

Introduction to Security Assessment and Testing

Introduction to Security Assessment and Testing

Purpose: Provide a clear, organized overview of why and how organizations evaluate the security of their systems, applications, and networks.

1. Why Perform Security Assessments?

Goal	Description
Identify Vulnerabilities	Discover weaknesses before attackers do.
Validate Controls	Confirm that existing security measures work as intended.
Compliance	Meet regulatory (e.g., PCI?DSS, GDPR, HIPAA) and contractual requirements.
Risk Management	Quantify risk to prioritize remediation and allocate resources.
Continuous Improvement	Feed findings back into the security development lifecycle (SDLC).

2. Core Concepts & Terminology

Term	Meaning
Asset	Anything of value that needs protection (data, hardware, services).
Threat	Potential cause of an unwanted incident (e.g., malware, insider).
Vulnerability	A flaw that can be exploited to compromise an asset.
Risk	Likelihood × Impact of a threat exploiting a vulnerability.
Control	Safeguard (technical, administrative, or physical) that mitigates risk.
Assurance	Confidence that controls are effective, often proven through testing.
Scope	Boundaries of the assessment (systems, networks, applications, time frame).
False Positive / Negative	Incorrectly reported finding vs. missed real issue.

3. Types of Security Assessments

Introduction to Security Assessment and Testing

Assessment	Primary Focus	Typical Techniques
Vulnerability Assessment (VA)	Broad identification of known weaknesses.	Automated scanners, credentialed scans, CVE mapping.
Penetration Testing (Pen? Test)	Exploitation of vulnerabilities to demonstrate impact.	Manual exploitation, social engineering, post? exploitation.
Red Team Exercise	Full?scale, realistic adversary simulation.	Multi?vector attacks, persistence, lateral movement, exfiltration.
Blue Team Review	Defensive detection and response capability.	Log analysis, SIEM tuning, incident response drills.
Purple Team Collaboration	Joint Red/Blue activities to improve detection and mitigation.	Real?time threat hunting, feedback loops.
Security Architecture Review	Evaluation of design and configuration.	Threat modeling, design walkthroughs, policy checks.
Code Review / Static Application Security Testing (SAST)	Source?code level weaknesses.	Manual review, automated static analysis tools.
Dynamic Application Security Testing (DAST)	Runtime behavior of applications.	Black?box testing, fuzzing, API testing.
Compliance Audits	Alignment with standards/regulations.	Checklist assessments, evidence collection.

4. Assessment Methodologies

Phase	Activities	Deliverables
1. Planning & Scoping	Define objectives, scope, rules of engagement, legal authorizations.	Scope document, test plan, risk acceptance matrix.
2. Information Gathering	Asset inventory, network mapping, OS/technology identification.	Network diagram, asset list, threat model.
3. Vulnerability Identification	Run scanners, review configs, perform manual checks.	Raw vulnerability list, CVSS scores.

Introduction to Security Assessment and

Phase	Activities	Deliverables
4. Exploitation / Validation	Attempt to exploit findings, establish proof of concept.	Exploit logs, screenshots, impact evidence.
5. Post-Exploitation (optional)	Pivot, maintain access, simulate data exfiltration.	Lateral movement map, data accessed

Testing