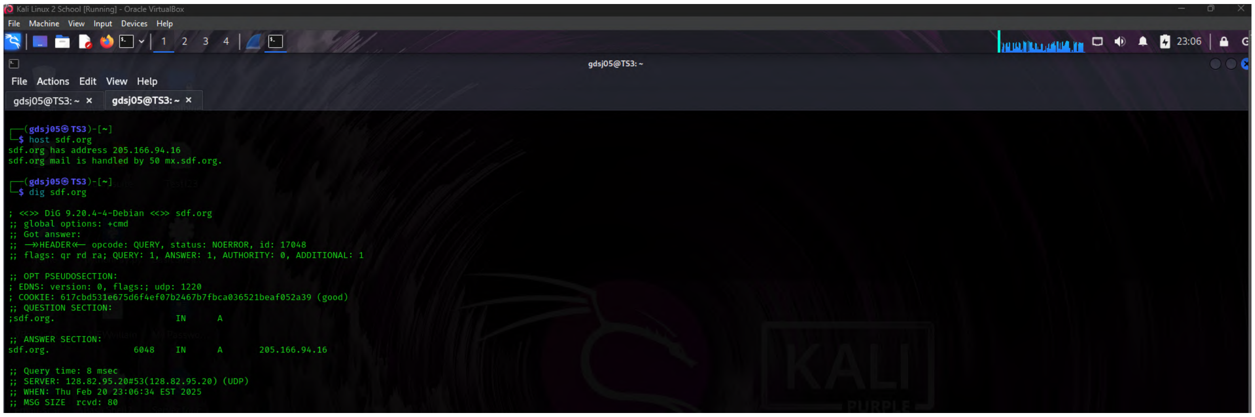
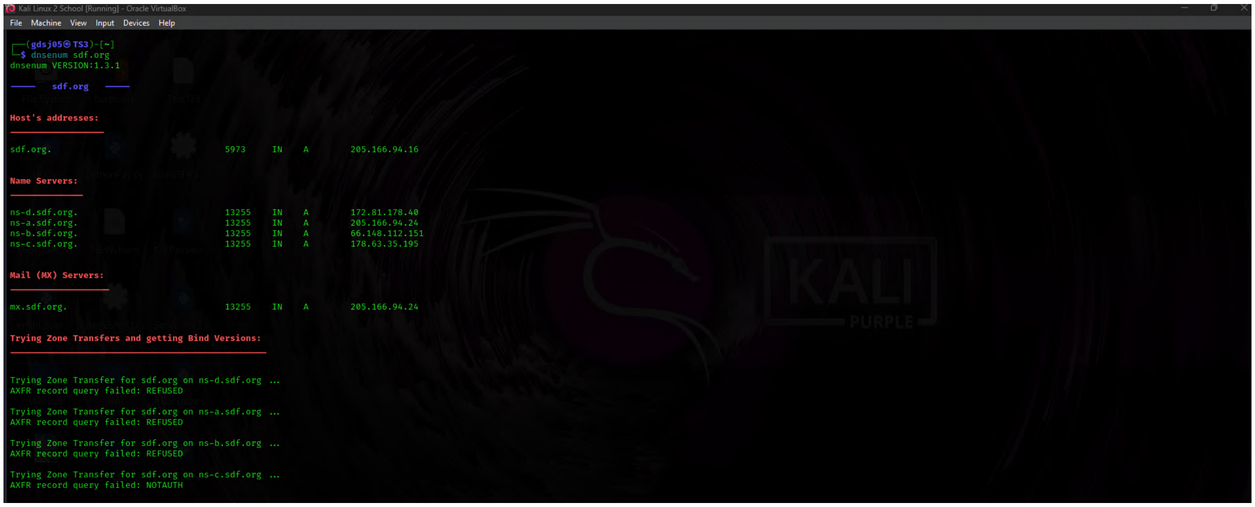
Question 1: Active Scanning

