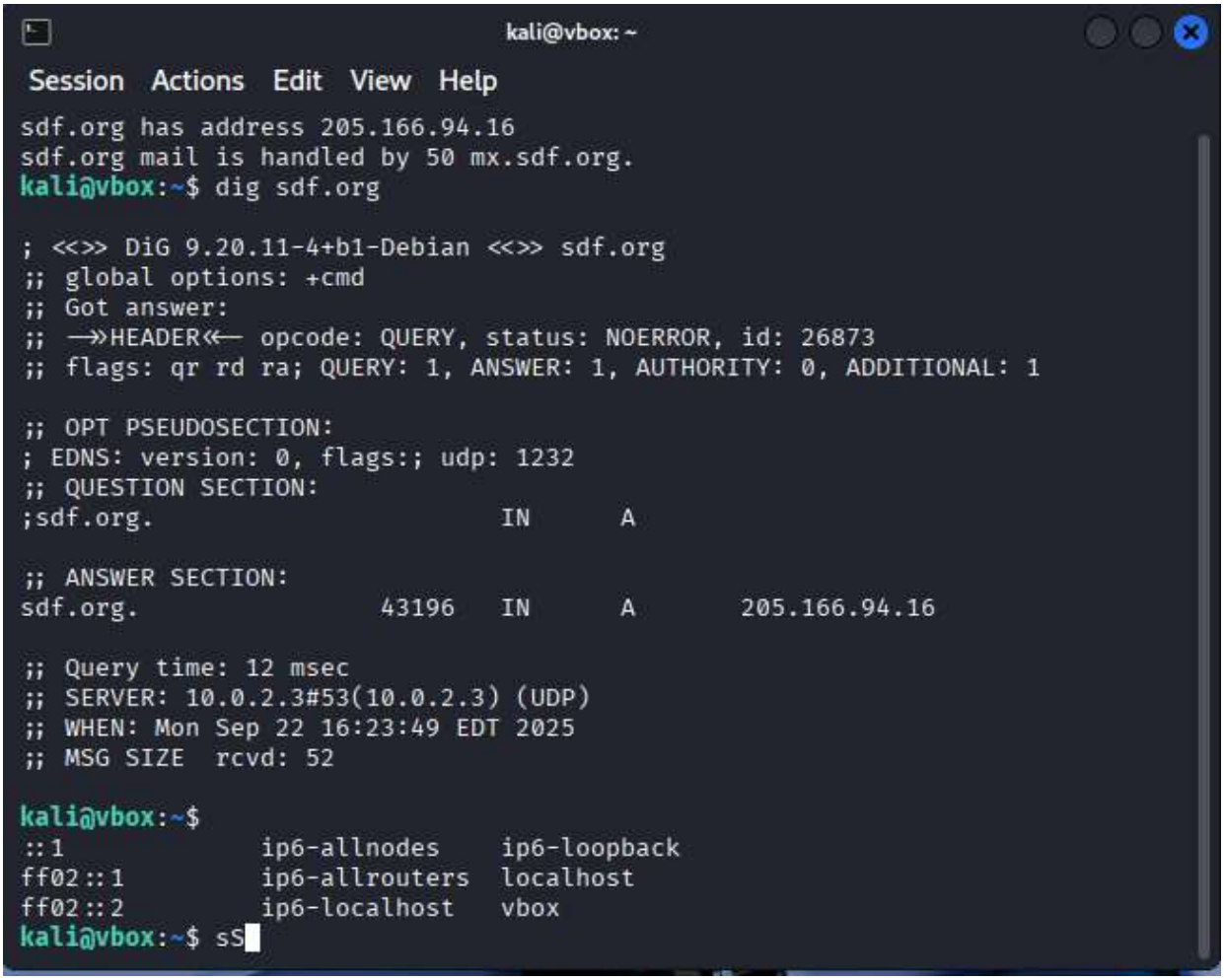
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing

Lab 3: Active Reconnaissance and Vulnerability Scanning

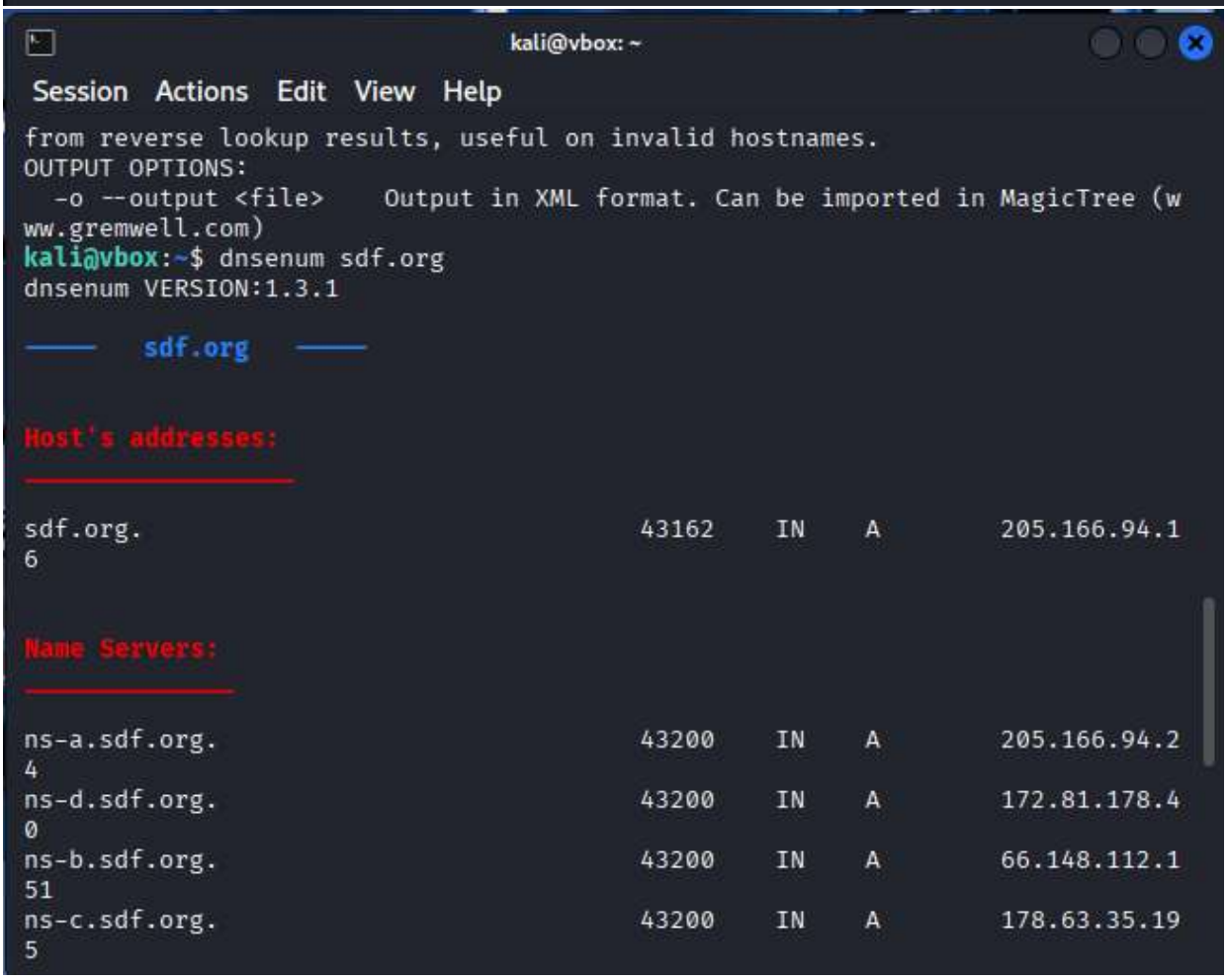
Total Points: 30

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**

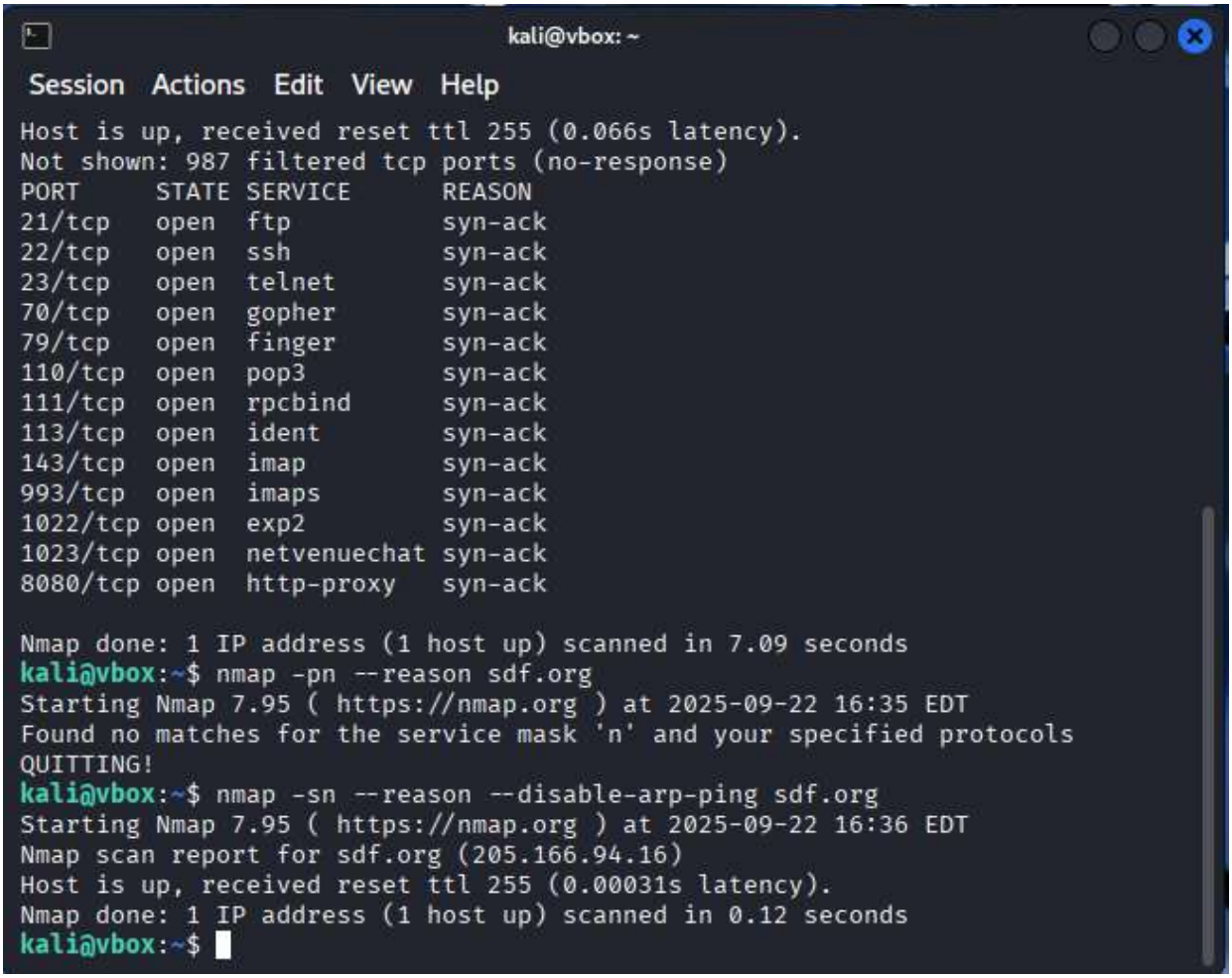


