Security
Assignment 12, Monday, December 12, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your names and student numbers are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 12*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your names and student numbers are included in the document (since it will be printed),
   - your names are part of the filename (example: PimVullers_FlavioGarcia-12.pdf), and
   - the file is a PDF document.

Deadline: Monday, December 19, 8:30 sharp!

1. For this assignment you need to use the network analyser Wireshark. The first task is to download, install and get familiar with the tool.
   (a) Surf to `http://www.wireshark.org` and download the latest version of this tool. It is available for Windows, Linux and Mac.
   (b) Wireshark is a very advanced tool that can be used to analyse all types of network packets. Run the tool and select the ethernet device you want to sniff on.
   (c) When you play around and generate some traffic by browsing some web pages you will recognize soon that there are a lot of packets passing by on your interface. Besides the higher level protocols you probably will also see a lot of transport layer messages like messages of the Address Resolution Protocol (ARP) that help machines to find out each others IP addresses on a local network.

   It is possible to apply filters to the intercepted messages so that we only see messages that we are interested in. In the latest version the filter syntax is equipped with auto-completion. We can construct rules like (using example IP-addresses):

   ```
   ip.src==192.168.0.1
   http.request.method==GET
   ```

   And combine them...

   ```
   ip.dst==131.174.69.27&&http.request.method==POST
   ```

2. Now you have played around a bit, we would like you to answer the following questions. (To keep the amount of *noise* as low as possible you should close all unneeded network services like mail, VoIP (Sskype) and instant messaging (MSN).)
   (a) Lets look at the way the ping command works:
      i. Make sure Wireshark is up and running.
      ii. Open a terminal window (Windows: *Start - Run - 'cmd.exe'*).
      iii. In this terminal window issue the ping command to ping Google.com: `ping google.com`.
      iv. Use Wireshark to find out which two protocols are used by the command we issued.
   (b) Lets look at the application level of the HTTP protocol. In Wireshark it is possible to inspect the packet details and unfold different segments of a package. We want to investigate what data is transferred and whether this is done encrypted for the following two Radboud services:

- **Library:** `http://sifnos.ubn.ru.nl:8080/LBS_WEB/login.htm`
- **Blackboard:** `http://blackboard.ru.nl/`

The most convenient way to do this is by using a filter. Since both URLs lead to a login form that uses the POST method (way of sending the webpage parameters) we can filter for traffic that belongs to this POST method. This refinement can be written as the following filter:

`http.request.method==POST`

Make sure Wireshark is up and running, apply the filter above and surf to the Radboud Library service. Fill in the login form (you may use wrong credentials since we do not need a successful login) and submit the form. Now, try to find the corresponding packet with Wireshark and analyse its contents.

Unfortunately this will not work with the Blackboard service because the packets of this web application are not recognized as HTTP packets. The reason for this is that the Blackboard service sends the login over HTTPS. This is the HTTP protocol running on top of the Secure Socket Layer (SSL) which ensures that all data will be encrypted between the client and the web server. Clear the filter and try to identify which packets belong to the Blackboard service when you submit the login form. Try to find out how this secure login works.

3. Hand in the following:

   (a) **(4 points)** The names of the protocols, and the corresponding packets, used by the `ping google.com` command in question 2(a).

   You can copy the packet from Wireshark to the clipboard by:
   `right-click on the packet` → `Copy` → `Bytes (Printable Text Only)`.

   (Make sure that you copy the whole packet und not just a part, for example a single line.)

   (b) **(3 points)** The packet that was sent when you posted the login form of the Radboud Library service in the first part of question 2(b).

   Replace the password in the packet by asterisks (*).

   (c) **(3 points)** A description of what happens when you login on blackboard, that is, what did you find out in the second part of question 2(b).