**Penetration Testing Methods**

**Black box pen testing**

Black box testing is carried out without the knowledge of evaluating infrastructure so pen tester will act as a real-world hacker in this case. The pen tester team will scan the entire infrastructure as an outsider to find vulnerabilities. Black-box penetration testing is based on a detailed review of currently running programs and systems. A black-box penetration tester should know both automated and manual penetration testing methodologies. Generally, this is the best approach because it helps pen testing team to think out of the box and carry out testing in all levels according to their realistic knowledge and expertise and they will also use all the techniques and methodologies available to them for simulating the level of persistence, knowledge, and expertise that a real-world hacker can perform.

**White box pen testing**

Pen testers will have full knowledge of the infrastructure and its internal design in white box pen testing and it is also known as clear box testing. The penetration tester seeks to obtain as much input as they can to gain more knowledge and better understand the system so that they can further expand their penetration tests. The main challenge with white-box testing is to analyze the vast amount of data and extract data to identify possible vulnerability points, making it the most time-consuming method of penetration testing. In white-box testing, we can find logical errors, syntax error or typographical errors, design flaws, human errors, etc. While performing the white box testing the pen testers will have full access to the system for performing audits on the high-risk area.

**Grey box pen testing**

Grey box testing is also known as translucent testing, it is more efficient but time consuming because some times testers will test every single input path or field . in grey box testing the tester will have limited information of internal working of system and source code .the grey box testing will not be useful during the development phase because grey box testing is carried out based on end-user perspective that aims to test the front-end functionality and the internal workings of the system. grey box pen testing will have benefits of box whit and box pentesing. grey box pentesting is very effective for web application testing, business domain testing and security assessment