ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Module 7. Exploitation using client-side attacks

Penetration testing course

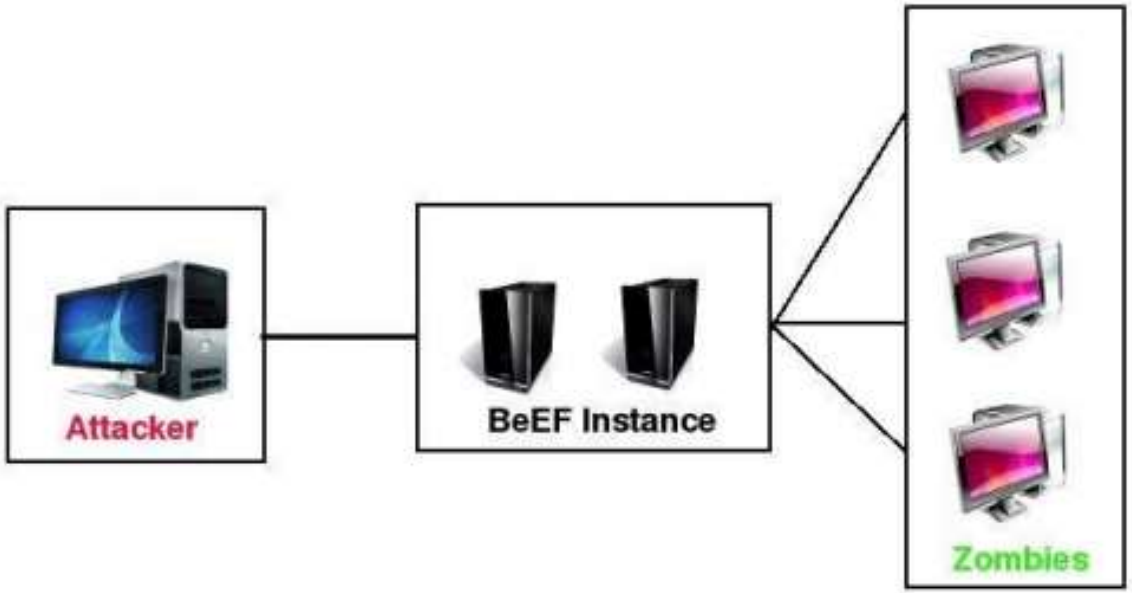
BeEF (The Browser Exploitation Framework)

- It is a penetration testing tool that focuses on the web browser.
- BeEF examines exploitability within the context of the one open door: the web browser.
- BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.

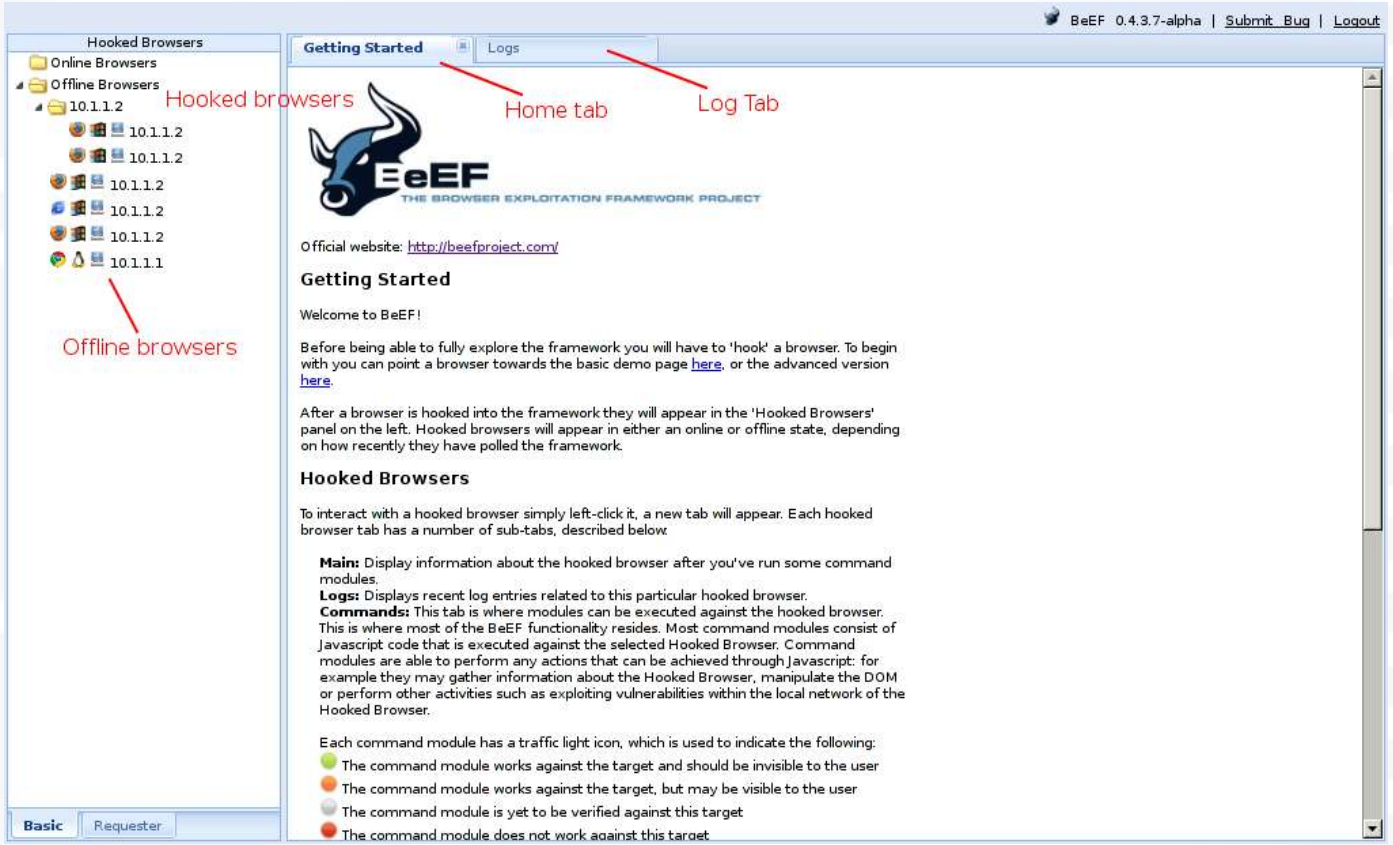
BeEF

- Open source penetration tool
- Tests and exploits Web and Browser-Based vulnerabilities
  - Use client-side attack vectors and leverages XSS
  - Hooks and fingerprints browsers
- BeEF server can issue the following commands:
  - Redirection of browser
  - Changing URLs
  - Dialog box generating on victim computer
  - Uploading of files to victim computer
  - …
- API integration with other tools
  - Integration with Metasploit and others

Attack scheme



BeeF user interface



BeEF commands for browser