

(주)한국정보보호교육센터

2024년 정규과정 안내



보안직무 공통	이산 수학부터 시작하는 암호학의 모든 것		
	4일 (32H)	입문	900,000원
	다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential		
	4일 (32H)	입문	900,000원
	다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential		
	4일 (32H)	입문	900,000원
	논리적 사고방식으로 이해하는 프로그래밍 기초		
	5일 (40H)	입문	900,000원
	어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론		
	5일 (40H)	입문	900,000원
위협&분석	다양한 실습으로 쉽게 이해하는 네트워크 Essential		
	3일 (24H)	입문	900,000원
	IT 기초 지식부터 보안까지! 보안 운영자를 위한 첫 걸음		
	5일 (40H)	초급	1,000,000원
	네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z		
	5일 (40H)	초급	1,000,000원
	Metasploit 과 다양한 취약점으로 알아보는 운영체제 해킹		
	5일 (40H)	초급	1,000,000원
	소프트웨어 취약점의 동작 원리부터 익스플로잇까지!		
	4일 (32H)	초급	1,000,000원
위협&분석	웹 구성 이해부터 시작하는 웹 해킹의 모든 것		
	5일 (40H)	초급	1,000,000원
	숨은 악성 행위를 찾아라! 기초부터 시작하는 악성코드 분석		
	5일 (40H)	중급	1,200,000원
	문서형 악성코드부터 실제 유포되는 악성코드까지!		
	APT 공격에 활용되는 악성코드 분석 심화		
	5일 (40H)	중급	1,200,000원
안전한 스마트 환경을 위한 준비! IoT 보안 Starter Kit			
5일 (40H)	중급	1,200,000원	

보안 운영 관리	네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영		
	4일 (32H)	초급	1,000,000원
	사이버 위협 대응을 위한 빅데이터 분석 환경 구축		
포렌식, 침해사고	4일 (32H)	초급	1,000,000원
	관리 체계와 법		
	4일 (32H)	중급	1,200,000원
진단	공격자의 전략, 전술을 추적하는 사이버 침해사고 분석/대응		
	5일 (40H)	중급	1,200,000원
	Digital Forensics and Incident Response (DFIR)		
개발 및 분석	5일 (40H)	고급	1,500,000원
	정보시스템 취약점 진단 입문자를 위한 핵심 가이드		
	5일 (40H)	중급	1,200,000원
개발 및 분석	안전한 웹사이트는 없다! 웹 취약점 진단 실무 과정		
	5일 (40H)	중급	1,200,000원
	공격해보고! 방어해보고! 시큐어 코딩 마스터		
모의해킹	3일 (24H)	중급	1,200,000원
	파이썬을 활용한 취약점 진단 자동화 개발		
	5일 (40H)	고급	1,500,000원
모의해킹	실무에 바로 쓰는 웹 모의해킹 with 미션드리븐		
	5일 (40H)	중급	1,200,000원
	최신 트렌드를 반영한 모의침투 테스트		
	5일 (40H)	중급	1,200,000원
모의해킹	모바일 앱 취약점 진단(Android)		
	3일 (24H)	중급	1,200,000원

1

이산 수학부터 시작하는 암호학의 모든 것

1. 교육 개요

교육시간	09:00~18:00 (4일, 32시간)	교육수준	입문
주제	기초 수학과 암호학에 대한 이해하는 과정에서 정보보안의 기본이 되는 내용을 학습하는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none">· 암호학의 기초와 그의 기반인 이산 수학에 대해 학습· 대칭키 암호와 비대칭키 암호를 식별할 수 있도록 학습· 보안의 기본이 되는 암호학의 원리와 암호학의 응용에 대해 파악
교육특징	<ul style="list-style-type: none">· 암호학의 기반이 되는 기초 수학부터 습득 가능· 암호학에서 자주 쓰이는 수학의 개념에 대해 학습으로 기본기 함양· 시대별 암호학의 개념에 대해 파악 가능

3. 교육 대상

대상
보안에서 사용되는 암호 알고리즘에 이해가 필요하신 분
시스템 상의 기본 연산에 대한 이해가 필요하신 분

4. 커리큘럼

주제	내용	
기초 수학	이산수학 개요	
	논리와 명제	명제
		부정
		논리곱
		배타적 논리합
		함축
		쌍방조건명제
		역, 이, 대우
		항진명제와 모순명제
		논리적 동치
		한정기호
	증명	수학적 귀납법
		직접증명법
		간접증명법
	집합	집합
집합의 종류		
원소		
관계	관계	
함수	함수	
행렬	행렬	
경우의 수	경우의 수	
	기본개념	
암호학	암호학 개요	암호학 소개
	암호학 기본 개념	암호학 용어 이해
		암호 기법 분류
		암호학 기본 개념
		암호화 보안 상식
		암호 알고리즘의 분류
	고전암호	고전암호 개념
	근대암호	근대암호 개념
	현대암호	현대암호
		대칭키 암호
		블록암호
		스트림 암호
		비대칭키 암호
대칭키와 비대칭키 암호 비교		

2

다양한 실습으로 쉽게 이해하는 윈도우 서버 Essential

1. 교육 개요

교육시간	09:00~18:00 (4일, 32시간)	교육수준	입문
주제	윈도우 서버 운영체제의 주요 구조부터 활용방법까지 학습하는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none">· 주요 프로세스, 구조 등을 학습하면서 윈도우 서버 운영체제 활용· 윈도우 운영체제의 기본 명령어 활용하고 레지스트리, 보안 정책 등 관리
교육특징	<ul style="list-style-type: none">· 가상환경 구축을 통해 윈도우 서버 운영체제의 기능 실습· 명령어 및 기능을 효과적으로 습득할 수 있도록 실습 위주의 학습

3. 교육 대상

대상
일상생활 속에서 사용하고 있는 윈도우의 추가적인 기능을 활용하고 싶으신 분
정보보안 입문을 위해 운영체제부터 공부하고 싶으신 분

4. 커리큘럼

주제	내용	
윈도우 개요와 역사	윈도우 개요	윈도우 개요
	윈도우 역사	윈도우 역사
윈도우 운영체제 구조 및 부팅 순서	윈도우 운영체제 구조	윈도우 아키텍처
	윈도우 운영체제 부팅 순서	윈도우 NT 아키텍처 윈도우 운영체제 부팅 순서
윈도우 주요 프로세스 및 서비스	윈도우 주요 프로세스	프로세스의 이해
		윈도우 주요 프로세스
	윈도우 주요 서비스	윈도우 서비스 개요
		윈도우 주요 서비스(선택)
윈도우 레지스트리의 이해	윈도우 레지스트리의 이해	레지스트리 개요
		윈도우 레지스트리의 이해
		윈도우 레지스트리 명령어
윈도우 계정	윈도우 계정의 이해	윈도우 계정의 이해
	윈도우 계정 관리	윈도우 계정 관리
윈도우 파일 시스템	파일시스템과 디스크의 이해	파일 시스템과 디스크의 이해
	파일시스템과 디스크 관리 실습	파일시스템 구성
윈도우 시스템 관리	공유 폴더 관리	공유 폴더 개요
		공유 폴더 관리
		서비스 관리
	로컬 보안 정책 관리	로컬 보안 정책
	이벤트 로그 관리	이벤트 로그의 활용
		이벤트 로그 분류
		이벤트 로그 종류
		이벤트 로그 속성
		이벤트 로그 수준 종류
		이벤트 로그
		보안 로그 필터링
이벤트 로그 관리 설정-이벤트 뷰어		
이벤트 로그 관리 설정-레지스트리		
윈도우 분석 도구 소개	Sysinternals	Windows Sysinternals
		Process Explorer
		Autoruns
		Process Monitor
		PsTools
		RootkitRevealer
		TCP View

3

다양한 실습으로 쉽게 이해하는 리눅스 서버 Essential

1. 교육 개요

교육시간	09:00~18:00 (4일, 32시간)	교육수준	입문
주제	리눅스 서버 운영체제의 주요 구조부터 활용방법까지 학습하는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none">· 리눅스 서버 운영체제, 기본 명령어를 활용할 수 있는 역량 개발· 리눅스에서 프로세스, 파일 및 디렉터리 등을 생성하고 관리할 수 있는 능력
교육특징	<ul style="list-style-type: none">· 가상환경 구축을 통해 리눅스 서버 운영체제의 기능 실습· 명령어 및 기능을 효과적으로 습득할 수 있도록 실습 위주 학습

