tryHackMe

Silver Platter

Prepared by: Sondos Farrah

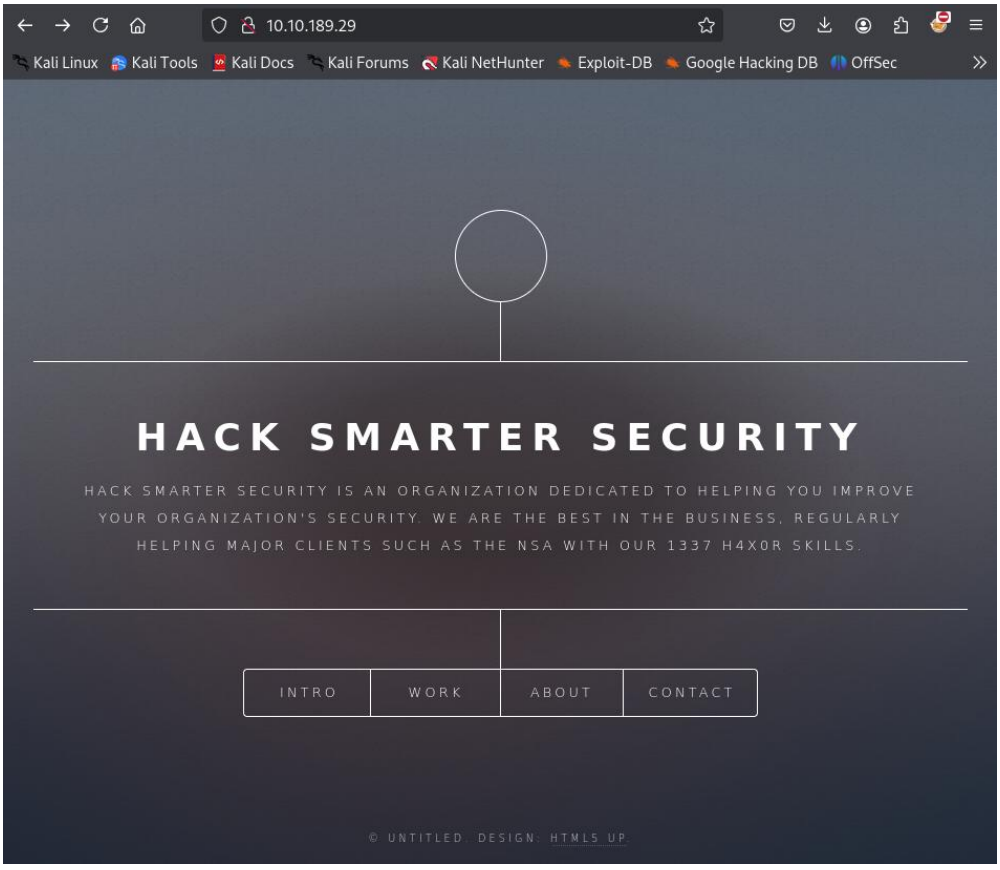
Date: March 7, 2025

Nmap Scan

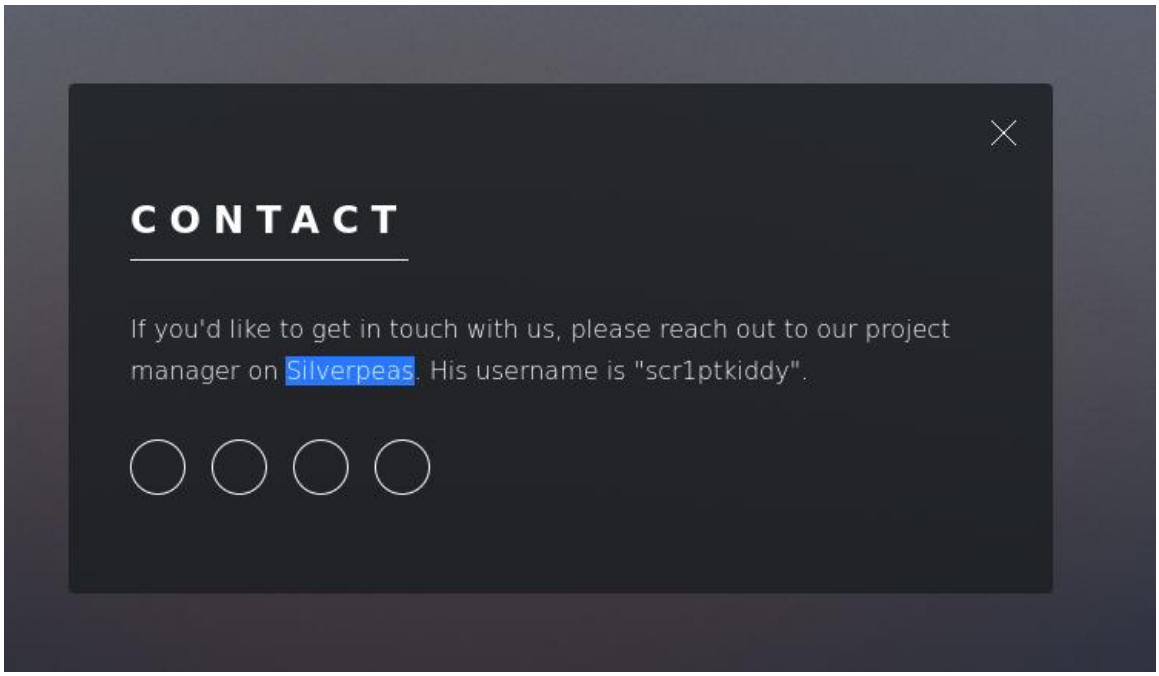
```
┌──(sondos㉿kali)-[~/Desktop/tryHackMe]
└─$ nmap -T4 10.10.189.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-07 06:19 CST
Nmap scan report for 10.10.189.29
Host is up (0.086s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
```

Not much information, but still some useful stuff. knowing that it has 2 HTTP services listening on ports 80 and 8080.

Port 80

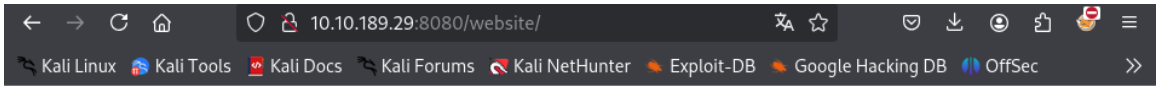


While clicking on the different tabs, we come across some useful information in the “contact” tab:



The contact tab leaks a potential username, as well as the name of some app called “Silverpeas”.

