INSTRUCTIONS:

Question 1: Active Scanning

• **Task1**: Using both host and dig commands, demonstrate whether the host sdf.org is live or not. Attach screenshots showing the results. 4 points

• **Task2**: Perform DNS enumeration using dnsenum command for the host sdf.org. Check whether the zone transfer is possible. Provide necessary screenshots. 4 points

• **Task3**: 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

• **Task4** Perform port scanning to determine all open ports and corresponding running services for the host sdf.org. Attach screenshots showing the results. 6 points

Question 2: Vulnerability Scanning

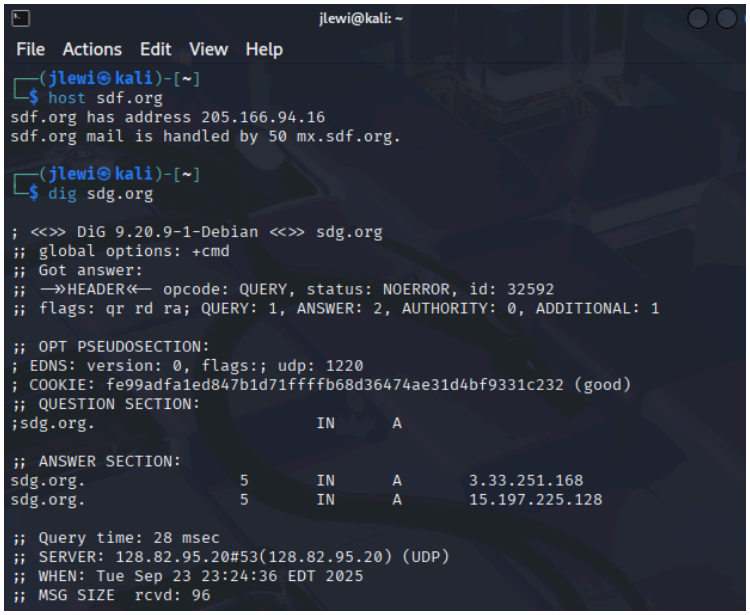
• **Task1**: Using NSE scripts, determine all known vulnerabilities present in the host sdf.org. Attach a screenshot showing your command and the results you got. 5 points

