Access Controls

Cybersecurity
Linux 1 Day 2

Today’s Objectives

By the end of class, you will be able to:

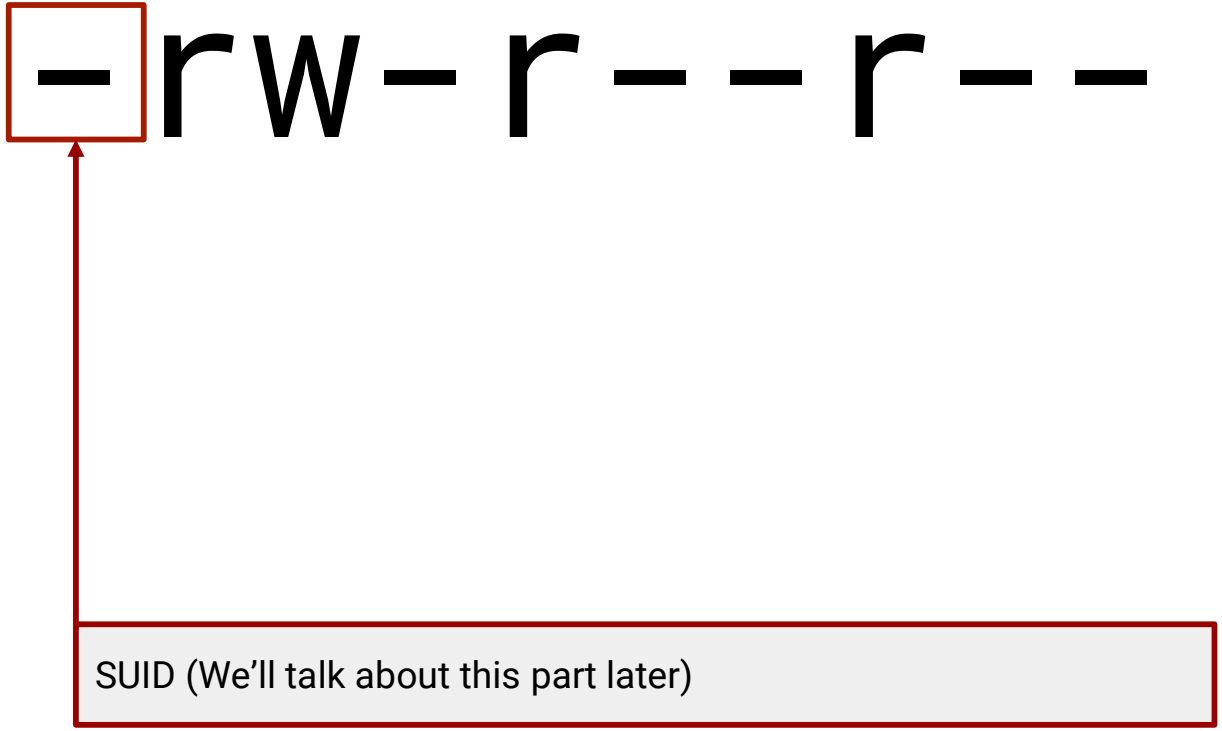
- ☐ Inspecting and setting file permissions.
- ☐ Create and manage users and groups.
- ☐ Elevate privileges with sudo and su

Like Google Docs,
Linux has access controls,
granting permission to access
documents and files on a host.

