**Getting Familiar with Linux System Administration**

**Goal and Deliverables**

Getting familiar with Linux system administration.

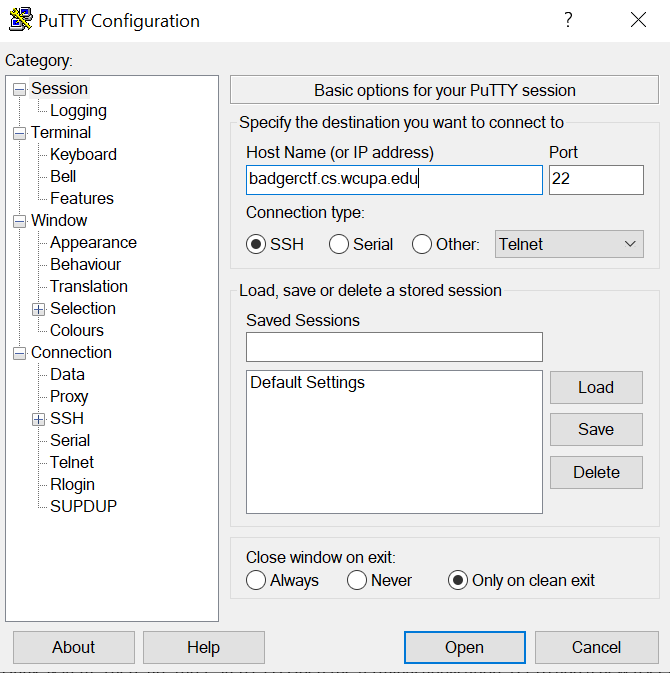
Deliverables: Please answer all of the question inside this lab report and submit it to the D2L submission folder.

Note that different Linux distribution may have different commands for the same purpose. So, the first thing you want to do is to check the distribution of the Linux system using command “***cat /etc/\*-release***”. Then, you could search specific commands like “ubuntu command for adding a user” or “redhat command for adding a group” or “manjaro command for update”. Here, “ubuntu, redhat, manjaro” are different Linux distrubtions, and “adding a user, adding a group, update” are the functions you want to reach.

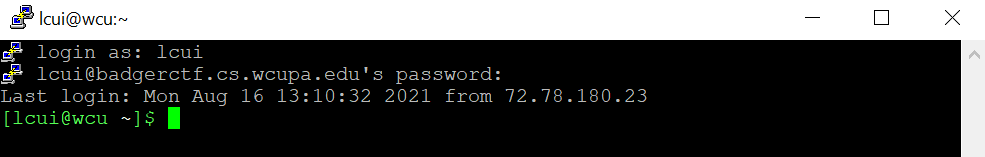
**1. Remote login**

Step 1: login to the Linux server, badgerctf. As soon as you log in, you will be automatically under your “home” directory.

1. For windows users, SSH software is helpful for remote login. If you don’t have a preferred one, Putty is a good choice. Here is the webpage to download Putty: <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>. After you download Putty, please run it, and you will see the following interface.



1. Mac users could use command like “ssh username@servername” in Terminal to login the server remotely.
2. Then, you need to enter username (my username is lcui, you have different one) and password. You will see a screen like the one below. Note that, when you enter the password, it display nothing. Please just enter the password and then click “Enter”.



Step 2: Let’s try some Linux command to get familiar with the system

|  |  |
| --- | --- |
| **Commands** | **Notes** |
| pwd | list the path of the current directory you are in |
| ls | list the content of the current directory |
| ls -l | list the content of the current directory, in long format |
| ls -a | list all the content of the current directory, including the hidden files |
| ls -al |  |
| mkdir CSC302 | make a new subdirectory under the current directory, called CSC302 |
| cd CSC302 | change directory into CSC302 |
| pwd | You can see the path has changed |
| nano test.txt | nano is a text editor. You are editing a file named test.txt. Type something into the file and follow the instructions on the bottom of the screen and save. ^ means Ctrl. |
| ls -l | You can see the new file you just created. Pay attention to the permissions of the file. |
| chmod 777 test.txt | You can see the permissions of the file has changed. It grants all the permissions to yourself (owner), group members, and all others. |
| ls -l | List the file again, and you will see the permissions change from “-rw-r- -r- -” to “-rwxrwxrwx”. |
| *explore some other permissions using chmod command and use ls –l to show the differences in the permissions setup.* | |

Step 3: show the commands you have tried by typing command “history”.

Please attack the screenshots of commands you tried here.

