tracesecurity
GRC Simplified...Finally

TraceCSO Vulnerability Scanner Installation Guide

6300 Corporate Blvd, Suite 200 | Baton Rouge, LA 70809 | Phone (225) 612-2121 | www.tracesecurity.com

Table of Contents

MINIMUM REQUIREMENTS

IMPORTANT

The TraceCSO Vulnerability Scanner is a virtual machine, and therefore requires hypervisor software to operate. Your chosen hypervisor will determine which version of the scanner you need to download.

INSTALLATION ON A TYPE 1 HYPERVISOR

If you are installing the scanner on a Type 1 Hypervisor (such as **VMware ESXi** or **Microsoft Hyper-V**), the minimum requirements are as follows:

Minimum Requirements for Installation on Type 1 Hypervisors	
Virtual Processors:	2 Cores
Virtual Memory (vRAM):	4 GB
Host Available Disk Space:	50 GB
Host System Processors:	4 Cores or More
Host System Memory (RAM):	8 GB or more

INSTALLATION ON A TYPE 2 HYPERVISOR

If you are installing the scanner on a Type 2 Hypervisor (such as **Oracle VirtualBox**, **VMware Workstation**, or **VMware Workstation Player**), the minimum requirements are as follows:

Minimum Requirements for Installation on Type 2 Hypervisors	
Virtual Processors:	2 Cores
Virtual Memory (vRAM):	4 GB
Host Available Disk Space:	50 GB
Host System Processors:	2 Cores
Host System Memory (RAM):	8 GB
Host Operating System:	Refer to your hypervisor software's support documentation for a list of supported host operating systems

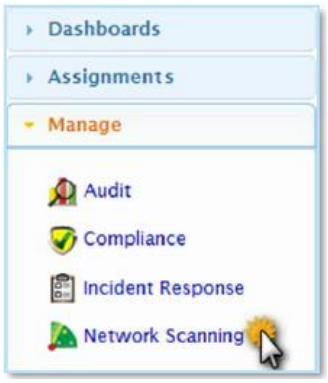
Note: *For Type 2 Hypervisor installations, the host must be a physical machine. We* ***do not recommend*** *using a domain controller as the host, and all power saving options on the host system must be* ***disabled****. Additionally, the scanner* ***does not*** *run as a service, so if the host is powered off in any way (i.e., if it shuts down due to inactivity, reboots for patches, or is manually shut down or rebooted), the scanner must be manually restarted.*

INSTALLING THE SCANNER

CONFIRM HYPERVISOR SOFTWARE IS INSTALLED

The Vulnerability Scanner is a virtual machine that, when installed and activated, links to your CSO account and populates it with your scan results. Because the scanner is a virtual machine, it can only be installed and activated properly on a computer with active hypervisor software. The scanner cannot be installed if you do not have this software.

DOWNLOAD THE SCANNER



Log into TraceCSO (https://cso.tracesecurity.com) and click **Manage** and then **Network Scanning** in the navigation menu on the left side of the screen to access the Network Scanning functional area.

Locate the **Install Scanners** heading in the functional area and then the "Add scanners to find vulnerability and configuration information" subheading. Click the **Add** button to the right of this subheading, and a **Create Scanner** wizard will open.

Step 1 of the wizard requires you to specify a name for the scanner and also provides you with the option to enter a brief description. Once you have entered the scanner's name, click **Save and Next**.

Step 2 of the wizard provides you with the download options for the scanner as well as the registration codes required for activation. You will need to download the version of the scanner appropriate for your chosen hypervisor software and also make note of the Regcodes located at the bottom of the window for later (these are case-sensitive and the hyphens must also be included). Since the scanner files are quite large (1.7 – 1.8 GB), the download will take some time. It may be best to wait until after business hours to begin the download in order to avoid potential connection issues.

To begin the download, simply click on the appropriate **Download ThreatScanner OVA** button.

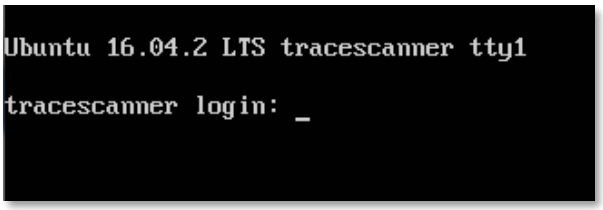
IMPORT/DEPLOY THE SCANNER

Once the download is complete, the process that immediately follows will vary depending on your chosen hypervisor, so this guide does not cover the specifics. You will need to follow your particular hypervisor software's instructions for importing/opening/deploying the scanner.

CONFIGURING THE SCANNER

Once the scanner has been imported/deployed in your hypervisor, first verify that it has been allocated sufficient resources (please refer to page 3 of this guide for the minimum virtual resource requirements) and then start the scanner to begin the boot process. Upon completion of the boot process, you will be prompted for login credentials.

