Penetration testing is a technique in which an ethical hacker exploits the company’s network to check its level of security. The company can deploy relative measures after a complete evaluation of their system’s security and by figuring out how to defend it better.

A penetration test goes through five essential stages to complete its goal:

### In-depth Company Research

The foremost step to start penetration testing is to have in-depth research of the company. The more information you have about the company, the better you can run the test. You can discover the technologies that the company uses and map out their entire network. Thus, you can now easily detect the weak spot and flaws in the system. You do not perform any test at this stage of penetration testing. However, it holds the most vital information from the perspective of an outsider without using any special tools.

### Inspection

In this phase of penetration testing, you start the actual procedure of the test. You can now start messing with the system of your target and send data packets. These data packets interpret the response by which they will gather important information like:

* Open ports
* IP addresses
* Operating system information
* Services installed

There are many tools to assist you in this stage of the penetration test. The ones which testers prefer the most are Nmap, Nessus, and OpenVAS. All these provide a complete scan report with detailed information about the target system.

### System Penetration and Exploitation

All the information which you gathered before will now be helpful to penetrate the system of the target. In this phase you aim to get access and maintain this access to different points in the system. The indication of successful exploitation is if you get at least a user-level access. From there, you build up the pace and perform privilege escalation. One of the favourite tools of testers is the Metasploit that is an open-source tool. The best thing about this tool is that it is open-source even at a commercial level that makes it easy to use. Furthermore, it gets regular updates which enhance its performance.

### Maintaining Access

It is not easy to gain access to a system. Thus, it is essential that once you gain access, you should maintain it at all times. Backdoors, keyloggers and another such piece of code will come in handy here. You can deploy them in the system.

### Presenting the Report

The major difference between an ethical hacker and illegal hacker is that the former presents a report after completing the test. Thus, your last step will be to present a complete report about how you got access to the system and what flaws exist, so that the company can take security measures accordingly.

If you need help with cyber security assessment of your organization, reach out to Aardwolf Security’s team of penetration testing experts.