The first thing I did was enumerate the website using dirbuster, gobuster, and nikto. I found some extensions but they were not that important. After browsing the site, I came across a dead link and had to direct 10.10.10.194 to the site (megahosting.htb) by editing the /etc/hosts file. I searched online and saw that the service could be vulnerable to a remote file inclusion exploit, but it didn’t work. I then realized that it was vulnerable to a local file inclusion exploit since the news.php extension mentioned that the site was taken down because of a data leak. I was able to get the /etc/passwd file by editing the extension so that it was
[site]/news.php?file=../../../../etc/passwd.

I then did some more research on Apache Tomcat and found that its username/password configuration files were located in the /usr/share/tomcat9/etc/tomcat-users.xml file. On the 8080 port, there was a link to the /manager extension. Further research about Apache Tomcat reveals that you can deploy a war file on the server as detailed here:
https://tomcat.apache.org/tomcat-9.0-doc/manager-howto.html

I crafted a shell.war payload using msfvenom and then using the command:

```
curl -T shell.war -u ‘tomcat:[password]’
‘http://10.10.10.194:8080/manager/text/deploy?path=/hackme’
```

I was able to upload a shell to the extension 10.10.10.194:8080/hackme. After getting the revere shell and doing some enumeration, I found a file that ash (the user) was the owner of. I did this by doing find / -user ash 2>/dev/null. The file was a password locked zip file. I used fcrackzip to crack the password to the zip file, specifically the command:

```
fcrackzip -D -u -p [...rockyou.txt] load.zip
```

The password ended up being admin@it.

I noticed that when I checked out my user id, there was an id reference to lxd. Using this technique, I was able to escalate my privileges:
https://www.hackingarticles.in/lxd-privilege-escalation/
Note: The steps for the most part are correct, but I also have to make sure that I run lxd init on the exploited machine.