산업융합연구 제20권 제3호 pp. 23-31, 2022
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2022.20.3.023

보안 전문 인력 양성을 위한 정보보안 수업 개선 방안 - 특성화 과정을 중심으로

박중오
성결대학교 파이데이아학부 조교수

Information Security Class Improvement Plan to Cultivate Security Professionals - Focusing on Specialization Course

Jung-Oh Park
Assistant Professor, Division of Paideia, Sungkyul University

요 약 최근 사이버공격 등을 방어하기 위한 보안 전문인력 양성에 대학 정보보안 학과의 역할의 중요성이 나날이 높아지고 있다. 현재 대학 보안 교육과정은 이론 교육에 비중이 높고 실무 교육의 전문성이 비교적 떨어진다는 문제점이 존재한다. 본 연구는 보안학과의 실무 능력 개선을 목적으로 최근 국/내외 외부 보안 교육기관의 교육 프로그램을 분석하였고, 핵심 특성화 과정에 적절한 수업 모델을 설계하고 방향성을 제시한다. 제안 모델은 기존 문제점인 기초수업 연계 및 보안 실무 교육과정 로드맵을 개선하고, 핵심 5가지 특성화 과목의 실습 프로그램을 추가 설명한다. 본 연구는 각 대학 보안학과 수업 과정의 질과 교육 모델의 개선에 이바지하고자 한다.

키워드 : 정보보안, 보안실습, 대학교육, 보안학과, 정보보호

Abstract Recently, the importance of the role of the university information security department in nurturing security experts to defend against cyber attacks is increasing day by day. The current university security curriculum has a problem in that the proportion of theoretical education is high and the professionalism of practical education is relatively low. This study analyzed the recent educational programs of domestic and foreign security education institutions for the purpose of improving the practical ability of the Department of Security, designing a class model suitable for the core specialization process, and suggesting the direction. The proposed model improves the existing problems of basic class connection and security practice curriculum roadmap, and additionally explains the practice program of the five core specialized subjects. This study intends to contribute to the improvement of the quality of the curriculum and educational model of each university's security department.

Key Words : Information Security, Security Practice, College Education, Security Department, Information Protection

1. 서론

국내 고등 교육기관으로써 대학은 교육 질적 수준을 확보해야 하는 책임이 있으며 전문인력 양성을 통해 우수 학생을 배출하는데 그 중요성이 높다. 공과대학 정보보안학과는 IT에 관련된 광범위한 지식과 교육과정의 확실한 방향성과 세부 프로그램에 체계적인 계획이 요구된다. 서경진(2015), 박기태(2016), 양정모(2018) 등은 앞선 연구에서 정보보호 전문가 양성을 위한 국내 대학의 보안학과 표준 모델 및 세부 프로그램 개발의

*Corresponding Author : Jung-Oh Park(pjo21@naver.com)
Received January 19, 2022 Revised February 25, 2022
Accepted March 20, 2022 Published March 28, 2022

필요성을 설명했다[1-3]. 대학에서 컴퓨터를 활용한 정보검색 및 S/W 활용은 필수이며, 교육자나 대학생 모두 우수한 인력 양성에 목적이 있다[4]. 보안 분야는 시스템/네트워크, 웹 보안, 악성코드 분석가, 포렌식 전문가, 침해대응, 취약점 점검 등 다양한 세부 특성화 과정이 존재한다. 송정호(2016)는 국가직무표준 능력(NCS)의 보안 세분류가 명확하지 않아 교육과정에 재설계가 필요하다고 설명했다[5]. 정진효(2019)는 대학 보안학과의 수업 관계 분석 결과, 교육 영역이 상이하며 수업 사이의 공통적 요소가 크게 부족하다고 분석했다[6]. 고등 교육기관의 보안학과는 대체로 수업 모델이 아직 정형화 초기 단계로써, 해결해야 할 문제점들이 많다.

본 연구는 대학 보안 수업 모델 개선과 실습수업 과정의 질적 향상 등을 위해 실무 전문가를 특성화하는 수업 모델과 세부 실습 프로그램 과정을 개발한다. 본 논문의 구성은 다음과 같다. 2장 기존 보안 전문인력 양성 연구를 분석하고, 직종별 특성화에 필요한 실무 교육과정 현황을 살펴본다. 3장은 실무과정 중심의 전체 보안 과정 로드맵과 핵심 수업 항목별 세부 프로그램 과정을 설명한다. 4장 결론 및 논의로 끝낸다.

2. 선행연구

2.1 보안 전문인력 양성 연구분석

Table 1은 최근 5년 이내 구글 학술 검색(2017년 이후) 보안 전문인력 양성을 위한 연구를 비교 분석한 결과이다[7-11].

