System Hardening Report

Name: Mitchelle Anduru
Date: 23/01/2026
Role: Junior DevOps Engineer

Executive summary

This hardening assessment identified multiple access-control and authentication weaknesses on the workstation, including unauthorized user accounts, incorrect group membership configuration, excessive sudo privileges, weak password aging controls, accounts without valid passwords, and insecure SSH defaults (root login enabled and password authentication not explicitly disabled). These issues increased the likelihood of unauthorized access, privilege escalation, and remote compromise while reducing accountability for administrative activity. Hardening priorities focused on restoring least-privilege access (removing unauthorized sudo membership and disabling unapproved accounts), enforcing baseline identity policies (correct group membership), strengthening authentication controls (valid passwords and password expiration), and securing remote administration by disabling root SSH logins and enforcing key-based access. After applying the recommended remediations and validating configurations, the workstation's exposure to credential-based attacks and unauthorized privilege use is significantly reduced, and administrative actions are more traceable to individual user accounts.

Key Findings

- Unauthorized account **"Kakamora"** existed and appeared enabled, expanding the attack surface and violating access control policy.
- **"Tala"** had **sudo privileges** despite being a standard user, breaking least privilege and increasing escalation risk.
- Multiple human users had **passwords set to never expire** and/or **no valid password set**, weakening authentication and accountability.
- SSH allowed **direct root login** and did not explicitly disable password authentication, increasing brute-force and credential attack risk.
- The required **"voyagers"** group policy was not enforced (missing mandatory members), weakening RBAC consistency.

Summary of Flags

Instructions: Copy and paste the contents of the flag_location.txt file here:

FLAG 1: Unauthorized user account 'Kakamora' found in /etc/passwd

FLAG 2: Unauthorized user 'Kakamora' has an active group membership, indicating an enabled account

FLAG 3: 'voyagers' group exists but has no members; required users (Moana, Pua, Heihei) are missing

FLAG 4: Unauthorized user 'Tala' is a member of the sudo group and has administrative privileges

FLAG 5: Password expiration policy not enforced for user 'Moana' (password set to never expire)

FLAG 6: Password expiration policy not enforced for user 'Tala' (password set to never expire)

FLAG 7: Password expiration policy not enforced for user 'Pua' (password set to never expire)

FLAG 8: Password expiration policy not enforced for user 'Heihei' (password set to never expire)

FLAG 9: User 'Heihei' has no valid password set in /etc/shadow

FLAG 10: User 'Pua' has no valid password set in /etc/shadow FLAG

11: User 'Tala' has no valid password set in /etc/shadow

FLAG 12: User 'Sina' has no valid password set in /etc/shadow

FLAG 13: Unauthorized user 'Kakamora' has no valid password set

FLAG 14: SSH permits direct root login (PermitRootLogin yes) in /etc/ssh/sshd_config

FLAG 15: SSH password authentication not explicitly disabled (PasswordAuthentication defaults to yes)

Vulnerabilities Identified

Instructions: Describe each vulnerability you identified, along with evidence from the system. Be specific about which configurations or settings did not meet company security policies.

1. **Vulnerability 1:** Unauthorized User Account Present on the System

During user enumeration using `/etc/passwd`, an unauthorized user account named

Kakamora was identified on the system. This user is not listed among the company's authorized administrators or authorized users. Further inspection showed that the account was active and had an associated group membership, indicating that the account was enabled rather than disabled or archived.

Evidence:

- cut -d: -f1 /etc/passwd ● groups Kakamora

The presence of unauthorized user accounts increases the system's attack surface and violates access control policies by allowing unapproved identities to exist on a production workstation.

2. **Vulnerability 2:** Improper Group Configuration for the "voyagers" Group

The company policy mandates that the **voyagers** group must contain exactly three members: Moana, Pua, and Heihei. However, auditing the group configuration showed that the voyagers group existed but had no assigned members.

Evidence:

- getent group voyagers

This misconfiguration prevents proper role-based access control and indicates a failure to enforce organizational group membership policies.

3. Vulnerability 3: Excessive Privileged Access Granted to Unauthorized User

The sudo group was audited to verify that only authorized administrators had privileged access. The user **Tala**, who is classified as an authorized standard user, was found to be a member of the sudo group, granting full administrative privileges.

Evidence:

- getent group sudo

Granting sudo access to non-administrative users violates the principle of least privilege and creates a high risk of accidental or malicious system compromise.

4. Vulnerability 4: Weak Password Aging and Expiration Policies

Password aging policies were reviewed using the chage command for both administrative and standard user accounts. Multiple users, including Moana, Tala, Pua, and Heihei, were found to have passwords configured to never expire, with a maximum password age set to 99999 days.

Evidence:

- chage -l Moana ● chage -l Tala ● chage -l Pua ● chage -l Heihei

The absence of enforced password expiration increases the risk of credential reuse and long-term compromise.

Vulnerability 5: User Accounts Without Valid Passwords

Inspection of /etc/shadow revealed that several human user accounts (Heihei, Pua, Tala, Sina, and Kakamora) did not have valid password hashes configured. While system service accounts correctly had locked passwords, the lack of valid passwords for human users violates the company's requirement that all user accounts be password-protected.

Evidence:

- /etc/shadow inspection using awk

Accounts without valid passwords undermine authentication controls and weaken accountability.

Vulnerability 6: Insecure SSH Configuration Allowing Root Login

The SSH server configuration was audited to assess remote access security. The configuration explicitly allowed direct root login over SSH.

Evidence:

- /etc/ssh/sshd_config showing PermitRootLogin yes

Allowing root login over SSH increases the risk of brute-force attacks and removes individual accountability for administrative actions.

Vulnerability 7: SSH Password Authentication Not Explicitly Disabled

The SSH configuration did not explicitly disable password-based authentication. When the PasswordAuthentication directive is absent, SSH defaults to allowing password authentication.

Evidence:

- Absence of PasswordAuthentication no in /etc/ssh/sshd_config

This configuration exposes the system to password-based attacks instead of enforcing more secure key-based authentication.

Remediation Strategies

Instructions: For each vulnerability identified above, propose a remediation strategy that aligns with the company's security policies. Explain how each recommendation addresses the vulnerability.

1. **Remediation for Vulnerability 1:** [Strategy and rationale]
2. **Remediation for Vulnerability 2:** [Strategy and rationale]
3. *[Continue as needed]*

Remediation for Vulnerability 1: Unauthorized User Accounts

All unauthorized user accounts should be disabled or removed after verification. User audits should be conducted regularly to ensure only approved identities exist on the system.

