

OS Information



Cybersecurity

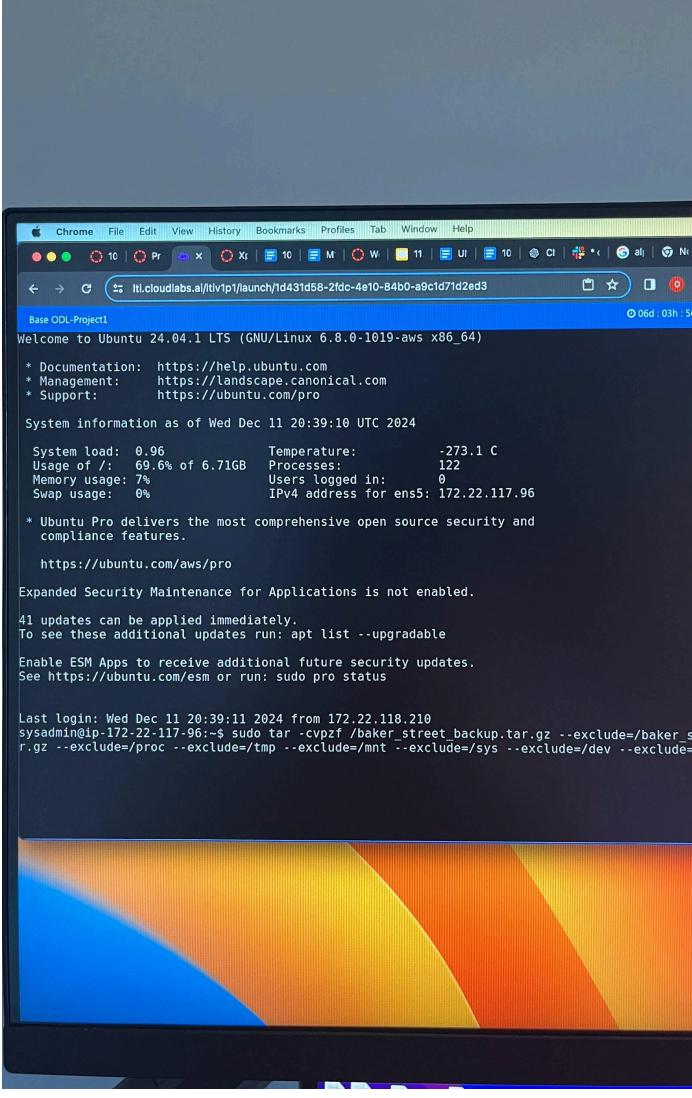
Project 1 Hardening Summary and Checklist

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	<u>Ip-172-22-117-96</u>
OS Version	<u>Uname -a ubuntu</u>
Memory information	<u>Free -h total 3.7 Gi</u>
Uptime information	<u>Uptime Up 5 min 1 user</u>

