PVS 5.0 User Guide

Last Updated: June 14, 2017
# Table of Contents

- **PVS 5.0 User Guide** ........................................................................................................ 1
- **Welcome to PVS** ........................................................................................................... 1
- **Getting Started with PVS** .............................................................................................. 2
  - PVS Workflow ........................................................................................................... 3
  - Hardware Requirements ............................................................................................... 4
  - Software Requirements ............................................................................................... 6
  - Licensing Requirements ............................................................................................. 8
- **Install, Upgrade, Configure, and Remove PVS** .............................................................. 9
  - Download PVS .......................................................................................................... 10
  - Install PVS ................................................................................................................ 11
    - Install PVS on Linux ................................................................................................. 12
    - Install PVS on Windows ........................................................................................ 14
    - Install PVS on macOS ............................................................................................ 21
  - Upgrade PVS ............................................................................................................... 24
    - Upgrade PVS on Linux ............................................................................................ 25
    - Upgrade PVS on Windows ...................................................................................... 26
    - Upgrade PVS on macOS ......................................................................................... 27
  - Set up PVS .................................................................................................................. 28
  - Configure PVS ........................................................................................................... 29
  - Register PVS Offline via the PVS Interface ................................................................ 31
  - Register PVS Offline via the CLI .............................................................................. 33
  - Configure High Performance Mode ........................................................................... 35
Remove PVS .............................................................................................................. 36
Remove PVS from Linux ............................................................................................... 37
Remove PVS from Windows ......................................................................................... 38
Remove PVS from macOS ............................................................................................ 39

PVS Features .............................................................................................................. 40

PVS Navigation ........................................................................................................... 41
Monitoring Page .......................................................................................................... 46
Dashboards Section .................................................................................................... 50
Hosts Section ............................................................................................................ 53
Vulnerabilities Section ................................................................................................ 58
Applications Section .................................................................................................. 59
Operating Systems Section ......................................................................................... 60
Connections Section .................................................................................................. 61
Mobile Devices Section ............................................................................................... 62

Results Page ............................................................................................................... 63
Users Page ................................................................................................................... 64

Configuration Page ................................................................................................... 65

PVS Settings Section .................................................................................................. 66

Feed Settings Section ................................................................................................. 75

Cloud Settings Section ............................................................................................... 76

Web Proxy Settings Section ....................................................................................... 77

Chart Settings Section ............................................................................................... 78

Email Settings Section ............................................................................................... 79

Plugin Settings Section .............................................................................................. 81

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
## Nessus Scanner Settings Section
---

### How To
---

**Monitoring Page** ................................................................. 86

**Rearrange Charts** ............................................................... 87

**Set a Range for the Dashboards Section** ................................. 88

**Refresh a Chart** ................................................................. 89

**Remove a Chart from a Dashboard** ........................................... 90

**Filter Results** ....................................................................... 91

**Export Results** ................................................................. 92

**Launch a Nessus Scan** .......................................................... 93

**Delete a Vulnerability** .......................................................... 94

**Results Page** ........................................................................ 95

**Upload a Report** ................................................................. 96

**Upload a Pcap** ..................................................................... 97

**Filter Results** ....................................................................... 98

**Users Page** ........................................................................... 99

**Create a New User** ............................................................... 100

**Modify a User Account** ......................................................... 101

**Reset a Locked Account** ....................................................... 102

**Delete a User** ....................................................................... 103

**Configuration Page** ............................................................. 104

**Configure the Performance Mode** ........................................... 105

**Download New Vulnerability Plugins** .................................... 107

**Create a Custom Chart** .......................................................... 108
Welcome to PVS

This user guide describes the Tenable Network Security PVS 5.0 (Patent 7,761,918 B2) architecture, installation, operation, integration with SecurityCenter CV and Tenable.io, and export of data to third parties. Please email any comments and suggestions to support@tenable.com.

Tip: If you are new to PVS, see the PVS Workflow.

Passive vulnerability scanning is the process of monitoring network traffic at the packet layer to determine topology, clients, applications, and related security issues. PVS can also profile traffic and detect compromised systems.

PVS can:

- Detect when systems are compromised with application intrusion detection.
- Highlight all interactive and encrypted network sessions.
- Detect when new hosts are added to a network.
- Track which systems are communicating and on which ports.
- Detect which ports are served and which are browsed by each system.
- Detect the number of hops to each monitored host.

Tip: For security purposes, Tenable does not recommend configuring PVS as internet facing software.
Getting Started with PVS

To ensure a streamlined installation process, it is important to ensure the appropriate hardware, software, and licensing requirements are in place prior to installation.

- Hardware Requirements
- Software Requirements
- Licensing Requirements
PVS Workflow

1. Ensure that your setup meets the minimum system requirements:
   - **Hardware requirements**
   - **Software requirements**

2. Obtain the proper [license or Activation Code for PVS](#) for your configuration.

3. Follow the installation steps depending on your operating system:
   - **Linux**
   - **Windows**
   - **macOS**

4. Perform the [initial configuration steps](#) for PVS in the web interface.

   After configuration, PVS begins scanning immediately.

   **Note:** If you are registering PVS offline or running PVS in [High Performance mode](#), there are additional configuration steps to follow.

5. [Create users in PVS](#) and set [administrative privileges](#) as necessary.

6. You can view live scan results in dashboards on the [Monitoring page](#) and historical data in snapshots and reports on the [Results page](#).
Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for PVS deployments include raw network speed, the size of the network being monitored, and the configuration of PVS.

The following chart outlines some basic hardware requirements for operating PVS:

<table>
<thead>
<tr>
<th>Version</th>
<th>Installation scenario</th>
<th>RAM</th>
<th>Processor</th>
<th>Hard disk requirements</th>
<th>Hard disk space</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Versions</td>
<td>PVS managing up to 50,000 hosts **</td>
<td>2 GB RAM (4 GB RAM recommended)</td>
<td>1 dual-core 2GHz CPU</td>
<td>Processor requirements increase with greater throughput and higher number of network interfaces. Memory requirements increase for networks with more hosts. The requirements for both of these components are affected by configurable options, such as setting a long report lifetime.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PVS managing more than 50,000 hosts **</td>
<td>Memory: 4 GB RAM (8 GB RAM recommended)</td>
<td>1 dual-core 3 GHz CPU (2 dual-core recommended)</td>
<td>Disk space requirements for PVS vary depending on the amount of data and length of time the data is stored on the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PVS running in High Performance mode</td>
<td>16 GB RAM (HugePages memory: 2 GB)</td>
<td>10 CPUs with hyper-threading enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The ability to monitor a given number of hosts depends on the bandwidth, memory, and processing power available to the system running PVS.
**For optimal data collection, PVS must be connected to the network segment via a hub, spanned port, or network tap to have a full, continuous view of the network traffic.**

**Note:** Please research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers.

### High Performance Mode

To run PVS in High Performance mode, a minimum of two of the following types of Intel NICs are required; one as a management interface and at least one as a monitoring interface:

- e1000 (82540, 82545, 82546)
- e1000e (82571, 82574, 82583, ICH8.ICH10, PCH.PCH2)
- igb (82575, 82576, 82580, I210, I211, I350, I354, DH89xx)
- ixgbe (82598, 82599, X540, X550)
- i40e (X710, XL710)
# Software Requirements

The Passive Vulnerability Scanner is available for the following platforms:

<table>
<thead>
<tr>
<th>Version</th>
<th>Software Requirements</th>
</tr>
</thead>
</table>
| 5.1+    | - Red Hat Linux ES 5 / CentOS 5 64-bit  
         | - Red Hat Linux ES 6 / CentOS 6 64-bit  
         | - Red Hat Linux ES 7 / CentOS 7 64-bit  
         | - Mac OS X 10.8 and 10.9 64-bit  
         | High Performance mode only available on:  
         | - CentOS 6.x 64-bit  
         | - CentOS 7.x 64-bit  
         | - Red Hat ES 6.6+ 64-bit  
         | - Red Hat ES 7.x 64-bit  
         | - Linux kernel version 2.6.34. |

<table>
<thead>
<tr>
<th>Previous Versions</th>
<th></th>
</tr>
</thead>
</table>
| 4.4.x to 5.0      | - Red Hat Linux ES 5 / CentOS 5 64-bit  
         | - Red Hat Linux ES 6 / CentOS 6 64-bit  
         | - Red Hat Linux ES 7 / CentOS 7 64-bit  
         | - Mac OS X 10.8 and 10.9 64-bit  
         | High Performance mode only available on:  
         | - CentOS 6.x 64-bit  
         | - CentOS 7.x 64-bit  
         | - Red Hat ES 6.6+ 64-bit  
         | - Red Hat ES 7.x 64-bit  

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
You can use ERSPAN to mirror traffic from one or more source ports on a virtual switch, physical switch, or router and send the traffic to a destination IP host running PVS. The following ERSPAN virtual environments are supported for PVS:

- VMware ERSPAN (Transparent Ethernet Bridging)
- Cisco ERSPAN (ERSPAN Type II)

**Tip:** Refer to the [Configuring Virtual Switches for Use with PVS](#) document for details on configuring your virtual environment.

### High Performance Mode

To run PVS in High Performance mode, you must enable HugePages support. HugePages is a performance feature of the Linux kernel and is necessary for the large memory pool allocation used for packet buffers. If your Linux kernel does not have HugePages configured at all, PVS automatically configures HugePages per the appropriate settings. Otherwise, if your Linux kernel has defined HugePages, refer to the Configuring HugePages instructions.

The following virtual environments are supported for running PVS in High Performance mode:

- VMware ESXi/ESX 5.5
- VMXNET3 network adapter
Licensing Requirements

PVS Subscription

A PVS subscription Activation Code is available that enables PVS to operate in Standalone mode. This mode enables PVS results to be viewed from an HTML interface enabled on the PVS server.

Activation Code

To obtain a Trial Activation Code for PVS, contact sales@tenable.com. Trial Activation Codes are handled the same way by PVS as full Activation Codes, except that Trial Activation Codes allow monitoring for only 30 days. During a trial of PVS, all features are available.

SecurityCenter Continuous View

SecurityCenter Continuous View includes PVS as part of a bundled license package with SecurityCenter. This license allows an unlimited number of PVS deployments to monitor an unlimited number of networks. SecurityCenter CV's IP view is constrained by the license purchased with it.

Tenable.io

Tenable.io pushes plugins down to PVS. The number of PVS deployments is determined by your Tenable.io licensing.

High Performance Mode

PVS running in High Performance Mode can be licensed in Standalone mode or bundled with SecurityCenter CV.
Install, Upgrade, Configure, and Remove PVS

This section includes the following instructions on machines running Linux, Windows, and macOS:

- [Download and Install PVS](#)
- [Upgrade PVS](#)
- [Configure PVS](#)
- [Remove PVS](#)
Download PVS

Steps

1. Access the [Tenable Support Portal](#).

2. On the left side of the page, in the **Main Menu** section, click **Downloads**.

3. Click **Passive Vulnerability Scanner** and select the correct version for your operating system.

   After you accept the license agreement, a download begins.

   **Note:** To ensure binary compatibility, ensure you download the correct build for your operating environment.

4. Confirm the integrity of the installation package by comparing the downloaded MD5 checksum with the one listed in the product [release notes](#).
Install PVS

This section describes how to perform an initial installation of PVS on the following platforms:

- **Linux**
- **Windows**
- **macOS**
Install PVS on Linux

Before You Begin

These steps assume you have [downloaded PVS](http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html) and are running all commands with root privileges. To ensure audit record time stamp consistency between PVS and SecurityCenter CV, ensure the underlying OS makes use of NTP as described in the following document:


The software license agreement for PVS is located in the directory `/opt/pvs/docs`. It is also available online in the following location:

http://static.tenable.com/prod_docs/Master_Software_License_and_Services_Agreement.pdf

Tip: Ensure that organizational and OS firewall rules permit access to port 8835 on the PVS server.

Steps


```
# rpm -ivh pvs-5.x.x-esx.x86_64.rpm
Preparing... #............................................................ [100%]
1:pvs #............................................................ [100%]
[*] PVS installation completed.
```

The installation creates the directory `/opt/pvs`, which initially contains the PVS software, default plugins, and directory structure.

2. Start PVS for Red Hat and CentOS systems using the following command:

```
# service pvs start
```

front end to log in for the first time.

Refer to Configure PVS to complete the initial login.
Install PVS on Windows

Before You Begin

These steps assume you have downloaded PVS and are running all programs as a local user with administrative privileges. To do so, when UAC is enabled, right-click on the installer program and select Run as Administrator.

Additionally, you must ensure the latest version of Microsoft Visual C++ 2010 Redistributable Package is installed for your 64-bit platform and architecture. Be sure to stop any other programs on your system that are utilizing WinPcap.

Steps

1. Double-click the .exe file downloaded from the Tenable Support Portal. The specific filename varies depending on your version.

   The InstallShield Wizard launches, which walks you through the installation process and required configuration steps.
2. Click the **Next** button.

The **License Agreement** screen appears. You must agree to the terms to continue the installation process and use PVS.

**Tip:** You can copy the text of the agreement into a separate document for reference, or you can click the **Print** button to print the agreement directly from this screen.
3. Click the **Next** button.

   The **Customer Information** screen appears. The **User Name** and **Company Name** fields are used to customize the installation, but are not related to any configuration options (e.g., for interfacing with SecurityCenter CV).
4. Click the **Next** button.

The **Choose Program Location** screen appears, where you can verify the location in which the PVS binaries are installed. Click the **Change** button to specify a custom path.
5. Click the **Next** button.

The **Choose Data Location** screen appears, where you can verify the location in which user data generated by PVS will be stored. Click the **Change** button to specify a custom path.

**Tip:** If you are connecting PVS to SecurityCenter CV, altering the data path will make SecurityCenter CV unable to retrieve reports.
6. Click the **Next** button.

The **Ready to Install the Program** screen appears, where you can review and edit the information supplied on previous screens.
7. Click the **Install** button.

The **Setup Status** screen appears. If the most recent version of WinPcap is already installed on the system, the PVS installation process asks if you want to force or cancel installation of WinPcap. If it does not detect WinPcap, or detects and older version, a second installer launches to install or upgrade the software.

**Tip:** Use the provided version of WinPcap or newer. PVS has been designed and tested using the supplied version of WinPcap.

8. **Start PVS**.
Install PVS on macOS

Before You Begin

These steps assume you have downloaded PVS and are running all programs as a root user or with equivalent privileges.

Steps

1. Double-click the .dmg file downloaded from the Tenable Support Portal to mount the disk image PVS Install. The specific filename varies depending on your version.

2. Double-click the Install PVS.pkg file.

   The Install Tenable PVS window appears, which walks you through the installation process and any required configuration steps.

3. Click the Continue button.

   The Software License Agreement screen appears. You must agree to the terms to continue the installation process and use PVS.
4. Click **Install** to begin the installation.

A window appears, asking for authentication permission to install the software.

5. Click the **Install Software** button.

A window appears, requesting permission to allow PVS to accept incoming network connections. If this option is denied, PVS is installed but functionality is severely reduced.

Immediately after the successful installation of PVS, the Installer automatically launches the Safari web browser to allow configuration of the PVS environment. When the identity dialog box appears, click **Continue**.

Tip: Once the installation process is complete, eject the PVS install volume.

Start and Stop PVS for macOS
1. Access the **System Preferences** and select **PVS.Preferences**.

   The **PVS.Preferences** window appears.

2. Select the **Start PVS** or **Stop PVS** button as needed.

   **Tip:** You can also issue a [command from terminal](#) to manually start or stop PVS.
Upgrade PVS

This section describes how to upgrade an existing PVS instance on the following platforms:

- Linux
- Windows
- macOS
Upgrade PVS on Linux

Before You Begin

These steps assume you have backed up your custom SSL certificates. It is also assumed that you are running all commands with root privileges.

Additionally, if you have used a PVS RPM to install PVS previously, an upgrade retains configuration settings. You must transfer the PVS RPM package to the system on which it is being installed. Confirm the integrity of the installation package by comparing the download MD5 checksum with the one listed in the product release notes.

Steps

1. Stop PVS with the following command:

   ```
   # service pvs stop
   ```

2. Install the PVS .rpm file downloaded from the Tenable Support Portal with the following command. Note that the specific filename varies, depending on your version:

   ```
   # rpm -Uvh pvs-5.x.x-esx.x86_64.rpm
   Preparing... #################################################### [100%]
   1:pvs ######################################################## [100%]
   [*] PVS installation completed.
   #
   ```

3. Once the upgrade is complete, start PVS with the following command:

   ```
   # service pvs start
   ```

4. Navigate to https://<ip address or hostname>:8835, which displays the PVS web frontend to log in.

   **Tip:** Ensure that organizational firewall rules permit access to port 8835 on the PVS server.
Upgrade PVS on Windows

Before You Begin

These steps assume you have backed up your custom SSL certificates. It is also assumed that you are running all programs as a local user with administrative privileges. To do so, when UAC is enabled, right-click on the installer program and select Run as Administrator.

Additionally, you must ensure the latest version of the Microsoft Visual C++ 2010 Redistributable Package is installed for your 64-bit platform and architecture. Be sure to stop any other programs on your system that are utilizing WinPcap.

Steps

1. Stop the Tenable PVS Proxy Service from the Windows Services control panel.

2. Double-click the .exe file downloaded from the Tenable Support Portal. Note that the specific filename varies, depending on your platform and/or version.

   The InstallShield Wizard launches and begins the upgrade process.

3. Click the Next button.

   The automated upgrade process begins.

   **Note:** If the version of WinPcap is not at the appropriate level during the upgrade process, an upgrade window appears and begins the process of upgrading WinPcap. Failure to install the recommended version of WinPcap may result in errors with PVS monitoring.

4. When the upgrade is complete, start PVS.

5. Navigate to https://<ip address or hostname>:8835 to display the PVS web frontend to log in.

   **Tip:** Ensure that organizational firewall rules permit access to port 8835 on the PVS server.
Upgrade PVS on macOS

Before You Begin

These steps assume that you have backed up your custom SSL certificates and you are running all programs with root privileges.

Steps

1. **Stop PVS.**

2. Double-click the .dmg file downloaded from the [Tenable Support Portal](#) to mount the disk image **PVS Install**. The specific filename varies depending on your version.

3. Double-click the **Install PVS.pkg** file.

   The Install Tenable PVS window appears, which walks you through the upgrade process and any required configuration steps.

4. Click the **Continue** button.

   The Software License Agreement screen appears. You must agree to the terms to continue the installation process and use PVS.

   **Tip:** You can copy the text of the agreement into a separate document for reference, or you can click the Print button to print the agreement directly from this screen.

5. Click the **Install** button.

   A window appears asking for authentication permission to install the software.

6. Click the **Install Software** button.

   A window appears requesting permission to allow PVS to accept incoming network connections. If this option is denied, PVS is installed but functionality is severely reduced.

7. Click the **Allow** button.

   After the upgrade is complete, your default web browser appears, displaying the PVS web frontend to log in. When the web browser appears, you can eject the PVS install volume.
Set up PVS

PVS configuration follows the same steps for all operating systems. This section provides instructions for the following:

- Configure PVS
- Register PVS Offline via the PVS Interface
- Register PVS Offline via the CLI
- Configure High Performance Mode
Configure PVS

Steps

1. In a web browser, navigate to https://<ip address or hostname>:8835. The default username and password are both admin. Enter these credentials and click the Sign In To Continue button.

2. The Change Default Password screen of the Quick Setup window appears, where you can change the default password. The new password must meet the following minimum requirements:
   - Minimum 5 characters long
   - One capital letter
   - One lowercase letter
   - One numeric digit
   - One special character from the following list: !@#$%^&* ()

3. Click the Next Step button.

   The Set Activation Code screen appears.

