IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

www.ijitce.com

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN 2347–3657
Volume10,Issue4,Nov2022

Wireless Network Security Design And Analysis Using Wireless Intrusion Detection System

1K. Kalpana,2Uma Devarakonda,3 Sk Saida

Article Info

Received: 13-08-2022 Revised: 27 -09-2022 Accepted: 12-10-2022

Abstract—

Network security measures are crucial for network maintenance; attacks that damage the connection system between linked devices are extremely dangerous. We must occasionally find using a network painful in order to accomplish network security; this is usually something to take into account when designing a network security system .The WIDS (Wireless Intrusion Detection System) method can be used to identify DOS (Denial of Service) attacks. Wireless networks can be shielded from potential threats by using the Linux operating system with Iptables acting as an attack handler and Snort acting as a sensor engine. Within the system configuration, a WAN (Wide Area Network) network is built to match the test. Every move the attacker makes on the network may be recognized, according to the results of the analysis of each test, enabling a fix to be applied before more harm is done.

Keywords: Wireless Intrusion Detection System, Network Security, Denial of Service.

1. **Introduction**:

A computer network is a group of independent computers that are connected by communication protocols and media for the interchange of data, software, and hardware like hard drives and printers. Additionally, a computer network can be described as a grouping of several communication terminals connected to numerous computers that aredispersed throughout various areas [1].

Thanks to the abundance of information and communication technology devices, wireless technology is developing at a dizzying rate. Computers, laptops, mobile phones, and their accessories are the devices most commonly used with wireless technology [2]. WLAN (Wireless Local Area Network) is a word used to describe the use of wireless technology in a local network. Page Layout

1. Assistant Professor, Department of CSE, RISE Krishna Sai Prakasam Group of Institutions, Ongole,
2.Assistant Professor, Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole
3.Assistant Professor, Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole.

2. Theoretical Support:

Network Architecture and Concepts

An electrical device for accurately and quickly manipulating data is a computer [4]. The term "computer" was initially used to refer to people who perform mathematical operations either with or without the use of tools, but over time, its definition was expanded to include the actual machine.Initially, information processing was almost solely devoted to arithmetic problems, but today's computers are employed for a variety of math- related tasks.A system that integrates computer and communication technologies is known as a computer network. Distributed data processing, which makes use of databases, application software, and hardware equipment applications simultaneously to support office automation and increase productivity, is made possible by this combination of technologies [5]. The goal of a computer network is resource sharing. A program called Snort may identify intruders by real-time monitoring packets passing across the network, storing them in a database, and identifying various attacks coming from outside the network. The snort application can be used in three different ways in this mode: as a packet sniffer to view packets as they move through the network, as a packet logger to record all packets moving through the network for later analysis, and as an NIDS (Network Intrusion Detection System) to detect network intrusions. Attacks that occur via computer networks will be recognized by Snort [8].The traits of Snort are: Because Snort is open source, usingit is completely free. As a result, Snort is the perfectchoice for a lightweight, affordable NIDS if a small business cannot use NIDS.

A tool called Snort can discover intruders by tracking down multiple attacks coming from outside the network and real-time anal zing packets as they pass across the network. The snort application can be utilized in three different ways inthis mode: Packet Sniffer to view packets flowing through the network, Packet Logger to record all packets passing through the network for further analysis, and NIDS (Network Intrusion Detection System).

3. System development methodology:

The system development process employs a variety of approaches or models. In this study, an IDS system will be built with a network-centric focus, and SPDLC (Security Policy Development Life Cycle) will be used as the system development approach or model.

The SPDLC technique establishes a plan for updating a network system within an organization; the network system development cycle is broken down into various segments. Luay A. Wahsheh and Jim Alves Foss state that the five stages of the SPDLC system's evolution were studied, starting with the Analysis stage. At this point, the problem formulation process was completed, the IDS, Ethereum and several network devices were identified, data were gathered, and the needs of everyone were defined .Figures must be numbered using Arabic numerals. Figure captions must be in 8 pt Regular font. Captions of a single line (e.g. Fig. 2) must be centered whereas multi-line captions must be justified (e.g. Fig. 1). Captions with figure numbers must be placed after their associated figures, as shown in Fig. 1.

