CC 기반 보안평가를 위한 침투방법론

강연희O*, 방영환*, 이강수**
(*) 한남대학교 컴퓨터공학과 ({dusi82O, bangyh}@se.hannam.ac.kr)
(**) 한남대학교 정보통신멀티미디어공학부 교수 (gslee@eve.hannam.ac.kr)

CC Based Penetration Testing Methodology for Security Evaluation

YeonHee KangO*, YoungHwan Bang*, GangSoo Lee**
(*)Dept. of Computer Engineering. HanNam University
(**)Dept. of Computer Science, HanNam University

요 약

정보의 불법적 유출 및 해킹 등과 같은 정보화 역기능을 해결하기 위해서 안전성과 신뢰성이 검증된 정보보호시스템을 사용하여 정보보호 수준 강화가 요구되고 있다. 우리나라를 비롯한 각국에서는 안전성과 신뢰성 평가를 위한 ITSEC, CC 등과 같은 평가기준들이 개발되어 평가를 시행중이며 이러한 평가기준들에 현존하는 보안위협에 정보보호시스템이 잘 대처하고 있는지를 평가하는 침투시험 항목이 공통적으로 존재한다. 본 논문에서는 정보보호시스템 개발자 및 평가자의 이해를 돕기 위하여 침투시험을 정의하고 침투시험을 이용한 평가방법론에 대하여 기술한다.

1. 서 론

오늘날 보안산업에서 조직들은 목표를 달성하기 위하여 정보시스템을 구축 및 운용하고 있다. 정보보호기능이 강화된 정보시스템을 "정보보호시스템"이라 하며 정보화 역기능을 해결하기 위해 정보보호시스템의 수요가 늘어가고 있다. 수요가 늘어감에 따라 정보보호시스템의 안전성과 신뢰성 검증이 요구되고 있으며 안전성과 신뢰성이 검증되어야 정보보호 수준 향상과 소비자도 믿고 제품을 구입할 수 있다.

하지만 주변의 방화벽 또는 필터링 된 내용과 안티 바이러스 보호 등의 보안 기술은 공격에 대한 비즈니스적 방어에 우수하지만 잠재적인 취약점이 존재할 수 있다. 또한 원격 네트워크 접근이 가능한 조직이 증가함에 따라 취약성 존재 및 내 · 외부적 침투자들이 존재하므로 조직에서 사용하고 있는 정보보호시스템에 대한 보안을 완벽히 테스트함으로서 비즈니스적 위험도를 낮춰야만 한다. 이에 취약평가와 보증을 위한 침투시험 평가방법이 유용하다. 침투시험은 지난 몇 해에 걸쳐 표준화되고 있으며 중요도와 사용성이 높아지고 있다[1][2].

본 논문에서는 정보보호 수준 향상과 신뢰성 있는 정보보호시스템 개발을 위해 침투시험을 이용한 평가방법론을 제시한다. 본 논문의 2장에서는 침투시험을 이용한 평가를 위해 침투시험을 정의하였으며 3장에서는 CC 기반 침투시험 평가방법론에 대하여 제시하였다. 4장에서는 3장에서 제시한 침투시험 평가방법론을 기반으로 TCSEC, ITSEC, CC 등의 평가기준별로 정의된 침투시험 요구사항에 대하여 보였으며 5장에서는 CC를 기준으로 침투시나리오 및 명세언어의 예를 제시하였다. 마지막으로 5장에서 결론을 맺는다.

2. 침투시험

"침투시험"이란 완성된 평가대상물이 개발시 의도했던 '요구사항 명세'(즉, 보안목표, 목적 및 정책)대로 평가대상물 내의 '대응 수단'들(즉, 보안강화 및 메커니즘)이 효과적으로 작동하는지의 여부 시험 및 취약점 색출을 위하여 시도하는 시험을 말한다. 침투가 성공했다는 표현은 인가되지 않은 사용자가 정보보호시스템내의 파일과 프로그램에 접근 또는 제어가 가능하다는 의미이다. 침투에는 외부 침투와 내부 침투로 분류할 수 있으며 외부 침투는 인가되지 않은 사용자의 시스템 접근이며 내부 침투는 인가된 사용자의 접근을 말한다. 표 1은 존재하는 위협에 대한 침투방법을 분류 한 것이며 그림 1은 내부 침투와 외부 침투를 표현한 것이다[3][9].

