Lab 6: BeEF

In this lab, we are going to use a malicious program that allows an attacker to hook the browser of a vulnerable machine. The program called BeEF. The following list of software is required to run this lab:

- Metasploitable linux machine (Victim)
- Kali linux (attacker)
- BeEF (pre-install in Kali Linux)
- VBox
- A single virtual network that hosts both the victim and the attacker platforms

Lab requirements:

1. Both the victim and the kali linux must be connect to the internet
2. Start BeEF on kali linux (attacker) to obtain the web address that used to open the graphical user interface of BeEF and couple sample webpages that can be used to hook browsers
3. Open an internet browser on the attacker machine and surf to 127.0.0.1:3000/ui/panel to view the user interface
4. Login into BeEF with username and password “beef”
5. Open the test page and click on “Advanced version” as it looks like a real webpage.
6. On the victim machine (Metasploitable) open a browser and surf to the malicious demo webpage that BeEF creates.
7. Make sure that the victim machine is hooked by viewing it in the BeEF control panel:
8. Start surfing the web on the victim machine and use the following tools to gather information from the victim machine:
   a. Lunch the social engineer attack to capture user credential like Facebook account information
   b. Modify the content of a webpage in real time that the victim machine is currently on. You will need to change only two links on the original webpage.

Deliverables:

Submit a report describes each of the following:

- A list of all steps including screen shots that details your attack approaches.
- The list of visited webpages by the victim machine.
- Provide the list of users’ credentials that you captured when running BeEF.
- Provide a copy of the original HTML source code of a webpage visited by the victim machine.
- Provide a copy of the maliciously modified webpage and highlight all links that you modified during the attack.