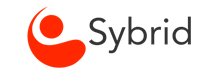


SYBRID SECURITY SERVICES

Product Datasheet

SYBRID PRIVATE LIMITED



Copyright © 2019 by SYBRID Technology Division

All rights reserved. This document or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a document review.

The SYSEC® logo is property of SYBRID where other logos used in document are the property of their respective owners

Table of Contents

[1. Introduction 4](#_Toc62795502)

[2. Objective 4](#_Toc62795503)

[3. Concept 4](#_Toc62795504)

[3.1. Guidelines 4](#_Toc62795505)

[3.1.1. Mechanism 4](#_Toc62795506)

[3.2. Method 6](#_Toc62795507)

[3.3. Compliance 6](#_Toc62795508)

[3.3.1. ISO 27001 for OWASP 6](#_Toc62795509)

[3.3.2. PCI for OWASP 6](#_Toc62795510)

[3.3.3. ISO 27001 for PTES 6](#_Toc62795511)

[3.4. Platform 7](#_Toc62795512)

[3.5. Tools 7](#_Toc62795513)

[3.6. Development 7](#_Toc62795514)

[3.6.1. Tools combination & sequence 7](#_Toc62795515)

[3.6.2. Scripting for integration of tools over kali platform for VA & PT 7](#_Toc62795516)

[3.6.3. Build for Vulnerability Test. 7](#_Toc62795517)

[3.6.4. Build for Pen Test 7](#_Toc62795518)

[4. Scope of Vulnerability Assessment 8](#_Toc62795519)

[5. Process of Vulnerability Assessment 8](#_Toc62795520)

[5.1. Information Gathering 8](#_Toc62795521)

[5.2. Threat Modeling 8](#_Toc62795522)

[5.3. Vulnerability Analysis 8](#_Toc62795523)

[5.4. Reporting 8](#_Toc62795524)

# Introduction

The purpose of the report is to build up a solution to conduct vulnerability assessment and penetration test on the organization level. The main target will be an IP by which we can search for the machines which are providing services and through scanning, finding the vulnerabilities and afterwards if required, exploiting those vulnerabilities. The vulnerabilities found during test out of them some of them are selected by an organization to get them checked and fixed. Moreover, compliances are included on behalf of which different methodologies are mapped to fulfill the required security features for an organization. The tools serving the purpose of testing are selected in accordance with the compliance which are also open-source and later, during the development stage those will be integrated, and the platform will provide services as per the requirement of the client.

# Objective

* To build a platform for vulnerability assessment and penetration testing.
* Methodologies selected and mapped in accordance with compliance requirements.
* Use of open-source tools to serve the purpose.
* Integrating tools and serving the required purpose as a platform.

# Concept

## Guidelines

To build a platform, the process is break down in two parts: first for the vulnerability assessment and second for penetration testing. The vulnerability assessment will perform only the analysis of the application or network and penetration test if needed will exploit those vulnerabilities further. The selection of methods is mentioned in 3.2. However, this one platform will provide services based on open-source tools which by integration will be the part in building this platform.

### Mechanism

#### Pre-Engagement

Pre-engagement is a step before conducting any of the test mentioned above, a meeting should be called to get the idea of the project and working out the scope of the test and the objective. The results of the test should be discussed as sometimes the outcome contains no clear results because purpose might be demonstration of the vulnerabilities which are exploitable and exists within the organization’s network. The form in which the results of the outcomes are showed should also be discussed with the organization.

#### Goal

Every penetration test should be goal-oriented which is to test and identify the specific vulnerabilities which could result in compromising the business or mission objectives of the client. It is not only to find un-patched systems but to identify the risks that could adversely impact the organization.

#### Metrics for Time Estimation

The time estimation depends on the expertise of the tester and whatever the time frame decided it better to add a padding of 20% to total time which acts as a backup as in scenarios continuous failure to scanning the target may lead to overtime. Also, it is possible that the network segment may go down or the founded vulnerability may result into involving many levels of management to address. Both of such events are time consuming and significantly could impact the original time which is why 20% added.