Table 1. Comparison of Security Expert Training Studies

Author	Feature	Problem
Park. J. S	Fostering human resources in the industrial security field	Limitations of Inclusive Teaching Methods
Lee. M. G	Training of information security experts	Classification of practical courses is not clear
Park, W. H	Improvement of NICE-based educational subjects	Absence of theoretical/practical linkages
Kim. C. B	Improvement of curriculum for lower grades	For security awareness training
Kim. S. J	Industrial Security Curriculum Improvement	Absence of detailed curriculum

기존 공학 계열 수업 과정의 기본(컴퓨터 구조, 운영체제 등)도 분류되는 수업 분류를 제외하고, 보안 수업 과정을 중심으로 나타난 주요 문제점은 다음과 같다. 첫째, 보안 수업의 범위가 제한적이고 세부 수업 과정이 명확하지 않았다[7,8]. 둘째, 전체 수업 과정의 흐름 연계와 실무 중심의 수업 과정의 비중이 부족한 문제점이다[9,10]. 셋째, 세부 프로그램이 명확하지 않아 보안 수업의 질이 떨어질 수 있다는 것이다[11]. 이는 실제 강의를 진행하는 교육자의 전문성에 의존적일 수밖에 없다.

본 연구는 선행연구로써 외부 기관에서 공개된 교육과정들을 조사하고, 어떤 보안 특성화 직종이 많이 다뤄지고 있는지 분석했다.

2.2 보안 실무 교육과정 현황 분석

Table 2는 2021년 기준 온/오프라인으로 운영 중인 보안 실무 교육기관을 나타낸다[12-17].

Table 2. Security Practical Training Curriculum Status

Institution	Training Course	Education Target
Korea Internet & Security Agency	Cultivating the most elite information security experts	Only companies and employees that have signed an agreement can apply
Korea Information Security Education Center	Customized 1:1 training process, job-related process	Training for a small number of people by curriculum
Korea Information Technology Research Institute	Academy - Information Security Field, Systematic Curriculum	Education for non-employment insurance subscribers and major employees
Korea Information Security Industry Association	Job creation support project, training new professional manpower	Locally limited, training for a small number of people
Global IT Human Resources Development Institute	Hacking, information system, ICT information security training	Job seekers, unemployed, college graduates
Korea Information and Education Institute	Cultivation of next-generation cloud (core technology talent)	For job seekers/workers

교육과정은 단기/장기 교육과정, 국가에서 전액을 지원하거나 일정 금액을 지급하는 민간 교육기관으로 분류된다. 수업 과정에 거주 지역과 취업준비생이나 직장인 대상 등 조건부로 수강할 수 있어 일반인은 수강하는데 진입 장벽이 존재했다. 단기 전문과 과정(39시간 이하)이고, 수업 내용이 비공개인 웹사이트는 조사 대상에서 제외했다.

대학 수업은 15주에 기준 중간/기말을 제외하고 3시간(또는 5시간) 수업 기준 39시간에서 최대 65시간이다. 외부 교육기관은 장기 수업 과정(65시간 이상)이 다수 존재했지만, 이는 이론/기초 이론과 실습을 포함한 시간으로 기존 대학 수업 모델과 큰 차이점이 없음을 확인했다. 교육자는 시간 내에 이론/실습 비중을 조정해야 하는데, 앞서 분석한 결과와 같이 실습의 전문성과 비중이 부족하므로 본 연구의 수업 모델에서는 이를 보완해야 할 필요성이 있다고 분석했다.

2.3 보안 전문가 직종 분석

Table 3은 앞서 분석한 전체 교육과정에서 주요 전문가 직종을 직접 키워드로 추출하고, 중첩되는 항목을 공통 직종으로 분류한 결과이다. 대체로 외부 기관들도 대학 보안 실습 과정에서 일반적인 시스템/네트워크/웹 보안 수업을 진행한다는 공통점을 확인했다.

Table 3. Specialization of Security Experts(by job type)

Institution	Course(Specialization)
Korea Internet & Security Agency	Digital forensics, malicious code analysis, breach response, mock hacking, security consulting
Korea Information Security Education Center	Digital forensics, malicious code analysis, web simulation hacking, vulnerability diagnosis, breach response
Korea Information Technology Research Institute	Digital forensics, S/W security, information security infrastructure, simulated hacking, infringement response
Korea Information Security Industry Association	System/Network Security, Digital Forensics, Malicious Code Analysis, Infringement Response, Security Control
Global IT Human Resources Development Institute	System/network security(basic, advanced), mock hacking, intrusion response
Korea Information Security Education Institute	System/network security, S/W security, security control

특성화 과정 추출 결과, 핵심 5가지(디지털 포렌식, 악성코드 분석, S/W 보안, 시스템/네트워크 보안, 모의해킹/침해대응) 항목이 정의되었다. 디지털 포렌식 과목은 보안학과에서 비중은 적지만 최근 새롭게 도입되고 있는 과목이다. 보안관제와 취약점 진단은 보안 전 분석 과정에서 다뤄지는 내용이기 때문에 추가 항목에서 제외했다.

