사이버보안 실습을 위한 가상 보안 훈련장 아키텍처 연구

이택, 김도훈, 신연균, 신승용, 인호
고려대학교 컴퓨터전파통신공학과
e-mail:{comtaek, karmy01, younkyun, syshin, hoh_in}@korea.ac.kr

An Architecture of Virtual Security Training Laboratory for Cybersecurity Exercise

Taek Lee, Do-Hoon Kim, Youn-Kyun Shin, Seung-Yong Shin, Hoh Peter In
Dept of Computer Science and Engineering, Korea University

요 약

본 논문에서는 정보시스템 운영시 발생하는 사용자 취약성(Human Vulnerability) 문제의 심각성에 대해 알아보고 이를 개선하기 위한 교육 및 훈련 프로그램을 다루고 있는 기존 관련 연구들을 조사 분석 한다. 아울러 기존 연구에서 보완되어야 할 개선 요구사항 들을 도출하여 향후 효과적인 취약성 개선 프로그램 제공을 위한 가상머신에 기반한 보안 훈련장 시스템 아키텍처를 제안한다.

1. 서론

많은 사람들이 보안은 기술적 요소에 의해 충분히 보장될 수 있다고 믿고 있는 경향이 있다. 하지만 어떠한 보안 솔루션도 스스로 알아서 자체적으로 운영되는 시스템은 없으며 결정적인 긴급상황 발생시 대응에 대한 최종 의사결정은 사람이 하게 된다. 결국 정보 시스템의 최종적인 보안성은 사람의 손에 의해 결정된다고 해도 과언이 아니다.

매년 발행되는 CSI/FBI 보안 설문자료[1]에 따르면 59%이상의 보안 사고가 내부 인원에 의한 접근권한 오용에서 유발되었고, 가장 큰 경제적 손해(연간 평균 2천만 달러)를 초래하는 위협들은 피싱이나, 랜섬, 산업스파이와 같은 경제적 사기(financial fraud) 사건들이었다. 이밖에 보안 위협 랭킹 리포트 관련 글들[2][3]에서도 컴퓨터 사용자들의 실수에 의해 유발되는 사고 심각성을 시사하고 있다. 많은 해킹 공격들이 기술적으로 구현된 시스템(예: 방화벽, IDS) 방어라인을 우회하기 위하여 사회공학적 방법(메신저 대화를 가장한 취약성 이용, 피싱 이메일 등, 악성 사이트 접속 유도)을 이용하기 시작한 것은 사실 어제 오늘의 일이 아니다.

이러한 정보시스템 관련 사용자 취약성 문제 해결을 위한 유일한 대응책은 실제적이고 실용적인 교육과 훈련이라고 할 수 있다. 시스템 사용자들로 하여금 보안 문제의 심각성을 자각시키고 이상 징후에 대해 스스로 예방하고 대처할 수 있는 적절한 훈련이 이루어져야 한다. 보안 교육의 특성상 실제 상황을 경험하지 않고는 현장에서 효과적으로 방어할 수 없다.

본 논문에서는 사용자 취약성 개선을 위해 선행된 기존 관련 연구들을 조사 분석하고 교육(훈련) 시스템 구현을 위한 요구사항들을 도출하며 해당 요구사항들을 달성하기 위한 가상 보안 훈련장 아키텍처를 제안하도록 한다.

2. 기존 관련 연구 동향 분석

다음은 보안 교육 및 훈련과 관련된 국내외 연구 사례들에 대한 조사 분석 내용이다.

