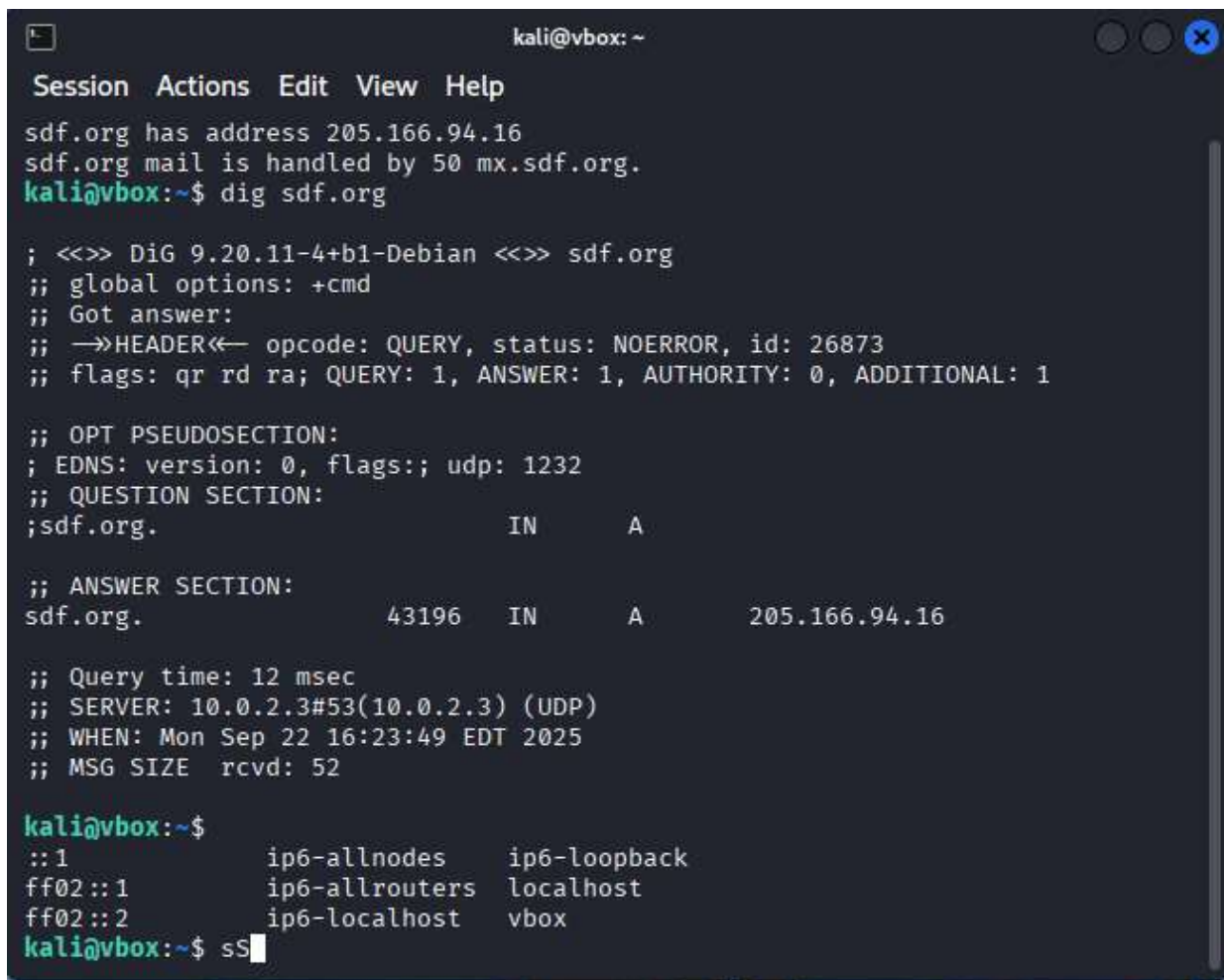


Lab 3: Active Reconnaissance and Vulnerability Scanning

Total Points: 30

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**



```
kali@vbox: ~  
Session Actions Edit View Help  
sdf.org has address 205.166.94.16  
sdf.org mail is handled by 50 mx.sdf.org.  
kali@vbox:~$ dig sdf.org  
  
; <<>> DiG 9.20.11-4+b1-Debian <<>> sdf.org  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26873  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
;; QUESTION SECTION:  
;sdf.org.                IN      A  
  
;; ANSWER SECTION:  
sdf.org.                43196  IN      A      205.166.94.16  
  
;; Query time: 12 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)  
;; WHEN: Mon Sep 22 16:23:49 EDT 2025  
;; MSG SIZE rcvd: 52  
  
kali@vbox:~$  
::1          ip6-allnodes   ip6-loopback  
ff02::1     ip6-allrouters localhost  
ff02::2     ip6-localhost  vbox  
kali@vbox:~$ sS
```

