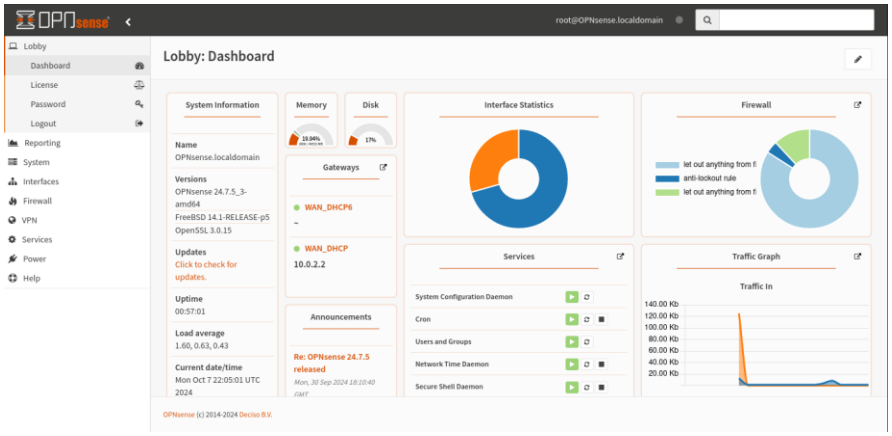
Intrusion Detection System (IDS) with OPNsense and Suricata in a Home Lab



Overview

This project demonstrates the configuration of OPNsense as a firewall and Suricata as an Intrusion Detection System (IDS) within a virtualized network environment. Using VirtualBox, OPNsense was installed and configured to monitor network traffic between a virtual LAN and WAN, detect potential intrusions (e.g., Nmap stealth scans), and log relevant alerts.

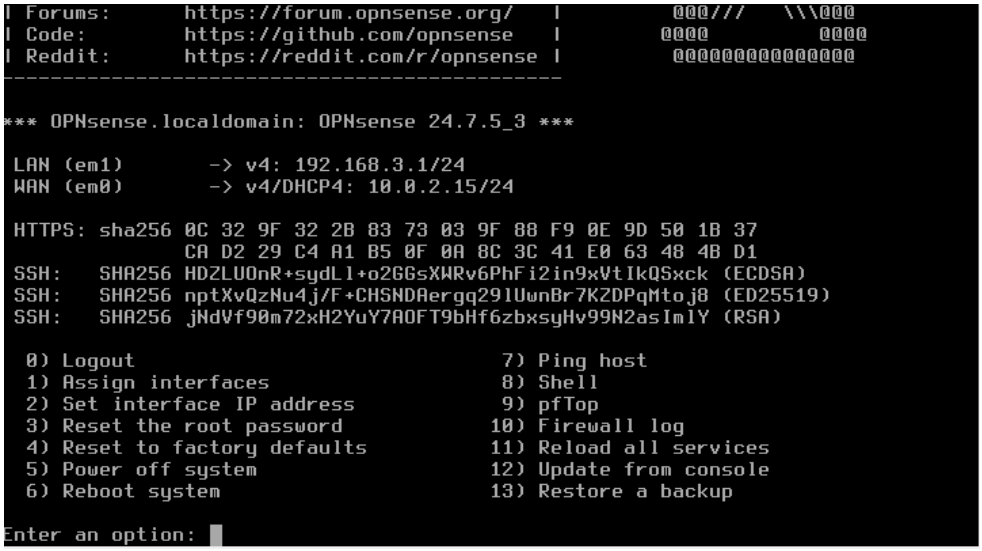
Project Setup

1. Environment Configuration:

VirtualBox was used to virtualize the environment, creating separate VMs for OPNsense and Kali Linux. OPNsense serves as the firewall and IDS, while Kali Linux is used for penetration testing.

2. OPNsense Installation:

A new virtual machine was created for OPNsense. Network Adapters were configured for both WAN and LAN interfaces. The LAN interface received the static IP '192.168.3.1/24'. This interface is used to access the OPNsense web GUI.

