

T1. Using both host and dig commands, demonstrate whether the host sdf.org is live or not. Attach screenshots showing the results

```
(alex@kali)~$ host sdf.org
sdf.org has address 205.166.94.16
sdf.org mail is handled by 50 mx.sdf.org.

(alex@kali)~$ dig sdf.org

; <<>> DiG 9.20.9-1-Debian <<>> sdf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 17417
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: c4b34b6ad189350a1416cae268d31db9dee7489ff824edf7 (good)
;; QUESTION SECTION:
;sdf.org.                                IN      A

;; ANSWER SECTION:
sdf.org.                7603    IN      A      205.166.94.16

;; Query time: 8 msec
```

T2. Perform DNS enumeration using dnsenum command for the host sdf.org. Check whether the zone transfer is possible. Provide necessary screenshots.

```
(alex@kali)~$ dnsenum sdf.org
dnsenum VERSION:1.3.1

sdf.org

Host's addresses:

sdf.org.                7555    IN      A      205.166.94.1
6

Name Servers:

ns-d.sdf.org.           8306    IN      A      172.81.178.4
0
ns-b.sdf.org.           8306    IN      A      66.148.112.1
51
ns-a.sdf.org.           8306    IN      A      205.166.94.2
4
ns-c.sdf.org.           8306    IN      A      178.63.35.19
5

Mail (MX) Servers:

mx.sdf.org.             8306    IN      A      205.166.94.2
4

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for sdf.org on ns-d.sdf.org ...
AXFR record query failed: REFUSED

Trying Zone Transfer for sdf.org on ns-b.sdf.org ...
AXFR record query failed: REFUSED

Trying Zone Transfer for sdf.org on ns-a.sdf.org ...
```

T3. Perform both ICMP Sweep and TCP Sweep for the host sdf.org using NMAP. Use the option --reason to show the details and disable the arp-ping. Attach screenshots showing the results.

```

$ nmap -PE --disable-arp-ping --reason sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 18:26 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received echo-reply ttl 255 (0.071s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
23/tcp    open  telnet       syn-ack ttl 64
70/tcp    open  gopher       syn-ack ttl 64
79/tcp    open  finger       syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
110/tcp   open  pop3         syn-ack ttl 64
111/tcp   open  rpcbind      syn-ack ttl 64
113/tcp   open  ident        syn-ack ttl 64
143/tcp   open  imap         syn-ack ttl 64
443/tcp   open  https        syn-ack ttl 64
993/tcp   open  imaps        syn-ack ttl 64
1022/tcp  open  exp2         syn-ack ttl 64
1023/tcp  open  netvenuechat syn-ack ttl 64
8080/tcp  open  http-proxy   syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds

(alex@kali)-[~]
$ nmap -PS80,443 --disable-arp-ping --reason sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 18:26 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received syn-ack ttl 64 (0.077s latency).
Not shown: 986 filtered tcp ports (no-response)

```

T4. Perform port scanning to determine all open ports and corresponding running services for the host sdf.org. Attach screenshots showing the results

```

(alex@kali)-[~]
$ nmap -p- --disable-arp-ping --reason sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 18:29 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.040s latency).
Not shown: 49184 filtered tcp ports (net-unreach), 16337 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
23/tcp    open  telnet       syn-ack ttl 64
70/tcp    open  gopher       syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
110/tcp   open  pop3         syn-ack ttl 64
111/tcp   open  rpcbind      syn-ack ttl 64
113/tcp   open  ident        syn-ack ttl 64
143/tcp   open  imap         syn-ack ttl 64
443/tcp   open  https        syn-ack ttl 64
993/tcp   open  imaps        syn-ack ttl 64
1023/tcp  open  netvenuechat syn-ack from 10.0.2.2 ttl 64
1965/tcp  open  tivoli-npm   net-unreach from 10.0.2.2 ttl 255
7902/tcp  open  tnos-dp      syn-ack ttl 64
8080/tcp  open  http-proxy   syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 142.02 seconds

(alex@kali)-[~]
$ nmap -sV --disable-arp-ping --reason sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 18:33 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.047s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 NetBSD lukemftpd
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 10.0 (protocol 2.0)
23/tcp    open  telnet       syn-ack ttl 64 BSD-derived telnetd
70/tcp    open  gopher?     syn-ack ttl 64
79/tcp    open  finger?     syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
110/tcp   open  ssh          syn-ack ttl 64 OpenSSH 10.0 (protocol 2.0)
111/tcp   open  rpcbind      syn-ack ttl 64 2-4 (RPC #100000)
113/tcp   open  ident        syn-ack ttl 64 mlidentd or bidentd
143/tcp   open  ssh          syn-ack ttl 64 OpenSSH 10.0 (protocol 2.0)
443/tcp   open  ssl/http     syn-ack ttl 64 Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
993/tcp   open  ssh          syn-ack ttl 64 OpenSSH 10.0 (protocol 2.0)
1022/tcp  open  nlockmgr     syn-ack ttl 64 0-4 (RPC #100021)
1023/tcp  open  ypbind       syn-ack ttl 64 2 (RPC #100007)
8080/tcp  open  ssh          syn-ack ttl 64 OpenSSH 10.0 (protocol 2.0)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-servi

```

Q2.

T1. sing NSE scripts, determine all known vulnerabilities present in the host sdf.org. Attach a screenshot showing your command and the results you got.

```
(alex@kali)-[~]
$ nmap --script vuln sdf.org -p- --disable-arp-ping --reason
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 18:49 EDT
Nmap scan report for sdf.org (205.166.94.16)

|_ http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDs: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|       http://ha.ckers.org/slowloris/
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 710.51 seconds
```

T2. Perform a brute force attack on sdf.org. You can choose any script from the followings: ftp-brute, snmp-brute, http-brute, and oracle-brute. Attach screenshots showing your command and the results you received.

```
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
/usr/share/nmap/scripts

(alex@kali)-[~]
$ nmap --script http-brute -p161 192.168.56.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 19:10 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00011s latency).

PORT      STATE      SERVICE
161/tcp   filtered  snmp

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```