International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 18 (2015) pp 39290-39293

A study on Penetration testing methodology

Yong-Suk Kang[1],Hee-Hoon Cho[2],Yongtae Shin[3]and Jong-Bae Kim[4*]

[1]Dept.of IT Policy and Mgmt., Graduate School of Soongsil Univ., Seoul 156-743, Korea
[2,4]Graduate School of Software, Soongsil Univ., Seoul 156-743, Korea*
[3]Dept. of Computer Science, Soongsil Univ., Seoul 156-743, Korea
E-mail:[1]postwin@gmail.com,[2]heehoonc@naver.com,[3]shin@ssu.ac.kr,[4]kjb123@ssu.ac.kr*
[4]Jong-Bae Kim (kjb123@ssu.ac.kr) is the corresponding author of this paper.*

Abstract
In recent years, information technology has been progressing rapidly. Yet as the technology has progressed, the threats and risks have also evolved quickly. In order to respond to this problem, enterprises and institutes are conducting Penetration Tests (Pen-Test) as one of the methods to strengthen security. Penetration tests have been performed under the same terms as simulated penetration tests after legal approval, or simulated hacking tests. In this test, the weak points of an invaded system are found, and then based on the test results the security of the system is actively evaluated and further strengthened. When the reliability and the test strength are not properly evaluated in the penetration test, it is difficult to receive a proper evaluation of the performance results for security improvement and thus it is not possible to say that the test has been conducted properly. With this in mind, the objective of this research is to propose the criteria for selecting the methodology of a penetration test, by investigating and comparing existing penetration test methodologies.

Keywords: System Security, Penetration Test, Methodology

1 Introduction

With the development of IT devices and networks, the operation of information systems has become more significant. As a result, there has been a rise in direct and indirect security breaches, such as external intrusions, malicious codes, and information leakage [1]. In recent security accidents, the trend of security weaknesses and threats to conventional and new business models has rapidly changed, and attack techniques have become more diverse and sophisticated. To respond, enterprises and institutes must regularly and constantly perform penetration tests. A Penetration Test(PenTest) is a trial that aims to identify the security vulnerabilities of a computer system by intentionally attacking the system after legal approval, in order to manage the computer system more safely. This is different from a "weakness diagnosis," which aims to review services and systems to find potential security problems. A penetration test is also known as simulated penetration testing and a simulated hacking test. As a way of evaluating the information security level of enterprises and institutes, it is executed from an actual attacker's position, and a person who performs a penetration test is called a Penetration Tester or a Pen Tester [2]. A critical aspect of a penetration test is selecting a penetration test method and tool suitable to the circumstances and purposes of enterprises and institutes. Many security companies apply various methods and procedures to execute penetration tests. However, the tests fail to accurately evaluate robustness and reliability. For this reason, it is necessary to research approved and reliable methodologies for penetration tests [3][10]. This study looked into each penetration test phase and conducted a comparative analysis on the methodologies used for penetration tests.

2Related Works

Penetration testing was first attempted by a security expert in the 1960s. In the 1990s, the Tiger Team was established, and expert groups began to execute penetration tests. In particular, the United State Air Force (USAF) signed a contract with James Anderson to test its Time-Sharing system. In the 1980s to 1990s, more attention was being paid to security systems.As a result, special books on security, such as “Improving the Security of Your Site by Breaking Into it” and “Hacking Exposed” began to be published. The main purpose of penetration testing is to confirm various potential security risks from an attacker's position and an insider's position. In other words, the aims are to perform a penetration test on critical information systems and services; to diagnose technical security weaknesses; and to come up with effective improvement plans to ensure the security and safety of information systems. Information protection encompasses the technical area, the management area, and the physical area, which are connected with one another systematically. Therefore, each item for information protection needs to be taken into account for regular security inspection, which ensures that handling information is safe. In this regard, regular penetration testing is capable of measuring confidentiality, integrity, and availability numerically and prioritizing actual risks. With the testing, it is possible to actively assess security process design issues, technical obstacles and weaknesses. In addition, such a test can be used for a variety of forms of security management, such as management of weaknesses, settings and accidents, management of web applications and DBMS, and

management of wired and wireless networks. Penetration testing areas include all IT assets. Penetration testing can be categorized into such areas as Network, System, Security, Application, and others. The penetration testing process consists of nine phases, and penetration tests can be categorized into six types [4].

3Types of penetration testing

3.1 Open Source Security Testing Methodology Manual

OSSTMM includes penetration testing methodologies and aims to achieve improvements in corporate security strategies and quality, and can be applied to almost all inspection types, including penetration testing, ethical hacking, security assessment, and vulnerability inspection [5].The OSSTMM consists of test modules for each area, as shown in Figure1.

