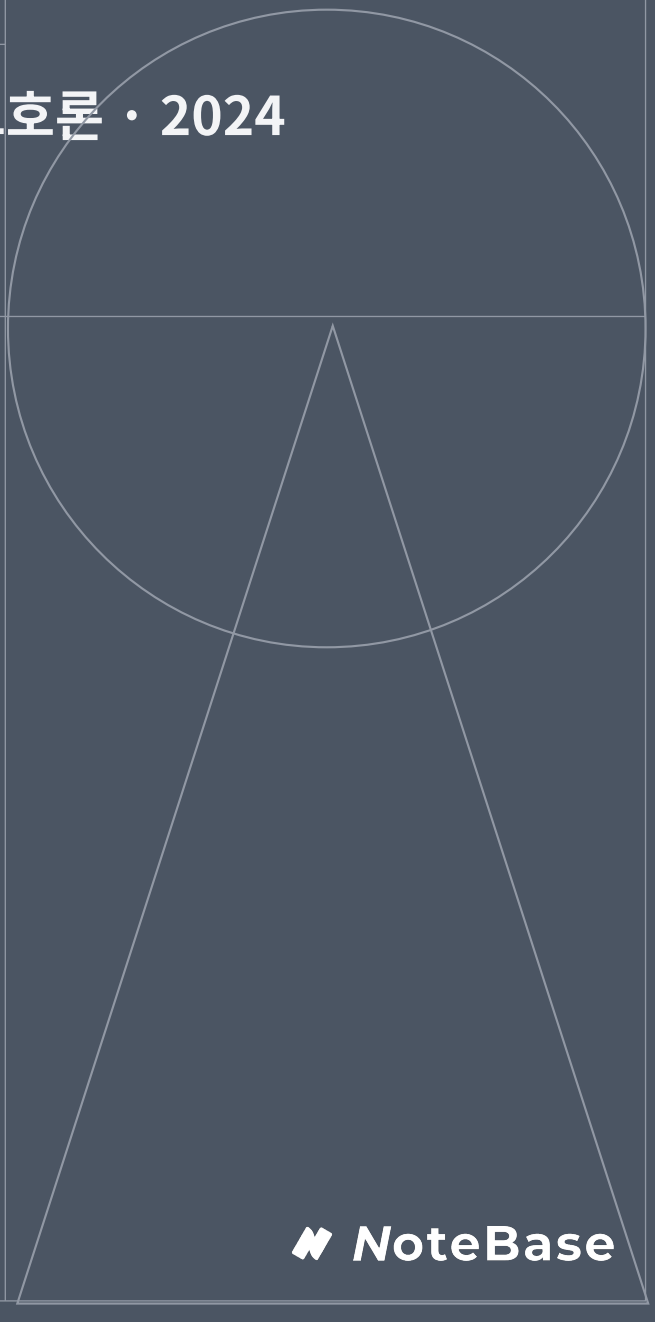
기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2024

공무원/군무원/9급 · 정보보호론 · 2024

1. 멀티 팩터 인증(Multi-Factor Authentication)에서 사용되는 인증 수단과 가장 거리가 먼 것은?
   ① 무엇을 알고 있나(지식)
   ② 어디에 있나(지리적 위치)
   ③ 무엇을 갖고 있나(소유)
   ④ 누구인가(생체 인식)

정답 2번

출제 포인트

다중 요소 인증에서 서로 독립된 고전적 인증 요소인 지식, 소유, 생체 특성을 구분하는 문제이다.

핵심 개념

다중 요소 인증은 서로 다른 종류의 인증 요소를 두 가지 이상 결합하여 사용자를 확인하는 방식이다.
지식 요소는 사용자가 아는 것(비밀번호·PIN), 소유 요소는 사용자가 가진 것(보안 토큰·스마트폰), 생체 요소는 사용자 자체의 특성(지문·얼굴)이다. 지리적 위치는 접속 상황을 평가하는 맥락 정보로 활용될 수 있지만, 이 세 가지 고전적 인증 요소와는 구분된다.

NoteBase

선지별 해설

① X
‘무엇을 알고 있나’를 다중 요소 인증과 가장 거리가 먼 수단으로 보는 것은 틀리다. 올바르게는 비밀번호나 PIN처럼 사용자가 아는 정보를 확인하는 지식 요소이며, 대표적인 인증 요소이다.

② O
‘어디에 있나’는 접속자의 지리적 위치를 확인하는 맥락 정보이다. 위험 기반 인증에 보조적으로 활용될 수는 있지만 지식·소유·생체로 이루어진 고전적 인증 요소 분류에는 포함되지 않으므로 가장 거리가 멀다.

③ X
‘무엇을 갖고 있나’를 다중 요소 인증과 가장 거리가 먼 수단으로 보는 것은 틀리다. 올바르게는 보안 토큰이나 스마트폰처럼 사용자가 가진 물건을 확인하는 소유 요소이며, 대표적인 인증 요소이다.

④ X
‘누구인가’를 다중 요소 인증과 가장 거리가 먼 수단으로 보는 것은 틀리다. 올바르게는 지문이나 얼굴처럼 사용자에게 고유한 생체 특성을 확인하는 생체 요소이며, 대표적인 인증 요소이다.

오답 포인트

②의 지리적 위치도 사용자 확인에 활용될 수 있다는 점 때문에 정식 인증 요소로 착각하기 쉽다. 그러나 이 문항은 활용 가능성보다 고전적인 인증 요소의 분류를 묻고 있으며, 위치는 보조적인 맥락 정보에 해당한다.

다시 나오면 이렇게 판단

선지를 ‘아는 것·가진 것·사용자 자체의 특성’에 각각 대응시킨다. 이 세 범주에 직접 대응하지 않고 접속 환경이나 행동 상황을 나타내면 전통적인 인증 요소가 아닌 보조 정보로 판단한다.

암기 포인트

지식은 아는 것, 소유는 가진 것, 생체는 사용자 자체이며, 위치는 맥락 정보이다.

NoteBase

2. 다음 중 정보 보안의 중요한 3대 요소와 가장 거리가 먼 것은?
① 가용성(Availability)
② 무결성(Integrity)
③ 기밀성(Confidentiality)
④ 중복성(Redundancy)

정답 4번

출제 포인트

정보보안의 3대 핵심 요소인 기밀성·무결성·가용성(CIA)과 그 밖의 개념을 구별하는 문제이다.

핵심 개념

기밀성(Confidentiality): 인가된 사람만 정보에 접근할 수 있도록 하는 성질이다. 키워드는 접근 통제와 정보 유출 방지이다.
무결성(Integrity): 정보가 권한 없이 변경·삭제되지 않고 정확성과 완전성을 유지하는 성질이다. 키워드는 위변조 방지이다.
가용성(Availability): 인가된 사용자가 필요할 때 정보와 시스템을 이용할 수 있는 성질이다. 키워드는 정상 이용과 서비스 지속이다.
이 세 요소의 영문 첫 글자를 따서 CIA 3요소라고 한다.

선지별 해설

① O — 가용성은 인가된 사용자가 필요할 때 정보와 서비스를 사용할 수 있게 보장하는 정보보안의 3대 요소이다.
② O — 무결성은 정보의 무단 변경이나 삭제를 막아 정확성과 완전성을 유지하는 정보보안의 3대 요소이다.
③ O — 기밀성은 비인가자의 정보 접근과 유출을 막는 정보보안의 3대 요소이다.
④ X — 틀린 표현은 '중복성(Redundancy)이 정보보안의 3대 요소이다'라는 부분이다. 중복성은 장애에 대비하여 장비나 데이터를 이중화하는 방법으로 가용성을 높일 수 있지만, CIA 3요소 자체는 아니다. 올바르게는 기밀성·무결성·가용성이 정보보안의 3대 요소이다. 따라서 가장 거리가 먼 것은 ④이다.

오답 포인트

중복성은 시스템 장애 시 서비스를 계속 제공하는 데 도움이 되므로 가용성과 밀접하다. 그러나 보안 목표인 가용성과 그 목표를 달성하는 수단인 중복성을 같은 수준의 3대 요소로 혼동하면 안 된다.

NoteBase

다시 나오면 이렇게 판단

선지가 보안이 달성해야 할 목표인지, 그 목표를 구현하는 수단인지 구분한다. 접근 허용 범위는 기밀성, 정보의 정확성과 변경 방지는 무결성, 필요할 때의 이용 가능성은 가용성으로 판단한다.

암기 포인트

CIA는 기밀성(Confidentiality)·무결성(Integrity)·가용성(Availability)이며, 중복성은 가용성을 높이는 수단이다.

NoteBase

3. 안티바이러스 프로그램에서 시그니처 기반 검출은 무엇을 기반으로 하는 것인가?
① 사용자 행동
② 알려진 바이러스 코드 패턴
③ 네트워크 트래픽
④ 시스템 성능 지표

정답 2번

출제 포인트

안티바이러스의 시그니처 기반 검출이 무엇을 대조하여 악성코드를 찾는지 묻는 문제이다.

핵심 개념

시그니처 기반 검출은 이미 분석된 악성코드에서 추출한 고유한 코드·바이트 패턴 등의 특징값을 검사 대상과 대조하여 일치 여부로 탐지하는 방식이다. 알려진 위협을 빠르고 정확하게 탐지하는 데 유리하지만, 시그니처가 없는 신종·변종 악성코드에는 한계가 있다.
행위 기반 검출은 실행 중인 프로그램이나 사용자의 비정상적인 동작을 관찰하며, 이상 기반 검출은 정상 상태에서 벗어난 네트워크 트래픽이나 시스템 성능 변화를 탐지한다.

선지별 해설

① X — 사용자 행동은 시그니처 기반 검출의 직접적인 대조 대상이 아니다. 틀린 표현은 '사용자 행동'이며, 올바르게는 행위 기반 또는 이상 기반 탐지에서 분석하는 대상이다.
② O — 알려진 바이러스의 코드 패턴을 미리 시그니처로 등록해 두고 검사 대상과 대조하는 것이 시그니처 기반 검출이다.
③ X — 네트워크 트래픽의 양상이나 비정상적 변화는 주로 네트워크 행위·이상 탐지에서 분석한다. 틀린 표현은 '네트워크 트래픽'이며, 올바르게는 '알려진 바이러스 코드 패턴'이다.
④ X — CPU 사용률, 메모리 사용량 같은 시스템 성능 지표의 비정상적 변화는 주로 행위·이상 탐지의 판단 자료이다. 틀린 표현은 '시스템 성능 지표'이며, 올바르게는 '알려진 바이러스 코드 패턴'이다.

오답 포인트

①·③·④도 보안 탐지에 활용될 수 있다는 점이 함정이다. 그러나 '시그니처 기반'이라는 표현이 나오면 일반적인 보안 관찰 자료가 아니라, 사전에 확보한 알려진 악성코드의 고유 패턴과의 일치 여부를 기준으로 판단한다.