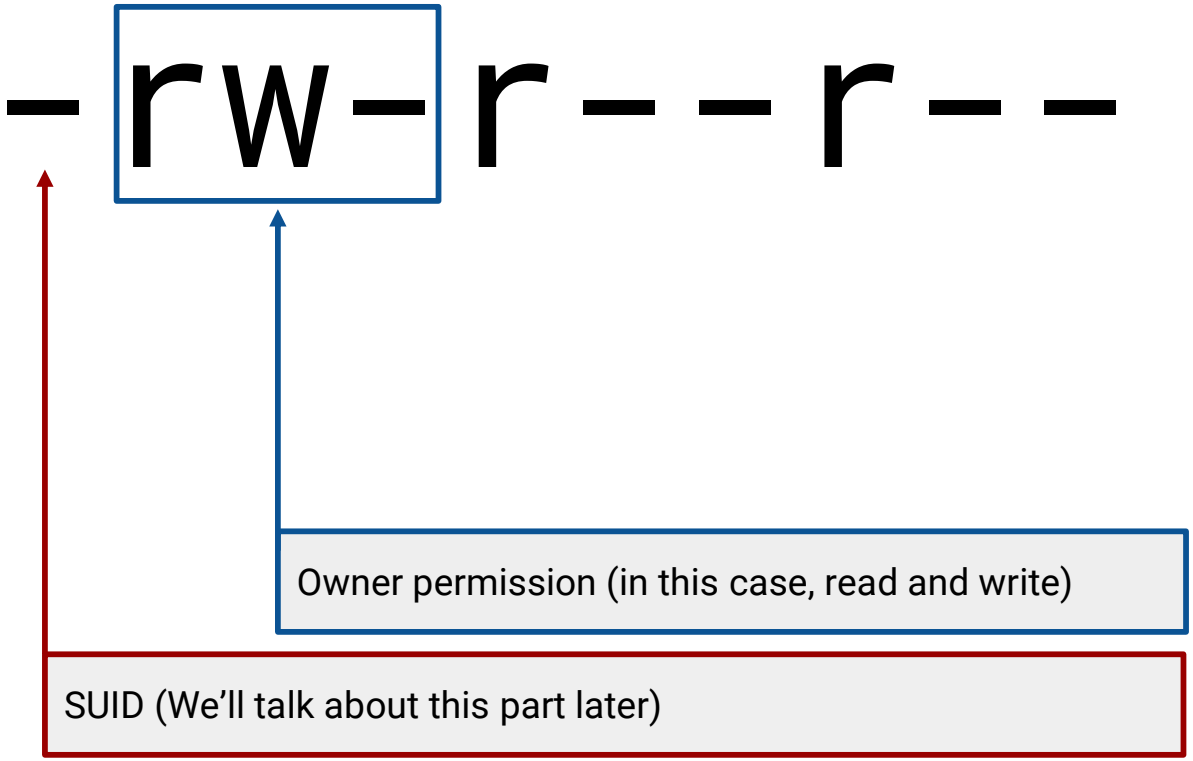
Inspecting File Permissions

```
-rw-r--r--
```

