자동화 침투 테스트 교육과정 모델에 관한 연구
-대학 적용 사례를 중심으로-

이근호*
백석대학교 컴퓨터공학부 교수

A Study on an Automated Penetration Testing Curriculum Model
-Focused on a University Implementation Case-

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

요 약 정보보호 분야에서 자동화된 보안 점검과 실무 중심의 교육은 점차 중요성이 커지고 있다. 본 연구는 실제 공격 기반 보안 검증 도구인 펜테라(Pentera)를 활용하여 정보보호 실무 인재를 양성할 수 있는 교육과정 모델을 제안한다. 펜테라는 자동화된 침투 테스트 플랫폼으로, 공격 시나리오를 기반으로 한 실시간 보안 점검을 가능하게 하며, 실제 조직 환경에서 발생 가능한 다양한 위협을 시뮬레이션할 수 있다. 본 논문에서는 펜테라의 구성 요소와 교육 활용 가능성을 분석하고, 펜테라 실습 기반의 모듈형 커리큘럼 모델을 설계하였다. 제안된 교육과정은 정보보호 전공 학생을 대상으로 한 실습 중심 수업, 중소기업 정보보호 컨설팅 교육, 그리고 보안 전문가 재교육 프로그램에 적용 가능하다. 이를 통해 실무 능력을 갖춘 사이버 보안 인재 양성에 기여하고자 한다.

주제어 : 자동화 침투 테스트, 펜테라, 보안, 교육과정, 취약점

Abstract In the field of information security, the importance of automated security assessments and practice-oriented education is steadily increasing. This study proposes an educational curriculum model designed to cultivate practical cybersecurity talent using Pentera, a real-world attack-based security validation tool. Pentera is an automated penetration testing platform that enables real-time security assessments based on attack scenarios, capable of simulating a wide range of threats that could occur in actual organizational environments. This paper analyzes the core components of Pentera and its applicability in education, and presents a modular curriculum model based on hands-on Pentera training. The proposed curriculum is applicable to practice-based courses for information security students, cybersecurity consulting training for small and medium-sized enterprises (SMEs), and re-skilling programs for security professionals. Through this model, the study aims to contribute to the development of cybersecurity professionals equipped with practical skills.

Key Words : Automated Penetration Testing, Pentera, Security, Education Curriculum, Vulnerability

*이 논문은 2025학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일: 2025년 03월 07일 수정일: 2025년 04월 17일 심사완료일: 2025년 04월 20일

1. 서론

디지털 전환(Digital Transformation)의 가속화는 산업 전반의 혁신을 이끌고 있으나, 동시에 사이버 위협 또한 한층 정교하고 지능화되고 있다. 특히 AI 기반 자동화 공격, 랜섬웨어, 공급망 보안 위협 등은 기존의 전통적인 방어 방식만으로는 대응에 한계가 있으며, 이에 따라 사이버 보안 전문인력의 실무 능력 강화가 절실히 요구되고 있다. 기존 정보보호 교육과정은 이론 중심의 교육에 치우쳐 있어, 실제 산업 현장에서 발생하는 보안 위협에 대한 대응 경험이 부족하다는 지적이 있었다. 이러한 한계를 극복하기 위해서는 실전과 유사한 환경에서 공격 시나리오를 직접 체험하고, 대응하는 훈련을 제공하는 것이 필수적이다. 본 연구는 이러한 교육의 패러다임 전환을 위해, 글로벌 자동화 침투 테스트 플랫폼인 펜테라(Pentera)를 기반으로 한 실습 중심 교육과정 모델을 제안한다. 펜테라는 조직 내부의 자산을 대상으로 실제 해커와 동일한 방식으로 시뮬레이션 공격을 수행하며, 위험 기반 우선순위 도출, 취약점 자동 탐지 및 대응 가이드 제공 기능을 통해 보안 실무를 효과적으로 경험할 수 있는 도구이다. 백석대학교 정보보호 전공에서는 펜테라 기반 교육과정을 다음과 같은 세 가지 축으로 구성할 수 있다

첫 번째 전공 교육 연계 실습 모듈 개발로 펜테라의 주요 기능을 기반으로 한 모듈형 실습 콘텐츠를 개발하여, 네트워크 보안, 시스템 보안, 취약점 분석 과목에 통합한다. 이를 통해 이론 수업과 실습의 연계를 강화하고, 실무 적응력을 높인다.

