TRAVA

Trava's Complete Guide: Vulnerability Scan Types

Stellar product.
Better people.

TABLE OF CONTENTS

Trava makes it easy for business leaders to create, enhance, and integrate cyber risk management programs that protect their company data from people who should not have access.

Malicious actors are getting more sophisticated and more aggressive, evidenced by the rising number of small and medium-sized businesses that are falling victim to cyber attacks—two out of every three last year, according to one study.1 Trava's automated assessments that check for vulnerabilities in external and internal environments predict how malicious actors might get into a system, informing better defenses against cyber threats.

This ebook details:

- A description of each scan type
- The benefits of performing each scan
- Recommended frequency for running each scan

External and Internal Scanning

provide insights for building better defenses by predicting how malicious actors might get into your system.

WHAT ARE THESE TYPES OF SCANS?

- **External Infrastructure Vulnerability Scans**
  are performed from outside of the network you are testing. These scans are targeted at your network's external IP addresses. Users will find useful information from these scans about vulnerabilities as well as a list of ports that are open to the internet.
- **Internal Network Vulnerability Scans**
  are performed from a location that has access to the internal network you are scanning. These scans show vulnerabilities at a greater depth as they can "see" more of the network compared to an external scan only.

WHAT ARE THE KEY INSIGHTS FROM EXTERNAL AND INTERNAL SCANS?

- **External Scans**
  - Weaknesses in your systems that could help avoid a potential incident.
  - Pressing security issues.
  - Changes like services or server setup and whether they present any new threats to the organization.
- **Internal Scans**
  - Known vulnerabilities that could compromise your network.
  - Patch trends and missing patches that need attention.
  - Verification that all issues are patched properly and are up to date.

WHOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- **External Scans**
  - Monthly
- **Internal Scans**
  - Weekly

01

WHY?

Organizations that scan with a steady cadence remediate flaws on average 15.5 days faster.

Certificate Scan

A digital certificate is a digital authentication tool that serves two primary functions. It authenticates the identity of the server. And the certificate binds a key pair (public and private) to that server.

Certificates are used to provide secure communication to your websites.

WHAT ARE THE KEY INSIGHTS FROM A CERTIFICATE SCAN?

- Discover all the certificates installed across various endpoints in your network and detect known vulnerabilities exposed by your certificates.
- Record certificate location, health, type, days to expiration, and position in the chain of trust.
- Ensure that your certificates are running the most current version.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Quarterly and whenever existing certificates are updated or new certificates are installed

WHY?

01

Certificates are used to provide secure communication to your websites. Certificates are fairly set once installed.

Breach Scan

A data breach is a successful cyber attack in which the malicious actors were able to gain access to and steal protected data. Malicious actors can target organizations of any size. The common types of data exposed in public breaches include personal information, health information, financial information, intellectual properties, usernames, passwords, and many more. Breach scans identify if any of your organization accounts have been compromised through a breach.

WHAT ARE THE KEY INSIGHTS FROM BREACH SCANS?

- Find out if any of your company's or employees' account has been compromised and is being sold/accessed on the dark web.
- Identify other characteristics of the breach that may have a negative impact (date of breach, compromised data types, whether it contains sensitive information)

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Weekly, at a minimum.

WHY?

Catching compromised accounts early is critical in preventing unauthorized access to user accounts.

Cloud Scan

WHAT IS THE PUBLIC CLOUD?

The public cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public internet without buying and maintaining computer hardware.

With the rapid shift to the cloud that many companies are making, security is often overlooked or misunderstood. A cloud scan analyzes your public cloud configuration to make sure it is set up correctly. It will look for any configuration settings that could expose your data or make you vulnerable to malicious actors. Beyond data exfiltration, malicious actors can also use your cloud environment to launch a variety of criminal activities.

WHAT ARE THE KEY INSIGHTS FROM PUBLIC CLOUD SCANS?

- Verification that your cloud environments are configured in a secure way, or if there are security vulnerabilities in your configurations.
- Ability to identify any of your cloud resources that may be inadvertently exposed to the world.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Weekly and whenever your cloud environment is significantly changed

01

WHY?

Don't overlook cloud security. Malicious actors can use your cloud environment to launch a variety of criminal activities.

Web Application Scans

WHAT IS A WEB APPLICATION?

A web application provides some kind of web-based service to users or customers. This could include e-commerce sites or other web-based or SaaS (software-as-a-service) applications. If your company hosts its own web application, this can greatly increase your exposure to cyber attacks.

A web application scan will crawl through all of the pages on your web app and look for security vulnerabilities. These vulnerabilities can be the result of poor coding practices or issues with commercial or open-source libraries that are used to develop your application. These vulnerabilities can allow malicious actors to breach your system and access sensitive data or services.

WHAT IS THE KEY INSIGHT FROM WEB APPLICATION SCANS?

- Verification that your web application (and the components used to develop it) are secure and not exposing vulnerabilities.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Monthly, as well as any time the web application is updated.
- Web applications are generally exposed to the internet, so they are common targets of malicious actors.
- Web application scanning is an important part of a secure Software Development Life Cycle (SDLC).

01

WHY?

