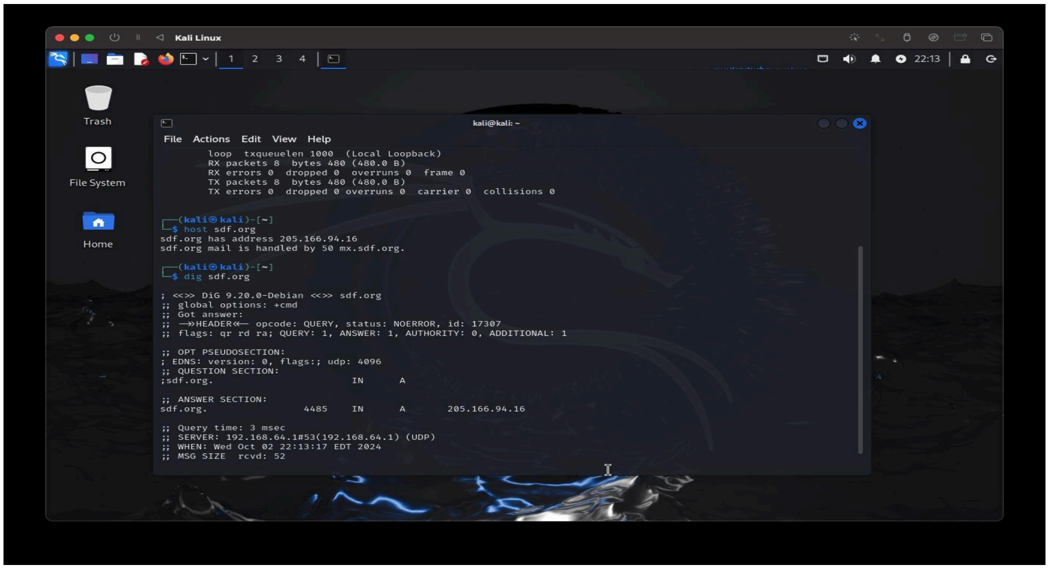
Active Reconnaissance and Vulnerability Scanning

