# Silver Platter (TryHackMe-Easy)

-Link: https://tryhackme.com/room/silverplatter

## I. Information Gathering and Vulnerabilitiy Assessment.

-Vẫn như thường lệ, ta sử dụng `nmap` để kiểm tra các cổng đang mơ:

```
sudo nmap IP_Address -Pn --disable-arp-ping -n -oN first1000.nmap -oX first1000.xml -vv -sC -sV
```

-Kết quả:

```
# Nmap 7.95 scan initiated Sat Jun 21 03:15:54 2025 as: /usr/lib/nmap/nmap -Pn --disable-arp-ping -n -oN first1000.nmap -oX first1000.xml -vv -sC -sV 10.10.205.127
Increasing send delay for 10.10.205.127 from 0 to 5 due to 214 out of 711 dropped probes since last increase.
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.1 \d\d\d (?:[^\r\n]*\r\n(?!\r\n))*?.*\r\nServer: Virata-EmWeb/R([\d_]+)\r\nContent-Type: text/html; ?charset=UTF-8\r\nExpires: .*<title>HP (Color |)LaserJet ([\w._ -]+)   '
Nmap scan report for 10.10.205.127
Host is up, received user-set (0.21s latency).
Scanned at 2025-06-21 03:15:56 EDT for 113s
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
```

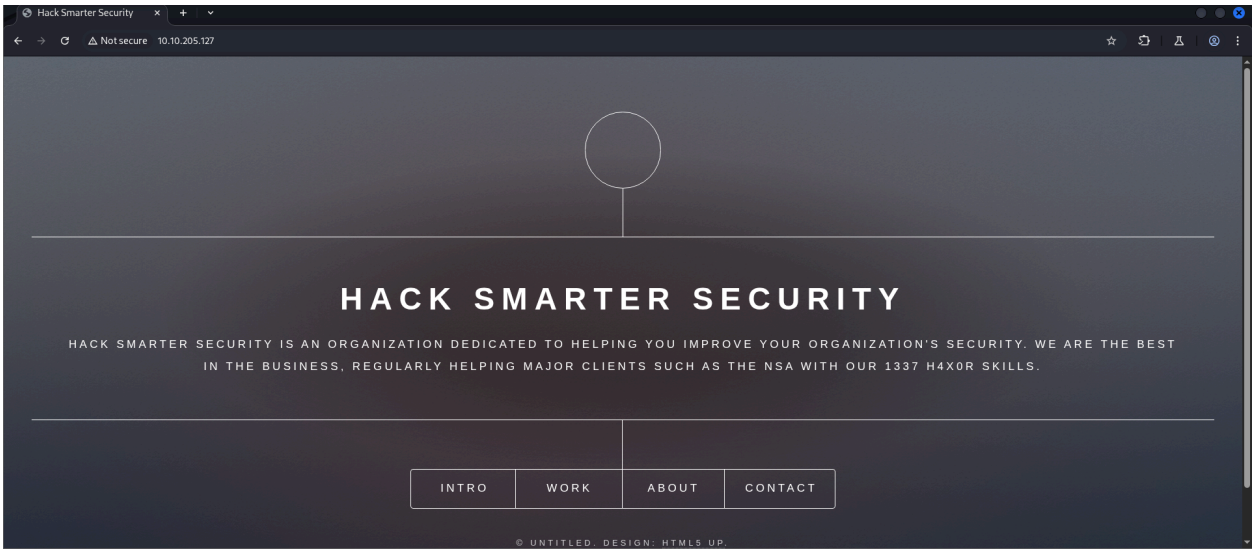
```
|   256 1b:1c:87:8a:fe:34:16:c9:f7:82:37:2b:10:8f:8b:f1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdH
AyNTYAAABBBJ0ia1tcuNvK0lfuy3Ep2dsElFfxouO3VghX5Rltu77M33pFvTeCn
9t5A8NReq3felAqPi+p+/0eRRfYuaeHRT4=
|   256 26:6d:17:ed:83:9e:4f:2d:f6:cd:53:17:c8:80:3d:09 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKecigNtiy6tW5ojXM3xQkbtTO
wK+vqvMoJZnIxVowju
80/tcp   open  http       syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Hack Smarter Security
8080/tcp open  http-proxy syn-ack ttl 62
|_http-title: Error
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 74
|     Content-Type: text/html
|     Date: Sat, 21 Jun 2025 07:16:19 GMT
|     <html><head><title>Error</title></head><body>404 - Not Found</body
></html>
|   GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, S
MBProgNeg, SSLSessionReq, Socks5, TLSSessionReq, TerminalServerCooki
e:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 74
|     Content-Type: text/html
|     Date: Sat, 21 Jun 2025 07:16:17 GMT
|     <html><head><title>Error</title></head><body>404 - Not Found</body
```

```
></html>
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Connection: close
|     Content-Length: 74
|     Content-Type: text/html
|     Date: Sat, 21 Jun 2025 07:16:18 GMT
|_    <html><head><title>Error</title></head><body>404 - Not Found</body
></html>
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.c
gi?new-service :
SF-Port8080-TCP:V=7.95%I=7%D=6/21%Time=68565C42%P=x86_64-pc-lin
ux-gnu%r(Ge
SF:tRequest,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20clos
e\r
SF:\nContent-Length:\x2074\r\nContent-Type:\x20text/html\r\nDate:\x20Sat,\
SF:x2021\x20Jun\x202025\x2007:16:17\x20GMT\r\n\r\n<html><head><title>
Error
SF:</title></head><body>404\x20-\x20Not\x20Found</body></html>")%r
(HTTPOpt
SF:ions,C9,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20close\r\n
Co
SF:ntent-Length:\x2074\r\nContent-Type:\x20text/html\r\nDate:\x20Sat,\x202
SF:1\x20Jun\x202025\x2007:16:18\x20GMT\r\n\r\n<html><head><title>Error
</ti
SF:tle></head><body>404\x20-\x20Not\x20Found</body></html>")%r(RTS
PRequest
SF:,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nC
onn
SF:ection:\x20close\r\n\r\n")%r(FourOhFourRequest,C9,"HTTP/1\.1\x20404\x2
0
SF:Not\x20Found\r\nConnection:\x20close\r\nContent-Length:\x2074\r\nCont
en
SF:t-Type:\x20text/html\r\nDate:\x20Sat,\x2021\x20Jun\x202025\x2007:16:19
\
```

