ETHICAL HACKING
LAB SERIES

Lab 7: Vulnerability Scanning with OpenVAS

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Ethical Hacking (CEH) Domains	SANS GPEN Objectives
3: Scanning Networks	16: Vulnerability Scanning

Document Version: 2016-03-09

Contents

Introduction

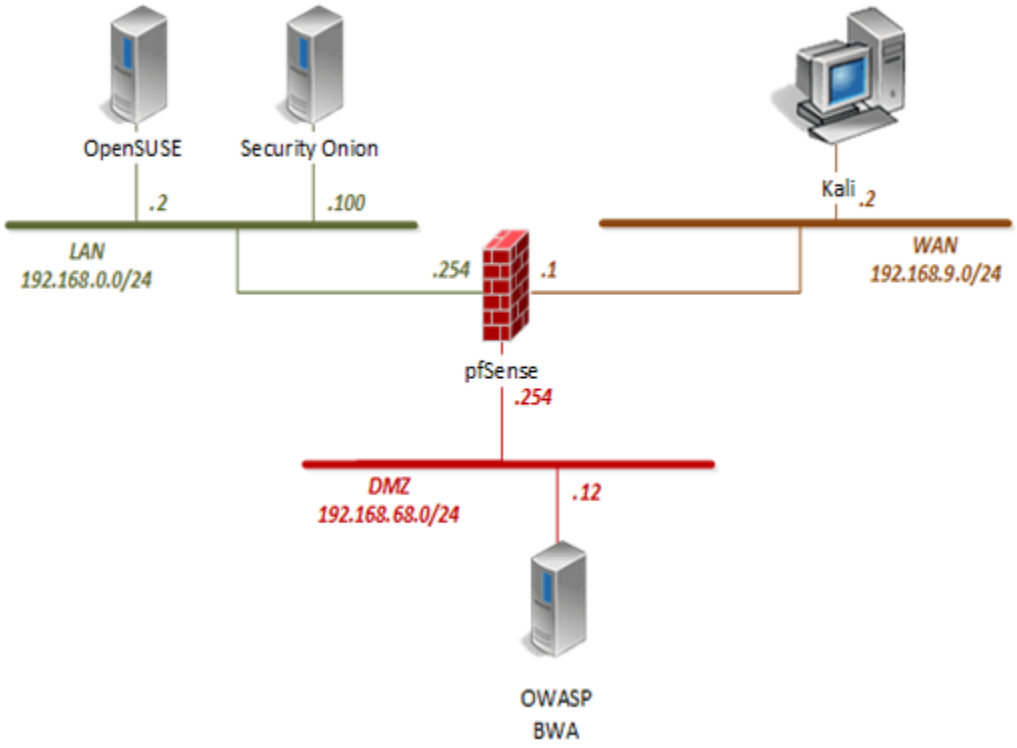
There are several commercial tools available for performing vulnerability scanning. In this lab, we will be using OpenVAS, an open source vulnerability scanner to perform security assessments.