3. 보안 수업 모델(실습수업 중심)

3.1 수업 로드맵 및 수업 모델

핵심 5가지 항목은 대학 기초수업에서 다루는 컴퓨터 구조, 운영체제, 정보보호개론(기본개념), 암호학(대수학 포함)이나 프로토콜(TCP/IP, 보안 프로토콜 등)과 같은 이론 과목의 학습이 선행되어야 한다. 교육부(학위수여 및 학력인정) 지침 기준으로 학사는 140학점 이상(교양 30학점 포함) 전공필수/선택 이수 점수가 약 110학점이 요구된다[18].

본 연구는 핵심 로드맵의 설계에 3학점 기준 이론/실습 포함 최대 35개 수업 진행을 가정했다. 표 4는 각 학년에서 필요한 1/2학기 수업 과정 연계를 나타낸다. 핵심 5가지 항목을 중심으로 1/2학기 학과의 이론/실습 교과목을 연계 및 재편성했다. 총 35개의 과목은 1학년 기초과정 이후 2, 3학년 과정의 기본/심화 과정과 4학년 프로젝트 과정으로 구분된다. 나머지 6개 수업 과정을 분배하여 1~3학년에 데이터베이스와 서버 과목과 연계되는 빅데이터와 보안, 데이터 분석(파이선), 인공지능 보안(1, 2)을 추가했다. 인공지능 분야(과학기술정보통신부)는 현재 교육 초기 단계이지만 고등교육기관에서 기계학습과 인공신경망 교육을 위한 핵심 교육 항목(차세대 S/W)으로 정의되어 추진되고 있다[19].

S/W나 악성코드 및 해킹을 분석하기 위해서는 데이터 패턴 분석 과목의 이해가 필수이다. 시큐어 코딩 과목 이외에, 4가지 핵심 과목은 해킹 분석(네트워크 보안), 모의 해킹(웹 보안), 해킹 방어(시스템 보안), 해킹 추적(포렌식)과정으로 상호 작용한다.

Table 4. Theory/Practice Course Roadmap by Grade

1	Class Course (1/2 Semester)	
	general mathematics	Cryptography
	Computer Science(Intro)	information security(Intro)
	Information and Communication(Intro)	Network protocol
	Programming(C)	Web programming (HTML/JavaScript)
	Programming(Python)	Database theory/practice
Beginning of Semester: Fundamental Theory and Language Focus		
2	Class Course (1/2 Semester)	
	Advanced programming (C++/JAVA)	**Secure Coding(JAVA)**
	Web Programming (JSP)	Web Security Basics (Code Analysis)
	Operating System Theory/Practice	System Security(Security Settings)
	Network Security(Security Protocols)	**Network Security(hacking analysis)**
	Web server construction/operation	Web Server Vulnerability Analysis
	Data Analysis(Python)	Big Data and Security

Table 4. Continued

Composition of practice-oriented subjects		
3	Class Course (1/2 Semester)	
	System Security Advanced(Hacking Defense)	Artificial Intelligence Security 2(Deep Learning)
	Artificial Intelligence Security 1(Machine Learning)	**Web Security Advanced(Hacking Test)**
	Basics of Malware Analysis (Introduction and Pattern Analysis)	Advanced malware analysis(PE, binary analysis)
	Advanced Programming (Assembler)	**Advanced digital forensics(S/W practice)**
Graduation Semester: Project-Based Classes (Specialization Choice)		
4	Common: Security Project (1/2 Semester)	
	Forensic case analysis	Forensic Investigation/Report
	S/W vulnerability analysis	S/W Vulnerability Defense
	Malware analysis	Malware Defense
	Hacking Technique Analysis	Hacking Technique Defense
	System/Network Analysis	System/Network Defense

수업 방법을 개선하는 방법은 연구자 스스로 수업에 적용하고, 직접 문제점을 찾아 개선하는 과정이 필수적이다. Table 5와 같이 S/W를 활용하는 실습수업을 중심으로 각 과목의 필요 요구사항은 다음과 같다.

Table 5. Requirements for Developing Instructional Programs

	Description
Education Method	Rational model
Educational Goals	Specialized Subject, Practical Skills
Class Progress	Partial repetition learning based on practice
Class Check	Check class progress
Class Evaluation	Quantitative/Qualitative Evaluation
S/W Selection	Popular, Universal
Practical Use	Security standards, Security guides, etc
Topic Classification	Specialization Subject(Override)

본 연구는 기본 교육 모델로써 실습 과정에서 확실하고 예측할 수 있는 목표를 달성을 추구하는 합리적 모델을 기반으로 한다[20]. 특성화 과목의 적절한 반복 실습으로 실무 경험을 쌓고, 부분 목표를 달성해 나가는 교육 모델로써 실습수업에 적합하다. 수업 모델의 방향성은 수업을 진행하는 교육자와 수업을 듣는 학생의 입장으로 구분하여 정의했다.

교육자 : 수업 목표 설정은 수업의 난이도(기본/심화)와 교육자의 역량에 따라 차이가 존재할 수 있다. Table 6은 추출된 5가지 대표 과목에 대한 수업 목표의 예를 나타낸다.

