모의 침투 테스트 방법 및 절차의 평가 방법에 관한 연구

강용석* · 최국현** · 신용태*** · 김종희**** · 김종배*****

*,**,***,****,***** 숭실대학교

A Study on the Evaluation Method for Penetration Test Method and Procedures

Yong-Suk Kang* · Yong-Tae Shin** · Jong-Hee Kim*** · Yong-Tae Shin**** · Jong-Bae Kim*****

*,**,***,****,***** Soongsil University

E-mail : *postwin@gmail.com, **khchoi@tsline.co.kr, ***shin@ssu.ac.kr, ****skyimo@hanmail.net, ***** kjb123@ssu.ac.kr

요 약

최근 보안 위협과 위험이 매우 빠른 속도로 변화하고 있어, 다각화 되는 공격기법에 대응하기 위한 필수 조건으로 기업 및 기관에서 모의 침투 테스트를 진행하고 있다. 침투 테스트(Penetration Test, PenTest)는 합법적이고 승인된 시도로 컴퓨터 시스템을 더 안전하게 하기 위해 시스템의 취약점을 찾아내고, 찾아낸 취약점에 대해 공격을 시도하는 것이다. 모의 해킹 테스트와 같은 용어로 사용되고 있으며 취약점이 어떻게 악용될 수 있는지 공격을 시도하여 보여준다. 한편, 현재 많은 보안 업체에서 다양한 방법 및 절차로 침투 테스트를 수행하고 있으나, 실제로 이러한 테스트의 강도와 신뢰성에 대한 평가는 아직 이루어지지 않고 있다. 따라서, 본 연구에서는 이와 같은 침투 테스트에 대하여 검증되고 신뢰할 수 있는 평가 방법을 제시한다. 본 연구에서 제시한 침투 테스트 평가 정보를 활용하여 보다 신뢰할 수 있는 평가 결과를 얻을 수 있고, 결과적으로 효율적인 침투 테스트가 가능할 것으로 기대된다.

ABSTRACT

Latest Inforamtion security threats and risks change very rapidly, and there to strengthen the security level of the major companies and organizations are diversified attack to respond to a penetration test conducted. Penetration test(PenTest) is safer for the purpose of looking for vulnerabilities in computer systems by taking advantage of vulnerabilities discovered in the same way as a hacker attack. How to make a security vulnerability could be exploited by attempting to attack show. On the other hand, many security companies are testing in a variety of ways to be penetrated. However, penetration testing to evaluate the strength and reliability has not performed yet. Therefore, in this study, Penetration testing to validate and present a reliable method of evaluation. In this study, penetration testing, assessment information to provide the evaluation results are more reliable. And, as a result, efficient penetration test is expected to be possible.

키워드

보안, 모의 침투 테스트, 취약점, 해킹, 평가

Ⅰ. 서 론

IT 기기 및 네트워크 발달로 정보시스템의 운영에 대한 비중이 높아짐에 따라, 직·간접적으로 외부침입행위, 악성코드, 정보유출 등의 보안 사고들이 증가하고 있다. 최근 발생된 보안 사고들

을 살펴보면, 기존/신규 비즈니스 모델의 보안 취약점 및 보안 위협에 대한 트렌드가 매우 빠른 속도로 변화되고 있으며, 다양하고 정교해진 공격 기법이 사용되고 있다는 것을 알 수 있다. 이를 대응하기 위해 기업 및 기관 에서는 주기적이고, 지속적으로 침투 테스트를 진행하고 있다.

침투 테스트(Penetration Test, PenTest)는 컴퓨터 시스템을 더욱 안전하게 관리하기 위해 합법적인 승인 후, 시스템에 대한 취약점을 찾아내고, 발견된 취약점에 대해 의도적으로 공격을 시도하는 것을 말한다[1].

본 연구에서는 각 침투 테스트 단계를 살펴보고, 현재 침투 테스트를 위해서 사용되고 있는 방법에 대해 간략히 소개하고자 한다.

II. 관련 연구

1. 침투테스트 연역

침투 테스트는 1960년대에 보안 전문가에 의해 처음 시도되었으며 1990년대에는 Tiger Team이 결성되어 침투 테스트를 수행하기 위한 전문 그룹이 나타났다. 특히, 미공군(USAF : United State Air Force)에서는 James Anderson과 계약하여 Time-Sharing system에 대한 테스트를 수행했었다. 전체적인 보안 시스템으로 초점이 맞춰진 것은 1980-1990년대이며 “Improving the Security of Your Site by Breaking Into it”와 “Hacking Exposed” 등 전문 서적들이 출판되기 시작했다[2].

