Laboratory 2

Software on your laptop

Assuming that you are running Red Hat Linux or Windows, you should install Ethereal (a packet analyzer). It is available on the website:
http://www.ethereal.com
More specifically
http://www.ethereal.com/download.html

Laboration

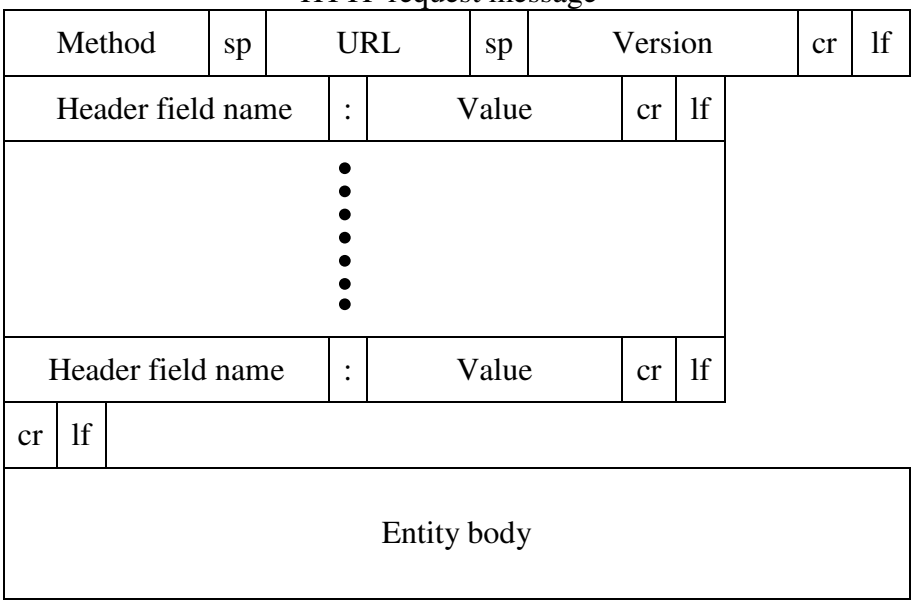
1. Open your email accounts like yahoo, hotmail, KTH etc.
2. In Windows, run the command **netstat** in Command Prompt. In Linux run **netstat –t** in a terminal. Check the status of TCP connections like ESTABLISHED, TIME_WAIT etc. Keep on running **netstat** and observe the changes in the connection status.
3. Now open messenger like yahoo, msn etc. and observe the output for **netstat**.
4. Start ethereal and go to the website http://csd.ssvl.kth.se/~csd2005-team2/
5. After opening this website, stop ethereal and enter the following expression in the filter to see the packets coming to or going out of your interface.
   Filter : ip.addr == Your IP address
6. Press apply button to apply this filter.
7. Find the three packets showing 3-way handshake of TCP connection establishment. Try to locate the three packets which are SYN, SYN-ACK and ACK. Observe how sequence numbers and other fields are changing in these packets.

