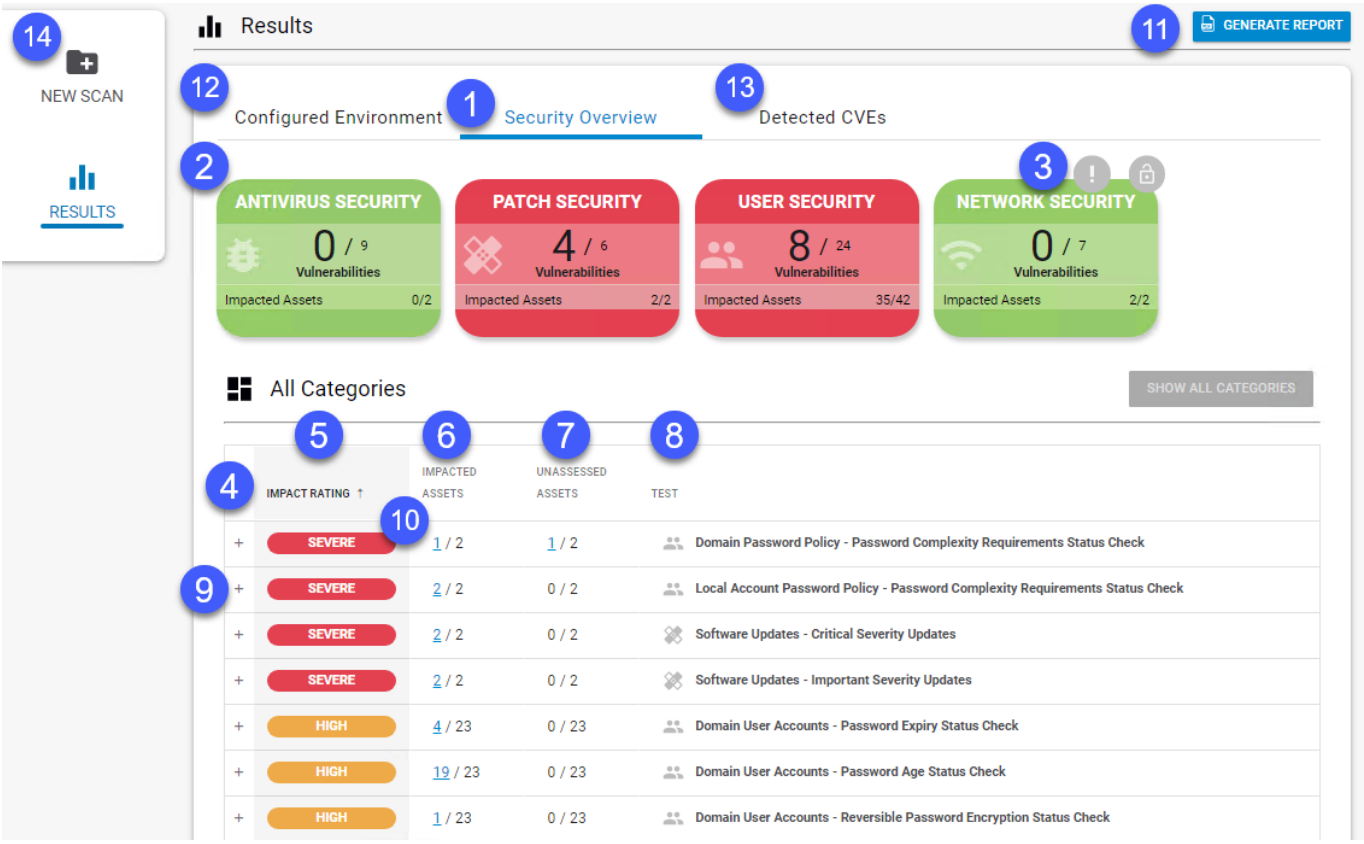
How to Read Your Security Score - Results Page

https://campus.barracuda.com/doc/97520142/

The **Results** page displays your security score, with information on:

- how the score was determined
- what tests were run
- what tests could not be run
- what is impacting the score
- what is not impacting the score
- which assets impact the score

On this page, you can also view additional details that help you determine why the site is receiving this score, as well as the suggested countermeasures to close security issues. See below for a tour of the **Results** page:



1. The **Security Overview** tab displays the results of the tests, sorted by category.
2. Click any **Category Card** to filter the page on that category and see only the results in that category.
3. The **Open Ports** icons appear if commonly abused ports are open and vulnerable to attack.

4. The results table displays the results of the scan, organized by test. By default, the table is sorted with the most serious test results appearing first, but you can sort the results using the **Impact Rating** column.
5. The **Impact Rating** column displays the impact of the test results.
6. The **Impacted Assets** column displays how many assets are affected, as a fraction of the total assets scanned.
7. The **Unassessed Assets** column displays how many assets are not assessed, due to a data collection issue, as a fraction of the total assets scanned.
8. The **Test** column displays an icon identifying the category the test belongs to, and the name of the test.
9. Click the plus icon next to any test to see more details about the test, its impact, countermeasures you can take to protect your network, and, depending on the test, which assets are affected.
10. When you see a blue underlined number, you can click the link to see a pop up with a list of the impacted assets.
11. Click **Generate Report** to output a customized report of the scan results as a PDF. You can choose the report customer name, company name, also decide which devices to include as well as whether to include the IP range or not.
12. Click the **Configured Environment** tab to to see the configuration for the current scan.
13. Click Detected CVEs to see the CVEs detected in the scan. For more information, see How to Read Your Security Score - Detected Common Vulnerabilities & Exploits (CVEs)
14. Click **New Scan** NEW SCANto return to the **New Scan/Configuration** page and run another scan.

Figures