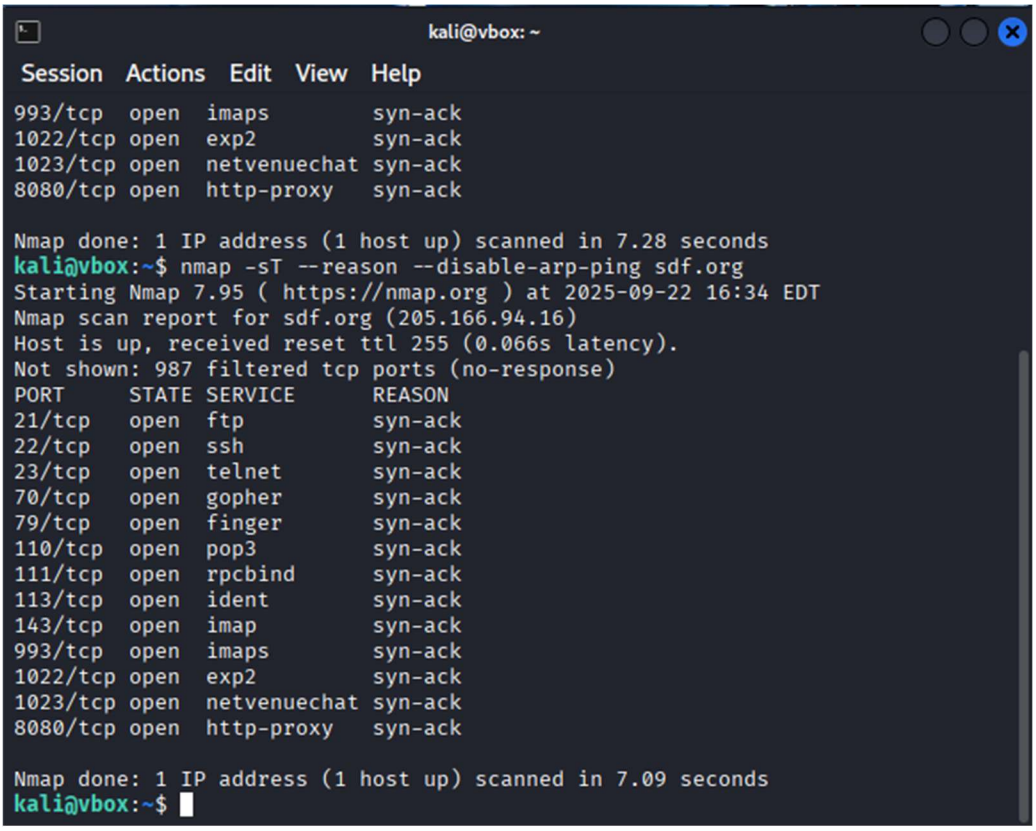
- **T2**: Perform **DNS enumeration** using ***dnsenum*** command for the host sdf.org. Check whether the **zone transfer** is possible. Provide necessary screenshots. **4 points**



