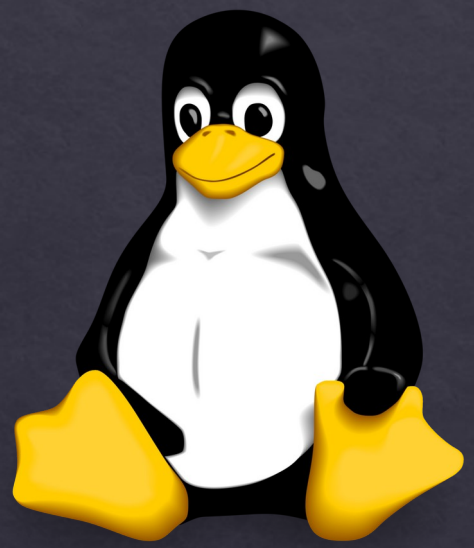
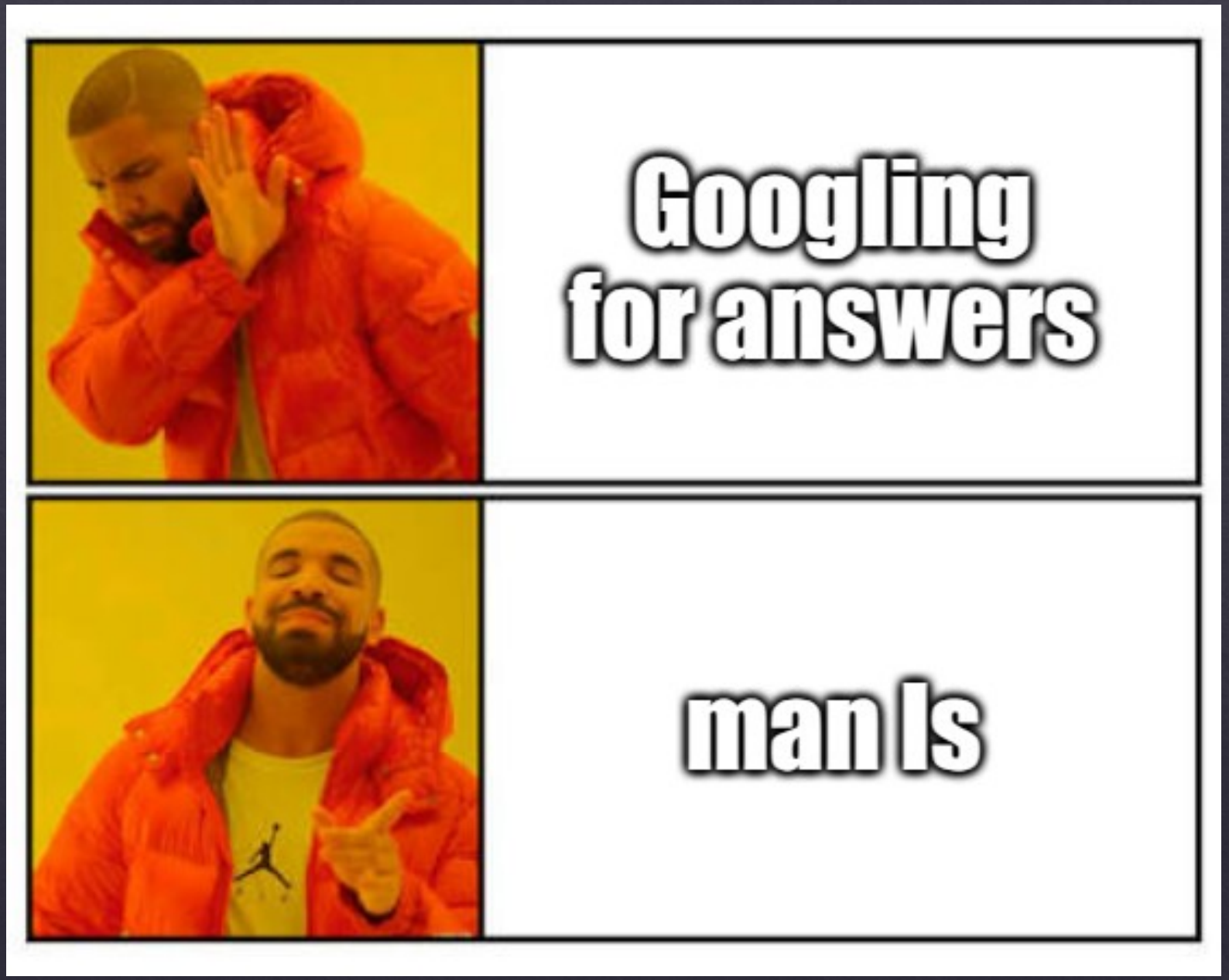


Linux Essentials for Cybersecurity

The Linux Command Line

Getting Help

- **man:** provides detailed documentation about Linux commands, system calls, configuration files, and more.
- **help:** used to get quick help on shell commands
- **info:** provides more detailed documentation than man
- The **–help** option**:** --help option for a brief summary
- Internet resources for Linux Documentation


Googling
for answers
man ls

Man Page Structure

- **NAME** – The command or function name and a short description.
- **SYNOPSIS** – Shows how to use the command (options and arguments).
- **DESCRIPTION** – Provides a detailed explanation of the command.
- **OPTIONS** – Lists available command options and their effects.
- **FILES** – Important files related to the command.
- **SEE ALSO** – Related commands or documentation references.
- **EXAMPLES** – Sometimes includes real-world usage examples.

