LA-UR-21-25056
Approved for public release; distribution is unlimited.

Title: Command Line Cheat Sheets

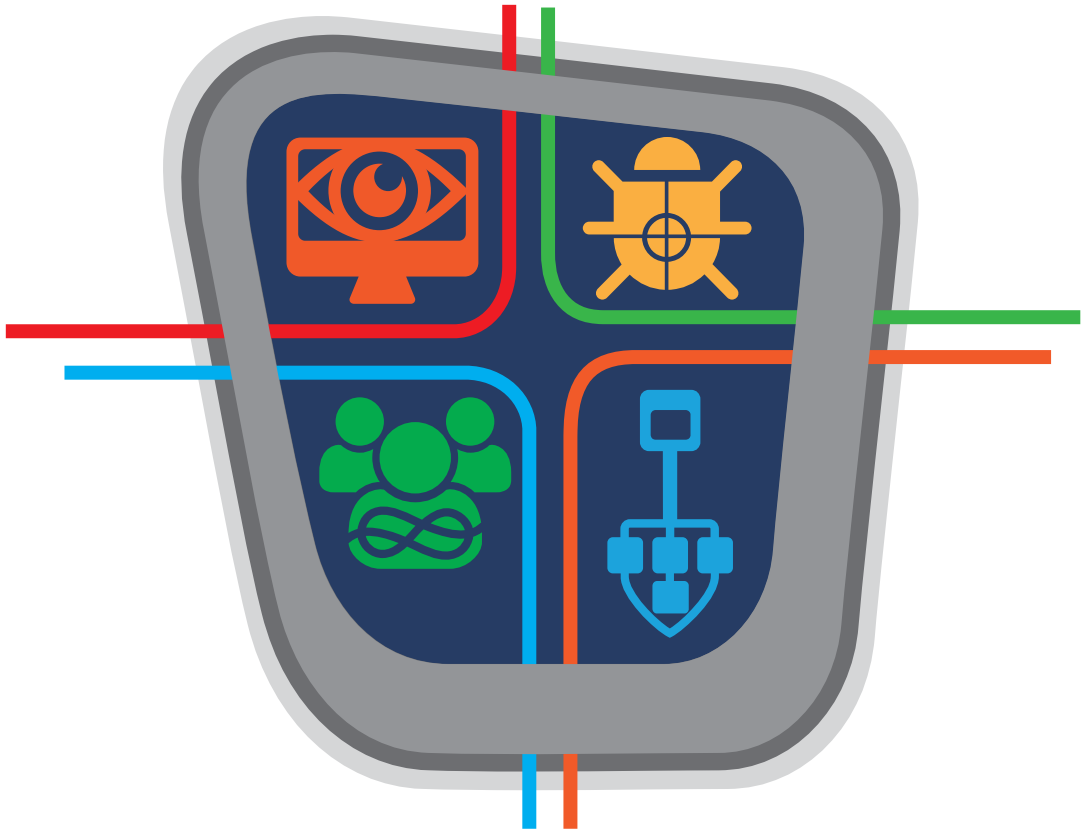
Author(s): Pope, Aaron Scott

Intended for: Cyber Fire summer school and other Cyber Fire events.

Issued: 2021-05-26

Command Line Cheat Sheets

Author: Aaron Scott Pope
A-4: Advanced Research in Cyber Systems



CYBERFIRE

Windows Command Line (CMD) Essentials Cheat Sheet

Getting around in the command line

help: Provides Help information for Windows commands.
Usage: `help` or `help <command>`

dir: Displays a list of files and subdirectories in a directory.
Usage: `dir` or `dir <directory>`

tree: Graphically displays the directory structure of a drive or path.
Usage: `tree` or `tree <directory>`

cd: Displays the name of or changes the current directory.
Usage: `cd` or `cd <directory>` (`cd ..` to go up a directory)

cls: Clears the screen.

echo: Displays messages, or turns command echoing on or off.
Usage: `echo` or `echo <text>`

exit: Quits the CMD.EXE program (command interpreter).

Manipulating files and directories

md: Creates a directory.
Usage: `md <directory>`

rd: Removes a directory.
Usage: `rd <directory>`

del: Deletes one or more files.
Usage: `del <filename> [<filename2> ...]`

copy: Copies one or more files to another location.
Usage: `copy <source> <destination>`

move: Moves one or more files from one directory to another directory.
Usage: `move <source> <destination>`

ren: Renames a file or files.
Usage: `ren <old name> <new name>`

Working with files

type: Displays the contents of a text file.
Usage: `type <filename>`

more: Displays output one screen at a time.
Usage: `more <filename>`

fc: Compares to files or sets of files, and displays the differences between them.
Usage: `fc <filename1> <filename2>`

>: Direct output into a file, overwriting if the file exists.
Example: `echo Hello! > hello.txt`

>>: Direct output into a file, appending if the file exists.
Example: `echo Hello again! >> hello.txt`

sort: Sorts input.
Usage: `sort [/R] <filename>`

Working with the Operating System

systeminfo: Displays machine specific properties and configuration.

tasklist: Displays all currently running tasks including services.

taskkill: Kill or stop a running process or application.
Examples: `taskkill /im calc.exe`
`taskkill /PID` <*process ID*>

set: Displays, sets, or removes Windows environment variables.

date: Displays or sets the date.

time: Displays or sets the system time.

find: Searches for a text string in a file or files.
Example: `find "hello" *.txt`

path: Displays or sets a search path for executable files.

