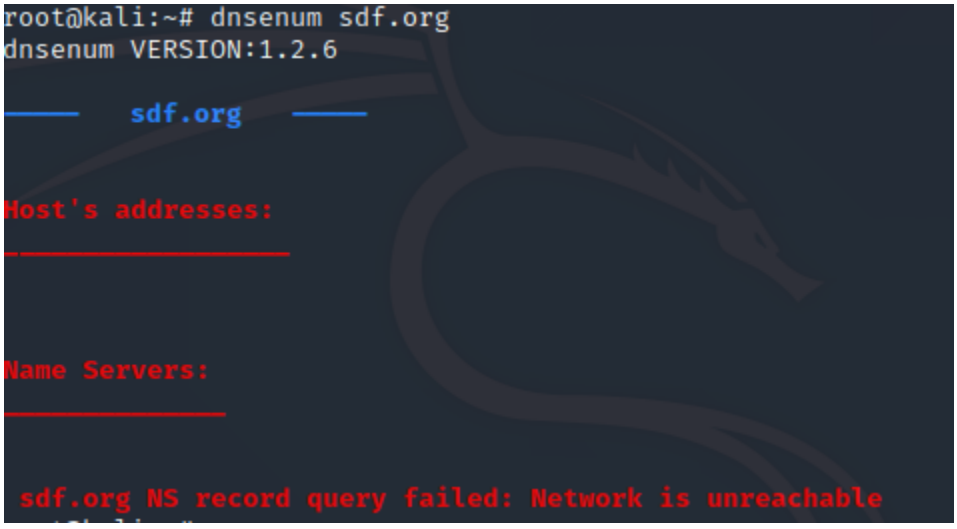
Old Dominion University CYSE 450: Ethical Hacking and Penetration Testing Lab 1: Active Reconnaissance and Vulnerability Scanning Handout Date: February 06, 2025 Due Date: February 20, 2025, 11:59 pm Total Points: 30

Tasks

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

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



• 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

```
root@kali:~# nmap -sT --reason sdf.org
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 11:39 EST
Failed to resolve "sdf.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.15 seconds
root@kali:~# nmap -sn --reason sdf.org
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 11:39 EST
Failed to resolve "sdf.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.01 seconds
```

• 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

```
root@kali:~# nmap sdf.org
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-19 11:40 EST
Failed to resolve "sdf.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.15 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. 5 points

```
root@kali:~# nmap --script sdf.org
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-20 09:34 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:818: 'sdf.org' did not match a category
, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:818: in local 'get_chosen_scrip
ts'
        /usr/bin/../share/nmap/nse_main.lua:1310: in main chunk
        [C]: in ?
```

• 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

```
root@kali:~# nmap --script ftp-brute -p 21 sdf.org
Starting Nmap 7.80 ( https://nmap.org ) at 2025-02-20 11:13 EST
Failed to resolve "sdf.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.50 seconds
```