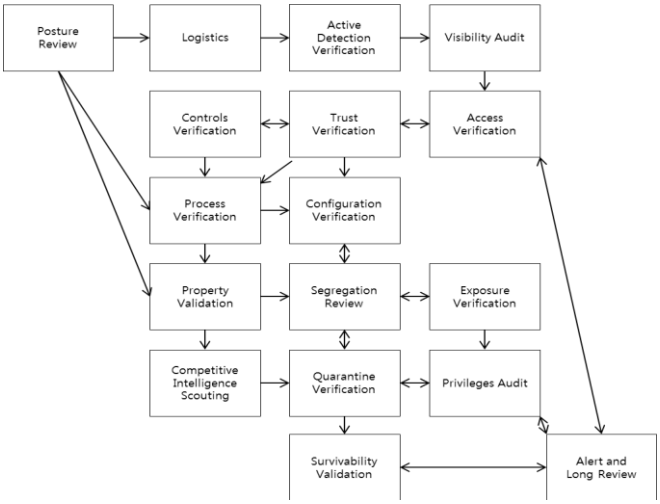

Fig 1. OSSTMM Methodology Test Module

3.2 Open Web Application Security Project

In 2008, OWASP Testing Guide V3 was released. V4 Project is being reviewed. The Testing Guide is used to investigate appropriate technologies and works, which can be performed in various phases of the Software Development Life Cycle (SDLC), in the framework unit, and provides a general development model and concrete guidelines that need to be followed according to process [6][7].Figure2 illustrates the OWASP Security Threat Route. Test items include information gathering, configuration management, authentication, session management, rights offering, business logic, data validation, Oracle test, and MySQL test [8].

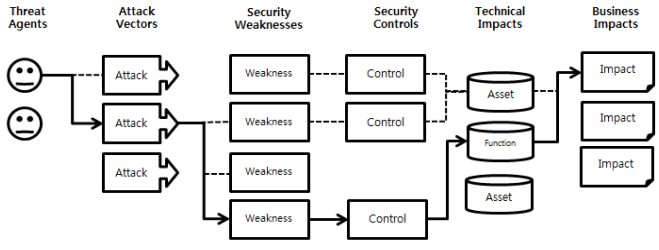

Fig.2.OWASP Security Threat Route

The OWASP Testing Guide is designed as a type of framework for testing web applications. The framework includes web application testing methods based on a Black box approach.

3.3 Information System Security Assessment Framework

ISSFS is designed in a structured framework type to assess various information systems as shown in Figure3. It suggests the assessment and testing standards for each domain, and has a security assessment that reflects actual scenarios. In terms of the assessment standards, each domain was reviewed by relevant experts. It is considered that they will be used as the criteria to meet security requirements. The assessment standards consist of purpose and objective, prerequisites for assessment, processes for assessment, information on expected results, recommended measures, and reference to external documents [9]. The aim of the Open Information Systems Security Group is to enumerate security assessment issues and provide security assessment standards based on the framework to achieve perfect, accurate, and efficient security assessment with the least effort. The framework consists of planning, assessment, processing, approval, and maintenance, and also includes risk assessments of general security, network security, application security, and database security, security policies, and penetration testing methodologies. ISSAF methodology is divided into penetration testing procedures and penetration testing methods.

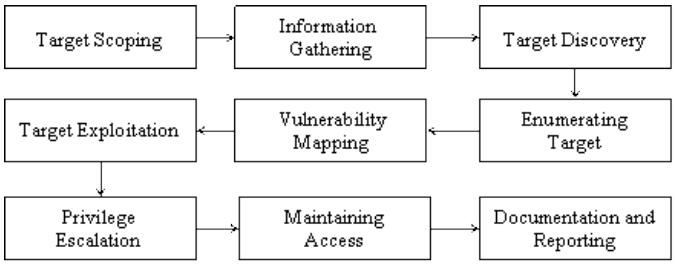

Fig.3. OISSG Pen Testing Methodology

3.4RSA

Through the penetration testing assessment, RSA classifies security into five levels: Critical, High, Medium, Low, and Informational. Since the security levels are determined with the calculated points of methodology, realism, and reporting & output, it suggests a maturity model.Based on the Table1, it is possible to find a simple penetration testing maturity model. In the methodology category of the maturity model, it is possible to assess the use, approach possibility, and potential vulnerability of a methodology; and in the reporting & output category, it is possible to judge how valuable penetration testing is and how much those concerned use the testing. In addition, by determining that the attacks in penetration testing can actually occur, it is possible to assess and judge security threats in penetration and various attack techniques. However, such assessment and judgment is very subjective, and can be changed depending on the Pen Tester or a tool.

