**Penetration Test Report: Intrusion Detection and Prevention Script**

**Introduction:**

This penetration test report documents the development and testing of an Intrusion Detection and Prevention System (IDPS) script. The purpose of this script is to monitor network traffic and block unwanted or unknown traffic originating from potentially malicious IP addresses. The script was tested using Nmap network scanning from a Windows 11 Machine to simulate an attacker's reconnaissance phase.

**Scope:**

* **Target System:** Windows 11 (Simulated environment)
* **Testing Environment:** Kali Linux (Intrusion Prevention Host)
* **Tools Used:** Python (for the IDPS script), Nmap (for scanning), iptables (for traffic blocking)
* **Objective:** Identify and block unauthorized network scans and intrusions from malicious IPs.

**Methodology:**

1. **Reconnaissance Phase:**
   * Used **Nmap** from the Metasploitable VM to scan the target's network.
   * Commands executed:

* Nmap -sS -p- <Target-IP>
* Nmap -sS -A <Target-IP>
* Nmap -sS -p 80,22,21 <Target-IP>
* **Purpose**: Simulate an attacker's attempt to gather information about open ports and services.

Detection and Logging:

* The Python-based IDPS script was set up to monitor network traffic.
* Suspicious activities were logged when unknown or unwanted IPs initiated network scans.

**Prevention Mechanism:**

* The script automatically blocked identified malicious IPs using iptables rules:
* **sudo iptables -A INPUT -s <Malicious-IP> -j DROP**
* The script was configured to notify the user upon blocking a potential attacker’s IP.

**Findings:**

|  |  |  |  |
| --- | --- | --- | --- |
| Scan Type | Source IP | Detection Status | Action Taken |
| SYN Scan (-sS) | 192.168.70.78 | Detected | Blocked via iptables |
| OS Detection (-A) | 192.168.70.78 | Detected | Blocked via iptables |
| Full Port Scan (-p-) | 192.168.70.78 | Detected | Blocked via iptables |
| Single Port Scan (-p) | 192.168.70.78 | Detected | Blocked via iptables |

* The script successfully detected Nmap scans originating from the Windows 11 Machine and blocked the attacker’s IP dynamically.
* Logs were generated and stored for further analysis.