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

Trying Zone Transfers and getting Bind Versions:

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

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

```
kali@vbox: ~  
Session Actions Edit View Help  
from reverse lookup results, useful on invalid hostnames.  
OUTPUT OPTIONS:  
  -o --output <file>    Output in XML format. Can be imported in MagicTree (w  
ww.gremwell.com)  
kali@vbox:~$ dnsenum sdf.org  
dnsenum VERSION:1.3.1  
  
———— sdf.org ————  
  
Host's addresses:  
  
sdf.org.          43162    IN      A       205.166.94.1  
6  
  
Name Servers:  
  
ns-a.sdf.org.    43200    IN      A       205.166.94.2  
4  
ns-d.sdf.org.    43200    IN      A       172.81.178.4  
0  
ns-b.sdf.org.    43200    IN      A       66.148.112.1  
51  
ns-c.sdf.org.    43200    IN      A       178.63.35.19  
5
```

- **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

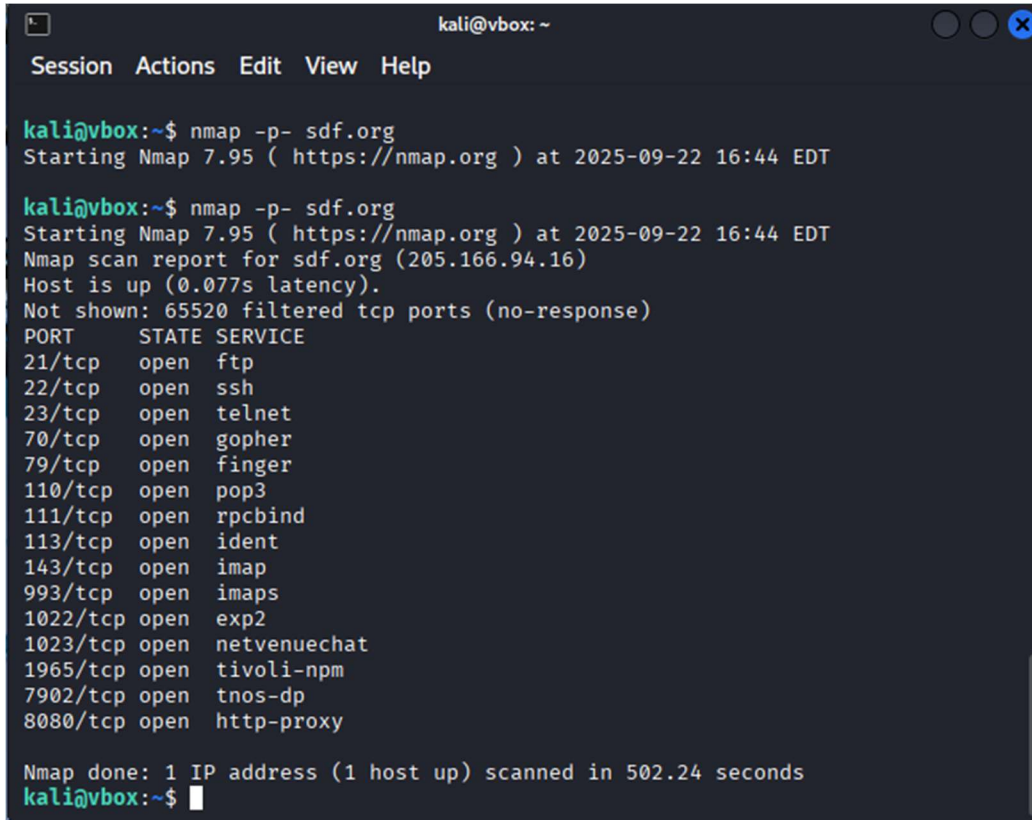
showing the results.