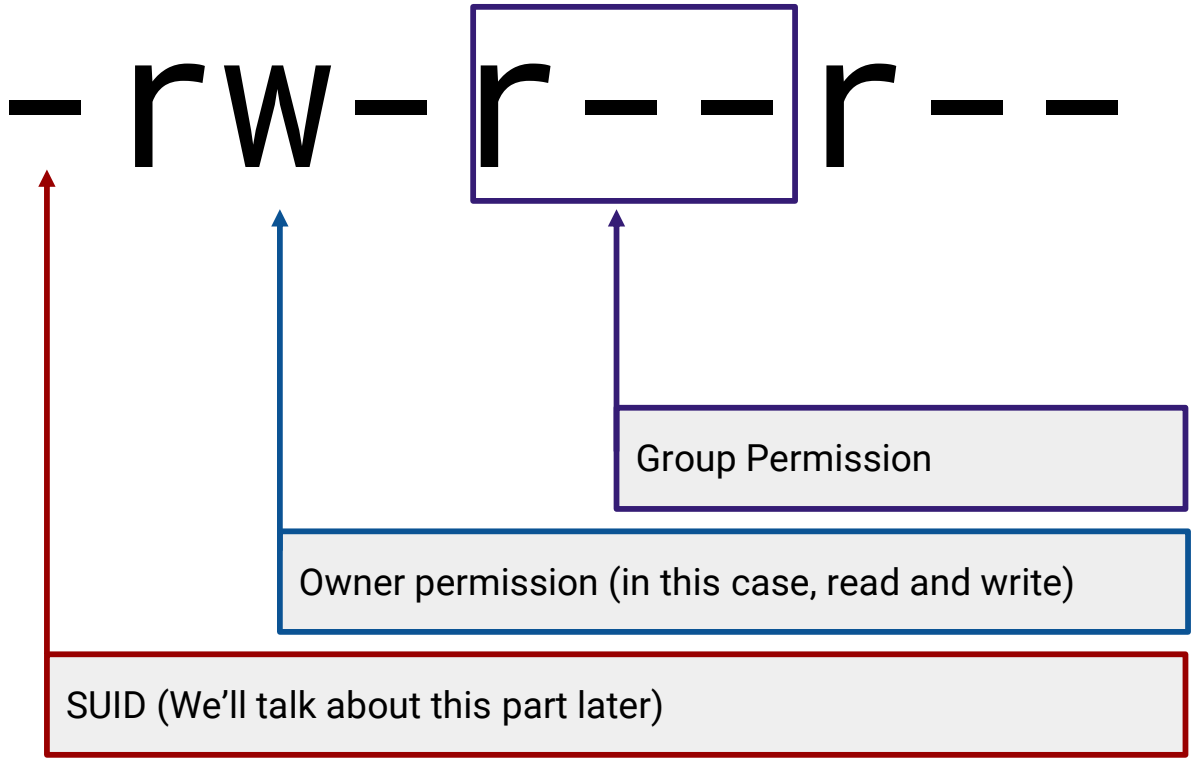
Inspecting File Permissions



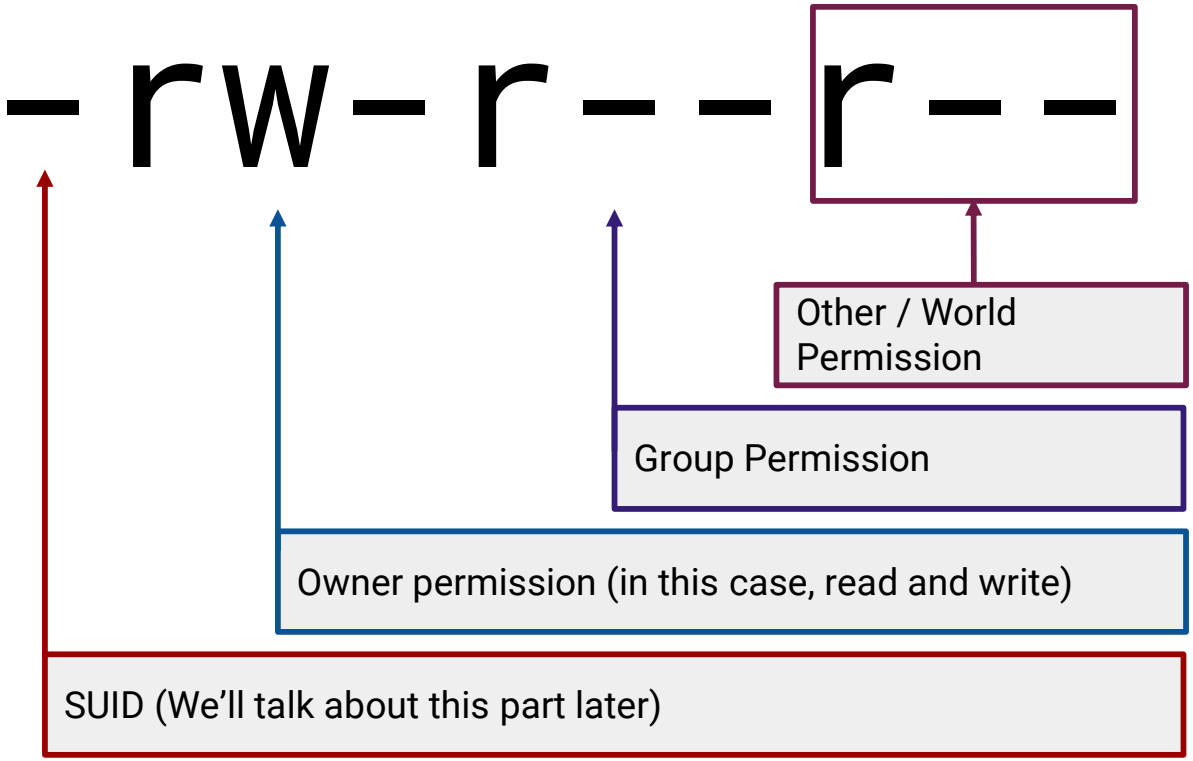
Inspecting File Permissions



Inspecting File Permissions



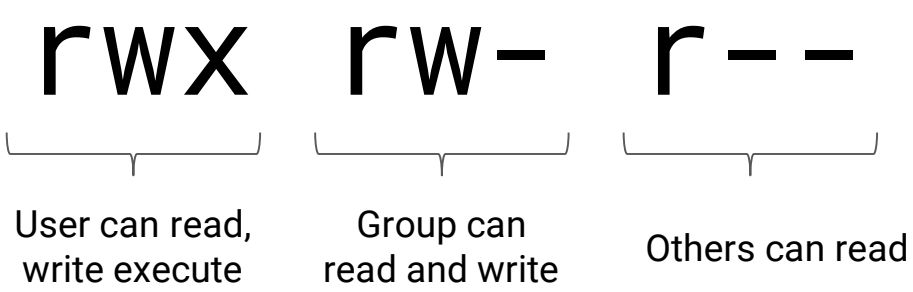
Inspecting File Permissions



Changing File Permissions

File permissions can be set using two different notations: Symbolic and Octal

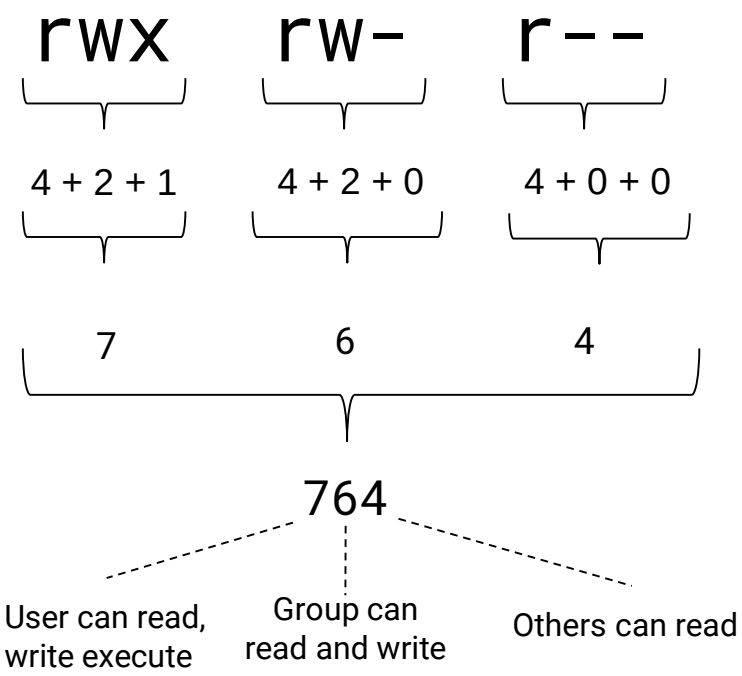
Symbolic Notation	
r	read
w	write
x	execute



Changing File Permissions

File permissions can be set using two different notations: Symbolic and Octal

Octal Notation				
	4	2	1	
0	-	-	-	No permission
1	-	-	x	Only execute
2	-	w	-	Only write
3	-	w	x	Write and execute
4	r	-	-	Only read
5	r	-	x	Read and execute
6	r	w	-	Read and write
7	r	w	x	Read, write and execute



Activity: File Permissions

