ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Τίτλος Εργασίας

ΣΥΓΚΡΙΤΙΚΗ ΑΠΟΤΙΜΗΣΗ ΕΠΙΔΟΣΗΣ ΣΥΣΤΗΜΑΤΩΝ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ (INTRUSION DETECTION SYSTEMS) ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΣΥΓΧΡΟΝΩΝ ΔΙΚΤΥΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Όνομα φοιτητή

ΚΟΥΤΣΟΔΗΜΗΤΡΟΠΟΥΛΟΥ ΑΝΑΣΤΑΣΙΑ



Αθήνα, 2019



ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΨΗΦΙΑΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΜΑΤΙΚΗΣ

Τριμελής Εξεταστική Επιτροπή

ΔΗΜΗΤΡΑΚΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ
Επίκουρος Καθηγητής, Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο

ΚΑΜΑΛΑΚΗΣ ΘΩΜΑΣ
Αναπληρωτής Καθηγητής, Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο

ΡΙΖΟΜΥΛΙΩΤΗΣ ΠΑΝΑΓΙΩΤΗΣ
Επίκουρος Καθηγητής, Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο

Η ΚΟΥΤΣΟΔΗΜΗΤΡΟΠΟΥΛΟΥ ΑΝΑΣΤΑΣΙΑ

δηλώνω υπεύθυνα ότι:

1) Είμαι ο κάτοχος των πνευματικών δικαιωμάτων της πρωτότυπης αυτής εργασίας και από όσο γνωρίζω η εργασία μου δε συκοφαντεί πρόσωπα, ούτε προσβάλει τα πνευματικά δικαιώματα τρίτων.

2) Αποδέχομαι ότι η ΒΚΠ μπορεί, χωρίς να αλλάξει το περιεχόμενο της εργασίας μου, να τη διαθέσει σε ηλεκτρονική μορφή μέσα από τη ψηφιακή Βιβλιοθήκη της, να την αντιγράψει σε οποιοδήποτε μέσο ή/και σε οποιοδήποτε μορφότυπο καθώς και να κρατά περισσότερα από ένα αντίγραφα για λόγους συντήρησης και ασφάλειας.

ΕΥΧΑΡΙΣΤΙΕΣ

Με την ολοκλήρωση της πτυχιακής μου εργασίας, θα ήθελα να ευχαριστήσω όλα εκείνα τα πρόσωπα που με στήριξαν, πίστεψαν σε εμένα και με βοήθησαν καθόλη τη διάρκεια των σπουδών μου.

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέπων καθηγητή της πτυχιακής μου εργασίας, κύριο Δημητρακόπουλο Γεώργιο, για την υποστήριξη και τις πολύτιμες συμβουλές του.

Θα ήθελα επίσης να ευχαριστήσω όλα τα μέλη της εξεταστικής επιτροπής, κύριο Καμαλάκη Θωμά και κύριο Ριζομυλιώτη Παναγιώτη, οι οποίοι μου έκαναν την τιμή να αξιολογήσουν την προσπάθεια μου.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, τους γονείς μου, που μου παρείχαν την αμέριστη στήριξη τους όλο αυτό το διάστημα, χωρίς την οποία τίποτα από όσα έχω καταφέρει μέχρι σήμερα δεν θα ήταν πραγματικότητα.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1 Εισαγωγη 13
1.1 Αντικειμενο Εργασιας 13
1.2 Διαρθρωση Εργασιας 13
2 Θεωρητικο Υποβαθρο 14
2.1 Intrusion Detection Systems 14
2.2 Επιθεσεις Επιπεδων TCP/IP 16
2.2.1 Network Layer 17
2.2.2 Transport Layer 18
2.2.3 Application Layer 19
3 Συστηματα Ανιχνευσης Εισβολων 20
4 Snort Intrusion Detection System 21
4.1 Εισαγωγη 21
4.2 Βασικα Στοιχεια 21
4.3 Αρχιτεκτονικη 23
4.3.1 Packet Decoder 24
4.3.2 Detection Engine 25
4.3.3 Logging and Alerting Subsystem 26
4.4 Advanced Snorting 26
4.4.1 Shoring up Commercial IDSs 27
4.4.2 Passive Traps 27
4.4.3 Focused Monitoring 28
4.5 Συμπερασματα 29
5 Darktrace 30
6 Darktrace Cyber AI 31
6.1 Εισαγωγη 31
6.2 Επιθεσεις 31
6.2.1 Insider Threat 31
6.2.2 Ransomware 32
6.2.3 Email Attacks 33
6.3 Darktrace Kai Cloud 35
6.3.1 Απειλες Στο Cloud 36
6.3.2 Darktrace Cloud 37
6.4 Συμπερασματα 37
7 Αλγοριθμος PCA – Principal Component Analysis 39

7.1 Εισαγωγη 39
7.2 Εφαρμογη PCA 39
7.3 Συμπερασματα 40
8 Ερευνητικο Υποβαθρο 42
8.1 Επιθεσεις 42
8.2 Χρονος 44
9 Συμπερασματα 46
9.1Περιληψη 46
9.2 Συμπερασμα 46
10 Πηγες Και Βιβλιογραφια 48

ΠΕΡΙΛΗΨΗ

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems) κατέχουν σημαντικό ρόλο στην ασφάλεια των πληροφοριακών συστημάτων. Η ασφάλεια των δεδομένων στα δίκτυα επικοινωνιών, αποτελεί μεγάλη πρόκληση με την ραγδαία αύξηση της κυκλοφορίας του δικτύου. Στα δίκτυα αυτά, κακόβουλοι χρήστες σχεδιάζουν τρόπους προκειμένου να διεισδύσουν στο δίκτυο. Τα IDSs έχουν αναπτυχθεί και προσαρμοστεί ώστε να λειτουργήσουν ως στρώμα προστασίας σε αυτές τις εξελισσόμενες επιθέσεις. Υπάρχουν πολλά Network Intrusion Detection Systems, αλλά η ακόλουθη έρευνα εστιάζει σε τρία συστήματα, τα οποία προσαρμόζονται περισσότερο στα δίκτυα επικοινωνιών. Η εργασία στοχεύει στον προσδιορισμό του συστήματος ανίχνευσης εισβολών με την καλύτερη επίδοση για να αντιμετωπίσει τις εκάστοτε επιθέσεις.

Ο Snort αποτελεί ένα σύστημα ανίχνευσης εισβολών ανοιχτού κώδικα, το οποίο δημιουργήθηκε το 1998 κι από τότε έχει εξελιχθεί σημαντικά. Το εργαλείο αυτό έχει τη δυνατότητα να εκτελεί ανάλυση της κυκλοφορίας σε πραγματικό χρόνο (real-time traffic analysis) και να καταγράφει πακέτα σε δίκτυο IP (Internet Protocol). Ένα θετικό χαρακτηριστικό του Snort αποτελεί η ικανότητα του να αποτρέπει τις απειλές. Επιθέσεις οι οποίες μπορούν να εντοπιστούν – και να αποτραπούν – από τον Snort είναι buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, καθώς και πολλές ακόμη. Ο Snort μπορεί ακόμη να χρησιμοποιηθεί με πιο «προχωρημένες» (advanced) επιλογές, οι οποίες παρουσιάζονται στα επόμενα κεφάλαια.

Ένα επιπλέον σύστημα ανίχνευσης εισβολών είναι το Cyber AI της Darktrace. Το συγκεκριμένο σύστημα έχει εξελιχθεί με στόχο όχι μόνο να ανιχνεύει, αλλά και να μετριάζει επιθέσεις σε πραγματικό χρόνο (real-time attacks) που βρίσκονται σε εξέλιξη (IPS). Το Darktrace Antigena βασίζεται στην τεχνητή νοημοσύνη – και αποτελεί ένα αυτοδίδακτο (self-learning) σύστημα, το οποίο μαθαίνει και προσαρμόζει το «φυσιολογικό μοντέλο ζωής» του συστήματος. Στην περίπτωση που παρατηρηθεί μια ασυνήθιστη δραστηριότητα, το AI ενεργοποιείται με στόχο να μετριάσει την απειλή. Ορισμένες επιθέσεις, οι οποίες εντοπίζονται από το Cyber AI της Darktrace, είναι Insider Threat, Ransomware attacks, καθώς και διάφορες ακόμη επιθέσεις, οι οποίες θα αναφερθούν αργότερα στην παρούσα έρευνα.

Από την άλλη πλευρά, ο PCA (Principal Component Analysis) αποτελεί μια κοινώς χρησιμοποιούμενη τεχνική μείωσης των διαστάσεων. Είναι σημαντικό να αναφερθεί πως ο αλγόριθμος αυτός μπορεί να χρησιμοποιηθεί με στόχο να ανιχνεύσει μια επίθεση, η οποία βρίσκεται σε εξέλιξη. Με βάση μια έρευνα που πραγματοποιήθηκε το 2007 [4], παρουσιάζεται μια προσέγγιση ανίχνευσης περιστατικών που χρησιμοποιεί πιθανοτικές μεθόδους δικτύου και επεξεργασίας για την εκμετάλλευση χωρικών και χρονικών συσχετισμών και εξαρτήσεων στα δίκτυα των οχημάτων.

Προκειμένου να εντοπιστεί πιο από τα παραπάνω IDS έχει καλύτερη επίδοση, πραγματοποιήθηκε μια έρευνα δύο σταδίων. Αρχικά, αναφέρονται οι επιθέσεις τις οποίες κάθε σύστημα ανιχνεύει επιτυχώς και στο δεύτερο μέρος, αναφέρεται ο χρόνος που απαιτείται προκειμένου να ανιχνευτούν οι επιθέσεις από τα IDSs.

Λέξεις κλειδιά: Ανίχνευση, Εισβολές, Τεχνητή Νοημοσύνη

ABSTRACT

Intrusion Detection Systems (IDSs) play a significant role in the security of information systems. Security of data in communication networks has become a major challenge, with the high increase of network traffic. In communication networks malicious users are devising ways of network intrusion and IDS has developed and adapted to act as a protection layer to these evolving attacks. There are several Network Intrusion Detection Systems, but the following research, focus on three systems; that adapted the most to communication networks. The study aims to determine which one of the IDSs has better performance to confront the emerging attacks.

Snort is an open source IDS that was created back in 1998 and has been evolving ever since. The tool has the capability to perform real-time traffic analysis and to record packets on Internet Protocol (IP) networks. On top of IDS Snort has the capability to prevent threats as well. Attacks that can be found – and prevented (IPS) – from Snort are buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort can also be used with more advanced options, that are presented in the following chapters.

Darktrace's Cyber AI is another IDS. It has evolved with the aim not only to detect, but also to mitigate real-time attacks that are on process (IPS). Darktrace Antigena is based on Artificial Intelligence – a self-learning system which learns and adapts the "normal pattern of life" of the system. In case an unusual activity takes place, the AI is activated in order to mitigate the threat. Some of the attacks that can be detected by Darktrace's Cyber AI are Insider Threat, Ransomware attacks, and various attacks that will be mentioned later on in this research.

On the other hand, PCA (Principal Component Analysis) is a commonly used dimensionality reduction technique. It is important to mention this algorithm can be used for attack detection. Based on a research in 2007 [4], an incident detection approach that uses probabilistic network and processing methodologies to exploit spatial and temporal correlations and dependencies in vehicular networks is presented.

In order to detect which of the above mentioned IDSs has better performance, a research of two stages was done. Firstly, are reported the attacks that each Intrusion Detection System successfully detects and as a second part, it is reported the time needed for the Intrusion Detection Systems to detect it.

Keywords: IDS, IPS, Snort, PCA, Darktrace

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: TCP/IP Layers [Jamie – 2019] 16
Εικόνα 2: Επίθεση IP Spoofing [Cloudflare.com] 17
Εικόνα 3: Επίθεση SYN-Floods [Cloudflare.com] 18
Εικόνα 4: Επίθεση Man-in-the-middle [imperva.com] 19
Εικόνα 5: Components of Snort [Pritika Mehra – 2012] 23
Εικόνα 6: Snort Architecture [Soumya Sen - 2007] 24
Εικόνα 7: Rule Chain Logical Structure [Martin Roesch - 1999] 25

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1: Είδη επιθέσεων στα IDSs 42

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
NIDS	Network Intrusion Detection System
HIDS	Host-based Intrusion Detection System
DoS	Denial of Service
IP	Internet Protocol
SLIP	Serial Line Internet Protocol
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
PCA	Principal Component Analysis
ITS	Intelligent Transportation System
AI	Artificial Intelligence
SaaS	Software As A Service
IaaS	Infrastructure As A Service
IoT	Internet of Things
SMB	Server Message Block
Tor	The onion router
OWASP	Open Web Application Security Project
CGI	Common Gateway Interface
ODBC	Open Database Connectivity
SQL	Structed Query Language
NIC	Network Interface Controller

1 ΕΙΣΑΓΩΓΗ

1.1 ΑΝΤΙΚΕΙΜΕΝΟ ΕΡΓΑΣΙΑΣ

Αντικείμενο της εργασίας είναι η αποτίμηση της επίδοσης των συστημάτων ανίχνευσης εισβολών (Intrusion Detection Systems – IDS) σε περιβάλλοντα δικτύων επικοινωνιών. Στη συνέχεια, παρουσιάζεται μια συγκριτική μελέτη των συστημάτων αυτών, με στόχο να εντοπιστεί εκείνο με την καλύτερη απόδοση.

Τα τελευταία χρόνια παρατηρείται έντονα η ανάγκη για προστασία των προσωπικών ηλεκτρονικών δεδομένων. Οι εισβολείς – γνωστοί και ως crackers – έχουν σημειώσει και συνεχίζουν να σημειώνουν αρκετές επιτυχημένες προσπάθειες με στόχο να εισβάλλουν σε αναγνωρισμένα δίκτυα εταιρειών. Παρόλο που οι τρέχουσες λύσεις ασφαλείας όπως τα firewalls, και λογισμικά anti-virus, κατέχουν σημαντικό ρόλο στην προστασία αυτών των οργανισμών, πολλές φορές δεν καταφέρνουν να εντοπίσουν όλους του τύπους επιθέσεων.

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) αποτελούν ένα μηχανισμό για την ανίχνευση διαφόρων επιθέσεων σε ένα δίκτυο. Υπάρχουν πολλά IDSs που διατίθενται σήμερα. Ορισμένα από αυτά είναι ανοιχτού κώδικα (open source) ενώ μερικά από αυτά διατίθενται για εμπορική χρήση (commercial use).

Αξίζει να σημειωθεί πως τα συστήματα ανίχνευσης εισβολών αποτελούν μέρος της υπολογιστικής υποδομής (computer infrastructure).

1.2 ΔΙΑΡΘΡΩΣΗ ΕΡΓΑΣΙΑΣ

Ο τρόπος διάρθρωσης της εργασίας, πραγματοποιείται με τον ακόλουθο τρόπο: Αρχικά, γίνεται μια παρουσίαση του απαραίτητου θεωρητικού υποβάθρου για τα συστήματα ανίχνευσης εισβολών (IDS). Στο τέταρτο κεφάλαιο, πραγματοποιείται η παρουσίαση του Snort ως σύστημα ανίχνευσης εισβολών. Αξίζει να σημειωθεί πως πραγματοποιείται και μια αναφορά και στις πιο «προχωρημένες» (advanced) επιλογές, με τις οποίες μπορεί να χρησιμοποιηθεί ο Snort. Στο πέμπτο κι έκτο κεφάλαιο, παρουσιάζεται το Cyber AI της εταιρείας Darktrace. Προκειμένου να γίνει περισσότερο κατανοητός ο τρόπος λειτουργίας του, πραγματοποιείται μια λεπτομερής αναφορά σε επιθέσεις τις οποίες το AI ανιχνεύει και μετριάζει με επιτυχία. Στο έβδομο κεφάλαιο, παρουσιάζεται ο αλγόριθμος PCA, καθώς και μια προσέγγιση ανίχνευσης περιστατικών στα δίκτυα των οχημάτων. Στο όγδοο κεφάλαιο, παρουσιάζονται στοιχεία για τις επιθέσεις τις οποίες αντιμετωπίζει το εκάστοτε IDS με επιτυχία, καθώς και ο απαραίτητος χρόνος που απαιτείται – για το καθένα ξεχωριστά – να εντοπίσει μια επίθεση, η οποία βρίσκεται σε εξέλιξη. Τέλος, πραγματοποιείται μια καταγραφή των συμπερασμάτων που εξήχθηκαν από τα στοιχεία, που συλλέχθηκαν στο προηγούμενο κεφάλαιο.

