사물인터넷융복합논문지 Vol. 11, No. 3, pp. 203-209, 2025 https://doi.org/10.20465/KIOTS.2025.11.3.203

자동화 침투 테스트 도구를 활용한 정보보호 교육 모델 개발 및 효과 분석

이근호*
백석대학교 컴퓨터공학부 교수

Development and Effectiveness Analysis of an Information Security Education Model Using Automated Penetration Testing Tools

Keun-Ho Lee*
Professor, Div. of Computer Engineering, BaekSeok University

요 약 정보보호 인력 양성에 대한 사회적 수요가 급증함에 따라 실무 중심의 보안 교육 강화가 요구되고 있다. 본 연구는 펜테라와 같은 자동화 침투 테스트 도구를 활용한 실습 기반 정보보호 교육 모델을 제안하고, 이를 대학 교육 현장에 적용하여 학습 효과를 실증적으로 분석하였다. 기존 보안 교육의 한계를 보완하고, 산업체가 요구하는 실무 역량을 체계적으로 강화할 수 있도록 설계된 본 교육 모델은 백석대학교 정보보호 전공 학부생을 대상으로 검증하였다. 교육 전후 설문조사, 실습 결과 분석, 전문가 평가를 통해 교육 효과성을 측정한 결과, 학습자의 보안 인식 및 기술 숙련도가 유의미하게 향상된 것으로 나타났다. 또한 산업 현장에서의 활용 가능성과 확장성 측면에서도 긍정적인 평가를 받았다. 본 연구는 향후 자동화 보안 도구를 활용한 정보보호 교육 모델 확산에 실질적인 기여를 할 수 있을 것으로 기대된다.

주제어 : 정보보호, 자동화 침투 테스트, 펜테라, 실습 교육, 사이버 보안

Abstract As the societal demand for cultivating skilled cybersecurity professionals rapidly increases, there is a growing need to strengthen practice-oriented security education. This study proposes a hands-on information security education model utilizing an automated penetration testing tool such as Pentera, and empirically analyzes its effectiveness when applied in a university setting. Designed to address the limitations of conventional security training and systematically enhance the practical competencies required by the industry, the proposed model was tested with undergraduate students majoring in information security at Baekseok University. The effectiveness of the training was evaluated through pre- and post-education surveys, analysis of practical results, and expert assessments. The findings indicate a significant improvement in learners' security awareness and technical proficiency. Moreover, the model was positively evaluated in terms of its applicability and scalability for real-world industry settings. This study is expected to contribute to the broader adoption of automated security tools in cybersecurity education moving forward.

Key Words : Information Security, Automated Penetration Testing, Pentera, Practice Training, Cybersecurity

*이 논문은 2025학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2025년 04월 07일 수정일 2025년 06월 07일 심사완료일 2025년 06월 10일

1. 서론

디지털 전환 가속화로 인해 사이버 위협은 더욱 고도화되고 있으며, 이에 따라 국가 및 산업 전반에서 정보보호 전문가의 역할은 점차 중요해지고 있다[1,2]. 한국인터넷진흥원(KISA)의 통계에 따르면 정보보호 전문 인력 수요는 매년 평균 10% 이상 증가하고 있으며, 특히 중소기업, 공공기관, 제조업 등 다양한 산업 분야에서 보안 실무 인력에 대한 수요가 두드러진다[3]. 그러나 현재 국내 대학에서 운영되는 정보보호 교육과정은 이론 중심 또는 단순 실습 위주의 교육이 대부분이며, 산업 현장에서 요구하는 실무 능력과는 괴리가 있는 경우가 많다.

기존 보안 실습은 대부분 모의해킹, 방화벽 설정, IDS/IPS 구성, 취약점 분석 등으로 구성되며[4], 학습자의 기술 수준에 따라 난이도가 편차를 보이거나, 실습 환경 구축에 많은 시간과 자원이 소요되어 반복 학습이 어려운 단점이 존재한다. 특히 중소규모 대학의 경우 실습 환경을 유지하는 데 드는 비용과 인프라 부담이 크기 때문에, 실효성 있는 실무형 교육을 지속적으로 제공하는 데 어려움이 따른다.

