# Security Scanning and Vulnerability Assessment: Essentials

**Duration**: 3 Days (24 Hours)

---

**Day 1: Security Tools for Testing and Scanning**
1.1 Introduction to Security Testing and Scanning
1.2 Categories of Security Tools

- Vulnerability Scanners
- Penetration Testing Tools
- Network and Application Testing Tools

1.3 Overview of Commonly Used Security Tools like Nmap, Nessus etc.

---

**Day 2: Procedures for Conducting Vulnerability Tests**
2.1 Understanding the Vulnerability Testing Lifecycle

- Pre-Assessment Planning
- Execution: Identifying and Analyzing Vulnerabilities
- Reporting and Post-Assessment Actions

2.2 Recognizing and Categorizing Vulnerabilities
2.3 Aligning Vulnerability Testing with Security Policies

---

**Day 3: Scheduling Security Scans and Defining Scope**
3.1 Defining the Scope of Security Scans

- Internal vs. External Scans
- Network and Application-Specific Scans

3.2 Developing a Security Scanning Schedule

- Frequency and Coverage Considerations
- Stakeholder Communication

3.3 Actionable Insights from Security Scanning Reports