Checklist

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

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

`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`

Base ODL-Project1

```
System load: 0.32 Temperature: -273.1 C
Usage of /: 69.6% of 6.71GB Processes: 121
Memory usage: 6% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 172.22.117.233

* Ubuntu Pro delivers the most comprehensive open source security
  compliance features.

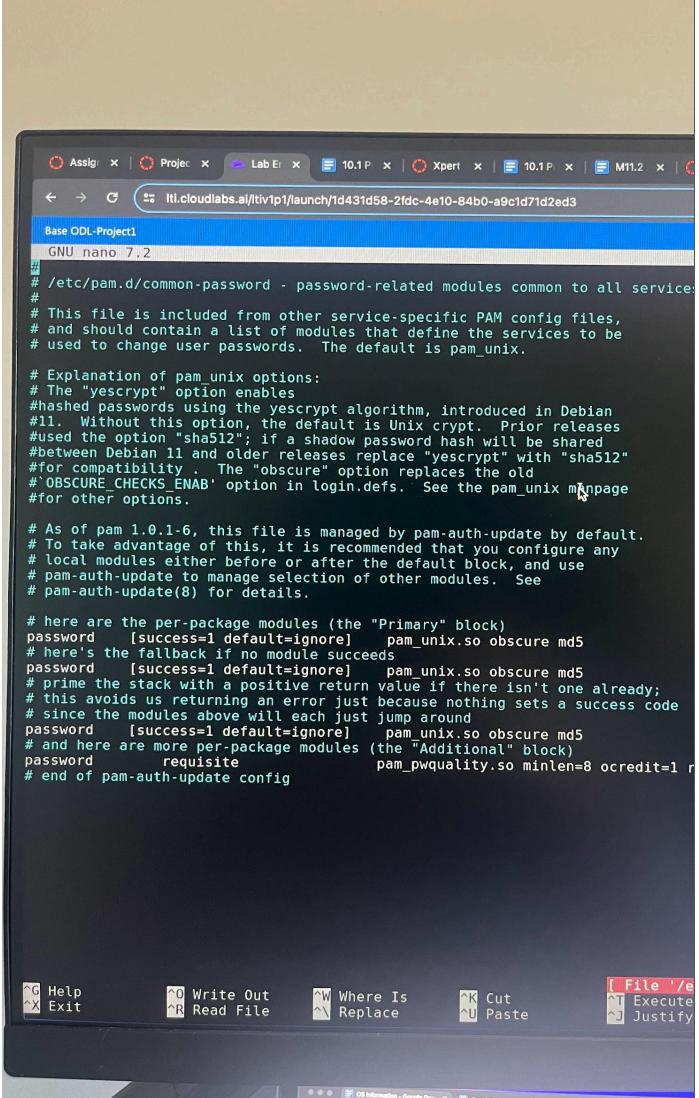
https://ubuntu.com/aws/pro

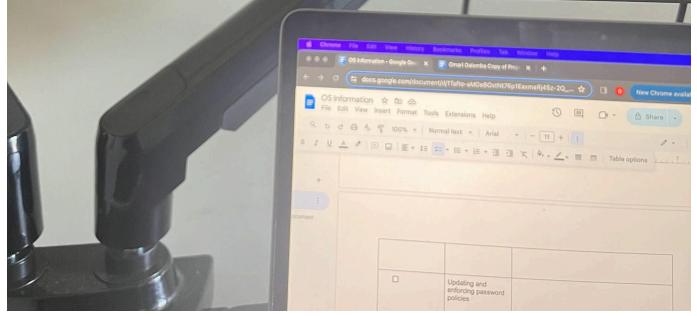
Expanded Security Maintenance for Applications is not enabled.

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 lestrade
fatal: The user `lestrade' does not exist.
root@ip-172-22-117-96:/home/sysadmin# deluser --remove-all-files irene
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#
```

<input type="checkbox"/>	<p>Updating and enforcing password policies</p>	<p>Update the password requirements to minimum 8 characters, At least one special character, allow 2 retries and at least one uppercase character</p> <p>nano /etc/pam.d/common-password</p> <p>Password requisite pam_pwquality.so minlen=8 ocredit=1 retry=2 uccredit=1</p> <p>Chage -d 0 Toby</p> <p>Chage -d 0 adler</p>  <pre> Base ODL-Project GNU nano 7.2 # /etc/pam.d/common-password - password-related modules common to all services # # This file is included from other service-specific PAM config files, # and should contain a list of modules that define the services to be # used to change user passwords. The default is pam_unix. # Explanation of pam_unix options: # The "yescrypt" option enables # hashed passwords using the yescrypt algorithm, introduced in Debian # 11. Without this option, the default is Unix crypt. Prior releases # used the option "sha512"; if a shadow password hash will be shared # between Debian 11 and older releases replace "yescrypt" with "sha512" # for compatibility. The "obscure" option replaces the old # "OBSCURE_CHECKS_ENAB" option in login.defs. See the pam_unix manpage # for other options. # As of pam 1.0.1-6, this file is managed by pam-auth-update by default. # To take advantage of this, it is recommended that you configure any # local modules either before or after the default block, and use # pam-auth-update to manage selection of other modules. See # pam-auth-update(8) for details. # here are the per-package modules (the "Primary" block) password [success=1 default=ignore] pam_unix.so obscure md5 # here's the fallback if no module succeeds password [success=1 default=ignore] pam_unix.so obscure md5 # prime the stack with a positive return value if there isn't one already; # this avoids us returning an error just because nothing sets a success code # since the modules above will each just jump around password [success=1 default=ignore] pam_unix.so obscure md5 # and here are more per-package modules (the "Additional" block) password requisite pam_pwquality.so minlen=8 ocredit=1 r # end of pam-auth-update config </pre>
--------------------------	---	--

