2022-군무원-7급-정보보호론-해설-곽후근

1. 다음 중 버퍼오버플로우 공격으로부터 가장 안전한 C언어 함수에 해당하는 것은?
① strcpy ② gets
③ sprintf ④ scanf_s

정답 체크
(4) MS에서 만든 안전한 함수이다(공통 함수가 아닌 특정 회사 함수를 시험 문제로 낸 것은 잘못이라고 여겨짐).
오답 체크
(1), (2), (3) 버퍼오버플로우 공격에 취약한 함수이다.

2. 다음 중 한국에서 개발한 암호화 알고리즘이 아닌 것은?
① AES ② ARIA ③ SEED ④ LEA

정답 체크
(1) 미국의 NIST에서 공모하였다.
오답 체크
(2) 경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.
(3) 전자상거래, 금융, 무선통신 등에서 전송되는 개인정보와 같은 중요한 정보를 보호하기 위해 1999년 2월 한국인터넷진흥원과 국내 암호전문가들이 순수 국내기술로 개발한 128비트 블록 암호 알고리즘이다.
(4) 빅데이터, 클라우드 등 고속 환경 및 모바일기기의 경량 환경에서 기밀성을 제공하기 위해 개발된 128비트 블록암호 알고리즘이다.

3. OSI 7계층은 다양한 네트워크 간의 호환을 위해 만든 표준 네트워크 모델이다. 다음 중 OSI 7계층 에서 네트워크 계층에 대한 설명으로 가장 옳은 것은?
① 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공한다.
② 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해준다.
③ 두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층으로 16진수 12개로 구성된 MAC 주소를 사용한다.
④ 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층으로 라우터를 통한 패킷 포워딩을 담당한다.

정답 체크
(4) 라우팅 역할을 수행한다.
오답 체크
(1) 응용 계층을 의미한다.

(2) 전송 계층을 의미한다.
(3) 데이터 링크 계층을 의미한다.

4. 다음은 TCP의 연결 설정 과정(3-way handshaking)을 무작위로 나열한 것이다. 이를 가장 올바른 순서로 나열한 것은?

A: 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고, 클라이언트에 연결을 해도 좋다는 의미로 SYN+ACK 패킷을 보낸다. B: 두 시스템이 통신을 하기 전 클라이언트는 포트가 닫힌 Closed 상태이고 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태이다. C: 클라이언트가 통신을 하려고 하면 임의의 포트 번호가 클라이언트 프로그램에 할당되고, 클라이언트는 서버에 연결하고 싶다는 의사 표시인 SYN Sent 상태가 된다. D: 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보낸다.

① A → C → B → D ② B → C → A → D ③ C → D → A → B ④ C → D → B → A

정답 체크
(2) B : 클라이언트는 닫혀 있고, 서버는 연결을 맺기 위해 대기한다.
C : 클라이언트는 임의의 포트이고, 서버는 특정 포트이다.
A : 서버는 SYN을 받고, SYN+ACK를 보낸다.
D : 클라이언트가 ACK를 보내면 연결을 맺은 상태가 된다.

5. 다음은 모바일 기기 상에서의 보안 관련 기술에 대한 설명이다. 해당 기술과 가장 가까운 것은?

- 응용 프로그램이 실행될 때 가상 머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 의미한다. - 사용자 앱은 기본적으로 앱 간에 데이터를 주고 받을 수 없고 시스템 파일에도 접근할 수 없다. - 앱 간 문서, 음악, 사진 등의 전송은 시스템 API에서 그 기능을 제공할 때만 가능하다.

① 샌드박스 ② 멀티 태스킹 금지
③ 원격 로그인 금지 ④ 응용 프로그램 서명

정답 체크
(1) 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이다.
오답 체크
(2) 빠른 실행 속도를 보장하기 위해 멀티 태스킹을 금지한다(예전 iOS에서 제공).
(3) 서버를 보호하기 위해 원격 로그인과 관리자 계정 로그인을 금지한다.
(4) 응용 프로그램의 배포자를 인증하고 변경되지 않았음을 나타낸다.

6. 다음은 WEP(Wired Equivalent Privacy)를 이용한 암호화 세션 생성을 무작위로 나열한 것이다. 이를 가장 올바른 순서로 나열한 것은?

