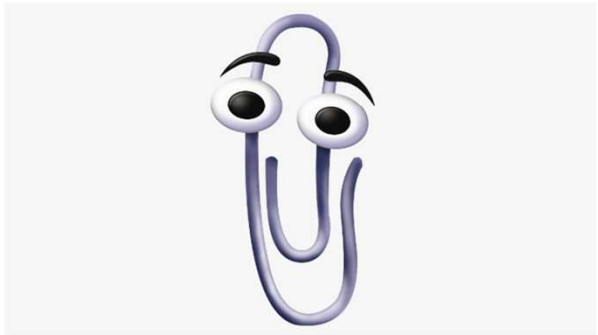
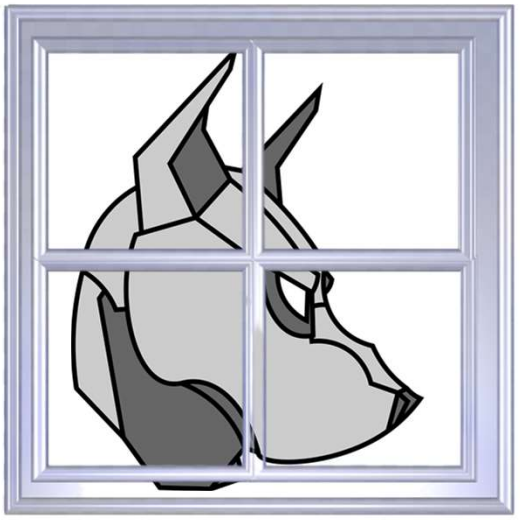
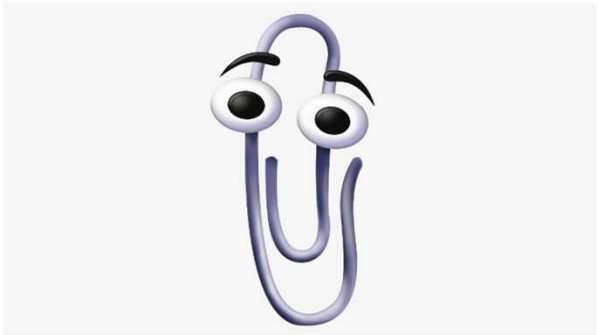
Cyber Defense Organization

Fall 2020 - Intro to Windows







Attendance

Please sign in!

https://tinyurl.com/CDOWindowsAttend

Hopefully you still have PuTTY installed

Just in case you uninstalled it in the past week...

https://www.putty.org/

already been fixed in those versions.

Package files

You probably want one of these. They include versions of all the PuTTY utilities.

(Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

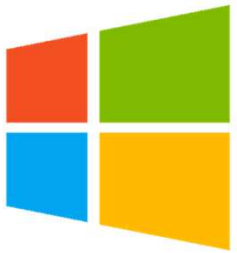
MSI ('Windows Installer')

32-bit:	putty-0.74-installer.msi	(or by FTP)	(signature)
64-bit:	putty-64bit-0.74-installer.msi	(or by FTP)	(signature)

Unix source archive

.tar.gz:	putty-0.74.tar.gz	(or by FTP)	(signature)

What is Windows?



- At its core, Windows is a GUI based OS
- Windows is extremely popular for large scale (enterprise) applications

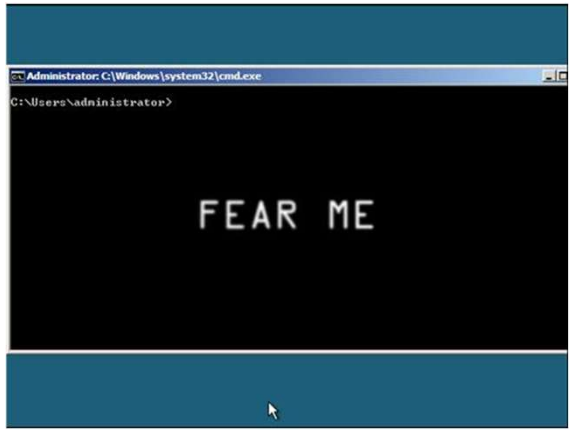
Windows can be used to host many different services including, but not limited to:

- AD (Most basic: Authentication)
- DNS
- IIS (Web Server)
- DHCP
- And More!

