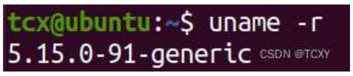
Linux内网渗透-信息收集命令基础篇

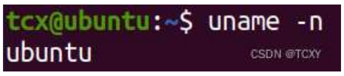
一、获取当前操作系统、设备、内核信息

1.1 获取内核版本信息 uname -r



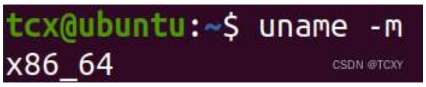
```
tcx@ubuntu:~$ uname -r
5.15.0-91-generic
```

1.2 获取系统主机名 uname -n



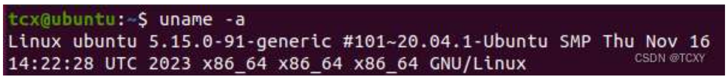
```
tcx@ubuntu:~$ uname -n
ubuntu
```

1.3 获取内核架构 uname -m



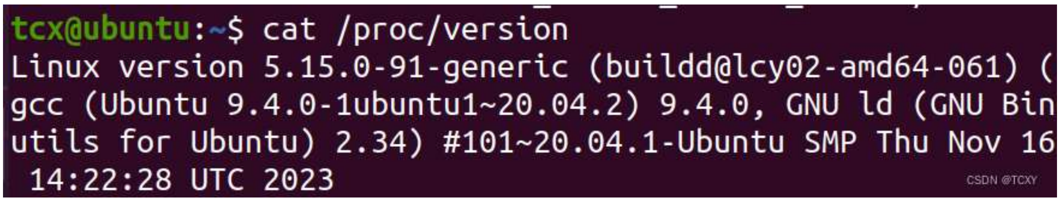
```
tcx@ubuntu:~$ uname -m
x86_64
```

1.4 获取所有版本信息 uname -a



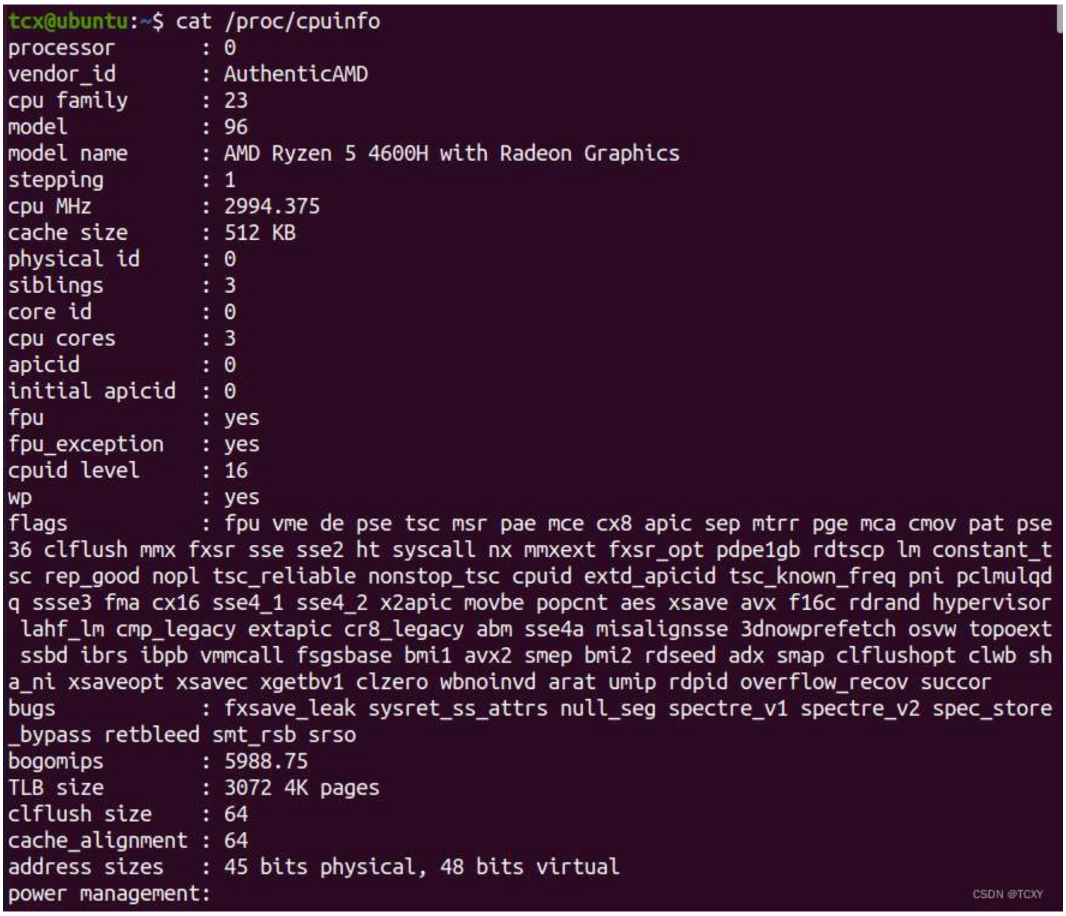
```
tcx@ubuntu:~$ uname -a
Linux ubuntu 5.15.0-91-generic #101~20.04.1-Ubuntu SMP Thu Nov 16
14:22:28 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

1.5 获取内核信息 cat /proc/version



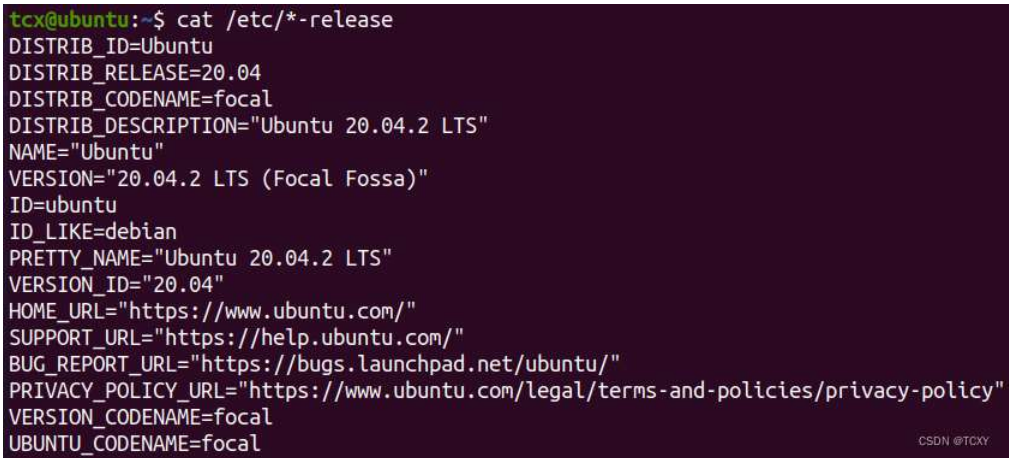
```
tcx@ubuntu:~$ cat /proc/version
Linux version 5.15.0-91-generic (buildd@lcy02-amd64-061) (
gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, GNU ld (GNU Bin
utils for Ubuntu) 2.34) #101~20.04.1-Ubuntu SMP Thu Nov 16
 14:22:28 UTC 2023
```

1.6 获取cpu信息 cat /proc/cpuinfo



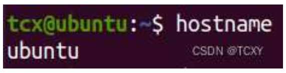
```
tcx@ubuntu:~$ cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 23
model           : 96
model name      : AMD Ryzen 5 4600H with Radeon Graphics
stepping        : 1
cpu MHz         : 2994.375
cache size      : 512 KB
physical id     : 0
siblings        : 3
core id         : 0
cpu cores       : 3
apicid          : 0
initial apicid  : 0
fpu             : yes
fpu_exception   : yes
cpuid level     : 16
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse
36 clflush mmx fxsr sse sse2 ht syscall nx mmxext fxsr_opt pdpe1gb rdtscp lm constant_t
sc rep_good nopl tsc_reliable nonstop_tsc cpuid extd_apicid tsc_known_freq pni pclmulqd
q ssse3 fma cx16 sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16c rdrand hypervisor
 lahf_lm cmp_legacy extapic cr8_legacy abm sse4a misalignsse 3dnowprefetch osvw topoext
 ssbd ibrs ibpb vmmcall fsgsbase bmi1 avx2 smep bmi2 rdseed adx smap clflushopt clwb sh
a_ni xsaveopt xsavec xgetbv1 clzero wbnoinvd arat umip rdpid overflow_recov succor
bugs            : fxsave_leak sysret_ss_attrs null_seg spectre_v1 spectre_v2 spec_store
_bypass retbleed smt_rsb srso
bogomips        : 5988.75
TLB size        : 3072 4K pages
clflush size    : 64
cache_alignment : 64
address sizes   : 45 bits physical, 48 bits virtual
power management:
```

1.7查看当先Linux　发行版本名称和版本号等发布信息 cat /etc/*-release



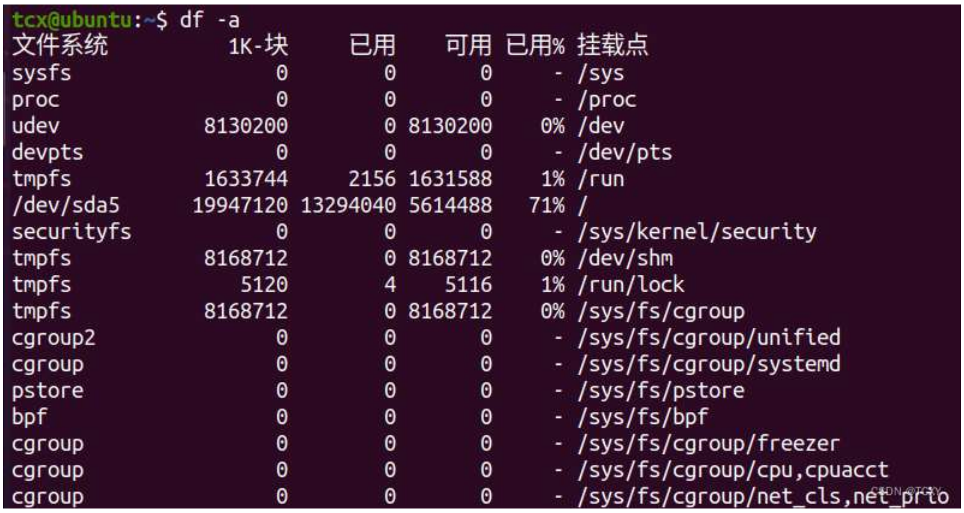
```
tcx@ubuntu:~$ cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=20.04
DISTRIB_CODENAME=focal
DISTRIB_DESCRIPTION="Ubuntu 20.04.2 LTS"
NAME="Ubuntu"
VERSION="20.04.2 LTS (Focal Fossa)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 20.04.2 LTS"
VERSION_ID="20.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=focal
UBUNTU_CODENAME=focal
```

1.8 查看主机名 hostname



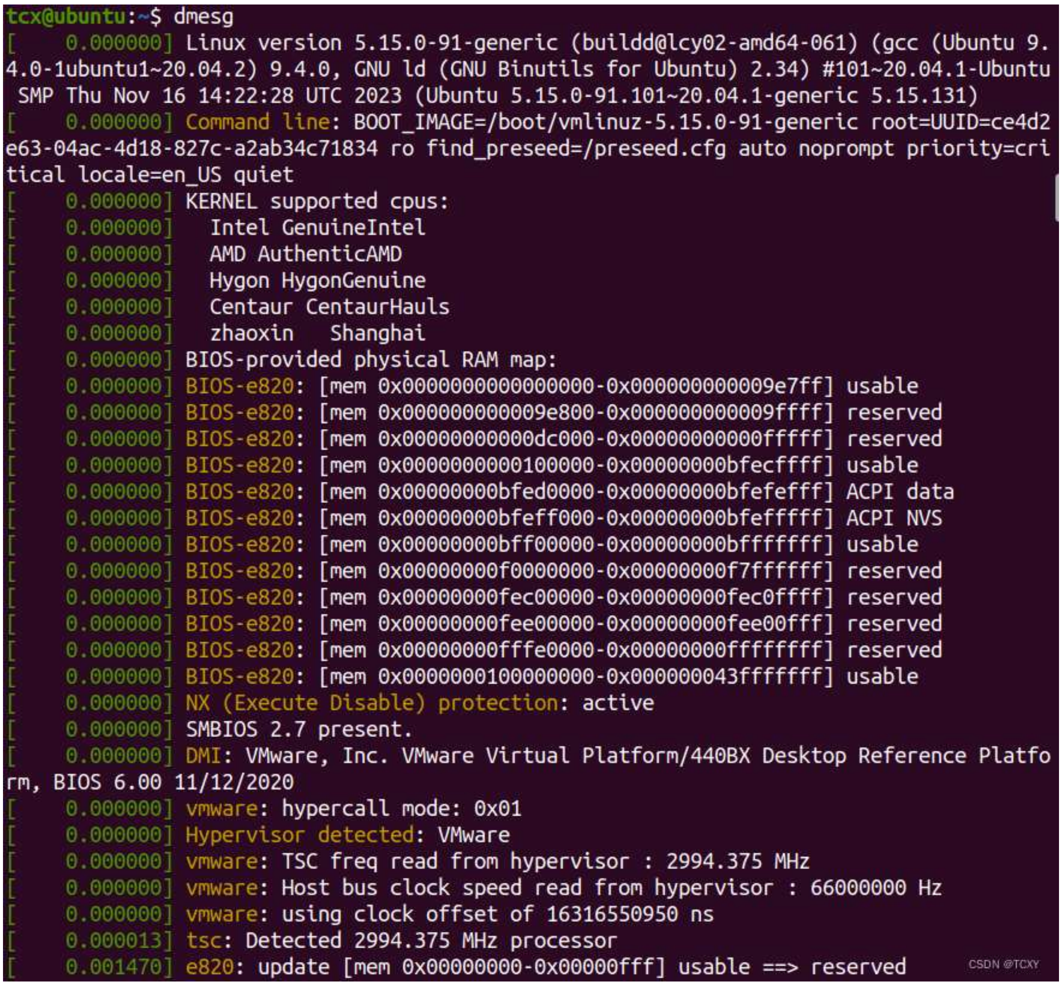
```
tcx@ubuntu:~$ hostname
ubuntu
```

1.9 查看系统中所有文件系统的磁盘使用情况（已用空间、可用空间以及使用百分比） df -a



