Indian Journal of Science and Technology, Vol 10(20), DOI: 10.17485/ijst/2017/v10i20/108940, May 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Analysis of Various Intrusion Detection Systems with a Model for Improving Snort Performance

Ravi Teja Gaddam* **and M. Nandhini**

Department of Computer Science, Pondicherry University, Puducherry - 605014, India;
raviteja.csebec@gmail.com, mnandhini2005@yahoo.com

Abstract

Objectives: To assess various Intrusion Detection Systems (IDS) against various types of attacks in different environments like Web, Enterprise, Cloud, etc. and to propose architecture for improving the Snort based IDS performance during typical attacks. **Methods:** Analytical approach was used to survey various research papers in this field of research. **Findings:** In this research, various approaches of IDS were analysed in various aspects like Detection Accuracy, False Alarm Rate, Scalability and Capability of detecting unknown attacks. Some approaches focused on particular type of issues while ignoring the others. This lead to performance degrading in several cases which is not tolerable in real time scenarios. **Improvements:** Among various studied approaches, we chose Snort based IDS to improve its performance in order to deploy in enterprise networks. Being an Open Source Software, Snort gives the flexibility to improve its functionality. We propose architecture to improve Snort's detection rate and to reduce the packet drops during critical attacks like Port Scanning, DoS, DDoS Attacks, etc.

Keywords: Attacks, DoS Attacks, DDoS Attacks, Detection Accuracy, False Alarm Rate, Intrusion Detection System, Open Source Software, Port Scanning Attacks, Snort, Scalability

1. Introduction

One of the major issues for today's enterprise networks is security. Many reputed company networks and Internet based services were bring down with several successful attacks by the hackers. To protect the network infrastructure and Internet based communication, several techniques have been developed. The use of firewalls, cryptography and virtual private networks are some of them. Detecting intruders is a comparatively new to such techniques. Intrusion detection techniques can be used to collect the information from known attacks and find out if anybody tries to attack host or network. This technique can be used to strengthen the network security. To protect from various attacks, security system can be set of tools, including:

- Firewalls to block malicious traffic of data.
- IDS to detect unauthorized activity to get into the system or network.
- Vulnerability assessment tools to find security breaches in the network. Information collected from these tools is used to define rules on firewalls to thwart security breaches from intruders.

This paper focuses on IDS because it emphasizes on the restriction of unauthorized access to the enterprise networks.

1.1 Intrusion Detection System (IDS)

Main usage of IDS is to detect malicious activities either at the network level or at the host level or at both[1]. IDS can be software, hardware or combination of both. An IDS may have various capabilities based on the complexity of components. Based on the network topology, IDS can put at one or more places. Type of intrusion actions like intra, inter or both can be monitored. If wish to monitor only external traffic and have only on entry point into our network then best place for IDS is inside the firewall.

*Author for correspondence

If network has multiple entry points then placing IDS at every point gives more security. If wish to detect internal activities then place IDS in every network. In general placing IDS in all network segments is not necessary and can limit it only to sensitive networks. It is obvious that more IDS mean more work and more maintenance costs. Figure 1 shows different locations to place IDS.

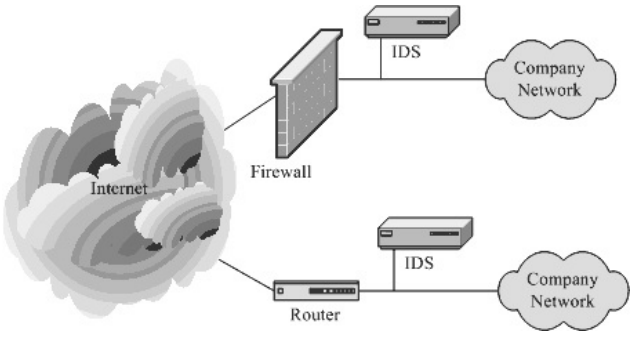

Figure 1. Placement of IDS.

IDS can be classified as: Signature-based and anomaly-based. Similar to computer viruses, intruders also have signatures that can be detected using IDS. It tries to search for packets that contain any known intrusion-related signatures or anomalies related toprotocols. Based on a set of signatures and rules, the IDS can detect and make a log of suspicious activities and generate alerts. On the other side anomaly-based depends on packet anomalies present in protocol headers. In certain contexts, Anomaly-based can give better performance compared to the signature based. In general, IDS detects the anomalies by applying rules to the data captured from network.

IDS can be Network based (NIDS) or Host based (HIDS). NIDS scans network data for malicious activity whereas HIDS detects attacks targeted to a particular system.

NIDS is liable for detecting anomalous and unauthorized activity in a network[1]. As shown in Figure 2, it captures packets on a network segment. Most NIDS are pattern based and require signature to alert the attack, or a set pattern in the payload.

HIDS resides on the host and scans activities[1]. Normally, it scans the log files of Operating System, Applications, or DBMS for the traces of activities. This means it fully depends on the log files. Hence, if the log data corrupted or manipulated by the attacker then HIDS will not able to detect the attack.

To understand various techniques and problems in the real time scenarios, this paper analyses various approaches of IDS. All the papers are categorized based on their working functionality, i.e. with Snort and without Snort. Snort[2] is an open source NIDS created by Martin Roesch in 1998.

