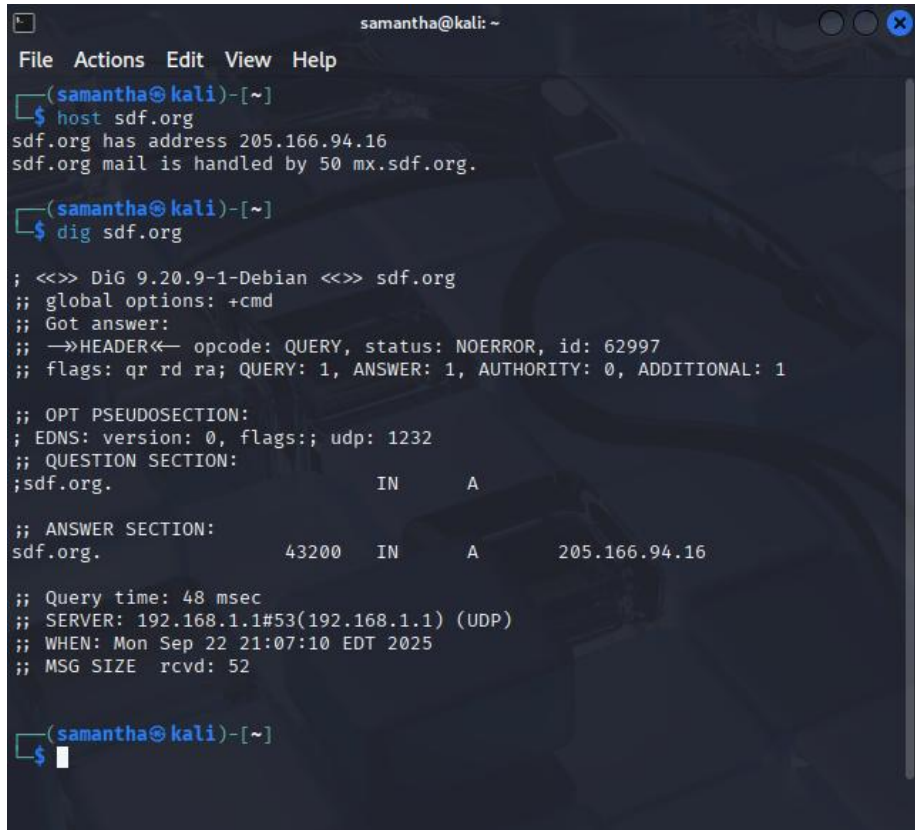


## Lab 3 – Active Reconnaissance and Vulnerability Scanning

### Question 1: Active Scanning

T1:



```
samantha@kali: ~  
File Actions Edit View Help  
(samantha@kali)-[~]  
└─$ host sdf.org  
sdf.org has address 205.166.94.16  
sdf.org mail is handled by 50 mx.sdf.org.  
  
(samantha@kali)-[~]  
└─$ dig sdf.org  
  
; <<>> DiG 9.20.9-1-Debian <<>> sdf.org  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 62997  
;; 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.                43200  IN      A      205.166.94.16  
  
;; Query time: 48 msec  
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)  
;; WHEN: Mon Sep 22 21:07:10 EDT 2025  
;; MSG SIZE rcvd: 52  
  
(samantha@kali)-[~]  
└─$
```

T2:

```
samantha@kali: ~  
File Actions Edit View Help  
  
(samantha@kali)-[~]  
└─$ dnsenum sdf.org  
dnsenum VERSION:1.3.1  
  
─── sdf.org ───  
  
Host's addresses:  
───  
sdf.org. 43200 IN A 205.166.94.1  
6  
  
Name Servers:  
───  
ns-b.sdf.org. 43200 IN A 66.148.112.1  
51  
ns-d.sdf.org. 43200 IN A 172.81.178.4  
0  
ns-a.sdf.org. 43200 IN A 205.166.94.2  
4  
ns-c.sdf.org. 43200 IN A 178.63.35.19  
5  
  
Mail (MX) Servers:  
───  
mx.sdf.org. 43200 IN A 205.166.94.2  
4
```

```
samantha@kali: ~  
File Actions Edit View Help  
  
Mail (MX) Servers:  


---



|             |       |    |   |              |
|-------------|-------|----|---|--------------|
| mx.sdf.org. | 43200 | IN | A | 205.166.94.2 |
|-------------|-------|----|---|--------------|

  
Trying Zone Transfers and getting Bind Versions:  


---



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



Trying Zone Transfer for sdf.org on ns-c.sdf.org ...  
AXFR record query failed: NOTAUTH

  
Brute forcing with /usr/share/dnsenum/dns.txt:  


---



|                 |       |    |   |              |
|-----------------|-------|----|---|--------------|
| agent.sdf.org.  | 43200 | IN | A | 205.166.94.8 |
| asia.sdf.org.   | 43200 | IN | A | 205.166.94.8 |
| backup.sdf.org. | 43200 | IN | A | 205.166.94.8 |
| d.sdf.org.      | 43200 | IN | A | 205.166.94.8 |
| e.sdf.org.      | 43200 | IN | A | 205.166.94.8 |
| es.sdf.org.     | 43200 | IN | A | 205.166.94.8 |


