E-ISSN: 2706-8927
P-ISSN: 2706-8919
www.allstudyjournal.com
IJAAS 2020; 2(4): 308-313
Received: 15-08-2020
Accepted: 23-09-2020

Abdul Qadeer Rasooli
Information Technology Department, Computer Science Faculty, Ghor Institute of Higher Education, Ghor, Afghanistan

Sayed Zabihullah Musawi
Information Technology Department, Computer Science Faculty, Kunduz University, Kunduz, Afghanistan

Corresponding Author:
Abdul Qadeer Rasooli
Information Technology Department, Computer Science Faculty, Ghor Institute of Higher Education, Ghor, Afghanistan

Analysis of intrusion detection and prevention systems

Abdul Qadeer Rasooli and Sayed Zabihullah Musawi

Abstract
Recently, the security of an individual computer to large networks as a result of a dramatic growth of new devices connecting to the internet, has become one of the biggest challenges. Along with growing new types of security attacks, many protection mechanisms have taken to improve the privacy and security of sensitive information. Detection of abnormal behavior can help network administrators to identify intrusions but cannot prevent them from breaking into home network. Furthermore, using traditional methods which firewall and IDPS systems reside in different machines that results to low performance by filtering and checking traffic in multi points.
This paper is providing an efficient and cost effective method of both detecting and preventing network threats. To achieve such goal, we are using a form Snort, Suricata, and Bro IDPS Systems.

Keywords: IDS, IPS, SNORT, SURICATA, BRO

1. Introductions
Intrusion Detection and Prevention Systems (IDPSs) is designed to monitor systems/network to find out suspicious activities and to generate an in real-time alarms to administrators as well as to react against to malicious traffics accordingly.
Intrusion detection and prevention systems (IDPS) are essentially a security measure to protect the network from both external and internal attacks. An external attack by a skilled hacker may be thwarted by the IDPS. On the other hand, an employee for a business with administrator powers may be blocked from bypassing the IDPS and reveal all trade secrets. An IDPS inspects all inbound/outbound network activity and takes note of any suspicious patterns.

2. Related Work
From security point of view, a great work has been done to both detecting and preventing malicious traffic from entering to the internal network such as customizing the detection and prevention part [4], using one of misuse or anomaly based systems at the same time etc. There are many methods and techniques [5, 6] that previous papers have dealt with to increase the security in the network while not affecting the performance of the system. But they are not as efficient as the size of network traffic is dramatically increasing. There should be such a system that can handle gbps traffic while the security of the system should not be affected. Here, this paper provides an efficient architecture of the IDPS that can overcome both the weaknesses.

3. Why IDPS is needed?
Before discussing the importance of IDPS, it is better to know the role of IPS in a network and how it can react to attacks.

3.1 IDPS: IPS or IDPS [1] is basically an IDS which can detect malicious traffic but at the same time it will be able to block them as it resides in-line on the network [13] and acts as a gateway, so that attacks such as DoS should not be succeeded to reach their targets. IPS systems plays a crucial role in detecting and blocking both intrusions such as malwares and DoS activities. Without an IPS system, an attacker can easily compromise the systems by propagating malwares or attacks like DoS which will result in deletion, modification and stealth of confidential data or unavailability of crucial services.

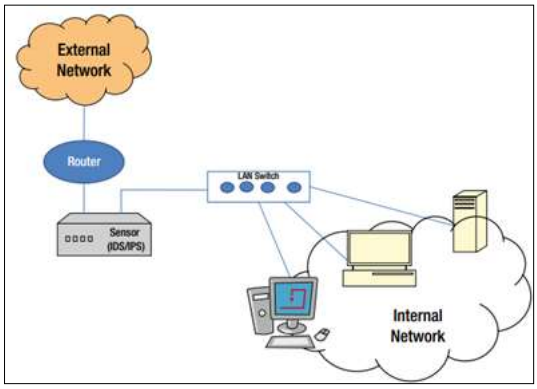

Fig 1: IDPS inline mode

IPSs are classified into four main types: [12, 13]

- Host -Based intrusion detection and prevention systems
- Network- Based intrusion detection and prevention systems
- Network Behavior Analysis
- Wireless –Based intrusion detection and prevention systems

3.2 Need for network IDPS: There are many advantages for selecting Network-based IDPS rather than other systems and they are:

- Only a single system is needed to monitor and protect a network of hundreds or thousands computers.
- A single system can be monitored and managed easily rather than multiple systems.
- NIDPS can protect a network against any type of attacks DoS, DDoS, Ping Flood etc.)
- This system can protect network devices such as Firewalls, routers, Printers etc. against attacks as well.