Question 1: Active Scanning

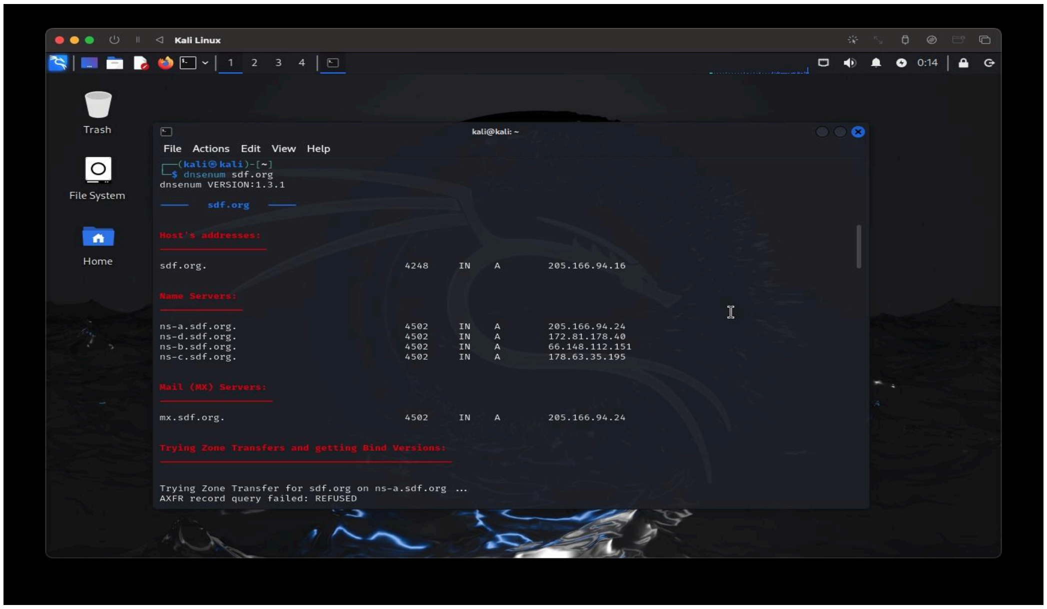
- **T1:**



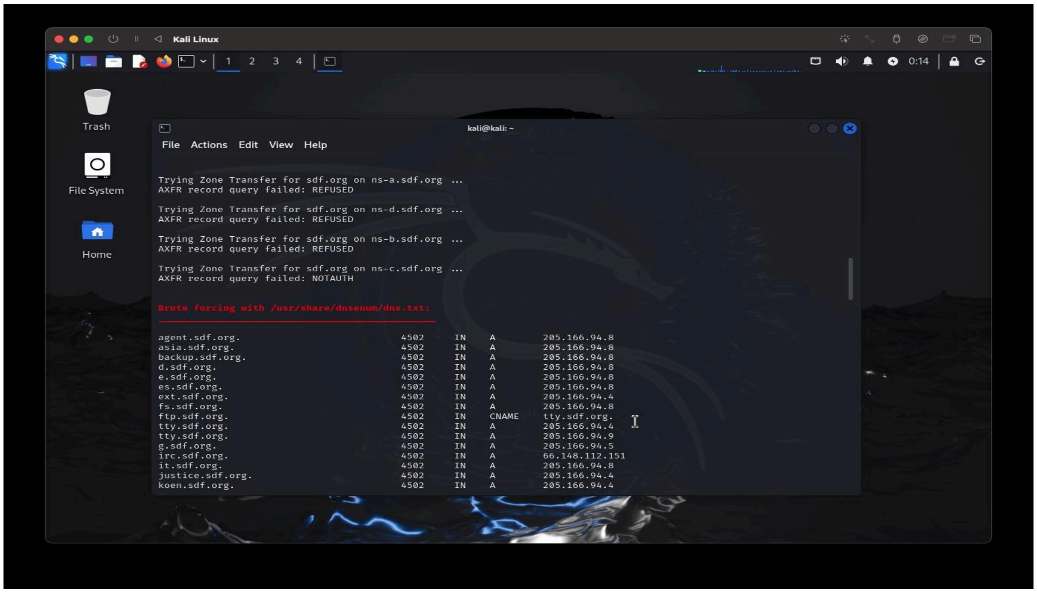
```
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

┌──(kali㉿kali)-[~]
└─$ dig sdf.org

; <<>> DiG 9.20.0-Debian <<>> sdf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17307
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sdf.org.                       IN      A

;; ANSWER SECTION:
sdf.org.                4485    IN      A       205.166.94.16

;; Query time: 3 msec
;; SERVER: 192.168.64.1#53(192.168.64.1) (UDP)
;; WHEN: Wed Oct 02 22:13:17 EDT 2024
;; MSG SIZE  rcvd: 52
```

After executing the host and dig command, the host, sdf.org, is live. The IP address (205.166.94.16) and the query time of 3msec, server (192.168.64.1), date, and time were outputted.

