**Suricata – Network Intrusion Detection**

**What I Learned From Project 🏆**

* **Suricata Setup and Configuration:**
  + Installing and configuring Suricata on your system to act as an Intrusion Detection System (IDS).
  + Understanding Suricata’s role in network monitoring and intrusion detection within a cybersecurity environment.
  + Setting up Suricata to monitor specific network interfaces and capture relevant traffic.
* **Rule Creation in Suricata:**
  + Writing and deploying custom detection rules in Suricata to trigger alerts for ICMP ping attacks.
  + Learning how to define rules based on packet headers, source/destination IP addresses, protocols, and more.
  + Testing the effectiveness of your ICMP ping detection rule by launching a simulated ping attack using the ping command.
* **Network Traffic Capture with Wireshark:**
  + Installing and setting up Wireshark for live packet capture on your network.
  + Understanding how to filter traffic in Wireshark to focus on specific types of packets (e.g., ICMP).
  + Capturing and logging ICMP ping requests and responses for further analysis.

**Steps to Complete Your Mission**

1. **Prepare Your Environment**
   * 💻 Use Kali Linux as your operating system.
   * 🖥️ Kali-Linux VM-Virtualbox – Network Adapter (Bridged)
2. **Install Suricata**
   * 📥 Open your terminal and update your package list:

**Command:** sudo apt update

* + 🛠 Install Suricata:

A computer screen shot of white text

AI-generated content may be incorrect.

**Command:** sudo apt install suricata

1. **Update Rule Sets**
   * 🔄 Update Suricata rule sets:

A screen shot of a computer

AI-generated content may be incorrect.

**Command:** sudo suricata-update

1. **Create a Custom Rule**
   * ✍️ Open the local.rules file:

**Command:** sudo nano /var/lib/suricata/rules/local.rules

A screenshot of a computer

AI-generated content may be incorrect.

* + 📝 Add the rule to **detect ICMP ping requests**:

plaintext

**Code for suricata rule:**

alert icmp any any -> any any (msg:"ICMP Ping Detected"; itype:8; sid:1000001; rev:1;)

**Definition:**

(Generate an alert on ICMP from any source IP and Port to any destination IP and Port. Alert message, “ICMP Ping Detected.” Type 8 responds to an ICMP type request which is actually used in ping operations. SID is the unique identifier of the signature and rev 1 indicates the revision number for that rule. This is actually format used for snort signatures which is what suricata uses to generate alerts based off snort rules listed within suricata.)

1. **Update Suricata Configuration**
   * ⚙️ Open the Suricata configuration file:

**Command:** sudo nano /etc/suricata/suricata.yaml

A screenshot of a computer

AI-generated content may be incorrect.

* + 📁 Set the **default-rule-path** and include **local.rules** in the **rule-files** section.

1. **Restart Suricata**
   * 🔄 Apply the changes by restarting Suricata:

**Command:** sudo systemctl restart suricata

1. **Verify Rule Loading**
   * ✔️ Run Suricata to verify rules are loaded:

A screen shot of a computer screen

AI-generated content may be incorrect.

**Command:** sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -v

**Definition:**

(Restart suricata use suricata.yaml config file and on network interface eth0. Double check that eth0 is interface we are using. Finally, the -v is requesting suricata to provide a detailed output.) A screen shot of a computer

AI-generated content may be incorrect.

1. **Generate ICMP Traffic**
   * 📶 Generate traffic to trigger the rule:

A screenshot of a computer program

AI-generated content may be incorrect.

**Command:** ping -c 4 8.8.8.8

1. **Check Suricata Logs**
   * 📄 Verify the detection in the logs:

**Command:**

sudo cat /var/log/suricata/eve.json | grep "ICMP Ping Detected"

**Definition:**

(Open ever.json log file where suricata stores the logs. Search for string “ICMP Detected”)

A screenshot of a computer screen

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

Rules automatically provided by suricata are located in suricata.rules file at above path.

**WIRESHARK**

* **Network Traffic Capture with Wireshark:**
  + Installing and setting up **Wireshark** for live packet capture on your network.

A screenshot of a computer

AI-generated content may be incorrect.

* + Understanding how to filter traffic in Wireshark to focus on specific types of packets (e.g., ICMP).

A screenshot of a computer program

AI-generated content may be incorrect.

* + Capturing and logging ICMP ping requests and responses for further analysis.
* **Analyzing ICMP Traffic:**
  + Understanding the structure and purpose of ICMP traffic, particularly ping requests (ICMP Echo Request) and responses (ICMP Echo Reply).

A screenshot of a computer program

AI-generated content may be incorrect.

* + Using Wireshark’s features to inspect packet details, such as source and destination IPs, payload, and TTL (time-to-live).