3. 교육 대상

대상
정보보안 입문을 위해 운영체제부터 공부하고 싶으신 분
리눅스 운영체제를 사용해야하는데 처음 접해보신 분

4. 커리큘럼

주제	내용		
리눅스 역사 및 종류와 소개	리눅스의 역사	리눅스의 역사	
	리눅스 종류와 소개	유닉스개요	
		유닉스 종류	
		리눅스 개요	
리눅스 부팅 과정 및 기본 환경 구성	부팅 과정의 이해	리눅스 종류	
		부팅 과정	
		프로세스 실행	
		매직키 설정	
	설치와 기본 환경 구성	가상 터미널 실행	
		다운로드	
		VMware 구성	
리눅스 기본 명령어	기초 명령어 및 파일 편집	CentOS 설치	
		X윈도우 설치	
네트워크 구성과 관리	네트워크 구성	기본 명령어 실습 및 VIM 에디터 사용하기	
		네트워크 구성의 이해	
파일, 파일시스템, 디렉터리 이해	파일과 디렉터리 이해	네트워크 구성	
		링크 파일	
	파일 시스템 이해와 디스크 관리	파일 시스템 이해	
		리눅스 파일시스템 이해	
사용자 및 퍼미션의 이해	사용자 이해와 관리	디스크 관리	
		계정의 이해	
		계정 관리	
		계정 관리 관련 파일 및 디렉터리	
	퍼미션의 이해와 관리	그룹 관리	
		퍼미션과 소유권	
		소유권 관리	
		퍼미션의 이해	
	프로세스 이해와 관리	퍼미션의 관리	SetUID, SetGID, Sticky bit
			프로세스
시그널			
데몬			
리눅스 시스템 관리	로그 이해와 관리	프로세스의 제어	
		rsyslog	
		logrotate	
	리눅스 접근통제 기법	로그 관련 주요 파일	
리눅스 방화벽(iptables)			
		리눅스 방화벽(TCP Wrapper)	

4

논리적 사고방식으로 이해하는 프로그래밍 기초

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	입문
주제	· 프로그래밍 기술을 외우는게 아닌 이해하고 활용할 수 있는 역량을 강화한다. · 프로그래밍 시 필요한 알고리즘 작성하는 방법을 이해한다.		

2. 교육목표 및 특징

교육목표	· 프로그래밍 기술을 외우는 게 아닌 이해하고 활용할 수 있는 역량 강화 · 프로그래밍 시 필요한 알고리즘 작성하는 방법 이해
교육특징	· 기본부터 응용까지 다양한 프로그래밍 기본 지식을 학습 · 여러가지 간단한 프로그램을 만들어 봄으로써 알고리즘을 작성하는 방법 학습

3. 교육 대상

대상
임베디드 시스템 개발자
C언어 기반의 프로그램 개발을 희망하는 자

4. 커리큘럼

주제	내용	
프로그래밍 기초 이론	프로그래밍 개요	프로그래밍 정의
		프로그래밍의 접근 방법
		프로그래밍(프로그래머) vs 코딩(코더)
		프로그래밍의 목적 및 순서
	프로그래밍 언어	프로그래밍 언어 개요
		프로그래밍 언어 분류
		프로그래밍 언어 순위
C 프로그래밍 실전	C언어 프로그래밍	C언어 개요 및 IDE 설치
		C언어 기본 구조
		변수와 기본 자료형
		데이터 입출력
		연산자
		반복문과 조건문
		함수
		배열과 포인터
		구조체
		문자열 관련 함수
		파일 입출력
		메모리 관리와 동적 할당
		헤더 및 전처리 지시자
		자료구조

어셈블리어 분석으로 프로그램을 재구축해보는 리버스 엔지니어링 개론

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	입문
주제	<ul style="list-style-type: none"> · 리버스 엔지니어링의 기초 개념과 각 분야별 활용법을 이해한다. · 시스템 아키텍처에 대한 이해를 바탕으로 정/동적 분석을 수행한다. 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 리버스 엔지니어링의 기초 개념과 각 분야별 활용법 이해 · 시스템 아키텍처에 대한 이해를 바탕으로 정적/동적 분석 수행
교육특징	<ul style="list-style-type: none"> · 리버스 엔지니어링 실습 시 어셈블리어부터 레지스터, 메모리까지 단계별 실습 · 프로그래밍 기반 기초 문법들로 구성하여 기본적인 루틴을 단계별 학습 · 프로그램 흐름을 파악하고 효율적인 분석을 방안 학습

3. 교육 대상

대상
리버싱 분야의 해킹대회 문제에 도전해보고 싶으신 분
리버스 엔지니어링을 실습위주로 이해하고 싶으신 분

4. 커리큘럼

주제	내용	
리버스 엔지니어링 기초	리버스 엔지니어링의 이해	리버스 엔지니어링 개요
		리버스 엔지니어링과 법
	컴퓨터 구조	컴퓨터 구조 개요
		CPU 구조 및 기능
		인텔 아키텍처의 이해
	메모리와 레지스터	메모리 구조
		레지스터의 이해
	어셈블리어 기초	어셈블리어의 이해
	리버스엔지니어링 툴 사용법	리버스 엔지니어링 툴 종류
		Ollydbg 사용법
IDA 사용법		
리버스 엔지니어링 실전	기본 프로그램 분석	데이터 입출력 프로그램 분석
		파라미터와 데이터 표현 방식
	분기문/반복문 흐름 분석	분기문
		반복문
	배열과 포인터 동작 분석	배열과 포인터
	구조체 동작의 이해 및 분석	구조체
	파일 입출력 흐름 분석	파일 입출력
	메모리 동적 할당	메모리 동적할당
	함수호출 규약의 이해	함수호출 규약
	문제풀이를 통한 실전 리버스 엔지니어링	실전 리버스 엔지니어링 실습

6

다양한 실습으로 쉽게 이해하는 네트워크 Essential

1. 교육 개요

교육시간	09:00~18:00 (3일, 24시간)	교육수준	초급
주제	· 네트워크의 이론을 이해한다. · 네트워크의 역사부터 현대까지의 흐름을 이해한다. · 네트워크 모델인 OSI 7 계층과 TCP/IP 모델을 학습한다.		

2. 교육목표 및 특징

교육목표	· 기본 용어, 모델에 대한 이해를 통해 네트워크의 전체적인 흐름 파악 · 네트워크 모델인 OSI 7 계층과 TCP/IP 모델 학습
교육특징	· 네트워크의 각 계층에서 주로 사용하는 프로토콜의 헤더를 보며 상세히 학습 · 네트워크 망 구축 실습을 통해 네트워크에 대한 이해

3. 교육 대상

대상
네트워크에 대한 이해를 필요로 하시는 분
네트워크 망 구축에 대한 역량을 강화하고 싶은 분

4. 커리큘럼

주제	내용	
네트워크 개요	네트워크 역사	글로벌 네트워크 역사
		국내 네트워크 역사
	네트워크 용어의 이해	네트워크란?
		프로토콜
		네트워크 분류
		토큰링
		CSMA/CD
		CSMA/CA
	네트워크 모델의 이해	추상화
		네트워크 모델의 종류
		OSI 7 Layer
		TCP/IP 모델 계층 구조
근거리 네트워크 구성	근거리 네트워크 구축 실습	Packet Tracer 시작
		환경 구성
		동일 네트워크 통신
		패킷 트레이서를 이용한 망 구축 1
	OSI 7 계층 모델 1, 2 계층	OSI 7 계층
		OSI 7 계층 구조
		물리 계층
		데이터링크 계층
	스위치 개요와 종류	스위치 개요
		스위치 종류
		L2 스위치
	데이터링크 계층의 이해	데이터링크 계층과 링크 계층
		서비스
	ARP의 이해	ARP 구조
		ARP 동작 원리
	MAC 주소 체계	개요
구조		
라우터가 포함된 망 구성	라우터가 포함된 네트워크 구성	다른 네트워크 통신
		패킷 트레이서를 이용한 망 구축 2
	OSI 7 계층 모델 3 계층	네트워크 계층
	IPv4의 이해	IP의 이해
		IPv4 클래스
		IP의 이해
	IPv6의 이해	IPv6
		IPv4와 IPv6
	ICMP의 이해	ICMP
	라우터와 라우팅 알고리즘	라우터 개요
		라우팅 알고리즘 종류
		라우팅 프로토콜

	NAT 의 이해	NAT
		NAT 통신 과정 예
		NAT 구성 상의 네트워크 통신
	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 4 계층	전송 계층
	TCP 와 UDP	TCP
		3-Way Handshake
		UDP
		TCP/UDP
	OSI 7 계층 모델 5~7 계층	세션 계층
		표현 계층
		어플리케이션 계층
		OSI 7 계층 정리
	대규모 망 구성	패킷 트레이서를 이용한 망 구축 3

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	보안 업무를 갓 시작한 신입 보안 담당자를 위한 IT 기초 지식부터 보안 인프라를 이해할 수 있도록 합니다.		
특이사항	<ul style="list-style-type: none"> · 기존에 보유한 기본 IT 지식을 바탕으로 하기에 교육 수강에 필요한 요소를 전반적으로 복습합니다. · 리눅스 명령어, 네트워크 기초 지식을 사전에 습득했다면 보다 수강하기 할 수 있습니다. 		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · IT 인프라 내 보안을 하기 위한 목적과 대상을 명확히 이해 · 기본적으로 알아야 하는 서버 및 장비 운용 핵심 지식 습득 · 보안 솔루션 장비의 종류와 기본적인 운용 방식 습득
교육특징	<ul style="list-style-type: none"> · 인프라를 기반으로 보안 직무와 그 역할 부터 데이터의 흐름까지 한 눈에 이해 · 초급 재직자를 위한 기반 지식 리마인드 및 직무별 팁 전수 · 특정 직무에 특화되지 않고, 모든 보안 직무에 공통적으로 알아야 할 내용으로 구성

