PART 09

사이버보안공학과

단과대학 교육목표

- 주어진 과제를 자기 주도적인 자세를 가지고 창의적으로 해결할 수 있는 능력을 갖춘 인재의 양성
- 본인이 잘할 수 있는 전공영역과 자신이 즐겨할 수 있는 교양영역의 심도 있는 지식을 갖추고 이를 사회를 위해 봉사할 수 있는 민주시민의 역량을 갖춘 인재의 양성
- 과제를 수행함에 있어서 타인과 협력하고, 조직을 이끌어갈 수 있는 리더십을 갖춘 인재의 양성
- 지역사회를 넘어 글로벌로 진출할 수 있는 도전정신을 갖춘 인재의 양성

학과 교육목표

- 정보사회가 요구하는 실무 인재 양성
- 사회에 봉사하는 인재 육성
- 정보 사회의 안전을 책임지는 자세 취득
- 자신의 의사를 표현할 수 있는 능력 배양
- 자신의 실무 영역에서 창의적 사고 능력 발휘
- 현대 정보사회에 필요한 사이버보안공학도를 육성하여 학문 및 정보사회의 발전에 공헌
- 해킹 및 바이러스 등의 전자적 침해에 대비하여 정보의 안전하고 신뢰성 있는 전달을 보장

학과 소개

◦ **교육목적**

정보화 시대의 고급화와 다변화되는 현실에서 사회 모든 분야(정부, 기업, 단체, 개인 등)에서 정보보호의 중요성은 더욱 강조되고 있다. 본 학과는 변화하는 사회적 현실에 적극적으로 대처하고 사회적 요구를 수용하여, 실무에서 경쟁력을 갖추고, 자신을 미래지향적으로 발전시켜 나갈 수 있는 사이버보안 분야의 전문 인력을 양성하고자 한다.

◦ **특성화 방안**

- (교육과정 특성화) 사이버보안분야에 있어서 시회수요 미스매치 해결을 위해 보안관제, 취약점 진단 및 모의해킹, 보안컨설팅, 보안개발 및 엔지니어 전문가 육성을 위해 기업 맞춤형 주문식 교육과정 운영
- (진로 특성화) 기업맞춤형 인재 양성을 위해 기업이 직접 참여하여 대학과 공동으로 수행하는 인재 예약형 교육시스템을 운영하여 인턴/취업 예약을 통한 취업경로 강화
- (전문 자격취득) 자격 취득 집중학기 운영을 통해 국가 실무 자격증 취득을 통한 사이버보안 직무역량 강화

◦ **졸업후 진로 (목표취업처)**
- 보안컨설팅, 보안관제, 취약점진단, 모의해킹 등 보안 전문업체
- 보안엔지니어
- 서버 및 네트워크 보안 관리
- 디지털 포렌식 전문가
- 모바일 앱 개발 및 보안장비 개발 업체
- 경찰청 사이버테러 대응센터 사이버수사요원

학과 역량 정의

학과 역량		
영역	**핵심 역량**	**세부 역량**
대학 핵심 역량	자기관리 역량	주도적 학습 능력 및 자기관리 역량
	리더십역량	실무형 전문지식을 갖춘 리더쉽 발휘 역량
		투철한 윤리의식을 갖고 국가와 지역사회에 봉사하는 리더쉽 발휘 역량
	의사소통역량	주제의 핵심 내용을 이해하는 의사소통 역량
		공학 정보의 정확하고 간결한 표현 및 작성 역량
	창의적문제해결역량	자료를 수집하고 분석하여 창의적 문제 해결 역량
		유연한 사고를 통한 창의적 문제 해결 역량
	자원활용역량	다양한 자원 수집 및 활용할 수 있는 자기 주도적 학습 역량
	글로벌능력	국제적 역할의 이해능력 발휘 역량
전공 특성화 역량	윤리적 해커 양성	컴퓨터 전반에 관한 이해할 수 있다.
		윤리의식이 투철한 해커.
		실무능력을 갖춘 해커양성.
	보안 컨설턴트 능력	정보 사회의 안전을 책임지는 자세를 갖춘다.
		기관의 보안현황을 분석하고 문제점을 발견할 수 있다.
		기관의 보안취약점에 대한 보안대책을 수립할 수 있다.
	보안 진단 능력	서버/네트워크/데이터베이스의 보안취약점을 진단할 수 있다.
		웹서비스의 취약점을 진단하고 대책을 제시할 수 있다.
		SCADA 및 IoT 장비의 보안취약점을 진단하고 대책을 제시할 수 있다.
	보안관리 능력	방화벽 등 보안장비를 운영할 수 있다.
		사이버보안 공격을 분석하고 대응할 수 있다.
		신규 보안취약점을 분석하고 대응할 수 있다.

학과 내규

사이버보안공학과의 학위 수여를 위한 졸업 요건은 다음과 같다.

1. 학칙 제 40조(졸업과 학위) 및 동 시행세칙에 의거 졸업 시험을 통과하여야 한다.
2. 졸업시험 자격요건
   ① 사이버보안공학을 전공하는 단일전공자 및 복수전공자는 졸업시험을 시행한다.
   ② 다음 조건을 모두 충족한 자만이 졸업시험에 응시할 자격을 갖는다.
      - 정보보안 및 IT관련 자격증 중 1개 이상을 취득한 자
      · 정보보안기사/산업기사, 정보처리기사 등 이에 준하는 자격 취득
      · 인터넷보안전문가2급, 리눅스마스터2급, 네트워크관리사2급, CCNA/CCNP, CPPG, 디지털포렌식 2급 등 이에 준하는 자격 취득

   ※ 이외 졸업시험 자격요건의 경우 학과 졸업심사위의 회의를 거쳐 결정한다.
3. 졸업시험 면제요건
   ① 재학 중 행정부처에서 실시하는 국가 공무원 공개 채용 시험 9급 이상 합격자
   ② 재학 중 국내외 유수기관에서 주관하는 전국규모의 이공계 관련 경진대회나 작품 공모전 등에서 3위 이상 입상한 자
   ③ 재학 중 전공과 관련하여 국내외 유수기업이나 기관, 연구소, 대학 등에서 주관하는 전국 규모의 대학(원)생 논문공모전에서 입상한 자
   ④ 공인된 기관에서 시행하는 정규 TOEIC 점수가 750점 이상 또는 TOEFL 점수가 (PBT 550, CBT 205, IBT 75)점 이상 취득한 자
   ⑤ 정보처리기사, 정보보안기사, 리눅스마스터 1급, 인터넷보안전문가 1급, 네트워크 관리사 1급, 정보보안관리사(ISM) 1급, CISSP, CISA의 자격증 중 1개 이상을 취득한 자는 졸업 전공 시험을 면제한다.
   ⑥ 기타 면제 요건은 졸업심사위원회(위원장: 학과장, 위원: 학과소속교수)에서 심의를 통하여 인정할 수 있다.
      ※ 단, 외국인 학생과 해외취업(연수자포함)을 한 학생의 경우 학과 졸업심사위의 회의를 거쳐 결정한다.
4. 졸업시험
   ① 졸업 시험 과목은 필수과목(5개 과목)을 응시해야 한다.
      - 컴퓨터구조와 디지털 저장매체, 실전웹서버 해킹과 대응, 실전 네트워크 일반, 운영체제 보안, 암호학
   ② 졸업시험의 통과(합격)는 5개 과목 평균 60점 이상을 취득하여야 하며, 각 과목별 점수가 40점 미만인 경우에는 과락으로 처리한다.
   ③ 졸업 시험은 두 번의 기회가 주어지며, 과락은 없으나 전체 평균 기준을 통과하지 못하였을 경우 과목별 재시험의 기회를 줄 수 있으며, 전체 평균 기준을 통과하였으나 응시 과목 중 과락의 경우에는 과락 과목만을 재응시 할 수 있다.