So, NIDPS is a mandatory and crucial system for any type of network ranging from small sized to medium and large sized networks.

4. Intrusion Detection Methods

4.1 Misuse/Signature-based Detection: The Signature based detection system uses from a database of known signatures (known attacks) for detection purposes. It is simple to configure and employ. It generates less false alarms compared to anomaly based system. But, the worst drawback of such systems is that they are unable to detect any attacks which does not match the signatures [7] (obfuscations). See example below:

script/./././/admin.pwd=script/admin.pwd

In this example, for a normal system both commands are the same while for signature-based IDS they are different commands. See Figure (2)

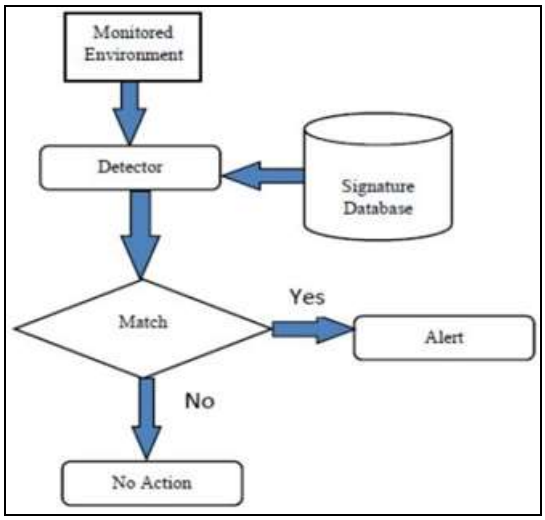

Fig 2: Signature based detection technique

4.2 Anomaly-based Detection: In anomaly detection method, the system first creates a baseline for normal behavior of the network and compares any change to the baseline. If there is any abnormal behavior, then it marks it as intrusion and generates alarm. Anomaly detection technique is excellent in detecting unknown or Zero-day attacks [2] but they are suffering from large number of false alarms.

Examples of abnormal behaviors are: highly consuming system resources, initiating many connections, consuming more network bandwidth etc. See Figure 3.

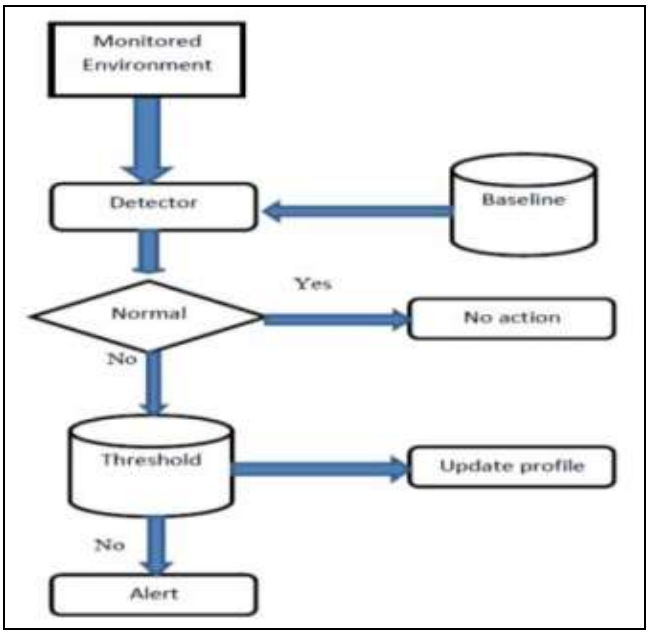

Fig 3: Anomaly based detection technique

4.3 Stateful Protocol Analysis: SPA identified as deep packet inspection, is a system which adds the stateful characteristic to normal protocol analysis. Protocol analysis helps to analyze TCP or UDP payloads that carries other protocols such as HTTP, FTP and DNS. IPSs knows how these protocols work based on their RFCs and any suspicious behavior can be easily detected but the protocol analysis examines only single request or response. An attack would not be carried on a single request but will succeeded on a series of request and response. To detect such attacks, stateful analysis will be the best one. Because it keeps and monitors the whole events within the whole session [14]. The main drawback of such systems is the resource requirements and the system overhead because of complex analysis of traffic [8].

