Jesua Gonzalez

Ethical Hacking

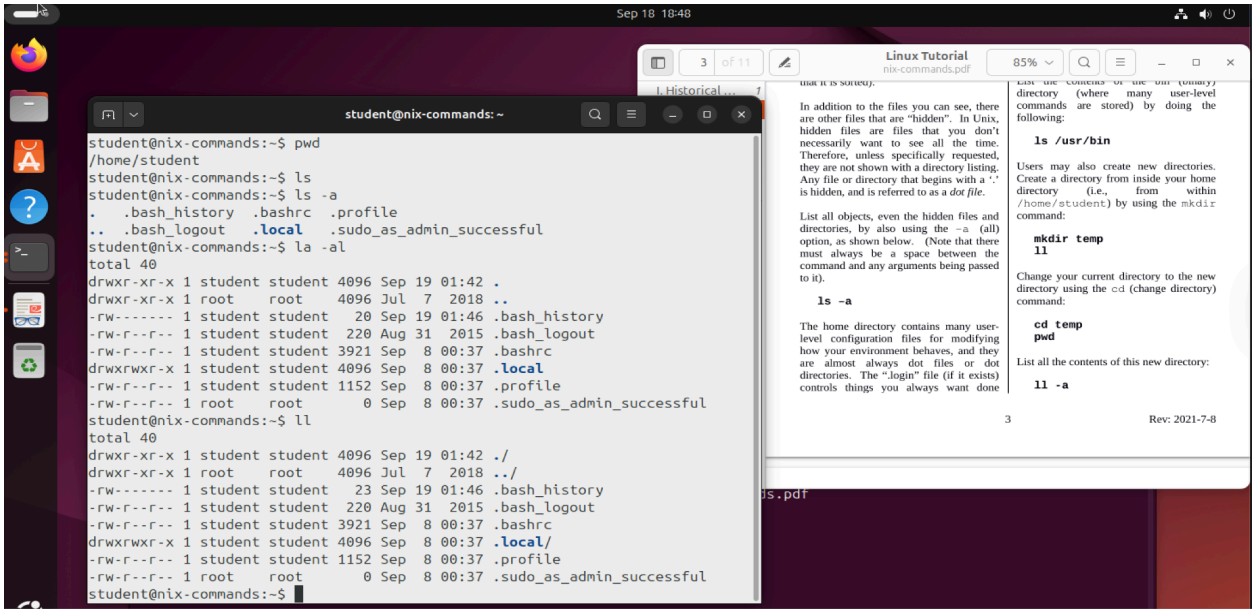
Linux Fundamentals & System Administration

Thu Sep 18

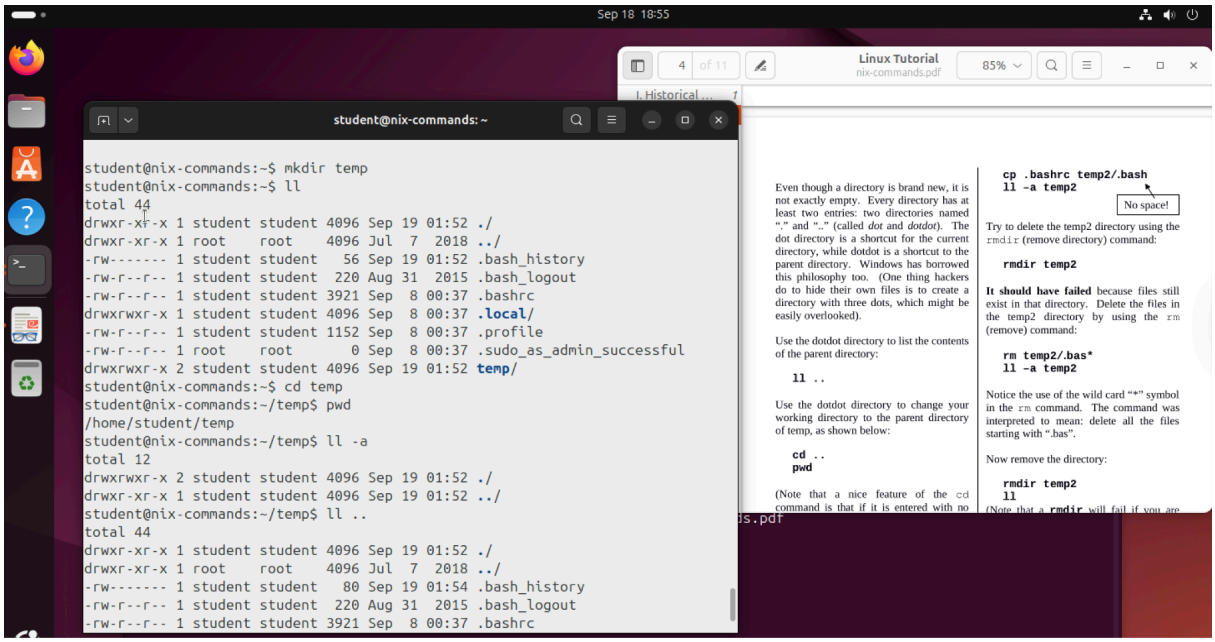
Through these interactive labs, I have learned fundamental Linux skills that are key to my success in penetration testing and overall ethical hacking. The Labtainer exercises helped me develop core competencies in user administration, file system management, and command-line navigation. These skills form the groundwork for diving into the more complex world of cybersecurity and future technical techniques I may encounter. The first lab introduced me to the most commonly used commands to navigate around directories and files. In essence, I was able to locate text files or patterns using commands like grep alongside commands such as find. I was also exposed to ways of creating/deleting new directories or files while simultaneously applying the correct permissions where needed, using commands such as chmod. In addition, I was able to understand the way in which a script is created using Leafpad, one of many editors, and then executing the new script. The demonstration used was pinging a known web server like Google.com to confirm my network IP was up and running.