이에 따라 최근에는 자동화된 보안 평가 및 공격 시뮬레이션 도구를 활용한 교육 접근법이 주목받고 있다[5]. 이러한 도구는 실시간으로 보안 취약점을 진단하고, 정량적 결과를 기반으로 리포트를 생성하여 학습자에게 직관적인 피드백을 제공한다. 반복 가능한 시나리오 기반 학습을 통해 학습자는 실전과 유사한 환경에서 다양한 공격 기법과 대응 방안을 학습할 수 있다.

펜테라는 기업 내부 시스템에 실제 해킹을 시도하는 방식으로, 공격 벡터를 자동 탐색하고 리포트를 제공함으로써 모의 해킹의 자동화를 구현한 대표적인 도구이다[6,7]. MITRE ATT&CK 프레임워크 기반의 공격 시나리오를 자동으로 실행하며, 공격 경로, 권한 상승, lateral movement 등 다양한 행위를 시뮬레이션할 수 있다. 본 연구에서는 이러한 펜테라를 활용한 정보보호 교육 모델을 설계하고, 이를 백석대학교 정보보호 전공 교육과정에 적용하여 그 효과를 분석하였다.

2. 관련 연구

2.1 전통적 정보보호 교육과 그 한계

전통적인 정보보호 교육은 주로 이론 강의와 정형화된 실습 위주로 구성되며[1,2], 이는 학습자의 개인별 수준 차이를 반영하기 어렵고, 실제 현장에서 발생할 수 있는 다양한 사이버 위협 상황에 대한 대응 역량을 체계적으로 길러주기 어렵다는 한계가 있다. 대부분의 교육 과정은 교과서 중심의 개념 전달이나 실습 매뉴얼에 기반한 결과 중심 수행에 그치기 때문에, 창의적 문제 해결력이나 실시간 의사결정 능력 배양에는 제약이 있다.

예를 들어, 취약점 스캐닝 도구를 활용한 실습은 탐지 결과 리포트의 해석에 집중되며, 취약점이 발생하는 원인과 그에 대한 구체적인 공격 시나리오나 대응 전략까지는 충분히 다루지 않는 경우가 많다. 학습자는 결과를 단순히 받아들이고 해석하는 수준에 머무르며, 능동적 사고나 시나리오 기반 판단력은 부족할 수 있다.

또한 교육 환경은 대부분 정적(static) 환경으로 구성되어 있어 실시간 변화에 따른 침해 사고 대응 훈련이 어렵고, 다양한 최신 공격 기법에 대한 실습 기회도 제한적이다. 보안 실무에서는 이상 징후 탐지, 신속한 대응, 피해 최소화를 위한 실전 경험이 중요하지만, 교육에서는 이를 재현하기 어렵다.

교육 인프라의 제약도 중요한 문제다. 실습 환경 구성에는 고사양 장비, 네트워크 구성, 가상화 기술 등이 요구되며, 이는 중소형 대학이나 일반 교육기관에서는 운영에 큰 부담이 된다. 특히 보안 장비나 침투 테스트 도구를 실제로 운용하고 응용하는 데 필요한 교수자의 전문성이나 기술 지원 인력이 부족한 경우가 많아, 교육 품질 유지에 어려움을 겪는다[8].

2.2 자동화 보안 도구를 활용한 교육 사례

자동화 보안 도구는 침투 테스트, 위협 탐지, 내부망 경로 분석, 취약점 자동 진단, 공격 시뮬레이션 실행, 대응 조치 권고, 그리고 상세한 리포트 제공 등의 기능을 통합적으로 제공한다[5,9]. 이러한 도구는 기존의 수작업 기반 보안 점검에 비해 시간과 자원을 절감할 수 있을 뿐만 아니라, 반복 가능성과 정량 평가가 가능하다는 점에서 교육 및 실무 양쪽 모두에 적합하다.

