SEKURITI SIBER
INDONESIA

Proposal

Penetration Testing

Compiled for :

2018

Penetration Test is one of the efforts to improve and test the quality of applications, infrastructure and systems in supporting the business processes of companies using IT services. With the Penetration Test Application, it is expected that the client can know the weaknesses and vulnerabilities contained in the Application and infrastructure from the point of view of hackers and always comply to regulations or regulations governing the distribution and manufacturing system. The existence of security attacks by hackers can have an impact on the application and the availability of data that implicate the disruption of business operations other than it could have an impact on the image of the company if there is leakage of important data.

Based on these, PT Sekuriti Siber Indonesia through this proposal will provide solutions to answer the needs of clients through the initiative of the implementation of Penetration Test work.

1.1. PURPOSE

The purpose of implementing Penetration Test initiatives using consultant services is to conduct assessment of client networks appropriate to the scope of work. Here are the main objectives of this job:

1. Figure out vulnerabilities that attackers can exploit against client networks.
2. Perform Penetration Testing with Black Box method and Gray Box Testing.
3. Know the risks, and the impact on the business.

1.2. SCOPE OF WORK

To meet the above objectives, the scope of work to be performed on Penetration Test Applications is as follows:

1. Perform Penetration Test against public IP.
2. Perform Penetration Test and security analysis of the applications.
3. Testing application is done by Black Box and Gray Box testing method.
4. *Re-Testing & Remediation Support*
5. The methodology for Penetration Test refers to OWASP and PTES
6. Activities include Project Management and execution

7. Project documentation.

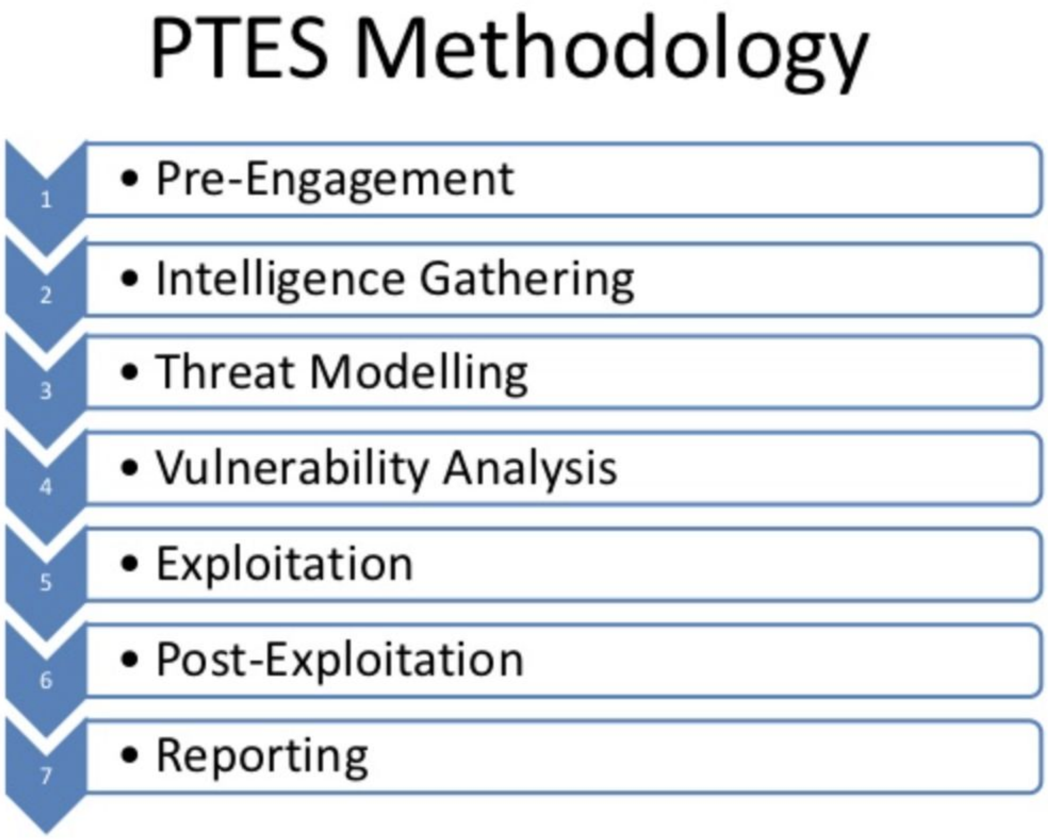
2. DESCRIPTION OF APPROACH AND METHODOLOGY

This section describes the description of the approach and methodology proposed by PT Sekuriti Siber Indonesia in conducting the Penetration Test.

