Fireside Friday's

Linux CLI - 101
Week 2

Thanks to our sponsors!

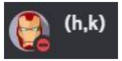
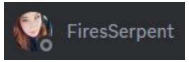
ACTIVE COUNTERMEASURES

BLACK HILLS
Information Security
• 2008 •

WILD WEST
HACKIN' FEST

Antisyphon Training

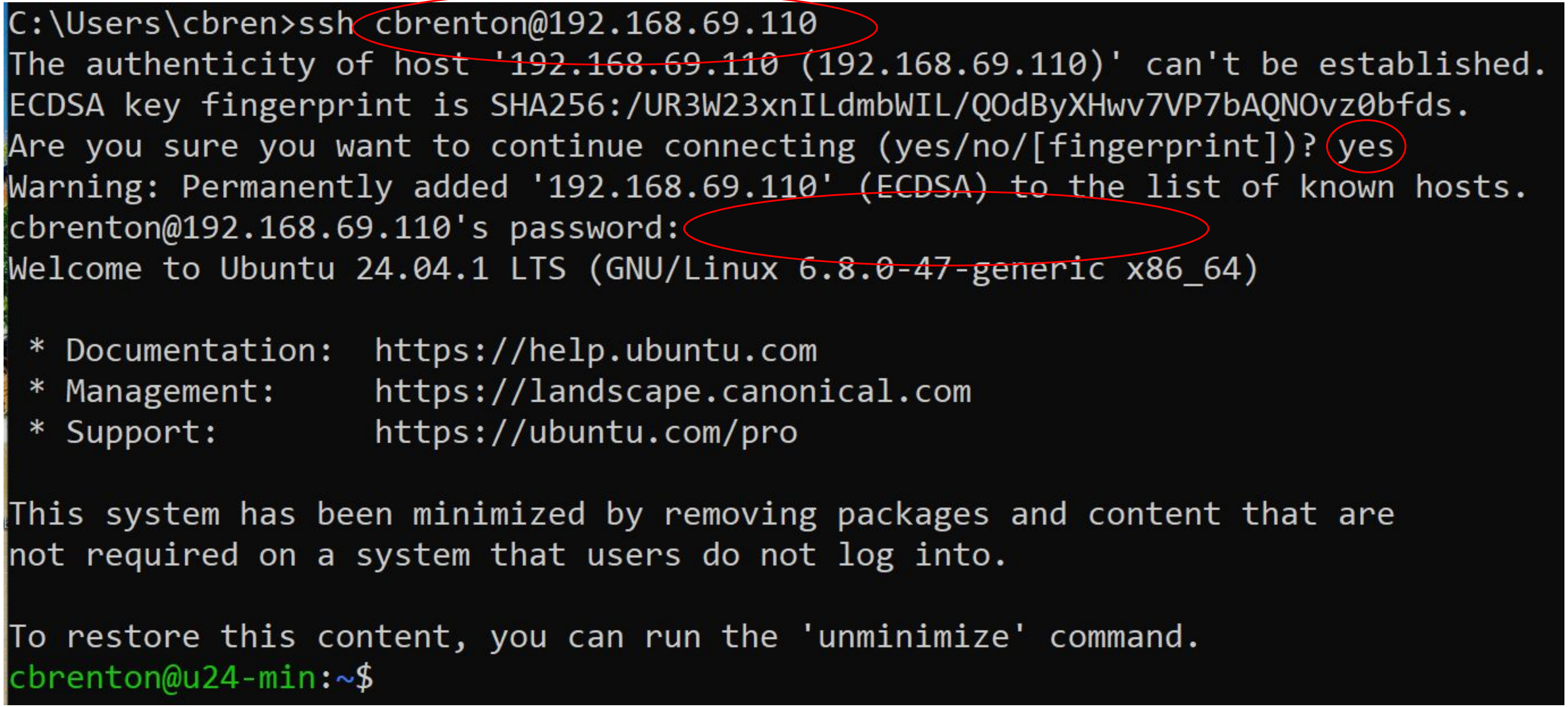
Special Thanks to…

- Hermon  (h,k)
- Emily  FiresSerpent
- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thanks" the next time you see them online

Lab requirements for this section

- Access to a modern Linux system
- Can be a VM or public cloud instance
- Need "sudo" access for some labs
- I'll be working with Ubuntu 24 LTS

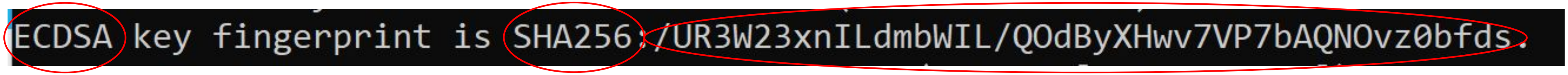
SSH to your Linux system



```
C:\Users\cbren>ssh cbrenton@192.168.69.110
The authenticity of host '192.168.69.110 (192.168.69.110)' can't be established.
ECDSA key fingerprint is SHA256:/UR3W23xnILdmbWIL/QOdByXHwv7VP7bAQNOvz0bfds.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.69.110' (ECDSA) to the list of known hosts.
cbrenton@192.168.69.110's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
cbrenton@u24-min:~$
```

Checking the SSH server key

First login provided info:

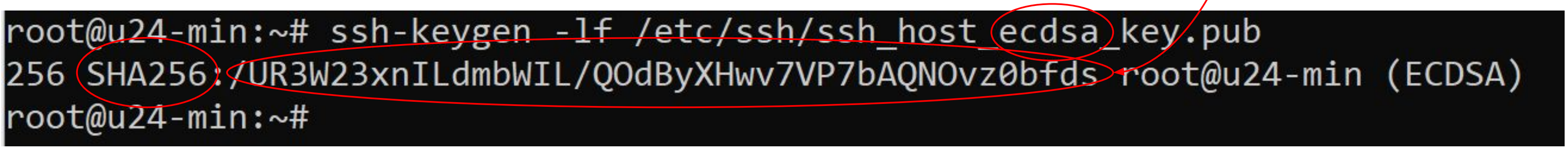


```
ECDSA key fingerprint is SHA256:/UR3W23xnILdmbWIL/QOdByXHwv7VP7bAQNOvz0bfds.
```

Perform at the console or by verified user:

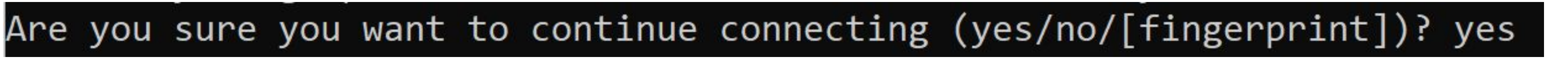
```
ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub
```

These values should match



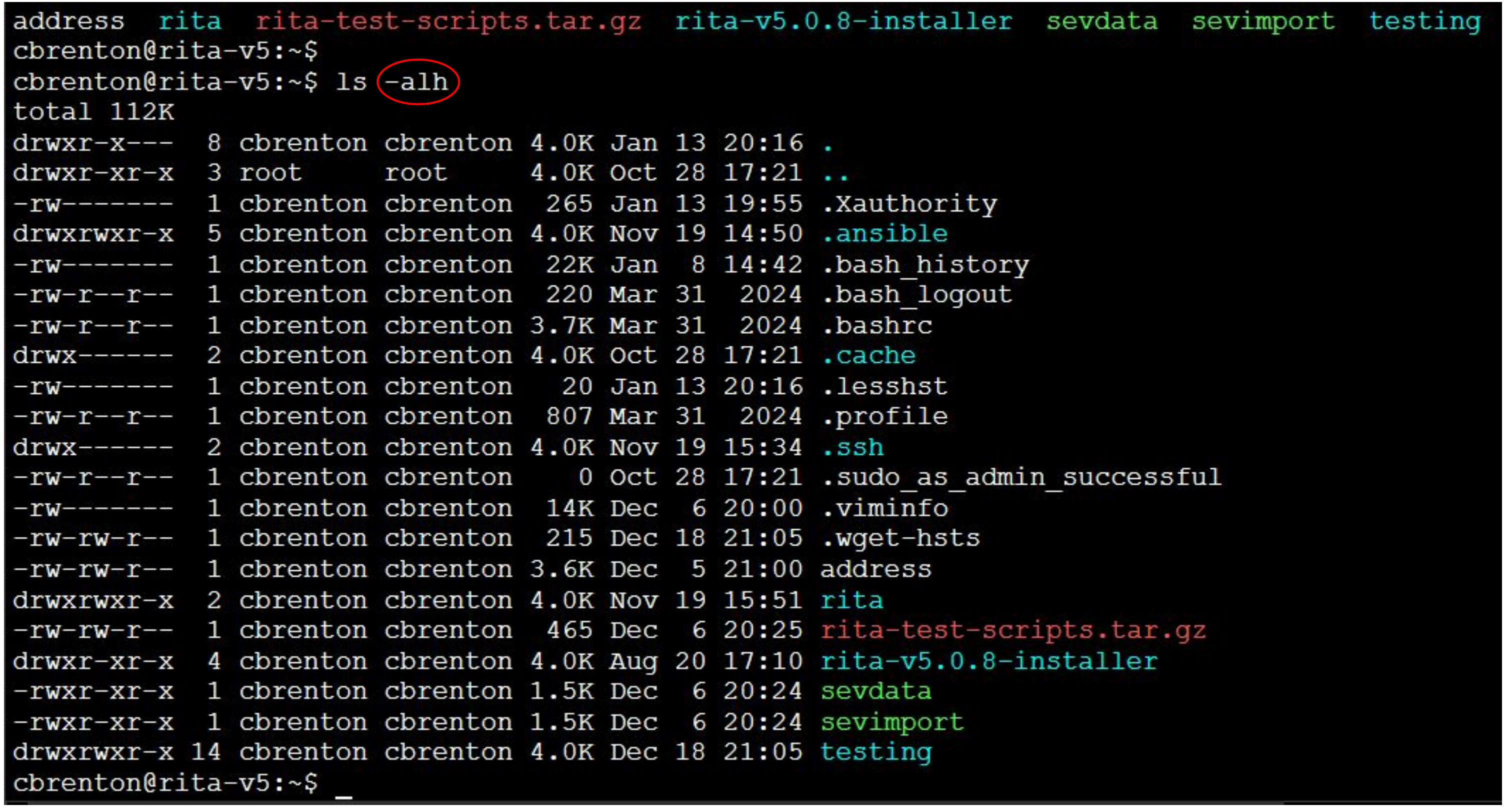
```
root@u24-min:~# ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub
256 SHA256:/UR3W23xnILdmbWIL/QOdByXHwv7VP7bAQNOvz0bfds root@u24-min (ECDSA)
root@u24-min:~#
```

To be done before answering "yes"



