The Wonderful World of Services

VINCE

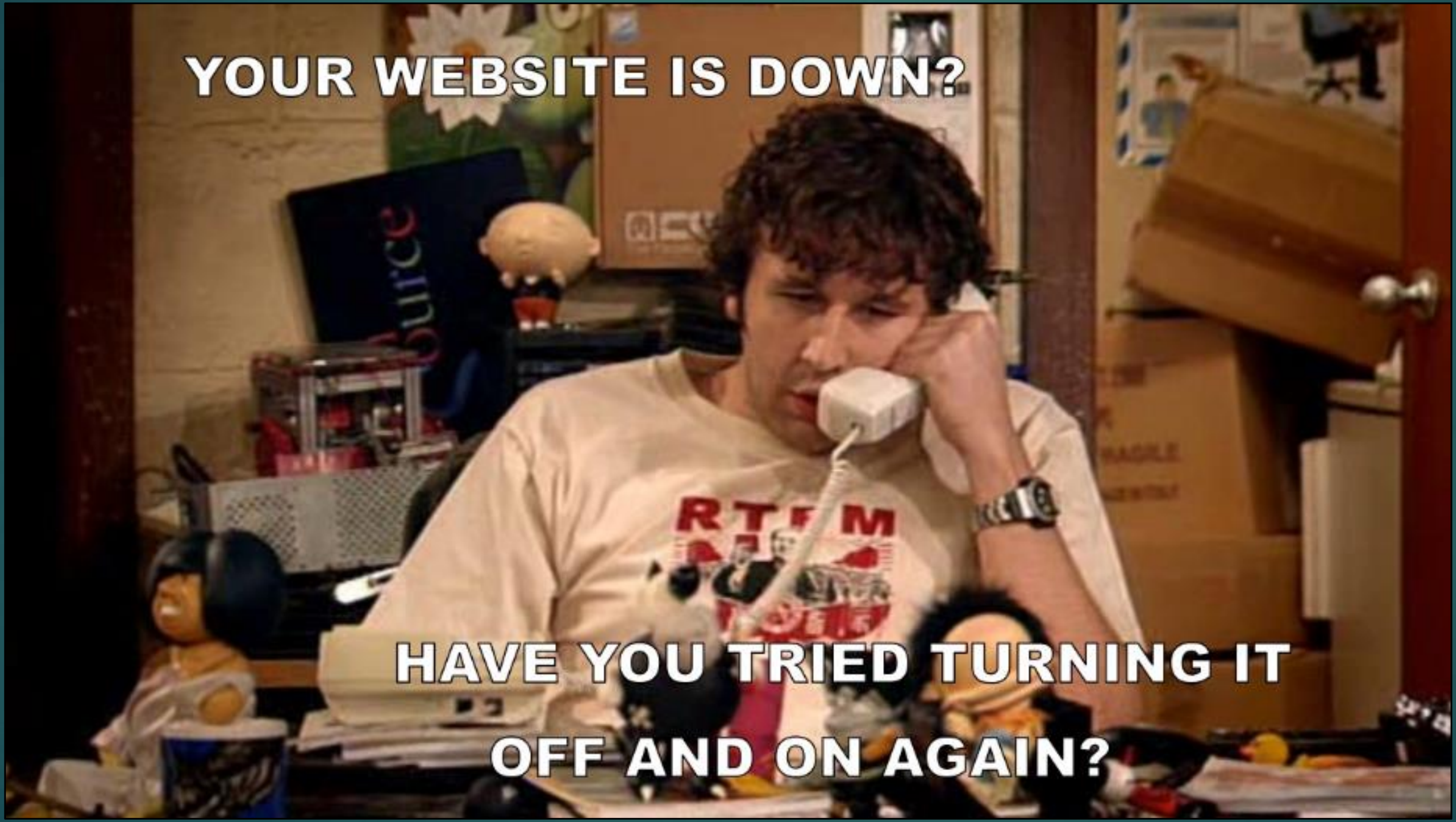
Agenda

- definitions
- services for Windows and Linux
- breaks?
- auditing Linux
- logs for Linux
- useful tools

Goals

- develop a better understanding of Linux and Windows
- services (How this ties in with Auditing)
- base level auditing
- understand logs
- pick up some useful tools!
- better understanding of what to do initially in a competition

Services


YOUR WEBSITE IS DOWN?
HAVE YOU TRIED TURNING IT OFF AND ON AGAIN?

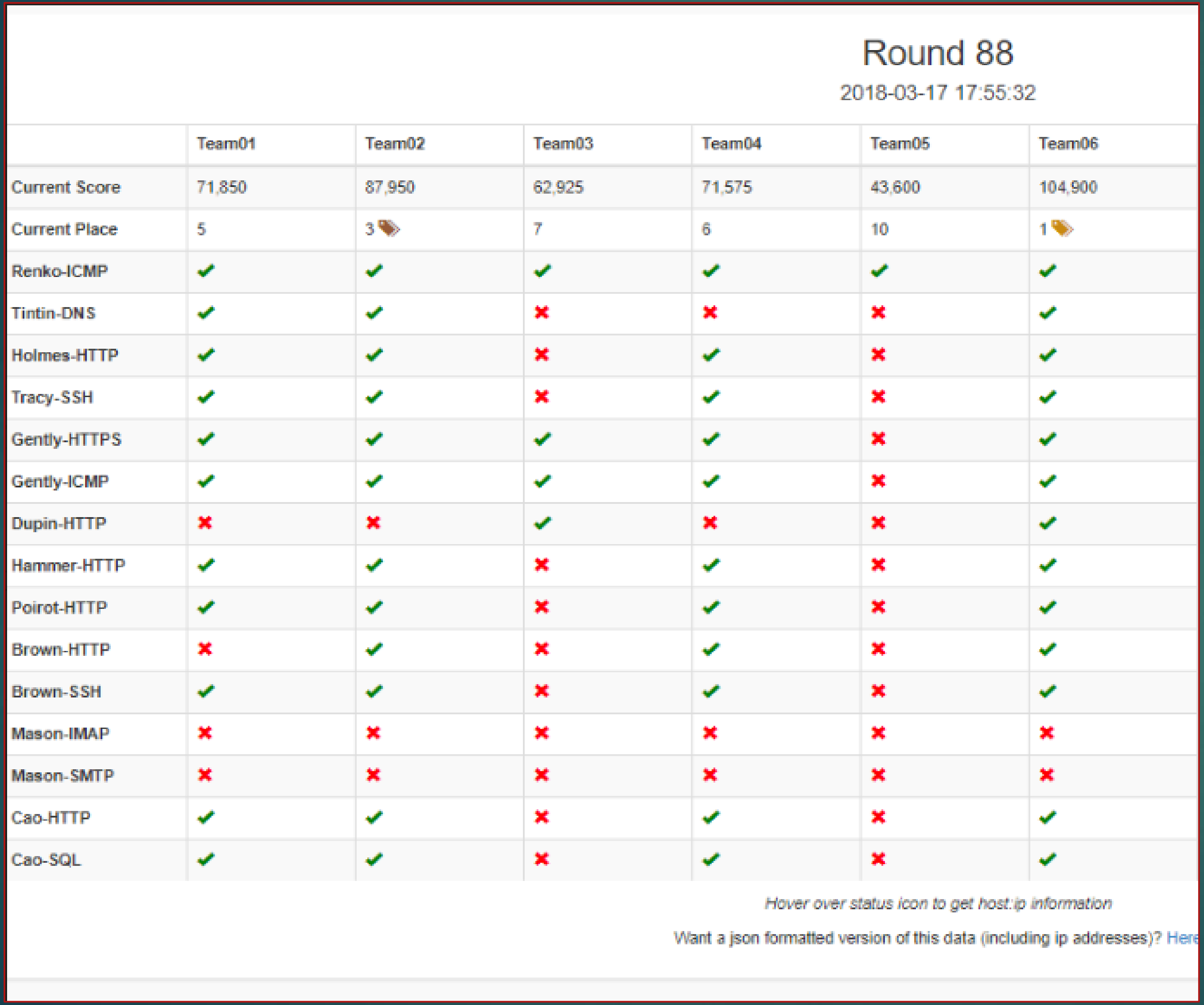
What is a Service?

- an application (or set of applications) that runs in the background
- this application can enable your box to do a certain task, or carry out essential tasks
  - such as running a web server

Some Common Services

- **D**omain **N**ame **S**ystem (DNS)
- **S**ecure **S**hell (SSH)
- Databases – MySQL, MongoDB (Graylog uses this!)
- APACHE – cross-platform web server
- **FTP** – File Transfer Protocol

NECCDC 2018 Services



Round 88

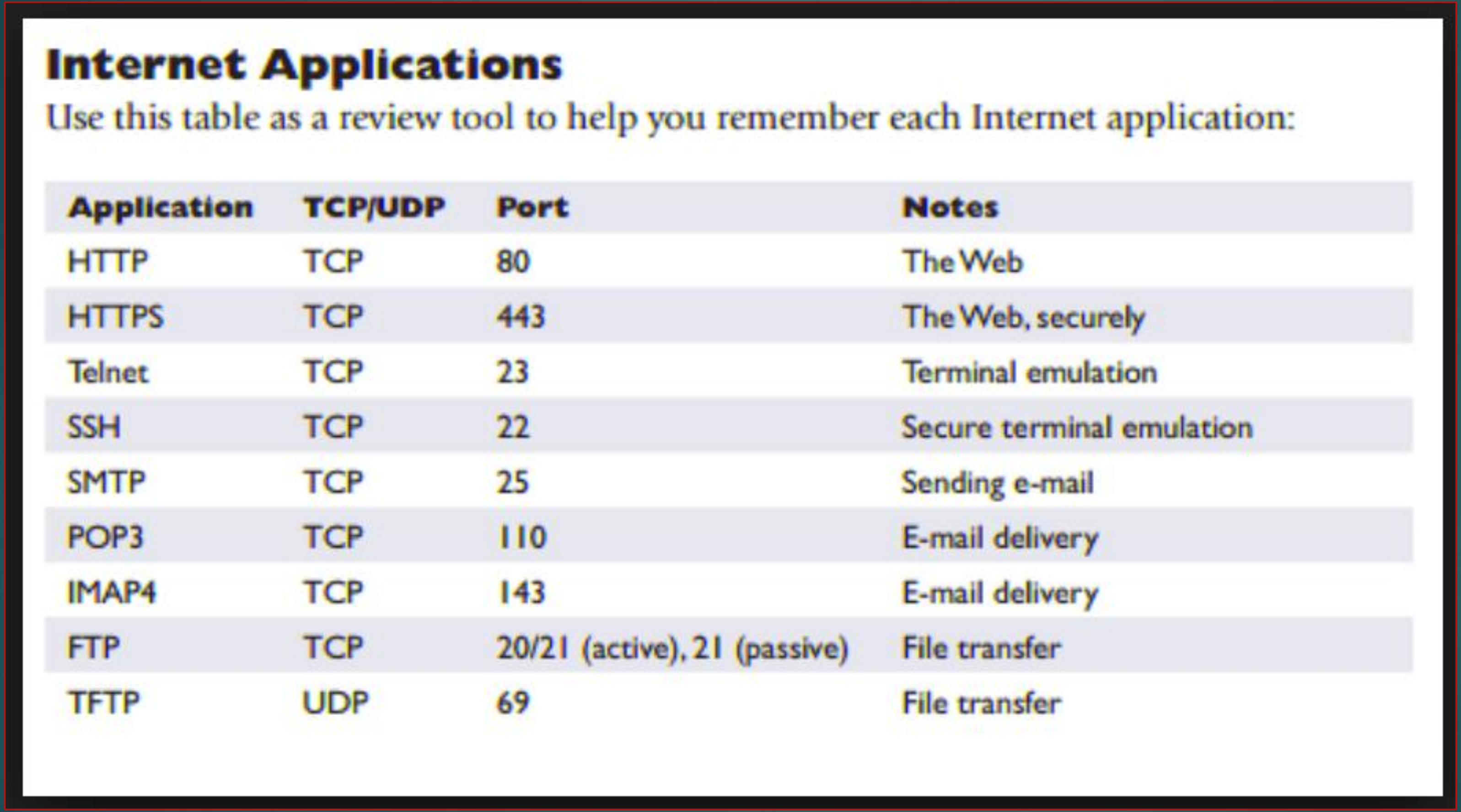
2018-03-17 17:55:32

	Team01	Team02	Team03	Team04	Team05	Team06
Current Score	71,850	87,950	62,925	71,575	43,600	104,900
Current Place	5	3 🏷	7	6	10	1 🏷
Renko-ICMP	✓	✓	✓	✓	✓	✓
Tintin-DNS	✓	✓	✖	✖	✖	✓
Holmes-HTTP	✓	✓	✖	✓	✖	✓
Tracy-SSH	✓	✓	✖	✓	✖	✓
Gently-HTTPS	✓	✓	✓	✓	✖	✓
Gently-ICMP	✓	✓	✓	✓	✖	✓
Dupin-HTTP	✖	✖	✓	✖	✖	✓
Hammer-HTTP	✓	✓	✖	✓	✖	✓
Poirot-HTTP	✓	✓	✖	✓	✖	✓
Brown-HTTP	✖	✓	✖	✓	✖	✓
Brown-SSH	✓	✓	✖	✓	✖	✓
Mason-IMAP	✖	✖	✖	✖	✖	✖
Mason-SMTP	✖	✖	✖	✖	✖	✖
Cao-HTTP	✓	✓	✖	✓	✖	✓
Cao-SQL	✓	✓	✖	✓	✖	✓

Hover over status icon to get host:ip information

Want a json formatted version of this data (including ip addresses)? Here

Services Operate Over Ports



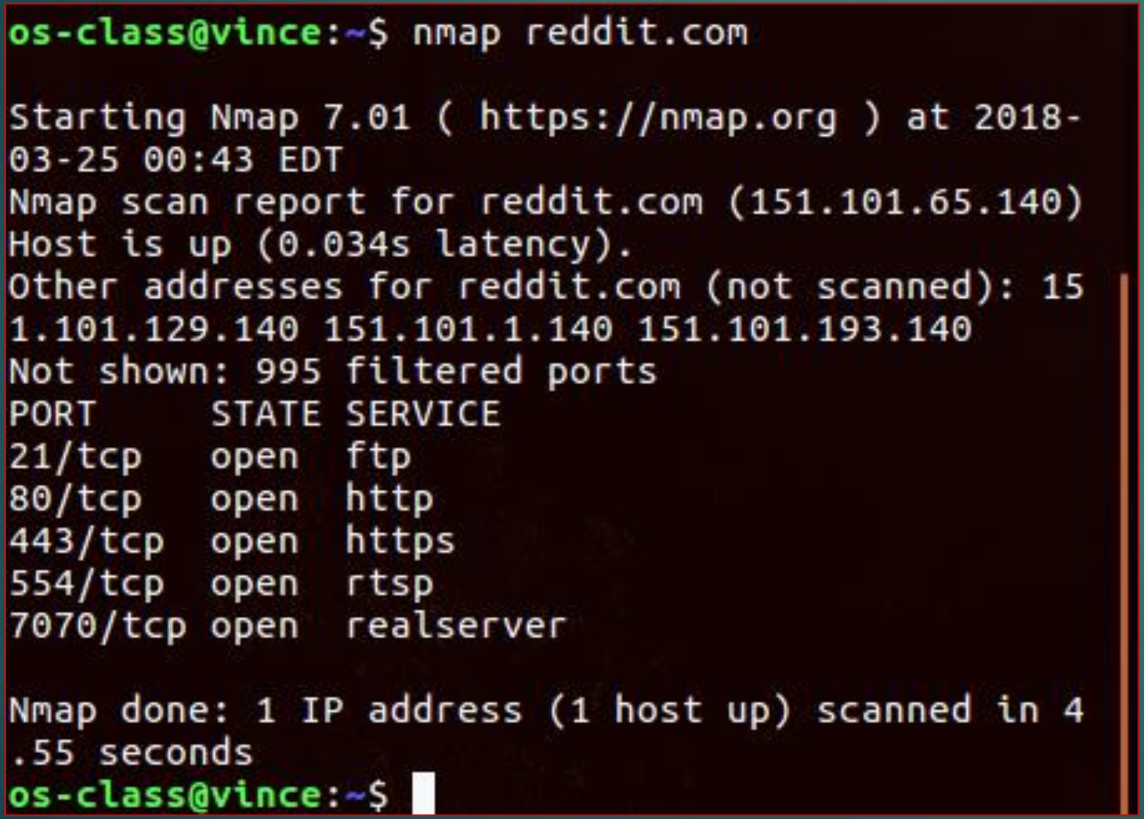
Internet Applications

Use this table as a review tool to help you remember each Internet application:

Application	TCP/UDP	Port	Notes
HTTP	TCP	80	The Web
HTTPS	TCP	443	The Web, securely
Telnet	TCP	23	Terminal emulation
SSH	TCP	22	Secure terminal emulation
SMTP	TCP	25	Sending e-mail
POP3	TCP	110	E-mail delivery
IMAP4	TCP	143	E-mail delivery
FTP	TCP	20/21 (active), 21 (passive)	File transfer
TFTP	UDP	69	File transfer

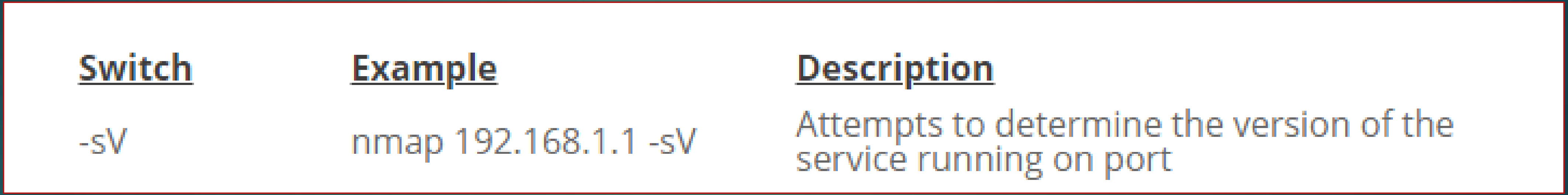
We can use **nmap** to check ports and services!

- We know a lot about **nmap** around these parts…

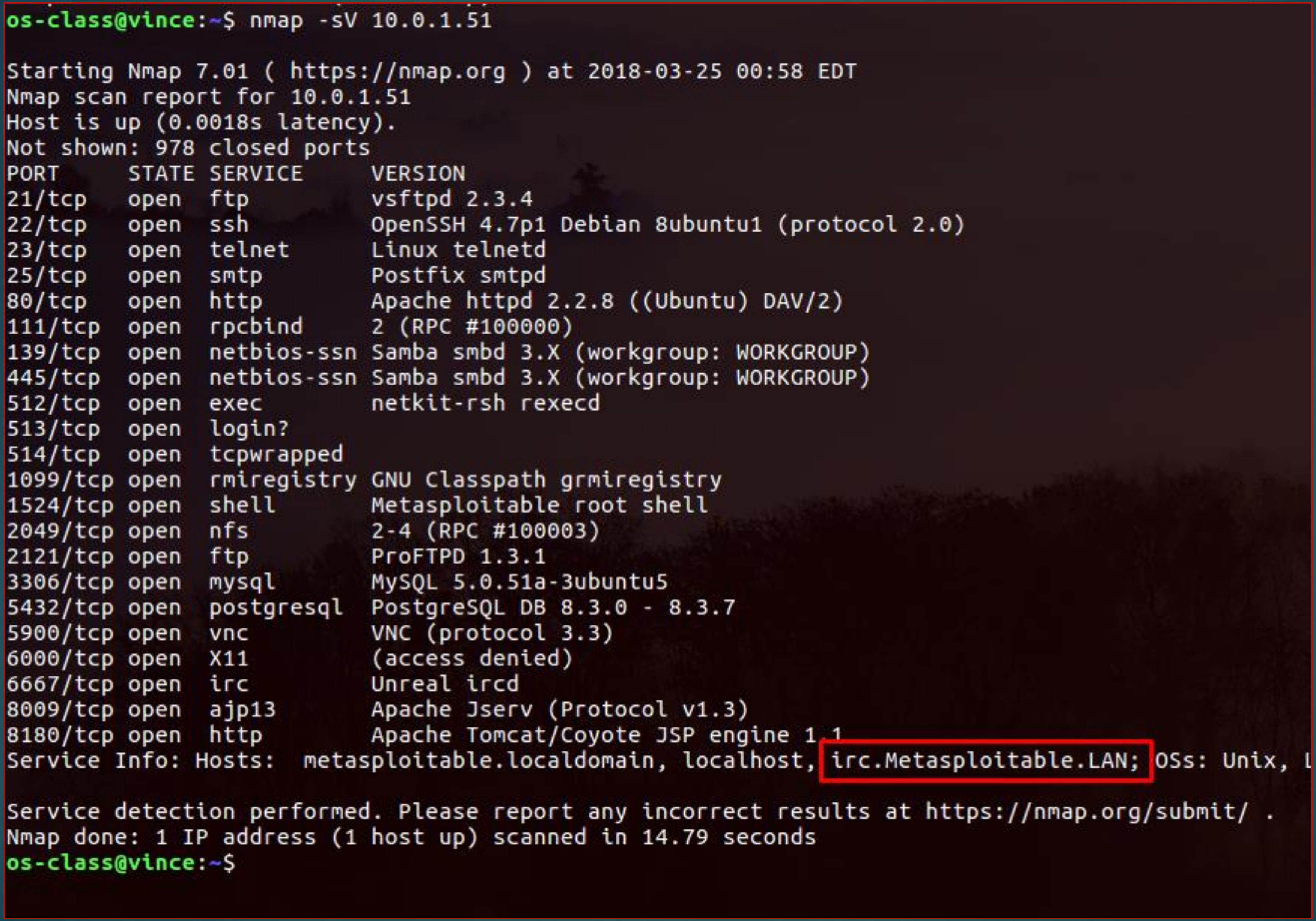


```
os-class@vince:~$ nmap reddit.com

Starting Nmap 7.01 ( https://nmap.org ) at 2018-
03-25 00:43 EDT
Nmap scan report for reddit.com (151.101.65.140)
Host is up (0.034s latency).
Other addresses for reddit.com (not scanned): 15
1.101.129.140 151.101.1.140 151.101.193.140
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
7070/tcp open  realserver

Nmap done: 1 IP address (1 host up) scanned in 4
.55 seconds
os-class@vince:~$
```

https://www.stationx.net/nmap-cheat-sheet/



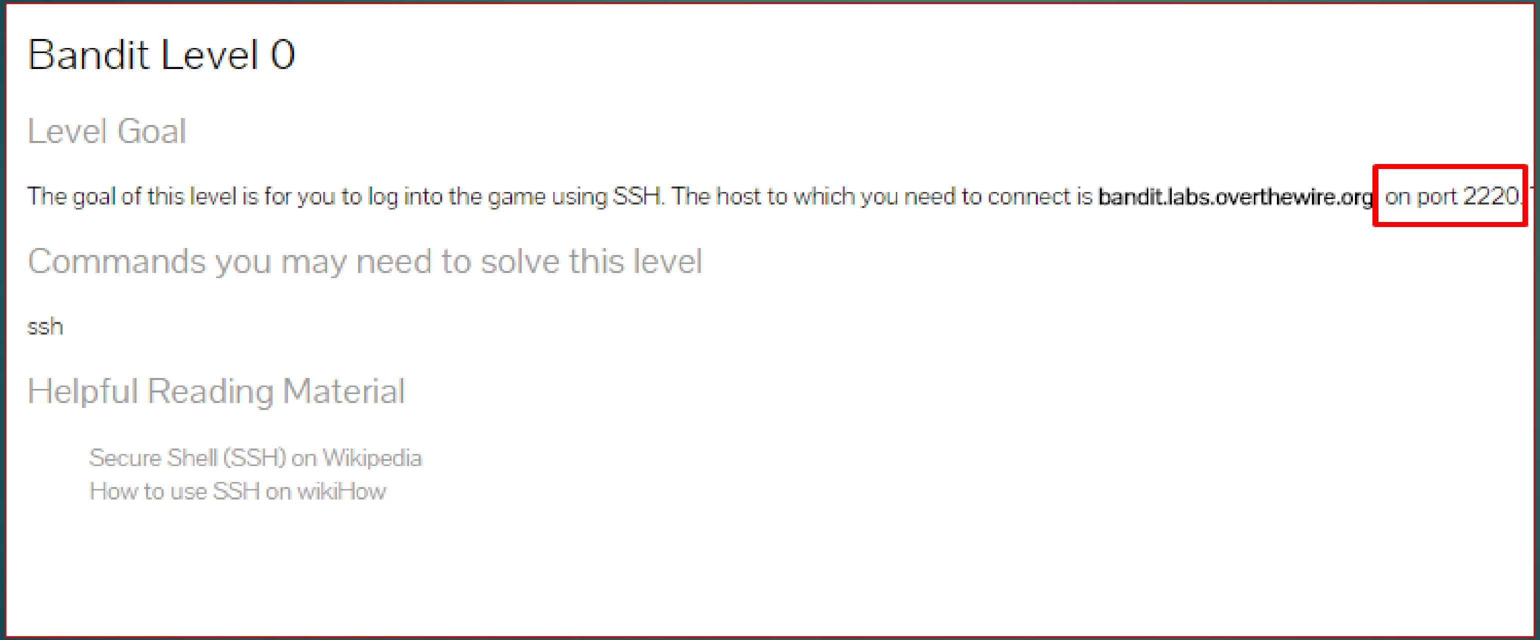
Switch	Example	Description
-sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port



```
os-class@vince:~$ nmap -sV 10.0.1.51

Starting Nmap 7.01 ( https://nmap.org ) at 2018-03-25 00:58 EDT
Nmap scan report for 10.0.1.51
Host is up (0.0018s latency).
Not shown: 978 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, L

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.79 seconds
os-class@vince:~$
```

Why do we need to know ports?