```

T3:

```
(samantha@kali)-[~]  
└─$ nmap -sn --disable-arp-ping -PE -PS -PA --reason sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 21:21 EDT  
Nmap scan report for sdf.org (205.166.94.16)  
Host is up, received syn-ack ttl 255 (0.093s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds  
  
(samantha@kali)-[~]  
└─$ █
```

T4:

```
(samantha@kali)-[~]
└─$ nmap --host-timeout 30m sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 23:29 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.037s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
113/tcp   open  ident
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.76 seconds
```

Question 2: Vulnerability Scanning

T1:

```
(samantha@kali)-[~]
└─$ nmap --script-timeout 30m --script vuln sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 23:30 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.015s latency).
Not shown: 928 filtered tcp ports (no-response), 59 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
79/tcp    open  finger
80/tcp    open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
| /test/: Test page
| /test.php: Test page
| /webmail/: Mail folder
| /robots.txt: Robots file
| /g/: Potentially interesting folder
| /l/: Potentially interesting folder w/ directory listing
| /analog/: Potentially interesting folder
| /cgi-bin/: Potentially interesting folder w/ directory listing
| /class/: Potentially interesting folder
| /icons/: Potentially interesting folder w/ directory listing
| /links/: Potentially interesting folder
| /manage/: Potentially interesting folder
| /map/: Potentially interesting folder
| /news/: Potentially interesting folder
| /proxy/: Potentially interesting folder (401 Unauthorized)
| /pub/: Potentially interesting folder w/ directory listing
| /sites/: Potentially interesting folder w/ directory listing
```

```
samantha@kali: ~  
File Actions Edit View Help  
|_ /webstats/: Potentially interesting folder (401 Unauthorized)  
|_ http-trace: TRACE is enabled  
110/tcp open pop3  
111/tcp open rpcbind  
113/tcp open ident  
143/tcp open imap  
443/tcp open https  
|_ http-dombased-xss: Couldn't find any DOM based XSS.  
| http-enum:  
| /test/: Test page  
| /test.php: Test page  
| /webmail/: Mail folder  
| /robots.txt: Robots file  
|_ /g/: Potentially interesting folder  
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_ http-trace: TRACE is enabled  
| http-csrf:  
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=sdf.org  
| Found the following possible CSRF vulnerabilities:  
|  
| Path: https://sdf.org:443/?join  
| Form id:  
| Form action: https://www.paypal.com/cgi-bin/webscr  
|  
| Path: https://sdf.org:443/?welcome  
| Form id:  
| Form action: https://sdf.org/mkacct.cgi  
993/tcp open imaps  
|_ ssl-ccs-injection: No reply from server (TIMEOUT)  
1022/tcp open exp2  
8080/tcp open http-proxy  
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
```

T2:

```
(samantha@kali)-[~]  
└─$ nmap --script-timeout 10m --script ftp-brute sdf.org  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 00:24 EDT  
Nmap scan report for sdf.org (205.166.94.16)  
Host is up (0.0017s latency).  
Not shown: 944 filtered tcp ports (no-response), 43 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
79/tcp    open  finger  
80/tcp    open  http  
110/tcp   open  pop3  
111/tcp   open  rpcbind  
113/tcp   open  ident  
143/tcp   open  imap  
443/tcp   open  https  
993/tcp   open  imaps  
1022/tcp  open  exp2  
8080/tcp  open  http-proxy  
  
Nmap done: 1 IP address (1 host up) scanned in 661.86 seconds  
  
(samantha@kali)-[~]  
└─$
```