# The Wonderful World of Services

VINCE

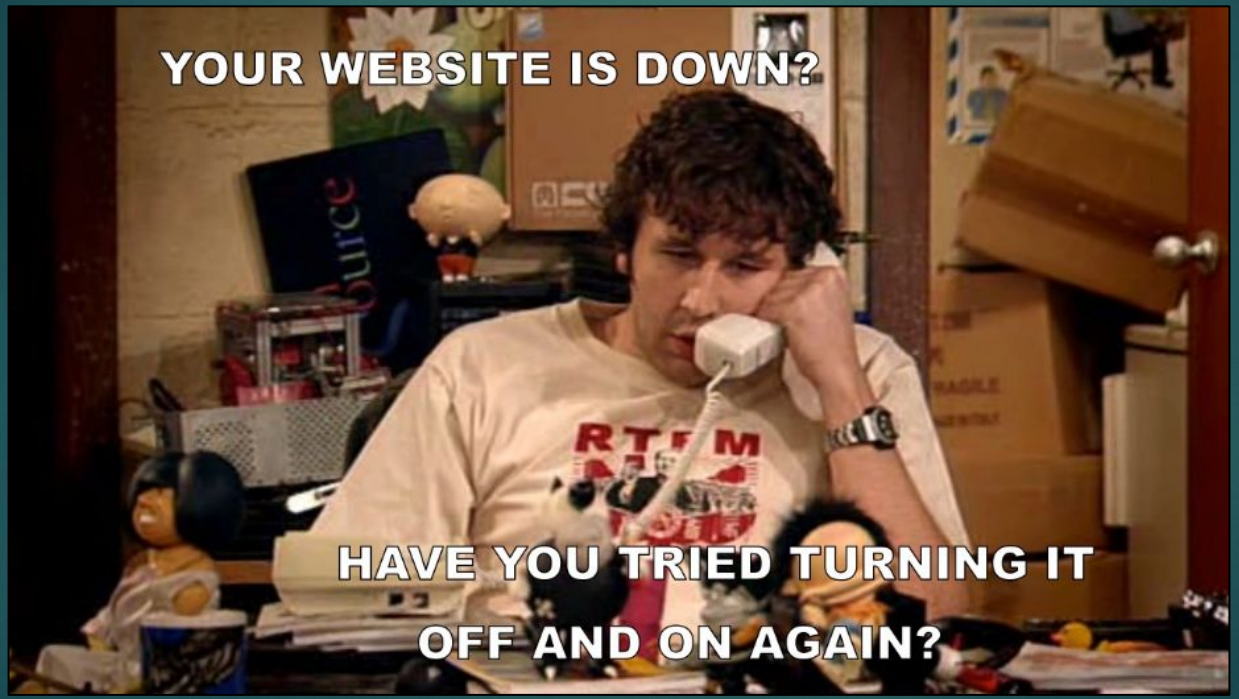
# AGENDA

- definitions
- services for Windows and Linux
- breaks?
- auditing Linux + I guess… Windows
- useful tools

# GOALS

- develop a better understanding of Linux and Windows
- services
- minor networking
- useful commands
- pick up some useful tools!

# SERVICES


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

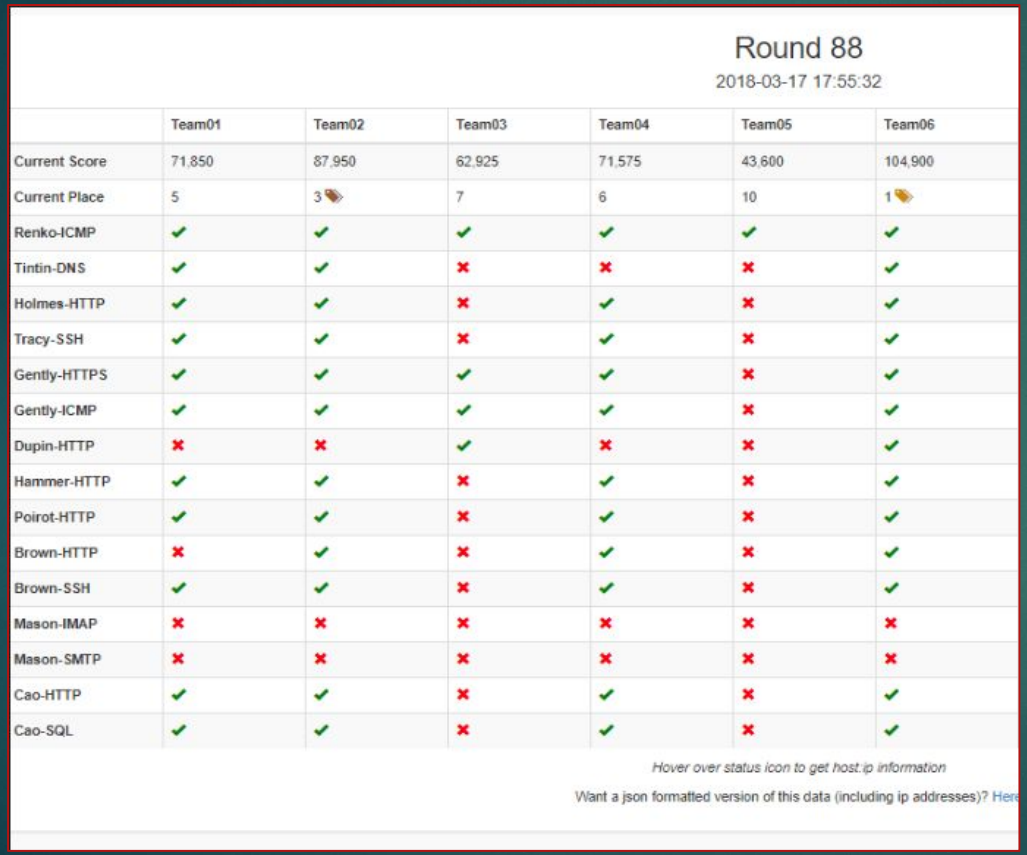
# What is a service?

- an application (or set of applications) that runs in the background (usually)
- 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