Being an Open Source IDS, Snort can be easily configured and deployed in any environment. To overcome the challenges with Snort this paper proposes architecture. To evaluate the improved Snort, offensive Operating System Kali Linux[3] environment can be used.

This paper is organized as follows: Section 2analyses various techniques of IDS from several papers followed by their performance comparison in Section 3. Section 4 gives an overview about Snort and its functionality followed by its limitations. Section 5 discusses potential directions of this paper by discussing some typical attacks followed by the proposal. In Section 6, we make a conclusion and discuss about future work.

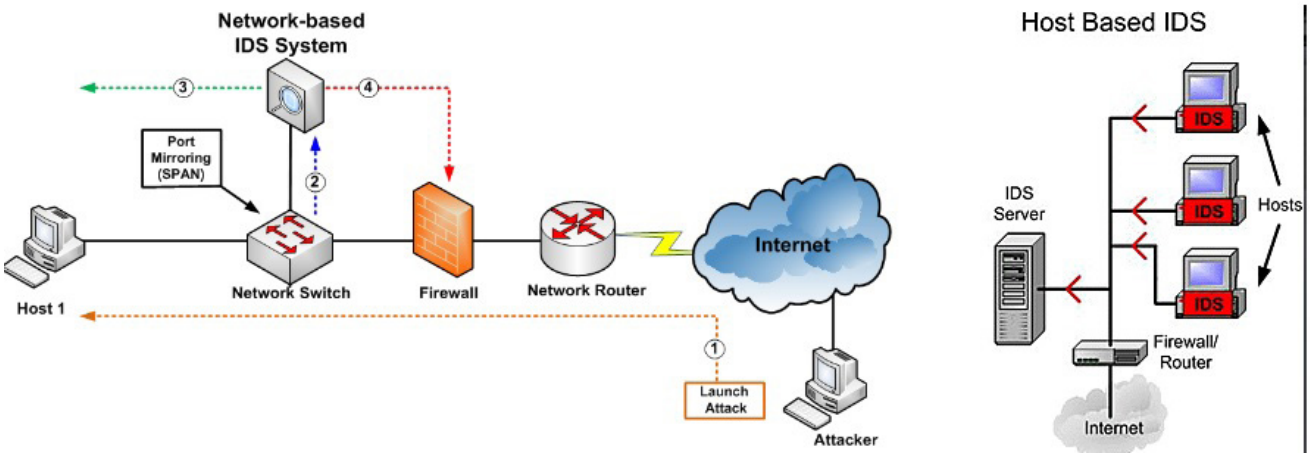

Figure 2. NIDS and HIDS.

2. Analysis of Existing Research Papers

This section discusses several research papers in the field of NIDS. The tree structure shown Figure 3 gives a schematic view of the research papers we took for analysis. All the papers are categorized based on their working functionality i.e., with and without Snort. Each sub-node of a particular domain gives the information regarding discussed paper and the approach used by the authors in that paper for intrusion detection.

2.1 Snort based NIDS

2.1.1 Data Mining Approach

Author in[4] proposed Behavior-Based Rules for Snort based on Bayesian Network Learning Algorithms. Here packets were captured using another tool called Wireshark and these packets were used to form Bayesian Network. Then created Snort rules based on behavior-based network traffic and concluded that the performance will be improved. One of the drawbacks identified is, it is based on rules. So it requires more rules to increase detection rate. Another drawback is it uses Bayesian Search Graph Algorithm, which checks several times for highest scoring graph.

2.1.2 Cloud Computing Approach

Authors of[5] discussed about the Intrusion Detection in Cloud based environment. This paper discussed various research works in this area and proposed a Smart Intrusion Detection Model based on virtual machines. To detect the malicious activities at virtual machines level, authors proposed a security tool named Smart Host based Intrusion Detection System (SHIDS). Each virtual machine equipped with OS software, User software and SHIDS. Architecture of SHIDS mainly consists of logger, IDS database and Data Mining Engine. Authors proposed architecture of centralized IDS for Cloud environment based on the principle of collaboration between many SHIDS deployed on different virtual machines.

