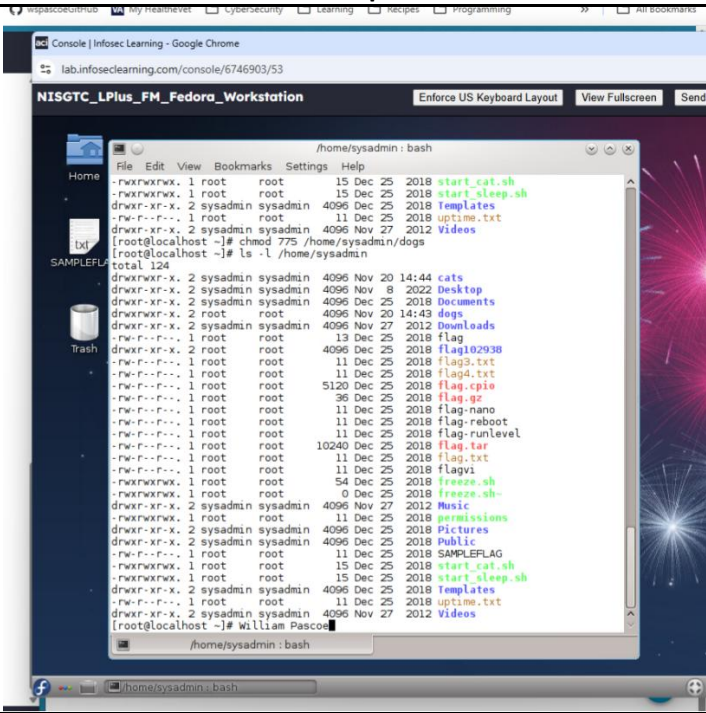
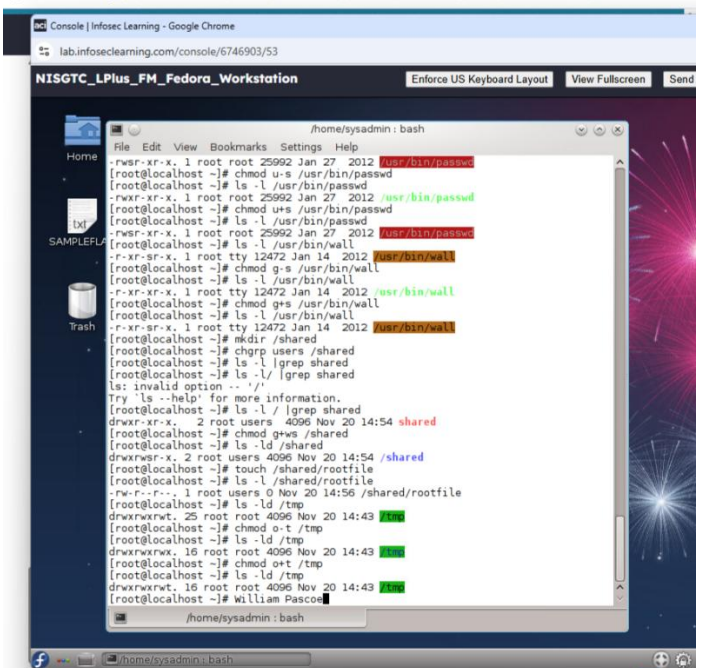


## CYB 230 Module Four Lab Worksheet

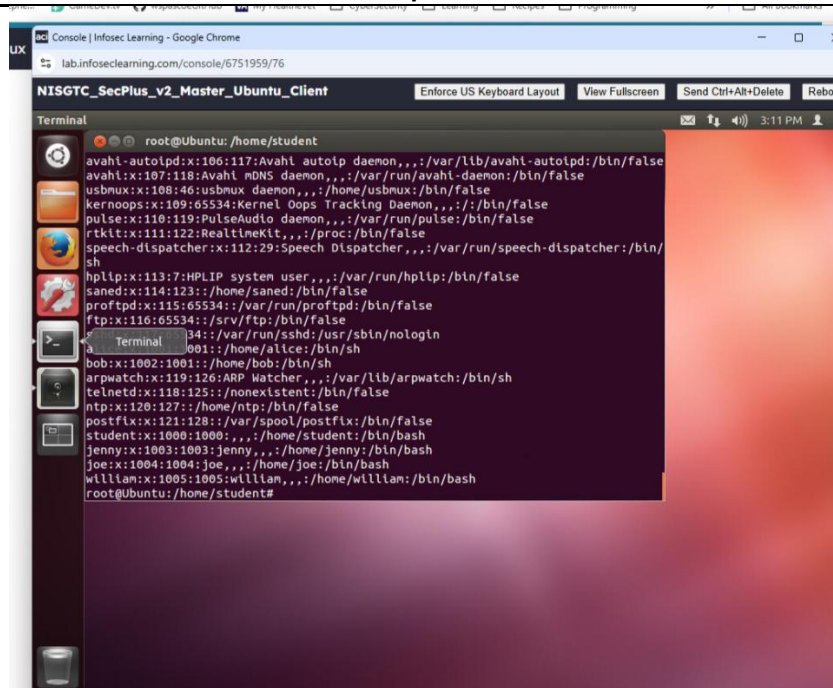
Complete this worksheet by replacing the bracketed phrases in the Response column with the relevant information.

