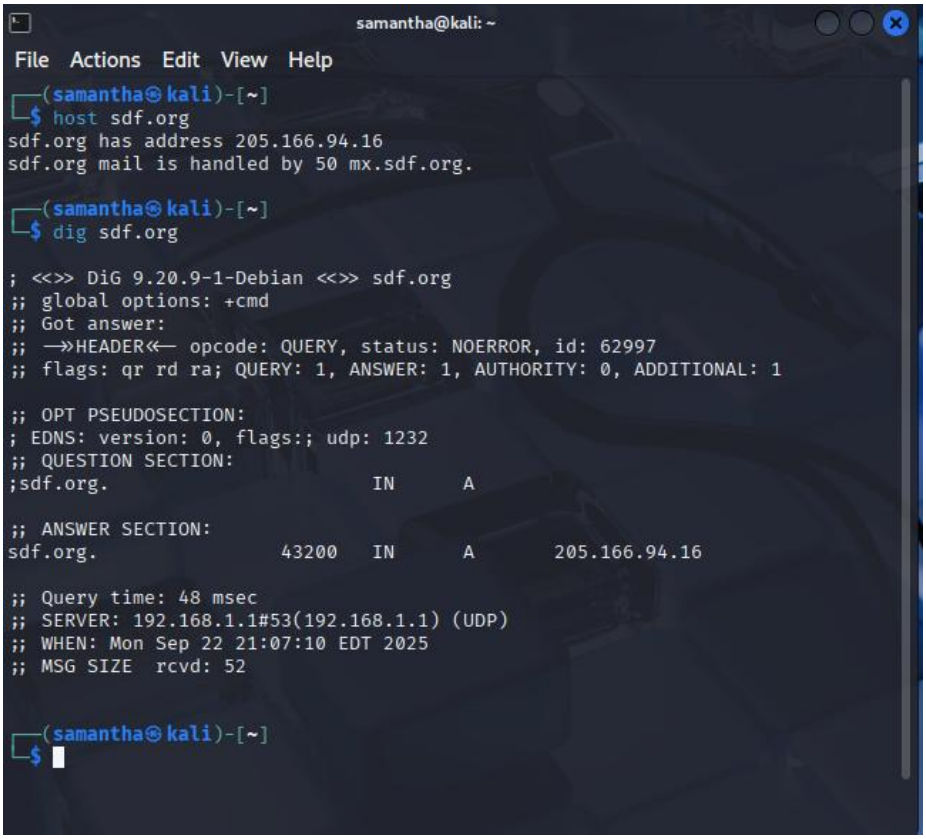
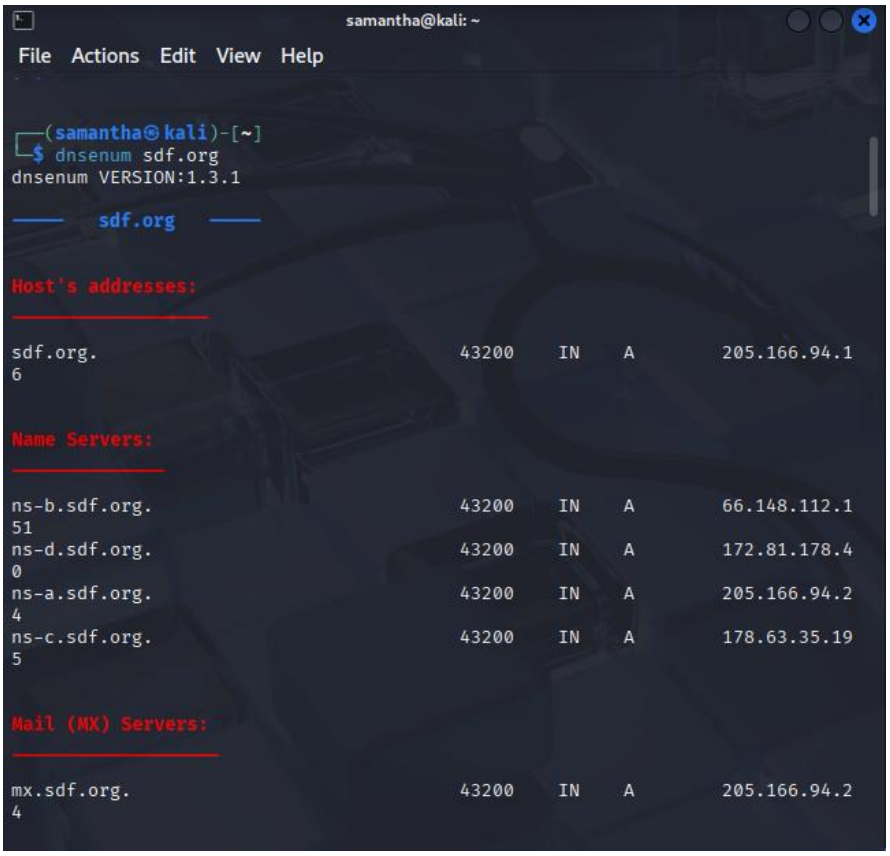
Lab 3 – Active Reconnaissance and Vulnerability Scanning

