Digital Policy Office

INFORMATION SECURITY

Practice Guide

for

Penetration Testing

Version 1.3

July 2024

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Included the stringent vulnerability management; Elaborated the penetrating testing and vulnerability scanning; Updated OWASP Top 10 Vulnerabilities	Pages 1,6 Annex A	1.1	June 2021
2	Updated normative references to include national GB standards related to information security; Introduced an additional option for information gathering during the pre-attack phase	Pages 2, 12, Annex A	1.2	December 2023
3	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”)		1.3	July 2024

TABLE OF CONTENTS

1. Introduction

In accordance with the IT Security Guidelines (G3), Bureaux and Departments (B/Ds) are required to conduct vulnerability scan and / or penetration test for all Internet-facing websites and web applications before production, prior to major enhancements and changes associated with websites or web applications and at least once every two years. All servers and devices deployed in systems containing or handling classified information should be subject to stringent vulnerability management, such as all known vulnerabilities should be fixed within a month after the release of security patches; and annual vulnerability scan or penetration test should be conducted for such systems. A penetration test should also be conducted subject to the results of security risk assessment. This practice guide is developed to help facilitate B/Ds in considering and planning to conduct a penetration test.

1.1 Purpose

The purpose of this document is to provide general knowledge and best practices on penetration testing. This practice guide presents an overview of the key concepts B/Ds need to understand in order to conduct penetration test, including definition and limitation of the penetration test, considerations in defining the scope and requirements of the penetration test, as well as major tasks that should be taken care of before, during and after the penetration testing. It is intended for staff who are involved in planning or conducting a penetration test.

This document describes an overview of the penetration testing and covers the following topics:

a) Overview of Penetration Testing
b) Penetration Testing Process
c) Penetration Testing Tools
d) Penetration Tester Selection Criteria

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of the Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of the Hong Kong Special Administrative Region
- Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2013

- Information technology – Security techniques – Code of practice for information security controls, ISO/IEC 27002:2013
- Information technology – Security techniques – Information security risk management, ISO/IEC 27005: 2018
- PCI Security Standards Council, "Information Supplement: Penetration Testing Guidance", September 2017

  (https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf?agreement=true&time=1620631951140)
- Open Web Application Security Project, "OWASP Testing Guide v4. 2" (https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf)
- The Association of Banks in Singapore, 2015, "Penetration Testing Guidelines for the Financial Industry in Singapore"

  (https://abs.org.sg/docs/library/abs-pen-test-guidelines.pdf)
- NIST Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment"

  (http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf)
- Patrick Engebreston, Syngress, "The Basics of Hacking and Penetration Testing", 2nd Edition 2013
- 中華人民共和國國家標準，《信息安全技術 信息安全風險評估方法》，GB/T 20984-2022
- 中華人民共和國國家標準，《信息安全技術 信息安全風險評估實施指南》，GB/T 31509-2015
- 中華人民共和國國家標準，《信息安全技術 網絡安全漏洞分類分級指南》，GB/T 30279-2020

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3 and the following apply.

Abbreviation and Terms	
NA	NA

1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to:

Email:	it_security@digitalpolicy.gov.hk
Lotus Notes mail:	IT Security Team/DPO/HKSARG@DPO
CMMP mail:	IT Security Team/DPO

2. Overview of Penetration Testing

2.1 What is Penetration Testing

Penetration testing is a kind of security assessment that encompasses the vulnerability assessment and verifies if vulnerabilities of a system can be exploited by attackers. Penetration testing is a manual process which requires expert knowledge to design test cases and select appropriate techniques or tools to identify logical vulnerability that cannot be identified through automated tools. The use of vulnerability scanning or other automated tools could usually facilitate penetration testers by alleviating some of the repetitive tasks.

During penetration test, automated tools are usually used to scan the network or system first, in order to create a complete map of connected workstations and servers, and to identify possible vulnerabilities. The scanning process could usually generate a huge amount of test cases and network traffic, which may render system inoperable during the course of penetration testing. After vulnerabilities scanning, the penetration tester would use the scanning results to conduct further testing.