- **해커스쿨 랩** : FHZ(Free Hacking Zone)을 구성하여 TELNET을 통해 drill.hackerslab.org으로 접속하여 해킹을 통해 레벨업(Level Up)을 하는 것을 목표로 한다. (http://www.hackerslab.org)
- **해커스쿨** : 일종의 그룹 스터디 동아리로서 보안강좌와 FTZ(Free Training Zone)을 구성하여 On/Offline 그룹 스터디 진행, 정기적 보안 기술 문서 작성, 연구 환경 지원 및 학습 방향 제시 그리고 팀원 간의 정보를 공유 운영한다. (http://www.hackerschool.org)
- **정보보호기술 온라인 학습장** : 한국정보보호진흥원에서 운영하는 정보보호시스템 구축 훈련을 할 수 있는 온라인 훈련공간으로 시스템 관리자는 공개 보안 SW를 이용해 침입차단시스템, 방화벽, 바이러스 월 등의 운영과 침해사고 분석, 시스템 취약성 점검, 불법 사용자 접근 통제 등 다양한 훈련 내용을 실습 해 볼 수 있다. (http://www.sis.or.kr)
- **Organized Competition Among Service Academies** : 2001년 미 국방 대학은 네트워크상에서 학교간 상호 방어 시스템을 디자인, 이용, 관리, 그리고 방어를 위한 다양한 가상 응용환경을 제공하는 연구를 수행한 바 있다 [4]. (http://www.itoc.usma.edu/cdx)

- **Small Internal Continuous Exercise** : Texas Austin 대학의 한 동아리에서 작고, 한정된 공간에서 지속적으로 연습할 수 있는 가상 시스템을 구축하였다.
- **Regional Capture-the-flag Exercise** : UC 산타바바라 대학에서 가상머신 워크스테이션을 통해 지정 시스템의 방어와 공격을 통한 선점식(깃발탈환) 교전 환경 시나리오를 제공하는 연구가 있었다 [4].
- **Semester-long Class Exercise** : 텍사스 A&M 대학에서 학생들의 기술과 지식 수준에 의해 공격과 방어 그룹을 형성하고 학점제 방식으로 폐쇄 환경에서 보안 프로젝트를 실시하여 결과 분석을 한 사례가 있다 [4].
- **Virtual Training Education** : 정보보증(information assurance), 컴퓨터 포렌식, 침해대응 뿐 아니라 여러 보안 주제에 대해 웹 기반의 가상 수업을 통해 관련 지식을 습득하고, VTE내의 가상공간에서 실제로 유저 스스로가 배운 기술을 시현해 볼 수 있는 공간이다. (http://vte.cert.org)

현장에서 공격과 방어를 실제로 훈련할 수 없으므로 보안 교육이 이론에만 머무르거나 매우 제한적인 경우가 많았다. 이를 현실세계에 영향을 주지는 않지만 현실세계와 같이 공격과 방어를 실제로 경험(실험)할 수 있는 보안 교육 및 훈련 공간이 매우 절실한 상태라 할 수 있다.

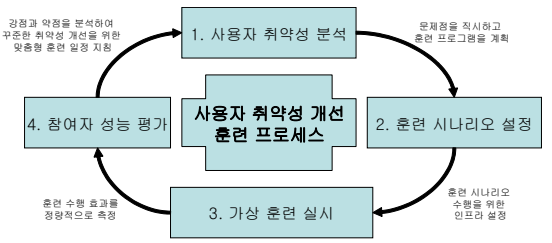
교육(훈련) 참여자들의 보안 활동 성능 향상 정도를 지속적으로 측정하여 부족한 부분에 대한 맞춤형 훈련 시나리오를 제공할 수 있는 시스템 영속성과 확장성이 제공되어야한다. 하지만 많은 경우가 일시적인 목적의 단발성 교육 및 훈련만을 목적으로 하여 시스템이 제안되는 경향이 있다. 아울러 개인 컴퓨터 사용자들을 대상으로 하는 학습이 아닌 팀원 상호 작용 활동에 대한 훈련 지원 시나리오도 필요하다.

3. 가상 보안 훈련장 아키텍처

3.1 가상 보안 훈련장 구현을 위한 요구사항

사용자 취약성 개선을 위하여 (그림 1)과 같은 지속적인 훈련 사이클이 필요하다. 다음은 온라인 가상 보안 훈련장을 통한 교육 시스템 구현 시 필요한 기능 요구사항들이다.

