Vulnerability Assessments

Vulnerability Assessment (VA) Definition

NIST SP 800-53 Rev. 4 Definition

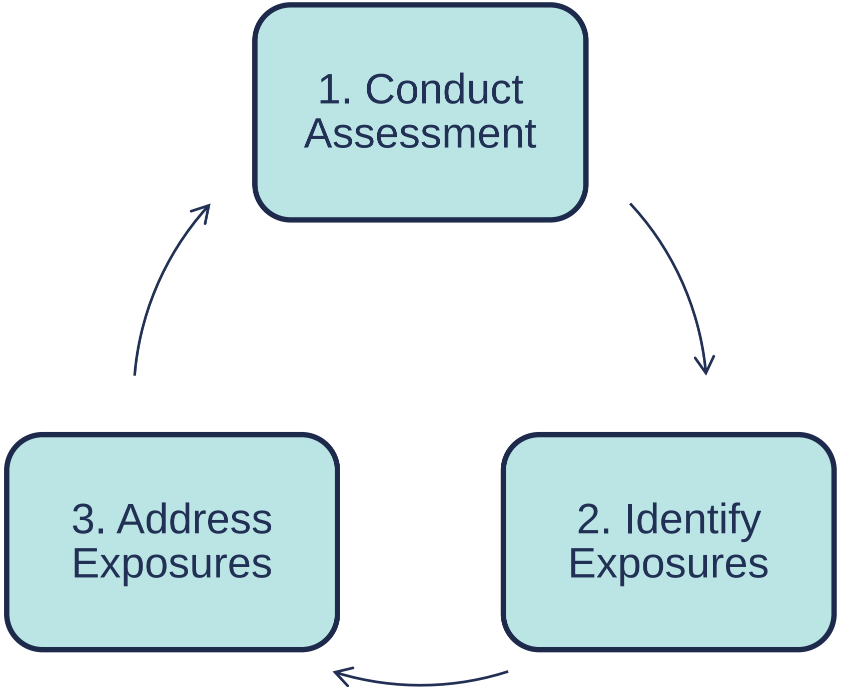
Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Short Definition

Performing an assessment to **identify vulnerabilities** that **could potentially be exploited**.

INSTRUCTOR
ALTON

Three Phase Cyclical VA Procedure (SANS)



A More Detailed Look at the VA

1. Planning
    - The first step is planning the scope of your VA, determining what systems and data will be scanned.
2. Scanning
    - The next step is to perform the VA scan with tools such as NMAP and Nessus.
3. Analysis
    - The next step is to analyze the results of your VA, reviewing identified vulnerabilities and their potential impact via a risk assessment process.
4. Remediation
    - Based on your risk assessment, prioritize and remediate identified vulnerabilities with appropriate control measures.
5. Repeat
    - Perform scans on a ongoing regular basis to identify new vulnerabilities.

Penetration Testing

Penetration Testing (Pen Test) Definition

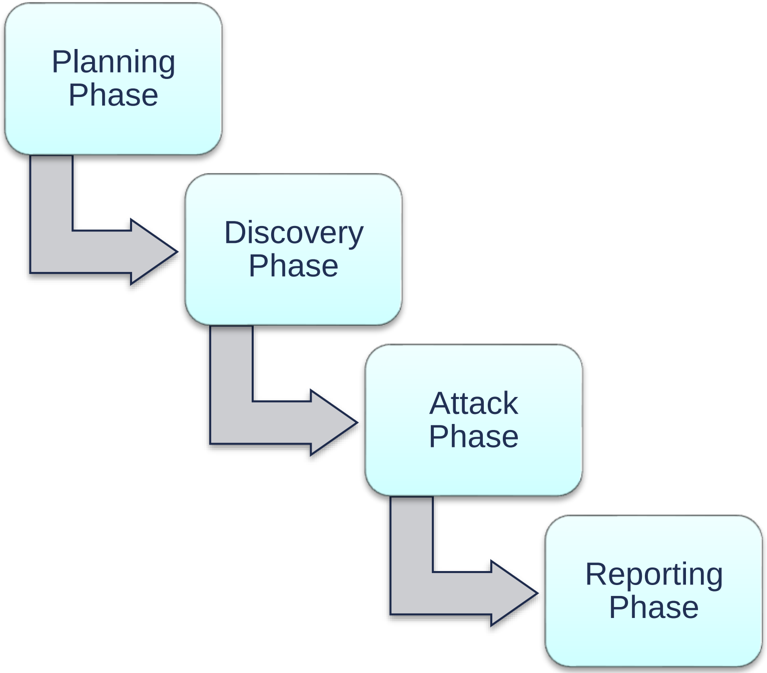
NIST SP 800-53 Rev. 4 Definition

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

Short Definition

Performing a simulated attack on a network and its information systems at the request of an organization to determine what vulnerabilities can actually be exploited.

The Pen Test Process



Types of Pen Tests

Type	Details
Black Box	The pen testers are placed in the role of a hacker, having no internal knowledge of the target network and systems.
Gray Box	The pen testers are provided some internal knowledge but not all information regarding the target network and systems.
White Box	This is the exact opposite of the black box test. Pen testers have full insider knowledge of the target network and systems.

Notes on Pen Tests

- Clearly defined rules of engagement must be agreed upon.
- Pen tests can be performed in-house or by an outside 3rd party vendor.
- Pen tests can be quite disruptive and “break things.”

Security Assessments

Security Assessments

- A comprehensive approach to assessing an organization’s security posture.
- Has a broad scope:
    - Policies and Procedures
    - Change and Configuration Management
    - Network Architectural Reviews
    - Vulnerability Assessments
    - Penetration Tests
    - Security Audits