In the second lab, I was able to further comprehend the foundation of user access management. To further explain, I was able to create 3 different users who each had a certain purpose and task. The first user, Bob, was added using useradd while I was in root admin. I was able to then create Bob’s password, but also making sure it expires after he attempts to log in; this was done through the passwd program. Besides Bob, Mary was also created in order to be added to the Bakers group to access key files for her to conduct her duties. Lastly, Lisa’s user account was made the same way as Bob's and Mary's, but she was granted privileged access. Lisa was added using usermod just as Mary, and then was able to remove/delete users no longer needed. Overall, these labs gave me a greater understanding of linux operations.

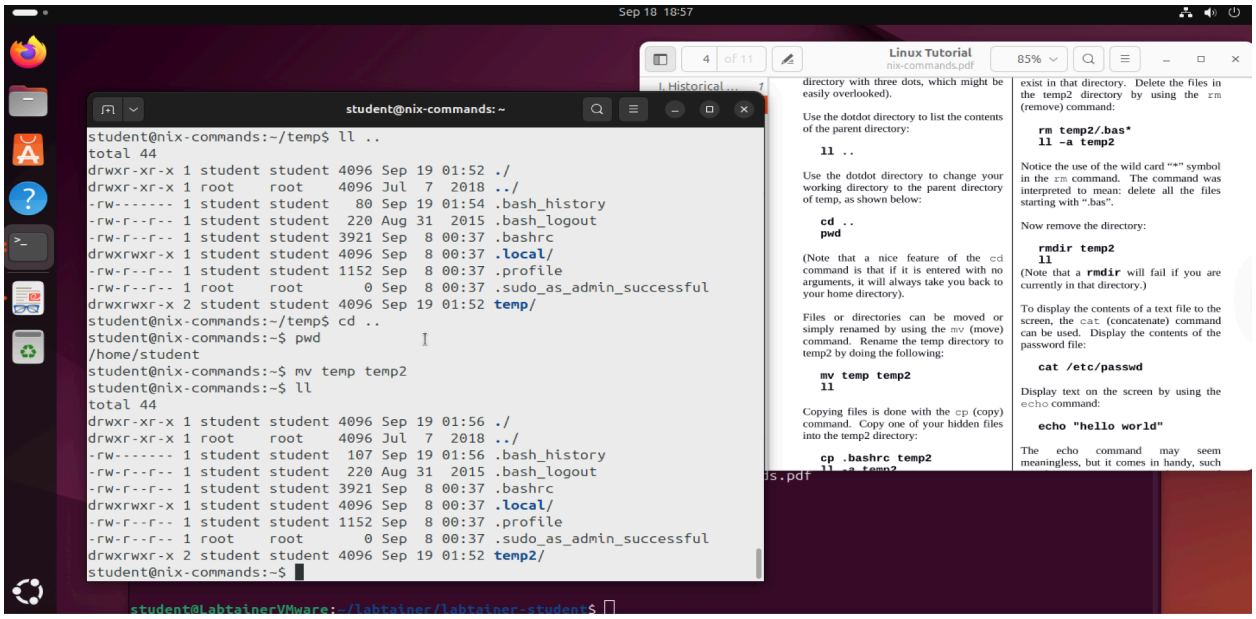
Lab 1: Nix-Commands



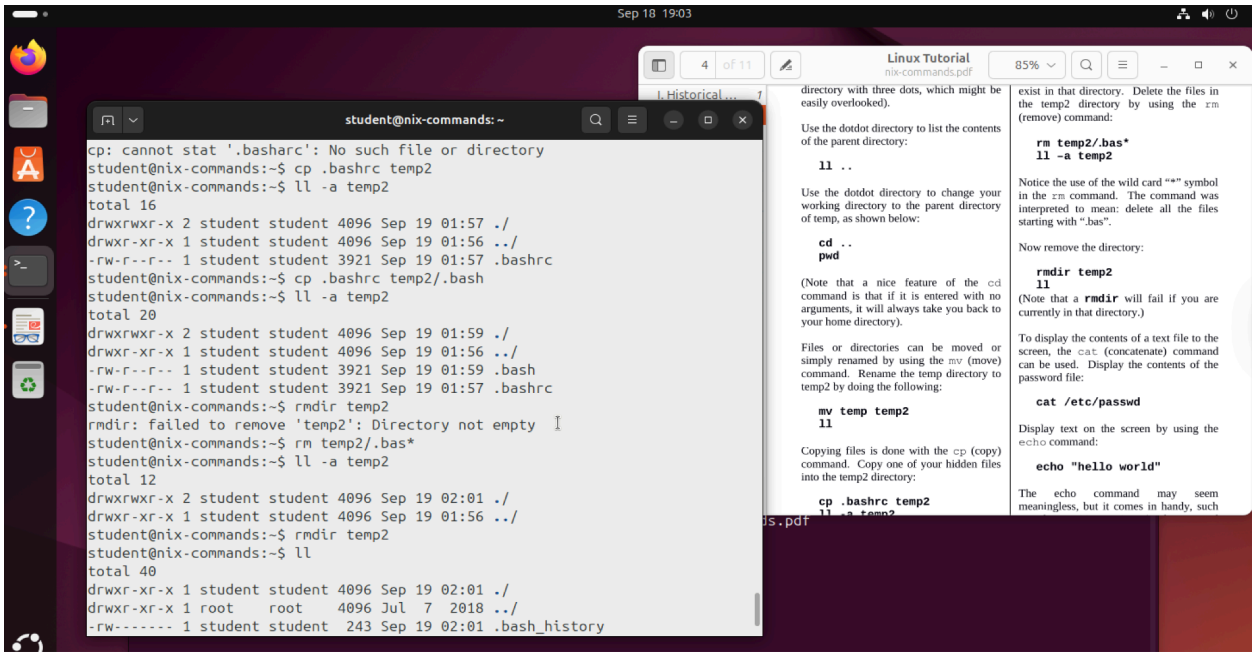
- Starting this lab, we see that we'll be working with the command line interface. First, 'pwd' is used to print out our current directory. 'ls' is then used to display any files and content in the current directory. Similarly, 'ls -a' lists hidden text files that start with a '.' and 'll' will be able to display their permissions and file details.



