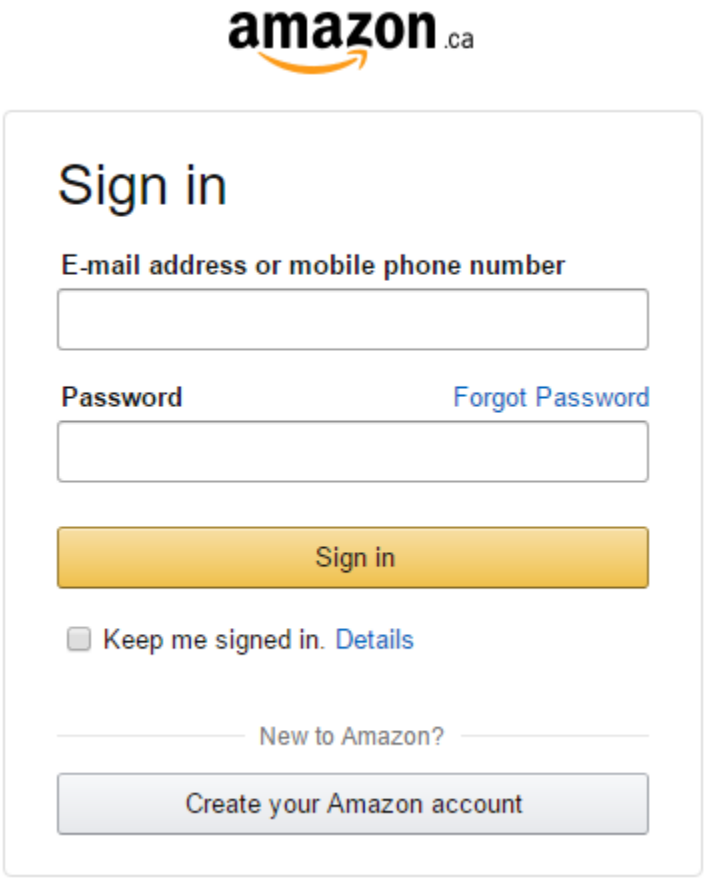
Lab 2: Encrypted Authentication Analysis, Social Engineering, and Steganography



Computer Security Laboratory (EECS 4481)

Department of Electrical Engineering and Computer Science

Khalil Abuosba, Ph.D.

Winter 2019

The purpose of this assignment is to sample different attacks that have been encountered on the web based on the Social Engineering approach.

General Information and Policies

- *Solutions must to be submitted on through the blackboard system.*
- *Ideal reports include screen snapshots of all of the exercises as well as copies of data segments where applicable.*

Objectives

- *Sample and test social engineering approaches.*
- *Attempt to reconstruct an attack.*
- *Review operating systems commands useful for credentials retrievals*
- *Install the XAMPP Platform..*

Keywords

Social Engineering, Phishing, Cross Site Scripting, C Shell,

Readings and Resources:

- Review Week-1 and Week-2 Lecture notes.
- Read about the functionalities of the keywords above.

Deliverables

- Lab Report.

Part 1: Telnet and SSH Connections Analysis

Retrieve the resource: http://overthewire.org/wargames/bandit/ and play the Bandit game. Once you reach level 10 of the game,

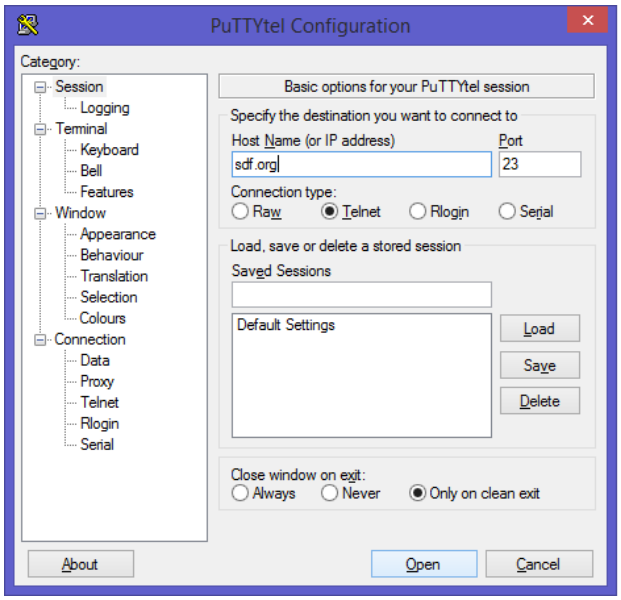
1. Telnet

- **Use the file Puttytel.exe that you have downloaded from the site** http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

