|  |  |  |
| --- | --- | --- |
| Week | Malware Analysis Tools and Techniques | Duration |
| 7 | Examining Malicious Pages | 120 mins |

**Lesson Objectives**

Examine Malicious Pages either using the manual method or using FireBug.

Note: Copy the folder Week7 in REMnux. The folder contains 3 files:

1. Source.html
2. Strom.js
3. Script.html

# Steps to use FireBug in REMnux

1. To launch FireFox browser type “firefox &”
2. Click the “bug” toolbar icon on right and enable “On for All Web Pages” option.
3. Open the malicious page using “notepad” (notepad script.html &) and then add the “debugger ;” statement as the first line after the script tag. When FireBug sees this statement it will pause the scripts execution so that we can set the necessary brakpoints.
4. Once you have saved the modified script, launch FireFox and open it using File > Open File Menu (Ctrl+O).
5. Right-click on the appropriate statement eg.eval and then select “Set Breakpoint” in the FireBug pop-up menu.
6. Click F8 to continue running the script until it reaches your breakpoint.
7. FireBug will show the content of the defined varaible on the right of its window in the “Watch” pane.
8. Expand the variable you are interested using + and save the content (copy and Paste) in a “txt” file.