

- i** In this lab you will create a report template which focusses on Microsoft Patch Tuesday vulnerabilities which have been discovered on Windows Server assets. Click on the **New button** to begin.

The screenshot shows the Qualys Cloud Platform interface. At the top, there is a navigation bar with links for VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. Below the navigation bar is a toolbar with tabs for Reports, Reports, Schedules, Templates (which is selected), Risk Analysis, Search Lists, and Setup. There are also buttons for Actions (0), New, Search, and Filters. On the right side of the toolbar, it shows page 1 - 15 of 15 and some settings icons. The main content area displays a list of report templates on the left and a detailed table of vulnerabilities on the right. The table has columns for Type, Vulnerability Data, User, and Modified. The data in the table is as follows:

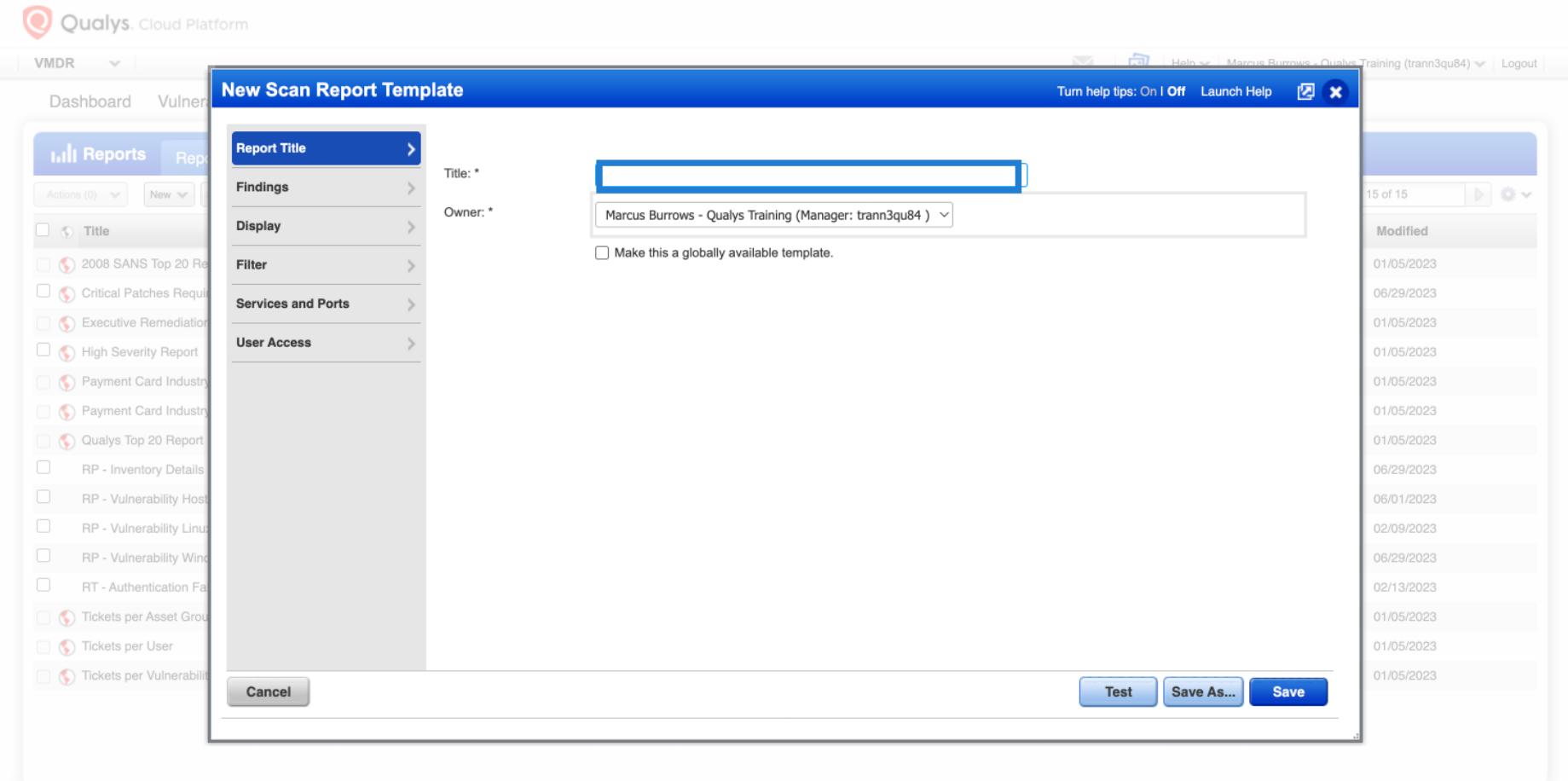
Type	Vulnerability Data	User	Modified
Host Based	System	01/05/2023	
Host Based	Marcus Burrows - Qualys Training	06/29/2023	
Host Based	System	01/05/2023	
Host Based	Marcus Burrows - Qualys Training	01/05/2023	
Scan Based	System	01/05/2023	
Scan Based	System	01/05/2023	
Host Based	System	01/05/2023	
Host Based	Marcus Burrows - Qualys Training	06/29/2023	
Scan Based	Marcus Burrows - Qualys Training	06/01/2023	
Host Based	Marcus Burrows - Qualys Training	02/09/2023	
Host Based	Marcus Burrows - Qualys Training	06/29/2023	
Scan Based	Marcus Burrows - Qualys Training	02/13/2023	
Host Based	System	01/05/2023	
Host Based	System	01/05/2023	
Host Based	System	01/05/2023	

1 Click Scan Template...

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports (which is the active tab), Remediation, Assets, KnowledgeBase, and Users. Below the navigation is a toolbar with Actions (0), New, Search, and Filters. A blue header bar contains the tabs: Reports, Reports, Schedules, Templates (which is the active tab), Risk Analysis, Search Lists, and Setup. A sub-menu is open under the 'Actions' dropdown, listing: Scan Template..., PCI Scan Template..., Patch Template..., Map Template..., Import from Library..., and Download... The main content area displays a table of vulnerability data. The columns are Type, Vulnerability Data, User, and Modified. The data includes various entries such as Host Based, Scan Based, and Ticket-based findings across different dates and users.