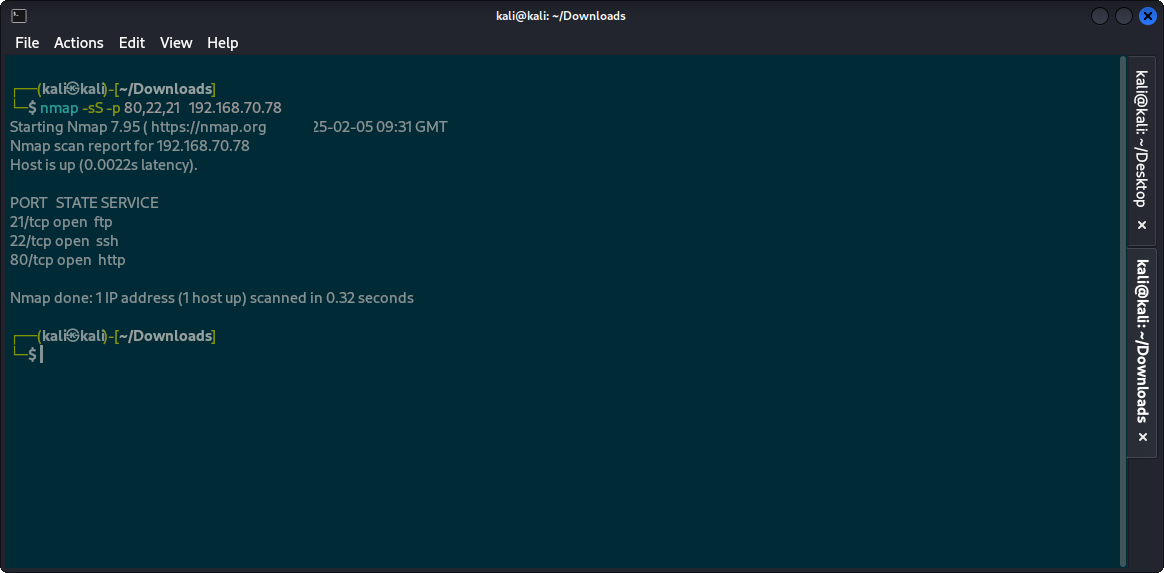
**Recommendations:**

1. **Enhance Logging:**
   * Implement centralized logging (e.g., using ELK Stack or Splunk) for better monitoring.
2. **Automate Threat Intelligence:**
   * Integrate a threat intelligence feed to detect known malicious IPs.
3. **Improve Whitelisting:**
   * Ensure that legitimate users are not mistakenly blocked.
4. **Extend Functionality:**
   * Add email or SMS notifications for critical alerts.

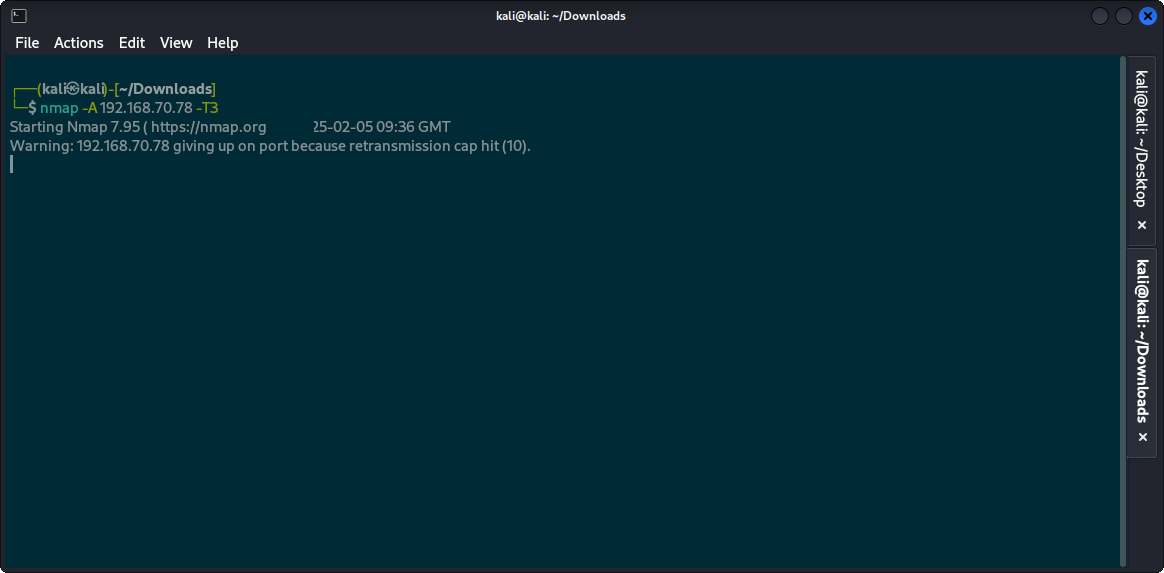
**Conclusion:**

The Intrusion Detection and Prevention script effectively identified and blocked unauthorized scanning attempts from an attacker's IP. Further improvements can be made by integrating machine learning for anomaly detection and automating response mechanisms. This proof-of-concept demonstrates the importance of proactive security measures in preventing reconnaissance and intrusion attempts.

