Diane Gilzow

February 23, 2026

CYSE 450: Ethical Hacking and Penetration Testing

Dr. Md Morshed Alam

Lab 4: Active Reconnaissance and Vulnerability Scanning

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.

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

Zone transfers are not possible, they were refused.

- **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.

```
┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap -sn -PE --disable-arp-ping --reason sdf.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 13:03 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received echo-reply ttl 255 (0.083s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds

┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap -sn -PS80,443 --disable-arp-ping --reason sdf.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 13:04 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received syn-ack ttl 64 (0.11s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

- **T4:** Perform port scanning to determine all **open ports** and corresponding **running services** for the host sdf.org. Attach screenshots showing the results.

```
┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap -p- -sV 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-20 15:18 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.016s latency).
Not shown: 47450 filtered tcp ports (net-unreach), 18073 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  tcpwrapped
22/tcp   open  tcpwrapped
23/tcp   open  tcpwrapped
79/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
110/tcp  open  tcpwrapped
111/tcp  open  tcpwrapped
113/tcp  open  tcpwrapped
143/tcp  open  tcpwrapped
443/tcp  open  tcpwrapped
993/tcp  open  tcpwrapped
8080/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 86.15 seconds
```

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.

```
└─$ nmap --script vuln 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 16:04 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.062s latency).
Not shown: 985 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
80/tcp   open  http
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_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
|   /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
|   /tmp/: Potentially interesting folder w/ directory listing
|   /top/: Potentially interesting folder
|   /usage/: Potentially interesting folder
|   /webalizer/: Potentially interesting folder w/ directory listing
|_  /webstats/: Potentially interesting folder (401 Unauthorized)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_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-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

```
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-trace: TRACE is enabled
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
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-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 271.24 seconds
```

