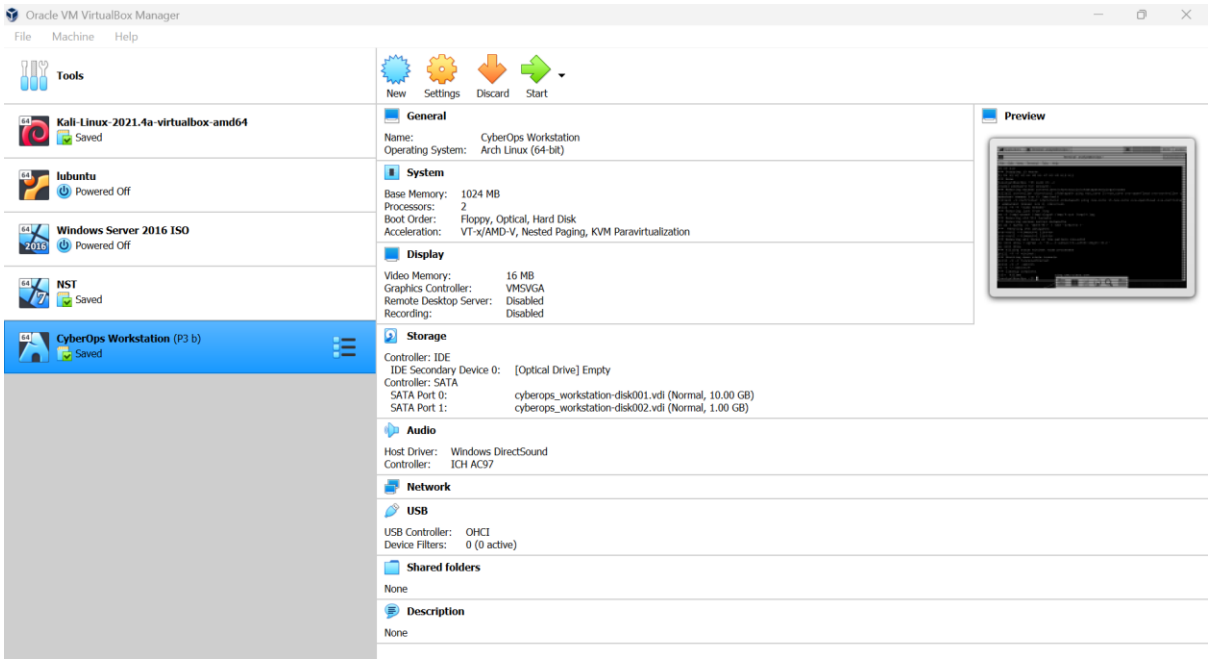
Lab: IDS monitoring with Snort and firewall rule tuning based on alerts.

Part 1: Preparing the Virtual Environment

- Virtual machines prepared in Oracle VirtualBox for the lab environment.
- Includes CyberOps Workstation and Kali Linux nodes connected via Mininet topology.

