Network Vulnerability Assessment Tools

A vulnerability assessment involves identifying and quantifying resources residing on a network, then identifying and prioritizing any vulnerabilities or potential threats to each of these resources.

Vulnerability analysis consists of several steps:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs.

(© TechTarget)

Nessus - Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments. Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network. Aprox. $3,000/year.

https://www.tenable.com/products/nessus-vulnerability-scanner

NMAP - Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Free.

https://nmap.org/

Microsoft Baseline Security Analyzer - provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. MS networks only.OpenVAS

http://www.microsoft.com/en-us/download/details.aspx?id=7558

OpenVAS – Open Vulnerability Assessment System is a free network security scanner platform, with most components licensed under the GNU General Public License (GNU GPL). The main component is available via several Linux packages or as a downloadable Virtual Appliance for testing/evaluation purposes. Though the scanner itself doesn't work on Windows machines, they offer clients for Windows.

http://www.openvas.org/