Penetration Testing Process: A Preliminary Study

[1]Tan Wai Hua, [2]Saiful Adli Ismail, [3]Hafiza Abas

[1,2,3]Razak Faculty of Technology and Informatics
Universiti Teknologi Malaysia
[1]tan.hua@graduate.utm.my, [2]saifuladli@utm.my,
[3]hafiza.kl@utm.my

Article history

Received:
23 May 2022

Received in revised form:
2 June 2022

Accepted:
15 June 2022

Published online:
30 June 2022

*Corresponding author
tan.hua
@graduate.utm.my

Abstract

Penetration testing also known as pen testing, ethical hacking, or white hat hacking. Ethical hacking is a similar activity that attempts to discover and fix vulnerabilities in a system. The objective of this paper is to identify several methods and vulnerability assessment processes used in penetration testing. Besides, the article has elaborated the benefit and challenges in adapting penetration testing in an organization. A literature review from analysis of academic published papers, articles, and other commercial articles are conducted through the research approach of this paper writing. The review focuses on various journals discussed on different of penetration testing methods and the fundamental differences between penetration testing methods and vulnerability assessment methods commonly practiced by organizations

Keywords: *Penetration testing, Security testing, Ethical hacking, Penetration Testing Process, Penetration Testing Method*

1. Introduction

Penetration test is referring to the ethical computer attack that simulating possible cyber-attacks to test the security level of an information system in order to detect system vulnerabilities and implement security vulnerabilities [1]. It is an authorized simulation on cyber-attack on a computer system and to perform evaluation on a computer system. Penetration testing can involve in attempting breaching of the computer system such as system protocol, application protocol interfaces, servers, databases by any methods which possible to attack and damage the system [2]. Penetration testing is needed for an organization to minimize any possibilities being attacked by cyber criminals. Due to the rapid growth of technology, continuous in reviewing the penetration testing methodologies and standards to ensure the existing methodologies still relevance to the current technology trend and able to detect any cyber-attack methods which can harm to the system.

* *Corresponding author. tan.hua@graduate.utm.my*

2. Literature Review

2.1 Overview of Penetration Testing

Penetration testing is a lawful and authorized in hacking a computer system with detecting and exploit computer systems for the purpose of improving the computer systems to be more secure [3]. It is done by simulating as a potential cybercriminal in hacking the system by using different hacking tools and methods [4]. With the advancement of technology and different hacking methods, penetration testing is getting more important and crucial [5]. Organizations often engaged penetration testers as a mitigation plan to reduce the computer system is being hacked [6]. With the various penetration testing methods, the testing will involve simulation scenarios within the system and networks to identify the system vulnerabilities. Besides, with the penetration testing method, it can be used to produce valuable analysis and information on the potential security risks and perform risk assessment on the likelihood for cybercrime exploitation [7].

2.2 Benefits and Challenges in Penetration Testing

Evolving in cyber-attack techniques have created awareness to organizations, government agencies as well as businesses about the importance of implementing cyber security in protecting the assets [8]. As such penetration testing is a process of simulating cyber-attacks against the computer system, networking, application and website. The main objective of penetration testing is to identify possible vulnerabilities which existence in the current system so that the security controls can be implemented to eliminate possible risks before exploitation by cyber criminals.

Below are some of the benefits when an organization implementing penetration testing.

2.2.1.1 Discovering system vulnerabilities

Penetration testing able to reveal the weaknesses in the target system [9]. It allows the possibility of real cyber security risks to be identified whereby improvement at the software and hardware such as system architecture or network infrastructure can be considered to improve the overall security implementation. The assessment report from the penetration testing provides the overview of the system can be used in analysis for the overall security architecture of the system.

2.2.1.2 Test on the system cyber –defence capability

Since the penetration testing able to help in identifying the possible vulnerabilities and cyber-attack methods, thus once the attack incident happening, via the penetration testing, respond time and possible action plans applied to the attack can be estimated to reduce the potential damage and losses to organization [10]. Once the intrusion is detected, the experts will evaluate the effectiveness of the cyber security policy strategies to further determine if any action or improvement needed to mitigate the potential risk and cyber-attacks.

2.2.1.3 Ensure business continuity and customer trust

Sensitive data leakage could cause the organization reputation impacted and lost trust from the customers, stakeholders as well as employees in the organization. When the penetration testing is completed, the cyber security control can strengthen for any vulnerabilities that being identified, thus when if the cyber-attacks are strike in, the organization able to response fast to the incident to reduce the impact and losses from the cyber-attack.

