<표 III-31> 학습과정의 수업계획서

1. 강의개요

학습과정명	보안시스템 운영및실습	학점	3	교강사명		교강사 전화번호	
강의시간	5	강의실		수강대상		E-mail	

2. 교육과정 수업목표

- 네트워크 환경에서 발생될 수 있는 공격의 유형 및 그 특징을 이해하고, 공격유형별 네트워크 트래픽을 해석할 수 있는 능력을 배양한다.
- 각종 보안시스템의 특징 및 역할을 이해하고, 네트워크 환경에서 이를 구성하여 각종 공격들을 탐지하고 차단하는 방법을 학습한다.
- 네트워크에 대한 공격을 적절히 보안하기 위해 모니터링 해야 하는 네트워크상의 주요 정보들을 이해하고, 실제 보안시스템을 이용하여 이를 수행할 수 있는 능력을 함양한다.
- 네트워크 공격 유형에 따른 보안 기술 및 보안도구의 사용법을 학습하여 공격에 적절히 대응할 수 있는 능력을 배양한다
- 네트워크 공격시 대응 절차를 이해하고, 수립할 수 있도록 학습한다.

3. 교재 및 참고문헌

주교재	보안관제학	저자	안성진 외 2인	출판사	이한미디어	출판년도	2014
부교재(참고문헌)	칼리 리눅스와 백트랙을 활용한 모의해킹	저자	조정원 외 4인	출판사	에이콘	출판년도	2014

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 : 정보보호의 절차 [2] 강의목표 : 정보보호의 원칙 및 보안 모니터링의 이해 [3] 강의세부내용 : ㉮ 정보보호와 위험[RISK] ㉯ 정보보호의 원칙 ㉰ 보안관제[모니터링]의 이해 ㉱ 보안관제를 위한 데이터 수집 및 분석, 보고절차 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.15-55 - 강의교안
제 2 주	1 2 3 4 5	[1] 강의주제 : 네트워크 공격을 사전조사 [2] 강의목표 : 네트워크 공격을 위한 정보수집 [3] 강의세부내용 : ㉮ 풋프린팅[Footprinting] ㉯ 포트스캔 및 OS탐지 절차와 방법 ㉰ 방화벽과 침입탐지 시스템의 탐지 ㉱ 취약점 검사와 목록화 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.167-181 - 부:P.130-160 - 강의교안

제 3 주	1 2 3 4 5	[1] 강의주제 : 네트워크 해킹기법 [2] 강의목표 : 스니핑과 스푸핑의 이해 [3] 강의세부내용 : ㉮ 스니핑 공격기법의 이해 ㉯ 스위칭 환경에서의 스니핑 ㉰ 스푸핑에 대한 이해 ㉱ ARP/IP/DNS 스푸핑 기법 이해 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.167-181 - 부:P.163-178 - 강의교안
제 4 주	1 2 3 4 5	[1] 강의주제 : 보안 모니터링 시스템 구축 [2] 강의목표 : 보안 모니터링를 위한 네트워크 및 시스템 구성 [3] 강의세부내용 : ㉮ 보안시스템 구성을 위한 네트워크 장치 ㉯ 보안관제를 위한 패킷의 수집 및 분석방법 ㉰ 무선망에서의 데이터 수집 ㉱ 침입탐지시스템의 역할과 아키텍쳐별 구성방법 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.58-92 - 강의교안 **[수시고사]**
제 5 주	1 2 3 4 5	[1] 강의주제 : 침입탐지시스템을 위한 데이터 수집 [2] 강의목표 : 네트워크 데이터 수집 및 분석 [3] 강의세부내용 : ㉮ 침입 탐지를 위한 데이터 수집의 필요성 ㉯ 공격 기법에 따른 네트워크 데이터 패턴 ㉰ tcpdump를 이용한 데이터 수집 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.184-209 - 부:P.559-581 - 강의교안
제 6 주	1 2 3 4 5	[1] 강의주제 : 침입탐지시스템 [2] 강의목표 : 침입탐지시스템의 이해 [3] 강의세부내용 : ㉮ 침입탐지시스템의 기능과 목적 ㉯ 침입탐지시스템의 구조 ㉰ Snort를 이용한 침입탐지시스템 운영방법실습 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.184-209 - 강의교안 참고자료 : IPS 운영매뉴얼
제 7 주	1 2 3 4 5	[1] 강의주제 : 터널링과 VPN 시스템 운영 [2] 강의목표 : 터널링과 VPN에 대한 이해 및 시스템 운영 [3] 강의세부내용 : ㉮ VPN의 목적과 필요성 ㉯ 터널링 기법 ㉰ IPSEC 프로토콜의 이해 ㉱ SSL 프로토콜의 이해 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.296-330 - 강의교안 참고자료 : VPN 운영매뉴얼
제 8 주	1 2 3 4 5	중 간 고 사	

