Data Privacy and Compliance Report

Name: Mitchelle Anduru
Date: 23 Jan 2026
Role: Junior Security Analyst

Executive Summary

This assessment evaluated Linux file permissions, ownership, and access-control configurations against GDPR security expectations (confidentiality, integrity, resilience, and accountability). Using Lynis findings and manual validation, key issues were identified: home directory ownership mismatches affecting accountability, an insufficiently restrictive default umask, security-sensitive directory permissions (e.g., /etc/sudoers.d), and audit log integrity risks from overly permissive permissions. Remediations were implemented to enforce least privilege and trustworthy auditability, including correcting home directory ownership and unique UID/GID assignment, setting umask to 027, locking down privileged configuration paths, restricting audit log access to root (0600), validating sticky bit controls on shared temp directories, and reducing exposure of service-related spool directories. Overall, these changes strengthen compliance alignment by reducing unauthorized access risk, preserving log integrity for investigations, and improving system accountability for environments processing personal data.

Key Findings

- Home directory ownership and UID/GID ambiguity weakened accountability and could enable unauthorized access to user data.
- Default umask was not sufficiently restrictive, risking overexposure of newly created files/directories.
- Privileged access-control paths (e.g., /etc/sudoers.d) required tighter permissions to prevent escalation paths.
- Audit logs needed strong integrity controls to preserve reliable incident evidence and accountability.
- Shared world-writable directories were acceptable **only** with sticky bit (1777) to prevent cross-user tampering.

Applicable Regulations and Standards

Summarize the regulatory framework relevant to this assessment.

- What key compliance requirements apply to file permissions and access control in this scenario?
- Why is meeting these requirements critical for safeguarding sensitive data?

Answer

This assessment focused on aligning Linux file permissions and home directory configurations with GDPR security expectations, especially protecting personal data from unauthorized access or tampering. GDPR requires organizations to implement appropriate technical and organizational measures to ensure confidentiality, integrity, and resilience of processing systems, and to demonstrate accountability through controls and auditability.

Key requirements relevant to this scenario include least privilege access control, secure default configurations (e.g., restrictive umask), correct ownership of user data (clear accountability), and protection of security-relevant files such as sudo configurations and audit logs. Meeting these requirements is critical because overly permissive permissions or ambiguous ownership can lead to unauthorized access to personal data, data breaches, and loss of trust and compliance posture.

Compliance Assessment Findings

Summarize the vulnerabilities identified during the Lynis audit.

- Key vulnerabilities flagged (e.g., overly permissive file permissions, incorrect ownership). ● Cross-reference findings with relevant compliance standards or best practices (e.g., CIS Benchmarks).
- Explain the potential risks associated with each vulnerability (e.g., unauthorized access, data breaches).

Answer

Using Lynis and manual verification commands, the following vulnerabilities were identified and prioritized (cross-referenced against common hardening best practices such as CIS-style permission controls):

1. Home directory ownership mismatch (HOME-9306) — High

- What was found: Lynis warned that some home directory ownership may be incorrect. Manual checks confirmed mismatched ownership (e.g., `/home/Benny` owned by another user). We also identified an identity/accountability issue where “AnotherUser” existed but resolved to Benny’s UID/GID, breaking user-level accountability.
- GDPR principle impacted: Accountability, Confidentiality
- Risk: Blurred identity boundaries can enable unauthorized access to personal data in home directories and prevents reliable attribution of actions.

2. Default umask not sufficiently enforced (AUTH-9328) — Medium ●
What was found: Lynis suggested a stricter default umask like 027.

- GDPR principle impacted: Confidentiality, Integrity

- Risk: New files/directories could be created with overly permissive defaults, increasing exposure of user data.

3. Permissions warning on privileged configuration directory `/etc/sudoers.d` — Medium ●

What was found: Lynis flagged the directory permissions for `/etc/sudoers.d`.

- GDPR principle impacted: Integrity, Confidentiality
- Risk: If sudo rules can be modified or accessed improperly, an attacker could escalate privileges and access personal data.

4. Overly permissive file permissions flagged (FILE-7524) — High (key driver was audit logging control)

- What was found: World-writable findings included sensitive paths; most importantly, permissions for audit logging were tightened to prevent tampering.
- GDPR principle impacted: Integrity, Accountability
- Risk: If audit logs can be modified by unauthorized users, incident investigations become unreliable and accountability is undermined.

5. World-writable shared directories present (e.g., `/tmp`, `/var/tmp`, `/run/lock`) — Medium (acceptable with sticky bit)

- What was found: These were world-writable but correctly had sticky bit set (`1777`), which mitigates cross-user tampering/deletion.
- GDPR principle impacted: Integrity
- Risk: Without sticky bit, users could delete/alter each other's files, increasing integrity and confidentiality risks.

Remediations Implemented

Document the actions you took to address the vulnerabilities.

- Detail specific fixes (e.g., `chmod 750 /home/Smith`, `chown root /etc/passwd-`) and their purpose.
- Explain how these actions mitigate the identified risks.
- Describe how the remediations align with compliance standards (e.g., improving access controls, ensuring data integrity).

Answer

he following technical fixes were implemented to remediate identified vulnerabilities and align with GDPR principles:

1. **Fixed home directory ownership mismatch + restored accountability (HOME-9306)**

   Actions taken: ○ Corrected ownership mismatch for

   Benny's home:

   ■ `chown -R Benny:Benny /home/Benny`

   ○ Resolved identity/accountability issue for AnotherUser by assigning a **unique UID/GID** and ensuring the correct group existed, then applying correct ownership:

   ■ `groupadd -g 1101 AnotherUser` ■ `usermod -u 1101 -g 1101 AnotherUser` ■ `chown -R AnotherUser:AnotherUser /home/AnotherUser`

   Why it helps: Ensures user data is controlled by the correct identity (least privilege + clear attribution).

   GDPR alignment: Supports **confidentiality** (prevents unintended access) and **accountability** (unique identity ownership for auditability).

2. **Hardened default umask (AUTH-9328)**

   Actions taken: Set default umask to **027** (restrictive baseline) in `/etc/login.defs` so new files/directories are not created overly permissive.