- **T2:**



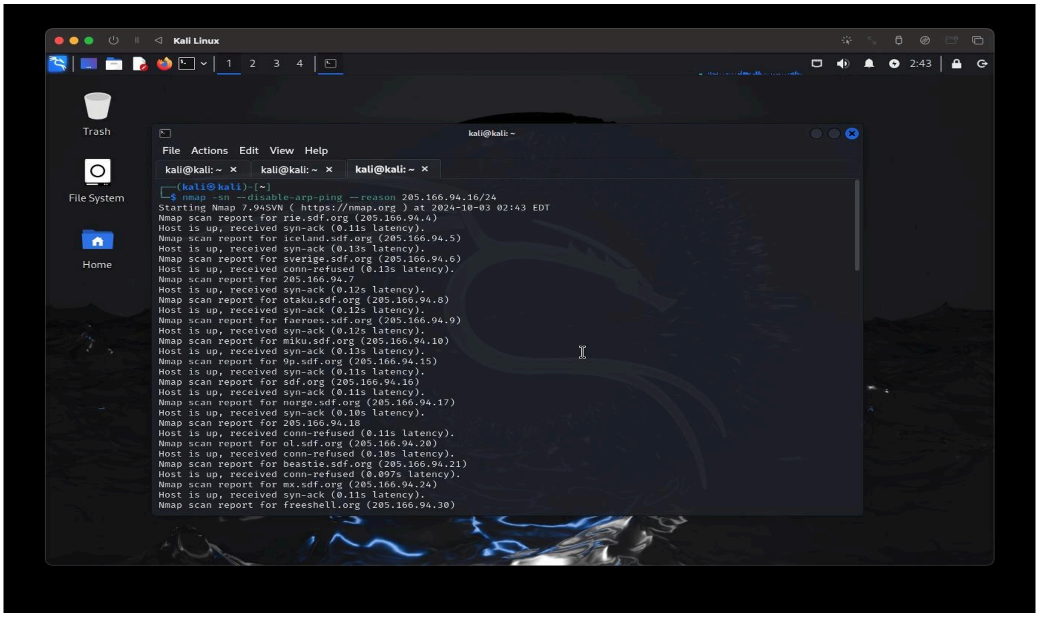
```
┌──(kali㉿kali)-[~]
└─$ dnsenum sdf.org
dnsenum VERSION:1.3.1

─────   sdf.org   ─────


Host's addresses:
__________________

sdf.org.                                 4248     IN    A        205.166.94.16


Name Servers:
______________

ns-a.sdf.org.                            4502     IN    A        205.166.94.24
ns-d.sdf.org.                            4502     IN    A        172.81.178.40
ns-b.sdf.org.                            4502     IN    A        66.148.112.151
ns-c.sdf.org.                            4502     IN    A        178.63.35.195


Mail (MX) Servers:
___________________

mx.sdf.org.                              4502     IN    A        205.166.94.24


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


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



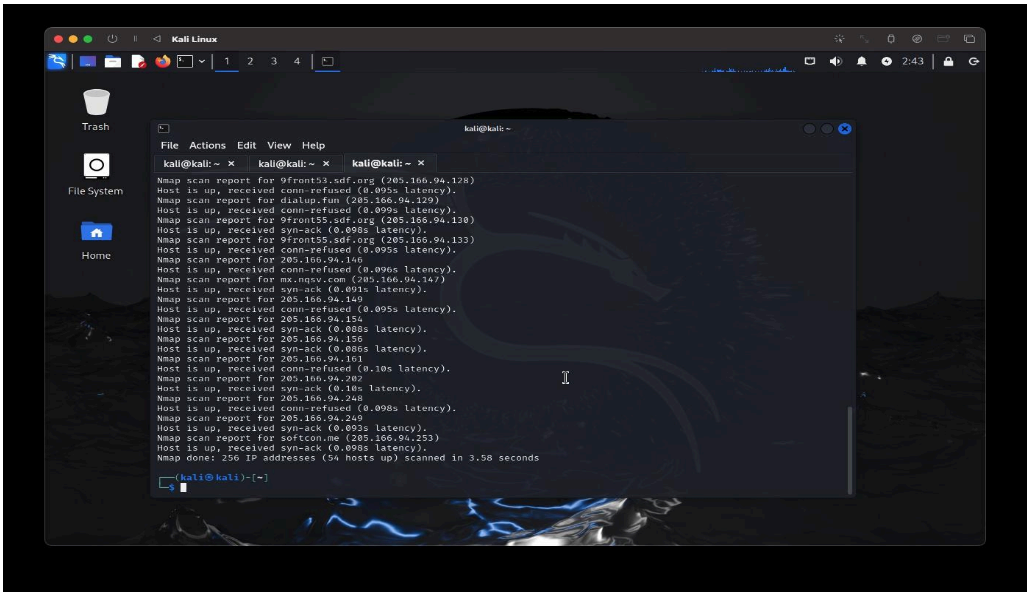
```
Trying Zone Transfer for sdf.org on ns-a.sdf.org ...
AXFR record query failed: REFUSED

