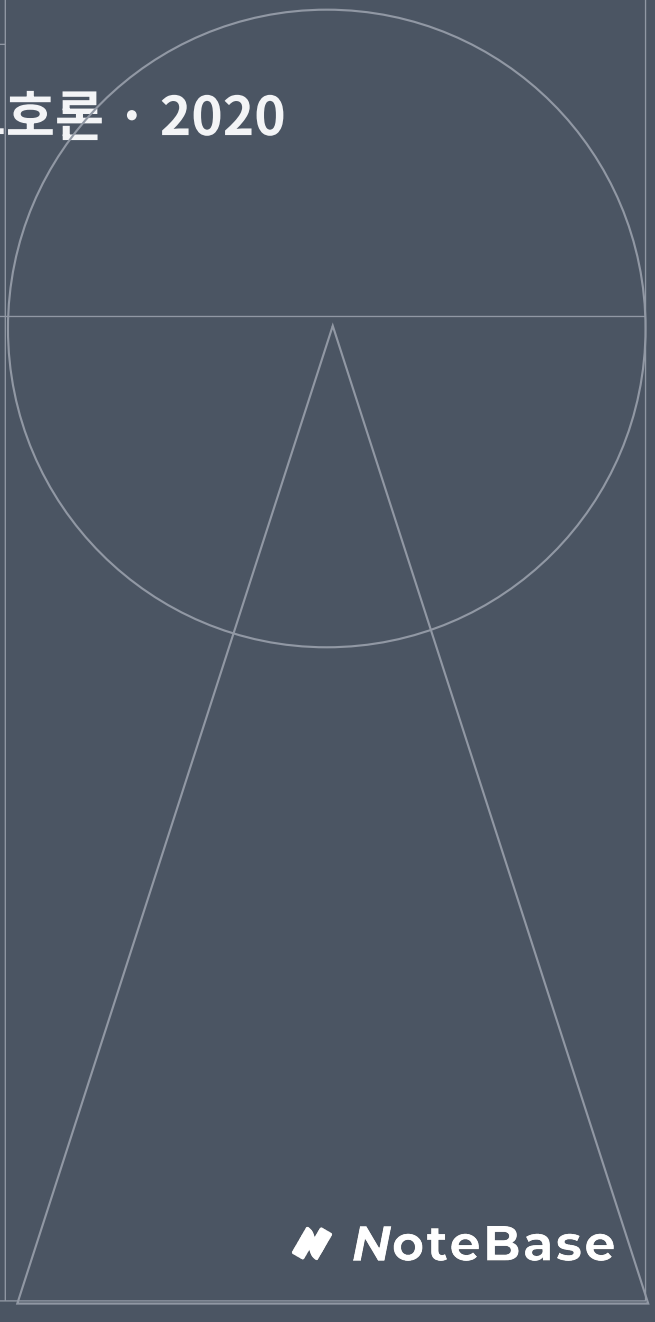
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2020



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2020

공무원/국가직/7급 · 정보보호론 · 2020

문 1. 패스워드 공격에 해당하지 않는 것은?

① 사전 대입 공격

② 이블 트윈 공격

③ 무작위 대입 공격

④ 레인보우 테이블을 이용한 공격

정답 2번

출제 포인트

이 문제는 비밀번호를 추측하거나 대조하는 공격과 무선 네트워크에서 가짜 AP로 사용자를 속이는 공격을 구별하는 문제이다.

핵심 개념

사전 대입 공격은 자주 쓰는 단어 목록을 넣어 비밀번호를 추측하는 방식이다. 키워드는 사전 목록이다.
무작위 대입 공격은 가능한 문자열을 전수 또는 반복 시도로 넣어 비밀번호를 찾는 방식이다. 키워드는 전수 시도이다.
레인보우 테이블 공격은 해시값과 미리 계산된 대응표를 대조해 원문 비밀번호를 찾는 방식이다. 키워드는 사전 계산된 해시표이다.
이블 트윈 공격은 정상 무선 AP와 비슷한 가짜 AP를 만들어 사용자를 연결시키는 무선 네트워크 기만 공격이다. 키워드는 가짜 AP이다.

NoteBase

선지별 해설

① X
사전 대입 공격은 대표적인 패스워드 공격이다. 자주 쓰는 단어, 이름, 사전형 문자열을 대입해 비밀번호를 찾는다.

② O
이블 트윈 공격은 패스워드 자체를 추측하거나 해시를 대조하는 공격이 아니라, 정상 AP로 오인하게 만드는 무선 네트워크 공격이다. 따라서 패스워드 공격에 해당하지 않는다.

③ X
무작위 대입 공격은 가능한 값을 반복 대입해 비밀번호를 찾는 대표적인 패스워드 공격이다. 틀린 표현은 패스워드 공격이 아니라는 취지이다. 올바르게는 가능한 비밀번호 후보를 직접 시도하는 패스워드 공격이다.

④ X
레인보우 테이블을 이용한 공격은 해시와 사전 계산표를 대조해 비밀번호를 역추적하는 패스워드 공격이다. 틀린 표현은 패스워드 공격이 아니라는 취지이다. 올바르게는 해시 기반 패스워드 크래킹 공격이다.

오답 포인트

②의 이블 트윈 공격도 인증정보 탈취로 이어질 수 있어서 패스워드 공격처럼 느껴질 수 있다. 그러나 직접 비밀번호를 추측·대입·역산하는 공격인지, 가짜 무선 환경을 만들어 사용자를 속이는 공격인지 공격 대상을 구분해야 한다.

다시 나오면 이렇게 판단

선지에 사전 목록, 반복 대입, 해시 대조처럼 비밀번호 자체를 맞히는 절차가 나오면 패스워드 공격으로 본다. 반대로 가짜 AP, 피싱 페이지, 중간자 유도처럼 접속 환경을 속이는 방식이면 패스워드 공격과 구분한다.

암기 포인트

사전·무작위·레인보우는 비밀번호를 노리고, 이블 트윈은 무선 접속 환경을 노린다.

NoteBase

문 2. 역할기반 접근제어(RBAC)에 대한 설명으로 옳은 것은?

① 정보의 소유자가 특정 사용자와 그룹에 특정 권한을 부여한다.

② 사용자에게 부여된 권한에 따라 사용자들을 역할로 분류하여 각 사용자에게 하나의 역할만 할당되도록 한다.

③ 역할 및 역할이 수행할 권한을 정의하고, 사용자들을 역할에 할당하는 방식이다.

④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.

정답 3번

출제 포인트

이 문제는 역할기반 접근제어(RBAC)의 구조를 알고, DAC와 MAC의 특징과 구별할 수 있는지를 묻는다.

핵심 개념

RBAC는 직무나 역할을 먼저 정의하고 그 역할에 권한을 연결한 뒤 사용자를 역할에 할당하는 방식이다.
DAC는 정보의 소유자가 사용자나 그룹별 접근 권한을 재량으로 부여하는 방식이다.
MAC는 보안등급과 분류 기준에 따라 중앙에서 강제적으로 접근을 통제하는 방식이다.

선지별 해설

1번: X. "정보의 소유자가 특정 사용자와 그룹에 특정 권한을 부여한다"는 설명은 DAC의 특징이다. RBAC는 소유자가 사용자별로 직접 권한을 주는 방식이 아니라 역할에 권한을 연결하고 사용자를 그 역할에 배정하는 방식이다.
2번: X. 틀린 부분은 "사용자에게 부여된 권한에 따라"와 "하나의 역할만 할당"이다. RBAC는 보통 직무 기준으로 역할을 정의하고 사용자를 역할에 할당하며, 한 사용자에게 여러 역할을 부여할 수 있다.
3번: O. RBAC의 핵심은 역할을 정의하고 각 역할에 필요한 권한을 연결한 뒤 사용자를 해당 역할에 할당하는 것이다. 선지의 설명이 RBAC의 기본 구조와 일치한다.
4번: X. "기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리"에 적합한 것은 MAC이다. RBAC는 조직의 직무 분리와 권한 관리 효율에 강점이 있고, 군사 등급 중심의 강제통제 모델과는 구별된다.

오답 포인트

1번은 소유자 재량이라는 표현 때문에 DAC를 RBAC로 착각하기 쉽고, 4번은 중앙집중형 보안 관리라는 표현 때문에 MAC를 RBAC와 혼동하기 쉽다. 2번은 역할 부여 개수를 하나로 제한하는 문구가 틀린 지점이다.

다시 나오면 이렇게 판단

권한을 누구에게 먼저 묶는지부터 본다. 사용자별로 직접 주면 DAC, 보안등급으로 강제하면 MAC, 역할에 권한을 묶고 사용자를 역할에 넣으면 RBAC이다.

NoteBase

암기 포인트

DAC는 소유자 재량, MAC는 등급 강제, RBAC는 역할 중심이다.

