White Box Testing

- **Description**: The tester has full knowledge of the system, including source code, configurations, and network architecture.
- **Advantages**:
  - Provides a comprehensive assessment, identifying deep vulnerabilities such as those in the source code.
  - Allows for thorough testing of internal systems, configurations, and protocols.
- **Disadvantages**:
  - Time-consuming due to the volume of information to be reviewed.
  - May miss vulnerabilities that could be discovered by an external attacker.
- **Real-World Scenario**: White box testing is best suited for **internal security audits** in a company where the goal is to assess the security of the application's code, network configuration, and internal systems.

Black Box Testing

- **Description**: The tester has no prior knowledge of the system or its internal workings, simulating an attack from an outsider with no insider information.
- **Advantages**:
  - Provides a realistic view of how an attacker would attempt to exploit vulnerabilities from the outside.
  - Helps assess the system's exposure to external threats and its defenses against attacks.
- **Disadvantages**:
  - The tester has to gather information from scratch, which can be time-consuming and may miss certain vulnerabilities.
  - Limited depth of testing due to the lack of internal knowledge.
- **Real-World Scenario**: Black box testing is ideal for **external penetration tests**, such as when a financial institution hires a team to test its public-facing web applications or systems for external vulnerabilities.

Grey Box Testing

- **Description**: The tester has partial knowledge of the system, typically in the form of access to user credentials or some system details, but not full access to the internal workings.
- **Advantages**:
  - Simulates an attacker with some insider knowledge, such as a compromised user account.
  - Provides a balanced scope of testing, targeting critical assets while still maintaining a realistic approach.
- **Disadvantages**:
  - May miss vulnerabilities that would be identified in a more comprehensive white box test.

    - The tester's partial knowledge may lead to a less thorough test compared to full access testing.
- **Real-World Scenario**: Grey box testing is suitable for **corporate network security assessments**, where the tester might have access to limited information, such as an employee's user account, and tests how far an attacker with this knowledge could compromise the network.