v4

# Penetration Testing Student

## Vulnerability Assessment

Section 03 | Module 03

# Table of Contents

## MODULE 03 | Vulnerability Assessment

# Learning Objectives

By the end of this module,  you should have a better understanding of:

- ✓ Automatic vunlerability detection
- ✓ Common tools that are used for vulnerability assessment

3.1

# Vulnerability Assessment

# 3.1 Vulnerability Assessment

## How does this support my pentesting career?

You should be able to:

- Identify vulnerabilities and security misconfigurations
- Prepare yourself for the exploitation phase

# 3.1 Vulnerability Assessment

During the *"Lifecycle of a Penetration test"* module, we saw that the **vulnerability assessment** is a phase of the penetration testing process.

Sometimes, however, a client just asks for a vulnerability assessment instead of a full pentest.

# 3.1 Vulnerability Assessment

As clients may not have the know-how to understand if they just need an assessment or a full penetration test, it is your duty to **understand their needs and help them** choose the best solution for their enterprise.

# 3.1 Vulnerability Assessment

Since a vulnerability assessment is a scan of the vulnerabilities found on networks and applications, it is also **faster** and has a **lighter load** on the infrastructure.

As opposed to a penetration test, during a vulnerability assessment, you do not proceed to the exploitation phase.

# 3.1 Vulnerability Assessment

This implies that you will not be able to **confirm** the vulnerabilities by testing them and giving proof of their existence.

Moreover, you will not be able to **cycle** after the exploitation phase.

# 3.1 Vulnerability Assessment

We can say that the vulnerability assessment is more of a linear process as opposed to a penetration test which is more in depth, both in terms of vulnerabilities **discovered** (thanks to the cyclic process) and vulnerabilities tested.

# 3.1.1 Vulnerability Scanners

A vulnerability assessment, in the same manner as a penetration test, can be carried out both locally and remotely.

Checking one or more systems for all the known vulnerabilities would be infeasible so that penetration testers can use a **vulnerability scanner**.

# 3.1.1 Vulnerability Scanners

Scanners use a database of known vulnerabilities and security audits to detect the vulnerabilities of a system. Scanners perform their probes on:

- Daemons listening on TCP and UDP ports
- Configuration files of operating systems, software suites, network devices, etc.
- Windows registry entries

The purpose is to find vulnerabilities and misconfigurations.

# 3.1.1 Vulnerability Scanners

The scanner's vendor keeps the tool up to date and constantly updates its database with new security checks and vulnerabilities signatures.

The more the database is up to date, the better and more relevant the scan results will be.

# 3.1.1 Vulnerability Scanners

There are a lot of vulnerability scanners out there, like OpenVAS, Nexpose or GFI LAN Guard.

Nessus is one of the most popular vulnerability scanners. You will see Nessus in action in the next chapter.

http://www.openvas.org/
http://www.rapid7.com/products/nexpose/index.jsp
http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
http://www.tenable.com/products/nessus

# 3.1.2 Manual Testing

If you have to test a custom application, a vulnerability scanner may not be enough; you have to test it **manually**!

Testing a custom application is very similar to testing a web application.

# 3.1.2 Manual Testing

Studying custom applications means:

- Learning and understanding its features
- Understanding how it exchanges data over the network
- Understanding how it accesses resources like databases, servers, local and remote files and so on
- Reverse engineering its logic

3.2

# Nessus

# 3.2 Nessus

**Nessus** is an easy to use yet powerful vulnerability scanner that works great both on a small and a large company network.

It has a free license for non-commercial use, so you can install and use it to secure your home network or to perform exercises in Hera Lab. You can download it here.

# 3.2.1 Architecture

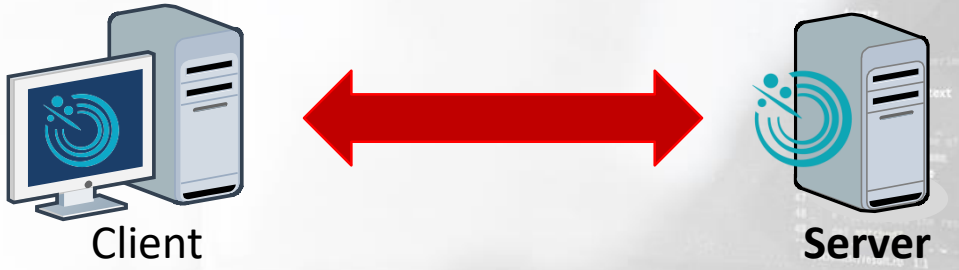
Nessus has two components: a **client** and a **server**. You will use the client to configure the scans and the server to actually perform the scanning processes and report the results back to the client.

# 3.2.1 Architecture

The **client component** provides you with a **web interface** to configure your scans.

# 3.2.1 Architecture

The **server component** performs the scans by sending probes to systems and applications, collecting the responses and matching them against its vulnerability database.



# 3.2.1 Architecture

You can run both components on the same machine; this is a simple yet effective configuration for a home network or a lab environment.

# 3.2.2 Under the Hood of a Vulnerability Scanner

Understanding how vulnerability scanners work will help you configure and use Nessus at its best.

Every vulnerability scanner roughly performs the same steps during a scan. Let's see them in detail.

# 3.2.2.1 Port Scanning

The first step is determining if the target hosts are alive and which ports are open on them; to do that, the vulnerability scanner performs a port scan to test the open ports on the systems. The more accurate the port scan is, the more useful results the vulnerability scanner will get.

You will see how port scanning works in the *Footprinting and Scanning* module.

# 3.2.2.2 Service Detection

For every open port found, the vulnerability scanner will send special probes to determine which application (name and version) is running on them.

