BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

Name	Rishabh Santosh Shenoy
UID no.	2023300222
Experiment No.	6

AIM:	To study about network mapping using NMAP
OBJECTIVE:	The objective of this lab assignment is to introduce with NMAP, a powerful network scanning tool widely used for network discovery and security auditing.
Question	
QUESTION :	Scan a given network range and identify all active hosts.
ANSWER :	The -sn flag in Nmap stands for "No port scan." It tells Nmap to only perform a ping scan to check which hosts are up in a given range, without scanning for open ports. The -sn flag helps identify active devices on a network without probing for specific services. For example, the command sudo nmap -sn 192.168.1.0/24 scans the range 192.168.1.0 to 192.168.1.255 for active hosts only.

```
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo nmap -sn spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:42 IST
Nmap scan report for spit.ac.in (172.16.10.2)
Host is up (0.14s latency).
Other addresses for spit.ac.in (not scanned): 172.16.10.3 172.16.10.6
rDNS record for 172.16.10.2: ns1.spit.ac.in
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$
```

Question	
QUESTION :	Identify the top 5 most commonly open ports on a specific target.

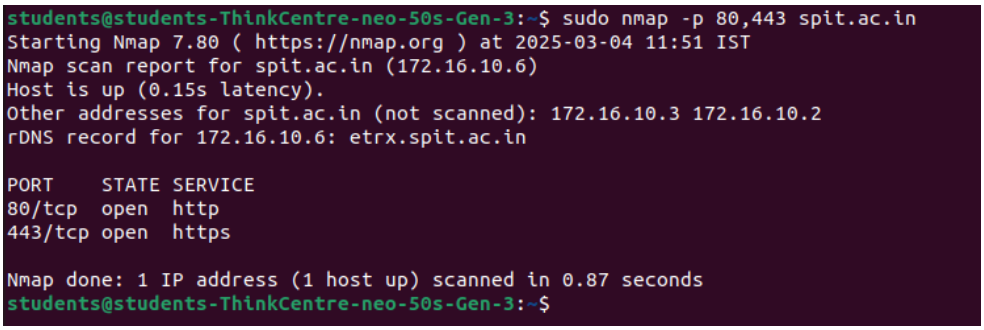
ANSWER :	Nmap is a network scanning tool used for discovering active hosts, detecting open ports, identifying service versions, and determining operating systems. By using commands like sudo nmap -sn spit.ac.in, sudo nmap -p 1-65535 spit.ac.in, and sudo nmap -sV spit.ac.in, you can perform these tasks. Custom scripts can automate scans, and specific ports can be targeted for more focused scanning.

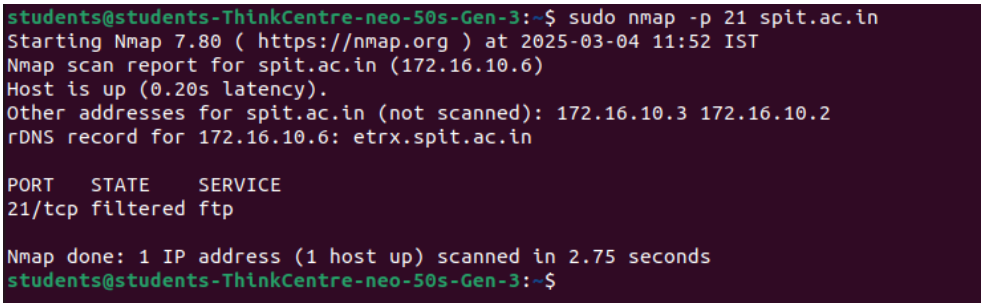
```
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo nmap -p 80,443 --script /home/students/ccn222.nse spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:47 IST
Nmap scan report for spit.ac.in (172.16.10.3)
Host is up (0.12s latency).
Other addresses for spit.ac.in (not scanned): 172.16.10.2 172.16.10.6
rDNS record for 172.16.10.3: ns2.spit.ac.in

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 2.85 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$
```

Question	
QUESTION :	Determine the MAC address of a target device using NMAP.
ANSWER :	Nmap can be used to determine the MAC address of a target device using the -O option for OS detection or -sn for a ping scan. The MAC address is displayed if the target is on the same local network. These methods help identify devices and their hardware addresses, assisting in network mapping and security analysis.

