Conducting a penetration test successfully is a challenge for every tester. It does not only require probing into systems by running testing tools. In fact, it needs a lot of experience and skill. A penetration tester should know what vulnerabilities to exploit, how to exploit them and where to locate them.

However, you will have more chances of a successful penetration test if you prepare yourself before carrying it out:

**Get the Approval and Discuss Scope of the Penetration Test**

You first need to get a formal approval of the organization for conducting the test. The process is just like an actual cyber-attack. Hence, whether you are an external or internal tester, the staff won’t be happy if you start without informing them. The approval process does not only include a green signal for testing. It also means that the testers and senior staff have a discussion with each other about which parts of the systems should be tested. These could include network testing, web application testing, wireless penetration testing or simulated phishing. The two parties should also agree on the scope of test, including what the team can and cannot do.

**Decide How to Conduct the Test**

A penetration test can be conducted in many ways:

**Zero Knowledge**

The tester is given very little detail about their target. It imitates a scenario where attacker does not have any inside knowledge.

**Partial Knowledge**

The tester is given some of the information about the target such as IP addresses, physical locations, network configurations and other relevant detail.

**Full Knowledge**

Testers are provided with all the information they need. This is common for internal testers who perform regular assessment of the organization.

**Blind Testing**

Test is carried out without the knowledge of administrators. This test is conducted to find out if admins are able to detect the attack and monitor the response or not.

**Select a Team**

You may already have a team of penetration testers who each have their own expertise. You can have your internal team perform the penetration test, or hire services of a cybersecurity consultancy for better results.

**Use Appropriate Tools**

The tools that you use should be appropriate for the test type. If you require to perform the test without being noticed, you will need lesser known tools and techniques. If your requirement is to perform the test quickly with fast results, you will need more noticeable, powerful tools.

Now that you have the scope, team and right tools in place, you can begin your penetration test.