LINUX Basics

NOTE: Commands are in (**“”**).

Activity 1: Install software in a Linux distribution

What you’ll do

You have multiple tasks in this lab:

- Confirm APT is installed in Bash
- Install Suricata with APT
- Uninstall Suricata with APT
- Install tcpdump with APT
- Reinstall Suricata with APT
- Update tcpdump with APT

Task 1. Ensure that APT is installed

- **“apt”**

Task 2. Install and uninstall Suricata

- **“sudo apt install suricata”**
- **“suricata”**
- **“sudo apt remove suricata”**
- **“suricata”**

Note: *The* `apt install` *and* `apt remove` *commands must be prefixed with the* `sudo` *command as elevated privileges are required to install and uninstall software in Linux.*

Task 3. Install tcpdump

- **“sudo apt install tcpdump”**

Task 4. List the installed apps

a. **“apt list --installed”**

Note: *The specific version of* `tcpdump` *that you see displayed may be different from what is shown above.*

Task 5. Reinstall Suricata

- **“sudo apt install suricata”**
- **“apt list --installed”**

Task 6. Update tcpdump

Getting latest packages information

- **“sudo apt update”**

This will fetch the latest package information from trusted sources.

apt update doesn't actually update your packages; instead, it finds if any packages can be upgraded.

Updating tcpdump:

To get the latest supported version of tcpdump, type the following:

- **“sudo apt upgrade tcpdump”**

You may be prompted: “Do you want to continue? [Y/n]”

Type “y” for Yes and press Enter to continue.

- **“apt --list upgradable”**

This command will show all packages which can be upgraded.

- **“sudo apt upgrade tcpdump”**

This command will intelligentially fully upgrade all packages to latest versions by removing older files and adding new files.

Note: It will take time and space.

Activity 2: Examine input and output in shell

What you'll do

You have multiple tasks in this activity:

- Generate output in the shell the ***echo*** command
- Perform basic calculations the ***expr*** command
- Clear the shell window the ***clear*** command
- Explore the commands further

Task 1. Generate output with echo command

- **"echo hello"**
- **"echo "hello""**
- **"echo "Your name""**

Note: *The output is the same as before. The quotation marks are **optional** in this case, but they tell the shell to group a series of characters together. This can be useful if you need to pass a string that contains certain characters that might be otherwise misinterpreted by the command.*

Task 2. Generate output with expr command

- **"expr 32 - 8"**
- **"expr 3500 * 12"**

Note: *The `expr` command requires that all terms and operators in an expression are separated by spaces. For example: `expr 32 - 8`, and **not** `expr 32-8`.*

Task 3. Clear bash shell

- **"clear"**

Note: *All previous commands and output will be cleared, and the user prompt and cursor will return to the upper left of the shell window.*

Task 4. (Optional) Perform more calculations with expr command

- **echo "Example text"**

The mathematical operators you can use with the `expr` command for **adding, subtracting, dividing,** and **multiplying** are `+`, `-`, `/` and `*`.

Note: *The `expr` command performs integer mathematical calculations only, so you cannot use the decimal point or expect a fractional result. All results are rounded down to the nearest integer. Also, all terms and operators in an expression need to be separated by spaces. For example: `expr 25 + 15`, and **not** `expr 25+15`.*

Activity 3: Find files with Linux commands

What you'll do

You have multiple tasks in this activity:

- Find your current working directory and display its contents
- Navigate to a directory and list subdirectories
- Display the contents of a file
- Display the first 10 lines of a file

Task 1. Get current directory information

- **"pwd"**
- **"ls"**

Task 2. Change directory and list subdirectories

- **"cd reports"**
- **"cd /home/analyst/reports"**
- **"ls"**

Note: *The `cd` command accepts absolute and relative paths. An absolute path includes all the directories from the root of the file system and starts with a `/`. An alternative is a relative path, which is expressed starting from the current directory and starts without the initial `/`. The above command uses a relative path.*

Recall the special paths:

Symbol	Stands for
`~`	Home directory
`/`	Root directory
`.`	Current directory
`..`	Parent directory

Task 3. Locate and read content of file

- **"cd /home/analyst/reports/users"**
- **"cd users"**
- **"ls"**
- **"cat Q1_added_users.txt"**
- **"cat /home/analyst/reports/users/Q1_added_users.txt"**

Note: *The `cat` command prints the contents of a file to the shell. You can specify the file to display using absolute or relative paths.*

Task 4. Navigate a directory and locate a file

- **"cd /home/analyst/logs"**

- **“ls”**
- **“head server_logs.txt”**

Note: *The `head` command displays just the beginning of a file, by default ten lines. You can specify how many lines to display using the `-n` argument, which specifies the number of lines to display.*

Activity 4: Filter with grep

What you'll do

You have multiple tasks in this activity:

- Search for error messages in a file
- Search for files that contain a specific string
- Search for information in user files