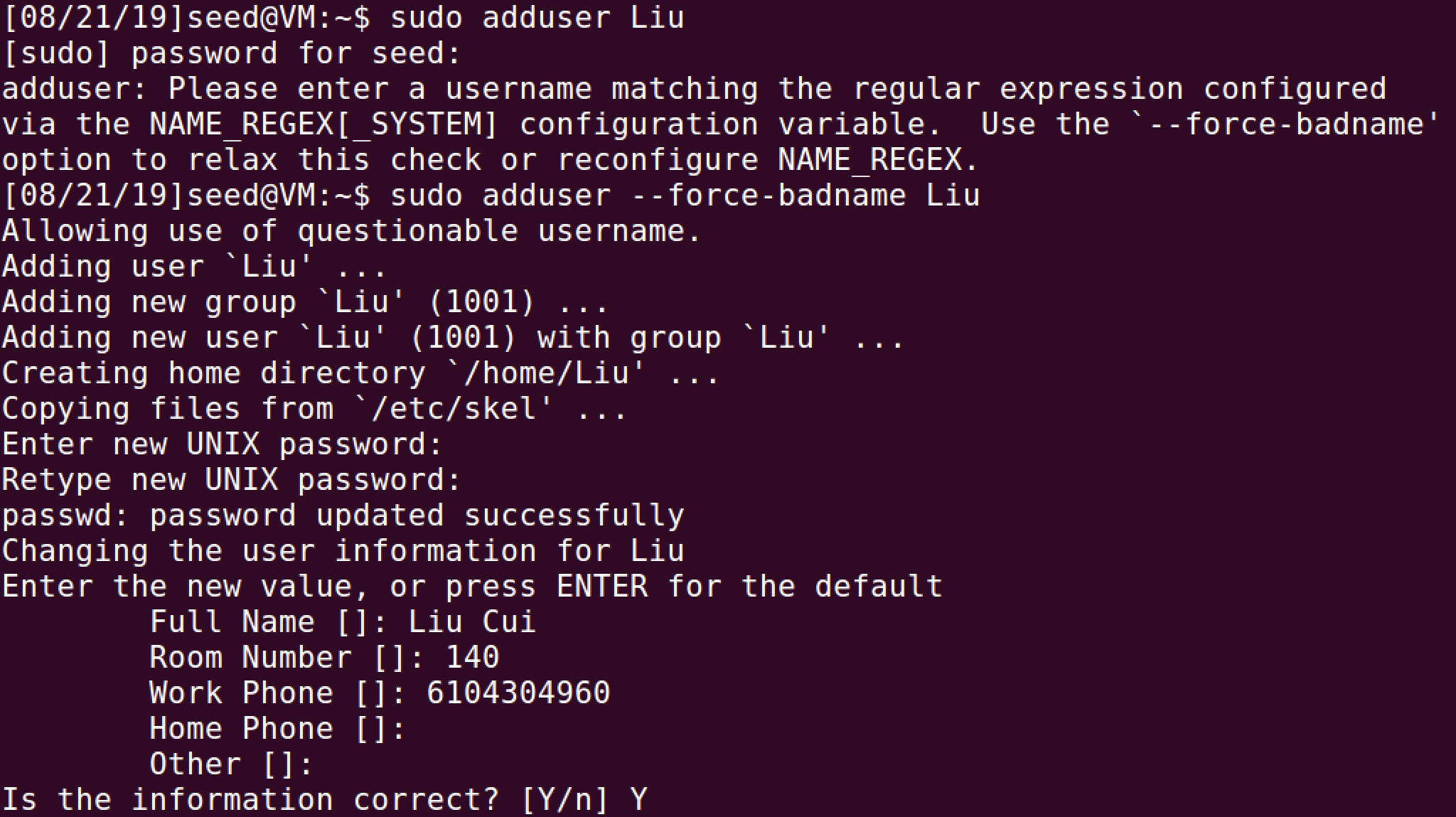
Text

Description automatically generated

**2. System Administration and Hardening**

Step 4: Set up user accounts

Setting up user accounts is the very basic operation you need to conduct, since you are not the only user for the Linux system. There are three steps: (1) Open the terminal application; (2) To add a new user in Ubuntu run ***sudo adduser username***; (3) Enter password and other needed information to create a user account on Ubuntu server.



