Project 1 Day 2 Scenario:

Today, you will continue to play the role of a security professional tasked with auditing and hardening a Linux server owned by BSC.

Today's focus is on BSC's Linux server's SSH settings, system packages, services, and logging configurations:

- **(1)** Auditing and securing SSH
- **(2)** Reviewing and updating system packages
- **(3)** Disabling unnecessary services
- **(4)** Enabling and configuring logging

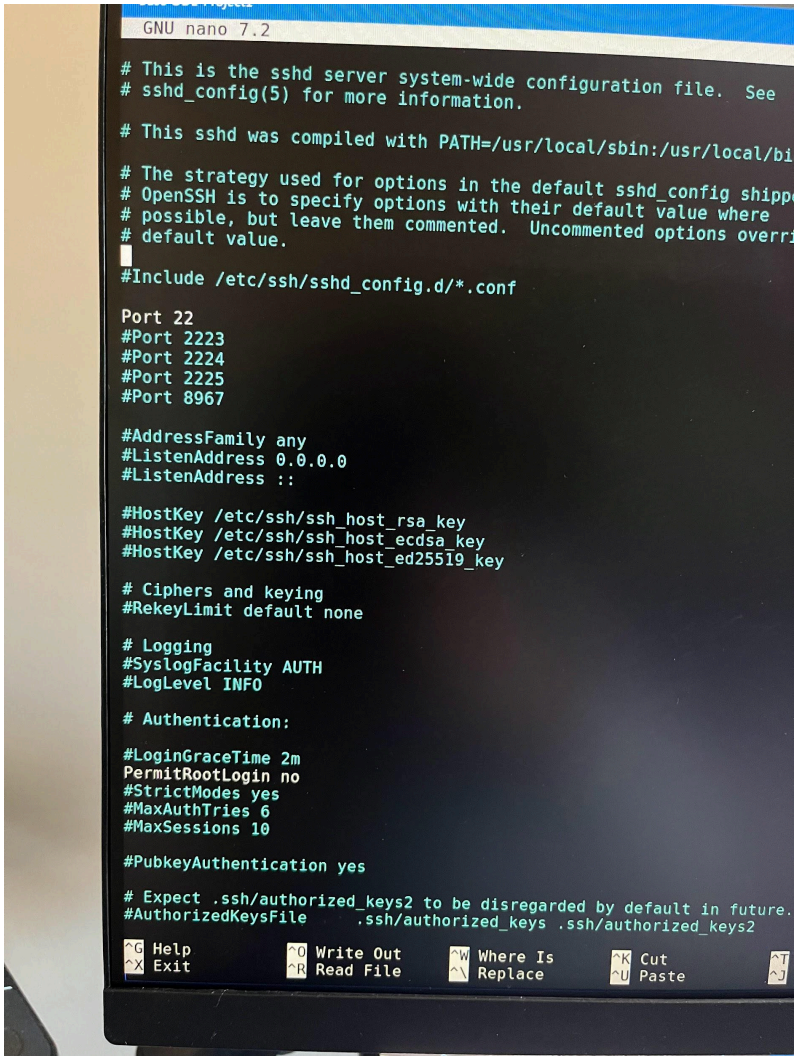
Part 1: Auditing and Securing SSH

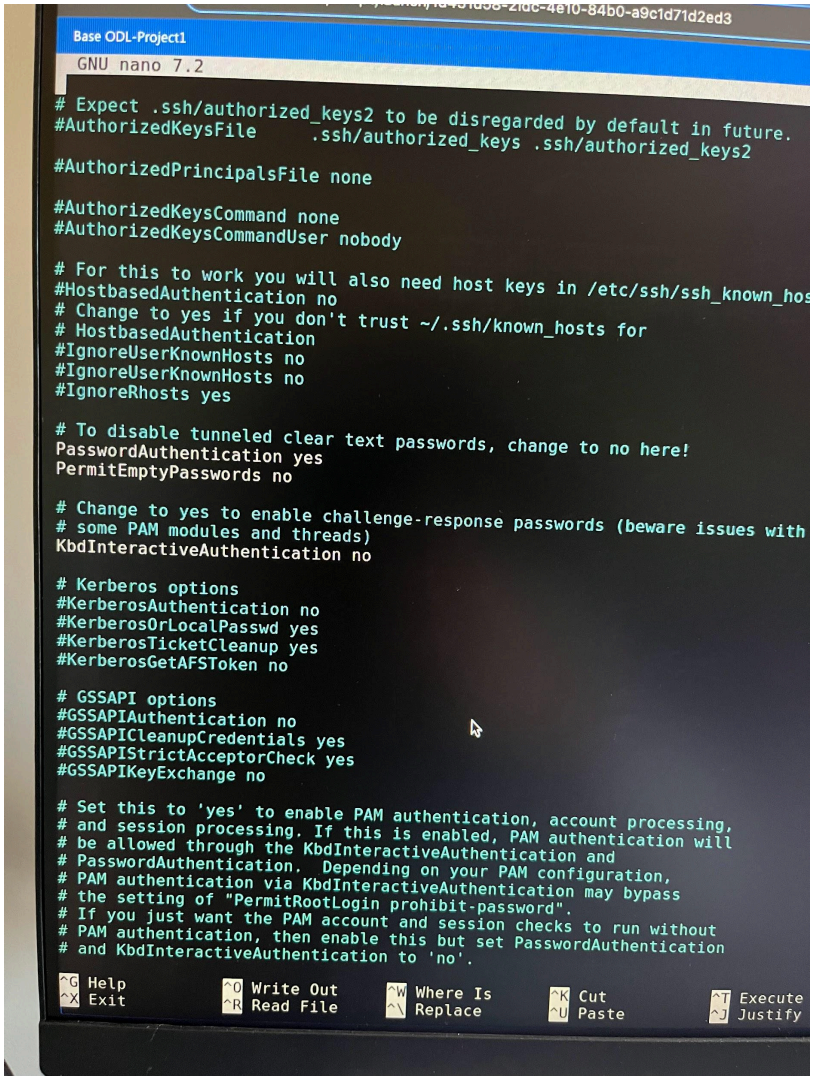
In Part 1 of today's activity, you will be hardening the SSH setting for BSC's Linux server. As SSH is a common method attackers use to breach remote Linux servers, it is important to harden SSH with strict controls.

Complete the following:

1. Configure SSH to **not** allow the ability to:
    a. SSH with empty passwords
    b. SSH with the root user
    c. SSH with any other ports besides 22
2. Enable SSH protocol 2.
3. Restart the SSH service to set your updates
    a. Use the following command: `*service ssh restart*`
4. Be sure to note on your checklist what you have completed.
    a. Don't forget to add in your screenshots!

1. `Sudo nano /etc/ssh/sshd_config` to go to the ssh configuration file.


GNU nano 7.2
This is the sshd server system-wide configuration file. See
sshd_config(5) for more information.
This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bi
The strategy used for options in the default sshd_config shipp
OpenSSH is to specify options with their default value where
possible, but leave them commented. Uncommented options overri
default value.
#Include /etc/ssh/sshd_config.d/*.conf
Port 22
#Port 2223
#Port 2224
#Port 2225
#Port 8967
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key
Ciphers and keying
#RekeyLimit default none
Logging
#SyslogFacility AUTH
#LogLevel INFO
Authentication:
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile   .ssh/authorized_keys .ssh/authorized_keys2
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T
^J



4. `Sudo service ssh restart` restarts the service so that all the updates and saved properly.

Part 2: Review, Update, and Add System Packages

In Part 2, you will be reviewing and updating your system packages. This is important because app developers often release patches to protect from security vulnerabilities. Having the latest version of your packages minimizes your security risks.

