

Installation Tutorial: OpenVAS

Christopher Raley

Department of Computer Science, University of Virginia

6/3/2018

This document presents a tutorial for OpenVAS on the Kali Attacker VM. There are step-by-step instructions on how to properly update your system in order to successfully install OpenVAS, as well as starting the proper services required to run it. This tutorial assumes that you already have the Kali Attacker VM and Metasploitable VM installed on your machine. This content has been provided for education purposes only.

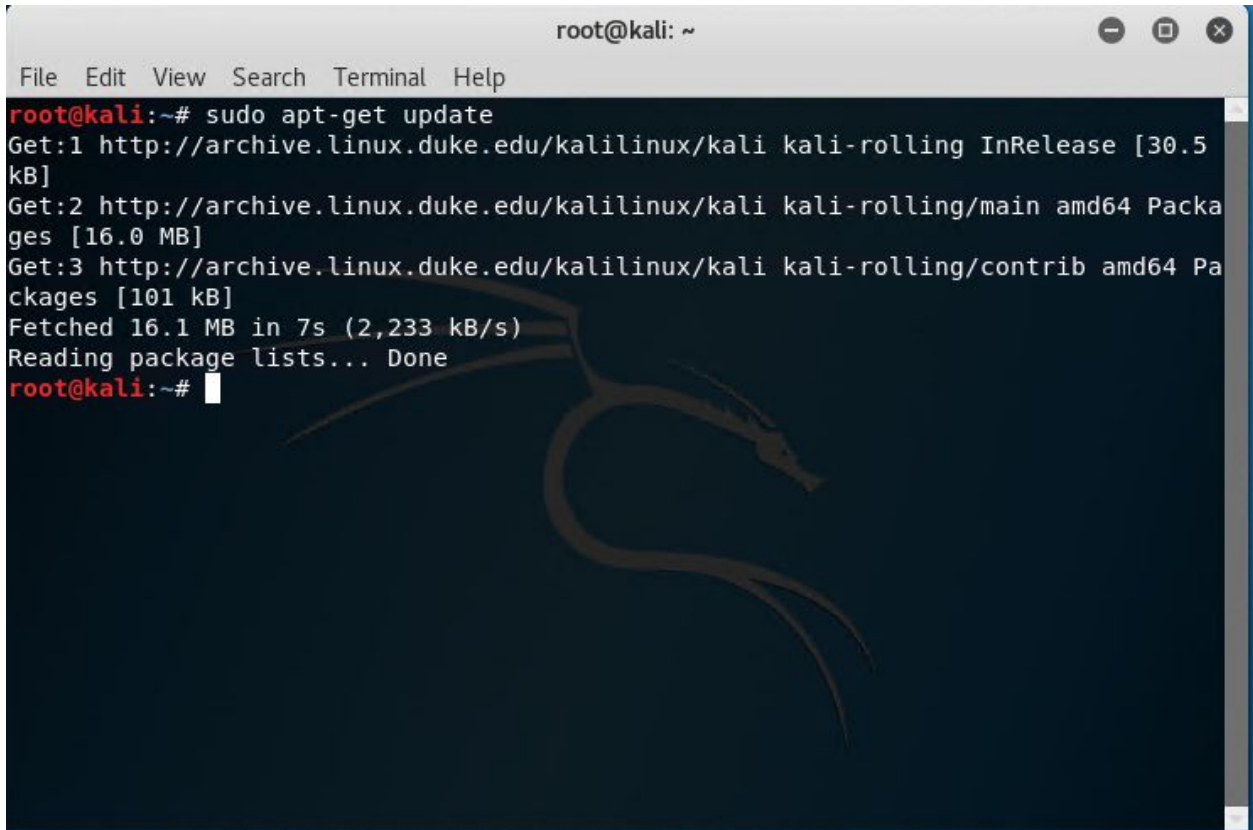
Introduction

OpenVAS is a framework that aids users in scanning vulnerable machines and assessing their vulnerabilities. Ultimately, the purpose of OpenVAS for us is to find any potential exploits that an attacker may try and patch them as soon as possible. There are many different types of tools and frameworks that would help us accomplish this goal, but for the sake of simplicity and consistency with regards to the rest of our tutorials, we will use OpenVAS. At the end of the tutorial, we will show you how to add Metasploitable 2 as one of our targets for OpenVAS's vulnerability scanning tool and how to scan it properly.

