INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 4 - V7I4-1898)
Available online at: https://www.ijariit.com

# An intrusion detection system in network traffic with the performance of snort in Wireshark to capture detailed information of data packets

*Isiaka O. S.*
*isiakaosalman2@gmail.com*
*Kwara State Polytechnic, Ilorin, Nigeria*

*Bolaji-Adetoro D. F.*
*bolajiadetorofunsho@gmail.com*
*Kwara State Polytechnic, Ilorin, Nigeria*

## ABSTRACT

***Ideal for any closed data communication system is Data Packet. Network security means data packet security. Every day there are terrible attacks on the Internet. Quality of service has become an issue that requires a powerful traffic analysis and distribution engine for network applications. Network operators can index all applications on their network and use their full set of packet analysis to act as the primary method of intrusion detection. This study mainly focuses on a network intrusion detection system using a network packet analyzer called Wireshark. Therefore, it provides network security through network monitoring tools so that intrusion detection systems can easily gather accurate information. Packet sniffers have the decisive advantage of being an intrusion detection system that detects and blocks a variety of malware and spyware activity in network traffic. It is therefore important to evaluate the performance of Snort in Wireshark to capture, analyze and log detailed information of data packets in a network traffic.***

***Keywords***: *Wireshark, Network Packet Analyzer, Intrusion Detection System, Snort, Packet Sniffer*

## 1. INTRODUCTION

Many different things can go wrong with the network in a computer system at any point in time, from a simple malicious infections to a convoluted failure in router configurations and it will be difficult to solve the problems immediately they occur (Vijayarani & Sylviaa 2015). All network problems occur at the packet level. Even the right application can detect malicious execution, and a trusted protocol can be malicious. The process of recording and interpreting data packets in real time as they traverse the network is called packet inhalation and allows for a more complete understanding of what is currently happening in the network (Dheerendra & Raj, 2016). One tool that runs actively on a network device and can passively receive all data link layer frames passing through the device's network adapter is a packet sniffer (Mohammad et al., 2012). A packet sniffer is used as a tool to collect raw network data over cables (Sharifi, Noorollahi & Farokhmanesh, 2014).

Network Intrusion Detection Network (NIDS) is a system used to detect activity of malicious or illegal user on a network, report appropriate action to a management station, and take immediate action. Identifiers is divided into two categories: anomaly-based diagnosis and signature-based (Vijayarani & Sylviaa, 2015). Wireshark is an open source graphical network interface analysis tool that captures data packets passing through network traffic in real time and displays detailed information about the packets. Similar to tcpdump, but with a graphical user interface and built-in sorting and filtering options. Officially called ether, it stores packets in a human-readable format (Faizal et al., 2010).

Intrusion is detected in real-time network traffic and logged by Snort, and captured packets are analyzed by Wireshark. Packets are received over wireless or wired networks and done intrusion detection on snort (Nureni et al., 2020). Snort is a free and open source network intrusion detection system developed by Roche Martin (Amrita & Brajesh, 2012). According to Roche, Snort is a lightweight intrusion detection system that can record and analyze network traffic in real time and log precise packets over IP networks. Snort is a signature based network analyzer. The snort analysis of network traffic is based on set of rules, called the VRT

Rules. The snort uses pre-processor and rules to analyze network. The snort rules gives a way to analyze single packets by set signatures while the pre-processor codes provide the possible means of analyzing data packet that cannot be analyzed by rules alone (Karl, 2002).

Intrusion detection systems provide strong protection against network hacking, identity theft, and data mining. Large corporations and government agencies use these programs to manage information and accounts, and monitor employee network activity to ensure that on-site facilities are not misused (Parati & Potteti, 2015). However, despite all the benefits, failure to differentiate between malicious and deliberate or illegal activity can interfere with intrusion detection systems, leading to network outages and loss of business and revenue (Vijayarani & Sylviaa, 2015).

