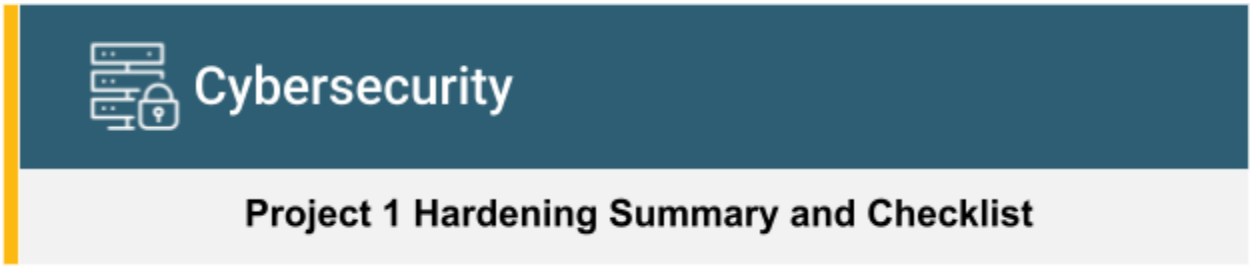
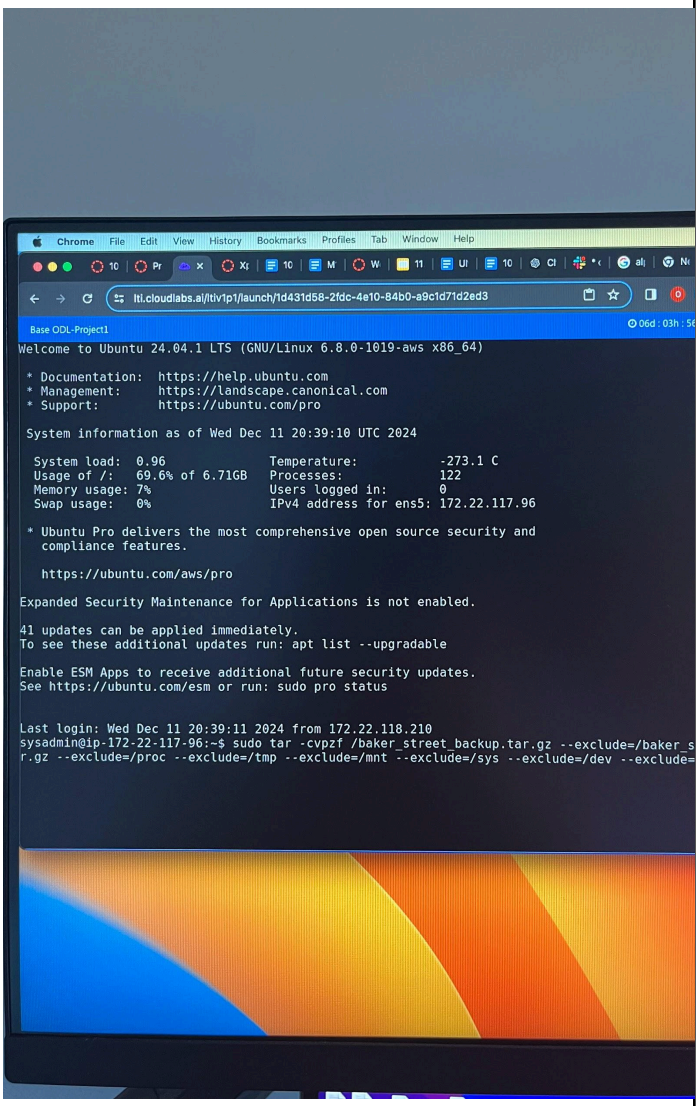
OS Information



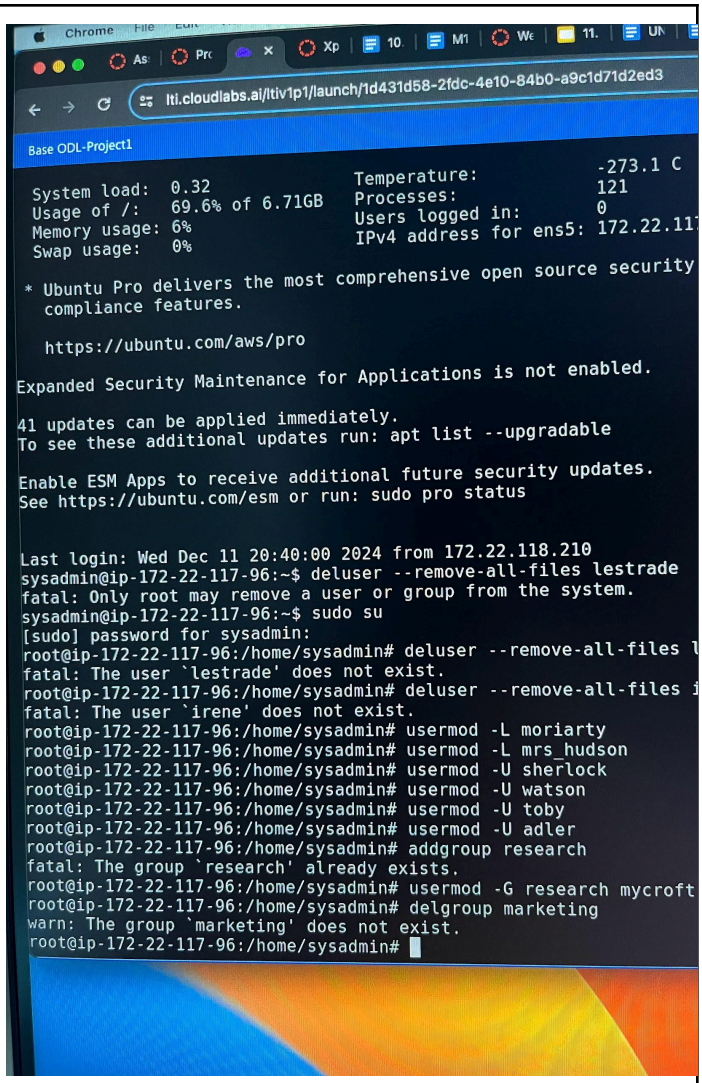
Heads up I took screenshots while I was going through the project but they never saved because my iCloud was full. So the pictures I have of my work are going back over work I already did.	
Customer	Baker Street Corporation
Hostname	**Ip-172-22-117-96**
OS Version	**Uname -a ubuntu**
Memory information	**Free -h total 3.7 Gi**
Uptime information	**Uptime Up 5 min 1 user**