   Why it helps: Prevents accidental overexposure of newly created user files.

   GDPR alignment: Supports **confidentiality** and **integrity** by enforcing secure defaults.

3. **Secured sudo configuration directory `/etc/sudoers.d`**

   Actions taken: Ensured strict permissions and ownership: `chown`

   ```
   root:root /etc/sudoers.d

   chmod 750 /etc/sudoers.d
   ```

   Why it helps: Protects privileged access control rules from unauthorized modification.

   GDPR alignment: Supports **integrity** (prevents unauthorized privilege escalation) and **confidentiality**.

4. **Protected audit log integrity (`/var/log/audit/audit.log`)**

Actions taken: Restricted access to audit log file:

```
chown root:root /var/log/audit/audit.log chmod 600 /var/log/audit/audit.log
```

Why it helps: Prevents log tampering and preserves trustworthy audit evidence.

GDPR alignment: Strongly supports **integrity** and **accountability**.

5. **Validated and maintained sticky bit on shared temp/lock directories**

   Actions taken: Confirmed correct sticky bit settings (and re-applied where relevant):

   `/tmp`, `/var/tmp`, `/run/lock` set to `1777`

   Why it helps: Allows shared use but prevents users deleting/modifying each other's files.

   GDPR alignment: Supports **integrity** and reduces risk of cross-user data interference.

6. **Restricted Samba spool directory permissions (risk reduction)**

   Actions taken: Tightened permissions on `/var/spool/samba`:

   ```
   chmod 0750 /var/spool/samba
   ```

   Why it helps: Reduces exposure of a service directory that could otherwise be used to drop/alter files.

   GDPR alignment: Supports **confidentiality** and **integrity** through least privilege.

Compliance Alignment and Broader Impact

Reflect on how your actions align with compliance frameworks and improve data security.

- How did your remediations address specific compliance requirements (e.g., restricting permissions on sensitive files)?
- How do these actions support broader data privacy goals for the organization?

Answer

These remediations directly strengthen **access control** and reduce the risk of unauthorized access to personal data stored in user home directories. Correct ownership and unique identity assignment ensure user data is attributable and protected, supporting GDPR's accountability expectations. Tightening umask establishes secure defaults so that new files are not inadvertently exposed.

Restricting audit log permissions improves **integrity** and preserves trustworthy evidence for investigations, supporting organizational accountability and governance. Securing sudo configurations and limiting sensitive service directories reduces the chance of privilege escalation that could lead to data breaches. Overall, the system's confidentiality and integrity controls are improved, reducing the likelihood and impact of unauthorized access or misuse of personal data

---

Compliance Reflection and Recommendations

Reflection on Compliance Efforts

Summarize how the steps taken in this report contributed to achieving compliance and improving data privacy.

- How did the compliance assessment, technical remediations, and broader safeguards align with compliance frameworks such as GDPR or HIPAA?
- Reflect on the overall impact of your efforts on the organization's data privacy posture.

Answer

This lab followed a compliance workflow: assess (Lynis + verification), remediate (permissions/ownership/umask hardening), and validate (re-audit). The changes align strongly with GDPR principles: **confidentiality** was improved through least-privilege permissions and correct ownership; **integrity** was strengthened by securing privileged paths (sudoers) and preventing audit log tampering; and **accountability** was reinforced by resolving ambiguous identity/ownership and protecting audit trails.

Lessons Learned

Identify key takeaways from the process.

- What did you learn about aligning technical changes with compliance goals?
- How did this experience reinforce the importance of continuous monitoring, employee training, or other compliance best practices?

Answer

Tool findings must be validated with system evidence (e.g., `ls -ld`, `stat`, user/group checks) before making changes.

Ownership is not just “nice to have”. It is central to **accountability** and reliable access control. Duplicate UID/GID scenarios can silently break auditability.
File permission remediations must be applied safely (protect essential shared directories with sticky bit rather than removing required write access).

Recommendations for Maintaining Compliance

Provide actionable recommendations for ensuring ongoing compliance.

- Propose specific steps to maintain compliance, such as conducting regular audits, updating policies as regulations evolve, or enhancing employee training programs.
- Highlight any unresolved issues or areas for improvement and explain how they could be addressed in the future.

Answer

Regular audits: Run Lynis on a defined schedule (e.g., monthly) and after major changes (user provisioning, new services, configuration changes). Track warning trends over time.
Automated permission monitoring: Implement monitoring/alerts for unexpected `chmod/chown` on sensitive paths (home directories, sudo configs, audit logs).

