Snort Assignment

Snort IDS Installation, Configuration & Attack Testing using Nmap

⚠️ IMPORTANT LAB RULES (MANDATORY)

- Perform this lab **ONLY on your own system / virtual machine**
- Do **NOT** scan public or real-world servers
- Internet use is **allowed for learning**
- Screenshots are **mandatory**
- Plagiarism is **strictly prohibited**

Basic Theory (Read First)

🔹 What is Snort?

Snort is an **open-source Intrusion Detection System (IDS)** that monitors network traffic and generates alerts when suspicious activity is detected.

🔹 What is Port Scanning?

Port scanning is a technique used to identify **open ports and running services** on a target system. Attackers use it for reconnaissance.

🧪 LAB SETUP

Role	System
IDS Machine	Ubuntu with Snort
Attacker	Kali Linux / Ubuntu
Network	NAT

TASK 1: Update Ubuntu System

Instructions:

1. Open Terminal
2. Update package list
3. Upgrade installed packages

📸 **Screenshot Required:** System update output

TASK 2: Install Snort

Instructions:

1. Install Snort & it's dependecies using apt
2. Select network interface during installation

📸 **Screenshot Required:** Snort installation screen

TASK 3: Verify Snort Installation

📸 **Screenshot Required:** Snort version output

TASK 4: Configure Snort (HOME_NET)

Instructions:

1. Open Snort configuration file
2. Set HOME_NET to your network range

📸 **Screenshot Required:** Edited configuration file

TASK 5: Test Snort Configuration

📸 **Screenshot Required:** Configuration validation success message

---

TASK 6: Run Snort in IDS Mode

📸 **Screenshot Required:** Snort running state

For Nmap use Different Machine (Kali/Ubuntu)

TASK 7: Install Nmap

📸 **Screenshot Required:** Nmap installation

TASK 8: Perform Nmap Port Scan

🔸 **Normal Scan**

```
nmap <Ubuntu-IP>
```

🔸 SYN Scan

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

🔸 Specific Port Scan

```
nmap -p 22,80,443 <Ubuntu-IP>
```

📸 **Screenshot Required:**

- Nmap scan output
- Snort alert on console

TASK 9: Create Custom Snort Rule

Instructions:

1. Open local rules file
2. Add ICMP or Port Scan rule

Commands:

```
sudo nano /etc/snort/rules/local.rules
```

Add:

```
alert tcp any any -> $HOME_NET any (msg:"TCP Port Scan Detected"; flags:S;
threshold:type both, track by_src, count 10, seconds 5; sid:1000002; rev:1;)
```

📸 **Screenshot Required:** Custom rule added

- Also write Meaning of above rule in txt file.

TASK 10: Test Custom Rule

1. Restart Snort
2. Run Nmap scan again
3. Observe alert message

📸 **Screenshot Required:** Custom alert triggered

TASK 11: View Snort Logs

📸 **Screenshot Required:** Alert log file

QUESTIONS

- Write Answer on text file.

1. What is IDS?
2. Difference between IDS and IPS
3. What is Snort?
4. What is port scanning?
5. What is Nmap used for?
6. What is HOME_NET?
7. What is a Snort rule?
8. What is SID in Snort?

SUBMISSION GUIDELINES

- Create a **GitHub repository**
- Upload:
  - Screenshots
  - Text file