

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/bin

# The strategy used for options in the default sshd_config shipped
# with OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override
# the 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      ^O Write Out     ^W Where Is     ^K Cut          ^T
^X Exit      ^R Read File     ^\ Replace      ^U Paste        ^J
```

```
# 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'.
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^Y Replace ^U Paste ^J Justify

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-Project
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

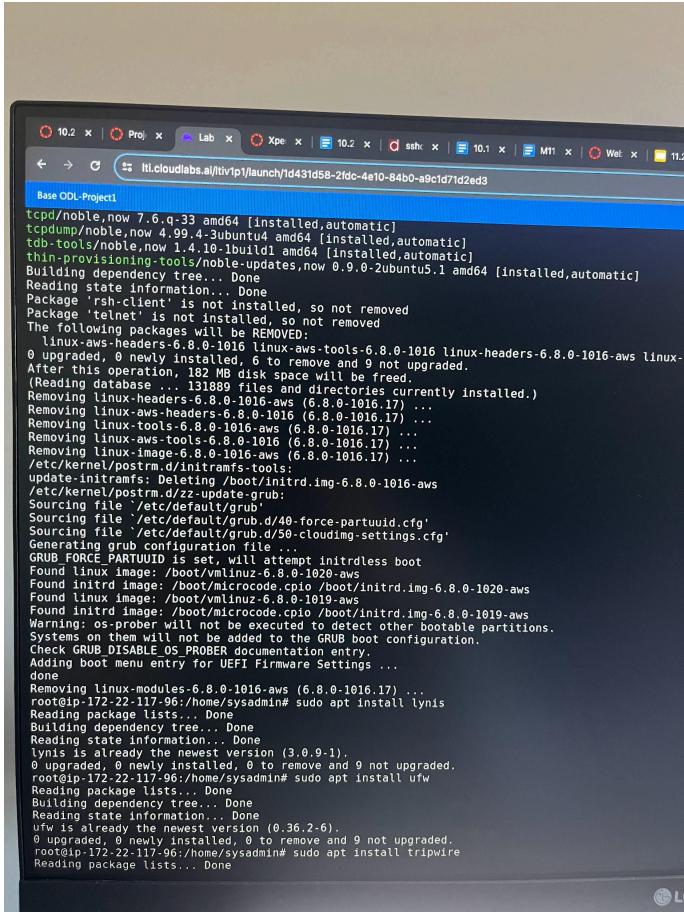
Expanded Security Maintenance for Applications is not enabled.

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
bcptid/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 3.29231019,1ubuntu2.1 amd64 [installe
aparmor/noble-updates,now 4.0.1really4.0.1-0ubuntu0.24.04.3 amd64 [installed,automatic]
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 1:0.2.1build0 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-build1 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 [instal
```



A screenshot of a terminal window titled "Base ODL-Project1". The terminal is displaying a series of commands and their outputs related to package management. It shows the removal of several packages, including "linux-aws-headers-6.8.0-1016", "linux-aws-tools-6.8.0-1016", and "ufw". The output indicates that 0 packages were upgraded, 0 were newly installed, and 6 were removed. The total disk space freed is 182 MB.

```
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/postrm d/intramfs.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 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 in 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 (3.0.0-1).
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
```

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

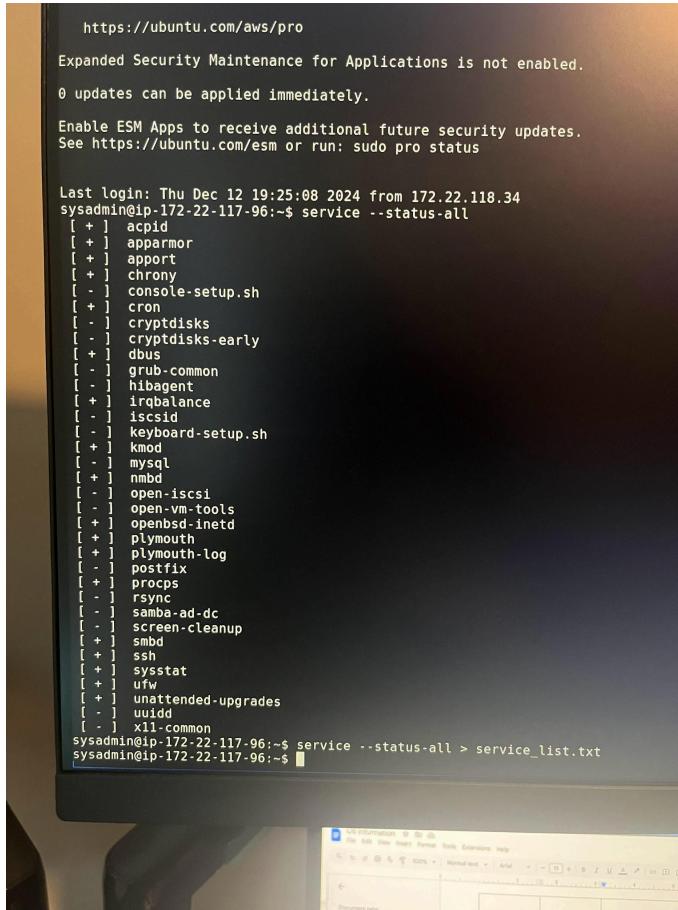
- Systemctl status mysql
- Systemctl status samba

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



