*". Το παραπάνω φίλτρο είναι απαραίτητο για την αποκωδικοποίηση σε αυτό το σύστημα καθώς τα δεδομένα που συλλέγουμε βρίσκονται σε Json μορφή.

Το φίλτρο εισόδου για την αποκωδικοποίηση των δεδομένων, το οποίο βρίσκεται στο αρχείο "pipeline.yml", περιέχει λογικές συνθήκες για να αντιλαμβάνεται από ποιο παραπλανητικό σύστημα έρχονται τα δεδομένα και να εφαρμόζει τις κατάλληλες στήλες. Επιπρόσθετα χρησιμοποιούνται regex εκφράσεις για την αντιστοίχιση κάθε λέξης σε ειδικό πεδίο ανάλογα με τον τύπο της όπως π.χ. αν είναι λογική τιμή ή αριθμός ή string. Παρακάτω φαίνεται το φίλτρο εισόδου.

```
input { # πεδίο που ορίζει τις πόρτες διαδικτυακής κίνησης
      beats {
            port => 5044
      }
      tcp {
            port => 5000
      }
}
## Add your filters / logstash plugins configuration here
filter { # πεδίο που ορίζει το φίλτρο αποκωδικοποίησης δεδομένων
    json { # ορίζουμε ότι τα δεδομένα θα έχουν json μορφή
      source => "message" # το πεδίο που θα αποκωδικοποιηθεί θα είναι το «message»
    }
    if [container][name] in "ssh_honeypot" { # λογική συνθήκη ΑΝ τα δεδομένα έρχονται από το honeypot ssh
      grok { # έκφραση regex για την εισαγωγή των δεδομένων σε στήλες
```

```
        match => { "log" => [ "\[%{DAY} %{MONTH} %{MONTHDAY} %{TIME} %{YEAR}\] %{IPV4:SourceIP} %{USERNAME:Username} %{GREEDYDATA:Password}" ] }

      }

      mutate { # φίλτρο για εισαγωγή πεδίου

       add_field => { "SrcIP" => "%{SourceIP}" } # εισαγωγή της IP address του επιτιθέμενου σε ξεχωριστό πεδίο με όνομα «SourceIP»

      }

      geoip { # φίλτρο geolocation για να βρει περισσότερες λεπτομερείς για την IP address του κακόβουλου χρήστη όπως χωρά προέλευσης

       source => "SourceIP"

       target => "IPGeolocation" #στήλη που θα εξάγει τις πληροφορίες

      }

    }

    if [container][name] in  "wordpot" { #  λογική συνθήκη αν τα δεδομένα προέρχονται από το honeypot wordpot

      grok { # φίλτρο για την αποκωδικοποίηση με grok μορφή

       match => { "log" => [ "\"%{GREEDYDATA:Request}\" " ] } # εξαγωγή των δεδομένων της επίθεσης στην στήλη με όνομα «requests»

      }

    if [container][name] in  “dionaea” #λογική συνθήκη
{
date {
match => [ "timestamp", "ISO8601" ]
#μετατροπή της ημερομηνίας/ώρας σε πρότυπο ISO8601
}
mutate {
rename => { # μετανομασία των στηλών
"dst_port" => "dest_port"
"dst_ip" => "dest_ip"
}
gsub => [
"src_ip", "::ffff:", "",
"dest_ip", "::ffff:", ""
```

```
]
}
if [credentials] { # λογική συνθήκη αν υπάρχει η επίθεση περιέχει όνομα χρήστη και κωδικό
mutate {
add_field => { # προσθήκη  στηλών
"username" => "%{#[credentials][username]}" # εξαγωγή του όνομα χρήστη στην στήλη “username”
"password" => "%{#[credentials][password]}" # εξαγωγή του κωδικού πρόσβασης στην στήλη “password”
}
remove_field => "[#credentials]" # Αν δεν περιέχει το όνομα χρήστη και τον κωδικού να γίνει απόκρυψη της στήλης “credentials”
}
}
}
if [container][name] in “mailoney” # λογική συνθήκη
{
date {
match => [# "timestamp", "ISO8601" ]μετατροπή ημερομηνίας/ώρας στο πρότυποISO
}
mutate {
add_field => { "dest_port" => "25" } # εισαγωγη στήλης  της πόρτας που εξυπηρετεί το honeypot
grok {  match => { "log" => [ "\"%{GREEDYDATA:Emails}  %{IPV4:SourceIP} \" " ] }   } # έκφραση regex για την εξαγωγή των δεδομένων σε στήλες

}
}
if [container][name] in  "printerhoneypot" { #  λογική συνθήκη αν τα δεδομένα προέρχονται από το honeypot printer
      grok { # φίλτρο για την αποκωδικοποίηση με grok μορφή
        match => { "message" => [ "\(%{IPV4:IPAddress} %{INTEGER:Port}\) " ] } # εξαγωγή των δεδομένων της επίθεσης στην στήλη με όνομα “IPAddress” και σε στην στήλη “Port”
```

```
      }
}
    }
  }
```

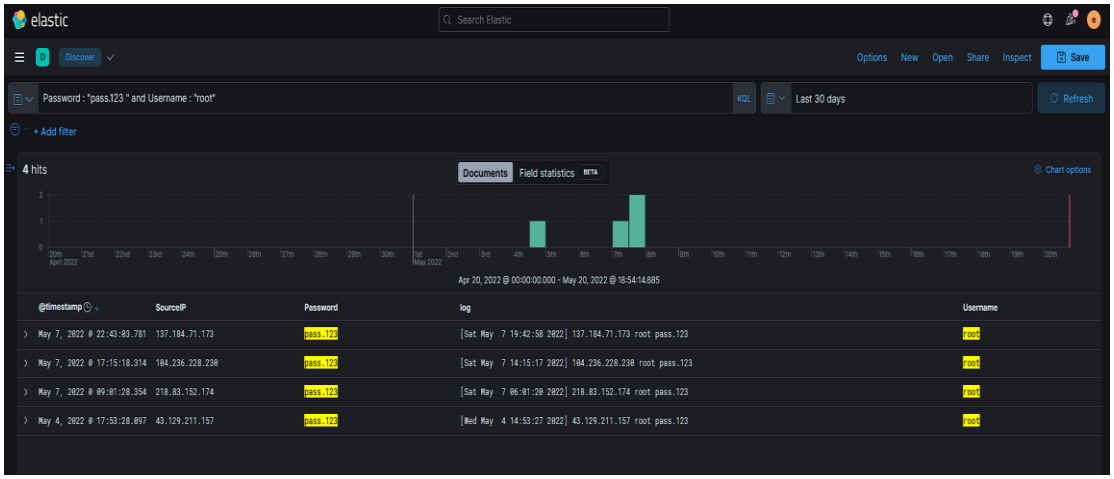
```
output { # πεδίο για την διάδοση δεδομένων στο elasticsearch
      elasticsearch {
           hosts => "X.X.X.X:9200" # ορισμός της IP address/πόρτας της υπηρεσίας Elasticsearch
          user => "user_of_logstash"  # ο λογαριασμός χρήστη που μεταφέρει τα δεδομένα από το logstash στο elasticsearch
          password => "password_of_logstashuser" } # κωδικός πρόσβασης του χρήστη
      stdout { codec => rubydebug } # εντολή να εμφανίζει τα μηνύματα λάθους και debugging στο πρόγραμμα logstash
```