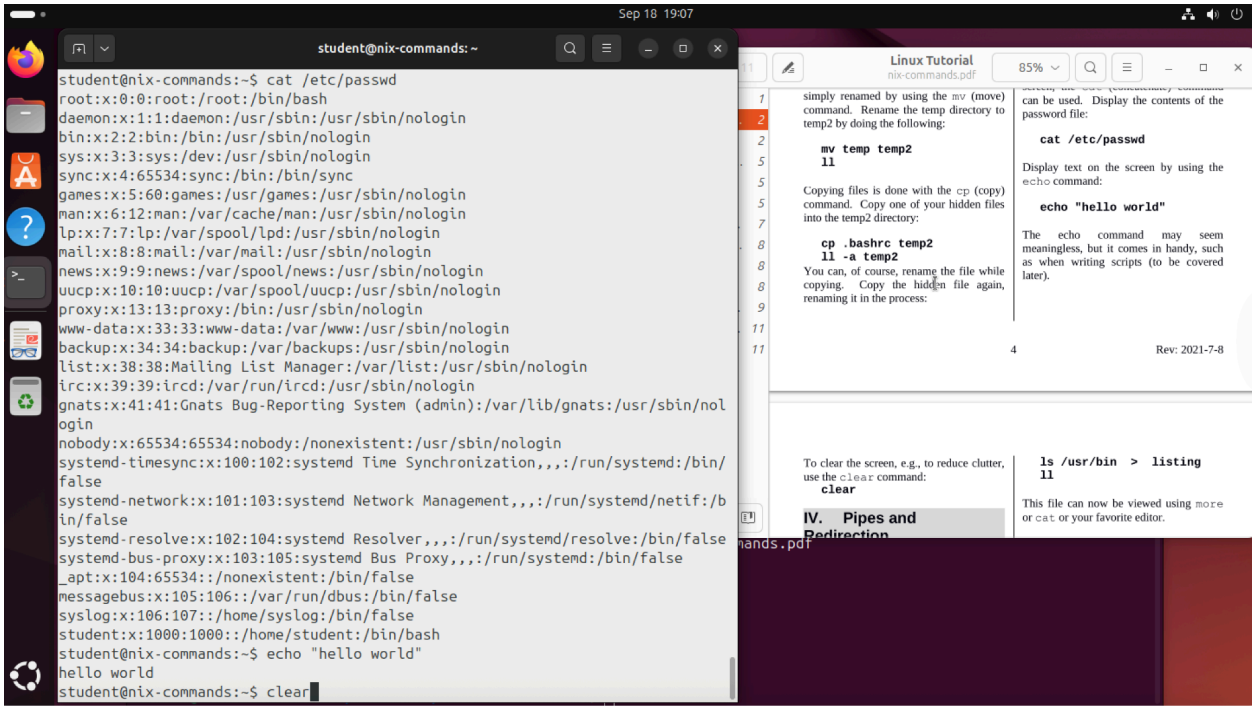
- Here we use 'mkdir', a command to create a new directory labeled temp. I am then able to enter that directory using the 'cd' command, short for change directory. And as before, 'll -a' helps display all files and their details, but combining 'll' with '..' will display content and details of the outside or parent directory before we entered "temp".



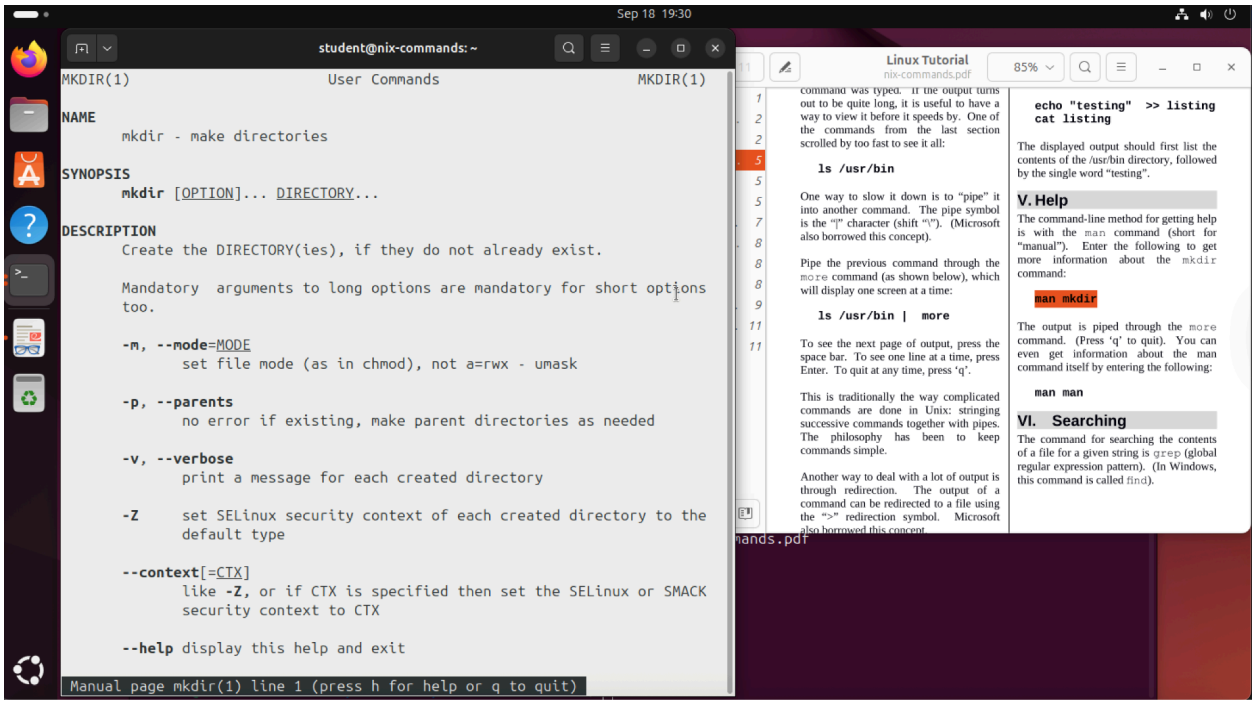
- Note that '..', otherwise known as dotdot, can also be used with 'cd' to change to the parent directory without specifically stating the path to it. I then use the 'mv' command to rename temp to temp2. This command is also able to move files or directories to other locations besides just renaming them.