대표적인 자동화 보안 도구로는 Pentera(펜테라), AttackIQ, SafeBreach 등이 있으며, 이들 도구는 대부분 MITRE ATT&CK 프레임워크 기반의 공격 전술·기법(Tactics, Techniques and Procedures: TTPs)을 자동화 시뮬레이션하는 기능을 제공한다[6,10,11]. 예를 들어, 펜테라는 인증 우회, 권한 상승, lateral movement, command & control 통신, 데이터 탈취 등 다양한 공격 단계를 체계적으로 실행하며, 결과는 시각화된 대시보드 및 리스크 기반 리포트 형태로 제공되어 학습자 또

는 관리자 모두가 손쉽게 분석할 수 있다.

이와 같은 자동화 도구는 기업의 정보보호관리체계(ISMS) 인증 준비, 침투 테스트 자동화, 보안 리스크 가시화, 보안 교육 및 훈련 등 다양한 분야에 활용되고 있다. 특히 시나리오 기반 공격 실행과 결과 피드백을 통해 보안 담당자의 실무 대응 능력뿐 아니라, 교육 현장에서 학습자의 체험적 학습 효과를 극대화할 수 있다.

국내에서는 일부 보안 전문기업, 금융기관, 공공기관 등에서 실무 보안 점검이나 보안 수준 검증 목적으로 도입하고 있으며, 대학 교육 분야에서는 아직 초기 도입 단계로서 산학협력 프로그램이나 보안 특화 학과를 중심으로 실험적 도입이 이루어지고 있다[12,13]. 전공 교수진의 전문성과 실습 환경의 기술적 요구 조건 등이 대학 도입의 주요 제한 요인으로 작용하고 있지만, 향후 교육 프로그램의 실효성 강화를 위해 점진적으로 확대될 가능성이 높다.

3. 펜테라 기반 정보보호 교육 모델 설계

3.1 교육 모델 개요

본 연구에서 설계한 펜테라 기반 정보보호 교육 모델은 산업 현장에서 요구하는 실무 역량을 체계적으로 배양할 수 있도록 설계되었으며, 다음과 같은 4단계로 구성된다.

- 1단계 : 펜테라 환경 구축 및 에이전트 설치

펜테라 플랫폼을 학습 환경에 구성하고, 각 조별 가상머신 또는 로컬 장비에 펜테라 에이전트를 설치한다. 학습자는 공격 대상 네트워크의 구조를 이해하고, 펜테라가 수집할 수 있는 자산 목록을 점검함으로써 보안 진단의 출발점을 인식한다.

- 2단계 : 공격 시나리오 실행 (권한 상승 등)

사전 정의된 공격 시나리오를 펜테라에서 실행하여 자동화된 공격 경로를 체험한다. 주요 내용은 다음과 같다:

·초기 접근(Initial Access)
·권한 상승(Privilege Escalation)
·횡적 이동(Lateral Movement)
·명령 및 제어(C2 Communication)
·민감 정보 추출(Data Exfiltration)

학습자는 이러한 전 과정을 실시간으로 시각화하여 위협의 흐름을 파악하고 대응 전략을 구상한다.

- 3단계 : 자동화 리포트 분석 및 시각화 결과 이해

펜테라는 공격 결과를 기반으로 우선순위 기반의 위험요소, 침투 경로, 미탐지 취약점 등을 리포트 형식으로 제공한다. 학습자는 이 리포트를 바탕으로 기업 환경에서 실제로 발생할 수 있는 위협 시나리오를 분석하며, 각 취약점에 대한 영향도를 평가하고 네트워크 내 상호작용 구조를 도식화한다.

- 4단계 : 취약점 보완 시뮬레이션 및 개선 활동 수행

펜테라가 제시한 권고사항을 바탕으로 방화벽 설정, 접근 통제 수정, 시스템 패치 적용 등의 대응 활동을 시뮬레이션한다. 이후 각 조는 개선 결과를 문서화하고 발표 자료로 구성하여 보고서를 제출하며, 보안 조치의 정당성과 효과에 대해 토의한다.

