

# Nmap Room Tryhackme

Nmap (Network Mapper) is a powerful and widely used open-source tool for network discovery and security auditing. It enables security professionals and system administrators to identify hosts on a network, discover open ports and services, determine operating systems, and detect potential vulnerabilities. Nmap supports various scanning techniques such as TCP connect, SYN scans, UDP scans, and more advanced options like service version detection and NSE (Nmap Scripting Engine) for automation. Due to its flexibility, speed, and detailed output, Nmap is considered an essential tool in the cybersecurity toolkit, especially in tasks like penetration testing, vulnerability assessment, and network troubleshooting.

## ***Task 1: Deploy***

Deploy the target VM. No further action is required beyond starting it

## ***Task 2: Introduction***

1. What networking constructs are used to direct traffic to the right application on a server ?

ANS: Ports

2. How many of these are available on any network-enabled computer? ANS: 65535

3. How many of these are considered “well-known” ?

ANS:1024

## ***Task 3: Nmap Switches***

```
root@ip-10-201-59-110:~# nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file

HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

▶ CAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
```

1. What is the first switch listed in the help menu for a syn scan?
2. ANS: -sS
3. Which switch would you use for a udp scan?  
ANS: -sU
4. If you wanted to detect which operating system the target is running on, which switch would you use ?  
ANS: -O
5. Nmap provides a switch to detect the version of the services running on the target. What is this switch ?  
ANS: -sV
6. The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity ?  
ANS: -v
7. Verbosity level one is good, but verbosity level two is better! How would you set the verbosity level to two ?  
ANS: -vv
8. What switch would you use to save the nmap results in three major formats  
? ANS: -oA
9. What switch would you use to save the nmap results in a “normal” format  
? ANS: -oN
10. A very useful output format: how would you save results in a “grepable” format?  
ANS: -oG

Sometimes the results we're getting just aren't enough. If we don't care about how loud we are, we can enable “aggressive” mode. This is a shorthand switch that activates service detection, operating system detection, a traceroute and common script scanning.

11. How would you activate this setting  
? ANS: -A
12. How would you set the timing template to level 5 ?  
ANS: -T5
13. How would you tell nmap to only scan port 80  
? ANS: -p 80
14. How would you tell nmap to scan ports 1000–1500 ?

ANS: -p 1000-1500

15. How would you tell nmap to scan *all* ports ?

ANS: -P-

16. How would you activate a script from the nmap scripting library (lots more on this later!) ?

ANS: --script

17. How would you activate all of the scripts in the “vuln” category ?

ANS: --script=vuln

## Scan Types

### ***Task 5: TCP Connect Scans***

1. Which RFC defines the appropriate behavior for the TCP protocol?

**Ans:** RFC 793

2. If a port is closed, which flag should the server send back to indicate this?

**Ans:** RST

### ***Task 6: SYN Scans***

1. There are two other names for a SYN scan. What are they?

**Ans:** Half-open, Stealth

2. Can Nmap use a SYN scan without Sudo permissions (Y/N)?

**Ans:** N

### ***Task 7: UDP Scans***

1. If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

**Ans:** open|filtered

2. When a UDP port is closed, by convention the target should send back a “port unreachable” message. Which protocol would it use to do so?

**Ans:** ICMP

### ***Task 8: NULL, FIN and Xmas Scans***

1. Which of the three scan types uses the URG flag?

**Ans:** Xmas

2. Why are NULL, FIN, and Xmas scans generally used?  
**Ans:** Firewall evasion
3. Which common OS may respond to a NULL, FIN, or Xmas scan with a RST for every port?  
**Ans:** Microsoft Windows

### ***Task 9: ICMP Network Scanning***

1. How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap (CIDR notation)?  
**Ans:** nmap -sn 172.16.0.0/16

### ***Task 10: NSE Scripts Overview***

1. What language are NSE scripts written in?  
**Ans:** Lua
2. Which category of scripts would be a very bad idea to run in a production environment?  
**Ans:** Intrusive