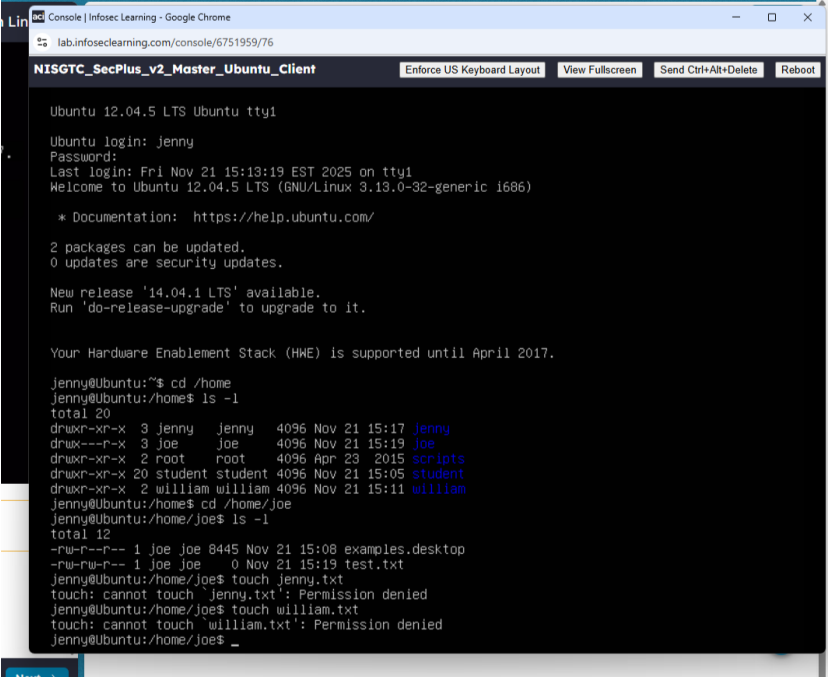
### Lab: Working With Files

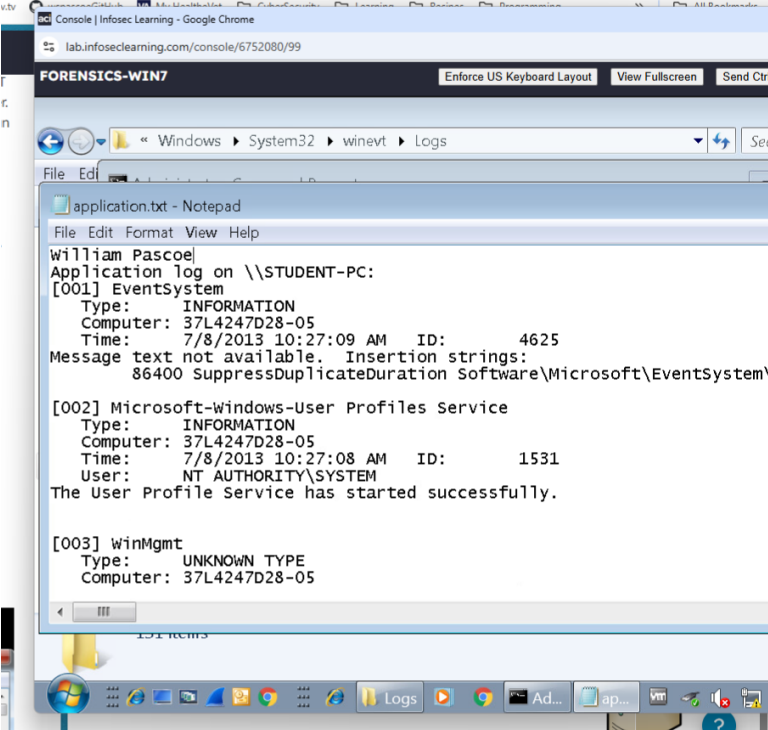
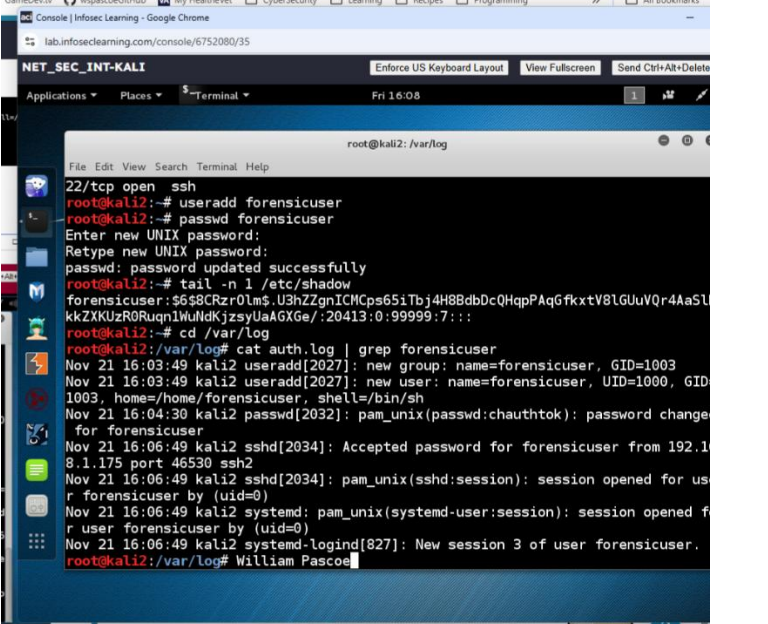
Prompt	Response
In the lab section "Using Chmod to Change Permissions," insert your name at the command line below the ending output and include it in your screenshot.	
In the lab section "Setting Special Permissions," insert your name at the command line below the ending output and include it in your screenshot.	