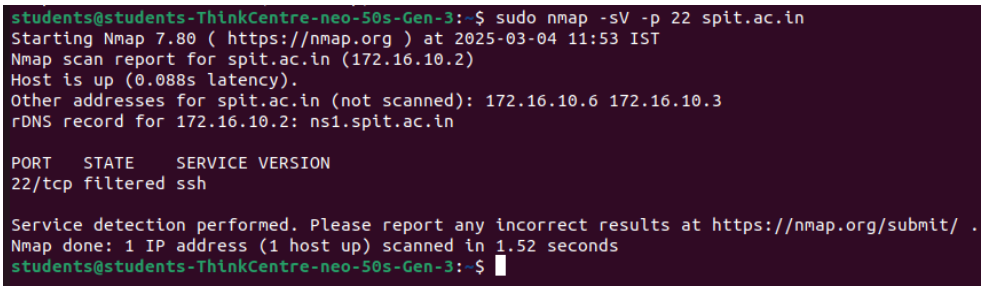
```
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo nmap -O spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:48 IST
Nmap scan report for spit.ac.in (172.16.10.3)
Host is up (0.37s latency).
Other addresses for spit.ac.in (not scanned): 172.16.10.6 172.16.10.2
rDNS record for 172.16.10.3: ns2.spit.ac.in
Not shown: 998 filtered ports
PORT   STATE  SERVICE
43/tcp closed whois
53/tcp open   domain
Aggressive OS guesses: Linux 2.6.18 - 2.6.22 (92%), Crestron XPanel control system (92%), HP PSC 2400-series Photosmart printer (91%), Vodavi
XTS-IP PBX (90%), Linux 2.6.9 - 2.6.18 (89%), Linux 3.10 - 4.11 (88%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Netgear WGR614v7 wireless b
roadband router (88%), Linux 2.6.18 (88%), Linux 3.2 - 4.9 (87%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.86 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$
```

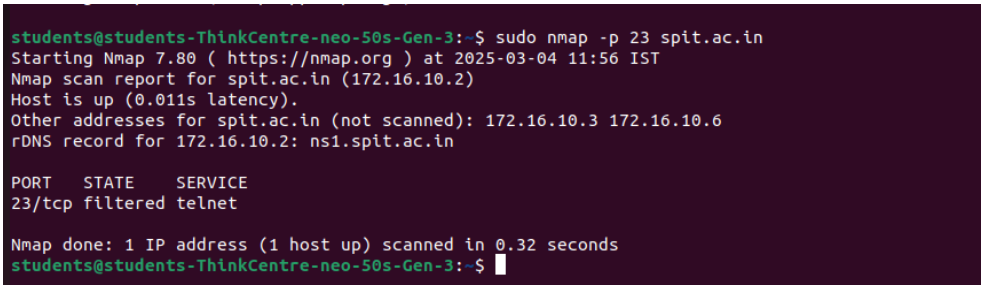
Question	
QUESTION :	Perform a scan to detect the presence of HTTP and HTTPS services on a

	target network
ANSWER :	 To detect HTTP (port 80) and HTTPS (port 443) services on a target network, Nmap can be used to scan these specific ports. Using the command sudo nmap -p 80,443 <target>, Nmap checks for the presence of these web services. This helps identify if the target is hosting web applications or secure websites, aiding in security analysis.

Question	
QUESTION :	Find out if a particular host has FTP service running on it.
ANSWER :	 To check if a host has FTP service running, Nmap can be used to scan port 21, the default port for FTP. The command sudo nmap -p 21 <target> checks if port 21 is open, indicating that FTP is active. This helps identify whether the target host allows file transfers through the FTP protocol, which may pose security risks.