표 1. 존재하는 위협에 대한 침투방법 분류

	인가되지 않은 데이터/프로그램 지원 침투자	인가된 데이터/프로그램 지원 침투자
인가되지 않은 침투자	외부 침투	
인가된 침투자	내부 침투	직권 남용

※ 본 논문은 한국과학재단 RRC(과제번호 : R12-2003-004-01001-0) 연구비지원에 의하여 수행되었음.

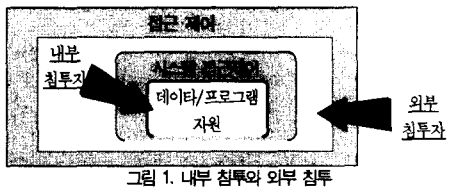

그림 1. 내부 침투와 외부 침투

유의할 점은 침투시험을 취약성 평가와 혼동하지 말아야 한다. 취약성 평가는 소프트웨어를 포함한 내 · 외부 시스템의 스캐닝 자동화의 여부를 확인 및 검증하는 것이며 침투시험은 시스템뿐만 아니라 조직의 정보까지 공격 가능하며 IT 방어, 호스트 보호, 통신 및 물리적 보호, 보안보증 수준을 포함한다[4].

2.1 시험의 분류

시험이란 프로그램간 상호 기능 및 인터페이스의 정상 작동여부와 성능 관련 요구사항의 수행여부를 시험하는 활동이며 시험에는 "블랙박스 시험"과 "화이트박스 시험"의 두 종류가 존재한다. 침투시험은 화이트박스 시험보다 블랙박스 시험의 성향이 강하다[1][10].

(1) 화이트박스 시험

화이트박스 시험은 프로그램 원시코드의 논리적인 구조를 커버하도록 테스트 케이스를 설계하는 방법으로 구조 시험이라고도 한다. 궁극적인 목표는 프로그램 내부 구조에 존재하는 모든 경로를 실행하는 것이지만 경로의 수가 대단히 많으므로 이를 모두 시험하는 것은 불가능하므로 합리적인 방법으로 시험 케이스를 선정하는 기준이 필요한 데, 커버 범위는 문장, 종류, 조건 등의 종류가 존재한다.

(2) 블랙박스 시험

블랙박스 시험은 각 기능이 요구분석 단계나 기본설계 단계에서 정의된 시험 요구사항 명세서에 서술된 대로 시스템으로 통합되는지를 확인하는 시험이다. 따라서 블랙박스 시험은 프로그램에 대한 모든 기능적 요구사항들을 충분히 조사할 수 있는 일련의 입력조건 등을 유도해 낼 수 있어야 한다. 블랙박스 시험은 화이트 박스 기법의 대체 방법이 아니며, 화이트 방법에서와는 다른 결점을 발견하기 위한 보완적인 방법이라 할 수 있다. 결점의 종류에는 부정확하거나 누락된 기능, 인터페이스 오류 등이 존재하며 프로그램 코드의 논리적인 오류를 찾아내기 위한 화이트박스 시험과는 달리 블랙박스 시험은 기능이 구현된 후에 수행된다. 즉, 프로그램 내부의 제어구조와는 무관하게 요구사항의 만족여부를 검사에 중점을 두고 진행된다. 블랙박스 시험에 사용되는 기법에는 균등분할, 경계값 분석, 원인-결과 그래프 기법, 비교 시험 등이 존재한다.

