Evaluation of a Graphical Attack Fingerprint Model and Comparison against the Snort IDS

By

Behnaz Saropourian

A Report Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Engineering

In the department of Electrical and Computer Engineering

University of Victoria

Supervisory Committee

Evaluation and Comparison of a Graphical Attack Fingerprint Model against the Snort IDS

By

Behnaz Saropourian
University of Victoria 2022

Supervisory Committee

Dr. Amirali Baniasadi
Department of Electrical and Computer Engineering

Dr. Issa Traoré
Department of Electrical and Computer Engineering

Table of Contents

List of Figures

List of Tables

Acronyms

AEN: Activity and Event network graph

AV: Anti-virus

DDoS: Distributed Denial of Service

DoS: Denial-of-service attack

DR: Detection Rate

FP: False Positive

FPR: False Positive Rate

FN: False Negative

FTP: File Transfer Protocol

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

IDS: Intrusion detection system

IP: Internet Protocol

ISOT: Information Security and Object Technology Research lab, at the University of Victoria

NIDS: Network Intrusion Detection Systems

PCAP: Packet Capture

PGQL: Property Graph Query Language

SSH: Secure Shell Protocol

TP: True Positive

TN: True Negative

TCP Transmission Control protocol

UDP: User Datagram Protocol

Acknowledgements

I would like to thank my supervisor, Dr. Amirali Baniasadi for his support and motivation throughout my progress.

I would like to thank Dr. Issa Traore for giving me the chance to be a part of this project and for his constant guidance, support, and motivation for my project and throughout my progress.

I would like also to thank Dr. Paulo Quinan, for his support and assistance throughout this project.

Dedication

Dedicated to my husband and parents, for all their support, motivation and encouragement.

Abstract

Today, the number of targeted attacks has increased extremely. The attacks have increased in sophistication and diversity. It is imperative to deploy effective and proactive countermeasures that can help mitigate the threats to organizations and citizens.

The Activity and Event Network (AEN) is a new knowledge graph that uses graph database technology to model security relevant network data items and their relationships as they change through time and apply various threat detection techniques.

The purpose of the project is to evaluate the performance of one of the AEN threat detection techniques based on graph-based attack fingerprints or signatures, and conduct a comparison with the Snort IDS, which is a popular signature-based IDS. The evaluation was conducted using the CICIDS2017 public dataset, and discussions of the strengths and limitations of the fingerprint model were conducted, paving the way for future improvements.

CHAPTER 1: INTRODUCTION

1.1 Context

Network security monitoring is one of several commonly used methodologies in information security operation centers. The network traffic and logs are monitored to detect any illegal activities within the network [1].

Intrusion detection is the prompt and automated detection of numerous threats that have the potential to damage an information system. Intrusion detection systems (IDS) can be classified into three types: host-based, network-based, or a hybrid of the two. IDS can also be categorized into signature-based detection and anomaly-based detection models.

An IDS that monitors both network traffic and device activity for suspicious or malicious activities is known as a host-based IDS. On local endpoints, such as computers, they are installed.

An IDS that only monitors network traffic is referred to as a network-based IDS. IDSs that are based on networks, however, simply watch network traffic. They will scan data packets and look for any signals of malicious or suspicious activities.

Signature-based IDS requires access to a current database of attack signatures, in signature-based detectors whenever an attack or malicious activity is detected, that traffic pattern is saved and programmed as a signature and used to detect future malicious traffic. While signature-based detection is good at detecting known attack patterns, it cannot detect new attack types before corresponding signatures are added to the detector's database. Anomaly-based IDSs, on the other hand, detect deviations from normal traffic or system behavior and report such deviations as potentially malicious. Unlike, signature-based detection, anomaly detection is more effective in detecting novel attack patterns. An IDS tool with an anomaly-based approach uses baselines rather than signatures. It will look for anomalous behavior that differs from historical statistical averages or previously observed activity. It is no wonder that anomaly-based intrusion detection is a productive field of study, as different machine learning approaches can generally be successfully applied to anomaly detection.

1.2 Project Objective

The Activity and Event Network (AEN) is a new security knowledge graph model developed at the Information Security and Object Technology (ISOT) Lab [4], which captures and analyzes various network security data items that occur at the network operation systems and data centers. The purpose of the AEN model is to provide a modelling and analytical framework to identify the attack patterns, particularly those related to long-term threats. The AEN graph is constructed by collecting data from various sources in the network and private or public repositories to identify common and new types of network cyber-attacks. It relies on a dynamic and probabilistic graphical model to model the entire monitored network and the relationships between the various network entities over time. This model serves as the basis for applying pattern matching, spatial and temporal graph analysis to reveal hidden relationships. Network traces, security events (e.g., from IDS, IPS, firewalls, AV), network events (e.g., from switch, router, or server data), or application logs are examples of data sources [1].

The AEN framework provides different algorithms for threat detection, which can work independently or in tandem. Some of the algorithms focus on detecting novel threat patterns, for instance, through unsupervised anomaly detection, while others focus essentially on known threat detection. One of the algorithms in the latter category uses graphical fingerprints as signatures for known and common threats. The purpose of the current project is to study the performance of the AEN graph fingerprint model compared with Snort, which is a popular signature-based IDS. The performance evaluation was conducted using the University of New Brunswick (UNB) CICIDS2017 dataset. Standard metrics, such as detection rate and false-positive rate are computed and compared during the performance evaluation. This obtained in the original evaluation of the fingerprint detection, which was conducted using the ISOT cloud IDS evaluation dataset.

1.3 Report Outline

The remaining chapters of this report are organized as follows. Chapter 2 provides background knowledge about the Snort IDS, the AEN graph model and the structure of the AEN fingerprints. Chapter 3 describes the experimental work by giving an overview of the dataset, presenting and discussing the performance results. Finally, chapter 4 makes concluding, remarks and discusses future work.

