|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: Nishchal Sreevathsa |  |  |  |  |

Using Public Key Encryption to Secure Messages

Ethical Hacking & Lab 14

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

[Highlights](#_Toc409378036)

[Objectives](#_Toc409378037)

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 14](#_Toc409378040)
2. [Conclusion & Wrap-Up 16](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

|  |  |
| --- | --- |
|  | To create certificates (public and private key pairs) for an administrator and student, using Kleopatra.  There will be an export and import of the certificates into Windows.  A message will be encrypted using Opera Mail and the recipient's public key.  The message will be decrypted on the receiving end using the recipient's private key. |

## Objectives

|  |  |
| --- | --- |
|  | You will learn how to protect sensitive data and files in this lab by using encryption. As distinct users, you will create certificates, encrypt a message, and decrypt the message. Learning how to secure communications using public key infrastructure (PKI) is the aim. |

# Lab Description Details

## Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives

**Step 1:** On the topology, click the internal Windows 10 icon. Next, launch the desktop **Kleopatra application**. On New Certificate, click. Press Make an **OpenPGP key pair for yourself**. Enter **student** in the Name field and **student@campus.edu** in the email field.

A computer screen shot of a computer screen

Description automatically generated

**Step 2:** Click **Create Key** on the Certificate Creation Wizard screen. Enter **student** as the passphrase on the pinentry screen.

A computer screen shot of a computer

Description automatically generated

**Step 3:** To exit the Certificate Creation Wizard, click **Finish**.

A screenshot of a computer

Description automatically generated

**Step 4:** Click the student certificate and select Export Certificates from the Kleopatra screen. On the desktop, save the **Student.asc** file.

A computer screen with a white box

Description automatically generated

**Step 5:** Launch the desktop version of Opera Mini. Next, write an email. Enter **administrator@campus.edu** in the To field. Enter "**My Public Key**" in the Subject box. Type **Here is my Public Key** in the body. Next, affix the file.

A computer screen with a white box

Description automatically generated

**Step 6:** Launch the Windows Server and login as **administrator** and enter the Password as **P@ssw0rd** and open the command prompt. On the VM, set the clock.

A computer screen shot of a black screen

Description automatically generated

**Step 7:** On the desktop, launch the Opera Mini application. Look in the send/receive tab for the student's email with the subject "My Public Key." On the PC, save the **student.asc** file.

A screenshot of a computer

Description automatically generated

**Step 8:** Launch the desktop Kleopatra application. On New Certificate, click. Press Make a **personal OpenPGP key pair** for yourself. Enter administrator in the Name field and [**administrator@campus.edu**](mailto:administrator@campus.edu) in the email field. Click Create Key on the Certificate Creation Wizard screen. Enter administrator as the Passphrase on the pinentry screen.

A computer screen shot of a computer

Description automatically generated

**Step 9:** To exit the Certificate Creation Wizard, click **Finish**.

A screenshot of a computer

Description automatically generated

**Step 10:** To import the **student.asc** file from the desktop, click Import Certificates. To get the Certificate Import Result - Kleopatra, click OK.

A screenshot of a computer

Description automatically generated

**Step 11:** Within the Windows Server Domain, On the desktop, Created a new **message.txt file** and opened it, wrote, "**The Secret is that I like Green Eggs and Ham**," and saved it.

A computer screen shot of a computer

Description automatically generated

**Step 12:** Encrypt can be selected by right-clicking on **message.txt**, then choosing More GpgEX options.

A screenshot of a computer

Description automatically generated

**Step 13:** On the Sign/Encrypt Files page, click Next. To pick the certificates for the **administrator** and the **student**, hold down Control. Press Add. The bottom box should display both certificates. Press **Encrypt**.

A screenshot of a computer

Description automatically generated

**Step 14:** The message "**Encryption succeeded**" shows up in blue. Once the operation is over, remove the check marked "Keep open." Hit the "Finish" option.