In this activity, you will practice inspecting and setting file permissions.

Instructions sent via Slack.

Suggested Time:
15 Minutes

Your Turn: File Permissions

Instructions

1. Inspect the permissions on the following files and directories:
   - `/etc/shadow`, `/etc/passwd`, `~/.bashrc`, the directories in `/home`

   - Make sure to record the file permissions for these files

2. Next, create two new directories in `~/Documents`, called `GroupFAQs` and `PrivateData`

3. In `GroupFAQs`, create three new files. Use any names you'd like

   - Grant "group" read access (but not write or execute), and restrict "other" access to these files

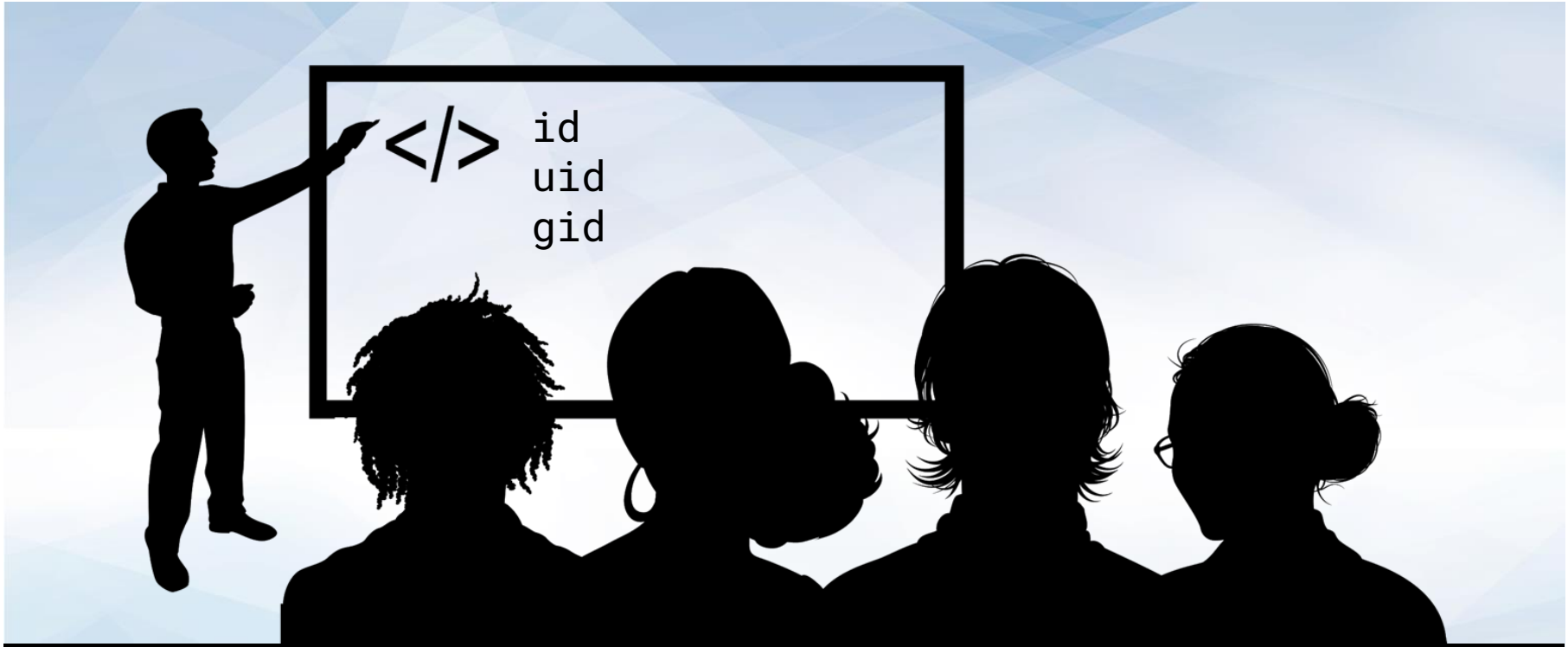
4. Change back to `~/Documents`. Update the permissions for files in `GroupFAQs` such that they have "group" read *and* write access.