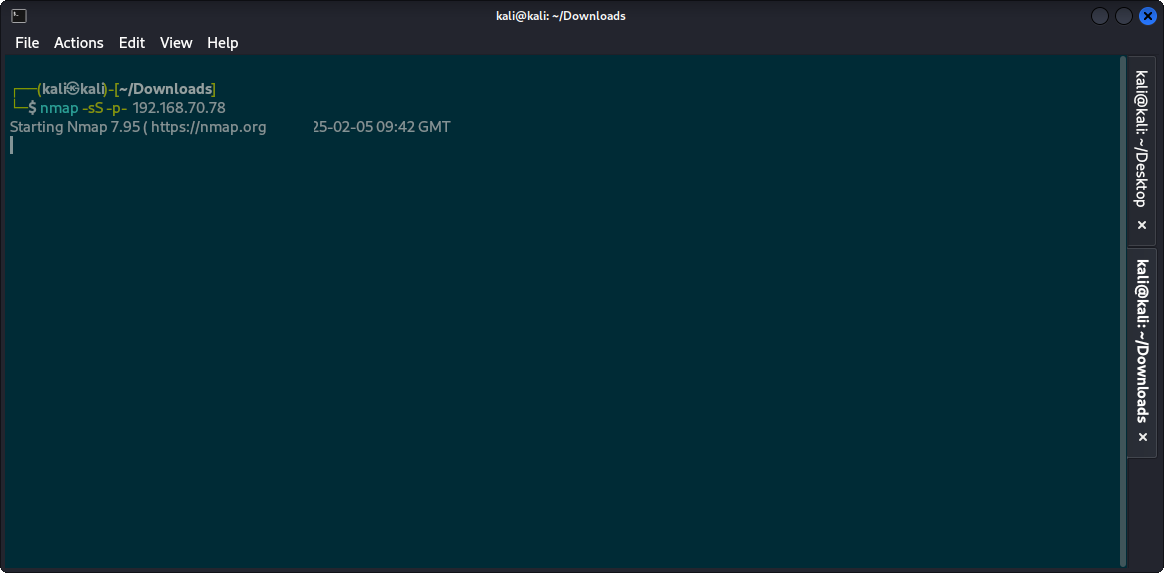
Appendix A: Sample Nmap commands used



Image\_2.png

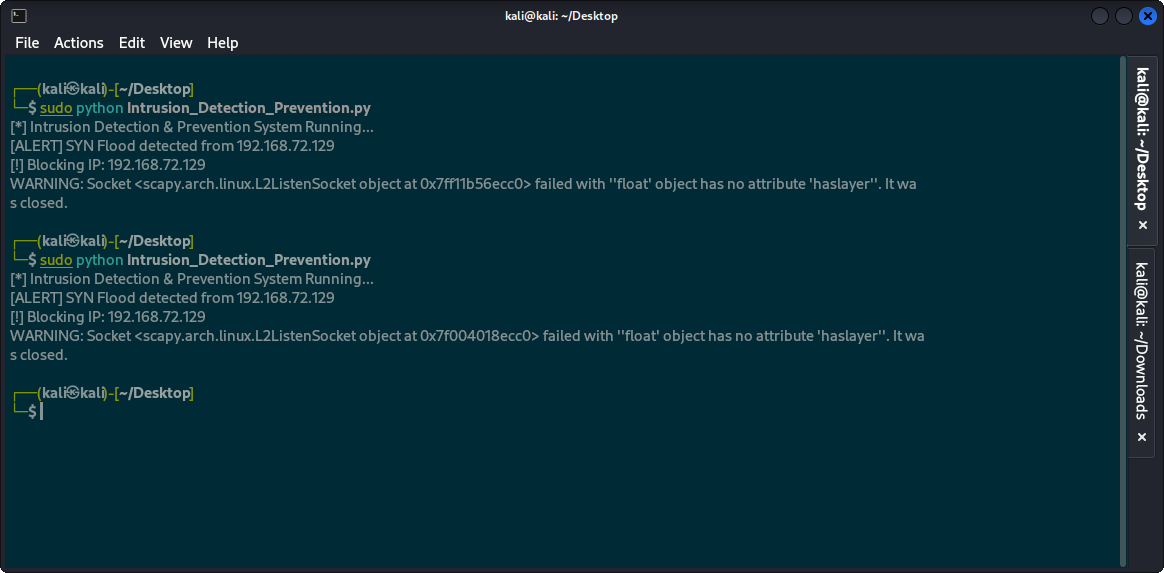


Image\_3.png



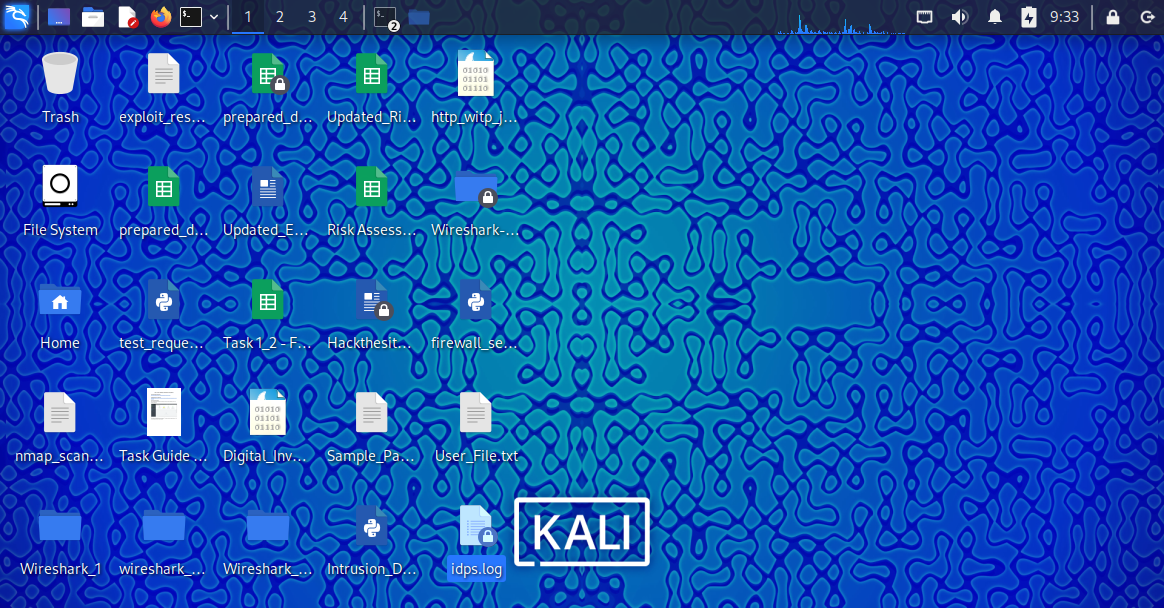
Image\_4.png