#### IP Ranges and Domains

Before starting a penetration test, all the targets must be identified. The target must be obtained from the client in the initial phase. Targets can be in the form of IP addresses, network ranges, or domain names by the customer. Moreover, it is also important to define that if there is any firewalls, IDS/IPS or networking equipment between the tester and the final target and as they are or not part of the scope. As, in some instances target only provides with the details of the name of the organization and expects the tester to identify the rest on their own. Also, check the IP’s provided to make sure whether they are valid and owned by the client itself or not because these could lead to severe legal consequences.

#### Dealing with the Third Parties

It is also observed that sometimes the client does not tell or forget to talk about the third involved so which means testing a service or application being hosted by the third party. In recent years, cloud services are widely implemented everywhere, and it is need of today to let those third party know or seek permission from them for testing. Failing to take permissions will possibly bring us in front of law.

#### Cloud Services

Testing cloud services may incur an issue of that data from multiple organizations are stored on one physical medium. The cloud services providers need to be alerted to the testing and needs acknowledge that the test is taking place and granting permission to testing organization to test. Moreover, security contract should be there that can be helpful in the event of finding security vulnerability which could impact the other cloud customers. Also, the cloud providers have specific procedures for penetration testers to follow, and may require request forms, scheduling or explicit permission from them before testing can begin.

#### ISP

The ISP terms and conditions should be considered before launching any attack because in many commercial situations the ISP will have specific conditions for testing. In certain situations, the ISP may block the traffic which is considered malicious. The client may approve the risk, but it must be always communicated before the beginning. Web hosting with the third parties, the scope and timing of the test needs to be clearly communicated with web hosting provider.

#### Incident Reporting Process

It is important to discuss the organizations incident response capabilities before the start of the engagement process. The penetration test is not just about testing the environment but to check the capabilities of the incident response team. If an entire engagement process can be completed without the target’s internal security teams ever noticing, then it means there is a big major gap in the security posture. Also inform some from the incident team about the test so the incident team does not start to call every member.

#### Rules of Engagement

As the scope defines what will be tested, the rules of engagement define how that testing is to occur.

#### Information Gathering

Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when performing vulnerability assessment or performing exploitation. The more information gathers during this phase, the more vectors of attack be able to use in the future.

#### Threat Modelling

This section defines a threat modeling approach as required for a correct execution of a vulnerability assessment or penetration testing. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results. The standard focuses on two key elements of traditional threat modeling - *assets and attacker* (threat community/agent).

#### Vulnerability Assessment

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design.

#### Exploitation

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions.

#### Reporting

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high-level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

## Method

The selection of method is based on the methodologies. For testing of web-based applications OWASP is selected as it is very known methodology for testing of web-based applications. To test the network infrastructure the PTES methodology is selected. Both methodologies have complete set of online documentation which also includes tools. The OWASP has 10 controls which deals with the web-based applications and guides proper testing in both phases whether only the vulnerability or also the penetration testing. PTES is a procedure of conduction penetration which can be adopted easily, and which is why it is very widely used for vulnerability and penetration testing.

## Compliance

As there are many compliances available online and up till now two of them i.e., ISO 27001 and PCI were used to observe controls provided by methods. The OWASP is mainly focused and tested under both compliances where PTES only with ISO 27001. The comparison to what the methods could relate with compliances are given below:

### ISO 27001 for OWASP

### PCI for OWASP

### ISO 27001 for PTES

## Platform

The platform is Debian based 64-bit operating system KALI Linux. It is well known platform among penetration testers and to conduct vulnerability assessments. It comes with pre-loaded tools and can be used for different infrastructures.

## Tools

The selection criteria for tools are that they are open-sourced and moreover fulfilling over requirement of integration although which will be checked during the development phase. The tools selected are not final and more tools could be added further as per the requirements. The tools which are selected is come with fulfilling the criteria of the compliances.