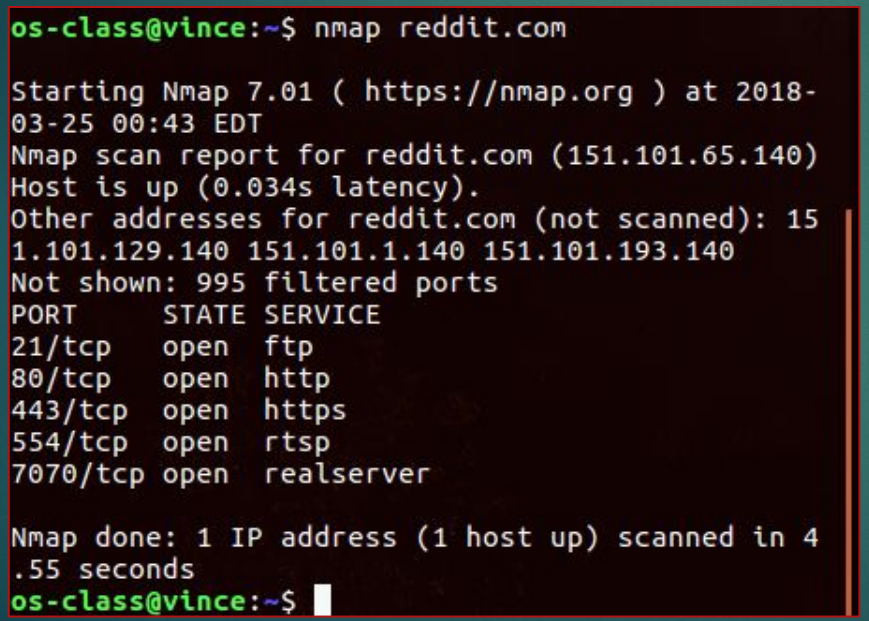
**Internet Applications**

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 |

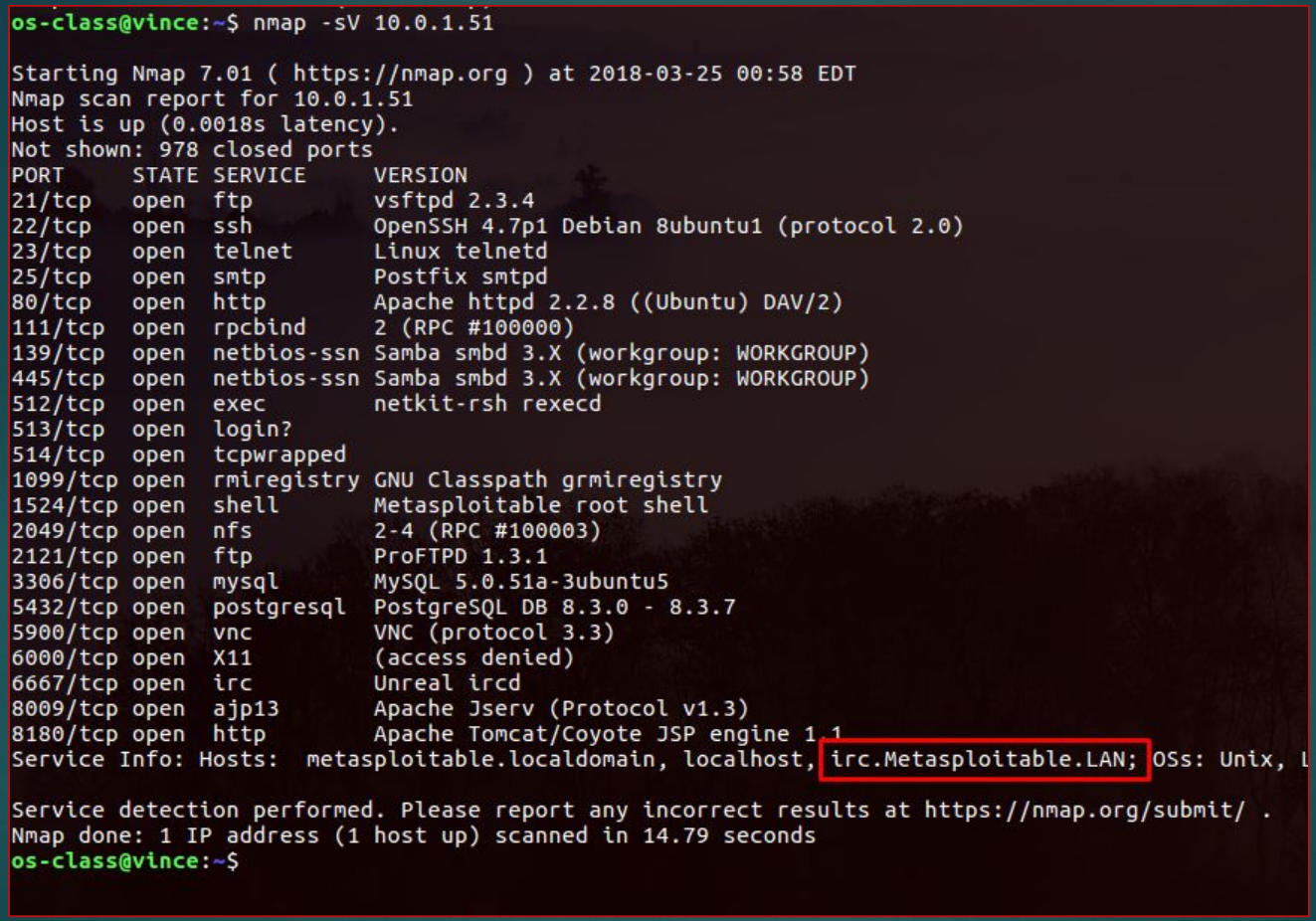
# We can use **nmap** to check ports and services!

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



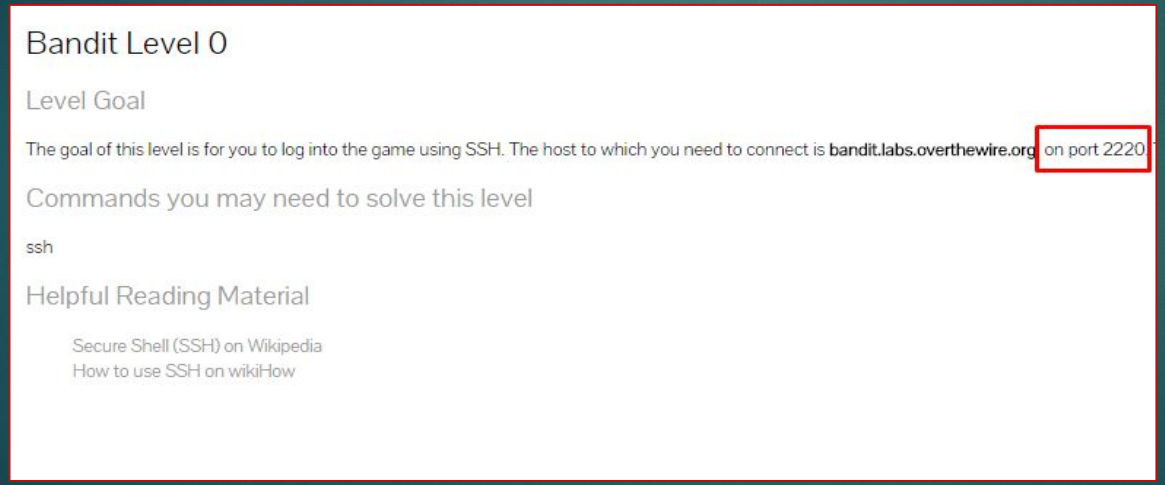
| Switch | Example | Description |
| --- | --- | --- |
| -sV | nmap 192.168.1.1 -sV | Attempts to determine the version of the service running on port |

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


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,
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:~$

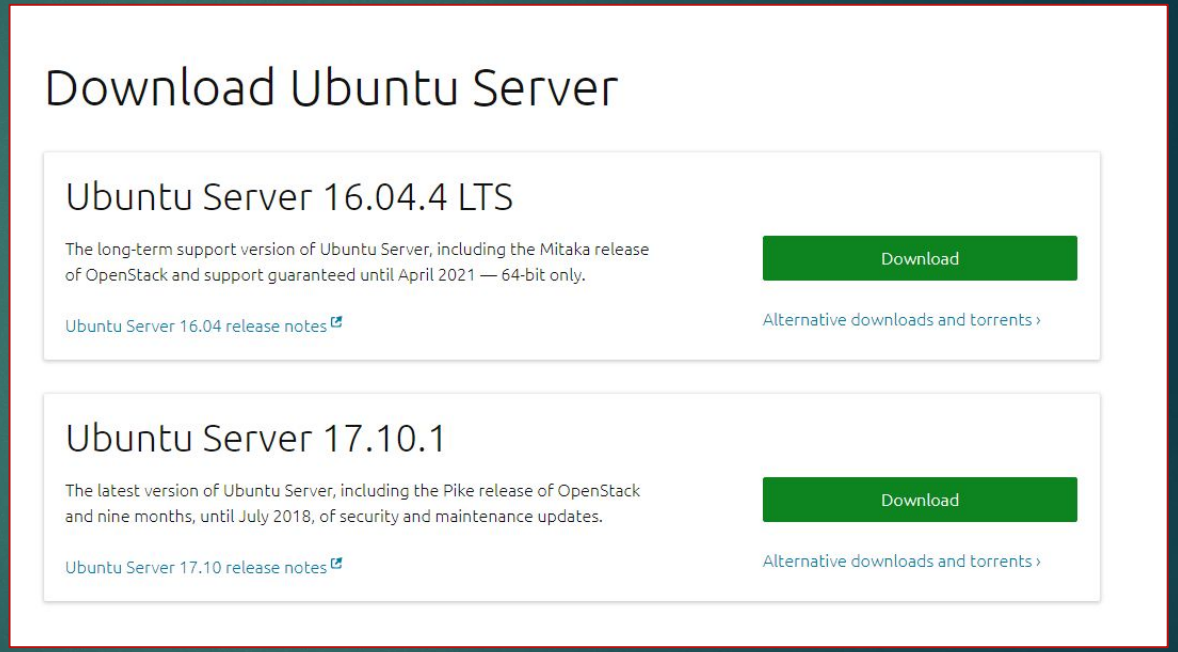
# Why do we need to know ports?