CHAPTER 2: BACKGROUND

2.1 AEN Graph Model and Fingerprints

The Information Security and Object Technology (ISOT) Lab developed the AEN Graph, a new security knowledge graph model which uses inputs from a variety of security-relevant data sources, such as network traffic, system logs, IDSs, Antiviruses, and firewalls, to identify various cyber-attacks and suspicious patterns of behavior [5]. The AEN graph is based on a multigraph model in which nodes are labeled, and they can have multiple relationships implying that they can have multiple edges. Relationships have their own set of properties that consist of a source and a destination.

Different threat detection models currently implemented in the graph engine can be applied to the graph model to identify various threats. One of these models is a graphical signature model which encodes and stores in a knowledge various attack patterns also referred to as attack fingerprints.

The AEN attack fingerprint package's structure is made up of two parts: a unique attack pattern component and a fingerprint implementation component. Attack strategies from different attack families are currently implemented in the graph engine. Distinct attack strategies were considered in each family as a proof of concept; these can simply be expanded by adding more attack methods. The following three families are taken into consideration: Password guessing, scanning, and denial of service.

The AEN graph is built on Oracle's PGX [6] engine, which is a graph database. The AEN attack fingerprints are implemented using Oracle's Property Graph Query Language (PGQL) [7], a query language that uses SQL-like syntax to query results based on a graph pattern. PGQL queries ar executed with Java APIs using the oracle.pgx.api java packages to query an in-memory snapshot that has been loaded into the in-memory analyzer on PGX [10].

PGQL provides a mechanism for retrieving results from the graph via queries. PQGL syntax is similar to SQL in most contexts. Figure 2.1 is an example of a PGQL query.

```
54                  OffsetDateTime time = TimeService.getInstance().getTestTime();
55
56                  return "SELECT s, d, count(e)" +
57                          " MATCH (s:" + hostLabel + ")-[e:" + sessionLabel + "]->(d:" + hostLabel
+ ")" +
```

Figure 2.1. Sample PGQL query

2.2 Snort IDS

SNORT is an open-source network intrusion detection system (IDS) which provides real-time network traffic analysis and data packet logging, in addition to its core intrusion detection functionality. It is a rule-based system that detects possibly malicious activities by relying on a set of predefined rules, which represent signatures of known attacks. The SNORT rules are defined using a simple, flexible rule definition language. Although the rules are simple to write, they are powerful enough to detect a wide range of suspicious traffic. Each rule has a fixed header and one or more options. SNORT can run in three different modes: IDS mode, logging mode, and sniffer mode.

In the packet sniffer mode of SNORT, IP packets are read and then displayed to the user on the console.

SNORT will log each IP packet that connects to the network while in packet logger mode.

Only malicious packets will be logged by SNORT in NIDS mode. It achieves this via rules that determine the default features of malicious packets.

2.2.1 SNORT Features

SNORT has several features that help network administrators to monitor the system and detect malicious activity [8]. The following features are explained in four categories as below.

A. Real-time traffic monitoring

Monitoring traffic in and out of the network. It monitors traffic in real time and alerts users when it detects potentially malicious packets or threats on Internet Protocol (IP) networks.

B. Packet Logging

SNORT enables packet logging via packet logging mode. This means that the packet will be recorded on disk. In this mode, SNORT collects each packet and records it in a hierarchical directory based on the IP address of the host network.

C. Log Analysis

SNORT supports log analysis. This is a network sniffing process that collects data in the log layer for additional analysis. This allows network administrators to further investigate potentially malicious data packets. This is important, for example, in the TCP/IP protocol specifications.

D. Content Matching

SNORT parses the rules according to protocols such as IP and TCP, then ports, and then with and without content. Rules containing content use multi-pattern matching. This improves performance, especially for protocols such as HTTP. Rules without content are always evaluated, which has a negative impact on performance.

2.2.2 SNORT Rules

Basically, SNORT can run in three different modes: IDS mode, logging mode, and sniffer mode. This project used SNORT in the IDS mode. Instead of a community ruleset, a ruleset based on a new update to the references SNORT data ruleset was added. All-new rules have been added to the community rules and combination of both rule sets generated the snort detection. The SNORT rules format is shown in Table 2.1.

Rule Header + (Rule Options)
Action - Protocol - Source/Destination IP's - Source/Destination Ports - Direction of the flow
Alert Example: alert udp !10.1.1.0/24 any -> 10.2.0.0/24 any
Actions: alert, log, pass, activate, dynamic, drop, reject, sdrop
Protocols: TCP, UDP, ICMP, IP

Table.2.1. SNORT rules format and components

CHAPTER 3: EXPERIMENTAL EVALUATION

In this project, we conducted an experimental evaluation of the AEN graph fingerprint model using a public dataset and compared with the results obtained for snort on the same dataset. In this section, we present the dataset and the performance results obtained for AEN fingerprints and snort.

3.1. Dataset

To conduct the experiments, we used the CICIDS2017 dataset. The CICIDS dataset is provided by the Canadian Institute for Cybersecurity (CIC), a training and research institute at the University of New Brunswick (UNB), known for its excellence in cybersecurity research [2],[3]. It contains both the original package files in pcap format and the generated netflow files in CSV format. The NetFlow data consists of timestamps, source and destination IPs, source and destination ports, protocol, and flows flagged based on the attack.

The dataset includes a comprehensive set of attack scenarios including Brute Force SSH, DoS, Heart Bleed Exploit, Web Attacks, Botnets and DDoS. It covers an extended timeframe: over a total period of 5 days, starting at 9am to 5pm on Monday, July 3, 2017, and ending on Friday, July 7, 2017 [9]. The attack scenarios for each day are as follows:

1- Monday is Normal Activity: All benign
2- Tuesday is Normal Activity + attack: FTP-Patator + SSH-Patator
3- Wednesday is Normal Activity + attack: DDoS slowloris, Slowhttptest, Hulk, GoldenEye
4- Thursday is Normal Activity + attack: Infiltration + Web Attack
5- Friday is Normal Activity + attack: Port Scanning + DDoS (LOIT)

The dataset contains attack information in the form of traffic data for 5 days, as shown in Table 3.2.

