Project 1 Day 1

Project Description

Today, you will play the role of a security professional tasked with hardening a Linux server owned by The Baker Street Corporation (BSC). The BSC has confidential data on their server and they need you to confirm that their system is properly configured to protect them from security breaches. If you determine any security issues, they also want you to make the necessary updates.

Today's focus is on the **BSC's** Linux server's users, groups, files, and directories. You will be completing 5 steps:

- **(1)** Pre-hardening steps: System inventory and backup
- **(2)** Auditing users and groups
- **(3)** Updating and enforcing password policies
- **(4)** Updating and enforcing sudo permissions
- **(5)** Validating and updating permissions on files and directories.

Part 1: Pre-Hardening Steps

In Part 1, before you start hardening the Linux Server, it is imperative that you document details about the operating system you are hardening and create a backup of the important files on the OS in case there is an issue during the hardening process. You will need to research any commands you aren't familiar with.

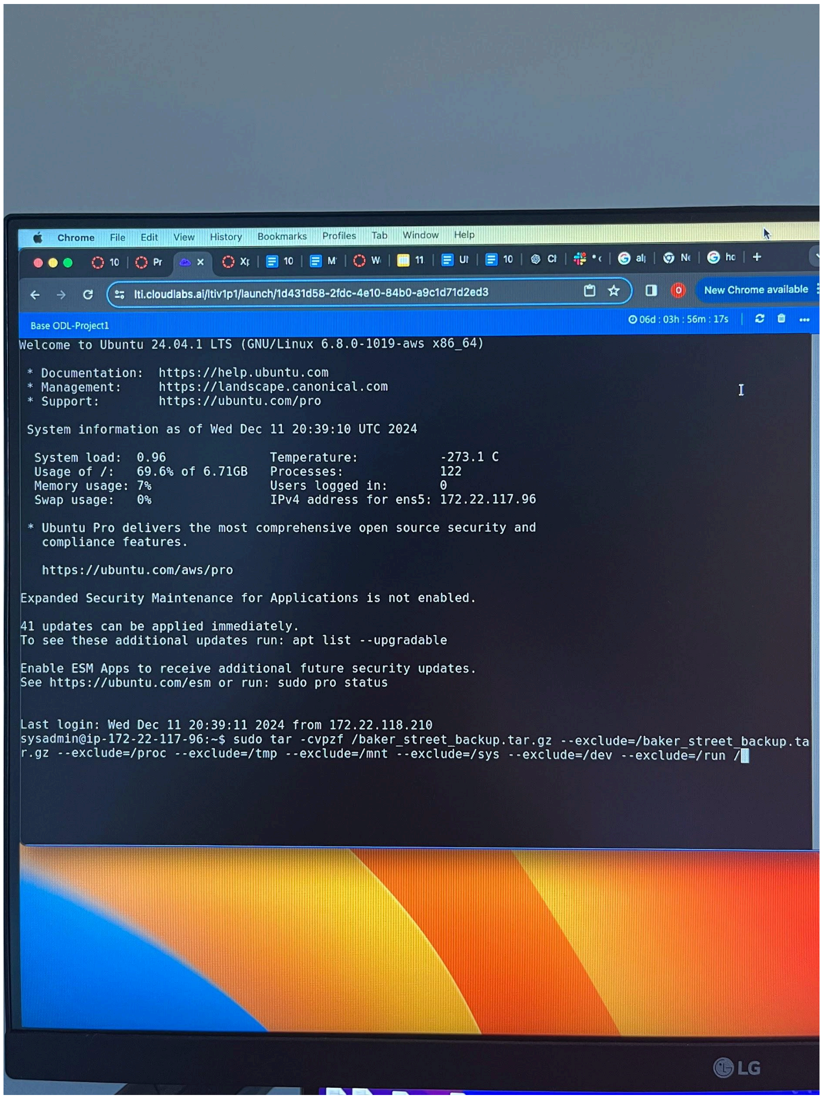
- *Be sure to research the commands to complete these tasks!*
  - HostName
  - OS version
  - Memory information
  - Uptime information

These are the following command to details about the operating system:

1. `Hostname` allows us to find the hostname on the linux system.
2. `uname -a` allows us to find the OS version of the linux system.
3. `free -h` allows us to find the memory information of the linux system.
4. `Uptime` allows us to get the uptime information for the system

- Now backup the OS with a command

1. `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/ `allows to OS to backup to save the system configurations



```
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1019-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Dec 11 20:39:10 UTC 2024

  System load:  0.96               Temperature:           -273.1 C
  Usage of /:   69.6% of 6.71GB    Processes:             122
  Memory usage: 7%                 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.

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 20:39:11 2024 from 172.22.118.210
sysadmin@ip-172-22-117-96:~$ sudo tar -cvpzf /baker_street_backup.tar.gz --exclude=/baker_street_backup.ta
r.gz --exclude=/proc --exclude=/tmp --exclude=/mnt --exclude=/sys --exclude=/dev --exclude=/run /
```

.

Part 2: Auditing Users and Groups

In Part 2, you are tasked with auditing BSC's employees to make sure all of the correct users and groups have the minimum required access to do their work.

- Note the current staff list and position updates:

	Employee Name	**Employment Status**
1	sherlock	Employed
2	watson	Employed
3	mycroft	Employed
4	moriarty	On temporary leave
5	lestrade	Terminated
6	irene	Terminated
7	mrs_hudson	On temporary leave
8	mary	Terminated
9	gregson	Terminated
10	toby	Employed
11	adler	Employed

- Remove all staff who have been terminated.
    - Be sure to remove all home directories and files.

1. `deluser -remove-all-files lestrade.`
2. `deluser -remove-all-files irene`
3. `deluser -remove-all-files mary`
4. `deluser -remove-all-files gregson`

- Lock all user accounts of staff on temporary leave.

1. `usermod -L moriarty.`
2. `usermod -L mrs_hudson`

- Unlock any users who are employed.

1. `usermod -U sherlock`
2. `Usermod -U watson`
3. `Usermod -U mycroft`
4. `Usermod -U toby`

5. `Usermod -U adler`

- Move all the employees who were in the marketing department to a new group called **research**. Create this group if it doesn't exist.

1. `addgroup research` to add a new group called research.

2. `cat /etc/group` to find all the employees who are in the marketing department and mycroft was the only employee

3. `usermod -G research mycroft` to move the employee mycroft to the research department

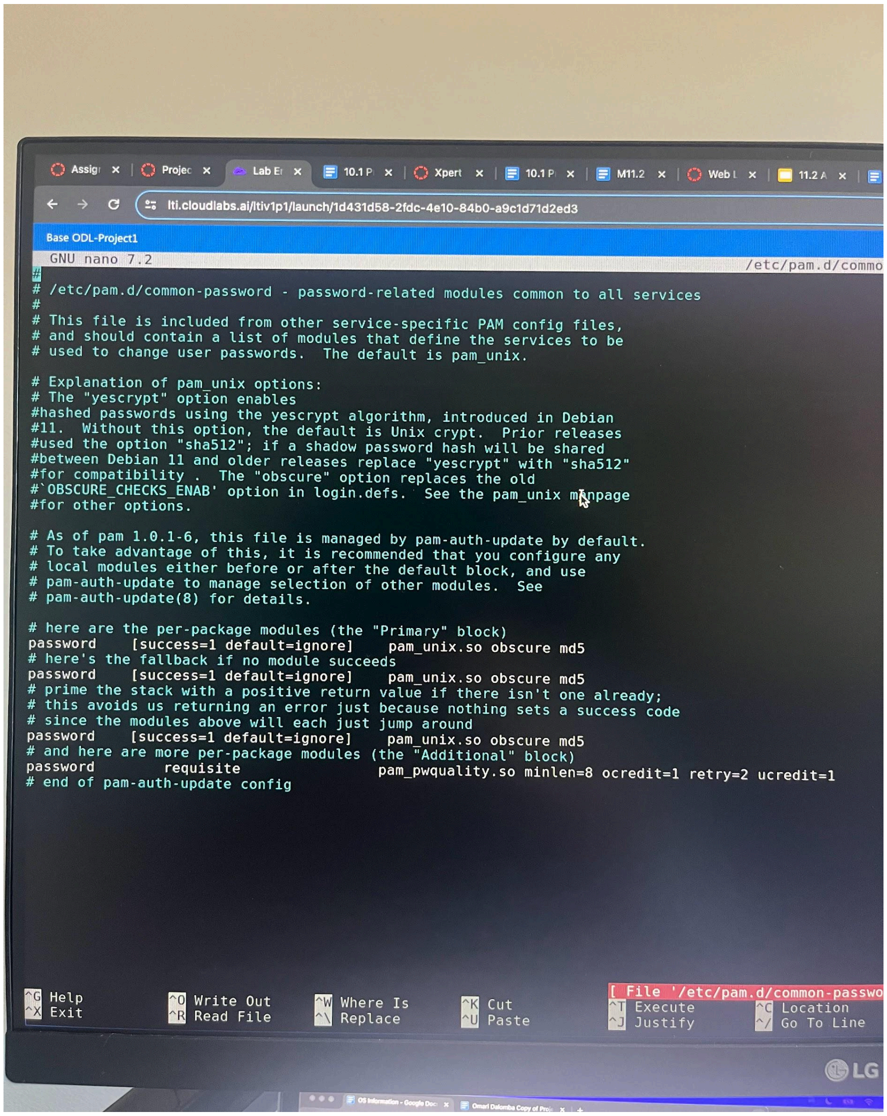
Part 3: Updating and Enforcing Password Policies

