Using Kali Linux at the Command Line

Morgan Villano

CYB 605 – Principles of Cybersecurity

Utica College

Using Kali Linux at the Command Line

**Introduction**

Kali Linux is an open-source, Debian-based Linux distribution that is used mainly for advanced penetration testing and security Auditing. Kali Linux contains many different tools that target information security tasks. Kali was released on March 13, 2013. Kali Linux is all based on years of knowledge and expertise. There are multiple different tools that are in Kali Linux such as Wireshark, password crackers, hashdeep, Vulnerability Analysis, and many more. This Lab will be a good example of basic knowledge. This lab can help beginners get started on learning the Linux commands and command line. **(*What is Kali Linux? Kali Linux documentation* 2022)**

**Objective:**

The purpose of the lab is to introduce students to Kali Linux. Knowledge of the command line provides the student an edge when performing information security related tasks. Use of the command line is an alternate way to automate tasks normally done manually through a graphical user interface (GUI).

**Overview:**

Kali Linux is an open-source Debian-based Linux distribution that allows users that are focused on information security, penetration testing, security auditing, computer forensics, and reverse engineering to have access to the top tools needed to achieve the tasks that are given to them.

**Lab Setup**

* Install Kali Linux on your virtual machine. The link to download Kali Linux is here: [www.kali.org/downloads/](http://www.kali.org/downloads/)
* Virtual Machine <https://www.virtualbox.org/>
* The link to watch a video that explains how to install Kali Linux is here:

<https://www.youtube.com/watch?v=1VW55ZC4cyM&t=11s>

**Results and Analysis**

1. **Navigate to the user account home directory. Create a file named test.txt which contains the text “HI I AM A TEST FILE” (no quotation marks). Output the contents of the file to verify that the file contains what it should.**

* To achieve the first step, the student must Download Kali Linux and create a Virtual Machine on Oracle Virtual box. Once the VM is created you download Kali Linux onto it. **(*Oracle virtual box*)**
* Next the student went to home directory (Command: cd home)
* Then the student went into the user account in the home directory as well as added the file into the Documents folder (Command: cd morgan) (Command: cd Documents)
* The student created the file by using the command touch. (Command: Touch test.txt) **(“How to Create a File in Linux | Linuxize”, 2019)**
* The student then lists the files within the directory (Command: ls)
* The student proceeded to add context to the file by using the command nano. (Command: nano test.txt) The context that was entered into the file was “HI I AM A TEST FILE”.
* Finally, the Student used the command cat. cat is a way for you to enter the file without editing it (Command: cat test.txt)