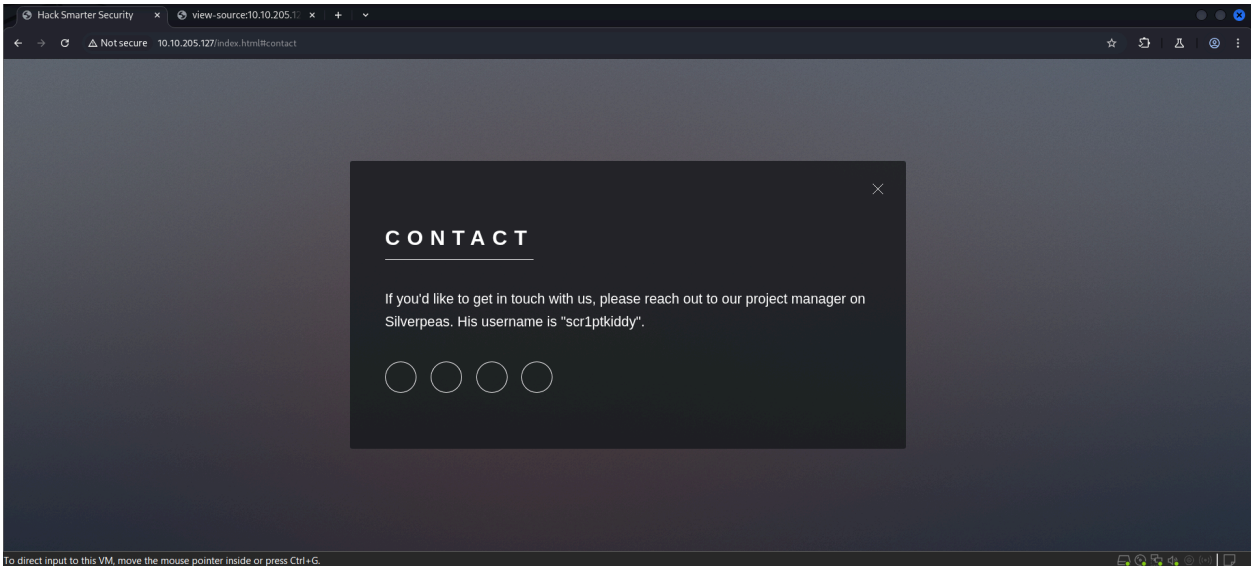
```
SF:x20GMT\r\n\r\n<html><head><title>Error</title></head><body>404\x20-
\x20
SF:Not\x20Found</body></html>")%r(Socks5,42,"HTTP/1\.1\x20400\x20Bad
\x20Re
SF:quest\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Gene
r
SF:icLines,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x20
0\
SF:r\nConnection:\x20close\r\n\r\n")%r(Help,42,"HTTP/1\.1\x20400\x20Bad\x
2
SF:0Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(S
S
SF:LSessionReq,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Lengt
h:\x
SF:200\r\nConnection:\x20close\r\n\r\n")%r(TerminalServerCookie,42,"HTTP/
1
SF:\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x
20
SF:close\r\n\r\n")%r(TLSSessionReq,42,"HTTP/1\.1\x20400\x20Bad\x20Requ
est\
SF:r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(Kerberos,42
SF:,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConn
ect
SF:ion:\x20close\r\n\r\n")%r(SMBProgNeg,42,"HTTP/1\.1\x20400\x20Bad\x20
Req
SF:uest\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r\n")%r(LPDStr
SF:ing,42,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r
\nC
SF:onnection:\x20close\r\n\r\n")%r(LDAPSearchReq,42,"HTTP/1\.1\x20400\x2
0B
SF:ad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\n\r
\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nm
```

```
ap.org/submit/ .
# Nmap done at Sat Jun 21 03:17:49 2025 -- 1 IP address (1 host up) scanned i
n 115.10 seconds
```

-Ta biết được là đang có 1 trang web, 1 proxy và 1 dịch vụ `ssh` đang mở, đưa nhiên là ta sẽ truy cập thử trang web trước.