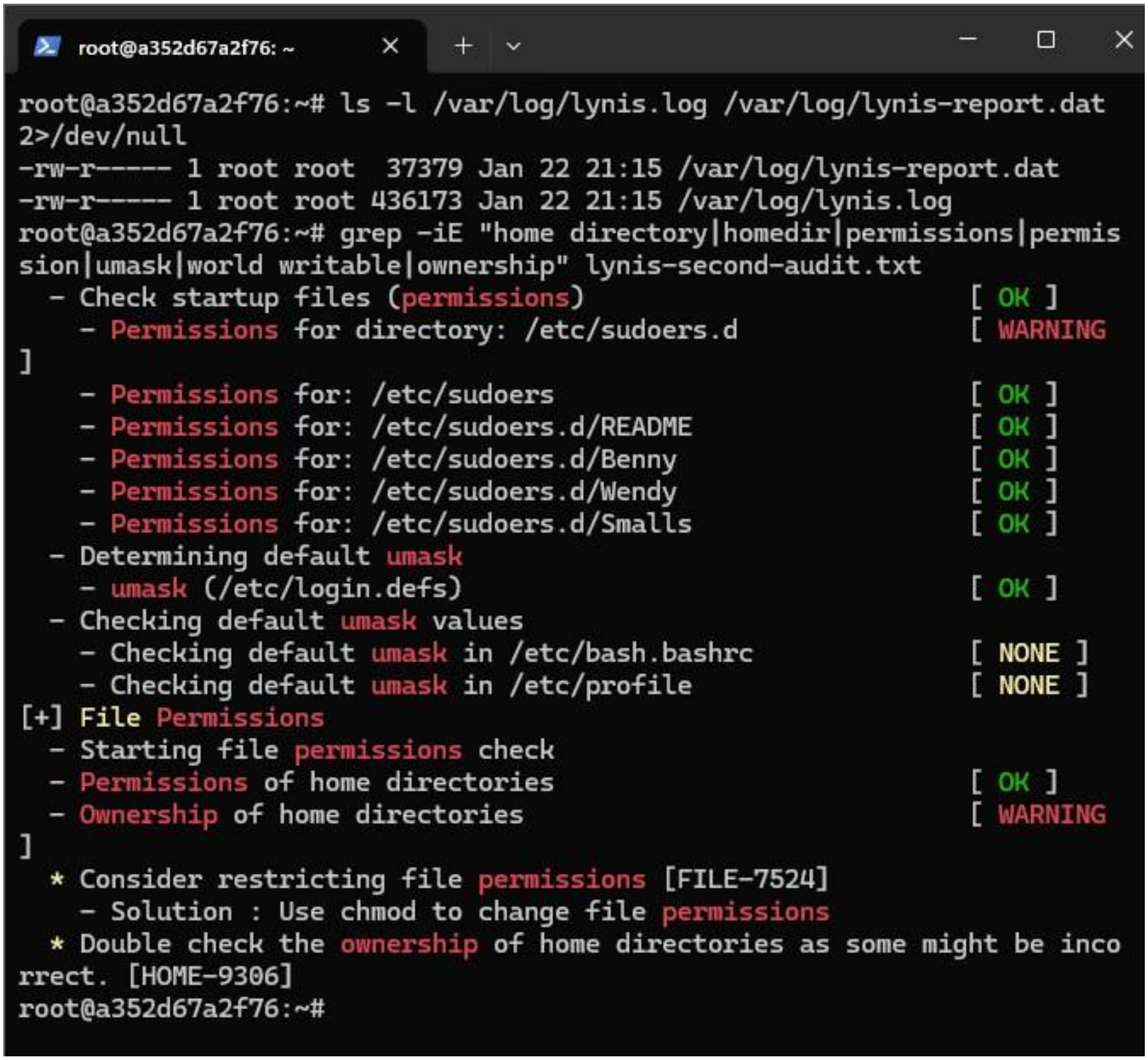
Access control policy: Enforce baseline standards: home dirs `750`, secure umask `027`, strict ownership matching user identity, audit logs restricted to root, and privileged configuration directories locked down.

Employee training: Train admins and staff on safe permission practices (avoid `chmod 777`, proper handling of sensitive files, and why logs/ownership matter). Provide a simple “permissions cheat sheet.”

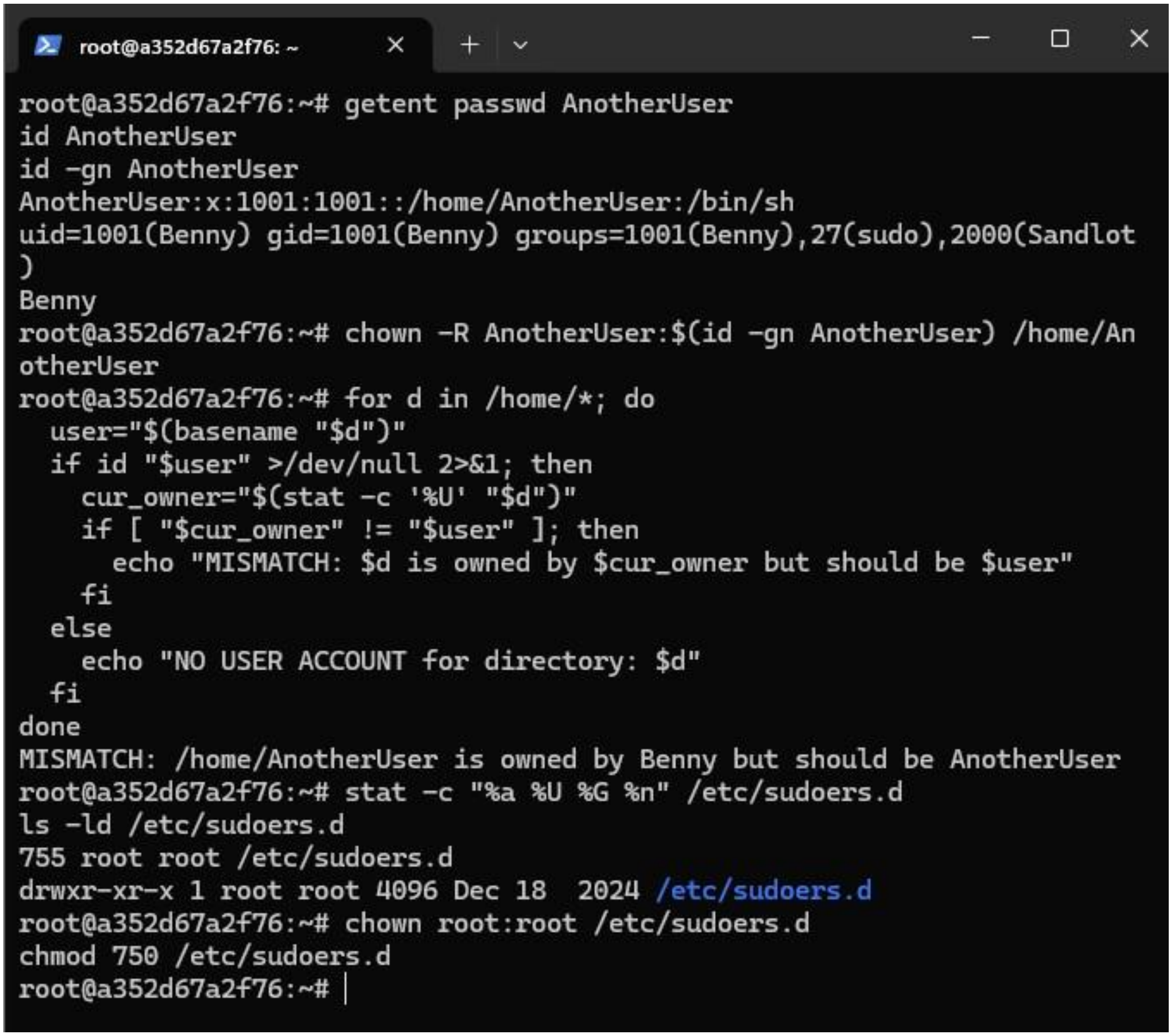
Exception handling: If any directories must remain world-writable for service reasons, require sticky bit and document justification, owner, and review frequency.

