TASK-4

Network Intrusion Detection System

Developing a network-based intrusion detection system using tools like Snort or Suricata. Set up rules and alerts to identify and respond to suspicious network activity.

Intrusion Detection System (IDS)

- An Intrusion Detection System (IDS) maintains network traffic looks for unusual activity and sends alerts when it occurs. The main duties of an Intrusion Detection System (IDS) are anomaly detection and reporting, however, certain Intrusion Detection Systems can take action when malicious activity or unusual traffic is discovered. In this article, we will discuss every point about the Intrusion Detection System.
- A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using an SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.

SNORT AND SURICATA

- Snort and Suricata both implement signature-based and anomaly-based detection. Signature-based detection measures packets against a pre-defined ruleset, allowing organizations to identify threats with great accuracy.
- SNORT:

Snort is based on library packet capture (libpcap). Libpcap is a tool that is widely used in Transmission control protocol/Internet protocol address traffic sniffers, content searching and analyzers for packet logging, real-time traffic analysis, protocol analysis and content matching.

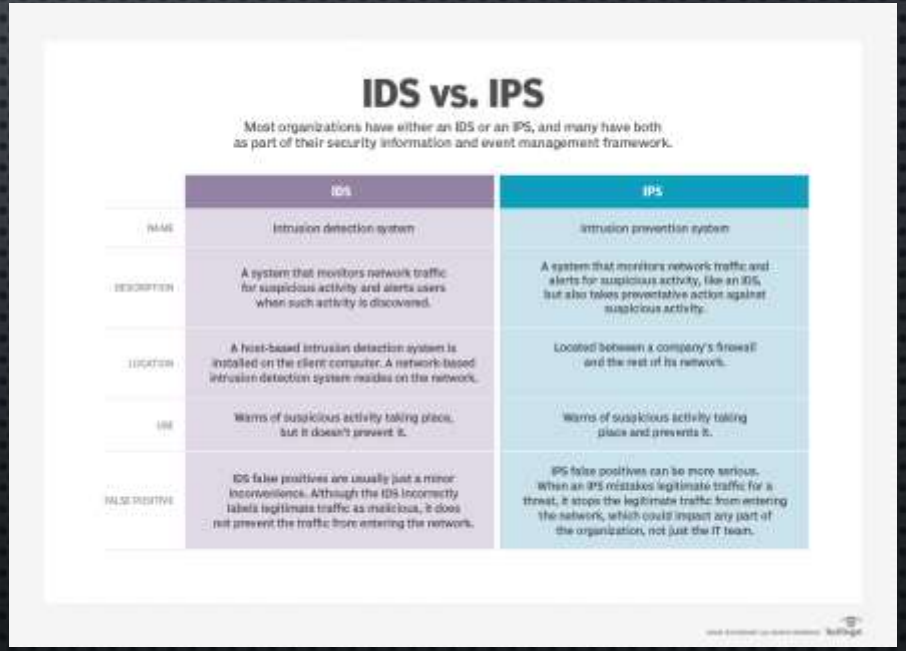
- SURICATA:

Suricata is a high-performance, open-source network analysis and threat detection software used by most private and public organizations, and embedded by major vendors to protect their assets.

- **Network Security Tools**
- **IDS (Intrusion Detection System):** An IDS helps alert your staff of potentially malicious activity in your network. However, it simply detects and alerts your IT department, this tool does not take action to prevent or remediate an attack.
- **IPS (Intrusion Prevention System):** An IPS is similar to an IDS, but in addition to identifying a potential breach, this tool can also take action to prevent an attack by blocking the suspicious activity in question.
- **DLP (Data Loss Prevention):** A DLP tool can help your organization ensure that your confidential information is secure and protected from unauthorized release or alteration.

- **SIEM (Security Incident and Event Management):** SIEMs encompass a variety of tools and solutions that monitor and control network activity.
- **THREAT HUNTNG GUIDELINES**

1. Understanding Snort or Suricata rule structure
2. Rule Actions
3. Rule Protocols
4. Rule Ips and Ports
5. Rule Directions
6. Rule options
7. Writing snort/suricata rules
8. Best Practices



Network intrusion detection system

Intrusion Detection System monitors all incoming and outgoing network activity and distinguishing weird patterns that show an attempt to break into the network. IDS can serve to confirm secure configuration and operation of other security mechanisms such as firewalls detection system functions

- Monitoring and analyzing both user and system activities.
- Analyzing system configurations and vulnerabilities.
- Assessing system and file integrity.
- Ability to recognize patterns typical of attacks by using signature or rules.
- Analysis of any abnormal network activity patterns.
- Tracking for any policy violations.

Developing a network-based intrusion detection system (NIDS) using either Snort or Suricata involves several steps. Here's a high-level overview of the process

1. Installation: Begin by installing either Snort or Suricata on your system. Both are open-source NIDS solutions and are available for various operating systems.

2. Configuration: After installation, you'll need to configure your chosen NIDS according to your network environment and security requirements. This includes setting up network interfaces, defining rules, and configuring logging options.

3. Rule Creation: Write custom rules or use pre-existing rule sets to detect suspicious or malicious network traffic. Rules can be created based on known attack signatures, anomaly detection, or specific patterns indicative of malicious activity.

4. Rule Management: Regularly update and manage your rules to adapt to evolving threats and changes in your network environment. This may involve tuning existing rules, disabling irrelevant rules, or creating new rules as needed.

- 5. Logging and Alerting: Configure logging and alerting mechanisms to notify administrators of detected threats or suspicious activity. This could involve sending alerts via email, syslog, or integrating with a security information and event management (SIEM) system for centralized monitoring

- 6. Testing and Tuning: Test your NIDS in a controlled environment to ensure it's effectively detecting and alerting on malicious activity without generating excessive false positives. Fine-tune your configuration based on testing results and ongoing monitoring of real-world traffic.

- 7. Deployment: Deploy your NIDS strategically within your network infrastructure to monitor traffic at key entry points, such as perimeter gateways or critical network segments.

- 8. Monitoring and Maintenance: Continuously monitor the performance of your NIDS and regularly update rule sets to stay ahead of emerging threats. Conduct periodic audits and reviews to ensure the effectiveness of your intrusion detection system.

- Both Snort and Suricata offer extensive documentation and community support to help you through each step of the development process.