•**Task2** 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

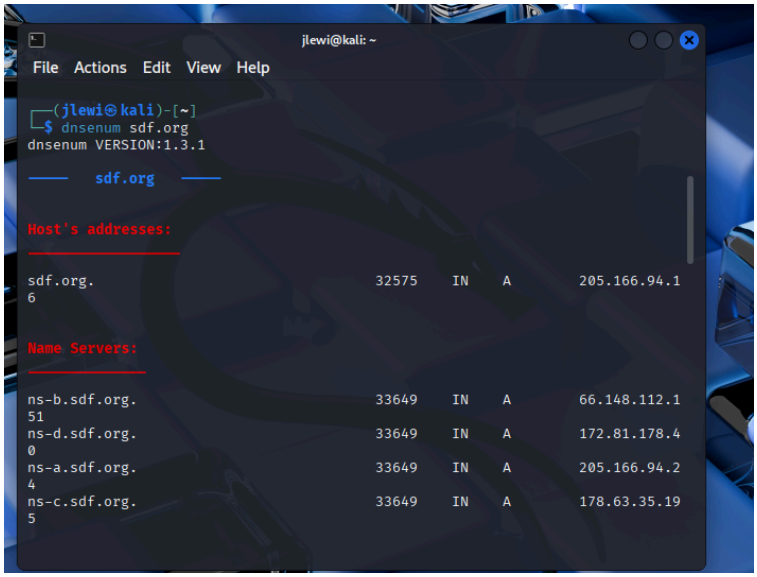
WORK

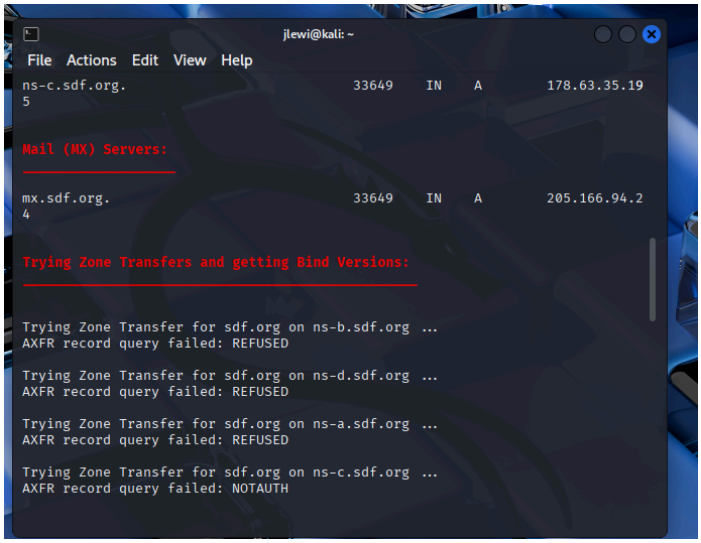
Question 1

T1:



T2:


jlewi@kali: ~
File Actions Edit View Help
(jlewi㉿kali)-[~]
$ dnsenum sdf.org
dnsenum VERSION:1.3.1
sdf.org
Host's addresses:
sdf.org. 32575 IN A 205.166.94.1
6
Name Servers:
ns-b.sdf.org. 33649 IN A 66.148.112.1
51
ns-d.sdf.org. 33649 IN A 172.81.178.4
0
ns-a.sdf.org. 33649 IN A 205.166.94.2
4
ns-c.sdf.org. 33649 IN A 178.63.35.19
5


jlewi@kali: ~
File Actions Edit View Help
ns-c.sdf.org. 33649 IN A 178.63.35.19
5
Mail (MX) Servers:
mx.sdf.org. 33649 IN A 205.166.94.2
4
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

T3:

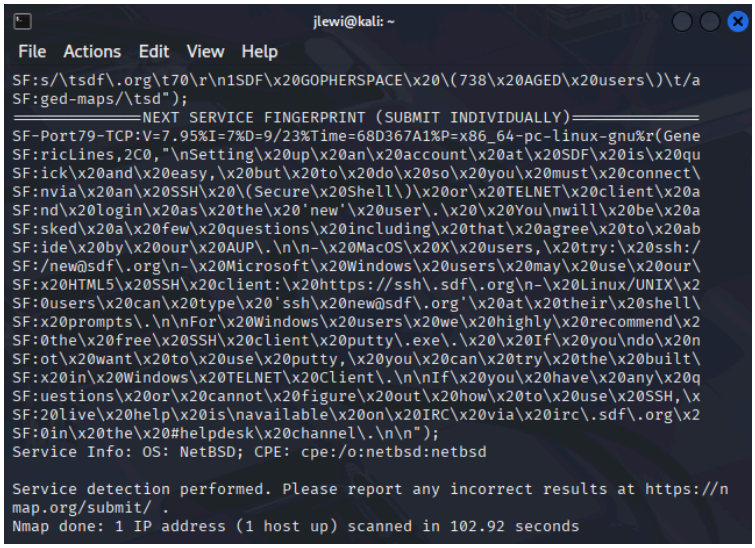
```
┌──(jlewi㉿kali)-[~]
└─$ nmap -sn sdf.org --reason --disable-arp-ping
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 23:35 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.00064s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

