**Information Security COMP 421**

**Spring 2025 Section B**

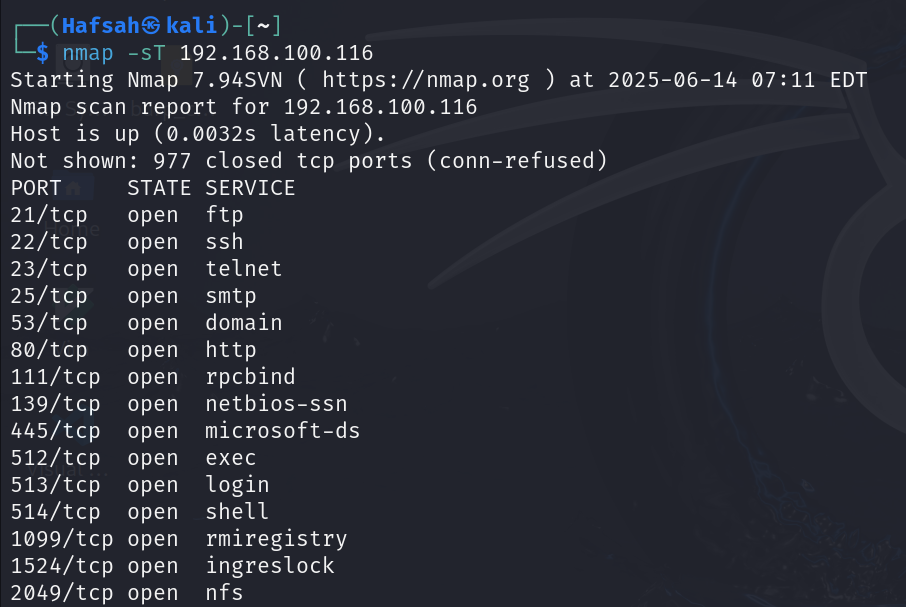
**Assignment 4**

**SSHafsah Shahbaz – 251684784**

This report demonstrates the use of various Nmap scanning techniques (TCP Connect, TCP SYN, and UDP Scans) on a Metasploit machine within a virtual network environment. Additionally, it includes Netcat-based manual probing of open ports and a summary of findings and learning outcomes.

**Nmap Scanning Results**

nmap -sT 192.168.100.116



**Observations**:

* This scan performs a full 3-way TCP handshake.
* Open ports like 21 (FTP), 22 (SSH), 80 (HTTP), and 445 (SMB) were detected.
* Slower but reliable; can be detected by firewalls/IDS easily.

nmap -sS 192.168.100.116

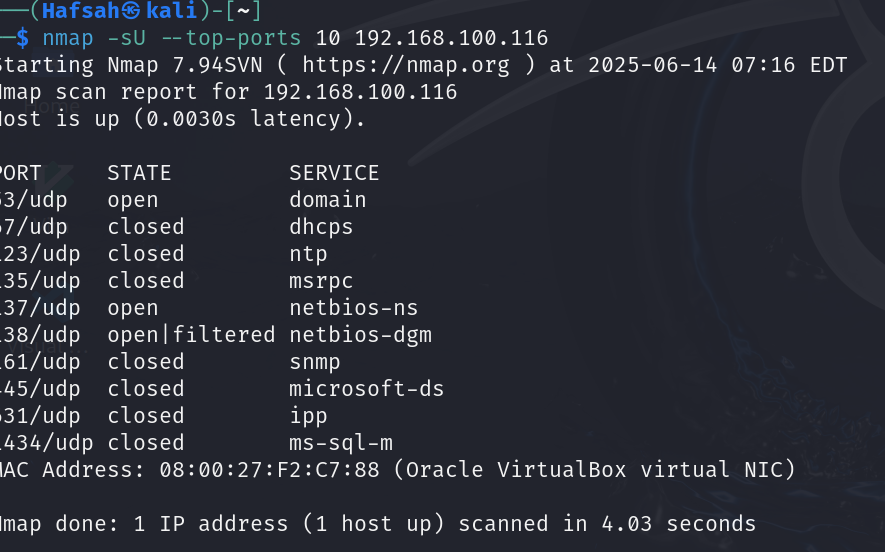
A computer screen shot of a computer

AI-generated content may be incorrect.

**Observations**:

* Stealthier scan: only SYN packets sent.
* Detected similar services as -sT, but faster and less noisy.
* Preferred for penetration testing.

nmap -sU --top-ports 10 192.168.100.116



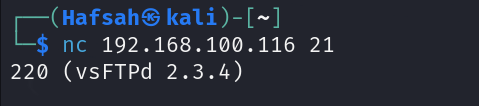
**Observations**:

* UDP port scanning is slower and can return filtered states.
* Common open ports might include 161 (SNMP), 69 (TFTP), or 137 (NetBIOS).
* Some ports may show as “open|filtered”.

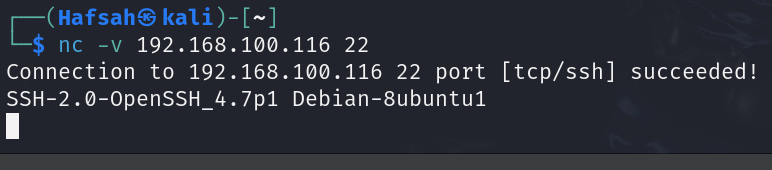
**Netcat Probing**

Using Netcat to interact with discovered ports

nc 192.168.100.116 21



nc -v 192.168.100.116 22



**Observations**:

* Port 21 responded with FTP service banner.
* Port 22 responded with an SSH service banner
* Helpful in banner grabbing and service enumeration.

**Lessons Learned & Observations**

* Nmap provides different scanning techniques depending on the need: stealth, speed, and reliability.
* TCP SYN (-sS) is faster and stealthier than TCP Connect (-sT).
* UDP scans are trickier due to lack of ACK and rely heavily on timeouts.
* Netcat is a simple but powerful tool for manual probing and testing of port responses.
* These tools form the backbone of any penetration testing toolkit.