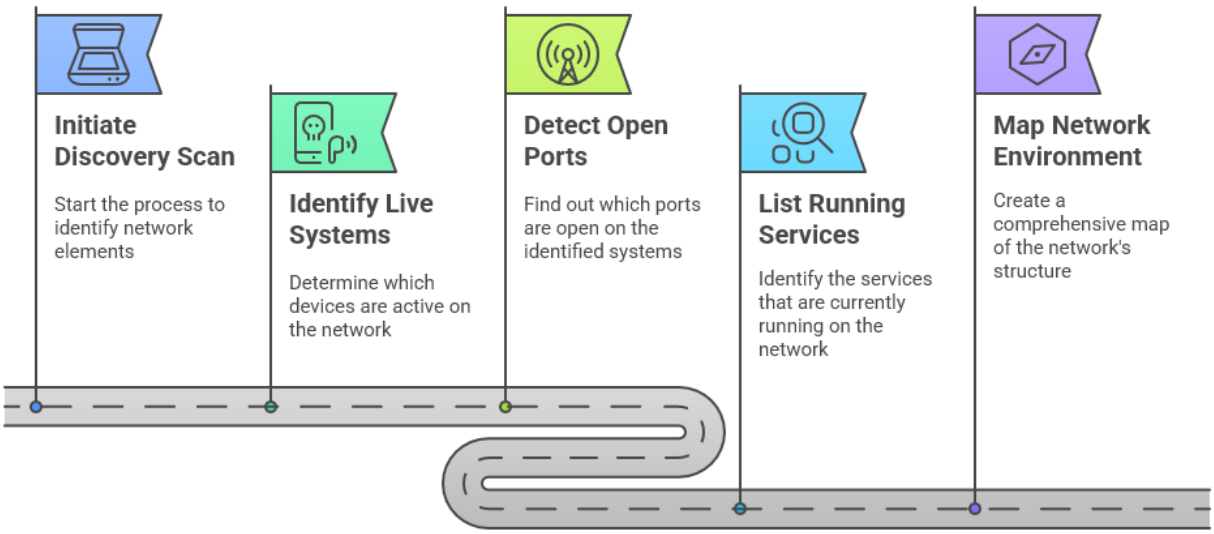
Scan Templates:

A scan template in Nessus is a predefined configuration used to create a vulnerability scan. Templates are scan blueprints — you pick a template, fill in the targets and credentials, and launch the scan. There are three scanner template categories in Tenable Nessus:

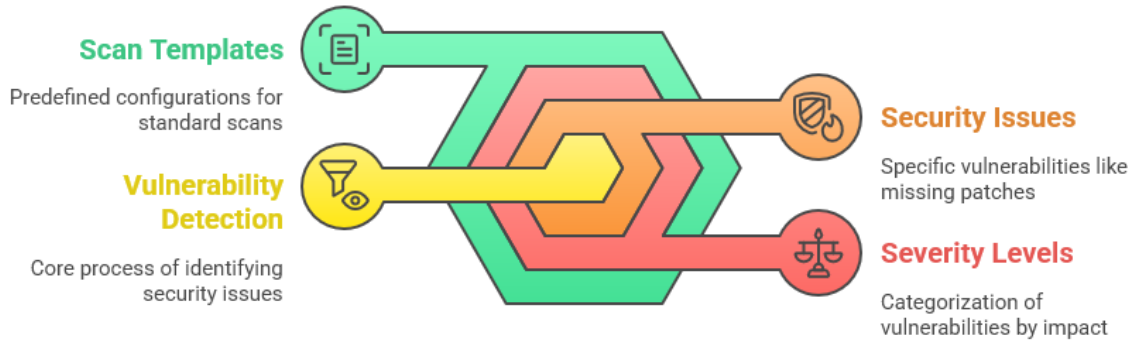
Discovery:

Find out what devices and systems are active on the network. Discovery scans are used to identify live systems, open ports, and running services on a network — they help map the environment before deeper scanning begins. For example, a Host Discovery scan can identify which devices respond to ping or have open ports, helping build a list of live assets.



Vulnerabilities:

Vulnerability scans focus on detecting known security issues like missing patches, misconfigurations, and exploitable weaknesses (e.g., CVEs), often categorized by severity levels (Critical, High, Medium, Low, Info). for instance, a Basic Network Scan might reveal a Windows server with an outdated SMB service vulnerable. Using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs.



Compliance:

Check if systems comply with organizational or regulatory standards. Compliance scans, on the other hand, assess whether systems meet specific security policies or regulatory standards such as CIS, NIST, or custom organizational baselines. Together, these scans provide a full picture of an organization's security posture — from knowing what is on the network, to identifying threats, to ensuring policy compliance. A good example is the CIS Compliance Scan, which verifies if a Linux server's password policies and SSH settings meet the CIS Benchmark guidelines. Compliance scans are sometimes referred to as configuration scans.