ASV external vulnerability scans

Approved Scanning Vendor external vulnerability scans explained

David Morris, PCI Compliance Analyst

Why do I have to do this?

It is a requirement of the Payment Card Industry Data Security Standard (PCI DSS) that any Internet-facing or externally accessible points of the Cardholder Data Environment must be scanned by an Approved Scanning Vendor (ASV). The ASV looks for vulnerabilities, or weaknesses, that could be misused by someone on the Internet to gain access to your Cardholder Data Environment and potentially to cardholder data. If you business operates an internet-facing payment environment, then regular external vulnerability scans of that environment might be required. Scanning and fixing the vulnerabilities identified will help to protect your Cardholder Data Environment against potential breaches.

What is a Cardholder Data Environment? The PCI DSS defines this environment as, 'the people, processes and technologies that store, process or transmit cardholder data and sensitive authentication data.' That is the environment that contains your cardholder data acceptance and processing systems.

The requirement to be scanned by an ASV is set out in 11.2.2 of the PCI DSS and reads as follows:

11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.

> 11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12- month period.
>
> 11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures).
>
> 11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).

The PCI DSS requires that these scans be conducted by a scanning vendor that the PCI Security Standards Council (SSC) has approved and trained: an ASV. The reason for this is that external networks are susceptible to a greater risk of compromise. The ASV must deploy a scan solution that fulfils all of the requirements of the ASV Program Guide, has been tested and approved by the PCI SSC and which is in adherence with the quality assurance program established and maintained by the PCI SSC.

To clarify, the external vulnerability scan requirement set out by PCI DSS 11.2.2 applies to any environment where cardholder data is stored, processed or transmitted and which has Internet-facing or externally accessible points of access. If your business stores, processes or transmits cardholder data at several locations (i.e. at multiple retail stores) then the external IP addresses for all of those locations must be scanned.

However, if your business is eligible to assess PCI DSS compliance for your internet-connected

Cardholder Data Environments using the Self-Assessment Questionnaire (SAQ) A, C-VT or P2PE, then you are not required to perform these external network vulnerability scans.

Where your cardholder data environment is externally hosted, it is permitted for your hosting provider to undergo the ASV external vulnerability scans on its own. They must be able to provide you with evidence of compliant ASV scans of your hosted environment. If you follow this approach, it is your responsibility to make sure that all of your Internet-facing IP ranges and domains have been scanned as part of the hosting provider's own passing ASV scans.

How do I do this?

Define the scope of your scan

The first step in undertaking an external vulnerability scan is to determine the scope of the scan. This is done by identifying the IP addresses or domain names for the points of the Cardholder Data Environment which are externally accessible. It is not always obvious which points of the Cardholder Data Environment are externally accessible. If a system is within the Cardholder Data Environment or connected to it and is internet-facing, it must then be scanned in order to fulfil PCI DSS requirement 11.2.2. This is the basic criterion for identifying the correct scan targets.

A common misconception is that the external vulnerability scan applies only to Internet-facing IP addresses and fully qualified domain names (e.g. mail.mybusiness.com or www.myshop.com) of the systems that are directly involved in the storage, processing or transmission of cardholder data. The reality in fact is that your Cardholder Data Environment consists of both systems and the network connecting those systems. The entire network and any Internet-facing systems that are part of that network, whether directly within the Cardholder Data Environment or providing a pathway to your Cardholder Data Environment, must be scanned by the ASV.

You may exclude Internet-facing or externally accessible systems from the ASV scan scope only if those systems are not part of, and are not connected to, the Cardholder Data Environment. Segmentation to exclude systems from the scan scope can be done through either physical or logical means. For example, physical segmentation of the Cardholder Data Environment through use of physically separate internet connections so that no physical connectivity exists between the in-scope environment and other systems in your business. Logical methods of segmentation include using properly configured internal network firewalls, routers with strong access control lists, or other technologies that enforce the restriction of access to/from a particular network segment.

Ultimately, it is your responsibility as the scan customer and business wishing to achieve PCI DSS compliance, to establish the scope of your scan. However, you should raise any questions you have regarding what constitutes proper segmentation with your ASV.

Review the scan and fix the vulnerabilities

Once the scan has been completed, the next step in the process is to review the scan report issued by the ASV. The scan will report all confirmed and potential vulnerabilities each of which is assigned a severity level. The severity level is used to determine whether you have achieved a passing scan or not. A vulnerability is classed as a fail if it receives a Common Vulnerability Scoring System (CVSS) score (or severity level) of 4.0 or higher, or has been deemed by the ASV to be an automatic fail in accordance with the PCI DSS. You need to address all failing vulnerabilities that have been detected during the scan.

For each failing vulnerability, you must either implement a solution for the failing or dispute the finding. The scan report will describe the type of vulnerability or risk, diagnose the associated issues, and provide guidance on how to fix or patch the vulnerability. The ASV must perform a repeat or re-scan to demonstrate that your solutions have been effective, resulting in a passing scan.

You may dispute the failing scan results with your ASV in a number of ways including:

- By raising a false positive to indicate that a vulnerability has been incorrectly found. You will need to provide detailed and accurate evidence to support your claim.

- By providing detailed information on the compensating controls you have in place that reduce or eliminate the risk presented by the vulnerability. The ASV will assess the relevance and applicability of the compensating controls.