```
tcx@ubuntu:~$ df -a
文件系统           1K-块     已用    可用 已用% 挂载点
sysfs                  0        0       0     - /sys
proc                   0        0       0     - /proc
udev             8130200        0 8130200    0% /dev
devpts                 0        0       0     - /dev/pts
tmpfs            1633744     2156 1631588    1% /run
/dev/sda5       19947120 13294040 5614488   71% /
securityfs             0        0       0     - /sys/kernel/security
tmpfs            8168712        0 8168712    0% /dev/shm
tmpfs               5120        4    5116    1% /run/lock
tmpfs            8168712        0 8168712    0% /sys/fs/cgroup
cgroup2                0        0       0     - /sys/fs/cgroup/unified
cgroup                 0        0       0     - /sys/fs/cgroup/systemd
pstore                 0        0       0     - /sys/fs/pstore
bpf                    0        0       0     - /sys/fs/bpf
cgroup                 0        0       0     - /sys/fs/cgroup/freezer
cgroup                 0        0       0     - /sys/fs/cgroup/cpu,cpuacct
cgroup                 0        0       0     - /sys/fs/cgroup/net_cls,net_prio
```

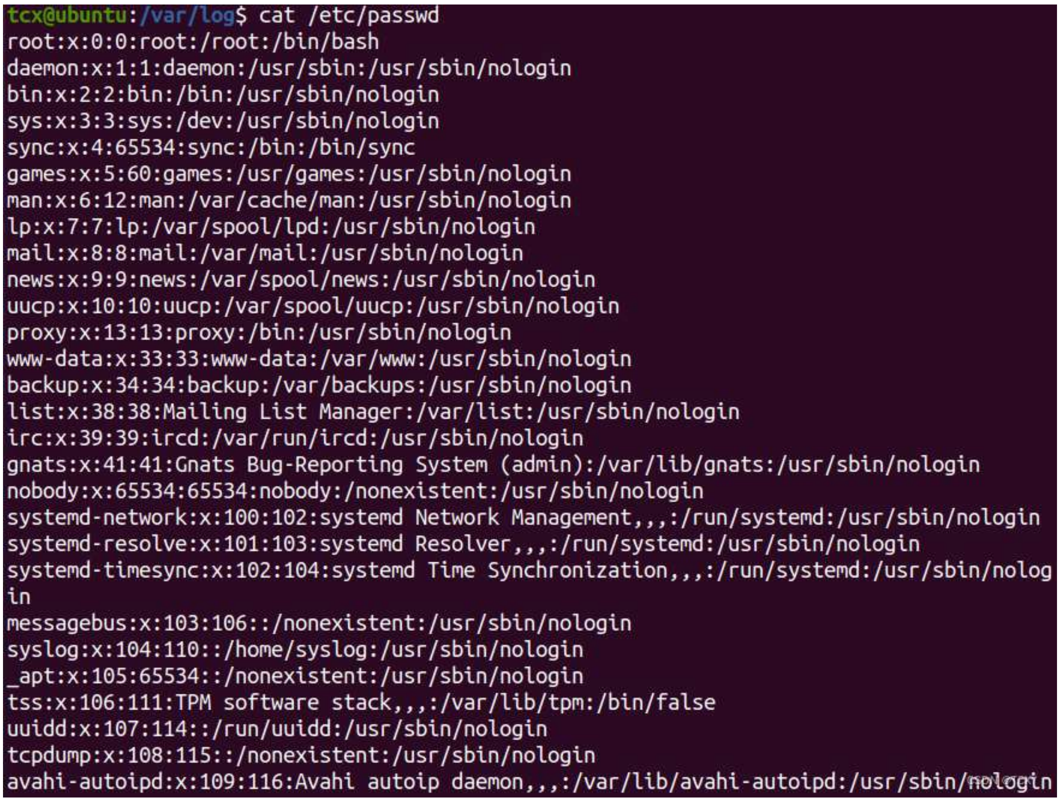
1.10 查看内核日志 demesg 或 /var/log/dmesg



```
tcx@ubuntu:~$ dmesg
[    0.000000] Linux version 5.15.0-91-generic (buildd@lcy02-amd64-061) (gcc (Ubuntu 9.
4.0-1ubuntu1~20.04.2) 9.4.0, GNU ld (GNU Binutils for Ubuntu) 2.34) #101~20.04.1-Ubuntu
 SMP Thu Nov 16 14:22:28 UTC 2023 (Ubuntu 5.15.0-91.101~20.04.1-generic 5.15.131)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.15.0-91-generic root=UUID=ce4d2
e63-04ac-4d18-827c-a2ab34c71834 ro find_preseed=/preseed.cfg auto noprompt priority=cri
tical locale=en_US quiet
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Hygon HygonGenuine
[    0.000000]   Centaur CentaurHauls
[    0.000000]   zhaoxin   Shanghai
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009e7ff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009e800-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bfecffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000bfed0000-0x00000000bfefefff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000bfeff000-0x00000000bfefffff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x00000000bff00000-0x00000000bfffffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000043fffffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.7 present.
[    0.000000] DMI: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platfo
rm, BIOS 6.00 11/12/2020
[    0.000000] vmware: hypercall mode: 0x01
[    0.000000] Hypervisor detected: VMware
[    0.000000] vmware: TSC freq read from hypervisor : 2994.375 MHz
[    0.000000] vmware: Host bus clock speed read from hypervisor : 66000000 Hz
[    0.000000] vmware: using clock offset of 16316550950 ns
[    0.000013] tsc: Detected 2994.375 MHz processor
[    0.001470] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
```

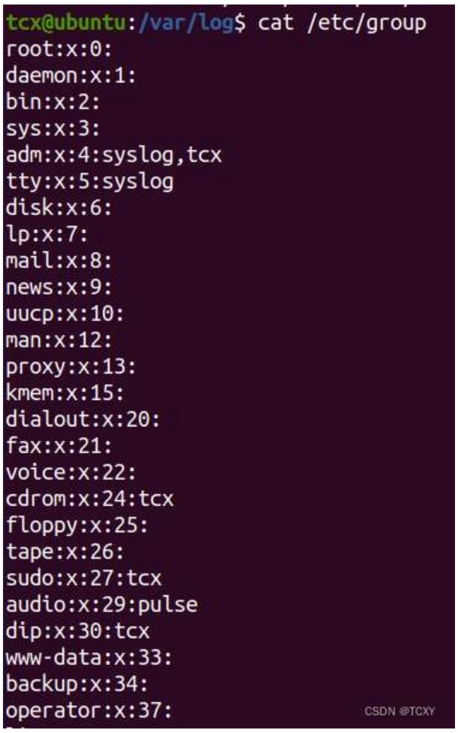
二、用户和组

2.1 列出系统所有用户 cat /etc/passwd



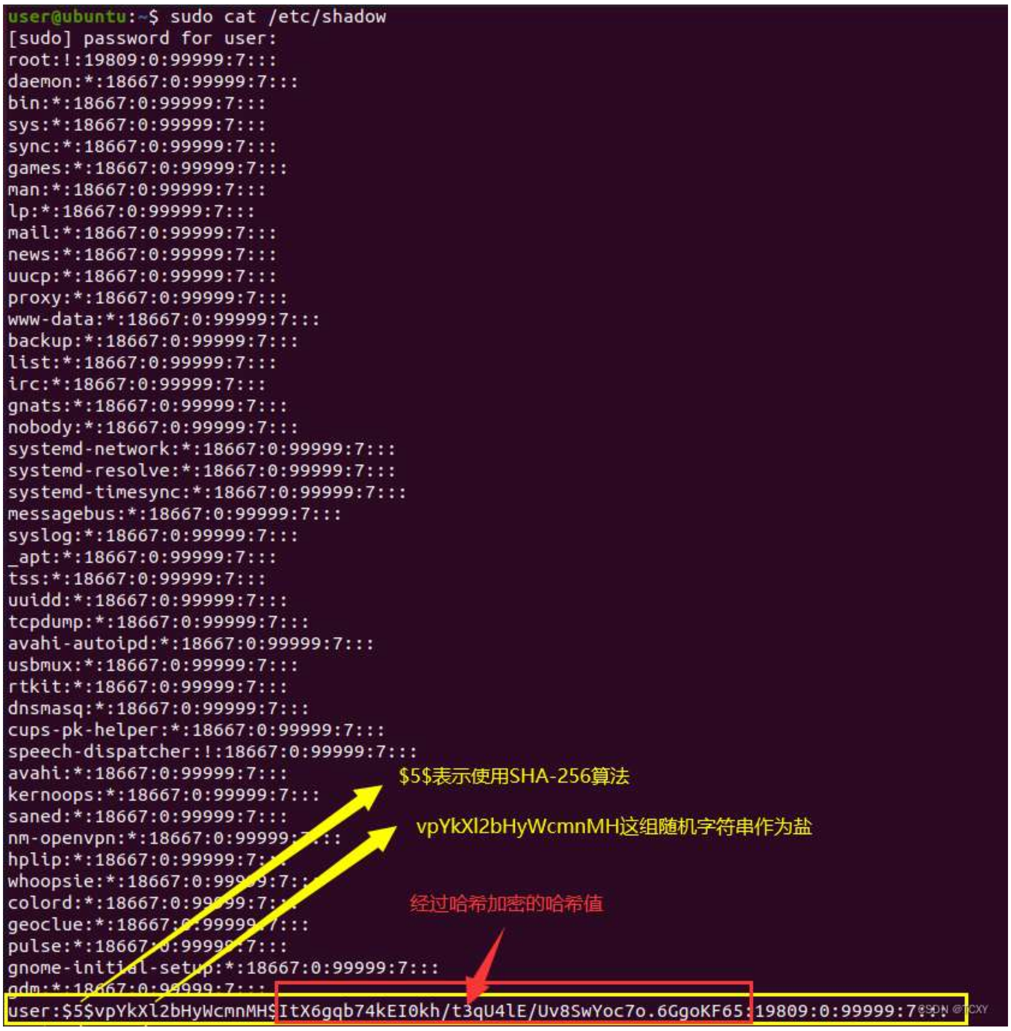
```
tcx@ubuntu:/var/log$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nolog
in
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
```

2.2 列出系统所有组 cat /etc/group



```
tcx@ubuntu:/var/log$ cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,tcx
tty:x:5:syslog
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:tcx
floppy:x:25:
tape:x:26:
sudo:x:27:tcx
audio:x:29:pulse
dip:x:30:tcx
www-data:x:33:
backup:x:34:
operator:x:37:
```

2.3 列出所有用户以及其口令对应的hash值 cat /etc/shadow



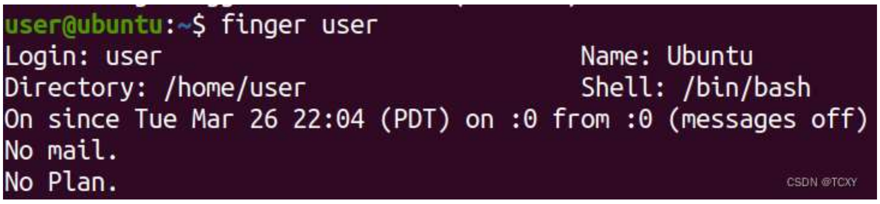
```
user@ubuntu:~$ sudo cat /etc/shadow
[sudo] password for user:
root:!:19809:0:99999:7:::
daemon:*:18667:0:99999:7:::
bin:*:18667:0:99999:7:::
sys:*:18667:0:99999:7:::
sync:*:18667:0:99999:7:::
games:*:18667:0:99999:7:::
man:*:18667:0:99999:7:::
lp:*:18667:0:99999:7:::
mail:*:18667:0:99999:7:::
news:*:18667:0:99999:7:::
uucp:*:18667:0:99999:7:::
proxy:*:18667:0:99999:7:::
www-data:*:18667:0:99999:7:::
backup:*:18667:0:99999:7:::
list:*:18667:0:99999:7:::
irc:*:18667:0:99999:7:::
gnats:*:18667:0:99999:7:::
nobody:*:18667:0:99999:7:::
systemd-network:*:18667:0:99999:7:::
systemd-resolve:*:18667:0:99999:7:::
systemd-timesync:*:18667:0:99999:7:::
messagebus:*:18667:0:99999:7:::
syslog:*:18667:0:99999:7:::
_apt:*:18667:0:99999:7:::
tss:*:18667:0:99999:7:::
uuidd:*:18667:0:99999:7:::
tcpdump:*:18667:0:99999:7:::
avahi-autoipd:*:18667:0:99999:7:::
usbmux:*:18667:0:99999:7:::
rtkit:*:18667:0:99999:7:::
dnsmasq:*:18667:0:99999:7:::
cups-pk-helper:*:18667:0:99999:7:::
speech-dispatcher:!:18667:0:99999:7:::
avahi:*:18667:0:99999:7:::
kernoops:*:18667:0:99999:7:::
saned:*:18667:0:99999:7:::
nm-openvpn:*:18667:0:99999:7:::
hplip:*:18667:0:99999:7:::
whoopsie:*:18667:0:99999:7:::
colord:*:18667:0:99999:7:::
geoclue:*:18667:0:99999:7:::
pulse:*:18667:0:99999:7:::
gnome-initial-setup:*:18667:0:99999:7:::
gdm:*:18667:0:99999:7:::
user:$5$vpYkXl2bHyWcmnMH$ItX6gqb74kEI0kh/t3qU4lE/Uv8SwYoc7o.6GgoKF65:19809:0:99999:7:::
```

5表示使用SHA-256算法

vpYkXl2bHyWcmnMH这组随机字符串作为盐

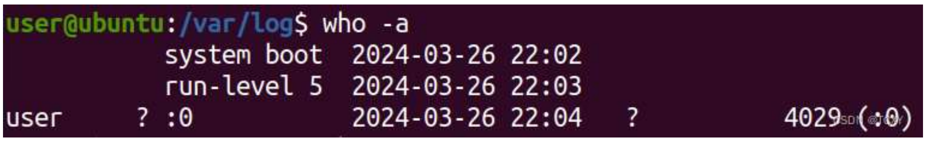
经过哈希加密的哈希值

2.4 查询xxx用户的基本信息 finger xxx



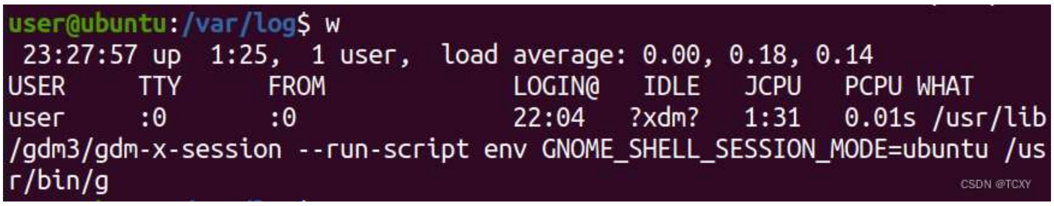
```
user@ubuntu:~$ finger user
Login: user                             Name: Ubuntu
Directory: /home/user                   Shell: /bin/bash
On since Tue Mar 26 22:04 (PDT) on :0 from :0 (messages off)
No mail.
No Plan.
```

2.5 查询当前登录用户信息 who -a



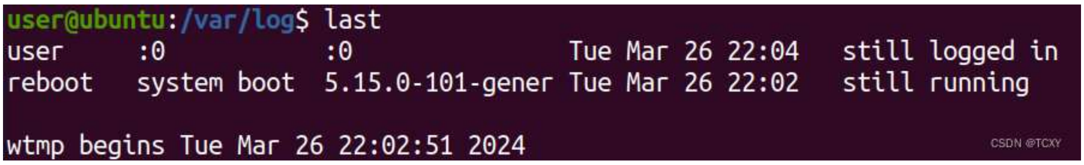
```
user@ubuntu:/var/log$ who -a
           system boot  2024-03-26 22:02
           run-level 5  2024-03-26 22:03
user     ? :0           2024-03-26 22:04   ?          4029 (:0)
```

2.6 查看目前登陆的用户 w



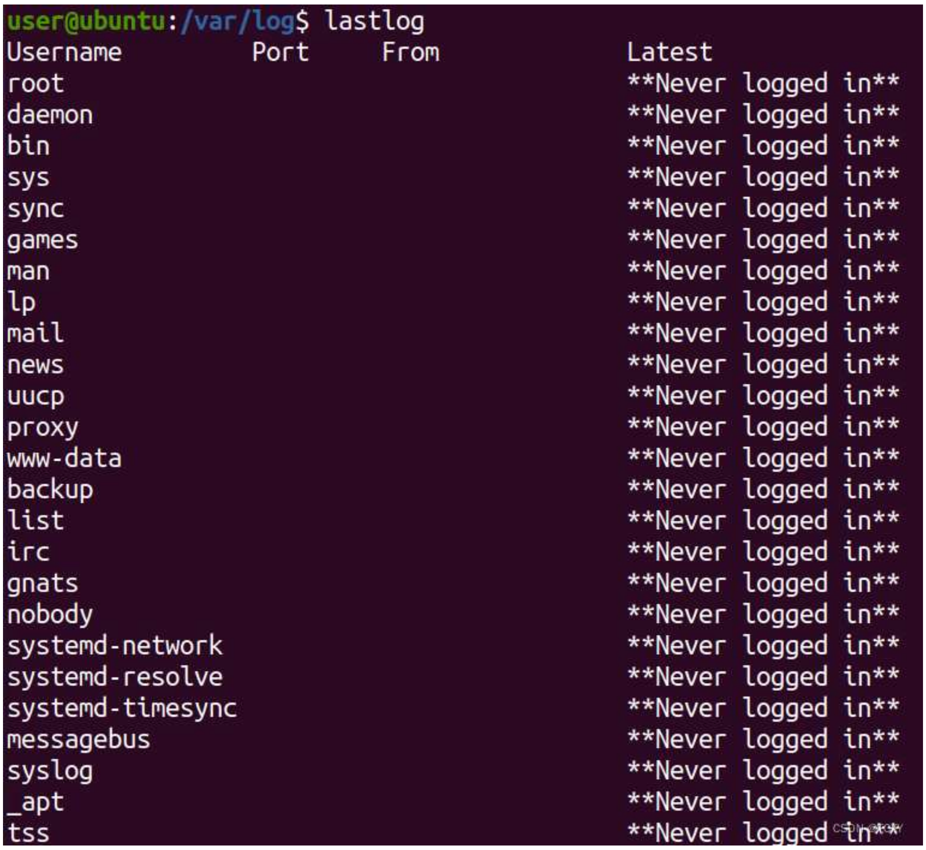
```
user@ubuntu:/var/log$ w
 23:27:57 up  1:25,  1 user,  load average: 0.00, 0.18, 0.14
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user     :0       :0               22:04   ?xdm?   1:31   0.01s /usr/lib
/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /us
r/bin/g
```

2.7 登录过的用户信息 last



