사이버 킬체인과 모의해킹의 관계 조사 보고서

1. 사이버 킬체인(Cyber Kill Chain)의 이해

사이버 킬체인은 록히드 마틴(Lockheed Martin)에서 제시한 사이버 공격 분석 프레임워크로, 공격자가 목표를 침투하고 피해를 주기까지의 과정을 **7단계**로 구분하여 설명합니다. 각 단계에서 방어자는 공격을 조기에 탐지하고 차단할 수 있는 기회를 얻게 됩니다.

사이버 킬체인 7단계

1. **정찰(Reconnaissance)**
   목표 시스템, 네트워크, 직원 등에 대한 정보 수집 단계
   예: OSINT(오픈소스 정보수집), 포트 스캐닝, SNS 정보 분석
2. **무기화(Weaponization)**
   악성 코드, 취약점 공격 도구를 제작 및 준비
   예: 익스플로잇 코드 작성, 악성 매크로 포함 문서 생성
3. **전달(Delivery)**
   공격 도구를 대상에게 전달
   예: 피싱 메일 발송, 악성 웹사이트 접속 유도
4. **취약점 악용(Exploitation)**
   시스템 취약점을 이용해 악성 코드 실행
   예: 브라우저 취약점, 문서 취약점
5. **설치(Installation)**
   악성 프로그램을 설치하여 지속적 접근 권한 확보
   예: 백도어 설치, 원격 제어 툴 배포
6. **명령 및 제어(Command & Control)**
   C2 서버와 통신하여 명령을 주고받음
   예: HTTP, HTTPS, DNS 터널링을 통한 통신
7. **목표 달성(Act on Objectives)**
   데이터 탈취, 시스템 파괴, 금전적 이득 등 공격 목적 수행
   예: 데이터 유출, 랜섬웨어 암호화

2. 모의해킹(Penetration Testing)과의 관계

모의해킹은 실제 공격자의 관점에서 시스템의 취약점을 찾아내고 보안 수준을 진단하는 보안 점검 방법입니다.

사이버 킬체인과의 관계는 다음과 같습니다.

- **정찰 단계**→ 모의해킹의 정보수집 단계와 동일
- **무기화~전달**→ 취약점 기반 공격 코드 제작 및 전달 실습
- **악용~설치**→ 시스템 침투 및 지속성 확보 실험
- **C2~목표 달성**→ 권한 상승, 데이터 접근, 내부 확산 시뮬레이션

즉, **모의해킹은 사이버 킬체인 단계를 실제 환경에서 재현**하여, 각 단계에서의 취약점과 방어 체계를 검증하는 역할을 합니다.

3. 개인 의견

사이버 킬체인은 방어 측면뿐 아니라 공격자의 사고방식을 이해하는데 매우 유용합니다.
모의해킹에 이를 적용하면, 단순 취약점 발견을 넘어 **공격 전체 시나리오 기반 보안 점검**이 가능하다고 생각합니다.
다만, 모든 단계를 실환경에서 실행하기 어려울 수 있으므로, 민감 데이터 유출 단계는 시뮬레이션 형태로 대체하는 등 법적·윤리적 절차를 준수해야 합니다.

참고자료
https://www.dailysecu.com/news/articleView.html?idxno=112743
https://itforest.net/solution01.php
https://anto.online/unveiling-network-weaknesses-penetration-testing-vs-the-cyber-kill

-chain/
https://www.cobalt.io/blog/cyber-kill-chain-understanding-how-cyberattacks-happen