㈜한국정보보호교육센터 서울캠퍼스

정규과정 안내

위　　치 : 서울특별시 강남구 남부순환로 2645 한독빌딩 5층 SPACEHUB
교육문의 : 02-921-1465　카카오채널 : “한국정보보호교육센터” 검색

Features.

한국정보보호교육센터만의 차별점

1. 관계사인 시큐리티콘텐츠허브의 최신 동향 분석과 지속적인 기술 연구를 통해 만든 훈련장 등의 전문적인 콘텐츠를 활용하여 **실무에서 활용 가능한 강의**를 제공합니다.
2. 정보보안 기초부터 심화까지 단계적으로 학습할 수 있도록 설계되어 있으며, 정보보안을 처음 접하는 분들도 쉽게 이해하고 따라올 수 있습니다.
3. 안내 드린 과정 외에도 원하시는 일정과 주제로 교육 진행이 가능합니다. 문의 주시면 상세하게 안내해 드리겠습니다. (☏ 문의처 : 02-921-1465 / E. edu@kisec.com)

Contents.

2026년도 서울캠퍼스 정규과정

* 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

보안 직무 공통

정규과정

- 암호학
- 윈도우 서버 기초
- 리눅스 서버 기초
- 프로그래밍 기초
- 리버스 엔지니어링 기초
- 네트워크 기초
- IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음

KISEC

이산 수학부터 시작하는 암호학의 모든 것

기초 수학과 암호학의 핵심 개념을 함께 학습해 보안 이론의 기초를 탄탄히 잡는 과정입니다. 대칭·비대칭 암호 등 주요 기술을 이해하며 실무에서 활용할 수 있는 기반 역량을 갖춥니다.

Overview
교육 개요

교육 일수	2일 (일 8시간, 총 16시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	입문
수강료	900,000원
교육 주제	1. 암호학의 기초와 그의 기반인 이산 수학에 대해 학습 2. 대칭키 암호와 비대칭키 암호를 식별할 수 있도록 학습 3. 보안의 기본이 되는 암호학의 원리와 암호학의 응용에 대해 파악
교육 특징	1. 암호학의 기반이 되는 기초 수학부터 습득 가능 2. 암호학에서 자주 쓰이는 수학의 개념에 대해 학습으로 기본기 함양 3. 시대별 암호학의 개념에 대해 파악 가능
교육 대상	1. 보안에서 사용되는 암호 알고리즘에 이해가 필요하신 분 2. 시스템 상의 기본 연산에 대한 이해가 필요하신 분

이산 수학부터 시작하는 암호학의 모든 것

Curriculum, 커리큘럼

주제	내용	
기초수학	이산수학 개요	이산수학 정의
		주요 주제
	논리와 명제	명제
		부정
		논리곱
		논리합
		배타적 논리합
		논리적 동치
	증명론	수학적 귀납법
	집합론	집합
		집합의 표현
		기수
		상등
		집합의 종류
	관계론	기본 관계
		n항 관계
		역관계
	행렬	행렬
	정수 집합	정수 연산
		모듈 연산
	군, 환, 체	이항연산
		군, 환, 체

이산 수학부터 시작하는 암호학의 모든 것

Curriculum, 커리큘럼

주제	내용	
암호학	암호학 개요	암호학 개요
	암호학 기본 개념	암호 기법 분류
		암호학 기본 개념
		암호와 보안 상식
		암호 알고리즘의 분류
		암호해독
	암호 해독 공격	암호문 단독 공격
		알려진 평문 공격
		선택 평문 공격
		선택 암호문 공격
		선택 원문 공격
	고전암호 개념	고전암호 개념
	전치암호	전치암호
	단순 치환 암호	카이사르 암호
		ROT13
		곱셈 암호
	근대암호 개념	근대암호 개념
	다중 치환 암호	비즈네르 암호
		플레이페어 암호

이산 수학부터 시작하는 암호학의 모든 것

Curriculum, 커리큘럼

주제	내용	
암호학	기계 치환 암호	기계 치환 암호
	현대암호	현대암호의 기술적 분류
		현대암호의 기능적 분류
		대칭키 암호
		블록암호
		스트림 암호
		비대칭키 암호
		대칭키와 비대칭키 암호 비교
	블록암호 (설계 / 운영 / DES / AES)	블록암호 설계
		블록암호 알고리즘
		블록 운영모드
		블록 운영모드 종류
		전자 코드북
		암호 블록 체인
		증식적 암호 블록 체인
		암호 피드백
		출력 피드백
		카운터
		블록 운영모드 비교
		DES 블록암호 알고리즘
		AES 블록암호 알고리즘

이산 수학부터 시작하는 암호학의 모든 것

Curriculum, 커리큘럼

주제	내용	
암호학	디피 헬만 키 합의	디피 헬만 키 합의 알고리즘
	RSA / ElGamal	RSA 개요
		RSA 활용
		RSA의 안전성
		RSA에 대한 공격
		RSA 디지털 서명메시지 다이제스트에 대한 RSA 서명
		ElGamal 개요
		ElGamal 분석
		ElGamal의 보안
		ElGamal 디지털 서명
	OpenSSL을 이용한 암호화 실습	OpenSSL을 이용한 암호화 실습
	카이사르 암호 해독	카이사르 암호 해독
	해시캣을 이용한 해시 크랙	해시캣을 이용한 해시 크랙
	Cryptool2을 이용한 암호 해독	Cryptool2
		Scytale 암호 해독
		DES 취약키 암호화
		DES 준 취약키 암호화

다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential

윈도우 서버 구조와 핵심 관리 기능을 중심으로 실무에서 꼭 필요한 운영 능력을 익히는 과정입니다. 명령어 활용과 보안 정책 설정 등 주요 기능을 직접 실습하며 서버 관리의 기본기를 쌓습니다.

Overview
교육 개요

교육 일수	4일 (일 8시간, 총 32시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	입문
수강료	900,000원
교육 주제	1. 주요 프로세스, 구조 등을 학습하면서 윈도우 서버 운영체제 활용 2. 윈도우 운영체제의 기본 명령어 활용하고 레지스트리, 보안 정책 등 관리
교육 특징	1. 가상환경 구축을 통해 윈도우 서버 운영체제의 기능 실습 2. 명령어 및 기능을 효과적으로 습득할 수 있도록 실습 위주의 학습
교육 대상	1. 일상생활 속에서 사용하고 있는 윈도우의 추가적인 기능을 활용하고 싶으신 분 2. 정보보안 입문을 위해 운영체제부터 공부하고 싶으신 분

다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential

Curriculum, 커리큘럼

주제	내용	
윈도우 개요	윈도우 개요 및 역사	윈도우 개요
		윈도우 역사
윈도우 아키텍처 및 부팅순서	윈도우 아키텍처	윈도우 NT 아키텍처
		유저 모드
		커널 모드
	윈도우 운영체제 부팅 과정	윈도우 운영체제 부팅 과정
주요 프로세스 및 서비스	윈도우 주요 프로세스	프로세스의 이해
		프로세스 종류(Windows 7)
		프로세스 종류(Windows 10)
	윈도우 주요 서비스	윈도우 서비스 개요
		서비스 확인
		주요 서비스
레지스트리	윈도우 레지스트리의 이해	레지스트리 개요
		윈도우 레지스트리 구성
		윈도우 레지스트리의 구조
		윈도우 레지스트리 명령어
파일 시스템	파일 시스템과 디스크의 이해	파일시스템
		윈도우 파일시스템 종류
		디스크

다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential

Curriculum, 커리큘럼

주제	내용	
윈도우시스템 관리	윈도우 계정의 이해	윈도우 계정 분류
	윈도우 계정 관리	명령어를 이용한 계정 관리
		GUI 환경을 이용한 계정 관리
	파일시스템과 디스크 관리 실습	파일시스템 구성
		윈도우 파티션 구성 실습
	공유 폴더 관리	공유 폴더 개요
		공유 폴더 사용을 위한 관련 서비스
		공유 폴더 관련 설정 및 고려사항
		공유 폴더 실습
	서비스 관리	윈도우 서비스 관리 방법
	로컬 보안 정책 관리	로컬 보안 정책 개요
		로컬 보안 정책 내보내기 & 불러오기
		로컬 보안 정책 – 계정 정책
		로컬 보안 정책 – 로컬 정책
	이벤트 로그 관리	이벤트 로그의 활용
		이벤트 로그 분류
		이벤트 로그 종류
		이벤트 로그 속성
		이벤트 로그 수준 종류
		이벤트 로그 감사 정책
		보안 로그 필터링
		이벤트 로그 관리 설정 – 레지스트리
윈도우 분석 도구	윈도우 분석 도구 소개	Windows Sysinternals

다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential

리눅스의 주요 구조와 필수 명령어를 바탕으로 서버 운영의 기본을 체계적으로 익히는 과정입니다. 파일·퍼미션·프로세스 등 핵심 기능을 실습하며 실무 환경에서도 활용 가능한 운영 역량을 확보합니다.

Overview
교육 개요

교육 일수	4일 (일 8시간, 총 32시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	입문
수강료	900,000원
교육 주제	1. 리눅스 서버 운영체제, 기본 명령어를 활용할 수 있는 역량 개발 2. 리눅스에서 프로세스, 파일 및 디렉터리 등을 생성하고 관리할 수 있는 능력
교육 특징	1. 가상환경 구축을 통해 리눅스 서버 운영체제의 기능 실습 2. 명령어 및 기능을 효과적으로 습득할 수 있도록 실습 위주 학습
교육 대상	1. 정보보안 입문을 위해 운영체제부터 공부하고 싶으신 분 2. 리눅스 운영체제를 사용해야 하는데 처음 접해보신 분

다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential

Curriculum, 커리큘럼

주제	내용	
리눅스 역사 및 종류	리눅스의 역사	리눅스의 역사
	리눅스 종류와 소개	유닉스개요
		유닉스 종류
		리눅스 개요
		리눅스 종류
리눅스 쉘 & 부팅과정	리눅스 쉘	리버스 서버 쉘의 이해
	리눅스 운영체제 부팅과정	부팅과정
		ROM-BIOS
		부트 로더 로딩
		프로세스 실행
		매직키 설정
		가상 터미널 실행
리눅스 설치 및 시작	설치와 기본 환경 구성	다운로드
		VMware 구성
		CentOS 설치
		X 윈도우 설치
	리눅스 기본 명령어	리눅스 기본 명령어
	Vim 에디터 사용법	Vim 에디터 사용법
네트워크 구성 및 관리	네트워크 구성	네트워크 구성의 이해
		네트워크 구성
		네트워크 트러블 슈팅
파일시스템 구조 및 디렉터리	파일과 디렉터리 이해	파일과 디렉터리 이해
		링크 파일
	파일시스템 이해와 디스크 관리	파일시스템 이해
		리눅스 파일시스템 이해
		디스크 관리

다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential

Curriculum, 커리큘럼

주제	내용	
사용자 및 퍼미션 관리	사용자 이해와 관리	계정의 이해
		계정 관리
		계정 관리 관련 파일 및 디렉토리
		계정 관리
		그룹 관리
	퍼미션의 이해와 관리	퍼미션과 소유권
		소유권 관리
		퍼미션의 이해
		퍼미션의 관리
		SetUID, SetGID, Sticky bit
리눅스 시스템 관리	프로세스 이해와 관리	프로세스
		시그널
		데몬
		데몬 관리
		프로세스의 제어
		프로세스와 /proc 디렉터리
		프로세스 스케줄링
	패키지 관리	리눅스 패키지 관리기법
		rpm
		yum
		dpkg
		apt-get
	로그 이해와 관리	rsyslog
		logrotate
		로그 관련 주요 파일
	리눅스 접근통제 기법	리눅스 방화벽(iptables)
		리눅스 방화벽(TCP Wrapper)

논리적 사고방식으로 이해하는 프로그래밍 기초

프로그래밍의 기본 개념과 알고리즘 사고를 이해하며 개발에 필요한 기초 역량을 쌓는 과정입니다. C언어 실습을 통해 프로그램 흐름과 제어 구조를 직접 구현해 보며 실무 적용력을 높입니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	입문
수강료	900,000원
교육 주제	1. 프로그래밍 기술을 외우는 게 아닌 이해하고 활용할 수 있는 역량 강화 2. 프로그래밍 시 필요한 알고리즘 작성하는 방법 이해
교육 특징	1. 기본부터 응용까지 다양한 프로그래밍 기본 지식을 학습 2. 여러가지 간단한 프로그램을 만들어 봄으로써 알고리즘을 작성하는 방법 학습
교육 대상	1. 임베디드 시스템 개발자 2. C언어 기반의 프로그램 개발을 희망하는 자

논리적 사고방식으로 이해하는 프로그래밍 기초

Curriculum, 커리큘럼

주제	내용	
프로그래밍 개요	프로그래밍 의미	프로그래밍의 학문적 정의
		프로그래밍의 간단한 정의
	프로그래밍 접근방법	컴퓨팅 사고력
	프로그래밍을 배워야 하는 이유	프로그래밍을 배워야 하는 이유
	프로그래밍 vs 코딩	프로그래밍 vs 코딩
	프로그래머의 딜레마	프로그래머의 딜레마
	프로그래머의 사고 방식	프로그래머의 사고 방식
	프로그래밍 순서	설계 과정
		구현 과정
		보완 과정
	프로그래밍 고려사항	프로그래밍 고려사항
프로그래밍 언어	프로그래밍 언어 개요	역사
		정의
		요소
	프로그래밍 언어 분류	처리 수준에 따른 분류
		해석 방식에 따른 분류
		패러다임에 따른 분류
	프로그래밍 언어 순위	프로그래밍 언어 순위

