Thank you for downloading Sagacity, a standalone web application designed to ingest, manage and report on vulnerability assessment and STIG compliance data. If you find it useful, please consider helping us make it better.

For usage instructions, please read the user guide, located on your Sagacity host: http://localhost/help.php?topic=all

We are constantly trying to improve our software. Please e-mail any bugs or feature ideas to developers@cyberperspectives.com subject Sagacity Bug, or you can enter a ticket in the SourceForge Project here: https://sourceforge.net/p/sagacity/tickets/

Table of Contents

System Requirements

Sagacity requires a relatively beefy system to do all the things that are necessary. Sagacity operates very well on Linux distributions. These are our recommendations.

Windows:

- Processor: 2.0 Ghz+ (recommend Intel i5+)
- Memory: 8GB
- Hard Drive: 50GB free (SSD recommended)

Linux:

- Processor: 2.0 Ghz+ (recommend Intel i5+)
- Memory: 4GB
- Hard Drive: 50GB (SSD recommended)

Software Requirements

Sagacity has the following software requirements. The versions listed are the minimum required for operation. For PHP, we recommend the closest version you can get to the one listed, further versions may deprecate features before we have the chance to update the code.

- PHP 7.2+
- MySQL 5.7+ or MariaDB 10+
- Apache 2.4+

Sagacity accomplishes a lot of data intensive tasks as such we recommend 1GB of memory for PHP (set in php.ini by the memory_limit directive). Other required settings are checked later in the install process. Any errors will need to be corrected before you can proceed.

Service Configurations

We have included hardened configuration files for Apache, MySQL/MariaDB, and PHP in the /conf directory. On Windows, these files get copied to the XAMPP directories automatically. Existing files are renamed to .old. On Linux, no changes are made because of the distributed nature of Linux distributions' configs. Some use several files for Apache and PHP (e.g. 1 for CLI and 1 for Apache). This makes it difficult and potentially confusing to copy the configs, thus they are not.

Windows Installation

The following software will need to be downloaded from the vendors. The versions listed indicate the tested version of the software, but these versions do not necessarily need to be used, just so long as there are no compatibility or accreditation issues. To perform most of these steps you will need administrative access to the client you are working on. During the installation if you are prompted to allow firewall access, then you will need to allow for Domain/Private networks.

- XAMPP v7.2.12
  - http://www.apachefriends.org/en/index.html
  - Apache v2.4.37
  - MariaDB v10.1.37
  - PHP v7.2.12
- MySQL Workbench v8.0.13 (highly recommended)
  - http://dev.mysql.com/downloads/tools/workbench/
  - Requires .NET Framework 4.5 and MSVC++ 2015 Redistributable. The links are on the page under prerequisites. Note: These may already be installed in Windows 10.
- TortoiseGit v2.7.0 (recommended)
  - http://tortoisegit.org/download
- If you want to use the OpenVAS plugin database, you will need a way to extract the nasl_plugins package. We recommend either 7zip, Cygwin, or using Bash for Windows for this, or extracting the files on a separate Unix system before loading them into the database.

XAMPP Installation

- Select "OK" on UAC dialog.
- When installing XAMPP, ensure that ONLY Apache, MySQL/MariaDB, and PHP are selected. All other options are unnecessary.
- Accept the default installation directory (C:\xampp)
- Uncheck "Learn more about BitNami for XAMPP"
- Click next two more times to complete the installation
- You may be prompted that the Windows Firewall has blocked the process. Allow communication for each of them on private networks.
- When the installation finishes, you can uncheck the box to open the XAMPP Control Center as it is not necessary to open, unless you want to test your installation (in which case see the header "Test XAMPP Install" below.

- We recommend that you add the PHP (C:\xampp\php) and MySQL (C:\xampp\mysql\bin) paths to your ENV PATH variable to simplify commands you may want to run. Right-click "Computer", select "Properties," "Advanced System Settings", "Environment Variables." Be sure to change the path for all users.