Enter optional user information here

To overwrite the regular expression, you need to use –force-badname

Enter password here

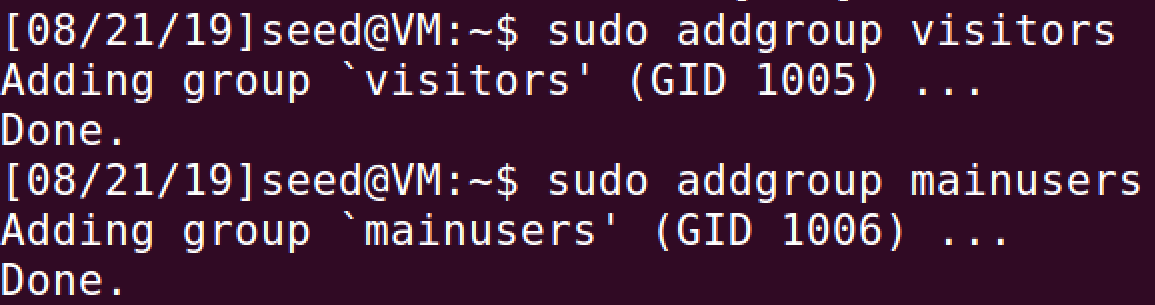
System information about this user

Enter password (can be found in Lab 1) here

If you want to delete a user account, please use command ***sudo deluser username*** or ***sudo userdel username***

Step 5: Set up groups

Please create at least three users (follow the above steps) before setting up groups. Use command ***sudo addgroup groupname*** or ***sudo groupadd groupname*** to create groups.



If you want to delete a personalized group, user command ***sudo delgroup groupname*** or ***sudo groupdel groupname***

Please show all of the users in the system by using command *cat /etc/passwd*

Text

Description automatically generated

Please show all of the groups in the system by using command *cat /etc/group*

*Text

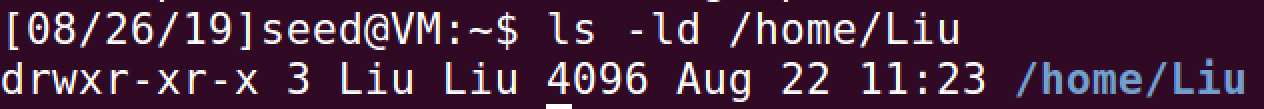
Description automatically generated*

*Text

Description automatically generated*

Step 6: Configure authorization policies

When a new user is created, the adduser utility creates a brand new home directory named /home/username. If your server will be home to multiple users, you should pay close attention to the user home directory permissions to ensure confidentiality. By default, user home directories in Ubuntu are created with world read/execute permission. This means that all users can browse and access the contents of other users home directories. This may not be suitable for your environment. Let’s configure appropriate authorization policies from verify current user home directory permissions by using following syntax: *ls –ld /home/username*



The above output shows that the directory /home/Liu has world-readable permission. To learn how to modify the permission on a file or a folder, please use command ***man chmod***. It shows everything about the permission modification that you need to know. ***man*** is the abbreviation of manual. You could use the syntax ***man commandname*** to check manuals for all commands.

Please remove the world executable permission to one of your user’s home directory, and attach the screenshot of ls - ld /home/username to show the result.

