

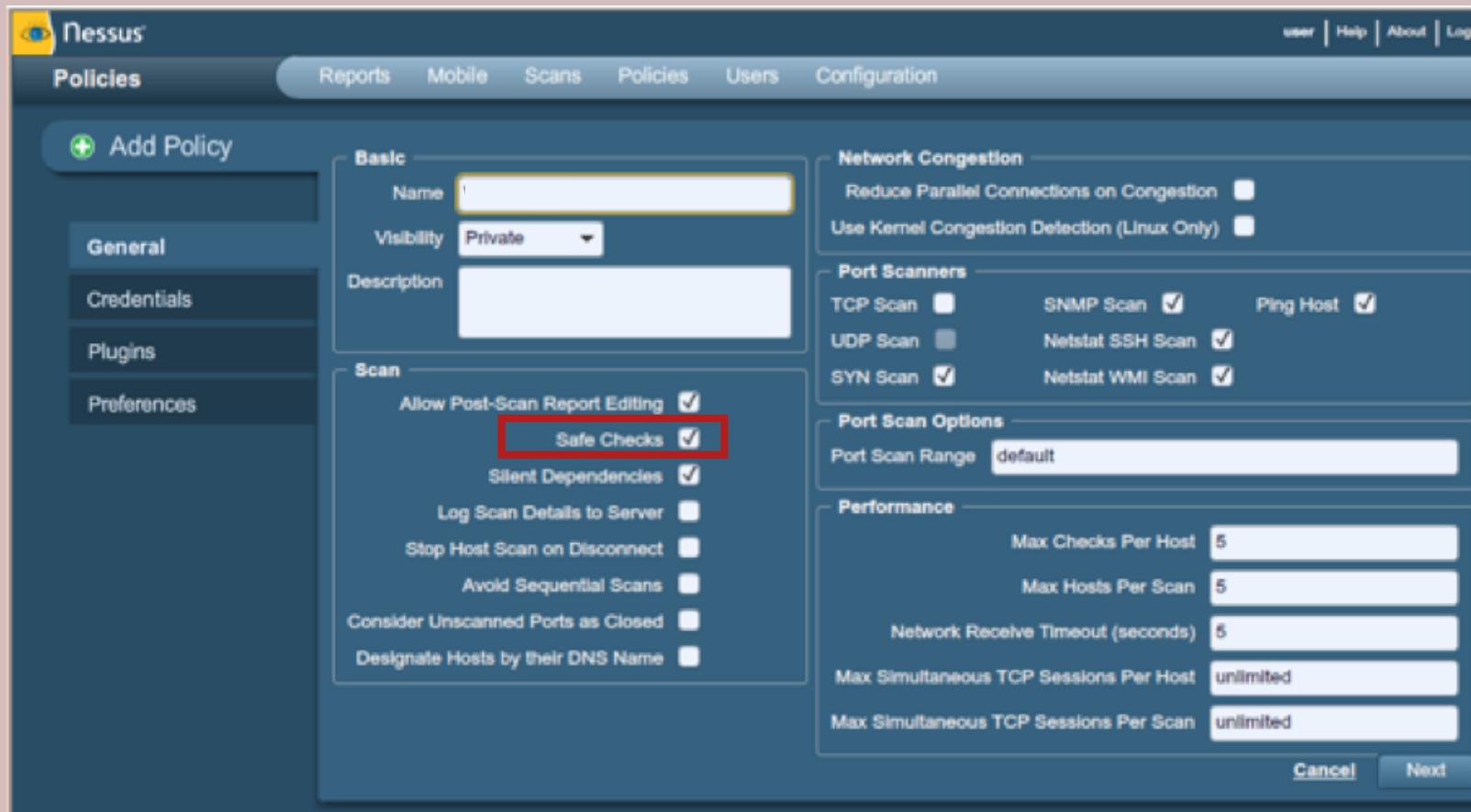


# Scanning Sensitivity

VULNERABILITY MANAGEMENT

# Scan Sensitivity Levels

- Choose level appropriate with objectives



The screenshot shows the Nessus web interface for configuring a policy. The left sidebar contains a menu with 'Policies' selected, and sub-items: 'Add Policy', 'General', 'Credentials', 'Plugins', and 'Preferences'. The main content area is divided into several sections:

- Basic:** Includes fields for 'Name', 'Visibility' (set to 'Private'), and 'Description'.
- Scan:** A list of checkboxes for scan options. The 'Safe Checks' checkbox is highlighted with a red box. Other options include 'Allow Post-Scan Report Editing', 'Silent Dependencies', 'Log Scan Details to Server', 'Stop Host Scan on Disconnect', 'Avoid Sequential Scans', 'Consider Unscanned Ports as Closed', and 'Designate Hosts by their DNS Name'.
- Network Congestion:** Includes checkboxes for 'Reduce Parallel Connections on Congestion' and 'Use Kernel Congestion Detection (Linux Only)'.
- Port Scanners:** A grid of checkboxes for various scan types: TCP Scan, UDP Scan, SYN Scan, SNMP Scan, Netstat SSH Scan, Netstat WMI Scan, and Ping Host.
- Port Scan Options:** Includes a 'Port Scan Range' dropdown set to 'default'.
- Performance:** Includes input fields for 'Max Checks Per Host', 'Max Hosts Per Scan', 'Network Receive Timeout (seconds)', 'Max Simultaneous TCP Sessions Per Host', and 'Max Simultaneous TCP Sessions Per Scan'.

At the bottom right of the configuration area are 'Cancel' and 'Next' buttons.



# Plug-ins

- Provide the scan functionality for different functions
- Enable/disable them based on your needs
- If Linux system, disable Windows plug-ins
- Some scans can disrupt your systems or cause loss of data...
- Ensure you are scanning safely and with permission



# Plug-ins

[user](#) | [Help](#) | [About](#) | [Log out](#)

[Reports](#) | [Mobile](#) | [Scans](#) | [Policies](#) | [Users](#) | [Configuration](#)

**Filters**   No Filters   [+ Add Filter](#)   [Clear Filters](#)

Families	Plugins	<a href="#">Enable Plugins</a>	<a href="#">Disable Plugins</a>
<ul style="list-style-type: none"><li><input type="radio"/> Solaris Local Security Checks</li><li><input type="radio"/> SuSE Local Security Checks</li><li><input type="radio"/> Ubuntu Local Security Checks</li><li><input type="radio"/> VMware ESX Local Security Checks</li><li><input type="radio"/> Web Servers</li><li><input checked="" type="radio"/> Windows</li><li><input type="radio"/> Windows : Microsoft Bulletins</li><li><input type="radio"/> Windows : User management</li></ul>	<ul style="list-style-type: none"><li><input type="radio"/> 58484 2X ApplicationServer TuxSystem ActiveX ExportSett</li><li><input type="radio"/> 58321 2X Client TuxClientSystem ActiveX InstallClient() M</li><li><input type="radio"/> 23735 3CTftpSvc Long Transport Mode Remote Overflow</li><li><input type="radio"/> 33218 3D-FTP Multiple Directory Traversal Vulnerabilities</li><li><input type="radio"/> 26020 3DGreetings Player ActiveX Multiple Buffer Overflow</li><li><input type="radio"/> 29749 3ivx MPEG-4 &lt; 5.0.2 Buffer Overflow</li><li><input type="radio"/> 31607 7-Zip &lt; 4.57 Archive Handling Unspecified Issue</li><li><input type="radio"/> 23750 7-Zip API File Handling Overflow</li></ul>		

**Plugin Description**  

I

Enabled Families: 44   Enabled Plugins: 54758   [Show Only Enabled Plugins](#) ☐   [Enable All](#)   [Disable All](#)

[Cancel](#)   [Back](#)   [Next](#)

