2022-국가직-정보보호론-가-해설-곽후근

1. 사용자의 신원을 검증하고 전송된 메시지의 출처를 확인하는 정보보호 개념은?
① 무결성
② 기밀성
③ 인증성
④ 가용성
정답 체크
(3) 인증성에는 사용자 인증과 메시지 인증이 존재한다.

2. TCP에 대한 설명으로 옳지 않은 것은?
① 비연결 지향 프로토콜이다.
② 3-Way Handshaking을 통해 서비스를 연결 설정한다.
③ 포트 번호를 이용하여 서비스들을 구별하여 제공할 수 있다.
④ SYN Flooding 공격은 TCP 취약점에 대한 공격이다.
정답 체크
(1) 연결 지향이다.

3. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?
① 일반적으로 대칭키 암호 알고리즘은 비대칭키 암호 알고리즘에 비하여 빠르다.
② 대칭키 암호 알고리즘에는 Diffie-Hellman 알고리즘이 있다.
③ 비대칭키 암호 알고리즘에는 타원 곡선 암호 알고리즘이 있다.
④ 인증서는 비대칭키 암호 알고리즘에서 사용하는 공개키 정보를 포함하고 있다.
정답 체크
(2) Diffie-Hellman은 공개키 암호 알고리즘이다.

4. TCP 세션 하이재킹에 대한 설명으로 옳은 것은?
① 서버와 클라이언트가 통신할 때 TCP의 시퀀스 넘버를 제어하는 데 문제점이 있음을 알고 이를 이용한 공격이다.
② 공격 대상이 반복적인 요구와 수정을 계속하여 시스템 자원을 고갈시킨다.
③ 데이터의 길이에 대한 불명확한 정의를 악용한 덮어쓰기로 인해 발생한다.
④ 사용자의 동의 없이 컴퓨터에 불법적으로 설치되어 문서나 그림 파일 등을 암호화한다.
정답 체크
(1) MITM 공격이다.
오답 체크
(2) boink, bonk, teardrop에 해당한다.
(3) 버퍼 오버플로우에 해당한다.
(4) 랜섬웨어에 해당한다.

5. 생체 인증 측정에 대한 설명으로 옳지 않은 것은?
① FRR는 권한이 없는 사람이 인증을 시도했을 때 실패하는 비율이다.

② 생체 인식 시스템의 성능을 평가하는 지표로는 FAR, EER, FRR 등이 있다.
③ 생체 인식 정보는 신체적 특징과 행동적 특징을 이용하는 것들로 분류한다.
④ FAR는 권한이 없는 사람이 인증을 시도했을 때 성공하는 비율이다.
정답 체크
(1) 권한이 있는 사람이 인증을 시도했을 때 실패하는 비율이다.

6. 블록암호 카운터 운영모드에 대한 설명으로 옳지 않은 것은?
① 암호화와 복호화는 같은 구조로 구성되어 있다.
② 병렬로 처리할 수 있는 능력에 따라 처리속도가 결정된다.
③ 카운터를 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.
④ 블록을 순차적으로 암호화복호화 한다.
정답 체크
(4) 블록을 병렬로 암호화복호화 한다.

7. AES 알고리즘에 대한 설명으로 옳지 않은 것은?
① 대먼과 리즈먼이 제출한 Rijndael이 AES 알고리즘으로 선정되었다.
② 암호화 과정의 모든 라운드에서 SubBytes, ShiftRows, MixColumns, AddRoundKey 연산을 수행한다.
③ 키의 길이는 128, 192, 256 bit의 크기를 사용한다.
④ 입력 블록은 128 bit이다.
정답 체크
(2) 마지막 라운드에서 MixColumns를 수행하지 않는다.

8. 비트코인 블록 헤더의 구조에서 머클 루트에 대한 설명으로 옳지 않은 것은?
① 머클 트리 루트의 해시값이다.
② 머클 트리는 이진트리 형태이다.
③ SHA-256으로 해시값을 계산한다.
④ 필드의 크기는 64바이트이다.
정답 체크
(4) 필드의 크기는 32바이트이다.

9. SET에 대한 설명으로 옳지 않은 것은?
① 인터넷에서 신용카드를 지불수단으로 이용하기 위한 기술이다.
② 인증기관은 SET에 참여하는 모든 구성원의 정당성을 보장한다.
③ 고객등록에서는 지불 게이트웨이를 통하여 고객의 등록과 인증서의 처리가 이루어진다.
④ 상점등록에서는 인증 허가 기관에 등록하여 자신의 인증서를 만들어야 한다.
정답 체크
(3) 해당 설명은 인증기관이고, 지불 게이트웨이는 결재를 수행한다.

10.「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)에 대한 설명으로 옳지 않은 것은?
① 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다.

② 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.
③ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공할 수 있다.
④ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 「개인정보 보호법」을 위반하여 발생한 손해배상책임에 대하여 수탁자를 개인정보처리자의 소속 직원으로 본다.
정답 체크
(3) 제26조(업무위탁에 따른 개인정보의 처리 제한) ⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

11. IPv6에 대한 설명으로 옳지 않은 것은?
① IP주소 부족 문제를 해결하기 위하여 등장하였다.
② 128 bit 주소공간을 제공한다.
③ 유니캐스트는 단일 인터페이스를 정의한다.
④ 목적지 주소는 유니캐스트, 애니캐스트, 브로드캐스트 주소로 구분된다.
정답 체크
(4) 브로드캐스트 대신 멀티캐스트를 제공한다.

