Komal Mazhar Mushtaq

STUDENT ID: CA/D1/6190

Task No. 4

Network Intrusion Detection System (IDS)

KMM

Table of Contents

Objective:

This assignment aims to develop and configure a network-based Intrusion Detection System (IDS) on a Windows machine using Snort or Suricata. The goal is to identify, analyze, and respond to suspicious network activity through the IDS while utilizing tools and techniques such as setting up custom rules and alerts and visualizing detected attacks.

Tools and Software Required:

- Snort or Suricata (IDS/IPS tools)
- Wireshark (for packet capturing and analysis)
- Windows Operating System (Windows 10 or later)
- Python (optional for alert processing or custom scripts)
- Grafana/Elasticsearch/Logstash/Kibana (ELK Stack) (optional for visualizing logs and alerts)

Prerequisites:

1. Basic understanding of networking concepts and protocols (e.g., TCP/IP, HTTP, ICMP, etc.).
2. Basic understanding of Intrusion Detection Systems and their components.
3. Familiarity with configuring and analyzing network security tools.
4. Administrative privileges on the Windows machine.

Steps to Complete the Assignment:

1. Install and Set Up Snort or Suricata on Windows:

For Snort:

1. Download the latest version of Snort from the official website.
2. Install Snort on Windows, ensuring necessary dependencies like WinPcap or Npcap are installed.
3. Configure Snort by editing the snort.conf file to set up paths and network variables and enable logging output.

For Suricata:

1. Download the Windows version of Suricata.
2. Install Suricata using the installer.
3. Configure Suricata by editing the suricata.yaml configuration file, specifying network interfaces and enabling logging.

Network Interface Configuration: Ensure your IDS tool monitors the correct network interface (e.g., Ethernet or Wi-Fi adapter).

2. Create Custom IDS Rules:

Develop custom Snort or Suricata rules to detect various types of suspicious network activities such as:
- Port scanning
- DDoS (Distributed Denial of Service) attacks
- Malware communication (e.g., C2 server traffic)
- Suspicious HTTP or DNS requests

Example Snort Rule:
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg:"HTTP Request from Suspicious Source"; flow:to_server,established; content:"GET"; nocase; sid:1000001;)
Example Suricata Rule:
alert http any any -> $HOME_NET 80 (msg:"Suspicious HTTP Request"; content:"GET"; http_method; sid:1000002;)

3. Configure Alerting and Logging:

Set up logging for detected events (e.g., output to a file, Syslog, or SIEM system).
Configure alerts for specific rule matches, ensuring that when an event occurs, an alert is triggered, and necessary information is logged.

4. Simulate Network Attacks:

Use tools like nmap (a network scanning tool) to simulate a port scan or hping3 (a packet crafting tool) to simulate DDoS traffic.
Ensure that your IDS tool detects these activities and generates alerts accordingly.
Example commands for attack simulation:
nmap for port scan:
nmap -sS -p 1-65535 <target_ip>
hping3 for DDoS simulation:
hping3 --flood -S <target_ip> -p 80

5. Visualize Detected Attacks (Optional):

If using the ELK Stack (Elasticsearch, Logstash, Kibana):
1. Set up Logstash to forward logs from Snort or Suricata to Elasticsearch.
2. Configure Kibana to visualize the logs and create dashboards that show detected attack patterns, source IPs, and other network statistics.
Grafana can also be used for real-time monitoring and alerting.

6. Analysis and Reporting:

Review the generated alerts and logs after setting up the IDS and simulating attacks.
Analyze the types of attacks detected, their severity, and the IDS's response.
Write a report summarizing:
- The setup process and configurations made.
- The types of attacks simulated.
- The effectiveness of the IDS in detecting and responding to those attacks.
- Recommendations for improving IDS detection and response mechanisms.

Deliverables:

1. IDS Configuration Files: The snort.conf or suricata.yaml file with custom rules and configuration.
2. Screenshots or Logs of Alerts: Evidence of detected attacks (alerts, logs, etc.).
3. Visualization Dashboards: If visualizing attacks using the ELK Stack or Grafana, provide screenshots or links to dashboards.
4. Analysis Report: A detailed report analyzing the effectiveness of the IDS, with findings and suggestions for improvement.

Evaluation Criteria:

- IDS Configuration: Proper installation and configuration of Snort or Suricata.
- Rule Development: The effectiveness and accuracy of custom intrusion detection rules.
- Alerting and Logging: Successful logging of detected events and alerts triggered.
- Attack Simulation and Detection: The ability to simulate attacks and verify IDS detection.
- Analysis Report: The quality and depth of analysis in identifying and responding to network threats.

Conclusion

The Network Intrusion Detection System (IDS) assignment offers one of the best ways of understanding the application of security protocols and principles on a live network through tools such as Snort and Suricata. When creating their own rules, emulating network attacks, and studying the threats that have been identified, the participants receive essential hands-on experience in recognizing potentially malicious activity in a given network space.

While not necessary for the core learning in the course, the inclusion of tools such as the ELK Stack and Grafana provides an elevated layer of learning for viewers, allowing them to observe and analyze network traffic in real time. This assignment fosters critical evaluation, decision-making ability, and problem-solving as students analyze and report detected attacks for this network security and intrusion detection system.

Upon successfully completing the assignment, the participants will not only learn how to configure IDS systematically but also understand that reviewing IDS is crucial in diagnosing and preventing network invasions in the future.