A: 사용하려는 무선랜 서비스의 SSID 값을 알아내어 무선랜 AP에 연결 요청 메시지를 전송한다.
B: 인증용 문자열(Challenge)을 받은 사용자는 자신이 가진 공유키로 WEP 암호화를 적용하여 암호문을 만든 다음 AP에 전송한다.
C: 사용자의 연결 요청 메시지를 받은 AP는 임의의 문장을 생성하여 원본을 저장하고 연결요청 응답 메시지를 이용하여 암호화 되지 않은 인증용 문자열(Challenge)을 전송한다.
D: 사용자가 공유키로 만든 암호문을 전송받은 AP는 자신이 가진 공유키로 암호문을 복호화한다. 그리고 복호화된 문장과 자신이 저장하고 있던 원본 문장을 비교하여 같으면 사용자가 자신과 같은 공유키를 가진 그룹원이라고 인식해 연결 허용 메시지를 전송한다.

① A → C → B → D ② B → C → A → D ③ C → A → B → D ④ C → B → A → D

정답 체크
(1) A : SSID가 숨겨져 있을 수도 있다.
C : Challenge를 전송한다.
B : Challenge에 대한 Response를 전송한다.
D : Response를 확인 후 연결을 맺는다.

7. 다음 중 인텔의 80x86 CPU의 범용 레지스터에 대한 설명으로 옳지 않은 것은?
① EAX(누산기): 산술 연산에 사용하며 함수의 결과 값을 저장한다.
② EBX(베이스 레지스터): 특정 주소를 저장하며 주소 지정을 확대하기 위한 인덱스로 사용한다.
③ ECX(카운터 레지스터): 반복적으로 실행되는 특정 명령에 사용한다. 루프의 반복 횟수나 좌우 방향 시프트 비트 수를 기억한다.
④ EDX(데이터 레지스터): 연산 결과 및 시스템 상태와 관련된 여러 가지 플래그 값을 저장한다.

정답 체크
(4) 부호 확장 명령 등에 쓰이는 레지스터이다.
오답 체크
(1) 산술(덧셈, 곱셈, 나눗셈 등), 논리 연산을 수행하며 함수의 결과 값이 이 레지스터에 저장된다.
(2) 메모리 주소를 저장하기 위한 용도로 사용된다.
(3) 주로 반복 명령어 사용시 반복 카운터로 사용되는 레지스터이다.

8. 아래에서 설명하는 전자우편 암호화와 가장 가까운 것은?

1991년에 IDEA 알고리즘과 RSA 알고리즘을 조합하여 만들어졌다. 세션키를 암호화하기 위해 IDEA 알고리즘을 이용하고 사용자 인증을 위한 전자 서명에는 RSA 알고리즘을 이용한다. 특히 해당 기술을 사용하는 사람들 간의 신뢰 관계를 통해 공개키를 인증하는 기법을 사용하고 있다.

① S/MIME(Secure MIME) ② PGP(Pretty Good Privacy)
③ PEM(Privacy Enhanced Mail) ④ SSL(Secure Socket Layer)

정답 체크
(2) 전자우편의 안전성을 위해 1991년 미국의 Phil Zimmermann에 의해 개발된 전자우편 보안 시스템이다.

오답 체크
(1) 안전한 전자메일 전송을 위한 산업체 표준 규약이다. 기존 MIME 형식의 전자메일 서비스에 암호 및 보안 서비스가 추가된 구조이다.
(3) 인터넷상에서 안전한 전자우편을 제공하기 위해 제안된 인터넷 표준안을 만드는 기술위원회(IETF: Internet Engineering Task Force) 표준안이다.
(4) 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있다.

9. 시스템 상에서 프로그램을 동작시키면 해당 프로그램을 동작하기 위한 가상의 공간이 메모리에 생성된다. 아래에서 설명하고 있는 메모리 구조와 가장 가까운 것은?

- 프로그램 로직이 동작하기 위한 인자(argument)와 프로세스 상태를 저장한다. - 해당 영역은 레지스터의 임시 저장, 서브루틴 사용 시 복귀 주소 저장, 서브루틴에 인자 전달 등의 용도로 사용된다. - 메모리의 상위 주소에서 하위 주소 방향으로 사용하며 후입선출(Last In First Out, LIFO) 원칙 에 따라 나중에 저장된 값을 먼저 사용한다.

① 스택 ② 힙
③ 레지스터 ④ 버퍼

정답 체크
(1) 지역 변수가 저장된다.
오답 체크
(2) 동적 메모리가 저장된다.
(3) 가장 빠른 접근 속도를 가진다(레지스터 파일로 만들어짐).
(4) 주기억장치에 생성되어 속도차를 완화한다.