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," <b>repeat the steps to add another user using your first name.</b> Provide a screenshot of the <b>cat etc/passwd</b> command when you are done.	 <pre> root@ubuntu: /home/student# cat /etc/passwd avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/bin/false pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false rkit:x:111:122:RealtimeKit,,,:/proc:/bin/false speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false saned:x:114:123:/:/home/saned:/bin/false proftpd:x:115:65534:/:/var/run/proftpd:/bin/false ftp:x:116:65534:/:/srv/ftp:/bin/false sshd:x:117:117:/:/var/run/ssh:/bin/false alice:x:1001:1001:/:/home/alice:/bin/sh bob:x:1002:1002:/:/home/bob:/bin/sh arpwatch:x:119:126:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh telnetd:x:118:125:/:/nonexistent:/bin/false ntp:x:120:127:/:/home/ntp:/bin/false postfix:x:121:128:/:/var/spool/postfix:/bin/false student:x:1000:1000:/:/home/student:/bin/bash jenny:x:1003:1003:jenny,,,:/home/jenny:/bin/bash joe:x:1004:1004:joe,,,:/home/joe:/bin/bash william:x:1005:1005:william,,,:/home/william:/bin/bash root@ubuntu: /home/student#                     </pre>

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><b>Note:</b> By default, some computer systems use the key sequence <b>Ctrl+Alt+F1</b> 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 <b>Ctrl+Alt+F7</b>.</p>	 <p>The screenshot shows a terminal window titled 'NISGTC_SecPlus_v2_Master_Ubuntu_Client'. It displays the Ubuntu 12.04.5 LTS login process for user 'Jenny'. After login, the user runs 'ls -l' in the /home directory, showing permissions for various files and directories. The output shows that Jenny has read and write permissions for her own files, while other users have different permissions. The terminal also shows updates and hardware information.</p>
<p>Using the <b>chmod</b> command, which commands would you use to set the following permissions to a file called <b>Answers.txt</b>? (Provide the one line used at the command line for each bulleted item.)</p> <ul style="list-style-type: none"> <li>User (read and write), group (execute) other (execute)</li> <li>User (read, write, execute), group (read and execute) other (write and execute)</li> <li>User (write), group (read) other (none)</li> </ul>	<pre>chmod 611 Answers.txt chmod 753 Answers.txt chmod 240 Answers.txt</pre>

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 titled 'application.txt - Notepad' is open, displaying the following text:</p> <pre> William Pascoe Application log on \\STUDENT-PC: [001] EventsSystem 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\EventsSystem\  [002] Microsoft-Windows-User Profiles Service Type: INFORMATION Computer: 37L4247D28-05 Time: 7/8/2013 10:27:08 AM ID: 1531 User: NT AUTHORITY\SYSTEM The User Profile Service has started successfully.  [003] WinMgmt Type: UNKNOWN TYPE Computer: 37L4247D28-05     </pre> <p>The background shows the Windows Event Viewer window with the path 'Windows &gt; System32 &gt; winevt &gt; Logs' selected.</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. The user has executed the command 'cat /var/log/auth.log   grep forensicuser'. The output shows several log entries related to useradd and sshd, including the name 'William Pascoe' at the bottom.</p> <pre> root@kali2: /var/log 22/tcp open  ssh root@kali2:~# useradd forensicuser root@kali2:~# passwd forensicuser Enter new UNIX password: Retype new UNIX password: passwd: password updated successfully root@kali2:~# tail -n 1 /etc/shadow forensicuser:\$6\$8CRzr0Lm5.U3hZ2gnICMcp65iTbj4H8BdbDcQHqpAqGfKxtV8lGUuVQr4Aa5L kkZXKUzR0Ruqn1WuIdKjzsyUaAGXGe/:20413:0:99999:7::: 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 passwd[2032]: pam_unix(passwd:chauthtok): password change for forensicuser Nov 21 16:06:49 kali2 sshd[2034]: Accepted password for forensicuser from 192.1 8.1.175 port 46530 ssh2 Nov 21 16:06:49 kali2 sshd[2034]: pam_unix(sshd:session): session opened for us r forensicuser by (uid=0) Nov 21 16:06:49 kali2 systemd: pam_unix(systemd-user:session): session opened f r 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 looking for information, like searching for a particular event, you are not bombarded with a bunch of opld entries and that the ones that do return are formateed to be able to read them quickly to determine if they warrant further investigation.</p>