Type	Vulnerability Data	User	Modified
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	01/05/2023
Scan Based	System	System	01/05/2023
Scan Based	System	System	01/05/2023
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Scan Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/01/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	02/09/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Scan Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	02/13/2023
Host Based	System	System	01/05/2023
Host Based	System	System	01/05/2023
Host Based	System	System	01/05/2023

 As the name for the Report Template, type **Windows Servers Patch Tuesday** and press Enter



The screenshot shows the Qualys Cloud Platform interface with the title "New Scan Report Template". On the left, there's a sidebar with "Reports" selected, listing various report types like "Title", "2008 SANS Top 20 Report", "Critical Patches Required", etc. The main dialog has a "Report Title" section with a "Title:" field containing "Windows Servers Patch Tuesday" (highlighted with a blue border), an "Owner:" dropdown set to "Marcus Burrows - Qualys Training (Manager: trann3qu84)", and a checkbox for "Make this a globally available template" which is unchecked. At the bottom are "Cancel", "Test", "Save As...", and "Save" buttons. To the right of the dialog, there's a list of 15 items, each with a date: 01/05/2023, 06/29/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 02/09/2023, 06/29/2023, 02/13/2023, 01/05/2023, 01/05/2023, 01/05/2023.

- 1 Click on the check box next to "Make this a globally available template". This will allow other users to use this Report Template.

The screenshot shows the 'New Scan Report Template' dialog box in the Qualys Cloud Platform. The dialog has a blue header bar with the title 'New Scan Report Template'. On the left is a sidebar with sections: 'Report Title', 'Findings', 'Display', 'Filter', 'Services and Ports', and 'User Access'. Under 'Report Title', the 'Title' field is set to 'Windows Servers Patch Tuesday' and the 'Owner' dropdown is set to 'Marcus Burrows - Qualys Training (Manager: trann3qu84)'. Below these fields is a checkbox labeled 'Make this a globally available template.' At the bottom of the dialog are three buttons: 'Cancel', 'Test', 'Save As...', and 'Save'. To the right of the dialog, there is a sidebar showing a list of 15 items, each with a date and a 'Modified' status. The dates range from 01/05/2023 to 06/29/2023.

1 Click on the Findings Tab

The screenshot shows the Qualys Cloud Platform interface for creating a new scan report template. The left sidebar has a 'Reports' section with various report types listed under 'Findings'. The main window is titled 'New Scan Report Template' and contains fields for 'Title' (Windows Servers Patch Tuesday) and 'Owner' (Marcus Burrows - Qualys Training (Manager: trann3qu84)). A checkbox for 'Make this a globally available template.' is checked. At the bottom are buttons for 'Cancel', 'Test', 'Save As...', and 'Save'.

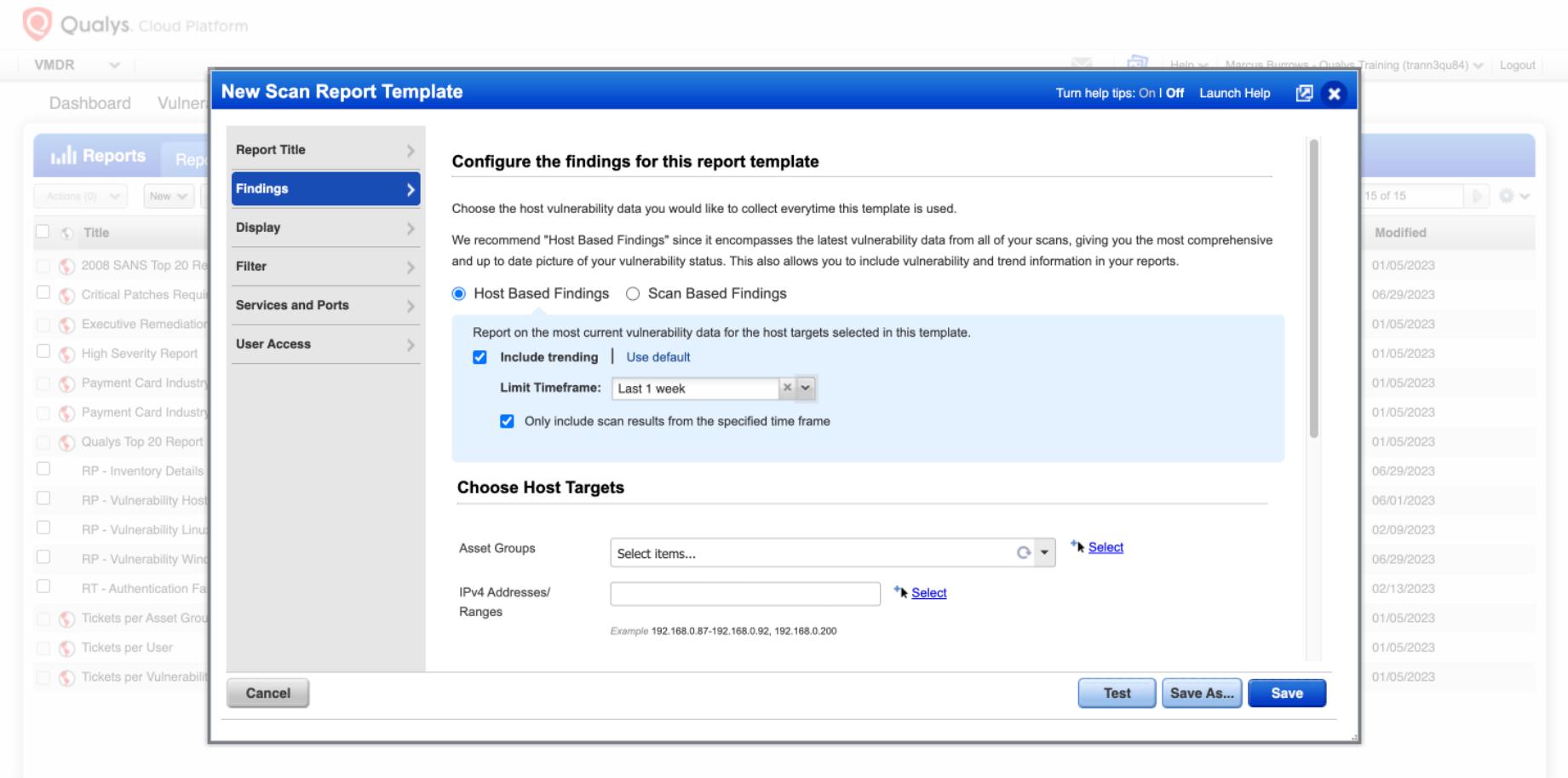
- 1 Host Based Findings is selected by default. Click on the check box next to "Include Trending".

