Intrusion prevention and detection systems

The Intrusion Prevention System (IPS) and the Intrusion Detection System (IDS) are interconnected security technologies that hold significant importance in safeguarding networks and systems. Both approaches share the common objective of detecting and addressing possible security risks, albeit with varying degrees of proactive defense.

Intrusion Detection system (IDS):

1. **Function:**
- Intrusion Detection Systems (IDS) are designed to observe and analyze network or system activity to identify any potentially malicious behavior or patterns associated with established attack methods.
- The system can detect and notifying administrators or security people if potential threats are detected.
2. **Types:**
- A Network-based Intrusion Detection System (NIDS) is a security mechanism that is designed to monitor and analyze network traffic.
- A host-based intrusion detection system (HIDS) is a security mechanism that observes and analyzes activity occurring on individual hosts.
3. **Response**:
- The focus of Intrusion Detection Systems (IDS) lies in the identification and notification of potential security breaches.
- The prevention or cessation of an ongoing attack does not occur through direct acts.
4. **Implementation**:
- Strategically positioned inside the network or on certain hosts.
- This process involves the examination of traffic patterns or host actions to detect any irregularities or recognizable patterns associated with malicious attacks.
5. **Use case:**
- This tool is helpful for the purpose of surveillance and detection of potential security breaches.
- This system alerts administrators to investigate and take appropriate action in response to security incidents.

Intrusion prevention system (IPS):

1. **Function:**
- In contrast to IDS, IPS expands upon the foundation of intrusion detection by implementing proactive procedures aimed at preventing or halting identified threats.
- The identified threat can be effectively mitigated through the automatic blocking or modification of network traffic.
2. **Types**:
- The Network-based Intrusion Prevention System (NIPS) operates at the network level with the purpose of obstructing harmful network traffic.
- A host-based intrusion prevention system (HIPS) is a security mechanism that functions at the level of individual hosts to mitigate the risk of local attacks.

3. **Response**:
- The Intrusion Prevention System (IPS) not only possesses the capability to identify security issues, but it also actively engages in preventing or mitigating such incidents.
- The system has the capability to perform automated operations, such as the blocking of IP addresses or the modification of firewall rules.

4. **Implementation**:
- The deployment of network gateways or individual hosts is a common practice.
- The system employs a combination of signature-based and anomaly-based detection techniques, akin to intrusion detection systems (IDS).

5. **Use case:**
- Provides a proactive approach to mitigating security threats.
- The ability to automatically respond to identified hazards can effectively decrease the necessity for manual intervention.

TOOL USED: SURICATA

In this workshop, we are using Suricata, a network IPS/IDS system.

Suricata

Suricata is an Intrusion Detection and Prevention System (IDPS) that operates on an open-source platform. It is specifically built to provide real-time monitoring of network traffic with the purpose of detecting and mitigating any security threats. The multi-threaded architecture of the system guarantees optimal performance, enabling the effective analysis of various network protocols. Suricata employs a rule-based detection engine to identify and match patterns or signatures that are linked to established threats. This process results in the generation of warnings or the initiation of predetermined reactions. By offering support for many protocols and incorporating comprehensive logging features, this tool facilitates the acquisition of useful data pertaining to network activity. Suricata, being an open-source project, derives advantages from its vibrant community and provides opportunities for integration with various security technologies. Suricata's versatility, combined with the inclusion of Emerging Threats rulesets, establishes it as a resilient network security solution that enables enterprises to efficiently identify and address a diverse array of cyber threats.

Configuration of Suricata:

“Installation and configuring Suricata is in the readme file provided.”

After the configuration, create basic rules.

Step1: Go to terminal, command: cd /etc/suricata/rules

Step2: nano (filename.rules)

Create rules as you like, but the syntax should be without errors.

Step 3: create the rule using the command:

alert tcp any any -> any 23 (msg:"TELNET connection attempt"; sid:1000001; rev:1;)

This syntax mean, when ever there is a telnet connection happening, alert me with a message

Detailed syntax breakdown;

alert: generate an alert

any: any ip address

any: any port number ->

any: any ip address the request is going

23: telnet runs on the port number 23

Msg: message that needed to show if any alert happens

Step4: the captured log files are stored at /var/log/suricata

To open the rules, we can use the command: **cat suricata.log | grep rule**

Now, make a telnet connection from the machine using telnet <ipaddress>

Messages can be seen at tail -f fast.log (it is used to show the captured message log files)

The output can be seen as:

11/26/2023-03:18:54.933602 [**] [1:2022973: TELNET CONNECTION ATTEMPT [**] [Classification: null] [Priority: 3] {tcp} 192.168.136.2.39150 -> 192.168.136.167.23

The output shows, the alert message.