  - **The next task calls for connecting to SDF UNIX server and create your own account on the server using Telnet connection**

1.1 Run the file puttytel.exe software that was downloaded in sections 1 or 2

1.2 Connect to the SDF server using the URL SDF.org

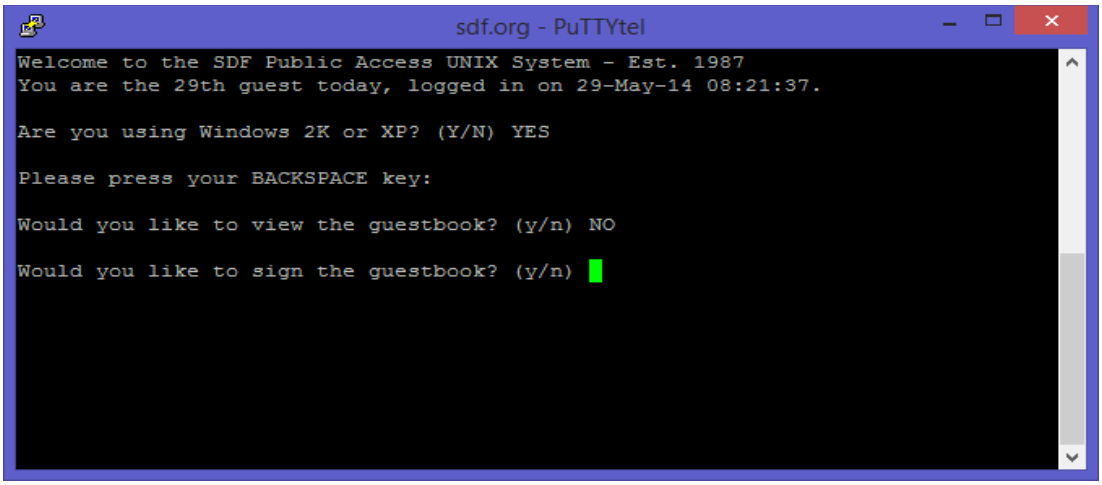


1.3 observe the port number that is being used.