The screenshot shows the 'New Scan Report Template' configuration interface. On the left, a sidebar lists various report types: Title, 2008 SANS Top 20, Critical Patches Required, Executive Remediation, High Severity Report, Payment Card Industry, Payment Card Industry, Qualys Top 20 Report, RP - Inventory Details, RP - Vulnerability Host, RP - Vulnerability Linux, RP - Vulnerability Windows, RT - Authentication Fail, Tickets per Asset Group, Tickets per User, and Tickets per Vulnerability. The 'Findings' section is currently selected. The main panel is titled 'Configure the findings for this report template'. It contains a note about choosing host vulnerability data, a recommendation for 'Host Based Findings', and a section for selecting 'Include trending'. Below this is a 'Choose Host Targets' section with fields for Asset Groups, IPv4 Addresses/Ranges, and Asset Tags. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

1 Click Select time frame

The screenshot shows the 'New Scan Report Template' dialog in Qualys Cloud Platform. The 'Findings' tab is selected in the left sidebar. A callout box highlights the 'Select time frame' button, which is part of a section titled 'Configure the findings for this report template'. This section includes a note about choosing host vulnerability data and a recommendation for 'Host Based Findings'. Below this, there's a checkbox for 'Include trending' which is checked, and a link to 'Select time frame'. To the right of the main dialog, a vertical sidebar lists 15 items, each with a date: 01/05/2023, 06/29/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 01/05/2023, 06/29/2023, 06/01/2023, 02/09/2023, 06/29/2023, 02/13/2023, 01/05/2023, 01/05/2023, and 01/05/2023.

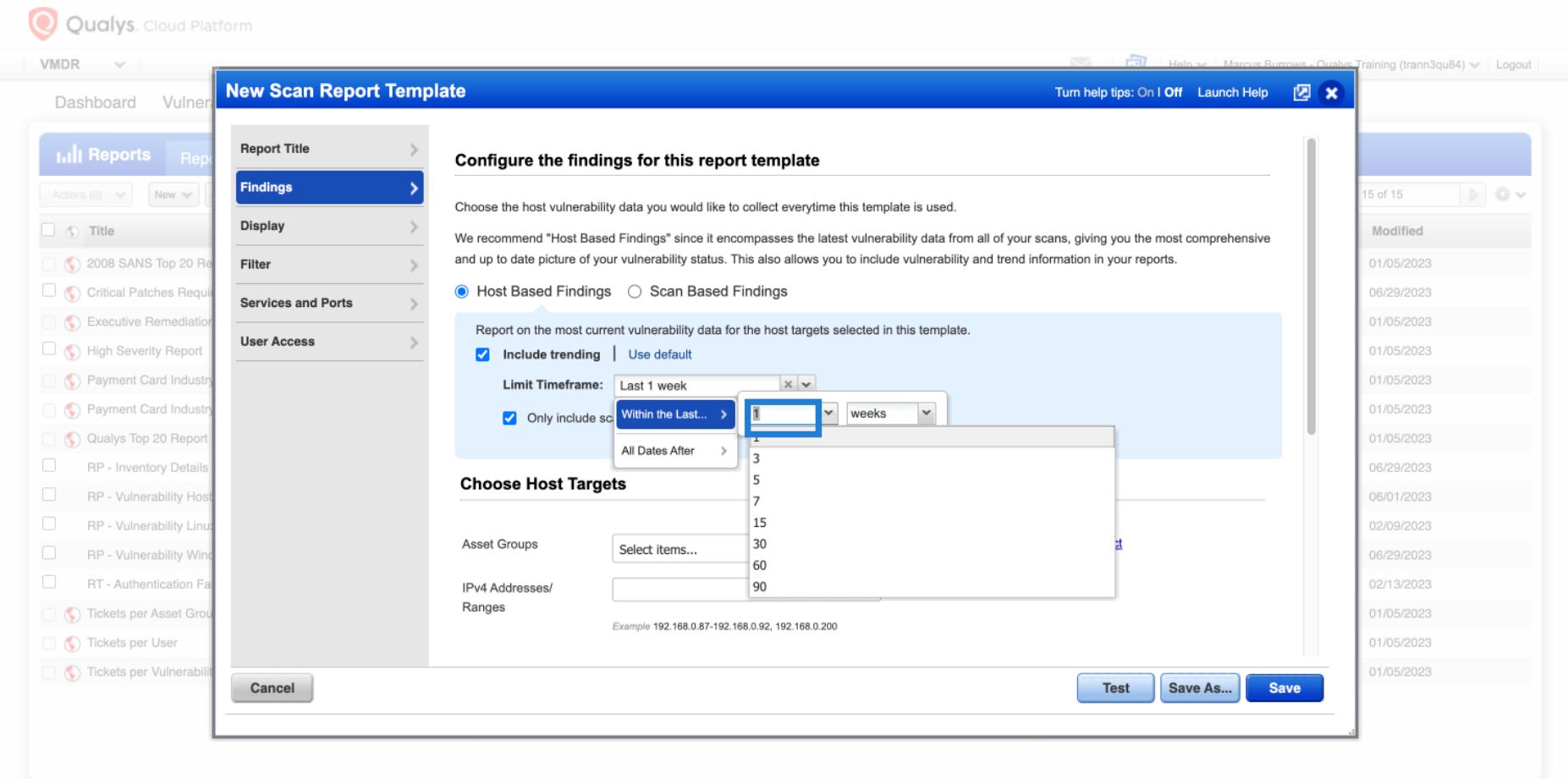
- 1 Click on the drop down to limit the timeframe.



The screenshot shows the 'New Scan Report Template' configuration page in the Qualys Cloud Platform. The left sidebar lists various report types under 'Reports'. The main panel is titled 'Configure the findings for this report template' and includes the following sections:

- Report Title:** A dropdown menu showing 'Findings' is selected.
- Findings:** A detailed section describing Host Based Findings as the recommended choice for collecting the latest vulnerability data from all scans. It includes two radio button options:
 - Host Based Findings
 - Scan Based Findings
- Limit Timeframe:** A dropdown menu set to 'Last 1 week'.
- Choose Host Targets:** Fields for selecting Asset Groups and IPv4 Addresses/Ranges.
- Buttons:** 'Cancel', 'Test', 'Save As...', and 'Save'.

 In the number field, type **4** and press Enter.



The screenshot shows the 'New Scan Report Template' dialog box from the Qualys Cloud Platform. The 'Findings' tab is selected in the left sidebar. The main configuration area is titled 'Configure the findings for this report template'. It includes a note about collecting host vulnerability data and a recommendation for 'Host Based Findings'. A 'Limit Timeframe' section is open, showing a dropdown menu with 'Within the Last...' selected. A numeric input field contains the value '4', which is highlighted with a blue selection bar. Below this, a list of time intervals (1, 3, 5, 7, 15, 30, 60, 90 weeks) is visible. The right side of the dialog shows a preview of 15 report results, each with a timestamp. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