NoteBase

문 3. 정보시스템의 침입자를 속이는 기법의 하나로, 가상의 정보시스템을 만들어 놓고 실제로 공격을 당하는 것처럼 보이게 하여 해커나 스팸, 바이러스를 유인하여 침입자들의 정보를 수집하고 추적하는 역할을 수행하는 것은?

① Honeypot

② IPS

③ ESM

④ DRM

정답 1번

출제 포인트

이 문제는 침입자를 유인해 공격 정보를 수집하는 허니팟과, 차단·통합관리·저작권보호 시스템을 구별하는지를 묻는다.

핵심 개념

Honeypot은 공격자를 일부러 끌어들일 미끼 시스템을 두고 행위와 정보를 관찰·수집하는 기법이다.
IPS는 침입을 실시간으로 탐지하고 차단하는 보안 장비이다.
ESM은 여러 보안 장비와 이벤트를 통합 관리하는 보안 관리 체계이다.
DRM은 디지털 콘텐츠의 사용 권한과 배포를 통제하는 기술이다.

선지별 해설

1번 O: Honeypot은 가상의 시스템이나 미끼 자원을 만들어 실제 공격 대상처럼 보이게 하고, 공격자의 접근 방식과 흔적을 수집·추적하는 기법이므로 지문과 일치한다.
2번 X: IPS는 Intrusion Prevention System으로 비정상 트래픽이나 공격을 탐지해 차단하는 장비이다. 틀린 표현은 '가상의 정보시스템을 만들어 공격을 유인한다'이고, 올바르게는 '공격을 탐지하고 차단한다'이다.
3번 X: ESM은 Enterprise Security Management로 여러 보안 시스템의 로그와 정책을 통합 관리하는 체계이다. 틀린 표현은 '침입자를 유인해 정보를 수집한다'이고, 올바르게는 '보안 이벤트와 장비를 통합 관리한다'이다.
4번 X: DRM은 Digital Rights Management로 문서·음원·영상 같은 디지털 콘텐츠의 열람, 복제, 배포 권한을 제어하는 기술이다. 틀린 표현은 '침입자를 속이는 기법'이고, 올바르게는 '콘텐츠 사용 권한을 통제하는 기술'이다.

오답 포인트

보안 제품이라는 공통점 때문에 IPS와 Honeypot을 같은 범주로 착각하기 쉽다. 그러나 문제의 핵심 단어는 '가상의 시스템', '유인', '정보 수집', '추적'이며, 이 조합은 허니팟의 특징이다.

NoteBase

다시 나오면 이렇게 판단

선지나 지문에 미끼 시스템, 유인, 관찰, 추적이 나오면 Honeypot을 먼저 떠올린다. 탐지·차단이면 IPS, 통합 모니터링과 관리면 ESM, 콘텐츠 권한 통제면 DRM으로 판단한다.

암기 포인트

Honeypot은 미끼, IPS는 차단, ESM은 통합관리, DRM은 저작권·사용권한 통제이다.

NoteBase

문 4. 공개키 기반구조(PKI)에 대한 설명으로 옳지 않은 것은?

① PKI는 인증기관, 등록기관, 저장소, 사용자 등으로 구성된다.

② 인증서의 폐지 여부를 확인하기 위해 인증기관은 인증서 폐지 목록(CRL)을 주기적으로 관리한다.

③ 유효기간 내의 인증서를 가지고 있다면, 사용자는 별도로 CRL을 조사할 필요가 없다.

④ 한 인증기관이 다른 인증기관의 공개키를 검증하는 것이 가능하므로, 사용자는 모든 인증기관의 공개키를 사전에 가지고 있을 필요가 없다.

정답 3번

출제 포인트

이 문제는 PKI의 구성요소와 인증서 유효기간, 인증서 폐지 확인 수단인 CRL의 의미를 구분하는 문제이다.

핵심 개념

PKI는 공개키와 사용자 신원을 인증서로 연결하고 이를 발급·관리하는 신뢰 기반 구조이다.
CRL은 인증서 유효기간이 남아 있어도 더 이상 신뢰할 수 없는 인증서를 인증기관이 목록으로 공지하는 폐지 정보이다.
인증서 유효기간은 기본 사용 가능 기간일 뿐이며, 유효기간 안이라도 폐지되면 신뢰할 수 없다.

NoteBase

선지별 해설

① O
PKI의 기본 구성요소에는 인증기관(CA), 등록기관(RA), 인증서 저장소, 사용자 등이 포함된다. PKI를 구성하는 주체를 묻는 설명으로 타당하다.

② O
인증기관은 폐지된 인증서를 사용자나 검증자가 확인할 수 있도록 CRL을 주기적으로 발행·관리한다. 인증서 상태 확인 기능에 대한 설명으로 맞다.

③ X
틀린 부분은 "유효기간 내의 인증서를 가지고 있다면, 사용자는 별도로 CRL을 조사할 필요가 없다"는 표현이다. 실제로는 유효기간이 남아 있어도 개인키 유출, 소유자 변경, 발급 오류 등으로 인증서가 폐지되므로 CRL이나 OCSP 등으로 폐지 여부를 확인해야 한다.
따라서 올바르게는 "인증서가 유효기간 내에 있더라도 폐지 여부를 확인해야 한다"이다.

④ O
PKI는 상위 인증기관이나 교차인증을 통해 인증경로를 구성하므로 사용자가 모든 인증기관의 공개키를 직접 보유할 필요는 없다. 일반적으로는 신뢰하는 루트 인증기관의 공개키와 인증서 경로 검증으로 신뢰를 확장한다.

오답 포인트

3번은 "유효기간이 남아 있다"와 "현재도 신뢰할 수 있다"를 같은 의미로 착각하게 만드는 함정이다. PKI에서는 만료 여부와 폐지 여부가 별개이므로, 유효기간 안이어도 폐지 확인 절차를 거쳐야 한다.

다시 나오면 이렇게 판단

인증서 문제에서는 먼저 유효기간 확인과 폐지 여부 확인을 분리해서 본다. 만료 전이라도 폐지될 수 있으면 CRL·OCSP로 확인해야 한다고 판단하면 된다.

암기 포인트

인증서 상태는 만료와 폐지를 따로 본다. 유효기간 내라도 폐지되면 사용할 수 없다.

NoteBase

문 5. HTTP 응답 메시지 상태코드의 의미가 옳지 않은 것은?

① 201 - Created

② 301 - Moved Permanently

③ 401 - Unauthorized

④ 501 - Bad Request

정답 4번

출제 포인트

이 문제는 HTTP 응답 상태코드 번호와 표준 의미의 정확한 대응을 묻는 문제이다.

핵심 개념

2xx는 성공 응답이다. 3xx는 리다이렉션 응답이다. 4xx는 클라이언트 오류 응답이다. 5xx는 서버 오류 응답이다. 201 Created는 요청 결과로 새 리소스가 생성된 상태이다. 301 Moved Permanently는 리소스가 영구적으로 다른 URI로 이동한 상태이다. 401 Unauthorized는 유효한 인증 자격 증명이 없어 요청이 적용되지 않은 상태이다. 501 Not Implemented는 서버가 요청을 처리하는 데 필요한 기능을 지원하지 않는 상태이다.

선지별 해설

① O
201 Created는 요청이 성공하여 하나 이상의 새 리소스가 생성되었음을 뜻한다.

② O
301 Moved Permanently는 대상 리소스에 새 영구 URI가 부여되었음을 뜻한다.

③ O
401 Unauthorized는 대상 자원에 대해 유효한 인증 자격 증명이 부족하여 요청이 적용되지 않았음을 뜻한다.

④ X
틀린 부분은 "501 - Bad Request"라는 대응이다.
501은 Not Implemented이며, 서버가 요청을 처리하는 데 필요한 기능을 지원하지 않는 경우이다.
Bad Request는 400이며, 잘못된 요청 구문이나 잘못된 요청 형식 같은 클라이언트 오류를 뜻한다.

NoteBase

오답 포인트

400과 401은 모두 4xx이고 500대는 서버 오류이므로, 숫자 계열을 먼저 보지 않으면 400 Bad Request와 501 Not Implemented를 서로 바꿔 적기 쉽다. 401도 단순한 권한 부족으로만 외우면 인증 자격 증명 문제라는 핵심을 놓치기 쉽다.

다시 나오면 이렇게 판단

먼저 첫 자리 숫자로 상태코드 계열을 구분한다. 2xx는 성공, 3xx는 이동, 4xx는 클라이언트 오류, 5xx는 서버 오류이다. 그다음 대표 코드의 짝을 대입하면 201 Created, 301 Moved Permanently, 401 Unauthorized, 400 Bad Request, 501 Not Implemented로 정리된다.

암기 포인트

400은 잘못된 요청, 401은 인증 자격 증명 부족, 301은 영구 이동, 501은 미구현이다.

NoteBase

문 6. 괄호 안에 들어갈 용어를 바르게 연결한 것은?

IPSec의 (㉠)는 발신지 인증과 데이터 무결성 그리고 데이터 기밀성을 제공한다. 두 호스트 사이의 논리적 관계인 SA(Security Association)를 생성하기 위하여 (㉡) 프로토콜을 사용하여 보안상 안전한 채널을 확보한다.