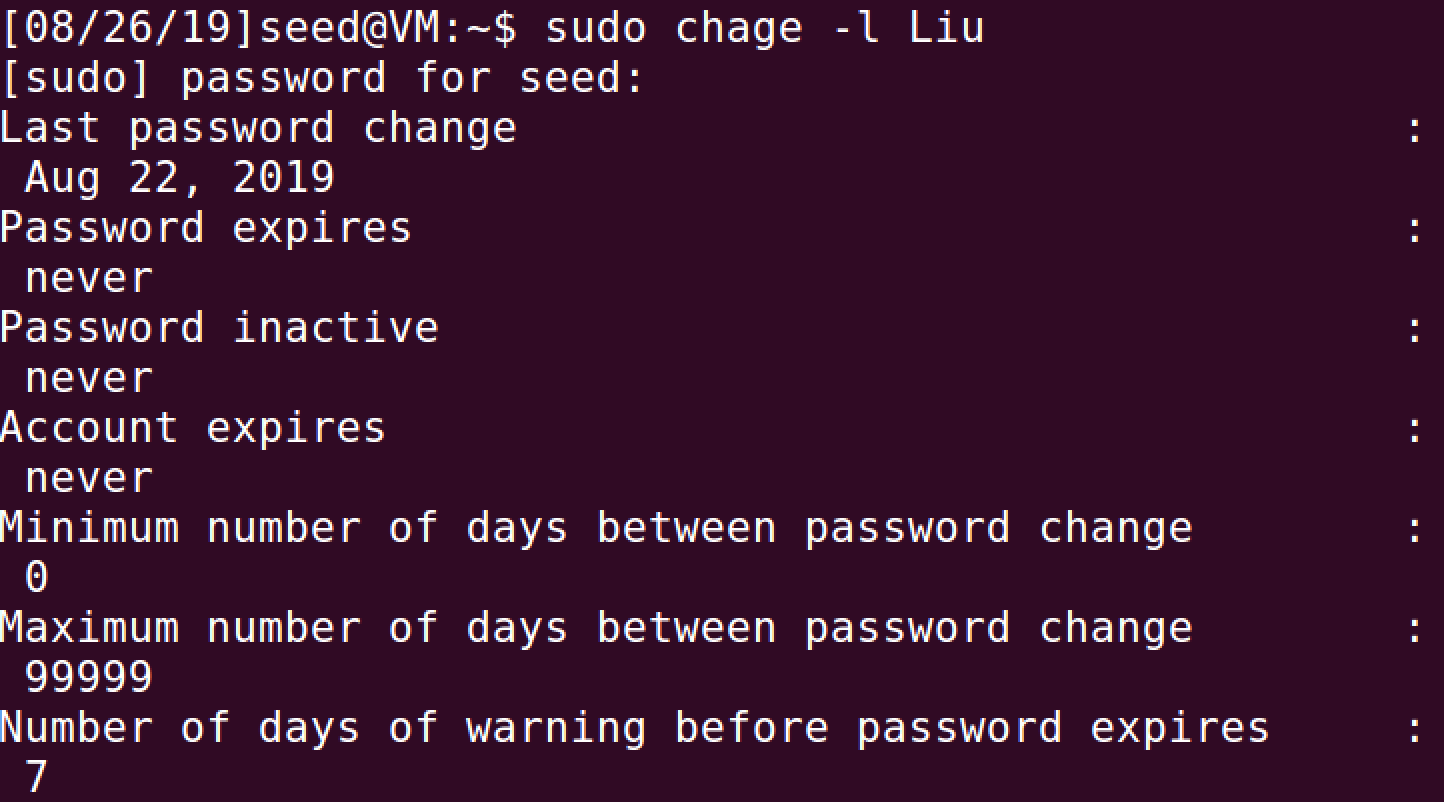
Graphical user interface, text, application, chat or text message

Description automatically generated

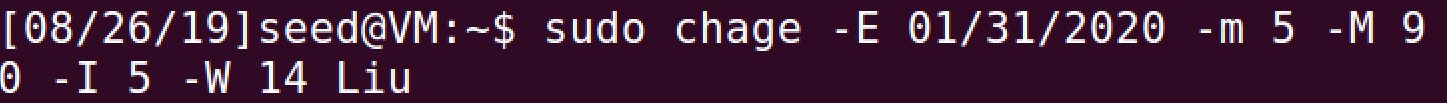
Step 7: appropriate authentication policies

A strong password policy is one of the most important aspects of your security posture. By default, Ubuntu requires a minimum password length of 6 characters, as well as some basic entropy checks. If you want to check the password requirements, please go to files -> etc -> pam.d -> passwd.

When creating user accounts, you should make it a policy to have a minimum and maximum password age forcing users to change their passwords when they expire. Before enforcing the limits, please check the current status of a user account by using syntax: *sudo chage -l username*. You will get information such as last password change, password expires, password inactive, etc. Please see the following figure as an example



If you want to change the expiration date (-E) to 01/31/2020, minimum password age(-m) of 5 days, maximum password age (-M) of 90 days, inactivity period (-I) of 5 days after password expiration, and a warning time period (-W) of 14 days before password expiration:



Then, use sudo chage -l username to verify changes. Please attach the screenshot here.

Text

Description automatically generated

Step 8: Install patches and updates, ensure all patches and updates are applied

One of the important operating system hardening practice is to install all patches and updates.

First, let us apply updates and patches on Linux by using command ***sudo apt-get upgrade*** or ***sudo pacman -Syu***.

Then, we need to get updated software list for Ubuntu by using command *sudo apt-get update* or *sudo pacman -Syu.* It will show you the number of upgradable packages. If you want to read the details, please use command *apt --list upgradeable*. It marks the package names in different colors. To upgrade individual packages, please use command *sudo apt install packagename*. For example, if you need to upgrade firefox, you can use command *sudo apt install firefox* to do that.

Please updates and patches your Ubuntu systems and show that you have 0 upgradeable packages.

