Lab 12.1: Capturing Network Packets
IN618 Security

May 18, 2015

Introduction

In this paper we've learned a bit about how to write more secure software and how to secure our systems. But our data frequently needs to travel over networks, and untrusted netnworks at that. In this lab we will see how easy it us to extract sensitive data as it traverses a network.

1 Procedure

First, visit the web page at `http://in618.sqrawler.com/secure-login`. Observe that you can log in with your Polytech user id and any password. Return to the login page.

Now we are going to repeat the login process, but we're going to capture the network packets as we do so.

1. Start the Wireshark network packet analyser. From the interface list, select your computer's ehternet card and click start.
2. In your web browser, fill out and submit the login form with a valid user name.
3. Take a minute to enjoy the picture of the kitten.
4. Go to the wireshark window and stop the capture by clicking the red square in the top menu.
5. In the main window you now have a long list of logged network packets captured by wireshark. We will filter that list. In the filter box at the top, enter "http" and then click apply.
6. In the filtered list, look for packets where the source or destination address is `54.66.229.216`. These are packets going to or coming from our web server.
7. Find the packet for which the info field contains "`POST /secure-login/login.php`". Highlight it.
8. In the detail pane below, find and expand the "`HTML Form URL Encoded`" item. In that field, find the username and password you provided when you submitted the form.
9. Now inspect the next packet in the exchange, which will say "`HTTP/1.1 302 Found`" in the info column. Expand the Hypertext Transfer Protocol section in the detail pane below and find the names and values of the cookies the server sent. Note those below

10. Inspect the other packets in the exchange. In particular, examine the application payloads that come from the server. We can see how any sensitive information that might be contained within is readable.

2 Reflection

The remarkable thing to note here is that we did not execute any sort of attack on the client or the server. All we have to do is get access to any part of the network that carries the data. What other sorts of network traffic may contain information that you would prefer to be kept private?