Upgrade Kali

Before we start installing OpenVAS, we need to make sure that our VM is up-to-date (parts of the OpenVAS installation requires our VM to be updated). We will first make sure our keys that access Kali's main repositories are not expired, then we will upgrade our distribution.

1. In order to check our keys aren't expired type "sudo apt-get update"
 - If you received an error saying that your signatures are invalid, then enter the following: "wget -q -O - https://archive.kali.org/archive-key.asc | apt-key add" and try updating again
 - If you received no errors, then that means your keys are not expired

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows the command 'sudo apt-get update' being executed. The output indicates that three repositories were updated: 'kali-rolling InRelease' (30.5 kB), 'kali-rolling/main amd64 Packages' (16.0 MB), and 'kali-rolling/contrib amd64 Packages' (101 kB). The total data fetched was 16.1 MB in 7 seconds at a rate of 2,233 kB/s. The package lists were read successfully. The terminal background features a faint, stylized dragon logo, which is the Kali Linux logo. The window has standard Linux window controls (minimize, maximize, close) in the top right corner.

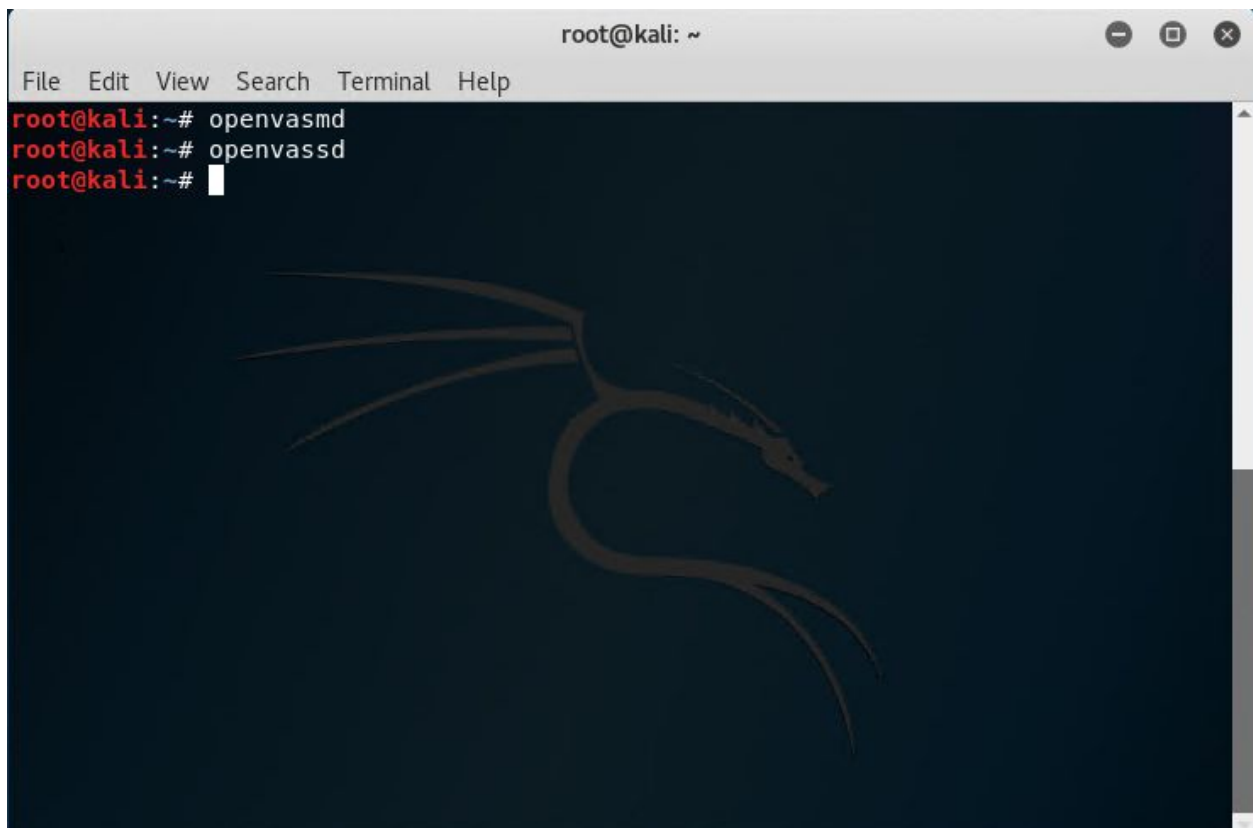
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sudo apt-get update  
Get:1 http://archive.linux.duke.edu/kalilinux/kali kali-rolling InRelease [30.5  
kB]  
Get:2 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/main amd64 Packa  
ges [16.0 MB]  
