2021-지방직-정보보호론-A형-해설-곽후근

1. 보안의 3대 요소 중 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것은? [2021 지방직 01]
① 무결성(integrity)
② 기밀성(confidentiality)
③ 가용성(availability)
④ 접근성(accessability)
정답 체크
(1) 비인가자에 의한 정보의 변경, 삭제, 생성을 보호하여 정보의 정확성과 완전성 보장한다(위조/변조).
오답 체크
(2) 정보의 소유자가 원하는 대로 비밀이 유지되어야 한다는 원칙이다.
(3) 정보시스템은 적절한 방법으로 작동되어야 하며, 정당한 방법으로 권한이 주어진 사용자에게 정보 서비스를 거부해서는 안 된다는 원칙이다(DoS).
(4) 보안의 3대 요소가 아니다.

2. 스트림 암호에 대한 설명으로 옳지 않은 것은? [2021 지방직 02]
① 데이터의 흐름을 순차적으로 처리해 가는 암호 알고리즘이다.
② 이진화된 평문 스트림과 이진 키스트림 수열의 XOR 연산으로 암호문을 생성하는 방식이다.
③ 스트림 암호 알고리즘으로 RC5가 널리 사용된다.
④ 구현이 용이하고 속도가 빠르다는 장점이 있다.
정답 체크
(3) RC5는 블록 암호이고, RC4는 스트림 암호이다.
오답 체크
(1) 데이터의 흐름을 비트 또는 바이트 단위로 순차적으로 처리한다.
(2) 스트림 암호에서는 XOR 연산을 사용한다.
(4) (2)에서 수행되는 연산으로 인해 구현이 용이하고 속도가 빠르다.

3. DES(Data Encryption Standard)에 대한 설명으로 옳지 않은 것은? [2021 지방직 03]
① 1977년에 미국 표준 블록 암호 알고리즘으로 채택되었다.
② 64비트 평문 블록을 64비트 암호문으로 암호화한다.
③ 페이스텔 구조(Feistel structure)로 구성된다.
④ 내부적으로 라운드(round)라는 암호화 단계를 10번 반복해서 수행한다.
정답 체크
(4) 16라운드로 구성된다.
오답 체크
(1) 1977년에 미국의 연방 정보처리 표준 규격(FIPS)으로 채택된 대칭 암호이다.
(2) 64비트 평문을 64비트 암호문으로 암호화하는 대칭 암호 알고리즘이다.
(3) 페이스텔 네트워크(Feistel network)를 사용한다.

4. 다음 (가) ~ (다)에 해당하는 악성코드를 옳게 짝 지은 것은? [2021 지방직 04]

> (가) 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드
> (나) 운영체제나 특정 프로그램의 취약점을 이용하여 공격하는 악성코드
> (다) 외부에서 파일을 내려받는 다운로드와 달리 내부 데이터로부터 새로운 파일을 생성하여 공격을 수행하는 악성코드

	(가)	(나)	(다)
①	드로퍼	익스플로잇	랜섬웨어
②	드로퍼	랜섬웨어	익스플로잇
③	랜섬웨어	익스플로잇	드로퍼
④	랜섬웨어	드로퍼	익스플로잇

정답 체크

(3) 랜섬웨어 : 컴퓨터 시스템을 감염시켜 접근을 제한하고 일종의 몸값을 요구하는 악성 소프트웨어의 한 종류이다.
익스플로잇 : 컴퓨터 소프트웨어와 하드웨어의 버그나 취약점 등을 이용하여 공격자가 원하는 악의적 동작을 하도록 하는 공격 방법이다.
드로퍼 : 대상 시스템에 악성코드를 설치하기 위해 설계된 프로그램이다. 악성코드는 드로퍼 내에 포함되어 있음으로써 바이러스 스캐너에 의한 탐지를 피하고, 실행된 이후에는 드로퍼에 의해 악성코드가 다운로드 됨으로써 설치될 수 있다.

5. ISO 27001의 정보보호영역(통제분야)에 해당하지 않은 것은? [2021 지방직 05]

① 소프트웨어 품질 보증(Software Quality Assurance)
② 접근통제(Access Control)
③ 암호화(Cryptography)
④ 정보보안 사고관리(Information Security Incident Management)

정답 체크

(1) ISO 27001:2013의 통제분야에 소프트웨어 품질 보증은 포함되지 않는다.