(TOOLS-PLATFORM-WORKING)

## Development

### Tools combination & sequence

The combination of tools is based on the procedure of gathering intelligence afterwards according to requirements performing vulnerability assessments and for that different combination of tools will be used and if penetration test will be required then for exploits different set of tools will be selected for testing. The controls of OWASP for web applications and PTES for network infrastructure are used and in even in future will be used to make different combinations of tools. Multiple tools like snort, OpenVas etc. will be built on kali Linux platform and will serve the purpose as per requirement as if someone needed them for vulnerability assessment and similarly if someone asks for exploits then to gather information regarding vulnerabilities such tools will be used again. Also, this platform is not limited to only these tools as this is initial stage of research and further as per requirements more tools will be come under it. Afterwards, reporting tools are also which can build a solid report however different features will be selected as per the requirements.

### Scripting for integration of tools over kali platform for VA & PT

The next phase after combination and sequence is their scripts. As selection is based on open source, so the scripts could be modified or specific part of them will be extracted and those features will be used to build up the strong platform. The scripts used for building vulnerability assessment will be different, but they will also be used in the penetration testing.

### Build for Vulnerability Test.

As mentioned, the vulnerability assessments will include the combination of intelligence gathering, enumeration, vulnerability scanner and post reporting tools. The build for them is based on the requirements set and more tools could be added to add more features in the platform.

### Build for Pen Test

As mentioned, the penetration test will include the combination of intelligence gathering, enumeration, vulnerability scanners, exploiting tools and some external resources like dictionaries globally used to do brute force etc., and post reporting tools. The build for them is also based on the requirements set and more tools could be added to add more features in the platform.

# Scope of Vulnerability Assessment

The scope of the test will be decided before performing any scan for assessment. Defining the scope is very important that what specifically is going to be tested and under what conditions. The scope is to identify the machines, systems and network, optional requirements and sometimes the staff involved. The other thing is to understand the mindset of the client that what services the client wants to get tested and to what extent the scans will be performed as there are conditions when no results are obtained or sometimes those vulnerabilities are obtained which are not exploitable but still needs to get fixed. The range of IP addresses should be discussed to know which of them are in the engagement process. It must be verified that the client owns all the components as involving the target environments: DNS server, email server, actual hardware their web servers run on and their firewall/IDS/IPS solution. At the end, the best approach is coming up with disclosure agreement and rules of engagement to fix the boundaries.

# Process of Vulnerability Assessment

Flowchart

## Information Gathering

Information gathering is the foundation of performing vulnerability assessment. The more useful information about the target the more chances of successes to find vulnerabilities. Some information is obtained simply by doing Google and some of it obtained through automated tools. The information could be of any type like business nature, physical location, business terms, business structure etc. moreover, if state is involved then this form of gathering information is level 3, including a lot of manual and heavy analysis also deep understanding is obtained during the whole process. The information will be gathered in form of end points of the client which can be physical, electronic or human. There are several things to observe as identification and naming of the target, consider the rules of engagement if any, make time metrics for the assessment and always keep the end goal of the test. After all the above process proceed to next phase.

## Threat and Risks Modeling

The model focusses on the two key element which are assets and attacker. Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities. While doing the modeling the business SWOT analysis will be considered and capabilities of the business which will target the technical side. So, basically it will be those activities performed for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities defining threat agents and assets. The questions during this phase which will be addressed are as:

* What are we working on?
* What can go wrong?
* What are we going to do about it?
* Did we do a good job

## Vulnerability Analysis

The process of discovering flaws in the system and applications which can lead towards halting or escalation privileges. The flaws can come from anywhere range from host and misconfiguration or issues in the application designs.

While performing vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. To reach the goals, things to consider are location of an assessment tool, authentication requirements, target networks, segments, hosts, application, inventories, etc.

The analysis is based on active or passive scanning involving automated tools as network scanners, service based, banner grabbing, web application scanners, directory listing, voice network scanners, monitoring traffic, etc. The vulnerabilities obtained are also marked as per there severity level grading on a scale 0 to 10 and report is presented in post-test report.