3.4.2 Εγκατάσταση και ρύθμιση του ElasticSearch

Το elasticsearch είναι η βάση δεδομένων πού αποθηκεύει τις καταγραφές των επιθέσεων και παράλληλα μία μηχανή αναζήτησης πραγματικού χρόνου και ανάλυση δεδομένων. Το πρόγραμμα έχει αναπτυχθεί στη γλώσσα προγραμματισμού Java και κυκλοφορεί ώς λογισμικό ανοικτού κώδικα. Τα αιτήματα (requests) και οι απαντήσεις (responses), για την αναζήτηση των δεδομένων γίνονται χρησιμοποιώντας δομές Json, προσδίδοντας ευελιξία και γρήγορα αποτελέσματα κατά την αναζήτηση. Αποθηκεύει τα αρχεία σε μία τοπολογία συμπλεγμάτων με κόμβους και με τα κατάλληλα φίλτρα μπορούμε να αναλύουμε γρήγορα μεγάλους όγκους δεδομένων. Οι εντολές που χρησιμοποιήθηκαν για την εγκατάσταση του elasticsearch είναι:

- *Docker build –tag elasticsearch .*
- *Docker run -p 9200:9200 elasticsearch*

Στη μηχανή αναζήτησης θέτοντας ως φίλτρο τις μεταβλητές που θέλουμε και τις τιμές τους μπορούμε να κάνουμε στοχευμένη ανάλυση δεδομένων. Υπάρχουν λογικές συνθήκες AND και OR που συνδυάζουν αποτελέσματα. Παραδείγματος χάρη στην εικόνα 26 γίνεται αναζήτηση στο Elasticsearch με φίλτρο να βρεθούν το μήνυμα της επίθεσης και η διεύθυνση διαδικτυακού πρωτοκόλλου του επιτιθέμενου όταν ο κωδικός που έχει χρησιμοποιήσει ο επιτιθέμενος είναι "pass.123" και το όνομα χρήστη είναι "root".



Εικόνα 26 Αναζήτηση στο Elasticsearch για τον κωδικό “pass.123” και για όνομα χρήστη “root”

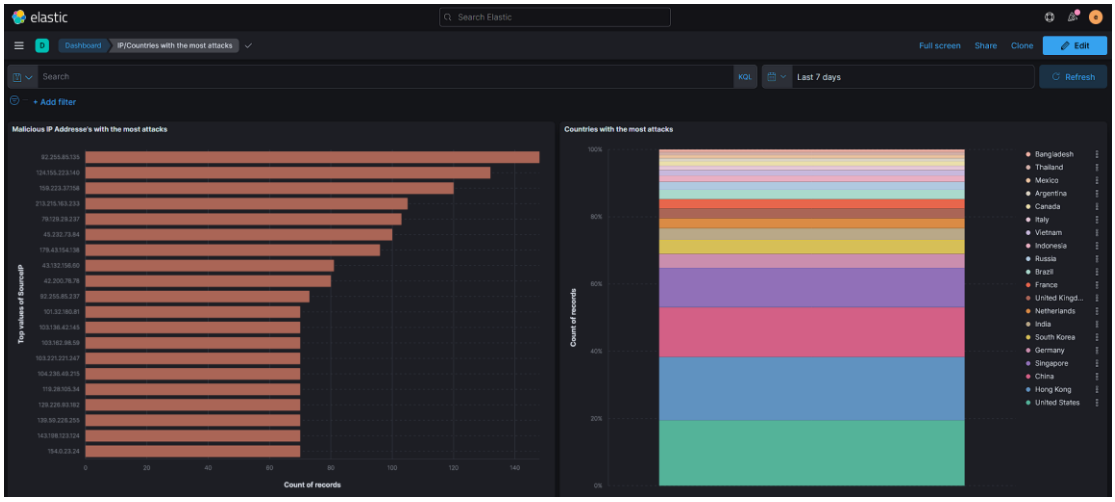
Τέλος του Elasticsearch διαθέτει στον χρήστη τη δυνατότητα να κάνει πιο ασφαλή την εφαρμογή. Στα πλαίσια αυτής της εργασίας δημιουργήθηκαν τέσσερις χρήστες και ρυθμίστηκαν οι ρόλοι τους. Ο διαχειριστής της εφαρμογής έχει το όνομα "admin" και έχει πρόσβαση σε όλες τις λειτουργίες του ELK Stack. Οι υπόλοιποι τρεις χρήστες "logstash_user", "kibana_user" και "elastic_user" έχουν δημιουργηθεί ως χρήστες υπηρεσίας με στόχο να ξεκινούν οι υπηρεσίες δικτύου και υπηρεσίες της εφαρμογής αυτής. Με αυτό τον τρόπο ο κίνδυνος μειώνεται καθώς μόνο αυτοί οι χρήστες έχουν δικαίωμα να εγκαταστήσουν και να διαμορφώσουν τις υπηρεσίες στο διακομιστή. Οι κωδικοί που χρησιμοποιήθηκαν για τους παραπάνω χρήστες έχουν αυστηρή πολιτική και είναι δύσκολο για τους επιτιθέμενους να του σπάσουν.

