Network Traffic Analysis for Malicious Activity Detection

Somika Kumari Ganesh

Computer Science and Information Systems

Project Goal

This research project focuses on analyzing network traffic to detect cyber threats and suspicious network activities. Using Snort, an open-source Intrusion Detection and Prevention System (NIDS/NIPS), I explored how real-time packet inspection can help identify and prevent security threats. This project was conducted using TryHackMe rooms to ensure a safe and controlled learning environment.

Procedure and Execution

Snort operates in multiple modes, each serving a different purpose in detecting malicious network activity.

➢ Sniffer Mode

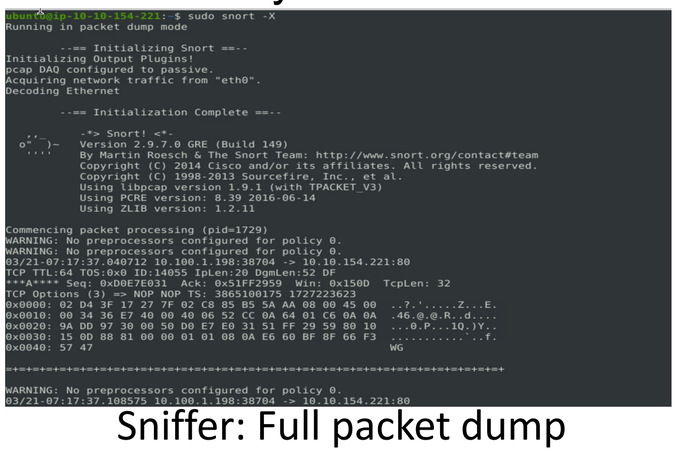
Sniffer Mode is used to inspect real-time network traffic and analyze packet structures for identifying suspicious patterns.

Commands Used:

```
sudo snort -v      # Display the TCP/IP output in the console
sudo snort -d      # Shows packet payloads
sudo snort -de     # Display link-layer headers
sudo snort -X      # Full packet dump in HEX format
```

Results:

Captured and displayed real-time network packets, including source/destination IPs, protocols, payloads, and headers.
Provided visibility into network activity, detecting HTTP, ICMP, and other protocol communications.



Sniffer: Full packet dump

➢ Packet Logger Mode

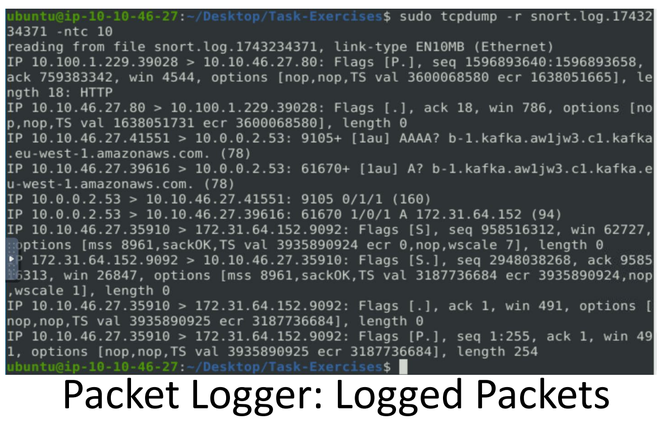
Logger Mode is used to log network packets for offline analysis and forensic investigations. Logs can be analyzed using tools like Wireshark, Snort, or tcpdump for deeper insights.

Commands Used:

```
sudo snort -dev -l    # Logs packets in default binary format
sudo snort -dev -K ASCII -l   # Logs packets in human-readable format
sudo snort -r logs/snort.log  # Reads logged packets in Snort
```

Results:

Successfully logged incoming and outgoing network traffic.
Generated two types of logs:
- Binary format (tcpdump-compatible): Requires Snort or Wireshark for analysis.
- ASCII format: Organized into separate directories based on IP addresses.



Packet Logger: Logged Packets

➢ IDS/IPS Mode

IDS/IPS mode helps manage the traffic according to user-defined rules.

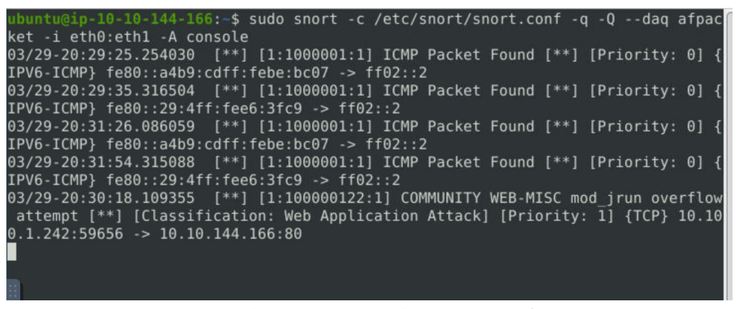
Commands Used (IDSIPS):

```
sudo snort -c /etc/snort/snort.conf -A fast  # Generates alert messages and timestamps
sudo snort -c /etc/snort/snort.conf -A console  # Runs IDS with alert logging
sudo snort –c /etc/snort/snort.conf -A cmg     #Basic header details with payload
sudo snort -c /etc/snort/snort.conf -A full     # Generates full alert logs
sudo snort -c /etc/snort/snort.conf -A none  # Disabling alerting.
```

Results:

Successfully detected ICMP and HTTP-based attacks.
Generated alerts with timestamps, source & destination IPs, and attack details.
Logged information based on the chosen alert mode (console, cmg, full, or fast).

IDS/IPS: Full Alert Logs



IPS: Dropping Packets

Command Used (IPS):

```
sudo snort -c /etc/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A console
```

Results:

Successfully blocked and dropped unauthorized ICMP and HTTP traffic.

➢ PCAP Investigation

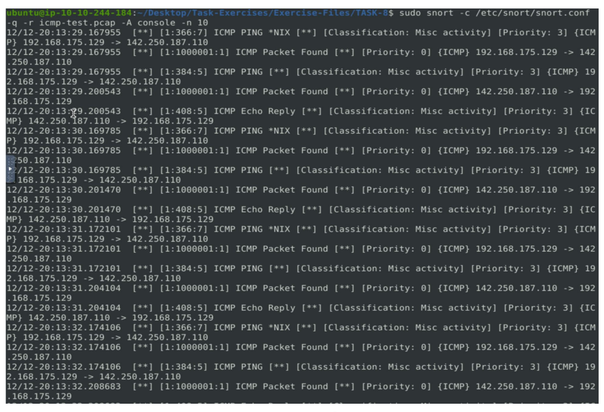
PCAP read/investigate mode helps work with pcap files.

Commands Used:

```
sudo snort -c /etc/snort/snort.conf -q -r icmp-test.pcap -A console -n 10  # Single PCAP
sudo snort -c /etc/snort/snort.conf -q --pcap-list="icmp-test.pcap http2.pcap" -A console -n 10  # Multiple PCAP
sudo snort -c /etc/snort/snort.conf -q --pcap-list="icmp-test.pcap http2.pcap" -A console --pcap-show # Multiple PCAP
```

Results:

Provided default traffic statistics with alerts depending on our ruleset for pcap files.



PCAP: Single PCAP

Key Takeaways

Real-time Traffic Monitoring: Sniffer mode provided live visibility into network activity.
Efficient Logging: Packet logger mode stored traffic data for forensic analysis.
Threat Detection & Prevention: IDS mode detected, and IPS mode blocked unauthorized traffic.
Forensic Analysis: PCAP mode helped investigate past attacks and improve security policies.