PoC of CyberSec Solutions

Quick-Win

Abstract

Context

To provide security solutions, building of own platform is very important which will include the vulnerability assessment and tools for penetration testing. However, it is a time taking process and considering current scenario, Sybrid must come up with the solution to provide vulnerability assessment and in the next phase conduction penetration testing. In doing so, it is required to develop a framework fulfilling all the requirements of vulnerability assessment and providing a detailed analysis report pointing out all the vulnerabilities.

Problem

The problem to cater is how much eligible we are to provide vulnerability or penetration testing solutions in the local or international market.

Method

The method currently being followed will be entirely based on the client's requirement for testing network. The tools will also be finalized as per the client's requirement however there are general tools selected which will be primarily used.

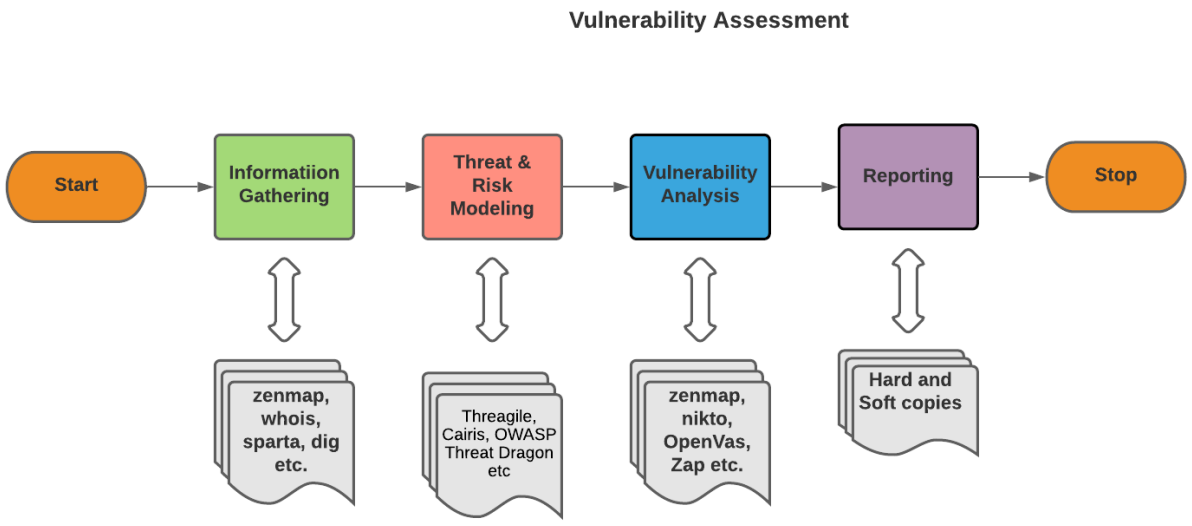
Results

The results of the assessment and pen-testing will be shown in the form of post report. The report will include the executive summary of the entire plan, vulnerabilities gathered along with their severity level and at the end giving solutions/recommendations to mitigate any issue which is required on urgent basis.

Design & Implementation

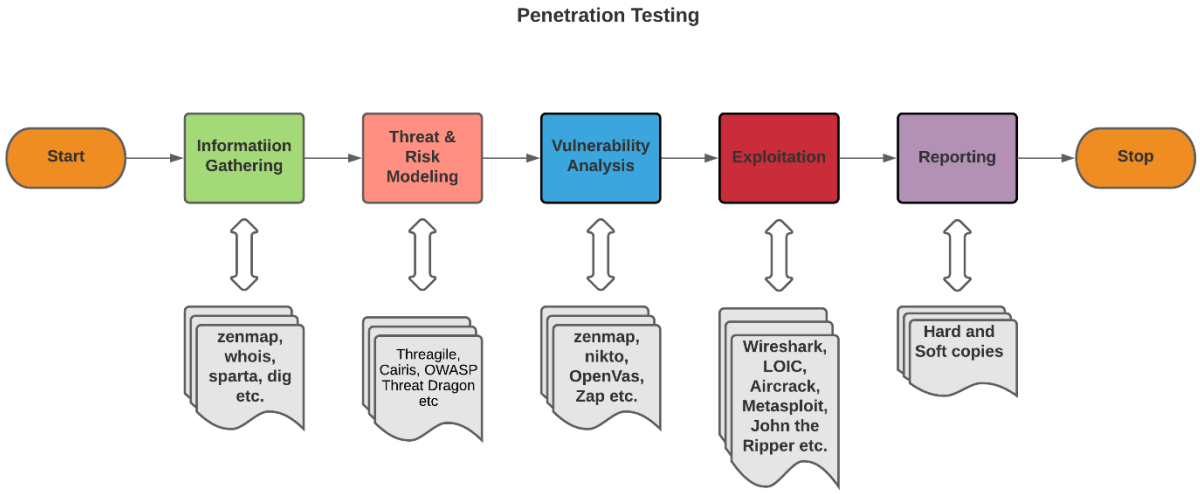
The design and implementation phase will show the flow of assessment and pen-testing with the help of following figures.