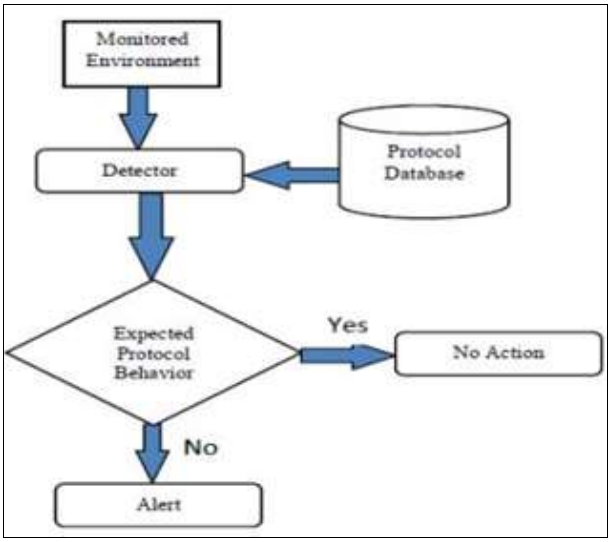

Fig 4: Stateful Protocol Analysis

4.4 Hybrid system: Such systems are created as a result of combining any two or more previous systems to increase the level of security. Such systems are monitored through a single console-line, to achieve high level of efficiency and accuracy while reducing the false positive/negatives remarkably [2]. Figure 5 shows the hybrid system.

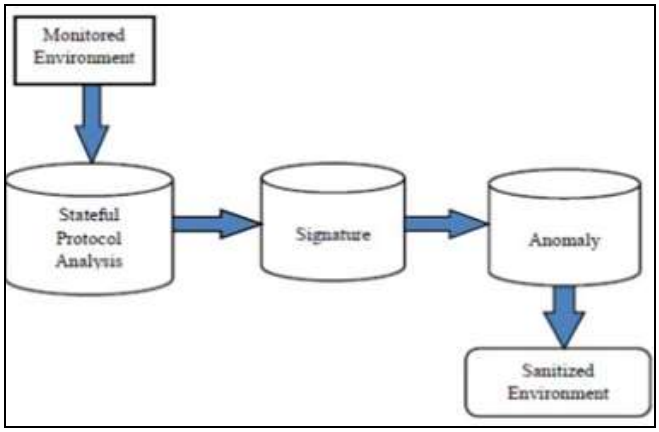

Fig 5: Hybrid detection technique

5. IDPS Systems

The intrusion detection and prevention system (IDPS) is designed to monitor the systems/network to find out the suspicious activity, and also send the report to the administrator, as well as react to malicious traffics accordingly. There are different methods for detection intrusion but false-positives /false negative are two common weaknesses of all types. Multiple techniques taken place to reduce two negative points such as using a hybrid system. We will have a brief review of each of them in the following including anomaly-based and signature-based detection methods. No matter which IDS tools and techniques are used, they should always consider both the security and performance; means that applying a high level of security should not degrade the performance [16].

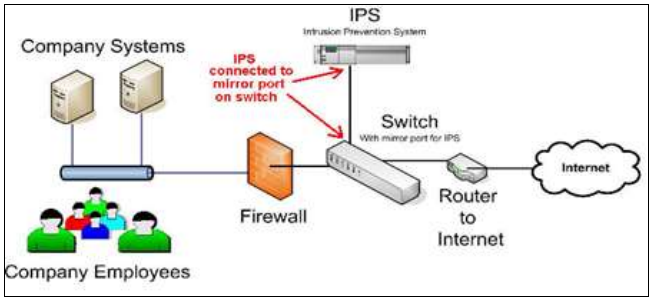

Fig 6: Architecture of NIDPS System (Yousufi *et al*., 2018)

6. IDSP Tools

There are different open source IDS systems available. Each of them has its own features and restrictions, which tool to select is depending on your needs. Below we have a short introduction to each of them.

6.1 Snort: Snort is the first Open Source IDS system introduced by Martin Roesch in 1998, lightweight IDS was available for many platforms like Linux, Mac OS, FreeBSD, and windows. This system is more reliable than other streams IDS systems like Bro and Suricata based on comparative analysis by (Albin & Rowe, 2012) an example Snort faster than Suricata the result of the analysis shows that Suricata consumes more computations, therefore, the processing costs are high.

