

1과목 : 과목 구분 없음

1. 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯하여 예방, 피해 복구 등의 임무를 수행하는 조직은?

① CISO                      ② CERT  
③ CPPG                     ④ CPO

2. OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

개인정보 침해, 누설, 도용을 방지하기 위한 물리적·조직적·기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)  
② 이용 제한의 원칙(Use Limitation Principle)  
③ 정보 정확성의 원칙(Data Quality Principle)  
④ 안전성 확보의 원칙(Security Safeguards Principle)

3. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은?

① CSRF 공격                      ② SQL 삽입 공격  
③ 취약한 인증 및 세션 공격      ④ DoS 공격

4. 스테가노그래피에 대한 설명으로 옳지 않은 것은?

① 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.  
② 원데이터에 비해 더 많은 정보의 은닉이 가능하므로 암호화보다 공간효율성이 높다.  
③ 텍스트·이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.  
④ 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법이 있다.

5. 다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은?

① L2TP                      ② SYN 플러딩  
③ PPTP                     ④ ARP 스푸핑

6. 해시 함수의 충돌에 대한 설명으로 옳은 것은?

① 동일한 해시 함수가 동일한 입력 값에 대해 다른 출력 값을 내는 것을 의미한다.  
② 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.  
③ 서로 다른 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.  
④ 해시 함수의 입력 메시지가 길어짐에 따라 생성되는 해시 값이 길어지는 것을 의미한다.

7. 암호화 기법들에 대한 설명으로 옳지 않은 것은?

① Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.  
② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.  
③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.

- ④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

8. 디지털 포렌식에 대한 설명에서 ㉠, ㉡에 들어갈 용어는? (순서대로 ㉠, ㉡)

( ㉠ ) 공간은 물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장 되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다. 이 때, 디지털 포렌식의 파일 ( ㉡ ) 과정을 통해 디스크 내 비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출할 수 있다.

① 실린더(Cylinder), 역어셈블링(Disassembling)  
② MBR(Master Boot Record), 리버싱(Reversing)  
③ 클러스터(Cluster), 역컴파일(Decompiling)  
④ 슬랙(Slack), 카빙(Carving)

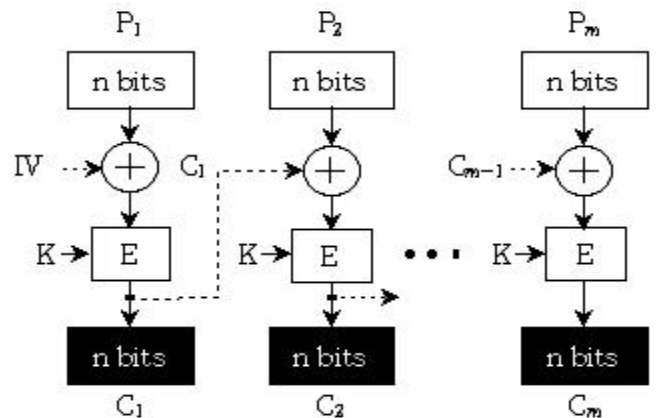
9. 버퍼 오버플로우 공격 대응 방법 중 ASLR(Address Space Layout Randomization)에 대한 설명으로 옳은 것은?

① 함수 호출 시 복귀 주소를 특수 스택에 저장하고 종료 시 해당 스택에 저장된 값과 비교하여 공격을 탐지한다.  
② 스택에 있는 함수 복귀 주소를 실행 가능한 임의의 libc 영역 내 주소로 지정하여 공격자가 원하는 함수의 실행을 방해한다.  
③ 함수의 복귀 주소와 버퍼 사이에 랜덤(Random) 값을 저장하여 해당 주소의 변조 여부를 탐지한다.  
④ 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.

10. 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는?

① PIPL-P                      ② ISMS-I  
③ PIMS-I                     ④ ISMS-P

11. 다음의 블록 암호 운용 모드는?