Vulnerability Assessment



The figure shows the flow of vulnerability assessment. Following the above flow, we will define the vulnerabilities, classification will be done, based on their severity will be prioritized and afterwards providing suitable recommendations.

Penetration Testing



The above is the flow of conduction a penetration test on the network. The Exploitation phase is added which make this process different than the

vulnerability assessment. The founded vulnerabilities will be exploited but as per the rules of engagement agreement.

Tools

The tools are gathered and installed on the kali linux platform. The tool selection however will remain dynamic because of the requirements of the client. The major selection criteria of tools are open source which can be later integrated for building a platform but for now in a sequential way they will be used to gather the information and later performing vulnerability assessment and the penetration testing. The tools are also classified in terms of web based and network infrastructure based.

Threat Methodology

The threat methodology is the process of identifying the assets and threat agents. The process will check for the flow of network and using data flow diagrams representing it. The threat modelling is part of every organization and therefore it is required by them to provide to penetration testers however if they want Sybrid to develop a threat modelling plan we will use STRIDE (Threat Model) which includes security controls like Spoofing, Tampering of data, Repudiation, Information Disclosure, DoS, and Elevation of privileges. These security controls cover mainly the issues of vulnerability assessments and penetration testing and it is the reason of selecting STRIDE on other threat methodologies. As following STRIDE, controls like: Authentication, Integrity, Non-repudiation, Confidentiality, Availability, and the Authorization will be checked to ensure the basic CIA triad. Moreover, the security controls by the compliances will also be considered during the formation of the threat model.

Laboratory

The lab is formed which will implement the entire process of vulnerability assessments and the penetration testing having tools installed and automated reports are also generation with respect to Sybrid. The lab is formed on the laptop but in short time it will be formed on the server and can be accessed remotely to perform all the above parameters. Moreover, we will also be able to run the in-house testing and can come with better solution in the future.

Standard Operating Procedure

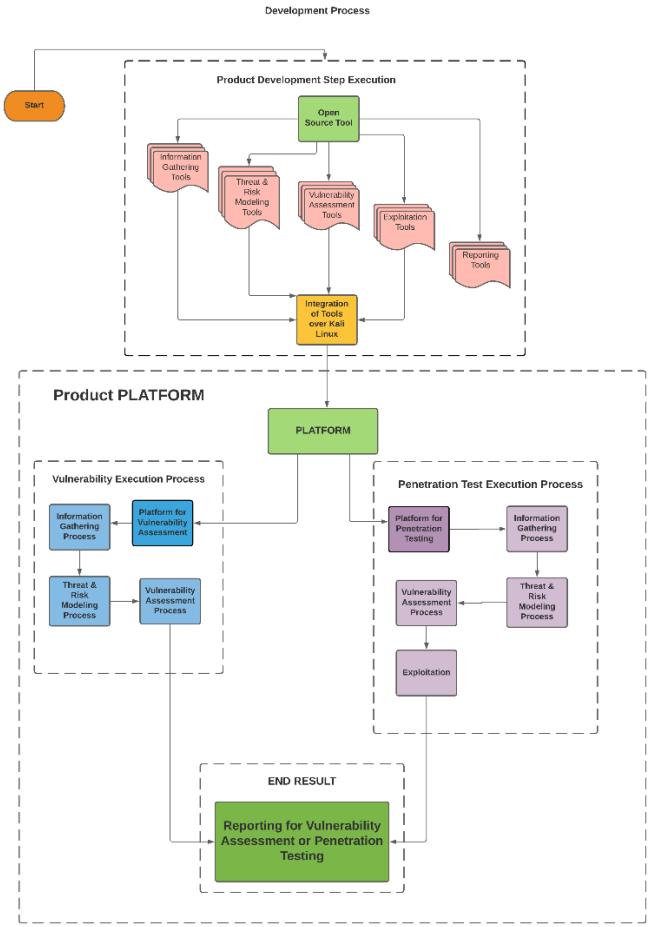
The sample standard operating procedures are also formed to show what the actual SOP will look like. The sample SOP's has all the steps from information gathering to post-report. The SOP will also be dynamic and changes as per the testing requirements or rules of engagement document.

Delivery

The deliverable product for the client will be the report based on vulnerabilities and detailed analysis of those vulnerabilities. The report will also include the recommendations or solutions. The report pattern will be based on the automated/manual discovered vulnerabilities and formatting will be based on the Sybrid approved template.

Conclusion

As far as quick-win situation, we can provide vulnerability assessment and penetration testing services. The platform building as mentioned earlier is a time taking process which is entirely based on this flow of execution as mentioned in the vulnerability assessment and penetration testing part. The below figure will show the platform building process using flowchart:



The above is the ultimate solution Sybrid is looking to develop in the future. The above figure is a platform but right now we can perform the left (Vulnerability

execution process) and right wing (Penetration testing execution process). At the end report will be generated on basis of findings.