논리적 사고방식으로 이해하는 프로그래밍 기초

Curriculum, 커리큘럼

주제	내용	
C언어 프로그래밍	C 언어 개요	탄생배경
		탄생 이후의 C 언어
		특징
		C 언어 표준
	IDE 설치	VS(Visual Studio) Code 개요
		VS(Visual Studio) Code 설치
		VS(Visual Studio) Code GCC 설치
		VS(Visual Studio) Code 빌드 설정
	C 언어 기본 구조	구성 요소
		키워드
		식별자
	변수와 기본 자료형	변수(Variables)
		상수(Constant)
		자료형(Data Type)
	데이터 입출력	표준 스트림(Standard steam)
		이스케이프 시퀀스(Escape Sequence)
		형식 지정자(Format Specifier)
		printf 함수
		scanf 함수
		puts 함수
		gets 함수
		putchar 함수
		getchar 함수

논리적 사고방식으로 이해하는 프로그래밍 기초

Curriculum, 커리큘럼

주제	내용	
C언어 프로그래밍	연산자	산술 연산자(Arithmetic operators)
		관계 연산자(Relational operators)
		논리 연산자(Logical operators)
		비트 연산자(Bitwise operators)
		대입 연산자(Assignment operators)
		기타 연산자
		C언어 연산자 우선순위 (C Operator Precedence)
	반복문과 조건문	반복문과 조건문
	함수	함수의 종류
		정의
		함수의 원형 선언
		변수의 유효 범위
		변수의 종류
		재귀 호출
	배열과 포인터	배열(Array)
		배열(Array) 선언 및 초기화
		N차원 배열(N-dimensional array)
		포인터의 개념
		포인터 연산자
		포인터 선언
		포인터 연산
		다양한 포인터
		배열과 포인터의 관계

논리적 사고방식으로 이해하는 프로그래밍 기초

Curriculum, 커리큘럼

주제	내용	
C언어 프로그래밍	구조체	구조체의 정의와 선언
		구조체 사용 이유
		typedef 키워드
		구조체 멤버 접근 방법
		구조체 변수의 초기화
		구조체 배열 선언
		구조체 포인터
		함수와 구조체
		중첩 구조체
	문자열 관련 함수	문자열 개요
		문자열 비교 함수
		문자열 복사 함수
		문자열 길이 확인 함수
		문자열 연결 함수
		기타 문자열 처리 함수
	파일 입출력	개요
		파일 스트림 생성
		파일 입출력 함수
	메모리 관리와 동적 할당	개요
		메모리 구조
		힙(Heap)
		메모리 동적 할당 시 사용되는 함수
	헤더 및 전처리 지시자	전처리 지시자 개요
		헤더 예제 및 연습 문제
	자료구조	개요
		선형 구조 종류 – 배열(Array)
		선형 자료구조 종류 – 연결 리스트(Linked list)
		선형 자료구조 종류 – 큐(Queue)
		선형 자료구조 종류 – 스택(Stack)
		비선형 자료구조 종류 – 트리(Tree)
		비선형 자료구조 종류 – 그래프(Graph)

어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론

어셈블리어와 시스템 구조를 이해하며 리버스 엔지니어링의 분석 흐름을 익히는 입문 과정입니다. 정적·동적 분석을 함께 실습해 프로그램 동작을 해석하는 능력을 기르며 기초 분석 역량을 강화합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	입문
수강료	900,000원
교육 주제	1. 리버스 엔지니어링의 기초 개념과 각 분야별 활용법 이해 2. 시스템 아키텍처에 대한 이해를 바탕으로 정적/동적 분석 수행
교육 특징	1. 리버스 엔지니어링 실습 시 어셈블리어부터 레지스터, 메모리까지 단계별 실습 2. 프로그래밍 기반 기초 문법들로 구성하여 기본적인 루틴을 단계별 학습 3. 프로그램 흐름을 파악하고 효율적인 분석을 방안 학습
교육 대상	1. 리버싱 분야의 해킹대회 문제에 도전해보고 싶으신 분 2. 리버스 엔지니어링을 실습위주로 이해하고 싶으신 분

어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론

Curriculum, 커리큘럼

주제	내용	
리버스 엔지니어링	리버스 엔지니어링 개요	정의
		분석 방법
		언어별 리버스 엔지니어링 방법
		리버스 엔지니어링의 순기능
		리버스 엔지니어링의 역기능
	리버스 엔지니어링과 법	리버스 엔지니어링과 법
CPU 구조	컴퓨터 구조 개요	하드웨어
		소프트웨어
		컴퓨터 하드웨어의 구성요소
		메인 메모리
		입출력 버스
		폰 노이만 구조
	구조 및 기능	CPU
		프로그램 실행
인텔 아키텍처의 이해	인텔 아키텍처 구성과 역사	인텔 아키텍처 구성과 역사
	인텔 아키텍처 기본 구조	인텔 아키텍처 기본 구조
메모리 구조	메모리 구조 개요	정의
		역할
		선형 주소 공간
		텍스트 영역
		데이터 영역
		힙 영역
		스택 영역
	OS에 따른 메모리 구조	OS에 따른 메모리 구조

어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론

Curriculum, 커리큘럼

주제	내용	
레지스터	레지스터의 이해	레지스터의 이해
	범용 레지스터	범용 레지스터
	세그먼트 레지스터	세그먼트 레지스터
	플래그 레지스터	플래그 레지스터
	명령 포인터 레지스터	명령 포인터 레지스터
어셈블리어 기초	어셈블리어 개요	정의
	어셈블리어 종류	스택 조작
		데이터 저장
		함수 호출
		연산
		어셈블리어 명령어
		데이터 타입 종류
		Operand 타입
리버스 엔지니어링 툴 소개	리버스 엔지니어링 툴 개요	리버스 엔지니어링 툴 개요
	리버스 엔지니어링 툴 종류	디스어셈블러(DisAssembler) – IDA pro
		디버거(Debugger) – WinDbg
		디버거(Debugger) – OllyDbg
	OllyDbg	OllyDbg
리버스 엔지니어링 실습	데이터 입출력 프로그램	데이터 입출력 프로그램
	파라미터와 데이터 표현방식	파라미터와 데이터 표현방식
	분기문	분기문
	반복문	반복문
	배열	배열
	구조체	구조체
	파일 입출력	파일 입출력
	메모리 동적 할당	메모리 동적 할당
	함수호출규약	함수호출규약
	리버스 엔지니어링 실습	리버스 엔지니어링 실습

다양한 실습으로 쉽게 이해하는 네트워크 Essential

네트워크의 기본 구조와 주요 프로토콜을 이해하며 통신 흐름을 전체적으로 파악하는 과정입니다. 패킷 분석 도구를 활용해 실제 네트워크 동작을 직접 확인하며 기초 네트워크 설계와 운영 능력을 갖춥니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 기본 용어, 모델에 대한 이해를 통해 네트워크의 전체적인 흐름 파악 2. 네트워크 모델인 OSI 7 계층과 TCP/IP 모델 학습
교육 특징	1. 네트워크의 각 계층에서 주로 사용하는 프로토콜의 헤더를 보며 상세히 학습 2. 네트워크 망 구축 실습을 통해 네트워크에 대한 이해
교육 대상	1. 네트워크에 대한 이해를 필요로 하시는 분 2. 네트워크 망 구축에 대한 역량을 강화하고 싶은 분

다양한 실습으로 쉽게 이해하는 네트워크 Essential

Curriculum, 커리큘럼

주제	내용	
네트워크 개요	네트워크 역사	글로벌 네트워크 역사
		국내 네트워크 역사
	네트워크 용어의 이해	네트워크의 의미
		프로토콜의 의미
		네트워크 분류
		토큰링
		CSMA/CD
		CSMA/CA
	네트워크 모델의 이해	추상화
		네트워크 모델의 종류
	OSI 7 계층 모델	OSI 7 계층
		OSI 7 계층 구조
		OSI 7 계층 정리
	TCP/IP 4 계층 모델	TCP/IP 모델 계층 구조
근거리 네트워크 구성	근거리 네트워크 구축 실습	근거리 네트워크 구축 실습
	OSI 7 계층 모델 1, 2계층	물리 계층
		데이터 링크 계층
	스위치 개요와 종류	스위치
		L2 스위치
		L3 스위치
		L3 스위치
		L4 스위치
		L7 스위치
	데이터링크 계층의 이해	데이터링크 계층과 링크 계층
		데이터링크 계층의 서비스
	ARP의 이해	ARP 구조
		ARP 동작 원리
	MAC 주소 체계	개요
		구조

다양한 실습으로 쉽게 이해하는 네트워크 Essential

Curriculum, 커리큘럼

주제	내용	
라우터가 포함된 망 구성	라우터가 포함된 네트워크 구성	라우터가 포함된 네트워크 구성
	OSI 7 계층 모델 3계층	OSI 7 계층 모델 3계층
	IPv4의 이해	IP의 이해
		IPv4 클래스
	서브넷의 이해	서브넷 마스크의 이해
		서브넷팅의 이해
	IPv6의 이해	IPv6의 이해
		IPv4와 IPv6
	ICMP의 이해	ICMP의 이해
	NAT의 이해	NAT의 이해
	터널링의 이해	개요
		종류
	터널링 구성 실습	GRE 터널링 구성 실습
		GRE over IPSEC 개요
		GRE over IPSEC 터널링 구성 실습
대규모 망 구성	OSI 7 계층 모델 4계층	전송 계층
	TCP와 UDP	TCP
		3-Way Handshake
		UDP
		TCP/UDP 비교
	OSI 7 계층 모델 5~7계층	세션 계층
		표현 계층
		어플리케이션 계층
	라우터와 라우팅 알고리즘	라우터 개요
		라우팅 알고리즘 종류
		라우팅 프로토콜
		라우팅 재분배
	여러 대의 라우터를 활용한 망	IP할당
		동적라우팅-OSPF
		정적라우팅

IT 기초 지식부터 보안까지 보안 운영자를 위한 첫 걸음

IT 기본 구조와 시스템 운영 개념을 이해하며 보안 운영에 필요한 기초 역량을 쌓는 과정입니다. 서버·네트워크·취약점 진단 등 핵심 요소를 폭넓게 학습해 보안 담당자로서의 기반을 마련합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. IT 인프라 내 보안을 하기 위한 목적과 대상을 명확히 이해 2. 기본적으로 알아야 하는 서버 및 장비 운용 핵심 지식 습득 3. 보안 솔루션 장비의 종류와 기본적인 운용 방식 습득
교육 특징	1. 인프라를 기반으로 보안 직무와 그 역할부터 데이터의 흐름까지 한 눈에 이해 2. 초급 재직자를 위한 기반 지식 리마인드 및 직무별 팁 전수 3. 특정 직무에 특화되지 않고, 모든 보안 직무에 공통적으로 알아야 할 내용으로 구성
교육 대상	1. **신입 보안담당자:** '일잘러'로 성장하기 위한 IT 기초 지식 및 보안 인프라 이해 2. **직무순환 대상자:** 보안 직무는 처음이라 막막한 직무순환 대상자를 위한 기초 교육 3. **신입 보안솔루션 운영자:** 보안 솔루션이 낯선 신입 운영자를 위한 기초 교육
Point !	기존에 보유한 기본 IT 지식을 바탕으로 하기에 교육 수강에 필요한 요소를 전반적으로 복습합니다. 리눅스 명령어, 네트워크 기초 지식을 사전에 습득했다면 보다 수강하기 수월할 수 있습니다.