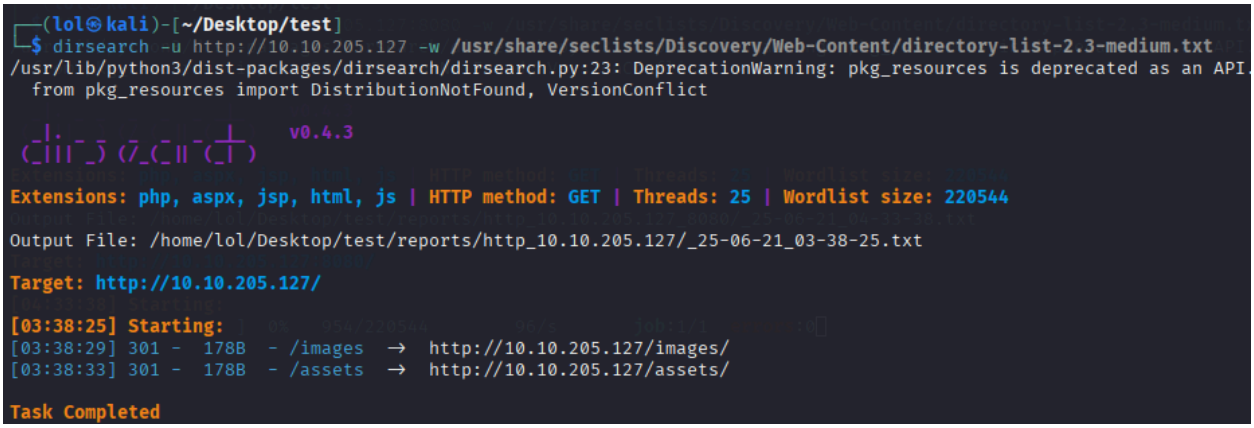



-Ta thử truy cập vào trang robots.txt, sitemap.xml như lại không tồn tại 2 trang này, sau 1 hồi lướt thì ta thấy được tên người dùng của ai đó.

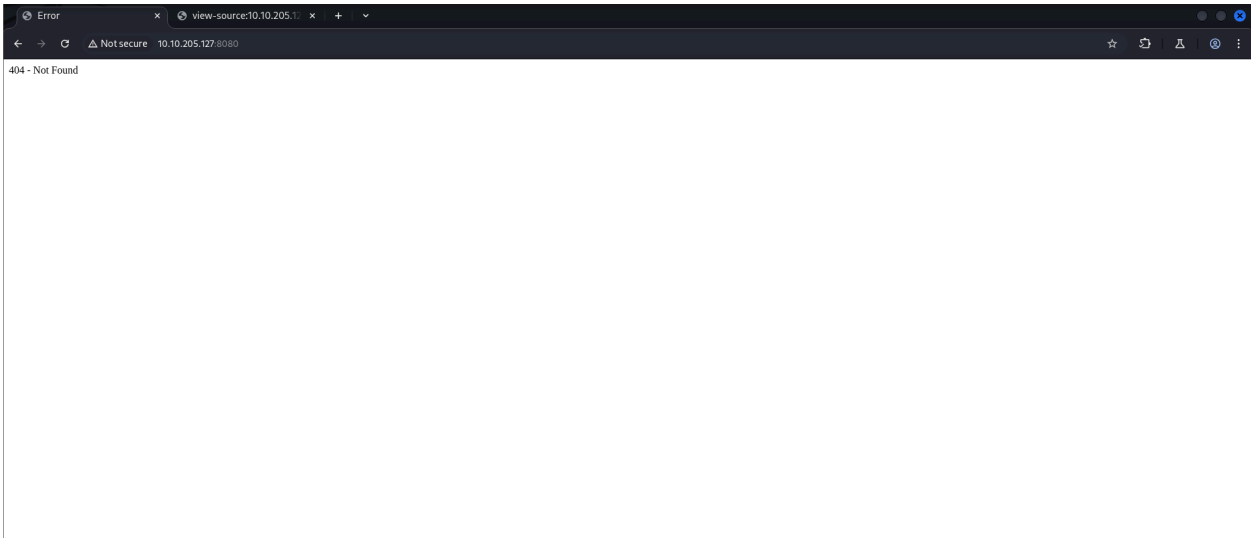


-Ngoài ra thì có vẻ không còn gì đặc biệt lắm, ta thử brute thư mục của trang web, nhưng có vẻ không có gì nhiều.

```
dirsearch -u http://IP_Address -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
```