NoteBase

다시 나오면 이렇게 판단

‘시그니처’가 제시되면 알려진 악성코드의 코드·바이트 패턴을 대조하는 방식으로 판단한다. 실행 동작은 행위 기반, 정상 범위를 벗어난 트래픽·성능 변화는 이상 기반으로 구분한다.

암기 포인트

시그니처는 ‘알려진 악성코드의 지문’, 행위·이상 탐지는 ‘움직임과 변화’이다.

NoteBase

4. 정보 기술 분야에서 클라우드 서비스 모델에 포함되지 않는 것은?
① PaaS(Platform as a Service)
② SaaS(Software as a Service)
③ RaaS(Role as a Service)
④ IaaS(Infrastructure as a Service)

정답 3번

출제 포인트

클라우드 서비스 모델의 기본 분류인 IaaS, PaaS, SaaS에 해당하지 않는 용어를 구별하는 문제이다.

핵심 개념

IaaS(Infrastructure as a Service)는 서버, 저장장치, 네트워크 등 IT 인프라를 서비스로 제공한다.
PaaS(Platform as a Service)는 애플리케이션을 개발하고 실행할 수 있는 플랫폼 환경을 서비스로 제공한다.
SaaS(Software as a Service)는 사용자가 설치·관리 부담을 줄이고 완성된 소프트웨어를 이용하게 하는 서비스이다.
클라우드 서비스 모델의 대표적인 기본 분류는 IaaS, PaaS, SaaS이다.

선지별 해설

① O — PaaS(Platform as a Service)는 애플리케이션 개발·실행 플랫폼을 제공하는 클라우드 서비스 모델이다.
② O — SaaS(Software as a Service)는 완성된 소프트웨어를 인터넷을 통해 이용하게 하는 클라우드 서비스 모델이다.
③ X — RaaS(Role as a Service)는 클라우드 서비스 모델의 대표적인 기본 분류에 포함되지 않는다. 틀린 표현은 'Role as a Service가 기본 클라우드 서비스 모델에 포함된다'는 취지이며, 올바르게는 기본 분류를 IaaS, PaaS, SaaS로 구분한다. 따라서 부정형 질문의 정답이다.
④ O — IaaS(Infrastructure as a Service)는 서버·저장장치·네트워크 등의 인프라 자원을 제공하는 클라우드 서비스 모델이다.

오답 포인트

③이 다른 선지처럼 'RaaS' 형태의 약어와 영어 풀이를 갖추고 있어 실제 기본 서비스 모델처럼 보이게 한 것이 함정이다. 또한 문제의 부정형 표현인 '포함되지 않는'을 놓치면 PaaS, SaaS, IaaS 중 하나를 잘못 고를 수 있다.

NoteBase

다시 나오면 이렇게 판단

클라우드 기본 서비스 모델을 묻는 문항에서는 제공 대상이 인프라인지, 개발 플랫폼인지, 완성된 소프트웨어인지 확인하여 각각 IaaS, PaaS, SaaS에 대응한다. 이 세 분류에 들지 않는 용어를 가려 내고, 마지막에 문제의 긍정형·부정형을 확인한다.

암기 포인트

IaaS는 인프라, PaaS는 개발 플랫폼, SaaS는 완성 소프트웨어이다. 기본 3종은 I-P-S이다.

NoteBase

5. BYOD(Bring Your Own Device) 업무 환경에서 필요한 사항으로 가장 적절하지 않은 것은?
① 다양한 애플리케이션의 지원
② 디바이스 암호화
③ 네트워크 접속에 대한 보안
④ 역할기반 인증

정답 1번

출제 포인트

BYOD 업무 환경에서 필요한 핵심 보안 통제와 단순한 업무 편의·호환성 지원을 구분하는 문제이다.

핵심 개념

BYOD는 개인 소유 단말을 업무에 사용하는 방식이므로 단말 분실·도난, 비인가 네트워크 접속, 과도한 업무 권한으로 인한 정보 유출을 통제해야 한다.
디바이스 암호화는 단말에 저장된 데이터를, 네트워크 접속 보안은 통신 및 접속 경로를, 역할기반 인증은 사용자의 역할에 따른 업무 자원 접근을 보호한다. 반면 다양한 애플리케이션 지원은 주로 사용 편의성과 호환성에 관한 사항이므로 이 문항의 핵심 보안 요구사항과는 거리가 있다.

선지별 해설

① X — '다양한 애플리케이션의 지원'은 업무 편의성과 호환성을 높이는 운영상 고려사항이지, BYOD의 정보 유출 위험을 직접 줄이는 핵심 보안 통제는 아니다. 올바르게는 '다양한 단말과 운영체제에 일관된 보안 정책과 관리 통제를 적용하는 기능의 지원'이 필요하다고 표현할 수 있다.
② O — 디바이스 암호화는 개인 단말을 분실하거나 도난당해도 저장된 업무 데이터가 평문으로 노출되는 위험을 줄이므로 필요하다.
③ O — 네트워크 접속에 대한 보안은 비인가 단말·사용자의 접속을 차단하고 통신 과정의 업무 정보를 보호하므로 필요하다.
④ O — 역할기반 인증은 사용자의 직무와 역할에 맞는 권한만 부여하여 불필요한 업무 자원 접근을 제한하므로 필요하다.

오답 포인트

①의 '다양한'이라는 표현 때문에 여러 종류의 개인 단말을 지원하는 BYOD의 필수 요건처럼 보일 수 있다. 그러나 애플리케이션 종류를 늘리는 것과 단말·데이터·접근 권한을 보호하는 것은 별개의 문제이다.

NoteBase

다시 나오면 이렇게 판단

각 선지가 BYOD의 위험을 직접 줄이는지 확인한다. 저장 데이터 보호, 안전한 접속, 최소 권한 부여에 해당하면 핵심 보안 통제이고, 단순한 기능 확대나 사용 편의 제공이면 우선순위가 낮다.

암기 포인트

BYOD 보안의 세 축은 단말 암호화, 안전한 네트워크 접속, 역할별 최소 권한이다.

NoteBase

6. 다음 중 정보보호 기본목표에 대한 설명으로 가장 적절한 것은?

○ 최근 사회적 혼란을 야기하기 위해 국내 정부 부처 웹사이트를 대상으로 (가) 공격이 증가하고 있다. ○ (가) 공격은 대상 웹서비스 중단을 목적으로 서버, 서비스 또는 네트워크에 인터넷 트래픽을 대량으로 보내는 악의적인 사이버 공격으로 정보보호의 기본목표인 (나) 을/를 훼손하기 위한 목적으로 시도되는 공격이다.

① (가): 세션 하이재킹(Session Hijacking)
(나): 기밀성
② (가): SQL 인젝션(SQL injection)
(나): 무결성
③ (가): 분산서비스 공격(Distributed Denial of Service)
(나): 가용성
④ (가): 제로데이 공격(ZeroDay Attack)
(나): 책임추적성

정답 3번

출제 포인트

대량의 인터넷 트래픽으로 웹서비스를 중단시키는 공격의 명칭과, 그 공격이 훼손하는 정보보호 기본목표를 연결하는 문제이다.

핵심 개념

분산서비스 거부 공격(DDoS): 여러 시스템에서 발생시킨 대량의 트래픽이나 요청을 목표 서버·서비스·네트워크에 보내 정상 이용을 방해하는 공격이다. 핵심 키워드는 '대량 트래픽'과 '서비스 중단'이다.
가용성: 정당한 사용자가 필요할 때 정보와 시스템을 이용할 수 있어야 한다는 정보보호의 기본목표이다.
기밀성은 인가되지 않은 정보 공개를 막는 성질이고, 무결성은 정보가 권한 없이 변경·훼손되지 않도록 하는 성질이며, 책임추적성은 행위의 주체와 경위를 추적할 수 있게 하는 성질이다.

NoteBase

선지별 해설

① X — 세션 하이재킹은 이미 성립된 통신 세션을 탈취하는 공격이므로, 제시문의 '대량 트래픽을 보내 서비스 중단'이라는 설명과 다르다. 또한 서비스 이용을 막는 공격이 직접 훼손하는 목표는 기밀성이 아니라 가용성이다. 틀린 표현인 '세션 하이재킹, 기밀성'은 '분산서비스 거부 공격, 가용성'으로 고쳐야 한다.
② X — SQL 인젝션은 입력값에 악의적인 SQL 구문을 삽입하여 데이터베이스를 비정상적으로 조회하거나 조작하는 공격이므로 제시문의 공격이 아니다. 제시문의 서비스 중단은 무결성이 아니라 가용성의 훼손에 해당한다. 틀린 표현인 'SQL 인젝션, 무결성'은 '분산서비스 거부 공격, 가용성'으로 고쳐야 한다.
③ O — 서버·서비스·네트워크에 대량의 인터넷 트래픽을 보내 웹서비스를 중단시키는 공격은 분산서비스 거부 공격이다. 정당한 사용자가 서비스를 이용하지 못하게 하므로 정보보호의 가용성을 훼손한다.
④ X — 제로데이 공격은 보안 패치가 마련되기 전의 알려지지 않았거나 대응되지 않은 취약점을 악용하는 공격이므로, 제시문의 대량 트래픽 공격과 다르다. 서비스 중단이 직접 훼손하는 목표도 책임추적성이 아니라 가용성이다. 틀린 표현인 '제로데이 공격, 책임추적성'은 '분산서비스 거부 공격, 가용성'으로 고쳐야 한다.

오답 포인트

공격 명칭만 보고 고르거나 정보보호 목표만 보고 고르면 혼동하기 쉽다. 이 문항의 결정적 표현은 '인터넷 트래픽을 대량으로 보낸다'와 '웹서비스 중단'이다. 전자는 DDoS를, 후자는 가용성 훼손을 가리키므로 두 매칭이 모두 맞는 ③을 선택해야 한다.

다시 나오면 이렇게 판단

먼저 공격 행위의 핵심 동사를 찾고, 그 결과 정당한 사용자의 이용이 막혔는지를 확인한다. 대량 요청·트래픽으로 자원을 고갈시켜 서비스를 못 쓰게 하면 DDoS이고, 사용할 수 없게 된 결과는 가용성 훼손으로 판단한다.

암기 포인트

DDoS는 대량 트래픽으로 서비스를 마비시키며, 서비스 마비는 가용성 훼손이다.

NoteBase

7. HTTP Request Methods 중 GET 방식에 대한 설명으로 가장 적절한 것은?
① GET 방식은 각 이름과 값을 '&'로 결합하고 URL의 글자수를 제한하고 있지 않다.
② GET 방식은 데이터가 주소 입력란에 표시되기 때문에 보안에 매우 취약한 방식이다.
③ GET 방식은 URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송하는 방식이다.
④ GET 방식의 요청은 브라우저 히스토리에 남지 않는다.