Name of Files	Day Activity	Attacks
Monday-WorkingHours.pcap_ISCX.csv	Monday	Benign (Normal human activities)
Tuesday-WorkingHours.pcap_ISCX.csv	Tuesday	Benign, FTP-Patator, SSH-Patator
Wednesday-workingHours.pcap_ISCX.csv	Wednesday	Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed
Thursday-WorkingHours-Morning-WebAttacks.pcap_ ISCX.csv	Thursday	Benign, Web Attack – Brute Force, Web Attack – SQL Injection, Web Attack – XSS
Thursday-WorkingHours-Afternoon-Infilteration.pcap_ ISCX.csv	Thursday	Benign, Infiltration DropBox Download, Cool disk – MAC
Friday-WorkingHours-Morning.pcap_ISCX.csv	Friday	Benign, Bot
Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv	Friday	Benign, PortScan
Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv	Friday	Benign, DDoS

Table.3.2. CICIDS2017 dataset breakdown

The entire dataset contains 3,119,345 instances (or records) and 83 features with 15 different labels (1 benign + 14 attack labels). The dataset has 288,602 instances missing class labels, and 203 instances missing information, according to the instances in the joined file. By removing such missing instances, the CICIDS 2017 totals 2,830,540 instances. Tables 3.3 and 3.4 break down the dataset characteristics and statistics.

Dataset Name	CICIDS2017
Dataset Type	Multi class
Year of release	2017
Total number of distinct instances	2830540
Number of features	83
Number of distinct labels	15

Table.3.3. Summary information of CICIDS2017 Dataset

Class Labels	Number of instances
BENIGN	2359087
DoS Hulk	231072
PortScan	158930
DDoS	41835
DoS GoldenEye	10293
FTP-Patator	7938
SSH-Patator	5897
DoS slowloris	5796
DoS Slowhttptest	5499
Bot	1966
Web Attack – Brute Force	1507
Web Attack – XSS	652
Infiltration	36
Web Attack – Sql Injection	21
Heartbleed	11

Table.3.4. Class wise instance occurrence of CICIDS2017 dataset

3.2 Intrusion Detection Performance Metric

The effectiveness of the intrusion detection models considered in the project is measured by comparing their ability to distinguish malicious and non-malicious records. This involves computing metrics such as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). When an IDS generates an alert despite a lack of malicious activity, this is called a false positive [8] on the other hands, Security alerts called as "False Positives" indicate there is a threat when there isn't. A false negative occurs when the intrusion detection system fails to generate an alert while there is an intrusion, or when the security system fails to detect a real threat, it produces a false negative. The correct detection of malicious activity is a true positive. When no alert is generated for legitimate activities, this is considered a true negative.

In practice, two performance metrics are used to evaluate the detection effectiveness for an IDS, namely detection rate (DR) and false positive rate (FPR).

DR is the ratio of the number of attacks detected by the system to the number of attacks actually executed [11]:

$$\text{DR}= \frac{\text{Number of attack instances detected}}{\text{Total number of attack instances}} = \frac{TP}{TP+FN}$$

The FPR is the ratio of false positives (FP) to the sum of FP and true negatives (TN). This metric is calculated with the following formula in the below.

$$\text{FPR}= \frac{\text{Number of normal instances detected as alerts}}{\text{Total number of normal instances}} = \frac{FP}{TN+FP}$$

Accuracy (AC) is calculated as follows:

$$\text{Accuracy}= \frac{TN+TP}{TP+TN+FN+FP}$$

3.3 Experiments Procedure and Results

3.3.1 Evaluation Based on Snort

In this project, we ran Snort's community ruleset to detect attacks from the dataset. Moreover, some customized rules to add functionality and improve attack coverage were added to the snort rule sets.

The results for different days are shown in Figures 1 to 5. Each record in the alert file that snorts output contains the timestamp (ts), the identifier of the source port (srcport), destination port (dstport), protocol (proto), destination IP (dst), messages (msg), and the source IP address (p).
Tables 3.5 to 3.8 show the alert file in the CICIDS2017 dataset's csv file for each day which contains information about source and destination IP address, and attacks of each day except Monday where all detection attacks were Benign.

TEU - attack label	Source IP	Destination IP
Benign	172.16.0.1	192.168.10.50
FTP patator	172.16.0.1	192.168.10.50
SSh patator		

Table.3.5. Malicious IPs involved in attacks on Tuesday

WED - attack label	Source IP	Destination IP
Benign	172.16.0.1	192.168.10.50
DOS golden	172.16.0.1	192.168.10.50
DOS hulk	172.16.0.1	192.168.10.50
DOS slow	172.16.0.1	192.168.10.50
DOS slosloris	172.16.0.1	192.168.10.51
Heartbleed	192.168.10.51	
	192.168.10.51	

Table.3.6. Malicious IPs involved tin attacks on Wednesday

THUR - attack label	Source IP	Destination IP
Infiltration	192.168.10.8	205.174.165.73
Benign	172.16.0.1	192.168.10.50
Web attack brute force	172.16.0.1	192.168.10.50
Web attack sql	172.16.0.1	192.168.10.50
Web attack xss	205.174.165.73	
	192.168.10.50	

Table.3.7. Malicious IPs involved in attacks on Thursday

FRI - attack label	Source IP	Destination IP
Dos	172.16.0.1	192.168.10.50
Benign	192.168.10.50	172.16.0.1
Portscan	192.168.10.12	52.6.13.28
Benign	192.168.10.14	205.174.165.73
Bot	192.168.10.15	205.174.165.73
	192.168.10.17	52.7.235.158
	192.168.10.5	205.174.165.73
	192.168.10.8	205.174.165.73
	192.168.10.9	205.174.165.73
	205.174.165.73	192.168.10.9
	205.174.165.73	192.168.10.14
		192.168.10.15
		192.168.10.5
		192.168.10.8

Table.3.8. Malicious IPs involved in attacks on Friday

The snort detection results on the CICIDS2017 dataset from Monday to Friday are shown in figures 3.2 to 3.6.