3. 교육 대상

대상	주요 학습 포인트
신입 보안담당자	'일잘러'로 성장하기 위한 IT 기초 지식 및 보안 인프라 이해
직무순환 대상자	보안 직무는 처음이라 막막한 직무순환 대상자를 위한 기초 교육
신입 보안솔루션 운영자	보안 솔루션이 낯선 신입 운영자를 위한 기초 교육

4. 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
		시스템 구조
	리눅스 기초	리눅스 종류와 소개
		리눅스 기본 명령어
		네트워크 구성과 관리
		퍼미션, 프로세스 이해와 관리
내 PC 부터 웹 접속까지 데이터 흐름 이해하기	네트워크 보안 배경지식	OSI 7Layer 모델의 이해
		TCP/IP 모델 계층 구조
	네트워크 장비	스위치/라우터 개요
		계층에 따른 네트워크 장비
필수로 알아야할 보안 장비 운영하기	보안 인프라 구성	보안 솔루션 종류와 이해
	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	담당자가 알아야할 주요 제도	정보보안 관련 법률과 제도 (정보통신망법, 개인정보보호법, GDPR 등)
		보안 인증제도 (ISMS, ISO27000 시리즈 등)
	참고할 만한 주요 가이드	공공 기관 주요 가이드 (주요정보통신기반시설 취약점 가이드, 기타 KISA 가이드 등)
		민간 기관 주요 가이드 (금보원 가이드, SK 쉐더스 가이드 등)
		국외 주요 가이드 (NIST, MITRE Cybersecurity Operation Center 등)

8 네트워크 해킹부터 공격 분석까지! 네트워크 보안 A-Z

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	<ul style="list-style-type: none"> · 네트워크의 공격 방법과 원리를 이해한다. · 공격 과정을 통해 대응할 수 있는 방법을 이해하고 실무 적용 역량을 키울 수 있다. 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 다양한 종류의 실습으로 네트워크의 공격 방법과 원리 이해 · 공격 과정을 통해 대응할 수 있는 방법을 이해하고 실무 적용 역량 향상
교육특징	<ul style="list-style-type: none"> · 네트워크 중심의 다양한 종류의 공격 방법 실습 · 침해사고 발생 시 네트워크 흔적을 분석하는 방법 학습 · 무선랜 환경에 대해 이해하고, 지나치기 쉬운 취약한 무선랜 보안에 대한 이해

3. 교육 대상

대상	주요 학습 포인트
네트워크 보안 담당자	공격 및 분석에 대해 실습하면서 유·무선 네트워크에서 발생할 수 있는 위협에 대비할 수 있는 실무 능력 향상에 도움
정보보호 관련 실무자	다양한 유형의 공격 실습으로 유·무선 네트워크 위협에 대해 이해하고
취업준비생, 대학생	네트워크 분야의 위협을 식별할 수 있는 역량 강화로 관련 분야 취업 준비에 도움

4. 커리큘럼

주제	내용	
네트워크 해킹	네트워크 해킹 개요	
	네트워크 스캐닝	네트워크 개요
		네트워크 스캐닝
		네트워크 스캐닝 실습
		hping3 를 이용한 스캐닝
		네트워크 스캐닝 실습
	근거리 네트워크 공격 개요	근거리 네트워크 위협
		ARP 스푸핑을 이용한 MITM 공격
		ARP 스푸핑 공격 실습
		DHCP Starvation 공격 실습
	DoS 공격의 이해와 종류	DoS 와 DDoS 오해
		DoS 공격 역사
		DoS 공격 종류
		DoS 공격 종류 - BPS
		DoS 공격 종류 - PPS
		DoS 공격 종류 - RPS
		DoS 공격 종류 - 기타
	BPS 유형 DoS 공격 실습	UDP Flood 공격
ICMP Flood 공격		
PPS 유형 DoS 공격 실습	SYN Flood 공격	
	ACK Flood 공격	
	FIN Flood 공격	
RPS 유형 DoS 공격 실습	RUDY 공격	
	TorsHammer 공격	
	Slowloris 공격	
	CVE-2018-6389 취약점	
TCP 연결 기반 DoS 공격 실습	TCP 연결 구조	
	TCP 연결 기반 DoS 공격 실습	
암호화 통신과 위협	SSL 과 TLS 의 이해	HTTPS 의 이해
		SSL 의 이해
	암호화 통신 공격의 이해	SSL MITM 공격의 이해
		SSL Strip 공격의 이해
		Heartbleed 의 이해
		POODLE 의 이해
	암호화 통신 공격 실습	실습 환경
		SSL Strip 공격 실습
	Heartbleed 공격 실습	실습 환경
		공격 실습

네트워크 패킷 분석	패킷 분석 방법	패킷 수집 기법
		와이어샤크 캡처
		와이어샤크 인터페이스
		와이어샤크 설정
		와이어샤크 주요 메뉴
		와이어샤크 필터링 기법
		공격별 분석 기법
		분석 상세 기법
		Snort 를 활용한 분석
	정규 표현식	정규 표현식 개요와 종류
		정규 표현식의 이해 및 실습
		정규 표현식 예제 실습
	YARA	개요
룰 구성		
Yara 사용 예		
Captipper 를 이용한 네트워크 분석	개요	
	Captipper 활용 분석	
무선 네트워크 위협	무선 네트워크 해킹 개요	무선 취약점 위협
		개인정보 유출
		스마트폰 보안 위협
		무선 공유기 보안 위협
		무선 보안 취약점
		Wi-Fi 구역 검색 방식
		주변 AP 스캐닝
		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 암호방식
		WPA 암호방식
		무선랜 인증 방식
		무선랜 암호화 방식
		GPU 를 이용한 WPA Cracking
WEP 암호화 방식 공격 실습	WEP Key Crack 실습	
WPA 암호화 방식 공격 실습	WPA/WPA2 Crack 실습	

9

Metasploit과 다양한 취약점으로 알아보는 운영체제 해킹

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	<ul style="list-style-type: none"> · 운영체제(윈도우, 리눅스)를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법에 대해 알 수 있다. · 공격 이후 이를 대응할 수 있는 방안에 대해 실제 현업에서 적용할 수 있는 사례 기반의 내용을 이해할 수 있다. 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 운영체제(윈도우, 리눅스)를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법에 대해 학습 · 공격 이후에 대응할 수 있는 방안에 대해 실제 현업에서 적용할 수 있는 사례 기반의 내용으로 이해
교육특징	<ul style="list-style-type: none"> · 실제로 운영체제를 공격할 때 많이 사용하는 툴을 이용하여 취약점 정보 수집 실습 진행 · 도구에 내장된 공격코드 뿐 아니라 최근 공격코드 관련해서 알아보고 이를 응용할 수 있는 방법에 대해 실습 · 대응방안 수립 시 일반적인 내용이 아닌 근본적인 대책과 차선책에 대해 학습

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	활용도가 높은 공격기법의 원리를 이해하여 모의해킹 업무의 수행 능력을 향상
정보보호 관련 실무자	입문부터 활용 단계까지 학습하여 윈도우, 리눅스 등 운영체제 해킹에 대한 이해를 통해 보안 강화
취업준비생, 대학생	모의해킹이나 취약점 분석 분야로 직무를 설정한 다음 그에 맞는 역량 강화를 준비하는데 도움

4. 커리큘럼

주제	내용	
공격기술을 배우기 전 알아야 할 보안윤리	윤리적이고 합법적인 해킹	컴퓨터 해커
		범죄적 해킹
		우호적 해킹
		법의 회색 지대
모의해킹 시작 전 알아야 할 실무적 절차	모의해킹 방법론	모의해킹 개요
		모의해킹과 범죄자 비교
		모의해킹 범위 - 시스템 접근 기준
		모의해킹 범위 - 수행 관점 기준
		모의해킹 종류
모의해킹 업무 절차		
도구를 활용한 정보수집 기법의 이해	정보수집	스캐닝 개요
		스캐닝 실습
대표적 공격 도구 활용 기초	Metasploit	Metasploit 개요
		Metasploit GUI
		Metasploit Console
		Metasploit 사용 방법
		Autopwn
		Shellcode 추출
		MS_08_067_Netapi
		Veil-Framework
활용도 높은 공격기법 원리이해(윈도우)	윈도우 침투테스트	리버스 커넥션
		패스워드 크랙
		MS17_010_Eternalblue
활용도 높은 공격기법 원리이해(리눅스)	리눅스 침투테스트	환경 구성
		Nmap 을 활용한 포트 스캐닝
		Searchsploit 을 활용한 취약점 검색
		CVE-2007-0882 취약점 Exploit
		SSH Bruteforcing Attack
		RPC(Remote Procedure Call)
		로그인 사용자 조희
		root 계정 패스워드 복호화
		Privilege Escalation
		SNMP Exploit
		X 윈도우 시스템

10 소프트웨어 취약점의 동작 원리부터 익스플로잇까지!