12. SSH를 구성하는 프로토콜에 대한 설명으로 옳은 것은?
① SSH는 보통 TCP상에서 수행되는 3개의 프로토콜로 구성된다.
② 연결 프로토콜은 서버에게 사용자를 인증한다.
③ 전송계층 프로토콜은 SSH 연결을 사용하여 한 개의 논리적 통신 채널을 다중화한다.
④ 사용자 인증 프로토콜은 전방향 안전성을 만족하는 서버인증만을 제공한다.
정답 체크
(1) 연결, 전송계층, 사용자 인증 프로토콜로 구성된다.
오답 체크
(2) 사용자 인증 프로토콜에 대한 설명이다.
(3) 연결 프로토콜에 대한 설명이다.
(4) 사용자인증만을 제공한다.

13. 유럽의 국가들에 의해 제안된 것으로 자국의 정보보호 시스템을 평가하기 위하여 제정된 기준은?
① TCSEC
② ITSEC
③ PIMS
④ ISMS-P
정답 체크
(2) 유럽은 ITSEC이다.

14. 「개인정보 보호법」 제3조(개인정보 보호 원칙)에 대한 설명으로 옳지 않은 것은?
① 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당

하게 수집하여야 한다.
② 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
③ 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비공개로 하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
④ 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.
정답 체크
(3) 제3조(개인정보 보호 원칙) ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

15. ISO/IEC 27001의 통제영역에 해당하지 않은 것은?
① 정보보호 조직
② IT 재해복구
③ 자산 관리
④ 통신 보안
정답 체크
(2) ISMS의 통제영역이다.

16. 접근제어 모델에 대한 설명으로 옳지 않은 것은?
① 접근제어 모델은 강제적 접근제어, 임의적 접근제어, 역할기반 접근제어로 구분할 수 있다.
② 임의적 접근제어 모델에는 Biba 모델이 있다.
③ 강제적 접근제어 모델에는 Bell-LaPadula 모델이 있다.
④ 역할기반 접근제어 모델은 사용자의 역할에 권한을 부여한다.
정답 체크
(2) Biba는 강제적 접근 제어 모델이다.

17. 운영체제에 대한 설명으로 옳지 않은 것은?
① 윈도 시스템에는 FAT, FAT32, NTFS가 있다.
② 메모리 관리는 프로그램이 메모리를 요청하면 적합성을 점검하고 적합하다면 메모리를 할당한다.
③ 인터럽트는 작동 중인 컴퓨터에 예기치 않은 문제가 발생한 것이다.
④ 파일 관리는 명령어들을 체계적이고 효율적으로 실행할 수 있도록 작업스케줄링하고 사용자의 작업 요청을 수용하거나 거부한다.
정답 체크
(4) 해당 설명은 프로세스 관리에 대한 설명이고, 파일 관리는 사용자별로 파일 접근 권한을 부여하고 접근 권한에 따라 파일을 할당하고 해제한다.

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 용어에 대한 설명으로 옳지 않은 것은?
① “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
② “통신과금서비스이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
③ “전자문서”란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서

형식의 자료로서 표준화된 것을 말한다.
④ 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위로 인하여 발생한 사태는 “침해사고”에 해당한다.
정답 체크
(2) 해당 용어는 “이용자”이고, “통신과금서비스”란 정보통신서비스로서 다음 각 목의 업무를 말한다.
가. 타인이 판매·제공하는 재화 또는 용역(이하 “재화등”이라 한다)의 대가를 자신이 제공하는 전기통신역무의 요금과 함께 청구·징수하는 업무
나. 타인이 판매·제공하는 재화등의 대가가 가목의 업무를 제공하는 자의 전기통신역무의 요금과 함께 청구·징수되도록 거래정보를 전자적으로 송수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 업무

19. 스니핑 공격에 대한 설명으로 옳지 않은 것은?
① 스위치에서 ARP 스푸핑 기법을 이용하면 스니핑 공격이 불가능하다.
② 모니터링 포트를 이용하여 스니핑 공격을 한다.
③ 스니핑 공격 방지책으로는 암호화하는 방법이 있다.
④ 스위치 재밍을 이용하여 위조한 MAC 주소를 가진 패킷을 계속 전송하여 스니핑 공격을 한다.
정답 체크
(1) 스위치는 LAN에 설치되므로 ARP 스푸핑이 가능하다.

20. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 인증심사원에 대한 설명으로 옳지 않은 것은?
① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.
② 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우에는 인증심사원의 자격이 취소될 수 있다.
③ 인증위원회는 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 자격유지를 위해 자격 유효기간 만료 전까지 수료하여야하는 보수 교육시간 전부를 이수한 것으로 인정할 수 있다.
④ 인증심사원의 등급별 자격요건 중 선임심사원은 심사원 자격취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자이다.
정답 체크
(3) 제15조(인증심사원 자격 유지 및 갱신) ③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.