6.2 Solutions and Guided Walkthrough

6.2.1 Solutions

1. *Change Password*

   To change a user account password on a Linux machine, first open a terminal. After launching a terminal, type the command:

   `passwd username`

   This command will begin an interactive dialog within which you will enter the current password and then the new password.

2. *Remove/Disable Unnecessary Accounts*

   There are many ways to disable or lock accounts in Linux systems, some of which do not preserve the current password associated with the account to be locked. One of the methods for disabling a Linux user account, while preserving the current password, is to use the following command:

   `passwd username -l`

   Once ready to unlock the account, run the command:

   `passwd username -u`

   The **/etc/shadow** file contains information related to usernames and passwords. Locking and unlocking an account using the method above modifies the contents of the **/etc/shadow** file to indicate if the account is locked. To delete a user, use the command:

   `userdel username`

3. *Enable Automatic Update Alerts*

   To enable automatic update alerts on the Linux machine, click the "Settings" button at the top right corner of the screen. This will display a dropdown menu, select the "Systems Settings", which will display the systems settings GUI. Next, under the "System" tab, click on the "Software & Upgrades" icon. Next, select the "Updates" tab and set the options as desired with automatic update alerts enabled.

4. *Disable or Harden SSH*

To SSH onto the machine, run the command:

```
ssh <targetuser>@<target-ip>
```

To stop the SSH service from running, use the command:

```
sudo service ssh stop
```

You can try to SSH into the machine after performing this step to confirm that it is no longer possible. In addition to disabling SSH, one can remove the SSH from the machine all together by running the following two commands:

```
sudo apt-get purge openssh-server
```

```
sudo apt-get purge openssh-client
```

To harden SSH by using SSH keys, run the following commands:

```
ssh-keygen -t rsa
```

Enter the location to save the keys to, as well as a passphrase if one will be required. Next, copy the public key to the remote machine which should have SSH access. This is accomplished by running the command:

```
ssh-copy-id <remoteuser>@<remote-ip>
```

5. *Remove Unnecessary Cronjobs*

   To remove Cronjobs, edit the Crontab file by using the command:

   ```
   crontab -e
   ```

   Scroll through the file until you find the job you would like to remove. It can be removed by either commenting out the line by appending a pound symbol (#) or by deleting the line altogether. Save and exit the Crontab file and allow the new Crontab file to install.

6.2.2 Guided Walkthrough

In order to complete the challenges in this laboratory exercise, see the steps in this walkthrough.

A Linux workstation is a staple at cyber defense competitions and in the workplace. Ensuring that the workstation is secure is integral to ensuring that all of the data on the machine is secure. Without proper workstation security, an malicious user does not need to perform a complex attack to gain access to secure files, but rather can simply use regular methods of accessing the

machine to gain access.

Challenge 1

The first step that you should do upon being given a machine is to change the password. Passwords should not only be changed once, but relatively frequently. To change your password on a Linux machine, use the **passwd** command. In Linux, you can specify the user for whom you are trying to change the password. Run the following command to change the password for an example user named *sampleuser*:

```
$ passwd sampleuser
```

This will allow you to change the password.

Challenge 2

Occasionally, you may discover accounts on your machine which are either unnecessary (Guest) or malicious. It is important to assess the situation and determine whether it is appropriate to disable or remove the user. In the following cases, the target user will be named *sampleuser*. Run the following command to lock/disable a user account in Linux:

```
$ passwd sampleuser -l
```

If determined that the account does not need to be locked/disabled, unlock the account by running the following command:

```
$ passwd sampleuser -u
```

If determined that the account needs to be deleted all together, run the following command:

```
$ userdel sampleuser
```

Challenge 3

Updates a cornerstone in secure systems. Vulnerabilities are discovered every day and patches for these vulnerabilities frequently come soon after the vulnerability is discovered. Though updates are critical, it can be challenging to remember to check for updates. For this reason, having auto updates enabled can be helpful. In order to enable automatic updates on a Linux Desktop machine, navigate to the “Settings” button in the top right corner of the display. This will display a dropdown menu, select the “Systems Settings”, which will display the systems settings GUI. Next, under the “System” tab, click on the “Software & Upgrades” icon. Next, select the “Updates” tab and set the options as desired with automatic update alerts enabled.

Challenge 4

SSH is a service on Linux machines which allows remote access to a machine. This can be helpful at times, but also poses a significant security risk. You should always assess whether certain services are necessary on your machine or not. If you cannot easily determine whether SSH is necessary, you can disable the service by stopping it from running temporarily. If the service is necessary, steps can be taken to harden SSH.

To SSH onto the machine, run the command:

```
ssh <targetuser>@<target-ip>
```

To stop the SSH service from running, use the command:

```
sudo service ssh stop
```

You can try to SSH into the machine after performing this step to confirm that it is no longer possible. In addition to disabling SSH, one can remove the SSH from the machine all together by running the following two commands:

```
sudo apt-get purge openssh-server
```

```
sudo apt-get purge openssh-client
```

To harden SSH by using SSH keys, run the following commands:

```
ssh-keygen -t rsa
```

Enter the location to save the keys to, as well as a passphrase if one will be required. Next, copy the public key to the remote machine which should have SSH access. This is accomplished by running the command:

```
ssh-copy-id <remoteuser>@<remote-ip>
```

Challenge 5

Cronjobs are helpful in automating tasks. Although, they are also an attack vector which is rarely considered. Because cronjobs allow a job to be run at fairly infrequent intervals, you may not even notice that the job is running unless you check. You can check the list of cronjobs on your machine by using the following command:

```
$ crontab -e
```

This will open the crontab file. You can then scroll through all the jobs and look for erroneous cronjobs. If you are unsure whether a job is necessary or not, you can comment the job out

using the pound symbol (#). If a job is not needed, you can remove the line from the file all together.