4. In the Activation Code box, enter the appropriate text based on your setup:
   - If PVS is acting as a standalone device, enter an Activation Code.
   - If PVS is managed by Tenable.io, enter the text Cloud.

     Four configuration options appear: Cloud Host, Cloud Port, Cloud Key, and PVS Name. Refer to the Cloud Settings section for more information.

     - If PVS is managed by SecurityCenter CV, enter the text SecurityCenter.

     -or-

     If PVS is registered offline, select the Register Offline check box and follow the Register PVS Offline instructions.

5. Click the Next Step button.

   The Monitoring Configuration screen appears.
- The **Monitored Network Interfaces** box displays those monitored interfaces PVS has identified. You can select one or more of the defined interfaces. The caret icon displays additional information about each interface.

- The **Monitored Network IP Addresses and Ranges** box displays the IP address ranges PVS monitors.

- The **Excluded Network IP Addresses and Ranges** box displays the IP address ranges PVS does not monitor.

  The **Monitored Network IP Addresses and Ranges** and **Excluded Network IP Addresses and Ranges** boxes accept both IPv4 and IPv6 CIDR address definitions. When multiple addresses are used, separate the entries using commas or new lines.

6. Click the **Finish** button.

   The **Monitoring** page appears. Once PVS has started monitoring traffic, the page displays various high-level charts about the vulnerabilities, assets, connections, and bandwidth usage that PVS has detected, as well as real-time events that PVS has triggered.
Register PVS Offline via the PVS Interface

Steps

1. In Step 4 of the Initial Configuration, on the Quick Setup window, select the Register Offline check box.

A challenge code and the Activation Key box appear.

2. Copy the challenge code, and in a web browser, navigate to https://plugins.nessus.org/v2/offline-pvs.php.

3. In the appropriate boxes, paste your challenge code and enter the Activation Code you received previously from Tenable. Click the Submit button.

The page generates a URL to download the PVS plugins tarball. Save this URL, as it will be used every time you update your plugins. In addition, a license key appears.

4. Copy the license key, navigate to the PVS interface, and paste the license key into the Activation Key box on the Quick Setup window.

5. Click the Next Step button, and then continue with Step 5 of the Initial Configuration.
instructions.

**Note:** After configuring PVS, upload the plugins tarball in the **Offline Update** area of the **Feed Settings** section.
Register PVS Offline via the CLI

If your PVS installation cannot reach the Internet directly, use the following procedure to register and update plugins:

On the system running PVS, type the following command:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command to Run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Linux / CentOS</td>
<td><code>#/opt/pvs/bin/pvs --challenge</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\Program Files\Tenable\PVS\pvs --challenge</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code>#/Library/PVS/bin/pvs --challenge</code></td>
</tr>
</tbody>
</table>

This produces a challenge code similar to the following:

```
569ccd9ac72ab3a62a3115a945ef8e710c0d73b8
```

Go to [https://plugins.nessus.org/v2/offline-pvs.php](https://plugins.nessus.org/v2/offline-pvs.php) and paste the challenge code as well as the Activation Code you received previously from Tenable into the appropriate text boxes. This produces a URL that gives you direct access to the PVS plugins. Save this URL, as it will be used every time you update your plugins. In addition, a license key and the associated `pvs.license` file are produced. Copy this file to the host running PVS in the appropriate directory.

Once the `pvs.license` file is copied, run the `pvs --register-offline` command to install the file:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Linux / CentOS</td>
<td><code>#/opt/pvs/bin/pvs --register-offline /path/to/pvs.license</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\Program Files\Tenable\PVS\pvs --register-offline &quot;C:\path\to\pvs.license&quot;</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code>#/Library/PVS/bin/pvs --register-offline /path/to/pvs.license</code></td>
</tr>
</tbody>
</table>

The newest plugins can be obtained by navigating to the URL provided in the previous step. Here, you receive a TAR file (e.g., `sc-passive.tar.gz`). Copy the file to PVS and then type the appropriate command for your platform:
<table>
<thead>
<tr>
<th>Platform</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Linux / CentOS</td>
<td><code># /opt/pvs/bin/pvs --update-plugins /path/to/sc-passive.tar.gz</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\Program Files\Tenable\PVS\pvs --update-plugins</code></td>
</tr>
<tr>
<td></td>
<td><code>C:\path\to\sc-passive.tar.gz</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code># /Library/PVS/bin/pvs --update-plugins /path/to/sc-passive.tar.gz</code></td>
</tr>
</tbody>
</table>
Configure High Performance Mode

Before You Begin

The following steps are required to operate PVS in High Performance mode. Alternatively, a user with administrative privileges can enable High Performance mode via the UI.

You must have a High Performance Activation Code in order to run PVS in High Performance mode.

PVS uses multiple cores to process packets received from the monitored interfaces. These cores are known as worker cores, and the default number of worker cores is 8. This number can be changed using the configuration parameter Number Of Worker Cores.

Note: If you set the Number Of Worker Cores parameter to 0, PVS automatically changes the value to the minimum number of worker cores needed to run PVS in High Performance mode.

For example, suppose you have 20 available logical cores. Four of those cores are used by the system for internal processing and the kernel. If you want to use the 16 available cores for PVS, then you may change the value for the parameter Number Of Worker Cores to 16.

Steps

1. Stop PVS with the following command:
   
   `# service pvs stop`

2. Enable High Performance mode with the following command:
   
   `/opt/pvs/bin/pvs --config "Enable High Performance Mode" "1"`

3. Confirm that the management network interface is different from the monitoring network interface that you configured initially.

   Note: If the configured monitored interface has bound IPv4 addresses, you cannot complete the Quick Setup Wizard to configure PVS because no usable NICs appear in the Monitored Network Interfaces list.

4. Start PVS with the following command:

   `# service pvs start`
Remove PVS

The following instructions describe how to remove PVS from the following platforms:

- Linux
- Windows
- macOS
Remove PVS from Linux

Steps

1. Stop PVS with the following command:

   ```
   # service pvs stop
   ```

2. Determine the name of the RPM file with the following command:

   ```
   # rpm -qa | grep pvs
   ```

   The name of the RPM file appears.

3. Remove the PVS RPM with the following command:

   ```
   # rpm -e <RPM name>
   ```

4. Some user-created and user-modified files are not removed with the -e command. Remove any remaining files with the following command:

   ```
   # rm -rf /opt/pvs
   ```

PVS is removed.
Remove PVS from Windows

Steps

1. On the Control Panel, under Programs, click Programs and Features, or Add or Remove Programs, depending on the version of Windows.

2. Select Tenable Passive Vulnerability Scanner and click Change/Remove.

   The InstallShield Wizard appears.

3. Follow the directions in this wizard to completely remove PVS.

4. Select Yes to remove the PVS program and all its files, folders, and features from the system.

   -or-

   Select No to remove only the PVS program. All user-created files and relevant file folders remain on the system.

5. Restart your machine to complete the removal.

6. Follow the same instructions to remove WinPcap.
Remove PVS from macOS

Steps

1. **Stop PVS.**

2. Delete the following directories (including subdirectories) and files with either sudo root or root privileges using the command line:

   - `rm /Library/LaunchDaemons/com.tenablesecurity.pvs*`
   - `rm -r /Library/PVS`
   - `rm -r /Library/PreferencePanes/PVS*`
   - `rm -r /Applications/PVS`

   PVS is removed from your macOS system.
PVS Features

The PVS web interface allows PVS to monitor network traffic and report results without needing SecurityCenter CV or another third party tool to analyze the data. The web interface can be used on web browsers that support HTML5, including the following:

- Microsoft Internet Explorer 9 and later
- Firefox 24 and later
- Google Chrome 30 and later

This section describes the following features in the PVS web interface:

- Navigation
- Monitoring
- Results
- Users
- Configuration
PVS Navigation

The top navigation menu displays two main pages: **Monitoring** and **Results**. All of PVS’s primary analysis tasks can be performed using these two pages. Click a page name to open that page.

On the right side of the top navigation menu, you can see both the icon and the username of the currently logged in user. Click the icon to display the Users and Configuration options, where you can make administrative changes to PVS. Click the username to display a drop-down menu with three options: **Change Password, Help & Support**, and **Sign Out**.

**Note:** The **Users** and **Configuration** pages are available only to users with administrative privileges.
Information

PVS Version 5.0.0

Web Server Version 1.6.0 (Build ID: 201601181)

HTML Client Version 1.6.0 (Build ID: 201601152)

Activation Status Managed by Nessus Cloud

Licensed For High Performance

Feed ID 201602021755

Feed Expiration 15 day(s)

Performance Mode High Performance

Documentation User Guide

Support Link Help & Support
The bell (🔔) icon toggles the **Notification History** box, which displays a list of notifications, successful or unsuccessful login attempts, errors, and system information generated by PVS. The color of the bell changes based on the nature of the notifications in the list. If there are no alerts, or all notifications are information alerts, then the bell is blue ( голубой 🔔). If there are error alerts in the notification list, then the bell is red (красный 🔔). The **Notification History** box displays up to 1,000 alerts. Once the limit is reached, no new alerts can be listed until old ones are cleared.
Notifications can be removed individually by Click the button to the right of the description of each event to remove notifications individually. Alternatively, click the Clear History button in the bottom right corner of the box to delete the entire notification history.

**Note:** Notifications are not preserved between sessions. Unread notifications are removed from the list when the user logs out.
Monitoring Page

The **Monitoring** page provides a centralized view of the vulnerabilities discovered by PVS. On this page, vulnerabilities may be viewed in several categories, including dashboards, hosts, vulnerabilities, applications, operating systems, connections, and mobile devices. The results may also be exported in different formats for use in other programs.

Across all of the viewable methods available on the **Monitoring** page, filter options are available to increase granularity when viewing results. Click the heading of a column to sort items within that section of the **Monitoring** in ascending or descending order.

The **Actions** drop-down menu allows you to export results, delete results, or launch a Nessus scan.

**Note:** After deleting results, you must restart PVS to see the most up-to-date information.

The **Filter <section name>** box allows for quick filtering based on entered text for the **Monitoring** page. To view a list of filterable plugin attributes, click the down arrow for any quick filter text field. Results display based on a match of **Any** or **All** entered fields. The search field contains example hints when empty, but if an incorrect filter value is entered, the field displays a red border.

**Note:** The **Filter <section name>** box is not available in the **Dashboards** section.

**Tip:** For instructions on performing the actions available on the **Monitoring** page, see the related **How To** section of this guide.
Filter Text

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bugtraq ID</td>
<td>Filter the results of discovered vulnerabilities based on their Bugtraq identifiers.</td>
</tr>
<tr>
<td>CPE</td>
<td>Filter the results of discovered vulnerabilities based on their CPE identifiers.</td>
</tr>
<tr>
<td>CVE</td>
<td>Filter the results of discovered vulnerabilities based on their CVE identifiers.</td>
</tr>
<tr>
<td>CVSS Base Score</td>
<td>Filter the results of discovered vulnerabilities based on the base CVSS score as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS Temporal Score</td>
<td>Filter the results of discovered vulnerabilities based on the temporal CVSS score as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS Temporal Vector</td>
<td>Filter the results of discovered vulnerabilities based on the CVSS temporal vector as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS Vector</td>
<td>Filter the results of discovered vulnerabilities based on the CVSS vector as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CVSS v3.0 Base Score</td>
<td>Filter the results of discovered vulnerabilities based on the CVSS v3.0 base score as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS v3.0 Temporal Score</td>
<td>Filter the results of discovered vulnerabilities based on the temporal CVSS v3.0 score as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS v3.0 Temporal Vector</td>
<td>Filter the results of discovered vulnerabilities based on the temporal CVSS v3.0 vector as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>CVSS v3.0 Vector</td>
<td>Filter the results of discovered vulnerabilities based on the CVSS v3.0 vector as reported by the vulnerability plugins.</td>
</tr>
<tr>
<td>Host</td>
<td>Filter the results of discovered vulnerabilities based on the discovered IP address of the device.</td>
</tr>
<tr>
<td>IAVA ID</td>
<td>Filter the results of discovered vulnerabilities based on the IAVA IDs of the vulnerabilities.</td>
</tr>
<tr>
<td>IAVB ID</td>
<td>Filter the results of discovered vulnerabilities based on the IAVB IDs of the vulnerabilities.</td>
</tr>
<tr>
<td>IAVT ID</td>
<td>Filter the results of discovered vulnerabilities based on the IAVT IDs of the vulnerabilities.</td>
</tr>
<tr>
<td>OSVDB ID</td>
<td>Filter the results of discovered vulnerabilities based on the discovered OSVDB identifiers.</td>
</tr>
<tr>
<td>Plugin Description</td>
<td>Filter the results of discovered vulnerabilities based on text available in the descriptions of the vulnerabilities.</td>
</tr>
<tr>
<td>Plugin Family</td>
<td>Filter the results of discovered vulnerabilities based on a family of discovered vulnerabilities.</td>
</tr>
<tr>
<td>Plugin ID</td>
<td>Filter the results of discovered vulnerabilities based on the IDs of the plugins that identified the vulnerabilities.</td>
</tr>
<tr>
<td>Plugin Name</td>
<td>Filter the results of discovered vulnerabilities based on text available in the names of the plugins that identified the vulnerabilities.</td>
</tr>
<tr>
<td>Plugin Output</td>
<td>Filter the results of discovered vulnerabilities based on text contained in the output of the plugin that discovered the vulnerability.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>Filter the results of discovered vulnerabilities based on the port the vul-</td>
</tr>
<tr>
<td></td>
<td>nerability was discovered on.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Filter the results of discovered vulnerabilities based on the detected pro-</td>
</tr>
<tr>
<td></td>
<td>tocol: tcp, udp, or icmp.</td>
</tr>
<tr>
<td>STIG Severity</td>
<td>Filter the results of discovered vulnerabilities based on STIG severity level</td>
</tr>
<tr>
<td></td>
<td>in the plugin.</td>
</tr>
<tr>
<td>See Also</td>
<td>Filter the results of discovered vulnerabilities based on the text available</td>
</tr>
<tr>
<td></td>
<td>in the See Also field of the plugin.</td>
</tr>
<tr>
<td>Severity</td>
<td>Filter the results of discovered vulnerabilities based on the identified sev-</td>
</tr>
<tr>
<td></td>
<td>erity.</td>
</tr>
<tr>
<td>Solution</td>
<td>Filter the results of discovered vulnerabilities based on text available in</td>
</tr>
<tr>
<td></td>
<td>the solution section of the plugin.</td>
</tr>
<tr>
<td>Synopsis</td>
<td>Filter the results of discovered vulnerabilities based on text available in</td>
</tr>
<tr>
<td></td>
<td>the synopsis section of the plugin.</td>
</tr>
<tr>
<td>System Type</td>
<td>Filter the results of discovered vulnerabilities based on the system type of</td>
</tr>
<tr>
<td></td>
<td>the device.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Filter the results of discovered vulnerabilities based on the VLAN ID of the</td>
</tr>
<tr>
<td></td>
<td>device.</td>
</tr>
</tbody>
</table>
Dashboards Section

The **Dashboards** section displays the contents of the vulnerability tab in a graphical layout. The default dashboard layout displays the following charts:

- Top 10 Hosts
- Top 10 Vulnerabilities
- Top 5 Applications
- Distribution by Operating System
- Top 10 Talkers
- Top 10 Mobile Devices
- Distribution of Mobile Devices by Operating System
- Top 10 Mobile Devices by Hardware
- Distribution of Mobile Applications by Application
- SCADA Vulnerability Distribution by Severity
- Top 10 SCADA Hosts
- SCADA Host Distribution by Protocol
- SCADA Host Distribution by System Type
- Client Connections
- Network Bandwidth by Byte Count
- Event Trending

Drag-and-drop charts to rearrange them on the dashboard for the duration of your session. The **Client Connections**, **Network Bandwidth by Byte Count**, and **Event Trending** charts cannot be moved.
The following table describes the options available in the **Dashboards** section.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;clicking on the chart&gt;</td>
<td>Opens a details section with more information about the data displayed in a chart.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You cannot click on the Top 10 Mobile Devices by Hardware chart.</td>
</tr>
<tr>
<td>✗ button</td>
<td>Removes the chart from the <strong>Dashboards</strong> section for the duration of your session.</td>
</tr>
<tr>
<td>🔄 button</td>
<td>Refreshes the chart.</td>
</tr>
<tr>
<td>🏐 button</td>
<td>Provides options to filter chart data based on a specified date range.</td>
</tr>
</tbody>
</table>

**Events Dashboard**

Access the **Events** dashboard by clicking on the **Event Trending** chart. Alternatively, access the **Events** dashboard pre-filtered on plugin 17 by clicking on the **Network Bandwidth by Byte Count** chart. The **Events** dashboard displays a graphical representation of the number of maximum viewable real-time events as defined in the **Realtime Events** setting type in the **PVS Settings** section.
The **Event Details** table can be customized by sorting columns, showing or hiding columns, filtering content using the **Filter Events** drop-down menu, or by clicking underlined columns in the table.
Hosts Section

The **Hosts** section of the Monitoring page displays a list of the discovered hosts, the system type of the hosts, and a stacked bar chart. The chart is labeled and color-coded to indicate both the number and severity level of vulnerabilities detected on the host.

Select a host from the list to display the host’s attributes and discovered vulnerabilities. In the drop-down menu at the top of the section, select one of the following options to view relevant information:

**Vulnerabilities**

Vulnerabilities detected on this host appear in descending order of severity. The vulnerabilities list displays the name of each vulnerability, vulnerability family, and the number of vulnerabilities discovered. Select a vulnerability from the list to display vulnerability details including a synopsis, description, solution, plugin information, risk information, reference information, and affected ports and services for the host.
Applications

Applications appear in descending order of severity. The applications list displays the name and number of each application. Select an application from the list to display information about the application observed on this host.
Client Connections

Hosts to which the selected host has connected are grouped by port. The client connections list displays information about connections from the selected host to other hosts, which port(s) were used, and, if known, the services.
Tip: Click on a client connection to display a Connections sidebar that displays Host Details, a Client Connections diagram, and, where applicable, a Recent Sessions table.

Server Connections

Hosts that have connected to the selected host are grouped by port. The server connections list displays information about connections to the selected host from other hosts, which port(s) were used, and, if known, the services.
Tip: Click on a server connection to display a **Connections** sidebar that displays **Host Details**, a **Server Connections** diagram, and, where applicable, a **Recent Sessions** table.
Vulnerabilities Section

The **Vulnerabilities** section of the **Monitoring** page provides a list of the vulnerabilities detected by PVS. Additionally, you can view a vulnerability's plugin family and the number of detected vulnerabilities.
Applications Section

The **Applications** section displays a list of discovered applications. Select an application to display a list of affected hosts. The list includes the name and number of discoveries, the affected port and protocol, the software and version, and the service as available.
Operating Systems Section

The **Operating Systems** section displays a list of discovered operating systems. The summary page lists the severity, operating system name as detected, and the number of discoveries. Select an operating system name from the list to display the severity, the version of the operating system, and service as available.
Connections Section

The Connections section displays information in two tabs:

- The **Client Connections** tab displays a list of hosts. Click on a host to display connections from the selected host to other hosts, the port(s) used, and, if known, the services.

