Contents

List of Figures

Chapter 1

Introduction

1.1 Preamble

Currently most devices we see around us are connected to the Internet for convenience and transfer of data. But with this advantage, there is another dark side to the benefits of being connected, the leakage of personal data. Cyber-Terrorists and hackers try to compromise network infrastructure for destruction or monetary gain.

Information Systems and Networks are subject to electronic attacks. Attempts to breach information security are rising every day, along with the availability of the Vulnerability Assessment tools that is widely available on the Internet. Tools such as Nmap can be used to scan, identify, probe, and penetrate your systems. Firewalls are put in place to prevent unauthorized access to the Enterprise Networks.

In the 1990's, IDS technology was developed using a method called anomaly detection to address the increasing number and sophistication of network attacks. It relied on identifying unusual behavioural patterns on the network, and provided alerts for any identified abnormality. In the advent of cloud computing and IoT, it resulted in the surge in the IDS market, IDS systems are designed to detect attacks that may occur despite

the presence of a firewall in a network.

1.2 Motivation

Considering that an Intrusion Detection System is one of the top selling security technologies for Enterprise Network Security, the logic and tactics IDS uses are more relevant today than ever before. An Intrusion Detection System is a software within the network that detects the abnormalities or the presence of an unauthorised user within a network. They can be either Detection Based or Range Based. A Detection based can be on the basis of a Signature id or an Anomaly. It also depends on where the IDS is placed within the network.

In the late 1990s, military and enterprise networks were prone to ICMP, TCP, UDP attacks. With the advent of smart devices, IoT, Cloud Computing and Big Data, enterprises were prone to more advanced attacks like DDoS, U2R, and malware attacks. Due to this sophistication, Intrusion Detection Systems have undergone improvements to intercept these attacks.

1.3 Scope and Objectives

With growing cyberthreats and intrusions within enterprise networks.This project is aimed at developing a more efficient real time Intrusion detection system to face threat adversaries to the network. With existing updated datasets and growing number of attacks everyday, this project aims to be implemented in the enterprise and personal level with less false positives and better mitigation options.

1.4 Organization of the report

The first chapter is an overview of the seminar. The motivation for this topic, scope and objective of the seminar are also discussed. The next chapter cites literature surveys of the journal papers used in the research of this seminar. Furthermore, the later chapters discuss about Firewalls and Intrusion Detection Systems. Next, the seminar describes SNORT: an IDS/IPS and its operation modes. The final chapter provides the concluding remarks of the seminar.

Chapter 2

Literature Survey

2.1 Machine Learning and Deep Learning Approaches for Cybersecurity: A Review

2.1.1 Introduction

Cybersecurity is defined as the process of implementing cyber protective measures and policies to protect data, programs, servers, and network infrastructures from unauthorized access or modification. The internet connects the majority of our computer systems and network infrastructure. As a result, cybersecurity emerged as the backbone for practically all types of corporations, governments, and even people to secure data, grow their businesses, and maintain privacy.

This paper discusses what an IDS is, the types of IDS, and evaluates various Machine Learning, Deep Learning and Hybrid Learning Models performed on various detection datasets like KDD Cup 99' and CIC - IDS 2017.

2.1.2 Intrusion Detection Systems

Intrusion Detection is the process of monitoring network traffic and events in computers in order to detect unexpected events, and it is called Intrusion Detection System (IDS).

Figure 4.1 depicts the deployment of a Network-Based Intrusion Detection System (NIDS) and a Host-Based Intrusion Detection System (HIDS). NIDS, examines packets gathered by network devices such as routers, while HIDS examines events on a host computer.

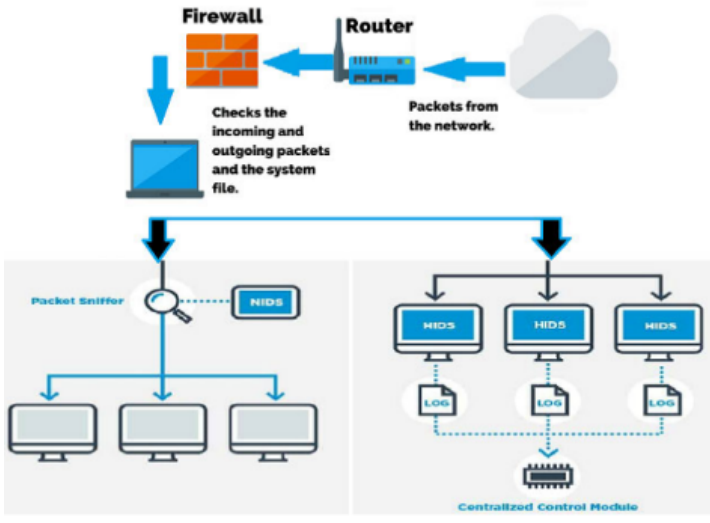


Figure 2.1: A Network Intrusion Detection System Vs A Host Based Intrusion Detection System

2.1.3 IDS Approach

Intrusion Detection techniques are classified into Anomaly and Signature based IDSs. Anomaly based IDS work on a set of baseline rules. When these rules are violated, the administrator is alerted of a abnormal activity via the management console. Signature based IDS works on the basis of a signature id defined by the administrator's detection dataset, if the action id is a match, the administrator is alerted of a malicious packet in the network.

2.1.4 Evaluation Metric

Used to assess an intrusion detection system's performance. These indicators are based on the confusion matrix component that contains four metrics: True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN), and the assessment indicators are as follows:

- Accuracy - A higher accuracy indicates a more accurate prediction by the learning model.
- Precision - A high precision rate equates to a low rate of false positives.
- Recall - The model's capacity to locate all positive records is the detection rate, as it quantifies the correctly predicted records.
- F1-Score - The sum of Precision and Recall; a higher F1 indicates a more effective learning model.
- False Positive Rate (FPR) - To compute the False Alarm Rate, divide the total number of normal records identified as attacks by the total number of normal records.

2.1.5 Datasets Used

- CIC-IDS 2017 - This dataset contains normal and attack scenarios and includes an abstract behavior for 25 users based on SSH, HTTPS, HTTP, FTP, and email protocols
- KDD Cup 1999 - This dataset is the most widely used dataset for intrusion detection, includes basic and high-level TCP connection information such as the connection window but no IP addresses. In

addition, this dataset contains over 20 different types of attacks and a record for the test subset.

Data Set	Year	Availability	No. of features	Kind of traffic
KDD Cup99	1998	Public	41	Emulated
NSL-KDD	1998	Public	41	Emulated
ISOT	2010	Public	49	Emulated
ISCX 2012	2012	Public	8	Emulated
UNSW-NB15	2015	Public	42	Emulated
KYOTO	2015	Public	24	Real traffic
CIC-IDS2017	2017	Public	84	Emulated

Figure 2.2: Comparison between Datasets

2.1.6 Limitations

- Imbalanced dataset: Existing datasets contain varying numbers of records for various types of attacks. These differences will affect the accuracy and detection rate of various types of attacks.

- Unavailability of up to date dataset: One of the challenges for IDS is to maintain an up-to-date dataset with sufficient records to cover the majority of attack types to ensure maximum efficiency.

- Hyper parameter Tuning: The activation function and optimization method, the number of nodes per layer, and the total number of layers in a network are all hyperparameters. They affect training and model building, with the ability to increase or decrease the IDS model's accuracy and detection rate.

- Performance in the Real World: An IDS model faces a challenge when it is implemented in a real-world environment, as the models are developed in the lab by testing and training.

2.1.7 Conclusion

Many researchers are developing a system that will secure data against malicious conduct. However, research into other applications of learning algorithms, such as establishing a new dataset or merging algorithms, is currently ongoing. As a result, this paper explains the concept of an intrusion detection system, types of attacks, and how to determine whether or not a system is effective.

2.2 Performance comparison of intrusion detection systems and application of machine learning to SNORT system

2.2.1 Introduction

Today many businesses rely on computer networks. These networks fulfil the needs of business, enterprises and government agencies to build knowledgeable, complicated information networks which integrate various technologies such as distributed data storage systems, encryption techniques, voice over IP (VoIP), remote or wireless access and web services.

The attackers act like normal users, generate data and hide their malicious activities under terabytes of data. Many security mechanisms cannot protect the networks due to the large amount of data stored, scalability issues or due to the lack of detection capabilities.

The enterprises and government agencies need to monitor their network traffic to detect malicious activities and perform analysis to differentiate the malicious and legitimate user activities to protect their networks. This

is done using intrusion detection systems (IDS) and in today's secure ICT infrastructure, the IDSs are part of most networks. However, the IDSs are only good if they have elite detection capabilities. It is critical that an IDS detection mechanism is accurate enough to differentiate between legitimate and malicious traffic that enter and leave the network.

The elite IDSs detect as much malicious traffic as possible and reduce the number of false alarms. This includes open source IDSs like SNORT, Suricata.

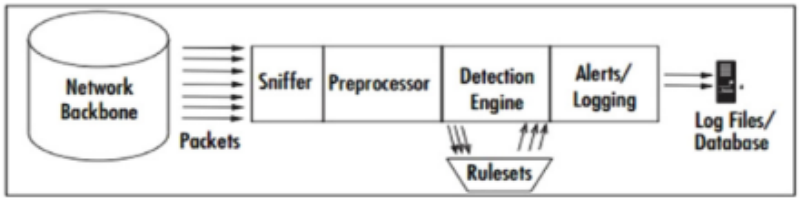


Figure 2.3: SNORT single threaded architecture

2.2.2 SNORT Vs. Suricata

The Snort IDS is extensively deployed in networks and researched into. Snort has a single threaded architecture as shown in Fig. 4.3 which uses the TCP/IP stack to capture and inspect network packets payload.

Suricata is publicised as a future next generation IDS integrating new ideas such as multithreading. Based on the previous research it has improved on Snort because it uses multi-thread architecture to quickly capture and decode network packets. It requires more processing power but more effective in detecting attacks than SNORT.