```
user@ubuntu:/var/log$ last
user     :0           :0               Tue Mar 26 22:04   still logged in
reboot   system boot  5.15.0-101-gener Tue Mar 26 22:02   still running

wtmp begins Tue Mar 26 22:02:51 2024
```

2.8 显示系统中所有用户最近一次登录信息 lastlog

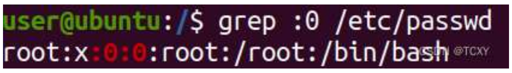


```
user@ubuntu:/var/log$ lastlog
Username         Port     From             Latest
root                                       **Never logged in**
daemon                                     **Never logged in**
bin                                        **Never logged in**
sys                                        **Never logged in**
sync                                       **Never logged in**
games                                      **Never logged in**
man                                        **Never logged in**
lp                                         **Never logged in**
mail                                       **Never logged in**
news                                       **Never logged in**
uucp                                       **Never logged in**
proxy                                      **Never logged in**
www-data                                   **Never logged in**
backup                                     **Never logged in**
list                                       **Never logged in**
irc                                        **Never logged in**
gnats                                      **Never logged in**
nobody                                     **Never logged in**
systemd-network                            **Never logged in**
systemd-resolve                            **Never logged in**
systemd-timesync                           **Never logged in**
messagebus                                 **Never logged in**
syslog                                     **Never logged in**
_apt                                       **Never logged in**
tss                                        **Never logged in**
```

2.9 登陆成功日志 /var/log/secure

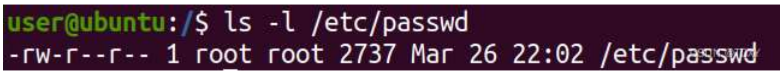
2.10 登陆失败日志 /var/log/faillog

2.11 查看特权用户 grep :0 /etc/passwd



```
user@ubuntu:/$ grep :0 /etc/passwd
root:x:0:0:root:/root:/bin/bash
```

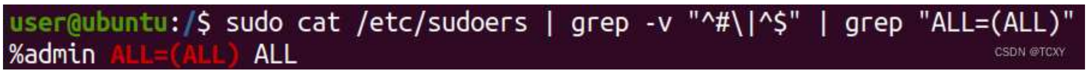
2.12 显示passwd最后修改时间 ls -l /etc/passwd



```
user@ubuntu:/$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2737 Mar 26 22:02 /etc/passwd
```

2.13 查看远程登陆账号 awk '/\$1|\$6/{print $1}' /etc/shadow

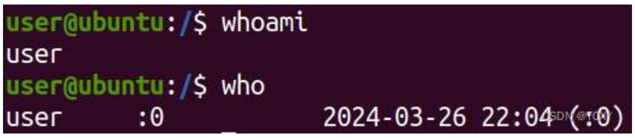
2.14 查看具有sudo权限的用户 cat /etc/sudoers | grep -v "^#|^$" | grep "ALL=(ALL)"



```
user@ubuntu:/$ sudo cat /etc/sudoers | grep -v "^#\|^$" | grep "ALL=(ALL)"
%admin ALL=(ALL) ALL
```

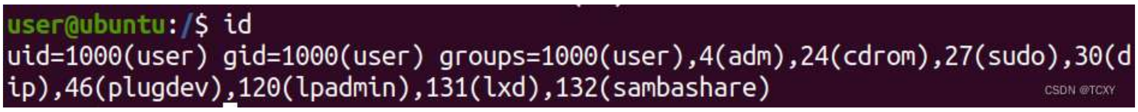
三、用户和权限信息

3.1 查看当前用户 whoami



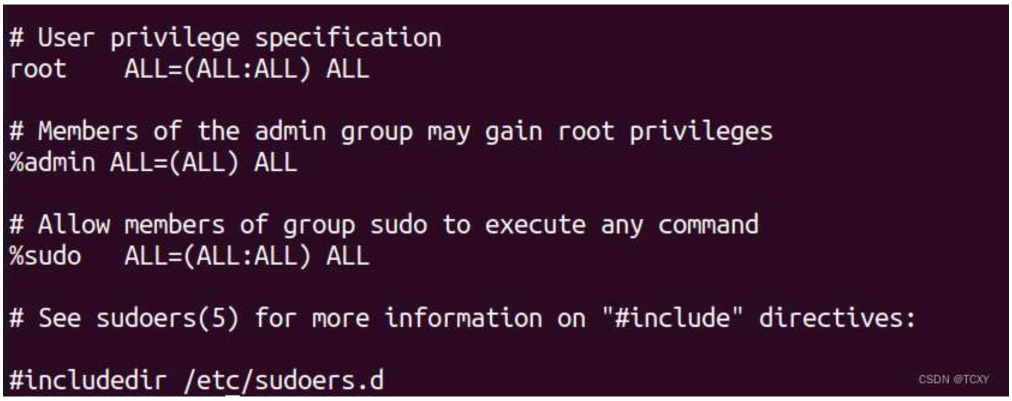
```
user@ubuntu:/$ whoami
user
user@ubuntu:/$ who
user     :0           2024-03-26 22:04 (:0)
```

3.2 当前用户信息 id



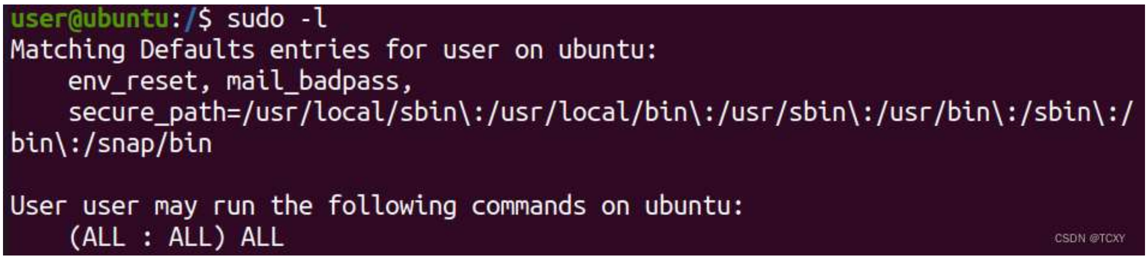
```
user@ubuntu:/$ id
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),27(sudo),30(d
ip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
```

3.3 可用sudo提升至root的用户 cat /etc/sudoers



```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

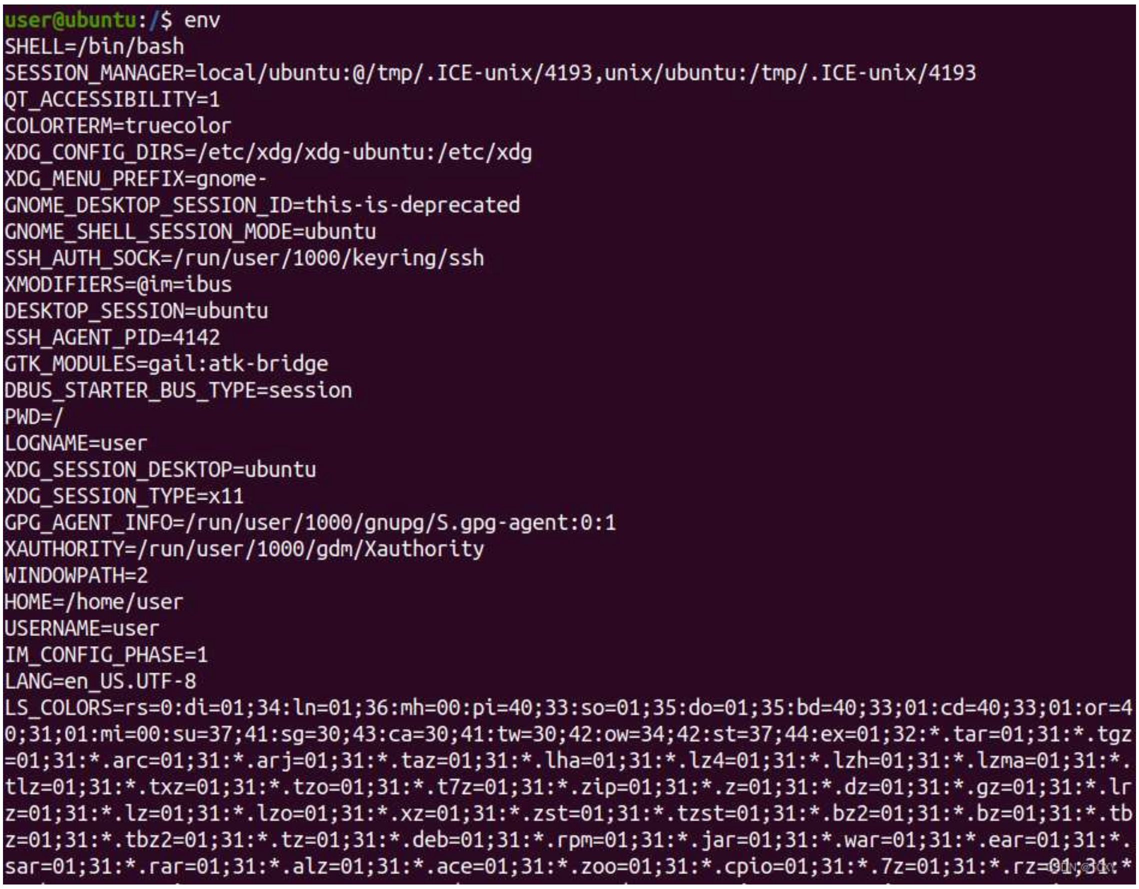
3.4 列出目前用户可执行与无法执行的指令 sudo -l



```
user@ubuntu:/$ sudo -l
Matching Defaults entries for user on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin\:/snap/bin

User user may run the following commands on ubuntu:
    (ALL : ALL) ALL
```

