



ETHICAL HACKING V2 LAB SERIES

Lab 05: Vulnerability Scanning with OpenVAS

Document Version: **2020-08-24**

Material in this Lab Aligns to the Following	
Books/Certifications	Chapters/Modules/Objectives
All-In-One CEH Chapters ISBN-13: 978-1260454550	3: Scanning and Enumeration
EC-Council CEH v10 Domain Modules	3: Scanning Networks 4: Enumeration
CompTIA Pentest+ Objectives	2.1: Given a scenario, conduct information gathering using appropriate techniques 2.2: Given a scenario, perform a vulnerability scan 2.3: Given a scenario, analyze vulnerability scan results 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	2: Getting to Know Your Targets 3: Network Scanning and Enumeration 4: Vulnerability Scanning and Analysis

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 OpenVAS Initial Setup	6
2 Quick Scanning with OpenVAS.....	8
3 Customized Scanning with OpenVAS.....	10

Introduction

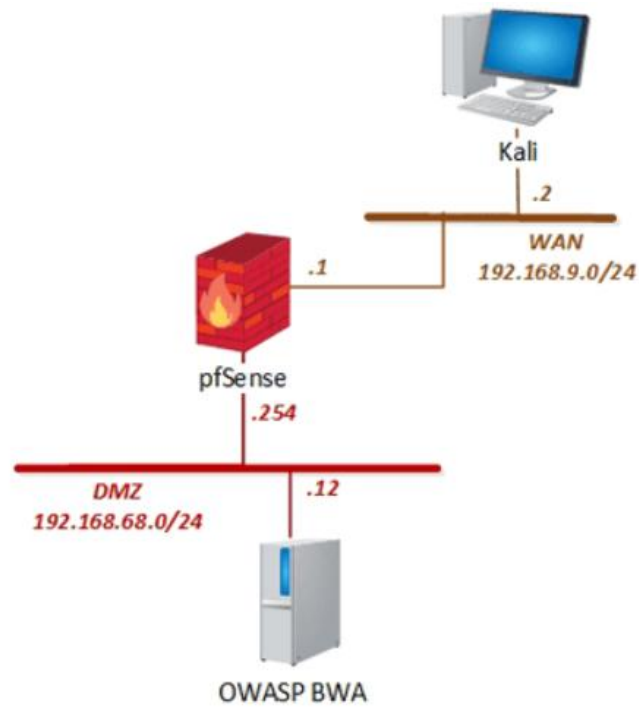
There are several commercial tools available for performing vulnerability scanning. In this lab, we will be using *OpenVAS*, an open source vulnerability scanner to perform security assessments.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Using OpenVAS
2. Quick Scanning with OpenVAS
3. Customized Scanning with OpenVAS

Pod Topology



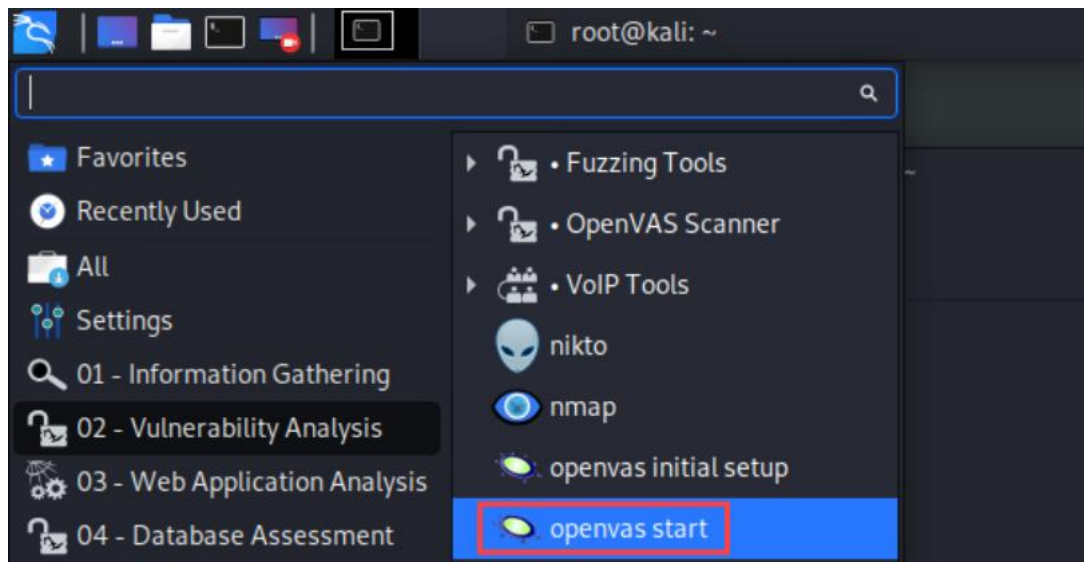
Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa

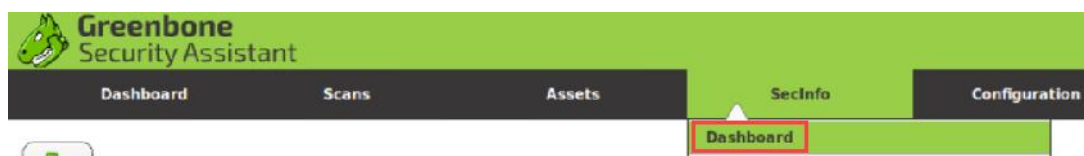
1 OpenVAS Initial Setup

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Press **Tab**.
4. Enter `toor` as the *password*. Click **Log In**.
5. Launch *OpenVAS* by clicking on the **Application Launcher** and selecting **02-Vulnerability Analysis > openvas start**.



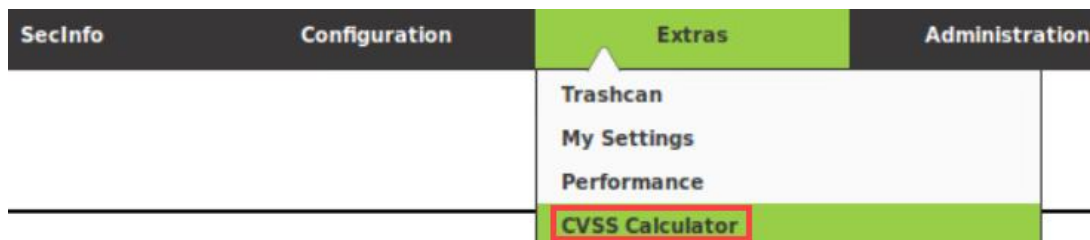
This may take a few minutes to launch all of the services.

6. Log into the *Greenbone Security Assistant* using the following credentials.
 - a. Username: `admin`
 - b. Password: `password`
 - c. Click **Login**.
7. Select **SecInfo > Dashboard** from the top pane.



Notice the categorized *network vulnerability tests* (NVT) by severity and *common vulnerability scoring system* (CVSS). Also, notice the *common vulnerabilities and exposures* (CVE) by CVSS and severity.

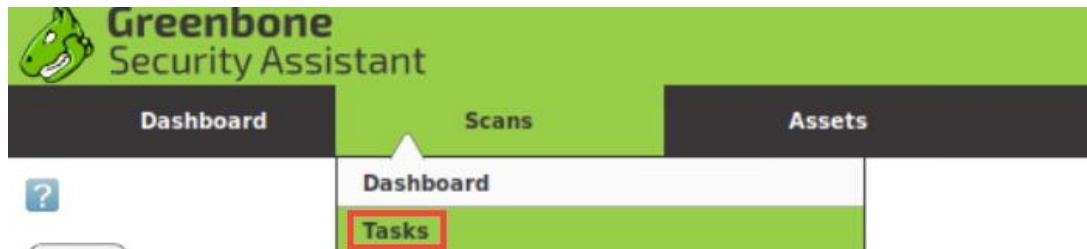
8. Select **Extras > CVSS Calculator** from the top pane.



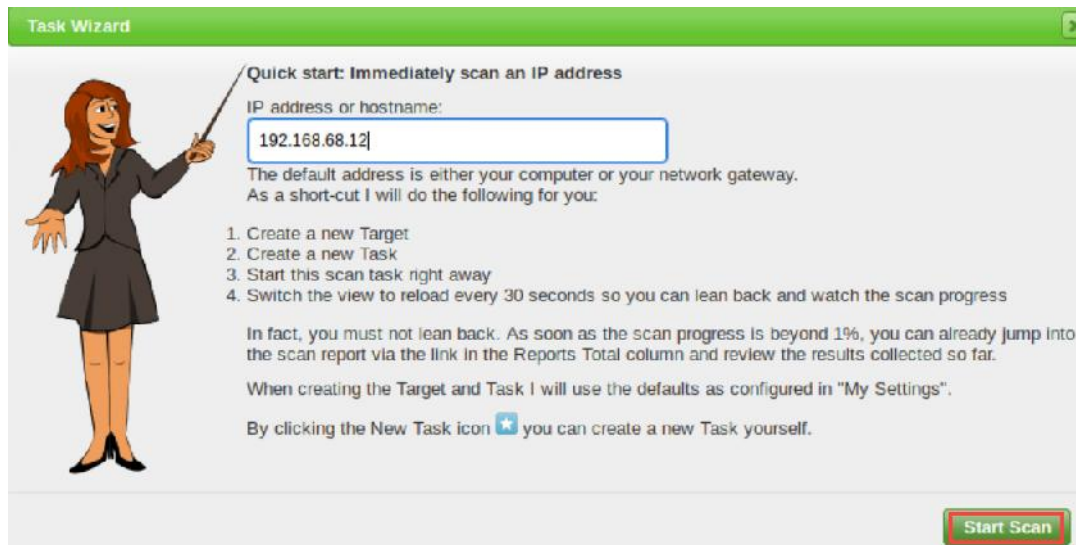
The calculator shown here can make calculations based on several different vectors to derive a CVSS score that is used for rating CVEs.

2 Quick Scanning with OpenVAS

1. Select **Scans > Tasks** from the top pane.



2. A popup will appear, last for 10 seconds, and close. Notice it goes to the purple icon in the upper-left. Click on the **purple wizard icon** to open the *Task Wizard*.
3. Configure a default scan against the OWASP server by typing the *IP address* 192.168.68.12 into the *Quick start* text field.
4. Click **Start Scan**.



This scan will take 10-20 minutes depending on your system; wait until the scan finishes before moving on to the next step. The scan will finish once the progress bar reaches 100% or "Done".

Name	Status
Immediate scan of IP 192.168.68.12	Done

Notice the screen will refresh periodically. If you see an authentication error, click on **Assumed sane state** and the page will refresh. This is a permission bug in the Openvas product with the small SQLite install.

- Once the scan finishes, click the number **1** under the *Reports Total* column.

Status	Reports	
	Total	Last
Done	1 1)	Jun 28 2020

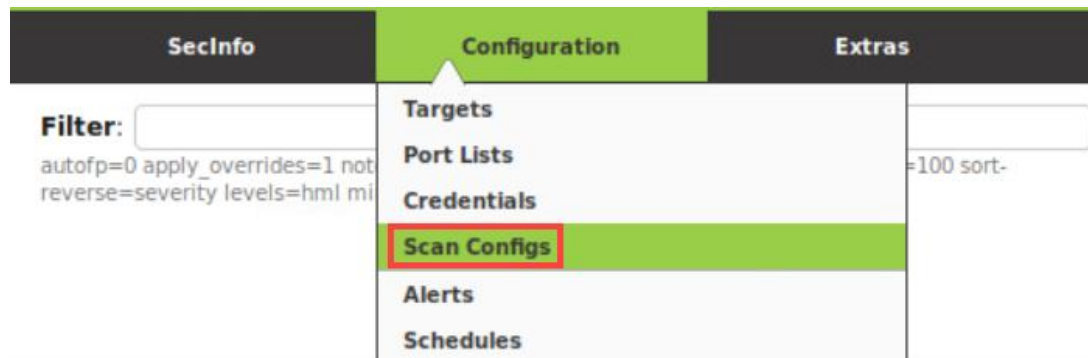
- Click on the specified date under the *Date* column to view the full report.

Date	Status	Task
Sun Jun 28 00:31:27 2020	Done	Immediate scan of IP 192.168.68.12

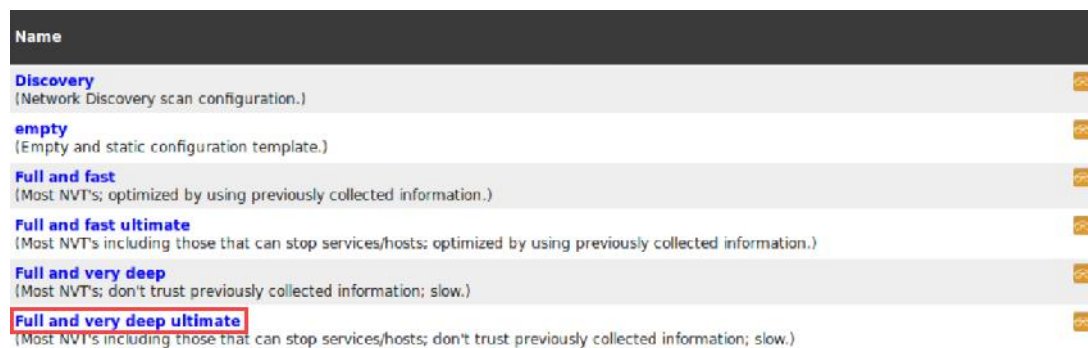
- Analyze the vulnerabilities listed in the report.

3 Customized Scanning with OpenVAS

1. Select **Configuration > Scan Configs** from the top pane.



2. Click on the **Full and very deep ultimate** link.

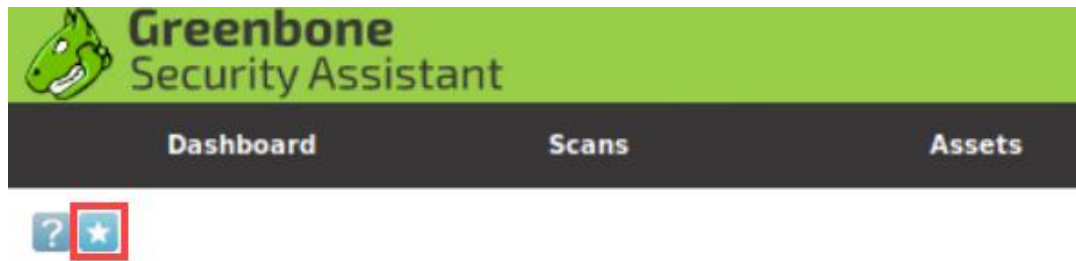


Analyze and scroll down through the options made available. There are many different types of *NVTs* (Network Vulnerability Tests) that can be initiated including *Nmap* scripts.

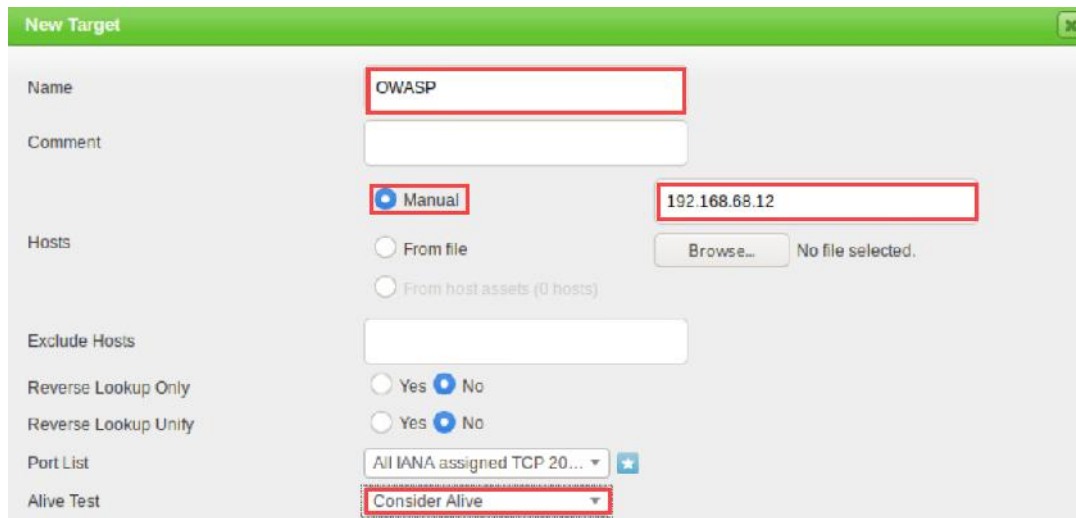
3. Select **Configuration > Targets** from the top pane.



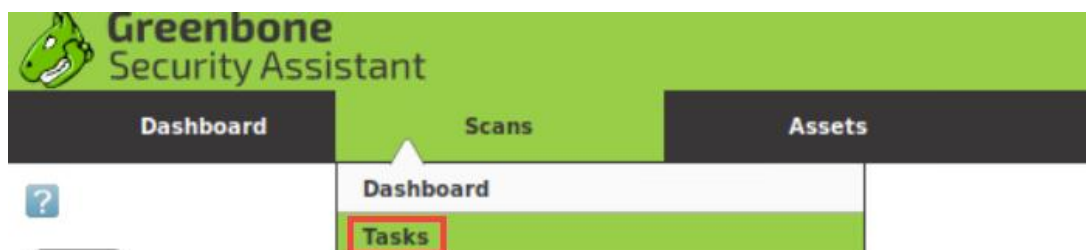
4. Click the **New Target** (star) icon.



