Final Report for Professional Diploma in Cybersecurity Capstone Project

Student Name: Maigari Timothy

Student ID: IDEAS/24/45176

Project Title: Network Security (Development of a Network Intrusion Detection System [NIDS])

Date: September 12, 2024

Instructor: Dr. Nasir B.A / Mr. Victor Idonor

1. Introduction

1.1 Project Overview

In today's connected world, almost everyone relies on the internet for essential activities such as bill payments and bank transfers. However, attacks on home networks are increasingly common, as the widespread connectivity allows attackers to exploit vulnerabilities. Cybercriminals and amateur hackers alike take advantage of this environment, often using various techniques to gain unauthorized access—either through virtual "front doors" by establishing connections or employing social engineering to steal user credentials. When an attack occurs, conducting a thorough and organized analysis is crucial to identify its causes and extent, minimize network downtime, and ensure uninterrupted business operations.

This project addresses the pressing need for network security by developing a functional Network Intrusion Detection System (NIDS) that monitors traffic for signs of intrusion, such as DoS, DDoS attacks, port scanning, unauthorized access, and brute-force attempts. Designed to analyze traffic in real time, the system raises alerts upon detecting malicious activity, offering a practical tool for protecting organizational networks from potential threats.

1.2 Background

As cyber threats become increasingly complex, the need for effective network security solutions has never been more critical. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, port scanning, and unauthorized access are among the most prevalent threats that organizations face. These attacks can cause significant damage, ranging from system downtime to data breaches. Industry reports highlight the growing frequency of these attacks, with over 10 million DDoS attacks reported globally in 2022 alone (Jacob, 2023) .

According to Kazienko and Dorosz (2003), an Intrusion Detection System (IDS) is a defense mechanism designed to detect hostile activities within a network. Without proper detection and prevention, systems are vulnerable to compromise. A key benefit of IDS is its ability to monitor unusual or unscrupulous activities, providing critical insights into network security. As

Amoroso (1999) defines, intrusion detection is “a process of identifying and responding to malicious activity targeted at computing and networking resources.”

Despite the use of firewalls and antivirus programs, computers can remain susceptible to unauthorized access. Incorporating a network intrusion detection and prevention system adds another layer of defense against potential hackers. Unlike standard firewall technology, Intrusion Detection and Prevention Systems (IDPS) not only control access but also detect unauthorized entries, integrating access control with detection measures.

There are four types of intrusion detection systems. A network-based detection system, often used on virtual private servers, remote access servers, and routers, analyzes various network protocols (Sturmer, 2013). A wireless intrusion detection system functions similarly, but specifically protects wireless networks (Adams). Host-based systems operate on individual computers, monitoring changes in the file system, unusual network traffic, and irregular application processes (Sturmer). Finally, network behavior analysis detects irregularities in system behavior and monitors traffic flow (Seehorn).

There are two main types of intrusions:

1. **Internal Intrusions**: These originate from within the network, often involving insider threats from trusted individuals.

2. **External Intrusions**: These come from outside the organization, typically over the internet.

Internal attacks can be particularly damaging, as attackers leverage trust and local access. Restricting these trusted users too closely can inhibit business operations. As the number of internal intrusions rises, organizations face increasing challenges in protecting sensitive data while adhering to regulatory compliance requirements.

Magalhaes (2003) provides the following statistics on IDS usage and challenges:

- Nearly 90% of interconnected networks that utilize IDS detected security breaches in the past year, despite multiple firewalls being in place.
- The Computer Security Institute (4/7/02) reported that 80% of surveyed organizations suffered financial losses exceeding $455 million due to intrusions and malicious acts.
- Millions of jobs have been affected by security breaches.
- Only 0.1% of companies allocate an adequate budget for IDS.
- IDS is frequently mistaken for, or assumed to be a substitute for, firewall technology.

An IDS serves as an additional layer of defense alongside antivirus software, providing essential security that many organizations find crucial.

This project addresses these issues by developing an IDS to detect and respond to common attack vectors in real time.

2. Methodology

2.1 Research Process

Methodology is known as the way a process or procedure used during the delivery of a project.

Research for the project was done by discussion between the developer and the client. The methodology used in this project is iterative development model. All phases in System Development Life Cycle are included in iterative development. Phases in iterative development model are:

- Planning – To plan what is needed to be done to make sure this system can be implemented on time.
- Analysis & Design – To determine the problem and solution.
- Implementation – To take the solution and implement it. Building the system.
- Deployment - Install the system and provide user manual, training and maintenance.

· Testing - Testing is conducted to make sure that each unit meets the user's requirement.

· Evaluation – Does the system follow the standards given?

