University of M'sila
Faculty of Mathematics and Computer Science
Department of Computer Science
branch: Master RTIC2

# Course 5: Penetration Testing

SAOUDI Lalia
Master RTIC :2025-2026

# vulnerability audit and Penetration Testing

**1- Introduction:** In the field of computer security, a vulnerability is a weakness in a computer system that allows an attacker to compromise the integrity of that system and the confidentiality and integrity of the data it contains.

A penetration test is a method of assessing the security of a system or network. The method involves simulating an attack by a malicious user or even malware.

# Penetration Testing

## 2. Definition:

A simulated cyber attack against a computer system, network, or web application to identify and exploit security vulnerabilities.

A penetration test begins with a vulnerability research phase

It is a proactive and authorized simulation, unlike a real-world hack.

Goal: To find security weaknesses before malicious actors do and provide actionable recommendations for remediation.

# 3. Vulnerability Audit & Penetration Testing

a vulnerability test aims to detect known vulnerabilities on systems, while a penetration test aims to simulate an attack by discovering and exploiting vulnerabilities.
In other words, a penetration test, in addition to identifying vulnerabilities, exploits them in order to verify the actual impacts of the intrusions.

# 4. Motivations

1- To know or verify the state of security of the technological infrastructure (workstations, servers, networks, etc.);

2- Validate the security of a system before it goes into production or during its development (coding, configuration, etc.).

# Key Terminology

**Vulnerability**: A weakness in a system that can be exploited.

**Exploit**: A piece of code, technique, or sequence of commands that leverages a vulnerability to cause unintended behavior.

**Payload**: The code that we deliver to the target system to achieve a specific goal (e.g., a reverse shell).

**Privilege Escalation**: Gaining higher-level permissions on a system (e.g., from a standard user to an administrator).

**Persistence**: Maintaining access to a system even after it reboots.

**Pivoting:** Using a compromised system to attack other systems on its internal network.

# 5. Penetration testing types

Penetration tests are categorized based on what is being tested (the target) and how it is tested (the perspective and knowledge level).

# 5. Penetration testing types : knowledge level

This defines the amount of information the tester has about the target at the start of the engagement :

**1. Black Box Testing** : The tester approaches the target as a real-world external attacker would, with no prior information about the internal systems, network structure, or source code.

**2. White Box Testing** : The tester is provided with complete information about the target, including network diagrams, source code, credentials, and system architecture.

**3. Gray Box Testing** : A hybrid approach. The tester is given some limited information, such as low-privilege user credentials or basic network layout.

# 5. Penetration testing types : TARGET / SCOPE level

This defines the technological focus of the test.

**1. Network Penetration Testing**

The most common type. Focuses on finding vulnerabilities in network infrastructure, including devices, servers, and services.

**External**: Tests the public-facing assets (IP addresses, DMZ) from the internet.

**Internal**: Tests the internal corporate network, simulating an attacker who has physical access or a compromised employee machine.

**Common Targets**: Firewalls, routers, switches, servers (SSH, SMB, RDP), and network services.

# 5. Penetration testing types : TARGET / SCOPE level

2. Web Application Penetration Testing

A deep-dive assessment of web applications (websites, APIs, web services) to find security flaws.

**Focus**: Identifying vulnerabilities from the OWASP Top 10 list, such as:

Injection (SQLi, Command Injection)

Broken Authentication

Sensitive Data Exposure

Cross-Site Scripting (XSS)

**Methodology**: Often follows the OWASP Testing Guide.

# 5. Penetration testing types : TARGET / SCOPE level

**3. Wireless (Wi-Fi) Penetration Testing**

Assesses the security of wireless networks within an organization's premises.

**Focus**:

Testing the strength of Wi-Fi encryption (WPA2, WPA3).

Rogue Access Point detection.

Testing guest network segregation.

Weak authentication protocols (e.g., LEAP).

# 5. Penetration testing types : TARGET / SCOPE level

**4. Social Engineering**

Tests the "human element" of security by manipulating personnel to break normal security procedures.

***Phishing***: Sending deceptive emails to trick users into clicking malicious links, downloading malware, or entering credentials on fake login pages.