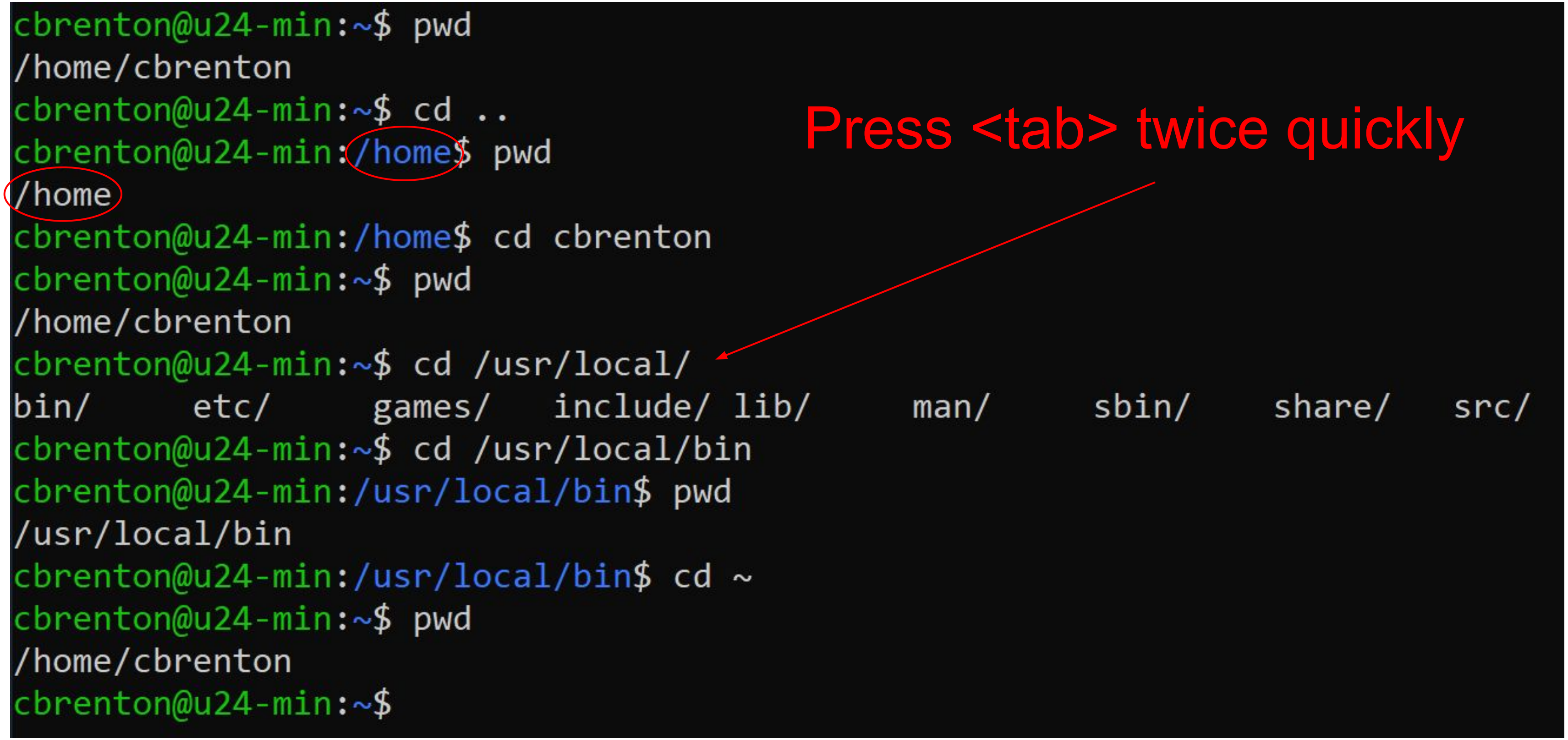
```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

"ls" = Listing files and directories



```
address  rita  rita-test-scripts.tar.gz  rita-v5.0.8-installer  sevdata  sevimport  testing
cbrenton@rita-v5:~$
cbrenton@rita-v5:~$ ls -alh
total 112K
drwxr-x---  8 cbrenton cbrenton 4.0K Jan 13 20:16 .
drwxr-xr-x  3 root     root     4.0K Oct 28 17:21 ..
-rw-------  1 cbrenton cbrenton  265 Jan 13 19:55 .Xauthority
drwxrwxr-x  5 cbrenton cbrenton 4.0K Nov 19 14:50 .ansible
-rw-------  1 cbrenton cbrenton  22K Jan  8 14:42 .bash_history
-rw-r--r--  1 cbrenton cbrenton  220 Mar 31  2024 .bash_logout
-rw-r--r--  1 cbrenton cbrenton 3.7K Mar 31  2024 .bashrc
drwx------  2 cbrenton cbrenton 4.0K Oct 28 17:21 .cache
-rw-------  1 cbrenton cbrenton   20 Jan 13 20:16 .lesshst
-rw-r--r--  1 cbrenton cbrenton  807 Mar 31  2024 .profile
drwx------  2 cbrenton cbrenton 4.0K Nov 19 15:34 .ssh
-rw-r--r--  1 cbrenton cbrenton    0 Oct 28 17:21 .sudo_as_admin_successful
-rw-------  1 cbrenton cbrenton  14K Dec  6 20:00 .viminfo
-rw-rw-r--  1 cbrenton cbrenton  215 Dec 18 21:05 .wget-hsts
-rw-rw-r--  1 cbrenton cbrenton 3.6K Dec  5 21:00 address
drwxrwxr-x  2 cbrenton cbrenton 4.0K Nov 19 15:51 rita
-rw-rw-r--  1 cbrenton cbrenton  465 Dec  6 20:25 rita-test-scripts.tar.gz
drwxr-xr-x  4 cbrenton cbrenton 4.0K Aug 20 17:10 rita-v5.0.8-installer
-rwxr-xr-x  1 cbrenton cbrenton 1.5K Dec  6 20:24 sevdata
-rwxr-xr-x  1 cbrenton cbrenton 1.5K Dec  6 20:24 sevimport
drwxrwxr-x 14 cbrenton cbrenton 4.0K Dec 18 21:05 testing
cbrenton@rita-v5:~$ _
```

cd = change directory, <tab> = autocomplete

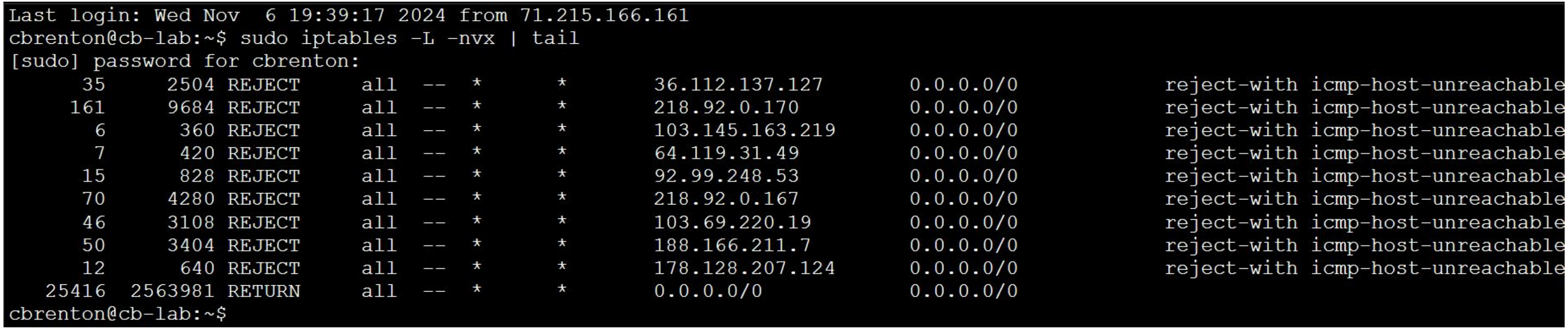


```
cbrenton@u24-min:~$ pwd
/home/cbrenton
cbrenton@u24-min:~$ cd ..
cbrenton@u24-min:/home$ pwd
/home
cbrenton@u24-min:/home$ cd cbrenton
cbrenton@u24-min:~$ pwd
/home/cbrenton
cbrenton@u24-min:~$ cd /usr/local/
bin/     etc/     games/   include/ lib/     man/     sbin/    share/   src/
cbrenton@u24-min:~$ cd /usr/local/bin
cbrenton@u24-min:/usr/local/bin$ pwd
/usr/local/bin
cbrenton@u24-min:/usr/local/bin$ cd ~
cbrenton@u24-min:~$ pwd
/home/cbrenton
cbrenton@u24-min:~$
```

Press <tab> twice quickly

sudo = Run command as another user

```
sudo iptables -L -nvx
```



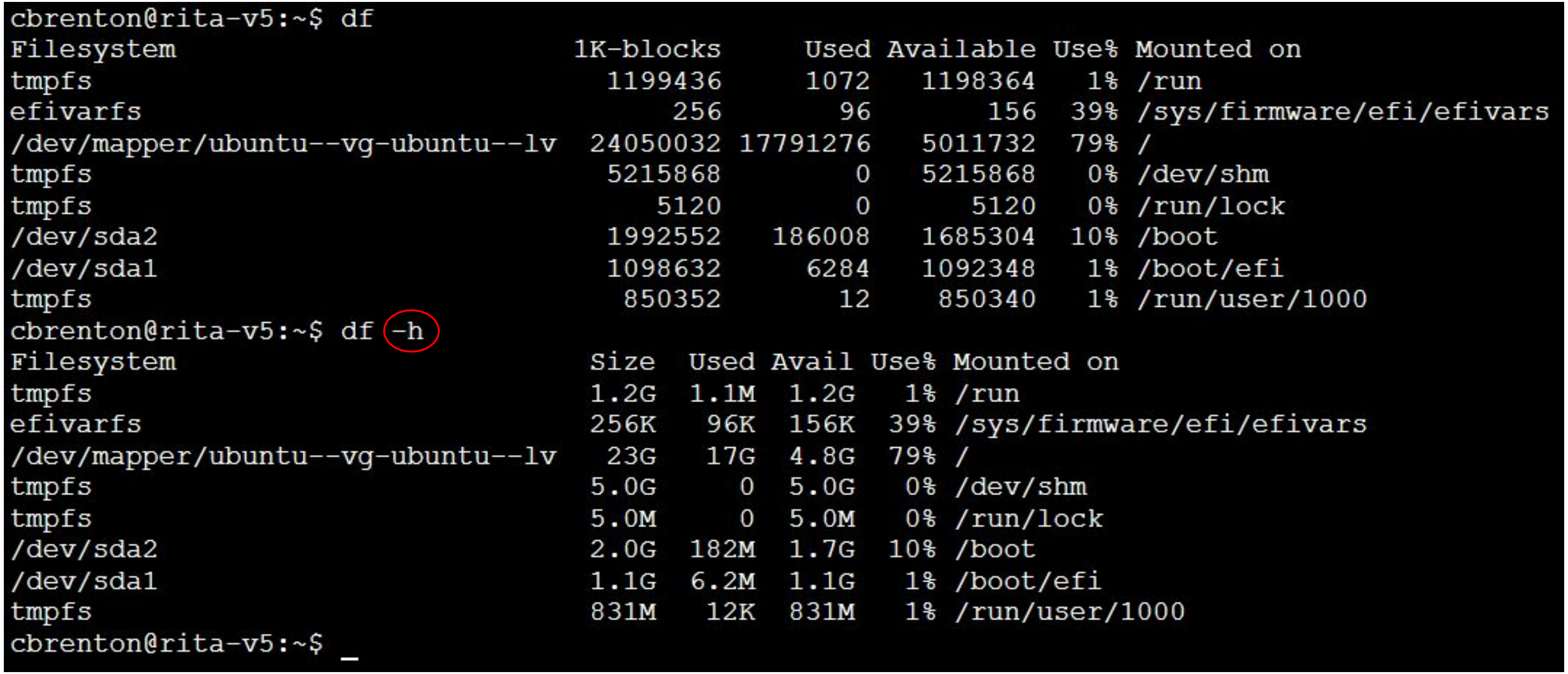
```
Last login: Wed Nov  6 19:39:17 2024 from 71.215.166.161
cbrenton@cb-lab:~$ sudo iptables -L -nvx | tail
[sudo] password for cbrenton:
      35     2504 REJECT     all  --  *      *       36.112.137.127       0.0.0.0/0           reject-with icmp-host-unreachable
     161     9684 REJECT     all  --  *      *       218.92.0.170         0.0.0.0/0           reject-with icmp-host-unreachable
       6      360 REJECT     all  --  *      *       103.145.163.219      0.0.0.0/0           reject-with icmp-host-unreachable
       7      420 REJECT     all  --  *      *       64.119.31.49         0.0.0.0/0           reject-with icmp-host-unreachable
      15      828 REJECT     all  --  *      *       92.99.248.53         0.0.0.0/0           reject-with icmp-host-unreachable
      70     4280 REJECT     all  --  *      *       218.92.0.167         0.0.0.0/0           reject-with icmp-host-unreachable
      46     3108 REJECT     all  --  *      *       103.69.220.19        0.0.0.0/0           reject-with icmp-host-unreachable
      50     3404 REJECT     all  --  *      *       188.166.211.7        0.0.0.0/0           reject-with icmp-host-unreachable
      12      640 REJECT     all  --  *      *       178.128.207.124      0.0.0.0/0           reject-with icmp-host-unreachable
   25416  2563981 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
cbrenton@cb-lab:~$
```

When the user is not specified, "root" is assumed

Needed to run high privilege commands

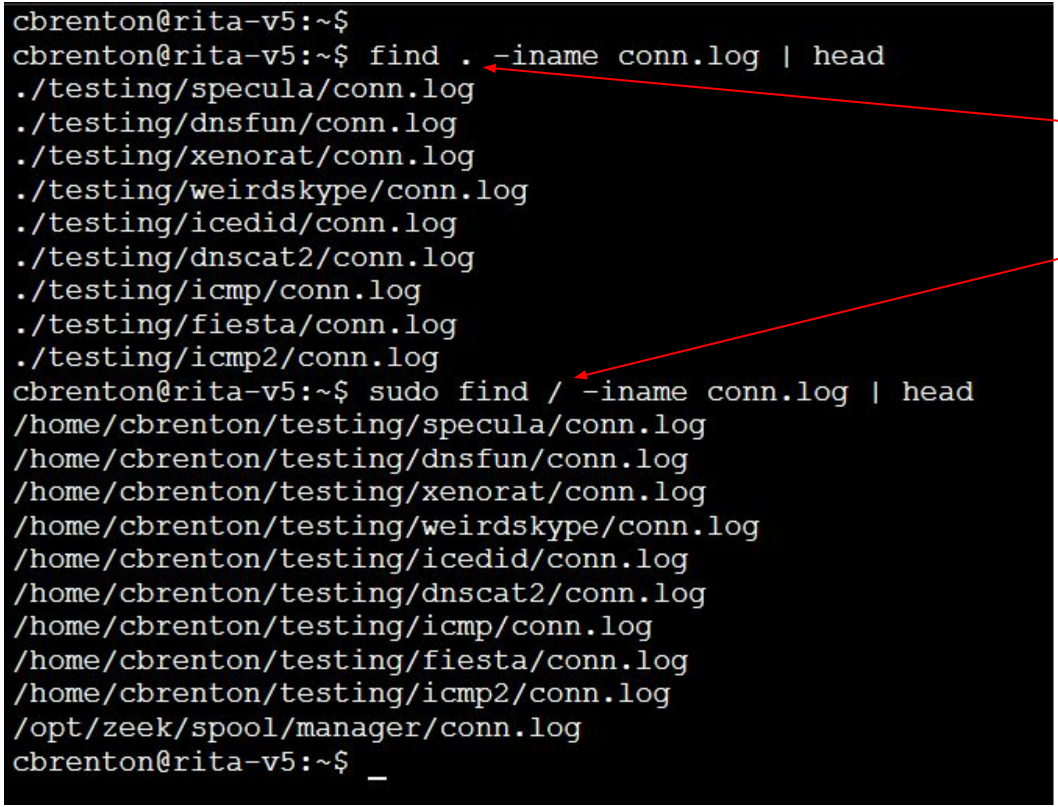
Need to be part of "sudo" group to use it

df = Report available disk space