이 교육 모델은 단순한 보안 실습을 넘어, 공격 시나리오 이해 → 결과 분석 → 대응 시뮬레이션 → 보고서 작성에 이르는 실무형 전 주기 기반 학습으로 구성되어 있다.

3.2 교육 목표 설정

본 펜테라 기반 실습 교육은 단순한 도구 사용법 습득에 그치지 않고, 실제 사이버 보안 사고 대응 역량을 종합적으로 향상시키는 것을 목표로 한다. 각 단계별 시나리오에 대응되는 학습 목표는 다음과 같이 구체적으로 설정된다.

- 내부 침투 및 권한 획득의 위험성 이해

학습자는 공격자가 네트워크에 침입하는 방식과 초기 접근 수단을 학습하며, 보안 설정이 미비한 시스템에서 발생할 수 있는 보안 리스크를 식별한다. 이를 통해 사회공학, 취약한 인증 구조, 신뢰구간 설정 오류 등에 대한 인식을 제고한다.

- 네트워크 경로 분석 및 Lateral Movement 구조 학습

펜테라를 통해 공격이 내부 시스템 간에 어떻게 전파되는지(Lateral Movement)를 시각화된 결과를 통해 학습한다. 이를 통해 네트워크 계층, 내부망 구조, 트래픽 흐름에 대한 구조적 이해를 심화하며, VLAN 분리, 방화벽 정책 구성 등 실무적 보안 설계 요소를 함께 다룬다.

- 자동화 리포트를 기반으로 한 보안 조치 실행 능력 배양

펜테라가 생성하는 자동화 리포트를 바탕으로 학습자는 각 취약점의 위험도를 정량적으로 평가하고, 대응 우선순위를 설정하여 보안 강화 방안을 도출한다. CVSS 점수 해석, 대응 전략 문서화, 위험관리 기법(Risk Matrix 등)의 적용도 포함된다.

- 팀 기반 리포트 작성 및 프레젠테이션 수행

실습 결과를 바탕으로 각 조는 보고서를 작성하고, 보안 문제에 대한 분석과 대응 전략을 정리하여 발표한다. 이를 통해 기술적 소통 능력, 보안 문서 작성 역량, 발표 및 협업 능력을 통합적으로 강화한다. 산업 현장에서 요구되는 실전 대응 역량 및 컨설팅 능력 함양에도 기여한다.

3.3 산업 현장 활용성과 교육 연계 방안

펜테라는 기업 내부에서 침투 테스트를 자동화하고, 리포트를 통해 보안 수준을 측정하는 데 실제 활용되고 있다. 실제 보안팀에서는 해당 도구를 통해 침투 경로의 실시간 가시화, 고위험 취약점 자동 탐지, 반복 테스트를 통한 개선 효과 추적 등을 수행하고 있으며, 이는 보안 관리의 정량화와 문서화에 큰 도움을 주고 있다.

교육 측면에서도 펜테라는 산업 현장의 실무 환경을 학습자가 그대로 경험할 수 있도록 지원한다. 학생들은 해당 도구를 통해 실제 보안 컨설팅 업무와 유사한 공격 분석 및 보고서 작성, 대응 방안 도출 훈련을 반복하게 되며, 이는 취업 후 빠른 적응력과 실무 대응력을 높이는 데 유리하게 작용한다.

또한 펜테라의 시나리오 기반 훈련은 산업체에서 진행되는 Red Team/Purple Team 훈련과 유사한 구조를 갖추고 있어, 현장에서 요구하는 침해 탐지, 위협 분석, 대응 전략 수립 등 다양한 보안 직무의 실무 프로세스를 간접적으로 체험할 수 있도록 한다. 이를 통해 교육과 산업 현장을 연계한 커리큘럼 설계가 가능하며, 산학협력 프로젝트, 캡스톤디자인 과제, 인턴십 실습 등과의 접목도 용이하다.