Table 6. Practical Security class Training goal Example

	Description
Secure Coding	Vulnerable code analysis and safe coding
Network security	Network attack detection and defense
System security	System hacking analysis and defense
Web security	Web vulnerability code analysis and defense
Digital forensics	Data analysis and tracking

보안 실습수업(기본/심화)에서 공통으로 추출할 수 있는 요소는 크게 2가지로 나눠진다. 첫 번째 기본 수업 과정에서 내용을 이해하고 분석할 수 있는가, 두 번째 심화 수업 과정에서 이에 대응하고 해결할 수 있는가에 중점을 둔다. 박원형은 2017년 기준 NICE 기반 실무 교육과정 분석 연구 결과, 전 수업 과정이 단계별로 기초, 공격, 방어 또는 대응 과목으로 구분됨을 분석했다[21].

본 연구의 분석과 같이 공격 및 방어/대응을 위한 실습 진행이 주요 핵심 과정임을 알 수 있다. 교육자는 실습수업 시작에 앞서 완성형 형태의 수업 자료를 제공한다. 완성형 형태의 자료는 학습자가 자료를 참고하여 정상적인 실습을 진행할 수 있는 전 과정을 포함한 수업 자료를 의미한다. 실습 진행이 교육자에 의존(장 의존적)하게 되면 수업의 시간적 효율성이 낮고, 수업의 질(주입식 교육 문제)이 크게 떨어질 수 있다[22].

학습자 : Table 7과 같이 앞서 정의(Table 4)한 선행 과목의 수업이 필수이고, 수업 주마다 실습 주제의 기본개념부터 세부 내용에 대한 이해를 위해서 교육자와 학습자의 상호작용이 중요하다. 기본 실습 진행은 학생 개인/그룹 사이에서 주도적으로 진행하지만, 실습 단계의 질의/응답을 유도하고 예외 상황은 교육자가 주도하여 빠르게 해결하는 방식으로 진행한다.

Table 7. Example of class Progress and Output

	Description
Class basics	Prerequisites, subject understanding
Practice progress	Step-by-step, Student-led
Practice Results	Check normal operation and results
Practice Detail 1	Analyze the result(vulnerability)
Practice Detail 2	Solve the output result(weak point)
Question/Answer/ Exception	Whole class, Educator-led

학습자는 정확한 실습 과정을 단계별로 진행해야 하고, 실습 완료 후에 결과가 명확해야 한다. 세부 1, 세부 2로 크게 분리하여 분석/해결 방법을 반복 학습한다. 단계별 결과 확인이 중요한 이유는 수업의 진행률과 매주 실습 진행 위치 파악이다. 진행 상황을 정확히 파악하는 것은 중요하다. 실습 진행이 다소 느리거나 이해가 부족해도 수업 집중력과 추진력을 끝까지 유지하기 위해서이다. Table 8은 교육자가 수업 진행 중에 학습자를 위한 수업 점검 사항을 나타낸다.

Table 8. Class Checklist Example

	Description
Learning Objectives	Practice items 1 to n(step by step)
Class material	Includes theory and practice(all courses)
Practice/Troubleshooting	Total Student Practical Success Percentage
Individual/collaborative	Inducing interaction
Q & A	Overall question frequency
Lecture time	Time Distribution/Speed Control

예) 3시간 수업 기준 수업 시작 단계에서 10~15분 이내 주차 별 간단한 이론적 배경과 문제점 등을 전달한다. 주제 설명은 학습자들의 전공과 나이에 적합한 관련 동향 분석이 수업 흥미 유발에 효과적이다. 교육자는 시간마다 실습 단계별로 학생들의 성공 비중을 확인하여 수업 진행 속도를 조절해야 한다. 이외 실습 분석과 문제해결에 그룹으로 협력하여 진행할 수 있음을 강조하고, 질의/응답을 적극적으로 유도한다. Table 9는 학습자의 성취도 평가 방법에 대한 예를 나타낸다.

Table 9. Class Evaluation Method Example

	Description	
quantitative evaluation	Written/Practice Test	Mid/Final
	Practice Detail 1(Analysis)	Report
	Step-by-step practice results	
qualitative evaluation	Class participation/Q&A	Check every class
	Analysis/Trouble shooting	Report
	Exercise Detail 2(Solved)	

수업 평가는 일반적인 정량/정성 평가를 혼합했다. 일반적인 평가 방법은 중간/기말시험과 보고서 등이 있다. 중간/기말시험을 통해서 이론적인 기반 이해도(실습 세부 1)를 평가하고, 보고서를 통해 실습 경험(실습 완료 상태)을 평가할 수 있다. 이외 수업 참여도와 보고서의 추가 문제해결에 세부 내용을 정성 평가(실습 세부 2)한다. 이는 학습자 각자 해석하는 의미가 다르고, 해결방안이 다양하게 나타날 수 있기 때문이다. 수업 참여도의 경우 실제 수업에서 항상 실습을 착실히 진행하고, 질의/응답을 적극적으로 요청하는 학습자에 대한 수시 체크가 필요하다.

Fig. 1은 앞서 설명한 교육 목표, 실습수업, 수업 점검부터 진행 및 평가까지 전체 모델 구조 및 연계 과정을 나타낸다.