They have comparable functions, detection rule sets and syntax. They are both under GNU GPL licence. They both support intrusion prevention system (IPS) feature and support medium to high-speed network, though Suricata is more scalable with its multi-threaded architecture. Both support IPv6 traffic and their installation and deployment are easy.

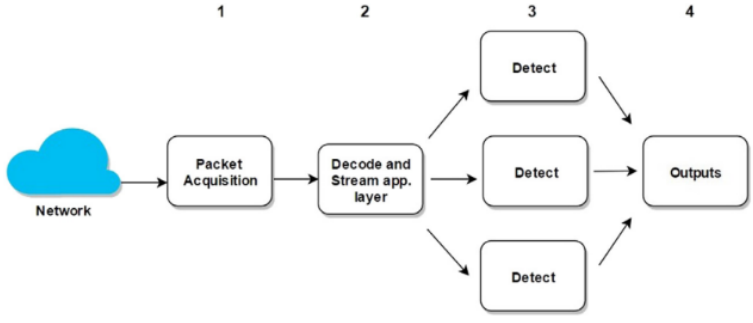


Figure 2.4: Suricata multi threaded architecture

2.2.3 The Attack Model

The attack model involved using Kali Metasploit Framework to generate 7 types of malicious traffic in a regulated traffic environment. They were injected to both SNORT and Suricata. Finally the two IDSs will monitor the traffic for malicious packets and if any is found to violate the ruleset, it will alert the administrator. The number of alarms (false positive, false negative and true positive) will show how accurately Snort and Suricata classifies the network traffic.

The first accuracy test was performed using the legitimate network traffic generator which injected UDP, TCP and ICMP packets to both IDSs. Snort's detection accuracy was found to be superior to Suricata in this scenario. The Suricata's false positive rate (FPR) was higher when processing UDP, TCP and ICMP packets than Snort's FPR.

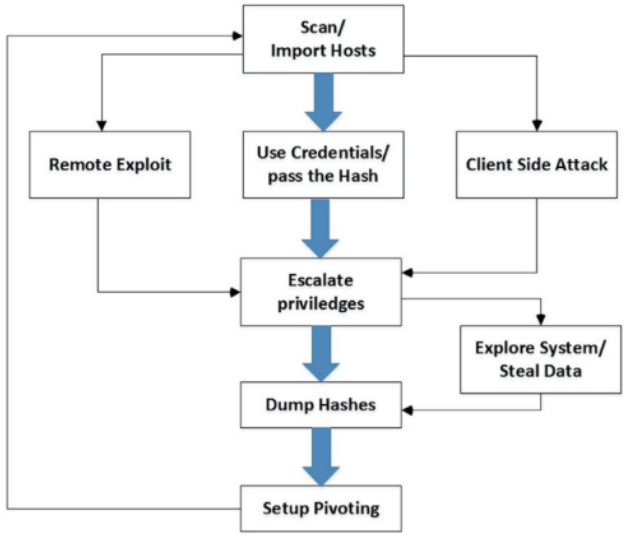


Figure 2.5: The attack model

SNORT detected 6 out of the 7 malicious types (Scan malicious attack being the exception) with less false positives than Suricata, which could not process the data link layer. The average FPR for Snort is 55.2% and for Suricata is 74.3%. Snort on average triggered 6.7% FNR and Suricata triggered 16.7%. SNORT being single threaded utilises much lesser processor power than Suricata but its FPR is a limitation, eventhough it is less than Suricata, it should be minimised.

2.2.4 SNORT using Machine Learning

The 5 machine learning algorithms conducted on SNORT were Support Vector Machines (SVM), Decision Tree, Fuzzy Logic, Bayes Net and Naive Bayes using the NSL-KDD dataset.

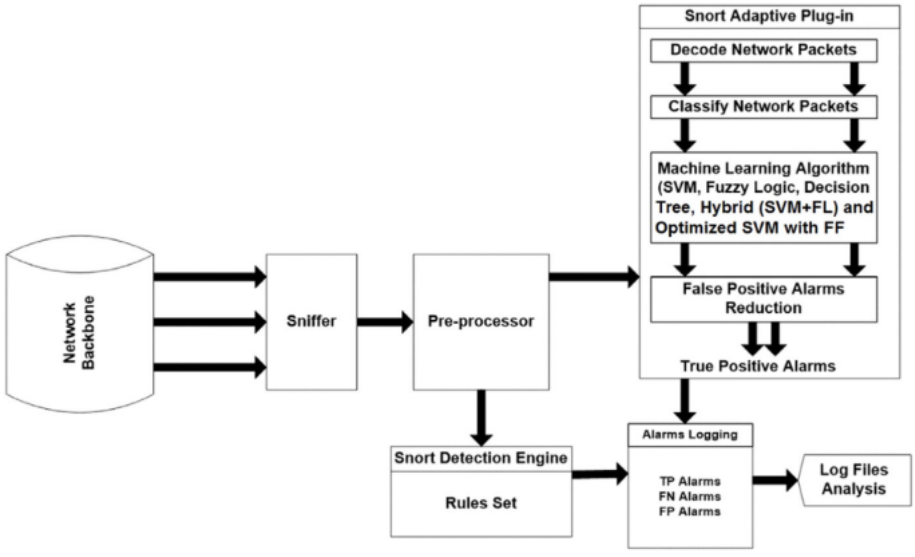


Figure 2.6: The proposed model of SNORT adaptive plug-in

2.2.5 Results

SNORT shows a FPR of 3.1% using SVM and an accuracy of 95.4% which was comparitively the best out of other machine learning algorithms. When a hybrid learning (SNORT adaptive plug-in) using SVM and firefly algorithm was conducted, it reduced the FPR to 2.2%. This paper showed why SNORT is the best open source IDS compared to Suricata.

2.3 On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures

2.3.1 Types of IDS

Network Intrusion Detection Systems (NIDS) provide a very efficient tool not only to detect such threats and attacks, but also to enforce usage policies to avoid internal misuse.

NIDS can be categorized according to the used detection method: Anomaly-based NIDS use behavior-based methods by defining a model of normal network behavior and then detecting deviations to this model. Knowledge based systems, on the other hand, use a precise definition of the attack and match incoming traffic against this definition. The most widespread variants of knowledge-based systems are signature or rule-based NIDS.

2.3.2 SNORT: A Knowledge Based IDS

In signature-based NIDS, a detection engine applies a rule-set to all received packets. The majority of state-of-theart Snort rules contain patterns that are matched against the payload of the received packets. These patterns range from specific bytes to complex Regular Expressions (RegExes) matching not only individual packets but also payload in a packet flow. Because of these performance intensive pattern matching operations, such systems can only cope with relatively low packet rates. SNORT obtains detailed description of packets which are later processed by Deep Packet Inspection (DPI) methods.

2.3.3 Flow Based Traffic Data

A Flow denotes a set of elements containing aggregated information of a number of packets sharing the same properties. These properties are composed by the following quintuple: source/destination addresses, source/destination ports, and transport protocol. The analysis of Flow-based traffic data requires an additional step in which the data is aggregated into so-called Flow records with the advantage of significantly reducing the amount of data to be analyzed.

2.3.4 IPFIX-based Signature based Intrusion Detection Systems (FIX-IDS)

IPFiX is associated with http payloads which makes FIXIDS supports HTTP-related rules. To be able to narrow the search space and speed up the pattern matching process, Snort offers the option to apply so called content modifiers to the pattern search. The idea is to restrict the search of content patterns to certain payload fields. Snort restricts the pattern search to HTTP related fields which shows again the importance of HTTP for intrusion detection.

To tackle this, Vermont; a Open Source packet monitoring toolkit is used. In this configuration, the IPFIX Flow Collector module listens to a configurable port for incoming Flows from a Flow source. These Flows are handed over to the FIXIDS module via a Flow queue. The FIXIDS module analyzes the incoming Flows comparing its fields with the patterns from the signatures in the rule file. In all the experiments for this work, FIXIDS is configured to use four pattern matching threads. Finally, all the detected events are written to the file given in the configuration.

2.3.5 Prerequisites of the Experiment

For the experiment, Cisco's TRex traffic generator is used. It enables stateful, timely, precise, and realistic high-speed traffic generation, and supports the custom creation of application layer payload. Generating Events for Signature Intrusion Detection Systems (GENES-IDS) framework is used to generate HTTP attacks and, thus, allows for straightforward generation of network traces (or live traffic) where the number of different detectable events is precisely defined by the given attack configuration. One of the

main advantages of GENES-IDS is that it uses the Snort syntax as input format and, thus, the user can take advantage of thousands of up-to-date and realistic attack definitions.

2.3.6 SNORT vs FIX-IDS

GENES-IDS created all 5,540 attacks over all runs. Snort as well as FIX-IDS have a reliably high true positive detection rate of more than 99 percent. Snort, on average, detected 5,489 true positives of the generated attacks with a maximum of 5,494 detected events and a minimum of 5,481. FIX-IDS detected slightly more with an average of 5,490 true positives of the generated attacks and a maximum of 5,495 detected events and a minimum of 5,483.

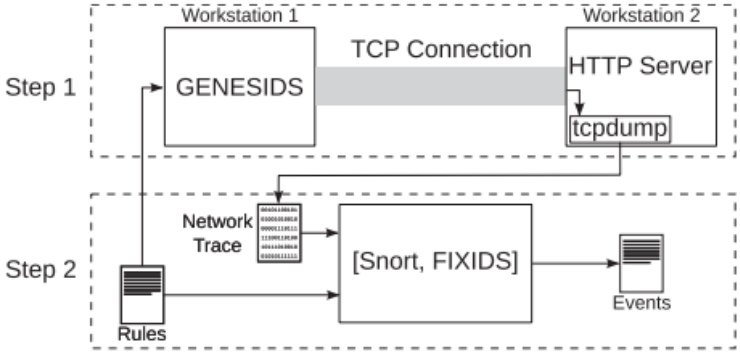


Figure 2.7: The proposed system architecture

These experiment results show that FIX-IDS has essentially the same detection accuracy as Snort and, thus, its detection functionality can be considered equal to the state-of-the-art. FIX-IDS processed most of the http packets and SNORT handled the non http packets.