4. 대학교 적용 사례 및 실험 분석

4.1 실습 구성 및 운영 환경

본 실습은 '시스템보안 이론 및 실습' 과목에서 총 3주간 6차시로 나누어 운영되었으며, 총 35명의 학부생이 7개 조로 구성되어 실습에 참여하였다. 실습 환경은 백석대학교 차세대보안실습실 내에 구축된 가상화 기반 보안 실습 서버 인프라를 기반으로 구성되었다.

각 조별로 VMware Workstation 기반의 개별 VM 환경을 구축하였으며, 내부망 구조와 유사한 형태로 Windows Server, Windows Client, Ubuntu Linux 등 다양한 운영체제가 배치되었다. 펜테라 에이전트는 Ubuntu Server에 설치되었으며, 실습에서는 펜테라와 SentinelOne(차세대 엔드포인트 보안 솔루션)을 함께 사용하여 실제 위협 탐지 및 대응 체계를 학습하였다.

각 조는 펜테라를 통해 사전 정의된 공격 시나리오(권한 상승, lateral movement 등)를 실행하고, 그에 따른 SentinelOne의 탐지 및 차단 반응을 확인하며 이중 검증 기반의 사이버 훈련을 수행하였다. 펜테라의 리포트를 기반으로 위협 발생 원인과 침투 경로를 분석한 뒤, SentinelOne에서 생성된 이벤트 로그 및 대응 내역을 함께 분석하여 실제 기업 환경에서의 보안 운영 절차를 유사하게 체험하였다.

실습 전에는 펜테라와 SentinelOne의 기능 및 구성 구조에 대한 이론 강의가 1차시 동안 제공되었으며, 이후 각 조는 공격 실행 → 결과 분석 → 대응 방안 도출 → 보고서 작성 및 발표의 과정을 반복 수행하였다. 실습 중에는 보안 전문가가 조별로 실시간 멘토링을 제공하여 도구 사용법, 사고 분석 절차, 보고서 작성 방법에 대한 피드백이 이루어졌다.

이러한 실습 구성은 학생들이 실제 보안 운영 환경에서 사용되는 침투 테스트 및 엔드포인트 보안 기술을 통합적으로 체험할 수 있도록 설계되었으며, 실무 현장에서의 적응력과 문제 해결 역량을 향상시키는 데 중점을 두었다.

4.2 교육 효과 분석: 설문조사 및 실습 결과

표 1은 기존의 시스템 보안 이론 및 실습 과목에 펜테라를 적용한 과목에 대한 비교표이다. 기존 과목은 방화벽 설정, IDS/IPS 구성 등 개별 보안 기술을 중심으로 하는 단편적 실습이 주를 이루었으며, 학습자 개인의 결과 제출을 중심으로 수업이 운영되었다. 이에 반해 펜테라 기반 실습 과목은 자동화된 공격 시뮬레이션 도구인 펜테라와 SentinelOne을 활용하여, 공격 실행부터 탐지, 대응, 보고서 작성에 이르는 전 주기 기반 실습 구조를 갖춘 것이 큰 특징이다. 또한, 기존 실습에서는 실습 도구의 기능 이해 및 매뉴얼 수행에 초점이 맞춰져 있어 실제 위협 시나리오나 네트워크 내 공격 경로를 체계적으로 학습하기 어려웠던 반면, 펜테라 실습은 MITRE ATT&CK 기반 공격 시나리오를 활용하여 실제 산업 현장에서 발생할 수 있는 침해사고 흐름을 시각적으로 체험할 수 있도록 구성되었다.

