0 - Table of Contents

Sagacity User Guide

Last Updated: 4 Jun 17

Welcome to Sagacity User Guide. This document provides a discussion of the assessment process and how to use the tool to support the process. It also includes instructions for some of the command line tools "under the hood" and a cheat sheet for common target and scanning commands used during the assessment.

Table of Contents

Top

1 - Introduction

The process of conducting a Security Assessment (a.k.a. Security Test and Evaluation – ST&E, Security Control Assessment – SCA, Vulnerability Assessment, Compliance Audit, etc.) and producing accurate, consistent and repeatable Risk Assessment results is incredibly challenging (if not impossible) without at least some level of automation. DISA has provided a number of automated tools that produce STIG checklist results, but they suffer from various shortcomings. The Sagacity, originally created as a set of Perl scripts written for a government customer to try to eliminate paper checklists and make sense of a mountain of scan data, has grown into a full-fledged web application that makes the Security Assessment data management problem much more manageable. Some of the issues that the Sagacity tries to solve are:

- Existing DISA and commercial tools only automate portions of vulnerability testing testing, requiring analysts to conduct extensive manual reviews using poorly designed and inefficient interfaces and often confusing and incomplete instructions. There is no easy-to-read, consistent data file or STIG checklist format that allows correlation of data across multiple systems of different types.
- The previous STIG Checklists were designed to be printed and filled out manually, introducing incredible inefficiency, waste and the potential for introducing errors while transcribing findings from paper to computer.

- The current XCCDF STIG Checklist Viewer works with data from one host and checklist at a time and is very inefficient for assessing multiple checklists across multiple systems.
- The RMF/CCI IA Control relationships for the individual Potential Discrepancy Items (PDIs) in the STIG Checklists are sometimes missing or incorrect.
- The VMSIDs and PDI Numbers (STIG IDs) are inconsistent and incomplete, and there is no way of easily comparing results with other vulnerability assessment tools like Tenable Nessus® or Security Compliance Checker.
- There is no way to easily consolidate and view host-level configuration information to make assessing some PDIs faster and more efficient.
- Tracking procedural RMF control findings, associating them with the correct technical findings, and producing a combined set of results for use in a Risk Assessment is very difficult and time-consuming.

This user guide describes the Sagacity web interface and additional tools to address the problems above. It will discuss the Security and Risk Assessment process, instructions for using Sagacity and finally ideas for future enhancements. It is more than just a guide for the tool, but a guide for performing security testing and creating Risk Assessments.

Top

1.1 - Audience

This user guide is written for two audiences. The first is the skilled, technical security analyst who will use the web interface and tools. The analyst must have a firm understanding of the assessment process and a working knowledge of tools like the SPAWAR Security Compliance Checker (SCC), Tenable Nessus™, nmap, Microsoft Baseline Security Analyzer and others as well as a strong background in Windows, Unix and networking. Additionally, the analyst must be experienced using office software like Microsoft Excel or LibreOffice Calc. Although not completely necessary, a basic knowledge of scripting in PHP and MySQL is also helpful.

The second audience is management personnel who may be considering having their organization use these tools. Section 2 on the assessment and Risk Assessment process provides an overview of the tools and the costs and benefits of using them.

Top

1.2 - Availability

Sagacity, produced by Cyber Perspectives, LLC is freely available as an open source tool from the Sagacity SourceForge Project Page.

Sagacity is a rebranded, significantly modified release of the ST&E Manager, which was licensed, per government direction, under the Modified BSD (3 Clause) License. ST&E Manager was created by Salient Federal Solutions and Science Applications International Corporation under Contracts W91260-09-D-0006-1201 and FA8823-07-D-0004. Under those contracts, Salient Federal Solutions and SAIC (now Leidos) own the copyright to their respective portions of that software, and the United States Government acquired unlimited rights to that computer software (48 C.F.R. 252.227-7014(a)(16)).

We would like to thank a number of individuals for their significant contributions to both the concepts and code. Please see Contributors.txt for a complete list.

We are excited to see the Sagacity user community grow and more people contribute their time and talents to its success. At Cyber Perspectives we are constantly trying to improve our software. Please e-mail any bugs or feature ideas to developers@cyberperspectives.com subject Sagacity Ideas or Sagacity Bugs, or you can create a Sagacity Ticket in the SourceForge Project Page.

Top

1.3 - No IA Functionality

The Sagacity web interface does not provide any IA or security-related functionality. It relies on the operating system, Apache web server and MySQL databases to provide that functionality. The latter two systems are configured to only allow connections from the local system (loopback interface). The operating system provides all user authentication, access control and audit functionality. *The web interface is not IA-enabled.*

Because of this, Sagacity cannot be used in a networked or multi-user configuration. Apache and MySQL **must not** be allowed to listen on the network. When installed and used as designed, Sagacity can be used on accredited systems and desginated as non-IA enabled software. It is currently approved for use on at least one AFSPC accredited system. Completed Apache and MySQL STIG eChecklists are available on request.

Top

2 - Security and Risk Assessment Process

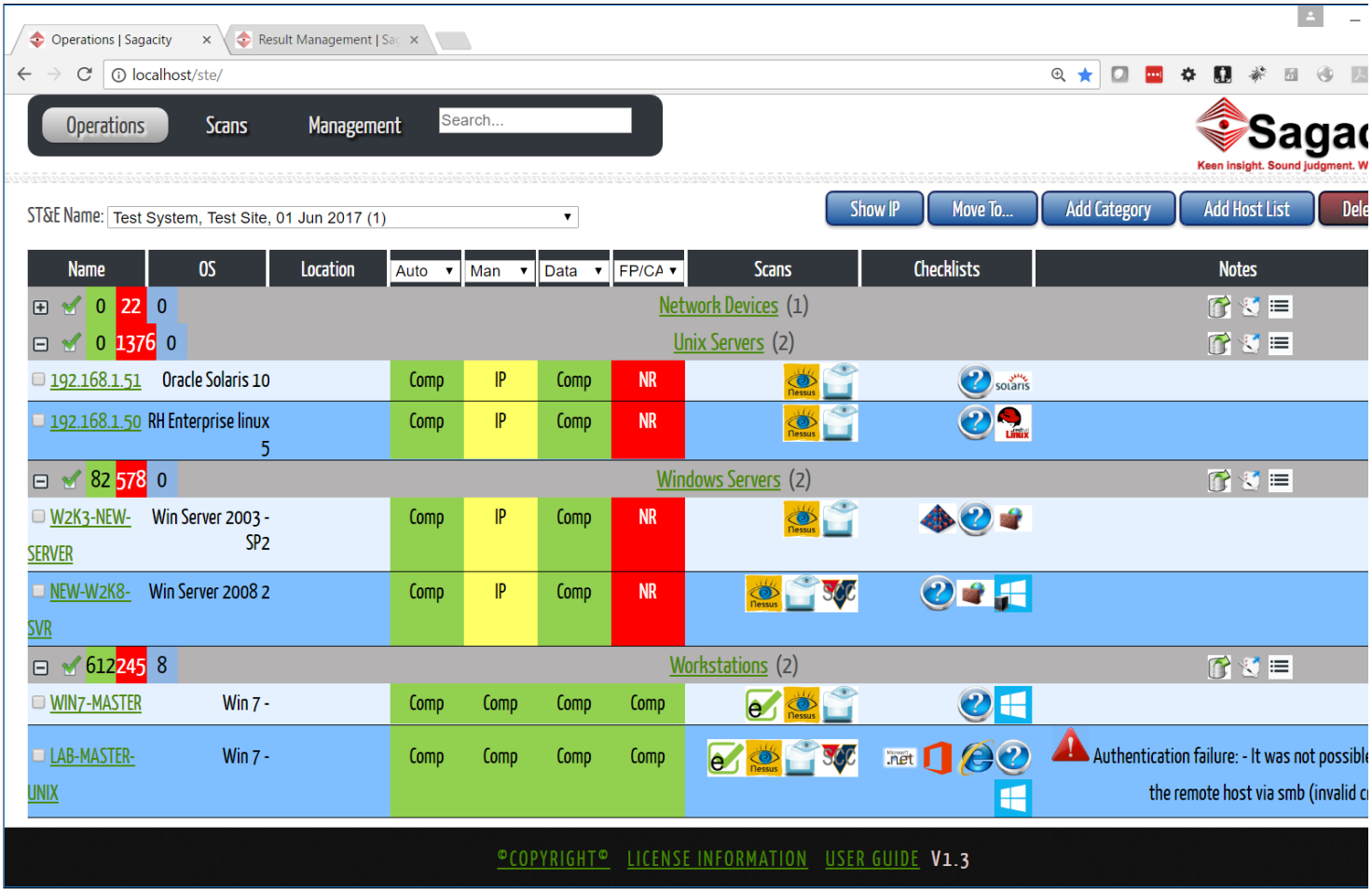
Sagacity provides a framework for collecting and analyzing assessment data and eventually will produce a portion of the Risk Assessment Report. This section provides a general description of the security and risk assessment processes that Sagacity is designed around. Section 3 describes tool usage in detail.

The following sections describe the tools and web interface used to feed data into the eChecklist database during the assessment, using the Excel eChecklists for data analysis and correlation, and exporting and converting the eChecklist data to produce a draft Risk Assessment.

Top

2.1 - Security Assessment

An assessment involves gathering configuration data from all systems within scope, performing automated and manual tests, collecting the test data in a central location and tracking progress. The Sagacity Web Interface was designed to streamline and track those tasks.



Sagacity Home Page

There are currently two primary pages in Sagacity interface (see the screenshot, above). The **Operations** menu contains ST&E Operations page, shown above. (In the future it will also contain Checklist Operations and Procedural Operations). **ST&E Operations**, shown above, provides the primary management interface, listing the targets (systems under test) by category (servers, workstations, etc.) and showing the status of various assessment tasks such as automated tests, manual reviews, data gathering and false-positive/Cat I finding reviews. Clicking on individual targets will bring up a host details page with TCP/UDP ports, installed software, applicable STIG checklists and other data. Clicking on the category names will open an eChecklist summary page for that group of targets that can be exported to Excel. This page and its functionality are covered in section 3.1

The **Scans** menu contains both the Results page and Add Scan shortcut. The **Result Management** page allows the user to import and manage test data from Nessus®, DISA Security Compliance Checker (SCC), STIG Viewer, NMap, collected host data, Microsoft Security Baseline Analyzer (MBSA) and eChecklists (more scan types will be added as development progresses), which populates the database with STIG findings and information about each target. It displays information about scan results as they are being processed as well as summary information about each input file, including the number of hosts and number of findings is included to assist with file management. This page and its functionality are covered in section 3.3. **Add Scan** is a shortcut to the Import button on the Results page, and provides an interface to upload new scan files.

The **Management** menu is a collection of tools to manage higher level information about the mission systems, sites and assessments in the database as well as administrative functions like catalog management, settings and a database search capability. This page and its functionality are covered in section 3.4.

Note at the bottom of the page the **Copyright**, **License Information** and **User Guide** links and version number.

The use of these interfaces is described in detail in the following sections, but the overall workflow for an assessment would be as described in the following sections.

Top

2.1.1 - Pre Assessment

- Under the Management menu, create a Mission System, Site(s) and ST&E(s) for the testing . Each system can have multiple sites, and each site can have multiple assessments. This helps to better organize the data and will provide a way to search and compare current data with previous tests or similar systems.
- Review the system hardware and software lists, identify the applicable STIG checklists for each host. Create a scan plan for providing the most coverage possible with automated scans. Identify checklists and hosts that require manual testing and plan the time required for that testing.
- Populate known targets requiring purely manual testing in the ST&E Operations page using the CSV formatted host list or previous scan results, hardware/software lists or network diagrams. Associate those targets with the expected manual STIG checklists and export those eChecklists beforehand. (Note that Sagacity has the ability to automatically populate targets and some checklists based on the operating system or software installed on the targets discovered by the automated scanning tools.)
- Group the targets into the appropriate categories like server, workstation, network device, printer, etc. A user can create, modify or delete any category except for the default “unassigned” category, allowing each assessment to be customized to the system. (There is also an autocategorize feature that can categorize targets based on detected operating system.)
- Select the appropriate assessment tasks (automated scans, manual testing, host data collection, false positive and Cat I reviews) for each target as part of the planning process.

Top

2.1.2 - During Assessment

- As automated scans are completed, import the scan data into the database using the Scans → Results page. Make sure that the expected hosts and findings are ingested and correctly categorized on the assessment Operations page. Based on scan results, Sagacity may identify hosts and checklists requiring testing that were previously overlooked.
- Review the STIG checklists associated with the targets and make any necessary changes. A post-processing script will identify additional applicable STIG checklists based on the installed software discovered by Nessus® scans and SCC results.
- Export eChecklists for assessment personnel to perform the remaining manual tests from the STIG checklists. This can be done either from the category bar or from within the category information page. Testing with multiple automated tools can reduce false positives and improve STIG coverage, reducing the amount of manual tests required.
- When manual tests and false positive/Cat I checks are complete, import the completed eChecklists using the Scans → Results page.
- Track task progress and for individual hosts using the task dropdowns on the assessment Operations page.
- Review the results to identify any missing results, conflicts, technical findings associated with the wrong IA control and other potential issues. Correct as many as possible before leaving the test site.

The recommended order of operations for loading scan results in Sagacity is:

- *Discovery and Vulnerability Scans*: Nmap, Nessus® discovery, Nessus® vulnerability. These scans help Sagacity identify the Operating Systems, installed software, network services and applicable STIGs for the hosts.
- *Compliance Scans*: Nessus® compliance scans, SCC. These scans provide automated STIG compliance testing data so Sagacity can identify the remaining manual tests required.
- (Export eChecklists, perform manual testing)
- *Manual compliance test results*: Completed eChecklists, STIG Viewer .ckl. This completes the STIG assessment and allows the final results to be exported as either eChecklists, STIG Viewer or both.

Top

2.1.3 - Post Assessment

- Review the results to identify incorrectly assessed checks, perform root cause and risk analysis and develop a list of recommendations for the program office.
- Export the final technical eChecklists for each category, which become artifacts for the Risk Assessment and C&A package. The final eChecklists can also be given to the site lead and/or vendor for remediation of findings.
- If needed, export the technical findings in STIG Viewer .ckl format.

Top

2.2 - Risk Assessment

Sagacity, originally developed to support DIACAP assessments, is transitioning to support the NISP SP 800-30 *Guide for Conducting Risk Assessments* methodology for a qualitative risk assessment.
Risk Assessment analysis and reporting will be one of the next priorities for development on Sagacity.