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



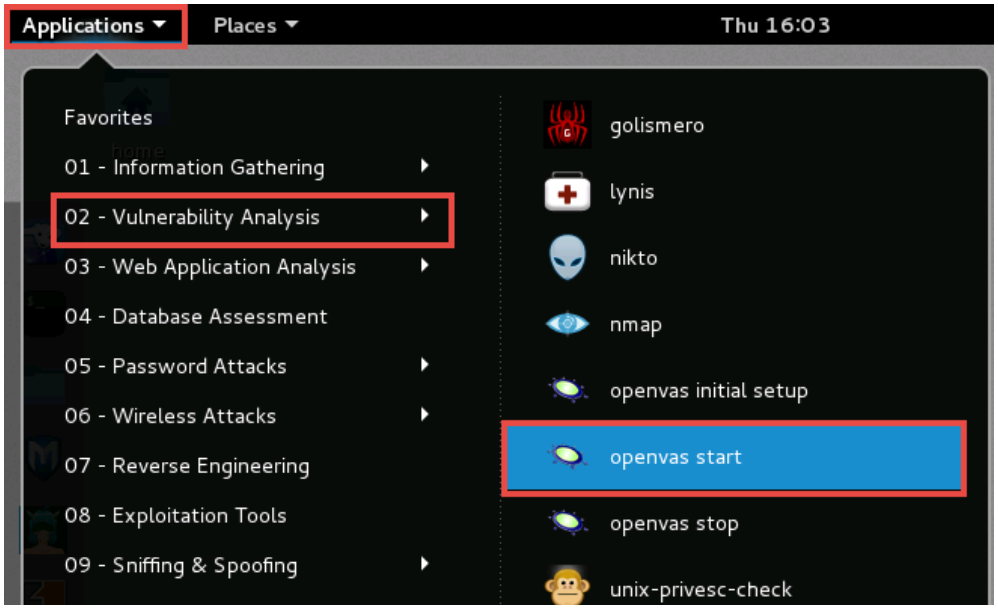
Lab Settings

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	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
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Using OpenVAS

1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Launch *OpenVAS* by clicking on the **Application Launcher** and selecting **Vulnerability Analysis > openvas start**.

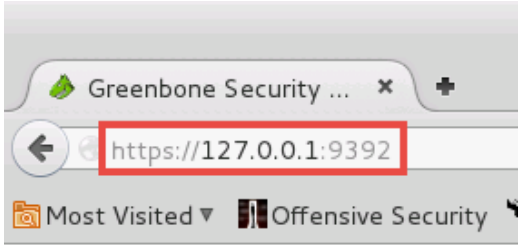


6. Notice a *Terminal* window appear. Use the same **Terminal** and type the command below to restart the *Apache* service. Press **Enter**.

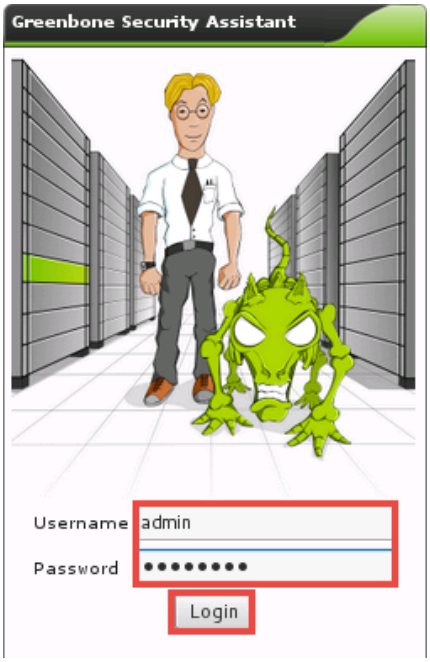
```
service apache2 restart
```

7. Once restarted, click on the **Iceweasel** icon located on the left panel.

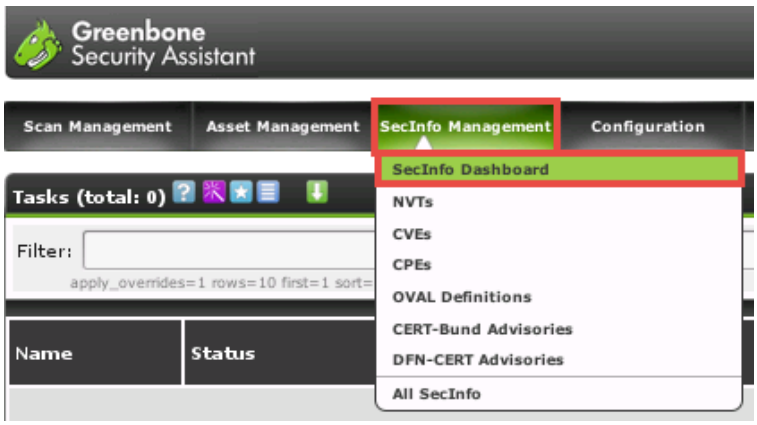
8. In the *Iceweasel* browser, type `https://127.0.0.1:9392` into the address field. Press **Enter**.