```
cbrenton@rita-v5:~$ df
Filesystem                        1K-blocks     Used Available Use% Mounted on
tmpfs                               1199436     1072   1198364   1% /run
efivarfs                                256       96       156  39% /sys/firmware/efi/efivars
/dev/mapper/ubuntu--vg-ubuntu--lv  24050032 17791276   5011732  79% /
tmpfs                               5215868        0   5215868   0% /dev/shm
tmpfs                                  5120        0      5120   0% /run/lock
/dev/sda2                           1992552   186008   1685304  10% /boot
/dev/sda1                           1098632     6284   1092348   1% /boot/efi
tmpfs                                850352       12    850340   1% /run/user/1000
cbrenton@rita-v5:~$ df -h
Filesystem                         Size  Used Avail Use% Mounted on
tmpfs                              1.2G  1.1M  1.2G   1% /run
efivarfs                           256K   96K  156K  39% /sys/firmware/efi/efivars
/dev/mapper/ubuntu--vg-ubuntu--lv   23G   17G  4.8G  79% /
tmpfs                              5.0G     0  5.0G   0% /dev/shm
tmpfs                              5.0M     0  5.0M   0% /run/lock
/dev/sda2                          2.0G  182M  1.7G  10% /boot
/dev/sda1                          1.1G  6.2M  1.1G   1% /boot/efi
tmpfs                              831M   12K  831M   1% /run/user/1000
cbrenton@rita-v5:~$ _
```

Finding files with "find"



```
cbrenton@rita-v5:~$
cbrenton@rita-v5:~$ find . -iname conn.log | head
./testing/specula/conn.log
./testing/dnsfun/conn.log
./testing/xenorat/conn.log
./testing/weirdskype/conn.log
./testing/icedid/conn.log
./testing/dnscat2/conn.log
./testing/icmp/conn.log
./testing/fiesta/conn.log
./testing/icmp2/conn.log
cbrenton@rita-v5:~$ sudo find / -iname conn.log | head
/home/cbrenton/testing/specula/conn.log
/home/cbrenton/testing/dnsfun/conn.log
/home/cbrenton/testing/xenorat/conn.log
/home/cbrenton/testing/weirdskype/conn.log
/home/cbrenton/testing/icedid/conn.log
/home/cbrenton/testing/dnscat2/conn.log
/home/cbrenton/testing/icmp/conn.log
/home/cbrenton/testing/fiesta/conn.log
/home/cbrenton/testing/icmp2/conn.log
/opt/zeek/spool/manager/conn.log
cbrenton@rita-v5:~$ _
```

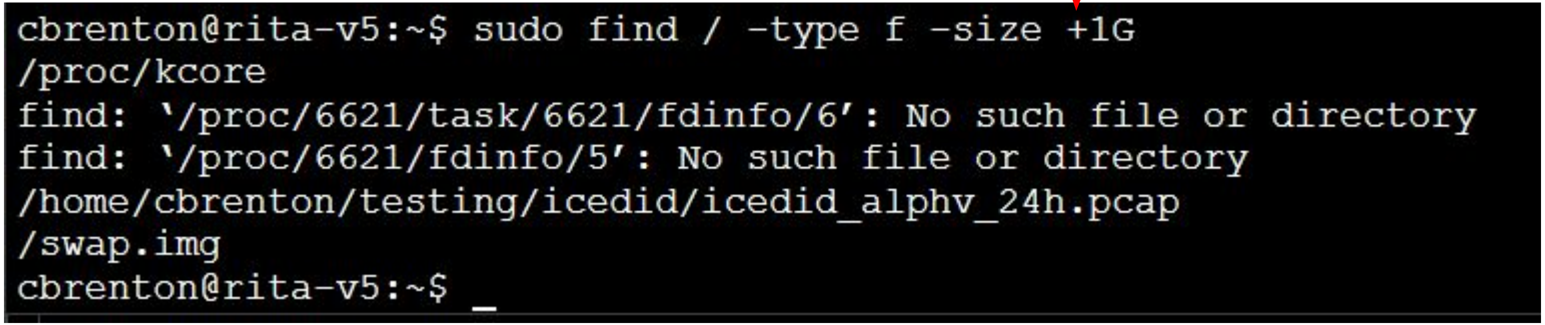
Search from this directory down

Search entire drive
Use "sudo" to avoid read errors

Wildcards can be used

Find files by size

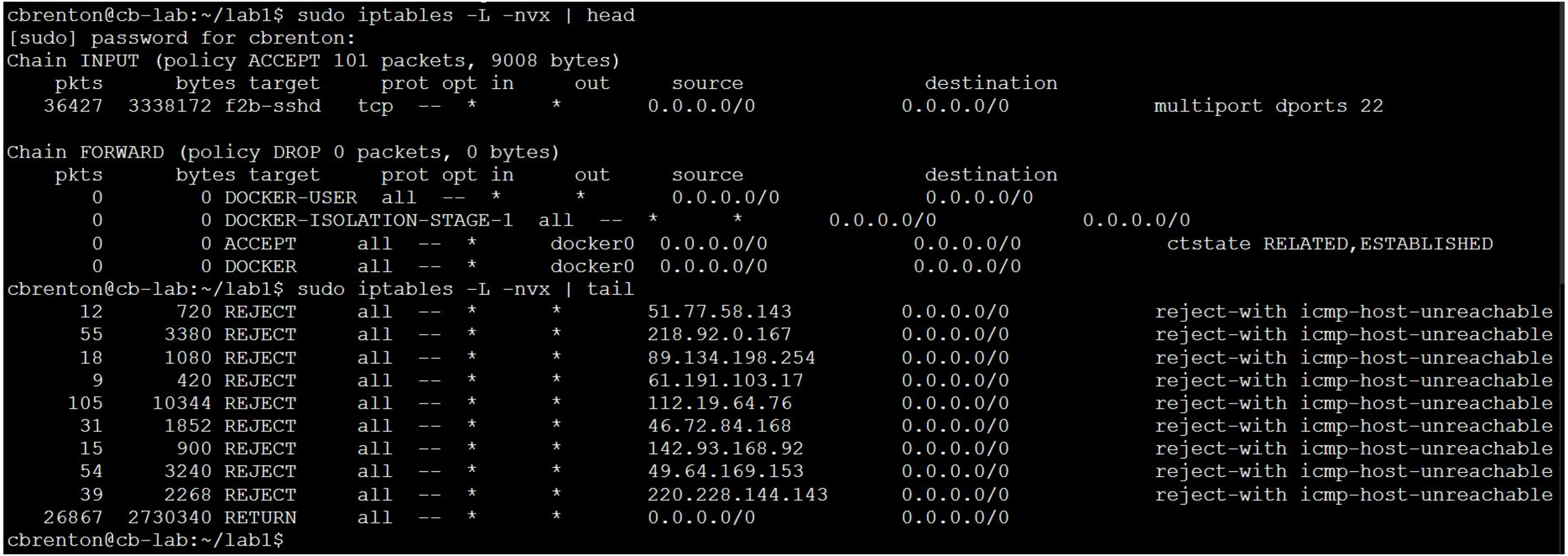
Specified size or larger



```
cbrenton@rita-v5:~$ sudo find / -type f -size +1G
/proc/kcore
find: ‘/proc/6621/task/6621/fdinfo/6’: No such file or directory
find: ‘/proc/6621/fdinfo/5’: No such file or directory
/home/cbrenton/testing/icedid/icedid_alphv_24h.pcap
/swap.img
cbrenton@rita-v5:~$ _
```

Read errors in "/proc/" are common

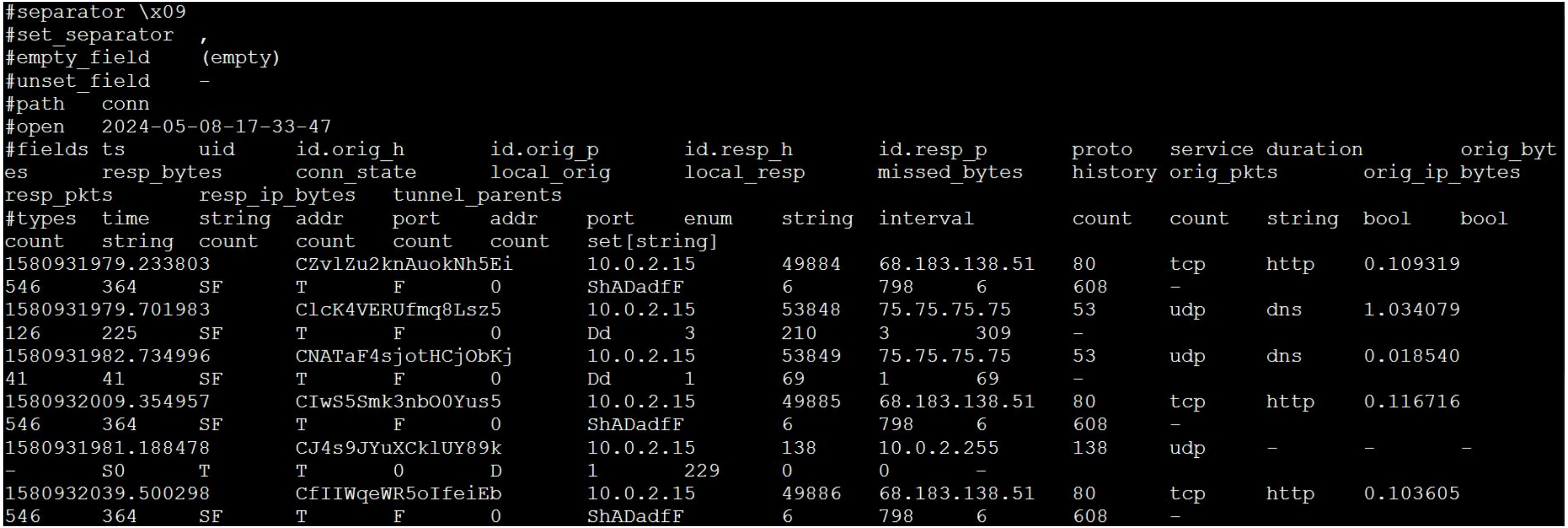
head = first 10 lines, tail = last 10 lines