Screenshots

Identifying which homes don’t match the account owner

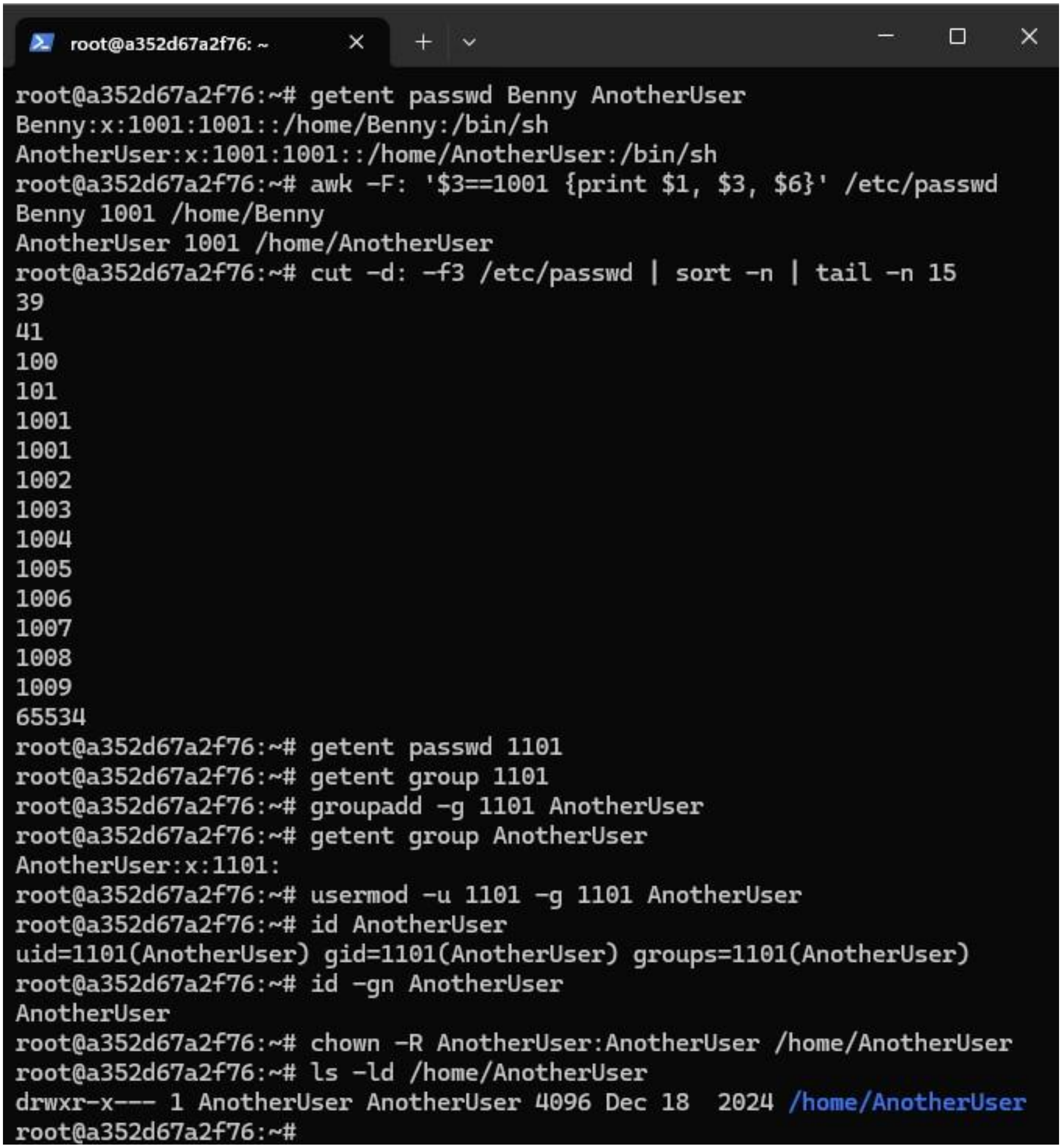


```
root@a352d67a2f76:~# ls -l /var/log/lynis.log /var/log/lynis-report.dat
2>/dev/null
-rw-r----- 1 root root  37379 Jan 22 21:15 /var/log/lynis-report.dat
-rw-r----- 1 root root 436173 Jan 22 21:15 /var/log/lynis.log
root@a352d67a2f76:~# grep -iE "home directory|homedir|permissions|permis
sion|umask|world writable|ownership" lynis-second-audit.txt
  - Check startup files (permissions)                         [ OK ]
    - Permissions for directory: /etc/sudoers.d               [ WARNING
]
    - Permissions for: /etc/sudoers                           [ OK ]
    - Permissions for: /etc/sudoers.d/README                  [ OK ]
    - Permissions for: /etc/sudoers.d/Benny                   [ OK ]
    - Permissions for: /etc/sudoers.d/Wendy                   [ OK ]
    - Permissions for: /etc/sudoers.d/Smalls                  [ OK ]
  - Determining default umask
    - umask (/etc/login.defs)                                 [ OK ]
  - Checking default umask values
    - Checking default umask in /etc/bash.bashrc              [ NONE ]
    - Checking default umask in /etc/profile                  [ NONE ]
[+] File Permissions
  - Starting file permissions check
  - Permissions of home directories                           [ OK ]
  - Ownership of home directories                             [ WARNING
]
  * Consider restricting file permissions [FILE-7524]
    - Solution : Use chmod to change file permissions
  * Double check the ownership of home directories as some might be inco
rrect. [HOME-9306]
root@a352d67a2f76:~#
```



