PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

Ferhat Abbas University Setif 1

Faculty of Sciences

IT Department

Cyber Security

Module: CCM

Title

Ethical Hacking (white box, black box and grey box testing techniques)

realized by:

- ***Yessad Djaafer***
- ***Bouzidi Aymene***

Supervised by:

Mr. GOUDJIL Lakhdar

Academic year: 2023/2024

I. Introduction

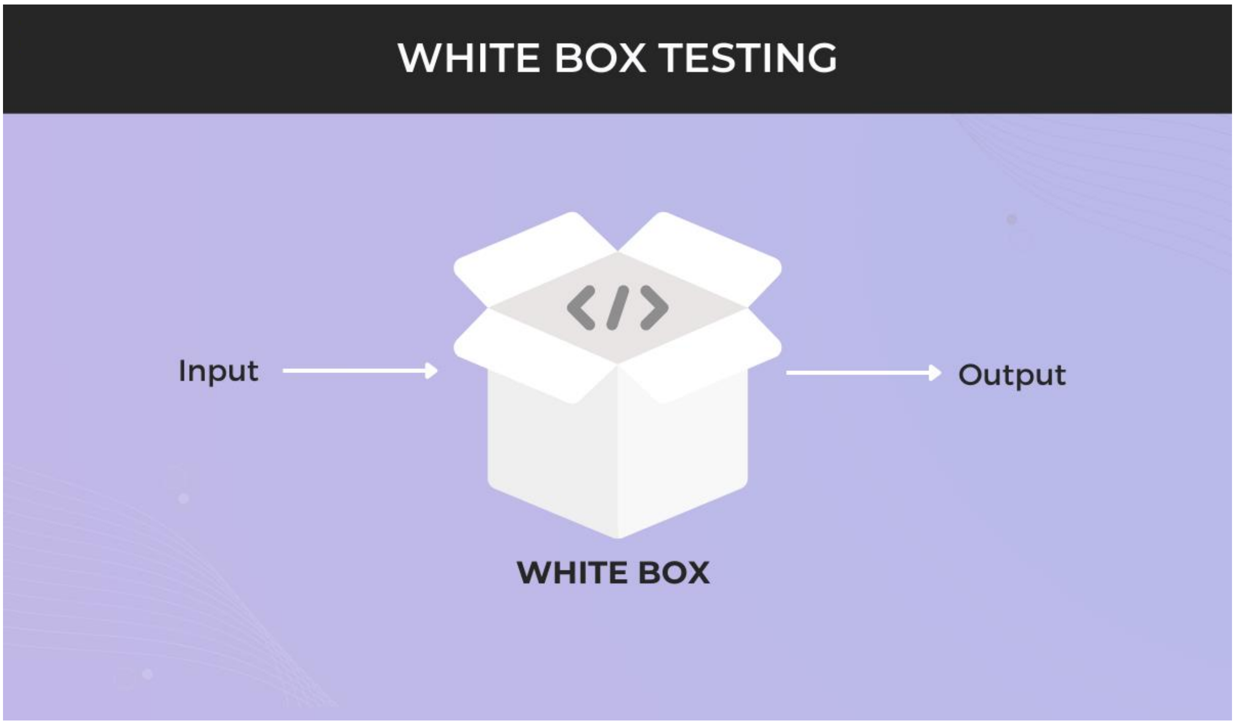
When you're starting out in cyber security specifically in pen testing and ethical hacking one of the more confusing things can be the different types of tests that you might perform this is a specifically talking about white box black box and grey box testing in this presentation we are going to see if we can remove some of that mystery.