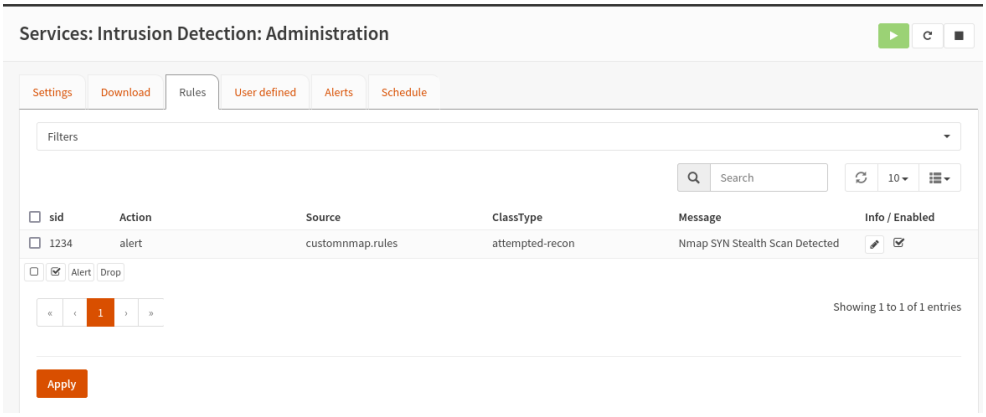


3. Accessing OPNsense Web GUI:

From the Kali Linux machine, the OPNsense web interface was accessed using the static LAN IP address '192.168.3.1'.

4. Configuring Suricata as an IDS:

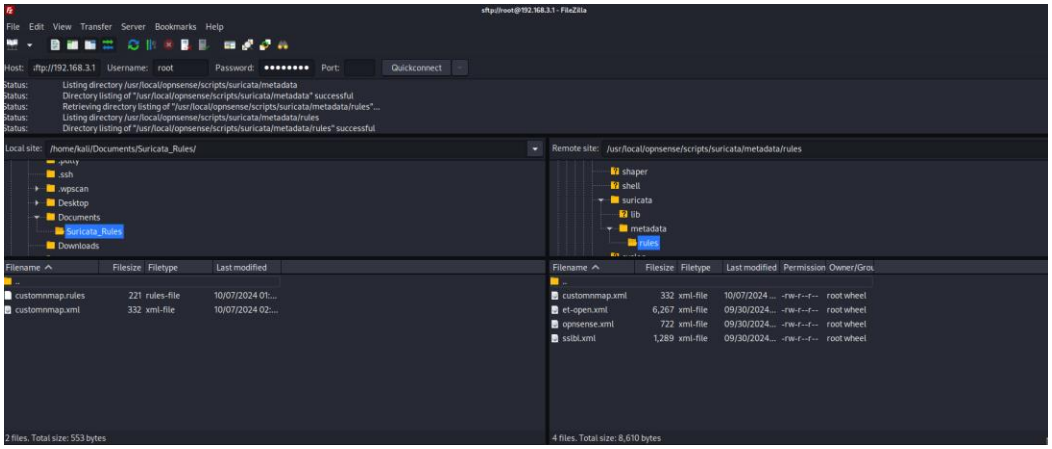
Suricata was enabled through the OPNsense web GUI. Custom Suricata rules were written to detect specific network activity, such as Nmap stealth scans.



Rule example: alert tcp any any -> any any (msg: "Nmap SYN Stealth Scan Detected"; flags:S; threshold:type both, track by_src, count 20, seconds 10; sid:1234; rev:1;)