Notes

- The Windows command prompt is generally case insensitive (`type hello.txt` is the same as `TYPE HeLlo.TXT`).
- You can reference a file in the current directory (`file.txt`), another directory (`\Users\bob\Documents\file.txt`), or another drive (`D:\Backups\file.txt`).
- You don't need to `cd` to another drive, just type the drive letter, a colon (:), and hit enter (e.g., "`d:`").

Windows PowerShell Essentials Cheat Sheet

Notes

- PowerShell commands, known as Cmdlets, are typically in "Verb-Noun" form, such as `Get-Content`.
- Most commands have shorter aliases. For instance, the aliases for `Get-Content` are `gc`, `type` (to mimic the CMD version), and `cat` (to mimic Linux environments).
- Commands can be chained as pipelines using the "`|`" (vertical bar) symbol. For example: `Get-Process | Format-List | Out-File ps.txt`

Getting around PowerShell

Get-Help (help): Get help with PowerShell or a Cmdlet
Usage: `get-help` or `help <cmdlet>`

Get-Command (gcm): Get a list of all available commands
Usage: `gcm` or `gcm -module <module>`

Get-Item (gi): Gets items, such as the files in the current directory
Example: `gi *`

Get-ChildItem (gci,dir,ls): Gets child items, such as the files in subdirectories
Example: `gci -recurse`

Get-Process (gps,ps): Get a list of running processes

Copy-Item (cpi,cp,copy): Copies an item from one location to another

Get-ComputerInfo (gin): Gets system and operating system properties

Move-Item (mi,mv,move): Moves an item from one location to another

New-Item (ni): Creates a new item, such as an empty file
Usage: `ni empty.txt`

Remove-Item (ri,rm,rmdir,del,erase,rd): Deletes the specified items

Rename-Item (rni,ren): Renames an item

Set-Location (sl,cd,chdir): Sets the current working location

Set-Content (sc): Writes new content or replaces existing content in a file
Example: `sc -path .\hello.txt -value 'Hello world!'`

Add-Content (ac): Adds content to an item, such as adding words to a file
Example: `gi hello.txt | ac -value 'Hello again!'`

Out-File: Sends output to a file
Example: `'This is a string' | out-file test.txt`

Scripting in PowerShell

Variables: `$variable_name = <value>`
Examples: `$s = "hello"` or `$a, $b = 0, 1`

Object Members: `$Object.Member`
Examples: `$date = Get-Date; echo $date.day; (Get-Date).month`

Comparison: `-eq, -ne, -gt, -ge, -lt, -le`
Examples: `5 -eq 5, 3 -le 6`

Logic: `-and, -or, -not`
Examples: `5 -eq 5 -and 3 -le 6, -not (5 -eq 4)`

Arrays: `$letters = "a", "b", "c"; $numbers = 1..5`

Membership: `-contains, -notcontains, -in, notin`
Examples: `1..5 -contains 3, -not ("c" -in "a", "b")`

Flow Control: `If(){} Elseif(){} Else {}`
Example: `If($n -eq 3){"Fizz"} Else {"Buzz"}`

While Loop: `While($n -lt 100){$n+=1; echo $n}`

For Loop: `For($i=0; $i -lt 10; $i++){echo $i}`

ForEach: `ForEach($file in dir){$file.name}`

Write-Host: Outputs to screen.
Example: `Write-Host "Hello!"`

Read-Host: Reads input.
Example: `$number = Read-Host "Input a number"`

Format-Table: Formats as a table.
Example: `Get-Date | Format-Table`

Format-List: Formats as a list.
Example: `Get-Process | Format-List`

Linux Command Line (Bash) Cheat Sheet

Notes

- Options for commands are usually proceeded by "-" (for single letter options) or "--" (for longer option names). E.g.: `ls -d` or `ls --directory`
- Commands can be chained as pipelines using the "|" (vertical bar) symbol. E.g.: `echo Hello world | sed 's/world/World!/g' | tee hello_world.txt`

Getting around in the Command Line

help: View shell help or help for a command.
Usage: `help` or `help <command>`

pwd: Show full path of current directory.

ls: List contents of a directory.
Examples: `ls` or `ls -ahl /home/user/Documents`

cd: Change to home or specified directory.
Usage: `cd` (goes home) `cd ..` (goes up a directory) `cd <directory>`

echo: Output string.
Usage: `echo "<string>"`

man: View the manual (man page) for a command.
Usage: `man <command>` (Scroll with arrows or PgUp/PgDn, use "q" to quit)

clear: Clears the screen.

exit: Exit the command line shell.

