Module 3 Exam

The Host discovery is

```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -l | grep PCS
192.168.20.127  08:00:27:8a:4f:c5       PCS Systemtechnik GmbH
```

Netscan

(i) The target ip address is 192.168.20.127. To perform half scan to all the port we need to do a tcp stealth scan which is half scan. -p- is used for all the ports. The command is : nmap -sT -p- 192.168.20.127

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT -p- 192.168.20.127
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 04:49 EST
Nmap scan report for 192.168.20.127
Host is up (0.00094s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
6667/tcp open  irc
MAC Address: 08:00:27:8A:4F:C5 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 9.51 seconds
```

ii) To perform OS discovery we use -O command and for customise ports we use -p and then give our desired ports which is 200-1500. The command is: nmap -O -p 200-1500 192.168.20.127

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -p 200-1500 192.168.20.127
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 04:47 EST
Nmap scan report for 192.168.20.127
Host is up (0.00085s latency).
Not shown: 1300 closed tcp ports (reset)
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:8A:4F:C5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.32 seconds
```

iii) For TCP scan we use -sT and for version we use the V in the -sTV. For all port we use -p- and for time template level 3 we use -T3. -A is used for aggressive scanning and -v is used for verbose scan.
The command is : nmap -sVT -p- -T3 -A -V 192.168.20.127

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sTV -p- -T3 -A -v 192.168.20.127
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 04:44 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating ARP Ping Scan at 04:44
Scanning 192.168.20.127 [1 port]
Completed ARP Ping Scan at 04:44, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:44
Completed Parallel DNS resolution of 1 host. at 04:44, 13.00s elapsed
Initiating Connect Scan at 04:44
Scanning 192.168.20.127 [65535 ports]
Discovered open port 6667/tcp on 192.168.20.127
Completed Connect Scan at 04:45, 18.02s elapsed (65535 total ports)
Initiating Service scan at 04:45
Scanning 1 service on 192.168.20.127
Completed Service scan at 04:45, 0.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.20.127
NSE: Script scanning 192.168.20.127.
Initiating NSE at 04:45
Completed NSE at 04:45, 10.04s elapsed
Initiating NSE at 04:45
Completed NSE at 04:45, 0.01s elapsed
Initiating NSE at 04:45
Completed NSE at 04:45, 0.00s elapsed
```

```
Host is up (0.0011s latency).
Not shown: 64884 closed tcp ports (conn-refused), 650 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
6667/tcp open  irc     InspIRCd
| irc-info:
|   server: Admin.local
|   users: 2
|   servers: 1
|   chans: 0
|   lusers: 2
|   lservers: 0
|   source ident: nmap
|   source host: 192.168.20.106
|_  error: Closing link: (nmap@192.168.20.106) [Client exited]
MAC Address: 08:00:27:8A:4F:C5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.038 days (since Thu Dec 15 03:50:06 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: Admin.local

TRACEROUTE
HOP RTT     ADDRESS
1   1.13 ms 192.168.20.127

NSE: Script Post-scanning.
Initiating NSE at 04:45
Completed NSE at 04:45, 0.00s elapsed
Initiating NSE at 04:45
Completed NSE at 04:45, 0.00s elapsed
Initiating NSE at 04:45
```

```
Initiating NSE at 04:45
Completed NSE at 04:45, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.08 seconds
           Raw packets sent: 23 (1.806KB) | Rcvd: 15 (1.278KB)
```

2. Script Scan

(i) To perform the default script scan we use -sC and for verbose mode we use -v. The command for this is: nmap -sC -v 192.168.20.127

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -v 192.168.20.127

Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 04:59 EST
NSE: Loaded 125 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:59
Completed NSE at 04:59, 0.00s elapsed
Initiating NSE at 04:59
Completed NSE at 04:59, 0.00s elapsed
Initiating ARP Ping Scan at 04:59
Scanning 192.168.20.127 [1 port]
Completed ARP Ping Scan at 04:59, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:59
Completed Parallel DNS resolution of 1 host. at 04:59, 6.57s elapsed
Initiating SYN Stealth Scan at 04:59
Scanning 192.168.20.127 [1000 ports]
Discovered open port 445/tcp on 192.168.20.127
Discovered open port 139/tcp on 192.168.20.127
Discovered open port 22/tcp on 192.168.20.127
Discovered open port 80/tcp on 192.168.20.127
Discovered open port 3306/tcp on 192.168.20.127
Discovered open port 6667/tcp on 192.168.20.127
Completed SYN Stealth Scan at 04:59, 0.12s elapsed (1000 total ports)
NSE: Script scanning 192.168.20.127.
Initiating NSE at 04:59
```

2 (ii) To perform a script “http-enum.nse” and verbose mode we use the following command : nmap --script http-enum.nse -v 192.168.20.127. The Host script result is given below.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script http-enum.nse -v 192.168.20.127
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 05:04 EST
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating ARP Ping Scan at 05:04
Scanning 192.168.20.127 [1 port]
Completed ARP Ping Scan at 05:04, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:04
Completed Parallel DNS resolution of 1 host. at 05:04, 1.18s elapsed
Initiating SYN Stealth Scan at 05:04
Scanning 192.168.20.127 [1000 ports]
Discovered open port 22/tcp on 192.168.20.127
Discovered open port 445/tcp on 192.168.20.127
Discovered open port 3306/tcp on 192.168.20.127
Discovered open port 139/tcp on 192.168.20.127
Discovered open port 80/tcp on 192.168.20.127
Discovered open port 6667/tcp on 192.168.20.127
Completed SYN Stealth Scan at 05:04, 0.11s elapsed (1000 total ports)
NSE: Script scanning 192.168.20.127.
Initiating NSE at 05:04
Completed NSE at 05:04, 1.87s elapsed
Nmap scan report for 192.168.20.127
Host is up (0.00064s latency).
Not shown: 994 closed tcp ports (reset)
```

Host Script result portion

```
Host script results:
|_clock-skew: mean: -3h20m00s, deviation: 5h46m24s, median: 0s
| smb2-time:
|   date: 2022-12-15T09:59:26
|_  start_date: N/A
| nbstat: NetBIOS name: BJIT-EXAM, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xero
x)
| Names:
|   BJIT-EXAM<00>        Flags: <unique><active>
|   BJIT-EXAM<03>        Flags: <unique><active>
|   BJIT-EXAM<20>        Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: \x00
|   NetBIOS computer name: BJIT-EXAM\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-12-15T19:59:26+10:00
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 04:59
Completed NSE at 04:59, 0.00s elapsed
Initiating NSE at 04:59
Completed NSE at 04:59, 0.00s elapsed
```