### ***Task 11: Working with the NSE***

1. What optional argument can the ftp-anon.nse script take?  
**Ans:** maxlist

### ***Task 12: Searching for Scripts***

1. What is the filename of the script which determines the underlying OS of the SMB server?  
**Ans:** smb-os-discovery.nse
2. What does the smb-os-discovery.nse script depend on?  
**Ans:** smb-brute

### ***Task 13: Firewall Evasion***

1. Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the -Pn switch?  
**Ans:** ICMP

2. Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

**Ans:** --data-length

### ***Task 14: Practical***

1. Does the target respond to ICMP (ping) requests (Y/N)?

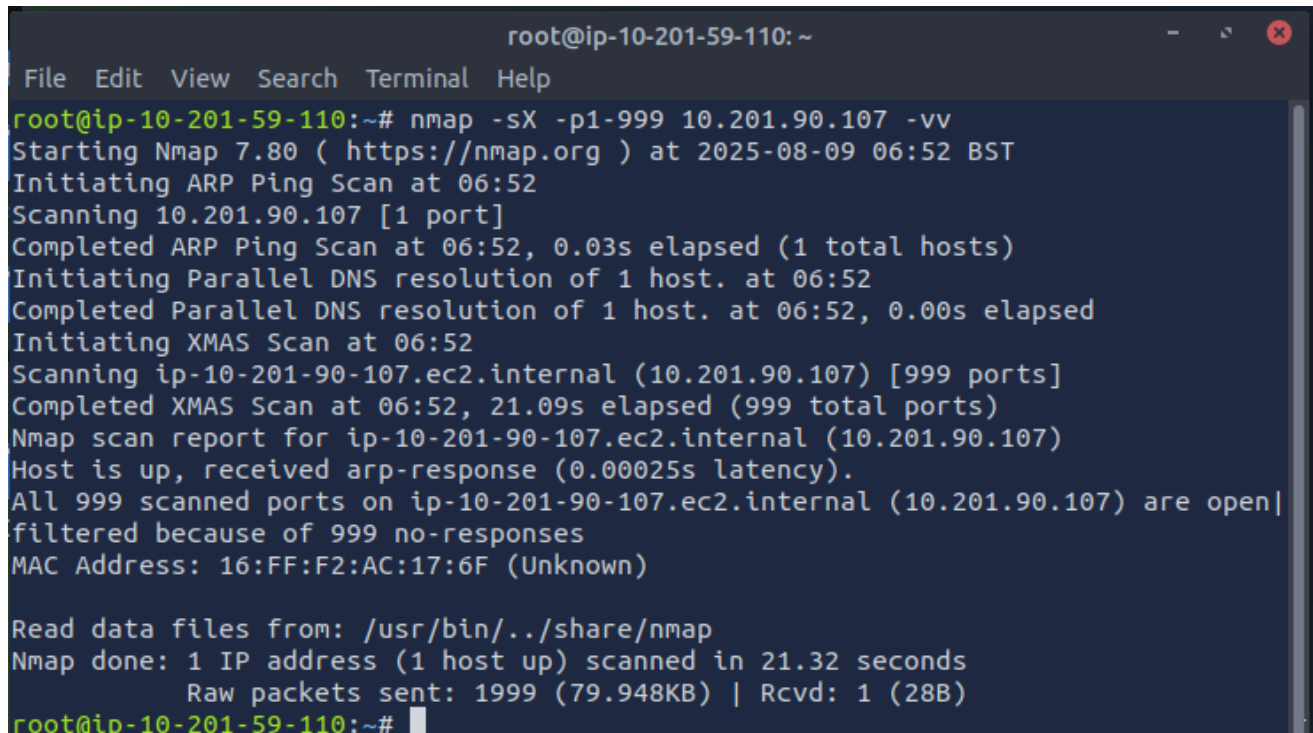
**Ans:** N

2. Perform an Xmas scan on the first 999 ports of the target — how many ports are shown to be open or filtered?

**Ans:** 999

3. What is the reason for the above result?

**Ans:** No response

A screenshot of a terminal window titled 'root@ip-10-201-59-110: ~'. The terminal shows the execution of an Nmap XMAS scan on the target IP 10.201.90.107. The command used is 'nmap -sX -p1-999 10.201.90.107 -vv'. The output indicates that the host is up, but all 999 scanned ports are filtered due to no responses. The scan took 21.32 seconds and sent 1999 raw packets.

```
root@ip-10-201-59-110: ~  
File Edit View Search Terminal Help  
root@ip-10-201-59-110:~# nmap -sX -p1-999 10.201.90.107 -vv  
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-09 06:52 BST  
Initiating ARP Ping Scan at 06:52  
Scanning 10.201.90.107 [1 port]  
Completed ARP Ping Scan at 06:52, 0.03s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 06:52  
Completed Parallel DNS resolution of 1 host. at 06:52, 0.00s elapsed  
Initiating XMAS Scan at 06:52  
Scanning ip-10-201-90-107.ec2.internal (10.201.90.107) [999 ports]  
Completed XMAS Scan at 06:52, 21.09s elapsed (999 total ports)  
Nmap scan report for ip-10-201-90-107.ec2.internal (10.201.90.107)  
Host is up, received arp-response (0.00025s latency).  
All 999 scanned ports on ip-10-201-90-107.ec2.internal (10.201.90.107) are open|  
filtered because of 999 no-responses  
MAC Address: 16:FF:F2:AC:17:6F (Unknown)  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 21.32 seconds  