정답 2번

출제 포인트

GET 방식이 요청 데이터를 URL에 표현하는 방법과 그에 따른 노출 특성을 묻는 문제이다.

핵심 개념

GET은 조회할 자원과 요청 데이터를 URL의 쿼리 문자열에 담아 서버로 보내는 HTTP 메서드이다. 쿼리 문자열에서는 이름과 값을 =로 연결하고, 여러 이름=값 쌍은 &로 구분한다. URL은 주소 표시줄, 브라우저 방문 기록, 서버 로그 등에 남을 수 있으므로 비밀번호와 같은 민감정보 전송에 적합하지 않다.

NoteBase

선지별 해설

① X
틀린 표현은 '각 이름과 값을 &로 결합'이다. 올바르게는 각 이름과 값을 =로 연결하고, 여러 이름=값 쌍을 &로 구분한다. 또한 HTTP 규격에 일률적인 URL 글자 수 한도가 없더라도 브라우저·서버 등 구현 환경에는 길이 제한이 있을 수 있다.

② O
GET 요청 데이터는 URL의 쿼리 문자열에 표시될 수 있어 주소 표시줄, 방문 기록, 로그 등에 노출될 수 있다. 따라서 GET 자체는 기밀성을 제공하지 않으며 민감정보 전송에 매우 취약하다는 설명이 적절하다.

③ X
틀린 표현은 'URL에 요청 데이터를 기록하지 않고 HTTP 헤더에 데이터를 전송'한다는 부분이다. 올바르게는 일반적인 GET 요청의 데이터가 URL 뒤의 쿼리 문자열에 기록되어 전송된다. 요청 데이터를 본문에 담는 방식과 혼동하면 안 된다.

④ X
틀린 표현은 '브라우저 히스토리에 남지 않는다'이다. 올바르게는 GET 요청의 URL이 방문 기록에 남을 수 있고, URL에 포함된 쿼리 문자열도 함께 저장될 수 있다.

오답 포인트

①은 &의 역할을 이름과 값의 연결 기호로 바꾸어 놓았다. ③은 URL 쿼리 문자열과 HTTP 헤더를 뒤바꾸었고, ④는 URL이 방문 기록에 남을 수 있다는 GET의 노출 특성을 반대로 서술하였다.

다시 나오면 이렇게 판단

GET 선지는 'URL에 데이터가 보이는가', '방문 기록·로그에 남을 수 있는가', '민감정보에 적합한가'를 기준으로 판단한다. 쿼리 문자열은 이름=값 형식이며 여러 쌍은 &로 구분한다.

암기 포인트

GET은 URL에 노출되고 기록에 남을 수 있다. 이름=값, 쌍과 쌍 사이는 &이다.

NoteBase

8. 다음 중 해시(Hash)에 대한 설명으로 가장 적절하지 않은 것은?

① 해시는 양방향 암호화 기법을 사용하고, 암호화(Encryption)는 단방향 암호화 기법을 사용한다.

② 해시 함수는 임의 길이의 입력값을 받아 고정된 길이의 출력값을 내는 함수이다.

③ 해시 알고리즘은 MD5, SHA-256 등이 존재하며 MD5는 보안상 매우 취약한 알고리즘으로 사용하는 것을 권고하고 있지 않다.

④ 해시는 입력값이 일부만 변경되어도 전혀 다른 결과값을 출력하는 특징을 가지고 있다.

정답 1번

출제 포인트

해시 함수와 암호화의 방향성, 해시값의 길이, 대표 해시 알고리즘의 안전성, 쇄도 효과를 구분하는 문제이다.

핵심 개념

해시 함수는 임의 길이의 입력을 고정 길이의 해시값으로 바꾸는 단방향 함수이다. 원래 입력을 복원하는 용도가 아니라 무결성 확인 등에 사용한다.

암호화는 평문을 암호문으로 바꾸고 정당한 키를 이용해 다시 복호화할 수 있는 가역적 변환이다. 양방향이라는 말은 대칭키·비대칭키의 구분이 아니라 암호화와 복호화가 가능하다는 뜻이다.

쇄도 효과는 입력의 아주 작은 변화가 출력 해시값 전반에 큰 변화를 일으키는 성질이다.

선지별 해설

① X — 해시와 암호화의 방향성을 반대로 설명하였다. 틀린 표현은 '해시는 양방향, 암호화는 단방향'이다. 올바르게는 해시는 단방향 함수이고, 암호화는 키를 이용한 복호화가 가능한 양방향 변환이다.

② O — 해시 함수는 임의 길이의 입력값을 받아 알고리즘별로 정해진 고정 길이의 해시값을 출력한다.

③ O — MD5와 SHA-256은 해시 알고리즘이다. MD5는 충돌 취약점 때문에 보안 목적의 사용을 권장하지 않으므로 설명이 적절하다.

④ O — 입력값의 일부만 바뀌어도 출력 해시값이 크게 달라지는 쇄도 효과를 설명한 것으로 적절하다.

NoteBase

오답 포인트

①의 '양방향'과 '단방향'을 서로 바꿔 놓은 표현이 핵심 함정이다. 암호화의 대칭키 방식과 비대칭키 방식은 키 구성에 관한 구분이며, 암호화 자체가 단방향이라는 뜻이 아니다.

다시 나오면 이렇게 판단

원문 복원이 목적이면 암호화와 복호화의 영역이고, 원문을 복원하지 않은 채 입력의 동일성이나 무결성을 확인하면 해시의 영역으로 판단한다. 이어서 입력 길이와 무관한 고정 길이 출력, 작은 입력 변화에 따른 큰 출력 변화, 오래된 알고리즘의 충돌 취약성을 확인한다.

암기 포인트

해시는 단방향·고정 길이·쇄도 효과, 암호화는 복호화 가능한 양방향 변환이다. MD5는 보안용으로 취약하다.

NoteBase

9. 다음 중 주요정보통신기반시설에 대한 설명으로 가장 적절한 것은?

① 주요정보통신기반시설은 「국가정보원법」에서 관련 근거 조항을 찾을 수 있다.

② 주요정보통신기반시설에 대한 취약점 분석·평가는 주요정보통신기반시설의 관리기관이 직접 수행하는 방법이 유일하다고 할 수 있다.

③ 주요정보통신기반시설로 신규 지정이 된 경우, 지정 후 10개월 이내에 취약점 분석·평가를 실시하여야 한다.

④ 주요정보통신기반시설에 대한 최초의 취약점 분석·평가를 한 후에는 매년 정기적으로 취약점 분석·평가를 실시하여야 한다.

정답 4번

쟁점

이 문제는 주요정보통신기반시설의 취약점 분석·평가에 관한 근거 법률, 수행 주체 및 실시 시기를 묻는 문제이다. 핵심은 최초 평가의 기한과 그 이후의 정기 평가 주기를 구별하는 것이다.

용어 풀이

취약점 분석·평가란 주요정보통신기반시설의 관리적·물리적·기술적 취약점을 조사하고 그 위험을 평가하는 절차이다. 관리기관은 해당 주요정보통신기반시설을 관리하는 기관이다.

핵심 구분

「정보통신기반 보호법」 제9조와 같은 법 시행령 제17조가 취약점 분석·평가의 수행 및 시기를 정한다. 주요정보통신기반시설로 지정되면 원칙적으로 지정 후 6개월 이내에 최초 평가를 실시하고, 특별한 사유가 있어 관할 중앙행정기관의 장의 승인을 받은 경우에는 지정 후 9개월 이내에 실시한다. 최초 평가 후에는 매년 평가한다. 관리기관은 전담반을 구성하여 평가할 수 있고, 법에서 정한 전문기관 등에 평가를 수행하게 할 수도 있다.

NoteBase

선지별 해설

① X
주요정보통신기반시설의 지정·보호와 취약점 분석·평가를 직접 규율하는 근거는 「국가정보원법」이 아니라 「정보통신기반 보호법」이다.
틀린 표현: 「국가정보원법」에서 관련 근거 조항을 찾을 수 있다.
올바른 표현: 「정보통신기반 보호법」에서 관련 근거 조항을 찾을 수 있다.

② X
관리기관이 직접 수행하는 방법만 있는 것은 아니다. 관리기관은 전담반을 구성할 수 있고, 한국인터넷진흥원·정보공유·분석센터·정보보호 전문서비스 기업·한국전자통신연구원 등 법정 기관에 분석·평가를 수행하게 할 수도 있다.
틀린 표현: 관리기관이 직접 수행하는 방법이 유일하다.
올바른 표현: 관리기관의 전담반이 수행하거나 법에서 정한 기관에 수행하게 할 수 있다.

③ X
신규 지정 시 최초 취약점 분석·평가는 원칙적으로 지정 후 6개월 이내에 실시한다. 특별한 사유가 있고 관할 중앙행정기관의 장의 승인을 받은 때에도 지정 후 9개월 이내이므로 10개월은 틀리다.
틀린 표현: 지정 후 10개월 이내에 실시하여야 한다.
올바른 표현: 원칙적으로 지정 후 6개월 이내에 실시하며, 특별한 사유와 승인이 있으면 지정 후 9개월 이내에 실시한다.

④ O
최초 취약점 분석·평가를 한 후에는 매년 정기적으로 취약점 분석·평가를 실시하여야 한다. 시설에 중대한 변화가 있거나 관리기관의 장이 필요하다고 판단하면 1년이 되기 전에도 추가로 실시할 수 있다.

오답 포인트

③의 '10개월'을 실제 기한인 '6개월, 예외적으로 9개월'과 혼동하거나, ②에서 관리기관의 책임 주체와 실제 평가 수행 주체를 같다고 보는 것이 함정이다.

다시 나오면 이렇게 판단

주요정보통신기반시설 문항에서는 먼저 「정보통신기반 보호법」을 근거로 잡고, '최초 평가: 6개월 이내, 승인 있는 예외: 9개월 이내, 이후: 매년'의 순서로 판단한다. 수행 방법은 관리기관 전담반과 법정 전문기관 활용이 모두 가능하다고 구분한다.

암기 포인트

주요정보통신기반시설 취약점 평가: 기반보호법, 최초 6개월·예외 9개월·이후 매년이다.

NoteBase

10. 블록체인(Blockchain) 기술에 대한 설명으로 가장 적절한 것은?
① 처리 노드의 다중화
② 중앙 집중식 데이터 관리
③ 데이터 무결성 및 분산 합의
④ 단일 실패 지점(SPOF) 방지

정답 3번

출제 포인트

블록체인의 핵심 특성이 데이터 무결성과 분산 합의에 있다는 점을 구별하는 문제이다.