- if you are setting up your firewall, it’s important to make sure you allow traffic over that port
- you can always change the port (config files)
- for example OverTheWire runs ssh over a different port



Bandit Level 0

Level Goal

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is **bandit.labs.overthewire.org** on port 2220.

Commands you may need to solve this level

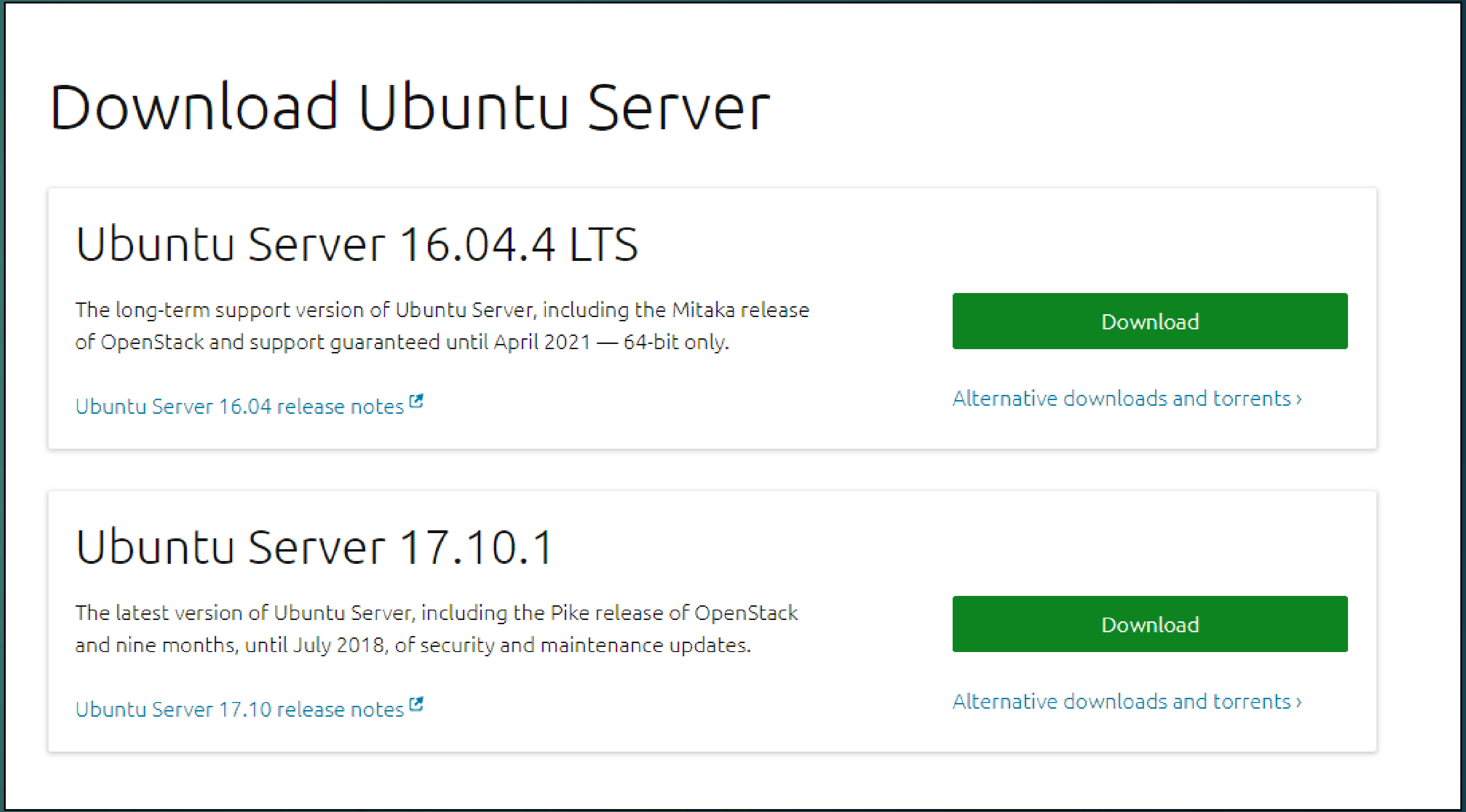
ssh

Helpful Reading Material

Secure Shell (SSH) on Wikipedia
How to use SSH on wikiHow

Services and Operating Systems

- server-oriented operating systems are good for services
- as you guys know there is Windows Server 20XX, you can use this… but no one likes Windows so, why?



Download Ubuntu Server

Ubuntu Server 16.04.4 LTS

The long-term support version of Ubuntu Server, including the Mitaka release of OpenStack and support guaranteed until April 2021 — 64-bit only.

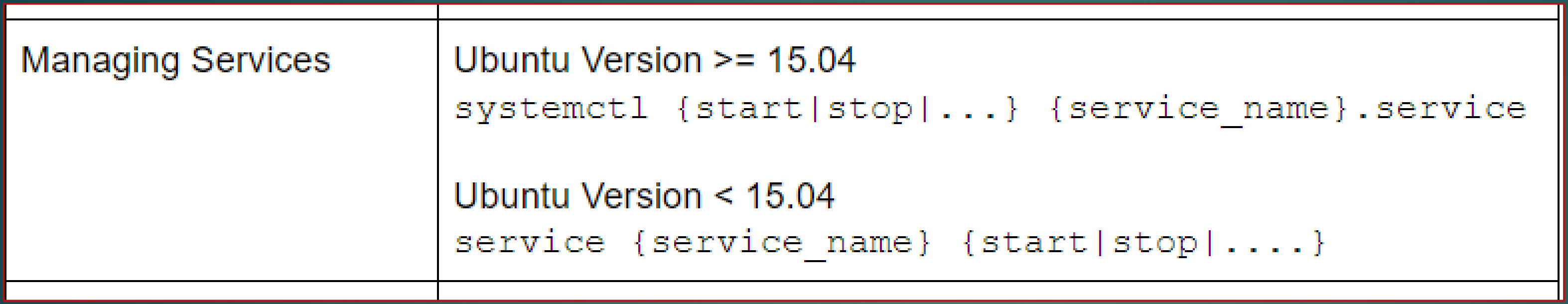
Ubuntu Server 16.04 release notes

Ubuntu Server 17.10.1

The latest version of Ubuntu Server, including the Pike release of OpenStack and nine months, until July 2018, of security and maintenance updates.

Ubuntu Server 17.10 release notes

What service(s) are on my box?



<table>
<tr><td>Managing Services</td><td>Ubuntu Version >= 15.04
systemctl {start|stop|...} {service_name}.service

Ubuntu Version < 15.04
service {service_name} {start|stop|....}</td></tr>
</table>

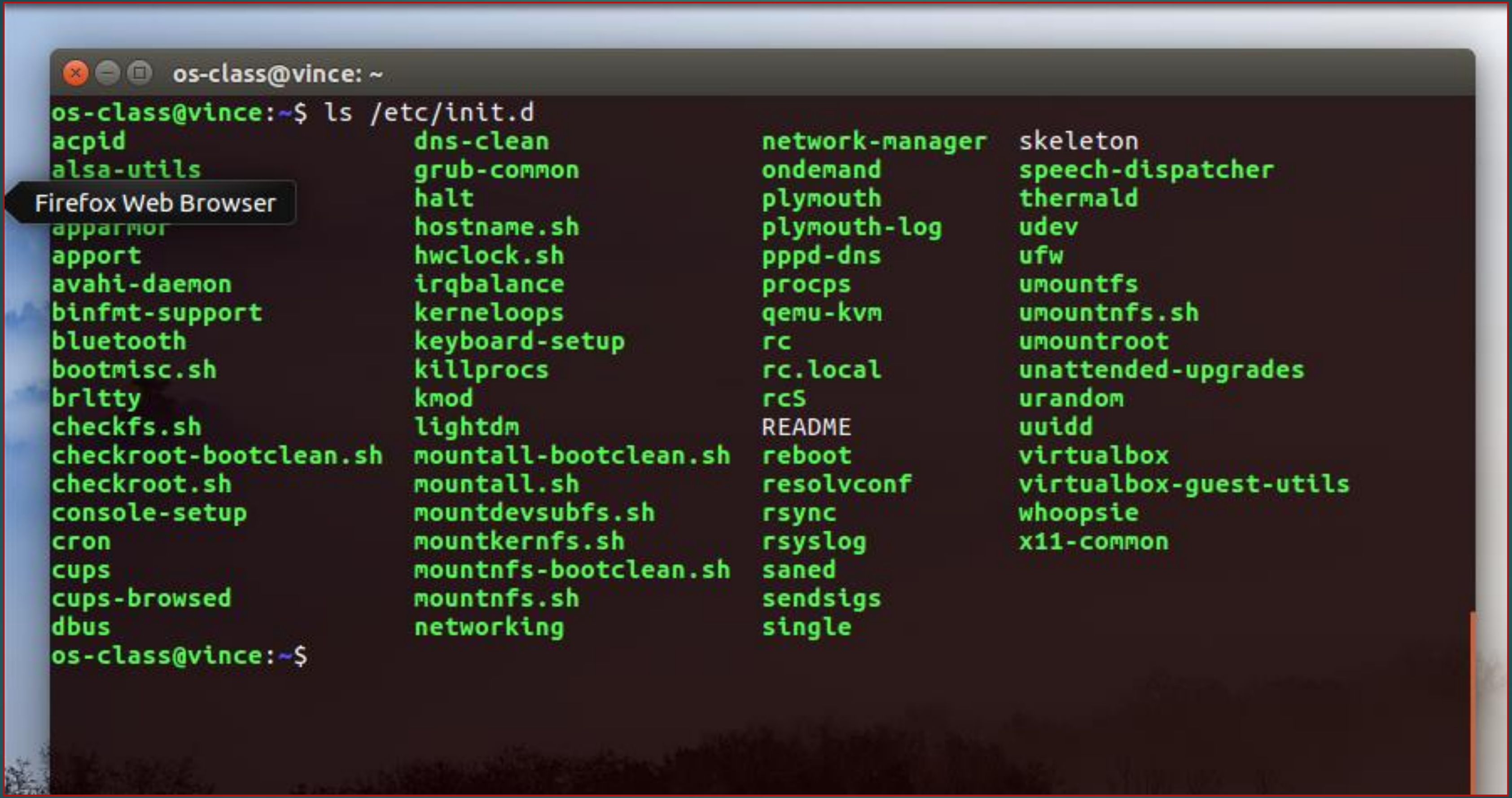
Older Architectures(S)

- **service [SERVICE_NAME] [start | stop | restart | reload | status]**

Newer Architectures(S)

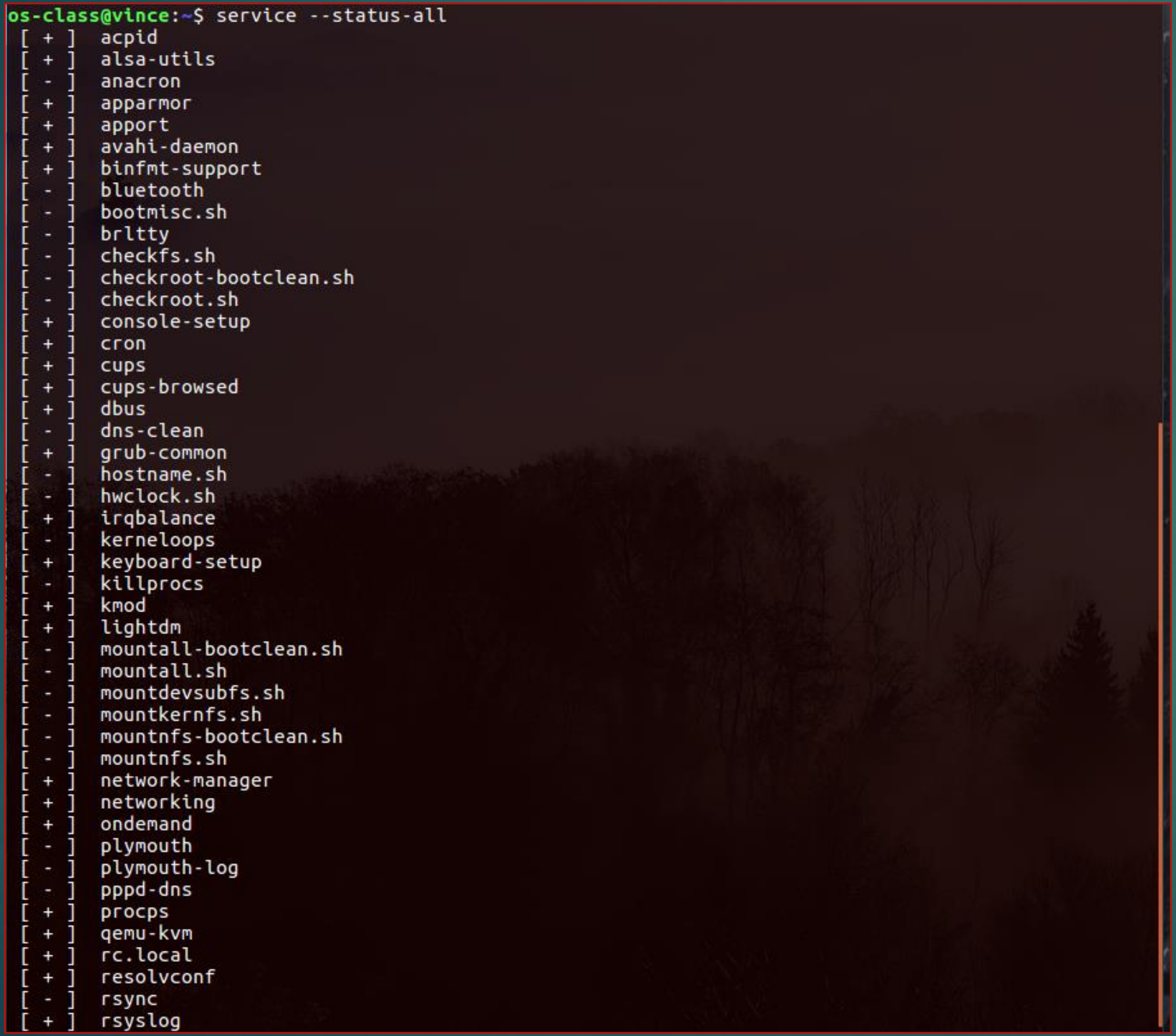
- **systemctl [start | stop | restart | reload | status] [SERVICE_NAME]**

ls /etc/init.d



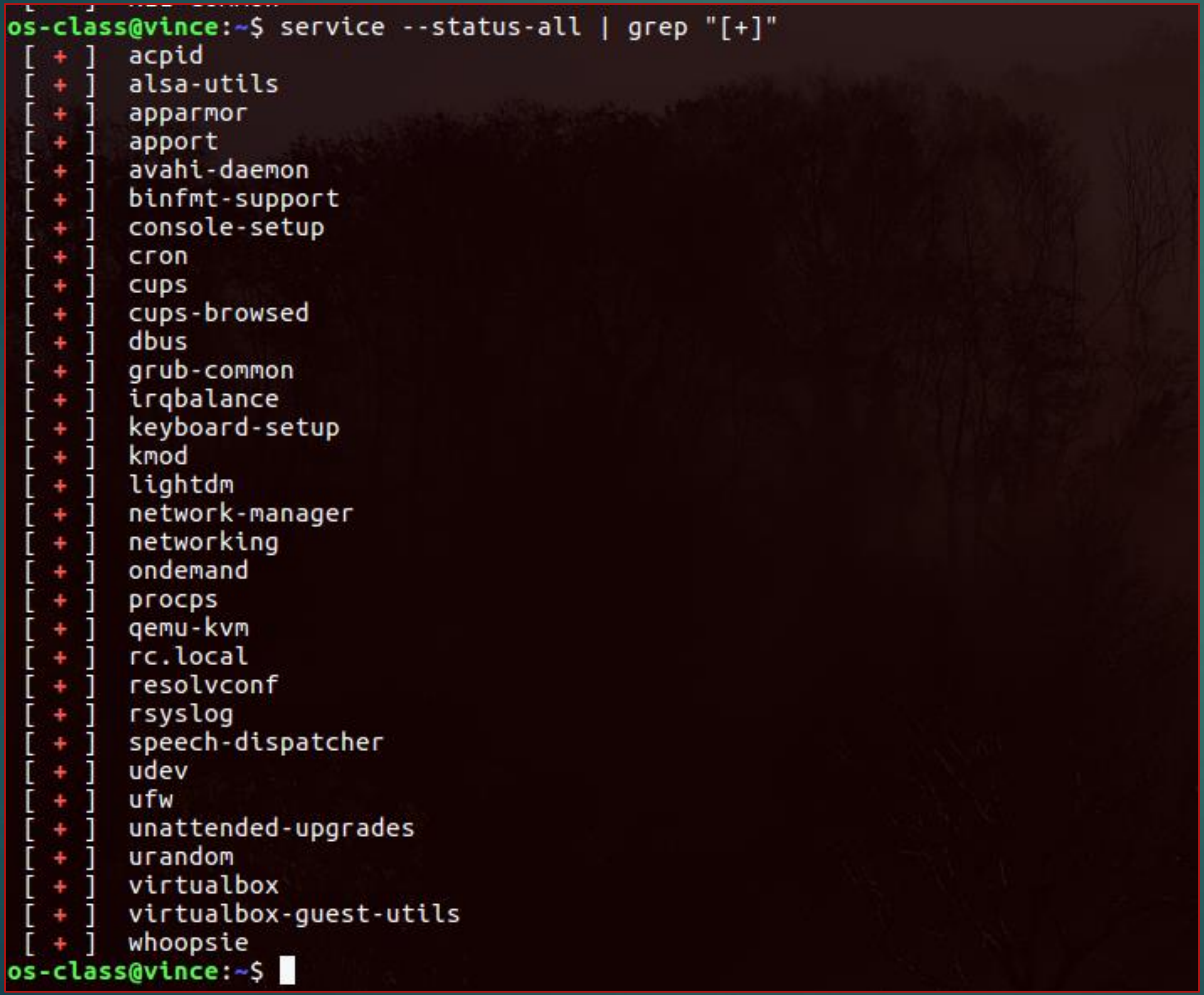
```
os-class@vince:~$ ls /etc/init.d
acpid                   dns-clean              network-manager  skeleton
alsa-utils              grub-common            ondemand         speech-dispatcher
                        halt                   plymouth         thermald
apparmor                hostname.sh            plymouth-log     udev
apport                  hwclock.sh             pppd-dns         ufw
avahi-daemon            irqbalance             procps           umountfs
binfmt-support          kerneloops             qemu-kvm         umountnfs.sh
bluetooth               keyboard-setup         rc               umountroot
bootmisc.sh             killprocs              rc.local         unattended-upgrades
brltty                  kmod                   rcS              urandom
checkfs.sh              lightdm                README           uuidd
checkroot-bootclean.sh  mountall-bootclean.sh  reboot           virtualbox
checkroot.sh            mountall.sh            resolvconf       virtualbox-guest-utils
console-setup           mountdevsubfs.sh       rsync            whoopsie
cron                    mountkernfs.sh         rsyslog          x11-common
cups                    mountnfs-bootclean.sh  saned
cups-browsed            mountnfs.sh            sendsigs
dbus                    networking             single
os-class@vince:~$
```

service --status-all



```
os-class@vince:~$ service --status-all
 [ + ]  acpid
 [ + ]  alsa-utils
 [ - ]  anacron
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  avahi-daemon
 [ + ]  binfmt-support
 [ - ]  bluetooth
 [ - ]  bootmisc.sh
 [ - ]  brltty
 [ - ]  checkfs.sh
 [ - ]  checkroot-bootclean.sh
 [ - ]  checkroot.sh
 [ + ]  console-setup
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ + ]  dbus
 [ - ]  dns-clean
 [ + ]  grub-common
 [ - ]  hostname.sh
 [ - ]  hwclock.sh
 [ + ]  irqbalance
 [ - ]  kerneloops
 [ + ]  keyboard-setup
 [ - ]  killprocs
 [ + ]  kmod
 [ + ]  lightdm
 [ - ]  mountall-bootclean.sh
 [ - ]  mountall.sh
 [ - ]  mountdevsubfs.sh
 [ - ]  mountkernfs.sh
 [ - ]  mountnfs-bootclean.sh
 [ - ]  mountnfs.sh
 [ + ]  network-manager
 [ + ]  networking
 [ + ]  ondemand
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ - ]  pppd-dns
 [ + ]  procps
 [ + ]  qemu-kvm
 [ + ]  rc.local
 [ + ]  resolvconf
 [ - ]  rsync
 [ + ]  rsyslog
```