Raw packets sent: 1999 (79.948KB) | Rcvd: 1 (28B)  
root@ip-10-201-59-110:~#
```

4. Perform a TCP SYN scan on the first 5000 ports of the target — how many ports are shown to be open?

**Ans:** 5

```

File Edit View Search Terminal Help
root@ip-10-201-59-110:~# sudo nmap -p1-5000 -sS 10.201.90.107 -Pn -vv
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-09 06:54 BST
Initiating ARP Ping Scan at 06:54
Scanning 10.201.90.107 [1 port]
Completed ARP Ping Scan at 06:54, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:54
Completed Parallel DNS resolution of 1 host. at 06:54, 0.00s elapsed
Initiating SYN Stealth Scan at 06:54
Scanning ip-10-201-90-107.ec2.internal (10.201.90.107) [5000 ports]
Discovered open port 3389/tcp on 10.201.90.107
Discovered open port 53/tcp on 10.201.90.107
Discovered open port 80/tcp on 10.201.90.107
Discovered open port 135/tcp on 10.201.90.107
Discovered open port 21/tcp on 10.201.90.107
Completed SYN Stealth Scan at 06:55, 30.14s elapsed (5000 total ports)
Nmap scan report for ip-10-201-90-107.ec2.internal (10.201.90.107)
Host is up, received arp-response (0.00031s latency).
Scanned at 2025-08-09 06:54:39 BST for 30s
Not shown: 4995 filtered ports
Reason: 4995 no-responses
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 128
53/tcp    open  domain       syn-ack ttl 128
80/tcp    open  http         syn-ack ttl 128
135/tcp   open  msrpc        syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
MAC Address: 16:FF:F2:AC:17:6F (Unknown)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 30.31 seconds
Raw packets sent: 15014 (660.600KB) | Rcvd: 29 (1.260KB)

```

5. Deploy the ftp-anon script against the box. Can Nmap login successfully to the FTP server on port 21 (Y/N)?

**Ans: Y**

## Conclusion

The “Further Nmap” room provides a comprehensive exploration of advanced Nmap scanning techniques. By covering TCP, SYN, UDP, NULL, FIN, and Xmas scans, as well as NSE scripting and firewall evasion, it reinforces critical skills used in network enumeration and security auditing. The hands-on tasks help learners understand how to detect services, bypass filters, and analyze host responses. Mastery of these Nmap features is essential for ethical hacking, penetration testing, and professional cybersecurity assessments.