Top

3 - Usage Instructions

The following sections provide specific instructions for using the Sagacity web interface. It will cover the three main tabs and provide the detailed steps for the process outlined in section 2.1.

Top

3.1 - ST&E Operations

The ST&E Operations page is the main "Home" page for Sagacity. The page provides a quick view of the progress of the overall assessment and provides an interface for organizing, reviewing and exporting assessmeht related data. The following sections describe the page in detail.

Top

3.1.1 - Categories

Individual hosts are organized into categories. The blue buttons on the top right of the page can be used to move hosts between categories, manage categories and create new targets. Categories should be customized for each system by separating targets into groups of like operating system and functionality. Changing categories in one assessment will not affect other assessments.

When you **Add Category** you can select the expected scans for targets in the category, then the scan images (shown in 3.1.2 below) will show grey until a scan of that type is ingested for that target.

Add Host List can be used to quickly add a large number of targets using a specially formatted .CSV file, located in the /docs folder.

The **Unassigned** category is the default category for all new auto-populated targets. It cannot be deleted or renamed, and will not appear if it does not contain any hosts. New targets should be moved from Unassigned to the appropriate category as soon as possible as this category has limited functionality. On the right side of the Unassigned category bar is the Auto-Categorization button. Clicking it will reassign any targets in unassigned to new categories based on the detected Operating System listed in the OS/Software column. Please note that targets with a Generic OS (unknown/unspecified) will not be auto-categorized.

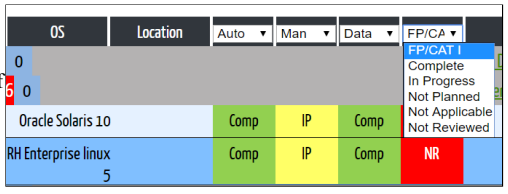
Clicking on the category name (except for Unassigned) will open the eChecklist export page, which is described in section 3.1.4. A quick eChecklist export can be accomplished with the green-arrowed export icon on the right side of the bar.

ST&E Operations Tab

Top

3.1.2 - Device/Category Table

The table on the assessment Operations page contains the individual targets and categories. The following list below defines each of the table columns and text fields being used.

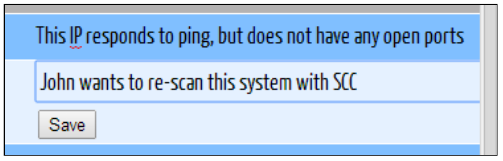


- **Device Name**: The formal name of the host is set by default to the hostname, the fully qualified domain name (FQDN) or IPv4 address. This name can be changed to the formal name of the target as you want to see it in the final reports. For example, cps1 could be renamed "Core Processing Server 1." Be aware, however, that changing the formal name could cause newly ingested scans to create a "new" host instead of adding results to the existing host. The **Show IP** button on the Ops page will toggle between displaying IP address and hostname.
- **OS/Software**: This is the Operating System of the host as set on the Host Information page. It is displayed here to help organize like systems. The **Auto-Categorize** button on the Unassigned category will create categories and move hosts based on the detected Operating System.
- **Location**: This is a text field set on the Host Information page used to describe where the target is physically located. The field is not required, but is helpful for organizing the targets and managing the assessment. It could be set to something like "Server Room" or "Ops Floor." This field is not used elsewhere (for now), so it will not show up in any reports.
- **Tasks**: The four task columns can be used to track which assessment tasks have been completed for each host. The four columns are, by default, Automated scans, Manual STIG checks, target data and configuration gathering, and False Positive/Cat I manual reviews. To change the status, select the target checkbox for the desired targets, then use the column heading drop down box to change the status. During the course of the assessment, the statuses will go from red to yellow to green after the page refreshes The statuses are:
  - *Complete*: The task is complete for this host.
  - *In Progress*: The task has started, but is not yet complete.
  - *Not Planned*: The task is applicable, but not planned for this assessment
  - *Not Applicable*: The task is not applicable for this target. For example, there may not be an automated scanner available for a network device or printer.
  - *Not Reviewed*: The default category is that the test is planned, but not yet started.

- **Scans:** The icons here represent the scan types providing information for this host. This can be useful for tracking assessment progress and also for identifying missing scan information for specific hosts.
- **Applicable Checklists**: This column contains a set of icons representing the STIG checklists that are associated with each target. Operating systems are listed first, followed by IA-enabled applications and finally by the *Orphan Checklist* (question mark icon), which is assigned if there are findings from the scanners (especially Nessus®) that are valid, but not part of any STIG Checklist. Hovering over each icon will provide a list of similar STIG checklists associated with that target. Checklists can be added or removed using the Target Page by clicking on the device name.
- **Notes**: The notes page can be edited on the Target Page. Notes can be used as reminders to perform certain actions, questions or statements about the host or anything else helpful to the team, however, these notes are only for the assessment team and will not be exported in any report. In some cases, Sagacity will add notes, most notably if it detects authentication failures from tools like Nessus® that rely on authenticated scans for accurate and complete tests.

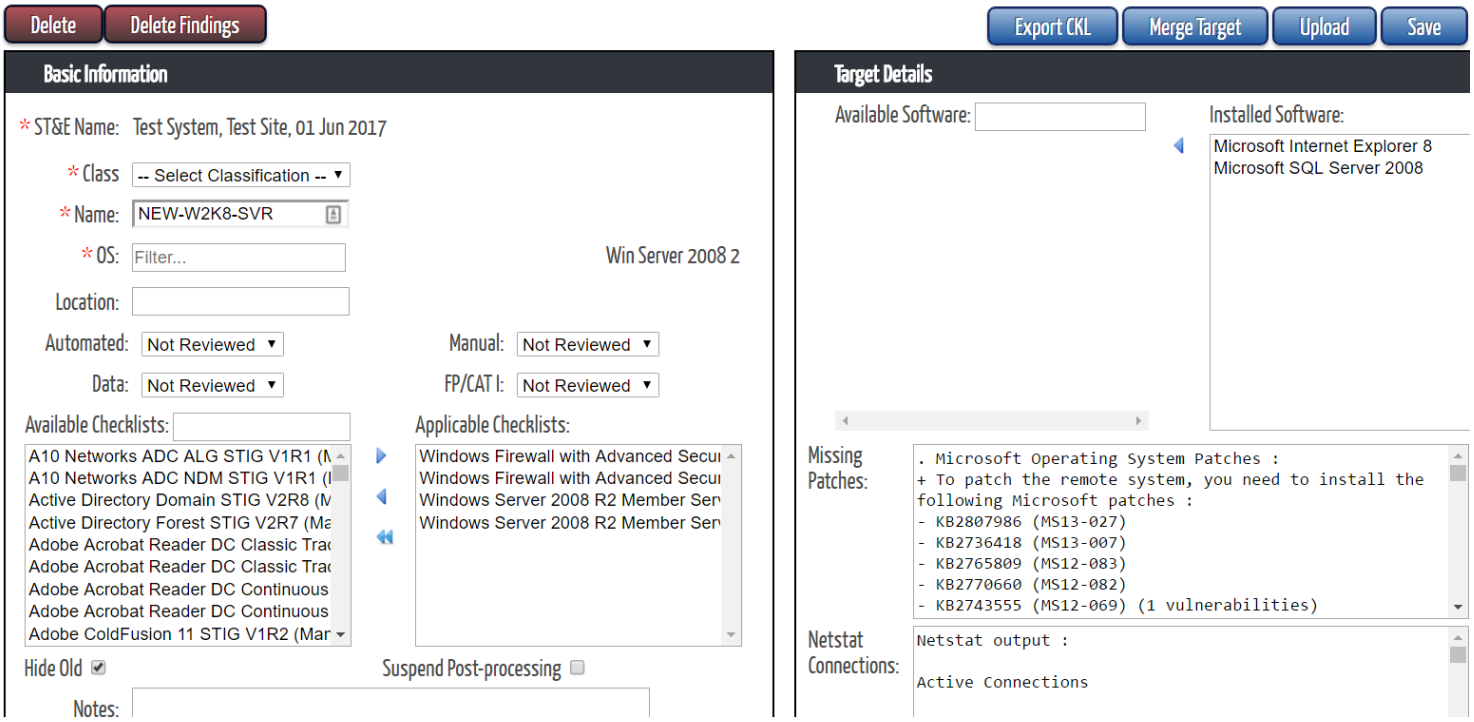
Top

3.1.3 - Hosts Page



The Host Page is accessed by clicking on the underlined target name on the assessment Operations page. The page collects detailed system data from Nessus® and other automated scan tools and user input to allow the user to perform in-depth security analysis of the system.

The **Delete**, **Upload**, **Save** and **Cancel** buttons appear at the top and bottom of the Host Page, and are used to delete the entire host (careful!), upload host data collected directly on the machine, save changes the user has made or simply cancel and return to the assessment Operations page.



Host Information Page (basic information)

The top of the Host Page, shown above, contains both basic and detailed information about the target.

- *Device Name*: This is the formal name of the target. It is automatically set on input as either the hostname, the first non-loopback IP address or the FQDN (in that order). This name can be changed to a common name used by the site/vendor to describe it.
- *OS*: The primary operating system of the system can be selected by searching for the CPE associated with the host. For example entering "*microsoft:windows_10*" will provide a list of Windows 10 variants to choose from. This will affect the Applicable Checklists for the system as long as the Suspend Post-processing checkbox is not checked.
- *Location*: The location, which appears on the main assessment Operations page, is the physical location of the system, and is used by the team to help organize the data.
- *Tasks*: The four dropdowns allow you to set the status of tasks for this target. By default, the four categories are for automated scanning (Nessus®, SCC, etc.), manual STIG checklist reviews, system configuration/data gathering and False Positive/Cat I finding reviews.
- *Notes*: The notes are for the assessment team only, and can contain reminders, system summary information, questions or anything else to help the team to conduct the assessment. Keep in mind the notes that you add on the host page notes field when saved, will be displayed on the assessment Operations tab table for that device row.
- *Missing Patches*: For some systems, Nessus® performs an analysis of missing patches. The list is displayed here and can allow an analyst to perform several IAVM checks without interacting with the target, saving time.
- *Netstat Connections*: If Nessus® was able to perform a netstat command (Windows, Linux or UNIX) the output will be displayed here, showing listening services and/or active TCP/IP connections between targets.

Available/Applicable Checklists:

One of the key concepts in Sagacity is associating the required STIG checklists with each target to provide a complete and accurate assessment of the system. Most servers and workstations will have at least three checklists and possibly quite a few more. The three basic checklists are the Benchmark, which contains the automated STIGs, the Manual checklist, containing almost all checks, and the IAVM STIG with the required patches. Additionally a system may have desktop applications such as Microsoft Office™, provide services such as web or database, or have roles like directory services provider that require associating additional checklists.

When Nessus® scan data is imported, the assessment Manger's post-processor will attempt to identify the target's operating system and installed software, and from there will automatically associate several STIG checklists with the host. This will also happen when a user identifies an OS or installed software. However, because of limitations in the scan data, it is sometimes necessary and highly recommended to manually review and update the checklists.

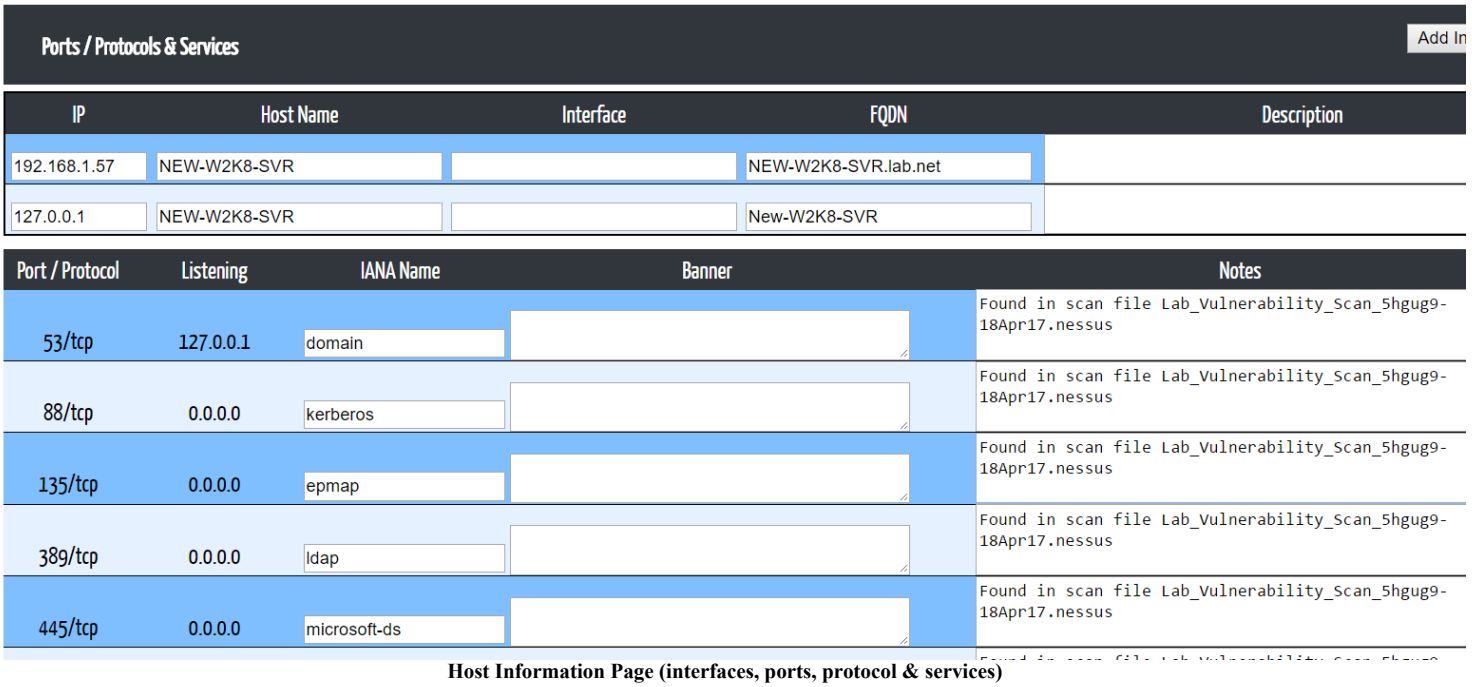
- *Available Checklists*: This is a list of all STIG checklists included in Sagacity's PDI catalog. Users can click on a single checklist or CTRL-click on several, then use the arrows to add them to the Applicable Checklists. Please note that the list will not include checklists listed in the Applicable box. Hovering over a STIG will give the full title, including the version number and whether it is a benchmark, a manual, or an IAVM.
- *Applicable Checklists*: These are the checklists that are currently associated with the target. The user can click a single checklist or CTRL-click several, then remove them using the arrows. The user should carefully review this list to make sure all required and applicable STIG checklists are associated with this target.
- *Move Arrows*: The arrows are used to move single or multiple checklists between the Available and Applicable lists.
- *Search/Filter*: The text box next to the Applicable Checklists label can be used to filter the long list of checklists. For example, typing "2008" will find all STIGS that have "2008" in the title.
- *Hide Old Checkbox*: Selecting this checkbox will hide old versions of the STIGs. Since assessment's are normally performed by evaluating a system against the latest STIGs, this box is checked by default.

