**Security Penetration Testing for PCI DSS: What You Need To Know**

The PCI Security Standards Council releases new version of its Data Security Standards every three years. This year it came as a surprise when PCI DSS version 3.1 was released just two years after the release of 3.0 in Nov, 2013. PCI DSS 3.1 formally replaced its older version from 30th June, 2015. The main reason believed to have resulted in the sudden release was major security flaws such as BEAST and POODLE in Secure Sockets Layer protocol and early version of its successor TLS i.e. Transport Layer Security. With the release of 3.1, SSL and early versions of TLS have been duly prohibited and security penetration testing is now no more an option, rather it is mandatory.

In particular, requirement 11.3 relates to security penetration testing.

*11.3 Implement a methodology for penetration testing that includes the following:*

* *Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)*
* *Includes coverage for the entire CDE perimeter and critical systems*
* *Includes testing from both inside and outside the network.*
* *Includes testing to validate any segmentation and scope-reduction controls*
* *Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5*
* *Defines network-layer penetration tests to include components that support network functions as well as operating systems*
* *Includes review and consideration of threats and vulnerabilities experienced in the last 12 months*
* *Specifies retention of penetration testing results and remediation activities results.*

New requirements relating to penetration testing that were considered as “best practices” in earlier versions are now compulsory. In simple words, without meeting these requirements, you cannot achieve PCI compliance. Although penetration testing has always been a part of PCI DSS, what is different in version 3.1 is how it has been mandated. PCI DSS 3.1 directs the inclusion of some key provisions to penetration testing, but does not specifically define what to do and how to meet those provisions.

The bottom-line of this requirement is that your penetration testing methodology should be in a written form and you must hire a qualified internal resource or a penetration testing firm carry out the tests according to the methodology and requirements of PCI DSS. It also asserts that penetration testing should not only be internal and external but it should also establish network segmentation for reducing scope and provide entire coverage of your cardholder data environment.

1. **Adopting a Methodology**

So what can be the best way to comply with this requirement? PCI DSS 3.0 does not specify the methodology in particular but it is obvious that a robust methodology is what it intends to stipulate. You can use NIST SP 800-15 which is used by PCI Security Standards Council as a reference to give an idea of what it really requires. You can also try publications by SANS, for instance, *Conducting a Penetration Test on an Organization*. That being said, when choosing a penetration testing firm to carry out the penetration test for you, choose a firm that has developed its own methodology and a reliable one too. You should make sure that whichever methodology for penetration testing you adopt, it must be detailed, easily examinable and justified.

**What Makes an Effective Penetration Testing Methodology?**

Penetration testing done for PCI clients is often low budget and bare-minimum process, mostly done as a vulnerability scan. For instance, if a compromise is detected in a missing patch, it is not the missing patch that is the vulnerability but rather the process that failed to apply the patch to the target. The focus of the penetration testing process should be to discover faults in the processes and procedures and find the missing links with given evidence to prove your findings.

As a general rule, what you need to know about what makes a good methodology can be summed up as follows:

* A goal or purpose of the test
* Simulation of threats and agents
* Attestation of security defense measures like alerts, IDS/IPS, responses
* Knowledge of attack vectors and their destinations
* Documentation of attempted attacks and their failure/success results
* Presentation of results in a planned and actionable way

1. **Segmenting the Data**

Segmentation of data within the cardholder data environment must also be a part of security penetration testing. In other words, penetration testing should test that the “ring fencing” that is supposed to be in place, actually is in place. This is important because you actually test that the segmentation controls are working, rather than only assuming that they are.

Testing the access to cardholder data from each network that comes under the umbrella of the merchant is necessary to prove to the Qualified Security Assessor (QSA) that each control is in place and functioning correctly. It helps ensure that the cardholder data is safe from not only external threats but internal ones as well. Another segmentation area that is overlooked quite often is penetration testing within the CDE and needs to be taken care of as well.

1. **Reality based Testing**

All businesses must consider and review the threats and vulnerabilities encountered during the last twelve months. This will require penetration testers to consider often-ignored threats like social engineering such as password hacking or phishing scams that have a high rate of success. The goal of this requirement is to provide a real-life scenario and test the system against it and help you analyze your security measures and flaw detection capability in case of a real attack.

**Small Merchants are not Excluded**

If you are a small merchant and thinking that this probably does not apply to you, you are wrong. Small merchants relying on Self-Assessment Questionnaires (SAQ) to validate PCI DSS compliance also need to comply with requirement 11.3. No matter what type of SAQ a small merchant is qualified to complete, whether SAQ A-EP, SAQ C, SAQ D, etc., they are all required to carry out security penetration tests.

It is hoped that this mandatory requirement of security penetration testing and implementation of a methodology will result in lesser cardholder data compromises, more secure networks and fewer breaches and frauds.