Times Up! Let’s Review.

File Permissions

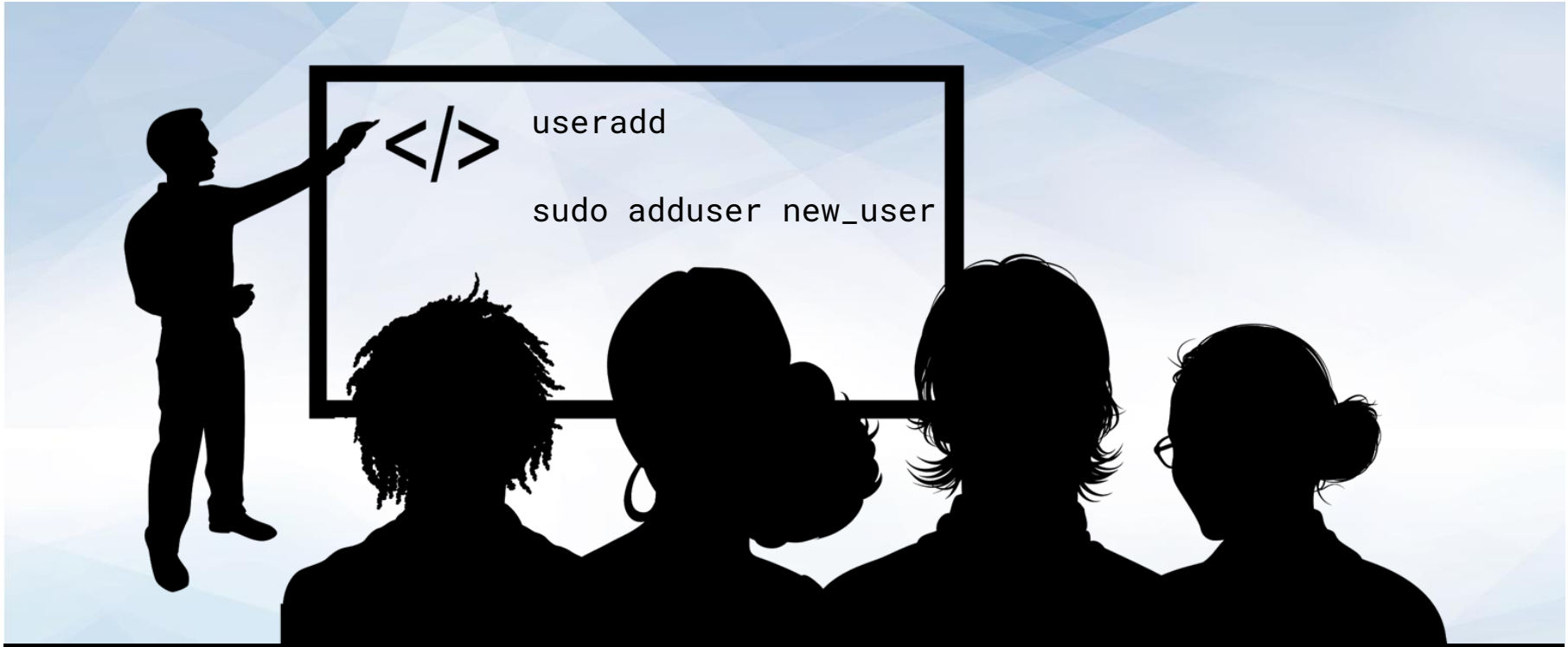
Users and Groups

Groups allow multiple related users to share file permissions.



