CYBER SECURITY

ASSIGNMENT 2

WHAT IS FOOTPRINTING AND RECONNAISSANCE

- Understanding the methods used by malicious individuals in the wide and constantly changing field of cybersecurity is essential for safeguarding sensitive data and preventing unauthorised access.
- Footprinting and reconnaissance are the two core tasks that each cyber attack is built upon. In order to find weaknesses and potential entry points, these pre-attack procedures entail acquiring data about a target system or network. Organisations may improve their defensive tactics and strengthen their cybersecurity posture by comprehensively understanding of the theories and techniques behind reconnaissance and footprinting.

WHAT IS FOOTPRINTING

- Footprinting is the process of identifying and understanding the security risks in an organisation. It involves gathering information about the target, both from publicly available sources and through more intrusive methods. This information helps build a profile of the organisation's security posture and identify vulnerabilities. The approach used depends on the desired information and level of access.

WHAT IS RECONNAISSANCE

- An important step in ethical hacking is reconnaissance, which includes leaving digital footprints. Data on the target system's network infrastructure, personnel information, and security rules are collected as part of this process. Finding potential attack routes and vulnerabilities is the aim of reconnaissance. Security policies, network specifics, employee contacts, and host information for vulnerability assessment are all pieces of information that are gathered while accomplishing this step.

TYPES OF FOOTPRINTING

- There are two types of footprinting. Active methods may include hacking or social engineering, while passive methods focus on publicly available data. Both types are based on how information is gathered:
- Passive Footprinting
- Active Footprinting

PASSIVE FOOTPRINTING

- In this type of footprinting, the attacker collects information about the target without directly interacting. It is useful for gathering undetected information. The attacker utilises publicly accessible data from online sources and analyses the target organisation's website. Valuable information can be obtained about customers, employees, history, and more.
- Passive footprinting methods offer additional options, including:
- Browsing the target's website
- Exploring the website to gather insights and potential vulnerabilities.
- Target monitoring using alert services
- Using monitoring tools to receive updates on changes or activities related to the target.
- Examining an employee's social media accounts
- Extracting information from publicly available profiles of individuals associated with the target.

ACTIVE FOOTPRINTING

- In active footprinting, the attacker directly interacts with the target to gather information. This approach increases the likelihood of the target detecting the activity. Methods used in active footprinting include human interaction, searching for digital files, email tracking, social engineering, performing WHOIS lookups, traceroutes, and more.
- Active footprinting techniques can be applied in various ways, such as:
- Traceroute analysis
- Tracing the network path to identify routers and potential vulnerabilities.
- Email tracking.
- Gathering information by tracking email interactions and analysing metadata.
- Whois lookup.
- Retrieving domain registration information to gather details about the target.