IT 기초 지식부터 보안까지 보안 운영자를 위한 첫 걸음

Curriculum, 커리큘럼

주제	내용	
사내 인프라 구성도로 보는 보안직무와 그 역할	직무 별 하는 일	인프라 구성도를 통한 직무별 이해
서버 또는 장비 관리를 위한 필수 기능 이해하기	시스템 개요	컴퓨터 시스템 개요
		컴퓨터 시스템 분류 방식
		처리 방식 기준
		처리 규모 기준
		시스템 구조
		폰 노이만의 시스템 구조
		하버드의 시스템 구조
	리눅스 기초	유닉스 개요 및 종류
		리눅스 개요 및 종류
		리눅스 기본 명령어
		네트워크 구성의 이해
		네트워크 구성
		네트워크 트러블 슈팅
		퍼미션과 소유권
		소유권 관리
		퍼미션의 이해 및 관리
		SetUID, SetGID, Sticky bit
		프로세스
		시그널
		데몬 관리
		프로세스의 제어
		프로세스와 /proc 디렉터리
		프로세스 스케줄링

IT 기초 지식부터 보안까지 보안 운영자를 위한 첫 걸음

Curriculum, 커리큘럼

주제	내용	
내 PC부터 웹 접속까지 데이터 흐름 이해하기	네트워크 보안 배경지식	OSI 7 계층 모델의 이해
		TCP/IP 4 계층 모델의 이해
		DoS 공격의 이해와 종류
		DDoS 공격의 이해와 종류
		DDoS 대응 프로세스
	네트워크 공격	대역폭 공격 실습
		자원 소진 공격 실습
		웹/DB 부하 공격 실습
	네트워크 장비	스위치 개요와 종류
	웹 서버의 이해	웹 서비스 구성
		클라이언트 & 서버
		클라이언트 & 서버 측 언어의 이해
		HTTP 프로토콜 이해
		SSL과 TLS의 이해
필수로 알아야할 보안 장비 운영하기	보안 인프라 구성	보안 솔루션 종류와 이해
		방화벽 이해와 종류
	오픈소스 방화벽 서비스 구축	방화벽 기능의 이해
		방화벽 구축 환경을 위한 설계 이해
		오픈소스를 활용한 방화벽 구축
	오픈소스 방화벽 운영	방화벽 룰 특징의 이해
		방화벽 룰 적용 실습
	오픈소스 IPS 구축	IDS/IPS 개요
		IPS 구축 환경을 위한 설계 이해
		오픈소스를 활용한 IPS 구축
	IDS/IPS 패턴 제작	룰의 이해
		IDS/IPS 룰 패턴 제작
		IDS/IPS 룰 패턴 실습
더 알아두면 좋은 정책과 가이드	정보보호 법·제도 현황	정보보호 법·제도 현황
	ISMS-P 인증	ISMS-P 인증
	기술적 취약점 분석·평가 방법 상세가이드	기술적 취약점 분석·평가 방법 상세가이드
	전자금융기반시설 보안 취약점 안내서	전자금융기반시설 보안 취약점 안내서
	정보보호시스템 구축을 위한 실무가이드	정보보호시스템 구축을 위한 실무가이드
	OWASP Top 10	OWASP Top 10

위협 & 분석

정규과정

- 네트워크 해킹
- 어플리케이션 해킹
- 운영체제 해킹
- 웹 해킹
- IoT 보안

KISEC

네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z

네트워크 환경에서 발생하는 다양한 위협을 이해하고 공격·방어 기술을 실습하는 과정입니다. 유·무선 구간별 보안 개념을 학습하며 패킷 분석과 대응 기법을 통해 실무형 네트워크 보안 역량을 강화합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 다양한 종류의 실습으로 네트워크의 공격 방법과 원리 이해 2. 공격 과정을 통해 대응할 수 있는 방법을 이해하고 실무 적용 역량 향상
교육 특징	1. 네트워크 중심의 다양한 종류의 공격 방법 실습 2. 침해사고 발생 시 네트워크 흔적을 분석하는 방법 학습 3. 무선랜 환경에 대해 이해하고, 지나치기 쉬운 취약한 무선랜 보안에 대한 이해
교육 대상	1. **네트워크 보안 담당자:** 공격 및 분석에 대해 실습하면서 유·무선 네트워크에서 발생할 수 있는 위협에 대비할 수 있는 실무 능력 향상에 도움 2. **정보보호 관련 실무자:** 다양한 유형의 공격 실습으로 유·무선 네트워크 위협에 대해 이해하고 학습 3. **취업준비생, 대학생:** 네트워크 분야의 위협을 식별할 수 있는 역량 강화로 관련 분야 취업 준비에 도움

네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z

Curriculum, 커리큘럼

주제	내용	
네트워크 해킹	네트워크 해킹 개요	네트워크 공격 통계
		개요
		네트워크 위협 요소
		보안 요소별 공격 유형 분류
	네트워크 스캐닝	네트워크 개요
		절차
		활동 범위 결정
		네트워크 목록 수집
		DNS 질의
		네트워크 정찰
		스캔 종류
	네트워크 스캐닝 실습	Nmap Option
		Nmap 활용
		스캔 종류
		TTL 값을 이용한 운영체제 추측
		Banner Grabbing
		Hping3를 이용한 스캐닝
		SYN 스캔
		UDP 스캔
		ICMP 스캔
	근거리 네트워크 공격 개요	근거리 네트워크 위협
		ARP 스푸핑을 이용한 MITM 공격
	ARP 스푸핑 공격 실습	환경 구성
		공격 실습
		ARP 스푸핑 공격 이후 URL 스캔 공격
		ARP 스푸핑 공격 이후 DNS 스푸핑 공격
	DHCP Starvation 공격 실습	환경 구성
		공격 실습

네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z

Curriculum, 커리큘럼

주제	내용	
네트워크 해킹	DoS / DDoS 공격의 이해와 종류	DoS와 DDoS 오해
		DoS 공격 역사
		DoS 공격의 최근 동향
		과거의 DoS 공격
		DoS 공격 종류
		DDoS 공격 종류 – 자원 소진
		DDoS 공격 종류 – 대역폭
		DDoS 공격 종류 – 대역폭(DRDoS)
		DDoS 공격 종류 – 웹/DB 부하
	DDoS 대응 프로세스	DDoS 예방 대책
		DDoS 방어 대책
	대역폭 공격 실습	UDP Flood 공격
		ICMP Flood 공격
	자원 소진 공격 실습	SYN Flood 공격
		ACK Flood 공격
		FIN Flood 공격
	웹/DB 부하 공격 실습	RUDY 공격
		TorsHammer 공격
		Slowloris 공격
	TCP 연결 기반 DoS 공격 실습	TCP 연결 구조
		환경 구성
		TCP 연결 강제 종료
암호화 통신과 위협	SSL과 TLS의 이해	HTTPS의 이해
		SSL의 이해
	암호화 통신 공격의 이해	SSL MITM 공격의 이해
		SSL Strip공격의 이해
		Heartbleed의 이해
		POODLE의 이해
	SSL Strip 공격 실습	실습 환경 구성
		공격 실습
	Heartbleed 공격 실습	실습 환경 구성
		공격 실습

네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z

Curriculum, 커리큘럼

주제	내용	
네트워크 패킷 분석	패킷 분석 방법	패킷 수집 기법
		Wireshark설정
		Wireshark 주요 메뉴
		Wireshark 필터링 기법
		공격별 분석 기법
		분석 상세 기법
		Snort를 활용한 분석
	정규 표현식	개요
		종류
		기본 문법
		정규 표현식의 이해 및 실습
		정규 표현식 예제 실습
무선 네트워크 위협	무선 네트워크 해킹 개요	국·내외 사례
		물리적인 취약요소
		기술적인 취약요소
		무선랜 보안기술
		무선 네트워크 위협 요인
		관리적인 취약요소
		무선랜 구축 시 고려사항
		무선랜 운영 시 고려사항
		무선랜 보안을 위한 주체 별 역할
		무선랜 보안 체크리스트
	무선랜 인증 방식의 이해	WEP
		무선랜 인증 방식
		무선랜 암호화 방식
		GPU를 이용한 WPA Cracking
	WEP 암호화 방식 공격 실습	WEP Key Crack 실습
	WPA 암호화 방식 공격 실습	WPA/WPA2 Crack 실습

소프트웨어 취약점의 동작 원리부터 익스플로잇까지! 어플리케이션 해킹

소프트웨어 취약점의 구조와 공격 원리를 이해하며 다양한 공격 기법을 다루는 과정입니다. 버퍼 오버플로우 등 주요 취약점을 실습 기반으로 익히며 보안 취약점이 실제로 어떻게 악용되는지 파악합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 소프트웨어 보안 취약점에 대해 이해하고 이를 해결할 수 있을 방안 이해 2. 해킹대회에 출제되는 다양한 Pwnable 문제에 대한 해결 역량 강화
교육 특징	1. 기초부터 단계적으로 학습함으로써 소프트웨어 취약점의 원리를 이해 2. 소프트웨어 보안을 위한 메모리 보호 기법의 원리를 학습하고 이를 우회하기 위한 방법 이해
교육 대상	1. 해킹대회(CTF) Pwnable 분야에 대한 공부를 시작하고 싶으신 분

소프트웨어 취약점의 동작 원리부터 익스플로잇까지! 어플리케이션 해킹

Curriculum, 커리큘럼

주제	내용	
어플리케이션 취약성 개요	소프트웨어 취약성 개요	버그(Bug)
		크래쉬(Crash)
		취약성(Vulnerability)
	어플리케이션 취약점과 취약성	소프트웨어 취약성
		취약점(Weakness) vs 취약성(Vulnerability)
		소프트웨어 취약성 판단
		소프트웨어 취약점 구분
		소프트웨어 취약점 파급력
메모리 구조	메모리 구조 개요	메모리 정의
		메모리 모델
		메모리 구조
	OS에 따른 메모리 구조	메모리 구조 차이
버퍼 오버플로우	버퍼 오버플로우 개요	버퍼 오버플로우
	스택 기반 버퍼 오버플로우	스택 기반 버퍼 오버플로우
	스택 기반 버퍼 오버플로우 실습	스택 기반 버퍼 오버플로우 실습
	Shellcode	Shellcode 개요
		Shellcode 제작
		Shellcode 삽입
		기타 Shellcode

소프트웨어 취약점의 동작 원리부터 익스플로잇까지! 어플리케이션 해킹

Curriculum, 커리큘럼

주제	내용	
메모리 보호 기법과 우회 기법	구조적 예외 핸들러	개요
		Windows 예외 처리 개요
		구조적 예외 핸들러 구조
		구조적 예외 핸들러 공격
	데이터 실행 방지	개요
		데이터 실행 방지 설정
		데이터 실행 방지 적용
	Return-to-Library(RTL)	개요
		Return-to-Library(RTL) 동작 원리
	임의의 주소 공간 배치 (ASLR)	개요
		임의의 주소 공간 배치 원리
	스택 카나리	개요
		Canary Leak을 이용한 메모리 보호기법 우회
	Return-to-Oriented-Programming(ROP)	개요
		Return to Oriented Programming 동작 원리
정수 오버플로우	정수 오버플로우 개요	정수 오버플로우 정의
		동작 원리
	정수 오버플로우 종류	정수 오버플로우 종류
		종류 별 정수 오버플로우 동작 원리
취약성 관리 체계	CVE 코드의 이해	CVE 개요
		번외 자료
	CVSS 산출 방식과 위험성 평가의 이해	CVSS 산출 방식과 위험성 평가의 이해
	CWE 코드의 이해	CWE 코드의 이해
		SANS CWE Top 25

Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹

운영체제의 취약점을 이해하고 Metasploit 등 도구를 활용해 공격·대응 절차를 익히는 과정입니다. 윈도우와 리눅스 환경을 실습해 실제 취약점 활용 방식과 방어 전략을 함께 경험할 수 있습니다.

Overview
교육 개요

교육 일수	4일 (일 8시간, 총 32시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 운영체제(윈도우, 리눅스)를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법에 대해 학습 2. 공격 이후에 대응할 수 있는 방안에 대해 실제 현업에서 적용할 수 있는 사례 기반의 내용으로 이해
교육 특징	1. 실제로 운영체제를 공격할 때 많이 사용하는 툴을 이용하여 취약점 정보 수집 실습 진행 2. 도구에 내장된 공격코드 뿐 아니라 최근 공격코드 관련해서 알아보고 이를 응용할 수 있는 방법에 대해 실습 3. 대응방안 수립 시 일반적인 내용이 아닌 근본적인 대책과 차선책에 대해 학습
교육 대상	1. **정보보안 컨설턴트:** 활용도가 높은 공격기법의 원리를 이해하여 모의해킹 업무의 수행 능력을 향상 2. **정보보호 관련 실무자:** 입문부터 활용 단계까지 학습하여 윈도우, 리눅스 등 운영체제 해킹에 대한 이해를 통해 보안 강화 3. **취업준비생, 대학생:** 모의해킹이나 취약점 분석 분야로 직무를 설정한 다음 그에 맞는 역량 강화를 준비하는데 도움

Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹

Curriculum, 커리큘럼

주제	내용	
운영체제 해킹 개요	윤리적이고, 합법적인 해킹	컴퓨터 해커
		범죄적 해킹
		우호적 해킹
		법의 회색 지대
	모의해킹 방법론	모의해킹 개요
		모의해킹과 범죄자 비교
		모의해킹 범위 – 시스템 접근 기준
		모의해킹 범위 – 수행 관점 기준
		모의해킹 종류
		모의해킹 업무 절차
정보수집	스캐닝 개요	스캐닝 대분류
	웹사이트 정보 수집	Whatweb
	DNS 정보 수집	dnsrecon
		dnsmap
	네트워크 정보 수집	fierce
		traceroute
		hping
		scapy
		nmap
		네트워크 스캐닝 실습
Metasploit	Metasploit 개요	정의 및 구조
		구성요소
		주요 기능
	Metasploit GUI	개요
	Metasploit Console	주요 명령어

Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹

Curriculum, 커리큘럼

주제	내용	
Metasploit	Metasploit 사용방법	개요
		MSF 공격 방법
		Module name
		exploit과 payload의 식별 구조
		Payload type
		Exploit Command
		Exploit 흐름에 대한 이해
		Payload – meterpreter
		MSF 기본 사용법
	Autopwn	개요
		실행 방법
	Shellcode 추출	정의
		순서
		결과
	MS_08_067_Netapi	공격 실습
	Veil-Framework	정의
		Veil-Evasion 설치
		Veil-Framework 실행
		Veil-Evasion 사용
		Veil-Evasion을 이용한 악성 페이로드 제작
		Veil-Evasion을 이용한 악성파일 제작
		Veil-Framework 활용
윈도우 침투테스트	리버스 커넥션	netcat
	패스워드 크랙	Password의 구조
		윈도우 인증 구조
		크래킹 실습 – Cain & Abel
	MS17_010_Eternalblue	MS17_010_Eternalblue 공격 실습
		Bypassuac 실습

Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹

Curriculum, 커리큘럼

주제	내용	
리눅스 침투테스트	환경 구성	환경 구성
	nmap을 활용한 포트 스캐닝	피해자 서버 스캐닝
	Searchsploit을 활용한 취약점 검색	취약점 검색
	CVE-2007-0882 취약점 Exploit	CVE-2007-0882 취약점 공격
		CVE-2007-0882 취약점 원리
	SSH Bruteforcing Attack	SSH 버전 확인
		hydra를 활용한 SSH Bruteforcing Attack
	RPC(Remote Procedure Call)	RPC 서비스 확인
	로그인 사용자 조회	rusers 클라이언트 설치
	root 계정 패스워드 복호화	RPC 취약점 검색
		CVE-1999-0209 공격
	Privilege Escalation	CVE-2017-3623 취약점 원인
		CVE-2017-3623 취약점 공격
	SNMP Exploit	UDP 포트 스캔
		Community name 무차별 대입
		snmp-check를 통해 SNMP v1 연결

웹 구성 이해부터 시작하는 웹 해킹의 모든 것

웹 서비스의 구조와 다양한 취약점을 이해하며 공격 기법을 단계적으로 실습하는 과정입니다. SQL Injection, XSS 등 핵심 취약점을 테스트 환경에서 직접 다뤄보며 웹 보안의 기본을 탄탄히 익힙니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 웹 서비스를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법 학습 2. 공격 이후 대응할 수 있는 방안에 대해 현업에 적용할 수 있는 사례 기반의 내용을 이해
교육 특징	1. 실제 웹 모의해킹 시 많이 사용하는 주요 공격기법의 상세한 설명과 테스트 사이트 내에서 응용실습 진행 2. 대응방안 수립 시 일반적인 내용이 아닌 현업에서의 근본적인 대책과 차선책에 대한 내용
교육 대상	1. **정보보안 컨설턴트:** 다양한 실습으로 웹 해킹 공격에 대한 실질적인 대응방안을 수립할 수 있는 업무 능력 향상 2. **정보보안 담당자:** 웹 해킹에 대한 이해를 통해 기관 또는 사내 웹 서비스의 취약점에 대한 대응방안을 수립하여 보안 강화 3. **취업준비생, 대학생:** 모의해킹이나 취약점 분석 분야로 직무를 설정한 다음 그에 맞는 역량 강화를 준비하는데 도움

웹 구성 이해부터 시작하는 웹 해킹의 모든 것

Curriculum, 커리큘럼

주제	내용	
웹 구성의 이해	웹 서비스 구성	구성요소
	클라이언트 & 서버	웹 요청 처리 과정
	클라이언트 & 서버 측 언어 이해	웹 서비스 구성 -언어
	URL과URI	정의
		구조
	인코딩	개념
		URL 인코딩
		Base64 인코딩
	메타문자 이해	정의
	HTTP 프로토콜 이해	개요
		HTTP Request
		HTTP Response
		HTTP Response Status Code
	쿠키, 세션 이해	쿠키
		세션

웹 구성 이해부터 시작하는 웹 해킹의 모든 것

Curriculum, 커리큘럼

주제	내용	
웹 해킹의 이해와 실습	웬 해킹 개요	정의 및 종류
		웹 취약점 진단
		웹 서비스 구성
		웹 서비스 보안 대상
		웹 취약점 진단과 모의해킹
		모의해킹
	웹 해킹 점검 도구	Burp Suite 개요
	주요 웹 취약점 및 공격	SQL Injection
		SQL Injection 위험성
		SQL Injection 시큐어코딩
		SQL Injection 보안강화
		XSS
		Reflected XSS(반사형)
		Stored XSS(저장형)
		XSS 공격 실습
		Stored XSS(저장형)
		파일 업로드
		파일 다운로드
		불충분한 인증 및 인가
	개발 보안 정적 분석	보안 요구사항 분석 및 설계

안전한 스마트 환경을 위한 준비! IoT 보안 Starter Kit

IoT 기기의 구조와 특성을 이해하고 펌웨어 분석을 기반으로 보안 취약점을 살펴보는 과정입니다. 실제 디바이스 실습을 통해 IoT 환경에서 발생하는 다양한 공격 기법과 대응 전략을 익힙니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	고급
수강료	1,200,000원
교육 주제	1. IoT 서비스에 대한 전반적인 구성 및 최근 보안 위협과 공격 영역 이해 2. IoT 디바이스 펌웨어 분석 및 취약점 분석에 필요한 도구 사용 방안 습득 3. IoT 디바이스 펌웨어 취약점 분석 방안을 적용한 IoT 취약점 분석 역량 강화
교육 특징	1. 실무에서 사용하는 도구들을 기반으로 다양한 기기들의 펌웨어 분석 2. 최신 취약점을 기반으로 한 펌웨어 취약점 분석 학습 3. 실제 사례를 기반으로 한 시나리오 재구성을 통한 실습 프로그램 구성
교육 대상	1. **IoT 기기 개발자:** 안전한 IoT 서비스를 제공하기 위해 IoT 기기에 대한 공격이 어떻게 일어나는지 이해 2. **IoT 보안 실무자:** 실무에도 적용할 수 있는 IoT 기기 분석 도구 활용법과 취약점 분석 방안 학습 3. **취업준비생, 대학생:** 요즘 대세인 융합보안을 실무에 가까운 실습 위주 학습 및 역량 향상
Tip !	실습에 필요한 기기는 교육 중에만 제공됩니다.

안전한 스마트 환경을 위한 준비! IoT 보안 Starter Kit

Curriculum, 커리큘럼

주제	내용
사물인터넷 개요	사물인터넷의 이해
	임베디드 시스템
사물인터넷 보안 위협	사물인터넷 보안 사건/사고 사례
	사물인터넷 보안 동향
	사물인터넷 공격 표면 분석
사물인터넷 펌웨어 추출 및 분석	펌웨어 및 구조의 이해
	펌웨어 접근 및 획득
	펌웨어 분석 도구 및 활용
	펌웨어 취약점 분석 도구 및 활용
실전 펌웨어 취약점 분석	D-Link 공유기 펌웨어 분석
	오픈소스 SmartTV 펌웨어 분석
	iptime 공유기 펌웨어 분석
	IoTGoat 취약점 분석
	IoT CTFd 를 활용한 취약점 분석
취약점 악용 해킹 시나리오 실습	공유기 DNS 변조 공격 시나리오 실습
	공유기 DNS 변조 공격 시나리오 풀이

모의해킹

정규과정

- 모의해킹
- 실무에 바로 쓰는 웹 모의해킹 with 미션드리븐

KISEC

최신 트렌드를 반영한 모의침투 테스트

최근 공격 기법과 시나리오를 중심으로 다양한 침투 과정과 대응 전략을 실습하는 과정입니다. 웹·시스템·네트워크 등 여러 환경을 다루며 실무에서 요구되는 침투 테스트 능력을 강화합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 최근 발생했던 해킹사건을 바탕으로 모의침투 시나리오를 작성하는 방법 이해 2. 다양한 시나리오를 바탕으로 대상별 공격방법에 대해 역량 강화
교육 특징	1. 실제와 같은 환경에 실제 발생했던 해킹사건을 모의침투 시나리오로 접목할 수 있는 실습 프로그램 구성 2. IT 인프라에 전체적으로 발생할 수 있는 웹, 앱, PC 등 다양한 모의침투 시나리오 컨텐츠 실습
교육 대상	1. **정보보안 컨설턴트:** 최신 공격 기법과 취약점에 대해 학습하여 모의해킹 실무를 수행할 때 활용하는 방안 학습 2. **정보보안 담당자:** 기관 또는 사내에서 발생할 수 있는 보안 사고 및 위협들에 대한 폭넓은 이해로 관리체계 수립에 활용 3. **취업준비생, 대학생:** 웹 포함 다양한 모의침투 방법 이해를 통해 모의해킹 직무에 대한 경험 및 포트폴리오로 강점 어필
Tip !	네트워크 기초 지식과 윈도우/리눅스 명령어에 대한 선수 학습이 필요합니다.

최신 트렌드를 반영한 모의침투 테스트

Curriculum, 커리큘럼

주제	내용	
모의해킹 방법론	모의해킹 실무 기본이론	모의해킹 개요
		모의해킹과 범죄자 비교
		모의해킹 범위 – 시스템 접근 기준
		모의해킹 범위 – 수행 관점 기준
		모의해킹 종류
		모의해킹 업무 절차
원데이 취약점 기반 침투테스트	Apache Struts2 Exploit	동향
		취약점 개요
		환경 설정
		프로젝트 생성
		공격 방법
		취약점 점검 방법
		Python POC
	Oracle WebLogic Exploit	개요
		취약점 개요
		환경 설정
		취약점 점검 방법 – 수동
		공격 방법
	SSRF Exploit	SSRF 개요
		SSRF 환경구성
		SSRF 공격
	Log4j Exploit	Log4j 개요
		Log4j 취약점 사고 사례
		Log4j 취약점 원리
		Log4j 취약점으로 보는 시사점

최신 트렌드를 반영한 모의침투 테스트

Curriculum, 커리큘럼

주제	내용	
USB 시나리오 기반 침투테스트	BadUSB를 활용한 악성코드 유포 공격	개요
		BadUSB
		시나리오 흐름도
		상세 시나리오
		공격 환경 구성
		공격자 환경 구축
		피해자 환경 구축
웹 시나리오 기반 침투테스트	타깃형 워터링홀 공격 시나리오	개요
		토폴로지
		고급 유포 기술
		드라이브-바이 다운로드 공격
		침투
		실습 – Win7
		딘 에드워드 팩커
실전 모의 침투테스트	웹 사이트 모의해킹 실전	웹 사이트 모의해킹 실습

실무에 바로 쓰는 웹 모의해킹 with 미션드리븐

웹 해킹 기법을 실전 시나리오 중심으로 학습하며 침투 과정을 직접 수행하는 과정입니다. 미션 기반 실습을 통해 취약점 진단과 우회 기법을 익히며 실무 대응력을 높입니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 웹 사이트에서 자주 발견되는 취약점 진단 역량 강화 2. 공격자가 자주 사용하는 웹 해킹 응용 기법 역량 강화 3. 미흡한 방어기재를 우회할 수 있는 기법 습득 4. 안전한 웹 사이트 운영을 위한 시큐어코딩 및 보안설정의 이해
교육 특징	1. 현재 모의해킹 컨설팅 실무를 수행하고 있는 강사의 노하우 전수 2. [미션드리븐]이라는 자기주도적 학습 병행을 통한 교육 효과성 증대 3. 실제 사례를 기반으로 한 시나리오 재구성을 통한 실습프로그램 4. 내부 f-NGS Lab 연구진들의 최신 웹 해킹 실습컨텐츠로 구성
교육 대상	1. **정보보안 컨설턴트:** 모의해킹 업무 수행 시 최신 공격기법과 취약점을 활용하는 역량 향상 2. **정보보안 담당자:** 사내 웹 서비스에 모의해킹을 통한 보안 강화 3. **취업준비생, 대학생:** 모의해킹 직무로 취업하고 싶은 취준생을 위한 기초 학습
Tip !	리눅스와 SQL 구문에 대한 기본적인 지식이 필요합니다. 중급 과정이긴 하나 초급자들도 이해하기 쉽도록 교육합니다.

