Understanding report content

SUGGEST EDITS

Reports contain a great deal of information. It’s important to study them carefully for better understanding, so that they can help you make more informed security-related decisions.

The data in a report is a static snapshot in time. The data displayed in the Web interface changes with every scan. Variance between the two, such as in the number of discovered assets or vulnerabilities, is most likely attributable to changes in your environment since the last report.

For stakeholders in your organization who need fresh data but don’t have access to the Web interface, run reports more frequently. Or use the report scheduling feature to automatically synchronize report schedules with scan schedules.

In environments that are constantly changing, Baseline Comparison reports an be very useful.

If your report data turns out to be much different from what you expected, consider several factors that may have skewed the data.

Scan settings can affect report data

Scan settings affect report data in several ways:

- Lack of credentials: If certain information is missing from a report, such as discovered files, spidered Web sites, or policy evaluations, check to see if the scan was configured with proper logon information. The application cannot perform many checks without being able to log onto target systems as a normal user would.
- Policy checks not enabled: Another reason that policy settings may not appear in a report is that

policy checks were not enabled in the scan template.

- Discovery-only templates: If no vulnerability data appears in a report, check to see if the scan was preformed with a discovery-only scan template, which does not check for vulnerabilities.
- Certain vulnerability checks enabled or disabled: If your report shows vulnerabilities than you expected, check the scan template to see which checks have been enabled or disabled.
- Unsafe checks not enabled: If a report shows indicates that a check was skipped because of Denial of Service (DOS) settings, as with the sd result code in CSV reports, then unsafe checks were not enabled in the scan template.
- Manual scans: A manual scan performed under unusual conditions for a site can affect reports. For example, an automatically scheduled report that only includes recent scan data is related to a specific, multiple-asset site that has automatically scheduled scans. A user runs a manual scan of a single asset to verify a patch update. The report may include that scan data, showing only one asset, because it is from the most recent scan.

Different report formats can influence report data

If you are disseminating reports using multiple formats, keep in mind that different formats affect not only how data is presented, but what data is presented. The human-readable formats, such as PDF and HTML, are intended to display data that is organized by the document report templates. These templates are more “selective” about data to include. On the other hand, XML Export, XML Export 2.0, CSV, and export templates essentially include all possible data from scans.

Understanding how vulnerabilities are characterized according to certainty

Remediating confirmed vulnerabilities is a high security priority, so it’s important to look for confirmed vulnerabilities in reports. However, don’t get thrown off by listings of potential or unconfirmed vulnerabilities. And don’t dismiss these as false positives.

The application will flag a vulnerability if it discovers certain conditions that make it probable that the vulnerability exists. If, for any reason, it cannot absolutely verify that the vulnerability is there, it will list the vulnerability as potential or unconfirmed. Or it may indicate that the version of the scanned operating system or application is vulnerable.

The fact that a vulnerability is a “potential” vulnerability or otherwise not officially confirmed does not diminish the probability that it exists or that some related security issue requires your attention. You can confirm a vulnerability by running an exploit if one is available. See Working with vulnerabilities. You also can examine the scan log for the certainty with which a potentially vulnerable item was fingerprinted. A high level of fingerprinting certainty may indicate a greater likelihood of vulnerability.

How to find out the certainty characteristics of a vulnerability

You can find out the certainty level of a reported vulnerability in different areas:

- The PCI Audit report includes a table that lists the status of each vulnerability. Status refers to the certainty characteristic, such as Exploited, Potential, or Vulnerable Version.
- The Report Card report includes a similar status column in one of its tables, which also lists information about the test that the application performed for each vulnerability on each asset.
- The XML Export and XML Export 2.0 reports include an attribute called test status, which includes certainty characteristics, such as vulnerable-exploited, and not-vulnerable.
- The CSV report includes result codes related to certainty characteristics.
- If you have access to the Web interface, you can view the certainty characteristics of a vulnerability on the page that lists details about the vulnerability.

Note that the Discovered and Potential Vulnerabilities section, which appears in the Audit report, potential and confirmed vulnerabilities are not differentiated.

Looking beyond vulnerabilities

When reviewing reports, look beyond vulnerabilities for other signs that may put your network at risk. For example, the application may discover a telnet service and list it in a report. A telnet service is not a vulnerability. However, telnet is an unencrypted protocol. If a server on your network is using this protocol to exchange information with a remote computer, it's easy for an uninvited party to monitor the transmission. You may want to consider using SSH instead.

In another example, it may discover a Cisco device that permits Web requests to go to an HTTP server, instead of redirecting them to an HTTPS server. Again, this is not technically a vulnerability, but this practice may be exposing sensitive data.

Study reports to help you manage risk proactively.

Using report data to prioritize remediation

A long list of vulnerabilities in a report can be a daunting sight, and you may wonder which problem to tackle first. The vulnerability database contains checks for over 12,000 vulnerabilities, and your scans may reveal more vulnerabilities than you have time to correct.

One effective way to prioritize vulnerabilities is to note which have real exploits associated with them. A vulnerability with known exploits poses a very concrete risk to your network. The Exploit ExposureTM feature flags vulnerabilities that have known exploits and provides exploit information links to Metasploit modules and the Exploit Database. It also uses the exploit ranking data from the Metasploit team to rank the skill level required for a given exploit. This information appears in vulnerability listings right in the Security Console Web interface, so you can see right away

Since you can’t predict the skill level of an attacker, it is a strongly recommend best practice to immediately remediate any vulnerability that has a live exploit, regardless of the skill level required for an exploit or the number of known exploits.

Report creation settings can affect report data

Report settings can affect report data in various ways:

- Using most recent scan data: If old assets that are no longer in use still appear in your reports, and if this is not desirable, make sure to enable the check box labeled **Use the last scan data only**.
- Report schedule out of sync with scan schedule: If a report is showing no change in the number of vulnerabilities despite the fact that you have performed substantial remediation since the last report was generated, check the report schedule against the scan schedule. Make sure that reports are automatically generated to follow scans if they are intended to show patch verification.
- Assets not included: If a report is not showing expected asset data, check the report configuration to see which sites and assets have been included and omitted.
- Vulnerabilities not included: If a report is not showing an expected vulnerability, check the report configuration to vulnerabilities that have been filtered from the report. On the *Scope* section of the *Create a report* panel, click **Filter report scope based on vulnerabilities** and verify the filters are set appropriately to include the categories and severity level you need.

Prioritize according to risk score

Another way to prioritize vulnerabilities is according to their risk scores. A higher score warrants higher priority.

The application calculates risk scores for every asset and vulnerability that it finds during a scan. The scores indicate the potential danger that the vulnerability poses to network and business security based on impact and likelihood of exploit.

Risk scores are calculated according to different risk strategies. See Working with risk strategies to analyze threats.