TCP Header

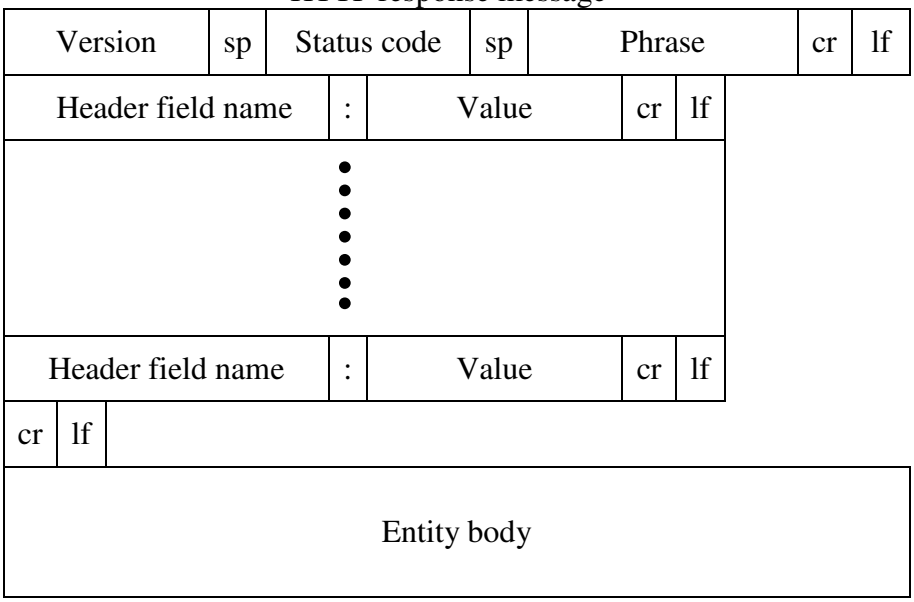
<table>
<tr><td colspan="8">Source port address
16 bits</td><td colspan="2">Destination port address
16 bits</td></tr>
<tr><td colspan="10">Sequence number
32 bits</td></tr>
<tr><td colspan="10">Acknowledgement number
32 bits</td></tr>
<tr><td>HLEN
4 bits</td><td colspan="2">Reserved
6 bits</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Window size
16 bits</td></tr>
<tr><td colspan="8">Checksum
16 bits</td><td colspan="2">Urgent pointer
16 bits</td></tr>
<tr><td colspan="10">Options and Padding</td></tr>
</table>

8. Now focus on the different HTTP messages and observe the request and response headers. An HTTP request message is shown below. Try to locate methods like GET, HEAD, POST etc. and retrieving of different logos.
9. Start ethereal and in your browser, ask for
   http://csd.ssvl.kth.se/~csd2005-team2/pix/kth_logo.gif
   Did you see any traffic? What did the packets contain?

HTTP request message



HTTP response message



10. Repeat using the url:
    http://web.it.kth.se/~maguire
    Is there any difference in the packets you see (or don't see)?
11. Now start ethereal and go to some secure website like https://auth.wan.it.kth.se and observe the differences from simple HTTP messages.
12. Start ethereal and in Command prompt (Windows) or terminal (Linux), start an ftp session by typing the following command:
    ftp ftp.sunet.se
    User: anonymous
    Password: Any email address

13. Type in **dir** (Windows) or **ls** (Linux) to see the list of directories and files at this ftp website.
14. Change to directory etc by typing **cd /pub/Linux/distributions/debian/doc.**
15. Get the file by typing get **mailing-lists.txt**.
16. Logout from the ftp session by typing **bye**.
17. Observe the FTP packets and transfer of the file in ethereal capture. How many well-known ports are being used?
18. Delete the text file.
19. Start ethereal again and type in ftp.sunet.se in the browser. Go to the directory **/pub/Linux/distributions/debian/doc** and double click the file **mailing-lists.txt** to save it on your hard disk. Do you see similar messages as in the previous case?
20. Now use telnet to establish a connection with the time server. Type in the command:
    telnet www.it.kth.se 13
    and
    telnet ripper.it.kth.se 13
21. Type QUIT finishing the session. What is the difference in behaviour? Why?
22. Now try some secure sessions via SSH. In Windows, download puTTY from the following website:
    http://www.openssh.com/windows.html
    SSH to ripper.it.kth.se using your IT.KTH.SE account user name and password.
    Type **exit** to logout.
    In Linux try
    ssh ripper.it.kth.se
23. Observe the packets. Which algorithm has been used for secret key exchange?
24. Start ethereal and start an ftp session:
    ftp 130.237.251.93 (IP address subject to change)
    user: int1305f
    password: indanger
    Type in **ls/dir**.
    Type **bye**.
    Observe the packets and find out the password. In ethereal, go to **Analyze > Follow TCP stream**. See what happens.
25. Start ethereal capture and start a telnet session:
    telnet 130.237.251.93 (IP address subject to change)
    user: int1305t
    password: regnadni
    Type **ls/dir**.
    Type **quit**.
    Observe the packets and find out the password. In ethereal, go to **Analyze > Follow TCP stream**. See what happens. Compare the result with SSH session.