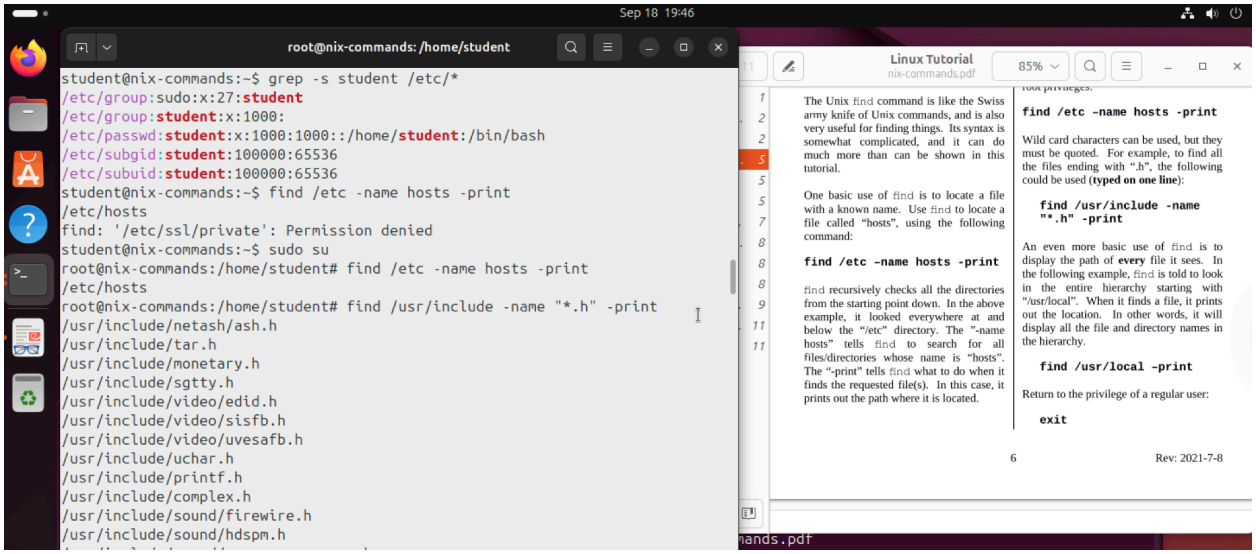
- I was able to copy a file named .bashrc into my temp2 directory using the 'cp' command. But there is also a way to copy a file into a directory using 'cp' as before, and then when specifying the location, you can add / and rewrite he file name in this case .bashrc to just .bash. I then explore the 'rm' command to remove all files starting with .bash using the '*' wildcard. We remove files first because a directory can't be removed if not empty.



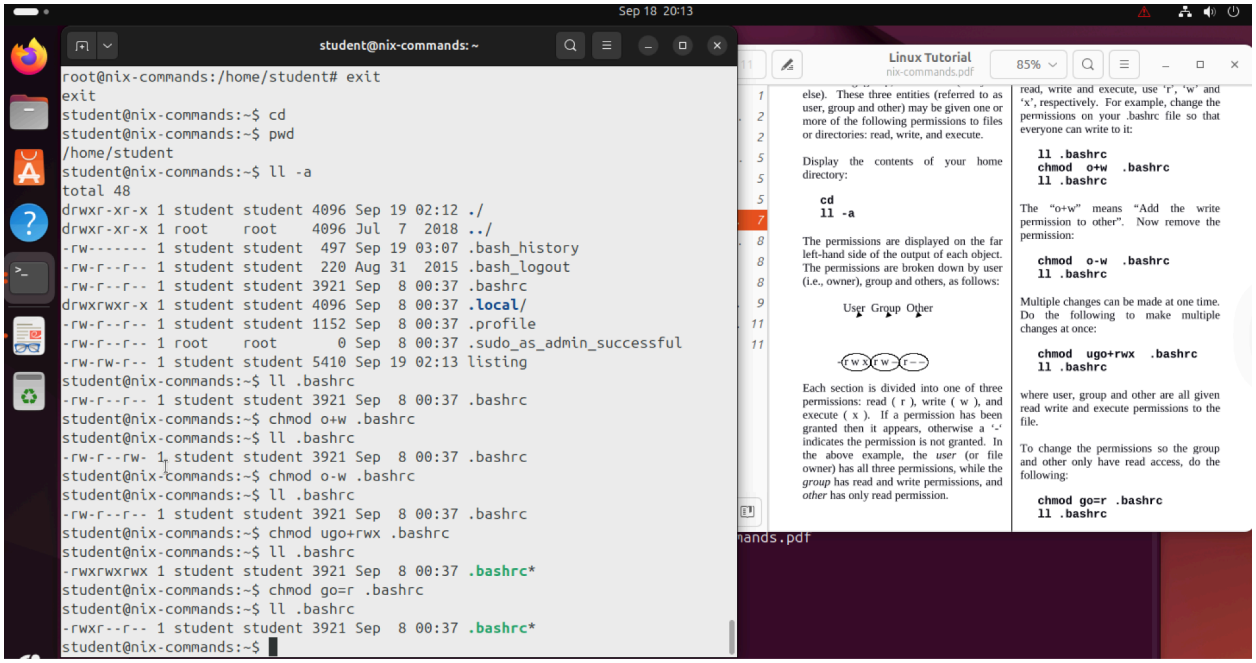
- Here I can read and display file contents using the ‘cat’ command. As well as being able to display writing on the terminal using the ‘echo’ command. In order to have a clean terminal, we can simply write ‘clear’ and the display gets cleared.