3.4.3 Εγκατάσταση και ρύθμιση του Kibana

Το Kibana είναι λογισμικό οπτικοποίησης δεδομένων και έχει αναπτυχθεί στη γλώσσα προγραμματισμού Java. Δημιουργεί διάφορες γραφικές απεικονίσεις, όπως πίνακες, διαγράμματα, χάρτες και ιστογράμματα, χρησιμοποιώντας τα αποθηκευμένα δεδομένα του “Elasticsearch”. Οι εντολές που χρησιμοποιήθηκαν για την εγκατάσταση του Kibana είναι:

- *docker build –tag kibana .*
- *docker run -p 5601:5601 kibana*
- *nano kibana.yml* || τα στοιχεία πρόσβασης του χρήστη kibana_user για την εύρυθμη λειτουργεία με το Elasticsearch

Τα διαγράμματα και πίνακες πού δημιουργήθηκαν περιέχουν στατιστικά δεδομένα όπως, οι 10 πιο χρησιμοποιημένοι κωδικοί χρηστών, πόσες επιθέσεις δέχεται το σύστημα καθημερινά, τεχνικές επιθέσεις χρησιμοποιούνται πιο συχνά κτλ. Στην εικόνα 27 παρατηρούμε διαγράμματα, με το αριστερό διάγραμμα να δείχνει τον αριθμό των επιθέσεων που πραγματοποιούνται από τις IP addresses των κακόβουλων χρηστών και το δεξί διάγραμμα να δείχνει το ποσοστό των επιθέσεων πού προέρχεται από κάθε χώρα. Στο Κεφάλαιο 4 θα παρουσιαστούν nanota δεδομένα που έχει καταγράψει το υψηλής αλληλεπίδρασης Honeypot και θα γίνει σχολιασμός τους.



Εικόνα 27 Διάγραμμα στην εφαρμογή Kibana, το οποίο δείχνει το πλήθος επιθέσεων από τις IP Addresses των επιτιθέμενων και τις χώρες προέλευσης αυτών.

Κεφάλαιο 4. Παρουσίαση και ανάλυση αποτελεσμάτων Honeypot

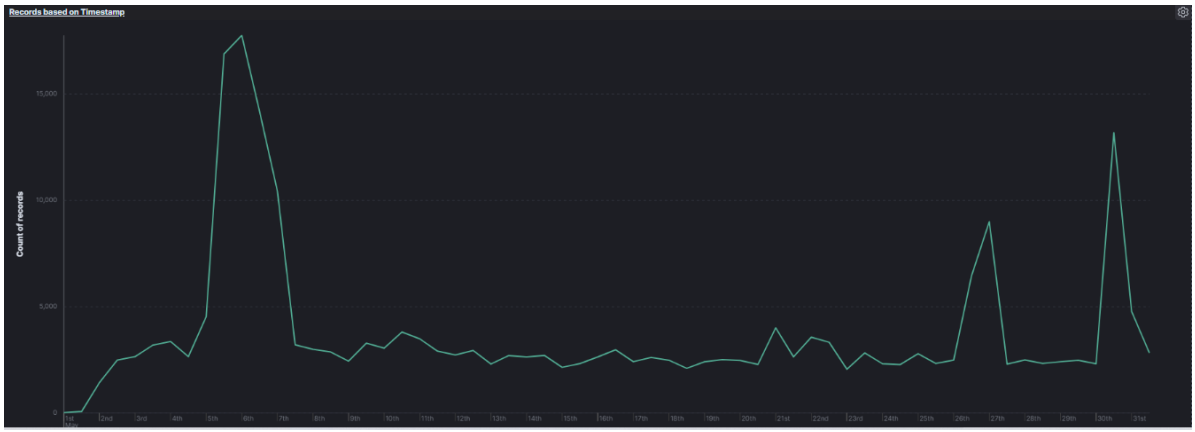
Στην παρούσα διπλωματική εργασία δημιουργήθηκε και υλοποιήθηκε ένα υψηλής αλληλεπίδρασης Honeypot, το οποίο αποσκοπεί στην ανίχνευση και ανάλυση των επιθέσεων που δέχεται. Αυτό το κεφάλαιο περιγράφει τα αποτελέσματα των επιθέσεων και γίνεται ανάλυση αυτών. Αρχικά το υψηλής αλληλεπίδρασης Honeypot ήταν σε πλήρη λειτουργία από τη 1 Μαρτίου 2022 έως τη 1 Ιουνίου 2022. Σε αυτό το διάστημα τα 5 honeypot κατέγραφαν επιθέσεις και το ELK stack μας έδινε τα αποτελέσματα. Ένα από τα κύρια αποτελέσματα που πρέπει να αναλυθούν πρώτα είναι η δυνατότητα εντοπισμού του Honeypot και αν κάποιος επιτιθέμενος προσπάθησε να αποκτήσει εξουσιοδότηση σε αυτό. Στη συνέχεια, αυτή η ενότητα προχωρά στην ανάλυση των αποτελεσμάτων από τα δεδομένα των επιθέσεων, συμπεριλαμβανομένων των κωδικών πρόσβασης, των ονομάτων χρήστη, των εντολών που χρησιμοποιήθηκαν για την παραβίαση των παραπλανητικών συστημάτων κτλ.

Κατά τη φάση κατασκευής και ανάπτυξης του Honeypot, πολλοί επιτιθέμενοι άρχισαν να πραγματοποιούν οριζόντιες σαρώσεις στο Honeypot προκειμένου να ανακαλύψουν τις υπηρεσίες που είναι εκτεθειμένες. Τα αποτελέσματα αφορούν την περίοδο του Μαρτίου μέχρι τα τέλη Ιουνίου, εκτός από μία βδομάδα του Απριλίου στην οποία πραγματοποιήθηκε αναβάθμιση του λογισμικού ELK stack. Στον Πίνακα 3 παρουσιάζεται το πλήθος των επιθέσεων για κάθε μήνα ξεχωριστά και παρατηρείται το πλήθος να αυξάνεται με την πάροδο του χρόνου.

Πίνακας 4 Το πλήθος επιθέσεων στο Honeypot

Μήνας	Συνολικός αριθμός επιθέσεων στο Honeypot
Μάρτιος	134773
Απρίλιος	85712
Μάιος	241133
Σύνολο	461618

Τον μήνα Απρίλιο τα παραπλανητικά συστήματα δέχτηκαν λιγότερες επιθέσεις από τους υπόλοιπους μήνες γιατί οι υπηρεσίες δεν ήταν εκτεθειμένες προς το διαδίκτυο. Επίσης σημαντικό ρόλο για το μεγάλο πλήθος των επιθέσεων είναι ο μεγάλος αριθμός υπηρεσιών, που εκτέθηκαν στο διαδίκτυο και οι ευπάθειες που έχουν τα παραπλανητικά συστήματα. Οι επιτιθέμενοι με συγκεκριμένα εργαλεία, που χρησιμοποιούνται για την παραβίαση υπολογιστικών συστημάτων, μπορούσαν να αποσπάσουν σημαντικές πληροφορίες για τα Honeypots όπως η έκδοση του λογισμικού και οι ευπάθειες αυτών προκειμένου να τα παραβιάσουν. Με την πάροδο του χρόνου, περισσότεροι κακόβουλοι χρήστες ανακάλυπταν αυτές τις πληροφορίες για τα παραπλανητικά συστήματα και πραγματοποιούσαν επιθέσεις όπως φαίνεται στην εικόνα 28.