2. 침투테스트의 목적

침투테스트는 공격자의 입장 또는 내부자의 입장에서 보안 위험이 실현화 될 수 있는 다양한 가능성들을 입증하는 것이 주된 목적이다. 즉 중요 정보 시스템 및 서비스를 대상으로 침투 테스트를 수행하여, 기술적 보안 취약성 진단을 실시하고, 이에 대한 효과적인 개선방안을 마련함으로써 정보 시스템들의 보안성과 안전성을 확보하는데 있다.

3. 침투테스트 프로세스

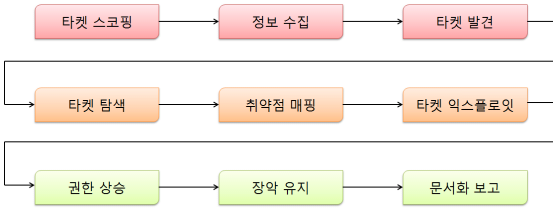
침투 테스트 프로세스는 다음과 같은 9개의 과정으로 설명할 수 있다[3].

1) 타켓 스코핑

타켓 네트워크 환경의 범위를 관찰하고 이해하는 단계로 감시자에게 주어진 네트워크의 entity 수에 따라 무엇을, 어떻게, 어떤 조건 하에 테스트를 할 것인지 테스트 가능한 수준과 얼마만큼의 시간이 소요되는지 비즈니스의 목표를 결정한다.

2) 정보 수집

다양한 공개 리소스를 통해 정보를 수집하는 단계이다. 주로 포럼, 게시판, 뉴스그룹, 기사, 블로그, SNS, 상업/비상업 사이트에서 수집하며 자동화된 툴을 이용하여 DNS 서버, whois, 이메일 주소, 전화번호, 개인정보 등으로 정보 수집할 수 있다.



(그림 1) 침투 테스트 프로세스

3) 타켓 발견

타켓의 네트워크 상태, 운영체제, 네트워크 구조를 파악하는 단계이다.

4) 타켓 탐색

정보 수집과 타켓 발견 단계에서 얻게 된 자료를 조합하여 타켓 시스템의 취약점을 검색하는 단계로 Web/Port Scan, 운영체제 버전, 어플리케이션 버전 등을 검색한다. 기업에서는 특정 서버에 대해서 침투 테스트를 승인할 경우, 1),2)과정이 생략될 수 있고 3)단계는 구조 파악 작업이 간소, 생략될 수 있다.

5) 취약점 매핑

타켓 탐색을 통해 알게 된 포트 번호, 버전 정보를 이용하여 취약점 검색하는 단계이다.

6) 타켓 익스플로잇

발견한 취약점을 살펴보고 exploit 공격을 통해 침투하는 단계로 SQL Injection, XSS, BOF 방법 등이 있다.

7) 권한 상승

공격에 성공하여 root 권한을 획득하거나 사용권한을 상승시키는 단계이다.

8) 장악 유지

타켓 시스템을 장악한 단계로 장악을 유지할 경우 전 단계를 다시 할 필요가 없으며, 시스템에 항상 가동되는 프로세스로 백도어, 마이그레이션

사용될 수 있다.

9) 문서화 보고

모든 단계의 진행 과정, 취약점 발견 및 검증 등 수행 결과를 발표하고 문서화하는 과정으로 관리자는 보완해야하는 보안 정책이 무엇이 있는지 파악하고 침투 테스트에 사용된 로그를 삭제해야 한다.

4. 침투테스트 유형

침투 테스트의 유형을 간단하게 정리하면 침투 테스트에는 White Box Test 내부에서 내부 환경 지식을 토대로 수행되는 테스트 시도, Black Box Test 외부 환경에서 수행되는 테스트 시도, Gray Box Test 2가지를 적절히 혼합하여 테스트하는 것으로 나누어지며 각 회사와 기관의 환경과 목적에 맞게끔 비용과 시간을 충분히 고려하여 테스트 수행 유형을 선택해야한다[4].