학점 이수체계(졸업에 필요한 최소 이수학점)

구분	창의융합과정(교양)				전공*	자율 선택	계*
	필수*	중점*	선택	계*			
학점	10	10	18	38	70	22	130

* 표기 학점은 졸업에 반드시 필요한 이수학점임.

교양필수 교육과정 일람표

구 분		교과목 코 드	교과목명	학점	시 수		이수시기		비 고
					이론	실습	학년	학기	
교양 필수 (11)	의사 소통	00076K	비판적 사고와 글쓰기	2	2		1		
		00070K	영어 I	1	2		1	1	
		00071K	영어 II	1	2		1	2	
		00072K	영어III	1	2		2	1	※ 동일 언어선택 · **영어III,영어IV** : 정기토익 700점 이상 · **중국어 I ,중국어 II** : 신HSK 5급(180점이상) · **일본어 I ,일본어 II** : JPT 700점 이상 상기 조건 충족의 경우 대체교과로 교양영역 2학점 이수 가능 (대상학생 선택)
		00077K	중국어 I						
		00079K	일본어 I						
		00073K	영어IV	1	2		2	2	
		00078K	중국어 II						
		00080K	일본어 II						
	인성과 도전	00084H	파트너십트레이닝 I	1	1		1	1	
		00085H	파트너십트레이닝 II	1	1		1	2	
		00006I	기업가정신과리더십	1	1		2	1	
		99544A	동기유발	1	1		1	1	
계			13(9)개 과목	10	14				

중점교양 사이버보안공학과 추천 교과목

이 수 구 분	교과목 코 드	교과목명	학 점	시 수		이 수 시 기		비고
				이론	실습	학년	학기	
중점 교양 (19)	00068K	4차 산업혁명과 기술	2	2		1	2	4차산업혁명
	00067K	인간사회과학의 미래학	2	2		2	1	4차산업혁명
	00020J	변화와 혁신	2	2		2	1	
	00058I	과학과 인간	2	2		1	1	
	00088F	법과 생활	2	2		2	2	

교양선택 사이버보안공학과 추천 교과목

이수 구분	교과목 코드	교과목명	학점	시수		이수 시기		비고
				이론	실습	학년	학기	
교양 선택	00054J	영화로 배우는 과학	2	2		1	2	
	00065K	융합적 인간이해	3	3		1	2	
	00070H	창업실무	2	2		2	1	
	00083E	취업상식	3	3		2	2	
	00090J	전략적 글쓰기	2	2				
	00095A	컴퓨터 I - 문서작성	2	2				
	00096A	컴퓨터 II - 스프레드시트	2	2				

전공 교육과정 일람표

교과목 코드	교과목명	학점	시수		이수 시기	
			이론	실습	학년	학기
99524A	전공몰입	1	1		1	1
50153B	웹프로그래밍언어	3	3		1	1
50146B	컴퓨터기초와 이해	3	3		1	1
50152B	네트워크 일반	3	3		1	2
50147B	정보보호개론과 윤리	3	3		1	2
50102C	정보수학	3	3		1	2
50193A	프로그래밍 언어	3	3		1	2
소 계	7개 과목	19	19			
50165B	데이터베이스 서버보안	3	3		2	1
50118B	리버스엔지니어링	3	3		2	1
50117B	유닉스/리눅스	3	3		2	1
50154B	컴퓨터구조와 디지털저장매체	3	3		2	1
50173B	JAVA	3	3		2	2
50103C	객체지향 프로그래밍	2	2		2	2
50101C	실전 사물인터넷(IoT)보안 실무	3	3		2	2

교과목 코 드	교과목명	학 점	시수		이 수 시 기	
			이론	실습	학년	학기
50172B	실전네트워크 해킹과 대응	3	3		2	2
50151B	실전시스템 해킹과 대응	3	3		2	2
50127B	암호학	3	3		2	2
50181B	윈도우구조와 원리	3	3		2	2
소 계	11개 과목	32	32			
50180B	모바일프로그래밍	3	3		3	1
50166B	사이버 포렌식	3	3		3	1
50100C	실전 웹서버해킹과 대응(캡스톤디자인)	3	3		3	1
50199B	운영체제보안(캡스톤디자인)	3	3		3	1
50123B	통신소켓프로그래밍	3	3		3	1
50197B	개인정보 침해대응	3	3		3	2
50178B	디지털포렌식과법규	3	3		3	2
50183B	모바일 어플리케이션	3	3		3	2
50189B	악성코드 제작 및 분석 실무	3	3		3	2
50190B	전자상거래보안 실무	3	3		3	2
50176B	침입탐지 및 차단	3	3		3	2
소 계	11개 과목	33	33			
50191B	모의해킹 실무	3	3		4	1
50192B	보안관제 실무	3	3		4	1
50194B	보안엔지니어 실무	3	3		4	1
50195B	보안컨설팅 실무	3	3		4	1
50196B	취약점진단 실무	3	3		4	1
50193B	포렌식실무	3	3		4	1
50157B	모바일보안	3	3		4	2
50144B	현장실습	18			4	2
소 계	8개 과목	39	21			
총 계	37개 과목	123	105			

취업로드별 관련 교육과정(졸업역량에 따른 목표취업처 선정)

취업로드	관련 교과목
보안관제	웹프로그래밍 언어, 네트워크 일반, 컴퓨터구조와 디지털저장매체, 데이터베이스 서버보안, 유닉스/리눅스, 서버구축, 리버스엔지니어링, 윈도우 구조와 원리, 객체지향 프로그래밍, 암호학, 실전네트워크 해킹과 대응, 실전 시스템 해킹과 대응, 통신소켓 프로그래밍, 실전 웹서버 해킹과 대응, 운영체제 보안, 전자상거래 실무, 침입탐지 및 차단, 개인정보 침해대응, 보안관제 실무, 실전 사물인터넷(IoT)보안 실무
보안컨설팅	웹 프로그래밍 언어, 네트워크 일반, 컴퓨터구조와 디지털 저장매체, 데이터베이스 서버 보안, 유닉스/리눅스, 윈도우 구조와 원리, 객체지향 프로그래밍, 암호학, 실전 네트워크 해킹과 대응, 실전 시스템 해킹과 대응, 모바일 프로그래밍, 통신소켓 프로그래밍, 실전 웹서버 해킹과 대응, 운영체제 보안, 모바일 애플리케이션, 전자상거래 실무, 보안컨설팅 실무, 실전 사물인터넷(IoT)보안 실무
모의해킹 및 취약점진단	웹 프로그래밍 언어, 네트워크 일반, 컴퓨터구조와 디지털 저장매체, 데이터베이스 서버 보안, 유닉스/리눅스, 리버스엔지니어링, 윈도우 구조와 원리, 객체지향 프로그래밍, 암호학, 실전 네트워크 해킹과 대응, 실전 시스템 해킹과 대응, 모바일 프로그래밍, 통신소켓 프로그래밍, 실전 웹서버 해킹과 대응, 운영체제 보안, 모바일 애플리케이션, 악성코드 제작 및 분석 실무, 전자상거래 실무, 모의해킹 실무, 취약점진단 실무, 실전 사물인터넷(IoT)보안 실무
보안 엔지니어	웹 프로그래밍 언어, 네트워크 일반, 컴퓨터구조와 디지털 저장매체, 데이터베이스 서버 보안, 유닉스/리눅스, 윈도우 구조와 원리, 객체지향 프로그래밍, 암호학, 모바일 프로그래밍, 통신소켓 프로그래밍, 실전 웹서버 해킹과 대응, 운영체제 보안, 모바일 애플리케이션, 악성코드 제작 및 분석 실무, 전자상거래 실무, 보안 엔지니어 실무, 실전 사물인터넷(IoT)보안 실무
디지털 포렌식	웹 프로그래밍 언어, 네트워크 일반, 컴퓨터구조와 디지털 저장매체, 데이터베이스 서버 보안, 유닉스/리눅스, 리버스엔지니어링, 윈도우 구조와 원리, 객체지향 프로그래밍, 암호학, 실전 네트워크 해킹과 대응, 실전 시스템 해킹과 대응, 사이버포렌식, 모바일 프로그래밍, 통신소켓 프로그래밍, 실전 웹서버 해킹과 대응, 운영체제 보안, 디지털 포렌식과 법규, 모바일 애플리케이션, 전자상거래 실무, 디지털 포렌식 실무, 사물인터넷(IoT)보안 실무

