|  |
| --- |
| Scans To Reports |
| Automating the Cyber Compliance Realm |

|  |
| --- |
| 2020 | By: Robert Weber |

****

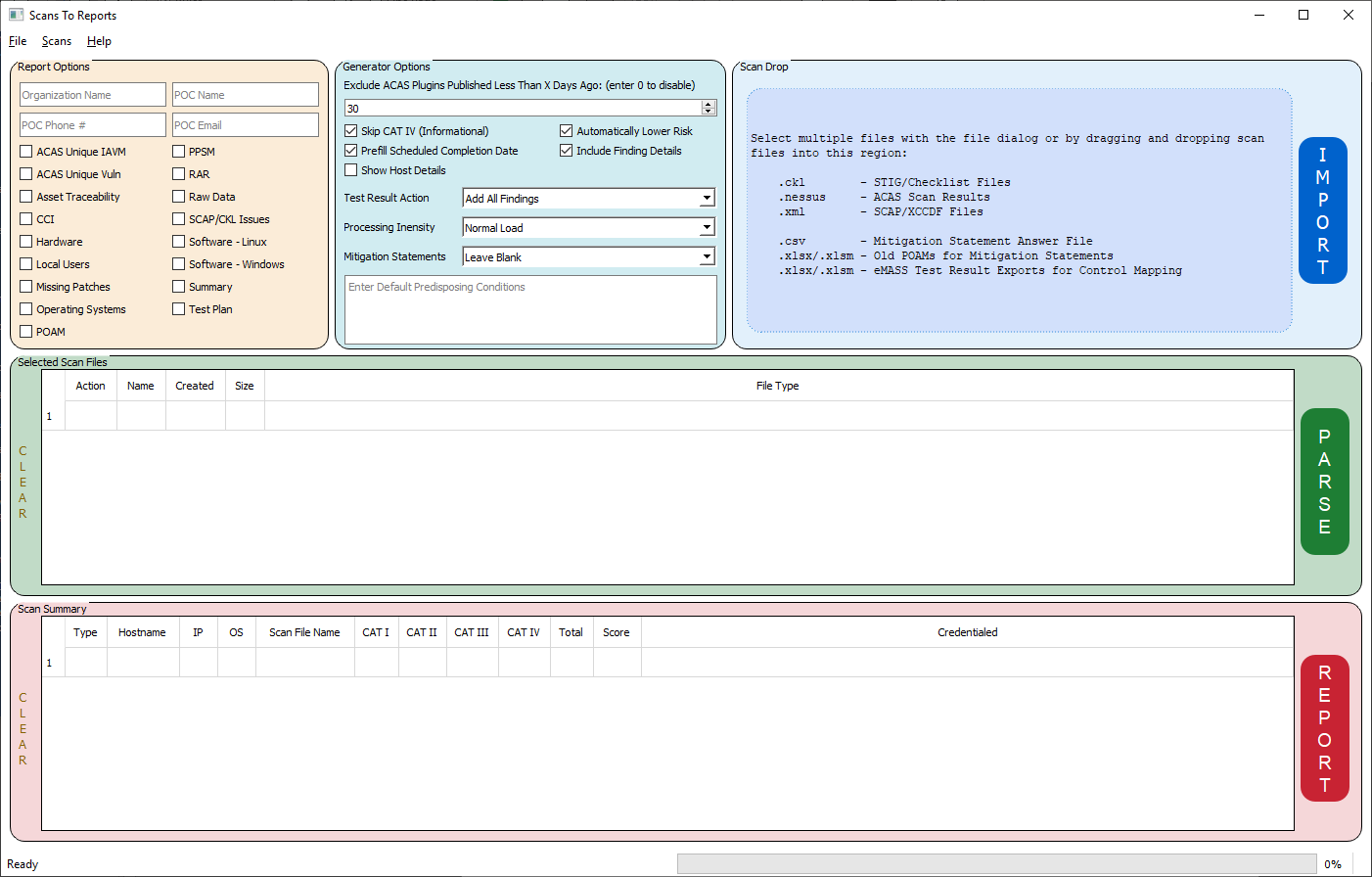
**A close up of a logo

Description automatically generated**

|  |
| --- |
| Scans To Reports |
| User Guide and Maintenance Manual |

# Overview

Scans To Reports is the current version of a set of projects that have been ongoing since 2015. The first version of this tool was a PowerShell v2.0 script that would parse scans and generate an eMASS compatible POAM/RAR. The overall goal of that project has been maintained and enhanced over the various iterations, culminating in this new cross platform tool suite. The current release has been completely rewritten in Python and cross-compiled into platform specific binaries, support Windows, Linux and MacOS systems. The Scans To Reports Generator makes it easy to verify the overall compliance of your systems and to glean useful information about all your assets. The final reports are also generated in a format that is compatible with eMASS POAM imports and artifact uploads. These reports make it much easier to clearly see the overall security posture of your program.



## Additional Functions

In addition to just generating the Scan Reports, additional scan utilities have been created and included with the latest release. The application is able to assist with merging and splitting draft ACAS files, and updating STIG Checklists by copying statuses and comments from old CKL files into new CKL files. These additional functions make it much easier to automate your scan processes.

## Possible Imports

The Scans To Reports generator is able to import many of the DoD mandated scan file types in order to generate the aggregated report package. These imports include:

* .ckl - STIG/Checklist files
* .nessus - ACAS Scan Results
* .xml - SCAP Scan Files (XCCDF)
* .csv - Mitigation Statement Answer Files
* .xlsx/xlsm - Old POAM's for mitigation statements, eMASS Test Result Exports for Control Mapping.

It should be noted that none of the above-mentioned files are 'required' for the application to run. For example, the application will generate the applicable reports if only CKL files are submitted. The Excel and CSV enhancements will just not be executed. The same goes for submitting just ACAS .nessus files. This ensures the tool is capable of working with the RMF package scans at any state in the package generation process.

## Interfaces

The Scans To Reports application is capable of running both as just a command line utility, for those that prefer scripting or terminal applications, and with a full-fledged Graphical User Interface, for those who prefer a point and click environment. The majority of the functions within the application are accessible from both interfaces. This guide will fully detail the operation of both interfaces. Future releases will also include a browser-based interface, accessible to the local host only.