```
cbrenton@cb-lab:~/lab1$ sudo iptables -L -nvx | head
[sudo] password for cbrenton:
Chain INPUT (policy ACCEPT 101 packets, 9008 bytes)
    pkts      bytes target     prot opt in     out     source               destination
   36427  3338172 f2b-sshd   tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            multiport dports 22

Chain FORWARD (policy DROP 0 packets, 0 bytes)
    pkts      bytes target     prot opt in     out     source               destination
       0        0 DOCKER-USER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 DOCKER-ISOLATION-STAGE-1  all  --  *      *       0.0.0.0/0            0.0.0.0/0
       0        0 ACCEPT     all  --  *      docker0  0.0.0.0/0            0.0.0.0/0            ctstate RELATED,ESTABLISHED
       0        0 DOCKER     all  --  *      docker0  0.0.0.0/0            0.0.0.0/0
cbrenton@cb-lab:~/lab1$ sudo iptables -L -nvx | tail
      12      720 REJECT     all  --  *      *       51.77.58.143         0.0.0.0/0            reject-with icmp-host-unreachable
      55     3380 REJECT     all  --  *      *       218.92.0.167         0.0.0.0/0            reject-with icmp-host-unreachable
      18     1080 REJECT     all  --  *      *       89.134.198.254       0.0.0.0/0            reject-with icmp-host-unreachable
       9      420 REJECT     all  --  *      *       61.191.103.17        0.0.0.0/0            reject-with icmp-host-unreachable
     105    10344 REJECT     all  --  *      *       112.19.64.76         0.0.0.0/0            reject-with icmp-host-unreachable
      31     1852 REJECT     all  --  *      *       46.72.84.168         0.0.0.0/0            reject-with icmp-host-unreachable
      15      900 REJECT     all  --  *      *       142.93.168.92        0.0.0.0/0            reject-with icmp-host-unreachable
      54     3240 REJECT     all  --  *      *       49.64.169.153        0.0.0.0/0            reject-with icmp-host-unreachable
      39     2268 REJECT     all  --  *      *       220.228.144.143      0.0.0.0/0            reject-with icmp-host-unreachable
   26867  2730340 RETURN     all  --  *      *       0.0.0.0/0            0.0.0.0/0
cbrenton@cb-lab:~/lab1$
```

Adding "-<number> to either changes the # of lines of output

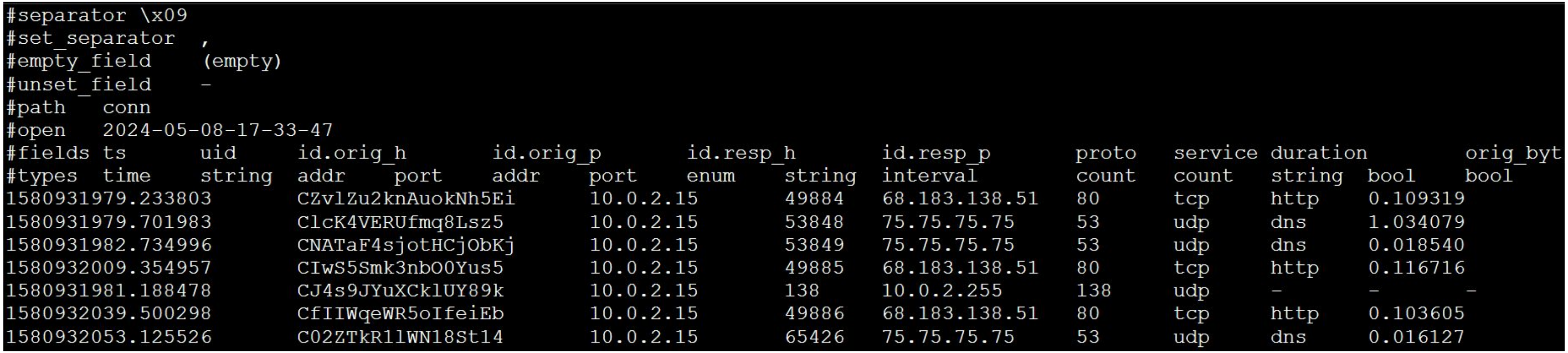
less = pause output at single page



```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2024-05-08-17-33-47
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_byt
es      resp_bytes      conn_state      local_orig      local_resp      missed_bytes    history orig_pkts       orig_ip_bytes
resp_pkts       resp_ip_bytes   tunnel_parents
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool
count   string  count   count   count   count   set[string]
1580931979.233803       CZvlZu2knAuokNh5Ei      10.0.2.15       49884   68.183.138.51   80      tcp     http    0.109319
546     364     SF      T       F       0       ShADadfF        6       798     6       608     -
1580931979.701983       ClcK4VERUfmq8Lsz5       10.0.2.15       53848   75.75.75.75     53      udp     dns     1.034079
126     225     SF      T       F       0       Dd      3       210     3       309     -
1580931982.734996       CNATaF4sjotHCjObKj      10.0.2.15       53849   75.75.75.75     53      udp     dns     0.018540
41      41      SF      T       F       0       Dd      1       69      1       69      -
1580932009.354957       CIwS5Smk3nbO0Yus5       10.0.2.15       49885   68.183.138.51   80      tcp     http    0.116716
546     364     SF      T       F       0       ShADadfF        6       798     6       608     -
1580931981.188478       CJ4s9JYuXCklUY89k       10.0.2.15       138     10.0.2.255      138     udp     -       -       -
-       S0      T       T       0       D       1       229     0       0       -
1580932039.500298       CfIIWqeWR5oIfeiEb       10.0.2.15       49886   68.183.138.51   80      tcp     http    0.103605
546     364     SF      T       F       0       ShADadfF        6       798     6       608     -
```

Arrow keys, page up/down to navigate
"q" to quit

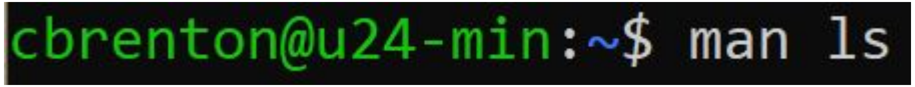
less -S = Prevent line wrapping



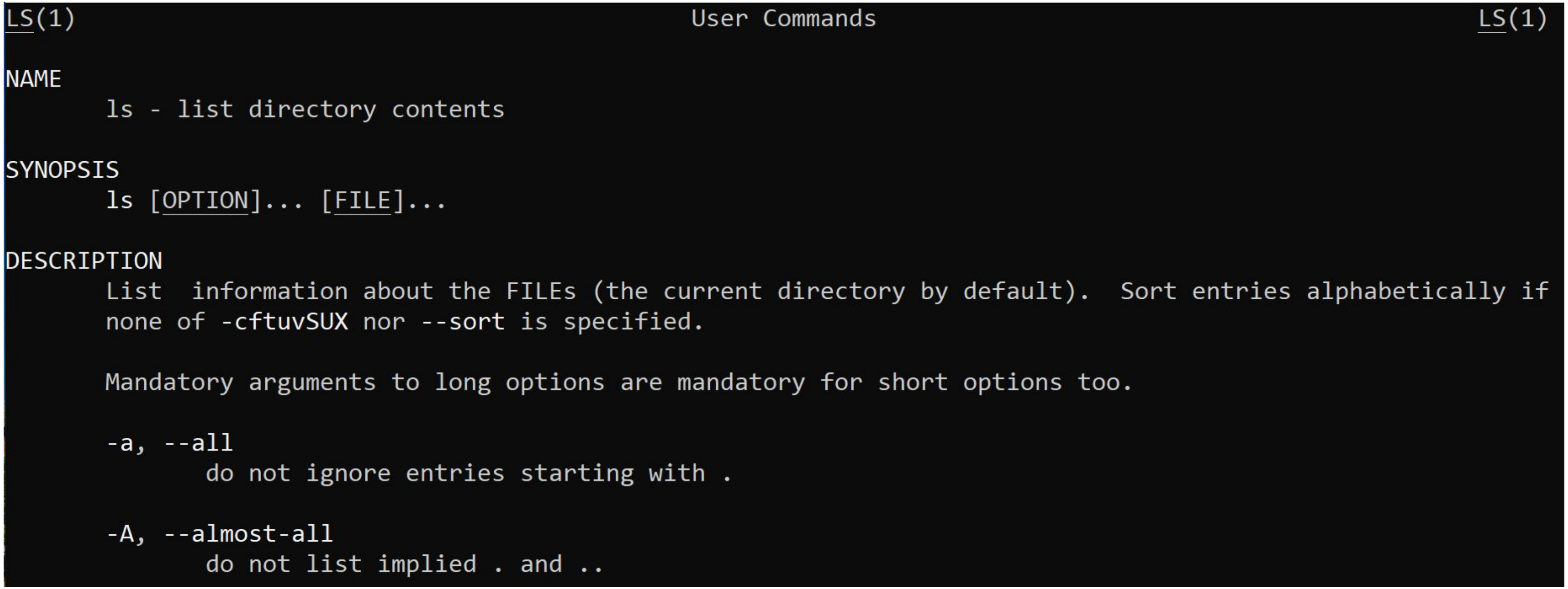
```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   conn
#open   2024-05-08-17-33-47
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_byt
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool
1580931979.233803       CZvlZu2knAuokNh5Ei      10.0.2.15       49884   68.183.138.51   80      tcp     http    0.109319
1580931979.701983       ClcK4VERUfmq8Lsz5       10.0.2.15       53848   75.75.75.75     53      udp     dns     1.034079
1580931982.734996       CNATaF4sjotHCjObKj      10.0.2.15       53849   75.75.75.75     53      udp     dns     0.018540
1580932009.354957       CIwS5Smk3nbO0Yus5       10.0.2.15       49885   68.183.138.51   80      tcp     http    0.116716
1580931981.188478       CJ4s9JYuXCklUY89k       10.0.2.15       138     10.0.2.255      138     udp     -       -       -
1580932039.500298       CfIIWqeWR5oIfeiEb       10.0.2.15       49886   68.183.138.51   80      tcp     http    0.103605
1580932053.125526       C02ZTkR1lWN18St14       10.0.2.15       65426   75.75.75.75     53      udp     dns     0.016127
```

Right arrow to see data off side of screen

man <command> = online help

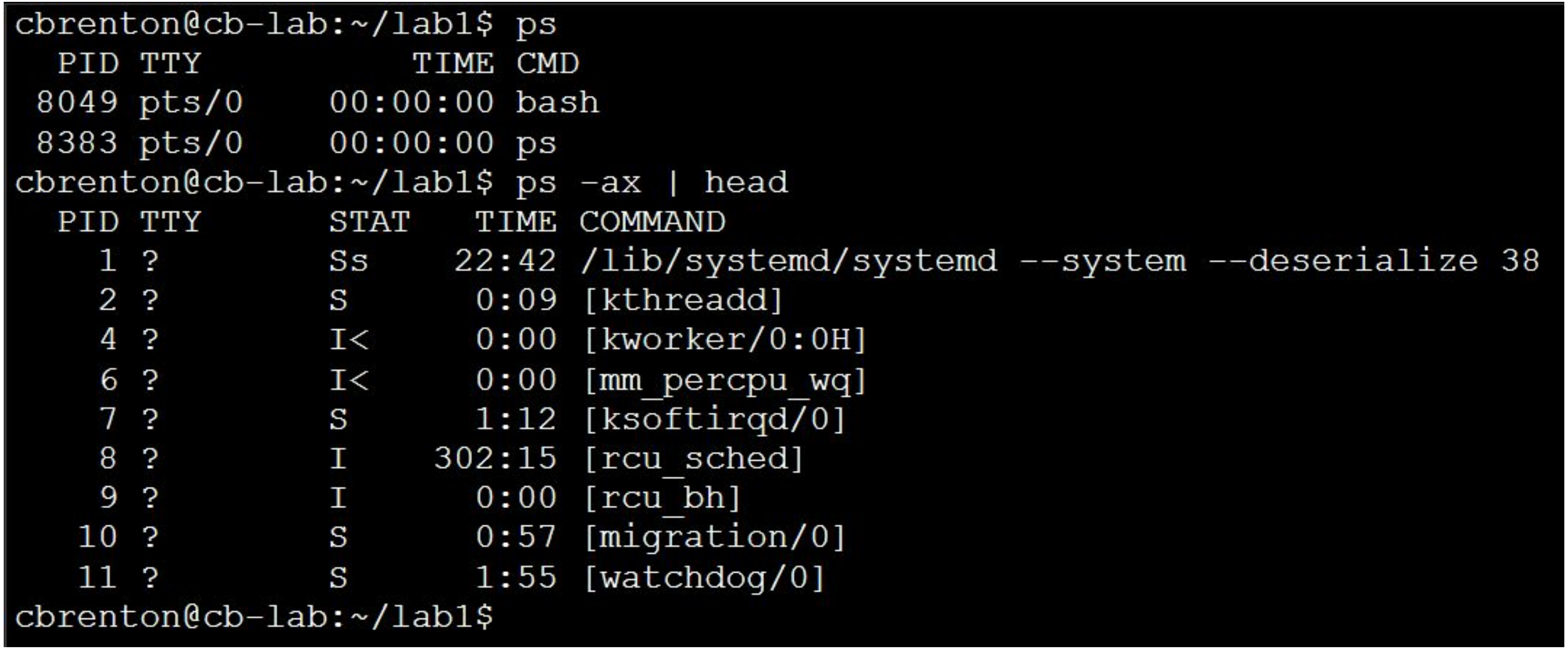


