Performance Evaluation of Network based Intrusion Detection Techniques with Raspberry Pi - a Comparative Analysis

Pawan Poonia
Dept. of Computer Science, HMR Institute of Technology and Management, Delhi

Vineet Kumar
Dept. of Computer Science, HMR Institute of Technology and Management, Delhi

Asst. Prof. Chitra Nasa
Dept. of Computer Science, HMR Institute of Technology and Management, Delhi

***Abstract*:- Initially, what is intrusion? An intrusion or an intruder is someone who is accessing the resources in a network without being a legitimate user to use that resource. It has its certain types; an intruder can be a misfeasor or a masquerade. It can be someone who is a legitimate user but isn't given a privilege to use the service it is already been using or someone who is not a legitimate user.**

Intrusion detection is based on computability and analysis based on statistics[1]. Characteristics of computational intelligence (CI) systems, such as adaptation, fault tolerance, high computational speed and error resilience in the face of noisy information fit the requirements of building a good intrusion detection model[1].

Somehow, intrusion is inevitable now as with the increased popularity of network now a day everything is being done or shared staying in the network and wireless networks being prone to so many attacks our information is something which needs to be secured. So in order to provide security to our network we try to find the intrusion in our network by some methods. And with the popularity of the internet we all have been using it at our homes but with the lack of knowledge people around might not realise router is the most important electronic device at our home as it connects all our devices to the internet and makes our information prone to hacking. And router being an intelligent device can analyse incoming and outgoing packets so other packets which could be sent by the intruder can be taken care of, in this paper we are addressing this issue and hence it shows the possibility of using a Raspberry Pi as a router and an Intrusion Detection System(IDS) in a home environment to increase network security.

Keywords: Intrusion, Network, Information, Raspberry Pi, Intrusion Detection System (IDS), Security.

1. INTRODUCTION

Not only the enterprises but also the home networks are vulnerable to the hacking as they are also targeted with the cyber-attacks as now a day's everything is being done online using the internet. From recharging DTH services to paying electricity bills and from shopping to sending money everything is being done using the internet. E-Banking being used the most these days and due to attacks on home networks E-banking users are being targeted the most. And increased numbers of devices connected to the home network makes the situation worse risking private data and financial data and identity theft. Due to a limited knowledge about these issues they cannot protect themselves. And rely just on anti-virus and anti-malware applications.

IDS arms your business against attacks by continuously monitoring network activity, ensuring all activity is normal. If IDS detects malicious activity, it responds immediately by destroying the attacker's access and shutting down the attack. IDS reads network traffic and looks for patterns of attacks or signatures, if a signature is identified, IDS sends an alert to the Management Console and a response is immediately deployed.

So as to avoid such attacks one needs to have knowledge and it is not feasible in every case. Home users can only make it through using a small scale solution which will include low installation cost, low maintenance and low implementation. One possible solution is to run intrusion detection software, for example Snort, on a Raspberry Pi. The device is affordable and flexible as it can run a number of operating systems and might therefore be a very suitable device to provide an entry level upgrade in network protection [2]. And a perfect replacement for a home router.

2. HISTORY

Intrusion detection journey started in early 1980's after the evolution of internet. During the late 1980's, with a growing number of shared networks, enterprise system administrators all over the world began adopting intrusion detection systems. But intrusion started in home networks as well with the increased popularity of internet and online transactions and for the same in 2013 a study was made on the possibility on using a Raspberry as an IDS in a home network. They performance tested a Raspberry Pi Model B+ running the operating system IPFire and the intrusion detection software Snort. The results from this study showed that a Raspberry Pi could be used as IDS [2].

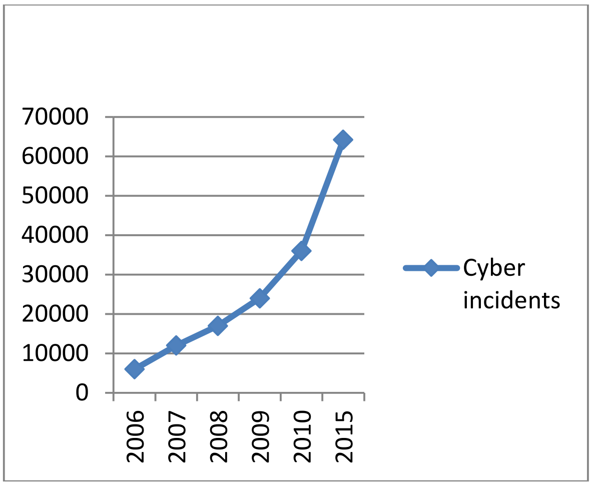

Fig 1. Number of Cyber Incidents Reported

The above chart from US-CERT shows how the cyber incidents rose in current internet network environment; this gives requirement of IDS deployment in network security model[5].

