**Vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack.**

**🡺 Vulnerability Research**

Vulnerability research is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaws that will expose an operating system and its applications to exploit, attack, or misuse.

**Security experts and vulnerability scanners classify vulnerabilities by:**

* Severity level (low, medium, or high)
* Exploit range (local or remote)

**🡺 Vulnerability Assessment**

vulnerability assessment is an in-depth examination of the ability of a system or application, including current security procedures and controls, to withstand exploitation. It scans networks for known security weaknesses, and recognizes, measures, and classifies security vulnerabilities in computer systems, networks, and communication channels. It identifies, quantifies, and ranks possible vulnerabilities to threats in a system.

**A vulnerability assessment may be used to:**

* Identify weaknesses that could be exploited
* Predict the effectiveness of additional security measures in protecting information resources from attack

Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

**There are two approaches to network vulnerability scanning:**

* **Active Scanning:** The attacker interacts directly with the target network to find vulnerabilities.
* **Passive Scanning:** The attacker tries to find vulnerabilities without directly interacting with the target network.

Attackers scan for vulnerabilities using tools such as Nessus, Qualys, GFI LanGuard, and OpenVAS. Vulnerability scanning enables an attacker to identify network vulnerabilities, open ports and running services, application and services configuration errors, and application and service vulnerabilities.

**🡺 Vulnerability Scoring Systems and Databases**

Vulnerability scoring systems and vulnerability databases are used by security analysts to rank information system vulnerabilities and to provide a composite score of the overall severity and risk associated with identified vulnerabilities. Vulnerability databases collect and maintain information about various vulnerabilities present in information systems

**Common Vulnerability Scoring System (CVSS)**

VSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Two common uses of CVSS are prioritizing vulnerability remediation activities and calculating the severity of vulnerabilities discovered on one’s systems. CVSS helps capture the principal characteristics of a vulnerability and produce a numerical score to reflect its severity.

**CVSS assessment consists of three metrics for measuring vulnerabilities:**

* Base Metric: Represents the inherent qualities of a vulnerability
* Temporal Metric: Represents the features that continue to change during the lifetime of the vulnerability.
* Environmental Metric: Represents vulnerabilities that are based on a particular environment or implementation.

**Common Vulnerabilities and Exposures (CVE)**

CVE is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. CVE provides a baseline for tool evaluation and enables data exchange for cybersecurity automation. CVE IDs provide a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization’s needs.

* One identifier for one vulnerability or exposure
* A dictionary rather than a database

**National Vulnerability Database (NVD)**

The NVD is the U.S. government repository of standards-based vulnerability management data. It uses the Security Content Automation Protocol (SCAP). The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics. The NVD performs an analysis on CVEs that have been published to the CVE Dictionary. The NVD does not actively perform vulnerability testing; it relies on vendors, third party security researchers, and vulnerability coordinators to provide information that is used to assign these attributes.

**Common Weakness Enumeration (CWE)**

Common Weakness Enumeration (CWE) is a category system for software vulnerabilities and weaknesses. It is sponsored by the National Cybersecurity FFRDC, which is owned by The MITRE Corporation, with support from US-CERT and the National Cyber Security Division of the U.S. Department of Homeland Security. It also has an advanced search technique where attackers can search and view weaknesses based on research concepts, development concepts, and architectural concepts.

**🡺 Vulnerability-Management Life Cycle**

The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. This includes defining the risk posture and policies for an organization, creating a complete asset list of systems, scanning and assessing the environment for vulnerabilities and exposures, and taking action to mitigate the vulnerabilities that are identified.

**The phases involved in vulnerability management are:**

* **Identify Assets and Create a Baseline:** This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration of each system in order to develop and maintain a system baseline. This is considered as Pre-Assessment phase.
* **Vulnerability Scan:** Security team perform scan to know vulnerabilities present or not. Vulnerability scans can also be performed on applicable compliance templates to assess the organization’s Infrastructure weaknesses against the respective compliance guidelines. The ultimate goal of vulnerability scanning is to scan, examine, evaluate, and report the vulnerabilities in the organization’s information system. It comes under vulnerability Assessment phase
* **Risk Assessment:** The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. This step onwards all steps comes under Post Assessment Phase
* **Remediation:** Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities.
* **Verification:** The security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets.
* **Monitor:** Organizations need to performed regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.