- T1: Using both host and dig commands, demonstrate whether the host sdf.org is live or not. Attach screenshots showing the results. 4 points



```
┌──(gdsj05㉿TS3)-[~]
└─$ host sdf.org
sdf.org has address 205.166.94.16
sdf.org mail is handled by 50 mx.sdf.org.

┌──(gdsj05㉿TS3)-[~]
└─$ dig sdf.org

; <<>> DiG 9.20.4-4-Debian <<>> sdf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17048
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 617cbd531e675d6f4ef07b2467b7fbca036521beaf052a39 (good)
;; QUESTION SECTION:
;sdf.org.                       IN      A

;; ANSWER SECTION:
sdf.org.                6048    IN      A       205.166.94.16

;; Query time: 8 msec
;; SERVER: 128.82.95.20#53(128.82.95.20) (UDP)
;; WHEN: Thu Feb 20 23:06:34 EST 2025
;; MSG SIZE  rcvd: 80
```

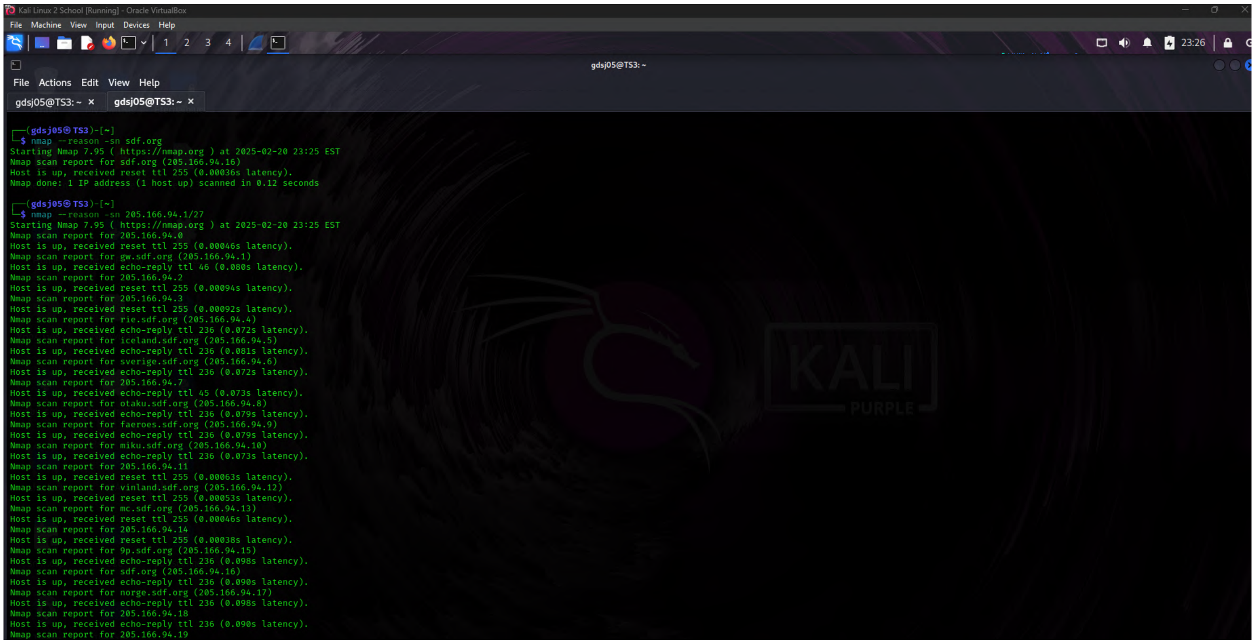
- T2: Perform DNS enumeration using dnsenum command for the host sdf.org. Check whether the zone transfer is possible. Provide necessary screenshots. 4 points



```
┌──(gdsj05㉿TS3)-[~]
└─$ dnsenum sdf.org
dnsenum VERSION:1.3.1

─────   sdf.org   ─────


Host's addresses:
__________________

sdf.org.                                 5973     IN    A        205.166.94.16


Name Servers:
______________

ns-d.sdf.org.                            13255    IN    A        172.81.178.40
ns-a.sdf.org.                            13255    IN    A        205.166.94.24
ns-b.sdf.org.                            13255    IN    A        66.148.112.151
ns-c.sdf.org.                            13255    IN    A        178.63.35.195


Mail (MX) Servers:
___________________

mx.sdf.org.                              13255    IN    A        205.166.94.24


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-a.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-c.sdf.org ...
AXFR record query failed: NOTAUTH
```