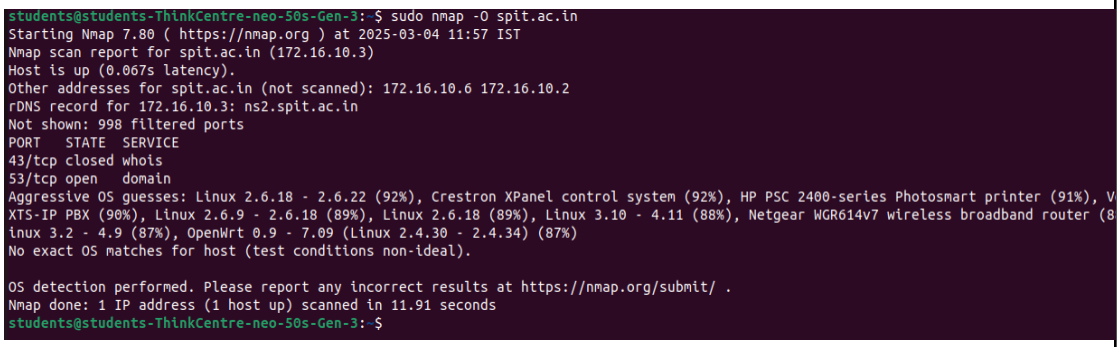
Question

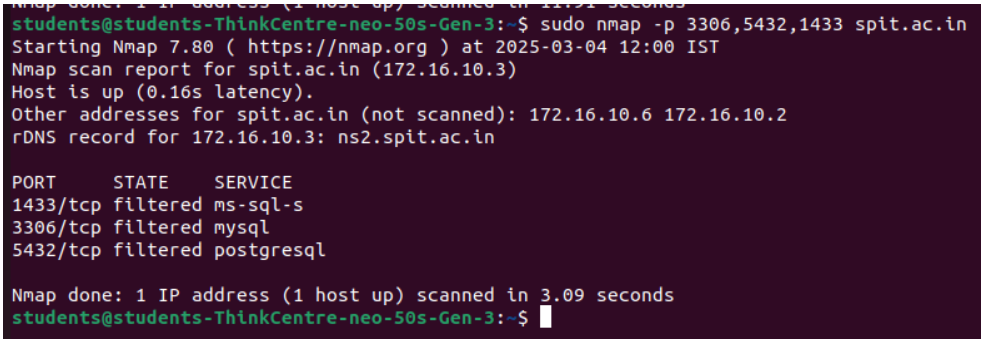
QUESTION :	Identify the SSH version running on a given host.
ANSWER :	 To identify the SSH version running on a host, Nmap can be used with the -sV option for version detection. By scanning port 22 (default for SSH), Nmap identifies the service version, helping assess potential security risks or vulnerabilities. The command sudo nmap -sV -p 22 <target> reveals detailed information about the SSH service, including its version and configuration.

Question	
QUESTION :	Scan a range of IP addresses and list all hosts that have Telnet service running.
ANSWER :	 To scan for Telnet service on a specific domain like spit.ac.in, Nmap can be used with the -p 23 option, which targets port 23, the default port for Telnet. The command sudo nmap -p 23 spit.ac.in will reveal whether the Telnet service is running on the target domain. Telnet is an older protocol often used for remote login, and detecting its presence can highlight potential security vulnerabilities, as it transmits data unencrypted.

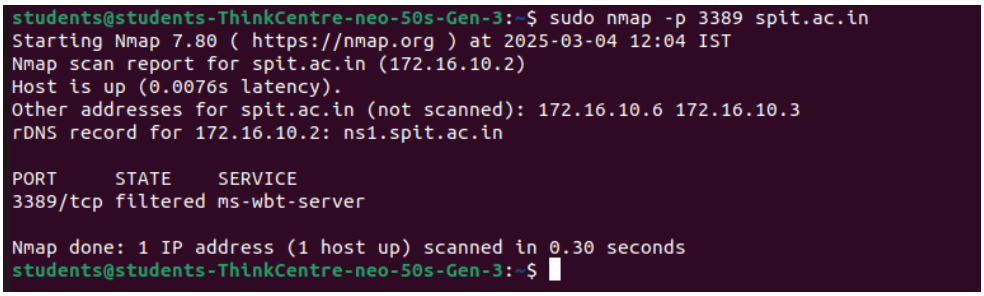
Question

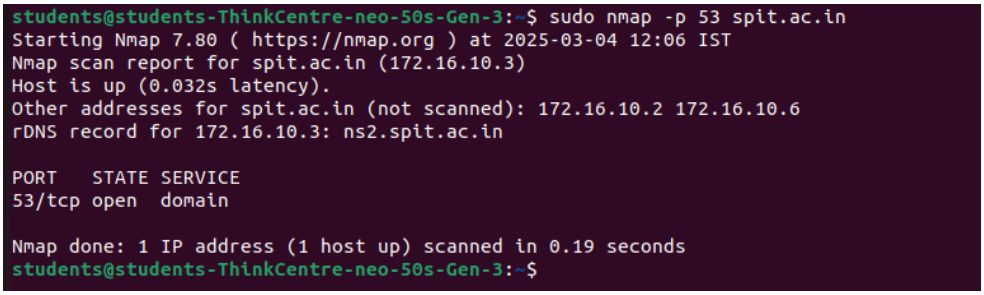
BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