In order for the system that is developed to be relevant to the system that has been designed, specifics of the design that will be used are shown in Figure 3 as instructions or a guide for the implementation phase. The installation and configuration steps make up the implementation procedure. by gathering all the equipment required at the research lab. Stage of enforcement: Following installation, there comes a stage of enforcement, and this step is crucial. The implementation phase is carried out by carrying out operational tasks and checking to see if the built- and-implemented IDS system is functioning properly.

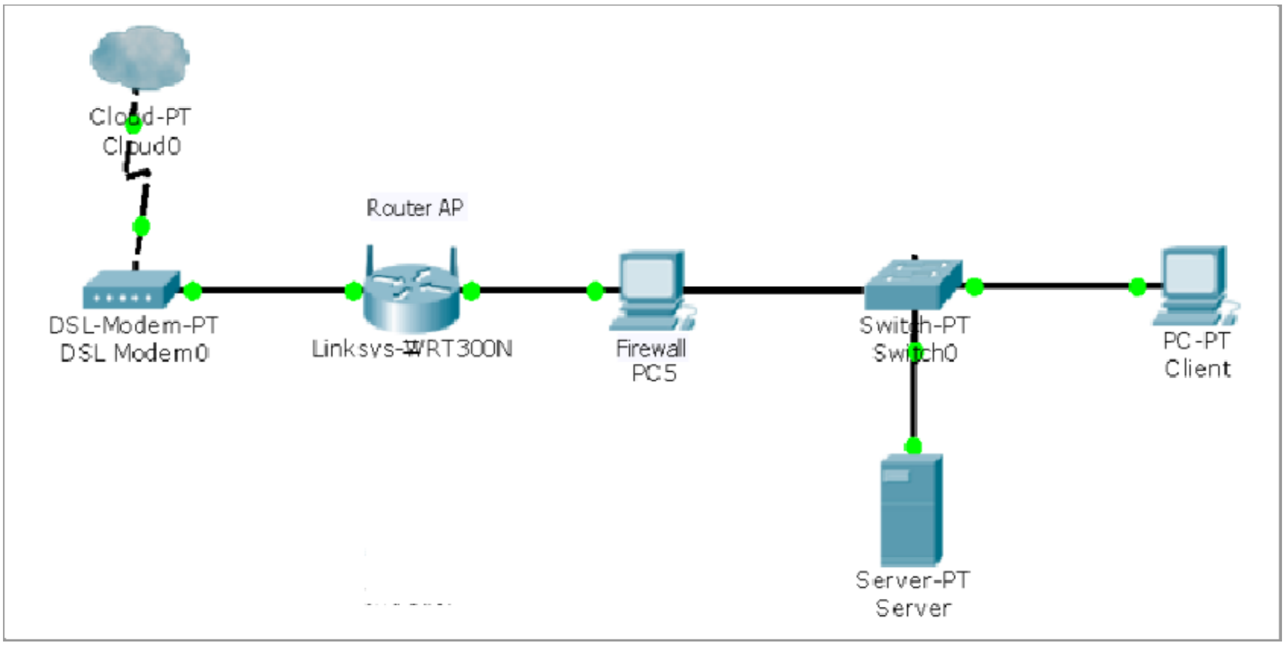

Figure 1. Network Topology Before Implementing IDS

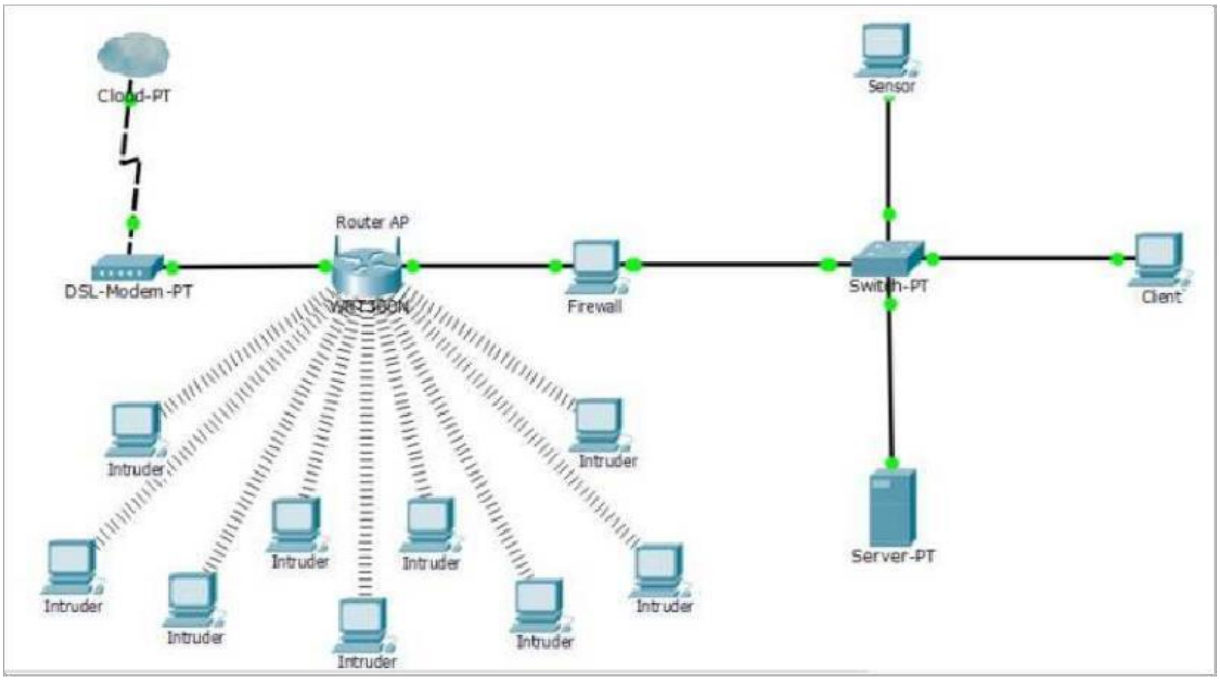

Figure 2. Network Topology After Implementing IDS

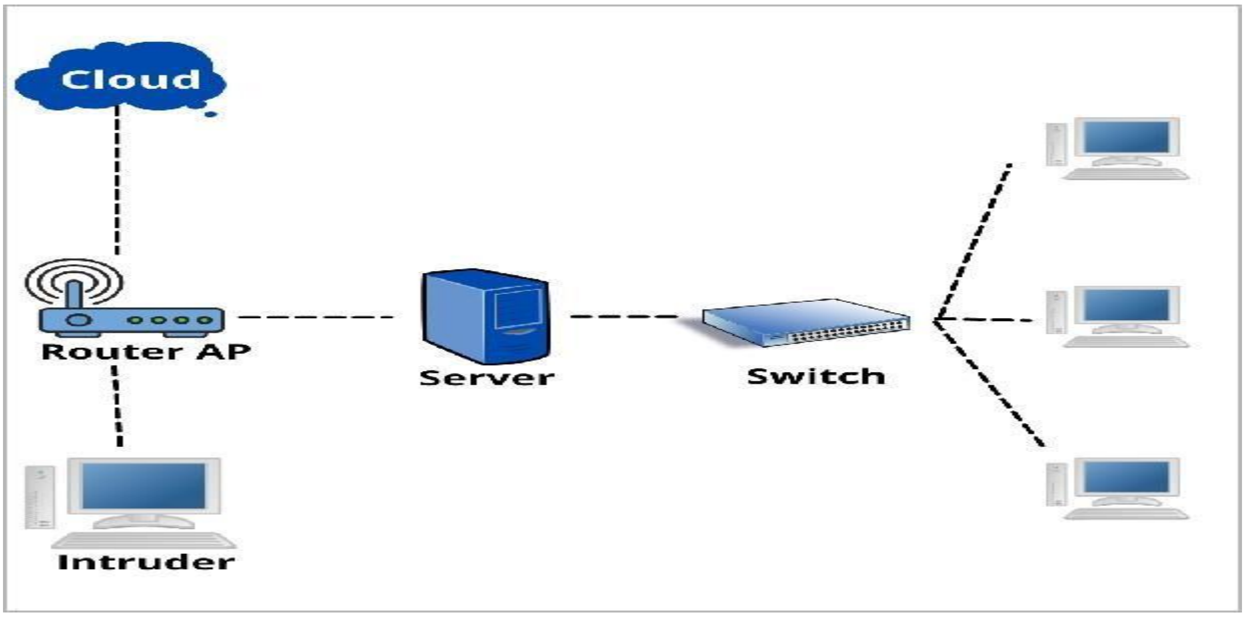

Figure 3. Network Topology Implementation

4. Findings and Conclusion:

This chapter explains how to put in place an open source IDS and Snort-based network security monitoring system.

Testing SNORT as Basic rules are used in Snort testing on the Sensor engine (as a representation of the description of particular types of attacks) to guarantee that Snort can recognize them. Start Snort with the following command if you want to report the results directly to the console screen: Snort -c eth0, -I /etc/snort/snort. Confb.

BASE Evaluation We evaluated the functioning of ACID-BASE by accessing and exporting the entire ACID-BASE system. As a result, the ACID-BASE has been successfully deployed and is able to track all network traffic and display snort events. Inter connect functionality for IDS Case studies can be used to assess the server protection capabilities of IDS systems.