Previously done studies suggests that it had following limitations:

- A limit on how many Snort-rules could be used due to limitations in memory[2].
- A noticeable degradation in throughput when Snort was active[2].

3. INTRUSION DETECTION SYSTEMS

An Intrusion Detection System (IDS) is basically a system comprises both hardware as well as software that monitors a network and detects any possible intrusion by statistical analysis using computational intelligence. It acts like an alarm or giving us the warning and it is completely different from the firewall. Firewall acts as a gateway for the packets and simply works on the rules defined by the administrator;it filters the traffic from the internet and will either pass the packet or will drop it whereas IDS will monitor the traffic from the internet for all possible attacks from intruder.

3.1. IDS Attacks

The various IDS attacks are as shown in figure 2:

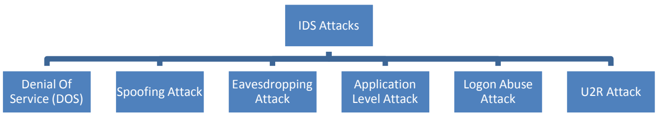

Fig. 2: IDS Attacks

3.1.1. DOS Attack: In DOS attack the targeted system or network is flooded with traffic resulting in flooding and overflow of bandwidth using multiple systems. The DOS attacks disable the services of the host connected to internet temporarily or indefinitely.

3.1.2. Spoofing Attack: Spoofing is said to be when an attacker impersonates another device or user on the network to get control over the system. Man-in-the-middle attack is carried out by spoofing IP address and ARP.

3.1.3. Eavesdropping Attack: A form of external attack where the critical information is sniffed which is transmitted over a network to acquired sensitive information like password, confidential information or session tokens.

3.1.4. Application-level Attack: In application level attacks the attacker attacks the application layer of network and exploit its weaknesses. SQL injections, Trojans, viruses, etc. are the methods to do so.

3.1.5. Logon Abuse Attack: A successful logon abuse attack would bypass the authentication and access control mechanisms and grant a user with more privileges that authorized [3].

3.1.6. User to Root Attack: An unauthorized person tries to access the system or root through the network. Buffer overflow attack is a typical U2R attack which occurs when a web service receives more data than it buffer[3].

3.2. IDS Types

An intrusion detection system is of two types as shown in figure 3: -

- HIDS (Host based IDS)
- NIDS (Network based IDS)

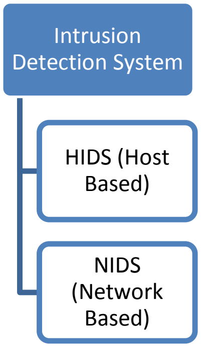

Fig. 3: Classification of IDS

3.2.1. Host-based IDS (HIDS): The host-based intrusion detection system basically monitors and analyses the internals of a computing system and the network packets on its interfaces. It checks intrusion in local system called host system. HIDS gets data from system logs and other logs generated by operating system and monitor and audit it. Host based system trust strongly on audit trail[4].

3.2.2. Network-based IDS (NIDS): The network-based intrusion detection systemdetects all malicious activity by monitoring the network traffic. The NIDS acts as a network sensor. The NIDS audits the network attacks while packets moving across the network [4]. NIDS can capture and analyse data to detect known attacks or illegal activities or analyse network and application protocol activity to identify anomalous and suspicious activity by traffic scanning [5]. NIDS can also be referred as “packet sniffers”, because it captures and collect the data in the form of internet packets passing through communication mediums [6].