## Download Locations

The releases for this application are maintained and available from two internet sources.

The source code and cross platform binaries are bundled together in a single zip file available for download from the Cyber Trackr website (<https://cyber.trackr.live>). Once on the site, click the Utilities -> Standalone Scans To Reports Generator link.

The source code is also under version control on GitHub and compiled releases are made available as new functions are added. The GitHub repository is available at:

https://github.com/CyberSecDef/scans2reports

The source can be cloned from the main page and the Releases page is updated with each new compilation.

## Compiled Releases

The source for the application is written in Python (3.7+) but is cross compiled to Windows and Linux formats using the Python PyInstaller modules. This means that computers will not require a Python installation in order to utilize the application. The compiled releases include miniature portable versions of Python to execute the compiled source code. As such, in order to execute the binary releases, you only need to unzip the files onto your computer and double click the applicable application file.

## Viewing Source/Forking

The source code is available for anyone to download from the GitHub repository. If any developers are interested in making their own 'version', they can fork the source code to their own repository. Any code updates submitted by external developers will be reviewed on a case by case basis for inclusion in the master branch.

# Instructions

## Bottom Line Up Front

The Scans To Report Generator was designed to operate out of the box with as little user intervention as possible. Once you have application running you can drop scan files on the applicable section, click the Parse button and then click the Report button. There are several settings that can be tweaked by the end user and those settings will be memorized for all future executions.

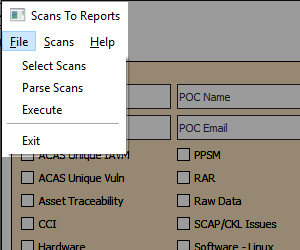
The command line interface also lets you set all applicable settings via application arguments. You can then create regular scheduled tasks to generate the reports based off a common collaborative folder that holds your scans.

## Graphical User Interface

The user interface is broken into several distinct and logical sections. Each section serves a distinct purpose and the overall application flow is from top to bottom.

### Main Menu

#### Files

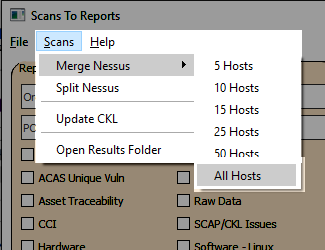


Select Scans - Used to select multiple scan files. Can be used multiple times to select scan files in different locations. Duplicated by the Blue 'Scan Drop' region of the application.