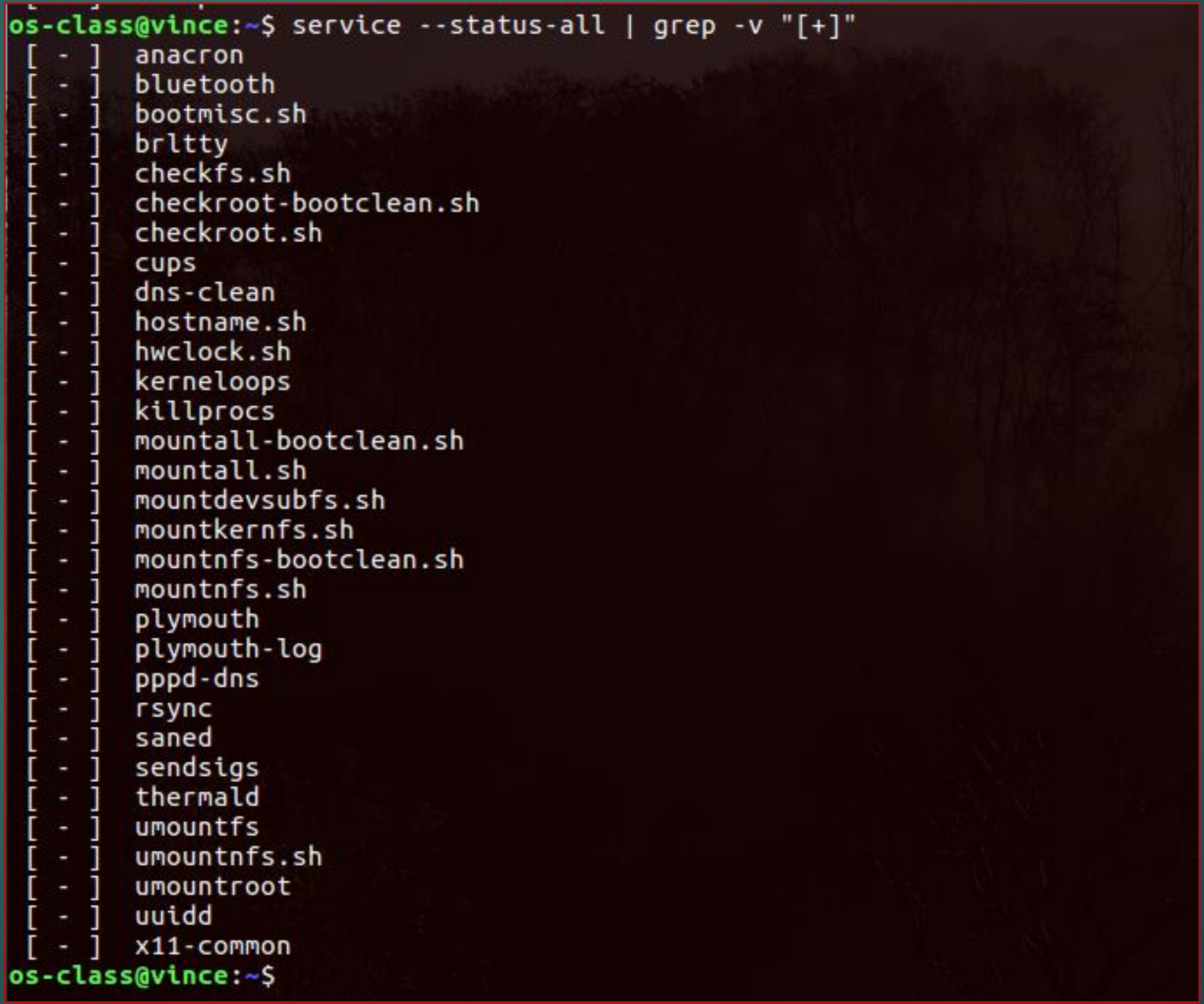
service --status-all | grep “[+]”



```
os-class@vince:~$ service --status-all | grep "[+]"
 [ + ]  acpid
 [ + ]  alsa-utils
 [ + ]  apparmor
 [ + ]  apport
 [ + ]  avahi-daemon
 [ + ]  binfmt-support
 [ + ]  console-setup
 [ + ]  cron
 [ + ]  cups
 [ + ]  cups-browsed
 [ + ]  dbus
 [ + ]  grub-common
 [ + ]  irqbalance
 [ + ]  keyboard-setup
 [ + ]  kmod
 [ + ]  lightdm
 [ + ]  network-manager
 [ + ]  networking
 [ + ]  ondemand
 [ + ]  procps
 [ + ]  qemu-kvm
 [ + ]  rc.local
 [ + ]  resolvconf
 [ + ]  rsyslog
 [ + ]  speech-dispatcher
 [ + ]  udev
 [ + ]  ufw
 [ + ]  unattended-upgrades
 [ + ]  urandom
 [ + ]  virtualbox
 [ + ]  virtualbox-guest-utils
 [ + ]  whoopsie
os-class@vince:~$
```

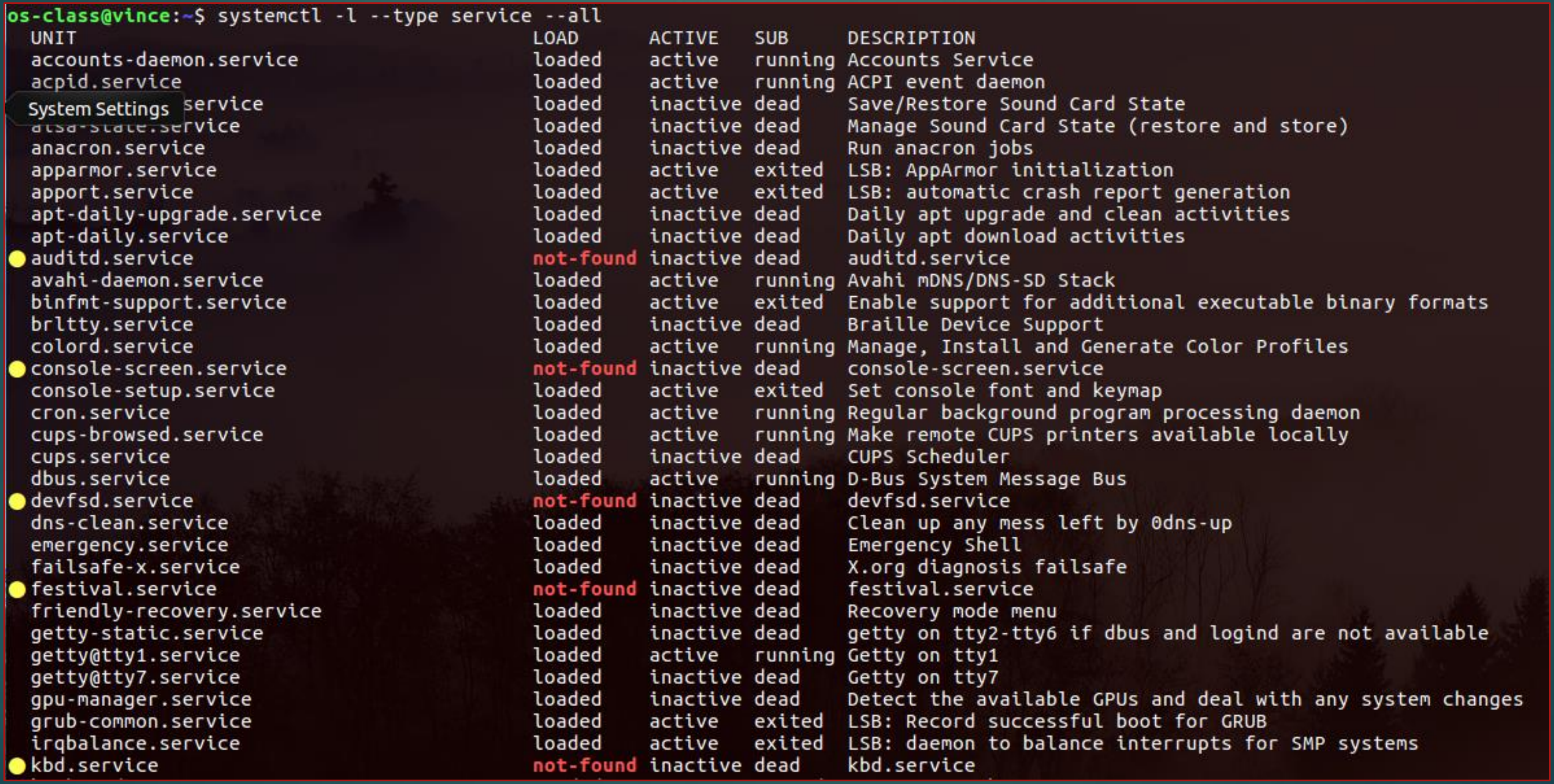
What about what is not running?

service --status-all | grep -v "[+]"



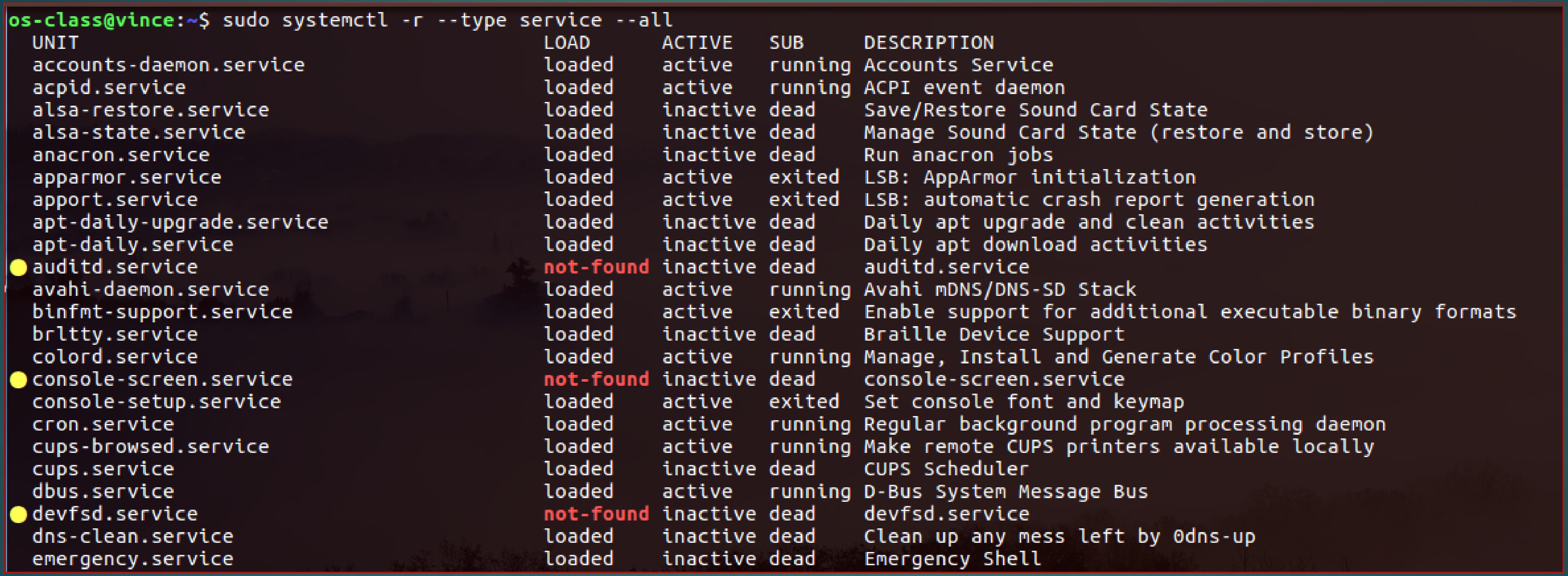
```
os-class@vince:~$ service --status-all | grep -v "[+]"
 [ - ]  anacron
 [ - ]  bluetooth
 [ - ]  bootmisc.sh
 [ - ]  brltty
 [ - ]  checkfs.sh
 [ - ]  checkroot-bootclean.sh
 [ - ]  checkroot.sh
 [ - ]  cups
 [ - ]  dns-clean
 [ - ]  hostname.sh
 [ - ]  hwclock.sh
 [ - ]  kerneloops
 [ - ]  killprocs
 [ - ]  mountall-bootclean.sh
 [ - ]  mountall.sh
 [ - ]  mountdevsubfs.sh
 [ - ]  mountkernfs.sh
 [ - ]  mountnfs-bootclean.sh
 [ - ]  mountnfs.sh
 [ - ]  plymouth
 [ - ]  plymouth-log
 [ - ]  pppd-dns
 [ - ]  rsync
 [ - ]  saned
 [ - ]  sendsigs
 [ - ]  thermald
 [ - ]  umountfs
 [ - ]  umountnfs.sh
 [ - ]  umountroot
 [ - ]  uuidd
 [ - ]  x11-common
os-class@vince:~$
```

systemctl -l --type service --all



```
os-class@vince:~$ systemctl -l --type service --all
  UNIT                                       LOAD      ACTIVE   SUB     DESCRIPTION
  accounts-daemon.service                    loaded    active   running Accounts Service
  acpid.service                              loaded    active   running ACPI event daemon
               service                       loaded    inactive dead    Save/Restore Sound Card State
  alsa-state.service                         loaded    inactive dead    Manage Sound Card State (restore and store)
  anacron.service                            loaded    inactive dead    Run anacron jobs
  apparmor.service                           loaded    active   exited  LSB: AppArmor initialization
  apport.service                             loaded    active   exited  LSB: automatic crash report generation
  apt-daily-upgrade.service                  loaded    inactive dead    Daily apt upgrade and clean activities
  apt-daily.service                          loaded    inactive dead    Daily apt download activities
● auditd.service                             not-found inactive dead    auditd.service
  avahi-daemon.service                       loaded    active   running Avahi mDNS/DNS-SD Stack
  binfmt-support.service                     loaded    active   exited  Enable support for additional executable binary formats
  brltty.service                             loaded    inactive dead    Braille Device Support
  colord.service                             loaded    active   running Manage, Install and Generate Color Profiles
● console-screen.service                     not-found inactive dead    console-screen.service
  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    inactive dead    CUPS Scheduler
  dbus.service                               loaded    active   running D-Bus System Message Bus
● devfsd.service                             not-found inactive dead    devfsd.service
  dns-clean.service                          loaded    inactive dead    Clean up any mess left by 0dns-up
  emergency.service                          loaded    inactive dead    Emergency Shell
  failsafe-x.service                         loaded    inactive dead    X.org diagnosis failsafe
● festival.service                           not-found inactive dead    festival.service
  friendly-recovery.service                  loaded    inactive dead    Recovery mode menu
  getty-static.service                       loaded    inactive dead    getty on tty2-tty6 if dbus and logind are not available
  getty@tty1.service                         loaded    active   running Getty on tty1
  getty@tty7.service                         loaded    inactive dead    Getty on tty7
  gpu-manager.service                        loaded    inactive dead    Detect the available GPUs and deal with any system changes
  grub-common.service                        loaded    active   exited  LSB: Record successful boot for GRUB
  irqbalance.service                         loaded    active   exited  LSB: daemon to balance interrupts for SMP systems
● kbd.service                                not-found inactive dead    kbd.service
```

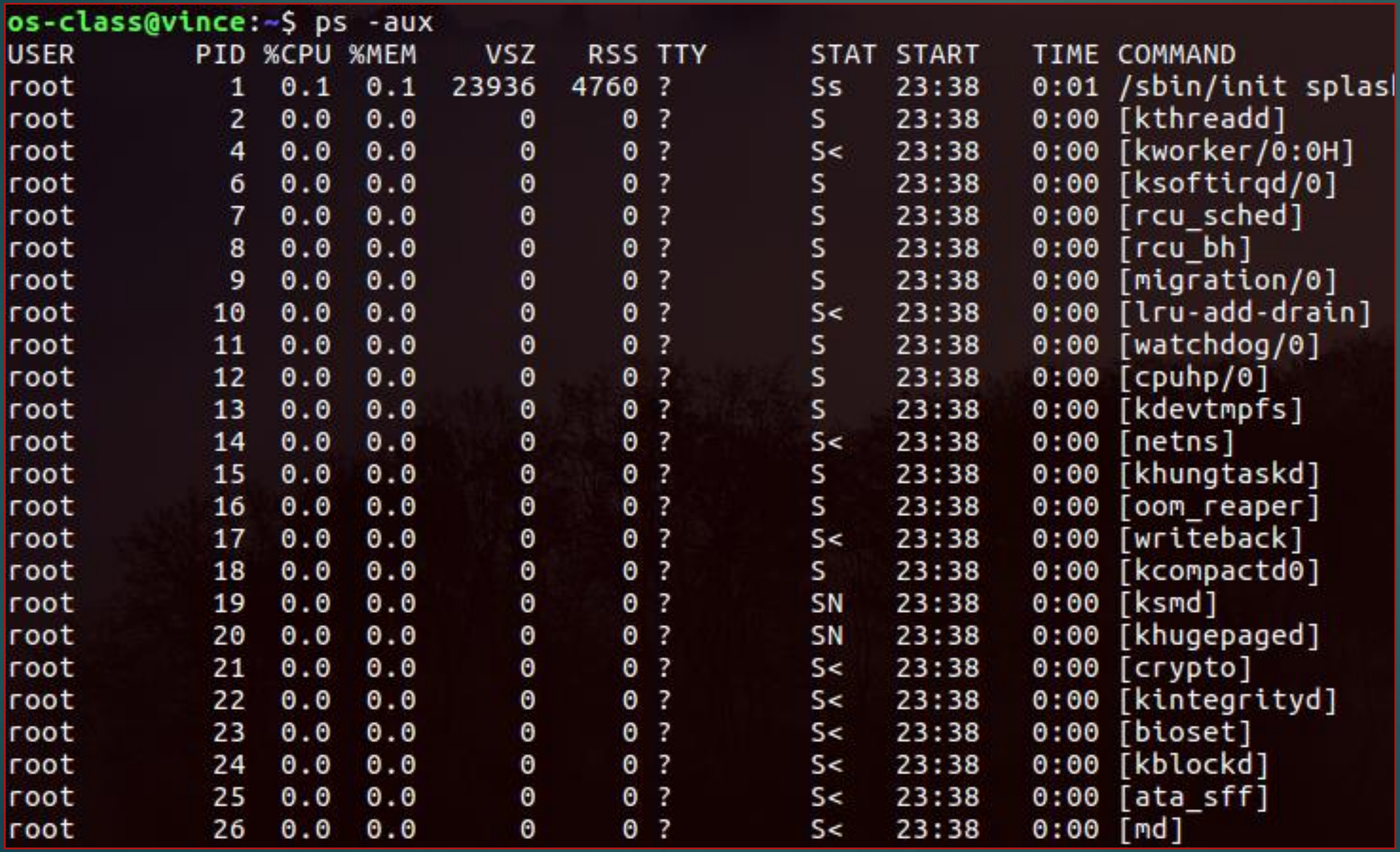
You can also run the previous command as root!



```
os-class@vince:~$ sudo systemctl -r --type service --all
  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    inactive dead    Save/Restore Sound Card State
  alsa-state.service                         loaded    inactive dead    Manage Sound Card State (restore and store)
  anacron.service                            loaded    inactive dead    Run anacron jobs
  apparmor.service                           loaded    active   exited  LSB: AppArmor initialization
  apport.service                             loaded    active   exited  LSB: automatic crash report generation
  apt-daily-upgrade.service                  loaded    inactive dead    Daily apt upgrade and clean activities
  apt-daily.service                          loaded    inactive dead    Daily apt download activities
● auditd.service                             not-found inactive dead    auditd.service
  avahi-daemon.service                       loaded    active   running Avahi mDNS/DNS-SD Stack
  binfmt-support.service                     loaded    active   exited  Enable support for additional executable binary formats
  brltty.service                             loaded    inactive dead    Braille Device Support
  colord.service                             loaded    active   running Manage, Install and Generate Color Profiles
● console-screen.service                     not-found inactive dead    console-screen.service
  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    inactive dead    CUPS Scheduler
  dbus.service                               loaded    active   running D-Bus System Message Bus
● devfsd.service                             not-found inactive dead    devfsd.service
  dns-clean.service                          loaded    inactive dead    Clean up any mess left by 0dns-up
  emergency.service                          loaded    inactive dead    Emergency Shell
```