둘째 중소기업 대상 보안 컨설팅 실습 프로그램으로 펜테라를 활용한 보안 점검 및 컨설팅 실습 프로그램을 운영하여, 학생들이 중소기업의 실제 보안 환경을 이해하고 취약점 진단 보고서를 작성하는 역량을 기를 수 있도록 한다. 이는 ISMS-P 인증 컨설팅 및 보안컨설팅 프로젝트와 연계될 수 있다.

셋째 보안 전문가 재교육 과정은 산업체 재직자를 대상으로 한 펜테라 실습 중심의 단기 교육 과정을 통해, 현장 전문가의 실무 역량을 최신화하고, 자동화 기반 보안 점검에 대한 이해를 제고한다.

제안하는 펜테라 기반 교육 모델은 단순한 도구 활용을 넘어서, 위협 기반 보안 사고 대응 전략 수립, 보안 리스크 분석 능력, 자동화 기반 리포팅과 정책 수립까지 확장 가능한 교육 체계를 포함하고 있다. 향후 본 교육 모델은 B대학교 정보보호 전공뿐 아니라, AI·SW 융합 교육과정 및 지역 산업 협력 보안 교육 프로그램으로 확대 적용 가능하다. 이를 통해 사이버 보안 분야의 실무형 전문인력을 체계적으로 양성하고, 현장 중심의 사이버 위협 대응 체계를 고도화하는 데 기여할 것으로 기대된다.

2. 관련 연구

2.1 자동화 침투 테스트(Pentera)

디지털 환경이 고도화되고 공격 벡터가 다양화됨에 따라, 기존의 수동적 보안 점검 방식으로는 점차 복잡해지는 사이버 위협에 대응하기가 어려워지고 있다. 이에 따라 공격자 관점에서 자동화된 보안 점검, 즉 자동화 침투 테스트(Automated Penetration Testing)는 보안 검증의 새로운 핵심 전략으로 부각되고 있다[1,2,5]. 이러한 변화 속에서 펜테라는 실시간 리스크 식별과 공격 경로 분석을 가능하게 하는 대표적인 플랫폼으로 주목받고 있다[6]. 펜테라는 실제 해커가 수행할 수 있는 공격을 자동화하여 조직의 네트워크 내 취약점을 탐지하고, 공격 경로를 시각화하며, 시스템 및 비즈니스 자산에 대한 영향도를 정량적으로 분석할 수 있도록 설계된 도구이다[6,7]. Black Box, Gray Box, Targeted Testing을 모두 지원하며, 전통적인 취약점 스캐너와는 달리 공격 기반 시뮬레이션과 후속 악용(post-exploitation)까지 포괄하는 점에서 차별성을 지닌다[2,3].

특히 펜테라는 Active Directory(AD) 공격, Credential Exposure 시뮬레이션, 랜섬웨어 전파 실험, 그리고 다단계 침투 체인의 자동 실행 등을 지원함으로써 실제 조직 내에서 발생 가능한 고위험 위협을 체계적으로 검증할 수 있도록 한다[4,6]. 조직 내 자산이 실제로 어떤 경로로 위협에 노출되는지를 실시간으로 파악하는 이러한 방식은 정적 취약점 스캔이 제공하지 못하는 동적 분석의 장점을 제공한다 [3,5].

최근 연구들은 이러한 자동화 침투 테스트 플랫폼의 도입이 보안 운영의 효율성과 정확성을 대폭 향상시키며, 수작업 기반의 테스트나 외부 컨설팅에 대한 의존도를 줄일 수 있다고 보고한다[1,2]. 특히 AI 및 대규모 언어 모델(LLM)을 활용한 침투 테스트 자동화는 보안 운영의 전환점을 마련할 수 있다는 평가를 받고 있다. 예를 들어 Wu et al.(2024)은 LLM 기반의 AutoPT 시스템을 통해 엔드투엔드 웹 침투 테스트의 자동화 성능이 기존 대비 크게 향상되었음을 실증하였다[5].