- *Suspend Post Processing Checkbox*: Checking this box will disable the post-processing that updates the Applicable Checklists based on the identified operating system and installed software. This would normally be used if the user wants to use an older version of a checklist or if the post-processing is selecting unnecessary checklists.

Available/Installed Software:

The software interface works much like the checklist interface. The Available Software list is a list of all software in the database. During scan data processing, the Manager will add new software to the catalog that it finds in the scan data. During post-processing, the Manager will look through the software list and add the necessary STIG checklists to the Applicable Checklists.

- *Available Software*: This is a list of all known software in the database.
- *Installed Software*: This is a list of all software installed on the system. It can include applications, patches and other packages. .
- *Search/Filter*: Typing in this field will filter the Available Software list for matching titles. For example, typing "IE " (IE space) will find the available Internet Explorer versions.
- *Move Arrows*: The arrows are used to move single or multiple software between the Available and Installed lists. The double arrow will clear the Installed Software list.



Host Information Page (interfaces, ports, protocol & services)

The bottom section of the host page, shown above, contains the detected system interfaces and the ports, protocols and services (PPS) information for the target. This includes all IP addresses, hostnames (if known) interface names and fully qualified domain names (FQDNs). The user can enter notes in the Description field for each interface, if needed.

The PPS listing lists the port and protocol, the IANA name (if it can be resolved), banner information, and any other information the scanner was able to determine for that service. The text fields are editable, and the Notes field is especially useful for taking notes when performing manual probes or other tests on the individual services. Like the other notes on this page, they are for assessment team use only and will not appear in any reports.

Top

3.1.3.1 - Upload Host Data Files

Even with all the best scanning utilities (Nessus®, Retina, SCC, etc), important configuration data about the host can be missed. In the *C:\xampp\www\exec\Target Host Tools* folder are a set of files that can be used to evaluate each computer individually and collect important configuration, registry and file information. The following is a description of the scripts and their purposes:

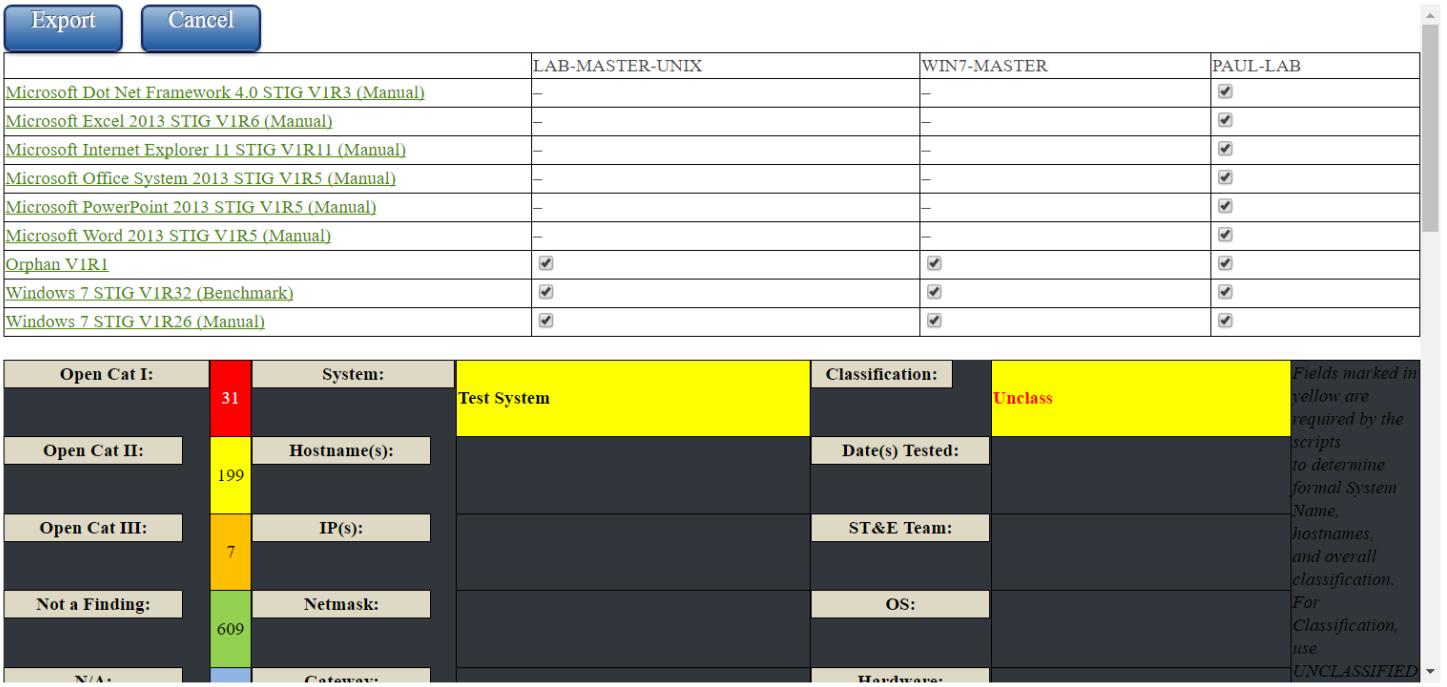
- Windows:
  - Windows Data Collection: This script collects Windows OS configuration, registry, registry permissions, file permission information and the outputs of several common Windows commands from the target host that is invaluable for understanding the security of the system. To use, copy the folder to the C:\TEMP folder on the target system and run the windows-data-collection.bat script as Administrator. The results will be in a folder named with the system hostname.
  - Windows Manual Tools: These are a set of sometimes difficult to find tools provided by DISA to aid in performing some STIG checks on various systems.
- Unix
  - linux-data-collection.sh: Similar to the Windows tool, this collects configuration files, file permissions and the outputs of several common system commands from Linux systems useful in evaluating STIG compliance and system security. Copy the script to /tmp and run with root privileges. The results will be in a .tgz file designated with the hostname.
  - solaris-data-collection.sh: This is the same script, customized with Solaris commands and filenames. It runs the same way.

Once the files are downloaded from the target host, use the Upload button to copy them to Sagacity and click the "Parse Host Data Collection" button. Sagacity will store them in the www/tmp/data_collection folder under that hostname. Sagacity also has the capability through the "tweak scripts" to run custom scripts evaluating the collected data to make determinations about the status of various Not Reviewed findings for the host. As of the 1.3 release, this capability is no longer being maintained, but is still available and rich with possibilities.

Top

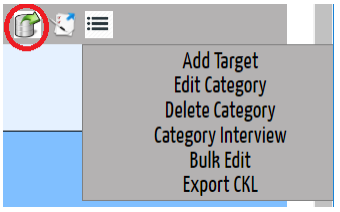
3.1.4 - eChecklist Export

Clicking on the category name on the assessment Operations page will bring up the eChecklist Export page. (NOTE: Clicking on the Unassigned category will not work. Hosts must be put in a valid category before the eChecklists can be exported.)



The table at the top of the page is a summary of hosts and checklists included in the export. Review it to make sure that the required data is included. The Export button will allow you to save the checklist as a multi-tabbed Microsoft Excel (.xlsx) eChecklist file. When the browser prompts you to either save or open the file, save it to disk, then open it from Windows Explorer. Some browsers have difficulty opening the file directly from Sagacity.

The user may also click on the eChecklist export button (shown below) to quickly perform a simple export all checklists for all targets assigned to this category. This will not, however, provide you way to review the findings.



Orphan Checklist

If there are valid findings from the scanners (especially Nessus®) that are not part of any STIG Checklist, they will be included in the Orphan Checklist. These findings can fall into a few categories:

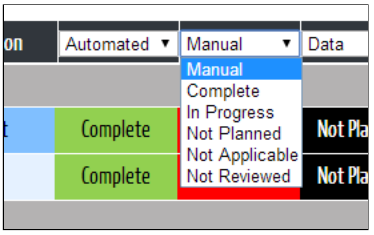
- *Vulnerabilities Not in the STIGs* – When using the latest Nessus® plugins, the scanner tests for the latest missing patches, new vulnerabilities and best-practice system configurations. The STIGs, released quarterly, may not have released guidance on these findings yet. Even though they are not in the STIGs, they are still valid security concerns and should be reported and remediated.
- *Unlinked IAVMs* – The database does its best to create links between Nessus® plugin IDs and IAVMs through CVE, BID, and advisory references, but there are plugins that are not linked. As mentioned above, Nessus® could be reporting a new patch that there is no IAVM for yet. A future release of the Manager will provide an interface for manually linking the IAVMs and Nessus® Plugins. For now, the missing patch will be reported in the Orphan Checklist.
- *Many to One Relationships* – Because of the way Nessus® tests for vulnerabilities, there are times when Nessus® will report several findings which really line up with a single STIG Potential Discrepancy Item (PDI). For example, the one PDI may require certain file permissions for log files, but Nessus® will produce a unique finding for each log file that does not meet the requirements. Trying to combine the individual findings into one PDI would result in a loss of information.

Top

3.1.5 - Tracking Assessment Tasks

Changing the status on assessment tasks can be done on the assessment Operations page (for many systems at once), through the **Bulk Editor** (section 3.1.7), or on the host data page for each individual target.

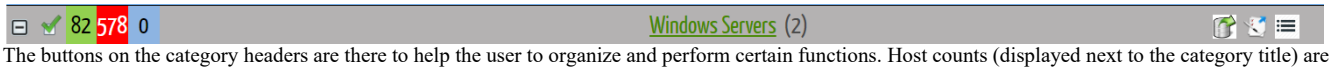
To change the status on the assessment Operations page, select the desired target checkboxes on the left hand side of the screen, then use the dropdown in the appropriate task column to make the change, as shown on the right.



This functionality is scheduled for a major revision in an upcoming version of Sagacity. A critical element in performing a successful security assessment is ensuring that all tests are completed and all data collected and reviewed for accuracy and completeness before leaving the test site.

Top

3.1.6 - Category Controls

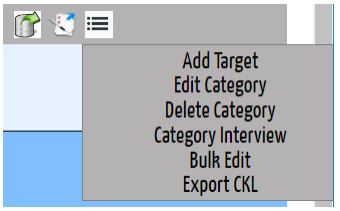


The buttons on the category headers are there to help the user to organize and perform certain functions. Host counts (displayed next to the category title) are always visible. Starting on the left, they are:

- *Collapse/Expand*: This button will simply collapse the targets so that only the category header is visible. After clicking on it the first time it changes to a "+" button. When clicking on the "+" button the targets will be revealed.
- *Select All/None*: This button will toggle the selection of buttons for that category. This is the only button that is available in the Unassigned category to more easily assign new targets to their appropriate category.

- *Findings Statistics*: These numbers indicate the number or percentage of Not a Finding, Open, Not Applicable and Not Reviewed findings for all hosts in that category. Please note that the numbers are only raw, and intended to gauge the completeness of the testing, not to determine the overall risk for that category.
- *Category Title*: The name of the category is also a hyperlink to preview the eChecklist header and export eChecklists for this category. It is followed by the number of hosts in parenthesis, and, if used, the name of the analyst assigned to that category.

To the right of the Category title are:

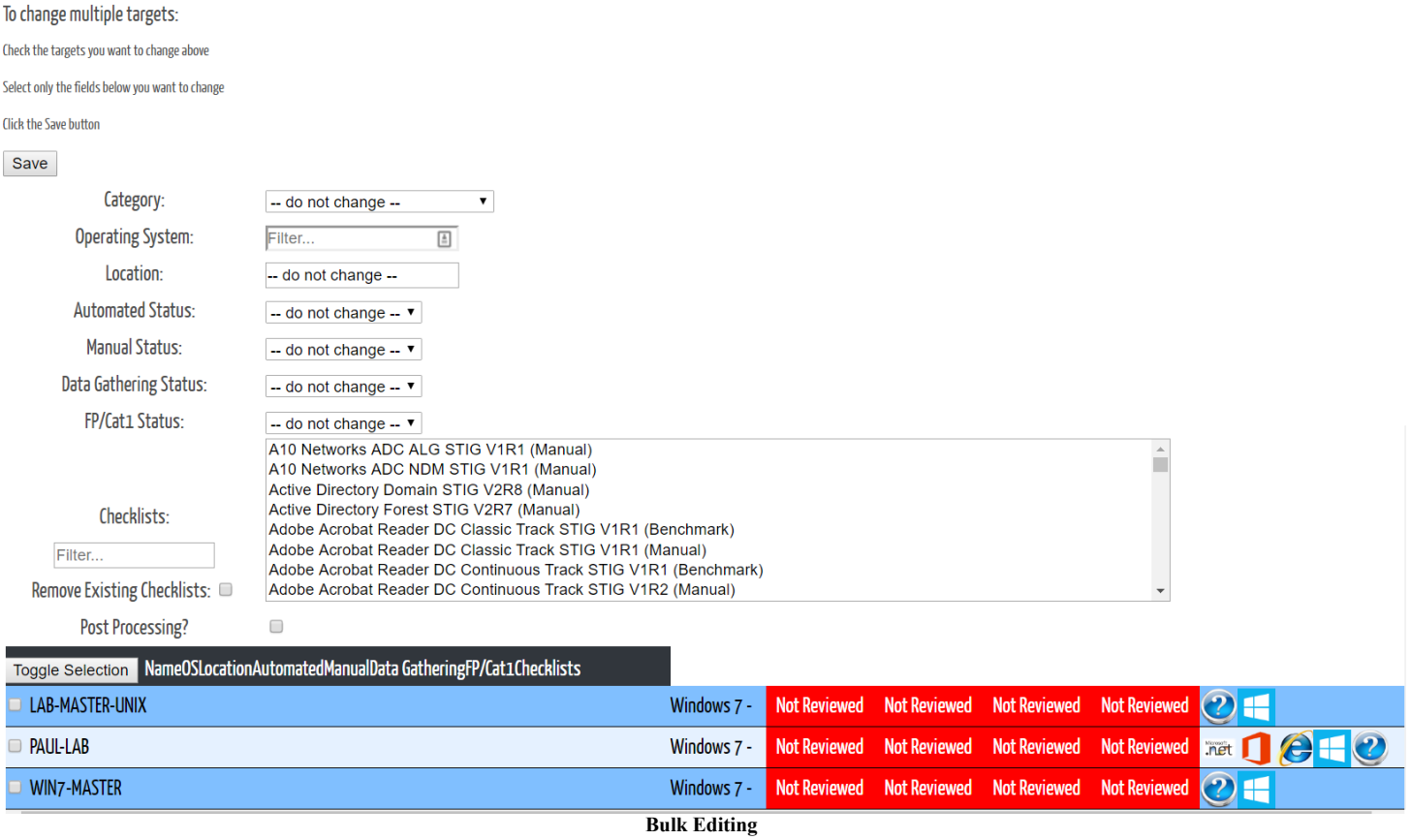


- *Export eChecklist*: This button will allow the user to export an eChecklist without having to review the results. It will export all checklists for all targets assigned to the category that was clicked on.
- *Assign Category to Analyst*: This button will display the prompt on the right and allow the user to input the name the person that is in charge of taking care of this category. This can be very useful for the assessment Lead when multiple analysts are helping perform manual checks or evaluating different segments of the system.
- *Category Menu*:
  - *Add Target*: Used to manually add a new target to this category. The interface will allow the selection of the classification, name and OS of the target as well as assigning any STIG checklists and other pertinent data.
  - *Edit Category*: This will allow the user to rename the category and assign an analyst. It will also will also allow editing the expected scans for that category.
  - *Delete Category*: This menu item will delete the category. Any hosts in the category will be moved to the Unassigned category. No host or finding data will be lost.
  - *Category Interview*: This is a deprecated feature associated with the Host Data Collection and tweak scripts, used in older Windows and Unix STIGs to mark large numbers of irrelavent checks as Not Applicable based on interviewing a sys admin about software installed on the system.
  - *Bulk Edit*: This button will open a new window and allow the user to change many options for multiple targets that are assigned to the category. Further details of this feature will be covered in section 3.1.7
  - *Export CKL*: This will export STIG Viewer .ckl formatted files for all hosts and all checklists in the category. Please note that due to a limitation in the .ckl file format this will produce a file for every host-checklist pair, which can be a large number of files in some cases.

Top

3.1.7 - Bulk Editing

Bulk editing allows users to select multiple targets and change multiple items for each of those targets in one pass. This is a helpful feature, and can speed up manually changing hosts, but always double check to make sure you are changing the hosts you want.



Bulk Editing

The user selects the items to change, then checks each target in this category they want changed, then presses the save button. The options are the same as the Host Details page with the exception of "Remove Existing Checklists". This checkbox will tell the system to delete any checklists that are already assigned, assign the checklists selected in the multi-select box, then perform post-processing (if that box is checked). This allows the user to simply add multiple checklists to multiple hosts without drastically affecting other hosts.

Top

3.2 - Procedural Operations

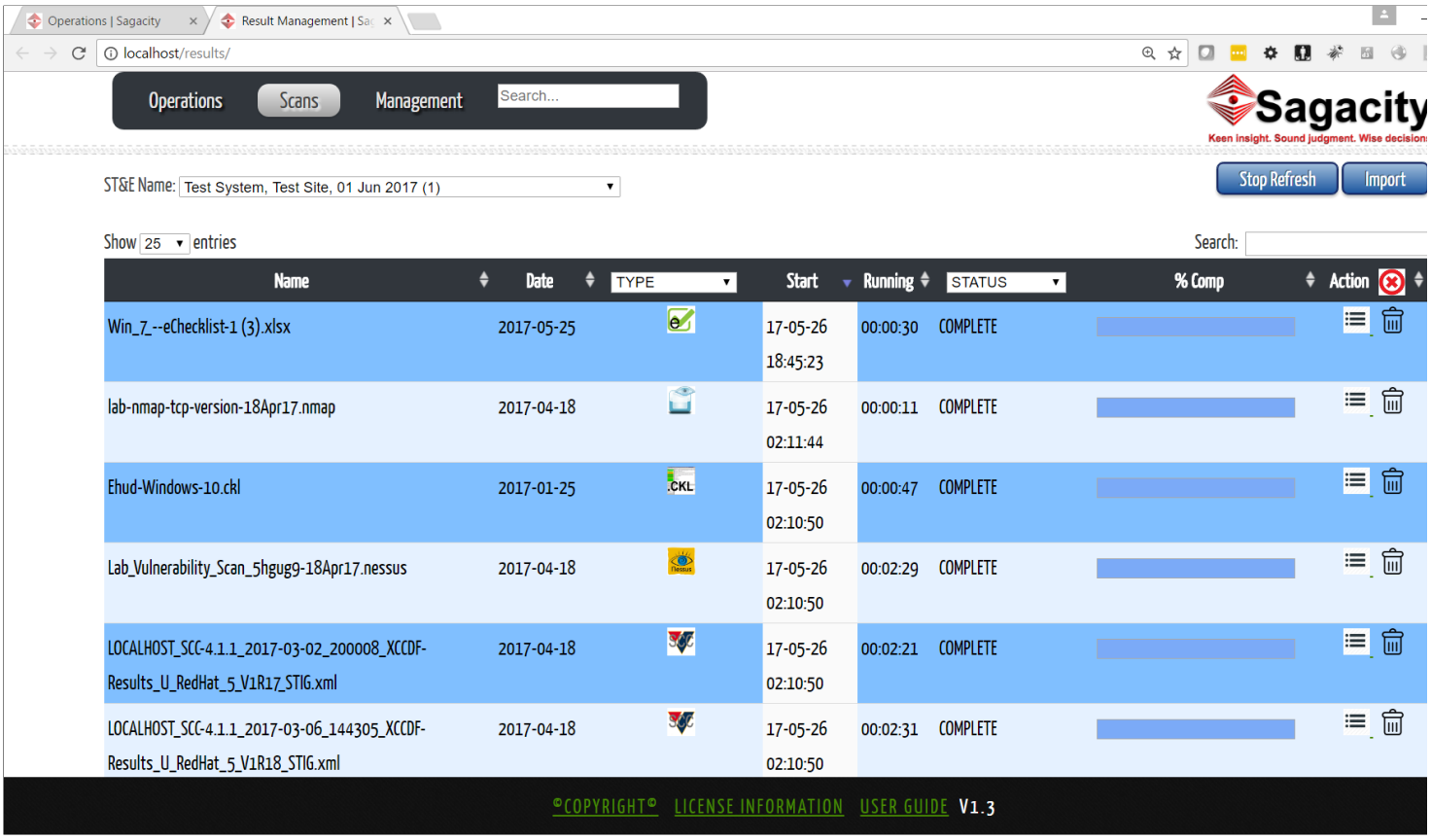
The original procedural operations page was designed for DIACAP assessments and is currently being redesigned to support RMF, and will be provided in a future release. For the curious, it can still be accessed in the _proc folder, but it is unsupported.

Please watch our page at http://www.cyberperspectives.com or our Facebook Page for upcoming announcements.

Top

3.3 - Results Management

The Results page (under Scans) is used to ingest, manage and delete results from a variety of sources. It lists the files that have been uploaded, the original file date, a source type, how long the import took and actions that the user can take.



Scan Management Tab

The dropdown on the top left corner is used, as on the ST&E Operations tab, to select the active assessment. Creating an assessment is covered in section 3.4.1.

This page provides information about the scan files that Sagacity has imported into the database in a table that can be filtered and sorted. The Show Entries dropdown at the top left controls how many results are shown per page, and the lower right of the table (not shown) has page controls to see other pages.

- *Name*: A list of results files that have been imported.
- *Date*: The date the scan was run,
- *Type:* These icons show the type of scan file that was loaded. This column is filterable to only display certain file types.
- *Start*: The date and time the file was uploaded.
- *Running*: Shows how long it took the file to load, to help measure performance.
- *Status*: Whether the file is In Queue for ingestion, Running, Complete, or resulted in an Error or was Terminated.
- *%Comp*: The completion task bar, while In Queue or Running will display the percentage complete for each file.
- *Action*: The first icon will list the host information. The trash can will delete the scan, with an option to also delete all associated hosts. (**Be careful! – See below!**) When the file is Running, a red X like that in the title bar will appear, allowing the user to cancel the import.

The **Stop Refresh** button is used to toggle automatic refresh of the completion bars. The **Import** button is used to select files for ingestion and will be described in the next section.

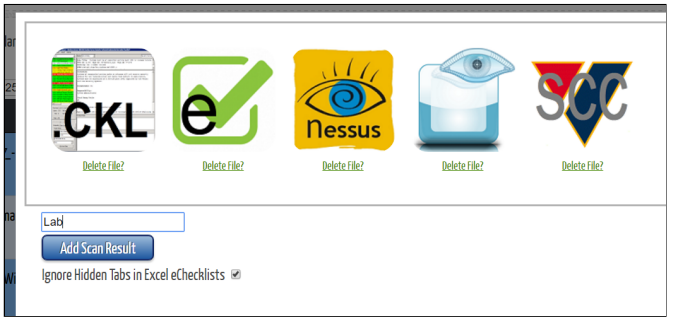
Top

3.3.1 - Importing Results Files

The **Import** button, on the top right (shown above), is used to import result files. Clicking anywhere in the **Upload Box** brings up the File Upload interface (shown here). Clicking the **Drop Files Here to Upload** text in the middle of the box will open a Windows Explorer window that can be used to select files to load. Otherwise, the user can drag and drop one or more input files into the box. General rules of thumb for importing files are:

- The recommended order of operations for using Sagacity is to upload files in the following order.
  - *Discovery Scans*: Nmap and Nessus® Discovery/Vulnerability Scans. These scans (especially Nessus®) have reliable data about operating system, installed software and running services used to identify and categorize the targets, accurately assign STIG checklists and associate IP addresses, hostnames and Fully Qualified Domain Names (FQDNs).
  - *Automated Compliance Scans*: Nessus® Compliance Scans. SCC Data, MBSA Results. These scans provide the most complete and valuable IAVM and STIG compliance data which reduce the amount of work required to perrform manual compliance testing.
  - *Manual Results*: eChecklist, STIG Viewer .CKL. Once the manual testing is complete, the remainder of the compliance results can be imported to ensure a complete test, support Risk Analysis and reporting and allow for a complete export of final eChecklists or STIG Viewer files for the final report package.
- For large files (over 100 MB), input one at a time to improve performance.

- Sagacity will parse multiple files simultaneously, based on the Max # of Result Scans on the settings page (default is 5)



Once the upload is complete click **Add Scan Result**. Sagacity will return to the Results page where the user can watch the progress bars to know when ingestion is complete. A background process is started that examines all the files in the /www/tmp directory, and starts a parser for each file that it finds. Once they are parsed they are moved to the subdirectories in /www/tmp for their respective file types. This helps to organize scan data for the assessment.

Top

3.3.2 - Result File Details

Clicking the **List Hosts** ( ) button will pop up a list of targets/hosts included in that result file, including the hostname, number of findings and IP address for each host.

Host List

Total Number of Hosts: 10 Total Number of Findings/Hosts: 2427

Show 25 entries Search:

Host Number	Host Name	Findings	IP Address
1	W2K3-NEW-SERVER	440	192.168.1.58
2	192.168.1.1	36	192.168.1.1
3	rhel5-2	453	192.168.1.50
4	Solaris10box1	246	192.168.1.51
5	linux-suse11	143	192.168.1.55
6	NEW-W2K8-SVR	295	192.168.1.57
7	WINXP-SP3	465	192.168.1.53
8	cen64svr00	139	192.168.1.52
9	192.168.1.254	9	192.168.1.254
10	MASTER-Laptop-WIN7	201	192.168.1.20

Showing 1 to 10 of 10 entries Previous 1 Next

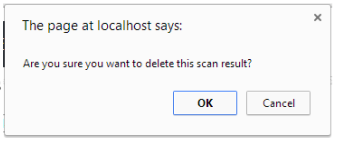
Results Host List

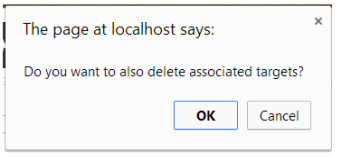
This information can provide a quick sanity check on the data and the upload process. The analyst can make sure that the expected hosts were found. On systems that have not been well secured, the number of findings can be an indication of whether the scan ran successfully, including whether or not the administrative portion of the Nessus® scan was successful. Only the first non-loopback IPv4 address will be displayed in the IP Address column. The columns can be sorted and filtered, and the number of entries can be controlled as well.

Top

3.3.3 - Deleting Results

The trash can Delete button to the right of each row can be used to delete the targets and findings associated with that file. However, there are a few important considerations for this function.





- Upon clicking the "Delete" button the user will be prompted to answer if they want to also delete targets that were found in this scan. After answer that question, they will then be prompted with a confirmation box making sure they want to delete the scan file and findings.
- Deleting the results file deletes findings.
- PDIs that are duplicated in other scans or imported eChecklists will not be deleted if they were imported after the deleted scan. For example, if a Nessus® scan is loaded, followed by an SCC scan for the same host and the analyst deletes the Nessus® scan, the common findings between the scans will remain. However, if the SCC scan were deleted, all of the common findings would be deleted.
- If there were conflicts between findings from scans, the most significant result will be used.

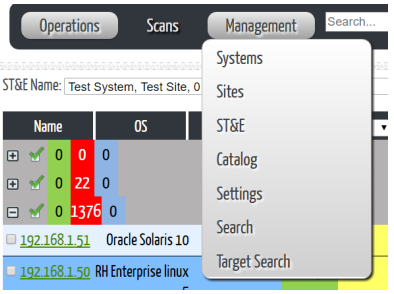
Top

3.4 - Management Tab

The **Management** Tab is used to manage the data in the database, configure the system and perform searches. Further explanation of the functionality is included in subsequent sections, but is summarized here:

- **Systems**: The mission system being assessed.
- **Sites**: The locations where the system operates.
- **ST&E**: The assessment of the System and Site(s).
- **Catalog**: A searchable listing of all STIGs in the database.
- **Settings**: Sagacity configuration settings.
- **Search**: A comprehensive database search capability.
- **Target Search**: A host details search capability.

Before the system can have assessment data loaded, the user must create a mission system, a site, and an assessment. Each mission system can have multiple sites, and each system / site group can have multiple assessments. A mission system is defined by the accreditation boundary. A site is a physical location where the mission system is operated, and an assessment is an individual test event conducted at a site.