Get:3 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/contrib amd64 Pa  
ckages [101 kB]  
Fetched 16.1 MB in 7s (2,233 kB/s)  
Reading package lists... Done  
root@kali:~#
```

2. Open up a terminal in the Kali VM and type the following "sudo apt-get dist-upgrade"
 - Make sure to accept every upgrade
 - Note: This can take a very long time, so you may need to leave your machine running for a while (may be up to a couple of hours)

Installing/Setting Up OpenVAS

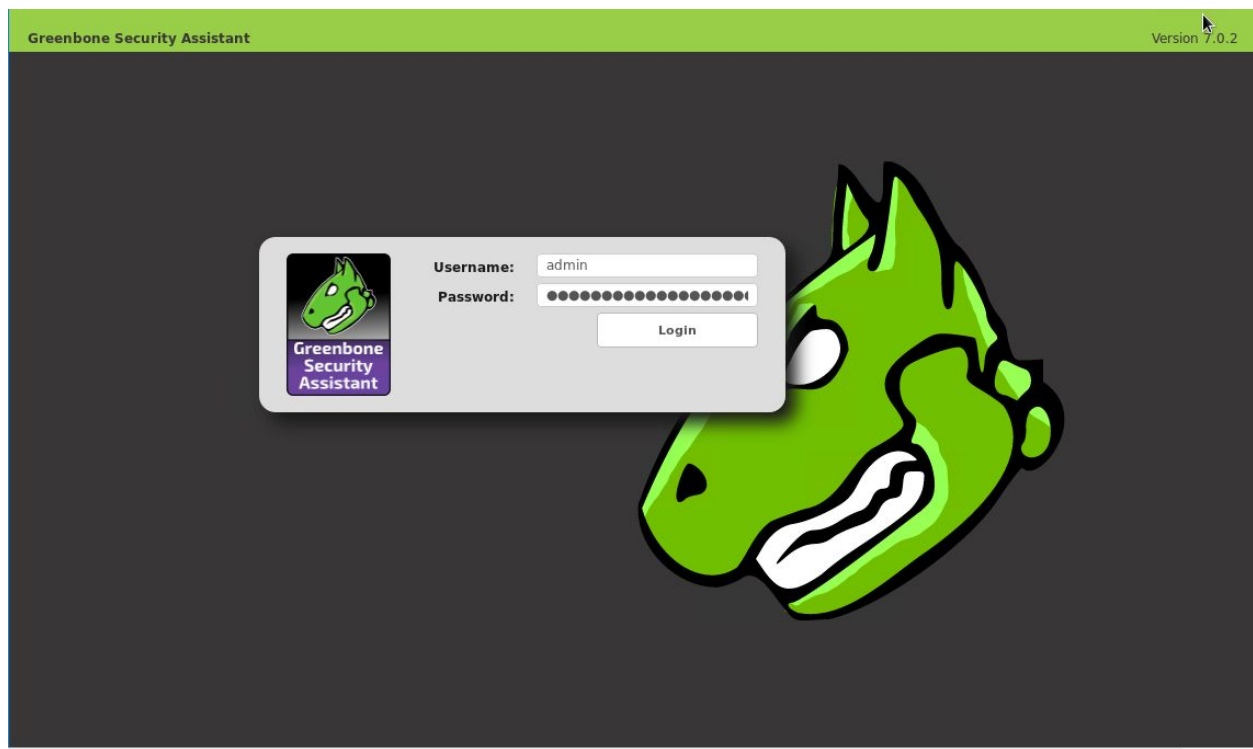
We are now ready to install OpenVAS which is a straightforward process. There are also a couple of services that need to be running before starting OpenVAS.

1. In a terminal type “sudo apt-get update && sudo apt-get install openvas”, this will start our installation process for OpenVAS
 - Do not clear the terminal, look towards the end of the installation as you will be given a password to record (do not forget it)
 - This password will be used in order to access the admin account
2. Now you are ready to start the program by using “openvas-start”
 - If you receive an error then make sure to type “openvasmd” and “openvassd” (services that must be running for OpenVAS to work)
 - Type “openvas-start” once those services are running

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal output shows three lines of commands entered at the root prompt: 'openvasmd', 'openvassd', and a blank line with a cursor. In the background, a faint Kali Linux dragon logo is visible.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# openvasmd  
root@kali:~# openvassd  
root@kali:~#
```