- The **Server Connections** tab displays a list of hosts. Click on a host to display connections to the selected host from other hosts, the port(s) used, and, if known, the services.
Mobile Devices Section

The **Mobile Devices** section displays a list of discovered mobile devices. The summary page displays the IP address, model, operating system, and last seen timestamp for each mobile device within the monitored network range. Select a device name from the list to display the device’s list of vulnerabilities and a list of applications for the mobile device.
The **Results** page contains snapshots of monitored data, results from Pcap files entered manually via the command line or the client GUI, and uploaded PVS reports. The **Monitored Data** snapshots generate regularly based on the **Report Frequency** setting. They are stored until deleted or the **Report Lifetime** setting goes into effect. Select a result grouping to view it using the same analysis tools described in the **Monitoring** section of this user guide. Additionally, to compare two snapshots, check the desired Snapshot results and select the **Diff Snapshots** option from the **Actions** drop-down menu.

**Tip:** For instructions on performing the actions available on the **Results** page, see the related **How To** section of this guide.
Users Page

The **Users** page provides a list of the available users on the PVS server and account configuration options for each. This page is visible only to users with administrative privileges.

**Tip:** For instructions on performing the actions available on the **Users** page, see the related [How To](#) section of this guide.
Configuration Page

The **Configuration** page allows users with administrative privileges to configure PVS for the local environment. There are eight sections available:

- PVS Settings
- Feed Settings
- Cloud Settings
- Web Proxy Settings
- Chart Settings
- Email Settings
- Plugin Settings
- Nessus Scanner Settings

**Tip:** For instructions on performing the actions available on the **Configuration** page, see the related **How To** section of this guide.
PVS Settings Section

The PVS Settings section provides options for configuring the network settings for PVS, including what network(s) are monitored or excluded, how to monitor those networks, and what network interfaces PVS has identified for monitoring. If your PVS is licensed to run in High Performance mode, you can also change the performance mode.
**Note:** The Network Interfaces Settings view only shows network interfaces that don't have IP addresses assigned to them. As a result, if all interfaces have assigned IP addresses, in High Performance mode, the list is empty.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **ACAS Classification** | Support for ACAS banners may be enabled from the command line of the PVS server service using the command `/opt/pvs/bin/pvs --config --add "ACAS Classification" "SECRET"`.  
SECRET may be replaced by UNCLASSIFIED, CONFIDENTIAL, TOP SECRET, or NOFORN. Once enabled, a drop-down menu for the ACAS option appears in the GUI front end.  
Support for ACAS banners may be disabled from the command line of the PVS server using the command `/opt/pvs/bin/pvs --config --delete "ACAS Classification"` from the binary directory on the server. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Banner</strong></td>
<td>A text box in which you can specify a login banner.</td>
</tr>
<tr>
<td><strong>Analysis Modules</strong></td>
<td></td>
</tr>
<tr>
<td>Enable SCADA/ICS Analysis Module</td>
<td>A check box that, when selected, enables the SCADA/ICS Analysis Module. Click the caret button to the left of the setting name to display a list of individual module detections within the module. Click on individual module detections within the list to disable/enable them. Disabling a SCADA/ICS module detection enables the legacy PASL. See <a href="https://example.com">SCADA/ICS Analysis Module</a> for more information.</td>
</tr>
<tr>
<td>Enable Connection Analysis Module</td>
<td>A check box that, when selected, enables the Connection Analysis Module. Click the caret button to the left of the setting name to display a list of individual module detections within the module. Click on individual module detections within the list to disable/enable them. See <a href="https://example.com">Connection Analysis Module</a> for more information.</td>
</tr>
<tr>
<td><strong>DNS Query</strong></td>
<td></td>
</tr>
<tr>
<td>DNS Cache Lifetime Analysis Module</td>
<td>A text box in which you can specify the amount of time PVS retains and stores a given host’s DNS record, in seconds. By default, this option is set to 43200 (12 hours), but can be set to any value between 3600 and 172800 (48 hours).</td>
</tr>
<tr>
<td>DNS Query Time Interval</td>
<td>A text box in which you can specify the delay between sets of DNS queries, in seconds. By default, this option is set to 5, but can be set to any value between 1 and 120.</td>
</tr>
<tr>
<td>DNS Queries per Interval</td>
<td>A text box in which you can specify the maximum number of concurrent DNS requests made at the time of the DNS Query, in seconds. By default, this option is set to 5, but can be set to any value between 0 and 1000. Setting this value to 0 disables this feature and prevent further DNS queries from being made.</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td></td>
</tr>
<tr>
<td>Sessions Cache Size</td>
<td>A text box in which you can specify the size, in megabytes, of the session table. Adjust the session size as needed for the local network. By default, this option is set to 50.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Packet Cache Size</td>
<td>A text box in which you can specify the maximum size, in megabytes, of the cache used to store the contents of the packets collected before processing. By default, this option is set to 128 MB with a maximum size of 512 MB. When the cache is full, any subsequent packets captured are dropped until space in the cache becomes available.</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
</tr>
<tr>
<td>Monitored Network Interfaces</td>
<td>A list of the network device(s) used for sniffing packets. Devices may be selected individually or in multiples. At least one interface must be selected from the list of available devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> High Performance mode does not support e1000 NICs as monitored interfaces on VMs. If you are running PVS on a VM in High Performance mode and select an e1000 monitored interface, PVS automatically reverts to Standard mode.</td>
</tr>
<tr>
<td>Monitored Network IP Addresses and Ranges</td>
<td>A text box in which you can specify the network(s) monitored. The default setting is 0.0.0.0/0, which instructs PVS to monitor all IPv4 addresses. This should be changed to monitor only target networks; otherwise PVS may quickly become overwhelmed. Multiple addresses must be separated by commas. When monitoring VLAN networks, you must use the syntax <code>vlan ipaddress/subnet</code>. Example: 192.168.1.0/24, 2001:DB8::/64, 10.2.3.0/22, vlan 172.16.0.0/16, 192.168.3.123/32</td>
</tr>
<tr>
<td>Excluded Network IP Addresses and Ranges</td>
<td>A text box in which you can specify, in CIDR notation, any network(s) to specifically exclude from PVS monitoring. This option accepts both IPv4 and IPv6 addresses. Multiple addresses must be separated by commas. When excluding VLAN networks, you must use the syntax <code>vlan ipaddress/subnet</code>. If this text box is left blank, no addresses will be excluded. Example: 192.168.1.0/24, 2001:DB8::/64, 10.2.3.0/22, vlan 172.16.0.0/16, 192.168.3.123/32</td>
</tr>
<tr>
<td>Extended Packet Filter</td>
<td>A text box in which you can specify a BPF primitive.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>The net, IP, IPv6, and VLAN primitives are not supported by this feature. Additionally, the protochain primitive is not supported on Windows platforms.</td>
<td></td>
</tr>
<tr>
<td>Click here for further information about the available primitives.</td>
<td></td>
</tr>
<tr>
<td><strong>PVS Proxy</strong></td>
<td></td>
</tr>
<tr>
<td>PVS Restart Attempts</td>
<td>A text box in which you can specify the number of times the PVS proxy attempts to restart the PVS engine in the event the engine stops running. By default, this option is set to 10, but can be set to any value between 1 and 15. Once the restart attempt limit is reached, the proxy stops trying for 30 minutes.</td>
</tr>
<tr>
<td>PVS Restart Interval</td>
<td>A text box in which you can specify the amount of time, in minutes, between PVS restart attempts. By default, this option is set to 10, but can be set to any value between 1 and 3600.</td>
</tr>
<tr>
<td><strong>PVS Web Server</strong></td>
<td></td>
</tr>
<tr>
<td>Enable SSL for Web Server</td>
<td>A check box that, when selected, enables SSL protection for connections to the web server. This check box is selected by default. Clearing the check box is not recommended, as it will allow unencrypted traffic to be sent between a web browser and PVS. Custom SSL certificates may be installed in the <code>/opt/pvs/var/pvs/ssl</code> directory. Changes to this setting require that PVS be restarted.</td>
</tr>
<tr>
<td>Note: Changing this option while PVS is running makes communication between the client and server either encrypted or unencrypted. If you select or clear the Enable SSL for Web Server check box, the Web Server automatically ends your current PVS session.</td>
<td></td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>A text box in which you can specify the lowest number of characters a password may contain. By default, this option is set to 5, but can be set to any value between 5 and 32.</td>
</tr>
<tr>
<td>PVS Web Server Port</td>
<td>A text box in which you can specify the PVS web server listening port. The default setting is 8835, but can be changed as appropriate for the local environment.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>PVS Web Server Idle Session Timeout</strong></td>
<td>A text box in which you can specify the number of minutes of inactivity before a web session becomes idle. By default, this option is set to 30, but can be set to any value between 5 and 60.</td>
</tr>
<tr>
<td><strong>Enable SSL Client Certificate Authentication</strong></td>
<td>A check box that, when selected, allows the web server to accept only SSL client certificates for user authentication.</td>
</tr>
<tr>
<td><strong>Enable Debug Logging for PVS Web Server</strong></td>
<td>A check box that, when selected, allows the web server to include debug information in the logs for troubleshooting issues related to the web server. The logs become very large if this option is routinely enabled.</td>
</tr>
<tr>
<td><strong>Maximum User Login Attempts</strong></td>
<td>A text box in which you can specify the number of times a user can enter an incorrect password in a 24 hour period before the user's account is locked.</td>
</tr>
<tr>
<td><strong>Max Sessions per User</strong></td>
<td>A text box in which you can specify the number of concurrent sessions a user can have running at one time.</td>
</tr>
<tr>
<td><strong>Enforce Complex Passwords</strong></td>
<td>A check box that, when selected, forces the user's passwords to contain at least one uppercase character, one lower case character, one digit, and one special character from the following: !@#$%^&amp;*.</td>
</tr>
</tbody>
</table>

**Plugins**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Process High Speed Plugins Only</strong></td>
<td>PVS is designed to find various protocols on non-standard ports. For example, PVS can easily find an Apache server running on a port other than 80. However, on a high traffic network, PVS can be run in High Performance mode, which allows it to focus certain plugins on specific ports. When High Performance mode is enabled and this check box is selected, any plugin that utilizes the keywords <code>hs_dport</code> or <code>hs_sport</code> are executed only on traffic traversing the specified ports.</td>
</tr>
<tr>
<td><strong>Enable Automatic Plugin Updates</strong></td>
<td>A check box that, when selected, allows PVS to update its plugins automatically from the Tenable website on a daily basis. If the PVS server is not connected to the Internet, it is recommended that you disable this option.</td>
</tr>
</tbody>
</table>

**Note:** If you change the value in this field, the Web Server automatically ends your current PVS session.
Name | Description
--- | ---
 | option.

**Tip:** When the HTML Client updates, the web browser needs to be refreshed to utilize the new client. In some cases, the web browser's cache must be deleted to view the new client.

### Realtime Events

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realtime Events File Size</td>
<td>A text box in which you can specify the maximum amount of data from real-time events that is stored in one text file. The option must be specified in kilobytes, megabytes, or gigabytes by appending a K, M, or G, respectively, to the value.</td>
</tr>
<tr>
<td>Log Realtime Events to Realtime Log File</td>
<td>A check box that, when selected, allows PVS detected real-time events to be recorded to a log file in the following location: /opt/pvs/var/pvs/logs/realtime-logs-##.txt This option can be configured via the CLI.</td>
</tr>
<tr>
<td>Enable Realtime Event Analysis</td>
<td>A check box that, when selected, allows PVS to analyze real-time events.</td>
</tr>
<tr>
<td>Maximum Viewable Realtime Events</td>
<td>A text box in which you can specify the maximum number of most recent events cached by the PVS engine. This setting is in effect only when Realtime Event Analysis is enabled.</td>
</tr>
<tr>
<td>Maximum Realtime Log Files</td>
<td>A text box in which you can specify the maximum number of realtime log files written to the disk.</td>
</tr>
</tbody>
</table>

### Reports

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Threshold</td>
<td>A text box in which you can specify the number of times the encryption detection algorithm executes during a session. Once the threshold is reached, the algorithm no longer executes during the session. By default, this option is set to 3.</td>
</tr>
<tr>
<td>Report Lifetime</td>
<td>A text box in which you can specify, in days, how long hosts, vulnerabilities, and snapshot reports are cached. After the configured number of days is met, PVS's discovered hosts, vulnerabilities, and snapshot reports are removed. This option can be set to a maximum value of 90</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Report Frequency</td>
<td>A text box in which you can specify, in minutes, how often PVS writes a report. By default, this option is set to 15. SecurityCenter 4.6 and higher retrieve the PVS report every 15 minutes.</td>
</tr>
<tr>
<td>Knowledgebase Lifetime</td>
<td>A text box in which you can specify, in seconds, the maximum length of time that a knowledgebase entry remains valid after its addition. By default, this option is set to 864000.</td>
</tr>
<tr>
<td>New Asset Discovery Interval</td>
<td>A text box in which you can specify, in days, how long PVS monitors traffic before detecting new hosts. PVS listens to network traffic and attempts to discover when a new host has been added. To do this, PVS constantly compares a list of hosts that have generated traffic in the past to those currently generating traffic. If it finds a new host generating traffic, it issues a “new host alert” via the real-time log. For large networks, PVS can be configured to run for several days to gain knowledge about which hosts are active. This prevents PVS from issuing an alert for hosts that already exist. For large networks, Tenable recommends that PVS operate for at least two days before detecting new hosts. By default, this option is set to 2.</td>
</tr>
<tr>
<td>Connections to Services</td>
<td>A check box that, when selected, enables PVS to log which clients attempt to connect to servers on the network and to what port they attempt to connect. They indicate only that an attempt to connect was made, not whether the connection was successful. Events detected by PVS of this type are logged as PVS internal plugin ID 2.</td>
</tr>
<tr>
<td>Show Connections</td>
<td>A check box that, when selected, instructs PVS to record clients in the focus network that attempt to connect to a server IP address and port and receive a positive response. The record contains the client IP address, the server IP address, and the server port that the client attempted to connect to. For example, if four different hosts within the focus network attempted to connect with a server IP over port 80 and received a positive response, then a list of those hosts are reported under PVS internal plugin ID 3 and port 80.</td>
</tr>
</tbody>
</table>

---

### Session Analysis

This section provides details on how PVS handles session analysis, which is crucial for understanding network traffic and identifying potential threats. It includes parameters such as the frequency of report generation, lifetime of knowledgebase entries, and intervals for detecting new assets. These settings help in maintaining an accurate and up-to-date view of the network environment, ensuring that security measures are effective and responsive to real-time threats.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted Sessions Dependency Plugins</td>
<td>A text box in which you can specify the Plugin IDs, separated by commas, used to detect encrypted traffic.</td>
</tr>
</tbody>
</table>
| Encrypted Sessions Excluded Network Ranges | A text box in which you can specify the IPv4 and IPv6 addresses and ports, in CIDR notation, excluded from monitoring for encrypted traffic.  
Example: 192.168.1.0/24,2001:DB8::/64,10.2.3.0/22,vlan 172.16.0.0/16,192.168.3.123/32 |
| Interactive Sessions Dependency Plugins | A text box in which you can specify the Plugin IDs, separated by commas, used to detect interactive sessions. |
| Interactive Sessions Excluded Network Ranges | A text box in which you can specify the IPv4 and IPv6 addresses and ports, in CIDR notation, excluded from monitoring for interactive sessions.  
Example: 192.168.1.0/24,2001:DB8::/64,10.2.3.0/22,vlan 172.16.0.0/16,192.168.3.123/32 |

### Syslog

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Realtime Syslog Server List | A text box in which you can specify the IPv4 or IPv6 address and port of a Syslog server to receive real-time events from PVS. A local Syslog daemon is not required. Syslog items can be specified to Standard or CEF formats as well as UDP or TCP protocols.  
Example: 192.168.1.12:4567,10.10.10.10:514,[2001:DB8::23B4]:514 |
| Vulnerability Syslog Server List | A text box in which you can specify the IPv4 or IPv6 address and port of a Syslog server to receive vulnerability data from PVS. A local Syslog daemon is not required. Syslog items can be specified to Standard or CEF formats as well as UDP or TCP protocols.  
Example: 192.168.1.12:4567,10.10.10.10:514,[2001:DB8::23B4]:514 |

**Note:** While PVS may display multiple log events related to one connection, it sends only a single event to the remote Syslog server(s).
Feed Settings Section

The **Feed Settings** section allows you to update the Activation Code, plugins, perform offline updates, and configure a custom plugin feed host. The Activation Code only needs to be updated when it expires.

The **Offline Update** allows a user with administrative privileges to manually update the plugins when the PVS host cannot connect to the Internet. After downloading the plugin update archive from Tenable, click **Choose File** and select the archive tarball to upload. Click the **Upload Archive** button to send the file to the PVS host, and click the **Upload Archive** button again to update the plugins. If a new client is part of the update, you must refresh the web browser to see the updated client.

The **Custom Plugin Feed Host** is an alternate feed host. These are typically hosted on a local network to provide custom PVS plugins.

When running Standalone PVS or PVS in High Performance mode as **Managed by SecurityCenter** or **Managed by Tenable.io**, you must enter an Activation Code before clicking the **Update** button. The **button schedules a plugin update when PVS is running in **Standalone** mode. Additionally, when registering PVS in **Offline** mode, you need the Activation Code to obtain the Activation Key.
The **Cloud Settings** section provides options for configuring PVS to communicate with Tenable.io.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Host</td>
<td>The domain name or IP address of the Tenable.io server.</td>
</tr>
<tr>
<td>Cloud Port</td>
<td>The port of the Tenable.io server.</td>
</tr>
<tr>
<td>Cloud Key</td>
<td>The key used to link this instance of PVS with a Tenable.io account.</td>
</tr>
<tr>
<td>Polling Frequency</td>
<td>The frequency, in seconds, with which PVS updates its status with Tenable.io and asks for a list of jobs.</td>
</tr>
<tr>
<td>PVS Name</td>
<td>The unique name used to identify this instance of PVS on Tenable.io.</td>
</tr>
</tbody>
</table>
Web Proxy Settings Section

The **Web Proxy Settings** section configures the settings for a web proxy if one is needed for plugin updates. These settings include the proxy host IP address, port, username, password, and, if a custom agent string is needed, a user-agent field.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>The host address of the web proxy server.</td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>User-Agent String</td>
<td></td>
</tr>
</tbody>
</table>
Chart Settings Section

The Chart Settings section displays all charts available, provides options for creating and configuring charts, and allows the user to add or remove charts in the Dashboards section.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Dashboard Family</th>
<th>View in Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution by Operating System</td>
<td>Distribution by operating system</td>
<td>Top N</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribution of Mobile Applications by Application</td>
<td>Distribution of mobile applications by application</td>
<td>Top N</td>
<td>Yes</td>
</tr>
<tr>
<td>Distribution of Mobile Devices by Operating System</td>
<td>Distribution of mobile devices by operating system</td>
<td>Top N</td>
<td>Yes</td>
</tr>
<tr>
<td>SCADA Host Distribution by Protocol</td>
<td>Distribution of SCADA hosts by protocol</td>
<td>SCADA</td>
<td>Yes</td>
</tr>
<tr>
<td>SCADA Host Distribution by System Type</td>
<td>Distribution of SCADA hosts by system type</td>
<td>SCADA</td>
<td>Yes</td>
</tr>
<tr>
<td>SCADA Vulnerability Distribution by Severity</td>
<td>Distribution of SCADA vulnerabilities by severity</td>
<td>SCADA</td>
<td>Yes</td>
</tr>
<tr>
<td>Top 10 Hosts</td>
<td>Chart of top 10 monitored hosts by vulnerability</td>
<td>Top N</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Email Settings Section

The Email Settings section provides options for configuring email reporting for PVS, including the recipients of the email notifications, what charts appear in email notifications, and the time and frequency with which email notifications are sent. In the Email Settings section, hover over an existing email notification and click the paper airplane icon to send a report immediately.

