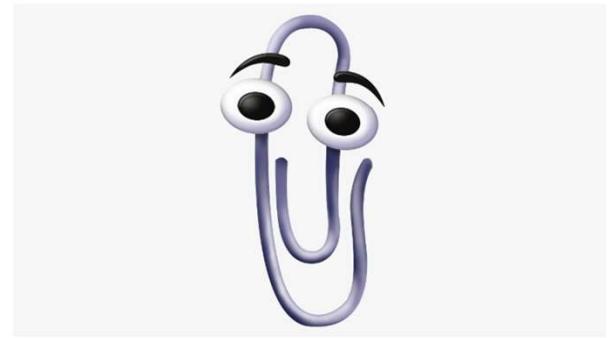
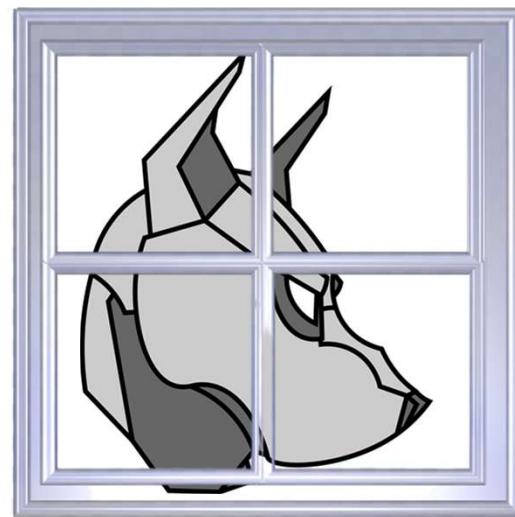
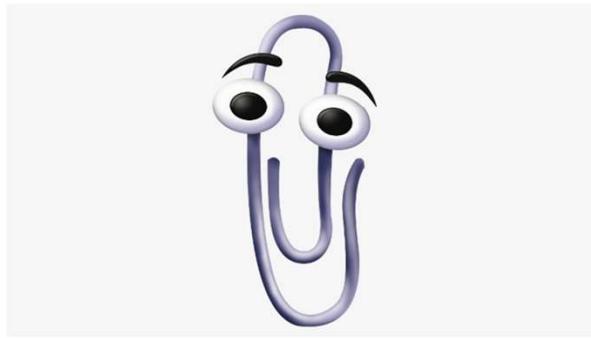


# Cyber Defense Organization

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:	<a href="#">putty-0.74-installer.msi</a>	(or by <a href="#">FTP</a> )	<a href="#">(signature)</a>
64-bit:	<a href="#">putty-64bit-0.74-installer.msi</a>	(or by <a href="#">FTP</a> )	<a href="#">(signature)</a>

**Unix source archive**

.tar.gz:	<a href="#">putty-0.74.tar.gz</a>	(or by <a href="#">FTP</a> )	<a href="#">(signature)</a>
----------	-----------------------------------	------------------------------	-----------------------------

# What is Windows?



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

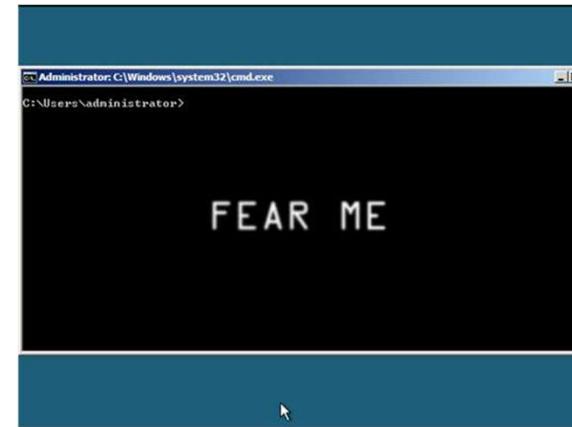
Windows can be used to host many different services including, but not limited to:

- 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

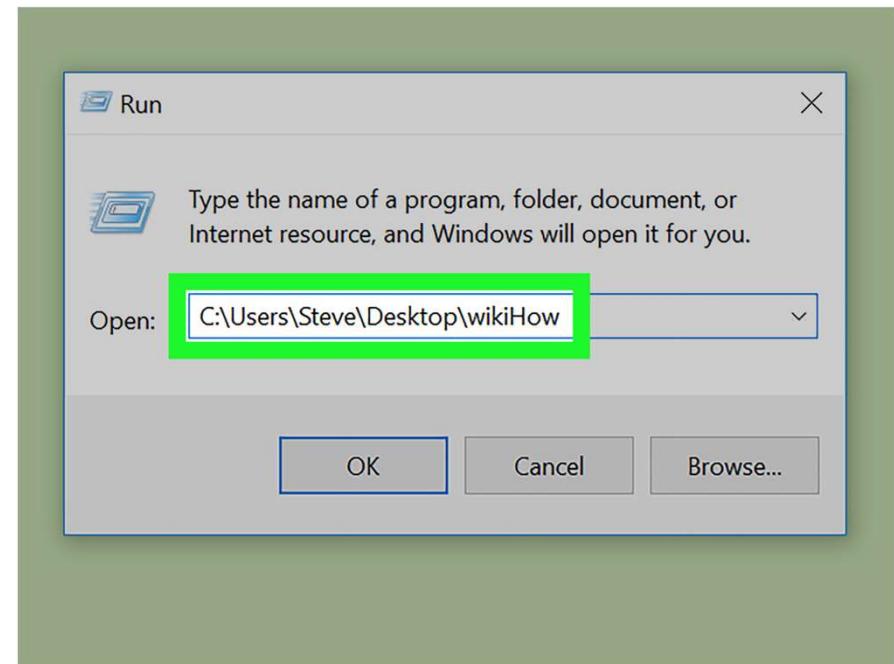
It's pretty straight forward.

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

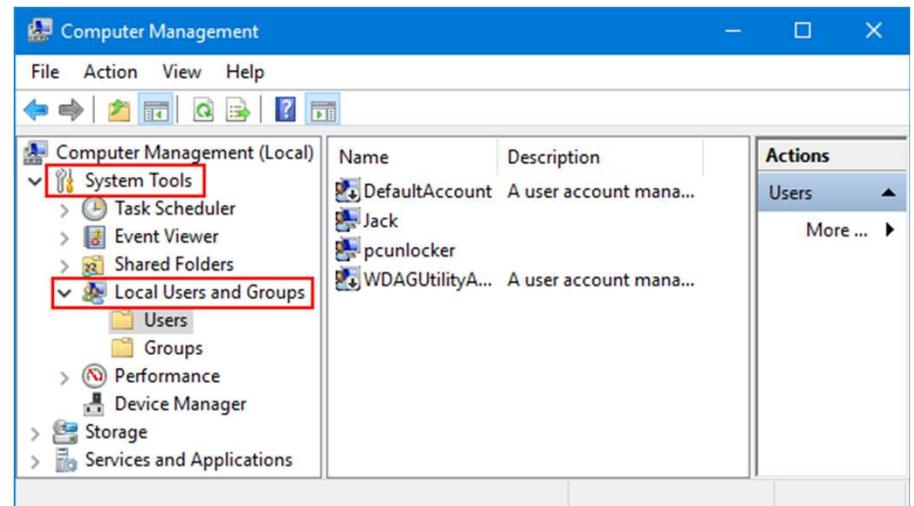
Just like Linux, there are users and groups which determines the amount of permissions that the user gets.