2 ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

2.1 INTRUSION DETECTION SYSTEMS

Χαρακτηρίζεται ως εισβολή (intrusion), οποιοδήποτε σύνολο ενεργειών που επιχειρούν να θέσουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα ή την διαθεσιμότητα ενός πόρου.[1]

Ενδεικτικές τεχνικές προκειμένου να αποτραπούν οι εισβολές αποτελούν η πιστοποίηση χρήστη (user authentication με χρήση κωδικών πρόσβασης ή βιομετρικών στοιχείων), η αποφυγή σφαλμάτων προγραμματισμού και η προστασία της πληροφορίας (ενδεικτικό παράδειγμα αποτελεί η κρυπτογράφηση – encryption). Η απλή αποτροπή μιας εισβολής δεν επαρκεί, επειδή τα συστήματα γίνονται όλο και πιο πολύπλοκα. Αξίζει να σημειωθεί πως υπάρχουν συνεχώς εκμεταλλεύσιμες αδυναμίες στα συστήματα λόγω σφαλμάτων σχεδιασμού, αλλά και προγραμματισμού ή ακόμη και διαφόρων τεχνικών διείσδυσης με «κοινωνικά σχεδιασμένο τρόπο». [1]

Τα συστήματα ανίχνευσης εισβολών (Intrusion Detection Systems - IDS) αποτελούν ένα από τα βασικά χαρακτηριστικά της ασφάλειας των υπολογιστικών υποδομών (computer infrastructures). Βασικός τους στόχους είναι να προστατεύουν - το δίκτυο - από τις προσπάθειες παραβίασης των αμυντικών μηχανισμών του.

Να σημειωθεί πως οι λύσεις ασφάλειας δικτύων μπορούν να ομαδοποιηθούν σε δύο κατηγορίες: τεχνικές αποτροπής *(prevention-based techniques)* και τεχνικές ανίχνευσης *(detection-based techniques).*

Οι τεχνικές αποτροπής, όπως είναι η κρυπτογράφηση (encryption) και η πιστοποίηση ταυτότητας (authentication) αποτελούν συχνά τον πρωτεύων αμυντικό μηχανισμό κατά των επιθέσεων.
Οι τεχνικές που βασίζονται στην ανίχνευση στοχεύουν στον εντοπισμό και αποκλεισμό του εισβολέα κατόπιν αποτυχημένων τεχνικών αποτροπής. Αυτού του είδους τεχνικές, χωρίζονται σε δύο μεγάλες κατηγορίες:

1. Ανίχνευση υπογραφής (signature detection): Οι παρούσες τεχνικές, ταιριάζουν με γνωστά προφίλ επίθεσης με τις τρέχουσες αλλαγές.
2. Ανίχνευση ανωμαλιών (anomaly detection): Το συγκεκριμένο είδος τεχνικής, χρησιμοποιεί τα καθιερωμένα κανονικά προφίλ και ανιχνεύει ασυνήθιστες αποκλίσεις από την κανονική συμπεριφορά.

Τα συστήματα ανίχνευσης εισβολών ταξινομούνται σε δύο κατηγορίες, με βάση τις πηγές πληροφοριών ελέγχου (audit information):

1. Host-based Intrusion Detection System (HIDS): Σε αυτή την κατηγορία, συγκαταλέγονται οι επιθέσεις, οι οποίες πραγματοποιούνται εναντίον ενός μόνο κεντρικού υπολογιστή. Το HIDS χρησιμοποιείται σε συστήματα τα οποία είναι πιο ευάλωτα σε επιθέσεις, όπως είναι ο Web Server (διακομιστής ιστού). Το HIDS προκειμένου να πραγματοποιήσει

ανίχνευση κάποιας εισβολής, οφείλει να συγκεντρώσει πληροφορίες από τις κλήσεις συστήματος, τις διαδρομές ελέγχου του λειτουργικού συστήματος, καθώς και τα αρχεία καταγραφής εφαρμογών. Παραδείγματα του HIDS αποτελούν το Tripware και το OSSSEC.

2. Network-based Intrusion Detection System (NIDS): Σε αυτή την κατηγορία ανιχνεύονται επιθέσεις, οι οποίες πραγματοποιούνται σε διάφορα συστήματα στο επίπεδο του δικτύου. Το NIDS χρησιμοποιεί την κυκλοφορία δικτύου (network traffic) προκειμένου να ανιχνεύσει ύποπτες δραστηριότητες και τελικά να αποτρέψει παράνομη πρόσβαση σε δικτυακούς πόρους (network resources). Ενδεικτικά παραδείγματα του NIDS αποτελούν ο Bro, ο Snort και ο Suricata.

Με βάση την ανάλυση των γεγονότων, υπάρχουν κυρίως δύο τύποι προσεγγίσεων: Τα misuse-based συστήματα ανίχνευσης εισβολών και τα anomaly-based συστήματα.

1. Misuse-Based Intrusion Detection System: Χρησιμοποιεί διάφορες τεχνικές αντιστοίχισης (matching techniques) προκειμένου να βρει μια αντιστοιχία μεταξύ των δραστηριοτήτων του συστήματος και των ήδη γνωστών υπογραφών επίθεσης (attack signatures) που είναι αποθηκευμένες στη βάση δεδομένων. Αξίζει να τονιστεί, πως μια άλλη ονομασία του παρόντος IDS αποτελεί η προσέγγιση με βάση την υπογραφή (Signature-based Approach).

Ωστόσο, υπάρχουν αρκετά θετικά και αρνητικά στοιχεία, τα οποία χαρακτηρίζουν τα Misused-Based IDSs και αξίζει να καταγραφούν.

Στα θετικά στοιχεία των συγκεκριμένων συστημάτων ανίχνευσης εισβολών, συγκαταλέγονται, η ανίχνευση επιθέσεων χωρίς τη σηματοδότηση false-positive συναγερμών (alarms), καθώς και η παροχή μιας εύκολης χρήσης εργαλείου, που έχει ως στόχο την παρακολούθηση των συστημάτων.

Ωστόσο, τα Misuse-Based συστήματα ανίχνευσης, δεν έχουν την δυνατότητα να ανιχνεύσουν νέες επιθέσεις καθώς κάθε φορά που εκτίθενται σε μια νέα επίθεση, είναι απαραίτητο τα συστήματα αυτά να ενημερώνονται. Αξίζει ακόμη να υπογραμμιστεί πως οι misuse detectors, προορίζονται να παρατηρούν επιθέσεις που διαθέτουν υπογραφές, ήδη γνωστές στο σύστημα. Το συγκεκριμένο σύστημα ανίχνευσης εισβολών, δεν δύναται να εντοπίσει γνωστές επιθέσεις, στην περίπτωση την οποία αυτές έχουν υποστεί τροποποίηση.

2. Anomaly-Based Intrusion Detection System: Τα συγκεκριμένα συστήματα ανίχνευσης εισβολών, εντοπίζουν τις συμπεριφορές των δραστηριοτήτων του χρήστη και του συστήματος. Αρχικά, δημιουργείται προφίλ χρηστών, εξυπηρετητών και όλων των συνδέσεων δικτύου. Κατόπιν, δημιουργείται ένας συναγερμός στην περίπτωση που τα νέα δεδομένα αποκλίνουν από εκείνα τα οποία

βρίσκονται αποθηκευμένα στη βάση δεδομένων των προφίλ χρηστών, των συστημάτων και των συνδέσεων του δικτύου.

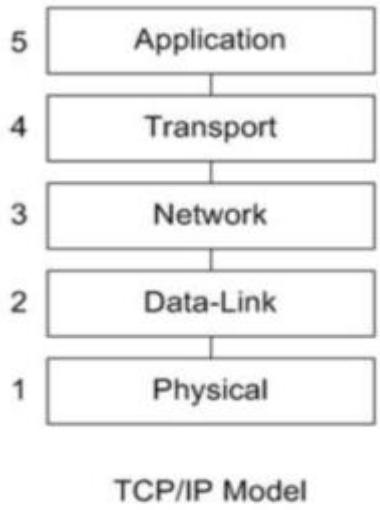
Και σε αυτή την περίπτωση, υπάρχουν ορισμένα θετικά και αρνητικά στοιχεία, τα οποία χαρακτηρίζουν τα Anomaly-Based IDSs και αξίζει να σημειωθούν.

Σε αντίθεση από τα Misused-Based IDSs, τα Anomaly-Based συστήματα ανίχνευσης εισβολών, είναι σε θέση να ανιχνεύσουν νέες επιθέσεις. Ακόμη κι όταν δεν υπάρχουν επαρκείς πληροφορίες για την επίθεση που βρίσκεται σε εξέλιξη. Αξίζει να αναφερθεί πως μπορούν να χρησιμοποιηθούν για την απόκτηση πληροφοριών υπογραφής που χρησιμοποιούνται από τα Signature-Based συστήματα ανίχνευσης επιθέσεων.

Από την άλλη πλευρά, τα Anomaly-Based IDSs, σηματοδοτούν ένα μεγάλο αριθμό false-positive ως συμπεριφορές των χρηστών και του δικτύου. Αυτή η προσέγγιση, απαιτεί ένα τεράστιο σύνολο δεδομένων κατάρτισης για τον καθορισμό των ορίων για τις συνήθεις δραστηριότητες των συστημάτων.

2.2 Επιθεσεις Επιπεδων TCP/IP

Το μοντέλο TCP/IP αποτελείται από 5(πέντε) στρώματα, όπως φαίνεται και στην εικόνα που ακολουθεί (Εικόνα 1). Πιο συγκεκριμένα, αποτελείται από το Physical Layer, το Data Link Layer, το Network Layer, το Transport Layer και το Application Layer. Τα επίπεδα τα οποία είναι πιο ευάλωτα σε επιθέσεις, είναι τα Network, Transport και Application Layers.



Εικόνα 1: TCP/IP Layers [Jamie – 2019]

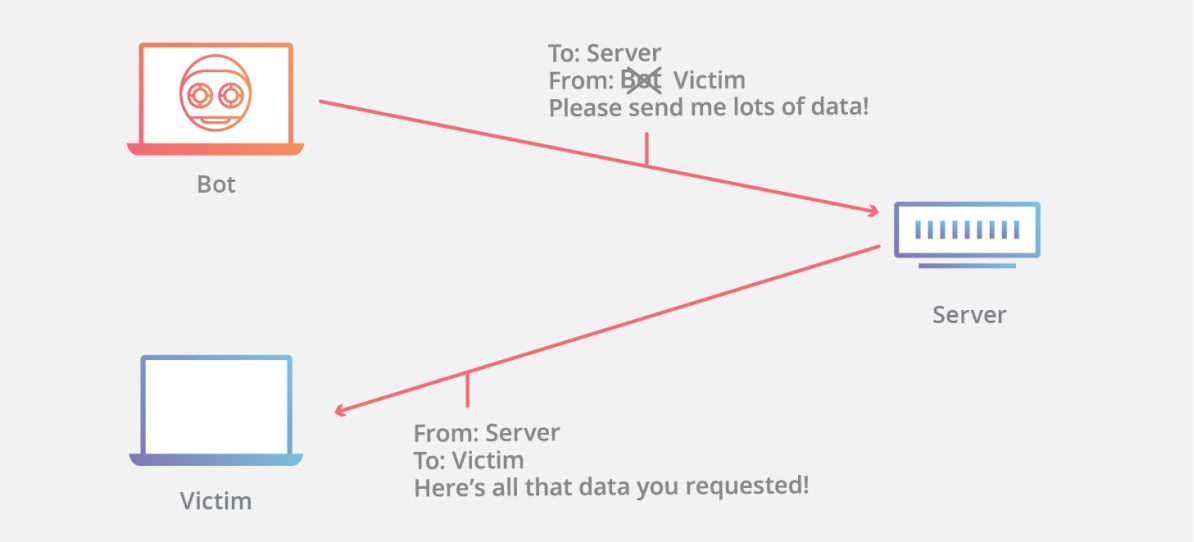
Οι πιο κοινές επιθέσεις που συμβαίνουν στα επίπεδα αυτά, παρουσιάζονται παρακάτω.

2.2.1 Network Layer

Υπάρχουν διάφορες επιθέσεις στο Network Layer, όπως είναι το eaves dropping, IP spoofing, Denial of Service, Man-in-the-middle Attack και Sniffer Attack.

Παρακάτω, παρουσιάζονται αναλυτικά οι επιθέσεις IP spoofing και Denial of Service, ως ενδεικτότερα είδη επιθέσεων τα οποία ενδέχεται να προκληθούν στο επίπεδο Δικτύου (Network Layer).

- IP Spoofing: Στην παρούσα περίπτωση επίθεσης, ο εισβολέας αποστέλλει μηνύματα με διεύθυνση forge IP στον κεντρικό εξυπηρετητή. Με αυτό τον τρόπο παρέχει την εντύπωση πως τα μηνύματα προέρχονται από έναν αξιόπιστο εξυπηρετητή. Βασικός σκοπός είναι να αποκτηθεί παράνομη πρόσβαση στον εξυπηρετητή - στόχο ή άλλους κόμβους του δικτύου. Σε πρώτο στάδιο, ο εισβολέας εφαρμόζει διάφορες τεχνικές προκειμένου να εντοπίσει μια διεύθυνση IP ενός αξιόπιστου διακομιστή στο δίκτυο και στη συνέχεια να αλλάξει τις κεφαλίδες πακέτων, έτσι ώστε να φαίνεται ότι ο αξιόπιστος εξυπηρετητής στέλνει τα πακέτα. Στην εικόνα που ακολουθεί (Εικόνα 2), φαίνεται ενδεικτικά ο τρόπος λειτουργίας του IP Spoofing.



Εικόνα 2: Επίθεση IP Spoofing [Cloudflare.com]

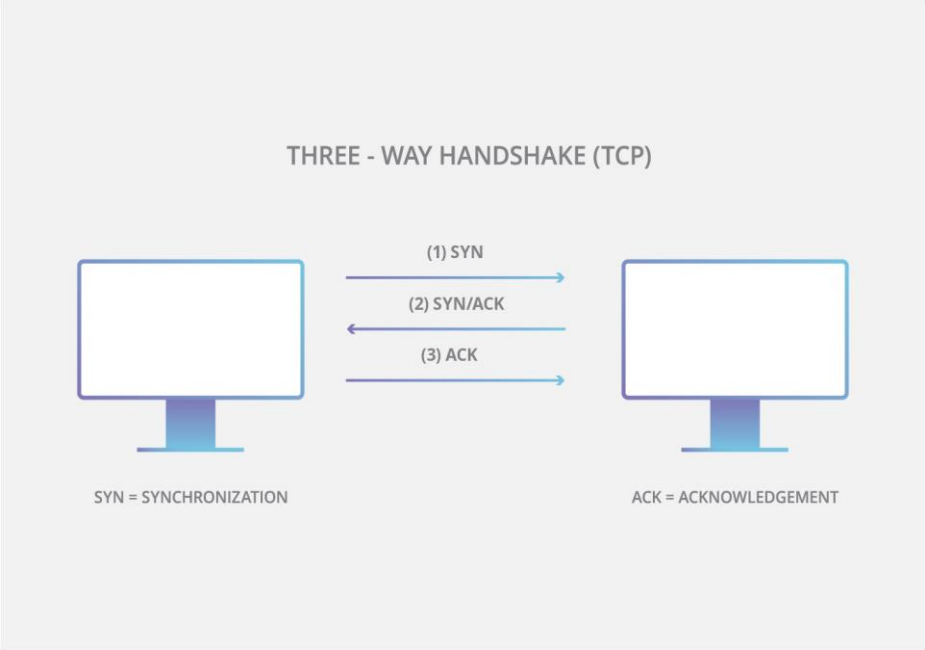
- Denial of Service (DoS) Attack: Το συγκεκριμένο είδος επίθεσης, αποτελεί μια προσπάθεια να καταστούν οι πόροι του συστήματος ή του δικτύου απρόσιτοι. Υπάρχουν πολλοί τρόποι προκειμένου να εκτελεστεί μια επίθεση άρνησης παροχής υπηρεσιών, όπως για παράδειγμα η επαναφορά των πληροφοριών κατάστασης των περιόδων σύνδεσης TCP ή SYN Floods. Η επίθεση DoS δύναται να πραγματοποιηθεί στο Network Layer, ωστόσο μπορεί να πραγματοποιηθεί στο Transport Layer και στο Application Layer.