Parse Scans - Parses the selected scan file. Can be used multiple times if needed as updated scans are imported. Duplicated by the Green 'Selected Scan Files' region of the application.

Execute - Generates the report based off the parsed scan. Duplicated by the Red 'Scan Summary' section.

#### Scans



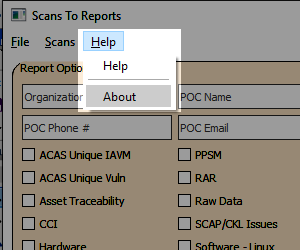
Merge Nessus - This will let you select multiple .nessus files and merge them all into a singular file based off of scan policies. This allows you to consolidate hundreds of scans into a single file upload for eMASS artifacts. If file size is an issue, you can choose to merge the files in chunks of between 5 and 50 hosts per file. The scan files can also be used in the Asset Manager section of eMASS.

Split Nessus - This is the inverse of the Merge Nessus function. This will take a single .nessus file and split it into multiple .nessus files, one per host. This makes it easy to remove 'bad' hosts in a scan and replace those scans with 'good' host scans.

Update CKL - This will let you select an old CKL file and copy all of the statuses, comments and finding details to a new CKL file. This comes in handy when updating from one release (V1R2) to the next (V1R2). The key used for the translation between CKL files is the vulnerability ID (V-12345), so changes between versions are likely not to yield great results.

Open Results Folder - This will open the 'results' folder the application uses to store the resulting reports using whatever platform option is available (Windows File Explorer, Nautilus, etc.).

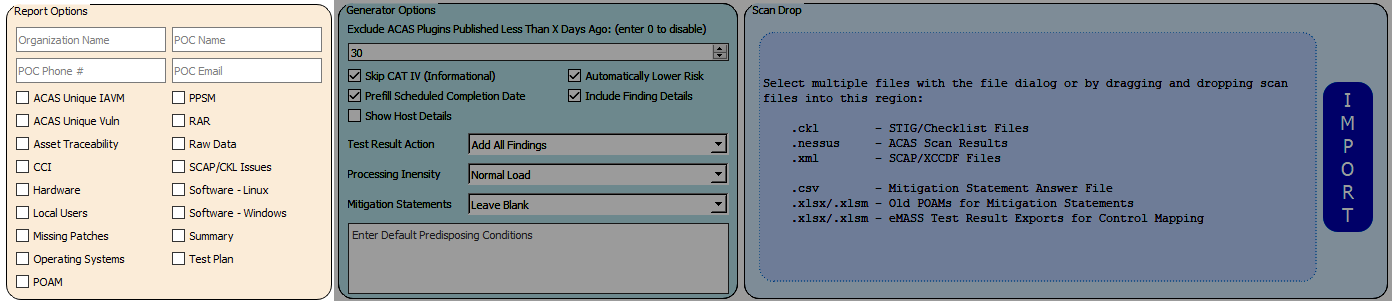
#### Help



Help - Shows a basic overview of the steps to use the application.

About - Shows the current version and release information.

### Report Options (Yellow Region)



This region of the application allows you to enter information to be outputted on the POAM/RAR tabs of the report. The data fields that accept user input are:

#### Organization Name

The name of the over-arching command or organization the package belongs to. This could be a base, a tenant, a company, etc. When utilizing the command line version of the application, this can be specified using the "-c" or "--command" arguments (e.g. scans2reports.exe --command "Cyber Trackr Live").

#### POC Name

The name for the main point of contact for the package. When utilizing the command line version of the application, this can be specified using the "-n" or "--name" arguments (e.g. scans2reports.exe --name "Robert Weber").

#### POC Phone #

The phone number for that POC. When utilizing the command line version of the application, this can be specified using the "-p" or "--phone" arguments (e.g. scans2reports.exe --phone "800-555-1212").