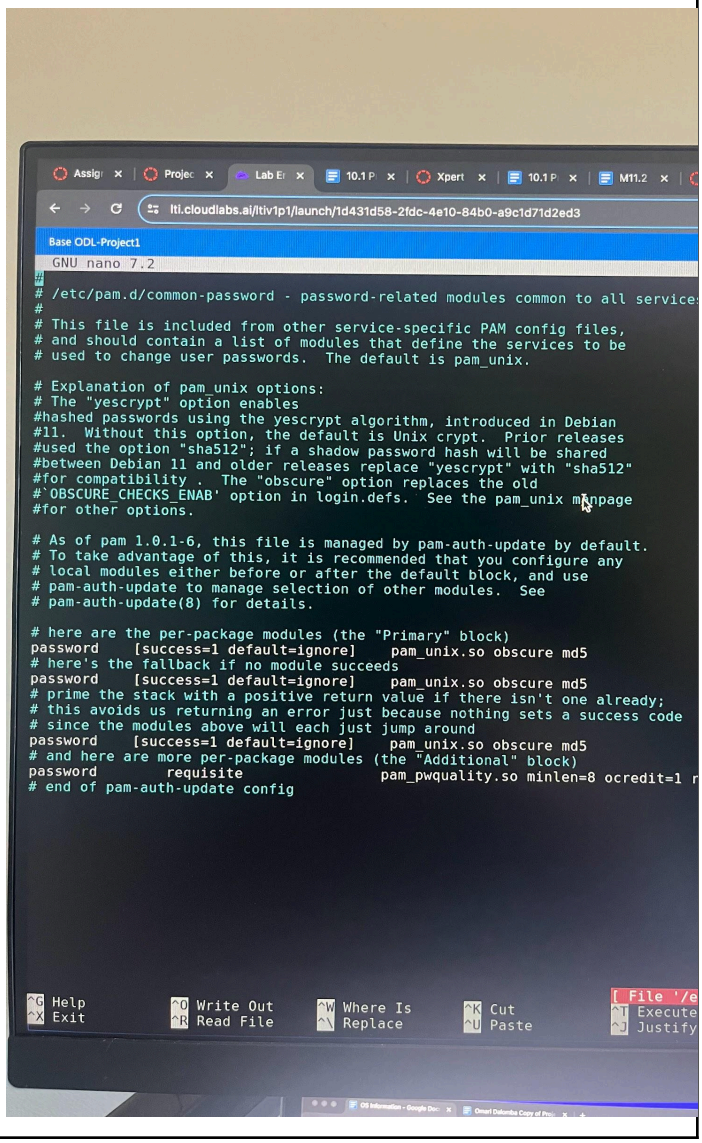
Checklist

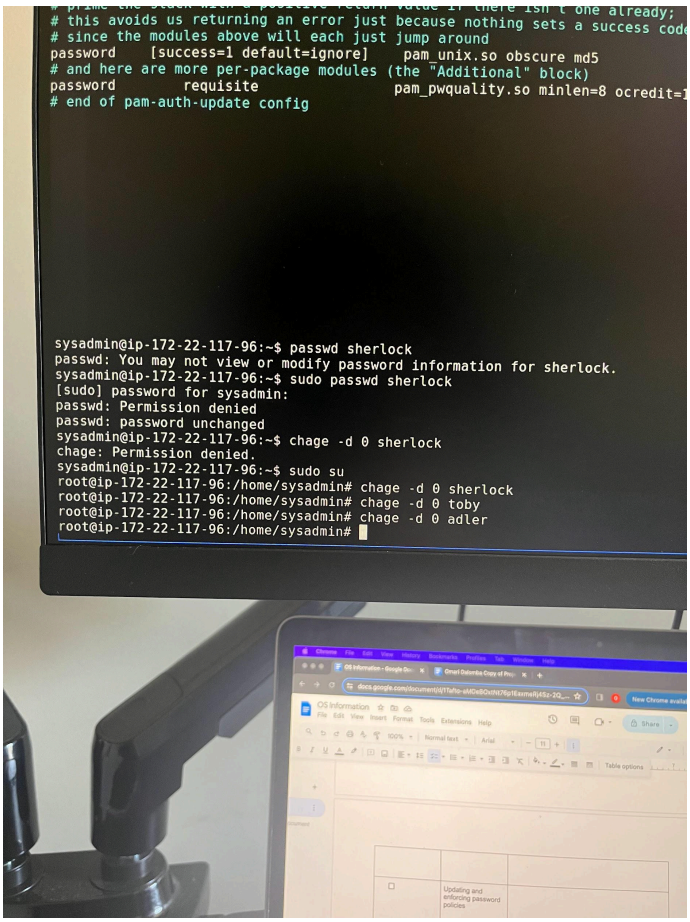
Completed	Activity	Script(s) used / Tasks completed / Screenshots

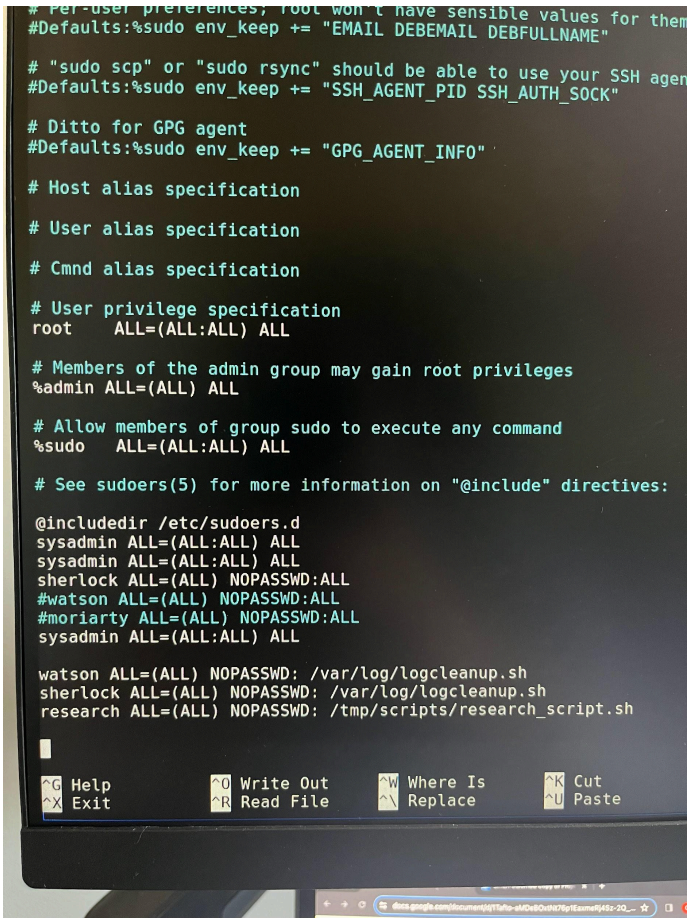
☑	OS backup	Sudo tar -cvpzf /baker_street_backup.tar.gz –exclude=/baker_street_backup.tar.gz –exclude=/proc –exclude=/tmp –exclude=/mnt –exclude=/sys –exclude=/dev –exclude=/run/ 
☐	Auditing users and groups	To Remove all staff who have been terminated: deluser –remove-all-files lestrade. Then do that some command for irene,mary and gregson To lock all user accounts on temporary leave. usermod -L moriarty. Then do the same for mrs_hudson as well. To unlock any users who are employed.