1.4 Login to the SDF server using “new”

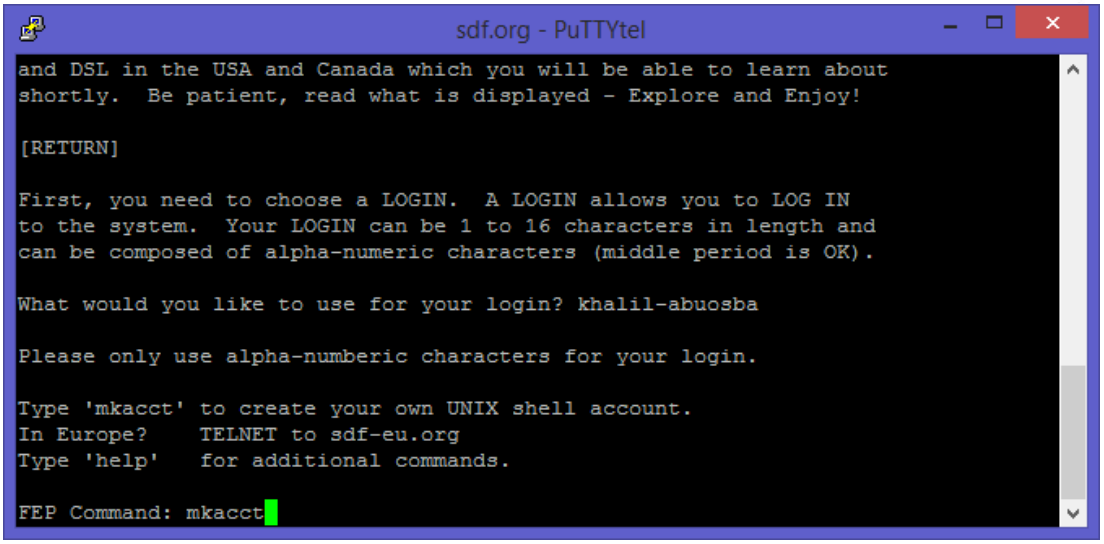
3.5 on the UNIX server login menu

3.6 Answer the questions below



3.7 Click the return key

3.8 Create your own account on the server as displayed below; use the mkacct command to create your account.



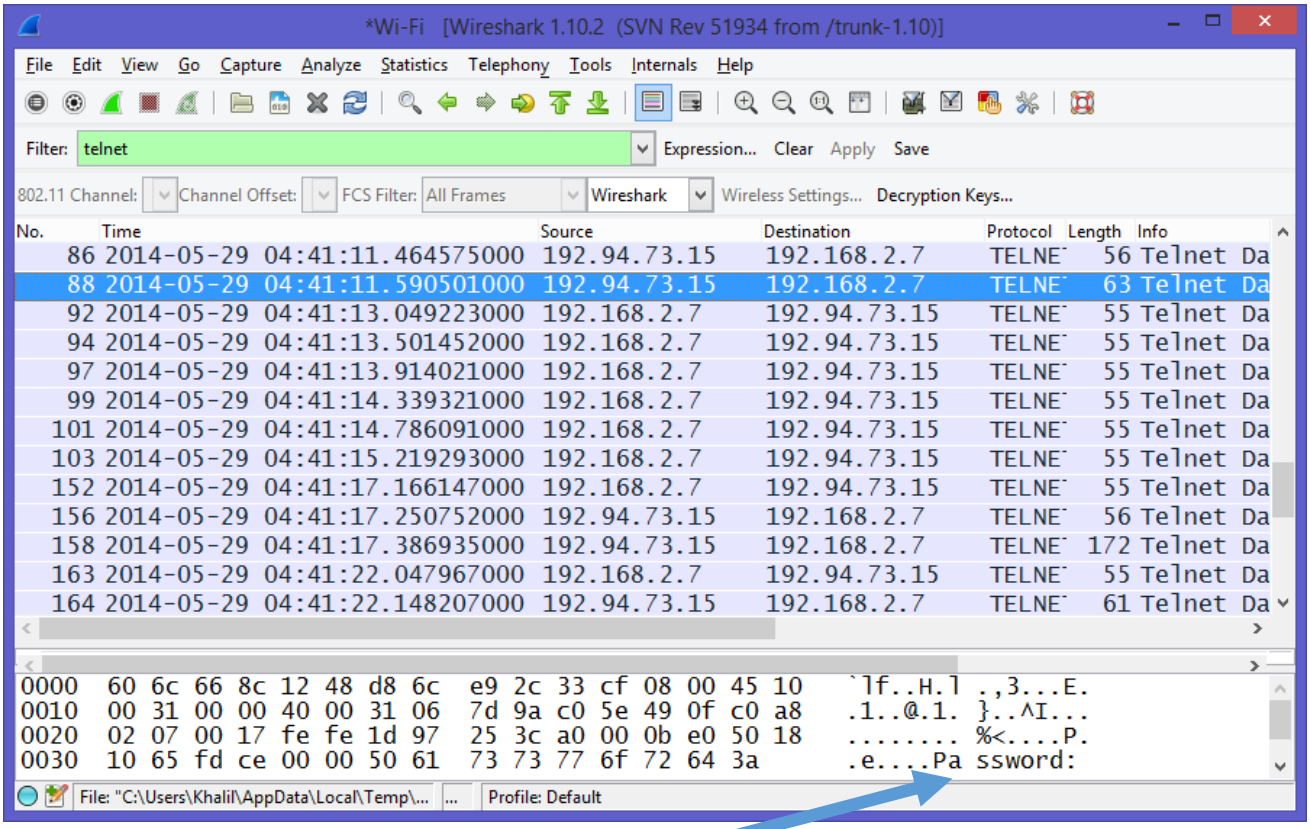
3.9 fulfill the registration process

3.10 Start Wireshark s/w and start capturing packets

3.11 Login to the SDF account using your account credentials (Login username and password)

3.12 As soon as you are prompted with the screen shown below, stop capturing packets.

3.13 In the Wireshark I/F create a telnet filter and apply it to the captured packets



3.14 observe the packet that signify your password input process

3.15 Notice that your password is captured in the succeeding packets; following this particular one. A character in each packet.