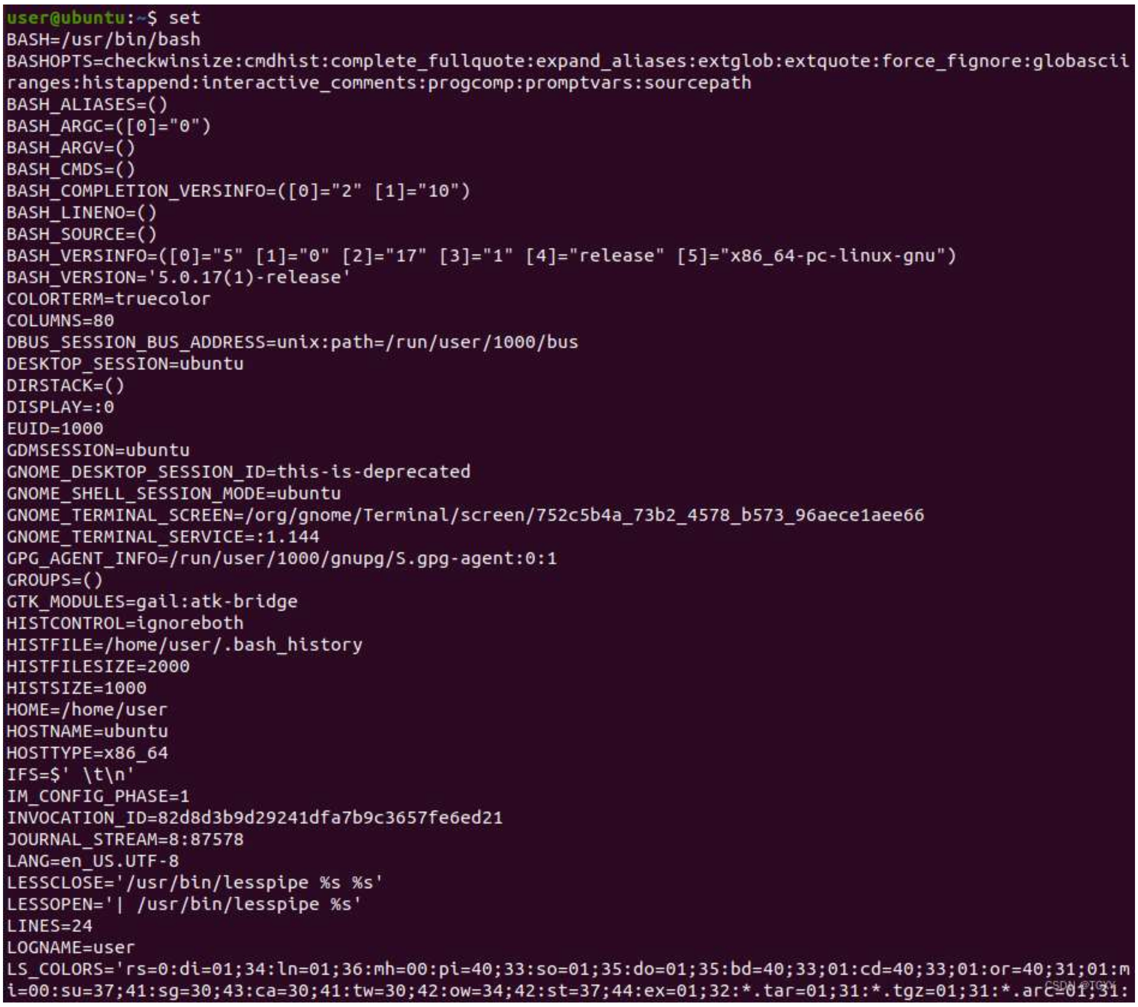
四、环境信息

4.1 打印系统环境信息 env



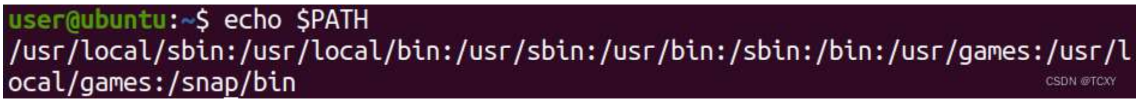
```
user@ubuntu:/$ env
SHELL=/bin/bash
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/4193,unix/ubuntu:/tmp/.ICE-unix/4193
QT_ACCESSIBILITY=1
COLORTERM=truecolor
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_MENU_PREFIX=gnome-
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
XMODIFIERS=@im=ibus
DESKTOP_SESSION=ubuntu
SSH_AGENT_PID=4142
GTK_MODULES=gail:atk-bridge
DBUS_STARTER_BUS_TYPE=session
PWD=/
LOGNAME=user
XDG_SESSION_DESKTOP=ubuntu
XDG_SESSION_TYPE=x11
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
XAUTHORITY=/run/user/1000/gdm/Xauthority
WINDOWPATH=2
HOME=/home/user
USERNAME=user
IM_CONFIG_PHASE=1
LANG=en_US.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=4
0;31;01:mi=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz
=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.
tlz=01;31:*.txz=01;31:*.tzo=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz=01;31:*.gz=01;31:*.lr
z=01;31:*.lz=01;31:*.lzo=01;31:*.xz=01;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tb
z=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.
sar=01;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;31:*
```

4.2 打印系统环境信息



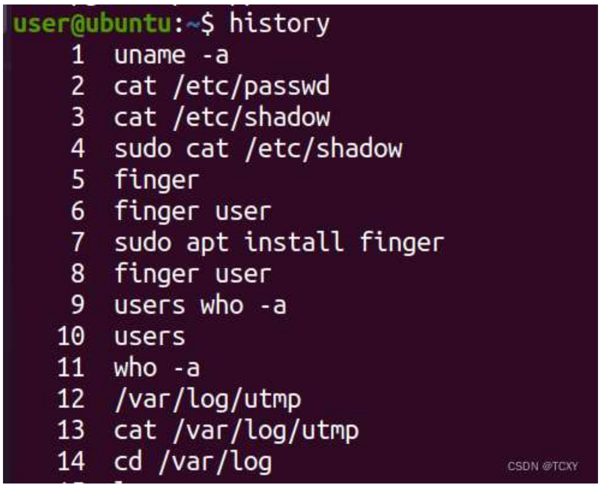
```
user@ubuntu:~$ set
BASH=/usr/bin/bash
BASHOPTS=checkwinsize:cmdhist:complete_fullquote:expand_aliases:extglob:extquote:force_fignore:globascii
ranges:histappend:interactive_comments:progcomp:promptvars:sourcepath
BASH_ALIASES=()
BASH_ARGC=([0]="0")
BASH_ARGV=()
BASH_CMDS=()
BASH_COMPLETION_VERSINFO=([0]="2" [1]="10")
BASH_LINENO=()
BASH_SOURCE=()
BASH_VERSINFO=([0]="5" [1]="0" [2]="17" [3]="1" [4]="release" [5]="x86_64-pc-linux-gnu")
BASH_VERSION='5.0.17(1)-release'
COLORTERM=truecolor
COLUMNS=80
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
DESKTOP_SESSION=ubuntu
DIRSTACK=()
DISPLAY=:0
EUID=1000
GDMSESSION=ubuntu
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
GNOME_SHELL_SESSION_MODE=ubuntu
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/752c5b4a_73b2_4578_b573_96aece1aee66
GNOME_TERMINAL_SERVICE=:1.144
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
GROUPS=()
GTK_MODULES=gail:atk-bridge
HISTCONTROL=ignoreboth
HISTFILE=/home/user/.bash_history
HISTFILESIZE=2000
HISTSIZE=1000
HOME=/home/user
HOSTNAME=ubuntu
HOSTTYPE=x86_64
IFS=$' \t\n'
IM_CONFIG_PHASE=1
INVOCATION_ID=82d8d3b9d29241dfa7b9c3657fe6ed21
JOURNAL_STREAM=8:87578
LANG=en_US.UTF-8
LESSCLOSE='/usr/bin/lesspipe %s %s'
LESSOPEN='| /usr/bin/lesspipe %s'
LINES=24
LOGNAME=user
LS_COLORS='rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;33;01:or=40;31;01:m
i=00:su=37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*.arc=01;31:
```

4.3 环境变量　中的路径信息 echo $PATH



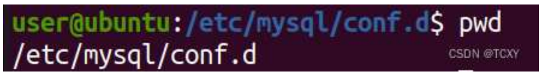
```
user@ubuntu:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/l
ocal/games:/snap/bin
```

4.4 打印历史命令 history



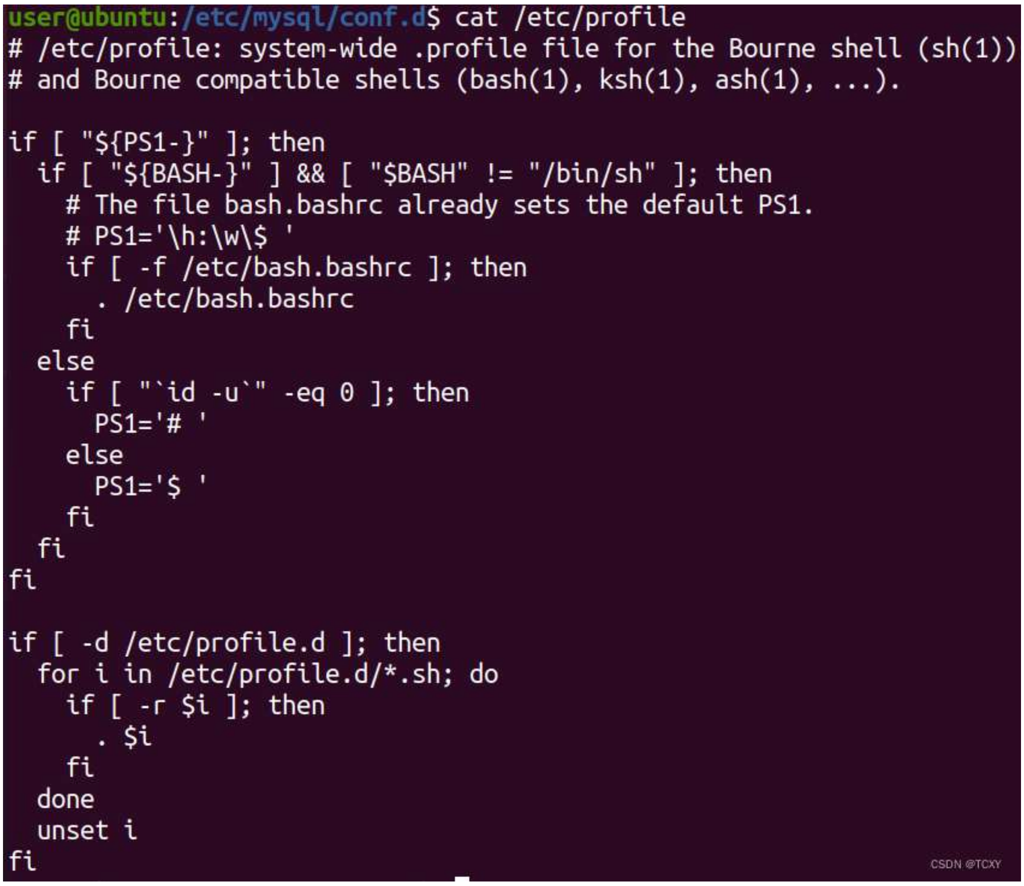
```
user@ubuntu:~$ history
    1  uname -a
    2  cat /etc/passwd
    3  cat /etc/shadow
    4  sudo cat /etc/shadow
    5  finger
    6  finger user
    7  sudo apt install finger
    8  finger user
    9  users who -a
   10  users
   11  who -a
   12  /var/log/utmp
   13  cat /var/log/utmp
   14  cd /var/log
```

4.5 显示当前路径 pwd



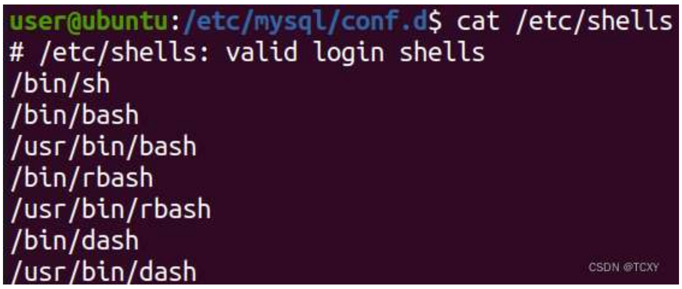
```
user@ubuntu:/etc/mysql/conf.d$ pwd
/etc/mysql/conf.d
```

4.6 显示默认系统遍历 cat /etc/profile



```
user@ubuntu:/etc/mysql/conf.d$ cat /etc/profile
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).

if [ "${PS1-}" ]; then
  if [ "${BASH-}" ] && [ "$BASH" != "/bin/sh" ]; then
    # The file bash.bashrc already sets the default PS1.
    # PS1='\h:\w\$ '
    if [ -f /etc/bash.bashrc ]; then
      . /etc/bash.bashrc
    fi
  else
    if [ "`id -u`" -eq 0 ]; then
      PS1='# '
    else
      PS1='$ '
    fi
  fi
fi

if [ -d /etc/profile.d ]; then
  for i in /etc/profile.d/*.sh; do
    if [ -r $i ]; then
      . $i
    fi
  done
  unset i
fi
```

4.7 显示可用的shell

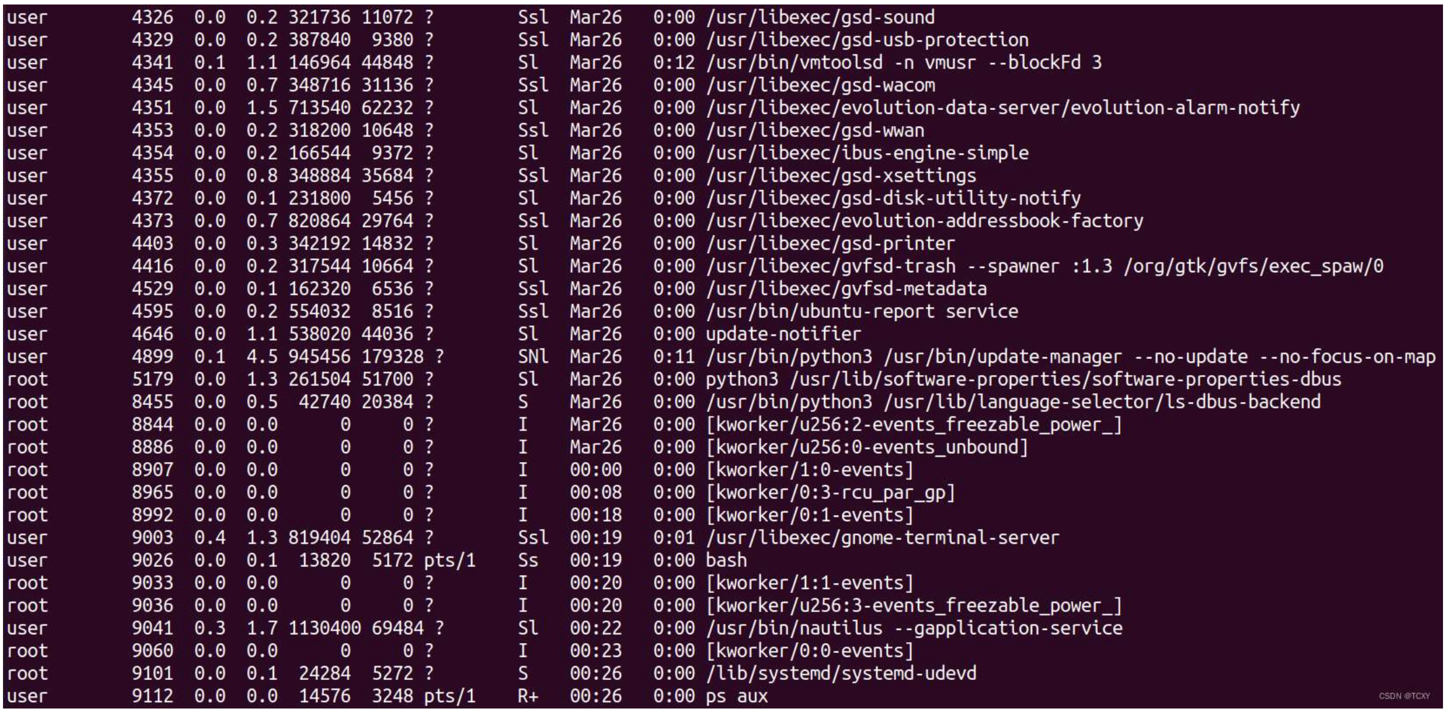


```
user@ubuntu:/etc/mysql/conf.d$ cat /etc/shells
# /etc/shells: valid login shells
/bin/sh
/bin/bash
/usr/bin/bash
/bin/rbash
/usr/bin/rbash
/bin/dash
/usr/bin/dash
```

