Pratical : 8

Objective

Deploy and configure a network-based Intrusion Detection and Prevention System (IDPS) in a lab environment, monitor real-time traffic, and analyze security alerts generated by the IDPS.[1][2][3]

Lab Setup Overview

- A virtual environment with at least:
  - One dedicated IDS/IPS server (e.g., running Suricata or Snort)
  - Victim machine(s) (e.g., Metasploitable, DVWA)
  - Attacker machine (e.g., Kali Linux)
- All components interconnected via a virtualized switch or network bridge.[2][4]

Steps for Deployment and Configuration

1. **Preparation**
   - Ensure hardware or VMs meet resource requirements.
   - Choose an IDS/IPS solution (e.g., Suricata, Snort, or equivalent).[5][2]
   - Obtain relevant ISO/OVA images.
2. **Install IDS/IPS**
   - Import an IDS/IPS-ready server image into your virtualization platform.
   - Install the chosen IDS/IPS (example: `sudo apt install suricata` or `snort`).[2][5]

- Configure the sensor to operate in Network-based mode for real-time packet capture.

3. **Network Configuration**
   - Assign a dedicated monitoring interface to the IDS/IPS sensor for SPAN, mirror, or promiscuous mode.[3][6]
   - Ensure traffic from victim and attacker machines flows through this interface.
4. **IDS/IPS Rule Configuration**
   - Load or customize detection/prevention rules (signature-based, anomaly-based, policy-based, etc.).[7][5]
   - Set thresholds and alert preferences accordingly.
5. **Initial Test**
   - Launch controlled attacks or suspicious activities from the attacker VM.
   - Examples: Ping sweeps, SQL injection, port scans.

Monitoring and Analysis

- Use management interfaces or log files (`/var/log/suricata/` or `/var/log/snort/`) to observe alerts.
- Analyze details in alerts:
  - Source/destination IP and port
  - Type of detected intrusion (e.g., scan, exploit)
  - Severity and timestamp
- Classify alerts as true positive, false positive, or benign activity.

Documentation and Observations

- Record:
  - Network diagram of the setup
  - IDS/IPS configuration files or screenshots

- Types of network attacks simulated and alerts triggered
- Analysis and remarks on each alert (including mitigations or follow-ups needed)[5][2]

Conclusion

Summarize:

- Effectiveness of the IDS/IPS in monitoring and responding to network threats
- Any limitations or challenges faced in deployment or analysis phase[10][9]
- Recommendations for real-world deployment improvements

References

Include documentation, tutorials, and references used:

- Suricata IDS Home-Lab and Snort Guides[2][5]
- NIST and vendor documentation for best practices[11][6][10]