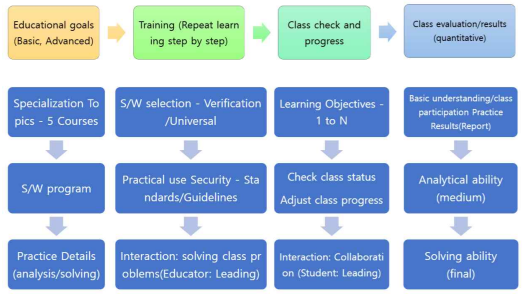

Fig. 1. Education Model Structure and Linkage Process

3.2 수업 별 실습 프로그램(세부)

Table 10-14는 핵심 5가지 특성화 과정(시큐어 코딩, 네트워크 보안, 시스템 보안, 웹 보안, 포렌식)에서 기초과정 이후(심화 기준) 주차 별 주제와 세부 실습 프로그램의 예를 나타낸다. Table 5의 요구사항으로 대표적인 S/W 유무, 보안 표준 등 실무 적합성을 고려하고, 특성화 과목별로 세부 실습 항목을 재정의했다.

Table 10. Secure Coding(JAVA)

week	Class Content	Detailed Course
1	Introduction to Secure Coding	-
2	Guide Introduction and Basic Practice	Explore Secure Coding
		Introduction to how to use the integrated IDE
3	Input data validation and representation	SQL Injection, Command Injection, XSS(Cross-site Scripting)
4		XQuery, XPath, LDAP Attack, Relative Path Traversal
5		System and External Control, Process Control, Unsafe Reflection
6	Security features	Authentication and Authorization settings, Weak Passwords, Plain Text Storage, Hard code Passwords
7		Key length/random Number Value, Cookie Information exposure, Comments, Hash function Problems

Table 10. Continued

week	Class Content	Detailed Course
8	Midterm exam	-
9	Security features	Integrity Check, Session Setup, Password Management, Multiple Connections
10	Time and Status	Race Condition, Recursive Function, Direct use of Thread, Symbolic Name Problem
11	Exception handling	Error Messages and Exception Handling, null Pointers, Resource Release, Infinite loop
12	Code error	Incorrect Code Handling Issue
13	Encapsulation	Invalid Session, Public Class, Debug Code, Time information Exposure
14	API misuse	DNS lookups, Connection/Socket Management, Comparison Operators
15	Etc	Using Overloaded Methods, Serialization Methods, Synchronization Methods
16	Final exam	-

행정안전부의 시큐어 코딩 가이드, CERT 오라클 보안 코딩 표준(JAVA) 취약점 항목(중복 제거)을 재정의했다[23,24]. 자바 이외 C, C++ 등 보안 가이드를 참고하여 세부 항목에서 삽입 공격, 암호 알고리즘과 취약성 등 중첩되는 항목을 통합했다. 통합 IDE 이클립스(Eclipse) 또는 비주얼 스튜디오(Visual Studio) 등을 사용한다[25,26]. 이외 핵심 도구로써 취약점 분석에 NIST 인증 분석 도구인 Find Security Bugs(네이티브 코드), OWASP ZAP(웹 환경)을 수업에 활용했다[27,28].

Table 11. Network Security(Hacking Analysis)

week	Class Content	Detailed Course
1	Introduction to network Security	-
2	Introduction to the protocol and basic practice	OSI7 layer and TCP/IP protocol
		Introduce how to use wire-shark
3	Traffic capture and analysis	Website - Explore different Protocols
4	Wireshark packet analysis (default protocol)	TCP/UDP - structures, flows, handshakes, etc
5		HTTP/HTTPS - Basic, Secure, Handshake, etc
6		SSL/TLS - normal/abnormal patterns, performance issues, etc
7		ARP Scan, ICMP Ping, TCP Port Scan
8	Midterm exam	-
9	Wireshark packet analysis (scanning detection)	UDP port, IP protocol, idle scan, ICMP code
10		Traceroute route, dynamic router detection, application mapping process
11		OS fingerprinting, spoofing address identification
12	Wireshark Packet Analysis (Anomalous Traffic Analysis)	Vulnerabilities in the TCP/IP resolution process (port, name, MAC, etc)
13		Find maliciously altered packets, identify 'unknown' destination addresses
14		Flooding and standard denial of service traffic, text passwords and data discovery
15		Abnormal protocols and applications, ARP contamination, IP fragmentation and overwriting
16	Final exam	-

리눅스 운영체제 배포판에서 네트워크 해킹 실습에 특화된 칼리 리눅스(Kali Linux)를 활용한다[29]. 해킹 공격 스크립트를 직접 실행하고, 세부 분석을 위해 패킷 분석 도구 와이어샤크(WireShark)를 활용한다[30]. 실습과 함께 분석 시간에 많은 시간이 필요한 과목이다. 분석 난이도로 인해 세부 항목 이해에 중급 난이도 이상의 보조 교재를 추가 활용했다[31,32].