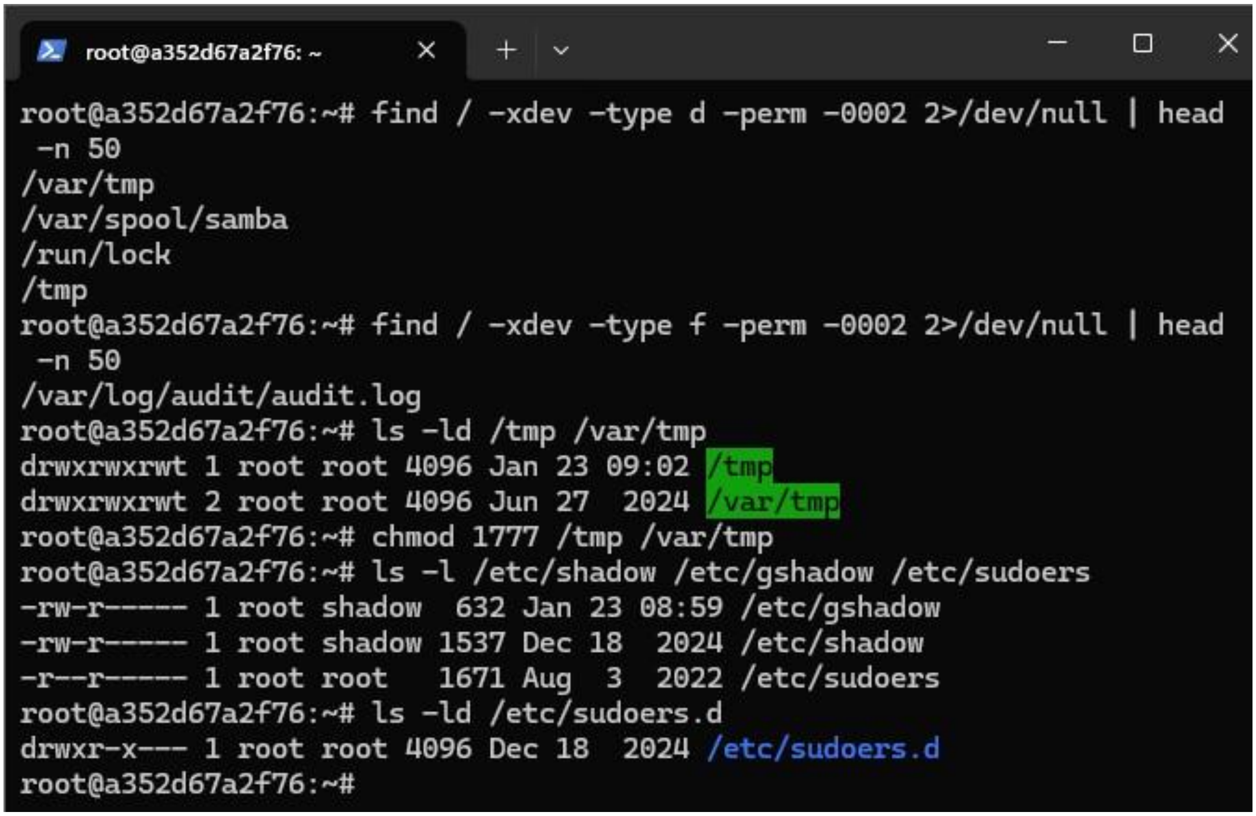
```
root@a352d67a2f76:~# getent passwd AnotherUser
id AnotherUser
id -gn AnotherUser
AnotherUser:x:1001:1001::/home/AnotherUser:/bin/sh
uid=1001(Benny) gid=1001(Benny) groups=1001(Benny),27(sudo),2000(Sandlot
)
Benny
root@a352d67a2f76:~# chown -R AnotherUser:$(id -gn AnotherUser) /home/An
otherUser
root@a352d67a2f76:~# for d in /home/*; do
  user="$(basename "$d")"
  if id "$user" >/dev/null 2>&1; then
    cur_owner="$(stat -c '%U' "$d")"
    if [ "$cur_owner" != "$user" ]; then
      echo "MISMATCH: $d is owned by $cur_owner but should be $user"
    fi
  else
    echo "NO USER ACCOUNT for directory: $d"
  fi
done
MISMATCH: /home/AnotherUser is owned by Benny but should be AnotherUser
root@a352d67a2f76:~# stat -c "%a %U %G %n" /etc/sudoers.d
ls -ld /etc/sudoers.d
755 root root /etc/sudoers.d
drwxr-xr-x 1 root root 4096 Dec 18  2024 /etc/sudoers.d
root@a352d67a2f76:~# chown root:root /etc/sudoers.d
chmod 750 /etc/sudoers.d
root@a352d67a2f76:~# |
```