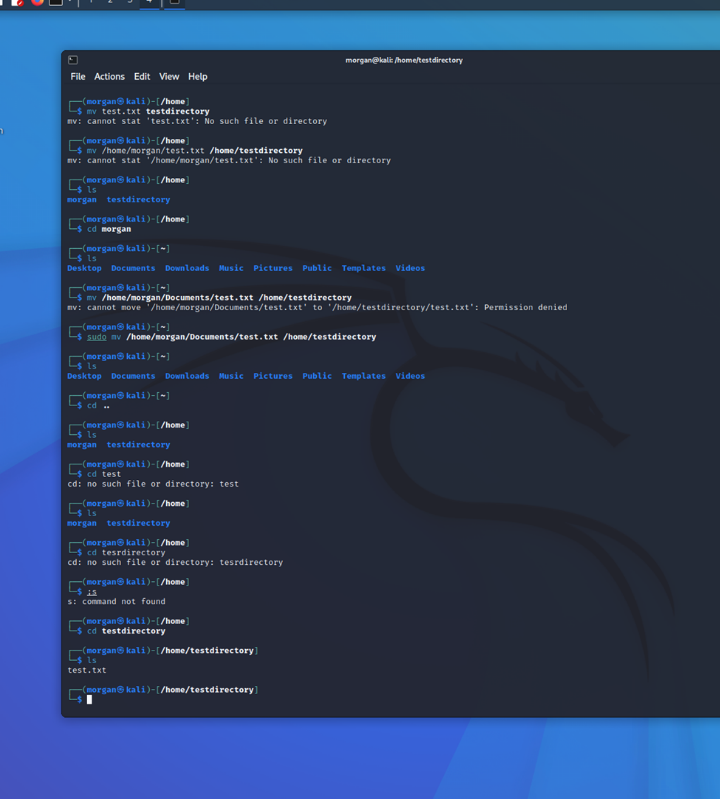
Graphical user interface, text

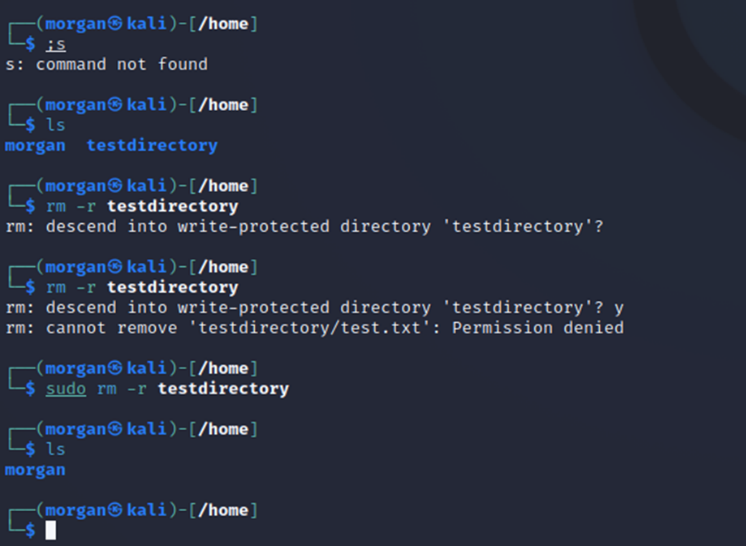
Description automatically generated

1. **Navigate to the user account home directory. Create a directory named testdirectory. Move the file test.txt (created in 1) to the testdirectory directory. List the contents of the testdirectory directory. Delete the directory testdirectory**.
   * The student needed to create a directory in the user account home directory. (Command: sudo mkdir testdirectory) **(*How to open, edit, move, and copy a file in Linux* 2021)**
   * The student had to move the test.txt file that was in the home user directory to the testdirectory (Command: sudo mv /home/morgan/Documents/test.txt /home/testdirectory) \*\*Make sure when you are moving files between the directories, you must do the full path of where the is and where it should be going to.\*\* **(Foundation, 2022)**
   * The student proceeded to make sure that the file was now in the new directory. The commands used were ls (ls was to list the directories within the home directory). cd (cd was to enter the testdirectory) ls (to list the files within the
   * Finally, the student had to remove the testdirectory by using the commands: (sudo rm -r testdirectory) **(*How to open, edit, move, and copy a file in Linux* 2021)**

A screenshot of a computer

Description automatically generated with medium confidence





1. **Launch a GUI application from the command line. Get a list of all the currently running processes. Identify which process corresponds to the GUI application you just launch and kill it from the command line** **(Brown, 2020).**

* To list all the running processes, the student had to use the command ps -A. **(Iambolajiayo, 2021)**
* The GUI Application that the student used was Firefox. To identify which process corresponds with the GUI application the command used was (ps -eF | grep firefox) **(Geek University).**
* To kill the GUI application, the command used was (kill -9 1214). The student specifically used 1214 because they identified which process corresponds with the GUI application, that number was the first to pop up **(Hoffman, 2017).**

A picture containing text, electronics, black

Description automatically generated

Text

Description automatically generated

1. **Open an FTP connection to ftp.cs.brown.edu (username is anonymous and no password) or to another FTP site. Open a new terminal, navigate to the user home directory, and capture a list of the current network connections to a file called 1.txt. Quit the FTP connection. Capture a list of the current network connections to a file called 2.txt. Run a command to compare the contents of the files 1.txt & 2.txt. What difference do you see, and why is it different? Finally, delete 1.txt and 2.txt.**