Table 12. System Security(Hacking Practice)

week	Class Content	Detailed Course
1	Introduction to network Security	-
2	Operating system introduction and basic practice	Operating System Structure and Kernel Analysis
		Kali Linux Building/operating
3	System information collection	CVE/CCE Vulnerability
		Scanning operating system key information(services, ports, etc)
4	Diagnosing vulnerabilities	Using vulnerability diagnosis S/W
		Vulnerability discovery through Nessus(Windows/Linux)
5	vulnerability attack	Understanding key vulnerability attacks
6		Utilize metasploit scripts
7		MySQL and PostgreSQL
		Utilize metasploit scripts
		Tomcat and PDF
		Utilize metasploit scripts
8	Midterm exam	-
9	Elevation of Privilege Attack	Understanding Elevation of Privilege Attacks
10		Authentication token and local authority
11		Data transfer and Characterization
		Payload delivery and trace removal
		Security Protocol Analysis
		man-in-the-middle attack(MITM)
13	password attack	Understanding Brute Force Attacks
		Online password attack, HTTP password cracking
14		Windows Password Structure Analysis
		Windows Password Cracking (John the Ripper)
15		Other Password Attacks
		Advance Attack and the Rainbow Table
16	Final exam	-

네트워크 보안에서 사용된 리눅스 운영체제 배포판 칼리 리눅스를 공통 활용한다. 주요 실습이 대표적인 해킹 도구(네서스, 메타스플로잇, 존 더 리퍼 등)와 터미널에서 직접 명령어 스크립트를 활용한다[33-35]. 앞서 특성화 과정인 네트워크와 웹 보안 실습이 중복되는 부분을 제거하고 시스템 해킹을 위한 실습 항목으로 새롭게 정의했다. 주요 세부 항목 정의에 중급 난이도 이상의 보조 교재를 추가 활용했다[36,37].

Table 13. Web Security (Hacking Practice)

week	Class Content	Detailed Course
1	Web Security Advanced Introduction	-
2	Execution Environment and Basic Practice	Introduction to OWASP, Setting up the practice environment
3	Damn Vulnerable Web App(DVWA) - Hacking 1	Brute Force
4		Command Injection
5		CSRF(XSRF)
6		File Inclusion(RFI, LFI)
7		File Upload
8	Midterm exam	-
9	Damn Vulnerable Web App(DVWA) - Hacking 2	Insecure CAPTCHA
10		SQL Injection
11		SQL Injection(Blind)
12		Weak Session IDs
13		XSS(DOM)
		XSS(Cross-site Scripting)
14		XSS(Reflected)
15		XSS(Stored)
16	Final exam	-

웹 보안 고급 실습은 해킹 스크립트 실행 환경을 위해 공격을 수행할 수 있는 환경이 요구된다. 칼리 리눅스 배포판 기반에 대표적인 웹 모의 해킹 환경인 Damn Vulnerable Web App(DVWA)를 활용했다[38]. DVWA는 실제 OWASP TOP 10의 웹 취약점을 코드 수준에서 세부 옵션을 테스트할 수 있다.

Table 14. Digital Forensics(S/W Practice)

week	Class Content	Detailed Course / Practice Program
1	Introduction to Digital orensics	-
2	Forensic Tools and Basic Practices	Create temporary drives, image disks, check devices
		FTK_Imager, Hwinfo64
3	Window system	Information such as systems, multimedia, tasks, networks, etc
		systeminfo, msinfo32, dxdiag, BCEDIT, tasklist, netstat
4	Windows memory 1	Dump Memory
		notmyfault64, LiveKD, Dump it, FTK Imager
5	Windows memory 2	Memory Analysis
		Volatility(image_info), Dump it
6	Windows registry	Registry Analysis
		regedit & Rega(Hive File), Volatility(image_info)
7	File system analysis	File System Analysis
		Winhex(BR, MFT)
8	Midterm exam	-
9	Restoring files and disks 1	Disk Recovery
		Winhex & NTFS Log Tracker(LogFile, UsnJrnl, File Signature)
10	File and Disk Restore 2	Partitions and files Recover
		Winhex(Partition), Hxd, FTK_Imager, NTFSWalker, Recuva(File)
11	Windows Artifact 1	Window Event, Slack Space & shadow, Job scheduler
		Logs, Winhex, Shadow Explorer, taskschd, TaskSchedulerView
12	Windows Artifact 2	Jump List, Prefetch
		Winhex, Recent, JumpLister, win_prefetch_view(Prefetch)
13	Windows Artifact 3	cache, reycycle, usb, sticky
		Winhex, Regedit, thumbnail cache viewer
14	Web artifacts	Web Browser(cache, history, cookie, Download list
		Google chrome, Mozilla firefox, Internet explorer
15	Forensic incident reporting	Forensics Practice Report
		Forensic Analysis Report(Digital Forensics Center)
16	Final exam	-

디지털 포렌식 관련 통합 프로그램은 무료 또는 교육 전용 버전이 없다. 대표적인 상용화 버전인 ENCASE 또는 FTK의 포렌식 소프트웨어 등은 유료 라이선스(Licence)를 구매해야 한다. 통합 실습 프로그램이 없으므로 각 주 수업마다 다양한 무료 프로그램(Table 14 내에 표기)을 활용해야 한다. 윈도 기반 실행되는 무료 해킹 도구와 칼리 리눅스 기반 포렌식 도구를 모두 활용한다. 최종 산출물로는 검찰에서 제공하는 표준 포렌식 보고서 양식으로 포렌식 관련 사건 정리하는 과정으로 끝마친다[39].

