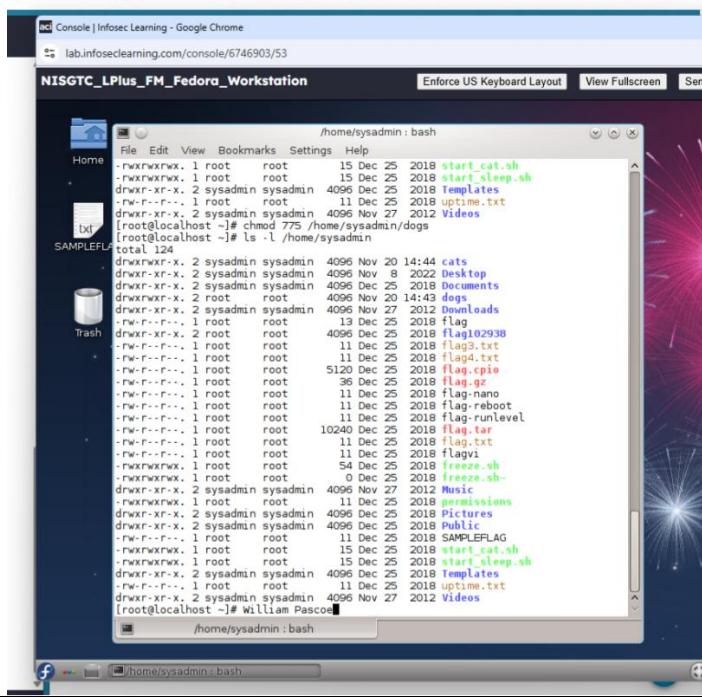
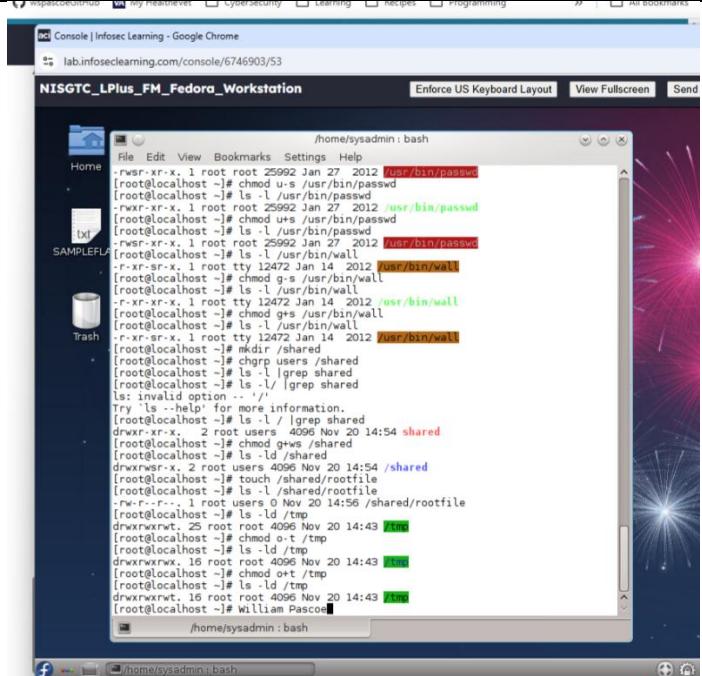


CYB 230 Module Four Lab Worksheet

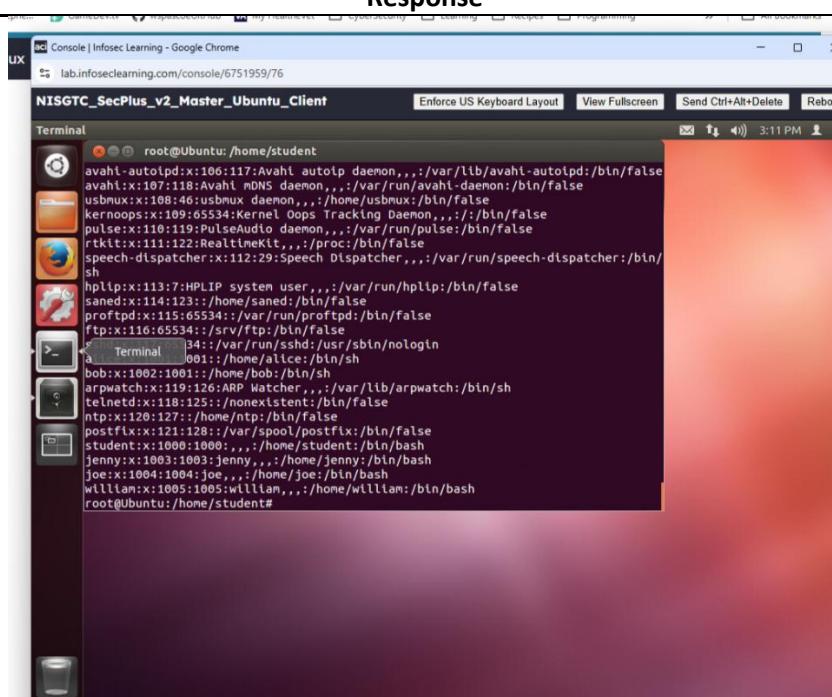
Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