Remediation for Vulnerability 2: Improper Group Configuration

The voyagers group should be populated strictly with Moana, Pua, and Heihei as specified by company policy. Group membership should be reviewed during onboarding and role changes.

Remediation for Vulnerability 3: Excessive Privileged Access

The user Tala should be removed from the sudo group immediately. Administrative privileges should be limited to Moana, Maui, Tui, and Tamatoa to enforce the principle of least privilege.

Remediation for Vulnerability 4: Weak Password Aging Policies

Password aging policies should be enforced using `chage` to require regular password rotation. A reasonable maximum password age (e.g., 90 days) should be configured for all human users.

Remediation for Vulnerability 5: Accounts Without Valid Passwords

All human user accounts should have valid, strong passwords set in compliance with company standards. Accounts that are no longer required should be disabled or locked.

Remediation for Vulnerability 6: SSH Root Login Enabled

Direct root login over SSH should be disabled by setting `PermitRootLogin no`.

Administrative access should be performed through individual accounts using sudo.

Remediation for Vulnerability 7: SSH Password Authentication

Password-based SSH authentication should be disabled by explicitly setting `PasswordAuthentication no`. Key-based authentication should be enforced for remote access

---

Hardening Process Summary

Instructions: Summarize your approach to hardening the system, from identifying issues to implementing security changes. Discuss the steps you took, the tools you used, and any challenges you encountered.

- **Overview of Hardening Process:** [Summary]

  The hardening process began with establishing a system baseline, followed by systematic auditing of users, groups, authentication policies, and remote access configurations. Each finding was evaluated against company security requirements.

- **Steps Taken:** [List or description of key steps, tools, and methodologies]

  Verified system baseline (OS version, hostname, active user)
  Audited local users and group memberships

  Reviewed sudo privileges and administrative access
  Assessed password aging and authentication settings
  Inspected SSH configuration for insecure defaults
  Logged findings in a structured flag tracking file

- **Challenges and Observations:** [Any issues encountered and how they were addressed]

  Some security weaknesses stemmed from default configurations, such as SSH authentication settings and password aging policies. Distinguishing legitimate system accounts from human user accounts required careful analysis to avoid false positives.

Conclusion

Instructions: Summarize the overall security posture of the workstation after hardening, any remaining vulnerabilities, and additional recommendations for maintaining security.

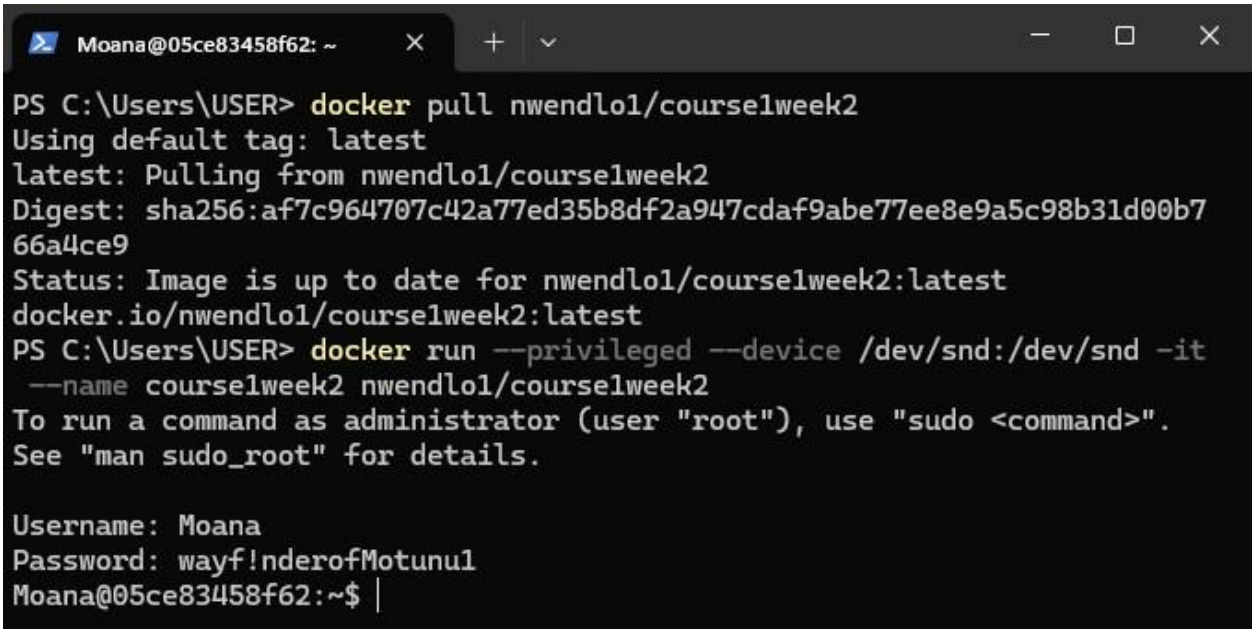
- **Summary of Post-Hardening Security Status:** [Overview]

  The audit identified multiple access control and authentication weaknesses that could expose the system to unauthorized access. While no active exploitation was observed, several configurations violated company security policies and required remediation.