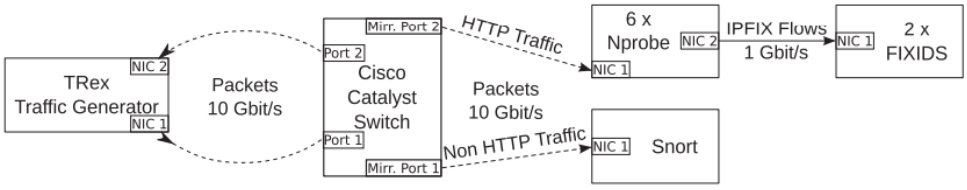


Figure 2.8: The proposed method in real time

2.3.7 Conclusion

FIX-IDS provides precise event detection in high-speed networks by using IP-FIX HTTP Flows for intrusion detection. It is the first signature-based Network Intrusion Detection System (NIDS) that completely operates on Flow information using the novel HTTP IP-FIX IEs. Besides custom attack signatures, FIX-IDS supports using signatures from the most widely used NIDS Snort. This ensures that thousands of community validated and up-to-date signatures are available for FIX-IDS. By using Flows the amount of data to be analyzed is much less compared to traditional DPI-based NIDS.

2.4 AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection

2.4.1 Introduction

An Intrusion Detection System (IDS) is used to identify intrusions, attacks, or violations of security policies in a network or host system promptly. An IDS system that inspects a packet of networks to detect attacks is called Network Intrusion Detection System (NIDS).

An NIDS runs mostly signature-based detection by Snort IDS rules. The analyst writes a user-defined pattern into the rules to detect an attack. When there is a malicious payload on the network traffic, the rule triggers

security events, including detection time, source/destination IP (metadata), and some raw packets (payloads). String or pattern match is reliable and generates very few false alarms but does not identify unknown or irregular pattern attacks.

2.4.2 AI-IDS

The AI-IDS is a flexible and scalable system that is implemented based on Docker images, and separates user-defined functions by independent images. AI-IDS process is as follows: (i) data save and splitting - collecting web traffic and splitting training data for each model (ii) data preprocessing and training by labeled analysis information (iii) prediction for suspicious payloads on new web-traffic.

The proposed AI-IDS trains the labeled analysis information based on HTTP data in-bounding from the managed services instead of metadata sets in a constrained environment. per day on legacy signature-based NIDS, and we perform about 10,000 automatic and manual analyses. During general security operations, malicious detection information is triggered by NIDS when an attack packet occurs in the network communication. Daily training-data on the production environment is labeled in real-time by security analysts using labeling tools. We detect about 200,000 attacks on about 1 billion HTTP

2.4.3 Optimized CNN-LSTM Model for Big Data

We demonstrated the process of model design in detail via performance evaluation between CNN-LSTM, LSTM-CNN, and DNN models based on fixed real-time data from HTTP request packets. Hyper-parameters were determined in each model through repeat experiments. An optimized neu-

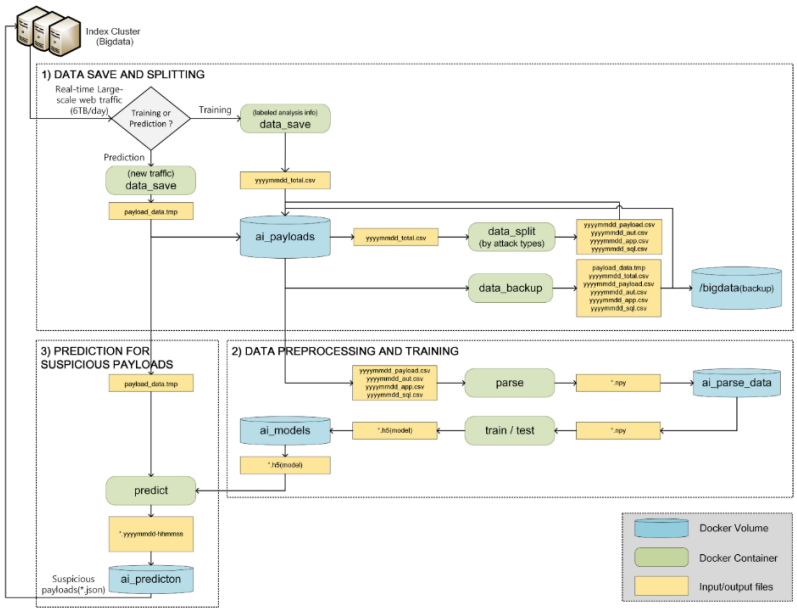


Figure 2.9: AI-IDS Architecture

ral network model was validated through experiments on public datasets (CSIC-2010, CICIDS2017) and fixed real-time data.

2.4.4 Conclusion

The AI-IDS distinguishes between normal and abnormal traffic on HTTP traffic that could not be detected in legacy signature-based NIDS because AI-IDS can formalize unknown patterns, help write or improve signature-based rules for new vulnerabilities, variants, and bypass attacks.

The AI-IDS performs continuous optimization by re-training analysis information that is labeled “benign”, “malicious,” and “unknown”. In practical security services, re-validation for predicted events is a required task because of the low tolerance for analysis errors.

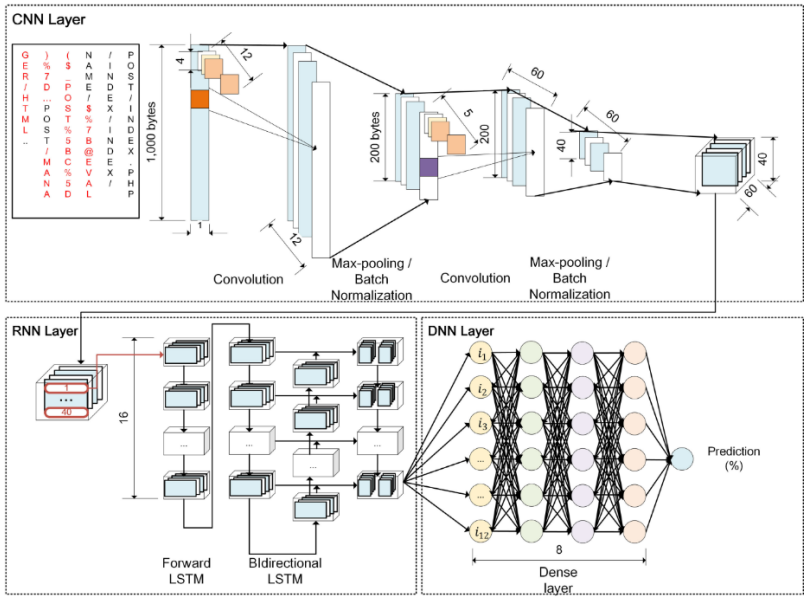


Figure 2.10: Structure of optimized convolutional recurrent neural networks

2.5 Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies

2.5.1 Introduction

AI has had a greater incidence in the detection of harmful software or anomalies and intrusions, generating new modules to support more efficient and robust decisions. This allows human interaction to focus on more abstract actions such as general monitoring of systems or the analysis of errors, i.e., false positives. In addition, AI techniques also help people responsible for IT security to manage and analyze the vast quantity of data that new information systems can generate.

Uses of AI includes the generation of new models of intrusion detection systems (IDS). These handle large volumes of data that must be evalu-

ated quickly while generating different types of alerts. In addition to the development of new and more efficient IDS, AI has been used as a basis for implementing IDS applying machine learning techniques for the categorization of patterns through explicit and implicit models. These techniques offer high adaptability to the inclusion and processing of new information.

One of the main problems is the abundance of data in contemporary cybersecurity datasets which requires intelligent algorithms, such as machine learning algorithms, for extracting meaningful information. Specifically, its application to IDS involves the need of high amount of features with the objective to select the best approach and detect the possibility of an attack. The problem is important, because a high number of characteristics in a dataset leads to a model overfitting, consequently turning into poor results on the validation datasets.

2.5.2 Neural Networks

Artificial neural networks are complex systems constructed by simple computational units called neurons, analogous to the behavior of neurons in biological brains. These neurons are interconnected through links that manage the activation state of adjacent neurons. Each neuron works according to an activation function, which relates its input to its output.

The application of artificial neural networks to the context of computer security is mainly focused on the detection of intrusions in a network since artificial neural networks are considered an efficient approach to pattern classification.

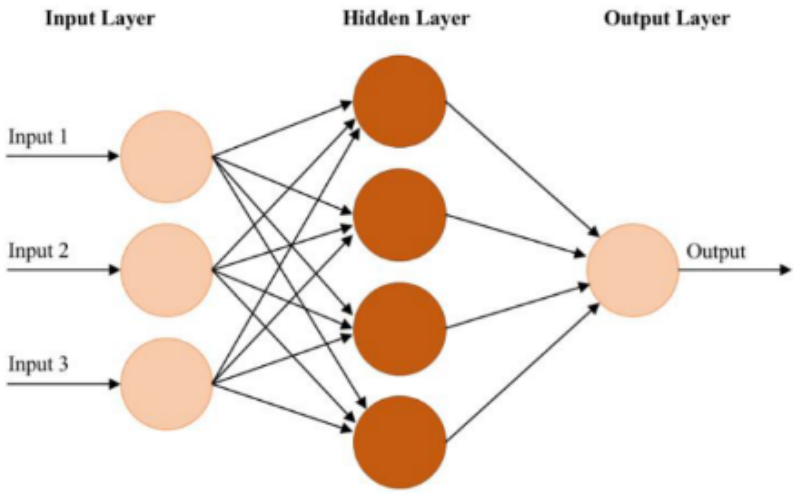


Figure 2.11: Neural Networks Architecture

2.5.3 Long Short Term Memory: A Recurrent Neural Network Architecture

LSTM minimises the problem of gradient descent. This neural network is composed of an LSTM neuron fed by a determined number of connections. These connections contain a distinct variable number of characteristics. The best accuracy obtained from this model is 98% using the UNSW-NB15 dataset.