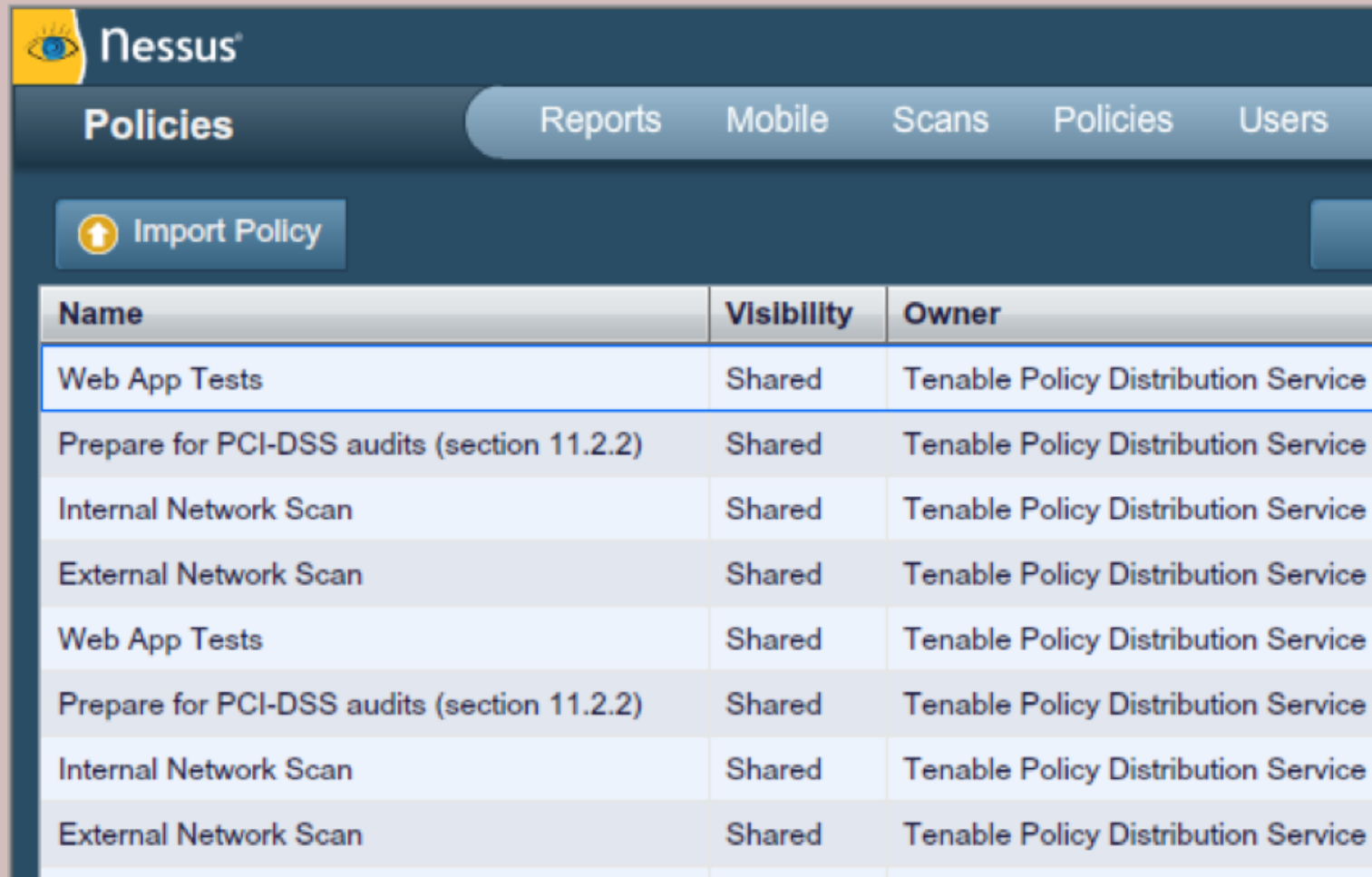


# Templates for Scans

- Vendors provide templates for scans with common settings
- Admins can also create their own templates for commonly used scans
- This prevents errors and saves time



# Templates for Scans

The image shows a screenshot of the Nessus web interface. At the top, there's a navigation bar with the Nessus logo and tabs for Policies, Reports, Mobile, Scans, Policies, and Users. Below the navigation bar, there's a button labeled 'Import Policy'. The main content area displays a table of policies. The table has three columns: Name, Visibility, and Owner. The policies listed are: Web App Tests, Prepare for PCI-DSS audits (section 11.2.2), Internal Network Scan, External Network Scan, Web App Tests, Prepare for PCI-DSS audits (section 11.2.2), Internal Network Scan, and External Network Scan. All policies have a visibility of 'Shared' and are owned by 'Tenable Policy Distribution Service'.

Name	Visibility	Owner
Web App Tests	Shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service
Web App Tests	Shared	Tenable Policy Distribution Service
Prepare for PCI-DSS audits (section 11.2.2)	Shared	Tenable Policy Distribution Service
Internal Network Scan	Shared	Tenable Policy Distribution Service
External Network Scan	Shared	Tenable Policy Distribution Service

