Assignment 1

Footprinting: Footprinting is the process of gathering information about a target system or network to create a profile or "footprint" of its infrastructure, services, and security posture. This information can include details about the organization's domain names, IP addresses, network topology, employee names, email addresses, and more. Footprinting techniques often involve passive information gathering through sources like search engines, social media, public databases, and company websites.

Reconnaissance: Reconnaissance, also known as "recon," is the active process of scanning and probing a target system or network to gather additional information beyond what is available through passive footprinting. Reconnaissance activities typically involve techniques such as network scanning, port scanning, banner grabbing, and vulnerability scanning to identify potential points of entry or weaknesses in the target's defenses. The goal of reconnaissance is to obtain detailed insights into the target's infrastructure, services, and security vulnerabilities to aid in further analysis or exploitation.

Step 1: Access Google by opening a web browser such as Chrome, Firefox, or Safari.

- In the search bar, which is typically located at the top of the browser window, paste the following URL: http://testphp.vulnweb.com/ and then press the "Enter" key on your keyboard. This action will take you to the specified website.

Step 2: Perform footprinting and reconnaissance on the provided website. Footprinting involves gathering information about the target system or network to identify potential vulnerabilities, while reconnaissance involves actively scanning and probing the target to gather more detailed information.

- You can use various tools and techniques such as WHOIS lookup, Google dorking, website analysis tools, and social engineering techniques to gather information about the target website.

Step 3: Use Nmap, a network scanning tool, to collect information about the target website. Nmap allows you to discover hosts and services on a computer network, thus providing valuable insights into the network topology and available services. With Nmap, you can scan for open ports, detect operating systems, and gather other network-related information.

Step 4: Document your findings. It's essential to record all the information you gather during the footprinting, reconnaissance, and Nmap scanning processes.

- This documentation helps in understanding the target environment, identifying potential vulnerabilities, and formulating an effective strategy for further analysis or penetration testing. You can create a detailed report containing the results of your scans, observations, and recommendations for mitigating any identified risks.