Penetration test helps to identify the weakness or vulnerability in computer systems. It also simulates multiple attack vectors to happen simultaneously and checks if it would result in a successful compromise. After penetration test, the effectiveness of the existing security controls against an active, human, skilled attacker would be understood. The result of the penetration testing would facilitate system owners to implement safeguards against the security risk.

The penetration testing should be performed after careful consideration and planning. Due to the high demand of expert knowledge and experiences in performing the exploitation, a penetration testing should be performed by qualified security experts.

2.1.1 Penetration Testing Objectives

Penetration test is a kind of security assessment activity. It can be performed with different approaches and different techniques, depending on test objectives. B/Ds should define their scope and objectives of their own penetration testing. Some examples of objectives of penetration testing are listed as follows:

a) Identify threats of the information assets;

b) Identify vulnerabilities such as the logic of the firewall security policy setting, time bomb and backdoor coded in programs that may be difficult or impossible to detect with automated network or application vulnerability scanning software;

c) Test and validate the efficiency of security protection and controls;

d) Test the defensive ability to detect and respond to attacks;

e) Evaluate the effectiveness of network security devices such as firewalls and routers; and

f) Demonstrate the ability of the system in guarding against real-world cyber attack.

2.1.2 Penetration Testing Approach

Depending on testing objectives, penetration testing could be conducted with different approaches. It can be conducted either in external network or internal network.

a) External testing is a more common approach for penetration testing. It involves a comprehensive analysis of an organisation's externally visible servers and devices, e.g. routers, firewalls, mail servers and web servers. The purpose of external testing is to identify potential weakness in the security of networks, systems and applications, and demonstrate the existence of known vulnerabilities that can be exploitable by an external attacker. It helps to check if the system is securely protected from intrusion, contemplation and information loss or disclosure.

b) Internal testing is conducted from the internal network with assumption that an attacker has penetrated through the perimeter defence, or an attack is originated by an insider. This testing focuses on organisation's internal resources, e.g. Demilitarised Zone (DMZ), internal network, system-level security, application and services configuration, and authentication and access control. It is used to identify the weakness of computer systems inside a particular network, and check if anyone can access the system inside the network by misusing user privileges.

Regardless of whether the penetration testing is conducted in external network or internal network, it can be performed by white-box, grey-box or black-box approach. These approaches are described below:

i) White-box testing:

Testing is performed with knowledge of the internal structure, design and implementation of the system being tested;

ii) Grey-box testing:

Testing is performed with partial knowledge of the internal structure, design and implementation of the system being tested; and

iii) Black-box testing:

Testing is performed without prior knowledge of the internal structure, design and implementation of the system being tested.

If the objective is to identify as much vulnerability as possible, white-box testing should be used and information such as program source code or configuration should be shared so that the penetration tester can perform analysis directly. On the other hand, if the objective is to evaluate the effectiveness of the security posture, black-box testing should be used and information mentioned should be withheld to project more realistic results.

Compared with white-box testing, the black-box testing would be more time consuming and costly to gather and discover system information. Some security areas may be missed under the black-box testing. However, it simulates a more realistic situation that an external attacker attempts to invade a system. On the other hand, the white-box testing can shorten the penetration testing time and a more thorough security assessment can be conducted because complete information e.g. network topology documents, asset inventory and application design information, are provided to the penetration tester under the white-box testing.

2.1.3 Penetration Testing Techniques

A variety of techniques are being used during penetration testing. The most common techniques are listed as follows:

a) Passive research:

Gather system configuration information of an organisation from public domain sources such as domain name server (DNS) record and name registries;

b) Operating system fingering and network mapping:

Identify the entire network configuration being tested;

c) Network sniffing:

Capture data as the data traffic flowing through a network;

d) Spoofing:

Use one machine to pretend to be a legitimate machine to capture information;

e) Trojan attack:

Install a Trojan, malicious software onto the victim's system through a variety of ways, such as email attachment, to access useful information;

f) Brute-force attack:

Crack passwords to gain access to systems or applications. It is the commonly known password cracking method or an attack being used to overload a system to prevent it from responding to legitimate requests;

g) Vulnerability scanning:

Discover weakness of a security system or application for further attack;

h) Social engineering:

Gather important information of an organisation. An attacker usually targets employees within an organisation in an attempt to gain sensitive information; and

i) Dumpster diving:

Find information about an organisation just by examining the trash and can be a part of the physical penetration testing.

