Chapter 5: Basics of the Linux Terminal

In this laboratory exercise, the student will be introduced to the basic usage of the Linux Terminal.

5.1 Laboratory Exercise

Basics of the Linux Terminal

5.1.1 Specifications

This exercise requires that students have access to a Linux machine of some sort. Ubuntu Linux was used during development for this exercise. Because the exercise focuses on the student using command line techniques, this exercise will be performed on an installation of Ubuntu Server 16.04.6. The machine will be preconfigured with many "flags" placed in various locations which the students will attempt to find.

5.1.2 Learning Objectives

- Basic Linux/Unix terminal commands
- Understanding of the Linux file system
- Understanding of key Linux directories

5.1.3 Mapping to NIST Nice Framework

This laboratory exercise is intended to familiarize the student with Linux, the Linux terminal, and the Linux filesystem. This exercise should be completed prior to attempting the other exercises. This laboratory exercise maps to the following KSAs from the NIST NICE Framework:

- Electronic Devices (K0114)

5.1.4 Necessary Background and Expected Completion Time

This laboratory exercise can be completed by students with varying background and experience. The following categories should help identify approximately how much time (in minutes) will be necessary to complete the laboratory exercise, for a student meeting the criteria for the respective experience level.

- Beginner: A student in this category has little to no experience with Linux, the Linux terminal, and the Linux filesystem.
- Intermediate: A student in this category has experience with Linux and the Linux terminal but is unfamiliar with the Linux filesystem.
- Advanced: A student in this category has experience with Linux and the Linux terminal as well as familiarity with the Linux filesystem.

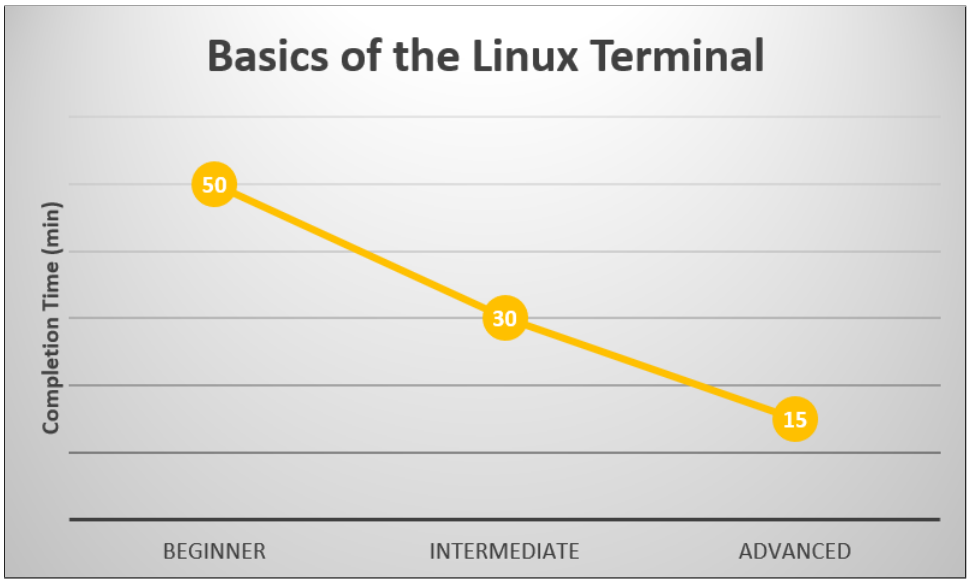

Figure 5.1: *Basics of the Linux Terminal Laboratory Exercise Expected Completion Time (min)*

5.1.5 Configuration and Setup

The machine used in this laboratory exercise is an installation of Ubuntu Server 16.04.6. It is pre-loaded with hidden flags across the filesystem (as performed by the initialization script). This machine is configured using the intialization script, listing **5.1**

Listing 5.1: *lt-initializationscript.sh*

```
#!/bin/bash

#flag1
echo "flag:\$encryptedpasswordsarekeptin/etc/shadow" >> /etc/shadow
echo "aOmpy3tFOB96wIwKAgX7GImPUuD1mLPADWXeXhZF2Hk2j" >> /etc/shadow
echo "thYYBSkDkE6ZzvkkBmWHiBoYjiDnRR3t95eEl6A1xUUUH" >> /etc/shadow
echo "wIttm0hwZxWfUbltKXU5JiqIS6rBGvk4MjEWpKmtmq8DC" >> /etc/shadow
echo "SfSPbJrr6Ny5oM9tArAF7wLQ876liujtnDONXE237iZeX" >> /etc/shadow
echo "Fi4xqO3PtdCL2rdYR4E8JTvBVL46pxqx4d23u7004NwB6" >> /etc/shadow

#flag2
echo "thingsarenotalwaysastheyappear" > /bin/weirdfile

#flag3
echo "system" > /sbin/tilapia
echo "binaries" > /sbin/salmon
echo "aren't" > /sbin/bass
echo "fishy" > /sbin/hering

#flag6
echo "itsalwaysgoodtokeeparecordofwhatversionswereinstalled" >> /var/backups/apt.
    extended_states.0

#flag8
echo "therearenogamesonthismachine!" > /usr/games/.spaceinvaders

#flag9
echo "ufwissuitedforhostbasedfirewalls" > /lib/ufw/flaaaag

#flag10
echo "ysiyndwnjceaxmdowgeyfapkfc" > /media/flag
```

5.1.6 Vulnerability List

This laboratory exercise does not contain any vulnerabilities. It's intended purpose is to familiarize the student with the Linux filesystem and navigating through Linux. The skills in this exercise will be necessary to perform the other exercises.

5.1.7 Challenges

Find as many of the flags hidden on the associated Linux machine as possible. The tasks do not have to done in order. Use the hints provided for finding each flag.

1. Flag 1 can be found where the configuration files are typically kept. Look where the passwords are cryptic.

2. Flag 2 can be found where user binaries are typically kept. Something is out of the ordinary.

3. Flag 3 can be found where system binaries are typically kept. Something seems fishy here.

4. Flag 4 can be found where device files are typically kept. Pages are typically 4K in size, but not always, where are larger pages handled?

5. Flag 5 can be found where process information is typically kept. The flag is the number of blocks in `sda2`. The number found will likely differ from the answer in the solution guide because the number of blocks in a partition varies from machine to machine.

6. Flag 6 can be found where variable files are typically kept. It is important to have a way to recall how things were earlier.

7. Flag 7 can be found where temporary files typically kept. You may have to ask about this one, the flag may be gone.

8. Flag 8 can be found where user programs are typically kept. Where might you find space invaders, maybe the flag is playing a popular childrens game (hide and seek) with you?

9. Flag 9 can be found where the system libraries are typically kept. Keep intruders out with a firewall.

10. Flag 10 can be found where removable devices are typically kept. You may have to decrypt the flag, what was the name of the cipher used? Vinegar or something like that. The key for the cipher is the name of the file which contains the ciphertext.