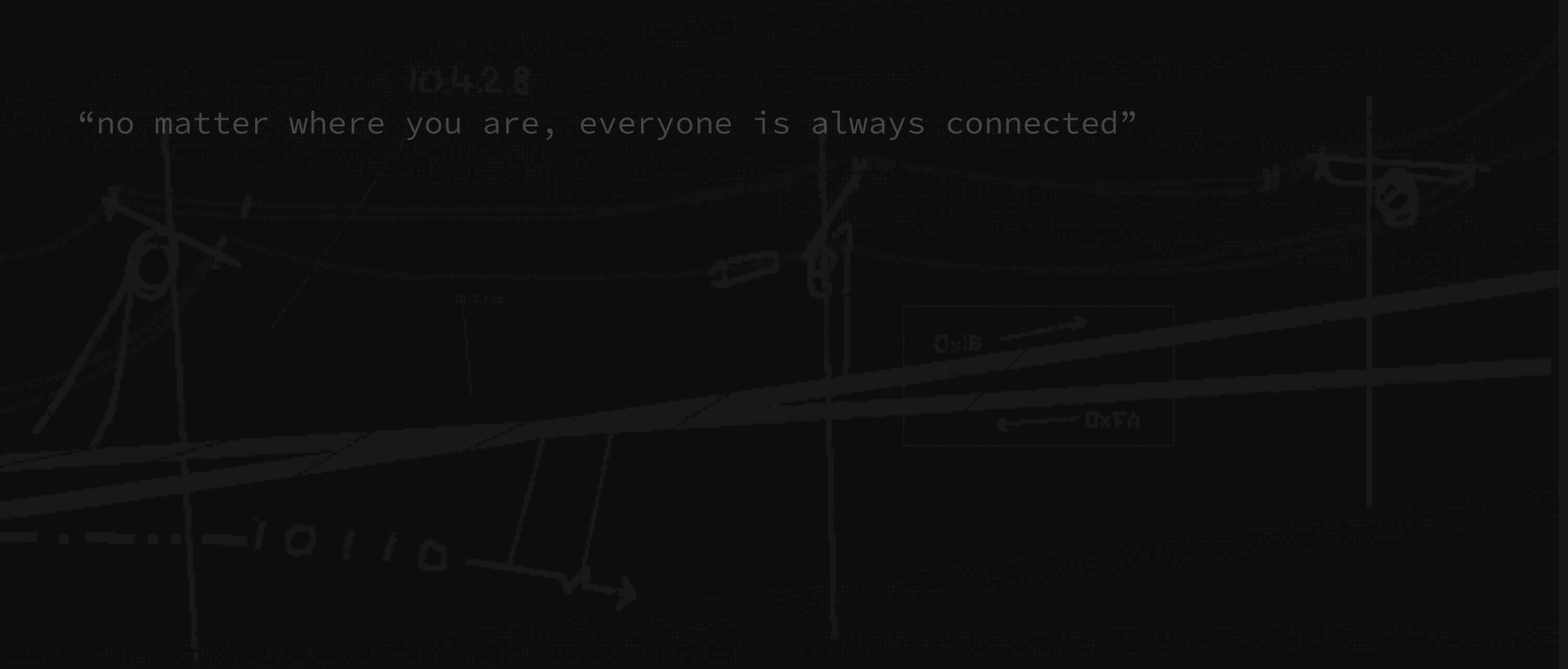

“no matter where you are, everyone is always connected”

05

Passwords and Privilege

Review

- How do I add and remove a user?
- How do I change a user's groups?
- How do I change a user's password?
- Which three files contain important user information?

Secure Passwords

What makes a secure password?

- common vs. uncommon
- length
- complexity
- content
- password history

How can we enforce password requirements on our system?

PAM

Pluggable Authentication Modules

- Separates authentication from applications
- Provides modularity to authentication
- This is how we can enforce different password requirements

Install PAM Libraries

in terminal

```
# sudo apt install libpam-pwquality
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
libpam-pwquality is already the newest
libpam-pwquality set to manually insta
0 upgraded, 0 newly installed, 0 to re
```

Check to see if the *libpam-pwquality* library is installed by running this command and install it if it is not.

apt is a package manager which allows us to install and remove certain software on our system. We will cover this in more detail soon.

Using PAM for Passwords

in file */etc/security/pwquality.conf*

```
difok = 5
minlen = 12
dcredit = -1
lcredit = -1
ucredit = -1
ocredit = -1
retry = 3
enforcing = 1
minclass = 1
```

With *pwquality* installed, we can now configure our password requirements.

We can include the following options to require a minimum length, certain characters, etc.

Using PAM for Passwords

in file */etc/pam.d/common-password*

```
# here are the per-package modules (the “Primary block)
password  requisite                     pam_pwquality.so retry=3
password  [success=2 default=ignore] pam_unix.so obscure use_aut
password  sufficient                    pam_sss.so use_authok
# here’s the fallback if no module succeeds
.
.
.
```

Now we need to make sure that PAM is using this configuration.

Enter this file and check to see if the following lines are there and add them if they are not.

Using PAM for Passwords

in file */etc/pam.d/common-password*

```
# here are the per-package modules (the “Primary block)
password  requisite                     pam_pwquality.so retry=3
password  [success=2 default=ignore] pam_unix.so obscure use_aut
password  sufficient                    pam_sss.so use_authok
# here’s the fallback if no module succeeds
.
.
.
```

Note that this line (pam_unix.so) should not include the words *nullok*. If the words *nullok* appear in this file, remove it.

Sudoers

The *sudo* command is useful, but we don't want everyone to have their hands on it.

To control who has access to the sacred *sudo* permissions, we can edit the /etc/sudoers file.

To Vie with Visudo

in terminal

```
# sudo visudo
```

We must be careful when editing */etc/sudoers* - a misconfigured *sudoers* file can remove all your power!

To safely edit this file, we can use *visudo*. As opposed to *nano*, this checks for errors in the *sudoers* file before saving.

Sudoer Configuration

in file */etc/sudoers*

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain
%admin ALL=(ALL) ALL

# Allow members of group sudo to execu
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information
@includedir /etc/sudoers.d
```

The following directives dictate that the following has access to sudo:

- The root user
- The *admin* group
- The *sudo* group

No other lines should be present on a typical setup.

Sudoer Configuration

in file */etc/sudoers*

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain
%admin ALL=(ALL) ALL

# Allow members of group sudo to execu
%sudo   ALL=(ALL:ALL) NOPASSWD: ALL

# See sudoers(5) for more information
@includedir /etc/sudoers.d
```

The highlighted *NOPASSWD*, when included, means that members of the sudo group do not need passwords for sudo commands.

If present, this should be removed.

Sudoer Configuration

in file */etc/sudoers*

```
# User privilege specification
creep   ALL=(ALL:ALL) ALL
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain
%admin ALL=(ALL) ALL

# Allow members of group sudo to execu
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information
@includedir /etc/sudoers.d
```

The highlighted line means that the user *creep* has access to sudo permissions!

In almost all circumstances, a line like this should not be present and should be removed.

Recap

Today we learned…
- How to enforce password policy with PAM and *pwquality*
- How to restrict *sudo* usage to administrators only

Key commands
apt install libpam-pwquality
visudo

Key files
/etc/pam.d/common-password
/etc/security/pwquality.conf
/etc/sudoers

Bonus Information

in terminal

```
# sudo vipw
# sudo vipw -s
# sudo vigr
```

visudo has equivalent commands for the /etc/password, /etc/shadow, and /etc/group.

You can use these commands to safely edit these files.