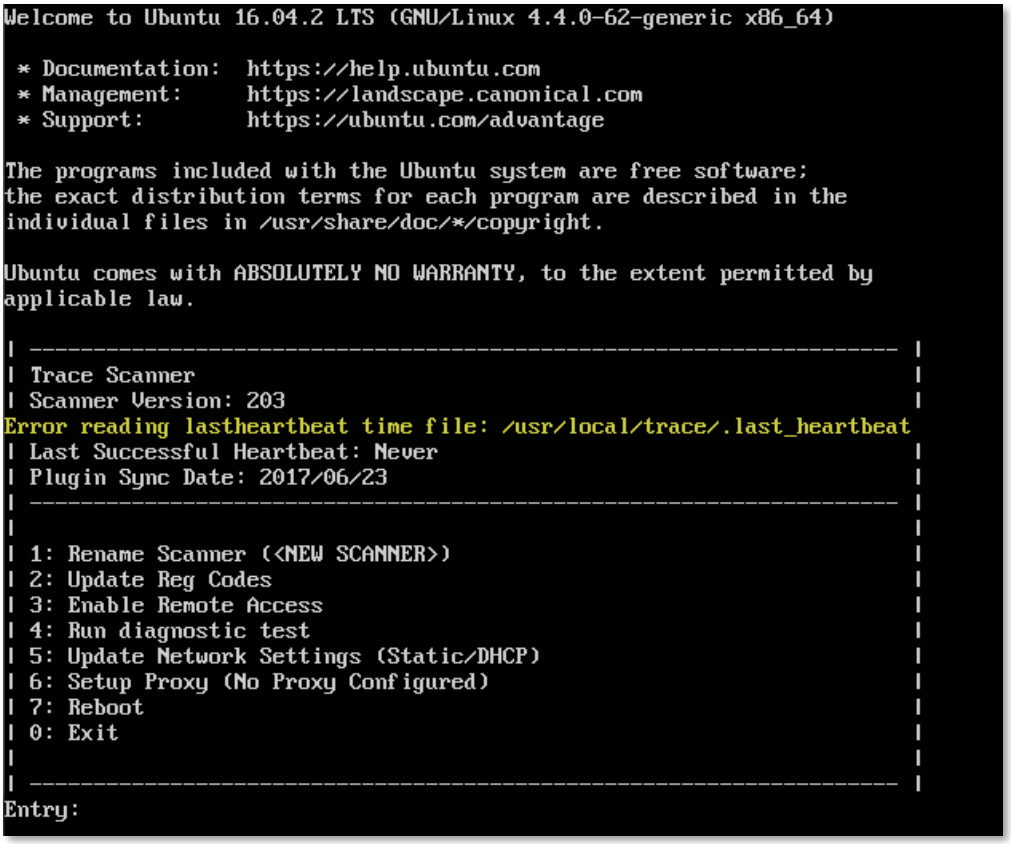
Enter the following credentials to access the scanner Main Menu:



Login: trace
Password: s3curity

Note: *The cursor will not move or input any placeholder characters when entering the password.*

The scanner Main Menu will initially display a heartbeat-related error. This is normal and will be replaced with the current date/time (listed in UTC) upon successful activation.



IMPORTANT

The scanner must have access to certain external resources in order to function:

- CSO Web application at **cso.tracesecurity.com over port 443** (SSL). All communication for scanning and web management occurs over SSL to this domain name. If there is a firewall separating the scanner from the Internet, outbound access must be allowed to this domain name over port 443.

- Signature updates occur using rsync and require access to **50.57.200.86 over port 873**.

- Remote Access for Support troubleshooting or internal service testing requires access to **18.216.164.53 over port 22**.

You will also need to ensure that the IP address assigned to the scanner is excluded from any web-content filtering systems (such as Websense) and/or any intrusion detection/prevention systems (such as SecureWorks). If these systems are maintained by a third-party vendor, please feel free to contact TraceSecurity Support with any questions you or they may have regarding scanner implementation.

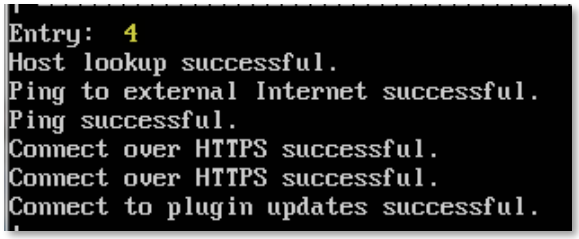
Lastly, the IP address assigned to the scanner must be whitelisted in any anti-virus/endpoint protection software in use. Failing to perform this step may result in excessively long scan times.

