# Pre-Engagement Interactions or Scoping

In this phase, the pen testing team will discuss in detail the scope of the assessment, objectives, legal implications, goals and organizational assets available in pre-engagement interactions or scoping phases. Penetration testers should collaborate with the organization to understand any threats, organizational culture, and best suited pen-testing technique for the organization, as well as all legal issues. In this process, organizational assets will has to categorize based on assets in scope (assets on which pen testing has to perform) and assets out of scope (not included in pen testing) based on gathered information on all organizational assets

# Reconnaissance

Reconnaissance or Open Source Intelligence gathering is one of the important step in penetration testing. A pen tester aims to gather as much as information and the potential targets for exploit required about client organization. Depending on the type of penetration test chosen, the penetration tester will have different degrees of organizational information collected during the first phase and may also find extra critical information on their own to locate hidden vulnerabilities and entry points in the system.

In generally pen testers will use the vast range Reconnaissance techniques which include searching in different search engines, Domain name searches or WHOIS lookups, social engineering, searching for tax records, internal Foot printing for email address, usernames and social networks accounts,tailgating,external Foot printing for port scanning ,reverse DNS,packet sniffing etc.

# THREAT MODELING & VULNERABILITY IDENTIFICATION

The Reconnaissance will act as information gathering phase in the In the threat modeling and Vulnerability Identification and this phase will also be pre-attack phase .In this phase pen testers will think like attackers and will scan the system as deep as they can and pen testers identifies different targets and also maps organizational attack vector based on threats, here targets will be business assets like employees data, customer data ,technical data and threats will be internal threats like management,employess,vendors,distributors etc and external threats like Ports, Network Protocols, Web Applications, Network Traffic, customers etc.

The internal threats will be somewhat in the control of organization and external threats will be out of control. In this phase the pen testers will use different automated tools and manual testing tools to scan all the organization in scope assets. After completion of this phase the information gained is different vulnerabilities in the servers, web application and all the in scope assets.

# EXPLOITATION

The pen tester team will try different exploits contained in network, applications, and data with a list of all potential vulnerabilities and entry points gathered in Threat Modeling & Vulnerability Identification. The main aim of the pen tester is to verify how far they can get into your system and find high-value targets without being avoid detected.

The pen tester will exploit the system based on scope defined in the first phase .the pen testers will use the standard exploits like Web Application Attacks, Network Attacks, Memory-based attacks, Wi-Fi attacks, Physical Attacks, Social engineering. In this phase the system has to exploit after developing the threat vector and attack plan based on vulnerabilities to gain access to system and sometimes the system can have the secure network which contains DMZ, firewall, honey pots, and honey well so that the pen tester should use different evacuation techniques to bypass these security devices.

# POST-EXPLOITATION

Upon completion of the exploitation process, the next aim is to record the methods used to gain access to valuable information of the organization. The pen tester should take all the evidences required to generate the report and after collecting the evidence the team should cleanup the system to revert the activities done during the exploitation phase. The clean up activities will include Removing any executables, scripts, and temporary files, Reconfiguring settings back to the original state prior to the test, Removing any user accounts created, removing any types of malware codes injected etc. The clean-up process should ensure that all installed backdoors or root kits should be removed, and it should return the system configuration to its original, pre-engagement state. Any credentials changed has to restore, and any additional usernames created should be removed.

# Reporting

This report is the best method to convey the findings of a pen test. This report will address managers and the technical team. From the manager's perspective, they will have information like different vulnerabilities available in the system and their Business impact on the system. In the technical Team, they will have information like different vulnerabilities exist in the system with its remediation.

The pen test report will begin with an executive summary outlining organizational business-related penetration test plan, defining outcomes by risk ranking. This section should be concise, and it could be the client's most important piece of decision-making and the business team can determine what to correct and what problems pose an appropriate level of risk. The remaining part is technical detail, which will be descriptive, specific and generic or ambiguous statements will helps technical team to resolve security issues .

# Resolution & Re-Testing

In this phase, the technical team tries to resolve the issues and technical team will get some assistant from team to solve the issues and Once vulnerabilities have been remediated, the client has to retest their systems to ensure that fixes were successful and has to test whether new vulnerability was created as a result of remediation or not. And the pen test should also be conducted whenever there will be any modification in the system for finding new vulnerabilities.