CYBRARY

Command Line Basics

Created By: Suketh Evani, Teaching Assistant

Module 1: Introduction to the Command Line

Lesson 1.1: Introduction and setup
Skills: command line, tools, setup

- Scope
  - Setting up of environment
  - Linux command line tools
  - Windows command line tools
- Modules
  - Introduction to command line
  - Command line tools
  - Saving time by using these tools
- About the instructor
  - Cristopher Haller
  - 8 years of industry experience
  - CISSP, CASP, GNFA, GERM. GCFA and more
  - Eight years with the US Navy
  - Four years as sysadmin, four years in Computer Incident Response
  - Loves golfing
- Course Goals
  - How to open the command line.
  - How to ask for help at the terminal.
  - Understand how to navigate the file system with CLI.
  - Use common CLI tools to perform time-saving tasks.
  - Chain together commands
- Prerequisites
  - Basic Computer Skills
  - Access to terminal of both windows and linux
  - Good attitude to learn

- Supplementary material
  - Virtual Box or Vmware free Software https://www.virtualbox.org/wiki/Downloads
  - Linux OS https://linuxmint.com/download.php
  - SANS 572Cheat sheets
  - Extra material at resources
- Target Audience.
  - Why do this course
  - Command line hosts very powerful tools
  - Tired of repetitive functions
  - What can you expect
  - Comfort executing commands without a GUI
  - Increased employer value
- Course structure
  - Slides
  - Live demonstrations
  - Online labs
- Pre-Assessment

  Which linux command allows you to read the contents of a file?

  A) Read
  B) Grep
  C) More
  D) Text

  Answer : B) grep

Lesson 1.2: Opening the command line
Skills: CLI, GUI , access CLI

- Learning Objectives
  - Learn why the CLI is important
  - Identify differences between the GUI and CLI
  - Open the command line on Windows

    - Open the terminal on Linux
- Pre-Assessment

  What advantages does the CLI provide over GUI

  A)The CLI makes a user appear as an elite hacker
  B)The CLI allows you to click on new interactions
  C)Pictures and videos look better at the CLI
  D)Actions at the CLI can be easily replicated

  Answer: D)Actions at the CLI can be easily replicated

- Why is the CLI Important ?
    - First way to interact with computers
    - Gives robust control up to the kernel level
    - Many advanced tools do not have a GUI
    - Automate boring tasks
    - Increase your value to employer
- GUI vs CLI
    - Graphical User Interface (GUI)
    - Easy to understand
    - Visual indicators
    - Command Line Interface (CLI)
    - Difficult entry barrier
    - Scrolling text, no pictures
- Opening the Command Prompt on Windows
    - Click ***start*** and type ***cmd***
    - Windows Key + R
    - **t**ype ***cmd***
    - Right click the Windows icon
    - Click ***Windows PowerShell***
- Opening the Terminal on Linux
    - Click the Terminal Icon
    - Some Linux distributions are CLI only

- Post-Assessment

  What is the best way to open the command line?

  A) Clicking the Terminal icon
  B) Using the Windows Run prompt
  C) Opening PowerShell
  D) All of the above, each method is equally effective

  Answer: D) All the above

Lesson 1.3: Asking For help
Skills: help, man commands, switches.

- Objectives
  - Understanding why asking for help is important
  - Learn how to ask for help at the CLI
  - Understand help switches
  - Learn about Linux man pages
- Pre-Assessment

  The linux manual pages can be accessed with which command?

  A) Manual
  B) man
  C) get manual
  D) linux man get

  Answer: B) man

- Why ask for help
  - Every computer professional asks for help
  - No one remembers all the commands that exists on the command line
  - Learn to interpret the help prompt
  - You may learn new tricks and techniques.
- How to ask for Help

    - Type help in the command line and hit help. The result of this command will be all the actions you can do in the command line
    - Similar process in linux environment. Enter the help command in the command line to view all the options available
- Help from each command
    - Syntax: <command><switch><parameters>
    - For windows environment use /help or /?
    - For linux environment use the -?, -h or -help
    - Note: for using words in switches, use "--"
- Linux
    - Try: grep --help command for more info
    - Ex: pwd --help
- Windows
    - Ex:tree /? displays(switches and parameters)
- Linux man pages.
    - Man pages are similar to help but give more information
    - Grep stands for GUI representatoin and will be used a lot.
    - Check linux course in cybrary to understand linux file hierarchy
    - Ex: man grep shows all the switches/ scrolling and extra into , press "q" to quit
    - Usr/share/man
- Post-Assessment

  What is the general format for commands?

  A) <parameters><switch>
  B) <command><switch><parameters>
  C) <switch><parameters>

  Answer: B) <command><switch><parameters>

Module 2 : Introductory Commands

Lesson 2.1: Command line survival part 1

Skills: Linux command line interface , hot keys, history.

- Objectives
  - Learn auto-complete techniques
  - Learn how the arrow keys are utilized at the CLI
  - Understand how to view command history
- Pre-Assessment

  What is the best way to resubmit a previously entered command?

  A) Press the control key+H
  B) Open the bash history of the file and copy/paste
  C) Use the up-arrow key
  D) Press the control key+Z

  Answer: C) Use the up-arrow

- Typing commands
  - Always try to understand what you want ta accomplish by entering that particular command.
  - General syntax for a command: <command> -[switch] parameter
  - Ex: grep - frankenstein . This command tries to search a file with the name “frankenstein”, -i is for case sensitive I.e Doesnt matter if the caps are on or off
  - Important commands that you must know
    - Pwd - shows the current directory you are working in
    - Dir/ls - lists all the files in the pwd
    - Cd - used for directory traversal.
- Use the TAB key to auto complete a command. If more than a match it will display all the commands hat match the entry.