1. Run *apt update* to update your package manager to make sure it has the latest version of all packages.

- `Apt update`

2. Next, run *apt upgrade -y* to update all already installed packages to the latest versions.

- `Apt upgrade -y`

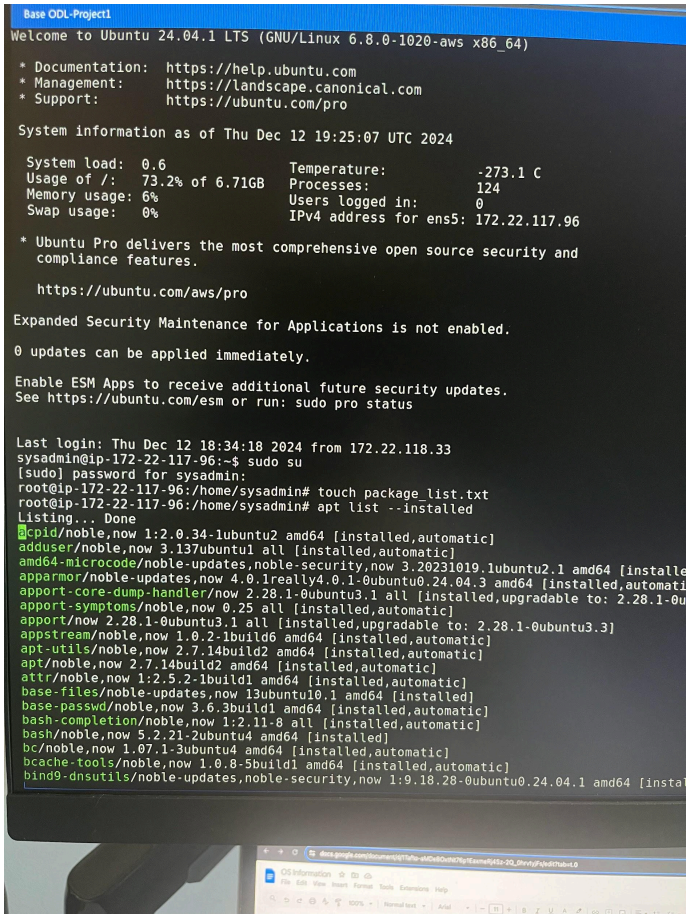
3. Create a file called package_list.txt, which contains all installed packages.
    - `Touch package_list.txt`

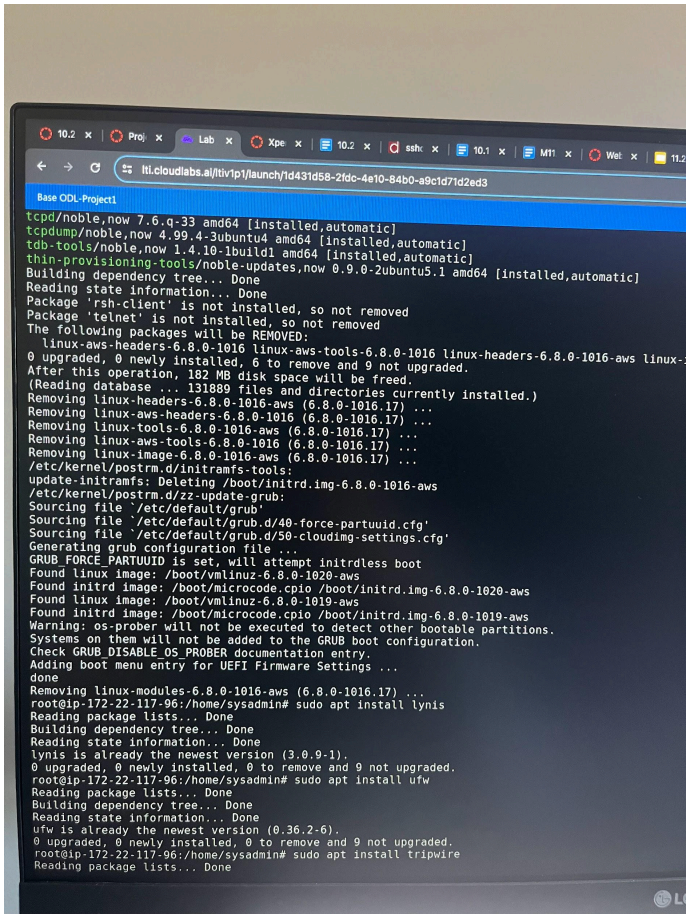
4. Identify if any of the following packages are on the list as having these could introduce a security issue:
        - telnet
        - rsh-client
    - If they are on the list, remove those packages.
        - Research and note why these could have security issues.
    - Remove all unnecessary dependencies of those packages

- `Sudo apt autoremove telnet rsh-client -y`

5. Add the following packages:
    a. ufw
    b. lynis
    c. tripwire

- `Sudo apt install ufw`
- `Sudo apt install lynis`
- `Sudo apt install tripwire`