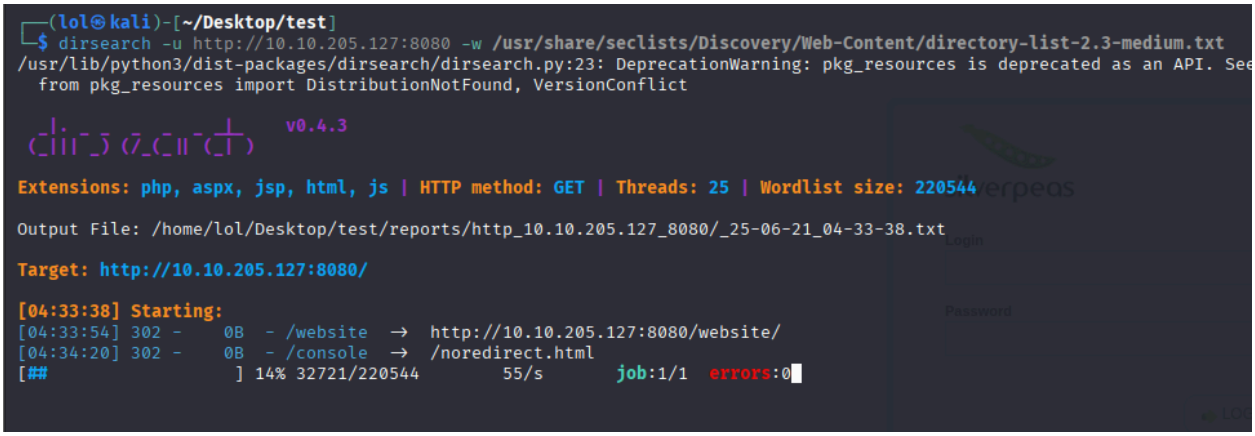

-Có vẻ thực sự không có gì đặc biệt tại cổng 80, ta chuyển sang cổng 8080.



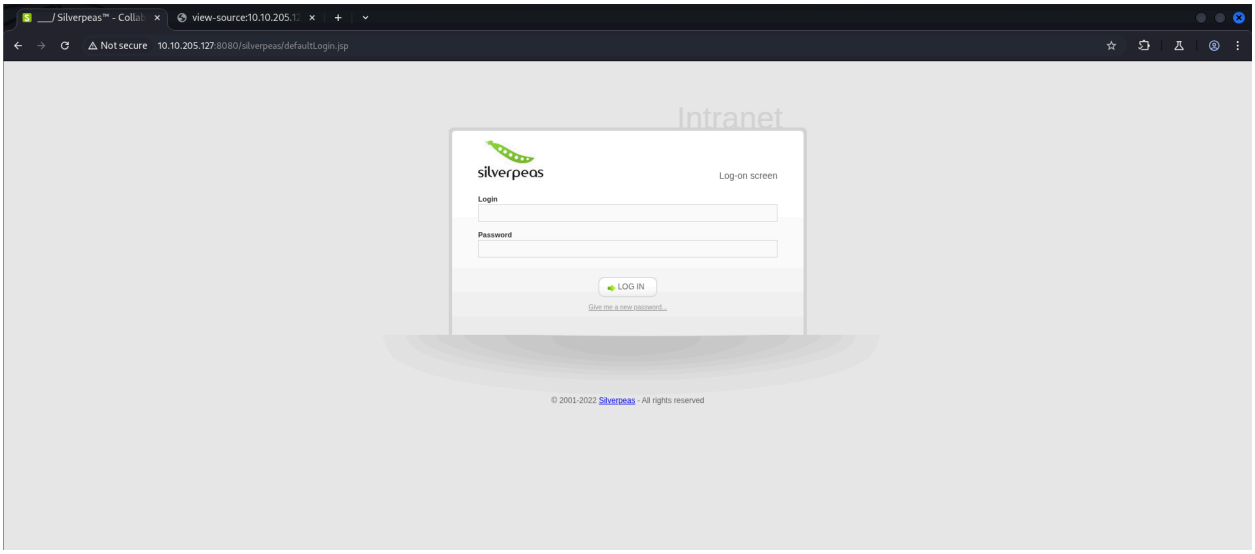

-Ta lại thử brute thư mục tiếp, nhưng có vẻ không được nhiều

```
dirsearch -u http://IP_Address:8080 -w /usr/share/seclists/Discovery/Web-Co
```