```
cbrenton@u24-min:~$ man ls
```



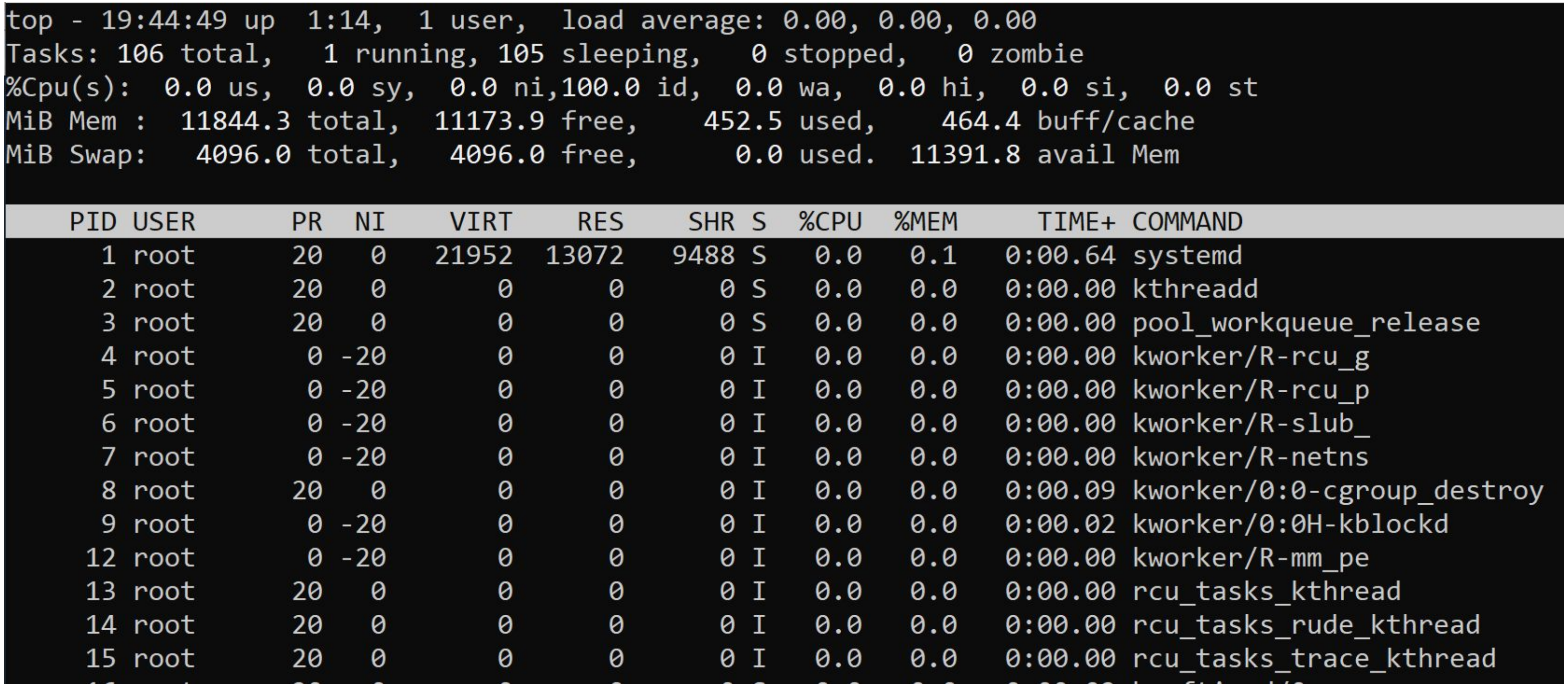
```
LS(1)                                    User Commands                                   LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List  information about the FILEs (the current directory by default).  Sort entries alphabetically if
       none of -cftuvSUX nor --sort is specified.

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..
```

ps = View running processes



```
cbrenton@cb-lab:~/lab1$ ps
  PID TTY          TIME CMD
 8049 pts/0    00:00:00 bash
 8383 pts/0    00:00:00 ps
cbrenton@cb-lab:~/lab1$ ps -ax | head
  PID TTY      STAT   TIME COMMAND
    1 ?        Ss    22:42 /lib/systemd/systemd --system --deserialize 38
    2 ?        S      0:09 [kthreadd]
    4 ?        I<     0:00 [kworker/0:0H]
    6 ?        I<     0:00 [mm_percpu_wq]
    7 ?        S      1:12 [ksoftirqd/0]
    8 ?        I    302:15 [rcu_sched]
    9 ?        I      0:00 [rcu_bh]
   10 ?        S      0:57 [migration/0]
   11 ?        S      1:55 [watchdog/0]
cbrenton@cb-lab:~/lab1$
```

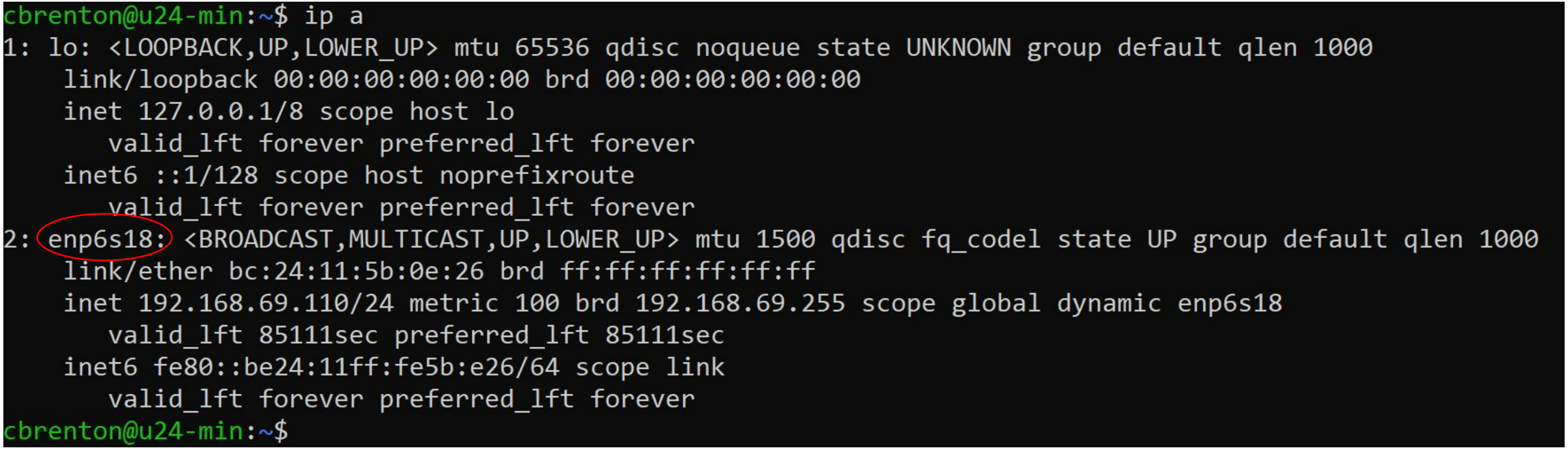
top = See CPU, memory & process stats



```
top - 19:44:49 up  1:14,  1 user,  load average: 0.00, 0.00, 0.00
Tasks: 106 total,   1 running, 105 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :  11844.3 total,  11173.9 free,    452.5 used,    464.4 buff/cache
MiB Swap:   4096.0 total,   4096.0 free,      0.0 used.  11391.8 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
      1 root      20   0   21952  13072   9488 S   0.0   0.1   0:00.64 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kthreadd
      3 root      20   0       0      0      0 S   0.0   0.0   0:00.00 pool_workqueue_release
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_g
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-rcu_p
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-slub_
      7 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-netns
      8 root      20   0       0      0      0 I   0.0   0.0   0:00.09 kworker/0:0-cgroup_destroy
      9 root       0 -20       0      0      0 I   0.0   0.0   0:00.02 kworker/0:0H-kblockd
     12 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/R-mm_pe
     13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_kthread
     14 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_rude_kthread
     15 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tasks_trace_kthread
```

Press "q" to quit this screen

ip = Show system IP address info

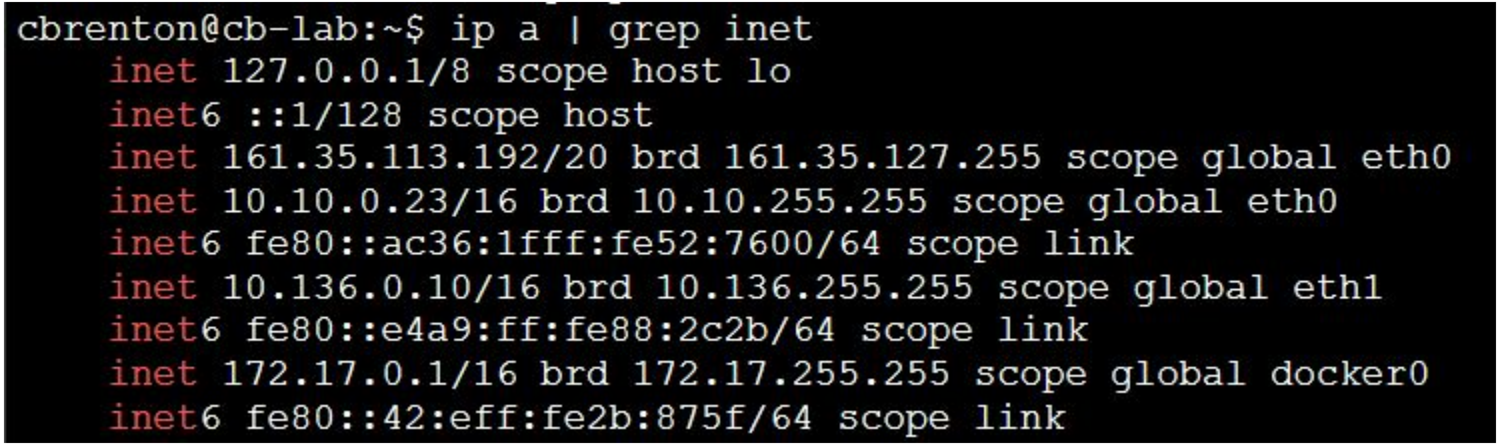