Are there different types of Windows?

Unlike Linux, there are not different distributions of Windows.

There are different utilities that Windows offers, such as Windows Server and Windows Server Core, which are used to manage services.



Windows Server Core is scary...

The Parts of Windows

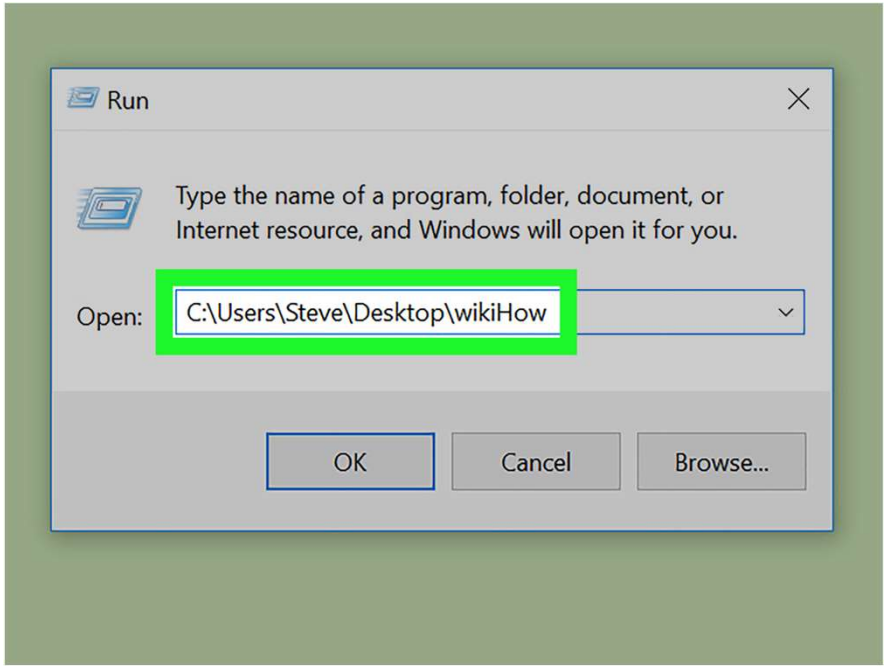
File Structure

It’s pretty straight forward.

The letter denotes which hard drive
(C,F,E,G, etc.)
Then you have directories like:

- Program Files - Where programs are installed (x86 is 32 bit applications)
- Users - Where user profiles are
- Windows - Where windows itself resides. Known as the “root” of the OS

It can get far more complicated but that is out of the scope of this workshop.