```
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
[ + ] kmmod
[ - ] mysql
[ + ] nmbd
[ - ] open-iscsi
[ - ] open-vm-tools
[ + ] openbsd-inetd
[ + ] plymouth
[ + ] plymouth-log
[ - ] postfix
[ + ] procps
[ - ] rsync
[ - ] samba-ad-dc
[ - ] screen-cleanup
[ + ] smbd
[ + ] ssh
[ + ] sysstat
[ + ] ufw
[ + ] unattended-upgrades
[ - ] uuid
[ - ] x11-common
sysadmin@ip-172-22-117-96:~$ service --status-all > service_list.txt
sysadmin@ip-172-22-117-96:~$
```

The screenshot shows a terminal window titled "Basic CDE-Project" with a blue header bar. The terminal is running on a Linux system with IP address 172.22.117.96. The user is root. The session starts with several failed attempts to disable the mysql service using sudo service disable mysql. It then lists the status of various services including mysql, samba, and mysql.service. The mysql.service entry shows it is active (running) with a main PID of 2549 and a status of "Server is operational". Following this, the user runs sudo systemctl stop mysql, which stops the service. Finally, the user runs sudo apt remove mysql, which removes the package. The terminal ends with a message from apt stating "E: Unable to locate package mysql".

```
root@ip-172-22-117-96:/home/sysadmin# sudo service disable mysql
disolve: 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# sudo 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)
         Status: "Server is operational"
          Tasks: 1 (limit: 4586)
        Memory: 426.7M (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#
```

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

```

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/journal.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
#ForwardToMsg=no
#ForwardToConsole=no
#ForwardToWall=yes
#TTYPath=/dev/console
#MaxLevelStore=debug
#MaxLevelSyslog=debug
#MaxLevelKMsg=notice
#MaxLevelConsole=info
#MaxLevelWall=emerg

^G Help      ^O Write Out    ^W Where Is    ^K Cut        ^T Execute
^X Exit      ^R Read File    ^X Replace    ^U Paste      ^J Justify

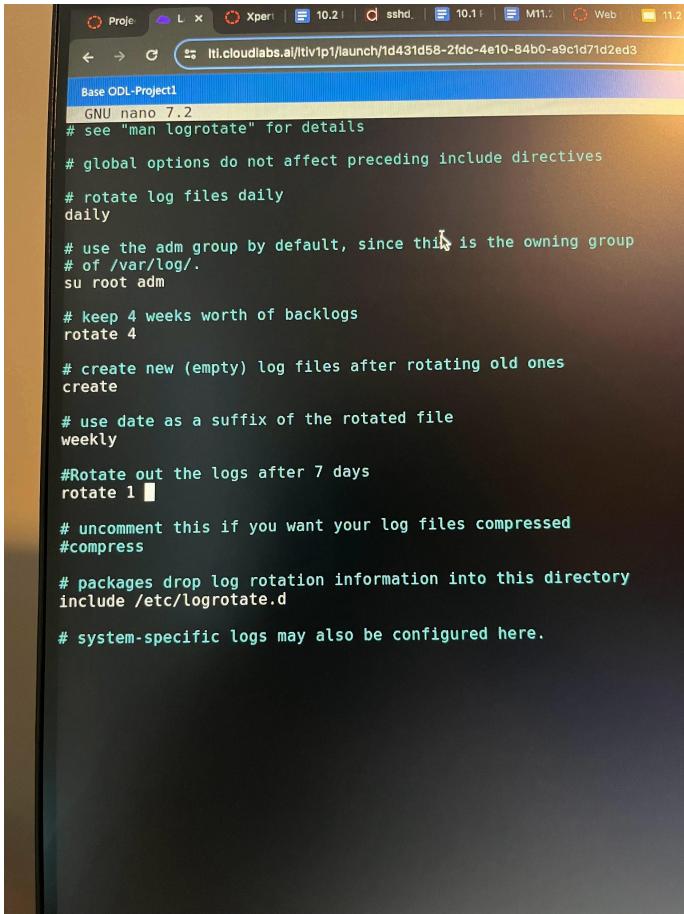
```

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



The screenshot shows a terminal window with a dark background and light-colored text. The title bar indicates the URL is `lti.cloudlabs.ai/ltiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3`. The content of the terminal is a logrotate configuration file:

```
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.
```