

SSH

This lab will help guide you through the steps required to use an SSH client, and to setup your system as an SSH server for secure remote access. Perform the indicated steps, and write the answers to questions in the appropriate spaces on this hand-out. Turn-in one filled in handout per computer system by the end of class. Be sure to include your name (and your partner's name, if you have one).

Configure the System

Bring the system up single-user and perform the initial network configuration

- Step 1. Boot your system into multi-user mode.
- Step 2. Configure your system to obtain its IP address using DHCP.

Install the SSH Packages

To run an ssh client and server, you need the openssh packages.

- Step 3. Ensure that you have the **openssh** packages **openssh**, **openssh-server**, and **openssh-clients**. If you do not have these packages, install them.

```
$ rpm -qa | grep openssh
```

Using the ssh Client

Connect to a system using the SSH client.

- Step 4. Log into your system as user **student**.
- Step 5. Use the SSH client to connect to the system **taipei.fhda.edu**. Since this is your first time connecting, ssh will warn you that it cannot verify the authenticity of the remote host.

```
$ ssh taipei.fhda.e
```

```
The authenticity of host 'taipei.fhda.edu' (153.18.75.207) can't be
established.
```

```
RSA key fingerprint is: ...
```

Q1. What is Taipei's RSA Key Fingerprint? _____

- Step 6. Type **yes** to continue the connection. You will get another warning that Taipei was permanently added to the list of known hosts.
- Step 7. SSH will now ask you for a password. You can be assured that the password is transmitted securely, since it is encrypted. Enter your account password for Taipei. You should now be connected.
- Step 8. Like rsh/rlogin, you can use an escape sequence to return to your originating shell. Type **~^Z** (~ followed by Control Z). This will return you to your shell, stopping the ssh shell connection.
- Step 9. Look in your system's home directory **~student/.ssh**
- Q2.** What file was created? _____
- Q3.** Describe its contents? _____
- Step 10. Resume your connection to Taipei by foregrounding the job with **fg**, and then exit that shell.
- Step 11. Connect once again to Taipei.
- Q4.** What was different this time? _____
- Step 12. Exit your connection.

Generate RSA Public/Private Keys

Use the `ssh-keygen` program to generate a public and private key pair and transfer the public key to another system for enhanced password security.

Step 13. Generate your RSA key public/private key pair using the `ssh-keygen` program. The default file specified is `fine`. Enter a passphrase to use.

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

Q5. What is the full path of your public key? _____

Q6. What is the full path of your private key? _____

Q7. What is your fingerprint? _____

Step 14. Open an FTP connection to Taipei using your real user account. Transfer your public key file `id_rsa.pub` to Taipei placing it as `~/.ssh/authorized_keys`.

Step 15. Exit the FTP connection and connect to Taipei again with `ssh`.

Q8. What question were you asked this time? _____

Set up the SSH Server

Configure your system to allow incoming `ssh` client connections.

Step 16. If the `sshd` daemon is not already started, enable and start it:

```
# chkconfig sshd on
# /etc/init.d/sshd start
```

Step 17. Examine the `sshd` configuration file `/etc/ssh/sshd_config`.

Step 18. Set the appropriate option(s) to disable any form of rhosts or host-based authentication.

Q9. Which options must be set? _____

Step 19. Add the line below to `/etc/ssh/sshd_config`:

```
Banner /etc/ssh/welcome
```

Step 20. Add the text "Connection is Secure!" to the file `/etc/ssh/welcome`.

Step 21. Restart the `sshd` daemon:

```
# /etc/init.d/sshd restart
```

Step 22. Connect to your own system using `ssh`.

Q10. What message was displayed prior to the connection? _____

Replace Insecure Services

Disabling the insecure services and replacing them with `ssh` provides superior security.

Step 23. Disable the insecure services (`telnet`, `rsh`, `rlogin`, `ftp`, and `wu-ftpd`) and replace them with `ssh`. You can use `chkconfig` and also remove the binaries themselves, replacing them with symbolic links to `ssh`.

Extra Credit

Step 24. Work out the details to forward a port through the SSH tunnel so that the insecure service is now secure.