		<pre># PRIME_SUCCEED_BY_DEFAULT=1 (which is the default value if there isn't one already) # this avoids us returning an error just because nothing sets a success code password [success=1 default=ignore] pam_unix.so obscure md5 # and here are more per-package modules (the "Additional" block) password requisite pam_pwquality.so minlen=8 ocredit=1 # end of pam-auth-update config</pre> <pre>sysadmin@ip-172-22-117-96:~\$ passwd sherlock passwd: You may not view or modify password information for sherlock. sysadmin@ip-172-22-117-96:~\$ sudo passwd sherlock [sudo] password for sysadmin: passwd: Permission denied passwd: password unchanged sysadmin@ip-172-22-117-96:~\$ chage -d 0 sherlock chage: Permission denied. sysadmin@ip-172-22-117-96:~\$ sudo su root@ip-172-22-117-96:/home/sysadmin# chage -d 0 sherlock root@ip-172-22-117-96:/home/sysadmin# chage -d 0 toby root@ip-172-22-117-96:/home/sysadmin# chage -d 0 adler root@ip-172-22-117-96:/home/sysadmin#</pre> 
<input type="checkbox"/>	Updating and enforcing sudo permissions	Sudo visudo

```
# Per-user preferences; root won't have sensible values for them
Defaults: %sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent
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

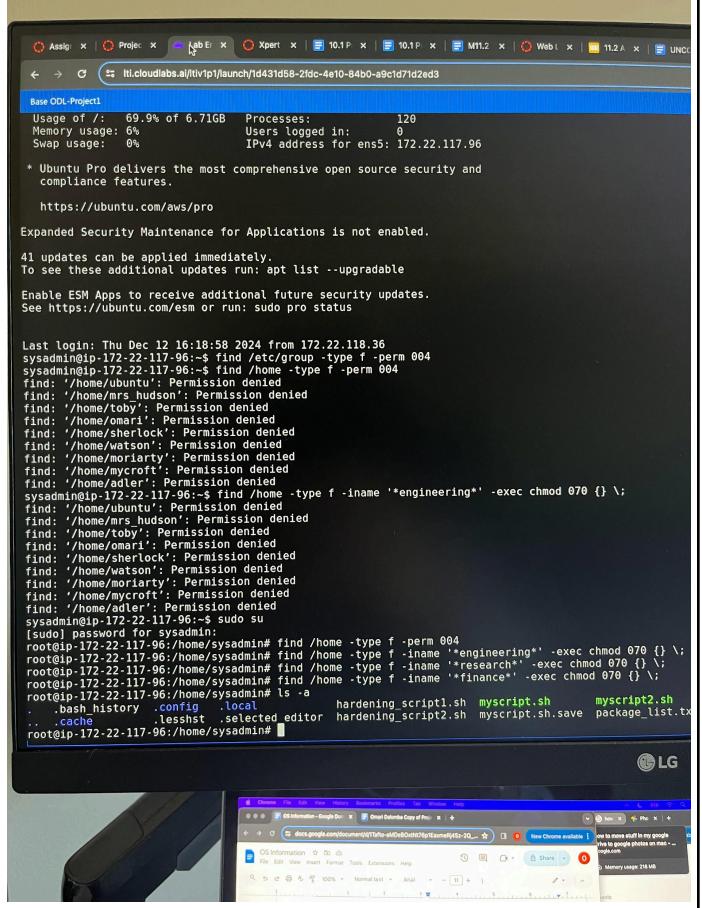
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

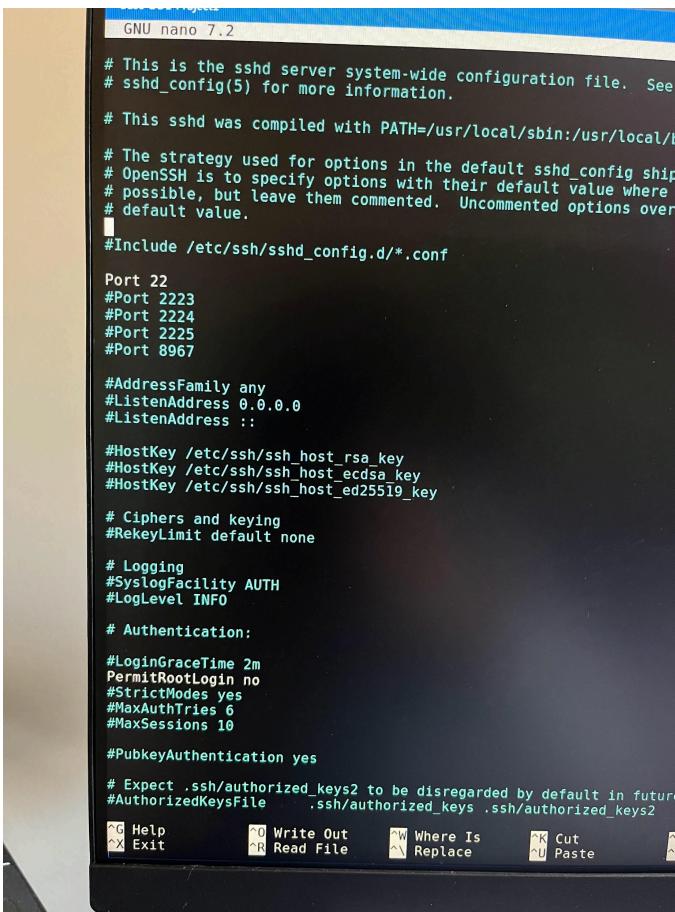
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# 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
```

