Thompson - Walkthrough

This is an easy level CTF room on TryHackMe that requires knowledge of using reverse shells & cron jobs.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

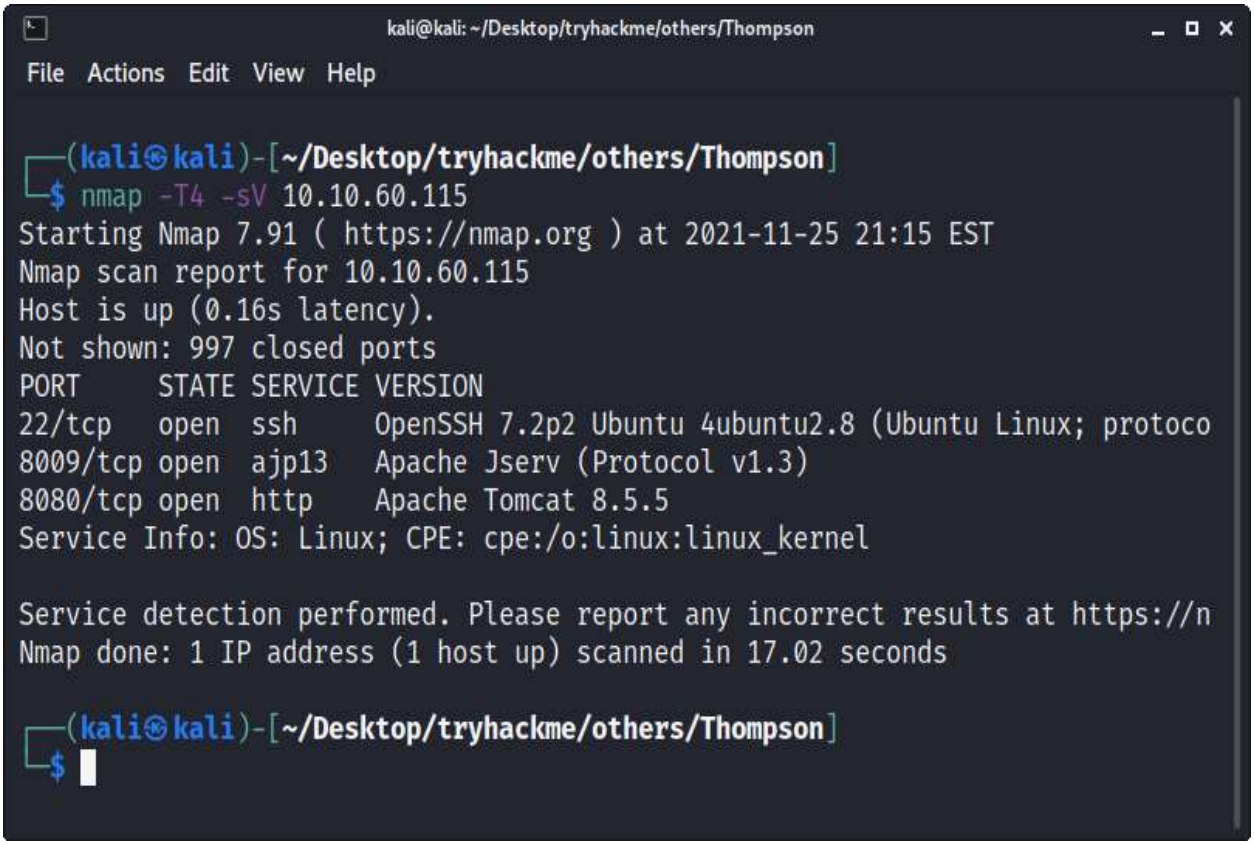
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, dirbuster, firefox, msfvenom, netcat

Scanning

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.