2.2 Penetration Testing vs Vulnerability Scanning

Vulnerability scanning is most often confused with penetration testing. These two terms are often used interchangeably, but they are different processes. Penetration testing would often include vulnerability scanning process but it would not a must. Therefore, an organisation must specify clearly in their service specification for both activities in order to have a more thorough testing.

Vulnerability Scanner vs Penetration Tester
A vulnerability scanner makes use of standard test cases to identify known technical vulnerabilities such as misconfiguration, kernel flaws, buffer overflows, insufficient input validation, incorrect file and directory permissions.

On the other hands, penetration testers need to make use of their skills and experience to understand the system workflow and then design specific test cases to identify logical vulnerabilities of the system. Besides, the penetration testers would try to exploit the vulnerabilities found in the scanning result and identify what type of information could be revealed.

Result Handling of Vulnerability Scanning
Vulnerability scanning is used to determine if weakness exists in a system. It involves the process of identifying, ranking and reporting the vulnerabilities. However, the results from vulnerability scanning cannot interpret if the vulnerabilities identified are truly exposing risk to the system. Nevertheless, it can be used as a baseline indicator to the potential attacks or threats of the system.

On the other hand, a penetration tester usually makes uses of the results from vulnerability scanning to determine if additional testing is required to identify vulnerability that cannot be identified through automated tools alone. Furthermore, penetration testing would deploy more specific methods to show how the vulnerability can be exploited or how to repeat the test result. In short, penetration testing produces more comprehensive results than vulnerability scanning.

Skill Set
Vulnerability scanner makes use a variety of automated tools while the process of exploitation of a penetration test involves a lot of trial and attempt, and it is highly dependent on the skill and experience of the penetration testers.

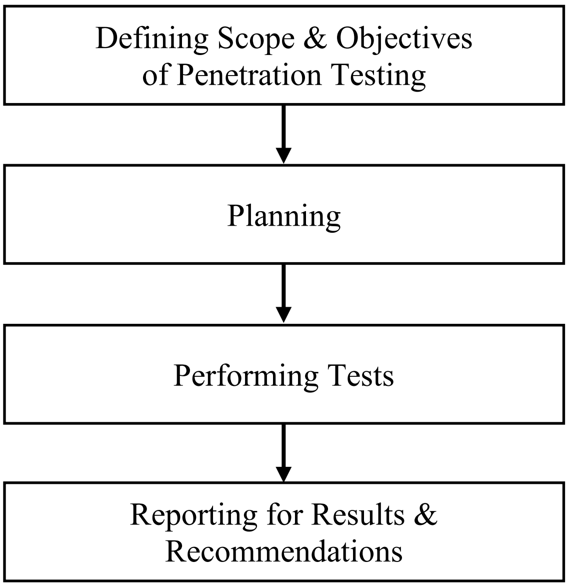
Process time

As vulnerability scanning is an automated process, it can be performed within a short period of time (say, a few hours). However, it may produce false positives, and thus may require manual verification. Penetration testing, in contrast, is a manual process which would usually base on vulnerability scanning results to further identify the vulnerabilities in the system. Therefore, it generally takes more planning and longer time than vulnerability scanning.