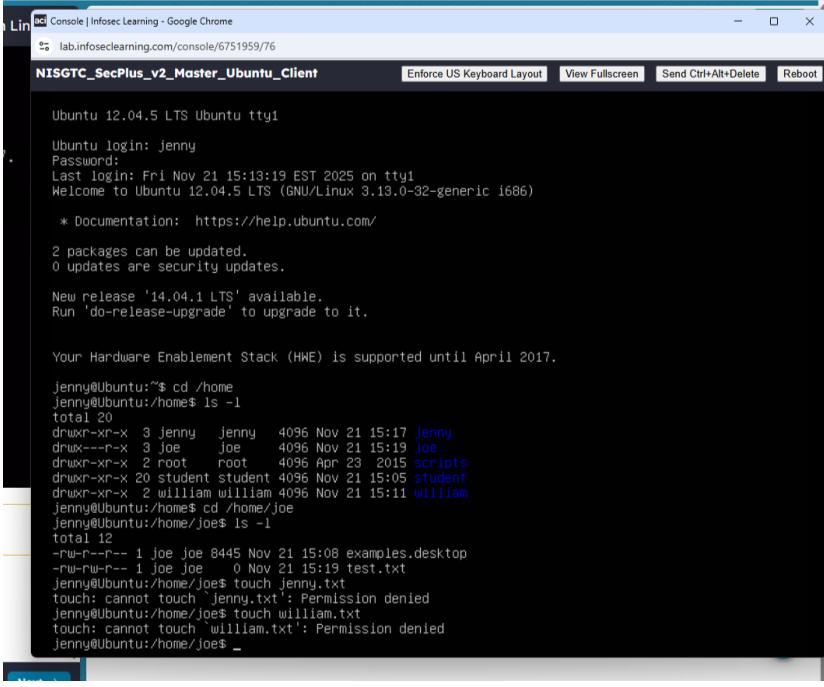
Lab: Working With Files

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 Linux desktop environment showing a terminal window titled "NISGTC_LPlus_FM_Fedora_Workstation". The terminal shows a directory listing of files and folders, including ".start_cat.sh", "Templates", "Videos", and various "flag" files. Below the listing, a command is entered: "[root@localhost ~]# chmod 775 /home/sysadmin/dogs". The user then types their name, "william Pascoe", at the command line. The terminal window has a blue header bar with the title and some icons.
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 Linux desktop environment showing a terminal window titled "NISGTC_LPlus_FM_Fedora_Workstation". The terminal shows a directory listing of files and folders, including ".start_cat.sh", "Templates", "Videos", and various "flag" files. Below the listing, a command is entered: "[root@localhost ~]# chmod u+s /usr/bin/passwd". The user then types their name, "william Pascoe", at the command line. The terminal window has a blue header bar with the title and some icons.