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


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

agent.sdf.org.                          4502     IN    A         205.166.94.8
asia.sdf.org.                           4502     IN    A         205.166.94.8
backup.sdf.org.                         4502     IN    A         205.166.94.8
d.sdf.org.                              4502     IN    A         205.166.94.8
e.sdf.org.                              4502     IN    A         205.166.94.8
es.sdf.org.                             4502     IN    A         205.166.94.8
ext.sdf.org.                            4502     IN    A         205.166.94.4
fs.sdf.org.                             4502     IN    A         205.166.94.8
ftp.sdf.org.                            4502     IN    CNAME     tty.sdf.org.
tty.sdf.org.                            4502     IN    A         205.166.94.4
tty.sdf.org.                            4502     IN    A         205.166.94.9
g.sdf.org.                              4502     IN    A         205.166.94.5
irc.sdf.org.                            4502     IN    A         66.148.112.151
it.sdf.org.                             4502     IN    A         205.166.94.8
justice.sdf.org.                        4502     IN    A         205.166.94.4
koen.sdf.org.                           4502     IN    A         205.166.94.4
```

After executing the dnsenum command, Linux outputted sdf.org servers and IPs. However, zone transfer failed, with queries being refused or not authorized.

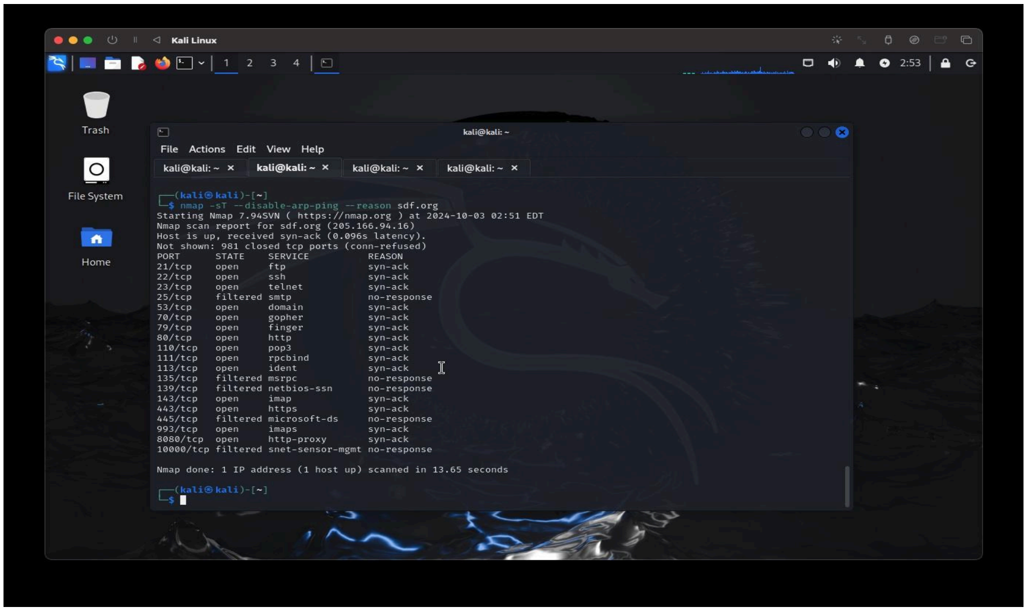
- **T3:**



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn --disable-arp-ping --reason 205.166.94.16/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 02:43 EDT
Nmap scan report for rie.sdf.org (205.166.94.4)
Host is up, received syn-ack (0.11s latency).
Nmap scan report for iceland.sdf.org (205.166.94.5)
Host is up, received syn-ack (0.13s latency).
Nmap scan report for sverige.sdf.org (205.166.94.6)
Host is up, received conn-refused (0.13s latency).
Nmap scan report for 205.166.94.7
Host is up, received syn-ack (0.12s latency).
Nmap scan report for otaku.sdf.org (205.166.94.8)
Host is up, received syn-ack (0.12s latency).
Nmap scan report for faeroes.sdf.org (205.166.94.9)
Host is up, received syn-ack (0.12s latency).
Nmap scan report for miku.sdf.org (205.166.94.10)
Host is up, received syn-ack (0.13s latency).
Nmap scan report for 9p.sdf.org (205.166.94.15)
Host is up, received syn-ack (0.11s latency).
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received syn-ack (0.11s latency).
Nmap scan report for norge.sdf.org (205.166.94.17)
Host is up, received syn-ack (0.10s latency).
Nmap scan report for 205.166.94.18
Host is up, received conn-refused (0.11s latency).
Nmap scan report for ol.sdf.org (205.166.94.20)
Host is up, received conn-refused (0.10s latency).
Nmap scan report for beastie.sdf.org (205.166.94.21)
Host is up, received conn-refused (0.097s latency).
Nmap scan report for mx.sdf.org (205.166.94.24)
Host is up, received syn-ack (0.11s latency).
Nmap scan report for freeshell.org (205.166.94.30)
```