Demonstration:

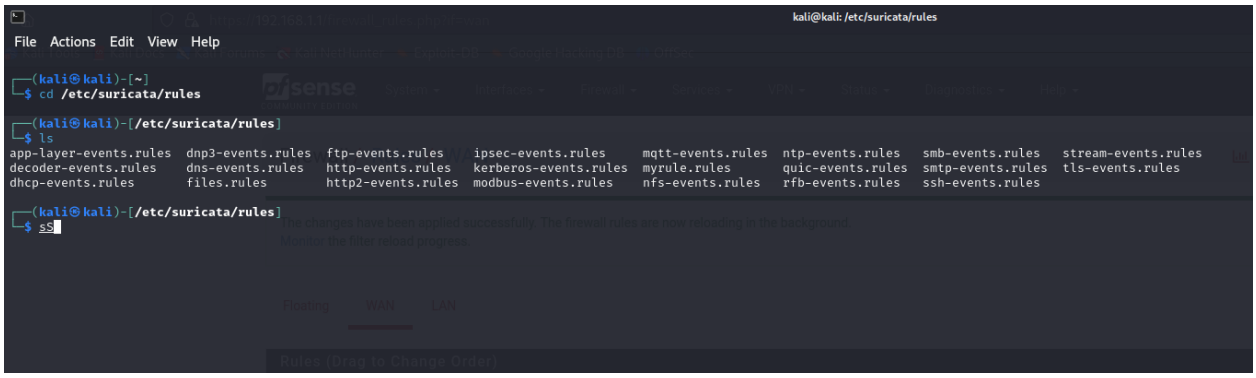

Figure 1

Figure 1 illustrates the directory containing the Suricata rules, which can be accessed by navigating to /etc/suricata/rules.

Figure 2

Figure 2 illustrates the process for creating rules by creating a file specifically for rules. . To achieve success, it is necessary to adhere to specific formats. You can find these formats at the following link: https://docs.suricata.io/en/suricata-6.0.0/rules/intro.html. This link acts as a point of reference to be followed. We are monitoring TCP connections with any source IP address and port number, targeting any destination IP address with a destination port of 23, which is commonly used for TELNET. Essentially, any source address with any port number that makes a telnet request to the machine's destination address will result in the display of a message indicating a telnet connection attempt.

Figure 3

Figure 3 shows the Metasploit running with IP address 192.168.136.141. Attempting a telnet connection at the IP address 192.168.136.143.

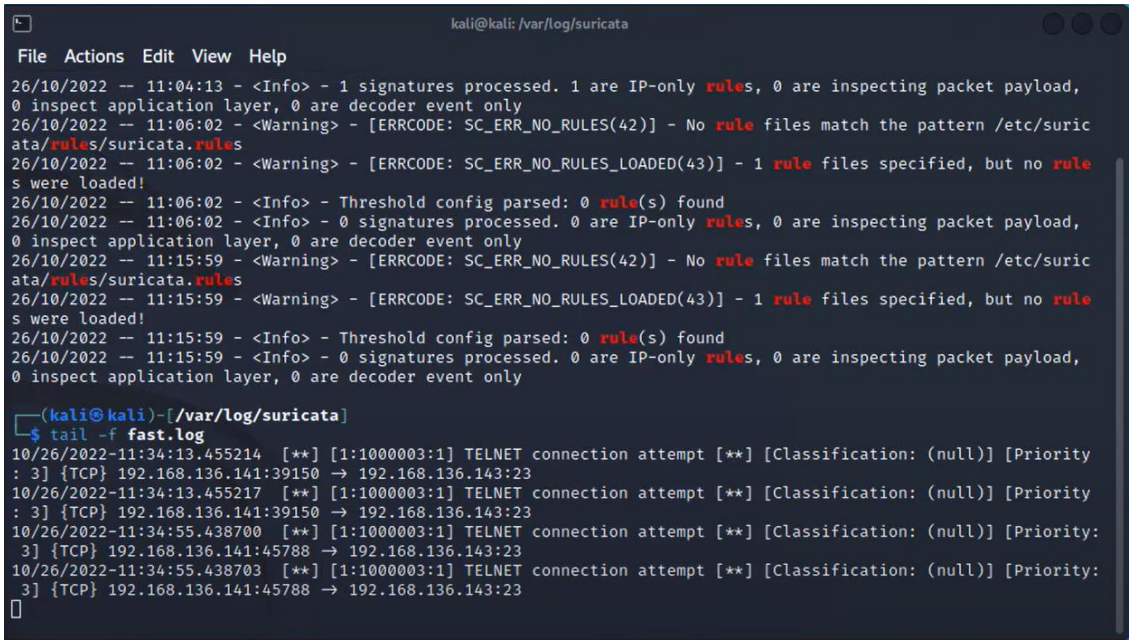

Figure 4

Figure 4 displays the log files of Suricata. The "tail -f" command displays the most recent 10 lines of a log or text file, specifically from the "fast.log" file. Earlier, our connection request was received as a telnet connection attempt, including the source IP, destination IP, and port numbers.