3.3. Function of IDS

There are four key IDS function as shown in figure 4:

- Data Collection
- Feature Selection
- Analysis
- Action

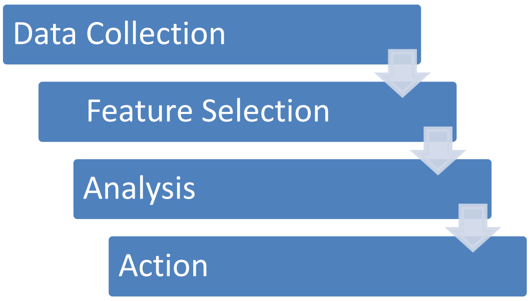

Fig. 4: Functions of IDS

3.3.1. Data Collection: The data collection module passes the data as input to IDS system. This data is saved in a file and is analysed. The data consist of system logs, kernel messages, port-map messages, login messages, etc. [7].

3.3.2. Feature Selection: After collections of data feature are selected i.e. specific functions are applied on the data. Various algorithms like filter algorithm or correlation based algorithm are used for feature selection[8].

3.3.3. Analysis: Once the selection of feature is completed the analysis of data is done for additional useful information. Overview system activity is analysed by changing parameters. The analysis reveals any type of intrusion or network problem.

3.3.4. Action: After detecting network problem or system intrusion preventive actions are takes by IDS tools to prevent attack on the network. The IDS also inform the administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports [4].

3.4. IDS Techniques

There are mainly two IDS techniques as shown in figure 5:

- Signature-based IDS
- Anomaly-based IDS

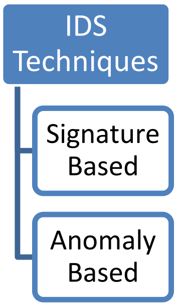

Fig. 5: IDS Techniques

3.4.1. Signature-based IDS: In Signature based detection the system will look for a particular pattern or rule in network packets. Each data set is labelled as normal intrusive and on these basis machine learning algorithms are used to teach and train each data set. Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities[9]. Techniques used in signature based detection are:

- **Expression matching:** In this it searches for the stream of events like log entries for the happening of exact pattern[4].
- **State transition analysis:** This model attacks the state or the transitions in the network[4].

3.4.2. Anomaly-based IDS: An Anomaly based detection technique will look for an anomaly or an outlier in a sequence of packets. Anomaly based detection requires machine learning by comparing new behaviour against the established model. Whenever there is a deviation in the behaviour pattern it will report it as possible intrusion. It identifies anomalies as deviations from “normal” behaviour and automatically detects any deviation from it, flagging the latter as suspect. Thus these techniques identify new types of intrusion as deviations from normal usage [9]. Techniques used in anomaly based detection are:

- **Statistical Models:** The statistical model shows the output as a statistical value[4].
- **Cognition Based Detection Techniques:**It works on audit of data. The set of predefined rules for the classes and attributes are identified from training dataset [10].

4. RASPBERRY PI

The Raspberry pi is a series on single board computers developed in United Kingdom to enhance the computer education in schools and colleges. It can support all the peripheral devices as well. The Raspberry Pi 3 is the third generation Raspberry Pi. It replaced the Raspberry Pi 2 Model B in February 2016. Compared to the Raspberry Pi 2 it has:

- A 1.2GHz 64-bit quad-core ARMv8 CPU
- 802.11n Wireless LANS
- Bluetooth 4.1 (BLE):
- 1GB RAM
- 4 USB ports
- Ethernet port
- 40 GPIO pins full HDMI port
- Display interface (DSI)
- VideoCore IV 3D graphics core

5. RASPBIAN

The Raspbian is a free operating system based on Debian optimized for the Raspberry Pi hardware. Following are the features of Raspbian:

- Kernel 4.1.18+ #846
- 15 secs boot (on RPi 2B)
- 31 MB RAM used

- 477 MB disk space used
- Support for RPi B, RPi B+, RPi 2B and the new RPi 3B
- DHCP client enabled
- SSHD enabled

6. PRESENTLY RUNNING NETWORK IDS

The IDS presently used by most of the users are:

6.1. Snort

Snort is a free and open source and signature based intrusion detection system which is capable of real time traffic analysis and packet logging. Snort was developed by Martin Roesch in 1998. Snort has no real GUI or easy to use administrative console. Some features of Snort are:

- Can work on any operating system
- Protocol examining capability
- Condition examining capability
- Packet reassembly capability

6.2. Suricata

Suricata is a free and open source which fast and robust network threat detection engine. It is capable of real time intrusion detection, inline intrusion prevention and network security monitoring. It inspects the network traffic using a powerful and extensive rules and signature language, and has powerful Lua scripting support for detection of complex threats. Some features of Suricata are:

- Supports all operating system
- Along with the IPS
- Automatic detection of protocols with high performance
- Network Security Monitoring
- Filtering of alerts and events
- Output format support many other tools to analyse data

6.3. Kismet

Kismet is a wireless network detector, sniffer, and intrusion detection system. Kismet works predominately with Wi-Fi (IEEE 802.11) networks, but can be expanded via plug-ins to handle other network types. Some features of Kismet are:

- 802.11 sniffing
- Standard PCAP logging (compatible with Wireshark, TCPDump, etc.)
- Client/Server modular architecture
- Plug-in architecture to expand core features
- Multiple capture source support
- Live export of packets to other tools via tun/tap virtual interfaces
- Distributed remote sniffing via light-weight remote capture
- XML output for integration with other tools

6.4. A Quick Comparison

It has been evaluated that on comparing Snort and Suricata it is observed that Snort should be preferred over Suricata. As shown in report [11]. The precision of snort is 81 percent with false positives of 3.6 percent. Whereas, in Suricata the precision is 91 percent but the false positive is 5.2 percent. And according to the paper [12] snort is preferred as it has following advantages over Kismet i.e., lesser false negatives, high throughput and better error reporting and recovery.

7. EXPERIMENT

We tested the network against a home Router, Raspberry Pi Model-3, Raspberry Pi Model-B+ and Raspberry Pi Model-B with Snort installed in all Raspberry Pi. Following tests are conducted for the experiment:

7.1. On The Basis of Rule Set A (Default Snort Rules)

- TCP capacity of the device over Ethernet
- TCP capacity of the device wirelessly
- TCP capacity of the device with window size of 8000 over Ethernet
- TCP capacity of the device with window size of 8000 wirelessly
- UDP capacity of the device over Ethernet
- UDP capacity of the device wirelessly

7.2. On The Basis of Rule Set B (Customised Snort Rules)

- TCP capacity of the device over Ethernet
- TCP capacity of the device wirelessly
- TCP capacity of the device with window size of 8000 over Ethernet
- TCP capacity of the device with window size of 8000 wirelessly
- UDP capacity of the device over Ethernet
- UDP capacity of the device wirelessly

7.3 Snort Turned Off

- TCP capacity of the device over Ethernet
- TCP capacity of the device wirelessly
- TCP capacity of the device with window size of 8000 over Ethernet
- TCP capacity of the device with window size of 8000 wirelessly
- UDP capacity of the device over Ethernet
- UDP capacity of the device wirelessly

7.4. Performing Security tests

- Mac Filtering
- Content Control
- Shell Code
- Virus
- Network Scanning
- Denial of Service

8. RESULT

8.1. Network Analysis

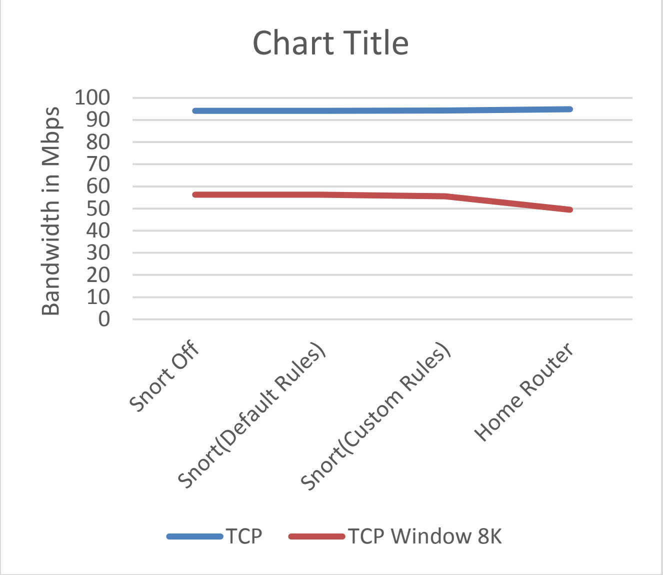

Fig 6: Comparison of Raspberry Pi 2 & Home Router over Ethernet

Table 1: Comparison of Raspberry Pi 3 & Home Router over Ethernet

	Snort Off	Snort(Default Rules)	Snort(Custom Rules)	Home Router
TCP (Mbps)	94.3	94.2	94.3	94.9
TCP Window 8K (Mbps)	46.2	46.2	46.2	49.5
UDP (Mbps)	1.05	1.05	1.05	1.07
Jitter (ms)	0.374	0.579	0.459	0.430
Loss	0/165	3/169	1/150	0/162