give AnotherUser a unique UID/GID + correct ownership



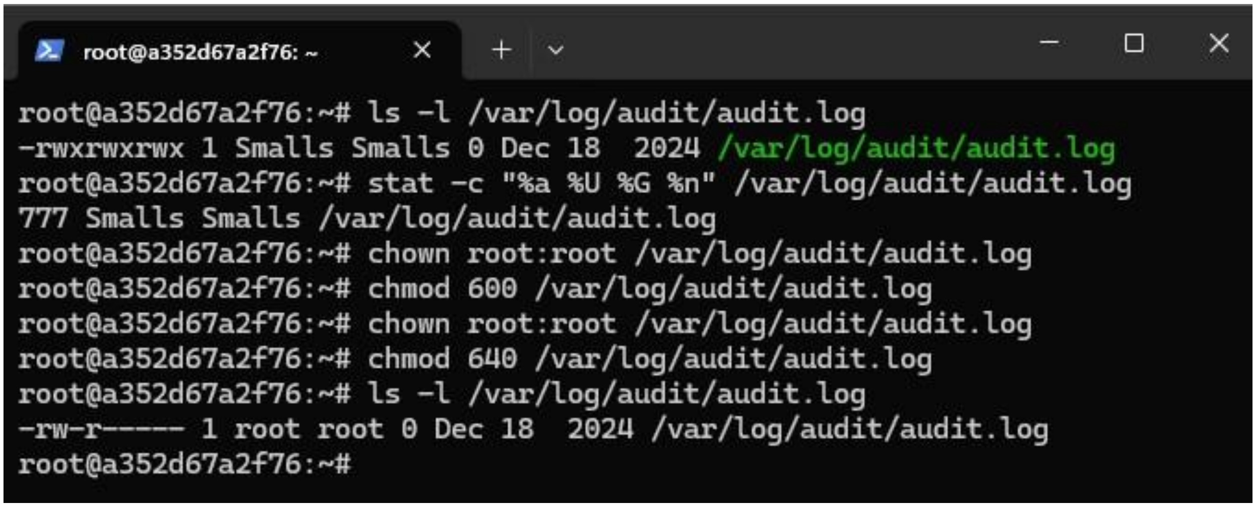
```
root@a352d67a2f76:~# getent passwd Benny AnotherUser
Benny:x:1001:1001::/home/Benny:/bin/sh
AnotherUser:x:1001:1001::/home/AnotherUser:/bin/sh
root@a352d67a2f76:~# awk -F: '$3==1001 {print $1, $3, $6}' /etc/passwd
Benny 1001 /home/Benny
AnotherUser 1001 /home/AnotherUser
root@a352d67a2f76:~# cut -d: -f3 /etc/passwd | sort -n | tail -n 15
39
41
100
101
1001
1001
1002
1003
1004
1005
1006
1007
1008
1009
65534
root@a352d67a2f76:~# getent passwd 1101
root@a352d67a2f76:~# getent group 1101
root@a352d67a2f76:~# groupadd -g 1101 AnotherUser
root@a352d67a2f76:~# getent group AnotherUser
AnotherUser:x:1101:
root@a352d67a2f76:~# usermod -u 1101 -g 1101 AnotherUser
root@a352d67a2f76:~# id AnotherUser
uid=1101(AnotherUser) gid=1101(AnotherUser) groups=1101(AnotherUser)
root@a352d67a2f76:~# id -gn AnotherUser
AnotherUser
root@a352d67a2f76:~# chown -R AnotherUser:AnotherUser /home/AnotherUser
root@a352d67a2f76:~# ls -ld /home/AnotherUser
drwxr-x--- 1 AnotherUser AnotherUser 4096 Dec 18  2024 /home/AnotherUser
root@a352d67a2f76:~#
```

File Permissions

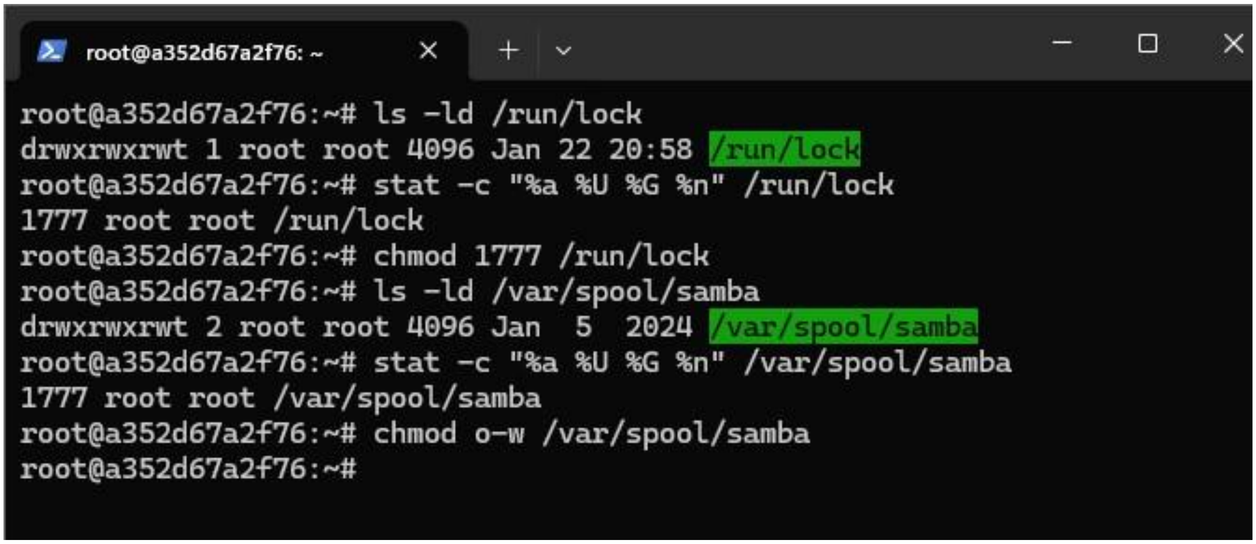


```
root@a352d67a2f76:~# find / -xdev -type d -perm -0002 2>/dev/null | head
 -n 50
/var/tmp
/var/spool/samba
/run/lock
/tmp
root@a352d67a2f76:~# find / -xdev -type f -perm -0002 2>/dev/null | head
 -n 50
/var/log/audit/audit.log
root@a352d67a2f76:~# ls -ld /tmp /var/tmp
drwxrwxrwt 1 root root 4096 Jan 23 09:02 /tmp
drwxrwxrwt 2 root root 4096 Jun 27  2024 /var/tmp
root@a352d67a2f76:~# chmod 1777 /tmp /var/tmp
root@a352d67a2f76:~# ls -l /etc/shadow /etc/gshadow /etc/sudoers
-rw-r----- 1 root shadow  632 Jan 23 08:59 /etc/gshadow
-rw-r----- 1 root shadow 1537 Dec 18  2024 /etc/shadow
-r--r----- 1 root root   1671 Aug  3  2022 /etc/sudoers
root@a352d67a2f76:~# ls -ld /etc/sudoers.d
drwxr-x--- 1 root root 4096 Dec 18  2024 /etc/sudoers.d
root@a352d67a2f76:~#
```