  Ex: ls in linux with <filename>, sudo command su(auto)

- Arrow keys at the CLI
  - Up to scroll to previous and down for next
- Command history

    - Windows environment;
    - Use the F7 or doskey/history NOTE windows by default does not have any persistent history
- Linux:
    - ~/.bash_history file stores the history. Use cat command to view the contents of the file.
    - Syntax: cat ~/.bash_history
- Post-Assessment :

  Which command tells you what directory you are in?

  A) pwd
  B) folder
  C) cat
  D) echo

  Answer: A) pwd

Lesson 2.2 : Command line survival part 2
Skills: CLI Tools, clear screen, customize CLI

- Learning Objectives
    - Customize the CLI environment
    - Understand various control functions
    - Learn how to clear the screen
- Pre-Assessment

  You enter a command, and your screen freezes.What do you do?

  A) ctr+C
  B) Hold down Enter
  C) ctrl+ Tab
  D) Just let it finish

  Answer: A) ctrl+C

- Customize the CLI Environment
    - What can be changed. Screen size, Colors, Text
    - In linux environment - Edit and preferences
    - In windows cmd - Click on properties on the left corner to bring down the properties window to view the settings that can be changed
    - Ex: In Windows Changing size/ font / colors . Linux - edit>preferences same.
- Control keys
    - While a process is running, press ctrl+C to interrupt the process and gain control over terminal
    - Use Ctrl+Z to pause a running process. Linux has an additional feature of continuing the process by entering the fg command in the terminal.
    - Use Ctrl+L to clear the current screen display
    - Demonstration. Note the process number when you pause a command using ctrl+Z to use the fg command with syntax fg <session no.> if you want to bring back that session.
    - Use the cls command in command prompt to clear screen. Similar to functionality as ctrl+L in linux
- Post-Assessment

  What command restarts a paused command?

  A) Restart
  B) Fg
  C) Front
  D) Unpause

  Answer: B) fg

Lesson 2.3: Changing directories
Skills : directory traversal, mkdir command, switches

- Learning objective
    - Learn how to change directories
    - Understand how to change drives

    - Use the tree command
    - Make new directories
- Pre-Assessment question
    - What command can be used to make new directories?
        A) Newdir
        B) Makedirectory
        C) Mkdir
        D) Dir --new

        Answer: C) mkdir

- Change directory
    - Use cd command to change directories. Syntax: cd <directory name>
    - Cd .. goes up a directory
    - Cd/d [drive] will change the drive you are using
    - Note linux has a single root directory.
    - Demonstration : windows : cd Desktop (not case sensitive)

        Used cd .. to go back to Desktop directory.
        Using cd ..\.. to go back two folders
        Use cd/d D:\ to change to D drive

- Use the tree command to graphically display folder and file structures. CLI is also graphical in nature.
- Use tree /f to show the complete strucutre of the files.
- Ex: pipe tree command with other params like more
- Make directories
    - In linux environment use mkdir command along with the directory name to create a directory. Syntax: mkdir <new dir name>
    - In windows use md in the similar fashion

- Post-Assessment

What is the tree command used for?

A) Create new folders
B) Read files
C) Searches through files
D) Graphically displays folder structure.

Answer: D) Graphically displays folder

Lesson 2.4: Common linux tools
Skills : read, copy, delete, search

- Learning Objectives:
  - Learn how to read files
  - Learn how to copy files
  - Understand how to delete files
  - Understand how to search through files
- Pre-Assessment

  Which command is the best to search through strings?

  A) strings
  B) text
  C) grep
  D) ngrep

  Answer C) grep regular expression tool\

- Read a text file
  - The **cat** (concatenate) command is used to display the contents of a file. Can work with 1 or more files at the same time to display the contents of all the files continuously.
  - **More** command is used to display the only single text files.
  - **Less** command allows you to scroll up and down through the terminal of contents which makes it slightly effective than the more command.

- Example: using cat to display content-syntax to concat two files, using more command and less command along with benefits.
- NOTE: Use enter to move down one line and space to move down a complete page

- Copy/Move files
  - To copy a file in the linux environment use the **cp** command.
  - Use the **mv** command to move files from one directory to another. This command can also be used to rename files.
  - Example: using the cp <file name> <destination directory> to cp a file to the given directory

  Using mv <file name> <directory name> to move a file to the given directory.
  Using mv <old file name> <new file name> command to change the file name from the old file name to the given new file name.

- Delete files
  - Use the **rm** command to delete files.
  - Some important switches -r fro recursive and -f to force . The force switch will stop the system from giving prompts
  - Syntax : rm <file name>
- grep command:
  - A very powerful linux tool used to search for strings. It is a pattern based search and can be efficiently used when piped with other commands.
  - Syntax : grep <string to find> <file to search in>
- Post - Assessment :

  Is it possible to concatenate multiple files ?

  A) No, only one file at a time.
  B) Yes, but only two files.
  C) No, you need to use the more command.
  D) Yes, there is no limit to the amount of files.

Answer: D) Yes, there is no limit

Lesson 2.5: Windows common tools
Skills: read, copy, delete, search

- Objectives
  - Learn how to read files
  - Learn how to copy files
  - Understand how to delete files
  - Understand how to search through files.
- Pre-Assessment

  Moving a file is a way to rename it?

  A) True
  B) False

  Answer: B) False

- Reading text files
  - The **type** command is used to display the contents of a file in a windows environment.
  - The **more** command is used to display the file one screen at a time similar to that of linux.
  - Demonstration <syntax is similar to that of linux>
- Copying files
  - The **copy** command is used in windows to copy files from one location to another
  - The **move** command is used to move files/folders from one location another in windows.
  - THere a an explicit command in the windows to rename files called **rename.**
- Deleting files
  - The **del** and **erase** command essentially have the same purpose of deleting files or directories in windows.
  - The **/s** switch can be used with the del command to delete sub-directories.
  - Demonstration: Using copy <source file> <destination file> command

  Using the del <file name> command to delete files.