Εικόνα 28 Το πλήθος των επιθέσεων που δέχτηκε το Honeypot, για κάθε μέρα του Μαΐου στο πρόγραμμα Kibana

Οι επιθέσεις πραγματοποιήθηκαν στα 5 παραπλανητικά συστήματα και ο Πίνακας 5 παρουσιάζει το πλήθος των επιθέσεων που δέχτηκε το κάθε ένα από αυτά. Βλέπουμε μια σταθερότητα στον συνολικό αριθμό που δέχονται τα Honeypot. Εξαίρεση αποτελεί το Dionaea, το οποίο έχει σημαντική αύξηση. Οι δύο λόγοι για την αύξηση είναι το πλήθος των υπηρεσιών που προφέρει και η ανίχνευση των επιθέσεων κρυπτογράφησης υπολογιστικών συστημάτων και συγκεκριμένα του Maze Ransomware, που είναι από τους πιο διαδεδομένους κινδύνους για τις εταιρίες.

Πίνακας 5 Το πλήθος των επιθέσεων στα παραπλανητικά συστήματα

Μήνας / Honeypot	Μάρτιος	Απρίλιος	Μάιος	Σύνολο
SSH Honeypot	63094	35413	98511	294020
Dionaea	44963	37095	109800	294225
HTTP Honeypot	9267	3511	7718	35018
Telnet Honeypot	12416	6493	18565	57974
Mailoney	5033	3200	6500	25159
Σύνολο	134773	85712	241133	

Οι επιθέσεις ωμής βίας ήταν οι πολυπληθέστερες και τα αποτελέσματα παρουσιάζονται στον Πίνακα 6 και στον Πίνακα 7. Πιο συγκεκριμένα, παρουσιάζονται τα 10 κορυφαία ονόματα χρηστών και οι 10 κορυφαίοι κωδικοί πρόσβασης που πληκτρολογήθηκαν από τους επιτιθέμενους.

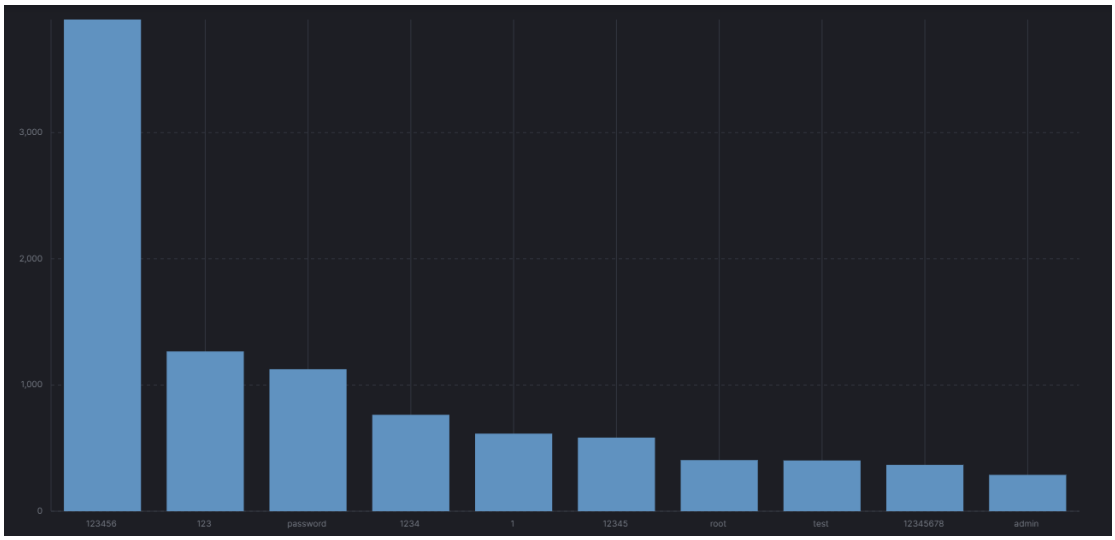
Πίνακας 6 Τα 10 κορυφαία ονόματα χρηστών για τον μήνα Μάιο

Όνομα χρήστη	Αριθμός Καταγραφών
root	93636
admin	4102
test	2876
user	2590
ubuntu	881
oracle	645
postgres	636
ftpuser	492
git	458
guest	351

Παρατηρούμε πως το όνομα χρήστη “root” βρίσκεται πρώτο στην λίστα καθώς διαθέτει δικαιώματα διαχειριστή. Επίσης τα ονόματα χρηστών που χρησιμοποιήθηκαν συνήθως ανήκουν και αποτελούν προαιρετικοί χρήστες του λειτουργικού συστήματος “Linux”. Στην Εικόνα 29 παρουσιάζονται οι δημοφιλέστεροι κωδικοί των επιθέσεων και σε σύγκριση με τις λίστες “SecLists” έχουν μεγάλη ομοιότητα. Οι λίστες “SecLists” είναι μια συλλογή πολλών τύπων λιστών που χρησιμοποιούνται κατά τις αξιολογήσεις ασφαλείας και περιέχουν ονόματα χρηστών, κωδικούς, ευαίσθητα μοτίβα δεδομένων κτλ. Οι λίστες αυτές είναι διαθέσιμες στο ιστότοπο "github.com/danielmiessler/SecLists".

