SecureCarolina University Information Security Office

Payment Card Industry (PCI) Penetration Testing Standard

Issued Date: 14 May 2015
Effective Date: 14 May 2015

Purpose

This standard outlines penetration-testing requirements for the university's Payment Card Industry (PCI) cardholder data environment (CDE). It also establishes a penetration-testing methodology to meet annual PCI compliance efforts.

Scope

This standard applies to:

- University Information Security Office (UISO),
- PCI Merchants in scope for penetrations tests, and
- The university's CDE.

Definitions

In the context of this document, the following terms are used as indicated here:

Application-layer testing – Testing that typically includes web sites, web applications, thick clients, or other applications.

Cardholder data environment – Areas of a computer system network that possesses cardholder data (or sensitive authentication data) and those systems and segments that directly attach or support cardholder processing, storage, or transmission.

Critical systems – Systems involved in the processing or protection of cardholder data.

Internal Testing – The internal perimeter of the CDE from the perspective of any out-of-scope LAN segment.

External Testing – The exposed perimeter of the CDE and critical systems connected or accessible to public network infrastructures.

Network-layer testing – Testing that usually includes external and internal testing of networks (LANS/VLANS), between interconnected systems, wireless networks, and social engineering.

Penetration test - A test methodology where assessors attempt to circumvent the security features of an information system.

(continued)

Penetration Test Requirements

External and Internal penetration tests must be:

- Performed annually and after any significant infrastructure or application changes to the environment;
- Conducted according to NIST Special Publication 800-115 “Technical Guide to Information Security Testing and Assessment” and PCI's "Information Supplement: Penetration Testing Guidance"; and
- Performed by qualified personnel approved by the UISO;

Penetration tests must:

- Include the entire CDE and critical systems;
- Confirm segmentation and scope reduction controls;
- Include network and application layer* tests;

*Application layer pen tests must include checks detailed in the most current *Open Web Application Security Project (OWASP) Top 10*.

Penetration Tester Requirements

- Testers must describe the qualifications and experience that make them qualified to perform pen tests.
- Testers must detail how they achieve organizational independence.

Tested Organization Requirements

The organization must provide the UISO with:

- A network diagram depicting all network segments in scope for the test;
- Cardholder data flow diagram;
- A list of all expected services and ports exposed at the CDE perimeter;
- Details of how authorized users access the CDE; and
- A list of all network segments that have been isolated from the CDE to reduce scope.

The organization must correct all exploitable vulnerabilities identified during the test and request a retest to confirm the vulnerability no longer exists.

Retention Period

The UISO and the tested organization must keep final reports along with remediation activity results for three years.

(continued)

Appendix A

Penetration Test Process

Overview

A penetration test is an evaluation that simulates real-world attacks in an effort to improve understanding of the system, uncover weaknesses, and enhance security measures.

Methodology

The UISO follows the testing processes described in NIST Special Publications 800-115 *Technical Guide to Information Security Testing and Assessment*.

Phases

There are four phases of penetration testing: Planning, Discovery, Attack, and Reporting.

Planning

The following sections highlight essential activities in the planning phase.

Scope

The organization being assessed is responsible for defining the scope. During the scoping process, the organization should provide the tester:

- A network diagram depicting all network segments in scope;
- Cardholder data flow diagram;
- A list of all expected services and ports exposed at the CDE perimeter;
- Details of how authorized users access the CDE; and
- A list of all network segments that have been isolated from the CDE to reduce scope.

The pen test lead can provide the organization guidance on which assets to include. For PCI penetration tests, the test's scope must include the entire CDE and any critical systems.

Rules of Engagement

Before testing begins, it is important to document how the test will be performed. The rules of engagement (ROE) capture this description and ensure the organization understands what to expect.

Additionally, the ROE authorizes the test and grants the tester approval to begin testing.

ROE Contents

A ROE will include items, such as:

- A time window for testing;
- Identification of systems that have known issues with automated scanning;

(continued)

- A plan for communicating any issues encountered during the engagement;
- A listing of security controls that would detect or prevent testing; and
- Signatures of the authorizing parties.

Scan Interference

The rules of engagement must address "scan interference." Scan interference often occurs when an active control, such as an intrusion prevention system, blocks or interferes with the test. The penetration test must be allowed to perform activities, such as scanning, without interference from active protection systems. Review the section titled “Scan Interference” in PCI’s Approved Scanning Vendors Program Guide for more detail on active protection systems.

Review of past threats and vulnerabilities

PCI DSS Requirement 11.3 requires a review and consideration of historical threats. The test lead will review vulnerabilities identified in the entity’s environment within the past 12 months. The tester will also obtain if available:

- Prior penetration test reports;
- Previously issued PCI compliance documentation, such as Reports on Compliance; and
- Current vulnerability scan test results.

Discovery

The discovery phase of penetration testing includes two parts. The first part is the start of actual testing, and covers information gathering and scanning.

The second part of the discovery phase is vulnerability analysis, which involves comparing the services, applications, and operating systems of scanned hosts against vulnerability databases and the testers’ knowledge of vulnerabilities.