2.5.4 Conclusion

This work explored the application of neural networks to the detection of cybersecurity intrusions with two main objectives. First, the categorization of a data set (UNSW-NB15), dividing its characteristics into basic, content, traffic statis- tics and direction-based methods, to analyze which of these groups are the most relevant for the detection of anomalies, and to reduce training and reduce the loss of the models implemented. The second objective focused on determining which neural network can offer a better

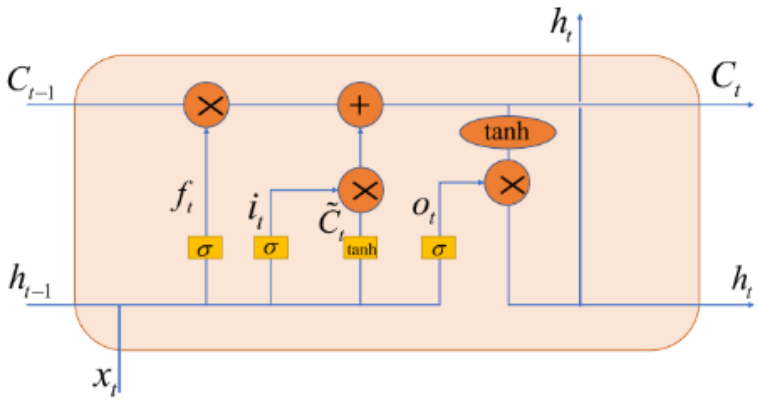


Figure 2.12: LSTM Architecture

performance according to the data available for its training.

2.6 An Effective Mechanism to Mitigate Real-Time DDoS Attack

2.6.1 Distributed Denial of Service

A DDoS attack is a malicious type of attack that sends mali- cious traffic to a specific node or a large number of nodes via a large number of distinct computers, which form part of a system (bot) that the attacker controls legitimately or not.

These compromised hosts send many packets to the target to flood the network and block services. The result of such an attack is that resources are overwhelmed handling illegitimate packets, and are unable to effectively deliver legitimate service requests. A DDoS attack becomes effective by utilizing the Internet to break into computers and utilizing them to attack a network.

These devices simultaneously transfer large number of packets without any break to some special victim who feels that these are original transmissions. For this, the host must communicate with many devices at the same time across the network with different type of packets.

2.6.2 The Protection Method

The protection method is designed based on traffic behavior analysis, packet header validation, used protocol validation and traffic matching with datasets. The protection method prevents the malicious traffic to reach the destination after analysis of network traffic for odd behavior or network abnormalities. This method works as an inline intrusion prevention system because it not only removes the malicious traffic by dropping it but also rerouting such traffic from the primary route to the secondary route for traffic redirection.

Every agent sends logs of every DDoS attacks to system controller for signature database and send SNMP trap to all devices with new ACL data, new iptable information and routing information. One of agent act as main controller gather all the attacks information and forward it as a solitary email to the network admin.

2.6.3 Implementation of the malicious network

The LOIC tool is placed in this framework for generating the malicious traffic as this provides the GUI and easy operating. It also has the capacity of generating the real-time traffic of TCP, UDP, and HTTP flood attacks which match the behavior of the DDoS profile.

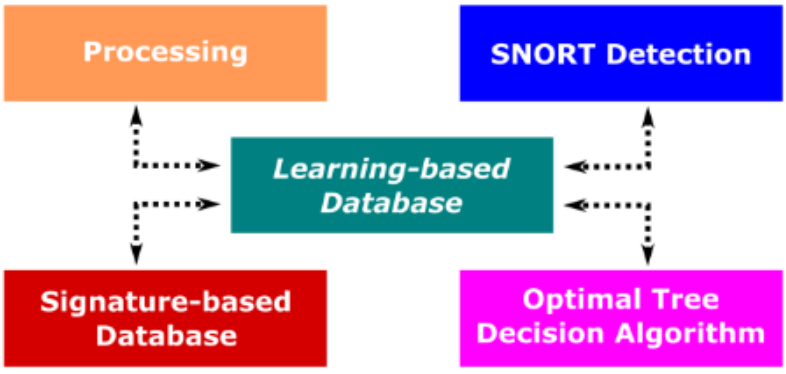


Figure 2.13: Learning mechanism of the proposed method

The three flooding attacks are used against the apache web server. The JMeter tool provides the GUI for generating the HTTP traffic with regular intervals of time as depends on several user threads selected. Using of datasets like DARPA and KDDCUP99 helped in generating the traffic.

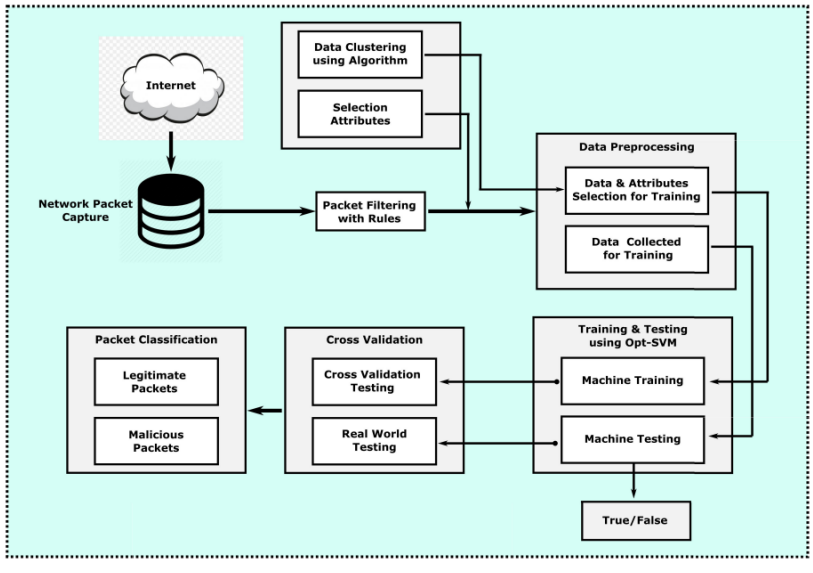


Figure 2.14: Deployment Architecture of the proposed method

2.6.4 Performance Evaluation

The proposed method performance is measured in terms of identification of attack (accuracy), detection rate (sensitivity) and false alarm rate (specificity) using different equations. The accuracy signifies the ratio of properly recognized results over the full data used by the proposed method or true negative results, while mistakenly recognized alarm are false positive and false negative results.

2.6.5 Results

The first phase of testing was legitimate traffic that seemed suspicious because of badly composed arrangement of snort rules. The second phase was represented as a case where an attacker made an attack on the network by LOIC tool for DDoS attack. The IPS obtained the best accuracy of 99%.

2.6.6 Conclusion

The proposed method goes far in lessening false positives without decreasing false negatives and opens a few ways of development that could additionally enhance the present systems of intrusion prevention. By learning from attacks instead of simply obstructing the attacker, it is conceivable that avoiding access to networks also helped in zero-day attack.

We utilized trained agents to recognize TCP, HTTP and UDP attacks utilizing the fundamental key examples that recognize genuine activity from DDoS attacks. A dump record of genuine network environment is utilized to begin the learning procedure. The zero day attack and multi-threading for packet processing are the only limitations of this method.

Chapter 3

Firewalls

3.1 Introduction

It is a computer element that tries to block access, to a private network connected to the Internet, to unauthorized users. Therefore, the firewalls focus on examining each of the messages that enter and leave the network to obstruct the arrival of those who do not meet certain security criteria, while giving free access to communications that are regulated. To clarify this concept, we will use a very simple metaphor: a firewall is to a computer network what a door to a house.

This door prevents the entry of unknown persons to our home in the same way that a firewall blocks the arrival of unauthorized users to a private network. The function of firewalls is very important, since, if not for it, a computer – or computer network – could be attacked and infected quite frequently. Some antivirus companies also offer additional firewall protection to improve the defense system and stop the entry and installation of malicious code.

3.2 Working

The main function of a firewall is to block any unauthorized access attempt to private internal devices of our data network (LAN) from the exter-

nal internet connections commonly called WAN. It provides a way to filter the information that is communicated through the network connection.

A firewall that is meant for an individual computer is called a Personal Firewall. When firewalls are present in an enterprise network for the protection of multiple computers, it is called a Network Firewall. It allows or blocks communication between teams based on rules.

Each rule defines a certain network traffic pattern and action to perform when detected. These customizable rules provide control and fluency over the use of the network. If traffic complies with the configured rules in firewalls, traffic can enter or leave our network. If not, then the traffic will be blocked and cannot reach its destination.

3.3 Firewall Architectures

3.3.1 Packet filtering routers firewall architecture

Many of the organization want the internet connectivity. If we enable internet connectivity, the organization without a firewall will be exposed to the external world. To avoid an external security attack, we need to install and configure the firewall. In the packet filtering routers, we have the router concept. Here, the router interface acts as the internet provider to the organization. The router is acting as an intermediate between the organization and the internet provider. On the same level, we are enabling the network packet filtering process.

If any unwanted packets may come, so it will filter them out on the same level. Hence the packages will drop or be rejected. It will not come in the organization level network. It is a very simple way to implement it. It

will also help to lower the risk from external security threats. But it has few concerns also. If we go with the packet filtering routers, then it will be less auditing on the network traffic. Similarly, we are also having the drawback of the strong authentication mechanism also. Day by day, the access control list will grow. Hence, it will be a very big overhead to filter the incoming network packets. Due to which it will decrease the network performance also. In few cases, we will face the lag.