- Searching through files
    - Find command is used to search for strings in a file
    - Findstr is a more robust command for searching strings in a file as it uses regular expressions ot identify patterns.
    - Ex: using find “<string to find>” <file to search>
- Post - Assessment

  Which command can be used to read text on windows?

  A) more
  B) less
  C) text
  D) type

  Answer: A,D both type and more can be used.

Lesson 2.6: Copy and paste in windows
Skills: select, copy, paste commands

- Learning objectives
    - How to select text on the cmd line
    - How to copy selection from the cmd
    - How to paste into the cmd line
- Pre - Assessment:

  The ctrl+C and ctrl+V keys work to copy and paste in the command line

  A) True
  B) False

  Answer: False

- Selection/Copy/Paste

- To make a selection click on top left> click on edit > select the the mark option> make the required selection > press enter
- Another option is to right click and select edit from the drop down menu.
- The selection made is stored in the clipboard/text editor temporarily.
- Paste the selected option by using the ctrl+V hot key or right click to select paste from the drop down. You can paste in any program that you want to.

- Post-Assessment

  Copying and Pasting information is effective in the command line ?

  A) True
  B) False

  Answer: A) True

Module 3: Linux Command Line tools

Lesson 3.1: Linux Basics Part 1
Skills: ls, cd , pwd commands

- Learn Objectives
  - Learn the **ls** command
  - Learn the **cd** command
  - Learn what **pwd** does
- Pre-Assessment

  Which **linux** command displays a directory's contents?

  A) dir
  B) ls
  C) content
  D) Cat

  Answer: B) ls

- **ls** command

    - The **ls** command is used to list all the contents of a directory
    - Important switches used
        - **ls -l** lists all the contents of a directory along with its permission and dates
        - **ls -a** shows all the content including hidden files and folders in a directory. Hidden files in linux start with a dot ex: .bash_hisotry, .profile
- Demonstration of difference between hidden and non hidden using commands.
- **cd** command
    - Cd sands for change directory and as its name suggests it is used to change the current working directory. It is used for directory traversal/ file travelling
    - Using cd .. as shortcuts to traverse on directory up instead of giving the full command
- **pwd** command
    - The pwd command which stands for print working directory is used to display the current working directory.
    - The root directory represented by "/" is the starting directory in linux .
    - Ex: interpreting the pwd command result:

      /home/user/Desktop - stands for root>home>user>Desktop

- Post-Assessment

  Which ls switch displays hidden files?

  A) -a
  B) -l
  C) -h
  D) --hidden

  Answer: A) -a

Lesson 3.2: Linux basics Part -2
Skills: cat, more, less, clear commands

- Learning objectives
    - Learn the cat command

- Learn the more command
- Understand the less command
- Clear the screen with clear command

- Pre-assessment

  Which command allows you to scroll up and down text?

  A) more
  B) cat
  C) less
  D) text

  Answer: C) less

- cat command
  - Cat command which stands for Concatenate is used to display the content of a file.
  - It can also be used to combine files which can vary from two to any number of files at once.
  - Ex: Using the cat <file 1> <file 2> .. command to display the contents of the respective files sat once.
  - Short coming in cat: Tough to view contents of a huge file.
- more command
  - It is used to display contents of a file on the screen one at a time.
  - Allows user to read through content at their own pace with different scrolling options
  - Use enter key to scroll down one line and space key to scroll down a page
  - Enter q key to exit the file
  - Shortcoming: cannot scroll up.

- less command
  - The less command is similar in functionality to more but has additional features.
  - less command supports scrolling up of the content displayed in a file.

    - Ex: Use the up and down arrows to scroll up and down respectively. Use q to exit.
- Clear command
    - The clear screen is used to remove all the content displayed on the screen and displayed a blank terminal .
    - This is used to refresh the CLI. Use the ctrl+L hotkey to refresh the screen
    - Although this won't refresh the history of commands and you can still press up and down arrows to scroll between previously used commands.
- Post-Assessment

  How many files can cat combine at once?

  A) Only one
  B) Two
  C) Three
  D) No limit!

  Answer: D) No limit!

Lesson 3.3: Linux Basics Part 3
Skills: CLI commands, file commands, sudo command

- Learning Objectives
    - Learn the locate command
    - Learn the nano command
    - Understand the sudo command
- Pre-Assessment

  By default , which user account does the sudo use?

  A) Administrator
  B) Guest
  C) System
  D) Root

Answer: D) root

- locate command
  - The locate command helps us find file in the linux file system.
  - It is very efficient and fast as it uses indexing databases. These databases are created constantly as you use the system.
  - Syntax: locate [file name or part of it] , gives the list of results that match the string entered. The output is the location of the file.
  - Use the updatedb command to update the indexed database manually.
  - Example: locate
  - Drawback: It might nit find files which are new and not indexed in the DB, gives no output.
  - The update DB requires sudo permission.
- nano command
  - Nano is a basic text editor application that comes with linux and can be used to create and edit files.
  - Syntax: nano <file name>, opens an existing file or creates a new file if not.
  - User friendly text editor and quite similar to vim.
  - Ex: Open a word.txt file using nano , scrolling using arrow keys . Make changes and use the ctrl+o from the many options available to save the changes. Use ctrl+x to exit.
- sudo
  - Sudo is one of the most important commands in linux which allows us to temporarily run a file as root user or any other user.
  - The root user us the user account in linux with highest privileges I.e. anything and everything can be done if you are using root account.
  - Ex: using sudo updatedb command to update the index database of the system. It will prompt you for the root account password .
  - Note: sudo -s commands opens the root user interactive shell
- Post-Assessment:

  The nano command will make a new file if one does not exist?