The Snort open-source can be configured in three modes such as:

- Sniffer mode,
- packet logger, and
- network intrusion detection

Sniffer mode read the all incoming packet of the network, after incoming the packet then the second mode of snort, packet logger it logs all packet of the network into the disk, and the last mode of Snort can monitor and analyze the network traffic [17].

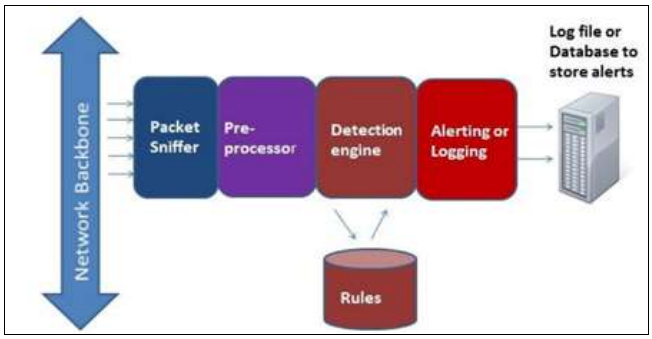

Fig 7: Architecture of SNORT

6.2 Suricata: "In 2009, the US Department of Homeland Security, along with a consortium of private companies, provided substantial grant funding to a newly created organization, the Open Information Security Foundation (OISF). The grant to build an alternative to Snort called Suricata. Suricata was first released in 2010 and worked primarily with version 1.2 released in January 2012.

Although all code is original, Suricata developers have made no attempt to disguise the many ways in which they are borrowing from the Snort architecture. The readily acknowledge Snort as "our collective roots". Suricata can even be used with the same rule sets used by Snort" [18].

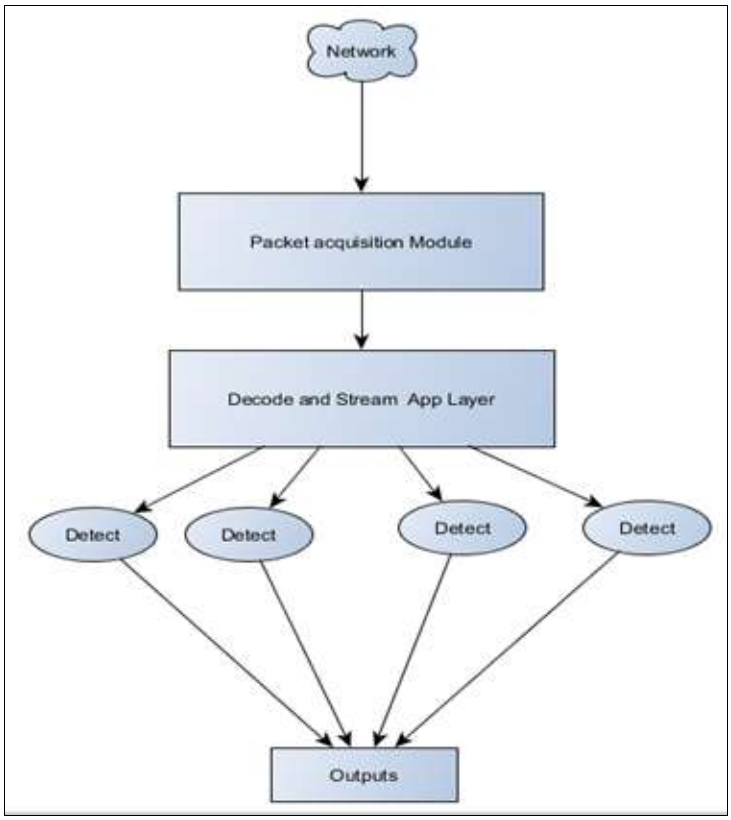

Fig 8: Architecture of Suricata IDPS

6.2 BRO: The new scripting language is created by script driven IDS system of Bro, and much pliable than other systems as snort or Suricata. Despite of this, it can cover a high rate of transferring to provide a worker based architecture and support multiple CPUs. It is the only Unix-based system. In which its processing per each core is low in contrast to the prior IDS system. Bro contains modules which consist of.