***Vishing***: Voice phishing (phone calls).

Smishing: SMS phishing.

***Physical Tailgating:*** Attempting to gain physical access to a restricted area by following an employee.

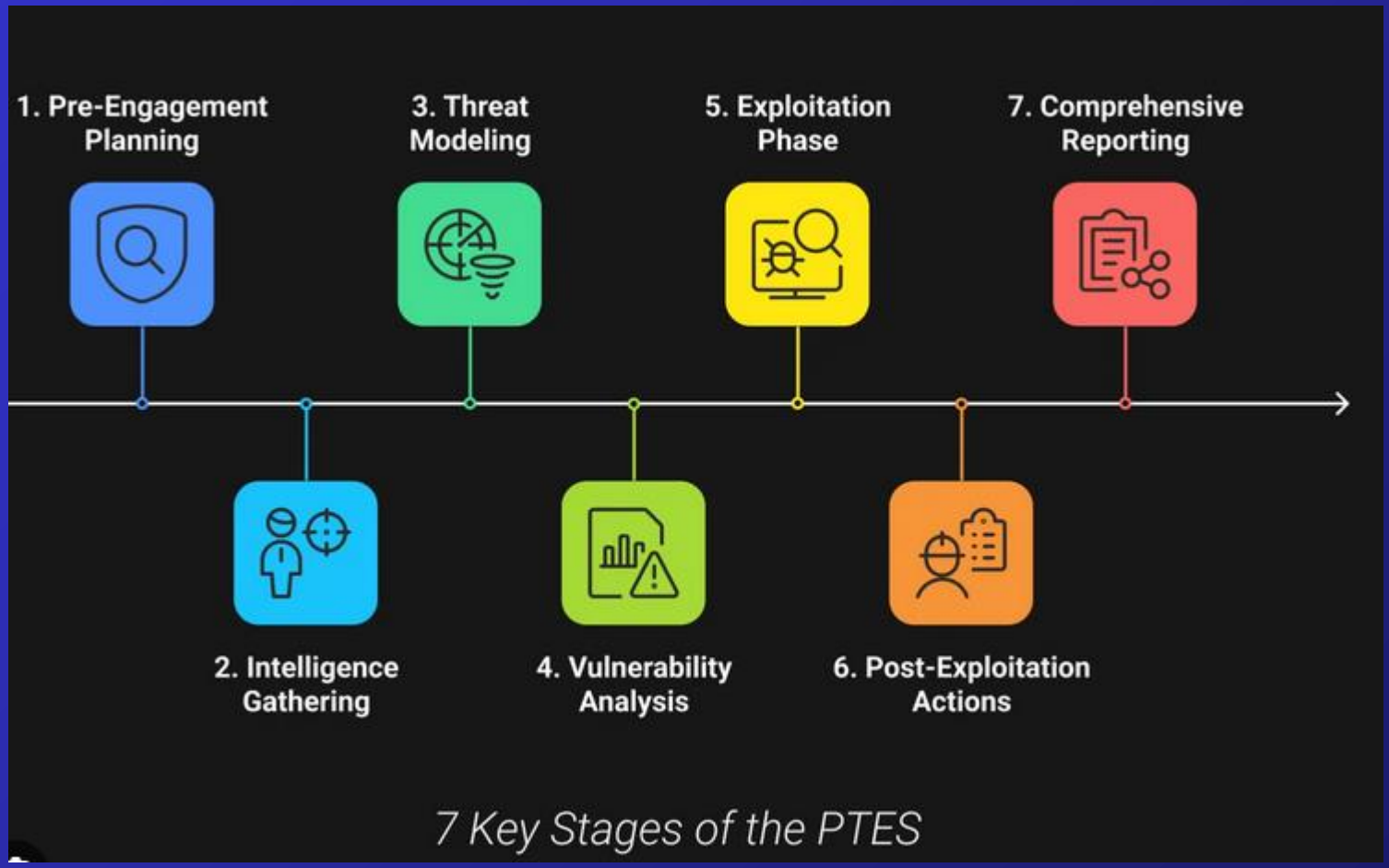
# 6. Red Team vs. Blue Team vs. Purple Team

**Red Teaming:** A full-scope, multi-layered attack simulation designed to test an organization's overall security posture and defensive capabilities (People, Processes, and Technology). It is goal-oriented (e.g., "steal the customer database") and is typically performed over a longer period without the Blue Team's knowledge of the specific tactics.