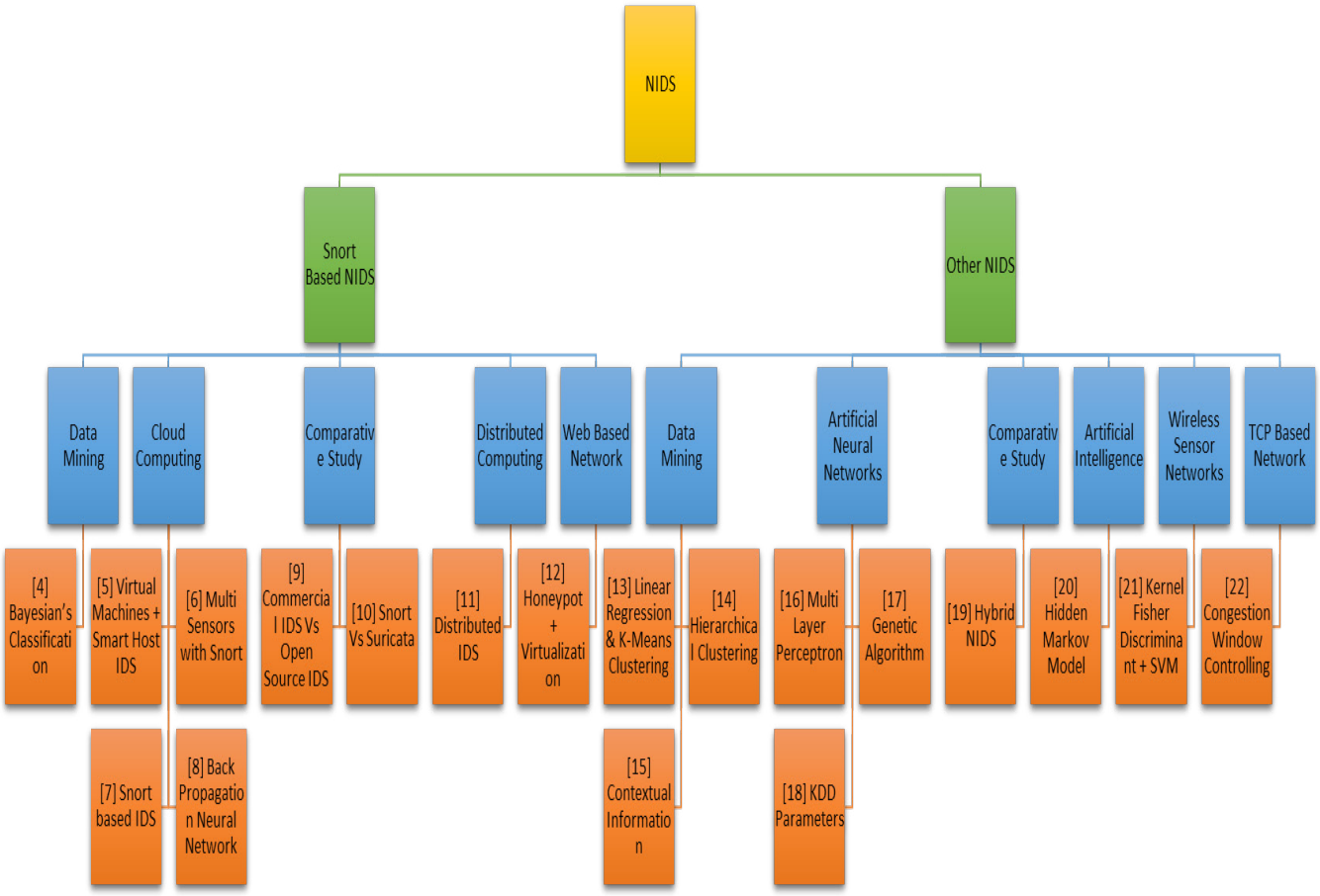

Figure 3. Schematic view of surveyed papers.

For experimental purpose, authors created three virtual machines, attacked on one virtual machine and resulted in transmitting this information to the centralized IDS virtual machine.

Author in[6] discussed about Intrusion Detection in private Cloud system. They proposed to improvise the Snort rules and multi-sensors for better behavior detection in private cloud. Authors proposed major rules for Snort like port scanning, behavior checking operating system, etc. For experimentation purpose this paper used virtual machines with roles like sensors, attackers, database and monitoring and running on Ubuntu and Windows OS. To evaluate the performance, authors used MIT-DARPA 1999 data set and Nmap. During testing different results identified at different sensors. Major drawback identified is preparing rules for every sensor and coordinating all sensors for better detection rate.

In[7], authors discussed about using Snort as IDS in Cloud Computing. This paper discussed the functionality of Snort and it's implantation in Cloud as a part of central administration. By modifying the snort.conf file, authors analysed the two modes functionality i.e. signature based and behavior based working of Snort. Major drawback identified is that the authors not suggested any special methods to overcome the limitations of Snort like packet loss and low detection rate during high traffic.

In[8] discussed about detecting attacks in Cloud environment by combining Snort and Back-Propagation Neural Network (BPN). To detect known attacks this paper used Snort and BPN for unknown attacks. By considering the weaknesses of BPN like slow detection speed, low detection accuracy, etc. Authors proposed an optimization algorithm to improvise BPN detection rate. Framework proposed is based on both signature based and anomaly based. This paper emphasizes on detecting Dos attacks but not concluded how the framework can efficiently prevent DoS and DDoS attacks and share this information among other IDS that are in the Cloud.

2.1.3 Comparative Study Approach

In[9], authors compared IDS that are available as commercial and open source. This paper describes the commercially available CISCO Adaptive Security Appliance (CASA). CASA uses Modular Policy Framework and it uses a CISCO catalyst switch to prevent attacker to communicate with Internet Service Provider. On the other hand authors described the usage of Snort as on open source firewall. Experimental results shows that both commercial and open source IDS can detect the attacks in different aspects. Several parameters like networking, configuration of device and price can play a major role while choosing the IDS. But when comes to reliability, commercial based IDS are much better than open source based IDS.

In[10] analysed the performance of two prominent open source Intrusion Detection Systems: Snort and Suricata. Authors discussed various features of both the systems like their capability, running modes, processing of packets, alerting, etc. According to this paper, Snort processing unit is single threaded whereas Suricata's is multi-threaded. It clearly states that Suricata has higher detection rate. However with great stability and good detection Snort has the bigger market share. To test both IDSs, authors used Security Onion Operating System and applied Host based IDS mode. Both Snort and Suricata run in two modes i.e., single and multi-threaded. Results are depicting that Suricata performance is better than that of Snort. From this it is clear that Snort needs enhancements in order to deploy in multi core environment to improve the detection rate.

