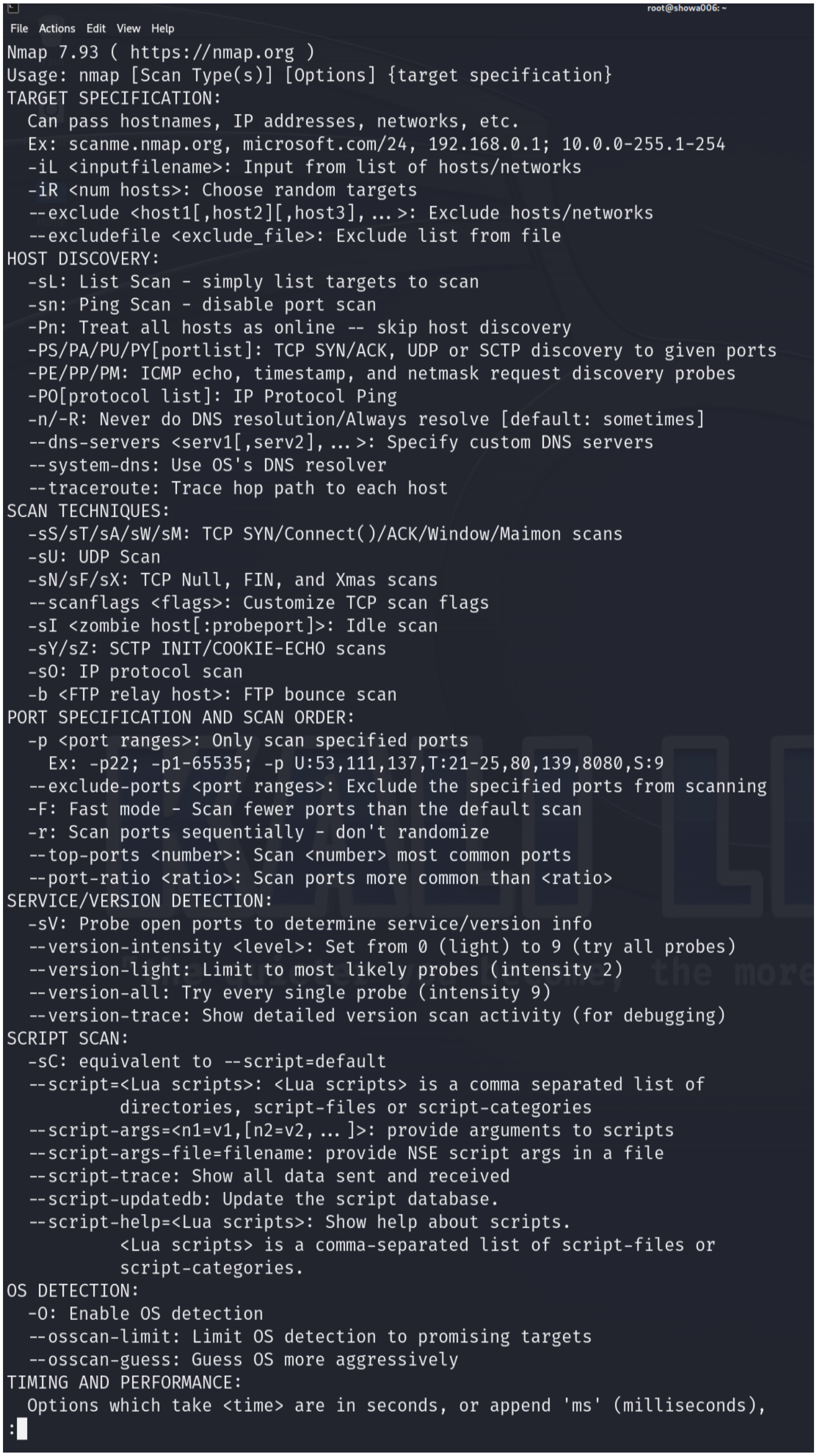
Assignment-4 -Vulnerability Scan
CYSE 450 -Ethical Hacking and Penetration Testing