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	<ul style="list-style-type: none"> · 소프트웨어 보안 취약점을 이해하고 이를 해결할 수 있을 방안을 이해한다. · 해킹대회에 출제되는 다양한 Pwnable 문제에 대한 해결 역량을 강화한다. 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 소프트웨어 보안 취약점에 대해 이해하고 이를 해결할 수 있을 방안 이해 · 해킹대회에 출제되는 다양한 Pwnable 문제에 대한 해결 역량 강화
교육특징	<ul style="list-style-type: none"> · 기초부터 단계적으로 학습함으로써 소프트웨어 취약점의 원리를 이해 · 소프트웨어 보안을 위한 메모리 보호 기법의 원리를 학습하고 이를 우회하기 위한 방법 이해

3. 교육 대상

대상
해킹대회(CTF) Pwnable 분야에 대한 공부를 시작하고 싶으신 분

4. 커리큘럼

주제	내용	
어플리케이션 취약성 개요	소프트웨어 취약성 개요	소프트웨어 취약성 개요
	어플리케이션 취약점과 취약성	소프트웨어 취약성 정의
		소프트웨어 취약성과 취약점
		소프트웨어 취약성 판단
		소프트웨어 취약점 구분
		소프트웨어 취약점 파급력
어플리케이션 해킹 기초 개념	메모리 구조 개요	메모리 정의
		메모리 모델-선형 주소 공간
		메모리 구조
	OS에 따른 메모리 구조	OS에 따른 메모리 구조 차이
버퍼 오버플로우 기초	버퍼 오버플로우 개요	버퍼 오버플로우 개요
	스택 기반 버퍼 오버플로우 이해 및 실습	스택 기반 버퍼 오버플로우 개요
		스택 기반 버퍼 오버플로우 원리 실습
	Shellcode 구조 및 동작 방식	Shellcode 개요
		Shellcode 제작
		Shellcode 삽입
		기타 Shellcode 개요
기타 Shellcode		
메모리 보호 기법과 우회 기법	구조적 예외 핸들러(SEH)	구조적 예외 핸들러 개요
		Windows 예외 처리 개요
	데이터 실행 방지(DEP) 이해 및 실습	데이터 실행 방지 개요
		데이터 실행 방지 설정
		데이터 실행 방지 적용
	Return to Library(RTL) 이해 및 실습	Return to Library(RTL) 개요
		Return to Library(RTL) 동작원리
	임의의 주소 공간 배치(ASLR) 이해 및 실습	임의의 주소 공간 배치 개요
		임의의 주소 공간 배치 원리
	Return to Oriented Programming(ROP) 이해 및 실습	Return to Oriented Programming 개요
Return to Oriented Programming 동작원리		
정수 오버플로우	정수 오버플로우 개요	정수 오버플로우 정의
		정수 오버플로우 동작원리
	정수 오버플로우 종류	정수 오버플로우 종류
		종류 별 정수 오버플로우 동작원리
취약성 관리 체계	CVE 코드의 이해	개요
		MITRE
	CVSS 산출 방식과 위험성 평가의 이해	MITRE
		CWE 코드의 이해

11 웹 구성 이해부터 시작하는 웹 해킹의 모든 것

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	<ul style="list-style-type: none"> · 웹 서비스를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법에 대해 알 수 있다. · 웹 공격 이후 이를 대응할 수 있는 방안에 대해 실제 현업에서 적용할 수 있는 사례 기반의 내용을 이해할 수 있다. 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 웹 서비스를 대상으로 취약한 정보를 수집하고 이를 공격할 수 있는 기법 학습 · 공격 이후 대응할 수 있는 방안에 대해 현업에 적용할 수 있는 사례 기반의 내용을 이해
교육특징	<ul style="list-style-type: none"> · 실제 웹 모의해킹 시 많이 사용하는 주요 공격기법의 상세한 설명과 테스트 사이트 내에서 응용실습 진행 · 대응방안 수립 시 일반적인 내용이 아닌 현업에서의 근본적인 대책과 차선책에 대한 내용

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	다양한 실습으로 웹 해킹 공격에 대한 실질적인 대응방안을 수립할 수 있는 업무 능력 향상
정보보안 담당자	웹 해킹에 대한 이해를 통해 기관 또는 사내 웹 서비스의 취약점에 대한 대응 방안을 수립하여 보안 강화
취업준비생, 대학생	모의해킹이나 취약점 분석 분야로 직무를 설정한 다음 그에 맞는 역량 강화를 준비하는데 도움

4. 커리큘럼

주제	내용	
웹 구성의 이해	웹 서비스 구성	웹 서비스 구성
	클라이언트 & 서버	클라이언트 & 서버
	클라이언트 & 서버 측 언어의 이해	웹 서비스 구성 - 언어
	URL 과 URI	URL 과 URI 개념
	인코딩	URL 구조 인코딩 개념

		URL 인코딩	
		Base64 인코딩	
		메타 문자 이해	메타 문자
		HTTP 프로토콜 이해	HTTP 개요
			HTTP Request
			HTTP Response
			HTTP Response Status Code
		쿠키, 세션 이해	쿠키
			세션
		웹 해킹의 이해와 실습	웹 해킹 개요
웹 취약점 진단			
웹 서비스 구성			
웹 서비스 보안 대상			
웹 취약점 진단과 모의 해킹			
모의해킹			
웹 해킹 점검 도구	Burp suite 개요		
주요 웹 취약점 및 공격	SQL Injection		
	SQL Injection 위험성		
	SQL Injection 시큐어코딩		
	XSS		
	Reflected XSS(반사형)		
	Stored XSS(저장형)		
	XSS 공격 실습		
	XSS 대응방안		
	파일 업로드		
	파일 업로드 취약점 원인 분석		
	파일 업로드 우회기법		
	파일 업로드 공격 시나리오		
	파일 업로드 대응방안		
	파일 다운로드		
	파일 다운로드 취약점 동작방식		
	파일 다운로드 우회기법		
	파일 다운로드 공격 시나리오		
	파일 다운로드 대응방안		
불충분한 인증 및 인가 개요			
불충분한 인증 및 인가 실습			
불충분한 인증 및 인가 대응방안			
웹 해킹 방어를 위한 개발보안	보안 요구사항 분석 및 설계	입력 값 검증	
		파일 처리	
		데이터베이스 처리	
		인증과 권한	
		에러처리	
		암호화	

12 숨은 악성 행위를 찾아라! 기초부터 시작하는 악성코드 분석

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	다양한 파일 형태로 존재하는 악성코드의 분석 방법을 이해하고, 실제 유포되었던 악성코드를 기반으로 APT 공격에 활용되는 악성코드의 공격 전략과 대응 방안에 대해 학습하는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 악성코드의 유형과 유입 경로 파악을 통해 침해사고가 발생할 수 있는 공격 벡터 이해 · 악성코드 동적/정적 분석을 통해 작성하는 결과 보고서를 이해하기 위한 기본 지식 학습 · 자동화 분석 시스템을 기반으로 다양한 케이스의 악성코드 분석하고 공격자들의 전략 이해
교육특징	<ul style="list-style-type: none"> · 트로이목마, 바이러스, 웹 악성코드 유형을 이해하고 크립토락커, 크립토 마이닝, RAT 등 다양한 유형을 분류하는 방법 이해 · 악성코드를 여러 관점에서 정적/동적분석을 해보고 위협지표를 찾는 방법 학습 · 자동화 분석 시스템 구축 및 운영을 통해 다양한 악성코드 분석 보고서를 보며 공격 방식 학습

3. 교육 대상

대상	주요 학습 포인트
악성코드 분석 실무자	다양한 악성코드의 유형 별로 효과적인 분석 방법 이해하면서 실무 역량 강화에 도움
정보보안 담당자	갈수록 진화하는 악성코드의 유형 파악 및 분석을 학습해 유형에 따른 대응방안을 수립하는데 도움
취업준비생, 대학생	정보보안 취업에 앞서, 다양한 유형의 악성코드 분석 기술 향상

4. 커리큘럼

주제	내용	
악성코드의 이해	악성코드 의미와 동향	악성코드 개요
		악성코드 및 해킹 최신 동향
	악성코드 유형별 이해	악성코드 대유형
		악성코드 소유형
		RAT 악성코드의 이해 및 실습
		랜섬웨어의 이해 및 실습
	악성코드 유입 경로	악성코드 유입 경로 이해
		USB를 이용한 악성코드 유포 이해 및 실습
		웹 페이지를 이용한 악성코드 유포 이해 및 실습
		이메일을 이용한 악성코드 유포 이해 및 실습
실전 악성코드 분석	악성코드 분석 개론	악성코드 분석 개요
		악성코드 분석 환경 개요
	악성코드 정적 분석 악성코드 동적 분석 악성코드 자동화 분석	악성코드 정적 분석 이해 및 실습
		악성코드 동적 분석 이해 및 실습
		악성코드 자동화 분석 이해 및 실습
악성코드 대응 방안	악성코드 대응 및 방어 실무	YARA 패턴 제작 및 활용
		악성코드 대응방안