When you select **SMTP Server** in the **Setting Type** drop-down menu, the following options for configuring the SMTP server will appear:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>The host or IP of the SMTP server (e.g., smtp.example.com).</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port of the SMTP server (e.g., 25).</td>
</tr>
<tr>
<td><strong>From</strong></td>
<td>The name that appears in the &quot;From&quot; line of the email report.</td>
</tr>
<tr>
<td><strong>PVS Location</strong></td>
<td>The IP address or hostname for your PVS server. This works only if the user that receives the email report can reach the PVS host.</td>
</tr>
<tr>
<td><strong>Auth Method</strong></td>
<td>The method by which the SMTP server is authenticated. Supported methods are None, Plain, NTLM, Login, and CRAM-MD5.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Username</td>
<td>The username used to authenticate to the SMTP server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password associated with the username, provided that a password is required by the SMTP server.</td>
</tr>
</tbody>
</table>

**Note:** If this option is set to None, the *Username* and *Password* fields are hidden.
The **Plugin Settings** section allows the user to create custom plugins and also to enable and disable existing plugins and PASLs.

The **Plugin Settings** section contains the following subsections:

- **Plugin Management**: displays a list each of enabled and disabled plugins, respectively, the options to move plugins between those lists.

- **PASL Management**: displays a list each of enabled and disabled PASLs, respectively, and the options to move PASLs between those lists.

- **Create Custom Plugin**: displays options for creating custom plugins and creating new plugin fields.

The following table provides a brief summary of each plugin field available for creating custom plugins.

<table>
<thead>
<tr>
<th>Custom Plugin Field</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique numeric ID of the plugin.</td>
</tr>
<tr>
<td>Custom Plugin Field</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the plugin. The plugin name should start with the vendor name.</td>
</tr>
<tr>
<td>Description</td>
<td>Full text description of the vulnerability.</td>
</tr>
<tr>
<td>Synopsis</td>
<td>Brief description of the plugin or vulnerability.</td>
</tr>
<tr>
<td>Solution</td>
<td>Remediation information for the vulnerability.</td>
</tr>
<tr>
<td>See Also</td>
<td>External references to additional information regarding to the vulnerability.</td>
</tr>
<tr>
<td>Risk</td>
<td><strong>Info, Low, Medium, High, or Critical</strong> risk factor.</td>
</tr>
<tr>
<td>Plugin Output</td>
<td>Displays dynamic data in PVS plugin reports.</td>
</tr>
<tr>
<td>Family</td>
<td>Family to which the plugin belongs.</td>
</tr>
<tr>
<td>Dependency</td>
<td>Other dependencies required to trigger the custom plugin.</td>
</tr>
<tr>
<td>NoPlugin</td>
<td>Prevents a plugin from being evaluated if another plugin has already matched. For example, it may make sense to write a plugin that looks for a specific anonymous FTP vulnerability, but disable it if another plugin that checked for anonymous FTP had already failed.</td>
</tr>
<tr>
<td>No Output</td>
<td>For plugins that are written specifically to be used as part of a dependency with another plugin. When enabled, this keyword causes PVS not to report anything for any plugin.</td>
</tr>
<tr>
<td>Client Issue</td>
<td>Indicates the vulnerability is located on the client side.</td>
</tr>
<tr>
<td>Plugin Type</td>
<td><strong>Vuln, realtime, or realtimeonly</strong> plugin type.</td>
</tr>
<tr>
<td>cve</td>
<td>CVE reference.</td>
</tr>
<tr>
<td>bid</td>
<td>Bugtraq ID (BID) reference.</td>
</tr>
<tr>
<td>osvdb</td>
<td>External reference (e.g., OSVDB, Secunie, MS Advisory).</td>
</tr>
<tr>
<td>nid</td>
<td>To track compatibility with the Nessus vulnerability scanner, Tenable associates PVS vulnerability checks with relevant Nessus vulnerability checks. Multiple Nessus IDs can be listed under one <strong>nid</strong> entry such as <strong>nid=10222,10223</strong>.</td>
</tr>
<tr>
<td>Custom Plugin Field</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
</tr>
<tr>
<td>cpe</td>
<td>Filters the result of discovered vulnerabilities based on their CPE identifier.</td>
</tr>
<tr>
<td>Match</td>
<td>This keyword specifies a set of one or more simple ASCII patterns that must be present in order for the more complex pattern analysis to take place. The <strong>match</strong> keyword gives PVS a lot of its performance and functionality.</td>
</tr>
<tr>
<td>Regex</td>
<td>Specifies a complex regular expression search rule applied to the network session.</td>
</tr>
<tr>
<td>Revision</td>
<td>Revision number associated with custom plugin.</td>
</tr>
<tr>
<td>Raw Text Preview</td>
<td>A preview of the custom plugin in raw text. Example of a custom plugin created to find a IMAP Banner of Tenable Rocks:</td>
</tr>
</tbody>
</table>

```plaintext
id=79000
name=IMAP Banner
description=An IMAP server is running on this port. Its banner is Tenable Rocks
risk=None
match=OK
match=IMAP
match=server ready
regex:^.*OK.*IMAP.*Tenable Rocks
```
Nessus Scanner Settings Section

The **Nessus Scanner Settings** section provides a list of the available Nessus 6.4+ scanners and the ability to add, edit, or remove a Nessus scanner. Each Nessus scanner must be configured with the following parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner Host</td>
<td>The domain name or IP address of the Nessus server.</td>
</tr>
<tr>
<td>Scanner Port</td>
<td>The port of the Nessus server.</td>
</tr>
<tr>
<td>Access Key</td>
<td>The first half of a Nessus API Key, which is used to authenticate with the Nessus REST API.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>The second half of a Nessus API Key, which is used to authenticate with the Nessus REST API.</td>
</tr>
</tbody>
</table>

**Note:** For details on how to obtain an API Key (Access Key and Secret Key), refer to the [Nessus user guide](https://www.tenable.com/docs/nessus).
How To

This section includes step-by-step instructions for performing the actions available in each page within the PVS web interface:

- Monitoring
- Results
- Users
- Configuration
Monitoring Page

The topics in this section explain how to perform the following actions available on the Monitoring page:

- **Rearrange Charts**
- **Set a Range for the Dashboards Section**
- **Refresh a Chart**
- **Remove a Chart from a Dashboard**
- **Filter Results**
- **Export Results**
- **Launch a Nessus Scan**
- **Delete a Vulnerability**

**Tip:** For more information about the Monitoring page, see the related Features section of this guide.
Rearrange Charts

Steps

1. In the **Dashboards** section, select the heading of the chart you want to reposition.

2. Drag the chart to a different location on the dashboard, and release the pointer.

   The chart moves and the dashboard configuration saves for the duration of your session.

   **Note:** You cannot move the **Client Connections**, **Network Bandwidth by Byte Count**, or **Event Trending** charts.
Set a Range for the Dashboards Section

Steps

1. In the **Dashboards** section, in the upper right corner, click the ⬇️ drop-down box.

2. In the drop-down menu, do one of the following:
   - Select one of the preset time intervals.
   - Select a start and end date from the available calendars and specify a time associated with each date.
   - Manually enter dates in the two text boxes in YYYY/MM/DD format and specify a time associated with each date.

All the charts on the page refresh to reflect the selected time interval.
Refresh a Chart

Steps

1. In the **Dashboards** section, in the upper right corner of the chart you want to refresh, click the ⌁ button.

   The selected chart refreshes.
Remove a Chart from a Dashboard

Steps

1. In the **Dashboards** section, in the upper right corner of the chart you want to remove, click the **x** button.

   The selected chart is removed from the dashboard for the duration of your session.
Filter Results

Steps

1. In the Hosts, Vulnerabilities, Applications, Operating Systems, Connections, or Mobile Devices section, in the upper right corner, click the Filter <section name> drop-down box.

2. Type the criteria by which you want to filter results directly into the box.
   -or-
   Click the ▼ button in the box.

The Filter Results window appears.

3. Configure the filter options as necessary and click the Apply Filters button.

   Note: On-the-fly filter results cannot be exported. If you want to export filter results, you must configure the filter(s) in the Filter Results window. Additionally, on-the-fly filter results are not stored when a user navigates to another page in PVS.
Export Results

Steps

1. On the Monitoring page, in the upper right corner, click the Actions drop-down box.

2. Select Export Results.

   The Export Results screen appears.

   ![](image)

3. Select the export format and chapter layout and click the Export button.

   An automatic download begins. You can save the report from the web browser.

   **Note:** On-the-fly filter results cannot be exported. If you want to export filter results, you must configure the filter(s) in the Filter Results window.
Launch a Nessus Scan

Steps

1. On the Monitoring page, in the upper right corner, click the Actions drop-down box.
   -or-
   In the Hosts or Mobile Devices section, select the check boxes for the hosts or devices you want to scan, and in the upper right corner, locate the Actions menu.

2. Select Launch Scan.

   The Launch Basic Nessus Scan window appears.

3. Configure the scan options as necessary and click the Launch button.

   The scan opens in the Nessus interface. Refer to the Nessus documentation for further instructions.

   **Note:** To launch scans on Nessus 6.8.x or higher, PVS must be configured to restrict access to TLS 1.2 or higher. See PVS Settings Section for more information.
Delete a Vulnerability

Steps

To delete one vulnerability:

1. In the Vulnerabilities section, hover over the vulnerability you want to delete.
2. On the right side of the row, click the ✗ button.
   The vulnerability is deleted.

To delete multiple vulnerabilities:

1. On the Vulnerabilities page, on the left side of the row for the vulnerability you want to delete, select the check box. Repeat this step for each vulnerability you want to delete.
2. In the upper right corner of the page, click the Actions drop-down box and select Delete Vulnerabilities.
   The vulnerabilities are deleted.
Results Page

The topics in this section explain how to perform the following actions available on the Results page:

- Upload a Report
- Upload a Pcap
- Filter Results

Tip: For more information about the Results page, see the related Features section of this guide.
Upload a Report

Steps

1. On the **Results** page, in the upper right corner, click the **Upload** drop-down box.

2. Select **Report**.

   The **Upload Results** window appears. Select a file to upload.

3. Click the **Upload** button.

   The report or appears in a new row at the top of the **Listing Results** list on the **Results** page.
Upload a Pcap

Before You Begin

The maximum total file size for uploaded Pcaps is 100 MB. Running a Pcap pauses live monitoring.

Steps

1. On the Results page, in the upper right corner, click the Upload drop-down box.
2. Select Pcap.
   
   The Upload Pcap window appears. Select to upload.
3. Click the Upload Pcap button.
   
   A new row for the Pcap appears at the top of the Listing Results list on the Results page.
Filter Results

Steps

1. On the Results page, in the upper right corner, click the Filter Results drop-down box.

2. Select Snapshot, Manual, or Pcap.

   The Listing Results list filters by the selected report type.
Users Page

In order to see the Users page, you must access PVS using an account with administrative privileges.

The topics in this section explain how to perform the following actions available on the Users page:

- Create a New User
- Modify a User Account
- Reset a Locked Account
- Delete a User

Tip: For more information about the Users page, see the related Features section of this guide.
Create a New User

Steps

1. On the Users page, in the upper right corner, click the New User button.

   The New User window appears.

   ![New User Window](image)

   - Username
   - Password
   - Confirm Password
   - Administrator

   ![Create User Button](image)

2. Enter the new user's information.

   **Note:** The username is case sensitive and the password must conform to the PVS password policy.

3. If the new user should have administrative privileges, select the Administrator check box.

   **Tip:** When a user is created it authenticates with SSL Client Certificates. The user name must match the Common Name in the certificate.

4. Click the Create User button.

   The user saves and appears in the Listing Users list.
Modify a User Account

Steps

1. On the **Users** page, select a user from the list.

   The **Edit User <username>** window appears.

2. Modify the properties as needed and click the **Update** button.

   To reset user account passwords via the command line, use the following command from the **pvs** binary directory:

   ```
   /opt/pvs/bin/pvs --users --chpasswd <username>
   ```
Reset a Locked Account

Steps

1. Depending on your operating system, use the following command:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code># rm /opt/pvs/var/pvs/users/&lt;locked account name&gt;/hash.-lockedout</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>del C:\ProgramData\Tenable\PVS\pvs\users\&lt;locked_account_name&gt;\hash.lockedout</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code># rm /Library/PVS/var/pvs/users/&lt;locked account name&gt;/hash.lockedout</code></td>
</tr>
</tbody>
</table>

**Tip:** Alternatively, a user with administrative privileges can navigate to this directory and manually delete the hash.lockedout file.

2. After deleting the hash.lockedout file, if needed, a user with administrative privileges can follow the steps under [Modify a User Account](#) to reset the user's password.
Delete a User

Steps

To delete one user:

1. On the Users page, hover over the user you want to delete.
   On the right side of the row, the \textbf{x} button appears.
2. Click the \textbf{x} button.
   A dialog box appears confirming your selection to delete the user.
3. Click the \textbf{Delete} button.
   The user is deleted.

To delete multiple users:

1. On the Users page, on the left side of the row for the user you want to delete, select the check box. Repeat this step for each user you want to delete.
2. In the upper right corner of the page, click the \textbf{Actions} drop-down box and select \textbf{Delete Users}.
   A dialog box appears confirming your selection to delete the user.
3. Click the \textbf{Delete} button.
   The users are deleted.
Configuration Page

The topics in this section explain how to perform the following actions available on the Configuration page:

- Configure the Performance Mode
- Download New Vulnerability Plugins
- Create a Custom Chart
- Delete a Chart
- Create an Email Notification
- Delete an Email Notification
- Add a Plugin Field
- Add a Nessus Scanner
- Delete a Nessus Scanner

Tip: For more information about the Configuration page, see the related Features section of this guide.
Configure the Performance Mode

Before You Begin

This option appears only when PVS is licensed to run in High Performance mode and the machine running PVS meets the hardware and software requirements for High Performance mode. By default, all instances of PVS run in Standard mode.

PVS must restart when switching between performance modes.

Steps

1. Access the PVS Settings section.

2. Under the Performance Mode heading, click the Enable High Performance Mode box to toggle between Yes and No. If you select Yes, continue to step 3. If you select No, continue to step 4.

![Performance Mode](image)

3. In the Number of Worker Cores drop-down menu, select the appropriate number of worker cores.

   **Note:** This option cannot be changed when PVS is already running in High Performance mode.

4. Click the Update button.

   A dialog box appears confirming your selection to change the performance mode.

5. Click the Confirm button.

   PVS restarts and the login screen appears. When the PVS server resumes, a notification appears indicating whether the configuration change was successful.
**Note:** PVS may use a different number of cores than the number you select. Based on system constraints and your selection, PVS selects the closest number of worker cores that it can feasibly support.

6. Log in to PVS.

   The performance mode updates.
Download New Vulnerability Plugins

Before You Begin

When PVS is registered in **Standalone** mode using an Activation code, plugins are updated automatically every 24 hours after the service is started.

If SecurityCenter CV or Tenable.io is used to manage PVS, new plugins for PVS are automatically sent at scheduled intervals.

Steps

1. Access the **Feed Settings** section.
2. In the **Feed Registration & Plugin Update** heading, click the ⚙ button.

   The plugins can also be updated by using the following command:
   ```bash
   # /opt/pvs/bin/pvs --update-plugins
   ```
Create a Custom Chart

Steps

1. Access the **Chart Settings** section.

2. In the upper right corner, click the **Create Chart** button.

   The **Create Chart** window appears.

   ![Create Chart Window](image)

3. Enter a name and description for the chart.

   **Note:** In this example, we are creating a chart that displays the top vulnerabilities for machines reporting associated BitTorrent activity.

4. In the **Chart Type** section, select the type of chart you want to display.

5. In the **Dashboard Family** section, enter a numeric value between 1 and 20 that represents the number of items returned for this chart. Click **Top** to add this value to the **Current Chart Query**.
section.

6. In the **Category** section, select a chart category. The selected category determines the type of items displayed on the chart, such as hosts, vulnerabilities, applications, operating systems, or connections.

7. In the **Filter** section, configure the options by which you want to filter the results and select the + button to apply the rule to the chart.

Note: In this example, we are creating a filter based on the Plugin ID 3920. This triggers when BitTorrent client activity is detected.

8. In the **Viewable** section, select whether you want the chart to be viewable on the main dashboard.

The configured options look like this:

9. Click the **Create Chart** button. The chart appears in the **Dashboards** section of the **Monitoring** page.
Delete a Chart

Steps

To delete one chart:

1. In the Chart Settings section, hover over the chart you want to delete. 
   On the right side of the row, click the x button.
2. Click the x button. 
   A dialog box appears confirming your selection to delete the chart.
3. Click the Delete button. 
   The chart is deleted.

To delete multiple charts:

1. In the Chart Settings section, on the left side of the row for the chart you want to delete, select the check box. Repeat this step for each chart you want to delete.
2. In the upper right corner of the page, click the Actions drop-down box and select Delete Charts. 
   A dialog box appears confirming your selection to delete the charts.
3. Click the Delete button. 
   The charts are deleted.

Note: You cannot delete default charts.
Create an Email Notification

Steps

1. Access the Email Settings section.

2. In the upper right corner, click the Create Email Notification button.
   The Create Email Notification window appears.

3. Enter a name and description for the email notification and click the Next Step button.
   The Add Charts screen appears.

4. Select the check boxes that correspond to the charts you want to add to the email notification.
   Reorder the charts by clicking and dragging the appropriate button.

5. Click the Next Step button.

6. Select the frequency, date, and time at which you want the email notification to be sent. Depending on the option you select in the Frequency box, the following additional options appear:

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once</td>
<td>None</td>
</tr>
<tr>
<td>Hourly</td>
<td>Repeat Every - a drop-down box that includes options from 1 to 20 hours.</td>
</tr>
<tr>
<td>Daily</td>
<td>Repeat Every - a drop-down box that includes options from 1 to 20 days.</td>
</tr>
<tr>
<td>Weekly</td>
<td>Repeat Every - a drop-down box that includes options from 1 to 20 weeks.</td>
</tr>
<tr>
<td></td>
<td>Repeat On - a multi-selectable list of the days of the week.</td>
</tr>
<tr>
<td>Monthly</td>
<td>Repeat Every - a drop-down box that includes options from 1 to 20 months.</td>
</tr>
<tr>
<td></td>
<td>Repeat By - a drop-down box that includes the options Week of Month and Day of Month.</td>
</tr>
<tr>
<td>Yearly</td>
<td>Repeat Every - a drop-down box that includes options from 1 to 20 years.</td>
</tr>
</tbody>
</table>

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
The **Summary** field updates automatically depending on your selection.

7. Click the **Next Step** button.

   The **Add Recipients** screen appears.

8. In the **Recipients** box, enter an email address and click the **button until you have added all desired recipients. Click the **Next Step** button.

   The **Review Email Notification** screen appears, which displays a summary of your email notification configuration.

9. Review the notification details and click the **Finish** button.
Delete an Email Notification

Steps

To delete one email notification:

1. In the Email Settings section, hover over the email notification you want to delete.
   
   On the right side of the row, click the × button.

2. Click the × button.
   
   A dialog box appears confirming your selection to delete the email notification.

3. Click the Delete button.
   
   The email notification is deleted and the corresponding notifications are no longer sent.

To delete multiple email notifications:

1. In the Email Settings section, on the left side of the row for the email notification you want to delete, select the check box. Repeat this step for each email notification you want to delete.

