Suricata IDS Lab Manual - Student Edition

Objective

This lab teaches how to install and configure Suricata (an open-source IDS) on Ubuntu to detect Nmap SYN scans and ICMP floods launched from a Kali Linux VM. You will write custom rules and analyze alerts.

Lab Requirements

- Ubuntu VM (with Suricata)
- Kali Linux VM (for scanning)
- Same virtual network (Bridged or Host-only)
- Internet access on Ubuntu
- sudo privileges on both VMs

Installing Suricata

Run on Ubuntu:

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

Identify Network Interface

Run: ip a

Note the interface with an IP (e.g., enp0s8, eth0). Use this in Suricata.

Configure Rule Files

Edit /etc/suricata/suricata.yaml

Make sure:

```
rule-files:
  - suricata.rules
  - local.rules
```

Add Custom Nmap Detection Rule

Suricata IDS Lab Manual - Student Edition

Edit /etc/suricata/rules/local.rules

Add:

```
alert tcp any any -> any any (msg:"Custom Nmap TCP Scan Detected"; flags:S; threshold:type both, track by_src, count 10, seconds 60; sid:1000001; rev:1;)
```

Restart Suricata

```
sudo pkill suricata
sudo rm /var/run/suricata.pid
sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8 -D
```

Scan from Kali

Run:

```
nmap -sS -T4 <Ubuntu-IP>
```

Optional:

```
nmap -sS -A -T4 <Ubuntu-IP>
```

View Alerts

On Ubuntu:

```
sudo tail -f /var/log/suricata/fast.log
grep -i nmap /var/log/suricata/eve.json
```

Detect ICMP Floods

Add to local.rules:

```
alert icmp any any -> any any (msg:"ICMP Flood Detected"; itype:8; threshold:type both, track by_src, count 100, seconds 10; sid:9990002; rev:1;)
```

Retest and Check

Run:

```
ping -f <Ubuntu-IP>
```

Or:

```
sudo hping3 --icmp --flood <Ubuntu-IP>
```

Then:

```
sudo tail -f /var/log/suricata/fast.log
```

Conclusion

You installed Suricata, configured rules, detected Nmap scans and ICMP floods, and viewed alerts. This builds hands-on cybersecurity monitoring skills.