결재	전공주임	교학부장

수 업 계 획 서

< 2017학년도 8월 21일 ~ 12월 8일 >

1. 강의개요

학습과정명	침해대응실습	학점	3	교강사명		교강사 전화번호	
강의시간	5시간	강 의 실		수강대상	정보보호	E-mail	

2. 교육과정 수업목표

침해사고 발생에 따른 침해 대응의 필요성과 개념을 이해하고, 방화벽, 침입탐지시스템, 통합보안시스템 등을 학습하여 침해 대응 기술을 습득한다. 또한 네트워크 기반의 패킷 및 IDS/IPS 등 보안 장비의 위협 로그의 효율적 분석 방법을 실습을 통해 학습한다.

3. 교재 및 참고문헌

주교재	보안 분석가의 사이버침해사고 분석 전략	저자	송대근	출판사	에이콘	출판년도	2016
부교재(참고문헌)		저자		출판사		출판년도	

4. 주차별 강의(실습·실기·실험) 내용

주별	차시	강의(실습·실기·실험) 내용	과제 및 기타 참고사항
제 1 주	1 2 3 4 5	**1] 강의주제: 보안 위협과 보안 시스템** **2] 강의목표: 보안 위협 및 관련 보안 시스템 이해** **3] 강의세부내용:** **① 애플리케이션 취약점** **② 지능형 지속 공격(APT)** **③ 네트워크 침입탐지 시스템** **④ 호스트 기반 침입탐지 시스템** **4] 수업방법: 강의 및 토론(질의/응답)**	o 학습자료: 주 p.21 ~ p.39 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 2 주	1 2 3 4 5	**1] 강의주제: 침해 정보 수집** **2] 강의목표: 패킷, 시스템 관련 침해 정보의 이해** **3] 강의세부내용:** **① 패킷 페이로드의 이해** **② 세션 정보 수집** **③ 시스템 정보 수집** **④ 보안 인텔리전스** **4] 수업방법: 강의 및 실습**	o 학습자료: 주 p.40 ~ p.54 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 3 주	1 2 3 4 5	**1] 강의주제: 침입 차단/탐지 정책** **2] 강의목표: 분석 기본 지식 습득** **3] 강의세부내용:** **① 전문 침해 대응** **② 네트워크, 데이터베이스** **③ 침입 차단 및 탐지 시스템의 이해** **④ 스노트 시그니처 학습** **4] 수업방법: 강의 및 실습**	o 학습자료: 주 p.55 ~ p.108 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 4 주	1 2 3 4 5	**1] 강의주제: 분석 도구** **2] 강의목표: 분석 도구의 이해 및 사용법 습득** **3] 강의세부내용:** **① 패킷 분석 도구** **② 파일 분석 도구** **③ 취약점 스캐너** **4] 수업방법: 강의 및 실습**	o 학습자료: 주 p.109 ~ p.122 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드 **o 과제: 침입차단시스템, IDS, IPS, 통합보안시스템 등 네트워크 보안 시스템 현황 조사**
제 5 주	1 2 3	**1] 강의주제: 보안 위협 이벤트 분석** **2] 강의목표: 침해사고 대응 절차의 이해** **3] 강의세부내용:**	o 학습자료: 주 p.124 ~ p.174 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드