학습 방식에 있어서도, 기존은 개인 수행 중심의 정적인 평가 구조였던 데 반해, 펜테라 수업은 조별 협업, 위

〈Table 1〉 Comparison Table: Traditional Security Practice Course vs. Pentera-Based Practice Course

Category	Traditional "System Security Theory & Practice"	Pentera-Based Security Practice Course
Practice Structure	Focused on individual tools (e.g., firewall, IDS)	Scenario-based, full-cycle learning using automated penetration testing
Learning Flow	Tool usage → result interpretation	Attack execution → analysis → response simulation → report writing
Threat Scenario Integration	Static and predefined tasks	Dynamic scenarios based on MITRE ATT&CK framework
Tool Utilization	Manual tools like Nmap, Wireshark	Integrated tools (Pentera + SentinelOne) for end-to-end security
Practice Environment	Individual VMs or local machines	Group-based internal network setup + agent deployment
Learner Activity Type	Individual practice and result reporting	Collaborative problem solving, team reporting, and presentation
Report Use	Screenshot or short-form task reports	Automated reports + visualized analysis and response strategies
Automation Level	Manual configuration and analysis	Automated attack simulation, reporting, and mitigation
Evaluation Method	Assignment submission and exams	Pre-post surveys, rubric-based report grading, participation review
Learning Effect Measurement	Grades and assignment completion	Quantitative (Likert-scale analysis) + qualitative (report/interview)
Industry Relevance	Introductory concept-based learning	Simulated consulting environment with expert feedback

협 탐지 결과 분석, 보안 개선안 도출, 발표 등 문제 해결 중심의 역동적인 학습 방식으로 전환되었으며, 사전·사후 설문조사, 루브릭 기반 보고서 평가, 참여도 피드백 등 다양한 정량·정성 평가 기법이 병행된다.

무엇보다도 펜테라 실습은 보안 컨설팅, 모의해킹, 기업 보안 점검 등과 유사한 경험을 제공함으로써, 학생들이 실제 보안 업무 흐름을 이해하고, 산업체와의 연계성 높은 실무 능력을 체득할 수 있도록 돕는다는 점에서 교육 효과의 우수성이 입증되었다.

실습 효과를 정량적으로 분석하기 위해 사전·사후 설문조사를 실시하였으며, 주요 항목은 보안 인식 수준, 기술 숙련도, 도구 활용 역량, 실무 응용 가능성 등으로 구성되었다. 각 항목은 Likert 5점 척도를 기반으로 응답을 수집하였다.

보안 인식 수준의 경우, 사전 평균 응답은 3.4점이었으며 실습 이후 4.5점으로 향상되었다. 특히 '자동화된 침투 테스트 도구의 필요성'과 '실시간 위협 대응의 중요성'에 대한 인식이 크게 증가하였다. 기술 숙련도의 경우, 사전에는 기초 수준 응답자가 60%를 차지했으나, 사후에는 중급 이상 응답자가 84%로 증가하며 실질적인 기술 역량 향상이 확인되었다.

또한 펜테라와 SentinelOne 도구에 대한 조작 이해도, 공격 결과 해석 능력, 리포트 기반 대응 전략 수립 역량도 눈에 띄게 향상되었다. 설문 항목 중 '실습 경험이 향후 산업체 실무에 도움이 될 것이라고 생각하는가'에 대해 91%의 학생이 '그렇다' 또는 '매우 그렇다'고 응답하였다.

실습 결과물인 팀별 보고서와 발표 자료를 통해 도출된 기술적 분석 내용, 보안 조치 권고안, 대응 시나리오 등은 교육자가 정성적으로 평가하였으며, 대부분의 조가 위협 모델링, 탐지 분석, 보안 설계 역량을 고르게 포함하고 있었다. 특히 일부 조는 SentinelOne 탐지 로그를 활용한 포렌식 분석 관점까지 확장하는 등 고급 수준의 성과를 도출하였다.

4.3 학생 및 전문가 피드백 종합

실습 종료 후 실시한 만족도 조사 및 인터뷰를 통해 학생들은 자동화된 침투 테스트 환경과 실시간 보안 도구의 연계 학습이 실제 현업과 매우 유사했다고 평가하였다. 다수의 학생은 "기존 실습에서는 보기 어려웠던 실제 공격 시나리오를 체험하면서 위협 흐름을 한눈에 이해할 수 있었다"고 응답했으며, "보안 리포트를 직접 해석하고 개선안을 도출한 경험이 가장 실무에 도움이 되었다"는 의견도 있었다. 또한 "SentinelOne을 통해 탐지된 이벤트를 분석하면서 실제 위협 상황을 대응하는 느낌이었다"고 밝힌 학생도 있었다.