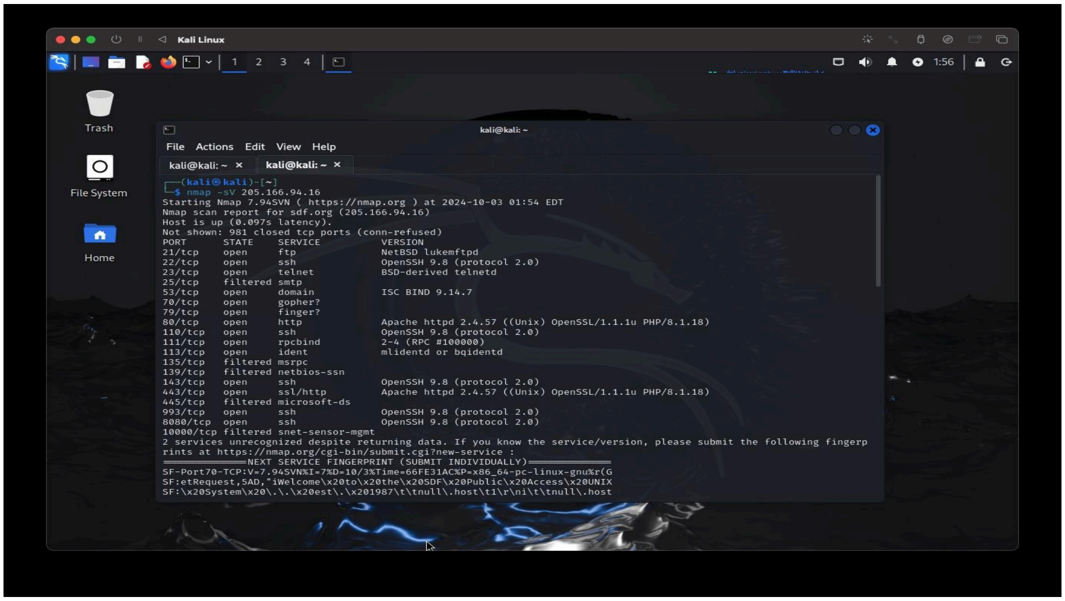
```
Nmap scan report for 9front53.sdf.org (205.166.94.128)
Host is up, received conn-refused (0.095s latency).
Nmap scan report for dialup.fun (205.166.94.129)
Host is up, received conn-refused (0.099s latency).
Nmap scan report for 9front55.sdf.org (205.166.94.130)
Host is up, received syn-ack (0.098s latency).
Nmap scan report for 9front55.sdf.org (205.166.94.133)
Host is up, received conn-refused (0.095s latency).
Nmap scan report for 205.166.94.146
Host is up, received conn-refused (0.096s latency).
Nmap scan report for mx.nqsv.com (205.166.94.147)
Host is up, received syn-ack (0.091s latency).
Nmap scan report for 205.166.94.149
Host is up, received conn-refused (0.095s latency).
Nmap scan report for 205.166.94.154
Host is up, received syn-ack (0.088s latency).
Nmap scan report for 205.166.94.156
Host is up, received syn-ack (0.086s latency).
Nmap scan report for 205.166.94.161
Host is up, received conn-refused (0.10s latency).
Nmap scan report for 205.166.94.202
Host is up, received syn-ack (0.10s latency).
Nmap scan report for 205.166.94.248
Host is up, received conn-refused (0.098s latency).
Nmap scan report for 205.166.94.249
Host is up, received syn-ack (0.093s latency).
Nmap scan report for softcon.me (205.166.94.253)
Host is up, received syn-ack (0.098s latency).
Nmap done: 256 IP addresses (54 hosts up) scanned in 3.58 seconds

┌──(kali㉿kali)-[~]
└─$ 
```



```
┌──(kali㉿kali)-[~]
└─$ nmap -sT --disable-arp-ping --reason sdf.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 02:51 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received syn-ack (0.096s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE    SERVICE          REASON
21/tcp    open     ftp              syn-ack
22/tcp    open     ssh              syn-ack
23/tcp    open     telnet           syn-ack
25/tcp    filtered smtp             no-response
53/tcp    open     domain           syn-ack
70/tcp    open     gopher           syn-ack
79/tcp    open     finger           syn-ack
80/tcp    open     http             syn-ack
110/tcp   open     pop3             syn-ack
111/tcp   open     rpcbind          syn-ack