- **T2:** Perform a brute force attack on sdf.org. You can choose any script from the following: ***ftp-brute, snmp-brute, http-brute,*** *and* ***oracle-brute***. Attach screenshots showing your command and the results you received.

```
┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap --script http-brute 205.166.94.16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 16:13 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.064s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
23/tcp   open   telnet
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
143/tcp  open   imap
443/tcp  open   https
| http-brute:
|_  Path "/" does not require authentication
993/tcp  open   imaps
1022/tcp open   exp2
1023/tcp open   netvenuechat
1723/tcp closed pptp
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp open   http-proxy

Nmap done: 1 IP address (1 host up) scanned in 11.65 seconds
```

```
┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap -sV --script ftp-brute sdf.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 14:41 EST
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] usernames: Time limit 10m00s exceeded.
NSE: [ftp-brute] passwords: Time limit 10m00s exceeded.
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.058s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      NetBSD lukemftpd
| ftp-brute:
|   Accounts: No valid accounts found
|_  Statistics: Performed 5893 guesses in 612 seconds, average tps: 9.7
22/tcp   open  ssh      OpenSSH 10.2 (protocol 2.0)
23/tcp   open  telnet   BSD-derived telnetd
70/tcp   open  gopher?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     iWelcome to the SDF Public Access UNIX System .. est. 1987 null.host 1
|     null.host 1
|     iOfficial Site of the Internet Gopher Club Underground Syndicate null.host 1
|     null.host 1
|     offer FREE and inexpensive memberships for people interested null.host 1
|     UNIX system and internetworking. Personal GOPHERSPACE null.host 1
|     available to all users as well as hundreds of UNIX utilities, null.host 1
|     igames and networking utilities. We are a federally recognized null.host 1
|     inon-profit 501(c)7 organization and we are supported entirely null.host 1
|     donations and membership dues. ssh://sdf.org null.host 1
|     null.host 1
|     visit the SDF gemini server, type 'go gem.sdf.org' null.host 1
|     null.host 1
|     1SDF PHLOGOSPHERE (427 phlogs) /phlogs/ gopher.club 70
|     1SDF GOPHERSPACE (1420 ACTIVE users) /maps/ sdf.org 70
|_    1SDF GOPHERSPACE (847 AGED users) /aged-maps/ sd
79/tcp   open  finger?
| fingerprint-strings:
|   GenericLines:
|     Setting up an account at SDF is quick and easy, but to do so you must connect
|     (Secure Shell) or TELNET client and login as the 'new' user. You
|     will be asked a few questions including that agree to abide by our AUP.
|     MacOS X users, try: ssh://new@sdf.org
|     Microsoft Windows users may use our HTML5 SSH client: https://ssh.sdf.org
|     Linux/UNIX users can type 'ssh new@sdf.org' at their shell prompts.
|     Windows users we highly recommend the free SSH client putty.exe. If you
|     want to use putty, you can try the built in Windows TELNET Client.
|     have any questions or cannot figure out how to use SSH, live help is
|_    available on IRC via irc.sdf.org in the #helpdesk channel.
80/tcp   open  http     Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
|_http-server-header: Apache/2.4.65 (Unix) OpenSSL/3.4.1 PHP/8.3.25
110/tcp  open  ssh      OpenSSH 10.2 (protocol 2.0)
```

```
┌──(tobythebaby㉿dgilz001)-[~]
└─$ nmap -sV --script snmp-brute sdf.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-02-23 15:00 EST
Nmap scan report for sdf.org (205.166.94.16)
Host is up (0.062s latency).
Not shown: 986 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 10.2 (protocol 2.0)
23/tcp   open  telnet   BSD-derived telnetd
70/tcp   open  gopher?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     iWelcome to the SDF Public Access UNIX System .. est. 1987 null.host 1
|     null.host 1
|     iOfficial Site of the Internet Gopher Club Underground Syndicate null.host 1
|     null.host 1
|     offer FREE and inexpensive memberships for people interested null.host 1
|     UNIX system and internetworking. Personal GOPHERSPACE null.host 1
|     available to all users as well as hundreds of UNIX utilities, null.host 1
|     igames and networking utilities. We are a federally recognized null.host 1
|     inon-profit 501(c)7 organization and we are supported entirely null.host 1
|     donations and membership dues. ssh://sdf.org null.host 1
|     null.host 1
|     visit the SDF gemini server, type 'go gem.sdf.org' null.host 1
|     null.host 1
|     1SDF PHLOGOSPHERE (427 phlogs) /phlogs/ gopher.club 70
|     1SDF GOPHERSPACE (1420 ACTIVE users) /maps/ sdf.org 70
|_    1SDF GOPHERSPACE (847 AGED users) /aged-maps/ sd
79/tcp   open  finger?
| fingerprint-strings:
|   GenericLines:
|     Setting up an account at SDF is quick and easy, but to do so you must connect
|     (Secure Shell) or TELNET client and login as the 'new' user. You
|     will be asked a few questions including that agree to abide by our AUP.
|     MacOS X users, try: ssh://new@sdf.org
|     Microsoft Windows users may use our HTML5 SSH client: https://ssh.sdf.org
|     Linux/UNIX users can type 'ssh new@sdf.org' at their shell prompts.
|     Windows users we highly recommend the free SSH client putty.exe. If you
|     want to use putty, you can try the built in Windows TELNET Client.
|     have any questions or cannot figure out how to use SSH, live help is
|_    available on IRC via irc.sdf.org in the #helpdesk channel.
80/tcp   open  http     Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
|_http-server-header: Apache/2.4.65 (Unix) OpenSSL/3.4.1 PHP/8.3.25
110/tcp  open  ssh      OpenSSH 10.2 (protocol 2.0)
111/tcp  open  rpcbind
113/tcp  open  ident    mlidentd or bqidentd
143/tcp  open  ssh      OpenSSH 10.2 (protocol 2.0)
443/tcp  open  ssl/http Apache httpd 2.4.65 ((Unix) OpenSSL/3.4.1 PHP/8.3.25)
|_http-server-header: Apache/2.4.65 (Unix) OpenSSL/3.4.1 PHP/8.3.25
993/tcp  open  ssh      OpenSSH 10.2 (protocol 2.0)
1022/tcp open  nlockmgr 0-4 (RPC #100021)
```