[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@154c2f28b19d4740be09c95aaab2d3a9?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

Reference <https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/>

**What to know about Vulnerability Scanners and Scanning Tools**

**What are vulnerability scanners**

A vulnerability scanner is an automated tool that identifies and creates an inventory of all IT assets (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network. For each asset, it also attempts to identify operational details such as the operating system it runs and the software installed on it, along with other attributes such as open ports and user accounts. A vulnerability scanner enables organizations to monitor their networks, systems, and applications for security vulnerabilities.

Most security teams utilize vulnerability scanners to bring to light security vulnerabilities in their computer systems, networks, applications and procedures. There are a plethora of vulnerability scanning tools available, each offering a unique combination of capabilities.

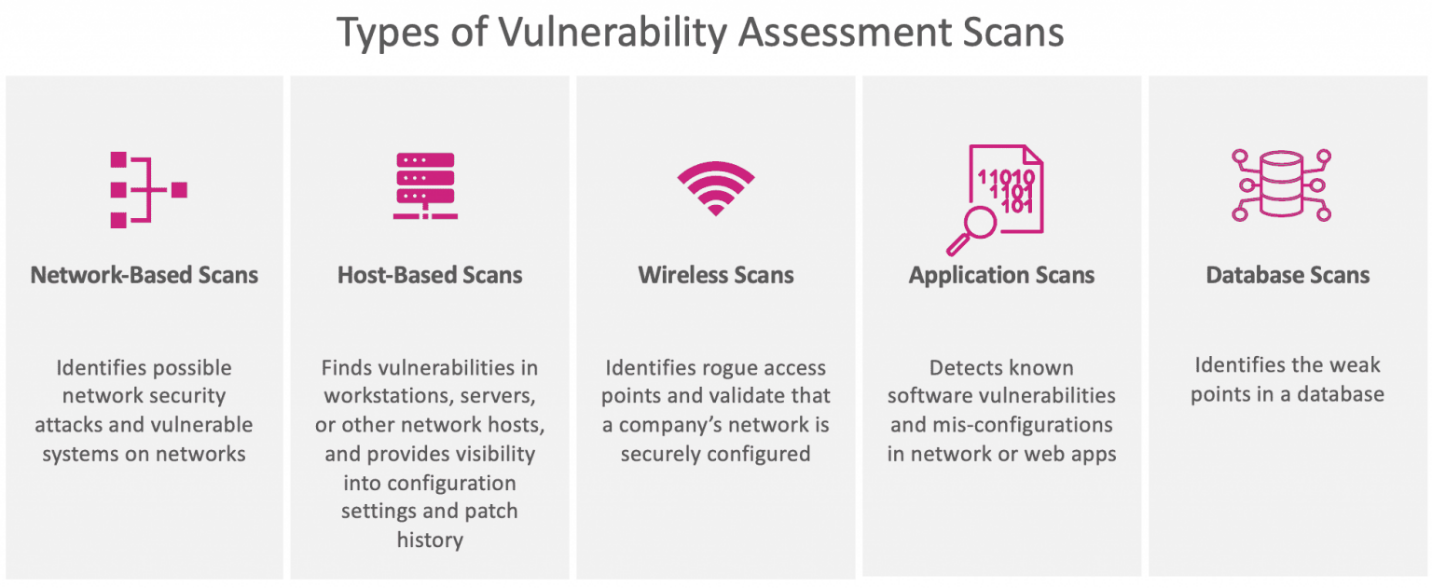
Leading vulnerability scanners provide users with information about:

1. Weaknesses in their environment
2. Insights into degrees of risk from each vulnerability
3. Recommendations on how to mitigate the vulnerability

Before purchasing a vulnerability scanning tool, it’s important to understand exactly how scanning will contribute to your more broad vulnerability management and [security posture](https://www.balbix.com/insights/what-is-cyber-security-posture/) strategy. Traditional vulnerability scanning tools can play an important role in catching common CVEs if the scans are conducted frequently. Companies typically conduct vulnerability scans on their networks and devices consistently because as their technology, software, etc. continue to develop and undergo changes, there is a higher risk for threats to appear.

**Five types of vulnerability scanners**

Vulnerability scanners can be categorized into 5 types based on the type of assets they scan.