실무에 바로 쓰는 웹 모의해킹 with 미션드리븐

Curriculum, 커리큘럼

주제	내용	
웹 모의해킹 기본이론	웹 해킹 개요	웹 해킹의 정의 및 종류
	웹 보안 위협	OWASP TOP 10
		주요정보통신기반시설 웹 점검 항목
	웹 서비스 구성	웹 서비스 구성
	클라이언트 & 서버	클라이언트 & 서버
	클라이언트 & 서버 측 언어 이해	웹 서비스 구성 – 언어
	URL과 URI	URL과 URI 개념
		URL 구조
	인코딩	URL 인코딩
		Base64 인코딩
	메타문자 이해	메타 문자
	HTTP 프로토콜 이해	HTTP 개요
		HTTP Request
		HTTP Response
		HTTP Response Status Code
	쿠키, 세션 이해	쿠키
		세션
웹 개발 운영·환경 정보 수집	Passive Scan	SHODAN
		CENSYS
		GHDB
	Active Scan	whatweb
		dirbuster
		HTTrack

실무에 바로 쓰는 웹 모의해킹 with 미션드리븐

Curriculum, 커리큘럼

주제	내용	
웹 애플리케이션 해킹	SQL Injection	개요
		취약성 및 위험성
		보안대책
	XSS(Cross Site Scripting)	개요
		취약성 및 위험성
		점검 방법
		공격 사례
		보안대책
	파일 업로드	개요
		취약성 및 위험성
		취약점 발생 원인
		우회 기법
		파일 업로드
		공격 사례
		대응방안
	파일 다운로드	개요
		동작 방식
		공격 문자
		진단 방법
		공격 사례
		파일 다운로드
	서버사이브 요청 위조(SSRF)	SSRF 개요
		SSRF 환경구성
		SSRF 공격
	프로세스 검증 누락	웹 취약점 수동 진단 항목
	불충분한 인증	웹 취약점 수동 진단 항목
	불충분한 인가	웹 취약점 수동 진단 항목

실무에 바로 쓰는 웹 모의해킹 with 미션드리븐

Curriculum, 커리큘럼

주제	내용	
웹 서버 해킹	Apache Struts2 취약점 공격	동향
		취약점 개요
		환경 설정
		프로젝트 생성
		취약점 점검 방법
		공격 방법
		Python POC
	Oracle WebLogic 취약점 공격	개요
		취약점 개요
		환경 설정
		취약점 점검 방법 – 수동
		공격 방법
웹 해킹 응용	타겟형 워터링 홀 공격 시나리오	타겟형 워터링 홀 공격 시나리오
	시나리오 기반 TTPs 도출	시나리오 기반 TTPs 도출
	시나리오 내 도출된 TTPs	시나리오 내 도출된 TTPs
	시나리오 재구성을 통한 공격	Reconnaissance
		Initial Access
		Credential Access
		Persistence
		Execution
		Discovery
		Initial Access
미션드리븐	웹 사이트 모의해킹 실전	웹 사이트 모의해킹 실습
	모의해킹 TIP	모의해킹 TIP

보안 운영 관리

정규과정

- 보안 솔루션 운영
- 통합 보안 운영
- 관리체계와 법

KISEC

네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영

네트워크 기반 보안 솔루션의 동작 방식과 구성 방법을 익히며 장비 운영 역량을 쌓는 과정입니다. 방화벽·IDPS·WAF 등 핵심 솔루션을 실습해 실제 환경에서 필요한 정책 구성과 운영 능력을 강화합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 여러가지 보안 솔루션의 종류에 대해 학습하고, 각 장비들의 장단점 이해 2. 방화벽, IDPS, 웹방화벽 등 보안 솔루션 각 세대별 차이와 실제 현업에서 사용하는 기능들 이해 3. 방화벽, IDPS, 웹방화벽 등 보안 솔루션 각 장비별 룰 구성에 대해 이해하고 응용할 수 있는 역량 강화
교육 특징	1. 보안 관제에서 많이 사용하는 장비의 종류들을 직접 구축해보고 실습 2. 사례기반으로 발생했던 공격들에 대한 룰을 제작하는 방법 학습
교육 대상	1. 보안 솔루션의 종류 운용 방법에 대해 습득하고자 하시는 분 2. 방화벽 룰 작성법에 대한 이해가 필요하신 분
Tip !	네트워크 기본 지식과 리눅스 활용 능력 필요 많은 양의 가상머신을 사용해야 하므로 고사양의 노트북, 컴퓨터 필요

네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영

Curriculum, 커리큘럼

주제	내용	
보안 솔루션 종류와 이해	보안 솔루션 개요	네트워크 보안 장비와 솔루션
	보안 솔루션 시장	정보보안 시장 규모
		보안 솔루션 시장 동향
	솔루션 인프라 구성도 예시	인프라 기반 장비 구성
		LAN 구성
	보안장비 종류	방화벽
		WAF
		IDS
		IPS
		WIPS
		NAC
		안티 디도스
		정보유출 방지 솔루션
		엔드포인트 보안 솔루션
		기타 보안 장비 및 솔루션
		SOAR
		ESM vs SIEM vs SOAR
	정탐, 오탐, 미탐	정탐, 오탐, 미탐의 의미
	혼동행렬 (Confusion Matrix)	정확도
		정밀도
		재현도
		F1 Score
		F1 Score 계산 예제
		정탐, 오탐, 미탐과 혼동행렬

네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영

Curriculum, 커리큘럼

주제	내용	
방화벽 구축과 운영	방화벽 종류	방화벽 개요
		주요기능
		세대별 방화벽 분류
	방화벽 형태별 정의	스크리닝 라우터
		배스천 호스트
		듀얼 홈드 게이트웨이
		스크린드 호스트 게이트웨이
		스크린스 서브넷 게이트웨이
	방화벽 구성	망 구성 기준 예시
		네트워크 접근통제 단계 고려
		NAT
		HA
	방화벽 룰	룰 적용시 고려사항
	방화벽 구축	방화벽 구축
	방화벽 룰 구조	방화벽 룰 구조
	방화벽 정책 설정 실습	방화벽 정책 설정 실습
침입 탐지/차단 시스템 구축 및 룰 적용 실습	IPS 구축 개요	환경 구성 시나리오
		디바이스 환경 구성
	IPS(suricata) 구축	IPS 구축
	환경 구성	환경 구성
	Iptables 구조	Iptables 구조
	포워딩 설정	포워딩 설정
	룰의 이해	Suricata 룰의 구조
	Suricata 로그의 이해	Suricata 로그의 이해
	룰 적용 테스트	Alert 룰 테스트
		Drop 룰 테스트
	IPS 룰 설정 실습	IPS 룰 설정 실습

네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영

Curriculum, 커리큘럼

주제	내용	
정규 표현식과 SNORT 룰 실습	정규 표현식 개요와 종류	정규 표현식 개요
		정규 표현식 종류
	정규 표현식의 이해 및 실습	기본 문법
		문자클래스
	Snort의 개요	Snort의 개요
	PCAP 파일 분석	개요
		명령어 옵션
	룰의 이해	Snort 룰 구조
		룰의 구조
		Action
		Protocol
		IP Address & Port Number
		Rule Options
	Snort 와 Wireshark 연동	연동 설정
		Snort 분석
호스트 기반 솔루션	HIDS 개요	HIDS 정의
		탐지 영역
		오픈소스 종류
		기법
		실행 형태
	캐슬(CASTLE)을 이용한 웹 방화벽 구축	웹 방화벽(WAF) 개요
		캐슬(CASTLE) 개요
		방화벽 구축 실습
	ModSecurity를 이용한 웹 방화벽 구축	ModSecurity 개요
		방화벽 구축 실습

사이버 위협 대응을 위한 빅데이터 분석 환경 구축

보안 이벤트 분석을 위한 SIEM 구조를 이해하고 로그 수집·정제·시각화 과정을 실습하는 과정입니다. Elastic Stack을 활용해 다양한 보안 데이터를 분석하며 관제 업무에 필요한 실무 감각을 익힙니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	초급
수강료	1,000,000원
교육 주제	1. 보안 관제 직무를 명확히 파악하고 종합 운영 대책을 마련할 수 있도록 역량 강화 2. 보안 인프라 환경 내 솔루션의 역할을 구분하고 통합 운영이 가능하도록 능력 향상 3. 각 보안 인프라 환경에서 발생하는 이벤트를 수집하고, 분석할 수 있는 역량 향상
교육 특징	1. 개별 PC에서 가상의 인프라 환경을 구축하고 실제로 운영해보며, 실무와 유사한 환경에서 학습 2. 각 솔루션에서 발생하는 이벤트 등을 수집하고 종합 분석이 가능하도록 학습
교육 대상	1. **정보보호 관련 실무자:** SIEM을 이용하여 빅데이터 분석 환경을 구축하는 능력 향상에 도움 2. **취업준비생, 대학생:** 보안 관제 분야 역할과 업무에 대해 알아보고 해당 직무로 취업하고 싶은 분

사이버 위협 대응을 위한 빅데이터 분석 환경 구축

Curriculum, 커리큘럼

주제	내용	
보안 관제 개요	보안 관제 개념	관제의 의미
	보안 관제 영역과 필요성	공격 유형 별 모니터링 영역
		사례를 통해 알아보는 보안 관제의 필요성
	국내 보안 관제 현황	보안 관제 세대별 동향
	보안 관제 운영 업무 이해	탐지의 절차
		탐지 준비
		상세 탐지
		지속 탐지
통합보안운영 개요	통합보안운영의 필요성	통합보안운영 배경
		통합보안운영 목적
	통합보안운영의 분류	ESM의 이해
		SIEM의 이해
		ESM과 SIEM의 비교
	보안시스템 구축을 위한 실무가이드	보안시스템 구축 개요
		구축 프로세스
		정보보호사업 요구사항 분석, 적용 단계별 수행활동
		보안시스템 구축 절차 상세

사이버 위협 대응을 위한 빅데이터 분석 환경 구축

Curriculum, 커리큘럼

주제	내용	
Elastic Stack 기초	Elastic Stack 소개	Elastic Stack의 이해
	Elastic Stack 활용 사례	다양한 업종에서의 활용 사례
	Elastic Stack 기본 개념 익히기	Elasticsearch의 이해
		Elasticsearch의 구조
		Logstash의 이해
		Kibana의 이해
		Beats의 이해
		Elastic Stack 설치
		Elasticsearch 활용하기
		Logstash 활용하기
	Suricata와 ELK연동	Suricata filebeat 설치
		apache로그를 ELK로
	Prometheus와 Grafana	개요
		Prometheus 및 Grafana설치
Elastic Stack을 활용한 통합보안 운영	가상 통합 보안 인프라 설계 및 구축	가상 시나리오 배경
	설계된 인프라를 활용한 위협 탐지	환경구성
		Snort를 활용한 위협 탐지

관리체계와 법

정보보호 관리체계의 구성 요소와 법적 요구사항을 이해하며 조직 보안의 기반을 마련하는 과정입니다. 위험 분석, 통제 수립 등 실무 절차를 사례 중심으로 학습해 관리체계 운영 역량을 높입니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 정보보호 관리체계 프로세스를 이해하고, 관련 법에 기초한 정보보호 관리체계 수립으로 역량 강화 2. 각종 사례 속 정보보호 관리체계의 문제점 진단해 정보 자산의 위험을 분석해 효과적 관리 방안 도출할 수 있는 능력 향상
교육 특징	1. 정보보호 관리체계 기본 개념과 컨설턴트로서의 올바른 자질에 대해 이해 2. 실제 컨설팅 수행하고 있는 강사의 현업 사례를 통한 상세 가이드 제시 3. 컨설팅 단계별로 어떤 전략을 가지고 고객과 커뮤니케이션을 해야 하는지 상세 가이드 제시
교육 대상	1. **정보보안 컨설턴트:** 컨설팅 실무를 학습하면서 고객과의 원활한 커뮤니케이션을 할 수 있도록 컨설턴트로서 전략을 세울 수 있도록 역량 강화에 도움 2. **정보보호 관련 실무자:** 정보보호 관리체계를 이해하면서 실습을 통해 컨설팅의 프로세스를 자세히 배워 활용하는데 도움 3. **취업준비생, 대학생:** 실제 컨설팅 사례를 토대로 정보보호 관리체계를 배우고 정보보호 컨설턴트가 되기 위해 필요한 자질이 무엇인지 배우는데 도움

관리체계와 법

Curriculum, 커리큘럼

주제	내용	
관리체계의 이해	관리체계의 정의와 활용	표준의 관리체계 정의
		Management의 정의
		System의 정의
		관리체계, 경영시스템의 재정의
		시스템 경영 기본구조
		HLS(HIGH Level Structure)의 개요
		HLS(HIGH Level Structure)의 구조
		HLS(HIGH Level Structure) 프레임워크와 통합경영시스템 구축의 연계
정보보호 관리체계	정보보호 관리체계의 이해	정보보호 맥락에서의 Management 정의
		정보의 정의
		정보의 특성
		정보의 가치변화
		기업 자산의 정확한 가치 판단
		정보관리의 필요성
		위험의 이해
		위험에 영향을 줄 수 있는 변수
		정보보호의 개념
		정보보호 관리체계의 정의
		글로벌 정보보호 관리체계 (미국, 유럽, 일본, 중국, 영국)
		KISA-ISMS-P 인증제도
	정보보호 관리체계의 수립	정보보호 관리체계 수립 전략
		정보보호 관리체계 수립 절차
		사전단계
		정보보호 정책수립 및 범위설정
		경영진 책임 및 조직구성
		위험관리
		정보보호 대책구현
		사후관리

관리체계와 법

Curriculum, 커리큘럼

주제	내용	
개인정보보호 관리체계	개인정보보호 관리체계의 이해	정보보호 관리체계와 개인정보보호 관리체계
		개인정보 보호법 개요
		개인정보 보호법 개정내용
		개인정보의 처리
		개인정보의 안전한 관리
		정보주체 권리 보장과 피해구제
	개인정보보호 관리체계 수립	개인정보 흐름 파악
정보보호 컨설팅 실무	정보보호 컨설팅 개요	컨설팅의 개념
		고객과 컨설턴트
		컨설팅의 요소
	컨설팅 프로세스	정보보호 컨설팅의 종류
		컨설팅 프로세스 사례
		컨설팅 조직 구성
		프로세스의 이해
		컨설팅 프로세스 개요
		Define Security requirement
		Define Scope
		Gap Analysis
		Define Vulnerability, Threat
		Risk Assessment
		Risk Treatment
		Master Plan
보고서 작성 방안	보고서 작성 원칙	고려사항
	보고서의 목차 구성	일반적인 보고서의 구조
		고도화 작업
	효과적인 전달 방법	보고 자료의 구성
		분석결과의 효과적인 전달방법