2.1.4 Distributed Computing Approach

Authors of[11] focused on the problem of Distributed Denial of Service (DDoS) attacks and proposed a Distributed Intrusion Detection System. This paper explained various types of DDoS attacks that can occur at Network Layer, Transport Layer and Application Layer. For better detection of DDoS attacks, authors proposed a client-server architecture where IDS is deployed on each client. Experimental results showed that TCP Flooding was successfully detected and logged to server. Problem is deploying and configuring the IDS on each client and making them communicate in distributed environment.

2.1.5 Web Based Network Approach

In this paper[12], authors discussed about the IDSto detect attacker's activities using a proactive defence technique called Honeypot. Authors discussed various Honeypot based research papers and related in the field of research on decoys in different areas to combat the attackers. This paper proposed a virtualization technique to overcome the security problem. This approach collaborates Honeynet, Honeyed and Honeypot to monitor unused activities. Snort used as IDS and honeyed gathers the

important information about the attackers. Authors used tcmdump analysis to analyse the traffic. Based on the analysed data, authors concluded that most of the attacks are on TCP, UDP, HTTP and FTP ports.

2.2 Without Snort NIDS

2.2.1 Data Mining Approach

In[13] emphasised the usage of different data mining techniques to inspect the traffic in NIDS. For experimental purpose authors used NSL-KDD data set. They pre-processed the data like transformation to map the names to values and normalization to enhance the performance. This paper used the algorithms like Linear Regression and K-Means Clustering to analyse the results. But the problem is accuracy rate is around 68% only.

In[14], authors focused on the Anomaly based NIDS. This paper described the hierarchical clustering technique and genetic algorithms usage for better false positive rate. Authors used input data set as NSL-KDD data and performed pre-processing and clustering. After that authors used a met heuristic method for intrusion detection generation. Experimental results showed that the False Positive Rate is reduced using hierarchical clustering when compared with K-means clustering.

In[15] discussed about the knowledge-based IDS to detect cyber-attacks. Authors emphasised on the limitation of knowledge-based IDS that it is lack of contextual information used to detect the attacks. Authors addressed several research challenges of intrusion detection technologies: lack of information about relationships between entities and prediction time, lack of awareness of the current situation, insufficient data at abstract level for analysis, lack of semantic inference to identify cyber-attacks and analysing unknown events. To overcome these challenges, authors proposed a contextual information framework which intelligently assists IDS to predict related suspicious activities.

2.2.2 Artificial Neural Networks Approach

Authors of[16] discussed about a network based intrusion detection system using machine learning approach. They discussed various Machine Learning Techniques proposed in multiple research papers. Authors proposed two-tier architecture to detect intrusions on network level. To analyse the network behaviour, authors considered TCP/IP packets and processed them using hierarchical agglomerative clustering. They also classified the data using KNN classification. It used various algorithms like MLP algorithm and Reinforcement algorithm for decision making regarding detection. For experiment, they used NSL-KDD dataset and WEKA data mining tool. Results show that the MLP algorithm detected the known attacks with accuracy rate of 99.95%. But the problem identified here is wasting the time in handling the clean data.

In[17], authors presented an approach like Artificial Immune System for Distributed NIDS. Authors correlated the functionality of human immune system with the IDS in the aspect of fighting with the outsiders/attackers. This paper proposed a Genetic Algorithm based approach to detect the attacks. For experimental purpose, authors created a network and trained it the self-traffic to recognize the non-self-elements. Authors used NSL-KDD data set and evaluated the detection rate and false alarm rate. But the problem with this Genetic Algorithm approach is that the training the IDS to recognize inside and outside data, which consumes lot of time if it be deployed in a distributed environment.

In[18], analysed various KDD parameters to develop a better IDS on Neural Network. Authors focused on four types of KDD attributes: basic attributes, content related attributes, time-based attributes based on window time and time-based attributes based on window connections. Later authors explained the activity of Artificial Neural Network in terms of training and testing. Authors considered three types of KDD data sets for evaluation purpose. Authors created the Confusion Matrices for the above discussed four types of KDD attributes and resulted that they effectively detected Dos attacks and Probe attacks. But these were failed in detecting U2R attacks.

2.2.3 Comparative Study Approach

Authors of[19] discussed a comparative study of different types of Hybrid IDS. This paper explained various types of attacks and Intrusion Detection classifications. Later different types of Hybrid IDS approaches were analysed in various aspects like Detection Accuracy, False Alarm Rate, Scalability, capability of unknown attacks, etc. Later it concluded that most of the approaches were not capable of finding unknown attacks because of the evolving networking techniques.

2.2.4 Artificial Intelligence Approach

In[20], authors inspired from the immune system and proposed a real time IDS using unsupervised clustering. After

discussing the analogy to the immune system, authors proposed an algorithm that consists mainly two units: T-cells and B-Cells. T-cells used to identify suspicious network activity and B-cells to make further decision. For empirical evaluation authors used KDD Cup 99 Training Dataset. The detection rate of the proposed algorithm is around 65% only. But the problem with this approach is that it can handle only known attacks and false alarm rate increases if any novel attack commence on it.

