SE 431 Lab1: Sniffing Network Traffic

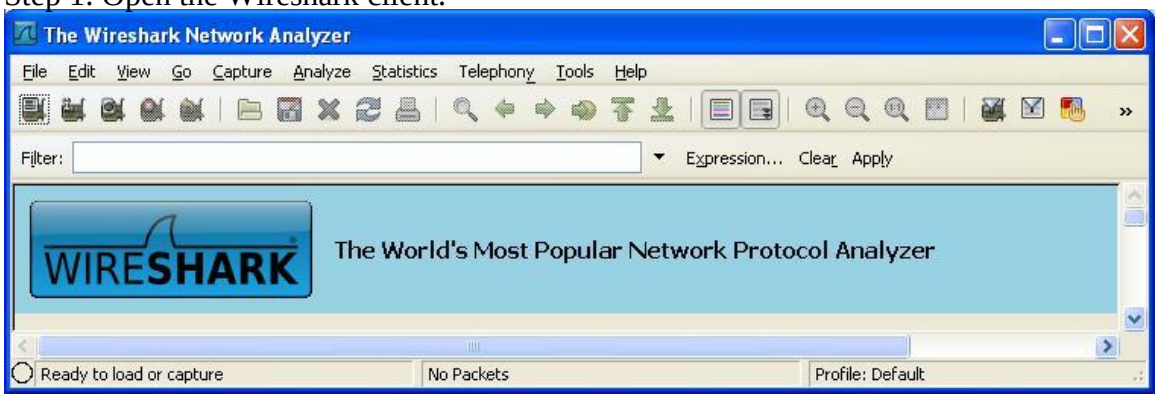
Goal: At the end of this assignment students will have demonstrated the clear text vulnerability of ftp and be able to retrieve user name and password.

Summary: This lab consists of two parts. Part I is to familiarize you with the wireshark packet analyzer and to see the difference between http &https protocols. In part II, you will be experimenting with Wireshark to sniff usernames and passwords in ftp applications.

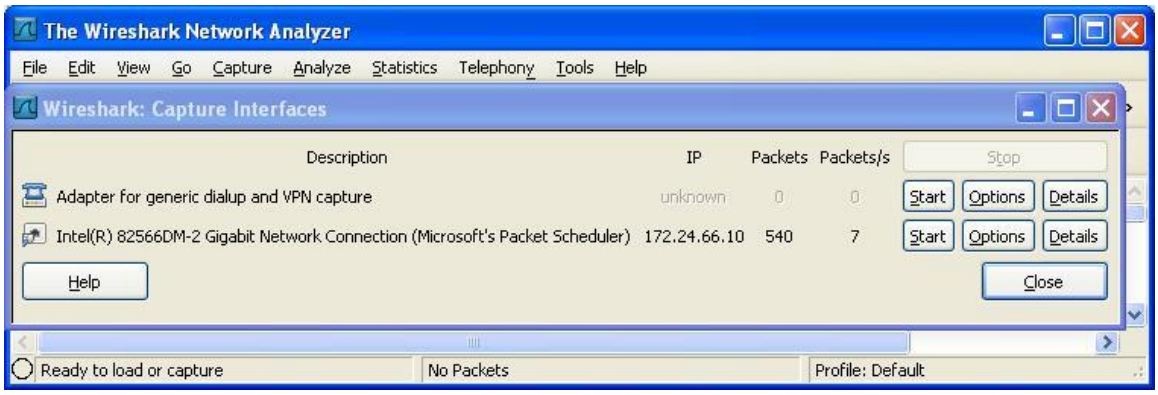
Part 1: Getting started with Wireshark

A)

Step 1: Open the Wireshark client.



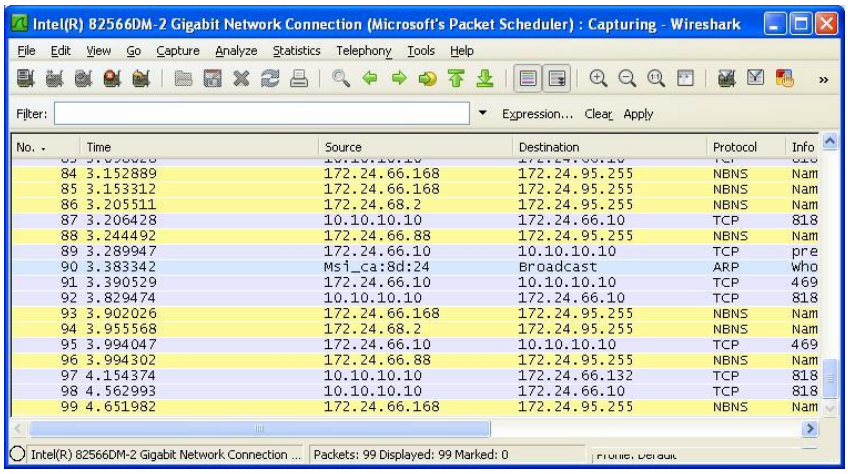
Step 2: From Capture Tab Select the Interface



Click the capture button next to the interface.

Step 3: Open your web browser, and visit http://www.cnn.com.

Step 4: After downloading the webpage stop the capture. On a busy network the traffic trace file can grow very large.



Deliverables for Section A:

- ❖ For this part provide detailed screen dumps (screen shots) for the following:

1. Show your ip address “using command line”
2. Filter the packets based on your ip address and https protocol
3. Filter the packets based on DNS protocol only
4. Show I/0 Graph for your network traffic

B)

Open your web browser, visit [httpWeb] and redo what we learned in Wireshark lab.

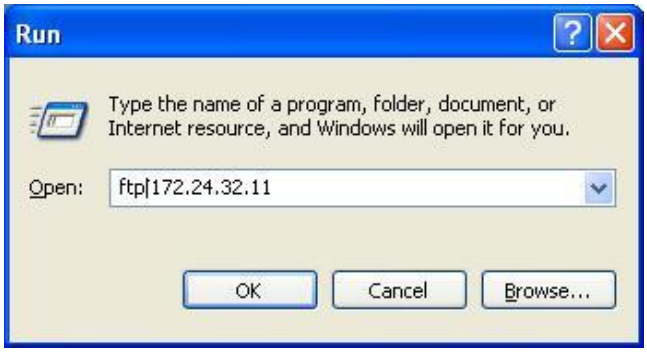
Deliverables for Section B:

- ❖ For this part provide detailed description using your own words and screen dumps (screen shots) about how you get the username and password in clear format.

Part 2: Using wireshark for Username and Password Sniffing

Step 1: Using the wireshark client, start a new capture
Step 2: Initiate FTP sessions

From the Run prompt on your machine establish ftp sessions to ftp.drivehq.com
e.g ftp ftp.drivehq.com. User name: SE431 and password: MeshMa3gool.



Step 3: stop the capture.
Step 4: Return to Wireshark Main Screen, Filter by Protocol (FTP) and continue as usual to See the username and password

Deliverables:

For this part provide screen dumps to show how you were able to find the username and password used in the FTP session in detail (also you should provide screen shot for CMD).