① ㉠: AH, ㉡: OSPF

② ㉠: AH, ㉡: IKE

③ ㉠: ESP, ㉡: IKE

④ ㉠: ESP, ㉡: OSPF

정답 3번

출제 포인트

이 문제는 IPsec의 AH와 ESP가 제공하는 보안 서비스의 차이와, SA를 협상하는 프로토콜인 IKE를 구분하는 문제이다.

핵심 개념

AH: IPsec에서 무결성, 발신지 인증, 재전송 방지를 제공하지만 데이터 기밀성은 제공하지 않는 인증 헤더이다.
ESP: IPsec에서 데이터 기밀성을 제공하고, 필요에 따라 무결성과 발신지 인증도 함께 제공할 수 있는 보안 페이로드이다.
IKE: IPsec 통신에 필요한 SA를 협상하고 생성하는 키 교환 프로토콜이다.
OSPF: IPsec SA를 만드는 프로토콜이 아니라 라우팅 정보를 교환하는 링크 상태 라우팅 프로토콜이다.

선지별 해설

① X: AH는 무결성과 발신지 인증은 제공하지만 데이터 기밀성은 제공하지 못하므로 ㄱ이 틀리고, OSPF는 SA 생성 프로토콜이 아니므로 ㄴ도 틀리다. 올바르게는 ESP, IKE의 연결이어야 한다.
② X: IKE는 SA를 생성하는 프로토콜이므로 ㄴ은 맞지만, AH는 데이터 기밀성을 제공하지 못하므로 ㄱ이 틀리다. 올바르게는 AH가 아니라 ESP이다.
③ O: ESP는 발신지 인증, 데이터 무결성, 데이터 기밀성을 제공할 수 있고, SA는 IKE를 통해 협상·생성하므로 두 연결이 모두 맞다.
④ X: ESP가 데이터 기밀성을 제공한다는 점에서 ㄱ은 맞지만, OSPF는 라우팅 프로토콜이어서 SA 생성에 쓰이지 않는다. 올바르게는 OSPF가 아니라 IKE이다.

NoteBase

오답 포인트

AH와 ESP를 모두 인증 프로토콜로만 외우면 AH도 기밀성을 제공한다고 착각하기 쉽다. 또 OSPF와 IKE를 모두 네트워크 프로토콜로 뭉뚱그리면 SA를 만드는 주체를 혼동하게 된다.

다시 나오면 이렇게 판단

선지에 기밀성이라는 표현이 있으면 먼저 AH를 지우고 ESP를 떠올리면 된다. 이어서 SA 생성·협상이라는 표현이 나오면 라우팅 프로토콜이 아니라 키 교환 프로토콜인 IKE인지 확인하면 된다.

암기 포인트

AH는 인증·무결성, ESP는 기밀성 포함, SA 협상은 IKE이다.

NoteBase

문 7. 괄호 안에 들어갈 접근 권한을 바르게 연결한 것은?

리눅스 시스템에서 umask 값을 027로 설정할 경우, 이후 생성되는 일반 파일의 접근 권한은 (㉠)이고, 디렉터리 접근 권한은 (㉡)이다.

① ㉠: 640, ㉡: 750

② ㉠: 750, ㉡: 640

③ ㉠: 644, ㉡: 755

④ ㉠: 755, ㉡: 644

정답 1번

출제 포인트

이 문제는 umask 값을 기본 생성 권한에 적용해 일반 파일과 디렉터리의 최종 접근 권한을 구하는 문제이다.

조건 정리

주어진 값: umask는 027이다.
구해야 할 값: 일반 파일 권한 (ㄱ), 디렉터리 권한 (ㄴ)이다.
주의할 조건: 일반 파일의 기본 생성 권한은 666이고 디렉터리의 기본 생성 권한은 777이다. 일반 파일은 기본적으로 실행 비트를 갖지 않는다.

사용할 공식

일반 파일은 666에 umask 027을 적용하고, 디렉터리는 777에 umask 027을 적용한다.
이 원리를 쓰는 이유: umask는 새로 만드는 파일이나 디렉터리에서 허용하지 않을 권한 비트를 제거하는 값이기 때문이다.

계산 과정

1. 일반 파일은 666에서 027을 적용하므로 소유자 6, 그룹 4, 기타 사용자 0이 되어 640이다.
2. 디렉터리는 777에서 027을 적용하므로 소유자 7, 그룹 5, 기타 사용자 0이 되어 750이다.
3. 따라서 (ㄱ, ㄴ)은 (640, 750)이다.

NoteBase

선지별 해설

① O: (ㄱ)이 640이고 (ㄴ)이 750이므로 계산 결과와 일치한다.
② X: (ㄱ)을 750으로 본 점이 틀렸다. 일반 파일은 기본 권한이 777이 아니라 666이므로 실행 비트가 생기지 않는다. 올바르게는 (ㄱ) 640, (ㄴ) 750이다.
③ X: (ㄱ)을 644로 본 점과 (ㄴ)을 755로 본 점이 틀렸다. 644는 umask의 마지막 자리 7을 제대로 반영하지 못한 값이고, 755는 그룹 쓰기 비트와 기타 사용자 쓰기·실행 비트를 제거하지 못한 값이다. 올바르게는 (ㄱ) 640, (ㄴ) 750이다.
④ X: (ㄱ)을 755로 본 점과 (ㄴ)을 644로 본 점이 모두 틀렸다. 파일과 디렉터리의 기본 권한을 서로 뒤섞어 적용한 결과이다. 올바르게는 (ㄱ) 640, (ㄴ) 750이다.

오답 포인트

일반 파일에도 디렉터리처럼 기본값 777을 적용한다고 착각하면 750이나 755 같은 오답이 나온다. 또 umask의 마지막 자리 7은 기타 사용자 권한을 모두 막는다는 점을 놓치면 644처럼 기타 사용자 읽기 권한을 남기는 실수를 하게 된다.

다시 나오면 이렇게 판단

리눅스 권한 계산 문제는 먼저 대상이 일반 파일인지 디렉터리인지 구분한 뒤 기본 권한을 각각 666, 777로 놓고 umask를 적용해 판단한다. 마지막에 실행 비트가 일반 파일에 불필요하게 살아 있지 않은지도 함께 확인한다.

암기 포인트

umask 계산의 출발점은 파일 666, 디렉터리 777이다.

NoteBase

문 8. ISMS-P에 대한 설명으로 옳지 않은 것은?

① 인증기준은 크게 3개 영역으로 나뉘며 총 102개의 인증기준으로 구성되어 있다.

② 관리체계 수립 및 운영 영역은 4개 분야 16개 인증기준으로 구성되어 있다.

③ 보호대책 요구사항 영역은 12개 분야 64개 인증기준으로 구성되어 있다.

④ 개인정보 처리단계별 요구사항 영역은 6개 분야 24개의 인증기준으로 구성되어 있다.

정답 4번

출제 포인트

이 문제는 ISMS-P 인증기준의 3개 영역별 구성과 각 영역의 세부 인증기준 수를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

ISMS-P 인증기준은 정보보호와 개인정보보호를 함께 심사하는 통합 기준이다.
관리체계 수립 및 운영 영역은 4개 분야 16개 인증기준이다.
보호대책 요구사항 영역은 12개 분야 64개 인증기준이다.
개인정보 처리단계별 요구사항 영역은 6개 분야 22개 인증기준이다.
따라서 전체 인증기준은 3개 영역 총 102개이다.

선지별 해설

① O: ISMS-P 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항의 3개 영역으로 나뉘고 총 102개 기준으로 구성되므로 옳다.
② O: 관리체계 수립 및 운영 영역은 4개 분야 16개 인증기준이므로 옳다.
③ O: 보호대책 요구사항 영역은 12개 분야 64개 인증기준이므로 옳다.
④ X: 틀린 부분은 "24개의 인증기준"이다. 개인정보 처리단계별 요구사항 영역은 6개 분야까지는 맞지만 인증기준 수는 24개가 아니라 22개이다. 올바르게는 "개인정보 처리단계별 요구사항 영역은 6개 분야 22개의 인증기준으로 구성되어 있다"이다.

오답 포인트

이 문항의 함정은 분야 수와 인증기준 수를 함께 제시해 일부만 맞는 선지를 그럴듯하게 보이게 만든 점이다. ④는 6개 분야라는 앞부분이 맞아서 지나치기 쉽지만, 끝의 24개를 22개와 혼동하면 오답이 된다.

다시 나오면 이렇게 판단

ISMS-P 구성 문제는 먼저 3개 영역과 총 102개를 잡고, 이어서 16-64-22의 수치를 영역별로 대입해 판단하면 된다. 선지에 분야 수와 세부 기준 수가 함께 나오면 둘 다 맞는지 분리해서 확인해야 한다.

NoteBase

암기 포인트

ISMS-P는 3영역 102개이며 세부 수치는 16-64-22이다.