1) Blind Test

검사 대상에 대한 정보 없이 수행하며 수행 시에 미리 검사 대상에 통보하고 수행한다. 미리 통지한다는 윤리적 측면 때문에 많이 사용한다.

2) Double Blind Test (Black Box Test)

해당 검사는 Pen Tester도 정보를 알지 못하지만 검사 대상 역시 모의침투테스트를 진행한다는 사실을 알지 못하기 때문에 실제 환경에 가장 근접한 테스트이다. 다만, 짧은 시간 안에 결과를 도출하기가 어려우며 프로젝트 기간이 길어질 수 있기 때문에 비용 대비 성과를 충분히 고려하여 선택해야 한다.

3) Grey Box Test

Pen Tester가 제한적인 지식만을 제공받아 수행하는 테스트 형태이다. 예를 들면, 취약점 점검 결과를 넘겨받거나 실제 수행할 수 있는 기회만을 받는다. 해당 테스트 역시 모의해킹을 시작하기 전 검사 대상에게 미리 통보해야 한다.

4) Double Grey Box Test (White Box Test)

감사의 시간이 제한되어 있고 채널과 벡터는 테스트하지 않는 점에서 Grey Box Test와 다르다.

5) Tandem Test

Pen Tester가 모든 결과 값을 볼 수 있는 것이 핵심이다. 검사 대상 역시 테스트 수행 전에 통보를 받는다 .해킹이 가능한 취약점을 확인 할 수 있으며, 가장 이상적인 결과를 제출 할 수 있다.

6) Reversal Test

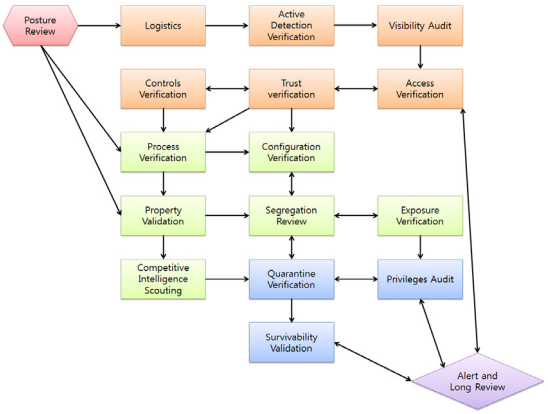
Pen Tester가 모든 정보를 알고 있지만 검사 대상은 검사가 실시된다는 사실을 모른다.

III. 침투테스트 방법론

1. Open Source Security Testing Methodology Manual(OSSTMM)

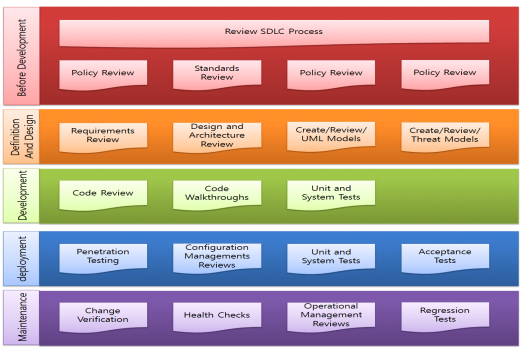
OSSTMM은 침투 테스트 방법론뿐만이 아니라 기업 보안 전략과 품질 향상에 집중되어 있으며 침투 시험, 윤리적 해킹, 보안 평가, 취약점 등 거의 모든 감사 유형에 적용될 수 있다[5].

OSSTMM 방법론은 각 분야에 대한 테스트 모듈 형태로 구성되어 있으며, 각 모듈은 작업 단위로 구성되어 있다.



(그림 2) OSSTMM 방법론 테스트 모듈

2. Open Web Application Security Project (OWASP)



(그림 3) OWASP 프레임워크 흐름

2008년 OWASP Testing Guide V3가 출시되었으며, 현재 V4 프로젝트는 검토 단계에 있다. Testing Guide는 소프트웨어 개발주기 (SDLC)의

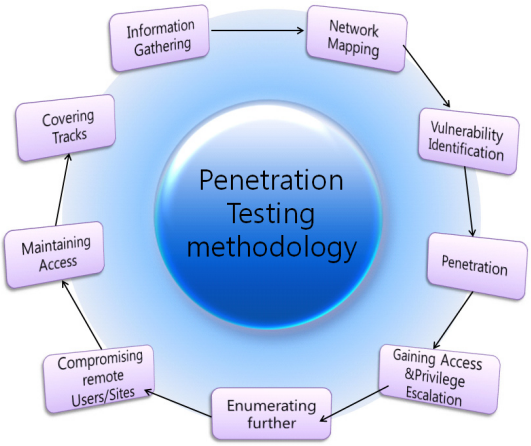
다양한 단계에서 수행될 수 있는 적절한 기술 및 작업들을 프레임워크 단위로 살펴 볼 수 있으며 일반적인 개발 모델을 제시하고 프로세스에 다라 준수해야 될 구체적인 지침들을 제공하고 있다 [6].