2.2.5 Wireless Sensor Networks Approach

Authors of[21] discussed how the intrusion detection schemes can be applied for Wireless Sensor Networks (WSN). Because of the openness of deployment area and broadcast nature, WSN are more vulnerable to the attacks. Authors used Kernel Fisher discriminant analysis theory for better detection in WSN. Authors experimented on the WSN data set taken from Naval Research Lab and evaluated on MATLAB. This paper focused on four types of attacks: Passive Sink Hole attacks, Periodic Route Error attacks, Active Sink Hole attacks and Denial of Service attacks. Simulation results showed that the proposed approach had a higher accuracy, timeliness and lower energy consumption.

2.2.6 TCP Based Network Approach

In[22] proposed IDS to identify the throughput degradation attack on TCP. Authors described about how Denial of Service attacks degrades the network performance. Here the authors focused on the TCP Congestion Control Mechanism which emphasised on congestion avoidance, fast retransmit and recovery. In this paper, attacker uses amplification attack to escape detection mechanism. Authors proposed an approach to detect the unnecessary retransmissions by collecting the data packets and ACKs and generating the alerts. For simulation purpose authors used dumbell topology with N senders and N receivers. Tabular results shows the proposed IDS catches all false duplicate ACKs.

After analysing various papers in the field of IDS in this section, next section gives a cumulative view of these papers in various performance based parameters.

3. Comparison of Various IDS

This section tries to compare several IDS approaches in various performance based parameters like Detection Accuracy, False Alarm Rate, Scalability and Capability to detect unknown attacks. By specifying the IDS approach of each paper, the following Table 1 summarizes the performance parameters for all the papers of Section 2. All of the above methods have their own pros and cons. Some of them focus in some particular issues, at the same time they are ignorant of some other important issues. Even though the parameters took for assessment may not benchmark the performance of an IDS approach, we limited to the stated parameters because these are desirable for any IDS.

From the above Table it is clear that several approaches require enhancements to overcome their cons. This paper focus on Snort based IDS. Being an Open Source IDS, Snort can be easily configured and deployed in any environment. To overcome the challenges with Snort this paper proposes architecture. Next section gives a brief overview about Snort and its functionality.

4. Snort

4.1 About Snort

Snort is an Open Source NIDS created by[3]. It can do real-time traffic analysis and packet logging on IP Networks. Also it can analyze the protocols and can search for matching content.

Snort can also be used to detect various attacks like fingerprinting attempts, Buffer Overflows; Stealth port scans and so on.

Snort can be configured in sniffer mode to read packets and display them on the console, in packet logger mode to log packets to the hard disk and in intrusion detection mode, to monitor network traffic and analyse it against a set of user defined rules. Later the system will act based on what has been detected.

4.2 Snort Architecture

Snort contains several logical components[23]. Attack detection and generating output as per requirements is the main functionality of these components.

Following are the key components of Snort based IDS:

- Packet Decoder.
- Pre-processors.
- Detection Engine.
- Logging and Alerting System.
- Output Modules.

Table 1. Assessment of various IDS approaches

Reference	Intrusion Detection Approach	Detection Accuracy	False Alarm Rate	Scalability	Capability to detect unknown attacks
4	Behavior-based Rule creation + Bayesian Network Learning Algorithm	------	------	No	Yes
5	Cloud Environment + Data Mining	100%	------	Yes	Yes
6	Multi Sensors in Private Cloud	51%	------	Yes	Yes
7	Cloud Computing	------	------	Yes	Yes
8	Cloud Computing + Back Propagation Neural Network	------	------	Yes	Yes
9	Commercial and Open Source based IDS	------	------	Yes	Yes
10	Snort Vs Suricata	Full - partial 8 - 19 19 - 58	------	Yes	Yes
11	Distributed approach to detect TCP Flood attack	Only TCP Flood Attacks 100%	------	Yes	Yes
12	Honeypot based IDS	63%	------	Yes	No
13	Data Mining + K-Means Clustering + Linear Regression	67.5% 80%	------	Yes	Yes
14	K-Means Clustering + Hierarchical Clustering	------	0.0017	Yes	Yes
15	Knowledge-based IDS + Contextual Information	------	------	Yes	Yes
16	Network based IDS + Machine Learning Approach + KNN Classification	99.95%	0.01	Yes	No
17	Artificial Immune System + Genetic Algorithm	98.9%	------	Yes	Yes
18	KDD Parameters+ Neural Network	70 - 99%	------	No	No
19	Hybrid IDS : Comparative study	------	------	------	------
20	Immune Inspired IDS	65%	15%	No	Yes
21	Wireless Sensor Networks + Kernel Fisher Discriminator + SVM	62 – 90% 69 – 97%	3.27 – 33.35 5.63 – 40.22	Yes	Yes
22	Active IDS + dumbell topology	50 – 100%	------	Yes	No

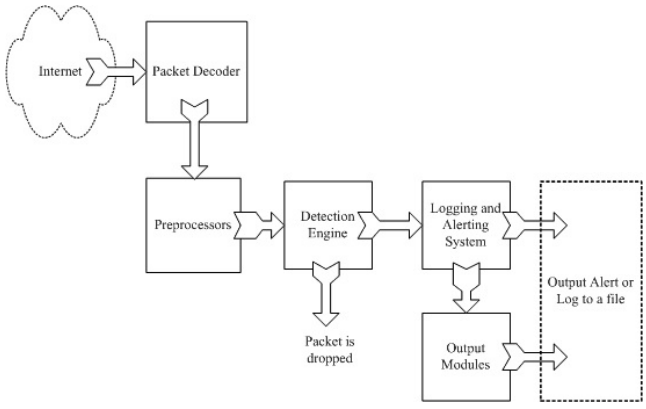

Figure 4. Snort architecture.