NoteBase

문 9. 「개인정보 보호법」 상의 개인정보 보호위원회에 대한 조항의 일부이다. 괄호 안에 들어갈 용어를 바르게 연결한 것은?

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 (㉠) 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.
② 보호위원회는 「정부조직법」 제2조에 따른 (㉡)으로 본다.

① ㉠: 대통령, ㉡: 중앙행정기관의 보조기관
② ㉠: 대통령, ㉡: 중앙행정기관
③ ㉠: 국무총리, ㉡: 중앙행정기관의 보조기관
④ ㉠: 국무총리, ㉡: 중앙행정기관

정답 4번

쟁점

이 문제는 개인정보 보호위원회의 법적 지위와 정부조직법상 기관 성격을 묻는 문제이다.
핵심은 '국무총리 소속'과 '중앙행정기관'을 정확히 구별하는 것이다.

용어 풀이

중앙행정기관은 법률에 따라 독립된 행정권한을 수행하는 기관이다.
보조기관은 중앙행정기관 내부에서 장을 보좌하는 차관, 실장, 국장 등의 내부 조직을 뜻한다.

핵심 구분

제시된 조문은 개인정보 보호위원회를 국무총리 소속으로 두고, 「정부조직법」 제2조에 따른 중앙행정기관으로 본다고 규정한다.
따라서 '국무총리 소속'은 위원회의 소속을, '중앙행정기관'은 위원회의 기관 성격을 뜻한다.
보조기관은 중앙행정기관 자체가 아니라 그 내부 보좌조직이므로 이 문항의 ㄴ에 들어갈 수 없다.

NoteBase

선지별 해설

① X
- ㄱ의 '대통령'이 틀렸다. 제시 조문은 보호위원회를 국무총리 소속으로 둔다.
- ㄴ의 '중앙행정기관의 보조기관'도 틀렸다. 보호위원회는 보조기관이 아니라 중앙행정기관으로 본다.
- 틀린 표현: 대통령 / 중앙행정기관의 보조기관
- 올바른 표현: 국무총리 / 중앙행정기관

② X
- ㄴ의 '중앙행정기관'은 맞지만 ㄱ의 '대통령'이 틀려 전체가 틀렸다.
- 틀린 표현: 대통령
- 올바른 표현: 국무총리

③ X
- ㄱ의 '국무총리'는 맞지만 ㄴ의 '중앙행정기관의 보조기관'이 틀려 전체가 틀렸다.
- 보호위원회는 독립적으로 사무를 수행하는 중앙행정기관이지 중앙행정기관 내부의 보조기관이 아니다.
- 틀린 표현: 중앙행정기관의 보조기관
- 올바른 표현: 중앙행정기관

④ O
- ㄱ에 '국무총리', ㄴ에 '중앙행정기관'이 들어가야 조문 내용과 정확히 일치한다.
- 따라서 제시된 두 빈칸을 모두 맞게 연결한 선지는 ④이다.

오답 포인트

'소속'과 '기관 성격'을 한 번에 묻는 문제라서 한쪽만 맞고 다른 쪽이 틀린 선지에 흔들리기 쉽다.
특히 '중앙행정기관의 보조기관'이라는 표현은 행정조직 용어상 그럴듯하지만, 보호위원회 자체를 보조기관으로 본다는 뜻이 아니므로 함정이다.

다시 나오면 이렇게 판단

법령 빈칸 문제는 각 빈칸이 소속, 주체, 권한, 기관 성격 중 무엇을 묻는지 먼저 나누어 본다.
그다음 조문에 나온 핵심 명사를 그대로 대응시키면 한 부분만 맞는 혼합선지를 걸러낼 수 있다.

암기 포인트

개인정보 보호위원회는 국무총리 소속, 기관 성격은 중앙행정기관이다.

NoteBase

문 10. 타원 곡선 암호에 대한 설명으로 옳은 것만을 모두 고른 것은?

ㄱ. 타원 곡선은 함수 $y^2 = x^3 + ax + b$의 형태로 $4a^3 + 27b^2 \neq 0$의 조건을 만족해야 한다.
ㄴ. 임의의 평문과 암호문은 타원 곡선상의 점으로 표현되며, 곡선상의 모든 점들이 암호에 사용될 수 있다.
ㄷ. 타원 곡선상의 서로 다른 두 점, P와 Q의 합의 연산 $(P + Q)$은 P와 Q를 연결하는 직선과 교차하는 곡선상의 점이다.
ㄹ. 타원 곡선 암호는, k와 P로부터 $Q = kP$를 만족하는 Q를 구하는 것은 비교적 쉽지만, 주어진 Q와 P로 k를 결정하는 것은 매우 어렵다는 점을 이용한 것이다. 여기서, P와 Q는 타원 곡선상의 점들이고 k는 일정 조건을 만족하는 값이다.

① ㄱ, ㄴ

② ㄱ, ㄹ

③ ㄱ, ㄷ, ㄹ

④ ㄴ, ㄷ, ㄹ

정답 2번

출제 포인트

이 문제는 타원 곡선의 정의 조건, 점 덧셈의 의미, 그리고 타원 곡선 이산로그 문제의 성질을 정확히 구분할 수 있는지를 묻는 문제이다.

핵심 개념

타원 곡선 암호는 비특이 타원 곡선 위의 점 연산을 이용하는 공개키 암호 방식이다.
표준적인 타원 곡선은 $y^2 = x^3 + ax + b$ 꼴에서 $4a^3 + 27b^2 \neq 0$이어야 하며, 이 조건이 있어야 특이점이 없는 정상적인 곡선이 된다.
점 덧셈은 직선이 곡선과 만나는 세 번째 점을 구한 뒤 그 점을 x축에 대하여 반사한 점을 결과로 삼는다.
또한 $Q = kP$를 계산하는 것은 쉽지만, 주어진 P와 Q로부터 k를 찾는 것은 매우 어려운데 이것이 타원 곡선 암호의 핵심 난제이다.

NoteBase

선지별 해설

① X
- ①은 ㄱ과 ㄴ을 모두 옳다고 본 조합인데, ㄱ은 옳지만 ㄴ이 틀리므로 오답이다.
- 틀린 표현은 ㄴ의 "곡선상의 모든 점들이 암호에 사용될 수 있다"이다. 올바르게는 메시지를 곡선의 점으로 대응시키는 과정이 필요하며, 곡선의 모든 점을 아무 제약 없이 그대로 사용한다고 볼 수는 없다.

② O
- ②는 ㄱ, ㄹ 조합이다. ㄱ의 $4a^3 + 27b^2 \neq 0$ 조건은 비특이 타원 곡선의 정의 조건이고, ㄹ은 타원 곡선 이산로그 문제의 성질을 정확히 설명하므로 옳다.

③ X
- ③은 ㄱ, ㄷ, ㄹ 조합인데, ㄷ이 틀리므로 오답이다.
- 틀린 표현은 ㄷ의 "$P + Q$는 P와 Q를 연결하는 직선과 교차하는 곡선상의 점"이다. 올바르게는 그 직선이 곡선과 만나는 세 번째 점을 구한 뒤, 그 점을 x축에 대하여 반사한 점이 $P + Q$이다.

④ X
- ④는 ㄴ, ㄷ, ㄹ 조합인데, ㄴ과 ㄷ이 모두 틀리므로 오답이다.
- 올바르게는 ㄱ과 ㄹ만 옳고 ㄴ, ㄷ은 틀리므로 이런 조합은 정답이 될 수 없다.

오답 포인트

ㄴ은 점 표현 가능성을 곧바로 모든 점의 자유로운 사용 가능성으로 일반화하게 만드는 함정이다. ㄷ은 직선과 세 번째 교점까지는 기억하면서 마지막 x축 대칭 단계를 빠뜨리기 쉬운 점을 노린 문장이다. 이 두 문장을 걸러 내지 못하면 ①, ③, ④가 모두 그럴듯해 보이게 된다.

다시 나오면 이렇게 판단

타원 곡선 암호 문제는 먼저 비특이 조건 $4a^3 + 27b^2 \neq 0$인지 확인하고, 점 덧셈은 "세 번째 교점 그 자체"가 아니라 "세 번째 교점의 x축 대칭점"인지 확인하며, 마지막으로 $Q = kP$는 쉽고 역으로 k를 찾는 것은 어렵다는 구조인지 대조하면 된다.

암기 포인트

타원 곡선 암호는 "비특이 조건, 세 번째 교점 후 대칭, 쉬운 kP와 어려운 역문제"로 정리된다.

NoteBase

문 11. 버퍼 오버플로우 공격에 대한 설명으로 옳지 않은 것은?

① 스택 오버플로우와 힙 오버플로우 공격 등이 있다.

② 버퍼에 일정한 크기 이상의 데이터를 입력하여 프로그램을 공격한다.

③ 취약한 C함수로는 strcpy(), strcat(), gets() 등이 있다.