Πίνακας 7 Οι 10 κορυφαίοι κωδικοί πρόσβασης για τον μήνα Μάιο

Κωδικός πρόσβασης	Αριθμός καταγραφών
123456	3896
123	1266
password	1125
1234	764
1	615
root	405
test	402
12345678	367
admin	288
qwerty	262



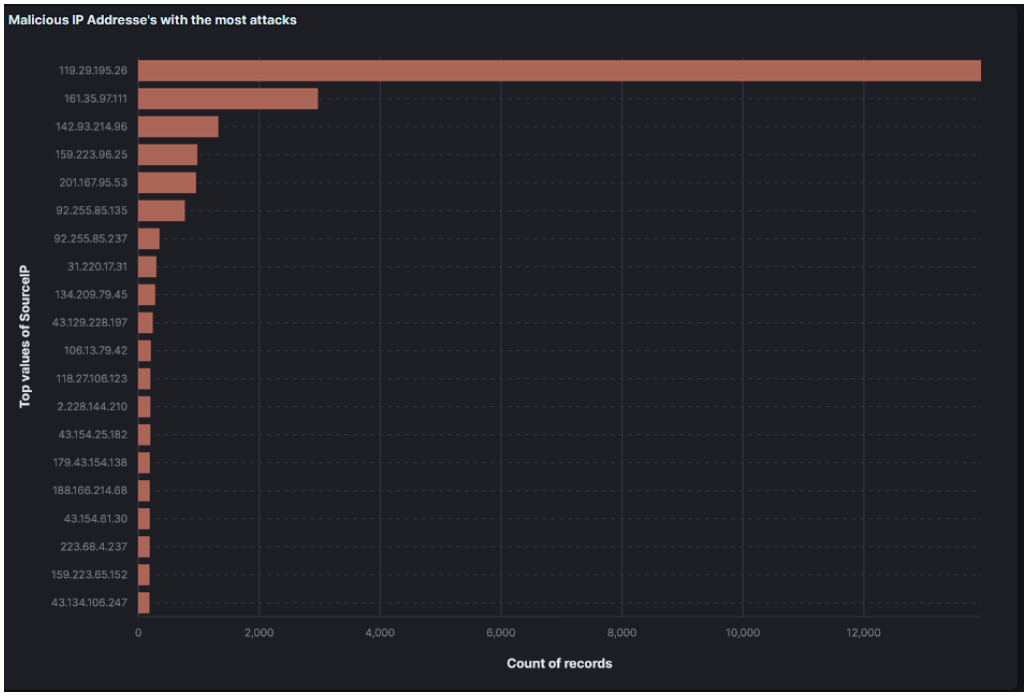
Εικόνα 29 Οι 10 κορυφαίοι κωδικοί πρόσβασης σε διάγραμμα μέσω του προγράμματος Kibana

Κατά την καταγραφή των επιθέσεων δημιουργήθηκε ειδικό φίλτρο που εντοπίζει την IP Address του επιτιθέμενου. Στην συνέχεια με την βοήθεια της βάσης δεδομένων του ELK stack πραγματοποιήθηκε αντιστοίχιση του ASN[24] της IP Address με την χώρα προέλευσης της επίθεσης. Η βάση δεδομένων του ELK stack ονομάζεται “GeoLite2-City”. Ο ρόλος του φίλτρου, που μας δείχνει τη χώρα προέλευσης της επιθέσης, είναι πολύ σημαντικός για κάθε εταιρεία καθώς τα τείχη προστασίας και όλα τα εργαλεία ασφάλειας υπολογιστικών συστημάτων διαθέτουν ειδικό αλγόριθμο που απαγορεύει τις επιθέσεις από συγκεκριμένες χώρες. Για παράδειγμα, γνωρίζοντας ότι η Κίνα, η Ινδία και η Σιγκαπούρη πραγματοποιούν πολλές επιθέσεις στο σύστημά μας, μπορούμε να απαγορεύσουμε οποιαδήποτε διεύθυνση διαδικτυακού πρωτοκόλλου από τις συγκεκριμένες χώρες να επικοινωνήσει με το διακομιστή μας. Αυτό εφαρμόζεται κυρίως σε εταιρείες και όχι στα πλαίσια αυτής της διπλωματικής, καθώς ο σκοπός είναι η έρευνα των επιθέσεων και δεν θέλουμε να μπλοκάρουμε κακόβουλες προσπάθειες από τις χώρες αυτές. Στον πίνακα 8 βλέπουμε τις κορυφαίες 20 χώρες από τις οποίες πραγματοποιήθηκαν οι κακόβουλες προσπάθειες.

Πίνακας 8 Οι 20 κορυφαίες χώρες προέλευσης επιθέσεων στο Honeypot

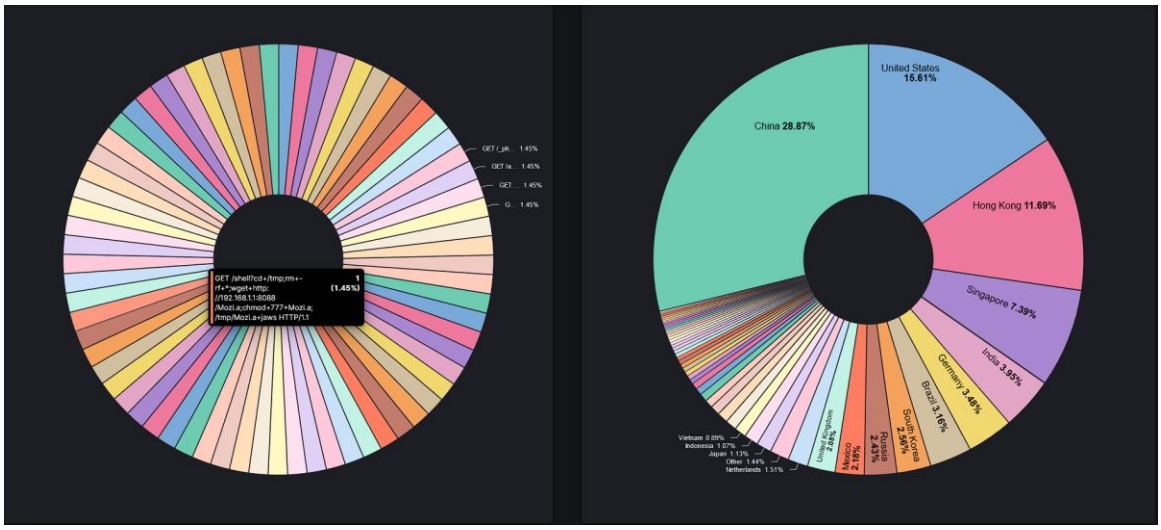
Χώρα	Ποσοστό Επιθέσεων
Κίνα	22,96%
ΗΠΑ	17,32%
Hong Kong	16,31%
Σιγκαπούρη	9,15%
Ινδία	5,86%
Γερμανία	4,21%
Νότια Κορέα	3,38%
Βραζιλία	3,23%
Ρωσία	2,69%
Αγγλία	2,48%
Ολλανδία	2,35%
Μεξικό	1,71%
Ινδονησία	1,63%
Γαλλία	1,35%
Βιετνάμ	1,3%
Ιαπωνία	1,06%
Καναδάς	0,85%
Κολομβία	0,77%
Ιταλία	0,77%
Αργεντινή	0,65%