3. Penetration Testing Process

3.1 Penetration Testing Steps

In spite of different types of penetration testing, there are some common activities that should be performed before and after penetration testing. Typically, they can be divided into the following steps:


Defining Scope & Objectives of Penetration Testing
Planning
Performing Tests
Reporting for Results & Recommendations

Steps for Penetration Testing

3.2 Defining Scope & Objectives of Penetration Testing

The security of a system covers various areas. Different types of penetration testing could be used to test against different security areas. The most common areas are listed as follows:

a) Network Security:
It is to identify all the possible network flaws and simulate a real attack on the vulnerabilities found;

b) System Software Security:
It is to identify all the possible system software flaws and simulate a real attack on the vulnerabilities found;

c) Client-side Application Security:
It is to identify all the possible application flaws, mainly on client-side functions, and simulate a real attack on the vulnerabilities found;

d) Server-side Application Security:
It is to identify all the possible application flaws, mainly on server-side functions, and simulate a real attack on the vulnerabilities found;

e) Physical Security:

It is to gain physical access to organisational resources, e.g. data centre before, during, and after business hours. Usually, all the physical security controls are tested;

f) Intrusion Detection:

It is to test the strength of an intrusion detection system, usually with the software tools; and

g) Incident Response:

It is to test if the proper procedure of incident response is in place and the readiness of the incident or emergency response team.

Initially, B/Ds should define the scope and objectives of the penetration testing based on the business needs, objectives to be achieved and the resource availability. B/Ds can then decide which type of penetrating testing should be performed. The scope can be determined by the following factors:

a) Size and number of applications, network devices, servers, e.g. only application system is being tested or all servers or entire architecture are included;

b) To conduct internal or external penetration testing or both; and

c) To conduct white-box, grey-box or black-box penetration testing or any combination of them. For grey-box and white-box penetration testing, B/Ds have to provide the information, on need-to-know basis, to meet the objective and purpose of the penetration testing.

3.3 Planning

Before a penetration testing, planning of the testing should include proper preparation, monitoring and control. Penetration testers should prepare and submit a penetration testing plan (please refer Annex C for the sample template of a penetration testing plan) before conducting the penetration testing. The content of the penetration testing plan should include, but not limited to the followings:

a) Scope
b) Objectives
c) Schedule
d) Roles & responsibilities of stakeholders
e) Testing approach and methodology
f) Tools being used
g) Fallback and recovery procedure

B/Ds have to work with the penetration testers on the testing schedule and to agree on which environment, such as production, pre-production or UAT, the penetration testing should take place. Since some penetration testing techniques test the application, system or network with actual exploits and may affect system availability and expose sensitive data, production environment should be avoided for the penetration testing whenever possible. It is also important to document and agree mutually upon the degree of exploitation, so that the penetration testing could be stopped when reaching a certain degree of exploitation, such as gaining access to a particular system, to avoid adverse effect to the system or data.

The following practices should be observed before penetration testing is conducted:

a) B/Ds should provide the contact list of system owner and IT administrators of the testing system to the penetration testers so that any issues raised during the test could be reported timely;

b) B/Ds should get the contact list of the penetration testers so that B/Ds can stop all tests promptly, if necessary;

c) B/Ds should consider if the existing security controls (e.g. intrusion protection systems (IPS) and web application firewall (WAF) that would affect the result of the penetration test) should be disabled or configured in order not to interfere the tests;

d) B/Ds should inform and alert the security monitoring service provider prior to the penetration testing, unless the objectives of penetration test involve assessing the effectiveness of the monitoring capability of the security monitoring service provider;

e) B/Ds should consider providing necessary testing credentials to penetration testers for effective testing application layer functionality;

f) B/Ds should ensure the latest full system backup of the testing system is available for restoration, in case the integrity of the system data are being affected;

g) B/Ds should mask all the test data which involves classified information or personal data;

h) B/Ds should arrange the penetration testing at non-peak working hours; and

i) B/Ds should require the penetration testers to sign a non-disclosure agreement to protect the privacy or confidentiality of the system data.

3.4 Performing Tests

Generally, penetration testing on application, system or network involves three phases: pre-attack, attack and post-attack.