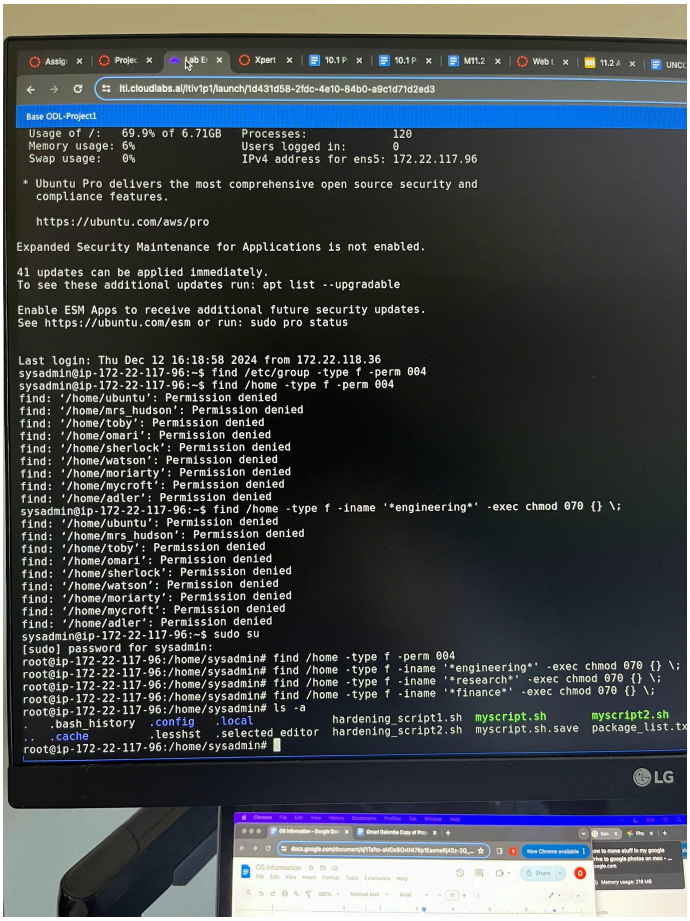
		usermod -U sherlock. Then do the same for Watson, Mycroft, Toby and adler. To add the research group addgroup research To move all the employees who were in the marketing group to the research group. To check who is in the marketing group: cat /etc/group Then to move mycroft to research usermod -G research mycroft

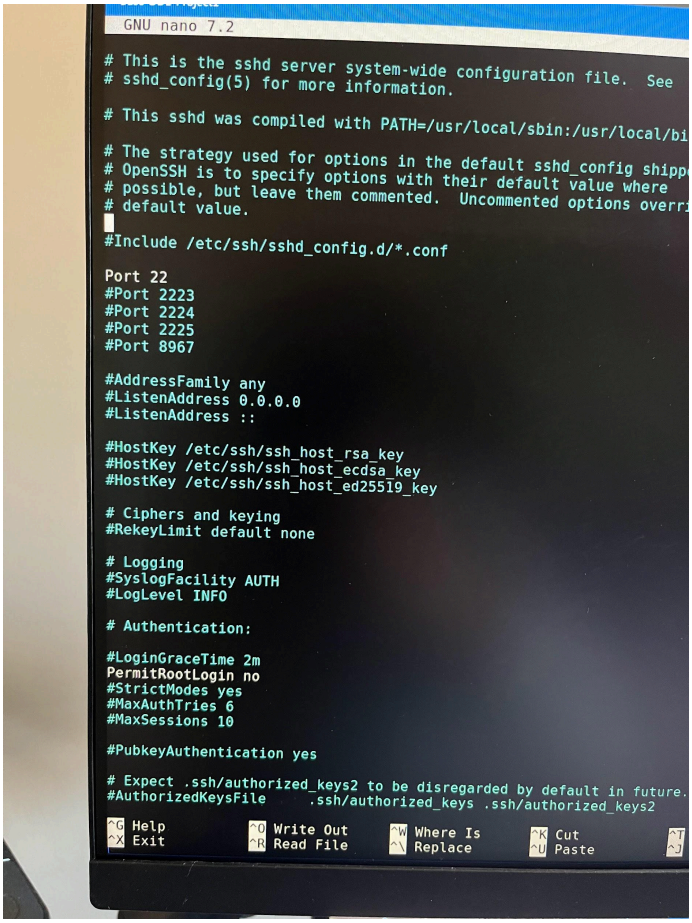

lti.cloudlabs.ai/ltiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
System load: 0.32
Usage of /: 69.6% of 6.71GB
Memory usage: 6%
Swap usage: 0%
Temperature: -273.1 C
Processes: 121
Users logged in: 0
IPv4 address for ens5: 172.22.11
* Ubuntu Pro delivers the most comprehensive open source security compliance features.
https://ubuntu.com/aws/pro
Expanded Security Maintenance for Applications is not enabled.
41 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
Last login: Wed Dec 11 20:40:00 2024 from 172.22.118.210
sysadmin@ip-172-22-117-96:~$ deluser --remove-all-files lestrade
fatal: Only root may remove a user or group from the system.
sysadmin@ip-172-22-117-96:~$ sudo su
[sudo] password for sysadmin:
root@ip-172-22-117-96:/home/sysadmin# deluser --remove-all-files l
fatal: The user `lestrade' does not exist.
root@ip-172-22-117-96:/home/sysadmin# deluser --remove-all-files i
fatal: The user `irene' does not exist.
root@ip-172-22-117-96:/home/sysadmin# usermod -L moriarty
root@ip-172-22-117-96:/home/sysadmin# usermod -L mrs_hudson
root@ip-172-22-117-96:/home/sysadmin# usermod -U sherlock
root@ip-172-22-117-96:/home/sysadmin# usermod -U watson
root@ip-172-22-117-96:/home/sysadmin# usermod -U toby
root@ip-172-22-117-96:/home/sysadmin# usermod -U adler
root@ip-172-22-117-96:/home/sysadmin# addgroup research
fatal: The group `research' already exists.
root@ip-172-22-117-96:/home/sysadmin# usermod -G research mycroft
root@ip-172-22-117-96:/home/sysadmin# delgroup marketing
warn: The group `marketing' does not exist.
root@ip-172-22-117-96:/home/sysadmin#