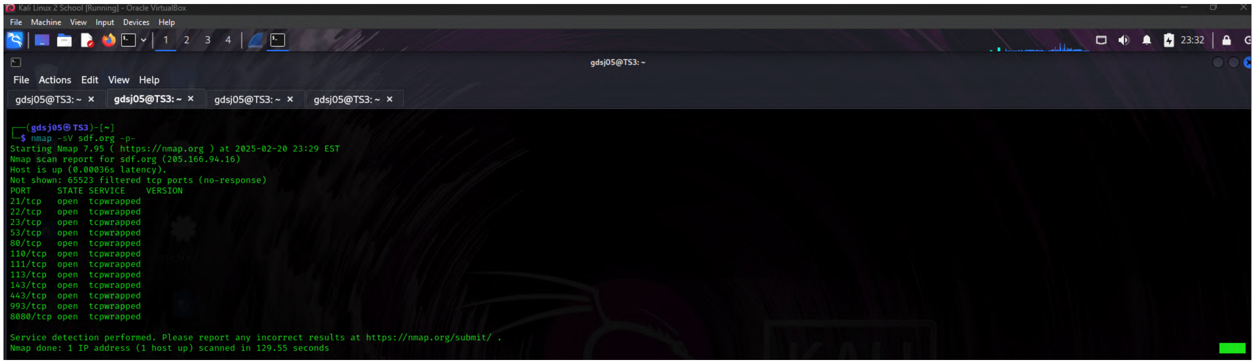
No

- 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. 6 points


Kali Linux 2 School [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:26
gdsj05@TS3: ~
File Actions Edit View Help
gdsj05@TS3: ~
gdsj05@TS3: ~

```
┌──(gdsj05㉿TS3)-[~]
└─$ nmap --reason -sn sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:25 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.00036s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

┌──(gdsj05㉿TS3)-[~]
└─$ nmap --reason -sn 205.166.94.1/27
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:25 EST
Nmap scan report for 205.166.94.0
Host is up, received reset ttl 255 (0.00046s latency).
Nmap scan report for gw.sdf.org (205.166.94.1)
Host is up, received echo-reply ttl 46 (0.080s latency).
Nmap scan report for 205.166.94.2
Host is up, received reset ttl 255 (0.00094s latency).
Nmap scan report for 205.166.94.3
Host is up, received reset ttl 255 (0.00092s latency).
Nmap scan report for rie.sdf.org (205.166.94.4)
Host is up, received echo-reply ttl 236 (0.072s latency).
Nmap scan report for iceland.sdf.org (205.166.94.5)
Host is up, received echo-reply ttl 236 (0.081s latency).
Nmap scan report for sverige.sdf.org (205.166.94.6)
Host is up, received echo-reply ttl 236 (0.072s latency).
Nmap scan report for 205.166.94.7
Host is up, received echo-reply ttl 45 (0.073s latency).
Nmap scan report for otaku.sdf.org (205.166.94.8)
Host is up, received echo-reply ttl 236 (0.079s latency).
Nmap scan report for faeroes.sdf.org (205.166.94.9)
Host is up, received echo-reply ttl 236 (0.079s latency).
Nmap scan report for miku.sdf.org (205.166.94.10)
Host is up, received echo-reply ttl 236 (0.073s latency).
Nmap scan report for 205.166.94.11
Host is up, received reset ttl 255 (0.00063s latency).
Nmap scan report for vinland.sdf.org (205.166.94.12)
Host is up, received reset ttl 255 (0.00053s latency).
Nmap scan report for mc.sdf.org (205.166.94.13)
Host is up, received reset ttl 255 (0.00046s latency).
Nmap scan report for 205.166.94.14
Host is up, received reset ttl 255 (0.00038s latency).
Nmap scan report for 9p.sdf.org (205.166.94.15)
Host is up, received echo-reply ttl 236 (0.098s latency).
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received echo-reply ttl 236 (0.090s latency).
Nmap scan report for norge.sdf.org (205.166.94.17)
Host is up, received echo-reply ttl 236 (0.098s latency).
Nmap scan report for 205.166.94.18
Host is up, received echo-reply ttl 236 (0.090s latency).
Nmap scan report for 205.166.94.19
```

