International Institute of Information Technology Hyderabad

System and Network Security (CS5.470)

Lab Assignment 3:
Signature and Anomaly-based Intrusion Detection and Prevention System (NIDPS)

Hard Deadline: 7 April 2025, Monday (23:59 PM)
Total Marks: 100

Note:- *It is strongly recommended that no group is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both parties will be given zero marks without any compromise. The rest of the assignments will not be evaluated further, and assignment marks will not be considered towards final grading in the course. No assignment will be taken after the deadline.* ***You can use C, C++ or Python programming language for implementation. No other programming language implementation will be accepted.***

Introduction

This assignment involves developing a Network-based Intrusion Detection System (NIDS) using Python or C++. The IDS should detect malicious activities through signature and anomaly-based detection techniques, log detected attacks, and provide a CLI-based interface for management and monitoring. Additionally, it should integrate basic intrusion prevention by dynamically blocking identified threats.

Assignment Requirements

1. Network Traffic Monitoring [Marks: 10]

- Utilize libraries like Scapy or libpcap to capture and analyze live network traffic (TCP packets).
- Monitor incoming and outgoing connections.
- Capture relevant packet information, including timestamps, source/destination IPs, protocols and ports.

2. Intrusion Detection Module [Marks: 30]

Create a detection engine using signature-based and anomaly-based detection methods.
Implement rules to detect various attack patterns, such as:

1. **Port Scanning Detection**
    - Identify hosts that attempt to connect to more than 6 different ports within 15 seconds.
    - Sequential port accesses from the same IP are flagged.
    - Log the attacker's IP address and targeted ports.
2. **OS Fingerprinting Detection**
    - Detect an IP that sends 5 different SYN, ACK, and FIN flag combinations within 20 seconds.
    - Log the IP address and the type of fingerprinting attempt.

3. Intrusion Prevention Mechanism [Marks: 20]

- Implement a prevention mechanism using iptables (Linux) or Windows firewall commands.
- Dynamically block malicious IPs upon detection.
- Provide an option to manually unblock previously blocked IPs.

4. Alert and Logging [Marks: 20]

- Maintain a log file (`ids.log`) with detailed records of detected intrusions.
- Log format:

    Date(DD-MM-YY) Time(HH::MM:SS) — Intrusion Type — Attacker IP — Targeted Ports/Flags — Time Span Of Attack

- Display a summary report of detected intrusions upon request.

5. Management Interface [Marks: 10]

Create a command-line interface (CLI) that provides the following functionalities:

- Start/Stop IDS
- View Live Traffic
- View Intrusion Logs
- Display Blocked IPs

- Clear Block List
- Unblock an IP
- Exit

Submission Requirements

Submit a zipped file named `_<team_number>_lab3.zip` containing:

- **Source Code files**
- **Documentaton / README [Marks: 10]**
  (with setup instructions of how to build and how to run each program and explanations of the implementation steps, input and outputs)
- Log file **(`ids.log`)** (with detected intrusions)