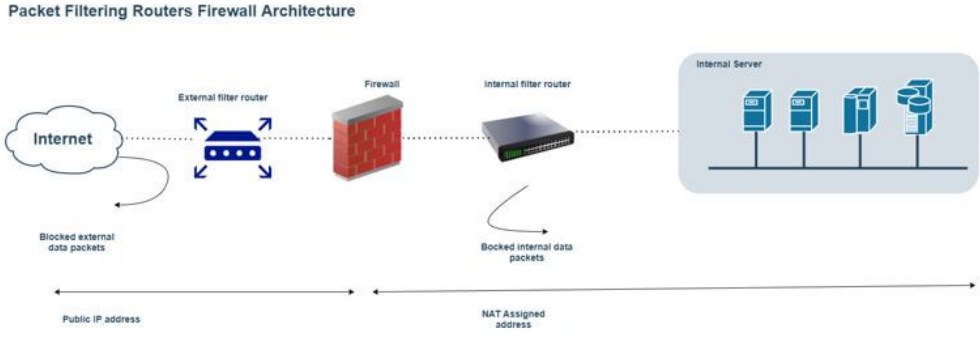


Figure 3.1: Packet Filtering Routers Firewall Architecture

3.3.2 Screened Host Firewall Architecture

In this architecture, we are using the packet filtering routers firewall technique with the dedicated or the separate firewall. It is known as the application proxy server. In the packet filtering router's firewall architecture, we have a very big overhead to filter the network traffic (once the access control list increases). Due to this, we are facing lots of issues. Here, we have tried to overcome it, and we have added the dedicated firewall. This technique will allow the router to the firewall. Due to this architecture, the routers will pre-screen the network traffic or the packets to minimize the network overhead. It will also help to distribute the load as well.

The separate application proxy server will work on layer 7 (on the TCP protocol). It will filter the packets on the application level. It is having the capability to filter out the packets like HTTP, HTTPS, FTP, SFTP, etc. In other words, the separate application proxy server is also known as the bastion host also. It will be a high chance for an external attack, and it will be less secure also. The action host or the separate application proxy server is holding the cached copies of the web documents. But in this architecture, the external attacker needs to compromise the two different systems. Before doing any attack, it will access the internal data also.

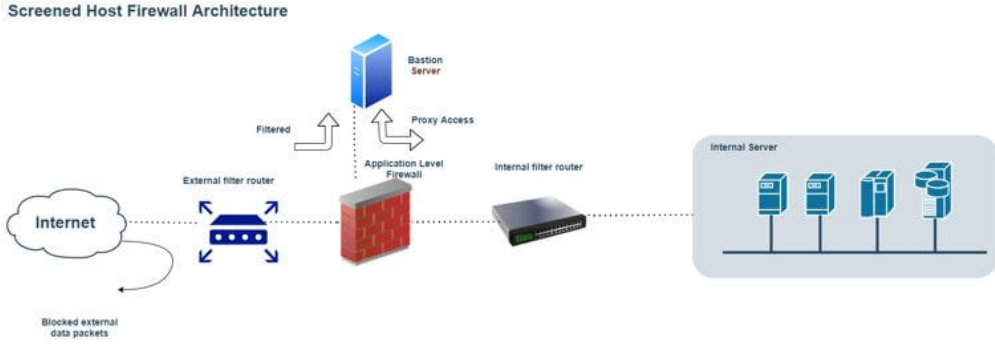


Figure 3.2: Screened Host Firewall Architecture

3.3.3 Work Flow Architecture

It is the basic technique to implement the firewall. Here, the ISP will provide an internet connection to the organization. Then, it is attached to the external filter router. First, on the firewall, we need to add the list of ACL's and configurations. Then, with the help of the same configuration, the network traffic will filter and pass to the internal filter router. Further, the internal filter router will separate out the network traffic into the internal organization-level network.

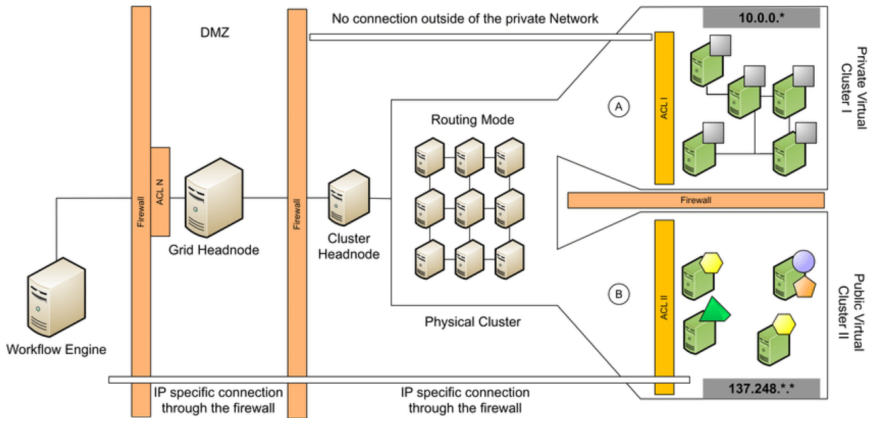


Figure 3.3: Work Flow Architecture

3.4 Types of Firewalls

3.4.1 Based on Physical Parameters

There are 2 types of Firewalls: Hardware and Software Firewall.

Hardware devices are an excellent solution in case we have to protect an enterprise network since the device will protect all the computers in the network and we can also perform the entire configuration at a single point that will be the same firewall. In addition to this, these hardware firewalls implement interesting features such as CFS, offering SSL or VPN technologies, integrated antivirus, antispam, load control, etc.

Software types are the most common and the ones used by home users in their homes. The software types are installed directly on the computers or servers that we want to protect and only protect the computer or server on which we have installed it. The functionalities that software firewalls usually provide are more limited than hardware firewalls, and once installed, the software will be consuming resources from our computer.

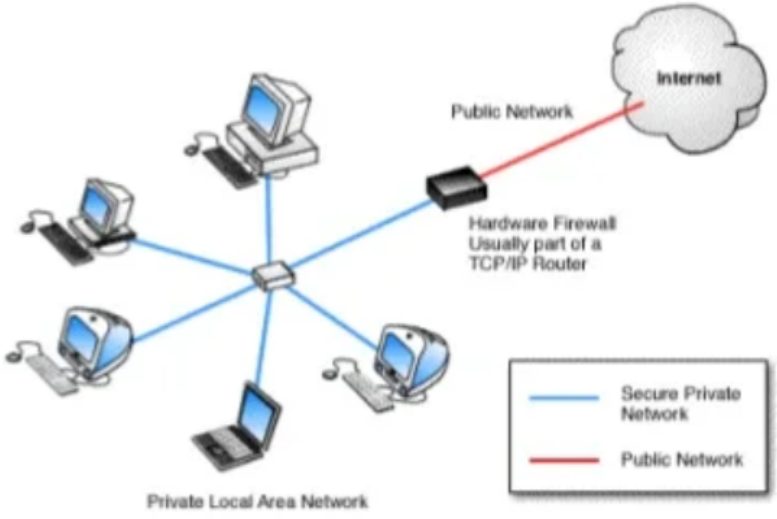


Figure 3.4: Hardware Firewall Architecture

3.5 Based on Detection Scope

Firewalls can be divided on the basis of the types of network it filters and the scope at which its action is significant. They can be: Web Application, Network Segmentation, Database, Cloud Based and Next Gen Firewalls.

3.5.1 Web Application Firewalls

A firewall for the web application is typically a proxy server between an application on a server and the users of an application that accesses the app from outside the corporate network. The proxy server takes input data and then creates a connection on behalf of the internal client with the request. A major advantage of this configuration is that the database is protected from port checks, attempts to locate the application server code or other malicious behavior driven by end-users. The proxy server also analyzes the data to prevent them from reaching the database for web apps to filter

malicious requests.

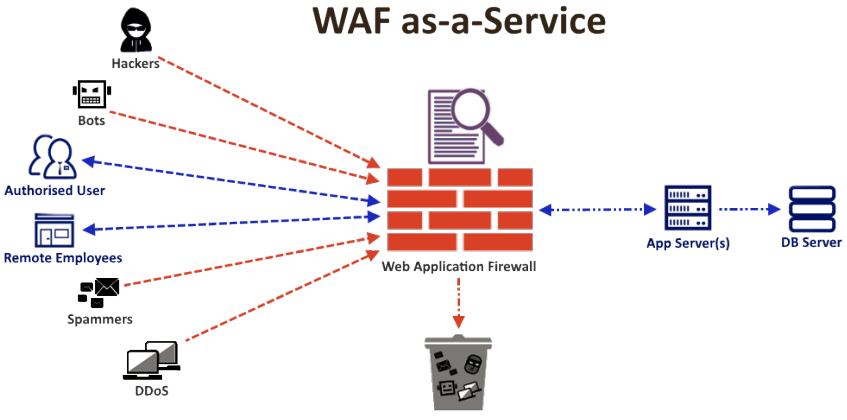


Figure 3.5: Web Application Firewall

Level of Protection: High because the web application server offers a buffer for unidentified and potentially malicious users who could otherwise have direct access to the Web application server. This is important because many applications carry secret data valuable to hackers that are particularly attractive in Web-facing applications.

Weaknesses and Strengths: Web application firewalls are simpler, less vulnerable, and easier to patch than web servers themselves. This means that hackers can consider applications behind the firewall substantially difficult. But proxy firewalls do not support all applications easily and can reduce the safe application performance for end-users.

3.5.2 Database Firewall

As its name implies, firewalls are a type of firewall for Web applications designed to protect databases. These are usually installed right onto the server of the database (or near to the network entry, where more than one

server has several servers designed to protect them). They aim to identify and avoid unique server attacks, such as cross-site scripts, which can lead to confidential information in databases accessed by attackers. Level of

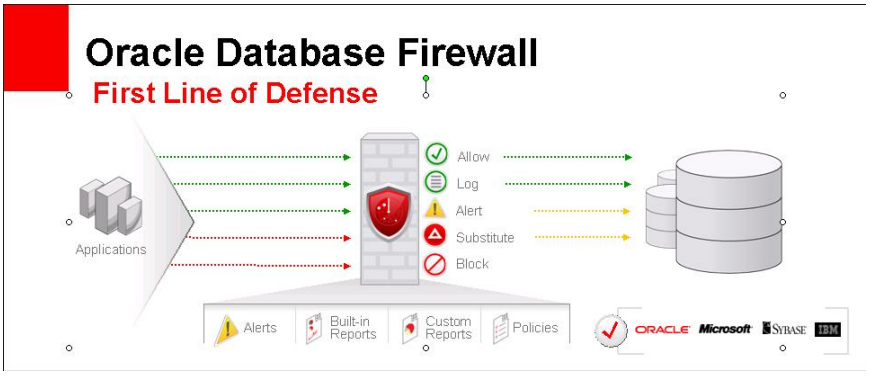


Figure 3.6: Database Firewall

Protection: The loss of confidential information is usually expensive and costly regarding lost credibility and poor ads. For this purpose, all appropriate steps are needed to protect the databases and their data. To the security of these stored data, a network firewall was added considerably.If you keep valuable or confidential database data, it is highly recommended that a firewall be used. According to Risk-Based Security, more than 4 billion records were stolen, four times higher than in 2013. When hackers continue to target databases effectively, this means that records are increasingly important.