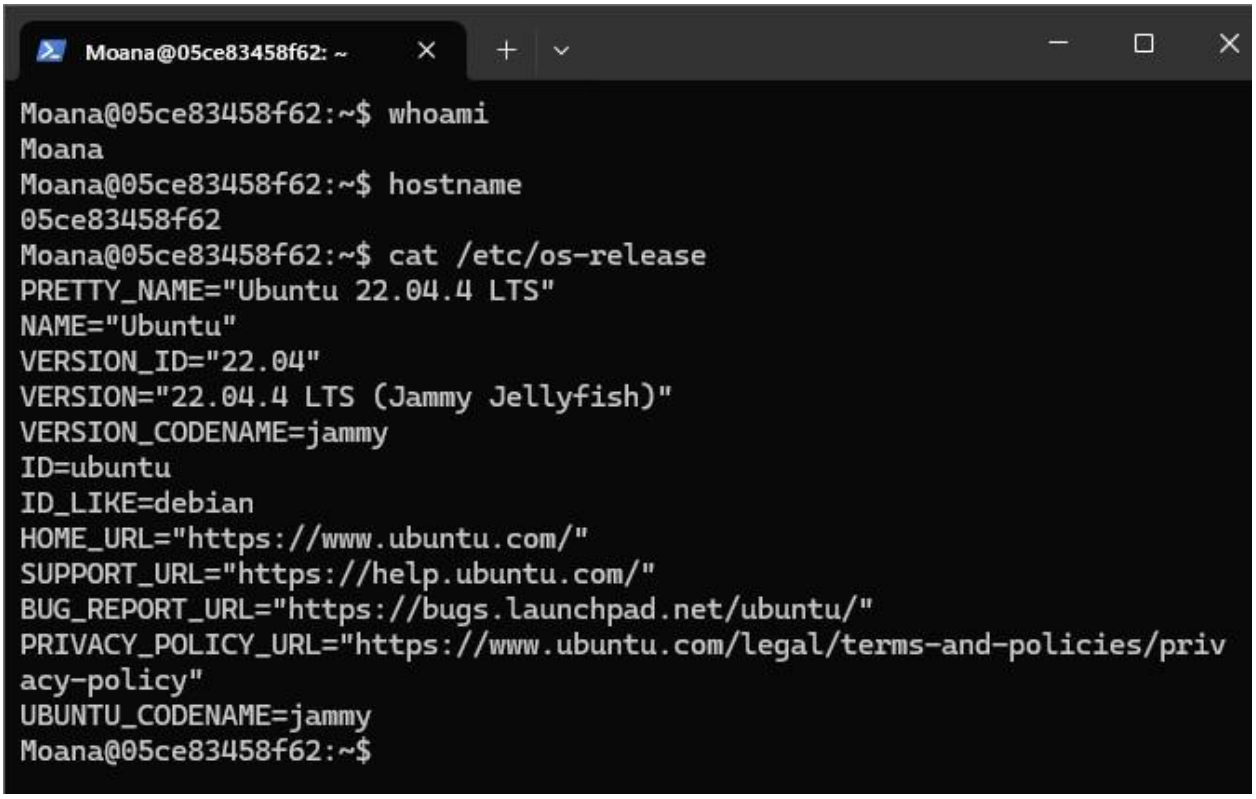
- **Additional Recommendations:** [Suggestions for continued compliance and improvement]

  Regular security audits, automated compliance checks, and centralized identity management tools are recommended to maintain long-term security. Enforcing configuration baselines and periodic reviews will reduce future risk.