- Libpcab: Libpcap packet capturing library is used to capture the network traffic.
- Event Engine: This module takes the filtered packets from Libpcab and performs integrity checks on packets to ensure the packets are correct. For this purpose, it checks the IP header checksum and fragmentation.
- Policy Script Interpreter: Bro open-source policy scripts or rules is written in Bro scripting language and is not relying on signature detections.

Bro can support a high level of analysis using its scripting language and is capable of deep packet inspection in application level [19].

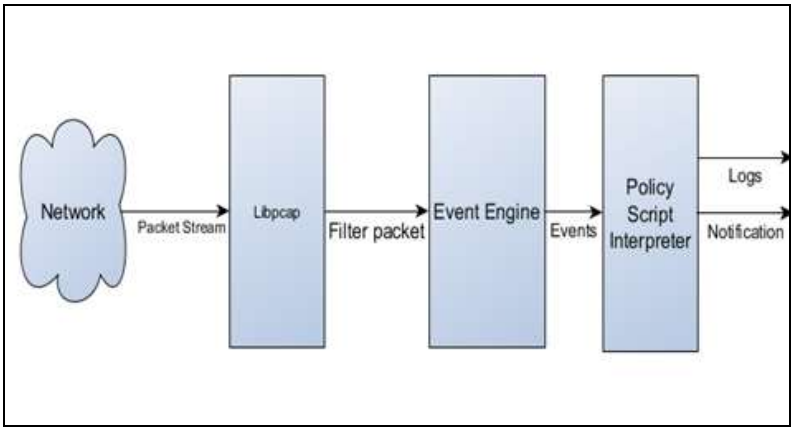

Fig 9: Architecture of Bro IDPS

7. Research Finding

7.1 Common and Popular Open-Source IDS/IPS Systems: The open source network intrusion detection systems had been available for extra than a decade in the past. Snort and Bro are the oldest and maximum popular network intrusion detection systems recognized nowadays. In, 1988, snort was released by means of Martin Roesch. In keeping with the snort corporation website online, over than 4 million downloads and greater than four handred 400,000 registered users display the huge popularity of snort as a deployed IDS answer. Bro was developed with the aid of Vern Paxson in 1999, commonly as a studies platform for intrusion detection and traffic evaluation.

Some other remarkable open source network intrusion detection system is Suricata advanced with the aid of Open Information Security Foundation (OISF). OISF is a non-earnings foundation and funded by department of Homeland Security Directorate for technology and knowledge (A.M. Ahmed, 2013).

7.2 Analysis of Snort, Suricata, and Bro based on performance: Author in our research paper (Cherkaoui, Zbakh, & Braeken, 2017) was done an experiment under open Stack cloud platform with 10 servers. In the experiment, they have tested the detection rate of malicious packets by common open-source (Snort, Bro, and Suricata) under a DDoS attack. The time of experiment was one hour, during the one-hour DDoS attack send 9000 HTTP packet to the web server, they are sending 150 packets per minute. The test was done three times to analyse the performance of each IDS separately with default configuration and default rules of each IDS. According to the result of the experiment, Snort dropped 10% of traffic (900 packets), Bro dropped 8% of traffic (720 packets), and Suricata dropped 5% of traffic (450 packets). The number of packets drops rate of Suricata was lower than Snort and Bro intrusion detection systems [20].

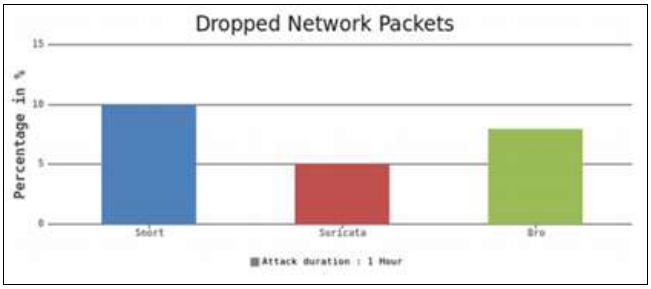

Fig 10: Percentage of Packet drop rate by Snort, Suricata, and Bro (Cherkaoui *et al*., 2017)

7.3 Analysis of Snort, Suricata, and Bro based on Accuracy detection rate: Another research paper (Thongkanchorn, Ngamsuriyaroj, & Visoottiviseth, 2013) discuss about the accuracy detection of three IDS tools such as Snort, Suricata, and Bro. This research paper evaluates all system using a different type of attacks including DoS attack, DNS attack, FTP attack, Scan port attack, and SNMP attack. The main objective of the IDS system is to have a good performance, good accuracy detection, low number of FPR/FNR, and no packet loss during the analysis of packet. One experiment of the mentioned research paper investigates about the rate of packet loss by Snort, Suricata, and Bro. The below figure 4. 14, show on details packet loss of three IDS tools by some attacks at the traffic rate of 400pps [21].