- 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



# 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?



# What service(s) are on my box?

| | |
|---|---|
| Managing Services | Ubuntu Version >= 15.04<br>`systemctl {start\|stop\|...} {service_name}.service`<br><br>Ubuntu Version < 15.04<br>`service {service_name} {start\|stop\|....}` |

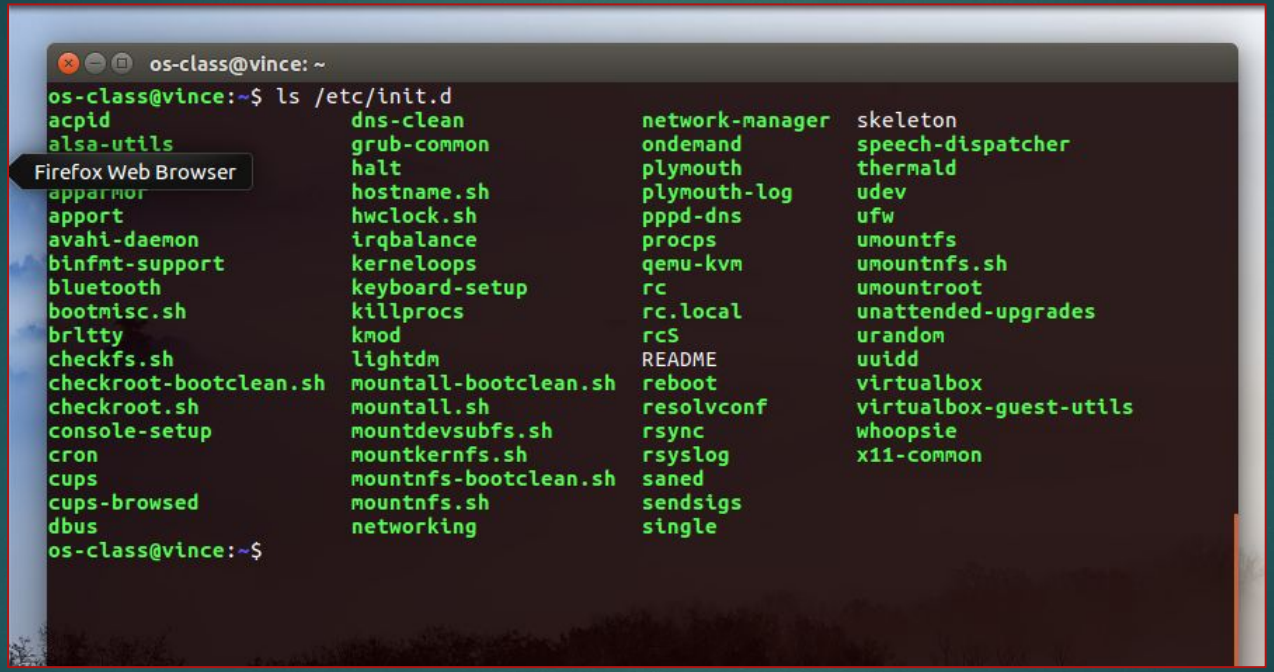
Older Architectures(S)

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

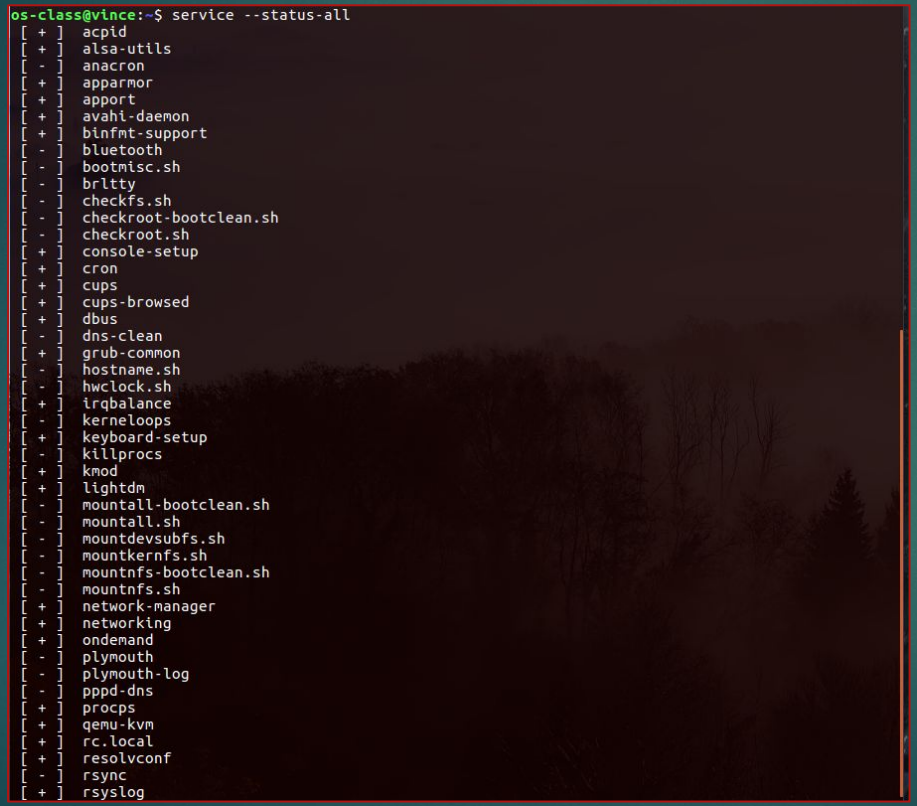
Newer Architectures(S)

