Penetration Test, otherwise known as a Pen Test, has become a necessary part of a comprehensive security program. It is a simulated security attack on PC frameworks and systems or a whole IT foundation. Penetration test uncovers the weaknesses in our operating systems, core attack vectors, application software, and network devices. The idea is to discover and secure vulnerabilities of our system before the attacker exploits them. Penetration test has never been a higher priority than it is today with phishing, ransomware, DDoS attacks, and other tactics used by cybercriminals. The best way to avoid those is to know your strengths and weaknesses by being proactive. A key segment of any effective security program is penetration testing. It permits companies to find and oversee weaknesses, avoid expensive downtime, and safeguard brand and company reputation.

## ****When to Conduct a Penetration Test?****

There is no exact answer to this question because every company or system is different and each has a different probability of getting attacked. Understanding the company’s business line is crucial for successful security testing. With continuous new changes, systems need to be tested consistently. Regardless of this, many companies decide to do the absolute minimum and run penetration tests just when required, for example, agreeing to authoritative consistency or administrative commitments, which results in a box-ticking activity to satisfy the examiners. And some companies conduct penetration tests only after they suffer from a breach of security. By that time, it’s too late. Hacker has already gained entrance and accomplished what they set out to do.

In normal circumstances, we should conduct penetration tests regularly, at least once or twice every year to guarantee more predictable network security by uncovering how newfound threats or arising weaknesses in our system may be abused by hackers. We should run a penetration test right away in case of some extraordinary circumstances such as when we:

* have an incident of any security breach.
* add a new web application or infrastructure to our network.
* add a new site to our network.
* move our business to a different location or if there is a case of a joint venture.
* use software that is more vulnerable such as open-source software.
* apply new security patches to our software.
* are in a company that is high-profile or prone to a security breach, for example, Banks (they need a high level of protection).
* modify the end-user policies.

Get your systems tested by professional penetration testing services today!