3. 침투시험 평가방법론

CC 기반 침투시험은 정보보호시스템(즉, 평가대상물)의 개발자가 개발

중의 시험단계에서 일차적으로 실시한 후 실시결과를 제출물로 평가자에게 전달한다. 평가자는 개발자가 실시한 침투시험이 정당했는가를 자체적인 침투시험 방법을 통해 확인 및 검증한다. 그림 2에서는 침투시험 방법론의 프레임워크를 제시한다. 침투시나리오란 여러 가지 경로의 침투방법이 존재하며 가장 침투 가능성이 크거나 도달 가능한 경로를 말한다. 이러한 침투시나리오들을 정형적인 명세언어를 통하여 표준화시키며 이를 평가에 이용하게 된다. 침투시나리오와 명세언어에 관한 사항을 5장에서 상세히 설명하도록 한다.

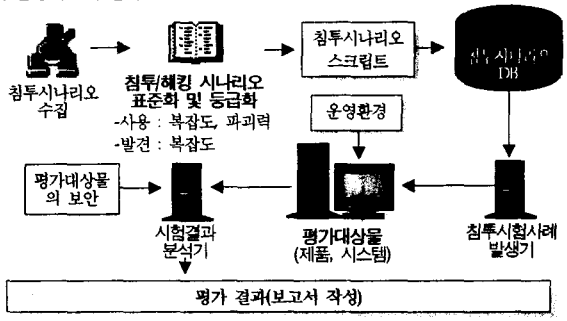

그림 2. 침투시나리오를 이용한 평가방법론 프레임워크[6]

침투시험 방법론을 크게 침투사례 목록 생성, 침투사례 확인, 침투사례 일반화, 침투사례 제거의 4가지 단계로 정의한다. 4가지 단계를 거쳐 침투시험 보고서를 작성한다.

① 침투사례 목록 생성 : 평가대상물을 이해하기 위해서 제출되는 문서를 이용하여 분석하여 침투사례 목록(예 : 유사한 시스템 평가시 습득한 지식, 부정확한 보안정책과 모델, 구현상의 오류 등)을 생성한다. 또한 평가자들 간의 브레인스토밍을 통하여 심도 있게 평가대상물을 분석 및 시스템 설계를 재검토한다.

② 침투사례 확인 : 평가자는 표준화된 침투시나리오와 원시 프로그램, 스펙 등과 같은 제출물에 대하여 분석하여 침투사례를 조사하며 확인된 침투사실은 문서화된다. 또한 침투시나리오를 이용하여 실제 침투시험을 실시하며 이는 기능시험의 블랙박스 시험과 비슷하다. 블랙박스 시험은 보안위험을 막기 위한 보안기능의 순기능적인 측면에 해당한다.

③ 침투사례 일반화 : 이 단계에서는 확인된 침투사례 평가 및 침투사례의 존재 이유를 분석하며 침투사례들의 연계적인 측면도 고려하여 강도가 낮은 여러 개의 침투사례가 모여 높은 피해효과를 미치는지 식별해야 한다.

④ 침투사례 제거 : 침투시험의 종합적인 결과를 고려하여 침투사례를 치유하는 방법을 권고하여 주며 제거하기 어려운 침투사례 또는 일부 허용 가능한 외부비밀통로 등의 침투사례는 잔존 가능성이 존재한다. 이는 운영환경상에서 위험으로 존재하나 외부적인 대응책을 권고하여주며 침투사례 제거 후 보완되었는지 재평가를 실시한다.

4. 평가기준별 침투시험 요구사항 분석

정보통신망 침입차단시스템평가기준의 경우에는 K2 이상, TCSEC의 경우는 B2 이상에서, ITSEC의 경우에는 평가등급에 관계없이 전 등급에서 침투시험을 수행하도록 규정하고 있다. 국제공통평가기준인 CC에서는 보안목표에 침투시험 관련 기능요구사항을 포함하는 개발대상물에 대하여 침투시험을 수행하도록 규정하고 있다. 침투시험은 개발된 시스템이 시스템의 보안을 침해하는 어떠한 결점도 없다는 것을 증명하는 것이므로 평가기준에 정의된 관계를 정확히 만족한다는 것을 의미한다[5].