9. Log into the *Greenbone Security Assistant* using the following credentials.
   a. Username: `admin`
   b. Password: `password`
   c. Click **Login**.

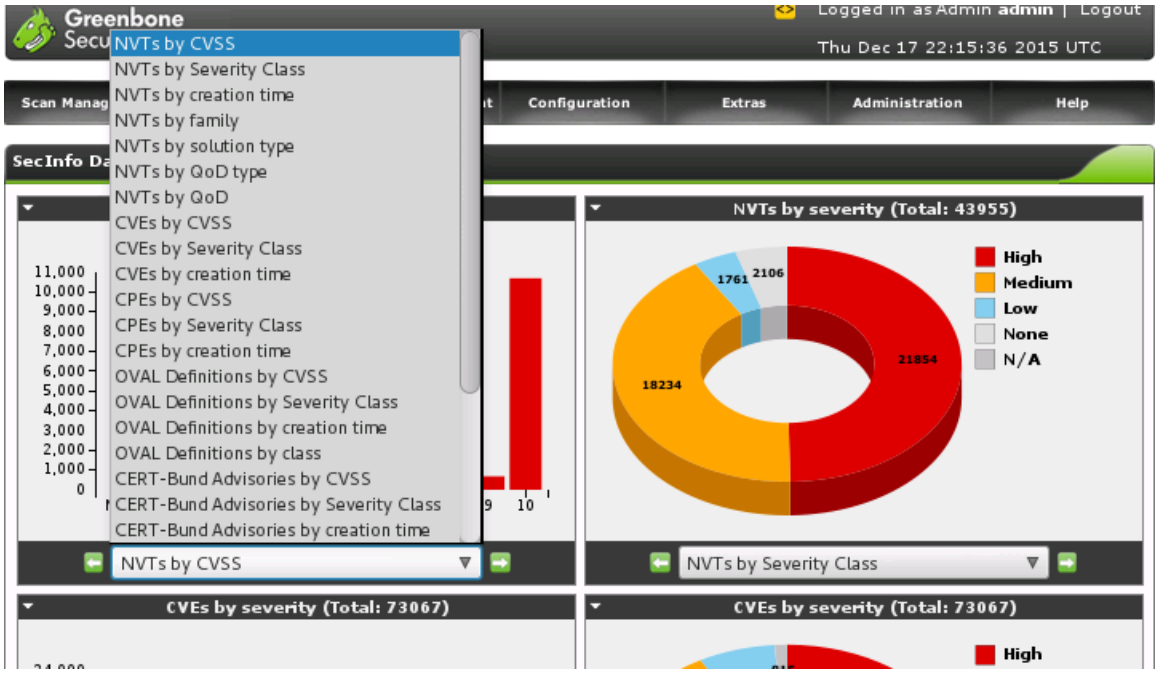


10. Select **SecInfo Management > SecInfo Dashboard** from the top pane.

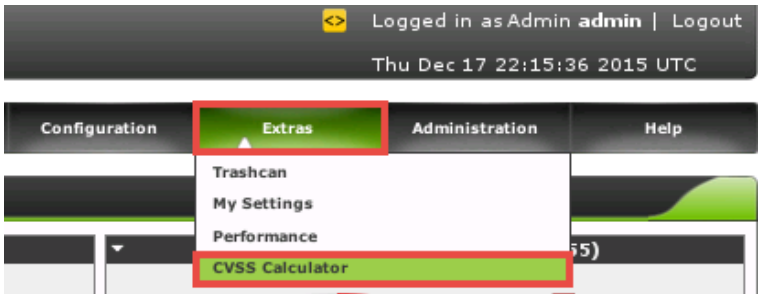


Notice the categorized *network vulnerability tests* (NVT) by severity and *common vulnerability scoring system* (CVSS). Also, notice the *common vulnerabilities and exposures* (CVE) by CVSS and severity.

