|  |  |  |
| --- | --- | --- |
| **Sheridan College** | | |
| **Course** | **INFO24178: Computer and Network Security** | |
| **Professor** | **Abdul Mustafa** | |
| **Student Name** | **Vsevolod (Steve) Ryabinin (group:Julio Tain Sueiras) juliosueiras@gmail.com** | |
| **Student ID** | **991243672** | |
| **Activity 2: Internet Traffic Analysis** | | |
| **Performed Date** | *Date: 28th January 2015* | |
| **Instructor's Sign** |  | **(marks)**  **(out of 10)** |

**IMPORTANT**: For all the activities, use of virtual machine is recommended.

**Note**: All the following activities should be performed in groups of 2 members.

|  |
| --- |
| **(A) Capturing and Analyzing FTP Traffic** |

**Task 1: Install and Run FTP Server**

(a) In one of the group member’s PC, install a free FTP server. Go to <http://www.cerberusftp.com/download/> and download the 32-bit version of the software. (You can use FTP server in IIS if you are using Windows, use any other FTP server of your choice.)

(b) Install the server and run it. Keep the ‘anonymous’ user name. You do not need to create any new user. (Of course, you can create one for testing.)

(c) Note that the server created a folder called ‘ftproot’ in your C drive. Create a text file by your name in the folder. Write something interested (and ‘confidential’!) in the text file and save it.

**Task 2: Download File and Capture FTP Transactions**

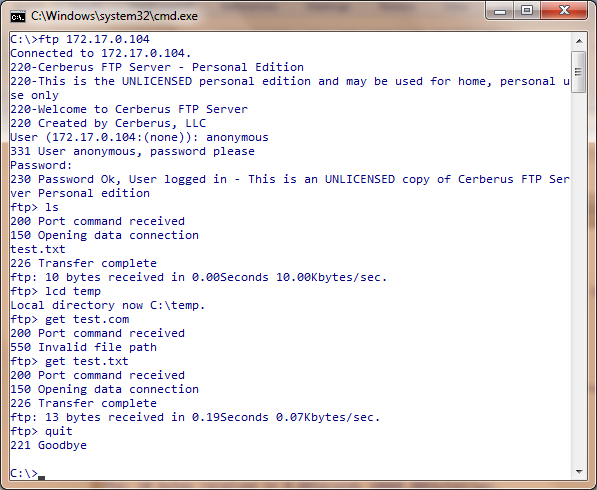
(a) Choose a PC in the group to be the ftp client. In C drive of this PC, create a folder called ‘tempftp’. You will download in this folder.

(b) Open a command window. Go to the folfer ‘tempftp’.

(c) Type ‘ftp *server \_ip\_address*’. BUT DON’T hit Enter yet.

(d) Start Wireshark and capturing in the relevant interface.

(e) Now hit Enter the command window. Perform the following steps to download the file from the FTP server. Follow Fig. 1.



(vi) Quit FTP session

(V) Download file

(I) Open FTP connection

(IV) Change local folder

(III) List files

(II) Supply username and password

**Figure 1**: FTP session

(I) Open the ftp connection. (Actually, you already did it in (e) above)

(II) Supply username and password. Username is ‘anonymous’, and password is any email address (e.g. me@abc.com).

(III) Use the ‘ls’ command to see the list of files in the server. You should see the file that your friend created.

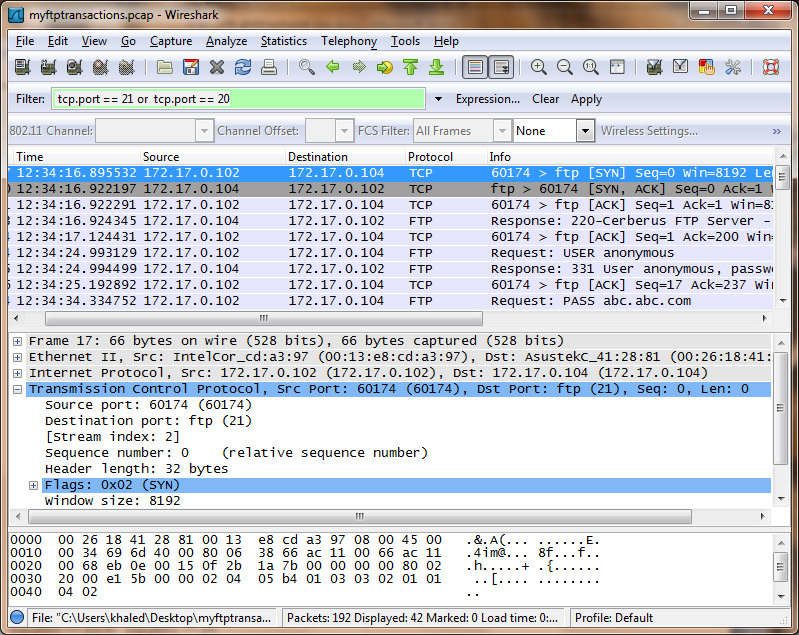
(IV) If you need, use ‘lcd’ command to change the local active folder (where the downloaded file will be saved).

