**PCI SSC Releases Guidelines for Penetration Testing**

**The Payment Card Industry Security Standards Council (PCI SSC) has recently released its penetration testing information supplement for organizations of all sizes and sectors. This document serves as a surrogate of the previous information supplement released by PCI SSC back in 2008, titled as** “Payment Card Industry Data Security Standard (PCI DSS) Requirement 11.3 Penetration Testing”.

**The supplement provides details on the components of a penetration test, with special emphasis on the difference between a penetration test and a vulnerability scan that includes network and application layer testing, scope, segment check and social engineering. It also provides the desirable qualifications of a penetration tester in terms of education and experience and gives a comprehensive detail on the pre-engagement, engagement and post-engagement phases of the process. Lastly, the supplement gives detailed guidelines on how the penetration test should be reported, along with a checklist for verification purposes of the organization or the assessor. To make organizations better understand the concepts and deal with the requirements, the PCI SSC has included 3 case studies at the end of the supplement.**

Before the release of this information supplement, there was no defined standard methodology for documenting penetration testing activities. Contrary to Approved Scanning Vendors (ASV), which are registered with and evaluated by the PCI Security Standards Council, there is no standardized body for companies that offer penetration testing services. As a result, there has never been a standard way of defining the scope or reporting the results of a penetration test. A defined set of guidelines will now allow all penetration testing companies to define the scope and report the results in a uniform and standardized manner. However, some small scale companies may adopt the bare minimum approach to avoid additional costs.

Penetration testing is a part of the requirement 11 of the PCI Data Security Standard. Over the years, there have been noteworthy changes to this requirement of the PCI DSS. In the early versions of the standard, the focus was on conducting a number of “testing procedures”, which were to be carried out by external organizations to test the security controls. With the passage of time as new versions were created, penetration testing made its place for these testing procedures and evolved as a demonstrable advancement in the fulfillment of industry standards. Penetration testing is now a fundamental process in the validation of security controls and in achievement of compliance. The Chief Technology Officer (CTO) of PCI Security Standards Council, Mr. Troy Leach, said in a statement that penetration testing is one of the most important and critical components of the PCI DSS. According to him, “It shines a light on weak points within an organization’s payment security environment which, if unchecked, could leave payment card data vulnerable."

However, compliance to this requirement still remains an issue for many organizations. Verizon, a Qualified Standard Assessor (QSA), in its compliance report of 2015 shows that requirement 11 was the least complied-with requirement last year. In 2013, approximately 40 percent companies passed penetration testing procedures while in 2014, this percentage was reduced to 33 percent. The lowest compliance rate in the study was found to be that of requirement 11.2 i.e. “perform quarterly internal vulnerability scans, and rescans as needed, until all significant vulnerabilities are resolved”. Compliance rate to this requirement is constantly going down, with 56% in 2013 to 49% in 2014, which means that less than half of the companies are complying with this requirement. Some experts are of the view that many organizations are still unable to distinguish between a penetration test and a vulnerability scan, and this confusion often leads to noncompliance. It is because of the very same reason that PCI SSC has explained the difference between the two in its penetration testing guidance supplement. A vulnerability scan or vulnerability assessment makes use of automated procedures and tools to search for known vulnerabilities within an IP range. The discovered vulnerabilities usually consist of wrongly configured or unpatched systems. Penetration tests on the other hand are conducted by individuals who scan systems for identifying IP addresses, operating systems, software and types of devices. This helps the penetration tester discover vulnerabilities, exploit those vulnerabilities, and evaluate the weaknesses in applications and networks.

Though penetration tests are required only four times a year to achieve compliance according to PCI Data Security Standard, it is advisable to conduct them more often. While many organizations are able to discover vulnerabilities, most of them do not implement any mitigation measures for months. However, the penetration testing guidelines recently released by PCI SSC can now help organizations develop a robust security testing process with a proactive and flexible approach to mitigate vulnerabilities.