GETTING STARTED
Tools of Trade

The infosec community has done a wonderful job creating a variety of open-source pentesting tools. Tools are available to enumerate web applications and gather the information that can be useful in identifying vulnerabilities and creating application/platform-specific payloads for attacks such as LFI and Command Injection. In this section, we will take a look at how to use popular open-source tools for reconnaissance and the automation of attacks.

What will you learn?

- Performing directory enumeration using various tools such as DirBuster, OpenDoor.
- Scanning web applications and identifying vulnerabilities.
- Exploiting the vulnerability using tools such as XSSer and SQLMap.
- Performing dictionary attacks on login forms and password protected directories.

References:

1. Gobuster (https://github.com/OJ/gobuster)
2. DirBuster (https://tools.kali.org/web-applications/dirbuster)
3. OpenDoor (https://github.com/stanislav-web/OpenDoor)
4. ZAProxy (https://www.zaproxy.org/)
5. Burp Suite (https://portswigger.net/burp)
6. THC Hydra (https://github.com/vanhauser-thc/thc-hydra)
7. SQLMap (http://sqlmap.org/)
8. Nikto (https://cirt.net/Nikto2)
9. XSSer (https://github.com/epsylon/xsser)

Labs:

- Directory Enumeration with Gobuster
  - Objective: Perform directory enumeration with Gobuster.
- Directory Enumeration with DirBuster
  - Objective: Perform directory enumeration with DirBuster.
- Directory Enumeration with OpenDoor
  - Objective: Perform directory enumeration with OpenDoor.
- Directory Enumeration with ZAProxy
  - Objective: Perform directory enumeration with ZAProxy.
- Directory Enumeration with Burp Suite
  - Objective: Perform directory enumeration with Burp Suite.
- Scanning Web Application with ZAProxy
  - Objective: Scan the web application with ZAProxy and identify the possible vulnerabilities.
- Scanning Web Application with Nikto
  - Objective: Scan the web application with Nikto and identify the possible vulnerabilities.
- SQL Injection with SQLMap
  - Objective: Perform a SQL Injection attack on the web application with SQLMap.
- XSS Attack with XSSer
  - Objective: Perform XSS Attack on the web application with XSSer.
- Passive Crawling with Burp Suite
  - Objective: Perform passive crawling on the web application with Burp Suite.
- Authenticated XSS Attack with XSSer
  - Objective: Perform authenticated XSS Attack on the web application with XSSer.
- Attacking HTTP Login Form with Hydra
  - Objective: Perform Dictionary Attack on the bWAPP login page using Hydra.