2.2.2 TRANSPORT LAYER

Υπάρχουν διάφορες επιθέσεις στο Transport Layer, όπως είναι η επίθεση SYN-Floods, η SSL Man-in-the-middle Attack, TCP Connection Hijacking (*Σημείωση: Πρόκειται για επίθεση Man-in-the-middle*), UDP Flood Attack και Port Scan Attack.

Μεταξύ όσων επιθέσεων προαναφέρθηκαν, παρακάτω παρουσιάζονται ενδεικτικά οι επιθέσεις SYN-Floods και TCP Connection Hijacking.

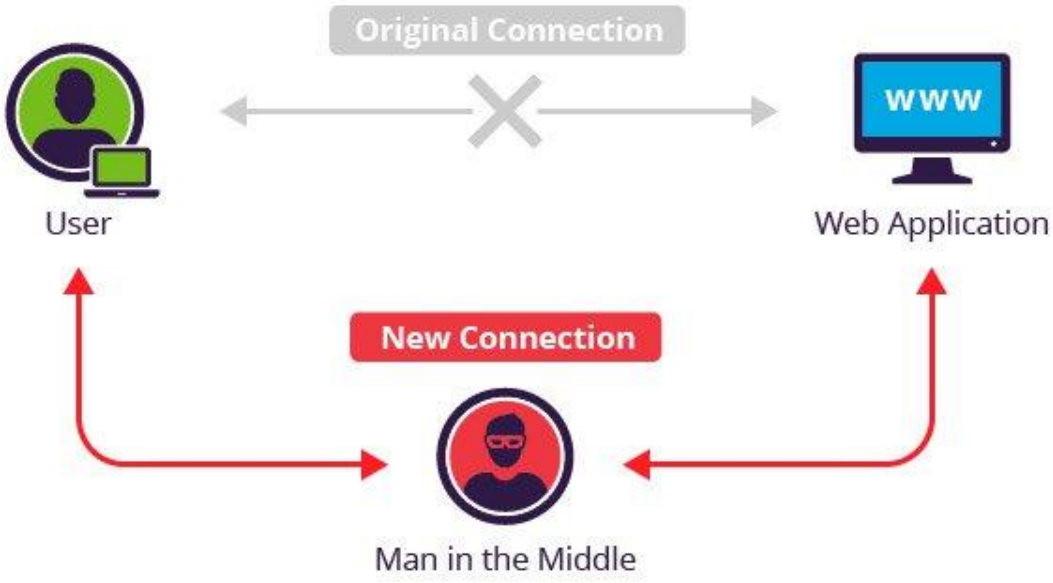
- SYN-Floods: Στην περίπτωση όπου ένας πελάτης επιθυμεί να δημιουργήσει μια σύνδεση TCP με έναν διακομιστή, τότε οφείλει να περάσει από τη διαδικασία 3(τριών) τρόπων "χειραψίας" – 3-way handshake process. Αρχικά, αποστέλλεται από τον διακομιστή ένα συγχρονισμένο μήνυμα γνωστό και ως SYN. Στη συνέχεια, ο διακομιστής αποστέλλει στον πελάτη μήνυμα επιβεβαίωσης (Acknowledgement message) γνωστό και ως SYN-ACK. Τέλος, ο πελάτης στέλνει ACK στον εξυπηρετητή και η σύνδεση δημιουργείται (Εικόνα 3). Η επίθεση SYN-Flood πραγματοποιείται με πλημμύρα (flooding) του εξυπηρετητή - στόχου με ψευδή αιτήματα σύνδεσης, αποστέλλοντας χιλιάδες SYN. Αυτή η διαδικασία είναι γνωστή ως SYN Floods. Εξαιτίας αυτής της επίθεσης, ο εξυπηρετητής φτάνει μέγιστο πλήθος πελατών που μπορεί να εξυπηρετήσει και πολλές εξουσιοδοτημένες αιτήσεις δεν θα απαντηθούν [2].



Εικόνα 3: Επίθεση SYN-Floods [Cloudflare.com]

- TCP Connection Hijacking: Το συγκεκριμένο είδος επίθεσης είναι επίσης γνωστό ως Man-in-the-Middle attack του Transport Layer. Αυτή η επίθεση συμβαίνει όταν ολοκληρωθεί ο έλεγχος ταυτότητας μεταξύ των εξυπηρετητών. Ο εισβολέας παίρνει τον έλεγχο της σύνδεσης και

στέλνει πλαστά πακέτα σε ένα από τους εξυπηρετητές για να ανακτήσει σημαντικές πληροφορίες (Εικόνα 4). Οι αριθμοί ακολουθίας των πακέτων από μια συνεχή σύνδεση αποκτώνται και τα πλαστά πακέτα, αποστέλλονται με τον επόμενο αριθμό ακολουθίας [2].



Εικόνα 4: Επίθεση Man-in-the-middle [imperva.com]

2.2.3 Application Layer

Στη σύγχρονη εποχή, το Application Layer αποτελεί κοινό στόχο των crackers. Ενδεικτικά είδη επιθέσεων είναι τα ακόλουθα: Scripting Vulnerabilities, Buffer Overflows, Cookie Poisoning, Hidden Field Manipulation, Parameter Tampering, Cross-Site Scripting, SQL Injection.

Παρακάτω παρουσιάζονται το SQL Injection καθώς και το Cross-Site Scripting.

- SQL Injection Attack: Στο συγκεκριμένο είδος επίθεσης, ο εισβολέας καταγράφει τις αρχικές εντολές σε Structured Query Language (SQL) και εισάγει ένα κομμάτι κώδικα SQL, με στόχο να προκαλέσει αλλαγές στην βάση δεδομένων. Μια ενεργή επίθεση SQL Injection, έχει τη δυνατότητα να διαβάσει ευαίσθητα δεδομένα από τη βάση δεδομένων, όπως και να να τροποποιήσει τα περιεχόμενα της βάσης.
- Cross-Site Scripting (XSS) Attack: Αποτελεί ένα είδος επίθεσης, το οποίο συναντάται συχνά σε επιθέσεις εφαρμογών Web. Ο επιτιθέμενος προσθέτει ένα browser-side script στις ιστοσελίδες, με αποτέλεσμα να επηρρεάζει το περιεχόμενο που βλέπουν οι τελικοί χρήστες. Το script αυτό εκτελείται από το browser του χρήστη. Ο browser δεν δύναται να γνωρίζει πως το συγκεκριμένο script δεν έπρεπε να εκτελεστεί, καθώς θεωρεί πως προέρχεται από μια έμπιστη πηγή. Έτσι, το script – και κατ'επέκταση κι ο cracker – έχει την δυνατότητα πρόσβασης σε cookies, session tokens, καθώς και άλλες ευαίσθητες πληροφορίες.

3 ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΩΝ

Τα συστήματα ανίχνευσης εισβολών που επιλέχθηκαν προκειμένου να πραγματοποιηθεί μελέτη στην απόδοση τους είναι, ο Snort, το Darktrace AI και ο αλγόριθμος PCA. Το δεύτερο, αποτελεί προϊόν της εταιρείας Darktrace, η οποία ειδικεύεται στην ασφάλεια πληροφοριακών συστημάτων.

Παρακάτω, παρατίθενται τα συστήματα αυτά, με αναλυτικές πληροφορίες, οι οποίες σχετίζονται με τον τρόπο λειτουργίας τους, την αρχιτεκτονική τους, καθώς και τις επιθέσεις τις οποίες δύνανται να αντιμετωπίσουν.

4 SNORT INTRUSION DETECTION SYSTEM

4.1 ΕΙΣΑΓΩΓΗ

Ο Snort αποτελεί ένα σύστημα ανίχνευσης εισβολών (intrusion detection system) ανοιχτού κώδικα καθώς και συστήματος «αποτροπής» (prevention system), το οποίο δημιουργήθηκε το 1998 από τον Martin Roesch. Η ανάπτυξη του κώδικα πραγματοποιήθηκε σε γλώσσα προγραμματισμού C. Στη σημερινή εποχή, αποτελεί ένα λογισμικό το οποίο προγραμματίζεται και κυκλοφορεί από την Cisco Systems. Αποτελεί ένα εργαλείο για μικρά δίκτυα, στα οποία πραγματοποιείται ελάχιστη χρήση πόρων. Ο Snort αποτελεί ένα χρήσιμο εργαλείο, του οποίου το κόστος δεν είναι υψηλό. Το κόστος των σύγχρονων συστημάτων ανίχνευσης εισβολών ανέρχεται σε πολλές χιλιάδες δολλάρια και σε ακραίες περιπτώσεις, οι τιμές ενδέχεται να αυξηθούν πολύ παραπάνω. Ο Snort διατίθεται υπό το GNU General Public License (GNU89) και είναι δωρεάν για χρήση σε οποιοδήποτε περιβάλλον.

Ο βασικός λόγος μελέτης του Snort, αποτελεί το γεγονός ότι είναι οικονομικά, τεχνικά ή και διοικητικά το ευκολότερα υλοποιήσιμο από άλλα εργαλεία ανοικτού κώδικα ή εμπορικά διαθέσιμα εργαλεία.

Ο Snort έχει τη δυνατότητα να εκτελεί ανάλυση κυκλοφορίας σε πραγματικό χρόνο (real-time traffic analysis), καθώς και να πραγματοποιεί καταγραφή πακέτων σε δίκτυα Internet Protocol (IP). Ως σύστημα ανίχνευσης επιθέσεων, ο Snort, μπορεί να αξιοποιηθεί για την ανίχνευση probes ή επιθέσεων, συμπεριλαμβανομένου, των προσπαθειών αποτύπωσης λειτουργικού συστήματος (system fingerprinting attempts), της κοινής διασύνδεσης πύλης (common gateway interface), της υπερχείλισης των buffer (buffer overflows), καθώς και των ανιχνευτών μπλοκ μηνυμάτων (server message block probes – SMB probes).

Υπάρχουν 3 κύριες λειτουργίες οι οποίες μπορούν να περιγράψουν με ακρίβεια το Snort. Οι λειτουργίες αυτές είναι:

- *Sniffer*: Οι λειτουργίες Sniffer διαβάζουν πακέτα δικτύου και τα εμφανίζουν στην κονσόλα, σε συνεχή ροή.
- *Καταγραφικό πακέτο (Packet Logger)*: Η λειτουργία καταγραφής πακέτων, έχει ως στόχο να καταγράφει τα πακέτα δικτύου στο δίσκο.
- *Ανίχνευση εισβολής δικτύου (Network Intrusion Detection)*: Η λειτουργία ανίχνευσης εισβολής σε δίκτυο, αποτελεί την περισσότερο πολύπλοκη από τις λειτουργίες που περιγράφηκαν παραπάνω. Η συγκεκριμένη λειτουργία, παρακολουθεί την κυκλοφορία του δικτύου και την αναλύει σε σχέση με ένα σύνολο κανόνων που ορίζει ο χρήστης.

4.2 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ

Ο διαχωρισμός του Snort έγεκιται σε δύο κατηγορίες: σε λογικά και πολλαπλά στοιχεία. Αυτά τα στοιχεία συνεργάζονται με στόχο να ανιχνεύσουν

συγκεκριμένες επιθέσεις και να παράγουν αποτελέσματα σε μια απαιτούμενη μορφή από το σύστημα ανίχνευσης.

Τα Intrusion Detection Systems τα οποία βασίζονται στο Snort αποτελούνται από τα ακόλουθα κύρια συστατικά μέρη:

1. Packet Decoder (Αποκωδικοποιητής πακέτων)
2. Pre-processors (Προ-επεξεργαστές)
3. Detection Engine (Μηχανή Ανίχνευσης)
4. Logging and Alerting System (Σύστημα καταγραφής και ειδοποίησης)
5. Output Modules (Μονάδες εξόδου)

Πιο συγκεκριμένα:

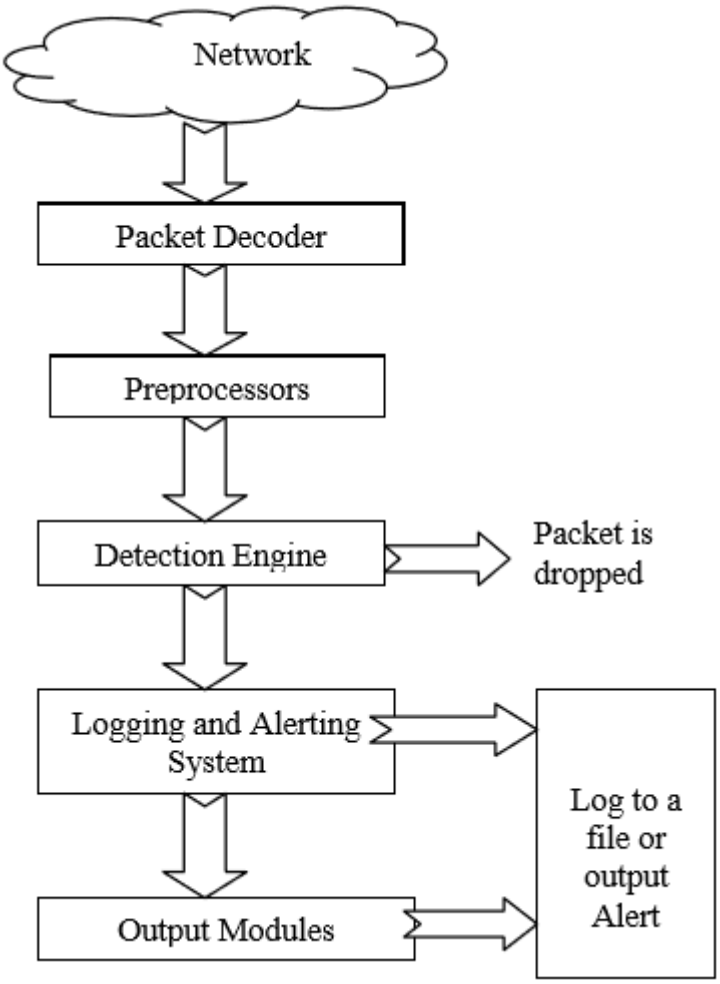
Packet Decoder: Ο αποκωδικοποιητής πακέτων λαμβάνει πακέτα από διάφορους τύπους διεπαφών δικτύου και προετοιμάζει τα πακέτα εκείνα που πρόκειται προ-επεξεργαστούν (Pre-processed) ή να αποσταλούν στη μηχανή ανίχνευσης (Detection Engine). Οι πιο συνήθεις διεπαφές είναι Ethernet, SLIP, και SSL.

Pre-processors or Input Plug-ins: Οι προ-επεξεργαστές αποτελούν συστατικά στοιχεία ή προσθήκες που μπορούν να χρησιμοποιηθούν σε συνδυασμό με το Snort για τη ρύθμιση ή την τροποποίηση των πακέτων δεδομένων. Αυτό είναι αναγκαίο να συμβεί προτού ο μηχανισμός ανίχνευσης κάνει κάποια λειτουργία προκειμένου να διαπιστώσει αν το πακέτο χρησιμοποιείται από τον εισβολέα. Αξίζει να σημειωθεί πως χρησιμοποιούνται επίσης για την ομαλοποίηση των κεφαλίδων πρωτοκόλλων (Protocol Headers), την ανίχνευση ανωμαλιών, την επανασυναρμολόγηση πακέτων (Packet Reassembly), καθώς και την επανασυναρμολόγηση της ροής TCP (TCP Stream Reassembly).

Detection Engine: Ο μηχανισμός ανίχνευσης αποτελεί το σημαντικότερο μέρος του Snort. Αυτός είναι υπεύθυνος να ανιχνεύσει την ύπαρξη δραστηριότητας παρείσδυσης σε ένα πακέτο.

Logging and Alerting Subsystem: Το σύστημα καταγραφής και ειδοποίησης δημιουργεί μηνύματα συναγερμού και ημερολογίου ανάλογα με το τι εντοπίζει η μηχανή ανίχνευσης μέσα σε ένα πακέτο.

Output Modules: Οι ενότητες εξόδου ή plug-ins ειδοποιούν, παράγουν και καταγράφουν τελική έξοδο.