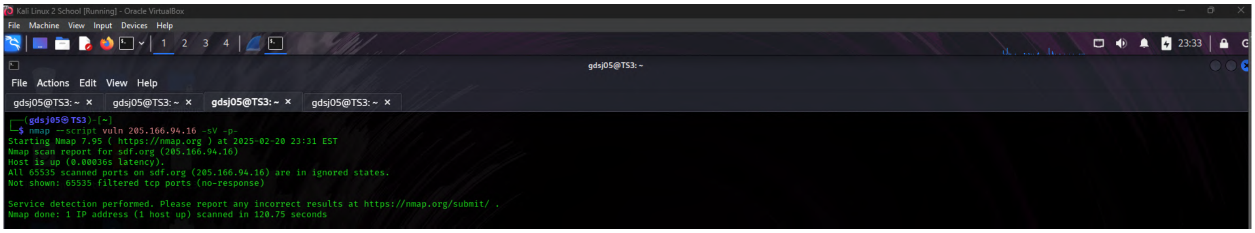
- T4: Perform port scanning to determine all open ports and corresponding running services for the host sdf.org. Attach screenshots showing the results. 6 points


Kali Linux 2 School [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:32
gdsj05@TS3: ~
File Actions Edit View Help
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~

```
┌──(gdsj05㉿TS3)-[~]
└─$ nmap -sV sdf.org -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:29 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.00036s latency).
Not shown: 65523 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  tcpwrapped
23/tcp   open  tcpwrapped
53/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
110/tcp  open  tcpwrapped
111/tcp  open  tcpwrapped
113/tcp  open  tcpwrapped
143/tcp  open  tcpwrapped
443/tcp  open  tcpwrapped
993/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.55 seconds
```

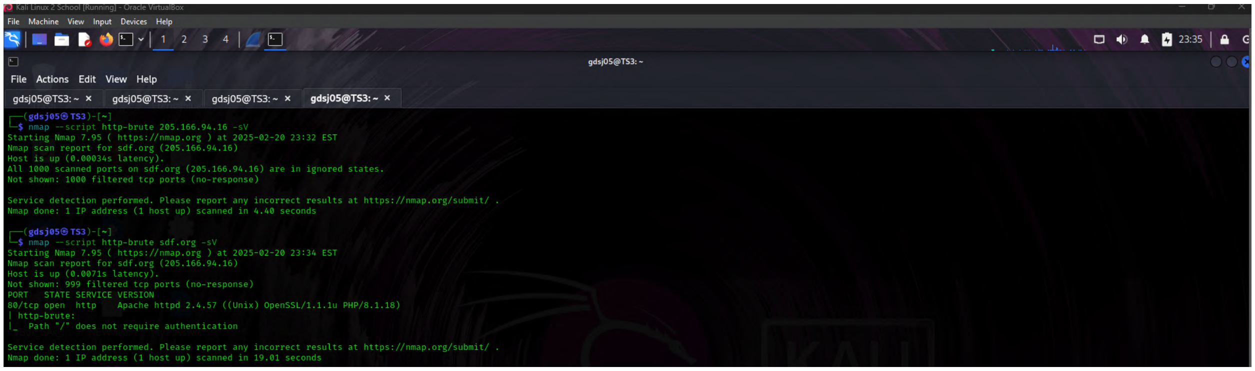
Question 2: Vulnerability Scanning

- T1: Using NSE scripts, determine all known vulnerabilities present in the host sdf.org. Attach a screenshot showing your command and the results you got. 5 points


Kali Linux 2 School [Running] - Oracle VirtualBox
File Machine View Input Devices Help
23:33
gdsj05@TS3: ~
File Actions Edit View Help
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~

```
┌──(gdsj05㉿TS3)-[~]
└─$ nmap --script vuln 205.166.94.16 -sV -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:31 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.00036s latency).
All 65535 scanned ports on sdf.org (205.166.94.16) are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 120.75 seconds
```

- T2: Perform a brute force attack on sdf.org. You can choose any script from the following: ftp-brute, snmp-brute, http-brute, and oracle-brute. Attach screenshots showing your command and the results you received. 5 points


Kali Linux 2 School [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
23:35
gdsj05@TS3: ~
File Actions Edit View Help
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~
gdsj05@TS3: ~

```
┌──(gdsj05㉿TS3)-[~]
└─$ nmap --script http-brute 205.166.94.16 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:32 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.00034s latency).
All 1000 scanned ports on sdf.org (205.166.94.16) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.40 seconds

┌──(gdsj05㉿TS3)-[~]
└─$ nmap --script http-brute sdf.org -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 23:34 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.0071s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Unix) OpenSSL/1.1.1u PHP/8.1.18)
| http-brute:
|_  Path "/" does not require authentication

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.01 seconds
```