  A) True

B) False

Answer A) true

Lesson 3.4: Linux files part 1
Skills: file commands, cp files, move files, remove files

- Learning Objectives
  - Learn the cp
  - Learn what mv does
  - Understand what the rm command does
- Pre-Assessment

  The rm command won't delete important system files

  A) True
  B) False

  Answer: False

- cp command
  - The cp command which stands for copy is used to copy a file to a new location.
  - Syntax: cp <old file> <new file>.
  - Use the -R switch for recursive copy in folders.
- mv command
  - It is used to move files to another location.
  - Syntax: mv <old file> <new file>
  - The main difference between the mv and cp command is that the former doesn't leave a copy of that file.
  - It can also be used to rename the file names.
  - Syntax mv <old file name> <new file name>.
- rm command
  - Use the rm command to remove/delete the files
  - Syntax: rm [file].

    - Be very careful with this command as it deletes the files even if they are operating system related files.
    - Use the -r switch for recursive delete and -f for force delete. Be very sure while using the -f switch.
- Post - Assessment

  Which command can also be used to rename files?

  A) cp
  B) mv
  C) sudo
  D) rm

  Answer: B) mv

Lesson 3.5: Linux Files Part 2
Skills: create file, file permissions

- Learning Objectives
    - Learn the touch command
    - Understand the chmod command
    - Understand the chown command.
- Pre- Assessment

  You need to execute a file, but lack the permissions. Which cmod switch allows you to execute files?

  A) +w
  B) -w
  C) +x
  D) -x

  Answer) C) +x

- Touch command

    - The touch command can be used to update the time modified.* This will help to update the last modified timestamp of a file*
    - It can also be used to create files.
    - Syntax : touch <file_name > will create a file with the given file name.
- Linux file permissions
    - There are 3 types of file permissions for linux files
        - R for read
        - W for write
        - X for executable.
- The convention to represent file permission for User , Group and other is represented as a string of 10 digits. The first digit represents the file type (types). The next three represent the users permission. The next three consecutive digit represents the permissions for the group and the last three bits are for Other user permissions
- chmod command
    - The chmod command stands for change file mode and is used to change the mode bits of a file which alter the file permissions
    - Syntax: chmod [permissions] [file]
    - You can use either the alphabets or bits to assign permissions
    - Only the owner of the file or root(use sudo) can change the file permissions.
- chown command:
    - This command is used to change the ownership of a file.
    - Syntax : chown root [file] . Use chown root:group [file]
    - To run the chown command you mat need root access (use sudo).
- Post-Assessment
    - Which can be used to create files?

    A) chown
    B) chmod
    C) touch
    D) rm

    Answer: C) touch

Lesson 3.6: Linux files part 3
Skills: find , grep commands, piping commands

- Learning objectives
    - Learn the find command
    - Learn the grep command
    - Understand how to pipe into grep
- Pre-Assessment

  What is true about the grep command?

  A) Can't search case-sensitive
  B) Can be used to search in binary files
  C) Cannot use regular expression

  Answer: B) can be used to search binary files

- find command
    - It is used to find files in a linux file system and is quite similar to locate command. This command doesnt use indexed database.
    - It searches all the directories in the system and hence may take longer but gives real-time outputs of the file locations. It is more robust and reliable
    - Syntax: find - name [file name]
    - Using the find / -name <file name> to search for the file from the root directory with the given file name.
- grep command
    - Very effective in searching through and find files and folders.
    - It uses pattern based searching and is used extensively.
    - Syntax: grep <switch> [search] [directory]
    - Can be used effectively with other commands.
- piping the grep command
    - The grep command is piped with other commands to search through the output obtained from that command.
    - Syntax : cat [file] | grep -I [string] is used to search and display the given string the file and -I switch is used to make the search case insensitive.
    - Use less piped with grep

- Post-Assessment:

  Which switch is used to search through binary files?

  A) -a
  B) -b
  C) -c
  D) --binary

  Answer : A) -a

Lesson 3.7: Linux Files Part 4
Skills: sort, uniq , sed

- Learning Objectives
  - Learn the sort command
  - Learn the uniq command
  - Understand the sed command
- Pre-Assessment :

  What can sed be used for ?

  A) Make changes to files
  B) Move files to new directory
  C) Edit a stream of text
  D) Search through files

  Answer: C) Edit a stream of texts

- sort command
  - The sort command is used to sort the file / standard inputs
  - It is very useful to organize text
  - It can be effectively used with other commands

    - Syntax: cat <filname> | sort is used to sort the words of the file in alphabetical order.
- uniq command
    - Used to remove redundant results
    - Generally used with the the sort command is get better results as the results are processed in order.
    - The -c switch is used to count the number of words.
- sed command
    - Stands for stream editor
        - Make changes to stream of texts
        - Search and replace text
        - Ex: s/old/new/g interpret as string/<search for string>/<replace with>/replace all strings found.
- Post-Assessment

  Which uniq switch counts the number of hits for an entry?

  A) -c
  B) --number
  C) -a
  D) --uniq

  Answer : A) -c

Lesson 3.8: Linux files Part 5
Skills : hashing , encoding , algorithms

- Learning objectives
    - Refresh on hashes and encoding
    - Understand the base 64 command
    - Learn the md5sum command
    - Learn the sha1 command
- Pre-Assessment

Once a file is encoded with base64, it cannot be read?