Εικόνα 5: Components of Snort [Pritika Mehra – 2012]

Αξίζει να τονιστεί πως ο Snort υποστηρίζεται σε διάφορες πλατφόρμες hardware και λειτουργικά συστήματα. Το σύστημα αυτό είναι διαθέσιμο για: Linux, OpenBSD, FreeBSD, NetBSD, Solaris (καθώς και Sparc και i380), HP-UX, AIX, IRIX, MacOS και Windows. Έτσι, το εργαλείο Snort τρέχει σε οποιοδήποτε σύγχρονο λειτουργικό σύστημα και κάθε παλιό υλικό.

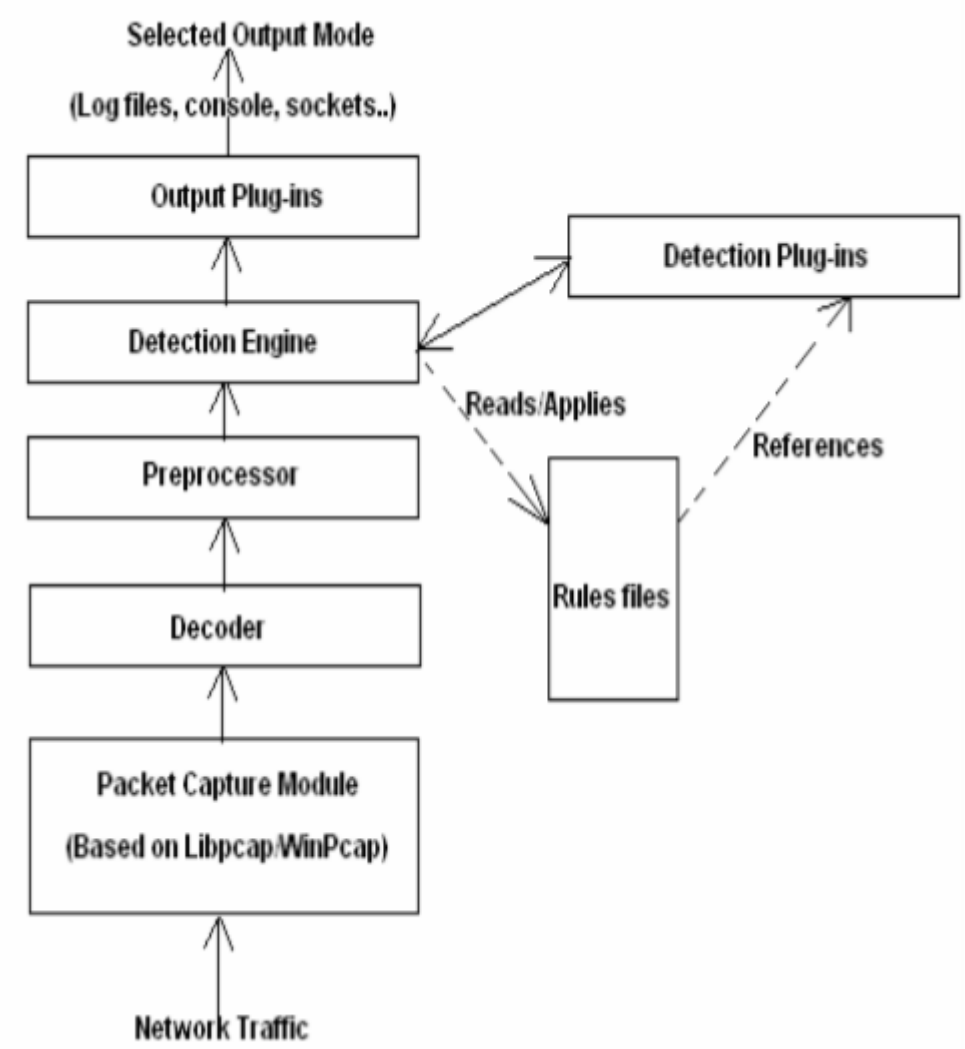
4.3 ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Η αρχιτεκτονική του Snort, επικεντρώνεται στην απόδοση, την απλότητα και την ευελιξία. Τα τρια κύρια υποσυστήματα που απαρτίζουν τον Snort είναι ο Packet Decoder, το Detection Engine και το Logging and Alerting Subsystem. Τα τρία αυτά υποσυστήματα βγαίνουν πάνω από το libpcap promiscuous πακέτο της sniffing βιβλιοθήκης, η οποία παρέχει ένα φορητό πακέτο Sniffing καθώς και την δυνατότητα φιλτραρίσματος.

Αξίζει να τονιστεί πως προτού ξεκινήσει η αρχικοποίηση της ενότητας του sniffer, σε πρώτο στάδιο είναι απαραίτητο να υλοποιηθούν τα εξής: Διαμόρφωση προγράμματος, ανίχνευση κανόνων και δομή δεδομένων. Με αυτό τον τρόπο, διατηρείται η ποσότητα ανά επεξεργασία πακέτων στο

ελάχιστο απαιτούμενο, προκειμένου να επιτευχθεί το βασικό πρόγραμμα λειτουργικότητας.

Πιο συγκεκριμένα, στην εικόνα που ακολουθεί παρουσιάζεται η αρχιτεκτονική του Snort (Εικόνα 6).



Εικόνα 6: Snort Architecture [Soumya Sen - 2007]

Στη συνέχεια καταγράφονται περισσότερες λεπτομέρειες, οι οποίες αφορούν τα αναφερόμενα υποσυστήματα.

4.3.1 PACKET DECODER

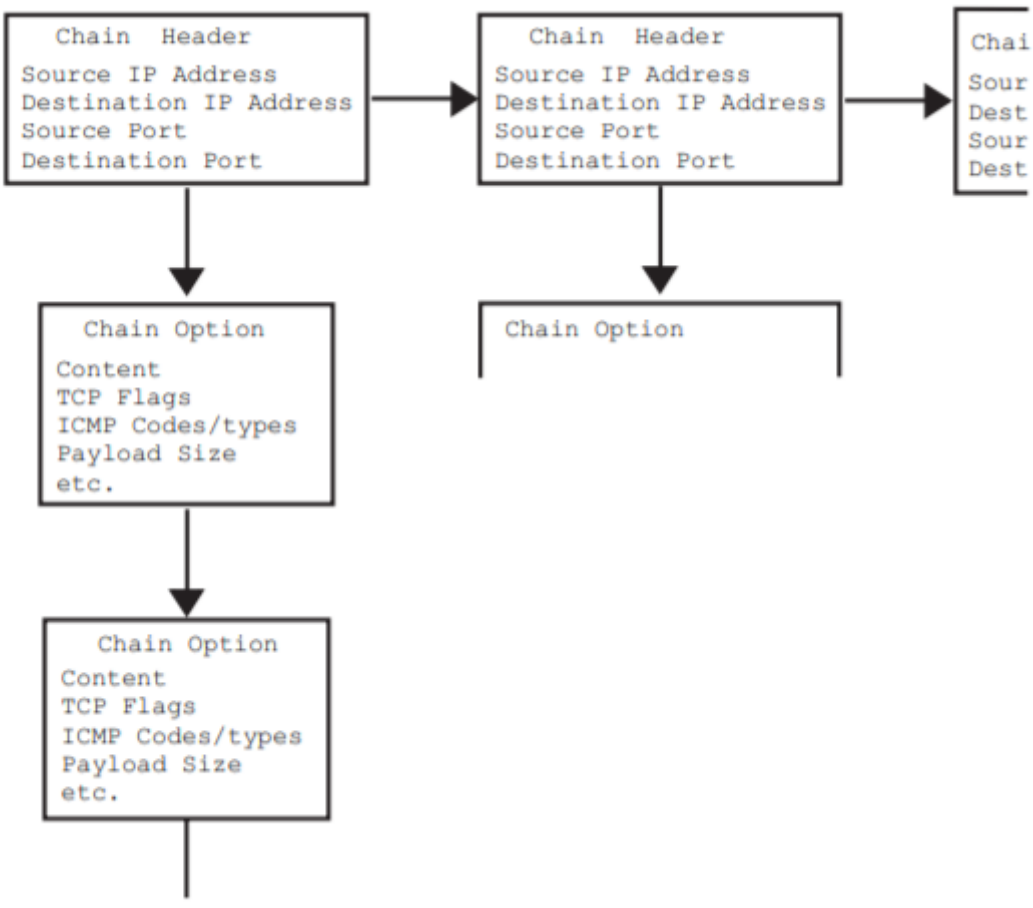
Ο αποκωδικοποιητής πακέτων, είναι οργανωμένος γύρω από τα στρώματα της στοίβας πρωτοκόλλων που υπάρχει στην υποστηριζόμενη σύνδεση δεδομένων και ορισμούς πρωτοκόλλου TCP/IP. Κάθε υπορουτίνα στον αποκωδικοποιητή επιβάλλει την τάξη στα πακέτα δεδομένων επικαλύπτοντας δομές δεδομένων στην πρωτογενή κίνηση του δικτύου. Αυτές οι ρουτίνες αποκωδικοποίησης καλούνται διαδοχικά στην στοίβα πρωτοκόλλων, από το επίπεδο σύνδεσης δεδομένων πάνω από το επίπεδο μεταφοράς (Transport

Layer) και τέλος στο επίπεδο εφαρμογής (Application Layer). Σε αυτό το τμήμα τονίζεται έντονα η ταχύτητα.

4.3.2 Detection Engine

Ο Snort διατηρεί τους κανόνες ανίχνευσης σε δισδιάστατη συνδεδεμένη λίστα των αλυσίδων Chain Headers και Chain Options. Οι συγκεκριμένες λίστες κανόνων έχουν συμπυκνωθεί σε μια λίστα κοινών ιδιοτήτων στις Chain Headers (Αλυσίδα Κεφαλίδων), με την ανίχνευση τροποποιητή που περιέχεται στις Chain Options (Αλυσίδα Επιλογών). Προκειμένου να πραγματοποιηθεί επιτάχυνση της διαδικασίας ανίχνευσης, αυτά τα κοινά στοιχεία συμπυκνώνονται σε ένα μόνο Chain Header και στη συνέχεια, οι ατομικές υπογραφές ανίχνευσης διατηρούνται σε δομές Chain Option.

Αυτές οι αλυσίδες κανόνων αναζητούν αναδρομικά κάθε πακέτο και προς τις δύο κατευθύνσεις. Η μηχανή ανίχνευσης ελέγχει μόνο τις επιλογές αλυσίδας (chain options) που έχουν ρυθμιστεί από τον rule parser κατά το χρόνο εκτέλεσης. Ο πρώτος κανόνας που αντιστοιχεί σε ένα αποκωδικοποιημένο πακέτο στη μηχανή ανίχνευσης ενεργοποιεί τη δράση που καθορίζεται στον ορισμό του κανόνα και επιστρέφει.



Εικόνα 7: Rule Chain Logical Structure [Martin Roesch - 1999]

4.3.3 Logging and Alerting Subsystem

Το υποσύστημα ειδοποίησης και καταγραφής επιλέγεται στο run-time με διακόπτες γραμμής εντολών. Να σημειωθεί πως τον Νοέμβριο του 1999 όταν ο Martin Roesch παρουσίασε τον Snort ανέφερε πως υπάρχουν τρεις επιλογές καταγραφής και πέντε ειδοποίησης. Οι επιλογές καταγραφής μπορούν να οριστούν σε πακέτα καταγραφής, σε μορφή αναγνώσιμη από άνθρωπο, σε μια δομή καταλόγου που βασίζεται σε IP ή σε δυαδική μορφή tcpdump σε ένα αρχείο καταγραφής. Η καταγραφή αποκωδικοποιημένης μορφής επιτρέπει γρήγορη ανάλυση των δεδομένων που συλλέγονται από το σύστημα.

Η μορφή του tcpdump είναι πολύ γρηγορότερη για την εγγραφή στο δίσκο και πρέπει να χρησιμοποιείται σε περιπτώσεις όπου απαιτείται υψηλή απόδοση. Επίσης, η καταγραφή μπορεί μπορεί να απενεργοποιηθεί εντελώς, αφήνοντας τις ειδοποιήσεις ενεργοποιημένες για ακόμη μεγαλύτερες βελτιώσεις απόδοσης.

Οι ειδοποιήσεις έχουν τη δυνατότητα είτε να σταλούν στο syslog είτε να συνδεθούν σε ένα “alert text file” σε δύο διαφορετικές μορφές ή να αποσταλούν ως μηνύματα WinPopUp χρησιμοποιώντας το πρόγραμμα Samba smbclient. Οι ειδοποιήσεις syslog αποστέλλονται ως μηνύματα ασφαλείας/εξουσιοδότησης, τα οποία παρακολουθούνται εύκολα με εργαλεία όπως το swatch. Οι ειδοποιήσεις του WinPopup επιτρέπουν την αποστολή ειδοποιήσεων συμβάντων σε μια λίστα από Microsoft Windows κονσόλες που έχει καθοριστεί από το χρήστη και εκτελούν το λογισμικό WinPopup.

Να σημειωθεί πως υπάρχουν δύο επιλογές για την αποστολή ειδοποιήσεων σε απλό αρχείο κειμένου. Αυτές είναι η πλήρης και η γρήγορη ειδοποίηση. Η πλήρης ειδοποίηση γράφει το μήνυμα προειδοποίησης και τις πληροφορίες κεφαλίδας πακέτων μέσω του πρωτοκόλλου στρώματος μεταφοράς (Transport Layer Protocol). Η επιλογή γρήγορης ειδοποίησης γράφει ένα συμπυκνωμένο υποσύνολο των πληροφοριών κεφαλίδας στο αρχείο ειδοποίησης. Με αυτό τον τρόπο, επιτρέπει μεγαλύτερη απόδοση υπό φορτίο σε σχέση με την πλήρη λειτουργία.

Τέλος, αξίζει να αναφερθεί πως υπάρχει και μια πέμπτη επιλογή με την οποία απενεργοποιείται εντελώς η ειδοποίηση. Η ειδοποίηση αυτή είναι χρήσιμη όταν η προειδοποίηση είναι περιττή ή ακατάλληλη, όπως όταν πραγματοποιούνται δοκιμές διείσδυσης δικτύου.

4.4 Advanced Snorting

Ο Snort αποτελεί ένα ευέλικτο εργαλείο με μεγάλη ποικιλία χρήσεων. Όπως σημείωσε το 1999 και ο Martin Roesch “Ο Snort προορίζεται να αξιοποιηθεί με την πιο κλασική έννοια ενός συστήματος ανίχνευσης εισβολής στο δίκτυο”. Το συγκεκριμένο σύστημα ανίχνευσης εξετάζει την κίνηση του δικτύου σε σχέση

με ένα σύνολο κανόνων και ειδοποιεί τους διαχειριστές σχετικά με την ύποπτη δραστηριότητα δικτύου, ώστε να αντιδράσει κατάλληλα. Αξίζει να σημειωθεί πως υπάρχουν πολλές ακόμη περιοχές στις οποίες ο Snort μπορεί να είναι χρήσιμος.

Παρακάτω, παρουσιάζονται ενδεικτικά μερικές από αυτές.

4.4.1 SHORING UP COMMERCIAL IDSS

Ο Snort μπορεί να αξιοποιηθεί στα εργαλεία ανίχνευσης εισβολής που βασίζονται στο δίκτυο του εμπορικού πωλητή (commercial vendor's network-based intrusion detection tools). Ενδεικτικό παράδειγμα αποτελεί μια νέα επίθεση, η οποία εμφανίστηκε στην κοινότητα των hacker/cracker και οι ενημερώσεις υπογραφών αργούσαν να έρθουν από τον πωλητή (vendor). Στην παρούσα περίπτωση, ο Snort μπορεί να χρησιμοποιηθεί για να χαρακτηρίσει τη νέα επίθεση τρέχοντας τοπικά σε ένα δοκιμαστικό δίκτυο και προσδιορίζοντας την υπογραφή του. Μόλις η υπογραφή γραφεί σε έναν κανόνα ο οποίος περιγράφεται από το Snort, το φιλτράρισμα της γραμμής εντολών BPF μπορεί να χρησιμοποιηθεί για να περιορίσει την κίνηση που αναλύει το Snort στην υπηρεσία ή το πρωτόκολλο ενδιαφέροντος.

Σε αυτό το σημείο θα ήταν σημαντικό να γίνει αναφορά πως ο Snort μπορεί να χρησιμοποιηθεί ως πολύ εξειδικευμένος ανιχνευτής για μια επίθεση (ή μιας οικογένειας επιθέσεων) στον παρόν τρόπο λειτουργίας.