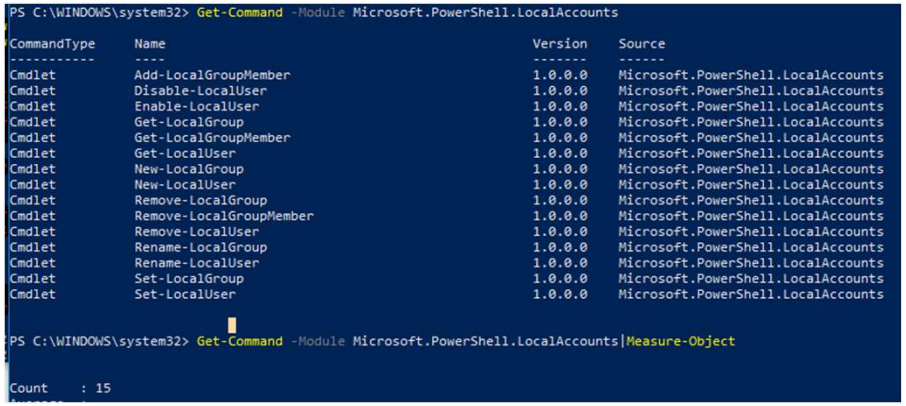


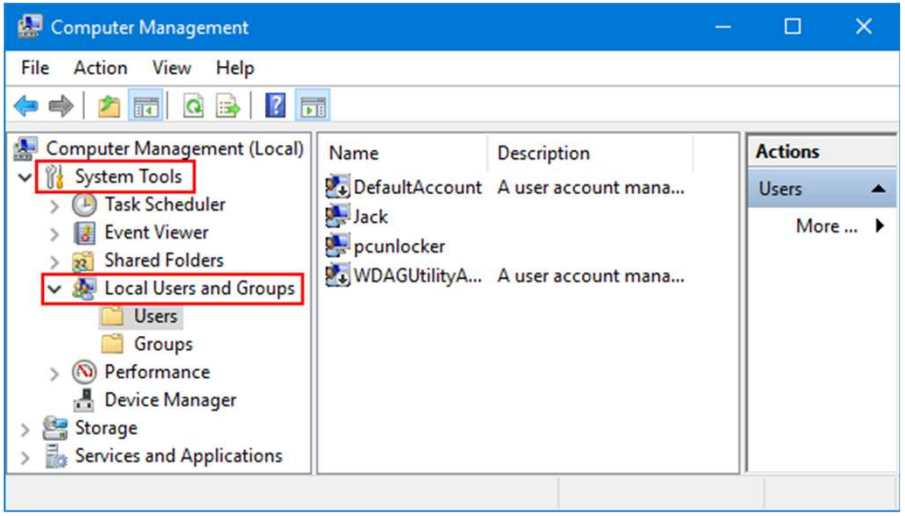
Users and Groups

Just like Linux, there are users and groups which determines the amount of permissions that the user gets.

Managing user can be done both through the GUI and through powershell.

This can be very important for competitions!





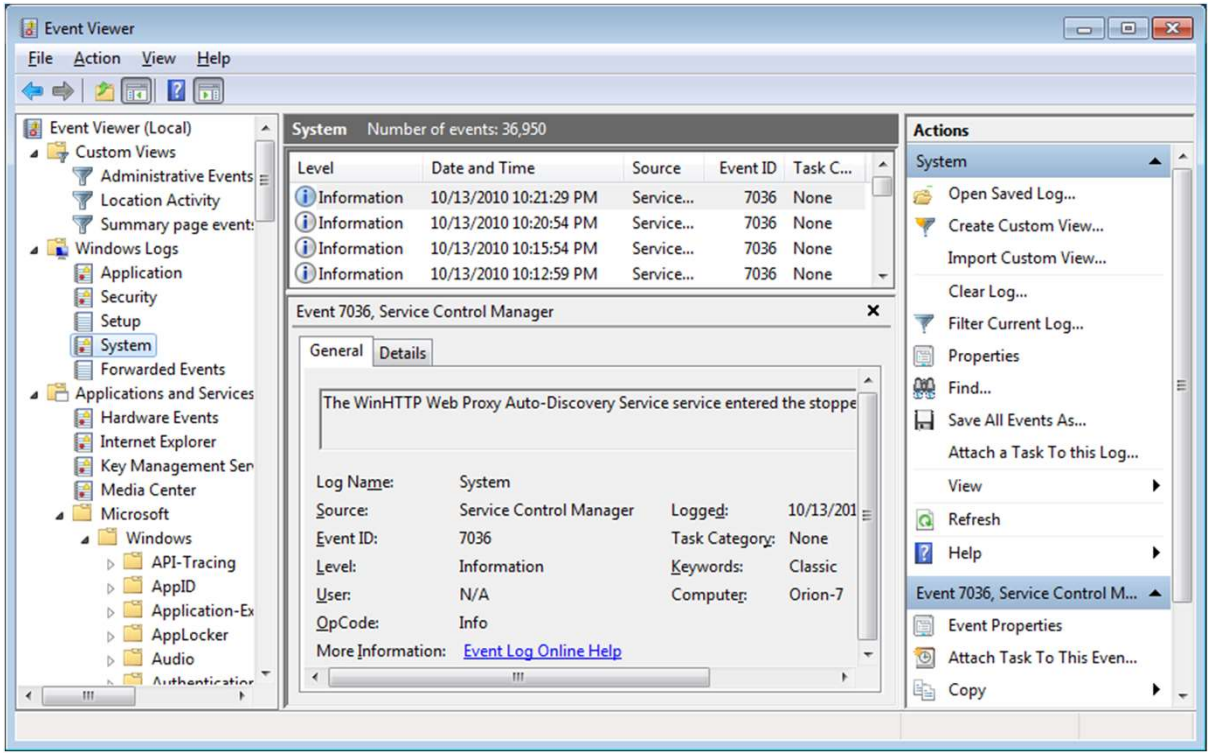
Events

Events on windows are essentially logs.

