Fundamentals of Unix and Linux System Administration Training

Security Principles
Password Policies in Linux

Caroline Gachuhi
System Administrator , KENET
cgachuhi@kenet.or.ke

Learning Objectives

- Understand the concept of Password Policies in Linux
- Identify common aspects of password policies
- Learn how to implement the password policies
- Understand the significance of setting Password policies

What are Password Policies ?

- In Linux, Password Policies are set of rules and configuration that govern the requirements and constraints for user passwords.

- These policies enhance the security of a Linux system by ensuring user passwords are sufficiently strong and less susceptible to unauthorized access.

- **Pluggable Authentication Module** is a system that enforces the policies in most Linux distributions

Common Aspects of Password Policies

a) **Password Length:** Involves setting a minimum password length thus ensuring that passwords are not too short, making them resistant to brute force attacks.

b) **Complexity Rules:** Password policies may require a combination of characters e.g. uppercase & lowercase letters, special case characters and numbers. This makes passwords more resilient against dictionary attacks.

•

c) **Password Expiration:** Passwords can be set to expire after a certain period of time in which users are required to change their passwords. This reduces the risk of compromised passwords

Common Aspects of Password Policies

d) Password History: Password policies can prohibit reuse of certain number of previous passwords which in turn prohibits users from recycling through small set of passwords.

•

e) Account Lockout: This allows an account to be temporarily locked in case of a certain number of failed login attempts. This reduces the risk of brute force attacks.

f) Account Inactivity: This allows the accounts to lock or expire if they have been inactive for a specified duration which protects against dormant/forgotten accounts.

Common Aspects of Password Policies

g) **Password Hashing:** Strong password policies require passwords to be stored as securely hashed values rather than plain text thus enhancing protection against data breaches.

h) **Auditing and Logging:** Enabling password auditing and logging helps administrators to track password-related events, aiding in the detection of suspicious activities and potential breaches.

i) **Two-Factor Authentication:** Enabling 2FA enhances security by requiring users to provide a second

Password Policy Implementation

Password Length

Change directory to /etc/pam.d/

~$ cd /etc/pam.d/

Use ll command to list

$ ll

Backup common-password file using cp command

$ sudo cp common-password common-password.backup

```
user@snf-5609:/etc/pam.d$ sudo cp common-password common-password.backup
user@snf-5609:/etc/pam.d$ ll
total 104
drwxr-xr-x  2 root root 4096 Oct 12 09:42 ./
drwxr-xr-x 96 root root 4096 Oct 12 06:26 ../
-rw-r--r--  1 root root  384 Nov 11  2021 chfn
-rw-r--r--  1 root root   92 Nov 11  2021 chpasswd
-rw-r--r--  1 root root  581 Nov 11  2021 chsh
-rw-r--r--  1 root root 1208 Jun 27 08:56 common-account
-rw-r--r--  1 root root 1242 Jun 27 08:56 common-auth
-rw-r--r--  1 root root 1620 Jun 27 08:56 common-password
-rw-r--r--  1 root root 1620 Oct 12 09:42 common-password.backup
-rw-r--r--  1 root root 1427 Jun 27 08:56 common-session
-rw-r--r--  1 root root 1435 Jun 27 08:56 common-session-noninteractive
-rw-r--r--  1 root root  606 Mar 17  2021 cron
-rw-r--r--  1 root root 4126 Mar 14  2022 login
-rw-r--r--  1 root root   92 Nov 11  2021 newusers
-rw-r--r--  1 root root  520 Aug 12  2020 other
-rw-r--r--  1 root root   92 Nov 11  2021 passwd
-rw-r--r--  1 root root  270 Feb 26  2022 polkit-1
-rw-r--r--  1 root root  143 Feb 20  2022 runuser
-rw-r--r--  1 root root  138 Feb 20  2022 runuser-l
-rw-r--r--  1 root root 2133 Nov 23  2022 sshd
-rw-r--r--  1 root root 2259 Feb 20  2022 su
-rw-r--r--  1 root root  330 Aug  3  2022 sudo
-rw-r--r--  1 root root  315 Aug  3  2022 sudo-i
-rw-r--r--  1 root root  137 Feb 20  2022 su-l
-rw-r--r--  1 root root  119 Sep 19  2022 vmtoolsd
user@snf-5609:/etc/pam.d$
```