## Reporting

The post reporting is a report which can be customized depending upon the nature of the assessment or as per the requirement of the client. Although, the report should include all the aspects of the assessment from first to last stage. The general structure of the report which is followed is as:

* Executive summary
* Background
* Risk Ranking
* Findings
* Technical Details
  + Information gathering
  + Threat & Risk model
  + Vulnerability Analysis
* Conclusion/Solution

# Scope of Pentest Assessment

The scope of the test will be decided before performing any scan and exploit for penetration testing. Defining the scope is very important that what specifically is going to be tested and under what conditions also the exploits to what extent are demanded from the client end. The scope is to identify the machines, systems and network, optional requirements and sometimes the staff involved. The other thing is to understand the mindset of the client that what services the client wants to get tested and to what extent the scans will be performed and then which vulnerabilities the client want to check for exploits as there are conditions when no results are obtained or sometimes those vulnerabilities are obtained which are not exploitable but still needs to get fixed and also such vulnerabilities if not exploitable then hassle of conducting penetration test will be costly and time consuming which is why scope needs to get defined. The range of IP addresses should be discussed to know which of them are in the engagement process. Moreover, it is also to know which IP specifically the client wants to get exploited as there might be range of IP’s. It must be verified that the client owns all the components as involving the target environments: DNS server, email server, actual hardware their web servers run on and their firewall/IDS/IPS solution. At the end, the best approach is coming up with disclosure agreement and rules of engagement to fix the boundaries.

# Process of Penetration Test

Flowchart

## Information Gathering

Information gathering is the foundation of performing penetration test. The more useful information about the target the more chances of successes to find vulnerabilities and exploiting those vulnerabilities. Some information is obtained simply by doing Google and some of it obtained through automated tools. The information could be of any type like business nature, physical location, business terms, business structure etc. moreover, if state is involved then this form of gathering information is level 3, including a lot of manual and heavy analysis also deep understanding is obtained during the whole process. The information will be gathered in form of end points of the client which can be physical, electronic or human. There are several things to observe as identification and naming of the target, consider the rules of engagement if any, make time metrics for the assessment and always keep the end goal of the test. After all the above process proceed to next phase.

## Threat and Risks Modeling

The model focusses on the two key element which are assets and attacker. Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities. While doing the modeling the business SWOT analysis will be considered and capabilities of the business which will target the technical side. So, basically it will be those activities performed for improving security by identifying objectives and vulnerabilities, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system. Threat modeling is a planned activity for identifying and assessing application threats and vulnerabilities defining threat agents and assets. The questions during this phase which will be addressed are as:

* What are we working on?
* What can go wrong?
* What are we going to do about it?
* Did we do a good job

## Vulnerability Analysis

The process of discovering flaws in the system and applications which can lead towards halting or escalation privileges. The flaws can come from anywhere range from host and misconfiguration or issues in the application designs.

While performing vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. To reach the goals, things to consider are location of an assessment tool, authentication requirements, target networks, segments, hosts, application, inventories, etc.

The analysis is based on active or passive scanning involving automated tools as network scanners, service based, banner grabbing, web application scanners, directory listing, voice network scanners, monitoring traffic, etc. The vulnerabilities obtained are also marked as per there severity level grading on a scale 0 to 10 and report is presented in post-test report.

## Exploitation

This phase is based on the prior phase i.e. vulnerability analysis. At this phase it is tried to get establish access to a system or resource by bypassing security restrictions. The exploitation phase should be much planned for a precision strike. The focus is laid to identify the main entry point into the organization and to identify high value target assets. If the phase completes properly than a high valued target list is compiled and suggestions for the attack vectors are provided. The exploitation is detailed process and sometimes based on hit and trial approach however the vulnerability analysis is the base which should be good so to get maximum of the success.

## Post-Exploitation Report

The post reporting is a report which can be customized depending upon the nature of the assessment or as per the requirement of the client. Although, the report should include all the aspects of the assessment from first to last stage. The general structure of the report which is followed is as:

* Executive summary
* Background
* Risk Ranking
* Findings
* Technical Details
  + Information gathering
  + Threat & Risk model
  + Vulnerability Analysis
  + Exploits
* Conclusion/Solution