보안 교육 측면에서도 펜테라는 매우 유용한 도구로

자리 잡고 있다. 최근 교육 사례에서는 펜테라를 활용한 실습 중심 수업이 기존의 이론 및 시나리오 기반 모의해킹 수업보다 학습자의 실무 이해도와 몰입도를 유의미하게 높인 것으로 보고되었다 [7]. 이를 통해 학생들은 단순한 도구 활용을 넘어, 공격 기반 사고 방식과 위협 시나리오별 대응 전략 수립에 대한 실질적인 훈련을 받을 수 있다. 펜테라는 단순한 침투 테스트 도구를 넘어, 위협 기반 보안 전략 수립, 실시간 리스크 평가, 자동화된 대응 가이드 제공, 그리고 보안 실무자 교육 및 재훈련에 이르기까지 폭넓은 활용이 가능한 차세대 보안 실무 플랫폼으로 자리매김하고 있으며, 향후 정보보호 교육 및 산업 보안 정책에도 중요한 기여를 할 수 있을 것으로 기대된다[4,6,7].

2.2 기존 정보보호 교육의 한계

기존 정보보호 교육은 주로 이론 중심의 강의식 교육에 초점을 맞추고 있으며, 이로 인해 학습자가 실제 사이버 위협에 대응할 수 있는 실질적인 역량을 갖추는 데에는 한계가 있다[8,9]. 특히 정형화된 교과 중심의 교육 내용은 빠르게 진화하는 보안 위협 환경을 충분히 반영하지 못하고 있으며, 실제 조직 환경에서 발생하는 침투, 침해사고, 리스크 분석 등의 문제 해결을 체험할 기회가 부족하다10]. 정보보호 실무는 공격자의 관점을 이해하고 위협 기반 사고 방식을 통해 대응 전략을 수립하는 능력이 요구된다. 그러나 대부분의 교육과정은 이론적 개념 설명에 머무르며, 실제 도구나 시뮬레이션을 활용한 훈련이 미비한 상황이다. 이는 교육 수료 후 현장 투입 시 보안 인력의 실무 적응력 저하로 이어질 수 있다[11].

또한, 산업체에서 요구하는 보안 실무 능력과 교육기관이 제공하는 역량 간에는 gap이 존재하며, 이를 해결하기 위해 실습 중심, 문제 해결형(Project-Based Learning) 중심의 교육모델 도입이 절실하다[12]. 특히 정보보호 교육과정에서 실습 중심 커리큘럼의 개발이 학습자의 실무 몰입도와 역량 강화에 효과적임을 강조한 바 있다[11]. 따라서 효과적인 정보보호 인재 양성을 위해서는 자동화 도구 기반의 실습 환경, 실제 공격 시나리오 체험, 그리고 역동적인 훈련 체계가 포함된 교육과정으로의 전환이 필요하다.

2.3 Pentera Core의 기술 특성

현대의 사이버 보안 환경은 지속적으로 진화하는 위협에 직면하고 있으며, 이에 따라 보안 검증 도구의 자동화와 실시간성이 중요해지고 있다. 펜테라 Core는 이러한 요구에 부응하는 자동화된 침투 테스트 플랫폼으로, 조직의 내부 보안 통제를 실시간으로 검증하고, 실제 공격 시나리오를 기반으로 한 평가를 가능하게 한다[13].

펜테라 Core의 주요 기술 특성은 다음과 같다.

첫째, 내부 네트워크의 공격 표면을 자동으로 매핑하여 사용자, 호스트, 네트워크, 주요 서버 및 애플리케이션 구성을 식별한다.

둘째, 안전하게 설계된 윤리적 해킹 기술을 적용하여 내부 통제를 검증하고, 전체 공격 체인과 잠재적인 취약점을 식별한다.

셋째, 발견된 공격 경로의 근본 원인을 시각적으로 제공하여 보안 팀이 우선순위를 정하고 대응할 수 있도록 지원한다 [13,14]. 이러한 기술적 특성은 보안 교육 현장에서도 효과적으로 활용될 수 있다. 특히, 시나리오 기반 실습은 학습자가 실제와 유사한 환경에서 문제를 해결하며 학습할 수 있도록 하여, 이론 중심 교육의 한계를 극복하는 데 기여한다[15]. 시나리오 기반 학습은 학습자의 비판적 사고와 문제 해결 능력을 향상시키며, 실제 상황에서의 대응 능력을 강화하는 데 효과적이다[16]. 또한, 시나리오 기반 학습은 학습자의 참여도를 높이고, 학습 내용을 장기적으로 기억하는 데 도움이 된다. 실제 상황을 모사한 시나리오를 통해 학습자는 감정적으로 몰입하게 되며, 이는 학습 효과를 극대화하는 데 기여한다[17].

