SK쉴더스 루키즈 13기 5분대기조 프로젝트 계획서

프로젝트명	APT 공격 시나리오 : 침해사고분석 및 포렌식을 통한 공격자 TTP 프로파일링
프로젝트 목적	북한 해킹 그룹 프로파일링을 위한 하나센터 개인정보 유출 시나리오 재현과 메모리/디스크 포렌식 기법을 활용한 악성코드 및 침해사고 분석을 목표로 한다.
프로젝트 개요	악성코드에 감염되거나 외부의 침입이 발생한 시스템에서 침해지표를 수집하고 유입경로 및 추가 이동경로를 확인할 수 있는 가상 시스템을 구축하고 침해사고 발생시 사고 대응 증거 수집 및 분석을 진행한다.
세부 계획	1. 침해사고의 이해 - 침해사고 지표(Forensic Artifact, IoC) - 침해사고 전술, 기술, 절차(TTP) - Cyber Killchain 및 MiTRE ATT&CK Framework 2. 공격 유형별 시나리오 및 공격 tool 준비/공격 수행 - 피해 대상 가상 시스템 구축 - CVE, Exploit 이해 및 구현 - 시나리오 기반 공격 수행 3. 침해사고 대응 - 휘발성 데이터 수집 및 분석 - 비휘발성 데이터 수집 및 분석 - 침해사고 지표 수집 및 분석 4. 각종 대응 절차 및 분석/대응 보고서 - ATT&CK Framework 활용 - TTP 확인 - 공격자 Profiling 적용 5. 습득 기술 - 침해지표 및 포렌식 아티팩트 - 사고 대응 도구 사용법 - 해킹 시나리오 - 시스템 취약점 및 해킹 기법 - 분석 보고서 작성 기술 - 휘발성/비휘발성 데이터 수집/분석 기술 - 가상시스템 활용 - 침해지표 수집/분석 기술
프로젝트 산출물	- 침해사고 분석 보고서 - 침해사고 기술 보고서 - 공격 시나리오 절차서 - NIST CFReDS Data Leakage Case Report

	- 2018 VAC Analysis Report - 공격 시연 동영상 - 시스템 구축 보고서 - 취약점 분석 보고서 - 최종 발표 PPT