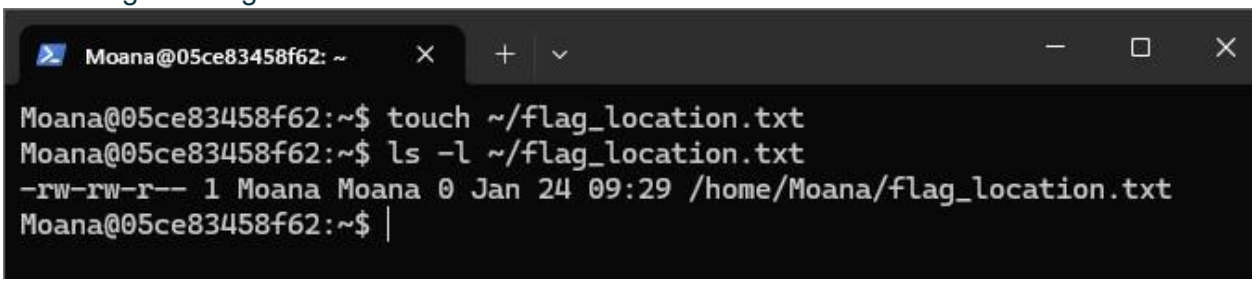
Screenshtots



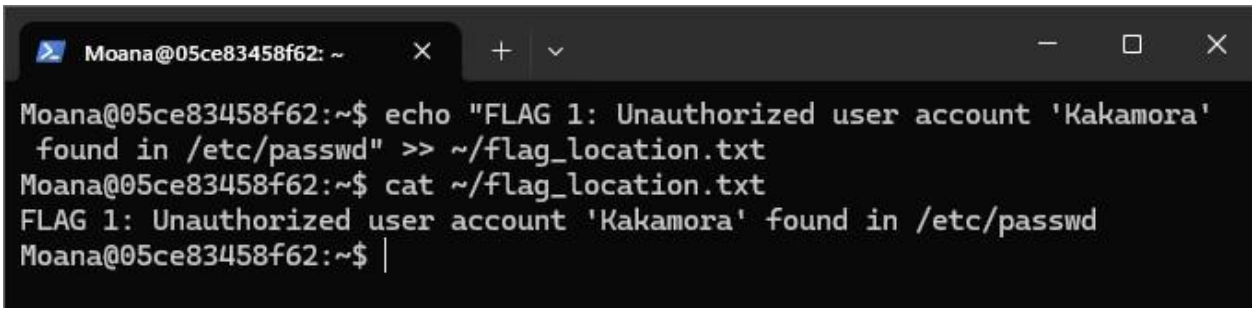
Baseline verification



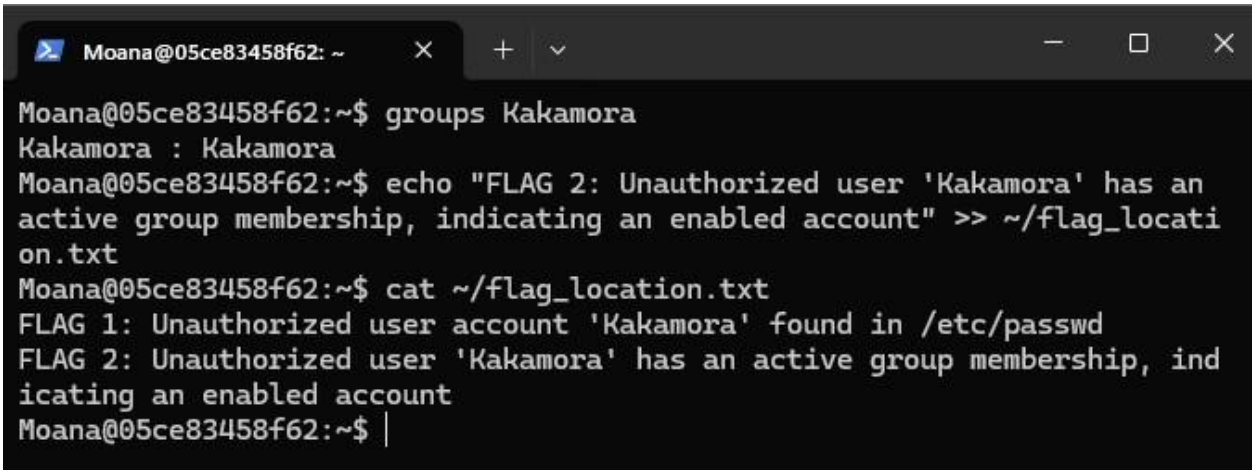
Create Flag Tracking File



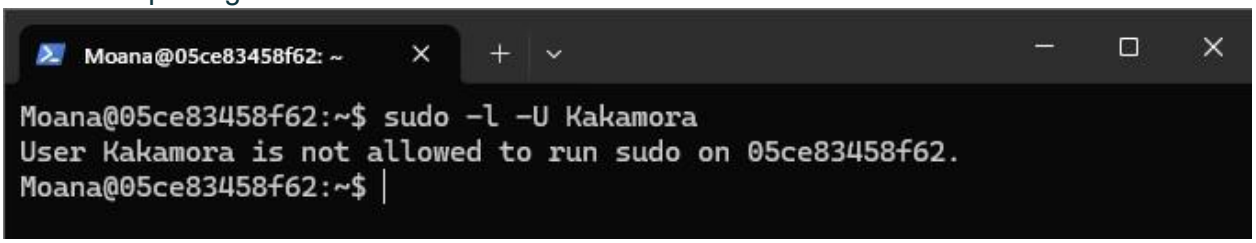
User, Access, and Password Policies