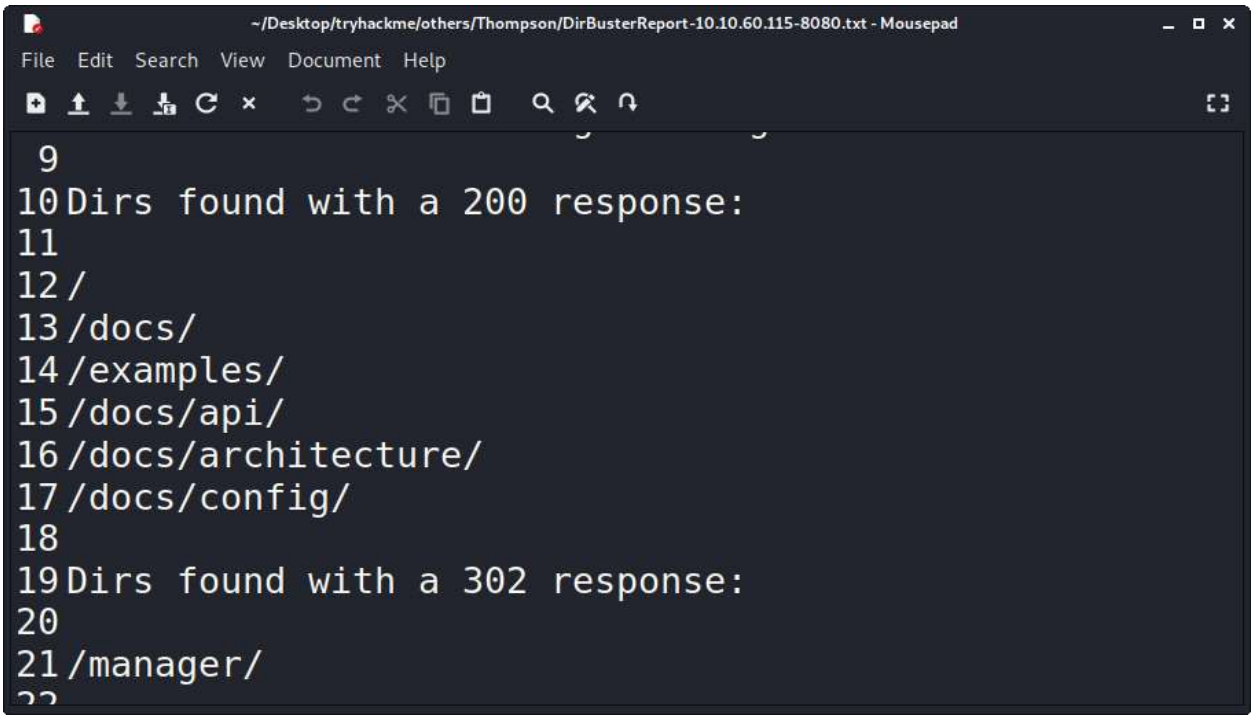


Apache tomcat server was running on port 8080

So, I visited the url: **http://10.10.60.115:8080** in the **firefox**.

