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



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

- Domain Name System (DNS)
- Secure Shell (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:~S 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:~S
```

Switch	<u>Example</u>	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:~S 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
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
        open http
80/tcp
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)
                          netkit-rsh rexecd
512/tcp open exec
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
                          MvSOL 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

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 2224

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 4

Download

Alternative downloads and torrents >

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

Download

Alternative downloads and torrents >

What service(s) are on my box?

```
Managing Services

Ubuntu Version >= 15.04
systemctl {start|stop|...} {service_name}.service

Ubuntu Version < 15.04
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
                                                network-manager skeleton
 acpid
                         dns-clean
alsa-utils
                         grub-common
                                                                 speech-dispatcher
                                                ondemand
                         halt
                                                plymouth
                                                                 thermald
Firefox Web Browser
                                                plymouth-log
                         hostname.sh
                                                                  udev
аррагиог
                         hwclock.sh
                                                pppd-dns
                                                                 ufw
 apport
                                                                 umountfs
 avahi-daemon
                         irgbalance
                                                DEOCDS
binfmt-support
                         kerneloops
                                                gemu-kvm
                                                                  umountnfs.sh
bluetooth
                         keyboard-setup
                                                                  umountroot
 bootmisc.sh
                         killprocs
                                                rc.local
                                                                 unattended-upgrades
 brltty
                         kmod
                                                                 urandom
                                                rcs
 checkfs.sh
                                                                 uuidd
                         lightdm
                                                README
 checkroot-bootclean.sh
                         mountall-bootclean.sh
                                                                 virtualbox
                                                reboot
                         mountall.sh
 checkroot.sh
                                                resolvconf
                                                                 virtualbox-quest-utils
 console-setup
                         mountdevsubfs.sh
                                                rsync
                                                                 whoopsie
                         mountkernfs.sh
                                                rsyslog
                                                                  x11-common
 CLOU
                         mountnfs-bootclean.sh
 CUDS
                                                saned
 cups-browsed
                         mountnfs.sh
                                                sendsias
 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
 [ + ] irgbalance
  - ] kerneloops
 [ + ] keyboard-setup
 [ - ] killprocs
 [ + ] kmod
 + 1 liahtdm
       mountall-bootclean.sh
       mountall.sh
  - 1 mountdevsubfs.sh
  - 1 mountkernfs.sh
       mountnfs-bootclean.sh
       mountnfs.sh
       network-manager
 [ + ] networking
 + 1 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
                        gemu-kvm
                        rc.local
                        resolvconf
                        rsyslog
                        speech-dispatcher
                        udev
                        ufw
                        unattended-upgrades
                     1 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
    lass@vince:~S
```

systemctl -1 --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
                                             loaded
                                                      inactive dead
                                                                       Save/Restore Sound Card State
 System Settings Service
 disd-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
                                                      inactive dead