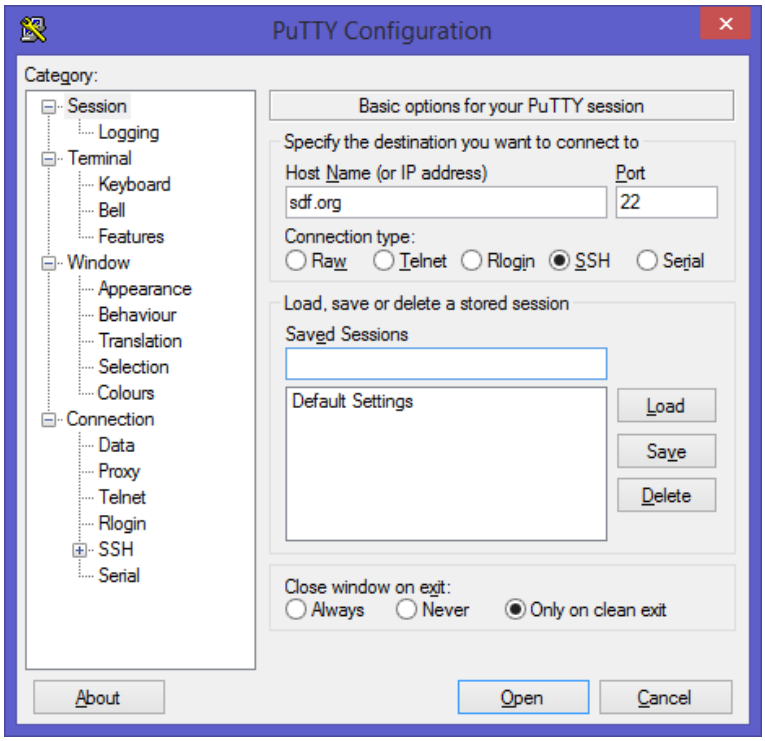
3.16 Document your findings

2. Secure Shell (**SS**H)

- Downloaded the putty.exe file from the site http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
  - The putty.exe s/w is an implementation of SSH; the next task calls for connecting to SDF UNIX server and create your own account on the server using SSH connection

4.1 Run the file putty.exe software

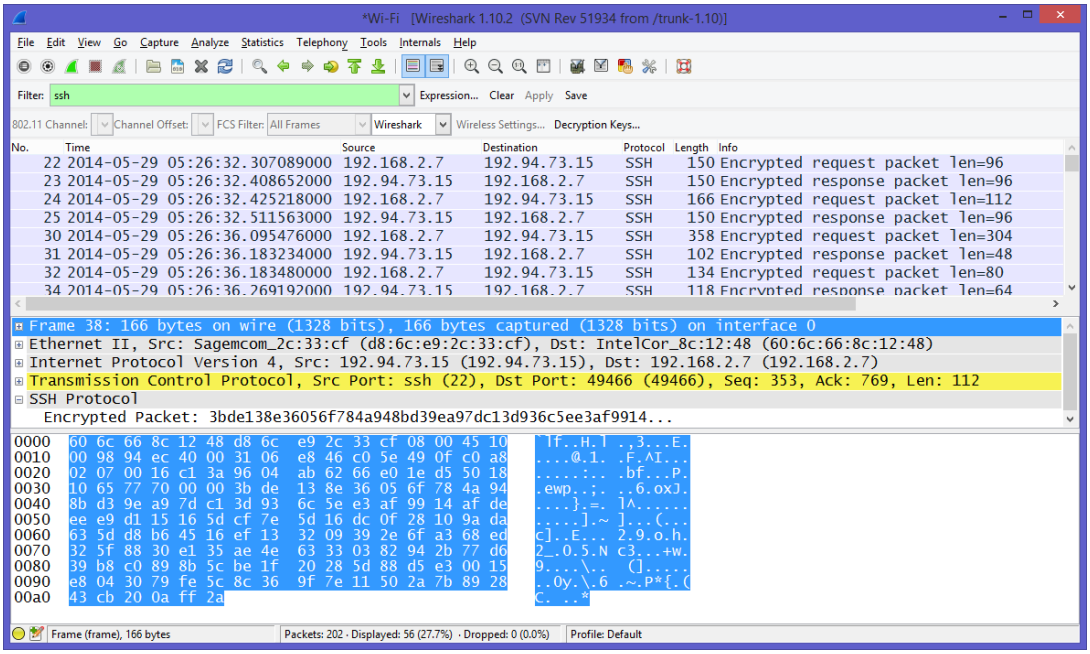
4.2 Connect to the SDF server using the URL SDF.org ➔ click open