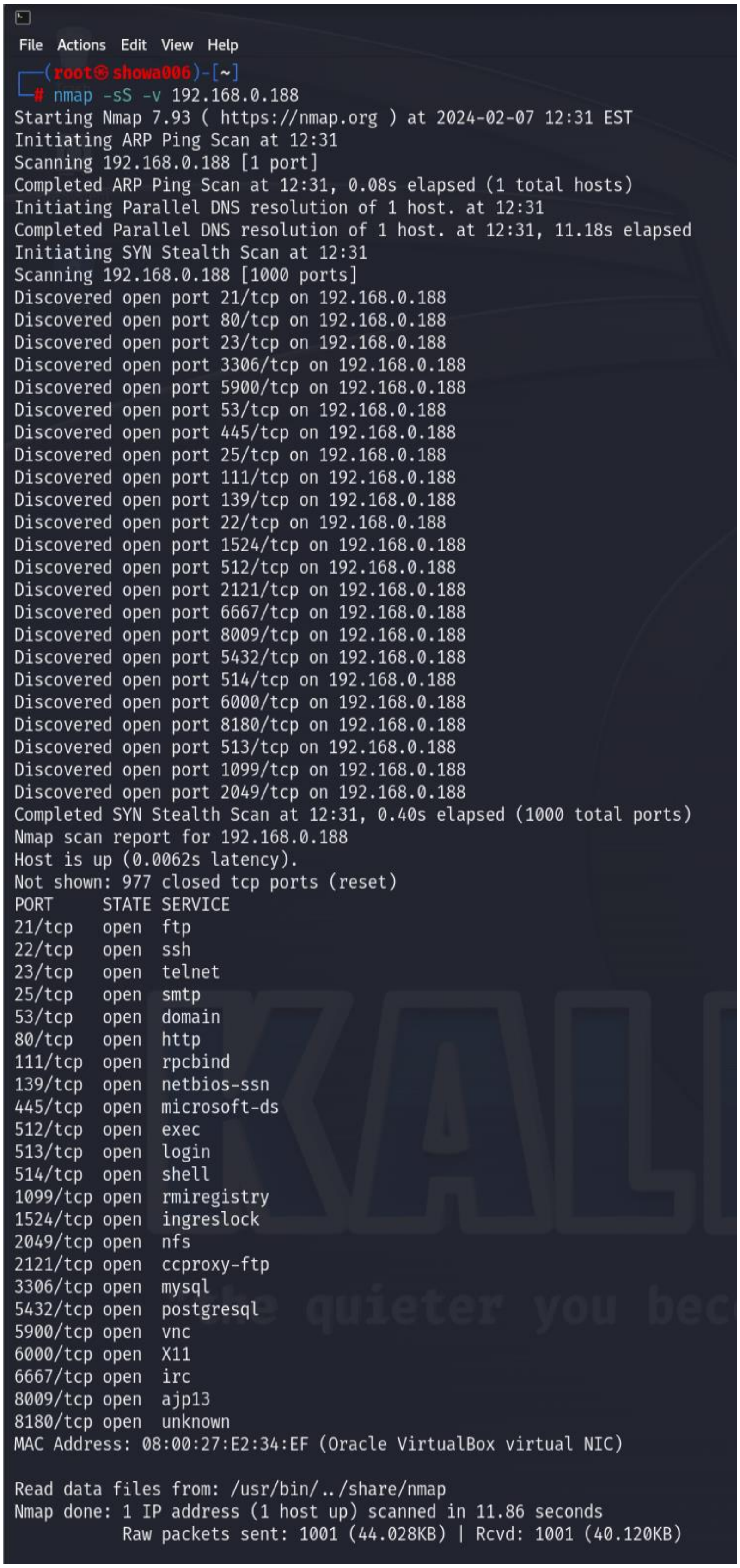
Task-A: Stealth Scan using nmap [40 Points]

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



```
Nmap 7.93 ( 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
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
:
```

2. What are the results of your SYN scan? Submit the screenshot. **nmap -sS -v <ip- of-metasploitableo or Windows VM>** and press **Enter**.