ntent/directory-list-2.3-medium.txt



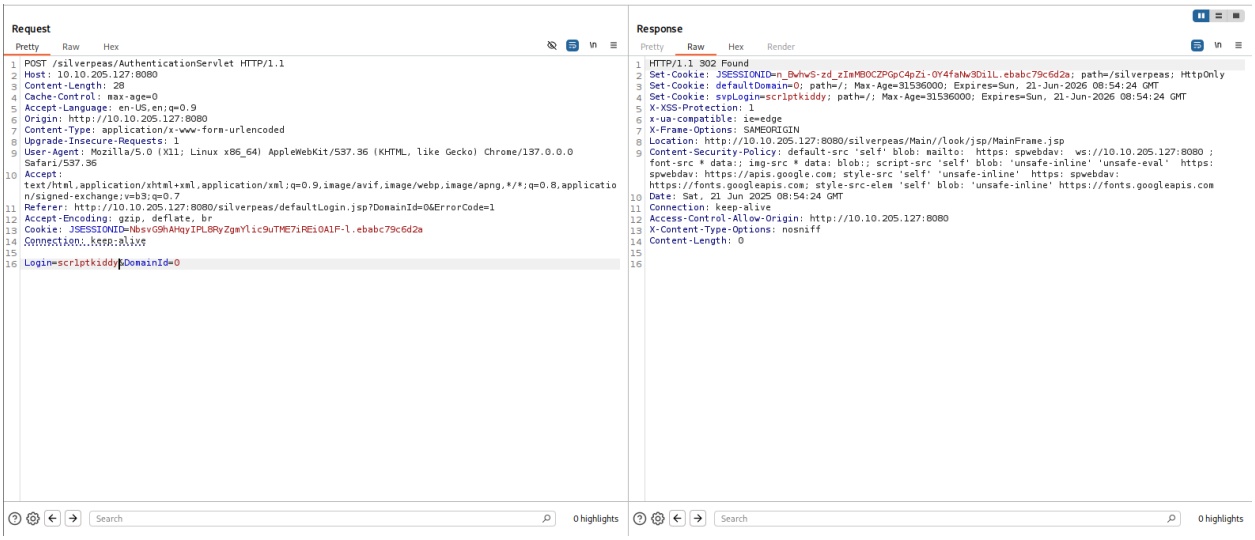

-Ta chuyển sang tra lỗ hổng `nginx 1.18.0`, nhưng cũng ko tìm được lỗ hổng nào có thể gây ra rce, ta thực sự hết cách. Nhưng khi nhớ lại thì ta nhớ lại tại nơi mà ta tìm được tên đăng nhập của ai đó, nó có nhắc tới việc truy cập vào “silverpeas”, có thể nó là tên thư mục nào đó, và đúng thật là vậy.

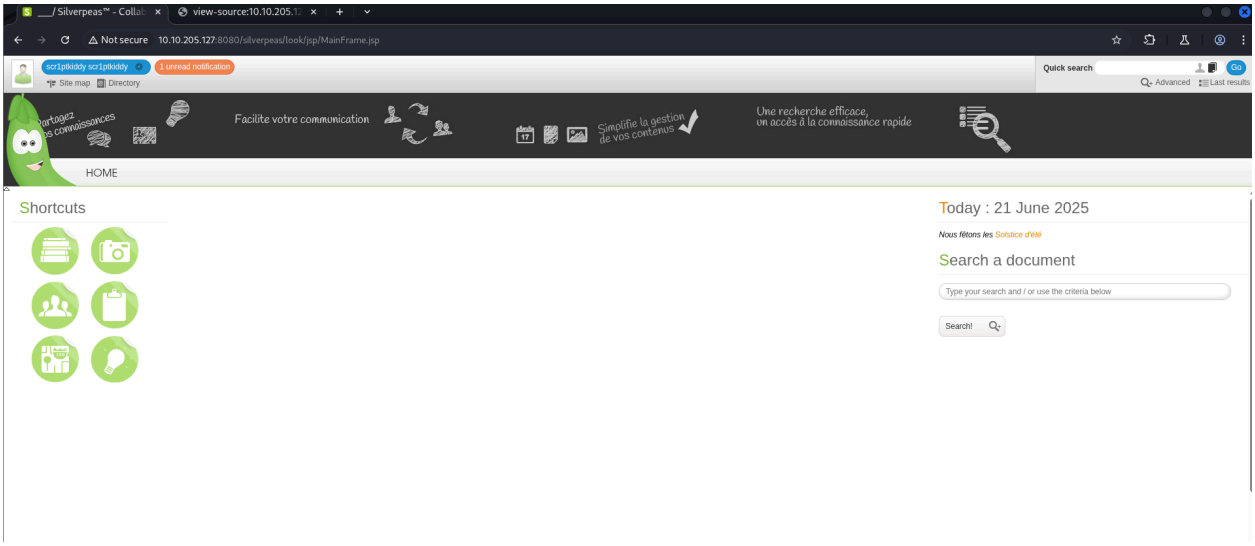



-Ta biết được là có tồn tại tên người dùng `scr1ptkiddy` ở đây , ta cũng biết được là sẽ không tồn tại mật khẩu của người dùng ấy trong `rockyou.txt` (đầu bài cho). Vì vậy ta nên xét các kĩ thuật tấn công khác.