The approach to formulate the methodology to be used in the Penetration Test will use the main reference PCI-DSS, ISO 27001 and PTES

2.1.1. PTES (Penetration Testing Execution Standard)

PTES (Penetration Testing Execution Standard) consists of 7 main parts. It covers everything related to penetration testing - from initial communication and reasoning behind the pentest, through intelligence gathering and threat modeling phases where testers work behind the scenes to gain a better understanding of the organization under test, through vulnerability research, exploitation and post-exploitations, in which technical security expertise of testers comes into play and is combined with an understanding of business engagement, and ultimately reporting, which captures the entire process, in a way that makes sense to the customer and gives the most value to it. Here's PTES's methodology:



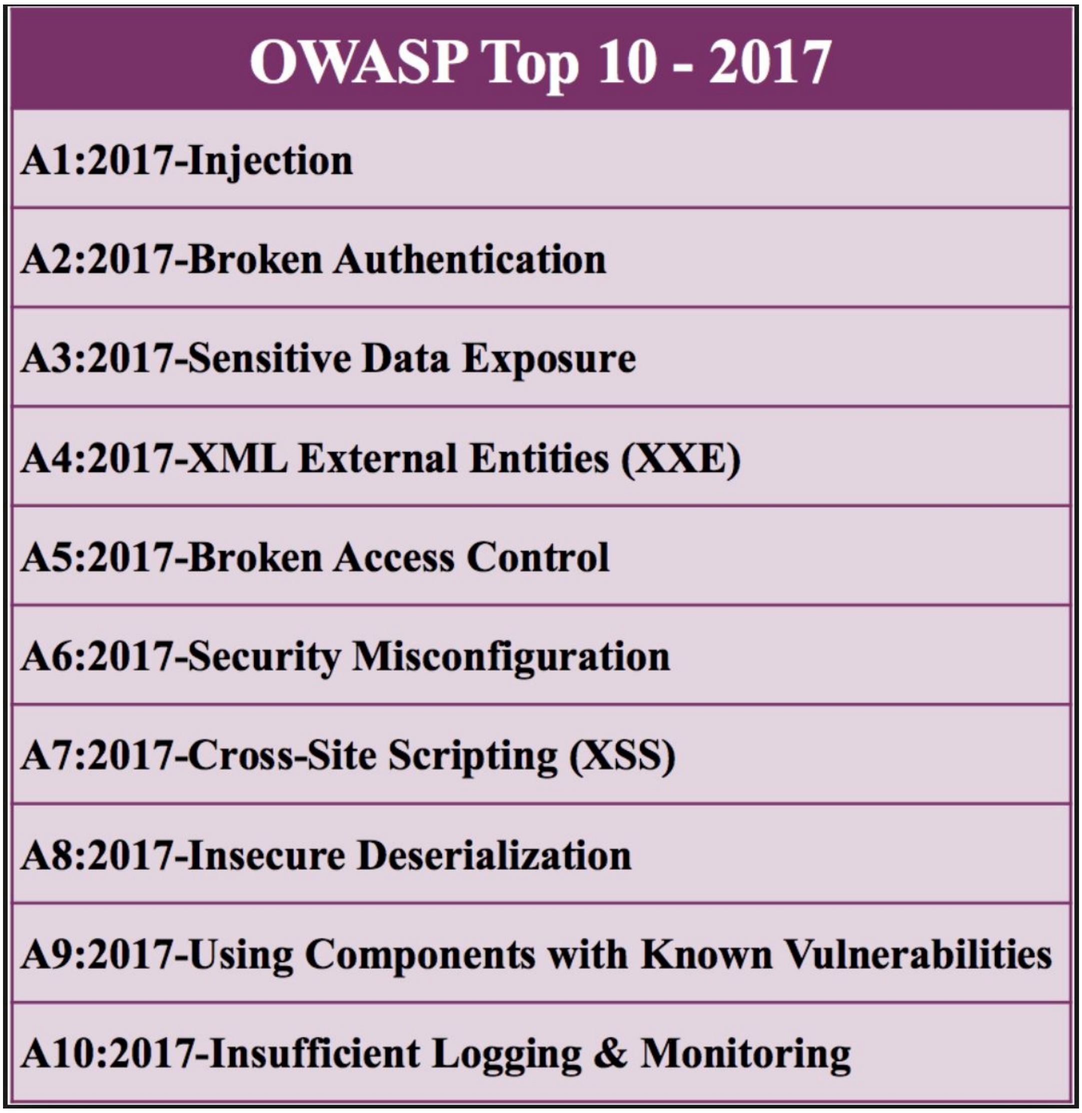
PTES Methodology

1. Pre-Engagement
2. Intelligence Gathering
3. Threat Modelling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

2.1.2. OWASP

OWASP (The Open Web Application Security Project) is an open community dedicated to carrying out efforts to develop, acquire, operate and maintain trusted applications.

