리버스 엔지니어링 및 악성코드 분석을 위한

Hex-Rays IDA Pro 실무 활용 교육

2일 교육과정

교육일정	교육내용	교육시간
1일차	**리버스 엔지니어링 개요** - 역공학, 리버스 엔지니어링이란? - 프로그램 생성 및 리버싱 분석 과정 이해 - 디어셈블러와 디컴파일 기술 이해	10:00 ~ 10:25
	IDA Pro 개요 - IDA Pro 소개 - 활용 범위 및 주요 기능 이해 - 시스템 요구 사항 - 버전 별 기능 차이점 이해	10:25 ~ 10:50
	IDA Pro 기본 사용법 - 분석 대상 파일 불러오기 - 데이터베이스 파일 사용 목적 이해 - 프로젝트 저장 방법	11:00 ~ 11:25
	IDA: Analysis Layout - 레이아웃 요소 별 설명 - Text/Graph View - View 전환 방법	11:25 ~ 11:50
	IDA: View Mode - PE 파일 구조 설명 - Function arguments - Execution flow arrows - 상호 참조 정보 (Cross-references) 분석 - 그래프 뷰 모드 사용 방법 (Graph View)	13:00 ~ 13:50
	IDA: Subsystems - Function window - Imports 뷰 데이터 분석 방법 - 정적 링크 라이브러리 vs 동적 링크 라이브러리 개념 설명 - Names 뷰 데이터 분석 방법 - 스트링 데이터 분석 방법 (Strings view)	14:00 – 14:50
	Reversing Crackme를 활용한 파일 분석 - IDA Pro를 활용하여 인증 번호 구조 분석 및 크래킹 실습 - 디버거 모드 사용 방법 설명 및 실습 - Code Patch 기능 활용 방법	15:00 – 15:50
	실제 악성코드 샘플 파일을 활용한 파일 분석 - 정보 유출 및 봇넷 (Botnet) 계열 악성코드 샘플 분석 실습 - 디컴파일 분석을 통한 코드 분석 방법 설명 및 실습 - IDA에서 악성코드 주요 행위 판별하는 방법 - 파일 생성 / 명령어 실행 / 자동 실행 등록 / 네트워크 연결 루틴 분석 실습	16:00 – 16:50
	패킹(Packing) 식별 및 구조 분석 - 패킹 (Packing) 기술 및 적용 목적 이해 - 패킹 적용 여부 식별 방법 - 패킹 해제 (MUP, Manual Unpacking) 실습	17:00 – 17:20
	패킹 해제 (MUP, Manual Unpacking) - UPX or ASPack (Others …) 압축 로직 분석 - 패킹 해제 (MUP, Manual Unpacking) 실습	17:20 – 17:40
	질문 & Review	18:00 ~

* 교육 시간 / 교육 내용 / 강의 순서는 교육센터 및 기관 사정에 따라 변동될 수 있으니 참고 바랍니다.

교육일정	교육내용	교육시간
2일차	**IDAPython: Python plugin for Interactive Disassembler** - IDAPython 소개 및 설치 - IDAPython 활용 방안 소개 - IDAPython 주요 API 설명	10:00 ~ 10:25
	IDAPython을 활용한 데이터 암호화 / 난독화 로직 분석 - XOR 암호화 동작 방식 이해 - IDAPython 기반 XOR 디코딩 스크립트 작성 실습	10:25 ~ 10:50
	ELF (Executable and Linkable Format) 파일 분석 – 1 - ELF 파일 포맷 구조 이해 (Headers and Sections)	11:00 ~ 11:25
	ELF (Executable and Linkable Format) 파일 분석 – 2 - IDA Pro를 활용한 ELF Crackme 대상 프로그램 리버싱 실습 - Linux Remote Debugger 사용법 설명 및 실습	11:25 ~ 11:50
	CVE (Common Vulnerabilities and Exposures) 취약점 분석 실습 – 1 - CVE 취약점 이해 및 등록번호 해석 방법 - CVE 취약점 등록 절차 - 취약점 공격 유형 설명	13:00 ~ 13:50
	CVE (Common Vulnerabilities and Exposures) 취약점 분석 실습 – 2 - 실제 등록 된 CVE 취약점을 기반으로 한 공격 방식 이해 - IDA Pro를 활용한 취약 대상 바이너리 분석 - 공격 백터 (Attack Vector) 판별 및 상세 분석 실습	14:00 – 14:50
	Process Injection 공격 기법 - 악성코드의 Process Injection 공격 기법 이해 - Process Injection 공격에 효과적인 대응 방안 설명	15:00 – 15:50
	IDA를 활용한 메모리 덤프 파일 분석 - Volatility 소개 및 설치 - Volatility를 활용한 프로세스 메모리 덤프 방법 설명 및 실습 - IDA를 활용한 덤프 파일 분석 방법 설명 및 실습	16:00 – 16:50
	IDA Integration: 플러그인 연동 분석 기술 - 악성코드 분석 및 프로그램 리버싱에 활용 가능한 IDA Plugin 종류 설명 - Hex-rays Plugin Contest	17:00 – 17:20
	IDA Integration: 플러그인 연동 분석 기술 - 타사 전문 분석 기술들과의 IDA Pro 연동 방법 설명 및 실습 (Joe Sandbox or Intezer)	17:20 – 17:40
	질문 & Review	18:00 ~

* 교육 시간 / 교육 내용 / 강의 순서는 교육센터 및 기관 사정에 따라 변동될 수 있으니 참고 바랍니다.