QUESTION :	Determine the operating system of a target host using NMAP.
ANSWER :	 Nmap can be used to determine the operating system of a target host using the -O option, which triggers OS detection. The command sudo nmap -O <target> analyzes network responses to guess the target's OS based on TCP/IP stack fingerprinting and other factors. This helps in identifying the underlying operating system, which can be useful for network inventory, security assessments, and vulnerability analysis. Accurate OS detection is critical for tailoring specific attacks or defenses.

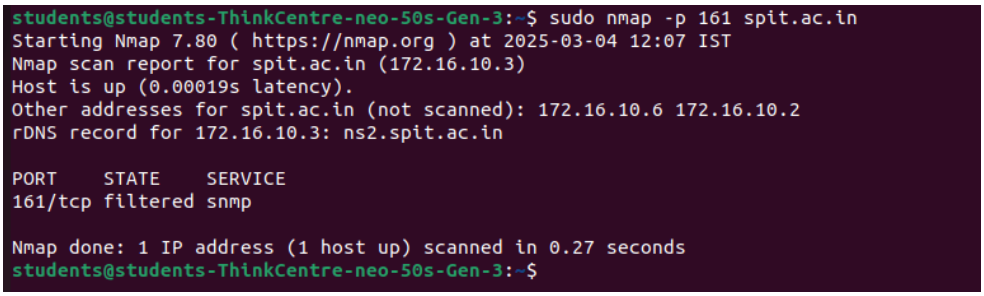
Question	
QUESTION :	Identify any SQL services running on a given network.
ANSWER :	 To identify SQL services on a network, Nmap can scan common SQL ports like 3306 (MySQL), 5432 (PostgreSQL), and 1433 (MS SQL) using the -p option. The command sudo nmap -p 3306,5432,1433 <target> will reveal if any of these SQL services are running on the target system, aiding in database security assessment.

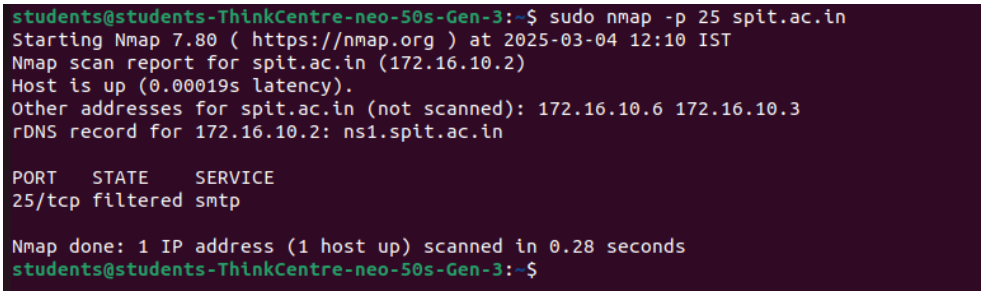
Question

QUESTION :	Find out if a specific host has Remote Desktop Protocol (RDP) enabled.
ANSWER :	 To determine if a specific host has Remote Desktop Protocol (RDP) enabled, Nmap can be used to scan port 3389, the default port for RDP. By running the command sudo nmap -p 3389 <target>, Nmap will check if the port is open on the target system. If the port is open, it indicates that RDP is enabled, allowing remote desktop connections. This is essential for identifying systems that are potentially vulnerable to remote access, as RDP is commonly targeted in security exploits and attacks.

