Old Dominion University

CYSE 450: Ethical Hacking and Penetration Testing

Lab 1: 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. **4 points**

```
┌──(zufan93㉿Kali)-[~]
└─$ host sdf.org
sdf.org has address 205.166.94.16
sdf.org mail is handled by 50 mx.sdf.org.

┌──(zufan93㉿Kali)-[~]
└─$ dig sdf.org

; <<>> DiG 9.20.7-1-Debian <<>> sdf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16053
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;sdf.org.                       IN      A

;; ANSWER SECTION:
sdf.org.                43200   IN      A       205.166.94.16

;; Query time: 91 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Apr 07 22:40:15 EDT 2025
;; MSG SIZE  rcvd: 52
```

- **T2**: Perform **DNS enumeration** using ***dnsenum*** command for the host sdf.org. Check whether the **zone transfer** is possible. Provide necessary screenshots. **4 points**

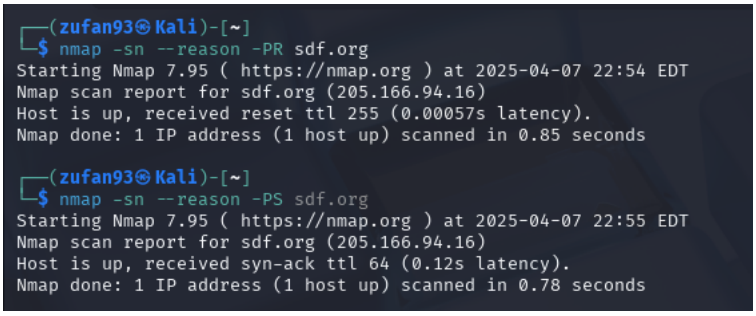
```
┌──(zufan93㉿Kali)-[~]
└─$ dnsenum sdf.org
dnsenum VERSION:1.3.1

-----   sdf.org   -----


Host's addresses:
__________________

sdf.org.                                42757   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
```

```
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
```

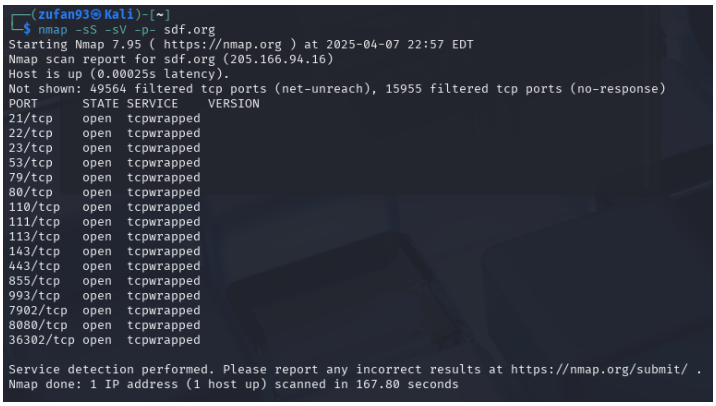
```
sdf.org class C netranges:
__________________________

 66.148.112.0/24
 172.81.178.0/24
 178.63.35.0/24
 205.166.94.0/24
 209.160.32.0/24


Performing reverse lookup on 1280 ip addresses:
_______________________________________________

1.94.166.205.in-addr.arpa.              172800  IN    PTR      gw.sdf.org.
4.94.166.205.in-addr.arpa.              172800  IN    PTR      rie.sdf.org.
5.94.166.205.in-addr.arpa.              172800  IN    PTR      iceland.sdf.org.
6.94.166.205.in-addr.arpa.              172800  IN    PTR      sverige.sdf.org.
8.94.166.205.in-addr.arpa.              172800  IN    PTR      otaku.sdf.org.
9.94.166.205.in-addr.arpa.              172800  IN    PTR      faeroes.sdf.org.
10.94.166.205.in-addr.arpa.             172800  IN    PTR      miku.sdf.org.
12.94.166.205.in-addr.arpa.             172800  IN    PTR      vinland.sdf.org.
```

```
72 results out of 1280 IP addresses.


sdf.org ip blocks:
__________________

205.166.94.1/32
205.166.94.4/31
205.166.94.6/32
205.166.94.8/31
205.166.94.10/32
205.166.94.12/31
205.166.94.15/32
```

- **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. **6 points**

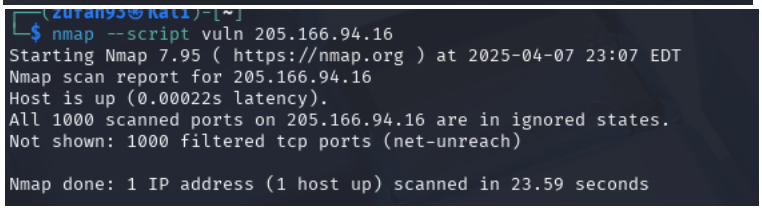


- **T4**: Perform port scanning to determine all **open ports** and corresponding **running services** for the host sdf.org. Attach screenshots showing the results. **6 points**



Question 2: **Vulnerability Scanning**

- **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. **5 points**



- **T2**: 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**

```
┌──(zufan93㉿Kali)-[~]
└─$ nmap --script ftp-brute -p 21 sdf.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 23:04 EDT
Failed to resolve "sdf.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
```

```
┌──(zufan93㉿Kali)-[~]
└─$ nmap --script ftp-brute -p 21 205.166.94.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 23:15 EDT
Nmap scan report for 205.166.94.16
Host is up (0.0025s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 13.18 seconds
```

```
┌──(zufan93㉿Kali)-[~]
└─$ nmap --script snmp-brute -p 161 205.166.94.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 23:21 EDT
Nmap scan report for 205.166.94.16
Host is up (0.00045s latency).

PORT    STATE    SERVICE
161/tcp filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

```
┌──(zufan93㉿Kali)-[~]
└─$ nmap --script http-brute -p 80 205.166.94.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 23:23 EDT
Nmap scan report for 205.166.94.16
Host is up (0.00059s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

```
┌──(zufan93㉿Kali)-[~]
└─$ nmap --script oracle-brute -p 1521 205.166.94.16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-07 23:24 EDT
Nmap scan report for 205.166.94.16
Host is up (0.0032s latency).

PORT     STATE    SERVICE
1521/tcp filtered oracle

Nmap done: 1 IP address (1 host up) scanned in 13.53 seconds
```