## 4. Suspicious Network Activity

## **Task Goal:**

Detect **suspicious network activity** (e.g., **port scanning**, **odd DNS queries**, etc.) using **Wireshark or tcpdump** by simulating an attack (e.g., nmap -sS scan).

Steps:

#### **Wireshark:**

* Open Wireshark on Ubuntu.
* Start capturing on the network interface (e.g., eth0, ens33, etc.).
* **Filter to focus on Nmap traffic later:**
* tcp.flags.syn == 1 and tcp.flags.ack == 0

#### **OR tcpdump (CLI):**

sudo tcpdump -i any tcp and 'tcp[13] == 2'

This filters **SYN packets** (common in scans).

### **Simulate the Suspicious Activity (From Kali)**

#### **Use Nmap to Scan the Victim**

nmap -sS 192.168.157.138(victim ip)

-sS = Stealth SYN scan (commonly used by attackers because it’s fast and less noisy than a full scan).

### **Observe in Wireshark or tcpdump**

#### In Wireshark:

* Use this filter:

tcp.flags.syn == 1 and tcp.flags.ack == 0

You'll see many SYN packets to different ports — this is a **classic sign of a port scan**.