핵심 개념

블록체인은 여러 참여 노드가 거래 기록을 분산하여 보관하고, 합의 절차를 통해 원장의 유효성과 일관성을 유지하는 분산원장 기술이다. 기록이 블록 단위로 연결되고 참여자들이 동일한 원장을 검증하므로 임의 변경이 어렵고 데이터 무결성을 확보할 수 있다.

선지별 해설

① X
처리 노드의 다중화는 장애 대비를 위한 일반적인 가용성 구성으로도 구현할 수 있으므로 블록체인의 핵심을 가장 정확하게 나타내는 설명은 아니다. '처리 노드의 다중화'보다는 '여러 노드가 원장을 분산 보관하고 검증한다'고 고치는 것이 정확하다.

② X
'중앙 집중식'이라는 표현이 틀렸다. 블록체인은 특정 중앙 관리 주체가 데이터를 단독으로 관리하는 방식이 아니라 여러 참여 노드가 원장을 분산 관리하는 방식이다.

③ O
블록체인은 블록의 연결 구조와 참여 노드의 검증으로 데이터의 임의 변경을 어렵게 하며, 합의 알고리즘을 통해 분산된 노드들이 원장의 유효성과 상태에 합의한다. 따라서 데이터 무결성 및 분산 합의가 가장 적절한 설명이다.

④ X
단일 실패 지점 방지는 분산 구조에서 얻을 수 있는 효과이지만, 블록체인 기술 자체의 핵심 작동 원리를 가장 직접적으로 설명한 선지는 아니다. '단일 실패 지점 방지'만으로 설명하기보다는 '분산 저장과 합의를 통해 무결성과 일관성을 유지하며, 그 결과 단일 실패 지점의 위험도 낮춘다'고 고치는 것이 정확하다.

NoteBase

오답 포인트

①과 ④는 블록체인의 분산 구조에서 나타날 수 있는 특성이나 효과이므로 그럴듯하다. 그러나 문제는 '가장 적절한' 설명을 묻고 있으므로, 일반적인 시스템 다중화나 파생 효과보다 블록체인의 핵심 원리인 무결성 확보와 분산 합의를 직접 제시한 ③을 선택해야 한다.

다시 나오면 이렇게 판단

블록체인 선지는 '분산원장·변경 곤란·참여 노드의 합의'가 함께 드러나는지를 먼저 확인한다. '중앙 집중식'은 반대 개념이며, 다중화나 장애 방지는 핵심 원리보다 일반적 특성 또는 파생 효과에 가깝다.

암기 포인트

블록체인의 핵심은 분산 저장, 데이터 무결성, 분산 합의이다.

NoteBase

11. 다음 중 공격과 이에 대한 대응 방안의 연결 중 가장 적절하지 않은 것은?
① sniffing – encryption
② spoofing – authentication
③ insecure defaults – reconfiguration
④ code injection – masquerading

정답 4번

출제 포인트

보안 공격의 작동 방식과 그 공격을 직접 예방·완화하는 대응 방안이 올바르게 연결되었는지를 묻는 문제이다.

핵심 개념

sniffing은 통신 중인 데이터를 몰래 가로채는 공격이고, encryption은 가로챈 데이터의 내용을 알아볼 수 없게 한다.
spoofing과 masquerading은 공격자가 다른 사용자나 시스템인 것처럼 신원을 속이는 공격이며, authentication은 상대의 신원을 확인하여 이를 막는다.
insecure defaults는 기본 계정·암호·권한·서비스 등이 안전하지 않게 설정된 상태이고, reconfiguration은 이를 안전한 값으로 다시 설정하는 대응이다.
code injection은 검증되지 않은 입력에 명령이나 코드를 넣어 실행시키는 공격이며, 입력값 검증·허용 목록·매개변수화된 질의 등으로 대응한다.

선지별 해설

① O — sniffing으로 통신 내용을 가로채더라도 encryption이 적용되어 있으면 평문 내용을 바로 해독하기 어렵다. 따라서 적절한 연결이다.
② O — spoofing은 공격자가 신원이나 출처를 속이는 공격이므로 authentication으로 사용자·시스템의 신원을 검증하는 것이 적절하다.
③ O — insecure defaults는 출고·설치 시의 취약한 기본 설정을 그대로 사용하는 문제이므로 기본 암호 변경, 불필요한 서비스 비활성화, 권한 축소 등의 reconfiguration이 적절하다.
④ X — 틀린 부분은 code injection의 대응 방안을 masquerading으로 연결한 것이다. masquerading은 정당한 사용자로 위장하는 공격 유형이지 대응 방안이 아니다. 올바르게는 code injection — 입력값 검증·허용 목록·매개변수화된 질의 등의 연결이다.

NoteBase

오답 포인트

④의 masquerading을 보안 기능처럼 오해하기 쉽지만, 이는 공격자가 타인의 신분을 가장하는 공격이다. 공격과 공격을 연결한 ④만 대응 관계가 성립하지 않는다.

다시 나오면 이렇게 판단

왼쪽 용어가 노리는 보안 속성과 오른쪽 용어의 기능을 대응시킨다. 도청에는 기밀성을 위한 암호화, 신원 위조에는 인증, 취약한 기본 설정에는 재설정, 코드 삽입에는 입력·명령 실행 통제가 대응한다.

암기 포인트

도청은 암호화, 위조는 인증, 기본값은 재설정, 삽입은 입력 검증이다. masquerading은 방어가 아니라 위장 공격이다.

NoteBase

12. 다음 중 SSO(Single Sign-On) 인증에 대한 설명으로 가장 적절하지 않은 것은?

① 1회 사용자 인증으로 다수의 애플리케이션 및 웹사이트에 대한 사용자 로그인을 허용하는 인증방식이다.

② ID와 패스워드를 개별적으로 관리하는 위험성을 해소하고, 중앙 집중 관리를 통해 보안을 강화하는 것을 목적으로 한다.

③ 관리자에게는 관리의 편의성을 제공하지만, 사용자에게는 사용의 편의성을 충분히 제공하지 못하는 단점이 있다.

④ SSO 서버가 단일 실패 지점(Single Point of Failure)이므로, 해당 서버가 침해되면 모든 서버의 보안이 위협받을 수 있는 위험이 있다.

정답 3번

출제 포인트

SSO의 정의와 장점, 중앙 집중 관리 효과, 단일 실패 지점 및 침해 확산 위험을 구분하는 문제이다.

핵심 개념

SSO(Single Sign-On)는 한 번의 사용자 인증으로 서로 연계된 여러 애플리케이션이나 웹사이트를 이용하게 하는 통합 인증 방식이다. 사용자는 반복 로그인을 줄일 수 있고, 관리자는 계정과 인증 정책을 중앙에서 관리할 수 있다. 다만 인증 기능이 한곳에 집중되므로 SSO 서버 장애가 전체 서비스 접근 장애로 이어질 수 있고, 인증 정보가 침해되면 연계 서비스로 피해가 확산될 수 있다.

NoteBase

선지별 해설

① O - 한 번의 사용자 인증으로 다수의 연계 애플리케이션과 웹사이트에 로그인할 수 있게 하는 방식은 SSO의 정의에 해당한다.
② O - 서비스마다 ID와 패스워드를 따로 관리할 때 생기는 중복·관리 부실 위험을 줄이고, 계정과 인증 정책을 중앙에서 통제하여 보안을 강화할 수 있다.
③ X - 틀린 표현은 '사용자에게는 사용의 편의성을 충분히 제공하지 못한다'이다. 실제로는 관리자의 중앙 집중 관리 편의성뿐 아니라 사용자에게도 반복 인증과 다수의 비밀번호 관리 부담을 줄이는 편의성을 제공한다.
④ O - SSO 서버는 인증이 집중되는 단일 실패 지점이 될 수 있다. 해당 서버가 장애를 일으키면 연계 서비스 이용이 중단될 수 있고, 침해되면 인증 정보나 권한이 악용되어 여러 연계 서버의 보안이 함께 위협받을 수 있다.

오답 포인트

③은 SSO가 관리자에게만 편리하다고 범위를 축소한 것이 함정이다. SSO의 대표적 장점은 관리자 측의 중앙 집중 관리와 사용자 측의 한 번 인증이라는 두 편의성을 함께 제공하는 데 있다.

다시 나오면 이렇게 판단

SSO 선지는 '한 번 인증·여러 서비스 이용', '중앙 집중 관리', '사용자와 관리자 모두의 편의성'을 장점으로 판단하고, '단일 실패 지점·침해 시 피해 확산'을 단점으로 판단한다.

암기 포인트

SSO는 한 번 인증으로 여러 서비스에 접속한다. 장점은 사용자 편의성과 중앙 관리이고, 단점은 장애 집중과 침해 확산이다.

NoteBase

13. 다음 중 리눅스(LINUX)의 특징에 대한 설명으로 가장 적절한 것은?

① 리눅스는 싱글유저 환경을 지원하는 시스템이다.

② 리눅스는 사용자가 쉘(Shell) 없이 직접 커널에 접속하여 명령을 수행하는 구조이다.

③ 리눅스는 다양한 쉘(Shell)을 제공하며, 쉘은 리눅스에서 명령어와 프로그래밍을 실행할 때 사용되는 인터페이스 역할을 한다.

④ 리눅스는 보안성을 강화하기 위해 프로그램 소스코드를 외부에 공개하지 않고 있다.

정답 3번

출제 포인트

리눅스의 다중 사용자 구조, 셸의 역할, 오픈 소스라는 핵심 특징을 구분하는 문제이다.

핵심 개념

리눅스는 여러 사용자가 자원을 공유할 수 있는 다중 사용자 운영체제이며, 소스 코드가 공개된 오픈 소스 운영체제이다.
셸은 사용자의 명령을 해석하여 커널이 처리할 수 있도록 전달하고, 프로그램 실행을 지원하는 사용자 인터페이스이다.
커널은 하드웨어와 시스템 자원을 관리하는 운영체제의 핵심 부분이다.

NoteBase

선지별 해설

① X
틀린 표현은 '싱글유저 환경을 지원하는 시스템'이다. 리눅스는 기본적으로 여러 사용자가 동시에 시스템 자원을 이용할 수 있도록 설계된 다중 사용자 운영체제이다. 올바르게는 '리눅스는 다중 사용자 환경을 지원하는 시스템이다'라고 해야 한다.

② X
틀린 표현은 '셸 없이 직접 커널에 접속하여 명령을 수행한다'이다. 사용자는 일반적으로 셸을 통해 명령을 입력하고, 셸이 그 명령을 해석하여 커널에 필요한 처리를 요청한다. 올바르게는 '사용자는 셸을 인터페이스로 사용하여 명령을 수행한다'라고 해야 한다.

③ O
리눅스는 Bash 등 다양한 셸을 제공한다. 셸은 명령어를 해석하고 프로그램을 실행하도록 연결하는 사용자와 운영체제 사이의 인터페이스 역할을 한다.