<input type="checkbox"/>	<p>Validating and updating permissions on files and directories</p>	<p>Find all files with world permissions: Find /home -type f -perm 004</p> <p>Only members of the engineering group can view edit or execute Find /home -type f -name “*engineering*” -exec chmod 070 {} \;</p> <p>Only members of the research group can view edit or execute Find /home -type f -name “*research*” -exec chmod 070 {} \;</p> <p>Only members of the finance group can view edit or execute Find /home -type f -name “*finance*” -exec chmod 070 {} \;</p> <p>Ls -a</p> 
--------------------------	---	---

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

```
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_hosts
#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'.

```

Help Write Out Where Is Cut
Exit Read File Replace Paste Execute
Justify

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

```
Base CDL-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 Temperature: -273.1 C
Usage of /: 73.2% of 6.71GB Processes: 124
Memory usage: 6% Users logged in: 0
Swap usage: 0% IPv4 address for ens5: 172.22.117.96

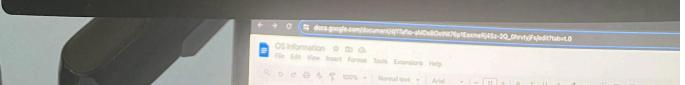
* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro

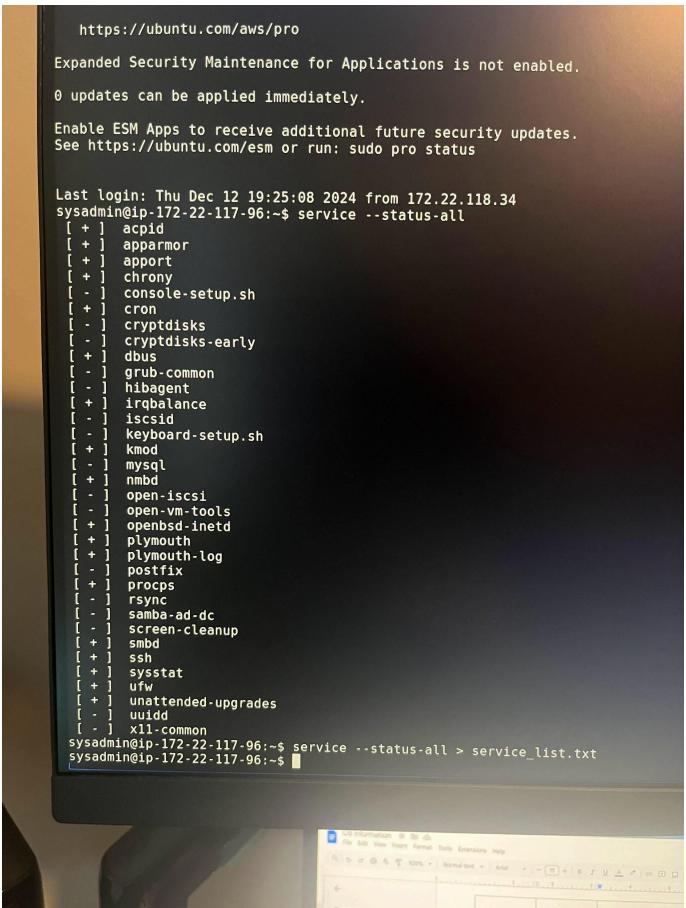
Expanded Security Maintenance for Applications is not enabled.
0 updates can be applied immediately.

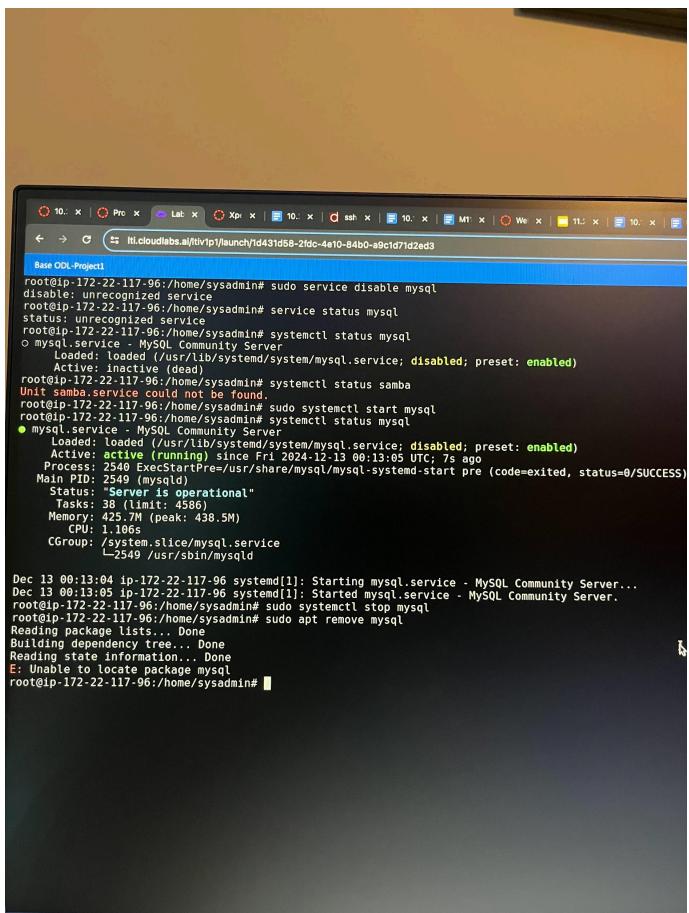
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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
cpuid/noble,now 1:2.0.34~lubuntu2 amd64 [installed,automatic]
adduser/noble,now 3.137ubuntu1 all [installed,automatic]
amd64-microcode/noble-updates,noble-security,now 3.20231019.1ubuntu2.1 amd64 [installed,automatic]
apparmor/noble-updates,now 4.0.1real4.0.1~ubuntu0.24.04.3 amd64 [installed,automatic]
apport-core-dump-handler/notebook,now 2.28.1-0ubuntu3.1 all [installed,upgradable to: 2.28.1-0u
apport-symptoms/noble,now 0.25 all [installed,automatic]
apport/notebook,now 2.28.1-0ubuntu3.1 all [installed,upgradable to: 2.28.1-0ubuntu3.3]
aptstream/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]
atrim/noble,now 1:2.5.2-1build2 amd64 [installed,automatic]
base-files/noble-updates,now 13~ubuntu16.1 amd64 [installed]
base-passwd/noble,now 3.6.3build1 amd64 [installed]
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
```