Instructor Demonstration

Determining Group Membership



Instructor Demonstration

Adding Users

Adding Users

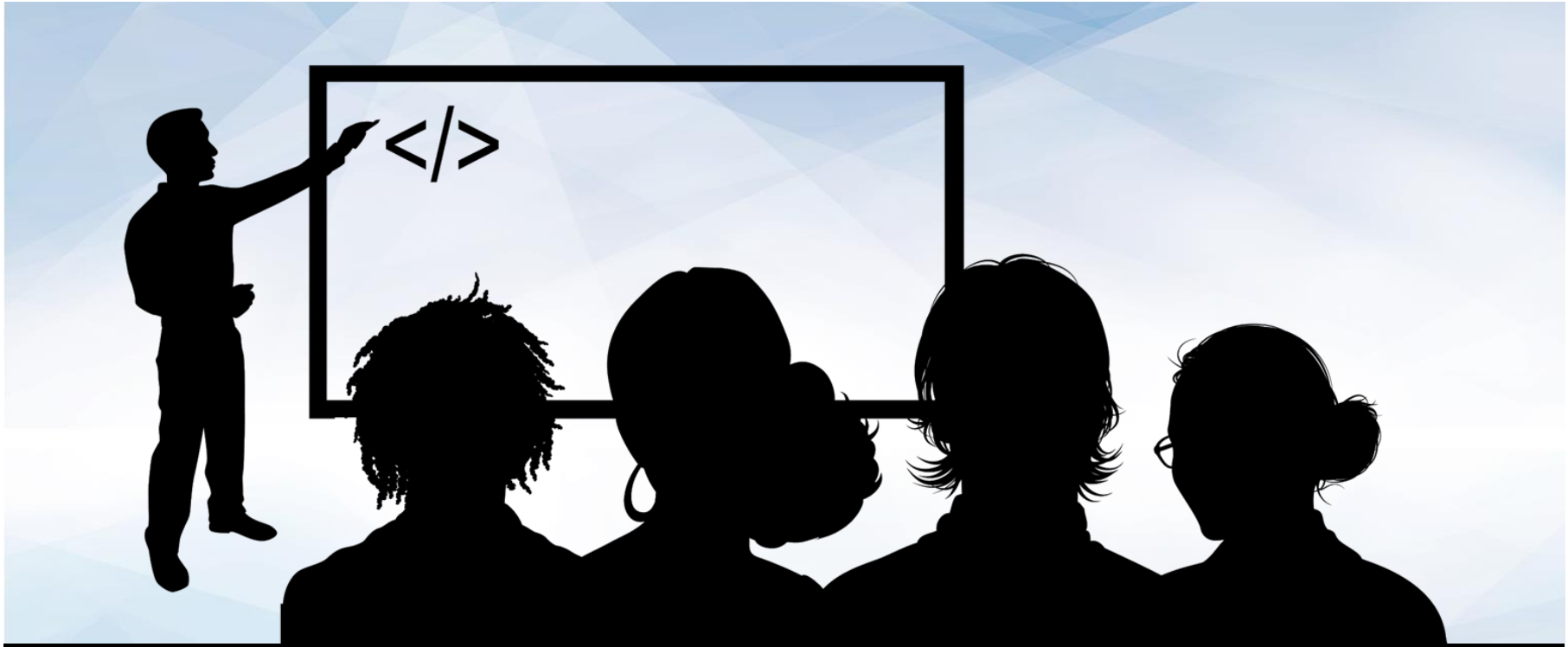
Instructor Demonstration

How do you add users to a system?

- `useradd, adduser`

Advantages of `adduser` over `useradd`

- Easier to customize user creation process
- set user passwords
- Create and manage groups / group memberships