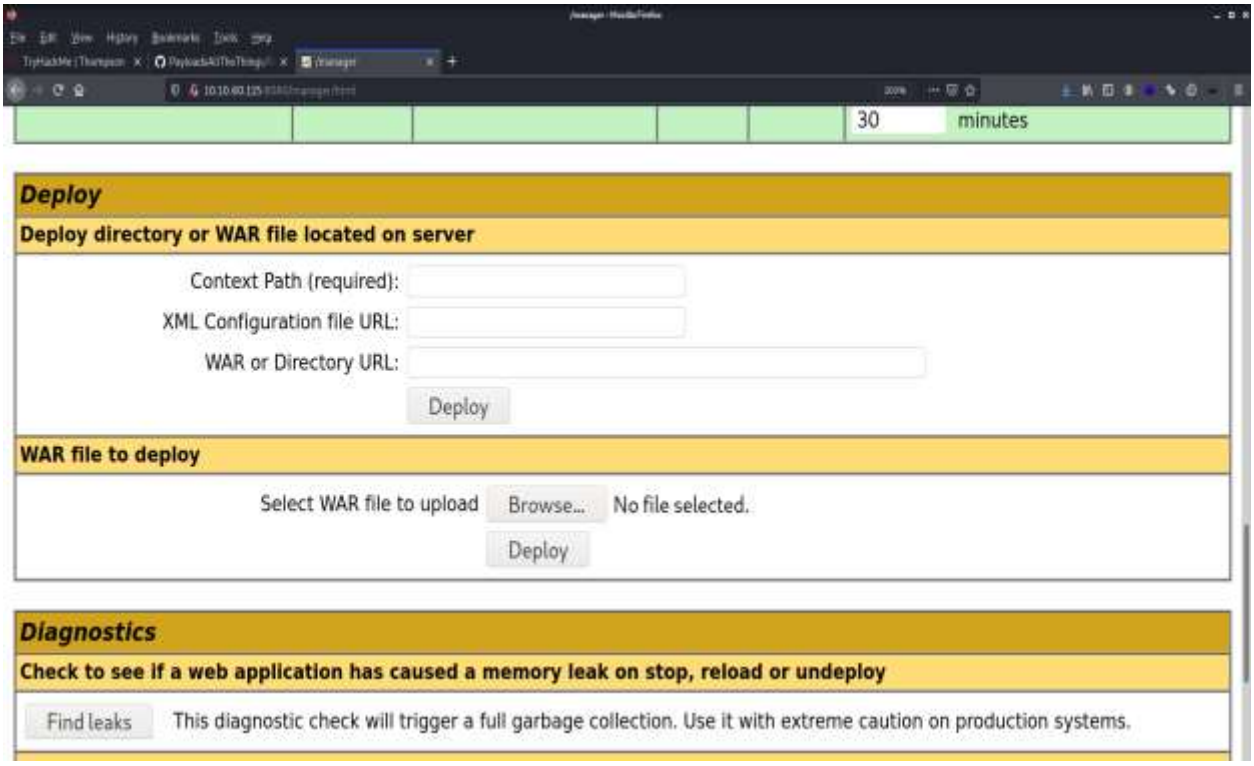
Reconnaissance

I viewed its source code but found nothing. Then I launched **dirbuster** & found an interesting directory.

