사이버 킬체인 분석 보고서

1. **사이버 킬체인이란?**

   사이버 킬체인(Cyber Kill Chain)은 사이버 공격을 단계별로 분석하고 방어 전략을 수립하기 위한 모델입니다. 원래는 군사 작전 개념에서 유래했으며 Lockheed Martin이 2011년에 사이버 보안에 적용하면서 널리 알려졌습니다.

   이 모델은 공격자가 목표 시스템을 침투하고 피해를 입히기까지의 과정을 8단계로 나누어 설명합니다.

2. **사이버 킬체인의 8단계**

단계	설명
정찰 (Reconnaissance)	공격자가 목표에 대한 정보를 수집 (도메인, 이메일, 시스템, 정보 등)
무기화 (Weaponization)	수집한 정보를 바탕으로 악성코드, 익스플로잇 등을 제작
전달 (Delivery)	이메일, 웹사이트, USB 등 다양한 경로로 악성코드를 전달
익스플로잇 (Exploitation)	시스템의 취약점을 이용해 악성코드를 실행
설치 (Installation)	악성코드가 시스템에 설치되어 지속적인 접근 가능
명령 및 제어 (Command and Control)	외부 서버와 연결해 공격자가 시스템을 원격 제어
행동 개시 (Actions on Objectives)	데이터 탈취, 시스템 파괴 등 공격 목적 수행
수익 창출 (Exfiltration)	탈취한 정보를 외부로 반출하거나 금전적 이득을 추구

3. **사이버 킬체인의 활용 목적**

- 공격자의 행동을 예측하고 차단할 수 있도록 보안팀이 각 단계에서 대응 전략을 수립
- 보안 솔루션 배치 및 로그 분석에 활용
- 조직의 보안 취약점 파악 및 우선순위 설정에 도움

4. **모의해킹과 사이버 킬체인의 관계**

모의해킹은 사이버 킬체인의 각 단계를 공격자 시점에서 재현함으로써 조직의 보안 대응력과 취약점 노출 수준을 실질적으로 평가합니다. 특히 킬체인 후반부(설치~수익 창출)는 탐지 회피, 권한 상승, 데이터 유출 등 고난도 공격 시나리오를 포함하므로 보안 운영팀의 대응 역량을 검증하는데 매우 중요합니다.

모의해킹은 단순히 취약점을 찾는 기술적 작업을 넘어 사이버 킬체인의 흐름을 따라가며 실제 공격자의 사고방식을 체험하는 과정입니다. 특히 킬체인의 각 단계가 모의해킹의 전략 수립에 직접적인 영향을 주기 때문에 이 둘은 단순한 연관성을 넘어서 상호보완적인 관계로 보여집니다.

예를 들어, 정찰 단계에서 수집된 정보가 무기화와 전달 방식에 영향을 주고 이후의 익스플로잇과 설치 단계는 조직의 보안 솔루션의 실효성을 검증하는데 핵심적인 역할을 합니다. 따라서 모의해킹이 킬체인을 기반으로 설계될 때 단순한 기술테스트를 넘어 조직의 보안 대응 체계 전반을 평가할 수 있는 강력한 도구가 될 수 있습니다.

다만 실제 공격자는 킬체인의 순서를 유연하게 넘나들거나 생략하기도 하기 때문에 모의해킹 역시 정형화된 킬체인 모델에만 의존하기보다는 유연한 사고와 시나리오 기반 접근이 병행되어야 한다고 생각합니다.

사이버 킬체인 단계	모의해킹 활동	목적 및 기대 효과
정찰	- OSINT(Open Source Intelligence) 활용 - 도메인 정보, IP, 이메일 주소, 직원 SNS 분석 - 서드파티 정보 수집	- 공격 표면 식별 - 취약한 자산 탐색 - 사회공학 기반 공격 준비
무기화	- 수집한 정보를 기반으로 악성 페이로드 제작	- 목표 환경에 맞는 공격 도구 준비

	- 취약점에 맞는 익스플로잇 코드 구성 - 피싱용 문서, 악성 링크 생성	- 탐지 우회 기법 적용
전달	- 피싱 이메일 발송 - 악성 URL 삽입된 문서 전달 - USB 등 물리적 매체 활용	- 보안 인식 수준 평가 - 이메일 필터링 및 사용자 대응 테스트
익스플로잇	- 웹 취약점 공격(SQL Injection, XSS 등) - 취약한 서비스에 대한 익스플로잇 실행 - 인증 우회 시도	- 시스템 침투 가능성 확인 - 취약점의 실제 영향도 검증
설치	- 백도어 설치 - 리버스 셸 연결 - 지속적 접근을 위한 악성코드 배포	- 지속적 침투 가능성 확인 - EDR·백신 탐지 여부 테스트
명령 및 제어	- C2 서버 구축 및 연결 - 트래픽 암호화 및 은닉 - 명령 전송 및 데이터 수집	- 네트워크 모니터링 회피 여부 확인 - 방화벽 및 IDS 대응력 평가
행동 개시	- 권한 상승(Lateral Movement) - 민감 정보 접근 및 수집 - 시스템 제어 및 데이터 조작	- 핵심 자산 보호 수준 평가 - 내부 보안 정책 검증
수익 창출	- 데이터 외부 전송 시도 - 클라우드·FTP·이메일 통한 유출 테스트 - 로그 삭제 및 흔적 은폐	- DLP(Data Loss Preventation) 효과성 검증 - 사고 대응 체계 점검