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

This can be very important for competitions!

```
PS C:\WINDOWS\system32> Get-Command -Module Microsoft.PowerShell.LocalAccounts
 CommandType      Name          Version   Source
 -----          ----          -----   -----
 Cmdlet          Add-LocalGroupMember 1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Disable-LocalUser   1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Enable-LocalUser   1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Get-LocalGroup     1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Get-LocalGroupMember 1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Get-LocalUser      1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          New-LocalGroup    1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          New-LocalUser     1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Remove-LocalGroup 1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Remove-LocalGroupMember 1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Remove-LocalUser   1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Rename-LocalGroup 1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Rename-LocalUser   1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Set-LocalGroup    1.0.0.0   Microsoft.PowerShell.LocalAccounts
 Cmdlet          Set-LocalUser     1.0.0.0   Microsoft.PowerShell.LocalAccounts

PS C:\WINDOWS\system32> Get-Command -Module Microsoft.PowerShell.LocalAccounts | Measure-Object
Count : 15
```



# Events

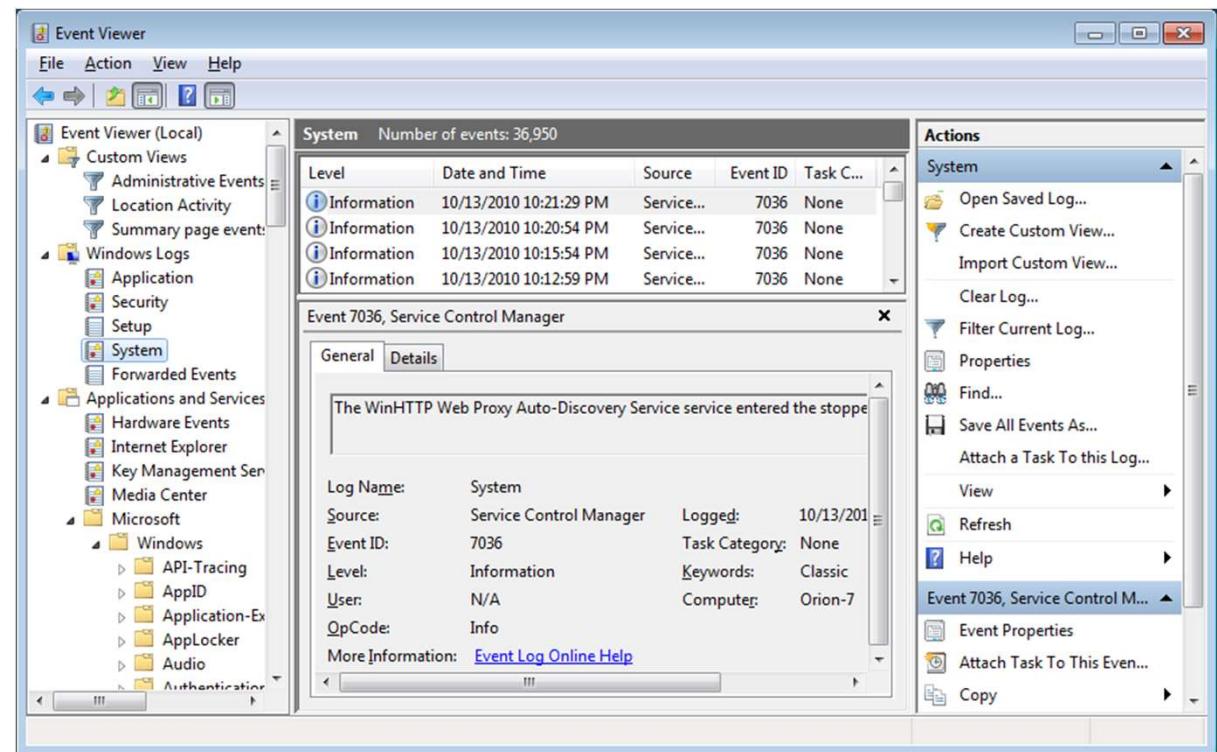


Events on windows are essentially logs.

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.