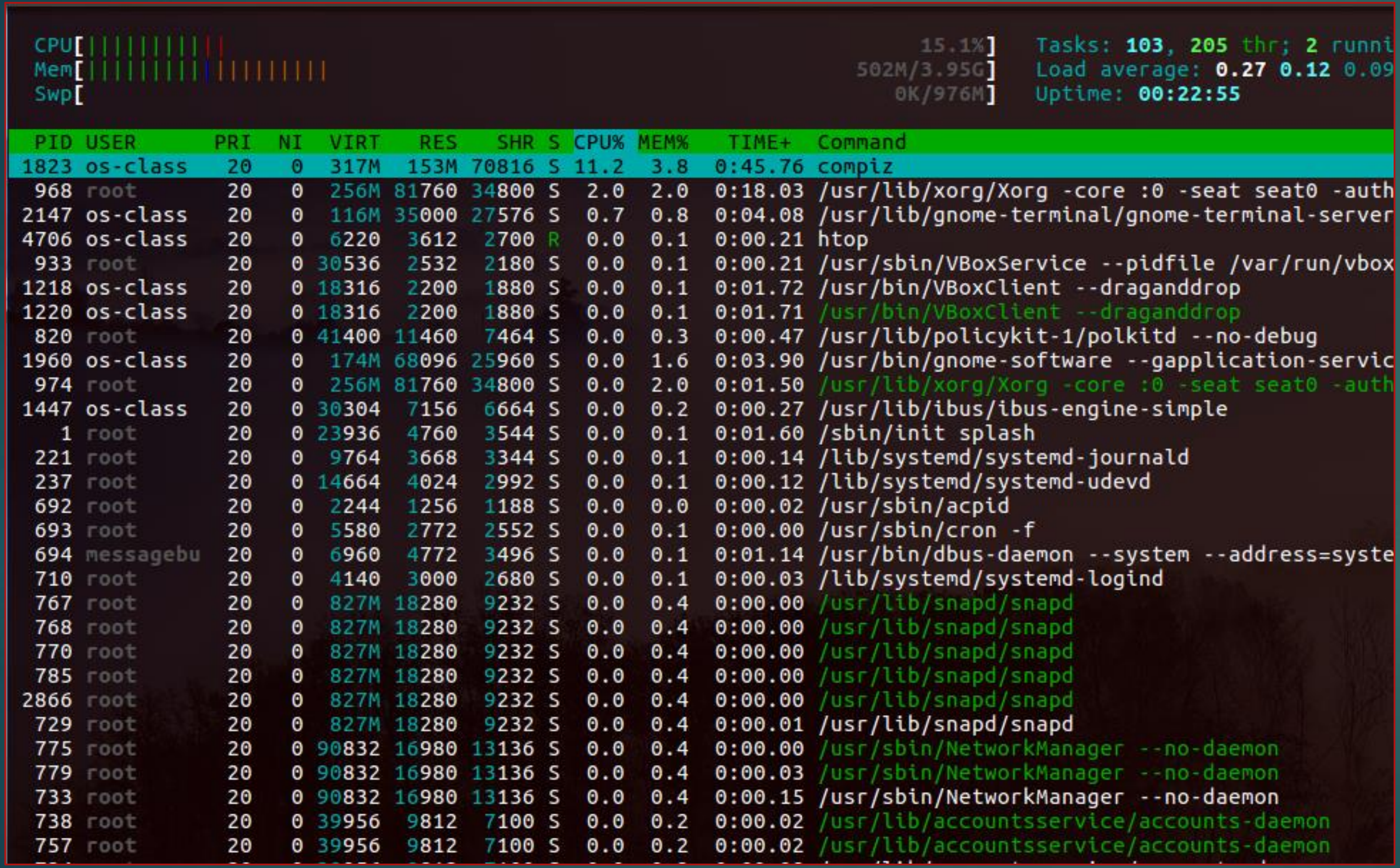
I AM ROOT
I AM ROOOOT

You can also look into your process manager to see services.



```
os-class@vince:~$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.1  23936  4760 ?        Ss   23:38   0:01 /sbin/init splas
root         2  0.0  0.0      0     0 ?        S    23:38   0:00 [kthreadd]
root         4  0.0  0.0      0     0 ?        S<   23:38   0:00 [kworker/0:0H]
root         6  0.0  0.0      0     0 ?        S    23:38   0:00 [ksoftirqd/0]
root         7  0.0  0.0      0     0 ?        S    23:38   0:00 [rcu_sched]
root         8  0.0  0.0      0     0 ?        S    23:38   0:00 [rcu_bh]
root         9  0.0  0.0      0     0 ?        S    23:38   0:00 [migration/0]
root        10  0.0  0.0      0     0 ?        S<   23:38   0:00 [lru-add-drain]
root        11  0.0  0.0      0     0 ?        S    23:38   0:00 [watchdog/0]
root        12  0.0  0.0      0     0 ?        S    23:38   0:00 [cpuhp/0]
root        13  0.0  0.0      0     0 ?        S    23:38   0:00 [kdevtmpfs]
root        14  0.0  0.0      0     0 ?        S<   23:38   0:00 [netns]
root        15  0.0  0.0      0     0 ?        S    23:38   0:00 [khungtaskd]
root        16  0.0  0.0      0     0 ?        S    23:38   0:00 [oom_reaper]
root        17  0.0  0.0      0     0 ?        S<   23:38   0:00 [writeback]
root        18  0.0  0.0      0     0 ?        S    23:38   0:00 [kcompactd0]
root        19  0.0  0.0      0     0 ?        SN   23:38   0:00 [ksmd]
root        20  0.0  0.0      0     0 ?        SN   23:38   0:00 [khugepaged]
root        21  0.0  0.0      0     0 ?        S<   23:38   0:00 [crypto]
root        22  0.0  0.0      0     0 ?        S<   23:38   0:00 [kintegrityd]
root        23  0.0  0.0      0     0 ?        S<   23:38   0:00 [bioset]
root        24  0.0  0.0      0     0 ?        S<   23:38   0:00 [kblockd]
root        25  0.0  0.0      0     0 ?        S<   23:38   0:00 [ata_sff]
root        26  0.0  0.0      0     0 ?        S<   23:38   0:00 [md]
```

htop



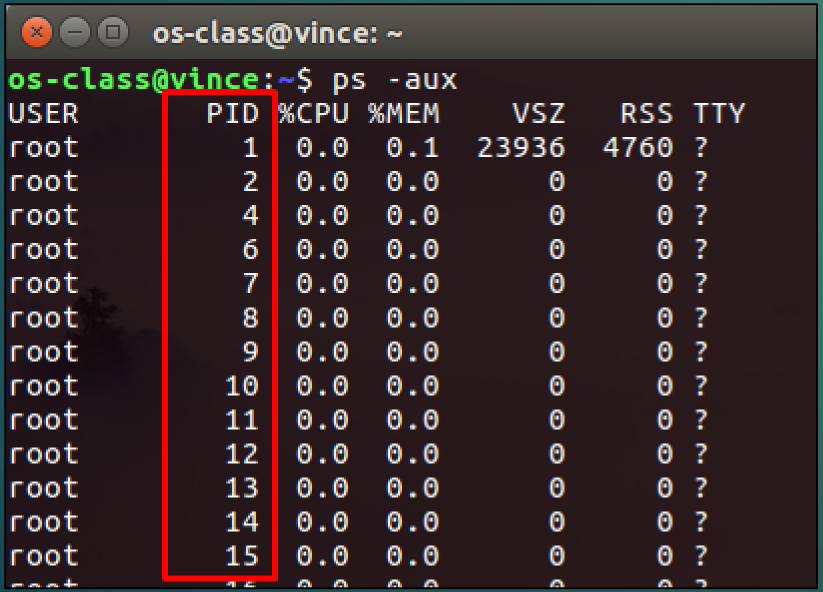
```
  CPU[|||||||||||                                              15.1%]   Tasks: 103, 205 thr; 2 runni
  Mem[|||||||||||||||||||                                 502M/3.95G]   Load average: 0.27 0.12 0.09
  Swp[                                                      0K/976M]    Uptime: 00:22:55

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 1823 os-class   20   0  317M  153M 70816 S 11.2  3.8  0:45.76 compiz
  968 root       20   0  256M 81760 34800 S  2.0  2.0  0:18.03 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth
 2147 os-class   20   0  116M 35000 27576 S  0.7  0.8  0:04.08 /usr/lib/gnome-terminal/gnome-terminal-server
 4706 os-class   20   0  6220  3612  2700 R  0.0  0.1  0:00.21 htop
  933 root       20   0 30536  2532  2180 S  0.0  0.1  0:00.21 /usr/sbin/VBoxService --pidfile /var/run/vbox
 1218 os-class   20   0 18316  2200  1880 S  0.0  0.1  0:01.72 /usr/bin/VBoxClient --draganddrop
 1220 os-class   20   0 18316  2200  1880 S  0.0  0.1  0:01.71 /usr/bin/VBoxClient --draganddrop
  820 root       20   0 41400 11460  7464 S  0.0  0.3  0:00.47 /usr/lib/policykit-1/polkitd --no-debug
 1960 os-class   20   0  174M 68096 25960 S  0.0  1.6  0:03.90 /usr/bin/gnome-software --gapplication-servic
  974 root       20   0  256M 81760 34800 S  0.0  2.0  0:01.50 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth
 1447 os-class   20   0 30304  7156  6664 S  0.0  0.2  0:00.27 /usr/lib/ibus/ibus-engine-simple
    1 root       20   0 23936  4760  3544 S  0.0  0.1  0:01.60 /sbin/init splash
  221 root       20   0  9764  3668  3344 S  0.0  0.1  0:00.14 /lib/systemd/systemd-journald
  237 root       20   0 14664  4024  2992 S  0.0  0.1  0:00.12 /lib/systemd/systemd-udevd
  692 root       20   0  2244  1256  1188 S  0.0  0.0  0:00.02 /usr/sbin/acpid
  693 root       20   0  5580  2772  2552 S  0.0  0.1  0:00.00 /usr/sbin/cron -f
  694 messagebu  20   0  6960  4772  3496 S  0.0  0.1  0:01.14 /usr/bin/dbus-daemon --system --address=syste
  710 root       20   0  4140  3000  2680 S  0.0  0.1  0:00.03 /lib/systemd/systemd-logind
  767 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.00 /usr/lib/snapd/snapd
  768 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.00 /usr/lib/snapd/snapd
  770 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.00 /usr/lib/snapd/snapd
  785 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.00 /usr/lib/snapd/snapd
 2866 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.00 /usr/lib/snapd/snapd
  729 root       20   0  827M 18280  9232 S  0.0  0.4  0:00.01 /usr/lib/snapd/snapd
  775 root       20   0 90832 16980 13136 S  0.0  0.4  0:00.00 /usr/sbin/NetworkManager --no-daemon
  779 root       20   0 90832 16980 13136 S  0.0  0.4  0:00.03 /usr/sbin/NetworkManager --no-daemon
  733 root       20   0 90832 16980 13136 S  0.0  0.4  0:00.15 /usr/sbin/NetworkManager --no-daemon
  738 root       20   0 39956  9812  7100 S  0.0  0.2  0:00.02 /usr/lib/accountsservice/accounts-daemon
  757 root       20   0 39956  9812  7100 S  0.0  0.2  0:00.02 /usr/lib/accountsservice/accounts-daemon
```

- htop is not always there
- **`sudo apt-get install htop`**

The **kill** command

Some Explanation

- the command is used to end a process without having to log out or reboot
- a process is also referred to as a *task* that is in a running state
- these processes are given *process identification numbers (PID) – we need this as reference!*



```
os-class@vince:~$ ps -aux
USER       PID %CPU %MEM    VSZ   RSS TTY
root         1  0.0  0.1  23936  4760 ?
root         2  0.0  0.0      0     0 ?
root         4  0.0  0.0      0     0 ?
root         6  0.0  0.0      0     0 ?
root         7  0.0  0.0      0     0 ?
root         8  0.0  0.0      0     0 ?
root         9  0.0  0.0      0     0 ?
root        10  0.0  0.0      0     0 ?
root        11  0.0  0.0      0     0 ?
root        12  0.0  0.0      0     0 ?
root        13  0.0  0.0      0     0 ?
root        14  0.0  0.0      0     0 ?
root        15  0.0  0.0      0     0 ?
```

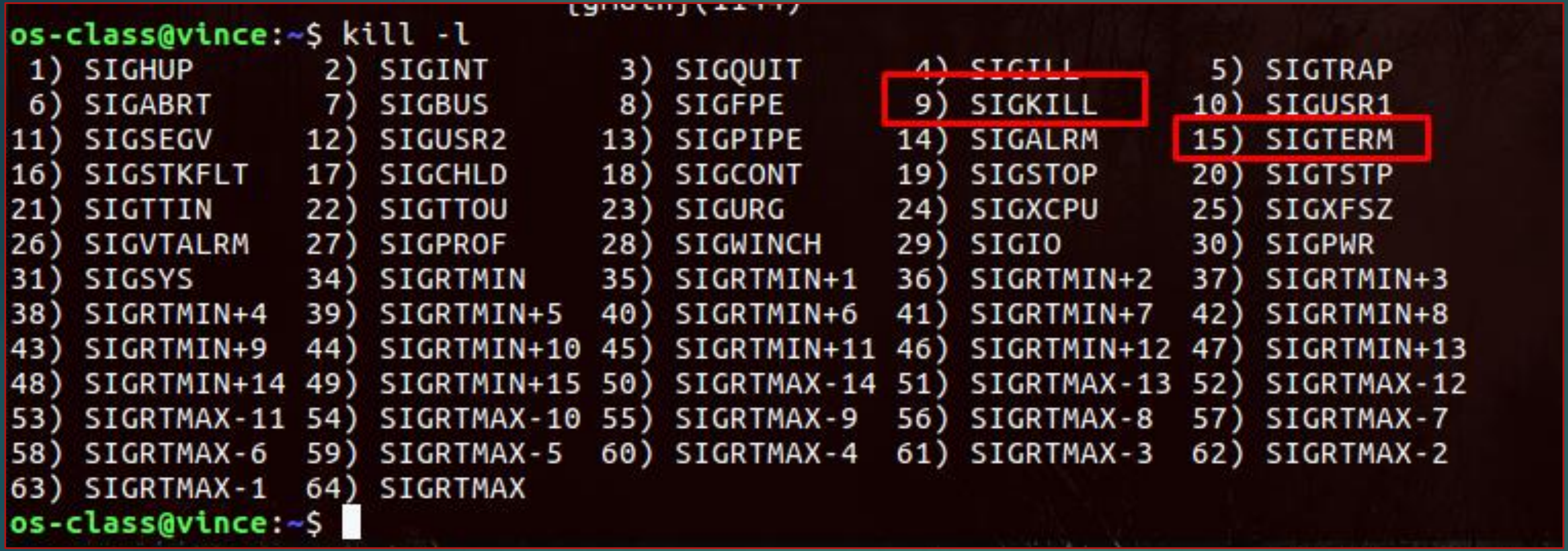
kill [PID]

- this works… but no guarantee the process will end
- this by default sends signal 15, sometimes services will ignore this

kill -9 [PID]

- this command is a little misleading, it doesn’t actually *kill the process rather it send a signal to that process*
- *what that process does with that signal is up to the process itself*
- *processes have signal handlers, these define what it does with a signal*
- *our command from before “kill [PID]” has no signal supplied, therefore it defaults to 15*
- ***`kill -9 [PID]`*** *is stronger, this signal is* ***SIGKILL***

kill -l



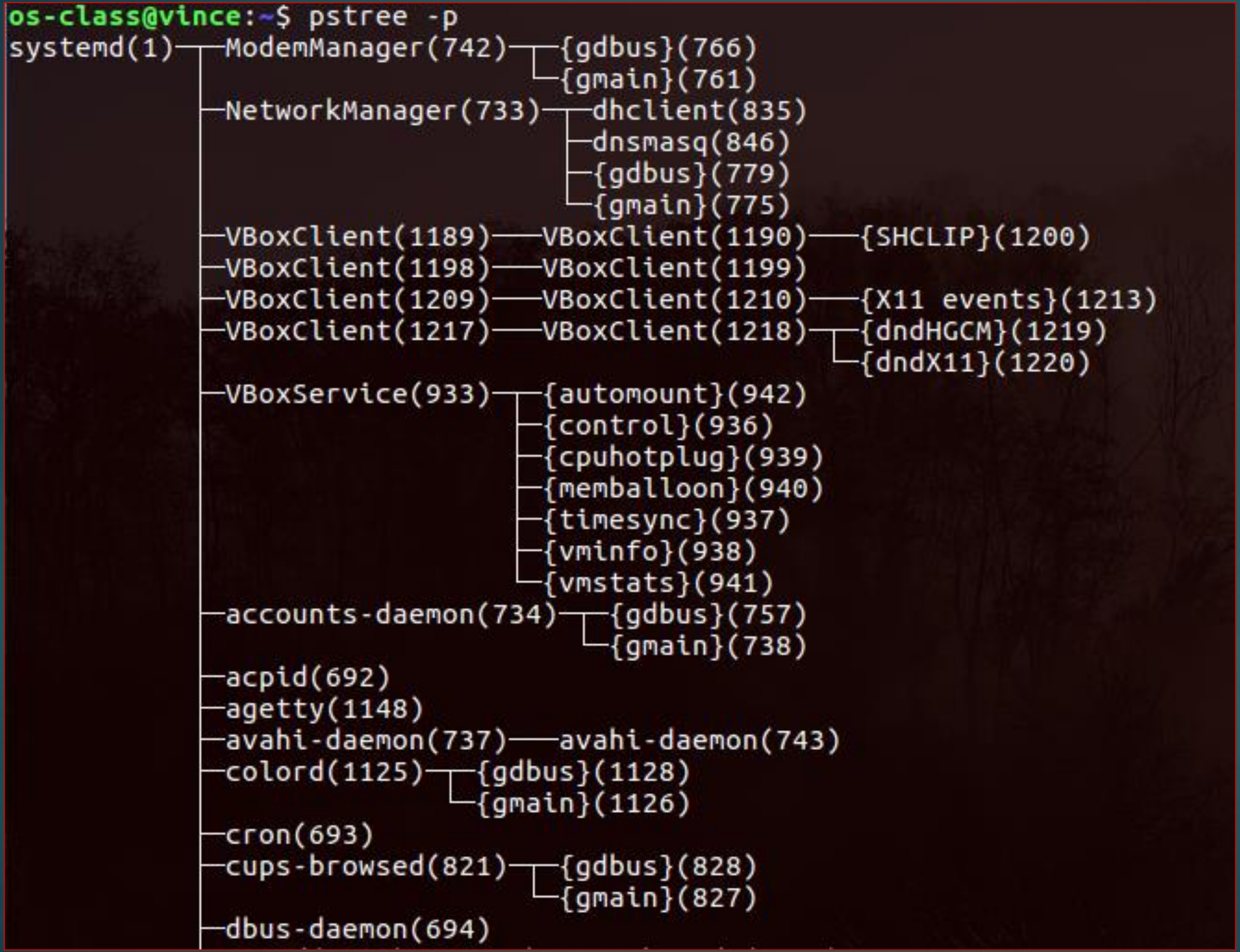
```
os-class@vince:~$ kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
os-class@vince:~$
```

- we can use this to see the signal handlers

http://www.linfo.org/kill.html

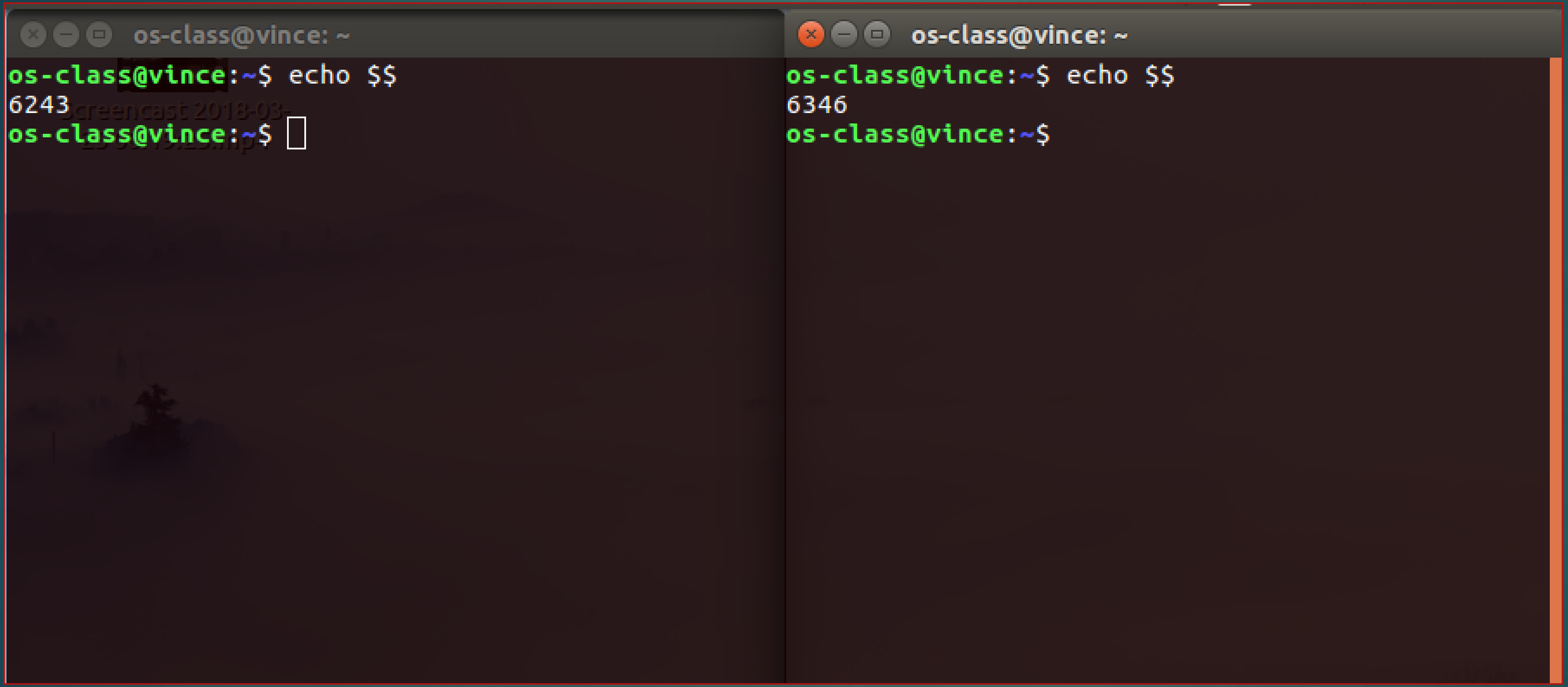
pstree -p

- this command is interesting…
- we can actually use this to see the parent/ child relationship of processes, and by killing the parent process this will kill the child processes
- this makes it much easier to end processes, versus manually finding each PID



```
os-class@vince:~$ pstree -p
systemd(1)─┬─ModemManager(742)─┬─{gdbus}(766)
           │                   └─{gmain}(761)
           ├─NetworkManager(733)─┬─dhclient(835)
           │                     ├─dnsmasq(846)
           │                     ├─{gdbus}(779)
           │                     └─{gmain}(775)
           ├─VBoxClient(1189)───VBoxClient(1190)───{SHCLIP}(1200)
           ├─VBoxClient(1198)───VBoxClient(1199)
           ├─VBoxClient(1209)───VBoxClient(1210)───{X11 events}(1213)
           ├─VBoxClient(1217)───VBoxClient(1218)─┬─{dndHGCM}(1219)
           │                                     └─{dndX11}(1220)
           ├─VBoxService(933)─┬─{automount}(942)
           │                  ├─{control}(936)
           │                  ├─{cpuhotplug}(939)
           │                  ├─{memballoon}(940)
           │                  ├─{timesync}(937)
           │                  ├─{vminfo}(938)
           │                  └─{vmstats}(941)
           ├─accounts-daemon(734)─┬─{gdbus}(757)
           │                      └─{gmain}(738)
           ├─acpid(692)
           ├─agetty(1148)
           ├─avahi-daemon(737)───avahi-daemon(743)
           ├─colord(1125)─┬─{gdbus}(1128)
           │              └─{gmain}(1126)
           ├─cron(693)
           ├─cups-browsed(821)─┬─{gdbus}(828)
           │                   └─{gmain}(827)
           ├─dbus-daemon(694)
```

