**E-Portfolio Linux Activity: Demonstrating Basic Linux Skills**

**Scenario: XYZ Financial Services, Inc.**

**Objective:** The objective of this e-portfolio activity is to assess undergraduate cybersecurity students' basic Linux skills. Students will demonstrate their ability to perform essential tasks in a Linux environment that are relevant to cybersecurity operations. They will create an e-portfolio showcasing their work. This e-portfolio has 3 parts: (1) Preliminary tasks that prepare your basic folder structure; (2) Building scripts that run on a CLI for five different skill areas (user management, file operations, file permissions and ownership, process management, and system information); and (3) running the scripts you built in part 2.

**Overview of Preliminary Tasks/Preparation:**

1. **Set Up a Linux Environment:** We will use a Kali Linux environment set up by ITCS on the Horizon VMware.
2. **Create Your Folders:** Create a folder structure to organize your e-portfolio files. Name your folder after your username. For example, I could set mine up with my ECU username killingsworthb:
   * /home/killingsworthb
3. **Prepare E-Portfolio Structure:** Inside your folder, create the following subfolders:
   * **Documentation**: For any textual documentation or notes.
   * **Scripts**: For storing Linux shell scripts they will create.
   * **Screenshots**: For storing screenshots of completed tasks.

**Overview of E-Portfolio Tasks**

**What are the tasks involved for this E-Portfolio Activity?** There are five tasks which are summarized below. You will find an exemplary response (with more detailed instructions from me) to this task starting on page 5 (and, if you are not familiar with Linux, you might want to walk through those detailed steps. Otherwise, you can review the Linux Commands provided in the written documents on Canvas and develop steps on your own to complete these five tasks. Remember that you are to create reflection statements for these tasks (e.g., Why This Matters)

**Task 1: User Management**

Objective: Create a new user account, set a password, and assign it to a specific group.

1. Create a new user account with the name "cyberstudent" and set the password to "secure123."
2. Add this user to the "cybersecurity" group.

**Task 2: File Operations**

Objective: Perform basic file operations in the Linux command line.

1. Create a new text file named "important.txt" in your home directory.
2. Copy "important.txt" to a subdirectory called "confidential."
3. Rename "important.txt" to "classified.txt."

**Task 3: Permissions and Ownership**

Objective: Manage file permissions and ownership.

1. Create a file named "topsecret.txt" in your home directory.
2. Change the ownership of "topsecret.txt" to the "root" user.
3. Deny all permissions to the group and others for "topsecret.txt."

**Task 4: Process Management**

Objective: Manage processes and understand system resource usage.

1. Start a background process named "myprocess" that runs the "top" command.
2. Find and display the process ID (PID) of "myprocess."
3. Terminate the "myprocess" background process.

**Task 5: System Information**

Objective: Retrieve system information and hardware details.

1. Display the system hostname.
2. List the CPU information.
3. List the available disk space.

**Reflection**

Task 1- Undertaking the user management task was a practical exercise in creating and configuring user accounts within a Linux environment. Beginning with the creation of a new user account named "cyberstudent" and setting a secure password for it, "secure123," emphasized the importance of adhering to strong security practices. Assigning the newly created user to the "cybersecurity" group ensured proper access privileges and group affiliations. This task highlighted the significance of user management in maintaining system security and organizing user permissions effectively.

Task 2- Engaging in file operations via the Linux command line provided hands-on experience with fundamental file manipulation tasks. Creating a new text file named "important.txt" underscored the simplicity of file creation commands. Copying the file to a subdirectory named "confidential" and subsequently renaming it to "classified.txt" demonstrated essential file management techniques. This task illuminated the versatility of command-line tools for organizing and manipulating files efficiently.

Task 3- Exploring permissions and ownership in Linux unveiled the intricacies of file security and access control. Creating a file named "topsecret.txt" and changing its ownership to the "root" user showcased the significance of ownership in determining file control. Denying all permissions to the group and others for "topsecret.txt" emphasized the granular control available for restricting file access. This task deepened understanding of file permissions and ownership dynamics critical for safeguarding sensitive data.

Task 4- Managing processes provided insight into controlling system resources and monitoring running applications. Initiating a background process named "myprocess" to execute the "top" command demonstrated the versatility of background tasks for executing non-interactive commands. Identifying and terminating the "myprocess" background process using its Process ID (PID) illustrated effective process management techniques. This task underscored the importance of understanding process lifecycles for optimizing system performance and resource allocation.

Task 5- Retrieving system information and hardware details facilitated a comprehensive overview of system characteristics. Displaying the system hostname provided basic identification information, while listing CPU information and available disk space offered insights into hardware specifications and resource availability. This task underscored the importance of accessing system information for troubleshooting, performance optimization, and capacity planning purposes.