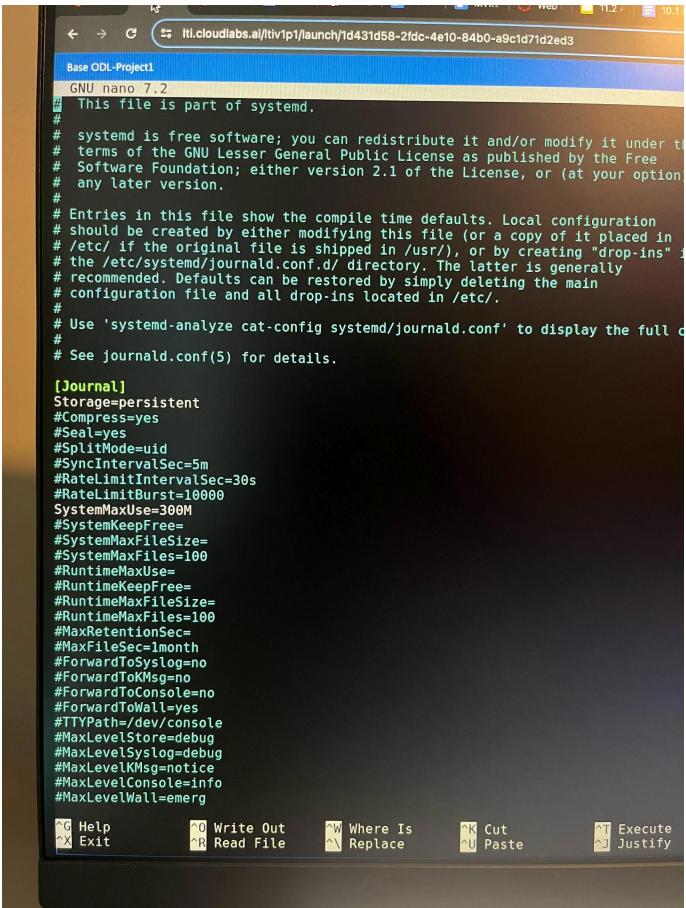
```
tcpdump/noble,now 7.6.q-33 amd64 [installed,automatic]
tcpdump/noble,now 4.99.4-3ubuntu4 amd64 [installed,automatic]
tdb-tools/noble,now 1.4.10-1build1 amd64 [installed,automatic]
thin-provisioning-tools/noble-updates,now 0.9.0-2ubuntu5.1 amd64 [installed,automatic]
Building dependency tree... Done
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 linux-
  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/postinst.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
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
```

