Week 02 – Penetration Testing Process Playbook

Prepared by: VIMAL A

Week: Week 02

Date: 30/01/2026

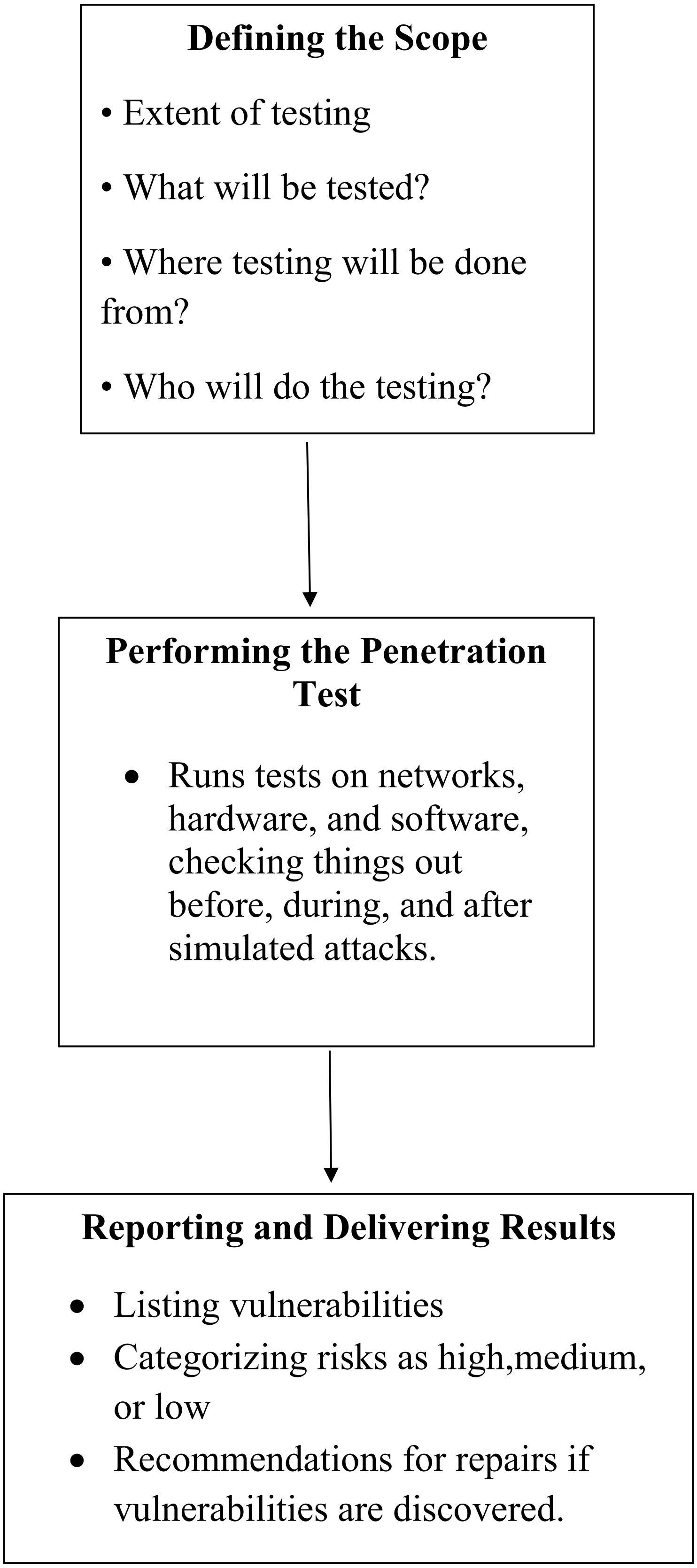
1. Penetration Testing Process

The penetration testing process defines the complete end-to-end workflow of a professional penetration testing engagement. It ensures that testing is performed in a structured, authorized, repeatable, and auditable manner.

The penetration testing process includes the following steps:

1. Understanding the engagement request and business objectives
2. Defining scope, assumptions, constraints, and out-of-scope areas
3. Obtaining formal authorization and approvals
4. Preparing the penetration testing methodology and plan
5. Performing information gathering and reconnaissance
6. Identifying potential threats and attack surfaces
7. Analyzing vulnerabilities in the target environment
8. Validating exploitability in a controlled manner
9. Collecting and preserving evidence
10. Analyzing risk and business impact
11. Mapping findings to standard frameworks
12. Reporting results and closing the engagement

Penetration Testing Process



Defining the Scope

- Extent of testing
- What will be tested?
- Where testing will be done from?
- Who will do the testing?

Performing the Penetration Test

- Runs tests on networks, hardware, and software, checking things out before, during, and after simulated attacks.

Reporting and Delivering Results

- Listing vulnerabilities
- Categorizing risks as high,medium, or low
- Recommendations for repairs if vulnerabilities are discovered.