II. Objectives of the Presentation

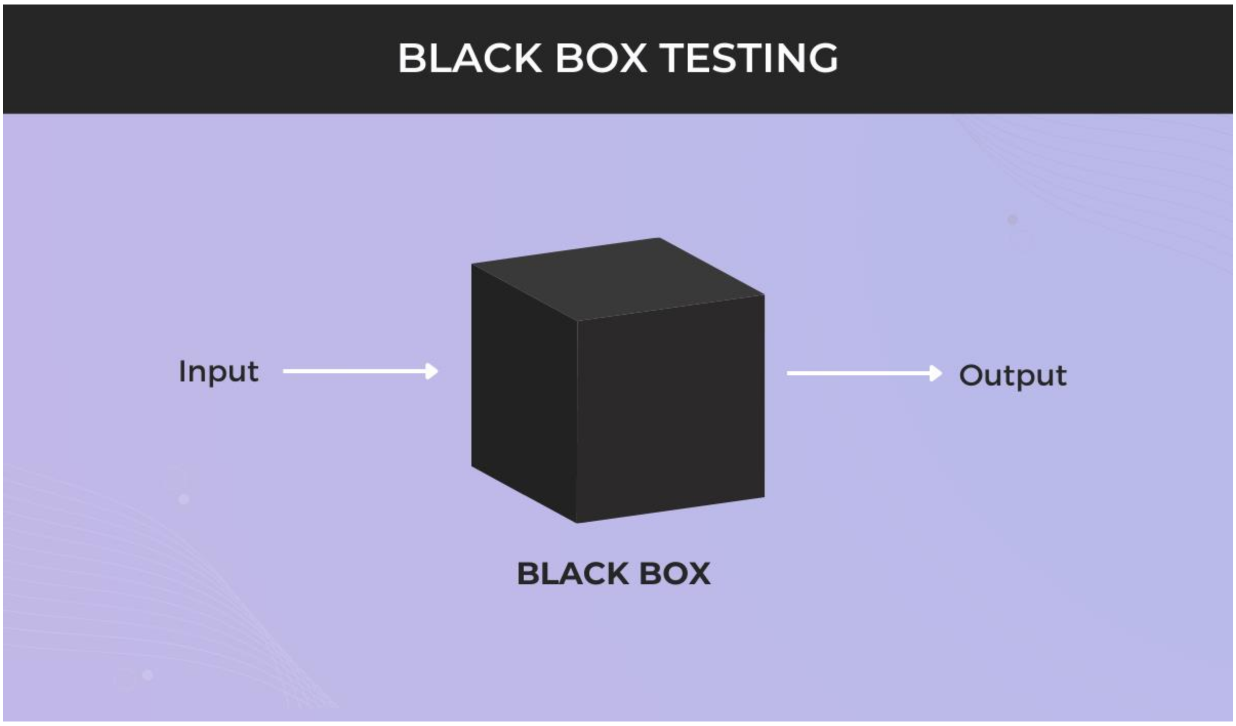
This presentation explores ethical hacking tools and methods, concentrating on software testing, particularly white box, black box, and grey box testing approaches. These techniques aid organizations in identifying and addressing defects, flaws, or errors in the application code.

III. Definitions

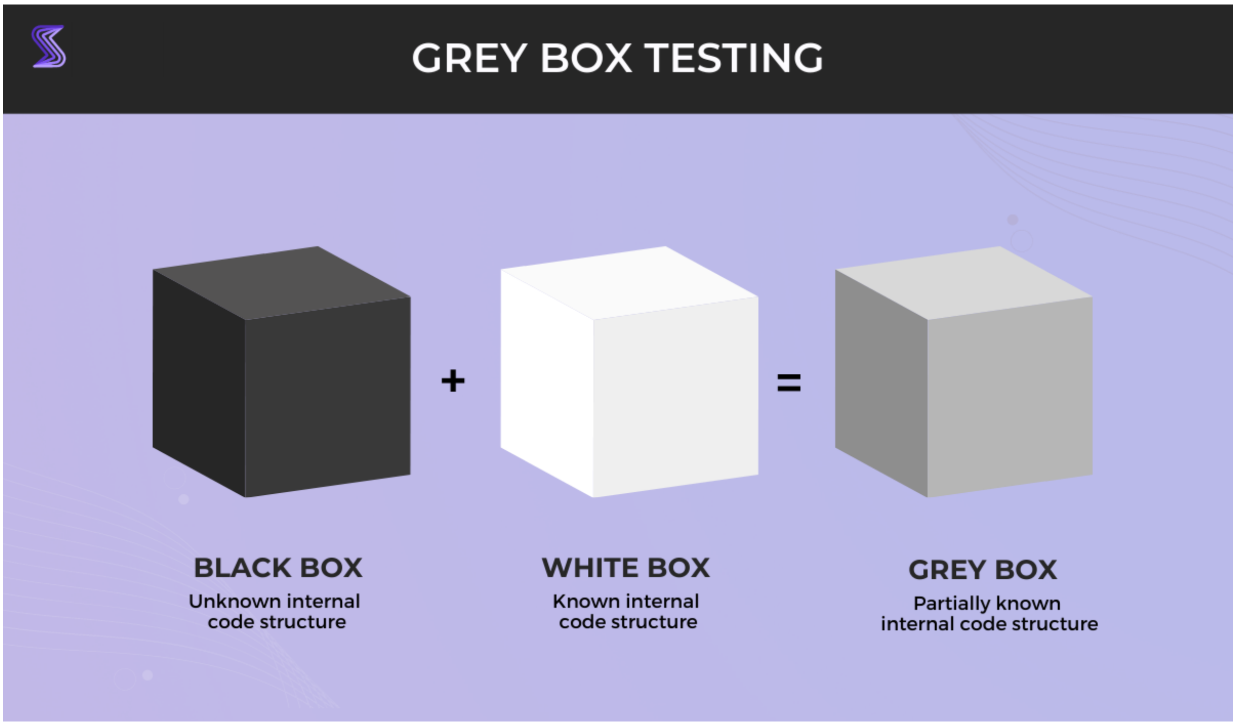
- **White box testing:** It is the detailed investigation of internal logic and structure of the code. In white box testing it is necessary for a tester to have full knowledge of source code.



- **Black box testing:** It is a technique of testing without having any knowledge of the internal working of the application. It only examines the fundamental aspects of the system and has no or little relevance with the internal logical structure of the system.



- **Grey box testing:** White box + Black box = Grey box, it is a technique to test the application with limited knowledge of the internal working of an application and also has the knowledge of fundamental aspects of the system.