```
┌──(jlewi㉿kali)-[~]
└─$ nmap -sS sdf.org --reason --disable-arp-ping
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 23:35 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.056s 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 7.10 seconds
```

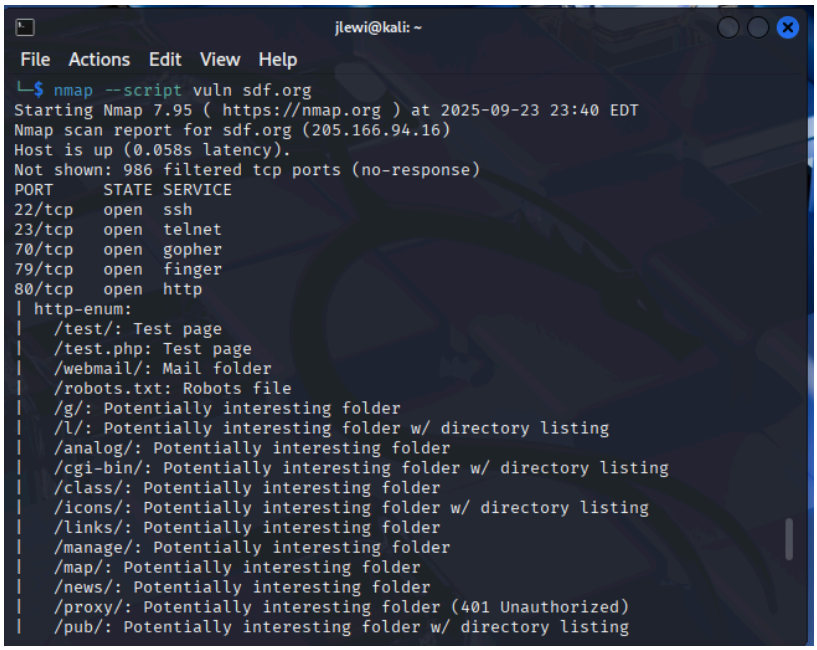
T4:

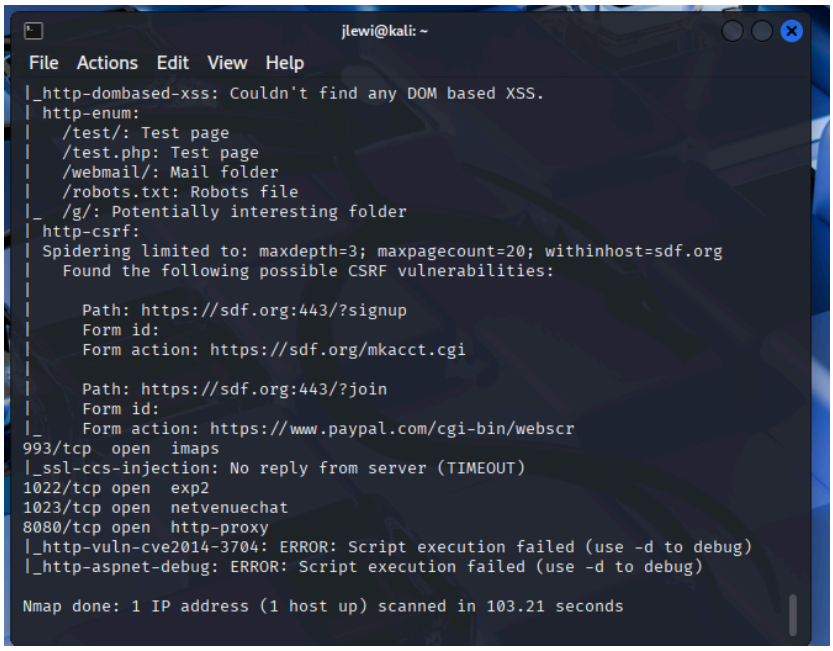
```
┌──(jlewi㉿kali)-[~]
└─$ nmap -sV sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-23 23:37 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.044s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      NetBSD lukemftpd
22/tcp   open  ssh      OpenSSH 10.0 (protocol 2.0)
23/tcp   open  telnet   BSD-derived telnetd
70/tcp   open  gopher?
79/tcp   open  finger?
80/tcp   open  http     Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
110/tcp  open  ssh      OpenSSH 10.0 (protocol 2.0)
111/tcp  open  rpcbind  2-4 (RPC #100000)
113/tcp  open  ident    mlidentd or bqidentd
143/tcp  open  ssh      OpenSSH 10.0 (protocol 2.0)
443/tcp  open  ssl/http Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
993/tcp  open  ssh      OpenSSH 10.0 (protocol 2.0)
1022/tcp open  nlockmgr 0-4 (RPC #100021)
1023/tcp open  ypbind   2 (RPC #100007)
8080/tcp open  ssh      OpenSSH 10.0 (protocol 2.0)
2 services unrecognized despite returning data. If you know the service/versi
on, please submit the following fingerprints at https://nmap.org/cgi-bin/subm