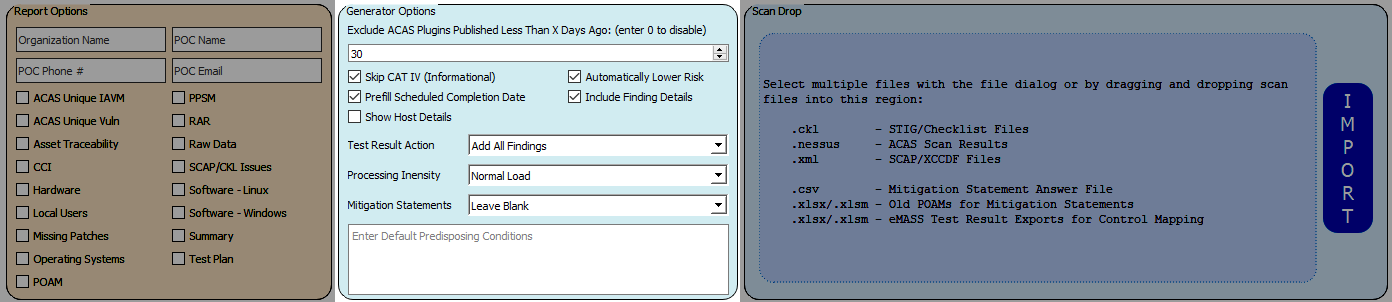
#### POC Email

The email address for that POC. When utilizing the command line version of the application, this can be specified using the "-e" or "--email" arguments (e.g. scans2reports.exe --command "wwwdaze2000@gmail.com").

#### Report Execution

This region also allows you to select/deselect the various tabs that will be generated in the resulting Excel file. The check boxes are automatically checked/unchecked based on the scan files that are parsed, but you can update the selections as you need once the parsing is completed. The report details are listed in the 'Generating Reports' section of this document.

### Generator Options (Teal Region)



This region allows you to change some of the inner workings of the application to suit your needs as a package developer. The details for those options are listed below.

#### Exclude ACAS Plugins Published Less Than X Days Ago

For most eMASS packages, ACAS plugins that are brand new do new have to be included in the final report sent to eMASS. This field allows you to select the number of days allowed in that grace period. This field defaults to 30 days, meaning a plugin that was released by Tenable 20 days ago would not show up on the POAM tab.

When utilizing the command line version of the application, this can be specified using the "-x" or "--exclude-plugins" arguments (e.g. scans2reports.exe -x 25)

#### Skip CAT IV (Informational)

This setting ensures any non-necessary CAT IV findings are not parsed, so they won't impact any of the report tabs. There are certain CAT IV plugins that are required for various functions in this application, such as 10399 which enumerates local users or 22869 which enumerates installed software. The CAT IV plugins that are used to determine those data sets will always be parsed, but any plugins outside this list of requirements will be skipped. This helps ensure the POAM/RAR tabs are not littered with hundreds of rows of unimportant findings.

When utilizing the command line version of the application, this can be specified using the "-i" or "--skip-info" arguments (e.g. scans2reports.exe --skip-info)

#### Automatically Lower Risk

This setting will automatically lower the risk of the open findings one step. For instance, all CAT I findings will be downgraded to CAT II automatically. This option is in place under the assumption a valid mitigation statement will either be imported or created for each open finding.

When utilizing the command line version of the application, this can be specified using the "-l" or "--lower-risk" arguments (e.g. scans2reports.exe --lower-risk)

#### Prefill Scheduled Completion Data

This will automatically fill in the Scheduled Completion Data on the POAM tabs based on the residual risk for each finding. The finding timelines are 3 years for CAT IV findings, 1 year for CAT III findings, 90 days for cat II findings and 30 days for CAT I findings.

When utilizing the command line version of the application, this can be specified using the "-s" or "--scd" arguments (e.g. scans2reports.exe --scd)

#### Include Finding Details

This toggle will populate that RAR and POAM comments column with each finding's "Details" (CKL, SCAP and ACAS). The information will show up at the bottom of the comments cell with the 'Finding Details' header. Some package chains require this information while others don't, so the toggle is available to support as many users as possible.

When utilizing the command line version of the application, this can be specified using the "-fd" or "--finding-details" arguments (e.g. scans2reports.exe -fd)

Show Host Details

This will populate additional scan level details for all affected devices for each finding on the POAM and RAR table. If this is unchecked, only the hostname will be displayed in this cell. If this is checked, each host will up as "hostname [CKL - Ver: 1, Rel/Feed: 10]" or "hostname [ACAS - V6.1.2, Rel/Feed: 20200601120000]".