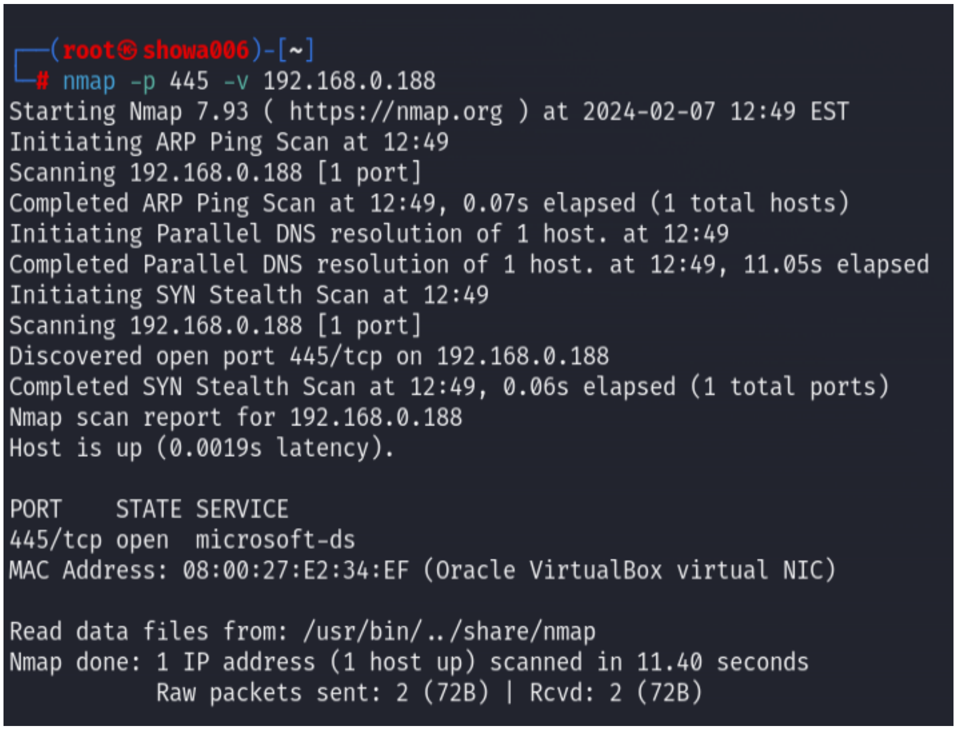


```
┌──(root㉿showa006)-[~]
└─# nmap -sS -v 192.168.0.188
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 12:31 EST
Initiating ARP Ping Scan at 12:31
Scanning 192.168.0.188 [1 port]
Completed ARP Ping Scan at 12:31, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:31
Completed Parallel DNS resolution of 1 host. at 12:31, 11.18s elapsed
Initiating SYN Stealth Scan at 12:31
Scanning 192.168.0.188 [1000 ports]
Discovered open port 21/tcp on 192.168.0.188
Discovered open port 80/tcp on 192.168.0.188
Discovered open port 23/tcp on 192.168.0.188
Discovered open port 3306/tcp on 192.168.0.188
Discovered open port 5900/tcp on 192.168.0.188
Discovered open port 53/tcp on 192.168.0.188
Discovered open port 445/tcp on 192.168.0.188
Discovered open port 25/tcp on 192.168.0.188
Discovered open port 111/tcp on 192.168.0.188
Discovered open port 139/tcp on 192.168.0.188
Discovered open port 22/tcp on 192.168.0.188
Discovered open port 1524/tcp on 192.168.0.188
Discovered open port 512/tcp on 192.168.0.188
Discovered open port 2121/tcp on 192.168.0.188
Discovered open port 6667/tcp on 192.168.0.188
Discovered open port 8009/tcp on 192.168.0.188
Discovered open port 5432/tcp on 192.168.0.188
Discovered open port 514/tcp on 192.168.0.188
Discovered open port 6000/tcp on 192.168.0.188
Discovered open port 8180/tcp on 192.168.0.188
Discovered open port 513/tcp on 192.168.0.188
Discovered open port 1099/tcp on 192.168.0.188
Discovered open port 2049/tcp on 192.168.0.188
Completed SYN Stealth Scan at 12:31, 0.40s elapsed (1000 total ports)
Nmap scan report for 192.168.0.188
Host is up (0.0062s latency).
Not shown: 977 closed tcp ports (reset)
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
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.86 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.120KB)
```

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.

