**Perform Reconnaissance**

**By: Long Trang**

**RECON METHOD AND TOOLS**

1. **Source: Artemis.org(Web search)**

**Method:** To initiate reconnaissance on the fictitious company Artemis, the initial step would be to conduct a comprehensive web search for the company's name and website. This approach will enable me to ascertain the company's online presence, including its website and social media profiles.

1. **Source: Pastebin**

**Method:** To safeguard sensitive company data, including credit card numbers, personal identifiable information of employees and customers, source code snippets exposing website functionality, network device configurations, critical employee names and roles, compromised Wi-Fi passwords, username and password dumps, and chat logs, one can gather intel and comb the web for any data breaches that have been publicly disclosed.

1. **Source: LinkedIn, Indeed, Monster, GlassDoor**

**Method:** Acquire intel on the latest and evolving IT/Security projects that are either planned for deployment or are still in the early stages of scouting for skilled technicians (engineers, cloud specialists, programmers) with specific IT-related expertise (programming languages, cloud providers, database administration, operating systems, etc.) Including summary of job description and function.

1. **Source: HaveIBeenPwned.com**

**Method:** Conduct surveillance to verify if any company emails, phone numbers, or passwords have already been exposed. Log all discovered credentials that could be leveraged as a potential hack or entry point.

1. **Source: LinkedIn Profile**

**Method:** Gather specific data pertaining to Artemis employees' contact details, job titles, professional networks, skill sets, and technology usage patterns. Analyze the company's security and IT personnel to identify recurring certifications and technology/security tools such as Cisco, AWS cloud, Microsoft Azure, Oracle, and so on. This will provide valuable insights into Artemis' current IT and security practices.

1. **Source: Youtube, Instagram, Twitter, Facebook, Tiktok**

**Method:** Collect relevant information on the employees of the target organization by examining their profiles on social networking sites. Record any details that could be useful in social engineering tactics or help in gaining a deeper understanding of the company's IT infrastructure.

1. **Source: Whois Lookup**

**Method:** Collect all pertinent information related to the target's IP address, including the name of the IP address space owner, registrant names, and the company's contact information, such as phone numbers and email addresses. This information can be utilized to create a comprehensive map of the target's organizational structure, as well as to gather personal information that may prove useful in later social engineering attacks.

1. **Source: Dumpster Diving and Scouting**

**Method:** Conduct surveillance on the critical IT infrastructure's operations center and physical security measures. Look for any potential points of entry such as open doors, and observe the accessibility of the database center, desktops, and other IT/security-related controls. Also, inspect trash bins and desks for any unattended sensitive material that has not been properly disposed of, as it may contain valuable information.

1. **Source: GitHub**

**Method:** Search for sensitive information that may have been leaked on Github. Use specific keywords and phrases relevant to the target company's IT infrastructure and practices, such as Oracle 12C, My SQL Password, Auth\_Token, Auth\_Key, AWS\_Key, and AWS\_SecretKey. This will aid in identifying any confidential data that may have been inadvertently exposed on the platform.

1. **Source: whatsmydns.net**

**Method:** Gather information on the target company's websites, data centers, and devices, including their respective IP addresses, IP address ranges, domain names, MX records (email), SRV records (VoIP), and Certificate Authority Authorization DNS records. This will provide insight into the organization's online presence and help identify potential attack surfaces.

1. **Source: Nmap, NetScanTools, and Fping.**

**Method:** Creating a visual representation of Artemis’s structure, including the location of hosts, firewalls, routers, and other devices. Scanning the target’s network for open ports, identify operating systems, and detect vulnerabilities. Perform ping sweeps, DNS lookups to identify the active hosts on the network and gather additional information about them.