

Assignment 4

Q. scan any two domains from the below list and perform a network scan using the nmap command on the below mentioned domains only.

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap --dns-servers 203.111.26.50
141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:23 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -PN 141.223.197.31

Command 'nmap' not found, did you mean:

  command 'nmap' from snap nmap (7.93)
  command 'nap' from snap nap-snippets (0.1.1)
  command 'nmap' from deb nmap (7.80+dfsg1-2build1)
  command 'nama' from deb nama (1.216-1)
  command 'nam' from deb nam (1.15-5build1)
  command 'pamp' from deb paml (4.9j+dfsg-1)

See 'snap info <snapname>' for additional versions.

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -PN 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Nmap scan report for 141.223.197.31
Host is up (0.015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
113/tcp   closed ident
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC: ~/IM/Akash/Ethical Hacking
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~/IM/Akash/Ethical Hacking$ nmap 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:19 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
snap/nmap/2944/usr/bin/nmap: option '-exclude' requires an argument
see the output of nmap -h for a summary of options.
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~/IM/Akash/Ethical Hacking$ nmap --exclude 203.111.26.50 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:22 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds

```

```
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap --exclude 203.111.26.50 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:23 IST
Nmap scan report for 141.223.197.31
Host is up (0.00062s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap --dns-servers 203.111.26.50 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:23 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 17.73 seconds
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$
```

Activities Terminal Feb 28 15:19 administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC: ~/IM/Akash/Ethical Hacking

```
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~/IM/Akash/Ethical Hacking$ nmap 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:19 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds
administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~/IM/Akash/Ethical Hacking$ ./studio.sh
```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -PN 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Nmap scan report for 141.223.197.31
Host is up (0.015s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
113/tcp   closed ident
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

```

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -n 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Nmap scan report for 141.223.197.31
Host is up (0.00064s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
587/tcp   open  submission

```

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ █

```

Nmap done: 1 IP address (1 host up) scanned in 4.53 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p80 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).

```

```

PORT      STATE SERVICE
80/tcp    open  http

```

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -6 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Warning: Hostname 141.223.197.31 resolves, but not to any IPv6 address. Try scanning without -6
Failed to resolve "141.223.197.31".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ █

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p80 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:26 IST
Nmap scan report for 141.223.197.31
Host is up (0.00060s latency).

```

```

PORT      STATE SERVICE
80/tcp    open  http

```

Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ █

```

Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p 80,443,23 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:27 IST
Nmap scan report for 141.223.197.31
Host is up (0.00062s latency).

```

```

PORT      STATE SERVICE
23/tcp    filtered telnet
80/tcp    open  http
443/tcp    open  https

```

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p 1-100 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:28 IST
Nmap scan report for 141.223.197.31
Host is up (0.00057s latency).
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

```

Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ █

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p smtp 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:30 IST
Nmap scan report for 141.223.197.31
Host is up (0.00057s latency).

```

```

PORT      STATE      SERVICE
25/tcp    filtered  smtp

```

```

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p [1-65535] 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:31 IST
Nmap scan report for 141.223.197.31
Host is up (0.00069s latency).

```

```

Not shown: 8361 filtered tcp ports (no-response)

```

```

PORT      STATE      SERVICE
80/tcp    open       http
110/tcp   open       pop3
143/tcp   open       imap
443/tcp   open       https
587/tcp   open       submission

```

```

Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -sP 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-03 13:29 IST
Nmap scan report for 141.223.197.31
Host is up (0.00042s latency).

```

```

Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -sP -Ps 141.223.197.31
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
QUITTING!

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -sP -PS 141.223.197.31

```

```

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-03 13:30 IST
Nmap scan report for 141.223.197.31
Host is up (0.00050s latency).

```

```

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -p smtp* 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-28 15:31 IST
Nmap scan report for 141.223.197.31
Host is up (0.00053s latency).

```

```

PORT      STATE      SERVICE
25/tcp    filtered  smtp
465/tcp    filtered  smtps

```

```

Nmap done: 1 IP address (1 host up) scanned in 1.22 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$ nmap -sP 141.223.197.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-03 13:29 IST
Nmap scan report for 141.223.197.31
Host is up (0.00042s latency).

```

```

Nmap done: 1 IP address (1 host up) scanned in 3.01 seconds

```

```

administrator@administrator-HP-ProDesk-400-G7-Small-Form-Factor-PC:~$

```