Suricata IDS IPS

Contents

Time required: 60 minutes

Suricata is an open-source high performance Network IDS, IPS and Network Security Monitoring engine.

We will install Suricata on your Kali Linux VM.

Install Suricata

Ensure your system is up-to-date:

```
sudo apt update
sudo apt upgrade -y
sudo apt install suricata -y
```

Configure Suricata

1. Ensure that your Kali Linux VM is on your bridged adapter.
2. **Find the IP address**: Identify the IP address you want to monitor:

```
ip a
```

3. Note the ip address
4. **Edit the Configuration File**: Open the main configuration file:

```
sudo mousepad /etc/suricata/suricata.yaml
```

Update the following sections:

- **HOME_NET**: Set the HOME_NET variable to define your network:
- HOME_NET: "[192.168.1.0/24]"

Suricata uses rule files to detect threats. Download the latest Emerging Threats rules:

```
sudo suricata-update
```

Add Ping Flood Rule

1. In Kali Linux in your home folder.

```
nano ping-flood.rules
```

2. Copy and Paste the following code into the file. Do not change the code.

NOTE: Each rule starts with alert. There are 2 rules. They should be in 2 long lines.
This rule is also attached to the assignment.

```
alert icmp any any -> $HOME_NET any (msg:"PING FLOOD DETECTION - Excessive ICMP Echo Requests";itype:8;flow:to_server;threshold: type limit, track by_src, count 100, seconds 10;classtype:attempted-dos;sid:21;)
alert icmp any any -> $HOME_NET any (msg:"PING FLOOD DETECTION - Rapid ICMP Echo Requests";itype:8;flow:to_server;detection_filter: track by_src, count 50, seconds 1;classtype:attempted-dos;sid:122;)
```

3. Save the file.

4. **Edit the Configuration File**: Open the main configuration file:

```
sudo mousepad /etc/suricata/suricata.yaml
```

5. Use CTRL-F to open the find dialog box at the bottom of the screen.

6. Type in rule-files → press Enter

7. Find the following section.

8. Add the third line

```
rule-files:
  - suricata.rules
  - /home/user/ping-flood.rules
```

9. **Test Configuration**: Verify the configuration file is error-free:

```
sudo suricata -T -c /etc/suricata/suricata.yaml -i eth0
```

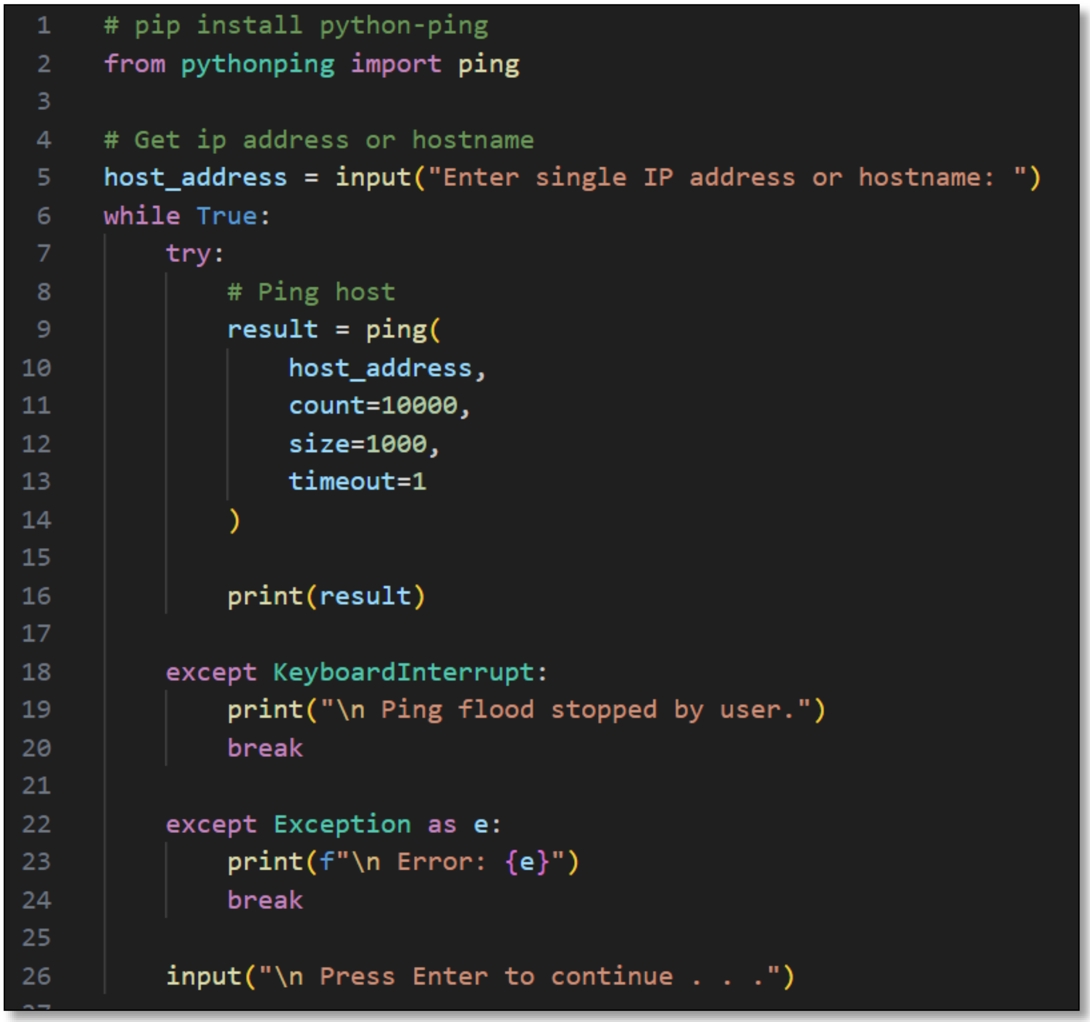
Python Ping Flood Attack

Create this program on your local computer. You will be the attacker.

This Python script will simulate a ping flood attack.

A ping flood attack, also known as an ICMP flood, is a type of denial-of-service (DoS) attack that overwhelms a network device or service with ICMP data packets:

The attacker sends a large number of ICMP echo-request packets (pings) to the target device. The target device responds with an equal number of reply packets, making it inaccessible to normal traffic.



```python
# pip install python-ping
from pythonping import ping

# Get ip address or hostname
host_address = input("Enter single IP address or hostname: ")
while True:
    try:
        # Ping host
        result = ping(
            host_address,
            count=10000,
            size=1000,
            timeout=1
        )

        print(result)

    except KeyboardInterrupt:
        print("\n Ping flood stopped by user.")
        break

    except Exception as e:
        print(f"\n Error: {e}")
        break

    input("\n Press Enter to continue . . .")
```

Start Suricata

Run Suricata in live mode to monitor traffic:

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

1. On your local computer, run the ping flood program.
2. In a new terminal → take a look at the log files. You should see a bunch of ICMP dos warnings from your ping flood.

```
# Summarized alerts
tail -f /var/log/suricata/fast.log
# Detail alerts in JSON format
tail -f  /var/log/suricata/eve.json
```

Assignment Submission

Attach a screenshot showing the ping flood logs to the assignment in Blackboard.