진단

정규과정

- 시스템 취약점 진단
- 웹 취약점 진단
- 모바일 앱 취약점 진단
- 파이썬을 활용한 취약점 진단 자동화 개발

KISEC

정보시스템 취약점 진단 입문자를 위한 핵심 가이드

시스템 운영 환경에서 발생하는 기본 취약점을 이해하고 진단 방법을 익히는 과정입니다. 리눅스·윈도우 기반 수동 점검과 스크립트 활용을 통해 실무 진단의 흐름을 자연스럽게 파악합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 기본적으로 알아야 하는 서버 및 장비 운용 핵심 지식 습득 2. 진단 기준에 따른 주요 항목에 대한 수동 진단 방법을 통해 항목별 진단 목적 이해 3. 쉘/배치 스크립트 작성 방법을 학습하여, 효율적인 진단 방안 습득
교육 특징	1. 정보시스템 취약점 진단을 수행해야 하는 보안 직무 특화 2. 가이드에 없는 실무에서 실제 정보시스템 취약점 진단 시 고려해야 하는 요소 전수 3. 기획 수립 부터 결과 보고서 작성까지 정보시스템 취약점 진단의 모든 절차 경험
교육 대상	1. **정보보안 컨설턴트:** 정확한 정보시스템에 대한 이해로 컨설팅 중 취약점 진단 업무 수행 능력 향상 2. **정보보안 담당자:** 진단을 하는 방법은 알지만 가이드 내용만으로 조치가 어려운 상황에 도움이 될 수 있는 직무 능력 향상 3. **정보보안 취업 준비생:** 정보시스템을 안전하게 운영하거나 진단하는 컨설팅 직무 역량 향상에 도움

정보시스템 취약점 진단 입문자를 위한 핵심 가이드

Curriculum, 커리큘럼

주제	내용	
서버 또는 장비 관리를 위한 필수 기능 이해하기	리눅스 서버의 이해	리눅스 서버 쉘의 이해 및 기본 명령어 사용법
		리눅스 서버 편집기 사용 방법
		리눅스 서버 주요 시스템 파일
		리눅스 서버 네트워크 설정 방법
		리눅스 서버 PAM 모듈
	윈도우 서버의 이해	윈도우 서버 기본 명령어 사용법
		윈도우 서버 레지스트리의 이해
		윈도우 서버 로컬 보안 정책
		윈도우 서버 로그 관리
정보 시스템 취약점 진단 기준 수립	정보시스템 진단 기준 마련하기	정보 시스템 취약점 진단 가이드의 종류
		정보 시스템의 종류와 특징
		정보 시스템 취약점 진단 절차
주요정보통신 기반시설 기준 항목별 수동 진단 방안	리눅스 서버 주요 항목 수동 진단	리눅스 서버 주요 항목 수동 진단
	윈도우 서버 주요 항목 수동 진단	윈도우 서버 주요 항목 수동 진단
쉘/배치 스크립트 활용 취약점 진단	리눅스 서버 정보시스템 진단 수행하기	리눅스 쉘 스크립트
		리눅스 서버 진단 with 쉘 스크립트
	윈도우 서버 정보시스템 진단 수행하기	윈도우 배치 스크립트
		윈도우 서버 진단 with 배치 스크립트
취약점 진단 결과 보고서 작성하기	취약점 진단 보고서 작성 가이드	취약점 진단 보고서 작성 가이드
	결과 파일 기반 보고서 작성 실습	결과 파일 기반 보고서 작성 실습

안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정

웹 서비스에서 발생하는 주요 취약점을 실제 환경에서 진단하고 분석하는 과정입니다. OWASP 기반 점검 절차와 스캐너 활용법을 익히며 진단 보고서 작성까지 실무 역량을 고르게 갖춥니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 웹 취약점 진단 실무 및 점검 항목에 대해 이해 2. 웹 서버 점검 항목별 취약점 수동진단 수행 능력, 진단 이행 후 보고서 작성 업무를 수행
교육 특징	1. 실무 학습 기반으로 웹 서버 대상 취약점 점검을 수행 2. 취약점의 존재 유무에 따른 웹 서버의 반응을 직접 확인 3. 보고서 작성의 모범사례를 확인하고 작성 요령 학습
교육 대상	1. **정보보안 컨설턴트:** 업무를 수행할 때 웹 취약점 수동 진단, 보고서 작성 능력 등 현업에 활용 가능한 능력 향상 2. **정보보호 관련 실무자:** 점검 항목에 대한 이해부터 실습, 사례를 통한 전반적인 웹 취약점 진단 실무 역량 강화 3. **취업준비생, 대학생:** 웹에서 발생할 수 있는 위협에 대한 이해 및 사례 학습으로 취업에 도움

안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정

Curriculum, 커리큘럼

주제	내용	
웹 취약점 진단 개요	웹 취약점 수동 진단 실무 방법	웹 취약점 수동 진단 실무 방법
	점검 항목 (OWASP TOP 10)	점검 항목 (OWASP TOP 10)
	점검 항목 (기반시설)	점검 항목 (기반시설)
웹 스캐너 올바른 활용 예	OWASP ZAP	OWASP ZAP – 설치
		OWASP ZAP – 스캔
		OWASP ZAP – 보고서
		OWASP ZAP – 검증
		OWASP ZAP – 제거
	오픈 소스 웹 스캐너 사용 시 유의사항	오픈 소스 웹 스캐너 사용 시 유의사항

안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정

Curriculum, 커리큘럼

주제	내용	
웹 취약점 수동 진단 실무	웹 취약점 수동 진단 항목	버퍼 오버플로우
		포맷 스트링
		LDAP 인젝션
		운영체제 명령 실행
		SQL 인젝션
		SSI 인젝션
		XPath 인젝션
		디렉터리 인덱싱
		정보 누출
		악성 콘텐츠
		크로스사이트 스크립팅
		약한 문자열 강도
		불충분한 인증
		취약한 패스워드 복구
		크로스사이트 리퀘스트 변조(CSRF)
		세션 예측
		불충분한 인가
		불충분한 세션 만료
		세션 고정
		자동화 공격
		프로세스 검증 누락
		파일 업로드
		파일 다운로드
		관리자 페이지 노출
		경로 추적
		위치 공개
		데이터 평문 전송
		쿠키 변조

모바일 앱 취약점 진단(Android)

모바일 앱 구조와 보안 취약점을 이해하고 안드로이드 환경에서 진단 절차를 실습하는 과정입니다. 정적·동적 분석을 통해 취약점 확인과 우회 기법을 학습하며 모바일 보안 능력을 강화합니다.

Overview
교육 개요

교육 일수	3일 (일 8시간, 총 24시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 체크리스트 기반 모바일 앱 취약점 진단 수행 역량 강화 2. 모바일 앱 위, 변조 방지 솔루션 우회기법 습득 3. 발견된 모바일 앱 취약점에 대한 명확한 대응방안 학습
교육 특징	1. 모바일 앱에서 자주 발견되고 위험도가 높은 주요 취약점 진단 방법 학습 2. 다양한 모바일 앱 진단 도구 활용을 통해 효율적 진단 방안 제시 3. 모바일 앱 위, 변조 방지 솔루션 우회 기법을 통해, 진단 전문성 강화
교육 대상	1. **정보보안 컨설턴트:** 웹 서비스 뿐만 아니라 모바일 앱도 진단할 수 있는 역량 향상 2. **앱 서비스 운영,담당자:** 모바일 앱에 대한 자체적인 취약점 점검 3. **취업준비생, 대학생:** 정보보안 취업에 앞서, 웹 뿐만 아닌 앱에 대한 취약점 역량 향상
Tip !	본 과정을 수강하기 위해서는 프로그래밍 기초 지식이 필요

모바일 앱 취약점 진단(Android)

Curriculum, 커리큘럼

주제	내용	
안드로이드 구조 및 분석 도구	안드로이드 운영체제 구조	안드로이드 운영체제 논리적 구조
		안드로이드 주요 디렉토리 및 접근권한
	안드로이드 어플리케이션 구조	안드로이드 어플리케이션 빌드 프로세스
		안드로이드 어플리케이션 실행구조
		안드로이드 어플리케이션 APK
		안드로이드 어플리케이션 APK 구성 정보
		안드로이드 어플리케이션 APK 생성 과정
		안드로이드 어플리케이션 내부 저장소
	정적분석 도구	정적분석 방법
		자바 클래스 및 안드로이드 실행파일 리버싱
		안드로이드 APP 설치 및 실행과정
		APK해제 / dex disassemble 방법
		ADB를 이용하여 로컬PC의 apk 파일 푸시 방법
		ADB를 이용하여 apk 파일 설치방법
		ADB를 이용하여 파일 추출방법
		apk파일 추출 (시스템 APP)
		apktool 설명
		apktool를 이용한 디컴파일
		apktool를 이용한 빌드
		Jd-gui 활용
	동적분석 도구	동적분석 방법
		에뮬레이터 환경에서 Proxy 설정
		BusyBox
		자동 동적 분석 서비스
	앱 분석환경 구성	프리다(FRIDA)환경 구축

모바일 앱 취약점 진단(Android)

Curriculum, 커리큘럼

주제	내용	
안드로이드 앱 취약점 진단	유추가능한 인증정보 이용(비밀번호)	유추가능한 인증정보 이용(비밀번호)
	단말기 내 중요정보 저장 여부	단말기 내 중요정보 저장 점검
	메모리 내 중요정보 노출 여부	메모리 내 중요정보 노출 점검
	소스코드 난독화 적용 여부	소스코드 난독화 적용 점검
	프로그램 무결성 검증	프로그램 무결성 검증
안드로이드 앱 솔루션 우회	솔루션 우회를 위한 후킹기법	어플리케이션 루팅 탐지 우회
		어플리케이션 암호 복호화
		어플리케이션 로그인 우회

파이썬을 활용한 취약점 진단 자동화 개발

파이썬을 이용해 취약점 진단 절차를 자동화하는 스크립트를 개발하며 보안 업무 효율을 높이는 과정입니다. HTTP 요청 처리, 데이터 파싱, 자동화 로직 구성 등을 실습해 실무에서 바로 활용 가능한 기술을 익힙니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	고급
수강료	1,500,000원
교육 주제	1. 각 운영체제 별 취약점 진단을 위한 스크립트 작성 능력 강화 2. 효율적인 취약점 진단을 위한 파이썬 활용 자동화 모듈 개발 능력 배양 3. 가이드에 따른 항목 별 취약점 진단 해석 능력 강화
교육 특징	1. 실무 기반의 취약점 진단 방법 및 모범사례 공유 2. 반복작업이 많은 취약점 진단 업무 상의 문제점을 파이썬 활용으로 해결할 수 있는 방안 학습
교육 대상	1. **정보보안 컨설턴트:** 정보시스템 취약점 진단 업무를 수행할 때 복사, 붙여넣기 하는 단순 작업을 파이썬을 활용한 자동화 모듈 구현으로 업무의 효율성을 높일 수 있도록 학습 2. **앱 서비스 운영,담당자:** 정기적으로 취약점 진단이 필요한 항목이나 자산에 대해 자동화 모듈을 적용할 수 있는 방안 학습 3. **취업준비생, 대학생:** 파이썬을 활용할 수 있다는 점이 취약점 진단 직무를 수행할 수 있는 차별화된 강점이 될 수 있도록 학습
Tip !	본 과정은 파이썬의 기본 문법에 대해서는 알려드리지 않으니, 참고하시기 바랍니다.

파이썬을 활용한 취약점 진단 자동화 개발

Curriculum, 커리큘럼

주제	내용	
정보 시스템 진단 기준	정보시스템 취약점 진단	개요
	정보시스템 취약점 진단 기준 수립	주요 취약점 진단 기준 가이드라인 소개
		정보시스템 진단 자동화의 필요성
취약점 진단 스크립트	쉘 스크립트(리눅스)	쉘 스크립트 개요
		주요 사용 문법 및 명령어
		쉘 스크립트 파일 작성 방법
	배치 스크립트(윈도우)	배치 스크립트 개요
		주요 사용 문법 및 명령어
		배치 스크립트 파일 작성 방법
시스템 정보 수집 자동화 모듈 개발	파이썬의 이해 및 문법	파이썬 개요
		파이썬 문법 특징
	스크립트 자동 생성 모듈 구현	수집 관련 설정 파일 구현 및 파싱
		수집 모듈 플러그인
		수집 스크립트 병합 및 생성
	진단항목 별 플러그인 수집 모듈 작성	리눅스 시스템 진단항목 별 수집 모듈 구현
		윈도우 시스템 진단항목 별 수집 모듈 구현

파이썬을 활용한 취약점 진단 자동화 개발

Curriculum, 커리큘럼

주제	내용	
수집 데이터 분석 자동화 모듈 개발	수집 결과 분석 모듈 구현	수집 데이터 파싱
		분석 모듈 플러그인 구현
	진단항목 별 플러그인 분석 모듈 작성	리눅스 시스템 진단항목 별 분석 모듈 구현
		윈도우 시스템 진단항목 별 분석 모듈 구현
보고서 작성 자동화 모듈 개발	파이썬 엑셀 제어 라이브러리	엑셀 제어 라이브러리 개요
		엑셀 제어 라이브러리 함수 활용
	진단 결과 보고서	분석 데이터 파싱
		엑셀 템플릿을 이용한 결과 보고서 모듈 구현

포렌식, 침해사고

정규과정

- 침해사고 분석/대응
- 악성코드 분석 기초
- 악성코드 분석 심화
- Digital Forensics and Incident Response (DFIR)