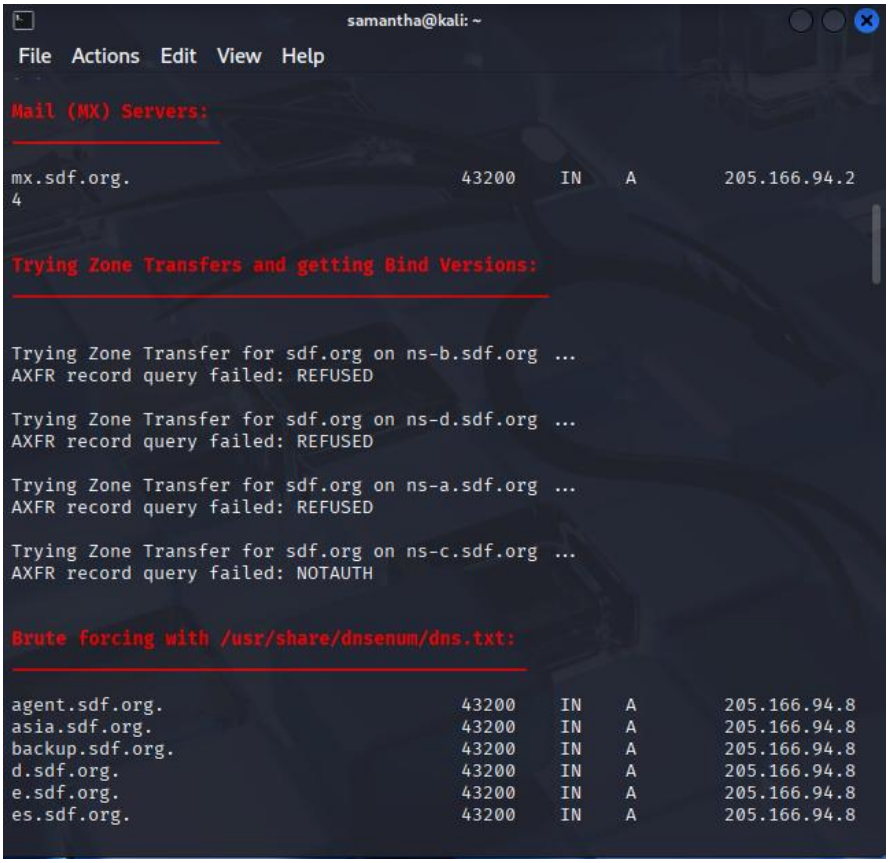
Question 1: Active Scanning

T1:

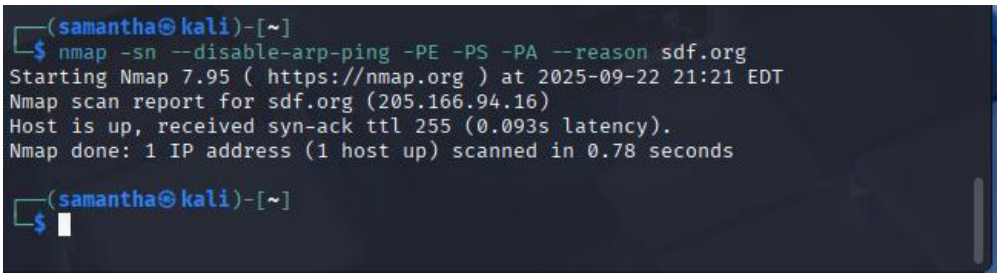


T2:

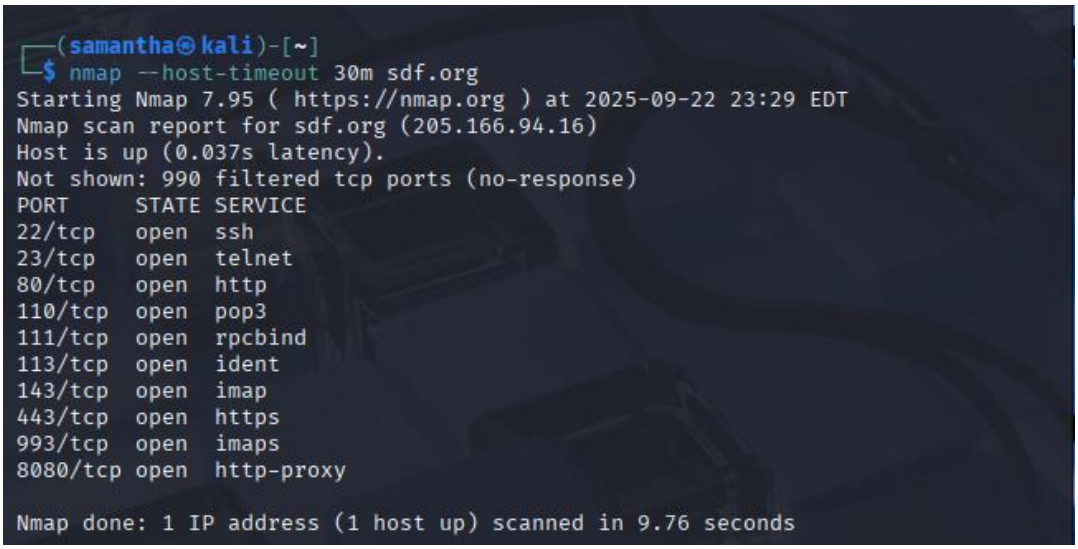

samantha@kali: ~
File Actions Edit View Help
(samantha㉿kali)-[~]
$ dnsenum sdf.org
dnsenum VERSION:1.3.1
sdf.org
Host's addresses:
sdf.org. 43200 IN A 205.166.94.16
Name Servers:
ns-b.sdf.org. 43200 IN A 66.148.112.151
ns-d.sdf.org. 43200 IN A 172.81.178.40
ns-a.sdf.org. 43200 IN A 205.166.94.24
ns-c.sdf.org. 43200 IN A 178.63.35.195
Mail (MX) Servers:
mx.sdf.org. 43200 IN A 205.166.94.24


samantha@kali: ~
File Actions Edit View Help
Mail (MX) Servers:
mx.sdf.org. 43200 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
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:

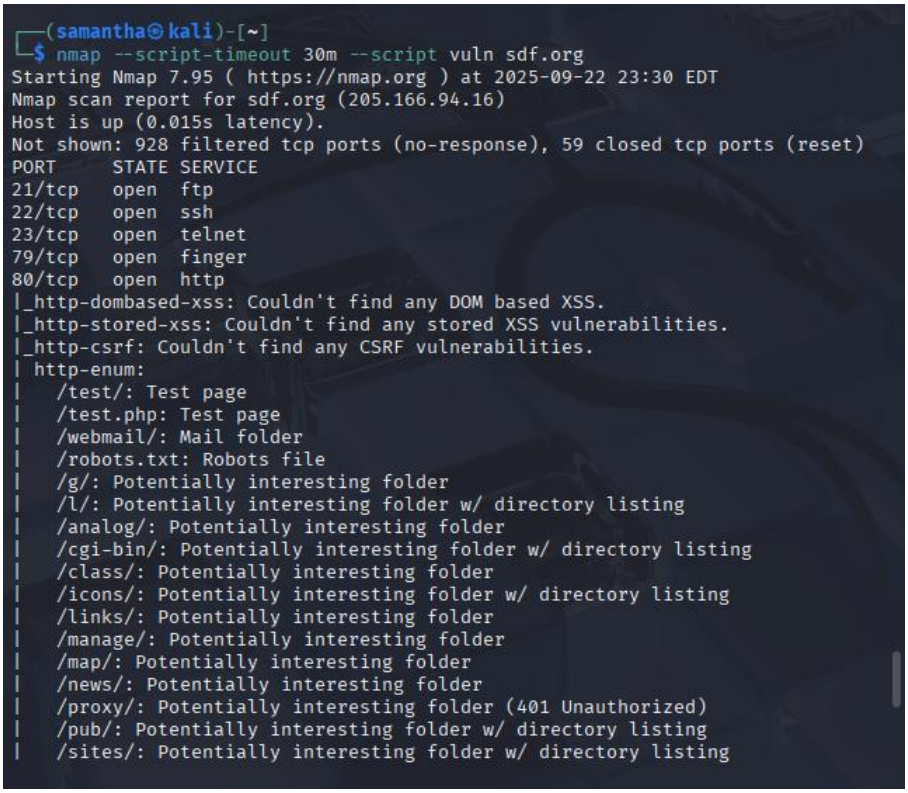

(samantha㉿kali)-[~]
$ nmap -sn --disable-arp-ping -PE -PS -PA --reason sdf.org
Starting Nmap 7.95 (https://nmap.org) at 2025-09-22 21:21 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received syn-ack ttl 255 (0.093s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.78 seconds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