11. Click on a pull-down menu and view the data for each group in different ways.



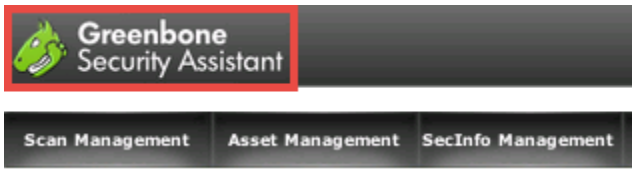
12. Select **Extras > CVSS Calculator** from the top pane.



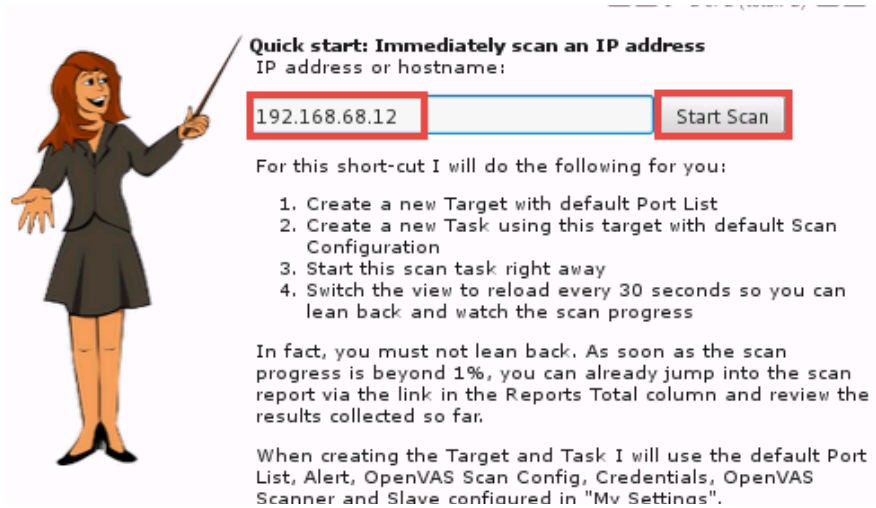
13. The calculator shown here can make calculations based on several different vectors a CVSS score that is used for rating CVEs.

2 Quick Scanning with OpenVAS

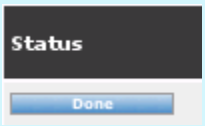
1. Navigate back to the home page by clicking on the **Greenbone Security Assistant** logo.



2. Configure a default scan against the OWASP server by typing the *IP* address [**192.168.68.12**] into the *Quick start* text field.
3. Click **Start Scan**.

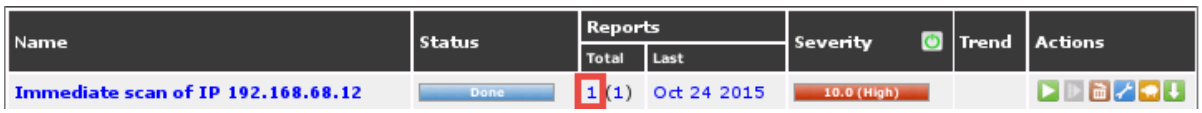


Wait about 15-20 minutes until the scan finishes before moving on to the next step. The scan will finish once the progress bar reach 100% or "Done".



Notice the screen will refresh periodically.

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



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

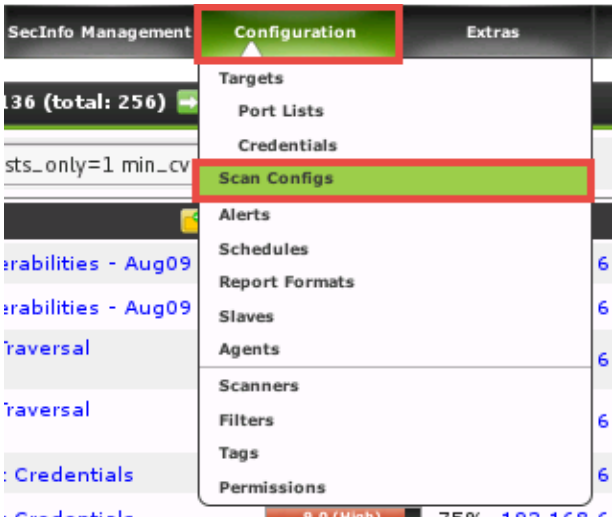
Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Sat Oct 24 16:48:27 2015	Done	Immediate scan of IP 192.168.68.12	10.0 (High)	19	35	5	77	0	

