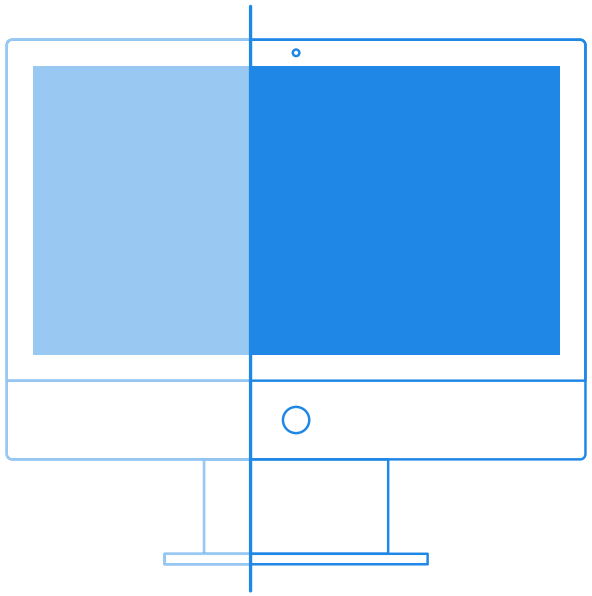
VULNERABILITY SCANNING 101

Best practices to secure against a data breach



securityMETRICS®

INTRODUCTION

PCI DSS Requirement 11.2 requires organizations that store, process, and/or transmit cardholder data electronically to run internal and external vulnerability scans.

Vulnerability scanning is one of the easiest ways to predict how hackers might get into your system. But vulnerability scanning isn't just about locating vulnerabilities in your environment; it's about remediating and changing your processes to ensure vulnerabilities are addressed on a prioritized basis.

In this white paper, you will learn the basics about vulnerability scanning, how vulnerability scanners work, how you can best perform vulnerability scanning, and tips to manage your network vulnerabilities.

VULNERABILITY SCANNING BASICS

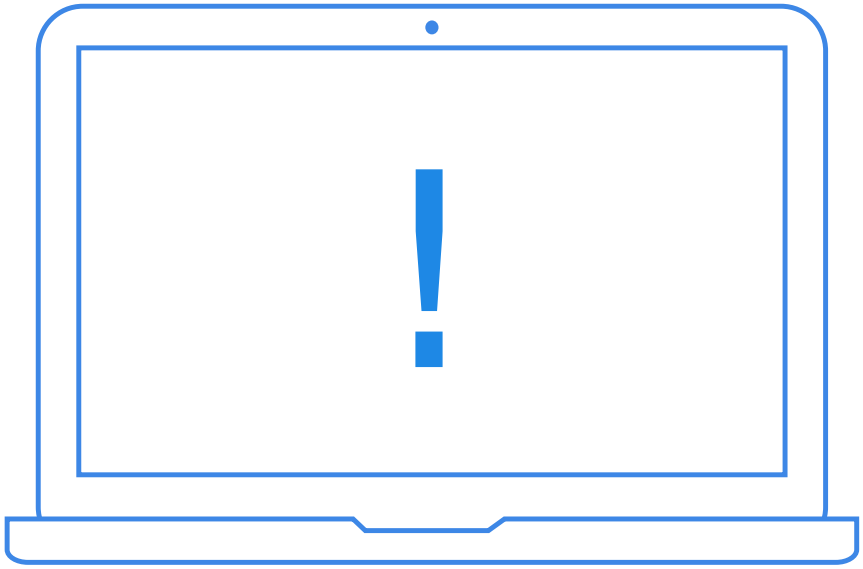
WHY ARE VULNERABILITY SCANS NECESSARY?

Based on data collected by SecurityMetrics Forensic Investigators from last year's breaches, it took an average of 166 days from the time an organization was vulnerable for an attacker to compromise the system. Once compromised, attackers had access to sensitive data for an average of 127 days.

These system compromises can and often do lead to irreparable brand damage and expensive data breach fines to breached organizations. Many of these compromises could have been avoided if they had tested their environment (e.g., vulnerability scans).

Due to inherent security weakness in systems or technology, some organizations have systems, environments, software, and/or website weaknesses that can be exploited by attackers from the day their environment is set up.

In other cases, an organization becomes vulnerable because they fail to apply a security patch or make system modifications without properly updating related security protocols.



To reduce your risk and prevent a data breach, critical vulnerabilities must be continuously identified, prioritized, and remediated.

Without regular vulnerability scanning, your probability of being exploited and compromised increases considerably. This is because there are an average of 19 new vulnerabilities reported daily, which can then be exploited (e.g., Heartbleed, WannaCry, Petya).