### *i. Types of Intrusion Detection Systems*

The two main types of intrusion detection systems as enumerated by (Santos et al., 2013) are:

a) Network Intrusion Detection Systems: The Network Intrusion Detection System (NIDS) sits at a strategic point in the network to monitor incoming and outgoing traffic from any device on the network. It scans all traffic on a subnet and logs traffic sent through it to a library of known attacks. Alerts can be sent to administrators when an attack is detected or anomalous behavior is observed (Sharifi et al., 2014; Jaydip, 2010). An example of NIDS is setting up a grid where there is a firewall to see if someone wants to enter the firewall. Ideally, all inbound and outbound traffic could be scanned, but this could cause damage that affects the overall speed of the network.

b) Host Intrusion Detection Systems: Host Intrusion Detection Systems (HIDS) operate on multiple hosts or devices on a network. HIDS only monitors I/O packets from devices and alerts users or administrators when suspicious activity is detected. Takes snapshots of existing system files and compares them to previous images. Alerts are sent to administrators to confirm when critical system files are changed or deleted (Sharifi et al., 2014; Jaydip, 2010). An example of the use of HIDS can be found on mission-sensitive computers where settings should not be changed. Intrusion detection systems can also be equipped with system-specific tools and traps.

### *ii. Classification of Intrusion*

The four classification of intrusion prevention systems as highligthed by Santos et al. (2013) are:

a) Network-based Intrusion Prevention System (NIPS), which analyzes protocol activity to detect suspicious data traffic across the entire network;

b) Network Behavior Analysis (NBA) that inspects network traffic to identify threats that cause abnormal traffic flows, such as distributed service attacks, malware, and policy violations;

c) Wireless Intrusion Prevention System (WIPS) that scans wireless network protocols for suspicious traffic; and

d) Host Intrusion Prevention System (HIPS) is a software package installed and used to analyze host incidents by monitoring for suspicious activity on the host.

## 2. LITERATURE REVIEW

Mohammad, Abdul and Abu (2012) implemented an intrusion detection system that uses genetic algorithms to efficiently identify different types of network intrusions. To implement and measure system performance, the logical detection rate was determined using the standard KDD99 data set. The standard deviation equation by distance was used to measure the proportions of chromosomes. They are convinced that the use of better or more innovative formulas in this discovery process will significantly improve detection rates and processes, especially false positives. In the near future, they plan to improve our intrusion detection system with more statistical analysis and in some cases more complex comparisons.

Vijayarani & Sylviaa (2015) reviewed necessity and usefulness of intrusion detection systems. This article provides a detailed analysis of detection systems, their lifecycles, different domains, types of attacks, and types of tools. IDS has become an integral part of security in today's business world. For network users, IPS defines security measures for network users. In the life cycle, phases develop and phases become clear. There are other challenges to overcome. This technique is performed specifically to diagnose abnormalities and to diagnose abuse, and other techniques may be used. The task uses a selective feedback method to continuously improve classification based on comparative analysis of some common data mining algorithms applied to recognition and classification systems.

Parati & Potteti (2015) investigated several new intrusion detection techniques and evaluated their performance based on KDD Cup99 intrusion data. They considered SVM and GP as models for intrusion detection. Next, they designed an SVM-GP hybrid model and an aggregation approach using SVM, GP, and SVM-GP models as the primary classification. Experimental results suggest that general practitioners generally have better or equivalent accuracy for probe, U2R, and R2L classes. The combined SVM-GP method provides a performance boost or similar offering for all classes through a simple SVM approach. Group Policy performed best in R2L tests and classes. The group approach shows 100% accuracy for the sample class, indicating that 100% accuracy is possible for other classes if an appropriate default classifier is chosen. In the end, they devised an intelligent hierarchical IDS model to take full advantage of the best choice of individual classifier and group approaches.

Dheerendra & Raj (2016) provided an overview of the requirements and benefits of intrusion detection systems. This document provides a detailed investigation into the types, lifecycles, different regions and types of attacks of intrusion detection systems. IDS has become an integral part of today's business and network user security. IPS regulates security measures. In the life cycle, phases develop and phases become clear. There are other challenges to overcome. This technique is performed specifically to diagnose abnormalities and to diagnose abuse, and other techniques may be used. Further work is underway on IDS classification based on comparative analysis of some common (classical) data mining algorithms used in IDS and classification using various optimization techniques.