113/tcp   open     ident            syn-ack
135/tcp   filtered msrpc            no-response
139/tcp   filtered netbios-ssn      no-response
143/tcp   open     imap             syn-ack
443/tcp   open     https            syn-ack
445/tcp   filtered microsoft-ds     no-response
993/tcp   open     imaps            syn-ack
8080/tcp  open     http-proxy       syn-ack
10000/tcp filtered snet-sensor-mgmt no-response

Nmap done: 1 IP address (1 host up) scanned in 13.65 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

After performing the ICMP with arp ping disabled, it found 256 IP addresses with 54 hosts up. After performing the TCP sweep with arp ping disables, it found all the open TCP ports.

- **T4:**

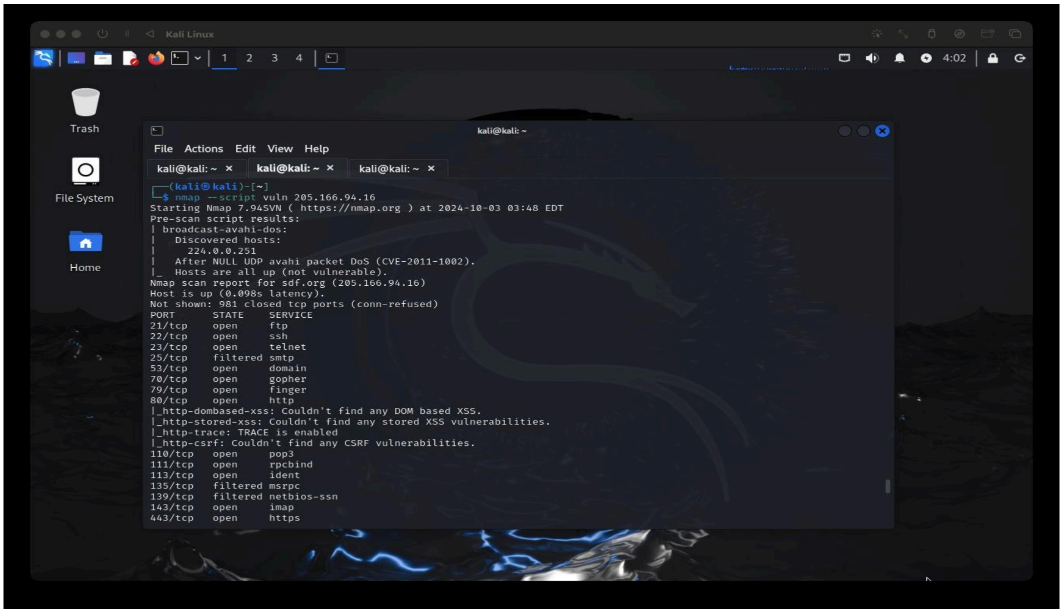


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 01:54 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.097s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE    SERVICE          VERSION
21/tcp    open     ftp              NetBSD lukemftpd
22/tcp    open     ssh              OpenSSH 9.8 (protocol 2.0)
23/tcp    open     telnet           BSD-derived telnetd
25/tcp    filtered smtp
53/tcp    open     domain           ISC BIND 9.14.7
70/tcp    open     gopher?
79/tcp    open     finger?
80/tcp    open     http             Apache httpd 2.4.57 ((Unix) OpenSSL/1.1.1u PHP/8.1.18)
110/tcp   open     ssh              OpenSSH 9.8 (protocol 2.0)
111/tcp   open     rpcbind          2-4 (RPC #100000)
113/tcp   open     ident            mlidentd or bqidentd
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     ssh              OpenSSH 9.8 (protocol 2.0)
443/tcp   open     ssl/http         Apache httpd 2.4.57 ((Unix) OpenSSL/1.1.1u PHP/8.1.18)
445/tcp   filtered microsoft-ds
993/tcp   open     ssh              OpenSSH 9.8 (protocol 2.0)
8080/tcp  open     ssh              OpenSSH 9.8 (protocol 2.0)
10000/tcp filtered snet-sensor-mgmt
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port70-TCP:V=7.94SVN%I=7%D=10/3%Time=66FE31AC%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,5AD,"iWelcome\x20to\x20the\x20SDF\x20Public\x20Access\x20UNIX
SF:\x20System\x20\.\.\x20est\.\x201987\t\tnull\.host\t1\r\ni\t\tnull\.host
```