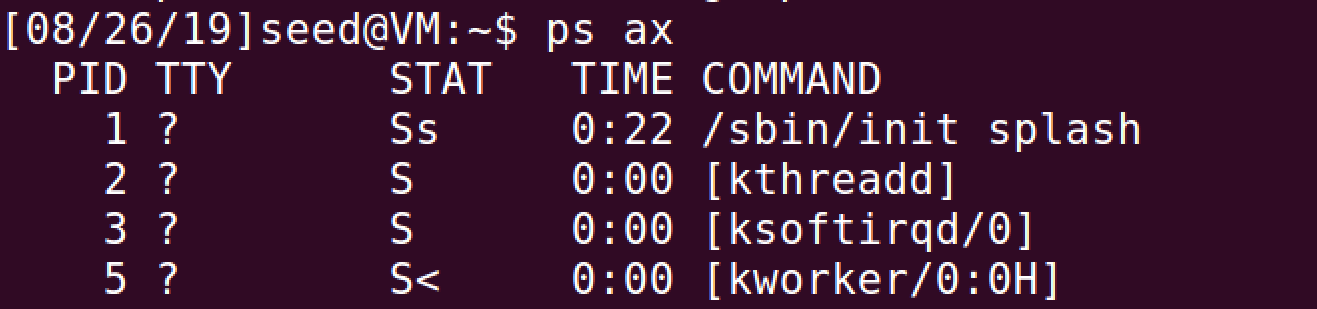
Text

Description automatically generated with medium confidence

Step 9: Remove or shutdown unnecessary components and services

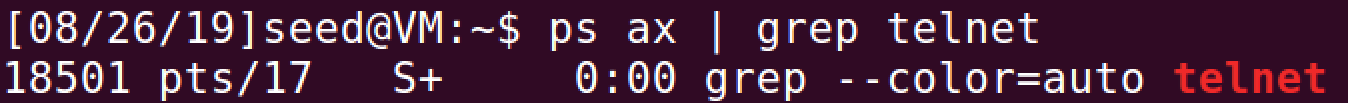
Removing and shutdown unnecessary components and services reduce the attack surface. So, attackers have less opportunity to compromise your system.

First, we need to know what kind of services are running on the system using command *ps ax*.



In the above output, you notice that some of the applications you may not needed on your server but they are still running. Some examples are: Telnet which is a bidirectional interactive text-oriented communication over internet or local area network; rlogin which allows you to log in to another host over network; automount which mounts different file systems automatically to bring up network file system, etc.

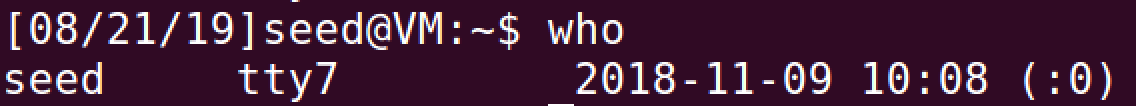
If you want to kill a process in Linux (you don’t need to actually do it in this lab, but you need to know how to do it), you need to get the process ID (PID) of the process by command *ps ax | grep telnet.*



Here, 18501 is the PID of “telnet”. To kill that PID, run command *kill -9 18501*.

**3. Security Monitoring and Auditing**

Step 10: Use command who to view which users are logged in



Text

Description automatically generated with medium confidence

***Nobody’s logged in? So I went and logged one of my users in***

***Text

Description automatically generated***

Step 11: Monitor System Authentication Logs

A fundamental component of authentication management is monitoring the system after you have configured your users. Here is an excellent article about system log, please feel free to read it and get deeper understanding <https://devconnected.com/syslog-the-complete-system-administrator-guide/>. The system log files are located at /var/log. So, you could use command ***cd /var/log/*** to go to the directory. Then use command ***ls -l*** to list all log files in the directory.

Please attach a screenshot of all system log files here.

A screenshot of a computer screen

Description automatically generated with medium confidence

Since the server is maintained by the department, not everyone has the authority to view the system log. Here, let’s check one log file, called lastlog. It formats and prints the contents of the last login log file, including the login name, port, and last login date and time.

Please try accessing system log files, and show the screenshot of *lastlog*.

Text

Description automatically generated



**4. Bonus: Please show that your system provide multi-factor authentication (5 points)**

As one of the users I created, I can use the google-authenticator to provide multi-factor authentication. However, I was unable to figure out how exactly to get it to work. Scanning the QR code opened my Microsoft authenticator app which kept providing me with the wrong code to use. I even tried downloading the Google Authenticator app, but it didn’t work either. What was I missing?

**Qr code

Description automatically generated**