6. 암호화 알고리즘과 복호화 알고리즘에서 각각 다른 키를 사용하는 것은? [2021 지방직 06]

① SEED
② ECC
③ AES
④ IDEA

정답 체크

(2) 비대칭키 암호 알고리즘이다.

오답 체크

(1), (3), (4) 대칭키 암호 알고리즘이다.

7. DoS(Denial of Service)의 공격유형이 아닌 것은? [2021 지방직 07]

① Race Condition
② TearDrop
③ SYN Flooding
④ Land Attack
정답 체크
(1) 한정된 자원을 이용하려는 여러 프로세스가 서로 경쟁을 벌이는 상황에서, 프로세스들이 여러 번 실행되는 과정에서 실행 순서가 뒤바뀌어 실행자가 원하는 결과를 얻는 것이다. 즉, DoS와 무관하다.
오답 체크
(2) 취약점 공격형 DoS이다(중간부터 순서 번호를 겹치게 하는 공격 방법).
(3) 자원 고갈형 DoS이다(존재하지 않는 클라이언트가 서버별로 한정되어 있는 접속 가능한 공간에 접속한 것처럼 속여 다른 사용자가 서버의 서비스를 제공받지 못하게 하는 공격).
(4) 취약점 공격형 DoS이다(패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소값을 똑같이 만들어서 공격 대상에게 보내는 공격).

8. 다음에서 설명하는 방화벽 구축 형태는? [2021 지방직 08]

○ 배스천(Bastion) 호스트와 스크린 라우터를 혼합하여 사용한 방화벽 ○ 외부 네트워크와 내부 네트워크 사이에 스크린 라우터를 설치하고 스크린 라우터와 내부 네트워크 사이에 배스천 호스트를 설치

① Bastion Host
② Dual Homed Gateway
③ Screened Subnet Gateway
④ Screened Host Gateway
정답 체크
(4) 1개의 배스천 호스트와 1개의 스크린 라우터로 구성된다.
오답 체크
(1) (2), (3), (4)의 기본 모듈로 사용된다.
(2) 1개의 배스천 호스트로 구성된다(2개의 NIC을 가짐).
(3) 1개의 배스천 호스트와 2개의 스크린 라우터로 구성된다.

9. 다음에서 설명하는 보안 기술은? [2021 지방직 09]

○ 해시 함수를 이용하여 메시지 인증 코드를 구현한다. ○ SHA-256을 사용할 수 있다.

① HMAC(Hash based Message Authentication Code)
② Block Chain
③ RSA(Rivest-Shamir-Adleman)
④ ARIA(Academy, Research Institute, Agency)
정답 체크
(1) SHA-1나 MD5와 같은 일방향 해시 함수를 이용하여 메시지 인증 코드를 실현한다.

오답 체크
(2) '블록(관리 대상 데이터)'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장된다.
(3) 비대칭키 암호 알고리즘이다.
(4) 대칭키 암호 알고리즘이다.

10. 스미싱 공격에 대한 설명으로 옳지 않은 것은? [2021 지방직 10]
① 공격자는 주로 앱을 사용하여 공격한다.
② 스미싱은 개인 정보를 빼내는 사기 수법이다.
③ 공격자는 사용자가 제대로 된 url을 입력하여도 원래 사이트와 유사한 위장 사이트로 접속시킨다.
④ 공격자는 문자 메시지 링크를 이용한다.
정답 체크
(3) 해당 설명은 파밍에 대한 설명이다.
오답 체크
(1) 역공학을 이용하여 앱에 악성 코드(해킹 툴)를 넣는다.
(2) 설치된 해킹 툴에 의해 개인 정보를 빼내간다.
(4) 문자 메시지 링크를 클릭하면 앱(해킹 툴)이 설치된다.

11. 디지털 포렌식을 통해 획득한 증거가 법적인 효력을 갖기 위해 만족해야 할 원칙이 아닌 것은? [2021 지방직 11]
① 정당성의 원칙
② 재현의 원칙
③ 무결성의 원칙
④ 기밀성의 원칙
정답 체크
(4) 기밀성의 원칙은 보안의 3대 요소로 디지털 포렌식의 원칙이 아니다.
오답 체크
(1), (2), (3) 이외에도 신속성의 원칙, 연계 보관성의 원칙이 존재한다.