보안 전문가들은 본 교육 모델에 대해 "보안 컨설팅, 모의 해킹, 침해 대응 등 실제 기업 업무 흐름과 유사하

〈Table 2〉 Comparative Analysis of Learning Outcomes Using Pentera & SentinelOne-Based Training

Evaluation Category	Pre-Education Avg. (out of 5)	Post-Education Avg. (out of 5)	Improvement Rate (%)
Security Awareness Level	3.4	4.5	+32.4%
Technical Proficiency (Intermediate or Higher)	40%	84%	+110%
Tool Utilization Proficiency	3.1	4.4	+41.9%
Anticipated Applicability to Practice	3.6	4.7	+30.5%

게 구성되어 있으며, 특히 펜테라와 SentinelOne 간의 연계 구조는 실제 실무 환경에서도 사용 가능한 훈련 모델"이라고 평가하였다. 또한 "학생들이 제출한 보고서의 완성도와 분석 관점이 상당히 성숙한 수준이며, 실습 내용을 중소기업 보안진단 컨설팅 프로젝트에 바로 활용 가능한 수준"이라는 의견도 있었다. 이러한 학생 및 전문가의 피드백은 본 교육 모델이 단순한 기술 습득에 그치지 않고, 현장 중심의 융합형 보안 인재 양성에 효과적임을 시사한다.

5. 성과분석 및 정량평가

본 실습의 성과를 정량적으로 평가하기 위해 사전·사후 비교 분석, 실습 결과물 평가, 만족도 조사 결과를 종합하여 분석하였다. 실습에 참여한 35명의 학생 전원을 대상으로 총 4개 영역(보안 인식, 기술 역량, 도구 활용 능력, 실무 적용 가능성)에 대한 변화를 다음 표2와 같이 정리하였다.

이러한 수치는 단순히 기능 습득을 넘어서, 실무에서 활용 가능한 문제 해결력, 도구 분석 능력, 위협 대응 시나리오 이해 수준이 실습을 통해 전반적으로 향상되었음을 의미한다. 또한 팀별 최종 보고서 7건에 대한 정성적 분석 결과, 다음과 같은 기술 역량이 공통적으로 포함되었음을 확인할 수 있었다

·펜테라 리포트를 활용한 위협 탐지 경로 시각화
·SentinelOne 로그 기반 실시간 탐지 결과 분석
·취약점 대응 방안 및 개선 조치 제안
·위협 모델링 도식 및 위험도 등급 평가

교육자는 보고서 완성도, 분석의 깊이, 실무 적용성에 대한 루브릭 기준을 통해 각 팀의 성과를 평가하였으며, 전반적으로 학습 목표와 부합하는 수준의 성과를 도출한 것으로 분석되었다. 특히 2개 조는 포렌식 관점의 대응 로그 분석까지 수행하며, 도구 기반 실습에서 기대 이상의 창의적 확장 능력을 보여주었다.

이러한 결과는 펜테라와 SentinelOne을 병행한 실습 기반 보안 교육 모델이 실무 현장에 가까운 복합적 문제 해결 훈련 환경을 제공하며, 차세대 보안 전문가 양성에 효과적인 접근 방식임을 실증적으로 입증한 사례라 할 수 있다.

6. 결론

본 연구는 펜테라 기반의 자동화 보안 실습 교육 모델을 SentinelOne과 연계하여 설계하고, 이를 백석대학교 정보보호 교육과정에 적용함으로써 학습자의 기술 역량 및 보안 인식 개선 효과를 실증적으로 분석하였다. 실습 참여 학생들은 단순한 도구 활용을 넘어서 실제 보안 사고의 발생 구조와 대응 과정까지 이해하게 되었으며, 교육 종료 후 보안 컨설팅 및 모의 해킹 과제에 적용할 수 있는 수준의 실무 능력을 확보하게 되었다. 전문가 집단으로부터도 해당 교육 모델은 중소기업 보안 진단 프로젝트에 바로 투입 가능한 실전형 훈련 모델이라는 평가를 받았다. 향후 연구에서는 다음과 같은 확장 방향을 제안할 수 있다.