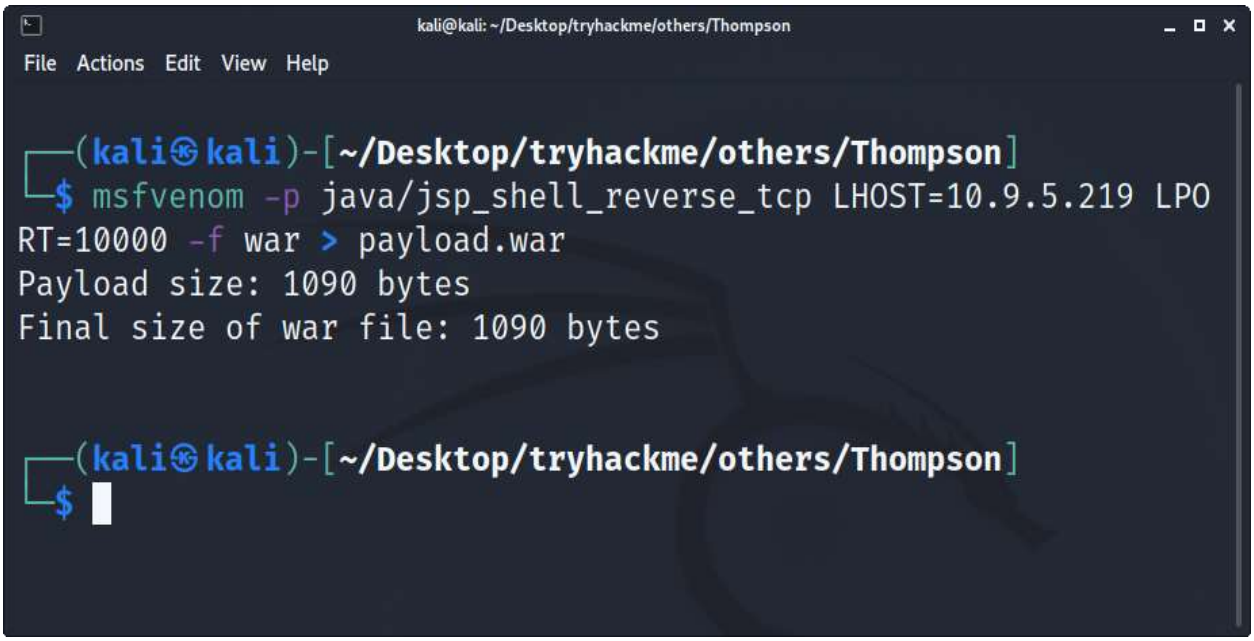


Exploitation

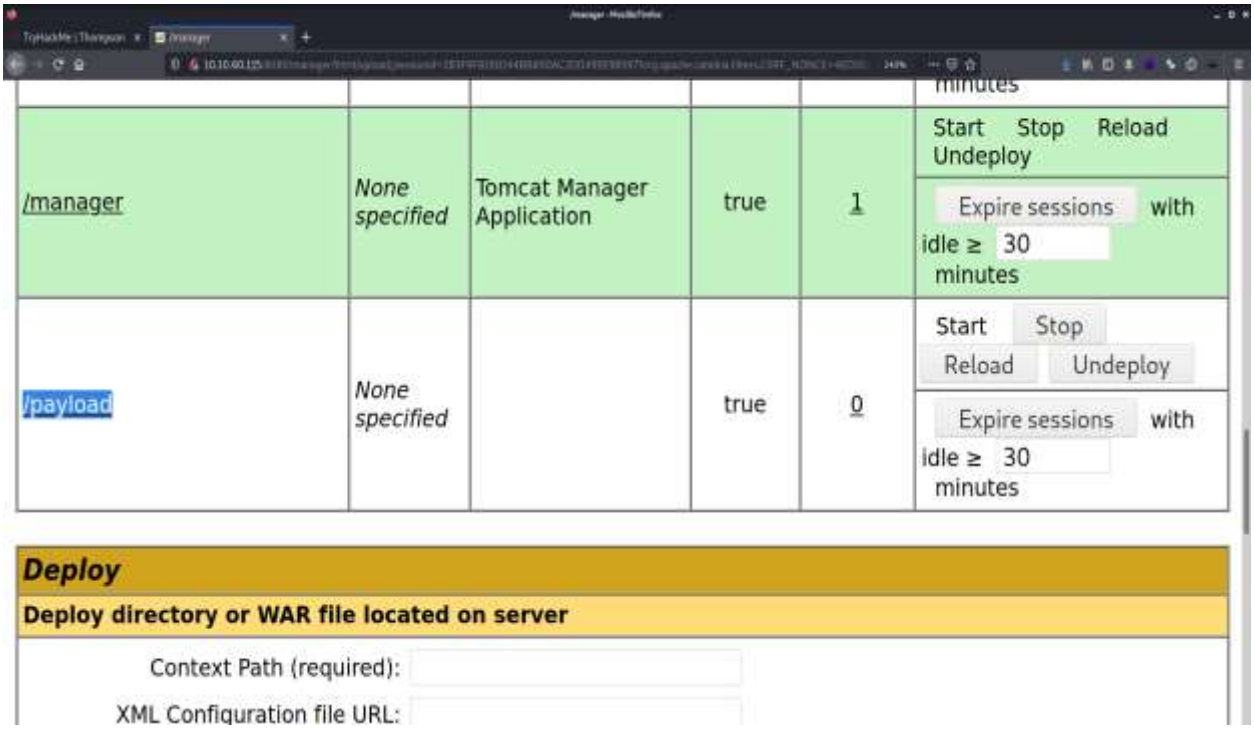
Then I visited **/manager/** directory & there was http basic authentication. So, I searched online for default credentials of Apache tomcat. I found that **tomcat:s3cret** were the default credentials for Apache tomcat.

