SSH LAB EXERCISE

This lab was developed for the Labtainer framework by the Naval Postgraduate School, Center for Cybersecurity and Cyber Operations under National Science Foundation Award No. 1438893. This work is in the public domain, and cannot be copyrighted.

Overview

This Labtainer explores the use of SSH from a client computer to connect securely to a server using public and private key pairs. In this example, mere possession of the private key is sufficient to access the remote host. In general, password-protected private keys are more secure.

Performing the lab

The lab is started from the Labtainer working directory on your Linux host, e.g., a Linux VM. From there, issue the command:

```
labtainer sshlab
```

The resulting virtual terminal is connected to a client computer.

Tasks

1. **Generate authentication keys (public/private RSA key pair) on the client computer input**:

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

Note: When prompted, DO NOT enter a passphrase.
This will create a private key and its corresponding public key and place them in your .ssh directory.

2. S**etup SSH on server for user to use their authentication keys**

The server's IP address is 172.20.0.3. The user is "ubuntu", and the user's password is also "ubuntu".

On the client computer:

- use this command:
  ```
  ssh-copy-id -i ~/.ssh/id_rsa.pub 172.20.0.3
  ```
- When prompted to "...continue connecting (yes/no):, type "yes".
- Provide the user password when prompted.

The above step will copy the public key to the ~/.ssh/authorized_keys file on the remote sever.

And that is it!

3. **Connect using SSH and display a file on the server**

On the client's computer:

A. `ssh ubuntu@172.20.0.3`
B. After connecting to the server: `cat filetoview.txt`
C. `exit`

Stop the Labtainer

When the lab is completed, or you would like to stop working for a while, run:

```
stoplab
```

From the Labtainer working directory. You can always restart the Labtainer to continue your work. When the Labtainer is stopped, a zip file is created and copied to a location displayed by the stoplab command. When the lab is completed, send that zip file to your instructor.