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	95.26	0 K	24 K		
System	4	0.21	184 K	1,664 K	0 K Hardware Interrupts and DPCs	
Interrupts	n/a	0.22	0 K			
smss.exe	404		596 K	460 K		
cors.exe	552	< 0.01	2,472 K	2,336 K		
wininit.exe	624		1,696 K	360 K		
services.exe	680		6,720 K	6,076 K		
svchost.exe	828		5,744 K	5,516 K Host Process for Windows S... Microsoft Corporation		
explorer.exe	3104	0.03	88,424 K	85,188 K Windows Explorer Microsoft Corporation		
ProcessExplorerPo...	7832	< 0.01	37,960 K	1,992 K Process Explorer Portable (P... PortableApps.com		
procexp.exe	7984		2,404 K	7,504 K Sysinternals Process Explorer Sysinternals - www.sysinter...		
procexp64....	7840	0.41	15,292 K	28,200 K Sysinternals Process Explorer Sysinternals - www.sysinter...		
WmiPrvSE.exe	7812		3,220 K	6,592 K		
svchost.exe	904	< 0.01	5,196 K	5,332 K Host Process for Windows S... Microsoft Corporation		
MsMpEng.exe	964	0.05	80,024 K	64,300 K Antimalware Service Execut... Microsoft Corporation		
atiesxxx.exe	844		1,760 K	684 K AMD External Events Servic... AMD		
atiexecbox.exe	1512		2,768 K	1,048 K		
svchost.exe	980		21,372 K	12,628 K Host Process for Windows S... Microsoft Corporation		
audiogd.exe	4948		18,704 K	14,396 K		
WUDFHost.exe	2616		2,372 K	3,744 K		
dwm.exe	340	0.09	46,228 K	43,472 K Desktop Window Manager Microsoft Corporation		
svchost.exe	1104	< 0.01	30,468 K	25,480 K Host Process for Windows S... Microsoft Corporation		
UnsignedThemesSvc.exe	1140		1,816 K	544 K Unsigned Themes Service The Within Network, LLC		
svchost.exe	1252	< 0.01	10,648 K	11,592 K Host Process for Windows S... Microsoft Corporation		
svchost.exe	1424	< 0.01	18,384 K	10,264 K Host Process for Windows S... Microsoft Corporation		
spoolsv.exe	1588		6,628 K	3,748 K Spooler SubSystem App Microsoft Corporation		
svchost.exe	1620		21,372 K	11,648 K Host Process for Windows S... Microsoft Corporation		
amsvc.exe	1740		1,232 K	500 K Adobe Acrobat Update Servi... Adobe Systems Incorporated		
EcommerceCache.exe	1789	< 0.01	47,920 K	132,220 K EcommerceCache Service Comodo's Technologies		

# **How do we get things done?**

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

# PowerShell

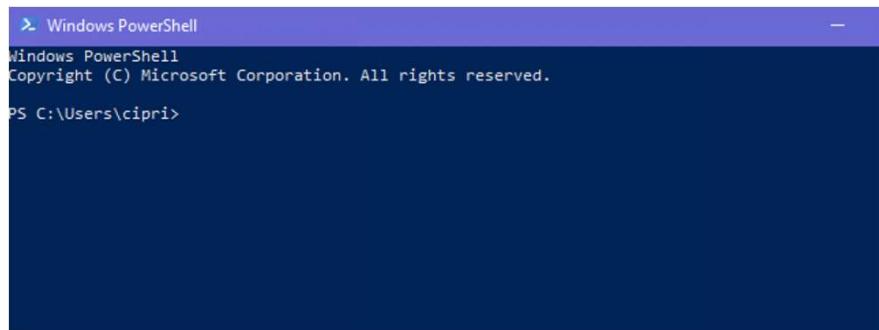
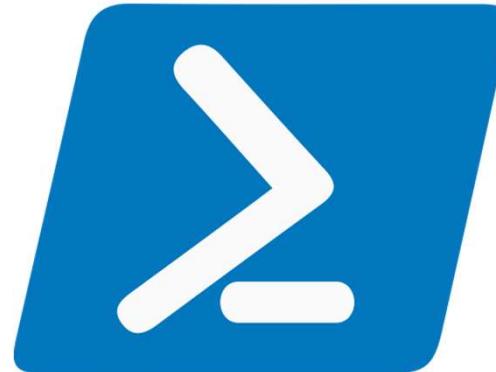
PowerShell is a command line shell, unlike a typical shell which will just accept and return text, PowerShell accepts and returns objects.