Penetration testing has its challenges when adapting in order to securing the system [4].

2.2.2.1 Damage in assets

Penetration testing involves hacking on the computer system. It can be exposed the risk on leakage sensitive data and damages if the activity is not conducted properly. Server may crash, crucial data may be corrupted [9].

2.2.2.2 Difficulty in defining test scenarios

Penetration testing can be expensive and complex. Ideally, conducting a penetration test on the entire network and infrastructure with wider scope is the best approach. However, due to the advancement in technology and cyber-attack methods, determine the scope and test coverage with identified testing tools can be time consuming and may also involve more resources in carrying out testing tasks. Furthermore, the penetration testers have to equip with the appropriate testing skillsets to ensure each and every test scenarios are explored in all aspect in the target system [11].

2.2.2.3 Unethical Penetration Testing

Penetration testing is defined as ethical hacking [1]. The penetration tester will use the same technique that cyber criminals use to search the vulnerabilities in the system. The organization has to decide and accept the view of ethical implication from the testing. Besides, some organizations will consider outsourcing the activities to third party, thus it is important for the organization to engage a good reputation penetration tester to perform the testing in an ethical manner [12].

2.3 Vulnerability assessment method

Generally, to ensure a successful penetration test, there are several assessment phases need to be considered. The assessment is designed at the initial stage of a penetration test. In additional, the exploitation of any found vulnerabilities is a phase that is added to a penetration test to confirm their occurrence and to identify the potential damage that could occur as a result of the vulnerability being exploited and the associated impact on the organisation [13].

2.3.1 Planning

The penetration tester will work with the organization to define the objective and scope of the testing, tools and techniques to be used. At this phase, the community will work together to understand the business needs, technical details, identifying and assess security risks. The scope of the penetration testing can be defined at this phase and based on the requirement defined by the organization [9].

2.3.2 Reconnaissance

The penetration tester will collect as much as information related to the system such as application used, architecture design, technology platform, IP address, server, network information and any other related to the computer system. With the collected information the testers can easily identify vulnerabilities of a system [14][1].

2.3.3 Scanning

By using selected penetration tools and techniques, the tester will scan the networking and web application of the target system and discover vulnerabilities. In this phase the tester will perform two types of analysis. Static analysis is a process which to find out vulnerability from the code, detecting error, logic that being implemented in the system. The objective is to find out the weakness within the source code before running the application. For dynamic analysis, the test is performed during the application execution. The objective is to find out error and performance in a running application [1].

2.3.4 Gaining Access

This step will use various types of web application attack to discover vulnerabilities from the target system such as an application, firewall or a server. The tester will try to exploit the identified vulnerabilities and gain access to the target system for accessing the data and disturbing the system traffic.

2.3.5 Maintaining Access

After gaining access stage, the penetration tester will need to ensure system access still remained accessible, even the system has been reset or changed. This is because the real cyber criminals who attack the system will remain access the system for long periods to steal the information from the target system.

2.3.6 Exploitation

In this phase, once the vulnerabilities have been identified, the tester will proceed to exploit the system by access the data and damage the system by using different techniques and tools [1].

2.3.7 Evidence collection and reporting

After all the phases are done, the exploited vulnerability evidence will be consolidated and reported for the organization review and mitigation plan. The management team will be based on the reporting to make decision on how to manage and access the risks in order to reduce the risk which will harm the organization assets.

2.4 Penetration testing methods

The results of the penetration tests can vary depending on which testing methods are used. Organizations are searching for most suitable and relevant penetration testing method to combat new forms of cyber-attacks while also looking solutions in securing the computer system and fixing vulnerabilities [15]. There are several penetration testing methodologies and standards have been discussed and evaluated [16].

2.4.1 External Penetration Testing

External penetration testing is a method of evaluating an organization's assets that are exposed to the outside the organization. During an external penetration test, the penetration tester uses vulnerabilities discovered on external assets to try to break into the internal network [17]. Alternatively, the tester could try to get access to sensitive data via external assets such as email, websites, and social media.

The attacker conducts reconnaissance on the in-scope assets during the test, obtaining intelligence on all assets in scope. For password attacks, this intelligence comprises exposed ports, vulnerabilities, and general knowledge about the organization's users. Once the perimeter has been successfully broken, the exterior penetration test's objectives have been met, and the tester moves on to the internal penetration test.