CSDN @TCXY

五、进程信息

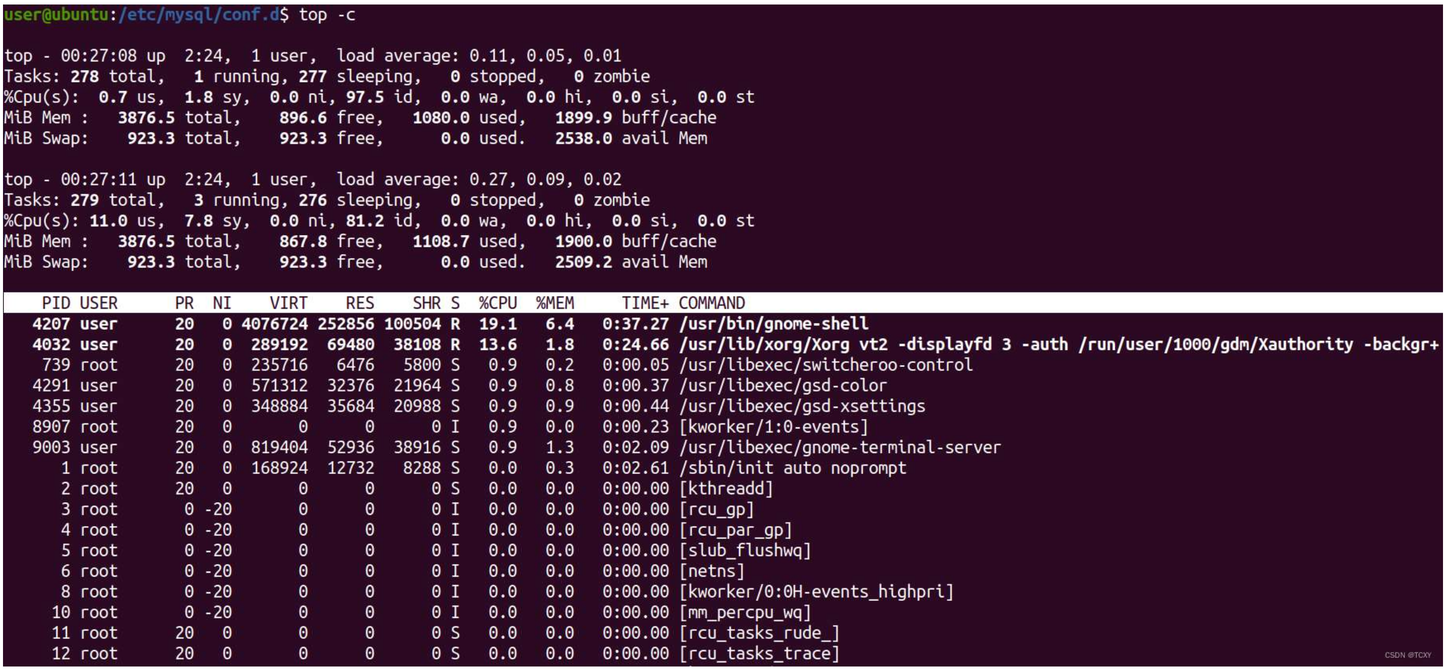
5.1 查看进程信息 ps aux



```
user        4326  0.0  0.2 321736 11072 ?        Ssl  Mar26   0:00 /usr/libexec/gsd-sound
user        4329  0.0  0.2 387840  9380 ?        Ssl  Mar26   0:00 /usr/libexec/gsd-usb-protection
user        4341  0.1  1.1 146964 44848 ?        Sl   Mar26   0:12 /usr/bin/vmtoolsd -n vmusr --blockFd 3
user        4345  0.0  0.7 348716 31136 ?        Ssl  Mar26   0:00 /usr/libexec/gsd-wacom
user        4351  0.0  1.5 713540 62232 ?        Sl   Mar26   0:00 /usr/libexec/evolution-data-server/evolution-alarm-notify
user        4353  0.0  0.2 318200 10648 ?        Ssl  Mar26   0:00 /usr/libexec/gsd-wwan
user        4354  0.0  0.2 166544  9372 ?        Sl   Mar26   0:00 /usr/libexec/ibus-engine-simple
user        4355  0.0  0.8 348884 35684 ?        Ssl  Mar26   0:00 /usr/libexec/gsd-xsettings
user        4372  0.0  0.1 231800  5456 ?        Sl   Mar26   0:00 /usr/libexec/gsd-disk-utility-notify
user        4373  0.0  0.7 820864 29764 ?        Ssl  Mar26   0:00 /usr/libexec/evolution-addressbook-factory
user        4403  0.0  0.3 342192 14832 ?        Sl   Mar26   0:00 /usr/libexec/gsd-printer
user        4416  0.0  0.2 317544 10664 ?        Sl   Mar26   0:00 /usr/libexec/gvfsd-trash --spawner :1.3 /org/gtk/gvfs/exec_spaw/0
user        4529  0.0  0.1 162320  6536 ?        Ssl  Mar26   0:00 /usr/libexec/gvfsd-metadata
user        4595  0.0  0.2 554032  8516 ?        Ssl  Mar26   0:00 /usr/bin/ubuntu-report service
user        4646  0.0  1.1 538020 44036 ?        Sl   Mar26   0:00 update-notifier
user        4899  0.1  4.5 945456 179328 ?       SNl  Mar26   0:11 /usr/bin/python3 /usr/bin/update-manager --no-update --no-focus-on-map
root        5179  0.0  1.3 261504 51700 ?        Sl   Mar26   0:00 python3 /usr/lib/software-properties/software-properties-dbus
root        8455  0.0  0.5  42740 20384 ?        S    Mar26   0:00 /usr/bin/python3 /usr/lib/language-selector/ls-dbus-backend
root        8844  0.0  0.0      0     0 ?        I    Mar26   0:00 [kworker/u256:2-events_freezable_power_]
root        8886  0.0  0.0      0     0 ?        I    Mar26   0:00 [kworker/u256:0-events_unbound]
root        8907  0.0  0.0      0     0 ?        I    00:00   0:00 [kworker/1:0-events]
root        8965  0.0  0.0      0     0 ?        I    00:08   0:00 [kworker/0:3-rcu_par_gp]
root        8992  0.0  0.0      0     0 ?        I    00:18   0:00 [kworker/0:1-events]
user        9003  0.4  1.3 819404 52864 ?        Ssl  00:19   0:01 /usr/libexec/gnome-terminal-server
user        9026  0.0  0.1  13820  5172 pts/1    Ss   00:19   0:00 bash
root        9033  0.0  0.0      0     0 ?        I    00:20   0:00 [kworker/1:1-events]
root        9036  0.0  0.0      0     0 ?        I    00:20   0:00 [kworker/u256:3-events_freezable_power_]
user        9041  0.3  1.7 1130400 69484 ?       Sl   00:22   0:00 /usr/bin/nautilus --gapplication-service
root        9060  0.0  0.0      0     0 ?        I    00:23   0:00 [kworker/0:0-events]
root        9101  0.0  0.1  24284  5272 ?        S    00:26   0:00 /lib/systemd/systemd-udevd
user        9112  0.0  0.0  14576  3248 pts/1    R+   00:26   0:00 ps aux
```

CSDN @TCXY

5.2 资源占有情况 top -c



```
user@ubuntu:/etc/mysql/conf.d$ top -c

top - 00:27:08 up  2:24,  1 user,  load average: 0.11, 0.05, 0.01
Tasks: 278 total,   1 running, 277 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.7 us,  1.8 sy,  0.0 ni, 97.5 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3876.5 total,    896.6 free,   1080.0 used,   1899.9 buff/cache
MiB Swap:    923.3 total,    923.3 free,      0.0 used.   2538.0 avail Mem

top - 00:27:11 up  2:24,  1 user,  load average: 0.27, 0.09, 0.02
Tasks: 279 total,   3 running, 276 sleeping,   0 stopped,   0 zombie
%Cpu(s): 11.0 us,  7.8 sy,  0.0 ni, 81.2 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3876.5 total,    867.8 free,   1108.7 used,   1900.0 buff/cache
MiB Swap:    923.3 total,    923.3 free,      0.0 used.   2509.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   4207 user      20   0 4076724 252856 100504 R  19.1   6.4   0:37.27 /usr/bin/gnome-shell
   4032 user      20   0  289192  69480  38108 R  13.6   1.8   0:24.66 /usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -backgr+
    739 root      20   0  235716   6476   5800 S   0.9   0.2   0:00.05 /usr/libexec/switcheroo-control
   4291 user      20   0  571312  32376  21964 S   0.9   0.8   0:00.37 /usr/libexec/gsd-color
   4355 user      20   0  348884  35684  20988 S   0.9   0.9   0:00.44 /usr/libexec/gsd-xsettings
   8907 root      20   0       0      0      0 I   0.9   0.0   0:00.23 [kworker/1:0-events]
   9003 user      20   0  819404  52936  38916 S   0.9   1.3   0:02.09 /usr/libexec/gnome-terminal-server
      1 root      20   0  168924  12732   8288 S   0.0   0.3   0:02.61 /sbin/init auto noprompt
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 [kthreadd]
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [rcu_gp]
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [rcu_par_gp]
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [slub_flushwq]
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [netns]
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [kworker/0:0H-events_highpri]
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 [mm_percpu_wq]
     11 root      20   0       0      0      0 S   0.0   0.0   0:00.00 [rcu_tasks_rude_]
     12 root      20   0       0      0      0 S   0.0   0.0   0:00.00 [rcu_tasks_trace]
```

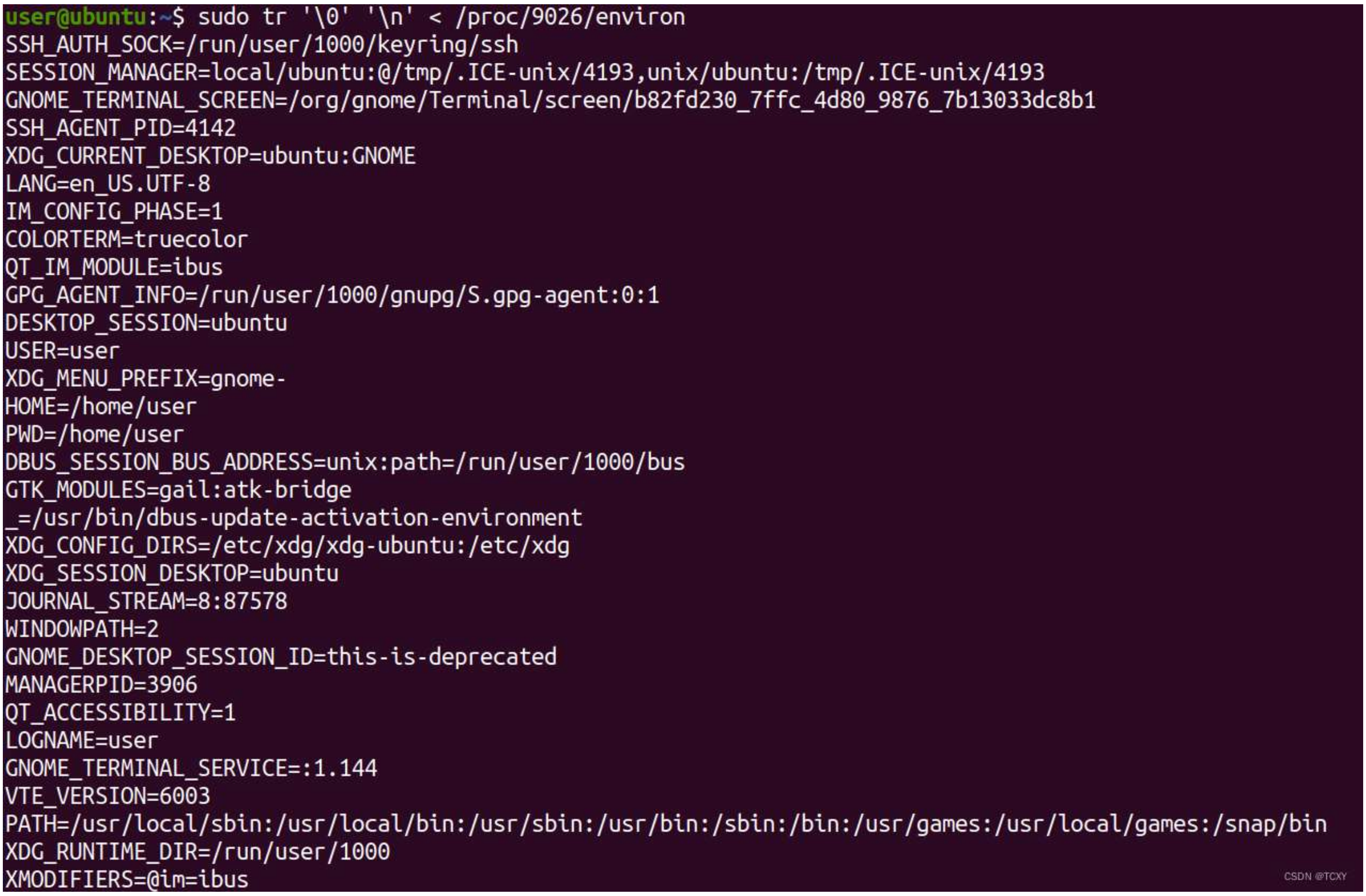
CSDN @TCXY

5.3 查看进程关联文件 lsof -c $PID

5.4 完整命令行　信息 /proc/$PID/cmdline

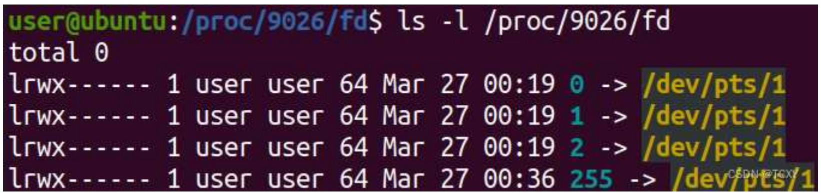
5.5 进程的命令名 /proc/$PID/comm

5.6 进程当前工作 目录 的符号链接 /proc/$PID/environ



```
user@ubuntu:~$ sudo tr '\0' '\n' < /proc/9026/environ
SSH_AUTH_SOCK=/run/user/1000/keyring/ssh
SESSION_MANAGER=local/ubuntu:@/tmp/.ICE-unix/4193,unix/ubuntu:/tmp/.ICE-unix/4193
GNOME_TERMINAL_SCREEN=/org/gnome/Terminal/screen/b82fd230_7ffc_4d80_9876_7b13033dc8b1
SSH_AGENT_PID=4142
XDG_CURRENT_DESKTOP=ubuntu:GNOME
LANG=en_US.UTF-8
IM_CONFIG_PHASE=1
COLORTERM=truecolor
QT_IM_MODULE=ibus
GPG_AGENT_INFO=/run/user/1000/gnupg/S.gpg-agent:0:1
DESKTOP_SESSION=ubuntu
USER=user
XDG_MENU_PREFIX=gnome-
HOME=/home/user
PWD=/home/user
DBUS_SESSION_BUS_ADDRESS=unix:path=/run/user/1000/bus
GTK_MODULES=gail:atk-bridge
_=/usr/bin/dbus-update-activation-environment
XDG_CONFIG_DIRS=/etc/xdg/xdg-ubuntu:/etc/xdg
XDG_SESSION_DESKTOP=ubuntu
JOURNAL_STREAM=8:87578
WINDOWPATH=2
GNOME_DESKTOP_SESSION_ID=this-is-deprecated
MANAGERPID=3906
QT_ACCESSIBILITY=1
LOGNAME=user
GNOME_TERMINAL_SERVICE=:1.144
VTE_VERSION=6003
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
XDG_RUNTIME_DIR=/run/user/1000
XMODIFIERS=@im=ibus
```