(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

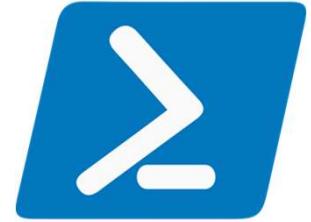
```
Get-Process -Name Explorer
```

A screenshot of a Windows PowerShell window. The title bar says "Windows PowerShell". The content area shows the command "Get-Process -Name Explorer" was run, and the output is empty, indicating there are no processes named "Explorer" running.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\cipri>
```

# 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

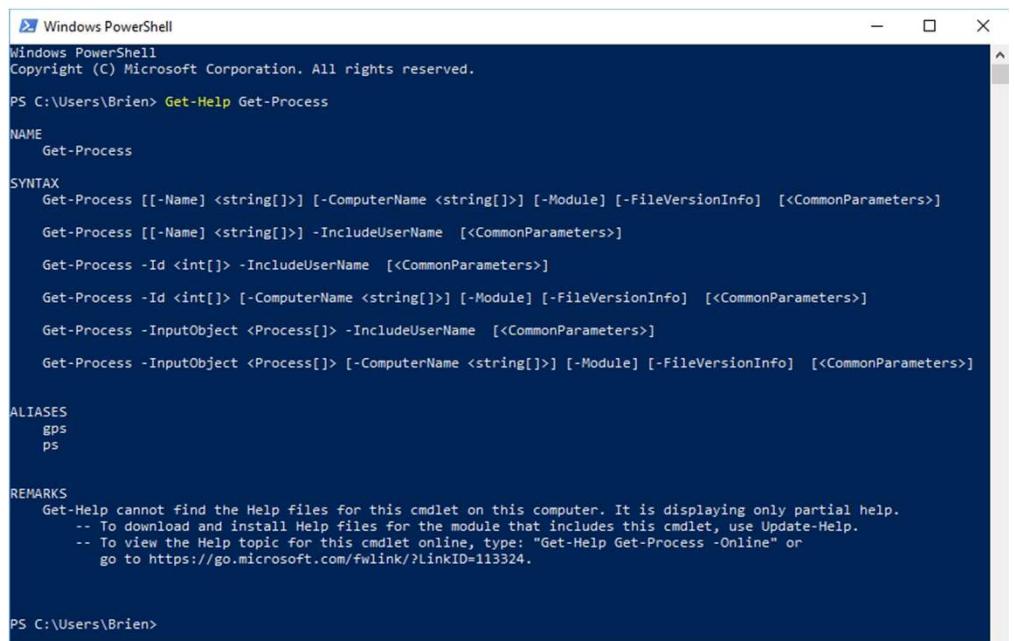
Just like Linux, windows has the equivalent to man pages, Get-Help.

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!



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Brien> Get-Help Get-Process

NAME
    Get-Process

SYNTAX
    Get-Process [[-Name] <string[]>] [-ComputerName <string[]>] [-Module] [-FileVersionInfo] [<CommonParameters>]
    Get-Process [[-Name] <string[]>] -IncludeUserName [<CommonParameters>]
    Get-Process -Id <int[]> -IncludeUserName [<CommonParameters>]
    Get-Process -Id <int[]> [-ComputerName <string[]>] [-Module] [-FileVersionInfo] [<CommonParameters>]
    Get-Process -InputObject <Process[]> -IncludeUserName [<CommonParameters>]
    Get-Process -InputObject <Process[]> [-ComputerName <string[]>] [-Module] [-FileVersionInfo] [<CommonParameters>]

ALIASES
    gps
    ps

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
    -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
    -- To view the Help topic for this cmdlet online, type: "Get-Help Get-Process -Online" or
       go to https://go.microsoft.com/fwlink/?LinkID=113324.

PS C:\Users\Brien>
```

# **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



# Add us on Social Media!

Twitter: [@ualbanyCDO](https://twitter.com/ualbanyCDO) 



Instagram: [@ualbany\\_cdo](https://www.instagram.com/ualbany_cdo) 



Myinvolvement: [Cyber Defense Org](#)

Twitch: [UACyberDef](#)

We have a discord!

(discord is for UAlbany Students only)