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

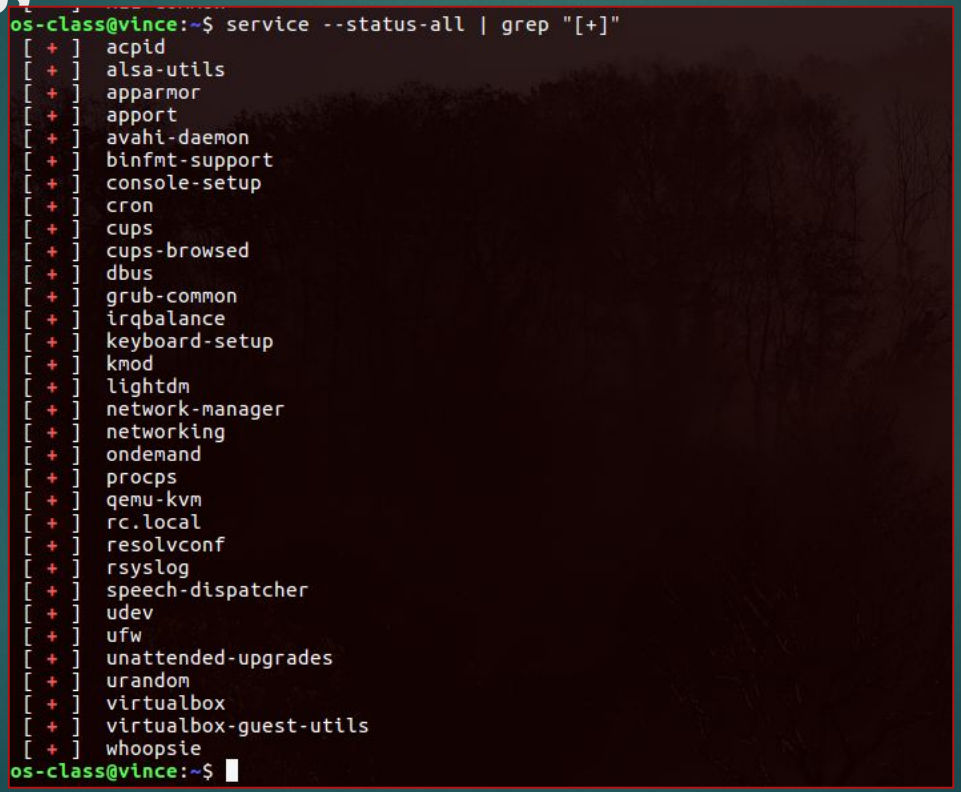
# ls /etc/init.d


os-class@vince: ~
os-class@vince:~$ ls /etc/init.d
acpid
alsa-utils
Firefox Web Browser
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
halt
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
networking
network-manager
ondemand
plymouth
plymouth-log
pppd-dns
procps
qemu-kvm
rc
rc.local
rcS
README
reboot
resolvconf
rsync
rsyslog
saned
sendsigs
single
skeleton
speech-dispatcher
thermald
udev
ufw
umountfs
umountnfs.sh
umountroot
unattended-upgrades
urandom
uuidd
virtualbox
virtualbox-guest-utils
whoopsie
x11-common
os-class@vince:~$