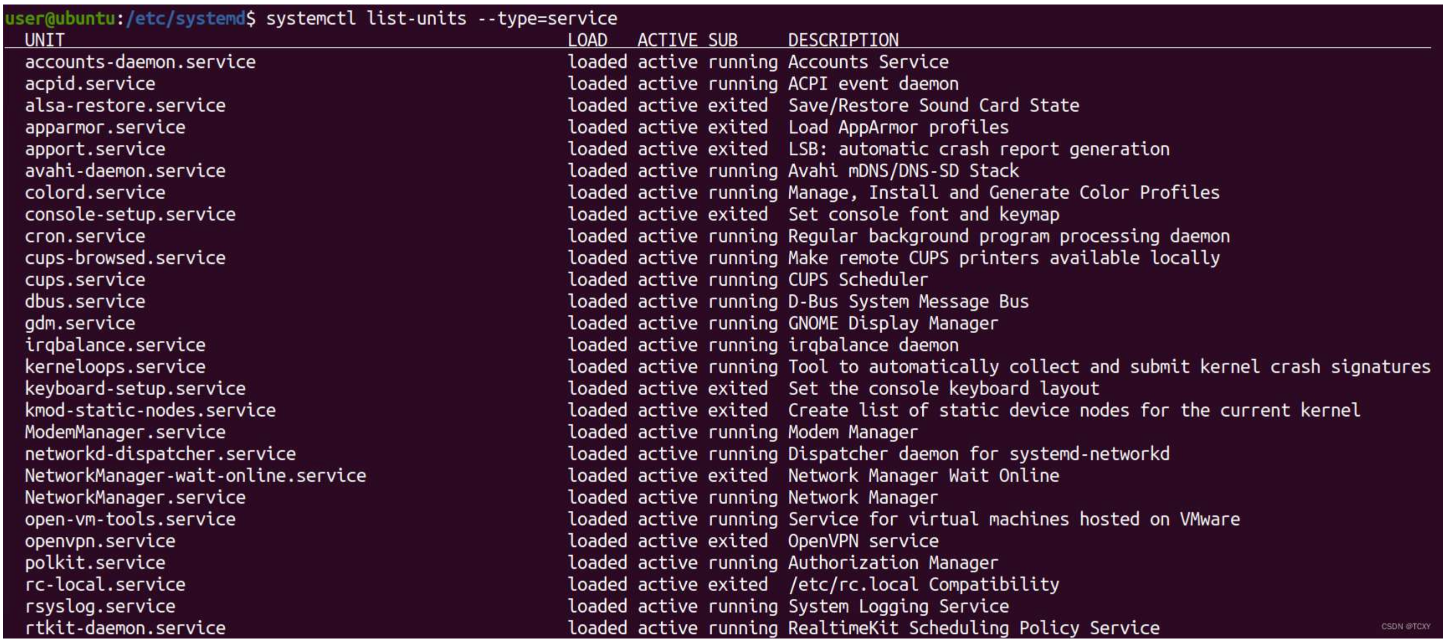
5.7 进程打开文件的情况 /proc/$PID/fd



```
user@ubuntu:/proc/9026/fd$ ls -l /proc/9026/fd
total 0
lrwx------ 1 user user 64 Mar 27 00:19 0 -> /dev/pts/1
lrwx------ 1 user user 64 Mar 27 00:19 1 -> /dev/pts/1
lrwx------ 1 user user 64 Mar 27 00:19 2 -> /dev/pts/1
lrwx------ 1 user user 64 Mar 27 00:36 255 -> /dev/pts/1
```

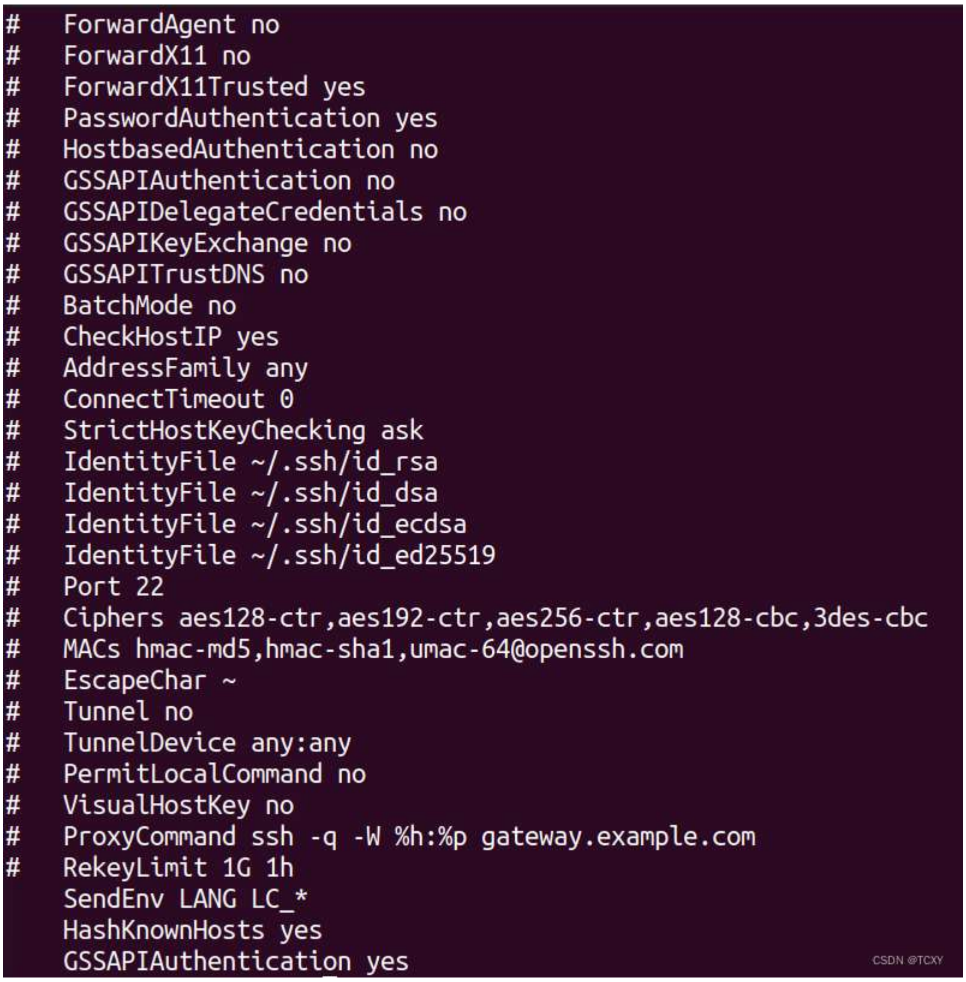
六、服务信息

6.1 由systemd管理的服务列表 systemctl list-units --type=service



```
user@ubuntu:/etc/systemd$ systemctl list-units --type=service
  UNIT                                                  LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service                               loaded active running Accounts Service
  acpid.service                                         loaded active running ACPI event daemon
  alsa-restore.service                                  loaded active exited  Save/Restore Sound Card State
  apparmor.service                                      loaded active exited  Load AppArmor profiles
  apport.service                                        loaded active exited  LSB: automatic crash report generation
  avahi-daemon.service                                  loaded active running Avahi mDNS/DNS-SD Stack
  colord.service                                        loaded active running Manage, Install and Generate Color Profiles
  console-setup.service                                 loaded active exited  Set console font and keymap
  cron.service                                          loaded active running Regular background program processing daemon
  cups-browsed.service                                  loaded active running Make remote CUPS printers available locally
  cups.service                                          loaded active running CUPS Scheduler
  dbus.service                                          loaded active running D-Bus System Message Bus
  gdm.service                                           loaded active running GNOME Display Manager
  irqbalance.service                                    loaded active running irqbalance daemon
  kerneloops.service                                    loaded active running Tool to automatically collect and submit kernel crash signatures
  keyboard-setup.service                                loaded active exited  Set the console keyboard layout
  kmod-static-nodes.service                             loaded active exited  Create list of static device nodes for the current kernel
  ModemManager.service                                  loaded active running Modem Manager
  networkd-dispatcher.service                           loaded active running Dispatcher daemon for systemd-networkd
  NetworkManager-wait-online.service                    loaded active exited  Network Manager Wait Online
  NetworkManager.service                                loaded active running Network Manager
  open-vm-tools.service                                 loaded active running Service for virtual machines hosted on VMware
  openvpn.service                                       loaded active exited  OpenVPN service
  polkit.service                                        loaded active running Authorization Manager
  rc-local.service                                      loaded active exited  /etc/rc.local Compatibility
  rsyslog.service                                       loaded active running System Logging Service
  rtkit-daemon.service                                  loaded active running RealtimeKit Scheduling Policy Service
```

6.2 查看ssh配置 /etc/ssh/ssh_config



```
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
```

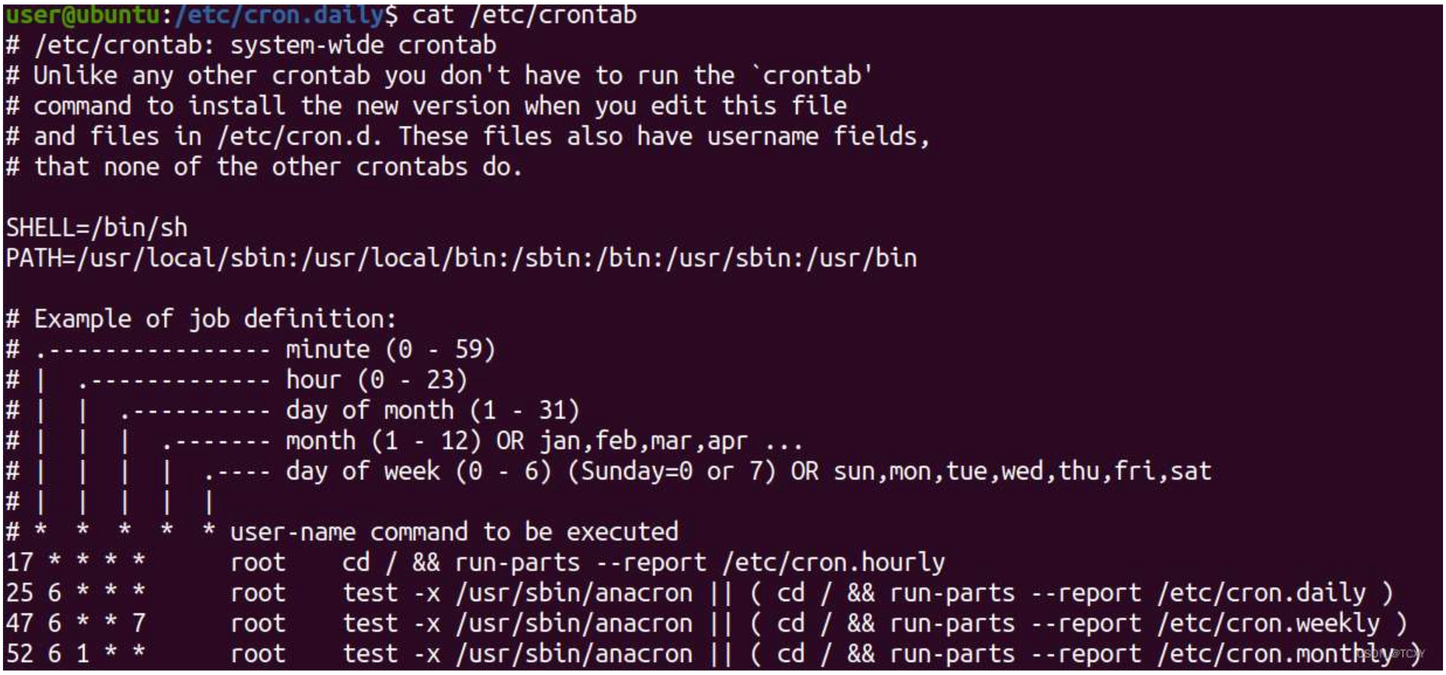
七、计划任务

涉及目录包括:

- /var/spool/cron/*
- /var/spool/anacron/*
- /etc/crontab
- /etc/anacrontab
- /etc/cron.*
- /etc/anacrontab