E: 암호화                      K: 암호화 키  
 $P_1, P_2, \dots, P_m$ : 평문 블록       $C_1, C_2, \dots, C_m$ : 암호 블록  
IV: 초기화 벡터                       $\oplus$ : XOR

- ① 전자 코드북 모드(Electronic Code Book Mode)
- ② 암호 블록 연결 모드(Cipher Block Chaining Mode)
- ③ 암호 피드백 모드(Cipher Feedback Mode)
- ④ 출력 피드백 모드(Output Feedback Mode)

12. 무결성을 위협하는 공격이 아닌 것은?

- ① 스누핑 공격(Snooping Attack)
- ② 메시지 변조 공격(Message Modification Attack)
- ③ 위장 공격(Masquerading Attack)
- ④ 재전송 공격(Replay Attack)

13. 다음에서 설명하는 접근 제어 모델은?

군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위레벨 읽기금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람할 수 없다. 또한, 인가받은 비밀 등급 미하의 정보 수정을 금지하는 '하위레벨 쓰기금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단한다.

- ① RBAC(Role-Based Access Control) 모델
- ② Biba 모델
- ③ Bell-LaPadula 모델
- ④ DAC(Discretionary Access Control) 모델

14. 유럽의 일반개인정보보호법(GDPR)에 대한 설명으로 옳은 것은?

- ① EU 회원국들 간 개인정보의 자유로운 이동을 금지하기 위한 목적을 갖는다.
- ② 그 자체로는 EU의 모든 회원국에게 직접적인 법적 구속력을 갖지 않는다.
- ③ 중요한 사항 위반 시 직전 회계연도의 전 세계 매출액 4% 또는 2천만 유로 중 높은 금액이 최대한도 부과액이다.
- ④ 만 19세 미만 미성년자의 개인정보 수집 시 친권자의 동의를 얻어야 한다.

15. IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은?

- ① SPI(Security Parameter Index)
- ② Payload Data
- ③ Padding
- ④ Next Header

16. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

- ① 암호화 기능을 사용하면 주고받는 데이터가 인터넷상에서 도청되는 위험성을 줄일 수 있다.
- ② 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가의 과정으로 이루어진다.
- ③ 웹 서비스 이외에 다른 응용 프로그램에도 적용할 수 있다.
- ④ 서버와 클라이언트 간 양방향 통신에 동일한 암호화 키를 사용한다.

17. KCMVP에 대한 설명으로 옳은 것은?

- ① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1부터 EAL7까지의 등급이 있다.
- ② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.
- ③ 개인정보 보호활동을 체계적·지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.
- ④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.

18. 「개인정보 보호법」상 개인정보 분쟁조정위원회에 대한 설명으로 옳지 않은 것은?

- ① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다.
- ② 위원장은 행정안전부·방송통신위원회·금융위원회 및 개인정보보호위원회의 고위공무원단에 속하는 일반직공무원 중에서 위촉한다.
- ③ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
- ④ 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

19. 전자화폐 및 가상화폐에 대한 설명으로 옳지 않은 것은?

- ① 가상화폐인 비트코인은 전자화폐와 마찬가지로 이중 지불(Double Spending)문제가 발생하지 않는다.
- ② 가상화폐인 비트코인은 분산원장기술로 알려진 블록체인을 이용한다.
- ③ 전자화폐는 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도로 규정하고 있지 않다.
- ④ 전자화폐는 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매 시 활용하는 결제 수단이며, 가상화폐는 전자화폐의 일종으로 볼 수 있다.

20. X.509 인증서(버전 3)의 확장(Extensions) 영역에 포함되지 않는 항목은?

- ① 인증서 정책(Certificate Policies)
- ② 기관 키 식별자(Authority Key Identifier)
- ③ 키 용도(Key Usage)
- ④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

전자문제집 CBT PC 버전 : [www.comcbt.com](http://www.comcbt.com)

전자문제집 CBT 모바일 버전 : [m.comcbt.com](http://m.comcbt.com)

기출문제 및 해설집 다운로드 : [www.comcbt.com/x](http://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
②	④	①	②	②	②	③	④	④	④
11	12	13	14	15	16	17	18	19	20
②	①	③	③	①	④	②	②	①	④