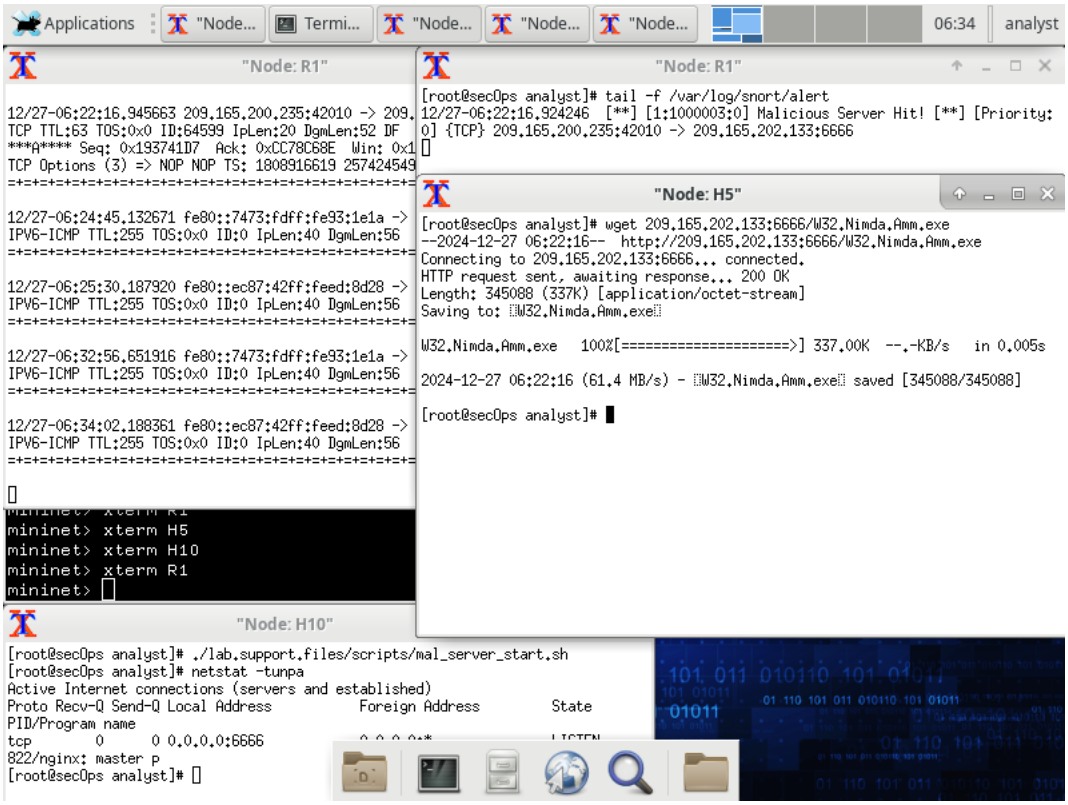


Part 2: Firewall and IDS Logs

Step 1: Real-Time IDS Log Monitoring a)- j)

- Snort configured and running on the security operations node.

- Real-time alerts captured in /var/log/snort/alert showing detection of malicious activity.



source ip add: 209.165.200.235

destination ip add: 209.165.202.133

source port: 42010

destination port: 6666

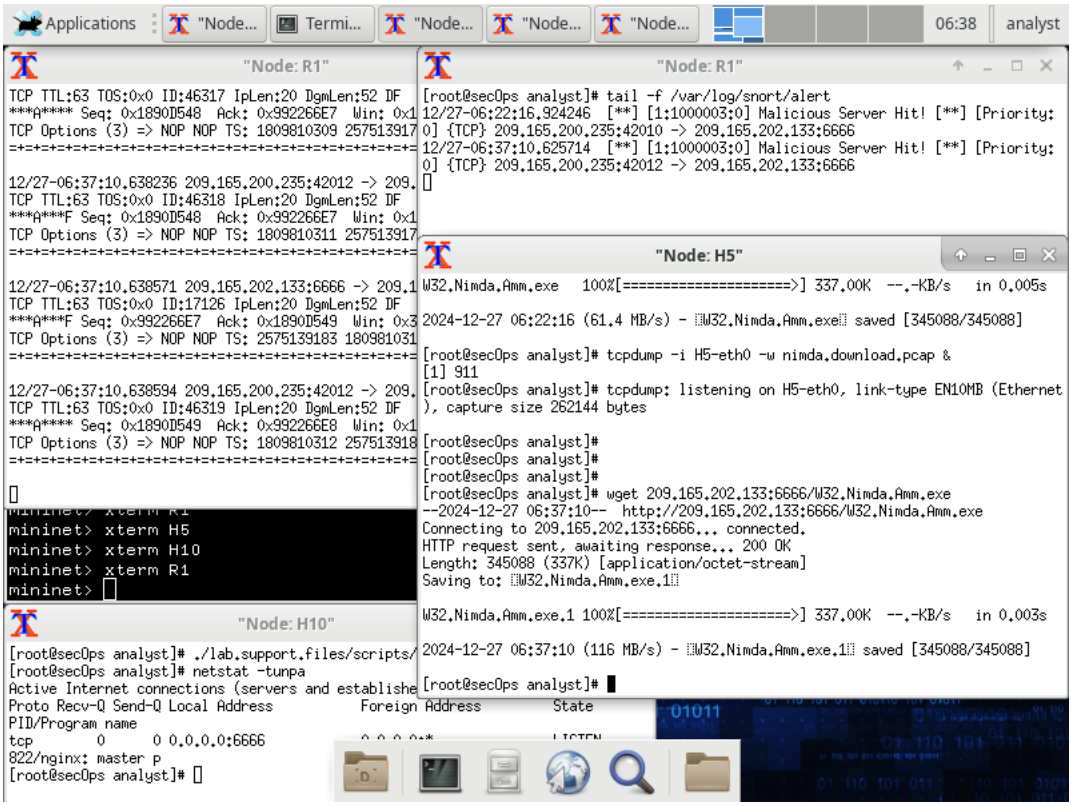
date and time: 27th Dec at 06:22:16.924246

message: Malicious Server Hit!

