Vulnerability assessment versus penetration testing

There is always a need to understand and practice the correct terminology for security assessment. Throughout your career, you may run into commercial grade companies and non-commercial organizations that are likely to misinterpret the term penetration testing when trying to select an assessment type. It is important that you understand the differences between these types of tests.

Vulnerability assessment is a process to assess the internal and external security controls by identifying the threats that pose serious exposure to the organizations' assets. This technical infrastructure evaluation not only points to the risks in the existing defenses, but also recommends and prioritizes the remediation strategies. The internal vulnerability assessment provides you with an assurance to secure the internal systems, while the external vulnerability assessment demonstrates the security of the perimeter defenses. In both testing criteria, each asset on the network is rigorously tested against multiple attack vectors to identify unattended threats and quantify the reactive measures. Depending on the type of assessment being carried out, a unique set of testing processes, tools, and techniques are followed to detect and identify vulnerabilities in the information assets in an automated fashion. This can be achieved using an integrated **vulnerability management** platform that manages an up-to-date vulnerabilities database and is capable of testing different types of network devices while maintaining the integrity of configuration and change management.

A key difference between the vulnerability assessment and penetration testing is that the penetration testing goes beyond the level of identifying vulnerabilities and hooks into the process of **exploitation**, **privilege escalation**, and **maintaining access** to the target system(s). On the other hand, vulnerability assessment provides you with a broad view of any existing flaws in the system without measuring the impact of these flaws to the system under consideration. Another major difference between both of these terms is that the penetration testing is considerably more intrusive than the vulnerability assessment and aggressively applies all of the technical methods to exploit the live production environment. However, the vulnerability assessment process carefully identifies and quantifies all the known vulnerabilities in a non-invasive manner.

Tip

Why penetration testing?

When there is doubt that mitigating controls such as firewalls, intrusion detection systems, file integrity monitoring, and so on are effective, a full penetration test is ideal. Vulnerability scanning will locate individual vulnerabilities; however, penetration testing will actually attempt to verify that these vulnerabilities are exploitable within the target environment.

This perception, while dealing with both of these assessment types, might confuse and overlap the terms interchangeably, which is absolutely wrong. A qualified consultant always attempts to work out the best type of assessment based on the client's business requirement rather than misleading them from one over the other. It is also the duty of the contracting party to look into the core details of the selected security assessment program before taking any final decision.

Note

Penetration testing is an expensive service in comparison to vulnerability assessment.