4. 결론 및 논의

고등 교육기관은 모든 분야에 걸쳐 정형화된 수업 체계를 개발/개선하고 양질의 수업을 제공하는데 큰 비중을 두어야 한다. 최근 대학 수업이 온라인 강좌나 유튜브 등 온라인 교육 플랫폼과 차별성이 크게 없어진다면, 코로나 사태 이후 대학 수업의 부정적인 인식은 더욱더 가속화될 가능성이 크다. 본 연구는 앞서 연구분

석을 통해 대학 보안 수업 과정의 설계 및 수업 관계, 공통 요소 부족 등 다양한 문제점을 분석했다. 이에 대한 해결책으로 보안 전문인력 기관을 분석하여 실무과정에 적합한 특성화 항목을 추출하고, 해당 교과목에 개선된 교육 모델과 실무과정 프로그램을 세부 설명했다. 표 15는 제안 모델의 문제점 개선사항을 나타낸다.

Table 15. Improvement of problems in the proposal model

Problem	Suggested Improvements
Limitations of Inclusive Teaching Methods	Rational model-based, step-by-step iterative learning
Classification of practical courses is not clear	Definition of Security Department's 5 Core Courses
Absence of theoretical/practical linkages	Linked application of basic/advanced learning classes by grade level
For security awareness training	Class content: greatly expanded the proportion of hands-on classes
Absence of detailed curriculum	Detailed program definition, S/W and textbooks, etc.

코로나 사태에 따른 온라인 원격 수업의 비중이 증가하고 있다. 공학 계열의 모든 실습수업은 대부분 전용 S/W를 활용하는데, 전체 수업의 진행 상황이나 학생 개인의 실습 상태, 문제 발생 시 해결의 어려움 등 실습수업의 시작부터 끝까지 사실상 교육자에 대부분 의존하게 된다. 기존의 보안 실습수업 계획은 온라인 수업에 적절하게 재구성될 수 있다. 그러나 학생의 주도적인 수업 진행을 위해서는 온라인 실습수업을 위한 전용 S/W가 필요하다.

향후 확장 연구로써, 실시간 화상 회의, 강의 자료 작성 및 S/W 내부 파일 로딩, UI 구성 및 실습수업 상태 확인 등 공개 소스 API를 활용하는 방법을 계획하고 있다. 본 제안 연구는 정형화된 수업 모델로써 실습 프로그램 개발에 필요한 선행연구로써 활용할 수 있을 것이다.

REFERENCES

[1] K. J. Seo, J. E. Choi & H. W. Kim. (2015). An Exploratory Study on Development of Information Security Manpower. *Journal of Association Of Information Systems, 24(2),* 73-96. DOI : 10.5859/KAIS.2015.24.2.73

[2] K. T. Park, H. J. Jun & T. S. Kim. (2016). A Study on the Cybersecurity Workforce Training Program Development by Level of a Characteristic of Training Program. *Journal of Information Technology Applications & Management, 23(4),* 127-138. DOI : 10.21219/JITAM.2016.23.4.127

[3] J. M. Yang. (2018). A Study on Development of Standard Modeling Education Program in Information Security : Focusing on Domestic University Cases. *Journal of Convergence Security Association, 18(5),* 99-104.

[4] S. M. JIN, L. W. DING, D. R. LIU & H. Y. LI. (2020). Research on Training Strategy of Information Technology Application Ability of Normal University Students. *International Journal of Advanced Science and Convergence, 2(4),* 17-24. DOI : 10.22662/IJASC.2020.2.4.017

[5] J. H. Song & H. R. Kim. (2016). A Study on the NCS based Curriculum for Educating Information Security Manpower. *Journal of the Korea Academia-Industrial cooperation Society, 17(11),* 537-544. DOI: 10.5762/KAIS.2016.17.11.537

[6] J. H. Jung & C. M. Jung. (2019). An Analysis of Industrial Security Curriculum's in Colleges. *Journal of Society for e-Business Studies, 24(2),* 29-53. DOI : 10.7838/jsebs.2019.24.2.029

[7] J. S. Park. (2019). A Study on the Improvement of Curriculum for Human Resources Development in the Industrial Security. *Journal of Association for Industrial Security, 9(1),* 141-163.