Strengths and Weaknesses: Server firewalls can provide an effective security measure and can also be used to track, review and report compliance for regulatory purposes. However, only if configured and modified correctly and offer little protection from zero-day exploits will they be effective.

3.6 Network Segmentation Firewall

A firewall for network segmentation (we can also say says internal network firewalls) is used to manage network traffic flows between locations, operational areas, divisions, or other business units. It is applied at subnet limits. In this way, there can be a network breach in one area and not throughout the network. It can also protect areas of the network that it guarantees, such as databases or research and development units. For very big companies or companies with network perimeters that are difficult to secure, network segmentation firewalls are most helpful.

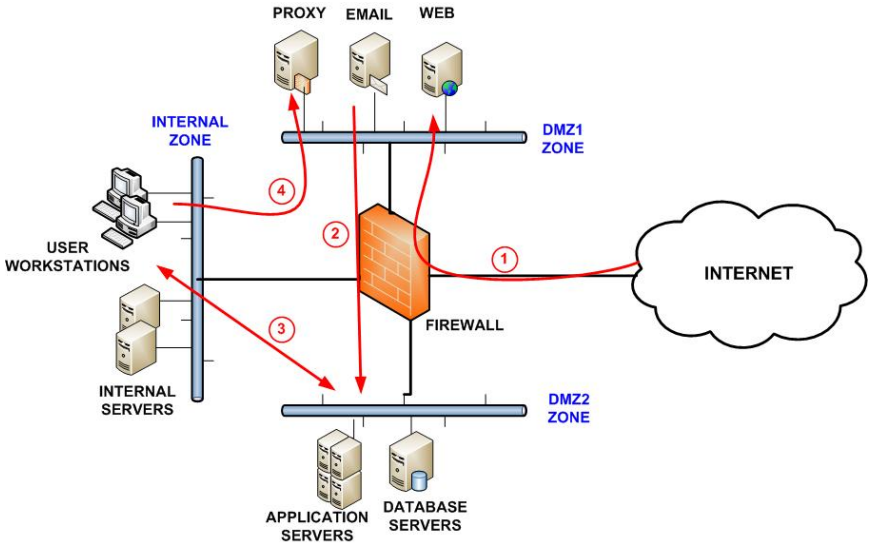


Figure 3.7: Network Segmentation Firewall

Level of Protection: While an attacker may be unable to move a network segmentation firewall from part of a network to another, it can only slow the progress of an attacker in practice if the initial break is quick to identify.

Strengths and Weaknesses: If an aggressor achieves network access, then it can be significantly more difficult for a network segmentation firewall to

access particularly sensitive information.

3.7 Conclusion

This chapter defined a Firewall and its working involving datasets and rules. The types of Firewall are discussed along with the various architectures used.

Chapter 4

Intrusion Detection Systems : An Overview

An intrusion detection system (IDS) is a security tool that is designed to automatically monitor and analyze a computer network or system for malicious activities or policy violations. It is essentially a network security mechanism that can be used to identify unauthorized access, misuse, and other security threats, and alert the system administrator or security personnel so that appropriate action can be taken to protect the network.

An IDS typically uses one or more of the following methods to detect intrusions:

Firstly, Signature-based detection involves comparing the network traffic or system activities against a database of known intrusion signatures. If a match is found, the IDS raises an alert. Secondly, Anomaly-based detection establishes a baseline of normal behavior for the network or system, and then monitoring for any deviations from this baseline. If an anomaly is detected, the IDS raises an alert.

IDSs can be classified into two main categories: host-based and network-based. Host-based IDSs are installed on individual host machines, and are used to monitor and analyze the activities of those specific machines. Network-based IDSs, on the other hand, are installed on network devices,

such as routers and switches, and are used to monitor and analyze network traffic for signs of intrusions.

Overall, IDSs are an important security tool that can help protect a computer network or system from intrusions and other security threats. However, it is important to note that IDSs are not a perfect solution, and can sometimes generate false positives or false negatives. It is therefore important to use them in conjunction with other security measures, such as firewalls and anti-virus software, to provide a comprehensive security solution.

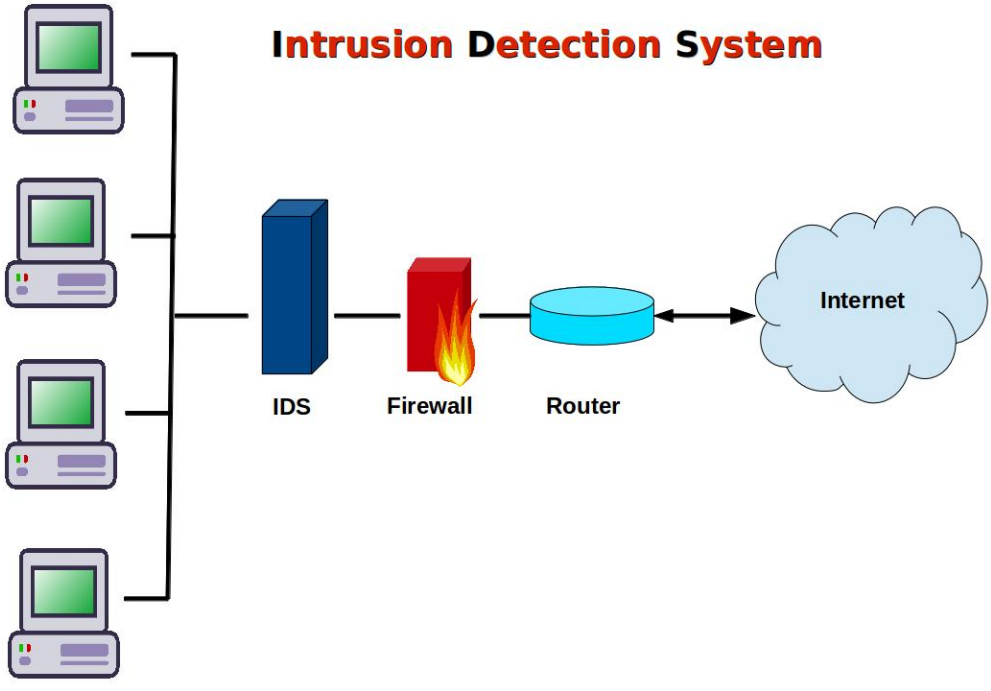


Figure 4.1: Intrusion Detection Systems

4.1 Intrusion Detection Systems Vs. Firewalls

Intrusion detection systems (IDS) and firewalls are both security tools that are used to protect computer networks and systems from unauthorized access and other security threats. However, there are some key differences between the two:

Firewalls are designed to prevent unauthorized access to a network or system by controlling the flow of network traffic based on predetermined security rules. In contrast, IDSs are designed to monitor and analyze network traffic or system activities for signs of intrusions or other security threats, and raise an alert if such activities are detected.

Firewalls are typically installed on network devices, such as routers and switches, and are used to protect the entire network. IDSs, on the other hand, can be host-based or network-based, and can be installed on individual host machines or on network devices.

Firewalls are primarily proactive in nature, in that they are designed to prevent unauthorized access to a network or system. IDSs, on the other hand, are primarily reactive, in that they are designed to detect intrusions

or other security threats after they have occurred, and then alert the system administrator or security personnel.

Firewalls are typically configured using predetermined security rules, which are used to control the flow of network traffic. IDSs, on the other hand, can use different methods to detect intrusions, such as signature-based detection, anomaly-based detection, or stateful protocol analysis.

Overall, firewalls and IDSs are complementary security tools that can be used together to provide a comprehensive security solution for a computer network or system. While firewalls are effective at preventing unauthorized access, IDSs can help detect and respond to security threats that manage to bypass the firewall.

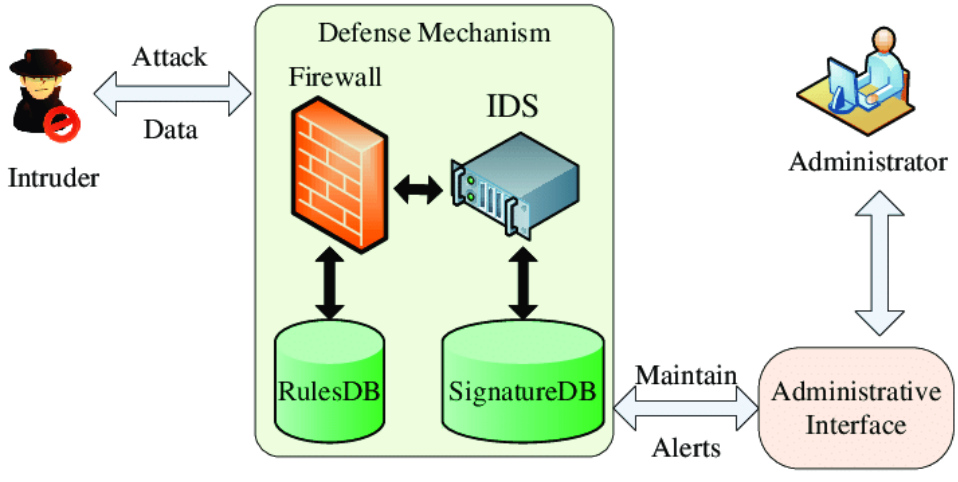


Figure 4.2: NIDS + Firewall

4.2 Architecture model of Intrusion Detection Systems

The architecture of an intrusion detection system (IDS) typically consists of sensors,analysis engine, database, and a management console. Sensors are responsible for monitoring network traffic or system activities. Analysis engine analyzes the data collected by the sensors, and identifying potential security threats. Database stores the information collected by the sensors, as well as the rules and signatures used by the analysis engine to detect intrusions. For example, CIC-IDS 2017, CIC-DDoS 2018, KDD CUP 99', NSL-KDD 2015 etc. Management console is used by the system administrator or security personnel to configure, monitor, and manage the IDS.