# service --status-all



# service --status-all | grep “[+]”

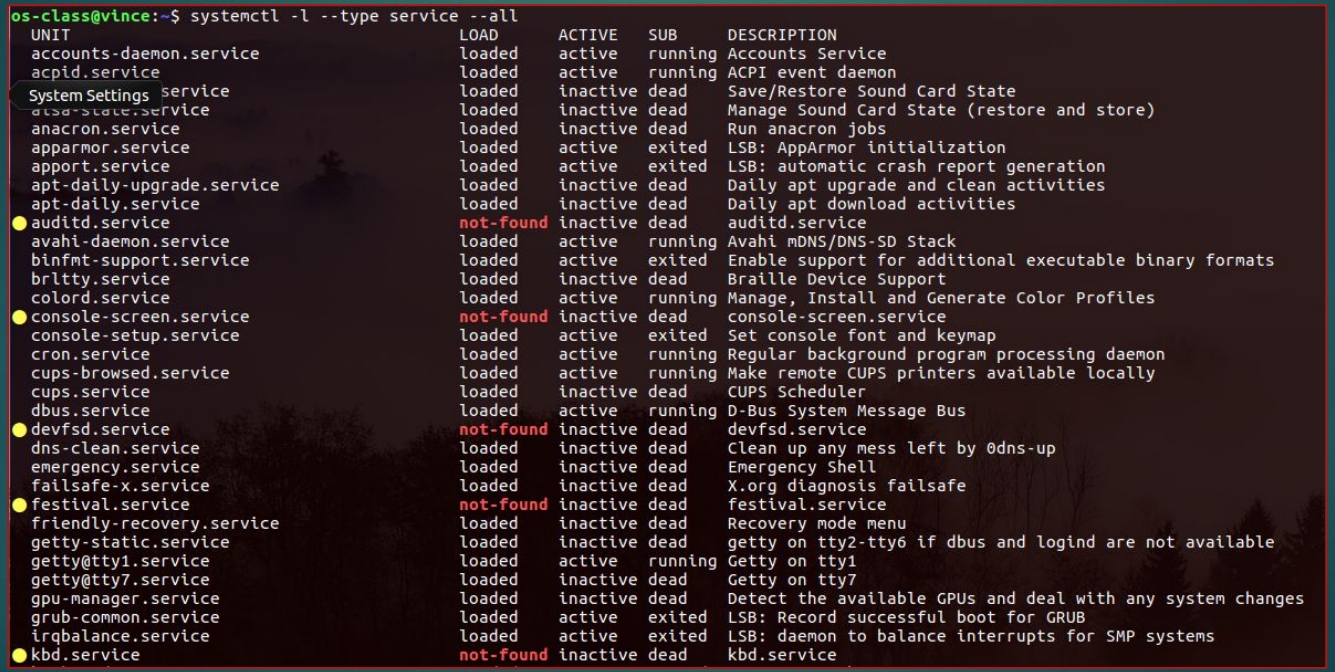


# What about what is not running?

**`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
  System Settings 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 commandS 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
```

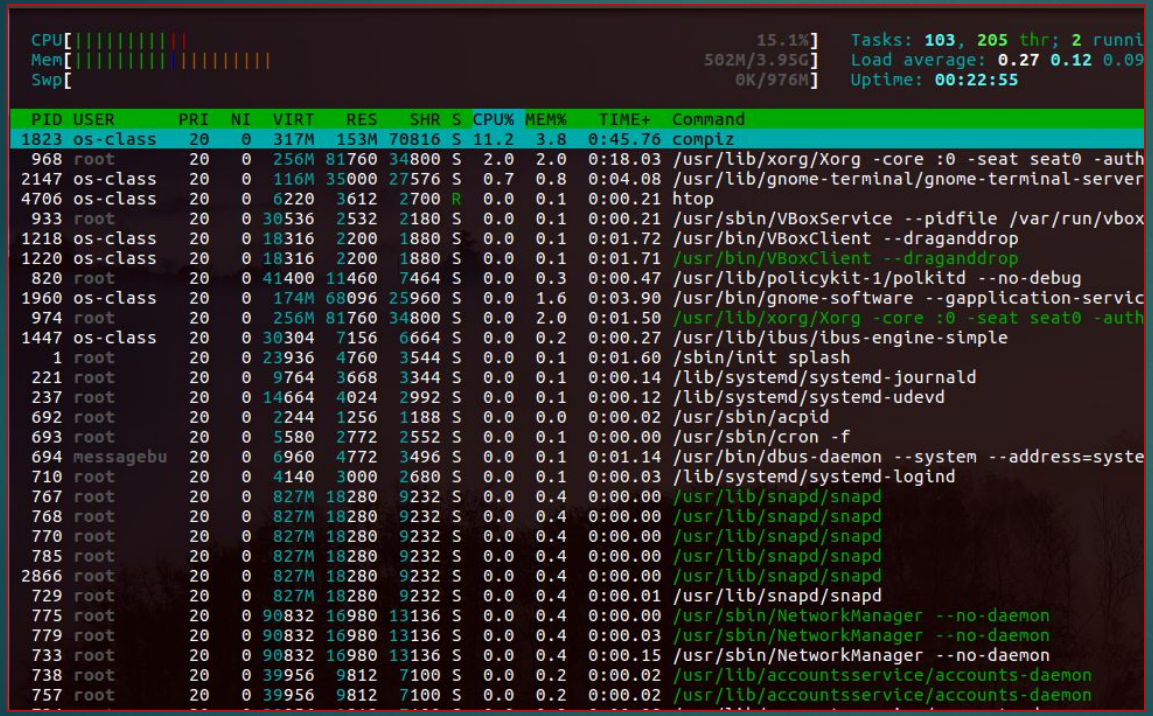

NECCDC 2018

SOURCE:
https://www.youtube.com/watch?v=X8nVTRyRRg8

# 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

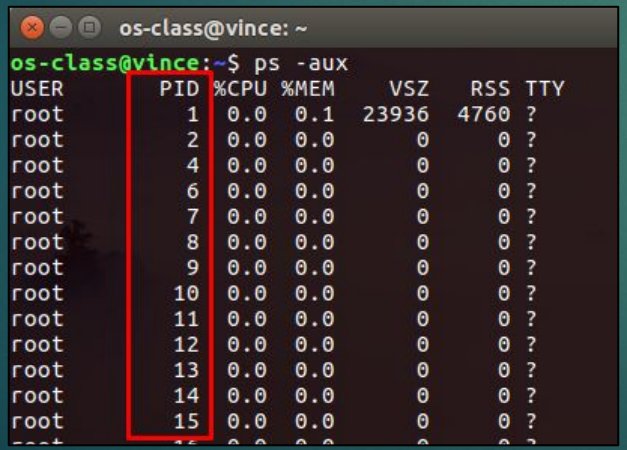



- htop is not always there
- **sudo apt-get install htop**

# 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!*



# 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

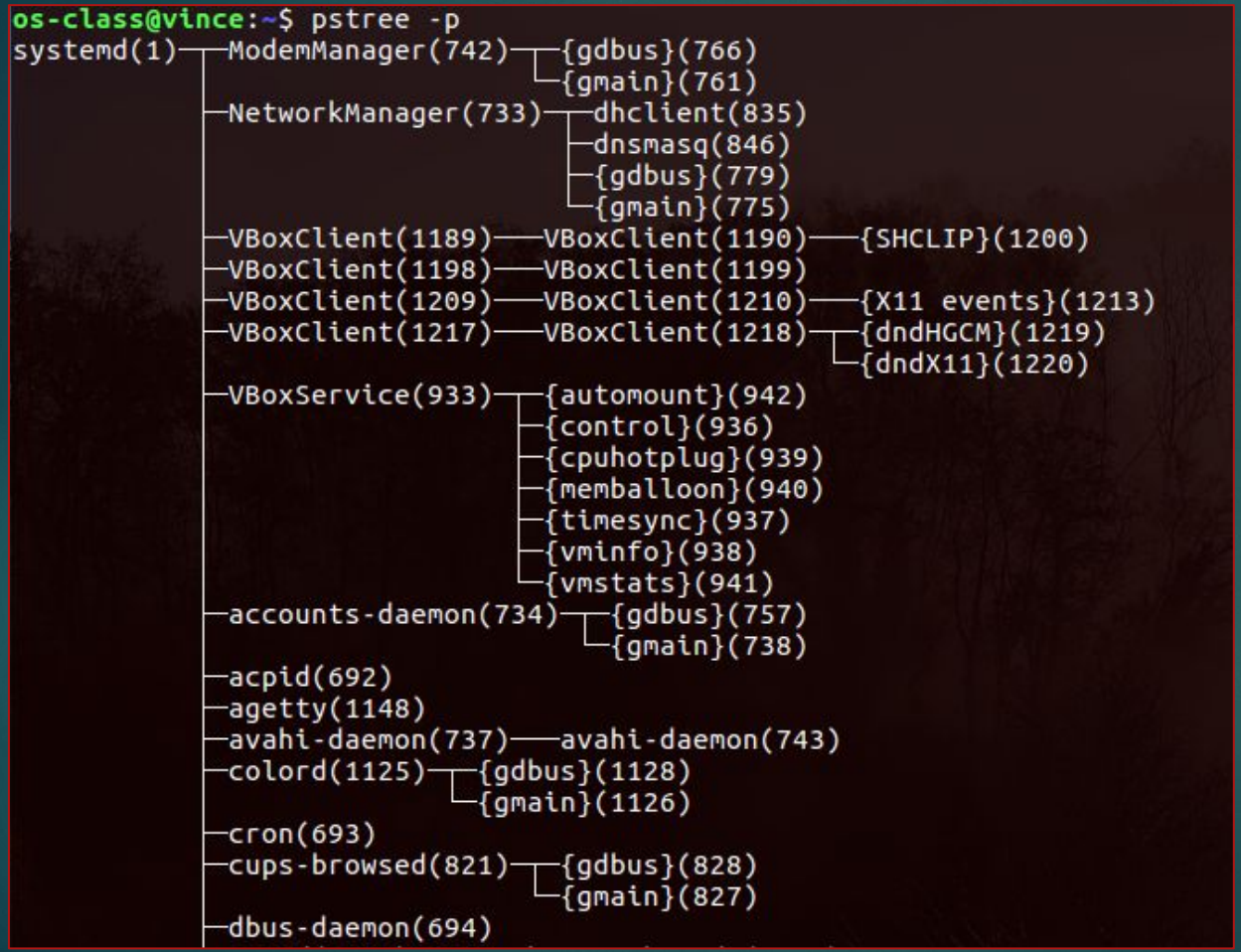
```
os-class@vince:~$ kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     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

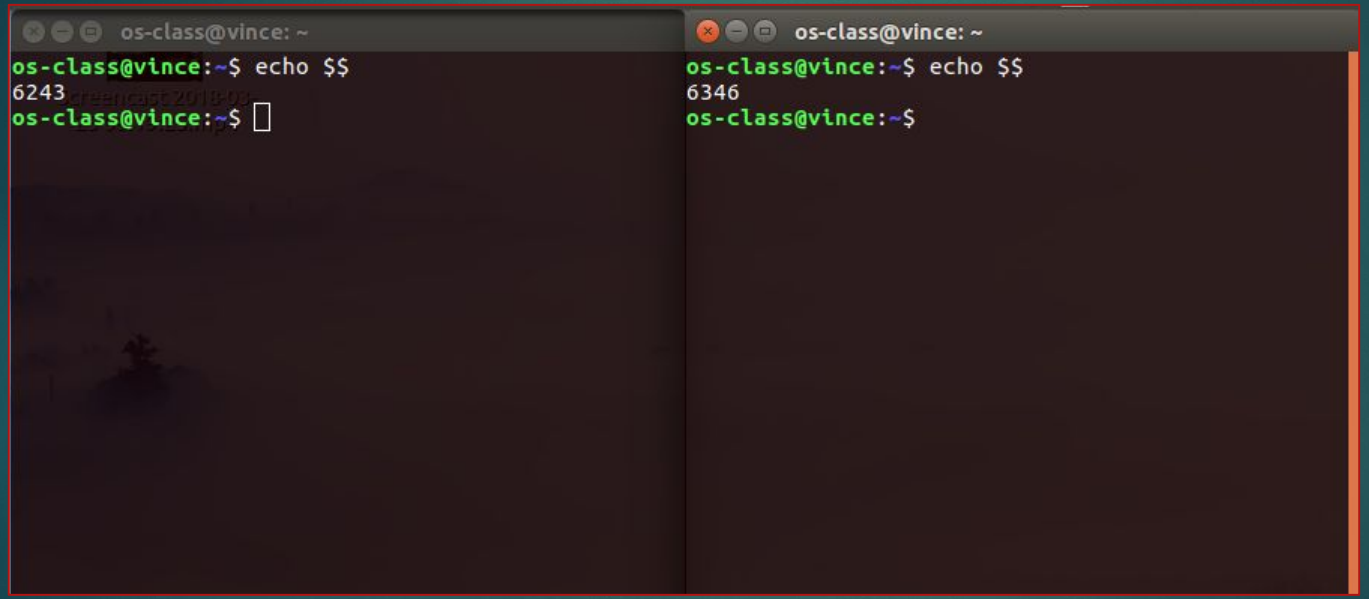
**SOURCE:**
http://www.linfo.org/kill.html