12. 「개인정보 보호법」상의 개인정보에 대한 설명으로 옳지 않은 것은? [2021 지방직 12]
① 개인정보 보호위원회의 위원 임기는 3년이다.
② 개인정보는 가명처리를 할 수 없다.
③ 개인정보 보호위원회의 위원은 대통령이 임명 또는 위촉한다.
④ 개인정보처리자는 개인정보파일의 운용을 위하여 다른 사람을 통하여 개인정보를 처리할 수 있다.
정답 체크
(2) 제2조(정의) 1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
오답 체크
(1) 제7조의4(위원의 임기) ① 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.
(3) 제7조의2(보호위원회의 구성 등) ② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대

통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.
(4) 제2조(정의) 5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

13. DoS 및 DDoS 공격 대응책으로 옳지 않은 것은? [2021 지방직 13]
① 방화벽 및 침입 탐지 시스템 설치와 운영
② 시스템 패치
③ 암호화
④ 안정적인 네트워크 설계
정답 체크
(3) 암호화는 기밀성 공격의 대응책으로, DoS 공격(가용성 공격)의 대응책이 아니다.
오답 체크
(1) 방화벽 및 침입 탐지 시스템을 이용하여 이상 탐지를 수행한다(임계값을 설정하여 임계값 이상의 패킷은 버림).
(2) 시스템을 패치하면 시스템이 좀비 PC로 사용되는 것을 막을 수 있다.
(4) 안정적인 네트워크를 설계하면 자원 고갈이 발생했을 때 이를 효과적으로 대처할 수 있다.

14. 국제 공통 평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은? [2021 지방직 14]
① CC는 국제적으로 평가 결과를 상호 인정한다.
② CC는 보안기능수준에 따라 평가 등급이 구분된다.
③ 보안목표명세서는 평가 대상에 해당하는 정보보호 시스템의 보안 요구 사항, 보안 기능 명세 등을 서술한 문서이다.
④ 보호프로파일은 보안 문제를 해결하기 위해 작성한 제품군별 구현에 독립적인 보안요구사항 등을 서술한 문서이다.
정답 체크
(2) 보안 기능이 아닌 보증 요구(보안 요구)에 따라 평가 등급이 구분된다.
오답 체크
(1) CCRA를 이용한다.
(3) 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의한다(개별 제품). 기술적인 구현 가능성을 고려한다.
(4) 사용자 또는 개발자의 요구사항을 정의한다(전체 제품). 기술적인 구현 가능성을 고려하지 않는다.

15. 생체인증(Biometrics)에 대한 설명으로 옳지 않은 것은? [2021 지방직 15]
① 생체 인증은 불변의 신체적 특성을 활용한다.
② 생체 인증은 지문, 홍채, 망막, 정맥 등의 특징을 활용한다.
③ 얼굴은 행동적 특성을 이용한 인증 수단이다.
④ 부정허용률(false acceptance rate)은 인증되지 않아야 할 사람을 인증한 값이다.
정답 체크
(3) 얼굴은 동적(행동적) 특성이 아닌 정적인 특성이다.
오답 체크
(1) 불변의 신체적 특징과 행동적 특징으로 구분할 수 있다.
(2) 신체적 특징은 각 개인의 얼굴 모양(Face)과 얼굴열상(Thermal image)을 이용하는 얼굴인식, 홍채(Iris)를 이용하는 홍채인식, 정맥(Vein)을 이용하는 정맥인식, 지문(Fingerprint)을 이용하는 지문인식과 그 외에 망막(Retina),

손모양(Hand geometry) 등을 이용한 것이 포함되고 있다(정적). 행동적 특징은 음성인식, 걸음걸이 인식, 서명인식 등이 있다(동적).
(4) 오인식률(FAR, 다른 사람을 나로 오인할 확률)과 오거부율(FRR, 나를 다른 사람으로 오인할 확률)이 존재한다.

16. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3(정보보호 최고책임자의 지정 등)에 따른 정보보호 최고책임자의 업무가 아닌 것은? [2021 지방직 16]
① 정보보호 사전 보안성 검토
② 정보보호 취약점 분석·평가 및 개선
③ 중요 정보의 암호화 및 보안서버 적합성 검토
④ 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치
정답 체크
(4) 제46조(집적된 정보통신시설의 보호) ① 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 정보통신서비스 제공자(이하 "집적정보통신시설 사업자"라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다.
오답 체크
(1), (2), (3) 제45조의3(정보보호 최고책임자의 지정 등) ④ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.
1. 정보보호관리체계의 수립 및 관리·운영
2. 정보보호 취약점 분석·평가 및 개선
3. 침해사고의 예방 및 대응
4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등
5. 정보보호 사전 보안성 검토
6. 중요 정보의 암호화 및 보안서버 적합성 검토
7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

17. 정보보호 및 개인정보보호 관리체계 인증에 대한 설명으로 옳은 것은? [2021 지방직 17]
① 인증기관 지정의 유효기간은 2년이다.
② 사후심사는 인증 후 매년 사후관리를 위해 실시된다.
③ 인증심사 기준은 12개 분야 92개 통제 사항이다.
④ 인증심사원은 2개 등급으로 구분된다.
정답 체크
(2) 사후심사는 인증 후 매년 실시된다.
오답 체크
(1) 인증기관 지정의 유효기간은 3년이다.
(3) 인증심사 기준은 21개 분야 102개 통제 사항이다.
(4) 인증심사원은 3개 등급(심사원보, 심사원, 선임심사원)으로 구분된다.

18. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은? [2021 지방직 18]
① RSA를 이용하여 메시지 다이제스트를 서명한다.
② 세션 키는 여러 번 사용된다.
③ 수신자는 자신의 개인키를 이용하여 세션 키를 복호화한다.
④ 세션 키를 이용하여 메시지를 암복호화한다.

정답 체크

(2) 세션 키는 임시키로 한번 사용된다.

오답 체크

(1) 서명 시간을 단축하기 위해 메시지 다이제스트(해시값)에 서명한다.

(3) 하이브리드 암호 방법을 이용한다(키 배송 문제를 해결하기위해 공개키를 이용하여 암복호화).

(4) 하이브리드 암호 방법을 이용한다(암호화 시간을 단축하기 위해 대칭키를 이용하여 암복호화).

19. 다음에서 설명하는 블록암호 운영 모드는? [2021 지방직 19]

○ 단순한 모드로 평문이 한 번에 하나의 평문 블록으로 처리된다. ○ 각 평문 블록은 동일한 키로 암호화된다. ○ 주어진 하나의 키에 대하여 평문의 모든 블록에 대한 유일한 암호문이 존재한다.

① CBC(Cipher Block Chaining Mode)

② CTR(Counter Mode)

③ CFB(Cipher-Feed Back Mode)

④ ECB(Electronic Code Book Mode)

정답 체크

(4) 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.

오답 체크

(1) 1 단계 앞에서 수행되어 결과로 출력된 암호문 블록에 평문 블록을 XOR 하고 나서 암호화를 수행한다.

(2) 블록을 암호화할 때마다 1씩 증가해 가는 카운터를 암호화해서 키 스트림(key stream)을 만든다.

(3) 1 단계 앞의 암호문 블록을 암호 알고리즘의 입력으로 사용한다.

20. BCP(Business Continuity Planning)에 대한 설명으로 옳지 않은 것은? [2021 지방직 20]

① BCP는 사업의 연속성을 유지하기 위한 업무지속성 계획과 절차이다.

② BCP는 비상시에 프로세스의 운영 재개에 필요한 조치를 정의한다.

③ BIA는 조직의 필요성에 의거하여 시스템의 중요성을 식별한다.

④ DRP(Disaster Recovery Plan)는 최대허용중단시간(Maximum Tolerable Downtime)을 산정한다.

정답 체크

(4) MTD는 DRP가 아닌 BCP에서 산정한다.

오답 체크

(1) 각종 재해나 재난의 발생을 대비하여 핵심 시스템의 가용성과 신뢰성을 회복하고 사업의 연속성을 유지하기 위한 일련의 사업지속성계획과 절차를 의미한다.

(2) 중요한 사업의 기능들을 비상시를 대비하여 자산(Assets)의 우선순위를 평가하거나, 대체 장소를 선택하는 등 재해나 재난 시에 원상 복귀하고자 미리 평가 계획을 하는 단계이다.

(3) 사업 중단 사태가 발생하였을 경우 기업에 미칠 수 있는 정성적(고객의 불만사항을 접수하지 못하는 경우)/정량적(경제적) 영향도를 파악하여 우선순위를 부여하고 문서화 하는 프로세스이다.