2. In the upper right corner of the page, click the Actions drop-down box and select Delete Notifications.
   
   A dialog box appears confirming your selection to delete the email notifications.

3. Click the Delete button.
   
   The email notifications are deleted and the corresponding notifications are no longer sent.
Add a Plugin Field

1. Access the Plugin Settings section.

2. In the Setting Type drop-down box, select Create Custom Plugin.

3. In the upper right corner, click the Add Plugin Field button.

   The Add Plugin Field window appears.

4. Configure the options as necessary and click the Add button.

   The new plugin fields appear below the No Output check box.
Add a Nessus Scanner

Steps

1. Access the **Nessus Scanner Settings** section.

2. In the upper right corner, click the **Add Nessus Scanner** button.
   
   The **Add Nessus Scanner** window appears. Enter the details for your Nessus scanner.

3. Click the **Add Nessus Scanner** button.
   
   The Nessus scanner appears in the **Nessus Scanner Settings** section.
Delete a Nessus Scanner

Steps

To delete one Nessus Scanner:

1. In the Nessus Scanner Settings section, hover over the scanner you want to delete.
   On the right side of the row, click the ✗ button.
2. Click the ✗ button.
   A dialog box appears confirming your selection to delete the scanner.
3. Click the Delete button.
   The scanner is deleted.

To delete multiple Nessus Scanners:

1. In the Nessus Scanner Settings section, on the left side of the row for the scanner you want to delete, select the check box. Repeat this step for each scanner you want to delete.
2. In the upper right corner of the page, click the Actions drop-down box and select Delete Nessus Scanners.
   A dialog box appears confirming your selection to delete the scanners.
3. Click the Delete button.
   The scanners are deleted.
Additional Resources

This section describes the following information about PVS that is not included in the Features and How To sections:

- Command Line Operations
- Unknown or Customized Ports
- Real-Time Traffic Analysis Configuration Theory
- Modules
- Internal PVS Plugin IDs
- PVS Plugins
- Working with SecurityCenter
- Syslog Message Formats
- Custom SSL Certificates
- Configure PVS for Certificates
Command Line Operations

The PVS engine provides many options to update and configure PVS from the command line in Linux, Windows, and macOS. All command lines should be run by users with root or administrative privileges.

- Common Command Line Operations
- Linux Command Line Operations
- Windows Command Line Operations
- macOS Command Line Operations
Common Command Line Operations

PVS can be run from the command line to update plugins, perform configuration tasks, and analyze Pcap files to generate a report file for use with SecurityCenter CV or other programs. Running the PVS binary with the –h option displays a list of available options.

Note: You must stop PVS before running command line operations.

PVS Binary Locations

The PVS binary for Linux can be found in the following location:

```
# /opt/pvs/bin/pvs
```

The PVS binary for Windows can be found in the following location:

```
C:\Program Files\Tenable\PVS\pvs.exe
```

The PVS binary for macOS can be found in the following location:

```
#/Library/PVS/bin/pvs
```

PVS Command Line Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a &lt;activation code&gt;</td>
<td>Enter the Activation Code to activate PVS to enable plugin updates and monitoring functions.</td>
</tr>
<tr>
<td></td>
<td>If your PVS system is managed by SecurityCenter and running in Standard mode, you can use the following command: -a SecurityCenter</td>
</tr>
<tr>
<td></td>
<td>If your PVS system is managed by SecurityCenter and running in High Performance mode, you can use the following command: -a SecurityCenter &lt;activation code&gt;</td>
</tr>
<tr>
<td></td>
<td>If your PVS system is managed by Tenable.io and running in Standard mode, you can use the following command: -a Cloud</td>
</tr>
<tr>
<td></td>
<td>If your PVS system is managed by Tenable.io and running in High Performance mode, you can use the following command: -a Cloud</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;activation code&gt;</td>
<td>Before running the <code>-a</code> command for PVS that is managed by Tenable.io, you should first configure the Cloud Host, Cloud Port, Cloud Key, and PVS Name parameters.</td>
</tr>
<tr>
<td>--config --add &quot;custom_parameter name&quot; &quot;parameter value&quot;</td>
<td>Add a custom configuration parameter for PVS or PVS Proxy. The double quote characters are required, although single quotes may be used when special characters are required.</td>
</tr>
<tr>
<td>--config --delete &quot;custom_parameter name&quot;</td>
<td>The delete command may be used to remove custom configuration parameters.</td>
</tr>
<tr>
<td>--config --list</td>
<td>Lists the current PVS and PVS Proxy configuration parameters. Parameter values are listed to the left of the colon character and are case sensitive. The value of the parameter displays to the right of the colon character.</td>
</tr>
<tr>
<td>--config &quot;parameter name&quot; [&quot;parameter value&quot;]</td>
<td>Displays the defined parameter value. If a value is added at the end of the command, the parameter updates with the new setting. The double quote characters are required, and single quotes may be used when special characters are required.</td>
</tr>
<tr>
<td>-d debug mode</td>
<td>Runs PVS in debug mode for troubleshooting purposes. This option causes the system to use more resources and should be enabled only when directed by a Tenable Support Technician.</td>
</tr>
<tr>
<td>-f packet_dump_file</td>
<td>Replace packet_dump_file with the path to the Pcap file you want PVS to process. Note: Windows does not support the pcapng format.</td>
</tr>
<tr>
<td>Option</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-h</td>
<td>Displays the command line options help file.</td>
</tr>
<tr>
<td>-k</td>
<td>Displays the PVS activation status.</td>
</tr>
<tr>
<td>-L</td>
<td>Displays a list of the license declarations.</td>
</tr>
<tr>
<td>-l</td>
<td>Displays a list of the plugin IDs that are loaded by PVS.</td>
</tr>
<tr>
<td>-m</td>
<td>Shows various aspects of memory usage during the processing of the <code>pvs</code> command.</td>
</tr>
<tr>
<td>-p packet_dump_file</td>
<td>Replace <code>packet_dump_file</code> with the local file name or path to file name to write the captured packets to a file.</td>
</tr>
<tr>
<td><code>pvs --users --add</code></td>
<td>Use to add a new user to PVS with the expected values of: [&quot;username&quot; &quot;password&quot; admin]: add new user. Expected values for “admin” flag are either 1 - grant user administrative privileges, or 0 - don’t grant user administrative privileges.</td>
</tr>
<tr>
<td><code>pvs --users --chpasswd</code></td>
<td>Use to change a PVS user's password.</td>
</tr>
<tr>
<td><code>pvs --users --delete</code></td>
<td>Use to remove a user from PVS.</td>
</tr>
<tr>
<td>--register-offline</td>
<td>Registers PVS in offline mode when you insert the license file obtained from Tenable.</td>
</tr>
<tr>
<td><code>&lt;license file&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>--update-plugins</code></td>
<td>If PVS is not running in offline mode, the tarball is optional. When no file is provided with this command, PVS contacts a plugin feed server to download plugins directly.</td>
</tr>
<tr>
<td>-v</td>
<td>Shows the version information about the installed instance of PVS.</td>
</tr>
</tbody>
</table>
Linux Command Line Operations

You must run all commands with root privileges.

Start, Stop, or Restart PVS

<table>
<thead>
<tr>
<th>Action</th>
<th>Command to Manage PVS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td><code># service pvs start</code> then `# ps aux</td>
</tr>
<tr>
<td>Stop</td>
<td><code># service pvs stop</code></td>
</tr>
<tr>
<td>Restart</td>
<td><code># service pvs restart</code></td>
</tr>
</tbody>
</table>

Once a day, as scheduled, if SecurityCenter CV has received new PVS plugins from Tenable, it installs them in the PVS plugin directory. PVS detects the change, automatically reloads, and begins using the new plugins.

Real-time PVS data is communicated to the configured LCE server or Syslog server(s) in real-time.

Configure HugePages

Before You Begin

These steps assume that your system meets the [hardware and software requirements](#) necessary for running PVS in High Performance mode.

Steps

1. Ensure your HugePages settings are correct by using the following command:

```
# grep Huge /proc/meminfo
AnonHugePages: 0kB
HugePages_Total: 1024
HugePages_Free: 1024
```
The Hugepagesize parameter is set to 2048 kB by default, but this option is configurable. PVS requires a minimum of 1024 HugePages that are at least 2048 kB in size.

**Note:** In some cases, the HugePages_Free parameter may be set to 0, however, this does not necessarily indicate insufficient HugePage memory.

2. Reserve a certain amount of memory to be used as HugePages by using the following command to update the kernel parameter manually:

```
/bin/echo 1024 > /sys/devices/system/node/node0/hugepages/hugepages-2048kB/nr_hugepages
```

The number of HugePages reserved by the kernel changes to 1024, and HugePages become available.

**Note:** If the kernel does not have enough memory available to satisfy this request, the command may fail without notifying the user. After running this command, the HugePages configuration should be checked again using the command in step 1.

3. To ensure that your HugePages configuration persists across system reboots, refer to the following section that corresponds to your Linux kernel version.

**Linux Kernel Version 6**

Update the persistent kernel configuration files using one of the following commands:

- In the `/etc/sysctl.conf` file, add the `vm.nr_hugepages=1024` parameter and reload the kernel configuration with the `sysctl -p` command. Alternatively, you can reboot the system.
- or-

- In the `/etc/grub.conf` file, on the kernel startup line, add the `hugepages=1024` parameter and reboot the system.

**Linux Kernel Version 7**

Update the persistent kernel configuration files using one of the following commands:
In the `/etc/sysctl.conf` file, add the `vm.nr_hugepages=1024` parameter and reload the kernel configuration with the `sysctl -p` command. Alternatively, you can reboot the system.

-or-

In the `/etc/sysconfig/grub` file, on the kernel startup command (`GRUB_CMDLINE_LINUX`), add the `hugepages=1024` parameter. Reload the kernel configuration with the `grub2-mkconfig -o /etc/grub2` command and reboot the system.

4. Connect the file system to the HugePages subsystem using the following steps:
   
a. Execute the `/bin/mkdir -p /mnt/pvs_huge` command.
   
b. Execute the `/bin/mount -t hugetlbfs nodev /mnt/pvs_huge` command.
   
c. Additionally, open the `/etc/fstab` file location and add the following record:

   ```
   nodev /mnt/pvs_huge hugetlbfs rw 0 0
   ```

File Locations

PVS installs its files in the following locations:

<table>
<thead>
<tr>
<th>Path</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/opt/pvs</code></td>
<td>Base directory.</td>
</tr>
<tr>
<td><code>/opt/pvs/bin</code></td>
<td>Location of the PVS and PVS Proxy executables, plus several helper tools for the PVS Proxy daemon.</td>
</tr>
<tr>
<td><code>/opt/pvs/docs</code></td>
<td>Contains the software license agreement for PVS.</td>
</tr>
<tr>
<td><code>/opt/pvs/var</code></td>
<td>Contains the folders for PVS and the PVS-Proxy.</td>
</tr>
<tr>
<td><code>/opt/pvs/var/pvs</code></td>
<td>Contains plugins, discovered vulnerabilities, log files, keys, and other miscellaneous items.</td>
</tr>
<tr>
<td><code>db</code></td>
<td>Contains the database files relating to the configuration, reports, and users for PVS.</td>
</tr>
<tr>
<td><code>kb</code></td>
<td>Stores the PVS knowledge base, if used.</td>
</tr>
<tr>
<td><code>logs</code></td>
<td>Contains PVS logs.</td>
</tr>
<tr>
<td><code>plugins</code></td>
<td>Contains the PVS plugins delivered via SecurityCenter, Tenable.io, the</td>
</tr>
<tr>
<td>Path</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pvs-services</td>
<td>A file PVS uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.</td>
</tr>
<tr>
<td>reports</td>
<td>Contains reports generated by PVS with the exception of <code>.nsr</code>. This folder contains the <code>.nessus</code> file generated by default.</td>
</tr>
<tr>
<td>scripts</td>
<td>Contains the files for the PVS Web server.</td>
</tr>
<tr>
<td>ssl</td>
<td>Contains SSL certificates used by the proxy and web server for the SSL connection between itself and SecurityCenter CV or the web browser.</td>
</tr>
<tr>
<td>users</td>
<td>Contains folders for user files and reports.</td>
</tr>
<tr>
<td>www</td>
<td>Contains the files for the PVS web front-end.</td>
</tr>
<tr>
<td>/opt/pvs/var/pvs-proxy</td>
<td>Parent folder for files used/created by the PVS proxy.</td>
</tr>
<tr>
<td>logs</td>
<td>Contains the PVS proxy and PVS proxy service logs.</td>
</tr>
<tr>
<td>scans</td>
<td>By default, PVS creates the <code>.nsr</code> file in the scans directory. The proxy is then responsible for handing the report to SecurityCenter CV when SecurityCenter CV attempts to pull it.</td>
</tr>
</tbody>
</table>

**Note:** If SecurityCenter CV is being used to manage the plugins, do not change this path from the default `/opt/pvs/var/pvs`. 
Windows Command Line Operations

You must run all programs as a local user with administrative privileges. To do so, when UAC is enabled, right-click on the installer program and select Run as Administrator.

Start or Stop PVS

<table>
<thead>
<tr>
<th>Action</th>
<th>Command to Manage PVS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td><code>net start &quot;Tenable PVS Proxy&quot;</code></td>
</tr>
<tr>
<td>Stop</td>
<td><code>net stop &quot;Tenable PVS Proxy&quot;</code></td>
</tr>
</tbody>
</table>

Alternatively, PVS can be managed via the Services control panel utility. Under the list of services, find Tenable PVS Proxy Service. Right click on the service to provide a list of options for the services, including the ability to start or stop the Tenable PVS or Tenable PVS Proxy service.

File Locations

PVS installs its files in the following locations:

<table>
<thead>
<tr>
<th>Path</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\Tenable\PVS</td>
<td>Contains PVS binaries and dependent libraries.</td>
</tr>
<tr>
<td>C:\ProgramData\Tenable\PVS</td>
<td>Contains all data files consumed and output by PVS and PVS Proxy (e.g., configuration, plugins, logs, and reports).</td>
</tr>
</tbody>
</table>

Note: This directory does not appear unless the Windows Hidden Files and Folders option is enabled.

The following table contains the folder layout under C:\ProgramData\Tenable\PVS:

<table>
<thead>
<tr>
<th>Folder</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>docs</td>
<td>Contains the software license agreement for PVS.</td>
</tr>
<tr>
<td>pvs</td>
<td>Parent folder for PVS logs, reports, plugins, and scripts directories. Also contains the pvs-services file.</td>
</tr>
<tr>
<td>Folder</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>db</td>
<td>Contains the database files relating to the configuration, reports, and users for PVS.</td>
</tr>
<tr>
<td>kb</td>
<td>Stores the PVS knowledge base, if used.</td>
</tr>
<tr>
<td>logs</td>
<td>Contains PVS logs.</td>
</tr>
<tr>
<td>plugins</td>
<td>Contains the PVS plugins delivered via SecurityCenter, Tenable.io, the PVS Feed, or updated via the command line or web interface if PVS is running in Offline mode.</td>
</tr>
<tr>
<td>pvs-services</td>
<td>A file PVS uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.</td>
</tr>
<tr>
<td>reports</td>
<td>Contains reports generated by PVS with the exception of .nsr. This folder contains the .nessus file generated by default.</td>
</tr>
<tr>
<td>scripts</td>
<td>Contains the files for the PVS Web server.</td>
</tr>
<tr>
<td>ssl</td>
<td>Contains SSL certificates used by the proxy and web server for the SSL connection between itself and SecurityCenter CV or the web browser.</td>
</tr>
<tr>
<td>users</td>
<td>Contains folders for user files and reports.</td>
</tr>
<tr>
<td>www</td>
<td>Contains the files for the PVS web front-end.</td>
</tr>
<tr>
<td>pvs-proxy</td>
<td>Parent folder for files used/created by the PVS proxy.</td>
</tr>
<tr>
<td>logs</td>
<td>Contains PVS proxy and PVS proxy service logs.</td>
</tr>
<tr>
<td>scans</td>
<td>By default, PVS creates the .nsr file in the scans folder. The proxy is then responsible for handling the report to SecurityCenter CV when SecurityCenter CV attempts to pull it.</td>
</tr>
<tr>
<td>run</td>
<td>Contains process ID temporary files.</td>
</tr>
</tbody>
</table>
macOS Command Line Operations

You must run all programs as a root user or with equivalent privileges.

Start or Stop PVS

<table>
<thead>
<tr>
<th>Action</th>
<th>Command to Manage PVS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td># launchctl load -w /Library/LaunchDaemons/com.tenablesecurity.pvs-proxy.plist</td>
</tr>
<tr>
<td>Stop</td>
<td># launchctl unload -w /Library/LaunchDaemons/com.tenablesecurity.pvs-proxy.plist</td>
</tr>
</tbody>
</table>

File Locations

PVS installs its files in the following locations:

<table>
<thead>
<tr>
<th>Path</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Library/PVS</td>
<td>Base directory.</td>
</tr>
<tr>
<td>/Library/PVS/docs</td>
<td>Contains the PVS license agreement in various file formats.</td>
</tr>
<tr>
<td>/Library/PVS/bin</td>
<td>Location of the PVS and PVS Proxy executables, plus several helper tools for the PVS Proxy daemon.</td>
</tr>
<tr>
<td>/Library/PVS/var/pvs</td>
<td>Contains plugins, discovered vulnerabilities, log files, keys, and other miscellaneous items.</td>
</tr>
<tr>
<td>db</td>
<td>Contains the database files relating to the configuration, reports, and users for PVS.</td>
</tr>
<tr>
<td>kb</td>
<td>Stores the PVS knowledge base, if used.</td>
</tr>
<tr>
<td>logs</td>
<td>Contains PVS logs.</td>
</tr>
<tr>
<td>plugins</td>
<td>Contains the PVS plugins delivered via SecurityCenter, Tenable.io, the PVS Feed, or updated via the command line or web interface if PVS is running in Offline mode.</td>
</tr>
<tr>
<td>Path</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><strong>Note:</strong> Do not change this path from the default /Library/PVS/var/pvs if SecurityCenter CV is being used to manage the plugins.</td>
<td></td>
</tr>
<tr>
<td>pvs-services</td>
<td>A file PVS uses to map service names to ports. This file may be edited by the user. Plugin updates do not overwrite modifications to the file.</td>
</tr>
<tr>
<td>reports</td>
<td>Contains reports generated by PVS with the exception of .nsr. This folder contains the .nessus file generated by default.</td>
</tr>
<tr>
<td>scripts</td>
<td>Contains the files for the PVS Web server.</td>
</tr>
<tr>
<td>ssl</td>
<td>Contains SSL certificates used by the proxy and web server for the SSL connection between itself and SecurityCenter CV or the web browser.</td>
</tr>
<tr>
<td>users</td>
<td>Contains files and reports for PVS users.</td>
</tr>
<tr>
<td>www</td>
<td>Contains the files for the PVS web front-end.</td>
</tr>
<tr>
<td>/Library/PVS/var/pvs-proxy</td>
<td>Parent folder for files used/created by the PVS proxy.</td>
</tr>
<tr>
<td>logs</td>
<td>Contains PVS proxy and PVS proxy service logs.</td>
</tr>
<tr>
<td>scans</td>
<td>By default, PVS creates the .nsr file in the scans folder. The proxy is then responsible for handing the report to SecurityCenter CV when SecurityCenter CV attempts to pull it.</td>
</tr>
</tbody>
</table>
Unknown or Customized Ports

Many networks contain traffic on ports PVS defines as different traffic types or alternate ports. If the port is not defined at all, it displays as Unknown. The pvs-services file may be edited to either customize or add the port information to provide accurate reporting for ports on the network.