10. 다음 중 대칭키 암호화 기법이 아닌 것은?
① RC4 ② ElGamal ③ LEA ④ ARIA

정답 체크
(2) 비대칭키 암호화 기법이다.
오답 체크
(1) 스트림 암호이다.
(3), (4) 블록 암호이다.

11. 다음은 XSS(Cross-Site Scripting) 공격 과정을 무작위로 나열한 것이다. 가장 올바른 순서로 나열한 것은?

A: 웹 서버는 사용자가 접근한 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다. B: XSS 취약점이 존재하는 서버에 XSS 코드를 작성하여 저장한다. 일반적으로 공격자는 사용자가 이용하는 게시판을 공격한다. C: 공격자가 작성해 놓은 XSS 코드에 해당 웹 서비스 사용자가 접근한다. 사용자는 공격자가 작

성해 놓은 XSS 코드에 접근한다는 것을 인지하지 못한다. 사용자는 어떤 게시판의 글을 읽는 과정에서 공격자의 XSS 코드에 접근하게 된다. D: 사용자의 시스템에서 XSS 코드가 실행되며 그 결과가 공격자에게 전달된다.

① C → A → B → D ② A → C → B → D ③ B → C → A → D ④ C → B → A → D

정답 체크

(3) B : 공격자가 악성 코드를 서버에 저장한다(저장 XSS 공격).

C : 클라이언트가 악성 코드에 접근한다.

A : 악성 코드가 클라이언트에 전달된다.

D : 악성 코드가 실행되고, 쿠키 정보 등이 공격자에게 전송된다.

12. 아래에서 설명하는 보안 솔루션과 가장 관련이 있는 기술은?

문서 보안에 초점을 둔 기술로 문서의 열람, 편집, 인쇄에 접근 권한을 설정하여 통제한다. 특정한 형태의 문서만 통제하는 것이 아니라 MS워드나 HWP, TXT, PDF 파일 등 사무에 사용하는 대부 분의 파일을 통제할 수 있다. 사내에서 사용하는 운영체제 커널에 해당 모듈을 삽입하는 형식으로 동 작시킬 수 있다.

① VPN(Virtual Private Network) ② DRM(Digital Right Management)

③ DLP(Data Leak Prevention) ④ ASIC(Application Specific Integrated Circuit)

정답 체크

(2) 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다.

오답 체크

(1) 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.

(3) 기업 내에서 이용하는 다양한 주요 정보인 기술 정보, 프로젝트 계획, 사업 내용, 영업 비밀, 고객 정보 등을 보호하고 외부 유출을 방지하기 위해서 사용된다.

(4) 범용 용도가 아닌 특정 용도에 맞게 맞춤 제작된 집적 회로를 말한다.

13. 다음은 OECD 개인 정보 보안 8 원칙 중 일부를 나열한 것이다. 8 원칙에 대한 설명으로 가장 옳지 않은 것은?

① 정보 정확성의 원칙(Data Quality Principle): 이용 목적상 필요한 범위 내에서 개인 정보의 정확성, 완전성, 최신성이 확보되어야 한다.

② 이용 제한의 원칙(Use Limitation Principle): 정보 주체의 동의가 있거나 법 규정이 있는 경우를 제외하고 목적 외에 이용하거나 공개할 수 없다.

③ 안전성 확보의 원칙(Security Safeguard Principle): 정보 주체의 개인 정보 열람•정정•삭제 청구권이 보장되어야 한다.

④ 책임의 원칙(Accountability Principle): 개인 정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

정답 체크
(3) 개인정보의 분실, 불법적인 접근, 파괴, 사용, 수정, 공개위험에 대비하여 합리적인 안전보호장치를 마련해야 한다.
오답 체크
(1) 개인정보는 그 이용목적에 부합하는 것이어야 하고, 이용목적에 필요한 범위 내에서 정확하고 완전하며 최신의 상태로 유지하여야 한다.
(2) 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다.
(4) 개인정보 관리자는 제시한 7개 원칙들이 지켜지도록 필요한 제반 조치를 취해야 한다.