④ X
틀린 표현은 '보안성을 강화하기 위해 프로그램 소스 코드를 외부에 공개하지 않는다'이다. 리눅스는 소스 코드가 공개되어 누구나 검토하고 수정·배포할 수 있는 오픈 소스 운영체제이다. 올바르게는 '리눅스는 프로그램 소스 코드를 공개하는 오픈 소스 방식이다'라고 해야 한다.

오답 포인트

②는 사용자와 커널 사이에 있는 셸을 생략한 표현이고, ④는 오픈 소스와 비공개 소스를 뒤바꾼 표현이다. 또한 ①의 '싱글유저'는 리눅스의 대표적 특징인 다중 사용자 환경과 반대되는 말이다.

다시 나오면 이렇게 판단

리눅스의 특징을 묻는 선지는 '다중 사용자', '셸을 통한 명령 해석', '오픈 소스'라는 세 기준으로 판단한다. 사용자 명령의 흐름은 사용자 → 셸 → 커널로 구분한다.

암기 포인트

리눅스는 다중 사용자·다중 셸·오픈 소스이며, 셸은 사용자와 커널을 연결한다.

NoteBase

14. 정보보호의 설명 중 가장 적절하지 않은 것은?
① 위험 평가(Risk Assessment)의 목적은 조직에 잠재적인 위험 요인을 식별하고 분석하는 것이다.
② 가상 사설망(VPN, Virtual Private Network)은 안전한 원격 접속 및 데이터 전송을 목적으로 한다.
③ 키로거(Keylogger)의 위협은 암호화된 키 입력 사용으로 대응할 수 있다.
④ 블랙햇 해커(Black Hat Hacker)는 공인된 보안 전문가를 지칭한다.

정답 4번

출제 포인트

위험 평가, VPN, 키로거 대응, 해커 유형의 기본 개념을 구분하고 정보보호에 관한 설명 중 적절하지 않은 것을 찾는 문제이다.

핵심 개념

위험 평가는 조직의 자산에 영향을 줄 수 있는 위협과 취약성 등 잠재적 위험 요인을 식별·분석하여 위험 수준을 판단하는 과정이다.
VPN은 공용 네트워크를 통해서도 암호화된 가상 통신 경로를 구성하여 원격 접속과 데이터 전송을 보호하는 기술이다.
키로거는 사용자의 키 입력을 몰래 기록하는 악성 프로그램 또는 장치이며, 보안 키보드나 키 입력 암호화 등으로 위험을 줄일 수 있다.
블랙햇 해커는 악의적 목적이나 불법적 이익을 위해 시스템을 공격하는 사람이고, 화이트햇 해커는 허가를 받아 취약점을 점검하고 보안을 강화하는 윤리적 보안 전문가이다.

NoteBase

선지별 해설

① O — 위험 평가는 조직에 잠재된 위협·취약성 등의 위험 요인을 식별하고 분석하여 위험의 크기와 대응 우선순위를 판단하는 과정이므로 적절한 설명이다.
② O — VPN은 암호화된 가상 통신 경로를 이용하여 원격 접속과 데이터 전송을 보호하므로 적절한 설명이다.
③ O — 키 입력을 암호화하면 키로거가 가로챈 입력값을 그대로 해석하기 어려워지므로 키 입력 암호화는 키로거 위협에 대한 대응 수단이 될 수 있다.
④ X — 틀린 표현은 '블랙햇 해커는 공인된 보안 전문가'이다. 블랙햇 해커는 악의적·불법적으로 시스템을 공격하는 사람이며, 공인된 보안 전문가를 가리키는 표현으로는 화이트햇 해커가 적절하다.

오답 포인트

④는 '해커'라는 공통 명칭 때문에 블랙햇과 화이트햇을 바꾸어 제시한 선지이다. 블랙햇의 핵심은 악의적·비인가 공격이고, 화이트햇의 핵심은 허가받은 보안 점검이라는 차이를 구분해야 한다.

다시 나오면 이렇게 판단

정보보호 용어 문제에서는 목적과 행위의 정당성을 기준으로 판단한다. 위험 평가는 위험의 식별·분석, VPN은 암호화된 통신 경로, 키로거는 키 입력 탈취, 화이트햇은 허가받은 방어 활동, 블랙햇은 악의적 공격에 대응한다.

암기 포인트

화이트햇은 허가받은 보안 전문가, 블랙햇은 악의적 공격자이다.

NoteBase

15. 운영체제/보안에서 레이스 컨디션(race condition)에 대한 설명으로 가장 적절한 것은?
① 경쟁 상대를 물리치기 위한 공격
② 네트워크 경쟁자의 성능을 측정하는 과정
③ 컴퓨터의 처리 속도를 최적화하기 위한 테크닉
④ 비동기적으로 실행되는 프로세스들 사이의 동기화에서 문제 발생

정답 4번

출제 포인트

레이스 컨디션의 원인이 비동기적으로 실행되는 프로세스나 스레드의 실행 순서와 공유 자원 접근 타이밍에 있음을 묻는 문제이다.

핵심 개념

레이스 컨디션은 둘 이상의 프로세스나 스레드가 공유 자원에 동시에 접근할 때, 실행 순서나 타이밍에 따라 결과가 달라지거나 오류가 발생하는 상태이다. 임계 구역에 상호 배제와 적절한 동기화를 적용하여 예방한다.

선지별 해설

① X
- 틀린 표현은 '경쟁 상대를 물리치기 위한 공격'이다. 여기서 race는 상대와 벌이는 경쟁이나 공격을 뜻하지 않는다. 올바르게는 여러 실행 주체가 공유 자원에 접근하는 순서와 타이밍 때문에 결과가 달라지는 동시성 문제이다.

② X
- 틀린 표현은 '네트워크 경쟁자의 성능을 측정하는 과정'이다. 이는 레이스 컨디션의 정의와 관계가 없다. 올바르게는 네트워크나 시스템의 성능 측정은 벤치마킹 또는 성능 시험에 해당한다.

③ X
- 틀린 표현은 '컴퓨터의 처리 속도를 최적화하기 위한 테크닉'이다. 레이스 컨디션은 최적화 기법이 아니라 동기화가 부족할 때 발생하는 오류 상태이다. 올바르게는 상호 배제, 락 등의 동기화 기법으로 레이스 컨디션을 방지한다.

④ O
- 비동기적으로 실행되는 프로세스들 사이의 동기화가 적절하지 않으면 공유 자원의 접근 순서에 따라 결과가 달라질 수 있으므로 레이스 컨디션이 발생한다.

NoteBase

오답 포인트

race라는 단어를 일반적인 경쟁이나 공격으로 해석하거나, 병렬 실행을 처리 속도 향상과만 연결하는 것이 함정이다. 핵심은 속도가 아니라 공유 자원에 접근하는 실행 순서와 타이밍이다.

다시 나오면 이렇게 판단

‘여러 프로세스·스레드’, ‘공유 자원’, ‘실행 순서나 타이밍에 따라 결과 변화’, ‘동기화 부족’이 함께 제시되면 레이스 컨디션으로 판단한다.

암기 포인트

레이스 컨디션은 속도 경쟁이 아니라 공유 자원 접근 순서 경쟁이다.

NoteBase

16. PKI에서 발급하는 전자 인증서를 보유한 주체로 가장 적절한 것은?
① 사용자 또는 장치
② 인증 기관(CA)
③ 등록 기관(RA)
④ 키 분배 센터

정답 1번

출제 포인트

PKI에서 전자 인증서를 보유하는 최종 개체와 인증서의 발급·등록을 담당하는 기관의 역할을 구별하는 문제이다.

핵심 개념

사용자 또는 장치는 자신의 공개키와 신원 정보를 연결한 전자 인증서를 발급받아 사용하는 최종 개체이다.
인증 기관(CA)은 신청자의 공개키와 신원 정보를 인증하고 전자서명한 인증서를 발급·관리하는 신뢰 기관이다.
등록 기관(RA)은 인증서 신청자의 신원을 확인하고 등록 절차를 처리하여 CA의 인증서 발급을 지원한다.
키 분배 센터(KDC)는 주로 대칭키 기반 환경에서 통신 주체에게 비밀키나 세션키를 안전하게 분배하는 기관이다.

NoteBase

선지별 해설

① O
사용자 또는 장치는 CA가 발급한 전자 인증서를 보유하고 인증·전자서명 등에 사용하는 인증서의 최종 주체이므로 가장 적절하다.

② X
틀린 표현은 '인증 기관(CA)'이다. CA도 신뢰 체계를 위해 자체 인증서를 가질 수 있지만, 이 문항에서 묻는 발급 인증서의 보유 주체가 아니라 인증서를 발급하고 관리하는 기관에 해당한다. 올바르게는 '인증서를 발급·관리하는 기관'이다.

③ X
틀린 표현은 '등록 기관(RA)'이다. RA는 인증서를 보유하는 최종 주체가 아니라 신청자의 신원을 확인하고 등록 정보를 CA에 전달하여 발급을 지원한다. 올바르게는 '인증서 신청자의 등록과 신원 확인을 담당하는 기관'이다.

④ X
틀린 표현은 '키 분배 센터'이다. 키 분배 센터는 전자 인증서의 보유 주체가 아니라 주로 대칭키 또는 세션키를 통신 주체에게 분배한다. 올바르게는 '비밀키나 세션키를 분배하는 기관'이다.

오답 포인트

②와 ③도 PKI에 관여하는 기관이어서 인증서의 '보유 주체'로 착각하기 쉽다. 그러나 CA는 발급·관리, RA는 신원 확인·등록 지원을 담당하며, 인증서를 발급받아 실제로 사용하는 최종 개체는 사용자 또는 장치이다.

다시 나오면 이렇게 판단

문장에서 요구하는 역할 동사를 먼저 확인한다. '보유·사용'이면 사용자나 장치, '발급·서명·관리'이면 CA, '신원 확인·등록'이면 RA, '대칭키·세션키 분배'이면 KDC로 판단한다.

암기 포인트

사용자·장치는 인증서 보유, CA는 발급, RA는 등록 확인, KDC는 키 분배이다.

NoteBase

17. 다음 중 생체인증(바이오) 시스템의 정확도(또는 성능측정)에 대한 설명으로 가장 적절하지 않은 것은?

① FRR(False Rejection Rate)은 시스템에 등록된 사용자가 사용 시 본인임을 확인하지 못하고 인증을 거부하는 오류로 Type 1 Error로 불리기도 한다.

② FAR(False Acceptance Rate)은 인증 권한이 없는 사용자가 인증을 시도했을 때 성공하는 경우를 의미하며 FAR에 비해 FRR이 높은 것은 정보보호 측면에서 더 심각한 문제가 될 수 있다.