Amrita & Brajesh (2012) argue that IDS should have the means to determine whether network traffic is malicious before it can be identified as a potential threat to the network. Therefore, this study presents a novel method for determining acute attack penetration using time-based diagnostics. A method used to identify anomalies based on the number of connections per second. For further verification, this method is performed on other real network traffic. Because this study only focuses on TCP connections, researchers will use a variety of protocols and science to learn more about fast attack activity in the near future. Inspection and references to other protocols can help identify rapid attack activity using UDP or ICMP. In conclusion, the approach presented in this research has been implemented in a production network to achieve anomaly detection performance with time-based diagnostics.

Santos et al. (2013) showed that better intrusion detection and prevention systems are needed to improve network security. They are unreliable enough (mostly due to false positives and false positives) and difficult to use. But today, it is clear that these systems are essential to ensuring the safety of businesses. It is recommended to incorporate various detection systems to ensure the safety of the computer. IPS, which seeks to partially mitigate these issues, are not robust enough to be used in construction.
Asmaa & Sharad (2014) describe the role and impact of intrusion detection and prevention systems in network environments. "IPS not only detects malicious packets from malware, bots, viruses and targeted attacks, but can also take action to prevent network damage to network activity." Declaration. The attacker's primary objective is to steal sensitive information and intellectual property by processing anything that can be obtained from customer data, such as employee information and financial data. IPS is designed to protect assets, resources, data and networks.

## 3. MATERIALS AND METHODS

A Network Intrusion Detection System (NIDS) is a common type of Intrusion Detection System (IDS) that monitors the network at all levels of the Open Systems Interconnection (OSI), determines the purpose of traffic, and analyzes suspicious activity. Most NIDSs can handle traffic from multiple systems simultaneously and can be easily distributed over a network. The proposed system is designed to work as follows.

(i) As shown in Figure 1.0-3.0, the user sends a request to the server that responds by providing the requested service.


**Figure 1.0: Testing server for intrusion detection**


**Figure 2.0: Intrusion Program Running on command line**

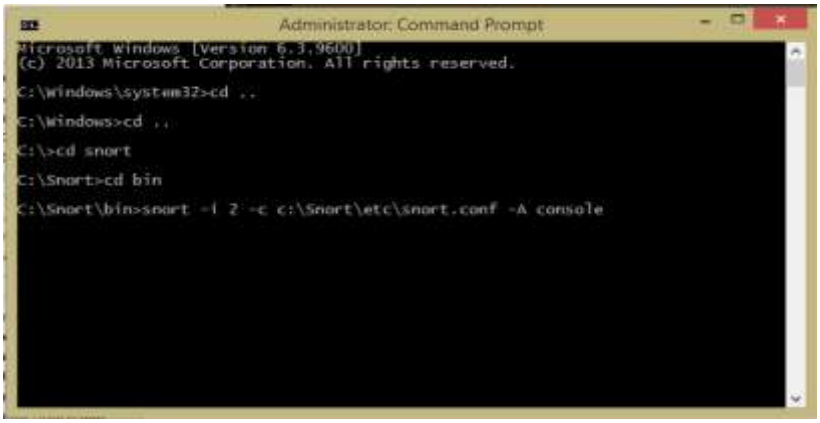



**Figure 3.0: Serving snot for intrusion purpose**

(ii) The network sends IP packets from source to destination as shown in Figure 4.0-5.0.