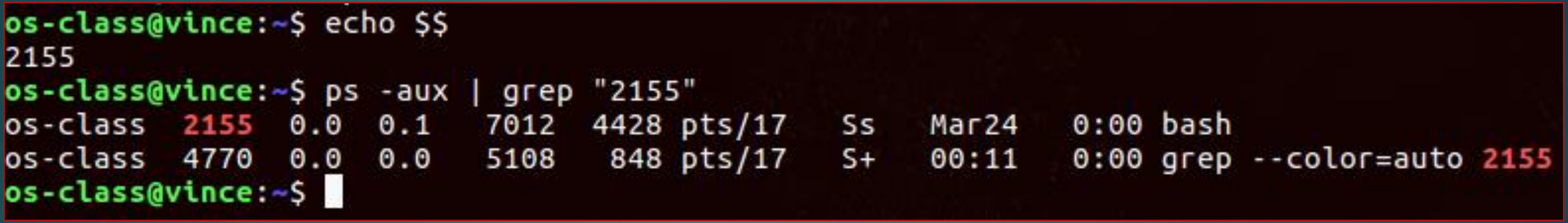
Ross Likes to Kill Bash Sessions



```
os-class@vince:~$ echo $$
6243
os-class@vince:~$ 
```

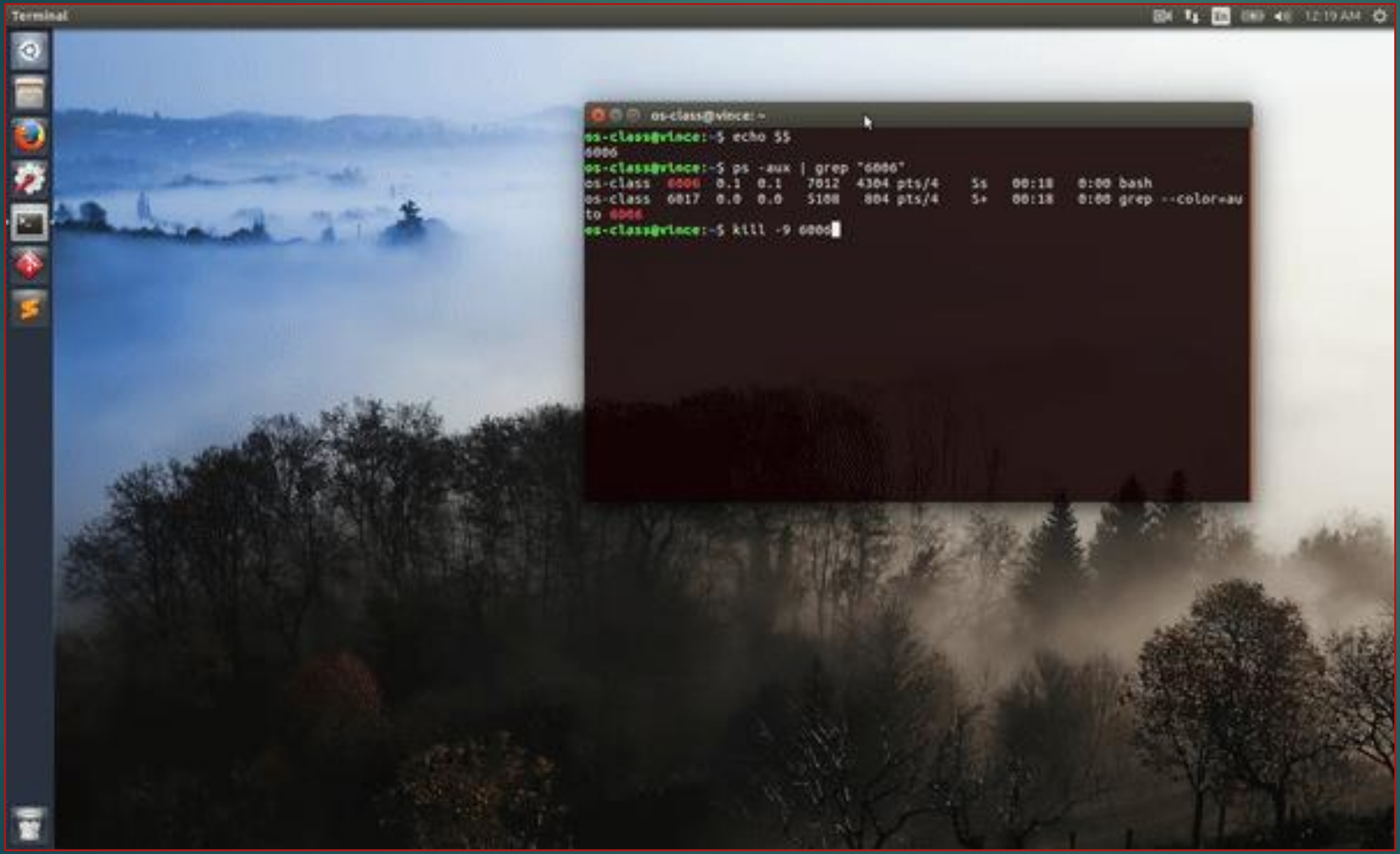
```
os-class@vince:~$ echo $$
6346
os-class@vince:~$
```

echo $$



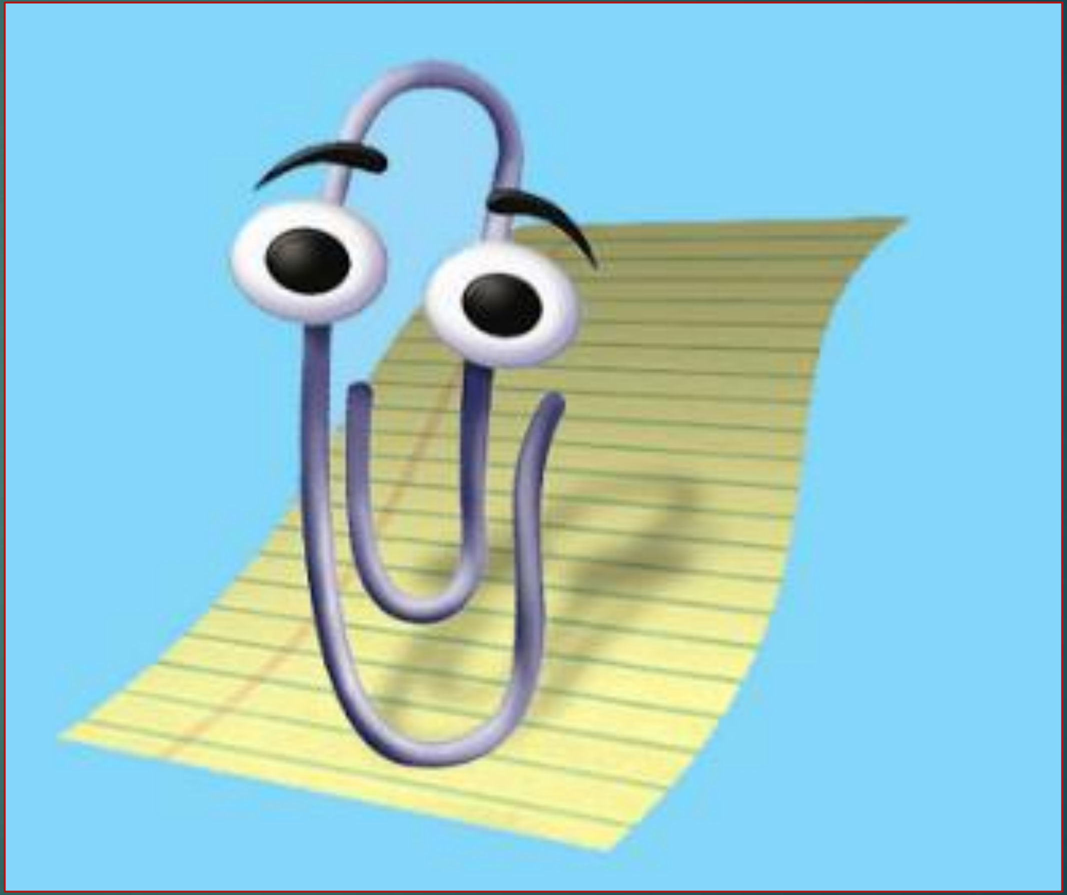
```
os-class@vince:~$ echo $$
2155
os-class@vince:~$ ps -aux | grep "2155"
os-class  2155  0.0  0.1   7012  4428 pts/17   Ss   Mar24   0:00 bash
os-class  4770  0.0  0.0   5108   848 pts/17   S+   00:11   0:00 grep --color=auto 2155
os-class@vince:~$
```

What happens if I do `kill -9 2155`?

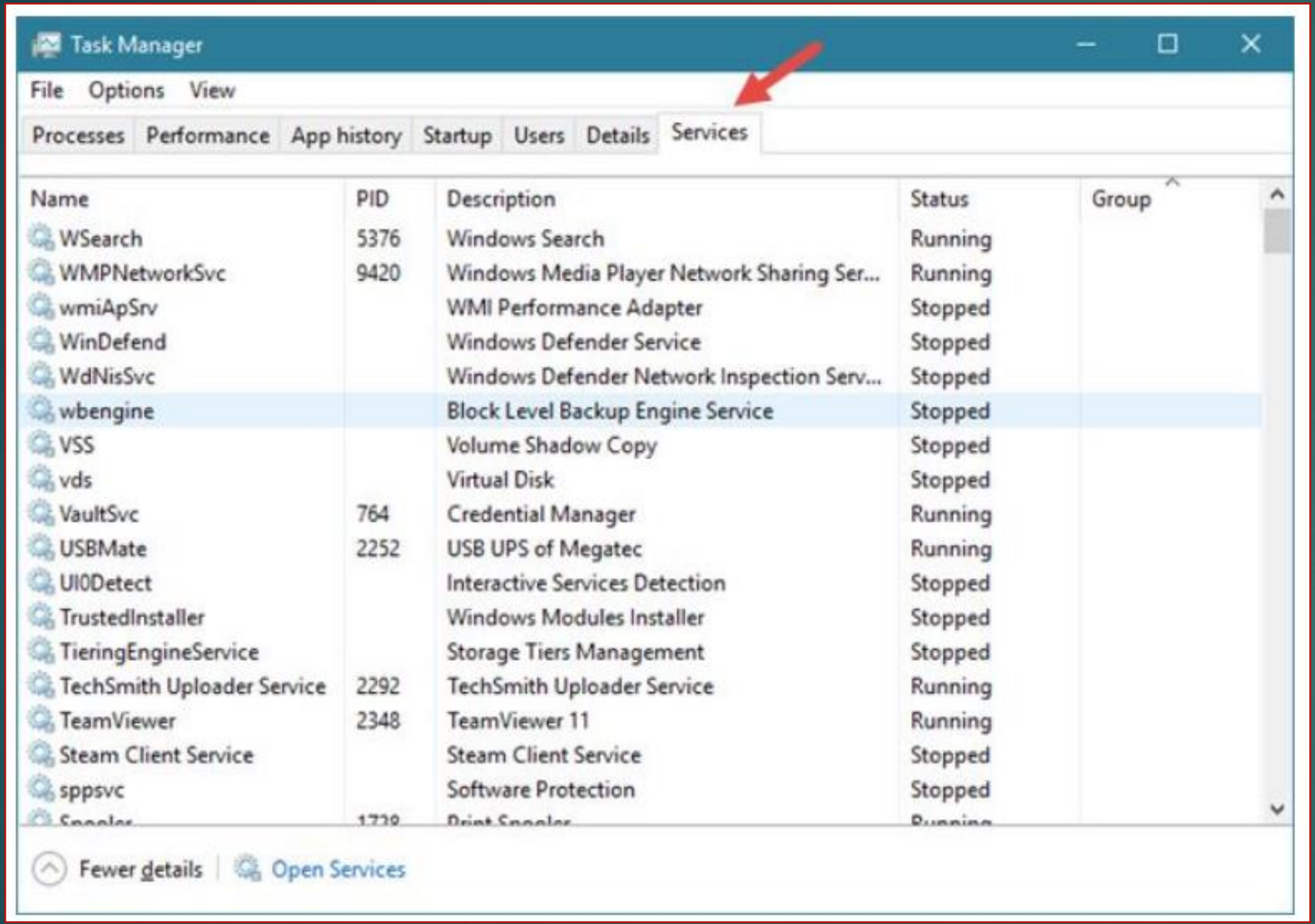


```
os-class@vince:~$ echo $$
6006
os-class@vince:~$ ps -aux | grep "6006"
os-class  6006  0.1  0.1   7012  4304 pts/4    Ss   00:18   0:00 bash
os-class  6017  0.0  0.0   5108   804 pts/4    S+   00:18   0:00 grep --color=au
to 6006
os-class@vince:~$ kill -9 6006
```

WINDOWS LAND!

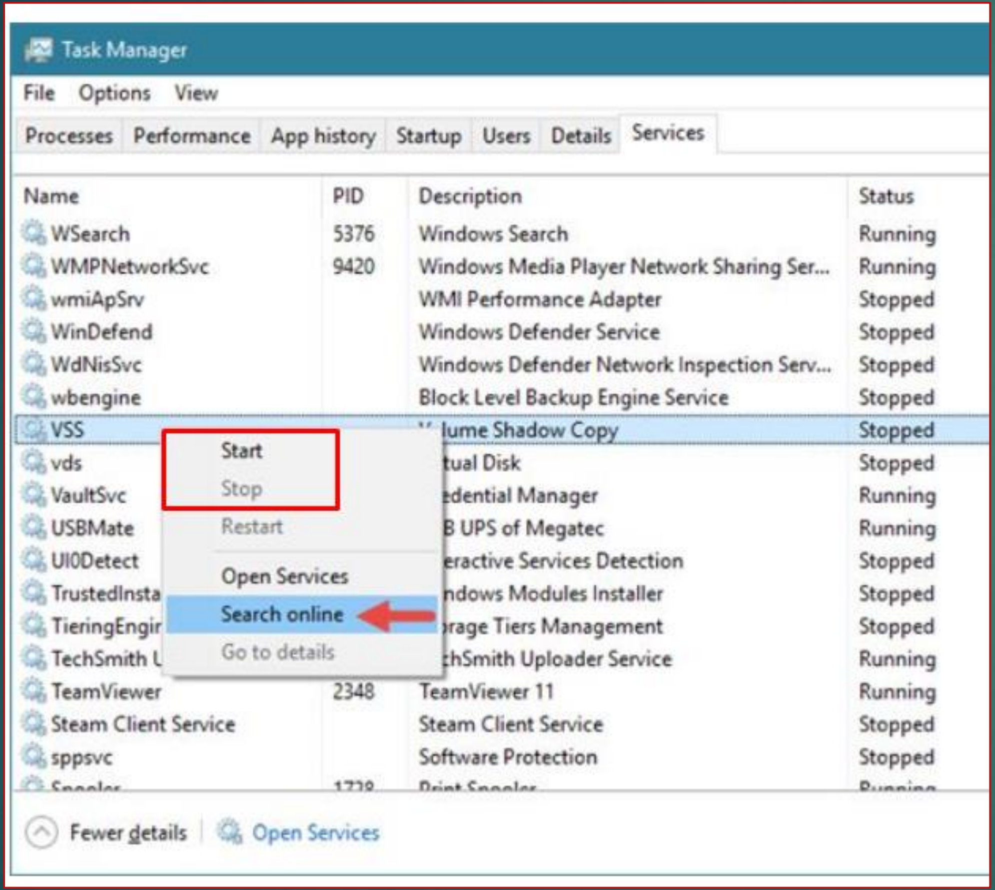


Task Manager



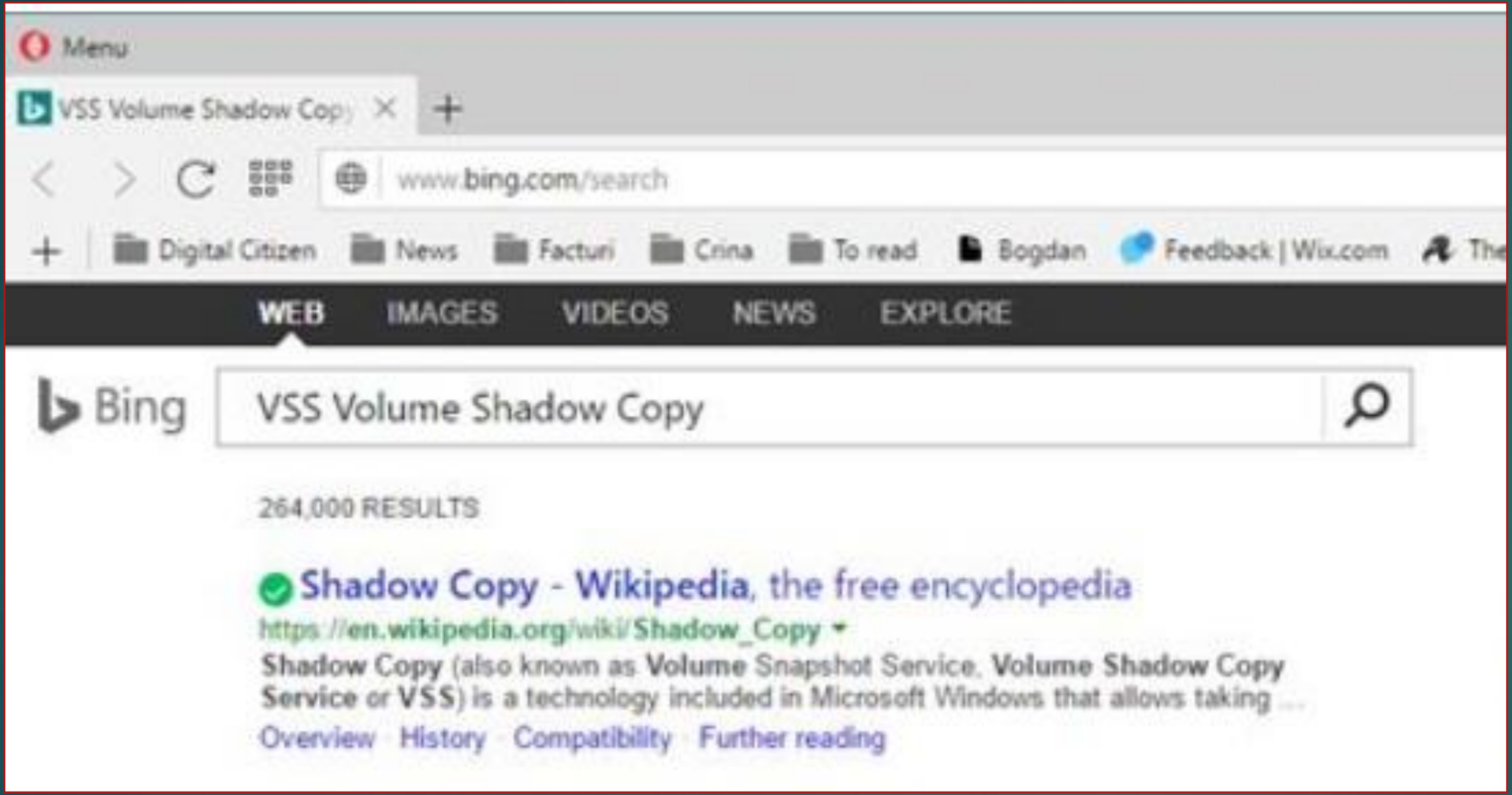
Name	PID	Description	Status	Group
WSearch	5376	Windows Search	Running	
WMPNetworkSvc	9420	Windows Media Player Network Sharing Ser...	Running	
wmiApSrv		WMI Performance Adapter	Stopped	
WinDefend		Windows Defender Service	Stopped	
WdNisSvc		Windows Defender Network Inspection Serv...	Stopped	
wbengine		Block Level Backup Engine Service	Stopped	
VSS		Volume Shadow Copy	Stopped	
vds		Virtual Disk	Stopped	
VaultSvc	764	Credential Manager	Running	
USBMate	2252	USB UPS of Megatec	Running	
UI0Detect		Interactive Services Detection	Stopped	
TrustedInstaller		Windows Modules Installer	Stopped	
TieringEngineService		Storage Tiers Management	Stopped	
TechSmith Uploader Service	2292	TechSmith Uploader Service	Running	
TeamViewer	2348	TeamViewer 11	Running	
Steam Client Service		Steam Client Service	Stopped	
sppsvc		Software Protection	Stopped	
Spooler	1728	Print Spooler	Running	

Right click on a service to start **or** stop it?



Name	PID	Description	Status
WSearch	5376	Windows Search	Running
WMPNetworkSvc	9420	Windows Media Player Network Sharing Ser...	Running
wmiApSrv		WMI Performance Adapter	Stopped
WinDefend		Windows Defender Service	Stopped
WdNisSvc		Windows Defender Network Inspection Serv...	Stopped
wbengine		Block Level Backup Engine Service	Stopped
VSS		lume Shadow Copy	Stopped
vds		tual Disk	Stopped
VaultSvc		edential Manager	Running
USBMate		B UPS of Megatec	Running
UI0Detect		eractive Services Detection	Stopped
TrustedInsta		ndows Modules Installer	Stopped
TieringEngir		rage Tiers Management	Stopped
TechSmith U		chSmith Uploader Service	Running
TeamViewer	2348	TeamViewer 11	Running
Steam Client Service		Steam Client Service	Stopped
sppsvc		Software Protection	Stopped
Spooler	1728	Print Spooler	Running

You can search online too!



