Understanding Information Security Threats and Attack Vectors

---

- Information Security Attacks:

$$Attack = Motive(Goal) + Method + Vulnerability$$

  - Motive originates from the notion that the target system stores or processes something valuable; this signals that the system may be under threat of an attack.

- Top Information Security Attack Vectors:
  - Cloud Computing Attacks: Flaws in one client's application cloud allow attackers to access other clients' data.
  - Advanced Persistent Threats (APT): an attack focused on stealing information from the victim machine without the user's awareness.
  - Viruses and Worms: the most prevalent networking threats and can infect a network within seconds.
    - A virus is a malicious self-replicating program that produces a copy of itself by attaching it to another program, computer boot sector, or document.
    - A worm is a malicious program that replicates, executes, and spreads across network connections.
  - Ransomware: restricts access to the computer system's files and folders and demands an online ransom payment to the malware creator(s) to remove the restrictions.
  - Mobile Threats: Focus of attackers has shifted to mobile devices due to increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls.

- Botnet: a huge network of the compromised systems used by an intruder to perform various network attacks
- Insider Attack: an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorized access to the network.
- Phishing: the practice of sending an illegitimate email falsely claiming to be from a legitimate site to acquire a user's personal or account information
- Web Application Threats: Attackers target web applications to steal credentials, set up phishing sites, or acquire private information to threaten the performance of the website and hamper its security.
- Internet Of Things (IOT) Threats: Flaws in the IoT devices allow attackers remote access to the device to perform various attacks.

❖ Information Security Threat Categories:

- Network Threats:
  - As information travels from one system to the other through the communication channel, a malicious person might break into the communication channel and steal the information while traveling over the network.
  - Examples: Information Gathering - Sniffing and Eavesdropping - Spoofing - Man-In-The-Middle - DNS and ARP Poisoning - Password-based - DOS - Compromised-Key - Firewall and IDS.
- Host Threats:
  - Target a particular system on which valuable information resides; attackers try to breach the security of the information system resource.
  - Examples: Footprinting - Profiling - Arbitrary code execution - Unauthorized access - Privilege Escalation - Backdoor Attacks - Physical security threats.
- Application Threats:
  - can be vulnerable if proper security measures are not taken while developing, deploying, and maintaining them. Attackers exploit the vulnerabilities present in an application to steal or destroy data.

        - Examples: Improper Data/Input Validation - Authentication and Authorization attacks - Improper Error Handling / Exception Management - Information disclosure.

- Threat: undesired event that attempts to access, exfiltrate, manipulate, or damagethe integrity, confidentiality, security, and availability of an organization's resource.
- Threat Actor: a person or entity responsible for harmful incidents or with the potential to impact the security of an organization's network.
    - Script Kiddies; An unskilled hacker who compromises a system by running scripts, tools, and software developed by real hackers
    - Organized Hackers: Professional hackers seeking to attack a system for profit.
    - Hacktivists: Individuals who promote a political agenda by hacking, especially by defacing or disabling websites.
    - State-sponsored Attackers: Individuals employed by the government to penetrate and gain top-secret information and/or to damage the information systems of other governments.
    - Insider Attackers: Threat originating from people within the organization such as disgruntled employees, terminated employees, and undertrained staff.
    - Cyber Terrorists: Individuals with a wide range of skills, motivated by religious or political beliefs to create fear of large-scale disruption of computer networks.
    - Recreational Hackers: Hackers who hack to learn and exploreby exploiting or manipulating technology.
    - Suicide Hackers: Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment.
    - Industrial Spies: Individuals who try to attack companies for commercial purposes.

- Information Warfare (InfoWar): the use of information and communication technologies (ICT) as competitive advantages over an opponent
  - Command-and-Control Warfare (C2 Warfare): the impact an attacker possesses over a compromised system or network that they control.
  - Intelligence-based Warfare: a sensor-based technology that directly corrupts technological systems. consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space.
  - Electronic Warfare: uses radio-electronic and cryptographic techniques to degrade communication.
  - Psychological Warfare: the use of various techniques such as propaganda and terror to demoralize one's adversary to succeed in battle.
  - Hacker Warfare: the purpose of this type of warfare can vary from shutdown of systems, data errors, theft of information, theft of services, system monitoring, false messaging, and access to data.
  - Economic Warfare: can affect the economy of a business or nation by blocking the flow of information.
  - Cyber Warfare: can affect the economy of a business or nation by blocking the flow of information. It is the broadest of all information warfare and includes information terrorism, semantic attacks (similar to hacker warfare, but instead of harming a system, it takes the system over while the system is still perceived as operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).
- Information Warfare Strategies:
  - Defensive Information Warfare: refers to all strategies and actions for security professionals and incident responders to defend their organization and its ICT assets from cyber attackers.
  - Offensive Information Warfare: refers to information warfare that involves attacks against ICT assets of an opponent, to compromise the target's assets.

Created by: Abdelrahim Alsadiq