Η επίθεση άρνησης υπηρεσίας IRDP, η οποία πρωτοεμφανίστηκε το 1999, αποκαλύφθηκε από το Lopht, το οποίο αποτελεί ένα καλό παράδειγμα της κατηγορίας των Commercial IDS's. Την ίδια μέρα που ανακοινώθηκε η συγκεκριμένη επίθεση, οι κανόνες Snort διατέθηκαν από την κοινότητα των χρηστών και τέτοιου είδους επιθέσεις ήταν ανιχνεύσιμες.

4.4.2 PASSIVE TRAPS

Μια ακόμη εφαρμογή στην οποία ο Snort αποτελεί το καταλληλότερο σύστημα ανίχνευσης εισβολών, είναι ως Honeypot Monitor. Τα Honeypots είναι προγράμματα ή υπολογιστές, οι οποίοι είναι αφιερωμένοι στην έννοια της εξαπάτησης των εχθρικών ομάδων, οι οποίες στοχεύουν στην υποκλοπή πληροφοριών από ένα δίκτυο. Τα περισσότερα συστήματα Honeypots καταγράφουν τα δεδομένα τους σε επίπεδο διακομιστή με μια μη αληθή υπηρεσία όπως ένας διακομιστής FTP που καταγράφει πραγματικά τα δεδομένα που του αποστέλλονται. Ενδεικτικό παράδειγμα αποτελεί το Fred Cohen & Associates Deception Toolkit.

Το πρόβλημα σε αυτό έγκειται στο γεγονός ότι οι υπηρεσίες που κάνουν την καταγραφή πρέπει να ξεκινήσουν προτού καταγράψουν οτιδήποτε. Αυτό έχει ως αποτέλεσμα τα γεγονότα όπως η σάρωση θύρας μυστικότητας (stealth port scans) ή οι δυαδικές ροές δεδομένων (binary data streams), είτε θα χάνονται,

είτε θα αλλοιώνονται σε honeypots, τα οποία δεν εκτελούν παρακολούθηση επιπέδου πακέτων. Ένα ακόμη πρόβλημα είναι ότι τα δεδομένα που προκύπτουν από ένα τέτοιο σύστημα, θα τείνουν να είναι πολύπλοκα.

Τα δεδομένα που προέρχονται από ένα honeypot απαιτούν από έναν ειδικευμένο αναλυτή να ερμηνεύσει σωστά τα αποτελέσματα. Ο Snort μπορεί να βοηθήσει σημαντικά τον αναλυτή/διαχειριστή με την ταξινόμηση πακέτων και τη λειτουργία αυτόματης ειδοποίησης. Με τις παρούσες δυνατότητες ένα honeypot μπορεί να θεωρηθεί ως ένας ανεξάρτητος μηχανισμός ανίχνευσης εισβολής. Δεν απαιτεί άλλη παρακολούθηση ή συντήρηση, επειδή ο Snort μπορεί να ρυθμιστεί ώστε να καταγράφει και να παράγει ειδοποίηση συμβάντος στο πρώτο πακέτο που φτάνει στο Honeypot.

Ο Snort μπορεί ακόμη να χρησιμοποιηθεί για την εφαρμογή μιας άλλης έννοιας, αυτή των “παθητικών παγίδων”. Μια παθητική παγίδα χρησιμοποιεί το “πλεονέκτημα τοπικού πεδίου”(“home field advantage”) που διαθέτουν οι διαχειριστές δικτύου κατά την διασφάλιση των δικτύων τους. Μια πτυχή της συγκεκριμένης έννοιας είναι ότι οι διαχειριστές γνωρίζουν ποιες υπηρεσίες είναι ή όχι διαθέσιμες στα δίκτυα τους. Κανόνες Snort μπορούν να γραφούν για να παρακολουθείται η κίνηση που κατευθύνεται για αυτές τις ανύπαρκτες υπηρεσίες. Τα πακέτα που διαπιστώνεται ότι χρησιμοποιούν αυτές τις θύρες μπορεί να αποτελούν ένδειξη σάρωσης θυρών (port scanning), οπισθίων σκελών (backdoors), ή κάποιας άλλης εχθρικής κυκλοφορίας. Να σημειωθεί πως υπάρχει η δυνατότητα να εφαρμοστεί είναι για τη ρύθμιση των κανόνων περάσματος για όλες τις υπηρεσίες που είναι γνωστό ότι εκτελούνται σε ένα δίκτυο και την καταγραφή εισερχόμενων συνδέσεων (log inbound connections) σε άλλες θύρες ή port ranges.

4.4.3 FOCUSED MONITORING

“Ελεγχόμενη Παρακολούθηση” (Focused Monitoring) είναι η έννοια της παρακολούθησης ενός μόνο κρίσιμου κόμβου ή υπηρεσίας σε ένα δίκτυο για ενδείξεις εχθρικής δραστηριότητας.

Ενδεικτικό παράδειγμα αποτελεί ο διακομιστής SMTP Sendmail, ο οποίος διαθέτει μια εκτεταμένη και γνωστή λίστα τρωτών σημείων και εκμεταλλεύσεων. Ένας και μόνο αισθητήρας Snort θα μπορούσε να αναπτυχθεί με ένα σύνολο κανόνων που καλύπτει όλες τις γνωστές επιθέσεις SendMail και παρέχει εξαιρετικά εστιασμένη παρακολούθηση αυτής της συγκεκριμένης κίνησης στο δίκτυο. Αυτοί οι κανόνες θα μπορούσαν ακόμη να επεκταθούν ώστε να παρέχουν μια τρέχουσα αφήγηση όλων των εντολών και απαντήσεων μέσα και έξω από τους διακομιστές SMTP στο υπερασπιζόμενο δίκτυο.

Αυτό μπορεί να κάνει λίγο πιο εύκολη την δουλειά των αναλυτών ασφάλειας δικτύων αφήνοντας το Snort να περιγράψει την κανονική ροή εντολών και απαντήσεων καθώς και τις επιθέσεις.

Τέλος, να σημειωθεί πως η "ελεγχόμενη παρακολούθηση" μπορεί να είναι ιδιαίτερα χρήσιμη σε περιπτώσεις όπου τα υπάρχοντα NIDS παρέχουν μη επαρκή κάλυψη.

4.5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Ο Snort σχεδιάστηκε για να ικανοποιεί τις απαιτήσεις ενός πρότυπου ελαφρού (lightweight) συστήματος ανίχνευσης εισβολής στο δίκτυο. Έχει γίνει ένα μικρό, ευέλικτο και εξαιρετικά ικανό σύστημα που χρησιμοποιείται σε όλο τον κόσμο τόσο σε μεγάλα όσο και σε μικρά δίκτυα.

Ο όρος «ελαφρύ» (lightweight) έχει δύο έννοιες. Η μια έννοια σχετίζεται με την εφαρμογή του σε σχετικά μικρά δίκτυα, ενώ η δεύτερη σχετίζεται με το μικρό μέγεθος του και την ευκολία εφαρμογής και χρήσης του.

Γενικότερα, έχει επιτύχει τους αρχικούς σχεδιαστικούς στόχους του και είναι μια πλήρως ικανή εναλλακτική λύση στα συστήματα ανίχνευσης εισβολών σε χώρους όπου είναι αναποτελεσματικό να εγκατασταθούν πλήρως εμπορικά συστήματα.

5 DARKTRACE

Η εταιρεία Darktrace ιδρύθηκε το 2013 από μαθηματικούς του Πανεπιστημίου του Cambridge, καθώς και κυβερνητικούς εμπειρογνώμονες του κυβερνοχώρου τόσο από τις Ηνωμένες Πολιτείες της Αμερικής, όσο και από το Ηνωμένο Βασίλειο. Σήμερα, η Darktrace αναγνωρίζεται ως η κορυφαία εταιρεία τεχνητής νοημοσύνης (Artificial Intelligence – AI) παγκοσμίως για την ασφάλεια στον κυβερνοχώρο.

Το 2016, η ηγετική θέση της Darktrace στην τεχνητή νοημοσύνη ενισχύθηκε με την κυκλοφορία της πρώτης τεχνολογίας αυτόνομης απάντησης, την Darktrace Antigena. Η καινοτομία αυτή, επέτρεψε στο Enterprise Immune System *(Σημείωση: Πρόκειται για μια αυτο-εκμάθητη τεχνολογία τεχνητής νοημοσύνης (self-learning cyber AI technology), η οποία ανιχνεύει νέες επιθέσεις και απειλές εμπιστευτικών πληροφοριών σε πρώιμο στάδιο)* να αντιδράσει σε επιθέσεις στον κυβερνοχώρο σε εξέλιξη με πολύ ακριβή τρόπο, παρέχοντας στις ομάδες ασφαλείας τον χρόνο που χρειάζονται, προκειμένου να αντιδράσουν εγκαίρως. Όταν οι επιθέσεις ransomware της WannaCry το 2017, έπληξαν αρκετούς οργανισμούς, το Darktrace Antigena αντέδρασε εγκαίρως, προστατεύοντας τα δίκτυα πελατών που διαθέτει. [9]

6 DARKTRACE CYBER AI

6.1 ΕΙΣΑΓΩΓΗ

Το Cyber AI της Darktrace, έχει εξελιχθεί με στόχο όχι μόνο να ανιχνεύει, αλλά και για να αντιμετωπίζει έξυπνα τις επιθέσεις, οι οποίες βρίσκονται σε εξέλιξη σε πραγματικό χρόνο. Οι παραδοσιακές προσεγγίσεις έχουν γίνει περισσότερο αυτοματοποιημένες στην αντιμετώπιση περιστατικών – από το IPS της δεκαετίας του 1990 έως τα "next gen" εργαλεία προστασίας από ιούς (antivirus) και τα e-mail gateways της σύγχρονης εποχής. Ουσιαστικά αυτό που απουσιάζει, είναι το πλαίσιο και μια εξελισσόμενη κατανόηση του φυσιολογικού «τρόπου ζωής» για κάθε χρήστη ή/και κάθε συσκευής σε μια επιχείρηση.

Λαμβάνοντας υπόψη αυτή την πλούσια και και εξελισσόμενη κατανόηση του «φυσιολογικού», το Darktrace AI έχει τη δυνατότητα να ανταποκριθεί σε πρώιμους δείκτες της απειλής του κυβερνοχώρου. Αξίζει να σημειωθεί πως αυτό γίνεται με πολύ στοχοθετημένο τρόπο. Το Darktrace Antigena – η αυτόνομη λύση απόκρισης του συστήματος – δρα στο φυσιολογικό «πρότυπο ζωής» για μια συσκευή η οποία είναι παγιδευμένη από κάποιο ιό, εξουδετερώνοντας την απειλή εντός ολίγων δευτερολέπτων, διατηρώντας ωστόσο κανονικά τις λειτουργίες από το σχεδιασμό.

Βάσει του τρόπου λειτουργίας του, το Darktrace Cyber AI, δίνει τον έλεγχο στους «υπερασπιστές» (defenders), πραγματοποιώντας ακόμη και τον πιο πολύπλοκο και ευάλωτο οργανισμό, σε μια ανθεκτική, αυτοδύναμη ψηφιακή επιχείρηση.

6.2 ΕΠΙΘΕΣΕΙΣ

Στη συνέχεια παρατίθενται ενδεικτικά ορισμένες επιθέσεις, οι οποίες παρεμποδίστηκαν και εξουδετερώθηκαν από το Cyber Defence AI. Ανάμεσα σε αυτές είναι οι Insider Threat, Ransomware και επιθέσεις IoT. Βασικό στόχο αποτελεί η κατανόηση της λειτουργίας του Cyber AI της Darktrace.

6.2.1 INSIDER THREAT

Το Insider Threat αντιπροσωπεύει μια από τις πιο κοινές επιθέσεις στις επιχειρήσεις. Αυτού του είδους οι απειλές προέρχονται από δυσαρεστημένους, απρόσεκτους, αλλά ακόμη και συμβιβασμένους υπαλλήλους, οι οποίοι εκμεταλλεύονται την πρόσβαση τους σε εσωτερικά συστήματα. Τα άτομα αυτά, αποτελούν μια ιδιαίτερα σημαντική απειλή για την επιχείρηση, καθώς η προνομιακή τους πρόσβαση και γνώση του δικτύου, τους επιτρέπουν να εκτελέσουν εκτεταμένες αποστολές επίθεσης και να εκμεταλλεύονται κρίσιμα δεδομένα χωρίς να προκαλέσουν καχυποψία.

Πρόσφατα, το Darktrace AI αναγνώρισε και εξουδετέρωσε ένα κακόβουλο insider σε μια μεγάλη επιχείρηση επενδύσεων στη Νότιο Αφρική. Το αυτοδίδακτο AI, εντόπισε μια επίμονη απειλή, καθώς «κινούταν» σε πολλαπλά

στάδια της αλυσίδας επίθεσης από την αναγνώριση σε script writes και script execution. Με την εκμάθηση «στη δουλειά» το Antigena προσαρμόστηκε στην απειλή καθώς εκείνη εξελίχθηκε και περιεχόταν σε κάθε στάδιο.

Το στάδιο της αναγνώρισης πραγματοποιήθηκε με ένα φορητό υπολογιστή – laptop – ο οποίος έκανε "pinging" σε εκατοντάδες εσωτερικές διευθύνσεις IP, με στόχο να εντοπίσει εκείνες που ήταν ενεργές. Στη συνέχεια, πραγματοποιήθηκε σάρωση του δικτύου για τα ονόματα των αποκρινόμενων μηχανών και τα ανίχνευσε, προκειμένου να εντοπίσει ανοικτά κανάλια επικοινωνίας. Το Darktrace AI σηματοδότησε την ύποπτη αυτή συμπεριφορά ως μια ασυνήθιστη δραστηριότητα σάρωσης του δικτύου και ώθησε το Antigena να λάβει δράση. Με βάση τη δυναμική αξιολόγηση μιας απειλής, το Antigena επέβαλε για μια ώρα το «μοντέλο ζωής» της συσκευής, εμποδίζοντας με αυτό τον τρόπο τον φορητό υπολογιστή να αποκλίνει από την προγενέστερη – της επίθεσης – συμπεριφορά του.

Ωστόσο, λίγες ώρες αργότερα η απειλή επανήλθε. Ο φορητός υπολογιστής άρχισε να εκτελεί εντολές σε εκατοντάδες άλλους εσωτερικούς υπολογιστές, στην περιοχή IP που είχε εντοπίσει αρχικά. Αυτό περιλάμβανε και την μετακίνηση αρχείων script πολλαπλών χρήσεων καθώς και τη χρήση του εργαλείου απομακρυσμένης διαχείρισης. Αυτά τα προγράμματα θα μπορούσαν να αξιοποιηθούν για τον εντοπισμό ευαίσθητων πληροφοριών και εγγράφων ή για να ανοίξουν ένα backdoor προκειμένου να επιτεθεί ένας εσωτερικός cracker.

Γενικότερα, δεν παρατηρήθηκαν άλλα παρόμοια file-writes σε όλο το δίκτυο κατά τη διάρκεια εκείνης της χρονικής περιόδου, κάτι το οποίο αποτέλεσε ένα εξαιρετικά ασύνηθιστο γεγονός για το Darktrace AI. Δεδομένης της εξελισσόμενης κατανόησης της απειλής στο πλαίσιο του δικτύου και της προηγούμενης αυτόνομης απάντησης, το Antigena αποφάσισε να αποκλείσει όλες τις εξερχόμενες συνδέσεις χρησιμοποιώντας το κανάλι μεταφοράς αρχείων SMB (SMB file-transfer channel), το οποίο περιέχει άμεσα οποιαδήποτε πλευρική κίνηση στο δίκτυο.

Μόλις εξουδετερώθηκε η απειλή, η ομάδα ασφαλείας κατάφερε να διερευνήσει και να επιβεβαιώσει ότι ο φορητός υπολογιστής ανήκε σε ένα μέλος της ομάδας IT. Ο υπάλληλος αυτός, είχε χρησιμοποιήσει ένα παράνομο εργαλείο σάρωσης, προκειμένου να αναζητήσει αδυναμίες στο δίκτυο. [10]

6.2.2 RANSOMWARE

Το 2019, ένας υπάλληλος σε μια εταιρεία τηλεπικοινωνιών, είχε πρόσβαση στο προσωπικό του email, μέσω εταιρικού smartphone και εξαπατήθηκε προκειμένου να κατεβάσει ένα κακόβουλο αρχείο, το οποίο περιείχε Ransomware. Δευτερόλεπτα αργότερα, η συσκευή άρχισε να συνδέεται με έναν εξωτερικό διακομιστή στο δίκτυο Tor.