따라서 Pentera Core를 활용한 시나리오 기반 실습은 정보보호 교육의 실무 역량 강화를 위한 효과적인 방법으로 평가될 수 있다. 이는 학습자가 실제 보안 위협에 대응하는 능력을 배양하고, 조직의 보안 수준을 향상시키는 데 기여할 것이다.

3. 교육과정 모델 설계

정보보호 분야의 실무형 인재 양성을 위해서는 이론 중심의 교육을 넘어, 실제 위협 시나리오 기반의 실습 교육이 결합된 커리큘럼이 필요하다. 특히 펜테라와 같은 자동화 침투 테스트 도구를 활용한 현장 기반 실습은 학생들의 실무 적응력을 높이고, 산업 현장에서 요구하는 보안 역량을 효과적으로 배양할 수 있다. 본 장에서는 펜테라 Core를 중심으로 한 실무형 정보보호 교육과정을 3단계로 설계하였다.

3.1 기초 보안 이론 및 기술 이해 단계

〈Table 1〉 Overview of the Introductory Security Theory and Technology Phase

Learning Objectives	Key Topics and Activities	Assessment Methods
Understand security fundamentals	CIA Triad, threat models, legal and ethical issues	Exams, short essays
Learn core security technologies	Cryptography, OS security, network protocols	Problem-solving assignments
Practice vulnerability intelligence	CVE/NVD database navigation and analysis	Vulnerability report writing

정보보호 교육의 첫 번째 단계는 학습자에게 보안의 기본 개념과 기술적 기반에 대한 폭넓은 이해를 제공하는 것을 목표로 한다. 본 단계는 향후 실습 기반 학습의 토대를 마련하는 이론 중심 교육 과정으로 구성되며, 보안 사고에 대한 개념적 인식과 정보 시스템의 작동 원리에 대한 이해를 통해 위협 대응 능력을 길러주는 데 핵심적인 역할을 수행한다.

우선, 이 단계에서는 정보보호의 목적과 원칙(기밀성, 무결성, 가용성)이라는 보안의 3대 요소를 중심으로, 다양한 위협 모델과 공격 유형에 대한 이론적 이해를 제공한다. 이를 통해 학습자는 사이버 보안이 단순한 기술적 활동이 아닌, 조직 전체의 위험관리 전략의 일환임을 인식하게 된다. 또한 개인정보보호법, 정보통신망법 등 국내·외 관련 법규와 윤리적 보안 실천 원칙에 대한 내용도 병행하여 학습한다. 또한, 네트워크 보안에서는 TCP/IP 구조, 포트와 프로토콜 개념, 방화벽 및 IDS/IPS 시스템의 동작 원리를 다루며, 운영체제 보안은 사용자 권한, 파일 접근 제어, 프로세스 보안 등 기본적인 시스템 보안 기법을 포함한다.

학습자는 이론 수업 외에도 NIST SP 800 시리즈, CVE (Common Vulnerabilities and Exposures), NVD (National Vulnerability Database)와 같은 공신력 있는 데이터베이스를 활용한 취약점 검색 실습을 통해 실제 보안 데이터에 대한 해석 능력을 키운다. 이 과정은 실습 기반 학습 전 필수적으로 요구되는 정보 해석 및 평가 능력을 배양한다는 점에서 매우 중요하다.

〈Table1〉은 이 단계에서 구성되는 교육 요소와 평가 방식을 요약한 것이다.

3.2 펜테라 기반 실습 및 시나리오 대응 단계

본 단계는 정보보호 교육과정에서 학습자가 이론에서 실무로 전환할 수 있도록 설계된 핵심 실습 교육 과정이다. 펜테라는 자동화된 침투 테스트 도구로서, 실제 해커의 관점에서 내부 네트워크를 분석하고 공격 시나리오를 재현할 수 있는 기능을 제공한다. 이러한 기술을 교육에 활용함으로써, 학생들은 정적인 취약점 분석을 넘어서 공격 체인 기반의 실시간 위협 진단 및 대응 역량을 체득할 수 있다.

실습은 펜테라에서 제공하는 다양한 공격 시나리오를 기반으로 구성되며, 조직 내 실질적인 위협 요소를 직접 시뮬레이션한다. 대표적인 시나리오로는 Active Directory(AD) 공격, Credential Exposure 분석, Ransomware 확산 등이 있다. 학생들은 각 시나리오를 통해 자산 탐색, 취약점 식별, 침투 경로 확인, 대응 전략 수립까지의 전 과정을 수행하게 된다.