For example, by default, there are two lines in the pvs-services file that define SMTP traffic. They read smtp 25/tcp and smtp 25/udp. If the organization routinely sends SMTP data over port 2525 those lines can be updated to read smtp 2525/tcp and smtp 2525/udp.
Real-Time Traffic Analysis Configuration Theory

This section describes how configuration options affect PVS operation and provides the following details on PVS architecture:

- **Focus Network**
- **Detecting Server and Client Ports**
- **Detecting Specific Server and Client Port Usage**
- **Firewall Rules**
- **Working with SecurityCenter**
- **Selecting Rule Libraries and Filtering Rules**
- **Detecting Encrypted and Interactive Sessions**
- **Routes and Hop Distance**
- **Alerting**
Focus Network

When a focus network is specified via the **networks** keyword, only one side of a session must match on the list. For example, if you have a DMZ that is part of the focus network list, PVS reports on vulnerabilities of the web server there, but not on web clients visiting from outside the network. However, a web browser within the DMZ visiting the same web server is reported.

In the diagram above, three sessions labeled A, B, and C are shown communicating to, from, and inside a focus network. In session A, PVS analyzes only those vulnerabilities observed on the server inside the focus network and does not report client side vulnerabilities. In session B, PVS ignores vulnerabilities on the destination server, but reports client side vulnerabilities. In session C, both client and server vulnerabilities are reported.

There is another filter that PVS uses while looking for unique sessions. This is a dependency that requires the host to run a major service. These dependencies are defined by a list of PVS plugin IDs that identify SSL, FTP, and several dozen other services.

Finally, the entire process of detecting these sessions can be filtered by specific network ranges and ports. For example, if a University ran a public FTP server that had thousands of downloads each hour, they may want to disable interactive sessions on port 21 on that FTP server. Similarly, disabling encryption detection on ports such as 22 and 443 also eliminates some noise for PVS.
Detecting Server and Client Ports

The method used by TCP connections to initiate communication is known as the “three-way handshake.” This method can be compared to how a common telephone conversation is initiated. If Bob calls Alice, he has effectively sent her, in TCP terms, a “SYN” packet. She may or may not answer. If Alice answers, she has effectively sent a “SYN-ACK” packet. The communication is still not established, since Bob may have hung up as she was answering. The communication is established when Bob replies to Alice, sending her an “ACK.”

The PVS configuration option “connections to services” enables PVS to log network client to server activity.

Whenever a system within the monitored network range tries to connect to a server over TCP, the connecting system emits a TCP “SYN” packet. If the port the client connects on is open, then the server responds with a TCP “SYN/ACK” packet. At this point, PVS records both the client address and the server port the client connects to. If the port on the server is not open, then the server does not respond with a TCP “SYN/ACK” packet. In this case, since PVS never sees a TCP “SYN/ACK” response from the server, PVS does not record the fact that the client tried to connect to the server port, since the port is not available to that client.

The **Connections to Services** configuration parameter does not track how many times the connection was made. If the same host browses the same web server a million times, or browses a million different web servers once, the host is still marked as having browsed on port 80. This data is logged as PVS internal plugin ID 2.

PVS detects many applications through plugin and protocol analysis. At a lower level, PVS also detects open ports and outbound ports in use on the monitored networks. By default, PVS detects any TCP server on the protected network if it sees a TCP “SYN-ACK” packet.

In combination, the detection of server ports and client destination ports allows a network administrator to see who on their network is serving a particular protocol and who on their network is speaking that protocol.
Detecting Specific Server and Client Port Usage

The **Show Connections** configuration parameter keeps track of host communication within the focus network. When the **Show Connections** configuration parameter is enabled, if one of the hosts is in the defined focus network, PVS records the client, server, and server port every time a host connects to another host. It does not track the frequency or time stamp of the connections – just that a connection was made.

The **Show Connections** configuration parameter provides a greater level of detail than the **Connections to Services** configuration parameter. For example, if your IPv4 address is 1.1.1.1 or your IPv6 address is 2001:DB8::AE59:3FC2 and you use the SSH service to connect to “some_company.com” then the use of these options records the following:

**Show Connections**

```
some_company.com:SSH
2001:DB8::AE59:3FC2 -> some_company.com
```

**Connections to Services**

```
SSH
2001:DB8::AE59:3FC2 -> SSH
```

Using the **Connections to Services** configuration parameter lets you know that the system at 1.1.1.1 and 2001:DB8::AE59:3FC2 uses the SSH protocol. This information may be useful regardless of where the service is used.

PVS does not log a session-by-session list of communications. Instead, it logs the relationship between the systems. For example, if system A is detected using the SSH protocol on port 22 connecting to system B, and both systems are within the focus network, PVS would log:

- System A browses on port 22
- System B offers a service (listens) on port 22
- System A communicates with System B on port 22
If system B were outside of the focus network, PVS would not record anything about the service System B offers, and would also log that System A browses outside of the focus network on port 22. PVS does not log how often a connection occurs, only that it occurred at least once. For connections outside of the focus network, PVS logs only which ports are browsed, not the actual destinations.

**Note:** If logging session-by-session network events is a requirement for your network analysis, Tenable offers the LCE product, which can log firewall, web server, router, and sniffer logs.
Firewall Rules

If PVS is placed immediately behind a firewall such that all of the traffic presented to PVS flows through the firewall, then the list of served ports, client side ports, and the respective IP addresses of the users are readily available. Tools such as SecurityCenter CV's Vulnerability Analysis interface allow information about these ports (both client and server) to be browsed, sorted, and reported on. You can also view lists of IP addresses and networks using these client and server ports.
Working with SecurityCenter CV

When SecurityCenter CV manages multiple PVS sensor, users of SecurityCenter CV can analyze the aggregate types of open ports, browsed ports, and communication activity that occurs on the focus network. Since SecurityCenter CV has several different types of users and privileges, many different IT and network engineering accounts can be created across an enterprise so they can share and benefit from the information detected by PVS.
Selecting Rule Libraries and Filtering Rules

Tenable ships an encrypted library of passive vulnerability detection scripts. This file cannot be modified by the end users of PVS. However, if certain scripts must be disabled, they can be specified by the PASL ID and “.pasl” appended. For example, 1234.pasl, disables the PASL with the ID of 1234 on a single line in the disabled-scripts.txt file.

If a plugin must be disabled, enter its ID on a single line in the disabled-plugins.txt file. If a plugin must be real-time enabled, enter its ID on a single line in the realtime-plugins.txt file.

When adding PVS plugins to the disabled plugin list, be sure to leave an empty blank line after entering in the last plugin to be disabled. Failure to return to the next line can result in a non-functional disabled plugin list.

Example: 1234 [return]

If any of the referenced files do not exist, create them using the appropriate method for the operating system. The file locations are in the following table for each operating system:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/opt/pvs/var/pvs</td>
</tr>
<tr>
<td>Windows</td>
<td>C:\ProgramData\Tenable\PVS\pvs</td>
</tr>
<tr>
<td>macOS</td>
<td>/Library/PVS/var/pvs</td>
</tr>
</tbody>
</table>

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
Detecting Encrypted and Interactive Sessions

PVS can be configured to detect both encrypted and interactive sessions. An encrypted session is a TCP or UDP session that contains sufficiently random payloads. An interactive session uses timing and statistical profiling of the packets in a session to determine if the session involves human input at a command line prompt.

In both cases, PVS identifies these sessions for the given port and IP protocol. It then lists the detected interactive or encrypted session as vulnerabilities.

PVS has a variety of plugins to recognize telnet, Secure Shell (SSH), Secure Socket Layer (SSL), and other protocols. Combined with the detection of the interactive and encryption algorithms, PVS may log multiple forms of identification for the detected sessions.

For example, PVS may recognize not only an SSH service running on a high port as an encrypted session, but also recognize the version of SSH and determine any vulnerabilities associated with it.
Routes and Hop Distance

For active scans, one host can find the default route and an actual list of all routers between it and a target platform. To do this, it sends one packet after another with a slightly larger TTL (time to live) value. Each time a router receives a packet, it decrements the TTL value and sends it on. If a router receives a packet with a TTL value of one, it sends a message back to the originating server stating that the TTL has expired. The server sends packets to the target host with greater and greater TTL values and collects the IP addresses of the routers sending expiration messages in-between.

Since PVS is entirely passive, it cannot send or elicit packets from the routers or target computers. It can however, record the TTL value of a target machine. The TTL value is an 8-bit field, which means it can contain a value between 0 and 255. Most machines use an initial TTL value of 32, 64, 128, or 255. Since there is a maximum of 16 hops between your host and any other host on the internet, PVS uses an algorithm to map any TTL to the number of hops.

For example, if PVS sniffed a server sending a packet with a TTL of 126, it detects that 128 is two hops away. PVS does not know the IP address of the in-between routers.

**Note:** Modern networks have many devices such as NAT firewalls, proxies, load balancers, intrusion prevention, routers, and VPNs that rewrite or reset the TTL value. In these cases, PVS may report inconsistent hop counts.
Alerting

When PVS detects a real-time event, it can:

- Send the event to a local log file.
- Send the event via Syslog to a log aggregator such as Tenable’s LCE, an internal log aggregation server.
- Send the event to a third party security event management vendor.

New Host Alerting

You can configure PVS to detect when a new host has been added to the network. By default, PVS has no knowledge of your network’s active hosts, so the first packets PVS sniffs trigger an alert. To avoid this, you can configure PVS to learn the network over a period of days. Once this period is over, any “new” traffic must be from a host that has not communicated during the initial training.

When PVS logs a new host, the Ethernet address saves in the message. When PVS is more than one hop away from the sniffed traffic, the Ethernet address is that of the local switch and not the actual host. If the scanner is deployed in the same collision domain as the sniffed server, then the Ethernet address is accurate.

For DHCP networks, PVS often detects a “new” host. Tenable recommends deploying this feature on non-volatile networks such as DMZ. Users should also consider analyzing PVS “new” host alerts with SecurityCenter CV, which can sort real-time PVS events by networks.
Internal PVS Plugin IDs

Each vulnerability and real-time check PVS performs has a unique associated ID. PVS IDs are within the range 0 to 10000.

Internal PVS IDs

Some of PVS's checks, such as detecting open ports, are built in. The following chart lists some of the more commonly encountered internal checks and describes what they mean:

<table>
<thead>
<tr>
<th>PVS ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Detection of Open Port</td>
<td>PVS has observed a SYN-ACK leave from a server.</td>
</tr>
<tr>
<td>1</td>
<td>Operating System Fingerprint</td>
<td>PVS has observed enough traffic about a server to guess the operating system.</td>
</tr>
<tr>
<td>2</td>
<td>Service Connection</td>
<td>PVS has observed browsing traffic from a host.</td>
</tr>
<tr>
<td>3</td>
<td>Internal Client Trusted Connections</td>
<td>PVS has logged a unique network session of source IP, destination IP, and destination port.</td>
</tr>
<tr>
<td>4</td>
<td>Internal Interactive Session</td>
<td>PVS has detected one or more interactive network sessions between two hosts within your focus network.</td>
</tr>
<tr>
<td>5</td>
<td>Outbound Interactive Sessions</td>
<td>PVS has detected one or more interactive network sessions originating from within your focus network and destined for one or more addresses on the Internet.</td>
</tr>
<tr>
<td>6</td>
<td>Inbound Interactive Sessions</td>
<td>PVS has detected one or more interactive network sessions originating from one or more addresses on the Internet to this address within your focus network.</td>
</tr>
<tr>
<td>7</td>
<td>Internal Encrypted Session</td>
<td>PVS has detected one or more encrypted network sessions between two hosts within your focus network.</td>
</tr>
<tr>
<td>8</td>
<td>Outbound Encrypted Session</td>
<td>PVS has detected one or more encrypted network sessions originating from within your focus network and destined for one or more addresses on the Internet.</td>
</tr>
<tr>
<td>9</td>
<td>Inbound Encrypted Session</td>
<td>PVS has detected one or more encrypted network sessions originating from one or more addresses on the Internet to</td>
</tr>
<tr>
<td>PVS ID</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>this address within your focus network.</td>
</tr>
<tr>
<td>12</td>
<td>Number of Hops</td>
<td>PVS logs the number of hops away each host is located.</td>
</tr>
<tr>
<td>14</td>
<td>Accepts External Connections</td>
<td>PVS detects an external connection to this host. Specific IP addresses are not reported by this plugin, but it does track the destination port and protocol used. You can view full connection details in the real-time event log. This is the opposite of plugin 16, which reports on outbound connections.</td>
</tr>
<tr>
<td>15</td>
<td>Internal Server Trusted Connections</td>
<td>PVS has logged a unique network session of source IP, destination IP, and destination port. Specific IP addresses are not reported by this plugin, but it does track which destination port and protocol was used. You can view full connection details in the real-time event log. This is the opposite of plugin 14, which reports on inbound connections.</td>
</tr>
<tr>
<td>16</td>
<td>Outbound External Connection</td>
<td>PVS has detected an external connection from this host.</td>
</tr>
<tr>
<td>17</td>
<td>TCP Session</td>
<td>PVS identifies TCP sessions and reports the start time, number of bytes of data downloaded during, and end time of these sessions. This plugin is reported at the end of each TCP session.</td>
</tr>
<tr>
<td>18</td>
<td>IP Protocol Detection</td>
<td>PVS detects all IP protocols.</td>
</tr>
<tr>
<td>19</td>
<td>VLAN ID Reporting</td>
<td>PVS reports all observed VLAN tags per host.</td>
</tr>
<tr>
<td>20</td>
<td>IPv6 Tunneling</td>
<td>PVS identifies and processes tunneled IPv6 traffic.</td>
</tr>
</tbody>
</table>
PVS Plugins

This section provides the following information about PVS plugins:

- [Vulnerability and Passive Fingerprinting](#)
- [PVS Fingerprinting](#)
- [PVS Plugin Syntax](#)
- [PVS Real-Time Plugin Syntax](#) and [Examples](#)
- [PVS Corporate Policy Plugins](#)
About PVS Plugins

PVS has two sources of plugin information: the .prmx and .prm plugin libraries in the plugins directory.

Tenable distributes its passive vulnerability plugin database in an encrypted format. The encrypted file is named tenable_plugins.prmx and, if necessary, can be updated daily. PVS plugins written by the customer or third parties have the .prm extension.

Tenable has also implemented passive fingerprinting technology based on the open-source SinFP tool. With permission from the author, Tenable includes the database of passive operating system fingerprints for the fingerprinting technology in this distribution of PVS.

Writing Custom Plugins

PVS customers can write their own passive plugins, which are added into the plugins directory in the PVS installation directory. The plugin must end with a .prm extension to be visible by PVS.

You must restart PVS if:

- You add a new custom plugin to the plugins directory. PVS does not fire the plugin until you restart.
- You delete a .prm file manually from the plugins directory. PVS continues to fire the plugin until you restart.
PVS Fingerprinting

Tenable uses a hybrid approach to operating system fingerprinting. Primarily, plugins are used to detect and identify the OS of a host. If this is not possible, PVS uses detected packets to identify the OS.

PVS has the ability to guess the operating system of a host by looking at the packets it generates. Specific combinations of TCP packet entries, such as the window size and initial time-to-live (TTL) values, allow PVS to predict the operating system generating the traffic.

These unique TCP values are present when a server makes or responds to a TCP request. All TCP traffic is initiated with a “SYN” packet. If the server accepts the connection, it sends a response known as a “SYN-ACK” packet. If the server cannot or will not communicate, it sends a reset (RST) packet. When a server sends a “SYN” packet, PVS applies these list of operating system fingerprints and attempts to determine the operating system type.

Tenable Network Security has permission to re-distribute the passive operating fingerprints from the author of SinFP open source project.
PVS Plugin Syntax

Plugins

PVS plugins allow spaces and comment fields that start with a number (#) sign. Each plugin must be separated with the word “NEXT” on a single line. Create a .prm file in the plugins directory to make it available for use. You must restart PVS to use new custom plugins.