Table 2: Comparison of Raspberry Pi 3 & Home Router Wirelessly

	Snort Off	Snort(Default Rules)	Snort(Custom Rules)	Home Router
TCP (Mbps)	19.2	13.2	18.2	26.0
TCP Window 8K (Mbps)	12.9	10.6	12.7	17.6
UDP (Mbps)	1.11	1.05	1.05	1.05
Jitter (ms)	1.872	2.954	2.473	2.235
Loss	0/170	1/160	1/161	0/159

8.2. Benchmarks

On comparing performances of different models of Raspberry Pi it is asserted that Raspberry Pi Model-3 is superior amongst other models on the basis of CPU performance, memory management and power consumption. Below are the graphs for its comparison:

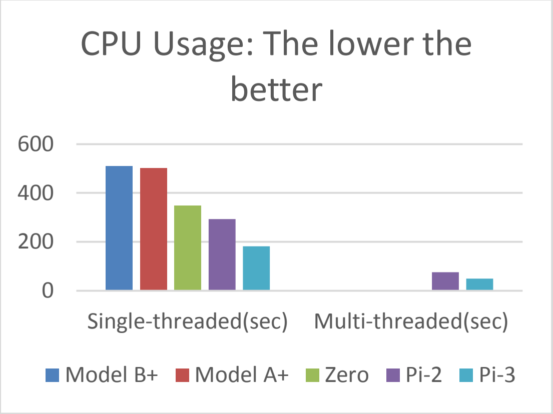

Fig 7. Comparison on Basis of CPU Usage

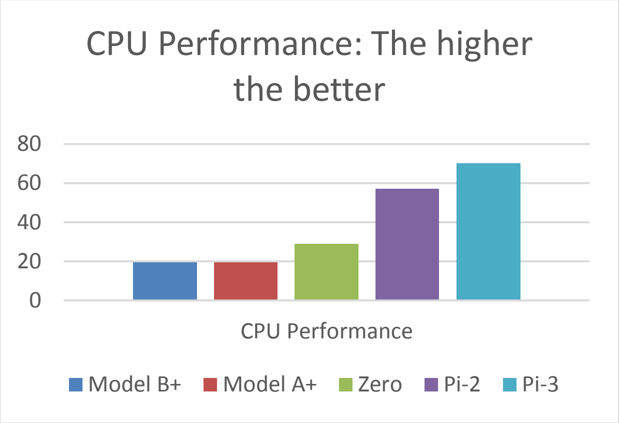

Fig 8. Comparison On Basis of CPU Performance

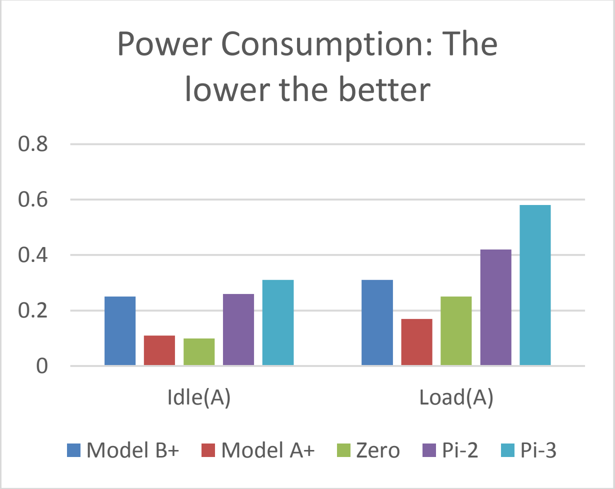

Fig 9. Comparison On Basis of Power Consumption

8.3. Security Features

A comparison of different security features is made between Raspberry Pi and Home Router to verify how effective the intrusion detection system is against network attacks. The comparison table of security feature is as shown:

Table 3: Comparison of Security Features Raspberry Pi & Home Router

	Raspberry Pi		Router
Security Feature/Rules	Custom Rules	Default Rules	Default
Mac Filtering	Yes	Yes	Yes
Content Control	Yes	Yes	Yes
Shell Code	No	Yes	No
Virus	Yes	Yes	No
Network Scan	Yes	Yes	No
DOS	No	Yes	No

9. CONCLUSION

The main objective of this paper is to provide an overview of necessity and utility of intrusion detection system. This paper covers allaspects of IDS which includes its types, functions and techniques, types of attack which may occur on network, overview of hardware and software used to implement Raspberry Pi as a replacement to a router for a secure home network. This paper also covers present scenario and their comparison which includes types of open source IDS available presently and related hardware.