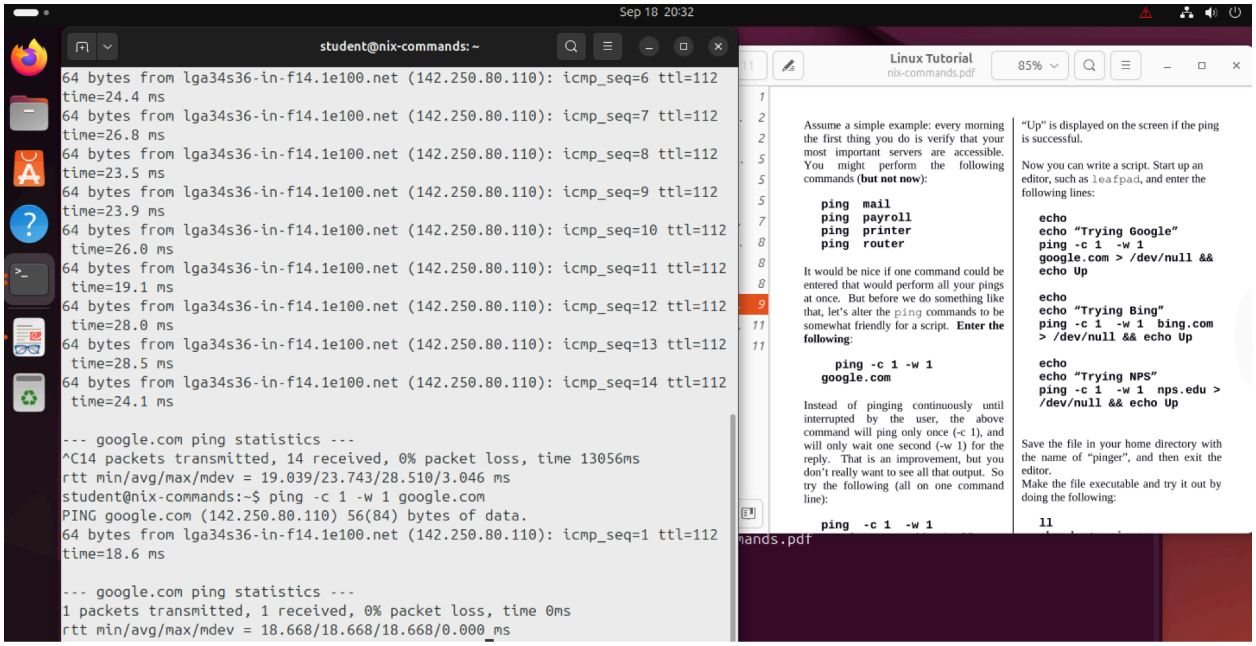
- The ‘man’ command is a very useful tool that helps look in the manual for help in understanding a command or its associated attributes. It's sort of like a dictionary for commands.



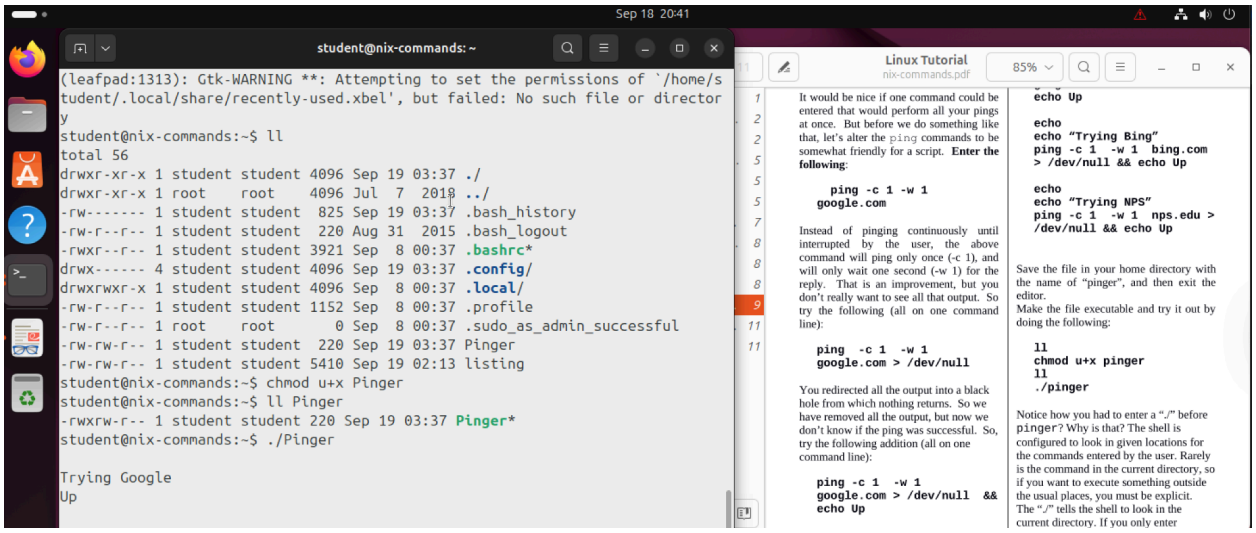
- The 'grep' command allows searching all files in reference to a certain keyword or text pattern. On the other hand, the 'find' command searches through subdirectories for a filename and file attributes.



- I explored file permissions in this section, recalling that 'll -a' displays file details and all files/directories, even hidden ones. Permissions are grouped by 3 classes: User, Group, and Other. The first character in the permissions detail is either a 'd' for directory or blank '-' for a file type. 'rwx' or read, write, execute are the permissions that can be given per group, but of course can be changed. 'chmod' is the command used for changing perms followed by the class initial and add or subtract symbol and the perm.

