Evidence (screenshots) showing misconfiguration discovery & fixes.

Task 1: Policy + create users/groups + set permissions, enable auditing.

Create a baseline policy document: who needs sudo, group roles, and file access requirements for a small team (e.g., admin, dev, auditor)

On an Ubuntu VM, create users and groups according to the policy (use useradd, groupadd).

```
┌──(kali㉿kali)-[~]
└─$ # Groups
sudo groupadd admin
sudo groupadd dev
sudo groupadd auditor

# Users (change names/emails as needed)
sudo useradd -m -G admin alice
sudo useradd -m -G dev bob
sudo useradd -m -G auditor carol
# Optionally set password
sudo passwd alice
sudo passwd bob
sudo passwd carol

New password:
Retype new password:
passwd: password updated successfully
New password:
Retype new password:
passwd: password updated successfully
New password:
Retype new password:
passwd: password updated successfully
```

Assign minimal privileges: configure sudoers using any text editor with least- privilege rules, set sudo rules for specific commands only.

```
┌──(kali㉿kali)-[~]
└─$ sudo visudo
```

Use POSIX permissions + ACLs for a shared project folder so that only the intended group has write access; others have read-only.

```
┌──(kali㉿kali)-[~]
└─$ sudo mkdir -p /srv/project
sudo chown :dev /srv/project
sudo chmod 2775 /srv/project  # group inheritance

# Set ACLs for auditors (read-only)
sudo setfacl -m g:auditor:rx /srv/project
sudo setfacl -m o:0 /srv/project  # Others: no access
```

Enable simple auditing (auditd) to log changes to /etc/sudoers and /etc/passwd.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install auditd
sudo auditctl -w /etc/passwd -p wa -k passwd_changes
sudo auditctl -w /etc/sudoers -p wa -k sudoers_changes
# Check logs:
sudo ausearch -k passwd_changes
sudo ausearch -k sudoers_changes

Hit:1 http://http.kali.org/kali kali-rolling InRelease
986 packages can be upgraded. Run 'apt list --upgradable' to see them.
auditd is already the newest version (1:4.1.2-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 986
Old style watch rules are slower
Old style watch rules are slower
Error opening /var/log/audit/audit.log (No such file or directory)
Error opening /var/log/audit/audit.log (No such file or directory)
```

In a separate vulnerable snapshot (instructor provides or students intentionally misconfigure), identify three misconfigurations (e.g., world- writable /etc/cron.d, unrestricted sudo NOPASSWD, weak file permissions on sensitive files).

```
┌──(kali㉿kali)-[~]
└─$ ls -ld /srv/project
getfacl /srv/project

drwxrws---+ 2 root dev 4096 Nov  5 08:03 /srv/project
getfacl: Removing leading '/' from absolute path names
# file: srv/project
# owner: root
# group: dev
# flags: -s-
user::rwx
group::rwx
group:auditor:r-x
mask::rwx
other::---
```

Task 2: Vulnerable snapshot analysis, fix issues, produce report + checklist.

Fix those misconfigurations, document steps, and show before/after evidence (ls -l, getfacl, audit logs).

```
┌──(kali㉿kali)-[~]
└─$ ls -l /etc/cron.d
# Look for files with "-rw-rw-rw-" or "-rw-r--rw-"

total 16
-rw-r--r-- 1 root root 188 Jul 30 15:39 e2scrub_all
-rw-r--r-- 1 root root 607 Jun  3 00:23 john
-rw-r--r-- 1 root root 712 Dec  4  2024 php
-rw-r--r-- 1 root root 400 Jan 15  2024 sysstat
```

Produce a remediation checklist and a short policy document for ongoing user management.

```
┌──(kali㉿kali)-[~]
└─$ ls -l /etc/shadow
# Should be -rw-r----- (640) root:shadow

-rw-r----- 1 root shadow 1909 Nov  5 08:00 /etc/shadow
```

Evidence (screenshots or text) showing misconfiguration discovery C fixes.

```
┌──(kali㉿kali)-[~]
└─$ # Before
ls -l /etc/cron.d
# Remediate
sudo chmod o-w /etc/cron.d/*
# After
ls -l /etc/cron.d

total 16
-rw-r--r-- 1 root root 188 Jul 30 15:39 e2scrub_all
-rw-r--r-- 1 root root 607 Jun  3 00:23 john
-rw-r--r-- 1 root root 712 Dec  4  2024 php
-rw-r--r-- 1 root root 400 Jan 15  2024 sysstat
total 16
-rw-r--r-- 1 root root 188 Jul 30 15:39 e2scrub_all
-rw-r--r-- 1 root root 607 Jun  3 00:23 john
-rw-r--r-- 1 root root 712 Dec  4  2024 php
-rw-r--r-- 1 root root 400 Jan 15  2024 sysstat
```

Audit logs snippet showing tracked changes.

```
┌──(kali㉿kali)-[~]
└─$ # Before
ls -l /etc/shadow
# Remediate
sudo chmod 640 /etc/shadow
sudo chown root:shadow /etc/shadow
# After
ls -l /etc/shadow

-rw-r----- 1 root shadow 1909 Nov  5 08:00 /etc/shadow
-rw-r----- 1 root shadow 1909 Nov  5 08:00 /etc/shadow
```

remediation checklist

```
┌──(kali㉿kali)-[~]
└─$ sudo ausearch -k passwd_changes
sudo ausearch -k sudoers_changes

Error opening /var/log/audit/audit.log (No such file or directory)
Error opening /var/log/audit/audit.log (No such file or directory)
```