WSE 380: Intrusion Detection
Session 0 — SSH Connections

Welcome to WSE 380: Honeypots and Intrusion Detection! Today, we will be setting up your devices with an SSH client to connect to a virtual machine that we will be running experiments on.

1 Installing an SSH Client

SSH (Secure SHell) is a network protocol that enables a computer to establish a secure connection to a remote computer that is running an SSH server. To connect over SSH, we need to make sure we have an SSH client on our devices. New versions of Windows (10 and later) and MacOS come with built-in SSH clients, so there is no need to install a separate client; Windows (10 and later) users can use the Windows Terminal application whereas MacOS users can use the `Terminal` application. However, if you are running an older version of Windows or if you would like to install a separate client, you can install PuTTY, a popular SSH client.

2 Connecting to a Remote Machine

The default syntax for the command to establish an SSH connection is `ssh -p 22 user@address`, where

- `ssh` is the name of the program,
- `-p 22` specifies a flag `-p` with a value of `22` (in this case, it means to connect to port 22),
- `user` is the username of the remote account, and
- `address` is an address to the remote machine. This can be a domain name (e.g., `google.com`) or an IP address (e.g., `1.2.3.4`) — in our case, we will be using IP addresses to connect to our remote machines.

As an example, if you are trying to establish an SSH connection to a remote machine with IP address `1.2.3.4` on port `5678` with a user account of `foobar`, you would execute the following command in your terminal:

```
wse380@wse380-22spr:~$ ssh -p 5678 foobar@1.2.3.4
```

If you are authenticating with a username and password, the SSH client should then prompt you to enter a password:

```
foobar@1.2.3.4's password:
```

Please refer to the email you received with the IP address and login credentials, and make sure that you can establish an SSH connection to it before our next meeting. If you have trouble connecting to your machine, please refer to this guide on how to connect to a machine over SSH or send me an email.

3 Extra: SSH Config and SSH Keys

To facilitate ease of working with remote machines, you can configure your own SSH configuration file and assign names to different machines. Typically, the SSH configuration file is located at `/.ssh/config`, where is the home directory of your user. An example configuration entry might be:

```
Host wse380-22spr
    HostName 1.2.3.4
    Port 3007
    User foobar
```

This way, you can just type `ssh wse380-22spr` instead of `ssh -p 3007 foobar@1.2.3.4`.

Additionally, you can connect over SSH using a public and private key pair to eliminate the use of a password. You can read more about them on a DigitalOcean tutorial or on GitHub documentation.