[8] M. G. Lee. (2017). A Development of Curriculum for Information Security Professional Manpower Training. *Journal of the Institute of Electronics and Information Engineers, 54(1),* 46-52. DOI : 10.5573/ieie.2017.54.1.046

[9] W. H. Park & S. J. Ahn. (2017). Enhancing Education Curriculum of Cyber Security Based on NICE. *KIPS Transactions on Computer and Communication Systems, 6(7),* 321-328. DOI : 10.3745/KTCCS.2017.6.7.321

[10] C. B. Kim. (2020). An Analysis of Information Security Curriculum in Elementary School practical arts, Secondary School Informatics Teaching and Suggestions for Improvement. *Journal of Society of Computer and Information, 25(10),* 69-75. DOI : 10.9708/jksci.2020.25.10.069

[11] S. J. Kim & Y. H. Jung. (2020). A Study on the Improvement of Industrial Security Curriculum Based on Industrial Demand: A Survey on IPA for Industrial Security Officers. *Journal of Korean Industrial Security, 10(3),* 169-186. DOI : 10.33388/kais.2020.10.3.169

[12] Korea Internet & Security Agency. Annual training at KISA Cyber Security Talent Center, Cyber Security Manpower Training (K-Shield) Regular Course, Retrieved from http://academy.kisa.or.kr

[13] Korea Information Security Education Center. KISEC Information Security Expert Course, Retrieved from https://www.kisec.com

[14] Korea Information Technology Research Institute. KITRI Academy - Security Field, Retrieved from http://academy.kitri.re.kr

[15] Korea Information Security Industry Association. KISIA Talent Support Education Project - Security, Retrieved from https://www.kisia.or.kr

[16] Global IT Human Resources Development Institute. Global IT - National-based strategic training, Retrieved from http://www.gith.co.kr

[17] Korea Information Security Education Institute. Cloud Security Expert Training Course, Retrieved from http://www.keduit.com

[18] Ministry of Education. Guidelines for business processing related to credit recognition, etc. [Ministry of Education Notification No. 2021-9, 2021.2.19., partially revised], Retrieved from https://www.moe.go.kr

[19] E. S. Jang. (2020). A Case Study on the Operation of Artificial Intelligence in a Liberal Arts Mandatory Curriculum, *Journal of General Education, 14(5),* 137-148.
DOI : 10.46392/kjge.2020.14.5.137

[20] R. W. Tyler. (2013). *Basic principles of curriculum and instruction.* University of Chicago press.

[21] W. H. Park & S. J. Ahn. (2017). Enhancing Education Curriculum of Cyber Security Based on NICE. *KIPS Transactions on Computer and Communication Systems, 6(7),* 321-328.
DOI : 10.3745/KTCCS.2017.6.7.321

[22] M. J. Choi & D, Y. Jeong. (2013). A Study on Effect of the Cognitive Style of Field Dependence/Independence to the Information-Seeking Behavior of Undergraduate Students. *Journal of the Korean Society for Library and Information Science, 47(1),* 125-147.
DOI : 10.4275/KSLIS.2013.47.1.125

[23] Ministry of Public Administration and Security. Secure Coding Guide(C, Java), Retrieved from https://www.mois.go.kr/

[24] Oracle. The CERT Oracle Secure Coding Standard for Java, Retrieved from https://www.oracle.com/

[25] Eclipse Foundation. Eclipse IDE, Retrieved from https://www.eclipse.org/

[26] Microsoft. Microsoft Visual Studio, Retrieved from https://visualstudio.microsoft.com/

[27] Philippe Arteau. FindSecurityBugs, Retrieved from https://find-sec-bugs.github.io/

[28] OWASP. OWASP® Zed Attack Proxy, Retrieved from https://www.zaproxy.org/

[29] OffSec Services. Kali Linux, Retrieved from https://www.kali.org/

[30] Wireshark Foundation. Wireshark, Retrieved from https://www.wireshark.org/

[31] C. Sanders. (2017). *Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems.* Seoul : acorn Publishing.

[32] L. Chappell, (2014). *Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide. Problems.* Seoul : acorn Publishing.

[33] Tenable. Nessus, Retrieved from https://www.tenable.com/

[34] Metasploit. Metasploit Tools, Retrieved from https://www.metasploit.com/

[35] Openwall. John the Ripper, Retrieved from https://www.openwall.com/john/

[36] Willie L. Pritchett. (2014). Kali Linux Cookbook. Seoul : acorn Publishing.

[37] L. Allen. (2015). *Kali Linux - assuring security by penetration testing :master the art of penetration testing with Kali Linux(2nd ed.).* Seoul : acorn Publishing.

[38] DVWA. Damn Vulnerable Web App, Retrieved from https://dvwa.co.uk/

[39] Digital Forensic Center. (Investigation form) Evidence analysis(Appendix No. 11 form), Retrieved from http://cfpa.or.kr/

박 중 오(Jung-Oh Park) [정회원]

· 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
· 2003년 3월 : 명지대학교 전자계산교육 석사
· 2011년 8월 : 숭실대학교 컴퓨터공학 박사
· 2016년 3월~현재 : 성결대학교 조교수
· 관심분야 : PKI, Network security, 암호학
· E-Mail : pjo21@naver.com