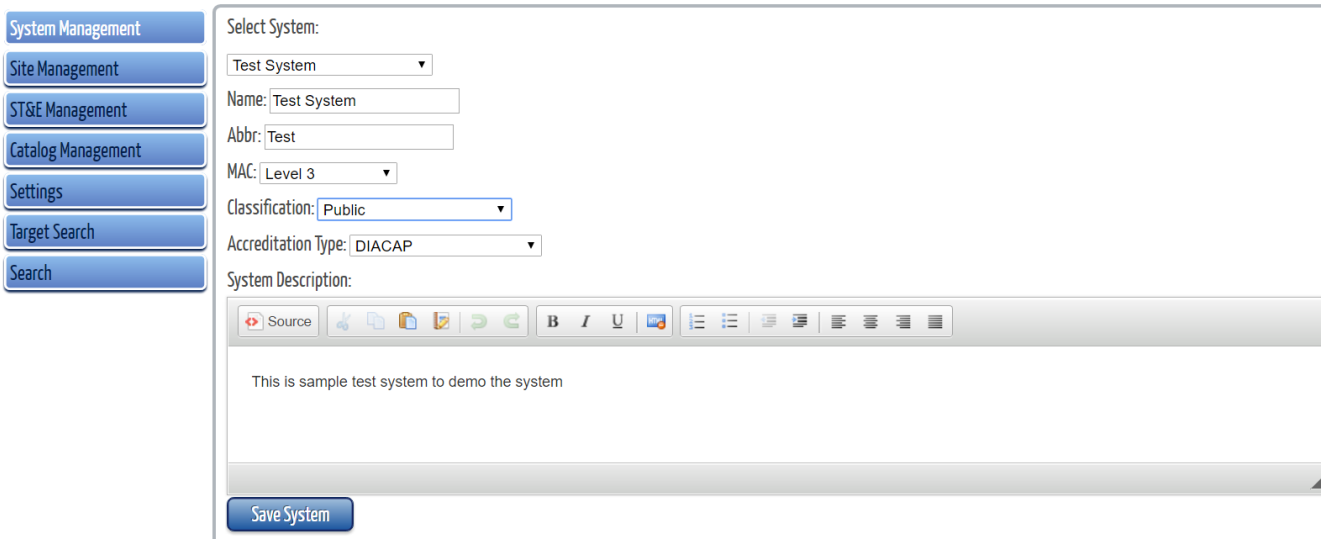
Top

3.4.1 - Mission System Creation / Modification

As shown below, under the Mission **System Management** side tab, select New. Fill in the name and Classification levels, and then click Save System. MAC Level is for DIACAP and can be safely ignored.

A popup will ask you if you want to move on to site management. Click OK to create a site.

To modify a system, select it using the dropdown, make any changes and then click "Update System." At this time, there is no way to delete a mission system using Sagacity.



Mission System Management

Top

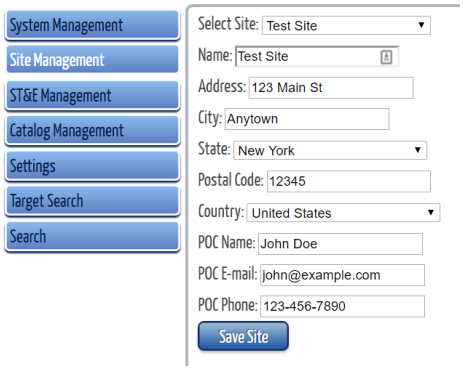
3.4.2 - Site Creation / Modification

To create a site, click on the **Site** Management side tab, then select "New" from the dropdown. Enter the site information, including site name and address and POC information.

The only required field is Name. The others are optional.

A popup will ask you if you want to move on to assessment management. Click OK to create an assessment.

To modify a site, select it using the dropdown, make any changes and then click “Update Site.” At this time, there is no way to delete a site using Sagacity.

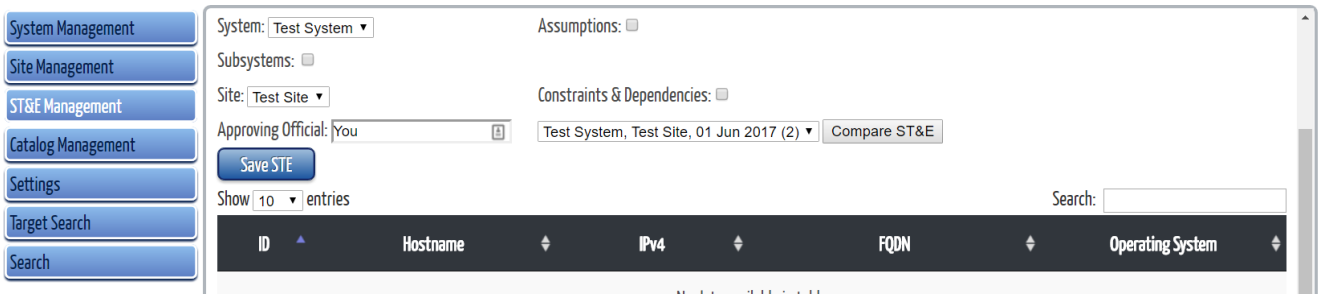


Site Managemenet

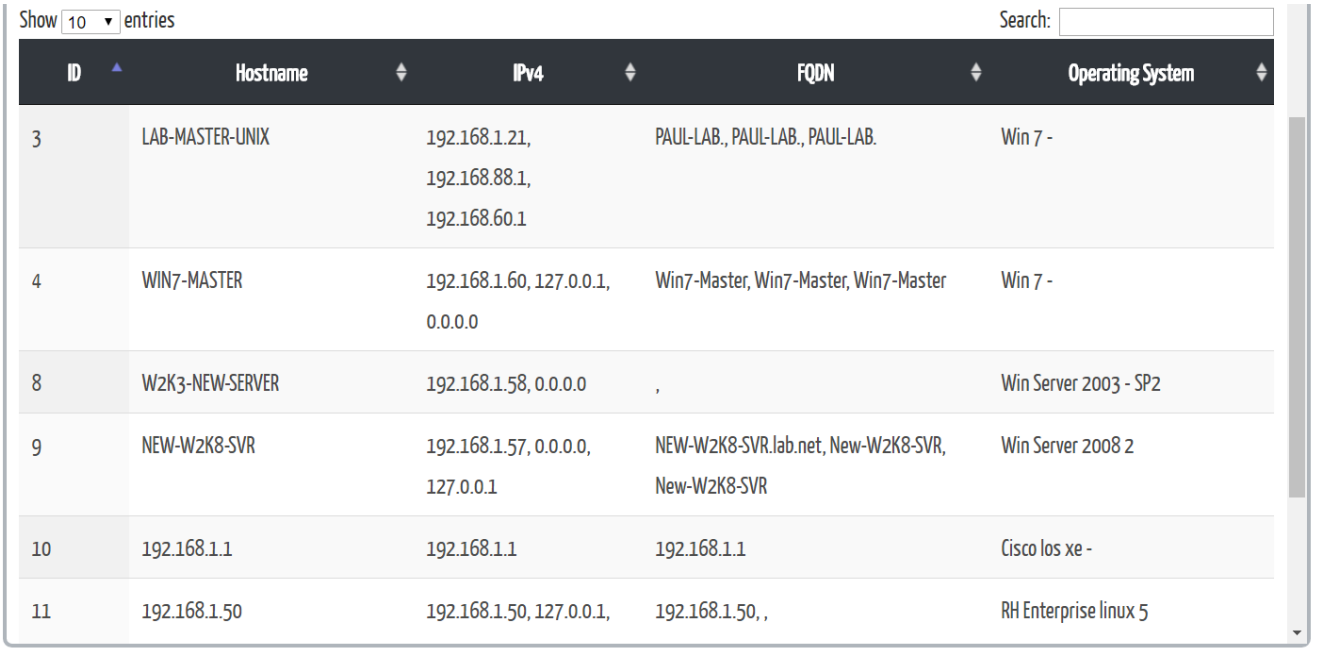
Top

3.4.3 - ST&E Creation / Modification

To create an assessment, click on the **ST&E Management** link, then select New from the dropdown. Fill in the Start and End dates. All fields (except "Subsystems") are required. The selection of a sub-system allows the creation of multiple assessments at once where one system is the primary and the others are created as subs under the primary. This is for reporting so that subsystems will be included in reporting the primary system. This will create another ST&E for each subsystem, so each subsystem can be independently managed.



To modify an assessment, select it using the dropdown, make any changes and then click "Update assessment."
The screenshot below depicts a list of all targets that have been imported for this assessment. Just like the host list on the **Results** page, this list can be sorted by clicking on the column headers.



Show 10 entries Search:

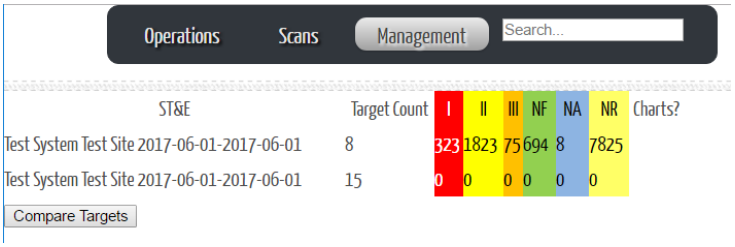
ID	Hostname	IPv4	FQDN	Operating System
3	LAB-MASTER-UNIX	192.168.1.21, 192.168.88.1, 192.168.60.1	PAUL-LAB., PAUL-LAB., PAUL-LAB.	Win 7 -
4	WIN7-MASTER	192.168.1.60, 127.0.0.1, 0.0.0.0	Win7-Master, Win7-Master, Win7-Master	Win 7 -
8	W2K3-NEW-SERVER	192.168.1.58, 0.0.0.0	,	Win Server 2003 - SP2
9	NEW-W2K8-SVR	192.168.1.57, 0.0.0.0, 127.0.0.1	NEW-W2K8-SVR.lab.net, New-W2K8-SVR, New-W2K8-SVR	Win Server 2008 2
10	192.168.1.1	192.168.1.1	192.168.1.1	Cisco Ios xe -
11	192.168.1.50	192.168.1.50, 127.0.0.1,	192.168.1.50, ,	RH Enterprise linux 5

Top

3.4.3.1 - Compare ST&Es

Sagacity has the rudimentary capability of comparing two ST&Es, allowing the user to identify differences at the category and host level. Using the dropdown on the lower right, select the ST&E to be compared to the current ST&E, then click on the **Compare ST&E** button. The next screen will show the two assessments in a table like the image on the right. This summary table provides counts of:

- Cat I, II and III findings,
- Not a Finding (compliant) checks
- Not Applicable checks
- Not Reviewed checks



The **Compare Targets** button at the bottom of the table will bring up the next screen, shown below.

This table contains a list of all targets in both assessments and summary counts of their findings. The grayed out sections of the table indicate that that host does not exist in that ST&E. This allows the analyst to determine which hosts are unique to each assessment and identify deltas in the numbers of findings.. Clicking on the **Hostname Button** will bring up another table similar to the eChecklist which will show all STIG checks and notes for that host from both assessments side by side.

The Assessment Comparison functionality is in its earliest stages. It was originally built as a proof of concept to fill a one-time requirement, but has a lot of promise. We look forward to including additional functionality like filtering, sorting and search, as well as more in-depth analysis tools to help you identify trends and deltas.

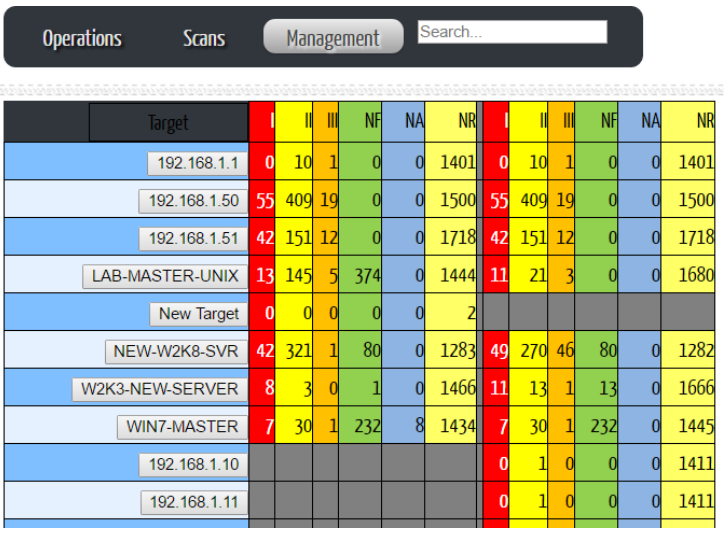
Top

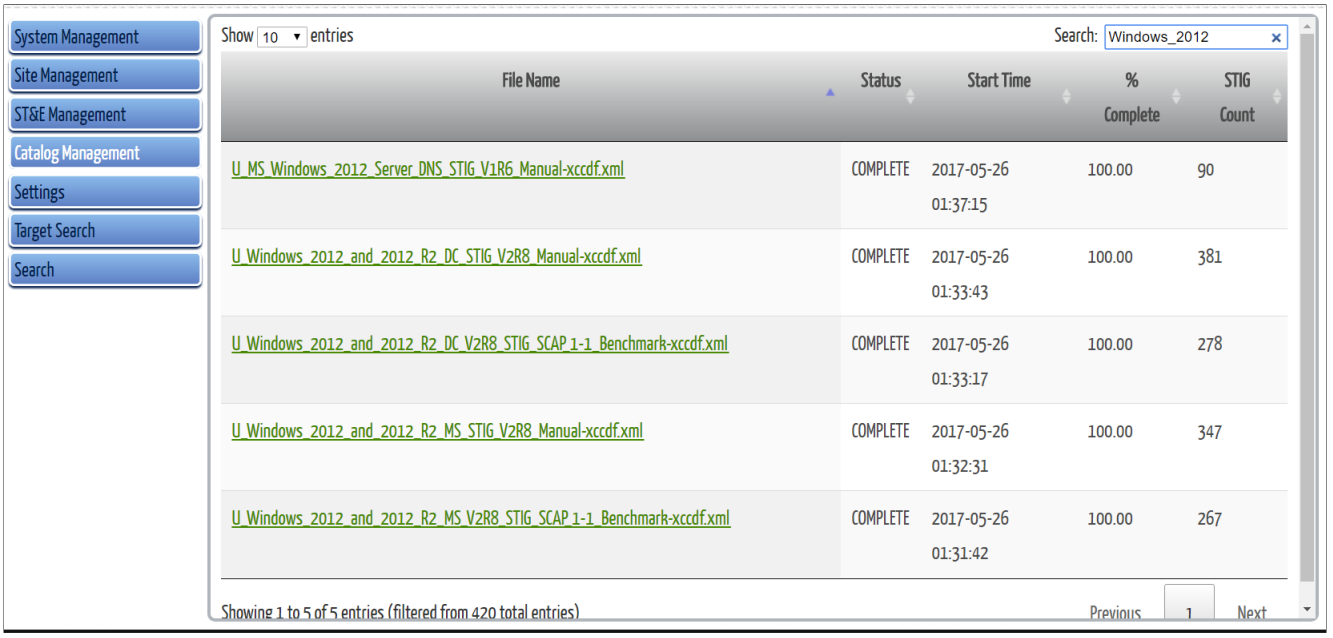
3.4.4 - Catalog Management

Catalog Management is used to view and search the STIGs in Sagacity's database. New or Legacy STIGs can be added to the database for use during an assessment. DISA releases updated STIG checklists at least quarterly, usually at the end of January, April, July and October. New STIGs can be uploaded as either individual XCCDF

formatted XML files or as the entire STIG Library .zip files (Unclassified and FOUO) available from http://iase.disa.mil/stigs/compilations/Pages/index.aspx. Individual STIGS can be found using the A-Z List, found at http://iase.disa.mil/stigs/Pages/a-z.aspx

The Search function, shown below looking for Windows 2012 STIGs, searches on the STIG filename. Clicking on the hyperlink will open a popup that can be used to associate STIGs with Common Platform Enumeration (CPE) identifiers to improve Sagacity's automated STIG detection capabilities. If you find that the STIG you need is not being automatically detected, you can set that here.





