# The Stages of the Penetration Test

1. **Pre-engagement**

   In the first pheas we've to write the agreement and doing the contract about everything for example understanding the customer goals from the pen test and what they worried about.

| | |
|---|---|
| **Scope** | determent what the Ip's and the domines, systems that involve in the testing. |
| **The testing window** | what a time that the client wants the testing is running. |
| **Contact information** | who has to contact to him if the tester find something serious. |
| **"get out of jail free" card** | Make sure you have authorization to perform a penetration test on the target, for example If a target is not owned by the company and it owned by third party. |
| **Payment terms** | when and how much they pay for you. |

2. **information-gathering**

   In this pheas you will analyze freely available sources of information, this process known as (OSINT) Open Source Intelligence.

3. **threat-modeling**

   In this pheas you will identifying any potential threat and vulnerability that may happened,
   this some of the activities that involve this pheas :

   i. Understanding the environment.
   ii. identifying the potential threat that may apply.
   iii. Understanding the countermeasures to those threats.

4. **vulnerability analysis**

   is identifying and addressing security weakness in computer systems, networks, etc..
   This is some of the activities that involve in this pheas :
   i. Scanning.
   ii. Assessment and analyzing.
   iii. Prioritization the vulnerabilities.

5. **Exploitation**

   now we run exploits against the vulnerabilities we've discovered in the previous pheas.

6. **post-exploitation**

   here we gather information about the attacked system, look for interesting files, sensitive data, password, hashes for others systems and now we decide if the attack is impact and do real damage to the client or not.

7. **Reporting**

   The final pheas is to reporting everything and every step you have taken and what the methodology you've taken to do the pen test, what the impact of the pen test you have done.