Figure 4 shows arrangement of these components. All incoming packets enter the packet decoder and move towards the output modules, either for dropping, logging or alerting.

4.2.1 Packet Decoder

It prepares the packets to be pre-processed or to be sent to the detection engine. These packets are taken from various interfaces like Ethernet, SLIP, PPP and so on.

4.2.2 Pre-Processors

Pre-processors are used to arrange or modify the data packets. Some pre-processors can detect activities by finding anomalies in packets and can generate alerts. For any IDS, this is a key component to prepare packets before analysis done by the detection engine.

4.2.3 Detection Engine

It is responsible to detect intrusion activities. It contains Snort rules for this purpose. All packets are matched against these rules. If there is a match, appropriate action like logging or alerting is taken; otherwise the packet is dropped. Detection engine depends on the power of machine and the number of rules defined to work effectively. If traffic is high, then it drops some packets and response is not accurate. Detection engine depends on the following factors:

- Rule Set.
- Snort Machine Power.
- Network Load.

4.2.4 Logging and Alerting System

After detection engine finds what is inside a packet, it may be used to log or generate the alert about the activity.

4.2.5 Output Modules

These can do different operations depending on how Snort generates output by the logging and alerting system of it. Based on the configuration, these can do the following:

- SNMP traps sending.
- Messaging to syslog facility.
- Database Logging.
- XML output generation.

4. 3 Limitations of Snort

Even though Snort offers the benefits like rapid response, greater accuracy and adaptability, it has several limitations that are identified during the analysis of various papers in Section 2 as stated below.

- Snort was not able to use contextual information in earlier stages, which makes automation and threat assessment more challenging.
- Snort performance depends on the resources available on the machine running it. The more traffic you have, the more resources (CPU/ Memory) you will need to available for Snort.
- Snort detects attacks when the traffic is normal. But when there is huge traffic, it makes a big delay to scan all traffic and detect the intrusion.
- Deployment of Snort based IDS in high speed networks can be challenging.
- Snort is not available with a pre-packaged hardware.
- Snort doesn't support automated tuning and impact assessment.
- Policy management is a critical task for the administrators who wish to use Snort as IDS.
- Detecting Port Scanning Attacks24, DoS Attacks25 and DDoS Attacks26 is very much challenging with Snort.

In order to overcome the above mentioned limitations, this paper focuses on typical attacks that degrade the Snort performance and propose architecture. Next Section discusses the major types of attacks this paper focusing along with the work proposal.

5. Potential Directions

As discussed in the previous section, the limitations can prove challenging while deploying Snort. Performance of any IDS can be improved by focusing on various typical attacks that degrades those IDS. As a potential direction, this paper proposes architecture to countermeasure these attacks and improves the performance of deployed Snort IDS.

5.1 Types of Attacks Focusing

Networks are vulnerable to many types of attacks that threaten the Confidentiality, Integrity and Availability of the services and network. Some of the attacks try to capture the data while some others try to modify. And some try to bring down the services and network. This type of attacks cost a lot in terms of financial, reputation, customer attrition, etc. So, this section focuses on that type of typical attacks which affect the network very much.

5.1.1 Port Scanning Attack

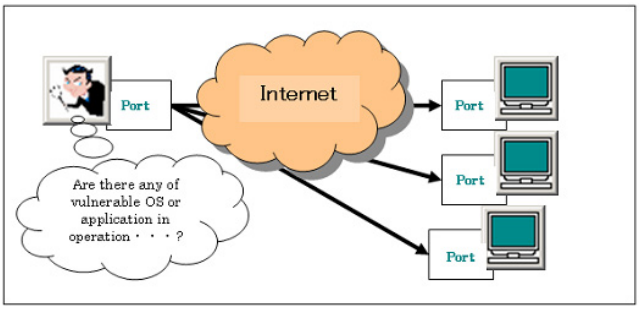

Figure 5. Port scanning.

As shown in Figure 5 Port Scanning[25] is used by attackers to discover services that they can exploit to break into systems. Every system connected to a network run several services that listen to ports. By port scanning, the attacker can get the information like: what services are running, who owns those services, whether anonymous logins are supported, and whether services require authentication. It can be done by sending messages to each port, one at a time. The received response illustrates the weaknesses of targeted system. Port scanners are important to security experts because they can identify possible security vulnerabilities.

5.1.2 Denial of Service (DoS) Attack

A Denial-of-Service (DoS) attack[25] makes the machine or network to shut down and making it inaccessible to legitimate users. DoS attacks accomplish this by flooding the target with traffic that triggers a crash as shown in Figure 6.

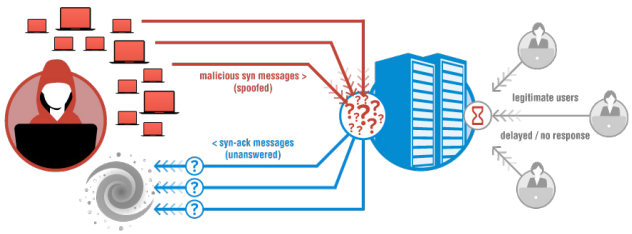

Figure 6. A typical SYN flood DoS attack.