Here are the top ten coverage of OWASP:



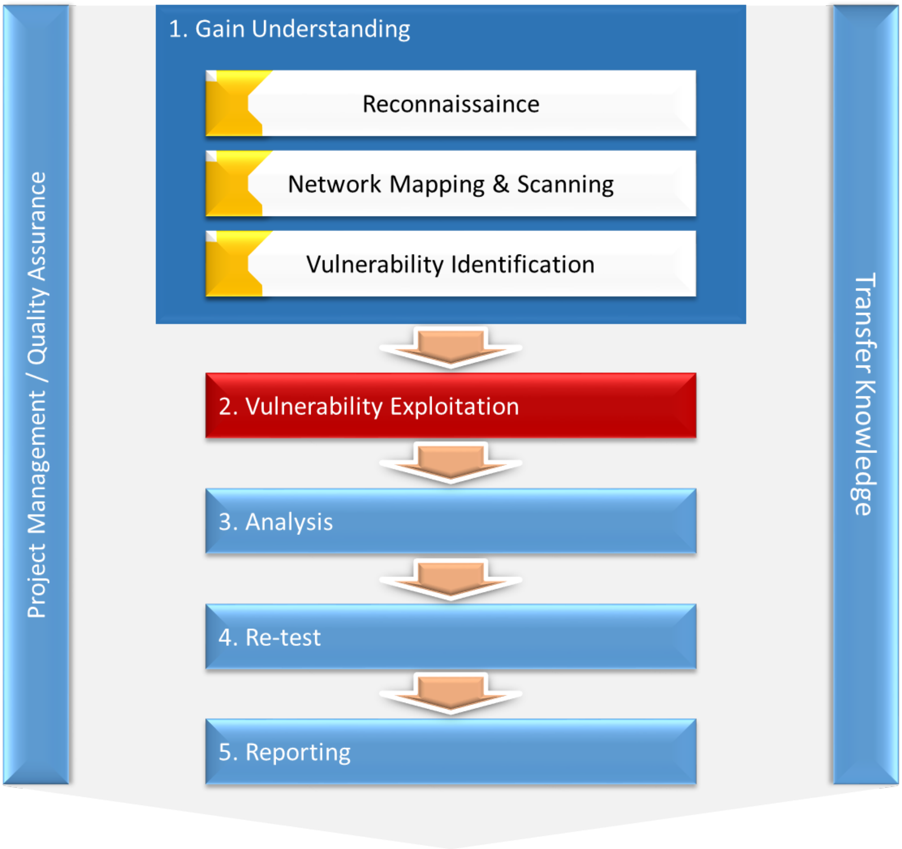
OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2.2. METHODOLOGY AND TOOLS

Based on the description of the approach described above, the following methodology and tools are used:

- *Penetration Test Method.*

  The following methodology will be used in the Penetration Test in the client based on the description of previous approaches.


Project Management / Quality Assurance
1. Gain Understanding
Reconnaissaince
Network Mapping & Scanning
Vulnerability Identification
2. Vulnerability Exploitation
3. Analysis
4. Re-test
5. Reporting
Transfer Knowledge

Picture 3. Metodology Penetration Test Equine

- Tools

  During the performance of Vulnerability Assessment and Penetration Test, pentester will use the tools to use tools and do it manually Penetration Test. In accordance with the conditions at the time of execution of the work, the tools that can be used by Pentester PT Sekuriti Siber Indonesia are:

	Tools	***Description***
1	Kali linux	*Comprehensive Penetration Testing*
2	Nessus	*Network and Server Vulnerability Scanner*
3	Nmap	*Port Scanner*
4	Metasploit	*Exploitation Framework*
5	OWASP ZAP	*Web Application Attack Proxy*
6	Burp Suite	*Web Application Vulnerability Scanner*
7	SQLmap	*SQL injection & Database takeover tool*
8	John The Ripper	*Password Cracker*
9	DirBuster	*Web Application Directory Bruteforcer*
10	Ettercap-NG	*Packet sniffer and interceptor*
11	Fire walk	*Firewall scanner*
12	dnsmap	*DNS Lookup*
13	FierceDNS	*DNS Lookup*
14	mtr	*Network Route*
15	theHarvester	*Domain Harvester*
16	Nikto	*Web Application Scanner*
17	Joomscan	*Web Application Scanner*

