

ICS017

Vulnerability Scanning with OpenVAS

Lab Objectives

In this lab, you will learn how to:

- Start the OpenVAS virtual appliance
- Perform a basic scan of a target with OpenVAS
- View scan reports
- Perform an advanced scan
- Examine detailed reports of specific vulnerabilities

Lab Environment

This lab will require a workstation with a preconfigured OpenVAS virtual appliance (provided).

Lab Duration

15-20 minutes

Lab Tasks

Import the virtual appliance, login to the Greenbone Security Manager, and perform a basic scan. View a detailed report that contains information about any detected vulnerabilities.

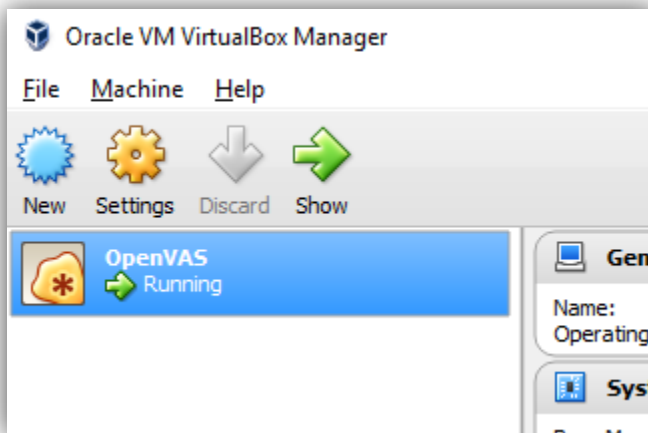
Lab Procedure- Vulnerability Scanning with OpenVAS

Starting the Application

To begin working in OpenVAS, we will first need to import and start the virtual application.

1. Follow the instructions at <http://openvas.org/vm.html> to import the newest version of the application. Make sure that your settings match the requirements listed for the current version. We will be using VirtualBox in our examples. For the virtual machine's network settings, if you only wish to scan the computer running the virtual machine, you can use a "host-only" adapter. To scan other devices on your network, you can use a "bridged" adapter.
2. After you have created the virtual machine, double-click on it in VirtualBox. The virtual machine will launch in a separate window.

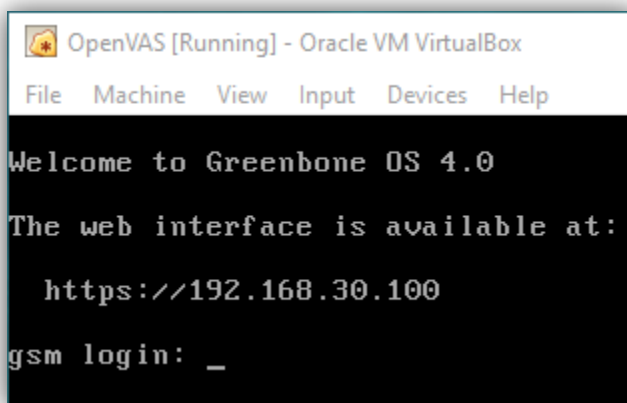
3. Follow the on-screen setup instructions to create the necessary accounts and update the feeds.



