Table of Contents

[Security Center (5.4 +) Vulnerability and Host Input for Firepower Management Center (6.0 +) 2](#_Toc500866520)

[Summary 2](#_Toc500866521)

[Usage – Setup 3](#_Toc500866522)

[Firepower Management Center Configuration 3](#_Toc500866523)

[Security Center 4](#_Toc500866524)

[Linux Endpoint 4](#_Toc500866525)

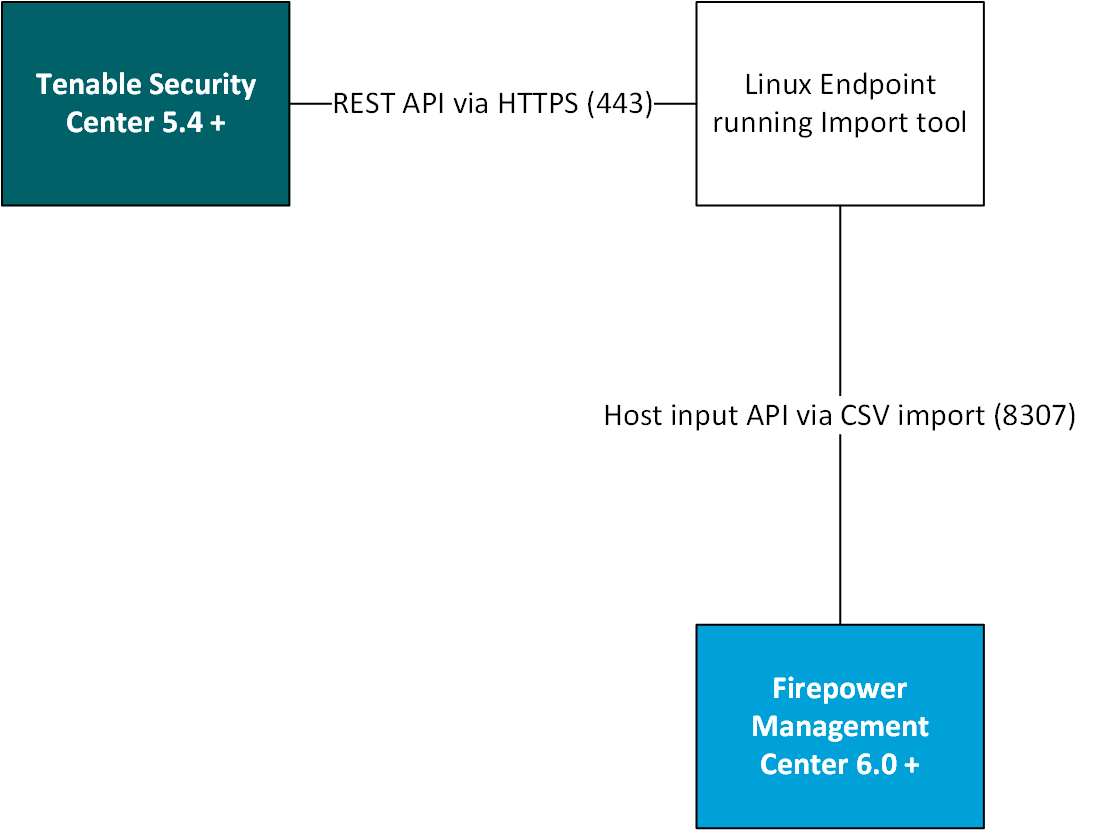
[Usage – Install and Run 6](#_Toc500866526)

# **Security Center (5.4 +) Vulnerability and Host Input for Firepower Management Center (6.0 +)**

This tool is written as a way to leverage vulnerability data from Tenable Security Center inside the Firepower Management Center to help build a more complete view of the network and IPS signatures required to ensure protection.

## **Summary**

This application is built to sit on a Linux endpoint that has IP connectivity to both the Security Center and Firepower Management Center. The diagram below demonstrates the setup required.



If there are network controls between the devices be sure to allow port access as per the diagram above.

Security Center 🡪 Linux Endpoint (TCP / 443)

Linux Endpoint 🡪 Firepower Management Center (TCP / 8307)

Currently the application is built as a point in time run, when run it will gather all vulnerable hosts from Security Center and import them as Third-Party Mappings in the Firepower Management Center.