√Apply to page contents

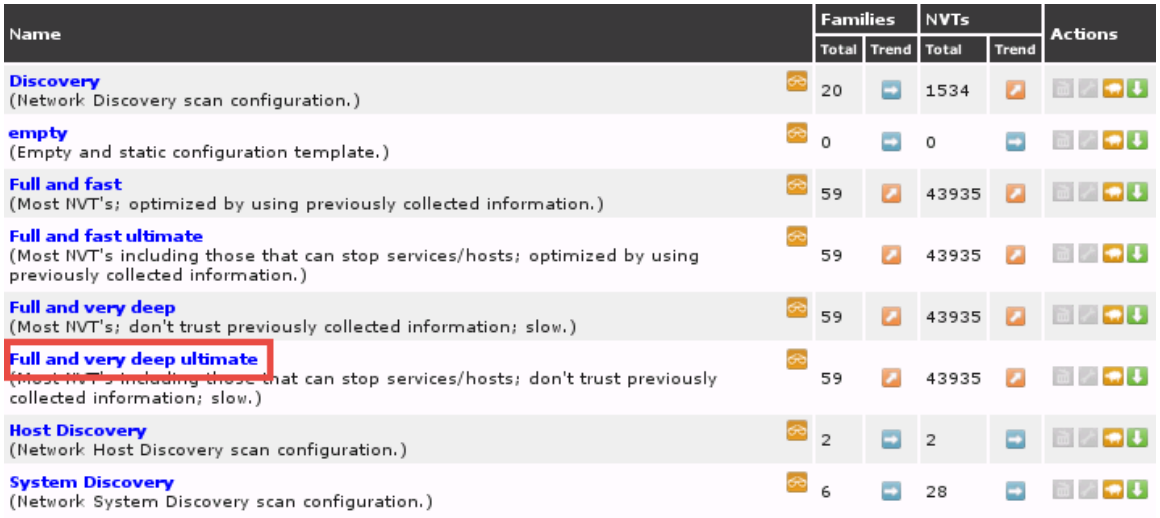
6. Analyze the vulnerabilities listed in the report.

3 Customized Scanning with OpenVAS

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



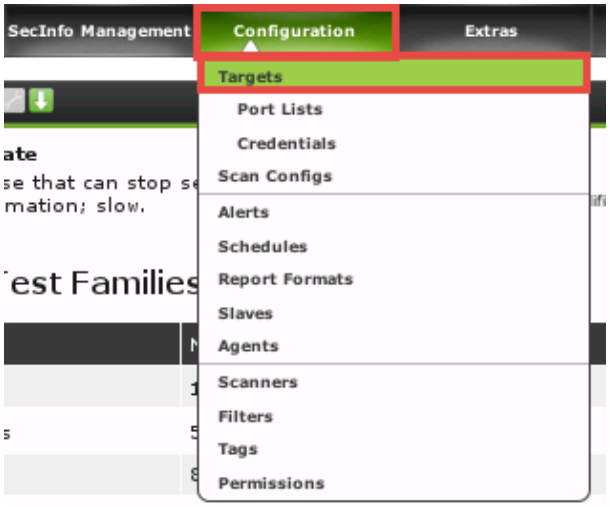
2. Click on the **Full and very deep ultimate** link.