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	다양한 파일 형태로 존재하는 악성코드의 분석 방법을 이해하고, 실제 유포되었던 악성코드를 기반으로 APT 공격에 활용되는 악성코드의 공격 전략과 대응방안 학습		
특이사항	<ul style="list-style-type: none"> · 샘플 악성코드는 실제 유포되었던 악성코드로 실습 시 반드시 안내에 따라 진행해주시기 바랍니다. · 본 교육은 스크립트 등 코드 분석 등이 포함되어 있어 기본적인 프로그래밍 지식이 필요합니다. 		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · EXE, 문서, 스크립트 등 다양한 형태의 악성코드 이해 및 분석 역량 강화 · 최신 악성코드 행위 분석을 통해 공격자들의 공격기법 및 방어 회피 전략 파악
교육특징	<ul style="list-style-type: none"> · 실제 APT 공격에 활용되었던 악성코드를 분석함으로써 공격자들의 행위 파악 · EXE, 문서, VBScript 등 다양한 형태의 악성코드 분석 방법 학습

3. 교육 대상

대상	주요 학습 포인트
악성코드 분석 실무자	다양한 악성코드를 유형 별로 효과적인 분석 방법을 알고 싶어요.
침해사고 대응 실무자	침해사고가 발생하는 주 원인인 악성코드를 분석해서 침해사고 대응에 활용하고 싶어요.
정보보안 담당자	날이 갈수록 진화하는 악성코드의 유형을 파악하고 각 유형에 따른 대응 방안을 배우고 싶어요.
취준생, 대학생	다양한 유형의 악성코드 분석 기술을 사용할 수 있다는 강점으로 관련 직무 취업 준비를 하고 싶어요.

4. 커리큘럼

주제		내용
악성코드 분석 개요	악성코드 분석 개요	악성코드 분석 의의
		악성코드 분석 방법론
케이스별 악성코드 분석 실습 - PE 악성코드	PE 악성코드 분석	PE 악성코드 분석 개요
		C/C++ 악성코드 분석
		C# 악성코드 분석
케이스별 악성코드 실습 - 문서형 악성코드	문서형 악성코드 분석	문서형 악성코드 개요 및 동향
		Script 형 악성코드 분석 개요
		Javascript 악성코드 분석
		VBScript 악성코드 분석
		PDF 악성코드 분석
		MS Office 악성코드 분석
		HWP 악성코드 분석
악성코드 대응	가이드를 통한 악성코드 대응 방안	
	IoC 의미와 활용 방안	

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	ICT 융합 사회를 대표하는 기술인 IoT(사물인터넷)에 대한 보안 위협을 이해하고 보안 수준을 높이기 위한 취약점 분석 방법을 학습하는 과정		
특이사항	실습에 필요한 기기는 교육 중에만 제공됩니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · IoT 서비스에 대한 전반적인 구성 및 최근 보안 위협과 공격 영역 이해 · IoT 디바이스 펌웨어 분석 및 취약점 분석에 필요한 도구 사용 방안 습득 · IoT 디바이스 펌웨어 취약점 분석 방안을 적용한 IoT 취약점 분석 역량 강화
교육특징	<ul style="list-style-type: none"> · 실무에서 사용하는 도구들을 기반으로 다양한 기기들의 펌웨어 분석 · 최신 취약점을 기반으로한 펌웨어 취약점 분석 학습 · 실제 사례를 기반으로 한 시나리오 재구성을 통한 실습 프로그램 구성

3. 교육 대상

대상	주요 학습 포인트
IoT 기기 개발자	안전한 IoT 서비스를 제공하기 위해 IoT 기기에 대한 공격이 어떻게 일어나는지 이해
IoT 보안 실무자	실무에도 적용할 수 있는 IoT 기기 분석 도구 활용법과 취약점 분석 방안 학습
취업준비생, 대학생	요즘 대세인 융합보안을 실무에 가까운 실습 위주 학습 및 역량 향상

4. 커리큘럼

대단원	중단원
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
	IoTCTFd 를 활용한 취약점 분석
취약점 악용 해킹 시나리오 실습	공유기 DNS 변조 공격 시나리오 실습
	공유기 DNS 변조 공격 시나리오 풀이

15 네트워크 구성도 이해부터 알아보는 보안 솔루션 구축 및 운영

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	초급
주제	네트워크 구성도를 보며 이해하는 보안 솔루션의 운영과 네트워크 장비의 취약점 진단을 진행하는 과정		
특이사항	<ul style="list-style-type: none"> · 네트워크 기본 지식과 리눅스 활용 능력 필요 · 많은 양의 가상머신을 사용해야 하므로 고사양의 노트북, 컴퓨터 필요 		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 여러가지 보안 솔루션의 종류에 대해 학습하고, 각 장비들의 장단점 이해 · 방화벽, IDPS, 웹방화벽 등 보안 솔루션 각 세대별 차이와 실제 현업에서 사용하는 기능들 이해 · 방화벽, IDPS, 웹방화벽 등 보안 솔루션 각 장비별 룰 구성에 대해 이해하고 응용할 수 있는 역량 강화
교육특징	<ul style="list-style-type: none"> · 보안 관제에서 많이 사용하는 장비의 종류들을 직접 구축해보고 실습 · 사례기반으로 발생했던 공격들에 대한 룰을 제작하는 방법 학습

3. 교육 대상

대상
보안 솔루션의 종류 운용 방법에 대해 습득하고자 하시는 분
방화벽 룰 작성법에 대한 이해가 필요하신 분

4. 커리큘럼

주제	내용	
보안 운영의 이해	보안 관제 운영업무 이해	탐지의 절차
		탐지 준비
		상세 탐지
		지속 탐지
	보안 솔루션 종류와 이해	개요
		보안 솔루션 시장
		기술의 변화
		솔루션 인프라 구성도
		보안장비 종류
	정탐, 오탐 그리고 미탐의 이해	혼동행렬
네트워크 기반 솔루션 운영	방화벽의 이해와 종류	방화벽의 이해와 종류
		방화벽 구성
		방화벽 룰
	네트워크 방화벽(Untangle) 구축	Untangle의 이해
		방화벽 환경 구성
		방화벽 환경 구축
	네트워크 방화벽(Pfsense) 구축	개요
		환경 구성
		방화벽 구축
		방화벽 룰 구조
		방화벽 정책 적용
		방화벽 정책 설정 실습
	네트워크 방화벽(OPNsense) 구축	개요
		환경 구성
		방화벽 구축
		방화벽 룰 구조
		방화벽 정책 적용
		방화벽 정책 설정 실습
	IPS(Suricata) 구축	환경 구성
		IPS(suricata) 구축
		포워딩 설정
		룰의 이해
		Suricata 로그의 이해
		룰 적용 테스트
정규표현식	정규 표현식 개요와 종류	
	정규 표현식의 이해 및 실습	
	정규 표현식 예제 실습	

	Snort 룰 이해 및 실습	Snort의 개요
		룰의 이해
		Snort와 Wireshark 연동
	웹 방화벽 구축(CASTLE)	캐슬(CASTLE) 개요
		구축 환경
		웹 방화벽 구축
		정책 적용 테스트
	웹 방화벽 구축(Mod_Security)	캐슬(CASTLE) 개요
		웹 방화벽 구축
엔드포인트 기반 솔루션 운영	DLP의 이해	개요
		원리
		관리절차
	DLP(MyDLP) 구축	DLP(MyDLP) 구축 실습
	DLP(MyDLP) 운영 실습	엔드포인트 환경 구성
		엔드포인트 관리
		스크린샷 정책 적용

16 사이버 위협 대응을 위한 빅데이터 분석 환경 구축

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	가상의 보안 인프라 환경에서 발생하는 이벤트 수집 및 분석을 하면서 SIEM를 이용한 빅데이터 분석 환경을 구축해볼 수 있는 보안 관제 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 보안 관제 직무를 명확히 파악하고 종합 운영 대책을 마련할 수 있도록 역량 강화 · 보안 인프라 환경 내 솔루션의 역할을 구분하고 통합 운영이 가능하도록 능력 향상 · 각 보안 인프라 환경에서 발생하는 이벤트를 수집하고, 분석할 수 있는 역량 향상
교육특징	<ul style="list-style-type: none"> · 개별 PC에서 가상의 인프라 환경을 구축하고 실제로 운영해보며, 실무와 유사한 환경에서 학습 · 각 솔루션에서 발생하는 이벤트 등을 수집하고 종합 분석이 가능하도록 학습

3. 교육 대상

대상	주요 학습 포인트
정보보호 관련 실무자	SIEM을 이용하여 빅데이터 분석 환경을 구축하는 능력 향상에 도움
취업준비생, 대학생	보안 관제 분야 역할과 업무에 대해 알아보고 해당 직무로 취업하고 싶은 분