2.4.2 Internal Penetration Testing

Internal penetration testing helps in the assessment by determining how far an attacker can travel laterally through a network following external attacks. The testing is conducted within the organization’s network.

During an internal penetration test, the tester will either use the exploited test environment from an external penetration test or do the assessment using a testing box or laptop on the internal network [17]. The testing will mirror an attack on the internal network by using the access rights from authorized employees or visitors. The preferable technique is to use a testing box or laptop, as this provides a more stable testing method than running tools over the attacked external asset.

This method frequently involves exploiting less-critical systems and then using the knowledge obtained from these systems to attack the network's more essential systems. The test is normally ended once the attacker has gained domain admin access or control over the organization's most valuable information.

2.4.3 Blind and Double-Blind Penetration Testing

A blind penetration test method mimics the methods of a real cyber attacker. This is accomplished by giving the penetration tester with extremely limited information or no information prior to the test procedure such as only website URL or company name [18]. The tester has to guess most of the test scenarios or based on general information to exploit to the system. Blind penetration testing can reveal a lot of unnoticed information about an organization such as internet access points, network connections and confidential information.

Double blind method is an extension of blind testing, which the only different is only a few employees such as security officer or project manager of the testing in the organization are aware to the testing activity [18]. This method is very crucial to measure and evaluate the effectiveness of the procedures for the organization response to the incidents during the testing.

However, this method is more time consuming and costly due to a lot of effort required to investigate the vulnerabilities with limited information.

2.4.4 Targeted Penetration Testing

Targeted testing combines both the organization's IT personnel and the penetration testing team to conduct the test. There is an understanding of the testing operations as well as knowledge on the aim and network design [19]. When the test's goal is to focus on the technical setting or network design rather than the organization's incident response and other operational procedures, a targeted test method may be more efficient and cost-effective. However, the testing may not provide a detailed view of the organization's security vulnerabilities and incident response capability.

3. Research Methodology

Research methodology is the techniques used to identify select, process and analyse the information about a research topic.

3.1 Design

The research method used in preparing this article is based on literature review which the sources of literature are mainly from published academic papers and official website from the defined topic. Penetration testing is widely discussed and there are numbers of studies are available from academic portals in the recent years, hence the target of research papers has been scope between years 2004 to 2020.

3.2 Data Collection

The information gathering from each literature was based on below assumptions:

i. Sources from academic portal such as: Emerald, Science Direct, ResearchGate, IEEExplore, Google Scholar which the articles are written in English and published.
ii. Article, papers, journal search keywords: Penetration testing, Security Testing, Penetration Testing Method, Ethical hacking from relevant articles or studies
iii. Classification of the study type such as discussion on the methods used based on the paper title, abstracts and introduction.
iv. Articles and papers focus on the discussed on penetration testing as in overview, benefits and challenges in penetration testing adoption in an organization, methodologies and methods used in penetration testing information.

3.3 Data Analysis

Based on the collected literature journals, articles or papers, the collected data is stored into a reference manager tool called Mendeley. Furthermore, a dedicated library and sub-libraries are created to store the downloaded data based on the categories which easier to insert into the paper writing.

4. Result and Discussion

The main objective in this paper is to identify the best penetration testing method for an organization in implementing and improving cyber security.

Based on literature review [4][5][8][18][20][21] generally penetration testing methods and vulnerability assessment are complex in nature due to the penetration testers have to design test specification to find the vulnerability in the system. The vulnerability assessment methods can be categorised to three main testing phases which are test preparation phase, test phases and test analysis phase (Table 1) (Figure 1) [2][16] [14] [15][11] [22].

Table 1. Vulnerability Assessment and process

Vulnerability Assessment	Details Process
Test Preparation Phase	Planning
Test Phase	Reconnaissance Scanning Gaining Access Maintain Access Exploitation
Test Analysis Phase	Evidence collection Reporting

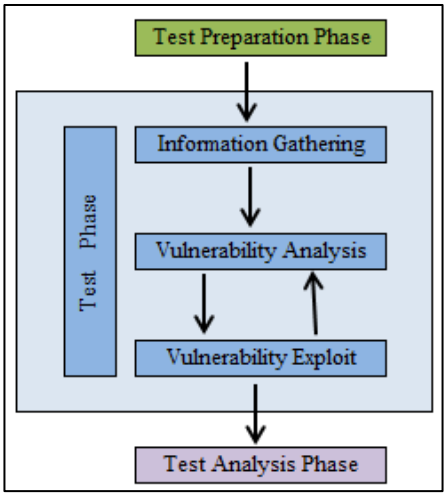

Figure 1. Vulnerability Assessment method

Based on one of the methods evaluations done in paper [7][11][16][18][23], the discussed penetration testing methods and assessment methods can be compared in the below based on the classification (Table 2).