For example, here were the top five failed vulnerabilities from last year that SecurityMetrics customers discovered after they performed their vulnerability scans:

- **TLS version 1.0 protocol detection:** Exists if the remote service accepts connections using TLS 1.0 encryption
- **SSL certificate with wrong hostname:** Happens when a SSL certificate for the tested service is for a different host
- **Web application potentially vulnerable to clickjacking:** Occurs if a remote web server does not set an X-Frame-Options response header in all content responses
- **SSL RC4 Cipher Suites Supported (i.e., Bar Mitzvah Attack):** Exists when the RC4 encryption algorithm is used in SSL/TLS transmission
- **SSL Self-Signed Certificate:** Occurs when organizations use an identity certificate that they create, sign, and certify rather than a trusted certificate authority (CA)

Often, attackers use the same vulnerability scanning tools that organizations are required to use to discover network vulnerabilities.

To keep ahead of attackers, you need to keep up to date on emerging vulnerabilities by regularly running internal and external vulnerability scans.

WHAT DOES A VULNERABILITY SCAN DO?

A vulnerability scan is an automated, high-level test that looks for and reports potential known vulnerabilities. For example, some vulnerability scans are able to identify over 50,000 unique external and/or internal weaknesses (i.e., different ways or methods that hackers can exploit your network).

PCI DSS requires two independent methods of PCI scanning: internal and external scanning. An external vulnerability scan is performed outside of your network (e.g., at your network perimeter), and it identifies known weaknesses in network structures. An internal vulnerability scan is performed within your network, and it looks at other hosts on the same network to identify internal vulnerabilities.

Think of your environment as a house. External vulnerability scanning is like checking to see if doors and windows are locked, while internal vulnerability scanning is like testing if bedroom and bathroom doors are locked.

Typically, vulnerability scans generate an extensive report of found vulnerabilities and gives references for further research on these vulnerability. Some even offer directions for how to fix the problem.

Despite what many businesses believe, scanning isn't enough. You shouldn't just scan and sit on the report. Act quickly on any discovered vulnerabilities to ensure security holes are fixed, and then re-scan to validate that vulnerabilities have been successfully addressed.

Vulnerability scanning identifies potential harmful vulnerabilities, so that you can remediate processes to ensure network security.

PROS OF VULNERABILITY SCANNING
Quick, high-level look at possible vulnerabilities
Very affordable compared to penetration testing
Automatic (can be automated to run weekly, monthly, quarterly)

CONS OF VULNERABILITY SCANNING
False positives
Businesses must manually check each vulnerability before testing again
Does not confirm a vulnerability is possible to exploit

VULNERABILITY SCANNING VS. PENETRATION TESTING

Some mistakenly believe vulnerability scanning is the same thing as a professional penetration test.

Here's the difference: A vulnerability scan is automated, while a penetration test includes a live person actually digging into your network's complexities.

A vulnerability scan only identifies vulnerabilities, while a penetration tester digs deeper to identify the root cause of the vulnerability that allows access to secure systems or stored sensitive data.

Vulnerability scans and penetration tests work together to improve network security. Vulnerability scans offer great weekly, monthly, or quarterly insight into your network security, while penetration tests offer a more thorough examination of your network security.

HOW DO VULNERABILITY SCANNERS WORK?

Unlike antivirus software, vulnerability scanner doesn't check every network file. Your scanner must be configured to scan specific interfaces, such as internal or external IP addresses (e.g., ports and services), for vulnerabilities.

Vulnerability scanning technology includes different tools and scripts designed to check for vulnerabilities. These tools can include PCI Approved Scanning Vendor (ASV) operated tools, command line scripts, GYI interfaces, open source technologies, and scanning tools (e.g., Nessus).

Scanning tools run a series of if-then scenarios on your systems (i.e., a vulnerability scan), which typically takes 1-3 hours to perform.

These if-then scenarios should identify system settings or actions that could lead to system exploitation. For example, if your scan checks for outdated operating system versions and discovers an Windows XP operating system on a workstation, it will flag the operating system as vulnerable.

Vulnerability scans are designed to be nonintrusive, similar to a security professional checking if your front door is unlocked and letting you know if it is (while not entering your environment). Vulnerability scans search your network and provides a logged summary of alerts for you to act on. Unlike penetration testing, a vulnerability scan doesn't exploit vulnerabilities in your network.

As you review your scan results, you may notice common vulnerability and exposure (CVE) numbers in your alerts or report. If you have questions about these CVE records, visit the National Vulnerability Database to help you identify and prioritize your risks if your product/vendor doesn't offer this for you.