④ 대응 방법의 하나인 스택 가드는 스택에서 권한을 제거해 스택에 로드된 공격자의 공격 코드가 실행될 수 없도록 한다.

정답 4번

출제 포인트

이 문제는 버퍼 오버플로우의 유형과 취약 함수, 대응 기법의 역할을 정확히 구별할 수 있는지를 묻는다.

핵심 개념

버퍼 오버플로우는 버퍼 크기를 넘는 입력으로 인접 메모리를 덮어쓰는 취약점이다. 스택 오버플로우는 스택 영역에서, 힙 오버플로우는 힙 영역에서 발생한다. 스택 가드는 반환 주소 앞에 카나리 값을 두어 변조를 탐지하는 기법이고, 스택 실행 권한 제거는 비실행 스택 기법의 역할이다.

선지별 해설

1번 O: 버퍼 오버플로우는 메모리 영역에 따라 스택 오버플로우와 힙 오버플로우로 나눌 수 있으므로 옳다.
2번 O: 버퍼가 수용할 수 있는 크기를 넘는 데이터를 입력해 프로그램의 메모리를 덮어쓰는 방식이 버퍼 오버플로우 공격이므로 옳다.
3번 O: strcpy(), strcat(), gets()는 경계 검사 없이 복사하거나 입력을 받아 버퍼 오버플로우를 일으키기 쉬운 대표적 취약 함수이므로 옳다.
4번 X: 틀린 부분은 "스택에서 권한을 제거해 ... 공격 코드가 실행될 수 없도록 한다"이다. 스택 가드는 카나리 값을 검사해 오버플로우 발생 여부를 탐지하는 기법이며, 스택 실행 권한을 제거해 코드 실행을 막는 것은 비실행 스택 또는 DEP 계열 보호 기법이다.

오답 포인트

스택 가드와 비실행 스택을 같은 대응 기법으로 섞으면 틀린다. 이 문항은 4번에서 탐지 기능과 실행 차단 기능을 뒤바꾼 표현을 함정으로 둔다.

다시 나오면 이렇게 판단

버퍼 오버플로우 관련 선지는 먼저 발생 위치가 스택인지 힙인지 구분하고, 대응 기법은 탐지형인지 실행 차단형인지 역할을 나누어 판단한다.

NoteBase

암기 포인트

스택 가드는 카나리로 탐지하고, 비실행 스택은 권한 제거로 실행을 막는다.

NoteBase

문 12. 공인인증기관의 지정 등 공인인증서 관련 사항을 규정한 법은?

① 전자정부법

② 전자서명법

③ 신용정보의 이용 및 보호에 관한 법률

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정답 2번

쟁점

이 문제는 공인인증기관의 지정과 공인인증서 관련 사항을 규율하던 법률을 구별하는 문제이다.
핵심은 공인인증제도 자체를 다루는 법과 전자정부 운영, 신용정보 보호, 정보통신망 이용을 다루는 법을 구분하는 것이다.

용어 풀이

공인인증기관 = 공인인증서를 발급하기 위하여 법에 따라 지정되던 인증기관이다.
공인인증서 = 전자서명의 검증에 쓰이는 전자적 증명서이다.

핵심 구분

공인인증기관의 지정, 공인인증서의 발급과 효력 등 공인인증제도 자체는 전자서명법이 규율하였다.
전자정부법은 행정의 전자적 처리와 전자정부 서비스에 관한 법이고, 신용정보의 이용 및 보호에 관한 법률은 신용정보의 이용과 보호에 관한 법이며, 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망과 정보통신서비스 이용 질서를 다루는 법이다.

NoteBase

선지별 해설

① X
전자정부법은 전자정부 구현, 행정정보의 공동이용, 전자민원 등 행정 영역의 전자적 운영을 규율하는 법이다. 공인인증기관의 지정과 공인인증서 제도를 직접 규정한 법은 아니다.
틀린 표현: 공인인증서 관련 사항을 규정한 법
올바른 표현: 전자정부법은 전자정부 서비스와 행정정보의 전자적 처리 등을 규정한 법이다.

② O
공인인증기관의 지정, 공인인증서의 발급, 효력과 같은 공인인증 관련 사항은 전자서명법에서 규율하였다. 선지의 법률명이 문제의 핵심 키워드와 정확히 대응한다.

③ X
신용정보의 이용 및 보호에 관한 법률은 개인신용정보, 신용정보회사, 신용조회와 같은 신용정보 분야를 규율하는 법이다. 공인인증기관 지정 제도를 다루는 법이 아니다.
틀린 표현: 공인인증서 관련 사항을 규정한 법
올바른 표현: 신용정보의 이용 및 보호에 관한 법률은 신용정보의 수집, 이용, 제공 및 보호를 규정한 법이다.

④ X
정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망 이용촉진, 정보보호, 정보통신서비스 제공자 의무 등을 규율하는 법이다. 공인인증기관의 지정과 공인인증서 제도를 직접 규정한 법은 아니다.
틀린 표현: 공인인증서 관련 사항을 규정한 법
올바른 표현: 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 정보통신망과 정보보호 관련 의무를 규정한 법이다.

오답 포인트

법률명에 전자, 정보보호, 정보가 들어가면 비슷하게 보이지만, 공인인증기관과 공인인증서라는 직접 키워드가 보이면 전자서명법으로 연결해야 한다. ④는 정보보호라는 단어 때문에 가장 많이 흔들리는 오답이다.

다시 나오면 이렇게 판단

문제에서 특정 제도나 인증수단의 법적 근거를 묻는 경우에는 그 제도의 이름이 직접 들어간 법을 먼저 찾으면 된다. 공인인증기관, 공인인증서, 전자서명이라는 묶음이 보이면 전자서명법으로 판단한다.

암기 포인트

공인인증기관-공인인증서-전자서명법으로 연결된다.

NoteBase

문 13. 상세 위험 분석 방법에 대한 설명으로 옳은 것은?

① 시스템에 대해 보호의 기준 수준을 정하고, 목표를 달성하기 위하여 일련의 보호 대책을 선택한다.

② 모든 시스템에 적절한 기준 보안 대책을 이행하고, 상위 수준의 위험 평가를 통하여 중요하고 위험이 높은 시스템을 식별하고 평가한다.

③ 숙달된 전문가의 경험에 따라서 효율적으로 위험 분석을 수행한다.

④ 정형화되고 구조화된 프로세스를 사용하여 모든 중요한 위험을 식별하고 그 영향을 고려한다.

정답 4번

출제 포인트

이 문제는 위험 분석 접근법 가운데 기준선 접근법, 복합 접근법, 비정형 접근법, 상세 위험 분석을 구별할 수 있는지를 묻는다.

핵심 개념

기준선 접근법은 모든 시스템에 공통으로 적용할 최소 보호 수준을 먼저 정해 그 수준에 맞는 대책을 고르는 방식이다.
복합 접근법은 기준선 접근법을 먼저 적용한 뒤, 상위 수준의 위험 평가로 중요한 시스템만 골라 추가 분석하는 방식이다.
비정형 접근법은 숙련된 전문가의 경험과 직관을 중심으로 위험을 판단하는 방식이다.
상세 위험 분석은 정형화된 절차로 자산, 위협, 취약점, 영향도를 체계적으로 식별하고 평가하는 방식이다.

선지별 해설

1번 X: 시스템의 보호 기준 수준을 정하고 그 목표를 달성할 보호 대책을 선택한다는 설명은 기준선 접근법에 해당한다. 틀린 표현은 상세 위험 분석으로 볼 수 있다는 점이다. 올바르게는 기준선 접근법에 대한 설명이다.
2번 X: 모든 시스템에 기준 보안 대책을 적용한 뒤 상위 수준의 위험 평가로 중요한 시스템을 다시 식별하는 방식은 복합 접근법이다. 틀린 표현은 상세 위험 분석과 같은 단일 정밀 분석으로 보는 점이다. 올바르게는 기준선 접근법과 상위 수준 평가를 결합한 복합 접근법이다.
3번 X: 숙달된 전문가의 경험에 따라 효율적으로 위험 분석을 수행한다는 설명은 비정형 접근법이다. 틀린 표현은 정형화된 상세 분석으로 보는 점이다. 올바르게는 전문가의 경험과 판단에 크게 의존하는 비정형 접근법이다.
4번 O: 정형화되고 구조화된 프로세스로 모든 중요한 위험을 식별하고 그 영향을 고려한다는 설명은 상세 위험 분석의 특징과 일치한다. 자산, 위협, 취약점, 영향도를 체계적으로 따지는 방식이라는 점이 핵심이다.

오답 포인트

1번의 기준 수준 설정, 2번의 기준 보안 대책 후 선별 평가, 3번의 전문가 경험 의존은 각각 다른 접근법의 핵심 키워드이다. 상세 위험 분석은 4번처럼 정형화된 절차와 영향 평가가 함께 나와야 한다.