Monday:

timestamps	sig_ge	sig_id	sig_rev	msg	proto	src	srcpo	dst	dstport	ethsrc	ethdst	ethlen	tcpflag	tcpseq	tcpack	tcpln	tcpwin	ttl	tos	id	dgmle	iplen	icmp	icmpcc	icmp	icmps
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.1		192.168.10.3		00:C1:I	18:66:[	0x46						255	192	53628	56	57344	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.1		192.168.10.3		00:C1:I	18:66:[	0x46						255	192	53629	56	57344	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.9		192.168.10.3		B8:AC:	18:66:[	0xA7						128	0	110	153	2E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.9		192.168.10.3		B8:AC:	18:66:[	0xA7						128	0	110	153	2E+05	3	3	0	0
2017/07/03-07	1	538	15	NETBIOS SMB IPC$	TCP	192.168.10.9	1063	192.168.10.3	139	B8:AC:	18:66:[	0x80	***AP	0xF6D/	0x35BF85A1	0xFD		128	0	309	114	1E+05				
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49031	106	1E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49031	106	1E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49066	106	1E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49066	106	1E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49328	106	1E+05	3	3	0	0
2017/07/03-07	1	402	16	PROTOCOL-ICMP de	ICMP	192.168.10.12		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	49328	106	1E+05	3	3	0	0
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	6605	18:66:[	B8:AC:	0x91						128	0	32332	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	6605	18:66:[	B8:AC:	0x91						128	0	32332	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	37867	18:66:[	B8:AC:	0x91						128	0	32336	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	37867	18:66:[	B8:AC:	0x91						128	0	32336	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	14742	18:66:[	B8:AC:	0x91						128	0	32342	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	14742	18:66:[	B8:AC:	0x91						128	0	32342	131	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	18450	18:66:[	B8:AC:	0x7A						128	0	32395	108	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.12	18450	18:66:[	B8:AC:	0x7A						128	0	32395	108	1E+05				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.17	54458	18:66:[	00:23:/	0x6C						128	0	7437	94	96256				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.17	54458	18:66:[	00:23:/	0x6C						128	0	7437	94	96256				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.17	4615	18:66:[	00:23:/	0x6C						128	0	7440	94	96256				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.17	4615	18:66:[	00:23:/	0x6C						128	0	7440	94	96256				
2017/07/03-07	1	254	16	PROTOCOL-DNS SP	UDP	192.168.10.3	53	192.168.10.17	11115	18:66:[	00:23:/	0x91						128	0	7534	131	1E+05				

Figure.3.2. Snort detection Alerts of Monday

Tuesday:

timest	sig_ge	sig_id	sig_rev	msg	proto	src	srcport	dst	dstpor	ethsrc	ethdst	ethlen	tcpflag	tcpseq	tcpack	tcpln	tcpwin	ttl	tos	id	dgmle	iplen	icmpty	icmpcc	icmpid	icmpseq
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	52825	18:66:[	B8:AC:	0x6E						128	0	7196	96	98304				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	54941	18:66:[	B8:AC:	0xAB						128	0	7208	157	2E+05				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	54941	18:66:[	B8:AC:	0xAB						128	0	7208	157	2E+05				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	60081	18:66:[	B8:AC:	0xD8						128	0	7212	202	2E+05				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	60081	18:66:[	B8:AC:	0xD8						128	0	7212	202	2E+05				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	54459	18:66:[	B8:AC:	0x5B						128	0	7248	77	78848				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	54459	18:66:[	B8:AC:	0x5B						128	0	7248	77	78848				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	65359	18:66:[	B8:AC:	0x5B						128	0	7249	77	78848				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.5	65359	18:66:[	B8:AC:	0x5B						128	0	7249	77	78848				
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.1		192.168.10.3		00:C1:I	18:66:[	0x46						255	192	44540	56	57344	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.1		192.168.10.3		00:C1:I	18:66:[	0x46						255	192	44588	56	57344	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.1		192.168.10.3		00:C1:I	18:66:[	0x46						255	192	44595	56	57344	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39457	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39457	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39465	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39465	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39468	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.51		192.168.10.3		B8:AC:	18:66:[	0x78						64	192	39468	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.17		192.168.10.3		00:23:/	18:66:[	0x78						64	192	49826	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.17		192.168.10.3		00:23:/	18:66:[	0x78						64	192	49826	106	1E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:	18:66:[	0xA5						128	0	13975	151	2E+05	3	3	0	0
2017/0	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:	18:66:[	0xA5						128	0	13975	151	2E+05	3	3	0	0
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.1	57694	18:66:[	B8:AC:	0x5C						128	0	24969	78	79872				
2017/0	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.10.1	57694	18:66:[	B8:AC:	0x5C						128	0	24969	78	79872				

Figure.3.3. Snort detection Alerts of Tuesday

Wednesday:

timestamp	sig_ge	sig_id	sig_re	msg	proto	src	srcport	dst	dstpor	ethsr	ethds	ethle	tcpfla	tcpse	tcpack	tcpln	tcpwi	ttl	tos	id	dgmle	iplen	icmpt	icmpc	icmpi	icmpseq
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	1917	16	INDIC	UDP	192.168.10.15	49792	239.255.255.250	1900	00:1E:	01:00:	0xB3						4	0	27394	165	168960				
2017/07/05-0	1	538	15	NETBI	TCP	192.168.10.12	37082	192.168.10.50	139	B8:AC	00:19:	0xA2	***AF	0xEB9	0xCF7AF5AC	0xF5		64	0	15591	148	151552				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	61826	18:66:	B8:AC	0x6E						128	0	4344	96	98304				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	61826	18:66:	B8:AC	0x6E						128	0	4344	96	98304				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	54167	18:66:	B8:AC	0x98						128	0	4351	138	141312				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	54167	18:66:	B8:AC	0x98						128	0	4351	138	141312				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	57660	18:66:	B8:AC	0x5B						128	0	4359	77	78848				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	57660	18:66:	B8:AC	0x5B						128	0	4359	77	78848				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	60619	18:66:	B8:AC	0x6B						128	0	4367	93	95232				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	60619	18:66:	B8:AC	0x6B						128	0	4367	93	95232				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	64055	18:66:	B8:AC	0xB2						128	0	4404	164	167936				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	64055	18:66:	B8:AC	0xB2						128	0	4404	164	167936				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	53003	18:66:	B8:AC	0x6E						128	0	4416	96	98304				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.9	53003	18:66:	B8:AC	0x6E						128	0	4416	96	98304				
2017/07/05-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.12	54103	18:66:	B8:AC	0x91						128	0	14789	131	134144				

Figure.3.4. Snort detection Alerts of Wednesday

Thursday:

timestamps	sig_ge	sig_id	sig_re	msg	proto	src	srcport	dst	dstport	ethsr	ethds	ethle	tcpfla	tcpse	tcpack	tcpln	tcpwi	ttl	tos	id	dgmle	iplen	icmpt	icmpc	icmpi	icmpseq
2017/07/06-0	1	2578	10	SERVI	UDP	192.168.10.19	49210	192.168.10.3	88	00:23:	18:66:	0x124						64	0	3794	278	22532				
2017/07/06-0	1	402	16	PROT	ICMP	192.168.10.15		192.168.10.3		00:1E:	18:66:	0xA5						128	0	7713	151	154624	3	3	0	0
2017/07/06-0	1	402	16	PROT	ICMP	192.168.10.15		192.168.10.3		00:1E:	18:66:	0xA5						128	0	7713	151	154624	3	3	0	0
2017/07/06-0	1	402	16	PROT	ICMP	192.168.10.15		192.168.10.3		00:1E:	18:66:	0xA5						128	0	7717	151	154624	3	3	0	0
2017/07/06-0	1	402	16	PROT	ICMP	192.168.10.15		192.168.10.3		00:1E:	18:66:	0xA5						128	0	7717	151	154624	3	3	0	0
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.15	57536	18:66:	00:1E:	0x5C						128	0	16127	78	79872				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.15	57536	18:66:	00:1E:	0x5C						128	0	16127	78	79872				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.5	53968	18:66:	B8:AC	0x5C						128	0	30027	78	79872				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.5	53968	18:66:	B8:AC	0x5C						128	0	30027	78	79872				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	53554	18:66:	B8:AC	0x6E						128	0	14014	96	98304				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	53554	18:66:	B8:AC	0x6E						128	0	14014	96	98304				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	55778	18:66:	B8:AC	0x8D						128	0	14021	127	130048				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	55778	18:66:	B8:AC	0x8D						128	0	14021	127	130048				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	53531	18:66:	B8:AC	0x8C						128	0	14029	126	129024				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	53531	18:66:	B8:AC	0x8C						128	0	14029	126	129024				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	59935	18:66:	B8:AC	0x6C						128	0	14040	94	96256				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	59935	18:66:	B8:AC	0x6C						128	0	14040	94	96256				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	57754	18:66:	B8:AC	0xD8						128	0	14045	202	206848				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	57754	18:66:	B8:AC	0xD8						128	0	14045	202	206848				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	54580	18:66:	B8:AC	0x6E						128	0	14065	96	98304				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	54580	18:66:	B8:AC	0x6E						128	0	14065	96	98304				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	58955	18:66:	B8:AC	0x14B						128	0	14072	317	62468				
2017/07/06-0	1	254	16	PROT	UDP	192.168.10.3	53	192.168.10.14	58955	18:66:	B8:AC	0x14B						128	0	14072	317	62468				
2017/07/06-0	1	1917	16	INDIC	UDP	192.168.10.15	63176	239.255.255.2	1900	00:1E:	01:00:	0xB3						4	0	16530	165	168960				

Figure.3.5. Snort detection Alerts of Thursday

Friday:

timestamp	sig_gen	sig_id	sig_rev	msg	proto	src	srcpor	dst	dstport	ethsrc	ethdst	ethler	tcpflags	tcpse	tcpac	tcpln	tcpwindo	ttl	tos	id	dgmle	iplen	icmpt	icm	icmp	icr
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	54608	18:66:DA:	B8:AC:6F:	0x5C						128	0	21401	78	79872				
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	61968	18:66:DA:	B8:AC:6F:	0x5C						128	0	4799	78	79872				
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	61968	18:66:DA:	B8:AC:6F:	0x5C						128	0	4799	78	79872				
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA5						128	0	20035	151	154624	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA5						128	0	20035	151	154624	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA5						128	0	20036	151	154624	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA5						128	0	20036	151	154624	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA7						128	0	20197	153	156672	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA7						128	0	20197	153	156672	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA7						128	0	20202	153	156672	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.14		192.168.10.3		B8:AC:6F:	18:66:DA:	0xA7						128	0	20202	153	156672	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.25		192.168.10.3		00:25:00:A	18:66:DA:	0x46						64	0	26838	56	57344	3	3	0	
2017/07/07-08	1	402	16	PROTOCO	ICMP	192.168.10.25		192.168.10.3		00:25:00:A	18:66:DA:	0x46						64	0	26838	56	57344	3	3	0	
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	63628	18:66:DA:	B8:AC:6F:	0x6C						128	0	22748	94	96256				
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	63628	18:66:DA:	B8:AC:6F:	0x6C						128	0	22748	94	96256				
2017/07/07-08	1	538	15	NETBIOS S	TCP	192.168.10.25	49162	192.168.1(	139	00:25:00:A	00:19:B9:0	0xA2	***AP*	0xC44	0xA7507C		0xFFFF	64	0	21447	148	151552				
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	41732	18:66:DA:	00:23:AE:	0x91						128	0	20791	131	134144				
2017/07/07-08	1	254	16	PROTOCO	UDP	192.168.10.3	53	192.168.1(	41732	18:66:DA:	00:23:AE:	0x91						128	0	20791	131	134144				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				
2017/07/07-08	1	1917	16	INDICATO	UDP	192.168.10.14	59345	239.255.2	1900	B8:AC:6F:	01:00:5E:7	0xB3						4	0	24360	165	168960				

Figure.3.6. Snort detection Alerts of Friday

Table 3.9 shows the false positive and false negative counts obtained for snort. Table 3.10 shows the rates computed from the obtained counts.