Appendix B: Sample Intrusion\_Detection\_and\_Prevention script blocking request



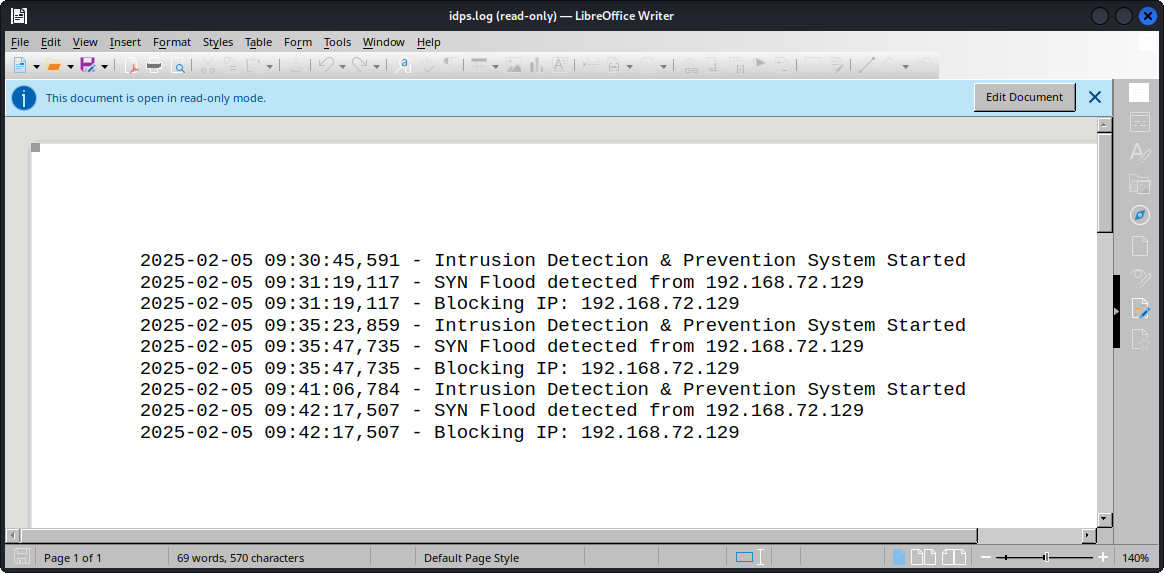
Image\_5.png

Appendix C: Sample Log File:



Image\_6.png

Appendix D: Sample Log Entries:



Image\_7.png