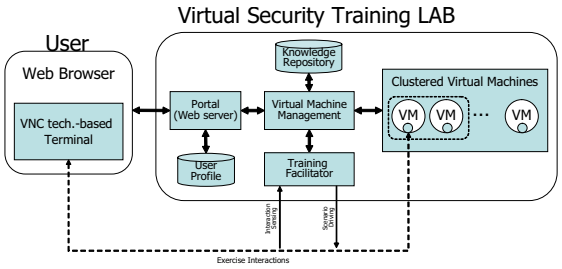
- **유저관리 기능**: 온라인 교육 및 훈련에 참여하는 참여자들의 훈련 달성도를 기록 관리하여 적절한 레벨의 훈련 지침을 제공해야 한다.
- **실습환경 구축**: 단순히 자료들(온라인 동영상, 문서자료 등)에 의존하는 피동적인 학습에서 벗어나 실질적인 실습 위주의 환경 제공해야 한다.
- **훈련 컨텐츠 제공**: 다양한 학습 레벨과 학습 목표 달성을 위한 준비된 교육(훈련) 시나리오가 필요하다.
- **훈련효과 정보수집**: 훈련 후 개선되는 보안 활동 성능을 측정하고 평가하여 향후 알맞은 훈련 레벨을 설정하는 것이 필요하다.
- **시스템 확장성과 일반성**: 단발성 학습이나 훈련이 아니라 다양한 사용자와 다양한 시나리오를 소화하기 위해 유연성 있는 가상 보안 훈련 시스템 아키텍처 설계가 필요하다.



(그림 1) 사용자 취약성 개선 사이클

3.2 가상 보안 훈련장 아키텍쳐 제안

앞서 제안한 사용자 취약성 개선 프로세스(그림1) 지원과 관련 기능 요구사항들을 충족시킬 수 있는 가상머신 기술에 기반한 가상 보안 훈련장(VSTL: Virtual Security Training Laboratory) 아키텍쳐를 제안한다.



(그림 2) 가상 보안 훈련장 아키텍쳐

다음은 제안 아키텍쳐(그림 2)에 대한 세부 기능 컴퍼넌트들에 대한 설명이다.

- **사용자 클라이언트**: 온라인 교육(훈련) 프로그램에 참여하는 참여자는 웹브라우저 상에서 모든 교육(훈련) 지침을 하달 받는다. 로그인 시스템을 통해 교육 및 훈련 전과정에 대한 유저프로파일 관리가 가능하며 원격에서 제공되는 가상머신 시스템 자원을 할당 받아 실습을 실시한다. 원격 작업을 위해 웹브라우저 상에 작업 가능한 터미널 창이 내장되어 제공되며 VNC 기술을 통해 원격 통신이 가능하도록 구성할 수 있다.
- **포탈서버**: 시스템 자원 스케쥴링, 유저 프로파일 관리, 훈련 시나리오 전달, 교육 컨텐츠 제공 등, 원격 사용자와 메인 시스템 간의 중계자 역할을 수행한다. 교육(훈련)의 참여에서 종료까지 전과정을 감독 지원한다.
- **사용자 프로파일**: 교육(훈련)에 참여하는 참여자들의 신상정보 및 교육 목표 달성도 수준, 향후 학습 조건들에 대한 정보를 수시로 저장 관리한다.
- **지식 저장소**: 교육 켄텐츠 자료 및 훈련 시나리오에 대한 정보들이 저장된다. 포탈서버는 유저 프로파일을

참고하여 현재 교육(훈련) 참여자의 상태를 파악하고 지식 저장소에 저장된 내용을 바탕으로 프로그램을 진행한다.

- **가상머신 관리**: 원격에서 접속하는 다수의 사용자들에게 할당 가능한 가상머신들을 생성하거나 더 이상 훈련에 이용되지 않는 실습 자원들은 회수하는 역할을 한다. 또한 포탈서버의 신호에 의해 마지막으로 학습하였던 교육(훈련) 시나리오에 대응하는 가상 머신 이미지 클러스터를 부팅업하여 원격 사용자 클라이언트에 내장되어 있는 터미널 작업창에 바인딩한다.
- **훈련 도우미 에이전트**: 지시되는 훈련 시나리오에 맞게 참여자가 정확히 주어진 미션을 수행하고 있는가를 모니터링하고 필요에 따라 웹브라우저를 통해 경고를 주거나 도움말 메시지를 전달하여 원할한 프로그램 진행을 주도한다. 또한 교육(훈련) 참여자들의 향후 교육 효과 평가를 위해 필요한 정보들(참여 집중도나 교육 목표 달성 여부 체크를 위한 행위 이벤트)을 수집한다. 수집된 정보는 교육(훈련) 후 개선된 보안 성능 정도를 평가하고 향후 포탈서버에 접속하는 프로그램 참여자에게 레벨업된 교육 컨텐츠 및 훈련 시나리오를 제공할 수 있다.
- **가상머신 이미지**: 다수의 교육(훈련) 참여자들에게 동일한 실습환경을 제공하기 위하여 필요한 실습 운영체제 환경 이미지들을 미리 준비되어 있어 가상머신 관리 에이전트의 신호를 받아 해당 이미지를 부팅업되고 바인딩된다.

