



ACCESS
INNOVATION
GROWTH



PCI Security Scan Procedures

Version 1.0

December 2004

Payment Card Industry Security Scanning Procedures



Disclaimer

The Payment Card Industry (PCI) Security Scanning Procedures is to be used as a 'guideline' for all entities that store, process, or transmit Visa cardholder data conducting network security scans to meet PCI requirements. Visa Asia Pacific, however, makes no warranty or claim that completion of network security scans will prevent security breaches or losses, and disclaims any responsibility or liability for any security breaches or losses incurred, whether the result of scans is compliant or not.

Important

The Payment Card Industry (PCI) Security Scanning Procedures is part of Visa Asia Pacific's Account Information Security (AIS) documentation suite. All Members and their agents (merchants and service providers) must ensure they process, store and transmit cardholder information in accordance with the PCI Data Security Standard (this standard supercedes Visa's AIS Standard v1.4, March 2000).

For more information on Visa Asia Pacific's AIS program please visit <http://www.visa-asia.com/secured>.



Objective and Audience

This document identifies the procedures and guidelines for conducting network security scans in compliance with Payment Card Industry (PCI) requirements.

The intended audience of the document is merchants and third party service providers who are scanning their infrastructures to demonstrate compliance.

Introduction

The PCI Data Security Standard details security requirements for members, merchants, and service providers that store, process or transmit cardholder data. To demonstrate compliance with the PCI Data Security Standard, merchants and service providers may be required to conduct network security scans on a regular basis as defined by each payment card company.

Network Security Scans are an indispensable tool to be used in conjunction with a vulnerability management program. Scans help identify vulnerabilities and mis-configurations of web sites or IT infrastructures containing externally facing IP addresses.

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

Network Security Scans apply to all merchants and service providers with external-facing IP addresses. Even if an entity does not offer Web-based transactions, there are other services that 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. These seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems and potential expose cardholder data if not properly controlled.



Scanning Procedures

To be considered compliant with the network scanning requirement, merchants and service providers must scan their web sites or IT infrastructures with externally facing IP addresses, according to the following guidelines:

1. All scans must be conducted by a third party compliant network security scanning vendor, selected from the list of approved vendors on https://sdp.mastercardintl.com/vendors/vendor_list.shtml. All compliant scanning vendors are required to conduct scans in accordance with a defined set of procedures. These procedures dictate that the normal operation of the customer environment is not to be impacted and that the vendor should never penetrate or alter the customer environment
2. Quarterly Scans are required for all merchants and service providers whose average monthly transaction volume exceeds 10,000.
3. If network or application modifications are made to the production environment, additional scans may be required to ensure that new vulnerabilities are not introduced into the infrastructure.
4. Prior to scanning the web site and IT infrastructure, merchants and service providers must;
 - Provide the scan vendor with a list of all active externally facing IP addresses.
 - Request the scan vendor to determine the entire externally facing IP range through network probing to determine which IP addresses and services are active.
5. Contract with the vendor to perform periodic scans of all active IP addresses and devices
6. Scan all filtering devices such as firewalls or external routers (if used to filter traffic). If using a firewall or router to establish a DMZ, these devices must be scanned for vulnerabilities.
7. 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 critical.
8. Scan application servers if present.

Application servers act as the interface or "middle-man" 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 could potentially store credit card data.



Some Web site configurations do not include application servers; the Web server itself is configured to act in an application server capacity.

9. Scan all custom Web applications.

The most elusive vulnerabilities are those introduced through a custom-developed e-commerce application of the merchant or service provider.

10. Scan Domain Name Servers (DNS).

DNS servers resolve Internet addresses by translating domain names into Internet Protocol (IP) addresses. Merchants or service provider 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 potentially spoof a merchant or service provider Web page and collect credit card information.

11. 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.

12. Scan all Load Balancers.

To increase the performance and the availability of an environment, a load balancer can spread the traffic load to more than one physical server. If the environment of the merchant or service provider is using a load balancer, merchants and service providers should scan all individual servers behind the load balancer.

Failure to scan all physical servers behind the load balancer could leave vulnerabilities undetected.

13. Scan Virtual Hosts.

All merchants whose websites are hosted must request their hosting provider to scan their entire externally facing infrastructure and demonstrate compliance.

It is common practice when using a hosted environment that one server contains more than one Web site. In this case, the merchant shares the server with other customers of the hosting company. This could potentially lead to an exploit of the server through Web sites other than the merchants.

14. Scan Wireless Access Points in wireless LANs (WLANs).

Usage of WLANs introduces new data security risks that need to be identified and mitigated. Merchants, processors, gateways, service providers and other entities must scan their wireless components to identify potential vulnerabilities and mis-configurations.

15. Configure the IDS/IPS in a way to accept the originating IP address of the scan vendor. Should this not be possible, the scan should be originated in a location which prevents the IDS/IPS from interfering with its actions



Compliance Reporting

Acquirers, merchants, and service providers will 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. Please contact your acquiring bank or check each payment card company's regional website to determine to whom the results should be submitted.

Reading and Interpreting Reports

Approved network scan vendors are able to produce an informative report, based on the results of the network scan

The scan report will describe 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.

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

The following table suggests how a compliant network scan solution may categorize vulnerabilities. This table is provided to demonstrate the types of vulnerabilities and risks which are considered high-level.

To be considered compliant, a scan must not contain high-level vulnerabilities. In the below example, this translates into vulnerabilities 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 and denial of service (DoS)
2	Medium	Sensitive information can be obtained by hackers on configuration
1	Low	Information can be obtained by hackers on configuration



- 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 also 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.*