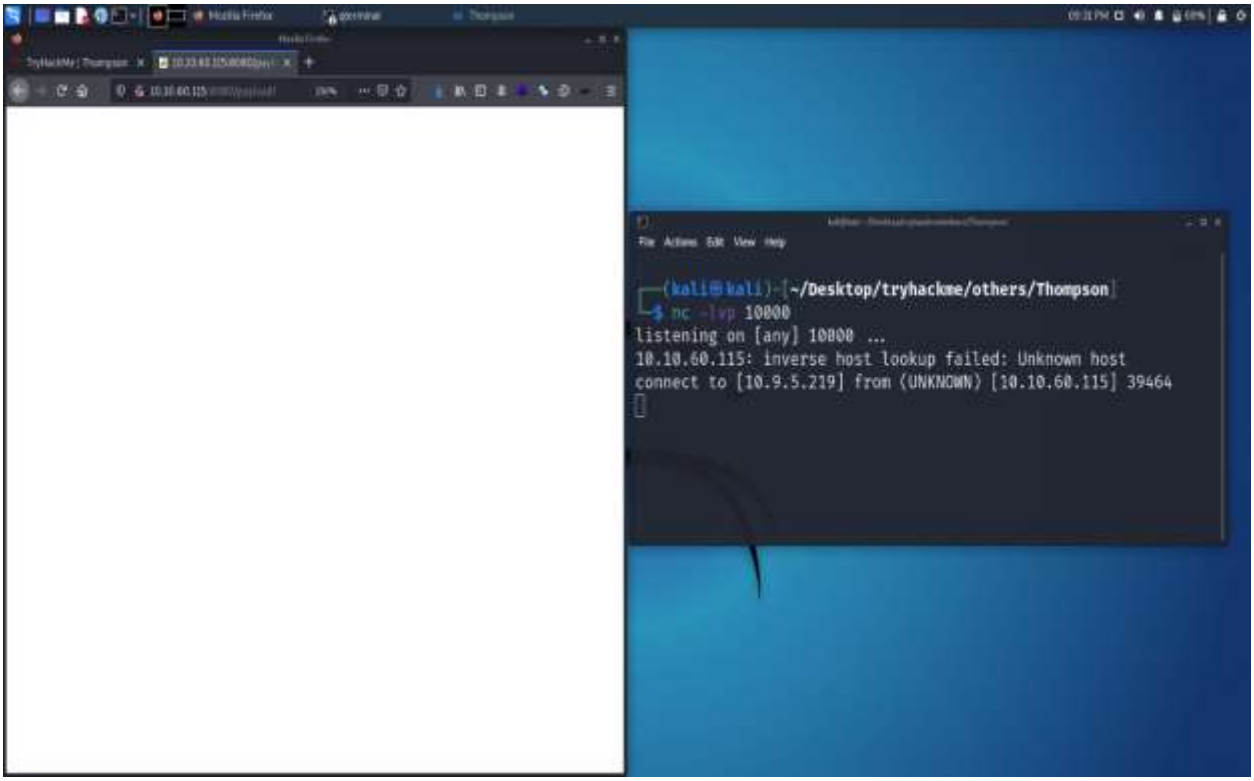


After entering the credentials, I got the access of the dashboard. There I found a file upload functionality which was accepting **.war** files. So, I used **msfvenom** to create a java reverse shell payload.



Then I uploaded the payload and started a **netcat listener** on my machine.