NoteBase

다시 나오면 이렇게 판단

선지에서 기준 수준을 먼저 정하면 기준선 접근법, 기준 대책 후 중요한 시스템만 다시 보면 복합 접근법, 전문가 경험을 강조하면 비정형 접근법, 구조화된 절차로 위험과 영향을 체계적으로 따지면 상세 위험 분석으로 판단한다.

암기 포인트

기준선은 최소수준, 복합은 선별추가, 비정형은 전문가경험, 상세분석은 구조화된 절차와 영향평가이다.

NoteBase

문 14. 설치된 백도어를 탐지하는 방법의 하나는 현재 동작 중인 프로세스를 확인하는 것이다. 다음 설명에 해당하는 윈도우 프로세스를 바르게 나열한 것은?

ㄱ. 시스템에 대한 백업이나 업데이트에 관련된 작업의 스케줄러 프로세스
ㄴ. DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스
ㄷ. 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스

① ㄱ: smss.exe, ㄴ: svchost.exe, ㄷ: csrss.exe
② ㄱ: smss.exe, ㄴ: csrss.exe, ㄷ: svchost.exe
③ ㄱ: mstask.exe, ㄴ: svchost.exe, ㄷ: csrss.exe
④ ㄱ: mstask.exe, ㄴ: csrss.exe, ㄷ: svchost.exe

정답 3번

출제 포인트

이 문제는 윈도우의 대표 시스템 프로세스인 mstask.exe, svchost.exe, csrss.exe, smss.exe의 기능을 구별할 수 있는지를 묻는다.

핵심 개념

mstask.exe는 작업 스케줄러 관련 프로세스로 예약된 백업·업데이트 작업을 수행한다.
svchost.exe는 DLL 형태의 서비스를 묶어 실행하는 서비스 호스트 프로세스이다.
csrss.exe는 Client/Server Runtime Subsystem으로 콘솔 창 관리, 스레드 생성·삭제, 32비트 가상 MS-DOS 환경 지원과 관련된다.
smss.exe는 Session Manager Subsystem으로 세션 초기화와 시스템 시작 초기에 필요한 하위 프로세스 실행을 담당한다.

NoteBase

선지별 해설

1번: X. ㄱ은 smss.exe가 아니라 mstask.exe에 해당한다. smss.exe는 세션 관리자이므로 백업·업데이트 스케줄러 프로세스라는 설명이 틀렸고, 올바르게는 세션 초기화와 csrss.exe 등의 시작을 담당하는 프로세스이다. ㄴ의 svchost.exe와 ㄷ의 csrss.exe 연결은 맞다.
2번: X. ㄱ을 smss.exe로 둔 점이 틀렸고, 올바르게는 mstask.exe이다. 또 ㄴ을 csrss.exe로 둔 점도 틀렸다. DLL 기반 서비스의 기본 호스트는 csrss.exe가 아니라 svchost.exe이다. 따라서 ㄷ에 와야 할 csrss.exe가 ㄴ과 뒤바뀌었다.
3번: O. ㄱ의 mstask.exe는 예약 작업 스케줄러와 관련되고, ㄴ의 svchost.exe는 DLL 기반 서비스 호스트이며, ㄷ의 csrss.exe는 콘솔 관리와 스레드 생성·삭제, 32비트 가상 MS-DOS 모드 지원과 관련되므로 세 설명이 모두 맞게 연결되었다.
4번: X. ㄱ의 mstask.exe는 맞지만 ㄴ과 ㄷ이 서로 뒤바뀌었다. csrss.exe는 DLL 서비스 호스트가 아니고, svchost.exe는 콘솔 창 관리와 32비트 가상 MS-DOS 모드 지원 프로세스가 아니다. 올바르게는 ㄴ이 svchost.exe, ㄷ이 csrss.exe이다.

오답 포인트

svchost.exe와 csrss.exe를 둘 다 핵심 시스템 프로세스로만 외우면 기능이 섞여 틀리기 쉽다. 서비스 호스팅은 svchost.exe, 콘솔·런타임 서브시스템은 csrss.exe라는 역할 축으로 나누어야 한다.

다시 나오면 이렇게 판단

설명에 예약 작업, DLL 서비스 호스트, 콘솔·스레드·MS-DOS 지원, 세션 초기화 중 어떤 키워드가 들어 있는지 먼저 찾은 뒤 각각 mstask.exe, svchost.exe, csrss.exe, smss.exe로 대응시키면 된다.

암기 포인트

mstask는 예약 작업, svchost는 서비스 호스트, csrss는 콘솔 런타임, smss는 세션 관리자이다.

NoteBase

문 15. 다음은 아래 범례를 사용하여 사용자 A가 사용자 B에게 메시지 M을 전송하기 위한 프로토콜을 순서대로 나타낸 것이다. 위의 프로토콜에 대하여 다음과 같은 순서로 공격이 가능하다. 이 공격에 대한 설명으로 옳지 않은 것은?

ID_U: U의 아이디, KU_U: U의 공개키, KR_U: U의 개인키
$E(K, M)$: 메시지 M을 키 K로 암호화하는 함수
$D(K, C)$: 암호문 C를 키 K로 복호화하는 함수
B → A: ID_B, KU_B
A → B: ID_A, C [단, $C = E(KU_B, M)$]
B: $M = D(KR_B, C)$
B → X: ID_B, KU_B
X → A: ID_B, KU_X
A → X: ID_A, C' [단, $C' = E(KU_X, M)$]
X: $M = D(KR_X, C')$
X → B: ID_A, C [단, $C = E(KU_B, M)$]
B: $M = D(KR_B, C)$

① A가 B의 공개키를 검증하지 못해서 발생하는 중간자 공격이다.

② 공격자 X가 A의 메시지를 가로채서 다시 보내는 재전송 공격이다.

③ 공개키 인증서를 사용하면 방지할 수 있다.

④ 디피-헬만 키 교환에서도 발생할 수 있다.

정답 2번

출제 포인트

공개키를 인증하지 않은 공개키 암호 통신에서 중간자 공격이 어떻게 성립하는지를 묻는 문제이다.

사례 정리

B의 공개키가 A에게 전달되는 과정에 공격자 X가 개입한다.
A는 B의 공개키라고 믿고 실제로는 X의 공개키로 메시지를 암호화한다.
X는 이를 자신의 개인키로 복호화한 뒤 B의 공개키로 다시 암호화하여 B에게 전달한다.

핵심 개념

중간자 공격은 통신 당사자 사이에 공격자가 끼어들어 키나 메시지를 바꿔치기한 뒤 내용을 읽거나 변조하는 공격이다.
이 사례의 성립 조건은 A가 받은 공개키가 진짜 B의 공개키인지 인증하지 못한다는 점이다.

NoteBase

적용 기준

이 사례에서는 암호문을 단순 전달했는지가 아니라 공격자가 공개키를 자신의 것으로 치환해 평문을 확인할 수 있는지를 봐야 한다.
핵심 판단 기준은 공개키 인증 부재와 복호화 후 재암호화 가능성이다.

선지별 해설

① O: A는 B의 공개키를 검증하지 못한 채 X가 보낸 공개키를 B의 것으로 믿는다. 따라서 X가 통신 중간에서 내용을 확인하고 다시 전달할 수 있으므로 중간자 공격 설명이 맞다.
② X: 이 공격은 재전송 공격이 아니다. X는 A의 암호문을 그대로 다시 보내는 것이 아니라 자신의 개인키로 복호화한 뒤 B의 공개키로 새로 암호화해 보낸다. 틀린 표현은 '재전송 공격'이고, 올바르게는 '공개키 치환을 이용한 중간자 공격'이다.
③ O: 공개키 인증서를 사용하면 A가 받은 공개키가 실제 B의 것인지 검증할 수 있으므로 이런 공개키 치환 공격을 방지할 수 있다.
④ O: 디피-헬만 키 교환도 상대 공개값의 진위를 인증하지 않으면 공격자가 각각과 별도 키를 형성하는 중간자 공격이 가능하다.

오답 포인트

가로채서 다시 보낸다는 겉모습만 보고 재전송 공격으로 오인하기 쉽다. 그러나 이 문항의 핵심은 암호문 반복 전송이 아니라 공개키를 바꿔 끼워 넣어 평문을 읽고 다시 암호화한다는 점이다.

다시 나오면 이렇게 판단

공개키나 키 교환값이 전달되는 절차가 나오면 먼저 상대 키의 진위 확인 절차가 있는지 본다. 인증이 없고 공격자가 자신의 키로 바꿔 넣을 수 있으면 중간자 공격으로 판단할 수 있다.

암기 포인트

공개키 암호도 키 인증이 없으면 안전하지 않으며, 인증 없는 키 교환은 중간자 공격에 취약하다.

NoteBase

문 16. 다음은 FTP에서 데이터 연결을 생성하는 과정을 순서대로 설명한 것이다. 괄호 안에 들어갈 용어를 바르게 나열한 것은?