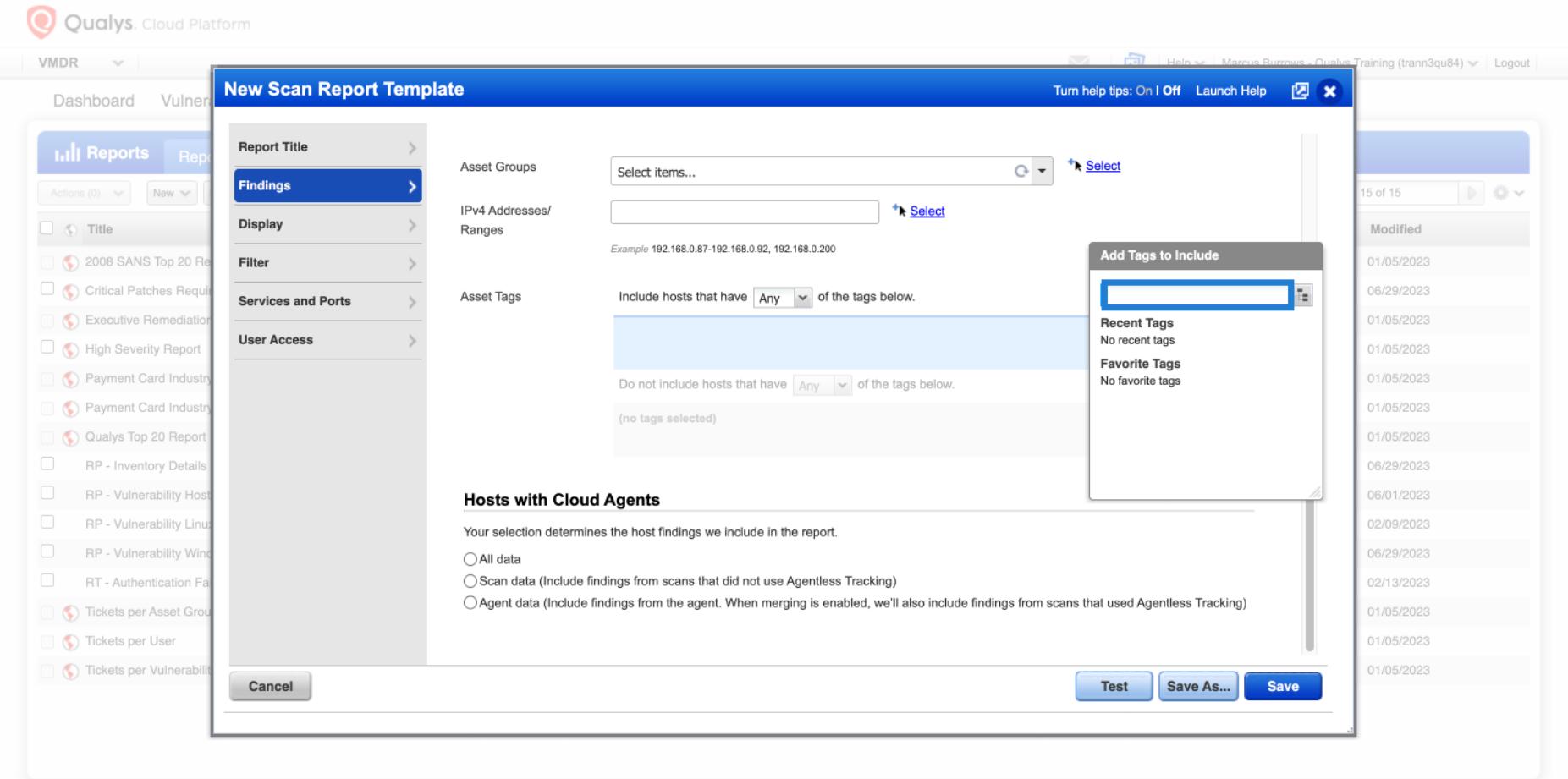
- 1 Click the scroll bar on the right of the dialog to scroll down.

The screenshot shows the 'New Scan Report Template' dialog in the Qualys Cloud Platform. The left sidebar lists various report types under 'Reports'. The main configuration area is titled 'Configure the findings for this report template'. It includes a note about collecting host vulnerability data and a recommendation for 'Host Based Findings'. A 'Limit Timeframe' dropdown is set to 'Last 1 week', with a sub-menu open showing options like 'Within the Last...', '4 weeks', 'days', 'weeks', and 'months'. Below this is a 'Choose Host Targets' section with fields for 'Asset Groups' and 'IPv4 Addresses/Ranges'. At the bottom are 'Test', 'Save As...', and 'Save' buttons. To the right of the dialog, a vertical scroll bar is visible, indicating more content can be viewed by scrolling down.

1 You will now select which Assets to report on. Click on the Add Tag link.

The screenshot shows the 'New Scan Report Template' dialog box from the Qualys Cloud Platform. The left sidebar lists various report templates like 'Findings', 'Display', 'Filter', etc. The main area is titled 'Report Title' with 'Findings' selected. It includes sections for 'Asset Groups' (with a 'Select items...' dropdown and a 'Select' button), 'IPv4 Addresses/Ranges' (with a text input field and a 'Select' button), and 'Asset Tags' (with two dropdown menus: 'Include hosts that have Any of the tags below.' and 'Do not include hosts that have Any of the tags below.', both with 'Add Tag' buttons). Below this is a section titled 'Hosts with Cloud Agents' with three radio button options: 'All data', 'Scan data (Include findings from scans that did not use Agentless Tracking)', and 'Agent data (Include findings from the agent. When merging is enabled, we'll also include findings from scans that used Agentless Tracking)'. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons. To the right of the dialog, there's a vertical list of modified scan reports from May 1st, 2023.

 In the search field, type **windows server** and press Enter



The screenshot shows the 'New Scan Report Template' dialog box in Qualys Cloud Platform. The left sidebar lists report categories: Reports (selected), Findings (highlighted in blue), Display, Filter, Services and Ports, and User Access. The main area is titled 'Report Title' with 'Findings' selected. It includes sections for Asset Groups (with a 'Select items...' dropdown and a 'Select' button), IPv4 Addresses/Ranges (with a dropdown and a 'Select' button), and Asset Tags (with dropdowns for 'Include hosts that have Any of the tags below.' and 'Do not include hosts that have Any of the tags below.', both showing '(no tags selected)'). A modal window titled 'Add Tags to Include' lists 'Recent Tags' (No recent tags) and 'Favorite Tags' (No favorite tags). At the bottom, there's a section titled 'Hosts with Cloud Agents' with radio button options: 'All data', 'Scan data (Include findings from scans that did not use Agentless Tracking)', and 'Agent data (Include findings from the agent. When merging is enabled, we'll also include findings from scans that used Agentless Tracking)'. Buttons at the bottom right include 'Cancel', 'Test', 'Save As...', and 'Save'.