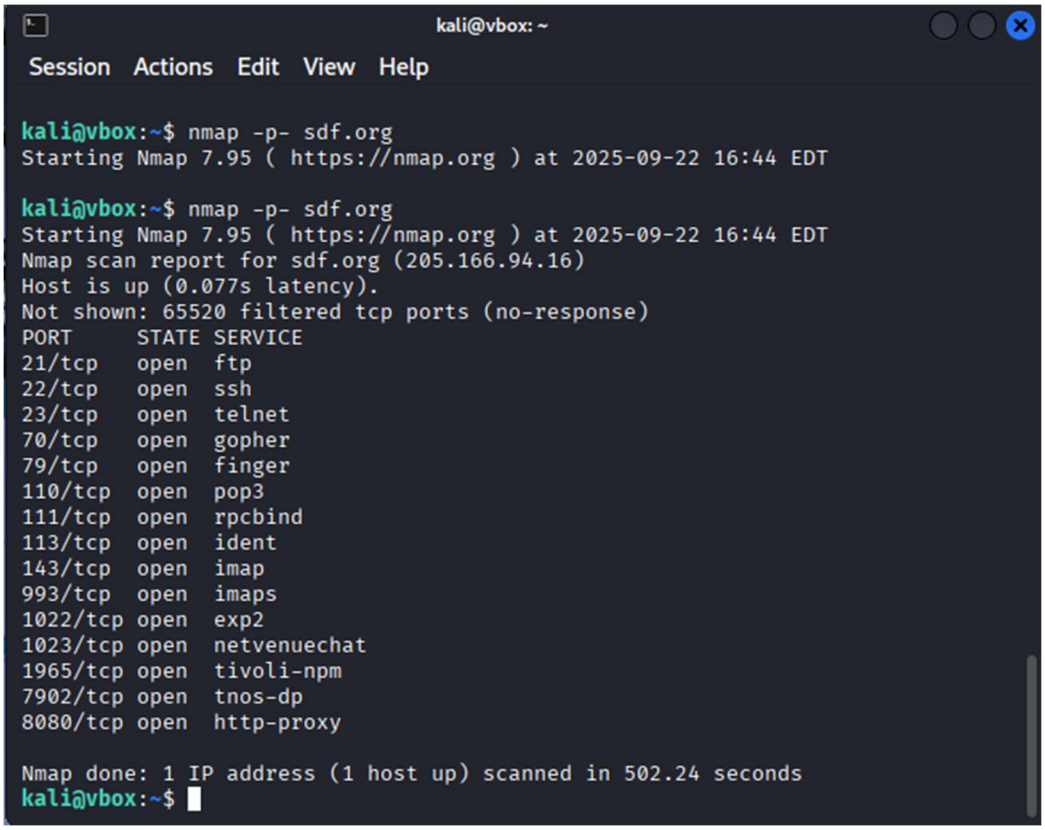
- **T3**: Perform both **ICMP Sweep** and **TCP Sweep** for the host sdf.org using NMAP. Use the option ***--reason*** to show the details and disable the ***arp-ping***. Attach screenshots