③ CER(Crossover Error Rate)은 FAR과 FRR이 그리는 곡선의 교차점을 말한다.

④ 생체인증(바이오) 시스템은 CER이 낮을수록 정확한 시스템이다.

정답 2번

출제 포인트

생체인증 시스템의 FRR, FAR, CER의 의미와 각 오류가 보안성·사용 편의성에 미치는 영향을 구별하는 문제이다.

핵심 개념

FRR(False Rejection Rate, 오거부율): 등록된 정당한 사용자를 잘못 거부하는 비율이다. 값이 높으면 주로 사용 편의성이 떨어진다.

FAR(False Acceptance Rate, 오인식률·오수락률): 권한이 없는 사용자를 잘못 받아들이는 비율이다. 값이 높으면 침입을 허용할 수 있어 보안상 더 심각하다.

CER(Crossover Error Rate, 교차오류율): 임계값을 조절할 때 FAR과 FRR이 같아지는 교차점의 오류율이다. 값이 낮을수록 두 오류를 함께 낮게 유지할 수 있으므로 시스템의 정확도가 높다.

NoteBase

선지별 해설

① O — FRR은 등록된 사용자를 본인이 아닌 것으로 잘못 판단하여 인증을 거부하는 오류이다. 정당한 사용자를 거부한다는 점에서 제1종 오류(Type I Error)라고도 한다.
② X — FAR을 권한 없는 사용자의 인증이 성공하는 비율이라고 설명한 부분은 맞지만, ‘FAR에 비해 FRR이 높은 것이 정보보호 측면에서 더 심각하다’는 부분이 틀렸다. 올바르게는 FRR보다 FAR이 높은 것이 비인가자를 허용하므로 정보보호 측면에서 더 심각하며, FRR의 증가는 주로 사용 편의성 저하와 관련된다.
③ O — CER은 임계값 변화에 따라 그린 FAR 곡선과 FRR 곡선이 만나 두 오류율이 같아지는 교차점의 오류율이다.
④ O — CER이 낮다는 것은 FAR과 FRR이 같아지는 수준 자체가 낮다는 뜻이므로 생체인증 시스템의 전반적인 정확도가 높다고 평가한다.

오답 포인트

②는 FAR의 정의를 정확하게 제시한 뒤 보안상 위험한 오류를 FRR로 바꾸어 놓았다. 비인가자를 받아들이는 FAR은 보안성의 문제이고, 정당한 사용자를 거부하는 FRR은 주로 편의성의 문제라는 구분이 핵심이다.

다시 나오면 이렇게 판단

오류의 대상부터 확인한다. 정당한 사용자를 거부하면 FRR, 비인가자를 받아들이면 FAR이다. 보안 침해 위험은 FAR, 이용 불편은 FRR과 연결하고, 두 오류율이 같아지는 값은 CER이며 낮을수록 정확하다고 판단한다.

암기 포인트

FRR은 진짜를 거부하여 불편, FAR은 가짜를 허용하여 보안 위험, CER은 낮을수록 정확하다.

NoteBase

18. 하드웨어 보안 모듈(HSM)의 사용 목적과 가장 가까운 것은?
① 고속 연산 처리
② 공개키 인프라(PKI) 내의 암호화키 관리
③ 하드웨어 구성 업데이트
④ 바이러스 실시간 탐지

정답 2번

출제 포인트

이 문제는 HSM의 핵심 목적이 암호키를 안전하게 생성·저장·관리하고 보호된 환경에서 암호 연산을 수행하는 데 있음을 묻는다.

핵심 개념

HSM(Hardware Security Module)은 암호키가 장치 외부에 노출되지 않도록 보호하면서 키 생성·저장·사용·폐기와 암호 연산을 수행하는 전용 보안 장치이다.
PKI에서는 인증기관이나 서버의 개인키 등 중요한 암호키를 안전하게 관리하는 용도로 활용된다.

선지별 해설

① X
'고속 연산 처리'는 HSM의 핵심 사용 목적을 지나치게 넓게 표현한 것이다. HSM이 암호 연산을 가속할 수는 있지만, 일반적인 고속 연산 처리가 목적은 아니다. 올바르게는 '암호키를 보호하고 보호된 장치 내부에서 암호 연산을 수행한다'이다.

② O
HSM은 PKI에서 개인키 등 중요 암호키를 안전하게 생성·저장·관리하고, 키를 외부에 노출하지 않은 채 서명·암호화 등의 연산을 수행하는 데 사용된다. 따라서 가장 가까운 사용 목적이다.

③ X
'하드웨어 구성 업데이트'는 HSM의 핵심 목적이 아니다. 올바르게는 '암호키의 생성·저장·사용·폐기 등 수명주기를 안전하게 관리한다'이다.

④ X
'바이러스 실시간 탐지'는 백신이나 엔드포인트 보안 솔루션의 기능이다. 올바르게는 'HSM은 암호키 보호와 안전한 암호 연산을 담당한다'이다.

NoteBase

오답 포인트

①의 '고속 연산'은 HSM이 암호 연산을 빠르게 수행할 수 있다는 부수적 특성을 일반 연산 장치의 목적으로 바꾼 표현이다. HSM의 중심은 속도가 아니라 키의 기밀성과 무결성을 하드웨어로 보호하는 데 있다.

다시 나오면 이렇게 판단

HSM이 나오면 '암호키가 장치 밖으로 노출되지 않도록 보호하는가'를 먼저 확인한다. 키 생성·저장·전자서명·암호 연산과 연결되면 HSM에 해당하고, 일반 연산·업데이트·악성코드 탐지와 연결되면 다른 기능이다.

암기 포인트

HSM은 키를 하드웨어 안에 지키고, 그 안에서 암호 연산을 수행한다.

NoteBase

19. 유닉스의 특수권한인 setuid, setgid, sticky bit에 대한 설명으로 가장 적절한 것은?

① setgid가 붙은 프로그램은 실행 시 소유자의 권한으로 전환된다.

② setuid를 설정하려면 root 권한으로 'chmod 2755 filename'와 같이 설정하면 된다.

③ sticky bit가 설정된 디렉터리는, 누구나 파일을 만들 수 있지만 자신의 소유가 아닌 파일은 삭제할 수 없다.

④ sticky bit는 파일과 디렉터리에 모두 설정할 수 있다.

정답 3번

출제 포인트

이 문제는 Unix 특수 권한인 setuid, setgid, sticky bit의 적용 대상과 실행 효과, 8진수 표기값을 구별하는 문제이다.

핵심 개념

setuid: 실행 파일에 설정하면 실행자의 유효 사용자 ID가 파일 소유자의 ID로 바뀌어 파일 소유자 권한으로 실행된다. 8진수 특수 권한값은 4이다.
setgid: 실행 파일에 설정하면 실행자의 유효 그룹 ID가 파일 소유 그룹의 ID로 바뀌어 그 그룹 권한으로 실행된다. 8진수 특수 권한값은 2이다. 디렉터리에 설정하면 새로 생성되는 파일이 그 디렉터리의 그룹을 상속한다.
sticky bit: 쓰기 가능한 공유 디렉터리에서 파일의 삭제·이름 변경을 파일 소유자, 디렉터리 소유자, root 등으로 제한하는 특수 권한이다. 8진수 특수 권한값은 1이다.

NoteBase

선지별 해설

① X — 틀린 표현은 '소유자의 권한으로 전환된다'이다. setgid가 설정된 실행 파일은 파일 소유자 개인의 권한이 아니라 파일 소유 그룹의 유효 그룹 ID로 실행된다. 파일 소유자의 유효 사용자 ID로 실행되는 것은 setuid이다.
② X — 틀린 부분은 'chmod 2755'이다. 맨 앞의 2는 setgid를 뜻한다. setuid를 설정하려면 맨 앞에 4를 사용하여 'chmod 4755 filename'과 같이 지정한다.
③ O — sticky bit가 설정된 공유 디렉터리에서는 쓰기·실행 권한이 있는 사용자들이 파일을 만들 수 있지만, 일반 사용자는 원칙적으로 자신이 소유하지 않은 파일을 삭제하거나 이름을 바꿀 수 없다. 정확히는 해당 파일의 소유자, 디렉터리 소유자, root 등이 삭제·이름 변경을 할 수 있으므로 선지는 일반 사용자 간의 삭제 제한을 설명한 것이다.
④ X — 틀린 표현은 '파일과 디렉터리에 모두 설정할 수 있다'이다. 현대 Unix/Linux에서 sticky bit는 디렉터리의 삭제·이름 변경을 제한하는 권한 기능으로 사용되며, 일반 파일에 표시되더라도 실질적인 권한 효과가 없다. 올바르게는 sticky bit는 공유 디렉터리에 적용하여 파일 삭제·이름 변경을 제한하는 특수 권한이라고 해야 한다.

오답 포인트

①은 setgid의 '그룹'을 setuid의 '소유자'와 바꾸어 놓았고, ②는 setuid와 setgid의 8진수 값을 바꾸어 놓았다. ③의 sticky bit는 파일 생성을 막는 기능이 아니라 다른 사용자가 소유한 파일의 삭제·이름 변경을 제한하는 기능이라는 점이 핵심이다. ④는 일반 파일에 비트가 표시될 수 있다는 사실과 현대 Unix/Linux에서 실제 권한 효과가 적용되는 대상을 혼동하게 한다.

다시 나오면 이렇게 판단

특수 권한은 먼저 숫자 4-2-1과 효과를 대응한다. setuid는 파일 소유자의 사용자 권한, setgid는 파일 소유 그룹의 그룹 권한, sticky bit는 공유 디렉터리에서 타인 파일의 삭제·이름 변경 제한으로 판단한다.

암기 포인트

특수 권한은 4=setuid(사용자), 2=setgid(그룹), 1=sticky(공유 디렉터리 삭제 제한)이다.

NoteBase

20. 다음에서 설명하는 네트워크 공격방식으로 가장 적절한 것은?

> ○ 네트워크 공격방식의 일종으로 source ip와 destination ip를 똑같게 해서, 공격 대상이 자기 자신에게 응답하도록 하는 공격방식이다.
> ○ 대응방법으로 출발지와 목적지 IP가 동일한 패킷을 방화벽 등에서 차단한다.

① Land Attack
② SMURF Attack
③ PING OF DEATH
④ SYN Flooding

정답 1번

출제 포인트

출발지 IP와 목적지 IP를 공격 대상의 동일한 IP로 설정하여 대상이 자기 자신에게 응답하게 만드는 Land Attack의 특징을 식별하는 문제이다.