4.3 Observe the port number that is being used

4.4 Start Wireshark s/w and start capturing packets

4.5 Login to your SDF account using the credentials that you have used in section 3Apply SSL filter to the captured packets



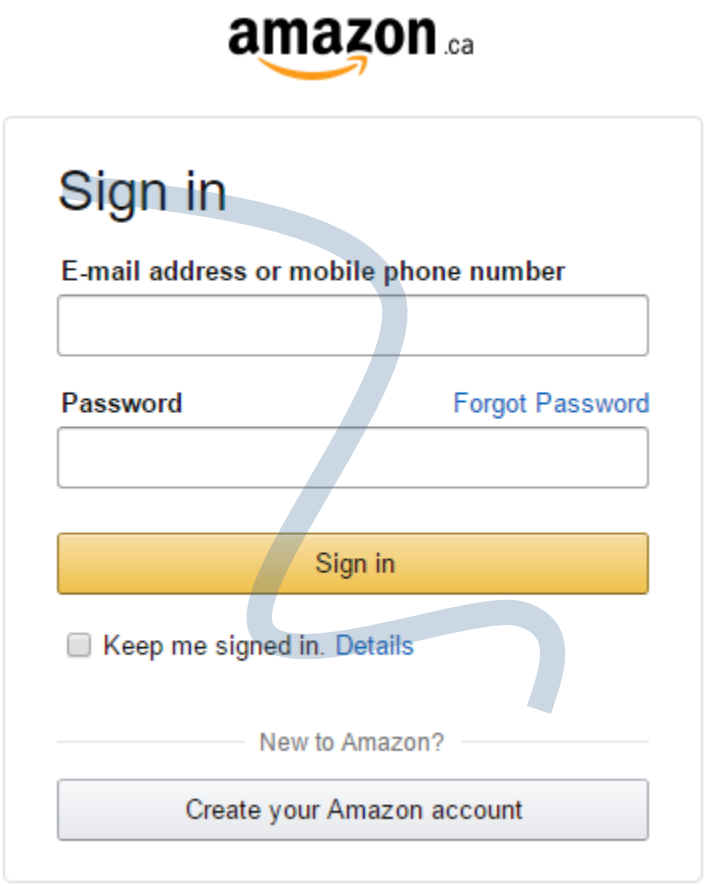
4.6 Investigate the possibility of capturing either the user name or password

4.7 Document your findings using screen snapshots (with captions) and upload copies of the Wireshark data files.

- Document your report in a .pdf file and attach your Wireshark segments to the submission.

Part 2: Social Engineering - Phishing

1. Use a website copying tool copy the login page of Amazon.ca (URL)



2. Modify the web page to direct the user to a bogus login page that capture their credentials.
3. Attempt sending the scheme to abuosba@eecs.yorku.ca
4. Document your work.

Part 3: Steganography Applications – Secret Hiding

A. Microsoft Windows Example

1. Using the Notepad, create a text file and insert the following line:
   Testing the Environment!
   Save the file as **a.txt**
2. Download the attached image file (b.png) to the same directory of the text file.
3. Parse the file using an image reader and document the output.
4. Attempt to read the file using the command: **type b.png** ➔ Document the output.
5. On the command prompt run the following command: **type a.txt >> b.png**.
6. Parse the file using an image reader and document the output.
7. Attempt to read the file using the command: **type b.png** ➔ Document the output.
8. Using a notepad session, open the file b.png and scroll down to the end file, document what you see.

B. Kali Linux Example

1. run the command: apt-get install steghide to install the steghide tool.
2. Create a text file that stores the statement "The password is in this phrase!" and name it z.txt
3. Download the attached file: lassonde.jpeg.
4. Run the command: steghide embed -ef z.txt -cf lassonde.jpeg
5. Run the command: rm z.txt
6. Run the command: steghide extract -sf lassonde.jpeg

Part 4

Retrieve the resource: http://overthewire.org/wargames/bandit/ and play the Bandit game. Once you reach level 10 of the game.

Using SELinux commands, solve the game for phases 1 through 6.

- For each phase/level document your solution.