```
cbrenton@u24-min:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp6s18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:5b:0e:26 brd ff:ff:ff:ff:ff:ff
    inet 192.168.69.110/24 metric 100 brd 192.168.69.255 scope global dynamic enp6s18
       valid_lft 85111sec preferred_lft 85111sec
    inet6 fe80::be24:11ff:fe5b:e26/64 scope link
       valid_lft forever preferred_lft forever
cbrenton@u24-min:~$
```

Please note your interface name for a later slide

Matching patterns with grep

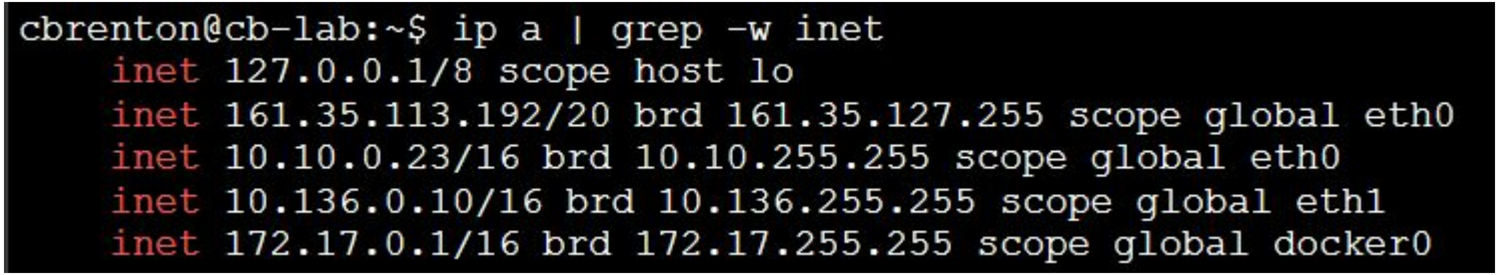
```
ip a| grep inet
```



```
cbrenton@cb-lab:~$ ip a | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 161.35.113.192/20 brd 161.35.127.255 scope global eth0
    inet 10.10.0.23/16 brd 10.10.255.255 scope global eth0
    inet6 fe80::ac36:1fff:fe52:7600/64 scope link
    inet 10.136.0.10/16 brd 10.136.255.255 scope global eth1
    inet6 fe80::e4a9:ff:fe88:2c2b/64 scope link
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    inet6 fe80::42:eff:fe2b:875f/64 scope link
```

Matching specific patterns

```
ip a| grep -w inet
```



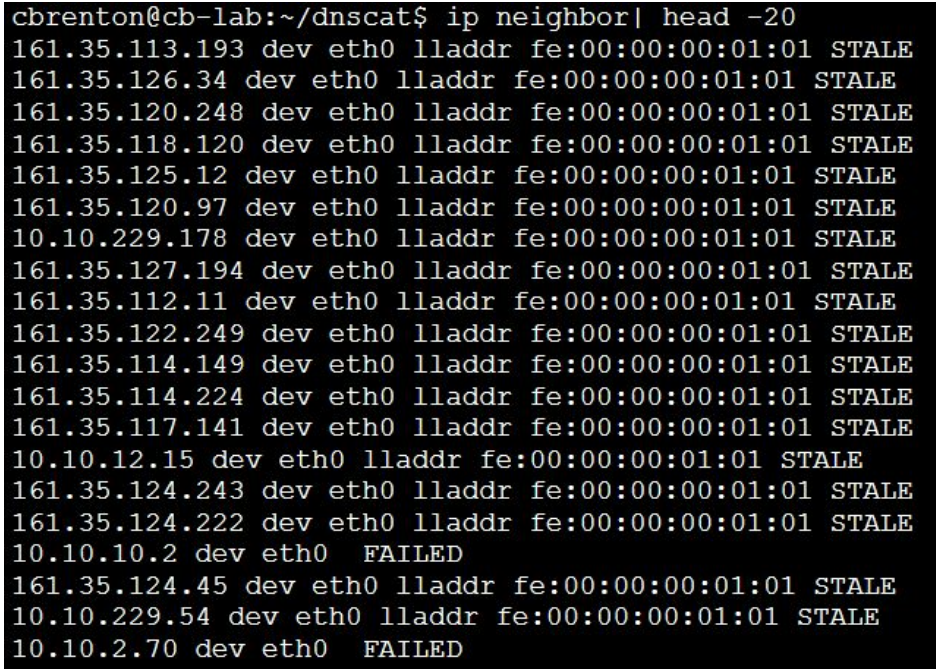
```
cbrenton@cb-lab:~$ ip a | grep -w inet
    inet 127.0.0.1/8 scope host lo
    inet 161.35.113.192/20 brd 161.35.127.255 scope global eth0
    inet 10.10.0.23/16 brd 10.10.255.255 scope global eth0
    inet 10.136.0.10/16 brd 10.136.255.255 scope global eth1
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
```

"-w" = Whole word match

String must start/end with non-word character

Note "inet6" no longer matches

MAC address info

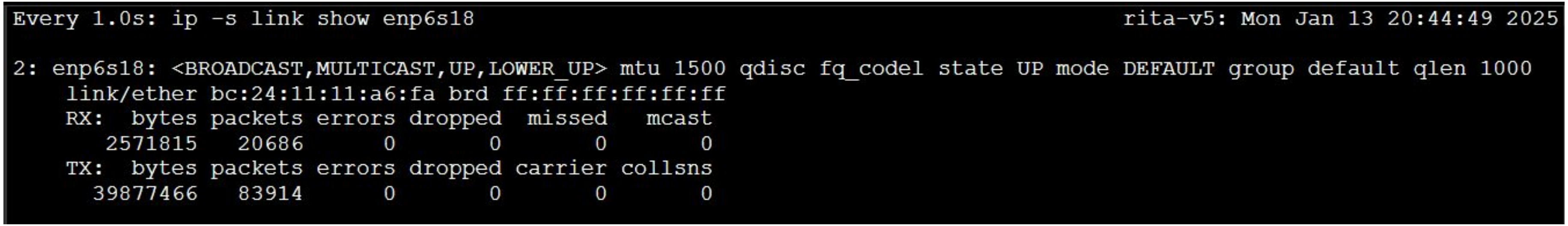


```
cbrenton@cb-lab:~/dnscat$ ip neighbor| head -20
161.35.113.193 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.126.34 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.120.248 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.118.120 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.125.12 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.120.97 dev eth0 lladdr fe:00:00:00:01:01 STALE
10.10.229.178 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.127.194 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.112.11 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.122.249 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.114.149 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.114.224 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.117.141 dev eth0 lladdr fe:00:00:00:01:01 STALE
10.10.12.15 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.124.243 dev eth0 lladdr fe:00:00:00:01:01 STALE
161.35.124.222 dev eth0 lladdr fe:00:00:00:01:01 STALE
10.10.10.2 dev eth0  FAILED
161.35.124.45 dev eth0 lladdr fe:00:00:00:01:01 STALE
10.10.229.54 dev eth0 lladdr fe:00:00:00:01:01 STALE
10.10.2.70 dev eth0  FAILED
```

Bogus MAC due to running in public cloud

Live monitoring network stats

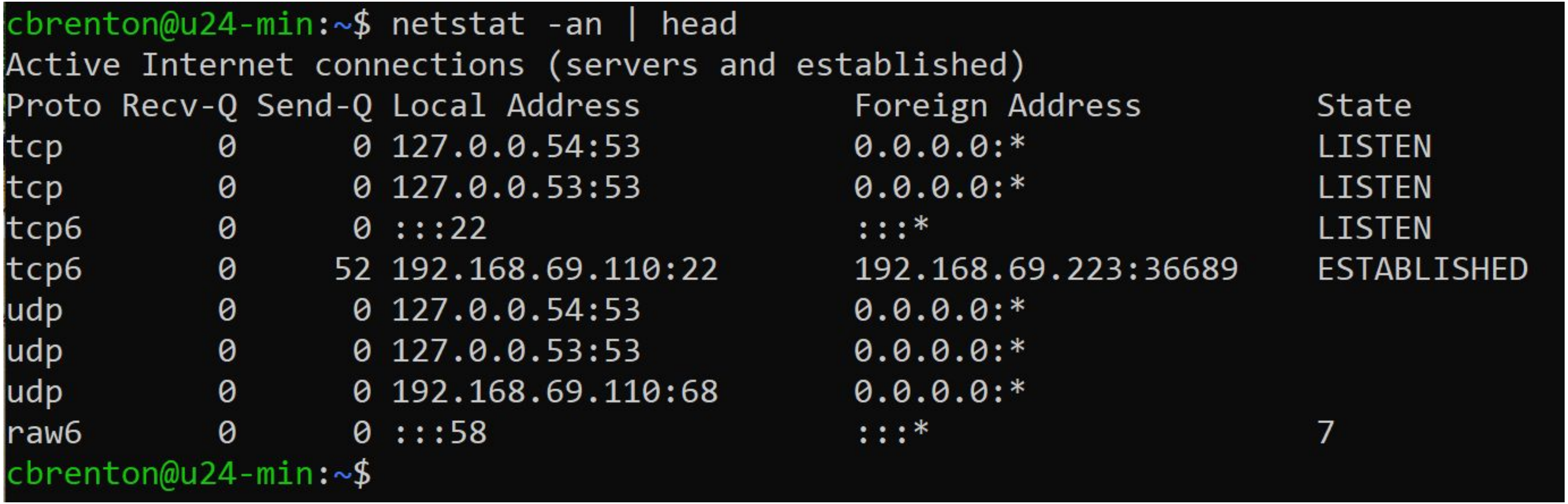
```
watch -n 1 "ip -s link show enp6s18"
```



```
Every 1.0s: ip -s link show enp6s18                                   rita-v5: Mon Jan 13 20:44:49 2025