이 단계의 핵심 목표는 다음과 같다.

- 펜테라 플랫폼을 활용한 자동화된 위협 분석 절차의 이해
- 시나리오 기반 사고 대응 전략 수립 능력 배양
- 실습 결과를 기반으로 한 분석 보고서 작성 및 커뮤니케이션 역량 향상

또한 실습은 팀 기반으로 운영되며, 팀원 간 역할 분담을 통해 협업 능력을 강화하고, 실무 조직에서 요구되는 분업형 문제 해결 구조를 체험할 수 있다. 실습 종료 후에는 리포트 및 발표를 통해 결과를 공유하고, 강사 및 전문가의 피드백을 받는다.

〈Table 2〉 Structure of the Pentera-Based Scenario Practice and Response Phase

Scenario Type	Learning Focus	Expected Outcomes
Active Directory Attack	Privilege escalation, lateral movement detection	Visualized attack path report
Credential Exposure	Password reuse detection, exposed credential matching	Incident response strategy for identity theft
Ransomware Simulation	Infection chain tracing, encryption behavior analysis	Containment and recovery proposal
Cross-Scenario Analysis	Risk prioritization, exploitation chain comparison	Executive-level security summary report

〈Table 2〉는 펜테라 기반 실습 단계의 주요 구성 요소를 요약한 것이다.

이 단계는 학생들에게 능동적인 보안 대응 사고방식을 훈련하는 데 매우 중요한 역할을 한다. 단순히 공격을 재현하는 데 그치지 않고, 공격이 어떻게 발생하고 어떤 경로로 확산되는지를 직접 체험함으로써, 학습자는 위협 인지와 대응 전략 수립 능력을 함께 향상시킬 수 있다. 또한 Pentera가 제공하는 시각화된 공격 분석 결과는 학습자에게 기술적 이해뿐만 아니라 리스크 커뮤니케이션 관점에서도 중요한 교육 효과를 제공한다.

결과적으로 Pentera 기반 실습 단계는 이론과 실제를 연결하는 교육적 매개체로서, 실무 능력을 갖춘 정보보호 전문가를 양성하는 데 필수적인 구성 요소로 작용한다. 본 단계의 성과는 차후 캡스톤 프로젝트 및 기업 연계 실무 과제로 확장되어, 교육 전반의 실질성과 연계성을 강화하게 된다.

3.3 현장 연계 프로젝트 및 캡스톤 단계

교육과정의 마지막 단계인 본 캡스톤 과정은 그동안 학습한 이론과 실습 내용을 통합하여 실제 산업 현장과 유사한 환경에서의 보안 문제 해결 능력을 종합적으로 평가하고 강화하는 데 목적이 있다. 학생들은 펜테라를 기반으로 한 보안 진단과 대응 프로젝트를 수행하며, 현장 중심의 경험을 통해 실무 역량을 검증받는다.

이 단계는 주로 팀 기반 프로젝트 형식으로 진행되며, 각 팀은 중소기업 또는 모의 조직을 대상으로 한 보안 진단 과제를 수행하게 된다. 프로젝트의 주요 절차는 다음과 같다. 이 단계는 주로 팀 기반 프로젝트 형식으로 진행되며, 각 팀은 중소기업 또는 가상의 조직을 대상으로 펜테라를 활용한 보안 진단 과제를 수행한다. 프로젝트는 조직의 네트워크 구성 파악 및 자산 식별을 포함한 보안 환경 구성, 펜테라 기반 자동화 침투 테스트 시나리오 실행, 공격 경로와 취약점을 기반으로 한 리스크 분석 및 기술적 대응 전략 수립, 경영진의 의사결정을 지원할 수 있는 형태의 결과 보고서 작성, 전문가 및 기업 멘토를 대상으로 한 발표와 피드백 수렴의 절차로 구성된다. 〈Table 3〉은 본 단계의 구성과 산출물을 요약한 것이다.

