

Introduction to Cyber Security Assessment

Introduction to Cyber Security Assessment and Testing

Designed as a quick-reference guide for students, new analysts, or anyone needing a clear overview.

1. What Is Cyber Security Assessment?

Aspect	Description
Purpose	Identify weaknesses, measure risk, and verify that security controls work as intended.
Scope	Can cover networks, applications, cloud environments, endpoints, people, and processes.
Outcome	Actionable findings (e.g., “unpatched server”) plus recommendations and a prioritized remediation plan.
Frequency	One-time (e.g., before a launch) or recurring (quarterly, annually, after major changes).

2. Core Assessment Types

Type	Goal	Typical Methods	When to Use
Vulnerability Assessment (VA)	Catalog known weaknesses.	Automated scanners, asset inventory, CVE databases.	Regular baseline checks; large asset pools.
Penetration Testing (Pen-Test)	Simulate real-world attack to see if vulnerabilities can be exploited.	Manual exploitation, automated tools, social engineering.	Before release, after major changes, compliance requirements.
Red Team Exercise	Full-scale adversary emulation (tactics, techniques, procedures).	Long-duration attacks, physical/social vectors, stealth.	High-value targets, maturity testing, executive buy-in.
Blue Team Assessment	Evaluate detection and response capabilities.	SOC monitoring review, incident-response drills, log analysis.	Ongoing operations, maturity assessments.

Introduction to Cyber Security Assessment and Testing

Type	Goal	Typical Methods	When to Use
Purple Team Collaboration	Combine Red and Blue to improve both offense and defense.	Joint exercises, shared debriefs, toolchain integration.	Continuous improvement cycles.
Security Posture Review	Holistic view of policies, governance, and controls.	Interviews, documentation review, gap analysis.	Strategic planning, audit preparation.

3. Standard Methodologies & Frameworks

Framework	Key Phases	Typical Deliverables
NIST SP 800-115 (Technical Guide to Information Security Testing)	Planning ? Discovery ? Attack ? Reporting	Test plan, evidence logs, risk rating.
OWASP Testing Guide (Web Apps)	Information Gathering ? Threat Modeling ? Vulnerability Identification ? Exploitation ? Reporting	OWASP Top-10 coverage matrix, proof-of-concept (PoC) scripts.
PTES (Penetration Testing Execution Standard)	Pre-engagement ? Intelligence Gathering ? Threat Modeling ? Vulnerability Analysis ? Exploitation ? Post-exploitation ? Reporting	Detailed scope, risk matrix, remediation checklist.
MITRE ATT&CK	Mapping of adversary techniques ? Detection gap analysis ? Mitigation planning	ATT&CK matrix heat map, detection coverage score.
ISO/IEC 27001 & 27002	Control selection ? Implementation ? Monitoring ? Review	Control effectiveness report, compliance gap analysis.

4. Assessment Lifecycle (Step-by-Step)

1. Define Scope & Objectives

Introduction to Cyber Security Assessment and Testing

- Identify assets, networks, applications, data classifications.
- Agree on rules of engagement (ROE), time windows, legal limits, data handling.

2. Gather Intelligence (Recon)

- Passive: WHOIS, DNS, public repositories, social media.
- Active: Port scanning, banner grabbing, API enumeration.

3. Threat Modeling

- Create **Attack Trees** or **STRIDE** diagrams.
- Prioritize high-value targets and likely attack paths.

4. **Vulnerability Identification