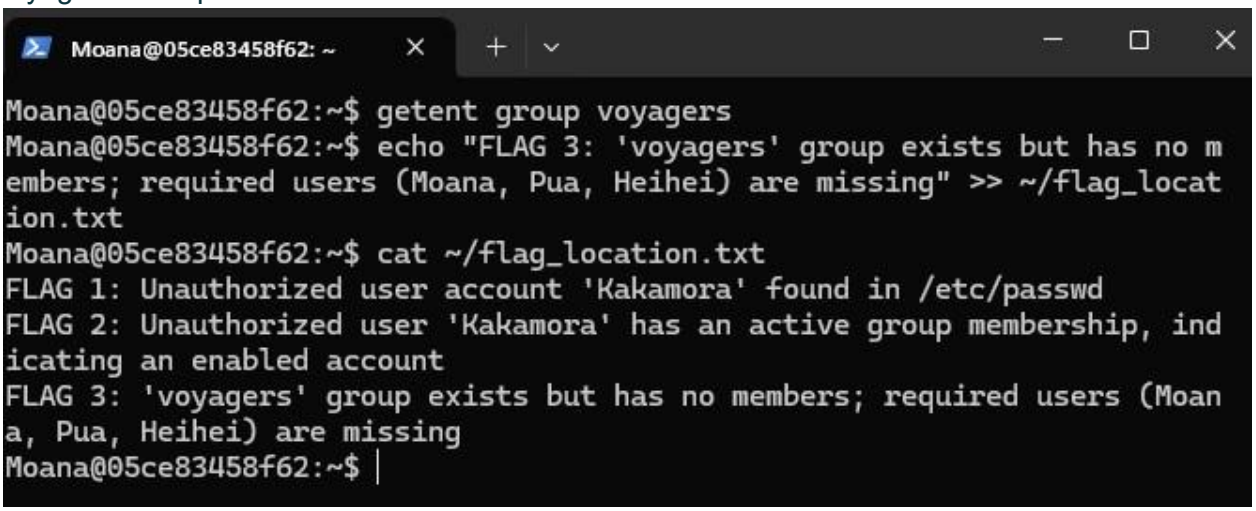
Group Membership Audit



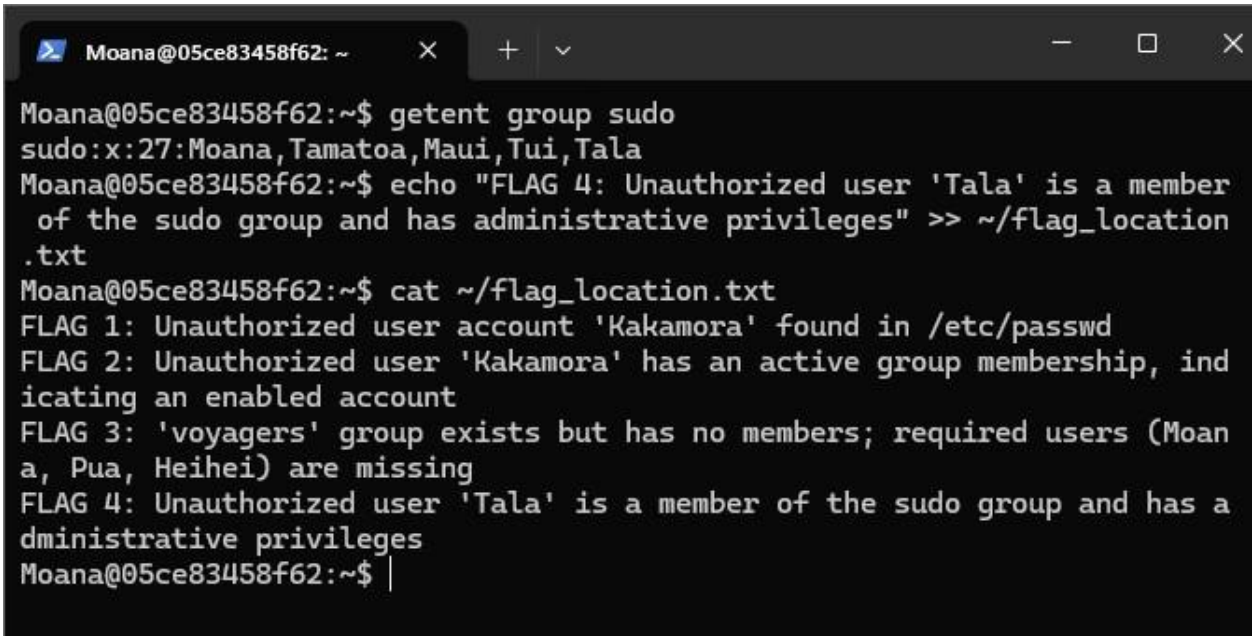
Check sudo privileges



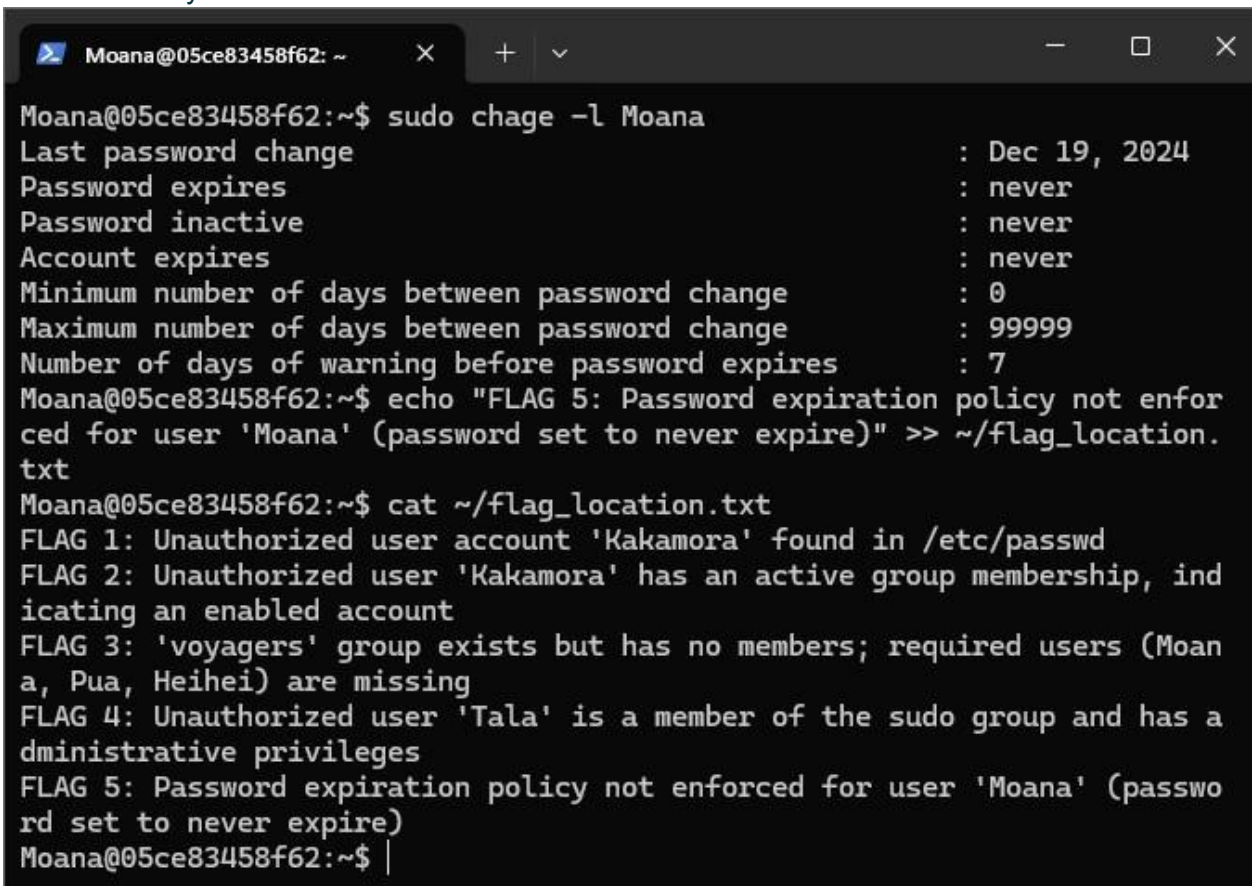
“voyagers” Group



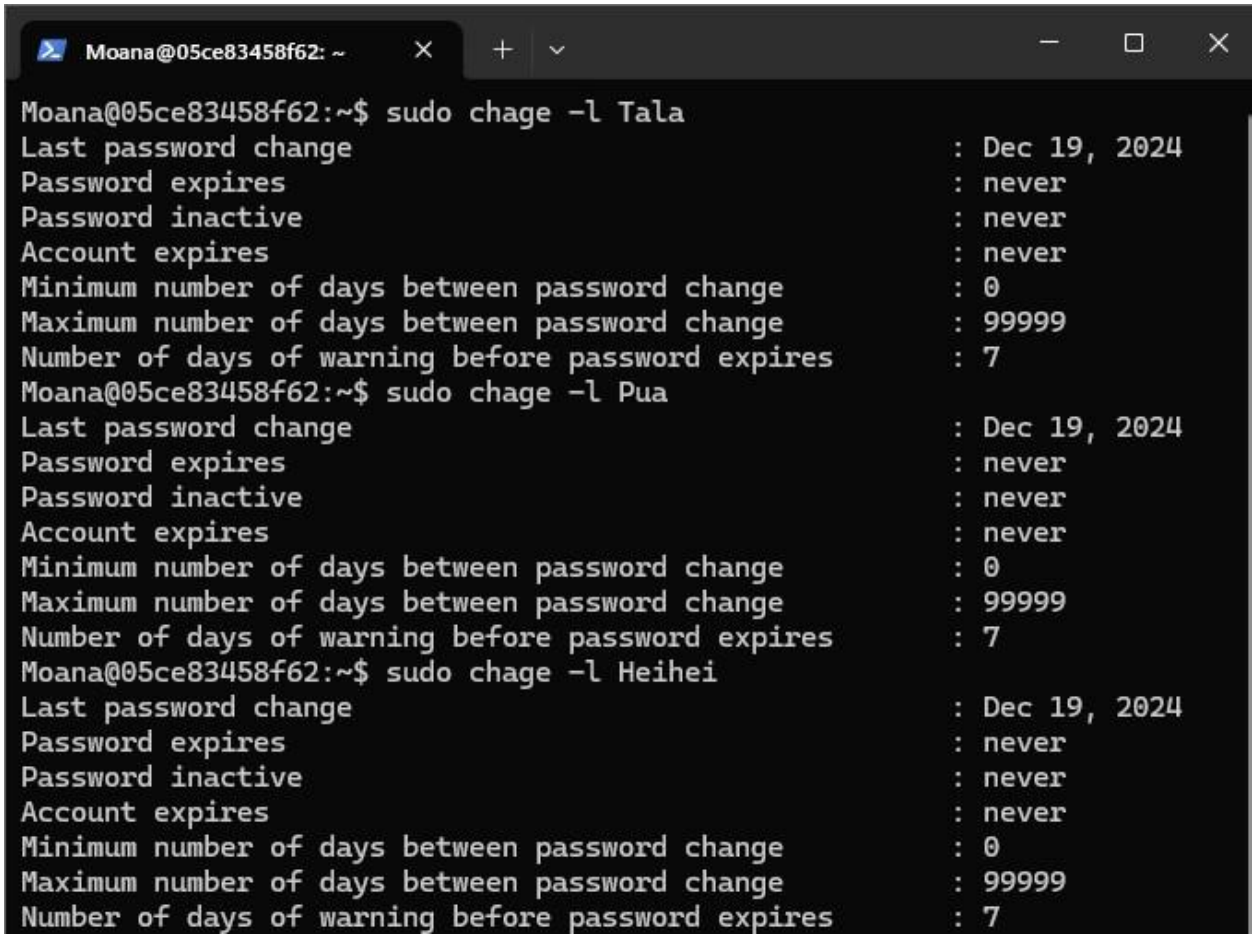
Check who has administrative (sudo) access



