TYPES

Aspect	White-Box Testing	Black-Box Testing	Grey-Box Testing
Definition	Full access to the system's code, architecture, and documentation is provided.	Tester has no prior knowledge of the system. Simulates an external attacker.	Limited knowledge about the system is provided, mimicking an insider threat or a semi-privileged user.
Objective	Comprehensive security assessment, covering internal and external vulnerabilities.	Identify vulnerabilities exposed to external attackers.	Balance between internal and external vulnerability identification.
Knowledge Required	High familiarity with the system (source code, architecture, etc.).	No prior knowledge required; focuses on exploration and exploitation.	Moderate system understanding with partial documentation or credentials.
Advantages	- Comprehensive coverage of vulnerabilities.	- Realistic simulation of external attacks.	- Effective at finding flaws accessible to semi-privileged users.
	- Quick identification of issues in the code.	- No assumptions bias the test results.	- Faster than white-box but more thorough than black-box testing.
Disadvantages	- Time-consuming and resource-intensive.	- Limited to vulnerabilities visible externally.	- Can miss vulnerabilities outside the provided knowledge scope.
	- Requires full cooperation and disclosure from the client.	- Less efficient at finding internal issues.	- Requires accurate scoping for meaningful results.
Tools Used	Static analysis tools, dynamic analysis tools, and code review utilities.	Scanning tools, automated exploit frameworks, and fuzzers.	Combination of static and dynamic tools depending on the given access.

Scenario	Testing a banking application where the organization has strict compliance needs.	Assessing the security of a public-facing e-commerce website.	Testing an internal HR portal where some access is assumed (e.g., login credentials).

Real-World Scenarios

1. **White-Box Testing:**
    - Suitable for: Large enterprises or critical systems like banking applications or military systems where security is paramount.
    - Scenario: A financial institution needs to ensure the robustness of its transaction processing system. The tester has full access to source code, APIs, and documentation to identify vulnerabilities at every level.
2. **Black-Box Testing:**
    - Suitable for: Public-facing systems or products such as websites or apps used by customers.
    - Scenario: An e-commerce company hires a penetration tester to evaluate how secure their website is against external hackers who have no internal knowledge of the system.
3. **Grey-Box Testing:**
    - Suitable for: Internal applications where users have some access, such as employee portals or content management systems.
    - Scenario: A company suspects insider threats and wants to test the security of an HR portal accessible by employees with limited privileges, providing testers with basic login credentials and partial documentation.