In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 817: Advanced Network Security

Mehdi Kharrazi *Azar 5^{th}, 1394*

Homework 3

Please email your answers/report in **PDF format** TO "kharrazi@sharif.edu" and CC "masalehi@ce.sharif.edu" and "masoudian@ce.sharif.edu" . The HW file name should be **"Your Lastname-817- HW-3"**. Also the same title should be used as the subject of your email. Please follow the formatting. This homework is due by **Azar 17th, 11:59 PM**. Also, you will have a face-to- face delivery, the time of which will be announced later.
Report what you write down should be your own words, analysis, reasons and results in approximately 20 pages with maximum size of 2MB (Try to include text result or reduce screenshot size included in your report.).
There will be a zero tolerance policy for cheating/copying HWs.

Part I: Theoretical

1. The Bank of Molvana adopted the following defense against phishing. The first time a user comes to the banks website, she enters her username and password as usual, and is given a choice between several pictures. The association between the username and the chosen picture is stored in the banks database. In all subsequent sessions, the user types in her username and expects to be shown a picture. Unless she sees the picture she chose during her first session, she does not type in her password. This helps users avoid giving their passwords to fake websites[1].

   (a) Describe a man-in-the-middle attack that allows a fake website to show the user her chosen picture. (Assume that this is not the users first session, i.e., she has already chosen the picture.)

   (b) Design a cookie-based defense for this anti-phishing scheme that prevents the man-in-the-middle attack you discovered in the previous part.

   (c) If every user of the banks website has a cookie identifying her to the bank, does this eliminate the need for passwords? Explain.

Part II: Practical

Honypot

Honeyd is a small daemon for simulating virtual hosts which are attractive for attackers. These hosts can be either configured to mimic different services or provide real services. The former is called a "low-interaction" honeypot while the latter is a "high-interaction" one. In this part, you are supposed to install Honeyd, a low interaction honeypot, in a VM and work with it.

(a) Where is the best location to deploy Honeyd software (e.g. behind firewall and in internal network, or in the DMZ, etc.)? Reason why this is the best location?

[1]This part of homework is retrieved from "https://www.cs.utexas.edu/ shmat/courses/cs361s"

(b) Honeyd uses different methods to log information. Explain each of them briefly.

(c) Use Honeyd to setup a virtual host with the following specifications:

i. Operating System : Windows XP SP1 Open Ports: 135 139 445 768 123 ethernet : 00:00:24:22:8c:12 dynamic ip

ii. Operating System : Linux Open Ports: 22 135 139 2045 ethernet : 00:00:24:22:8c:14 static ip 10.10.10.2

(d) Scan the Linux host using nmap and analyze the log information which honeyd provides .

(e) Run/emulate DNS services on Windows host which you have created . Try sending DNS requests to it and analyze the logs .

(f) Run/emulate FTP and SSH on Windows host which you have created. Use masquerading iptable rules to forward FTP and SSH requests which are sent to your machine towards the virtual host. Send FTP and SSH requests to your machine. These requests should be forwarded to Windows host. Analyze Honeyd logs and report your results.

Traffic Analysis

In this part of the homework, you are given a network traffic of a mobile device, captured from different activities of a user. Therefore, you should analyze the packets and answer the following questions:

(a) Analyze the traffic and report user's activities such as the websites the user vists, the apps that the user may have used, etc. You should specify the sender and receiver ip addresses, the protocols, the content and duration of each activity.

(b) The user has also used a message application for chatting with a friend , sending texts or music files. This application encrypts the data and you can not see the content. You are given the plain music files and texts that are likely to be found in their communications .

i. What are the ip addresses of the clients?

ii. Enumerate the number of packets, average size of packets in bytes and the time of each connection per client ? (By connection, means you should consider the packets when client A is texting client B or vice versa)

iii. What is the algorithems used for encrypting data? How secure is it?

iv. Can you define the music files being sent? What about texts?