I don’t have port 443 on XP or Metasploitable, so I used 445



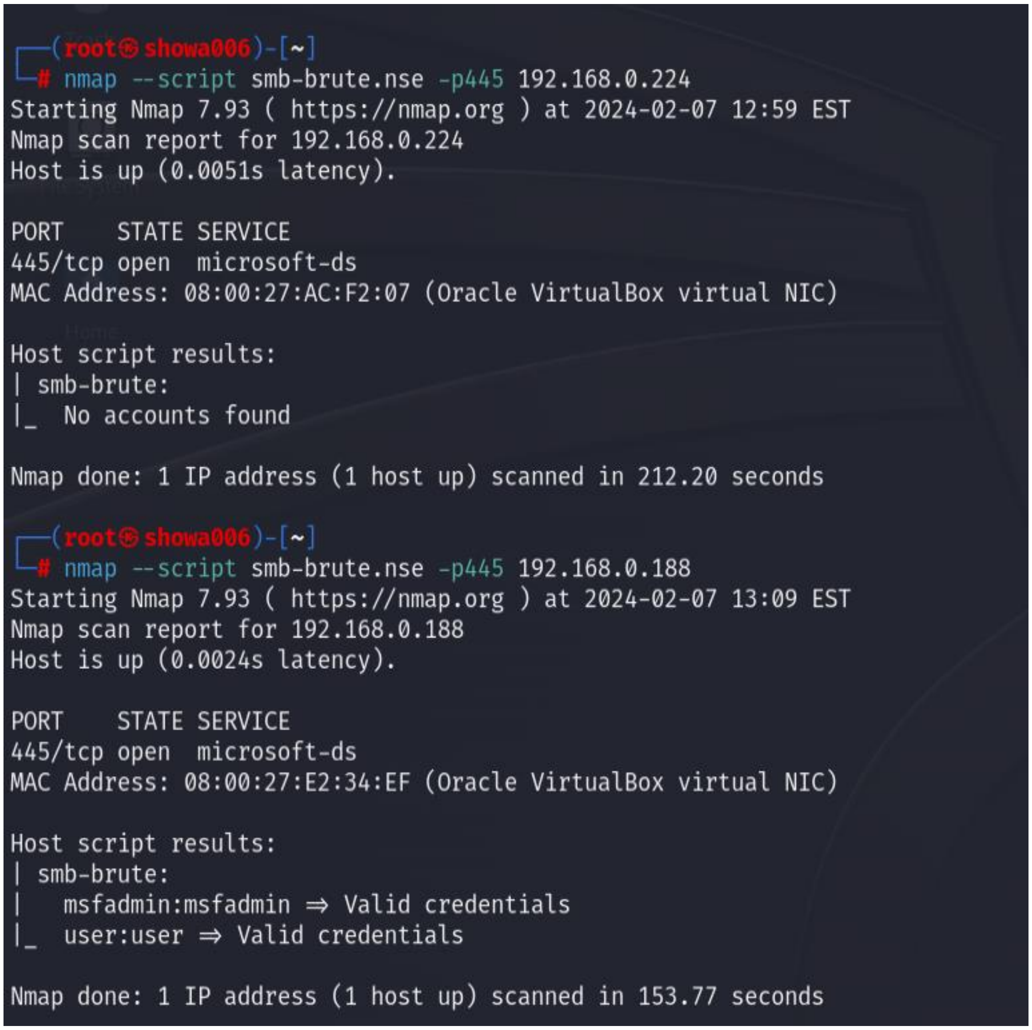
```
┌──(root㉿showa006)-[~]
└─# nmap -p 445 -v 192.168.0.188
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 12:49 EST
Initiating ARP Ping Scan at 12:49
Scanning 192.168.0.188 [1 port]
Completed ARP Ping Scan at 12:49, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:49
Completed Parallel DNS resolution of 1 host. at 12:49, 11.05s elapsed
Initiating SYN Stealth Scan at 12:49
Scanning 192.168.0.188 [1 port]
Discovered open port 445/tcp on 192.168.0.188
Completed SYN Stealth Scan at 12:49, 0.06s elapsed (1 total ports)
Nmap scan report for 192.168.0.188
Host is up (0.0019s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

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.



```
┌──(root㉿showa006)-[~]
└─# nmap --script smb-brute.nse -p445 192.168.0.224
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 12:59 EST
Nmap scan report for 192.168.0.224
Host is up (0.0051s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:AC:F2:07 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-brute:
|_  No accounts found

Nmap done: 1 IP address (1 host up) scanned in 212.20 seconds

┌──(root㉿showa006)-[~]
└─# nmap --script smb-brute.nse -p445 192.168.0.188
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-07 13:09 EST
Nmap scan report for 192.168.0.188
Host is up (0.0024s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E2:34:EF (Oracle VirtualBox virtual NIC)

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

Nmap done: 1 IP address (1 host up) scanned in 153.77 seconds
```

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 web-based proxy is a tool that intercepts web traffic and allows hackers to analyze, modify, and exploit vulnerabilities in web applications or servers. It can scan and crawl web apps, test its robustness and error handling, bypass security mechanisms, and spoof the identity or location of the attacker. Some examples of proxies for secure hacking environments Burp Suite, ZAP, CyberGhost, ExpressVPN, NordVPN, Private Internet Access, and IPVanish.

To use a web-based proxy for an attack, the attacker must configure the browser or application to connect to the proxy as a gateway to the web server. This is done by setting the proxy address and port or by using tools like ProxyCap or Proxifier. The attacker installs the proxy's certificate in the browser or application to avoid SSL errors when intercepting HTTPS traffic. Once set up, the attacker can capture and manipulate web traffic to perform attacks on the web application or server.

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

Macchanger is a tool used in hacking to change the MAC address of a network interface to avoid being tracked or detected by security tools. By impersonating other devices, hackers can bypass authentication mechanisms and access control. This command-line tool can be installed on Linux systems and can change the MAC address to a specific, random, or vendor list value. Moreover, Macchanger can reset the MAC address to its original value after the device is rebooted.