PDI Catalog Management Interface

Sagacity also keeps a repository of the original XCCDF formatted STIGs and CSV eChecklist files in *C:\xampp\www\reference\stigs*

Top

3.4.5 - Settings

The Settings page allows a user to configure Sagacity for their environment.
The first section is for company information. This is used to populate the eChecklist cover page and will be used for reportring in future releases.

The second section contains web settings. Most of these are set at installation and should not be changed. The exception is the **Log Level**, which can be made more verbose for troubleshooting and development.

The **Flatten eChecklist** check box will suppress the output of the comparison columns in the eChecklist.
Wrap E-Checklist Check Contents will set the Short Title and Check Contents columns in the eChecklists to word wrap. This is a user preference, with some analysts preferring to see a more compressed view and others wanting all of the text to be easily visible.
Audible Notifications will cause an audible alert to sound every time a scan file ingestion completes. This can be useful for large, long running files, but rather repetitive for large numbers of files. The sound can be customized by replacing the */results/complete2.mp3* file with the file of your choice.

Port Ingestion Limit controls the number of TCP and UDP ports recorded in the database for each host. This overcomes issues with nmap and Nessus® where port scanning can sometimes identify all scanned ports as open, filling up the database with incorrect port information.
Max # of Result Scans controls the number of threads used to ingest result scans. The default is 5. The Maximum is 20, but please note unless you have a beefy system, this could result in system performance issues.
Output Format is the format of the eChecklist. This can be set to Microsoft Excel.(xlsx or .xls) or Open/LibreOffice (.ods).

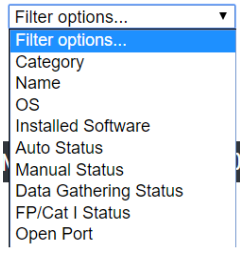
The next five path settings are set at installation and should normally not be changed. Likewise, the DB server and path settings should nornally not be changed.

Finally, the page concludes with **Save Settings** written in large, friendly letters. This is largely self-explanatory.

Top

3.4.6 - Target Search

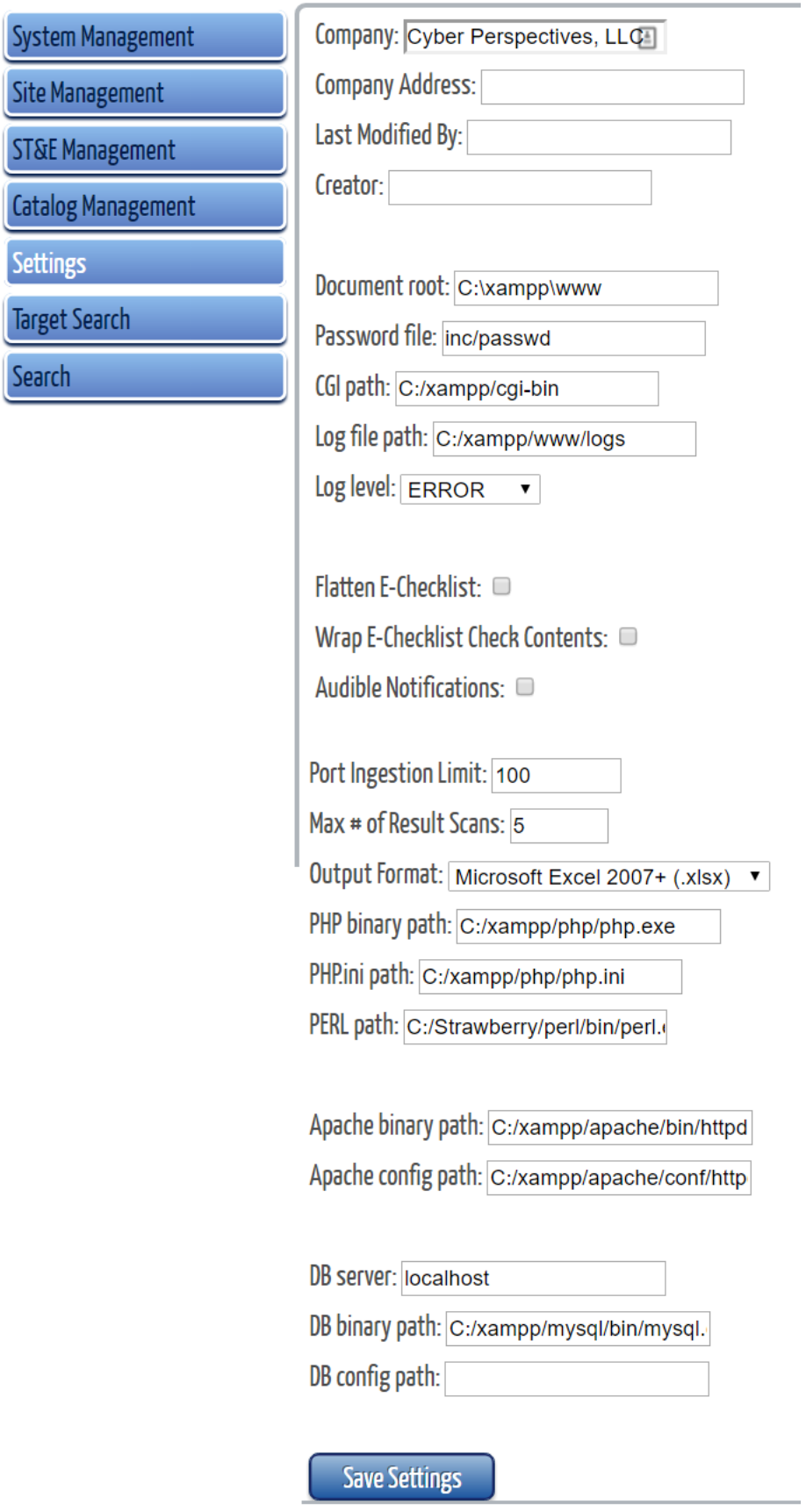
Sagacity now provides a fairly robust target search capability. Analysts can search for targets based on a number of attributes:

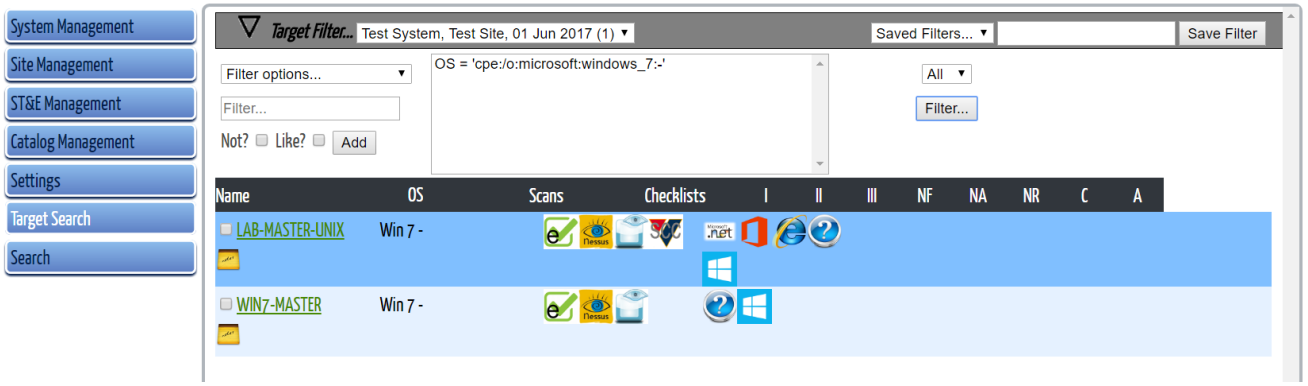


- Category: These are the primary host categories as seen on the Ops Page.
- Name: The system hostname or FQDN.
- OS: The Operating System Common Platform Enumeration (CPE) identifier.
- Installed Software: The CPE of installed software.
- Task Status (Auto, Manual, Data Gathering, FP/Cat I Review):
- Open Port: Search for open TCP or UDP ports.

To perform a target search, first select a filter type in the filter options drop down. Next type a filter string in the Filter… box and hit **Add**. This adds the filter to the options list. (You can double-click it to remove.) Finally, hit the **Filter** button to see the search results.

The example below shows a search for Windows_7 systems in the current assessment.



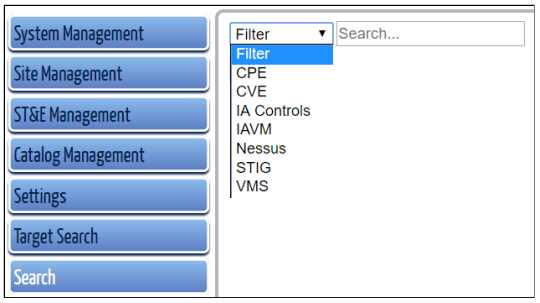


If you want to save a query, then just type the name in the box at the header and hit "Save Filter", then you can just select the saved filter from the drop down and it will put the filters in the box and execute the filter for you displaying the results below. There is currently not a way to delete a saved filter.

The search results are in much the same format as the ST&E Operations page, providing hostname, Operating System, loaded scans and Checklists. Development is proceeding on also providing counts of Cat I, II and III open findings, Not a Finding, Not Applicable, Not Reviewed and percentage Compliant.

Top

3.4.7 - Search



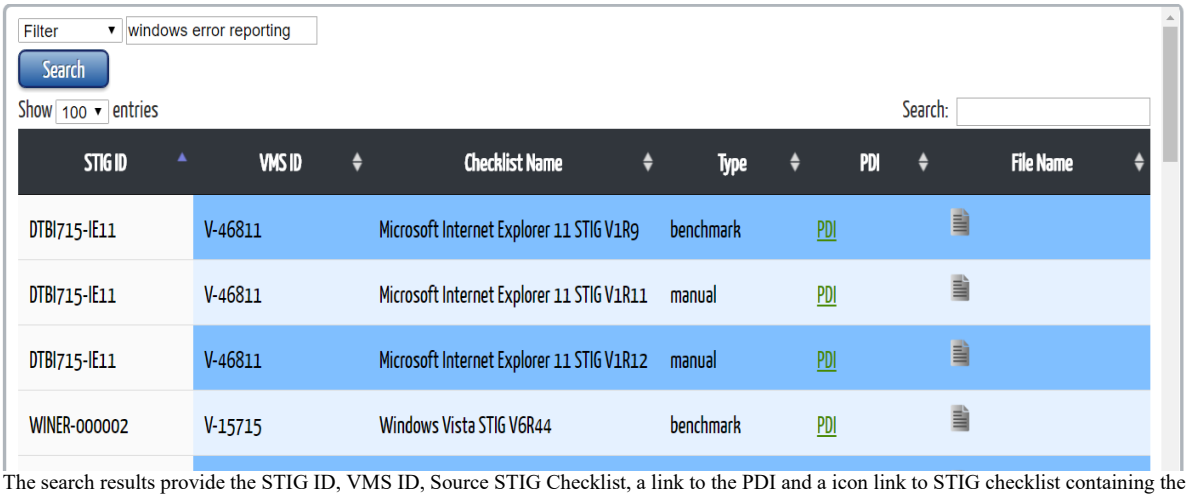
The search function provides a comprehensive database search capability which includes, CVE, CPE, STIGs, IAVMs (if imported), IA Controls, Nessus Plugins (only as they are linked to STIGs), and VMS IDs.

Entering a text string will search the PDI catalog's Title, Description and Check Contents fields, using a database LIKE. The wildcard '%' can be used as well. An example of search results for "windows error reporting" is below.

For a more precise search, the user can use a "prefix=" search to search for specific STIG ID, VMS ID, IA controls, IAVM, CVE, Checklist or Nessus® plugin IDs. Prefixes are case insensitive and can be enters as 'STIG' or 'stig', for example. Some search examples are:

- CPE=%/o%windows_7%
- CVE=%-2016-%
- STIG=2.005
- IA=%CCI-127% (You will want to search with the wildcards because the IA Controls field is a concatenated list of all the controls associated with that STIG)
- VMS=V-12345

Please note, Nessus search will find PDIs that are linked to the searched for Nessus Plugin ID. There are plans to expand this to include details about the plugin itself.