3.4.1 Pre-attack

Pre-attack phase focuses on gathering information about the targeted application, system or network. Unless white-box testing approach is being used, reconnaissance is the preliminary step to locate, gather, identify, and record information about the application, system and network to be tested. It aims at digging out as much information as possible in different ways to formulate/facilitate an attack. There are two kinds of reconnaissance: passive and active. Passive reconnaissance is an attempt to gather information about the target application, system or network without actively engaging with the systems. This includes techniques like collecting data from public sources like public file repositories. The penetration tester may also request for a walkthrough to the system in order to understand its business logic. Active reconnaissance engages the target application, system or network actively by employing automated tools such as vulnerability scanner, network sniffers to send probes to the targets in the forms of port scans, network sweeps and enumeration of user accounts. Information collected during the pre-attack phase can be:

a) Network registration information, e.g. domain name, registrant name and email address;

b) DNS and mail server information, e.g. DNS name and mail server name;

c) Operating system information, e.g. type and version number of operating system;

d) Authentication and credential information, e.g. user login name and password for the target system;

e) Contact information, e.g. organisation contact person and phone number;

f) Website information, e.g. website Uniform Resource Locator (URL), website Internet Protocol (IP) address and program source code; and

g) Any other information that facilitates the exploitation of the targeted application, system and network.

After relevant information is gathered, vulnerability analysis starts either automatically by the vulnerability scanner to compare the information collected from applications, operating systems and network against the vulnerability database or manually based on the penetration tester's knowledge of vulnerabilities. Manual processes can identify false positives found in the scanning result, and new vulnerabilities that automated tools may have missed, but it usually requires more effort and time.

3.4.2 Attack

Depending on the scope and objectives of the penetration test, penetration testers should decide the most appropriate approaches, tools, or techniques to perform the penetration test in the attack phase. It is a manual process which requires skills and experience to decide specific test cases and select appropriate techniques or tools to identify flaws. The use of vulnerability scanning or other automated tools could facilitate the penetration testers by providing a baseline of potential attack surface of the system.

This phase usually involves the actual compromise of the application, system and network by attempting to exploit the vulnerabilities discovered during the pre-attack phase. The attack phase usually involves three main activities, i.e. gaining access, escalating privileges and installing additional tools.

The testers would initially try to gain access of the system being exploited. After the system or application is accessed for vulnerability exploitation, attacks such as structured query language (SQL) injection and system data modification, would be performed. Moreover, escalation of user privilege on the application and system would be attempted with the target to gain access to more sensitive information. The testers would also install additional software or tools, if possible, to the targeted system to launch further attack or exploit more vulnerabilities.

During this process, the penetration testers should design test cases specific to the system and record the testing methods (i.e. how to reproduce the same successful exploitation) and collect evidence for preparation of penetration testing report. If a serious vulnerability which would affect the existing system is identified, the penetration testers should document the detailed procedure on how to cause the serious vulnerabilities and notify the responsible party immediately.

3.4.3 Post-attack

Post-attack phase involves performing environment clean up, restoring of the system to pre-test state and capturing logs for proof of successful attack. The typical activities carried out in the post-attack phase are listed below:

a) Extract the relevant logs as evidence for the test;

b) Clean up all files uploaded to the tested system;

c) Remove all files generated during the test;

d) Delete any user accounts created for the test;

e) Uninstall all tools for performing the test on the tested system;

f) Reverse all changes in user privilege and settings; and

g) Restore system or application configurations or settings

It is important that penetration testers have to document and disclose to the responsible party any alterations made to the environment during the test. The penetration tester or responsible party has to restore the targeted environment to the pre-test state.

Examples of conducting penetration test for web application and IT Infrastructure are enclosed in Annex A and B respectively for demonstrating how to apply these three phases of attacks in performing the penetration test.

3.5 Reporting for Results & Recommendations

A penetration testing report is required upon completion of the penetration testing (In most of the cases, there will be a debriefing session for the penetration testers to explain the details of the report). The penetration testing report should record down the details of testing activities performed and the findings with recommendation. The contents of the penetration testing report should include, but not limited to:

a) Executive summary:
A high level summary of the penetrating testing scope, objectives and findings;

b) Project scope:
A detailed description on the scope of application, system or network being tested;

c) Testing methodology:
A detailed description on the testing approach and methodology used to complete the testing;

d) Tools used;

e) Limitations and constraints:
A detailed description on any restrictions imposed on testing such as stipulated testing hours, special testing requirement for legacy systems, etc.;

f) Testing activities:
A detailed description of what attack activities performed;

g) Findings with recommendations:
A detailed description of the vulnerability found, vulnerability risks ranking, vulnerability attacks performed for each vulnerability, attack results, evidence supporting the findings and the risk mitigation recommendations; and

h) Environment clean up after the penetration testing:
A detailed description and directions on how clean up should be performed and how to verify the restoration of security controls.