Task 1. Search for error message in a log file

- **"cd logs"**
- **"grep error server_logs.txt"**

Note: *If you enter a command incorrectly and it fails to return to the command-line prompt, you can press* ***CTRL+C*** *to stop the process and force the shell to return to the command-line prompt.*

Note: *The first argument passed to* `grep` *is the string you're searching for, and the second argument is the name of the file you're searching through.*

Task 2. Find files containing specific string

- **"cd /home/analyst/reports/users"**
- **"ls | grep Q1"**
- **"ls | grep access"**

Note: *Piping sends the standard output of one command to the standard input of another command for further processing. In the example, the output of the* `grep` *command is piped to the* `ls` *command and the output displayed in the shell.*

Task 3. Search more file contents

- **"ls"**
- **"grep jhill Q2_deleted_users.txt"**
- **"grep "Human Resources" Q4_added_users.txt"**

Note: *In order for* `grep` *to interpret a string of two or more words correctly, you must enclose it in quotes (*`"Human Resources"`*).*

Activity 5: Manage files with Linux command

What you'll do

You have multiple tasks in this activity:

- Create a new directory
- Remove a directory
- Move a file and delete a file
- Create a file and add text using nano

Task 1. Create a new directory

- **"mkdir logs"**
- **"ls"**

Task 2. Remove a directory

- **"rmdir temp"**
- **"ls"**

Task 3. Move a file

- **"cd /home/analyst/notes"**
- **"cd notes"**
- **"mv Q3patches.txt /home/analyst/reports/"**
- **"ls"**

Task 4. Remove a file

- **"rm tempnotes.txt"**
- **"ls"**

Task 5. Create a new file

"touch tasks.txt"

"ls"

Task 6. Edit a file

- **"nano tasks.txt"**
- **Ctrl+0, enter, Ctrl+X**
- **"clear"**
- **"cat tasks.txt"**

Note: *This action changes the shell from the normal Bash interface to the nano text editor interface.*

Note: *The recommended sequence of commands for saving a file with the nano text editor is to use* ***CTRL+O*** *to tell nano to save the file and then use* ***CTRL+X*** *to exit immediately.*

Activity 6: Manage authorization

What you'll do

You have multiple tasks in this activity:

- Check permissions for files in a directory
- Check for incorrect file permissions and change permissions as needed
- Remove unauthorized access to a directory

Task 1. Check files and directories in detail

- **"cd projects"**
- **"ls -l"**
- **"ls -la"**

Task 2. Change file permissions

- **"ls -l"**
- **"chmod o-w project_k.txt"**
- **"ls -l"**
- **"chmod g-r project_m.txt"**

Note: *Permissions are granted for three different types of owners, namely user, group, and other.*

In the `chmod` command, `u` sets the permissions for the user who owns the file, `g` sets the permissions for the group that owns the file, and `o` sets the permissions for others.

Task 3. Change file permissions on a hidden file

- **"ls -la"**
- **"chmod u-w, g-w, g+r .project_x.txt"**

Note: *Be sure to start the name of a hidden file with a period (.).*

Task 4. Change directory permission

- **"ls -l"**
- **"chmod g-x drafts"**

Activity 7: Add and manage users with Linux commands

What you'll do

You have multiple tasks in this activity:

- Add a new employee
- Change ownership of a file
- Add the new employee to a new group
- Delete the employee from the system

Task 1. Add a new user

- **"sudo useradd researcher9"**
- **"sudo usermod -g research_team researcher9"**
- **"sudo useradd researcher9 -g research_team"**

Task 2. Assign file ownership

- **"sudo chown researcher9 /home/researcher2/projects/project_r.txt"**

Task 3. Add the user to a secondary group

- **"sudo usermod -a -G sales_team researcher9"**

Note: *Options for Linux commands are case-sensitive, so make sure you use a lowercase* `-a` *and an uppercase* `-G`.

Task 4. Delete a user

- **"sudo userdel researcher9"**
- **"sudo groupdel researcher9"**

Activity 8: Get help in command line

What you'll do

You have multiple tasks in this activity:

- Explore commands that help you learn more about other commands
- Find options for a command
- Determine the differences between two commands
- Identify the command needed to create a new group

Task 1. Learn more about commands

- **"whatis cat"**
- **"man cat"**
- **"apropos -a first part file"**

Note: *There is no right and wrong when using* `apropos` *in terms of keywords. Think of it as a very focused search. It will only return commands that correspond to keywords you supply. Keep trying if the first returned command does not provide what you need. Also, keep in mind that using the* `-a` *option will limit results to only those commands that match all keywords supplied.*

Task 2. Explore the user add command

- **"man useradd"**

Task 3. Explore the rm and rmdir command

- **"whatis rm"**
- **"whatis rmdir"**

Task 4. Determine which command to use

- **"apropos -a create new group"**