When utilizing the command line version of the application, this can be specified using the "-hd" or "--host-details" arguments (e.g. scans2reports.exe -hd)

#### Test Result Action

If an eMASS export Test Result file is imported along with the scan files, this drop-down menu's action becomes relevant. If "Add All Findings" is selected, all parsed findings will be processed for the various reports. If "Mark As Closed" is selected, findings related to RMF Security Controls that are not part of the package will be automatically marked as closed with the applicable comment automated added to the comment column. If "Convert to CM-6.5" is selected, any findings that not part of the package controls will be added as Open with a comment stating CM-6.5 was selected as the finding security control.

When utilizing the command line version of the application, this can be specified using the "--test-results" argument followed by either 'add', 'convert', or 'close' (e.g. scans2reports.exe --test-results convert).

#### Processing Intensity

This drop-down menu selects how intense the parsing and report generation functions should run on your system. There are three options available in the user interface. You can select "Normal Load", "Light Load", or "Make My CPU Bleed".

From the command line interface, you can set this with the -t or --threads argument, followed by a number from 1 to 3 (e.g. scans2reports.exe --threads 2)

#### Mitigation Statements

This drop-down menu is used to select how the mitigation statement column on the POAM/RAR tabs will be populated. The possible options are:

Leave Blank - will leave the cell blank for each finding.

Existing POAM or Answer File CSV - will populate the mitigation statement as it is entered in the applicable file.

CKL Comments - will populate the cell based on the comments field in the applicable CKL file.

POAM/CSV, then CKL (Prefer Existing POAM/CSV) - This will populate the mitigation statement first by previously submitted POAMs or CSV Answer files. If there are no applicable mitigation statements in those files, the comments field from the CKL file will be used. If that is also blank, then a blank cell will be used.

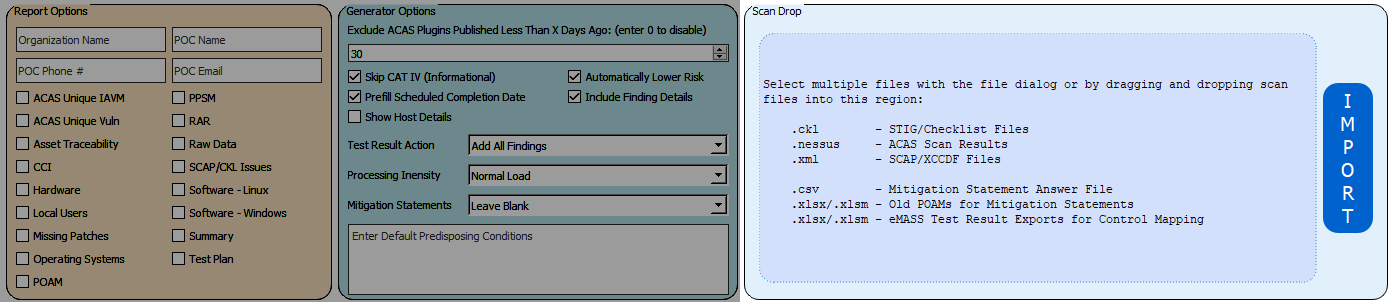
When utilizing the command line version of the application, this can be specified using the "--mitigation-statements" argument followed by either 'blank', 'poam', 'ckl', or 'both' (e.g. scans2reports.exe --mitigation-statements poam)

#### Predisposing Conditions

This text area allows you to enter a paragraph or two of text that will pre-populate in the predisposing conditions field of the RAR/POAM tabs. This will be added to every finding populated on those two sheets.

When utilizing the command line version of the application, this can be specified using the "--predisposing-conditions" argument followed by a quoted string of text (e.g. scans2reports.exe --predisposing-conditions "this is a paragraph of text")