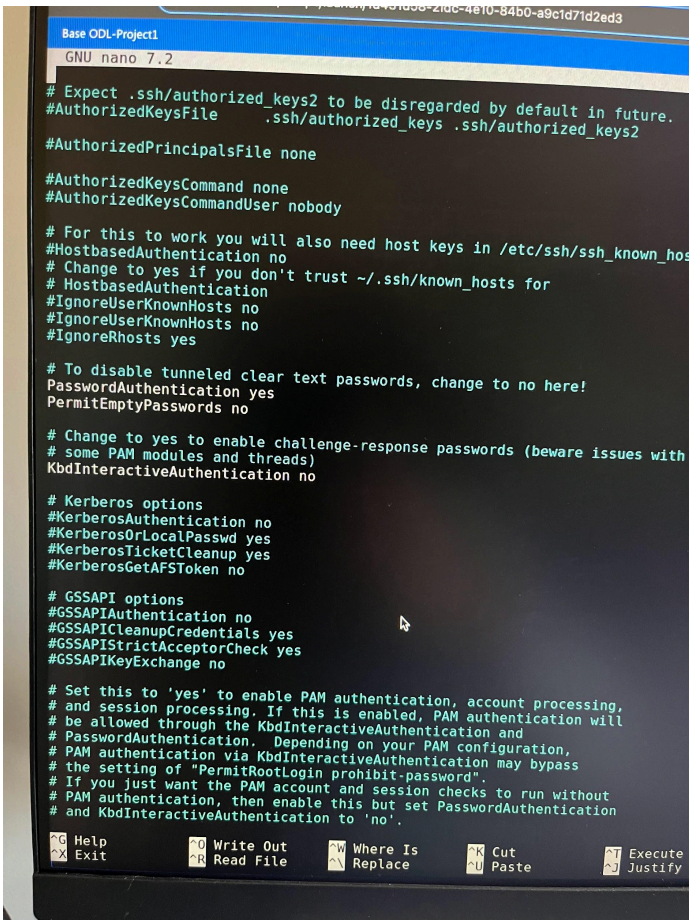
☐	Updating and enforcing password policies	Update the password requirements to minimum 8 characters, At least one special character, allow 2 retries and at least one uppercase character nano /etc/pam.d/common-password Password requisite pam_pwqaulity.so minlen=8 ocredit=1 retry=2 ucredit=1 Chage -d 0 Toby Chage -d 0 adler 

		
☐	Updating and enforcing sudo permissions	Sudo visudo

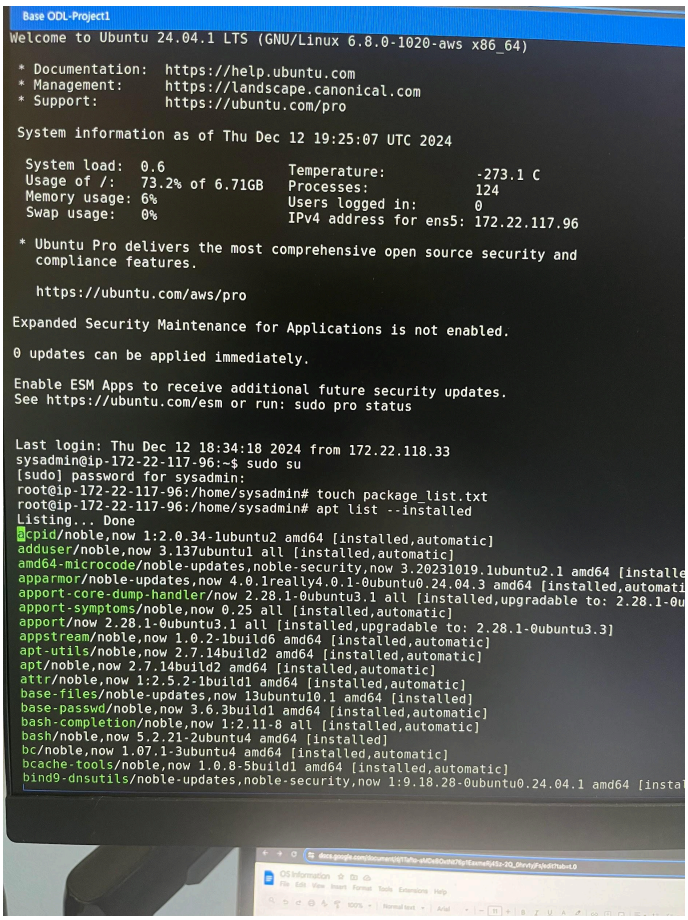

#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"
Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"
Host alias specification
User alias specification
Cmnd alias specification
User privilege specification
root ALL=(ALL:ALL) ALL
Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
See sudoers(5) for more information on "@include" directives:
@includedir /etc/sudoers.d
sysadmin ALL=(ALL:ALL) ALL
sysadmin ALL=(ALL:ALL) ALL
sherlock ALL=(ALL) NOPASSWD:ALL
#watson ALL=(ALL) NOPASSWD:ALL
#moriarty ALL=(ALL) NOPASSWD:ALL
sysadmin ALL=(ALL:ALL) ALL
watson ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
sherlock ALL=(ALL) NOPASSWD: /var/log/logcleanup.sh
research ALL=(ALL) NOPASSWD: /tmp/scripts/research_script.sh
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste

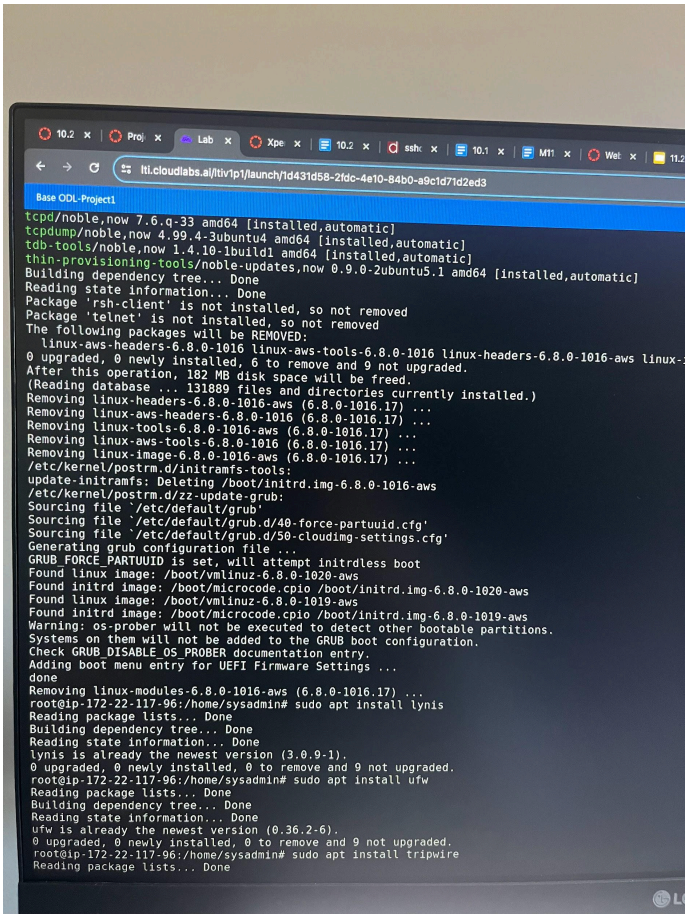
☐	Validating and updating permissions on files and directories	FInd all files with world permissions: Find /home -type f -perm 004 Only members of the engineering group can view edit or execute Find /home -type f -name '**engineering**' -exec chmod 070 {} \; Only members of the research group can view edit or execute Find /home -type f -name '**research**' -exec chmod 070 {} \; Only members of the finance group can view edit or execute Find /home -type f -name '**finance**' -exec chmod 070 {} \; Ls -a 

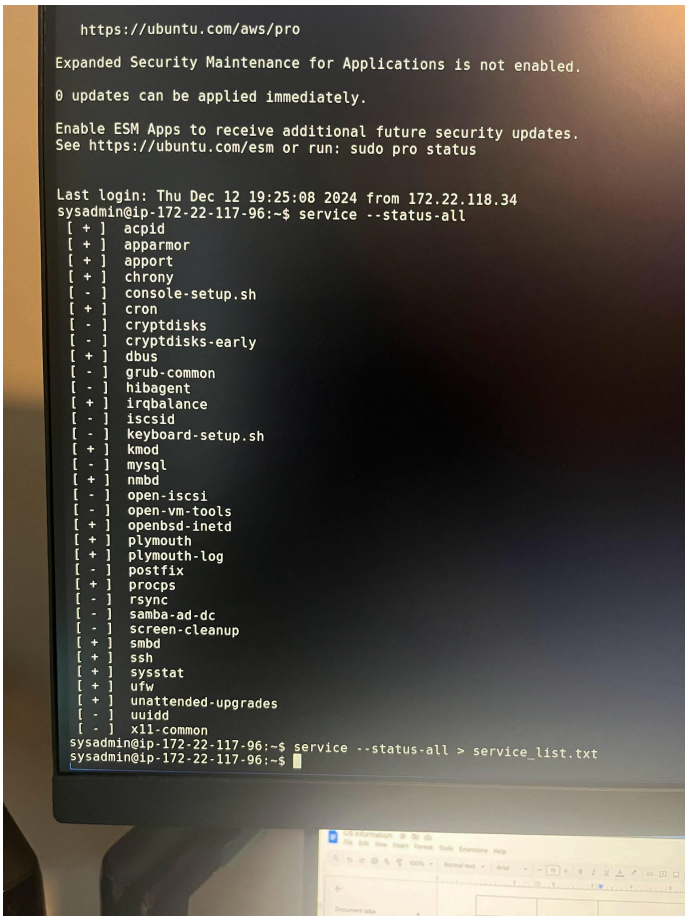
☐	Optional: Updating password hashing configuration	
☐	Auditing and securing SSH	Sudo nano /etc/ssh/sshd_config Restart the ssh service. Sudo service ssh restart 