In Part 3, you are tasked with validating the security of the passwords of BSC's employees. Additionally, you will update the minimum complexity and force users to update their passwords on their next login.

Complete the following:

- Update the password requirements for all users to have:
  - Minimum 8 characters
  - At least one special character
  - Allow 2 retries
  - At least one uppercase character
- To make this update:
  - Edit the following file: **/etc/pam.d/common-password**
  - Add settings to the following line:
    - *password requisite pam_pwquality.so*

1. `nano /etc/pam.d/common-password` allows us to go to the password configuration file


Assig
Projec
Lab Er
10.1 P
Xpert
10.1 P
M11.2
Web L
11.2 A
lti.cloudlabs.ai/ltiv1p1/launch/1d431d58-2fdc-4e10-84b0-a9c1d71d2ed3
Base ODL-Project1
LG
OS Information - Google Doc
Omari Dalomba Copy of Proj

```
  GNU nano 7.2                                              /etc/pam.d/commo
#
# /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 retry=2 ucredit=1
# end of pam-auth-update config




                                                   [ File '/etc/pam.d/common-passwo
^G Help       ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit       ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

Part 4: Updating and Enforcing sudo Permissions

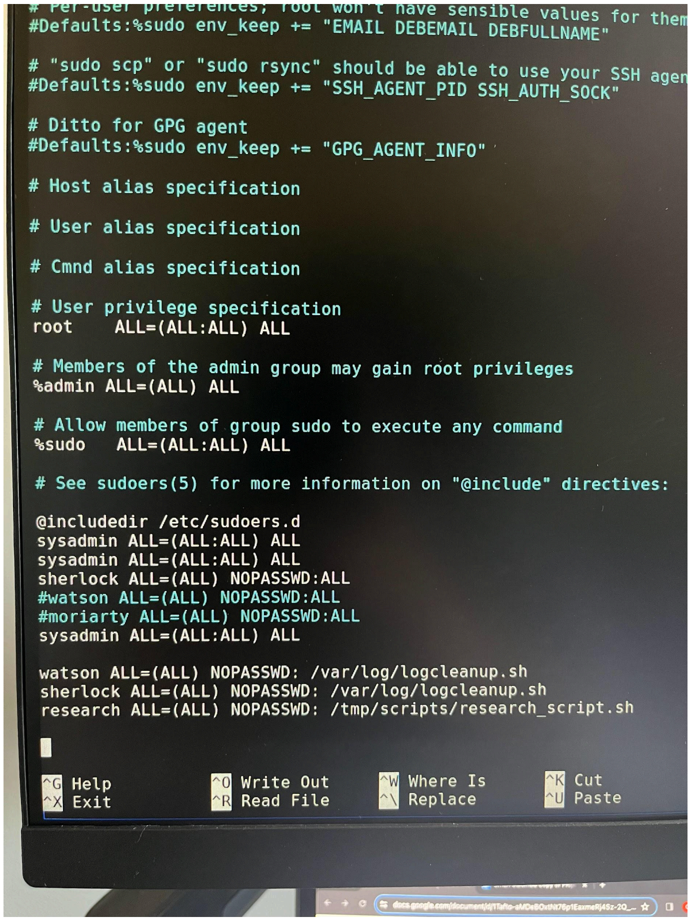
In Part 4, you are tasked with validating and updating the sudo file. BSC only wants a small group to be able to use sudo, and for those who have sudo, the only privileges they should have are to complete very specific tasks.

Complete the following:

- The only employee who should have **full sudo privileges** is Sherlock. Remove all other full privileged users.
- Watson and Mycroft should only have sudo privileges to run a script located here:

    - /var/log/logcleanup.sh
- All employees who belong to the **research** group should have sudo privileges to run the following script:
    - /tmp/scripts/research_script.sh
- Be sure to note on your checklist what you have completed.

`1. Sudo visudo` brings us to a file that controls who can run commands with sudo.



