

Introduction to Cybersecurity Assessment

Introduction to Cybersecurity Assessment and Testing

Key concepts, objectives, and common methodologies

1. Why Assess & Test Security?

Goal	What It Achieves
Identify weaknesses	Finds gaps before attackers exploit them
Validate controls	Confirms that security measures work as intended
Prioritize remediation	Provides risk-based ranking of issues
Compliance	Satisfies regulatory and standards requirements (e.g., PCI-DSS, ISO 27001)
Continuous improvement	Supplies data for refining policies, architecture, and training

2. Core Terminology

Term	Definition
Vulnerability	A flaw in software, hardware, or process that could be leveraged to compromise a system.
Threat	Any circumstance or actor that could exploit a vulnerability.
Risk	The probability of a threat exploiting a vulnerability and the impact of that exploitation.
Asset	Anything of value to the organization (data, services, devices, reputation).
Control	A safeguard (technical, administrative, or physical) that reduces risk.
Assessment	Systematic evaluation of security posture (often documentation-heavy).
Testing	Active attempts to exploit weaknesses (e.g., penetration testing, red-team exercises).

3. Assessment & Testing Lifecycle

Introduction to Cybersecurity Assessment and Testing

1. Planning & Scoping

- Define objectives, boundaries, and rules of engagement.
- Identify assets, stakeholders, and compliance drivers.

2. Information Gathering

- Asset inventory, network diagrams, system configurations.
- Open-source intelligence (OSINT) on external exposure.

3. Vulnerability Identification

- Automated scanning (Nessus, OpenVAS, Qualys).
- Manual review of code, configurations, policies.

4. Risk Analysis

- Map vulnerabilities to threats and assets.
- Use a scoring model (CVSS, custom risk matrix).

5. Exploitation / Testing

- **Penetration Testing** – controlled attacks to prove exploitability.
- **Red-Team Exercise** – realistic, multi-vector attack simulation.
- **Blue-Team Validation** – detection and response testing.

6. Reporting

- Executive summary (business impact, high-level findings).
- Technical details (vulnerability description, evidence, remediation steps).
- Prioritized action plan (short-, medium-, long-term).

7. Remediation & Verification

- Apply patches, configuration changes, policy updates.
- Re-test to confirm closure of findings.

8. Continuous Monitoring

- Integrate findings into security dashboards, SIEM, and vulnerability management programs.

Introduction to Cybersecurity Assessment

4. Major Assessment Types and Testing

Type	Focus	Typical Tools	When to Use
Vulnerability Assessment	Broad identification of known flaws	Nessus, Qualys, OpenVAS	Regular baseline checks, compliance audits
Penetration Test (Pen-Test)	Exploitability proof, depth over breadth	Metasploit, Burp Suite, Cobalt Strike	Pre-deployment, post-major change, compliance
Red-Team Exercise	Full-scale adversarial simulation	Custom scripts, C2 frameworks, physical/social engineering kits	Executive risk validation, incident response readiness
Blue-Team / SOC Assessment	Detection, monitoring, and response capability	SIEM, EDR, IDS/IPS logs	