Table 2. Comparison between vulnerability assessment method and Penetration Testing methods

Vulnerability assessment method	Penetration testing method
This is the process of discovering and assessing a system's vulnerability.	To identify vulnerabilities and exploits them to attack over the system.
To discover and scanning vulnerabilities.	To simulating vulnerabilities.
Lower cost due to only follow the defined process to discover vulnerabilities.	Higher cost due to need to identify vulnerability in the system, and most of the time with limited information and need qualified skillset penetration testers
Can be performed by internal employees.	Qualified skillset penetration testers
When there is any new/changes to the networking equipment is deployed.	Minimum once a year.
Limited details about the vulnerabilities as the report only focus on the vulnerability and risk assessment at the organization level.	Comprehensive details reporting of vulnerabilities as the report has to include all the information how are the identified vulnerability could harm to the system and recommendation on preventing the attacks.

Information security threats are not fix. Furthermore, based on the advancement in technologies and emerging in various different type of system hacking methods, there is a need to consistently to review and monitoring the existing adopted penetration testing methods to ensure the efficiency and effectiveness of the penetration testing processes still relevant to the organization mission in reducing and mitigating cyber threats.

A vulnerability assessment is less intrusive than a penetration test and does not always involve the same technical skills. Unfortunately, conducting such a thorough review that ensures the most dangerous vulnerabilities (i.e., high risk) are found may be unfeasible [2][24].

In the penetration testing profession, the difference between a penetration test and a vulnerability assessment is becoming increasingly important. Many penetration testers claim to be penetration testers but are merely capable of completing vulnerability assessments. If a corporation is unfamiliar with the process, it may believe that a networked system has been thoroughly evaluated when it has not [14][17].

Even though, there are plenty of methods in penetration testing, as long as the adopted method is aligned and agreed with the business requirement prior to kick start the testing and consider the best approach of these requirements can be met [4].

5. Conclusion

As the technology has emerged rapidly in various industries, penetration testing methods and standard have to be always being reviewed and strengthen with align to the organization cyber security objectives. This also to ensure the methods are always updated with the latest technologies and potential cyber attack methods and tools. By doing so, the penetration testing methods able to provide clear benchmark to assess the cyber security level of the organization and also to avoid the potential cyber attacks from cyber criminals. Thus, established and adoption to a set of effective and updated penetration testing method and standard is a must to ensure the scope of testing and the coverage of the penetration testing scenarios can be maximized. Besides, based on the testing result and finding, the organization able to make a decision based on the report analysis of the possible vulnerabilities to improve the cyber security level of the organization.

Acknowledgement

I would like to thank Universiti Teknologi Malaysia (UTM) for support in getting the journal while conducting the research. Financial support number FRGS R.K130000.7856.5F502.

References

[1] P. Engebretson, *The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy*. 2011.

[2] D. T.Pandikumar and T. Eshetu, “Detecting Web Application Vulnerability using Dynamic Analysis with Penetration Testing,” no. 6, pp. 1–8, 2016, [Online]. Available: https://www.westernsydney.edu.au/__data/assets/pdf_file/0006/1254786/Literature_review_purpose.pdf.

[3] H. Singh, J. Singh, and P. Tester, “Analysis of Various tools of Penetration Testing,” pp. 1184–1195.

[4] J. Creasey, “A guide for running an effective Penetration Testing programme,” *Crest*, no. April, pp. 1–64, 2017, [Online]. Available: https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf.

[5] B.-T. B. C. Aileen G. Bacudio, Xiaohong Yuan and M. Jones, “An overview of penetration testing,” *Int. J. Digit. Crime Forensics*, vol. 6, no. 4, pp. 50–74, 2011, doi: 10.4018/ijdcf.2014100104.

[6] A. Shanley, “Penetration Testing Frameworks and Methodologies: A comparison and evaluation,” *Grants Regist. 2021*, vol. 2015, pp. 344–345, 2015, doi: 10.1057/978-1-349-95988-4_335.