(1) TCSEC : B2급 이상의 시스템에서 보안기능 시험의 일환으로 침투시험을 수행하도록 규정하고 있다. 표 2는 TCSEC에서 규정하고 있는 보증수준별 침투시험 요구사항과 산출물에 포함되어야 할 내용을 나타낸 것이다[6].

(2) ITSEC : ITSEC에서는 평가등급에 관계없이 전 등급에서 침투시험을 수행하도록 규정하고 있으며 표 3은 ITSEC에서 규정하고 있는 보증수준별 침투시험 요구사항과 산출물에 포함되어야 할 내용을 나타낸 것이다[7].

(3) CC : CC는 평가대상물 개발시 보안목표(보호프로파일/보안목표명세서)에 침투시험과 관련된 보안기능 포함되면 보증수준과 관계없이 침투시험을 수행한다. 표 4는 CC에서 규정하고 있는 보증수준별 침투시험 요구사항과 산출물에 포함되어야 할 내용을 나타낸 것이다[8].

표 2. TCSEC에 정의된 침투시험 요구사항

보증수준	침투시험 관련 요구사항	산출물(문서)포함내용
D-B1	-	-
B2	1. 시스템은 **침투를 다소 방어할** 수 있어야 함. 2. 보안가능 및 침투시험, 비밀통로 분석 3. TCB(Trusted Computing Base) 구현이 **기술적 최상위 단계 명세서(DTLS)**와 일관성을 유지하여야 함. (프로그램과 스펙 사이의 일치성 분석) 4. DTLS와 보안모델의 일치성 분석 5. 보안모델의 공리(Axiom) 증명(ADP 시스템의 보안메커니즘은 시스템 문서에 요구된 대로 테스트되어야 함.)	· 형상관리문서, 보안관리지침서(Trusted Facility Manual), 사용자 가이드 · 보안정책 모델 · DTLS · TCB 시험계획, 절차, 결과 · 코드(프로그램) · 비밀채널 분석 · 비밀채널 처리 효과성 테스트결과 · DTLS와 TCB의 일치성
B3	1'. 시스템은 **침투에 높은 저항성**이 있어야 함. 4'. DTLS와 보안모델의 일치성 분석 및 **신뢰성 있는 설명** 6. TCB는 **침투를 방어할** 수 있음이 밝혀져야 함.	· 비밀채널 **철저히** 분석 · DTLS와 TCB의 일치성(**비정형적** 기술 이용)
A1	2'. 보안가능 및 침투시험, 비밀통로 **정형적** 분석 4'. 정형화된 검증 7. TCB 구현과 **기술적 정형적 최상위 단계 명세서(FTLS)**와 일관성 분석 8. FTLS와 원시코드를 위한 FTLS의 수동 또는 기타 매핑 결과 분석(침투시험)	· FTLS · FTLS와 TCB 원시코드간의 매핑결과

표 3. ITSEC에 정의된 침투시험 요구사항

보증수준	침투시험 관련 요구사항	산출물(문서) 포함내용
E0 ~ E6	- 평가 보증수준별로 알려진 취약성이 악용 가능한가 체크 - (메커니즘 강도 조사) **메커니즘의 요구된 최소 강도를 확인** 또는 반박(disprove)에 필요한 침투시험 실시 - (개발 취약성 조사) 알려진 **취약성이 실제로 악용(exploitable) 가능**한가 확인 또는 반박하기 위한 침투시험 실시 - (사용 용이성 조사) **사용 용이성 분석**을 반박 또는 확인할 때 필요한 다른 시험 실시 - (운영 취약성 조사) **알려진 취약성이 실제로 악용 가능**한가 확인 또는 반박하기 위한 침투시험 실시 - 외부 보안 수단을 위한 모든 가정과 요구사항이 적절히 문서화 되었는가 체크	· 바인딩 분석 · 사용 용이성 분석 (평가 대상물의 불안전한 운영 모드 조사 및 분석) · 개발 취약성 목록 (정제 오류 및 추가된가능을 조사 및 분석) · 운영 취약성 목록 (비정보기술 대응수단이 알려진 개발 취약성에 대응하는지 조사 및 분석) · 메커니즘 강도 분석(최소 강도를 만족하지 못하는 메커니즘 식별) · 침투시험 결과