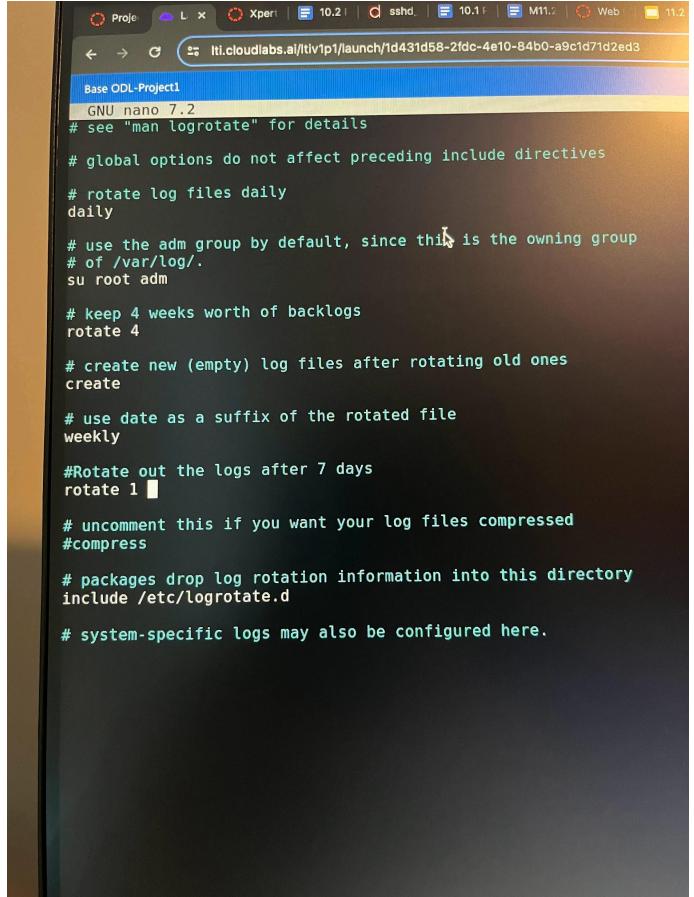
<input type="checkbox"/>	Disabling unnecessary services	<p>Service --status-all</p> <p>List out all services and output into a file Service --status-all > service_list.txt</p> <p>See if any of the services are running Systemctl status mysql Systemctl status samba</p> <p>Stop,disable and remove the services Systemctl stop mysql Systemctl stop samba Systemctl disable mysql Systemctl disable samba</p>  <pre> 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 19:25:08 2024 from 172.22.118.34 sysadmin@ip-172-22-117-96:~\$ service --status-all [+] acpid [+] apparmor [+] apport [+] chrony [-] console-setup.sh [+] cron [-] cryptdisks [-] cryptdisks-early [+] dbus [-] grub-common [-] hibagent [+] irqbalance [-] iscsid [-] keyboard-setup.sh [+] kmiod [-] mysql [+] nmbd [-] open-iscsi [-] open-vm-tools [+] opensbsd-inetd [+] plymouth [+] plymouth-log [-] postfix [+] procps [-] rsync [-] samba-ad-dc [-] screen-cleanup [+] smbd [+] ssh [+] sysstat [+] ufw [+] unattended-upgrades [-] uidd [-] x11-common sysadmin@ip-172-22-117-96:~\$ service --status-all > service_list.txt sysadmin@ip-172-22-117-96:~\$ </pre>



```
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)
       Docs: man:mysqld(8)
Unit mysql.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
       Main PID: 2549 (mysqld)
          CPU: 1.106s
         Tasks: 38 (limit: 4586)
        Status: "Server is operational"
        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#
```

