Overview of Vulnerability Management

- Vulnerability management: a proactive approach designed to identify, classify, and mitigate vulnerabilities.
- Vulnerability: the existence of a weakness, whether in design or implementation, that when exploited by attackers leads to an unexpected and undesirable event compromising the security of the system
- Vulnerability research: the process of discovering vulnerabilities and design flaws that will open a network, operating system, or applications to attack or misuse.
- Security Experts and Vulnerability Scanners classify vulnerabilities by:
  - Security level (low, medium, or high).
  - Exploit range (local or remote).
- Common Vulnerability Scoring System (CVSS): a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- Vulnerability Classification:
  - Misconfigurations: the most common vulnerability mainly caused by human error, and allows attackers to gain unauthorized access to a system
  - Default Installations: Not changing the default settings while deploying the software or hardware allows the attacker to guess the settings and break into the systems.
  - Buffer Overflows: attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer.
  - Unpatched Servers: As servers serve as a hub for the network, unpatched servers can also serve attackers as an entry point into it.
  - Design Flaws: such as incorrect encryption or poor validation of data constitute logical flaws in the functionality of a system that are exploited by attackers to bypass detection mechanisms and acquire access to secure systems.

  - Operating System Flaws: applications such as Trojans, worms, and viruses pose threats. These attacks are performed using malicious code, scripts, or unwanted software, which result in loss of sensitive information and loss of control of computer operations.
  - Application Flaws: vulnerabilities in applications that are exploited by attackers. Applications should be secured using validation and authorization requirements for users.
  - Open Services: Open ports and services may lead to loss of data, enable DoS attacks, and allow attackers to perform further attacks on other connected devices.
  - Default Passwords: users may forget to update the passwords and continue using the default passwords, making devices and systems vulnerable to various attacks, such as brute-force and dictionary attacks.
- Vulnerability Assessment: an examination of the ability of a system or application, including current security procedures and controls, to withstand assault.
- Types of Vulnerability Assessment:
  - Active Assessment: uses network scanners to scan the network to identify the hosts, services, and vulnerabilities present in that network. They have the capability to reduce the intrusiveness of the checks they perform.
  - Passive Assessment: sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. They also provide a list of the users who are currently using the network.
  - External Assessment: assess the network from a hacker's point of view to find out what exploits and vulnerabilities are accessible to the outside world.
  - Internal Assessment: involves scrutinizing the internal network to find exploits and vulnerabilities.
  - Application Assessments: focuses on transactional web applications, traditional client-server applications, and hybrid systems. It analyzes all elements of an application infrastructure, including deployment and communication within the client and server.
  - Wireless Network Assessments: determines the vulnerabilities in an organization's wireless networks.

- Vulnerability Management Life-Cycle:
  - Baseline Creation: critical assets are identified and prioritized to create a good baseline for vulnerability management.
  - Vulnerability Assessment: the security analyst identifies the known vulnerabilities in the organizational infrastructure.
  - Risk Assessment: summarizes the vulnerability and risk level identified for each of the selected assets, whether high, moderate, or low.
  - Remediation: the process of reducing the severity of vulnerabilities.
  - Verification: provides clear visibility into the firm and allows the security team to check whether all the previous phases are perfectly applied and employed.
  - Monitoring: Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.