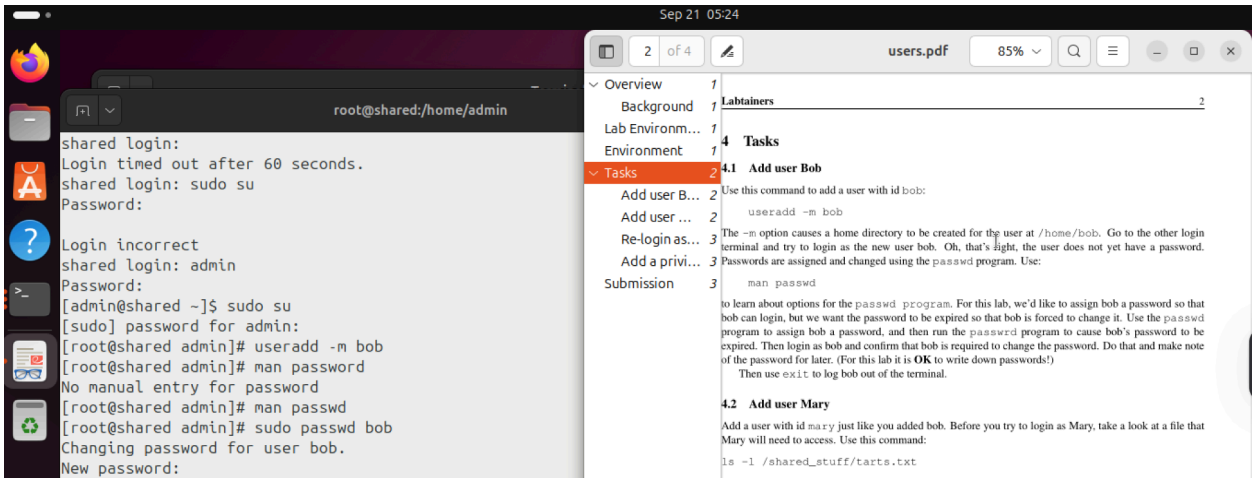


- The ‘ping’ command gives us the ability to check our connection to the outside world. The image shows a ping of 1 ICMP packet to google.com, which results in 0% packet loss, concluding a successful connection test.

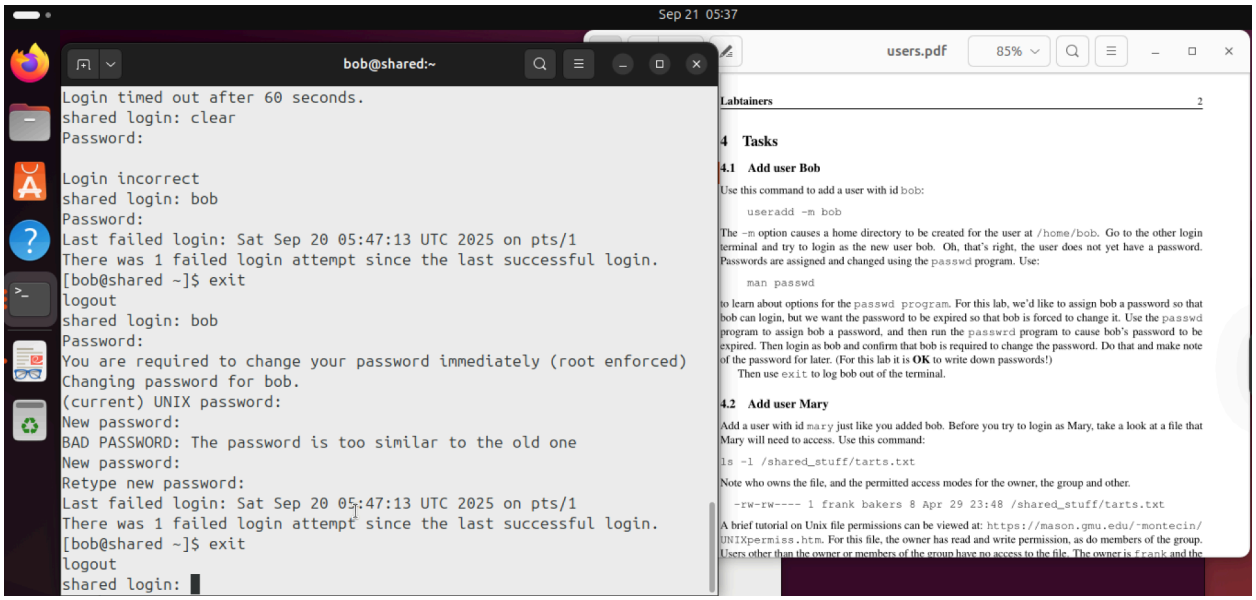


- Bringing back ‘echo’, we can utilize it when using Leafpad, a text editor that can help create a script and ‘ping’ many sites at once. Once leafpad is opened when then create pings just as before while using ‘echo’ to display text on the terminal. The file is saved to the home directory, where the User permission is granted the power to execute the script. To run the script, ‘./’ is used to tell the shell the script can be found in the current working directory. The outputs spat out are the process in which echo was used to confirm its functionality by saying it's “trying” and then confirming its success by replying “Up”.

