Pentesting Lifecycle

1. Defining the Scope
IP ranges, hosts, and applications should be test

2. Information Gathering
Collect data about the target

3. Vulnerability Detection

4. Initial Foothold

5. Privilege Escalation

6. Lateral Movement

7. Reporting/Analysis

8. Lessons Learned/Remediation

Information Gathering

Passive Information Gathering
Also knows as Open-source Intelligence (OSINT)
non or almost non direct interaction with that target

Whois Enumeration

Active Information Gathering

By **LILIANEZ**
cheatography.com/lilianez/

Not published yet.
Last updated 10th September, 2023.
Page 1 of 1.