4. 제안 아키텍쳐 비교 분석

기본적으로 기존 관련 연구에서는 네트워크 중심의 교육 실습이 주였다면 제안 시스템은 사용자 보안 취약성을 파악하고 개선하는데 주안점을 두었다.

또한 기존 연구가 제한된 소규모 실험망에서 실시되었다면 제안 시스템은 원격에서 접속하여 필요한 자원을 활용할 수 있도록 지원하여 시공간적인 제약조건을 해결하고자 하였다.

아울러 훈련 시스템의 오작동 시에도 마지막 훈련 시점으로 롤백이 손쉽도록 가상머신 이미지 관리 기능을 고려하였다.

마지막으로 기존 연구처럼 개인에만 해당한 교육 프로그램이 아니라 팀원들 간의 팀웍 훈련 시나리오 지원을 위해 커뮤니케이션 채널을 웹 인터페이스(예: 웹브라우저 내에 메시지 전달 채널 구현)를 통해 구현할 수 있도록 하였다. 팀원 상호간의 상호작용을 통해 개인이 달성 가능한 보안 성능 개선 이상의 시너지 효과를 얻을 수 있을 것이다.

<표1>은 기존 관련 연구들과 제안 가상 보안 훈련장(VSTL) 시스템 간의 기능 요구사항별 차이점을 비교한 결과이다.

연구명	유저 관리	실습환경 구축	훈련 컨텐츠 제공	훈련효과 정보수집	연구의 확장성/일반성
해커스쿨 (랩)	예	예	예 (아니오)	아니오	아니오
정보보호기술온라인 학습장	예	아니오	예	예	아니오
Organized Competition	예	예	아니오	아니오	예
Small, Internal, Continuous Exercise	아니오	아니오	아니오	아니오	아니오
Regional Capture The Flag Exercise	아니오	예	아니오	아니오	아니오
Semester Long Class Exercise	예	아니오	아니오	예	예
Virtual Training Education	아니오	예	예	아니오	예
제안 시스템 (VSTL)	예	예	예	예	예

<표 1> 제안 시스템과 기존 관련 연구들과의 비교 평가

5. 결론

많은 기존 연구 논문들에서 자신이 고안한 보안 이론과 알고리즘을 테스트하기 위하여 전용의 테스트베드를 구축하는 사례는 많이 있었으나 대부분 네트워크 중심의 알고리즘 테스트가 목적이였으며 일반화된 목적이 아닌 일시적인 실험 목적의 비개방성 실험망이 대부분이었다.

본 연구에서 제안하는 가상 보안 훈련장 시스템은 사용자 취약성 분석을 위한 신뢰성 있는 시스템-사용자 상호작용 데이터를 자동으로 수집하고 가공하여 훈련 시나리오반영을 통해 참여자들의 현 보안성능평가 상태를 인지시키고 향후 향상된 미션 수행을 지속적으로 지원하여 기관의 보안 성숙도에 기여하고자 끊임없는 자기개선 라이프사이클을 제공하는 것을 목표로 삼는다.

사 사 (謝辭)

이 논문은 2008년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. R01-2008-000-10343-0)

참고문헌

[1] “2007 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute (CSI), 2007.

[2] Robert McMillan, "SANS: Human error top security worry", IDG News Service, Nov. 15, 2006.

[3] John Leyden, "Human error blamed for most security breach", The Register®, 2004.

[4] Lance J. Hoffman, Tim Rosenberg, Ronald Dodge, and Daniel Ragsdale, “Exploring a National Cybersecurity Exercise for Universities”, IEEE Security & Privacy, Sep./Oct. 2005.