18	WPScan	*Web Application Scanner*
19	W3AF	*Web Application Assessment Tool*
20	Fimap	*File Inclusion Exploiter*
21	XSSRays	*XSS Vulnerability Scanner*
22	BeEF	*Client-side XSS Exploiter*
23	Skipfish	*Web Application Vulnerability Scanner*
24	Hydra	*Brute Force*

Tabel 1. Tools Penetration Test

2.2.1. *Project Management, Quality Assurance, dan Knowledge Transfer*

Project Management, Quality Assurance, and Knowledge Transfer is an activity where all the elements in the above methodology are ensured to run thoroughly and interconnected with each other, and ensure the deliverable quality generated by the methodology can be maintained at a good quality level .

In addition, this activity ensures knowledge related to the scope of work can be understood and applied by key person according to the needs and operational processes. The pentest stages are:

2.2.2. *Gain Understanding*

At this stage we do an understanding of the overall network infrastructure, operating systems used, and services that run on every system. This stage includes reconnaissance, network mapping & scanning, and vulnerability identification.

2.2.2.1. *Reconnaissance*

At this stage, all potential pathways that can be utilized to infiltrate the target are mapped and then validated.

Tabel 2. Activity and Output in the Reconnaissance Phase

Activity	● Identify potential targets ● Conduct an in-depth analysis of the targets ● Using the banner-grabbing technique to find the type and version of the service running. ● Doing DNS Query for information gathering process (get zone transfers, etc.)
Output	● Information on target network infrastructure and operating system

2.2.2.2. *Network Mapping & Scanning*

At this stage, any information (service, operating system, etc.) that has been discovered will be identified and tested with known gaps and possible gaps. Where possible, brute force techniques will be used to test weak passwords.

Tabel 3. Activity and Output in Network Mapping & Scanning Stage

Aktivity	● Scanning ports of all IP addresses in the network to determine the network chart, network configuration, operating system used, services running, etc. ● Use equipment to map network structure. ● Determine the policies and roles used by Firewall.
Output	● *An open port, potentially exploitable configuration* ● Network topology ● Weakness of network infrastructure

2.2.2.3. *Vulnerability Identification*

In this phase we scanned the infrastructure targets.

Tabel 4. Aktivitas dan *Output* dalam Tahap *Vulnerability Identification*

Aktivity	● Specifies the target IP scanning ● Scans the target IP infrastructure
Output	● List of weaknesses of infrastructure and operating systems that can be exploited

2.2.3. *Vulnerability Exploitation*

In many cases, the process of exploitation of security holes will only be given limited access to the system. By doing a deeper exploit it will be possible to get the highest access on the system (root, Administrator).

Tabel 5. Activities and Outputs in the Vulnerability Exploitation Phase

Aktivity	● Use the weaknesses gained to exploit the infrastructure network ● Perform port scanning, fingerprinting and banner grabbing activities to identify server flaws ● Check which version of the operating system to use whether it has a security hole. ● Check the patch level version of the operating system. ● Trying to get a valid user by bruteforce the services that utilize the password-based authentication model. ● Conducting service probing and identification activities. ● Check each service / service (native) from the default OS whether it runs max. ● Check whether the service is running in accordance with the server function, this is to detect whether the server function is already optiomal, and can also detect whether there is unwanted service (malicious). ● Check the version of the service / service if it has a security hole. ● Check the network configuration service against Name Server / Domain to server ● Perform network routing checks from user to server, to get an idea of possible security hole arising from topology. ● Check for possible server configuration errors ● Check for possible configuration errors from the network device ● *Login to the target system or system to be used as launching pad and then dig as much information as possible for use on the next infiltration*
Output	● Lists of systems, infrastructure, networks and applications that can be exploited

2.2.4. *Analysis*

At this stage, all vulnerability findings are ranked risk based on severity by considering likelihood in exploiting these weaknesses.

Tabel 6. Activity and Output in Analysis Stage

Aktivity	● Determining the risk rating on the vulnerability of exploitation results
Output	● List of findings and risk categories

Here are four risk ratings to be assigned to each vulnerability found.

1. **High** : Security issues that have to be fixed immediately because of potentially can be exploited.
2. **Medium** : Security concerns have to be taken into consideration even though the vulnerability is difficult to exploit.
3. **Low** : Security issues with limited impact.

High

Medium

Low

2.2.5. Reporting

Each stage that has been done will produce a report. Reports from each stage will be compiled and produce a comprehensive final report.

2.3. SCENARIO PENETRATION TESTING

2.1.1. *Black Box Testing*

In testing with Black Box testing type, Pentester will only be given IP target which will be Penetration Test. The purpose of black box testing is to provide an image of the attack from the external environment. By doing this black box testing, the expected result is an analysis of attacks from external.

