Trustwave®
Smart security on demand

FAQ: Trustwave Vulnerability Management

April 2018

This document lists and answers common questions customers have about the Trustwave Vulnerability Management product. If you have other questions about the product, contact Trustwave Support at https://www.trustwave.com/Company/Support

Will running a scan have a negative impact on my network?

The Trustwave scan is a non-intrusive, external vulnerability scan, meaning it does not attempt to break into your network or bring your network down. You may experience some latency on your Internet connection while this scan occurs (because the scan will use a portion of your available bandwidth while it is running), but it should not affect your infrastructure or cause any devices to stop responding.

If you still have concerns, we recommend scheduling your scan for a date and time when your infrastructure is not likely to be in heavy use.

For customers who have legacy infrastructure, there is the ability to customize a scan to accommodate these environments. Contact Trustwave Support for information.

How long will the scan take?

Scanning performance depends upon the following environmental factors:

- **Bandwidth**: The network capacity that a network can transmit over a period of time and is shared by all devices using the connection. Bandwidth is represented as a certain amount of data over a set period of time. This is rarely a problem for most networks.
- **Network latency**: The time between a request being sent and the response. Network latency is affected by the number of hops between sender and receiver and the quality of the connection. In general, the longer the distance traveled the higher the latency. Networks that have high latency generally suffer from long delays during connections and can cause problems when performing vulnerability scans.
- **Types of Targets**: Different types of hosts take different amounts of times to scan, roughly based on the number of exposed services. Certain services, such as web servers with large amount of content can significantly increase scan times for a single host. Understanding how the general ratio of webservers, desktops, servers, and other network devices will help estimate scan times.

How does the scanner find vulnerabilities?

Network vulnerability scanning is a multi-step process to identify security vulnerabilities on computers and network devices. The following steps are performed during scanning:

- **System Discovery** – The first step identifies systems on the network that can be tested for vulnerabilities.
- **Service Discovery** – Next, the scanner determines which network services are available on each discovered system, such as mail and web servers.
- **Vulnerability Detection** – Next, a series of tests are performed to identify security vulnerabilities such as missing patches or misconfigurations.
- **Reporting** – Finally, a report is generated consisting of all identified vulnerabilities as well as recommendations on how to address each vulnerability.

How do you rank, categorize, and score vulnerabilities?

Vulnerabilities are scored with using the Common Vulnerability Scoring System (CVSS), an industry-wide standard for calculating vulnerability risks. (Note: Trustwave products follow CVSS 2.0.)

For PCI purposes, any vulnerability over 4.0 constitutes a PCI failure. The following table shows how CVSS scores map to PCI scan scores:

CVSS Score	Severity Level	ASV Scan Result	Guidance
7.0 through 10.0	High Severity	**Fail**	To achieve a passing ASV scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report(s) that shows a passing ASV scan).
4.0 through 6.9	Medium Severity	**Fail**	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical, until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	**Pass**	While passing ASV scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

Source: https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.0.pdf

Additional information about CVSS can be found at http://nvd.nist.gov/cvss.cfm

The scan found vulnerabilities, how do I fix them?

In the scan report, a detailed description of each vulnerability will be provided as well as the steps required to resolve the vulnerability. Additionally, external links to security resources such as CVE, OWASP, and other security sites are suggested for more details on each vulnerability.

After the vulnerabilities have been fixed, the "Rescan" button can be used to confirm if the vulnerability has been properly resolved.

What can I do if I believe some of the reported vulnerabilities are false positives or incorrect?

Due to the nature of vulnerability scanning and certain compliance requirements, there may be times when scans report vulnerabilities that are incorrect or are not valid security risks because they are mitigated through technical or non-technical controls or processes. When these cases occur, vulnerabilities can be disputed using the “Dispute Findings” button. When selected, a form will display where comments can be entered regarding the vulnerability finding. For non-PCI compliance affecting scans, these disputes will be automatically accepted. For PCI scans, a support representative will review the information provided and help resolve the issue.

In addition to disputing a single finding, multiple vulnerability findings can be selected and then disputed at the same time if they are the same finding across different hosts to quickly address vulnerabilities across multiple systems.

What IP addresses will the scans originate from?

The scan may originate from IP addresses in these ranges:

64.37.231.0/24 (64.37.231.1 through 64.37.231.254)

111.108.90.138-111.108.90.139

124.211.46.74-124.211.46.75

204.225.91.58-204.225.91.59

209.90.139.122-209.90.139.123

220.101.105.8-220.101.105.9

220.101.107.8-220.101.107.9

My scan failed because of ‘Scan Interference,’ what do I do?

Whitelist the Trustwave IP addresses where the scan is originating (see above).

We recommend ensuring that any active defense measures like IPS (Intrusion Prevention System), WAF (Web Application Firewalls), SYN Flood Protection, and similar devices are configured to allow our connections. IPS devices or modules should be set to allow our scanners’ source IP addresses but we do not recommend whitelisting these addresses on your firewall (only whitelist us on the IPS module on the firewall if there is one). Many IPS devices will block the scanner’s packets because they send so many requests in a short amount of time and some of those may be detected as suspicious or malicious since they are probing for possible vulnerabilities.

My scan failed because of “Host(s) not detected’. What do I do?

Refer to the Knowledge Base article that answers this question:https://www3.trustwave.com/support/kb/KnowledgebaseArticle20965.aspx

If your scan fails due to Host(s) not detected, you can customize your discovery options to enable a full comprehensive scan with the Advanced Configuration option in the Configuration > Scan Profile > Edit area. In some situations, this may increase the ability for hosts in your environment to become discoverable.

What is the difference between a scan series and a single scan?

A scan series is a scan that reoccurs over a set period of time. When a scan is part of a series, only the date and time can be modified for an individual scan. To modify additional scan settings, such as scan name, targets, or blackouts, the entire scan series needs to be edited. A dropdown with each scan date on the scan schedule screen can be used to navigate between a scan series and a single scan in a series.

How do I add additional scan profiles?

When logged in and viewing the “schedule” screen, click on the “new scan” button in the top left corner. Name the profile, set the scan schedule, select the scan type, and then add targets and save.