[7] NIST 800-115, “Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology,” *Nist Spec. Publ.*, vol. 800, pp. 1–80, 2008, [Online]. Available: http://books.google.com/books?hl=en&lr=&id=EHrf6q7GobUC&oi=fnd&pg=PR7&dq=Technical+Guide+to+Information+Security+Testing+and+Assessment+Recommendations+of+the+National+Institute+of+Standards+and+Technology&ots=FTcnroLXL8&sig=DE.

[8] J. N. Goel and B. M. Mehtre, “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology,” *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015, doi: 10.1016/j.procs.2015.07.458.

[9] A. Tewai, “Evaluation and Taxonomy of Penetration Testing,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 3, no. 8, pp. 5297–5302, 2015.

[10] P. Kesharwani, S. S. Pandey, V. Dixit, and L. K. Tiwari, "A study on Penetration Testing Using Metasploit Framework," *Cent. Comput. Sci. Ewing Christ. Coll. Pray.*, vol. 5, no. 12, pp. 193–200, 2018.
[11] S.-P. Oriyano, "Information System Security Assessment Framework (ISSAF)," *CEH™v9*, pp. 549–564, 2017, doi: 10.1002/9781119419303.app2.
[12] A. G. J. and M. J. W. Justin D. Pierce1, "PENETRATION TESTING PROFESSIONAL ETHICS: A CONCEPTUAL MODEL AND TAXONOMY," vol. 16, no. 2, pp. 1321–1323, 2006.
[13] F. A. A and F. S. Y, "Methodology for penetration testing," *Int. J.* , vol. 2, no. 2, pp. 43–50, 2009, [Online]. Available: http://www.earticle.net/Article.aspx?sn=147732.
[14] C. T. Phong, "A Study of Penetration Testing tools and Approaches," *Comput. Fraud Secur. Bull.*, vol. 2, no. 5, pp. 10–11, 2016, [Online]. Available: http://aut.researchgateway.ac.nz/bitstream/handle/10292/7801/ChiemTP.pdf?sequence=3&isAllowed=y.
[15] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *J. Brazilian Comput. Soc.*, vol. 23, no. 1, pp. 1–16, 2017, doi: 10.1186/s13173-017-0051-1.
[16] A. Shanley and M. N. Johnstone, "Selection of penetration testing methodologies: A comparison and evaluation," *Aust. Inf. Secur. Manag. Conf. AISM 2015*, vol. 2015, pp. 65–72, 2015, doi: 10.4225/75/57b69c4ed938d.
[17] G. Kaur, G. Kaur, and K. Maha Vidyalaya, "Penetration Testing: Attacking Oneself to Enhance Security," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 5, no. 4, pp. 574–577, 2016, doi: 10.17148/IJARCCE.2016.54141.
[18] K. Božić, N. Penevski, and S. Adamović, "Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods," no. January, pp. 229–234, 2019, doi: 10.15308/sinteza-2019-229-234.
[19] K. B. Chowdappa, S. S. Lakshmi, and P. N. V. S. Pavan Kumar, "Ethical Hacking Techniques with Penetration Testing," *K.Bala Chowdappa al, / Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 3389–3393, 2014.
[20] S. M, S. M, S. CHAKRABORTY, and W. HASAN, "A Comparative Overview on Penetration Testing," no. October, pp. 25–28, 2015, doi: 10.15224/978-1-63248-069-9-17.
[21] R. Budiarto, S. Ramadass, A. Samsudin, and S. Noor, "Development of penetration testing model for increasing network security," *Proc. - 2004 Int. Conf. Inf. Commun. Technol. From Theory to Appl. ICTTA 2004*, no. March 2014, pp. 563–564, 2004, doi: 10.1109/ictta.2004.1307886.
[22] A. S. Al-Ahmad, H. Kahtan, F. Hujainah, and H. A. Jalab, "Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications," *IEEE Access*, vol. 7, pp. 173524–173540, 2019, doi: 10.1109/ACCESS.2019.2956770.
[23] S. UMRAO, M. KAUR, and G. K. GUPTA, "Vulnerability Assessment and Penetration Testing," *Int. J. Comput. Commun. Technol.*, vol. 7, no. 3, pp. 200–203, 2016, doi: 10.47893/ijcct.2016.1367.
[24] T. Dimkov, A. Van Cleeff, W. Pieters, and P. Hartel, "Two methodologies for physical penetration testing using social engineering," *Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC*, no. January, pp. 399–408, 2010, doi: 10.1145/1920261.1920319.