Details of five types of vulnerability assessment scanners – 1. network based scanners 2. Host bases scanners 3. Wireless scanners 4. Applications scanners, and 5. Database scanners

**1. Network-based scanners**

Network based vulnerability scanners identify possible network security attacks and vulnerable systems on wired or wireless networks. Network-based scanners discover unknown or unauthorized devices and systems on a network, help determine if there are unknown perimeter points on the network, such as unauthorized remote access servers, or connections to insecure networks of business partners.

**2. Host-based scanners**

Host based vulnerability scanners are used to locate and identify vulnerabilities in servers, workstations, or other network hosts, and provide greater visibility into the configuration settings and patch history of scanned systems. Host-based vulnerability assessment tools can also provide an insight into the potential damage that can be done by insiders and outsiders once some level of access is granted or taken on a system.

**3. Wireless scanners**

Wireless vulnerability scanners are used to identify rogue access points and also validate that a company’s network is securely configured.

**4. Application scanners**

Applications vulnerability scanners test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications.

**5. Database scanners**

Database vulnerability scanners identify the weak points in a database so as to prevent malicious attacks

**External vs Internal vulnerability scans**

An **external vulnerability scan** can help organizations to identify and fix security vulnerabilities that an adversary can use to gain access to its network. External vulnerability scan is performed from outside an organization’s network, targeting IT infrastructure that is exposed to the internet including web applications, ports, networks etc..

An external scan can detect vulnerabilities in the perimeter defenses such as:-

* Open ports in the network firewall
* Specialized web application firewall.

An **internal vulnerability scan** is carried out from inside an enterprise network. These scans allow you to harden and protect applications and systems that are not covered by external scans. An internal vulnerability scan can detect issues such as: –

1. Vulnerabilities that can be exploited by an adversary who has penetrated the perimeter defenses
2. Threat posed by malware that has made it to inside the network
3. Identify “insider threats” posed by disgruntled employees or contractors

**Authenticated vs. Unauthenticated vulnerability scans**

To ensure that vulnerability scans have no lapse in detection, it is suggested that both authenticated and unauthenticated vulnerability scans are conducted. While the authenticated scan allows the tester to log in as a user and see vulnerabilities from a trusted user’s perspective, the unauthentic scan does the opposite and offers the perspective of an intruder. Scanning under all circumstances, again, ensures that even with constantly evolving technology, companies are safe from threats.

**Going beyond scanning with Balbix**

While leveraging numerous types of scans is an important step for mitigating risk, an [effective vulnerability assessment program](https://www.balbix.com/insights/vulnerability-assessments-drive-enhanced-security-and-cyber-resilience/) will go beyond scanning intermittently.

Balbix continuously and automatically identifies and creates an inventory of all IT assets including servers, laptops, desktops, mobile devices, IoT, etc and analyzes and detects vulnerabilities across an enterprise’s entire attack surface. It identifies and prioritizes which vulnerabilities are most critical to your business based on importance of assets and their susceptibility to 100+ attack vectors. Vulnerabilities are prioritized based on 5 factors: severity, threats, asset exposure, business criticality and security controls, and then dispatched to risk owners for automatic or supervised mitigation.

While vulnerability scanners only provide a screenshot of risk from a specific point in time, Balbix provides ongoing analysis of a company’s entire attack surface continuously and in real time.

Contents

1. [What are vulnerability scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#What-are-vulnerability-scanners-0)
2. [Five types of vulnerability scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#Five-types-of-vulnerability-scanners-1)
   1. [1. Network-based scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#1-Network-based-scanners-2)
   2. [2. Host-based scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#2-Host-based-scanners-3)
   3. [3. Wireless scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#3-Wireless-scanners-4)
   4. [4. Application scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#4-Application-scanners-5)
   5. [5. Database scanners](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#5-Database-scanners-6)
3. [External vs Internal vulnerability scans](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#External-vs-Internal-vulnerability-scans-7)
4. [Authenticated vs. Unauthenticated vulnerability scans](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#Authenticated-vs-Unauthenticated-vulnerability-scans-8)
5. [Going beyond scanning with Balbix](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#Going-beyond-scanning-with-Balbix-9)
6. [Frequently Asked Questions](https://www.balbix.com/insights/what-to-know-about-vulnerability-scanning-and-tools/#Frequently-Asked-Questions-About-Vulnerability-Scanners-0)