OWASP 테스트 항목으로는 정보 수집, 구성 관리, 인증, 세션 관리, 권한 부여, 비즈니스 논리, 데이터 유효성, 오라클 테스트, MySQL 테스트 등이 기술되어 있다.

3 Information Systems Security Assessment Framework(ISSAF)

ISSFS는 여러 정보 시스템의 평가를 위한 구조화된 프레임워크 형태로 구성되어 있으며 각 도메인에 대한 평가 및 시험 기준을 제시하고 실제 시나리오를 반영한 보안 평가에 대해 다루고 있다. 평가 기준은 도메인이 각 분야 전문가에 의해 검토되었으며 보안 요구 사항을 충족시키기 위한 기준으로 사용 가능할 것으로 생각된다[8].

ISSAF 방법론은 침투 테스트를 수행하는 과정에 대한 내용과 침투 테스트 방법에 대한 내용으로 나누어져 있다.



(그림 4) OISSG Pen Testing Methodology

Ⅳ. 결 론

네트워크와 기술의 발달과 함께 다양한 형태 취약점 발견되고 공격 방법이 다각화되어 심각한 보안 사고로 이어지고 있다. 최근에는 이러한 문제에 대응하기 위한 방법으로 취약점 분석을 실시하고 발생 가능한 취약점에 대해 다양한 침투 테스트가 이루어지고 있으며, 침투 테스트는 보안 프로세스 내 문제점을 검색하고, 설계 문제, 기술 장애 및 취약점을 능동적으로 평가할 수 있기 때문에 의심스러운 영역 및 취약점을 찾아 시험함으로써, 전반적인 보안 인식을 강화시키거나, 보안 시스템의 구성 또는 새로운 기술을 확인할 수 있다.

하지만 지능화되고 다각화되는 공격 패턴에 비해 개발자나 프로젝트 관리자 등 참여자들의 보안 개발 및 인식이 부족한 상태에서 수행된 침투 테스트의 평가 결과는 취약점이 존재하지만 정상인 것처럼 판단하는 사례가 발생할 수 있다.

국외의 경우, 신뢰할 수 있고 완성도 높은 침투 테스트방법론 정보를 활용하여 전반적인 정보보안 또는 웹 어플리케이션에 대해 보다 신뢰할 수 있는 침투 테스트 및 평가를 수행하고 있다.

반면, 국내에서는 이러한 지침 또는 평가 방법에 대한 연구가 부족하기 때문에 다양한 공격 방법과 취약점에 대응하기 위한 침투 테스트 시나리오 및 신뢰할 수 있는 침투 테스트 방법론에 대한 연구가 필요하다.

또한, 세분화된 분야 또는 제품군에 따른 취약점을 분석하고 침투 테스트 방법들을 목록화 하여 침투 테스트 방법론에 대한 지침 및 제도를 만든다면, 보다 신뢰할 수 있는 평가 결과를 얻을 수 있고, 효율적인 침투 테스트가 가능할 것으로 예상된다.

참고문헌

[1] wikipedia.org/wiki/Penetration_test
[2] Dave Shackleford, "A Penetration Testing Maturity and Scoring Model", RSACONFERENCE, 2014.
[3] http://www.metasploit.com
[4] Pete Herzog, "OSSTMM 3 LITE", ISECOM, 2008.
[5] Pate Herzog, "OSSTMM 2.1 Open-Source Security Testing Methodology Manual", ISECOM, 2003.
[6] Matteo Meucci, "OWASP Testing Guide V3.0", OWASP, 2008.
[7] 박형근, "OWASP Top 10 2010", SecurityPlus, 2010.
[8] Balwant Rathore, "Information Sstems Security
[9] Assessment Framewok(ISSAF) Draft 0,2,1", OISSG, 2006.