Base ODL-Project1
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1020-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
System information as of Thu Dec 12 19:25:07 UTC 2024
System load: 0.6
Usage of /: 73.2% of 6.71GB
Memory usage: 6%
Swap usage: 0%
Temperature: -273.1 C
Processes: 124
Users logged in: 0
IPv4 address for ens5: 172.22.117.96
* Ubuntu Pro delivers the most comprehensive open source security and compliance features.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Thu Dec 12 18:34:18 2024 from 172.22.118.33
sysadmin@ip-172-22-117-96:~$ sudo su
[sudo] password for sysadmin:
root@ip-172-22-117-96:/home/sysadmin# touch package_list.txt
root@ip-172-22-117-96:/home/sysadmin# apt list --installed
Listing... Done
acpid/noble,now 1:2.0.34-1ubuntu2 amd64 [installed,automatic]
adduser/noble,now 3.137ubuntu1 all [installed,automatic]
amd64-microcode/noble-updates,noble-security,now 3.20231019.1ubuntu2.1 amd64 [installe
apparmor/noble-updates,now 4.0.1really4.0.1-0ubuntu0.24.04.3 amd64 [installed,automati
apport-core-dump-handler/now 2.28.1-0ubuntu3.1 all [installed,upgradable to: 2.28.1-0u
apport-symptoms/noble,now 0.25 all [installed,automatic]
apport/now 2.28.1-0ubuntu3.1 all [installed,upgradable to: 2.28.1-0ubuntu3.3]
appstream/noble,now 1.0.2-1build6 amd64 [installed,automatic]
apt-utils/noble,now 2.7.14build2 amd64 [installed,automatic]
apt/noble,now 2.7.14build2 amd64 [installed,automatic]
attr/noble,now 1:2.5.2-1build1 amd64 [installed,automatic]
base-files/noble-updates,now 13ubuntu10.1 amd64 [installed]
base-passwd/noble,now 3.6.3build1 amd64 [installed,automatic]
bash-completion/noble,now 1:2.11-8 all [installed,automatic]
bash/noble,now 5.2.21-2ubuntu4 amd64 [installed]
bc/noble,now 1.07.1-3ubuntu4 amd64 [installed,automatic]
bcache-tools/noble,now 1.0.8-5build1 amd64 [installed,automatic]
bind9-dnsutils/noble-updates,noble-security,now 1:9.18.28-0ubuntu0.24.04.1 amd64 [insta



Part 3: Disabling Unnecessary Services

In Part 3, you will be reviewing and disabling any unnecessary services. This is important because having unnecessary services running increases your attack surface. Follow the below steps to identify and remove any unnecessary services.

1. Run the command to list out all services. Output this into a file called service_list.txt.

- `Service -status-all > service_lists.txt`

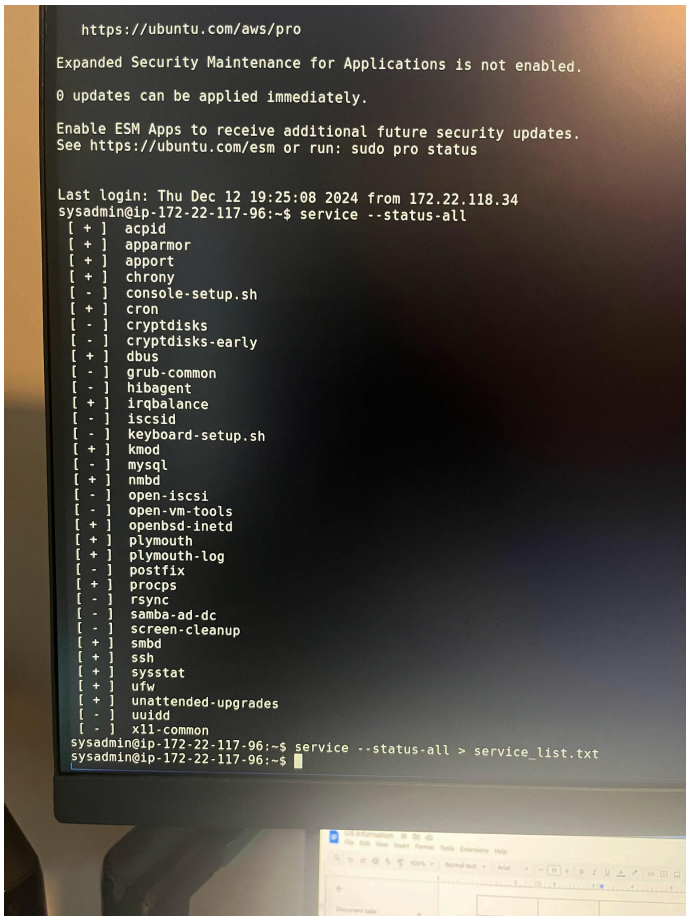
2. Identify if any of the following services are running:
    a. mysql
    b. samba

