

## Study Guide

### Kali Linux Fundamentals

Created By: Jose Llerena, Teaching Assistant

#### Module 1.

##### Lesson 1.0: The Beginning

*Skills Learned From This Lesson: Live Boot, Forensics Mode, Disk Encryption.*

- There are a vast variety of Linux Distributions
- Linux Kernel controls CPU, Memory and Devices
- Some of Kali application categories are Information Gathering, Vulnerability Analysis, Wireless Attacks, Web Applications, Exploitation Tools.

##### Lesson 1.1: Getting Kali up and running

*Skills Learned From This Lesson: Download, Install, Checksum.*

- Hypervisor
  - VMWARE
  - Virtual Box
- Installation: Preferably 64bit.
- Different Desktop Environments like KDE also possible to download
- Checksum: SHA-256
- Live CD to test distribution without the need of a full install

##### Lesson 1.2: Moving around

*Skills Learned From This Lesson: Terminal, Applications, Settings*

- Show Applications option to search a specific application
- Settings to configure Kali Linux most common options
- Free explore the system to discover its features

#### Module 2.

##### Lesson 2.0: The Terminal

*Skills Learned From This Lesson: Commands, Root.*

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Pwd command: To list current directory
- Ls command: To list directory content
- Cd .. command: The two dot parameter is to leave current directory and go to immediate parent directory.
- Cd command is to change directory, specifying the directory where I want to go.
- Cat command: *cat filename* is to show the content of a file.
- Rm command: *rm filename* is to delete a file
- Mkdir command: *mkdir dirname* is to create a new directory
- Mv command: Moves a file or directory to another location

## Lesson 2.1: File System

### *Skills Learned From This Lesson: Permissions, Directories*

- /bin/: basic programs
- /root/: administrator personal files
- /mnt/: temporary mount points
- /etc/: configuration files
- /dev/: device files
- Permissions: 0 none, 1 execute, 2 write, 4 read, combining those permissions will result in the sum of its value, for example, if a user has a permission only for read and execute, it will be 5, or if permission is set to write and execute, it will be 3.
- Permissions is set in 3 groups, the first one is permission for the owner, second is for the group and the third is for others. When executing command *chmod 755 filename*, the permission is set for full permission for owner and execute and read permission for group and others.

## Lesson 2.2: Useful commands

### *Skills Learned From This Lesson: Scripting, Text Editor, Skill*

- Clear command: To clear text in terminal window
- Man command: *man command* to open the manual for the corresponding command
- Echo command is to output text, is more used in programming and scripting
- Most known text editors are nano, vi, vim.
- Whoami: This command show the user I am.
- Id prints my user and group id
- Df command shows disk usage by partition

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

- Passwd command: *passwd user* prompts to change a user password, this is possible only with root, with regular users only work using passwd alone in order to change my own password.

## Module 3.

### Lesson 3.1: Basic Network Commands

#### *Skills Learned From This Lesson: Network commands*

- Ipconfig command: to show current network configuration, it is usually executed to know user ip address
- Ping command: to test connection to a remote server.
- Traceroute command: to show the path of server to where user passes through before reaching the final destination
- Netstat command show routing tables as well as current PC connections
- Nslookup command queries domain name servers and shows the ip associated with that DNS
- Dig command shows more detailed info in relation of nslookup
- Iwconfig command shows wireless interface

### Lesson 3.2: Services

#### *Skills Learned From This Lesson: Service, Apache, Process*

- Ps command show processes, using the options aux show all users processes, displays the owner of the process and shows processes not attached to a terminal
- Ssh it is a secure service to connect to a remote shell securely
- Nano it is widely used not only to edit text files but also to modify configuration files

### Lesson 3.3: Managing Users

#### *Skills Learned From This Lesson: User management, password, group*

- */etc/passwd*: In old distros password key used to be stored here, newer distros it lists users
- */etc/group*: File with groups information
- Adduser command adds new user
- Userdel command deletes a user

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

---

# CYBRARY

---

## Module 4.

### Lesson 4.1: Troubleshooting basics

*Skills Learned From This Lesson: Physical troubleshoot, network troubleshooting, services*

- Basic troubleshooting implies checking physical connections, another basic check is to restart devices.
- Check network connections with its basic commands: ping, netstat, traceroute, etc.
- Checking the services is very important with command `service service_name status/restart`.
- Googling and checking blogs/forums is very helpful

### Lesson 4.2: The tools chest

*Skills Learned From This Lesson: Tools*

- Going to <https://tools.kali.org/tools-listing> is very useful to find the list of all Kali tools

CYBRARY

---

Brought to you by:

**CYBRARY** | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.