

1과목 : 과목 구분 없음

1. 2009년 Moxie Marlinspike가 제안한 공격 방식이며, 중간자 공격을 통해 사용자와 서버 사이의 HTTPS 통신을 HTTP로 변경해서 비밀번호 등을 탈취하는 공격 방식으로 가장 옳은 것은?

- ① SSL stripping ② BEAST attack
③ CRIME attack ④ Heartbleed

2. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

- ① 게시판 등의 웹페이지에 악의적인 코드 삽입이 가능하다는 취약점이 있다.
② 공격 코드를 삽입하는 부분에 따라 저장 XSS 방식과 반사 XSS 방식이 있다.
③ 악성코드가 실행되면서 서버의 정보를 유출하게 된다.
④ Javascript, VBScript, HTML 등이 사용될 수 있다.

3. <보기>에서 설명하는 보안 목적으로 가장 옳은 것은?

정보가 허가되지 않은 방식으로 바뀌지 않는 성질

- ① 무결성(Integrity) ② 가용성(Availability)
③ 인가(Authorization) ④ 기밀성(Confidentiality)

4. 「개인정보 보호법」상 용어 정의로 가장 옳지 않은 것은?

- ① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
② 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
④ 개인정보관리자: 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

5. Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

- ① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

6. 디지털 서명에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

ㄱ. 디지털 서명은 부인방지를 위해 사용할 수 있다.
ㄴ. 디지털 서명 생성에는 개인키를 사용하고 디지털 서명 검증에는 공개키를 사용한다.
ㄷ. 해시 함수와 공개키 암호를 사용하여 생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.

- ① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

7. 분산반사 서비스 거부(DRDoS) 공격의 특징으로 가장 옳지 않은 것은?

- ① TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한다.
② 공격자의 추적이 매우 어려운 공격이다.
③ 악성 봇의 감염을 통한 공격이다.
④ 출발지 IP 주소를 위조하는 공격이다.

8. 침입탐지시스템의 비정상행위 탐지 방법에 대한 설명으로 가장 옳지 않은 것은?

- ① 정상적인 행동을 기준으로 하여 여기서 벗어나는 것을 비정상적으로 판단한다.
② 정량적인 분석, 통계적인 분석 등을 사용한다.
③ 오람률이 높으며 수집된 다양한 정보를 분석하는 데 많은 학습 시간이 소요된다.
④ 알려진 공격에 대한 정보 수집이 어려우며, 새로운 취약성 정보를 패턴화하여 지식데이터베이스로 유지 및 관리하기가 쉽지 않다.

9. 메모리 변조 공격을 방지하기 위한 기술 중 하나로, 프로세스의 중요 데이터 영역의 주소를 임의로 재배치하여 공격자가 공격대상 주소를 예측하기 어렵게 하는 방식으로 가장 옳은 것은?

- ① canary ② ASLR
③ no-execute ④ Buffer overflow

10. 퍼징(fuzzing)에 대한 설명으로 가장 옳은 것은?

- ① 사용자를 속여서 사용자의 비밀정보를 획득하는 방법이다.
② 실행코드를 난독화하여 안전하게 보호하는 방법이다.
③ 소프트웨어 테스트 방법 중 하나로 난수를 발생시켜서 대상 시스템에 대한 결함이 발생하는 입력을 주입하는 방법이다.
④ 소스 코드를 분석하는 정적 분석 방법이다.

11. 보안 측면에서 민감한 암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고자 나온 개념으로, TCG 컨소시엄에 의해 작성된 표준은?

- ① TPM ② TLS
③ TTP ④ TGT

12. 사회 공학적 공격 방법에 해당하지 않는 것은?

- ① 피싱 ② 파밍
③ 스미싱 ④ 생일 공격

13. 접근 제어 방식 중, 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산시스템 환경에서 많이 사용되는 방식은?

- ① 접근 제어 행렬(Access Control Matrix)
② 접근 가능 목록(Capability List)
③ 접근 제어 목록(Access Control List)
④ 방화벽(Firewall)

14. WPA2를 공격하기 위한 방식으로, WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격 방식으로 가장 옳은 것은?

- ① KRACK ② Ping of Death

- ③ Smurf ④ Slowloris

15. 오일러 함수 $\phi(\)$ 를 이용해 정수 $n=15$ 에 대한 $\phi(n)$ 을 구한 값으로 옳은 것은? (단, 여기서 오일러 함수 $\phi(\)$ 는 RSA 암호 알고리즘에 사용되는 함수이다.)

- ① 1 ② 5
③ 8 ④ 14

16. 능동적 공격으로 가장 옳지 않은 것은?

- ① 재전송 ② 트래픽 분석
③ 신분위장 ④ 메시지 변조

17. 무선랜 보안에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

ㄱ. WEP는 RC4 암호 알고리즘을 사용한다.
ㄴ. WPA는 AES 암호 알고리즘을 사용한다.
ㄷ. WPA2는 EAP 인증 프로토콜을 사용한다.

- ① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

18. BLP(Bell & La Padula) 모델에 대한 설명으로 가장 옳지 않은 것은?

- ① 다단계 등급 보안(Multi Level Security) 정책에 근간을 둔 모델이다.
② 기밀성을 강조한 모델이다.
③ 수학적 모델이다.
④ 상업용 보안구조 요구사항을 충족하는 범용 모델이다.

19. <보기>와 관련된 데이터베이스 보안 요구 사항으로 가장 옳은 것은?

서로 다른 트랜잭션이 동일한 데이터 항목에 동시적으로 접근하여도 데이터의 일관성이 손상되지 않도록 하기 위해서는 로킹(locking) 기법 등과 같은 병행 수행 제어 기법 등이 사용되어야 한다.

- ① 데이터 기밀성 ② 추론 방지
③ 의미적 무결성 ④ 운영적 무결성

20. RSA에 대한 설명으로 가장 옳지 않은 것은?

- ① AES에 비하여 암호, 복호화 속도가 느리다.
② 키 길이가 길어지면 암호화 및 복호화 속도도 느려진다.
③ 키 생성에 사용되는 서로 다른 두 소수(p , q)의 길이가 길어질수록 개인키의 안전성은 향상된다.
④ 중간자(man-in-the-middle) 공격으로부터 안전하기 위해서는 2,048비트 이상의 공개키를 사용하면 된다.

전자문제집 CBT PC 버전 : www.comcbt.com
전자문제집 CBT 모바일 버전 : m.comcbt.com
기출문제 및 해설집 다운로드 : www.comcbt.com/x

전자문제집 CBT란?

종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.

PC 버전 및 모바일 버전 완벽 연동
교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

1	2	3	4	5	6	7	8	9	10
①	③	①	④	③	①	③	④	②	③
11	12	13	14	15	16	17	18	19	20
①	④	②	①	③	②	②	④	④	④