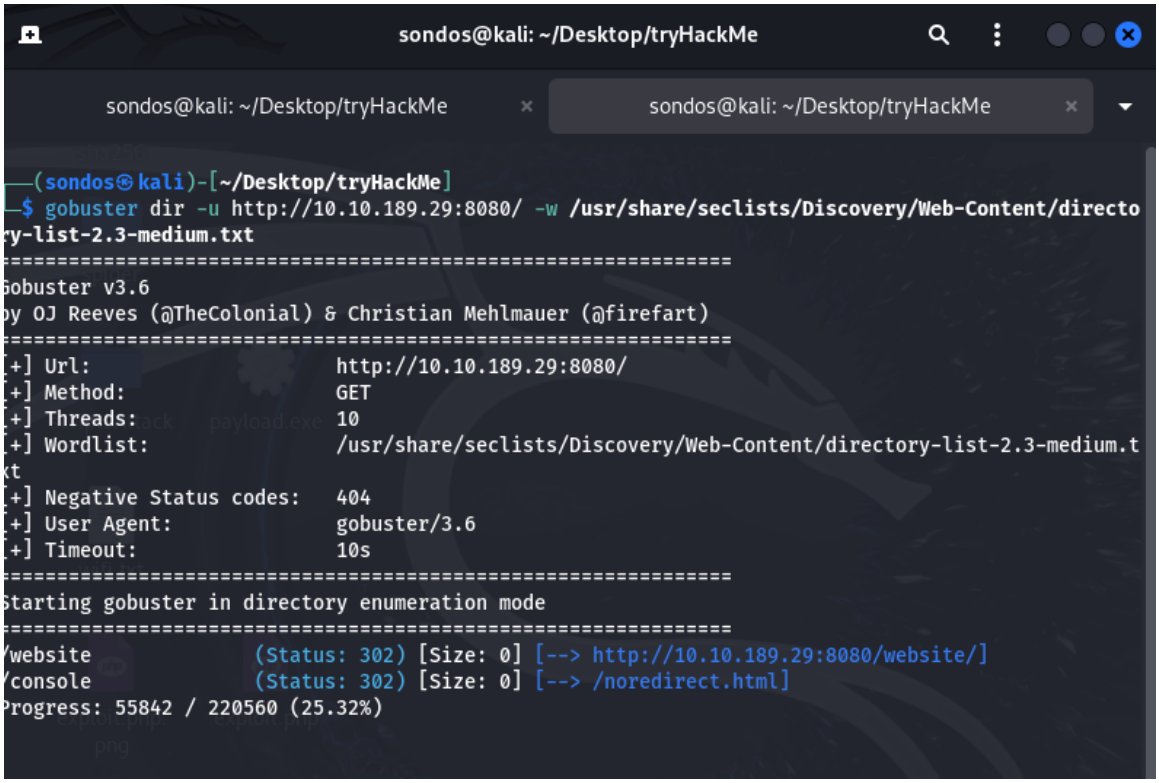
Port 8080



Forbidden

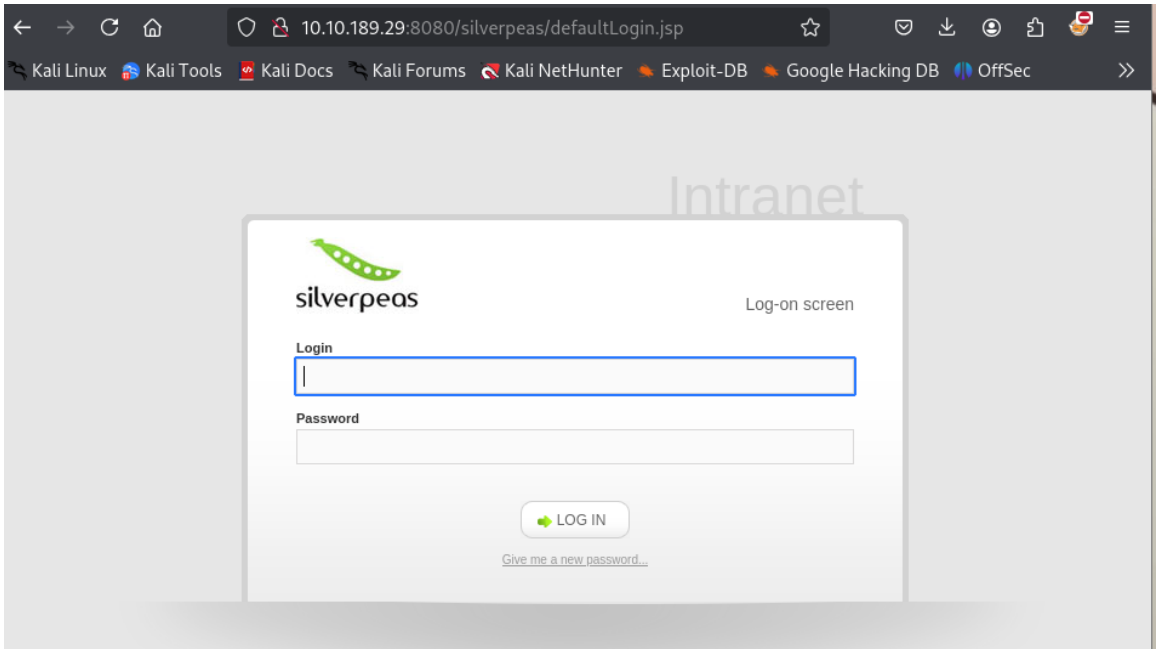
Unfortunately, we get a 404 not found error when we visit port 8080.