○ (㉠)가 임시 포트로 (㉡) 연결 설정을 시도한다.
○ (㉠)는 이 포트 번호를 PORT 명령어를 사용하여 (㉢)에 전송한다.
○ (㉢)는 포트 번호를 수신한 후, 잘 알려진 포트 20과 임시 포트 번호를 사용하여 (㉣) 연결 설정을 시도한다.

① ㉠: 클라이언트, ㉡: 수동적, ㉢: 서버, ㉣: 능동적
② ㉠: 클라이언트, ㉡: 능동적, ㉢: 서버, ㉣: 수동적
③ ㉠: 서버, ㉡: 수동적, ㉢: 클라이언트, ㉣: 능동적
④ ㉠: 서버, ㉡: 능동적, ㉢: 클라이언트, ㉣: 수동적

정답 1번

출제 포인트

이 문제는 FTP 데이터 연결에서 PORT 명령을 사용하는 능동 모드의 생성 순서와, 그 안에서 누가 수동적으로 대기하고 누가 능동적으로 접속하는지를 묻는 문제이다.

올바른 순서

1. 클라이언트가 임시 포트를 열고 수동적으로 연결을 기다린다.
2. 클라이언트가 그 임시 포트 번호를 PORT 명령으로 서버에 알려 준다.
3. 서버가 클라이언트가 알려 준 포트를 받는다.
4. 서버가 자신의 잘 알려진 포트 20에서 클라이언트의 임시 포트로 능동적으로 접속을 시도한다.

왜 이 순서인가: 서버가 어디로 접속해야 하는지는 클라이언트가 PORT 명령으로 임시 포트 번호를 먼저 알려 주어야 결정되므로, 클라이언트의 수동적 대기와 PORT 전송이 서버의 능동적 접속보다 먼저이다.

NoteBase

선지별 해설

① O: (ㄱ) 클라이언트, (ㄴ) 수동적, (ㄷ) 서버, (ㄹ) 능동적이 맞다. FTP 능동 모드에서는 클라이언트가 임시 포트를 열어 수동적으로 기다리고, PORT 명령으로 그 포트를 서버에 알린 뒤, 서버가 포트 20에서 클라이언트 쪽으로 능동적으로 데이터 연결을 건다.
② X: 틀린 부분은 '(ㄴ) 능동적'과 '(ㄹ) 수동적'이다. 올바르게는 클라이언트가 수동적으로 대기하고 서버가 능동적으로 접속한다. PORT 명령이 나온 시점에서 서버가 클라이언트로 접속하는 구조이므로 역할이 뒤집힐 수 없다.
③ X: 틀린 부분은 '(ㄱ) 서버'와 '(ㄷ) 클라이언트'이다. 올바르게는 PORT 명령으로 임시 포트 번호를 보내는 쪽이 클라이언트이고, 그 정보를 받아 포트 20에서 접속하는 쪽이 서버이다.
④ X: '(ㄱ) 서버, (ㄷ) 클라이언트'도 틀리고 '(ㄴ) 능동적, (ㄹ) 수동적'도 틀리다. 올바르게는 클라이언트가 수동적으로 열어 둔 임시 포트 정보를 서버에 보내고, 서버가 능동적으로 데이터 연결을 시작한다.

오답 포인트

이 문항의 함정은 '수동적'이라는 말을 보고 곧바로 FTP의 passive mode로 오해하는 데 있다. 여기의 수동적 연결 설정은 TCP 관점에서 기다리는 쪽을 뜻하고, PORT 명령이 보이면 전체 흐름은 FTP 능동 모드라고 판단해야 한다.

다시 나오면 이렇게 판단

FTP 문제에서 PORT 명령이 보이면 먼저 클라이언트가 자신의 임시 포트를 서버에 알려 주는 능동 모드인지부터 판단한다. 그다음 포트를 알려 주는 쪽은 클라이언트, 그 포트로 접속하는 쪽은 서버라는 순서로 정리하면 선지를 빠르게 가를 수 있다.

암기 포인트

PORT는 클라이언트가 알리고, 데이터 연결은 서버가 포트 20에서 건다.

NoteBase

문 17. 안전한 소프트웨어 개발 방법론의 하나인 MS사의 SDL(Secure Development Lifecycle)의 소프트웨어 개발 프로세스 중 위협 모델링을 수행해야 하는 단계는?

① 계획 · 분석

② 설계

③ 구현

④ 시험 · 검증

정답 2번

출제 포인트

이 문제는 MS사의 SDL에서 위협 모델링이 어느 개발 단계에 위치하는지를 묻는 절차형 문제이다.

올바른 순서

1. 계획·분석 - 보안 요구사항과 개발 기준을 정하는 단계이다.
2. 설계 - 시스템 구조, 데이터 흐름, 신뢰 경계 등을 바탕으로 위협 모델링을 수행하는 단계이다.
3. 구현 - 설계에서 정한 보안 대책을 코드와 설정에 반영하는 단계이다.
4. 시험·검증 - 구현 결과가 안전한지 테스트와 검토로 확인하는 단계이다.

왜 이 순서: 위협 모델링은 설계 산출물인 구조와 데이터 흐름이 있어야 가능하고, 여기서 도출한 대응책이 이후 구현과 시험의 입력이 된다.

NoteBase

선지별 해설

① X
계획·분석 단계는 보안 요구사항과 목표를 정하는 초기 단계이다. 이 단계에서는 아직 구조 설계가 구체화되지 않았으므로 위협 모델링의 직접 수행 단계로 보기 어렵다.
틀린 표현: 위협 모델링을 계획·분석 단계에서 수행한다.
올바르게는: 위협 모델링은 설계 단계에서 수행한다.

② O
설계 단계에서는 시스템 구조, 데이터 흐름, 신뢰 경계, 공격면을 검토할 수 있으므로 위협 모델링을 수행하기에 적절하다. Microsoft SDL에서도 위협 모델링은 설계 단계의 핵심 보안 활동으로 다뤄진다.

③ X
구현 단계는 이미 정해진 설계를 바탕으로 코드를 작성하고 보안 기능을 반영하는 단계이다. 위협 모델링 결과를 구현에 반영할 수는 있지만, 위협 모델링 자체를 이 단계의 중심 작업으로 보지는 않는다.
틀린 표현: 위협 모델링을 구현 단계에서 수행한다.
올바르게는: 구현 단계에서는 설계 단계에서 도출한 보안 대책을 코드에 반영한다.

④ X
시험·검증 단계는 보안 테스트, 코드 검토, 취약점 점검으로 설계와 구현 결과를 확인하는 단계이다. 위협 모델링은 검증 이전에 위험을 예측하고 설계에 반영하는 활동이다.
틀린 표현: 위협 모델링을 시험·검증 단계에서 수행한다.
올바르게는: 시험·검증 단계에서는 위협 모델링 결과가 구현에 제대로 반영되었는지를 확인한다.

오답 포인트

위협 모델링을 보안 테스트와 같은 검증 활동으로 오해하면 ④로 흐르기 쉽다. 그러나 위협 모델링은 취약점을 실제로 시험하는 절차가 아니라, 설계 시점에 가능한 위협을 구조적으로 식별하는 활동이라는 점이 핵심 함정이다.

다시 나오면 이렇게 판단

절차형 보안 문제에서는 해당 활동이 요구사항을 정하는 일인지, 설계를 검토하는 일인지, 코드를 작성하는 일인지, 결과를 시험하는 일인지를 먼저 구분한다. 구조, 데이터 흐름, 신뢰 경계, 공격면이 기준어로 나오면 설계 단계 활동으로 판단한다.

암기 포인트

위협은 설계에서 찾고, 구현에서 반영하고, 시험에서 검증한다.

NoteBase

문 18. 엔트로피에 대한 설명으로 옳은 것만을 모두 고른 것은?

ㄱ. 한 비트가 가질 수 있는 엔트로피의 최댓값은 1이다.
ㄴ. 블록 암호문의 엔트로피는 낮을수록 안전하다.
ㄷ. 엔트로피는 정보량 또는 정보의 불확실도를 측정하는 수학적 개념이다.
ㄹ. 어떤 확률변수가 가질 수 있는 모든 값의 발생 확률이 같을 경우, 엔트로피는 최솟값을 갖는다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 2번

출제 포인트

이 문제는 엔트로피의 정의와 최대·최소 조건을 정확히 구별하는지를 묻는 문제이다.

핵심 개념

엔트로피는 확률분포의 불확실성 또는 평균 정보량을 수치화한 개념이다.
한 비트의 엔트로피는 두 값이 동일한 확률로 나올 때 최대가 되며 그 최댓값은 1비트이다.
엔트로피는 모든 값이 동일 확률일 때 최대가 되고, 한 값으로 완전히 결정될 때 최소가 된다.

NoteBase

선지별 해설

1번 X
- 1번은 ㄱ, ㄴ의 조합이다.
- ㄱ은 맞다. 한 비트가 0과 1을 각각 0.5의 확률로 가질 때 엔트로피는 최대이며 값은 1비트이다.
- ㄴ은 틀리다. 블록 암호문의 엔트로피가 낮을수록 규칙성과 예측 가능성이 커져 안전하다고 보기 어렵다.
- 틀린 표현은 "낮을수록 안전하다"이다. 올바르게는 "암호문은 가능한 한 균등하고 예측하기 어려워 높은 엔트로피 특성을 보일수록 바람직하다"이다.