Με τη βοήθεια των φίλτρων αναζήτησης του “Elasticsearch” μπορούμε να δούμε πόσες επιθέσεις πραγματοποιεί μία διεύθυνση διαδικτυακού πρωτοκόλλου, σε ποιες υπηρεσίες στοχεύουν οι επιθέσεις, το επίπεδο της επίθεσης δηλαδή αν ο επιτιθέμενος χρησιμοποιεί προηγμένες τεχνικές για την παραβίαση των συστημάτων. Όταν όμως θέλουμε να συγκεντρώσουμε τα αποτελέσματα τότε χρησιμοποιούμε τα φίλτρα αναζήτησης του “Kibana”. Στην εικόνα 30, η οποία δείχνει τις διευθύνσεις διαδικτυακού πρωτοκόλλου που έχουν επιχειρήσει τις περισσότερες κακόβουλες προσπάθειες, παρατηρούμε ότι πολλές IP addresses επιχειρούν πολλαπλές επιθέσεις σε διαφορετικές υπηρεσίες. Το συγκεκριμένο διάγραμμα μας δείχνει την επιμονή του επιτιθέμενου να παραβιάσει το Honeypot μας. Επιπρόσθετα, υπάρχει πιθανότητα πολλές από τις διευθύνσεις διαδικτυακού πρωτοκόλλου που παρουσιάζονται στο διάγραμμα, να είναι “proxy IP address” δηλαδή ο επιτιθέμενος για να μην φανερώσει την πραγματική του διεύθυνση πραγματοποιεί την επίθεση μέσω μιας διαφορετικής IP address, η οποία αποτελεί τον κόμβο για να περάσει η διαδικτυακή κίνηση μέσω αυτής.



Εικόνα 30 Οι κορυφαίες 20 IP Addresses που πραγματοποίησαν τις περισσότερες επιθέσεις

Τέλος, δημιουργήθηκε διάγραμμα που παρουσιάζει τις τεχνικές επίθεσης που χρησιμοποιήθηκαν. Η ανάλυση του συγκεκριμένου διαγράμματος, από ειδικούς πάνω στην ασφάλεια υπολογιστών και δικτύων, θα αναδείξει καινούριες τεχνικές, προγράμματα, γλώσσες προγραμματισμού και ευπάθειες που χρησιμοποιήθηκαν. Στην Εικόνα 31 φαίνονται τα γραφήματα, τα οποία περιέχουν κακόβουλές εντολές από τους επιτιθέμενους.



Εικόνα 31 Γραφήματα στο "Kibana" με τις τεχνικές επίθεσης που πραγματοποιήθηκαν στα παραπλανητικά μας συστήματα

Κεφάλαιο 5. Συμπεράσματα

Σε αυτό το κεφάλαιο, συνοψίζεται και αναλύεται η μεθοδολογία των πειραμάτων και τα αποτελέσματα της παρούσας διπλωματικής. Ο κύριος σκοπός της διπλωματικής ήταν η δημιουργία ενός υψηλής αλληλεπίδρασης Honeypot, το οποίο περιέχει τέσσερα δημοφιλή παραπλανητικά συστήματα και ένα πέμπτο Honeypot το οποίο δημιουργήθηκε να καλύψει τις ανάγκες αυτής. Με την εγκατάσταση και την ρύθμιση των κατάλληλων υπηρεσιών υλοποιήθηκε η εύρυθμη λειτουργία των παραπλανητικών συστημάτων με την πλατφόρμα εικονοποίησης των επιθέσεων “ELK stack”. Στην υπηρεσία “Logstash” δημιουργήθηκε ειδικό φίλτρο προκειμένου ο κώδικας των επιθέσεων να μετατρέπεται σε μορφή εύκολη και κατανοητή προς τους χρήστες. Στη συνέχεια τα δεδομένα αποθηκεύονταν στο “Elasticsearch” και παρουσιάζονταν στο “Kibana”, τα οποία εργαλεία αποθήκευσαν περίπου 500.000 επιθέσεις στο διάστημα τριών μηνών που ήταν λειτουργικό το Honeypot. Από τη 1 Μαρτίου έως τα τέλη Μαΐου, το σύστημα αποθήκευσε πολλά δεδομένα τα οποία έγινε ανάλυση και σχολιασμός στο τέταρτο κεφάλαιο, όπως οι συχνότεροι κωδικοί πρόσβασης που χρησιμοποιήθηκαν, τα συχνότερα ονόματα χρηστών που χρησιμοποιήθηκαν, τεχνικές παραβίασης των παραπλανητικών συστημάτων κτλ. Τέλος εγκαταστάθηκε το πρόγραμμα Fail2ban το οποίο αποτελεί πρόγραμμα αποκλεισμού των κακόβουλων χρηστών και απέτρεψε πολλές επιθέσεις στις πραγματικές υπηρεσίες του διακομιστή.

Συμπερασματικά, τα Honeypots αποτελούν ένα εργαλείο για την εκμάθηση των μεθόδων και των τεχνικών που χρησιμοποιούν οι κακόβουλες χρήστες. Επιπλέον συνδυάζοντας τα με μεγάλες αμυντικές τεχνικές, όπως τείχη προστασίας και συστήματα ανίχνευσης επιθέσεων, αυξάνουμε το επίπεδο στην ασφάλεια των υπολογιστικών συστημάτων. Ο ρόλος των Honeypot δεν είναι μόνο ερευνητικός καθώς μπορούν να αποτρέψουν και να ανιχνεύσουν σοβαρές επιθέσεις στην παραγωγή κάθε εταιρείας. Για την προτροπή μιας επίθεσης πρέπει πρώτα να ανιχνευθεί η κακόβουλη συμπεριφορά του χρήστη και εδώ έρχεται η αξία του Honeypot που είναι εξίσου σημαντική με την αξία των τείχων προστασίας και των antivirus.

Μελλοντικές Επεκτάσεις

Στόχος της διπλωματικής εργασίας είναι η δημιουργία ενός υψηλής αλληλεπίδρασης Honeypot, το οποίο θα ανιχνεύσει και θα αποτρέψει τις κυβερνοεπιθέσεις στα υπολογιστικά συστήματα μιας εταιρίας ή ενός οργανισμού και θα βοηθήσει τους ερευνητές στην καλύτερη ανάλυση των διαδικτυακών απειλών. Το εργαλείο αυτό είναι διαθέσιμο στον προσωπικό λογαριασμό στο github στο url “https://github.com/Bogiatzis”. Το συγκεκριμένο εργαλείο έχει δυνατότητες ανάπτυξης μετατρέποντας το σε SOC (Security Operation Center).