Web applications are generally exposed to the internet, so vulnerabilities can allow malicious actors to access sensitive data.

Agent Scans (also known as endpoint scans)

WHAT IS AN ENDPOINT?

An endpoint is a device used to access your network and other resources, usually a laptop, desktop, or server. In addition to often containing sensitive information and being critical to your businesses operation, endpoints are frequent targets of cyber attacks.
An endpoint scan searches an endpoint for any known security vulnerabilities or configuration issues. An endpoint scan is performed by installing a small program on the device that scans for known issues on a periodic basis. Endpoint scans can be run on any Windows, Mac, or Linux computer.

WHAT ARE THE KEY INSIGHTS FROM ENDPOINT SCANS?

- Find out if any of your users have security issues on their computers.
- Expose vulnerabilities in work-from-home environments where devices are not connected to your company's network.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Weekly. This is the most effective defense against breaches that could occur due to user errors or careless behavior on local computers.
- Allows you to keep up with multiple software programs updated at different intervals.

WHY?

Agent scans are critical for exposing vulnerabilities in work-from-home environments where devices are not connected to your company's network.

WordPress Scans

WHAT IS WORDPRESS?

WordPress is a free, open-source website creation platform. On a more technical level, WordPress is a content management system (CMS) written in PHP that uses a MySQL database. Known for its ease of use, WordPress is a popular website builder for small and medium-sized businesses. This scan is specific to WordPress users.

WHAT ARE THE KEY INSIGHTS FOR WORDPRESS USERS FROM RUNNING WORDPRESS SCANS?

- Find out if any of your users have security issues on their computers.
- Expose vulnerabilities in work-from-home environments where devices are not connected to your company's network.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Monthly and whenever your WordPress site is updated.
- WordPress sites are regularly updated, and with each update comes potential for a new set of security holes.
- The number of new vulnerabilities has been increasing steadily since WPScan first started tracking in 2014. As of April 14, 2021, WPScan has reported an additional 4,400.[3]

WHY?

Regular updates can help find changes that you, WordPress, or your website hosting service have made that can leave your website vulnerable to security threats.

Microsoft 365 Scans

WHAT IS MICROSOFT 365?

Microsoft 365, formerly Office 365, is a cloud-based SaaS (software-as-a-service) subscription plan that allows use of the Microsoft Office software suite over the life of the subscription for business environments. This scan is specific to Microsoft 365 users.

WHAT ARE THE KEY INSIGHTS FOR MICROSOFT 365 USERS FROM RUNNING MICROSOFT 365 SCANS?

- Validation of your security patch deployment on applicable system components.
- Detection of known vulnerabilities and security misconfigurations.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Weekly. Malicious actors target cloud environments to launch a variety of criminal activities.

WHY?

01

Cloud environments are a common target for malicious actors to launch a variety of criminal activities.

DNS Scan

WHAT IS DNS?

The Domain Name System (DNS) is a system responsible for connecting domain names (i.e. www.travasecurity.com) to IP addresses (i.e. 1.2.3.4) and allowing users on the Internet to browse web sites and resources in an easier way rather than relying on hard-to-remember numbers. DNS is essential for email to work, as mail servers need to know where to send emails to. Additionally, DNS has features that can be used to prevent emails from being spoofed and protect organizations from phishing attacks.

WHAT ARE THE KEY INSIGHTS FOR DNS SCAN USERS FROM RUNNING DNS SCANS?

- Misconfigured or missing SPF (Sender Policy Framework) record in a domain's DNS that could lead to emails being spoofed.
- Misconfigured or missing DMARC (Domain-based Message Authentication, Reporting & Conformance) record in a domain's DNS that could lead to emails being spoofed and other deliverability issues.

HOW FREQUENTLY SHOULD YOU RUN THESE SCANS?

- Monthly and whenever your email system is updated.
- Malicious actors target organizations with missing SPF and DMARC records to use their domains to launch phishing attacks against other entities, most often their customers.

WHY?

Domains with missing or misconfigured SPF and DMARC records are often targeted and used for phishing activities.

Conclusion

No one scan will fully expose your vulnerabilities, nor will single instances or infrequent scans. In order to protect your company's data and your clients' data, run each of these automated scans on a regular cadence, prioritize according to the most severe risk level, and take immediate action to resolve vulnerabilities. This is a critical component in a comprehensive cyber risk management strategy.

References

[1] 2018 State of Cybersecurity in Small and Medium-Sized Businesses report, Ponemon Institute, LLC, November 2018

[2] Goslin, Hope, Nature vs. Nurture Tip 2: Scan Frequently and Consistently, Veracode, 7 December 2020. Retrieved 19 July 2021
www.veracode.com/blog/intro-appsec/nature-vs-nurture-tip-2-scan-frequently-and-consistently

[3] O'Driscoll, Amy, 25+ cyber security vulnerability statistics and facts of 2021, Comparitech, 14 April 2021. Retrieved 19 July 2021
www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics

Cybersecurity doesn't have to be complicated. **We'll prove it.**

433 N Capitol Ave Suite 500, Indianapolis, IN 46204
contact@travasecurity.com

www.travasecurity.com