2번 O
- 2번은 ㄱ, ㄷ의 조합이다.
- ㄱ은 맞다. 한 비트의 최대 엔트로피는 1비트이다.
- ㄷ은 맞다. 엔트로피는 정보량 또는 정보의 불확실성을 측정하는 대표적 수학 개념이다.
- 따라서 옳은 것만 묶은 조합은 2번이다.

3번 X
- 3번은 ㄴ, ㄹ의 조합이다.
- ㄴ은 틀리다. 낮은 엔트로피는 안전성 증가가 아니라 예측 가능성 증가와 연결된다.
- ㄹ도 틀리다. 모든 값의 발생 확률이 같을 때 엔트로피는 최소가 아니라 최대가 된다.
- 틀린 표현은 ㄹ의 "최소값"이다. 올바르게는 "모든 값의 발생 확률이 같을 경우 엔트로피는 최댓값을 갖는다"이다.
- 올바른 조합으로 고치면 ㄱ, ㄷ이 되어야 한다.

4번 X
- 4번은 ㄷ, ㄹ의 조합이다.
- ㄷ은 맞다. 엔트로피는 불확실성과 평균 정보량을 나타낸다.
- ㄹ은 틀리다. 최소 엔트로피는 특정 값이 확률 1로 결정되어 전혀 불확실하지 않을 때이다.
- 틀린 표현은 "발생 확률이 같을 경우, 엔트로피는 최소값"이다. 올바르게는 "발생 확률이 같을 경우, 엔트로피는 최댓값"이다.
- 따라서 4번은 옳은 것만 모은 선택지가 아니다.

오답 포인트

엔트로피의 최대·최소 조건을 뒤집어 외우면 ㄹ 때문에 3번이나 4번으로 흔들리기 쉽다. 또 암호문 보안성과 엔트로피의 관계를 반대로 이해하면 ㄴ을 맞는 문장으로 착각하게 된다.

NoteBase

다시 나오면 이렇게 판단

엔트로피 문제는 먼저 "불확실성이 클수록 엔트로피가 커진다"는 기준을 적용하면 된다. 모든 경우가 고르게 나오면 최대, 한 경우로 결정되면 최소라고 판단하면 선지의 진위를 빠르게 가를 수 있다.

암기 포인트

균등분포는 최대 엔트로피, 확정분포는 최소 엔트로피이다.

NoteBase

문 19. 사용자 B가 메시지 M과 함께 $H(M \text{ XOR } K_{AB})$를 MAC로 하여 사용자 A에게 보내고, A는 수신한 MAC와 M으로부터 산출한 MAC를 비교함으로써 보안을 강화한 경우에 대한 설명으로 옳지 않은 것은? (단, K_{AB}는 A와 B의 공유 비밀키, H는 해시 함수)

① A는 메시지 M의 무결성을 확신할 수 있다.

② A는 메시지 M의 출처가 B라는 것을 확신할 수 있다.

③ A는 B가 메시지 M에 대하여 부인하지 못하도록 하는 부인 봉쇄를 보장받을 수 있다.

④ MAC에 시간이나 순서 정보가 포함되어 있지 않다면, 재전송 공격이 발생할 가능성이 있다.

정답 3번

출제 포인트

이 문제는 공유 비밀키를 사용하는 MAC이 제공하는 보안 기능과 제공하지 못하는 보안 기능의 차이를 묻는 문제이다.

핵심 개념

무결성은 전송 중 메시지 내용이 변조되지 않았는지를 확인하는 성질이다.
메시지 인증은 올바른 비밀키를 아는 상대가 만든 메시지인지를 확인하는 성질이다.
부인봉쇄는 송신자가 나중에 자신이 보냈다는 사실을 부인하지 못하게 하는 성질인데, 공유키 방식 MAC만으로는 보장되지 않는다.
재전송 공격은 과거의 정상 메시지와 MAC을 다시 보내 시스템을 속이는 공격이다.

NoteBase

선지별 해설

① O
수신자 A는 받은 M에 대해 같은 공유키 K_{AB}로 MAC을 다시 계산해 비교하므로 메시지 M이 중간에 바뀌었는지 확인할 수 있다. 따라서 무결성 확인은 가능하다.

② O
유효한 MAC을 만들려면 공유 비밀키 K_{AB}를 알아야 하므로, A는 이 메시지가 정당한 키 보유자 측에서 생성되었음을 확인할 수 있다. 이 문맥에서는 B가 송신 주체라는 메시지 인증 기능에 해당한다.

③ X
틀린 부분은 "부인하지 못하도록 하는 부인 봉쇄를 보장받을 수 있다"는 표현이다.
공유키 MAC은 A와 B가 같은 키를 함께 알고 있으므로, 나중에 제3자에게 B만이 생성했다고 증명할 수 없다.
올바르게는 "MAC은 무결성과 메시지 인증은 제공하지만 부인봉쇄는 제공하지 않는다"이다.

④ O
MAC에 시간 정보나 순서 번호가 없으면 과거에 정상적으로 전송된 M과 MAC을 그대로 다시 보내는 재전송 공격이 가능하다.

오답 포인트

②의 메시지 인증과 ③의 부인봉쇄를 같은 개념으로 섞으면 틀리기 쉽다. 공유키 MAC은 상대가 같은 키를 안다는 점까지는 확인해도, 제3자에게 특정 송신자만의 행위였다고 증명하는 기능은 없다.

다시 나오면 이렇게 판단

공유키 기반 MAC 문제가 나오면 먼저 무결성, 메시지 인증, 재전송 방지, 부인봉쇄를 나눠서 본다. 공유키 MAC은 무결성과 메시지 인증은 가능하고, 시간값이나 순서값이 없으면 재전송 공격에 취약하며, 부인봉쇄는 전자서명 같은 공개키 방식이 있어야 가능하다고 판단한다.

암기 포인트

공유키 MAC은 무결성·인증은 가능하고, 부인봉쇄는 불가능하다.

NoteBase

문 20. 「정보통신기반 보호법」상의 정보통신기반보호위원회에 관한 사항으로 옳지 않은 것은?

① 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 “위원회”라 한다)를 둔다.

② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.

③ 위원회의 위원장은 과학기술정보통신부장관이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.

④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.

정답 3번

쟁점

이 문제는 「정보통신기반 보호법」상 정보통신기반보호위원회의 소속, 위원장, 위원 구성, 실무위원회 설치를 정확히 구별하는 문제이다.
핵심은 위원회가 국무총리 소속이라는 점과 위원장이 국무조정실장이라는 점을 서로 다른 내용으로 나누어 보는 것이다.

용어 풀이

정보통신기반보호위원회는 주요정보통신기반시설의 보호에 관한 사항을 심의하는 위원회이다.

핵심 구분

위원회의 소속은 국무총리 소속이고, 위원회의 위원장은 국무조정실장이다.
즉, 위원회가 국무총리 소속이라고 해서 위원장까지 국무총리나 과학기술정보통신부장관이 되는 것은 아니다.
또한 위원은 위원장 1인을 포함한 25인 이내이고, 공공분야와 민간분야를 담당하는 실무위원회를 둔다.

NoteBase

선지별 해설

① O
- 위원회는 법 제8조에 따라 지정된 주요정보통신기반시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 둔다.
- 위원회의 설치 목적과 소속을 함께 묻는 기본 조문 그대로의 내용이다.

② O
- 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
- 위원 정수에 관한 설명으로 맞는 내용이다.

③ X
- 위원회의 위원장이 과학기술정보통신부장관이라는 부분이 틀리다.
- 틀린 표현: "위원회의 위원장은 과학기술정보통신부장관이 되고"
- 올바른 표현: 위원회의 위원장은 국무조정실장이 되고, 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.
- 뒤의 위원 구성 부분은 대체로 맞지만, 위원장 주체를 잘못 적었으므로 선지 전체는 틀린다.

④ O
- 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 둔다.
- 위원회 아래에 두는 실무위원회의 종류를 정확히 적은 내용이다.

오답 포인트

③은 정보통신기반 보호 업무가 과학기술정보통신부와 관련된다는 점을 이용해 위원장도 과학기술정보통신부장관일 것처럼 혼동하게 만든 선지이다. 이 문제는 소관 부처와 법정 위원회 위원장을 동일시하면 틀리기 쉽다.

다시 나오면 이렇게 판단

위원회 관련 선지는 소속 기관, 위원장, 위원 정수, 실무위원회 설치 여부를 분리해서 본다. 특히 "소속"과 "위원장"이 누구인지는 별도 항목으로 바로 대조하면 함정 선지를 빠르게 걸러낼 수 있다.

암기 포인트

정보통신기반보호위원회는 국무총리 소속, 위원장은 국무조정실장이다.

NoteBase