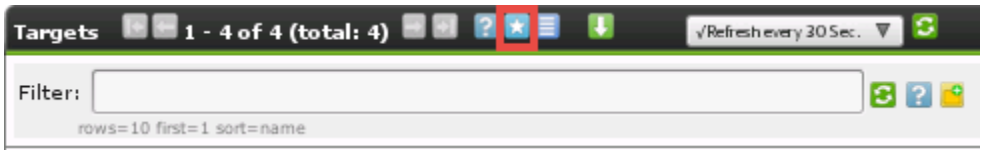
Name	Families Total	Families Trend	NVTs Total	NVTs Trend	Actions
Discovery (Network Discovery scan configuration.)	20		1534		
empty (Empty and static configuration template.)	0		0		
Full and fast (Most NVT's; optimized by using previously collected information.)	59		43935		
Full and fast ultimate (Most NVT's including those that can stop services/hosts; optimized by using previously collected information.)	59		43935		
Full and very deep (Most NVT's; don't trust previously collected information; slow.)	59		43935		
Full and very deep ultimate (Most NVT's including those that can stop services/hosts; don't trust previously collected information; slow.)	59		43935		
Host Discovery (Network Host Discovery scan configuration.)	2		2		
System Discovery (Network System Discovery scan configuration.)	6		28		

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.

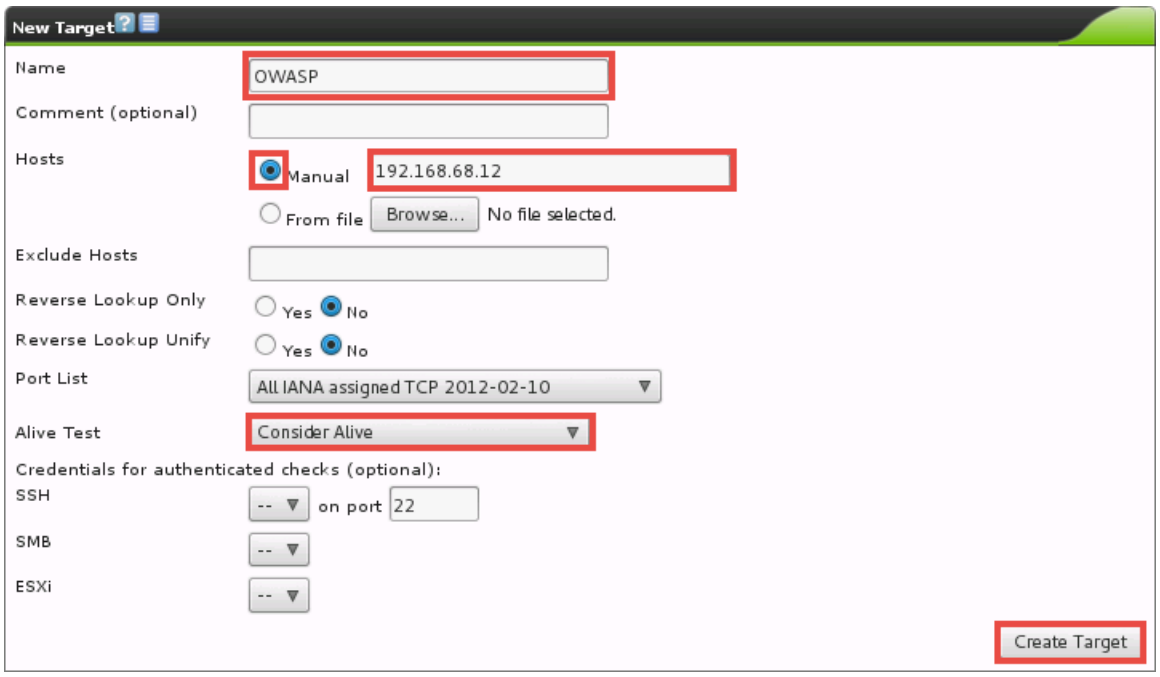
3. Select **Configuration > Targets** from the top pane.