Before the project acceptance of the penetration testing, B/Ds should verify the following:

a) Non-disclosure agreements are signed and submitted;
b) All the required post-attack tasks are performed by the service providers or the penetration testers;
c) Project requirements specified in the work assignment brief are all being implemented; and
d) Sufficient and correct details are provided in the submitted reports such as penetration testing report and penetration testing plan.

3.6 Follow-up actions

Upon receiving the penetration testing report, it is important that B/Ds should follow-up with the remediation in a reasonable period of time after the test.

The result of the penetration testing might not be always exhaustive to identify every instance of a vulnerability. For example, finding an instance of cross site scripting vulnerability of an application does not indicate that this vulnerability does not appear in other area. B/Ds should carefully investigate the presence of these vulnerabilities and ensure all of them could be handled by the remediation.

After the remediation is performed, B/Ds should arrange a retest to validate the newly implemented controls if they have mitigated the original risk.

4. Penetration Testing Tools

Penetration testing tools can assist penetration testers to improve the efficiency of penetration testing process. Although there are a variety of penetration testing scope such as network, application and intrusion detection system, different types of penetration testing tools in the market are designed to perform specific testing functions. In general, the penetration testing tools mainly serve two purposes:

a) Gathering target system/application information; and

b) Performing attacks based on specific vulnerabilities.

Some penetration testing tools can be used for identifying existing vulnerabilities on the application, network (network-based) or on specific hosts (host-based) and launching attacks. Whilst some tools are designed to perform vulnerability scanning, they would not perform real attacks.

For network security penetration testing, tools with functions for network mapping, network sniffing and vulnerability scanning would usually be used for discovering information below:

a) Network topology;

b) Active servers and network devices; and

c) Operating system type, application, services running on active servers and network devices.

After IT infrastructure related vulnerabilities are identified, attacks can be performed manually or using automated penetration testing tools, with attack capability, according to the process as specified in the Annex B - Penetration Testing for IT Infrastructure.

For web application penetration testing, tools with functions below would usually be used for information gathering and identifying vulnerability:

a) Intercepting proxy:

   Inspect and modify HTTP traffic between browsers and target applications;

b) Web application spider:

   Crawl the web application content and functionality to uncover missed or hidden web content to provide a detailed picture of the application’s content; and

c) Web vulnerability scanning:

   Discover application vulnerabilities such as SQL injection, cross-site scripting and directory traversal.

After gathering information and identifying vulnerabilities related to the application, penetration tester can make use of the result to judge if additional test is required. Further attacks can be performed either manually or using automated penetration testing tools, to test against the list of common critical web application vulnerabilities listed in Annex A - Penetration Testing for Web Application.

The choice of penetration testing tools depends on:

a) Type of penetration testing, e.g. network penetration testing or application penetration testing; and
b) Preference or professional judgement of the penetration tester.

Commercially available tools, together with penetration tester's own developed tools can be used to conduct the penetration test.

5. Penetration Tester Selection Criteria

Qualified penetration testers should possess relevant certification and work experience to conduct the penetration test.

Certification held by a penetration tester may indicate the skill level and competence of a potential penetration tester. The following are some examples of common penetration testing certifications:

a) Certified Cybersecurity Penetration Assessment Professional (NSATP-A);

b) Certified Ethical Hacker (CEH);

c) Certified Information Security Professional - Penetration Testing Engineer (CISP-PTE);

d) Certified Information Security Professional - Penetration Testing Specialist (CISP-PTS);

e) CREST Penetration Testing Certifications;

f) Global Information Assurance Certification (GIAC) Certifications; and

g) Offensive Security Certified Professional (OSCP).