* To perform the FTP connection, the student had to run the command ftp ftp.cs.brown.edu. After, it asked for a username which the student put anonymous.
* As that FTP connection was running, the student then opened a new terminal and navigated to the user home directory and capture the list of current network connections in which we saved those files as 1.txt & 2.txt.
* To save those network connections to a file you must run the commands: netstat -nltp > 1.txt and netstat -nltp > 2.txt.
* Finally, you see the difference between files 1.txt and 2.txt, the student had to use the command diff -u . (Command: diff -u 1.txt 2.txt) **(*Diff command in Linux with examples* 2021).**

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text

Description automatically generatedGraphical user interface

Description automatically generated with medium confidence

Graphical user interface, text, application

Description automatically generated

**Conclusion:**

The Kali Linux lab was a great way to introduce students to the command line and what the Linux system has to offer. It made everyone who participated in this lab accustomed and familiar with Kali Linux and its operating system as well as the tools that come along with it. Overall, this lab was a great way to brush up on the skill you already have and helped the students learn new commands that they might need in the future.

**References:**

6, A. K. A. S. H. G. U. P. T. A. 6@A. K. A. S. H. G. U. P. T. A. (2021, September 16). *Diff command in Linux with examples*. GeeksforGeeks. Retrieved June 8, 2022, from <https://www.geeksforgeeks.org/diff-command-linux-examples/>

Brown, K. (2020, November 24). *GUI software installers for Kali Linux*. Linux Tutorials - Learn Linux Configuration. Retrieved June 8, 2022, from <https://linuxconfig.org/gui-software-installers-for-kali-linux>

Foundation, T. L. (2022, January 9). *Classic sysadmin: How to move files using Linux commands or file managers*. Linux Foundation. Retrieved June 8, 2022, from <https://www.linuxfoundation.org/blog/classic-sysadmin-how-to-move-files-using-linux-commands-or-file-managers/>

Geek University. (n.d.). *List all running processes: Linux#*. Geek University. Retrieved June 8, 2022, from <https://geek-university.com/list-all-running-processes/#:~:text=The%20most%20common%20way%20to,handy%20when%20troubleshooting%20your%20system.&text=The%20most%20used%20options%20with%20ps%20are%20a%2C%20u%20and%20x>.

Hoffman, C. (2017, July 12). *How to kill a desktop application or background process on Linux*. How. Retrieved June 8, 2022, from <https://www.howtogeek.com/211153/how-to-kill-a-desktop-application-or-background-process-on-linux/>

How to Create a File in Linux | Linuxize. (2019, May 10). Retrieved June 8, 2022, from <https://linuxize.com/post/create-a-file-in-linux/>

*How to open, edit, move, and copy a file in Linux*. Hivelocity Hosting. (2021, January 29). Retrieved June 8, 2022, from <https://www.hivelocity.net/kb/how-to-open-edit-move-and-copy-a-file-in-linux/>

Iambolajiayo. (2021, June 29). *Linux list processes – how to check running processes*. freeCodeCamp.org. Retrieved June 8, 2022, from <https://www.freecodecamp.org/news/linux-list-processes-how-to-check-running-processes/>

*Linux diff command help and examples*. help and examples. (2021, November 6). Retrieved June 8, 2022, from <https://www.computerhope.com/unix/udiff.htm>

*oracle virtual box*. Moved. (n.d.). Retrieved June 8, 2022, from <https://docs.oracle.com/cd/E19253-01/806-7612/files-20/index.html>

*What is Kali Linux? Kali Linux documentation*. Kali Linux. (2022, March 30). Retrieved June 8, 2022, from <https://www.kali.org/docs/introduction/what-is-kali-linux/>