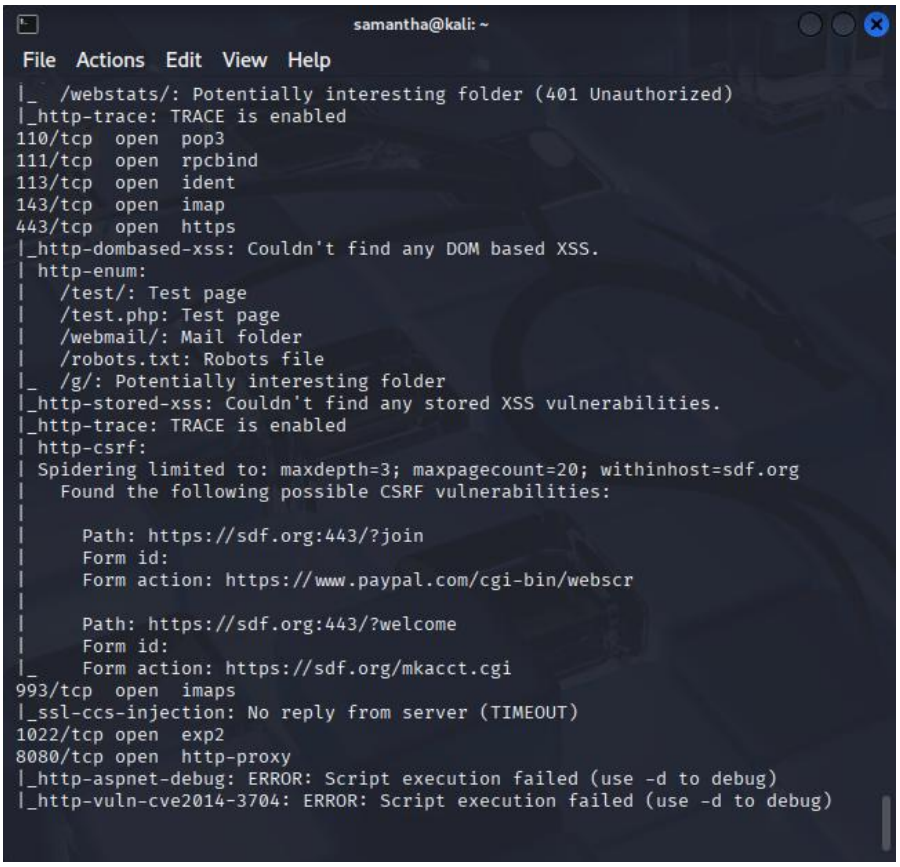
T4:



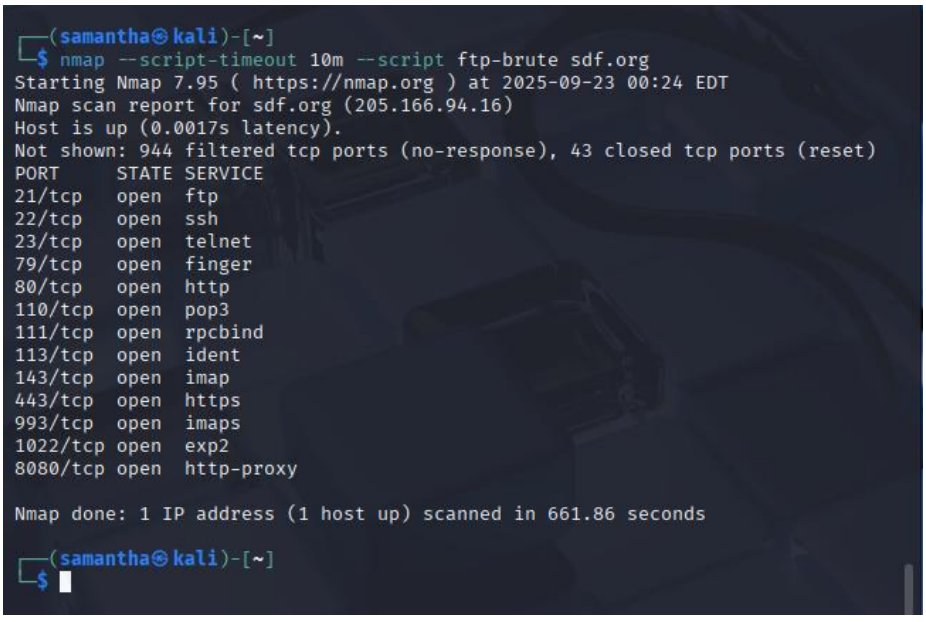
Question 2: Vulnerability Scanning

T1:




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)-[~]
$