- AI 기반 이상 징후 탐지 시스템(예: EDR 기반 행위 분석 도구)과의 통합 실습을 구성하여 자동화 탐지와 실시간 대응 훈련을 강화할 수 있다.
- 클라우드 기반 보안 환경(예: AWS, Azure 상의 보안 설정, 침해 시뮬레이션)을 포함한 시나리오를 도입하여, 현재 산업 전환 흐름에 부합하는 클라우드 보안 교육을 확장할 수 있다.
- 펜테라 외에도 SafeBreach, Cymulate 등 다양한 공격 시뮬레이션 플랫폼을 비교 분석하여 각 도구의 교육 효과, 적용성, 비용 효율성 등을 종합적으로 연구할 수 있다.
- 산학협력 연계 프로젝트를 통해 중소기업 대상 보안

컨설팅 과제나 보안 인프라 설계 실습을 커리큘럼과 연동함으로써 현장 기반 교육 효과를 더욱 강화할 수 있다.

이러한 후속 연구들은 정보보호 교육의 실무 중심성과 지속 가능성을 더욱 강화하고, 사이버보안 분야에서 요구되는 융합형 전문 인력 양성 체계를 보다 현실적이고 체계적으로 구축하는 데 기여할 수 있을 것이다.

REFERENCES

[1] D. Tymoshchuk, V. Yatskiv, V. Tymoshchuk, and N. Yatskiv, "Interactive cybersecurity training system based on simulation environments," arXiv preprint arXiv:2501.00186, 2024.

[2] J. Vykopal, P. Čeleda, P. Švábenský, and D. Tovarňák, "Scalable learning environments for teaching cybersecurity hands-on," arXiv preprint arXiv:2110.10004, 2021.

[3] D. Tymoshchuk and V. Yatskiv, "Using hypervisors to create a cyber polygon," arXiv preprint arXiv:2501.10403, 2025.

[4] P. Nespoli, M. Albaladejo-González, J. A. Ruipérez-Valiente, and J. Garcia-Alfaro, "SCORPION Cyber Range: Fully customizable cyber exercises," arXiv preprint arXiv:2401.12594, 2024.

[5] SANS & Pentera, "Why security validation matters now: Review of the Pentera platform," SANS Institute White Paper, 2021.

[6] Pentera Inc., "Automated Security Validation Report – ROI Assessment (525–600%)," White Paper, Aug. 2024.

[7] Pentera Inc., "What is Automated Security Validation (ASV)?," https://www.pentera.io/glossary/automated-security-validation

[8] Pentera Inc., "Pentera Platform Datasheet," https://www.pentera.io/resources/platform-datasheet

[9] PeerSpot, "Pentera vs. SafeBreach – User Comparison and Review Insights," https://www.peerspot.com/products/comparisons/pentera_vs_safebreach

[10] Wikipedia, "Pentera (company)," https://en.wikipedia.org/wiki/Pentera

[11] CloudShare, "What is cybersecurity simulation training?," https://www.cloudshare.com/virtual-it-labs-glossary/cyber-security-simulation-training

[12] SANS & Stratejm, "Automated Security Validation – Pentera," Technical White Paper, Nov. 2021.

[13] EM360Tech, "Pentera: Automated Security Validation Platform," White Paper, Jan. 2024.

[14] TheMoonlight.io, "Interactive cybersecurity training system based on simulation environments," https://themoonlight.io/pentera-training-review/

[15] Wikipedia, "CyberCIEGE," https://en.wikipedia.org/wiki/CyberCIEGE

이 근 호(Keun Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
침해사고대응, 융합보안, 개인정보보호, 블록체인, 산업보안, 취약점분석, 모의해킹 등