표 4. CC에 정의된 침투시험 요구사항

보증수준	침투시험 관련 요구사항	산출물(문서) 포함내용
EAL1 ~ EAL7	- 보안감사 분석 : 예측되는 보안 위반이나 실제 보안 위반을 찾기 위한 **시스템 행동과 감사 데이터** 분석 - **복잡공격 학습** : TSF는 TSP에 대한 위반임을 지적하는 다음과 같은 알려진 **침투시나리오와 시그너처 사건들의 내부적 표현**을 유지할 수 있어야 함. - TSF는 시스템 행동을 결정하기 위하여 **사용될 정보**를 조사 및 분석하여 **침투시나리오** 동과 비교 - 시그너처 사건이나 연속된 사건과 일치시 취약성 지적 - TSF 물리적 보호 - **물리적 공격의 탐지 및 통보, 저항** - TSF는 TSF를 손상시킬 수 있는 **물리적 침해**에 대하여 명확한 탐지를 제공해야 함(물리적 공격의 수동 탐지). - TSF 장치, 구성요소에 대한 침투시험실시 - TSF는 TSP가 위반되지 않도록 **TSF 장치, 구성요소의 목록에 대한 물리적 침해시나리오와 비교 및 저항** - TSF **기능 관리 통제 여부** 조사 및 분석	· 잠재적 위반을 나타내는 시그너처 사건 목록 · 시스템 행동의 기록들 · TSF(TOE Security Function) 기능 목록 · TSF 기능 관리 통제 여부 · TSF 장치/구성요소의 목록 · 물리적 침해 시나리오 · 침투시험 결과

현재 TCSEC과 ITSEC 등의 평가기준은 각국의 평가기준 일원화의 노력으로 인해 CC로 대체되고 있다. 또한 우리나라도 CC를 채택하여 정보보호 시스템의 평가를 수행중이며 2005년도에는 침입차단시스템 등의 평가기준은 사라질 예정이다.

5. 침투시나리오

침투시험을 수행하기 위해서는 표준화된 침투 시나리오가 존재하여야 하며 시험의 정확성과 자동화를 유도할 수 있다. 기존의 해킹 사례를 분석하

여 침투 시나리오를 작성하며 이는 이미 범행에 사용된 침투 시나리오이므로 시나리오의 현실성이 높다[9].

5.1 침투시나리오 표현

침투방법에는 트로이목마, 트랩도어, 살라미 기법, 슈퍼 잽핑, 비동기성 공격, CDMA 프로토콜 발신호 침투 공격 등 여러 가지 종류가 존재하지만 본 논문에서는 몇 가지만 간략히 다루도록 한다.

(1) 트로이 목마(Trojan horse)

트로이목마는 정상적인 기능을 하는 프로그램으로 가장하여 프로그램 내에 숨어서 의도하지 않은 기능을 수행하는 프로그램의 코드 조각을 말한다. 트로이 목마 중 가장 많은 피해를 입히고 있는 사례는 백오리피스, 넷버스, Sub7 등이 있다.

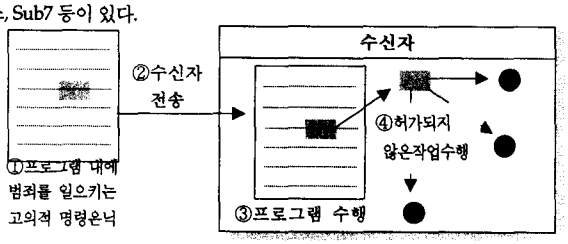

그림 3. 트로이 목마 침투 시나리오

(2) 트랩도어(Trapdoor)

트랩도어는 OS나 대형 응용 프로그램을 개발하면서 전체 시험실행을 할 때 발견되는 오류를 쉽게 하거나 처음부터 중간에 내용을 볼 수 있는 부정루틴을 삽입해 컴퓨터의 정비나 유지보수를 핑계삼아 컴퓨터 내부의 자료를 뽑아가는 행위를 말한다.