Password Policy Audit

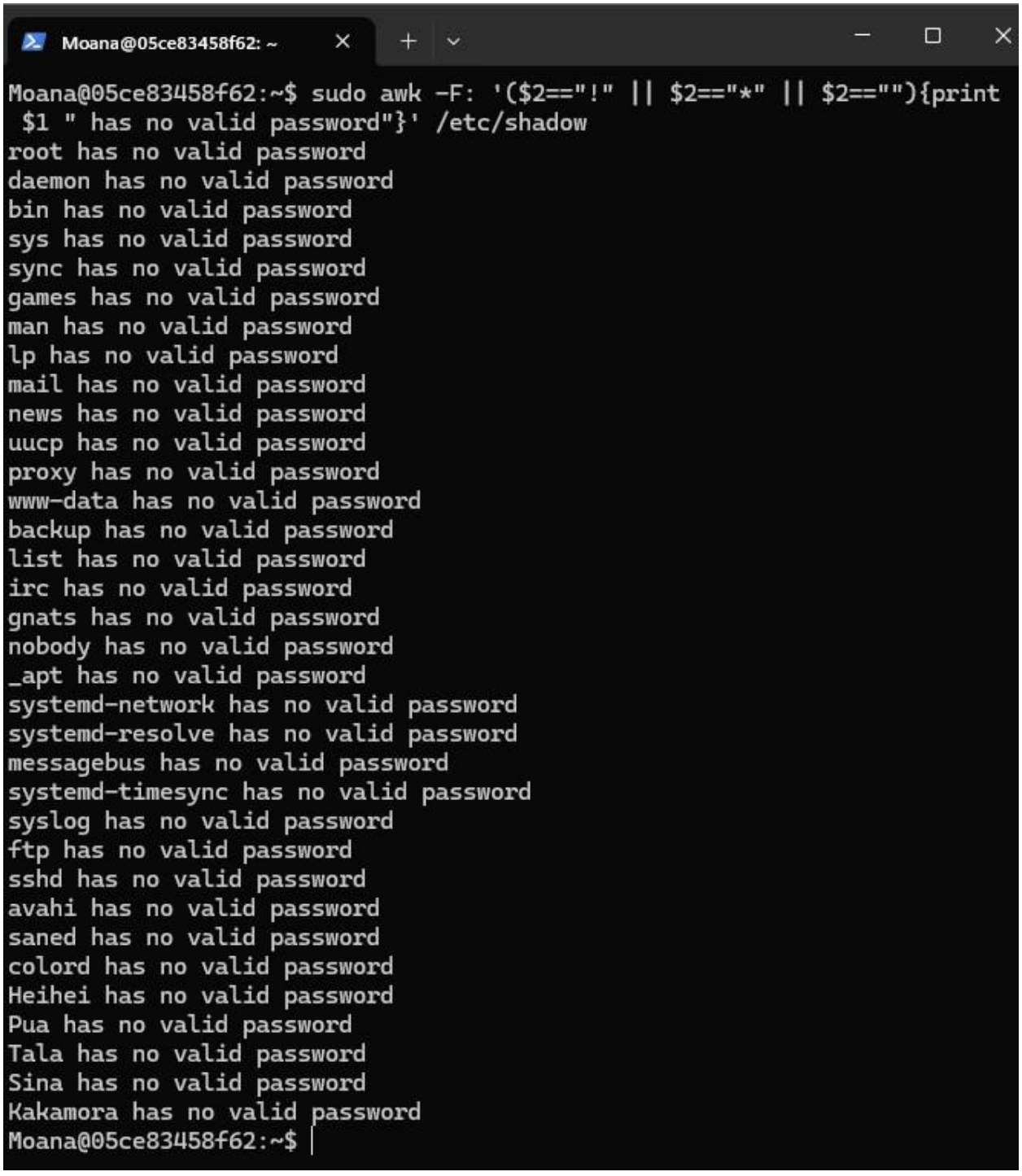


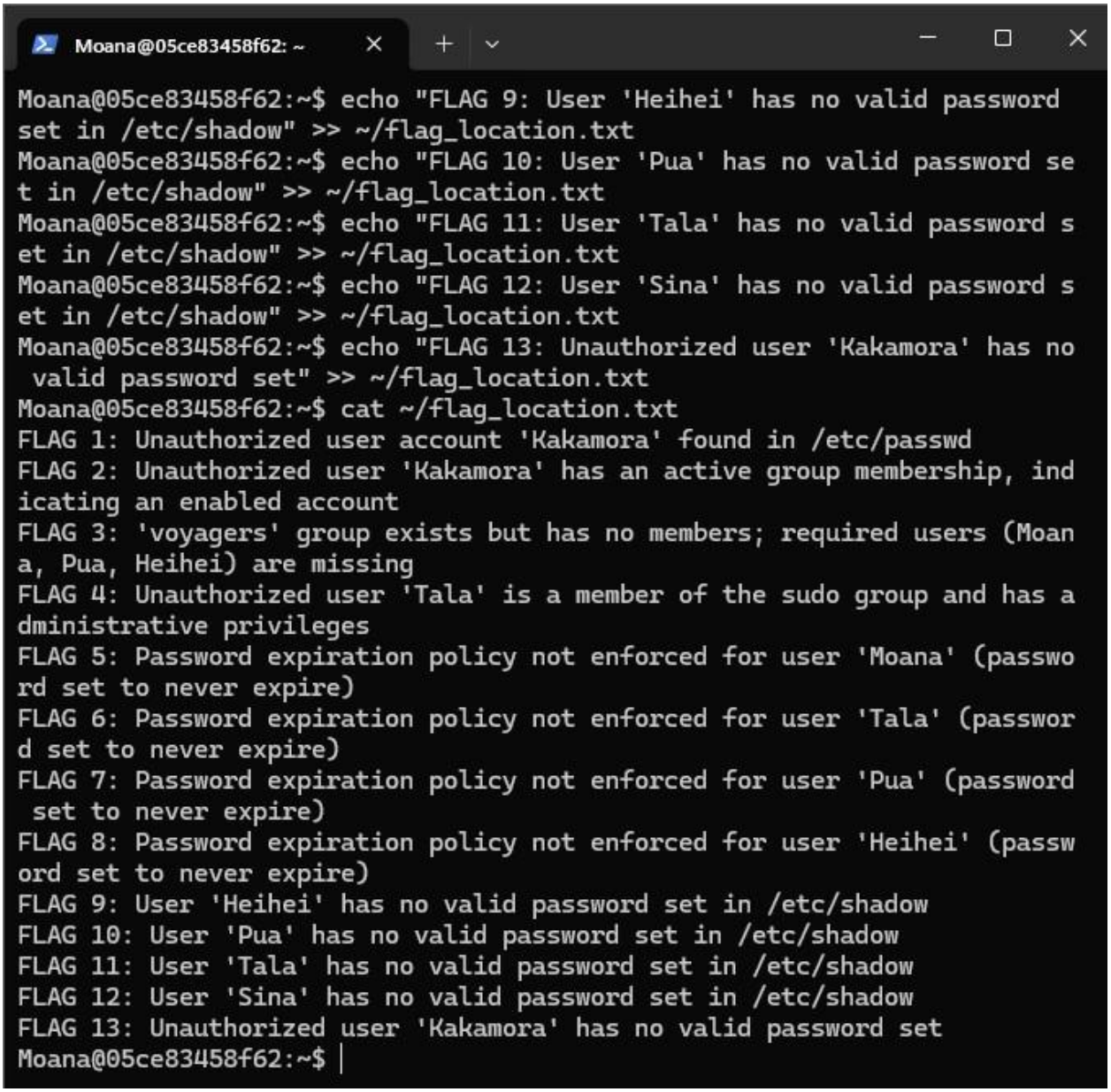
Check password policy for OTHER users


Moana@05ce83458f62: ~
Moana@05ce83458f62:~$ sudo chage -l Tala
Last password change : Dec 19, 2024
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
Moana@05ce83458f62:~$ sudo chage -l Pua
Last password change : Dec 19, 2024
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
Moana@05ce83458f62:~$ sudo chage -l Heihei
Last password change : Dec 19, 2024
Password expires : never
Password inactive : never
Account expires : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7

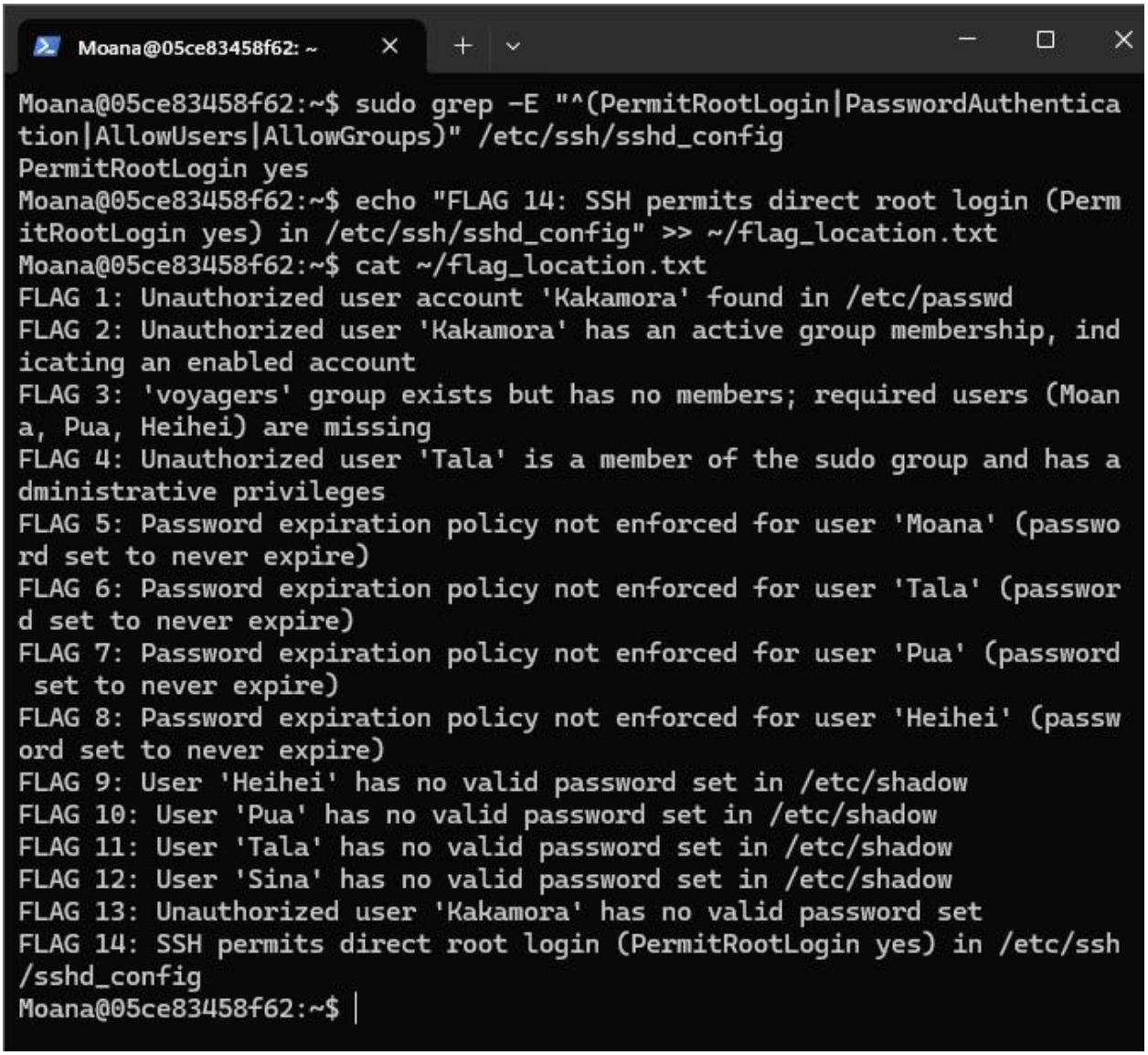
```
Moana@05ce83458f62:~$ echo "FLAG 6: Password expiration policy not enfor
ced for user 'Tala' (password set to never expire)" >> ~/flag_location.t
xt
echo "FLAG 7: Password expiration policy not enforced for user 'Pua' (pa
ssword set to never expire)" >> ~/flag_location.txt
echo "FLAG 8: Password expiration policy not enforced for user 'Heihei'
(password set to never expire)" >> ~/flag_location.txt
Moana@05ce83458f62:~$ cat ~/flag_location.txt
FLAG 1: Unauthorized user account 'Kakamora' found in /etc/passwd
FLAG 2: Unauthorized user 'Kakamora' has an active group membership, ind
icating an enabled account
FLAG 3: 'voyagers' group exists but has no members; required users (Moan
a, Pua, Heihei) are missing
FLAG 4: Unauthorized user 'Tala' is a member of the sudo group and has a
dministrative privileges
FLAG 5: Password expiration policy not enforced for user 'Moana' (passwo
rd set to never expire)
FLAG 6: Password expiration policy not enforced for user 'Tala' (passwor
d set to never expire)
FLAG 7: Password expiration policy not enforced for user 'Pua' (password
 set to never expire)
FLAG 8: Password expiration policy not enforced for user 'Heihei' (passw
ord set to never expire)
Moana@05ce83458f62:~$
```

