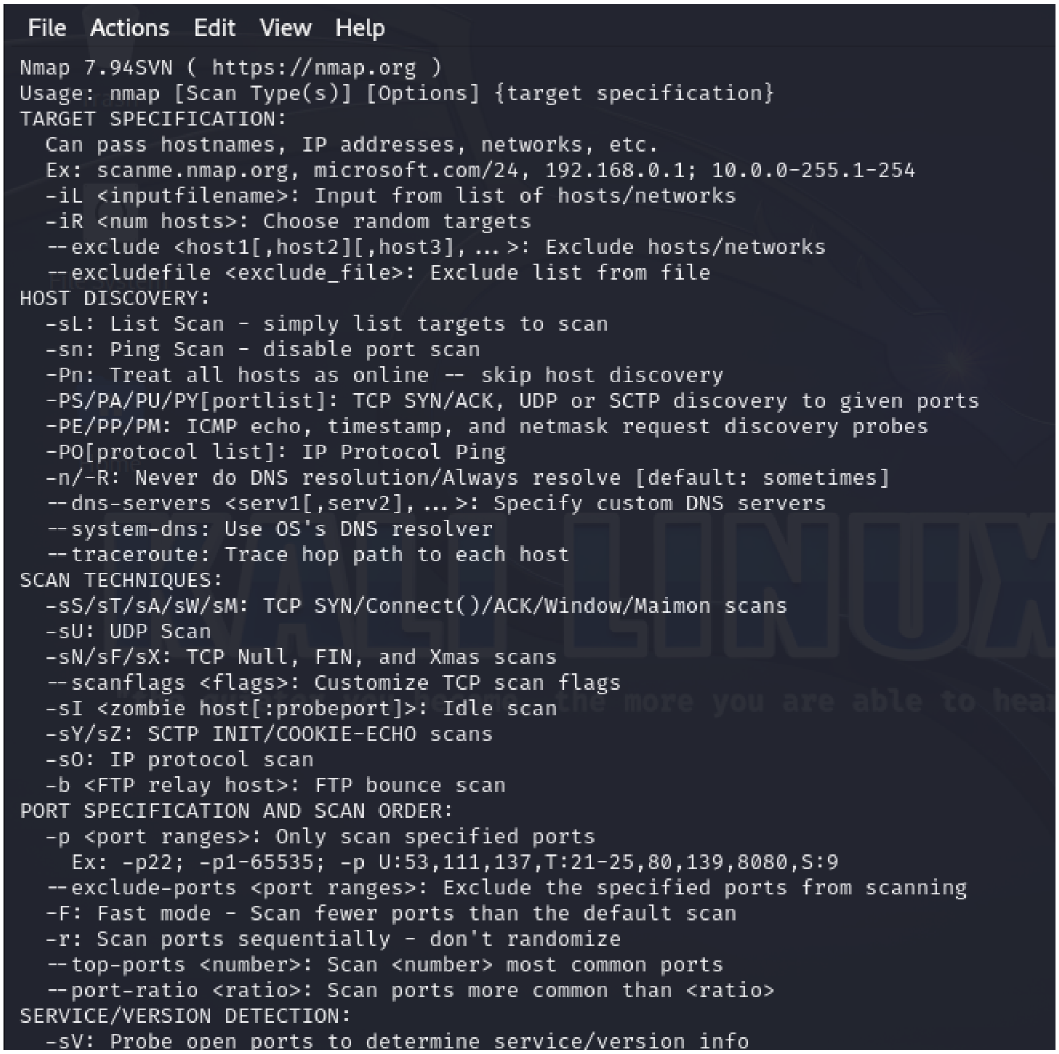
# Assignment-4 -Vulnerability Scan

## CYSE 450 -Ethical Hacking and Penetration Testing

### Task-A:  Stealth Scan using nmap [40 Points]

1. Open the **Root Terminal** in Kali Linux. Type **nmap -h** | **less** and press **Enter** to see all available Nmap commands. Submit the screenshot for the results.

