Lab 10.2: SSH Tunneling with Putty
IN618 Security

May 5, 2016

Introduction

In the first part of the lab we saw how unencrypted network traffic is easily captured, possibly revealing sensitive information. Sometimes we need to send data using an insecure protocol over an untrusted network. One way we can do this more safely is to *tunnel* our connection using ssh. Since ssh is encrypted, this will protect our data.

1 Procedure

1. Start Putty. In the left side menu, click on Connection → SSH → Tunnels.
2. Find the "Source Port" box in the dialogue and enter `8000` in it.
3. In the "Destination" box enter `sec-student.foo.org.nz:80`.
4. Click "Add".
5. Now select "Session" in the left side menu. Log into `sec-student.foo.org.nz`.
6. Start a new Wireshark capture like we did earlier.
7. In your web browser, enter `localhost:8000/secure-login` in the address bar. Complete your log in. Your http session is being forwarded through Putty on your local machine to the remote server using encryption.
8. Stop the Wireshark capture. Use the filter to find ssh packets. Inspect the packet data and note that you cannot read the encrypted payloads.

2 More on tunneling

SSH tunneling is a common tactic used to transport data safely over an untrusted network. It can also be used to pass traffic that may be blocked by firewalls provided that the firewall allows SSH through (many do). In this sense it can serve as a kind of ad-hoc VPN for technical users, but it's not really a solution for general users.