7 TIPS TO MANAGE VULNERABILITIES

When managing your network security, a vulnerability management plan is vital for your organization's security and compliance efforts. Follow these 7 tips to best discover existing and potential weaknesses in your network.

1. CONFIRM YOUR SCOPE

PCI DSS requires you to run vulnerability scans on in-scope networks, processes, and systems. In-scope systems are directly involved in the cardholder data environment (CDE), meaning that the system component stores, processes, or transmits cardholder data. The system can also be on the same network segment as systems that deal with cardholder data.

These types of systems are all part of the CDE, and they need to follow all applicable PCI DSS requirements to protect cardholder data.

Sample systems considered in-scope:

- POS devices
- Servers containing card data
- Firewalls providing segmentation of the CDE

When defining your PCI DSS scope, you should consult with a security professional, such as PCI DSS Qualified Security Assessors (QSAs). If you don't properly scope your environment, your scans might overlook important networks and what needs to be scanned to attest PCI compliance.

Most small organizations don't need to worry about this issue because they typically set up a flat network (i.e., where everything inside a network can connect to everything else). When organizations have flat networks, their entire network must be scanned.

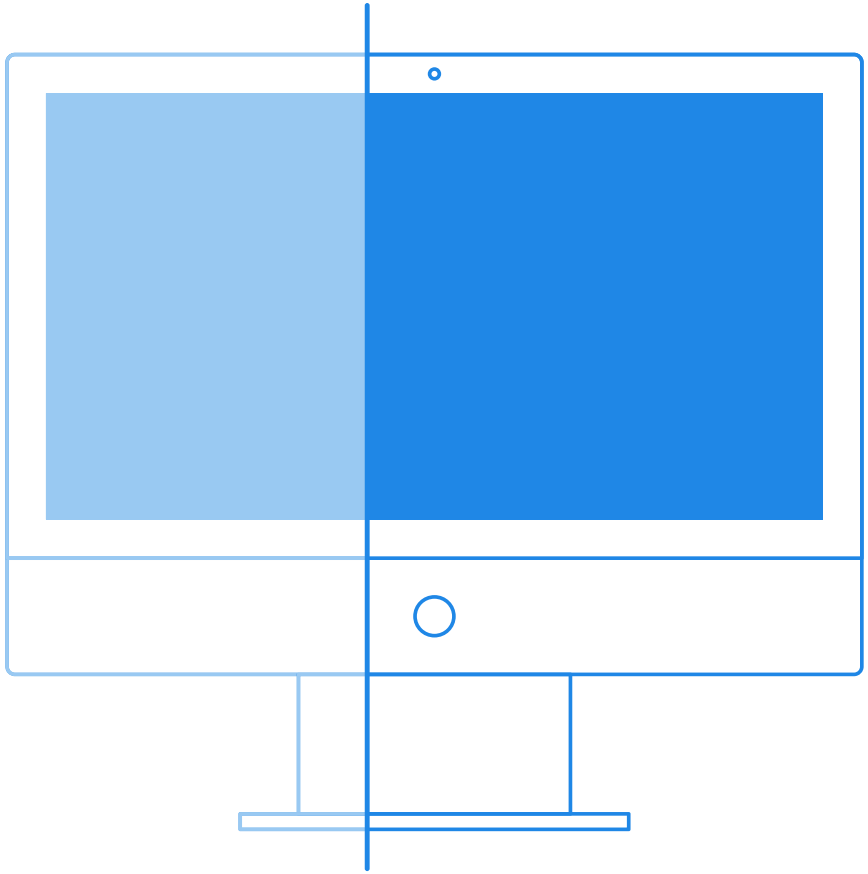
Complex networks using segmentation to reduce their PCI DSS scope should pay attention to how and if their scope changes throughout the year, then adjust vulnerability scans accordingly.

2. RUN EXTERNAL VULNERABILITY SCANS

External scans must be performed by a PCI Approved Scanning Vendor (ASV) to validate your PCI compliance.

An ASV is required to go through a rigorous yearly recertification process, during which each ASV runs their PCI scanning tool on PCI Council-approved sites riddled with vulnerabilities to test which vulnerabilities the tool finds and/or misses.

But just because an ASV runs your external vulnerability scan, this doesn't mean your organization is secure. After receiving your scan report, you're responsible for fixing any discovered vulnerabilities and then rescanning until vulnerabilities have been properly addressed.



3. RUN INTERNAL VULNERABILITY SCANS

One of the biggest misconceptions with vulnerability scanning is thinking that "If my ASV does my PCI scans, that must mean I'm compliant." If your ASV currently performs your external quarterly scans, understand they're likely not handling your internal quarterly vulnerability scanning.

