Security Standards Council™

Standard: Data Security Standard (DSS)
Version: 1.2
Date: **March 2008**
Requirement: 11.3
Author: PCI Security Standards Council

Information Supplement:

Penetration Testing

General

PCI DSS Requirement 11.3 addresses penetration testing, which is different than the external and internal vulnerability assessments required by PCI DSS Requirement 11.2. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing should include network and application layer testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

Who performs penetration testing

The PCI DSS does not require that a QSA or ASV perform the penetration test—it may be performed by either a qualified internal resource or a qualified third party. If internal resources are being used to perform penetration tests, those resources must be experienced penetration testers. The individuals performing penetration testing should be organizationally separate from the management of the environment being tested. For example, the firewall administrator should not perform the firewall-penetration testing.

Reporting and documentation

It is recommended that both the penetration test methodologies and results are documented. PCI SSC has no reporting requirements for penetration tests, however the results should be retained to follow up on the identified issues and as evidence to be reviewed by those performing the PCI DSS assessment.

Scope

The scope of penetration testing is the cardholder data environment and all systems and networks connected to it. If network segmentation is in place such that the cardholder data environment is isolated from other systems, and such segmentation has been verified as part of the PCI DSS assessment, the scope of the penetration test can be limited to the cardholder data environment.

Frequency

Penetration testing should be performed at least annually and anytime there is a significant infrastructure or application upgrade or modification (for example, new system component installations, addition of a sub-network, or addition of a web server). What is deemed “significant” is highly dependent on the configuration of a given environment, and as such cannot be defined by PCI SSC. If the upgrade or modification could impact or allow access to cardholder data, then it should be considered significant. Significance within a highly segmented network where cardholder data is clearly isolated from other data and functions is very different than significance in a flat network where every person and device can potentially access cardholder data. As a security best practice, all upgrades and modifications should be penetration-tested to ensure that controls assumed to be in place are still working effectively after the upgrade or modification.

Preparation

There are several methodologies that can be used for penetration testing. The first decision that needs to be made is how much knowledge the tester has of the system being tested. Having no prior knowledge is known as “black box testing,” where the tester must first identify the location of the systems before attempting any exploits. Having explicit knowledge is known as “white box testing.”

If it is determined that it would be beneficial for the tester to have prior knowledge, there are several items required by other PCI DSS requirements that generate information that can be used. Those PCI DSS items include:

- A network diagram (1.1.2)
- Results from a QSA review or Self-Assessment Questionnaire (SAQ)
- Quarterly testing for presence of wireless access points (11.1)
- Results from quarterly external and internal vulnerability scans (11.2)
- Results from the last penetration test (11.3)
- Annual identification of threats and vulnerabilities resulting in a risk assessment (12.1.2)
- Annual review of security policies (Policies that need to be updated may identify new risks in an organization.) (12.1.3)

Documentation from all of the above should be evaluated, and threats and vulnerabilities identified as part of the normal assessment processes should be considered for inclusion.

Methodology

Once the threats and vulnerabilities have been evaluated, design the testing to address the risks identified throughout the environment. The penetration test should be appropriate for the complexity and size of an organization. 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 penetration tests should attempt to exploit vulnerabilities and weaknesses throughout the cardholder data environment, attempting to penetrate both at the network level and key applications. The goal of penetration testing is to determine whether unauthorized access to key systems and files can be achieved. If access is achieved, the vulnerability should be corrected and the penetration test re-performed until the test is clean and no longer allows unauthorized access or other malicious activity.

Components

Consider including all of these penetration-testing techniques (as well as others) in the methodology, such as social engineering and the exploitation of exposed vulnerabilities, access controls on key systems and files, web-facing applications, custom applications, and wireless connections.

Important Considerations

- With respect to PCI compliance, testing of vulnerabilities or misconfigurations that may lead to DoS attacks which target resource (network/server) availability should not be taken into consideration by the penetration testing since these vulnerabilities would not lead to compromise of cardholder data.
- Communicate timing and scope of penetration testing to all affected parties throughout the organization.
- Perform testing in accordance with critical company processes including change control, business continuity, and disaster recovery.
- Perform all penetration testing during a monitored maintenance window.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Entry Device (PED) Security Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.