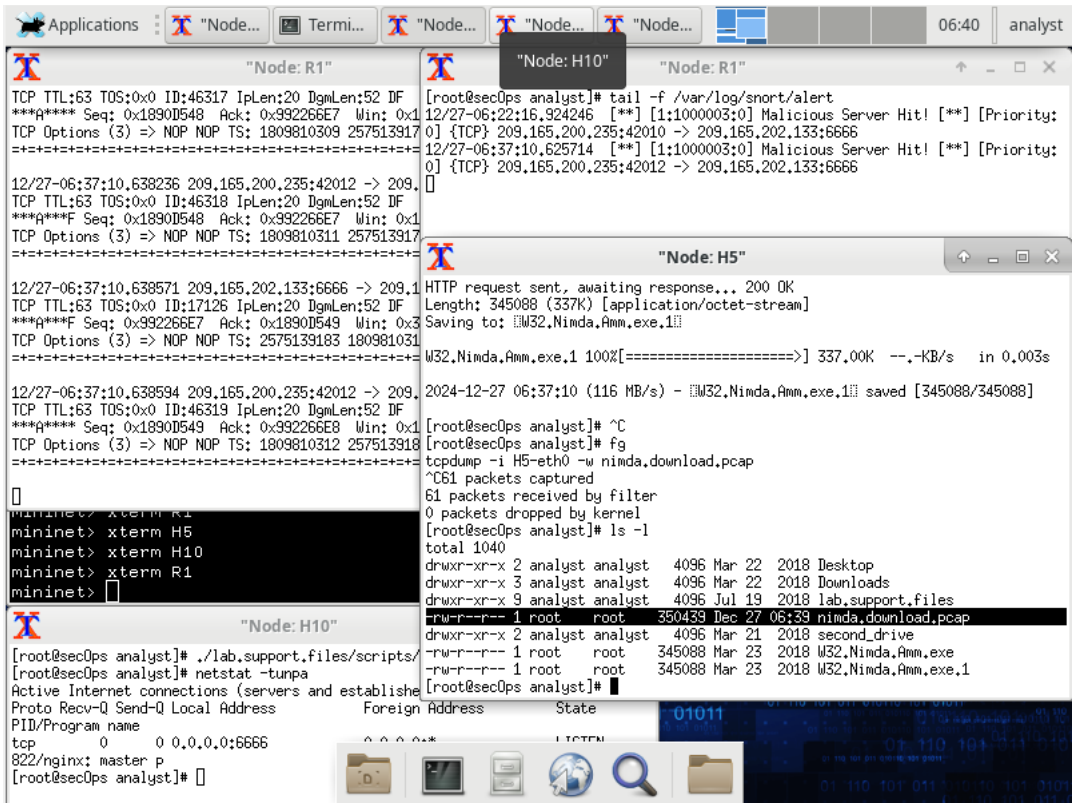
k)-l)

- Attempted download of W32.Nimda.Amm.exe from malicious server (209.165.202.133:6666) using wget.

- Snort detected and logged the activity as suspicious.



m)-n)