Overall, the architecture of an IDS is designed to provide a flexible and scalable solution for monitoring and analyzing network traffic or system activities for signs of intrusions or other security threats. The specific components and configuration of an IDS may vary depending on the specific requirements and environment of the network or system being protected.

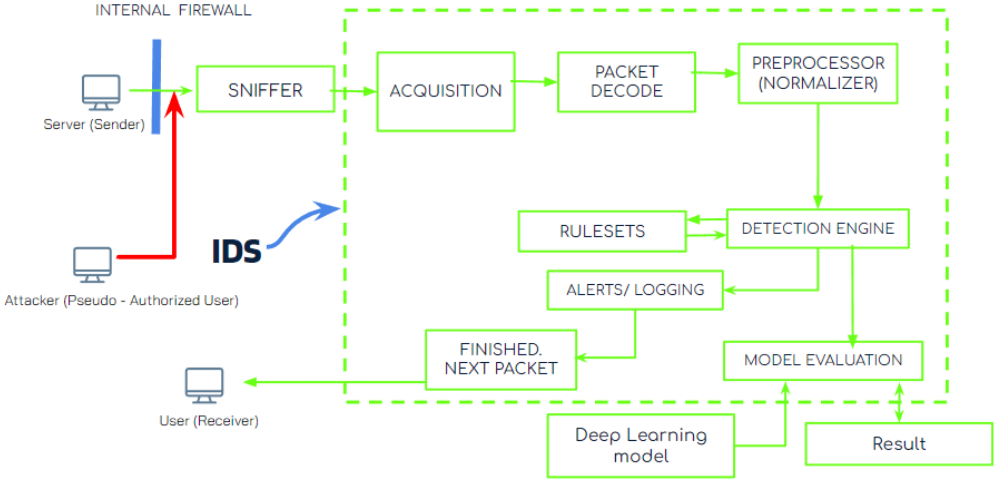


Figure 4.3: Network Intrusion Detection system Architecture

4.3 Deep Learning Model Architecture

In an Intrusion Detection System (IDS), a neural network deep learning model can be used to improve the accuracy and effectiveness of the IDS in detecting security threats.

The architecture of a neural network deep learning model for intrusion detection typically consists of a input layer which receives the input data, such as network traffic or system activities, that the deep learning model will use to learn and make predictions.Next, hidden layers are responsible for learning the patterns and relationships in the input data. The number of hidden layers and the number of neurons in each layer can be adjusted to optimize the performance of the model. Thirdly, an Output layer which produces the final predictions made by the deep learning model. In the context of intrusion detection, the output layer might produce predictions of whether a particular network traffic or system activity is malicious or benign. Finally, the activation functions are the mathematical functions that are used to process the input data and generate the predictions made by the deep learning model. Different activation functions can be used in different layers of the neural network to optimize the performance of the model.

Overall, the architecture of a neural network deep learning model for intrusion detection is designed to enable the model to learn complex patterns and relationships in the input data, and use that knowledge to make accurate predictions of potential security threats. The specific architecture and configuration of the model may vary depending on the specific requirements and environment of the network or system being protected.

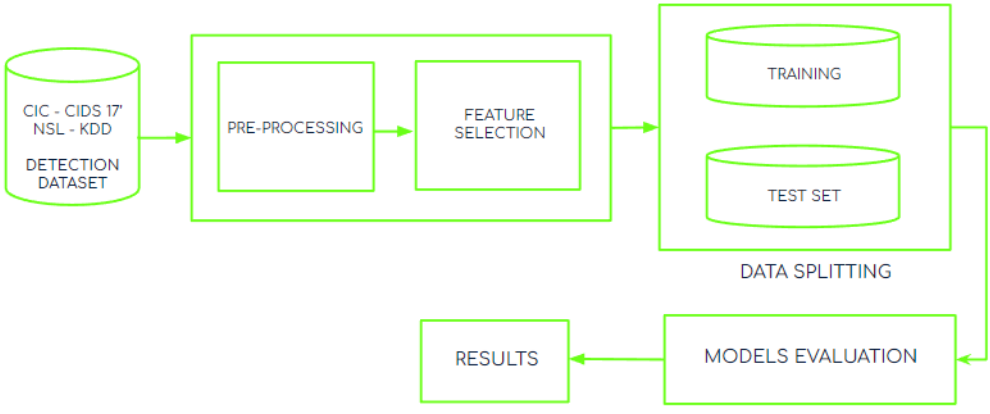


Figure 4.4: Deep Learning model Architecture

Chapter 5

SNORT: A Real-Time Intrusion Detection System

SNORT (Simple Network Over Real-Time) is an open-source intrusion detection system (IDS) that is used to monitor network traffic and identify potential security threats. SNORT uses a combination of signature-based and anomaly-based detection techniques to identify malicious activity on a network.

Signature-based detection involves matching the traffic on a network against a known set of "signatures" or patterns that are associated with known security threats. For example, if SNORT is configured to look for a particular type of malware, it will use a signature for that malware to identify any instances of it on the network.

Anomaly-based detection involves analyzing the traffic on a network and identifying patterns that are unusual or unexpected. For example, if SNORT detects a large number of connections to a single IP address, it might flag this as potential malicious activity.

SNORT is often used in combination with other security tools, such as firewalls and intrusion prevention systems (IPS), to provide a comprehensive security solution. It can be configured to alert administrators to poten-

Figure 5.1: SNORT NIDS

tial security threats, or to take automatic action, such as blocking network traffic or quarantining infected systems.

Overall, SNORT is a powerful and versatile intrusion detection system that can be used to monitor and protect networks from a wide range of security threats. It is widely used by organizations of all sizes, and its open-source nature allows for community-driven development and customization.

5.1 SNORT modes

SNORT can be run in three main modes: sniffer mode, packet logger mode, and network intrusion prevention system (NIPS) mode.

5.1.1 Sniffer Mode:

In sniffer mode, SNORT analyzes network traffic in real-time and alerts administrators to potential security threats. This mode is useful for detect-

ing and responding to security threats in real-time, as it allows administrators to take action as soon as a threat is detected.

5.1.2 Packet Logger Mode:

In packet logger mode, SNORT logs network traffic for later analysis. This mode is useful for reviewing network traffic after the fact and identifying potential security threats that may have been missed in real-time. It is also useful for analyzing large amounts of network traffic that would be impractical to process in real-time.

5.1.3 Network Intrusion Prevention System Mode:

In NIPS mode, SNORT actively blocks network traffic that it identifies as malicious. This mode is useful for providing an additional layer of protection against security threats, as it prevents potential threats from reaching their intended targets.

5.2 Conclusion

Overall, the three modes of SNORT provide different capabilities and can be used in different situations depending on the specific needs and requirements of the organization. Sniffer mode is best for detecting and responding to security threats in real-time, packet logger mode is best for offline analysis and review of network traffic, and NIPS mode is best for providing an additional layer of protection against security threats.

Chapter 6

Concluding remarks

6.1 Conclusion

The seminar dealt with Intrusion Detection Systems (IDS). Network IDS is used to monitor the network for malicious packets and abnormal activities within the network.

The various features of the Intrusion detection System is that it provides a 2 step defense mechanism, traffic monitoring and anomaly detection. The seminar discusses the benefits of an Intrusion detection System network than a enterprise firewall. SNORT is a IDS/IPS. The seminar covers the 3 SNORT modes and their applications.

Finally, the seminar concludes by citing the architecture of the Deep Learning model and the Network Intrusion Detection System.

References

[1] Asma Halbouni, Teddy Surya Gunawan, Mohamed Hadi Habaebi, Mira Kartiwi and Robiah Ahmad, *"Machine Learning and Deep learning Approaches in Cybersecurity"*, IEEE Access Vol. 10; 2022.

[2] Syed Ali Raza Shah, Biju Issac, *"Performance comparison of intrusion detection systems and application of machine learning to Snort system"*, Future Generation Computer Systems Vol. 80, Science Direct; 2018.

[3] Felix Erlacher, Falko Dressler, *"On High-Speed Flow-Based Intrusion Detection Using Snort-Compatible Signatures"*, Transactions on Dependable and Secure Computing, IEEE Access Vol. 19, No. 1, 2022.

[4] Aechan Kim, Mohyun Park, and Dong Hoon Lee, *"AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection"*, Scalable Deep Learning for Big Data, IEEE Access Vol. 8; 2020.

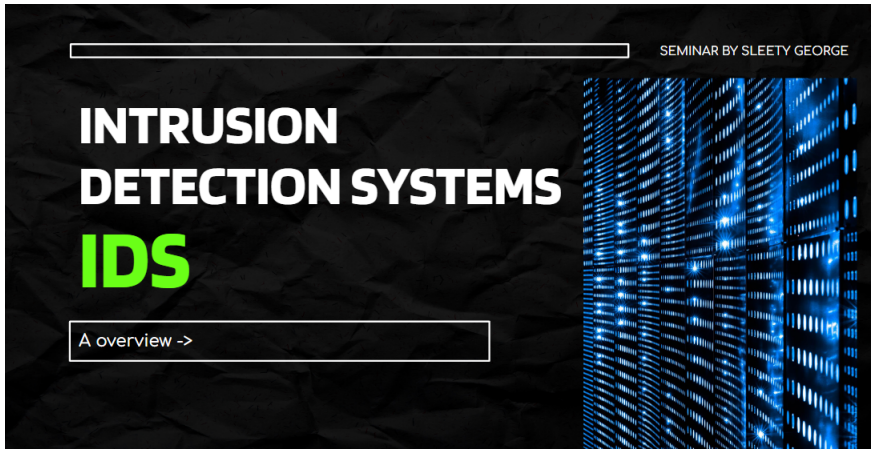
[5] Xavier A. Larriva-Novo, Mario Vegabarbas, Victor A. Villagra, and Mario Sanz Rodrigo, *"Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies"*, Emerging Approaches to Cyber Security, Vol. 8, IEEE Access; 2020.