(V) Use the GET command to download the file.

(VI) Use ‘quit’ command to terminate the connection.

(f) Stop Wireshark capture.

(g) Use the filter ‘**tcp.port == 21 or tcp.port == 20**’ to see only ftp related transactions. You should see something similar to Fig. 2.



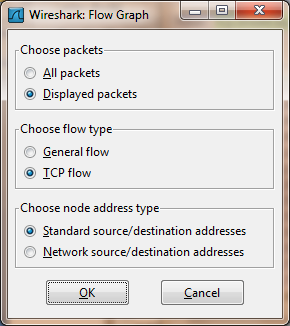
**Figure 2**: Captured FTP packets

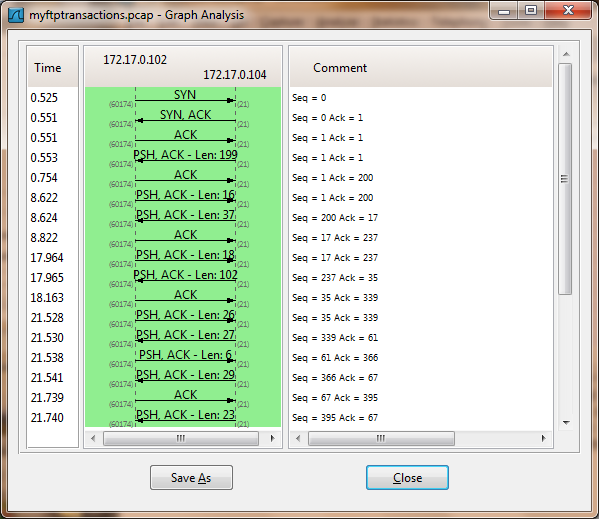
(h) In the listed packets, identify the initial ftp login transactions.

(i) From the menu, select ‘Statistics🡪FlowGraph’. In the next window, choose ‘Displayed packets’, ‘TCP flow’ and ‘Standard source’, as shown in Fig. 3. A transaction diagram, similar to Fig. 4 will appear. This graph clearly shows the handshaking in TCP level and FTP level.

(j) Find out how many 3-way hand shaking occurred. Note the port numbers.

|  |
| --- |
| Output#1: Graph Analysis of packets |
|  |

 **Figure 3**: Flow Graph options

 **Figure 4**: Flow graph

(k) Now, in the main capture window, find you the frames corresponding to username and password transaction. Notice that both username and password was supplied in clear text! Take a screenshot and add to the report.

|  |
| --- |
| Output#2: Username and Password of FTP in wireshark |
|  |

(l) Find the frames corresponding to the transfer of the file. Notice that the file is transferred in clear text. Take a screenshot and add to the report.

|  |
| --- |
| Output#3: File transfer packet in wireshark |
|  |

|  |
| --- |
| **(B) Capturing and Analyzing Telnet Traffic** |

**Task 1: Install/Enable and Run Telnet Server**

(a) In of the PCs of the group, install/enable Telnet service in your Windows machine (Vista or 7). Also, enable Telnet client. (Do a little web search if you need help for this task).

(b) Run the server.

(c) Create a temporary user account (with password) in the server PC.

**Task 2: Log in using Telnet**

(a) In the client machine, open a command prompt. Use this command.

‘telent *server’s\_IP\_Address*’

(b) Supply the temporary username and password when asked for authentication.

(c) If the login is successful, go to the next task. Otherwise troubleshoot.

(d) Take screenshot of your command transactions in the ‘cmd’ window and add in the report.

|  |
| --- |
| Output#4: Telnet connection |
|  |

**Task 3: Capture and Analyze Telnet Transactions**

(a) Log out the Telnet access from the client PC.

(b) Start capture using Wireshark.

(c) Log in again to the Telnet server.

(d) After login is complete, stop the capture.

(e) Again, analyze the captured frames and look for frames that contains authentication transactions. Can you see the username and password supplier by the client in clear text? Take a screenshot and add in the report.

|  |
| --- |
| Output#5: Password packet In wireshark(telnet) |
|  |

**(C ) Secure Communication**

1. Search the web for solutions for secure communication while using file transfer or remote login services.
2. Find some software tools- investigate their features. Find out the underlying protocols, port numbers, authentication/encryption mechanisms, etc. being used.
3. Write your observation below.

|  |
| --- |
|  |

**Task 5: Submit the Report**

1. Show your results to the professor.

Upload the completed word file in SLATE2 Dropbox. (**IMPORTANT**: Name the file according to your name. 10% reduction for wrong file naming.)