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

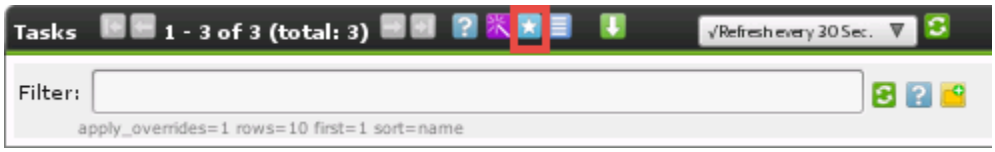


5. Configure the new target with the information below:
   a. Name: **OWASP**
   b. Hosts: **Manual**
      192.168.68.12
   c. Alive Test: **Consider Alive**
   d. Leave rest defaults.

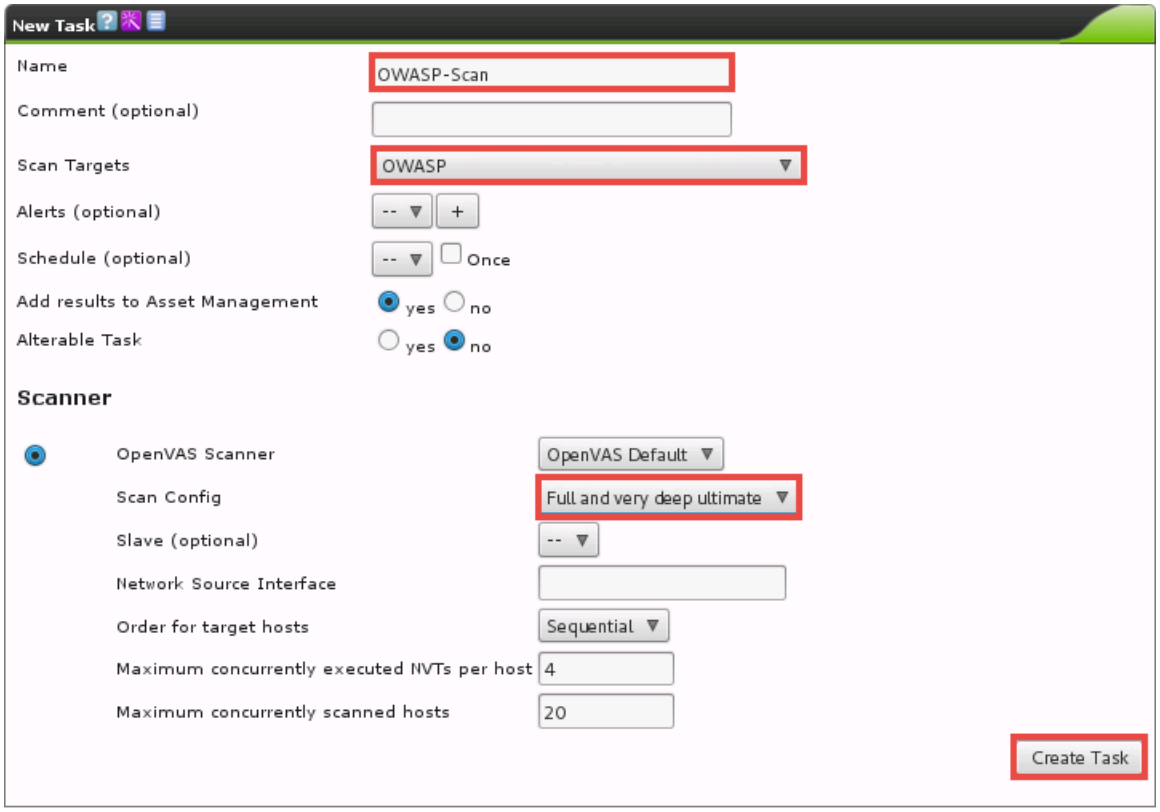


6. Click **Create Target**.
7. Click on **Scan Management** from the top pane.

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 rest defaults



10. Click **Create Task**.

11. 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 in 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.

12. Close the **Kali** PC viewer.