On comparing different IDS, it was observed that Snort is the best alternative amongst the three as it overcomes the shortcomings of Kismet and Suricata. Snort is found to have a better precision with less number of false positives. Moreover, the error reporting in Snort unimpeachable.

Raspberry Pi Model-3 is best suited for this scenario which could be inferred from the charts above. Raspberry Pi Model-2 and Raspberry Pi Model-B+ has few shortcomings which are power consumption level, poor memory management and lower throughput. Moreover, Raspberry Pi Model-3 has dedicated Wi-Fi adapter which enables it to be used as a wireless access point.

A domestic Home Router is not capable of analysing incoming and outgoing traffic. Thus lacks in providing security to the devices connected to the network. The above table depicts the same. Hence to make the home network more secure Raspberry Pi coupled with Snort is great alternate to a relatively insure Home Router. This hardware can be configured precisely to the needs of the customer for better security solution which includes DOS and DDOS protection, anti-malware and anti-virus alerts, content control and other numerous features as per requirements.

10. REFERENCE

[1] The Use of Computational Intelligence in Intrusion Detection Systems: A Review (2008) by Shelly Xiaonan, Wu Wolfgang Banzhaf, Shelly Xiaonan, Wu Wolfgang Banzhaf http://www.mun.ca/computerscience/research/MUN-CS-2008-05.pdf

[2] IDS on Raspberry Pi A Performance Evaluation by Andreas ASPERNÄS,Thommy SIMONSSON https://www.eecis.udel.edu/~cshen/367/Assignments/IDS-RPi.pdf

[3] Karthikeyan. K.R and A. Indra- “Intrusion Detection Tools and Techniques a Survey” http://www.ijcte.org/papers/260-G778.pdf

[4] INTRUSION DETECTION SYSTEM – A STUDY by Dr.S.Vijayarani and Ms. Maria Sylviaa.S http://airccse.org/journal/ijsptm/papers/4115ijsptm04.pdf

[5] Asmaa Shaker Ashoor (Department computer science, Pune University) Prof.Sharad Gore (Head department statistic, Pune University),” Importance of Intrusion Detection System (IDS)”, International Journal of Scientific & Engineering Research, Vol. 2, Issue 1, Jan 2011. http://www.ijser.org/researchpaper%5CImportance_of_Intrusion_Detection_System.pdf

[6] An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications by Hussain Ahmad MadniUppal , MemoonaJaved and M.J. Arshad, International Journal of Computer Science and Telecommunications [Volume 5, Issue 2, February 2014] http://www.ijcst.org/Volume5/Issue2/p4_5_2.pdf

[7] Intrusion Detection Data: Collection and Analysis by Robert F. Erbacher and Bill Augustinehttps://pdfs.semanticscholar.org/4436/e1055b2d9915d69295d813c4ccabcb2957cb.pdf

[8] Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detection System by You Chen, Yang Li, Xue-Qi Cheng, and Li Guohttp://hiplab.mc.vanderbilt.edu/~ychen/survey2006.pdf

[9] Vera Marinova-Boncheva- “A Short Survey of Intrusion Detection Systems”-. Bulgarian academy of sciences http://www.iit.bas.bg/PECR/58/23-30.pdf

[10] SriramSundarRajan, Vijaya Krishna Cherukuri- “An Overview of Intrusion Detection Systems”. http://www.idt.mdh.se/kurser/ct3340/ht09/ADMINISTRATION/IRCSE09-submissions/ircse09_submission_18.pdf

[11] A COMPARATIVE ANALYSIS OF THE SNORT AND SURICATA INTRUSION-DETECTION SYSTEMS byEugene Albin http://www.dtic.mil/dtic/tr/fulltext/u2/a552115.pdf

[12] A Performance Metrics Scorecard Based Approach to Intrusion Detection System Evaluation for Wireless Network by Rupinder Singh &Dr.Jatinder Singh https://globaljournals.org/GJCST_Volume12/1-A-Performance-Metrics-Scorecard-Based-Approach.pdf