Specifics on what vulnerabilities are imported:

* Plugin in security center is “active”
* Severity of vulnerability is anything but “Informative” (meaning Critical, High, Medium, and Low)

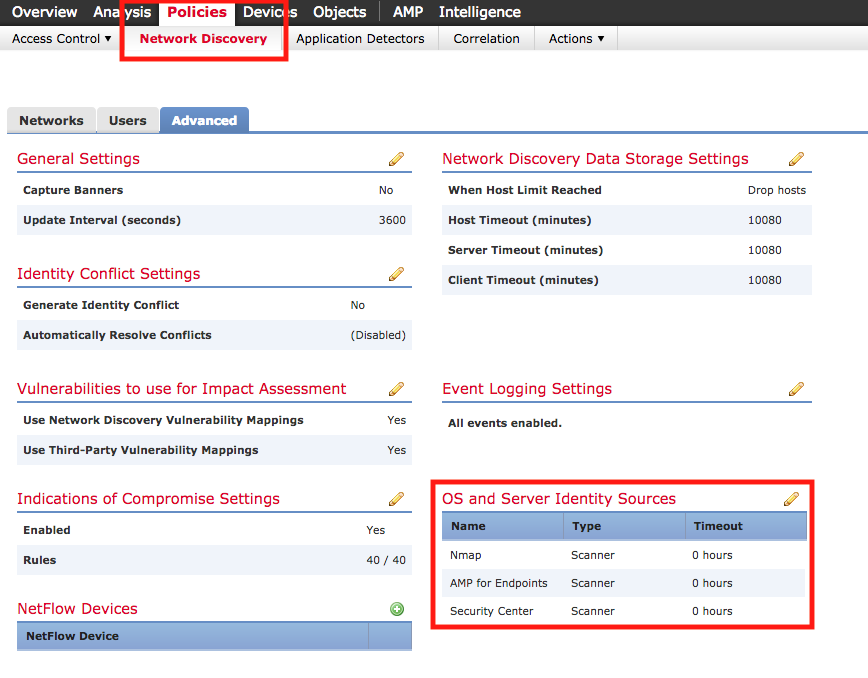
## **Usage – Setup**

Before the tool can be run the environment must be set up with the correct dependencies and configurations as described below:

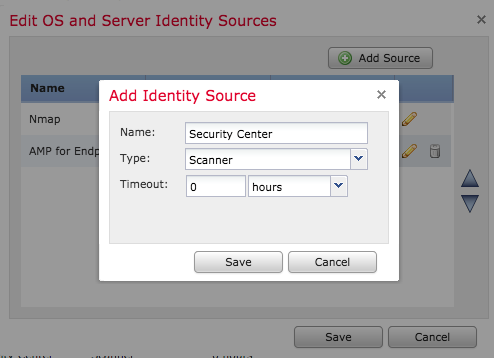
### **Firepower Management Center Configuration**

This tool will be importing host data as a third-party mapping so the Firepower Management Center “Network Discovery” policy must be configured properly to accept it.

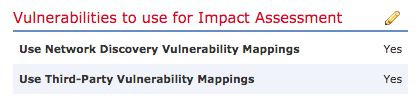
* Login to the Firepower Management Center UI and Navigate to “Policy” 🡪 “Network Discovery”
* Select the “Advanced” tab in the center of the screen
* Select “Edit” on the “OS and Server Identity Sources” Section



* In the new windows select “Add Source” at the top right and enter the details as seen below:
  + Name: Security Center
  + Type: Scanner
  + Timeout: 0 Hours



* Press “Save” on the “Add Identity Source” screen as well as the “Edit OS and Server Identity Sources” screen
* You will be returned to the “Advanced” page of the Discovery Policy, here ensure that “Use Third-Party Vulnerability Mappings” is set to “Yes”



*At this point the Firepower Management Center is ready to accept data from the tool and Security Center*

### **Security Center Configuration**

There is no additional configuration that needs to be made on the Security Center as the API is accessible with valid user credentials.

*Note: User credentials are required the “admin” credentials used to setup the Security Center will not work for the API calls.*

### **Linux Endpoint Configuration**

The Linux endpoint should have the proper Python and Perl libraries needed to make the toolset run. The dependencies are listed below and also steps to install them.

*Note: The tool is built to run on Linux only if you are trying to run on Windows you may run into issues.*

#### **Perl:**

Perl must be installed on the Linux endpoint to make use of this tool. Steps for installing Perl on both CentOS and Debian are outlined below.

*Note: If you plan to use the same system which was running the old host input client for Firepower Management Center you can skip this section and move right to python.*

CentOS

1. Open terminal and run

**$ yum install perl**

1. Ensure perl is installed and check version

**$ perl –v**

**This is perl 5, version 18, subversion 2 (v5.18.2) built for darwin-thread-multi-2level**

**(with 2 registered patches, see perl -V for more detail)**

**Copyright 1987-2013, Larry Wall**

**Perl may be copied only under the terms of either the Artistic License or the**

**GNU General Public License, which may be found in the Perl 5 source kit.**

**Complete documentation for Perl, including FAQ lists, should be found on**

**this system using "man perl" or "perldoc perl".  If you have access to the**

**Internet, point your browser at http://www.perl.org/, the Perl Home Page.**

Debian

1. Open terminal and run

**$ sudo apt install perl**

1. Ensure perl is installed and check version

**$ perl –v**

**This is perl 5, version 18, subversion 2 (v5.18.2) built for x86\_64-linux-gnu-thread-multi**

**(with 2 registered patches, see perl -V for more detail)**

**Copyright 1987-2013, Larry Wall**

**Perl may be copied only under the terms of either the Artistic License or the**

**GNU General Public License, which may be found in the Perl 5 source kit.**

**Complete documentation for Perl, including FAQ lists, should be found on**

**this system using "man perl" or "perldoc perl".  If you have access to the**

**Internet, point your browser at http://www.perl.org/, the Perl Home Page.**

#### **Python:**

Python 2.7.x must be installed on the Linux endpoint to make use of this tool. Steps for installing Python on both CentOS and Debian are outlined below.

CentOS

1. Open terminal and run

**$ yum install python**

1. Ensure perl is installed and check version

**$ python –V**

**Python 2.7.14**

Debian

1. Open terminal and run

**$ sudo apt install python**

1. Ensure perl is installed and check version

**$ python –V**

**Python 2.7.14**

*At this point your Linux endpoint is configured as it needs to be it is ready for the installation of the host input tool*

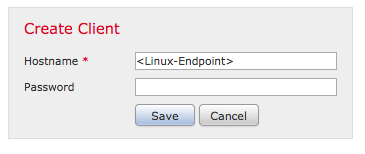
## 

## **Usage – Install and Run**

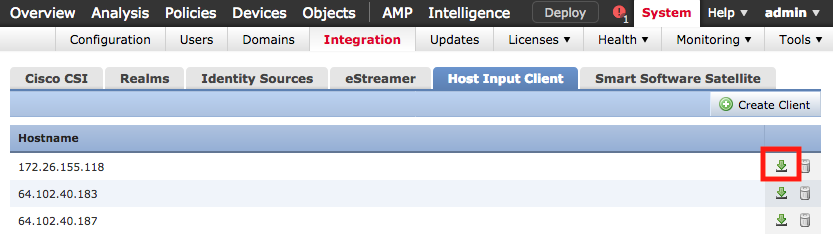
Once the system is ready to run the tool download and extract the “sc-fmc.zip” to a location of your choice.

Before running the tool you will need to generate a certificate from the FMC for the Linux endpoint to authorize insertion of host data.

1. Login to the Firepower Management Center
2. Navigate to “System” and “Integration”
3. Click the tab for “Host Input Client”
4. Select “Create Client” in the top right



1. Enter the hostname of your Linux Endpoint, and press “Save”
2. Back on the main menu you should see your host, select the green Download button for your host and download the certificate



1. Place the certificate into the same directory you extracted “sc-fmc”

To run the tool you must first provide it with details surround your environment, things like Hostnames and credentials.

1. Navigate to the folder directory

**$ cd /<path-to-directory>/sc-fmc**

1. Edit the “parameters.json” file with the editor of your choice (in this example we will use “nano” for ease

**$ nano parameters.json**

1. Edit the file following the guidelines:

**{**

**"hostname" : "*<hostname or ip of security center>*",**

**"FMCHostname" : "*<hostname or ip of FMC>*",**

**"username" : "*<Security Center Username>*",**

**"password" : "*<Security Center Password>*",**

**"debug" : true,**

**"netrange" : "*<IP Range of hosts to add>*",**

**"addHosts" : true**

**}**

1. When complete press “cntrl-o” to write changes and “cntrl-x” to exit the editor

Once the parameters.json file is edited with the proper parameters we can run the tool.

1. Navigate to the folder directory (if you are not already there)

**$ cd /<path-to-directory>/sc-fmc**

1. Run tool

**$ python query\_vuln.py**

*At this point if all your configuration is correct you should start to see debug logs on the screen indicating that vulnerabilities are being processed. If you run into errors please make sure all dependencies are met as listed in this document and IP connectivity is present.*