Network and Web Security

Exercise - Web-Based Malware Analysis*

February 26, 2024

In this exercise we practice the analysis of web-based malware. This is based on Question 4 part (b) of the 2017 exam. Before attempting this exercise, you are advised to review Modules 16 JavaScript and module 17 Browser Security, and to repeat the simpler malware analysis from the slides (code here). When you are ready, you should aim to complete sections (i) and (ii) in about 25 minutes, and section (iii), which was meant to be the most difficult, in about 20 minutes. Each section awarded approximately 6% of the total exam points, for a 3 hours exam with 3 questions.

Instructions

1. Open `kali-vm` and open a command shell. These instruction assume `kali-vm` has IP `10.6.66.64` (if not, change the address below).
2. Copy the file `/vol/co331/VMS/q4b-2017.zip`, unzip it, and **don't look inside the `q4b-2017` directory** that has just been created, to simulate the exam conditions, where the malware was served from a different host you had no access to.
3. Set up local domain name resolution by editing the file `/etc/hosts` (you need to be `root` or use `sudo` to do it) and adding the lines:

   ```
   10.6.66.64    www.lloyd5bank.com
   10.6.66.64    report.hit.e25rt.cc
   ```

   In the exam there was an external DNS server so you would not know about the existence of the second domain above, so just pretend you don't know it (as yet).
4. Serve the malware from `kali-vm`, on the standard HTTP port 80, by running
   `php -S 10.6.66.64:80 -t q4b-2017/`

Question 4

b Your startup implements a system to automatically classify the web pages pointed to by reported URLs. Yet, for some reason the URL `http://www.lloyd5bank.com/login.asp` fails to be classified automatically. You are tasked to analyse it in your pentesting environment.

i) Analyse the web page and identify what kind of attack it is trying to deploy: if you are on the right trail, you will discover a clearly marked flag that you need to report.

ii) Briefly describe what kind of vulnerability you think the attacker is trying to exploit, and whether or not the attack has been successful. Suggest a mitigation for this vulnerability.

iii) Continuing your analysis of the attack in part (b.i) above, find a way to send a message to the attacker that will signal that the attack has succeeded (if you manage, you will obtain a flag from the attacker in response).

*Sample answers will be released by Revision week.