KISEC

공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응

침해사고 발생 원인을 분석하고 대응 절차를 이해하는 실무 중심 과정입니다. 로그·프로세스·타임라인 분석 등 실제 상황 기반 실습을 통해 사고 대응 흐름과 재발 방지 전략을 익힐 수 있습니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,500,000원
교육 주제	1. 공격자의 행위로 발생할 수 있는 다양한 이벤트 이해 2. 침해사고 발생 시 필요한 도구를 준비하고 활용 3. 침해사고 분석 시 타임라인을 도출하여 원인을 파악하고 재발 방지
교육 특징	1. 앞으로 발생할 수 있는 다양한 사고를 분석할 수 있도록 관점과 역량 강화 2. 사이버 범죄를 재구성한 가상환경을 실전과 같이 분석하고 보고서를 작성하여 실무 역량 강화 3. 사고대응 분야에서 대두되고 있는 ATT&CK 프레임워크를 사고 분석에 접목해 공격자의 TTP 도출
교육 대상	1. **침해사고 담당자:** 발생했거나 앞으로 발생할 수 있는 침해사고에 대해 기술적으로 분석하고 신고부터 대응까지 절차를 마련하는데 도움 2. **직무순환 대상자:** 직무순환 등의 이유로 침해사고 분석의 기초부터 습득하고 싶을 경우 실습을 통해 능력 향상 3. **취업준비생, 대학생:** 가상의 환경에서 직접 침해사고를 분석해보면서 침해사고 분석, 대응에 기초부터 습득하는데 도움

공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응

Curriculum, 커리큘럼

주제	내용	
침해사고 대응 준비	Warm-Up	선수 지식 요약
		정의
	침해사고의 주요 원인	침해사고 특징
		침해사고 유형
		침해사고 사례 파악
		사이버 보안 위협 – 악성코드
		사이버 보안 위협 – 공격 유형
		사이버 보안 위협 동향
	사고대응체계 수립	침해사고 대응 절차 7단계 (KISA)
	사고대응 준비를 위한 고려사항	사고대응 준비를 위한 고려사항
	초기대응 단계를 위한 고려사항	초기대응 단계를 위한 고려사항
	사고분석 단계를 위한 고려사항	사고 분석 단계를 위한 고려사항
	복구 및 해결단계를 위한 고려사항	복구 및 해결단계를 위한 고려사항
침해사고의 흔적들	윈도우 주요 아티팩트	아티팩트의 이해
		프로세스의 이해
		드라이버의 이해
		파일시스템과 디스크의 이해
		윈도우 계정의 이해
		프리패치의 이해
		레지스트리의 이해
		Windows 이벤트 로그의 이해
		포트의 이해
		DNS의 이해
		ARP의 이해
		브라우저 히스토리의 이해
		윈도우 서비스의 이해
		작업 스케줄러의 이해

공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응

Curriculum, 커리큘럼

주제	내용	
침해사고 흔적 수집	흔적 수집 대상	흔적 수집 대상 예시
		정보 수집 절차
	명령을 활용한 정보 수집	커맨드 라인 명령 활용
		시간
		운영체제 버전
		프로세스
		네트워크
		서비스
		작업 스케줄
		사용자 정보
	프리웨어를 활용한 흔적 수집/분석	윈도우 보안 분석 도구
	배치스크립트 활용 실습	윈도우 배치 스크립트
		스크립트 제작
	활성 시스템 조사 실습	활성 시스템 조사 실습
침해사고의 분석 실습	Case 1: Ransomware	Case 별 침해사고 분석 실습
	Case 1-1: DBD (PC)	
	Case 1-2: DBD (Server)	
	Case 2: Deface	
	물리 메모리 정보 분석	
	디스크 이미징 개요	
	디스크 이미지 분석	
	Case 3: WanaCry	

빠른 침해사고 대응을 위한 악성 코드 초동 분석

악성코드의 유형과 동작 원리를 이해하고 기본적인 정적·동적 분석 기법을 익히는 과정입니다. 주요 도구 활용과 실제 사례 분석을 통해 악성코드가 시스템에 미치는 영향을 파악합니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. 악성코드의 유형과 유입 경로 파악을 통해 침해사고가 발생할 수 있는 공격 벡터 이해 2. 악성코드 동적/정적 분석을 통해 작성하는 결과 보고서를 이해하기 위한 기본 지식 학습 3. 자동화 분석 시스템을 기반으로 다양한 케이스의 악성코드 분석하고 공격자들의 전략 이해
교육 특징	1. 트로이목마, 바이러스, 웜 악성코드 유형을 이해하고 크립토락커, 크립토 마이닝, RAT 등 다양한 유형을 분류하는 방법 이해 2. 악성코드를 여러 관점에서 정적/동적분석을 해보고 위협지표를 찾는 방법 학습 3. 자동화 분석 시스템 구축 및 운영을 통해 다양한 악성코드 분석 보고서를 보며 공격 방식 학습
교육 대상	1. **악성코드 분석 실무자:** 다양한 악성코드의 유형 별로 효과적인 분석 방법 이해하면서 실무 역량 강화에 도움 2. **정보보안 담당자:** 갈수록 진화하는 악성코드의 유형 파악 및 분석을 학습해 유형에 따른 대응방안을 수립하는데 도움 3. **취업준비생, 대학생:** 정보보안 취업에 앞서, 다양한 유형의 악성코드 분석 기술 향상

빠른 침해사고 대응을 위한 악성 코드 초동 분석

Curriculum, 커리큘럼

주제	내용	
악성코드 의미와 동향	악성코드 개요	악성코드 정의
		악성코드 종류
		악성코드 네이밍 스키마
		악성코드 패밀리 종류
	악성코드 및 해킹 최신 동향	POS 악성코드
		산업기반 시설 악성코드
		특수망 해킹
		정치적 해킹
		상업 해킹
		기업 해킹
		불특정 다수 해킹
		가상화폐거래소 해킹
악성코드 유형별 이해	악성코드 대유형	바이러스 개요
		웜 개요
		트로이목마 개요
		PUP 개요
	악성코드 소유형	협박
		도청 & 감시
		접근 & 강탈
		다운로드
		기타

빠른 침해사고 대응을 위한 악성 코드 초동 분석

Curriculum, 커리큘럼

주제	내용	
악성코드 유형별 이해	RAT 악성코드 이해 및 실습	RAT 악성코드 정의
		RAT 악성코드 흐름
		RAT 악성코드 역사
		Orcus 동향
		Orcus 실습
	랜섬웨어 악성코드 이해 및 실습	랜섬웨어 정의
		랜섬웨어 역사
		랜섬웨어의 특징
		랜섬웨어 감염 경로
		랜섬웨어 악성코드 실습
악성코드 유입 경로	악성코드 유입 경로 이해	감염경로
	USB를 이용한 공격 이해 및 시연	User Really Do Plug in USB Drives They Find
		Infection via USB (with Supply Chain Attack)
		BadUSB
	드라이브-바이 다운로드 공격 이해 및 실습	개요
		토폴로지
		고급 유포 기술
		드라이브-바이 다운로드
		(Drive-By Download) 공격
		실습
악성코드 분석 개론	이메일을 이용한 악성코드 유포 이해 및 실습	감염 경로
		이메일을 통한 악성코드 감염
	악성코드 분석 개요	악성코드 분석 정의와 분석 이유
		악성코드 분석 시 고려사항
		악성코드 분석 흐름
	악성코드 분석 방법론	기술적 관점
		대응적 관점
		악성코드 분석 방법론 동향

빠른 침해사고 대응을 위한 악성 코드 초동 분석

Curriculum, 커리큘럼

주제	내용	
악성코드 분석 개론	악성코드 분석 환경 개요	샌드박스 개요와 유형
		샌드박스 이용 목적
		샌드박스 사용 사례
		하이퍼바이저 이해
		윈도우 운영체제 선택 시 고려사항
	하이퍼바이저 환경 구성	가상화 기술 지원 확인
		VM웨어 워크스테이션 설치
		VM웨어 워크스테이션 설정
		가상머신 생성
	취약한 윈도우 환경 구성	설정
악성코드 분석 실무	악성코드 정적 분석 이해 및 실습	정적 분석 개요
		악성코드 정적 분석 도구 소개
		악성코드 정적 분석 실습
	악성코드 동적 분석 이해 및 실습	악성코드 동적 분석 개요
		악성코드 동적 분석 도구 소개
		악성코드 동적 분석 실습
	악성코드 자동화 분석 이해 및 실습	악성코드 자동화 분석 개요
		악성코드 자동화 분석 도구 소개
		쿡쿠 샌드박스 개요
		쿡쿠 샌드박스 구축
		쿡쿠 웹서비스
		쿡쿠 샌드박스 운영
		쿡쿠 API를 이용한 쿡쿠 샌드박스 설정
		쿡쿠 샌드박스와 다양한 분석 툴 연동
악성코드 대응 및 방어 실무	YARA 패턴 제작 및 활용	YARA 개요
		YARA 적용
	악성코드 대응방안	대응방안 요약
		정책
		인식
		취약성 완화
		위협 완화
		방어 아키텍처
		침해사고대응 프로세스

문서형 악성코드부터 실제 유포되는 악성코드까지! APT 공격에 활용되는 악성코드 분석 심화

고도화된 공격에 사용되는 악성코드를 중심으로 분석 기법을 익히는 심화 과정입니다. 다양한 파일 형태와 스크립트를 다루며 위협 행위자의 전략과 전술을 파악하는 능력을 높입니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,200,000원
교육 주제	1. EXE, 문서, 스크립트 등 다양한 형태의 악성코드 이해 및 분석 역량 강화 2. 최신 악성코드 행위 분석을 통해 공격자들의 공격기법 및 방어 회피 전략 파악
교육 특징	1. 실제 APT 공격에 활용되었던 악성코드를 분석함으로써 공격자들의 행위 파악 2. EXE, 문서, VBScript 등 다양한 형태의 악성코드 분석 방법 학습
교육 대상	1. **악성코드 분석 실무자:** 다양한 악성코드를 유형 별로 효과적인 분석 방법 학습 2. **침해사고 대응 실무자:** 침해사고가 발생하는 주 원인인 악성코드를 분석해서 침해사고 대응에 활용 3. **정보보안 담당자:** 날이 갈수록 진화하는 악성코드의 유형을 파악하고 각 유형에 따른 대응 방안 학습 4. **취업준비생, 대학생:** 다양한 유형의 악성코드 분석 기술을 사용할 수 있다는 강점으로 관련 직무 취업 준비
Tip !	샘플 악성코드는 실제 유포되었던 악성코드로 실습 시 반드시 안내에 따라 진행 필수 본 교육은 스크립트 등 코드 분석 등이 포함되어 있어 기본적인 프로그래밍 지식이 필요

문서형 악성코드부터 실제 유포되는 악성코드까지! APT 공격에 활용되는 악성코드 분석 심화

Curriculum, 커리큘럼

주제	내용	
악성코드 분석 개론	악성코드 분석 개요	악성코드 분석 정의와 분석 이유
		악성코드 분석 시 고려사항
		악성코드 분석 흐름
	악성코드 분석 방법	악성코드 분석 방법론
		레지스트리 구조 이해
		웹 아티팩트의 이해
		윈도우 정상 프로세스의 이해
플랫폼 별 악성코드 분석	PE 악성코드 분석	윈도우의 이해
		윈도우 프로그래밍
		Windows 프로그래밍 기본 구조
		이벤트와 메시지
		프로세스와 스레드
		라이브러리
		라이브러리 링크
		DLL 특징
		DLL 함수 호출 과정
	문서형 악성코드 분석	문서형 악성코드 공격 현황
		문서형 악성코드 분석 환경 구성
		문서 악성코드 분석 지표
		문서 악성코드 분석 기법
		JavaScript 분석
		PDF 분석
		VBA 스크립트 분석
		악성 문서 빠른 분석 기법
		Office 문서 분석
		HWP 악성코드 분석

문서형 악성코드부터 실제 유포되는 악성코드까지! APT 공격에 활용되는 악성코드 분석 심화

Curriculum, 커리큘럼

주제	내용	
가이드를 중점에 둔 악성코드 대응 방안	피싱 예방 및 대응 방안 가이드	피싱 메일 공격 예방 및 대응 방법
		피싱 경유지사고 처리
		피싱 경유지 피해 시스템 분석
		보안 강화 방안
		개인 사용자 관리
	멀버타이징 예방 및 대응 방안 가이드	온라인 광고 신규 계약 점검
		광고 서버의 기술적 점검
		광고 서버의 관리적 점검
		이용자 측면에서의 멀버타이징 예방법
	공급망 공격 예방 및 대응 방안 가이드	인증서 및 개발 시스템 (SVN, 빌드 서버 등) 관리
		업데이트 체계 관리
	랜섬웨어 예방 및 대응 방안 가이드	랜섬웨어 정의
		랜섬웨어 특징
		기업 해킹
		랜섬웨어 예방법
		랜섬웨어 감염 시 대응절차
IoC 의미와 활용 방안	IoC 개요	IoC 정의
		IoC 관련 도구
	IoC 활용 방안	멀웨어 조사
		공격 지표(Indicator of Attack)
		MISP를 이용한 위협 정보 공유 시스템 운영

Digital Forensics and Incident Response (DFIR)

디지털 포렌식 절차와 분석 기법을 이해하고 다양한 증거 확보 과정을 실습하는 과정입니다. 파일 분류, 로그 분석 등 핵심 기술을 익히며 침해사고 대응에 필요한 종합 역량을 기릅니다.