14. 다음 중 양자 컴퓨팅과 관련한 설명으로 가장 옳지 않은 것은?
① 양자 컴퓨터에 Shor 알고리즘을 적용하면 현재 알려진 다수의 대칭키 암호화 알고리즘이 다항 시간 내에 공격 가능해지므로 안전하지 않게 된다.
② 양자키 분배(quantum key distribution)에서는 양자 물리학의 중첩과 얽힘의 성질을 이용하여 도청으로부터 안전한 키 분배 방식을 제공한다.
③ 양자 내성 암호(post-quantum cryptography)는 양자 컴퓨터가 등장하더라도 안전성을 보장하는 암호 알고리즘을 일컬으며, NIST에 의해 후보 알고리즘이 검토되고 있다.
④ 마이크로소프트에서는 양자 알고리즘을 개발하고 실행하기 위한 Q# 오픈 소스 프로그래밍 언어를 개발하였다.

정답 체크
(1) 대칭키가 아닌 비대칭키 알고리즘이다.
오답 체크
(2) 1984년 C. H. Bennett과 G. Brassard가 제안하였으며, 기존에 있던 대부분의 암호체계가 대부분 수학적 복잡성에 기반하는데 비해, 양자암호는 자연현상에 기반하고 있는 특징을 띄며, 암호에 사용되는 원타임 패드를 생성하는 이상적인 방법 중 하나다.
(3) 양자 컴퓨터를 이용한 공격에 다항 시간 내에 뚫리지 않을 것으로 기대되는 암호이다.
(4) Q# 및 Quantum 개발 키트의 도구를 제공한다.

15. 다음 중 부 채널 분석(side-channel analysis)에 대한 설명으로 가장 옳지 않은 것은?
① 주로 구현 상에서 발생하는 시간 차, 전력 소모 등의 부가적인 정보로부터 민감한 정보를 유추하는 기법이다.
② 하드웨어에 대한 부 채널 분석뿐 아니라 소프트웨어 기반 부 채널 분석 또한 가능하다.
③ 공통평가기준(Common Criteria, CC) 및 암호모듈평가체계(Cryptographic Module Validation Program, CMVP) 등에서 비 침습 공격에 대한 평가가 이루어지며, 비 침습 공격은 부 채널 분석을 포함한다.
④ 알고리즘의 이론적 오류로 인한 정보 유출 취약점을 활용한다.

정답 체크
(4) 부채널이 아닌 정채널 공격이다(정채널은 부채널의 반대 개념으로 저자가 지어낸 용어).
오답 체크

(1) 알고리즘의 약점을 찾거나(암호 해독과는 다름) 무차별 공격을 하는 대신에 암호 체계의 물리적인 구현 과정의 정보를 기반으로 하는 공격 방법이다. 예를 들어, 소요 시간 정보, 소비 전력, 방출하는 전자기파, 심지어는 소리를 통해서 시스템 파괴를 위해 악용할 수 있는 추가 정보를 얻을 수 있다.
(2) 하드웨어와 소프트웨어 모두 가능하다.
(3) CC와 CMVP에 포함된다.

16. 다음 중 블록체인 기반 가상화폐에 대한 설명으로 가장 옳지 않은 것은?
① 중앙집중화된 관리자나 제3의 중재자가 없다.
② 블록에는 하나의 거래 내역이 암호화되어 저장된다.
③ 거래장부에 해당하는 블록은 공개되어 분산 관리된다.
④ 분산된 모든 블록을 위조하는 어려움에 기반하여 가상화폐의 안전성이 보장된다.

정답 체크
(2) 여러 개의 거래 내역이 저장된다.
오답 체크
(1) P2P 방식이다.
(3) Peer 들에게 분산 관리된다.
(4) 블록이 연결되어 있기 때문에 하나를 수정하면 이후의 모든 블록이 수정되어야 한다.

17. 다음 중 위험분석 방법론의 성격이 가장 다른 것은?
① 전문가 집단을 구성하여 위험을 분석 및 평가하여 다양한 위협과 취약성을 토론을 통해 분석한다.
② 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정한다.
③ 비교 우위 순위 결정표에 위험 항목들의 서술적 순위를 결정한다.
④ 위협의 발생 빈도를 계산하는 식을 이용하여 위험 순위를 결정한다.

정답 체크
(4) 정량적 분석(수학공식접근법)에 해당한다.
오답 체크
(1) 정성적 분석(델파이법)에 해당한다.
(2) 정성적 분석(시나리오법)에 해당한다.
(3) 정성적 분석(순위결정법)에 해당한다.