Τα τελευταία χρονιά στον χώρο της ασφάλειας υπολογιστών και δικτυών τα προηγμένα εργαλεία για την ανάλυση κυβερνοεπιθέσεων είναι τα Honeypot και το Soc. Η βασική τους διαφορά είναι ότι το Soc περιέχει κανόνες που ανιχνεύουν ύποπτη δραστηριότητα από τους χρήστες και ορίζουν την κρισιμότητα της επίθεσης. Για παράδειγμα, ο κανόνας που αφορά τις επιθέσεις Ddos θα ενεργοποιηθεί, όταν δει ότι μια ή πολλές διευθύνσεως διαδικτυακού πρωτοκόλλου πραγματοποιούν πάρα πολλές αιτήσεις προς τον διακομιστή και ανάλογα με τον αριθμό των αιτήσεων θα στείλει στο διαχειριστή της πλατφόρμας ειδοποίηση με βάση την κακόβουλη κίνηση που γίνεται και τον αριθμό κρισιμότητας της επίθεσης ο οποίος ανεβαίνει όσο ανεβαίνουν και οι αιτήσεις.

Συνεπώς για την ανάπτυξη του υψηλής αλληλεπίδρασης honeypot προτείνεται η εγκατάσταση του εργαλείου ElasticAlert, το οποίο είναι συμβατό με το ELK stack και την ρύθμιση κανόνων για την καλύτερη ανίχνευση κυβερνοεπιθέσεων.

ΕΡΜΗΝΙΑ ΑΓΓΛΙΚΩΝ ΩΡΩΝ

Αριθμός	Ορολογία	Ερμηνία	Ιστοσελίδα
[1]	Botnet		https://www.paloaltonetworks.com/cyberpedia/what-is-botnet
[2]	Hacker	Κακόβουλος χρήστης που πραγματοποιεί επιθέσεις	https://www.techtarget.com/searchsecurity/definition/hacker
[3]	MITRE ATTACK	Τεχνικές επίθεσης MITRE	https://attack.mitre.org/
[4]	Javascript	Γλώσσα προγραμματισμού	https://el.wikipedia.org/wiki/JavaScript
[5]	Trojan	Ιός με μεγάλη κρισιμότητα	https://www.kaspersky.com/resource-center/threats/trojans
[6]	Firewall	Τείχος προστασίας	https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/
[7]	Security Email Gateway	Τείχος προστασίας σε Email διακομιστή	https://www.forcepoint.com/cyber-edu/secure-email-gateway
[8]	Antivirus	Αμυντικό εργαλείο ενάντια στους ιούς	https://us.norton.com/internetsecurity-malware-what-is-antivirus.html
[9]	Cloud Monitor Analysis	Πλατφόρμα ανάλυσης δεδομένων σε cloud server	https://www.netapp.com/knowledge-center/what-is-cloud-monitoring/
[10]	User Behavior Analysis	Ανάλυση συμπεριφοράς χρήστη	https://en.wikipedia.org/wiki/User_behavior_analytics
[11]	VirusTotal	Πρόγραμμα	https://www.virustotal.com
[12]	Cisco	Εταιρία ασφάλειας υπολογιστών	https://www.cisco.com
[13]	Checkpoint	Εταιρία ασφάλειας υπολογιστών	https://www.checkpoint.com/
[14]	Blacklists	Βάσεις δεδομένων κακόβουλων IP Addresses	https://en.wikipedia.org/wiki/Blacklist_(computing)
[15]	0-day επιθέσεις	Ιοί με μεγάλη κρισιμότητα	https://en.wikipedia.org/wiki/Zero-day_(computing)
[16]	Linux debian 5	Λειτουργικό σύστημα	https://en.wikipedia.org/wiki/Debian
[17]	Deutsche Telekom Security	Εταιρία ασφάλειας υπολογιστών	https://www.telekom.com
[18]	ELK stack	Στοίβα ELK Stack	https://www.elastic.co/what-is/elk-stack
[19]	Hypervision	Λειτουργικό σύστημα	https://www.vmware.com/topics/glossary/content/hypervisor.html
[20]	Fail2ban	Τείχος προστασίας	https://www.fail2ban.org
[21]	Iptables	Εφαρμογή που ρυθμίζεις το δίκτυο	https://en.wikipedia.org/wiki/Iptables
[22]	Github	Ιστοσελίδα για προγραμματιστές	https://github.com/

[23]	Dockerhub	Βάση δεδομένων για Docker προγράμματα	https://hub.docker.com/
[24]	ASN	Αριθμός που φανερώνει την τοποθεσία της διεύθυνσης	https://www.whatismyip.com/asn/
[25]	DMZ	Αποστασιοποιημένη ζώνη στο τείχος προστασίας	https://en.wikipedia.org/wiki/DMZ_(computing)
[26]	Worm	Κατηγορία κακόβουλων προγραμμάτων	https://www.malwarebytes.com/computer-worm
[27]	Honeynet	Δίκτυο από Honeypot	https://www.techtarget.com/searchsecurity/definition/honeynet
[28]	Docker	Πρόγραμμα υλοποίησης κοντέινερ	https://www.docker.com/
[29]	Server	Διακομιστής	https://ti-einai.gr/server/
[30]	Containers	Ψεύτικα περιβάλλοντα εκτέλεσης λειτουργικού λογισμικού	https://www.docker.com/resources/what-container/
[31]	IP address	Διεύθυνση διαδικτυακού πρωτοκόλλου	https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address
[32]	cgroups	Εφαρμογή στο λειτουργικό Linux Debian	https://en.wikipedia.org/wiki/Cgroups
[33]	Virtual machine	Εικονική μηχανή	https://www.vmware.com/topics/glossary/content/virtual-machine.html
[34]	Kippo	Παραπλανητικό σύστημα honeypot	https://www.honeynet.org/projects/old/kippo/
[35]	Social Engineering	Κατηγορία επιθέσεων κοινωνικής μηχανικής	https://www.imperva.com/learn/application-security/social-engineering-attack/
[36]	Mac Address	Διεύθυνση που φανερώνει το κατασκευαστή του υπολογιστικού μηχανήματος	https://en.wikipedia.org/wiki/MAC_address
[37]	Payload	Ο κώδικας της επίθεσης και οι εντολές που εκτελούνται	https://www.techslang.com/definition/what-is-a-malicious-payload/