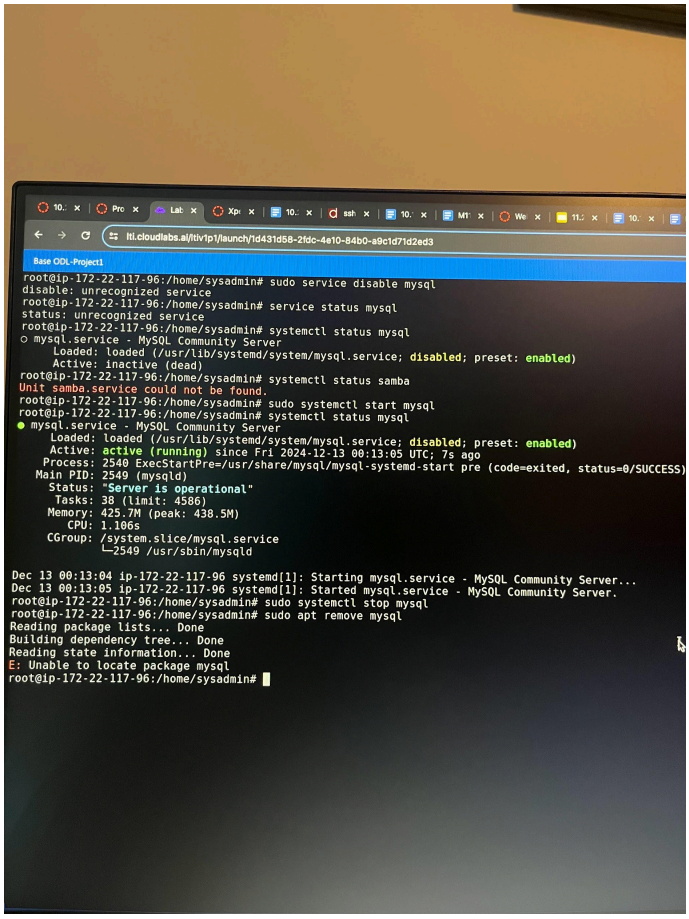
- `Systemctl status mysql`
- `Systemctl status samba`

3. If any of the above services are running,
    - Stop them
    - Remove them

4. For Step 2&3, use the `service` and the `apt remove` command, as systemctl is not installed.

- `Systemctl stop mysql`
- `Systemctl stop samba`
- `Systemctl disable mysql`
- `Systemctl disable samba`





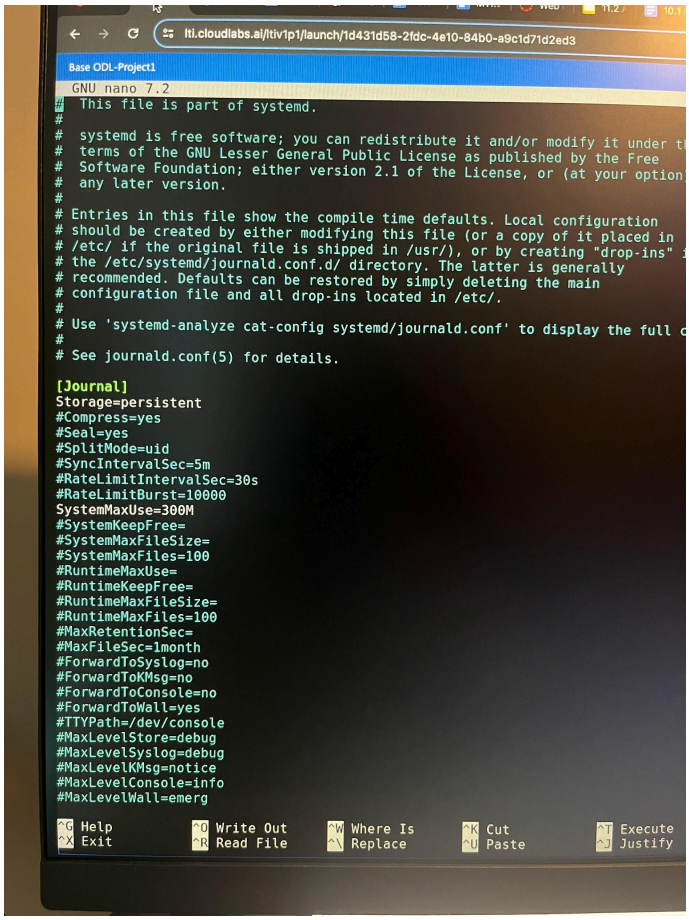
Part 4: Enabling and Configuring Logging

