**1. Planning and preparation**

* Define goals: Identify what you want to achieve with security testing.
* Scope definition: Determine the boundaries and scope of the test, including the systems, applications, and data to be tested.
* Resource allocation: Allocate resources, including tools, personnel, and time.

**2. Reconnaissance**

* Information gathering: Gather as much information as possible about the target system. This can include domain names, IP addresses, network topology, and employee details.
* Footprinting: Identify potential vulnerabilities through passive information gathering techniques such as WHOIS queries, DNS queries, and social engineering.

**3. Vulnerability scanning**

* Automated scanning: Use automated tools to scan for common vulnerabilities such as open ports, outdated software, and known vulnerabilities.
* Manual testing: Manually verify the results of automated tools and explore complex vulnerabilities.

**4. Threat modeling**

* Identify threats: List potential threats based on the information collected and known vulnerabilities.
* Risk assessment: Assess the impact and likelihood of these threats.

**5. Penetration Testing**

* Exploiting vulnerabilities: Attempting to exploit identified vulnerabilities to understand their impact.
* Privilege escalation: Testing whether low-level access can be elevated to higher privileges.

**6. Secure Code Review**

* Static Analysis: Reviewing source code for security vulnerabilities using automated tools and manual inspections.
* Dynamic Analysis: Testing running applications to identify security issues in the dynamic behavior of the application.

**7. Security Control Validation**

* Authentication and Authorization: Ensure that user authentication mechanisms are strong and access controls are properly implemented.
* Data Protection: Verify that data encryption in transit and at rest is properly implemented.
* Logging and Monitoring: Check that logging and monitoring systems are in place and operating effectively.

**8. Configuration and Deployment Review**

* Server and Network Configuration: Review server settings and network configuration for security vulnerabilities.
* Application Configuration: Ensure that application configuration does not expose it to unnecessary risk.

**9. Compliance Testing**

* Regulatory Compliance: Verify that the application complies with relevant regulations and industry standards (e.g., GDPR, PCI-DSS).

**10. Reporting and Documentation**

* Documenting findings: Documenting all discovered vulnerabilities, their impact, and potential fixes.
* Risk Mitigation: Provide recommendations to mitigate identified risks.
* Management Reporting: Prepare a report for stakeholders summarizing findings and recommending next steps.

**11. Remediation and Retesting**

* Fix vulnerabilities: Work with development teams to address identified vulnerabilities.
* Retesting: Retest applications to ensure that fixes are effective and no new vulnerabilities have been introduced.

**12. Continuous Monitoring**

* Regular Scanning: Perform regular security scans to catch new vulnerabilities.
* Security Updates: Update systems and software with the latest security patches.