사이버강좌 교과목

교과목명
컴퓨터구조와 디지털저장매체

자격증 관련 교과목 일람표

자격증명	관련 교과목
정보보안기사/산업기사	네트워크 일반, 암호학, 실전네트워크해킹과 대응, 실전시스템 해킹과 대응, 실전 웹서버해킹과 대응, 침입탐지 및 차단, 정보보호개론과 윤리, 윈도우구조와 원리, 컴퓨터구조와 디지털저장매체, 유닉스/리눅스, 악성코드분석 및 제작, 취약점진단 실무
정보처리기사	컴퓨터 기초와 이해, 프로그래밍 언어, 유닉스/리눅스, 데이터베이스 서버보안, 서버구축, 통신소켓프로그래밍, 윈도우 구조와 원리, 전자상거래보안, 네트워크 일반, 컴퓨터 구조와 디지털 저장매체
인터넷보안전문가	유닉스/리눅스, 네트워크일반, 실전네트워크해킹과 대응, 모의침투평가, 통신소켓프로그래밍, 실전웹서버 해킹과대응, 서버구축, 리버스엔지니어링, 전자상거래보안, 실전시스템 해킹과 대응, 디지털포렌식과 법규, 개인정보 침해대응
CISSP	유닉스/리눅스, 암호학, 네트워크 일반, 실전웹서버 해킹과대응, 통신소켓프로그래밍, 모의침투평가, 서버구축, 리버스엔지니어링, 실전네트워크 해킹과보안, 데이터베이스서버보안, 실전시스템 해킹과 대응, 개인정보 침해대응
디지털 포렌식 전문가	리버스엔지니어링, 컴퓨터구조와 디지털저장매체, 데이터베이스 서버보안, 윈도우 구조와 원리, 인터페이스 프로그래밍, 디지털 포렌식과 법규, 안티 포렌식, 정보보호개론과 윤리, 프로그래밍 언어, 사이버포렌식

기업연계 교과목 일람표

교 과 목 명
악성코드 제작 및 분석 실무, 전자상거래보안 실무, 모의해킹 실무, 보안관제 실무, 포렌식 실무, 보안엔지니어 실무, 보안컨설팅 실무

통합교과목(분담) 교과목 일람표

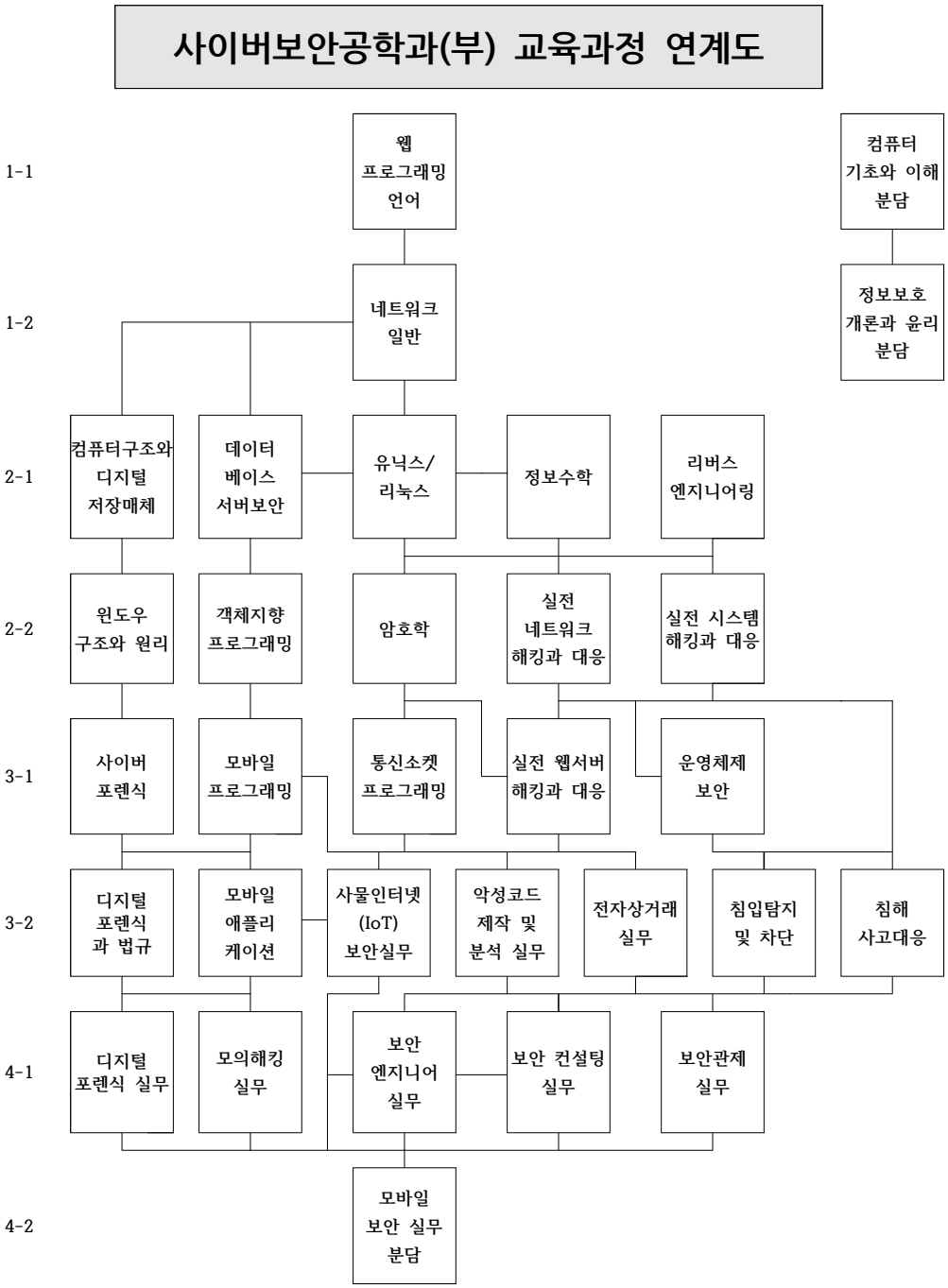
교과목명	참여교수 명단(성명, 직급, 담당시수)
학습동기유발	차건상(코디), 양계탁, 정승욱, 김동원, 이후기
전공몰입	차건상(코디), 양계탁, 정승욱, 김동원, 이후기
컴퓨터 기초와 이해	정승욱(코디), 양계탁, 차건상, 김동원, 이후기
정보보호개론과 윤리	김동원(코디), 양계탁, 차건상, 정승욱, 이후기
모바일보안	양계탁(코디), 차건상, 정승욱, 김동원, 이후기