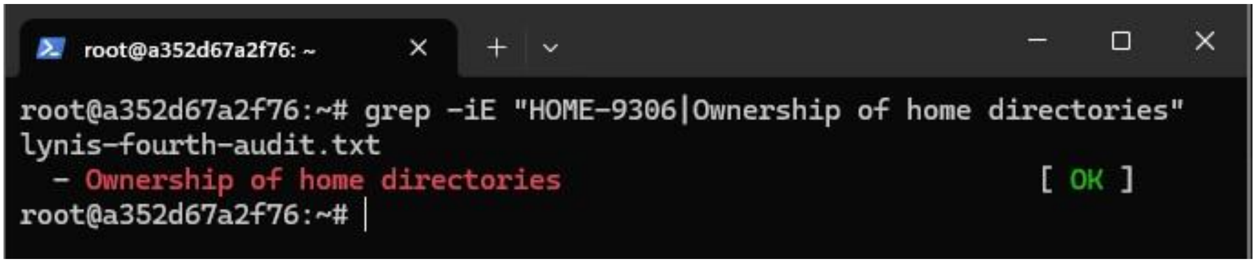
Fix the world-writable file



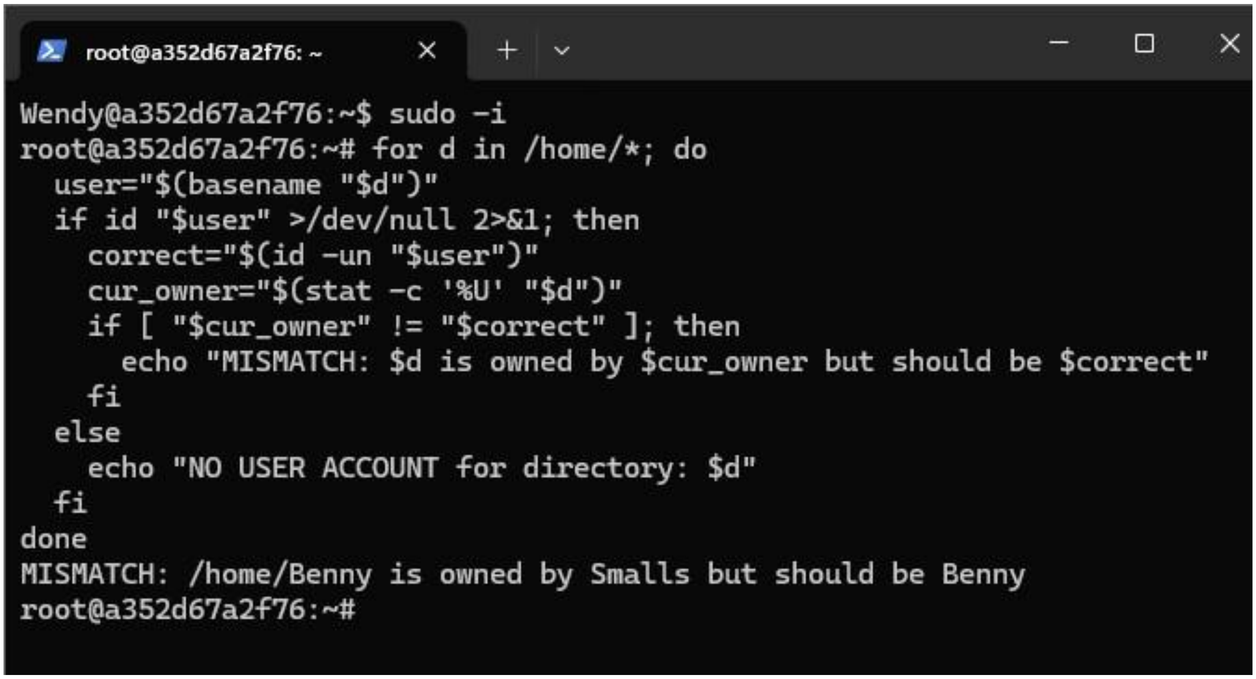
```
root@a352d67a2f76:~# ls -l /var/log/audit/audit.log
-rwxrwxrwx 1 Smalls Smalls 0 Dec 18  2024 /var/log/audit/audit.log
root@a352d67a2f76:~# stat -c "%a %U %G %n" /var/log/audit/audit.log
777 Smalls Smalls /var/log/audit/audit.log
root@a352d67a2f76:~# chown root:root /var/log/audit/audit.log
root@a352d67a2f76:~# chmod 600 /var/log/audit/audit.log
root@a352d67a2f76:~# chown root:root /var/log/audit/audit.log
root@a352d67a2f76:~# chmod 640 /var/log/audit/audit.log
root@a352d67a2f76:~# ls -l /var/log/audit/audit.log
-rw-r----- 1 root root 0 Dec 18  2024 /var/log/audit/audit.log
root@a352d67a2f76:~#
```