Η ανταπόκριση του Darktrace AI ήταν άμεση. Μόλις εννέα δευτερόλεπτα από την έναρξη των δραστηριοτήτων κρυπτογράφησης SMB, η Darktrace έθεσε μια προειδοποίηση, υποδηλώνοντας ότι αυτός ο συγκεκριμένος μη ομαλός τρόπος λειτουργίας απαιτούσε άμεση διερεύνηση. Καθώς η συμπεριφορά εξακολούθησε τα επόμενα δευτερόλεπτα, η Darktrace ενεργοποίησε το Antigena.

Η ανταπόκριση του Antigena ήταν αυτόνομη – καθώς λόγω μη εργάσιμης ημέρας, οι υπάλληλοι απουσίαζαν από το γραφείο – διακόπτοντας όλες τις προσπάθειες για την εγγραφή κρυπτογραφημένων αρχείων σε κοινόχρηστα δίκτυα. Αυτό είχε ως αποτέλεσμα την άμεση εξουδετέρωση της απειλής, προτού αυτή εξαπλωθεί στην εκτεταμένη υποδομή του τηλεπικοινωνιακού δικτύου, δίνοντας με αυτό τον τρόπο στην ομάδα ασφαλείας τον κατάλληλο χρόνο να δράσει.

Καθώς τα αυτοματοποιημένα στελέχη του Ransomware συνεχίζουν να εμφανίζονται στο Dark Web και σε εταιρικά δίκτυα σε όλο τον κόσμο, οι εταιρείες θα χρειαστεί να αντιμετωπίσουν την τεχνητή νοημοσύνη, προκειμένου να καταφέρουν να διατηρήσουν το ρυθμό τους. Όπως και σε άλλα είδη επιθέσεων, έτσι κι εδώ, η απόκριση του Darktrace Cyber AI αποτελεί ένα κρίσιμο συστατικό στις επιθέσεις ταχείας επέμβασης, προτού να έχουν χρόνο να κρυπτογραφήσουν κρίσιμα δεδομένα και να παρεμποδίσουν την ομαλή λειτουργία της εταιρείας. [10]

6.2.3 Email Attacks

Στην προηγούμενη υποενότητα, πραγματοποιήθηκε μια αναφορά στο Ransomware, το οποίο σχετιζόταν με μια επίθεση που πραγματοποιήθηκε στο email του εργαζόμενου. Ωστόσο, πέρα από το Ransomware, επιθέσεις που σχετίζονται άμεσα με το e-mail, αποτελούν το Spear Phishing και το E-mail Account Hijacking. Ειδικά στην τελευταία περίπτωση, ο επιτιθέμενος εκμεταλλεύεται μια αξιόπιστη σχέση μεταξύ αποστολέα και παραλήπτη.

7.2.3.1 Spear Phishing

Τα Phising e-mails ξεκινούν στο πλαίσιο αδιάκριτων εκστρατειών «μετάδοσης». Το παράδειγμα που περιγράφεται στη συνέχεια, έδειχνε να αποτελεί μια συντονισμένη και εξελιγμένη επίθεση στον κυβερνοχώρο. Κάθε μήνυμα ηλεκτρονικού ταχυδρομείου ήταν καλά επεξεργασμένο και προσαρμοσμένο στον παραλήπτη. Ο επιτιθέμενος είχε επίσης πάρει το βιβλίο διευθύνσεων της πόλης, καθώς η επίθεση παραδόθηκε στους παραλήπτες αλφαβητικά, από Α ως Ζ. Ωστόσο, ενώ κάθε μήνυμα ηλεκτρονικού ταχυδρομείου εμφανίστηκε αβλαβές και προσαρμόστηκε στον παραλήπτη, όλα τα μηνύματα περιείχαν ένα κακόβουλο φορτίο που κρύβονταν πίσω από ένα κουμπί το οποίο παρουσιαζόταν ως σύνδεσμος με το Netflix, το Amazon και άλλες αξιόπιστες υπηρεσίες. Το Darktrace AI κατάφερε να αναλύσει αυτές τις κρυφές συνδέσεις σε σχέση με τα φυσιολογικά «πρότυπα ζωής» των

προορισμένων παραληπτών στο δίκτυο. Όταν ήρθε η πρώτη διεύθυνση email, το Antigena αναγνώρισε αμέσως ότι ούτε ο παραλήπτης ούτε κάποιος από τους υπόλοιπους πολίτες είχε επισκεφτεί αυτό το domain πριν. Το Antigena έθεσε αμέσως μια ειδοποίηση υψηλής εμπιστοσύνης και πρότεινε να κλειδώσει αυτόνομα κάθε σύνδεσμο καθώς εκείνος εισερχόταν στο δίκτυο. [10]

6.2.3.2 HIJACKING E-MAIL ACCOUNT

Με το e-mail account hijacking ενός αξιόπιστου συνεργάτη ή πωλητή κατά μήκος της αλυσίδας εφοδιασμού (Supply Chain) ο επιτιθέμενος μπορεί να εξαπατήσει τους παραλήπτες, προκειμένου να επισκεφθούν έναν κακόβουλο σύνδεσμο ή να μεταφέρουν εκατομμύρια από την επιχείρηση.

Το Darktrace AI εντόπισε μια επίθεση αυτού του είδους, με στόχο μια εταιρεία παραγωγής ταινιών στο Λος Άντζελες της Αμερικής, αφού οι λεπτομέρειες του λογαριασμού μιας επαφής σε έναν έμπιστο προμηθευτή είχαν παραβιαστεί.

Οι λεπτομέρειες του λογαριασμού μπορούν να αξιοποιηθούν για πολλούς ειδεχθής σκοπούς. Παρόλα αυτά, στην προαναφερθήσα περίπτωση, ο επιτιθέμενος είχε ως στόχο να διαβάσει την αλληλογραφία της επαφής με έναν υπάλληλο του στούντιο. Αφού εξέτασε τα προηγούμενα θέματα και μάθαινε πώς επικοινωνεί συνήθως η επαφή και ο υπάλληλος, έστειλε μια εύλογη απάντηση στο τελευταίο μήνυμα ηλεκτρονικού ταχυδρομείου του υπαλλήλου.

Το μήνυμα ηλεκτρονικού ταχυδρομείου ήταν πειστικό, καθώς αντικατόπριζε το ύφος και των τόνο γραφής της επαφής και είχε νόημα στο πλαίσιο της σχέσης και των προηγούμενων συζητήσεων. Αξίζει να σημειωθεί πως το μήνυμα περιλάμβανε έναν κακόβουλο σύνδεσμο που θα φαινόταν αβλαβής για κάθε λογικό υπάλληλο που το έλαβε από μια γνωστή επαφή σε μια γνωστή επιχείρηση. Αυτοί οι τύποι επιθέσεων είναι ολοένα και συχνότεροι και είναι πολύ δύσκολο να εντοπιστούν.

Το Darktrace Cyber AI διακρίνει τους αδύναμους δείκτες που αποκάλυψαν ότι αυτή η «έμπιστη επαφή» ήταν ένας λογαριασμός ο οποίος ελεγχόταν πλήρως από έναν εισβολέα/επιτιθέμενο. Η ανταπόκριση του AI πυροδότησε το δίκτυο με τη γνώση ότι το ηλεκτρονικό ταχυδρομείο και το περιεχόμενό του ήταν έξω από το «πρότυπο ζωής» του υποτιθέμενου αποστολέα. Ο υπάλληλος ειδοποιήθηκε και το κακόβουλο ωφέλιμο φορτίο εξουδετερώθηκε.

Η απόφαση του Antigena πάρθηκε από το γεγονός ότι αυτός ο συγκεκριμένος σύνδεσμος ήταν σπάνιος τόσο για τον αποστολέα όσο και για τον παραλήπτη δεδομένης της προηγούμενης επικοινωνίας του και των συνήθων «μορφών ζωής» του εργαζόμενου στο δίκτυο. [10]

6.3 DARKTRACE ΚΑΙ CLOUD

Η ταχεία υιοθέτηση υπηρεσιών Cloud και SaaS έχουν εξελίξει το Digital Business και έχουν αναμορφώσει θεμελιωδώς την πρόκληση της υπεράσπισης της επιχείρησης από προηγμένες επιθέσεις. Η μετάβαση στο Cloud αποτελεί πλέον έναν απαραίτητο αγωγό για έργα ψηφιακού μετασχηματισμού – από την εφαρμογή προηγμένων αναλυτικών στοιχείων σε μεγάλα σύνολα δεδομένων έως την υποστήριξη υπολογιστών και συσκευών, τα οποία αποτελούν τη βάση για τις «έξυπνες πόλεις» έως τα συνδεδεμένα αυτοκίνητα.

Αξίζει να αναφερθεί πως οι προκλήσεις ασφαλείας που παρουσιάζει το Cloud, διέπονται σε μεγάλο βαθμό από ένα μοντέλο κοινής ευθύνης, το οποίο περιγράφει τους αντίστοιχους τομείς του Cloud που αναμένεται να διαχειρίζονται και να διασφαλίζουν οι πάροχοι και οι πελάτες.

Σε αυτό το σημείο αξίζει να σημειωθεί πως οι λύσεις κατασκευαστών όπως οι Cloud Access Security Brokers (CASBs) και Cloud Workload Protection Platforms (CWPPs), μπορούν να είναι χρήσιμες για τα Cross-Cloud. Ωστόσο, δυσκολεύονται να ανιχνεύσουν λεπτές απειλές και ανώμαλες συμπεριφορές, οι οποίες δεν έχουν προηγουμένως εντοπιστεί. Καθώς οι απειλές εξελίσσονται, απαιτείται μια νέα, ριζική προσέγγιση για την διασφάλιση του περιβάλλοντος του Cloud από τις προηγμένες επιθέσεις, προτού αυτές έχουν χρόνο να εξελιχθούν σε κρίση. Επίσης, υπάρχουν και ορισμένα σενάρια τα οποία χρειάζεται να ληφθούν υπόψη για το Cloud Security. Πιο συγκεκριμένα:

- Επαναδημιουργία (recreate) ενός στιγμιότυπου, παρακάμπτοντας το IT και την ασφάλεια.
- Τα δεδομένα παραγωγής μεταφέρονται σε λιγότερο ασφαλή συστήματα δοκιμών.
- Πλευρική κυκλοφορία μέσα στο Cloud.
- Οι χρήστες του Office 365 και του Salesforce μετακινούν δεδομένα εκτός του Cloud.
- Συσκευές Edge, οι οποίες χρησιμοποιούν το Cloud ως αγωγό.
- Ασυνήθιστες, λεπτές αλλαγές στη συμπεριφορά των χρηστών.
- Επιθέσεις που κινούνται με μηχανική ταχύτητα που απαιτούν άμεση δράση.
- Συσχέτιση και ανάλυση συμφραζομένων για την ανίχνευση ανωμαλιών.
- Εξουδετέρωση κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου. στο Office 365, ειδικά από αξιόπιστους αποστολείς κατά μήκος της αλυσίδας εφοδιασμού (Supply Chain).

Προωθούμενη από τους μηχανισμούς μηχανικής μάθησης και τους αλγορίθμους τεχνητής νοημοσύνης, οι τεχνολογίες Cyber AI της Darktrace εκτείνουν την προστασία τους. Με τη χρήση λογισμικού και αισθητήρων, το Darktrace Cloud καλύπτει όλες τις περιπτώσεις χρήσης που αναφέρονται

παραπάνω αναλύοντας την πλούσια ροή κίνησης και δεδομένων σε περιβάλλοντα Cloud και SaaS.

Όπως αναφέρθηκε και στην προηγούμενη υποενότητα, το Darktrace AI μαθαίνει το «φυσιολογικό σχέδιο ζωής» του κάθε χρήστη, της κάθε συσκευής, χωρίς να βασίζεται σε προηγούμενες παραδοχές ή τη χειροκίνητη εισαγωγή (manual input). Αυτή η εξελισσόμενη κατανόηση του «φυσιολογικού» επιτρέπει στην πλατφόρμα να ανιχνεύει αυτόματα και να ανταποκρίνεται σε εξωτερικές επιθέσεις και εσωτερικές απειλές σε πραγματικό χρόνο, παρέχοντας παράλληλα πλήρη προβολή σε όλο το Digital Business (ψηφιακή επιχείρηση).

6.3.1 Απειλες Στο Cloud

Στην προηγούμενη υποενότητα έγινε αναφορά στο Insider Threat. Σε αυτό το σημείο αξίζει να αναφέρουμε πως αυτό το είδος απειλής, έχει λάβει μια νέα διάσταση και κινείται ευέλικτα μέσα στο πλαίσιο του Cloud. Εκτός από αυτό από το Insider Threat, με το οποίο έρχονται αντιμέτωπες οι εταιρείες στο Cloud, υπάρχουν και ορισμένα άλλα είδη απειλών.

Οι λανθασμένες ρυθμίσεις (misconfigurations) σε περιβάλλον IaaS αποτελούν ένα είδος αυτών των απειλών. Σύμφωνα με τους Crowd Research Partners (*Σημείωση: Πρόκειται για μια εταιρεία η οποία ειδικεύεται στο marketing περιεχομένου με βάση την έρευνα και την ζήτηση. Γενικά, πραγματοποιούν προσαρμοσμένο marketing κατ'απαίτηση προκειμένου να ανταποκρίνεται στις μοναδικές ανάγκες marketing των πωλητών-εταιρειών ασφάλειας στον κυβερνοχώρο. Τέτοιου είδους εταιρείες αποτελούν η Cisco, η IBM και πολλές ακόμη άλλες.*) ότι οι λανθασμένες ρυθμίσεις των πλατφορμών Cloud (Misconfiguration of Cloud Platforms) αποτελούν τη μεγαλύτερη απειλή στο Cloud Security. Ενώ το ανθρώπινο σφάλμα ορισμένες φορές δεν είναι εύκολο να αποφευχθεί, οι λανθασμένες ρυθμίσεις αποτελούν συχνά μια φυσική συνέπεια του deployment, καθώς και της ταχείας εμφάνισης συνόλων δοκιμών, οι οποίες διευκολύνονται από το Cloud. Το γεγονός αυτό, οδηγεί αρκετές φορές τους χρήστες να κινούνται σε βάρος της ασφάλειας.

Επιπροσθέτως, τα μη ασφαλισμένα APIs καθίστανται ως ένα από τα πιο αντίξοα misconfigurations στο Cloud. Αξίζει να γίνει αναφορά πως το 2017 συμπεριλήφθησαν στα Κορυφαία 10 OWASP Application Security Risks. Το API μιας εφαρμογής είναι συνδεδεμένο με δεδομένα back-end, συνεπώς κάθε ευπάθεια στο χειρισμό της απόκρισης σφάλματος, αποτελεί στόχο για τους επιτιθέμενους, οι οποίοι διαθέτουν μια σειρά κινήτρων.

Το Edge Computing αναπτύχθηκε τα τελευταία χρόνια, με τη ραγδαία ανάπτυξη του Cloud. Αποτελεί ένα από τα πιο αξιοσημείωτα off-shoots, ακόμη κι αν αντιπροσωπεύει μια ριζική μετατόπιση από την επεξεργασία δεδομένων σε κεντρικούς κόμβους (central nodes). Να σημειωθεί πως φέρνει τη λογική

των υπολογιστών πλεισιέστερα στις φυσικές πηγές δεδομένων, με στόχο να μειώσει την καθυστέρηση και να αυξήσει το εύρος ζώνης.

6.3.2 DARKTRACE CLOUD

Η τεχνολογία του Cyber AI της Darktrace, έχει φέρει μια διαφορετική προσέγγιση στην ασφάλεια και υπεράσπιση του κυβερνοχώρου σε πραγματικό χρόνο (real-time) στο Cloud. Το Darktrace Cloud βασίζεται στη μηχανική μάθηση, χωρίς έλεγχο, καθώς και στην τεχνητή νοημοσύνη. Έχει τη δυνατότητα να αναλύει τις ροές δεδομένων εντός των εφαρμογών του Cloud και των εφαρμογών SaaS, μαθαίνοντας ένα «φυσιολογικό μοντέλο ζωής» για κάθε χρήστη και κάθε συσκευή. Το Darktrace Cloud συνδυάζει τις λεπτές αποκλίσεις στην συμπεριφορά σε πραγματικό χρόνο και έχει τη δυνατότητα να εντοπίσει και να σταματήσει το πλήρες φάσμα κυβερνο-απειλών στο Cloud από κακόβουλα μέσα και εξωτερικές επιθέσεις, έως κρίσιμες παρανοήσεις, οι οποίες μπορούν να οδηγήσουν την επιχείρηση σε σημείο το οποίο να επιφέρει μεγάλη επίπτωση στην ψηφιακή της περιουσία.