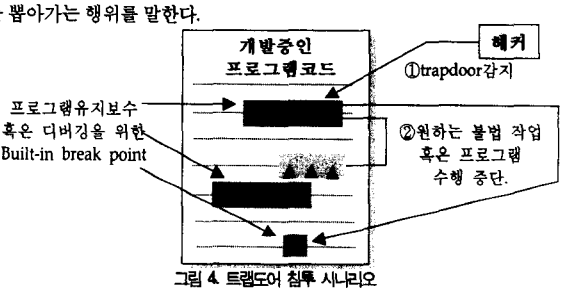

그림 4. 트랩도어 침투 시나리오

(3) CDMA 인증 프로토콜 발신호 침투 공격 시나리오

① 정상적인 사용자가 발신호를 시도한다.
② 이동국이 인증 서명 값을 생성하고 기지국으로 호 연결요구 신호를 보낸다.
③ 침입자가 이 신호를 도청하여 기지국으로 재 전송한다.
④ 정상적인 호와 같은 과정으로 인증에 성공한다.

5.2 침투시나리오 명세언어

침투시나리오의 표현 형태는 다양하고 추상적이므로 침투시험 시에 시험사례로 적용하기 어렵다. 즉, 시험 결과 또는 평가 결과의 공정성, 객관성, 반복성, 재생성이 결여될 수 있다. 따라서, 침투시나리오의 명세언어(또는 스크립트)가 필요하며 가급적 정형적인 명세언어이어야 한다. 이와 같이 정형적인 명세언어를 이용하면 침투시험 환경에 독립적인 침투시나리오를 정의할 수 있고 표준화 정립이 가능하다[9][11].

(1) 명세언어 요구사항

명세언어가 갖추어야 할 조건은 다음과 같다.

- 분명한 구문 : 명세언어는 논리적으로 엄격하게 규정된 일련의 구문들로 구성된다.
- 의사 기호 : 명세언어의 구문은 명확하고 간결해서 언어 구문의 해석을 모호하게 하는 일이 없도록 해야한다.
- 내부 균일성 : 명세언어의 구문은 내부적으로 균일해야 하며 명세언어의 규칙들이 내부에서 상호 모순되지 않아야 한다.
- 다중 부여 : 명세언어 문법의 각 단말 기호는 그것이 이해를 도울 수 있는 한 한가지의 의미를 가지고 있는 정의만을 지원해야 한다.
- 정확성 조건 : 명세언어는 정확성을 갖춘 표현 능력이 있어야 한다.

(2) 명세언어의 예

위와 같은 정형화 방법으로 현재 FDM(Formal Development Method,), Z, VDM(Vienna Development Method), LOTOS(Language Of Temporal Ordering Specification), RAISE(Rigorous Approach to Industrial Software Engineering), SDL(Specification and Description Language) 등과 같은 많은 정형화 명세언어가 개발되어 사용되고 있다[12].

- Z : 기본적인 집합이론과 논리 개념을 사용한 모델 근간의 언어이다.
- VDM : 모델 근간의 언어로 이산수학과 집합이론을 사용한다.
- RAISE : VDM과 Z에 기반을 두며 모듈화, 병렬성 등의 기능이 추가되었다.