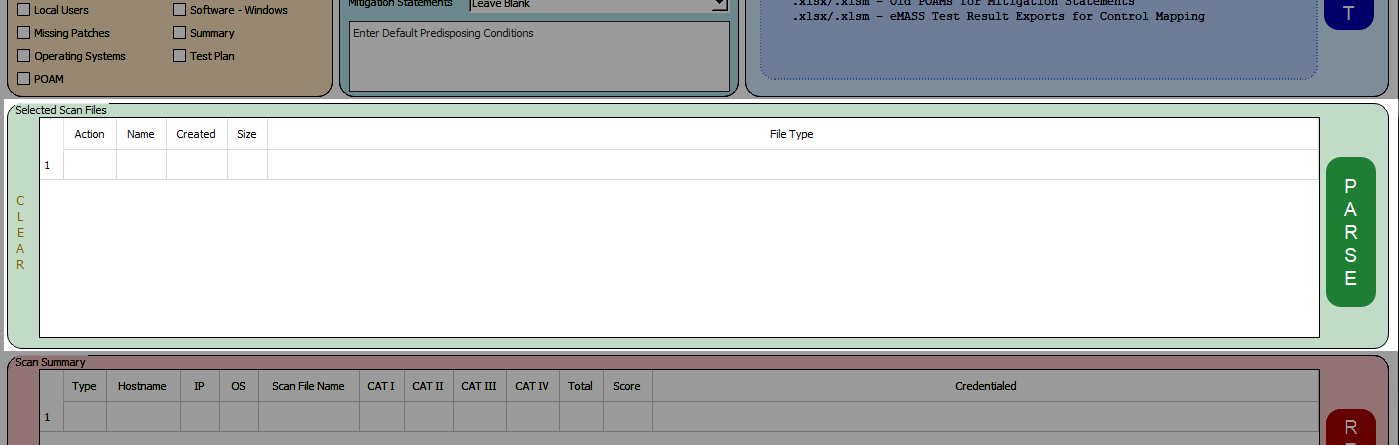
### Scan Drop (Blue Region)



This region is where you can drag and drop your scan files and other artifacts onto the application. As you drop them, they will populate in the "Selected Scan Files" below. You can also click the Blue "Import" button to open a file selection dialog to do the same. Any non-supported files will be ignored.

Point to note - Dropping thousands of files on this Blue region can cause the application to freeze for a few seconds. If that happens, just wait until the application unfreezes.

### Selected Scan Files (Green Region)

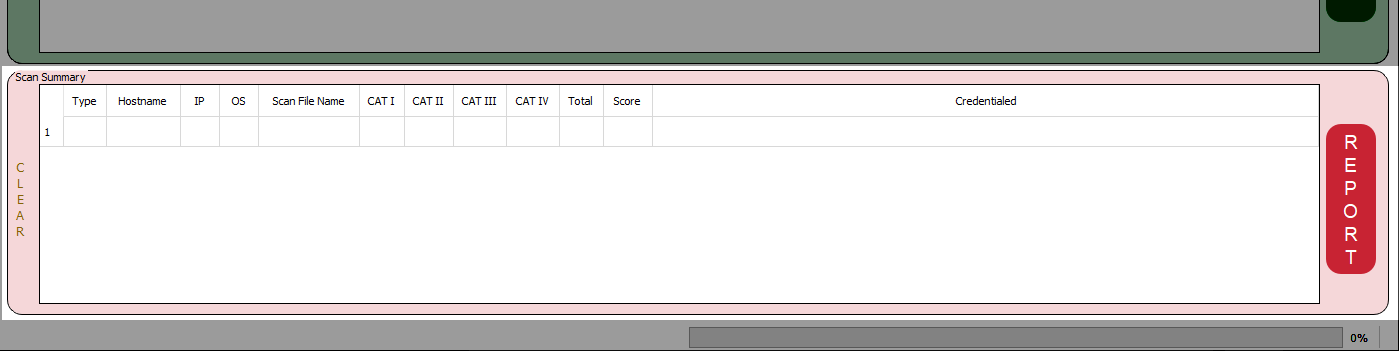


This table populates with scan file data for all the selected scan files. The table is sortable by clicking on the column headers. Individual scan results can be deleted by clicking on the "DEL" button in the specific files row. To clear the entire table of scan files, click on the "CLEAR" button to the left of the table. After reviewing all the selected files populated in this table, click on the Green "Parse" button to begin processing each file.

As the scan files are parsed, the Yellow "Report Options" section will pre-select the applicable report types based on the scans read. For instance, the POAM and RAR check boxes will automatically check for any CKL, ACAS or SCAP files read in. The ACAS Unique IAVM check box will automatically check once an ACAS file is read in. The only report that won't automatically check is the SCAP/CKL Issues report as this report will take an extensive amount of time to render when large numbers of files are submitted.