Το Darktrace Cloud, αντί να βασίζεται σε προκαθορισμένους κανόνες και πολιτικές, προσπαθεί να αντιμετωπίσει την αβεβαιότητα που είναι εγγενής στο σύνθετο ψηφιακό περιβάλλον. Όλες οι σημαντικές αποκλίσεις παρατηρούνται και συσχετίζονται με αποτέλεσμα την ανίχνευση πραγματικών απειλών, χωρίς να δημιουργούνται πλημμύρες false-positives.

Όπως έχει προαναφερθεί, το Darktrace Antigena, η αυτόνομη ικανότητα απόκρισης της πλατφόρμας, χρησιμοποιεί τεχνητή νοημοσύνη για τη λήψη στοχοθετημένων, μετρημένων ενεργειών ως απάντηση σε απειλές στον κυβερνοχώρο. Με αυτό τον τρόπο, παρεμποδίζεται η εξάπλωση τους σε πραγματικό χρόνο και δίνεται στην ομάδα ασφαλείας έγκυρος χρόνος προκειμένου να δράσει.

Τέλος, αξίζει να τονιστεί πως οι τύποι ενεργειών του Darktrace Antigena μπορούν να διαφέρουν ανάλογα με το συγκεκριμένο περιβάλλον Cloud ή την εφαρμογή SaaS που χρησιμοποιείται.

6.4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Όλο και περισσότεροι οργανισμοί/εταιρείες με το πέρασμα του χρόνου, βασίζονται στις Cloud υπηρεσίες και στις εφαρμογές SaaS με στόχο τον εξορθολογισμό των επιχηρηματικών πρακτικών, το οικείο πρότυπο της περιμέτρου του δικτύου. Τα πλεονεκτήματα του Cloud Computing θα διασφαλίσουν ότι οι μετακινήσεις θα συνεχίσουν με αυξημένη ταχύτητα. Ωστόσο, οι μοναδικές προκλήσεις ασφαλείας που θα παρουσιαστούν από το Cloud θα απαιτήσουν πιο ευέλικτη νοοτροπία, καθώς και τεχνολογίες αυτοδιδασκαλίας. Οι τεχνολογίες αυτές δύνανται να κινούνται με την ταχύτητα των cloud deployments και να εντοπίζουν μικρές αποκλίσεις μιας

απειλής παρέχοντας παράλληλα πλήρη προβολή σε πραγματικό χρόνο σε ολόκληρη την ψηφιακή επιχείρηση.

Η θέση που κατέχει η Darktrace στον τομέα της τεχνητής νοημοσύνης για την ασφάλεια στον κυβερνοχώρο καθιστά μια αποτελεσματική λύση για την ανίχνευση πρωτοφανών απειλών και ανώμαλων περιστατικών στο cloud. Η πλατφόρμα AI της Darktrace βοηθάει στην εξάλειψη τυφλών σημείων και στην προστασία των προσωπικών δεδομένων.

7 ΑΛΓΟΡΙΘΜΟΣ PCA – PRINCIPAL COMPONENT ANALYSIS

7.1 ΕΙΣΑΓΩΓΗ

Σε προβλήματα ανίχνευσης επιθέσεων, τα δεδομένα βρίσκονται σε μεγάλες διαστάσεις. Προκειμένου να πραγματοποιηθεί εύκολα ανάλυση των δεδομένων, κρίνεται αναγκαίο να ελλατωθεί η διαστασιολόγηση τους (dimensionality of the data). Για αυτό το σκοπό χρησιμοποιείται ο PCA, ο οποίος αποτελεί μια κυρίαρχη τεχνική μείωσης διαστάσεων. Να σημειωθεί πως ο PCA εφαρμόζεται ευρέως σε σύνολα δεδομένων σε πολλούς διαφορετικούς επιστημονικούς τομείς.

Το βασικό πρόβλημα του PCA είναι να βρει τις σωστές κατευθύνσεις (principal directions). Για online computing ο συντελεστής συνάρτησης/συσχετισμού δεν είναι δυνατό να υπολογιστεί σε πολλές εφαρμογές. Για εφαρμογές με μεγάλα data sets, δεν είναι επίσης πρακτικό να υπολογιστούν οι ιδιοτιμές και των αντίστοιχων ιδιοκυμάτων απευθείας. Να σημειωθεί πως υπάρχει τεράστια ποικιλία προσαρμοστικών αλγορίθμων, οι οποίοι έχουν διαφορετικές υπολογιστικές απαιτήσεις και ακρίβεια για την ενημέρωση της επέκτασης του PCA.

7.2 ΕΦΑΡΜΟΓΗ PCA

Με βάση την ανάλυση βασικών συστατικών στοιχείων (principal component analysis – PCA) παρακάτω παρουσιάζεται μια ολοκληρωμένη και αποτελεσματική προσέγγιση ανίχνευσης περιστατικών, που χρησιμοποιεί πιθανοτικές μεθόδους δικτύου και επεξεργασίας, για την εκμετάλλευση χωρικών και χρονικών συσχετισμών και εξαρτήσεων στα δίκτυα των οχημάτων και κατ’ επέκταση για την επίτευξη αξιόπιστης εικόνας του πλαισίου οδήγησης.

Η προσέγγιση που ακολουθεί – η οποία βασίζεται σε μια έρευνα που πραγματοποίηθηκε το 2007[4] – παρέχει ένα ολοκληρωμένο τρόπο αποτελεσματικής επεξεργασίας και οργάνωσης συσσωρευμένων χωροχρονικών πληροφοριών από διάφορες τοποθεσίες, οχήματα και πηγές και ενσωματώνονται σε ένα συνολικό αποτέλεσμα.

Ενώ τα σημερινά car-use systems (συστήματα χρήσης αυτοκινήτων) είναι σε θέση να αντιληφθούν το περιβάλλον τους, τα συστήματα αυτά δεν ανταλλάσουν ενεργά πληροφορίες μεταξύ οχημάτων και μεταξύ οχημάτων και οδικού δικτύου. Παρόλα αυτά, επιτρέποντας την επικοινωνία μεταξύ των οχημάτων με το οδικό δίκτυο, δίνεται στα συστήματα των οχημάτων και στους οδηγούς μια καλύτερη επίγνωση του περιβάλλοντος τους, έτσι ώστε να έχουν τη δυνατότητα να μπορούν να αποφύγουν επικίνδυνες και δυσάρεστες καταστάσεις.

Αξίζει να αναφερθεί, πως τα δίκτυα οχημάτων, αποτελούν σημαντικό συστατικό των προβλεπόμενων ευφυών συστημάτων μεταφορών (intelligent

transportation systems - ITSs). Τα δίκτυα αυτά μπορούν να συμβάλλουν σε πιο ασφαλείς και αποτελεσματικούς δρόμους, παρέχοντας έγκαιρες πληροφορίες στους οδηγούς και τις ενδιαφερόμενες αρχές. Αυτό επιτυγχάνεται με την παροχή της δυνατότητας επικοινωνίας μεταξύ των οχημάτων, μέσω της επικοινωνίας όχημα με όχημα (V2V) και με τους σταθμούς βάσης στην οδό μέσω της οδικής επικοινωνίας (R2V). Για ευφυείς μεταφορικούς σκοπούς, μπορεί να χρησιμοποιηθούν ολοκληρωμένες και περιεκτικές παρατηρήσεις σχετικά με τις μεταφορές και τις ταχύτητες του οχήματος, για την εκτίμηση διαφόρων παραμέτρων, όπως πιθανές καθυστερήσεις και αναμενόμενος χρόνος άφιξης σε βασικά σημεία.

Για την επίτευξη των προαναφερθέντων στόχων, έγινε χρήση PCA. Η Principal Component Analysis (PCA) έχει αποδειχθεί ότι παρέχει αποτελεσματικούς τρόπους για την μοντελοποίηση των συσχετισμών χωροχρονικών δεδομένων και οι βασικές αρχές της έχουν χρησιμοποιηθεί σε αρκετούς τομείς, όπως η ανίχνευση εισβολής σε δίκτυο υπολογιστών και η ανίχνευση ανωμαλιών στην κυκλοφορία δικτύου υπολογιστών (network traffic anomaly detection).

Όσον αφορά την αρχιτεκτονική του παραπάνω συστήματος, σκοπός της PCA είναι να μειώσει την διαστατικότητα ενός συνόλου δεδομένων το οποίο στο οποίο υπάρχει ένας μεγάλος αριθμός αλληλένδετων μεταβλητών διατηρώντας όσο το δυνατόν περισσότερο τη διακύμανση που υπάρχει στα δεδομένα. Τα εξαγόμενα μη συσχετιζόμενα συστατικά, ονομάζονται κύρια συστατικά (principal components - PCs) και υπολογίζονται από τους ιδιοδιανύτες του πίνακα διακύμανσης των αρχικών μεταβλητών.

Μια μελλοντική σκέψη αποτελούν κινούμενα οχήματα εξοπλισμένα με συσκευές επικοινωνίας τα οποία στοιχειοθετούν ένα μεγάλο mobile ad hoc network. Σε αυτά τα δίκτυα - αποκαλούμενα ως ad hoc networks - οι πληροφορίες σχετικά με την τοποθεσία και την διαδρομή έχουν αναγνωριστεί ως crucial components. Τα συγκεκριμένα components εξαλείφουν ορισμένους από τους περιορισμούς υφιστάμενων πρωτοκόλλων που βασίζονται στην τοπολογία. Έτσι, επιτρέπεται ο σχεδιασμός έγκαιρων αντιδράσεων σε ένα διαγνωσμένο πρόβλημα ή περιστατικό. Η βασική λειτουργία βασίζεται μόνο στα δεδομένα που συλλέγονται από τους σταθερούς αισθητήρες και αναφέρεται ως Intelligent Incident Detection (IID). Η δεύτερη λειτουργία αυξάνεται με πρόσθετες μετρήσεις ή/και πληροφορίες που λαμβάνονται από τα οχήματα και του ενσύρματου δικτύου - αναφέρεται ως vehicle assisted IID (VIID) - και επιτρέπει την συλλογή εξειδικευμένων μετρήσεων ανά όχημα όπως για παράδειγμα ο χρόνος της διαδρομής του οχήματος στο οδικό δίκτυο, η κατάσταση του οχήματος και πληροφορίες σχετικά με τη διαδρομή του.

7.3 ΣΥΜΠΕΡΑΣΜΑΤΑ

Με την πρόσφατη ανάπτυξη των ασύρματων δικτύων επικοινωνιών και των Ad Hoc Networks, οι επικοινωνίες V2V και R2V έχουν τη δυνατότητα να

συμβάλλουν σε πιο αποτελεσματικούς και ασφαλείς δρόμους, παρέχοντας έγκαιρη πληροφόρηση τόσο στους οδηγούς, όσο και στις αρχές.

Η προσέγγιση που προτάθηκε στο άρθρο[4] χρησιμοποιεί και εφαρμόζει ταυτόχρονα PCA σε πολλαπλές μετρήσεις που λαμβάνονται από διάφορους αισθητήρες. Η προσέγγιση του PCA έχει επιλεγεί ως ένας αποτελεσματικός τρόπος μείωσης των διαστάσεων του συνόλου δεδομένων στο οποίο υπάρχει ένας μεγάλος αριθμός αλληλοσυνδεόμενων μεταβλητών, διατηρώντας όσο δυνατόν περισσότερο, τη διακύμανση που υπάρχει στο σύνολο δεδομένων.

Σύμφωνα με την έρευνα αυτή [4], τα αποτελέσματα επίδοσης που προέκυψαν από την παραπάνω μεθοδολογία που καταγράφηκε είναι τα ακόλουθα: Επιτυγχάνεται υψηλό ποσοστό ανίχνευσης για διάφορα σενάρια συμβάντων και διαφορετικούς λόγους ανωμαλιών (anomaly ratios). Ως εκ τούτου επιτρέπεται η ανάπτυξη αποτελεσματικών συστημάτων μεταφοράς, οι οποίοι μπορούν να αντιμετωπίσουν διαφορετικά επίπεδα αβεβαιότητας. Μεταξύ άλλων, μπορούν ακόμη να ερμηνεύσουν με ορθότητα τα δεδομένα, να αντλήσουν τα κατάλληλα συμπεράσματα και να παρέχουν στον οδηγό τις σωστές πληροφορίες με έγκυρο, έγκαιρο και ουσιαστικό τρόπο.

8 Ερευνητικο Υποβαθρο

Στις υποενότητες που ακολουθούν, παρουσιάζεται μια έρευνα προκειμένου να άγει το συμπέρασμα ποιο από τα συστήματα ανίχνευσης επιθέσεων που παρουσιάστηκαν παραπάνω, διαθέτει την καλύτερη απόδοση.

Προκειμένου να θεωρηθεί ένα intrusion detection system ως το πιο αποδοτικό θα πρέπει να ληφθούν υπόψη οι εξής δύο παράμετροι. Οι επιθέσεις – και πιο συγκεκριμένα, το πλήθος των επιθέσεων – τις οποίες μπορεί να αντιμετωπίσει και ο χρόνος τον οποίο χρειάζεται προκειμένου να εντοπίσει μια επίθεση η οποία βρίσκεται σε εξέλιξη.

8.1 Επιθεσεις

Στην παρούσα υποενότητα, θα πραγματοποιηθεί μια σύγκριση μεταξύ των συστημάτων ανίχνευσης εισβολών, τα οποία μελετήθηκαν παραπάνω, ως προς το επίπεδο των επιθέσεων. Βασικός στόχος αυτής της σύγκρισης είναι να εξαχθεί ένα συμπέρασμα ως προς το πιο από τα προαναφερόμενα IDSs – Snort και Darktrace Cyber AI – δύναται να αντιμετωπίσει τις περισσότερες εισβολές επιτυχώς.

Στον πίνακα που ακολουθεί (Πίνακας 1) φαίνονται τα συστήματα ανίχνευσης και στην πρώτη στήλη καταγράφονται ορισμένα είδη επιθέσεων. Πιο συγκεκριμένα, γίνεται αναφορά ποιο σύστημα ανίχνευσης εισβολών, εντοπίζει την εκάστοτε επίθεση.

	Snort	Darktrace Cyber AI
Real-time Traffic Analysis Attacks	✓	✓
Packet logging on IP Networks Attacks	✓	✓
E-mail Attacks	✓	✓
Insider Threat	✗	✓
CGI Attacks	✓	✗
SQL Injection Attack	✓	✗
Integrity Attacks	✗	✗
Cloud Attacks	✗	✓

Πίνακας 1: Είδη επιθέσεων στα IDSs

Παρατηρώτας τον παραπάνω πίνακα, υπάρχουν κάποια σημεία για τα οποία αξίζει να παραγματοποιηθεί μια περαιτέρω ανάλυση. Πιο συγκεκριμένα:

Real – time Traffic Analysis Attacks: Το συγκεκριμένο είδος επίθεσης, μπορεί να αντιμετωπιστεί με επιτυχία από τον Snort και το Darktrace AI.

Packet Logging on IP Networks Attacks: Αυτό το είδος επίθεσης το αντιμετωπίζουν με επιτυχία ο Snort και το Cyber AI της Darktrace. Να σημειωθεί πως ο Snort έχει την δυνατότητα να αντιμετωπίσει επιθέσεις μόνο σε IP δίκτυα.

E-mail Attacks: Πρόκειται για ένα γενικό τίτλο επιθέσεων ο οποίος έχει ως στόχο να συμπεριλάβει όλα τα είδη επιθέσεων που σχετίζονται με e-mail που έχουν σταλεί στους παραλήπτες και είναι παγιδευμένα με διάφορους τρόπους. Αξίζει να σημειωθεί πως ο Snort από το 1999 που εμφανίστηκε για πρώτη φορά, έχει τη δυνατότητα να αντιμετωπίζει επιθέσεις SendMail. Από την άλλη πλευρά, το Darktrace Cyber AI, έχει τη δυνατότητα να εντοπίζει και πιο σύνθετες επιθέσεις που σχετίζονται με «παγιδευμένα» e-mail. Πιο συγκεκριμένα, τέτοια είδη επιθέσεων αποτελούν το Ransomware, Spear Phishing, Hijacking E-mail Account. Οι επιθέσεις αυτές περιγράφησαν αναλυτικά στα προηγούμενα κεφάλαια.