GREY BOX TESTING
+
=
BLACK BOX
Unknown internal code structure
WHITE BOX
Known internal code structure
GREY BOX
Partially known internal code structure

IV. Testing techniques

A. White Box Testing:

- **Control Flow Testing:** Imagine your program's flow is like a road map. Control Flow Testing checks different roads to ensure everything runs smoothly. It prefers simple roads over complicated ones.
- **Branch Testing:** Picture your code as a series of decision points. Branch Testing checks every possible choice (true or false) at these points, even when decisions get a bit complex.
- **Basis Path Testing:** Think of your code as a city with streets and intersections. Basis Path Testing figures out how complex the city is, then plans routes to cover all important areas, making sure no street is left unexplored.
- **Data Flow Testing:** Imagine your program is like a network of pipes (data flow). Data Flow Testing marks where the pipes start and end, ensuring the data flows correctly through your program.

- **Loop Testing:** If your code has loops (repeating parts), Loop Testing checks if they work correctly. It's like making sure a revolving door spins smoothly and doesn't get stuck.

B. Black Box Testing:

- **Equivalence Partitioning:** It can reduce the number of test cases, as it divides the input data of a software unit into partition of data from which test cases can be derived.
- **Boundary Value Analysis:** tests whether the software delivers the correct output when the input contains the lower or upper limit of the input variable.
- **Fuzzing:** Fuzz testing helps discover implementation bugs by injecting malformed or semi-malformed data in an automated or semi-automated session.
- **Cause-Effect Graph:** A Cause-Effect Graph is a testing technique that starts by creating a graph to establish relationships between the effect and its causes. It uses four basic symbols—identity, negation, logic OR, and logic AND—to express the interdependencies between causes and effects.
- **Orthogonal Array Testing:** Orthogonal Array Testing (OAT) is a systematic software testing technique that aims to reduce the number of test cases required for effective testing while still providing comprehensive coverage of the input domain. It is particularly useful when the number of potential input combinations is large, making exhaustive testing impractical.
- **State Transition Testing:** State Transition Testing is a method that checks how a system or application behaves when it encounters different states or conditions. It's useful for systems that show different behaviors depending on their internal state changes.

C. Grey Box Testing:

- **Matrix Testing:** Matrix testing is a technique that examines all variables in an application. You can use this technique to identify unused or un-optimized variables.
- **Regression Testing:** To check whether the change in the previous version has regressed other aspects of the program in the new version.
- **Pattern Testing:** This testing is performed on the historical data of the previous system defects. Unlike black box testing, gray box testing digs within the code and determines why the failure happened.
- **Orthogonal Array Testing:** Orthogonal Array Testing (OAT) is a systematic software testing technique that aims to reduce the number of test cases required for effective testing while still providing comprehensive coverage of the input domain. It is particularly useful when the number of potential input combinations is large, making exhaustive testing impractical.

V. Advantages & Disadvantages

A. White Box Testing:

1. Advantages:

- It identifies errors in code and thus makes the debugging process easier.
- Maximum coverage is attained during test scenario writing.
- It removes extra lines of code that are not required in the program. So, the optimization of the program becomes easy and efficient.

2. Disadvantages:

- It is very expensive as it requires a skilled tester to perform it.
- Many paths will remain untested as it is very difficult to look into every nook and corner to find out hidden errors.
- Some of the codes omitted in the code could be missed out.

B. Black Box Testing:

1. Advantages:

- No programming skills or knowledge of IT are required to test through this method. Tester perception is very simple.
- Quicker test case development.
- Tests have lower complexity.

2. Disadvantages:

- Only a selected number of test scenarios are actually performed. As a result, there is only limited coverage.
- Without clear specification test cases are difficult to design.
- The root cause of the test failure is difficult to identify.
- It is difficult to automate.

C. Grey Box Testing:

1. Advantages:

- Grey box testing provides combined benefits of white box and black box testing techniques.
- In grey box testing, the tester can design excellent test scenarios.
- The test is done from the user’s point of view rather than designer’s point of view.

1. Disadvantages:

- Test coverage is limited as the access to source code is not available.
- Many program paths remain untested.
- If the software designer has already run a test case, the tests can be redundant.

VI. Differences

Black Box Testing	Grey Box Testing	White Box Testing
No knowledge of internal working	Partial knowledge of internal working	Full knowledge of internal working
Performed by end users and also by tester and developers	Performed by end users and also by tester and developers	It is performed by developers and testers
It is least exhaustive and time consuming	It is somewhere in between	Potentially most exhaustive and time consuming
It can test only by trial and error method	It is somewhere in between	Test better: data domains and internal boundaries
Not suited for algorithm testing	Not suited for algorithm testing	It is suited for algorithm testing (suited for all)

VII. Conclusion

You now know three different ways to test software.

Remember, all of these methods are vital to the software testing process, but the key is knowing when to use each one.

While black box testing is more suitable when you want to test the software’s functionality, white box testing is best used when you want to check if all code paths are covered.

Gray box testing falls somewhere in the middle when you want to inspect both aspects of the software–its internal and external workings.

Hopefully, this article has provided some clarity on the subject and will help guide your future efforts.