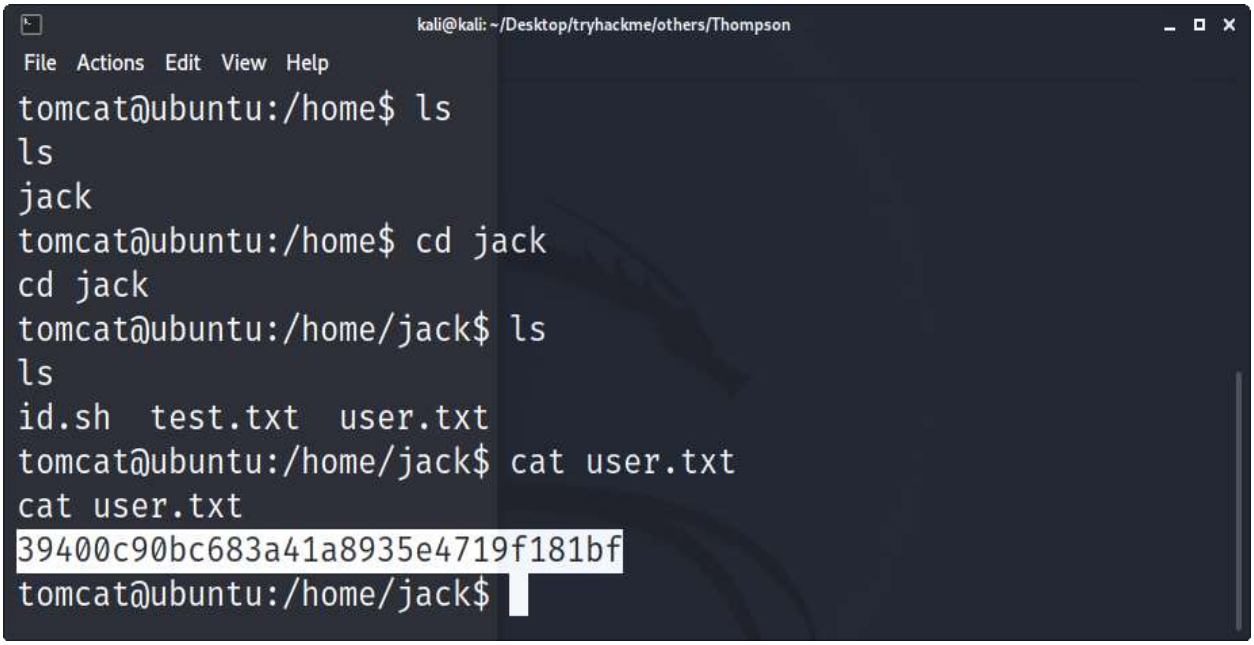


When I clicked the payload, I **got the reverse shell** with **user tomcat**. Then I made the shell interactive with the below commands:

python3 -c 'import pty;pty.spawn("/bin/bash")'