Insider Threat: Όπως έχει προαναφερθεί, το παρόν είδος επίθεσης σχετίζεται με απειλές που προέρχονται από τους ίδιους τους εργαζομένους μιας επιχείρησης, είτε ηθελημένα, είτε άθελα τους. Το συγεκριμένο είδος επίθεσης, αντιμετωπίζεται επιτυχώς από το Darktrace AI.

CGI Attacks: Το CGI – γνωστό και ως Common Gateway Interface – έχει την δυνατότητα να βοηθά ένα διακομιστή ιστού να αποδώσει δυναμικές ιστοσελίδες (dynamic web pages). Προκειμένου να δημιουργήσει μια απάντηση για ένα αίτημα που λήφθηκε από τον πελάτη/χρήστη το πρόγραμμα CGI καλεί άλλες εφαρμογές στον διακομιστή για να δημιουργήσει μια συγκεκριμένη απάντηση. Κατά την ολοκλήρωση των απαιτούμενων λειτουργιών, το πρόγραμμα CGI επιστρέφει την έξοδο στον διακομιστή ιστού ο οποίος στη συνέχεια στέλνει μια απάντηση στον πελάτη/χρήστη. Αυτού του είδους οι επιθέσεις αντιμετωπίζονται με επιτυχία από τον Snort.

SQL Injection Attacks: Αποτελούν ένα γενικευμένο τίτλο για επιθέσεις που σχετίζονται με εισαγωγή SQL scripts σε μια βάση δεδομένων, με στόχο να υποκλαπούν χρήσιμες πληροφορίες ή ακόμη και να πραγματοποιηθούν αλλαγές στη βάση. Σε αυτή την κατηγορία επιθέσεων ανήκουν και οι ODBC SQL Attacks, οι οποίες αντιμετωπίζονται με επιτυχία από τον Advanced Snort.

Integrity Attacks: Το παρόν, σχετίζεται με επιθέσεις που αφορούν την ακεραιότητα των δεδομένων, όταν αυτά μεταφέρονται από ένα σημείο Α, σε ένα σημείο Β, μέσα στο δίκτυο. Αυτού του είδους οι επιθέσεις αντιμετωπίζονται με επιτυχία από τον αλγόριθμο PCA.

Cloud Attacks: Όπως περιγράφηκε και στο προηγούμενο κεφάλαιο, οι συγκεκριμένες επιθέσεις απασχολούν το Cloud, το οποίο εξελίσσεται ραγδαία τα τελευταία χρόνια. Συνεπώς, το Darktrace Cloud το οποίο βασίζεται σε ένα

συνδυασμό μηχανικής μάθησης και τεχνητής νοημοσύνης, έχει την δυνατότητα να μαθαίνει ένα «φυσιολογικό μοντέλο ζωής» για κάθε χρήστη και κάθε συσκευή. Με αυτό τον τρόπο, έχει τη δυνατότητα να εντοπίσει και να σταματήσει το πλήρες φάσμα κυβερνο-απειλών στο Cloud από κακόβουλα μέσα και εξωτερικές επιθέσεις.

8.2 ΧΡΟΝΟΣ

Στην παρούσα υποενότητα, παρουσιάζεται ο χρόνος τον οποίο χρειάζονται ο Snort και το Darktrace AI, προκειμένου να αντιμετωπίσουν μια εισβολή.

Είναι σημαντικό να αναφερθεί η αναγκαιότητα που υπάρχει για συνεχή ανάπτυξη των συστημάτων ανίχνευσης εισβολών. Στο Snort, τα μεγαλύτερα σύνολα κανόνων (set of rules) απαιτούν περισσότερους χρονικούς περιορισμούς όσον αφορά τη διαχείρηση πακέτων (packet handling) και την αντιστοίχηση διατάξεων (pattern matching). Η μη επιτυχημένη αντιμετώπιση τους δύναται να επιφέρει επιδείνωση της απόδοσης και απώλεια πακέτων (packet loss). Βάση μιας έρευνας που πραγματοποιήθηκε το 2007 [13], για ένα συγκεκριμένο εύρος ζώνης, ο αριθμός των πακέτων που παράγονται είναι μεγαλύτερος σε περίπτωση φορτίων με μικρότερο ωφέλιμο φορτίο IP (smaller IP payload), από την περίπτωση όπου το ωφέλιμο φορτίο είναι μεγάλο. Όταν παράγονται μεγάλοι αριθμοί πακέτων, τότε καθίσταται δύσκολο να διαβαστούν όλοι από το NIC και επομένως υπάρχει απώλεια πακέτων. Προκειμένου να αντισταθμιστεί αυτό και να επέλθει γρηγορότερη επεξεργασία πακέτων, οι αριθμοί των κανόνων είναι αναγκαίο να μειωθούν δραστικά, στην περίπτωση όπου τα μεγέθη πακέτων είναι μικρά. Ο κύκλος της διαδικασίας που λαμβάνει ο Snort ξεκινά με τη λήψη αρχείων κανόνων (rule files), την κατασκευή του state machine και ολοκληρώνεται με την έρευνα pattern matches μέσω input strings. Σε αυτό το σημείο είναι σημαντικό να τονιστεί πως το βασικότερο στοιχείο του Snort, αποτελεί ο αλγόριθμος αντιστοίχησης διατάξεων (Pattern Matching Algorithm). Το 70%-80% του χρόνου του Snort, δαπανάται στην ανίχνευση διατάξεων (pattern detection).

Ένα αρνητικό χαρακτηριστικό του Snort, αποτελούν οι false-positives συναγερμοί που ενεργοποιεί. Είναι σημαντικό οι πολιτικές (policies) του Snort να εφαρμόζουν στις τυπικές δραστηριότητες του δικτύου και να περιοριστεί η εμφάνιση false-positive περιστατικών. Η συγκεκριμένη λαναθασμένη ενεργοποίηση του συστήματος ανίχνευσης, επηρρεάζει σε ένα βαθμό – με αρνητικό αντίκτυπο – την επίδοση του συστήματος.

Από την άλλη πλευρά, υπάρχει και το Darktrace Cyber AI. Από άποψη απόδοσης, το AI είναι πιο αποτελεσματικό και δρα έγκαιρα προκειμένου να εντοπίσει και στη συνέχεια να μετριάσει μια απειλή. Πιο συγκεκριμένα, στην επίθεση Ransomware, η οποία περιγράφηκε σε προηγούμενο κεφάλαιο, το AI λειτούργησε ως εξής: Εντόπισε την ασυνήθιστη δραστηριότητα η οποία προκλήθηκε στο δίκτυο και την μετρίασε. Λόγω του γεγονότος ότι, το AI βασίζεται στο self-learnig (αυτο-εκμάθηση) των «συνήθων μορφών ζωής» του

συστήματος, όταν συμβαίνει κάποια ασυνήθιστη δραστηριότητα, το AI την εντοπίζει. Ωστόσο, επειδή ασυνήθιστες δραστηριότητες – ασυνήθιστες για τα δεδομένα του AI – συμβαίνουν συχνά, στην επίθεση Ransomware, το AI, επέλεξε περιμένει λίγο, προκειμένου να βεβαιωθεί προτού αντιδράσει. Τη χρονική στιγμή όπου η ασυνήθιστη δραστηριότητα ήταν 73%, το Darktrace Cyber AI, επενέβει και αντιμετώπισε την απειλή. Ο χρόνος που χρειάστηκε το AI προκειμένου να μετριάσει την απειλή, ανέρχεται στα 6 δευτερόλεπτα.

Ένα άλλο είδος επίθεσης το οποίο παρατηρείται αρκετά συχνά, είναι το Insider Threat. Σύμφωνα με πληροφορίες από την ίδια την εταιρεία Darktrace, το Cyber AI έχει την δυνατότητα να εντοπίζει 7 τέτοιου είδους απειλές το λεπτό. Είναι σημαντικό επίσης να τονιστεί πως το Cyber AI της Darktrace έχει τη δυνατότητα εκτός από τον εντοπισμό των απειλών, την αποτροπή τους. Μαζί με το Snort μπορούν εκτός από Intrusion Detection Systems, να θεωρηθούν και Intrusion Prevention Systems.

9 ΣΥΜΠΕΡΑΣΜΑΤΑ

9.1ΠΕΡΙΛΗΨΗ

Στα προηγούμενα κεφάλαια περιγράφηκε ο τρόπος λειτουργίας του Snort, του Darktrace Cyber AI, καθώς και του αλγορίθμου PCA. Με περισσότερες λεπτομέρειες παρουσιάστηκε ο τρόπος λειτουργίας του AI, μέσω της περιγραφής ορισμένων επιθέσεων, τις οποίες καταφέρνει να εντοπίσει και να μετριάσει με επιτυχία. Στη συνέχεια, πραγματοποιήθηκε μια σύγκριση μεταξύ των δύο συστημάτων ανίχνευσης εισβολών – Snort και Cyber AI – προκειμένου να βρεθεί πιο από αυτά διαθέτει την καλύτερη απόδοση. Ο αλγόριθμος PCA, εξαιρέθηκε από την σύγκριση αυτή. Ωστόσο ήταν σημαντικό να πραγματοποιηθεί μια αναφορά για αυτόν στην εργασία, καθώς πρόκειται για έναν αλγόριθμο ο οποίος δύναται να ανιχνεύσει επιθέσεις που βρίσκονται σε εξέλιξη.

Προκειμένου να αποδοθεί ένα συμπέρασμα, σε πρώτο στάδιο πραγματοποιήθηκε μια καταφραφή συγκεκριμένων επιθέσεων, με στόχο τον εντοπισμό του συστήματος που δύναται να τις ανιχνεύσει. Σε επόμενο στάδιο, πραγματοποιήθηκε μια σύγκριση ως προς τον χρόνο τον οποίο χρειάζονται τόσο ο Snort, όσο και το Cyber AI της Darktrace προκειμένου να αντιμετωπίσουν μια εισβολή.

Παρακάτω, παρουσιάζονται τα συμπεράσματα που άγονται από αυτή την έρευνα.

9.2 ΣΥΜΠΕΡΑΣΜΑ

Προκειμένου να θεωρηθεί ένα σύστημα ανίχνευσης εισβολών αποδοτικό υπάρχουν δύο σημαντικοί παράγοντες οι οποίοι οφείλουν να ληφθούν υπόψη. Αυτοί είναι, το πλήθος των επιθέσεων τις οποίες καταφέρνει να εντοπίσει και ο χρόνος τον οποίο χρειάζεται προκειμένου να επιτευχθεί αυτό.

Όπως προαναφέρθηκε, σε πρώτο στάδιο πραγματοποιήθηκε μια καταγραφή συγκεκριμένων επιθέσεων, με στόχο τον εντοπισμό του συστήματος που δύναται να τις ανιχνεύσει. Από αυτή την καταγραφή, εξήχθει το συμπέρασμα ότι ο Snort και το Cyber AI, καταφέρνουν να ανιχνεύσουν τις ίδιες επιθέσεις με ορισμένες εξαιρέσεις. Ένα παράδειγμα εξαίρεσης αποτελούν τα SQL Injections, τα οποία ο Snort καταφέρνει να ανιχνεύσει με επιτυχία, σε αντίθεση με το AI.

Στη συνέχεια, πραγματοποιήθηκε μια καταγραφή του χρόνου, που απαιτείται από το εκάστοτε σύστημα, προκειμένου να ανιχνεύσει επιτυχώς μια επίθεση σε εξέλιξη.

Σαν τελικό συμπέρασμα σημειώνεται ότι ο αλγόριθμος Snort είναι ιδιαίτερα χρήσιμος και διευκολύνει σημαντικά στον εντοπισμό επιθέσεων που σχετίζονταν με buffer overflows, SQL Injections, καθώς και πολλές άλλες που

σημειώθηκαν καθόλη τη διάρκεια της εργασίας. Ωστόσο, ένα αρνητικό χαρακτηριστικό του Snort, αποτελούν οι false-positives συναγερμοί που ενεργοποιεί. Είναι απαραίτητο οι πολιτικές (policies) του Snort να εφαρμόζουν στις τυπικές δραστηριότητες του δικτύου προκειμένου να περιοριστεί η εμφάνιση false-positive περιστατικών. Η λαναθασμένη ενεργοποίηση του συστήματος ανίχνευσης, επηρρεάζει σε μεγάλο βαθμό – με αρνητικό αντίκτυπο – την επίδοση του συστήματος.

Από την άλλη πλευρά, το Cyber AI της Darktrace διαθέτει, αρκετά καλή απόδοση. Αυτό οφείλεται κυρίως στο γεγονός ότι είναι το μόνο από τα συστήματα που περιγράφησαν, το οποίο εντοπίζει επιτυχώς επιθέσεις που πραγματοποιούνται σε επίπεδο Cloud. Λόγω του γεγονότος ότι η πελιοψηφία των υπολογιστικών πόρων είναι διαθέσιμοι μέσω διαδικτύου – και κατ'επέκταση τα κεντρικά συστήματα βρίσκονται απομακρυσμένα από τον τελικό χρήστη – το καθιστά κατάλληλο για την αντιμετώπιση επιθέσεων που συμβαίνουν στο Cloud. Επίσης, είναι σημαντικό να τονιστεί πως το AI, χρησιμοποιεί τεχνητή νοημοσύνη, με στόχο το self-learning και καταφέρνει να εξελίσσεται και να προσαρμόζεται κάθε φορά στα καινούργια δεδομένα του συστήματος.

Τέλος, επειδή το Darktrace AI αποτελεί ένα Intrusion Detection System εμπορικής χρήσης (commercial use) – σε αντίθεση με τον Snort που είναι Open Source – το πλήθος των πληροφοριών είναι περιορισμένο.

Λαμβάνοντας υπόψη τα δεδομένα που επικρατούν στη σημερινή εποχή και τον σημαντικό ρόλο του Cloud, το Cyber AI της Darktrace είναι το καταλληλότερο προς χρήση σύστημα ανίχνευσης εισβολών, καθώς είναι πιο αποδοτικό. Ωστόσο, για άλλου τύπου χρήσεις όπως είναι η ανίχνευση επιθέσεων SQL Injections ή επιθέσεων CGI, ο Snort κρίνεται αποδοτικότερος και πιο κατάλληλος, προκειμένου να τις ανιχνεύσει.

10 Πηγες Και Βιβλιογραφια

[1] Wenke Lee, Salvatore J. Stolfo (1998) “Data Mining Approaches for Intrusion Detection”. United States.

[2] Kajal Rai, M. Shyamala Devi (2013) “Intrusion Detection Systems: A Review”. India

[3] Pritika Mehra (2012) “A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems”. India

[4] Vasilis Chatzigiannakis, Maria Grammatikou, Symeon Papavasiliou (2007) “Extending Driver’s Horizon Through Comprehensive Incident Detection in Vehicular Networks”. Greece

[5] Mohamed Faisal Elrawy, T.K. Abdelhamid, A.M. Mohamed (2013) “IDS in Telecommunication Network using PCA”. Egypt

[6] Bing Zhang, Zhiyang Liu, Yanguo Jia, Jiadong Ren, Xiaolin Zhao “Network Intrusion Detection Method Based on PCA and Bayes Algorithm”. China

[7] Travis Earl Russel, Peter Joseph Marsico (2006) “Methods and Systems for Detecting and Mitigating Intrusion Events in a Communications Network”. United States

[8] Martin Roesch (1999) “Snort – Lightweight Intrusion Detection for Networks”. United States

[9] Darktrace Company Overview (www.darktrace.com)

[10] Darktrace white paper (2019) “Autonomous Response: Threat Report 2019”

[11] Darktrace white paper (2019) “Cyber AI & Darktrace Cloud”

[12] ACE Team (www.loginsoft.com) (2018) “Introduction to common gateway interface and CGI vulnerabilities”

[13] Soumya Sen (2007) “Performance Characterization & Improvement of Snort as an IDS”.

[14] Darktrace Video regarding time needed to detect an Insider Threat and Ransomware attack (www.darktrace.com)

[15] TCP/IP Layers Image extracted from https://jamieoo.com/archives/7

[16] IP Spoofing Image extracted from www.cloudflare.com

[17] SYN-Floods Attack Image extracted from www.cloudflare.com

[18] Man-in-the-middle Attack Image extracted from www.imperva.com