Password Policy Implementation

Password Length

Change directory to /etc/pam.d/

~$ cd /etc/pam.d/

Use ll command to list

$ ll

Backup common-password file using cp command

$ sudo cp common-password common-password.backup

Use your favorite editor to edit the common-password file

$ sudo vim common-password

Locate the line starting with success and add **minlen=(number)** at the end of the line.

Save and exit file

```
# here are the per-package modules (the "Primary" block)
password        [success=1 default=ignore]      pam_unix.so obscure yescrypt  minlen=7
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# 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        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

Password Policy Implementation

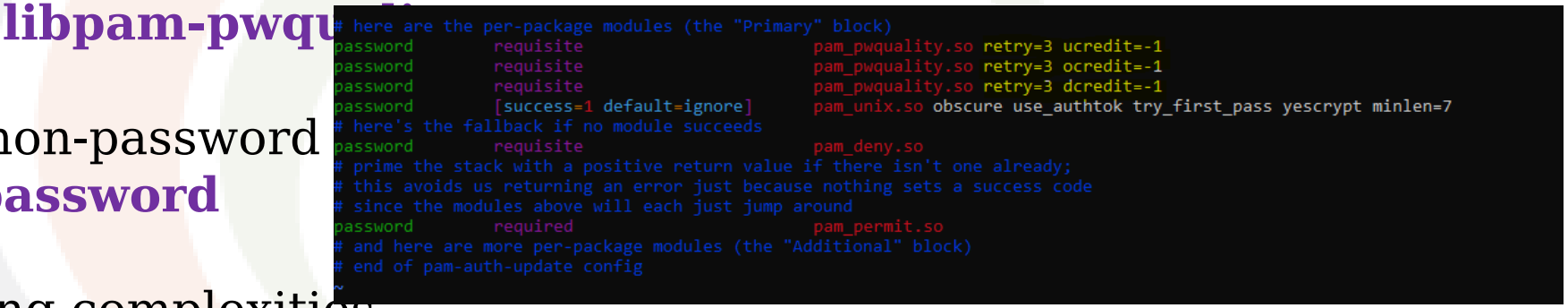
Password Complexity

Install the libpam-pwquality package

$ sudo apt-get install libpam-pwqu

Open and edit the common-password

$ sudo vim common-password



You may add the following complexities

Ucredit=-1 for uppercase

Dcredit=-1 for lowercase

Ocredit=-1 for special character

Save and Exit file

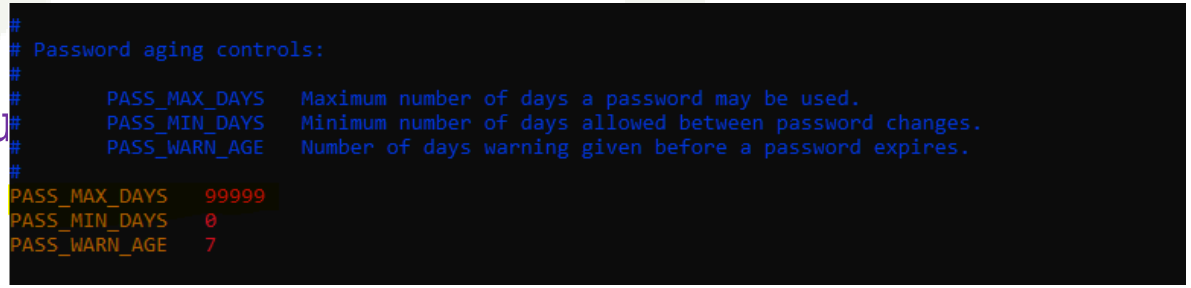
Password Policy Implementation

Password Expiration

$ cd /etc

Create a backup using the cp command

$ sudo cp login.defs login.defs.backu



Edit the login.defs file

$ sudo vim login.defs

Search for the **PASS_MAX_DAYS** and change it to your prefered time/number of days.

Save and exit file.

Verify the set policies

- Users are located in the directory
- **$ cat /etc/passwd**

- Add user
- **$ sudo adduser test**

- Check if the user was added
- **$ cat /etc/passwd**