**Blue Teaming:** The defensive team (the organization's SOC and IT security staff) whose goal is to detect, respond to, and mitigate the Red Team's attacks.

**Purple Teaming:** A collaborative exercise where the Red Team provides continuous feedback to the Blue Team during the engagement. The goal is not just to test defenses but to improve them in real-time.

# 7 phases of Penetration Testing Execution Standard (PTES)



# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 1: Pre-engagement Interactions**

**Goal**: To define the scope, rules, and goals of the test before any technical work begins.

This phase is critical for legal and operational safety.

**Key Activities:**

- ***Scope Definition:*** Clearly outlining what is in and out of bounds.

  ***Targets:*** Specific IP addresses, URL domains, network ranges, or physical locations.

  **Restrictions**: Systems that are off-limits (e.g., production databases), types of tests that are prohibited (e.g., Denial-of-Service attacks).

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 1: Pre-engagement Interactions**

**Key Activities:**

***Rules of Engagement (RoE):*** A formal document specifying:

- Timing: When the test can occur (e.g., business hours, after-hours).
- Communication: How and when to report critical findings.
- Authorization: The "get out of jail free" card that legally permits the test.
- Goal Setting: Determining the objective (e.g., "achieve domain administrator access," "steal a specific file," "compromise the web application").

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 1: Pre-engagement Interactions**

**Example**:

A client, "XYZ," wants a test of their external perimeter and new web application.

Scope: 192.0.2.1-192.0.2.50 and https://www.XYZ.com.

RoE: Testing is authorized between 6:00 PM and 2:00 AM for one week.

Do not test the IP 192.0.2.10 (their main mail server).

Immediately notify the CISO if a critical vulnerability is found.

Goal: Determine if an attacker can access the customer database on the web server.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 2: Intelligence Gathering (Reconnaissance)**

**Goal**: To collect as much information as possible about the target to identify potential attack vectors.

**Key Activities:**

***Passive Reconnaissance***: Gathering information without sending any packets to the target.

Tools: whois, nslookup, theHarvester, social media (LinkedIn), search engines (Google Hacking).

***Active Reconnaissance:*** Directly interacting with the target to discover details.

**Tools**: nmap (port scanning), Nikto (web server scanning), enum4linux (SMB enumeration).

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 2: Intelligence Gathering (Reconnaissance)**

**Example:**

***Passive:*** A whois lookup for abccorp.com reveals the domain's registration information and name servers.

LinkedIn shows an employee named "John Smith" who is a "System Administrator."

***Active:*** An nmap scan of 192.0.2.1-50 finds that 192.0.2.25 has port 80 (HTTP) and 443 (HTTPS) open.

A scan of the web server with Nikto reveals it's running Apache 2.4.41 on Ubuntu.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 3: Threat Modeling**

**Goal**: To analyze the gathered intelligence and prioritize potential threats based on the value of the assets and the likelihood of an attack.

**Key Activities:**

1) ***Identify Assets:*** What is valuable? (e.g., customer database, source code, financial records).

2) ***Identify Threats:*** Who would attack it and why? (e.g., a competitor might want the customer list, hacktivists may want to deface the website).

3) ***Identify Vulnerabilities:*** Based on Phase 2, what weaknesses can be leveraged? (e.g., an outdated web server version, an exposed login page).

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 3: Threat Modeling**

**Example**:

Asset: The customer database on https://shop.abc.com.

Threat: A financially motivated attacker wanting to steal credit card information.

Vulnerability Analysis: The login page (/admin) is a high-value target.

The Apache version might have known exploits. The employee "admin" could be targeted for a phishing attack.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 4: Vulnerability Analysis**

**Goal**: To systematically discover and validate vulnerabilities in the targeted systems.

**Key Activities:**

***Automated Scanning:*** Using tools to quickly scan for known vulnerabilities.

Tools: Nessus, OpenVAS, Nexpose.

