Capstone Project Proposal

Student Name: Maigari Timothy

Student ID: IDEAS/24/45176

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

Date: September 11, 2024

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

1. Project Overview

Objective:

The main purpose of this project is to develop a prototype Network Intrusion Detection System (NIDS) that monitors the network traffic in order to identify anomalies, detects attacks or intrusion(e.g: DoS/DDoS/Port scan/A brute force login attempt), and raise alarms when suspicious activities are happening or being detected. The system will be developed using Python, and have the Key network security feature integrated for creating real-time detection.

Problem Statement:

Due to the increase of network attacks, organizations are continuously being faced with the challenge of protecting their networks from Integrity Breaches, Confidentiality and/or Denial-of-services. Traditional security systems like firewalls and antivirus are not good enough to defend or detect advanced attacks on an immediate basis. The aim of this Project is to design an Intrusion Detection System which can detect intruders, trigger alerts and log the intrusion attempts so as to prevent further security breaches.

Scope:

The scope of my project will cover the following aspect:

- Detection of DoS/DDoS attacks, port scans, brute-force attacks, and unauthorized network access.
- Development of an alerting mechanism that logs events and notifies administrators.
- Implementation of a graphical user interface (GUI) for easy interaction with the NIDS.
- Real-time monitoring of network traffic using Python and Scapy.

This project will not cover large-scale enterprise networks, use of machine learning(ML) algorithms will not be implemented due to time constraints and resource availability.

2. Methodology

Research Approach:

For me to be able to work on the Network Security and build a Network Intrusion Detection System (NIDS), I will begin by going through some literature to get an understanding on what people have written or made research on in relation to Network Security and NIDS. I will also need to watch some YouTube videos to get a clearer understanding on Network Security and its challenges. I need to understand the methods and protocols being used on traditional antivirus and firewall and see how I can improve their flaws with the IDS I am developing. I will have to study cases of real world attacks as this helps me to get a pattern on previous network intrusion which will be of great help in developing my app. And lastly, I will have to perform an experiment on the app on a small scale network so that I can be able to calibrate the thresholds for different attack types incorporated in the app.

Tools and Technologies:

- **Python**: For the development of NIDS, I will be using the python programming language because of its flexibility and simplicity of use.
- **Scapy**: For packet sniffing and analysis scapy will be a great package to use.
- **tkinter**: For creating the graphical user interface to make it easy to use, I will use the python graphical UI package, Tkinter.
- **bcrypt**: Bcrypt will be used for encrypting user login data.
- **PyGame**: In a situation where an IT staff is not close to see the alert box of an intrusion, PyGame will be used to play an alert sound.
- **Wireshark**: Wireshark will be used to analyze network traffic and validate detection mechanisms.

Project Plan:

1. **Week 1**: Research and gather information on network attacks, develop the core NIDS functions, and implement packet sniffing and detection mechanisms.
2. **Week 2**: Integrate user authentication, develop the alerting system, and build the GUI.
3. **Week 3**: Test the system with various network attack scenarios, debug, and finalize the prototype.

3. Expected Outcomes

Deliverables:

- A functional NIDS prototype that detects and alerts on common network intrusion attempts (DoS/DDoS attacks, Port Scanning and Unauthorized Access).

· A GUI for administrators to interact with the system, configure thresholds, and view logs.

· A final project report documenting the system's architecture, design, and performance.

Impact:

The NIDS prototype will demonstrate an effective approach to detecting network intrusions, addressing the increasing need for real-time cybersecurity solutions. It will provide a solid foundation for understanding and combating network-based attacks and can serve as a model for future development and enhancements.

References

Ahmed, N. B. (2024). *CYBER SECURITY*. YouTube. https://www.youtube.com/playlist?list=PLdSKJ_83-bQxmcmDrdwzjyKYKjLHo5gAU

Goyal, P., & Deshmukh, M. (2017). *Python network programming cookbook* (2nd ed.). Packt Publishing. https://www.packtpub.com/product/python-network-programming-cookbook-second-edition/9781786463999

Gu, G., Porras, P., Yegneswaran, V., Fong, M., & Lee, W. (2007). *An overview of DDoS attacks and defense mechanisms*. Penn State University. https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf

Python Software Foundation. (n.d.). *bcrypt documentation*. PyPI. https://pypi.org/project/bcrypt/

SecDev. (n.d.). *Scapy documentation*. Scapy. https://scapy.net/

Simplilearn. (n.d.). *What is network security? | Introduction to network security | Network security tutorial*. YouTube. https://youtu.be/NQ1cvwEvh44

Simplilearn. (2021). *What is Wireshark? | What is Wireshark and how it works? | Wireshark tutorial 2021*. YouTube. https://youtu.be/Lb-PJl9u3z8