- By raising an exception, supported by evidence that the failing does not pose a risk to the Cardholder Data Environment, which may be accepted by the ASV.

Confirm and attest your passing scan result

Once you have achieved a passing scan, the final step in the process is confirming and attesting the scan result. This step is the confirmation by both you and the ASV that the scan was performed against the correct scope for your Cardholder Data Environment, that the scan was properly carried out in accordance with the ASV Program Guide, that the information provided by you and reported by the ASV in the scan report is an accurate reflection of the scanned environment.

Please note that a passing scan may be reported where the IP addresses scanned are found as ‘hosts not alive’. While this result may be valid and reflect a highly secure, locked down network, it may also be caused by configuration issues and not be a true result. For example, your ISP may assign dynamic IP addresses to your external router. If that router has been shut down since you last checked your external IP address, it may now have a different IP to the one expected; hence your currently assigned IP address may not have been included in the scan, resulting in a ‘hosts not alive’ report.

Once the passing scan report is attested you will have achieved a fully compliant result, allowing you to validate your compliance with PCI DSS requirement 11.2.2. In order to maintain scan compliance, you must run an ASV scan, resolving identified failing vulnerabilities and attesting the passing ASV scan report each quarter, as described above.

What are my responsibilities to ensure a valid scan result?

For the scan to be successfully and accurately performed, you need to ensure that you have no system or technology in place that could interfere with the scan. For example, your network may be protected by 'active protection systems' such as firewall port scan or intrusion prevention systems that could interfere with the scan, meaning that the scan results may not truly reflect the vulnerabilities and weaknesses in your internet-facing Cardholder Data Environment,

Due to time constraints, the scan process generates a lot of activity that is easily detected by network traffic monitoring and active protection systems. You may need to temporarily reconfigure these 'active protection systems' to allow the scan to be performed unimpeded. Temporary changes should only be made to offset the response of your active protection systems to this 'noisy' activity specifically. The purpose of making these temporary adjustments is to allow the ASV scan the same degree of access as an attacker with no time constraints could achieve. An attacker will typically approach a network target with stealth using techniques that may not trigger or be detected by traffic monitoring and active protection systems.

The active protection systems that could interfere with the scan include, but are not limited to, the following list of examples provided by the PCI SSC:

- Intrusion prevention systems (IPS) that drop non-malicious packets based on previous behavior from originating IP address (for example, blocking all traffic from the originating IP address for a period of time because it detected one or more systems being scanned from the same IP address)
- Web application firewalls (WAF) that block all traffic from an IP address based on the number of events exceeding a defined threshold (for example, more than three requests to a login page per second)
- Firewalls that shun/block an IP address upon detection of a port scan from that IP address
- Next generation firewalls (NGF) that shun/block IP address ranges because an attack was perceived based on previous network traffic patterns
- Quality of Service (QoS) devices that limit certain traffic based on traffic volume anomalies (for example, blocking DNS traffic because DNS traffic exceeded a defined threshold)
- Spam filters that blacklist a sending IP address based on certain previous SMTP commands originating from that address

Any reconfiguration changes to these 'active protection systems' are only to allow the scan to be performed unimpeded and are required only for the duration of the scan. You do not need to make any changes to 'static' systems, such as your firewall, that protect your Cardholder Data Environment by consistently blocking or controlling network traffic based on established rules. Coordination with your ISP or hosting provider may also be required to allow the ASV scan to be performed without interference from their active protection systems. This will ensure that the scan result is an accurate reflection of your network's security.

It is your responsibility to resolve any inconclusive or incomplete ASV scan results. Load balancing technologies, able to distribute incoming network traffic across a number of servers or systems, can impact the scan process. Load balancing can result in a partial assessment of the systems behind the load balancer, or prevent the full range of in-scope IP addresses from being detected or seen by the scanner. The ASV requires you to identify any use of load balancing technologies. You must provide assurance to the ASV that the configuration and use of load balancing has not prevented the successful scanning of all in-scope IP addresses and domains.

What are the benefits of the scan process?

Aside from being a requirement for businesses for whom PCI DSS requirement 11.2.2. is mandated, maintaining compliance with the PCI DSS External Vulnerability scan requirement will greatly assist you in maintaining the security of your network. The ASV scan reports provide useful information for protecting your networks from Internet-based attacks, identifying known weaknesses and exploitable vulnerabilities and providing guidance to help you resolve them. Added to that ASV scan reports can provide evidence of the effectiveness of your, or your third-party provider's, vulnerability and patch management processes. Utilising these standards in the management of payment card processing infrastructures will ultimately reduce the risk of a data breach impacting your business and help protect your customers' payment card data.

Notes/Additional Information/Further Reading:

1) The following article on revision 1.1 of version 3.2 of the PCIDSS provides useful illustrations and guidance on the fundamentals of determining the scope of the Cardholder Data Environment and network segmentation: https://sysnetgs.com/wp-content/uploads/2017/03/PCI-DSS-v3.2-revision-1.1-SAQs.pdf

2) For the official and comprehensive guide to the ASV scan process, please see https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

“Sysnet builds and supports mutually beneficial relationships between our clients and their customers globally through market-leading software, end-to-end services and best-in-class support.”

Email: info@sysnetgs.com
Phone: +353 1 495 1300 | +1 404 991 3110
Web: sysnetgs.com

sysnet® global solutions