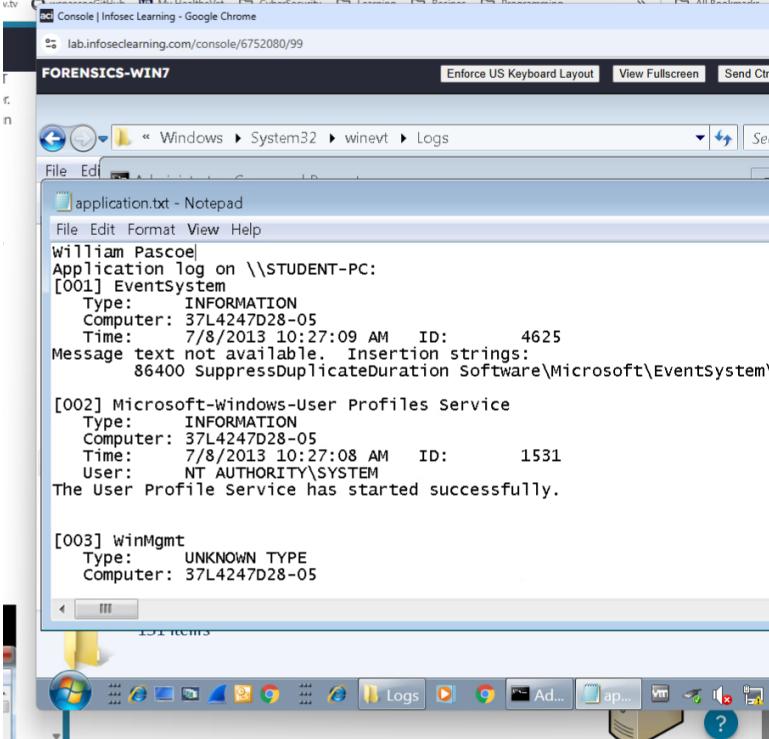
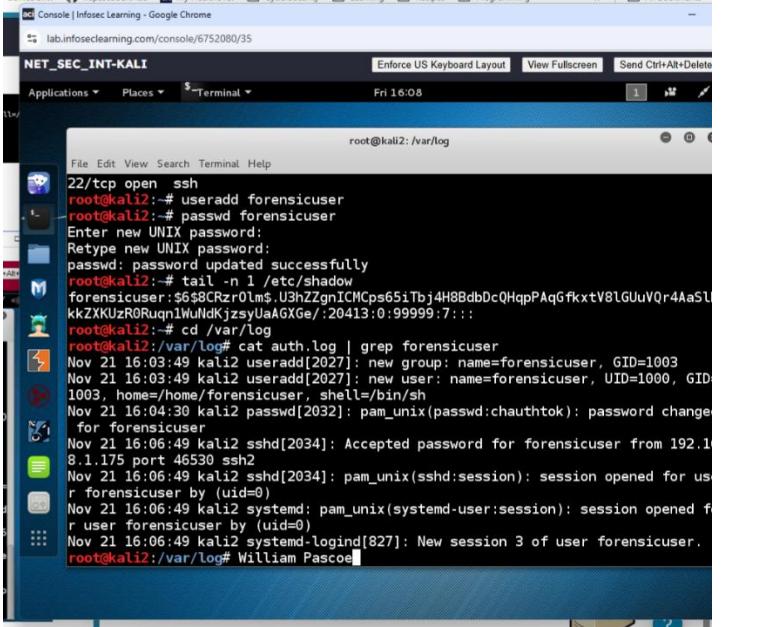
Prompt	Response
Implementing the sticky bit on the directory can stop people from accidentally deleting files that they don't own. How can this technique be used to implement the concept of least privilege, and how can it be used to assure file availability?	Using the sticky bit ensures least privilege because only the owner of the file or the root user can delete the file. This also ensures that no one else can delete it thus it will ensure availability.

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 terminal window titled "Console Infosec Learning - Google Chrome". The window shows the URL "lab.infoseclearning.com/console/6751959/76". The terminal itself has a dark background and displays the output of the "cat /etc/passwd" command. The output lists various system users and their home directories and shells. Some entries include "root@Ubuntu:/home/student", "avahi@Ubuntu:~", "usbmuxd@Ubuntu:~", and several user accounts like "jenny", "joe", and "william". The terminal window is part of a desktop environment with other icons visible in the background.