Internet Resources

- The Linux Documentation Project (LDP)
  https://tldp.org/
- GNU Manuals
  http://gnu.ist.utl.pt/manual/manual.html
- Linux Kernel Documentation
  https://docs.kernel.org/
- Ubuntu forums
  https://ubuntuforums.org/
- Search engines (Google, DuckDuckGo, Bing, etc)

Paths

- **Path:** a string of characters that specifies the location of a file or directory within a file system's hierarchical structure.
- **Absolute Pathnames**: begin with the root (/) directory and follows the tree branch by branch until the path to the desired directory or file is completed.
  - `$ cd /home/user/Documents`
- **Relative Pathnames:** A relative path specifies a file or directory location in relation to the current working directory. It does not start with (/)
  - `$ cd Documents`

Special Relative Path Symbols

SYMBOL	MEANING
.	Current directory
..	Parent directory (one level up)
~/	Home directory

Navigation

- **pwd (Print Working Directory):** displays the absolute path of the current directory. It helps you know exactly where you are in the directory structure.
- **cd (Change Directory):** The cd command allows you to navigate between directories.

- **ls (List):** The ls command lists files and directories in the current directory.
  - Detailed listing: $ ls -l
  - Show hidden files: $ ls -a

Managing Files and Directories

- **mkdir (Make Directory):** to create a new directory.
  - $ mkdir new_dir
- **cp (Copy):** command is used to copy files or directories
  - $ cp file1 file2
  - $ cp -r dir1/ dir2/
- mv (Move/Rename): move files or directories, or rename them.
  - $ mv oldname newname
  - $ mv file1.txt /home/user/Downloads

Managing Files and Directories

- **rm (Remove):** removes files or directories.
  - $ rm a_file.txt
  - $ rm -r a_folder/
- **touch (Create/Update File):** create a new, empty file or to update the access and modification timestamps of an existing file.
  - $ touch newFile.txt
- **file:** determine the type of a file
  - $ file document.txt


Delete all .txt files
rm *.txt
- Open File Explorer
- Select all .txt files
- Press "Delete"
imgflip.com

File Viewing

- **less:** a pager program that lets you view large files one screen at a time.
  - $ less file_with_long_content.txt
- **head:** displays the first 10 lines of a file. Specify the number of lines using the -n flag.
  - $ head long_file.txt
  - $ head -n 23 long_file.txt
- **tail:** displays the last 10 lines of a file. Use the -f flag to watch real-time updates to a file.
  - $ tail file1.txt
  - $ tail -f file1.txt

less Commands

COMMAND	ACTION
G	Move to the end of the text file
1G or g	Move to the beginning of the text file
/characters	Search forward to the next occurrence of characters
n	Search for the next occurrence of the previous search
h	Display help screen
q	Quit less

Environment Variables

- They are named objects that contain data used by one or more applications.
- They store system and user settings.
- To display the list of Linux environment variables, use printenv
  - $ printenv
  - $ printenv USER
- “$” is used to reference or expand the value of a variable
- Use “echo” and reference the value to display its value.
  - $ echo $USER
  - $ echo $PATH

Environment Variables

- **PATH:** directories where executables are searched
- **USER:** current user logged in
- **HOSTNAME:** system hostname
- **HOME:** path to your home directory.
- **SHELL:** path to your default shell.
- **TERM:** type of terminal you're using.
- **OSTYPE:** the operating system type
- **MACHTYPE:** the machine architecture.

Input/Output Redirection

- **Redirecting Standard Output:**
  - > redirects output to a file, replacing existing content
    - $ cut -d: -f1 /etc/passwd > users.txt
  - >> appends output to a file without overwriting
    - $ uptime >> report.txt
- **Redirecting Standard Input:**
  - < takes input from a file instead of typing manually
    - $ wc -l < some_file.txt

Redirecting Error Output

- Linux separates standard **output (1)** and **standard error (2)**
- **Redirecting Errors to a File:**
  - $ ls /nonexistentfolder 2> errors.log
- **Suppressing Errors:**
  - $ ls /nonexistentfolder 2> /dev/null
- **Redirecting Both Standard Output and Errors:**
  - cp myfile.txt /destination/ &> combined.txt

Searching and Filtering

- **find:** searches for files based on name, type, size, or modification time
  - $ find /home -name "document.txt"
  - $ find /home -type d
- **grep:** searches for patterns inside files or command outputs
  - $ grep "error" logfile.txt
- **sed:** modifies text in files without opening them
  - $ sed 's/apple/orange/g' file.txt
  - $ sed '/^$/d' file.txt

Piping

- Pipes (|) send output of one command as input to another.
  - $ ls -l | grep ".txt"
  - $ ps aux | wc -l

Thank you