A) True
B) False

Answer B) False

- Hashing and encoding
  - Encoding converts plaintext to a different non-readable format which can be easily reversed/read using an interpreter.
  - Hashing is a one way algorithm which cannot be reversed to get the plain text hence is used to validate the integrity of a file/data.
  - Various algorithms for hashing
- base64 command
  - Used to convert standard input or output to base64 format
  - Encodes plaintext to non-human readable format
  - General applications : file transfers, emails
  - Used to hide malicious code by converting into a base64 format making it unidentifiable
  - Syntax: [stdin] | base64 , use the -d switch to decode a base64 message
- md5sum command
  - The md5sum command is used to generate a hash of an stdinput/file using the md5 algorithm.
  - Syntax : md5sum [file]
- sha1sum
  - It is very similar to the md5sum command but uses the sha1 algorithm to generate the hash of a stdin/file .
  - Syntax : sha1sum -[file]
- Post-Assessment

  Hashes can be reversed to read the encrypted message?

  A) True.
  B) False.

Answer: B) False

Lesson 3.9: Linux systems Part 1
Skills: sudo, apt-get , whoami, uname

- Learning Objective:
  - Learn the sudo command
  - Learn the apt-get command
  - Understand the whoami command
  - Understand the uname command.
- Pre-Assessment

  Using the sudo command allows users to run programs as root?

  A) True
  B) False

  Answer: True

- sudo command
  - Using sudo allows you to run any command with root privilege.(similar to running an application as admin in windows)
  - It is used from normal user account to temporarily run command as root users.
  - Prevents the mis-use of root privileges
  - Syntax: sudo [command]
- apt-get command
  - This command allows the user to install packages in linux that do not come pre-installed.
  - Use apt list [search] /apt search[search] to list available packages
  - Usually needs root permission (use sudo).
- whoami command
  - Used to display the current user account logged into.
  - Useful when remote ssh connections are made to find out the user logged into.
- uname command
  - Used to display the linux system properties.

    - se -a switch to view all the information which can be used to find vulnerabilities.
- Post-assessment:

  Which command would search through available packages for a terminal program?

  A) apt-get terminal
  B) sudo apt-get terminal
  C) apt list terminal
  D) apt --list terminal

  Answer: C) apt list terminal

Lesson 3.10: Linux Systems Part 2
Skills: CLI commands, process commands , kill process

- Learning objectives
    - Learn the id command
    - Understand the last command
    - Learn the ps command
    - Learn the kill command
- Pre - assessment

  The ps command lists all the running processes by default?

  A) True
  B) False

  Answer: False

- id command
    - Id [user]
    - Used to print user and group info
    - Can show permissions for other users
- last command

    - Shows the users that last logged in
    - Shows what they used to log in as well
- ps command
    - Used to display running processes
    - Displays only current user process by default
    - Ps aux displays all processes on system
- Kill command
    - Ends a running process
    - Uses the pid of a process
- Post-Assessment

  The kill command can be used to end other user processes.

  A) True
  B) False

  Answer: True

Lesson 3.11: Linux Networking
Skills: network commands, lsof, switches

- Learning Objectives
    - Learn the ifconfig command
    - Learn the netstat command
    - Learn the lsof command
- Pre-Assessment

  Which command is the best way to find your IP address?

  A) Netstat
  B) Ndstat
  C) Lsof
  D) Ifconfig

  Answer: D) ifconfig

- ifconfig command
    - This command shows network configuration for all the current network interfaces
    - Syntax: ifconfig . You can use specific interface name.
    - Use ifconfig <interface> add <ip address> to set ipaddress to an interface.
    - Use ifconfig interface down to disable an interface. Use “up” to enable the interface
- netstat command
    - This command shows information about linux networking and all the open connections.
    - Use the -r switch to show routing table.
    - Used to identify any unwanted connection or malware.
- lsof command
    - Stands for list open files and is used to show all current files open
    - Files may relate to system usage also.
- Post - Assessment

  The ifconfig command cannot be used to change your IP

  A) True
  B) False

  Answer: B) False

Lesson 3.12: Linux Networking 2
Skills: telnet, ssh, netcat commands

- Learning Objectives
    - Learn the telnet command
    - Learn the ssh command
    - Learn the nc command
- Pre-Assessment

  Which command provides encryption by default?

A) nc
B) ssh
C) telnet

Answer: B) ssh

- telnet command
  - Is used to connect to another device's terminal remotely.
  - It is not widely used as it doesnt use encryption and sends all the communication in clear text.
  - Syntax: telnet <ipaddress> connects to the given ip address using telnet.
- ssh command
  - Stands for secure shell and has the same functionality as telnet.
  - It is secure as it uses certificate based encryption and doesn't send its messages in plain text.
  - Syntax: ssh <username>@<ip address>
- nc command
  - It is a versatile and simple to use network protocol to make quick and easy connections.
  - It is generally used in malwares to make connections to the target systems.
  - Use the nc -lp <port> to open and listen on the given port.
- Post-Assessment

  Is it not alarming to find nc.exe listening for connections on port 4444.

  A) True
  B) False

  Answer: False

Module 4 : Windows command line tools

Lesson 4.1: Windows Basics
Skills: windows cmd, cls commands , directory traversal

- Learning objectives

    - Refresh the dir and cd command
    - Learn the type command
    - Clear the screen with cls
- Pre-Assessment

  Which command is used to read a text file on Windows?

  A) cat
  B) find
  C) dir
  D) type

  Answer: D) type

- Dir and cd command
    - Similar in functionality to the linux ls and cd command.
    - Use **cd/d** to change drives.
    - Syntax:
    - Note: windows is not case sensitive
- type command
    - Use the type command to read the contents of a text file
    - Syntax: type <filename>
    - Pipe it with the more command to scroll through large files.
- cls command
    - Stands for clear screen and used to remove all the content on the terminal screen
    - Similar to clear command in linux

- Post-Assessment

  Which cd switch is used to change a drive?