                                                                       Daily apt download activities
                                            loaded
auditd.service
                                                                       auditd.service
                                             not-found inactive dead
  avahi-daemon.service
                                                      active running Avahi mDNS/DNS-SD Stack
                                            loaded
                                                      active exited Enable support for additional executable binary formats
 binfmt-support.service
                                             loaded
 brlttv.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
                                                               exited Set console font and keymap
 console-setup.service
                                             loaded
                                                      active
 cron.service
                                             loaded
                                                      active
                                                               running Regular background program processing daemon
 cups-browsed.service
                                            loaded
                                                              running Make remote CUPS printers available locally
                                                      active
                                                                       CUPS Scheduler
 cups.service
                                            loaded
                                                      inactive dead
  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 Odns-up
  emergency.service
                                             loaded
                                                      inactive dead
                                                                       Emergency Shell
 failsafe-x.service
                                                                       X.org diagnosis failsafe
                                            loaded
                                                      inactive dead
festival.service
                                            not-found inactive dead
                                                                       festival.service
 friendly-recovery.service
                                            loaded
                                                      inactive dead
                                                                       Recovery mode menu
                                                                       getty on tty2-tty6 if dbus and logind are not available
 getty-static.service
                                             loaded
                                                      inactive dead
  getty@tty1.service
                                            loaded
                                                      active running Getty on ttv1
                                                      inactive dead
 getty@tty7.service
                                            loaded
                                                                       Getty on ttv7
  qpu-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
  irabalance.service
                                                      active exited LSB: daemon to balance interrupts for SMP systems
                                            loaded
bd.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
                                                     ACTIVE SUB
                                                                      DESCRIPTION
                                            LOAD
 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
                                            loaded
                                                                      Manage Sound Card State (restore and store)
  alsa-state.service
                                                     inactive dead
  anacron.service
                                            loaded
                                                     inactive dead
                                                                      Run anacron jobs
                                            loaded
                                                     active exited LSB: AppArmor initialization
  apparmor.service
  apport.service
                                            loaded
                                                     active exited LSB: automatic crash report generation
 apt-daily-upgrade.service
                                            loaded
                                                                      Daily apt upgrade and clean activities
                                                     inactive dead
 apt-daily.service
                                            loaded
                                                                      Daily apt download activities
                                                     inactive dead
auditd.service
                                            not-found inactive dead