Most of the DoS attacks target the servers of banks, online stores, media, traders and government organizations. Even though DoS attacks don't steal the information, they cost the victim lot of time and money to control it.

In general DoS attacks focus on flooding and crashing the services. These attacks pumps too much traffic to the target system and causing the target to slow down and eventually stop. Some of the flood attacks like:

- Buffer overflow attacks – To send huge traffic to a target than its capacity
- ICMP flood – forces misconfigured devices to ping every computer on the network. The network is then triggered to amplify the traffic. It is also called as ping of death or smurf attack.
- SYN flood – sends a request to connect to a server, but handshaking explicitly avoided. This process continues till the ports are saturated.

Some other DoS attacks make the target systemto crash. For this type of attacks, input is send that takes advantage of loopholes in the target and later crash the system, so that it can't be used[25].

5.1.3 Distributed Denial of Service (DDoS) Attack

A Distributed Denial-of-Service (DDoS) attack[26] occurs when multiple systems flood the traffic to a targeted system. This type of attack is a result of botnet that floods the target with traffic as shown in Figure 7. A botnet is a network of compromised computers controlled by the attacker. When a server is overloaded with connections, it can't accept subsequent connections. Attacker using a DDoS attack gains the advantage because of multiple controlled machines are harder to shut down quickly. This is a big challenge for defense mechanisms. As a result, website crashes for several times[26].

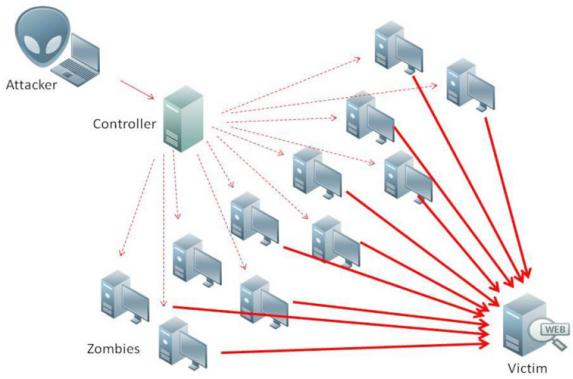

Figure 7. Distributed DoS attack.

DDoS attacks come in many different forms as discussed below[27].

- TCP Connection Attacks

To bring sown the network devices by availing all the connections.

- Fragmentation Attacks

Flooding packets to a victim to reduce the performance.

- Volumetric Attacks

To cause congestion, these attacks consume the bandwidth between target and Internet.

- Application Attacks

To overwhelm a specific service making them difficult to detect and mitigate.

5.2 Our Proposal for Improvement

To detect and prevent the above discussed attacks along with known attacks and to overcome the above discussed limitations, this paper proposes a new architecture as shown in Figure 8. The system needs to perform the task accurately[28].

5.2.1 Design the Layers

To reduce complexity and to make it incremental and ensures security features at all levels of network. This design focus on maintaining the three most important features of an enterprise network: Confidentiality, Integrity and Availability. Attacks like Port Scanning, Packet Capturing, etc. threaten Confidentiality. Man-in-the-middle and Application-Layer attacks threaten the integrity while DoS, DDoS type attacks target the Availability of the network services.

We need to ensure these features must be entrusted by the network. As a proposal, a level based design may ensure these features by with standing all types of attacks.

5.2.2 Integrate the Design into Snort Tool

To prove the efficiency of proposed design, integrate it into Snort Tool using Code Refactoring. Code Refactoring is a technique which can be used to modify or enhance the functionality of an existing program. After identifying the critical parts of Snort where it is lagging in performance and refactoring those components can give better detection results.

5.2.3 Deploy and Evaluate in Kali Linux

After completing the code refactoring, deploy the modified Snort into a Kali Linux based system of a network and evaluate it by attacking the network with various types of attacks. Kali Linux is an open source Operating System which can be used to exploit the vulnerabilities of a system/network. After evaluation, compare the results with previous approaches and prove the efficiency of the proposed level based design.

6. Conclusion

Several approaches of IDS are discussed in this paper to upkeep the security of an organization against attacks. Different types of IDS using efficient rules, Bayesian Network, Honeypot, Neural Networks and Multi-Sensors like techniques can protect from simple intrusions to dangerous DoS type attacks with considerable drawbacks. Assessment of these IDS was done based on some considerable performance parameters which show they need necessary attention. There are still many ways to enhance the efficiency of Intrusion Detection System. This paper proposed architecture to ensure Confidentiality, Integrity and Availability of network. Layer based design can be integrated into Snort to improve its performance. In future we fully design the proposed model and evaluate it to achieve better detection rate against critical DoS type attacks also.

7. Acknowledgement

We would like to thank the anonymous reviewers for their valuable feedback. We would like to acknowledge all the authors of respective research papers that are consulted for our analysis purpose. We would like to thank our Computer Science Department for providing necessary resources for our work. This paper reflects the views only of the authors, and others cannot be held responsible

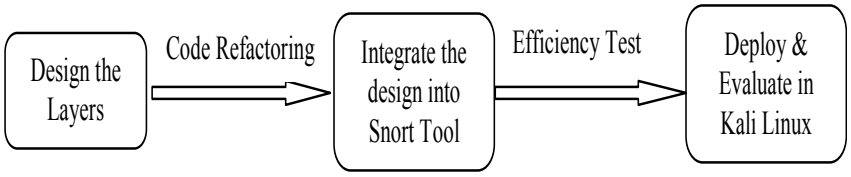

Figure 8. Proposed architecture.

for any use which may be made of the information contained therein.