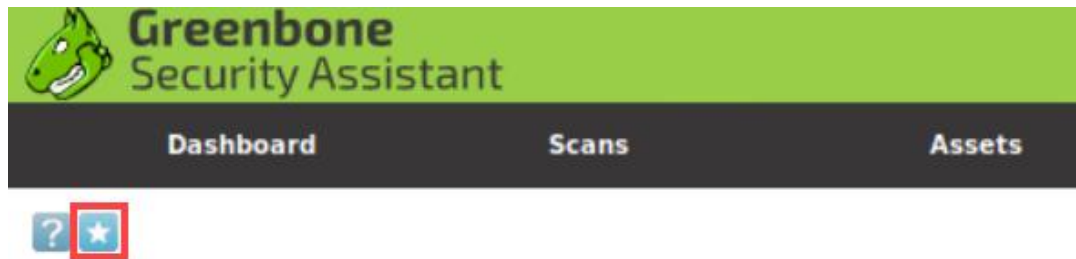
5. Configure the new target with the information below:
 - a. Name: **OWASP**
 - b. Hosts: **Manual**
192.168.68.12
 - c. Alive Test: **Consider Alive**
 - d. Leave the rest as defaults.



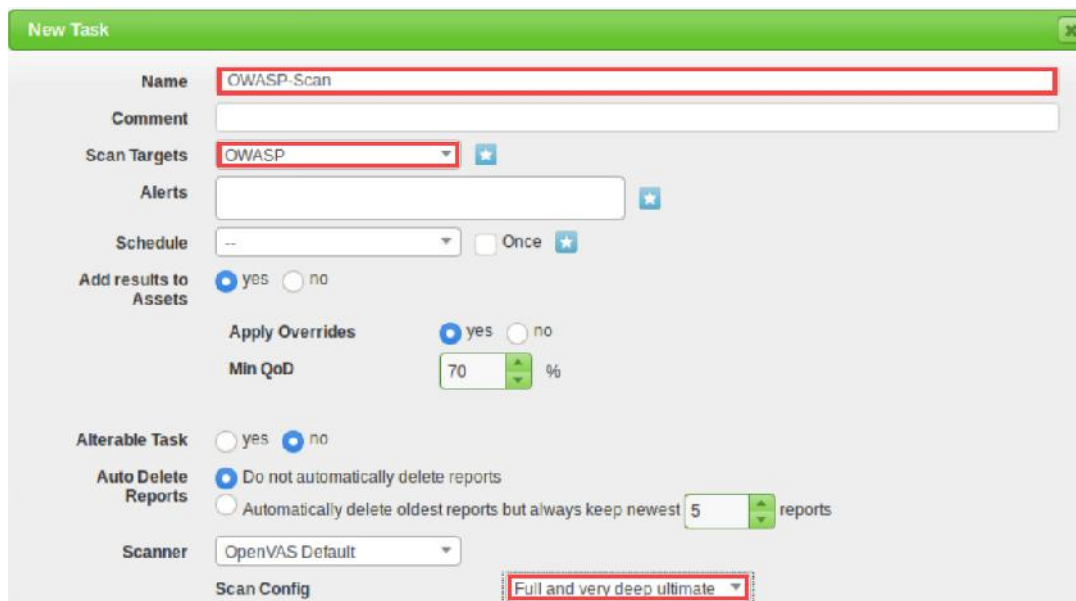
6. Click **Create**.
7. Click on **Scans > Tasks** from the top pane.



8. Click the **New Task** (star) icon.



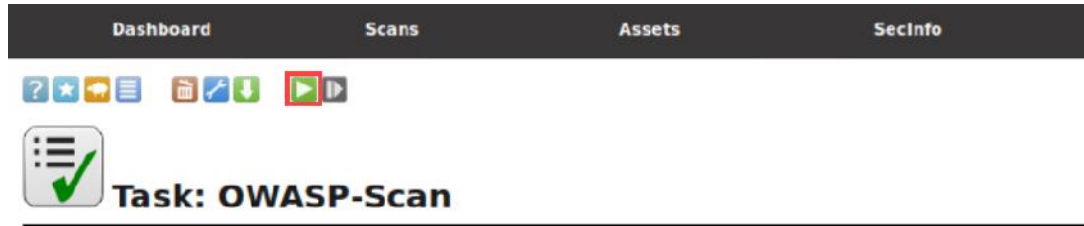
9. Configure the new task with the information below:
 - a. Name: **OWASP-Scan**
 - b. Scan Targets: **OWASP**
 - c. Scan Config: **Full and very deep ultimate**
 - d. Leave the rest as defaults



10. Click **Create**.
11. At the bottom of the window, click on the **OWASP-Scan** task.

Name	Status
Immediate scan of IP 192.168.68.12	Done
OWASP-Scan	New

12. Click the **Start** (green arrow) icon to initiate the scan.



This particular scan will take more time than the first quick scan that was initiated at the beginning of the lab. If you wish, you may choose to run the scan for a period of time for analysis. When ready, click the **Stop** (yellow square) icon to stop the scan.

13. You may now end your reservation.