정형화 명세언어의 이점은 침투시나리오의 문제점을 실제 침투시험 직전에 분석해볼 수 있으며 모호성, 불완전성 및 모순성을 해결할 수 있는 수학적인 논리와 집합 이론의 표현력을 가지므로 구현결과의 부정확성 시험에 용이하다. 또한 정형화 명세언어의 정형화된 구조 특성은 기계적인 번역 또는 조작을 가능하게 함에 따라 시험과정의 상당부분 자동화가 가능하며 보안 관련 표준들을 구조적 형태로 포함시켜 Z와 VDM 같은 모델 근간의 언어를 이용하는 것이 적절하다. 정형화 명세언어로의 변환은 쉬운 작업이 아니며 이에 대한 연구는 향후과제로 남긴다.

6. 결 론

침투시험은 전통적인 보안평가 방법이다. 정보보호시스템의 신뢰성과 안전성을 평가하고 높은 보안수준으로 향상시키기 위해 침투시험은 필수 불가결한 존재가 되어가고 있다. 본 논문에서는 최근 중요도가 높아지고 있는 침투시험을 정의하였으며 CC를 기반으로 한 침투시험 평가방법론을 제시하였다. 또한 우리나라 및 선진 각국에서 채택하고 있는 평가기준에 정의되어 있는 침투시험 요구사항에 대하여 조사 및 분석하였으며 침투시험을 손쉽게 수행하기 위한 침투시나리오를 정의하였다. 침투시나리오의 표현 형태는 다양하고 추상적이므로 침투시험 사례로 적용하기 위해 정형화된 명세언어를 이용하여야 하며 명세언어의 요구사항 및 예를 보였다.

침투시험은 "해커"들이 행하는 공격방법과 유사하나 해커는 정보보호시스템에 대해 한가지의 결점만 찾아내는 것이 목적이며 평가자가 행하는 침투시험은 잠재적 루트까지 찾아 내야한다. 또한 해커들은 침투시험에 시간제한을 두지 않으므로 침투시험의 평가기간 등을 설정하기 어려우며 침투시험시 평가대상물을 손상시킬 가능성이 존재하므로 시험 비용을 예측하기 어렵다. 그러므로 향후 연구과제로 이러한 단점들을 보완하고 침투시나리오들을 표준화 및 등급화하여 객관성과 일관성을 유지하며 명세언어로의 구현 및 비용 효과적인 보안평가를 수행하기 위한 자동화된 침투시험평가도구 개발이다.

참고문헌

[1] Diane Seddon, "Penetration Testing : thinking outside the (black) box," Aug. 2002.
[2] Jane Frankland, "Automated penetration testing : nothing more than a false sense of security!," Aug. 2003.
[3] James P. Anderson Co, "Computer Security Threat Monitoring and Surveillance," Apr. 1980.
[4] Anton Chunvakin, "Standardizing Penetration Testing," May. 2002
[5] 정보보호뉴스, "정보보호 기술 해설 : 보안기능 신뢰도 평가를 위한 침투시험", 1998. 5월. (통권 11호)
[6] DoD, "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)," Dec. 1985.
[7] European Communication, "Information Security Evaluation Criteria(ITSEC)," Ver. 1.2, June. 1991.
[8] CCEB, "Common Criteria for Information Technology Security Evaluation(CC)," Version 2.1, CCIMB-99-033, http://csrc.ncsl.gov, Aug. 1999. (정보보호시스템 공통평가기준, 정보통신부, 2002.8과 내용 동일)
[9] 한국정보보호센터, "정보보호시스템 평가방법론 연구", 수탁기관:한남대학교,1996. 12.
[10] 한국전산원, "감리 시험기법/도구 적용지침 연구", 2001. 12.
[11] National Computer Security Center, "Guidelines for Formal Verification System," NCSC-TG-014-89, 1989.
[12] NPL Data Security Group, "Report of a workshop on formal methods in data security standards," NPL Technical Memorandum DITC 70/93, Jan. 1993.
[13] Corsaire, "Penetration testing guide"
[14] Thomas Rude, "A Guide to Penetration Testing," Oct. 2000.
[15] Ulf Lindqvist, " Observation on the Nature of Computer Security Intrusions," Dec. 1996.