4. 커리큘럼

주제	내용	
보안 관제 개요	보안 관제 개념	관제의 의미
		보안 관제 영역
		보안 관제의 필요성
	보안 관제 운영 업무 이해	탐지의 절차
		탐지 준비
		상세 탐지
통합보안운영 개요	통합보안운영의 필요성	통합보안운영 배경
		통합보안운영 목적
	통합보안운영의 분류	ESM의 이해
		SIEM의 이해
	보안시스템 구축을 위한 실무가이드	보안시스템 구축 개요
		구축 프로세스
정보보호사업 요구사항 분석, 적용 단계별 수행활동		
		보안시스템 구축 절차 상세
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	
	Elastic Stack을 활용한 로그 수집	윈도우 로그 수집
Suricata 로그 수집		
Elastic Stack을 활용한 통합보안운영	가상 통합 보안 인프라 설계 및 구축	가상 시나리오 배경
	설계된 인프라를 활용한 위협 탐지	환경구성
		Snort를 활용한 위협 탐지

17 관리 체계와 법

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	정보보호 관리체계 프로세스를 이해하고 실제 컨설팅을 수행한 사례를 학습하면서 컨설턴트로서 컨설팅 실무 능력을 향상시킬 수 있는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 정보보호 관리체계 프로세스를 이해하고, 관련 법에 기초한 정보보호 관리체계 수립으로 역량 강화 · 각종 사례 속 정보보호 관리체계의 문제점 진단해 정보 자산의 위험을 분석해 효과적 관리 방안 도출할 수 있는 능력 향상
교육특징	<ul style="list-style-type: none"> · 정보보호 관리체계 기본 개념과 컨설턴트로서의 올바른 자질에 대해 이해 · 실제 컨설팅 수행하고 있는 강사의 현업 사례를 통한 상세 가이드 제시 · 컨설팅 단계별로 어떤 전략을 가지고 고객과 커뮤니케이션을 해야 하는지 상세 가이드 제시

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	컨설팅 실무를 학습하면서 고객과의 원활한 커뮤니케이션을 할 수 있도록 컨설턴트로서 전략을 세울 수 있도록 역량 강화에 도움
정보보호 관련 실무자	정보보호 관리체계를 이해하면서 실습을 통해 컨설팅의 프로세스를 자세히 배워 활용하는데 도움
취업준비생, 대학생	실제 컨설팅 사례를 토대로 정보보호 관리체계를 배우고 정보보호 컨설턴트가 되기 위해 필요한 자질이 무엇인지 배우는데 도움

4. 커리큘럼

주제	내용	
관리체계 이해	정보보호 관리체계의 이해	기본 개념의 이해
		정보보호 관리체계의 정의
		해외의 정보보호 관리체계 - 영국, 미국, 일본, 독일
		KISA-ISMS 인증제도
	정보보호 관리체계의 수립	정보보호 관리체계 관리모델
		정보보호 관리체계 수립 전략
		정보보호 관리체계 수립 절차
		사전 단계
		정보보호 정책수립 및 범위설정
		경영진 책임 및 조직구성
		위험관리
		정보보호 대책구현
		사후관리
개인정보보호 관리체계	개인정보보호 관리체계의 이해	정보보호 관리체계와 개인정보보호 관리체계
		개인정보의 정의
		개인정보의 가치
		개인정보 유출사고 Top 10
		개인정보 침해 경험
		개인정보보호 인식 정도
		개인정보 침해유형 (1차 피해)
		개인정보 침해유형 (2차 피해)
		개인정보보호법 주요내용
	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
		컨설팅 프로세스 개요
		Define Security requirement
		Define Scope
		Gap Analysis
		Define Vulnerability, Threat
		Risk Assessment
		Risk Treatment
		Master Plan

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	가상의 환경에서 발생한 침해사고에 대해 준비단계부터 분석 실전까지 실습하면서 앞으로 발생할 수 있는 침해사고에 대응을 할 수 있도록 준비할 수 있는 과정		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 공격자의 행위로 발생할 수 있는 다양한 이벤트 이해 · 침해사고 발생 시 필요한 도구를 준비하고 활용 · 침해사고 분석 시 타임라인을 도출하여 원인을 파악하고 재발방지
교육특징	<ul style="list-style-type: none"> · 앞으로 발생할 수 있는 다양한 사고를 분석할 수 있도록 관점과 역량 강화 · 사이버 범죄를 재구성한 가상환경을 실전과 같이 분석하고 보고서를 작성하여 실무 역량 강화 · 사고대응 분야에서 대두되고 있는 ATT&CK 프레임워크를 사고 분석에 접목해 공격자의 TTP 도출

3. 교육 대상

대상	주요 학습 포인트
침해사고 담당자	발생했거나 앞으로 발생할 수 있는 침해사고에 대해 기술적으로 분석하고 신고부터 대응까지 절차를 마련하는데 도움
직무순환 대상자	직무순환 등의 이유로 침해사고 분석의 기초부터 습득하고 싶을 경우 실습을 통해 능력 향상
취업준비생, 대학생	가상의 환경에서 직접 침해사고를 분석해보면서 침해사고 분석, 대응에 기초부터 습득하는데 도움

4. 커리큘럼

주제	내용	
침해사고대응 개요	Warm-Up	흔적 미리보기
		선수 지식 요약
	침해사고의 주요 원인	침해사고의 유형별 특징
		침해사고 사례
		실제 사건 속의 사고대응을 위한 키워드
	사이버 보안 위협 종류와 동향	
침해사고 대응 준비	사고대응체계 수립	침해사고대응절차 7단계
		침해사고대응 단계별 고려사항
	침해사고의 흔적들	주요 아티팩트 소개
침해사고 조사 및 분석 기법	침해사고 초동대응	운영체제 명령어 학습
		초동대응 스크립트 제작
		초기 데이터 수집/분석
	침해사고 흔적 분석	운영체제 로그 분석(Windows, Linux)
		웹, 브라우저 기록 수집 및 분석
		파일시스템 분석
		메모리 분석
	디스크 이미지 분석	
침해사고 분석 실전	응용실습	시나리오에 따른 침해사고 분석
		타임라인 기반 원인 파악 및 범죄의 재구성
		서버, 엔드포인트 관점의 침해사고분석 풀이
	보고서 작성	타임라인 도출
		침해지표 작성
		공격자의 TTP도출
		보고서 리뷰

19 Digital Forensics and Incident Response (DFIR)

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	고급
주제	분석 도구를 활용해 파일 복구 실습을 단계별로 수행하면서 침해사고 대응 분석을 해볼 수 있는 디지털 포렌식 통합과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 디지털 포렌식에 대한 개요, 유형, 절차 등 기본 지식 이해 · 실습을 통해 디지털 포렌식 분석 도구 활용 방법 습득 · 디지털 포렌식 업무의 완벽한 이해로 역량 강화
교육특징	<ul style="list-style-type: none"> · 디지털포렌식 기초 도구 사용법에 대해 실습 진행 · 초보자도 할 수 있는 파일 복구 실습 진행 · 단계별로 실습을 진행하면서 침해사고 분석 기법에 대해 학습

3. 교육 대상

대상	주요 학습 포인트
포렌식/침해사고 담당자	침해사고와 더불어 디지털 포렌식에 대한 통합과정이 필요한 담당자
정보보호 실무자	포렌식 분석을 입문부터 활용까지 상세하게 학습하면서 침해사고 대응 분석 능력 향상에 도움
취업준비생, 대학생	포렌식, 침해사고 대응 분석의 업무 수행하고자 취업을 준비하는데 도움

4. 커리큘럼

대단원	중단원	소단원
디지털 포렌식 개요	디지털 포렌식 개요	
	디지털 포렌식 유형	
	디지털 포렌식 절차	
디지털 포렌식 증거 수집	비활성 데이터 수집	디스크 이미징
		디스크 복사
		HDD (Hard Disk Drive)
	활성 데이터 수집	시스템 기본 정보 수집
		네트워크 정보 수집
		포트 별 서비스 정보 수집
		로컬 서비스 & 프로세스 정보 수집
	파일 시스템의 이해	파일 시스템의 구조
		MBR
	완전 삭제 및 복구에 대한 이해	NTFS 파일 생성, 삭제 및 복구
		빠른 포맷 vs 일반 포맷
		메타데이터 복구
		Metadata 기반 복구
Carving		
AVI, MP3 file Format		
DFIR	악성코드 분석 방식	
	무엇을 찾아야 할까?	
	Malware Life Cycle	
	무엇을 조사해야 할까?	
	어떤 것들을 조사해야 할까?	
	악성코드 탐지	
	윈도우 레지스트리	
	레지스트리 루트 키	
	Base Block (Hive Header)	
	Hive Bin Header	
	Key Cell (Root Cell 포함)	
	시스템에서 실행된 프로그램 조사	
	Root Cause 분석	
응용프로그램 사용 흔적 조사	웹 브라우저 흔적	
	구글 크롬	
	이메일 응용프로그램 흔적	
	워드 프로세서 흔적	
물리 메모리 정보 분석	물리 메모리 분석 개요	
	물리 메모리 수집 및 분석 개요	
	물리 메모리 정보 수집 및 분석 개요	물리 메모리 정보 수집 방법 물리 메모리 정보 분석 방법
모의침해 시나리오 포렌식 실습	디지털 포렌식 실습 1(PC 분석)	
	디지털 포렌식 실습 2(서버 분석)	
	디지털 포렌식 실습 3(메모리 분석)	