	4 5	① 분석 방법론(임계치, 시그니처) ② 방화벽, IDS, IPS 등의 로그 수집 ③ 위험 확인 및 영향도 분석 ④ 대응방안 수립, 결과 공유와 의사 결정 4] 수업방법: 강의 및 토론(질의/응답)	
제 6 주	1 2 3 4 5	1] 강의주제: 공격 흔적 찾기 I 2] 강의목표: 휘발성 증거의 이해 및 분석 방법 습득 3] 강의세부내용: ① 세션 정보의 수집 ② 세션별 실행 파일 ③ 사례 분석 ④ 세션 테이블 리스트 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.175 ~ p.182 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 7 주	1 2 3 4 5	1] 강의주제: 공격 흔적 찾기 II 2] 강의목표: 프로세스 증거 이해 및 분석 방법 습득 3] 강의세부내용: ① 프로세스 정보의 수집 ② 실전 사례 ③ 프로세스와 네트워크 ④ 기타 로그 분석 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.182 ~ p.222 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 8 주	1 2 3 4 5	중 간 고 사	**[필기시험]** **(객관식:1점 20문항,** **주관식:2점 5문항,** **총30점)**
제 9 주	1 2 3 4 5	1] 강의주제: 공격 경로 분석 2] 강의목표: 공격 경로 분석 능력 함양 3] 강의세부내용: ① 방화벽, IPS, IDS 등 네트워크 정보 수집 ② 세션 재구성 및 타임 테이블 분석 ③ 실전 훈련 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.223 ~ p.246 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 10 주	1 2 3 4 5	1] 강의주제: 피해 분석 I 2] 강의목표: 사용자 계정 및 애플리케이션 분석 3] 강의세부내용: ① 사용자 및 관리자 계정 점검 (Windows) ② 사용자 및 관리자 계정 점검 (Linux) ③ 실전 사례 분석 ④ 애플리케이션 분석 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.247 ~ p.272 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드 **o 과제: 최근 해킹 사고 동향 조사**
제 11 주	1 2 3 4 5	1] 강의주제: 피해 분석 II 2] 강의목표: 파일 점검 3] 강의세부내용: ① 공유 목록 점검 ② 파일 접근 검색 ③ 백업 및 시스템 파일 점검 ④ 보안 설정 점검 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.273 ~ p.293 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 12 주	1 2 3 4 5	1] 강의주제: 피해 분석 III 2] 강의목표: 실전 능력 함양 3] 강의세부내용: ① 사전식 대입 공격 ② 실 사례 실습 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.294 ~ p.298 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 13 주	1 2 3	1] 강의주제: 윈도우 레지스트리 분석 2] 강의목표: 레지스트리의 이해 및 분석 기술 함양 3] 강의세부내용:	o 학습자료: 주 p.299 ~ p.322 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드

	4 5	① 레지스트리 추출 ② 삭제 레지스트리 추출 ③ 레지스트리 분석 4] 수업방법: 강의 및 실습	
제 14 주	1 2 3 4 5	1] 강의주제: 통합 모니터링 환경 구축 2] 강의목표: 통합 보안 시스템 구축 기술 습득 3] 강의세부내용: ① 보안 대응 범위 정의 ② 침입차단시스템/침입탐지시스템 설정 ③ 웹방화벽 설정 ④ 통합 보안 모니터링 구축 4] 수업방법: 강의 및 실습	o 학습자료: 주 p.323 ~ p.338 o 기자재: 실습용PC, 빔 프로젝터, 스크린, 화이트보드
제 15 주	1 2 3 4 5	기 말 고 사	[필기시험] (객관식:1점 20문항, 주관식:2점 5문항, 총30점)

5. 성적평가 방법

중간고사	기말고사	과 제 물	출 결	기 타	합 계	비 고
30 %	30 %	15 %	20 %	5 %	100 %	

6. 수업 방법(강의, 토론, 실습 등)

강의 : 강의주제에 맞는 주교재와 부교재를 활용하여 해킹과 이에 대한 대응 방안 강의

실습 : 팀별로 침해사고 사례를 유형별로 실습

발표 및 토론 : 팀별 침해사고 사례 발표, 과제 발표와 침해사고와 대응의 적절성에 대하여 토론 유도

7. 수업에 특별히 참고하여야 할 사항

윈도우즈, 리눅스 시스템 및 네트워크에 대한 기본 지식을 선행하여 학습하여야 함

8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)

교강사와 학습자가 1:1로 수업을 할 수 없기 때문에 실습이 원활히 이루어질 수 있는 방안이 필요하므로 먼저 우등생과 열등생을 골고루 섞어 조를 편성해 주고, 모르는 것이 있을 때는 1차적으로 조안에서 상의하여 해결하게 하고, 안될 때는 교강사와 논의하게 한다.