Days	TP	TN	FP	FN
Monday	0	252202	52181	0
Tuesday	11899	1936	45232	386842
Wednesday	175888	395770	44261	77211
Thursday	2423	410482	44023	2040
Friday	2091	286832	41471	148076

Table3.9. The total number of TP, TN, FP, and FN obtained by running Snort on the dataset for each day

Day	**Accuracy %**	**Attacks**	**DR %**	**FPR%**
Monday	82.85	Benign	N/A	17.1432
Tuesday	3.10	Benign, FTP-Patator, SSH-Patator	2.98	95.89
Wednesday	82.47	Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed	69.49	10.05
Thursday	89.96	Benign, Web Attack-Brute Force, Web Attack-Sql Injection, Web Attack-XSS, Infiltration	54.29	9.68
Friday	60.38	Benign, Bot, PortScan, DDoS	13.92	1.38
Average	63.75		28.13	16.83

Table.3.10. Snort's Accuracy, DR, and FPR per day and average in percentage

The performance of Snort, particularly on Wednesday and Thursday is better than on the other days of UNBCIC2017. However, the overall detection capability is relatively low.

3.3.2 Evaluation Using the AEN Fingerprint Detection

JSON files are used as input for the AEN FINGERPRINT detection model. As a first step, the captured packet data from the dataset's pcap files must be converted to JSON files. In this project, the fingerprint is working on the PGX engine.

This project only uses fingerprints for dos attacks. After launching the detector, it examines the graph for suspicious IP addresses. The fingerprint detection after uploading JSON files of each day based on the dataset indicated that only Monday, Wednesday, Thursday, and Friday were detected. No attack fingerprint was detected on Tuesday. These two days malicious IPs were detected as a probing port scan.

The list of IPs that were detected for Monday, Wednesday, Thursday, and Friday is shown in Table 3.11.

Monday		
Type	Victim	Attackers
Probing port scan	Host (192.168.10.25)	Host (192.168.10.12)
Tuesday		
Type	Victim	Attackers
N/A	N/A	N/A
Wednesday		
Type	Victim	Attackers
Probing port scan	Host (192.168.10.25)	Host (192.168.10.50)
Thursday		
Type	Victim	Attackers
Probing port scan	Host (192.168.10.12)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.5)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.9)	Host (192.168.10.8)

Probing port scan	Host (192.168.10.17)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.19)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.51)	Host (172.16.0.1)
Probing port scan	Host (192.168.10.15)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.25)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.51)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.16)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.50)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.14)	Host (192.168.10.8)
Probing port scan	Host (192.168.10.25)	Host (192.168.10.19)
Friday		
Type	Victim	Attackers
Probing port scan	Host (172.16.0.1)	Host (192.168.10.50)
Probing port scan	Host (192.168.10.50)	Host (172.16.0.1)
Probing port scan	Host (192.168.10.25)	Host (192.168.10.50)

Table 3.11. Suspicious IP address detected by the AEN Attack fingerprint

Tables 3.12 provides the number of suspicious IPs detected and misclassified by the detector. Table 3.13 shows provides the corresponding performance rates. Table 3.14 depicts the attack instances detected and the triggered fingerprints.

Days	Attack Fingerprint IPs	Labeled Malicious IPs
Monday	'192.168.10.12', '192.168.10.25'	Benign
Tuesday	N/A	172.16.0.1, 192.168.10.50,
Wednesday	'192.168.10.50', '192.168.10.25'	172.16.0.1,192.168.10.50, 192.168.10.51
Thursday	‘192.168.10.12’,‘192.168.10.5’, ‘192.168.10.9’,‘192.168.10.17’,	192.168.10.8,205.174.165.73,172.16.0.1, 192.168.10.50,

	‘192.168.10.19’,‘192.168.10.51’,‘192.168.10.15’,‘192.168.10.25’,‘192.168.10.16’,‘192.168.10.50’,‘192.168.10.14’,‘192.168.10.8’, ‘172.16.0.1’	
Friday	'172.16.0.1', '192.168.10.50', '192.168.10.25'	192.168.10.12,192.168.10.14, 192.168.10.15,192.168.10.17, 192.168.10.5, 192.168.10.8, 192.168.10.9,205.174.165.73, 52.6.13.28, 52.7.235.158,

Table.3.12. Suspicious IP addresses detected by the AEN attack fingerprints

The information on the false positive, false negative, true positive, and true negative is calculated in the tables. 3.13 1nd 3.14 below. Moreover, the accuracy (AC) is obtained from this information.