VSS Volume Shadow Copy

264,000 RESULTS

Shadow Copy - Wikipedia, the free encyclopedia

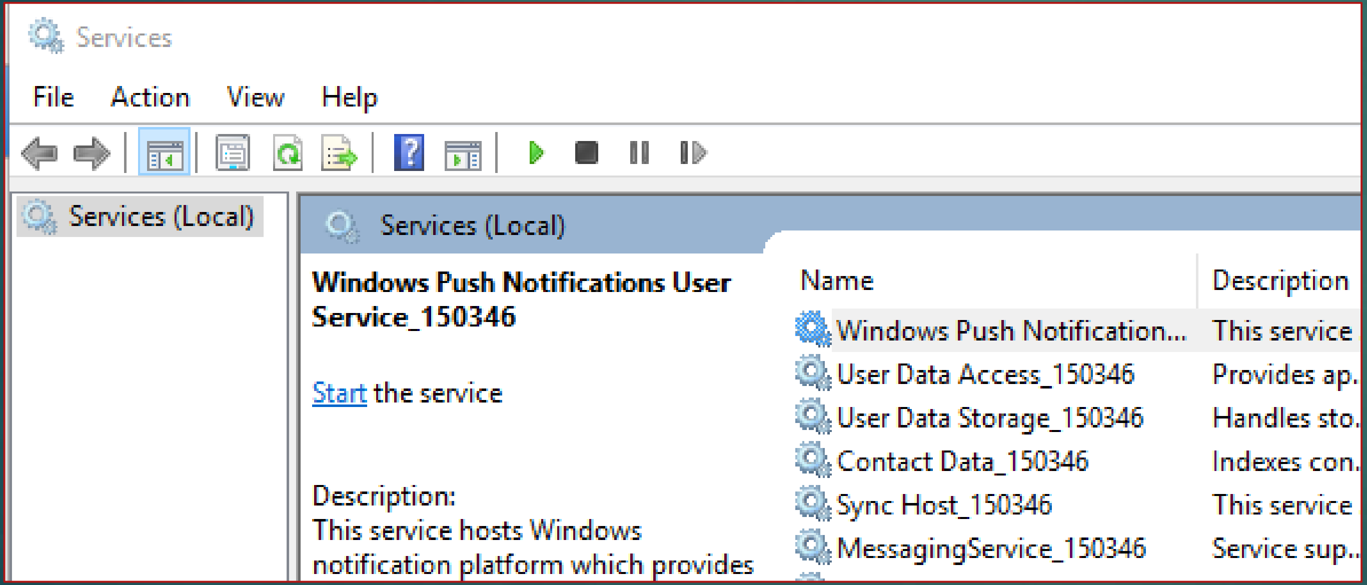
https://en.wikipedia.org/wiki/Shadow_Copy

Shadow Copy (also known as **Volume** Snapshot Service, **Volume Shadow Copy Service** or **VSS**) is a technology included in Microsoft Windows that allows taking ...

Overview · History · Compatibility · Further reading

services.msc

- CMD -> services.msc
- Windows search for “Services”



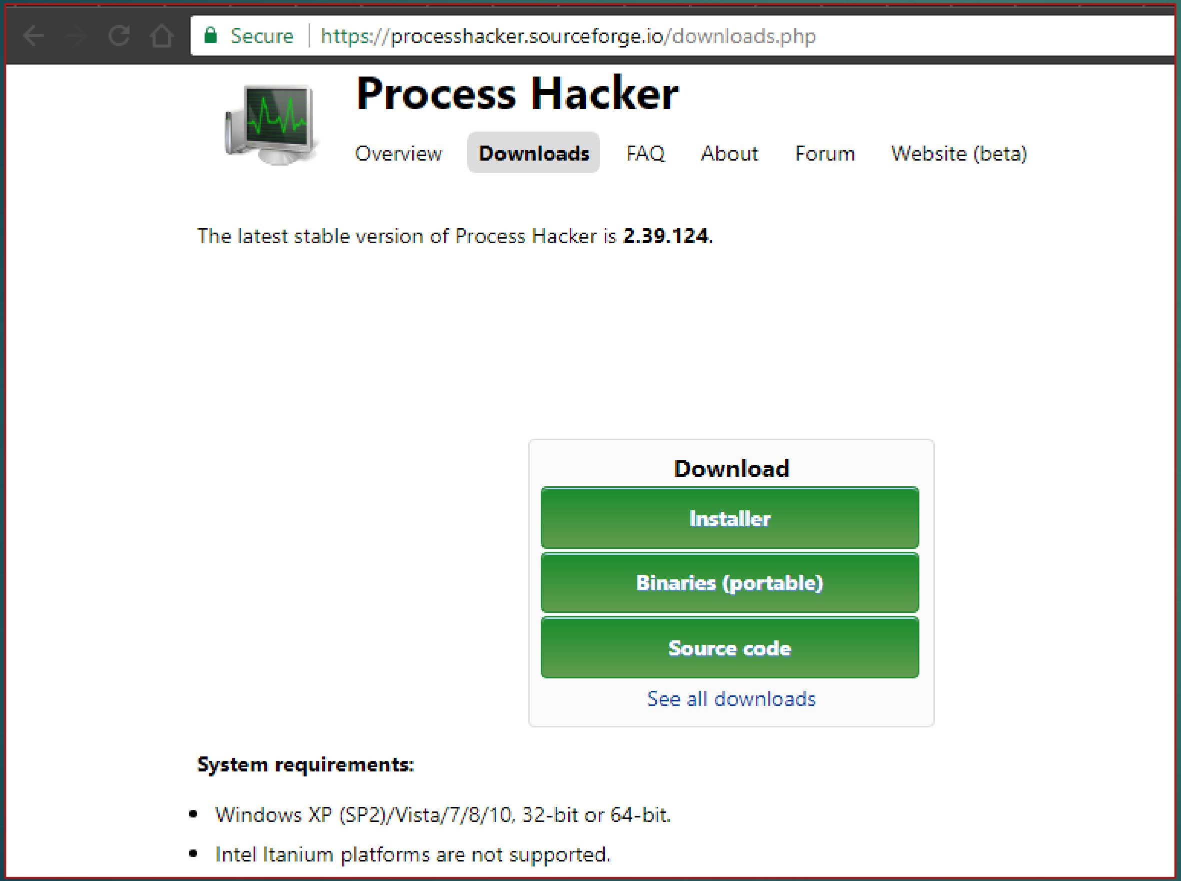
Windows Push Notifications User Service_150346

Start the service

Description:
This service hosts Windows notification platform which provides

Name	Description
Windows Push Notification...	This service
User Data Access_150346	Provides ap..
User Data Storage_150346	Handles sto..
Contact Data_150346	Indexes con..
Sync Host_150346	This service
MessagingService_150346	Service sup..

These tools are sort of… bland… incomes “Process hacker”

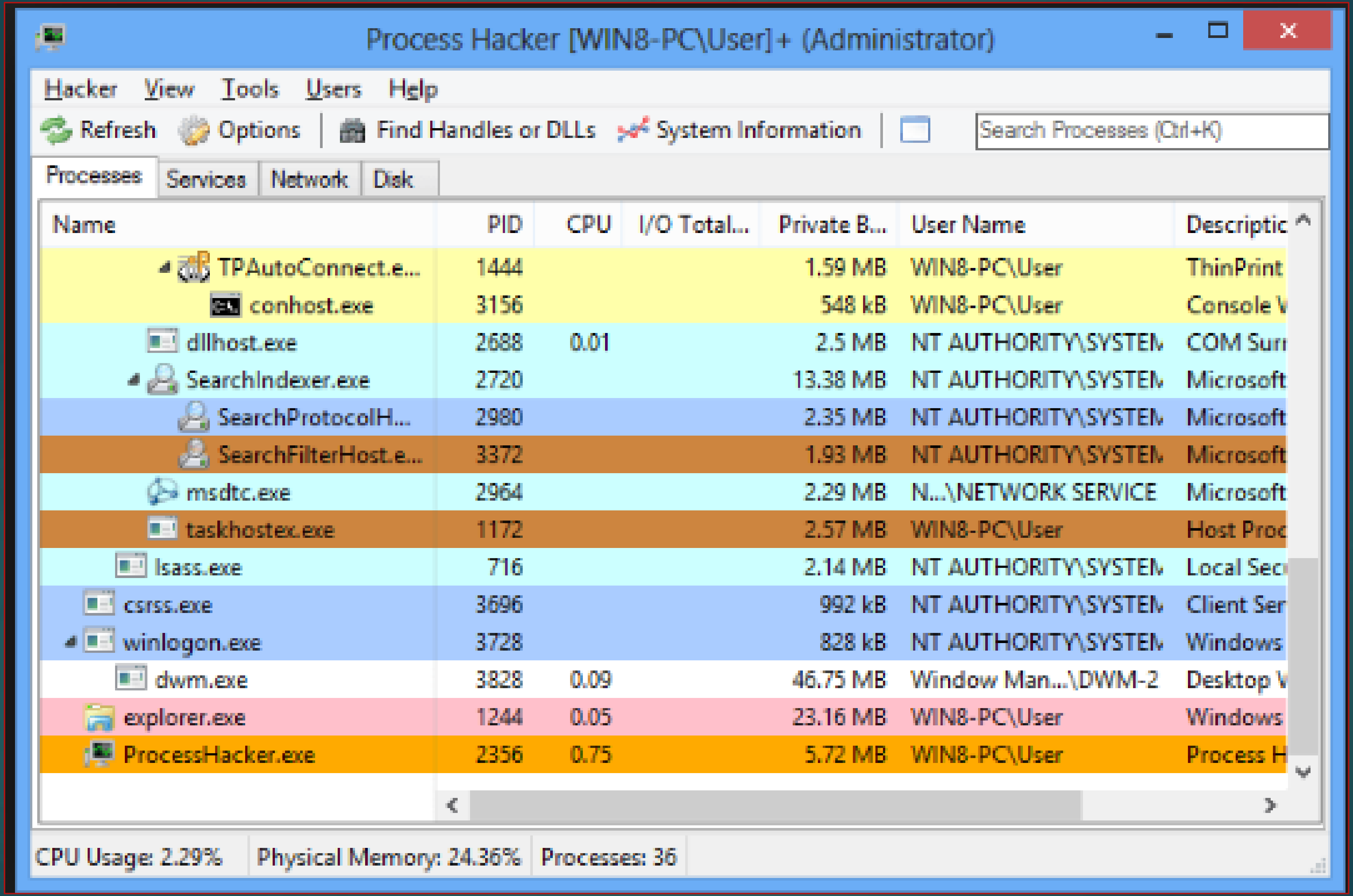


Process Hacker

The latest stable version of Process Hacker is **2.39.124**.

System requirements:

- Windows XP (SP2)/Vista/7/8/10, 32-bit or 64-bit.
- Intel Itanium platforms are not supported.

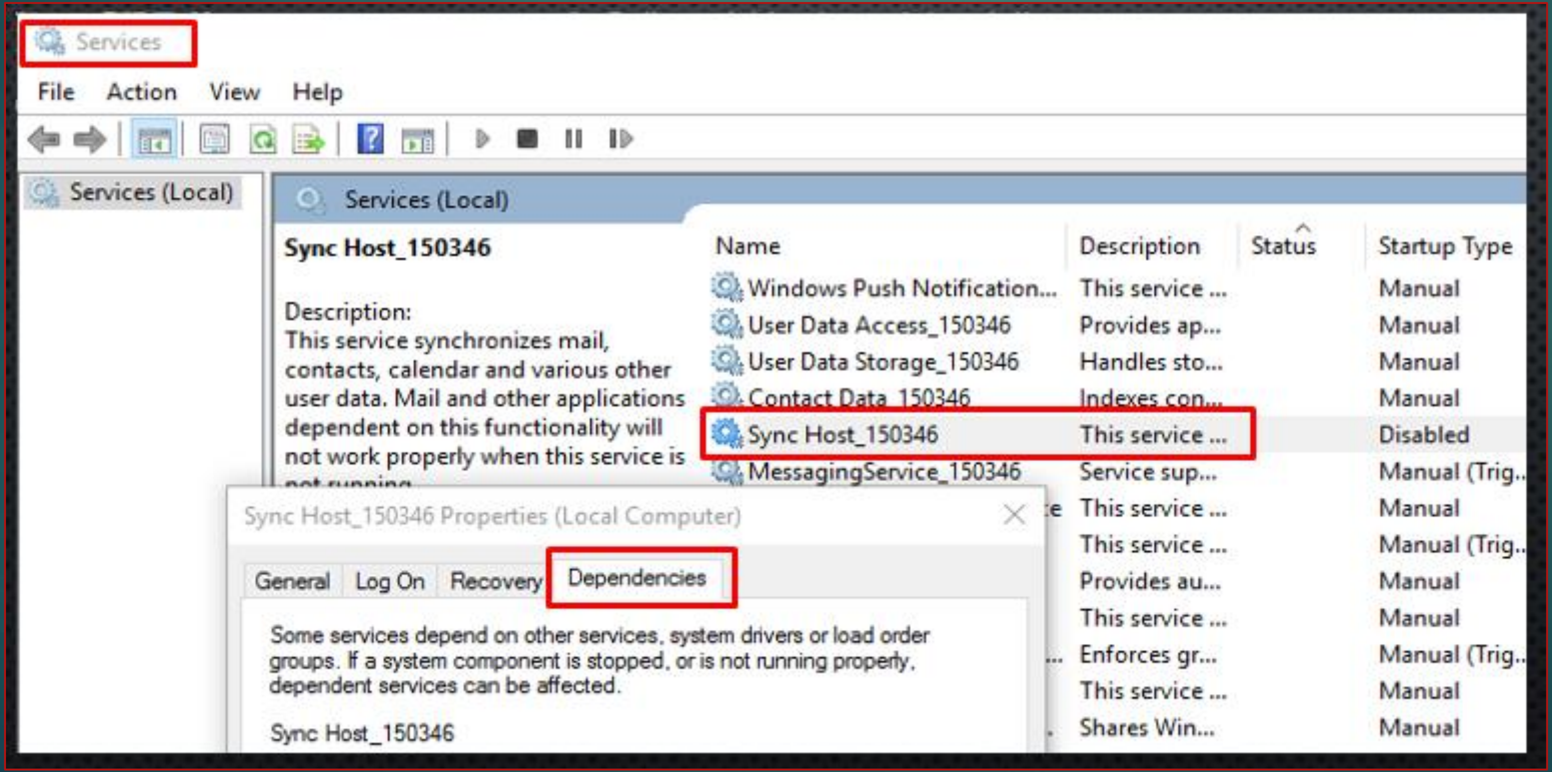


Name	PID	CPU	I/O Total...	Private B...	User Name	Descriptic
TPAutoConnect.e...	1444			1.59 MB	WIN8-PC\User	ThinPrint
conhost.exe	3156			548 kB	WIN8-PC\User	Console
dllhost.exe	2688	0.01		2.5 MB	NT AUTHORITY\SYSTEM	COM Surr
SearchIndexer.exe	2720			13.38 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchProtocolH...	2980			2.35 MB	NT AUTHORITY\SYSTEM	Microsoft
SearchFilterHost.e...	3372			1.93 MB	NT AUTHORITY\SYSTEM	Microsoft
msdtc.exe	2964			2.29 MB	N...\NETWORK SERVICE	Microsoft
taskhostex.exe	1172			2.57 MB	WIN8-PC\User	Host Proc
lsass.exe	716			2.14 MB	NT AUTHORITY\SYSTEM	Local Sec
csrss.exe	3696			992 kB	NT AUTHORITY\SYSTEM	Client Ser
winlogon.exe	3728			828 kB	NT AUTHORITY\SYSTEM	Windows
dwm.exe	3828	0.09		46.75 MB	Window Man...\DWM-2	Desktop W
explorer.exe	1244	0.05		23.16 MB	WIN8-PC\User	Windows
ProcessHacker.exe	2356	0.75		5.72 MB	WIN8-PC\User	Process H

CPU Usage: 2.29% | Physical Memory: 24.36% | Processes: 36

Beware some services have dependencies!

- Windows firewall service depends on base filtering engine
- some services may not stop or start if a dependency is stopped



Sync Host_150346

Description:
This service synchronizes mail, contacts, calendar and various other user data. Mail and other applications dependent on this functionality will not work properly when this service is not running.

Name	Description	Status	Startup Type
Windows Push Notification...	This service ...		Manual
User Data Access_150346	Provides ap...		Manual
User Data Storage_150346	Handles sto...		Manual
Contact Data_150346	Indexes con...		Manual
Sync Host_150346	This service ...		Disabled
MessagingService_150346	Service sup...		Manual (Trig...
e	This service ...		Manual
	This service ...		Manual (Trig...
	Provides au...		Manual
	This service ...		Manual
...	Enforces gr...		Manual (Trig...
	This service ...		Manual
.	Shares Win...		Manual

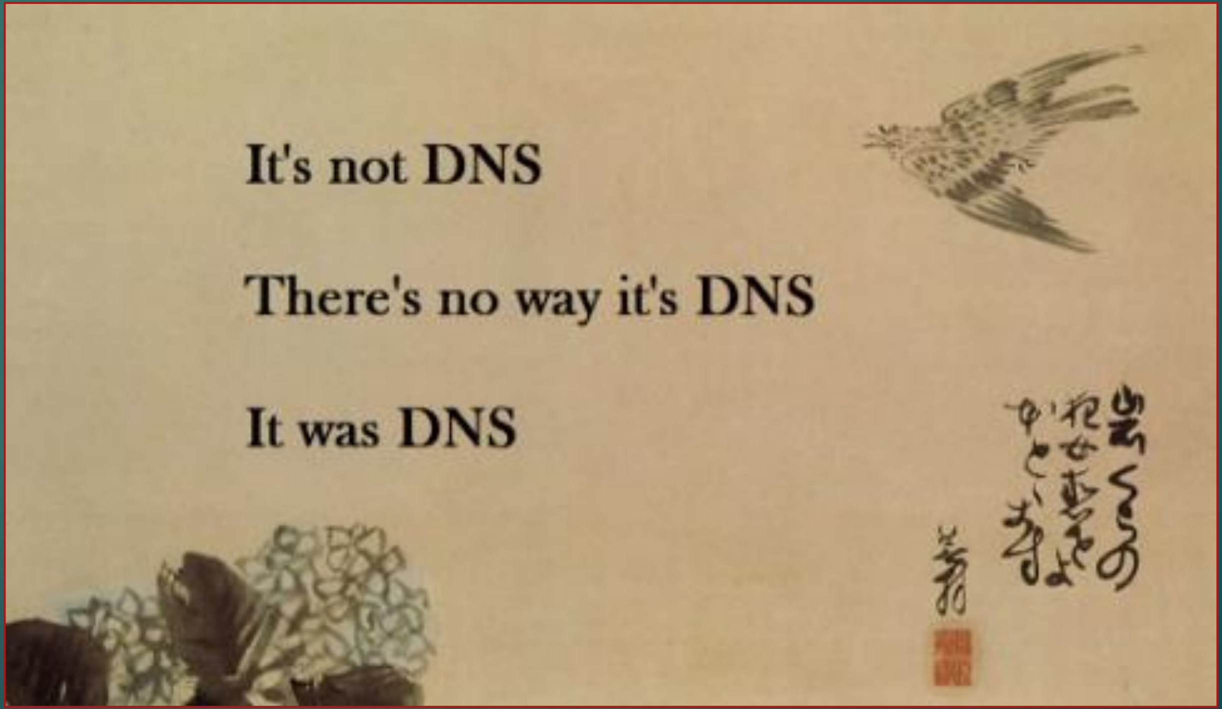
Sync Host_150346 Properties (Local Computer)

Some services depend on other services, system drivers or load order groups. If a system component is stopped, or is not running properly, dependent services can be affected.

Sync Host_150346

Active Directory

- this is a major Windows directory service!
- is AD broken?
  - check DNS
    - it was DNS…

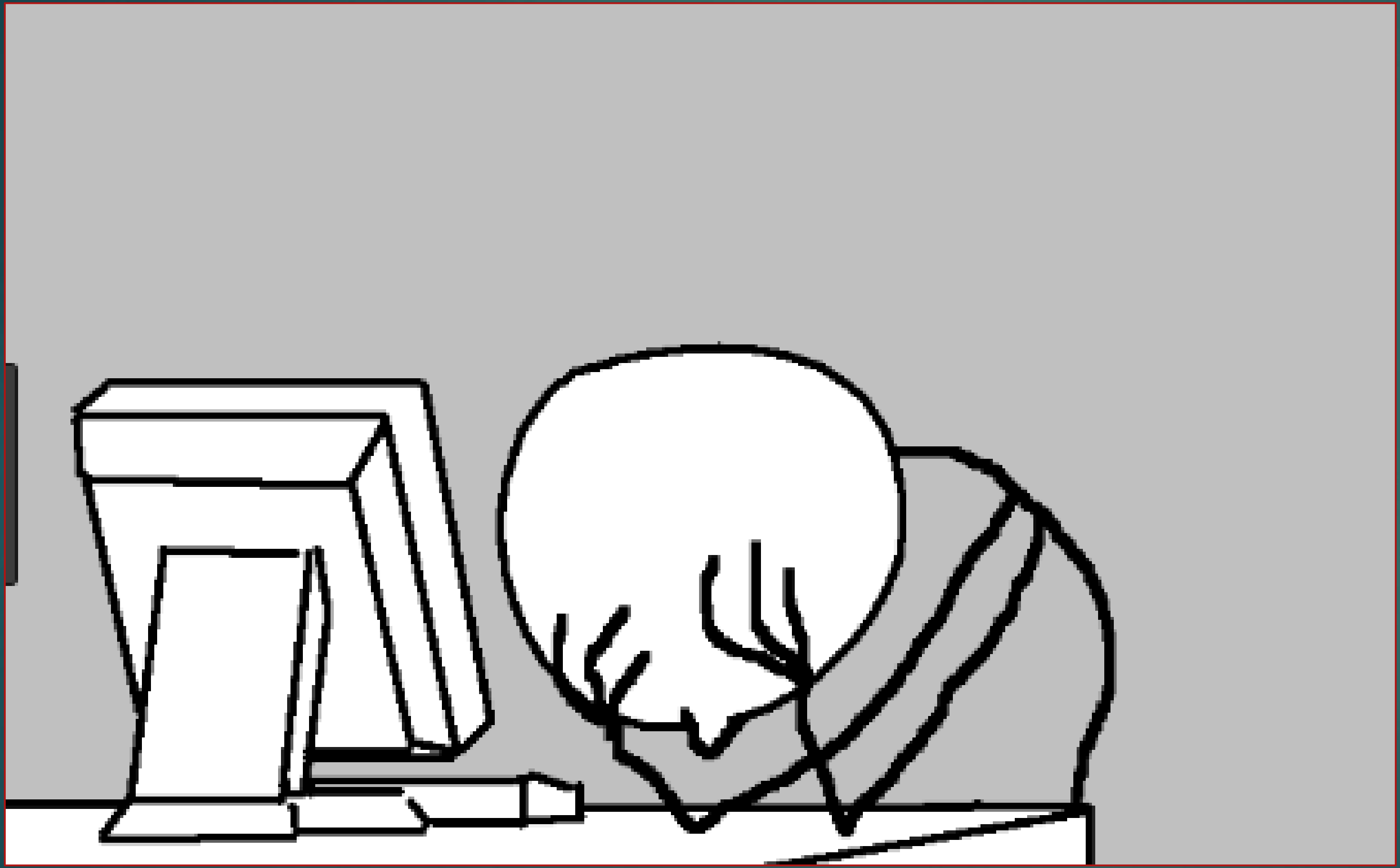


It's not DNS

There's no way it's DNS

It was DNS

That’s all for services, any questions?



These next slides are mainly competition help!

Welcome to Lockdown.