  A) /drive

B) /a
C) /z
D) /d

Answer: D) /d

Lesson 4.2: Windows Files Part 1
Skills: Window cmd, icacls command, echo commands

- Learning Objectives
  - Learn the echo command
  - Learn the icacls command
  - Understand the fc command
- Pre-Assessment

  The icacls command is used to change file permissions

  A) True
  B) False

  Answer: A) true

- echo command
  - Used to return the information to the command prompt.
  - Very effective when combined with environment variables.
  - Syntax: echo [env. Var.]
- icacls command
  - Stands for Integrity Control Access Control Lists and used to change file permissions
  - It can be used to add or remove file inheritance.
  - Syntax: icacls <file> / grant <user>:<permissions>
- fc command
  - Stands for File Compare and is used to compare two files to identify differences bw them.
  - Syntax: fc <file1> <file2>

    - The output is the different string in both the files
- Post-Assessment

  Which command displays messages to the prompt?

  A) icacls
  B) echo
  C) cat
  D) fc

  Answer: B) echo

Lesson 4.3: Windows Files Part 2
Skills: copy, robocopy, xcopy commands

- Learning Objectives
    - Refresh on copy and move.
    - Learn the robocopy command.
    - Learn the xcopy command.
- Pre Assessment

  What is an advantage to use robocopy instead of copy?

  A) robocopy can copy only changed files
  B) robocopy can copy on local systems only
  C) copy offers login
  D) copy can mirror remote folder structures.

  Answer: A)robocopy can copy only changed files

- Copy and move command
    - The copy command is used to create a copy of the file in another location. Two copies of the same file exist

    - Move has the same functionality but it removes the older copy and can also be used to rename files.
- xcpoy command
    - Used to copy files and directories
    - It faster and more robust due to its increased buffer size and hence used to copy directories
    - Syntax: xcopy <>
- robocopy command
    - Stands for Robust Copy and supports logging, mirroring and purging(compare two folder structures) of files along with copy functionality.
    - Can select only changed files and is very specific and significant functional switches
- Post-Assessment

  Which command should be used to create a log of all files

  A) copy
  B) xcopy
  C) robocopy
  D) fc

  Answer: C) robocopy

Lesson 4.4: windows system command
Skills: systeminfo, whoami, system commands

- Learning Objectives
    - Learn the systeminfo command
    - Learn the data and time command
    - Understand the whoami command
    - Get the command history.
- Pre-Assessment

  Which command will display the current computer name?

A) whoami
B) system
C) chkdsk
D) systeminfo

Answer: D) systeminfo

- systeminfo command:
  - Display various types of information regarding the computer which include:
    - Computer name
    - Patch level
    - Domain
    - BIOS
    - Last boot time
    - CPU/GPU
- Date and time
  - Used to show the current date and time of the system and also change these values if necessary.
  - Very reliable in a kerberos environment
  - Similar to time command.
- whoami
  - Similar to the linux command and is used to display the current user logged in along with the domain.
- command history
  - Use the doskey /history command to display the previously entered commands
  - Only the history of that session is stored.
- Post-Assessment

  Why is a systeminfo command important to a pentester?

  A) Shows the domain password
  B) May help to display vulnerabilities
  C) Gives SYSTEM privileges
  D) Shows the kerberos TGT

Answer: B) may help display vulnerabilities.

Lesson 4.5: Windows system Part 2
Skills: tasklist, taskkill, sc commands

- Learning objective
  - Understand the tasklist command
  - Understand the taskkill command
  - Learn the sc command
- Pre-Assessment

  The sc command can be used to start and stop services?

  A) True
  B) False

  Answer True

- tasklist command
  - Used to display all running processes and other information like process ID, memory usage, and name.
  - It is essentially used to troubleshoot systems and find unwanted processes.
- taskkill command
  - Used to end a running process.
  - Syntax: taskkill <PID>.
  - Use to kill stuck processes.
- sc command
  - Sc stands for Service control and can interact with service control manager.
  - Manage query, start, stop and pause services
  - Create actions for failure scenarios
  - Syntax: sc <action> <servicename> . Ex: sc query adobermservices
- Post Assessment

  What does the task command need to end a process?

A) PID
B) Systeminfo
C) Service failure action
D) The process must be paused

Answer: A) PID

Lesson 4.6: Windows System Part 3
Skills: fsutil, sfc and chkdisk commands

- Learning Objectives
  - Learn the fsutil command
  - Understand the sfc command
  - Learn the chkdsk command
- Pre-Assessment

  The chkdsk command can be used to potentially repair hard drive

  A) True
  B) False

  Answer: A) True

- fsutil command
  - Stands for File System Utilities
  - Used to identify NTFS quotas , repair file system and and find the Uniform Sequence Number.
  - Can repair bad clusters

- sfc command
  - Stands for System File Check , checks for system files and recovers corrupted OC files
- chkdisk command

    - Stands for checkdisk and is used for many functions regarding the systems hard disk such as
        - Validating disk for good and bad sectors
        - Repair sectors
        - Useful for recovery mode in case system doesn't boot properly
- Post-Assessment

  Which command is useful to validate and repair windows OS files

  A) fsutil
  B) chkdsk
  C) recovery mode
  D) sfc

  Answer: D) sfc specific to windows file systems

Lesson 4.7: Windows Networking Part 1
Skills: ipconfig, getmac, nslookup commands

- Learning Objectives
    - Learn the ipconfig command
    - Learn the getmac command
    - Understand the nslookup command
- Pre assessment

  A computer cannot connect to the network, hat command do you run

  A) getmac
  B) ipconfig
  C) nslookup
  D) ping

  Answer: B) ipconfig

- ipconfig command

    - Stands for internet protocol configuration and is used to display the internet configuration of a specific interface.
    - Shows information such as
        - IP address
        - Subnet mask
        - Mac address
- getmac command
    - Stands for get MAC address and can be used to get mac address of interface only.
    - It can be used remotely.
- nslookup command
    - Stands for Name service lookup, validate and IP address and troubleshoot DNS services.
    - Ex: nslookup <domain name> command gives the resolved ip address as result, server command
- Post-Assessment

  What layer of the OSI model is the IP address?