Day	TP	FP	FN	TN
Monday	0	1	0	304382
Tuesday	N/A	N/A	N/A	N/A
Wednesday	1	0	252671	440031
Thursday	3	10	2213	456742
Friday	1	2	288922	190045

Table.3.13. The total number of TP, TN, FP, and FN obtained by running Fingerprint on the dataset for each day

Day	Labeled as malicious	Accuracy%	DR%	FPR%
Monday	Benign	99.99	0	0
Tuesday	Benign, FTP-Patator, SSH-Patator	N/A	N/A	N/A
Wednesday	Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoSslowloris, Heartbleed	63.52	0.00039	0
Thursday	Benign, Web Attack-Brute Force,WebAttack-Sql Injection, Web Attack-XSS, Infiltration	99.51	0.1353	0.0021
Friday	Benign, Bot, PortScan, DDoS	39.67	0.00034	0.0010
Average		60.54	0.02720	0.00062

Table.3.14. Fingerprint's Accuracy, DR, and FPR per day and average in percentage

3.3.3 Discussions

The average accuracy of this study for attack fingerprints is 60.54%. The DDoS attacks were detected by fingerprint attacks utilizing dataset data on Friday as well as Wednesday. In addition, the port scan was performed on Friday using dataset data from Friday. Three malicious IP addresses were reported on Friday by the attack fingerprint model. However, one of them was detected with the UNBCIC2017 dataset. As a result, there are two false positives which means that they were not malicious in the dataset but were detected as malicious by the attack fingerprint. On Monday, 2 IP addresses were identified as false positives. Both IP addresses triggered an attack fingerprint. On Monday, no malicious IP addresses were discovered, according to the dataset. In addition, three types of attacks were launched on Thursday, including infiltration, a Web attack, and a Web Attack Brute force.

In this research we calculated three evaluations after evaluate TN, TP, FP, FT. Accuracy, Detection Rate and False Positive Rate.

In this context, four possibilities occur, corresponding to the relationship between the detection result for an evaluated activity, the regular and the intrusion activities. False positives, true positives, false negatives, and true negatives are all possible scenarios.

False positives (FP) happen when an event is analyzed and labelled malicious even though it is safe or benign from a security perspective.

If the analyzed event is appropriately classified as an intrusion or malicious, it is a true positive (TP).

If the analyzed event is malicious but is classified as normal or benign, it is a false negative (FN).

If the analyzed event is correctly identified as normal or benign, it is a true negative (TN).

Low FP and FN rates, along with high TP and TN rates, will clearly result in high efficiency values.

In this research the TP and TN of Wednesday, Thursday, and Friday and also Monday because of all activities are Benign higher than FP and FN, so the Accuracy of those days are high in Snort detection result.

According to the information of the Table.3.9 and Table.3.10 report, the snort detection efficiency rate of all days except Tuesday are the good.

And also, in AEN Graph Fingerprint detection the TP and TN of Thursday higher than FP and FN, so the Accuracy of Thursday is higher than other days.

According to the information of the Table.3.13 and Table.3.14 report, the AEN graph Finger print detection in the better performance and efficiency on Thursday.

On Thursday, three different types of web attacks were launched. On Thursday, three of the thirteen victim hosts' IP addresses were identified by an attack fingerprint. Table 3.13 displays the fingerprint attack results in, FP, TP, FN, TN, Accuracy, DR, and FPR. All the IP addresses generated in Table 3.12 were clearly detected by the attack fingerprint detector. Due to a lack of system resources and software development, there were no more results for Tuesday in this dataset. Tuesday's

file size is the same as the other days in UNBCIC2017, so the lack of results was not dependent on the file size. However, no malicious IP addresses were detected by the attack fingerprint detector on Tuesday. On Tuesday, there are three attacks: an SSH, an FTP, and a brute-force attack.

In an SSH brute force attack, an attacker tries various combinations of credentials to gain access to a server. Vulnerabilities are not required for the success of brute force attacks.

A brute force attack is a hacking technique that makes use of trial and error to break encryption keys, passwords, and login credentials. It is a straightforward but effective strategy for getting unauthorized access to user accounts, company systems, and networks.

FTP bounce attack is an FTP protocol exploit in which an attacker uses the PORT command to request access to ports indirectly via the victim system, which acts as a proxy for the request, similar to an Open mail relay using SMTP.

In order to be able to identify SSH and brute force attacks, the AEN graph must have defined the password guessing component to detected those attack on Tuesday.

In a previous evaluation of the AEN attack fingerprint research using the ISOT cloud intrusion detection (ISOT CID) dataset, Attack Fingerprints based on the Activity and Event Network (AEN) Model [12], only attacks on Friday, Wednesday and Monday were detected for this dataset, CIC IDC 2017. Although, in current research attacks on all days were detected except Tuesday.

The result of this part illustrates that the fingerprint can detect that there is an attack, but the specific type of attack may be incorrect. In this research, the IP address was detected properly but the type of attack for all days is labeled as a ports scan. More information about the attack fingerprint and mapping with malicious IPs detected in a dataset in Table 3.11 and Table 3.12 above.

The result of the previous research indicated that the number of false positives is often larger than the number of false negatives. This is because the fingerprint tests more generic behavior, and attacks with specific features are detected as unrecognized.

In current research is the same and only in this research large amount of data in UNBCIC2017 detected by attack fingerprint. According to the information on IPs and type of attacks each day, the results illustrated that the IP address detected in the attack fingerprint belonged to which type of attack.

On Friday, only a DDoS attack was detected by a fingerprint detector. However, all attacks type in attack fingerprint labeled as a port scan. This is the issue of fingerprint detectors.

On Wednesday, the IP address was detected as a port scan. It is the only attack type the fingerprint that was detected correctly.

On Thursday, all IP addresses were detected as infiltration, Benign, and three different web attacks such as web attack brute force, web attack SQL injection, and web attack XSS.

On Tuesday, no IPs were detected by attack fingerprint.

Finally, on Monday both IP addresses were detected as not correct. A false positive occurs when a fingerprint attack wrongly identifies something as malicious when it is safe.

The accuracy of Thursday was higher than on other days in this research because the number of IPs related to each attack detected by this system was higher. According the information of both tables Table 3.2 and 3.12, on Thursday all type of attacks such as web attack brute force, web attack SQL injection, XSS and a majority of attacks of infiltration were detected correctly by AEN graph attack fingerprint.

The result of attack fingerprint shown in the table below.