2.1.2. Black Box Testing Work Limit

Penetration Test is done in Black Box testing condition where Pentester is given IP target in Penetration Test implementation.

Specifically, the method of black box testing done in the implementation of Penetration Test work on the client by doing through an external network.

This Penetration Test condition simulates a situation like hackers who do not know or have access to the client's internal network system and try to find vulnerabilities to the client system.

2.1.3. *Grey Box Testing*

In testing with Gray Box testing type, Pentester will only be given limited information related to the target that will be in Penetration Test. The purpose of Gray Box testing is to provide an overview of attacks from the external and internal environment. Pentester will act as an employee user and can be like someone else who has not known the Flow of the app

.

2.1.4. *Grey Box* Testing Work Limit

Penetration Test is done in Gray Box testing condition where Pentester is only given limited information related to application which will be Penetration Test.

Specifically, gray box testing method is performed in the implementation of Penetration Test work on the client by doing it through internal network and external network.

This Penetration Test condition simulates a situation like hackers who do not know or have access and simulate situations like employees of the company to enter into the client's internal office network system and try to find vulnerabilities to the client system.

3. PROJECT MANAGEMENT

The project management section describes scheduling, list of reports / deliverables, organizational structure, composition of experts assigned to this work..

3.1. SCHEDULE OF JOB IMPLEMENTATION

To produce a good deliverable quality, the consultant will work with the counterpart of the client according to the scope requirements at each stage. Each consultant and counterpart work for 1 week effective in Penetration Test, where 4 (four) days is done by penetration test, 1 (one) day for report preparation and 2 (two) days re-tested.

3.2. REPORTS (*DELIVERABLES*)

Reports generated based on five milestones:

Tabel 8. Reports (*Deliverables*)

Kegiatan	*Deliverable*
Report Penetration Test	
Report Penetration Test After Re-test	

The report will be presented in the form of power point and hardcopy of a number of attendees, as confirmation before the submission of the final report. Each report consists of:

1. *Executive Summary*

   This section contains summaries of findings that provide clear information on Penetration Test results.

2. *Fact and Finding*

   This section includes results and views on findings and provides clear information on alternative solutions to mitigate potential risks to the findings.

   In this section is also done first verification of the assessment results before the findings submitted to the Indonesian client as a weakness, every use tools (tools) to perform Penetration Test.

3. *Risk Analysis*

   This section covers risk analysis and risk levels resulting from the vulnerability of Penetration Test results.

4. Recommendations for fixing

   This section includes recommendations for improvement as a result of the findings in the implementation of Penetration Test work.

WORK ASSUMPTIONS

- The work is done off site from the client's Office location according to the work schedule.
- the client assigns a special Project Manager to oversee this work, as a partner with the Project Manager from PT Sekuriti Siber Indonesia.

4. PT Sekuriti Siber Indonesia

The profile section of PT Sekuriti Siber Indonesia describes the company profile, the translation of PT Sekuriti Siber Indonesia, and the project portfolio ever undertaken by PT Sekuriti Siber Indonesia.

4.1. COMPANY PROFIL

PT Sekuriti Siber Indonesia is a company focused on professional IT consulting services, PT Sekuriti Siber Indonesia provides 3 (three) service pillars for leading companies in Indonesia, as shown in the picture below.

PENETRATION TESTING

SECURITY ASSESSMENT

SECURITY TRAINING

picture 4. Our Services

4.2. PORTFOLIO PROJECTS A TYPE

Below is a similar work portfolio of Companies and Consultants to support our proven solutions in several companies.

Tabel 11. Our Portofolio

No	Company		Project
1	BPJS Ketenagakerjaan	BPJS Ketenagakerjaan	*Web Application Penetration Testing, Mobile Application Penetration Testing*
2	PT. Mitra Transaksi Indonesia (Yokke), PT	yokke!	*Penetration Testing Service*
3	Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia	KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI MELAYANI MASYARAKAT	*Web Application Penetration Testing*
4	PT Kredit Pintar Indonesia	KreditPintar	*Android Apps, Backend, and data center recovery*

So we submit this proposal, in the hope that the client gives us confidence to assist in this Penetration Test work.

PT Sekuriti Siber Indonesia, with Pentester personnel and Consultants deployed in this work, is committed to delivering the best service in accordance with clients' needs. Personnel consultants who are involved always strives to create effective communication in every job execution activity.

Hopefully the cooperation between client and PT Sekuriti Siber Indonesia can produce optimal results and benefits for both parties.