# 3.2.2.3 Vulnerabilities Database Lookup

For each detected service (also known as a daemon), the scanner queries its database looking for known vulnerabilities.

When configuring the scanner, you can configure which vulnerabilities you want to check for.

Example:

*You can configure a scanner to ignore the operating system vulnerabilities and test only known web server vulnerabilities.*

# 3.2.2.4 Probing

During the last step, the scanner sends **probes** to verify if the vulnerability actually exists.

This phase is prone to **false positives** as some probes could be too mild to effectively identify a real vulnerability.

# 3.2.3 Video – Nessus

## Nessus

In this video, you will see how to install and configure Nessus on Kali Linux. You learn how to configure Nessus' policies and start a scan. Finally, you will see the report produced by Nessus and how to download it.


**Videos are only available in Full or Elite Editions of the course. To upgrade, click HERE. To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*

# 3.2.4 Hera Lab – Nessus

You are now ready to practice in the Hera Lab environment. In this lab, you will use *Nessus* to perform a vulnerability scan on a target machine.

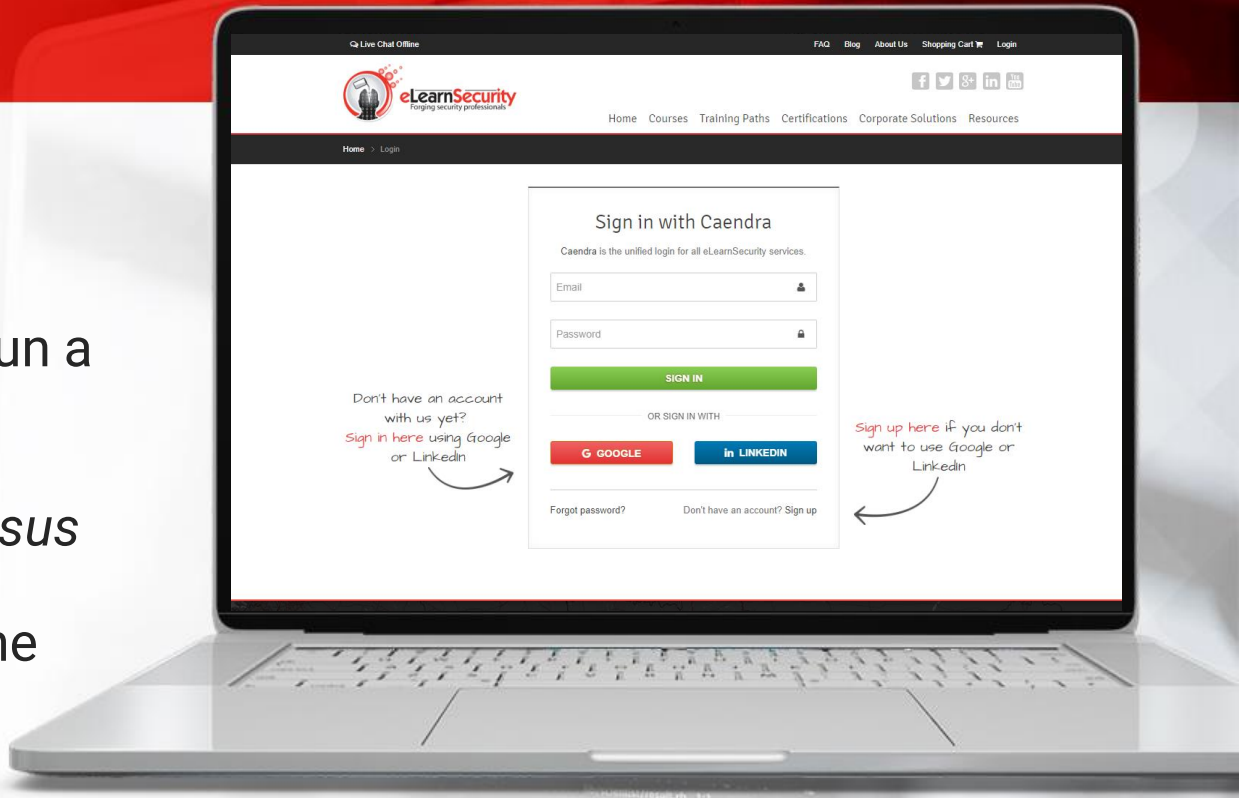
As usual, try to solve the challenge by yourself. If you get stuck, you can check the solutions in your Members Area.

# 3.2.4 Hera Lab – Nessus Lab

## Nessus

In this lab you will:

- Configure *Nessus* to run a vulnerability scan
- Run the scan
- Review the report *Nessus* produces
- Prepare yourself for the exploitation phase




**Labs are only available in Full or Elite Editions of the course. To upgrade, click **HERE**. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.*

# References

# References

## Nessus

http://www.tenable.com/products/nessus

## Nexpose

http://www.rapid7.com/products/nexpose/index.jsp

## OpenVAS

http://www.openvas.org/

## GFI LAN Guard

http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard

# References

Top Vulnerability Scanners

http://sectools.org/tag/vuln-scanners/

# Videos

## Nessus

In this video, you will see how to install and configure Nessus on Kali Linux. You learn how to configure Nessus' policies and start a scan. Finally, you will see the report produced by Nessus and how to download it.

**Videos are only available in Full or Elite Editions of the course. To upgrade, click HERE. To access, go to the course in your members area and click the resources drop-down in the appropriate module line.*

# Labs

## Nessus

Perform a vulnerability scan with Nessus.

**Labs are only available in Full or Elite Editions of the course. To upgrade, click HERE. To access, go to the course in your members area and click the labs drop-down in the appropriate module line or to the virtual labs tabs on the left navigation.*