Lab 6 - Snort (Intrusion Detection & Prevention)

In this lab, we explore **Snort**, one of the world's most widely used Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) (owned by Cisco).

Snort can analyze network traffic in real time and detect a wide range of attacks, intrusions, exploits, and suspicious behaviors.

Snort operates in three modes:

1. **Sniffer Mode**: displays raw packet headers.
2. **Packet Logger Mode**: logs packets to disk.
3. **Network Intrusion Detection System (NIDS) Mode**: uses rules to detect attacks.

Answer the following questions and send the report to: <csclass.dz@gmail.com>
Team information (one report by team):

- First Name Last Name: ……………………………………………..
- First Name Last Name: ……………………………………………..
- First Name Last Name: ……………………………………………..

Deadline: Wednesday, Dec 17, 2025.

Check if Snort is installed by default on your Kali machine. If not, install it (type installation commands).

…………………………………………………………………

…………………………………………………………………

Report how you solved the issues related to Snort installation (used commands).

…………………………………………………………………

…………………………………………………………………

Do not scan or attack systems you do not own (or have explicit permission to test). Unauthorized sniffing, probing, or intrusion of networks, IP addresses, or domains is illegal and may result in criminal or civil penalties.

Part 1 — Getting Started with Snort

1. Check the Snort version

Run on your Kali machine:

`snort -V` or `snort –-version`

Questions

- What version of Snort is installed?
  ……………………………………………………………………
- Why is it important to keep IDS/IPS tools updated?
  ……………………………………………………………………

2. Sniffer Mode

Run snort in sniffer mode: ………………………………….

Questions

- What kind of information does Snort show in this mode?
  ……………………………………………………………………
- How could this be useful for an attacker?
  ……………………………………………………………………
- Why is it insufficient as a full IDS?
  ……………………………………………………………………

3. Packet Logger Mode

Create a directory for logs: `mkdir /tmp/snortlog`
Run snort in packet logger mode: ……………………………………………………………….
Then from your **Metasploitable**, ping the Kali machine.
Stop Snort.

Questions

- Which files were created in `/tmp/snortlog?`
  ……………………………………………………………………
- What information can an incident responder recover from these logs?
  ……………………………………………………………………

Part 2 — Running Snort in IDS Mode

Snort uses rules stored under: ……………………………………………………………….
and a main configuration file: ………………………………………………………………….

4. Testing Snort with a Basic Custom Rule

Create a simple rule file: `nano /etc/snort/rules/local.rules`
Add: `alert icmp any any -> any any (msg:"ICMP test detected"; sid:1000001; rev:1;)`
Save the file.

Run Snort in IDS mode: ………………………………………………………………………

From your **Metasploitable**, ping the Kali machine. Watch Snort detect it.

Questions

- What alert message appears?
  ……………………………………………………………………
- What does **SID** mean in Snort rules?
  ……………………………………………………………………
- Why is alerting on ICMP useful (or not)?
  ……………………………………………………………………

Stop Snort with **Ctrl + C**.

Part 3 — Testing Real Snort Attack Rules

5. Enable community rules (already included in Snort on Kali)

List the rules: `ls /etc/snort/rules`

Questions

- How many rule files do you see?
  ……………………………………………………………………
- Which ones seem related to web attacks?
  ……………………………………………………………………
- Which ones seem related to malware or exploits?
  ……………………………………………………………………

6. Detecting a Port Scan

Snort contains rules that detect Nmap scans.
Start Snort: ……………………………………………………………………

From Kali (in a second terminal), run: `nmap -sS <Metasploitable IP>`
Return to Snort’s terminal.

Questions

- Which alerts were triggered?
  ……………………………………………………………………
- Which Snort rule category detected the scan?
  ……………………………………………………………………
- Why is SYN scan detection important?
  ……………………………………………………………………

Stop Snort.

7. Detecting Web Attacks

Start Snort again.

From Kali, run: `curl http://<Metasploitable IP>:80`

Then try an obvious attack pattern:

```
curl "http://<Metasploitable IP>/index.php?id=1 OR 1=1"
```

Questions

- Which Snort alerts were triggered?
  ………………………………………………………………………
- Did Snort detect potential SQL injection?
  ………………………………………………………………………
- What signatures or rules were responsible?
  ………………………………………………………………………

Stop Snort.

Part 4 — Writing Advanced Snort Rules

8. Write a rule to detect access to a forbidden directory

Edit local rules: `nano /etc/snort/rules/local.rules`
Add: `alert tcp any any -> any 80 (msg:"Suspicious /admin access"; content:"/admin"; sid:1000002; rev:1;)`
Start Snort.

From Kali: `curl http://<Metasploitable IP>/admin`

Questions

- Did Snort generate an alert?
  ………………………………………………………………………
- Why is detecting access to /admin directories helpful?
  ………………………………………………………………………
- How could attackers evade this rule?
  ………………………………………………………………………

Stop Snort.

9. Write a rule to detect Telnet usage

Many attacks are done via Telnet due to its lack of encryption.

Add the rule : `alert tcp`…………………………………………………..
Start Snort.

From Kali: `telnet <Metasploitable IP>`

Questions

- Did Snort detect the Telnet connection?
  ………………………………………………………………….
- What information is visible to attackers when Telnet is used?
  ………………………………………………………………….
- Which secure alternative should be used instead?
  ………………………………………………………………….

Stop Snort.

Part 5 — Snort as an IPS (Optional Advanced Section)

Run Snort as an IPS.

………………………………………………………………….

Then modify/add one of your local rules to block Telnet.

Questions

- Is the Telnet connection blocked?
  ………………………………………………………………….
- How does IPS differ from IDS?
  ………………………………………………………………….
- What are the risks of enabling drop rules on production networks?
  ………………………………………………………………….