                                                                      auditd.service
 avahi-daemon.service
                                            loaded
                                                     active running Avahi mDNS/DNS-SD Stack
                                                     active exited Enable support for additional executable binary formats
 binfmt-support.service
                                            loaded
 brltty.service
                                            loaded
                                                     inactive dead
                                                                      Braille Device Support
                                                     active running Manage, Install and Generate Color Profiles
 colord.service
                                            loaded
console-screen.service
                                            not-found inactive dead
                                                                      console-screen.service
                                                     active exited Set console font and keymap
  console-setup.service
                                            loaded
                                                     active running Regular background program processing daemon
  cron.service
                                            loaded
                                                     active running Make remote CUPS printers available locally
 cups-browsed.service
                                            loaded
 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 Odns-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										
PID	%CPU	%MEM	VSZ	RSS	TTY		STAT	START	TIME	COMMAND
1	0.1	0.1	23936	4760	?		Ss	23:38		/sbin/init splas
2	0.0	0.0	0	0	?		S	23:38	0:00	[kthreadd]
4	0.0	0.0	0	0	?		S<	23:38	0:00	[kworker/0:0H]
6	0.0	0.0	0	0	?		S	23:38	0:00	[ksoftirqd/0]
7	0.0	0.0	0	0	?		S	23:38	0:00	[rcu_sched]
8	0.0	0.0	0	0	?		S	23:38	0:00	[rcu_bh]
9	0.0	0.0	0	0	?		S	23:38	0:00	[migration/0]
10	0.0	0.0	0	0	?		S <	23:38	0:00	[lru-add-drain]
11	0.0	0.0	0	0	?		S	23:38	0:00	[watchdog/0]
12	0.0	0.0	0	0	?		S	23:38	0:00	[cpuhp/0]
13	0.0	0.0	0	0	?		S	23:38	0:00	[kdevtmpfs]
14	0.0	0.0	0	0	?		S<	23:38	0:00	[netns]
15	0.0	0.0	0	0	?		S	23:38	0:00	[khungtaskd]
16	0.0	0.0	0	0	?		S	23:38	0:00	[oom_reaper]
17	0.0	0.0	0	0	?		S<	23:38	0:00	[writeback]
18	0.0	0.0	0	0	?		S	23:38	0:00	[kcompactd0]
19	0.0	0.0	0	0	?		SN	23:38		[ksmd]
20	0.0	0.0	0	0	?		SN	23:38	0:00	[khugepaged]
21	0.0	0.0	0	0	?		S<	23:38	0:00	[crypto]
22	0.0	0.0	0	0	?		S<	23:38	0:00	[kintegrityd]
23	0.0	0.0	0	0	?		S<	23:38	0:00	[bioset]
24	0.0	0.0	0	0	?		S<	23:38	0:00	[kblockd]
25	0.0	0.0	0	0	?		S<	23:38	0:00	[ata_sff]
26	0.0	0.0	0	0	?		S<	23:38		[md]
	PID 1 2 4 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	PID %CPU 1 0.1 2 0.0 4 0.0 6 0.0 7 0.0 8 0.0 9 0.0 10 0.0 11 0.0 12 0.0 13 0.0 14 0.0 15 0.0 16 0.0 17 0.0 18 0.0 19 0.0 20 0.0 21 0.0 22 0.0 23 0.0 24 0.0 25 0.0	PID %CPU %MEM 1 0.1 0.1 2 0.0 0.0 4 0.0 0.0 6 0.0 0.0 7 0.0 0.0 8 0.0 0.0 9 0.0 0.0 10 0.0 0.0 11 0.0 0.0 12 0.0 0.0 13 0.0 0.0 14 0.0 0.0 15 0.0 0.0 16 0.0 0.0 17 0.0 0.0 18 0.0 0.0 19 0.0 0.0 20 0.0 0.0 21 0.0 0.0 22 0.0 0.0 23 0.0 0.0 24 0.0 0.0 25 0.0 0.0	PID %CPU %MEM VSZ 1 0.1 0.1 23936 2 0.0 0.0 0 4 0.0 0.0 0 6 0.0 0.0 0 7 0.0 0.0 0 8 0.0 0.0 0 9 0.0 0.0 0 10 0.0 0.0 0 11 0.0 0.0 0 12 0.0 0.0 0 13 0.0 0.0 0 14 0.0 0.0 0 15 0.0 0.0 0 16 0.0 0.0 0 17 0.0 0.0 0 18 0.0 0.0 0 19 0.0 0.0 0 20 0.0 0.0 0 21 0.0 0.0 0 22 0.0 0.0 0 23 0.0 0.0 0 24 0.0 0.0 0 25 0.0 0.0 0	PID %CPU %MEM VSZ RSS 1 0.1 0.1 23936 4760 2 0.0 0.0 0 0 4 0.0 0.0 0 0 6 0.0 0.0 0 0 7 0.0 0.0 0 0 8 0.0 0.0 0 0 9 0.0 0.0 0 0 10 0.0 0.0 0 11 0.0 0.0 0 12 0.0 0.0 0 13 0.0 0.0 0 14 0.0 0.0 0 15 0.0 0.0 0 16 0.0 0.0 0 17 0.0 0.0 0 18 0.0 0.0 0 19 0.0 0.0 0 19 0.0 0.0 0 20 0.0 0.0 0 21 0.0 0.0 0 22 0.0 0.0 0 23 0.0 0.0 0 24 0.0 0.0 0 25 0.0 0.0 0	PID %CPU %MEM VSZ RSS TTY 1 0.1 0.1 23936 4760 ? 2 0.0 0.0 0 0 0 ? 4 0.0 0.0 0 0 0 ? 6 0.0 0.0 0 0 0 ? 7 0.0 0.0 0 0 0 ? 8 0.0 0.0 0 0 0 ? 9 0.0 0.0 0 0 0 ? 10 0.0 0.0 0 0 ? 11 0.0 0.0 0 0 ? 12 0.0 0.0 0 0 ? 13 0.0 0.0 0 0 ? 14 0.0 0.0 0 0 ? 15 0.0 0.0 0 0 ? 16 0.0 0.0 0 0 ? 17 0.0 0.0 0 0 ? 18 0.0 0.0 0 0 ? 19 0.0 0.0 0 0 ? 21 0.0 0.0 0 0 ? 22 0.0 0.0 0 0 ? 23 0.0 0.0 0 0 ? 24 0.0 0.0 0 0 ? 25 0.0 0.0 0 0 ?	PID %CPU %MEM	PID %CPU %MEM VSZ RSS TTY STAT 1 0.1 0.1 23936 4760 ? Ss 2 0.0 0.0 0 0 ? Ss 4 0.0 0.0 0 0 ? Ss 6 0.0 0.0 0 0 ? Ss 7 0.0 0.0 0 0 ? Ss 8 0.0 0.0 0 0 ? Ss 9 0.0 0.0 0 0 ? Ss 10 0.0 0.0 0 ? Ss 11 0.0 0.0 0 ? Ss 12 0.0 0.0 0 ? Ss 13 0.0 0.0 0 ? Ss 14 0.0 0.0 0 ? Ss 15 0.0 0.0 0 ?	PID %CPU %MEM VSZ RSS TTY STAT START 1 0.1 0.1 23936 4760 ? SS 23:38 2 0.0 0.0 0 0 ? S 23:38 4 0.0 0.0 0 0 ? S 23:38 6 0.0 0.0 0 0 ? S 23:38 7 0.0 0.0 0 0 ? S 23:38 8 0.0 0.0 0 0 ? S 23:38 9 0.0 0.0 0 ? S 23:38 10 0.0 0.0 0 ? S 23:38 11 0.0 0.0 0 ? S 23:38 12 0.0 0.0 0 ? S 23:38 13 0.0 0.0 0 ? S 23:38	PID %CPU %MEM VSZ RSS TTY STAT START TIME 1 0.1 0.1 23936 4760 ? SS 23:38 0:01 2 0.0 0.0 0 0 ? S 23:38 0:00 4 0.0 0.0 0 0 ? S 23:38 0:00 6 0.0 0.0 0 0 ? S 23:38 0:00 7 0.0 0.0 0 0 ? S 23:38 0:00 8 0.0 0.0 0 0 ? S 23:38 0:00 9 0.0 0.0 0 ? S 23:38 0:00 10 0.0 0.0 0 ? S 23:38 0:00 11 0.0 0.0 0 ? S 23:38 0:00 12 0.0 0.0 0

htop