2: enp6s18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether bc:24:11:11:a6:fa brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped  missed   mcast
       2571815   20686      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
      39877466   83914      0       0       0       0
```

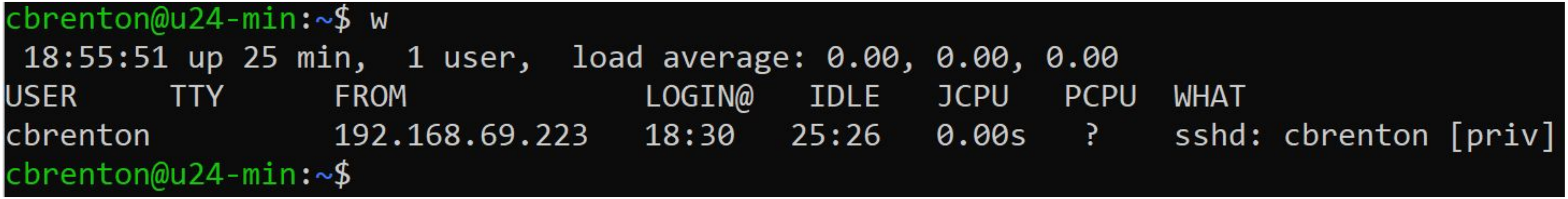
Replace "enp6s18" with your interface from the last slide
"CTRL-c" to quite this screen

netstat = Show open port info



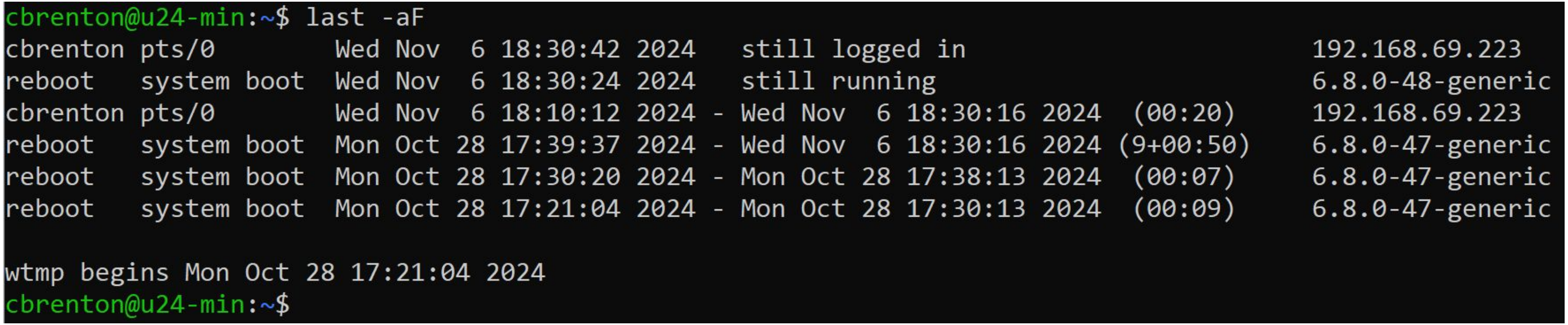
```
cbrenton@u24-min:~$ netstat -an | head
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0     52 192.168.69.110:22       192.168.69.223:36689    ESTABLISHED
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.69.110:68       0.0.0.0:*
raw6       0      0 :::58                   :::*                    7
cbrenton@u24-min:~$
```

w = See currently logged in users



```
cbrenton@u24-min:~$ w
 18:55:51 up 25 min,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU  WHAT
cbrenton          192.168.69.223   18:30   25:26   0.00s   ?    sshd: cbrenton [priv]
cbrenton@u24-min:~$
```

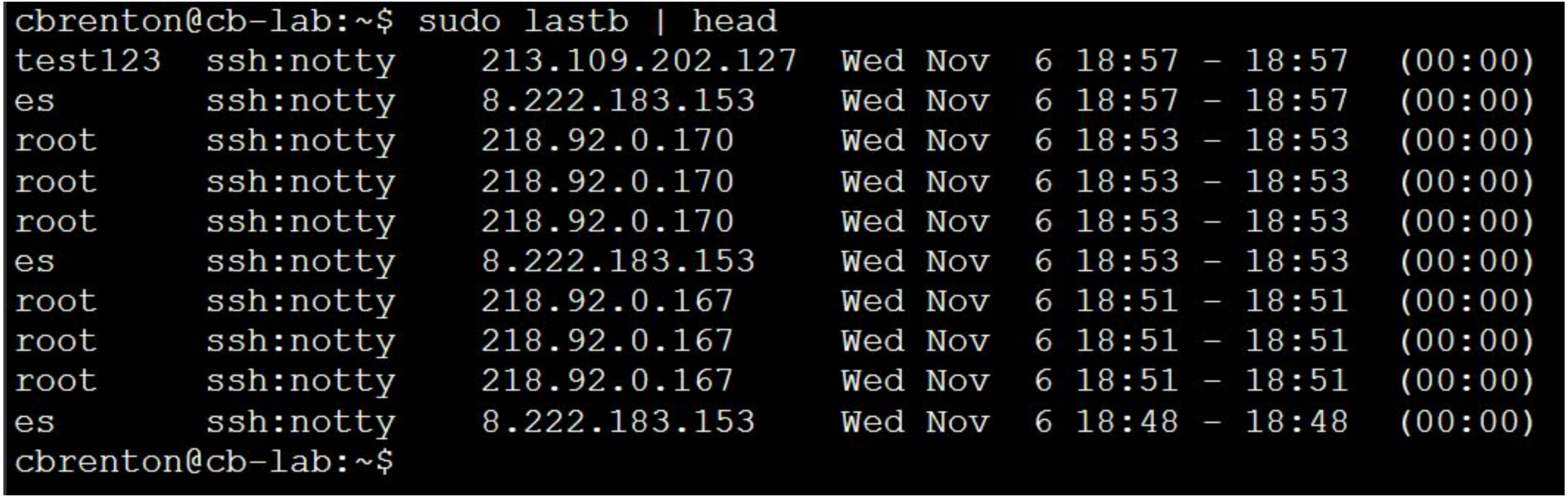
last = See successful login history



```
cbrenton@u24-min:~$ last -aF
cbrenton pts/0        Wed Nov  6 18:30:42 2024   still logged in                         192.168.69.223
reboot   system boot  Wed Nov  6 18:30:24 2024   still running                           6.8.0-48-generic
cbrenton pts/0        Wed Nov  6 18:10:12 2024 - Wed Nov  6 18:30:16 2024  (00:20)     192.168.69.223
reboot   system boot  Mon Oct 28 17:39:37 2024 - Wed Nov  6 18:30:16 2024 (9+00:50)    6.8.0-47-generic
reboot   system boot  Mon Oct 28 17:30:20 2024 - Mon Oct 28 17:38:13 2024  (00:07)     6.8.0-47-generic
reboot   system boot  Mon Oct 28 17:21:04 2024 - Mon Oct 28 17:30:13 2024  (00:09)     6.8.0-47-generic

wtmp begins Mon Oct 28 17:21:04 2024
cbrenton@u24-min:~$
```

Does not start tracking logins until the first time you run the command

lastb = Show failed login attempts

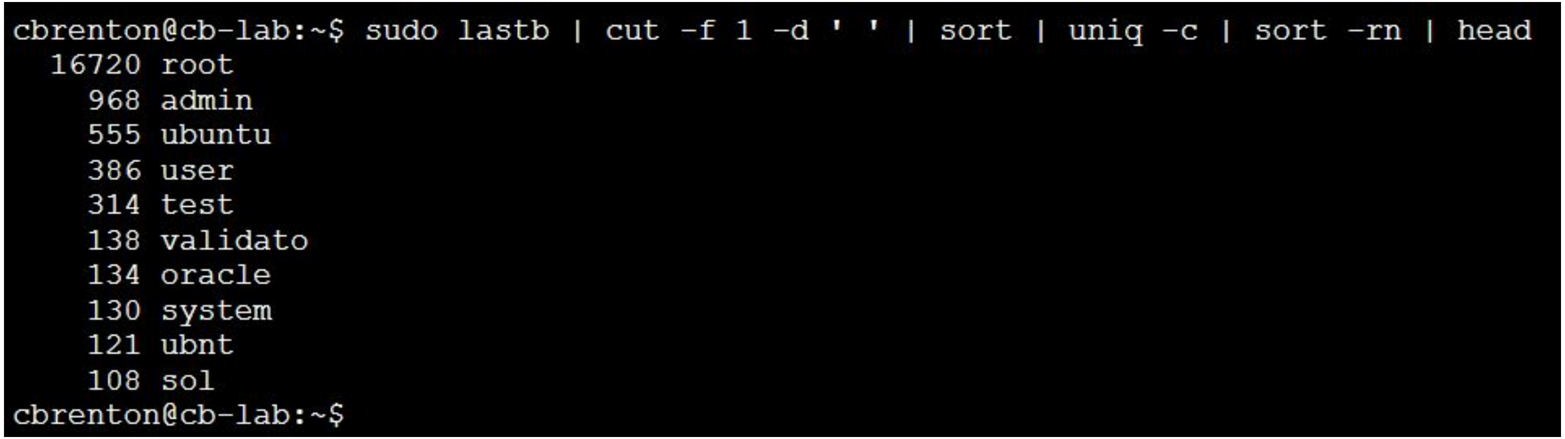


```
cbrenton@cb-lab:~$ sudo lastb | head
test123  ssh:notty    213.109.202.127  Wed Nov  6 18:57 - 18:57  (00:00)
es       ssh:notty    8.222.183.153    Wed Nov  6 18:57 - 18:57  (00:00)
root     ssh:notty    218.92.0.170     Wed Nov  6 18:53 - 18:53  (00:00)
root     ssh:notty    218.92.0.170     Wed Nov  6 18:53 - 18:53  (00:00)
root     ssh:notty    218.92.0.170     Wed Nov  6 18:53 - 18:53  (00:00)
es       ssh:notty    8.222.183.153    Wed Nov  6 18:53 - 18:53  (00:00)
root     ssh:notty    218.92.0.167     Wed Nov  6 18:51 - 18:51  (00:00)
root     ssh:notty    218.92.0.167     Wed Nov  6 18:51 - 18:51  (00:00)
root     ssh:notty    218.92.0.167     Wed Nov  6 18:51 - 18:51  (00:00)
es       ssh:notty    8.222.183.153    Wed Nov  6 18:48 - 18:48  (00:00)
cbrenton@cb-lab:~$
```

You should be using failed2ban which will be covered in another class

List of accounts with brute force attempts

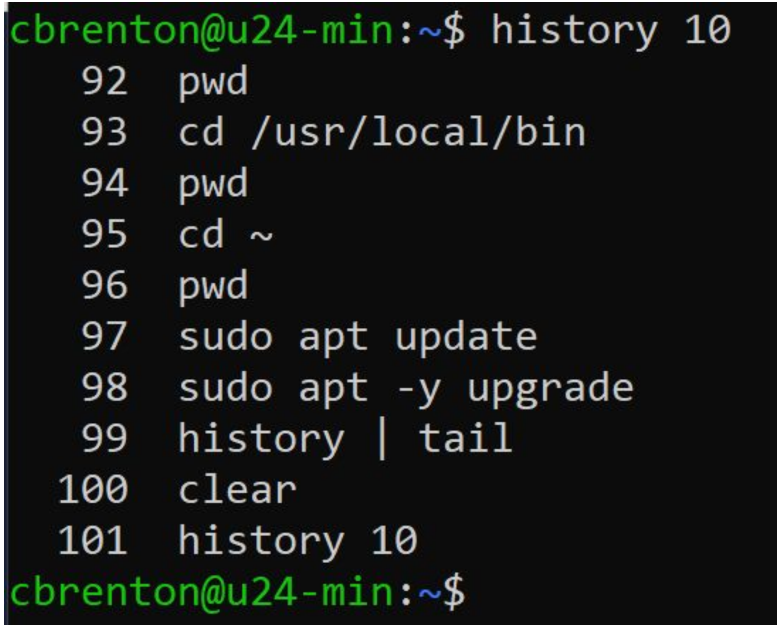
```
sudo lastb | cut -f 1 -d ' ' | sort | uniq -c | sort -rn | head
```