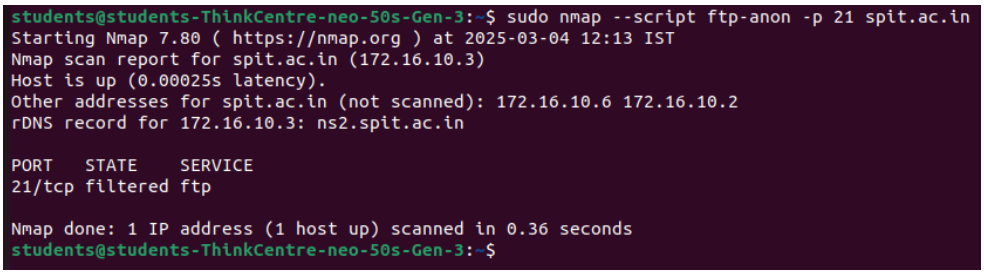
Question	
QUESTION :	Scan a target network and determine if any hosts are running DNS services.
ANSWER :	 To determine if any hosts on a target network are running DNS services, Nmap can be used to scan port 53, which is the default port for DNS. By running the command sudo nmap -p 53 <target-network>, Nmap checks if port 53 is open on the target hosts. If open, it indicates the presence of DNS services, which are responsible for resolving domain names to IP addresses. This helps identify DNS servers and assess their security on the network.

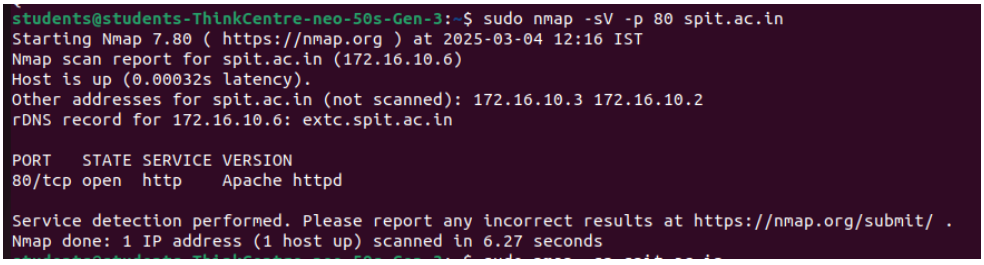
Question

QUESTION :	Detect if a host has SNMP (Simple Network Management Protocol) enabled.
ANSWER :	 To detect if a host has SNMP enabled, Nmap can scan port 161, the default for SNMP. Using the command sudo nmap -p 161 <target>, Nmap will identify if this port is open, indicating that SNMP is running. SNMP is used for network management, and its presence may expose sensitive device information if not properly secured.

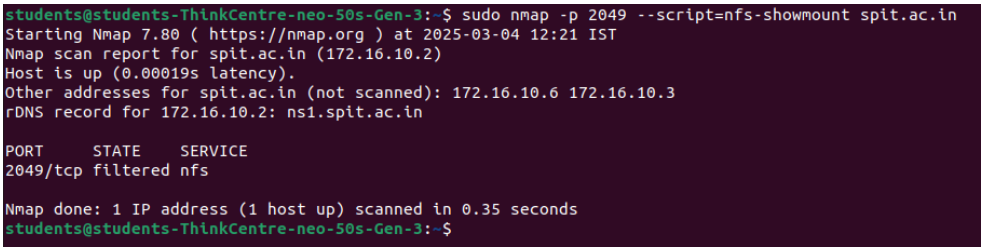
Question	
QUESTION :	Perform a scan to identify any SMTP (Simple Mail Transfer Protocol) servers on a network
ANSWER :	 To identify SMTP (Simple Mail Transfer Protocol) servers on a network, Nmap can scan port 25, the default port used by SMTP. Running the command sudo nmap -p 25 <target-network> checks if this port is open, indicating the presence of an SMTP server. SMTP is used for sending emails, and identifying its presence on a network helps in understanding email flow and securing email-related services against unauthorized access.

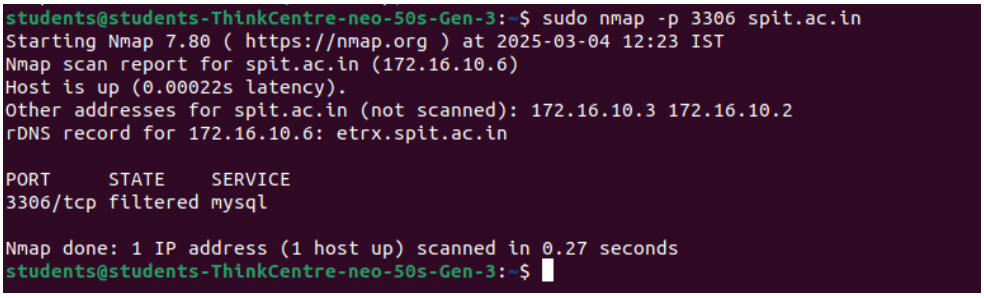
Question

QUESTION :	Determine if a target network has any active FTP servers allowing anonymous login
ANSWER :	 To determine if a target network has active FTP servers allowing anonymous login, Nmap can be used with the ftp-anon script. The command sudo nmap --script ftp-anon -p 21 <target-network> scans port 21 (FTP) and checks if any servers accept anonymous login. Allowing anonymous login on FTP servers can pose security risks, as unauthorized users may gain access to sensitive files or manipulate data.