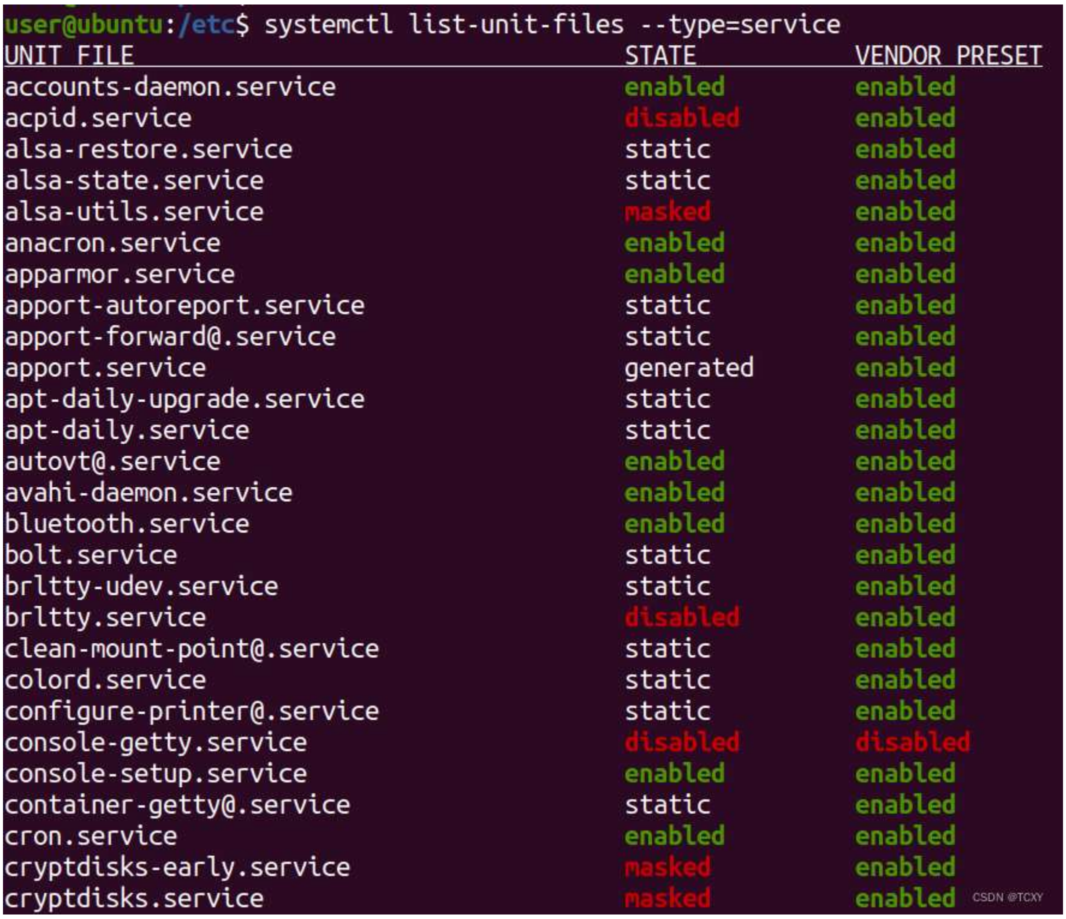
7.1显示xxx用户的计划作业 crontab -l -u xxx

7.2 计划任务 /etc/crontab



```
user@ubuntu:/etc/cron.daily$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

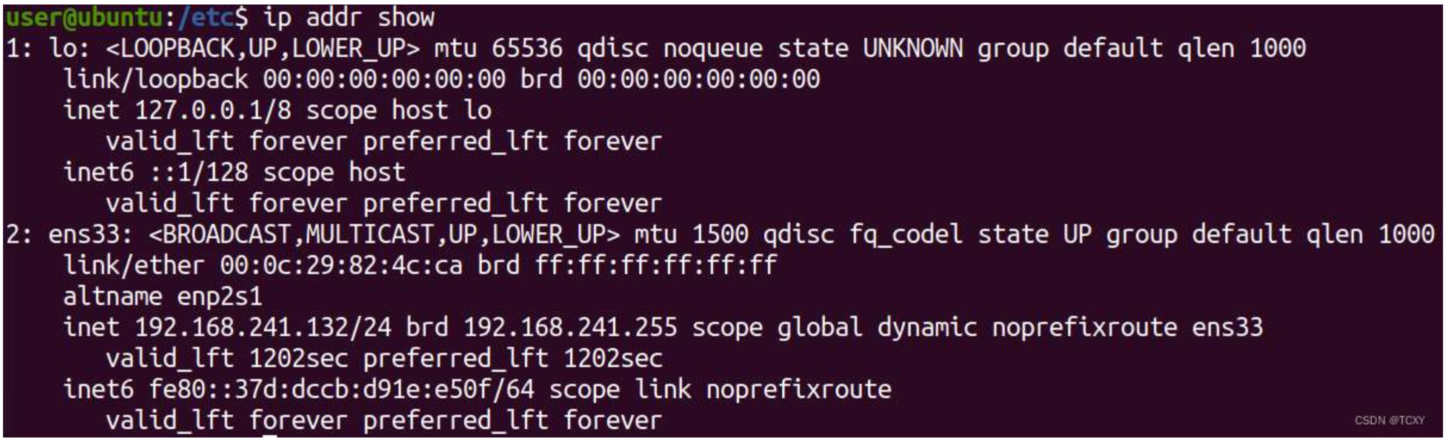
7.3 查看开机自启项 systemctl list-unit-files --type=service



```
user@ubuntu:/etc$ systemctl list-unit-files --type=service
UNIT FILE                                  STATE           VENDOR PRESET
accounts-daemon.service                    enabled         enabled
acpid.service                              disabled        enabled
alsa-restore.service                       static          enabled
alsa-state.service                         static          enabled
alsa-utils.service                         masked          enabled
anacron.service                            enabled         enabled
apparmor.service                           enabled         enabled
apport-autoreport.service                  static          enabled
apport-forward@.service                    static          enabled
apport.service                             generated       enabled
apt-daily-upgrade.service                  static          enabled
apt-daily.service                          static          enabled
autovt@.service                            enabled         enabled
avahi-daemon.service                       enabled         enabled
bluetooth.service                          enabled         enabled
bolt.service                               static          enabled
brltty-udev.service                        static          enabled
brltty.service                             disabled        enabled
clean-mount-point@.service                 static          enabled
colord.service                             static          enabled
configure-printer@.service                 static          enabled
console-getty.service                      disabled        disabled
console-setup.service                      enabled         enabled
container-getty@.service                   static          enabled
cron.service                               enabled         enabled
cryptdisks-early.service                   masked          enabled
cryptdisks.service                         masked          enabled
```

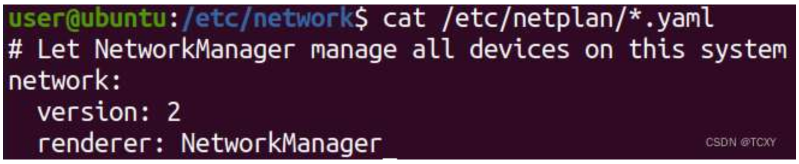
八、网络、路由和通信

8.1 查看网络接口信息 ifconifg 或 ip addr show



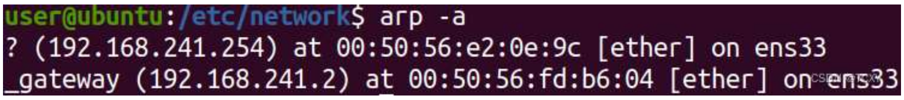
```
user@ubuntu:/etc$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:82:4c:ca brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.241.132/24 brd 192.168.241.255 scope global dynamic noprefixroute ens33
       valid_lft 1202sec preferred_lft 1202sec
    inet6 fe80::37d:dccb:d91e:e50f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

8.2 列出网络接口信息



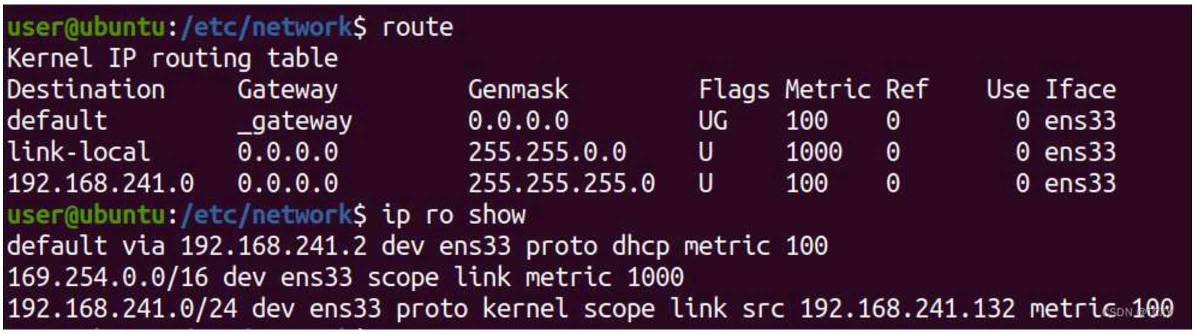
```
user@ubuntu:/etc/network$ cat /etc/netplan/*.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
```

8.3 查看系统arp表 arp -a



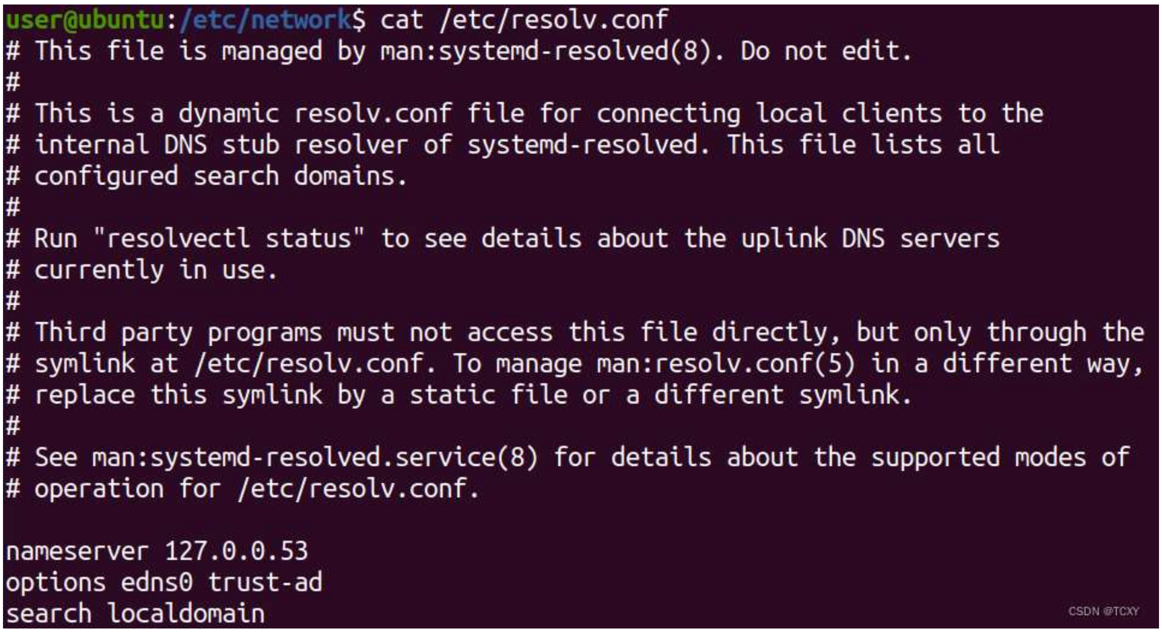
```
user@ubuntu:/etc/network$ arp -a
? (192.168.241.254) at 00:50:56:e2:0e:9c [ether] on ens33
_gateway (192.168.241.2) at 00:50:56:fd:b6:04 [ether] on ens33
```

8.4 查看路由表 route 或 ip ro show



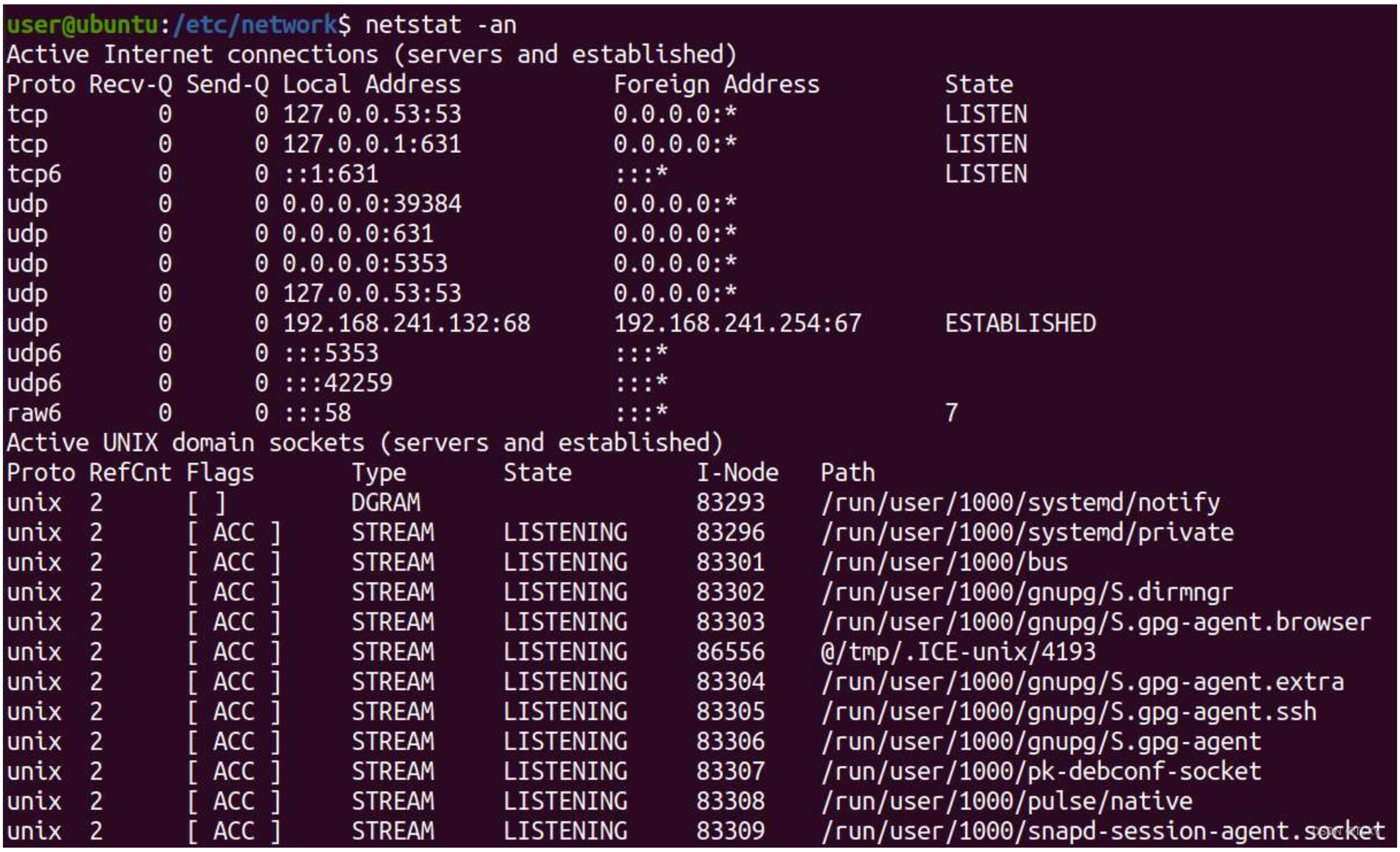
```
user@ubuntu:/etc/network$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 ens33
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 ens33
192.168.241.0   0.0.0.0         255.255.255.0   U     100    0        0 ens33
user@ubuntu:/etc/network$ ip ro show
default via 192.168.241.2 dev ens33 proto dhcp metric 100
169.254.0.0/16 dev ens33 scope link metric 1000
192.168.241.0/24 dev ens33 proto kernel scope link src 192.168.241.132 metric 100
```