You may have an internal vulnerability scanning tool or appliance (e.g., SecurityMetrics' Vision) set up inside your network by your ASV, but chances are they're not handling or monitoring your internal vulnerability scanning requirements. Make sure that your internal vulnerability scans are actually being routinely performed.

There are a variety of tools to help you comply with internal vulnerability scan requirements. For example, you can:

- Purchase an internal vulnerability scanning tool from your ASV or another service provider
- Download an open source internal vulnerability scanning tool

Keep in mind that the tool you use still needs to be configured by a security expert after you purchase or download it. If you purchase a vulnerability scanning tool/appliance, IT support service is typically included. If you download scanning tools, take time to research and implement configuration best practices.

Remember, your organization is in charge of internal vulnerability scanning from initial download/purchase, configuration, actual scanning, alert analysis, to vulnerability management.

4. INDEPENDENT AND QUALIFIED TESTING

Internal vulnerability scanners should be handled only by a qualified person independent of the scanned target (e.g., device, component, network).

Basically, the person managing your vulnerability scanner should be separate from the person managing and/or remediating any discovered vulnerabilities.

For example, if run an internal scan on your firewalls, you can either choose a qualified security professional (e.g., your ASV) or a qualified employee who's not in charge of firewall administration. Basically, if an employee is not independent of the scanned system, they cannot run the scan.

It doesn't matter if you only have one IT employee doing the job of 15 employees. If they're not independent from managing the system, they shouldn't administered the scans.

5. REGULARLY RUN VULNERABILITY SCANS

Every organization should run quarterly internal and external scans. If you only had a single target, that would be eight total scans per year (i.e., one internal and one external scan per quarter).

Many organizations routinely run quarterly external vulnerability scans, but they often overlook running internal vulnerability scans. Others think vulnerability scanning is an occasional spot check process, focusing on addressing immediate issues (e.g., WannaCry ransomware).

Remember, Requirement 11.2 requires you to run at least four passing external vulnerability scans per year (i.e., one per quarter), and four passing internal vulnerability scans per year (i.e., one per quarter), and all of your scans need to be in a passing state.

Many vendors allow unlimited vulnerability scanning for a single target, so if you fail your first scan, make sure to remediate your network's vulnerabilities and then re-scan until passing. You'll likely need to run additional scans beyond your quarterly vulnerability scans.

On average, it took SecurityMetrics customers 1.68 scans and 11 days to achieve a passing scan.

6. RUN SCANS AFTER SIGNIFICANT NETWORK CHANGES

In addition to running your vulnerability scans quarterly, scans need to be run after any significant change.

What defines a significant change? A significant change depends on how your environment is configured. But in general, "if an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant."

Scanning after significant changes means it should happen within a reasonable timeframe. If you make significant changes to your system the day after your quarterly internal or external scan, test your changes and scan that week.

Here are some examples of significant changes:

- Adding new servers or system components
- Modifying firewall rules
- Changing network structures
- Altering interfaces
- Transferring cardholder data to a new server
- Upgrading products
- Changing your firewall product
- Adding middleware (e.g., JBOSS)
- Removing/instituting new systems that store cardholder data
- Adding encryption applications

Here are some examples of non-significant changes:

- Switching file integrity monitoring products
- Changing antivirus products
- Removing terminated administrative employees from configurations

7. ESTABLISH A TOP-DOWN APPROACH

When it comes to gaining executive support, IT departments often have trouble enforcing security-related policies and procedures.

Your IT team needs to have executive approval and support to perform regular vulnerability scanning and making necessary organizational changes when vulnerabilities are found.

Remember, your IT team would need a significant amount of time to repair and recover from vulnerability exploitation (i.e., a data breach), which would have a far greater impact on your organization than the amount of time it takes to regularly find and fix vulnerabilities.

CONCLUSION

Because cybercriminals discover new and creative ways to hack businesses daily, it's important to scan your network often.

Remember, vulnerability scanning isn't just about locating and reporting vulnerabilities. It's also about establishing a repeatable and reliable process for fixing problems.

After a vulnerability scan finishes, it's crucial to fix any located vulnerabilities on a prioritized basis. Start by prioritizing vulnerabilities based on risk and required effort; then, run scans until results are clean.

ABOUT SECURITYMETRICS

We help customers close security and compliance gaps to avoid data breaches. Our forensic, penetration testing, and audit teams identify best security practices and simplify compliance mandates (PCI DSS, HIPAA, HITRUST, GDPR). As an Approved Scanning Vendor, Qualified Security Assessor, Certified Forensic Investigator, we have tested over 1 million systems for security.

https://www.securitymetrics.com/pci-audit