교과목별 역량 매트릭스

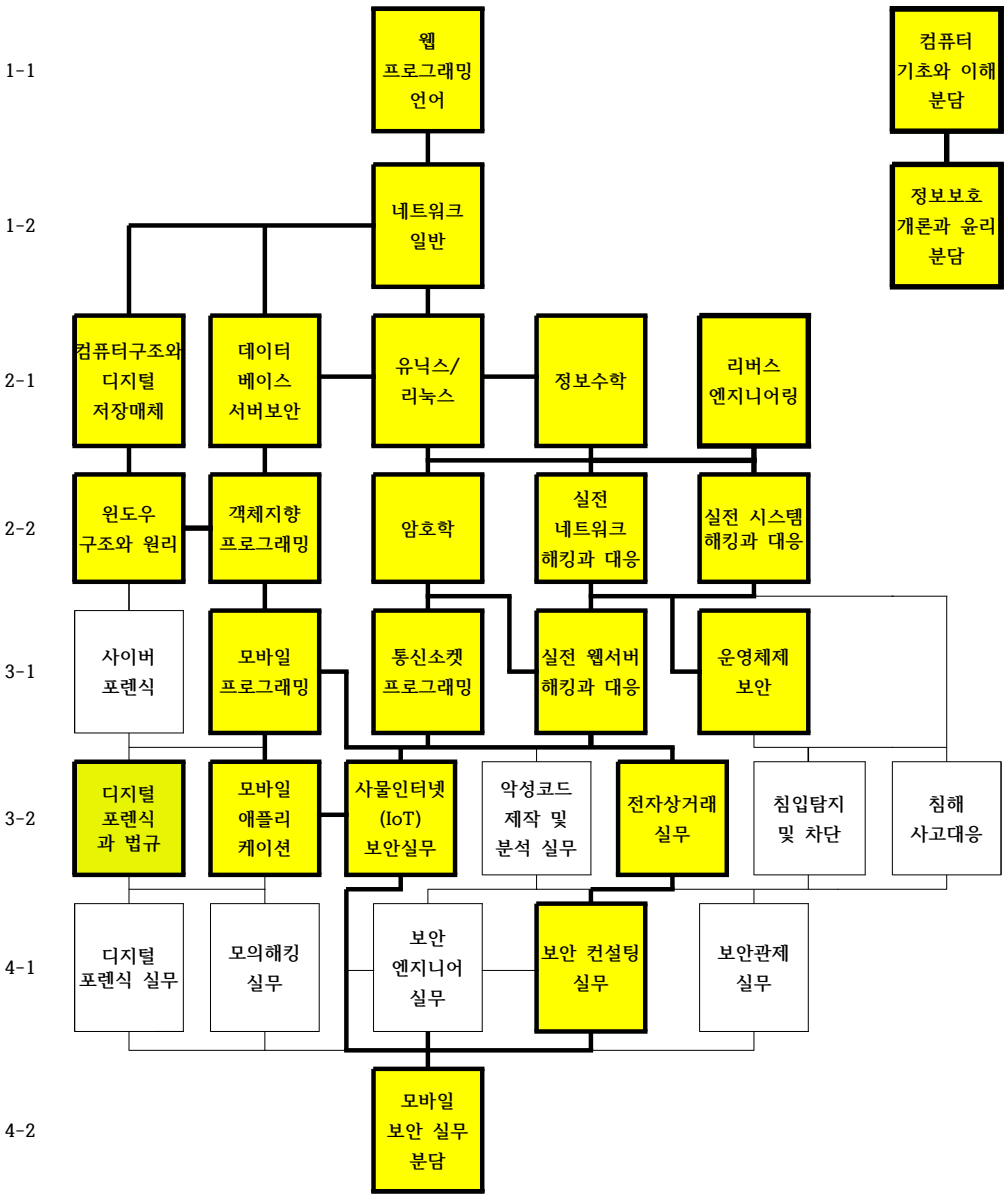
이수시기	교과목명	대학 핵심역량						전공특성화역량		
		자기관리역량	리더십역량	의사소통역량	창의적문제해결역량	자원활용역량	글로벌역량	보안컨설팅능력	보안진단능력	보안관리능력
1-1	컴퓨터 기초와 이해	●		O	O	O		O	O	O
1-1	웹프로그래밍언어				O	O		O	O	O
1-2	정보보호개론과 윤리	●		O	O	O	O	O	O	O
1-2	네트워크일반	●		O	O	O		O	O	O
1-2	정보수학				O	O		O	O	O
2-1	컴퓨터구조와 디지털 저장매체	●		O	O	O		O	O	O
2-1	유닉스/리눅스	O			O	●		O	O	
2-1	데이터베이스 서버보안				●	O		O	O	O
2-1	서버구축				O	●		O	O	O
2-1	리버스엔지니어링				●	O	O	O	O	O
2-2	윈도우 구조와 원리	●			O	O		O	O	O
2-2	암호학				●	O		O	O	O
2-2	객체지향 프로그래밍				●	O		O	O	O
2-2	실전 네트워크 해킹과 대응 (캡스톤디자인)			●	O	O	O	O	O	O
2-2	실전 시스템 해킹과 대응				●	O	O	O	O	O
2-2	실전 사물인터넷(IoT) 보안실무		O		●	O	O	O	O	O
3-1	사이버 포렌식				●	O	O	O	O	O

이수시기	교과목명	대학 핵심역량						전공특성화역량		
		자기관리역량	리더십역량	의사소통역량	창의적문제해결역량	자원활용역량	글로벌역량	보안컨설팅능력	보안진단능력	보안관리능력
3-1	통신소켓 프로그래밍				●	O			O	
3-1	모바일 프로그래밍				●	O	O	O	O	O
3-1	실전 웹서버 해킹과대응		●		O	O	O	O	O	O
3-1	운영체제 보안(캡스톤디자인)				●	O		O	O	O
3-2	디지털 포렌식과 법규	●			O	O	O	O	O	
3-2	전자상거래 실무		O		O	●		O	O	
3-2	침입탐지 및 차단			O	●	O		O	O	
3-2	모바일 어플리케이션	O			●	O	O		O	O
3-2	개인정보침해대응	O		●	O	O	O	O	O	O
3-2	악성코드 제작 및 분석 실무		O	O	●	O		O	O	
4-1	취약점진단 실무			O	●	O	O	O	O	
4-1	디지털 포렌식 실무			●	O	O	O	O	O	O
4-1	보안엔지니어 실무			O	O	●	O	O	O	O
4-1	모의해킹 실무			O	●	O	O	O	O	
4-1	보안관제 실무			●	O	O	O	O	O	O
4-1	보안 컨설팅 실무			●	O	O	O	O	O	
4-2	모바일보안	●			O	O	O	O	O	O

