- Vulnerability: A weakness that can be exploited by a threat.
- Exposure: A mistake that can be exploited by a threat.
- Exploit: A way of taking advantage of a vulnerability.
- Zero-day Exploit: An exploit that was previously unknown.
- Vulnerability Management: The process of finding and patching vulnerabilities.
- **Vulnerability Management Steps:**
  - Identify Vulnerabilities.
  - Consider Potential Exploits.
  - Prepare Defenses against threats.
  - Evaluate those defenses.
- Common Vulnerabilities and Exposures List (CVE List): An openly accessible dictionary of known vulnerabilities and exposures.
- CVE Numbering Authority (CNA): An organization that volunteers to analyze and distribute information on eligible CVEs.
- **CVE List Criteria:**
  - Vulnerabilities must be independent of other issues.
  - Vulnerabilities must only affect one codebase (source code).
  - Vulnerabilities must be recognized as a potential security risk.
  - Vulnerabilities must be submitted with supporting evidence.
- MITRE: A collection of non-profit research and development centers.
- Common Vulnerability Scoring System (CVSS): A measurement system that scores the severity of a vulnerability.

- Open Worldwide Application Security Project (OWASP): An open platform that security professionals from around the world use to share information, tools, and events that are focused on securing the web.
- **These are the most regularly listed vulnerabilities that appear in OWASP Top 10 rankings to know about:**
    - Broken access control.
    - Cryptographic failures.
    - Injection.
    - Insecure design.
    - Security misconfiguration.
    - Vulnerable and outdated components.
    - Identification and authentication failures.
    - Software and data integrity failures.
    - Security logging and monitoring failures.
    - Server-side request forgery.

- **Defense in depth strategy layers:**
  - **Perimeter Layer:**
    - A user authentication layer that filters external access.
    - Only allow access to trusted partners to reach the next layer of defense.
    - Examples: username and passwords.
  - **Network Layer:**
    - More closely aligned with authorization.
    - Made up of firewalls, etc.
  - **Endpoint Layer:**
    - Endpoints: devices that have access on a network.
    - Examples: antivirus software.
  - **Application Layer:**
    - Includes all the interfaces that are used to interact with technology.
    - Security measures are programmed as part of an application.
    - Example: Multi-factor Authentication (MFA).
  - **Data Layer:**
    - Has the critical data that must be protected, such as PII.
    - Assets classification is important security control here.

- Vulnerability Assessment: the internal review process of an organization's security systems.
- **Vulnerability Assessment Process:**
  - Identification.
  - Vulnerability analysis.
  - Risk assessment.
  - Remediation.
- Vulnerability Scanner: A software that automatically compares known vulnerabilities and exposures against the technologies on the network.
- **Scan Types:**
  - **External vs. Internal:**
    - External: test the perimeter layer outside of the internal network.
    - Internal: start from the opposite end by examining an organization's internal systems.
  - **Authenticated vs. Unauthenticated:**
    - Authenticated: might test a system by logging in with a real user account or even with an admin account.
    - Unauthenticated: simulate external threat actors that do not have access to your business resources.
  - **Limited vs. Comprehensive:**
    - Limited: analyze particular devices on a network, like searching for misconfigurations on a firewall.
    - Comprehensive: all devices connected to a network. This includes operating systems, user databases, and more.

- Penetration Testing: a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.
- **Penetration Testing Strategies:**
  - **Open-box testing:**
    - When the tester has the same privileged access that an internal developer.
    - Also called internal, full knowledge, white-box, and clear-box penetration testing.
  - **Closed-box testing:**
    - When the tester has little to no access to internal systems, similar to a malicious hacker.
    - Also called external, black-box, or zero knowledge penetration testing.
  - **Partial knowledge testing:**
    - When the tester has limited access and knowledge of an internal system.
    - Also known as gray-box testing.
- Proactive simulations: assume the role of an attacker by exploiting vulnerabilities and breaking through defenses. This is sometimes called a red team exercise.
- Reactive simulations: assume the role of a defender responding to an attack. This is sometimes called a blue team exercise.

- Attack Vector: the pathways that attackers use to penetrate security defenses.
- **Practicing attacker mindset:**
    - Identify the target
    - Determine how the target can be accessed.
    - Evaluate attack vectors that can be exploited.
    - Find the tools and methods of attack.
- **Defending attack vectors:**
    - Educating users.
    - Applying the principle of least privilege.
    - Using the right security controls and tools.
    - Building a diverse security team.

Created By: Abdelrahim Alsadiq