ControlScan

How does a penetration test differ from a vulnerability scan?

Penetration testing and vulnerability scanning are both required by the Payment Card Industry Data Security Standard (PCI DSS), but there is often confusion about the differences between the two services. This document offers clarification on how to differentiate between the two.

A vulnerability scan looks for known vulnerabilities in your systems and reports potential exposures. A penetration test is intended to exploit weaknesses in the architecture of your IT network and determine the degree to which a malicious attacker can gain unauthorized access to your assets. A vulnerability scan is typically automated, while a penetration test is a manual test performed by a security professional. Here's a good analogy: A vulnerability scan is like walking up to a door, checking to see if it is unlocked and stopping there. A penetration test goes a bit further; it not only checks to see if the door is unlocked, but it also opens the door and walks right in.

View the chart below for a side-by-side comparison of the two services.

	Vulnerability Scan	Penetration Test
Purpose	A vulnerability scan looks for known vulnerabilities in your systems and reports potential exposures that, if exploited, could result in a compromise of a system. The scan ranks and reports each vulnerability. An external vulnerability scan is conducted from outside the organization. An internal vulnerability scan is conducted from inside the organization.	A penetration test is a simulated attack against your network infrastructure or information systems that attempts to evade or overthrow the security features of system components. It is designed to exploit discovered weaknesses and determine your level of risk. It can be performed internally or externally.
Who	A vulnerability scan is performed using a combination of automated tools. A Managed Security Service Provider (MSSP) or qualified technician then manually reviews and confirms the results. In order to achieve PCI DSS compliance validation, an external vulnerability scan must be conducted by an Approved Scanning Vendor (ASV), and you and your ASV must attest to the scan results.	A penetration test is performed by a "White-hat Hacker" or "Ethical Hacker" who is skilled at accessing systems and networks using a variety of tools and techniques. Vulnerability scanning may be utilized by an ethical hacker as one method of finding potential attack vectors.

	Vulnerability Scan	Penetration Test
When	Vulnerability scans should be conducted continuously, but at least quarterly, especially after installing new equipment or making any other significant changes.	On average, penetration tests should be performed at least once a year and especially after installing new equipment or making any significant changes. Effective 1/2018, the PCI DSS will require service providers to test segmentation bi-annually.
Cost	Relatively low cost. Depending on scope, scans can cost hundreds to thousands of dollars annually.	Moderate to high cost. Depending on scope size, it can cost thousands to tens of thousands of dollars for each penetration test.
Value	Vulnerability scans identify areas of risk either within your network or areas outside of your network that could be exploited by a hacker.	A penetration test identifies your risk exposure and gives you full visibility into how malicious entities may be attacking your systems and to what extent they are at risk.
Reporting	The output is a comprehensive report that outlines any vulnerabilities that exist and may be exploited (software, expired patches, etc.).	The report details level of risk and potential exposure by ranking vulnerabilities high, medium or low. It identifies what high vulnerabilities could be exploited and how, and what data can be compromised (if any).
Regulation Requirements	PCI DSS 11.2	PCI DSS 11.3 11.3.1 for External Penetration Testing and 11.3.2 for Internal Penetration Testing

To further simplify what's included with each solution, check out the chart below.

	Vulnerability Scan	Penetration Test
Automated tools used to identify vulnerabilities	✓	✓
Scheduled (quarterly (PCI)) or on-demand service	✓	
Manual exploitation of identified vulnerabilities		✓
Performs "attacks" on external or internal systems (tries fake passwords, manipulates code, "tricks" web servers into giving sensitive information)		✓
Provides assurance on segmentation within a network or environment		✓

For more information about vulnerability scans and penetration tests, or to receive a complimentary assessment of your current security and compliance posture, give us a call at 800-825-3301 x 2 or visit www.controlscan.com.