```
CPU[]]]]]]]]
                                                                            Tasks: 103, 205 thr: 2 runni
Mem[||||||||||||||
                                                               502M/3.95G
                                                                            Load average: 0.27 0.12 0.09
Swp
                                                                  OK/976M
                                                                            Uptime: 00:22:55
                                   SHR S CPU% MEM%
PID USER
                             RES
                                                     TIME+ Command
1823 os-class
                                                   0:45.76 compiz
                            153M 70816 5 11.2 3.8
                                          2.0 2.0 0:18.03 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth
968 root
2147 os-class
                      116M 35000 27576 S
                                               0.8 0:04.08 /usr/lib/qnome-terminal/qnome-terminal-server
                                          0.7
4706 os-class
                      6220
                             3612
                                          0.0
                                              0.1 0:00.21 htop
                                          0.0 0.1 0:00.21 /usr/sbin/VBoxService --pidfile /var/run/vbox
933 root
                   0 30536
                            2532
1218 os-class
                   0 18316
                            2200
                                              0.1 0:01.72 /usr/bin/VBoxClient --draganddrop
                                          0.0
1220 os-class
                   0 18316
                            2200
                                  1880 S
                                          0.0 0.1 0:01.71 /usr/bin/VBoxClient --draganddrop
820 root
                                              0.3 0:00.47 /usr/lib/policykit-1/polkitd --no-debug
                                               1.6 0:03.90 /usr/bin/gnome-software --gapplication-servic
1960 os-class
974 root
                   0 256M 81760 34800 S
                                          0.0 2.0 0:01.50 /usr/lib/xorg/Xorg -core :0 -seat seat0 -auth
1447 os-class
                            7156
                                          0.0
                                              0.2 0:00.27 /usr/lib/ibus/ibus-engine-simple
                                          0.0 0.1 0:01.60 /sbin/init splash
  1 root
                   0 23936
                            4760
                                  3544 S
221 root
                      9764
                                              0.1 0:00.14 /lib/systemd/systemd-journald
                                              0.1 0:00.12 /lib/systemd/systemd-udevd
237 root
                   0 14664
                            4024
                                  2992 S
                                          0.0
692 root
                      2244
                            1256
                                  1188 S
                                          0.0 0.0 0:00.02 /usr/sbin/acpid
693 root
                                              0.1 0:00.00 /usr/sbin/cron -f
694 messagebu
                       6960
                            4772
                                               0.1 0:01.14 /usr/bin/dbus-daemon --system --address=syste
710 root
                       4140
                                          0.0
                                              0.1 0:00.03 /lib/systemd/systemd-logind
767 root
                       827M 18280
                                  9232 S
                                                   0:00.00 /usr/lib/snapd/snapd
768 root
                      827M 18280
                                  9232 S 0.0 0.4 0:00.00 /usr/lib/snapd/snapd
770 root
                       827M 18280
                                  9232 S 0.0
                                              0.4 0:00.00
                                                           /usr/lib/snapd/snapd
785 root
                       827M 18280
                                  9232 S 0.0
                                              0.4 0:00.00
                                                            /usr/lib/snapd/snapd
2866 root
                      827M 18280
                                  9232 S 0.0 0.4 0:00.00 /usr/lib/snapd/snapd
729 root
                      827M 18280
                                  9232 S
                                          0.0
                                              0.4 0:00.01 /usr/lib/snapd/snapd
775 root
                                                   0:00.00
779 root
                   0 90832 16980 13136 S
                                          0.0 0.4 0:00.03 /usr/sbin/NetworkManager --no-daemon
733 root
                                          0.0 0.4 0:00.15 /usr/sbin/NetworkManager --no-daemon
738 root
                   0 39956
                                  7100 S 0.0 0.2 0:00.02 /usr/lib/accountsservice/accounts-daemon
                            9812
757 root
                   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	@vinc	e: ~			
os-class	@vince	-\$ p	s -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	?
	4.5	0.0	0 0	۵	۵	3

