

REPORT

Perform vulnerability assessment on any IP/Website

Step 1 - Scan website on Nessus

The screenshot displays the Nessus Essentials web interface in a browser window. The address bar shows the URL <https://localhost:8834/#/scans/reports/15/hosts>. The interface includes a sidebar with folders (My Scans, College, All Scans, Trash) and resources (Policies, Plugin Rules, Terrascan). The main content area is titled "Metasploit" and shows a table of hosts with a single entry: 192.168.204.129. The table includes columns for Host, Vulnerabilities, Remediations, Notes, and History. The Vulnerabilities column shows a bar chart with counts: 13 Critical, 7 High, 25 Medium, and 8 Low. The Scan Details panel on the right provides information about the scan: Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (December 7 at 10:15 AM), End (December 7 at 10:39 AM), and Elapsed (24 minutes). A Vulnerabilities donut chart is also present, showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Host	Vulnerabilities	Remediations	Notes	History
192.168.204.129	13 Critical, 7 High, 25 Medium, 8 Low	3	3	1

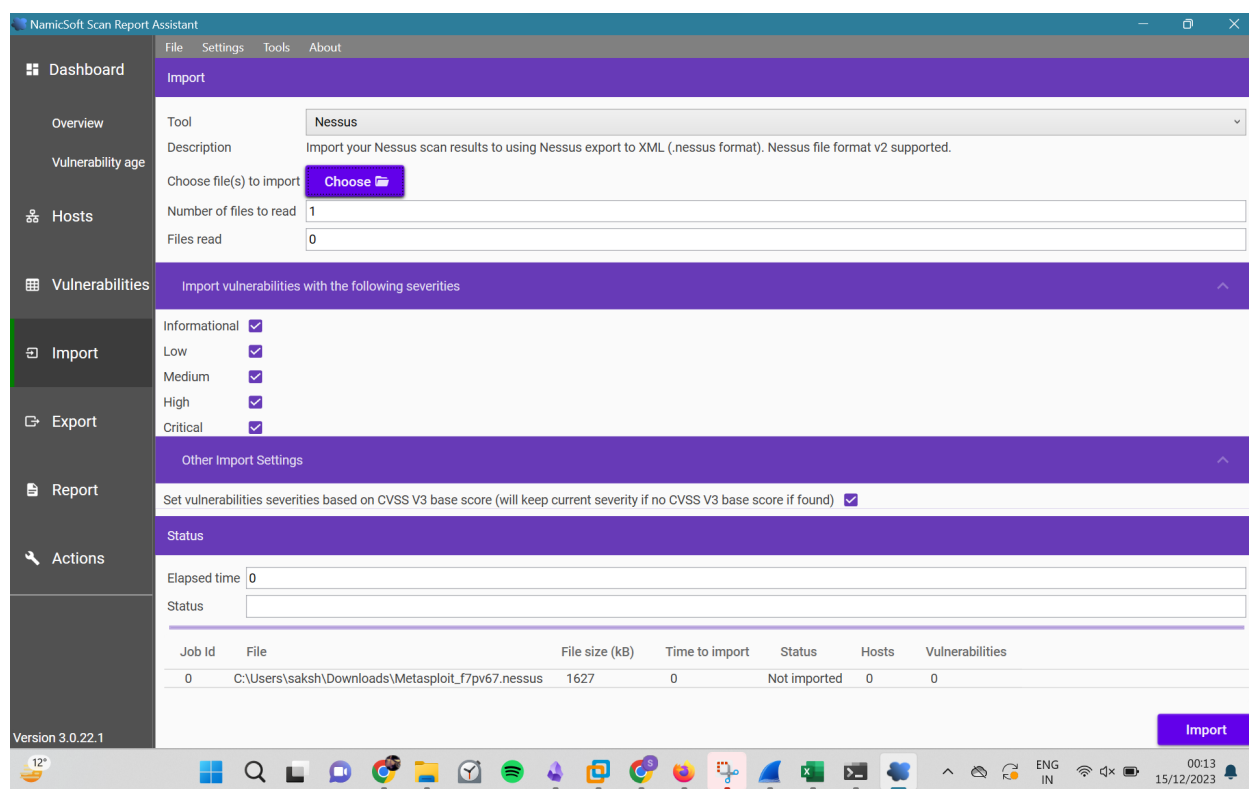
Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: December 7 at 10:15 AM
- End: December 7 at 10:39 AM
- Elapsed: 24 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Step 2 - Download nessus file and import it into Namic Soft



Step 3 - Export the file and prepare a report in Excel/Google sheet

https://docs.google.com/spreadsheets/d/18pQ44i7Kt3gbklVqvg8O2Jbgx1I_PCSE6h2sesfiRs8/edit?usp=s haring