It has very detailed descriptions of what happened, at what time, and so on.

View them in Event Viewer or C:\Windows\System32\Winevt\Logs

These can give you a ton of information!

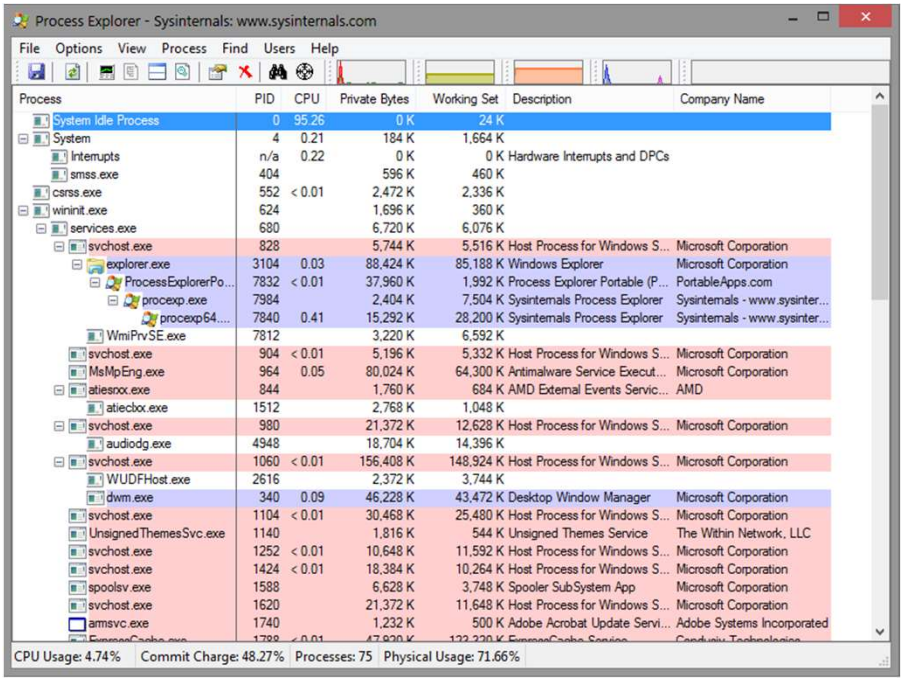


Processes

Basically, a process is when you run a program.

This can be anything from Google Chrome to malware.

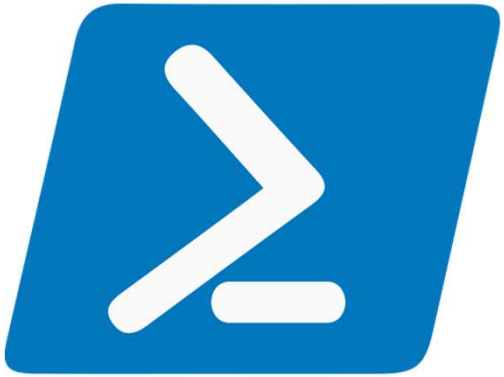
You can view these very basically with task manager, or from a more detailed view with ProcessExplorer.



How do we get things done?

We can use the GUI, but that can be slow and tedious.

PowerShell



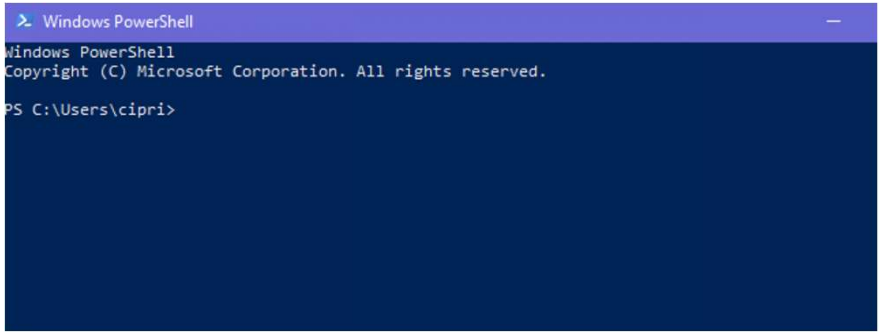
PowerShell is a command line shell, unlike a typical shell which will just accept and return text, PowerShell accepts and returns objects.