Prompt	Response
<p>After completing the lab section “Absolute Permission,” repeat the process using your first name as the text file. Provide a screenshot of the output.</p> <p>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.</p> <p>To exit the tty1 or tty2 window, use the key sequence Ctrl+Alt+F7.</p>	 <pre> Lin [Console] Infosec Learning - Google Chrome lab.infoseclearning.com/console/6751959/76 NISGTC_SecPlus_v2_Master_Ubuntu_Client Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete Reboot Ubuntu 12.04.5 LTS Ubuntu tty1 Ubuntu login: jenny Password: Last login: Fri Nov 21 15:13:19 EST 2025 on tty1 Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-32-generic i686) * Documentation: https://help.ubuntu.com/ 2 packages can be updated. 0 updates are security updates. New release '14.04.1 LTS' available. Run 'do-release-upgrade' to upgrade to it. Your Hardware Enablement Stack (HWE) is supported until April 2017. Jenny@Ubuntu:~\$ cd /home Jenny@Ubuntu:/home\$ ls -l total 20 drwxr-xr-x 3 jenny jenny 4096 Nov 21 15:17 jenny drwxr--r--x 3 joe joe 4096 Nov 21 15:19 joe drwxr-xr-x 2 root root 4096 Apr 23 2015 scripts drwxr-xr-x 20 student student 4096 Nov 21 15:05 student drwxr-xr-x 2 william william 4096 Nov 21 15:11 william Jenny@Ubuntu:/home\$ cd /home/joe Jenny@Ubuntu:/home/joe\$ ls -l total 12 -rw-r--r-- 1 joe joe 8445 Nov 21 15:08 examples.desktop -rw-rw-r-- 1 joe joe 0 Nov 21 15:19 test.txt Jenny@Ubuntu:/home/joe\$ touch jenny.txt touch: cannot touch 'jenny.txt': Permission denied Jenny@Ubuntu:/home/joe\$ touch william.txt touch: cannot touch 'william.txt': Permission denied Jenny@Ubuntu:/home/joe\$ _ </pre>
<p>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.)</p> <ul style="list-style-type: none"> • 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) 	<p>chmod 611 Answers.txt chmod 753 Answers.txt chmod 240 Answers.txt</p>

Lab: Log Analysis

Prompt	Response
<p>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.</p>	 <p>The screenshot shows a Windows desktop environment. A Notepad window is open, displaying event log entries. The first entry is:</p> <pre>application.txt - Notepad File Edit Format View Help William Pascoe Application log on \\STUDENT-PC: [001] EventSystem Type: INFORMATION Computer: 37L4247D28-05 Time: 7/8/2013 10:27:09 AM ID: 4625 Message text not available. Insertion strings: 86400 suppressDuplicateDuration Software\Microsoft\EventSystem\</pre> <p>Subsequent entries include:</p> <ul style="list-style-type: none"> [002] Microsoft-Windows-User Profiles Service [003] WinMgmt <p>The taskbar at the bottom shows icons for various applications like File Explorer, Task Manager, and a browser.</p>
<p>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.</p>	 <p>The screenshot shows a Kali Linux terminal window. It starts with adding a user:</p> <pre>root@kali2:~# useradd forensicuser root@kali2:~# passwd forensicuser Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully</pre> <p>Then it tail-seds the auth.log file for the new user:</p> <pre>root@kali2:~# tail -n 1 /etc/shadow forensicuser:\$6\$CRzr0lMs.U3hZZgnICMCps65iTbj4H8BdbDcQHqpPAqGfkxtV8lGUuVQr4Aa5L kkZXKUzR0Ruqn1uUldkjzsyluaAGXGe/:20413:0:99999:7:::</pre> <pre>root@kali2:~# cd /var/log root@kali2:/var/log# cat auth.log grep forensicuser Nov 21 16:03:49 kali2 useradd[2027]: new group: name=forensicuser, GID=1003 Nov 21 16:03:49 kali2 useradd[2027]: new user: name=forensicuser, UID=1000, GID=1003, home=/home/forensicuser, shell=/bin/sh Nov 21 16:04:30 kali2 passwdd[2032]: pam_unix(passwd:chauthtok): password changed for forensicuser Nov 21 16:06:49 kali2 sshd[2034]: Accepted password for forensicuser from 192.168.1.175 port 46530 ssh2 Nov 21 16:06:49 kali2 sshd[2034]: pam_unix(sshd:session): session opened for user forensicuser by (uid=0) Nov 21 16:06:49 kali2 systemd: pam_unix(systemd-user:session): session opened for user forensicuser by (uid=0) Nov 21 16:06:49 kali2 systemd-logind[827]: New session 3 of user forensicuser. root@kali2:/var/log# William Pascoe</pre>
<p>What is the importance of maintaining clean log files that are well formatted?</p>	<p>The reason that you want to keep log files clean and well formatted is so that when you are looking for information, like searching for a particular event, you are not bombarded with a bunch of old entries and that the ones that do return are formatted to be able to read them quickly to determine if they warrant further investigation.</p>



Southern
New Hampshire
University