Working with the Operating System

date: Show system date and time.

env: Show environment variables and their values.

ps: Show running processes.
Usage: `ps` or `ps aux` (show all processes for all users)

top: Show updating list of running processes and resources.
Usage: `top` ("q" to quit)

kill: Kill a process by process ID (PID).
Usage: `kill <pid>` or `kill -9 <pid>` (terminate with KILL signal)

pkill: Kill a process by name.
Usage: `pkill <process name>`

Working with files

mkdir: Create directory.
Usage: `mkdir <directory>`

rmdir: Remove empty directory.
Usage: `rmdir <directory>`

touch: Create empty file (does not overwrite existing file).
Usage: `touch <filename>`

cat: Print file(s) to screen.
Usage: `cat <filename> [<filename2> ...]`

cp: Copy file.
Usage: `cp [-r] <source> <destination>` (`-r`: recursive)

mv: Move file or directory.
Usage: `mv <source> <destination>`

rm: Delete file(s).
Usage: `rm <filename>` or `rm -r <directory>` (be careful with this)

head/tail: Print the beginning (or end) of a file to screen.
Usage: `head [-n <number of lines>] <filename>`

less: View file in paginated form.
Usage: `less <filename>`

>: Redirect output to file (overwriting existing file).
Example: `echo "Hello!" > hello.txt`

>>: Append output to file.
Example: `echo "Hello again!" >> hello.txt`

find: Find files in a directory.
Examples: `find . -name test.txt` or `find / -user bob`

grep: Search a file or stream for a pattern.
Usage: `grep <pattern> <filename>` or `<command> | grep <pattern>`

Command Line Networking Cheat Sheet

Networking on Windows Command Line

ping: Test network connection to an address.
Usage: `ping <address>`

tracert: Trace route to an address.
Usage: `tracert <address>`

netstat: View active connections and listening ports.
Usage: `netstat -ab` to view connections, listening ports, and processes
`netstat -e` for statistics, `netstat -r` for routing table

arp: View Address Resolution Protocol information.
Usage: `arp -a` or `arp -N <interface>` or `arp -a <remote address>`

hostname: Prints the name of the current host.

ipconfig: View and modify IP configuration details.
Usage: `ipconfig /all`

nslookup: Use DNS to resolve an address.
Usage: `nslookup <address>`

route: View or configure IP routing table.
Usage: `route PRINT` (See `route /?` for other uses)

Networking on Linux Command Line

ping: Test network connection to an address.
Usage: `ping <address>`

traceroute: Trace route to an address.
Usage: `traceroute <address>`

ip: Show and manipulate routing, network devices, interfaces and tunnels.
Examples: `ip addr`, `ip link`, or `ip route` (See `ip --help`)

ss: Utility to investigate socket usage.
Usage: `ss -atu`

arp: View Address Resolution Protocol information.
Usage: `arp -e` or `arp -i <interface>`

hostname: Prints the name of the current host.

nslookup: Use DNS to resolve an address.
Usage: `nslookup <address>`

Common Ports

TCP 20-21: File Transfer Protocol (FTP)

TCP 22: Secure Shell (SSH)

TCP 23: Telnet

TCP 25: Simple Mail Transfer Protocol (SMTP)

TCP/UDP 53: Domain Name System (DNS)

UDP 67-68: Dynamic Host Configuration Protocol (DHCP)

UDP 69: Trivial File Transfer Protocol (TFTP)

TCP 80: Hypertext Transfer Protocol (HTTP) Note: HTTP/3 can use UDP

UDP 88: Kerberos authentication

TCP 110: Post Office Protocol (POP)

UDP 123: Network Time Protocol (NTP)

TCP/UDP 137-139: NetBIOS

TCP 143: Internet Message Access Protocol (IMAP)

TCP/UDP 161-162: Simple Network Management Protocol (SNMP)

TCP 179: Border Gateway Protocol (BGP)

TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)

TCP 443: HTTP over SSL/TLS (HTTPS)

TCP/UDP 636: LDAP over SSL/TLS (LDAPS)

TCP 989-990: FTP over SSL/TLS (FTPS)

TCP 3389: Remote Desktop Protocol (RDP)

Useful Networking Utilities

nmap: Network exploration and security scanner.

tcpdump: Command line packet capture and analysis.

nc/ncat/netcat: Send and receive arbitrary data.