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 -1

```
[Ana cul] ( ++ 1 1)
os-class@vince:~$ kill -l
1) SIGHUP
                 2) SIGINT
                                                  A) STOTLL
                                 3) SIGOUIT
                                                                  5) SIGTRAP
                                 8) SIGFPE
                                                    SIGKILL
6) SIGABRT
                 7) SIGBUS
                                                                 10) SIGUSR1
11) SIGSEGV
                12) SIGUSR2
                                13) SIGPIPE
                                                                 15) SIGTERM
                                                 14) SIGALRM
16) SIGSTKFLT
                17) SIGCHLD
                                18) SIGCONT
                                                 19) SIGSTOP
                                                                 20) SIGTSTP
21) SIGTTIN
                22) SIGTTOU
                                23) SIGURG
                                                    SIGXCPU
                                                                 25) SIGXFSZ
                27) SIGPROF
26) SIGVTALRM
                                28) SIGWINCH
                                                 29) SIGIO
                                                                 30)
                                                                    SIGPWR
31) SIGSYS
                   SIGRTMIN
                                35) SIGRTMIN+1
                                                 36) SIGRTMIN+2
                                                                    SIGRTMIN+3
38) SIGRTMIN+4
                39) SIGRTMIN+5
                                40) SIGRTMIN+6
                                                 41) SIGRTMIN+7
                                                                 42) SIGRTMIN+8
43) SIGRTMIN+9
                   SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47)
                                                                    SIGRTMIN+13
                   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
   SIGRTMAX-6
                59) SIGRTMAX-5
                                60) SIGRTMAX-4
                                                 61) SIGRTMAX-3
                                                                 62) SIGRTMAX-2
63) SIGRTMAX-1 64)
                   SIGRTMAX
os-class@vince:~S
```