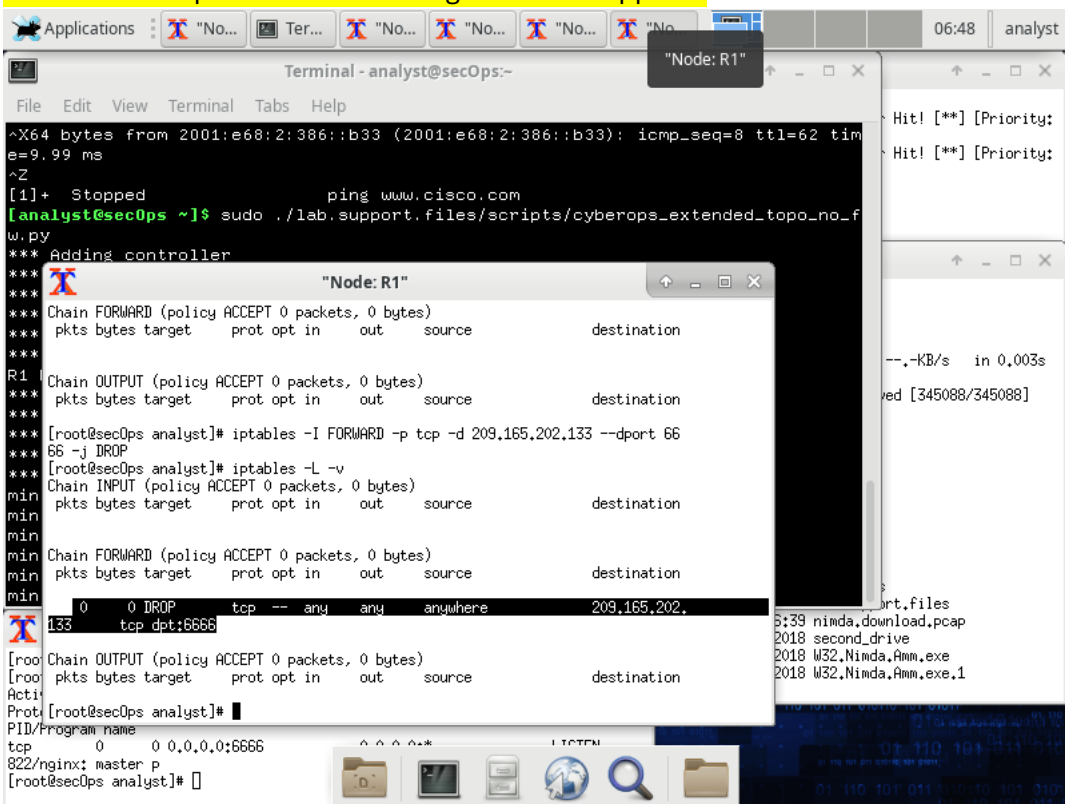


Step 2: Tuning Firewall Rules Based on IDS Alerts a)-d)

Based on IDS alerts, firewall rules were updated using iptables:

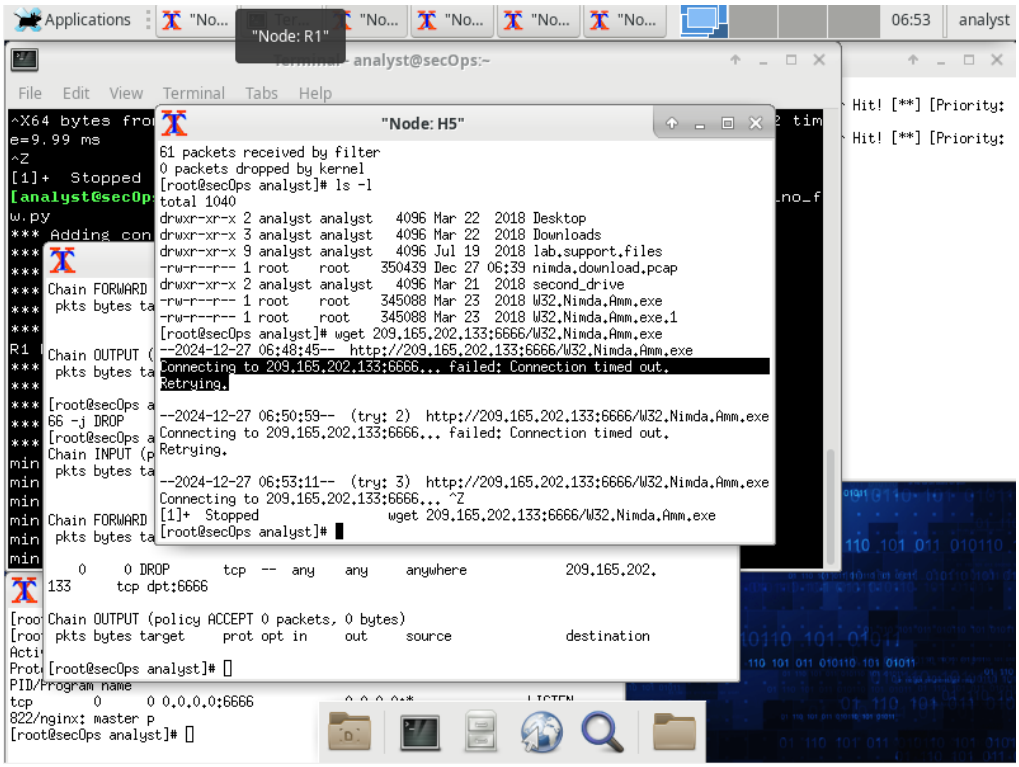
- Rule added to drop TCP traffic to destination port 6666 on malicious server IP.

- Verified with iptables -L -v showing DROP rule applied.



e) After applying firewall rule, repeated attempts to download the malicious file failed with Connection timed out.

Confirms firewall successfully blocked traffic to the malicious server.



Part 3: Terminate and Clear Mininet Process a)-b)

- Mininet processes terminated and environment cleared using cleanup commands.

- Ensures lab topology and virtual environment reset after testing.