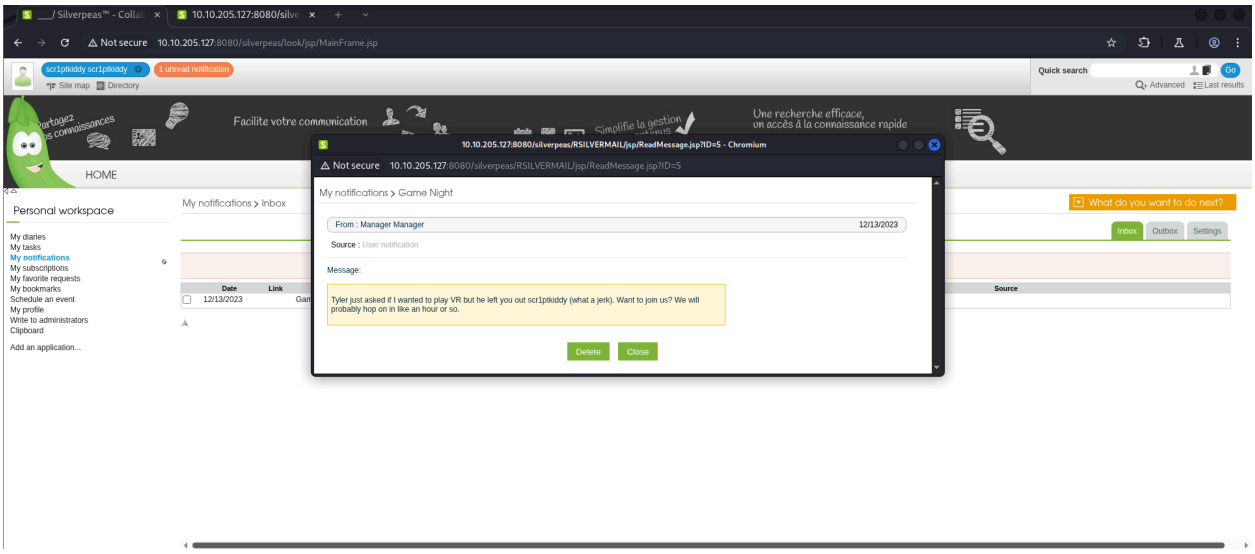
# II. Exploitation.

-Vậy nếu ta xóa tham số `password` đi thì chuyện gì sẽ xảy ra? Kết quả là ta được phép đăng nhập thẳng vào trang mà không cần nhập mật khẩu. Thực chất đây chính là do tồn tại lỗ hổng `CVE-2024-42849` trong `silverpeas`.

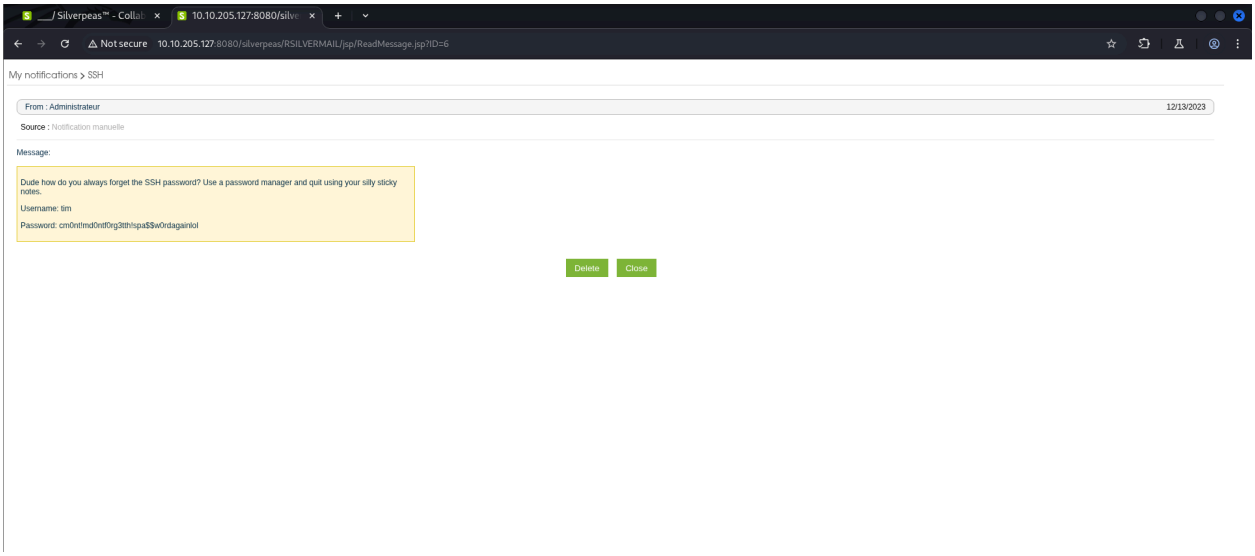



-Tại `unread notifications`, ta thấy được 1 thông báo tới từ `Tyler` nhắn cho `scr1ptkiddy`, ta để ý tại URL thì thấy tham số `ID`, vậy tức là có tồn tại tin nhắn có id khác.