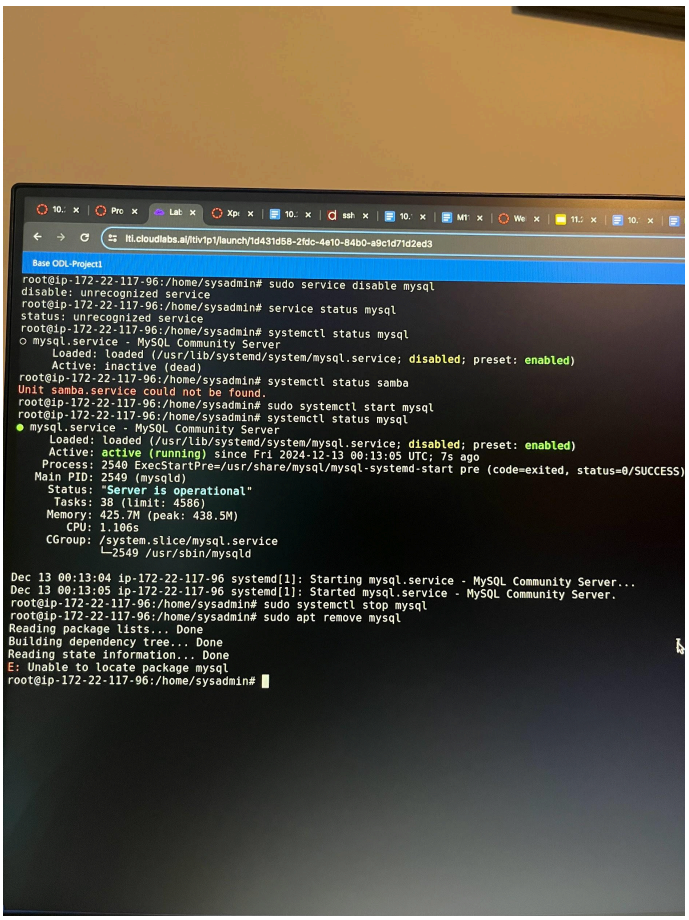

Base ODL-Project1
GNU nano 7.2
Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
For this to work you will also need host keys in /etc/ssh/ssh_known_hos
#HostbasedAuthentication no
Change to yes if you don't trust ~/.ssh/known_hosts for
HostbasedAuthentication
#IgnoreUserKnownHosts no
#IgnoreUserKnownHosts no
#IgnoreRhosts yes
To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PermitEmptyPasswords no
Change to yes to enable challenge-response passwords (beware issues with
some PAM modules and threads)
KbdInteractiveAuthentication no
Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
Set this to 'yes' to enable PAM authentication, account processing,
and session processing. If this is enabled, PAM authentication will
be allowed through the KbdInteractiveAuthentication and
PasswordAuthentication. Depending on your PAM configuration,
PAM authentication via KbdInteractiveAuthentication may bypass
the setting of "PermitRootLogin prohibit-password".
If you just want the PAM account and session checks to run without
PAM authentication, then enable this but set PasswordAuthentication
and KbdInteractiveAuthentication to 'no'.
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify

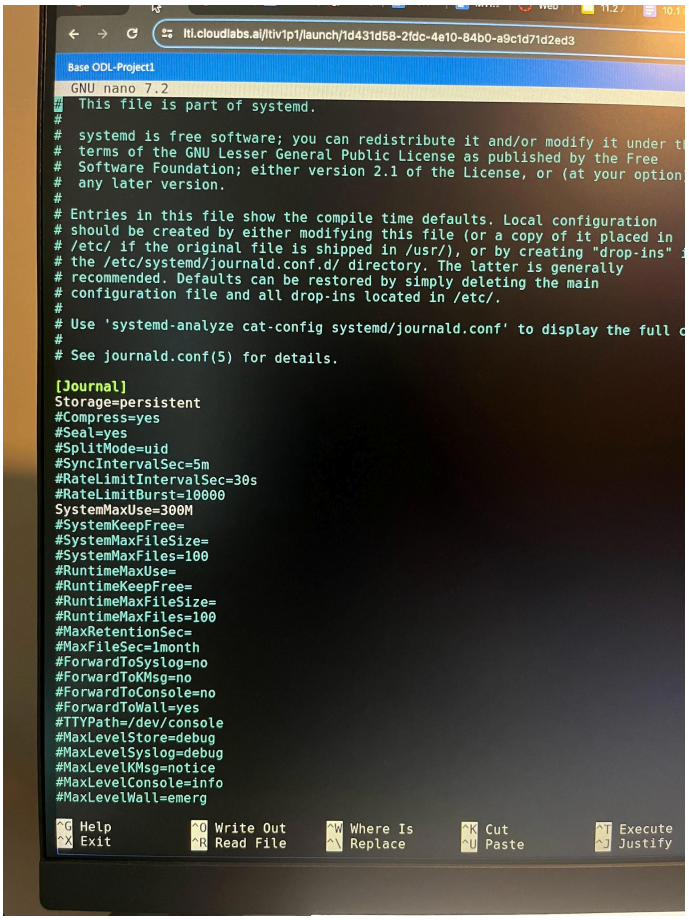
☐	Reviewing and updating system packages	Apt update Apt upgrade -y Create a file Touch package_list.txt View all installed packages Apt list –installed Remove telnet and rsh-client packages Sudo apt autoremove telnet rsh-client -y Add the packages, ufw, lynis, tripwire Sudo apt install ufw Sudo apt install lynis Sudo apt install tripwire Lynis: can perform in depth security audits and identify vulnerabilities across multiple systems. Ufw: It provides an easy to use interface for managing firewall rules on Linux systems Tripwire: It focuses on file integrity and monitoring

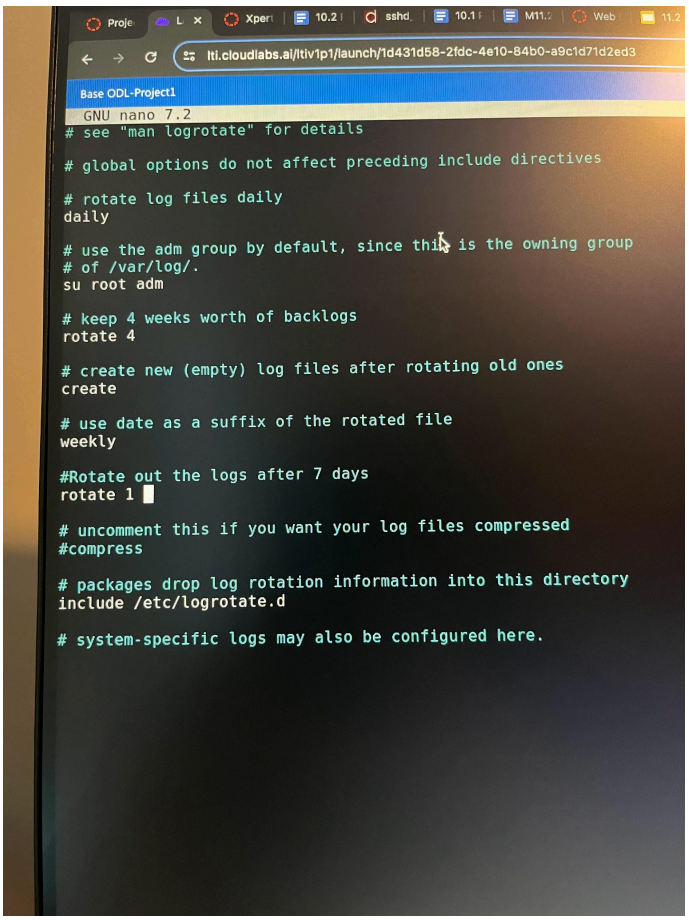
		 Base ODL-Project1 Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1020-aws x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/pro System information as of Thu Dec 12 19:25:07 UTC 2024 System load: 0.6 Usage of /: 73.2% of 6.71GB 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