1 Click on the OS - Windows Server Asset Tag

The screenshot shows the 'New Scan Report Template' page in the Qualys Cloud Platform. On the left, there's a sidebar with various report templates like 'Findings', 'Display', 'Filter', 'Services and Ports', and 'User Access'. The main area has sections for 'Report Title' (set to 'Findings'), 'Asset Groups' (with a dropdown menu), 'IPv4 Addresses/Ranges' (with a dropdown menu), and 'Asset Tags'. Under 'Asset Tags', it says 'Include hosts that have Any of the tags below.' Below that is a list of tags with '(no tags selected)'. A modal window titled 'Add Tags to Include' is open, showing a search bar with 'windows server' and a list of tags. One tag, 'OS - Windows Server', is highlighted with a yellow background. At the bottom right of the main screen are 'Test', 'Save As...', and 'Save' buttons.

- 1 You can include both scan data and Cloud Agent data in this report. Towards the bottom of the dialog, click the radio button next to **All data**

The screenshot shows the 'New Scan Report Template' dialog box. On the left, a sidebar lists various report types like 'Findings', 'Display', 'Filter', etc. The main area has sections for 'Asset Groups' (with a dropdown menu), 'IPv4 Addresses/Ranges' (with a dropdown menu), and 'Asset Tags'. Under 'Asset Tags', there's a section to 'Include hosts that have Any of the tags below.' with a dropdown menu showing 'OS - Windows Server'. Below it is a section to 'Do not include hosts that have Any of the tags below.' with a dropdown menu showing '(no tags selected)'. A modal window titled 'Add Tags to Include' is open, showing a search bar with 'windows server' and a list of tags under '01 All Operating Systems', with 'OS - Windows Server' highlighted. At the bottom, there's a section titled 'Hosts with Cloud Agents' with three radio button options: 'All data' (selected), 'Scan data (Include findings from scans that did not use Agentless Tracking)', and 'Agent data (Include findings from the agent. When merging is enabled, we'll also include findings from scans that used Agentless Tracking)'. At the very bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

1 Click on the Filter tab

The screenshot shows the 'New Scan Report Template' dialog box from the Qualys Cloud Platform. The 'Filter' tab is selected in the left sidebar. The main area contains several configuration sections:

- Asset Groups:** A dropdown menu labeled "Select items..." with a "Select" button.
- IPv4 Addresses/Ranges:** An input field with a "Select" button. Example: 192.168.0.87-192.168.0.92, 192.168.0.200.
- Asset Tags:** Includes two sections:
 - "Include hosts that have Any of the tags below." with a "Add Tag" button. One tag is listed: "OS - Windows Server".
 - "Do not include hosts that have Any of the tags below." with a "Add Tag" button. No tags are selected.
- Hosts with Cloud Agents:** A section with three radio button options:
 - All data
 - Scan data (Include findings from scans that did not use Agentless Tracking)
 - Agent data (Include findings from the agent. When merging is enabled, we'll also include findings from scans that used Agentless Tracking)

At the bottom are "Cancel", "Test", "Save As...", and "Save" buttons.

- 1 By default, a Report Template will include all vulnerabilities for the target assets. Click on the [radio button](#) next to "Custom".

The screenshot shows the 'New Scan Report Template' dialog box in the Qualys Cloud Platform. On the left, a sidebar lists various report types: Reports, Findings, Display, Filter (which is selected), Services and Ports, and User Access. The main area has two sections: 'Selective Vulnerability Reporting' and 'Included Operating Systems'. In 'Selective Vulnerability Reporting', there is a note about complete or custom reporting, a radio button for 'Complete' (selected), a radio button for 'Custom', and a checkbox for 'Exclude QIDs'. In 'Included Operating Systems', a list of systems is shown with checkboxes, many of which are checked. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

1 Click Add Lists

The screenshot shows the 'New Scan Report Template' dialog box from the Qualys Cloud Platform. On the left, a sidebar lists various report types: Title, 2008 SANS Top 20 Report, Critical Patches Required, Executive Remediation, High Severity Report, Payment Card Industry, Payment Card Industry, Qualys Top 20 Report, RP - Inventory Details, RP - Vulnerability Host, RP - Vulnerability Linux, RP - Vulnerability Windows, RT - Authentication Fail, Tickets per Asset Group, Tickets per User, and Tickets per Vulnerability. The 'Filter' option is selected. The main area is titled 'Selective Vulnerability Reporting' and contains two sections: 'Services and Ports' and 'User Access'. Under 'Services and Ports', there are two entries: 'Info Title' (with a note 'There is no data in this list.') and another 'Info Title'. Below these are 'Add Lists' and 'Clear All' buttons. There is also a checkbox for 'Exclude QIDs'. The right side of the dialog box shows a preview of the report results, which are mostly empty. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

- 1 Click on the check box next to "Patch Tuesday - Microsoft - October 2023".

Select Vulnerability Search Lists

Search List	Info	Title	Source	User	Modified
Search List Library	<input type="checkbox"/>	Adobe Vulnerabilities v.1	Dynamic	Marcus Burrows - Qualys Training	02/17/2023
	<input type="checkbox"/>	Cloud Agent QIDs	Dynamic	Marcus Burrows - Qualys Training	09/18/2023
	<input type="checkbox"/>	Inventory Results v.1	Static	Marcus Burrows - Qualys Training	02/17/2023
	<input type="checkbox"/>	Log4Shell Dynamic Search List v1.1	Dynamic	Marcus Burrows - Qualys Training	02/17/2023
	<input type="checkbox"/>	Patch Tuesday - Microsoft - October 2023	Static	Marcus Burrows - Qualys Training	09/29/2023
	<input type="checkbox"/>	Patchable Severity 4+5 Vulnerabilities v.1	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	Predicted High Risk Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	03/28/2023
	<input type="checkbox"/>	Ransomware	Dynamic	Marcus Burrows - Qualys Training	09/18/2023
	<input type="checkbox"/>	SL - Adobe Flash Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - All New Vulns (24 hours)	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - Authentication Failures	Static	Marcus Burrows - Qualys Training	05/10/2023
	<input type="checkbox"/>	SL - CA Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - CVSS EQ or GT 0	Dynamic	Marcus Burrows - Qualys Training	06/29/2023

OK Close

1

Click OK

Select Vulnerability Search Lists

Search List	Info	Title	Source	User	Modified
	<input type="checkbox"/>	Adobe Vulnerabilities v.1	Dynamic	Marcus Burrows - Qualys Training	02/17/2023
Search List Library	<input type="checkbox"/>	Cloud Agent QIDs	Dynamic	Marcus Burrows - Qualys Training	09/18/2023
	<input type="checkbox"/>	Inventory Results v.1	Static	Marcus Burrows - Qualys Training	02/17/2023
	<input type="checkbox"/>	Log4Shell Dynamic Search List v1.1	Dynamic	Marcus Burrows - Qualys Training	02/17/2023
	<input checked="" type="checkbox"/>	Patch Tuesday - Microsoft - October 2023	Static	Marcus Burrows - Qualys Training	09/29/2023
	<input type="checkbox"/>	Patchable Severity 4+5 Vulnerabilities v.1	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	Predicted High Risk Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	03/28/2023
	<input type="checkbox"/>	Ransomware	Dynamic	Marcus Burrows - Qualys Training	09/18/2023
	<input type="checkbox"/>	SL - Adobe Flash Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - All New Vulns (24 hours)	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - Authentication Failures	Static	Marcus Burrows - Qualys Training	05/10/2023
	<input type="checkbox"/>	SL - CA Vulnerabilities	Dynamic	Marcus Burrows - Qualys Training	06/29/2023
	<input type="checkbox"/>	SL - CVSS EQ or GT 0	Dynamic	Marcus Burrows - Qualys Training	06/29/2023

OK Close

- 1 The report will now contain only information about discovered vulnerabilities which are included in this particular Search List. Click on the **Display tab** to continue.

