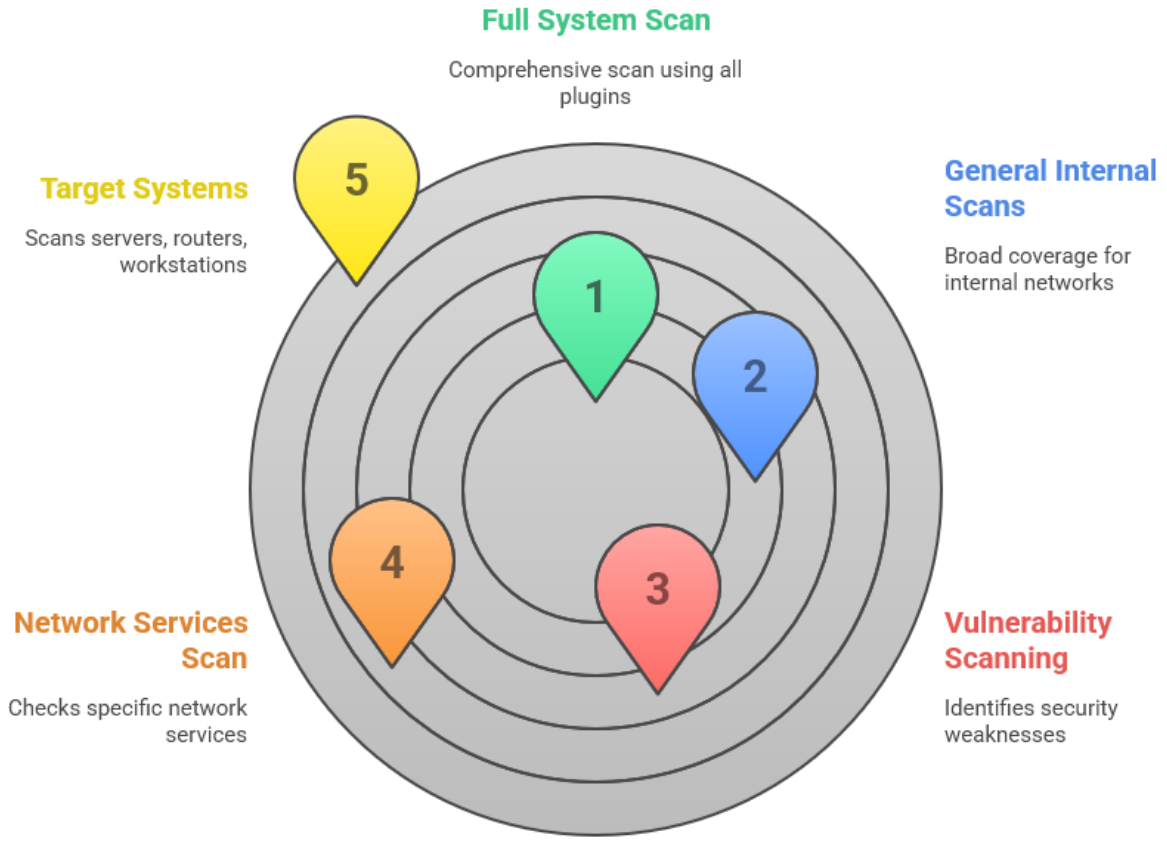
Basic Network Scan:

Designed for scanning a traditional network or systems, such as servers or workstations. Performs a comprehensive vulnerability scan on any host using all available plugins. Suitable for general internal scans and provides broad coverage. It scans for vulnerabilities across various network services and checks for common issues like missing patches or weak configurations. Performs a full system scan that is suitable for any host. Use this template to scan an asset or assets with all of Nessus's plugins enabled.

Ideal for scanning servers, routers, switches, or workstations to find security weaknesses or misconfigurations.

Feature	Description
Unauthenticated Scan	No need for system credentials can be added if needed
Port Scanning	Uses Nmap-like techniques to find open TCP/UDP ports
Service Detection	Identifies services running on open ports (e.g., Apache, MySQL)
Vulnerability Detection	Matches findings against Nessus plugins includes CVEs, patches, exploits
Severity Ratings	Classifies vulnerabilities as Critical, High, Medium, Low, or Info
OS Fingerprinting	Tries to determine the OS running on the target
Plugin Selection	Uses a broad set of Nessus plugins not fine-tuned



Common Vulnerabilities Detected:

- Missing software or OS patches
- Open ports with risky services
- Deprecated or vulnerable protocols (e.g., SMBv1, SSLv2)
- Weak/default credentials for certain services
- Misconfigured web servers, FTP, SSH, etc.