-Ta kiểm tra thì lại phát hiện ra tại `ID=6`, ta thấy 1 thông báo chứa thông tin xác thực của người dùng `tim` qua `ssh`.




-Ta thử dùng nó để đăng nhập qua ssh, và tất nhiên là được.

```
┌──(lol㉿kali)-[~/Desktop/test]
└─$ ssh tim@10.10.205.127
tim@10.10.205.127'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 Sat Jun 21 09:11:01 AM UTC 2025

  System load:  0.0732421875   Processes:             125
  Usage of /:   90.4% of 8.33GB   Users logged in:       0
  Memory usage: 58%            IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%             IPv4 address for ens5:    10.10.205.127

  ⇒ / is using 90.4% 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.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

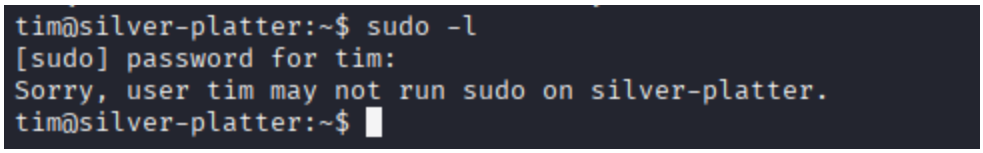
-Tại nhà của người dung này, ta có được cờ đầu tiên trong `user.txt`.

```
Last login: Wed Dec 13 16:33:12 2023 from 192.168.1.20
tim@silver-platter:~$
tim@silver-platter:~$ ls
user.txt
tim@silver-platter:~$ cat user.txt
THM{c4ca4238a0b923820dcc509a6f75849b}
tim@silver-platter:~$
```

⇒ `THM{c4ca4238a0b923820dcc509a6f75849b}`

# III. Pillaging.

-Ta thử sử dụng `sudo -l` để kiểm tra xem `tim` có thể dùng `sudo` không, và có vẻ là không được.



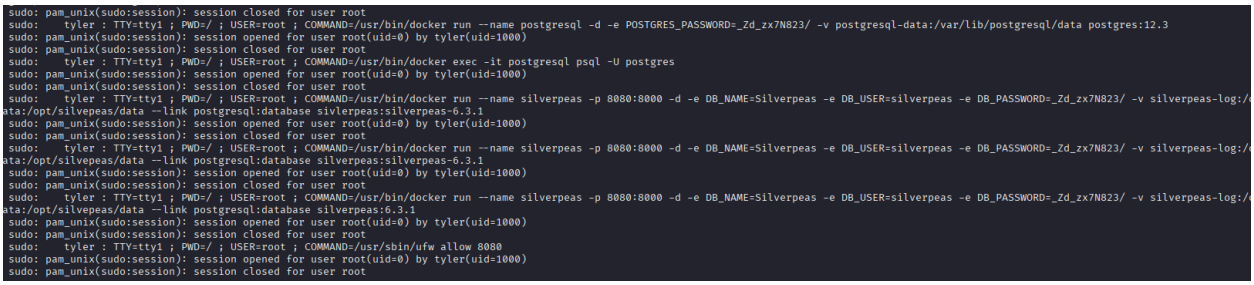

-Ta cũng check các file như `/etc/passwd`, `/etc/crontab`, ... thử `su` để đổi sang các người dùng khác, ... và ta rút ra kết luận sau:

- Có 2 người dùng trong hệ thống này là `tim` và `tyler`
- Ta không thể `su` sang người dùng khác mà không cần nhập mật khẩu
- Không có miền phụ trong máy chủ
- `crontab` chỉ có script `backup` nên không thể dùng để khai thác.
- Người dùng `tim` thuộc nhóm `adm`, nhóm này cho phép ta đọc các `file log` trong máy.

-Ta cũng được biết thì `file log` là 1 trong những loại file có cơ hội cho ta thông tin quan trong nên giờ ta sẽ đọc tất cả những `file log` mà ta có thể động vào được.