Instructor Demonstration

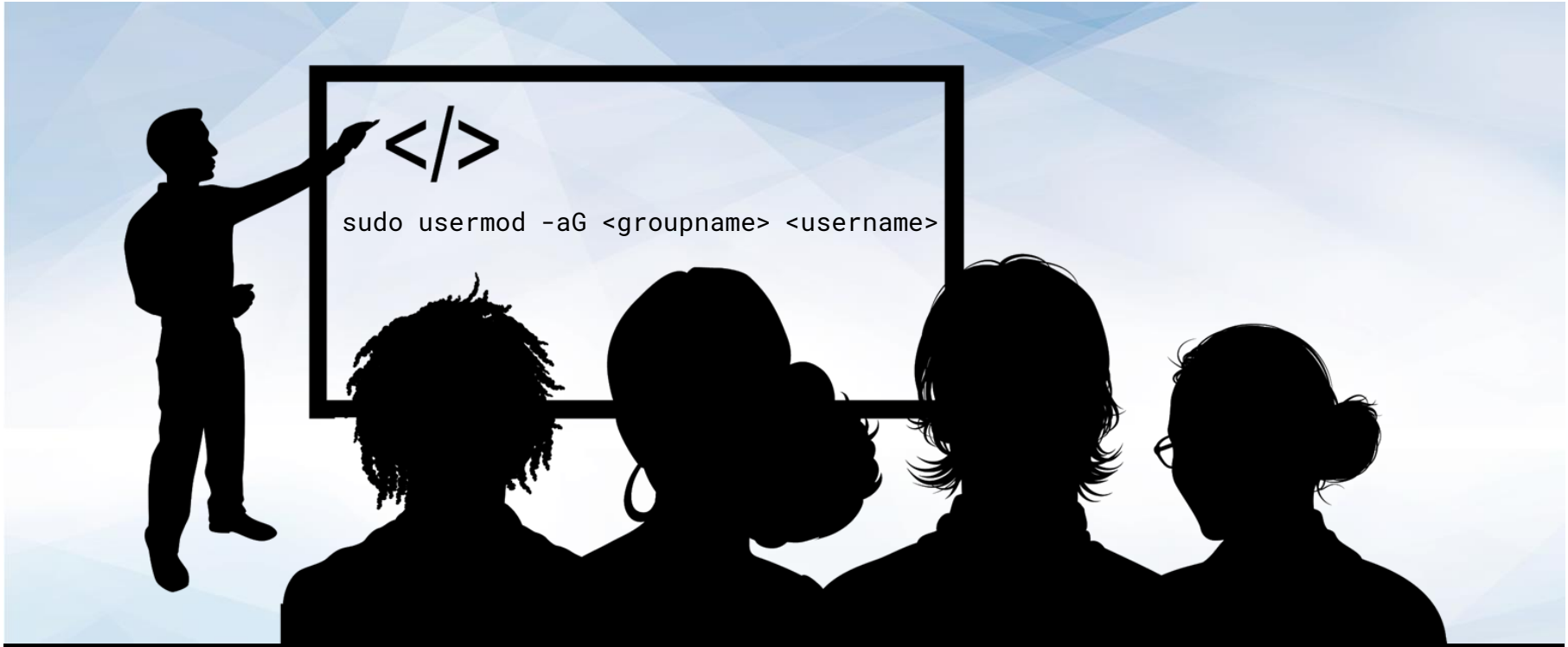
Primary and Secondary Groups

Primary and Secondary Groups

Instructor Demonstration

A user’s primary group sets the group owner of a file or process when that user creates a file.

A user’s secondary group determines which files they have access to.



Instructor Demonstration

Creating and Managing Groups

Activity: User and Group

In this activity, you will run user and group commands and then answer the provided questions.

Instructions sent via Slack.

Suggested Time:
15 Minutes

Times Up! Let’s Review.

User and Groups

Sudo

Sudo

Sudo is a safe way for normal users to run privileged commands that they shouldn’t always have access to.

- sudo stands for superuser, allowing normal users to run a privileged command by entering their password.
- Set up by installing the sudo package and then adding privileged users to the sudo group.
- Once a member of the sudo group, they will have to enter a password everytime they want to run privileged commands.
- The system administrator can also control which commands the user can run as root.

Instructor Demonstration

Using sudo

Activity: Sudo Wrestling

In this activity, you will interpret suspicious activity occurring in an `auth.log` file.

Instructions sent via Slack.

