Your experience with the lab
- Key concepts or skills learned
- Challenges faced
- Overall takeaways

Lab 1:
This lab taught me the functions of echo, date, ls, and pwd. This was a beginner lab so there weren't any challenges faced here. Overall I'm able to see some beginner commands and how Linux can be used. There are a lot of possibilities and I can't wait to see what I can do.

Lab 2:

This lab helped me become more comfortable navigating and managing files in a Linux environment. I learned how to use both absolute and relative paths, as well as commands like ls, cp, mv, and rm to manipulate files and directories. One challenge I faced was dealing with permission issues when copying system directories, but it helped me understand how Linux handles access control. Overall, the hands-on steps reinforced how powerful and efficient the command line can be. This lab gave me a stronger foundation for future work in cybersecurity and system administration.

Lab 3:

This lab helped me get hands-on experience using the vi editor and practicing essential text-editing commands. I learned how to navigate through a file, insert and delete text, search for words, and copy and paste lines using vi's command mode. One challenge I faced was remembering which keystrokes belonged to command mode versus insert mode, but practicing each step made it easier. I also gained a better understanding of how powerful vi is for editing system files directly from the terminal. Overall, this lab strengthened my confidence using vi and showed me how important these skills are for working in Linux environments.

Lab 4:

This lab gave me practical experience managing user and group accounts in Linux using terminal commands. I learned how to create users, assign passwords, modify default shells, add users to groups, and manage group ownership of files. One of the biggest challenges was remembering the correct flags for commands like useradd, groupmod, and usermod without mixing them up. Working through these tasks helped me better understand how Linux handles permissions, identity, and account structure behind the scenes. Overall, this lab strengthened my confidence with administrative tasks and showed how essential user and group management is in system administration and cybersecurity.

Lab 5:

This lab helped me understand how password cracking works in practice by creating users with different password complexities and using John the Ripper to test their strength. I learned how

to export password hashes, run cracking tools in wordlist mode, and see firsthand how quickly weak passwords can be recovered. A challenge I faced was choosing passwords that fit each requirement while still being realistic enough for the cracking tool to detect. Running John the Ripper also showed me how dramatically password complexity affects cracking time. Overall, this lab reinforced the importance of strong password practices and gave me valuable experience with a real penetration-testing tool.

Lab 6:

This lab gave me hands-on experience working with Linux permissions, group ownership, umask values, and SGID settings, which are all essential for secure file-sharing environments. I learned how to create users and groups, assign primary and secondary group memberships, configure directory permissions, and control access using octal permission values. One challenge I faced was keeping track of when to switch between users and understanding how each permission change affected access for different accounts. Setting and unsetting SGID permissions also helped me better understand how shared project directories maintain consistent group ownership. Overall, this lab strengthened my understanding of Linux access control and how proper configuration is crucial for collaboration and security.

Lab 7:

This lab helped me understand how Linux manages storage by having me inspect disk devices, create a virtual disk, format it, mount it, and interact with it like a real partition. I learned important concepts such as loop devices, filesystems, mounting points, and how tools like fdisk, parted, and df reveal system-level storage details. One challenge I faced was keeping track of which commands needed sudo and making sure I was working with the correct loop device so I didn't accidentally modify a real system partition. Mounting and unmounting the virtual disk also showed me how Linux separates physical storage from the directory structure, which helped the concepts make more sense. Another key insight was seeing that /cyse becomes empty after unmounting, proving that a mount point is just a temporary access location for a filesystem. Overall, this lab strengthened my understanding of disk management and gave me practical experience that is important in cybersecurity, system administration, and digital forensics.

Lab 8:

This lab helped me get hands-on practice writing and executing shell scripts using Bash, which made me more comfortable automating tasks in Linux. I learned how to use the shebang line, conditional statements, user input with read, and basic file-checking commands to make scripts interactive and functional. One challenge I faced was making sure my scripts ran without errors, especially when checking whether an input was a file, directory, or nonexistent. Running the scripts also helped me understand the importance of file permissions, since the script had to be made executable before it would run. Overall, this lab strengthened my confidence in shell scripting and showed me how powerful and efficient automation can be in cybersecurity and system administration.

Lab 9:

This lab helped me understand how Linux handles user management, automated backups, and scheduled tasks using cron. I learned how to write a script that creates timestamped tar archives of a user's home directory, compresses them, and stores them safely in /var/backups. One challenge I faced was figuring out how to configure crontab so the backup script would run every 3 minutes, since the cron syntax can be confusing at first. Once I learned the correct format (*/3 * * * *), it helped me see how powerful and flexible automated system tasks can be. Overall, this lab strengthened my shell scripting skills and showed me how important backup automation and cleanup routines are for maintaining system stability and security.

Lab 10:

This lab helped me get more comfortable with subnetting by walking through each step of calculating network, broadcast, and host ranges. I learned how to break down an IP address using the subnet mask to determine block sizes and valid host addresses. One challenge I faced was keeping the binary conversions and subnet increments organized, especially when working with different prefix lengths. Overall, the lab strengthened my confidence in subnetting and gave me a clearer, more structured way to approach similar problems in the future.

Lab 11:

This lab allowed me to compare how NAT and bridged network modes affect a virtual machine's connectivity. I learned that NAT allows the VM to access the Internet through the host, while bridged mode connects the VM directly to the local network, which can change its IP and accessibility. Observing differences in IP addresses, routing tables, and connectivity helped me understand how network configuration impacts communication. Overall, the lab highlighted the practical effects of different VM network modes and their importance in networking and cybersecurity tasks.