Test XAMPP Install

- To test the XAMPP installation, open the XAMPP Control Center from the Start menu. Start the MySQL service (you might be prompted to allow by the UAC), then start the Apache service (you might be prompted to allow by the UAC)
- Once they are started you can open a browser and go to http://localhost and it will show you an Apache test page.
- If Apache does not start, see the Troubleshooting section at the end of this document to see common known issues.
- Close the browser
- Go back to the XAMPP Control Center and stop the Apache and MySQL services, then close the XAMPP Control Center (make sure it is also not running in the task tray

Setup Git Repository

- Install TortoiseGit, accept the default options
- Open a Windows Explorer and browse to "c:\xampp" folder
- Click on an empty space (ensure that there is no directory selected) and click "Git Clone..." from the menu
- In the URL box, type "https://github.com/cyberperspectives/sagacity"
- In the Directory box, type "c:\xampp\www" (remove the "sagacity" at the end)
- If you would like the latest development version, you can check the "Branch" checkbox and then type the latest version number in the box "v1.3.4" as of this edit (open the Github page and look at the branch drop down for the exact branch name)
- Then click "OK" to start cloning the repository. You may need to enter your GitHub credentials

Download ZIP

- If you would rather just download the ZIP file from the GitHub repo you can do that as well and just extract the files to c:\xampp\www then continue with the "Install Sagacity" step

Install Sagacity

- Browse to "*c:\xampp\www*"
- If installing on Windows 10, right-click on the www folder, select "Properties" and make sure that the folder is not set to Read Only. If it is:
    - Uncheck the "Read Only" box and click "Apply"
    - Make sure that the "Apply changes to this folder, subfolder and files" box is selected.
    - Click OK
- Right-click on "*install.bat*" and select "Run as Administrator"
- Enter admin credentials, if prompted
- This script will copy hardened config files for Apache, MySQL/MariaDB, and PHP to the appropriate directories (after renaming existing files to .old) and create the system services for Apache and MySQL/MariaDB.

NOTE: Sagacity is designed to operate with the Apache and MySQL/MariaDB services listening on localhost (127.0.0.1) ONLY. If you change the configuration files to listen on the network, your vulnerability information will be available to anyone on the network!

NOTE: if you choose not to install the services you will have to open the XAMPP Control Center to start your services from there after each time you reboot.

- You will have to answer a couple prompts. Install dev or production configs and if you want to continue the setup process which will open your default browser
- If you don't say "Y" to the last question of the install.bat script, then visit http://localhost/. This will take you to a wizard for setting up your Sagacity installation. The page will first verify that you have everything installed and enabled before it allows you to continue the setup process. Just follow any requirements it sets up before continuing.
    - Database:
        - Enter the information listed on the page and select if you want to preload CPE, CVE, and STIG data (add'l settings are available by clicking "Adv Web Settings"). Once you click 'Next', Sagacity will get the install process running. It will download the necessary files and get them loaded to the database. You can do these separately if you like by following Appendix B.1 in the User Guide
    - Company: Enter information here that will get updated in the eChecklist files upon exporting.
    - Options: These are personal options for how Sagacity will operate.

Congratulations. You can now proceed to Database Initialization (Windows and Linux), below to finish installing Sagacity.

Linux Installation

Sagacity has been tested on Ubuntu 14.04 LTS and CentOS 7.4, but should be able to run on most major Linux distributions, including RedHat/CentOS and SUSE. These instructions are based on CentOS 7.4, so your specifics might vary a little.

Because Sagacity creates, copies, moves, and reads files, you may run into issues if SELinux is enabled and enforcing. We recommend either putting into "permissive" mode or excluding the web root from its enforcement.

Install the packages listed below from the distribution repository. To perform most of these steps, you will need root access to the client you are working on.

- PHP 7.2
    - PHP MySQLi
    - PHP openssl
    - PHP ZipArchive
- Apache 2+
- MySQL Server 5.7+
- Git

NOTE: As stated in the intro section, there are hardened configuration files available in the "conf" directory. If you wish to use them you will have to update them for use on your specific Linux distribution because they were made for a XAMPP windows install.