  A) 1 physical
  B) 2 data link
  C) 3 networking
  D) 4 transport

  Answer: 3 networking

Lesson 4.8: Windows networking Part 2
Skills: ping, tracert, arp commands

- Learning Objectives
    - Learn the ping command
    - Understand the tracert command
    - Understand the arp command

- Pre-Assessment

  You need to verify connectivity the domain controller. What is the best command?

  A) getmac
  B) ipconfig
  C) nslookup
  D) ping

  Answer: D) ping

- ping command
  - Used to check the connectivity to the internet and troubleshoot
  - It is very effective and causes less overhead and easy to use. Sends ICMP packets to address
  - Syntax: ping <address>
- tracert command
  - Similar to ping but records all the hops made to reach the destination address.
  - Troubleshoot latency
  - Syntax: tracert <address>
- arp command
  - Stands for address resolution protocol
  - Sends requests layer 2 MAC addresses
  - Use -a switch to show arp table which consists of all the mac addresses communicating to the system.
  - <Nw and MAC addresses working>
- Post-Assessment

  Why is the arp cache important?

  A) Can be poisoned
  B) Use to determine host IP address
  C) Uses the layer 7 protocols
  D) Can corrupt the file system

Answer: A) can be poisoned

Lesson 4.9: Windows Networking Part 3
Skills: netstat, ftp, shh commands

- Learning Objectives
  - Learn the netstat command
  - Understand the ftp command
  - Learn the ssh command
- Pre-Assessment

  You need to access the command line for another terminal. What is the best command for this?

  A) telnet
  B) ftp
  C) ssh
  D) net

  Answer: C) ssh

- netstat command
  - Stands for network statistics and is used to display all active connections
  - Can be used to identify malware if any unintended connection is found .
  - Syntax: netstat
- ftp command
  - Stands for File transfer protocol
  - Used to list , download ad upload files from a web server
  - It is not secure by default, SFTP a secure alternative
  - Syntax: ftp <ip addresses>
- SSH protocol
- Stands for Secure Shell protocol
- Used to make remote connections and make secure connections to access terminal services

- The communications is encrypted.
- Syntax: ssh [user]@[ip address]
- Post-Assessment

  What does ftp stand for?

  A) Free trade protocol
  B) File transfer protocol
  C) Field Take protocor
  D) File trading Protocol

Lesson 4.10: Net command
Skills: net commands, switches

- Learning Objectives
  - Learn the capabilities of the net command
  - Add users from the command line
  - Create groups
  - Start and stop services
  - Mount remote file shares
- Pre-Assessment

  Which command is used to mount a remote share?

  A) net remote
  B) net share
  C) net use
  D) net file

  Answer C) net use

- Intro to the net command
  - Add users
  - Add groups
  - Start/stop services

    - Connect to other computers
- Adding users
    - net user [username] [password]
    - Can be automated
- Adding groups
    - net group [groupname]
    - /add [usernames]
    - /delete [usernames]
- Start and stop services
    - net start [service] Starts a service
    - net stop [service]Stops a service
    - Can be used to list services as well!
- Remote file shares
    - net use
    - net use H:\\computername\share
    - Used to connect to shared folders
- Post-Assessment

  What actions can't be done with the net command?

  A) Connect to other computers
  B) Create admin accounts
  C) Start or stop services
  D) Shutdown a computer

Answer: D, Shutdown a computer.

Module 5 : Advanced Command Line Techniques

Lesson 5.1: Windows Advanced Piping and Ampersand
Skill: piping, ampersand, CLI tools

- Learning Objectives
    - Learn what piping is used for
    - Learn what single and double pipes do
    - Understand the & and && operands
- Pre-Assessment

  Which operand runs cmd2 if cmd1 fails?

  A) cmd1 | cmd2
  B) cmd1 || cmd2
  C) cmd1 & cmd2
  D) cmd1 && cmd2

  Answer: B) cmd1 || cmd2

- Single pipe
    - Piping is used to pass the output of the first command to the second command I.e used to link two commands together.
    - Mostly used with grep/ ledd
    - Syntax: <command 1> | <command 2>
    - Ex: cat file.txt | grep word | less , this command reads the file.txt and searches for the string “word” and displays is in on a scroll able screen
- Double Pipe
    - Executes the second command if first one fails (works like a conditional statement)
    - Used for functionality and scripting
    - Syntax: <command 1> || <command 2>
- Ampersand “&”
    - Used in windows , executes multiple commands without checking for errors or success
    - Basic functionality is to execute multiple commands in one line
    - Syntax <cmd 1> & <cmd 2>
    - Although this command in linux is used to run a specific command in the background

    - General usage
        - Launch terminal applications without losing access to terminal
        - Launch GUI(at the background) from the CLI
        - Gives the PID as output
- Double ampersand
    - Quite opposite to the double pipe it executes the second command only if the first command executes successfully.
- Post-Assessment

  Which operand will execute cmd2 if cmd1 is successful?

  A) cmd1 & cmd2
  B) cmd1 && cmd2
  C) cmd1 &| cmd2
  D) cmd1 || cmd2

  Answer: B) cmd1 && cmd2

Lesson 5.2: Windows command Redirection
Skills: conditional commands, redirections

- Learning Objectives:
    - Understand the purpose of redirection
    - Learn what the > does
    - Learn what the >> does
    - Understand what < does
- Pre-Assesment

  Which operand appends to an existing file?

