ElevateLabs Cybersecurity Internship 2025 DAY01

Task 01

Default nmap Scan on network:172.20.10.2/28

```
┌──(abhipnair㉿kali)-[~]
└─$ sudo nmap 172.20.10.2/28
[sudo] password for abhipnair:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 19:20 IST
Nmap scan report for 172.20.10.1
Host is up (0.00091s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
49152/tcp open  unknown
62078/tcp open  iphone-sync
MAC Address: E8:10:72:2D:1E:62  (Unknown)

Nmap scan report for 172.20.10.3
Host is up (0.00023s latency).
Not shown: 969 filtered tcp ports (no-response), 28 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:ED:BE:6A (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.20.10.5
Host is up (0.00024s latency).
All 1000 scanned ports on 172.20.10.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2:F7:13:54:0F:23 (Unknown)

Nmap scan report for 172.20.10.2
Host is up (0.0000050s latency).
All 1000 scanned ports on 172.20.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 16 IP addresses (4 hosts up) scanned in 7.96 seconds
```

TCP SYN or PING SCAN to check the hosts alive in ip: 172.20.10.2/28

```
┌──(abhipnair㉿kali)-[~]
└─$ sudo nmap -sn 172.20.10.2/28
[sudo] password for abhipnair:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 19:43 IST
Nmap scan report for 172.20.10.1
Host is up (0.00058s latency).
MAC Address: E8:10:72:2D:1E:62 (Unknown)
Nmap scan report for 172.20.10.3
Host is up (0.00023s latency).
MAC Address: 08:00:27:ED:BE:6A (Oracle VirtualBox virtual NIC)
Nmap scan report for 172.20.10.5
Host is up (0.00023s latency).
MAC Address: D2:F7:13:54:0F:23  (Unknown)
Nmap scan report for 172.20.10.2
Host is up.
Nmap done: 16 IP addresses (4 hosts up) scanned in 1.53 seconds
```

Nmap Agressive Scan to find open ports, services, service version, os fingerprinting, traceroute

```
┌──(abhipnair㉿kali)-[~]
└─$ sudo nmap -A 172.20.10.2/28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 19:25 IST
Stats: 0:00:31 elapsed; 12 hosts completed (3 up), 3 undergoing Script Scan
NSE Timing: About 94.66% done; ETC: 19:26 (0:00:00 remaining)
Nmap scan report for 172.20.10.1
Host is up (0.00070s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
53/tcp   open  domain     (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|  version
|  bind
|  root-servers
|  nstld
|_ verisign-grs
49152/tcp open  tcpwrapped
62078/tcp open  tcpwrapped
```

```
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94SVN%I=7%D=5/26%Time=683472E9%P=x86_64-pc-linux-gnu%r(D
SF:NSVersionBindReqTCP,6B,"\0i\0\x06\x81\x83\0\x01\0\0\0\x01\0\0\x07versio
SF:n\x04bind\0\0\x10\0\x01\0\0\x06\0\x01\0\0\x0e\x10\0@\x01a\x0croot-serve
SF:rs\x03net\0\x05nstld\x0cverisign-grs\x03com\0x\xb3\xd9\xb8\0\0\x07\x08\
SF:0\0\x03\x84\0\t:\x80\0\x01Q\x80")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x
SF:90\x04\0\0\0\0\0\0\0\0");
MAC Address: E8:10:72:2D:1E:62 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint: deleted due to security reasons

Network Distance: 1 hop

TRACEROUTE
HOP RTT  ADDRESS
1   0.70 ms 172.20.10.1

Nmap scan report for 172.20.10.3
Host is up (0.00035s latency).
Not shown: 969 filtered tcp ports (no-response), 28 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp    vsftpd 3.0.5
22/tcp open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 67:bb:3c:82:b9:33:1f:28:87:33:a8:6b:c1:6a:72:97 (RSA)
|   256 77:5b:0f:34:b3:41:75:54:f0:ce:ab:01:a2:4e:4a:7b (ECDSA)
|_  256 47:43:6c:16:51:2c:67:5d:50:3e:d7:47:d8:1b:cb:bb (ED25519)
80/tcp open  http   Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Haunted CTF Challenge
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:ED:BE:6A (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.8 (94%), Linux 5.1
(93%), Linux 2.6.32 - 3.13 (93%), Linux 2.6.39 (93%), Linux 5.0 - 5.5 (92%), Linux
2.6.22 - 2.6.36 (91%), Linux 3.10 - 4.11 (91%), Linux 5.0 (91%), Linux 3.10 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
TRACEROUTE
HOP RTT  ADDRESS
1   0.35 ms 172.20.10.3

Nmap scan report for 172.20.10.5
Host is up (0.00012s latency).
All 1000 scanned ports on 172.20.10.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2:F7:13:54:0F:23 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT  ADDRESS
1   0.12 ms 172.20.10.5

Nmap scan report for 172.20.10.2
Host is up (0.000032s latency).
All 1000 scanned ports on 172.20.10.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 16 IP addresses (4 hosts up) scanned in 38.37 seconds
```

Note: This scan leaves much fingerprinting in the network so avoid while doing in real time pentesting.

Points to Note;

IP Address	MAC Address	Open Ports	Services & Versions
172.20.10.1	E8:10:72:2D:1E:62	21, 53, 49152, 62078	FTP (tcpwrapped), DNS (generic), Unknown TCP (tcpwrapped)
172.20.10.2	Unknown	None	All 1000 ports closed
172.20.10.3	08:00:27:ED:BE:6A	21, 22, 80	FTP (vsftpd 3.0.5), SSH (OpenSSH 8.2p1), HTTP (Apache 2.4.41, Ubuntu)
172.20.10.5	D2:F7:13:54:0F:23	None	All 1000 ports closed

📌 Important Points to Note

1. **Live Host Detection:**
    - 4 hosts are up using `-sn` ping scan.
    - MAC addresses help identify vendor/hypervisor (e.g., VirtualBox detected on .3).
2. **Filtered Ports:**
    - Host .3 had **969 filtered ports**, indicating possible **firewall or security group** rules blocking access.
3. **Aggressive Scan (`-A`) Outputs:**
    - Service versions, OS detection, and traceroute info collected.
    - Host .3 revealed detailed service banners (vsftpd, OpenSSH, Apache).
4. **Unusual/Open High Ports:**

- Host .1 has ports **49152** and **62078** open (used by certain devices like **iOS sync or dynamic RPC**).

5. **OS Fingerprinting:**
   - OS detection succeeded partially:
     - .3: Linux 5.0–5.4 (approx. 98% certainty).
     - .1 and .5: Too many matches or inconclusive due to response fingerprinting limits.

6. **TCPwrapped Services:**
   - Several ports (like FTP on .1) are marked as **tcpwrapped**, meaning they may drop connections without banners—common in hardened environments.

7. **Nmap Footprint Warning:**
   - The aggressive scan leaves **network fingerprints**, making it **unsuitable for stealthy or production environments**.