Templates:

Think of a template like a ready-made form for common types of scans. You choose a template when you're creating a new scan. Each template is pre-configured for a certain task.
Predefined or customizable configurations used to create a new scan in Nessus. Each template is designed for a specific purpose (e.g., network scanning, web app testing, compliance auditing) and includes default settings for plugins, scan scope, and other parameters. Templates simplify the scan creation process by providing a starting point that can be modified as needed.

The New Scan page displays a list of available templates, organized by categories Vulnerabilities, Compliance, Web Applications. Each template has a brief description such as Basic Network Scan: Scans for vulnerabilities without credentials.

Policy:

A policy is a custom set of scan rules you create or use. It controls what Nessus scans and how it scans. You can create and save a policy, and then use it again later for similar scans. A policy is like custom scan.
A policy is the underlying configuration of a scan, defining the technical details of what Nessus checks (e.g., plugins, ports, credentials) and how it behaves (e.g., scan speed, timeouts). Every scan template is associated with a policy. When you create a scan, you either use the default policy tied to a template or select a custom policy. Policies can be saved, reused, and shared across multiple scans for consistency.

Templates are user-friendly starting points for creating scans, while policies are the detailed configurations that templates reference. You select a template to start a scan, then customize or assign a policy to fine-tune it.

A **custom scan policy** in Nessus allows you to create reusable settings for scans that match your organization's specific needs. These policies can be based on existing templates enabling granular control over scan behavior, plugin selection, performance, and reporting. This helps maintain consistency and control over your scanning process.

Why Custom Policy:

- Scan specific ports or plugin families
- Use saved credentials for deeper scans
- Exclude certain IP addresses or networks
- Improve scan speed or stealth
- Apply internal security or compliance standards