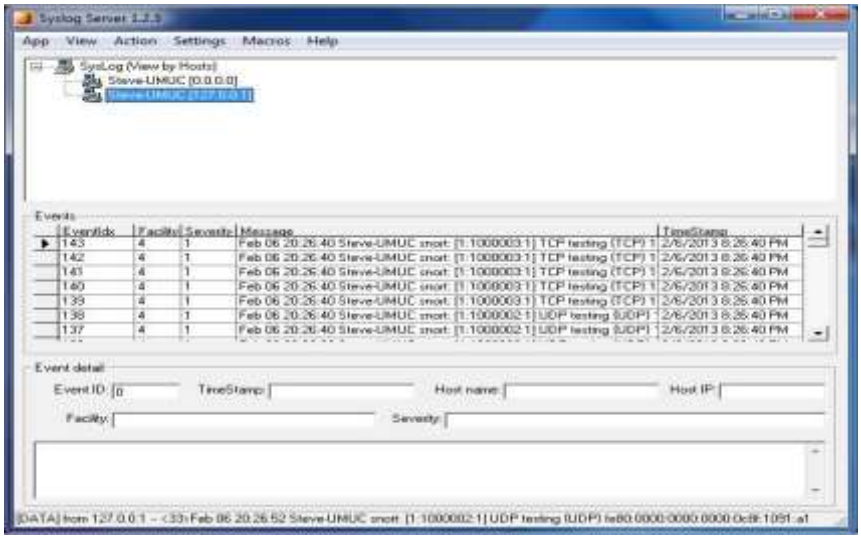



**Figure 4.0: Syslog Server logging intrusion information communicating with snort**

| | AIX | FreeBSD | HP-UX | Irix | Linux | Mac OS X | NetBSD | OpenBSD | Solaris | Tru64 UNIX | Windows |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Physical Interfaces | | | | | | | | | | | |
| ATM | Unknown | Unknown | Unknown | Unknown | Yes | No | Unknown | Unknown | Yes | Unknown | Unknown |
| Bluetooth | No | No | No | No | Yes[1] | No | No | No | No | No | No |
| CiscoHDLC | Unknown | Yes | Unknown | Unknown | Yes | Unknown | Yes | Yes | Unknown | Unknown | Unknown |
| Ethernet | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| FDDI | Unknown | Unknown | Unknown | Unknown | Yes | No | Unknown | Unknown | Yes | Unknown | Unknown |
| FrameRelay | Unknown | Unknown | No | No | Yes | No | Unknown | Unknown | No | No | No |
| IrDA | No | No | No | No | Yes | No | No | No | No | No | No |
| ppp[2] | Unknown | Unknown | Unknown | Unknown | Yes | Yes | Unknown | Unknown | No | Unknown | Yes |
| TokenRing | Yes | Yes | Unknown | No | Yes | No | Yes | Yes | Yes | Unknown | Yes |
| USB | No | No | No | No | Yes[3] | No | No | No | No | No | No |
| WLAN[4] | Unknown | Yes | Unknown | Unknown | Yes | Yes | Yes | Yes | Unknown | Unknown | Yes |
| Virtual Interfaces | | | | | | | | | | | |
| Loopback | Unknown | Yes | No | Unknown | Yes | Yes | Yes | Yes | No | Yes | N/A[5] |
| VLAN Tags | Yes | Yes | Yes | Unknown | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Figure 5.0: Networks Supported for intrusion simulation**

(iii) An Intrusion Detection System (IDS) takes packets from the network and analyzes them as shown in Figure 6.0-7.0.

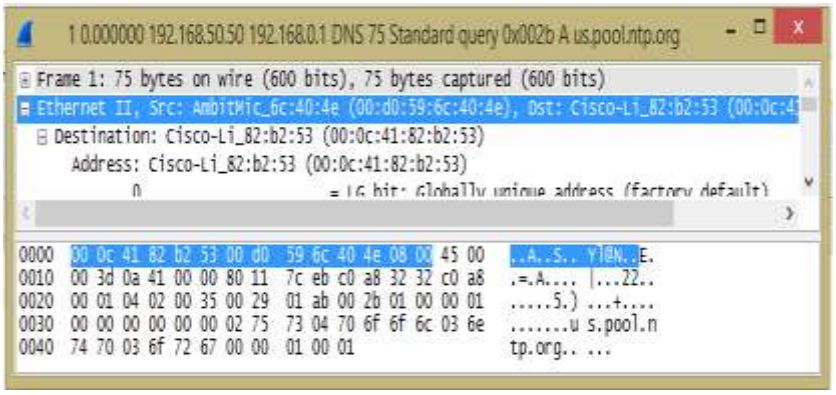



**Figure 6.0: Analysis of information sent and received on network**

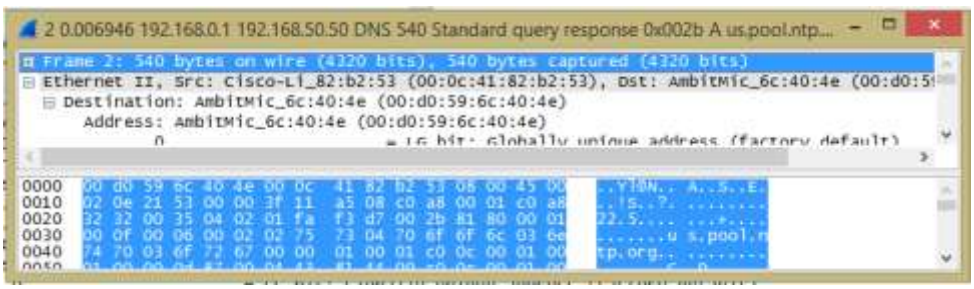



**Figure 7.0: Analysis of Intrusion on LAN network**

(iv) An Intrusion Detection System (IDS) notifies system administrators of suspicious activity or attacks, as shown in Figure 8.0-9.0.