```
user@snf-5609:/etc$
user@snf-5609:/etc$ sudo adduser test
Adding user `test' ...
Adding new group `test' (1001) ...
Adding new user `test' (1001) with group `test' ...
Creating home directory `/home/test' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password contains less than 1 uppercase letters
Retype new password:
```

```
user@snf-5609:/etc$ sudo adduser test2
Adding user `test2' ...
Adding new group `test2' (1002) ...
Adding new user `test2' (1002) with group `test2' ...
Creating home directory `/home/test2' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
BAD PASSWORD: The password contains less than 1 non-alphanumeric characters
passwd: password updated successfully
Changing the user information for test2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

Verify the set policies

- To check password policies for each user, run the command
- **$ sudo chage -l test**
- To effect changes on exixting users
- Sudo chage –expiredate (date –d +90days +%y-%m-%d)
- **$ sudo chage -d 2024-03-03 test**
- **$ sudo chage -E 12/04/2024 -M 90 -W 7 test**
- To revert the expiry policy for each user
- **$ sudo chage -E -1 test**

```
user@snf-5609:/etc$ sudo chage -E -1 test3
user@snf-5609:/etc$ sudo chage -l test3
Last password change                                    : Dec 12, 2023
Password expires                                        : Mar 11, 2024
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
user@snf-5609:/etc$
```

```
user@snf-5609:/etc$
user@snf-5609:/etc$ sudo chage -l test3
Last password change                                    : Oct 12, 2023
Password expires                                        : Jan 10, 2024
Password inactive                                       : never
Account expires                                         : never
Minimum number of days between password change          : 0
Maximum number of days between password change          : 90
Number of days of warning before password expires       : 7
user@snf-5609:/etc$
```

Other Useful Commands

```
Usage: chage [options] LOGIN

Options:
  -d, --lastday LAST_DAY        set date of last password change to LAST_DAY
  -E, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -h, --help                    display this help message and exit
  -i, --iso8601                 use YYYY-MM-DD when printing dates
  -I, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -l, --list                    show account aging information
  -m, --mindays MIN_DAYS        set minimum number of days before password
                                change to MIN_DAYS
  -M, --maxdays MAX_DAYS        set maximum number of days before password
                                change to MAX_DAYS
  -R, --root CHROOT_DIR         directory to chroot into
  -W, --warndays WARN_DAYS      set expiration warning days to WARN_DAYS
```

Significance of Password Policies

What is the importance of Implementing Password Policies?

Significance of Password Policies

- Longer Passwords are harder to guess or crack
- Complex passwords are less predictable and harder to crack
- Frequent password changes limit the window of opportunity for attackers who may have gained access to a User's password
- Prevents users from repeatedly using same passwords thus improving overall security
- Reduces risk of attackers gaining unauthorized access through multiple incorrect login attempts
- Reduces the attack surface by disabling unused accounts
- Passwords stored as hashes are more secure and even if the system is compromised, the passwords remain hidden.
- Allows for monitoring and incident response when security event occurs.

kenet
Kenya Education Network

Thank You!

Transforming education through ICT

kenet
Kenya Education Network

THANK YOU!

www.kenet.or.ke

Support@kenet.or.ke

Jomo Kenyatta Memorial Library, University of Nairobi
P. O Box 30244-00100
Nairobi.

Transforming learning, research and working environments with ICT