교재 선정

학습과목명	교재종별	저자명	교 재 명	출 판 사	출판년도
침해대응실습	주교재	최상용	해킹사고의 재구성	에이콘	2013
	부교재	조 피체라 외	네트워크 침해사고 분석	비제이퍼블릭	2014

학습과목의 강의계획서

주	강 의 내 용	수업방법	학습자료 [과제포함]	기자재 [보조교구]
1	1] 강의주제: 보안관제와 해킹사고 대응 절차 2] 강의목표: 해킹 사고 대응 절차 3] 강의세부내용: ① 보안관제 절차 ② 해킹사고 분석 절차	강의	주: p22~43	빔 프로젝트 스크린 실습PC
2	1] 강의주제: 로그의 이해 1 2] 강의목표: IDS/IPS 로그의 이해 3] 강의세부내용: ① 해킹사고의 분류와 그 흔적 ② 침입 탐지 방법 ③ IDS/IPS의 구성 형태 ④ IDS/IPS 로그 분석	강의 **실습**	주: p46~58	빔 프로젝트 스크린 실습PC
3	1] 강의주제: 로그의 이해 2 2] 강의목표: 방화벽 로그의 이해 3] 강의세부내용: ① 방화벽의 주요 기능 ② 방화벽의 구성 형태 ③ 방화벽 로그 분석	강의 **실습**	주: p60~78	빔 프로젝트 스크린 실습PC
4	1] 강의주제: 로그의 이해 3 2] 강의목표: 웹 접근 로그의 이해 3] 강의세부내용: ① 웹 접근로그 및 오류로그 분석 ② 웹 접근 탐지 및 차단 방법 ③ 웹 어플리케이션 방화벽(WAF)의 이해 ④ WAF 로그 분석 ***과제제출 : OWASP TOP 10에 대하여**	강의 **실습**	주: p90~96	빔 프로젝트 스크린 실습PC
5	1] 강의주제: 로그의 이해 4 2] 강의목표: 운영체제 및 안티 DDOS 로그의 이해 3] 강의세부내용: ① 유닉스 계열 운영체제 로그와 분석 ② 윈도우즈 운영체제 로그와 분석 ③ 안티 DDOS 시스템의 차단 기능 ④ 안티 DDOS 시스템의 로그 분석	강의 **실습**	주: p79~85, p97~111	빔 프로젝트 스크린 실습PC
6	1] 강의주제: 보안 관제 시스템 2] 강의목표: ESM 로그의 이해 3] 강의세부내용: ① ESM의 이해 ② ESM 관제에 따른 로그의 분석 ③ DBMS 로그 분석	강의 **실습**	주: p112~114	빔 프로젝트 스크린 실습PC
7	1] 강의주제: 해킹 사고 유형 2] 강의목표: 해킹사고 유형과 증상의 이해 3] 강의세부내용: ① 위/변조 사고 ② 정보 유출 사고 ③ DDos 공격	강의 **실습**	주: p116~148 부: p35~71	빔 프로젝트 스크린 실습PC
8	중 간 고 사			

주	강 의 내 용	수업방법	학습자료 [과제포함]	기자재 [보조교구]
9	1] 강의주제: 증거 추적 2] 강의목표: 증거 추적 기법 및 실습 3] 강의세부내용: ① 시스템, 홈페이지 등 변조 탐지 기법 ② SQL Injection, ID/Password 유추, URL/파라미터 조작 등 ③ 특정 프로그램 설치 유도 및 CSRF ④ 탐지 유형별 정보 유출 신고 접수 ⑤ DDos 공격 탐지 및 추적 ⑥ 사고의 재구성	강의 **실습**	주: p149~215 부: p119~164	빔 프로젝트 스크린 실습PC
10	1] 강의주제: 웹 해킹사고 사례 분석 1 2] 강의목표: 홈페이지 변조 악성코드 유포 3] 강의세부내용: ① 확인과 증상 ② 환경 분석과 로그 수집 ③ 해킹사고 분석 ④ 해킹사고 분석 보고서 작성 및 발표 ***과제제출 : 최근 해킹 사고 동향 조사**	강의 **실습** **조별발표**	주: p218~237 부: 165~208, p209~219	빔 프로젝트 스크린 실습PC
11	1] 강의주제: 웹 해킹사고 사례 분석 2 2] 강의목표: 웹셸 업로드 3] 강의세부내용: ① 확인과 증상 ② 환경 분석과 로그 수집 ③ 해킹사고 분석 ④ 해킹사고 분석 보고서 작성 및 발표	강의 **실습** **조별발표**	주: p238~247 부: p209~219	빔 프로젝트 스크린 실습PC
12	1] 강의주제: DDos 공격 사건 사례 분석 2] 강의목표: DDos 공격과 사고 대응 3] 강의세부내용: ① 확인과 증상 ② 환경 분석과 로그 수집 ③ 해킹사고 분석 ④ 해킹사고 분석 보고서 작성 및 발표	강의 **실습** **조별발표**	주: p248~268 부: p209~219	빔 프로젝트 스크린 실습PC
13	1] 강의주제: SQL 인젝션 사례 분석 2] 강의목표: SQL 인젝션과 사고 대응 3] 강의세부내용: ① 확인과 증상 ② 환경 분석과 로그 수집 ③ 해킹사고 분석 ④ 해킹사고 분석 보고서 작성 및 발표	강의 **실습** **조별발표**	주: p269~313 부: p209~219	빔 프로젝트 스크린 실습PC
14	1] 강의주제: 사이버 침해 대응 모델 2] 강의목표: 사이버 침해 대응 이론과 실제 3] 강의세부내용: ① 이론과 실제의 차이 ② 사이버 침해 대응 모델	강의 **실습**	주: p316~330	빔 프로젝트 스크린 실습PC
15	기 말 고 사			

성적 산출을 위해 사용한 평가 요소 목록

학 습 과 목 명	평 가 요 소	배 점 비 율
침해대응실습	중간·기말고사 수시평가 및 과제물 수업기여도 출석율	중간 : 30%, 기말 : 30% 수시평가 및 과제물 : 15% 수업기여도 : 5% 출 석 율 : 20%