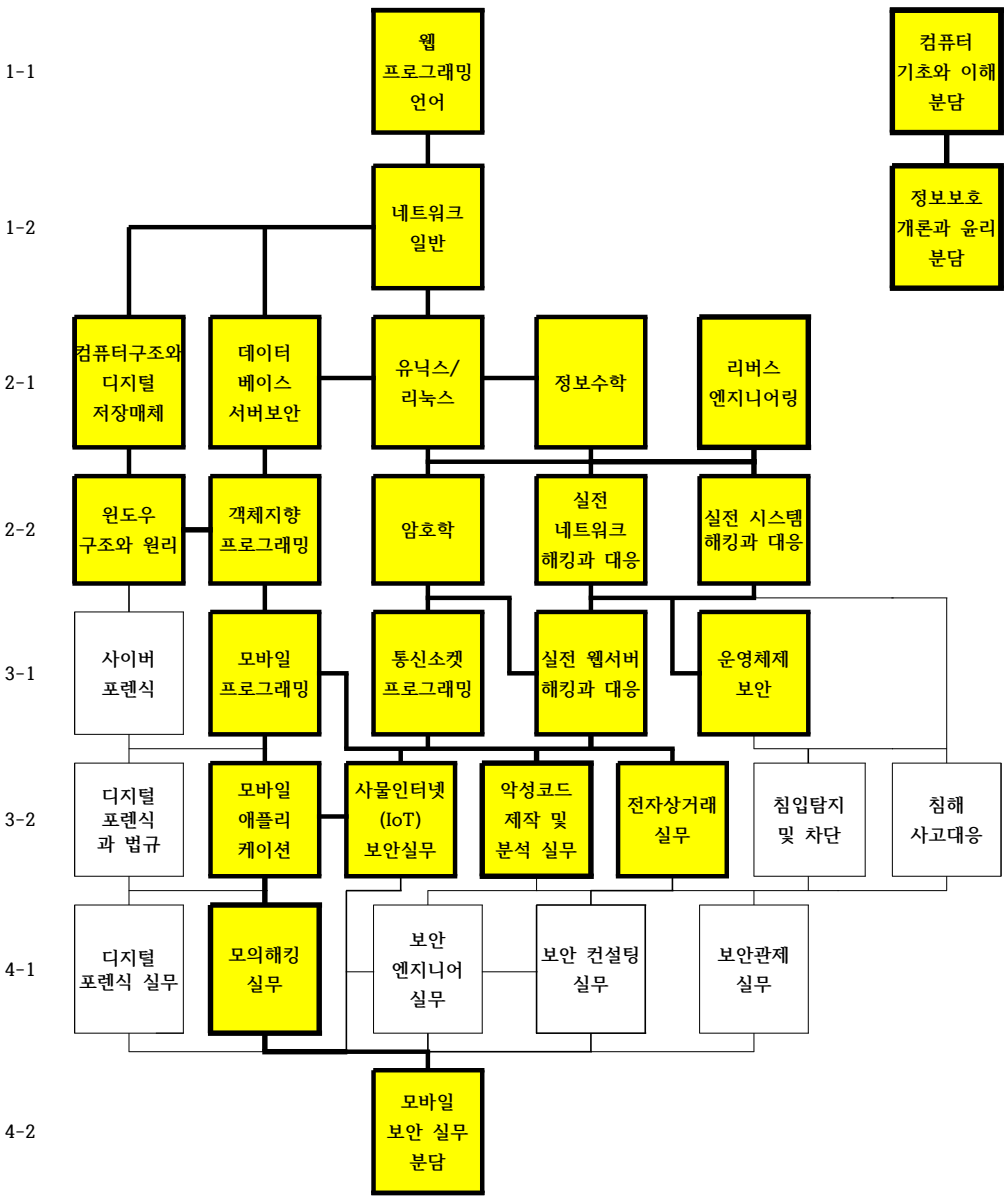
취업로드 / 트랙 교육과정 연계도



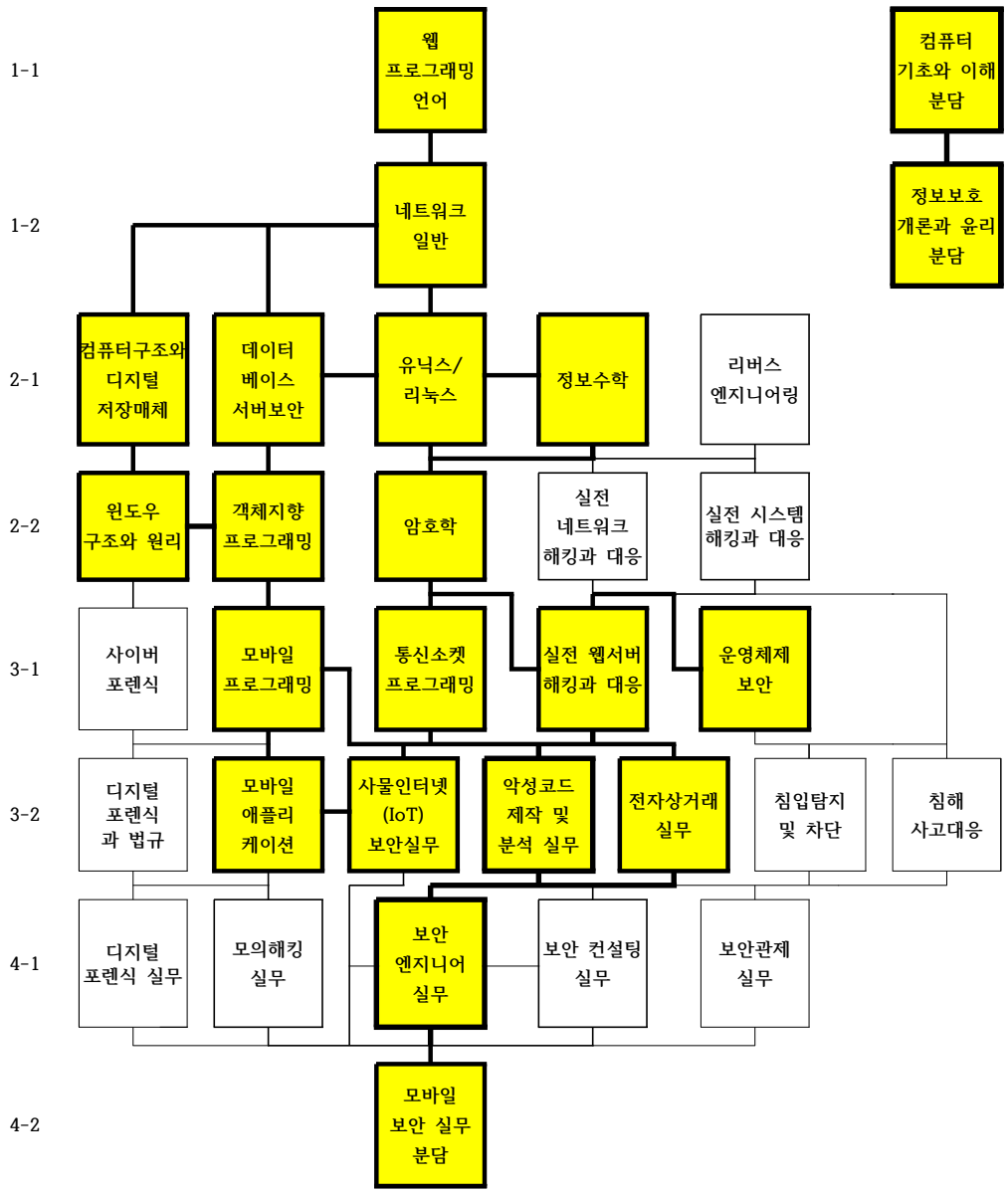
사이버보안공학과(부) 트랙별 교육과정 연계도
- 보안 컨설팅 -



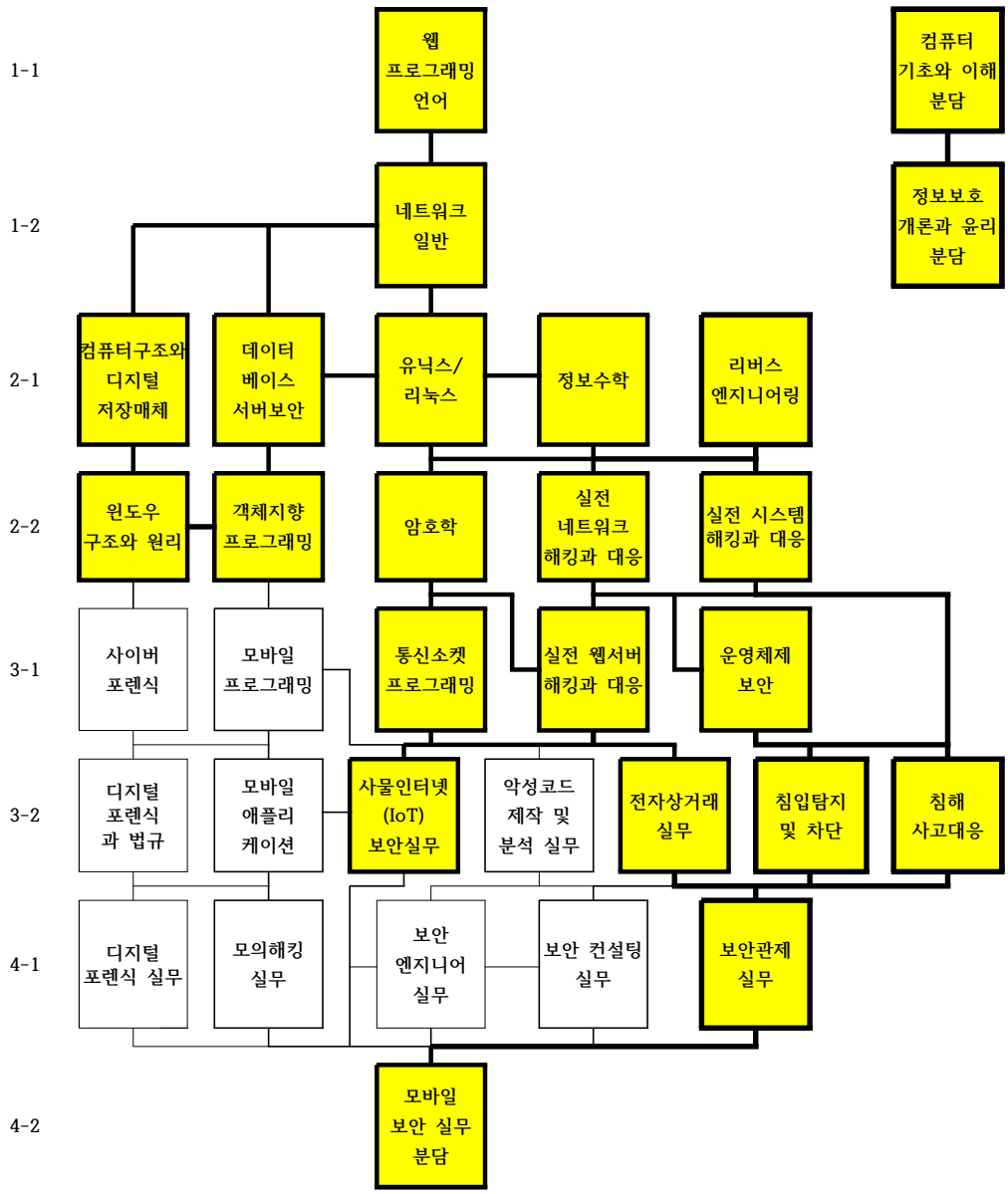
사이버보안공학과(부) 트랙별 교육과정 연계도
- 모의해킹 및 취약점진단 -



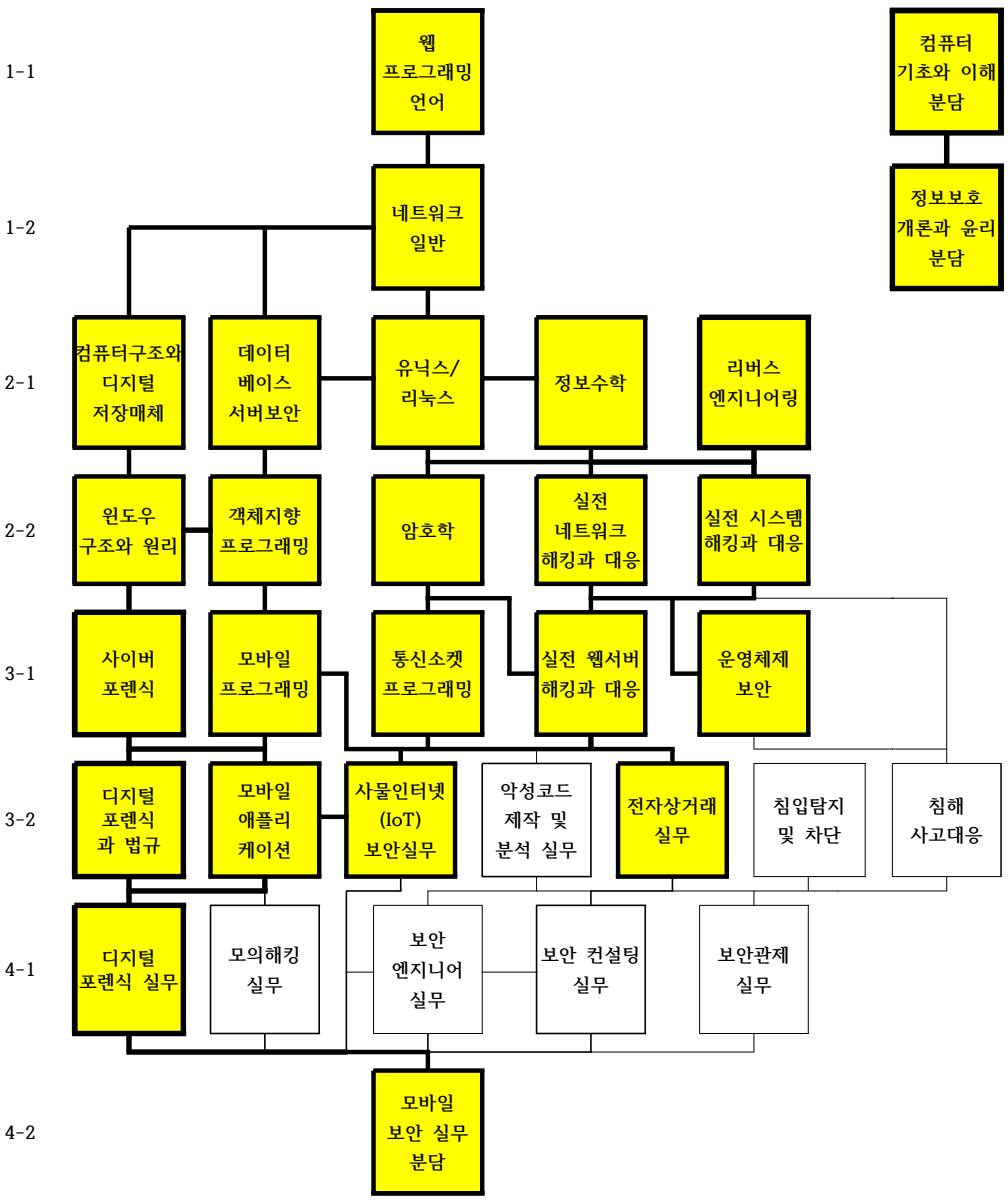
사이버보안공학과(부) 트랙별 교육과정 연계도
- 보안 엔지니어 -



사이버보안공학과(부) 트랙별 교육과정 연계도
- 보안 관제 -



사이버보안공학과(부) 트랙별 교육과정 연계도
- 디지털 포렌식 -



교과목 개요

50153B 웹프로그래밍언어 〈Web Programming〉

HTML/CSS, ASP를 다루는 교과과정으로, HTML은 인터넷에서 문서를 보여주기 위한 하이퍼텍스트 표준 언어로써 태그 형식의 요소(element)들로 구성되어있는 마크업언어이다. CSS는 웹페이지의 레이아웃과 디자인을 구성하는 스타일시트 표준안이다. ASP를 사용하여 다양한 프로젝트를 작성하고, 네트워크 관리자로서 웹서버의 제작 및 관리를 학습한다.

50146B 컴퓨터 기초와 이해 〈Understanding of Computers〉

컴퓨터를 이해할 수 있는 기초적인 내용을 중심으로 정보보호 전공의 학습을 위한 주제를 중심으로 수업이 진행된다. 컴퓨터의 최근 기술 동향과 인터넷 환경에서의 정보기술과 응용 환경 등에 관하여 학습한다.

50152B 네트워크 일반 〈General Network〉

OSI 7계층, IP addressing와 서브네팅 등 TCP/IP 일반, Unix/Windows 네트워크 서비스, IP Routing, 네트워크 장비 이해, PDA와 WAP 등 무선통신, 네트워크기반 프로그램을 이해하고 활용 방법 등에 관하여 학습한다.