it.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
```



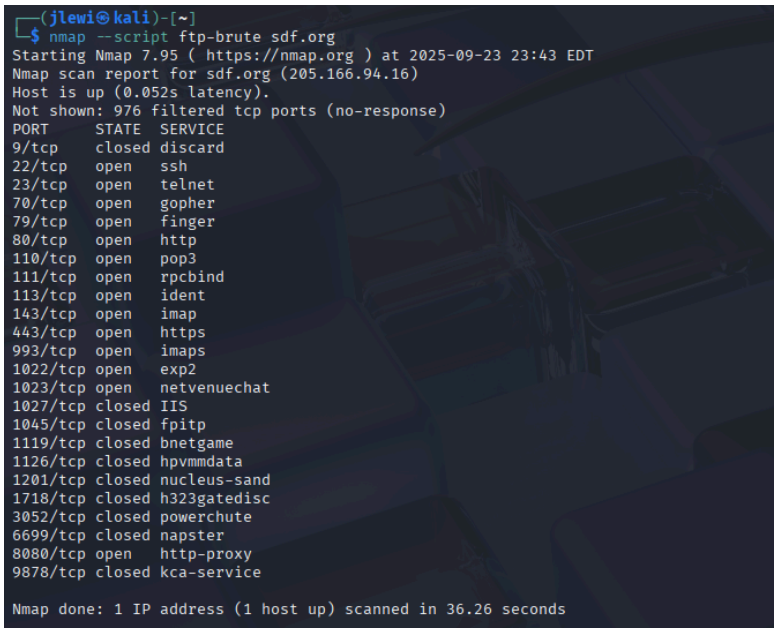
Question 2

Task 1:




jlewi@kali: ~
File Actions Edit View Help
|_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-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=sdf.org
| Found the following possible CSRF vulnerabilities:
|
| Path: https://sdf.org:443/?signup
| Form id:
| Form action: https://sdf.org/mkacct.cgi
|
| Path: https://sdf.org:443/?join
| Form id:
|_   Form action: https://www.paypal.com/cgi-bin/webscr
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-aspnet-debug: ERROR: Script execution failed (use -d to debug)
Nmap done: 1 IP address (1 host up) scanned in 103.21 seconds

T2:


┌──(jlewi㉿kali)-[~]
└─$ nmap --script ftp-brute sdf.org
Starting Nmap 7.95 (https://nmap.org) at 2025-09-23 23:43 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.052s latency).
Not shown: 976 filtered tcp ports (no-response)
PORT   STATE SERVICE
9/tcp   closed discard
22/tcp   open   ssh
23/tcp   open   telnet
70/tcp   open   gopher
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
1023/tcp open   netvenuechat
1027/tcp closed IIS
1045/tcp closed fpitp
1119/tcp closed bnetgame
1126/tcp closed hpvmmdata
1201/tcp closed nucleus-sand
1718/tcp closed h323gatedisc
3052/tcp closed powerchute
6699/tcp closed napster
8080/tcp open   http-proxy
9878/tcp closed kca-service
Nmap done: 1 IP address (1 host up) scanned in 36.26 seconds