Apart from the certification possessed by the penetration tester, the following working experience attributes of the penetration tester should be considered to determine whether the penetration tester is qualified for a penetration testing project:

a) Number of years the penetration tester on penetration testing.

   Note: It is rather arbitrary to determine the required number of years of experience. To ensure the penetration tester has adequate experience to perform the testing, a higher number of years is preferred.

b) Knowledge and work experience which are relevant to the technologies in the target environment, i.e. operating system, hardware, web application, network services, protocols and etc.

c) Number of projects of similar penetration testing areas performed previously.

Annex A: Penetration Testing For Web Application

Web Application Penetration Process

To perform the web application penetration testing, the following three phases would be involved.

Pre-attack Phase

The web application penetration testing under the pre-attack phase is to:

a) Gather information such as sitemap or application URL;
b) Analyse the functionality, core security mechanism such as session management and access control of the application; and
c) Identify the technologies employed for the web application.

The purpose is to identify the attack surfaces the application exposed and design the approach to identify the application vulnerabilities.

An automated web application scanner would usually be used. Since most web application vulnerabilities are signature based, an automated web scanner is able to detect known vulnerabilities on the operation system level such as outdated software version, missing patches, buffer overflow and misconfiguration. It can also detect some application level vulnerabilities such as cookies issues, cross-site scripting (XSS), directory traversal and SQL injection. Generally, an automated web application scanner provides a baseline of potential vulnerabilities and attack vectors to the penetration tester. The penetration tester can make use of the results to decide if additional testing is required:

a) Collect basic information of the application, such as the operation systems, application server version and web server version. It also browses all web pages, directories and indexes of all files making up the web applications; and
b) Identify application level vulnerabilities such as cookies issue, directory traversal and SQL injection.

However, some common vulnerabilities below do not have a standard signature and cannot be detected by automated tools:

a) Weak access control, e.g. a user can access other’s user data or a low-privileged users can access administrative functions;
b) Flaw in design of the application functionality, e.g. weak password rules or enumerate username from the login failure message;
c) Leakage of sensitive information, e.g. web application response is being analysed and inspected for vulnerabilities, or public file repositories are being inspected for leaked resources such as program source code and configuration files;

d) Modification of a parameter value that has special meaning of the application, e.g. a vulnerability scanner cannot know the meaning of a hidden field; and

e) Flaw in session management.

Attack Phase

After studying the results from vulnerability scanning, the penetration tester should walkthrough the web application and test the function of the testing application. The tester then designs specific test cases and looks for possible vulnerability by professional judgement and experience.

The penetration tester could use intercepting proxy to modify the HTTP traffic between the browser and application to perform the test. Automated tools or manual techniques would be used to initiate attacks such as structured query language (SQL) injection, system data modification, escalation of user privilege or installation of additional software or tools, if possible, to the target system to launch further attack or exploit more vulnerabilities.

Post-Attack Phase

Web application post-attack phase, similar to other types of penetration testing, involves performing environment clean up, restoring of a system or configuration file to pre-test state, capturing logs for proof of successful attack and uninstallation of any installed software.

OWASP Top 10 Vulnerabilities

The Open Web Application Security Project (OWASP) is an online community, which presents a family of the most critical web application flaws that are easy to find, easy to exploit, and frequently occur in web applications. B/Ds should ensure that the scope of penetration test has included testing all these most critical vulnerabilities. The 2021 OWASP Top 10 vulnerabilities are listed as follows:

a) Injection;

b) Broken Authentication;

c) Sensitive Data Exposure;

d) XML External Entities (XXE);

e) Broken Access Control;

f) Security Misconfigurations;

g) Cross-Site Scripting (XSS);

h) Insecure Deserialization;

i) Using Components with Known Vulnerabilities; and

j) Insufficient Logging and Monitoring.

Annex B: Penetration Testing for IT Infrastructure

IT Infrastructure Penetration Process

IT infrastructure penetration testing is confined to the exploitation on vulnerabilities existed in network security devices and servers such as firewall, router, web server, application server and database server. To perform the IT infrastructure penetration testing, three phases: pre-attack, attack and post-attack would be involved.