Βιβλιογραφία

1. Elasticsearch, URL:https://www.elastic.co/products/elasticsearch. Νοέμβριος 2021
2. Elastic Logstash, URL: https://www.elastic.co/products/logstash. Νοέμβριος 2021
3. Elastic Kibana, URL: https://www.elastic.co/products/kibana. Νοέμβριος 2021
4. Deutsche Telekom, URL: http://sicherheitstacho.eu/. Σεπτέμβριος 2021
5. IANA, URL:https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=1
6. dtag-dev-sec, URL: https://github.com/dtag-dev-sec/elasticpot. Σεπτέμβριος 2021
7. ELK Stack, URL: https://github.com/dtag-dev-sec/elk. Νοέμβριος 2021
8. MushMush, URL: https://github.com/mushorg/glastopf. Νοέμβριος 2021
9. kippo - SSH Honeypot, URL:https://github.com/desaster/kippo. Νοέμβριος 2021
10. Gosney, J. M. (2013). Top 100 adobe passwords with count. URL: http://stricture-group.com/files/adobe-top100.txt. Νοέμβριος 2021
11. Mirkovic, J. and Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review. Σεπτέμβριος 2021
12. Oracle Corporation, “Anatomy of a Cyber Attack: The Lifecycle of a Security Breach,” Νοέμβριος 2021.
13. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead.,” Computer Networks. Νοέμβριος 2021.
14. Statista GmbH, “IoT: Number of Connected Devices Worldwide 2012-2025 Statista.” URL: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Νοέμβριος 2021
15. United Nations, Department of Economic and Social Affairs Population Division, “World Population Prospects: The 2017 Revision, Key Findings and Advance Tables,” 2017. Νοέμβριος 2021
16. C. M. Lonvick and T. Ylonen, 2006, “The Secure Shell (SSH) Authentication Protocol.”. Νοέμβριος 2021
17. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the Mirai Botnet,” in 26th USENIX Security Symposium (USENIX Security). Σεπτέμβριος 2021
18. Supriyo Biswas, 2017, “An Introduction to the Docker Ecosystem - Boolean World.URL:”https://www.booleanworld.com/introduction-docker-ecosystem/”. Σεπτέμβριος 2021

19. Trost,2014, "Modern Honey Network Anomali."https://www.anomali.com/blog/mhn-modern-honey-network". Σεπτέμβριος 2021
20. T. Luo, "IoTCandyJar: Towards an Intelligent-Interaction Honeypot for IoT Devices," in Black Hat, (Las Vegas, NV, USA), 2017. Δεκέμβριος 2021
21. C. Leita, M. Dacier, and G. Wicherski, "SGNET: A Distributed Infrastructure to handle Zero-Day Exploits,", 2017. Δεκέμβριος 2021
22. A. Kedrowitsch, D. D. Yao, G. Wang, and K. Cameron, "A First Look: Using Linux Containers for Deceptive Honeypots," in Proceedings of the 2017 Workshop on Automated Decision Making for Active Cyber Defense, Dallas, USA. Δεκέμβριος 2021
23. N. Miramirkhani, M. P. Appini, N. Nikiforakis, and M. Polychronakis, "Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts", 2017. Δεκέμβριος 2021
24. J. Cito, V. Ferme, and H. C. Gall, "Using Docker Containers to Improve Reproducibility in Software and Web Engineering Research," Springer International Publishing, 2016. Δεκέμβριος 2021
25. Docker INC,"Docker Security/Docker Documentation." https://docs.docker.com/engine/security/security/, 2018. Νοέμβριος 2021
26. J. Chelladhurai, P. R. Chelliah, and S. A. Kumar, "Securing Docker Containers from Denial of Service (DoS) Attacks," in 2016 IEEE International Conference on Services Computing. Νοέμβριος 2021
27. M.Oosterhof, "cowrie/INSTALL.md at master-cowrie/cowrie. URL:" https://github.com/cowrie/cowrie/blob/master/INSTALL.md".
28. V. Ferme,2013,"Using Docker Containers to Improve Reproducibility in Software and Web Engineering." https://www.slideshare.net/vincenzoferme/using-docker-containers-to-improve-reproducibility-in-software-and-web-engineering. Νοέμβριος 2021
29. Elasticsearch Inc., "Heap: Sizing and Swapping — Elasticsearch: The Definitive Guide [2.x] — Elastic", URL: https://www.elastic.co/guide/en/elasticsearch/guide/current/heap-sizing.html" Ιανουάριος 2022
30. Mitchell Anicas, "How To Install Elasticsearch, Logstash and Kibana (ELK Stack) on Ubuntu 14.04 — DigitalOcean." URL: https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04.Ιανουάριος 2022
31. Fernando Dominiguez, 2021, "Logging Cowrie logs to the ELK stack." URL: http://blog.fernandodominguez.me/logging-cowrie-logs-to-the-elk-stack/. Ιανουάριος 2022
32. Check Point Software Technologies Ltd., "CheckPoint Software." URL: "https://www.checkpoint.com/defense/advisories/public/2021/cpai-2021-1016.html". Ιανουάριος 2022
33. Docker Inc., "Limit a container's resources — Docker Documentation." URL: https://docs.docker.com/config/containers/resource constraints/, 2022. Ιανουάριος 2022

34. Niels Provos. A Virtual Honeypot Framework 2003. URL: “citi.umich.edu/u/provos/papers/honeyd.pdf”. Ιανουάριος 2022
35. Jonathan White, Social network attack simulation with honeytokens. 2021. url: “http://link.springer.com/article/10.1007/s13278-014-0221-5”. Ιανουάριος 2022
36. The Honeynet Project “Know your Enemy: Learning about Security Threats”, Addison-Wesley Professional, 2nd edition. Ιανουάριος 2022
37. Honeypots: “Catching the Insider Threat “, Lance Spitzner Ankit Anubhav. Ιανουάριος 2022
38. Understanding the IoT Hacker — A Conversation With Owari/Sora IoT Botnet Author, 2018. URL “https://blog.newskysecurity.com/understanding-the-iot-hacker-a-conversation-with-owari-sora-iot-botnet-author-117feff
39. Sam Edwards and Ioannis Profetis, 2020. “Analysis of a decentralized internet worm for IoTdevices”. Ιανουάριος 2022
40. Niels Provos. Honeyd: A Virtual Honeypot Daemon, 2015,URL: http://repository.mdp.ac.id/ebook/library-sw-hw/linux-1/HONEYPOTS/honeyd/docs/honeyd-eabstract.pdf. Ιανουάριος 2022
41. Remco Verhoef. What is Honeytrap, URL: http://docs.honeytrap.io/docs/concepts/overview/what-is-honeytrap/. Ιανουάριος 2022