Starting the virtual machine

Logging in

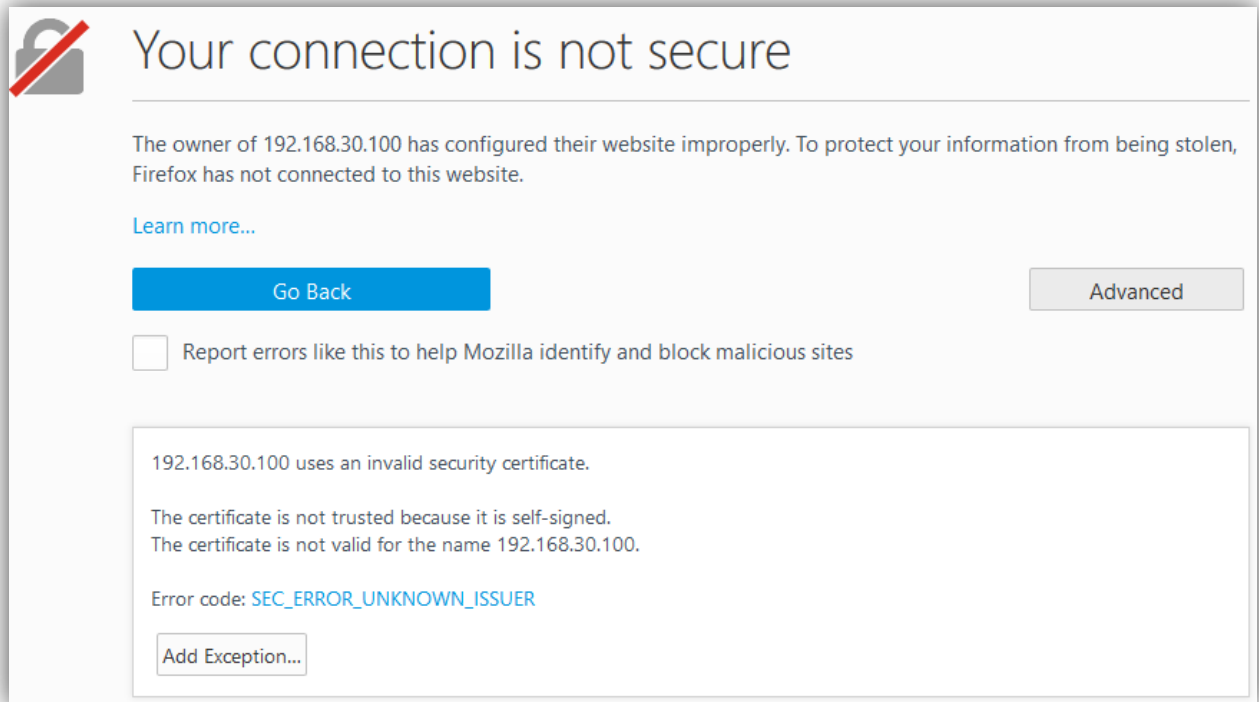
After the virtual machine finishes booting up, it should display an IP address you will use to log into the web interface. Once you make note of this address, feel free to minimize (but do not power off) the virtual machine, because we will be doing the rest of the lab within a web browser. If the displayed address is "https://127.0.0.1", however, you will likely need to log into the virtual machine by using the credentials for the administrator account you created earlier and edit the network settings.



Displaying the IP address of the virtual machine

1. Open a web browser, such as Firefox or Google Chrome
2. Type the full address displayed on your virtual machine (including the "http://") into the address bar of your web browser, just as you would navigate to a web site.

3. If a warning appears stating that the page is not secure, you will need to add a security exception to the browser. If you do not see this option on the page, look for an “advanced” or “more info” option that will allow you to do so, as this will vary by browser. Once the exception is added, the page should reload and you should now be able to log in.

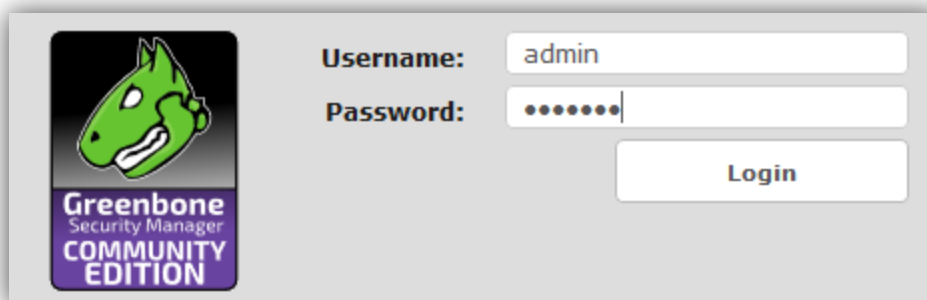


In Firefox, we would select Advanced, then Add Exception, then Confirm Security Exception in the new dialog box that appears.

On the Greenbone Security Manager login page:

- Enter the credentials for the “webuser” you specified during the creation of the virtual machine and click “Login.”

Note: on a new installation of OpenVAS, the admin account will be assigned a random password, unless otherwise specified. This can later be changed.



Logging in to Greenbone Security Manager

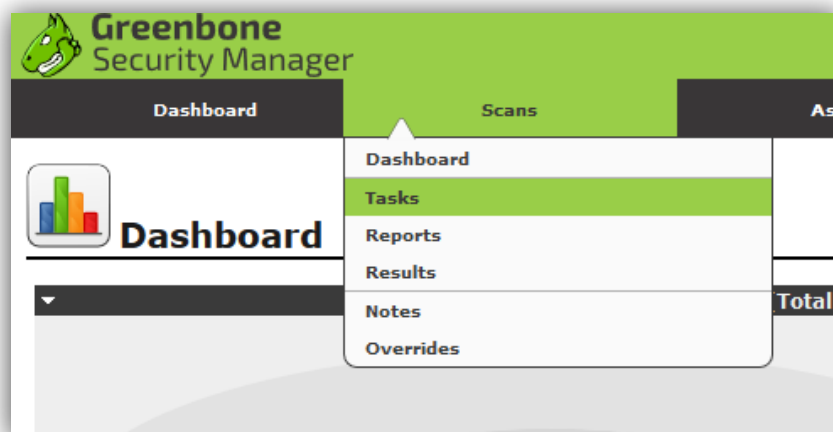
Performing a Basic Scan

Now that we are logged-in to Greenbone, we can start our first scan.

For a relatively quick, basic scan, perform the following steps:


1. Under the "Scans" tab, select "Tasks."
2. A pop-up should appear displaying the purple "task wizard" icon (🧙). You can close this or wait for it to go away. When it does, click the "task wizard" icon in the top left of the page.
3. In the pop-up that appears, enter the IP address of the target and click "Start Scan." For our following example images, we scanned a very vulnerable host and displayed the results.

Note: You can perform more thorough scans by selecting "Advanced Task Wizard" when hovering the cursor over the "task wizard" icon.



Opening the "Tasks" page

Task Wizard



Quick start: Immediately scan an IP address


IP address or hostname:

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

By clicking the New Task icon  you can create a new Task yourself.

Start Scan

Starting a basic scan

The scan will start immediately. The page will refresh on its own so that we can track the progress of our scan. When it is complete, the progress bar will show "done."

1. When the scan is finished, click on the scan's name to view the details.
2. When you are finished viewing the details, click on "Results" to see what the scan found.

| Name | Status |
|-----------------------------------------------------|--------|
| Immediate scan of IP 192.168.30.101 | Done |

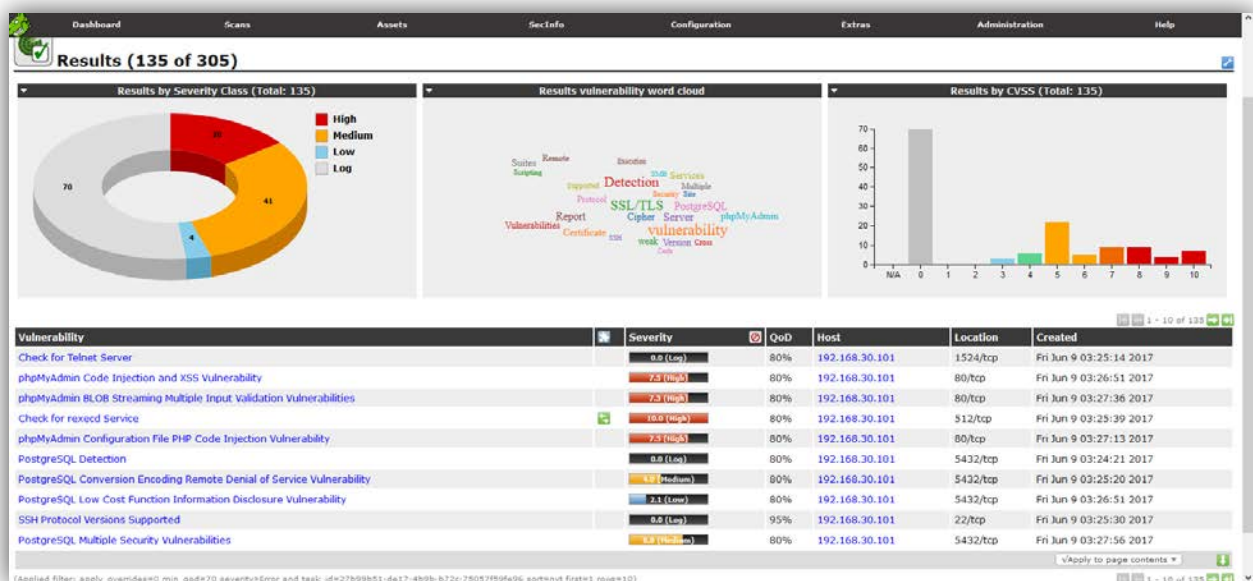
A completed scan



Task: Immediate scan of IP 192.168.30.101

| | |
|------------------------|-------------------------------------------------------------------------------------|
| Name: | Immediate scan of IP 192.168.30.101 |
| Comment: | |
| Target: | Target for immediate scan of IP 192.168.30.101 |
| Schedule: | (Next due: over) |
| Add to Assets: | yes |
| | Apply Overrides: yes |
| | Min QoD: 70% |
| Alterable Task: | no |
| Auto Delete Reports: | Do not automatically delete reports |
| Scanner: | OpenVAS Default (Type: OpenVAS Scanner) |
| | Scan Config: Full and fast |
| | Order for target hosts: N/A |
| | Network Source Interface: |
| | Maximum concurrently executed NVTs per host: 10 |
| | Maximum concurrently scanned hosts: 30 |
| Status: | Done |
| Duration of last scan: | 25 minutes 23 seconds |
| Average scan duration: | 25 minutes 23 seconds |
| Reports: | 1 (Finished: 1 , Last: Jun 9 2017) |
| Results: | 134 |

[Viewing the scan's details](#)



Viewing the scan's results

The results page lists everything detected by the scan. This may include basic information about the host, services detected, vulnerabilities, and sometimes steps for remediation. Not everything listed here is necessarily a security vulnerability. To view more information about a detection:

- Click the name of the item under the "Vulnerability" column that you want to examine.

On this detailed result page, we have a wealth of information about the detected vulnerability and how it affects our host. The CVE ID can also be used to research even more information outside of OpenVAS, including publicly available exploits that an attacker might be able to use against our host. Using this information, we can take the necessary steps towards securing it.

Dashboard
Scans
Assets
SecInfo
Configuration
Extras
Administration
Help

Result: phpMyAdmin Code Injection and XSS Vulnerability

Created: Fri Jun 9 03:26:51 2017
Modified: Fri Jun 9 03:26:51 2017
Owner: admin

| Vulnerability | Severity | QoD | Host | Location | Actions |
|-----------------------------------------------------------------|------------|-----|----------------|----------|---------|
| phpMyAdmin Code Injection and XSS Vulnerability | 7.5 (High) | 80% | 192.168.30.101 | 80/tcp | |

Summary

phpMyAdmin is prone to a remote PHP code-injection vulnerability and to a cross-site scripting vulnerability. An attacker can exploit this issue to inject and execute arbitrary malicious PHP code in the context of the webserver process. This may facilitate a compromise of the application and the underlying system other attacks are also possible. Versions prior to phpMyAdmin 2.11.9.5 and 3.1.3.1 are vulnerable.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Vendor updates are available. Please see <http://www.phpmyadmin.net> for more information.

Vulnerability Detection Method

Details: phpMyAdmin Code Injection and XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.100077)
Version used: \$Revision: 5016 \$

Product Detection Result

Product: **cpe:/a:phpmyadmin:phpmyadmin:3.1.1**
Method: phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)
Log: [View details of product detection](#)

References

CVE: [CVE-2009-1151](#)
BID: [34236](#), [34251](#)
Other: <http://www.securityfocus.com/bid/34236>
<http://www.securityfocus.com/bid/34251>

Viewing a detailed overview of a detected vulnerability