50147B 정보보호 개론 및 윤리 〈Introduction to Information Security〉

정보보호 전공의 내용과 방향을 이해하도록 돕기 위해 정보보호에 관련된 암호기술, 시스템 보안 기술, 네트워크 보안 기술, 응용 서비스 보안 기술에 사용되는 기술, 정보보호관리, 평가, 표준, 윤리 등을 소개한다. 컴퓨터시스템의 기본 구성요소에 대하여 주제별로 배운 후 정보보호에 대한 전반 개념인 암호학, 시스템 보안, 네트워크 보안, 악성코드, 최신 정보보호용 소프트웨어 정보보호 정책 및 법제도 등을 주요 용어, 기본기술을 중심으로 학습함으로써, 컴퓨터시스템 및 정보보호에 대한 일반적인 개념을 확립하여 정보보호전공 교과목 수강을 위한 기본지식을 습득한다.

50102C 정보수학 〈Mathematics for information〉

정보수학은 MSC 과목 중의 하나로 공학인증을 위한 필수과목이다. 기초수학으로 공학교육에 필요한 수학의 개념을 익힌다.

50193A 프로그래밍언어 〈Programming Language〉

C프로그래밍 언어를 중심으로 그 구조와 프로그래밍 기법을 익히고 다양한 문제의 실질적인 해결을 위한 실습을 통하여 언어를 이해한다. 한편 자료구조론의 실습 언어로서 이용되므로 자료구조론의 선수과목 역학을 한다.

50117B 유닉스/리눅스 〈Linux/Unix Language〉

파일과 디렉토리 그리고 통신 관련 명령어, VI편집기, 리다이렉션과 파이프, 파일시스템과 디스크 관리, 사용자 관리, 시스템 성능 관리, Networking, 쉘프로그래밍 등에 관하여 학습한다.

50165B 데이터베이스 서버 보안 〈Database Security Setting〉

실제 가장 중요한 자산인 데이터에 대한 보안은 매우 중요하다. DB 보안 문제는 내부 사용자 거래에 의한 사고이고 점차 회사가 손실을 입는 액수가 점차 커지고 있다. 내부 사용자가 접근할 수 없는 곳은 통제하고, 접근 가능한 곳은 로깅을 하여 감사 추적할 수 있어야 한다. 본 과목에서는 IP도용의 위험성, SQL Injection 공격, 사회공학적인 공격 등을 알아보고 그 대응책을 공부할 것이다.

50118B 리버스 엔지니어링 〈Reverse Engineering〉

이미 만들어진 시스템을 역으로 추적하여 처음의 문서나 설계 기법 등의 자료를 얻어낸다. 시스템을 이해하여 적절히 변경하는 소프트웨어 유지 보수 과정을 이해한다. CPU 레지스터와 어셈블리 언어, 로우레벨 소프트웨어, 리버싱 툴, 리버싱 실전, 파일 포맷 분석, 프로그램 바이너리 검사, 악성코드리버싱, 안티 리버싱기술, 보호기술파괴, 디컴파일러 등에 관하여 학습한다.

50154B 컴퓨터구조 및 디지털 저장매체 〈Computer Structure & Digital Storage〉

컴퓨터의 하드웨어 구조를 이해하고, 컴퓨터 구조와 저장매체에 대한 의 기본적인 이론과 내용을 체계적으로 알아본다. 이로서 정보보안 분야의 기본 지식을 습득하고, 디지털 포렌식을 위한 기초 지식을 얻는다.

50173B JAVA 〈JAVA〉

자바는 다양한 운영체제가 존재하는 인터넷상에서의 프로그래밍에 용이하다는 특징 때문에 단기간에 널리 보급되었다. 자바를 이용할 경우, 인터넷에서 프로그램 자제를 주고받을 수 있기 때문에 시시각각 변하는 금융관계 그래프나 애니메이션, 쌍방향 게임 등 동적인 구성이 가능하며, 하나의 프로그램을 다양한 OS로 취급하는 인터넷 환경에서 이상적인 언어로 평가받고 있다. 자바는 추후 웹프로그램에서 JSP, 모바일 보안에서 응용된다.

50103C 객체지향 프로그래밍 〈object-oriented programming〉

객체지향 개념 및 개발방법 학습을 통해 절차지향 프로그래밍과의 차이점을 학습하고, 모든 데이터를 오브젝트(object;물체)로 취급하여 프로그래밍 하는 방법으로, 처리 요구를 받은 객체가 자기 자신의 안에 있는 내용을 가지고 처리하는 방식을 학습함

50101C 실전 사물인터넷(IoT) 보안 실무 〈IoT security of Professional Practice〉

현재 혹은 가까운 近미래에는 사물인터넷을 활용한 센서기반의 시대가 도래할 것으로 예측하고 있다. 사이버보안은 어플리케이션 영역에서 하드웨어 영역으로 빠르게 이동하고 있는 추세이다. 이에 따라 본 강의에서는 Kali Linux와 Metasploit을 활용한 기본적인 모의침투 테스트를 학습하고, 아두이노(Arduino)를 통한 기초적인 하드웨어를 다뤄본다. 또한, 무선공유기, 스마트 캠, RF 스위치, 하드웨어 기반 Key Logger 등을 실습함으로써 IoT 시대를 대비한 하드웨어 해킹 기초를 학습한다.

50172B 실전 네트워크 해킹과 대응 〈Practical Network Hacking & Response〉

스캐닝, 스니핑 및 암호화 프로토콜, Spoofing, 터널링, 서비스 거부공격, 분산서비스 거부 공격, 네트워크 스캐닝, Session hijacking, 각종 remote attack, 각종 trojan 및 exploit 이해, 무선네트워크 공격 등을 실습하고 대응 방법에 관하여 학습한다.

50151B 실전 시스템해킹과 대응 〈Practical System Hacking & Response〉

운영체제의 이해, 패스워드 크래킹, SetUID, 백도어, 레이스 컨디션, 버퍼 오버플로우, 포맷스트링, 운영체제 설정과 취약점, 시스템 로그분석, 흔적제거와 침입 추적 등 시스템 해킹과 관련된 해킹 기법을 실습하고 대응 방법을 학습한다.

50127B 암호학 〈Cryptography〉

암호 관련 용어, 정보이론, 암호 공격 방식, 스트림 암호, 블록 암호(DES, AES, SEED), 블록 암호 공격, 공개키 암호(배낭문제, RSA, Elgamel, ECC), 해시 함수와 설계 원리, 디지털서명, 특수 서명, 인증 및 키분배, 키 분배 프로토콜, 메시지인증, 영지식 증명 등을 학습하고 이를 프로그래밍언어(C/C++/Java)로 프로그래밍한다.

50181B 윈도우 구조와 원리 〈Operating System〉

컴퓨터 운영체제의 구조와 각각의 원리를 이해함으로써 응용프로그램의 수행과정에서 발생할 수 있는 문제점을 이해하고 컴퓨터의 운영 방법에 관하여 학습할 수 있다. CPU스케줄링, 프로세스의 동기화, Deadlock, 메모리 관리방법, 디스크 스케줄링 등의 원리를 살펴보고 이해한다.

50180B 모바일 프로그래밍 〈Mobile Programming〉

안드로이드 프로그래밍 개요, 유저 인터페이스, SQLite 데이터베이스, 액티비티와 프로세스, 스레드와 서비스, 네트워크, 멀티미디어에 관하여 학습한다.

50166B 사이버포렌식 〈Cyber Forensic〉

정보화 사회의 지속적인 진화는 많은 다양한 범죄가 사이버 세계에서 발생하고 있다. 이러한 사이버 세계의 과학적 수사를 말하는 사이버 포렌식을 이해하고, 컴퓨터에 남겨진 여러 자료들을 수집하여 법정에 제출하기까지의 과정을 학습할 수 있다.