CONCLUSIONS

5. Conclusions and Advice:

As a consequence of the thorough investigation that followed the argument that was detailed, the following conclusions were made:

1. The IDS system analyzes numerous sources and network traffic to find threats.
2. The functional principles of the BASE and Snort systems, which have been successfully deployed. The snort and ACID systems were put to the test using Ping attack and Digital Blaster.
3. It is possible to use iptables as a defense against assaults. Create an iptable rule that limits traffic based on IP address to protect your network against intruder attacks like ping attacks on servers.
4.To assess the connectivity between the application and the sensor engine, the approach of documenting the operations is utilized.

5.Once the IDS implementation process has been completed in its many parts, it is easy to implement. According to the results of utilizing this IDS, only a machine or computer that functions as a sensor in the network and has access to all of its events may monitor a computer network.

Suggestions:

The analysis of the attack detection system's effectiveness using WIDS led to the following recommendations. The wireless network security system should be stacked with WIDS, especially for the early detection of attacks. To counter risks to the security of wireless networks, we were employing sophisticated testing procedures.

Acknowledgment

I want to express my sincere appreciation al l the people and groups who made a substantial contribution to the effective design and analysis of our wireless network k security system, which makes use of a Wireless Intrusion Detection System (WIDS). This project represents the culmination of many efforts, and it would not have been possible without the help and direction the outstanding people.

First and foremost, I would like to extend my sincere gratitude to [Advisor's Name], my academicadvisor, whoseuflinching support and knowledge have been crucial to this effort. Critical advice, direction, and encouragement from [Advisor's Name] helped to define the course of our research. Their dedication to this undertaking and to my academic development has been nonexistent.

References

[1] [6] "Po TS: Proof of Tunnel Signature for Certificate Based on Block chain Technology," International Journal of Cyber and IT Service Management, vol. 1, no. 1, pp. 101-114, 2021. D. Immaniar, N. Azizah, D. Supriya nti, N. Septiani, and M. Hardini.

[2] Block chain Technology: Can Data Security Change Higher Education Much Better? [7]M. Mulyati, I. Ilamsyah, A. Aris, and M. S. Zahran, "Block chain Technology: Can Data Security Change Higher Education Much Better?," International Journal of Cyber and IT Service Management, vol. 1, no. 1, pp. 121–135, 2021.

[3] [8]T. Nurhaeni, S. Watini, and L. Meria, "Development Of Village Office Service Models To Community Based On Mobile Computing," International Journal of Cyber and IT Service Management, vol. 1, no. 2, pp. 189-196, 2021.

[4] "CRM-Based E-Business Design (Customer Relationship Management) Case Study: Shoe Washing Service Company,"