we can use this to see the signal handlers

SOURCE:

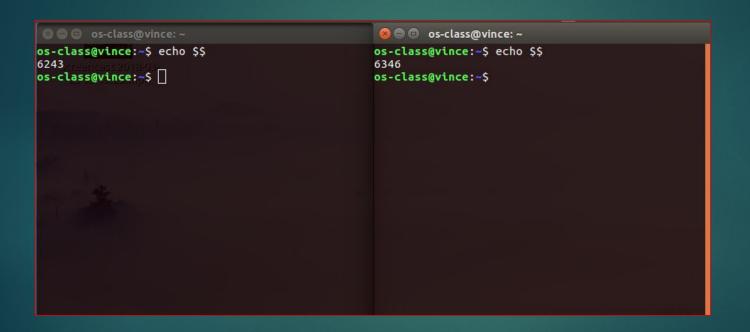
http://www.linfo.org/kill.html

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)
                                -{qdbus}(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)
            -{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)
                            -{gdbus}(1128)
             -colord(1125)-
                            {gmain}(1126)
            -cron(693)
            -cups-browsed(821)
                                -{gdbus}(828)
                                 {gmain}(827)
             -dbus-daemon(694)
```

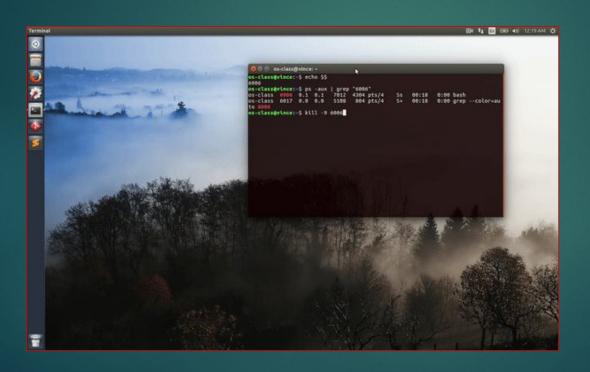
Ross likes to kill bash sessions...



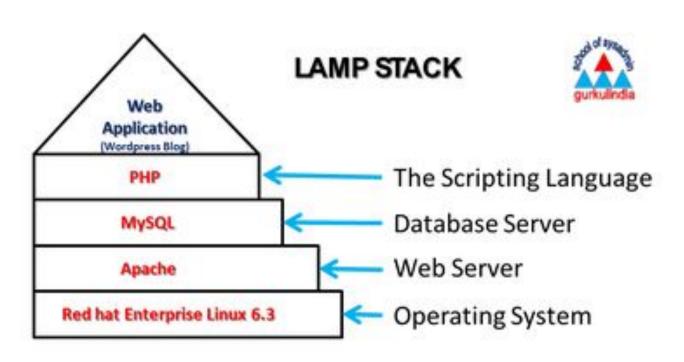
echo \$\$

```
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?

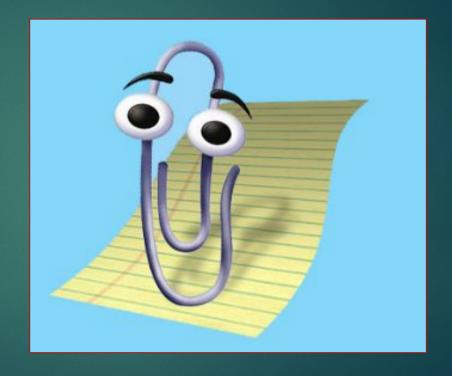


LAMP Stack

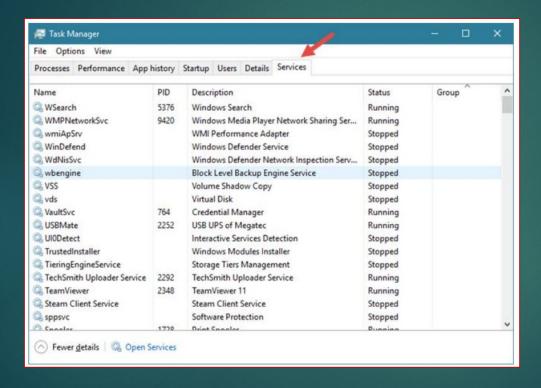


VISIT DUR SNACK B

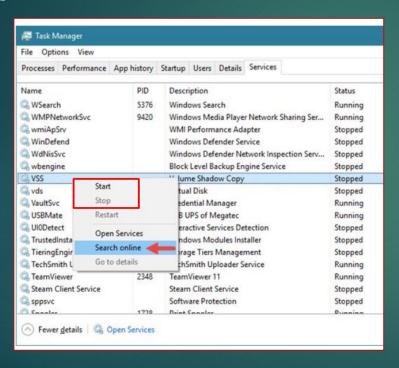
WINDOWS LAND!