Setup Git Repository

To download the code base, you can either "clone" the code base to your local install, then copy it to your server, or "clone" the code base directly to the document root of the web server (e.g. /var/www/html).

To clone the repo you can run the following command:

```
git clone https://github.com/cyberperspectives/sagacity /var/www/html
```

if you want to clone the latest dev release you can add "--branch {branch name}" right after the "clone" argument e.g....

```
git clone --branch v1.3.4 https://github.com/cyberperspectives/sagacity
/var/www/html
```

Install Sagacity

Since the hardened configurations are not copied on Linux you will need to update the system php.ini file to include the following (this is also displayed on the next step):

- request_order “GPCS” OR request_order “GPC”
- include_path “./:/var/www/html:/var/www/html/classes:/var/www/html/inc”
- memory_limit 1G
- upload_max_filesize & post_max_size should match and be a little bigger than the largest file you expect to have to upload (100M is a good starting number)

Visit http://{hostname}/. This will then take you to a setup page that will verify that all required modules and settings are as needed, then take you to a multi-step setup process.

- Database:
    - Enter the information listed on the page and select if you want to preload CPE, CVE, and STIG data (add’l settings are available by clicking “Adv Web Settings”). Once you click ‘Next’, Sagacity will get the install process running. It will download the necessary files and get them loaded to the database. You can do these separately if you like by following Appendix B.1 in the User Guide
- Company: Enter information here that will get updated in the eChecklist files upon exporting.
- Options: These are personal options for how Sagacity will operate.

NOTE: As you step through the process, the script will be updating the Sagacity configuration file, populating the database with databases, tables, routines, and baseline data. You should see occasional popup’s telling you where it is in the process. If you do not see anything take a look at the log files.

Congratulations. You can now proceed to Database Initialization (Windows and Linux), below to finish installing Sagacity.

Database Initialization (Windows and Linux)

If you checked the checkboxes on the Database page of the setup process, you just need to wait until that completes (approx 20-60 mins) before you can begin using Sagacity as it has to load all reference content. You can script updating the reference material as often as you like using your preferred scripting engine and cron tool. Just follow the steps in the User Guide, Appendix B.1

NOTE: The standard file naming convention for Unclassified STIG library compilation files is "U_SRG-STIG_Library_{year}_{mon}.zip" where {year} is a 4-digit year and {mon} = 01, 04, 07, or 10. Visit DISA's IASE website (http://iase.disa.mil/stigs/compilations/Pages/index.aspx) to verify that the current file is in that format. If anything different (e.g. "U_SRG-STIG_Library_2017_01**_v2**.zip", copy the URL and add the -u="{url}" parameter to the update_db.php script (BEFORE all the -- parameters).

NOTE: If you have a Nessus® (Nessus Professional™ or SecurityCenter™) license, you can copy the .nasl files to {document root}/tmp/nessus_plugins BEFORE running the update_db.php script.

- Windows ProfessionalFeed™: `C:\ProgramData\Tenable\Nessus\nessus\plugins`
- Unix ProfessionalFeed™: `/opt/nessus/data/nasl`
- Unix SecurityCenter™: `/opt/sc/data/nasl/`

If you want to use the OpenVAS NASL plugins on Windows, you will need either 7zip or Cygwin to extract the files, or use a separate Unix system to extract them and then copy them back to your host. NOTE: You will have to add '`--nasl`' the the command below

NOTE: If you have access to the FOUO STIG content you can manually download the zip compilation file and put it in the {document_root}/tmp folder also BEFORE running the script. The script will automatically extract the .zip file and include those files while parsing.