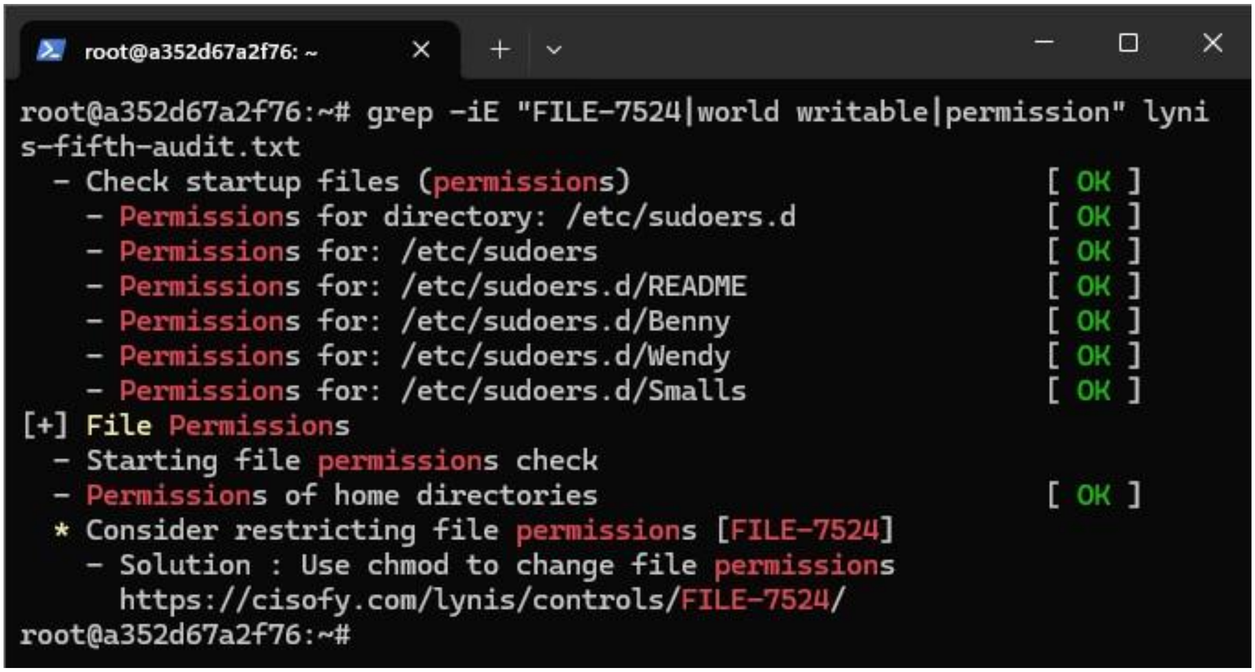
```
root@a352d67a2f76:~# ls -ld /run/lock
drwxrwxrwt 1 root root 4096 Jan 22 20:58 /run/lock
root@a352d67a2f76:~# stat -c "%a %U %G %n" /run/lock
1777 root root /run/lock
root@a352d67a2f76:~# chmod 1777 /run/lock
root@a352d67a2f76:~# ls -ld /var/spool/samba
drwxrwxrwt 2 root root 4096 Jan  5  2024 /var/spool/samba
root@a352d67a2f76:~# stat -c "%a %U %G %n" /var/spool/samba
1777 root root /var/spool/samba
root@a352d67a2f76:~# chmod o-w /var/spool/samba
root@a352d67a2f76:~#
```



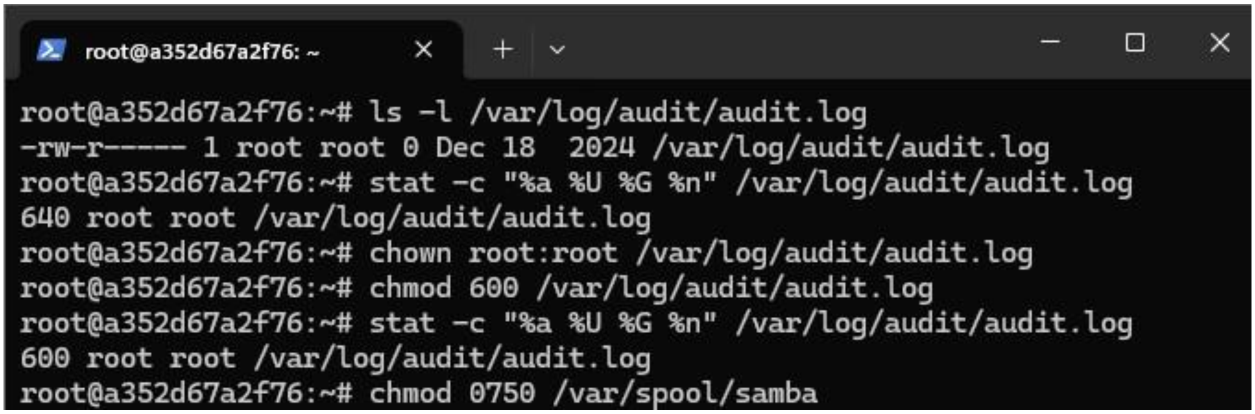
```
root@a352d67a2f76:~# grep -iE "HOME-9306|Ownership of home directories"
lynis-fourth-audit.txt
  - Ownership of home directories                            [ OK ]
root@a352d67a2f76:~# |
```



```
Wendy@a352d67a2f76:~$ sudo -i
root@a352d67a2f76:~# for d in /home/*; do
  user="$(basename "$d")"
  if id "$user" >/dev/null 2>&1; then
    correct="$(id -un "$user")"
    cur_owner="$(stat -c '%U' "$d")"
    if [ "$cur_owner" != "$correct" ]; then
      echo "MISMATCH: $d is owned by $cur_owner but should be $correct"
    fi
  else
    echo "NO USER ACCOUNT for directory: $d"
  fi
done
MISMATCH: /home/Benny is owned by Smalls but should be Benny
root@a352d67a2f76:~#
```



```
root@a352d67a2f76:~# grep -iE "FILE-7524|world writable|permission" lyni
s-fifth-audit.txt
  - Check startup files (permissions)                            [ OK ]
    - Permissions for directory: /etc/sudoers.d                  [ OK ]
    - Permissions for: /etc/sudoers                              [ OK ]
    - Permissions for: /etc/sudoers.d/README                     [ OK ]
    - Permissions for: /etc/sudoers.d/Benny                      [ OK ]
    - Permissions for: /etc/sudoers.d/Wendy                      [ OK ]
    - Permissions for: /etc/sudoers.d/Smalls                     [ OK ]
[+] File Permissions
  - Starting file permissions check
  - Permissions of home directories                              [ OK ]
  * Consider restricting file permissions [FILE-7524]
    - Solution : Use chmod to change file permissions
      https://cisofy.com/lynis/controls/FILE-7524/
root@a352d67a2f76:~#
```



```
root@a352d67a2f76:~# ls -l /var/log/audit/audit.log
-rw-r----- 1 root root 0 Dec 18  2024 /var/log/audit/audit.log
root@a352d67a2f76:~# stat -c "%a %U %G %n" /var/log/audit/audit.log
640 root root /var/log/audit/audit.log
root@a352d67a2f76:~# chown root:root /var/log/audit/audit.log
root@a352d67a2f76:~# chmod 600 /var/log/audit/audit.log
root@a352d67a2f76:~# stat -c "%a %U %G %n" /var/log/audit/audit.log
600 root root /var/log/audit/audit.log
root@a352d67a2f76:~# chmod 0750 /var/spool/samba
```