Check for users with empty or locked passwords

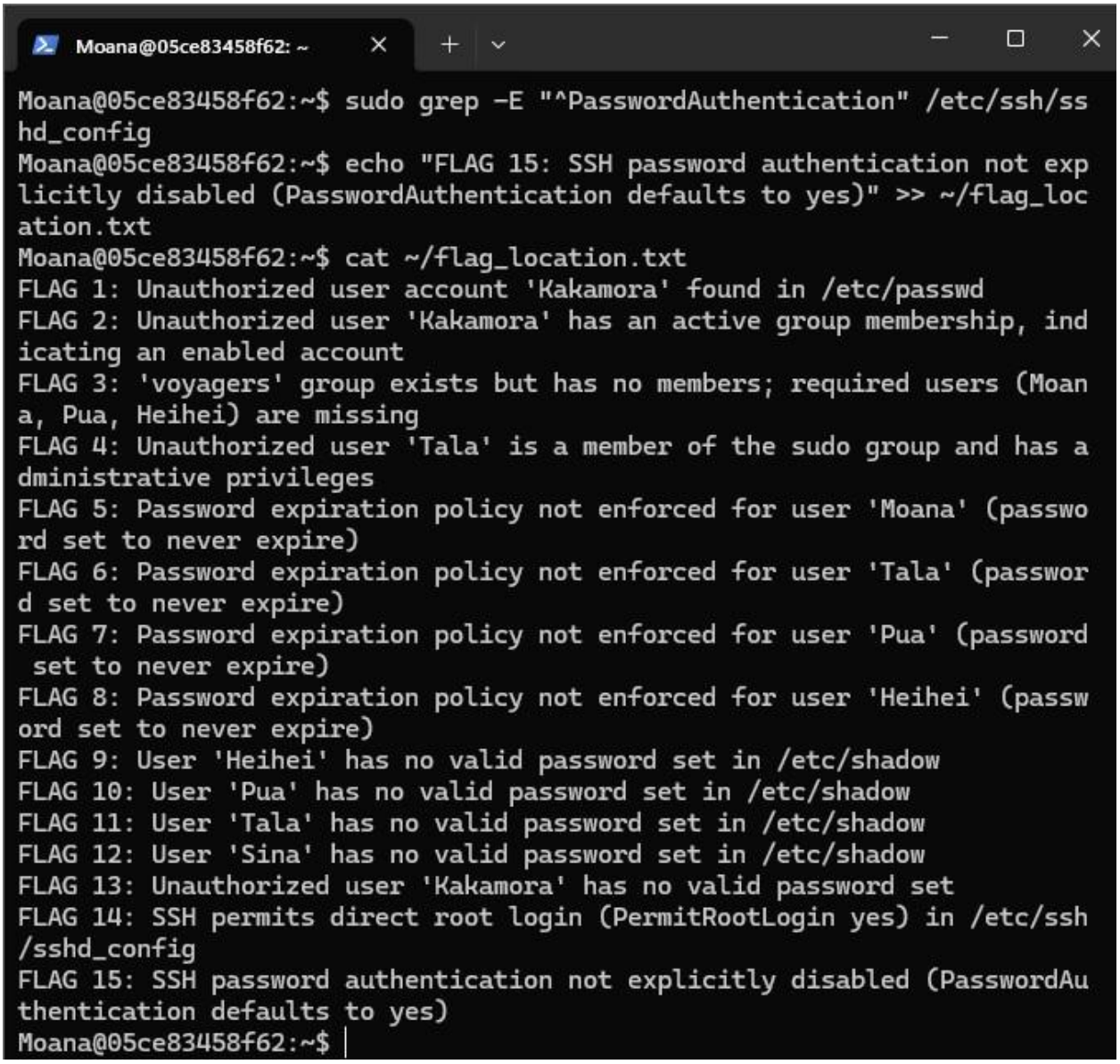

Moana@05ce83458f62: ~
Moana@05ce83458f62:~$ sudo awk -F: '($2=="!" || $2=="*" || $2==""){print
$1 " has no valid password"}' /etc/shadow
root has no valid password
daemon has no valid password
bin has no valid password
sys has no valid password
sync has no valid password
games has no valid password
man has no valid password
lp has no valid password
mail has no valid password
news has no valid password
uucp has no valid password
proxy has no valid password
www-data has no valid password
backup has no valid password
list has no valid password
irc has no valid password
gnats has no valid password
nobody has no valid password
_apt has no valid password
systemd-network has no valid password
systemd-resolve has no valid password
messagebus has no valid password
systemd-timesync has no valid password
syslog has no valid password
ftp has no valid password
sshd has no valid password
avahi has no valid password
saned has no valid password
colord has no valid password
Heihei has no valid password
Pua has no valid password
Tala has no valid password
Sina has no valid password
Kakamora has no valid password
Moana@05ce83458f62:~$



SSH Hardening



Check SSH password authentication


Moana@05ce83458f62: ~
Moana@05ce83458f62:~$ sudo grep -E "^PasswordAuthentication" /etc/ssh/sshd_config
Moana@05ce83458f62:~$ echo "FLAG 15: SSH password authentication not explicitly disabled (PasswordAuthentication defaults to yes)" >> ~/flag_location.txt
Moana@05ce83458f62:~$ cat ~/flag_location.txt
FLAG 1: Unauthorized user account 'Kakamora' found in /etc/passwd
FLAG 2: Unauthorized user 'Kakamora' has an active group membership, indicating an enabled account
FLAG 3: 'voyagers' group exists but has no members; required users (Moana, Pua, Heihei) are missing
FLAG 4: Unauthorized user 'Tala' is a member of the sudo group and has administrative privileges
FLAG 5: Password expiration policy not enforced for user 'Moana' (password set to never expire)
FLAG 6: Password expiration policy not enforced for user 'Tala' (password set to never expire)
FLAG 7: Password expiration policy not enforced for user 'Pua' (password set to never expire)
FLAG 8: Password expiration policy not enforced for user 'Heihei' (password set to never expire)
FLAG 9: User 'Heihei' has no valid password set in /etc/shadow
FLAG 10: User 'Pua' has no valid password set in /etc/shadow
FLAG 11: User 'Tala' has no valid password set in /etc/shadow
FLAG 12: User 'Sina' has no valid password set in /etc/shadow
FLAG 13: Unauthorized user 'Kakamora' has no valid password set
FLAG 14: SSH permits direct root login (PermitRootLogin yes) in /etc/ssh/sshd_config
FLAG 15: SSH password authentication not explicitly disabled (PasswordAuthentication defaults to yes)
Moana@05ce83458f62:~$