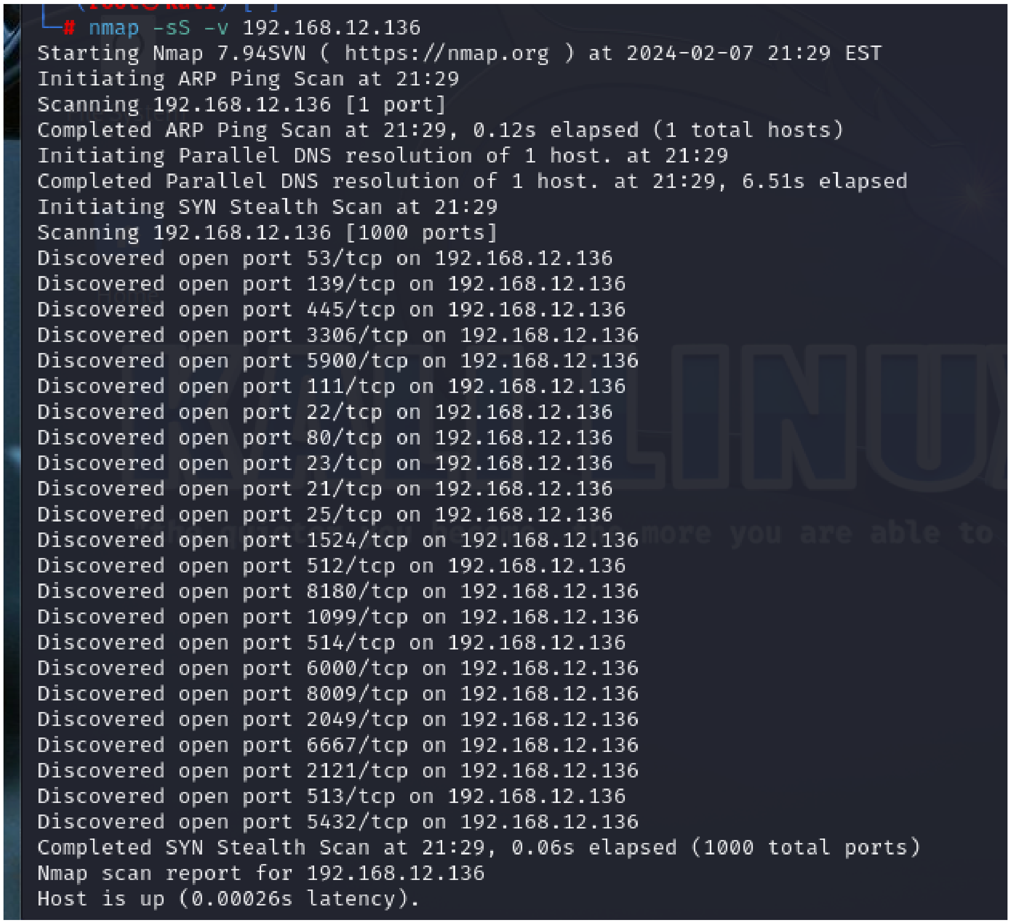


```
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
```