Table 1.RSA Penetration Test Assessment

Methodology		Realism		Reporting/Output	
Does a stated methodology exist?	Y	Is a "Black box" approach taken?	Y	Is the report customized with remediation guidance suitable to the organization?	N
Is all major phase of testing incorporated, from Reconnaissance to Exploitation?	Y	Were efforts made to avoid detection?	Y	Are all false positives removed from the report?	N
Are both manual testing and automated tools involved?	Y	Was "malware" dropped or Emulated on some way?	N	Are result put in industry/vertical context?	Y
Is actual exploitation allowed?	Y	Was Social engineering involved/included?	Y	Are vulnerabilities assessed for contextual risk?	N
Is Prove from on compromised system to another permitted?	Y	Was data exfiltrated?	Y	Are the tests described in enough detail to be repeatable?	N
Methodology Score	5	Realism Score	4	Reporting/Output Score	1

5 Conclusions

Table 2. Comparative Analysis

Penetration Testing Methodologies	Testing Phases of Methodology	Features
OSSTMM	6 phases	Applicable to most inspection types
OWASP	9 phases	Suggests a model and guidelines that can be applied in various phases of SDLC
ISSFS	9 phases	Making security assessment of actual scenarios
RSA	5 phases	Possible to derive various results of penetration through a maturity model

Each of the penetration testing methodologies is presented in the above Table 2. OSSTMM can be applied to a wide range of inspections, including penetration testing, ethical hacking, security assessment, and vulnerability analysis. OWASP has the test framework for web applications established. ISSFS is designed in a structured framework type to assess various information systems, suggests the assessment and testing standards of each domain, and performs security assessment that reflects actual scenarios. RSA determines security levels on basis of the points calculated, suggests a maturity model with them, and thus helps to realize the influence of outputs. Given all of this, it is important to apply a penetration testing methodology suitable to each enterprise and institute in order to achieve the maximum efficiency.With the development of networks and technologies, various weaknesses have been found in systems. As a result, attacks on the systems have been diversified, leading to severe security accidents. As a way of responding to them, vulnerability analysis is performed, and various penetration tests are conducted on possible vulnerabilities. Penetration testing helps to identify security process problems, and actively assess design problems and technical obstacles and weaknesses. Therefore, by finding and testing dubious and weak points, it is possible to enhance the overall security awareness and check security system components and new technologies. Although attack patterns are becoming more intelligent and diversified, developers and project managers still have poor security development and awareness. As a result, despite the fact that security weaknesses are found through penetration testing, they seem to consider their systems as normal. Information protection encompasses the technical area, the management area, and the physical area, and these are systematically connected with one another. Therefore, by measuring confidentiality, integrity, and availability numerically and prioritizing real risks, it is possible to accomplish efficient security operation and management. Overseas,trustworthy and well-designed penetration testing methodologies are being applied to achieve reliable penetration testing and assessment of overall information security or web applications.Based on the comprehensive testing methodology, a penetration test is planned and executed according to the system or software development life cycle. If the guidelines and system for penetration testing methodologies are created after the weaknesses in each specific area and product are analyzed and penetration testing methods are listed, it is expected to that more reliable assessment results can be produced through efficient penetration tests.

References

[1] Ji Yeon Hong, Ik Jun Kang, Seong Baeg Kim and Chan Jung Park.,"Development of Information Security Contents for Learning Hacking Principles",International Journal of Security and Its Applications,7, 6, (2013), 137-146.

[2] Selcuk Levent, Gökce H Suleyman, Kayabali Kamil, Simsek Osman,"A Nondestructive Testing Technique: Nail Penetration Test", ACI Structural Journal, 109, 2 , (2012), 245-252.

[3] Farkhod Alisherov A.,Feruza Sattarova Y., "Methodology for Penetration Testing" International Journal of Grid and Distributed Computing, 2, 2, (2009), 43-50.

[4] Pete Herzog, "OSSTMM 3 LITE", ISECOM, (2008) http://www.delmarlearning.com/companions/content/1435486099/osstmm/OSSTMM_3.0_LITE.pdf

[5] Pate Herzog,"OSSTMM 2.1., Open-Source Security Testing Methodology Manual", ISECOM, (2003) http://isecom.securenetltd.com/osstmm.en.2.1.pdf

[6] Matteo Meucci, "OWASP Testing Guide V3.0", OWASP, (2008) https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[7] Khairul Anwar Sedek, Norlis Osman, Mohd Nizam Osman, Hj. Kamaruzaman Jusoff,"Developing a Secure Web Application Using OWASP Guidelines", CCSE, 2, 4, (2009), 137-143.

[8] Dave Wichers,"OWASP Top 10-2010", The OWASP Foundation, (2010) https://www.owasp.org/images/6/67/OWASP_AppSec_Research_2010_OWASP_Top_10_by_Wichers.pdf

[9] Balwant Rathore, "Information Systems Security Assessment Framework (ISSAF) Draft", OISSG, (2006) http://cs.uccs.edu/~cs591/penetrateTest/issaf0.1.pdf

[10] Yong-Suk Kang, Hee-Hoon Cho, Yongtae Shin and Jong-Bae Kim,"Comparative Study of Penetration Test Methods", Proc. of ASTL, 38, (2015), 34-37.

Received: Month xx, 20xx