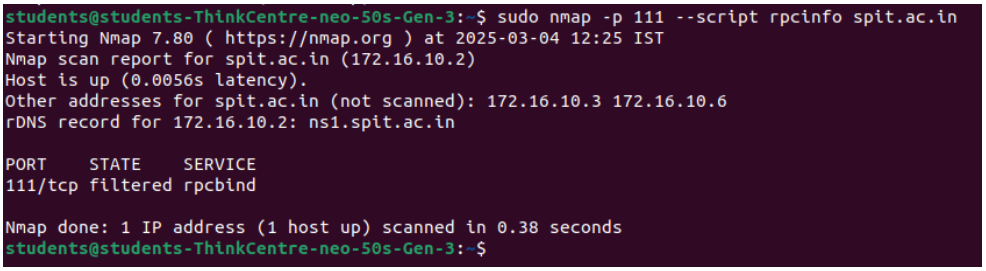
Question	
QUESTION :	Find out if any hosts in a network are running vulnerable versions of the Apache HTTP server.
ANSWER :	 The command sudo nmap -sV -p 80 spit.ac.in is used to detect the version of the service running on port 80 (HTTP) of the target domain spit.ac.in. The -sV option enables service version detection, providing details about the software version of the Apache server or any other service running on that port. This helps identify vulnerabilities based on known versions.

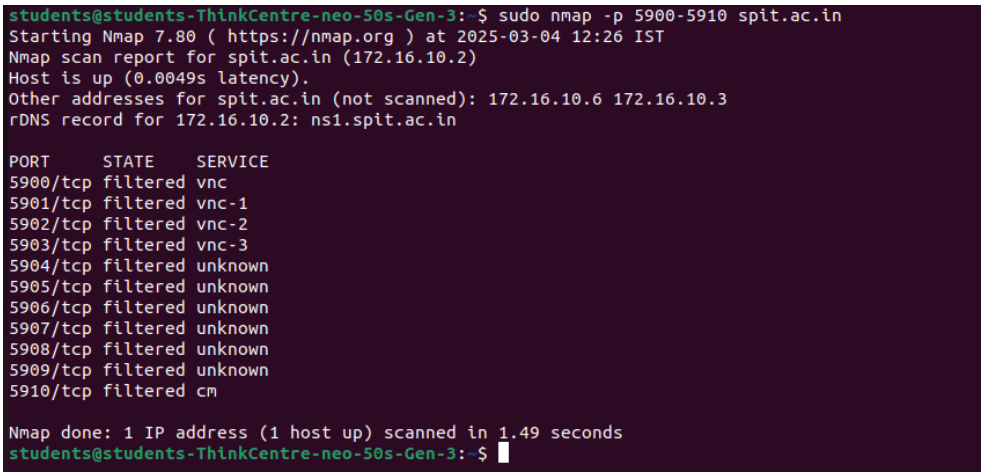
Question	
QUESTION :	Detect if a target host has any open NFS (Network File System) shares.

ANSWER :	 To detect open NFS (Network File System) shares on a target host, Nmap can be used with the --script=nfs-showmount option, which queries port 2049 (the default port for NFS). The command sudo nmap -p 2049 --script=nfs-showmount <target> checks for active NFS shares, providing insight into any exposed file systems. This helps identify security risks if sensitive files are unintentionally shared over the network.