2. To send a SYN packet to an IP address of metasploitable 2 /Windows VM, type the following in Kali terminal.

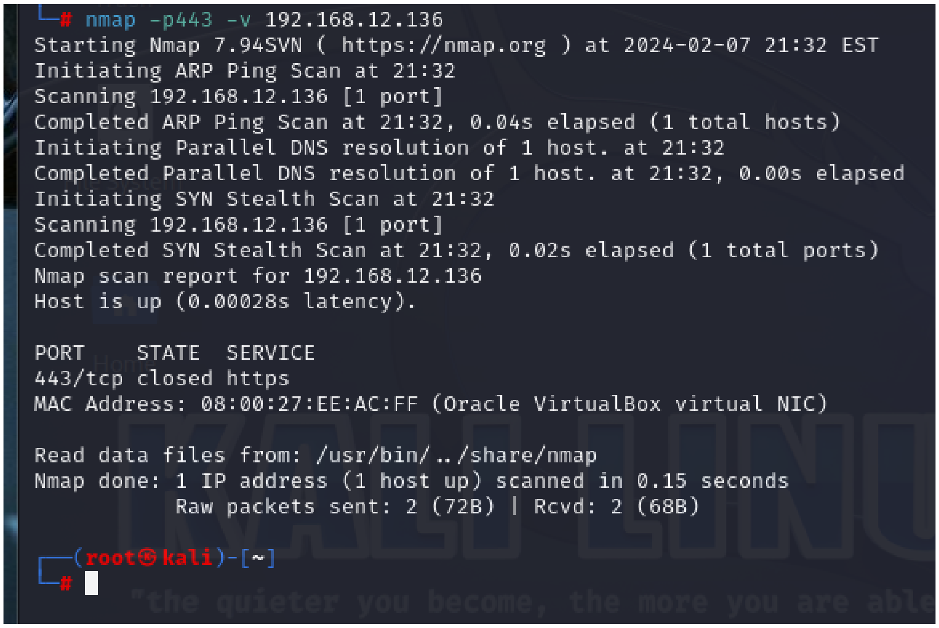
   **nmap -sS -v <ip-of-metasploitableo  or Windows VM>** and press **Enter**.

What are the results of your SYN scan? Submit the screenshot.



```
└─# nmap -sS -v 192.168.12.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 21:29 EST
Initiating ARP Ping Scan at 21:29
Scanning 192.168.12.136 [1 port]
Completed ARP Ping Scan at 21:29, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:29
Completed Parallel DNS resolution of 1 host. at 21:29, 6.51s elapsed
Initiating SYN Stealth Scan at 21:29
Scanning 192.168.12.136 [1000 ports]
Discovered open port 53/tcp on 192.168.12.136
Discovered open port 139/tcp on 192.168.12.136
Discovered open port 445/tcp on 192.168.12.136
Discovered open port 3306/tcp on 192.168.12.136
Discovered open port 5900/tcp on 192.168.12.136
Discovered open port 111/tcp on 192.168.12.136
Discovered open port 22/tcp on 192.168.12.136
Discovered open port 80/tcp on 192.168.12.136
Discovered open port 23/tcp on 192.168.12.136
Discovered open port 21/tcp on 192.168.12.136
Discovered open port 25/tcp on 192.168.12.136
Discovered open port 1524/tcp on 192.168.12.136
Discovered open port 512/tcp on 192.168.12.136
Discovered open port 8180/tcp on 192.168.12.136
Discovered open port 1099/tcp on 192.168.12.136
Discovered open port 514/tcp on 192.168.12.136
Discovered open port 6000/tcp on 192.168.12.136
Discovered open port 8009/tcp on 192.168.12.136
Discovered open port 2049/tcp on 192.168.12.136
Discovered open port 6667/tcp on 192.168.12.136
Discovered open port 2121/tcp on 192.168.12.136
Discovered open port 513/tcp on 192.168.12.136
Discovered open port 5432/tcp on 192.168.12.136
Completed SYN Stealth Scan at 21:29, 0.06s elapsed (1000 total ports)
Nmap scan report for 192.168.12.136
Host is up (0.00026s latency).
```

