

Verifying Your Ecommerce Integrity: Penetration Testing and PCI

Many in the Ecommerce realm are aware of Payment Card Industry (PCI) security standards but that by no means indicates that they have a grasp of the requirements' technical specificity with regards to things like file integrity monitoring, vulnerability assessments and penetration testing. For the sake of this piece we will delve into penetration testing, often referred to as penTesting with relevance to security standards and safeguarding the Ecommerce ecosystem. Having recently undergone our first annual penetration test, ShopVisible is cognizant of the burgeoning importance of online security in Ecommerce. In an effort at reducing fraud and enhancing ROI for online merchants, things like penTests will clearly and inevitably surface for many in the next fifteen months.



Comprehending and indeed paying for PCI compliance can be complicated, time consuming and costly. PCI's twelve seemingly esoteric requirements call for stringently protective guidelines, built to preserve the sanctity (and segregation) of the CDE or cardholder data environment from threats of fraud and information breach. PenTesting is addressed in the critical section eleven of the PCI requirements. This particular section however can be rather confusing for Ecommerce agents as well as certified QSAs (qualified security assessors) and ASVs (approved scanning vendors) because while 11.2 taps into measures encompassing internal and external vulnerability assessments, 11.3 gets to the heart of the penTest which in actuality, is quite different than the former sub section's requirements .

A vulnerability assessment deals primarily with the identification of noted vulnerabilities whereas the more robust and fleshed out penTest is concerned with efforts to "exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible" with regards to breaching the CDE. Genuine penTesting should include both application and network level, layer testing as well as in the controls and processes surrounding these. The penTest should examine the protocols related to entering the network from the outside and analogously, how cardholder information can be leaked out of the network. Anytime significant changes are made to servers and/or hardware, penTesting may be required to verify new vulnerabilities. In some cases, if servers are located off-site at a data center, hardware boxes can be installed to monitor and in fact test automatically without sending a live QSA tester to scope the changes and newly perceived (if any) vulnerabilities.

The scope of most penTesting measures the CDE's susceptibility to intrusive breach. PCI notes in its Information Supplement: PCI DSS requirements 11.3, that "if network segmentation is in place such that the [CDE] is isolated from other systems, and such segmentation has been verified as part of the PCI DSS assessment, the scope of the [penTest] can be limited to the [CDE]." The test itself as well as its results and methodology must be documented in a technical format. These should also be logged for further review so as to be able to view results in an incrementally patterned assessment for PCI. Ideally, this content will rest in the company's organizational ISP containing all relevant security policies and procedures. Extensive audit logging is demanded by PCI so assessors can view the past changes and subsequent implementations. Records should be kept of who makes changes, when they are made and what is being done to augment the eco-system.



To maintain scope and stay in line with PCI's growing requirements, "[penTesting] should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification" like hardware installations and additions, sub-network reconfiguration or server amendments. Basically, if servers are touched and changed, or if upgrades impact the CDE, they should be deemed significant enough to call for another penTest to verify that the changes made are structured in accordance with PCI change management requirements. On a higher level, one more commensurate with PCI's enhanced security protocols, and "as a security best practice, all upgrades and modifications should be [penTested] to ensure that controls assumed to be in place are still working effectively after the upgrade or modification."

In preparation for penTesting an organization must determine whether their evaluation will be performed internally or by a third party QSA. Per PCI's requirements, several different methodologies can be used for penTesting. First, it must be determined how much knowledge and familiarity the tester has with regards to the system. Having no prior knowledge is called "black box testing," in which the tester must "first identify the location of the systems before attempting any exploits." When a user can evidence prior explicit knowledge of the system it is called "white box testing."



If the company or organization undergoing the test predetermines it would be advantageous for the PCI audit process to use a knowledgeable tester, there are certain items required by PCI needed to generate information:

- a network diagram (PCI 1.1.2)
- results from the QSA SAQ (self-assessment questionnaire)
- annual control testing to identify vulnerabilities and halt unauthorized control access (PCI 11.1)
- results from internal/external (at a minimum, quarterly) vulnerability scans (PCI 11.2)
- penTest results (PCI 11.3)
- annual threat and vulnerability identification leading to a risk assessment (PCI 12.1.2)
- annual review of security policies as seen in the organization's ISP or information security policy (PCI 12.1.3)

When scoping the penTest for an Ecommerce company, size and organizational complexity should be addressed. PCI notes that "all locations of cardholder data, all key applications that store, process, or transmit cardholder data, all key network connections, and all key access points should be included." The test by nature is designed to create a concerted effort at the exploitation of APs or access points and verification of vulnerability and weakness in the CDE. Penetration at both the network and the application level is to be wrought by the penTest in an attempt to "determine if unauthorized access to key systems and files can be achieved. If access is achieved, the vulnerability should be corrected and the [penTest] re-performed until the test is clean and no longer allows unauthorized access or other malicious activity."

Summary article written by ShopVisible Marketing Manager, Vijay Mahoney; citations and quotations derived from PCI Information Supplement: Req. 11.3 Penetration Testing, 4/15/2008.