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	안전한 정보시스템 운영을 위해 기본적으로 알아야 하는 요소들과 이를 확인하는 취약점 진단의 수동 확인 방법, 스크립트를 활용한 확인 방법 등을 학습합니다.		
특이사항	· 본 과정은 취약점 진단 자산 중 서버만을 학습합니다.		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 기본적으로 알아야 하는 서버 및 장비 운용 핵심 지식 습득 · 진단 기준에 따른 주요 항목에 대한 수동 진단 방법을 통해 항목별 진단 목적 이해 · 셸/배치 스크립트 작성 방법을 학습하여, 효율적인 진단 방안 습득
교육특징	<ul style="list-style-type: none"> · 정보시스템 취약점 진단을 수행해야 하는 보안 직무 특화 · 가이드에 없는 실무에서 실제 정보시스템 취약점 진단 시 고려해야 하는 요소 전수 · 기획 수립 부터 결과 보고서 작성까지 정보시스템 취약점 진단의 모든 절차 경험

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	정확한 정보시스템에 대한 이해로 컨설팅 중 취약점 진단 업무 수행 능력 향상
정보보안 담당자	진단을 하는 방법은 알지만 가이드 내용만으로 조치가 어려운 상황에 도움이 될 수 있는 직무 능력 향상
정보보안 취업 준비생	정보시스템을 안전하게 운영하거나 진단하는 컨설팅 직무 역량 향상에 도움

4. 커리큘럼

주제	내용	
서버 또는 장비 관리를 위한 필수 기능 이해하기	리눅스 서버의 이해	리눅스 서버 셸의 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
주요정보통신기반시설 기준 항목별 수동 진단 방안	리눅스 서버 주요 항목 수동 진단	
	윈도우 서버 주요 항목 수동 진단	
셸/배치 스크립트 활용 취약점 진단	리눅스 서버 정보시스템 진단 수행하기	리눅스 셸 스크립트
		리눅스 서버 진단 with 셸 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	
	결과 파일 기반 보고서 작성 실습	

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	취약점 진단 실습, 모범사례를 통한 보고서 작성 요령 등을 학습하면서 웹 서버 대상으로 발생할 수 있는 취약점을 진단해보는 과정		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 웹 취약점 진단 실무 및 점검 항목에 대해 이해 · 웹 서버 점검 항목별 취약점 수동진단 수행 능력, 진단 이행 후 보고서 작성 업무를 수행
교육특징	<ul style="list-style-type: none"> · 실무 학습 기반으로 웹 서버 대상 취약점 점검을 수행 · 취약점의 존재 유무에 따른 웹 서버의 반응을 직접 확인 · 보고서 작성의 모범사례를 확인하고 작성 요령 학습

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	업무를 수행할 때 웹 취약점 수동 진단, 보고서 작성 능력 등 현업에 활용 가능한 능력 향상
정보보호 관련 실무자	점검 항목에 대한 이해부터 실습, 사례를 통한 전반적인 웹 취약점 진단 실무 역량 강화
취업준비생, 대학생	웹에서 발생할 수 있는 위협에 대한 이해 및 사례 학습으로 취업에 도움

4. 커리큘럼

주제	내용	
네트워크 기초 지식 이해	네트워크 보안 배경지식	OSI 7 Layer 모델의 이해
		TCP/IP 모델 계층 구조
	네트워크 장비	스위치/라우터 개요
		계층에 따른 네트워크 장비
	네트워크 위상에 따른 분류 및 특징	네트워크 분류
		토큰링
네트워크 구성 실습	패킷트레이서를 활용한 네트워크 구성	패킷트레이서 설치
		네트워크 망 구성도 실습
	GNS3 를 활용한 네트워크 구성	GNS3 설치 및 연동
		네트워크 망 구성도 실습
네트워크 기반 위협	네트워크 위협 이해	네트워크 위협 동향
		네트워크 위협 분류
	네트워크 위협 종류	근거리 네트워크 위협
		DoS 공격 이해
네트워크 기반 보안 솔루션 구축과 운영	보안 인프라 구성	보안 솔루션 종류
		인프라 구성도 분석
	방화벽 구축 실습	Untangle 구축 실습
		Pfsense 구축 실습
	보안솔루션 구축 실습	IPS 구축 실습 및 룰 제작
그 외 보안 솔루션 구축 실습		
네트워크 장비 관리를 위한 필수 기능 이해하기	네트워크 장비 운용	L2 스위치 운용 및 관리
		L3 스위치 운용 및 관리
	네트워크 장비 취약점 진단	정보시스템 취약점 진단 기준
		네트워크 장비 진단 항목
	네트워크 장비 보안 설정 실습	네트워크 장비 계정관리 보안 설정 실습
		네트워크 장비 접근관리 보안 설정 실습

1. 교육 개요

교육시간	09:00~18:00 (3일, 24시간)	교육수준	중급
주제	보안을 적용하지 않은 소프트웨어 개발이 야기할 수 있는 웹 공격 기법들을 이해하고, 보안 약점과 취약점을 제거하기 위한 개발 보안 방법론과 시큐어 코딩을 학습하는 과정		
특이사항	본 과정을 수강하기 위해서는 프로그래밍 기초 지식이 필요합니다.		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 소프트웨어 개발 방법론, 실무관점 적용방안의 이해 · 공격자가 자주 사용하는 웹 해킹 기법의 원리를 바탕으로 한 시큐어코딩 역량 강화 · 시큐어코딩 모범사례를 비즈니스 로직에 적용할 수 있는 방안 학습
교육특징	<ul style="list-style-type: none"> · 단순히 시큐어코딩 방법 적용이 아닌 공격의 원인을 파악하고, 그에 맞는 적절한 시큐어 코딩 방안 제시 · 실제 공격을 수행해보고, 시큐어코딩을 적용한 후 이행점검으로 시큐어코딩 적용의 유효성 검증 · 소스코드 보안약점을 효율적으로 진단할 수 있는 다양한 진단도구 활용

3. 교육 대상

대상	주요 학습 포인트
SW 개발자	보안약점의 명확한 기준과 보안대책을 통해 실질적인 시큐어코딩 적용 방법 학습
정보보안 담당자	보안약점을 최소화하기 위한 가장 효율적인 방법 이해
개발자 지망생	개발과 보안을 모두 할 수 있는 개발자로 취업 위한 발돋움
보안약점 진단 지망생	보안약점을 진단하고 대책을 제시하는 방법 이해

4. 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
파일처리		
데이터베이스 처리		
인증과 권한		
에러처리		
암호화		

23

파이썬을 활용한 취약점 진단 자동화 개발

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	고급
주제	주요정보통신기반시설 가이드를 기반으로 보다 더 정확한 취약점 진단 방법과 그에 따른 스크립트 제작 방법을 학습하여, 효율적으로 취약점 진단을 수행할 수 있도록 파이썬의 다양한 모듈을 활용해보고 자동화 모듈을 구현할 수 있도록 합니다.		
특이사항	본 과정은 파이썬의 기본 문법에 대해서는 알려드리지 않으니, 참고하시기 바랍니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 각 운영체제 별 취약점 진단을 위한 스크립트 작성 능력 강화 · 효율적인 취약점 진단을 위한 파이썬 활용 자동화 모듈 개발 능력 배양 · 가이드에 따른 항목 별 취약점 진단 해석 능력 강화
교육특징	<ul style="list-style-type: none"> · 실무 기반의 취약점 진단 방법 및 모범사례 공유 · 반복작업이 많은 취약점 진단 업무 상의 문제점을 파이썬 활용으로 해결할 수 있는 방안 학습

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	정보시스템 취약점 진단 업무를 수행할 때 복사, 붙여넣기 하는 단순 작업을 파이썬을 활용한 자동화 모듈 구현으로 업무의 효율성을 높일 수 있도록 학습
정보보안 담당자	정기적으로 취약점 진단이 필요한 항목이나 자산에 대해 자동화 모듈을 적용할 수 있는 방안 학습
취업준비생, 대학생	파이썬을 활용할 수 있다는 점이 취약점 진단 직무를 수행할 수 있는 차별화된 강점이 될 수 있도록 학습

4. 커리큘럼

주제	내용	
정보 시스템 진단 기준	정보시스템 취약점 진단	
	정보시스템 취약점 진단 기준 수립	주요 취약점 진단 기준 가이드라인 소개
		정보시스템 진단 자동화의 필요성
취약점 진단 스크립트	셸 스크립트(리눅스)	셸 스크립트 개요
		주요 사용 문법 및 명령어
		셸 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		
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

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	공격자가 주로 사용하는 웹 해킹 기법을 이해하고, 시나리오를 기반으로 실제와 같은 웹 사이트에 적용해보는 모의해킹 과정		
특이사항	<ul style="list-style-type: none"> · 리눅스와 SQL 구문에 대한 기본적인 지식이 필요합니다. · 중급 과정이긴 하나 초급자들도 이해하기 쉽도록 교육합니다. 		
참고사항	· 본 과정은 국민내일배움카드로 수강 가능하며, 이외 일반 교육생도 참여 가능합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 웹 사이트에서 자주 발견되는 취약점 진단 역량 강화 · 공격자가 자주 사용하는 웹 해킹 응용 기법 역량 강화 · 미흡한 방어기재를 우회할 수 있는 기법 습득 · 안전한 웹 사이트 운영을 위한 시큐어코딩 및 보안설정의 이해
교육특징	<ul style="list-style-type: none"> · 현재 모의해킹 컨설팅 실무를 수행하고 있는 강사의 노하우 전수 · [미션드리븐]이라는 자기주도적 학습 병행을 통한 교육 효과성 증대 · 실제 사례를 기반으로 한 시나리오 재구성을 통한 실습프로그램 · 내부 f-NGS Lab 연구진들의 최신 웹 해킹 실습컨텐츠로 구성