In Part 4, you will be configuring and checking logging settings on Baker Street's Linux server. Logging is a crucial part of the hardening process as logging can help identify security issues such as suspicious network activity, unauthorized access, or other anomalous activity.

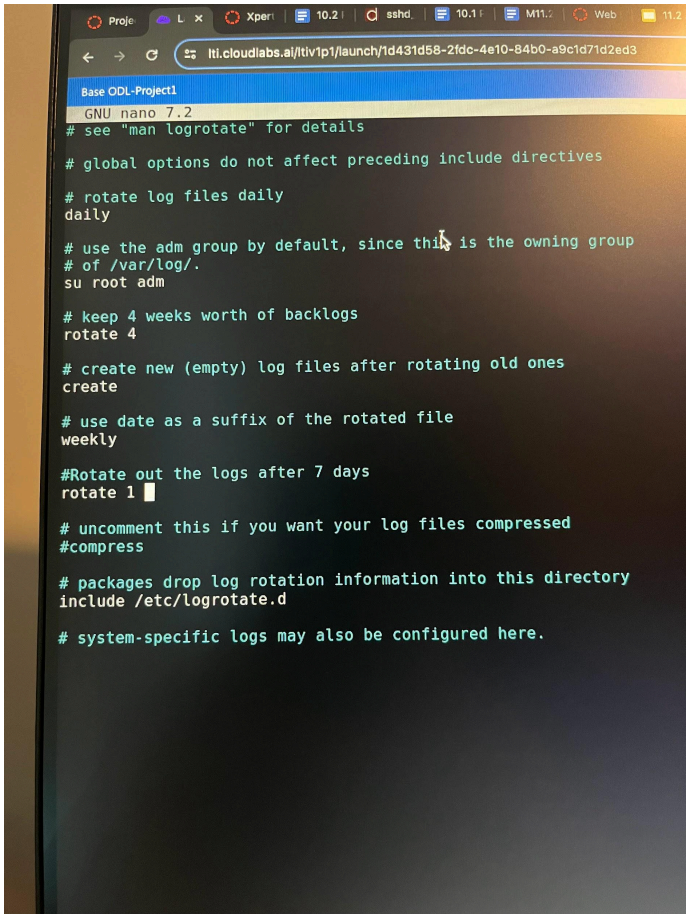
Complete the following:

1. Access the *journald.conf* file located */etc/systemd/*.
2. Use nano to edit the following settings in the file. Be sure to uncomment the lines!
    a. Set "**storage=persistent"**
        i. This setting will save the logs locally on the machine.
    b. Set "**systemMaxUse=300M"**
        i. This setting configures the maximum disk space the logs can utilize.

- `Nano /etc/systemd/journal.conf` allows us to access journal.conf file
- `Nano /etc/logrotate.conf` allows us to access to logrotate.conf file



3. To prevent logs from taking up too much space, you will need to configure log rotation.
   (Use the following guide to assist: https://linux.die.net/man/8/logrotate)
   a. Edit the file: /etc/logrotate.conf with the following settings:
      i. Change the log rotation from weekly to daily.
      ii. Rotate out the logs after 7 days.
4. Save your changes


lti.cloudlabs.ai/ltiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
GNU nano 7.2
see "man logrotate" for details
global options do not affect preceding include directives
rotate log files daily
daily
use the adm group by default, since this is the owning group
of /var/log/.
su root adm
keep 4 weeks worth of backlogs
rotate 4
create new (empty) log files after rotating old ones
create
use date as a suffix of the rotated file
weekly
#Rotate out the logs after 7 days
rotate 1
uncomment this if you want your log files compressed
#compress
packages drop log rotation information into this directory
include /etc/logrotate.d
system-specific logs may also be configured here.