Depending on the speed of your computer and the "Processing Intensity" selected above, this parsing process can take a while to complete. The overall status and progress will be displayed at the bottom of the application along with an ETA for completion.

### Scan Summary (Red Region)



Once all the files are parsed, the applicable scan information will be populated in this table. This summary will show a brief list of details for each host per scan file, including information like the number of findings per category and the credential status for each scan. To clear this information, click on the "CLEAR" button to the left of the table. Once you are satisfied with the review of this table, click on the Red "Report" button to begin generating the report file.

This process will also take a fair amount of time to finish, mainly depending on the number of scans selected. The current report being rendered, and the overall status will be displayed in the status bar area at the bottom of the application.

### Status Bar/Progress

This section displays the current status of the application, as well as the overall progress completed.

## Command Line Execution

The scan related functions can all be executed via direct command line parameter calls. The scan2reports binaries all include an option to display the 'help' file by calling the -h parameter. The general order of the command line execution parameters is:

usage: scans2reports.exe [-i] [-fd] [-g] [-hd] [-l] [--mitigation-statements {blank,poam,ckl,both}]

[--predisposing-conditions PREDISPOSING\_CONDITIONS] [-s] [--test-results {add,convert,close}]

[-t THREADS] [-x EXCLUDE\_PLUGINS] [-c COMMAND] [-e EMAIL] [-n NAME] [-p PHONE] [-h]

[input\_folder]

required arguments:

input\_folder The folder to collect scans from.

optional arguments:

-i, --skip-info Skip Informational Findings

-fd, --finding-details Whether or not to include the finding details in the POAM/RAR Comments

-g, --gui Use the GUI instead of the console

-hd, --host-details Show affected devices as

hostname [SCAN\_TYPE - Ver: #, Rel/Feed: # ]

on the POAM/RAR tabs

-l, --lower-risk Automatically Lower Risk on POAM

--mitigation-statements {blank,poam,ckl,both}

Import Mitigation Methods (blank, poam, ckl, both)

--predisposing-conditions “PREDISPOSING\_CONDITIONS”

Enter default Predisposing Conditions

-s, --scd Prefill Estimated SCD to POAM

--test-results {add,convert,close}

Add, Close or Convert CCI Mismatches

-t THREADS, --threads THREADS

How intensive should the generator run (1-3). Defaults to 2.

-x EXCLUDE\_PLUGINS, --exclude-plugins EXCLUDE\_PLUGINS

Exclude plugins newer than this number of days. Defaults to 30.

-c COMMAND, --command COMMAND

Add Responsible Command/Organization Caption to POAM

-e EMAIL, --email EMAIL

Add POC Email Address to POAM

-n NAME, --name NAME

Add POC Name to POAM

-p PHONE, --phone PHONE

Add POC Phone Number to POAM

-h, --help Show this help message and exit

# Generated Reports

The following reports are generated by the Scans To Reports generator. These are all included as separate tabs within the Excel Report.

## ACAS Unique IAVM

This report shows any open IAVM findings found by parsing ACAS Files. This report will show the applicable Plugin ID, IAVM Number, Plugin Name, Plugin Family, Severity and the total number of hosts that have this finding open. This report is identical to the Security Center Report Template but is applied to all ACAS scans submitted as opposed to a single ACAS scan.

## ACAS Unique Vuln

This report shows a summary of every Unique Vulnerability found by parsing ACAS files. This report will show the applicable Plugin ID, Plugin Name, Plugin Family, Severity and the total number of hosts affected. This report is identical to the Security Center Report Template but is applied to all ACAS scans submitted as opposed to a single ACAS scan.

## Asset Traceability

This report shows a breakdown of individual assets cross referenced against all scan types. The column headers in this report are auto filterable so you can use this to ensure each host has the required scan types executed against them. The applicable versions and release data points is also populated on this report.

## CCI

This is just a raw data dump and is not directly tied to specific scan results. This tab is populated for research purposes, so the reviewers have easy access to CCI data while validating the applicable reports within the resulting Excel file. All applicable CCI information, including Security Control links, is populated in this report.

