Payment Card Industry (PCI) Data Security Standard

Security Scanning Procedures

Version 1.1

Release: September 2006

Table of Contents

Purpose

This document explains the purpose and scope of the Payment Card Industry (PCI) Security Scan for merchants and service providers who undergo PCI Security Scans to help validate compliance with the PCI Data Security Standard (DSS). Approved Scanning Vendors (ASVs) also use this document to assist merchants and service providers determine the scope of the PCI Security Scan.

Introduction

The PCI DSS details security requirements for merchants and service providers that store, process, or transmit cardholder data. To demonstrate compliance with the PCI DSS, merchants and service providers may be required to have periodic PCI Security Scans conducted as defined by each payment card company.

PCI Security Scans are scans conducted over the Internet by an ASV. PCI Security Scans are an indispensable tool to be used in conjunction with a vulnerability management program. Scans help identify vulnerabilities and misconfigurations of web sites, applications, and information technology (IT) infrastructures with Internet-facing internet protocol (IP) addresses.

Scan results provide valuable information that support efficient patch management and other security measures that improve protection against Internet attacks.

PCI Security Scans may apply to all merchants and service providers with Internet-facing IP addresses. Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible. Basic functions such as e-mail and employee Internet access will result in the Internet-accessibility of a company's network. Such seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems and potentially expose cardholder data if not properly controlled.

Scope of PCI Security Scanning

The PCI requires all Internet-facing IP addresses to be scanned for vulnerabilities. If active IP addresses are found that were not originally provided by the customer, the ASV must consult with the customer to determine if these IP addresses should be in scope. In some instances, companies may have a large number of IP addresses available while only using a small number for card acceptance or processing. In these cases, scan vendors can help merchants and service providers define the appropriate scope of the scan required to comply with the PCI. In general, the

following segmentation methods can be used to reduce the scope of the PCI Security Scan.

- Providing physical segmentation between the segment handling cardholder data and other segments

- Employing appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments

Merchants and service providers have the ultimate responsibility for defining the scope of their PCI Security Scan, though they may seek expertise from ASVs for help. If an account data compromise occurs via an IP address or component not included in the scan, the merchant or service provider is responsible.

Scanning Procedures

To comply with the PCI Security Scanning requirement, merchants and service providers must have their web sites or IT infrastructures with Internet-facing IP addresses scanned, according to the following procedures:

1. All scans must be conducted by an ASV selected from the list of approved scanning vendors provided by the PCI Security Standards Council

    ASVs are required to conduct scans in accordance with the "Technical and Operational Requirements for Approved Scanning Vendors (ASVs)" procedures. These procedures dictate that the normal operation of the customer environment is not to be impacted and that the ASV should never penetrate or alter the customer environment.

2. Quarterly Scans are required in accordance with PCI DSS Requirement 11.2

3. Prior to scanning the web site and IT infrastructure, merchants and service providers must:

    - Provide the ASV with a list of all Internet-facing IP addresses and/or IP address ranges

    - Provide the ASV with a list of all domains that should be scanned if domain-based virtual hosting is used

4. Using the IP address range provided by the customer, the ASV must conduct network probing to determine which IP addresses and services are active

5. Merchants and service providers must contract with the ASV to perform periodic scans of all active IP addresses (or domains, if applicable) and devices

6. The ASV must scan all filtering devices such as firewalls or external routers (if used to filter traffic). If a firewall or router is used to establish a demilitarized zone (DMZ), these devices must be scanned for vulnerabilities

7. The ASV must scan all web servers

   Web servers allow Internet users to view web pages and interact with web merchants. Because these servers are fully accessible from the public Internet, scanning for vulnerabilities is essential.

8. The ASV must scan application servers if present

   Application servers act as the interface between the web server and the back-end databases and legacy systems. For example, when cardholders share account numbers with merchants or service providers, the application server provides the functionality to transport data in and out of the secured network. Hackers exploit vulnerabilities in these servers and their scripts to get access to internal databases that potentially store credit card data.