[6] Rana Abubakar, Abdulaziz Aldegheishem, Muhammad Faran Majeed, Amjad Mehmood, Hafsa Maryam, Nabil Ali Alrajeh, Carsten Maple,

and Muhammed Jawad, *"An Effective Mechanism to Mitigate Real-Time DDoS Attack"*, IEEE Access, Vol.8, 2020.

[7] *"https://resources.infosecinstitute.com/topic/firewalls-and-ids-ips/"*,Oct 5, 2020.

Appendix A


SEMINAR BY SLEETY GEORGE
INTRUSION
DETECTION SYSTEMS
IDS
A overview ->
MAIN QUESTION: WHAT IS IDS?
• IDS is a passive monitoring solution for detecting possible malicious activities/patterns, abnormal incidents, and policy violations.
• It is responsible for generating alerts for each suspicious event.

WHAT MAKES HAVING AN IDS BETTER?

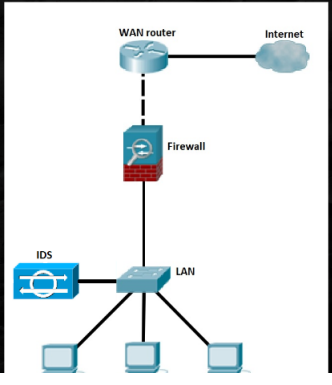
01 2 STEP DEFENSE

02 TRAFFIC MONITOR

03 ANOMALY DETECTION

SEMINAR BY SLEETY GEORGE

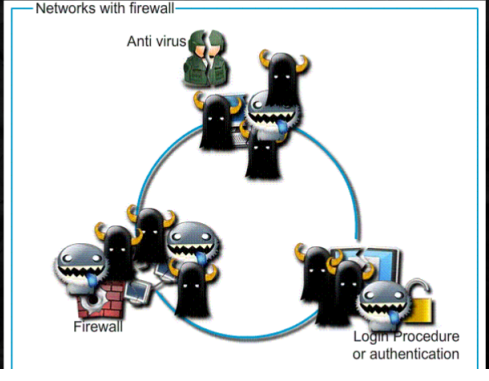
01 2 STEP DEFENSE



SEMINAR BY SLEETY GEORGE

WHAT HAPPENS WITHOUT AN IDS?

- CAN BE VULNERABLE TO INLINE FLOODING, ZERO TRUST, DDoS ATTACKS.



HOW ITS DONE IDS | IPS

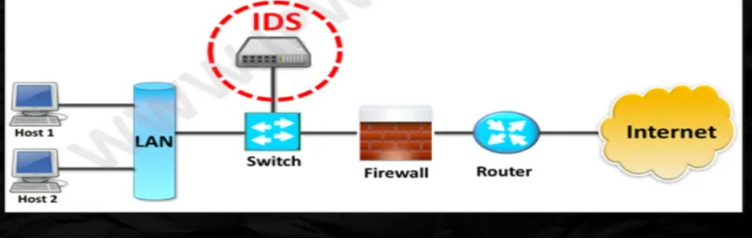
1. A NETWORK WITH FIREWALL ONLY

HOW ITS DONE IDS | IPS

2. A NETWORK WITH A IPS AND FIREWALL

HOW ITS DONE IDS | IPS

3. A NETWORK WITH A IDS AND FIREWALL



SEMINAR BY SLEETY GEORGE

02

TRAFFIC MONITOR

FORTINET

at&t

LET'S TALK ABOUT SNORT....

WHAT IS IT?

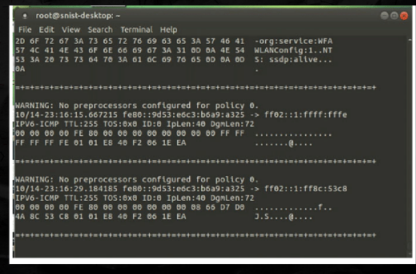
SNORT is an open-source, rule-based Network Intrusion Detection and Prevention System (NIDS/NIPS). It was developed and still maintained by Martin Roesch, open-source contributors, and the Cisco Talos team.

SNORT MODES

- SNIFFER MODE
- PACKET LOGGER MODE
- IDS MODE

1. SNIFFER MODE

Sniffer mode or verbose mode sniffs all packets in the network and retrieve information about them for the user.



2. PACKET LOGGER MODE

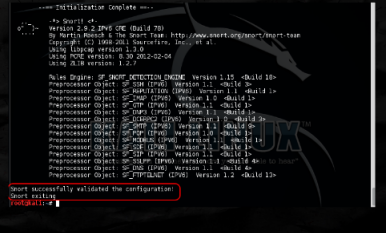
Here, SNORT logs all the packets in the network within a configuration file under the libpcap library. This log file can be read by wireshark/tcpdump.

```
root@debian:~# ls /var/log/snort/
alert  snort.log.1365405855  tcpdump.log.1365404187
root@debian:~#
```

3. IDS MODE (ATTACK MODE)

SNORT is a open source, full blown INTRUSION DETECTION SYSTEM/ INTRUSION PREVENTION SYSTEM.

Attack mode that acts as a inline firewall but better, it acts on the basis of a admin configured set of rules , which when violated turns the entire system offline and send alerts to the users about a suspicious or malicious activity.



SEMINAR BY SLEETY GEORGE

03 ANOMALY DETECTION

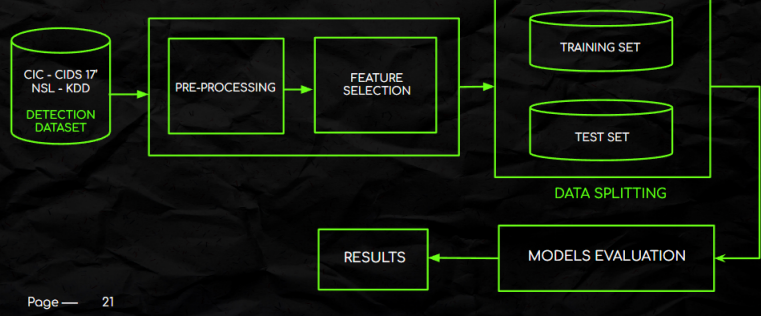
FIREWALL

- A FIREWALL EMPLOYS RULES TO FILTER INCOMING AND OUTGOING NETWORK TRAFFIC.
- IT USES IP ADDRESSES AND PORT NUMBER TO FILTER TRAFFIC.
- FIRST LINE OF DEFENSE AND SHOULD BE INSTALLED IN THE NETWORK PERIMETER.

IDS

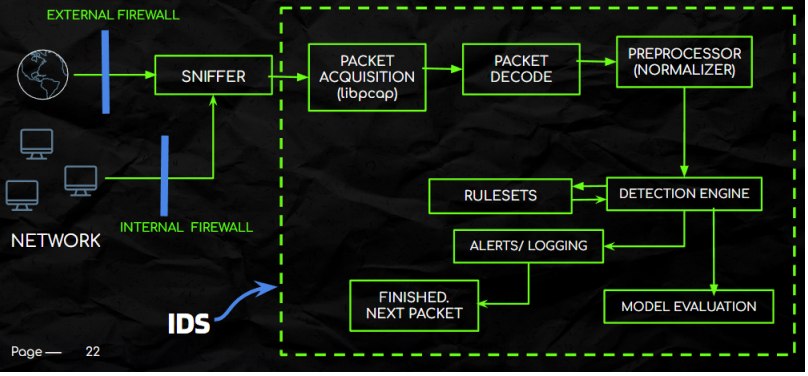
- IDS ANALYZES INCOMING NETWORK TRAFFIC FOR MALICIOUS ACTIVITIES OR POLICY BREACHES AND ISSUES ALERTS WHEN THEY ARE DETECTED.
- DETECTS REAL TIME TRAFFIC AND SEARCHES FOR ATTACK SIGNATURES OR TRAFFIC PATTERNS, THEN SENDS OUT ALARMS.
- SECOND LINE OF DEFENSE AND SHOULD BE INSTALLED WITHIN THE NETWORK.

ARCHITECTURE OF INTRUSION DETECTION SYSTEMS (DEEP LEARNING MODEL)



Page — 21

ARCHITECTURE OF INTRUSION DETECTION SYSTEMS



Page — 22

REFERENCES

PAPERS

- ASMAA HALBOUNI, TEDDY SURYA GUNAWAN, MOHAMED HADI HABAEBI, MIRA KARTIWI, AND ROBIAH AHMAD : MACHINE LEARNING AND DEEP LEARNING APPROACHES FOR CYBERSECURITY: A REVIEW , *IEEE ACCESS VOL 10*, (FEBRUARY, 2022)
- FELIX ERLACHER, AND FALKO DRESSLER: ON HIGH SPEED FLOW BASED INTRUSION DETECTION USING SNORT COMPATIBLE SIGNATURES, *IEEE VOL 19* , (FEBRUARY, 2022)
- RANA ABRAHAM, ABDULAZIZ ALDEGHEISHEM, MOHAMMAD FARAN MAJEED, AMJAD MEHMOOD, NABIL ALI ALRAJEH, CARSTEN MAPLE, AND MOHAMMED JAWAD: AN EFFECTIVE MECHANISM TO MITIGATE REAL TIME DDoS ATTACKS, *IEEE ACCESS VOL 8*, (JULY, 2020)

REFERENCES

SITES

- https://fortinet.com/blog/threat-research
- https://tryhackme.com/room/snort
- https://study-ccna.com/firewalls-ids-ips-explanation-comparison
- https://learningnetwork.cisco.com/s/question/0D53i00000KsuxDCAR/cisco-idsips-fundamentals
- https://resources.infosecinstitute.com/topic/firewalls-and-ids-ips/