CYBRARY

# Offensive Penetration Testing Commands Guide

**Created By:** Somesh K Tiwari, Teaching Assistant

1. **alias command -** The alias command lets you give your own name to a command or sequence of commands. You can then type your short name, and the shell will execute the command or sequence of commands for you.
2. **cat command -** The cat command (short for "concatenate") lists the contents of files to the terminal window.
3. **cd command -** The cd command - change directory - will allow the user to change between file directories. As the name command name suggest, you would use the cd command to circulate between two different directories.
4. **chmod command -** The chmod command sets the file permissions flags on a file or folder. The flags define who can read, write to or execute the file.
5. **chown command -** The chown command allows you to change the owner and group owner of a file.
6. **curl command -** The curl command is a tool to retrieve information and files from Uniform Resource Locators (URLs) or internet addresses. The curl command may not be provided as a standard part of your Linux distribution.
7. **df command -** The df command shows the size, used space, and available space on the mounted filesystems of your computer.
8. **diff command -** The diff command compares two text files and shows the differences between them. There are many options to tailor the display to your requirements.
9. **echo command -** The echo command can show the value of environment variables, for example, the $USER, $HOME, and $PATH environment variables. These hold the values of the name of the user, the user's home directory, and the path searched for matching commands when the user types something on the command line.
10. **exit command -** The exit command will close a terminal window, end the execution of a shell script, or log you out of an SSH remote access session.
11. **find command -** Use the find command to track down files that you know exist if you can't remember where you put them. You must tell find where to start searching from and what it is looking for.

12. **finger command -** The finger command gives you a short dump of information about a user, including the time of the user's last login, the user's home directory, and the user account's full name.
13. **free command -** The free command gives you a summary of the memory usage with your computer. It does this for both the main Random-Access Memory (RAM) and swap memory.
14. **grep command -** The grep utility searches for lines which contain a search pattern. The grep command can also search the contents of files.
15. **groups command -** The groups command tells you which groups a user is a member of.
16. **gzip command -** The gzip command compresses files. By default, it removes the original file and leaves you with the compressed version. To retain both the original and the compressed version, use the -k (keep) option.
17. **head command -** The head command gives you a listing of the first 10 lines of a file. If you want to see fewer or more lines, use the -n (number) option.
18. **history command -** The history command lists the commands you have previously issued on the command line. You can repeat any of the commands from your history by typing an exclamation point! and the number of the command from the history list.
19. **kill command -** The kill command allows you to terminate a process from the command line. You do this by providing the process ID (PID) of the process to kill.
20. **less command -** The less command allows you to view files without opening an editor.
21. **ls command -** the list command - functions in the Linux terminal to show all of the major directories filed under a given file system
22. **man command -** The man command - the manual command - is used to show the manual of the inputted command. Inputting the man command will show you all information about the command you are using.
23. **mkdir command -** The mkdir - make directory - command allows the user to make a new directory. Just like making a new directory within a PC or Mac desktop environment, the mkdir command makes new directories in a Linux environment.
24. **mv command -** The mv command - move - allows a user to move a file to another folder or directory. Just like dragging a file located on a PC desktop to a folder stored within the "Documents" folder, the mv command functions in the same manner.
25. **passwd -** The passwd command lets you change the password for a user. Just type passwd to change your own password. You can also change the password of another user account, but you must use sudo. You will be asked to enter the new password twice.

26. **ping -** The ping command lets you verify that you have network connectivity with another network device. To use ping, provide the IP address or machine name of the other device.
27. **ps -** The ps command lists running processes. Using ps without any options causes it to list the processes running in the current shell.
28. **pwd -** Nice and simple, the pwd command prints the working directory (the current directory) from the root / directory
29. **shutdown -** The shutdown command lets you shut down your Linux system. Using shutdown with no parameters will shut down your computer in one minute.
30. **ssh command -** Use the ssh command to make a connection to a remote Linux computer and log into your account. To make a connection, you must provide your user name and the IP address or domain name of the remote computer.
31. **sudo command -** The sudo command is required when performing actions that require root or superuser permissions, such as changing the password for another user.
32. **tail command -** The tail command gives you a listing of the last 10 lines of a file. If you want to see fewer or more lines, use the -n (number) option.
33. **tar command -** With the tar command, you can create an archive file (also called a tarball) that can contain many other files. This makes it much more convenient to distribute a collection of files. You can also use tar to extract the files from an archive file. It is common to ask tar to compress the archive. If you do not ask for compression, the archive file is created uncompressed. To create an archive file, you need to tell tar which files to include in the archive file, and the name you wish the archive file to have.
34. **uname command -** You can obtain some system information regarding the Linux computer you're working on with the uname command.
35. **w command -** The w command lists the currently logged in users.
36. **whoami command -** Use whoami to find out who you are logged in as or who is logged into an unmanned Linux terminal.

**References –**

1. https://www.geeksforgeeks.org/
2. https://www.howtogeek.com/
3. http://www.informit.com/