- You will be greeted with a login screen. For username enter “admin” and for password enter the password that was generated for you during the installation



- After logging in, go to the navigation bar at the top and select Configuration → Targets



- Click on the blue button with the star at the top left of the page
- Enter “Metasploitable 2” for the name and change “192.168.1.23” to the IP address of the Metasploitable machine then press Create

New Target

Name

Metasploitable 2

Comment

Hosts

☒ Manual

192.168.1.23

☐ From file

Browse... No file selected.

☐ From host assets (0 hosts)

Exclude Hosts

Reverse Lookup Only

☐ Yes
 ☒ No

Reverse Lookup Unify

☐ Yes
 ☒ No

Port List

All IANA assigned TCP 20...

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

-- on port 22

Create

- We will now create a task which will tell the scanner what type of scan we want.
Go to Scans → Tasks

Greenbone Security Assistant

No auto-refresh

Logged in as Admin **admin** | Logout
Sun Jun 3 19:51:21 2018 UTC

Dashboard

Scans

Assets

SecInfo

Configuration

Extras

Administration

Help

Dashboard

Tasks

Reports

Results

Notes

Overrides

Filter:

rows=10 first=1 sort=name

Name	Hosts	IPs	Port List	Credentials - sort by: SSH	Actions
Metasploitable 2	192.168.1.23	1	All IANA assigned TCP 2012-02-10		

(Applied filter: rows=10 first=1 sort=name)

Backend operation: 4.03s

- Click on the blue button with the start at the top left of the page and then go to New Task

Greenbone Security Assistant

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name

New Task New Container Task New Task

Tasks (1 of 1)

Tasks by Severity Class (Total: 1)

Tasks with most High results per host

Tasks by status (Total: 1)

Name	Status	Reports	Severity	Trend	Actions
		Total	Last		
Scan Metasploitable 2	Done	1 (1)	May 31 2018	10.0 (High)	

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

https://127.0.0.1:9392/omp?cmd=new_task&next=get_task&filter=min_qod=70 apply_overrides=1 rows=10 first=1 sort=name&filt_id=&token=072f8260-6ee2-45b1-a047-44910371ccbd

- Make sure to name the task “Scan Metasploitable 2”, set the target to be “Metasploitable 2”, and check the Only Once box then click Create

New Task

Name Scan Metasploitable 2

Comment

Scan Targets Metasploitable 2

Alerts

Schedule -- ☒ Once

Add results to Assets ☒ yes ☐ no

Apply Overrides ☒ yes ☐ no

Min QoD 70 %

Alterable Task ☐ yes ☒ no

Auto Delete Reports ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 reports