   Some web site configurations do not include application servers; the web server itself is configured to act as an application server

9. The ASV must scan Domain Name Servers (DNSs)

   DNS servers resolve Internet addresses by translating domain names into IP addresses. Merchants or service providers may use their own DNS server or may use a DNS service provided by their Internet Service Provider (ISP). If DNS servers are vulnerable, hackers can spoof a merchant or service provider web page and collect credit card information

10. The ASV must scan mail servers

    Mail servers typically exist in the DMZ and can be vulnerable to hacker attacks. They are a critical element to maintaining overall web site security.

11. The ASV must scan Virtual Hosts

    It is common practice when using a shared hosting environment that a single server will host more than one web site. In this case, the merchant shares the server with the hosting company's other customers. This could lead to the merchant's web site being exploited through other web sites on the host's server.

    All merchants whose web sites are hosted must request their hosting provider to scan their entire Internet-facing IP range and demonstrate compliance while merchants are required to have their own domains scanned.

12. The ASV must scan wireless access points in wireless LANs (WLANs)

Use of WLANs introduces data security risks that need to be identified and mitigated. Merchants, processors, gateways, service providers, and other entities must scan wireless components connected to the Internet to identify potential vulnerabilities and misconfigurations

13. Arrangements must be made to configure the intrusion detection system/intrusion prevention system (IDS/IPS) to accept the originating IP address of the ASV. If this is not possible, the scan should be originated in a location that prevents IDS/IPS interference

Compliance Reporting

Merchants and service providers need to follow each payment card company's respective compliance reporting requirements to ensure each payment card company acknowledges an entity's compliance status. While scan reports must follow a common format, the results must be submitted according to each payment card company's requirements. Contact your acquiring bank or check each payment card company's regional web site to determine to whom results should be submitted.

Reading and Interpreting Reports

ASVs produce an informative report based on the results of the network scan.

The scan report describes the type of vulnerability or risk, a diagnosis of the associated issues, and guidance on how to fix or patch the isolated vulnerabilities. The report will assign a rating for vulnerabilities identified in the scan process.

ASVs may have a unique method of reporting vulnerabilities; however, high-level risks will be reported consistently to ensure a fair and consistent compliance rating. Consult your vendor when interpreting your scan report.

Table 1 suggests how a compliant network scan solution may categorize vulnerabilities and demonstrates the types of vulnerabilities and risks that are considered high-level.

To demonstrate compliance, a scan must not contain high-level vulnerabilities. The scan report must not contain any vulnerabilities that indicate features or configuratons that are a PCI DSS violation. If these exist, the ASV must consult with the client to determine if these are, in fact, PCI DSS violations and therefore warrant a noncompliant scan report.

High-level vulnerabilities are designated as level 3, 4, or 5.

Level	Severity	Description
5	**Urgent**	Trojan Horses; file read and writes exploit; remote command execution
4	**Critical**	Potential Trojan Horses; file read exploit
3	**High**	Limited exploit of read; directory browsing; DoS
2	**Medium**	Sensitive configuration information can be obtained by hackers
1	**Low**	Information can be obtained by hackers on configuration

Table 1 Vulnerability Severity Levels

Level 5

Level 5 vulnerabilities provide remote intruders with remote root or remote administrator capabilities. With this level of vulnerability, hackers can compromise the entire host. Level 5 includes vulnerabilities that provide remote hackers full file-system read and write capabilities, remote execution of commands as a root or administrator user. The presence of backdoors and Trojans also qualify as Level 5 vulnerabilities.

Level 4

Level 4 vulnerabilities provide intruders with remote user, but not remote administrator or root user capabilities. Level 4 vulnerabilities give hackers partial access to file-systems (for example, full read access without full write access). Vulnerabilities that expose highly sensitive information qualify as Level 4 vulnerabilities.

Level 3

Level 3 vulnerabilities provide hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders. Examples of Level 3 vulnerabilities include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, susceptibility to denial of service (DoS) attacks, and unauthorized use of services such as mail relaying.

Level 2

Level 2 vulnerabilities expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks against a host.

Level 1

Level 1 vulnerabilities expose information, such as open ports.