Not much we can do here, so we should look for more content with gobuster:



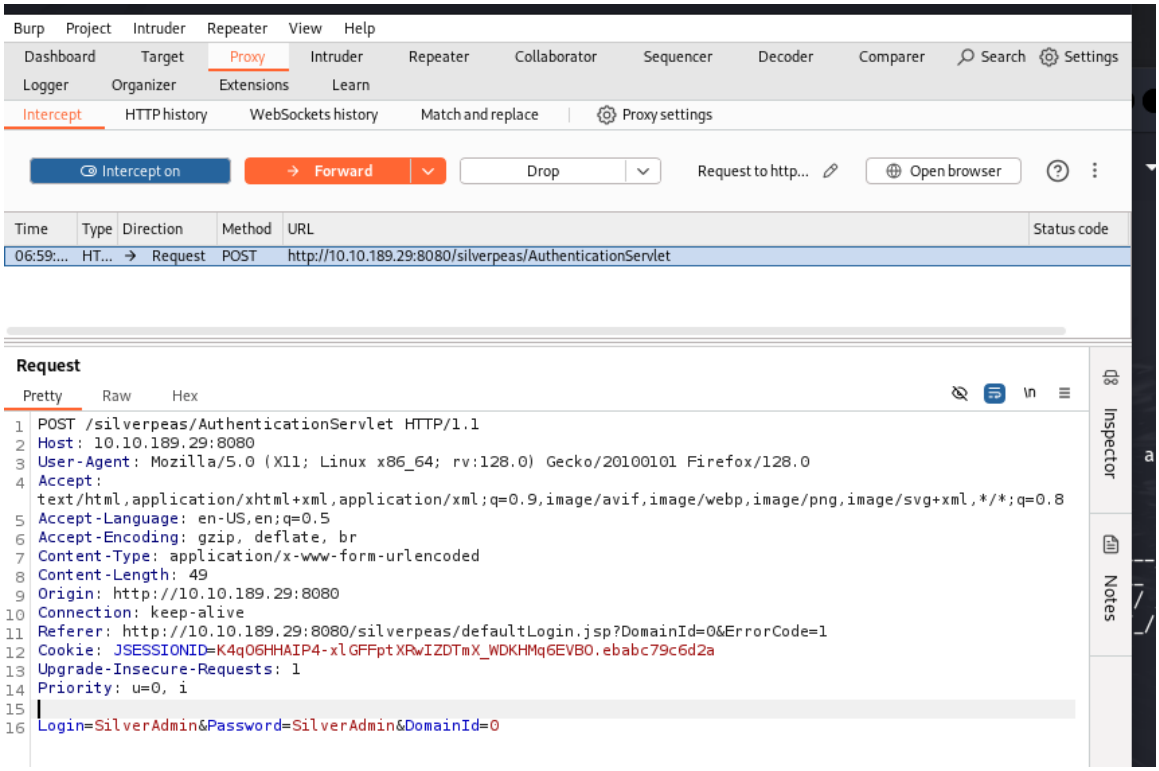
Two interesting endpoints are encountered, but upon further research, it is discovered that they are both likely dead ends. The /website endpoint returns a “Forbidden” error, and the /console endpoint redirects to a 404 page.

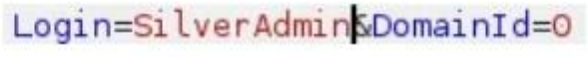
However, it should be recalled that the message on the contact tab earlier mentioned “Silverpeas”. What if the directory that is needed is /silverpeas? On port 80, nothing is found. However, on port 8080...