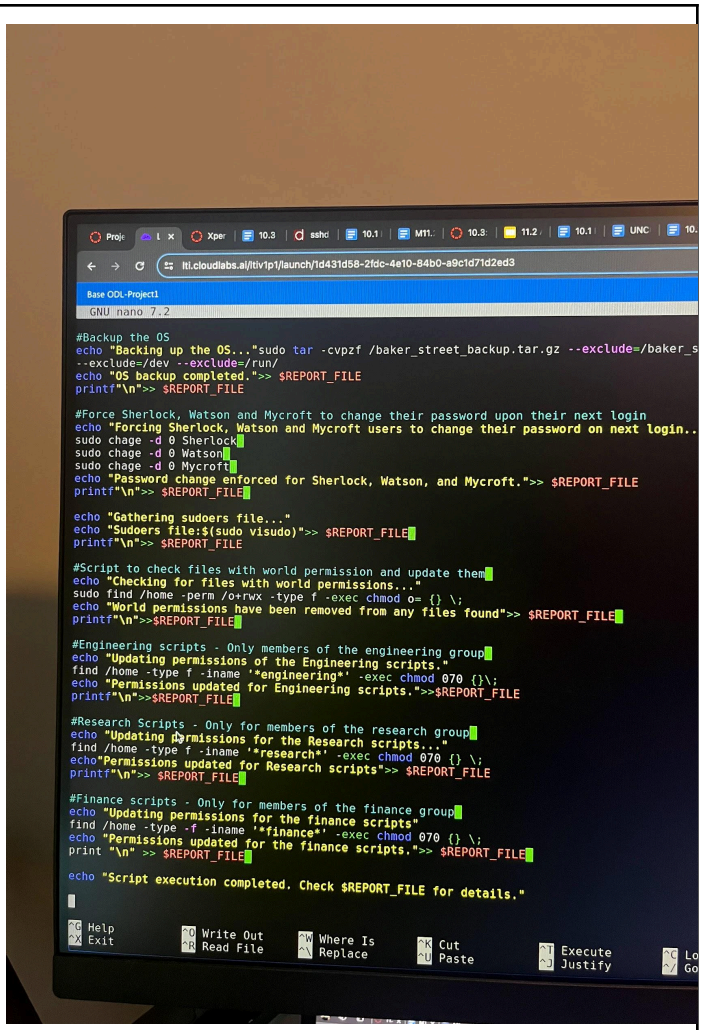

lti.cloudlabs.ai/tiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
tcpd/noble,now 7.6.q-33 amd64 [installed,automatic]
tcpdump/noble,now 4.99.4-3ubuntu4 amd64 [installed,automatic]
tdb-tools/noble,now 1.4.10-1build1 amd64 [installed,automatic]
thin-provisioning-tools/noble-updates,now 0.9.0-2ubuntu5.1 amd64 [installed,automatic]
Building dependency tree... Done
Reading state information... Done
Package 'rsh-client' is not installed, so not removed
Package 'telnet' is not installed, so not removed
The following packages will be REMOVED:
linux-aws-headers-6.8.0-1016 linux-aws-tools-6.8.0-1016 linux-headers-6.8.0-1016-aws
0 upgraded, 0 newly installed, 6 to remove and 9 not upgraded.
After this operation, 182 MB disk space will be freed.
(Reading database ... 131889 files and directories currently installed.)
Removing linux-headers-6.8.0-1016-aws (6.8.0-1016.17) ...
Removing linux-aws-headers-6.8.0-1016 (6.8.0-1016.17) ...
Removing linux-tools-6.8.0-1016-aws (6.8.0-1016.17) ...
Removing linux-aws-tools-6.8.0-1016 (6.8.0-1016.17) ...
Removing linux-image-6.8.0-1016-aws (6.8.0-1016.17) ...
/etc/kernel/postrm.d/initramfs-tools:
update-initramfs: Deleting /boot/initrd.img-6.8.0-1016-aws
/etc/kernel/postrm.d/zz-update-grub:
Sourcing file `/etc/default/grub'
Sourcing file `/etc/default/grub.d/40-force-partuuid.cfg'
Sourcing file `/etc/default/grub.d/50-cloudimg-settings.cfg'
Generating grub configuration file ...
GRUB_FORCE_PARTUUID is set, will attempt initrdless boot
Found linux image: /boot/vmlinuz-6.8.0-1020-aws
Found initrd image: /boot/microcode.cpio /boot/initrd.img-6.8.0-1020-aws
Found linux image: /boot/vmlinuz-6.8.0-1019-aws
Found initrd image: /boot/microcode.cpio /boot/initrd.img-6.8.0-1019-aws
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
Removing linux-modules-6.8.0-1016-aws (6.8.0-1016.17) ...
root@ip-172-22-117-96:/home/sysadmin# sudo apt install lynis
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
lynis is already the newest version (3.0.9-1).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
root@ip-172-22-117-96:/home/sysadmin# sudo apt install ufw
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ufw is already the newest version (0.36.2-6).
0 upgraded, 0 newly installed, 0 to remove and 9 not upgraded.
root@ip-172-22-117-96:/home/sysadmin# sudo apt install tripwire
Reading package lists... Done

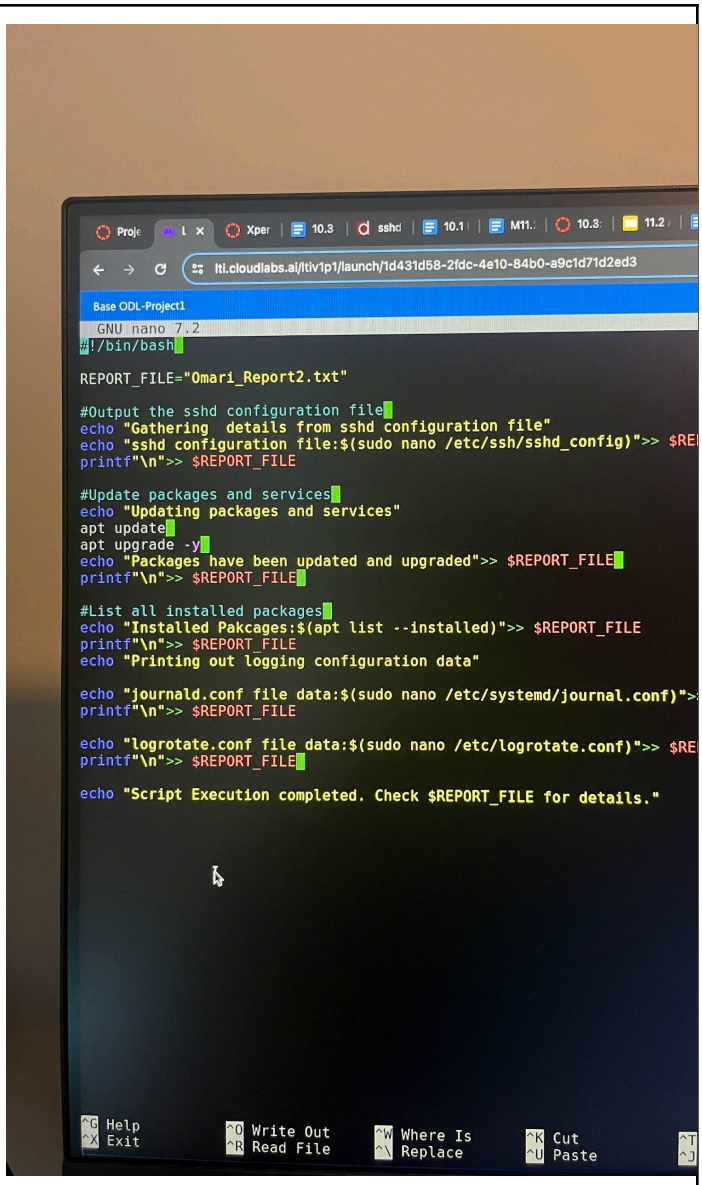
☐	Disabling unnecessary services	Service –status-all List out all services and output into a file Service –status-all > service_list.txt See if any of the services are running Systemctl status mysql Systemctl status samba Stop,disable and remove the services Systemctl stop mysql Systemctl stop samba Systemctl disable mysql Systemctl disable samba 