## Hardware

This is a hardware list populated based on all submitted scan files. Each asset will appear only once in this list, along with information such as the asset type, IP address, manufacturer, model, serial number, Operating System, etc. Some information, such as 'Virtual Asset?' needs to be populated by the reviewer if this is going to be used as an artifact in eMASS or in an A&A document.

## Local Users

This is a list of all the local users found on each of the hosts that had applicable ACAS scans executed against them. This report shows the hostname, Operating System, and local username.

## Missing Patches

This is a list of all the missing patches that need to be installed on the assets within the package. This information is populated from ACAS Plugin 66334. This report will display the hostname, operating system and applicable action to take to remediate the finding.

## Operating Systems

This is a list of all the operating systems found in the processed scans, along with the count of the number of hosts that have that operating system installed.

## POAM

This is an eMASS compatible POAM populated with all the scan findings parsed. The cells on this sheet can be copy/pasted into the template available for download from the eMASS website.

## PPSM

This is a list of the Ports, Protocols and Services found during the ACAS Scan Executions. This report matches the format expected for the eMASS A&A documentation.

## RAR

This is a RAR compatible for upload as an artifact into eMASS, if needed. The RAR file requirement is being removed from RMF Cyber Packages, but this report is being maintained for legacy purposes.

## Raw

This is a dump of all the raw data parsed from all the submitted scan files. Most data fields from the selected scan files are outputted on this report so this report can be used to verify and validate the results found on all the other tabs.

## SCAP/CKL Issues

This report shows inconsistencies between CKL scans and SCAP Scans. For instance, if a SCAP scan shows a particular finding is open, and that same vulnerability is marked as closed in submitted CKLs, that data point will be populated on this report. Ideally, this report should be empty. That being said, this report does not mean there are definite issues with the scans, only that someone should verify the findings are being properly marked. This report is also disabled by default as it takes an excessive amount of time to generate for executions with larges mounts of scans. This should only be used at the beginning of package validation processes.

## Software (Windows)

This report shows all the Windows based software that was present on the hosts scanned with ACAS. The applicable software name, version, and host are listed on this report.

## Software (Linux)

This report shows all the Linux based software that was present on the hosts scanned with ACAS. The applicable software name, version, and host are listed on this report.

## Summary

This summary report shows a breakdown of the number of findings per host per scan, much like the Summary table shown in the Red 'Scan Summary' region of the application. This report shows the applicable scan type, hostname, IP, operating system, scan filename, scan date, scan duration, version, release, policy, credential status, scan user and finding count per category.

## Test Plan

This is an eMASS compatible Test Report that can be included as an artifact or appendix to the A&A document based on all the scans submitted.

# Errors

This application is under active development, but bugs and errors may occur with its use. If you do find any issues, want to provide feedback or request new features, you can always reach out to me. The preferred contact methods are:

## GitHub Issues

You can view the issues open with this project by going to the GitHub ScansToReports Repository and clicking on the Issues tab at the top of the browser window. You can open issues directly on GitHub for my review and resolution. Please provide as much detail as possible and try to follow the templates provided for Bugs and Feature requests. If I need additional information, I will reach out to you.

## Cyber Trackr

Feel free to get in touch with me via the 'Contact Us' page on the Cyber Trackr website. Its available on the black banner at the top of the website.

## Email

You can also email direction at <wwwdaze2000@gmail.com>

# Future Changes

## Web UI

One of the main updates I am seeking to add is a web user interface for the application. This will provide the same functionality as the typical GUI interface, but will be available using a web browser at a URL like <http://localhost:5000/>

## Rest API Functions

After the Web User Interface is created, I am going to see about making this a client/server type application as well with a full REST API schema available for use. This will allow the application to be utilized across an entire organization.

## Add Cancel Button

Right now, once a process is underway there is no way to cancel it. Part of this is because of the multi-threaded libraries and configurations in use. I am going to work on adding the ability to 'STOP' a process mid-way incase settings or additional files need to be added to the workload.

## ACAS XCCCDF/SCAP Parsing

Right now, the only way to parse SCAP scan files is via the SPAWAR created SCAP Compliance Checker scanning tool. This tool outputs SCAP Scan results in a specific format (XCCDF). ACAS is capable of performing SCAP scans as well, but the resulting scan file format does not match the typical SCAP or ACAS format. I am working to add this additional feature in the next release.