2017년 여름방학 정보보안 특강

안전한 인터넷 행복한 미래

일자	시간	내용	비고
1일차 (해킹기법) 7월 17일	10:00 ~ 11:00	○웹의 구조 ○웹취약점의 발생 원리 ○웹 해킹기법의 종류	
	11:00 ~ 13:00	○File Upload/Download 공격 - 기본원리 및 실습 - Advanced File Upload 공격 ○SQL-Injection 공격 - 기본원리 및 실습 - Advanced SQL-Injection 공격 ○XSS & CSRF 공격 - 기본원리 및 실습 - Advanced CSRF 공격	
	14:00 ~ 15:00	○메모리 구조와 작동 매커니즘 ○시스템 취약점의 발생 원리 ○시스템 해킹기법의 종류	
	15:00 ~ 18:00	○Buffer Overflow 공격 - 기본원리 및 Shell Code 제작 실습 - Local Buffer Overflow 공격 실습 - Remote Buffer Overflow 공격 실습 ○Advanced Buffer Overflow 공격 - RTL, ROP 등 고급 공격기법	
2일차 (사고분석) 7월 18일	10:00 ~ 11:00	○로그파일 분석(1) - 로그파일의 종류 - 각 로그파일의 필드 분석	
	11:00 ~ 12:00	○로그파일 분석(2) - 공격 유형별 로그파일 분석 - 각 로그파일 분석을 통한 공격자 행위 추출 - 로그파일 분석을 통한 공격자 행위 추출 실습	
	13:00 ~ 16:00	○해킹 피해 시스템 분석 - 피해 시스템 초동 분석 - 휘발성/비휘발성 데이터 분석 - 피해 시스템 분서을 통한 공격자 행위 재구성	
	16:00 ~ 18:00	○파일 시스템 분석과 개별 파일 복구 - 파일 삭제와 복구(리커버링, 카빙) - 파일 복구를 위한 주요파일 구조 분석 - 주요파일 시그니처를 활용한 파일 복구(카빙)	