**🡺 Vulnerability Classification**

* **Misconfiguration:** It is the most common vulnerability and is mainly caused by human error, which allows attackers to gain unauthorized access to the system.
* **Default installations:** They are usually user-friendly. Failing to change the default settings while deploying the software or hardware allows the attacker to guess the settings to break into the system.
* **Buffer overflows:** They are common software vulnerabilities that happen due to coding errors that allow attackers to gain access to the target system. In a buffer overflow attack, the attackers undermine the functioning of programs and try to take control of the system by writing content beyond the allocated size of the buffer. Insufficient bounds checking in the program is the root cause.
* **Unpatched Servers:** Organizations run unpatched and misconfigured servers that compromise the security and integrity of the data in their system. Hackers look out for these vulnerabilities in the servers and exploit them. As these unpatched servers are a hub for the attackers, they serve as an entry point into the network.
* **Design vulnerabilities** such as incorrect encryption or the poor validation of data refer to logical flaws in the functionality of the system that attackers exploit to bypass the detection mechanism and acquire access to a secure system.
* **Operating System Flaws:** Due to vulnerabilities in the operating systems, applications such as trojans, worms, and viruses pose threats. These attacks use malicious code, script, or unwanted software, which results in the loss of sensitive information and control of computer operations.
* **Application Flaws:** Flawed applications pose security threats such as data tampering and unauthorized access to configuration stores. If the applications are not secured, sensitive information may be lost or corrupted.
* **Open ports and services** may lead to the loss of data or DoS attacks and allow attackers to perform further attacks on other connected devices.
* **Default Passwords**

**🡺 Types of Vulnerability Assessment**

* **Active Assessment:** It is a type of vulnerability assessment that uses network scanners to identify the hosts, services, and vulnerabilities present in a network. Active network scanners can reduce the intrusiveness of the checks they perform.
* **Passive Assessment:** It sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.
* **External Assessment:** It examines the network from a hacker’s point of view to identify exploits and vulnerabilities accessible to the outside world. An external assessment estimates the threat of network security attacks from outside the organization.
* **Internal Assessment:** It examines the internal network to find exploits and vulnerabilities.
* **Host-based assessments:** It is a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise.
* **Network-based Assessment:** These assessments discover network resources and map the ports and services running to various areas on the network. It evaluates the organization’s system for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption. Network assessment professionals use firewalls and network scanners, such as Nessus. It helps organizations determine how systems are vulnerable to Internet and intranet attacks
* **Application Assessment**: It analyzes all elements of an application infrastructure, including deployment and communication within the client and server. This type of assessment tests the webserver infrastructure for any misconfiguration, outdated content, or known vulnerabilities.
* **Database Assessment**: These assessments mainly concentrate on testing various database technologies like MYSQL, MSSQL, ORACLE, and POSTGRESQL to identify data exposure or injection type vulnerabilities.
* **Wireless Network Assessment**: This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization’s perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys.
* **Distributed Assessment**: This type of assessment, employed by organizations that possess assets like servers and clients at different locations, involves simultaneously assessing the distributed organization assets, such as client and server applications, using appropriate synchronization techniques.
* **Credential Assessment**: This type of assessment is challenging since it is highly unclear who owns particular assets in large enterprises, and even when the ethical hacker identifies the actual owners of the assets, accessing the credentials of these assets is highly tricky since the asset owners generally do not share such confidential information.
* **Non-Credential Assessment:** This type of assessment generates a brief report regarding vulnerabilities; however, it is not reliable because it does not provide deeper insight into the OS and application vulnerabilities that are not exposed by the host to the network. This assessment is also incapable of detecting the vulnerabilities that are potentially covered by firewalls.
* **Manual Assessment:** In this type of assessment attacker manually rank the vulnerabilities and score them by referring to vulnerability scoring standards like CVSS and vulnerability databases like CVE and CWE.
* **Automated Assessment:** The ethical hacker does not perform footprinting and network scanning. They employ automated tools that can perform all such activities and are also capable of identifying weaknesses and CVSS scores, acquiring critical CVE/CWE information related to the vulnerability.

