Advanced Scan:

To create a fully customized vulnerability scan. This template gives you control over every aspect ports, scan types, plugins, credentials, performance settings, and more.
The most configurable scan type. You can configure this scan template to match any policy. This template has the same default settings as the basic scan template, but it allows for additional configuration options.

Section	Description
Basic Settings	Name, description, folder, targets (IPs, ranges, hostnames)
Discovery	Define how hosts are detected (ICMP, TCP SYN, ARP, etc.)
Port Scanning	Set specific ports or ranges, scan types (SYN, TCP connect, etc.)
Assessment	Choose which types of vulnerabilities to assess (e.g., web, Windows, SCADA)
Credentials	Add local credentials (Windows, Linux, SNMP, etc.) for deeper scans
Plugins	Enable/disable specific plugin families (e.g., brute force, Windows)
Preferences	Fine-tune behavior, e.g., CGI scanning, HTTP login, timeout thresholds
Advanced	Set performance limits, network timeout, rate limits, logging, debugging

Feature	Description
Full Plugin Control	Choose specific vulnerability tests to include/exclude
Custom Port Lists	Define which ports to scan or ignore
Protocol-specific Scans	Tailor scans for web apps, databases, email, etc.
Credentialed Scanning	Provide usernames/passwords/keys for authenticated scans
Web Application Options	Adjust behavior like login forms, cookies, max crawl depth
Performance Tuning	Throttle number of checks, connections, timeout limits
Safe Checks Toggle	Enable/disable checks that might crash services
Timeouts & Rate Control	Control how aggressively Nessus scans the network