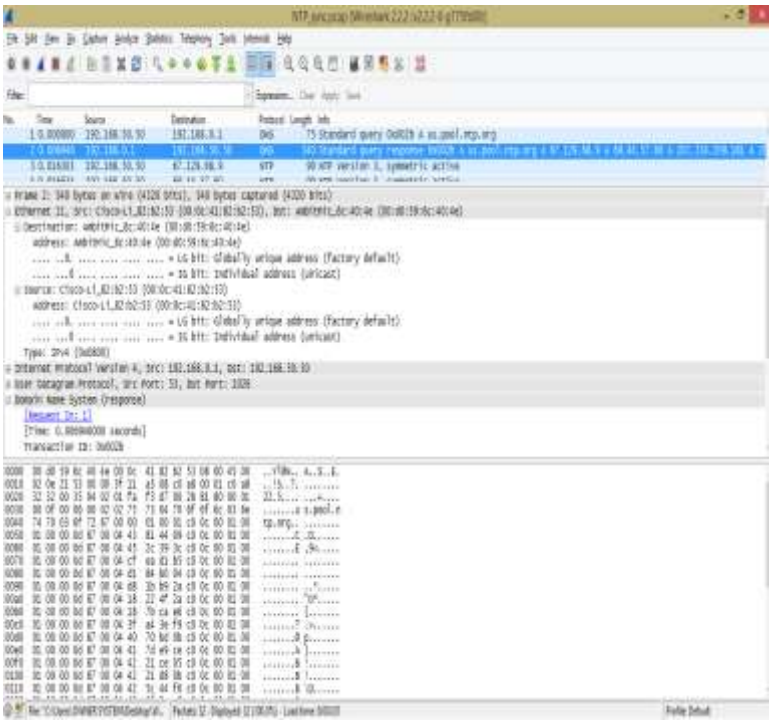
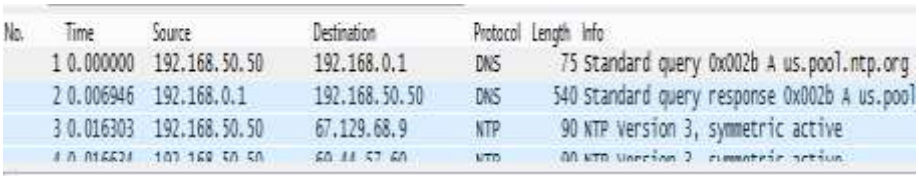


**Figure 8.0: List of connected networks and their respective information**



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.50.50 | 192.168.0.1 | DNS | 75 | Standard query 0x002b A us.pool.ntp.org |
| 2 | 0.006946 | 192.168.0.1 | 192.168.50.50 | DNS | 540 | Standard query response 0x002b A us.pool |
| 3 | 0.016303 | 192.168.50.50 | 67.129.68.9 | NTP | 90 | NTP Version 3, symmetric active |

**Figure 9.0: Intrusion Detection Page**

## 4. RESULTS AND DISCUSSION

To achieve the proposed system goal, we use Wireshark and Snort to develop an intrusion detection system. Snort is the most widely used open source IDS system today and is supported on Unix and Windows systems (Stawowski, 2006). This is done by monitoring the incoming network traffic (typically VLANs) connecting the server to the NACIO network hub. This traffic is compared against a database of known signatures and attack anomalies, and alerts are sent when a violation is detected. Signatures are so widely used that they target new types of hacking and update exploits appearing in databases.