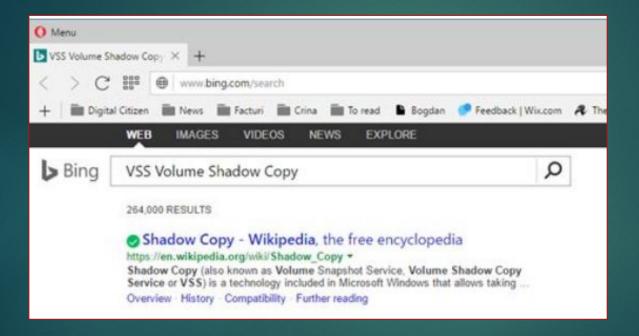
Task Manager



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

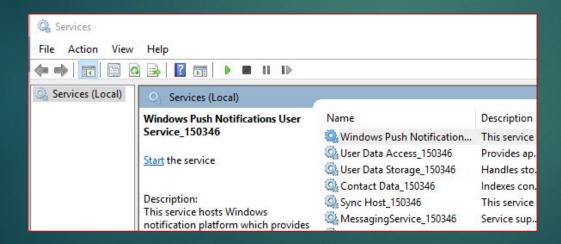


You can search online too!

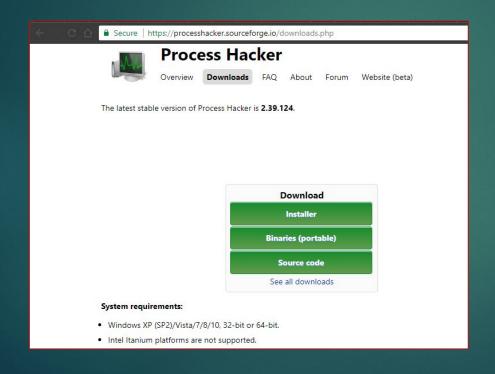


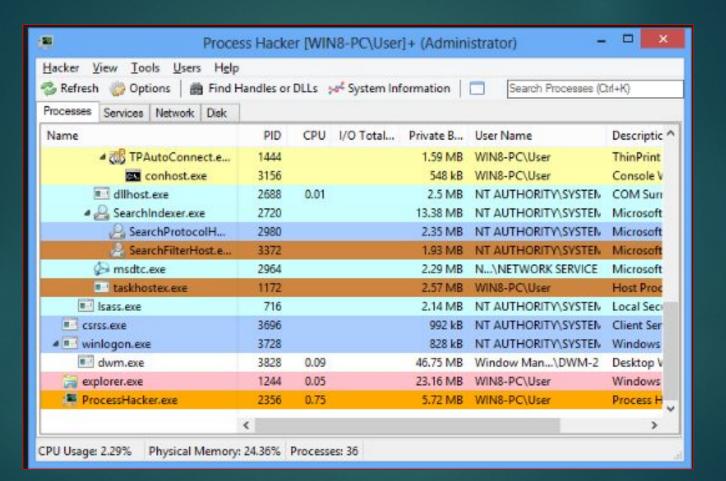
services.msc

- ► CMD -> services.msc
- Windows search for "Services"



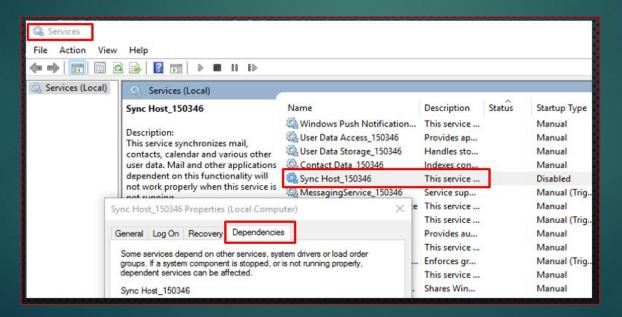
These tools are sort of... bland... incomes "Process hacker"





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=PLuWOygG yQTQWreyGno5FzLq44Jw2FQ1Sy
- 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 Isattr commands
- ssh keys and securing ssh
- /etc/shadow
- /etc/pam.d
- ▶ lot's of Windows stuff):
- logs,

That's all for services, any questions?

