Project Abstract

Setting Up a Firewall Paired with Intrusion Detection and Prevention System to block malicious Traffic.

This project demonstrates the deployment and testing of an open-source firewall—OPNsense—against simulated cyber threats, specifically focusing on Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. The core objective was to understand how modern firewall systems detect, log, and mitigate such attacks using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and to assess the performance and responsiveness of these mechanisms under simulated hostile network conditions.

The testbed was built entirely using virtualization, leveraging VMware Workstation Pro to host multiple virtual machines on a single physical system. The firewall was implemented using OPNsense, an open-source FreeBSD-based firewall and routing platform known for its powerful user interface and built-in support for IDS/IPS via Suricata. The attacking machine used to simulate DDoS behavior was Kali Linux, a penetration testing distribution equipped with various offensive tools. An internal victim machine (Ubuntu) was also deployed to represent the local network being protected by the firewall.

Networking was configured using NAT mode in VMware to simulate a typical home or small enterprise network. The WAN interface of the OPNsense VM was connected to the NAT adapter, while the LAN interface connected to an internal VMware network. The attacking Kali Linux VM was also connected to the NAT interface to generate attack traffic toward the OPNsense WAN interface, simulating a real-world external attacker scenario.

Key technologies used in this project:

- OPNsense Firewall: For traffic filtering, logging, and active prevention.
- Suricata IDS/IPS: Enabled within OPNsense to detect suspicious traffic patterns and block malicious packets.
- Kali Linux: Used to launch simulated DDoS attacks (e.g., via hping3, slowloris, or custom traffic floods).
- Ubuntu Linux: Simulated a LAN-side user to confirm normal network behavior and response under attack.
- VMware Workstation: Provided an isolated and configurable lab environment.

Key features of the implementation include:

- Real-time monitoring of inbound and outbound packets via the OPNsense dashboard.
- Activation of IDS and IPS rules based on threat intelligence feeds (e.g., ET Open rules).
- Testing the effectiveness of Suricata by launching flood attacks from Kali to the OPNsense WAN interface.
- Observing how quickly the system logs were updated with alerts and whether active prevention rules dropped the packets.
- Network segmentation via NAT to isolate attacker traffic from LAN users, while still reflecting realistic Internet-like behavior.

Through this experiment, detailed observations were made regarding how quickly IDS alerts are generated, the behavior of the firewall under high-volume traffic, and the effectiveness of IPS in mitigating these threats in real time. The project provides a practical understanding of firewall configurations, rule management, and threat detection capabilities in a controlled lab setting. It also serves as a learning exercise in both network defense and offense, bridging the gap between theory and hands-on cybersecurity skills.