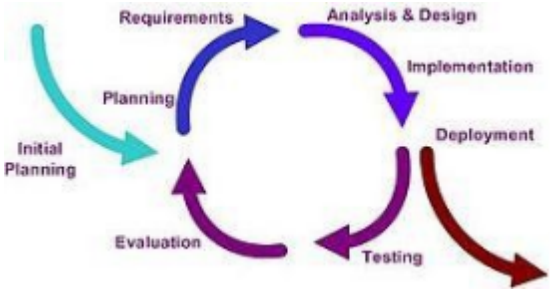

Figure 1: Iteration Development Model

Below are the project activities involved in developing Network Intrusion Detection System:

Planning is conducted during the early stages to determine the purpose of the system and the needs of the potential user.

Design of the system was done after the requirement has been identified by the developer based on the planning stage.

Construction (implementation) of the system was made with code from the design stage.

Testing of the system was conducted in the testing stage to determine if the system meets the requirement gathers during the early part of the development.

Evaluation is the stage whereby testing is conducted on the system based on the requirement.

Deployment will be conducted after the system meets the requirements and if there is no additional requirements.

2.2. Use Case Diagram

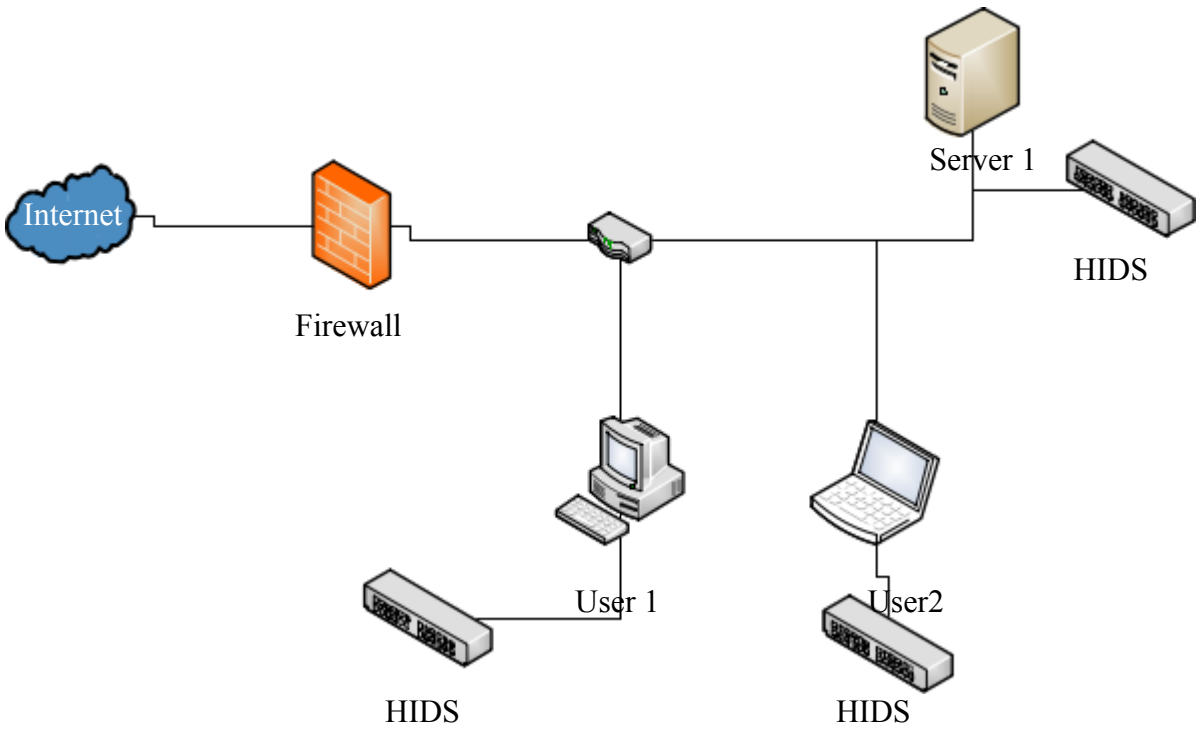

Figure 2: Detailed network diagram of HIDS location

Figure 2 shows an example of deployment of host-based intrusion detection system in a network layout. This system will be installed in each of the host computers in a network system. It will detect any anomaly that is going into the host computers through the given rules.

Figure 3: USE Case diagram for Intrusion Detection System

1) Anomaly Detection

If Intrusion Detection System detects any abnormality in the network traffic, then it triggers the alert system

2) Signature recognition

Intrusion Detection System examines the traffic looking for well-known patterns of attack, which are saved in pattern database and triggers the alert system, if a match is found.

3) Alert System

Whenever triggered by anomaly detection or signature recognition, it alerts the system administrator.