```
# 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 agen
#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
```

Part 5: Validating and Updating Permissions on Files and Directories

In Part 5, you are tasked with validating and updating any files and directories that have weak security permissions.

- In every user’s home directory, there should be **no files** that have any world permissions to read, write, or execute.
    - Find any of them and update to remove the world permissions.

`1. Find /home -type f -perm 004` is to find all the files with world permissions and remove them.

- Find the following files and make the associated updates:
  (**Hint:** Search with the case-insensitive option.)
    - **Engineering scripts (scripts with the word ‘engineering’ in the filename):** Only members of the engineering group can view, edit, or execute.
    - **Research scripts:** Only members of the research group can view, edit, or execute.
    - **Finance scripts:** Only members of the finance group can view, edit, or execute.

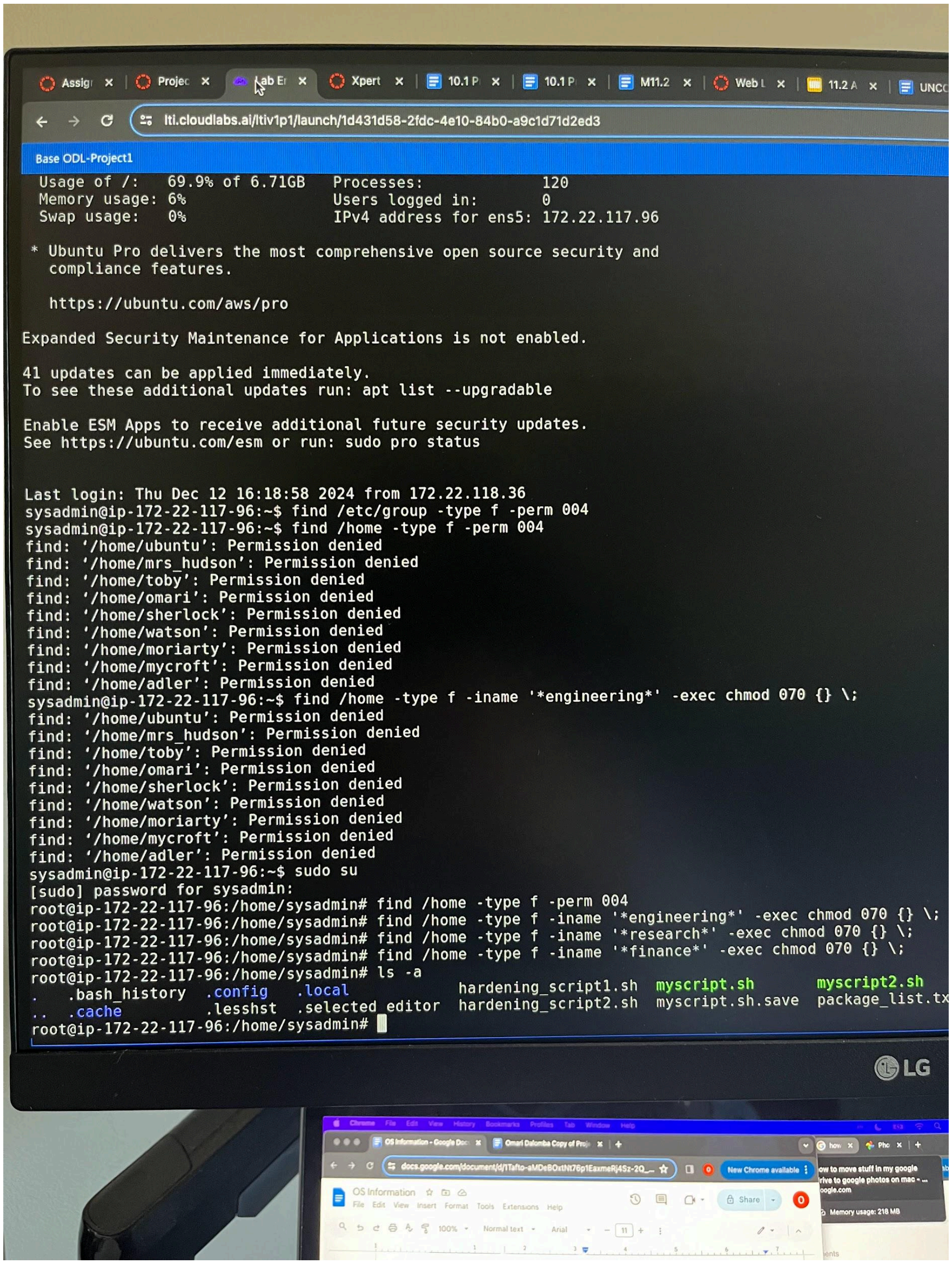
1. `Find /home -type f -name ‘*engineering*’ -exec chmod 070 {} \;` allows only members on the engineering group to view, edit or execute

2. `Find /home -type f -name ‘*research*’’ -exec chmod 070 {} \;` allows only members of the research group to view, edit or execute

3. `Find /home -type f -name ‘*finance*’’ -exec chmod 070 {} \;` allows only members of the Finance group to view, edit or execute

- Some employees may leave files with hidden passwords. Find those files and remove them as no employee should have their passwords stored on the server.

1. `Ls -a` allows us to look for all hidden files and passwords.