showing the results. **6 points**



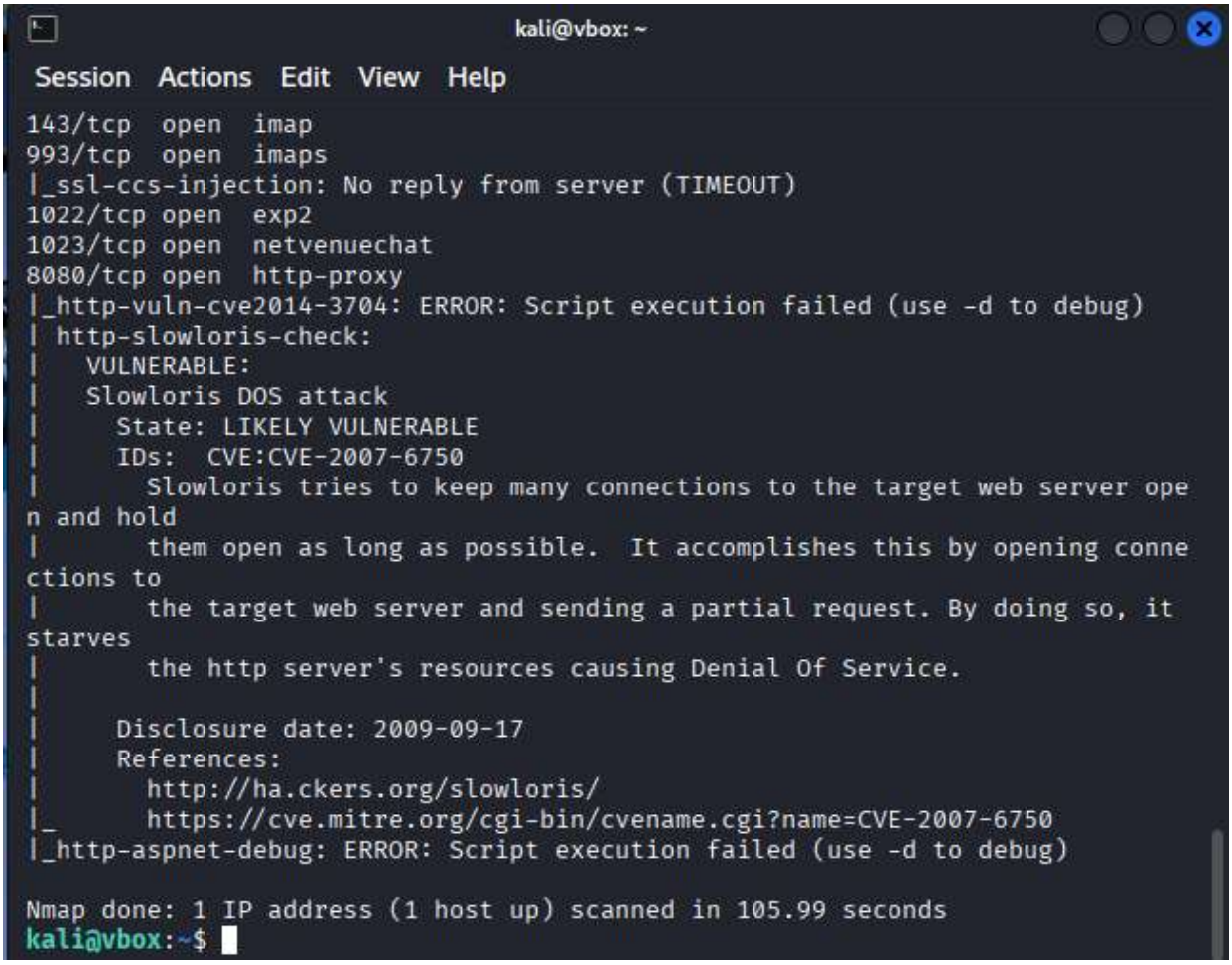

kali@vbox: ~
Session Actions Edit View Help
993/tcp open imaps syn-ack
1022/tcp open exp2 syn-ack
1023/tcp open netvenuechat syn-ack
8080/tcp open http-proxy syn-ack
Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds
kali@vbox:~$ nmap -sT --reason --disable-arp-ping sdf.org
Starting Nmap 7.95 (https://nmap.org) at 2025-09-22 16:34 EDT
Nmap scan report for sdf.org (205.166.94.16)
Host is up, received reset ttl 255 (0.066s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack
23/tcp open telnet syn-ack
70/tcp open gopher syn-ack
79/tcp open finger syn-ack
110/tcp open pop3 syn-ack
111/tcp open rpcbind syn-ack
113/tcp open ident syn-ack
143/tcp open imap syn-ack
993/tcp open imaps syn-ack
1022/tcp open exp2 syn-ack
1023/tcp open netvenuechat syn-ack
8080/tcp open http-proxy syn-ack
Nmap done: 1 IP address (1 host up) scanned in 7.09 seconds
kali@vbox:~$

- **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**