Suggested Time:
10 Minutes

Sudo Wrestling

Instructions

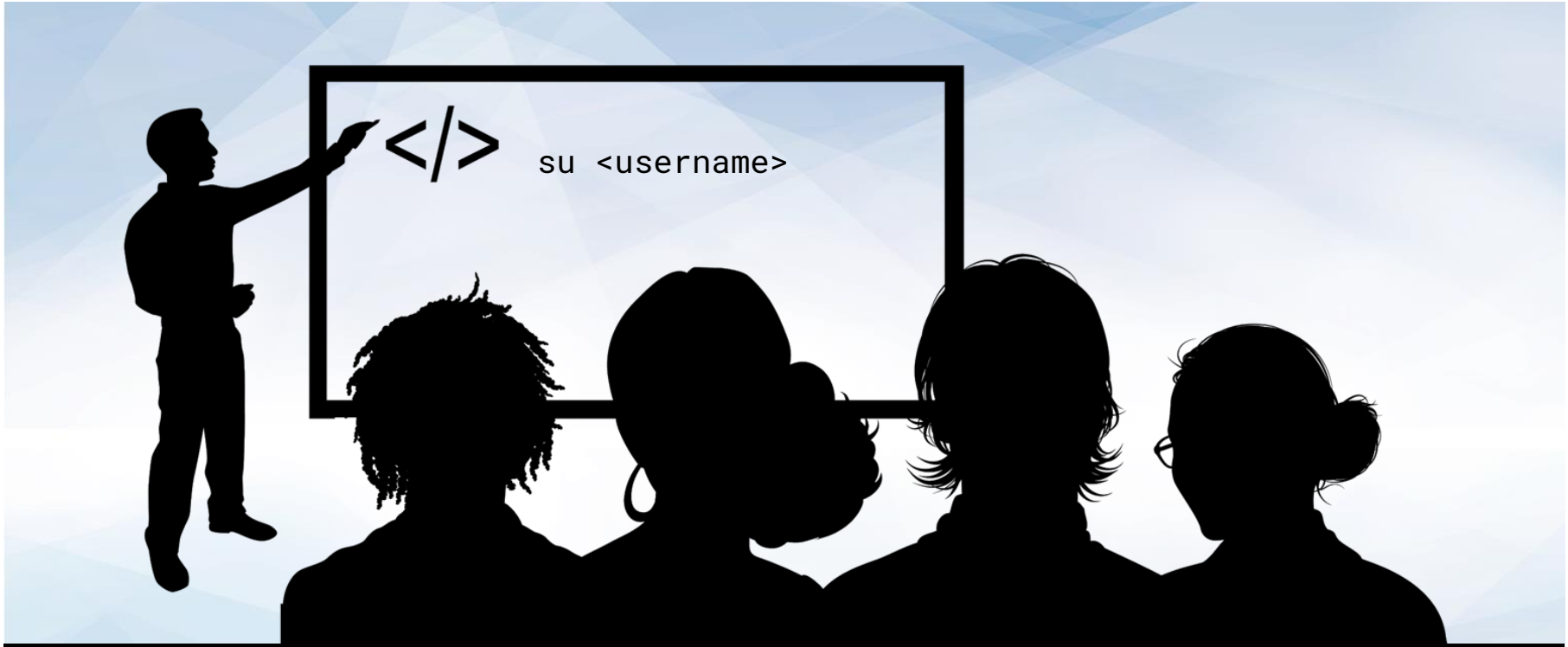
- ☐ Add your new user to the sudo group to allow them to run `nano` and/or vi as root.
  - This allows them to read and modify `root`-owned files, such as `/etc/passwd` and /etc/shadow
- ☐ Determine which user's account has been compromised
- ☐ Inspect `sudoers` log for evidence of brute-force attempts to `sudo cp /etc/shadow` to a directory in `/home`
- ☐ Identify which user was attempting `sudo`
- ☐ Search for other suspicious activity in that user's `.bash_history`
- ☐ Remove that user from privileged groups
- ☐ Change that user's password *or* remove their account

10 Minutes

Times Up! Let’s Review.

Sudo Wrestling

Switching Users



Instructor Demonstration

Switching User

Activity: su-per Privileged

In this activity, students will crack user passwords, and then use su to run files they ordinarily don’t use

Instructions sent via Slack.

Suggested Time:
10 Minutes

Your Turn: su-per Privileged

Instructions

Cracking Passwords

- ☐ What happens when you try to read `/etc/shadow`? Why does this happen?
- ☐ An administrator left a copy of `/etc/shadow` in one of the tmp directories. Find it.
- ☐ Create a new folder in your `Documents` directory, called `.hidden`, and change into it.
- ☐ Move the copied `shadow` file you found into `.hidden`, and change into `.hidden`.
- ☐ There's a program called `john-the-ripper` on your VM. Run it, and pass the shadow file as argument.
- ☐ What do you see when `john` finishes running? Record your response.

Finding the Flag

- ☐ One of the users has a "flag" file somewhere in their home directory that is executable.
- ☐ Find out who, and what the path to the file is.
- ☐ Use the passwords you just cracked to login as the user who owns the flag.
- ☐ Move into the directory you found, and run the flag file.
- ☐ If all goes well, you should get a message verifying that you have found the flag!

Times Up! Let’s Review.

su-per Privilege

Today’s Objectives

By the end of class, you will be able to:

- Inspecting and setting file permissions.
- Create and manage users and groups.
- Elevate privileges with sudo and su