lti.cloudlabs.ai/ftlv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
root@ip-172-22-117-96:/home/sysadmin# sudo service disable mysql
disable: unrecognized service
root@ip-172-22-117-96:/home/sysadmin# service status mysql
status: unrecognized service
root@ip-172-22-117-96:/home/sysadmin# systemctl status mysql
○ mysql.service - MySQL Community Server
Loaded: loaded (/usr/lib/systemd/system/mysql.service; disabled; preset: enabled)
Active: inactive (dead)
root@ip-172-22-117-96:/home/sysadmin# systemctl status samba
Unit samba.service could not be found.
root@ip-172-22-117-96:/home/sysadmin# sudo systemctl start mysql
root@ip-172-22-117-96:/home/sysadmin# systemctl status mysql
● mysql.service - MySQL Community Server
Loaded: loaded (/usr/lib/systemd/system/mysql.service; disabled; preset: enabled)
Active: active (running) since Fri 2024-12-13 00:13:05 UTC; 7s ago
Process: 2540 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
Main PID: 2549 (mysqld)
Status: "Server is operational"
Tasks: 38 (limit: 4586)
Memory: 425.7M (peak: 438.5M)
CPU: 1.106s
CGroup: /system.slice/mysql.service
└─2549 /usr/sbin/mysqld
Dec 13 00:13:04 ip-172-22-117-96 systemd[1]: Starting mysql.service - MySQL Community Server...
Dec 13 00:13:05 ip-172-22-117-96 systemd[1]: Started mysql.service - MySQL Community Server.
root@ip-172-22-117-96:/home/sysadmin# sudo systemctl stop mysql
root@ip-172-22-117-96:/home/sysadmin# sudo apt remove mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package mysql
root@ip-172-22-117-96:/home/sysadmin#

☐	Enabling and configuring logging	Access the both of the files Nano /etc/systemd/journal.conf Nano /etc/logrotate.conf 

		
☐	Scripts created	Nano myscript.sh Nano myscript2.sh chmod +x cp myscript.sh hardening_script1.sh cp myscript2.sh hardening_script2.sh


lti.cloudlabs.ai/ltiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
GNU nano 7.2
#Backup the OS
echo "Backing up the OS..."sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_s
--exclude=/dev --exclude=/run/
echo "OS backup completed.">> $REPORT_FILE
printf"\n">> $REPORT_FILE
#Force Sherlock, Watson and Mycroft to change their password upon their next login
echo "Forcing Sherlock, Watson and Mycroft users to change their password on next login..
sudo chage -d 0 Sherlock
sudo chage -d 0 Watson
sudo chage -d 0 Mycroft
echo "Password change enforced for Sherlock, Watson, and Mycroft.">> $REPORT_FILE
printf"\n">> $REPORT_FILE
echo "Gathering sudoers file..."
echo "Sudoers file:$(sudo visudo)">> $REPORT_FILE
printf"\n">> $REPORT_FILE
#Script to check files with world permission and update them
echo "Checking for files with world permissions..."
sudo find /home -perm /o+rwx -type f -exec chmod o= {} \;
echo "World permissions have been removed from any files found">> $REPORT_FILE
printf"\n">>$REPORT_FILE
#Engineering scripts - Only members of the engineering group
echo "Updating permissions of the Engineering scripts."
find /home -type f -iname '*engineering*' -exec chmod 070 {}\;
echo "Permissions updated for Engineering scripts.">>$REPORT_FILE
printf"\n">>$REPORT_FILE
#Research Scripts - Only for members of the research group
echo "Updating permissions for the Research scripts..."
find /home -type f -iname '*research*' -exec chmod 070 {} \;
echo"Permissions updated for Research scripts">> $REPORT_FILE
printf"\n">> $REPORT_FILE
#Finance scripts - Only for members of the finance group
echo "Updating permissions for the finance scripts"
find /home -type -f -iname '*finance*' -exec chmod 070 {} \;
echo "Permissions updated for the finance scripts.">> $REPORT_FILE
print "\n" >> $REPORT_FILE
echo "Script execution completed. Check $REPORT_FILE for details."
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify


lti.cloudlabs.ai/itiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
GNU nano 7.2
#!/bin/bash
REPORT_FILE="Omari_Report2.txt"
#Output the sshd configuration file
echo "Gathering details from sshd configuration file"
echo "sshd configuration file:$(sudo nano /etc/ssh/sshd_config)">> $RE
printf"\n">> $REPORT_FILE
#Update packages and services
echo "Updating packages and services"
apt update
apt upgrade -y
echo "Packages have been updated and upgraded">> $REPORT_FILE
printf"\n">> $REPORT_FILE
#List all installed packages
echo "Installed Pakcages:$(apt list --installed)">> $REPORT_FILE
printf"\n">> $REPORT_FILE
echo "Printing out logging configuration data"
echo "journald.conf file data:$(sudo nano /etc/systemd/journal.conf)">
printf"\n">> $REPORT_FILE
echo "logrotate.conf file data:$(sudo nano /etc/logrotate.conf)">> $RE
printf"\n">> $REPORT_FILE
echo "Script Execution completed. Check $REPORT_FILE for details."
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste

☐	Scripts scheduled with cron	Crontab -e