50100C 실전 웹서버 해킹과 대응(캡스톤디자인)

〈Practical Web hacking & Response (capstone design)〉

웹 해킹 대응실무는 실무 중심의 교육과정으로서 실습을 통하여 다양한 웹 해킹기술을 이해하고, 해킹 대상 시스템에 대해 해커가 어떤 절차 및 방법을 이용하여 해킹을 수행하는지 실습을 통하여 이해하고 대응 방법을 학습한다.

50199B 운영체제 보안(캡스톤디자인) 〈Operating Systems Security (capstone design)〉

윈도우, 유닉스/리눅스 등 운영체제에 관련된 구조를 이해하고, 취약점을 분석한다. 운영체제별 취약점을 이용한 해킹 기법들을 알아보고, 해킹에 대응하기 위한 운영체제별 보안 설정에 관하여 학습한다. 컴퓨터 운영체제 상에 내재된 보안상의 결함으로 인하여 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 추가하는 방법을 학습한다.

50123B 통신소켓프로그래밍 〈Socket Programming for Communication〉

파일과 소켓, 네트워크 바이트순서, TCP 소켓 프로그래밍, UDP 소켓 프로그래밍, 멀티프로세스 소켓 프로그래밍, IPC, 고급 입출력 함수와 입출력 제어, 입출력 다중화, 멀티 스페드 소켓프로그래밍, RPC, 멀티캐스팅, IPV6 프로그래밍 등에 관하여 학습한다.

50197B 개인정보 침해대응 〈Personal Information Emergency Response〉

개인정보보호 및 개인정보 침해사고에 대응하는 개인정보보호법과 개인정보보호 Lifecycle, 개인정보보호관리체계(PIMS), 개인정보보호 영향평가(PIA)를 학습하고, 개인정보 관리자의 실무 능력 및 침해사고 발생 대처능력을 배양한다. 조직에 적합한 개인정보 침해대응체계를 구축할 수 있는 능력과 침해대응 세부 절차마다 고려해야 할 전반적인사항을 실습위주로 습득한다.

50178B 디지털 포렌식과 법규 〈Digital Forensic & Law〉

디지털 포렌식이란 컴퓨터에 남겨진 자료들을 수집하여 법적으로 효율성 있는 자료를 뽑아내는 작업이라 할 수 있다. 이러한 디지털 포렌식을 위한 분석 도구의 활용과 기본 원칙, 그리고 관련된 법률을 살펴본다.

50183B 모바일 애플리케이션 〈Mobile Application〉

안드로이드 응용 설계, 안도로이드 일반 응용 개발, 안드로이드 응용 기획 및 설계, 다양향 디바이스 및 고급 프로그래밍, 응용 프로젝트를 설계 및 개발한다.

50189B 악성코드 제작 및 분석 실무

〈Malicious Code Programming and Analysis of Professional Practice〉

기업과 연계하여 윈도우 바이러스, 매크로 바이러스, 트로이 목마와 웜, 인스턴트 메시징, 악성 자바 애플릿, 악성 액티브 X 컨트롤, 스마트폰 악성 코드, 랜섬웨어 등을 분석하고, 이들의 제작 과정을 이해하며, 이론과 실습을 병행하여 학습한다.

50190B 전자상거래 보안 실무 〈Electronic Commerce Security of Professional Practice〉

기업과 연계하여 전자 상거래 개요, 구현 요건, 암호 기술, 전자서명, 공개키 기반 구조, 전자지불시스템, 전자화폐 프로토콜, 전자입찰 프로토콜, 무선 플랫폼에서의 전자상거래보안, e-business를 위한 ebXML 보안, 공개키 기반구조(PKI) 개요 및 활용분야, SET, 전자 지불 시스템, 스마트 카드 보안 기술, 관련 법규 및 정보 윤리에 대해 이론과 실습을 병행하여 학습한다.

50176B 침입 탐지 및 차단 〈Intrusion Detection Blocking〉

침입 차단 시스템(Firewall), 침입탐지시스템(IDS) 그리고 침입 방지 시스템(IPS)의 이해, 원리, 종류, 작동방식, 특징, 구성, 실제 활용 등을 학습한다. 실무적으로 이들 시스템을 구축하고, 작동 원리를 이해한다. 가상 사설망(VPN)의 이해, 원리, 작동방식, 특징, 구성, 실제 활용 등을 학습한다.

50191B 모의해킹 실무 〈Penetration Testing of Professional Practice〉

기업과 연계하여 웹 기반 공격(SQL 인젝션, 파일 업로드 등) 애플리케이션 취약점을 악용하거나 시스템 권한을 획득하는 등 최근 공격 트랜드에 맞춘 네트워크 및 취약점 기반 모의해킹, 다양한 모의해킹 시나리오를 바탕으로 하여 실무 감각을 키울 수 있게 하고 침투테스트에 대한 결과 보고서를 작성하는 방법을 학습한다.

50192B 보안관제 실무 〈Information Security Controller of Professional Practice〉

기업과 연계하여 실제 호스트 및 IDS, 방화벽, 라우터 등 각종 네트워크 장비의 로그 및 패킷분석을 통하여 해커의 공격 방식을 이해하고 대응 능력을 키운다. IP 추적과 메일 추적, 공격자 모니터링 정책, 네트워크와 시스템 모니터링, 서버 모니터링 등을 통하여 침입에 대비한다. 공격자를 역추적 하고 사고에 대응하는 방법을 이론과 실습을 병행하여 학습한다.

50194B 보안 엔지니어 실무 〈Security Engineer of Professional Practice〉

기업과 연계하여 보안관련 어플리케이션, 솔루션, 장비 등에 필요한 개발능력, 보안설정 능력, 장비운영, 유지보수, 보안 프레임워크 설계, 보안 프로그래밍 등 실무와 연계하여 현장에 필요한 보안 엔지니어 능력을 양성하기 위하여 학습한다.

50195B 보안 컨설팅 실무〈Information Security Consulting of Professional Practice〉

기업과 연계하여 정보보호관리체계(ISMS), ISO27001, 개인정보보호관리체계(PIMS), 개인정보영향평가(PIA), 위험관리(Risk Management), 보안성평가(Common Criteria) 등 정보보안 컨설팅 방법등을 실무와 연계하여 학습한다.

50196B 취약점 진단 실무 〈Vulnerability Assessment of Professional Practice〉

시스템에 존재하는 취약점을 식별, 탐지하고 이를 활용한 공격과 방어방법을 학습한다. 또한 운영체제 취약점을 악용하거나 시스템 권한을 획득하는 등 최근 공격 트랜드에 맞춘 다양한 취약점 진단 능력을 배양한다. 기업에서 요구하는 취약점 진단을 위한 자동화 도구와 진단 스크립트 개발 및 적용 등 실습위주로 습득한다.

50193B 포렌식 실무 〈Digital Forensic of Professional Practice〉

기업과 연계하여 포렌식의 개념, 데이터를 영구 삭제하는 디가우징(degaussing) 등의 장비, 디스크 영역에 난수나 '0'을 덮어쓰는 방식으로 데이터를 삭제하는 와이핑(wiping) 기법, 데이터 은닉 기법과 같은 안티 포렌식의 각종 기법, 대응 방향 등 포렌식 우회기법의 이론과 실습을 병행하여 학습한다.

50157B 모바일 보안 〈Mobile Security〉

기업과 연계하여 아이폰 보안 프로그래밍, 안드로이드 보안 프로그래밍, 안드로이드 보안 프레임워크 설계, 스마트폰 보안 프로그래밍, 권한/정보 유출 악성 어플리케이션 보안, 플랫폼/기타 악성 어플리케이션 보안 위협, 무선 N/W 보안 프로젝트 등에 관하여 학습한다.

50144B 현장실습 〈Field Placement〉

현장에 나가 그 분야에서 필요로 하는 실무를 익히고 현장감을 기른다. 강의에서 배운 이론을 바탕으로 현장에서의 경험을 조율하여 효율적인 방법을 익힌다.