<input type="checkbox"/>	Enabling and configuring logging	<p>Access the both of the files</p> <p>Nano /etc/systemd/journal.conf</p> <p>Nano /etc/logrotate.conf</p>  <pre> Base ODL-Project1 GNU nano 7.2 # This file is part of systemd. # # systemd is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version. # # Entries in this file show the compile time defaults. Local configuration should be created by either modifying this file (or a copy of it placed in /etc/), if the original file is shipped in /usr/, or by creating "drop-ins" in the /etc/systemd/journald.conf.d/ directory. The latter is generally recommended. Defaults can be restored by simply deleting the main configuration file and all drop-ins located in /etc/. # # Use 'systemd-analyze cat-config systemd/journald.conf' to display the full configuration. # # See journald.conf(5) for details. [Journal] Storage=persistent #Compress=yes #Seal=yes #SplitMode=uid #SyncIntervalSec=5m #RateLimitIntervalSec=30s #RateLimitBurst=10000 SystemMaxUse=300M #SystemKeepFree= #SystemMaxFileSize= #SystemMaxFiles=100 #RuntimeMaxUse= #RuntimeKeepFree= #RuntimeMaxFileSize= #RuntimeMaxFiles=100 #MaxRetentionSec= #MaxFileSec=1month #ForwardToSyslog=no #ForwardToKMsg=no #ForwardToConsole=no #ForwardToWall=yes #TTYPath=/dev/console #MaxLevelStore=debug #MaxLevelSyslog=debug #MaxLevelKMsg=notice #MaxLevelConsole=info #MaxLevelWall=emerg </pre>

		
<input type="checkbox"/>	Scripts created	<pre>Nano myscript.sh Nano myscript2.sh chmod +x cp myscript.sh hardening_script1.sh cp myscript2.sh hardening_script2.sh</pre>

```
Proj Xper 10.3 sshd 10.1 MTI 10.3 11.2 10.1 UNC 10.1
It.cloudlabs.ai/itv/p/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
GNU nano 7.2

#Backup the OS
echo "Backing up the OS.. `sudo tar -cvzf /baker_street_backup.tar.gz --exclude=/baker_s
--exclude=/nv --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

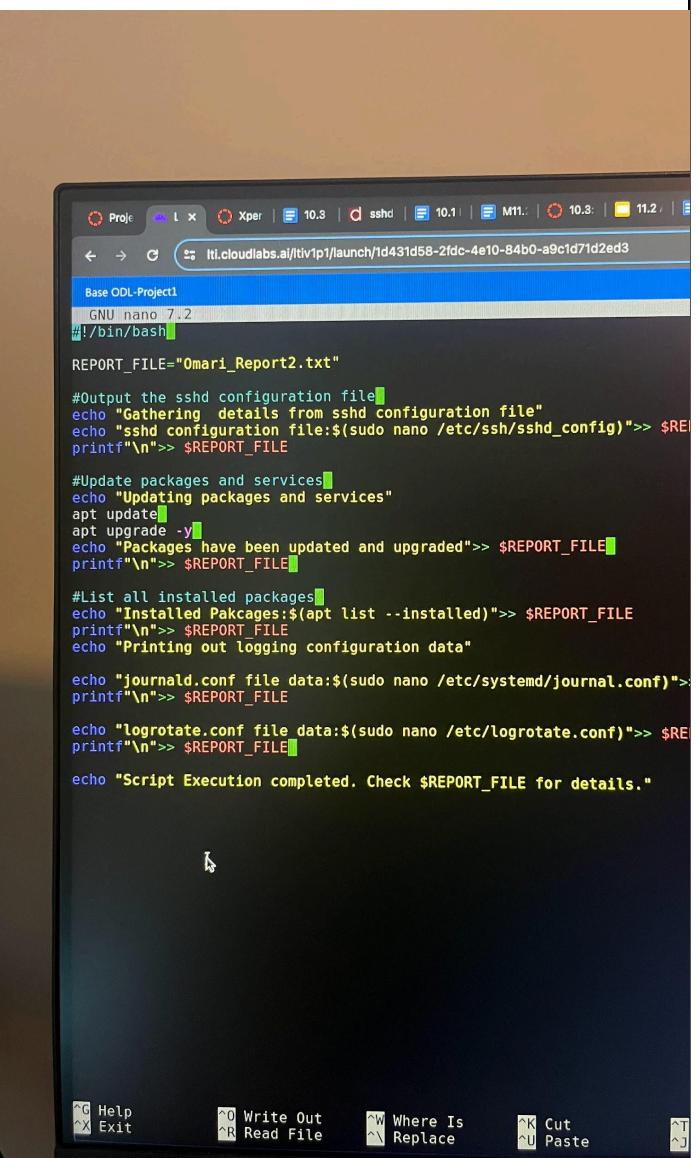
#Script to check files with world permission and update them
echo "Checking for files with world permissions..."
sudo find /home -type f -perm /+rwx -exec chmod o={} \;
echo "World permissions have been removed from any files found">> $REPORT_FILE
printf "\n">>> $REPORT_FILE

#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."
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a blue header bar with various icons and the URL `lti.cloudlabs.ai/litv/p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3`. Below the header, the terminal title is "Base ODL-Project1" and the prompt is "#!/bin/bash". The script content is as follows:

```
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)">> $REPORT_FILE
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

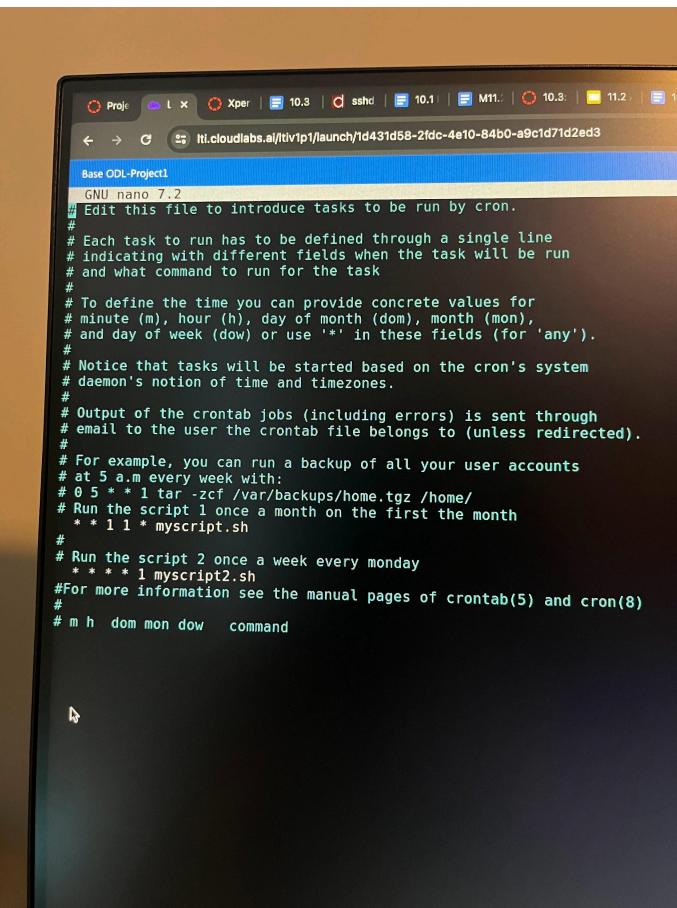
#List all installed packages
echo "Installed Packages:$(apt list --installed)">> $REPORT_FILE
printf"\n">> $REPORT_FILE
echo "Printing out logging configuration data"

echo "journald.conf file data:$(sudo nano /etc/systemd/journal.conf)">> $REPORT_FILE
printf"\n">> $REPORT_FILE

echo "logrotate.conf file data:$(sudo nano /etc/logrotate.conf)">> $REPORT_FILE
printf"\n">> $REPORT_FILE

echo "Script Execution completed. Check $REPORT_FILE for details."
```

At the bottom of the terminal window, there's a menu bar with the following options: Help (Alt+G), Exit (Alt+A), Write Out (Alt+O), Read File (Alt+R), Where Is (Alt+W), Replace (Alt+M), Cut (Alt+K), Paste (Alt+U), and a separator key (Alt+T).

<input type="checkbox"/>	Scripts scheduled with cron	<p>Crontab -e</p>  <pre> GNU nano 7.2 Edit this file to introduce tasks to be run by cron. # # Each task to run has to be defined through a single line # indicating with different fields when the task will be run # and what command to run for the task # # To define the time you can provide concrete values for # minute (m), hour (h), day of month (dom), month (mon), # and day of week (dow) or use '*' in these fields (for 'any'). # # Notice that tasks will be started based on the cron's system # daemon's notion of time and timezones. # # Output of the crontab jobs (including errors) is sent through # email to the user the crontab file belongs to (unless redirected). # # For example, you can run a backup of all your user accounts # at 5 a.m. every week with: # 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/ # Run the script 1 once a month on the first the month * * 1 1 * myscript.sh # # Run the script 2 once a week every monday * * * * 1 myscript2.sh #For more information see the manual pages of crontab(5) and cron(8) # m h dom mon dow command </pre>