18. 다음 중 암호학적 해시 함수(h)에 대한 설명으로 가장 옳지 않은 것은?
① 주어진 출력 y에 대하여 h(x) = y를 만족하는 x를 구하기 어렵다.
② 임의 메시지에 대하여 동일한 해시값을 가지는 메시지가 없다.
③ 동일한 해시값을 가지는 서로 다른 x 와 x'을 구하기 어렵다.
④ 주어진 입력 x 에 대하여 h(x') = h(x), x' ≠ x를 만족하는 x가 아닌 x'을 구하기 어렵다.

정답 체크
(2) 충돌이 발생할 수 있다.

오답 체크
(1) 일방향성 또는 pre-image attack이다.
(3) 강한 충돌 내성이다.
(4) 약한 충돌 내성 또는 second pre-image attack이다.

19. 다음 중 정보통신기반 보호법에 대한 설명으로 옳지 않은 것은?
① 전자적 침해행위에 대비하여 주요정보통신 기반 시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장 하는 것을 목적으로 한다.
② 주요정보통신기반 시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요 정보통신기반 시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책을 수립·시행하여야 한다.
③ 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반 시설이 교란 · 마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원 중 하나의 기관에 반드시 그 사실을 통지하여야 한다.
④ 관리기관의 장은 소관 주요정보통신기반 시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반 시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

정답 체크
(3) 제13조(침해사고의 통지) ①관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란 · 마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원(이하 “관계기관등”이라 한다)에 그 사실을 통지하여야 한다. 이 경우 관계기관등은 침해사고의 피해확산 방지와 신속한 대응을 위하여 필요한 조치를 취하여야 한다. (관계 행정기관은 필수이다)
오답 체크
(1) 제1조(목적) 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립 · 시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.
(2) 제5조(주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 “관리기관”이라 한다)의 장은 제9조제1항 또는 제2항에 따른 취약점 분석 · 평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적 · 기술적 대책을 포함한 관리대책(이하 “주요정보통신기반시설보호대책”이라 한다)을 수립 · 시행하여야 한다.
(4) 제14조(복구조치) ①관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

20. 다음 중 유닉스 시스템에서의 파일 또는 디렉터리의 권한 관리에 대한 설명으로 가장 옳지 않은 것은?
① SetUID가 설정된 프로그램이 실행되면, 일반 사용자가 소유자 권한을 위임받아 특정 명령을 실행시킬 수 있다.
② 새롭게 생성되는 파일이나 디렉터리는 umask에 의해 결정되는 디폴트 권한으로 생성된다.
③ Stickybit가 설정된 디렉터리는 해당 디렉터리 내의 파일을 임의대로 삭제할 수 없고, root와 소유자에게 삭제 변경 권한이 부여된다.

④ SetGID 명령은 chmod 명령에서 ‘chmod 1755 setgid_program’과 같이 1000번대 인자를 주어 설정할 수 있다.

정답 체크
(4) ‘chmod 2755 setgid_program’으로 해야 한다.
오답 체크
(1) 8진수로 4000으로 표현한다. 사용자가 실행 파일의 사용자 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.
(2) 파일은 666, 디렉토리는 777이 디폴트이다.
(3) 8진수로 1000으로 표현한다. 디렉토리에 sticky bit가 설정되면 디렉토리 안의 파일들은 파일 소유자, 디렉토리 소유자 또는 관리자(root)만이 수정하거나 삭제할 수 있다.

21. 다음 중 국내 정보보호 관리체계 및 인증 제도에 대한 설명으로 옳지 않은 것은?
① 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 ‘관리체계 수립 및 운영’, ‘보호대책 요구사항’의 2개 영역에서 80개의 인증 기준을 적용받게 된다.
② 관리체계 수립 및 운영은 관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선의 4개 분야 16개 인증 기준으로 구성된다.
③ ISMS 인증은 의무 대상자가 아니더라도 자발적으로 신청하여 인증심사를 받을 수 있다.
④ 정보보호 관리체계를 유지하는 기업을 대상으로, 정보보호 수준을 측정하여 ‘우수’, ‘최우수’ 등급을 부여하는 정보보호 등급제 인증제도가 운영되고 있다.

정답 체크
(1) ‘관리체계 수립 및 운영’, ‘보호대책 요구사항’, ‘개인정보 처리단계별 요구사항’의 3개 영역에서 102개의 인증 기준을 적용받게 된다.
오답 체크
(2) 관리체계 기반 마련(6), 위험관리(4), 관리체계 운영(3) 관리체계 점검 및 개선(3)으로 구성된다.
(3) 의무 대상자를 제외하고 자발적 참여를 권장한다.
(4) 등급을 받으면 ISMS-P가 일부 면제된다.