(An object being structured information that is more than just a string of characters. Command outputs always contain extra info.)

Command syntax is really straight forward:

This will get the process named Explorer

```
Get-Process -Name Explorer
```



PowerShell

Commands are called cmdlets and are structured in Verb-Noun: Move-Item, Copy-Item, Join-CDO

PowerShell is not case sensitive!

Move-Item, move-item, and MoVe-ItEm are all the same.

PowerShell is very powerful. You can automate things, script, and even go as far as administrate a system using PowerShell as your main interface.

“But what about cmd?”

PowerShell is an advancement of cmd, think of PowerShell as cmd++

Get-Help is your best friend

Get-Help

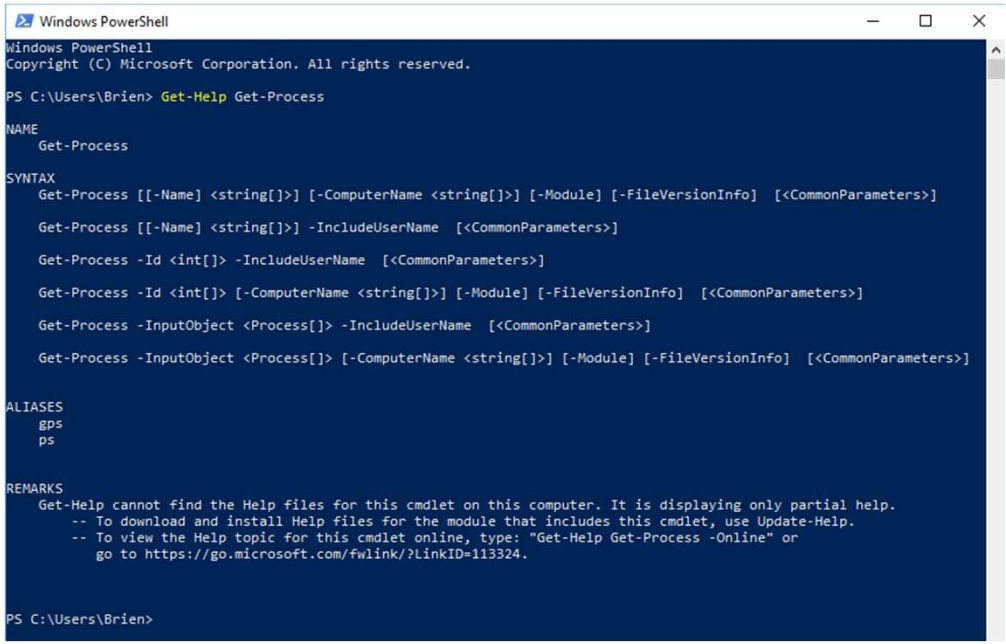
Just like Linux, windows has the equivalent to man pages, Get-Help.

Get-Help has in depth explanations of concepts of commands and the correct syntax of commands.

If I wanted to know more about the command Get-Process

I would type Get-Help Get-Process:

Sidenote: for those used to other systems and other commands, you can set up an alias for a command. In fact, Powershell has some Linux aliases preset. This is useful for keeping muscle memory intact!



Activity Time

Under The Wire

https://tinyurl.com/cdowindows2020

Join us on Discord for the hands on portion of the workshop

We will work together through the first few levels of Century

Next Week...

Intro to networking with Max

MAX

Add us on Social Media!

Twitter: **@ualbanyCDO**

Instagram: **ualbany_cdo**

Myinvolvement: **Cyber Defense Org**

Twitch: UACyberDef

We have a discord!

(discord is for UAlbany Students only)