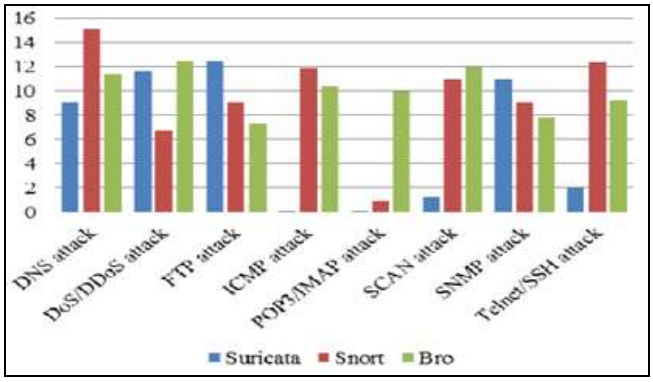

Fig 11: Packet loss of some attacks at the traffic rate of 400pps (Thongkanchorn *et al*., 2013).

According to figure 4.14, Snort loss a lot of packets on the DNS, ICMP, and Telnet/SSH attacks. Suricata has small loss packets rate than two other IDS tools at the POP3/IMAP, SCAN, ICMP, and Telnet/SSH attacks. The Bro IDS loss a lot of packets at the DoS/DDoS, and Scan attacks.

7.4 Analysis of Snort, Suricata, and Bro based on CPU & Memory utilization: The author in thesis document (Pihelgas, 2012) also done an experiment about the CPU utilization of Snort, Suricata, and Bro, in default setting or configuration. This experiment was done on the one host it has a quad-core CPU with Hyper-threading enabled. Which means that 8 logical processors are available to the operating system. According to the result of this experiment, the Suricata CPU utilization is higher than Snort, and Bro, the reason of higher usage CPU in Suricata was using detection engine in multi-threaded, but the reason of low CPU usage of Snort and Bro was the use of detection engine in single threaded [22].

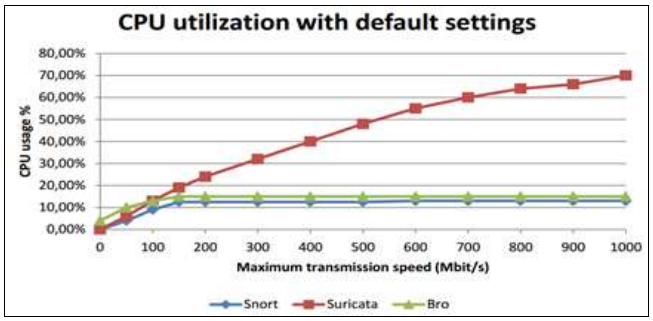

Fig 12: Percentage of CPU usage by Snort, Suricata, and Bro in Default setting (Pihelgas, 2012).

8. Conclusion

There are many systems and techniques to detect or prevent network attacks and one very effective way to protect networks and personal data from being stolen or alteration in time, is using the IDS/IPS systems. IDS and IPS both are similar but the only difference is that IDS systems can reside anywhere in the network while IPS systems have to sit in-line, means that IPS should be acting as a bridge and all traffic should pass through it. In this thesis, a comparative analysis and evaluation are performed on three popular open-source intrusion detection and preventions

systems with a brief description of each one. After review of different journal papers and thesis documents related to the mentioned popular open-source intrusion detection and prevention systems, we came up with the following result: Snort is the most widely deployed worldwide open-source intrusion detection system with nearly 4 million people registered users at Snort website. It has a well document for Windows, Linux, Mac and BSD operating systems. Suricata intrusion detection system is a younger competitor of Snort and Suricata has a lot of CPU/Memory usage, and also Suricata doesn't have a well document for all platforms such as Windows, Linux, Unix, and Mac OS. Finally, Bro intrusion detection systems is an alternative to Snort and Suricata that also provides a comprehensive platform. After a deep comparative evaluation and analysis of Snort, Suricata, and Bro under different criteria (i.e. Performance, Accuracy Detection Rate, and CPU/Memory utilization), the bellow result is achieved: Snort is recommended for small to medium networks with low and medium speed. Because Snort uses a single-threading CPU. On the contrary, Suricata is recommended for large networks with high-speed data rate because Suricata supporting the multi-threading-CPU. Bro also works with high-speed network but it has some significant limitations such as:

- Bro not support the IPV6 traffic,
- configuration is very difficult,
- The Bro open-source does not offer inline intrusion prevention features,
- Working with Bro command line is very difficult.
- Bro works only with UNIX operating system
- Bro does not have contribution facility where you can download new attack signatures.