The screenshot shows the 'New Scan Report Template' dialog in the Qualys Cloud Platform. The 'Filter' tab is selected. Under 'Selective Vulnerability Reporting', the 'Custom' option is chosen, and a list of vulnerabilities is displayed, including 'Patch Tuesday - Microsoft - October 2023'. Below this, there is an 'Included Operating Systems' section with checkboxes for 3Com, AB, ADTX, and AIX, all of which are checked. On the right side of the dialog, a sidebar shows a list of modified items from June 2023. At the bottom right of the dialog are 'Test', 'Save As...', and 'Save' buttons.

- 1 There are different display options to choose from, depending on who the report is for, and what the report is intended to convey. Click on the **scroll bar** on the right of the dialog to scroll down.

The screenshot shows the 'New Scan Report Template' dialog box. On the left, there's a sidebar with various report templates like 'Title', '2008 SANS Top 20 Report', 'Critical Patches Required', etc. The main area has a title 'Report Summary' and a sub-section 'Summary of Vulnerabilities' with a checked checkbox for 'Text Summary'. Below that is a 'Graphics' section with many checkboxes for different types of reports. At the bottom is a 'Custom Footer' section with a checkbox for 'Include this text in the report footer' and a text input field. At the very bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons. To the right of the dialog, there's a vertical scroll bar, and further right, a sidebar showing a list of modified dates from '01/05/2023' to '01/05/2023'.

1 Click the **check box** next to Vulnerability Details

The screenshot shows the 'New Scan Report Template' dialog box in the Qualys Cloud Platform. The left sidebar lists report categories: Reports, Findings, Display (selected), Filter, Services and Ports, and User Access. The main area is titled 'Include the following detailed results in the report'. Under 'Display', the 'Text Summary' checkbox is checked. Other checkboxes include 'Vulnerability Details' (unchecked), 'Threat' (unchecked), 'Impact' (unchecked), 'Solution' (unchecked), 'Patches and Workarounds' (unchecked), 'Virtual Patches and Mitigating Controls' (unchecked), 'Compliance' (unchecked), 'Exploitability' (unchecked), 'Associated Malware' (unchecked), 'Results' (unchecked), 'Reopened' (unchecked), 'Detection Logic' (unchecked), 'TruRisk Details(TruRisk Score, ACS, QDS)' (checked), and 'Appendix' (unchecked). Below this is a section titled 'Exclude Account ID' with a note: 'By default we'll include the account login ID in the filename of downloaded reports and in the report content. Select this option to remove the login ID.' A checkbox for 'Exclude account login ID' is unchecked. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons. To the right of the dialog, a sidebar shows a list of modified items from page 15 of 15, with dates ranging from 01/05/2023 to 01/05/2023.

1 Click the **check box** next to Results

The screenshot shows the 'New Scan Report Template' dialog box from the Qualys Cloud Platform. The left sidebar lists report categories: Reports, Findings, Display (which is selected), Filter, Services and Ports, and User Access. The main content area is titled 'Include the following detailed results in the report'. Under 'Display', several checkboxes are available, with 'Vulnerability Details' and 'TruRisk Details(TruRisk Score, ACS, QDS)' being checked. Other options like 'Text Summary', 'Threat', 'Impact', 'Solution', and various compliance and exploitability details are also listed. Below this is a section titled 'Exclude Account ID' with a checkbox for 'Exclude account login ID'. At the bottom are 'Cancel', 'Test', 'Save As...', and 'Save' buttons.

1 Click Save

The screenshot shows the 'New Scan Report Template' dialog box in the Qualys Cloud Platform. The left sidebar lists report categories: Reports, Findings, Display (selected), Filter, Services and Ports, and User Access. The main area is titled 'Include the following detailed results in the report'. It contains several checkbox groups:

- Text Summary
- Vulnerability Details
 - Threat
 - Impact
- Solution
 - Patches and Workarounds
 - Virtual Patches and Mitigating Controls
- Compliance
- Exploitability
- Associated Malware
- Results
 - Reopened
 - Detection Logic
- TruRisk Details(TruRisk Score, ACS, QDS)
- Appendix