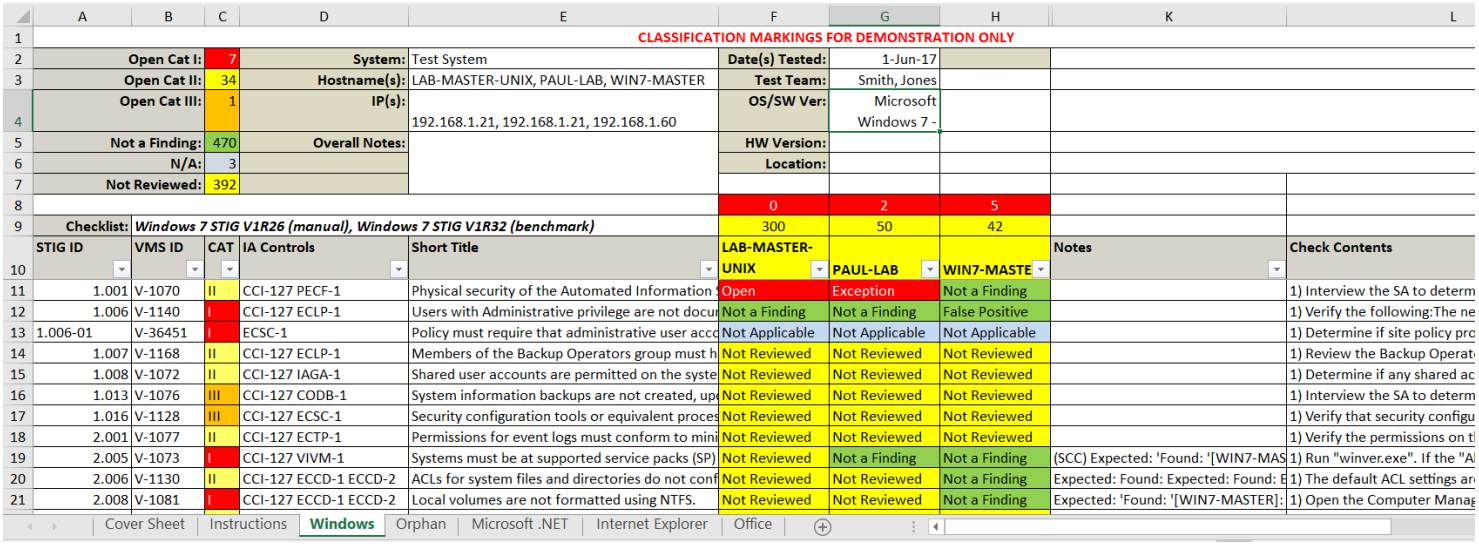
The search results provide the STIG ID, VMS ID, Source STIG Checklist, a link to the PDI and a icon link to STIG checklist containing the PDI.

Top

3.5 - eChecklists

The eChecklist, shown below, provides a easily readable, concise way of communicating technical findings and conducting manual STIG checks. Once completed, it can be provided as a record of the assessment results to be provided as an artifact with the C&A package or to the system vendor or administrators responsible for correcting the issues found.

The header information in the eChecklist provides counts of Cat I, II, and III findings, Not a Finding, Not Applicable and Not Reviewed items as well as information about the hosts being tested. Sagacity pre-populates many of these, like the Hostnames, IP addresses and Operating System. The analyst is responsible for entering the Dates Tested, Test Team, OS/Software Version and Location. The Overall Notes cell is for recording overall findings or impressions about the security posture of the software being evaluated.



	A	B	C	D	E	F	G	H	K	L
1	CLASSIFICATION MARKINGS FOR DEMONSTRATION ONLY									
2		Open Cat I:	7	System:	Test System	Date(s) Tested:	1-Jun-17			
3		Open Cat II:	34	Hostname(s):	LAB-MASTER-UNIX, PAUL-LAB, WIN7-MASTER	Test Team:	Smith, Jones			
4		Open Cat III:	1	IP(s):	192.168.1.21, 192.168.1.21, 192.168.1.60	OS/SW Ver:	Microsoft Windows 7 -			
5		Not a Finding:	470	Overall Notes:		HW Version:				
6		N/A:	3			Location:				
7		Not Reviewed:	392							
8						0	2	5		
9	Checklist:			Windows 7 STIG V1R26 (manual), Windows 7 STIG V1R32 (benchmark)		300	50	42		
10	STIG ID	VMS ID	CAT	IA Controls	Short Title	LAB-MASTER-UNIX	PAUL-LAB	WIN7-MASTE	Notes	Check Contents
11	1.001	V-1070	II	CCI-127 PECF-1	Physical security of the Automated Information	Open	Exception	Not a Finding		1) Interview the SA to determ
12	1.006	V-1140	I	CCI-127 ECLP-1	Users with Administrative privilege are not docu	Not a Finding	Not a Finding	False Positive		1) Verify the following:The ne
13	1.006-01	V-36451	I	ECSC-1	Policy must require that administrative user acc	Not Applicable	Not Applicable	Not Applicable		1) Determine if site policy pro
14	1.007	V-1168	II	CCI-127 ECLP-1	Members of the Backup Operators group must h	Not Reviewed	Not Reviewed	Not Reviewed		1) Review the Backup Operat
15	1.008	V-1072	II	CCI-127 IAGA-1	Shared user accounts are permitted on the syste	Not Reviewed	Not Reviewed	Not Reviewed		1) Determine if any shared ac
16	1.013	V-1076	III	CCI-127 CODB-1	System information backups are not created, up	Not Reviewed	Not Reviewed	Not Reviewed		1) Interview the SA to determ
17	1.016	V-1128	III	CCI-127 ECSC-1	Security configuration tools or equivalent proces	Not Reviewed	Not Reviewed	Not Reviewed		1) Verify that security configu
18	2.001	V-1077	II	CCI-127 ECTP-1	Permissions for event logs must conform to mini	Not Reviewed	Not Reviewed	Not Reviewed		1) Verify the permissions on t
19	2.005	V-1073	I	CCI-127 VIVM-1	Systems must be at supported service packs (SP)	Not Reviewed	Not a Finding	Not a Finding	(SCC) Expected: 'Found: '[WIN7-MAS	1) Run "winver.exe". If the "A
20	2.006	V-1130	II	CCI-127 ECCD-1 ECCD-2	ACLs for system files and directories do not conf	Not Reviewed	Not Reviewed	Not a Finding	Expected: Found: Expected: Found: E	1) The default ACL settings ar
21	2.008	V-1081	I	CCI-127 ECCD-1 ECCD-2	Local volumes are not formatted using NTFS.	Not Reviewed	Not Reviewed	Not a Finding	Expected: 'Found: '[WIN7-MASTER]:	1) Open the Computer Manag

Cover Sheet | Instructions | Windows | Orphan | Microsoft .NET | Internet Explorer | Office

- *Cover Sheet Tab*. Changing the classification marking to SECRET in the top cell will change it for the entire tab. Enter the system name and the title of the test event.
- *Instructions Tab*. This tab contains information about using the eChecklist.
- *STIG Checklist Tabs*. The primary fields are:
  - *STIG_ID*: This is the STIG Identification field from the DISA STIG Checklists.
  - *VMS ID*: This is the Vulnerability Management System ID from the Checklists. It provides an *almost* unique identifier for each finding.
  - *CAT*: This is the STIG Severity Category, Cat I, II and III.
  - *IA_Controls*: This is a list of related IA Controls. The relationships are taken directly from the STIG Checklists, which currently are a mix of RMF CCIs and DIACAP controls.
  - *Short_Title*: This is a brief, general description of the finding. For a more detailed discussion, refer either to the STIG Checklist itself or the PDI Catalog.
  - *Status/System*: This can be one or multiple columns describing the status of this finding. The possible values for this column are given below. The number in red above the system name is the count of Cat I findings. The number in yellow is the count of remaining Not Reviewed items.
  - *Notes*: The notes column should be used to provide specific details about the finding. The source of the notes is in parenthesis, and any data provided by the automated scanning tools or Sagacity (script) are included to assist the engineer in performing finding analysis.
  - *Check_Contents*: This field contains the check procedures from the STIG, if available.
- *Orphan Tab*: The Orphan is a special checklist tab containing all findings for the hosts that are not included in the currently applied STIG checklists. These can include vulnerablity scanner results that do not map to a particular STIG check, outdated checks found by compliance scanners that are no longer in the STIG, or checks from a STIG that should have been applied to the hosts. The STIGs are not a complete measure of a system's security. There are vulnerabilities and security requirements above and beyond the STIGs.

DO NOT MODIFY the column headings or you may have problems re-importing the checklist.

The status options for the findings are:

- **Open:** The finding is valid for this host.
- **Not a Finding:** The finding is not valid for this host.
- **Not Applicable:** The finding does not apply to this host.
- **Not Reviewed:** The finding has not yet been reviewed.
- **Exception:** The finding cannot be changed because of an operational need or other configuration requirements. A request of the DAA/AO will request acceptance of the vulnerability.
- **False Positive:** It was determined that the system is a valid check.
- **No Data:** Because dissimilar checklists were merged, there is no data available for this item. It is not common to see this status in an eChecklist.

Instructions:

eChecklist Header Information
1. Make sure that the classification markings (A1, G2) are filled out correctly.
2. System Name (E2) is the name of the overall system being assessed.
3. Fill out the Hostname (E3) and Networking information (E3-6) for the host.
4. Fill in the Operating System (G5), Hardware (G6) and system location (G7).
5. Include the names of the test team and administrators (G3) and date tested (G2).
6. The Checklist(s) field (B9) is a list of the STIG checklists included in that tab.
7. Any overall notes can be included in the Checklist Notes field (I3).

eChecklist Body
1. Use the Check Contents to evaluate the target system and determine the outcome of the check.
2. Use the dropdowns in the status column (F and following) to select the correct finding status. Copy and paste or the Excel fill handle to quickly copy the status to other hosts.
3. Enter notes to explain how you arrived at the status. Concise notes are normally sufficient, but some findings may require elaboration.
4. There are two hidden columns between the status columns and notes. Overall Status is a rollup of the finding statuses for all hosts, and Consistent is a binary 1 (yes) or 0 (no) describing whether the results were consistent across all hosts. These can be helpful during testing or analysis to identify deltas between systems or possible configuration management issues.
5. Column filters, sorting and search can be helpful for testing similar checks or for post-test analysis.
6. Save often!

NOTE: The filename must include the string "eChecklist" to be parsed by Sagacity.

Top

3.6 - eChecklist Data Analysis and Correlation

Data analysis and correlation includes reducing false positives, prioritizing findings, identifying inconsistencies between systems, and root-cause analysis. In the example above, the findings from three Windows 7 systems are merged into a single checklist.

By including similar systems in columns (like *system1* and *system2*, above), the analyst can quickly identify differences between the systems which can point to inconsistent administration or errors in the assessment analysis. The data can be sorted by Status and Severity Category level to help determine which findings present the biggest risk to the system and how pervasive (what percentage of hosts are affected) the findings are. Further sorting by IA Control/CCI can help to identify root causes for the findings, such as an ineffective IAVM program or lack of configuration control.

Top

4 - The Way Ahead

Sagacity and the eChecklist have come a long way since the initial Perl scripts and CSV flat files originally written in 2009, but the goal of providing a single, streamlined, efficient way of handling assessment data remains. As we look at how far we've come, we realize just how far we still have to go. The DoD's transition from DIACAP to RMF, and the Federal Government's adoption of the DISA STIGs are driving a merging of compliance standards, but not without cost. RMF is almost too detailed, and RMF assessments of well over 1,000 controls are time-consuming and difficult. From a technical standpoint, systems are becoming more complex, requiring compliance with more STIGs than ever. (Our assessment laptops alone have 14 applicable STIGs!)

To help our customers meet these challenges, Sagacity's next steps will include

- Results parsing for even more vulnerability and compliance scanners
- Improved test management and tracking capabilities
- Additional ways to view, organize and analyze test data
- Assessment Export and Import
- Database extensions, including the National Vulnerability Database, vendor advisories, exploit information and more!
- Improved target search capabilities.
- Improved Assessment Comparison capabilities, including trending and delta analysis

Developing these functions is not easy and not cheap. To accomplish this, we need users, developers and eventually customers. The base version of Sagacity, with ever improving technical assessment functionality, will always be free, but we are also planning a paid version early next year with advanced features like full NIST 800-53/53A RMF Control Assessments and compatibility with systems like eMASS. Please follow our Facebook page and website and watch for updates!

At Cyber Perspectives, we are committed to the ideals of Open Source Software. Working together, the cybersecurity community can accomplish far more than they can individually. If you are interested in contributing to Sagacity, please contact us!

http://www.cyberperspectives.com
https://www.facebook.com/cyberperspectives

Top

Appendix A - Sagacity Directory Structure

This is a description of the directory structure found in the *C:\xampp\www* folder. Non-administrators should generally leave the other folders alone or risk impairing web interface functionality.

C:\xampp\www	Installation files and updates, README's, index and file uploads
| *classes*	Class files for the web interface
| *conf*	Default PHP, Apache and MySQL configuration files
| *data*	Management tab web content
| *docs*	Documentation, including DB design, DOXYgen file and user guide
| *exec*	All executable scripts
| *img*	Web application image files for the web site
| *checklist_icons*	Images to display for the checklists
| *help_doc*	Image file for this help documentation
| *scan_types*	Image files that represent the uploaded scan files
| *waiting*	AJAX images for searching
| *inc*	Global include path used throughout application
| *vendor\...*	3rd party vendor libraries compiled using composer
| *logs*	Contains log files that are generated throughout Sagacity
| *reference*	Contains all reference files
| *cve*	Contains raw CVE XML files used in the Search feature
| *iavm*	Contains raw IAVM XML files used in the Search feature
| *stigs*	Contains raw STIG XML files and converted CSV files used in the Search feature
| *results*	Scans tab web content
| *scripts*	JavaScript files and 3rd party libraries used in the web interface
| *ste*	Operations Tab web content
| *style*	CSS files used throughout application
| *tmp*	Where user files are uploaded after drag and drop operations, additional subdirectories are created as needed

Top

Appendix B - Command Line Reference
Sagacity has a number of PHP scripts available at the command line. Some are designed to be used that way, and others are better run from the web interface. The following sections will provide a list of those commands and their usage. Commands not listed in the following sections should generally not be used at the command line and may cause unexpected and often undesirable results.

