Sharif University of Technology
Department of Computer Engineering

Advance Network Security
Instructor: Dr.AmirMahdi SadeghZadeh *16 Azar, 1402*

Homework 3[*]

1 Part One: Theorical

1.1 The Bank of Molvana

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 xbetween 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.

(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.

2 Part Two: Practical

2.1 Botnet

In the Homework2, you got familier with botnet topologies and some wellknown examples of it. Now, you should analyze a botnet traffic dump prepared in a pcap file and answer the following questions:

(a) What is the C&C server of this botnet?

(b) Based on communication streams, what type of commands and data were exchanged between clients and C&C server ?

(c) What is the attack type of this botnet.

(d) Find victims' IP addresses.

(e) How many packets are sent out by this botnet to each victim?

(f) Report the 5 top source port number who sent out most packets.

(g) Assume that the C&C server IP address is variable. now block the communication between client and C&C server with DPI (Deep Packet Inspection) technique

[*] Acknowledgement: This homework was orginally developed by Behnam Momeni

2.2 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?

(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.

3 HW Submission

Deliverables:

You should submit .pdf file containing answers to theorical questions , a detailed report for practical questions, with screenshots for Terminals to describe what you have done and what you have observed, as well as the program source code. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits.

Your report must be written in your own words to demonstrate your own analysis, reasoning, and obtained results. The use of ChatGPT or other generative AI technologies is not permitted. There will be a zero tolerance policy for cheating/copying HWs.

Finally, submit all of your answers in .zip file on the Quera course page with the following format: HW[HWNo]-[FamilyName]-[stdNo] .zip (For example, HW3-Hoseini-401234567.zip)