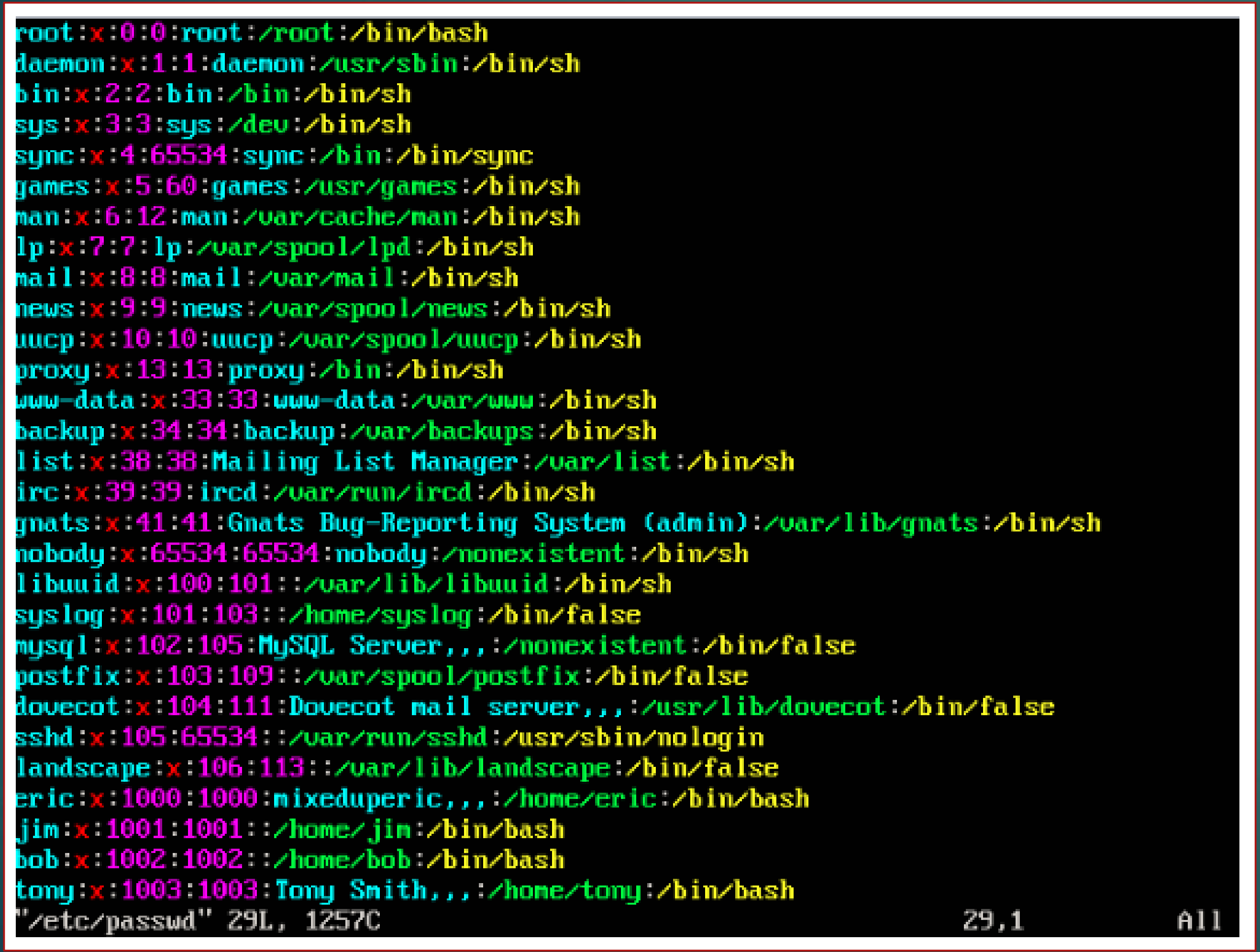
Lockdown is a defensive security competition run by the University at Buffalo Network Defense.

Auditing Your Box

- this is very important to in competitions!
- we actually covered a lot of auditing by just looking at services!

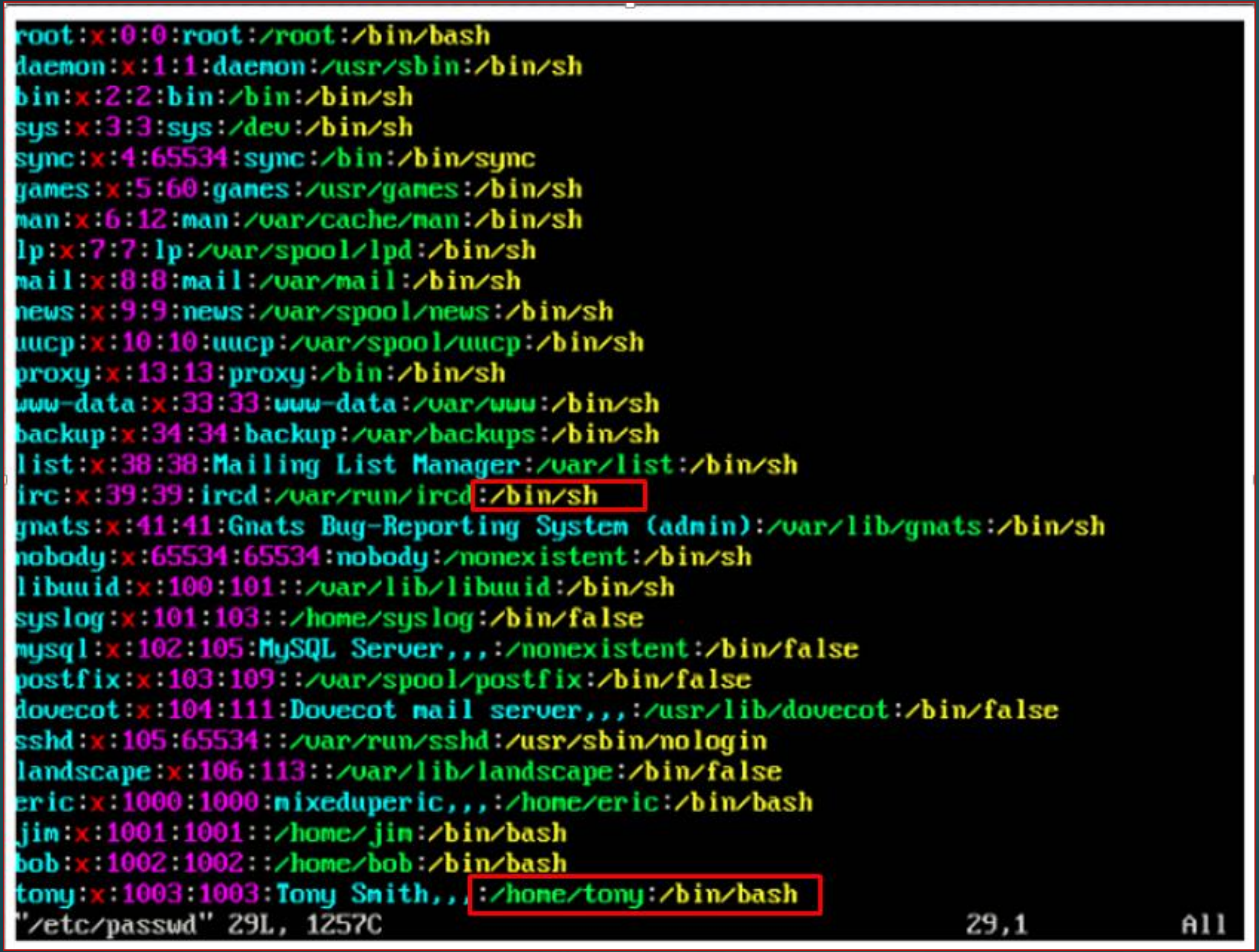
1st Step, Check the Users

`cat /etc/passwd`



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:103:109::/var/spool/postfix:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:106:113::/var/lib/landscape:/bin/false
eric:x:1000:1000:mixeduperic,,,:/home/eric:/bin/bash
jim:x:1001:1001::/home/jim:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
tony:x:1003:1003:Tony Smith,,,:/home/tony:/bin/bash
"/etc/passwd" 29L, 1257C                                  29,1          All
```

What do you notice?



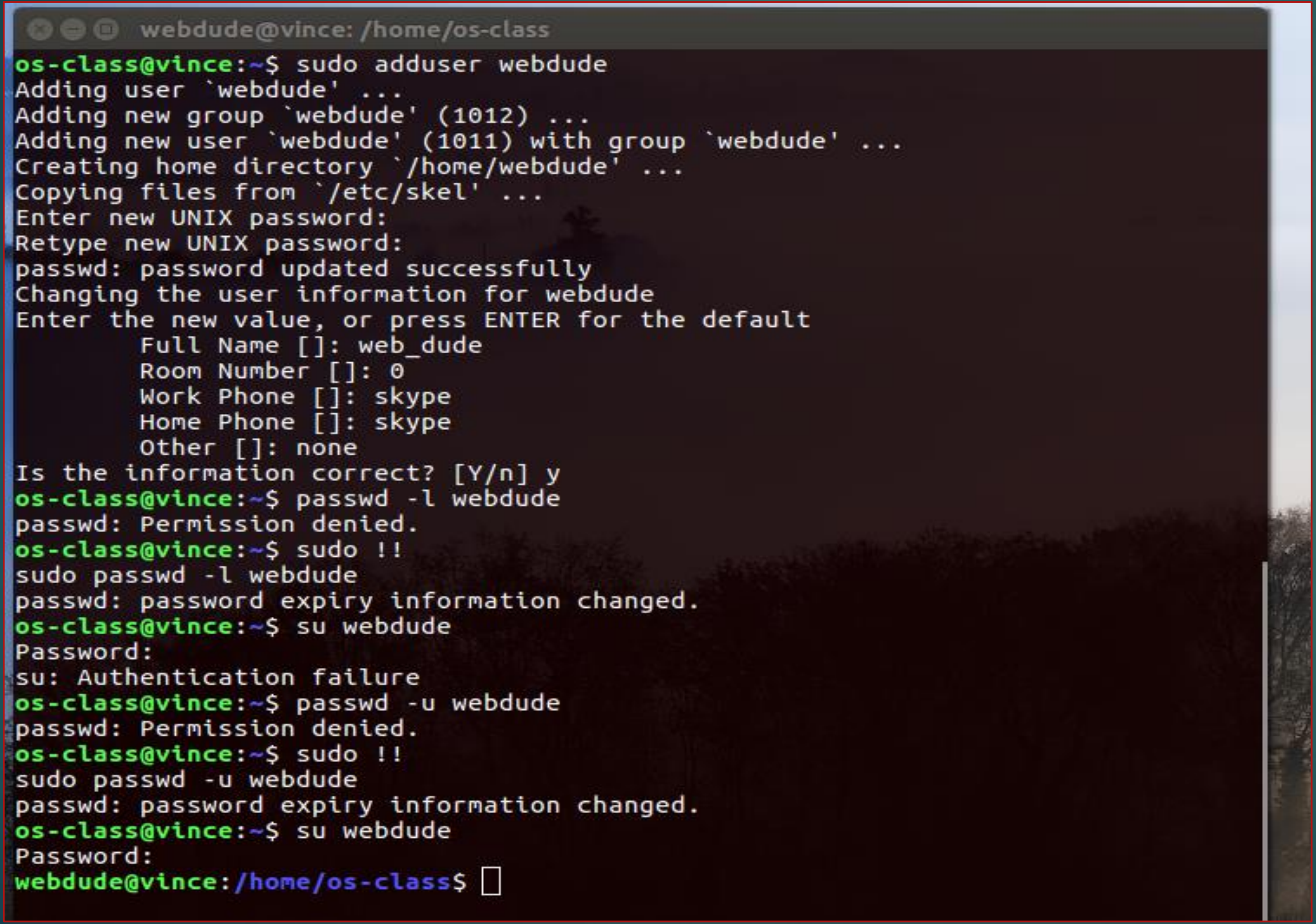
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:103:109::/var/spool/postfix:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
landscape:x:106:113::/var/lib/landscape:/bin/false
eric:x:1000:1000:mixeduperic,,,:/home/eric:/bin/bash
jim:x:1001:1001::/home/jim:/bin/bash
bob:x:1002:1002::/home/bob:/bin/bash
tony:x:1003:1003:Tony Smith,,,:/home/tony:/bin/bash
"/etc/passwd" 29L, 1257C                                    29,1          All
```

What to do with these users?

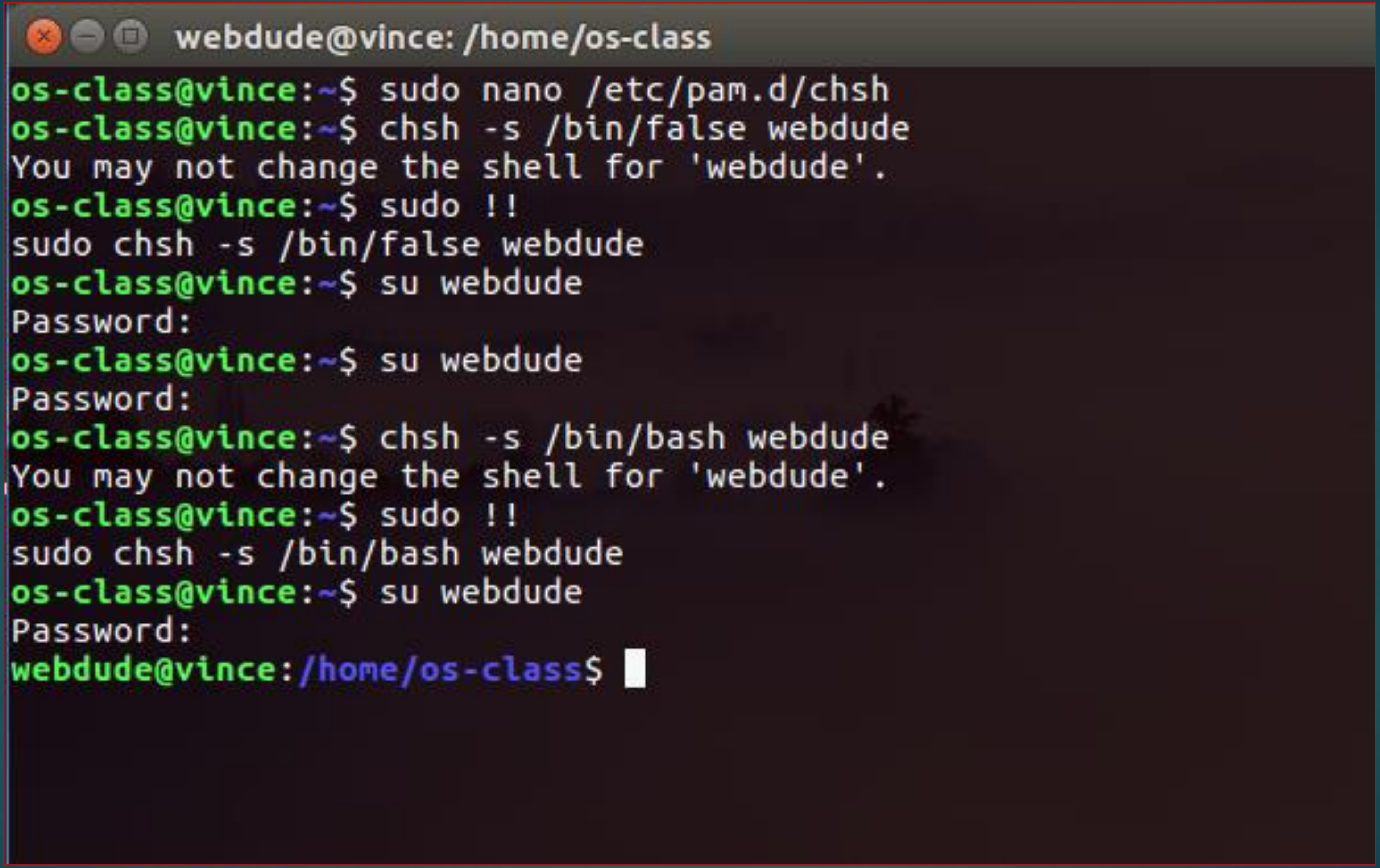
- lock them
  - `passwd –l [USERNAME]`

  or unlock them
  - `passwd –u [USERNAME]`
- disable them
  - `passwd –d [USERNAME]`
- change their shell
  - `chsh –s /bin/false [USERNAME]`

Let’s create the user **webdude**, what happens when we lock that account?



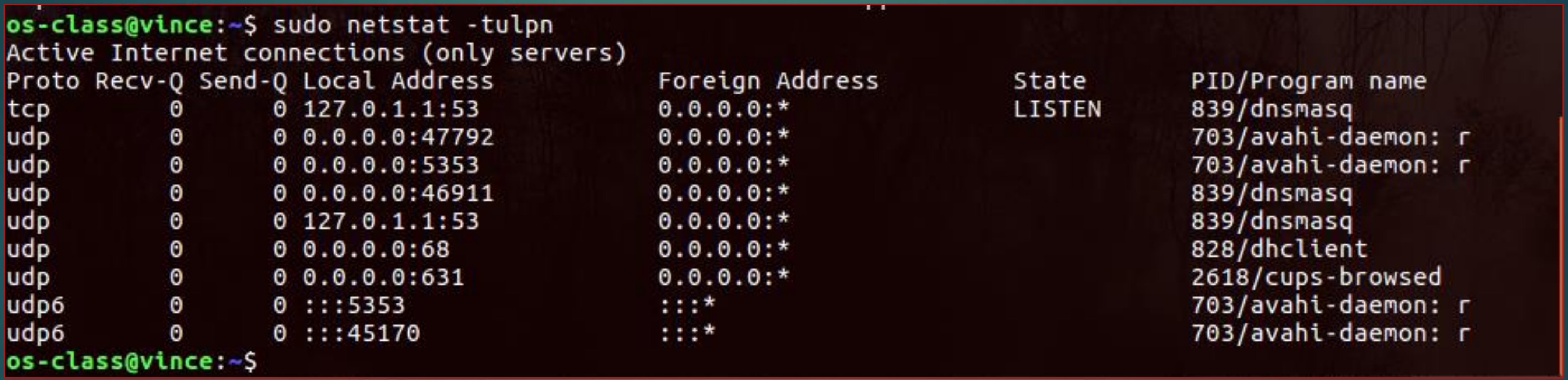
```
os-class@vince:~$ sudo adduser webdude
Adding user `webdude' ...
Adding new group `webdude' (1012) ...
Adding new user `webdude' (1011) with group `webdude' ...
Creating home directory `/home/webdude' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for webdude
Enter the new value, or press ENTER for the default
        Full Name []: web_dude
        Room Number []: 0
        Work Phone []: skype
        Home Phone []: skype
        Other []: none
Is the information correct? [Y/n] y
os-class@vince:~$ passwd -l webdude
passwd: Permission denied.
os-class@vince:~$ sudo !!
sudo passwd -l webdude
passwd: password expiry information changed.
os-class@vince:~$ su webdude
Password:
su: Authentication failure
os-class@vince:~$ passwd -u webdude
passwd: Permission denied.
os-class@vince:~$ sudo !!
sudo passwd -u webdude
passwd: password expiry information changed.
os-class@vince:~$ su webdude
Password:
webdude@vince:/home/os-class$
```



```
os-class@vince:~$ sudo nano /etc/pam.d/chsh
os-class@vince:~$ chsh -s /bin/false webdude
You may not change the shell for 'webdude'.
os-class@vince:~$ sudo !!
sudo chsh -s /bin/false webdude
os-class@vince:~$ su webdude
Password:
os-class@vince:~$ su webdude
Password:
os-class@vince:~$ chsh -s /bin/bash webdude
You may not change the shell for 'webdude'.
os-class@vince:~$ sudo !!
sudo chsh -s /bin/bash webdude
os-class@vince:~$ su webdude
Password:
webdude@vince:/home/os-class$
```

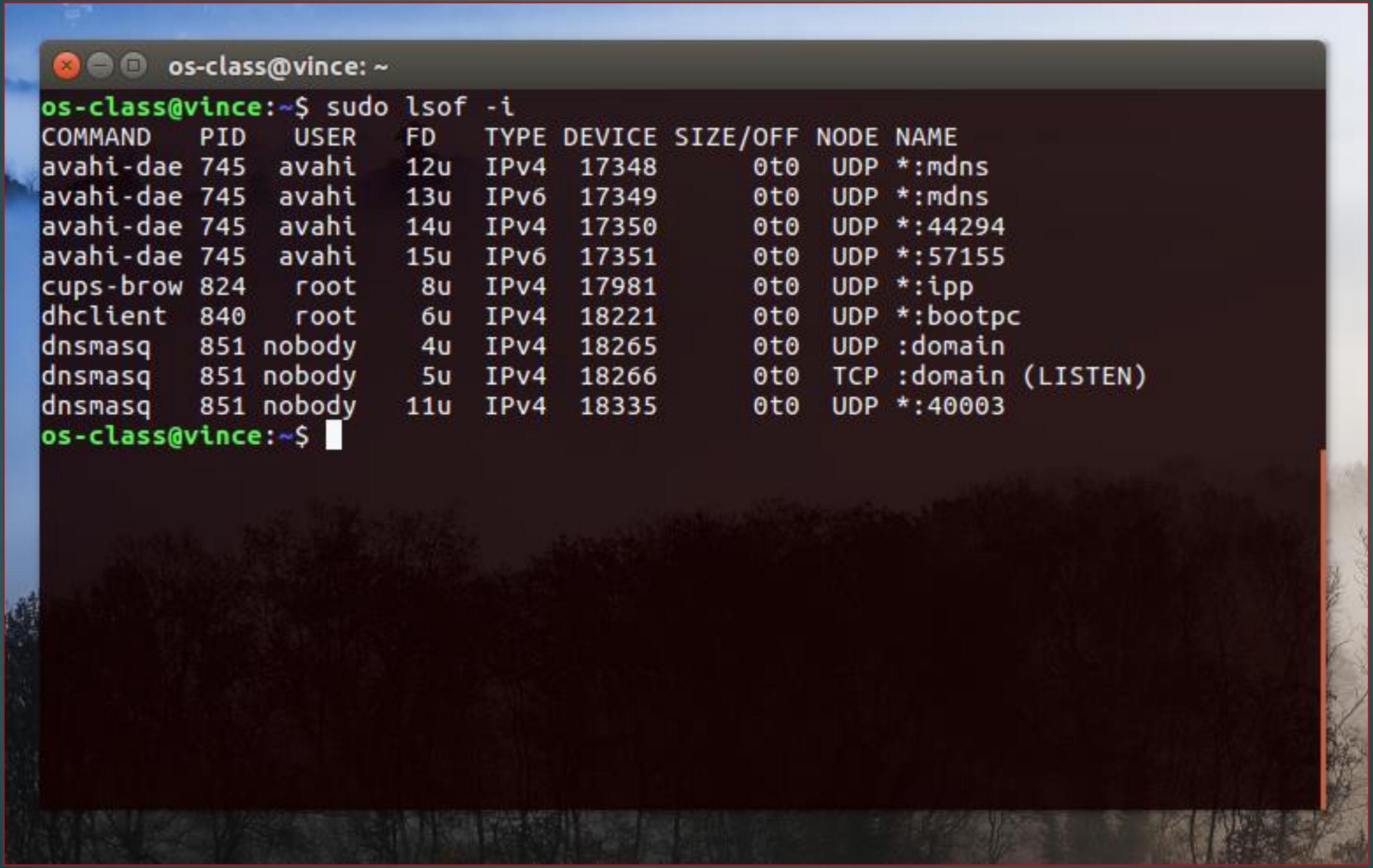
Ports your box is listening on?