Top

B.1 - Catalog Management Commands
update_db.php: The purpose of this script is to bulk update the CVE, CPE, STIG and Nessus plugin databases either from the Internet or local hard drive
Usage: php **update_db.php** [--cpe] [--cve] [--nasl] [--stig] [--do] [--po] [-h|--help]
--cpe To download and update the CPE catalog

--cve To download and update the CVE catalog
--nasl To download OpenVAS NVT library and update NASL files
You can also extract *.nasl files from the Nessus library to C:/xampp/www/tmp/nessus_plugins and it will include these in the update
--stig To download and update the STIG library
--do To download the files only...do not call the parsers
--po To parse the downloaded files only, do not download
-u={url} [optional] Used only for STIGs because sometimes DISA will use a non-standard link which makes it difficult to download the file.
-h|--help This screen

parse_cpe.php: Parses the NIST CPE file
Usage: php **parse_cpe.php** -f={CPE list file} [--debug] [--help]
-f={CPE file} The CPE file to parse retrieved from http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.3.xml
--debug Debugging output
--help This screen
Output: You will see either a . (dot), * (asterisk), or - (hyphen) for each CPE.
. - CPE was already in the DB
* - CPE was added to the DB
- - CPE was removed from the DB (CPE deprecated)
Purpose: To parse a CSV E-Checklist file

parse_cve.php: Parses the CVE file (allitems.xml) retrieved from http://cve.mitre.org/data/downloads/allitems.xml
Usage: php **parse_cve.php** -f={CVE filename} [--debug] [--help]
-f={CVE filename} The file to be parsed (allitems.xml). Can be absolute or relative path.
--debug Debugging output
--help This screen

parse_stig.php: To parse a STIG XCCDF checklist file and populate/update the database
Usage: php **parse_stig.php** -f={STIG file} [--debug] [--ia_reset] [--draft] [--help]
-f={STIG file} The file to be parsed
--debug Debugging output
--ia_reset To delete any existing mapped IA controls and repopulate with what is in the checklist file
--draft This will allow the importing of a draft STIG file (normally excluded)
--help This screen

nessus-plugin-import.php: The purpose of this script is a bulk update of all Nessus plugins in the tmp/nessus_plugins folder. It is called by update_db.php --nessus, and calls nessus_plugin-to-database.php for each plugin found.
Usage: php **nessus-plugin-import.php** [-h|--help]
-h|--help This screen

nessus-plugin-to-database.php: This script is for reading NASL files and adding them to the database
Usage: php **nessus-plugin-to-database.php** -f={NASL file to parse} [--debug]
-f={NASL file} The .nasl file to parse
--debug This will output what was parsed by the script and NOT add anything to the database

parse_iavm.php: Imports an IAVM file and populate/update the database
Usage: php **parse_iavm.php** -d={IAVM Directory} [-f={XCCDF result file}] [--debug] [--help]
-d={IAVM directory} The directory to import the files from. This will crawl the directory and import all the IAVMs
-f={XCCDF file} The IAVM file specifically
--debug Debugging output
--help This screen

parse_cce.php: Parses the NIST CCE list
Usage: php **parse_cce.php** -f={cce list file} [--debug] [--help]
-f={cce file} The CCE list file retrieved from http://static.nvd.nist.gov/feeds/xml/cce/cce-COMBINED-5.20130214.xml
--debug Debugging output
--help This screen

parse_cci.php: The purpose is to parse the NIST CCI list
Usage: php **parse_cci.php** -f={CCI list file} [--debug] [--help]
-f={CCI file} The CCI file to parse
--debug Debugging output
--help This screen

parse_nvd_cve.php: To import the National Vulnerability Database (NVD) CVE annual files
Usage: php **parse_nvd_cve.php** -f={CVE file} [--debug] [--help]
-f={CVE file} The CVE file to import
--debug Debugging output
--help This screen

parse_iavm_cve.php: Imports the cve-to-iavm(u).xml file retrieved from http://iasecontent.disa.mil/stigs/xml/iavm-to-cve%28u%29.xml
Usage: php **parse_iavm_cve.php** -f={file} [--debug] [--help]
-f={file} The file to import
--debug Debugging output
--help This screen

Top

B.2 - Result File Ingestion Commands

background_results.php: This program was written to look at all files in the /tmp directory, determine what parser is needed, then call that parser with the appropriate flags.
Usage: php **background_results.php** -s={ste_id} [-i=1] [-t=1] [--help]
-s={STE ID} The ID of the ST&E to know what to assign the results to
-i=1 Ignore hidden Excel worksheets (only used on Excel eChecklist files) (defaulted to false)

-t={Target Name} The name of the target to evaluate (only used on host data collection)

--help This screen

parse_excel_echecklist.php: Imports an Excel eChecklist file.
Usage: php **parse_excel_echecklist.php** -f={eChecklist File} [-i] [--debug] [--help]
-f={eChecklist File} The file to import
-i Ignore hidden worksheets. This run by default when run through Sagacity
--debug Debugging output
--help This screen

parse_nessus.php: Imports a Nessus result file
Usage: php **parse_nessus.php** -s={ST&E ID} -f={Nessus result file} -d={document root} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={Nessus file} The result file to import
-d={document root} The document root of the web server
--debug Debugging output
--help This screen

parse_nmap.php: Imports an NMap result file
Usage: php **parse_nmap.php** -s={ST&E ID} -f={NMap result file} -d={Document root} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={NMap file} The result file to import (will import text, XML, and grepable files)
-d={Document Root} The document root of the web server
--debug Debugging output
--help This screen

parse_scc_xccdf.php: To import an XCCDF result file from Security Compliance Checker 3.1+
Usage: php **parse_scc_xccdf.php** -s={ST&E ID} -f={XCCDF result file} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={XCCDF file} The result file to import (will not import oval, dictionary, or other files)
--debug Debugging output
--help This screen

parse_stig_viewer.php: To parse a STIG Viewer output result file
Usage: php **parse_stig_viewer.php** -f={STIG Viewer file} [--debug] [--help]
-f={STIG Viewer file} The STIG Viewer result file that is being imported
--debug Debugging output
--help This screen

parse_mbsa.php: Imports an MBSA result file
Usage: php **parse_mbsa.php** -s={ST&E ID} -f={result file} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={result file} The result file to import
--debug Debugging output
--help This screen

Deprecated scripts. The following scripts are not used anymore because of changes to the way Sagacity works.

parse_csv_echecklist.php: Sagacity does not require the use of CSV formatted eChecklists.
Usage: php **parse_csv_echecklist.php** -s={ST&E ID} -f={CSV eChecklist} [--debug] [--help]
-s={ST&E ID} The ST&E ID that this result file is going to be imported for
-f={E-Checklist file} The E-Checklist file to import
--debug Debugging output
--help This screen

parse_mssql.php: Imports the MSSQL SRR result file from DISA.
Usage: php **parse_mssql.php** -s={ST&E ID} -f={result file} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={result file} The result file to import
--debug Debugging output
--help This screen

parse_proc_echecklist.php: To import a DIACAP procedural eChecklist file that is filled out
Usage: php **parse_proc_echecklist.php** -s={ST&E ID} -f={Procedural eChecklist File} [--debug] [--help]
-s={ST&E ID} The ST&E ID this result file is being imported for
-f={file} The file to import
--debug Debugging output
--help This screen

Top

B.3 - Other Potentially Useful Commands

post_process_all.php: Perform bulk post-processing, which associates STIGS with targets based on OS and installed software
Usage: php **post_process_all.php** [--ste={ST&E ID}] [--help|-h] [--debug]
NOTE: If no ST&E specified then will get all targets that have the pp_flag field in the database set to '1'
--ste={ST&E ID} The ST&E ID to evaluate targets
--debug Debugging output
--help | -h This screen

php export-ckl.php: This script was written to be able to export CKL files from the data contained in the database.
Usage: **php export-ckl.php** [-d={destination}] -s={ste id} [-c={category id}] [-t={target id}] [-h|--help]
-s={STE ID} Export a CKL for each assigned checklist for ALL targets in this ST&E

-c={Category ID} Export CKL files for all targets contained in this Category
-t={Target ID} Export CKL file for each assigned checklist for this target
-d={destination} Location of where you want the files saved
-h|--help This screen
--debug Debugging output

Top

Appendix C - Assessment Cheat Sheet

We put together the following cheat sheet as a reminder of commands and steps to take during an assessment. These commands or procedures may or may not be useful to you for your testing, but is provided here for your reference. The analyst is responsible for knowing how the tools work and their proper and safe use.

Top

C.1 - Unix Systems

Host Data Collection

The host data collection scripts for Unix are found in the *C:\xampp\www\exec\Target Host Tools\Unix* folder. The scripts are *linux-data-collection.sh* and *solaris-data-collection.sh* for the respective Operating Systems. Upload the script to the target /tmp folder and run it. The results will be in a folder called *hostname*-baseline. The script will attempt to gzip the results into a tarball called hostname-*baseline.tgz*. This file can be taken back to the system running Sagacity and uploaded for that target.

Secure Copy (scp) the resulting tar file to the laptop with your username and password. Results will be in your Cygwin home directory.

- scp resultsfile.tar user@laptop IP:~/.
- (e.g. scp ws1.tar odegardj@192.168.3.5:~/.)

The file will be in Cygwin in /home/*username*

If SSH is not available, use FTP as a last resort. Do not forget to use binary mode!

- ftp *laptop IP*
- Enter username and password. If you fail the login, you can use the *user* username command to try again.
- Enter the following three commands, in order: bin, hash, prompt.
- Use put or mput to upload the files to the laptop, e.g. mput *.tar

The file will be in Cygwin in */home/username*

Command Line SCC Instructions

For GUI Instructions, see the Windows section. The basic steps are the same in the Unix GUI.

1. As root, run *./cscc --config*
2. “1. Configure SCAP content”
3. “9. Exit, save changes, and execute scan.”
4. At the end of the run, SCC will inform you of the Session Results folder location.
5. Copy the SCAP results folder in its entirety to a central location. The SCAP folders from different hosts can be safely merged together.
    a. Ultimately, we are only looking for the XCCDF-Results XML files in the XML sub-folder.
6. Once the scan is complete and the results are collected, you can delete the folder from the C:\temp or /tmp directory.

Top

C.2 - Windows Systems

Host Data Collection

The Windows target host tools are located in *C:\xampp\www\exec\Target Host Tools\Windows*.

To run MBSA, run *mbsa.bat* as Administrator. Export the findings XML file and copy it to the system running Sagacity. Upload the results using the Scans → Result Management page.

To run Windows Data Collection, run *windows-data-collection.bat* as Administrator. Findings will be located in *C:\temp*. If possible, the script will create a file called *hostname-DataCollection.zip* that can be copied to the system running Sagacity and uploaded to the target.

Transferring files to the testing system can be done using a NetBIOS share, CDROM, or USB hard drive, if allowed. As a last resort, you can use FTP. See the FTP instructions in section C.1 if you are unsure how to use it.

SCC GUI Instructions

1. Windows: Right click on the *scc.exe* executable and select “Run as Administrator”
2. Unix: Open a root command terminal and run *./scc*
3. From the menu, select Edit à Content and Options
    a. Select the appropriate checklists for the hosts. Leaving unnecessary checklists selected will not affect the outcome, since SCC will automatically select applicable checklists.
    b. Click OK.
4. Ensure “Local Computer” is selected, then click “Analyze Selected Computer(s)”
5. When the test is finished, select “Results à Open Results Directory” There will be a resuls folder with the Time/Date stamp of the run. Inside this folder is an SCAP results folder.
6. Copy the SCAP results folder in its entirety to a central location. The SCAP folders from different hosts can be safely merged together.
    a. Ultimately, we are only looking for the XCCDF-Results XML files in the XML sub-folder.
7. Once the scan is complete and the results are collected, you can close SCC and delete the folder from the C:\temp directory.

Top

C.3 - Network Devices

The following instructions are provided to gather network device configurations for offline assessment.

Collection methods.

- Unix/Cygwin: Open a terminal window and run the following commands. The system administrator will have to provide credentials.
  - *script <hostname>-config.txt*
  - *ssh <hostname ip> (login)*
  - *enable (to enter administrative mode)*
  - *when finished: exit / exit / exit (to close out the script command)*
- Putty:
  - In the Putty Configuration, got to Sessionà Logging
  - Select either "Printable output" or "All session output"
  - Set the log file name to *<hostname>-config.txt*
  - Click "Open" to start the SSH session.

All devices commands:

- *show config*
- *show run*
- *show version*
- *show logging*
- *show ip route*
- *show snmp (if in use)*
- *show snmp user (if in use)*
- *show cdp neighbor (if in use)*
- *show cdp nei det (if in use)*
- *show environment* (if required by the ASCA)
- *show arp* (if required by the ASCA)
- *show interface* (if required by the ASCA)
- *show interface status* (if required by the ASCA)
- *show flash:* (if required by the ASCA)
- *show nvram:* (if required by the ASCA)

Switch specific commands

- *show vlan*
- *show interface trunk*
- *show port-security interface*
- s*how mac address-table* (if required by the ASCA)

Router specific commands

- *show policy-map control-plane*
- *show ip pim interface (and/or show ipv6 pim interface, if in use)*
- *show ip cef (and/or show ipv6 cef, if in use)*
- *show ip ospf database (if in use)*
- *show ip nat trans (if in use)*

ASA Firewall specific commands

- *show asp table socket*

*Once you have saved the text file (exit the script command or exported the session to a text file, depending on your collection method), s*anitize all password hashes (watching for weak encryption and re-used passwords) and SNMP strings. Replace the strings with "*** *[weak/duplicate] password hash* ***", "*** *[guessable/string] community string* ***", etc. Those good descriptions will help the security analyst performing the assessment.

Top

C.4 - Nmap

In Cygwin: *cd /home/assessments/system/project/network*

Test Connectivity

- *nmap -T4 -n -sP target network/24 --exclude myIP -oN filename-ping.nmap*
- *nmap -T4 -n -sn target network/24 --exclude myIP -oN filename-ping.nmap*

Quick TCP Scan to get started and make sure things work

- *nmap -T4 -n -sS -F target network/24 --exclude myIP -oN filename-tcp-fast.nmap*
- *nmap -T4 -n -sS -p 1-6500 target network/24 --exclude myIP -oN filename-tcp-6k.nmap*

Full TCP Scan

- *nmap -T4 -n -sS -p 1-65535 target network/24 --exclude myIP -oN outputfile-tcp.nmap*

Quick UDP Scan

- *nmap -T4 -n -sU -F target network/24 --exclude myIP -oN output file-udp-fast.nmap*
- *nmap -T4 -n -sU -p7,13,19,49,53,69,111,123,161,162,514,517,518,2049,6000 target network/24 --exclude myIP -oN output file-udp-limited.nmap*

Longer UDP Scan. Do not do *-p 1-65535* unless you plan on running it at least overnight.

- *nmap -T4 -n -sU -p 1-2049,6000 target network/24 --exclude myIP -oN output file-udp.nmap*

Nmap IPv6 Scanning

- *nmap -iflist* (determine which interface is your Local Area Connection – eth1 on the laptops)
- *nmap -6 --script=targets-ipv6-multicast-** (basic IPv6 discovery using all the multicast scripts)
- *nmap -6 --script=targets-ipv6-multicast-* --script-args=newtargets -PS --top-ports=10000* (adds 10K TCP port scan)
- *nmap -6 --script=targets-ipv6-multicast-echo.nse --script-args 'newtargets,interface=eth1'* (just run the one script)

nmap --help is your friend.

Top