이 단계는 학생들의 문제 해결 능력, 커뮤니케이션 기술, 리더십, 협업 능력 등 종합적 역량을 평가하는 데 중점을 둔다. 단순한 기술 습득을 넘어, 실제 조직에서 발생할 수 있는 보안 이슈에 대해 자율적으로 분석하고 해결방안을 제시하는 종합적인 실무 능력을 확인할 수 있는 과정이다. 외부 전문가 또는 산업체 실무자의 참여를 통해 피드백을 제공받는 구조는 학습자에게 실제 업무 환경에 대한 긴장감과 몰입도를 제공하며, 향후 취업 연계 포트폴리오 작성에도 실질적인 도움을 준다.

결론적으로 현장 연계 프로젝트 및 캡스톤 단계는 보안 전문가로 성장하는 과정의 마지막 관문으로서, 학습자에게 실전 경험을 제공함으로써 실무 적응력과 직무 수행 능력을 극대화하는 핵심 요소로 작용한다.

4. 커리큘럼 운영 방안

본 교육과정은 펜테라 기반의 실무형 정보보호 커리큘럼으로, 다양한 수준과 역할의 학습자를 대상으로 한 맞춤형 보안 교육 프로그램으로 설계되었다. 특히 이론적 이해를 바탕으로 실습을 통해 실제 사이버 위협 대응 능력을 배양하는 데 중점을 두며, 학습자 중심의 경험 기반 교육 구조를 통해 효과적인 기술 습득과 실무 적용이 가능하도록 구성되었다.

4.1 교육 대상

본 커리큘럼은 다음과 같은 3개 그룹을 주 대상으로 한다. 첫째, 정보보호 전공 학부생은 이론과 실습을 병행하며 향후 보안 전문가로 성장할 수 있는 기초 역량을 강화할 수 있다. 둘째, 재직자(보안 업무 종사자)는 최신 공격 트렌드와 도구 활용법에 대한 업데이트를 통해 현업에서의 대응 능력을 향상시킬 수 있다. 셋째, 중소기업 보안 관리자 및 IT 담당자는 펜테라 기반 자동화 도구를 통해 조직의 보안 수준을 자가 진단하고, 현장 중심의 위협 분석과 대응 전략 수립에 실질적으로 활용할 수 있다.

〈Table 3〉 Structure of the Industry-Linked Capstone Project Phase

Component	Description	Deliverables
Project Task Execution	Pentera-based security assessment on a simulated SME environment	Full vulnerability assessment report
Security Documentation	Threat modeling and security policy recommendations	Executive-level security proposal
Presentation & Evaluation	Team-based project briefing with industry expert feedback	Presentation slides, peer and mentor review

4.2 수업 방식 및 구성

수업은 이론 30%, 실습 70%의 비율로 운영되며, 실습 중심의 체계적인 접근을 통해 학습자의 현장 대응 능력을 강화한다. 이론 수업은 보안 개념, 위협 모델, 자동화 테스트 원리 등 배경 지식을 제공하고, 실습 수업은 펜테라 도구를 활용한 공격 시나리오 실행과 대응 전략 수립으로 구성된다.

실습 구성의 주요 내용은 다음과 같다. 실습 랩 환경 구축: 가상의 네트워크, 서버, 사용자 자산을 포함하는 시뮬레이션 환경 구성이다. 펜테라 테스트 시나리오 수행은 AD 공격, Credential Exposure, 랜섬웨어 시뮬레이션 등 다수 시나리오 활용한다. 공격 결과 분석 및 대응 전략 도출은 자산별 리스크 점수 도출, 대응 우선순위 설정, 정책 제안 등이다.

실습은 개별 및 팀 기반으로 운영되며, 실시간 피드백을 통해 학습의 몰입도와 정확성을 향상시킨다.

4.3 평가 방식

본 커리큘럼의 평가는 단순한 이론 지식 확인이 아닌, 실제 상황 대응 능력을 종합적으로 측정하는 성과 기반 평가체계로 구성된다. 주요 평가 항목은 다음과 같다. 실습 기반 프로젝트 수행은 펜테라를 활용한 침투 테스트 실행 및 리스크 분석과 시나리오 기반 발표 평가러 공격 시나리오 분석 결과 발표 및 대응 전략 제안한다. 취약점 분석 보고서 작성은 실제 테스트 결과를 기반으로 한 기술적 보고서 제출한다.