Scanner OpenVAS Default

Create

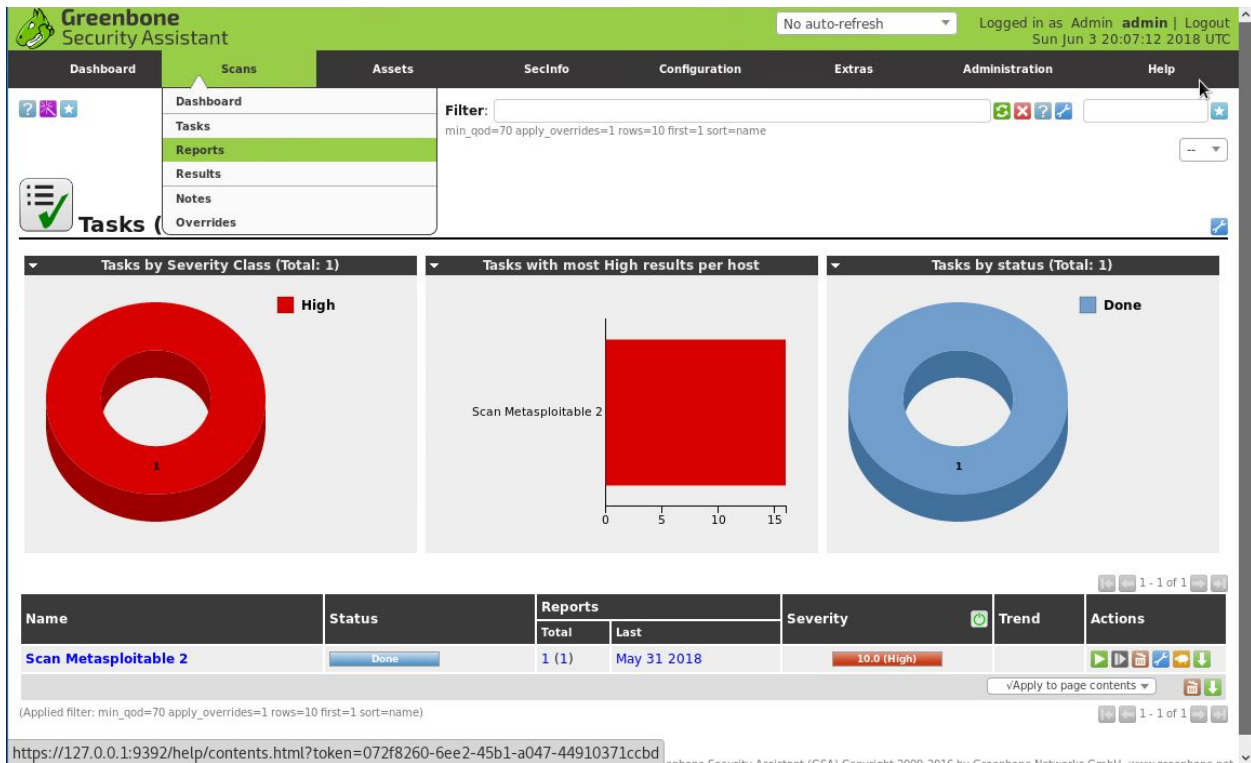
- In order to scan the machine we will go to the bottom of the page where we see a row with the name "Scan Metasploitable 2". In the actions column, click the green play button (this will start the scan)

Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Scan Metasploitable 2	Done	1 (1)	May 31 2018	10.0 (High)		<div> <div>Start</div> <div> <div>1 of 1</div> </div> </div>

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

- Refresh the page in order to see the progress of the scan

- Once the scan has finished, go to Scans → Reports from the navigation bar




- Click on the date that you started the scan


Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu May 31 06:37:51 2018	Done	Scan Metasploitable 2	10.0 (High)	16	28	3	75	0	<div> <div>Start</div> <div> <div>1 of 1</div> </div> </div>

(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)

13. You will now be able to see all the vulnerabilities within Metasploitable 2









































DashboardScansAssetsSecInfoConfigurationExtrasAdministrationHelp

**Report: Results (47 of 337)**

ID: 1766f88a-2af9-4a7a-b789-a90df08630f0
Modified: Thu May 31 07:06:23 2018
Created: Thu May 31 06:38:30 2018
Owner: admin

1 - 47 of 47

Vulnerability	Severity	QoD	Host	Location	Actions
Check for rexecd Service	10.0 (High)	80%	192.168.1.23	512/tcp	 
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80%	192.168.1.23	80/tcp	 
OS End Of Life Detection	10.0 (High)	80%	192.168.1.23	general/tcp	 
Possible Backdoor: Ingreslock	10.0 (High)	99%	192.168.1.23	1524/tcp	 
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99%	192.168.1.23	8787/tcp	 
DistCC Remote Code Execution Vulnerability	9.3 (High)	99%	192.168.1.23	3632/tcp	 
PostgreSQL weak password	9.0 (High)	99%	192.168.1.23	5432/tcp	 
MySQL / MariaDB weak password	9.0 (High)	95%	192.168.1.23	3306/tcp	 
DistCC Detection	8.5 (High)	95%	192.168.1.23	3632/tcp	 
Check for rlogin Service	7.5 (High)	70%	192.168.1.23	513/tcp	 
phpinfo() output accessible	7.5 (High)	80%	192.168.1.23	80/tcp	 
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5 (High)	80%	192.168.1.23	80/tcp	 
Test HTTP dangerous methods	7.5 (High)	99%	192.168.1.23	80/tcp	 
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.1.23	6200/tcp	 
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99%	192.168.1.23	21/tcp	 
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.1.23	22/tcp	 
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80%	192.168.1.23	80/tcp	 
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.168.1.23	5432/tcp	 
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99%	192.168.1.23	25/tcp	 
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80%	192.168.1.23	80/tcp	