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	모의해킹 업무 수행 시 최신 공격기법과 취약점을 활용하는 역량 향상
정보보안 담당자	사내 웹 서비스에 모의해킹을 통한 보안 강화
취업준비생, 대학생	모의해킹 직무로 취업하고 싶은 취준생을 위한 기초 학습

4. 커리큘럼

주제	내용	
웹 모의해킹 기본이론	웹 모의해킹 방법론(컨설팅)	모의해킹과 불법해킹의 차이
		웹 모의해킹의 방법 및 목적
		웹 서비스 구조도의 이해
	웹 취약점 점검항목	점검항목이란?
		최신 OWASP TOP 10
주요정보통신기반시설 점검항목		
웹 개발 운영 환경 정보수집	정보수집	OSINT(open source intelligence)활용한 웹 정보수집
웹 주요 해킹기법	SQL 인젝션	심화된 SQL 인젝션 기법 적용방안
		스크립트 제작을 통한 DB 정보탈취
		다양한 우회기법 적용방안
		SQL 인젝션 시큐어코딩 적용방안
		DBMS 권한관련 보안설정 제안
	파일 업로드	단일 공격구문 웹쉘 제작
		다중 공격구문 웹쉘 제작
		이미지 형식의 웹쉘 제작
		심화된 파일 업로드 공격 적용방안
		도구를 활용한 업로드 실행경로 찾기
		웹쉘 실행을 통한 2차 공격 실행 방안 테스트
	파일 다운로드	위험한 형식 파일업로드 시큐어코딩
		악성파일 실행 보안설정 방안
		파일 다운로드 구현방식의 이해
		파일 다운로드 공격구문 및 우회기법 실습
		애플리케이션별 주요 설정파일 다운로드를 통한 2차 공격 테스트
		중요 파일 다운로드 및 암호화 해제 기법 실습
	SSRF	다운로드 무결성 검사 시큐어코딩
		SSRF 공격의 원인 및 위험성의 이해
		환경구성 및 취약점 진단(우회기법)
		환경구성 및 심화된 공격기법의 실습
	부적절한 인증 및 인가	화이트리스트 방식의 IP/Port 필터링을 이용한 접근제어
		부적절한 입력값 유효성 검증 시큐어코딩
		적절한 인증 없는 중요기능허용 공격실습
	WEB & WAS 취약점 공격	부적절한 인가 공격실습
		부적절한 인증 및 인가 시큐어코딩
	Log4Shell	Apache Struts2 최신 취약점 진단 및 자동화 공격(Python)
Oracle WebLogic 최신 취약점 진단 및 자동화 공격(Python)		
log4j를 활용한 어플리케이션 취약점 진단		
미션드리본	웹 주요 해킹기법 다른 사이트에 적용해보기	웹 사이트를 대상으로 CVE-2021-44228 취약점 공격
		실사이트(현재서비스종료) 대상 웹 주요 해킹기법 자가실습 강사 시연을 통한 Best Practice 해설 및 Q&A

25 최신 트렌드를 반영한 모의침투 테스트

1. 교육 개요

교육시간	09:00~18:00 (5일, 40시간)	교육수준	중급
주제	최근 발생했던 보안사고 및 공격자가 많이 사용하는 해킹기법에 대해 알아보고, 나아가 운영하는 정보시스템의 침해사고를 사전에 방지할 수 있는 모의해킹 과정		
특이사항	네트워크 기초 지식과 윈도우/리눅스 명령어에 대한 선수 학습이 필요합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 최근 발생했던 해킹사건을 바탕으로 모의침투 시나리오를 작성하는 방법 이해 · 다양한 시나리오를 바탕으로 대상별 공격방법에 대해 역량 강화
교육특징	<ul style="list-style-type: none"> · 실제와 같은 환경에 실제 발생했던 해킹사건을 모의침투 시나리오로 접목할 수 있는 실습 프로그램 구성 · IT 인프라에 전체적으로 발생할 수 있는 웹, 앱, PC 등 다양한 모의침투 시나리오 콘텐츠 실습

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	최신 공격 기법과 취약점에 대해 학습하여 모의해킹 실무를 수행할 때 활용하는 방안 학습
정보보안 담당자	기관 또는 사내에서 발생할 수 있는 보안사고 및 위협들에 대한 폭넓은 이해로 관리 체계 수립에 활용
취업준비생, 대학생	웹 포함 다양한 모의침투 방법 이해를 통해 모의해킹 직무에 대한 경험 및 포트폴리오로 강점 어필

4. 커리큘럼

주제	내용	
모의해킹 개요	모의해킹 기본이론	모의해킹 방법론
		취약점 진단 VS 모의해킹
	OSINT 를 활용한 취약점 정보수집	인터넷을 활용한 취약점 정보수집 기법
		오프라인 도구를 활용한 취약점 정보수집 기법
취약한 사이트를 이용한 내부망 침투	타깃형 워터링홀 공격 시나리오	목표조직 S/W(브라우저) 취약점 Exploit 코드 작성
		Exploit 서버 및 악성코드 저장소 구성
		사이트 취약점을 이용한 악성스크립트 삽입(난독화)
		감염된 내부 시스템 원격데스크톱(RDP) 터널링 공격
	SSRF 취약점 공격 시나리오	SSRF 취약점 진단
		유효한 내부 IP 확인
		내부망 중요정보 탈취
	Log4Shell 취약점 공격 시나리오	log4j 를 활용한 어플리케이션 취약점 진단
		웹 사이트를 대상으로 CVE-2021-44228 취약점 공격
	이동식 저장장치를 이용한 내부망 침투	Bad USB 를 활용한 악성코드 유포 공격
Bad USB 컴퓨터 연결 시 악성코드 감염		
감염된 내부 시스템 원격데스크톱(RDP) 터널링 공격		
모바일 애플리케이션 침투테스트	안드로이드 앱 취약점 진단	자주 발생하는 앱 주요 취약점 진단 실습
	안드로이드 앱 솔루션 우회	OS 변조 탐지 우회
		화면 강제실행에 의한 인증우회
		바이너리 분석 및 패킷 변조

26 모바일 앱 취약점 진단(Android)

1. 교육 개요

교육시간	09:00~18:00 (3일, 24시간)	교육수준	중급
주제	모바일 기기 사용의 증가와 함께 모바일 위협 또한 지속적으로 증가하고 있어, 보다 안전한 모바일 앱을 위한 취약점 진단과 대응방안을 배웁니다.		
특이사항	본 과정을 수강하기 위해서는 프로그래밍 기초 지식이 필요합니다.		

2. 교육목표 및 특징

교육목표	<ul style="list-style-type: none"> · 체크리스트 기반 모바일 앱 취약점 진단 수행 역량 강화 · 모바일 앱 위, 변조 방지 솔루션 우회기법 습득 · 발견된 모바일 앱 취약점에 대한 명확한 대응방안 학습
교육특징	<ul style="list-style-type: none"> · 모바일 앱에서 자주 발견되고 위험도가 높은 주요 취약점 진단 방법 학습 · 다양한 모바일 앱 진단 도구 활용을 통해 효율적 진단 방안 제시 · 모바일 앱 위, 변조 방지 솔루션 우회 기법을 통해, 진단 전문성 강화

3. 교육 대상

대상	주요 학습 포인트
정보보안 컨설턴트	웹 서비스 뿐만 아니라 모바일 앱도 진단할 수 있는 역량 향상
앱 서비스 운영,담당자	모바일 앱에 대한 자체적인 취약점 점검
취업준비생, 대학생	정보보안 취업에 앞서, 웹 뿐만 아닌 앱에 대한 취약점 역량 향상

4. 커리큘럼

주제	내용	
취약점 진단 기초	안드로이드 아키텍처	리눅스 커널
		라이브러리
		안드로이드 런타임
		디바이스 파일 디렉터리 구조
	취약점 진단 도구	정적분석도구 소개
		동적분석도구 소개
안드로이드 취약점 진단 환경	환경 구축	애몰레이터 설치
		Python(Anaconda) 설치
		Frida-Server 설치
취약점 진단 실무	취약점 진단 체크리스트	모바일 OWASP TOP 10 해설
		국내 모바일 앱 체크리스트 해설
	안드로이드 취약점 진단 실습	단말기 중요정보 저장금지
		메모리 중요정보 저장금지
		OS 변조 탐지
		소스코드 보호
		앱 위변조 방지
솔루션 우회 진단 실무	안드로이드 앱 솔루션 우회	OS 변조 탐지 우회
		화면 강제실행에 의한 인증우회
		바이너리 분석 및 패킷 변조