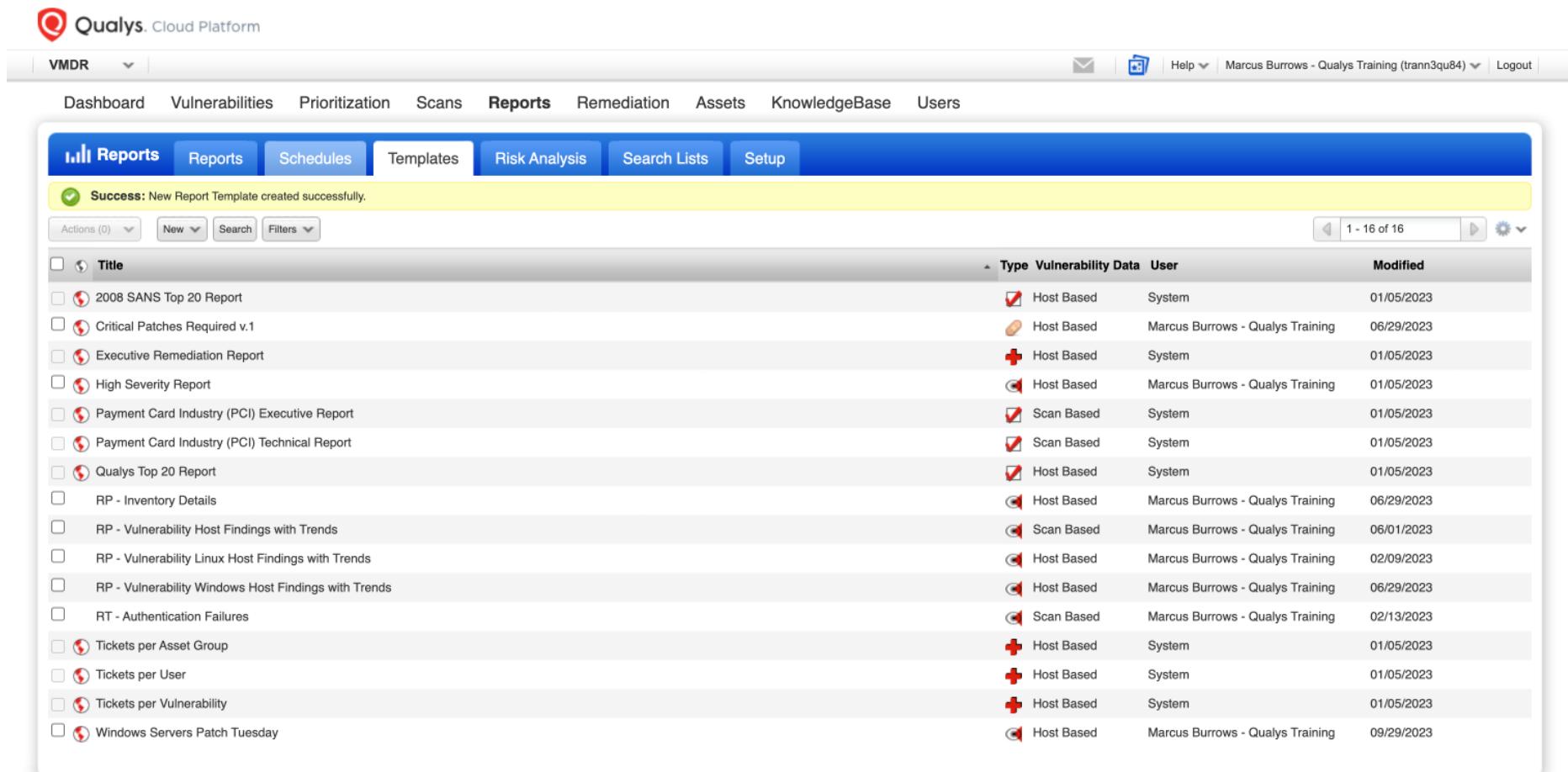
Exclude Account ID

By default we'll include the account login ID in the filename of downloaded reports and in the report content. Select this option to remove the login ID.

Exclude account login ID

At the bottom are three buttons: Cancel, Test, Save As..., and Save (highlighted in blue).

- 1 The Report Template has been successfully created. Next, click on the Reports tab.



The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports (which is the active tab), Remediation, Assets, KnowledgeBase, and Users. A success message at the top states "Success: New Report Template created successfully." Below the message is a toolbar with buttons for Actions (0), New, Search, and Filters. The main content area displays two tables. The left table lists various report templates with icons and titles such as "2008 SANS Top 20 Report", "Critical Patches Required v.1", and "Qualys Top 20 Report". The right table lists vulnerability data with columns for Type (Host Based or Scan Based), Vulnerability Data, User (System or Marcus Burrows - Qualys Training), and Modified date. There are 16 items listed in the right table, ranging from 01/05/2023 to 09/29/2023.

Type	Vulnerability Data	User	Modified
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	01/05/2023
Scan Based	System	System	01/05/2023
Scan Based	System	System	01/05/2023
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Scan Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/01/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	02/09/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	06/29/2023
Scan Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	02/13/2023
Host Based	System	System	01/05/2023
Host Based	System	System	01/05/2023
Host Based	System	System	01/05/2023
Host Based	Marcus Burrows - Qualys Training	Marcus Burrows - Qualys Training	09/29/2023

- 1 Click on the New button

The screenshot shows the Qualys Cloud Platform interface. At the top, there's a navigation bar with links like VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports (which is currently selected), Remediation, Assets, KnowledgeBase, and Users. Below this is a toolbar with buttons for Reports, Schedules, Templates, Risk Analysis, Search Lists, and Setup. The main area is titled 'Reports' and contains a table with columns: View, Report Title, Type, Launched, Report Template, User, Format, Created, Expires, Size, and Status. A search bar at the top of the table allows filtering by 'Actions (0)', 'New', 'Search', and 'Filters'. A message 'No reports found.' is displayed below the table. The 'New' button in the toolbar is highlighted with a blue border.

- 1 Click on "Template Based ..."

The screenshot shows the Qualys Cloud Platform interface. The top navigation bar includes links for VMDR, Dashboard, Vulnerabilities, Prioritization, Scans, Reports (which is the active tab), Remediation, Assets, KnowledgeBase, and Users. Below the navigation is a toolbar with icons for Actions, New, Search, and Filters. A dropdown menu is open under the 'New' button, showing options like Scan Report, Scorecard Report..., Map Report..., Patch Report..., Authentication Report, Remediation Report..., Compliance Report..., Asset Search Report..., and Download... The 'Scan Report' option is highlighted with a yellow background. A sub-menu for 'Scan Report' is displayed, containing 'Template Based...' and 'PCI Scan Template...'. The main content area shows a table header for 'Reports' with columns: User, Format, Created, Expires, Size, and Status. The message 'No reports found.' is displayed below the table.

-  As the name for this report, type **Patch Tuesday Report** and press Enter

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: *  [Select](#)

Report Format: *  [HTML pages](#)

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups    [Select](#)

IPv4 Addresses/
Ranges    [Select](#)

Example 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags Any  of the tags below. [Add Tag](#)

(no tags selected)

Do not include hosts that have Any  of the tags below. [Add Tag](#)

- 1 You now need to select the Template which you created earlier. Click on the [Select](#) hyperlink.

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: *  [Select](#)

Report Format: * 

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups    [Select](#)

IPv4 Addresses/
Ranges  [Select](#)

Example 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags of the tags below. [Add Tag](#)

(no tags selected)

Do not include hosts that have of the tags below. [Add Tag](#)

- 1 Click on the radio button next to "Windows Servers Patch Tuesday".

