Information Gathering.

In This Article We Will Learn About :

1 • What does the information gathering phase mean ?

2 • What are the different types of information gathering stages ?

3 • Why is it so important in the penetration testing phase ?

What is information gathering ? :

Information gathering is one of the most important phases in penetration testing.
It involves collecting data about a company, website, or system. This phase is critical because the more extensive the information collected about a target, the greater the likelihood of successfully compromising that system .

There are two main types of information gathering: Passive and Active .

1 • Passive Information Gathering :

In this phase, the goal is to collect as much information as possible without directly interacting with the target. This minimizes the chance of detection and helps build an intelligence profile using publicly available data sources.

2 • Active Information Gathering:

This involves direct interaction with the target to obtain detailed and specific information about its systems, services, and potential vulnerabilities. While it provides more accurate data, it also increases the risk of detection.

Objectives of Information Gathering ? :

Understand the target's scope: Identify which systems, services, and assets belong to the target.

Reveal potential information-level weaknesses: Find weaknesses in exposed data or configurations (not executing attacks).

Prepare a prioritized testing plan: Create a ranked list of targets and areas to focus on during subsequent tests.

Reduce surprises during testing: Anticipate obstacles and unknowns so active testing proceeds more smoothly.

Phases :

Mental steps for information gathering (general) :

---

1 • ***Define the target scope — Clearly determine what is in-scope and out-of-scope for testing.***

2 • ***Collect basic data — Gather high-level information about the organization: company details, domains, and IP ranges (at a high level).***

3 • ***Analyze public sources — Review the company website, public profiles, social media, job postings, press releases, and other open sources.***

4 • ***Build a mental map (recon map) — Correlate collected data: who works there, public-facing services, third-party vendors and integrations.***

5 • ***Assess risk and prioritize — Decide which findings deserve follow-up during active testing and rank them by likely impact and exploitability.***

6 • ***Document and produce a preliminary report — Record everything gathered with notes on source reliability and confidence levels.***

With best regards (Rashid Al-Tayyar - Ox 3fret .)