정보보안개론_최종정리

↗ 과목(Class)	정보보안개론
≔ 키워드	

📚 Subject: 정보보안개론 (Information Security Basics)

> 학습 개요
>
> - **기간:** 2025.03 ~ 2025.06 (총 18주, 60시간)
> - **교재:** 자체 강의록(이론 중심), 2025 알기사 정보보안기사(심화 학습)
> - **성취:** 정보보안기사 및 정보보안산업기사 필기 합격 (2025.09), 정보보안기사 실기 응시 완료 (결과 대기 중)
> - **학습 목표:** 정보보안의 핵심 개념(CIA, 암호학, 접근통제) 정립 및 실무 용어(영어) 습득

🔑 상세 학습 내용 (Technical Concepts & Keywords)

1. 보안 거버넌스 및 핵심 목표 (Security Governance)

보안의 기술적 조치 이전에 '보호의 목적'을 정의하는 논리적 기반을 확립함.

- **정보보호 5대 목표 (CIA + 2):**
  - **기밀성 (Confidentiality):** 인가된 사용자만 정보에 접근 가능 (비인가자 열람 불가).
  - **무결성 (Integrity):** 비인가된 위·변조 방지 (변경 권한 제한).
  - **가용성 (Availability):** 인가된 사용자가 필요할 때 언제든 서비스 이용 가능 (DoS 방지).
  - **인증 (Authentication):** 사용자의 신원 및 출처의 신뢰성 확인.
  - **책임추적성 (Accountability):** 개체의 행동을 유일하게 추적하여 부인 방지(Non-repudiation) 구현.
- **위협 관리 (Risk Management):**
  - **위협(Threat) vs 위험(Risk):** 보안에 해를 끼치는 잠재적 존재(해커, 악성코드)인 **위협**과, 취약점을 통해 실제 피해가 발생할 **가능성 및 영향도**인 **위험**의 개념 명확히 구분.

2. 암호학 (Cryptography) - 이론과 실무 연결

정보보안기사 시험 핵심 영역이자 데이터 보호 기술의 근간 이해.

- **암호 알고리즘 비교:**
  - **대칭키 암호 (Symmetric Key):** 암호화/복호화 키가 동일하며 속도가 빠름(AES, DES). 대량 데이터 처리에 적합하나 키 분배 문제 존재.
  - **공개키 암호 (Public Key):** 키가 분리(공개키/개인키)되어 키 공유 문제 해결 및 인증/서명에 활용(RSA, ECC). 속도가 느린 단점 존재.
  - **하이브리드 암호 (Hybrid System):** 대칭키의 속도와 공개키의 보안성을 결합하여 실무에서 사용하는 방식 학습.
- **해시 함수 (Hash Function):**
  - **특성: 단방향성(One-way)**, **고정 길이 출력**, **충돌 회피성(Collision Resistance)**을 가지며, 패스워드 저장 및 무결성 검증에 사용 (MD5, SHA-256 등).
- **디지털 서명 (Digital Signature):**
  - **원리:** 개인키로 서명(도장)하고 공개키로 검증(확인)하여 **'내가 보냈음'을 증명**하고 내용 변조를 확인하는 메커니즘.
- **기타 암호 기술:**
  - **OTP (One Time Password):** 매번 새로운 값을 생성하여 재사용 공격을 방지하는 고보안 인증 수단.
  - **디피-헬만 (Diffie-Hellman):** 비대칭 암호 기반의 안전한 키 교환 프로토콜.

3. 시스템 위협 및 은닉 기법 (Threats & Attacks)

공격 기법의 특징을 이해하고 이를 탐지/방어하기 위한 이론적 토대 마련.

- **악성코드 분류 (Malware Types):**
  - **바이러스 (Virus):** 파일에 감염되어 자기 복제하며 사용자 실행 필요.
  - **웜 (Worm):** 네트워크를 통해 스스로 전파되며 시스템 자원 소모.
  - **트로이목마 (Trojan):** 정상 프로그램으로 위장하여 백도어 설치 등 악성 행위 수행.
- **사회공학적 공격:**
  - **피싱(Phishing) vs 파밍(Farming):** 가짜 메일/사이트를 통한 정보 탈취(Phishing)와 DNS 조작 등을 통한 가짜 사이트 유도(Farming) 구분.
- **은닉 채널 및 유출 기법:**

- **커버트 채널 (Covert Channel):** 보안 정책을 우회하여 타이밍이나 스토리지를 조작해 은밀하게 정보를 유출하는 기법.
- **스테가노그래피 (Steganography):** 이미지나 오디오 파일 속에 메시지를 숨겨 존재 자체를 은폐하는 기술.

4. 보안 통제 및 대응 (Security Controls)

국제 표준(CISSP 등) 기반의 시점별 통제 유형 학습.

- **통제 유형 (Control Types):**
  - **예방(Preventive):** 위협을 사전에 차단.
  - **탐지(Detective):** 발생한 위협을 식별.
  - **교정(Corrective):** 사고 발생 후 즉시 수정.
  - **복구(Recovery):** 시스템을 원상 복구.
  - **억제(Deterrent) & 보완(Compensative):** 공격 의지 저하 및 대안 제시.

💡 학습 회고 (Learning Reflection)

> "비전공자로서 처음 접한 보안 이론은 방대했지만, *'보안은 결국 효율을 다루는 학문'*이라는 강사님의 말씀에 집중하며 흥미를 느꼈습니다. 복잡한 암호학 수식보다는 *'대칭키와 공개키가 왜 분리되었고, 실제 전자서명에는 어떻게 응용되는가'*와 같은 구조적 이해에 주력했습니다.
> Zero Trust, 커버트 채널이나 스테가노그래피 같은 은닉 기법을 배우며, 눈에 보이는 보안 시스템뿐만 아니라 보이지 않는 위협까지 고려해야 함을 깨달았습니다. 짧은 기간이었지만 정보보안기사 자격증 도전을 병행하며, 보안을 수행하는 실무자로서 갖춰야 할 이론적 기초와 'Why'를 고민하는 태도를 다질 수 있었습니다."