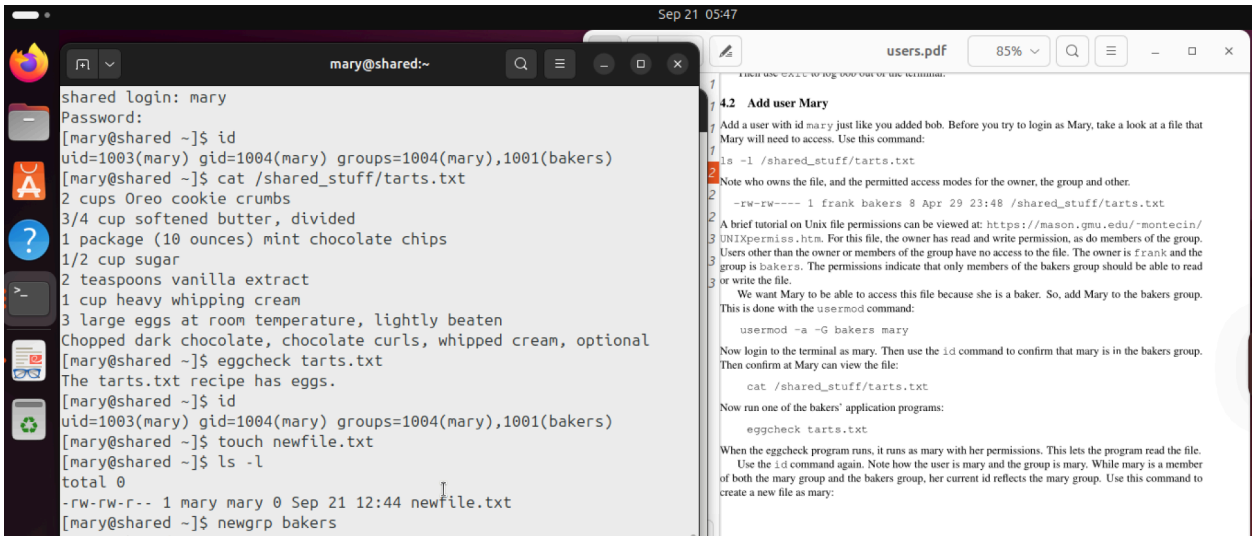
Lab 2: Users



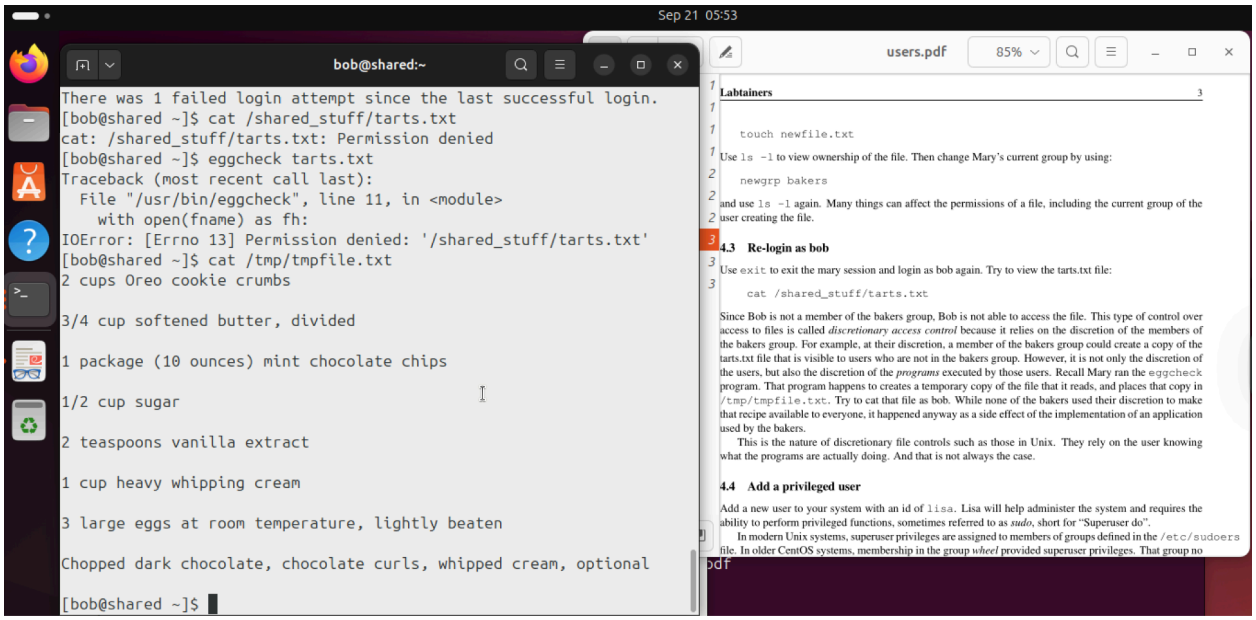
- After logging into my admin account, I elevate my access to root user using ‘sudo su’ command. Therefore, I can create new users using ‘useradd’ and ‘-m’ adds a home directory for the user in this case, Bob. In addition, using the passwd program allowed me to create a password for Bob to log in. I also used ‘sudo passwd -e Bob’ to expire his password which will prompt him to create a new password when attempting to log in.



