Title: Suricata IDS Tutorial – Detecting Nmap Scans in a Virtual Lab

---

🎯 Objective:

This tutorial demonstrates how to install, configure, and use **Suricata** (an open-source IDS) on **Ubuntu** to detect **Nmap SYN scans** originating from a **Kali Linux VM**. It covers rule configuration (default and custom), scan testing, and troubleshooting.

🧰 Part 1: Lab Requirements

- Ubuntu VM (for Suricata)
- Kali Linux VM (for scanning)
- Both VMs on the same network (VirtualBox Host-only, NAT, or Bridged)
- Internet access (for Suricata updates)
- sudo privileges on both systems

⚙️ Part 2: Installing Suricata (on Ubuntu)

sudo apt update && sudo apt upgrade -y

sudo apt install suricata suricata-update -y

sudo suricata-update # Pull latest community rules

🌐 Part 3: Identify Network Interface

On Ubuntu VM:

ip a

Note the active interface (e.g., enp0s8, eth0). You'll use this in Suricata startup.

🛠️ Part 4: Configure Rule Files in Suricata

Edit the main config:

sudo nano /etc/suricata/suricata.yaml

Find the rule-files: section and ensure it includes both:

rule-files:

  - suricata.rules   # Default rules

  - local.rules   # Custom rules

✅ suricata.rules comes from community updates.
✅ local.rules is where you define your custom rules.

✍️ Part 5: Add a Custom Nmap Detection Rule

Edit or create the local.rules file:

sudo nano /etc/suricata/rules/local.rules

Paste the rule:

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;)

This triggers an alert if 10 SYN packets come from the same source within 60 seconds.

🔁 Part 6: Restart Suricata with Custom Rules

Replace enp0s8 with your actual interface:

sudo pkill suricata

sudo rm /var/run/suricata.pid 2>/dev/null

sudo suricata -c /etc/suricata/suricata.yaml -i enp0s8 -D

✅ Suricata is now running in daemon mode with your custom rule and community rules.

🧪 Part 7: Scan from Kali Linux

Find the Ubuntu IP address:

ip a

Then from Kali:

nmap -sS -T4 <Ubuntu-IP>

Optional: Use aggressive mode to ensure more packets:

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

🔍 Part 8: View Suricata Alerts

On Ubuntu VM:

- View quick alerts:

cat /var/log/suricata/fast.log

- View detailed structured logs:

grep -i nmap /var/log/suricata/eve.json

✅ Look for this:

[**] [1:1000001:1] Custom Nmap TCP Scan Detected [**]

🛠️ Part 9: Troubleshooting Tips

Problem: No alerts in fast.log or eve.json

- Is Suricata running on the correct interface?
- Did you save your custom rule in local.rules?

- Is local.rules included in suricata.yaml under rule-files:?
- Try more aggressive scan:

nmap -sS -p1-1000 -T4 <Ubuntu-IP>

- Check logs manually:

less /var/log/suricata/eve.json

Problem: Suricata won't start?

sudo pkill suricata

sudo rm /var/run/suricata.pid

✅ Conclusion