The Insider — Write-up (Administrator)

Challenge text

An employee has been locked out for suspected leaking of confidential information.
You have been provided with a forensic image of their workstation.

Analyze the system, reconstruct its activity, recover the password used, and extract the hidden data that contains the flag.

```
sha256sum disk.img.xz
52489c8cc44c7548eaf3ebb6249b2f0019a682b6db78f9a305af7fa4e3d95cee  disk.img.xz
```

General Information

- Suspect user: insider
- Original user password: forensic123 (account locked)
- Steganography password: M3t*r3d
- Flag: flagmx{you_find_it}
- Carrier file: memories.bmp at ~/home/insider/Pictures/
- Filesystem: ext4 on a flat disk.img (no partition table)

1. Mount the image and explore the filesystem

With disk.img:

```
mkdir mnt_img
sudo mount -o loop,ro disk.img mnt_img
```

2. Identify suspicious activity of user insider

Examine their personal directory:

```
ls -lh mnt_img/home/insider
ls -lh mnt_img/home/insider/Pictures
```

You will notice:
- Normal files (team_building.jpg, vpn_config.ovpn, etc.)
- A file unusually large and with a different timestamp: memories.bmp
- A report.pdf in Documents (decoy, no flag)

3. Search for traces of removed tools (steal.sh)

steal.sh was originally in .local/bin but was deleted using shred.
This leaves traces in unallocated blocks (not recoverable via extundelete).

Brute-force string search:

```
sudo strings -a disk.img | grep -i "M3t"
```

More precise search:

```
sudo binwalk -R "M3t" disk.img
```

Offsets with partial text M3t... appear.

Extract data around an offset to reconstruct:

```
sudo dd if=disk.img bs=1 skip=227259000 count=4096 of=frag.bin
strings frag.bin | grep -i "M3t"
```

Expected to find:
Recovered script fragment: PASS="M3t*r3d"

This reveals the password for the hidden content.

4. Extract the hidden file with steghide

Using the recovered password:

```
steghide extract -sf mnt_img/home/insider/Pictures/memories.bmp -p "M3t*r3d"
```

This extracts report.zip.

5. Decompress the report and read the flag

```
unzip -P "M3t*r3d" report.zip
pdftotext report.pdf -
```

Relevant content:
...the monitoring script reported checksum flagmx{you_find_it} in accordance...

Flag found: flagmx{you_find_it}

6. Optional artifacts for deeper investigation

- Inconsistent timestamps in files (ls -l --full-time)
- Empty .bash_history (intentionally wiped)
- Modified cron records (anti-forensic traces)
- False fragments inserted in free space to mislead

Expected Outcome

Artifact	Evidence
steal.sh (deleted)	Contained PASS="M3t*r3d"
memories.bmp	Contains report.zip hidden with steghide
report.pdf	Contains the flag flagmx{you_find_it}

This write-up is for administrator use only and must not be included in the player challenge package.