Penetration Testing Phases

The engagement is divided into the following phases:

1. Pre-Attack phase
2. Attack phase
3. Post-Attack phase

Each high-level phase is further broken down into detailed operational phases to ensure clarity, repeatability, and proper evidence handling

Main Phase	Detailed Operational Phases
Pre-Attack	Preparation, Reconnaissance, Threat Modeling
Attack	Vulnerability Analysis, Exploitation
Post-Attack	Post-Exploitation, Reporting and Closure

1. Preparation

2. Reconnaissance

3. Threat Modeling

4. Vulnerability Analysis

5. Exploitation (Validation Only)

6. Post-Exploitation (Impact Validation)

7. Reporting and Closure

Phase 1: Preparation

Item	Description
Goal	Ensure testing is authorized, planned, and legally compliant
Inputs Required	Scope document, authorization letter, assumptions, constraints
Activities Performed	Define rules of engagement, finalize methodology, plan evidence handling

Item	Description
Evidence to Collect	Signed authorization, approved scope document
Output Artifacts	Penetration testing plan, engagement rules
Common Failure Modes / Risks	Testing without authorization, unclear scope

Phase 2: Reconnaissance

Item	Description
Goal	Understand the target environment and exposed attack surface
Inputs Required	Target details, scope boundaries
Activities Performed	Information gathering, asset identification
Evidence to Collect	Recon notes, identified assets list
Output Artifacts	Reconnaissance summary
Common Failure Modes / Risks	Gathering out-of-scope information

Phase 3: Threat Modeling

Item	Description
Goal	Identify potential attacker paths and high-risk areas
Inputs Required	Reconnaissance results
Activities Performed	Analyze attacker objectives and entry points
Evidence to Collect	Threat scenarios, attack flow notes
Output Artifacts	Threat model documentation
Common Failure Modes / Risks	Ignoring business context

Phase 4: Vulnerability Analysis

Item	Description
Goal	Identify weaknesses that could be exploited
Inputs Required	Threat model, asset list
Activities Performed	Vulnerability identification and validation
Evidence to Collect	Vulnerability descriptions, screenshots
Output Artifacts	Vulnerability list
Common Failure Modes / Risks	False positives, missing critical issues

Phase 5: Exploitation

Item	Description
Goal	Validate exploitability without causing damage
Inputs Required	Confirmed vulnerabilities
Activities Performed	Controlled exploit validation
Evidence to Collect	Proof-of-access screenshots, logs
Output Artifacts	Exploitation evidence
Common Failure Modes / Risks	Excessive exploitation, instability

Phase 6: Post-Exploitation

Item	Description
Goal	Assess business impact of successful exploitation
Inputs Required	Exploitation results
Activities Performed	Privilege validation, access confirmation
Evidence to Collect	Access proof, impact notes
Output Artifacts	Impact assessment
Common Failure Modes / Risks	Overstepping scope

Phase 7: Reporting and Closure

Item	Description
Goal	Communicate findings clearly and professionally
Inputs Required	Evidence from all phases
Activities Performed	Risk analysis, report writing
Evidence to Collect	Final report, evidence references
Output Artifacts	Penetration testing report
Common Failure Modes / Risks	Poor documentation, unclear findings

Need for Methodology / Framework

A penetration testing methodology ensures:

- **Legal** – so that testing is authorized and does not violate laws
- **Repeatable** – so that another tester can follow the same steps and get similar results
- **Auditable** – so that all actions can be reviewed and verified
- **Defensible** – so that findings can be proven if questioned

Without a methodology, testing becomes **tool-centric**, inconsistent, and difficult to defend.

How Methodology Reduces Risk and Increases Repeatability

A penetration testing methodology reduces risk by providing a clear and controlled structure for how testing is performed. It ensures that only approved systems are tested, unsafe actions are avoided, and evidence is consistently captured. In CPENT, structured phases and strict evidence handling make every action explainable, verifiable, and defensible, protecting both the organization and the tester from technical, legal, and reporting risks.

A methodology also improves repeatability by ensuring that no critical steps are missed, evidence is always collected, and testing results remain consistent across different engagements.

EC-Council’s LPT Methodology Mapping

LPT Component	Where It Fits
Preparation	Phase Engagement Preparation
Modus Operandi	Phases Intelligence Gathering Exploitation
Evidence Handling	All phases
Reporting	Phase Post-Exploitation

Preparation ensures legal and ethical readiness.
Modus Operandi defines how testing actions are carried out consistently.

Qualities of a Licensed Penetration Tester

Quality		Process Relevance
Ethical responsibility	—	Preparation
Technical depth	—	Exploitation

Attention to detail	—	Evidence handling
Risk awareness	—	All execution phases
Communication skills	—	Reporting
Discipline	—	Methodology adherence
Accountability	—	Evidence & audit
Professional judgment	—	Impact assessment