ASSIGNMENT - 1

KRISHNA SATHVIKA GANNI
4TH YEAR,B.TECH
RCEE
06-02-2024

FOOTPRINTING:

- ➔ Footprinting, also known as fingerprinting, is a methodology used by penetration testers, cybersecurity professionals, and even threat actors to gather information about a target organization to identify potential vulnerabilities.
- ➔ Footprinting is the first step in penetration testing. It is one of the best methods of finding vulnerabilities.
- ➔ The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners.
- ➔ This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.
- ➔ There are two types of Footprinting that can be used: active Footprinting and passive Footprinting.

RECONNAISSANCE:

- ➔ Reconnaissance, often referred to as 'cyber reconnaissance' or 'cyber intelligence gathering', is the process of collecting information about potential targets, vulnerabilities, and attack vectors.
- ➔ Reconnaissance refers to a set of processes and techniques, such as footprinting and scanning and enumeration, that are used to gather and covertly discover as much information as possible about a target system.
- ➔ Reconnaissance is an essential step in locating and stealing confidential information. In a proper recon, attackers would have access to detailed information.
- ➔ In this way, reconnaissance, in information security, is used for penetration testing. To gain information without actively engaging with the network, an attacker uses

recon to interact with the network’s open ports, running services, etc.

➔ The information it provides can help gain access to networks beyond the internet.

STEPS:

Step 1: **Access the Target Website Open a web browser (Chrome, Firefox, Safari, etc.).**

➔ In the address bar, paste the URL: http://testphp.vulnweb.com/ and press Enter.

Step 2: **Footprinting and Reconnaissance**

➔ **WHOIS Lookup:** Use tools like WHOIS to gather information about the domain registration, including the owner's contact details and registration date.

➔ **Google Dorking:** Utilize specific search queries on Google to find sensitive information, files, or vulnerabilities associated with the target website.

➔ **Website Analysis Tools:** Employ tools like BuiltWith or Wappalyzer to identify technologies, frameworks, and plugins used on the website.

➔ **Social Engineering:** Gather information through social media platforms or other online sources to learn about the organization, its employees, and potential vulnerabilities.

Step 3: **Network Scanning with Nmap Install Nmap if you haven't already (you can download it from https://nmap.org/).**

➔ Execute Nmap commands to scan the target website for open ports, services, and operating systems.

➔ Example command: nmap -A testphp.vulnweb.com

Step 4: **Documentation**

➔ Record all the information gathered during footprinting, reconnaissance, and Nmap scanning processes.

➔ Create a detailed report containing: Summary of findings Information about the target website (domain registration details, technologies used) Results of Nmap scans (open ports, services, OS detection) Observations and potential vulnerabilities Recommendations for mitigating identified risks