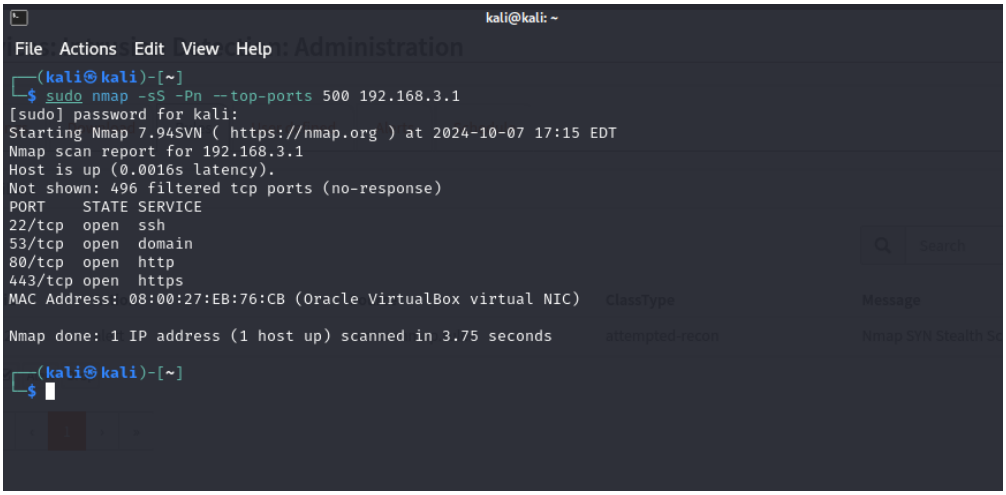
5. Uploading Custom Suricata Rules:

A custom .rules file ('customnmap.rules') was created and uploaded to the OPNsense VM using FileZilla (SFTP). The rules were uploaded to '/usr/local/opnsense/scripts/suricata/metadata/rules/'.



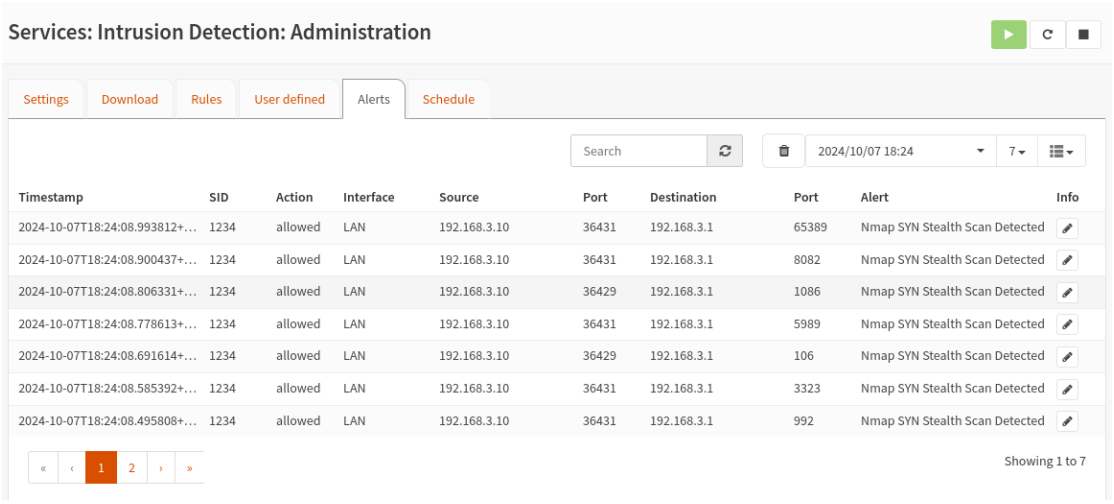
6. Penetration Testing with Kali Linux:

Kali Linux was used to simulate an attack by performing an Nmap SYN stealth scan targeting the OPNsense firewall



7. Viewing Alerts in OPNsense:

After running the Nmap scan, Suricata successfully detected the attack. Alerts were logged and could be viewed from the Intrusion Detection section of the OPNsense web interface.



Challenges and Results

Writing and testing custom Suricata rules to detect specific attacks, like Nmap SYN scans, required understanding Suricata's rule syntax. Additionally, tuning the rules to avoid false positives without missing legitimate threats was a challenge. Testing with Nmap to trigger the Suricata alerts required some adjustment in scanning parameters. At first, some scans didn't trigger the rules until thresholds for detection were optimized.

This project provided practical experience in configuring firewalls, IDS systems, and testing network security. The entire process—from setup to detection—enhanced understanding of network security monitoring.