Pre-attack Phase

In the pre-attack phase, it is to identify the vulnerabilities of the servers, network devices and the networking environment exposed and design the approach to exploit the vulnerabilities. Under the pre-attack phase, IT infrastructure penetration testing usually performs the tasks below:

a) Network Discovery:

   Passive or active techniques can be used to discover active and responding network devices and servers to figure out the network topology. Passive techniques using a network sniffer to monitor network traffic and identify the IP addresses, ports in use as well as operating systems of the active network devices and servers. Active techniques, through the use of automated tools, send various types of network packets such as Internet control message protocol, to request responses from network devices and servers;

b) Network Port and Service Identification:

   Based on the IP addresses identified on the network discovery process, a scanner tool is used to find out network ports, services, applications and services running on active network devices and active servers. Through the processes named as operating system fingerprinting, service identification and banner grabbing, the port scan can identify the operating system type, applications running on the network devices and active servers as well as the application version respectively; and

c) Vulnerability Scanning:

   Port scanner can identify active devices, operating systems, ports, services and applications. However, it cannot identify vulnerabilities. An automated vulnerability scanning tool would attempt to identify vulnerabilities based on the information gathered from the network port and service identification process. It would identify outdated software version, missing patches and misconfiguration by matching the information collected with the known vulnerabilities stored in the scanner’s vulnerability database.

Attack Phase

After vulnerabilities are identified, the exploitation of vulnerabilities would start by gaining access of the targeted network devices or active servers, trying to escalate privileges using automated tools, self-developed programs or manual technique as well as installing additional tools or software for further attack.

Post-attack Phase

IT infrastructure post-attack phase, similar to other types of penetration testing, involves performing environment clean up, restoring of the system or configuration files to pre-test state, capturing logs for proof of successful attack, deleting any testing accounts and files creating for testing purpose, and uninstalling any installed software.

IT Infrastructure Vulnerability Exploitation Category

Listed below are the most common vulnerabilities exploited by the penetration testing on the IT infrastructure:

a) Misconfiguration:
   Misconfigured security setting on the device, such as insecure default settings;

b) Kernel flaws:
   Kernel code is the core of an operating system and enforces the overall security model for the system. Any security flaws in the kernel become vulnerability being exploited;

c) Incorrect file and directory permission:
   File access rights assigned to users and processes are controlled by file and directory permission. Inappropriate permission induces various types of attacks such as reading or modification of the password file;

d) Missing security patches:
   Missing security patches causing vulnerabilities to be exploited for malicious attack; and

e) Privilege escalation:
   System vulnerabilities are exploited to gain access of the highest possible administration privilege to access to the entire network and sensitive information.

Annex C: Sample Template of Penetration Testing Plan

a) Scope

This section specifies the scope of the project. Information of IP addresses that has been tested, type of penetration testing performed, e.g. application or network as well as any other information that affect the time and budget of the project.

b) Objectives

This section provides the objectives that the Government department will gain the benefit after knowing the risks related to the penetration of the target IP addresses/ systems or applications and what benefits can be reaped after mitigating these risks by implementing the recommendations in the penetration testing.

c) Schedule

This section provides the penetration testing start and end dates. It provides the target audiences with information below:

- Testing duration.
- Tested IP address' risks, from penetration testing point of view, during the testing period.
- Penetration tester does not hold any responsibilities if some risk aroused after this period of time due to some changes in the target systems.

d) Roles & responsibilities of stakeholders

This section lists out the tasks that should be performed by the stakeholders for the penetration testing.

e) Testing approach and methodology

This section provides the information about how the penetration testing is conducted. What steps should be followed to collect the information, analyse them, the risk rating methodology used to calculate the risk for each piece of vulnerability.

f) Tools being used

This section provides the information of the tools used by the penetration tester for each penetration testing stage.

g) Fallback and recovery procedure

This section provides the fallback and recovery procedure taken by the stakeholder during the penetration testing period.