핵심 개념

Land Attack: 출발지 IP와 목적지 IP를 모두 공격 대상의 IP로 위조하여 대상이 자신에게 응답하게 만들고 시스템 자원을 소모시키는 서비스 거부 공격이다.
SMURF Attack: 피해자의 IP를 출발지로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 집중되게 하는 공격이다.
PING OF DEATH: 허용 크기를 초과하도록 조작되거나 비정상적으로 분할된 ICMP 패킷을 보내 재조립 과정에서 시스템 장애를 유발하는 공격이다.
SYN Flooding: 다량의 TCP SYN 패킷으로 반쯤 열린 연결을 누적시켜 서버의 연결 자원을 고갈시키는 공격이다.

NoteBase

선지별 해설

① O — Land Attack은 출발지 IP와 목적지 IP를 공격 대상의 동일한 IP로 위조하여 대상이 자기 자신에게 응답하게 만드는 공격이므로 제시문과 일치한다. 출발지와 목적지 IP가 동일한 패킷을 방화벽 등에서 차단하는 대응도 제시된 특징과 맞는다.
② X — 틀린 표현은 'SMURF Attack'이다. SMURF Attack은 피해자의 IP로 출발지를 위조한 ICMP 요청을 브로드캐스트하여 다수의 응답을 피해자에게 집중시키는 공격이다. 제시문의 공격명은 'Land Attack'으로 고쳐야 한다.
③ X — 틀린 표현은 'PING OF DEATH'이다. PING OF DEATH는 크기 제한을 초과하도록 조작되거나 비정상적으로 분할된 ICMP 패킷의 재조립 과정에서 장애를 일으키는 공격이다. 제시문의 공격명은 'Land Attack'으로 고쳐야 한다.
④ X — 틀린 표현은 'SYN Flooding'이다. SYN Flooding은 다량의 TCP 연결 요청을 보내 반쯤 열린 연결을 누적시키고 서버 자원을 고갈시키는 공격이다. 제시문의 공격명은 'Land Attack'으로 고쳐야 한다.

오답 포인트

네 공격이 모두 서비스 거부 공격이라는 공통점 때문에 공격명을 혼동하기 쉽다. 이 문항의 결정적 표현은 'source IP와 destination IP를 똑같게 한다'와 '자기 자신에게 응답한다'이며, 이는 Land Attack만의 식별 단서이다.

다시 나오면 이렇게 판단

출발지 IP와 목적지 IP가 피해자의 동일한 주소이면 Land Attack, 브로드캐스트를 이용한 ICMP 응답 증폭이면 SMURF Attack, 비정상적으로 큰 ICMP 패킷이면 PING OF DEATH, TCP의 반쯤 열린 연결 누적이면 SYN Flooding으로 판단한다.

암기 포인트

Land는 출발지와 목적지가 같은 땅, SMURF는 브로드캐스트 증폭, PING OF DEATH는 초대형 ICMP, SYN Flooding은 반쯤 열린 연결의 범람이다.

NoteBase

21. 블록 암호화 운영모드 중 ECB(Electronic CodeBook) 모드에 대한 설명으로 가장 적절한 것은?

① 가장 단순한 모드로 블록단위로 나누어 순차적으로 암호화하는 구조이다.

② 블록 암호화 모드 중 보안이 가장 강력한 암호화 모드로 평가된다.

③ 동일한 평문 블록이라도 서로 다른 암호문 블록으로 암호화된다.

④ 암호화, 복호화에 쓰이는 키는 서로 다르다는 특징이 있다.

정답 1번

출제 포인트

ECB 모드의 블록 처리 방식과 보안상 특징을 구분하는 문제이다.

핵심 개념

ECB(Electronic CodeBook)는 평문을 일정한 크기의 블록으로 나누고 각 블록을 서로 독립적으로 암호화하는 가장 단순한 블록 암호 운용모드이다. 같은 키를 사용하면 동일한 평문 블록은 동일한 암호문 블록으로 변환되므로 평문의 반복 패턴이 암호문에 드러날 수 있다.

NoteBase

선지별 해설

① O — ECB는 평문을 블록 단위로 나누고 각 블록을 앞뒤 블록과 연계하지 않은 채 독립적으로 암호화한다. 따라서 가장 단순한 운용모드라는 설명이 적절하다.

② X — 틀린 표현은 '보안이 가장 강력한 암호화 모드'이다. ECB는 동일한 평문 블록이 동일한 암호문 블록으로 나타나 반복 패턴이 노출되므로 보안성이 강한 모드로 평가되지 않는다. 올바르게는 'ECB는 구조가 단순하지만 평문의 패턴이 노출될 수 있어 보안성이 낮은 운용모드'이다.

③ X — 틀린 표현은 '동일한 평문 블록이라도 서로 다른 암호문 블록으로 암호화된다'이다. 같은 키로 암호화하면 동일한 평문 블록은 동일한 암호문 블록이 된다. 올바르게는 '동일한 키를 사용하는 ECB에서는 동일한 평문 블록이 동일한 암호문 블록으로 암호화된다'이다.

④ X — 틀린 표현은 '암호화, 복호화에 쓰이는 키는 서로 다르다'이다. ECB는 블록 암호의 운용모드이며 일반적으로 대칭키 블록 암호를 사용하므로 암호화와 복호화에 같은 비밀키를 사용한다. 올바르게는 'ECB의 암호화와 복호화에는 동일한 비밀키를 사용한다'이다.

오답 포인트

ECB의 '각 블록을 독립적으로 처리한다'는 특징을 '동일한 평문도 매번 다른 암호문이 된다'는 뜻으로 오해하기 쉽다. 독립 처리는 블록 간 연쇄가 없다는 뜻이며, 초기화 벡터나 블록별 무작위성이 없으므로 동일 평문 블록의 결과도 동일하다.

다시 나오면 이렇게 판단

ECB가 나오면 '블록별 독립 처리 → 동일 평문 블록은 동일 암호문 블록 → 반복 패턴 노출'의 흐름으로 판단한다. 단순성과 병렬 처리 가능성은 장점이지만 강한 보안성을 뜻하지는 않는다.

암기 포인트

ECB는 독립·동일·노출이다. 블록은 독립적으로 처리되고, 같은 평문은 같은 암호문이 되며, 패턴이 노출된다.

NoteBase

22. 다음 중 정보보호 및 개인정보보호 관리체계 인증체계(ISMS-P)에 대한 설명으로 가장 적절하지 않은 것은?

① 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)가 통합된 관리체계이다.
② 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합한지에 대해 한국인터넷진흥원 또는 인증기관이 증명하는 제도이다.
③ 개인정보보호법에 따라 일정 규모의 개인정보처리자는 정보보호 및 개인정보보호 관리체계 인증을 의무적으로 신청해야 한다.
④ 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항 등으로 구분된다.

정답 3번

쟁점

이 문제는 ISMS-P의 성격, 인증 주체, 의무대상 및 인증기준의 구성을 구별하는 문제이다. 핵심은 개인정보 보호 인증의 임의성과 정보통신망법상 ISMS 인증 의무를 혼동하지 않는 것이다.

용어 풀이

ISMS-P는 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)를 통합하여 정보보호와 개인정보보호 조치 전반을 인증하는 제도이다.

핵심 구분

개인정보 보호법 제32조의2에 따른 개인정보 보호 인증은 개인정보처리자가 받을 수 있는 임의 인증이다. 반면 정보통신망법 제47조 제2항의 요건에 해당하는 정보통신서비스 제공자 등은 ISMS 인증을 받아야 하며, 이 의무대상자는 ISMS와 ISMS-P 중 하나를 선택하여 인증을 취득할 수 있다. 따라서 일정 규모의 개인정보처리자라는 이유만으로 ISMS-P를 의무적으로 신청하는 것은 아니다.

NoteBase

선지별 해설

① O
ISMS-P는 기존 정보보호 관리체계(ISMS)와 개인정보보호 관리체계(PIMS)를 통합하여 운영하는 인증제도이다.

② O
정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합한지를 한국인터넷진흥원 또는 지정된 인증기관이 심사하여 증명하는 제도이다.

③ X
개인정보 보호법은 개인정보처리자의 개인정보 보호 인증을 임의 인증으로 규정하므로, 일정 규모의 개인정보처리자에게 ISMS-P 신청을 일반적으로 강제하지 않는다. 정보통신망법상 ISMS 의무대상자는 인증을 받아야 하지만 ISMS와 ISMS-P 중 하나를 선택할 수 있다.
틀린 표현: 개인정보 보호법에 따라 일정 규모의 개인정보처리자는 ISMS-P 인증을 의무적으로 신청해야 한다.
올바른 표현: 개인정보 보호 인증은 원칙적으로 임의 인증이며, 정보통신망법상 ISMS 의무대상자는 ISMS 또는 ISMS-P 중 하나를 선택하여 인증을 받아야 한다.

④ O
ISMS-P 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항의 세 영역으로 구성된다.

오답 포인트

③은 개인정보처리자의 규모에 따른 다른 법정 의무와 ISMS-P 인증 의무를 섞은 선지이다. 특히 '인증할 수 있다'는 임의 인증과 '인증을 받아야 한다'는 ISMS 의무대상 규정을 구별해야 한다.

다시 나오면 이렇게 판단

ISMS-P 의무 여부를 묻는 경우 먼저 근거 법률과 대상자를 확인한다. 개인정보 보호법상 개인정보 보호 인증은 임의이고, 정보통신망법상 ISMS 의무대상자는 ISMS 또는 ISMS-P를 선택하여 인증을 취득한다는 순서로 판단한다.

암기 포인트

ISMS-P는 ISMS와 PIMS의 통합 인증이며, 개인정보처리자 일반의 의무 인증이 아니다.

NoteBase

23. 패스워드 크래킹(Password Cracking) 방법 중 레인보우 테이블(Rainbow Table)을 이용한 공격 방법에 대한 설명으로 가장 적절한 것은?

① 윈도우 LM(Lan Manager) 패스워드를 몇 분 만에 크래킹하면서 유명해진 해킹방법으로 패스워드와 해시로 이루어진 테이블을 무수히 만들어 놓은 체인을 이용한다.

② 패스워드를 모아서 하나의 사전파일로 만든 후 하나씩 대입하여 패스워드 일치 여부를 확인하는 방법이다.

③ 비밀번호로 사용될 수 있는 모든 문자를 대입하여 패스워드 일치 여부를 확인하는 방법이다.

④ 사전 공격(Dictionary Attack) 기법과 무차별 대입 공격(Brute Force Attack)을 혼합하여 사용하는 방법이다.

정답 1번

출제 포인트

이 문제는 레인보우 테이블 공격을 사전 공격, 무차별 대입 공격, 혼합 공격과 구별하는 문제이다.

핵심 개념

레인보우 테이블 공격: 해시 함수와 환원 함수를 반복해 미리 만든 체인을 이용하여 대상 해시와 대응하는 비밀번호를 찾는 시간-메모리 절충형 공격이다. 계산 결과를 사전에 준비하므로 공격 시점의 연산 시간을 줄일 수 있다.