# 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)

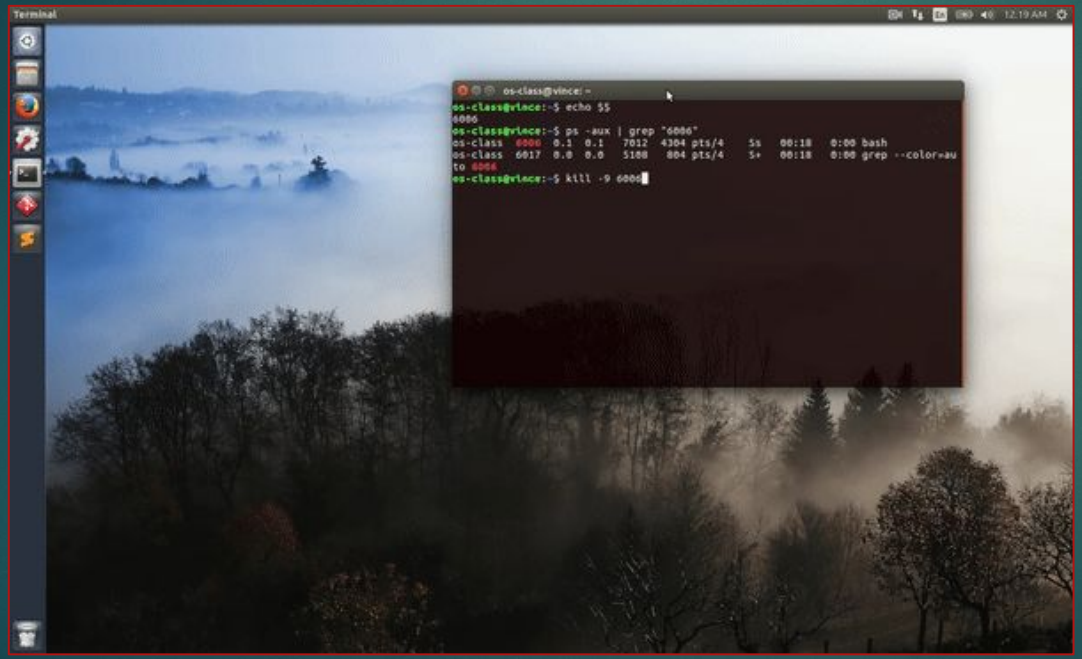
# Ross likes to kill bash sessions…



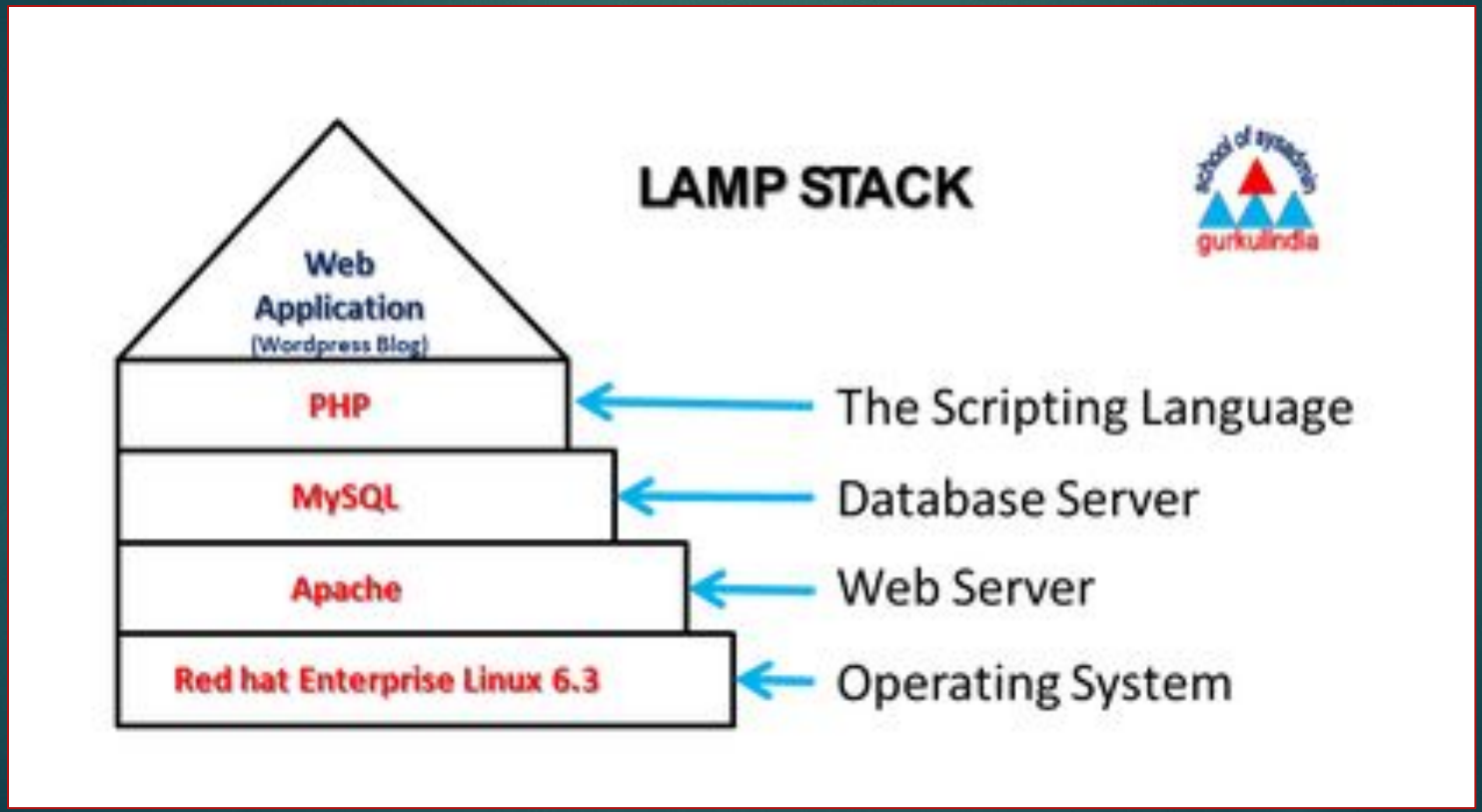
# echo $$

```
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`?

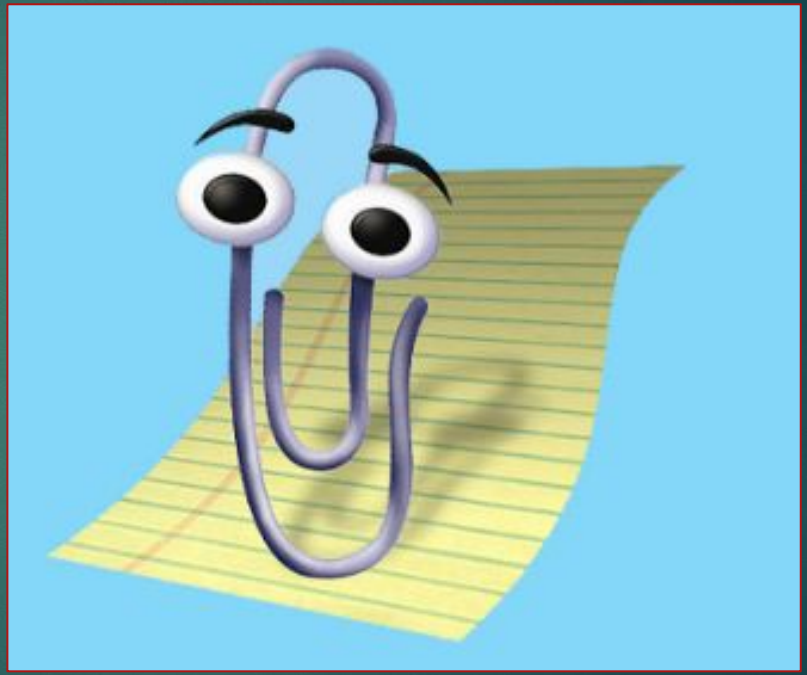


# LAMP Stack

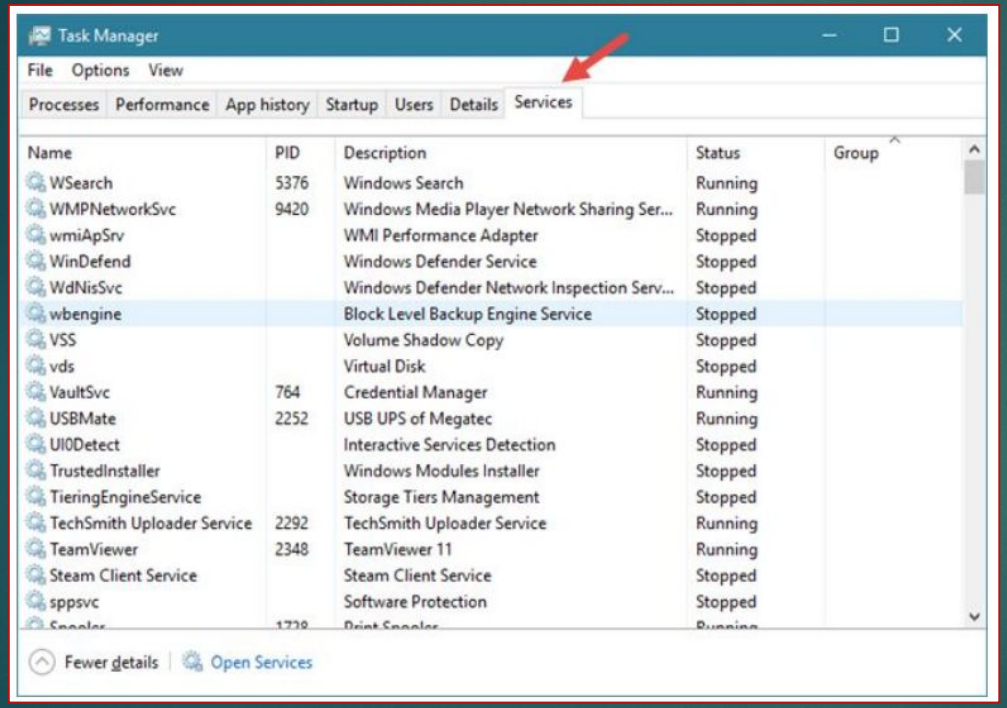

LAMP STACK
Web Application
(Wordpress Blog)
PHP
MySQL
Apache
Red hat Enterprise Linux 6.3
The Scripting Language
Database Server
Web Server
Operating System


INTERMISSION
1
10
9
2
8
3
7
4
6
5
VISIT OUR SNACK BAR
DRIVE-IN

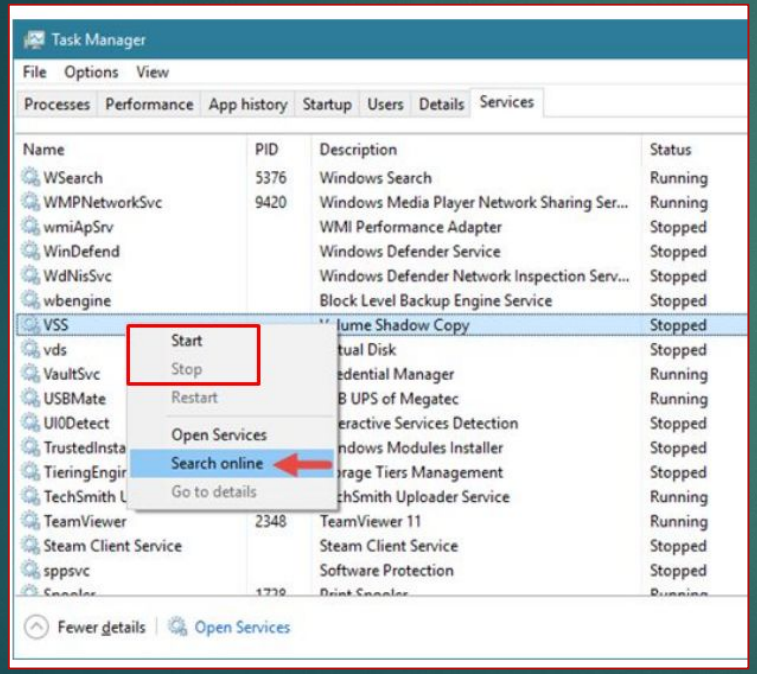