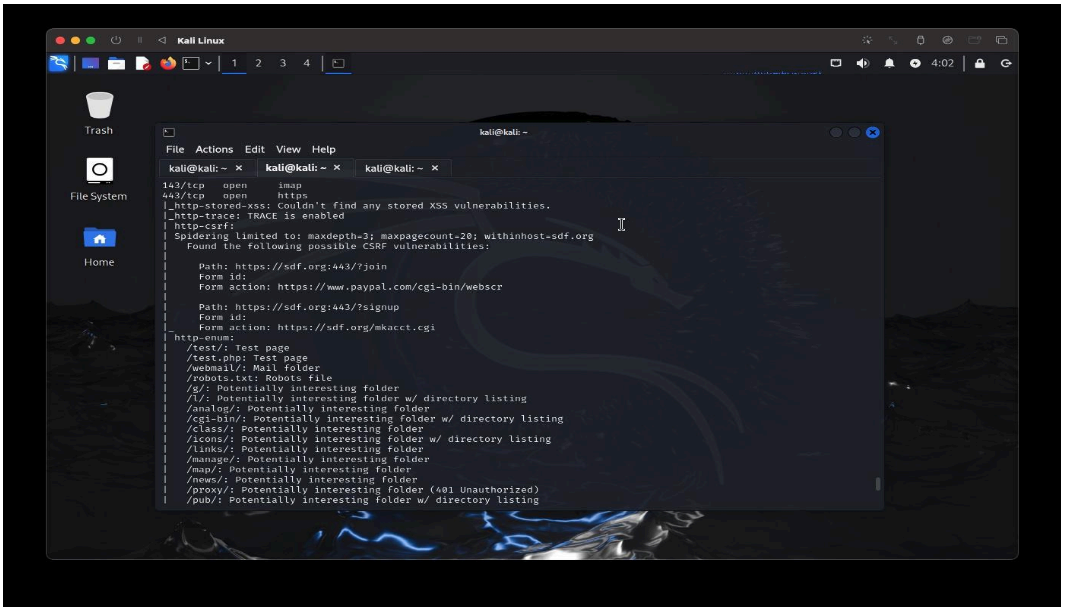
After executing the nmap -sV command for the host, I found the open ports and their services.

