# CYB 230 Module Four Lab Worksheet

Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

## Lab: Working With Files

| **Prompt** | **Response** |
| --- | --- |
| In the lab section “Using Chmod to Change Permissions,” insert your name at the command line below the ending output and include it in your screenshot. | A screenshot of a computer  Description automatically generated |
| In the lab section “Setting Special Permissions,” insert your name at the command line below the ending output and include it in your screenshot. | A screenshot of a computer  Description automatically generated |
| Implementing the sticky bit on the directory can stop people from accidentally deleting files that they don’t own. How can this technique be used to implement the concept of least privilege, and how can it be used to assure file availability? | Implementing the sticky bit on a directory is vital for enforcing the concept of least privilege and ensuring file availability. It restricts deletion permissions so users can only remove files they own, even if they have broader access to the directory. This prevents accidental or malicious deletions, helping maintain the integrity and availability of files in shared environments, thereby supporting seamless collaboration and data protection. |

## Lab: Permissions, Users, and Groups in Linux

| **Prompt** | **Response** |
| --- | --- |
| After completing the lab section “Adding Groups, Users, and Passwords,” **repeat the steps to** add another user using your first name. Provide a screenshot of the **cat** **etc/passwd** command when you are done. | A screenshot of a computer screen  Description automatically generated |
| After completing the lab section “Absolute Permission,” repeat the process using your first name as the text file. Provide a screenshot of the output.  **Note:** By default, some computer systems use the key sequence **Ctrl+Alt+F1** to access a shortcut for other programs such as the Intel Graphics Control Panel. If this is the case, you will need to change the key sequence from the default to complete this step.  To exit the tty1 or tty2 window, use the key sequence **Ctrl+Alt+F7**. | A screenshot of a computer  Description automatically generated |
| Using the **chmod** command, which commands would you use to set the following permissions to a file called **Answers.txt**? (Provide the one line used at the command line for each bulleted item.)   * User (read and write), group (execute) other (execute) * User (read, write, execute), group (read and execute) other (write and execute) * User (write), group (read) other (none) | * chmod 611 Answers.txt * chmod 753 Answers.txt * chmod 240 Answers.txt |

## Lab: Log Analysis

| **Prompt** | **Response** |
| --- | --- |
| In the lab section “Examining Windows Event Logs, IIs Logs, and Scheduled Tasks,” add your name as the top line of the file and then take a screenshot. | A screenshot of a computer  Description automatically generated |
| In the lab section “Examining Linux Log Files,” insert your name at the command line below the ending output and include it in your screenshot. | A screenshot of a computer  Description automatically generated |
| What is the importance of maintaining clean log files that are well formatted? | Maintaining clean and well-formatted log files is essential because it helps with efficient system troubleshooting and monitoring. Clean log files are easier to read and analyze, which speeds up the identification and resolution of issues. Well-formatted logs also support security measures by clearly showing all actions taken, making detecting unauthorized access or other malicious activities simpler. Additionally, clean logs are crucial for compliance with regulations that require accurate and accessible records of system activities. |