sudo netstat -tulpn



```
os-class@vince:~$ sudo netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN      839/dnsmasq
udp        0      0 0.0.0.0:47792           0.0.0.0:*                           703/avahi-daemon: r
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           703/avahi-daemon: r
udp        0      0 0.0.0.0:46911           0.0.0.0:*                           839/dnsmasq
udp        0      0 127.0.1.1:53            0.0.0.0:*                           839/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*                           828/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*                           2618/cups-browsed
udp6       0      0 :::5353                 :::*                                703/avahi-daemon: r
udp6       0      0 :::45170                :::*                                703/avahi-daemon: r
os-class@vince:~$
```

Another Command,
`sudo lsof -i`



```
os-class@vince:~$ sudo lsof -i
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
avahi-dae 745  avahi   12u  IPv4  17348      0t0  UDP *:mdns
avahi-dae 745  avahi   13u  IPv6  17349      0t0  UDP *:mdns
avahi-dae 745  avahi   14u  IPv4  17350      0t0  UDP *:44294
avahi-dae 745  avahi   15u  IPv6  17351      0t0  UDP *:57155
cups-brow 824   root    8u  IPv4  17981      0t0  UDP *:ipp
dhclient  840   root    6u  IPv4  18221      0t0  UDP *:bootpc
dnsmasq   851 nobody    4u  IPv4  18265      0t0  UDP :domain
dnsmasq   851 nobody    5u  IPv4  18266      0t0  TCP :domain (LISTEN)
dnsmasq   851 nobody   11u  IPv4  18335      0t0  UDP *:40003
os-class@vince:~$
```

Don’t forget about **nmap**!

```
80/tcp      open        http
81/tcp      open        hosts2-ns
```

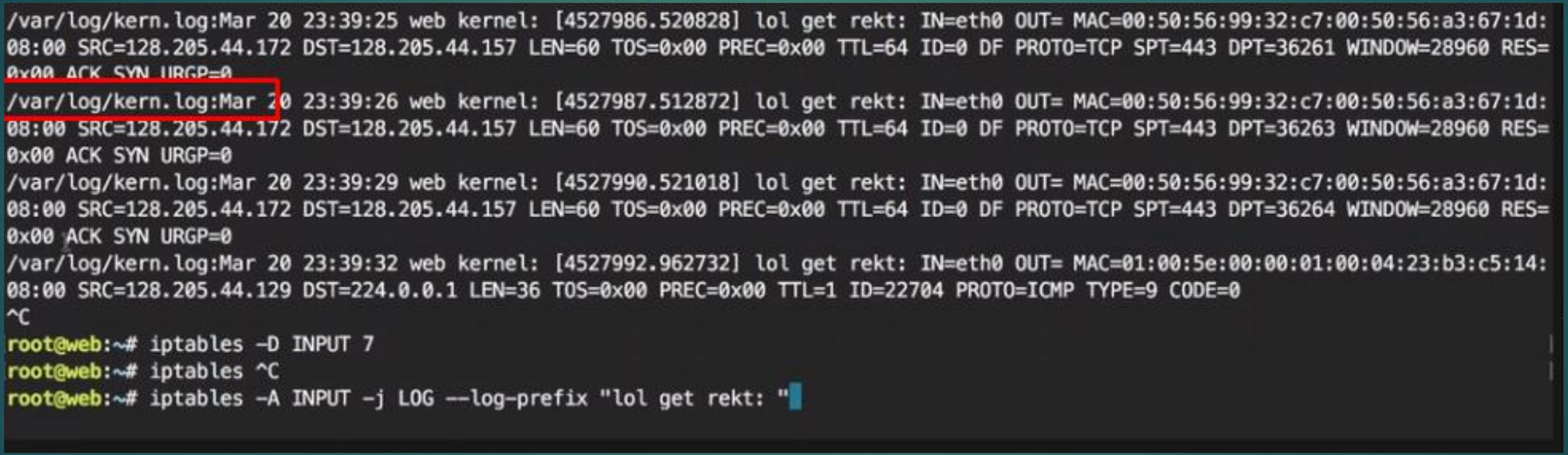
```
$ nmap -v -sS -O 10.2.2.2

Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: c
Port        State        Service
22/tcp      open         ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanned
$ sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
$ ssh 10.2.2.2 -l root
root@10.2.2.2's password: █
```

Logs

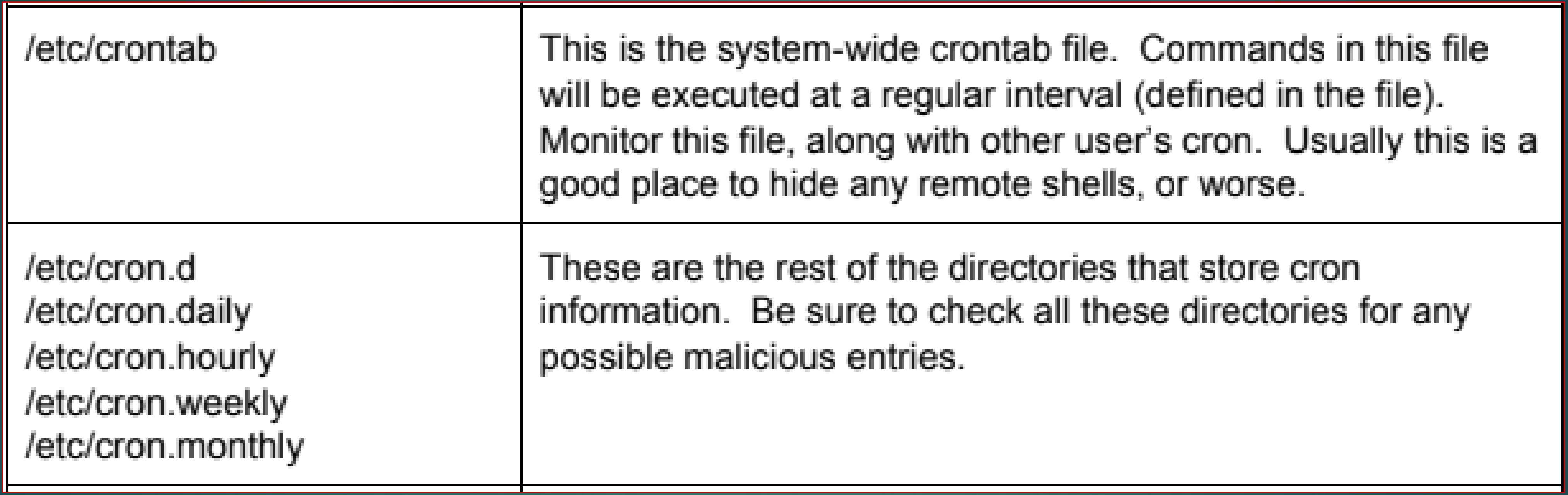
A Bit About Linux on Logs

- Linux logs provide a timeline of events for the Linux OS, applications, and system
- verify useful trouble shooting tool
- logs are stored in plaintext and found in **/var/log**
- the next few slides are important logs on debian based systems

/var/log/kern.log

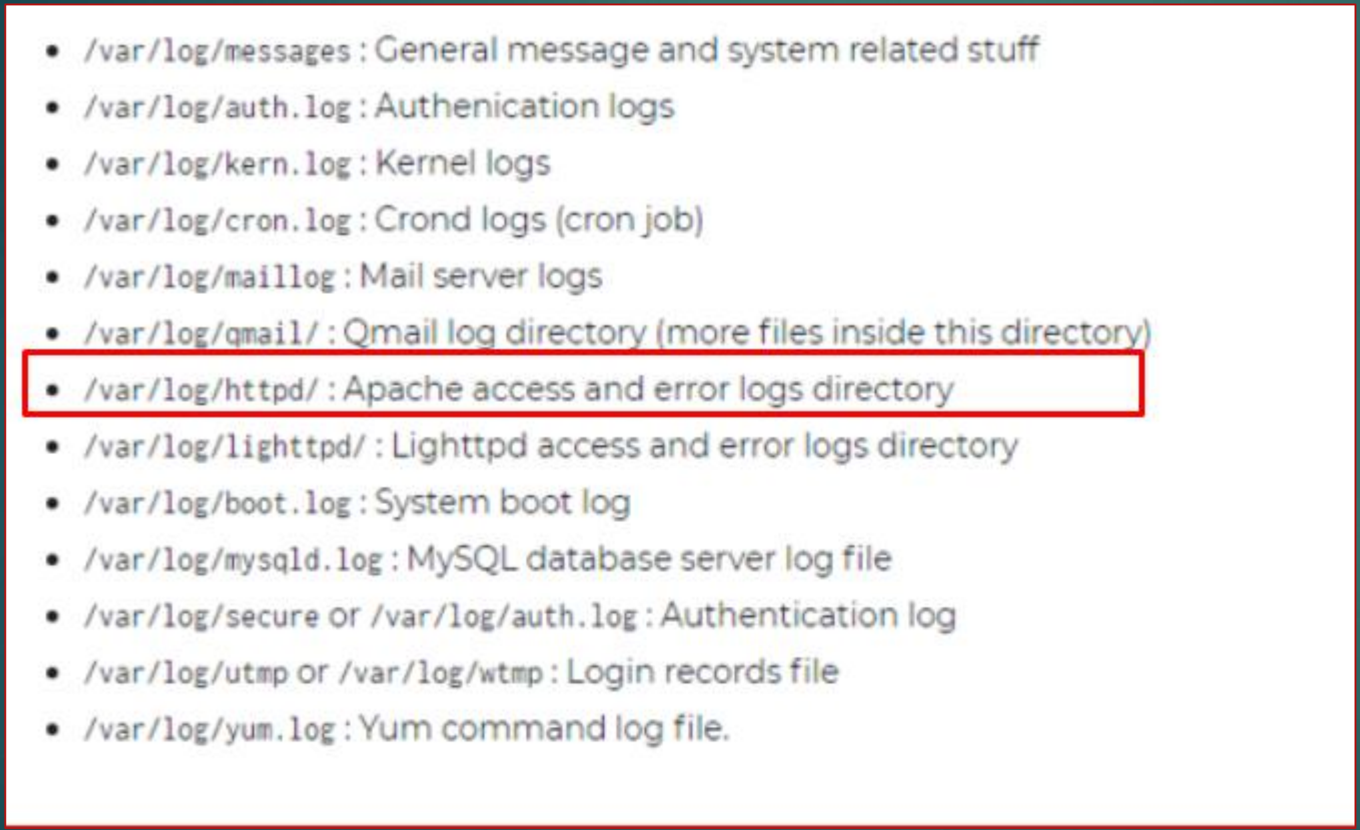


```
/var/log/kern.log:Mar 20 23:39:25 web kernel: [4527986.520828] lol get rekt: IN=eth0 OUT= MAC=00:50:56:99:32:c7:00:50:56:a3:67:1d:
08:00 SRC=128.205.44.172 DST=128.205.44.157 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=443 DPT=36261 WINDOW=28960 RES=
0x00 ACK SYN URGP=0
/var/log/kern.log:Mar 20 23:39:26 web kernel: [4527987.512872] lol get rekt: IN=eth0 OUT= MAC=00:50:56:99:32:c7:00:50:56:a3:67:1d:
08:00 SRC=128.205.44.172 DST=128.205.44.157 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=443 DPT=36263 WINDOW=28960 RES=
0x00 ACK SYN URGP=0
/var/log/kern.log:Mar 20 23:39:29 web kernel: [4527990.521018] lol get rekt: IN=eth0 OUT= MAC=00:50:56:99:32:c7:00:50:56:a3:67:1d:
08:00 SRC=128.205.44.172 DST=128.205.44.157 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=TCP SPT=443 DPT=36264 WINDOW=28960 RES=
0x00 ACK SYN URGP=0
/var/log/kern.log:Mar 20 23:39:32 web kernel: [4527992.962732] lol get rekt: IN=eth0 OUT= MAC=01:00:5e:00:00:01:00:04:23:b3:c5:14:
08:00 SRC=128.205.44.129 DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=22704 PROTO=ICMP TYPE=9 CODE=0
^C
root@web:~# iptables -D INPUT 7
root@web:~# iptables ^C
root@web:~# iptables -A INPUT -j LOG --log-prefix "lol get rekt: "
```



/etc/crontab	This is the system-wide crontab file. Commands in this file will be executed at a regular interval (defined in the file). Monitor this file, along with other user's cron. Usually this is a good place to hide any remote shells, or worse.
/etc/cron.d /etc/cron.daily /etc/cron.hourly /etc/cron.weekly /etc/cron.monthly	These are the rest of the directories that store cron information. Be sure to check all these directories for any possible malicious entries.

There are tons of log’s for services too. Sometimes a service will generate it’s own log file, such as apache.



- `/var/log/messages` : General message and system related stuff
- `/var/log/auth.log` : Authenication logs
- `/var/log/kern.log` : Kernel logs
- `/var/log/cron.log` : Crond logs (cron job)
- `/var/log/maillog` : Mail server logs
- `/var/log/qmail/` : Qmail log directory (more files inside this directory)
- `/var/log/httpd/` : Apache access and error logs directory
- `/var/log/lighttpd/` : Lighttpd access and error logs directory
- `/var/log/boot.log` : System boot log
- `/var/log/mysqld.log` : MySQL database server log file
- `/var/log/secure` or `/var/log/auth.log` : Authentication log
- `/var/log/utmp` or `/var/log/wtmp` : Login records file
- `/var/log/yum.log` : Yum command log file.

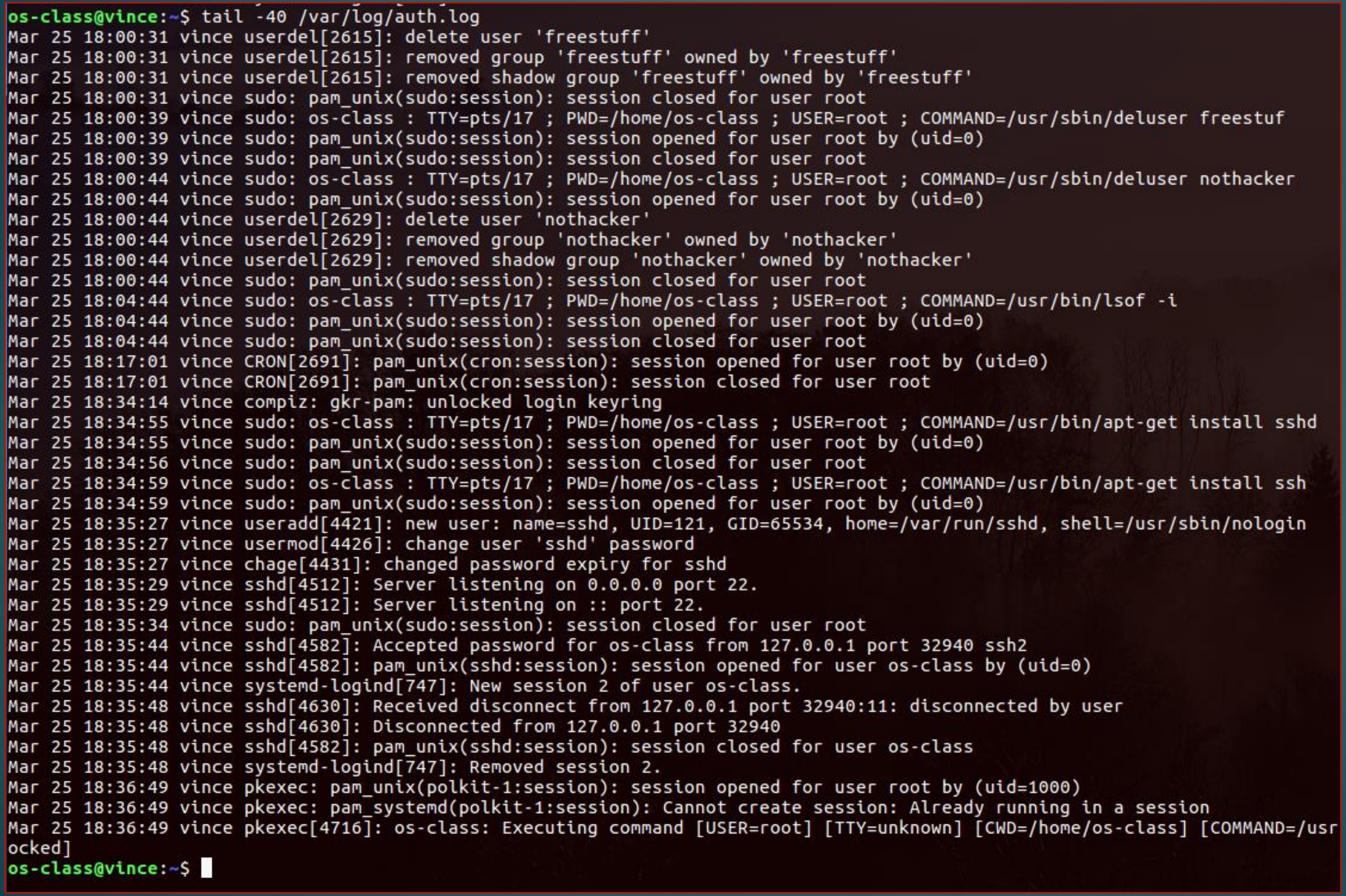
auth.log

- this log contains all successful authentication attempts and failed!

What can or should you look for?

- multiple failed login attempts from a single outside IP
- login attempts for system users, (cron) or any unknown user
- any know login attempts to **root** that were not you!

tail -40 /var/log/auth.log



```
os-class@vince:~$ tail -40 /var/log/auth.log
Mar 25 18:00:31 vince userdel[2615]: delete user 'freestuff'
Mar 25 18:00:31 vince userdel[2615]: removed group 'freestuff' owned by 'freestuff'
Mar 25 18:00:31 vince userdel[2615]: removed shadow group 'freestuff' owned by 'freestuff'
Mar 25 18:00:31 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:00:39 vince sudo: os-class : TTY=pts/17 ; PWD=/home/os-class ; USER=root ; COMMAND=/usr/sbin/deluser freestuf
Mar 25 18:00:39 vince sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 18:00:39 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:00:44 vince sudo: os-class : TTY=pts/17 ; PWD=/home/os-class ; USER=root ; COMMAND=/usr/sbin/deluser nothacker
Mar 25 18:00:44 vince sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 18:00:44 vince userdel[2629]: delete user 'nothacker'
Mar 25 18:00:44 vince userdel[2629]: removed group 'nothacker' owned by 'nothacker'
Mar 25 18:00:44 vince userdel[2629]: removed shadow group 'nothacker' owned by 'nothacker'
Mar 25 18:00:44 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:04:44 vince sudo: os-class : TTY=pts/17 ; PWD=/home/os-class ; USER=root ; COMMAND=/usr/bin/lsof -i
Mar 25 18:04:44 vince sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 18:04:44 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:17:01 vince CRON[2691]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 25 18:17:01 vince CRON[2691]: pam_unix(cron:session): session closed for user root
Mar 25 18:34:14 vince compiz: gkr-pam: unlocked login keyring
Mar 25 18:34:55 vince sudo: os-class : TTY=pts/17 ; PWD=/home/os-class ; USER=root ; COMMAND=/usr/bin/apt-get install sshd
Mar 25 18:34:55 vince sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 18:34:56 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:34:59 vince sudo: os-class : TTY=pts/17 ; PWD=/home/os-class ; USER=root ; COMMAND=/usr/bin/apt-get install ssh
Mar 25 18:34:59 vince sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Mar 25 18:35:27 vince useradd[4421]: new user: name=sshd, UID=121, GID=65534, home=/var/run/sshd, shell=/usr/sbin/nologin
Mar 25 18:35:27 vince usermod[4426]: change user 'sshd' password
Mar 25 18:35:27 vince chage[4431]: changed password expiry for sshd
Mar 25 18:35:29 vince sshd[4512]: Server listening on 0.0.0.0 port 22.
Mar 25 18:35:29 vince sshd[4512]: Server listening on :: port 22.
Mar 25 18:35:34 vince sudo: pam_unix(sudo:session): session closed for user root
Mar 25 18:35:44 vince sshd[4582]: Accepted password for os-class from 127.0.0.1 port 32940 ssh2
Mar 25 18:35:44 vince sshd[4582]: pam_unix(sshd:session): session opened for user os-class by (uid=0)
Mar 25 18:35:44 vince systemd-logind[747]: New session 2 of user os-class.
Mar 25 18:35:48 vince sshd[4630]: Received disconnect from 127.0.0.1 port 32940:11: disconnected by user
Mar 25 18:35:48 vince sshd[4630]: Disconnected from 127.0.0.1 port 32940
Mar 25 18:35:48 vince sshd[4582]: pam_unix(sshd:session): session closed for user os-class
Mar 25 18:35:48 vince systemd-logind[747]: Removed session 2.
Mar 25 18:36:49 vince pkexec: pam_unix(polkit-1:session): session opened for user root by (uid=1000)
Mar 25 18:36:49 vince pkexec: pam_systemd(polkit-1:session): Cannot create session: Already running in a session
Mar 25 18:36:49 vince pkexec[4716]: os-class: Executing command [USER=root] [TTY=unknown] [CWD=/home/os-class] [COMMAND=/usr
ocked]
os-class@vince:~$
```

Bringing it all together, this is what it is like in the wild…

- https://www.youtube.com/watch?v=W8_Kfjo3VjU

- Was there anything wrong with the web server?
- What command did “web dude” use to reboot the webserver?
- How did “web dude” access Chip’s computer?
- Anything else you noticed?

STUFF I DIDN’T COVER

- crontabs
- firewall appliances (UFW, IPTABLES)
- central logging (Graylog!)
- host based IDS (OSSEC)
- IDS in general (Snort)
- **chmod** and **lsattr** commands
- ssh keys and securing ssh
- /etc/shadow
- /etc/pam.d
- lot’s of Windows stuff):