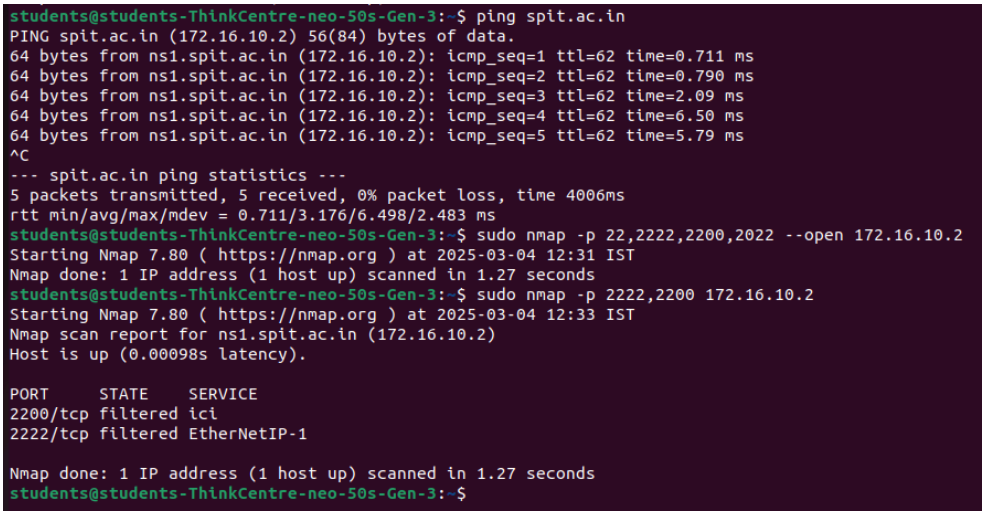
Question	
QUESTION :	Identify the presence of any MySQL database servers on a given network
ANSWER :	 To identify the presence of MySQL database servers on a network, Nmap can scan port 3306, the default port for MySQL. Running the command sudo nmap -p 3306 <target-network> checks if this port is open on any hosts within the specified network. If port 3306 is open, it indicates that a MySQL server is running, which can be useful for database management, auditing, or security assessments.

Question	
QUESTION :	Scan a network to determine if any hosts have the Remote Procedure Call (RPC) service running.

ANSWER :	 To determine if any hosts in a network have the Remote Procedure Call (RPC) service running, Nmap can be used to scan port 111, the default port for RPC. The command sudo nmap -p 111 --script rpcinfo <target-network> queries this port and gathers information on active RPC services. Identifying open RPC services helps assess network security, as RPC is often targeted for exploits and unauthorized access attempts.

Question	
QUESTION :	Detect if a specific host has any open VNC (Virtual Network Computing) ports
ANSWER :	 To detect if a specific host has any open VNC (Virtual Network Computing) ports, Nmap can be used to scan the typical VNC port range 5900-5910. The command sudo nmap -p 5900-5910 <target-ip> checks if these ports are open, which would indicate that a VNC server is running. VNC allows remote desktop access, so identifying open VNC ports helps in assessing the potential for unauthorized access or security risks in the network.

BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India
Department of Computer Engineering

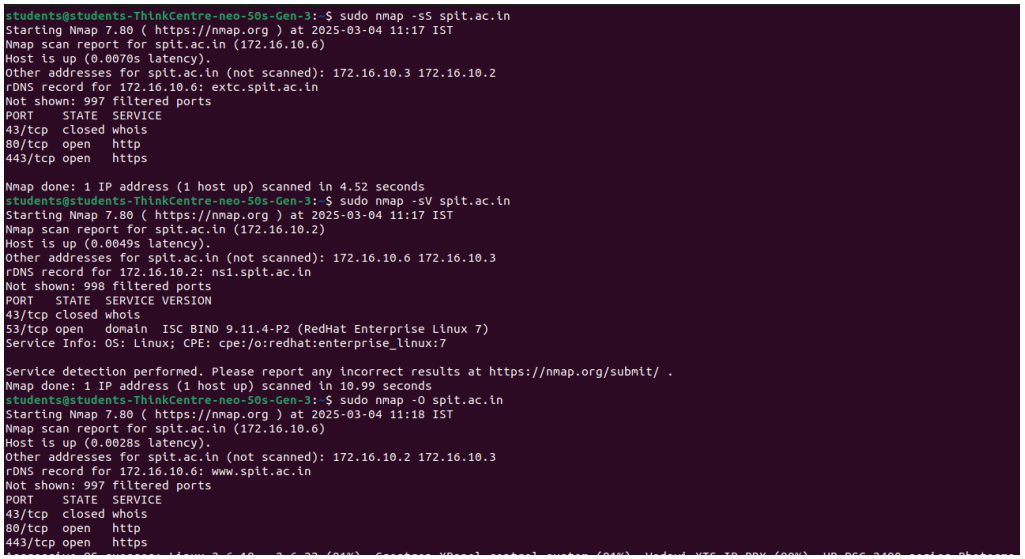
Question	
QUESTION :	Perform a scan to identify any hosts with the Secure Shell (SSH) service running on non-default ports.
ANSWER :	 To detect SSH services running on non-default ports, Nmap can be used to scan specific ports like 2222, 2200, and 2022, which are commonly used for SSH. The command sudo nmap -p 22,2222,2200,2022 --open <target-ip> checks these ports on the target system. By specifying --open, Nmap only returns results for ports that are open, helping quickly identify any non-default SSH services, which could enhance security assessments by uncovering alternative access points.