DHCP CONFIGURATION

The scanner is configured to use DHCP by default. This means it will automatically obtain an available IP Address along with the appropriate Net Mask, Default Gateway, and DNS Server.

If a proxy is being used, select '**Setup Proxy (No Proxy Configured)**' from the menu by typing the corresponding option number and pressing Enter. When prompted, enter the proxy information in the specified format and press Enter.

Select '**Run diagnostic test**' from the menu by typing in the corresponding option number and pressing Enter (please note that this test may take a few moments to complete).



If all diagnostic tests are successful, proceed to the section of this document titled 'ACTIVATING THE SCANNER'.

If all diagnostic tests fail, contact TraceSecurity Support at tracesupport@tracesecurity.com or 877-798-7223.

If the first diagnostic test is successful but either of the "Connect over HTTPS" tests fail:

- Ensure that the scanner is able to access the CSO Web application at **cso.tracesecurity.com over port 443** (SSL). If there is a firewall separating the scanner from the Internet, outbound access must be allowed to this domain name over port 443.

- Ensure that the scanner is excluded from any web-content filtering system (such as Websense) and/or any intrusion detection/prevention system (such as SecureWorks).

If the first diagnostic test is successful but the final diagnostic test for plugin updates fails:

- Ensure that the scanner is able to communicate with **50.57.200.86 over port 873**. This communication is required for the scanner to obtain signature updates.

STATIC IP CONFIGURATION

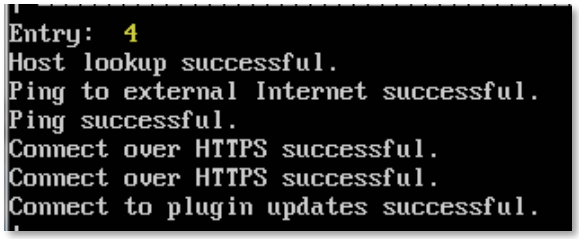
If you wish to manually assign a static IP to the scanner, select '**Update Network Settings (Static/DHCP)**' from the menu by typing the corresponding option number and pressing Enter.

Follow the prompts to enter the necessary configuration information, including IP Address, Net Mask, Default Gateway, and DNS Server.

Note: *The IP Address will need to be an unused IP address on your internal network, as this will be the IP address for the scanner. Entering an IP address that is already in use will cause a conflict, and the scanner will not function properly.*

If a proxy is being used, select '**Setup Proxy (No Proxy Configured)**' from the menu by typing the corresponding option number and pressing Enter. When prompted, enter the proxy information in the specified format and press Enter.

Select '**Run diagnostic test**' from the menu by typing in the corresponding option number and pressing Enter (please note that this test may take a few moments to complete).



If all diagnostic tests are successful, proceed to the next section of this document.

If all diagnostic tests fail, select the '**Reboot**' option from the menu by typing the corresponding option number and pressing Enter. After the scanner reboots, enter the login credentials when prompted, then select '**Run diagnostic test**' again. If all diagnostic tests fail, contact TraceSecurity Support at tracesupport@tracesecurity.com or 877-798-7223.

If the first diagnostic test is successful but either of the "Connect over HTTPS" tests fail:

- Ensure that the scanner is able to access the CSO Web application at **cso.tracesecurity.com over port 443** (SSL). If there is a firewall separating the scanner from the Internet, outbound access must be allowed to this domain name over port 443.
- Ensure that the scanner is excluded from any web-content filtering system (such as Websense) and/or any intrusion detection/prevention system (such as SecureWorks).

If the first diagnostic test is successful but the final diagnostic test for plugin updates fails:

- Ensure that the scanner is able to communicate with **50.57.200.86 over port 873**. This communication is required for the scanner to obtain signature updates.

ACTIVATING THE SCANNER

Once any necessary configuration information has been entered into the scanner and its access to the TraceSecurity Network has been allowed/confirmed, it will need to be activated by entering the previously-obtained registration codes.

Select '**Update Reg Codes**' from the scanner menu by typing the corresponding option number and pressing Enter. When prompted, type each registration code exactly as it appears in CSO, then press Enter (remember that the regcodes are case-sensitive and the hyphens must also be typed). If registration is successful, no errors will be generated and the main menu will re-display.

To confirm successful activation, again select '**Run diagnostic test**' from the menu by typing in the corresponding option number and pressing Enter. Once the test has completed and the main menu again re-displays, the **Last Successful Heartbeat** (located above the numbered menu options) should reflect the current date/time (please note that the time is listed in UTC).

The scanner should remain online and idle (i.e., without running any scans) for 24 hours after successful activation so that it can install any necessary updates and so that the plugin sync can occur. Please note that if any scans are run before the plugin sync has successfully occurred, those scans may either not return any results or the results may not include the latest vulnerabilities.

Please also note that the scanner may automatically reboot during the update process, and this is not cause for concern.