WIRESHARK

1. INTRODUCTION

1.1 OBJECTIVES

During the class you should analyse several traffic captures.

1.2 LEARNING OUTCOMES

At the end of this assignment, you should know:

- How to use wireshark to analyse traffic.
- How the HTTP protocols works.

2. GENERAL GUIDELINES

2.1 PREPARATION

No preparation is required, besides reading the assignment.

3. LAB ACTIVITIES

Use Wireshark and the provided traffic captures. Filter the traffic so that only HTTP traffic is displayed. Based on the analysis of the traffic, answer the questions. Do not forget to justify your answers.

3.1 HTTP BASIC SERVICE

For this set of questions, use the provided "HTTP-basic.pcapng" file.

A similar capture can be obtained by opening the address:

http://web.tecnico.ulisboa.pt/~ist13242/basic/

1. What is the number of objects of the page?
2. How many HTTP requests are sent by the client?
3. Is the server able to successfully respond to each one of the requests? How do you know it?
4. What is the version of HTTP protocol that is used?
5. What type of browser is used to access the site?
6. What is the URI of the first image requested by the client?
7. How does the client know that it needs to GET two images to complete the page transfer?
8. Does the client wait for the reception of the first image to request the second one?
9. What is the length of the GET message correspondent to the request of the cat.jpg image?
10. What is the size of the cat.jpg image?

11. Draw the message diagram that describes the exchange of HTTP messages between the client and the server. You may use Wireshark menu "Statistics → Flow Graph" and select "Show: displayed packets", provided you have a filter for HTTP traffic applied.
12. Remove the HTTP filter. How many TCP connections were established? How many TCP connections were closed?
13. What are the source and destination IP addresses and ports for each TCP connection?
14. What is the initial sequence number for the entity that opened the first TCP connection? What is the initial relative sequence number for the entity that opened the first TCP connection? Note you may alternate between real and relative sequence number by going to Edit-Preferences-Protocols-TCP-Relative Sequence Number, and unticking or ticking this option.
15. How much time the first TCP connection took to be opened?

3.2 HTTP WITH AUTHENTICATION

For this set of questions, use the provided "HTTP-auth.pcapng" file.

A similar capture can be obtained by opening the following address and providing username "irc", password "secreta":

http://web.tecnico.ulisboa.pt/~ist13242/auth/

16. What is the number of objects of the page?
17. How many HTTP requests are sent by the client?
18. Why does the server answers with a code "401" when it receives the first request from the client?
19. What type of HTTP header is included in the "401" response message to inform the client about the expected action?
20. What type of authentication is required?
21. What is the message that the user receives in the browser?
22. What new type of HTTP header is included in the second GET message?
23. Can you read the username and password from the capture? If so, what are they?
24. Is there any difference between the GET messages used to request the cat.jpg image in this example and the GET messages used to request it in the previous example? If yes, what is that difference?
25. Draw the message diagram that describes the exchange of HTTP messages between the client and the server.

3.3 HTTP WITH FORMS

For this set of questions, use the provided "HTTP-form.pcapng" file.

A similar capture can be obtained by clicking the submit button at the address:
http://web.tecnico.ulisboa.pt/~ist13242/form/

26. What is the new method used by the client?
27. What is the name of the script that was executed by the server?
28. How many items are included in the form?
29. What is the pair (key, value) of the first item?
30. Is the information of the form transmitted to the server in plain text or is it encrypted?
31. After receiving the response from the server, what does the user see in the browser?
32. Is there any dynamic content in the response sent by the server? If so, what is this content?
33. Draw a message diagram that describes the exchange of HTTP messages between the client and the server.

4. REPORT

A report should be delivered through the Fenix project Delivery System in PDF format, until 48h before the next laboratory class.

The report should include:

- The answers to the questions.