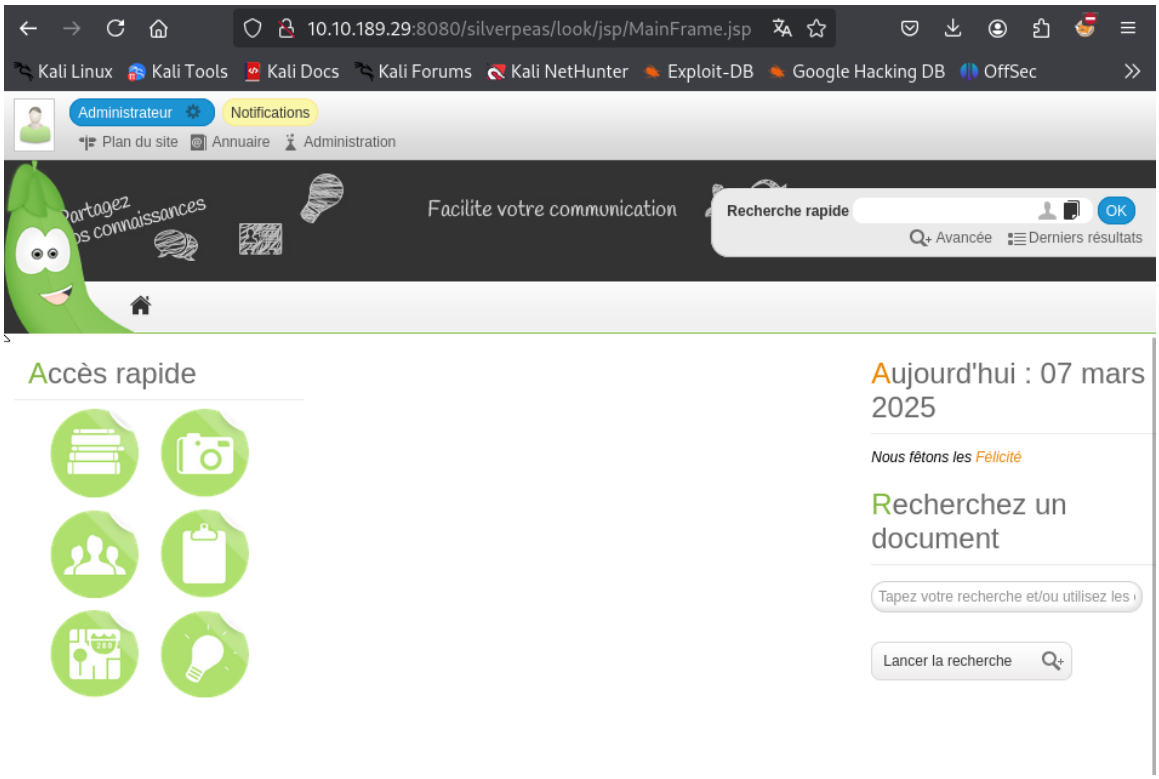


So now searching for “SilverPeas CVEs” on google:

Upon reviewing the details, it appears that the login request must be captured in BurpSuite, with the password field removed from the request.





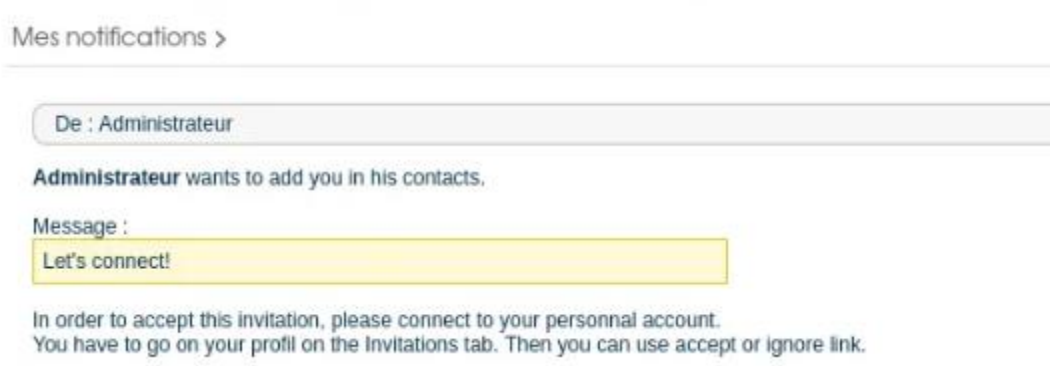


The admin panel is now logged into, but nothing is understood from this language, so Google is searched, and this is found to try:

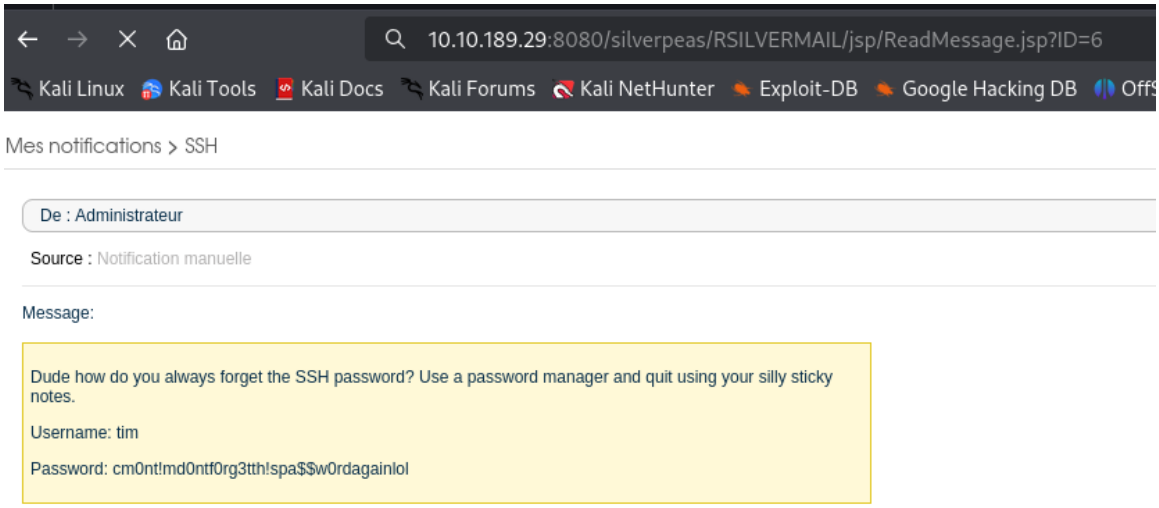
4. CVE-2023-47323: Broken Access Control Allows Attacker to Read All Messages

Lets try:

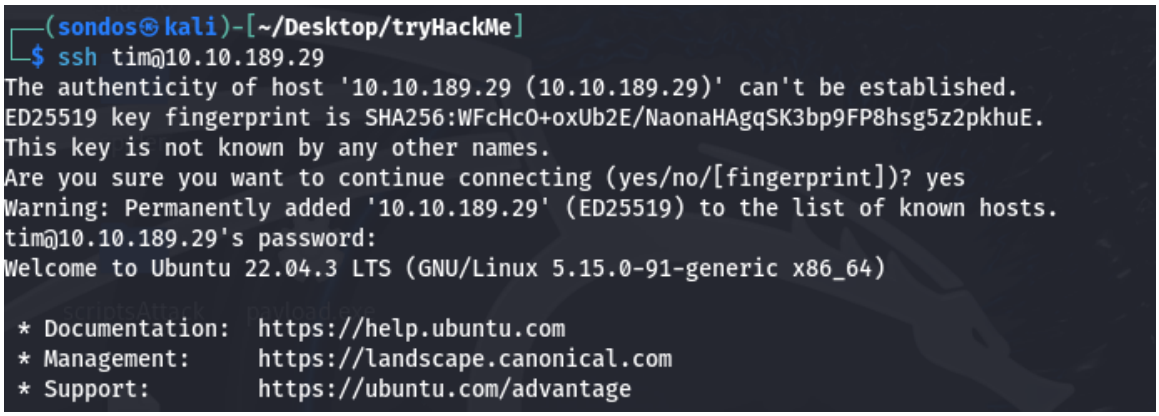
http://10.10.189.29:8080/silverpeas/RSILVERMAIL/jsp/ReadMessage.jsp?ID=1