Network Intrusion Detection System (NIDS) is a system network intrusion monitoring system. Intrusion detection is performed in the same way as signature pattern matching and anomaly detection. Error detection is a method of recording normal network activity to detect network anomalies, including sudden increases in the rate of network traffic (IP packets per second). Signature pattern comparison is a method of comparing network data with known database attack techniques. For example, the IDS monitoring web server can be programmed to look for the string "phf" as the CGI attack index. An intrusion is detected and the system type is reported to the system administrator when one of the following events occurs: Firstly, when external inventory is found in the registry. Secondly, when users try to access information out of their reach. Finally, when critical system resources criteria such as file entries, CPU utilization, disk activity, and user logging are measured.

## 5. CONCLUSION

Wireshark cannot do the intrusion alone that is the reason for using it along with snort, syslog and the proper intrusion mechanism. This research records network traffic in real time and uses Wireshark and Snort to perform detailed analysis of the captured packets. Wireshark itself cannot issue warnings or take action to prevent unauthorized access. When an intrusion occurs, the intrusion detection device locks the system and generates an alert of unusual activity. Intrusion detection systems (IDS) play an important role in detecting suspicious activity and preventing harmful effects. An existing signature-based IDS is running and takes a lot of memory, mainly due to the pattern matching process.

## 6. REFERENCES

[1] Amrita A. and Brajesh P. (2012). An overview on intrusion detection system and types of attacks it can detect considering different protocols. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(8), 94-98.

[2] Asmaa S. A. and Sharad G. (2011). Intrusion detection system (IDS) & intrusion prevention system (IPS): case study. *International Journal of Scientific & Engineering Research*, Vol.2, Issue 7, pp.1-3.

[3] Dheerendra K. P. and Raj K. P. (2016). A review on variety of intrusion detection system and their functional approaches. *International Journal of Engineering Sciences & Management.* Patel & Paul, *6*(3).

[4] Faizal, M.A., Mohd Zaki M., Shahrin S., Robiah, Y., Siti R., S., and Asrul H., Y. (2010, Sept. 22-23). Time based intrusion detection on fast attack for network intrusion detection system [Conference Session]. Second International Conference on Network Applications, Protocols and Services, (IEEE), Malaysia. http://doi.org/10.1109/NETAPPS.2010.33

[5] Jaydip S. (2010). An agent-based intrusion detection system for local area networks. *International Journal of Communication Networks and Information Security*, *2*(2), 128-140.

[6] Karl L. (2002). Intrusion detection: Current capabilities and future direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE.

[7] Mohammad S. H. Abdul M. and Abu N. B. (2012). An implementation of intrusion detection system using genetic algorithm. *International Journal of Network Security & Its Applications*, *4*(2), 109-120. http://doi.org/10.5121/ijnsa.2012.4208

[8] Nureni A. A., Taiwo M. B., Sanjay M., Adewole A., Charles V. V. and Ravin A. (2020). Intrusion detection and prevention systems: an updated review. *Data Management, Analytics and Innovation*, 685-696. http://doi.org/10.1007/978-981-32-9949-8_48

[9] Parati N. and Potteti S. (2015). Intelligent intrusion detection system using SVM and Genetic Algorithm (SVM-GA). *International Journal of Science and Applied Information Technology*, *4*(2), 1–5.

[10] Santos B. K., Chandra T. S., Raju P., Ratnakar M., Dawood B. Sk. and Sudhakar N. (2013). Intrusion detection system - types and prevention. *International Journal of Computer Science and Information Technologies*, *4*(1), 77–82.

[11] Sharifi A., Noorollahi A.B. and Farokhmanesh F. (2014). Intrusion detection and prevention systems (IDPS) and security issues. *International Journal of Computer Science and Network Security*, *14*(11), 80-84.

[12] Sharifi A., Zad F.F., Farokhmanesh F., Noorollahi A. & Sharifi J. (2014). An overview of intrusion detection and prevention systems (IDPS) and security issues. *Journal of Computer Engineering*, *16*(1), 47-52.

[13] Stawowski, M. (2006). The principles and good practices for intrusion prevention systems design. *25*. https://pdfs.semanticscholar.org/8cac/01d90c44ae710719df662f858ca17ffc96d1.pdf

[14] Vijayarani S. and Sylviaa S. (2015). Intrusion detection system– a study. *International Journal of Security Privacy and Trust Management*, *4*(1), 31-44. http://doi.org/10.5121/ijsptm.2015.4104