2.2 Development Process

The system was developed using Python as the primary programming language. The Scapy library was used to capture and analyze network packets, while PyGame was integrated to provide audio alerts. The bcrypt library was utilized to secure user credentials with encryption. Tkinter was used to create the system's graphical user interface (GUI), which allows for the setting of thresholds, exporting logs, and starting or stopping the IDS.

The system also implements a brute-force protection mechanism by locking the system after three failed login attempts, with alarms raised for critical intrusions such as DoS/DDoS attacks.

2.3 Challenges and Solutions

One of the primary challenges encountered during the project was managing real-time packet sniffing without impacting system performance. This was resolved by utilizing Python's multi-threading capabilities to ensure the IDS could operate in the background without slowing down the main application. Another challenge was managing multiple attack detection patterns within the same framework. The solution involved modularizing the detection algorithms for scalability.

3. Results

3.1 Findings

The developed IDS successfully detected and logged intrusions, including DoS, DDoS, and port-scanning attacks. Below is an example of how the IDS reacts when a DDoS attack is detected:

Python Copy code Sample

```
def detect_dos_ddos(packet):
    if packet.haslayer(IP):
        src_ip = packet[IP].src
        packet_count[src_ip] += 1
        if packet_count[src_ip] > DOS_THRESHOLD:
            alert = f"[ALERT] Possible DoS/DDoS attack from {src_ip}"
            log_alert(alert, critical=True)
```

The system also successfully secured login credentials and prevented unauthorized access after multiple failed attempts.

3.2 Analysis

The IDS prototype met the objectives outlined in the project proposal. The system's real-time detection capabilities allowed for immediate response to intrusions, mitigating potential harm. The modular design of the detection

algorithms ensures that future attack patterns can be integrated with minimal system modification. While the IDS was not tested on a large-scale enterprise network, the findings indicate that the system performs well in smaller environments.

4. Discussion

4.1 Implications

This project contributes to the field of cybersecurity by providing a scalable, lightweight solution for detecting network intrusions. The open-source nature of the tools used allows for the IDS to be further developed and customized for different security needs. It also underscores the importance of real-time threat detection in preventing successful attacks.

4.2 Limitations

The main limitation of this project was the restricted network environment used for testing. Larger networks may have different traffic patterns, which could impact the accuracy of intrusion detection. Additionally, the system currently focuses on signature-based detection, which may not catch sophisticated or zero-day attacks that rely on novel techniques.

4.3 Future Work

Future research should focus on enhancing the IDS by incorporating machine learning algorithms to improve its ability to detect unknown threats. Additionally, deploying the system on a larger network will provide a more comprehensive evaluation of its scalability and effectiveness.

5. Conclusion

5.1 Summary

This project developed a Network Intrusion Detection System to detect and respond to network-based threats such as DoS, DDoS, and unauthorized access. Python and various open-source tools were utilized to create a scalable and effective solution. The project met its objectives, providing a functional prototype that could be expanded in the future.

5.2 Final Thoughts

Working on this project deepened my understanding of network security and the practical application of cybersecurity tools. It also highlighted the ongoing challenges organizations face in protecting their networks from ever-evolving threats. Moving forward, I aim to expand my knowledge in this area, particularly in developing more advanced detection techniques using machine learning.

6. References

- Simplilearn. (2021, April 12). *What Is Network Security? | Introduction To Network Security* [Video]. YouTube. https://youtu.be/NQ1cvwEvh44
- Dörk, K., Domingues, C., Murta, L., & Fortes, R. (2022). *Case Studies on DoS and DDoS Attacks: Strategies for Mitigation.* Springer.
- *Scapy Documentation.* (n.d.). https://scapy.readthedocs.io
- *bcrypt Documentation.* (n.d.). https://pypi.org/project/bcrypt/
- Violino, B. (2022). "DDoS Attacks: What You Need to Know." *CSO Online*. https://www.csoonline.com
- Jacob. (2023, December 8). *Top cybersecurity statistics for 2024*. Cobalt. https://www.cobalt.io/blog/cybersecurity-statistics-2024
- Adams. (n.d.). *Wireless intrusion detection systems*. [Publisher or Source information if available].
- Amoroso, E. (1999). *Intrusion detection: An introduction to Internet surveillance, correlation, traps, trace back, and response*. Intrusion.Net Books.
- Kazienko, P., & Dorosz, P. (2003). Intrusion detection systems (IDS) as a network security technology. *Proceedings of the International Conference on Information Technology (ICIT)*, 2003, 1–4.

- Magalhaes, M. (2003). *Statistics on the effectiveness of intrusion detection systems*. [Publisher or Source information if available].
- Seehorn, R. (n.d.). *Network behavior analysis and intrusion detection*. [Publisher or Source information if available].
- Sturmer, S. (2013). *Types of intrusion detection systems and their applications*. [Publisher or Source information if available].