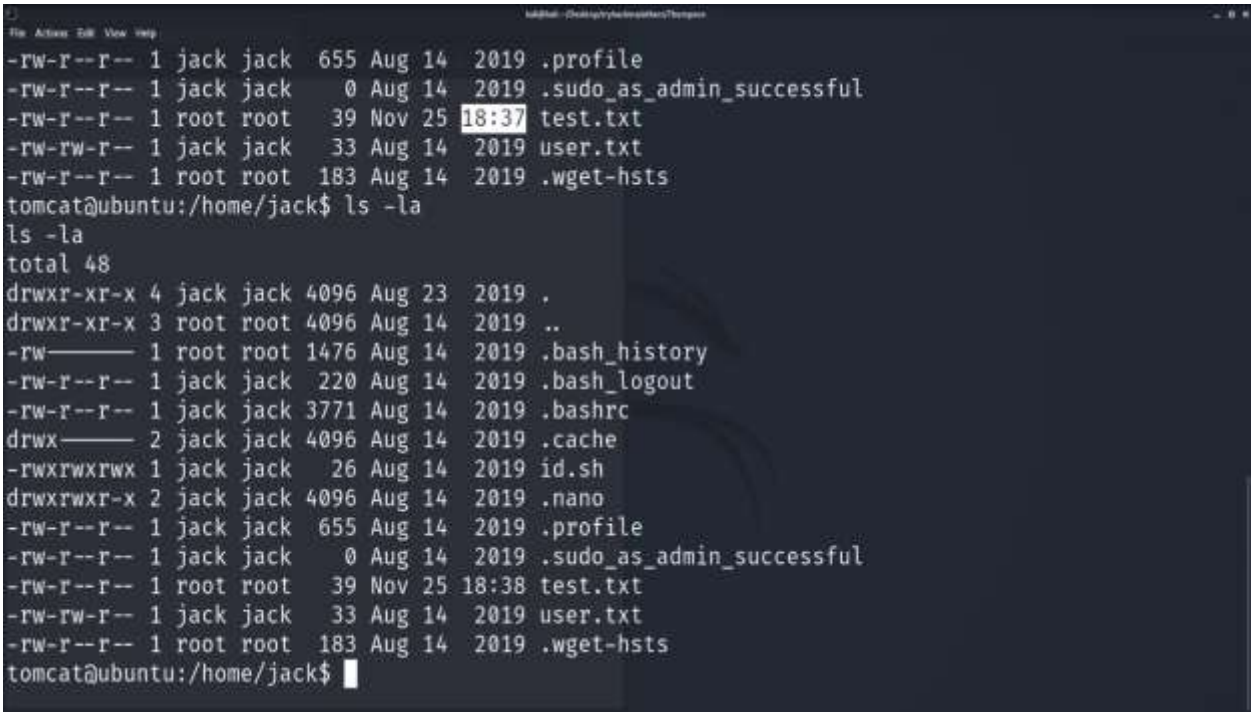
export TERM=xterm

Then, in the **/home/jack/user.txt** file, I **found the user flag**.