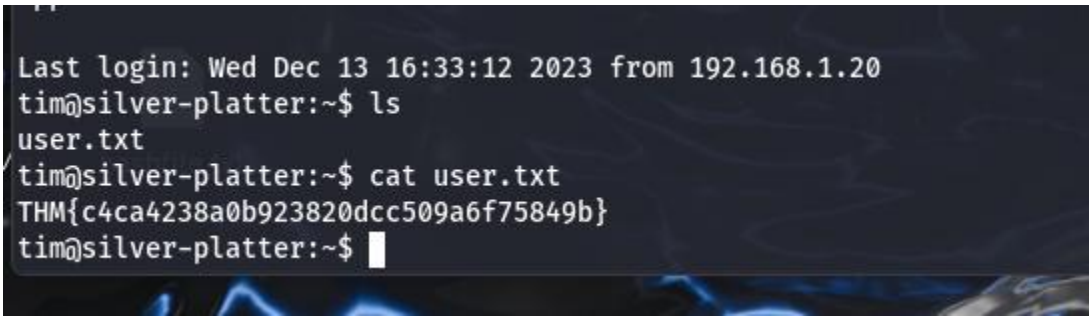


It seems that this works. We can continue to browse through the messages until an interesting one is found.



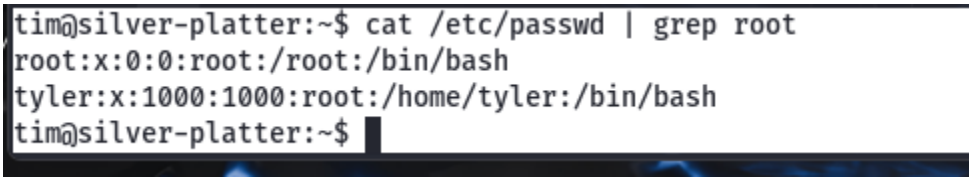
Logging as tim via ssh





User flag is found!!

Now searching for root one:

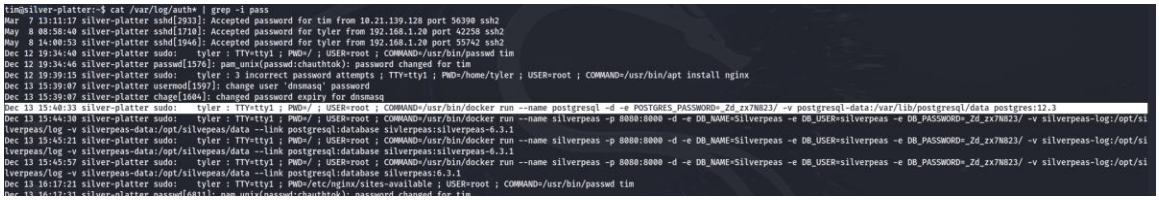


/etc/passwd tells us that there is also a user called “tyler”, as well as the root user of course.

```
tim@silver-platter:~$ id
uid=1001(tim) gid=1001(tim) groups=1001(tim),4(adm)
```

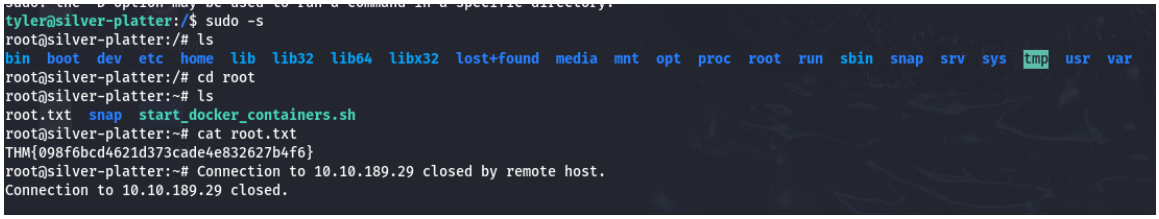
It can be seen that Tim is part of the “adm” group. This gives Tim read access to the log files on the system.

cat /var/log/auth* | grep -i pass



There is a password found

This password usefull fro Tylor to get root the system



And that’s it, root flag found!!