# WINDOWS LAND!



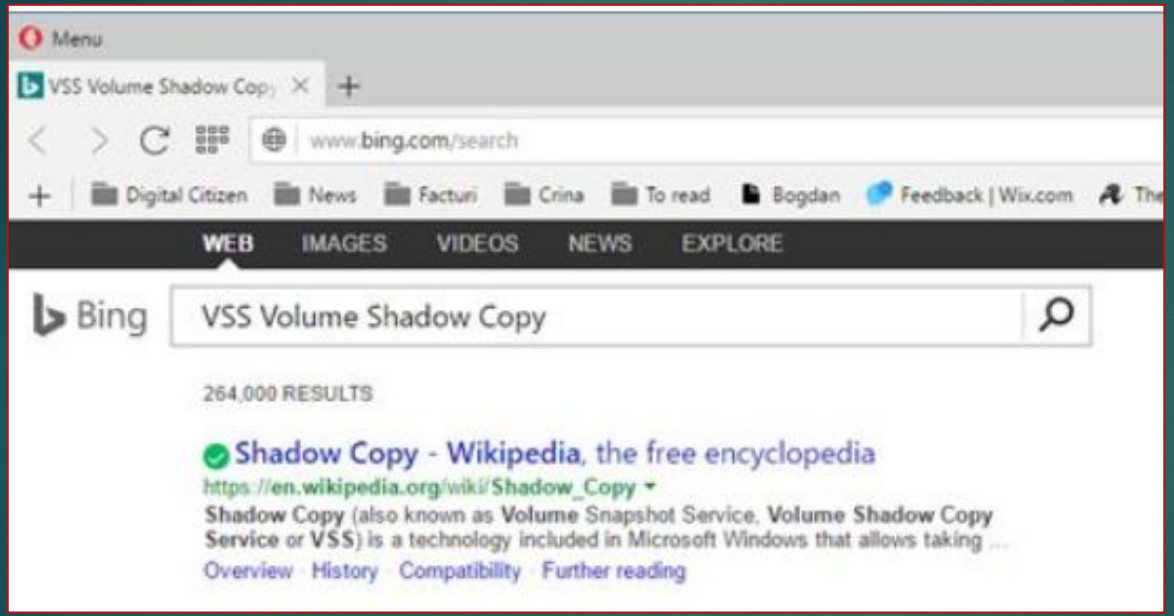
# Task Manager



# Right click on a service to start **or** stop it.

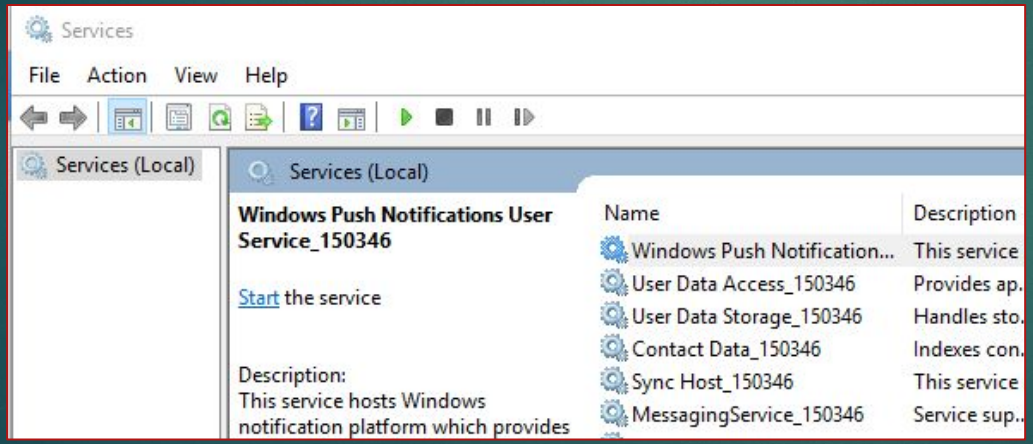


# You can search online too!

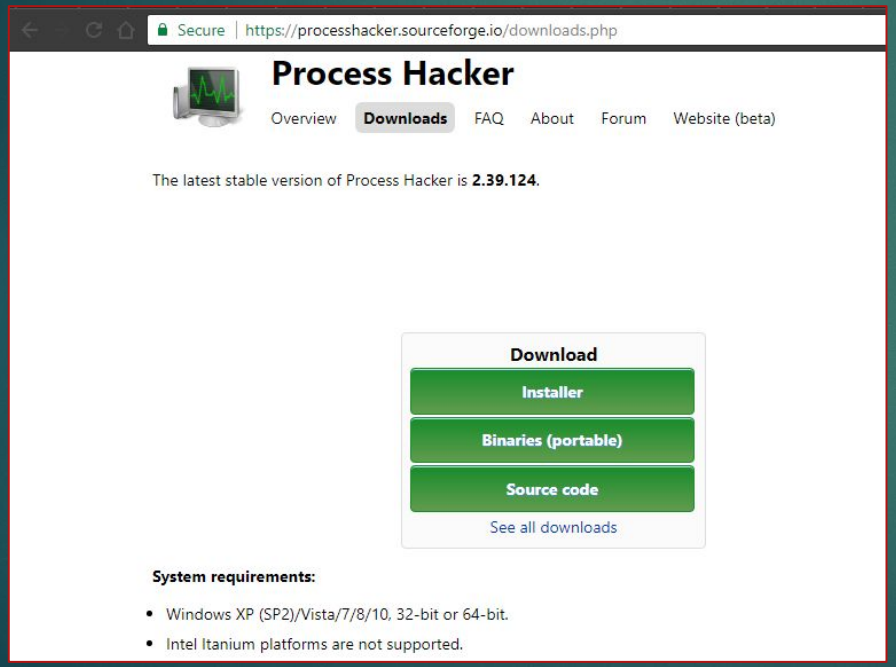


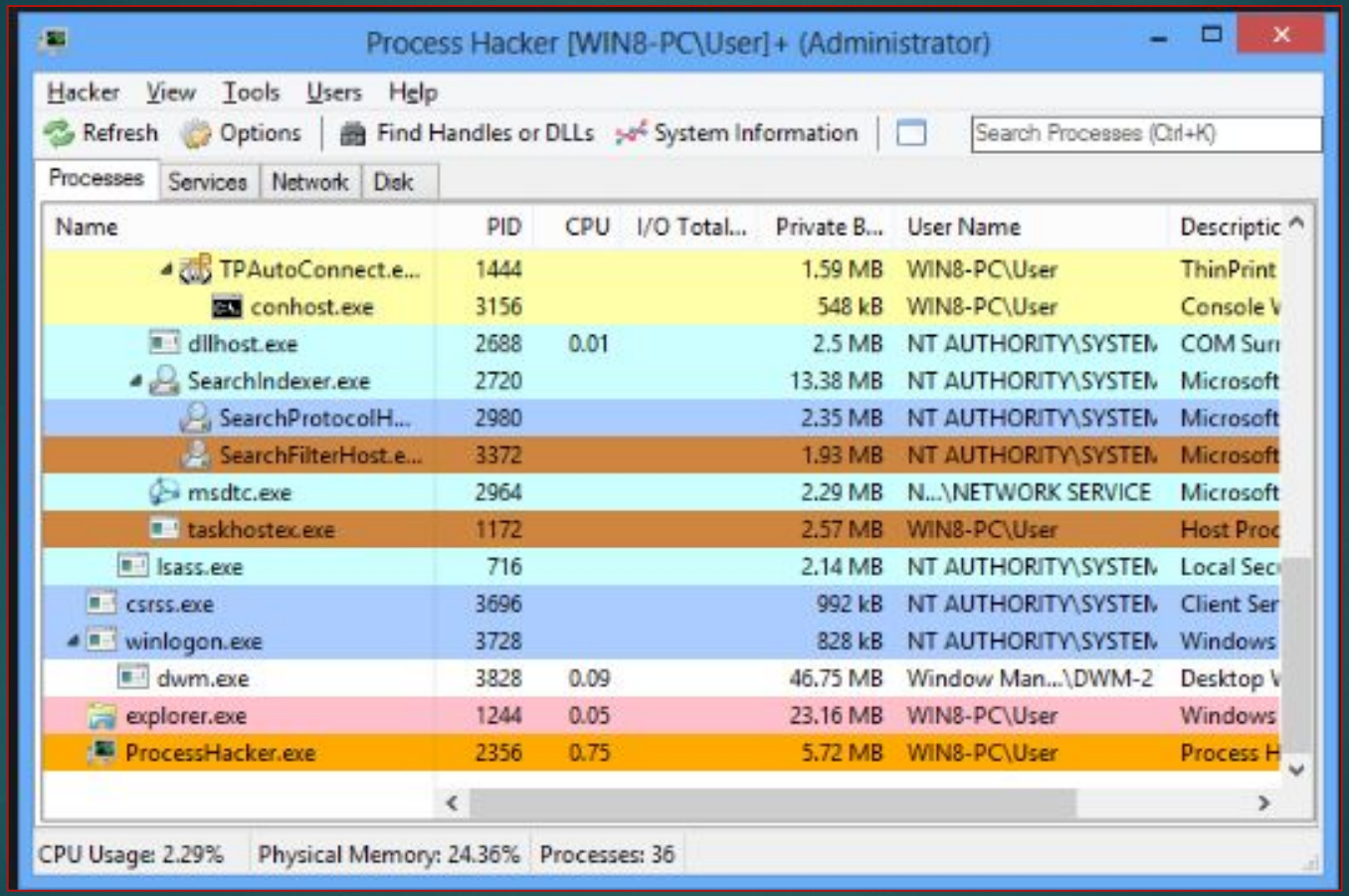
# services.msc

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



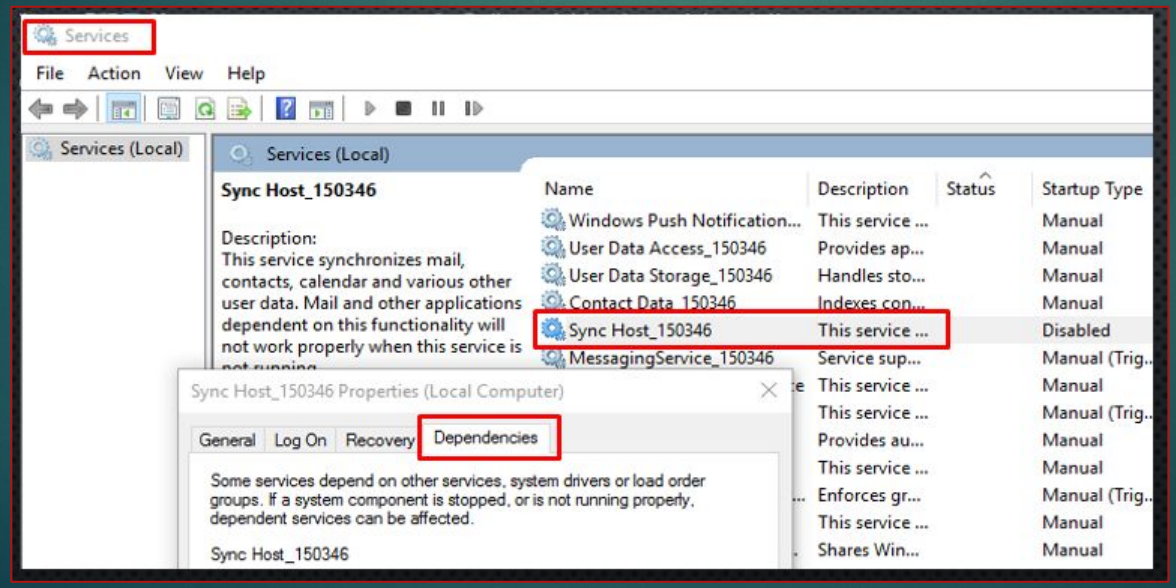
# These tools are sort of… bland… incomes “Process hacker”




Process Hacker [WIN8-PC\User]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find Handles or DLLs System Information
Search Processes (Ctrl+K)
Processes Services Network Disk
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 Sur
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
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



# Awesome Windows talks that Ross recommends

- https://www.youtube.com/watch?v=pjKNx41Ubxw&list=PLuWOygGyQTQWreyGno5FzLq44Jw2FQ1Sy

- https://www.youtube.com/watch?v=Wuy_Pm3KaV8

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

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

# STUFF I DIDN'T COVER

- crontabs
- Firewall appliances (UFW, IPTABLES, Palo Alto)
- 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 ):
- logs,

# That’s all for services, any questions?