Overview
교육 개요

교육 일수	5일 (일 8시간, 총 40시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	고급
수강료	1,500,000원
교육 주제	1. 디지털 포렌식에 대한 개요, 유형, 절차 등 기본 지식 이해 2. 실습을 통해 디지털 포렌식 분석 도구 활용 방법 습득 3. 디지털 포렌식 업무의 완벽한 이해로 역량 강화
교육 특징	1. 디지털포렌식 기초 도구 사용법에 대해 실습 진행 2. 초보자도 할 수 있는 파일 복구 실습 진행 3. 단계별로 실습을 진행하면서 침해사고 분석 기법에 대해 학습
교육 대상	1. **포렌식/침해사고 담당자:** 침해사고와 더불어 디지털 포렌식에 대한 통합과정이 필요한 담당자 2. **정보보호 실무자:** 포렌식 분석을 입문부터 활용까지 상세하게 학습하면서 침해사고 대응 분석 능력 향상에 도움 3. **취업준비생, 대학생:** 포렌식, 침해사고 대응 분석의 업무 수행하고자 취업을 준비하는데 도움

Digital Forensics and Incident Response (DFIR)

Curriculum, 커리큘럼

주제	내용
디지털 포렌식 이해	디지털 포렌식 개념
	디지털 포렌식과 침해사고 대응
	디지털 포렌식 절차
디지털 포렌식 기초	로카르드 교환 법칙
	증거능력
	디지털 증거와 주요 사례
	증거물 수집
파일 시스템 구조	일반적인 하드 디스크 구조
	파일시스템
	파티션과 슬랙 공간
	FAT/NTFS의 이해
	메타 데이터와 파일 카빙
디지털 증거 분석 개요	디지털 포렌식 절차
	Chain of Custody
	시간 정보와 데이터 표현방식

Digital Forensics and Incident Response (DFIR)

Curriculum, 커리큘럼

주제	내용
윈도우 증거분석(1) 휘발성 데이터	Live Forensic
	휘발성 데이터 수집과 분석
	메모리 구조와 분석
	휘발성 데이터 분석 도구
윈도우 증거분석(2) 비휘발성 데이터	비휘발성 아티팩트
	레지스트리 구조와 증거 분석
	주요 폴더 / 파일 증거 분석
	웹 브라우징 / 이벤트 로그 증거
	실습 도구 사용 방법 이해
네트워크 포렌식	네트워크 패킷의 이해
	네트워크 기반의 증거
	도구를 이용한 수집과 분석
DFIR CTF	DFIR CTF (LAB)
포렌식 동향	디지털 포렌식 트렌드
	다양한 관점에서 디지털포렌식 역할

개발 및 분석

정규과정

- 공격해보고!방어해보고! 시큐어코딩 마스터

KISEC

공격해보고! 방어해보고! 시큐어코딩 마스터

웹 취약점의 동작 원리를 실제로 공격해보고, 이를 방어하는 코드를 구현하며 시큐어코딩의 핵심을 익히는 과정입니다. 입력 검증, 인증·인가 등 주요 항목을 실습 중심으로 다뤄 안전한 개발 역량을 강화합니다.

Overview
교육 개요

교육 일수	3일 (일 8시간, 총 24시간)
교육 시간	9:00 ~ 18:00 (점심시간 12:00 ~ 13:00)
교육 수준	중급
수강료	1,500,000원
교육 주제	1. 소프트웨어 개발 방법론, 실무관점 적용방안의 이해 2. 공격자가 자주 사용하는 웹 해킹 기법의 원리를 바탕으로 한 시큐어코딩 역량 강화 3. 시큐어코딩 모범사례를 비즈니스 로직에 적용할 수 있는 방안 학습
교육 특징	1. 단순히 시큐어코딩 방법 적용이 아닌 공격의 원인을 파악하고, 그에 맞는 적절한 시큐어코딩 방안 제시 2. 실제 공격을 수행해보고, 시큐어코딩을 적용한 후 이행점검으로 시큐어코딩 적용의 유효성 검증 3. 소스코드 보안약점을 효율적으로 진단할 수 있는 다양한 진단도구 활용
교육 대상	1. **SW 개발자:** 보안약점의 명확한 기준과 보안대책을 통해 실질적인 시큐어코딩 적용 방법 학습 2. **정보보안 담당자:** 보안약점을 최소화하기 위한 가장 효율적인 방법 이해 3. **개발자 지망생:** 개발과 보안을 모두 할 수 있는 개발자로 취업 위한 발돋움 4. **보안약점 진단 지망생:** 보안약점을 진단하고 대책을 제시하는 방법 이해
Tip !	본 과정을 수강하기 위해서는 프로그래밍 기초 지식이 필요

공격해보고! 방어해보고! 시큐어코딩 마스터

Curriculum, 커리큘럼

주제	내용	
소프트웨어 개발보안 이해	소프트웨어 개발보안의 필요성	웹 응용프로그램 보안사고 사례 원인분석
	소프트웨어 개발보안 방법론	소프트웨어 개발보안 제도
		취약성과 취약점의 차이
		소프트웨어 보안약점 항목(해외)
		소프트웨어 보안약점 항목(국내)
		개발단계별 주요 보안활동
소프트웨어 보안분석 도구	효과적인 보안약점 진단방안	정적진단과 동적진단 병행 프로세스
	정적분석도구	소스코드 진단도구 소개 및 활용방안
	동적분석도구	응용프로그램 진단도구 소개 및 활용방안
입력값 유효성 검증 주요항목	SQL 인젝션	SQL 인젝션 실습을 통한 공격분석
		SQL 인젝션 대응을 위한 시큐어코딩 적용 및 이행점검
	XSS(Cross Site Scripting)	XSS 실습을 통한 공격분석
		악성코드 유포 위험성 실습
		XSS 대응을 위한 시큐어코딩 적용 및 이행점검
	위험한 형식 파일 업로드	파일 업로드 실습을 통한 공격분석
		원격명령 실행을 통한 웹서버 장악 위험성 확인
		파일 업로드 대응을 위한 시큐어코딩 적용 및 이행점검
	파일 다운로드	파일 다운로드 실습을 통한 공격분석
		중요 소스코드 다운로드를 통한 정보탈취
		파일 다운로드 시큐어코딩 적용 및 이행점검
소프트웨어 개발보안 가이드 라인	웹 응용프로그램 개발코딩 가이드 라인	입력 값 검증
		파일처리
		데이터베이스 처리
		인증과 권한
		에러처리
		암호화

공격해보고! 방어해보고! 시큐어코딩 마스터

Curriculum, 커리큘럼

주제	내용	
소프트웨어 개발보안 이해	소프트웨어 개발보안의 필요성	웹 응용프로그램 보안사고 사례 원인분석
	소프트웨어 개발보안 방법론	소프트웨어 개발보안 제도
		취약성과 취약점의 차이
		소프트웨어 보안약점 항목(해외)
		소프트웨어 보안약점 항목(국내)
		개발단계별 주요 보안활동
소프트웨어 보안분석 도구	효과적인 보안약점 진단방안	정적진단과 동적진단 병행 프로세스
	정적분석도구	소스코드 진단도구 소개 및 활용방안
	동적분석도구	응용프로그램 진단도구 소개 및 활용방안

공격해보고! 방어해보고! 시큐어코딩 마스터

Curriculum, 커리큘럼

주제	내용	
입력값 유효성 검증 주요항목	SQL 인젝션	SQL 인젝션 실습을 통한 공격분석
		SQL 인젝션 대응을 위한 시큐어코딩 적용 및 이행점검
	XSS(Cross Site Scripting)	XSS 실습을 통한 공격분석
		악성코드 유포 위험성 실습
		XSS 대응을 위한 시큐어코딩 적용 및 이행점검
	위험한 형식 파일 업로드	파일 업로드 실습을 통한 공격분석
		원격명령 실행을 통한 웹서버 장악 위험성 확인
		파일 업로드 대응을 위한 시큐어코딩 적용 및 이행점검
	파일 다운로드	파일 다운로드 실습을 통한 공격분석
		중요 소스코드 다운로드를 통한 정보탈취
		파일 다운로드 시큐어코딩 적용 및 이행점검
소프트웨어 개발보안 가이드 라인	웹 응용프로그램 개발코딩 가이드 라인	입력 값 검증
		파일처리
		데이터베이스 처리
		인증과 권한
		에러처리
		암호화

정규과정 일정표

월별 일정

※ 원하시는 달을 클릭하시면 이동합니다.

- 1월
- 2월
- 3월
- 4월
- 5월
- 6월
- 7월
- 8월
- 9월
- 10월
- 11월
- 12월

KISEC

08. 정규과정 일정표

1월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
05	06	07	08	09
네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z				
12	13	14	15	16
IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음				
19	20	21	22	23
		공격해보고! 방어해보고! 시큐어코딩 마스터		
26	27	28	29	30
빠른 침해사고 대응을 위한 악성코드 초동 분석				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

2월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
02	03	04	05	06
공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응				
09	10	11		13
안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정				
16 설날 연휴	17 설날	18 설날 연휴	19	20
23	24	25	26	27+

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

3월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
02 대체 휴일	03	04	05	06
09	10	11	12	13
			이산 수학부터 시작하는 암호학의 모든 것	
16	17	18	19	20
다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential				
23	24	25	26	27
다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential				
30	31	4/1	4/2	4/3
논리적 사고방식으로 이해하는 프로그래밍 기초				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

4월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
06	07	08	09	10
어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론				
13	14	15	16	17
다양한 실습으로 쉽게 이해하는 네트워크 Essential				
20	21	22	23	24
네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z				
27	28	29	30	5/1 근로자의 날
소프트웨어 취약점의 동작 원리부터 익스플로잇까지! 어플리케이션 해킹				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

5월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
04	05 어린이날(강의X)	06	07	08
Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹				
11	12	13	14	15
웹 구성 이해부터 시작하는 웹 해킹의 모든 것				
18	19	20	21	22
25 대체 휴일	26	27	28	29

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

6월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
01	02	03 지방선거일(강의O)	04	05
네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z				
네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영				
08	09	10	11	12
어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론				
사이버 위협 대응을 위한 빅데이터 분석 환경 구축				
15	16	17	18	19
최신 트렌드를 반영한 모의침투 테스트				
공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응				
22	23	24	25	26
IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음				
관리체계와 법				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

7월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
6/29	6/30	01	02	03
실무에 바로 쓰는 웹 모의해킹 with 미션드리븐				
빠른 침해사고 대응을 위한 악성코드 초동 분석				
06	07	08	09	10
공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응				
정보시스템 취약점 진단 입문자를 위한 핵심 가이드				
13	14	15	16	17
안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정				
20	21	22	23	24
		공격해보고! 방어해보고! 시큐어코딩 마스터		
27	28	29	30	31
빠른 침해사고 대응을 위한 악성코드 초동 분석				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

8월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
03	04	05	06	07
최신 트렌드를 반영한 모의침투 테스트				
10	11	12	13	14
문서형 악성코드부터 실제 유포되는 악성코드까지! APT 공격에 활용되는 악성코드 분석 심화				
17 광복절 대체 휴일	18	19	20	21
		모바일 앱 취약점 진단(Android)		
24	25	26	27	28
Digital Forensics and Incident Response (DFIR)				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

9월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
8/31	01	02	03	04
안전한 스마트 환경을 위한 준비! IoT 보안 Starter Kit				
07	08	09	10	11
네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z				
14	15	16	17	18
웹 구성 이해부터 시작하는 웹 해킹의 모든 것				
21	22	23	24 추석 연휴	25 추석
28	29	30	10/1	10/2

보안의 시작 : 정보보안 기초와 실무 과정

2026.08.24 ~ 2026.09.18

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

08. 정규과정 일정표

10월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
05 대체 휴일	06	07	08	09 한글날
12	13	14	15	16
공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응				
19	20	21	22	23
정보시스템 취약점 진단 입문자를 위한 핵심 가이드				
26	27	28	29	30
빠른 침해사고 대응을 위한 악성코드 초동 분석				
최신 트렌드를 반영한 모의침투 테스트				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

11월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
02	03	04	05	06
		공격해보고! 방어해보고! 시큐어코딩 마스터		
IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음				
09	10	11	12	13
실무에 바로 쓰는 웹 모의해킹 with 미션드리븐				
안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정				
16	17	18	19	20
공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응				
문서형 악성코드부터 실제 유포되는 악성코드까지! APT 공격에 활용되는 악성코드 분석 심화				
23	24	25	26	27
IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음				
정보시스템 취약점 진단 입문자를 위한 핵심 가이드				
30	12/1	12/2	12/3	12/4
빠른 침해사고 대응을 위한 악성코드 초동 분석				

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)

12월

※ 상세 과정명을 클릭하시면 과정 안내 페이지로 이동합니다.

월	화	수	목	금
07	08	09	10	11
안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정				
14	15	16	17	18
파이썬을 활용한 취약점 진단 자동화 개발				
21	22	23	24	25 성탄절
28	29	30	31	1/1 신정

Notice

- 상단의 일정은 경우에 따라 변동될 수 있습니다.
  - 원하시는 일정이 별도로 있으시거나 모듈 구성 커스텀이 필요하시면 센터로 문의 바랍니다.
- 유선으로 개강확정 안내 후, 메일로 입과 안내 예정입니다.
- 홈페이지를 통한 신청이 어려우시면 유선을 통해 신청 도와 드리겠습니다.
  (☏ 문의처 : 02-921-1465)