Often people misunderstand the difference between vulnerability scanning and penetration testing and use the two terms interchangeably. A vulnerability scan seeks to search a system for known vulnerabilities, whereas a penetration test attempts to exploit a weakness in a network environment. Vulnerability scans can be automated but penetration tests require different expertise levels.

Vulnerability scanning at regular intervals is important to maintain an organization’s information security. It is always recommended to perform scans for every new equipment before deploying it at first. Afterward, organizations should perform vulnerability scans at least quarterly. If there are any changes to an equipment, it should again be followed by a vulnerability scan. Vulnerability scanning helps to detect any issues like missing patches and outdated certificates, services or protocols.

Organizations need to manage baseline reports of their equipment and investigate any changes in added services or open ports. A vulnerability scanner can raise an alarm to network defenders if it detects any unauthorized changes to the environment. Integrating the changes with change control records helps determine if they were authorized changes that occurred as a result of a problem such as violation by a staff member in change-control policy or a malware infection.

Penetration testing, on the other hand, is different. It attempts at identifying unsecured business processes, weak security settings or any other weakness that a hacker can exploit. A penetration test can discover issues such as password reuse, transmitting unencrypted passwords or an old database storing user credentials. A penetration test should not necessarily be conducted as often as a vulnerability scan. However, it must be performed regularly.

A third-party vendor providing specialized penetration testing services can conduct the test better than internal staff members. This ensures the avoidance of conflict of interest and provides a clear, honest and objective view of network environment. There are various tools involved in a penetration test. However, for the test to yield effective results the tester must be reliable and professionally experienced. They must have in-depth knowledge of information technology, be able to think abstractly and have proactive approach towards anticipating threats. It requires thorough and comprehensive focus.

A penetration test report is brief and to-the-point. Though it can give specific details as appendices, but the main report should concisely mention the what and how of compromised data. A useful report also mentions the attack and exploit method, value of data exploited and recommendations to improve the security posture of the organization.