Post-Exploitation

A compromised system may contain sensitive information, such as user data, access keys, credentials etc. It may then be possible to use this information to compromise other machines on the same network. The attacker can also turn the machine into a zombie computer and use it to perform attacks on other machines in a planned attack on a future date. The objective of this section is to teach students how to look for sensitive information on a machine, crack password protected files and perform the lateral movement on the network.

What will you learn?

- Using Metasploit modules to retrieve sensitive information from a compromised system
- Extracting valuable information from browser preferences data
- Compromising other machines on the same network

References:

1. Post Exploitation (http://www.pentest-standard.org/index.php/Post_Exploitation)
2. Pentesting with Metasploit (https://www.pentesteracademy.com/course?id=10)

Labs:

Metasploit Post Modules:

- Post Exploitation Lab I
  - Objective: Exploit the vulnerable file sharing service and use various Metasploit post modules to find more information about the system.
- Post Exploitation Lab II
  - Objective: Exploit the vulnerable file sharing service and use various Metasploit post modules to retrieve credentials present on the system.

Browser Forensics:

- Firefox: Logins and Passwords
  - Objective: Analyze Firefox preference data and enumerate saved logins and passwords.
- Firefox: History
  - Objective: Analyze Firefox preference data and enumerate saved history.
- Firefox: Cookies
  - Objective: Analyze Firefox preference data and enumerate cookies.
- Chrome: Bookmarks
  - Objective: Analyze Chrome preference data and enumerate bookmarks.
- Chrome:Cookies
  - Objective: Analyze Chrome preference data and enumerate cookies.

Lateral Movement:

- Internal Network I
  - Objective: Find information stored on the system and leverage it to compromise other systems on the network.

More labs for this topic are available under the Metasploit and Forensics section on AttackDefense.