1016일 정보보안 정리

1.

정보보안의 대상 – 물건이나 오프라인 사람의 관리 또한 정보보안의 대상이다.

정보보안의 3대 요소 – 기밀성,가용성, 무결성이란 무엇인가. – 옳고 그름을 파악해야 한다. (정의 개념의 옳고 그름) -> 6대 목표로 확산할 수 있다.

보안의 취약점 – 소프트웨어 뿐만 아니라 종류가 다양하다.

해킹 – 악성 프로그램 종류 (이런 게 있었다.), 사전적 의미

사회공학의 단어의 뜻과 의미 – 시스템에 접근할 수 있는 사람을 공격하는 것.

2. 정보보안의 역사

중요한 요소들은 객관식

– 역사 중에서 틀린 부분 찾기 (외울 필요는 X / 왜 점점 더 해킹이 심해지는 가 => 기술 발달로 인해서 보안 신경쓴다. 근데 왜 더 늘어날까 ? => **대리전** – 전쟁 대신 선택한 것이 **‘해킹’**)

사이버 테러 – 스턱스넷

3. 시스템 보안 – 시스템이란 무엇인가, **접근 제어** (**세션의미와 보호하는 방법**, 권한 관리 등 6가지)

- **접근제어의 개념 (주체와 객체 사이의 흐름) -> 3A가 무엇이지 쓸 수 있어야 한다. (예시와 개념을 알기.) -> 뭐하는 지**

- 운영체제 등 계정 관리를 어떻게 하는지. (권한관리)

- 접근 제어의 원칙의 옮고 그름을 판단. – 각각의 단어가 무슨 뜻인지.

- 접근 제어 모델 -> 무엇이 있는지. 각 모델의 개념이 무엇인지.

- 모바일 보안 -> 앱이 시스템을 건들지 못하게 하기 위해서 만든 구조 => **샌드박스 (커널에 접근하지 못하도록)**

시스템 보안 (2)

- 프로세스와 커널의 구조를 알기

- 운영체제에서 커널이 뭐하는지

- 보안 커널이 뭔지.

- 참조 모니터란 무엇인지.

- TCB가 무엇인지.

- TCB와 참조 모니터의 관계 (그림)

- 그림을 보고 판단할 수 있어야 한다. 무엇인지.

- SELinux가 뭔지.

- 원도우 보안 하부 구조의 이름 -> 6개 (그림)

- TPM이란 무엇인가. 왜 쓰는가 ?

- **3-워에 핸드셰이킹 – 연결과정과 해제과정이 어떻게 이루어져 있는지.**

- IPv4, 6는 공부할 필요는 없다.

- DNS의 개념

- Dos, DDos의 각각의 공격의 특징. -> 설명을 주고, 이게 무슨 공격이냐 ???

- 스니핑과 스포핑

- 방화벽의 종류 파일 -> 단어의 의미 (O,x 문제, 객관식)

웹과 HTTP의 이해

- get, post

- 프록시가 무엇인지.

- robot.txt

- SQL injection, XSS 공격의 서로간의 비교 차이점.

- 취약한 점근제어 -> 왜 위험한가.

- CSRF 살펴보기

- 네트워크 방어 장비 등 옳고 그름

- IBS, IDS가 무엇인지

- 라우팅 프로토콜 = 단어 위주로.

- 생체인식