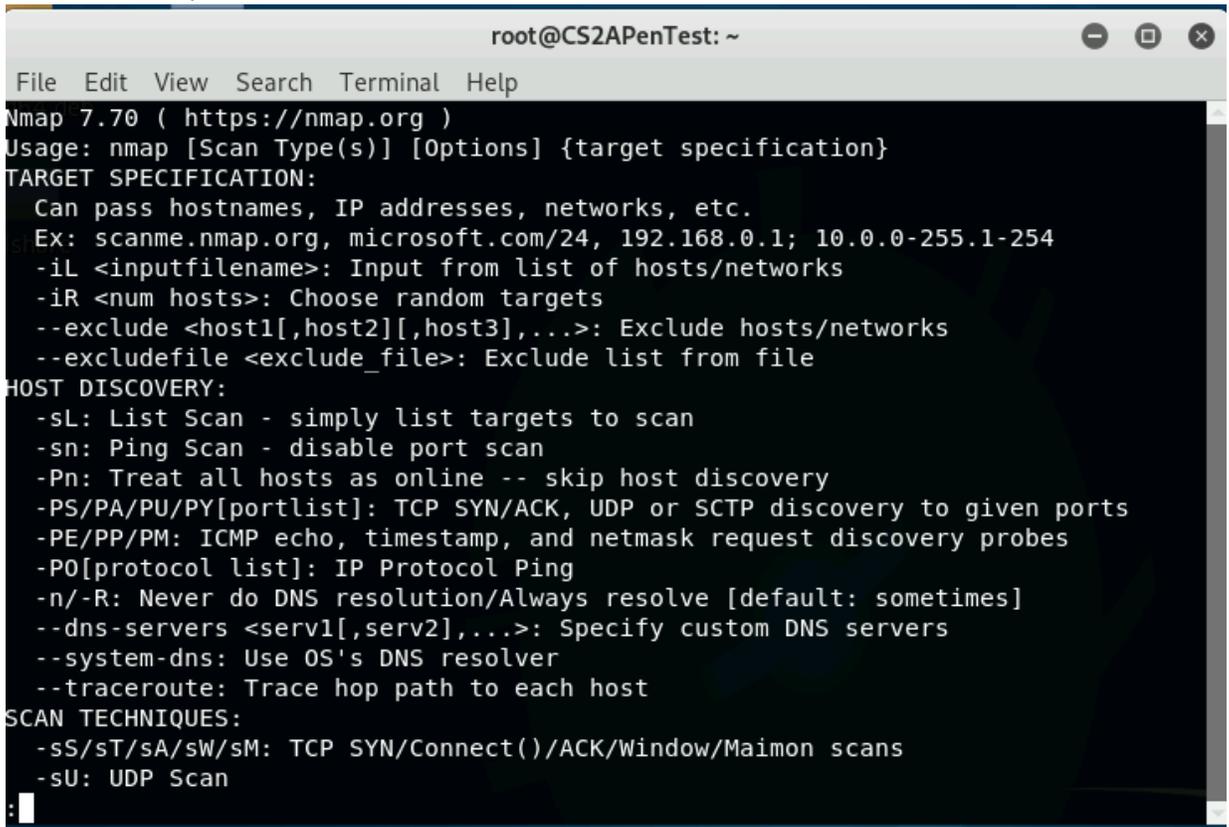


## Assignment-4 -Vulnerability Scan

### 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.



```
root@CS2APenTest: ~
File Edit View Search Terminal Help
Nmap 7.70 ( 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
```

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-metasploitable0 or Windows VM>** and press **Enter**.

```
Nmap scan report for 192.168.10.11
Host is up (0.035s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
nam
```

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

3. Limit the scope so you scan only port 443 by using the `-p` flag (**`nmap -p443 -v ip-ofmetasploitable`**). This makes the Nmap scan more targeted and less noticeable. Please submit the screenshot.

```
root@CS2APenTest:~# nmap -p443 -v 192.168.10.11
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-09 01:17 EST
Initiating ARP Ping Scan at 01:17
Scanning 192.168.10.11 [1 port]
Completed ARP Ping Scan at 01:17, 0.07s elapsed (1 total hosts)
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 01:17
Scanning 192.168.10.11 [1 port]
Completed SYN Stealth Scan at 01:17, 0.07s elapsed (1 total ports)
Nmap scan report for 192.168.10.11
Host is up (0.012s latency).

PORT      STATE SERVICE
443/tcp   closed https
MAC Address: 00:15:5D:40:57:2A (Microsoft)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
Raw packets sent: 2 (72B) | Rcvd: 2 (68B)
root@CS2APenTest:~#
```

### 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.

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

```
root@CS2APenTest: # sudo nmap -sU -sS --script smb-brute.nse -p U:137,T:139 192.168.10.11
Starting Nmap 7.70 ( https://nmap.org ) at 2024-02-09 01:33 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:03:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Stats: 0:04:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.10.11
Host is up (0.0080s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn
137/udp    open  netbios-ns
MAC Address: 00:15:5D:40:57:2A (Microsoft)

Host script results:
| smb-brute:
|   msfadmin:msfadmin => Valid credentials
|_  user:user => Valid credentials
```

### 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. Creating a secure hacking environment using a web-based proxy involves several steps to anonymize network traffic and hide the attacker's true IP address. To start, the attacker selects a reliable web-based proxy service that offers features such as HTTPS encryption, anonymity, and reliable uptime, such as TOR, ProxySite, HideMyAss, or CyberGhost. Once chosen, the attacker configures their web browser or network tools to use the selected web-based proxy, typically by entering the proxy server's address and port number in the network settings of the application. After configuring the proxy settings, the attacker verifies their anonymity by testing the connection to ensure that their traffic is being routed through the web-based proxy and that their real IP address is hidden. This can be done using online services like WhatIsMyIPAddress or IPLeak. With the secure hacking environment set up, the attacker can then proceed to conduct penetration testing, vulnerability assessments, or other security assessments against target systems, ensuring to follow ethical guidelines, obtain proper authorization, and respect the privacy and security of others at all times.
2. What is the purpose of using Macchanger tool in hacking?

The Macchanger tool, available on Unix-like operating systems such as Linux, serves the purpose of manipulating the MAC address of network interfaces. This unique identifier is assigned to network interfaces and changing it can provide anonymity and privacy, particularly in scenarios where network traffic monitoring or tracking based on MAC addresses is a concern. Macchanger is used primarily for anonymizing network traffic by changing the MAC address of the network interface, making it difficult for network administrators or attackers to track activities based on MAC addresses. It can also aid in evading MAC address filtering, a security measure implemented by some networks to only allow specific devices to connect. Macchanger allows users to spoof a MAC address that is allowed on the network, enabling unauthorized devices to connect. In penetration testing or ethical hacking scenarios, Macchanger can simulate different devices on a network, test network security controls, or bypass MAC address-based security mechanisms. However, it's essential to note that while Macchanger can provide anonymity and aid in certain hacking scenarios, its use must comply with legal and ethical standards. Unauthorized manipulation of MAC addresses or network interfaces may be illegal and unethical, necessitating proper authorization before using such tools in security assessments or penetration tests.