22. 다음 중 접근 통제의 성격이 가장 다른 것은?
① 보안클래스를 보안의 중요도에 따라 비교 우위를 가려 이를 선행으로 나열하는 접근 통제이다.
② 주체의 책임과 역할을 기반으로 하는 접근 통제이다.
③ 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이다.
④ 개인의 역할을 기반으로 하는 접근 통제이다.

정답 체크
(1) LBAC에 해당한다.
(3) MAC에 해당한다.
오답 체크
(2), (4) RBAC에 해당한다.

23. 다음 중 신뢰 컴퓨팅 기반(Trusted Computing Base, TCB)에 대한 설명으로 가장 거리가 먼 것은?
① TCB의 각 계층은 고유의 보안 정책을 정의하고, 기존의 TCB를 재사용 또는 확장할 수 있다.
② 운영 TCB는 기본적인 보호 환경을 구축하고, 신뢰성 있는 시스템에 필요한 부가적인 사용자 서비스를 제공한다.
③ 일반적으로 컴퓨터의 메인보드에 설치되어 하드웨어 버스를 사용하여 시스템의 다른 부분과 통신한다.
④ 보안 정책의 정확한 적용 능력은 오직 TCB 내의 메커니즘과 보안 정책 관련 정보의 입력에 따른다.

정답 체크
(3) TPM에 해당한다.
오답 체크
(1) TCB 내부에서 발생하는 버그 또는 취약점이 전체 시스템의 보안 속성을 손상시킬 수 있다는 점에서 보안에 중요한 모든 하드웨어, 펌웨어 및 소프트웨어 구성 요소의 집합이다.
(2) 신뢰성있는 컴퓨터 시스템을 위한 기본적인 보호 환경과 추가적 사용자 서비스를 제공하고, 보안정책이 TCB 내의 메커니즘을 통해 정확히 수행될 수 있는 환경을 제공한다.
(4) 보안 정책의 정확한 적용의 능력은 오직 TCP 내의 메커니즘과 보안 정책 관련 정보의 입력에 달려있다.

24. 다음 중 인공지능 보안에 대한 설명으로 가장 옳지 않은 것은?
① 학습 과정에 무작위 오류가 존재하는 노이즈를 고의적으로 추가함으로써 인공지능이 잘못된 판단을 하도록 하는 회피 공격(evasion attack)과 같은 데이터 변조 공격을 수행할 수 있다.
② 수많은 질의를 보내고 산출된 결과를 분석함으로써 인공지능에 사용된 데이터를 추출하는 전도 공격(inversion attack)이 존재한다.
③ 동일한 데이터를 반복 학습함으로써 편향된 성향을 가지도록 하는 재전송 공격(replay attack)이 존재한다.
④ 악의적 데이터를 주입함으로써 정상적인 서비스가 불가능하게 하는 중독공격(poison attack)과 같은 공격 기법이 존재한다.

정답 체크
(3) 편향성(bias)이라고 한다.
오답 체크
(1) 입력 데이터에 최소한의 변조를 가해 머신러닝을 속이는 기법이다.
(2) 머신러닝 모델에 수많은 쿼리를 던진 후 산출된 결과값을 분석해 모델 학습을 위해 사용된 데이터를 추출하는 공격이다.
(4) 의도적으로 악의적인 학습 데이터를 주입해 머신러닝 모델을 망가뜨리는 공격을 의미한다.

25. 다음 중 트래픽 분석(traffic analysis)에 대한 설명으로 가장 옳은 것은?
① 사용자가 보낸 메시지 사본을 획득하여 나중에 그 메시지를 사용하기 위한 목적으로 이용하는 소

극적 공격이다.
② 시스템의 서비스를 느리게 하거나 완전히 차단하는 적극적 공격이다.
③ 송수신되는 데이터를 가로채거나 획득 후 정보를 조작하는 적극적 공격이다.
④ 송수신되는 데이터 자체 외의 다른 정보를 유추하는 소극적 공격이다.

정답 체크
(4) 기밀성(트래픽 분석) 공격이다.
오답 체크
(1) 무결성(replay) 공격이다.
(2) 가용성(DoS) 공격이다.
(3) 무결성(modification) 공격이다.