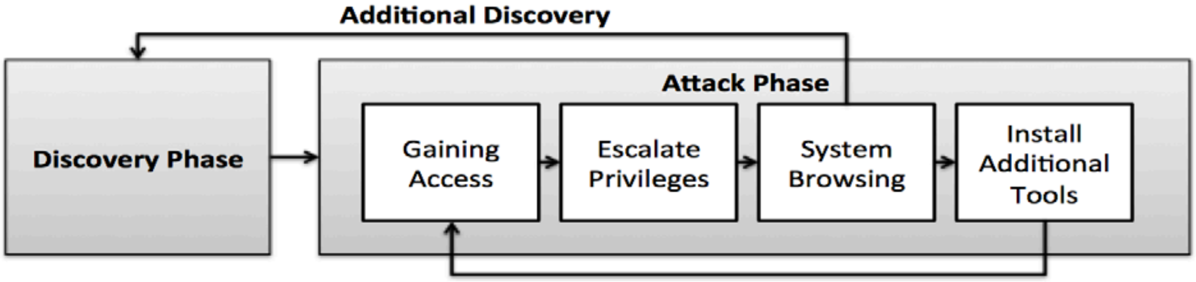
During this phase, the tester will document all identified open network ports and services—from both the external and internal perspectives.

Attack

Executing an attack is at the heart of any penetration test. In the attack phase, the tester will attempt to exploit identified vulnerabilities.

The following figure represents the individual steps of the attack phase.

(continued)



Internal Testing

The scope of the internal penetration test is the internal perimeter of the CDE from the perspective of any out-of-scope LAN segment that has access to a unique type of attack on the CDE perimeter.

External Testing

The scope of an external penetration test is the exposed perimeter of the CDE and critical systems connected or accessible to public network infrastructures.

An external test should assess any unique access to the scope from the public networks, including services that have access restricted to individual external IP addresses.

Both internal and external testing must include application-layer and network-layer assessments. External penetration tests must also include remote access vectors such as dial-up and VPN connections.

Segmentation

If the organization has segmentation controls, the tester will confirm these controls are operational. The tester will perform these checks from any non-CDE environment that the organization intended to be completely segmented from the CDE perimeter.

Application Layer Testing

Application layer testing applies to any software written by or specifically for the organization that is part of the CDE is subject to both an application and network-layer penetration test.

It is common for an environment to host a web application that was not specifically coded for the organization such as commercial web-mail interfaces, document-sharing tools, and network-device administrative interfaces. In these instances, the web application does not typically need an application-layer pen test as the entity is not responsible for the source code of this type of software. Instead, the tester should perform a network-layer test and ensure the software was implemented, configured, and is currently being maintained in a secure manner (disabling or uninstalling unused services, blocking unused ports, applying current updates, etc.).

(continued)

*If a payment application has been PA-DSS validated, the application's functionality does not need to be tested as part of the entity's PCI DSS compliance validation. However, the implementation of the application does need to be tested. This includes both the operating system and any exposed services, but not the payment application's functionality (e.g., authentication, key management, transaction processing, etc.) since this was validated as part of the PA-DSS application validation.

Application layer testing requirements

The tester will evaluate applications against the Open Web Application Security Project (OWASP) Top 10.
The tester will also perform testing from the perspective of the defined roles of the application.

Social Engineering

PCI DSS does not require the use of social-engineering techniques. However, the tester can incorporate it into the penetration testing methodology and ROE.

Reporting

Upon completion of the analysis, the tester will generate a report that identifies system, network, and organizational vulnerabilities along with recommended mitigation actions.

The report will list:

- A summary listing of items that need remediation and retesting, and
- A detailed listing of items that need remediation and retesting.

The tester will also describe attempts to exploit the identified vulnerability and clearly state the potential result/risk that each potential exploit may pose to the environment.

Cleaning up the Environment Post-Penetration Test

After testing there may be tasks the tester or customer needs to perform to restore the target environment (i.e., update/removal of test accounts or database entries added or modified during testing, uninstall of test tools or other artifacts, restoring active protection-system settings, and/or other activities the tester may not have permissions to perform, etc.).

The tester will provide directions on how clean up should be performed and how to verify security controls have been restored.

Remediation

The organization should take steps to remediate any exploitable vulnerability within a reasonable period after the original test. When the organization has completed these steps, the tester should perform a retest to validate the newly implemented controls mitigate the original risk.

(continued)

Appendix B

Example Penetration Test Report Outline

Organization Information

- Contact Information
- Credentials and qualifications of analysts
- Description of how the individuals are organizationally independent of the management of the environment being tested
- Dates the engagement was performed
- Date the report was issued

Executive Summary

- Summarizes testing performed
- Summarizes results of testing
- Summarizes steps for remediation

Statement of Scope

A detailed definition of the scope of the network and systems tested as part of the engagement

- Clarification of CDE vs. non-CDE systems or segments that are considered during the test.
- Identification of critical systems in or out of the CDE and explanation of why they are included in the test as targets.

Statement of Methodology

A description of the methodology used and how it meets industry best practices, such as NIST.

Statement of Limitations

Document any restrictions imposed on testing such as designated testing hours, bandwidth restrictions, or special testing requirements for legacy systems.

Testing Narrative

- Provide details as to the testing methodology and how testing progressed. For example, if the environment did not have any active services, explain what testing was performed to verify restricted access.
- Document any issues encountered during testing (e.g., interference was encountered as a result of active protection systems blocking traffic).

Segmentation Test Results

Summarize the testing performed to validate segmentation controls if used to reduce the scope of PCI DSS.

(continued)

Findings

- Description of finding
- Risk ranking/severity of each vulnerability
- Targets affected
- References (e.g. CVE or BID)

Tools Used

Information gathering, scanning, and exploitation tools are used during the test.

Revision History

Author	Date Test	Comments
Jeremy Parrott	10 April 2015	Initial Draft
Kyle S. Brown	23 April 2015	Formatting
Jeremy Parrott	5 May 2015	Updates based on comments