A screenshot of a computer screen

Description automatically generated

**Step 15:** Launch Opera Mail, select the Unread Messages tab, and start a new email message. Type **student@campus.edu** in the To box. Enter **Encrypted Message** in the Subject field. Within the body, Please read the attached Encrypted Message, and attach the message.txt.gpg file.

A screenshot of a computer

Description automatically generated

**Step 16:** Go back to the Windows 10 machine and open the Opera mail application, check for the Encrypted message from the administrator in the send/receive message tab. Open the email from the administrator and save the **message.txt.gpg file** on the desktop.

A screenshot of a computer

Description automatically generated

**Step 17:** To decrypt a message, right-click on it, choose More GpgEX options, then select **Decrypt**. Click OK after entering "**student**" as the passphrase. A blue message with the words "**Decryption succeeded**" shows. After the operation is finished, remove the check marked "Keep open." Press the OK icon.

A screenshot of a computer

Description automatically generated

**Step 18:** After decrypting it, open the **message.txt** file to view the secret key message.

A screenshot of a computer

Description automatically generated

**Step 19:** Log off as **Administrator login** and sign in as **student 1** using the password **P@ssw0rd**. Select the "Unread" tab.

A screenshot of a computer login screen

Description automatically generated

**Challenge #1:** Opened the **flag2 email** and captured the **flag2: 223776**.

A screenshot of a computer

Description automatically generated

**Step 20:** Log off from **student1** and log in as **student2** and enter the password as **P@ssw0rd**.

**Challenge #2:** Opened the **flag3.txt** file and captured the **flag3: 776112**.

A screenshot of a computer

Description automatically generated

**Challenge #3:** Opened the Opera Mail and opened the **flag4 email** and captured the **flag4: 555779**.

A screenshot of a computer

Description automatically generated

**Step 21:** Log off from student2 and log in as **student3** and enter the password as **P@ssw0rd**.

**Challenge #4:** Opened the **flag5.txt file** and captured the **flag5: 918772**.

A screenshot of a computer

Description automatically generated

**Challenge #5:** Decrypted **flag6.txt** and captured the **flag6: 665544**.

A screenshot of a computer

Description automatically generated

# Supporting Evidence

**Screenshots, Research, Etc.**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Conclusion & Wrap-Up

## Summary with observations, Success & Failures, Challenges

Using Kleopatra, certificates with public and private keys were made for the administrator and student. After being exported from Kleopatra, the certificates were imported into the Windows computers. The administrator used the student's public key to encrypt a message, which was then sent through Opera Mail. Using their private key, the student was able to decrypt the message.

**Observations:**

Using Kleopatra to generate key pairs and certificates was simple. The certificates were successfully imported and exported between Kleopatra and Windows. It was successful to encrypt and decrypt the message in Opera Mail using the public and private keys.

**Success:**

* Admin and student credentials were generated successfully.
* communication that has been encrypted, decrypted, and signed with a private key.

**Risks:**

* When private keys are used with weak passphrases, it is possible for an attacker to figure out the passphrase and decrypt messages.
* Unencrypted private keys kept on disk are susceptible to theft in the event that the disk is misplaced, taken, or compromised.
* A man-in-the-middle attack could be executed by an attacker if certificates are not properly validated.
* False certificates could be issued by an attacker if the certificate authority is compromised.
* Breach of keys and antiquated encryption algorithms could result in brute force attacks.

**Remediations:**

* Make sure your private key passphrases are long enough and complex enough to prevent guessing.
* Protect encryption keys and store private keys encrypted on disk. When feasible, encrypt the entire disk.
* Before trusting certificates, make sure you thoroughly validate certificate chains and review certificate revocation lists.
* Make sure to choose trustworthy certificate authorities and keep an eye on their security procedures.
* Employ modern encryption techniques (such as RSA 2048+ bit, ECC, and AES 256) and gradually replace antiquated ones.