Day	**Labeled as malicious**	**Alerts fingerprint labeled**	**Accuracy%**	**DR%**	**FPR%**
Monday	Benign	port scan	99.99	0	0
Tuesday	Benign, FTP-Patator, SSH-Patator	N/A	N/A	N/A	N/A
Wednesday	Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoSslowloris, Heartbleed	port scan	63.52	0.00039	0
Thursday	Benign, Web Attack-Brute Force,WebAttack-	port scan	99.51	0.1353	0.0021

	Sql Injection, Web Attack-XSS, Infiltration				
Friday	Benign, Bot, PortScan, DDoS	port scan	39.67	0.00034	0.0010
Average			60.54	0.02720	0.00062

Table.3.15. Fingerprint's Accuracy

CHAPTER 4: CONCLUSION

As the rate of data breaches has risen rapidly in recent decades, there is an urgent need to deploy the optimal strategies and select the best detection and prevention solutions to safeguard cyber networks. Given the wide range of IDSs currently available, whether open-source or license-based software, network-based or host-based, a deeper understanding of their performance is essential. Intrusion detection systems utilize two basic approaches to identifying threats: signature-based and anomaly-based. The two primary approaches for detecting and alerting about threats are signature-based and anomaly-based detections. Signature-based detection is often used to detect known threats. It uses a pre-programmed list of known threats and their indicators of compromise to operate. When a signature-based IDS analyses packets passing through the network, it compares them to a database of known attack signatures to detect any suspicious activity. In this research, the snort detection is better performance as an IDS than an attack fingerprint detector. Both Snort and AEN graph finger print are worked as a signature-based detector.

The current AEN model works on a PGX-only as an attack fingerprint. On a 24 GB RAM system, we can only process a restricted amount of dataset IPs at this moment. It is fair to presume that a significant amount of memory has been exposed. To solve the memory problem, the Java Virtual Machine (JVM) speed should be optimized.

Therefore, the attack fingerprint detector detects just reports port scans with the present fingerprint detector. This program defines the DDoS attack; however, the threshold needs to be modified to correctly detect it. All attacks detected by fingerprint were identified as port scans. More sorts of attacks, such as bots, infiltration, and various Web attacks like brute force, SQL Injection, and XSS, supported by this fingerprint's detector. Fingerprints must also be used to identify different types attacks like DDoS attacks, and Heartbleed.

The performance of the AEN graph attack fingerprint detector was compared to the Snort IDS in this research. These data show that the Snort IDS detects attacks more effectively than the AEN attack fingerprint. More data and information about snort detection can be found in Tables 5–8, as well as the result of the AEN graph based on attack fingerprints in table 3.15. The Table 4.16 indicates the brief comparison between Snort detection as an IDS and AEN graph finger print that both are signature-based detection. In Snort the large number of attacks type detected correctly but in finger print only port scan was detected.

Day	**Labeled as malicious in CIC 2017 Dataset**	**Alerts fingerprint labeled**	**Fingerprint Accuracy%**	**Snort Accuracy%**
Monday	Benign	port scan	99.99	82.85
Tuesday	Benign, FTP-Patator, SSH-Patator	N/A	N/A	3.10
Wednesday	Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoSslowloris, Heartbleed	port scan	63.52	82.47
Thursday	Benign, Web Attack-Brute Force, Web Attack-SQL Injection, Web Attack-XSS, Infiltration	port scan	99.51	89.96
Friday	Benign, Bot, PortScan, DDoS	port scan	39.67	60.38
Average			60.54	63.75

Table.4.16. Snorts and Fingerprint’s Accuracy Comparison

REFERENCE

[1] Venugopalan S R, Ashok Kumar D, Intrusion Detection Systems: A Review Intrusion Detection Systems: A Review, Project: Network Anomaly Detection System, Volume 8, No. 8, September-October 2017, pages 356-370.

[2] Https://Www.Kaggle.Com/Datasets/Cicdataset/Cicids2017

[3] Https://Www.Unb.Ca/Cic/Datasets/Ids-2017.Html

[4] https://www.uvic.ca/ecs/ece/isot/publications/by-area/intrusion-detection/index.php

[5] Issa Traore, Paulo Gustavo Quinan, Waleed Yousef, "The Activity and Event Network (Aen) Model: Graph Elements And Construction", Technical Report, Isot Lab, Ece Department, University Of Victoria, January 2020.

[6] Oracle. Oracle Labs Pgx: Parallel Graph Analytix, https://www.oracle.com/middleware/technologies/parallel-graph-analytix.html

[7] Oracle. Property Graph Query Language. View Data As A Graph, Discover Insights, Unlock Endless Querying Possibilities, https://docs.oracle.com/en/database/oracle/property-graph/20.4/spgdg/property-graph-query-language-pgql.html

[8]Https://Www.Cloudsavvyit.Com/6424/How-To-Use-The-Snort-Intrusion-Detection-System-On-Linux/#:~:Text=Snort%20analyzes%20network%20traffic%20in%20real-Time%20and%20flags,Snort%20should%20do%20if%20a%20rule%20is%20triggered.

[9] Iman Sharafaldin, Arash Habibi Lashkari, And Ali A. Ghorbani, "Toward Generating A New Intrusion Detection Dataset And Intrusion Traffic Characterization", 4th International Conference On Information Systems Security And Privacy (Icissp), Portugal, January 2018, pages 108-116.

[10] Https://Docs.Oracle.Com/En/Database/Oracle/Property-Graph/20.4/Spgdg/Property-Graph-Query-Language-Pgql.Html#Guid-301ff092-1a07-43d2-91e5-0c5aff3467cc

[11] Ayodele Lasisi, Rozaida Ghazali, And Tutut Herawan, " Application Of Real-Valued Negative Selection Algorithm To Improve Medical Diagnosis" Emerging Topics in Computer Science and Applied Computing2016, Pages 231-243.

[12] Chenyang Nie," Attack Fingerprints Based On The Activity And Eventnetwork(Aen) Model", UVicSpace Home → Faculty of Engineering → Department of Electrical and Computer Engineering → Graduate Projects (Electrical and Computer Engineering), 2020-08-12.