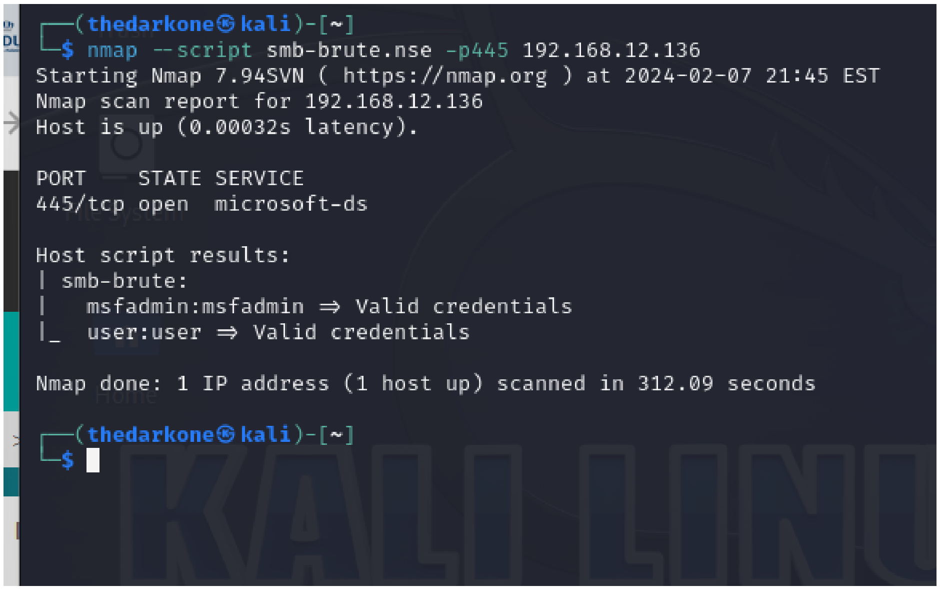
3. Limit the scope so you scan only port 443 by using the –p flag (**nmap –p44 3 –v ip-ofmetasploitable**). This makes the Nmap scan more targeted and less noticeable. Please submit the screenshot.



```
└─# nmap -p443 -v 192.168.12.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 21:32 EST
Initiating ARP Ping Scan at 21:32
Scanning 192.168.12.136 [1 port]
Completed ARP Ping Scan at 21:32, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:32
Completed Parallel DNS resolution of 1 host. at 21:32, 0.00s elapsed
Initiating SYN Stealth Scan at 21:32
Scanning 192.168.12.136 [1 port]
Completed SYN Stealth Scan at 21:32, 0.02s elapsed (1 total ports)
Nmap scan report for 192.168.12.136
Host is up (0.00028s latency).

PORT    STATE  SERVICE
443/tcp closed https
MAC Address: 08:00:27:EE:AC:FF (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (68B)

┌──(root㉿kali)-[~]
└─# 
```

## Task-B: Vulnerability Scan Using Nmap Script [20 Points]

1. Open the terminal in Kali Linux.
2. Using **nmap script** for brute force attack, scan the target machine (IP of Metasploitable or Windows) to guess its username/password.



```
┌──(thedarkone㉿kali)-[~]
└─$ nmap --script smb-brute.nse -p445 192.168.12.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-07 21:45 EST
Nmap scan report for 192.168.12.136
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-brute:
|   msfadmin:msfadmin ⇒ Valid credentials
|_  user:user ⇒ Valid credentials

Nmap done: 1 IP address (1 host up) scanned in 312.09 seconds

┌──(thedarkone㉿kali)-[~]
└─$ 
```

HINT: Please refer to the recording for the lecture (in Media Gallery on Canvas) and/or https://nmap.org/nsedoc/scripts/smb-brute.html

## Task-C: Secure Hacking Environment [20 Points]

1. How can you create a secure hacking environment, using web-based proxy, as an attacker? Please explain with examples.

   **A proxy server is like a gateway that anonymously passes data between users and the internet. In essence, a proxy server speaks on behalf of the user to the internet. In terms of how a hacker could use them, they could use them to hide malicious network activities like DDoS attacks or rootkits, so they can stay anonymous. This is a way to secure a hacking environment.**

2. What is the purpose of using Macchanger tool in hacking?

**Mac changer is a hacking tool used for Mac address spoofing. Mac addresses are hard coded in computers; however, the tool allows the user to make the OS believe the NIC has the Mac address of the user's (hacker) choice. This tool is used to increase anonymity, bypass filters, and impersonate other devices.**

## Extra Credit Question:

**Research question [10 points]**

1. Open your web browser and go to https://osintframework.com/.
2. Explore the framework by expanding nodes to discover different tools. Choose two tools. In 2-3 paragraphs describe what these two tools can do, how to use them, and how they would be useful in footprinting.

**Note:** Your Answer should contain 2-3 paragraphs, at least one paragraphs per tool chosen. The **name** of the tool, **website location**, **brief instructions**, and how the tool is useful in footprinting should be discussed.