Chapter 5

Vulnerability Analysis

Theory

Vulnerability

A bug or flaw or a state of being exposed which leads to a critical hacking attack from the Hacker is called Vulnerability.

Vulnerability Research

It is the process by which security flaws in technology are identified. Vulnerability research does not always involve reverse engineering, code analysis, etc. Performing vulnerability research against technology pre-release enables technology vendors to provide their customers with higher quality products and higher levels of trust and security.

List of vulnerability research websites

- securityfocus.com
- vulnerability-lab.com
- us-cert.gov
- packetstormsecurity.com
- nvd.nist.gov
- cvedetails.com

Vulnerability Analysis

Vulnerability analysis is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications or network infrastructure. This phase allows the organization to perform security assessment with the necessary knowledge, awareness and risk background to understand the threats and react appropriately.

Attackers perform vulnerability analysis to identify security loopholes in the target organization's network or communication infrastructure. Attackers take advantage of identified vulnerabilities to perform further exploitation of that target network.

The vulnerability scanner (software) compares details about the target attack surface to a database of information about known security vulnerabilities in services and ports, anomalies in packet construction, and potential paths to exploitable programs or scripts.

Objectives

- Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
- Document the vulnerabilities so that the developers and networks administrators can easily identify and reproduce the findings.
- Create guidance to assist network administrators and developers with remediating the identified vulnerabilities

Common types of Vulnerabilities

- Missing data encryption
- SQL injection
- Buffer-overflow
- Missing authentication for critical functions
- Missing authorization
- Unrestricted upload of dangerous file types
- Cross-site request forgery
- Download of codes without integrity checks
- Weak passwords
- Path/Directory traversal

List of network vulnerability scanners

- Nessus
- GFI LanGuard - Scans both Hardware & Software Vulnerabilities.
- Qualys guard - Works both on LAN & WAN
- Saint
- Nexpose - Paid and free solution available from Offensive security
- Core impact - Scanner and Exploit framework
- OpenVAS

Types of Vulnerability Assessment Reports

- Technical Report - Includes detailed description related to vulnerabilities found on the target computer(s)
- Non-Technical Report - Brief report on vulnerabilities found on the target computer(s). This report includes graphs and charts that are easy to understand the risk.

CVE (Common Vulnerabilities and Exposures)

CVE is a dictionary of standardized identifiers for common software vulnerabilities and exposures. CVE IDs, i.e., CVE-2018-1002100 which are assigned by CVE Numbering Authorities from around the world, ensures confidence when used to share information about a unique software or firmware vulnerability, provides a baseline for tool evaluation, and enables data exchange. CVE IDs act as a benchmark for evaluating security services

CVSS (Common Vulnerability Scoring System)

CVSS is a published standard that provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities. CVSS assessment consists of three metrics for measuring vulnerabilities

1. **Base Metrics:** It represents the inherent qualities of a vulnerability
2. **Temporal Metrics:** It represents the features that keep on changing during the lifetime of a vulnerability.
3. **Environmental Metrics:** It represents the vulnerabilities that are based on a particular environment or implementation.

Each metrics sets a score from 1-10, ten being the most severe. CVSS score is calculated and generated by a vector string, which represents the numerical score for each group in the form of a block of text. CVSS calculator is developed to rank the security vulnerabilities and provide the user with overall severity and risk related to the vulnerability.