사전 공격: 사전에 수록한 단어·자주 쓰는 비밀번호 후보를 차례로 시험한다.

무차별 대입 공격: 가능한 문자 조합을 체계적으로 모두 시험한다.

혼합 공격: 사전의 단어에 숫자·기호 등을 덧붙이거나 변형하여 후보를 확장한다.

NoteBase

선지별 해설

① O — 비밀번호 후보에서 생성한 해시·환원 체인을 미리 계산해 둔 레인보우 테이블을 조회하여 해시와 대응하는 비밀번호를 찾는 설명이다. 특히 빠른 계산이 가능하고 솔트가 없는 LM 해시처럼 사전 계산 공격에 취약한 방식에 효과적이라는 점도 타당하다.
② X — 틀린 표현은 '패스워드를 모아서 하나의 사전파일로 만든 후 하나씩 대입'하는 부분이다. 이는 레인보우 테이블 공격이 아니라 사전에 수록한 비밀번호 후보를 차례로 시험하는 사전 공격이다.
③ X — 틀린 표현은 '사용될 수 있는 모든 문자를 대입'하는 부분이다. 이는 레인보우 테이블 공격이 아니라 가능한 모든 문자 조합을 체계적으로 시험하는 무차별 대입 공격이다.
④ X — 틀린 표현은 '사전 공격 기법과 무차별 대입 공격을 혼합'하는 부분이다. 이는 레인보우 테이블 공격이 아니라 사전 단어에 숫자·기호 등의 변형을 결합해 후보를 확장하는 혼합 공격이다.

오답 포인트

②~④는 모두 실제 패스워드 공격 방식이지만 후보를 만들어 대입하는 규칙이 서로 다르다. 이 문제의 함정은 '미리 계산한 해시·환원 체인'이라는 레인보우 테이블의 결정적 특징을 단순한 후보 대입 방식과 혼동하게 하는 데 있다.

다시 나오면 이렇게 판단

'해시값을 미리 계산한 체인·테이블'이면 레인보우 테이블, '사전의 단어 후보'이면 사전 공격, '가능한 모든 조합'이면 무차별 대입 공격, '사전 단어의 변형'이면 혼합 공격으로 판단한다.

암기 포인트

레인보우는 사전 계산 체인, 사전 공격은 단어 목록, 무차별 대입은 모든 조합, 혼합 공격은 단어 변형이다.

NoteBase

24. 다음 중 「개인정보의 안전성 확보조치 기준」에 대한 설명으로 가장 적절한 것은?

① 개인정보 암호화 대상은 주민등록번호, 여권번호, 비밀번호 등이 있으며 모두 복호화가 가능한 암호화 알고리즘을 사용하여 암호화하여야 한다.

② 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

③ 개인정보처리자는 개인정보취급자의 개인정보처리시스템에 대한 접속기록을 6개월 이상 보관·관리하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 1년간 보관하여야 한다.

정답 2번

쟁점

이 문제는 「개인정보의 안전성 확보조치 기준」상 개인정보처리시스템의 암호화, 접근 통제, 접속기록 보관 및 접근 권한 관리에 관한 문제이다. 핵심은 비밀번호의 일방향 암호화와 복호화 가능한 암호화의 차이, 접속기록과 권한 변경 기록의 보관기간을 구별하는 것이다.

용어 풀이

일방향 암호화 = 암호화된 값에서 원래 비밀번호를 복원할 수 없도록 저장하는 방식이다.
접속기록 = 개인정보처리시스템에 누가 언제 접속하여 어떤 업무를 수행했는지 확인할 수 있도록 전자적으로 남긴 기록이다.

NoteBase

핵심 구분

「개인정보의 안전성 확보조치 기준」 제5조부터 제8조까지에 따르면 비밀번호는 복호화되지 않도록 일방향 암호화하여 저장하고, 일정시간 업무처리를 하지 않으면 자동 접속 차단 등의 조치를 하여야 한다. 접속기록은 원칙적으로 1년 이상 보관하되 일정한 경우에는 2년 이상 보관하며, 접근 권한의 부여·변경·말소 내역은 최소 3년간 보관한다.

선지별 해설

① X
비밀번호까지 모두 복호화 가능한 암호 알고리즘으로 암호화하여야 한다는 부분이 틀렸다. 비밀번호는 원문을 복원할 필요가 없고 유출 시 피해가 크므로 복호화되지 않도록 일방향 암호화하여 저장하여야 한다.
틀린 표현: 주민등록번호, 여권번호, 비밀번호 등을 모두 복호화 가능한 암호 알고리즘으로 암호화하여야 한다.
올바른 표현: 주민등록번호와 여권번호 등은 안전한 암호 알고리즘으로 암호화하되, 비밀번호를 저장할 때에는 복호화되지 않도록 일방향 암호화하여야 한다.

② O
개인정보처리자는 불법적인 접근 및 침해사고를 방지하기 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않으면 자동으로 접속이 차단되도록 하는 등 필요한 조치를 하여야 한다.

③ X
접속기록의 일반적인 최소 보관기간을 6개월이라고 한 부분이 틀렸다. 접속기록은 원칙적으로 1년 이상 보관·관리하여야 하며, 5만명 이상의 정보주체에 관한 개인정보를 처리하는 시스템 등 고시가 정한 경우에는 2년 이상 보관·관리하여야 한다.
틀린 표현: 접속기록을 6개월 이상 보관·관리하여야 한다.
올바른 표현: 접속기록은 원칙적으로 1년 이상 보관·관리하고, 고시가 정한 특별한 경우에는 2년 이상 보관·관리하여야 한다.

④ X
접근 권한의 부여·변경·말소 내역 보관기간을 최소 1년이라고 한 부분이 틀렸다. 해당 내역은 기록하고 최소 3년간 보관하여야 한다.
틀린 표현: 그 기록을 최소 1년간 보관하여야 한다.
올바른 표현: 그 기록을 최소 3년간 보관하여야 한다.

오답 포인트

①에서는 모든 암호화 대상에 같은 방식을 적용한다고 오해하기 쉽지만 비밀번호만은 복호화가 불가능한 일방향 암호화가 원칙이다. ③과 ④에서는 서로 다른 기록의 보관기간을 혼동하기 쉽다. 접속기록은 원칙적으로 1년 이상이고, 접근 권한의 부여·변경·말소 기록은 최소 3년이다.

NoteBase

다시 나오면 이렇게 판단

암호화 선지는 먼저 비밀번호인지 확인하여 일방향 암호화 여부를 판단한다. 기록 보관기간 선지는 기록의 종류를 먼저 구분한 뒤 접속기록은 원칙적으로 1년 이상, 권한 부여·변경·말소 내역은 최소 3년이라는 기준을 적용한다. 장시간 미사용 시 자동 접속 차단은 접근 통제 조치로 판단한다.

암기 포인트

비밀번호는 일방향, 미사용은 자동 차단, 접속기록은 원칙 1년, 권한기록은 3년이다.

NoteBase

25. 다음 중 윈도우(Windows) 인증에 대한 설명으로 가장 적절하지 않은 것은?

① LSA(Local Security Authority)는 모든 계정의 로그인을 검증하고 시스템 자원(파일 등)에 대한 접근 권한을 검사한다.

② SAM(Security Account Manager)은 인증된 사용자에게 SID(Security ID)를 부여한다.

③ SRM(Security Reference Monitor)은 SID를 기반으로 파일이나 디렉터리에 접근을 허용할지 결정하고 이에 대한 감사 메시지를 생성하는 역할을 수행한다.

④ 윈도우 인증과정에서 사용되는 주요 서비스로 LSA, SAM, SRM이 있다.

정답 2번

출제 포인트

Windows 인증·접근 통제에서 LSA, SAM, SRM이 각각 담당하는 역할과 SID가 부여되는 시점을 구분하는 문제이다.

핵심 개념

LSA(Local Security Authority): 사용자 로그온을 인증하고 로컬 보안 정책과 권한 정보를 관리하는 보안 기관이다.

SAM(Security Account Manager): 로컬 사용자·그룹 계정 정보를 SAM 데이터베이스에 저장하고 관리한다.

SRM(Security Reference Monitor): 접근 토큰의 SID·권한과 객체의 보안 정보를 대조하여 실제 접근 허용 여부를 집행하고 감사 정보를 생성한다.

SID(Security Identifier): 사용자나 그룹 같은 보안 주체를 식별하는 고유 값이며, 인증할 때 새로 받는 번호가 아니라 계정이나 그룹이 생성될 때 만들어져 계정 정보와 함께 저장된다.

NoteBase

선지별 해설

① O — LSA는 사용자 로그온을 인증하고 로컬 보안 정책 및 권한 정보를 다루는 Windows 보안의 중심 구성 요소이다. 개별 파일 등의 실제 접근 요청은 SRM이 집행하지만, 선지는 LSA의 인증·권한 관리 기능을 포괄적으로 설명한 것으로 볼 수 있다.
② X — 틀린 표현은 '인증된 사용자에게 SID를 부여한다'이다. SID는 인증이 끝난 사용자에게 SAM이 새로 부여하는 값이 아니다. 올바르게는 'SAM은 로컬 계정 정보를 저장·관리하며, SID는 계정이나 그룹을 생성할 때 보안 기관에 의해 생성되어 계정 정보와 함께 저장된다'이다. 로그온 후에는 이미 존재하는 SID가 접근 토큰에 포함되어 권한 판정에 사용된다.
③ O — SRM은 접근 토큰에 담긴 SID·권한과 파일·디렉터리 등 객체의 보안 정보를 대조하여 접근 허용 여부를 결정·집행하고 감사 이벤트를 생성한다.
④ O — LSA, SAM, SRM은 각각 로그온 인증·보안 정책, 로컬 계정 데이터 관리, 객체 접근 통제를 담당하는 Windows 인증·보안 체계의 주요 구성 요소이다.

오답 포인트

②는 SAM이 계정을 관리한다는 사실을 이용해 SID까지 '인증된 사용자에게 부여한다'고 바꾸어 놓았다. 핵심 함정은 담당 구성 요소뿐 아니라 시점이다. SID는 계정 생성 시 만들어지고, 인증 시에는 그 기존 SID가 접근 토큰에 사용된다. 또한 ①의 권한 관리와 ③의 실제 객체 접근 검사는 구분해야 한다.

다시 나오면 이렇게 판단

로그온 인증·보안 정책은 LSA, 로컬 계정 데이터베이스는 SAM, 객체별 접근 허용과 감사는 SRM으로 구분한다. SID에 관한 선지는 '계정 생성 시 생성·저장'인지 '인증 후 새로 부여'인지 시점을 먼저 확인한다.

암기 포인트

LSA는 로그인, SAM은 계정 저장, SRM은 접근 판정이다. SID는 인증 때가 아니라 계정 생성 때 만들어진다.

NoteBase