Penetration Testing

What is Web Penetration Testing ?

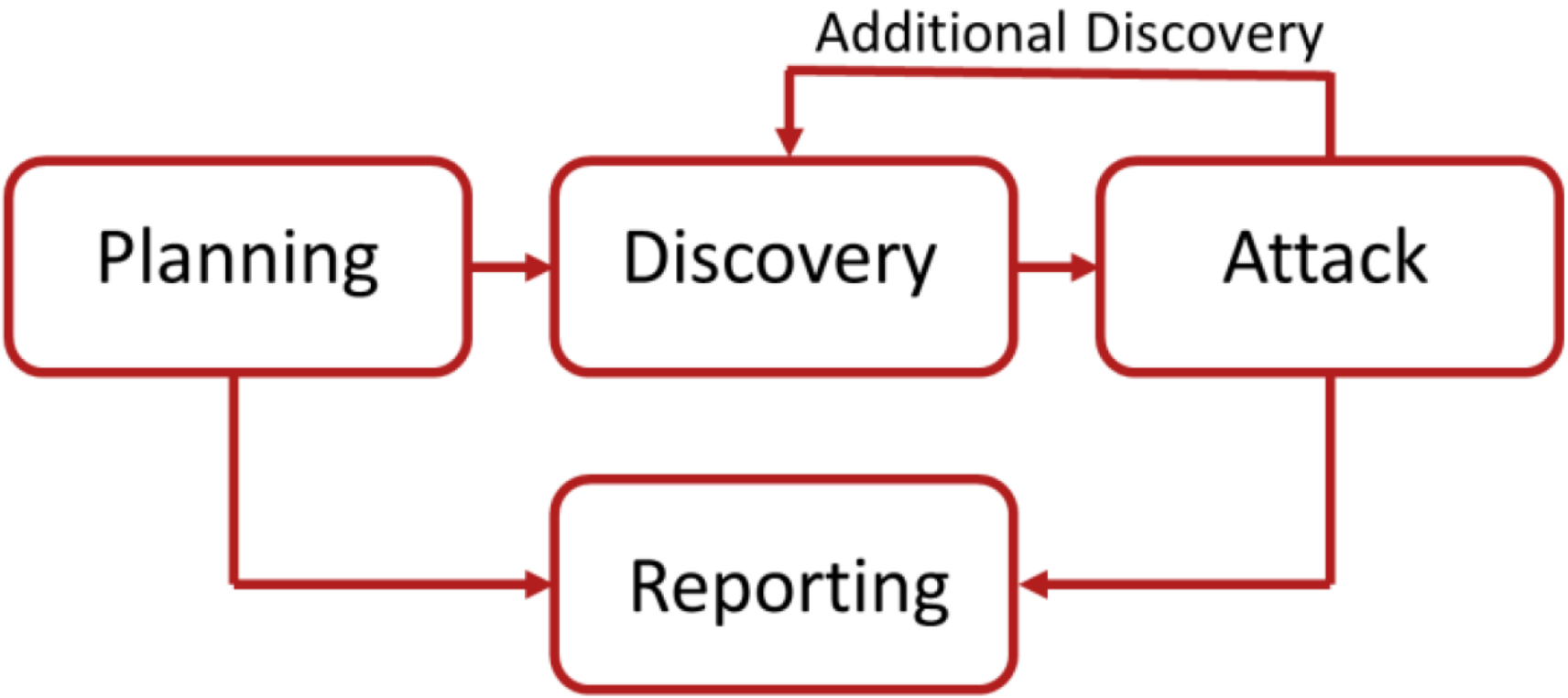
- Set of tests that simulates the same way a hacker would attack the system.

Goal:

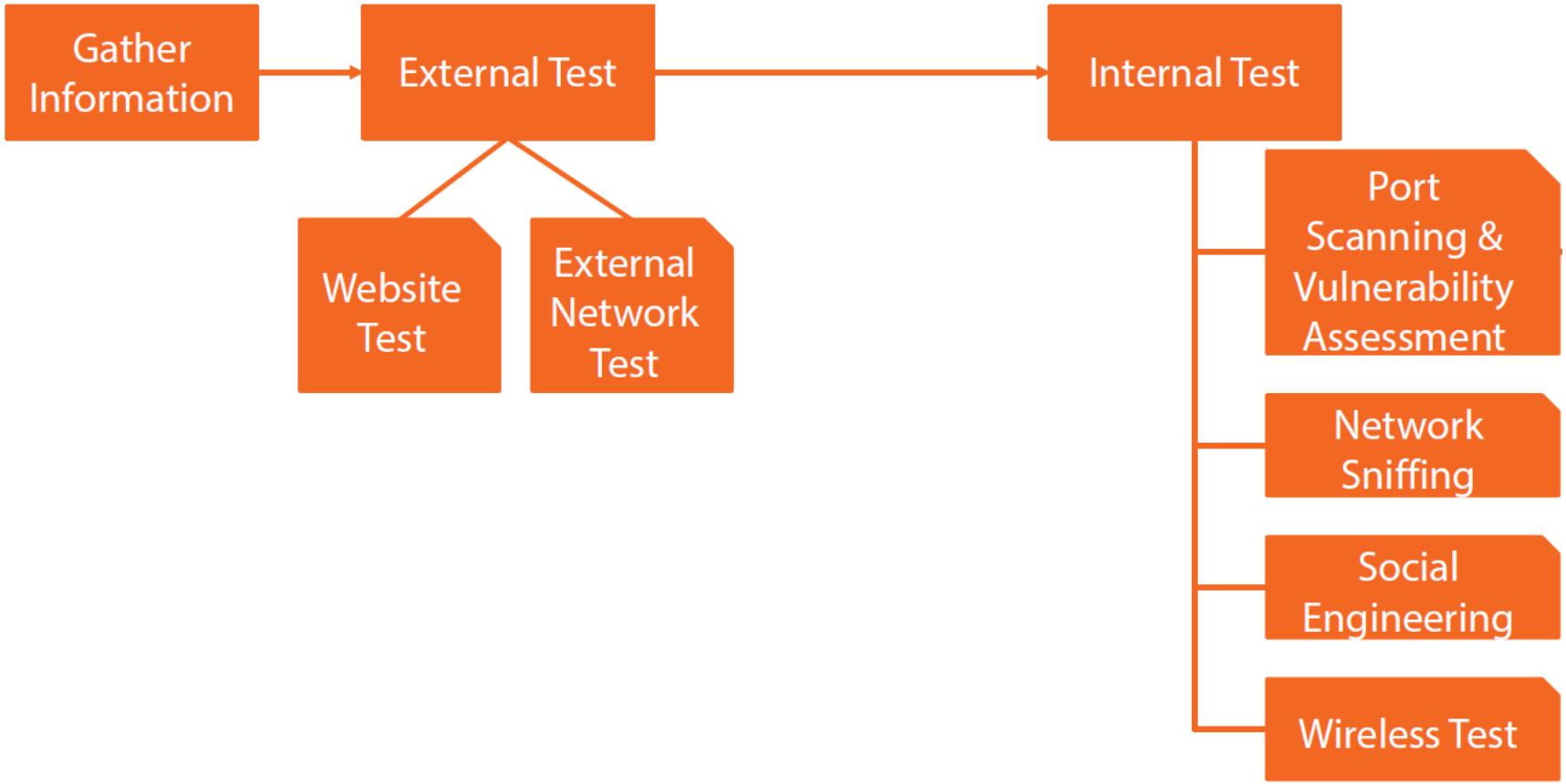
- Discover the security vulnerabilities of a system before an attacker can benefit from them
- Validate the effectiveness of its security controls

CompTIA Pen Testing methodology

NIST SP 800-115 Pen Testing Phases



Pen Testing – Vulnerability Identification



1. Planning & Scoping

- Define the goals of the test
- Scope of the test (servers, networks, apps to be tested)
- Schedule and Budget ($)

2. Info Gathering and Vulnerability Identification

Get detailed information about the target system:

- IP address and IP block
- System platforms (Windows or Linux)
- Open ports and services
- Info from https://centralops.net/co/ and https://www.dnsstuff.com
- Nmap to scan the network
- Vulnerabilities databases https://nvd.nist.gov/ & https://www.cvedetails.com/

3. Attacks and Exploits

- Performs an active attack on the system to exploit the identified vulnerabilities
  - E.g., SQL injection and Cross-site- scripting.

4. Reporting

- Evaluate and analyze the collected data collected

  - Determine vulnerabilities with associated risks

  - Risks can be classified by type (high ,medium, low), main cause and consequences.

- Suggest remediations