9. References

1. Shivaji P, Mirashe NV, Kalyankar. 3Why We Need the Intrusion Detection Prevention Systems -IDPS) In IT Company. IEEE 2010.
2. Rajeev Agrawal, David Mudzingwa. A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS). IEEE 2012.
3. Justin Ellingwood. A Deep Dive into Iptables and Netfilter Architecture, 20 Aug 2015. https://www.digitalocean.com/community/tutorials/a-deep-dive-into-iptables-and-netfilter-architecture
4. Minoo Sadat Mirpuryan, Tina Tavizi, Hossein Gharaee. A Comprehensive Network Intrusion Detection and Prevention System Architecture, 6th International Symposium on Telecommunications (IST'2012), IEEE 2012.
5. Alsubhi K, Aib I, Franc Jois, Boutaba R. Policy-based security configuration management application to intrusion detection and prevention, in IEEE conference on Communications (ICC), IEEE 2009.
6. Wattanapongsakorn S, Srakaew C, Charnsripinyo. A Practical Network-based Intrusion Detection and Prevention System, IEEE 2012.
7. Corbin Del Carlo. Intrusion detection evasion: How Attackers get past the burglar alarm. SANS Institute, SANS Great Lakes, Chicago Illinois 2003;1.4b:25.
8. Nagesh Vaidya, Parikshit Godbole. Hardware Implementation of Key Functionalities of NIPS for High Speed Network, IEEE 2015.
9. Baoliang Wang, Kaining Lu, Peng Chang. Design and Implementation of Linux Firewall Based on the Frame of Netfilter/IPtable, IEEE 2016.
10. Eugene Albin, Neil C Rowe. A Realistic Experimental Comparison of the Suricata and Snort Intrusion-Detection Systems IEEE 2012.
11. Michael Rash. Linux Firewalls. No Starch Press 2007, 09.
12. Scarfone K, Mell P. Guide to Intrusion Detection and Prevention Systems, NIST Special Publications 2007.
13. Libnetfilter Queue Project. http://www.netfilter.org/projects/libnetfilter_queue/index.html
14. Umesh Hodeghatta Rao, Umesh Nayak. The Infosec Handbook. Apress 2014, 125-243.
15. Klaus Wehrle, Frank Pählke, Hartmut Ritter, Daniel Müller, Marc Bechler. The Linux Networking Architecture: Design and Implementation of Network Protocols in the Linux Kernel. Prentice Hall 2004, 323-325.
16. Yousufi RM, Lalwani P, Potdar MB. A network-based intrusion detection and prevention system with multi-mode counteractions. Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017-2018 Janua 1-6. https://doi.org/10.1109/ICIIECS.2017.8276023
17. Albin E, Rowe NC. A realistic experimental comparison of the Suricata and Snort intrusion-detection systems. Proceedings - 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2012, 122-127. https://doi.org/10.1109/WAINA.2012.29
18. White JS, Fitzsimmons TT, Matthews JN. (N.D.). Quantitative Analysis of Intrusion Detection Systems: Snort and Suricata.
19. Bhosale DA. Comparative Study and Analysis of Network Intrusion Detection Tools 2015, 312-315.
20. Cherkaoui R, Zbakh M, Braeken A. Ubiquitous Networking 2017;10542:206-213. https://doi.org/10.1007/978-3-319-68179-5
21. Thongkanchorn K, Ngamsuriyaroj S, Visoottiviseth V. Evaluation studies of three intrusion detection systems under various attacks and rule sets. IEEE Region 10 Annual International Conference, Proceedings/Tencon 2013;6:6-9. https://doi.org/10.1109/TENCON.2013.6718975
22. Pihelgas M. A Comparative Analysis of Open- Source Intrusion Detection. 1. Journal 2012, 1-67.