8.5 查看DNS配置信息



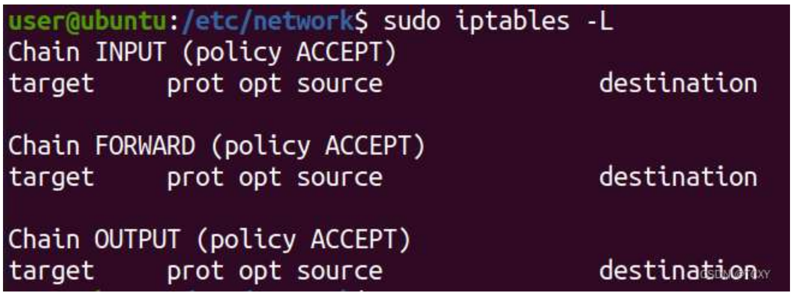
```
user@ubuntu:/etc/network$ cat /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do not edit.
#
# This is a dynamic resolv.conf file for connecting local clients to the
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs must not access this file directly, but only through the
# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
# replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search localdomain
```

8.6 打印本地端口开放信息 netstat -an



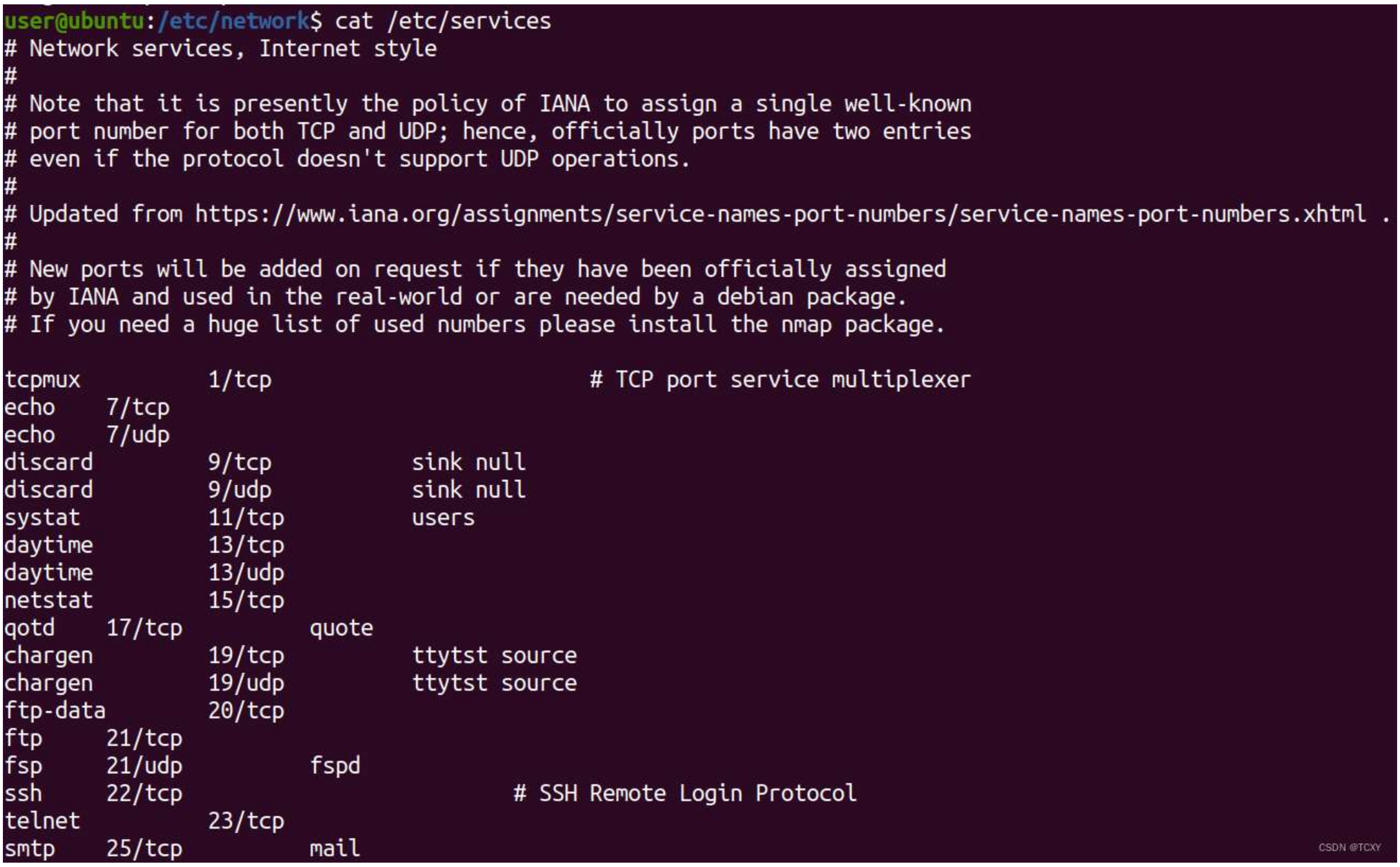
```
user@ubuntu:/etc/network$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 0.0.0.0:39384           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.241.132:68      192.168.241.254:67      ESTABLISHED
udp6       0      0 :::5353                 :::*
udp6       0      0 :::42259                :::*
raw6       0      0 :::58                   :::*                    7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    83293    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     83296    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     83301    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     83302    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     83303    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     86556    @/tmp/.ICE-unix/4193
unix  2      [ ACC ]     STREAM     LISTENING     83304    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     83305    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     83306    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     83307    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     83308    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     83309    /run/user/1000/snapd-session-agent.socket
```

8.7 列出iptable的配置规则 iptables -L



```
user@ubuntu:/etc/network$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

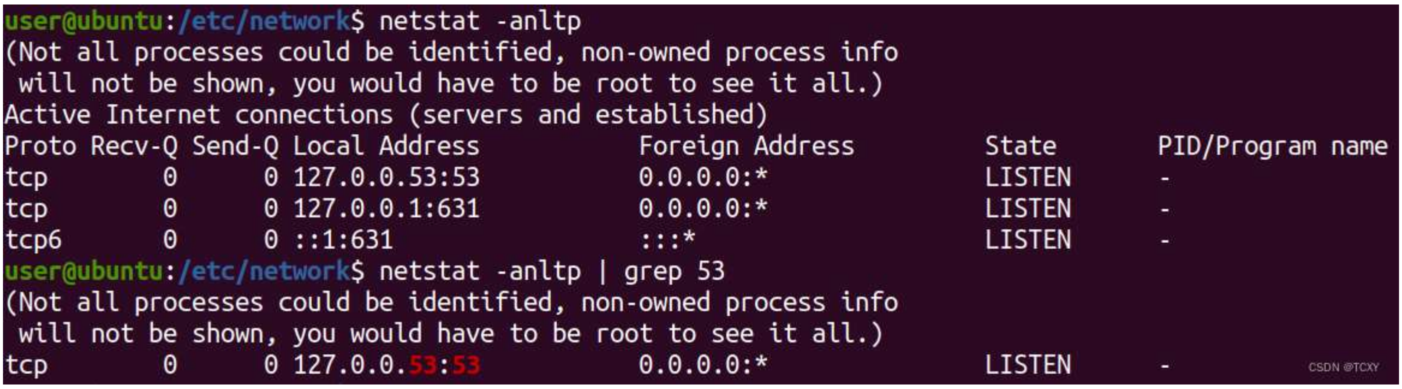
8.8 查看端口服务映射 cat /etc/services



```
user@ubuntu:/etc/network$ cat /etc/services
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, officially ports have two entries
# even if the protocol doesn't support UDP operations.
#
# Updated from https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml .
#
# New ports will be added on request if they have been officially assigned
# by IANA and used in the real-world or are needed by a debian package.
# If you need a huge list of used numbers please install the nmap package.

tcpmux          1/tcp                           # TCP port service multiplexer
echo    7/tcp
echo    7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
daytime         13/tcp
daytime         13/udp
netstat         15/tcp
qotd    17/tcp          quote
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp     21/tcp
fsp     21/udp          fspd
ssh     22/tcp                          # SSH Remote Login Protocol
telnet          23/tcp
smtp    25/tcp          mail
```

CSDN @TCXY

8.9 查看进程端口情况 netstat -anltp | grep $PID

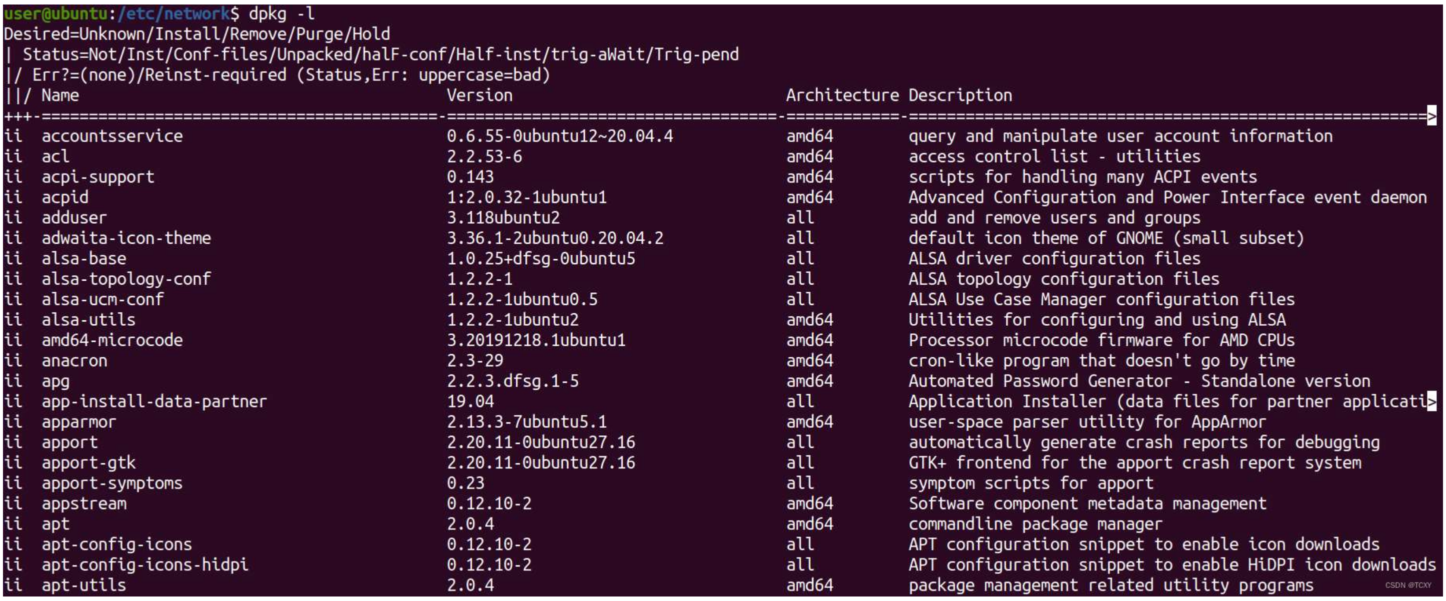


```
user@ubuntu:/etc/network$ netstat -anltp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
user@ubuntu:/etc/network$ netstat -anltp | grep 53
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
```

CSDN @TCXY

九、查看已安装程序

9.1 dpkg -l



```
user@ubuntu:/etc/network$ 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                           0.6.55-0ubuntu12~20.04.4           amd64        query and manipulate user account information
ii  acl                                       2.2.53-6                           amd64        access control list - utilities
ii  acpi-support                              0.143                              amd64        scripts for handling many ACPI events
ii  acpid                                     1:2.0.32-1ubuntu1                  amd64        Advanced Configuration and Power Interface event daemon
ii  adduser                                   3.118ubuntu2                       all          add and remove users and groups
ii  adwaita-icon-theme                        3.36.1-2ubuntu0.20.04.2            all          default icon theme of GNOME (small subset)
ii  alsa-base                                 1.0.25+dfsg-0ubuntu5               all          ALSA driver configuration files
ii  alsa-topology-conf                        1.2.2-1                            all          ALSA topology configuration files
ii  alsa-ucm-conf                             1.2.2-1ubuntu0.5                   all          ALSA Use Case Manager configuration files
ii  alsa-utils                                1.2.2-1ubuntu2                     amd64        Utilities for configuring and using ALSA
ii  amd64-microcode                           3.20191218.1ubuntu1                amd64        Processor microcode firmware for AMD CPUs
ii  anacron                                   2.3-29                             amd64        cron-like program that doesn't go by time
ii  apg                                       2.2.3.dfsg.1-5                     amd64        Automated Password Generator - Standalone version
ii  app-install-data-partner                  19.04                              all          Application Installer (data files for partner applicati>
ii  apparmor                                  2.13.3-7ubuntu5.1                  amd64        user-space parser utility for AppArmor
ii  apport                                    2.20.11-0ubuntu27.16               all          automatically generate crash reports for debugging
ii  apport-gtk                                2.20.11-0ubuntu27.16               all          GTK+ frontend for the apport crash report system
ii  apport-symptoms                           0.23                               all          symptom scripts for apport
ii  appstream                                 0.12.10-2                          amd64        Software component metadata management
ii  apt                                       2.0.4                              amd64        commandline package manager
ii  apt-config-icons                          0.12.10-2                          all          APT configuration snippet to enable icon downloads
ii  apt-config-icons-hidpi                    0.12.10-2                          all          APT configuration snippet to enable HiDPI icon downloads
ii  apt-utils                                 2.0.4                              amd64        package management related utility programs
```

CSDN @TCXY

十、日志

10.1 /var/log/boot.log

- 这个文件包含了系统引导过程中产生的日志信息，如内核启动消息、系统服务的启动等。

10.2 /var/log/cron

- 这个文件记录了 cron 定时任务的执行情况，包括定时任务的执行结果和错误信息。

10.3 /var/log/faillog

- 这个文件记录了登录失败的信息，包括登录失败的用户和登录尝试的时间等。

10.4 /var/log/lastlog

- 这个文件记录了系统上所有用户最后一次登录的相关信息，如最后登录时间和登录位置等。

10.5 /var/log/messages

- 这个文件包含了系统和应用程序产生的一般性日志信息，通常是一些系统事件、警告和错误信息。

10.6 /var/log/secure

- 这个文件记录了与系统安全相关的日志信息，如用户的登录和认证信息。

10.7 /var/log/syslog

- 这个文件包含了系统日志的大部分信息，包括内核消息、系统服务的日志等。

10.8 /var/log/wtmp

- 这个文件记录了用户的登录和注销信息，可以用于查看用户登录系统的历史记录。

10.9 /var/log/utmp

- 这个文件包含了当前已登录用户的信息，包括用户名、终端、登录时间等。