TASKS SCREENSHOT

TASKS:

```
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo apt update
[sudo] password for students:
Hit:1 https://brave-browser-apt-release.s3.brave.com stable InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [594 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,354 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [2,114 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [762 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [392 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [330 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [103 kB]
Get:13 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 DEP-11 Metadata [212 B]
Get:14 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [1,192 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [43.1 kB]
Get:16 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [2,904 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [759 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [359 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [7,048 B]
Get:21 http://in.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 DEP-11 Metadata [212 B]
Get:22 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [17.7 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 DEP-11 Metadata [212 B]
Get:24 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [510 kB]
Get:25 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 DEP-11 Metadata [208 B]
Get:26 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [652 kB]
Get:27 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [966 kB]
Get:28 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [125 kB]
Get:29 http://security.ubuntu.com/ubuntu jammy-security/multiverse amd64 DEP-11 Metadata [208 B]
Fetched 14.6 MB in 10s (1,463 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
110 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Skipping acquire of configured file 'main/binary-i386/Packages' as repository 'https://brave-browser-apt-release.s3.brave.com stable InRele
ase' doesn't support architecture 'i386'
```

```
N: Skipping acquire of configured file 'main/binary-i386/Packages' as repository 'https://brave-browser-apt-release.s3.brave.com stable InRele
ase' doesn't support architecture 'i386'
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1).
0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.
students@students-ThinkCentre-neo-50s-Gen-3:~$ nmap -sn https://www.spit.ac.in/
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:14 IST
Unable to split netmask from target expression: "https://www.spit.ac.in/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$ nmap -sn http://www.spit.ac.in/
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:15 IST
Unable to split netmask from target expression: "http://www.spit.ac.in/"
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.00 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$ nmap -sn spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:15 IST
Nmap scan report for spit.ac.in (172.16.10.6)
Host is up (0.024s latency).
Other addresses for spit.ac.in (not scanned): 172.16.10.3 172.16.10.2
rDNS record for 172.16.10.6: extc.spit.ac.in
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
students@students-ThinkCentre-neo-50s-Gen-3:~$ nmap -sS spit.ac.in
You requested a scan type which requires root privileges.
QUITTING!
students@students-ThinkCentre-neo-50s-Gen-3:~$ sudo nmap -sS spit.ac.in
Starting Nmap 7.80 ( https://nmap.org ) at 2025-03-04 11:17 IST
Nmap scan report for spit.ac.in (172.16.10.6)
Host is up (0.0070s latency).
Other addresses for spit.ac.in (not scanned): 172.16.10.3 172.16.10.2
rDNS record for 172.16.10.6: extc.spit.ac.in
Not shown: 997 filtered ports
PORT    STATE  SERVICE
43/tcp  closed whois
80/tcp  open   http
```



CONCLUSION :

In this experiment, I have learned how to use Nmap to perform network scanning and identify services running on non-default ports. By scanning for SSH services on alternative ports such as 2222, 2200, and 2022, I gained insights into how systems might be configured with non-standard ports for better security or to avoid default port scans. Using Nmap's powerful options, such as --open, helped me focus only on open ports, making the scanning process more efficient and precise. I also understood how to resolve issues related to DNS and domain resolution while working with both domain names and IP addresses.

This experiment has greatly enlightened my knowledge of network security

	and the importance of conducting thorough scans to detect open services. It reinforced the need for securing services by using non-default ports, which can help prevent unauthorized access attempts. Overall, this hands-on experience with Nmap has significantly enhanced my practical understanding of network scanning and security assessment techniques.