***Manual Analysis & Validation:*** Manually testing for vulnerabilities that scanners might miss.

***Techniques***: Fuzzing web inputs, analyzing application logic, manually inspecting source code (if white-box).

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 4: Vulnerability Analysis**
**Example**:

- An automated Nessus scan flags the Ubuntu server as having a potential OpenSSL vulnerability (CVE-2021-3449).
- Manually testing the login form at https://shop.abc.com/admin, you try SQL injection payloads and find it causes a database error, indicating it might be vulnerable.

# phases of Penetration Testing Execution Standard (PTES)

**Tools for collecting public information:**

-The RIPE Whois database lists all subnetworks and their respective owners: http://www.ripe.net/db/whois/whois.html..

-Websites.

**B- Stage of mapping the target network**

The tools used in this stage gather information regarding the network topology to determine its structure. Among these tools, we can find:

**ROUTING TOOLS:**

To determine the machines located between the target servers and ourselves, we will study the routing of exchanged packets. For this, we use: traceroute

**SMTP ROUTING**

Sending an email to a non-existent address in the domain triggers the return of an error email containing interesting information.

**PORT SCANS**

Port scanning is the least discreet discovery method, but it is most often indispensable. It involves sweeping the target to determine which ports are open (listening) for each supported protocol on the machines.

# phases of Penetration Testing Execution Standard (PTES)

**key elements necessary for vulnerability research:**

***the types of services***

For example, a web service, an incoming/outgoing email service, an instant messaging service, a database service, etc.

***the products used to provide the service:***

For example, for a database service, among others, we find MySQL, MSSQL Server, PostgreSQL, etc.

***the version of the products used***

For example, for the MS SQL Server product, there are several versions and, for each, there could be revisions or service packs.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 5: Exploitation**

***Goal***: To actively exploit the identified vulnerabilities to gain unauthorized access to the target systems.

***Key Activities:***

Attempting to breach the system using the vulnerabilities found.

Using tools like the Metasploit Framework or custom exploits.

Gaining an initial foothold, often a shell on the target machine.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 5: Exploitation**

***Example:***

***You find OpenSSl service installed***

You search for the OpenSSL vulnerability (CVE-2021-3449) in Metasploit and find an exploit module.

You configure the module with the target's IP and run it.

Success! The exploit works, and you receive a meterpreter shell on the target web server with the user privileges

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 6: Post-Exploitation**

**Goal:** To demonstrate the business impact of the initial breach, maintain access, and pivot to other systems.

**Key Activities:**

Privilege Escalation: Gaining higher-level privileges .

Persistence: Installing a backdoor to maintain access after a reboot.

Lateral Movement: "Pivoting" from the compromised host to others on the internal network.

Data Exfiltration: Stealing sensitive data (as defined in the RoE) to prove impact.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 7: Reporting**

**Goal**: To deliver a clear, actionable report that details the findings, the risks, and the steps for remediation. This is the most important phase.

**Key Activities:**

Creating a report with two main components:

Executive Summary: For management. Non-technical, focusing on business risk and impact.

Technical Report: For system administrators. Includes detailed steps, proof-of-concept code, screenshots, and specific remediation advice.

# 7 phases of Penetration Testing Execution Standard (PTES)

**Phase 7: Reporting**

**Goal**: To deliver a clear, actionable report that details the findings, the risks, and the steps for remediation. This is the most important phase.

**Key Activities:**

Creating a report with two main components:

Executive Summary: For management. Non-technical, focusing on business risk and impact.

Technical Report: For system administrators. Includes detailed steps, proof-of-concept code, screenshots, and specific remediation advice.

# CONCLUSION

Penetration testing is indeed necessary, especially before launching a new Internet platform, as it is the last means of ensuring its level of security against external threats.
Complementing traditional audits, they notably allow us to check that nothing has been overlooked.

# Course Questions 5

Q1: Why conduct a penetration test?
Q2: What is the difference between a vulnerability audit and a penetration test?
Q3: Name the three levels of penetration testing.
Q4: What are the different stages of conducting a penetration test?
Q5: List the tasks to be carried out in each stage.
Q6: What is the difference between a network attack and a penetration test?