6 points

```
kali@vbox: ~  
Session Actions Edit View Help  
Host is up, received reset ttl 255 (0.066s latency).  
Not shown: 987 filtered tcp ports (no-response)  
PORT      STATE SERVICE      REASON  
21/tcp    open  ftp          syn-ack  
22/tcp    open  ssh          syn-ack  
23/tcp    open  telnet       syn-ack  
70/tcp    open  gopher       syn-ack  
79/tcp    open  finger       syn-ack  
110/tcp   open  pop3         syn-ack  
111/tcp   open  rpcbind      syn-ack  
113/tcp   open  ident        syn-ack  
143/tcp   open  imap         syn-ack  
993/tcp   open  imaps        syn-ack  
1022/tcp  open  exp2         syn-ack  
1023/tcp  open  netvenuechat syn-ack  
8080/tcp  open  http-proxy   syn-ack  
  
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds  
kali@vbox:~$ nmap -pn --reason sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 16:35 EDT  
Found no matches for the service mask 'n' and your specified protocols  
QUITTING!  
kali@vbox:~$ nmap -sn --reason --disable-arp-ping sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 16:36 EDT  
Nmap scan report for sdf.org (205.166.94.16)  
Host is up, received reset ttl 255 (0.00031s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds  
kali@vbox:~$ █
```

```
kali@vbox: ~  
Session Actions Edit View Help  
993/tcp open  imaps      syn-ack  
1022/tcp open  exp2       syn-ack  
1023/tcp open  netvenuechat syn-ack  
8080/tcp open  http-proxy syn-ack  
  
Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds  
kali@vbox:~$ nmap -sT --reason --disable-arp-ping sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 16:34 EDT  
Nmap scan report for sdf.org (205.166.94.16)  
Host is up, received reset ttl 255 (0.066s latency).  
Not shown: 987 filtered tcp ports (no-response)  
PORT      STATE SERVICE      REASON  
21/tcp    open  ftp          syn-ack  
22/tcp    open  ssh          syn-ack  
23/tcp    open  telnet       syn-ack  
70/tcp    open  gopher       syn-ack  
79/tcp    open  finger       syn-ack  
110/tcp   open  pop3         syn-ack  
111/tcp   open  rpcbind      syn-ack  
113/tcp   open  ident        syn-ack  
143/tcp   open  imap         syn-ack  
993/tcp   open  imaps        syn-ack  
1022/tcp  open  exp2         syn-ack  
1023/tcp  open  netvenuechat syn-ack  
8080/tcp  open  http-proxy   syn-ack  
  
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds  
kali@vbox:~$
```

- **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@vbox: ~
Session Actions Edit View Help

kali@vbox:~$ nmap -p- sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 16:44 EDT

kali@vbox:~$ nmap -p- sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 16:44 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.077s latency).
Not shown: 65520 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
70/tcp    open  gopher
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
143/tcp   open  imap
993/tcp   open  imaps
1022/tcp  open  exp2
1023/tcp  open  netvenuechat
1965/tcp  open  tivoli-npm
7902/tcp  open  tnos-dp
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 502.24 seconds
kali@vbox:~$
```

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@vbox: ~
Session Actions Edit View Help
143/tcp open  imap
993/tcp open  imaps
|_ssl-ccs-injection: No reply from server (TIMEOUT)
1022/tcp open  exp2
1023/tcp open  netvenuechat
8080/tcp open  http-proxy
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
| 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:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
Nmap done: 1 IP address (1 host up) scanned in 105.99 seconds
kali@vbox:~$
```

- **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.

5 points

```
kali@vbox: ~  
Session Actions Edit View Help  
| References:  
| http://ha.ckers.org/slowloris/  
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750  
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  
  
Nmap done: 1 IP address (1 host up) scanned in 105.99 seconds  
kali@vbox:~$ nmap --script http-brute sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 17:00 EDT  
Nmap scan report for sdf.org (205.166.94.16)  
Host is up (0.051s latency).  
Not shown: 987 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
70/tcp    open  gopher  
79/tcp    open  finger  
110/tcp   open  pop3  
111/tcp   open  rpcbind  
113/tcp   open  ident  
143/tcp   open  imap  
993/tcp   open  imaps  
1022/tcp  open  exp2  
1023/tcp  open  netvenuechat  
8080/tcp  open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds  
kali@vbox:~$
```