```
  Usage of /:   69.9% of 6.71GB   Processes:             120
  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.

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: Thu Dec 12 16:18:58 2024 from 172.22.118.36
sysadmin@ip-172-22-117-96:~$ find /etc/group -type f -perm 004
sysadmin@ip-172-22-117-96:~$ find /home -type f -perm 004
find: '/home/ubuntu': Permission denied
find: '/home/mrs_hudson': Permission denied
find: '/home/toby': Permission denied
find: '/home/omari': Permission denied
find: '/home/sherlock': Permission denied
find: '/home/watson': Permission denied
find: '/home/moriarty': Permission denied
find: '/home/mycroft': Permission denied
find: '/home/adler': Permission denied
sysadmin@ip-172-22-117-96:~$ find /home -type f -iname '*engineering*' -exec chmod 070 {} \;
find: '/home/ubuntu': Permission denied
find: '/home/mrs_hudson': Permission denied
find: '/home/toby': Permission denied
find: '/home/omari': Permission denied
find: '/home/sherlock': Permission denied
find: '/home/watson': Permission denied
find: '/home/moriarty': Permission denied
find: '/home/mycroft': Permission denied
find: '/home/adler': Permission denied
sysadmin@ip-172-22-117-96:~$ sudo su
[sudo] password for sysadmin:
root@ip-172-22-117-96:/home/sysadmin# find /home -type f -perm 004
root@ip-172-22-117-96:/home/sysadmin# find /home -type f -iname '*engineering*' -exec chmod 070 {} \;
root@ip-172-22-117-96:/home/sysadmin# find /home -type f -iname '*research*' -exec chmod 070 {} \;
root@ip-172-22-117-96:/home/sysadmin# find /home -type f -iname '*finance*' -exec chmod 070 {} \;
root@ip-172-22-117-96:/home/sysadmin# ls -a
.   .bash_history  .config   .local           hardening_script1.sh  myscript.sh       myscript2.sh
..  .cache         .lesshst  .selected_editor  hardening_script2.sh  myscript.sh.save  package_list.tx
root@ip-172-22-117-96:/home/sysadmin#
```