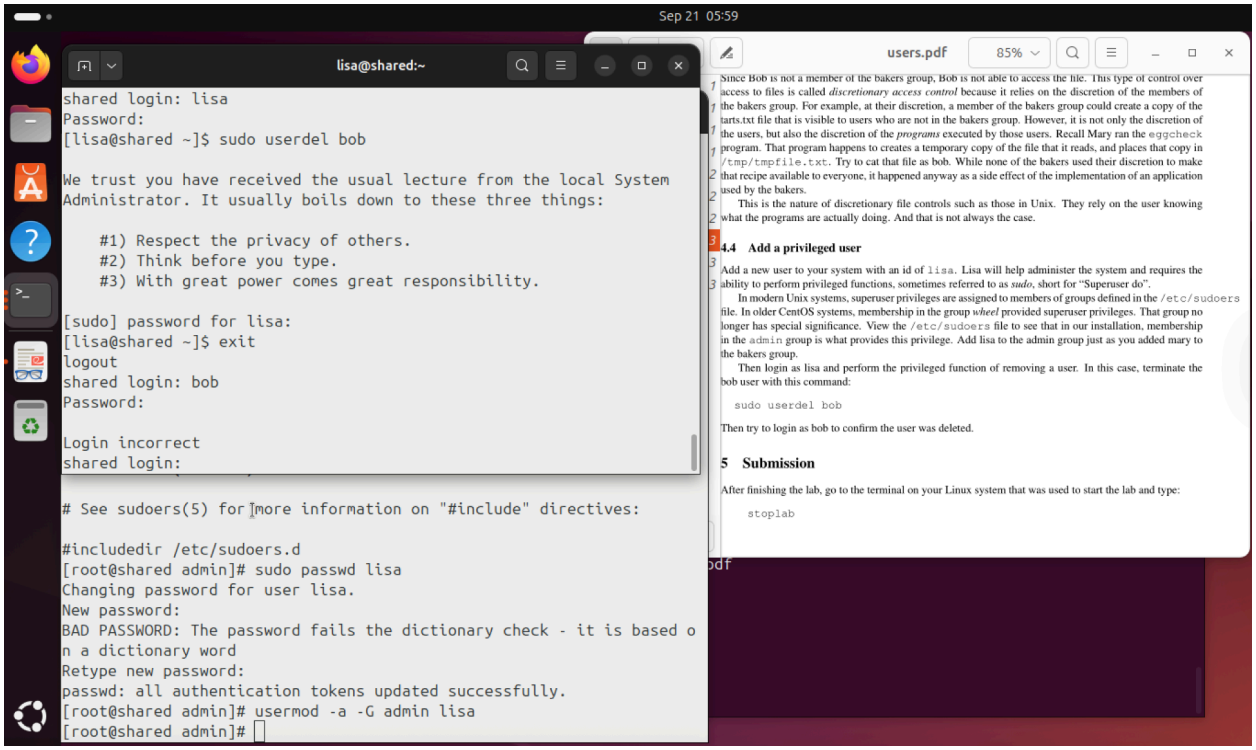
- As Bob I tried loging in before the expire option was but in place and was able to successfully log in. To leave the user account, a simple ‘exit’ is given to the terminal, which logs me out. Once the ‘-e’ or expire option was put in place, and I attempted to log in again I was swiftly prompted to change my password. There were some issues related to password security, in which the Unix password regulation does not allow similar or too short a password, so creating strong password unrelated to the User is very much obliged.



- In the same manner Bob was created Mary was also added as a user using 'useradd'. Mary had to pertain to a certain group to access certain files to perform her baker duties. On the admin terminal, 'usermod' was used to add Mary to the baker group. So on the Mary terminal, we can input 'id' and it now displays bakers as part of one of Mary's groups that she is in. Resulting in file access and being able to view the shared info.



- Here Bob is not part of any group and can not access the same files as Mary due to the discretionary access control that the bakers group have set up. But when Bob runs the same egg check program as Mary, he is denied permission due to his status, but the program has already ran and stores a temporary file on his system, but it was not shown on the terminal due to his status. But due to the program creating a temporary file, Bob can access that file with a simple 'cat' command, a big downside to bad configuration of a program in regards to its original set of permission rules.



- Lastly, Lisa was a user created with privileged access to help with administrative work. She was added to the special file of sudo users '/etc/sudoers/' with the command 'usermod -a -G admin lisa'. When logging into Lisa, she can now use the 'sudo' command to escalate her power and use certain commands. In this example, she can do 'sudo userdel bob', which removes Bob from the system completely.

```
[root@shared admin]# sudo passwd -S bob
passwd: Unknown user name 'bob'.
[root@shared admin]#
```

- To confirm, we can check the status of Bob's password, which returns unknown user, meaning that there is no longer a user under Bob. You can also try logging into Bob's account, but it will not be successful.

Reflection Section

1. How do Linux file permissions contribute to system security?

- File permissions play a major role when it comes to system security because one of the major concepts of cybersecurity is confidentiality, meaning files should always be set up so that only those who should know, do know. Unmanaged permissions can lead to open vulnerabilities that threat actors can exploit and cause damage. With file permissions, users, groups, and other groups are restricted on what they can read, write, or execute.

2. What are the potential security risks of improper user management?

- Improper user management can lead to a whole list of negatives, such as unauthorized access for non-users to sensitive data, or you can have users who weren't configured correctly being able to escalate their own privileges. Strong user management will prevent these events from happening, and it secures users from small things like password management to user permissions.

3. How might an attacker exploit weak file permissions during a penetration test?

- An attacker might exploit weak file permissions in many ways. For example, bad file configuration can have unwanted users or groups accessing confidential files, and if the wrong permissions are set, these files can be overwritten or data can be stolen. An attacker can simply go around opening files using the ‘cat’ command based on the file permissions displayed when ‘ll -a’ is used.

4. Why is command-line proficiency essential for cybersecurity professionals?

- The CLI is home to lots of cybersecurity tools, such as nmap, tcpdump, Wireshark, etc. As well as its versatility with a lot of different OS models, it is very common and being able to understand the CLI will give an edge against, say a GUI in terms of efficiency and precision.

5. What challenges did you encounter during the labs, and how did you overcome them?

- Some challenges I faced when completing the labs were understanding the switches that follow commands. I was able to figure my way through by using the ‘man’ command to open up the manual and read up on the command and its functionality. There were also times of stumbling over the same issue, but taking a quick break or some time to refocus and back track to understand where I went wrong has helped instead of simply trying to push through with no progress.

6. How do these fundamental skills relate to advanced ethical hacking techniques?

- In advanced hacking, many techniques are built upon the foundations of the command line, file permissions, scripting, and privileged escalation. Understanding these everyday concepts allows for critical thinking to then perform better techniques that can promote more efficient and precise results.

Concluding Summary

The Labtainer exercises helped me develop core competencies in user administration, file system management, scripting and command-line navigation. Thus helping me prepare for more advanced ethical hacking techniques that require understanding how these topics function and work alone or together. Creating users such as bob, mary and lisa has exposed me to file permissions and management in coordinating users into groups or specific roles. This provides insight on how defense against attackers can be set up but also how vulnerabilities made present themselves if not careful. When playing with ping it helped me learn how to quickly diagnose connection issues or even create my own script that can automate the process of connectivity to a number of servers. Moving forward, I will continue to build on these fundamentals through scripting, regular permission audits on my personal device, and controlled lab practice so I can safely progress to more advanced techniques to ensure the confidentiality, integrity, and availability of data for clients and further develop my career in cybersecurity.