**Lab 11**

**Object: NMAP - A Stealth Port Scanner**

1. **What is the difference between a TCP-connect scan and a SYN scan?**

A **TCP-connect scan** and a **SYN scan** are both methods used in network scanning, but they differ in how they interact with the target system. Here’s a quick overview of each:

**1. TCP-Connect Scan**

* **How it works:** This type of scan completes the **entire TCP handshake** (SYN, SYN-ACK, ACK) to establish a connection with the target port. After the connection is made, it is immediately closed.
* **Pros:** Since it completes the full connection, it doesn’t require special permissions (root access).
* **Cons:** More easily detected by the target because it generates a complete log entry in their systems.

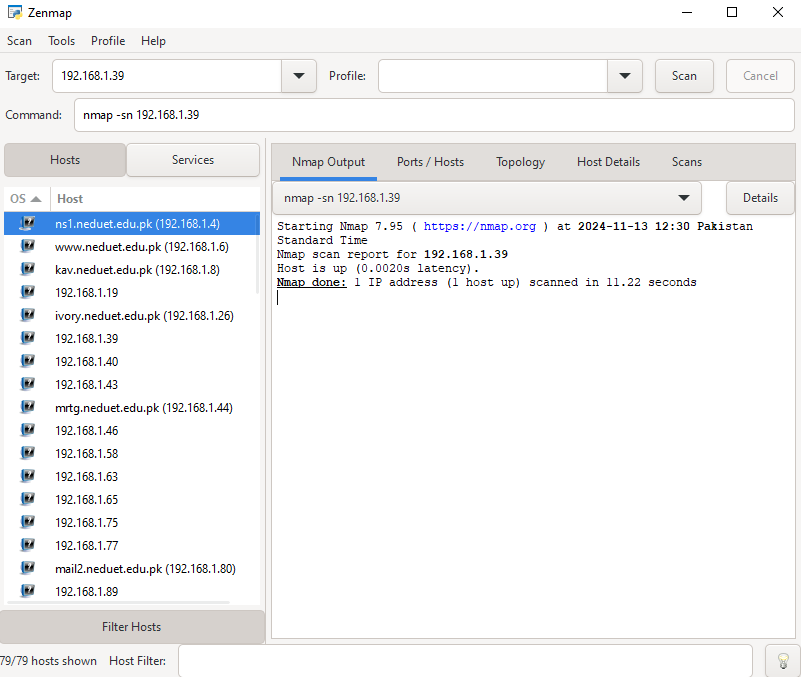
**2. SYN Scan**

* **How it works:** Also known as a "half-open" scan, the SYN scan only sends a **SYN packet** and waits for a SYN-ACK response. Once the SYN-ACK is received, it does not complete the handshake and instead sends an RST (reset) packet to drop the connection.
* **Pros:** Faster and stealthier, as it doesn’t complete the full TCP connection. Requires root privileges.
* **Cons:** Needs elevated permissions (root access) to send raw packets.

**2. What is the purpose of the –sP command line switch? Show practical demonstration.**

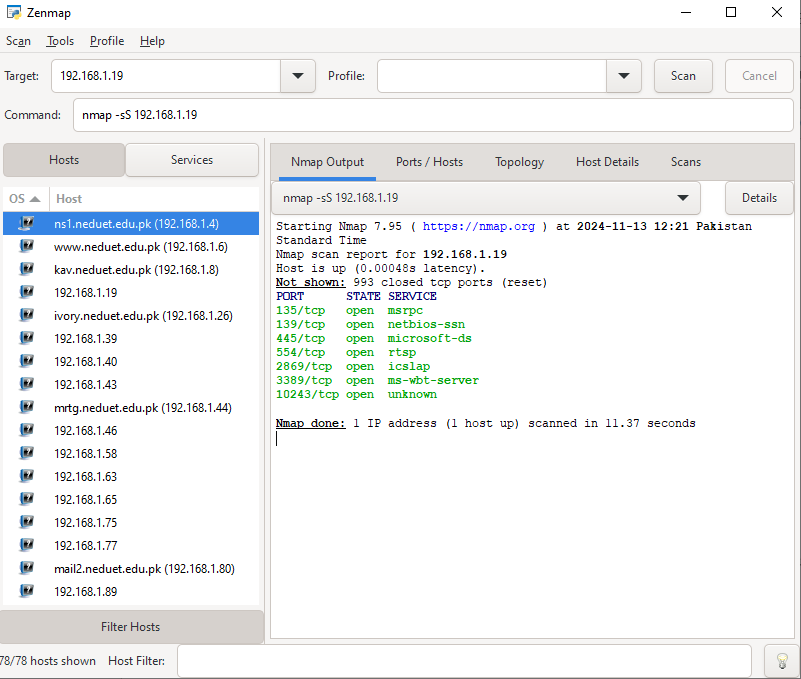
The **-sP** command line switch in Nmap (used in Zenmap as well) is for a **ping scan**. This scan is used to discover which hosts on a network are up and reachable, without scanning any specific ports. The **-sP** command is great for quickly identifying live hosts without overwhelming the network with full scans.

The command is **Nmap –sn 192.168.1.39**

****

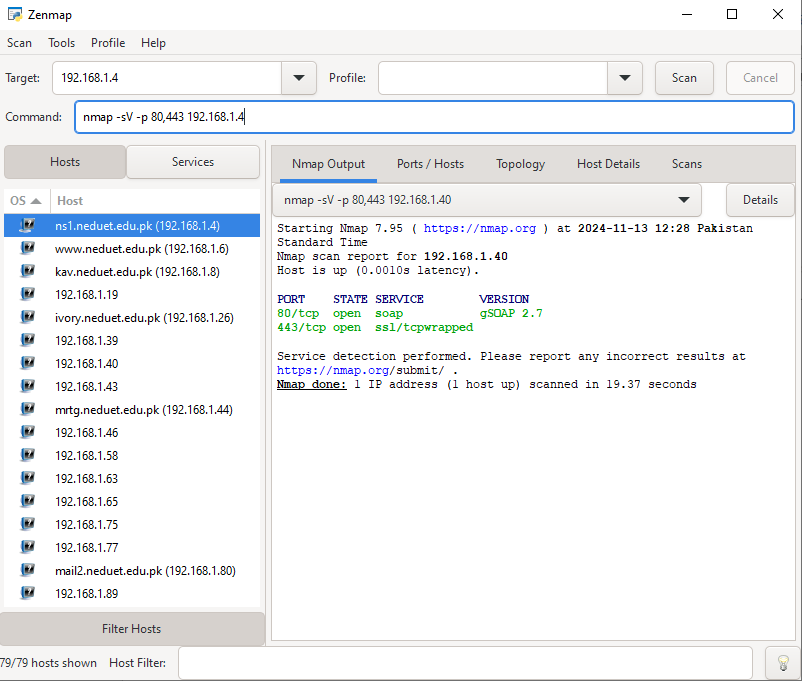
**3. What is the purpose of the –sS command line switch? Show practical demonstration.**

The command is **Nmap –sS 192.168.1.19**

****

**4.**  **What command would you issue to scan for computers running web servers?**

The command is **Nmap –sV –p 80,443 192.168.1/4**

****