**🡺 Vulnerability Assessment Solutions**

* **Product-Based Solutions:** They are installed either on a private or non-routable space or in the Internet-addressable portion of an organization’s network. If they are installed on a private network, they cannot always detect outside attacks.
* **Service-Based Solutions:** Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can audit the network from the outside.
* **Tree-Based Assessment:** In a tree-based assessment, the auditor selects different strategies for each machine or component of the information system. This approach relies on the administrator to provide a starting piece of intelligence, and then to start scanning continuously without incorporating any information found at the time of scanning.
* **Inference-**Based Assessment: In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

**Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:**

* **Locating Nodes:** Locating live hosts in the target network
* **Performing service and OS discovery on them:** Enumerate the open ports and services along with the operating system on the target systems.
* **Testing those services and OS for known vulnerabilities**

**🡺 Types of Vulnerability Assessment Tools**

* **Host-Based Vulnerability Assessment Tools:** The host-based scanning tools are appropriate for servers that run various applications, such as the Web, critical files, databases, directories, and remote accesses. A host-based vulnerability assessment tool identifies the OS running on a particular host computer and tests it for known deficiencies. It also searches for common applications and services.
* **Depth Assessment Tools:** Depth assessment tools are used to discover and identify previously unknown vulnerabilities in a system. Generally, tools such as fuzzers, which provide arbitrary input to a system’s interface, are used to identify vulnerabilities to an unstable depth.
* **Application-Layer Vulnerability Assessment Tools:** Application-layer vulnerability assessment tools are designed to serve the needs of all kinds of operating system types and applications. The network vulnerability information is updated regularly into the tools. Application-layer vulnerability assessment tools are directed towards web servers or databases.
* **Scope Assessment Tools:** These tools provide standard controls and a reporting interface that allows the user to select a suitable scan. These tools generate a standard report based on the information found.
* **Active & Passive Tools:** Active scanners perform vulnerability checks on the network functions that consume resources on the network. The main advantage of the active scanner is that the system administrator or IT manager has good control of the timing and the parameters of vulnerability scans. Passive Scanners only observe system data and perform data processing on a separate analysis machine. They first receive system data that provide complete information on the processes that are running and then assesses that data against a set of rules.
* **Location & Data Examination Tools:**
* Network-Based Scanners
* Agent-Based Scanners
* Proxy Scanners
* Cluster Scanners

**🡺 Vulnerability Assessment Tools**

* **Qualys VM** is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them.

Features:

* Agent-based detectionConstant monitoring and alerts
* Comprehensive coverage and visibility
* VM for the perimeter-less worldDiscover forgotten devices and organize the host assets
* Scan for vulnerabilities everywhere, accurately and efficiently
* Identify and prioritize risks
* Remediate vulnerabilities
* **Nessus Professional** is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment.

Features:

* High-speed asset discovery
* Vulnerability assessment
* Malware and Botnet detection
* Configuration and compliance auditing
* Scanning and auditing virtualized and cloud platforms
* **GFI LanGuard** scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort.

Features:

* Patch management for operating systems and third-party applications
* Vulnerability assessment
* A Web reporting console
* Track latest vulnerabilities and missing updates
* Integration with security applications
* Network device vulnerability checks
* Network and software auditing
* Support for virtual environments

**🡺 Vulnerability Assessment Report**

The vulnerability assessment report discloses the risks that are detected through scanning the network. Tools such as Nessus, GFI LanGuard, and Qualys Vulnerability Management are used for vulnerability assessment. These tools provide a comprehensive assessment report in a specified format. The report alerts the organization to possible attacks and suggests countermeasures.

The report provides details of all the possible vulnerabilities with regard to the company’s security policies. The vulnerabilities are categorized based on severity into three levels: High, Medium, and Low risk.

High-risk vulnerabilities are those that might allow unauthorized access to the network. These vulnerabilities must be rectified immediately before the network is compromised. The report describes different kinds of attacks that are possible given the organization’s set of operating systems, network components, and protocols.