```
cbrenton@cb-lab:~$ sudo lastb | cut -f 1 -d ' ' | sort | uniq -c | sort -rn | head
  16720 root
    968 admin
    555 ubuntu
    386 user
    314 test
    138 validato
    134 oracle
    130 system
    121 ubnt
    108 sol
cbrenton@cb-lab:~$
```

The above only works if you are running fail2ban

history = Show previous commands



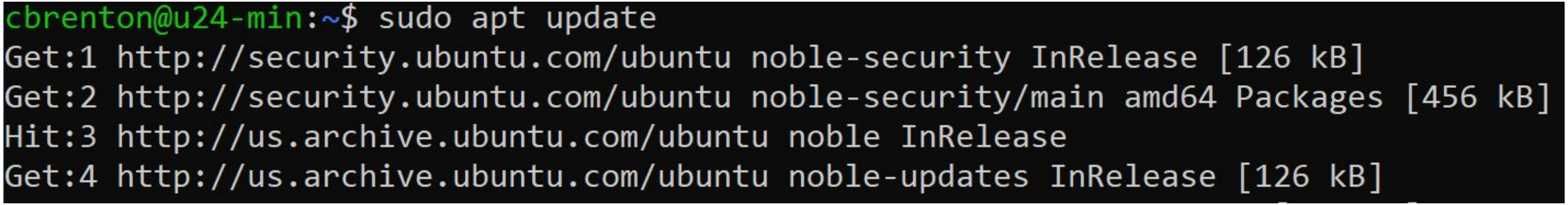
```
cbrenton@u24-min:~$ history 10
   92  pwd
   93  cd /usr/local/bin
   94  pwd
   95  cd ~
   96  pwd
   97  sudo apt update
   98  sudo apt -y upgrade
   99  history | tail
  100  clear
  101  history 10
cbrenton@u24-min:~$
```

Distro dependent, but usually saves last 2,000 commands

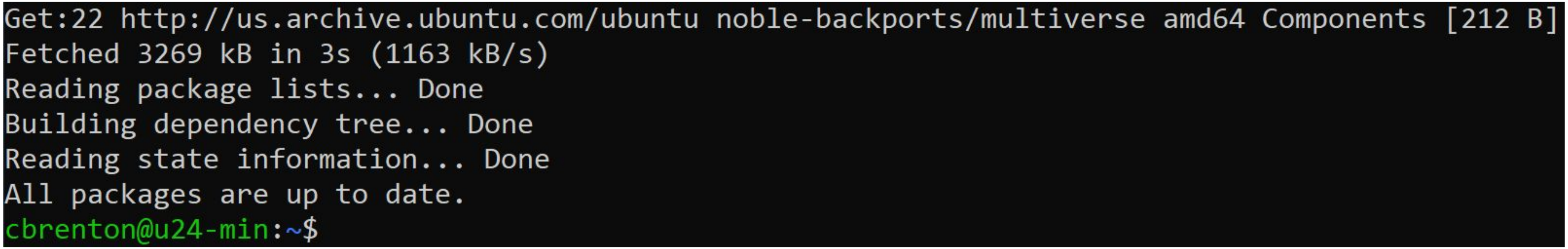
Patching

- Most Linux system default to installing security patches
- You may need to manually install functional patches
- Two popular patch management systems
    - apt = Debian, Ubuntu, other variants
    - yum = Red Hat, CentOS, Fedora, other variants
- Examples I'll give are specific to "apt" but "yum" is similar

Check to see if patches are available



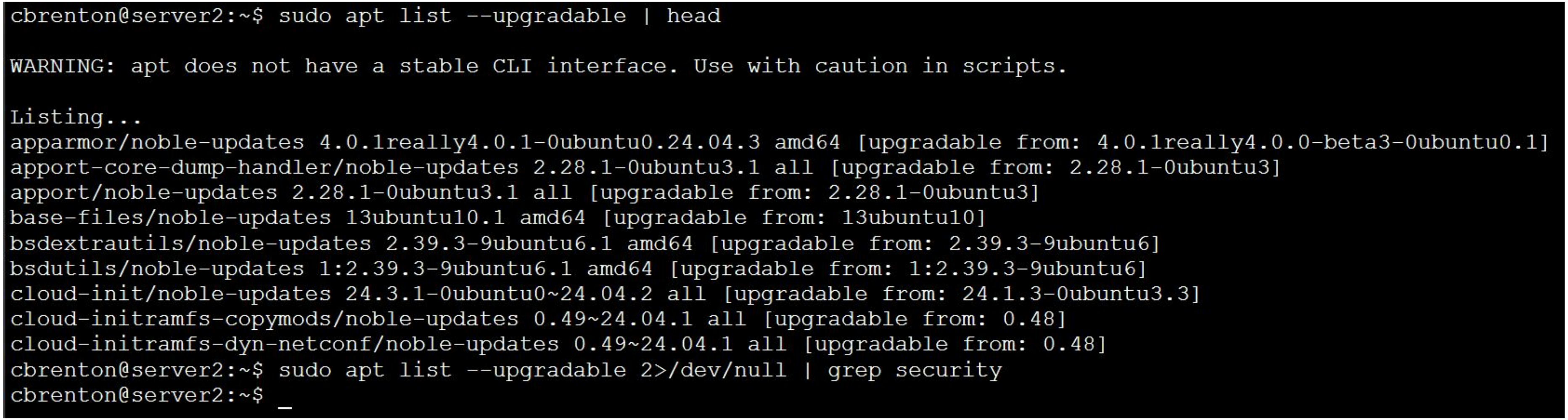
```
cbrenton@u24-min:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:2 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [456 kB]
Hit:3 http://us.archive.ubuntu.com/ubuntu noble InRelease
Get:4 http://us.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
```



```
Get:22 http://us.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Fetched 3269 kB in 3s (1163 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
cbrenton@u24-min:~$
```

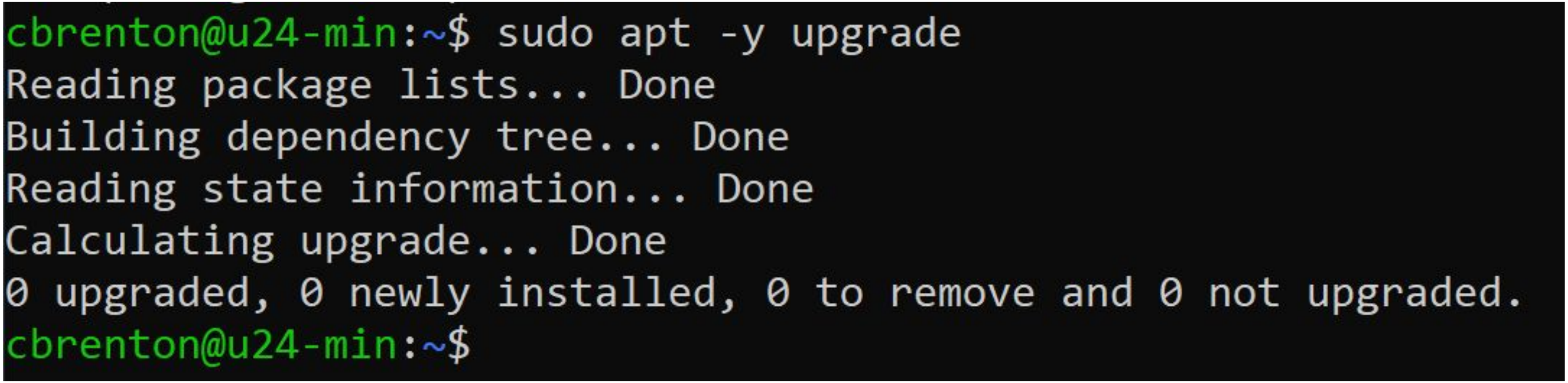
Run before other "apt" commands so they work properly

View missing patches (optional)



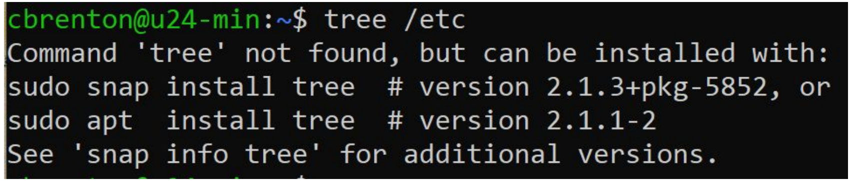
```
cbrenton@server2:~$ sudo apt list --upgradable | head

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Listing...
apparmor/noble-updates 4.0.1really4.0.1-0ubuntu0.24.04.3 amd64 [upgradable from: 4.0.1really4.0.0-beta3-0ubuntu0.1]
apport-core-dump-handler/noble-updates 2.28.1-0ubuntu3.1 all [upgradable from: 2.28.1-0ubuntu3]
apport/noble-updates 2.28.1-0ubuntu3.1 all [upgradable from: 2.28.1-0ubuntu3]
base-files/noble-updates 13ubuntu10.1 amd64 [upgradable from: 13ubuntu10]
bsdextrautils/noble-updates 2.39.3-9ubuntu6.1 amd64 [upgradable from: 2.39.3-9ubuntu6]
bsdutils/noble-updates 1:2.39.3-9ubuntu6.1 amd64 [upgradable from: 1:2.39.3-9ubuntu6]
cloud-init/noble-updates 24.3.1-0ubuntu0~24.04.2 all [upgradable from: 24.1.3-0ubuntu3.3]
cloud-initramfs-copymods/noble-updates 0.49~24.04.1 all [upgradable from: 0.48]
cloud-initramfs-dyn-netconf/noble-updates 0.49~24.04.1 all [upgradable from: 0.48]
cbrenton@server2:~$ sudo apt list --upgradable 2>/dev/null | grep security
cbrenton@server2:~$ _
```

Install all patches (but not upgrades)

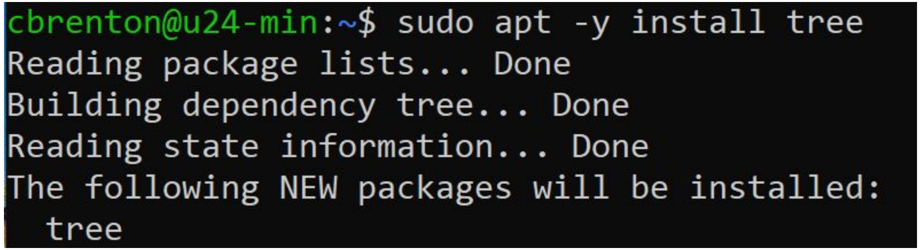


```
cbrenton@u24-min:~$ sudo apt -y upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
cbrenton@u24-min:~$
```

Installing software

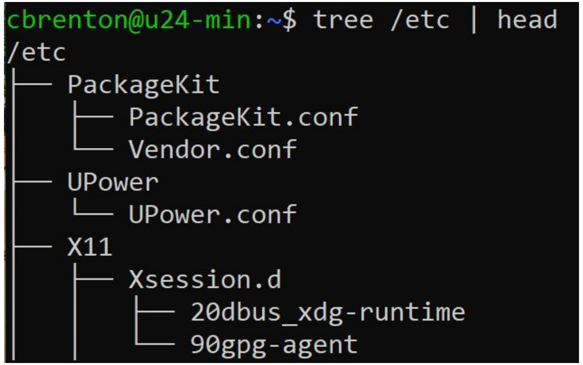


```
cbrenton@u24-min:~$ tree /etc
Command 'tree' not found, but can be installed with:
sudo snap install tree  # version 2.1.3+pkg-5852, or
sudo apt  install tree  # version 2.1.1-2
See 'snap info tree' for additional versions.
```



```
cbrenton@u24-min:~$ sudo apt -y install tree
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  tree
```

Man pages are installed as well



```
cbrenton@u24-min:~$ tree /etc | head
/etc
├── PackageKit
│   ├── PackageKit.conf
│   └── Vendor.conf
├── UPower
│   └── UPower.conf
├── X11
│   ├── Xsession.d
│   │   ├── 20dbus_xdg-runtime
│   │   └── 90gpg-agent
```

"`tree -d`" to list only dir names

Where can I learn more?

- Bill Stearns has some awesome content
- Anything every written/presented by Hal
- Ryan's Tutorials has some awesome walk throughs
- Linux Journey has some decent online content
- Linux Survival has some good references/tutorials

Missing a reference you think is useful?
Please toss it into chat and share the love!

Wrap up

- Thank you for attending!
- Certs & video usually go out in 24 hours
- If you have any lingering questions, the Discord channel will remain active
    - Also a good chance to socialize with others in the class
    - Have other tips and tricks? Please share with others!
    - Posting screenshots can be helpful :-)