Plugin Keywords

There are several keywords available for writing passive vulnerability plugins for PVS. Some of these keywords are mandatory and some are optional. In the table below, mandatory keywords are highlighted in blue.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bid</td>
<td>Tenable assigns SecurityFocus Bugtraq IDs (BID) to PVS plugins. This allows a user reading a report generated by PVS to link to more information available at <a href="http://www.securityfocus.com/bid">http://www.securityfocus.com/bid</a>. Multiple Bugtraq entries can be entered on one line if separated by commas.</td>
</tr>
<tr>
<td>bmatch</td>
<td>This is the same as match but can look for any type of data. A bmatch must always have an even number of alphanumeric characters.</td>
</tr>
<tr>
<td>clientissue</td>
<td>If a vulnerability is determined in a network client such as a web browser or an email tool, a server port is associated with the reported vulnerability.</td>
</tr>
<tr>
<td>cve</td>
<td>Tenable also assigns Common Vulnerability and Exposure (CVE) tags to each PVS plugin. This allows a user reading a report generated by PVS to link to more information available at <a href="http://cve.mitre.org/">http://cve.mitre.org/</a>. Multiple CVE entries can be entered on one line if separated by commas.</td>
</tr>
<tr>
<td>dependency</td>
<td>This is the opposite of noplugin. Instead of specifying another plugin that has failed, this keyword specifies which plugin must succeed. This keyword specifies a PVS ID that should exist to evaluate the plugin. In addition, this plugin can take the form of dependency=ephemeral-server-port, which means the evaluated server must have an open port above port 1024.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dport</td>
<td>This is the same as <strong>sport</strong>, but for destination ports.</td>
</tr>
</tbody>
</table>
| Exploitability: | Displays exploitability factors for the selected vulnerability. For example, if the vulnerability is exploitable via both Canvas and Core and has a unique CVSS temporal score, the following tags may be displayed in the plugin output:  
  - CANVAS : D2ExploitPack  
  - CORE : true  
  - CVSSTEMPORAL : CVSS2#E:F/RL:OF/RC:C                                                                                                                                                                                                                                           |
<p>| canvas |                                                                                                                                                                                                                                                                                                                                           |
| core   |                                                                                                                                                                                                                                                                                                                                           |
| cvsstemporal |                                                                                                                                                                                                                                                                                                                                           |
| metasploit |                                                                                                                                                                                                                                                                                                                                         |
| family | Each Tenable plugin for PVS is included in a family. This designation allows Tenable to group PVS plugins into easily managed sets that can be reported on individually.                                                                                                                                                                        |
| hs_dport | This is the same as <strong>hs_sport</strong> except for destination ports.                                                                                                                                                                                                                                                                              |
| hs_sport | Normally, when PVS runs its plugins, they are either free ranging looking for matches on any port, or fixed to specific ports with the <strong>sport</strong> or <strong>dport</strong> keywords. In very high speed networks, many plugins have a fallback port, known as a high-speed port, which focuses the plugin only on one specific port. In High Performance mode, the performance of a PVS plugin with an <strong>hs_sport</strong> keyword is exactly the same as if the plugin was written with the <strong>sport</strong> keyword. |
| id     | Each PVS plugin needs a unique rule ID. Tenable assigns these 16 bit numbers within the overall PVS range of valid entries. A list of the current PVS plugin IDs can be found on the <a href="https://tenable.com">Tenable website</a>.                                                                                                                                                      |
| match  | This keyword specifies a set of one or more simple ASCII patterns that must be present in order for the more complex pattern analysis to take place. The <strong>match</strong> keyword gives PVS a lot of its performance and functionality. With this keyword, if it does not see a simple pattern, the entire plugin does not match.                                                                                                                       |
| name   | This is the name of the vulnerability PVS has detected. Though multiple PVS plugins can have the same name, it is not encouraged.                                                                                                                                                                                                            |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nid</td>
<td>To track compatibility with the Nessus vulnerability scanner, Tenable associates PVS vulnerability checks with relevant Nessus vulnerability checks. Multiple Nessus IDs can be listed under one nid entry such as nid=10222,10223.</td>
</tr>
<tr>
<td>nooutput</td>
<td>For plugins that are written specifically to be used as part of a dependency with another plugin, the nooutput keyword causes PVS not to report anything for any plugin with this keyword enabled.</td>
</tr>
<tr>
<td>noplugi</td>
<td>This keyword prevents a plugin from being evaluated if another plugin has already matched. For example, it may make sense to write a plugin that looks for a specific anonymous FTP vulnerability, but disable it if another plugin that checked for anonymous FTP has already failed.</td>
</tr>
<tr>
<td>pbmatch</td>
<td>This is the same as bmatch except for binary data on the previous side of the reconstructed network session.</td>
</tr>
<tr>
<td>plugin_output</td>
<td>This keyword displays dynamic data for a given vulnerability or event. The dynamic data is usually represented using %L or %P, and its value is obtained from the regular expressions defined using regex, regexi, pregex, or pregexi.</td>
</tr>
<tr>
<td>pmatch</td>
<td>This keyword is the same as match but is applied against the previous packet on the other side of the reconstructed network session.</td>
</tr>
<tr>
<td>pregex</td>
<td>This is the same as regex except the regular expression is applied to the previous side of the reconstructed network session.</td>
</tr>
<tr>
<td>pregexi</td>
<td>This is the same as pregex except the pattern matching is not case sensitive.</td>
</tr>
<tr>
<td>protocol_id</td>
<td>This keyword is used to specify the protocol number of the protocol causing the plugin to fire.</td>
</tr>
<tr>
<td>regex</td>
<td>This keyword specifies a complex regular expression search rule applied to the network session.</td>
</tr>
<tr>
<td>regexi</td>
<td>This is the same as regex except the pattern matching is not case sensitive.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>risk</td>
<td>All PVS plugins need a risk setting. Risks are classified as INFO, LOW, MEDIUM, HIGH, and CRITICAL. An INFO risk is an informational vulnerability such as client or server detection. A LOW risk is an informational vulnerability such as an active port or service. A MEDIUM risk is something that may be exploitable or discloses information. A HIGH risk is something that is easily exploitable. A CRITICAL risk is something that is very easily exploitable and allows for malicious attacks.</td>
</tr>
<tr>
<td>seealso</td>
<td>If one or more URLs are available, this keyword can be used to display them. Multiple URLs can be specified on one line if separated by commas. Example entries for this include CERT advisories and vendor information websites.</td>
</tr>
<tr>
<td>solution</td>
<td>If a solution is available, it can be described here. The report section highlights the solution with different text.</td>
</tr>
<tr>
<td>sport</td>
<td>This setting applies the PVS plugin to just one port. For example, you may wish to write a SNMP plugin that just looks for activity on port 162. However, for detection of off-port services like a web server running on port 8080, a <strong>sport</strong> field is not used in the plugin.</td>
</tr>
<tr>
<td>stripped_description</td>
<td>This field describes on one line the nature of the detected vulnerability. This data is printed out by PVS when printing the vulnerability report. Macros are available that allow the printing of matched network traffic such as banner information and are discussed in the examples below. For line breaks, the characters “\n” can be used to invoke a new line.</td>
</tr>
<tr>
<td>timed-dependency</td>
<td>This keyword slightly modifies the functionality of the <strong>noplugin</strong> and <strong>dependency</strong> keywords such that the evaluation must have occurred within the last N seconds.</td>
</tr>
<tr>
<td>udp</td>
<td>This keyword specifies that plugins are to be based on the UDP protocol rather than TCP protocol.</td>
</tr>
</tbody>
</table>

**Tip:** In addition to tcp or udp, the following protocols are supported: sctp, icmp, igmp, ipip, egp, pup, idp, tp, rsvp, gre, pim, esp, ah, mtp, encap, comp, raw or other.

Related Information

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
• Network Client Detection
• Pattern Matching
• Time Dependent Plugins
• Plugin Examples
Network Client Detection

Match patterns that begin with the \^ symbol mean at least one line in the packet payload must begin with the following pattern. Match patterns that begin with the ! symbol indicate that the string must NOT match anything in the packet payload. In this case, the ! and \^ symbols are combined to indicate that PVS should not evaluate any packet whose payload contains a line starting with the pattern Received:

The \^ is more expensive to evaluate than the > symbol. So, while both match patterns \^<pattern> and >\<pattern> would find <pattern> at the beginning of a packet payload, the use of > is more desirable as it is less costly. Use \^ when looking for the occurrence of a string at the beginning of a line, but not at the beginning of the packet payload. In the latter case, use the > character instead.

```
id=79526
hs_dport=25
clientissue
name=Buffer overflow in multiple IMAP clients
description=The remote e-mail client is Mozilla 1.3 or 1.4a which is vulnerable to a boundary condition error whereby a malicious IMAP server may be able to crash or execute code on the client.
solution=Upgrade to either 1.3.1 or 1.4a
risk=HIGH
match=\^From:
m.match=\^To:
m.match=\^Date:
m.match=\^User-Agent: Mozilla
m.match=!\^Received:
regex=\^User-Agent: Mozilla/.*
\(.*rv:(1\.|3|1\.|4a)
Pattern Matching

PVS Can Match "Previous" Packets

PVS allows matching on patterns in the current packet as well as patterns in the previous packet in the current session. This plugin shows how we can make use of this feature to determine if a Unix password file is sent by a web server:

```plaintext
id=79175
name=Password file obtained by HTTP (GET)
family=Generic
sport=80
description=It seems that a Unix password file was sent by the remote web server when the following request was made :\n\nWe saw : \n\n
pmatch=>GET /
pmatch=HTTP/1.
march=root
match=daemon
match=bin
regex=root:.*:0:0:*:*:*:
```

Here we see `match` patterns for a root entry in a Unix password file. We also see `pmatch` patterns that match against a packet that makes an HTTP GET request to a web server. The `match` patterns apply the current packet in a session and the `pmatch` patterns apply to the packet that was captured immediately before the one in the current session. To explain this visually, we are looking for occurrences of the following:

```
GET / HTTP/1.*
```

1) client -----------------> server:port 80

Contents of password file:

```
root:.*:0:0:*:*:*:
```

2) client <--------------------- server:port 80

Our `match` pattern would focus on the contents in packet 2) and our `pmatch` pattern would focus on packet 1) payload contents.

PVS Can Match Binary Data
PVS also allows matching against binary patterns. Here is an example plugin that makes use of binary pattern matching to detect the usage of the well-known community string “public” in SNMPv1 response packets (The “#” is used to denote a comment):

```plaintext
###
# SNMPv1 response
# Matches on the following:
# 0x30 - ASN.1 header
# 0x02 0x01 0x00 - (integer) (byte length) (SNMP version - 1)
# 0x04 0x06 public - (string) (byte length) (community string - "public")
# 0xa2 - message type - RESPONSE
# 0x02 0x01 0x00 - (integer) (byte length) (error status - 0)
# 0x02 0x01 0x00 - (integer) (byte length) (error index - 0)
###
id=71975
udp
sport=161
name=SNMP public community string
description=The remote host is running an SNMPv1 server that uses a well-known community string - public
bmatch=>0:30
bmatch=>2:020100
bmatch=>5:04067075626c6963a2
bmatch=020100020100
```

Binary match patterns take the following form:

```
bmatch=[<>[off]:]<hex>
```

Binary match starts at <off>'th offset of the packet or at the last <offset> of the packet, depending on the use of > (start) or < (end). <hex> is a hex string we look for.

```
bmatch=<:ffffffff
```
This matches any packet whose last four bytes are set to 0xFFFFFFFF.

```
bmatch=>4:41414141
```
This matches any packet that contains the string “AAAA” (0x41414141 in hex) starting at its fourth byte.

```
bmatch=123456789ABCDEF5
```
This matches any packet that contains the hex string above.
Negative Matches

PVS plugins can also be negated. Here are two examples:

```
pmatch=!pattern
pbmatch=>0:!414141
```

In each of these cases, the plugin does not match if the patterns contained in these “not” statements are present. For example, in the first `pmatch` statement, if the pattern named “pattern” is present, then the plugin does not match. In the second statement, the binary pattern of “AAA” (the letter “A” in ASCII hex is 0x41) only matches if it does not present the first three characters.
Time Dependent Plugins

The last plugin example shows some more advanced features of the PVS plugin language that allows a plugin to be time dependent as well as make use of the evaluation of other plugins. The plugin shows how PVS detects an anonymous FTP server. Use the **NEXT** keyword to separate plugins in the plugin file.

```plaintext
id=79200
nououtput
hs_sport=21
name=Anonymous FTP (login: ftp)
pmatch=^USER ftp
match=^331
NEXT #-----------------------------------------------
```

```plaintext
id=79201
dependency=79200
timed-dependency=5
hs_sport=21
name=Anonymous FTP enabled
description=The remote FTP server has anonymous access enabled.
risk=LOW
pmatch=^PASS
match=^230
```

Since we want to detect an anonymous FTP server, we must look for the following traffic pattern:

```
USER ftp
1) FTP client ----------------------> FTP server
   331 Guest login ok, ...
2) FTP client <---------------------- FTP server
   PASS joe@fake.com
3) FTP client ----------------------> FTP server
   230 Logged in
4) FTP client <---------------------- FTP server
```

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
Here we cannot use a single plugin to detect this entire session. So, instead we use two plugins: the first plugin looks for packets 1) and 2) and the second plugin looks for packets 3) and 4).

A review of the above plugin shows that plugin 79200 matches 1) and 2) in the session by keying on the patterns “USER ftp” and the 331 return code. Plugin 79201 matches on 3) and 4) by keying on the patterns “PASS” and the 230 return code.

Notice that plugin 79201 contains the following field: dependency=79200. This field indicates the plugin 79200 must evaluate successfully before plugin 79201 may be evaluated.

To complete the plugin for the anonymous FTP session, we must ensure both plugins are evaluating the same FTP session. To do this, we attach a time dependency to plugin 79201. The field time-dependency=5 indicates that plugin 79200 must evaluate successfully in the last five seconds for 79201 to evaluate. This way, we can ensure that both plugins evaluate the same FTP session.
Plugin Examples

Basic Example

This plugin illustrates the basic concepts of PVS plugin writing:

```
id=79873
nid=11414
hs_sport=143
name=IMAP Banner
description=An IMAP server is running on this port. Its banner is :::\n%L
risk=NONE
match=OK
match=IMAP
match=server ready
regex=^.*OK.*IMAP.*server ready
```

This example uses the following fields:

- **id** - A unique number assigned to this plugin.
- **nid** - The Nessus ID of the corresponding Nessus NASL script.
- **hs_sport** - The source port to key on if High Performance mode is enabled.
- **name** - The name of the plugin.
- **description** - A description of the problem or service.
- **match** - The set of match patterns that must be found in the payload of the packet before the regular expression can be evaluated.
- **regex** - The regular expression to apply to the packet payload.

**Tip:** The description contains the %L macro. If this plugin evaluates successfully, then the string pattern in the payload that matched the regular expression is stored in %L and prints out at report time.

Complex Example

```
id=79004
nid=10382
```
cve=CVE-2000-0318
bid=1144
hs_sport=143
name=Atrium Mercur Mailserver
description=The remote imap server is Mercur Mailserver 3.20. There is a flaw in this server (present up to version 3.20.02) which allow any authenticated user to read any file on the system. This includes other user mailboxes, or any system file.
Warning : this flaw has not been actually checked but was deduced from the server banner
solution=There was no solution ready when this vulnerability was written; Please contact the vendor for updates that address this vulnerability.
risk=HIGH
match=>*  OK
match=MERCUR
match=IMAP4-Server
regex=\^\*  OK.*MERCUR  IMAP4-Server.*v3\.20\..*$

Tip: The first match pattern makes use of the > symbol. The > symbol indicates that the subsequent string must be at the beginning of the packet payload. Use of the > symbol is encouraged where possible as it is an inexpensive operation.

Case-Insensitive Example

There is a tool called **SmartDownLoader** that uploads and downloads large files. Unfortunately, versions 0.1 through 1.3 use the capitalization **SmartDownloader**, versions 1.4 through 2.7 use **smartdownloader** and versions 2.8 through current use **SMARTdownloader**. Searching for the various combinations of this text with purely the `regex` command would cause us to use a statement that looks like this:

`regex=[sS][mM][aA][rR][tT][dD]own[lL]oader`

However, with the `regexi` command, the search string is much less complex and less prone to creating an error:

`regexi=smartdownloader`

By using `regexi`, we can more quickly match on all three versions as well as future permutations of the string **smartdownloader**. In a case such as this, `regexi` is the logical choice.
A complete example PVS plugin using the `regexi` keyword is shown above. The use of the `match` keyword searching for the string `ownloader` is not a typo. By searching for network sessions that have this string in them first, PVS can avoid invoking the expensive `regexi` search algorithm unless the `ownloader` pattern is present.
PVS Real-Time Plugin Syntax

Real-Time Plugin Model

PVS real-time plugins are exactly the same as PVS vulnerability plugins with two exceptions:

- They can occur multiple times.
- Their occurrence may not be recorded as a vulnerability.

For example, an attacker may attempt to retrieve the source code for a Perl script from an Apache web server. If PVS observes this event, it would be logical to send a real-time alert. It would also be logical to mark that the Apache server is potentially vulnerable to some sort of Perl script source code download. In other cases, it may be more logical to just log the attempt as an event, but not a vulnerability. For example, a login failure over FTP is an event that may be worth logging, but does not indicate a vulnerability.

As the real-time plugins are written, there are two keywords that indicate to PVS that these are not regular vulnerability plugins. These are the \texttt{real-time} and \texttt{realtimeonly} keywords.

In the previous example, the FTP user login failure would be marked as a \texttt{realtimeonly} event because we would like real-time alerting, but not a new entry into the vulnerability database.

Real-Time Plugin Keywords

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{real-time}</td>
<td>If a plugin has this keyword, then PVS will generate a SYSLOG message or real-time log file entry the first time this plugin matches. This prevents vulnerabilities that are worm related from causing millions of events. For example, the plugins for the Sasser worm generate only one event. Output from plugins with this keyword will show up in the vulnerability report.</td>
</tr>
<tr>
<td>\texttt{realtimeonly}</td>
<td>If a plugin has this keyword, then PVS will generate a SYSLOG message or real-time log file entry each time the plugin evaluates successfully. These plugins never show up in the report file.</td>
</tr>
<tr>
<td>\texttt{track-session}</td>
<td>This keyword will cause the contents of a session to be reported (via SYSLOG or the real-time log file) a specified number of times after the plugin containing this keyword was matched. This is an excellent way to discover what a hacker “did next” or possibly what the contents of a retrieved...</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>trigger-dep</td>
<td>Normally if a plugin has multiple dependencies, then all of those dependencies must be successful for the current plugin to evaluate. However, the trigger-dep keyword allows a plugin to be evaluated as long as at least one of its dependencies is successful.</td>
</tr>
<tr>
<td>file were</td>
<td>real-time.</td>
</tr>
<tr>
<td>file</td>
<td>were real-time.</td>
</tr>
</tbody>
</table>
Real-Time Plugin Examples

Failed Telnet Login Plugin

The easiest way to learn about PVS real-time plugins is to evaluate some of those included by Tenable. Below is a plugin that detects a failed Telnet login to a FreeBSD server.

```bash
# Look for failed logins into an FreeBSD telnet server
id=79400
hs_sport=23
dependency=1903
realtimeonly
name=Failed login attempt
description=PVS detected a failed login attempt to a telnet server
risk=LOW
match=Login incorrect
```

This plugin has many of the same features as a vulnerability plugin. The ID of the plugin is 79400. The high-speed port is 23. We need to be dependent on plugin 1903 (which detects a Telnet service). The `realtimeonly` keyword tells PVS that if it observes this pattern, then it should alert on the activity, but not record any vulnerability.

Under SecurityCenter CV, events from PVS are recorded alongside other IDS tools.

Finger User List Enumeration Plugin

The `finger` daemon is an older Internet protocol that allowed system users to query remote servers to get information about a user on that box. There have been several security holes in this protocol that allowed an attacker to elicit user and system information that could be useful to attackers.

```bash
id=79500
dependency=1277
hs_sport=79
track-session=10
realtimeonly
name=App Subversion - Successful finger query to multiple users
description=A response from a known finger daemon was observed which indicated that the attacker was able to retrieve a list of three or more valid user names.
risk=HIGH
```
This plugin looks for these patterns only on systems where a working finger daemon has been identified (dependency #1277). However, the addition of the track-session keyword means that if this plugin is launched with a value of 10, the session data from the next 10 packets is tracked and logged in either the SYSLOG or real-time log file.

During a normal finger query, if only one valid user is queried, then only one home directory will be returned. However, many of the exploits for finger involve querying for users such as NULL, .., or 0. This causes vulnerable finger daemons to return a listing of all users. In that case, this plugin would be activated because of the multiple “Directory:” matches.

Unix Password File Download Web Server Plugin

This plugin below looks for any download from a web server that does not look like HTML traffic, but does look like the contents of a generic Unix password file.

The plugin is dependent on PVS ID 1442, which detects web servers. In the match statements, we are attempting to ignore any traffic that contains valid HTML tags, but also has lines that start with common Unix password file entries.

Generic Buffer Overflow Detection on Windows Plugin
One of PVS’s strongest intrusion detection features is its ability to recognize specific services, and then to look for traffic occurring on those services that should never occur unless they have been compromised. Since PVS can keep track of both sides of a conversation and make decisions based on the content of each, it is ideal to look for Unix and Windows command shells occurring in services that should not have those command shells in them. Here is an example plugin:

```
# look for Windows error when a user tries to
# switch to a drive that doesn't exist
id=79201
include=services.inc
trigger-dependency
track-session=10
realtimeonly
name=Successful shell attack detected - Failed cd command
description=The results of an unsuccessful attempt to change drives on a Windows
machine occurred in a TCP session normally used for a standard service. This may
indicate a successful compromise of this service has occurred.
risk=HIGH
pmatch=!>GET
pregexi=cd
match=!>550
match=^The system cannot find the
match=specified.
```

This plugin uses the `include` keyword that identifies a file that lists several dozen PVS IDs, which identify well known services such as HTTP, DNS, and NTP. The plugin will not even get evaluated unless the target host is running one of those services.

The keyword `trigger-dependency` is needed to ensure the plugin is evaluated even if there is only one match in the `services.inc` file. Otherwise, PVS would evaluate this plugin only if the target host was running all PVS IDs present in the `services.inc` file. The `trigger-dependency` keyword basically says that at least one PVS ID specified by one or more dependency or include rules must be present.

Finally, the logic of plugin detection is looking for the following type of response on a Windows system:

```
C:\> cd someplace not there
The system cannot find the path specified.
C:\>
```

Copyright © 2017. Tenable Network Security, Inc. All rights reserved. Tenable Network Security, Nessus, SecurityCenter Continuous View, Passive Vulnerability Scanner, and Log Correlation Engine are registered trademarks of Tenable Network Security, Inc. All other products or services are trademarks of their respective owners.
In this case, a user has attempted to use the cd command to change directories within a file system and the attempt was not allowed. This is a common event that occurs when a remote hacker compromises a Windows 2000 or Windows 2003 server with a buffer overflow. The PVS plugin looks for a network session that should not be there.

Looking at the plugin logic, there are \texttt{pmatch} and \texttt{pregexi} statements that attempt to ensure that the session is not an HTTP session, and that the previous side of the session contains the string \texttt{cd}.

\textbf{Tip}: The \texttt{pregexi} statement could be expanded to include the trailing space after the “d” character and also the first character.

The plugin then looks for the expected results of the failed \texttt{cd} command. The first match statement makes sure this pattern is not part of the FTP protocol. It turns out that looking for “cd” in one side of a session and the error of attempting to change to a directory in an FTP session would cause false positives for this plugin. Adding a rule to ignore if a line starts with “550” avoids this. While writing and testing this plugin, Tenable considered having a different set of plugins just for FTP, but the additional filter statement took care of any false positives. Finally, the last two match statements look for the results of the failed change directory attempt. They are spread across two match statements and could have been combined into one regular expression statement, but there was enough content in the basic message to have them split into higher-speed matching.
PVS Corporate Policy Plugins

Most companies have an “Acceptable Use Policy” that defines appropriate use of the company's IT facilities. Often, this policy is abused to some extent since detecting abuse can be difficult.

PVS can help in this regard through use of PVS Corporate Policy plugins. These plugins can be used to look for policy violations and items such as credit card numbers, Social Security numbers, and other sensitive content in motion.

Tenable ships PVS with a large number of plugins that are frequently updated. The primary focus of these plugins is to discover hosts, applications and their related client/server vulnerabilities. To search for a specific plugin, visit http://www.tenable.com/pvs-plugins.

Many of the available plugins already detect activities that would fall into the “Inappropriate Use” category in most companies. Some of the activities that are detected through these plugins include (but are not limited to):

- Game servers
- Botnet clients and servers
- Peer to peer file sharing
- IRC clients and servers
- Chat clients
- Tunneling software or applications like Tor, GoToMyPC, and LogMeIn

Related Information

- [Detecting Custom Activity Prohibited by Policy](http://www.tenable.com)
- [Detecting Confidential Data in Motion](http://www.tenable.com)
Detecting Custom Activity Prohibited by Policy

The plugins provided with PVS are useful for detecting generally inappropriate activities, but there may be times when more specific activities need to be detected. For example, a company may want to have an alert generated when email is sent to a competitor’s mail service or if users are managing their Facebook accounts from the corporate network.

Tenable provides the ability for users to write their own custom plugins, as documented in PVS Plugin Syntax. These plugins are saved as .prm files.

The following example shows how to create a custom plugin to detect users logging into their Facebook accounts. First, a unique plugin ID is assigned, in this case 79420. So, the first line of our plugin will be:

\texttt{id=79420}

Next, we will want to have a description of what the vulnerability detects:

\texttt{description=The remote client was observed logging into a Facebook account. You should ensure that such behavior is in alignment with corporate policies and guidelines. For your information, the user account was logged as: \%L}

The %L will be the results of our regular expression statement that will be created later. Basically, we want to log the source address of the offending computer as well as the user ID that was used to log in. Next, we create a distinct name for our plugin.

\texttt{name=POLICY - Facebook usage detection}

Note that the name begins with the string POLICY. This will make all POLICY violations easily searchable from the SecurityCenter CV interface.

You could also define a SecurityCenter CV dynamic asset list that contains only POLICY violators.

The next field defines a family. For this example, the application is a web browser, so the family ID is defined as follows:

\texttt{family=Web Clients}

Since this is a web browser, a dependency can be assigned that will tell PVS to look at only those clients that have been observed surfing the web:

\texttt{dependency=1735}

Further, since we are looking at client traffic, we will define:
clientissue

Next, we assign a risk rating for the observed behavior:

risk=MEDIUM

In the final section we create match and regex statements that PVS will look for passively. We want all of these statements to be true before the client is flagged for inappropriate usage:

match=>POST /

The web request must begin with a POST verb. This will weed out all “GET” requests.

match=^Host: *.facebook.com

The statement above ensures that they are posting a host with a domain of *.facebook.com.

Finally, we have a match and regex statement that detects the user’s login credentials:

match=email=
regex=email=.*%40[^&]+

Putting it all together, we have a single plugin as follows:

```plaintext
id=79420
category=Web Clients
clientissue
dependency=1735
name=Facebook_Usage
description=The remote client was observed logging into a Facebook account. You should ensure that such behavior is in alignment with Corporate Policies and guidelines. For your information, the user account was logged as:
risk=MEDIUM
solution=Stay off of Facebook.
match=>POST /
match=^Host: *.facebook.com
match=email=
regex=email=.*%40[^&]+```

This plugin could be named `Facebook.prm` and added into the `/opt/pvs/var/pvs/plugins/` directory. If SecurityCenter CV is being used to manage one or more PVS systems, use the plugin upload dialog to add the new `.prm` file.
If you wish to create a policy file that includes multiple checks, use the reserved word `NEXT` within the policy file. For example:

```plaintext
id=79420
...
rest of plugin
...
NEXT
id=79421
...
```

etc.
Detecting Confidential Data in Motion

Many organizations want to ensure that confidential data does not leave the network. PVS can aid in this by looking at binary patterns within observed network traffic. If critical documents or data can be tagged with a binary string, such as an MD5 checksum, PVS will have the ability to detect these files being passed outside the network. For example:

Create a document that has a binary string of:

0xde1d7f362734c4d71ecc93a23bb5dd4c and 0x747f029fbf8f7e0ade2a6198560c3278

A PVS plugin could then be created to look for this pattern as follows:

```
id=79580
trigger-dependency
dependency=2004
dependency=2005
hs_dport=25
description=POLICY - Confidential data passed outside the corporate network. The Confidential file don'tshare.doc was just observed leaving the network via email.
name=Confidential file misuse
family=Generic
clientissue
risk=HIGH
bmatch=de1d7f362734c4d71ecc93a23bb5dd4c
bmatch=747f029fbf8f7e0ade2a6198560c3278
```

These binary codes were created by simply generating md5 hashes of the following strings:

"Copyright 2006 BigCorp, file: don'tshare.doc"

"file: don'tshare.doc"

The security compliance group maintains the list of mappings (confidential file to md5 hash). The md5 hash can be embedded within the binary file and could then be tracked as it traversed the network.

Similar checks can be performed against ASCII strings to detect, for example, if confidential data was cut-and-pasted into an email. Simply create text watermarks that appear benign to the casual observer and map to a specific file name. For example:

"Reference data at \192.168.0.2\c$\shares\employmentfiles for HR data regarding Jane Mcintyre" could be a string which maps to a file named Finances.xls.
A PVS plugin could look for the string as follows:

| id=79581  |
| trigger-dependency    |
| dependency=2004    |
| dependency=2005    |
| hs_dport=25    |
| description=POLICY - Confidential data passed outside the corporate network. Data from the confidential file Finances.xls was just observed leaving the network via email.    |
| name=Confidential file misuse    |
| family=Generic    |
| clientissue    |
| risk=HIGH    |
| match=Reference data at    |
| match=192.168.0.2\c$\shares\employmentfiles    |
| match=for HR data regarding Jane McIntyre    |

The two example plugins above (IDs 79580 and 79581) would detect files leaving the network via email. Most corporations have a list of ports that are allowed outbound access. SMTP is typically one of these ports. Other ports may include FTP, Messenger client ports (e.g., AIM, Yahoo and ICQ), or Peer2Peer (e.g., GNUTELLA and BitTorrent). Depending on your specific network policy, you may wish to clone plugins 79580 and 79581 to detect these strings on other outbound protocols.
Working with SecurityCenter CV

PVS can operate under the control of SecurityCenter, which provides PVS with passive vulnerability data and retrieves scanned data. SecurityCenter has a variety of reporting, remediation, and notification mechanisms to efficiently distribute vulnerability information across large enterprises. In addition, it can also control a distributed set of Nessus active vulnerability scanners. By combining active and passive vulnerability scanning, SecurityCenter can be used to efficiently and accurately manage security across large networks.

This section contains the following information about PVS integration with SecurityCenter.

- Managing Vulnerabilities
- Updating the PVS Management Interface
Managing Vulnerabilities

Below is a screen capture of SecurityCenter CV displaying a summary of vulnerabilities detected by PVS. These vulnerabilities can be independently viewed by many different users with different access control. SecurityCenter CV also enables security managers to issue recommendations that help guide network administrators as to which vulnerabilities should be mitigated.

PVS is Real-Time

Since PVS's vulnerability data is constantly fed into SecurityCenter CV and PVS's plugins are updated by Tenable, the accuracy of the passive vulnerability data in SecurityCenter CV greatly enhances the quality of the security information available to SecurityCenter CV's users.
Updating the PVS Management Interface

On occasion, the PVS management interface must be updated to provide new or updated features. When managed by SecurityCenter 4.8.1 or earlier, the PVS web server and interface do not update automatically by the plugins provided through SecurityCenter CV. Therefore, web components must be updated manually on each PVS.

To manually update the plugins:

1. Download the latest plugins using the URL created during the offline registration process.
2. Next, log in to the PVS interface as a user with administrative privileges.
3. Navigate to the Configuration page, and locate the Feed Settings section.
4. In the Offline Update section, navigate to Browse. A dialog box opens.
5. Select the archive file to upload.
6. Click Upload Archive to send the file to the PVS host, which updates the plugins.
7. Stop and then restart PVS on the host. The new interface is available for use.
Syslog Messages

PVS provides options to send real-time and vulnerability data as Syslog messages. This section describes the available Syslog message types:

- Standard Syslog Message Types
- CEF Syslog Message Types
Standard Syslog Message Types

Message Types

- Syslog message format for real-time Syslog entries generated by realtimeonly PRMs:

```
<priority>timestamp pvs: src_ip:src_port|dst_ip:dst_port|protocol|plugin_id|plugin_name|matched_text_current_packet|matched_text_previous_packet|risk
```

- Syslog message format for vulnerability and real-time Syslog entries generated by PASLs, PRMs, and internal plugins:

```
<priority>timestamp pvs: src_ip:src_port|dst_ip:dst_port|protocol|plugin_id|plugin_name|plugin_description|plugin_output|risk
```

Message Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst_ip</td>
<td>Displays the destination IP address for reported traffic.</td>
</tr>
<tr>
<td>dst_port</td>
<td>Displays the destination port for reported traffic.</td>
</tr>
<tr>
<td>matched_text_current_packet</td>
<td>Reports the payload, causing a match in the packet to trigger the PVS event.</td>
</tr>
<tr>
<td>matched_text_previous_packet</td>
<td>Reports the payload that was observed prior to the payload in the matched_text_current_packet field.</td>
</tr>
<tr>
<td>plugin_id</td>
<td>Displays the reported PVS plugin or PASL ID triggered by reported traffic.</td>
</tr>
<tr>
<td>plugin_name</td>
<td>Displays the name of the PVS plugin or PASL ID triggered by reported traffic.</td>
</tr>
<tr>
<td>plugin_output</td>
<td>Displays dynamic data for a given vulnerability or event. This field may be empty if there is no plugin-specific data.</td>
</tr>
<tr>
<td>priority</td>
<td>Displays the Syslog facility level of the message.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>protocol</td>
<td>Reports the integer value for the protocol used for the reported traffic.</td>
</tr>
<tr>
<td>risk</td>
<td>Displays the associated risk level of the reported vulnerability. This can be <strong>NONE</strong>, <strong>LOW</strong>, <strong>MEDIUM</strong>, <strong>HIGH</strong>, <strong>CRITICAL</strong>, or <strong>INFO</strong>.</td>
</tr>
<tr>
<td>src_ip</td>
<td>Displays the source IP address reported for the traffic.</td>
</tr>
<tr>
<td>src_port</td>
<td>Displays the source port for the reported traffic.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Displays the date and time of the Syslog message.</td>
</tr>
</tbody>
</table>
CEF Syslog Message Types

Message Type

Syslog message format for vulnerability and real-time Syslog entries generated by PASLs, PRMs, and internal plugins:

```
timestamp CEF: Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

Message Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Product</td>
<td>Displays the name of the product on the detected sending device.</td>
</tr>
<tr>
<td>Device Vendor</td>
<td>Displays the vendor of the product on the detected sending device.</td>
</tr>
<tr>
<td>Device Version</td>
<td>Displays the version of the product on the detected sending device.</td>
</tr>
<tr>
<td>Extension</td>
<td>Displays key-value pairs for one or more of the following additional fields: src, dst, spt, dpt, proto, and msg.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the PVS plugin or PASL ID triggered by the reported traffic.</td>
</tr>
<tr>
<td>Severity</td>
<td>Displays the associated severity level of the reported vulnerability.</td>
</tr>
<tr>
<td>Signature ID</td>
<td>Displays the reported PVS plugin or PASL ID triggered by the reported traffic.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Displays the date and time of the Syslog message.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version of the CEF format version.</td>
</tr>
</tbody>
</table>
Custom SSL Certificates

By default, PVS is installed and managed using HTTPS and SSL support and uses port 8835. Default installations of PVS use a self-signed SSL certificate.

To avoid browser warnings, use a custom SSL certificate specific to your organization. During the installation, PVS creates two files that make up the certificate: servercert.pem and serverkey.pem. You must replace these files with certificate files generated by your organization or a trusted CA.

Before replacing the certificate files, stop the PVS server. Replace the two files and re-start the PVS server. If the certificate was generated by a trusted CA, subsequent connections to the scanner do not display an error.

Certificate File Locations

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/opt/pvs/var/pvs/ssl/servercert.pem</td>
</tr>
<tr>
<td></td>
<td>/opt/pvs/var/pvs/ssl/serverkey.pem</td>
</tr>
<tr>
<td>Windows</td>
<td>C:\ProgramData\Tenable\PVS\pvs\ssl\servercert.pem</td>
</tr>
<tr>
<td></td>
<td>C:\ProgramData\Tenable\PVS\pvs\ssl\serverkey.pem</td>
</tr>
<tr>
<td>macOS</td>
<td>/Library/PVS/var/pvs/ssl/servercert.pem</td>
</tr>
<tr>
<td></td>
<td>/Library/PVS/var/pvs/ssl/serverkey.pem</td>
</tr>
</tbody>
</table>

Optionally, you can use the /getcert switch to install the root CA in your browser, which removes the warning:

https://<IP address>:8835/getcert

To set up an intermediate certificate chain, place a file named serverchain.pem in the same directory as the servercert.pem file.

This file must contain the 1-n intermediate certificates (concatenated public certificates) necessary to construct the full certificate chain from the PVS server to its ultimate root certificate (one trusted by the user’s browser).

SSL Client Certificate Authentication
PVS supports use of SSL client certificate authentication. When the browser is configured for this method, use of SSL client certificates is allowed.

PVS allows for password-based or SSL Certificate authentication methods for user accounts. When creating a user for SSL certificate authentication, use the pvs-make-cert-client utility through the command line on the PVS server.
Configure PVS for Certificates

To allow SSL certificate authentication, you must first configure the PVS web server with a server certificate and CA.

This process allows the web server to trust certificates created by the CA for authentication purposes. Generated files related to certificates must be owned by root:root and, by default, have the correct permissions by.

This section contains the following instructions:

- [Create a Custom CA and Server Certificate](#)
- [Create PVS SSL Certificates for Login](#)
- [Connect with Certificate Enabled Browser](#)
Create a Custom CA and Server Certificate

Steps

1. Optionally, create a new custom CA and server certificate for the PVS server using the `pvs-make-cert` command. This places the certificates in the correct directories.

   When prompted for the host name, enter the DNS name or IP address of the server in the browser (eg., https://hostname:8835/ or https://ipaddress:8835/). The default certificate uses the host name.

2. If you wish to use a CA certificate instead of the PVS generated one, make a copy of the self-signed CA certificate using the appropriate command for your OS:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td># cp /opt/pvs/var/pvs/ssl/cacert.pem /opt/pvs/var/pvs/ssl/ORIGcacert.pem</td>
</tr>
<tr>
<td>Windows</td>
<td>copy \ProgramData\Tenable\PVS\pvs\ssl\cacert.pem C:\ProgramData\Tenable\PVS\pvs\ssl\ORIGcacert.pem</td>
</tr>
<tr>
<td>macOS</td>
<td># cp /Library/PVS/var/pvs/ssl/cacert.pem /Library/PVS/var/pvs/ssl/ORIGcacert.pem</td>
</tr>
</tbody>
</table>

3. If the authentication certificates are created by a CA other than the PVS server, the CA certificate must be installed on the PVS server. Copy the organization's CA certificate to the appropriate location for your OS:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>/opt/pvs/var/pvs/ssl/cacert.pem</td>
</tr>
<tr>
<td>Windows</td>
<td>C:\ProgramData\Tenable\PVS\pvs\ssl\cacert.pem</td>
</tr>
<tr>
<td>macOS</td>
<td>/Library/PVS/var/pvs/ssl/cacert.pem</td>
</tr>
</tbody>
</table>

4. Once the CA is in place, restart the PVS services.
After PVS is configured with the proper CA certificate(s), users may log in to PVS using SSL client certificates.
Create PVS SSL Certificates for Login

To log in to a PVS server with SSL certificates, you must create the certificates using the `pvs-make-cert` command.

**Note:** When asked if you want to create a server certificate, select **no** to be prompted for the user certificate information.

**Steps**

1. On the PVS server, run the `pvs-make-cert` command.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code># /opt/pvs/bin/pvs-make-cert</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\Program Files\Tenable\PVS\pvs-make-cert</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code># /Library/PVS/bin/pvs-make-cert</code></td>
</tr>
</tbody>
</table>

2. Configure the client certificate by answering the various questions.

   The client certificates generate in a temporary directory.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code>/tmp/</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\users\&lt;username&gt;\AppData\Local\Temp</code>, where <code>&lt;username&gt;</code> is the user currently logged in.</td>
</tr>
<tr>
<td>macOS</td>
<td><code>/tmp/</code></td>
</tr>
</tbody>
</table>

3. Two files are created in the temporary directory. In an example where the user name is admin, the files `cert_admin.pem` and `key_admin.pem` are created. These two files must be combined and exported into a format that may be imported into the web browser, such as `.pfx`. You can accomplish this with the openssl program and the following command:
The resulting file `combined_admin.pfx` is created in the directory from which the command is launched. This file must then be imported into the web browser’s personal certificate store.

**Note:** The username you enter must correspond with an existing username in PVS. By default, PVS has only one administrative user. If you add another administrative user, then you can use more than one certificate.

4. Configure the PVS server for certificate authentication using the appropriate command for your OS. Once certificate authentication is enabled, username and password login is disabled.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td><code># /opt/pvs/bin/pvs --config &quot;Enable SSL Client Certificate Authentication&quot; &quot;1&quot;</code></td>
</tr>
<tr>
<td>Windows</td>
<td><code>C:\Program Files\Tenable\PVS\pvs --config &quot;Enable SSL Client Certificate Authentication&quot; &quot;1&quot;</code></td>
</tr>
<tr>
<td>macOS</td>
<td><code># /Library/PVS/bin/pvs --config &quot;Enable SSL Client Certificate Authentication&quot; &quot;1&quot;</code></td>
</tr>
</tbody>
</table>
Connect to PVS with a User Certificate

Steps

1. In a web browser, navigate to https://<ip address or hostname>:8835.
   The browser displays a list of available certificates.

2. Select the appropriate certificate.
   The certificate becomes available for the current PVS session.

3. Click the Sign In button.
   You are automatically logged in as the designated user and PVS can be used normally.

Note: If you log out of PVS, the standard PVS login screen appears. If you want to log in with the same certificate, refresh your browser. If you want to use a different certificate, restart your browser session.