```
tim@silver-platter:/home$ find / -type f -group adm 2>/dev/null
/var/log/kern.log
/var/log/syslog.3.gz
/var/log/kern.log.2.gz
/var/log/syslog.2.gz
/var/log/auth.log.1
/var/log/kern.log.1
/var/log/dmesg.4.gz
/var/log/dmesg
/var/log/unattended-upgrades/unattended-upgrades-dpkg.log
/var/log/unattended-upgrades/unattended-upgrades-dpkg.log.1.gz
/var/log/apt/term.log.1.gz
/var/log/apt/term.log
/var/log/dmesg.3.gz
/var/log/syslog.1
/var/log/dmesg.0
/var/log/dmesg.2.gz
/var/log/installer/subiquity-client-info.log.2016
/var/log/installer/subiquity-server-debug.log.2061
/var/log/installer/curtin-install/subiquity-curthooks.conf
/var/log/installer/curtin-install/subiquity-initial.conf
/var/log/installer/curtin-install/subiquity-extract.conf
/var/log/installer/curtin-install/subiquity-partitioning.conf
/var/log/installer/subiquity-server-info.log.2061
/var/log/installer/autoinstall-user-data
/var/log/installer/subiquity-client-debug.log.2016
/var/log/installer/installer-journal.txt
/var/log/installer/cloud-init.log
/var/log/installer/subiquity-curtin-apt.conf
/var/log/nginx/access.log
/var/log/nginx/error.log.1
/var/log/nginx/access.log.2.gz
/var/log/nginx/access.log.1
/var/log/nginx/error.log
/var/log/cloud-init.log
/var/log/dmesg.1.gz
/var/log/syslog
/var/log/auth.log
/var/log/kern.log.3.gz
/var/log/cloud-init-output.log
/var/log/auth.log.2.gz
/var/log/auth.log.2
/etc/cloud/ds-identify.cfg
/etc/cloud/clean.d/99-installer
/etc/cloud/cloud.cfg.d/99-installer.cfg
/etc/hosts
/etc/hostname
tim@silver-platter:/home$
```

-Tại file `/var/log/auth.log.2` , ta tìm thấy được là có thể máy chủ đang chạy `postgresql` thông qua docker.

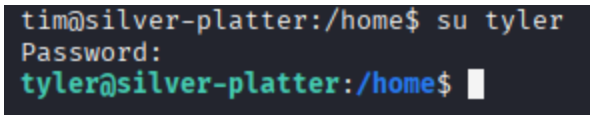



-Từ đây chứng tỏ 1 điều nếu ta có thể truy cập vào cơ sở dữ liệu thông qua thông tin có được từ đây thì ta sẽ có mật khẩu của người dùng `tyler` .

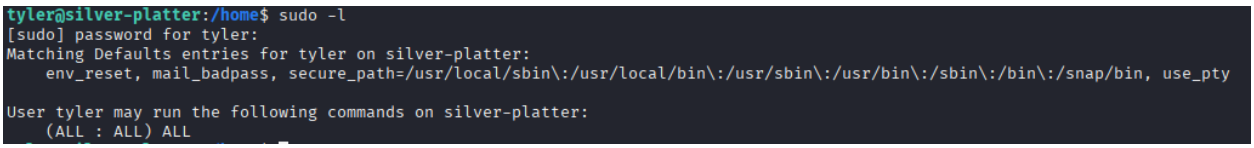
# IV. Post-Exploitation.

-Sau khi loay hoay 1 hồi thì ta còn chẳng thể nào truy cập vào cơ sở dữ liệu do không có bất cứ công cụ nào cho phép ta tương tác với cơ sở dữ liệu tại máy.

-Hoặc là có thể, mật khẩu mà ta có được thông qua `file log` của 1 người dùng khác, vì mật khẩu được đặt khi mà người dùng `tyler` đang truy cập trong máy nên ta thử nó với `tyler` . Và từ mật khẩu đó, ta đã có thể chuyển qua người dùng `tyler` .




-Ta thử dùng `sudo -l` để kiểm tra, và phát hiện ra `tyler` có thể chạy bất cứ câu lệnh nào với quyền của người dùng `root` , đến đây ta chỉ cần liệt kê nội dung có trong file `root.txt` .



```
tyler@silver-platter:/home$ sudo ls -la /root
total 48
drwx------  5 root root 4096 May  1  2024 .
drwxr-xr-x 19 root root 4096 Dec 12  2023 ..
-rw-------  1 root root  287 May  8  2024 .bash_history
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
-rw-------  1 root root   20 Dec 13  2023 .lesshst
drwxr-xr-x  3 root root 4096 Dec 13  2023 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r--r--  1 root root   38 Dec 13  2023 root.txt
-rw-r--r--  1 root root   66 Dec 13  2023 .selected_editor
drwx------  3 root root 4096 Dec 12  2023 snap
drwx------  2 root root 4096 Dec 12  2023 .ssh
-rwxr-xr-x  1 root root   97 Dec 13  2023 start_docker_containers.sh
-rw-r--r--  1 root root    0 Dec 13  2023 .sudo_as_admin_successful
tyler@silver-platter:/home$ sudo cat /root/root.txt
THM{098f6bcd4621d373cade4e832627b4f6}
tyler@silver-platter:/home$
```

⇒ `THM{098f6bcd4621d373cade4e832627b4f6}`