제 9 주	1 2 3 4 5	[1] 강의주제 : 서비스 거부공격 [2] 강의목표 : 서비스 거부공격에 대한 이해 [3] 강의세부내용 : ㉮ 종류별 서비스거부 공격 기법에 대한 이해 ㉯ DOS와 DDOS의 공격기법의 차이점 ㉰ DDOS 공격기법의 특징 ㉱ DOS와 DDOS의 공격에 대한 대응방법 ㉲ Anti-DDOS 시스템 운영실습 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.126-144 - 강의교안 참고자료: Anti-DDos 운영매뉴얼
제 10 주	1 2 3 4 5	[1] 강의주제 : 침입차단시스템[방화벽] [2] 강의목표 : 침입차단시스템의 이해 [3] 강의세부내용 : ㉮ 방화벽의 기능과 목적 ㉯ 방화벽의 구조 ㉰ 방화벽의 패킷필터링 방식 ㉱ 브릿지모드와 라우팅모드의 차이점 ㉲ NAT와 프록시 기능 이해 [4] 수업방법 : 강의 및 팀별 발표	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.211-222 - 부:P.163-178 - 강의교안 참고자료:방화벽운영매뉴얼 **[과제:침입차단시스템, Anti-DDOS,VPN운영관리에 관한 팀별 평가실시]**
제 11 주	1 2 3 4 5	[1] 강의주제 : 침입차단시스템의 운영 [2] 강의목표 : 침입차단시스템의 운영 방법 실습 [3] 강의세부내용 : ㉮ Iptables를 이용한 방화벽의 룰설정 ㉯ Cisco 방화벽을 이용한 룰설정 ㉰ 룰의 백업 및 복구 ㉱ 방화벽의 로그 분석 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.223-230 - 강의교안
제 12 주	1 2 3 4 5	[1] 강의주제 : 웹해킹기법 이해 [2] 강의목표 : HTTP프로토콜과 웹 공격의 이해 [3] 강의세부내용 : ㉮ HTTP 프로토콜의 이해 ㉯ HTTP 프로토콜 헤더의 변조를 이용한 공격 ㉰ OWASP 10대 취약점 이해 ㉱ XSS와 SQL 인젝션 공격 이해 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.145-160 - 부:P.239-309 - 강의교안 참고자료 : WAF 운영매뉴얼
제 13 주	1 2 3 4 5	[1] 강의주제 : WAF[Web Application Firewall] [2] 강의목표 : WAF 시스템 운영을 통한 웹해킹 방어방법 [3] 강의세부내용 : ㉮ Web knight를 이용한 웹해킹 방어 ㉯ Mod Security를 이용한 웹해킹 방어 ㉰ WAPPLES를 이용한 웹해킹방어 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 - 주:P.248-255 - 부:P.487-514 - 강의교안

제 14 주	1 2 3 4 5	[1] 강의주제 : ESM[Enterprise Security Management] [2] 강의목표 : ESM을 이용한 보안시스템의 통합운영 [3] 강의세부내용 : ㉮ ESM의 Agent와 Manager 아키텍쳐 ㉯ SNMP와 Syslog를 이용한 보안시스템의 로그수집 ㉰ SpiderTM을 이용한 보안 시스템 통합관리 ㉱ 연관성 분석을 통한 공격 탐지 방법 [4] 수업방법 : 강의, 실습, 토론	기자재 - 실습용PC, DLP Cube - 스크린, 화이트보드 학습자료 : - 주:P.183-209 - 부:P.187-239 - 강의교안 참고자료 : ESM 운영매뉴얼
제 15 주	1 2 3 4 5	기 말 고 사	

5. 성적평가 방법

중간고사	기말고사	과 제 물	출 결	기 타	합 계	비 고
30%	30%	10%	20%	10%	100%	

6. 수업 방법(강의, 토론, 실습 등)

- 강의, 실습, 토론

7. 수업에 특별히 참고하여야 할 사항

8. 문제해결 방법(실험·실습 등의 학습과정의 경우에 작성)