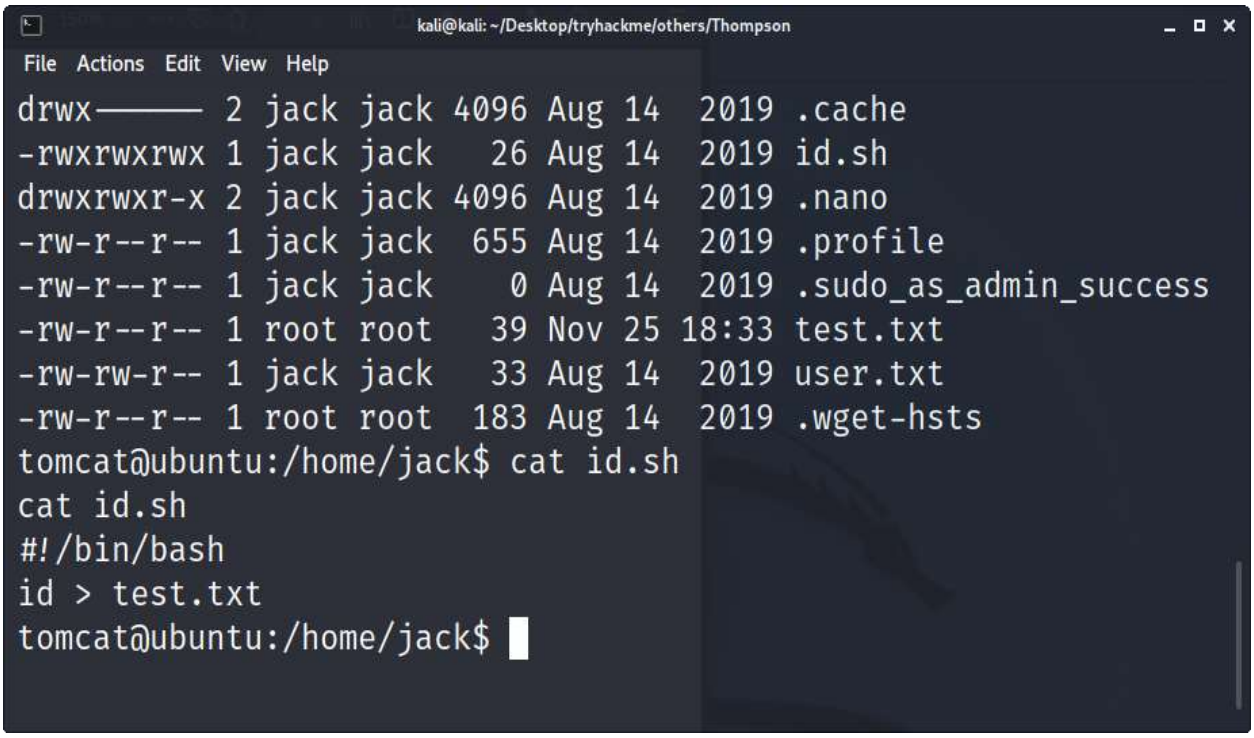


Privilege Escalation

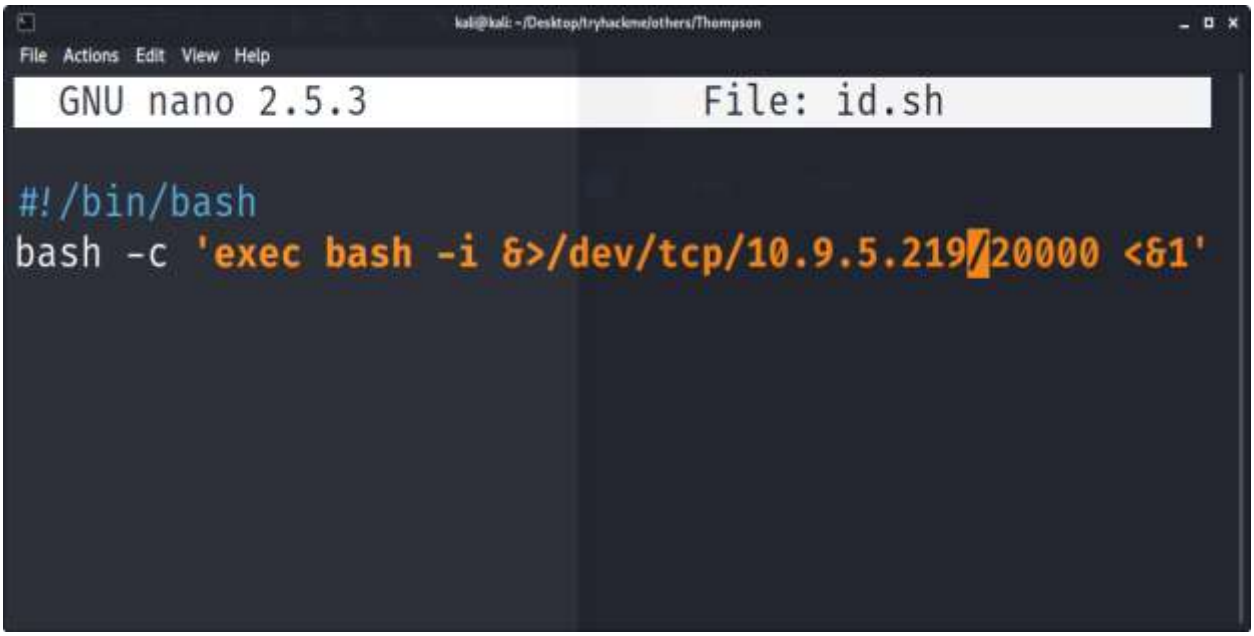
There, I also found a file named **test.txt** which was getting updated every minute.



I found that **id.sh** script was getting executed with root permissions & updating this file every minute & I **had read, write & execution permissions** for id.sh script file.



Then I stored a bash reverse shell in the file id.sh and started a netcat listener on my machine on port 20000.



Then after a minute, I got the reverse shell **with root permissions**. Then in the **/root/root.txt** file, I **found the root flag**.