PCI DSS Penetration Testing Standard for University of Tennessee Merchants

Revision: August 25, 2015

Purpose

To outline the key roles and responsibilities, requirements, and notification methods when network penetration testing is required by the Payment Card Industry Data Security Standard (PCI DSS).

Scope

This standard applies to the University of Tennessee system-wide merchants who are completing PCI DSS Self-Assessment Questionnaire (SAQ) C, and where segmentation is used to isolate the Cardholder Data Environment (CDE) from other networks.

Requirements differ for merchants completing SAQ A-EP or SAQ D. UT should have no merchants completing these SAQ types, but if you feel you fall under SAQ A-EP or SAQ D, please contact the UTSA ISO at once.

Key Roles and Responsibilities

Merchant

- Works with the campus CIO/ISO to define the specific scope for that merchant by providing list of all systems used for processing credit cards.
- Notifies campus CIO/ISO when there is any change to the list of systems.

Campus Chief Information Officer/Information Security Officer

- Maintains updated list of all systems used for processing credit cards.
- Maintains CDE for that campus.
- Maintains segmentation controls and methods documentation.
- Determines the scope for the testing based on segmentation controls and methods.
- Provides the scope, the segmentation controls and methods, and the penetration test evidence to the UTSA ISO.

University of Tennessee System Administration Information Security Office (UTSA ISO)

- Reviews penetration test evidence.
- Produces penetration test report on behalf of the Treasurer's Office.
- Maintains the *PCI DSS Penetration Testing Standard for University of Tennessee Merchants*.

Penetration Testing Requirements for PCI v3.x

PCI DSS Requirement 11.3.4 requires penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the CDE.

Therefore, a robust approach to penetration testing is recommended to satisfy this requirement by actively attempting to identify routes and paths from networks outside the CDE into the CDE. All segmentation methods need to be specifically tested. In very large networks, with numerous internal LAN segments, it may be unfeasible for the penetration tester to conduct specific tests from every individual LAN segment. In this case, the testing needs to be planned to examine each type of segmentation methodology in use (i.e., firewall, VLAN ACL, etc.) in order to validate the effectiveness of the segmentation controls. The level of testing for each segmentation methodology should provide assurance that the methodology is effective in all instances of use. In order to effectively validate the segmentation methodologies, it is expected that the penetration tester has worked with the organization to clearly understand all methodologies in use in order to provide complete coverage when testing.

The penetration tester may choose to include systems located in these isolated LAN segments not directly related to the processing, transmission, or storage of cardholder data to ensure these systems could not impact the security of the CDE if compromised.

The penetration testing process will follow these guidelines:

- Pen tests must be performed at least annually.
- Pen tests must be performed after any changes to segmentation controls/methods.
- The penetration tester may be a resource internal or external to the entity.
- The penetration tester must be given knowledge of segmentation technologies used.
- The segmentation check is performed by conducting tests used in the initial stages of a network penetration test.
    - Tests may be simple port scans using nmap.
- The segmentation check should verify that all isolated LANs do not have access into the CDE.
- The penetration tester should verify that each network segment reported to be isolated from the CDE truly has no access to the CDE.
- Testing of each unique segmentation methodology should be used to ensure that all security controls are functioning as intended.
- If it is determined during the segmentation check that the LAN segment has access into the CDE, either the organization needs to restrict that access or a full network-layer penetration test should be performed to characterize the access.

Notification

The penetration tester will notify the campus CIO/ISO immediately if cardholder data is accessed during the test and will keep detailed documentation as to what was accessed and how it was accessed. The campus CIO/ISO should then immediately review how the cardholder data was retrieved and should take steps to execute the incident response plan, when applicable. If cardholder data was accessed by the penetration tester, this data must be secured in accordance with PCI DSS.

The UTSA ISO provides official reporting to the Treasurer's Office, campus Chief Business Officer, campus CIO/ISO, and merchant. The penetration test report shall include the following:

- Executive Summary
- Statement of Scope
- Statement of Methodology
- Statement of Limitations
- Testing Narrative
- Segmentation Test Results
- Findings
- Tools Used
- Post-Penetration Test Cleanup

Definitions

- Cardholder Data Environment (CDE) – The cardholder data environment consists of the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components.
- Penetration Test – Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing, as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
- Network Segmentation – Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not.