Select a Report Template

Info	Title	Type	Source	User	Modified
<input checked="" type="radio"/>	High Severity Report	Host	Based	Marcus Burrows - Qualys Training	01/05/2023
<input type="radio"/>	RP - Inventory Details	Host	Based	Marcus Burrows - Qualys Training	06/29/2023
<input type="radio"/>	RP - Vulnerability Host Findings with Trends	Scan	Based	Marcus Burrows - Qualys Training	06/01/2023
<input type="radio"/>	RP - Vulnerability Linux Host Findings with Trends	Host	Based	Marcus Burrows - Qualys Training	02/09/2023
<input type="radio"/>	RP - Vulnerability Windows Host Findings with Trends	Host	Based	Marcus Burrows - Qualys Training	06/29/2023
<input type="radio"/>	RT - Authentication Failures	Scan	Based	Marcus Burrows - Qualys Training	02/13/2023
<input type="radio"/>	Windows Servers Patch Tuesday	Host	Based	Marcus Burrows - Qualys Training	09/29/2023

Search Filters 1 - 7 of 7

Templates > Template Library >

Select Cancel

- 1 Click Select

Select a Report Template

Info	Title	Type	Source	User	Modified
<input type="radio"/>	High Severity Report	Host Based	Marcus Burrows - Qualys Training	01/05/2023	
<input type="radio"/>	RP - Inventory Details	Host Based	Marcus Burrows - Qualys Training	06/29/2023	
<input type="radio"/>	RP - Vulnerability Host Findings with Trends	Scan Based	Marcus Burrows - Qualys Training	06/01/2023	
<input type="radio"/>	RP - Vulnerability Linux Host Findings with Trends	Host Based	Marcus Burrows - Qualys Training	02/09/2023	
<input type="radio"/>	RP - Vulnerability Windows Host Findings with Trends	Host Based	Marcus Burrows - Qualys Training	06/29/2023	
<input type="radio"/>	RT - Authentication Failures	Scan Based	Marcus Burrows - Qualys Training	02/13/2023	
<input checked="" type="radio"/>	Windows Servers Patch Tuesday	Host Based	Marcus Burrows - Qualys Training	09/29/2023	

Select **Cancel**

- 1 There are different report formats to choose from. Again, the choice will depend on who the report is for, and how the recipient intends to use the information. Click on the [drop down](#) next to "Report Format".

New Scan Report

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: * [Select](#)

Report Format: * [Select](#)

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups [Select](#)

IPv4 Addresses/
Ranges [Select](#)

Example 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags of the tags below. [Add Tag](#)

OS - Windows Server [X](#)

Do not include hosts that have of the tags below. [Add Tag](#)

1 Click Comma-Separated Value (CSV)

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title: Patch Tuesday Report

Report Template: * Windows Servers Patch Tuesday Select

Report Format: * HTML pages CSV Comma-Separated Value (CSV) XML Extensible Markup Language (XML) HTML pages DOC Microsoft Document (DOCX) PDF Portable Document Format (PDF) MHT Web Archive (MHT) -- Internet Explorer for Windows o...

Report Source*

Select at least one asset type:

Asset Groups

IPv4 Addresses/
Ranges

Asset Tags

Include hosts that have Any of the tags below. Add Tag

OS - Windows Server X

Do not include hosts that have Any of the tags below. Add Tag

- 1 Click on the scroll bar on the right of the dialog box to scroll down.

New Scan Report Launch Help

Use the following form to create a new report on scan data.

Report Details

Title:

Report Template: *  [Select](#)

Report Format: * 

Do not show header in CSV report layout.

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups   [Select](#)

IPv4 Addresses/
Ranges  [Select](#)

Example 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags Include hosts that have of the tags below. [Add Tag](#)

 [X](#)

Do not include hosts that have of the tags below. [Add Tag](#)

- 1 Notice that the target assets setting has been inherited from the template, but could be changed if required. Click on Run.

Report Settings Comma-separated Value (CSV)

Do not show header in CSV report layout.

Report Source*

Select at least one asset group or IP to draw data from.

Asset Groups [Select](#)

IPv4 Addresses/
Ranges [Select](#)

Example 192.168.0.87-192.168.0.92, 192.168.0.200

Asset Tags of the tags below. [Add Tag](#)

OS - Windows Server

Do not include hosts that have of the tags below. [Add Tag](#)

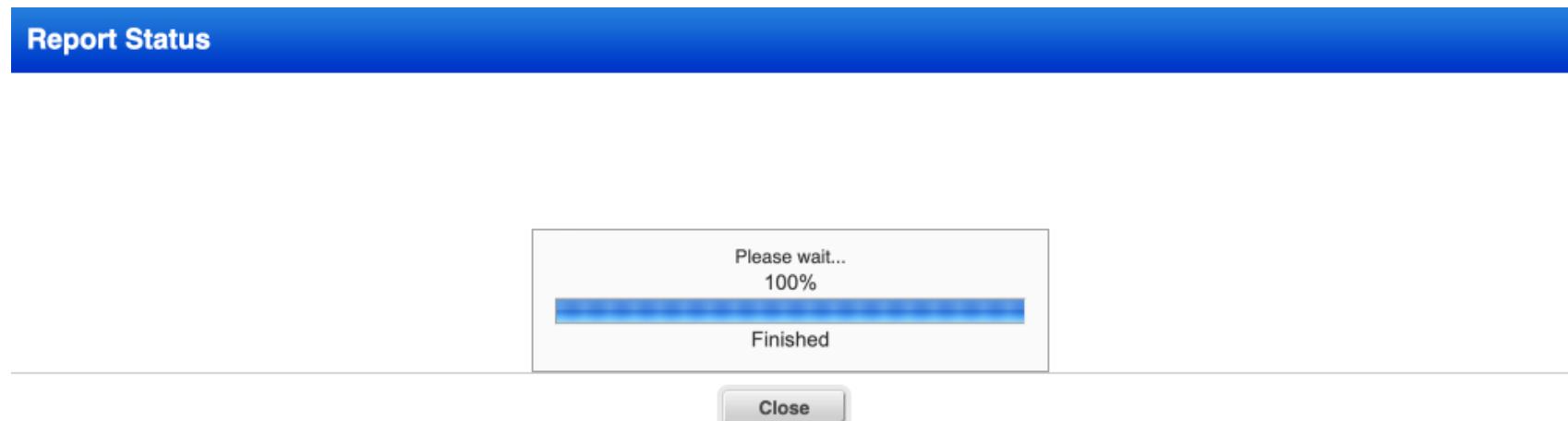
(no tags selected)

Report Options

Scheduling

[Run](#) [Cancel](#)

- i** The report runs immediately. When the report has completed running, the user is prompted to download the CSV file to the local computer. Click [Close](#)



- 1** In this lab, you have created a Report Template and run a report based on that template. When required, the template could be changed to include a different Search List with the latest Patch Tuesday vulnerabilities. That's it. You're done.

diorad | Creating a custom report

The screenshot shows the Qualys Cloud Platform interface, specifically the Reports section. The top navigation bar includes links for Dashboard, Vulnerabilities, Prioritization, Scans, Reports, Remediation, Assets, KnowledgeBase, and Users. The Reports tab is currently selected. Below the navigation is a toolbar with Actions (0), New, Search, and Filters buttons. A progress bar indicates 1 - 1 of 1. The main content area displays a table with one row of data:

View Report Title	Type Launched Report Template	User	Format	Created	Expires	Size	Status
<input type="checkbox"/> Patch Tuesday Report	Windows Servers Patch Tuesday	Marcus Burrows - Qualys Training	CSV	09/29/2023	10/06/2023	1003 bytes	Finished



Scan to go to the interactive player