Question 2: Vulnerability Scanning

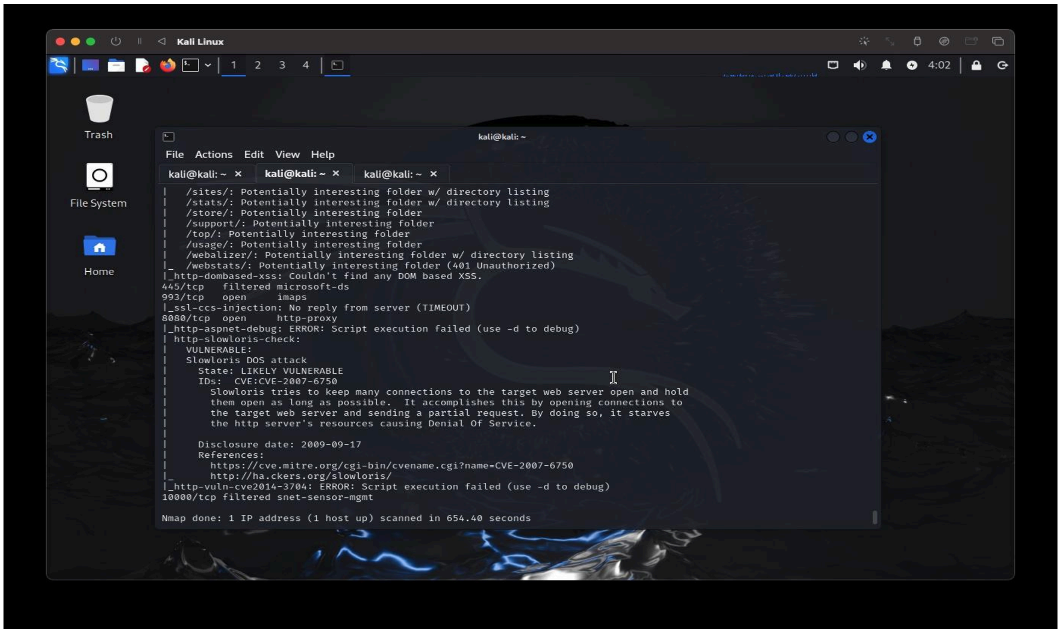
- **T1:**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 03:48 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.098s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    filtered smtp
53/tcp    open     domain
70/tcp    open     gopher
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-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
110/tcp   open     pop3
111/tcp   open     rpcbind
113/tcp   open     ident
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
```

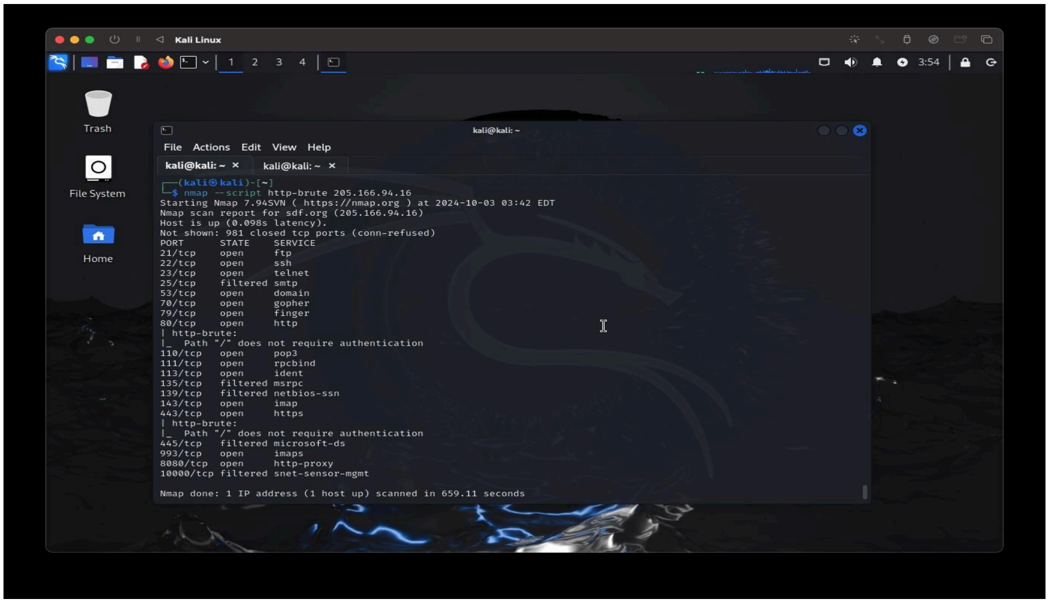


```
143/tcp   open     imap
443/tcp   open     https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=sdf.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://sdf.org:443/?join
|     Form id:
|     Form action: https://www.paypal.com/cgi-bin/webscr
|
|     Path: https://sdf.org:443/?signup
|     Form id:
|_    Form action: https://sdf.org/mkacct.cgi
| 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
|   /stats/: Potentially interesting folder w/ directory listing
|   /store/: Potentially interesting folder
|   /support/: Potentially interesting folder
|   /top/: Potentially interesting folder
|   /usage/: Potentially interesting folder
|   /webalizer/: Potentially interesting folder w/ directory listing
|_  /webstats/: Potentially interesting folder (401 Unauthorized)
|_http-dombased-xss: Couldn't find any DOM based XSS.
445/tcp   filtered microsoft-ds
993/tcp   open     imaps
|_ssl-ccs-injection: No reply from server (TIMEOUT)
8080/tcp  open     http-proxy
|_http-aspnet-debug: 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:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
10000/tcp filtered snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 654.40 seconds
```

- **T2:**



```
┌──(kali㉿kali)-[~]
└─$ nmap --script http-brute 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-03 03:42 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.098s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    filtered smtp
53/tcp    open     domain
70/tcp    open     gopher
79/tcp    open     finger
80/tcp    open     http
| http-brute:
|_  Path "/" does not require authentication
110/tcp   open     pop3
111/tcp   open     rpcbind
113/tcp   open     ident
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
| http-brute:
|_  Path "/" does not require authentication
445/tcp   filtered microsoft-ds
993/tcp   open     imaps
8080/tcp  open     http-proxy
10000/tcp filtered snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 659.11 seconds
```