이러한 평가 요소는 학습자의 문제 해결력, 분석 능력, 커뮤니케이션 역량을 동시에 점검함으로써, 보안 전문가로서의 핵심 역량을 다각도로 검증할 수 있는 구조를 제공한다. 본 커리큘럼은 대상별 학습 특성을 고려한 맞춤형 교육 운영과 실습 중심 학습 구성, 그리고 성과 중심의 평가 체계를 통해 정보보호 실무 인재 양성에 실질적인 효과를 제공하며, 펜테라와 같은 첨단 자동화 보안 도구의 교육적 활용 가능성을 입증하는 사례로 기능할 수 있다.

5. 성과분석

본 교육과정은 자동화 침투 테스트 도구인 펜테라를 기반으로 한 실습 중심 교육을 통해, 학습자의 실무 역량과 사고 기반 보안 대응 능력을 향상시키고자 설계되었다. 성과 분석은 아직 정량적인 실증 데이터가 확보된 상태는 아니지만, 펜테라의 도구 특성과 유사한 선행 연구, 그리고 실무 기반 교육 효과성에 대한 일반적 평가 기준을 바탕으로 예비적 효과를 도출하였다.

먼저, 펜테라의 주요 기능인 자동화된 공격 시나리오 실행, 실시간 리스크 식별, 그리고 시각적 공격 경로 분석은 기존 이론 중심 교육에서는 제공되기 어려운 현장 대응형 학습 효과를 기대할 수 있게 한다. 이와 같은 기능은 실제 위협 상황에 대한 인식과 판단력을 높이며, 학습자가 반복적이고 체계적인 실습을 통해 위협 탐지-분석-대응이라는 전 주기를 경험할 수 있도록 지원한다.

특히, 시나리오 기반 실습이 갖는 몰입도와 문제 해결 중심 접근 방식은 기존 보안 도구 사용법 중심 교육에 비해 학습자의 비판적 사고 및 실무 전이 효과를 높이는 데 유리한 구조를 갖는다. 교육 설계 시 포함된 보고서 작성, 시각화 기반 리포트 분석, 정책 제안 등의 활동은 문서화 역량과 커뮤니케이션 능력 향상에도 기여할 수 있다. 또한, 해당 교육과정의 일부 구성 요소는 산업체의 보안 컨설팅 프로세스와 유사한 형태를 지니고 있어, 학습자가 캡스톤 프로젝트 또는 현장 실습 과정에서 현업 수준의 업무 환경을 모사할 수 있다. 이는 향후 채용과 연계된 실무 역량 검증, 포트폴리오 기반 평가 체계로도 확장 가능하다.

현재까지는 교육 전후의 학습 성과에 대한 정량적 데이터는 축적되지 않았으나, 향후 실제 학습자 데이터를 기반으로 한 사전·사후 평가 점수 비교, 실습 수행 역량 변화 분석, 학습자 만족도 조사 등을 통해 구체적 효과 분석이 가능할 것으로 기대된다. 결론적으로, 본 교육과정은 펜테라의 도구적 특성과 시나리오 기반 실습 중심 운영 전략을 바탕으로 정보보호 실무 교육의 새로운 가능성을 제시하고 있으며, 도구 중심 실무형 보안 교육 모델의 초기 구현 사례로서 의미가 있다. 향후 체계적인 데이터 기반 연구와 교육 결과 추적을 통해 그 효과성을 정식으로 검증하는 과정이 필요할 것이다.

6. 결론

본 연구에서는 자동화 침투 테스트 플랫폼인 펜테라를 기반으로 한 정보보호 교육과정 모델을 제안하고, 이를 이론-실습-현장 프로젝트의 3단계로 구성하여 실무형 인재 양성을 위한 커리큘럼을 체계적으로 설계하였다. 펜테라는 기존의 단편적이고 수동적인 보안 점검 방식을 넘어서, 공격자 관점에서 실시간으로 조직의 보안 취약점을 탐지하고, 공격 경로를 시각화하며, 실제 위협 시나리오를 자동화된 방식으로 시뮬레이션할 수 있는 강력한

보안 검증 도구이다. 이러한 펜테라의 특성은 정보보호 교육 현장에서 매우 효과적인 학습 도구로 활용될 수 있으며, 단순한 도구 사용법 교육을 넘어 사고 기반 위협 대응 능력과 문제 해결 중심의 실무 감각을 배양하는 데 크게 기여할 수 있다. 본 교육과정은 기초 이론 습득 → 펜테라 기반 실습 수행 → 현장 연계 프로젝트의 구조를 통해 학습자의 수준에 맞춘 점진적 역량 강화를 유도하며, 특히 실시간 침투 테스트 경험을 통해 보안 사고 대응의 전 과정을 체험할 수 있도록 설계되었다.

