OCLAT

Dificultad : Muy fácil
Probado: VirtualBox 6.x
Objetivo: Obtener la flag de user.txt
Web: Home : - Web CTF de la Comunidad de Hacking Ético
Enlace Descarga:

> Enlace mega
> Enlace gofile

Reconocimiento

> **IP:** ***10.6.8.11***

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxrwxrwx    1 0        0              21 Jan 08  2020 root.txt [NSE:
writeable]
|_-rwxrwxrwx    1 1000     1000           15 Dec 28  2019 user.txt [NSE:
writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.6.8.7
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e6:0e:5d:ec:a3:0f:09:1e:bc:a8:11:8f:f5:b7:02:ae (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCeCUoPXHKqUvT1UVOVTopSYnhd1xx/zu9Q65yJUTKLUA4d
```

```
EEidu5Dzi8ax1CX71p232Zi1J/YUPXVGHZz4xoBVAAK0UqBgAcO2jsCOuP1hctQ+Uzk/+H6Vl5bM
bCf8nb0MuGJP19U6w8hN8Yt2T/rx2Y289JortIOat1649W3SUYTyZ4dhLKc/mEk2CaqSfEp/iE6Y
WoOpSDmP+agsPTNloiX8KT2I4EMSs0yKTX1Rttr3gC6H1E1TySYNKXEu6RVQTstdbh64t1K/cpdD
0mUVGgBKCQSmd0+bSs6iIIt9qlKA67AgOlgsaRjo5rGI7HE2+vYcc+Oe6xH/jIj7kCTl
|   256 bf:cb:b4:ee:b8:91:e8:25:04:00:94:b4:24:34:3f:d1 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCNnxo0RmsOMfLdsDf2B1+lf
udqmQSnXOyhEBaPQx8jZ2zOsoXZDZmA4GypK9GSfJxMY+1kgQr6Q1pgJn82GL6Y=
|   256 57:4a:70:3c:e9:54:2b:61:16:bf:ea:34:c8:52:5b:7b (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAICrF8IKW+T38B1CA9ajGDReGdrKS4aFVEJ1aV3KBOHWT
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Anotaciones

Se observa que la maquina tiene el **puerto 21** abierto con el servicio de **FTP**, versión: **vsftpd 3.0.3** y adicional el **puerto 22** con el servicio **SSH** con la versión: **OpenSSH 7.2p2**

Análisis de vulnerabilidades

> El escaneo con nmap muestra que existe el archivo `root.txt` y `user.txt` en el resultado del puerto 21 FTP
>
> ```
> 21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
> | ftp-anon: Anonymous FTP login allowed (FTP code 230)
> | -rwxrwxrwx    1 0        0              21 Jan 08  2020 root.txt [NSE: writeable]
> |_-rwxrwxrwx    1 1000     1000           15 Dec 28  2019 user.txt [NSE: writeable]
> ```

¿Como descargar archivos por FTP?

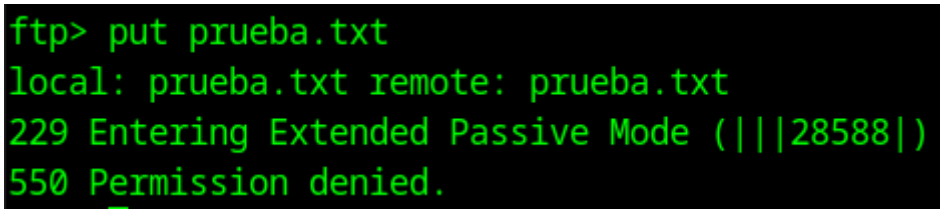
Usando el comando: `get +nombreDeArchivo`

```
ftp> get user.txt
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (|||29428|)
150 Opening BINARY mode data connection for user.txt (15 bytes).
100% |***************************************************************|
226 Transfer complete.
```

Explotación de vulnerabilidades

> Logramos conectarnos por FTP con usuario anonymous y descargar los dos archivos: `root.txt` y `user.txt` correspondiente a las flags del reto.

¿Y si intentamos otra forma de ingreso?

> Como fue muy fácil y rápido el proceso, pues intentemos ver si existe otro vector de ataque, otra forma de ingreso, ¿que podríamos hacer?
>
> Intentemos subir un archivo de texto por FTP.
>
> > Resultado: no tengo permiso para hacerlo
> >
> > 
> >
> >
> > Intentemos enviar el archivo usando `curl` por FTP:
> > `curl -T prueba.txt ftp://10.6.8.11 -u anonymous:anonymous`
> > Resultado: `curl: (25) Failed FTP upload: 550`
>
> Busquemos alguna vulnerabilidad en los servicios:
>
> > `searchsploit vsftpd 3.0.3`
> > `searchsploit OpenSSH 7.2p2`
> > Resultado: pues nada interesante, al parecer denegación de servicio y enumeración de usuario.
>
> ¡Por ahora no encontramos otra forma de acceso!

Escalada de privilegios

> ¡No realizado! para esta maquina, no es necesario.

Bandera(s)

Flag

`User = 4b5b6daa66328696e9e8a4e98c0d65ed`
`Root = df3529cfe9f737801b09dff8b7cb9ef4`

Comandos

Resumen de comandos utilizados

>_ `arp-scan -I enp0s31f6 -l`

>_ `ping -c 1 10.6.8.11`

>_ `nmap -p- --open -sC -sS -sV --min-rate=5000 -n -vvv -Pn 10.6.8.11 -oN scan-oclat`

>_ `ftp 10.6.8.11`

>_ `ftp> get user.txt`

> `cat user.txt`

>_ `ftp> get root.txt`

> `cat root.txt`