8. References

1. Basics of intrusion detection systems. Available from: https://www.hackthis.co.uk/articles/basics-of-intrusion-detection-systems
2. Snort-network intrusion detection and prevention system. Available from: https://www.snort.org/
3. Kali Linux. Available from: https://en.wikipedia.org/wiki/Kali_Linux
4. Jongsawat N, Decharoenchitpong J. Creating behavior-based rules for snort based on Bayesian network learning algorithms. The International Conference on Science and Technology (TICST); 2015. p. 267–70. Available from: Crossref
5. Derfouf M, Eleuldj M, Enniari S, Diouri O. Smart intrusion detection model for the cloud computing. Advances in Intelligent Systems and Computing. 2016; 411–21.
6. Sengaphay K, Saiyod S, Benjamas N. Creating snort-IDS rules for detection behavior using multi-sensors in private cloud. Lecture Notes in Electrical Engineering; 2016. p. 589–601. Available from: Crossref
7. Mishra V, Vijay V, Tazi S. Intrusion detection system with snort in cloud computing advanced IDS. Advances in Intelligent Systems and Computing. 2016; 457–65. Crossref
8. Chiba Z, Abghour N, Moussaid K, Omri A, Rida M. A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. Procedia Computer Science. 2016; 83:1200–6. Crossref
9. Hock F, Kortis P. Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks. 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA); 2015. p. 1–4.
10. Park W, Ahn S. Performance comparison and detection analysis in snort and suricata environment. Wireless Pers Communication. 2016; 1–12.
11. Kshirsagar D, Sawant S, Wadje R, Gayal P. Distributed intrusion detection system for TCP flood attack. Proceeding of International Conference on Intelligent Communication Control and Devices; 2016. p. 951–8.
12. Reddy JK, Kumar SB, Kumar SM, Babu SK. Honeypot-based intrusion detection system- A performance analysis. 3rd International Conference on Computing for Sustainable Global Development (INDIACom); 2016. p. 2347–51.
13. Gupta D, Singhal S, Malik S, Singh A. Network intrusion detection system using various data mining techniques. International Conference on Research Advances in Integrated Navigation Systems (RAINS); 2016. p. 1–6. Crossref
14. Sangve S, Thool R. ANIDS anomaly network intrusion detection system using hierarchical clustering technique. Proceedings of the International Conference on Data Engineering and Communication Technology; 2016. p. 121–9.
15. AlEroud A, Karabatis G. Using contextual information to identify cyber-attacks. Studies in Computational Intelligence; 2016. p. 1–16.
16. Divyatmika, Sreekesh M. A two-tier network based intrusion detection system architecture using machine learning approach. International Conference on Electrical Electronics and Optimization Techniques (ICEEOT); 2016. p. 42–7. Crossref
17. Igbe O, Darwish I, Saadawi T. Distributed network intrusion detection systems an artificial immune system approach. IEEE 1st International Conference on Connected Health Applications Systems and Engineering Technologies (CHASE); 2016. p. 101–6. Crossref
18. El Farissi I, Chadli S, Emharraf M, Saber M. The analysis of KDD-parameters to develop an intrusion detection system based on neural network. Lecture Notes in Electrical Engineering; 2016. p. 491–503.
19. Dalai A, Jena S. Hybrid network intrusion detection systems a decade's perspective. Lecture Notes in Electrical Engineering; 2016. p. 341–9.
20. Jha M, Acharya R. An immune inspired unsupervised intrusion detection system for detection of novel attacks. IEEE Conference on Intelligence and Security Informatics (ISI); 2016. p. 292–7. Crossref
21. Hu Z, Zhang J, Wang X. Intrusion detection for WSN based on kernel fisher discriminant and SVM. Advances on P2P Parallel Grid Cloud and Internet Computing. 2016; 197–208.
22. Bhandari A, Agarwal M, Biswas S, Nandi S. Intrusion detection system for identification of throughput degradation attack on TCP. 22nd National Conference on Communication (NCC); 2016. p. 1–6. PMCid:PMC4763522. Crossref
23. Rehman R. Intrusion detection systems with Snort. 1st ed. PTR Upper Saddle River: Prentice Hall; 2003. PMCid:PMC165152
24. Christopher R. Port scanning techniques and the defense against them. https://www.sans.org/reading-room/white-papers/auditing/port-scanning-techniques-defense-70
25. What is a denial of service attack? Available from: https://www.paloaltonetworks.com/documentation/glossary/what-is-a-denial-of-service-attack-dos
26. Denial-of-service attack. Available from: https://en.wikipedia.org/wiki/Denial-of-service_attack
27. What is a DDoS Attack. Available from: http://www.digitalattackmap.com/understanding-ddos/

28. Raviteja G, Nandhini M. An analysis of various snort based techniques to detect and prevent intrusions in networks. IEEE International Conference on Inventive Communication and Computational Technologies (ICICCT 2017); Coimbatore. 2017. p. 10–15. PMid:28384978 PMCid:PMC5376830.