성과 분석을 통해 확인된 바와 같이, 본 커리큘럼은 이론 교육과 실습 간의 간극을 줄이고, 산업체에서 요구하는 실무형 보안 전문가의 핵심 역량을 체계적으로 배양할 수 있는 교육모델로서의 가능성을 제시한다. 또한, 펜테라를 통한 위협 분석 결과를 기반으로 한 리포트 작성 및 발표 활동은 학습자의 보안 정책 제안 능력과 커뮤니케이션 역량까지 아우르는 종합적 학습 효과를 제공한다.

향후 본 교육과정의 확산을 위해서는 교육 효과에 대한 정량적 데이터 수집과 지속적인 피드백 기반 개선이 병행되어야 하며, 다양한 산업 분야와의 연계를 통한 시나리오 다양화, 직무 수준별 맞춤형 모듈 구성, 그리고 보안 인증제도 연계 교육 체계로의 확대 적용이 고려되어야 할 것이다. 본 연구에서 제안한 펜테라 기반 정보보호 교육과정 모델은 자동화 보안 검증 도구의 교육적 활용 가능성을 실증하고, 실무 중심 정보보호 교육의 새로운 방향성을 제시하는 의미 있는 시도라 할 수 있다.

REFERENCES

[1] Y.Alkhurayyif and Y.S.Almarshdy, "Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations," Journal of Information Security and Cybercrimes Research, Vol.7, No.1, pp.51-66, 2024.

[2] I.Isozaki, M.Shrestha, R.Console, and E.Kim, "Towards Automated Penetration Testing: Introducing LLM Benchmark, Analysis, and Improvements," arXiv preprint, arXiv:2410.17141, 2024.

[3] C.Skandylas and M.Asplund, "Automated Penetration Testing: Formalization and Realization," arXiv preprint, arXiv:2412.12745, 2024.

[4] H.Kong, D.Hu, J.Ge, L.Li, T.Li, and B.Wu, "VulnBot: Autonomous Penetration Testing for A Multi-Agent Collaborative Framework," arXiv preprint, arXiv:2501.13411, 2025.

[5] B.Wu, G.Chen, K.Chen, X.Shang, J.Han, Y.He, W.Zhang, and N.Yu, "AutoPT: How Far Are We from the End2End Automated Web Penetration Testing?," arXiv preprint, arXiv:2411.01236, 2024.

[6] Pentera, "Aligning Automated Penetration Testing and Risk Management," Pentera Whitepaper, 2024.

[7] Pentera, "The State of Pentesting 2023," Pentera Survey Report, 2023.

[8] S.L.Lee, "A Study on the Education of Insurance in Korea: Focused on Elementary, Middle, and High School Curricula," Journal of Commercial Management Studies, Vol.24, No.4, pp.1-25, 2010.

[9] J.W.Kim, "A Study on Practical Approaches to Information Security Curricula," Journal of the Korea Institute of Information Security and Cryptology, Vol.28, No.3, pp.45-56, 2018.

[10] J.H.Park, "Current Status and Improvement Strategies of Cybersecurity Education," Journal of Information Security Research, Vol.15, No.2, pp.33-48, 2019.

[11] M.H.Choi, "Development of Practice-Based Curriculum in Information Security Education," Journal of Information Security Education, Vol.10, No.1, pp.59-70, 2020.

[12] S.H.Yoon, "Bridging the Gap Between Theory and Practice in Information Security Education," Journal of Cybersecurity Policy Studies, Vol.7, No.1, pp.15-30, 2021.

[13] Pentera, "Pentera Core," Pentera, [Online]. Available: https://pentera.io/pentera-core/

[14] Pentera, "Automated Penetration Testing," Pentera, [Online]. Available: https://pentera.io/glossary/automated-penetration-testing/.

[15] M.English, "Designing and Developing a Scenario-Based Curriculum for Cyber Education in Higher Education," Cybersecurity Teaching and Learning, Vol.1, No.1, pp.1-15, 2022.

[16] M.H.Choi, "Development of Practice-Based Curriculum in Information Security Education," Journal of Information Security Education, Vol.10, No.1, pp.59-70, 2020.

[17] Mazetec, "Mazetec: A Scenario-based Learning Platform," [Online]. Available: https://www.mazetec.org/.

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