You will need to open a terminal/command prompt navigate to the "exec" folder in the document root and then run the following command to download and update your database:

```
php update_db.php --cpe --cve --stig
```

You can also run this script anytime to update your database to the latest content or establish a cron job/scheduled task to automate recurring updates. CPE, CVE, and OpenVAS content is updated as needed. The STIG compilation zip file is updated quarterly. You can also download

any individual STIG xml files and copy them to {tmp}/stigs/xml, then run the following command to import them.

```
php update_db.php --stig --po
```

For offline database updates, run the following on an *online* system:

```
php update_db.php --cpe --cve --stig --do
```

The --do parameter tells the script to download only. This will only download the files to the {document root}/www/tmp directory, then you can copy the downloaded STIG, CPE and CVE files (in tmp, tmp/cpe and tmp/cve, respectively) to your offline system tmp folder and run the command again (with the --po instead of --do) to import the data.

```
php update_db.php --cpe --cve --stig --po
```

The files can also be downloaded directly from the sources:

- https://static.nvd.nist.gov/feeds/xml/cpe/dictionary/official-cpe-dictionary_v2.3.xml
- http://cve.mitre.org/data/downloads/allitems.xml
- http://iase.disa.mil/stigs/compilations/Pages/index.aspx Download the FOUO (CAC required) or non-FOUO STIG Library.
- Copy the three files to the tmp folder on the Sagacity host and run the --do command shown above.

Complete!

You are now ready to visit http://{hostname} to start managing your security assessment results!

1. Go to the Management tab and add a System, Site and ST&E.
2. Go to the Results tab, select your ST&E, and start adding scan results. They will be displayed on the ST&E Operations tab.
3. For more information, see the Sagacity User Guide, located at http://localhost/help.php?topic=all

Troubleshooting

The following sections include solutions to some common installation issues encountered when getting Sagacity up and running.

Windows

XAMPP Apache Won't Start

The most common problem with XAMPP is that Apache will not start after XAMPP is installed. This is usually because Windows is using the port(s) that Apache wants, 80 and 443. To find what web ports are listening on the system:

1. In a command prompt, use `netstat -na | more` to see what ports are in use on the system. Specifically, check 80, 443 and 8080.

In Windows 10, the World Wide Web Publishing Service runs by default on port 80. There are two solutions for this: disable the service or move Sagacity to another port:

1. Open Computer Management --> Services and Applications --> Services
2. Scroll down to World Wide Web Publishing Service. Right-click and Stop.
3. Right click again and select Properties. Change the Startup Type to Manual or Disabled.
4. Try to start Apache.

To move Sagacity to another port:

1. Open C:\xampp\apache\conf\httpd.conf in a text editor.
2. Find the uncommented Listen line: `Listen 80`. Change it to: `Listen 127.0.0.1:8080` or another unused port. NOTE: For security purposes, Sagacity needs to be configured to listen on 127.0.0.1 only. The Sagacity app does not have the security features (yet) to be exposed to the network!
3. Save the httpd.conf file and try to start Apache.
4. Please note that you will have to append the new port to your URLs when using Sagacity: `http://localhost:8080/install.php`

If you have VMWare installed, the vmware-hostd service runs on port 443. Since vmware requires this service, disable SSL in Apache. Because Sagacity is a localhost-only tool, this should not affect system security.

1. Open C:\xampp\apache\conf\httpd.conf in a text editor.
2. Find the line "`Include conf/extra/httpd-ssl.conf`" (around line 539), and comment it out: `# Include conf/extra/httpd-ssl.conf`
3. Save the httpd.conf file and try to start Apache.

Linux

The most common problem on Linux systems is permissions. After downloading Sagacity and before running anything, make sure the permissions are set such that Sagacity can write to the {document_root} directory and all subdirectories. Permissions need to be as follows for the Apache user:

Directories = rwx
Files = rw

If you run into any issues, you can run the following commands to get it working (from the parent directory of the document root):

```
sudo chown -R apache:apache {document root}
sudo find {document root} -type d -exec chmod 755 '{}' \;
sudo find {document root} -type f -exec chmod 644 '{}' \;
```

Also, if you manually run scripts, you may need to run in a sudo context so that the Apache user owns the files. `` `sudo -u apache {script}` ``