  A) <
  B) <<
  C) >>
  D) >

Answer : C) >>

- Redirection
  - Allows user to perform various functions with the input or output
  - Ex: Direct output and input using > and < respectively
  - Can redirect the standard input and output such as keyboards and monitors
- Single >
  - This command is used to redirect the output of specific command to the specified file.
  - Will create a file if it doesn't exist else will overwrite the file. Not suitable if previous data is to be retained.
  - Ex: echo "hello there!" > hello.txt will save the string in the file.
- Double >>
  - Similar to the single > but slightly different in functionality as it appends the output and doesn't overwrite it.
  - Useful to retain the original info while writing to a file.
  - Ex: echo "this didn't overwrite everything" >> hello.txt, this command will append the string to the end of the hello.txt file.
- Single <
  - Used to take input from the specified and will not change the content of the file.
  - Will not create the file of not present , have to file the file name that exists
  - Ex: sort "file.txt" will take the contents of the file.txt and provide them as input to the sirt command
- Redirecting stderr
  - Is essential to redirect the errors of a specific command or program to a specified location. The errors are thus dropped and not displayed
  - Syntax : 2> <folder>, here "2>" is to specify the stderr only and redirect it to the specified folder
- Post-Assessment

  Which operand overwrites an existing file?

  A) <
  B) <<

C) >
D) >>

Answer: C) >

Lesson 5.3: For and While loops
Skills: condition loops, file loops, CLI tools

- Learning objectives
  - Understand the purpose of a command loop
  - Learn linux loops
  - Learn windows loops
- Pre-Assessment

  Why are loops useful?

  A) Complete repetitive tasks
  B) Do not overload the system
  C) They will stop automatically if too resource intensive
  D) They will automatically execute new commands.

  Answer: A

- For and While loops:
  - Commands are executed until a specific requirement is met and then it breaks out.
  - Can run for specific number of time or forever.
  - For takes an input and while evaluated whether the condition is true or not

- Linux loops
  - The loop consists of 3 basic steps to complete one cycle of execution
    - Parameter definition and loop condition
    - Command to run

        - Done
- Linux file loops
    - Can use the file input fr looped commands
        - Generally used to execute commands from input
        - The $(cat[file]) executes the command
- Syntax : for I in $(cat words.txt); do echo $i; done
- Windows loops
    - Similar functionality as linux but has various subsets
    - /L for a list of numbers.
    - /F for file inputs.
    - Syntax: for /L %G in (1,1,15) do echo %G , here %G is the parameter. The first digit in brackets stands for the value of increment and the second number separated with a comma stands for the starting followed by the ending value separated with a comma.
    - For /L %G in () do echo “oops!” echos string infinitely.
    - For /F %G in (words.txt) do echo %G echos content in file, here it is words.txt .
- Post-assessment

  What is the purpose of the parameter in a for loop?

  A) Marks the files for input
  B) Creates unlimited looping
  C) Assigns multiple variables
  D) Used to track the completion of the loop

  Answer: D) used to track the completion of the loop

Lesson 5.4: Linux shell scripting
Skills: shell script, write, execute

- Learning objectives
    - Understand the purpose of a shell script
    - Learn how to write a shell script

    - Execute a script
- Pre-Assessment

  What is the well-known file extension for shell scripts

  A) .shell
  B) .sh
  C) .script
  D) .shscript

  Answer: B) .sh

- Purpose of shell script
    - Best used to automate processes similar to previous for/while loops
    - File extension : .sh
- Writing a shell script
    - Specify the shebang at the start of the shell script to indicate which interpreter to use
    - #!/bin/bash
- Execute a shell script
    - Use the "./" before an executable file to run the shell script
    - Note that the user should have permission to execute the file (use chmod)
- Post-Assessment

  You write a shell script but don't have the permission to run it. What command do you execute?

  A) nano
  B) vim
  C) ifconfig
  D) chmod

  Answer: chmod

Lesson 5.5: Windows Bash Scripting

Skills: bash scripts, write, execute

- Learning Objectives
    - Understand the purpose of bash script for windows
    - Learn how to write a batch script
    - Execute a batch script
- Pre-Assessment

  What is the well-known file extension for batch scripts

  A) .bat
  B) .batch
  C) .vbs
  D) .macro

  Answer: A) .bat

- Purpose of batch script
    - Used to automate processes.
    - Similar to linux .sh files and the for/while loops.
    - Has the .bat extension.
    - Can be executed at any terminal or any other processes.
- Writing a batch script
    - Functions are used to perform a specific set of tasks which can be used as labels and few important functions are:
        - The :label function creates a separate section of the script.
        - The goto label accesses the label section.

- Execute a batch file
    - Type the file name into the command prompt with the extension to execute.
    - Note: File must be in the current working directory.
- Post-Assessment:

How do you create labels in a batch script?

A) ;
B) :
C) “
D) /

Answer: B) :

Lesson 5.6: Conclusion:
Skills: CLI tools ,help, CLI tools

- Learning objectives
  - How to open command line
  - How to ask for help at the terminal
  - Understand how to navigate the file system with the CLI
  - Use common CLI tools to perform time-saving tasks
  - Chain commands together.
- How to open the command line
  - Using terminal to interact with system using specific commands
  - Similar in windows and linux
- Asking for help:
  - Crucial functionality of the CLI where you can access the documentation of the command.
  - Always use the internet to learn more and research about command .
- Navigate the file system
  - There is a difference in the file system between GUI and CLI
  - Use the cd(linux) and dir(in windows) for directory traversal.
  - Use the ls(linux) and dir(windows) to view directory content, Don’t forget pwd if you are lost.
- Use the CLI to save time
  - Identify the goal and use the right tool for the job.
  - Learn and sort through the output.
- Chain commands together

    - Pipe commands together to get effective output and save time.
    - Use the & and > command wisely.
- Additional resources
    - Other cybrary videos
    - Linux manual
    - SANS cheat sheet https://www.danielowen.com/2017/01/01/sans-cheat-sheets/
    - Internet :
        - https://www.linux.org
        - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands