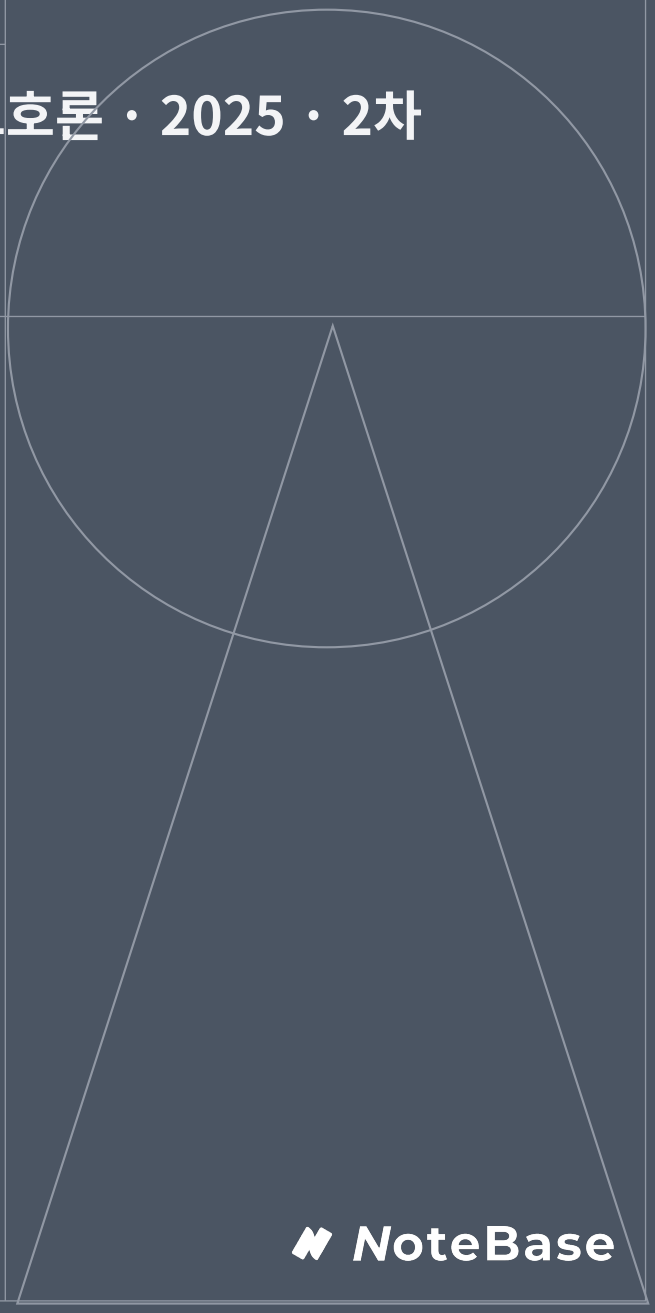
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2025 · 2차



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2025 · 2차

공무원/국가직/7급 · 정보보호론 · 2025 · 2차

문 1. 정보보안 목표와 그 목표에 대한 위협 요소를 바르게 연결한 것만을 모두 고르면?

ㄱ. 기밀성 - 재전송(replaying)
ㄴ. 무결성 - 가장(masquerading)
ㄷ. 가용성 - 서비스 거부(DoS)

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 3번

출제 포인트

이 문제는 정보보안의 기본 목표인 기밀성, 무결성, 가용성과 대표 위협 요소를 정확히 연결하는지를 묻는 문제이다.

핵심 개념

기밀성은 인가되지 않은 주체에게 정보가 노출되지 않는 성질이며 키워드는 도청, 유출, 노출이다.
무결성은 데이터나 정보의 출처가 무단으로 변조되거나 위조되지 않는 성질이며 키워드는 변조, 위조, 가장이다.
이 문제처럼 보안 목표를 기밀성·무결성·가용성으로 단순 분류하면 가장은 무결성 침해 쪽에 둔다.
가용성은 인가된 사용자가 필요할 때 자원과 서비스를 사용할 수 있는 성질이며 키워드는 서비스 거부, 자원 고갈, 중단이다.

NoteBase

선지별 해설

① X
ㄱ이 틀렸으므로 오답이다. 보기 ㄱ의 틀린 부분은 "기밀성"이다. 재전송은 이미 전송된 메시지를 다시 보내 부당한 효과를 만드는 공격이므로 기밀성 침해로 보기 어렵고, 올바르게는 무결성 또는 인증 관련 위협으로 본다. 보기 ㄴ은 이 문제의 분류에서는 가장을 무결성 침해로 연결하므로 맞다.

② X
ㄱ이 틀렸으므로 오답이다. 보기 ㄱ의 틀린 부분은 역시 "기밀성"이다. 재전송은 도청이나 노출처럼 비밀을 새어 나가게 하는 공격이 아니라 메시지의 정당성과 처리 결과를 흔드는 공격이므로, 올바르게는 무결성 또는 인증 관련 위협이다. 보기 ㄷ은 서비스 거부가 가용성을 해치는 대표 공격이므로 맞다.

③ O
ㄴ과 ㄷ이 모두 맞으므로 정답이다. 가장은 다른 사용자인 척하여 데이터의 출처와 정당성을 속이는 공격이므로 이 문제의 보안 목표 분류에서는 무결성 침해에 해당한다. 서비스 거부는 정당한 사용자가 서비스를 이용하지 못하게 하므로 가용성 침해가 맞다.

④ X
ㄱ이 틀렸으므로 오답이다. 보기 ㄱ의 틀린 부분은 "기밀성"이다. 재전송은 기밀성 위협이 아니라 무결성 또는 인증 관련 위협으로 연결해야 한다. 따라서 ㄴ, ㄷ은 맞더라도 ㄱ까지 포함한 ④는 성립하지 않는다.

오답 포인트

재전송과 가장은 둘 다 적극적 공격이라서 기밀성, 무결성, 인증성을 뒤섞기 쉽다. 이 문제의 함정은 "replaying"과 "masquerading"의 영문 용어에 끌려 막연히 외우는 데 있다. 도청·노출은 기밀성, 위조·변조·가장은 무결성, 서비스 중단은 가용성이라는 축으로 정리하면 헷갈림이 줄어든다.

다시 나오면 이렇게 판단

먼저 위협이 비밀을 새게 하는지, 내용을 바꾸거나 속이게 하는지, 아예 못 쓰게 하는지를 본다. 비밀 노출이면 기밀성, 위조·변조·가장이면 무결성, 사용 불가나 지연이면 가용성으로 연결하면 된다.

암기 포인트

기밀성은 노출, 무결성은 위조·변조, 가용성은 서비스 중단으로 묶는다.

NoteBase

문 2. CA(Certification Authority)가 사용자 A에게 발급한 X.509 버전 3 형식의 인증서에 포함되는 정보가 아닌 것은?

① A의 공개키

② A의 개인키

③ 인증서의 유효 기간

④ CA가 사용한 서명 알고리즘

정답 2번

출제 포인트

이 문제는 X.509 버전 3 인증서에 들어가는 공개 정보와 인증서에 절대 들어가면 안 되는 비밀 정보를 구별할 수 있는지를 묻는다.

핵심 개념

X.509 인증서는 주체의 신원을 공개키와 연결해 주는 공개 문서이다. 인증서에는 주체의 공개키, 유효 기간, 발급자 정보, 서명 알고리즘 등이 포함되지만 주체의 개인키 같은 비밀 정보는 포함되지 않는다.

선지별 해설

① O: 인증서에는 주체 A의 공개키가 반드시 포함된다. 인증서의 핵심 기능이 공개키를 신원과 바인딩하는 것이므로 공개키 정보가 없으면 인증서 역할을 할 수 없다.
② X: 틀린 부분은 "A의 개인키"이다. 개인키는 오직 소유자만 안전하게 보관해야 하는 비밀 정보이므로 인증서에 포함되지 않는다. 올바르게는 A의 공개키가 인증서에 포함된다.
③ O: 인증서에는 유효 시작 시각과 만료 시각으로 구성된 유효 기간이 포함된다. 수신자는 이 기간 안에 있는지 확인하여 인증서 사용 가능 여부를 판단한다.
④ O: 인증서에는 CA가 서명할 때 사용한 서명 알고리즘 식별 정보가 포함된다. 검증자는 이 정보를 보고 어떤 알고리즘으로 서명을 검증할지 결정할 수 있다.

오답 포인트

공개키 기반구조에서 공개키와 개인키를 한 쌍으로 외우면서 둘 다 인증서에 실린다고 착각하기 쉽다. 이 문제의 함정은 "키 쌍 중 무엇이 공개 정보인가"를 묻는 데 있으며, 개인키는 인증서가 아니라 사용자 측 비밀 저장 영역에 남아 있어야 한다.

다시 나오면 이렇게 판단

인증서 관련 선지를 보면 먼저 "누가 봐도 되는 공개 정보인가"를 확인한다. 공개적으로 배포되어도 되는 정보이면 인증서에 들어갈 수 있고, 노출되면 안 되는 비밀 정보이면 인증서에 들어가지 않는다.

NoteBase

암기 포인트

인증서는 공개키의 신분증이고, 개인키는 소유자만 가진 비밀이다.

문 3. 다음 설명에 해당하는 암호학적 해시함수 h의 특성은?

주어진 x와 $h(x)$에 대해 $h(x) = h(y)$를 만족하는 $y (y \neq x)$를 찾는 것이 계산적으로 불가능해야 한다.

① 무결성(integrity)
② 일방향성(one-way property)
③ 강한 충돌 저항성(strong collision resistance)
④ 약한 충돌 저항성(weak collision resistance)

정답 4번

출제 포인트

이 문제는 암호학적 해시함수의 일방향성, 강한 충돌 저항성, 약한 충돌 저항성의 정의 차이를 구분하는 문제이다.

핵심 개념

일방향성은 주어진 해시값 $h(x)$만 보고 원래 입력 x를 찾기 어려운 성질이다.
강한 충돌 저항성은 어떤 두 입력이든 $h(x) = h(y)$가 되도록 짝을 찾기 어려운 성질이다.
약한 충돌 저항성은 특정 입력 x가 주어졌을 때 $y \neq x$이면서 $h(x) = h(y)$가 되는 다른 입력 y를 찾기 어려운 성질이다.

선지별 해설

① X: 무결성은 정보가 인가되지 않게 변경되지 않았음을 뜻하는 보안 목표이다. 틀린 부분은 해시함수의 세부 성질로 본 점이다. 올바르게는 해시함수는 무결성 검증에 활용될 수 있지만, 제시문이 직접 설명하는 성질은 아니다.
② X: 일방향성은 $h(x)$가 주어졌을 때 원래의 x를 역으로 찾기 어려운 성질이다. 틀린 부분은 같은 해시값을 만드는 다른 입력을 찾는다고 본 점이다. 올바르게는 그것은 역상 탐색이 아니라 충돌 관련 성질이다.
③ X: 강한 충돌 저항성은 특정한 입력이 주어지지 않은 상태에서 서로 다른 두 입력 x, y를 찾아 $h(x) = h(y)$가 되게 만들기 어려운 성질이다. 틀린 부분은 주어진 x와 $h(x)$를 전제로 본 점이다. 올바르게는 주어진 입력 기준이면 약한 충돌 저항성이다.
④ O: 문제는 주어진 x와 $h(x)$에 대해 $y \neq x$이면서 $h(x) = h(y)$인 y를 찾기 어렵다고 했다. 이는 제2 역상 저항성이라고도 하는 약한 충돌 저항성의 정의와 일치한다.

오답 포인트

일방향성과 약한 충돌 저항성을 혼동하기 쉽다. 핵심은 무엇을 찾는지이다. 원래 입력 x를 찾으면 일방향성이고, 주어진 x와 같은 해시값을 내는 다른 y를 찾으면 약한 충돌 저항성이다. 또 강한 충돌 저항성은 특정 x가 미리 주어지지 않는다는 점에서 약한 충돌 저항성과 다르다.

NoteBase

다시 나오면 이렇게 판단

발문에서 주어진 정보가 해시값만인지, 특정 입력과 해시값 쌍인지, 아니면 아무 제약 없이 두 입력을 찾는지부터 구분하면 된다. 해시값에서 원문 복원은 일방향성, 특정 입력과 같은 해시를 만드는 다른 입력 탐색은 약한 충돌 저항성, 아무 두 입력의 충돌 탐색은 강한 충돌 저항성이다.

암기 포인트

원문 찾기 = 일방향성, 주어진 원문과 같은 해시 찾기 = 약한 충돌 저항성, 아무 충돌이나 찾기 = 강한 충돌 저항성이다.

NoteBase

문 4. 다음은 하이브리드 암호시스템을 이용하여 송신자가 메시지 M을 수신자에게 전달하기 위한 과정을 4단계로 나타낸 것이다. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

1. 송신자는 임의로 (가) K를 선택한다.
2. 송신자는 K를 이용하여 M을 (나) 암호 알고리즘으로 암호화한다.
3. 송신자는 K를 (다) 암호 알고리즘으로 암호화한다.
4. 송신자는 단계 2, 3에서 생성한 암호문을 수신자에게 전송한다.

① (가): 세션키, (나): 대칭키, (다): 공개키

② (가): 세션키, (나): 공개키, (다): 대칭키

③ (가): 공개키, (나): 대칭키, (다): 공개키

④ (가): 공개키, (나): 공개키, (다): 대칭키

정답 1번

출제 포인트

이 문제는 하이브리드 암호에서 세션키를 생성하고, 메시지는 대칭키로, 세션키는 공개키로 보호하는 절차를 묻는 문제이다.

올바른 순서

1. 송신자는 임의의 세션키 K를 선택한다.
2. 송신자는 K를 이용해 메시지 M을 대칭키 암호 알고리즘으로 암호화한다.
3. 송신자는 K를 수신자의 공개키 암호 알고리즘으로 암호화한다.
4. 단계 2와 단계 3의 결과를 함께 전송한다.

왜 이 순서인가: 메시지 M을 암호화하려면 먼저 세션키 K가 정해져 있어야 하고, 수신자만 K를 복호화할 수 있도록 K는 수신자의 공개키로 별도 보호해야 한다.

선지별 해설

① O: (가)=세션키, (나)=대칭키, (다)=공개키의 연결이 맞다. 하이브리드 암호는 데이터 본문은 빠른 대칭키로 암호화하고, 그 대칭키는 수신자의 공개키로 암호화해 전달한다.

② X: 틀린 부분은 (나)를 공개키, (다)를 대칭키로 둔 점이다. 올바르게는 메시지 M은 대칭키 알고리즘으로 암호화하고, 세션키 K는 공개키 알고리즘으로 암호화한다.

③ X: 틀린 부분은 (가)를 공개키로 둔 점이다. 올바르게는 송신자가 임의로 선택하는 것은 공개키가 아니라 일회성 세션키 K이다. 공개키는 수신자가 미리 가지고 공개한 키이다.

④ X: 틀린 부분은 (가)를 공개키, (나)를 공개키로 둔 점이다. 올바르게는 처음 선택하는 키는 세션키이고, 메시지 본문은 공개키가 아니라 대칭키로 암호화한다.

NoteBase

오답 포인트

공개키 암호가 더 안전하다는 인상 때문에 메시지 본문까지 공개키로 암호화한다고 착각하기 쉽다. 그러나 하이브리드 암호의 핵심은 본문은 속도 때문에 대칭키, 키 전달은 안전 때문에 공개키라는 역할 분담에 있다.

다시 나오면 이렇게 판단

하이브리드 암호 문제는 무엇을 암호화하는지 대상을 둘로 나누어 판단한다. 본문 데이터는 대칭키로 처리하고, 그 대칭키 자체는 수신자의 공개키로 보호한다고 연결하면 된다.

암기 포인트

본문은 대칭키, 키 전달은 공개키, 처음 고르는 키는 세션키이다.

NoteBase

문 5. AES에 대한 설명으로 옳지 않은 것은?

① SPN 구조를 사용한다.

② 128비트 블록 단위로 암호화한다.

③ 암호화 함수와 복호화 함수가 동일하다.

④ 키 길이에 따라 10, 12, 14 라운드로 구성된다.

정답 3번

출제 포인트

이 문제는 AES의 구조적 특징과 Feistel 구조와의 차이를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

AES는 대표적인 SPN(Substitution-Permutation Network) 기반 대칭키 블록암호이다. 블록 크기는 128비트로 고정되고, 키 길이에 따라 128비트는 10라운드, 192비트는 12라운드, 256비트는 14라운드로 동작한다. Feistel 구조는 암호화와 복호화가 같은 구조를 공유하지만, AES 같은 SPN 구조는 복호화에서 역치환, 역행이동, 역열혼합 등 역연산을 사용하므로 암호화 함수와 복호화 함수가 동일하지 않다.

선지별 해설

① O

AES는 치환과 순열을 반복하는 SPN 구조를 사용한다. Feistel 구조가 아니라는 점이 핵심이므로 이 선지는 옳다.

② O

AES는 128비트 블록 단위 블록암호이다. 키 길이는 128, 192, 256비트로 달라질 수 있지만 블록 크기는 128비트로 고정되므로 이 선지는 옳다.

③ X

틀린 부분은 "암호화 함수와 복호화 함수가 동일하다"는 표현이다. AES는 SPN 구조이므로 복호화 시 암호화와 동일한 함수를 그대로 쓰지 않고 각 단계의 역연산을 사용한다. 올바르게는 "AES는 암호화와 복호화에서 서로 대응되는 역연산을 사용하므로 함수가 동일하지 않다"이다.

④ O

AES는 키 길이에 따라 라운드 수가 달라진다. 128비트 키는 10라운드, 192비트 키는 12라운드, 256비트 키는 14라운드이므로 이 선지는 옳다.

NoteBase

오답 포인트

③은 Feistel 구조의 성질을 AES에 잘못 가져오면 틀리기 쉽다. 대칭키 블록암호라고 해서 모두 암호화와 복호화 구조가 같은 것은 아니며, AES는 SPN, DES는 Feistel이라는 구조 차이를 함께 묻는 함정이다.

다시 나오면 이렇게 판단

블록암호 선지에서는 먼저 구조를 구분한다. Feistel이면 암호화와 복호화의 큰 구조가 같고, SPN이면 복호화에 역연산이 필요하다고 판단하면 빠르게 정답을 고를 수 있다. 이어서 블록 크기와 키 길이에 따른 라운드 수를 분리해서 확인하면 된다.

암기 포인트

AES는 SPN, 블록은 128비트 고정, 라운드는 10·12·14, 복호화는 역연산 사용이다.

NoteBase

문 6. 인증 프로토콜에 대한 설명으로 옳지 않은 것은?

① S/Key 인증은 해시함수 체인을 사용한다.

② 공개키 암호를 이용한 인증에서는 상대방의 공개키를 알고 있어야 한다.

③ 영지식 증명(zero-knowledge proof)으로 비밀정보를 노출하지 않고 비밀정보의 소유를 증명할 수 있다.

④ 커버로스(Kerberos)에서 티켓발급 서버(TGS)는 서비스 서버의 접속에 필요한 티켓을 사용자의 공개키로 암호화하여 전달한다.

정답 4번

출제 포인트

이 문제는 S/Key, 공개키 기반 인증, 영지식 증명, Kerberos의 인증 방식과 사용 키를 구별하는 문제이다.

핵심 개념

S/Key는 일회용 패스워드를 위해 해시함수 체인을 쓰는 인증 방식이다. 공개키 기반 인증은 상대방의 공개키를 알고 있어야 서명 검증이나 공개키 암호화 기반 확인이 가능하다. 영지식 증명은 비밀 자체를 드러내지 않고 그 비밀을 알고 있음을 증명하는 방식이다. Kerberos는 기본적으로 대칭키 기반 티켓 인증 체계이며 공개키로 서비스 티켓을 주고받는 구조가 아니다.

선지별 해설

① O: S/Key는 해시값을 거꾸로 검증하는 일회용 패스워드 방식이므로 해시함수 체인을 사용한다.
② O: 공개키 암호를 이용한 인증에서는 상대방의 서명을 검증하거나 상대에게만 읽히는 값을 보내기 위해 상대방의 공개키를 알고 있어야 한다.
③ O: 영지식 증명은 비밀정보 그 자체를 공개하지 않으면서도 그 비밀을 알고 있음을 입증할 수 있는 방식이다.
④ X: 틀린 표현은 "사용자의 공개키로 암호화"이다. Kerberos의 TGS는 서비스 서버가 확인할 수 있도록 서비스 티켓을 서비스 서버의 비밀키로 암호화한다. 사용자에게 돌려주는 정보도 전통적 Kerberos에서는 사용자의 공개키가 아니라 사용자와 공유한 비밀정보를 바탕으로 보호된다.

오답 포인트

④는 공개키 인증과 Kerberos를 섞어 놓은 선지이다. 인증 프로토콜 문제에서는 어떤 키 체계를 쓰는지부터 구분해야 하는데, Kerberos를 공개키 기반 구조로 착각하면 바로 흔들린다.

다시 나오면 이렇게 판단

인증 프로토콜 선지는 먼저 사용 기술을 한 줄로 분류하면 빨라진다. S/Key는 해시 체인, 영지식 증명은 비밀 비노출 증명, Kerberos는 대칭키 티켓 방식으로 잡으면 공개키 관련 왜곡 선지를 바로 걸러낼 수 있다.

NoteBase

암기 포인트

S/Key는 해시 체인, ZKP는 비밀 비노출, Kerberos는 대칭키 티켓 인증이다.

NoteBase

문 7. 양자 컴퓨터 시대의 암호에 대한 설명으로 옳은 것은?

① AES는 키 길이를 증가시켜도 더 이상 안전성을 유지할 수 없다.

② 양자 키 분배 프로토콜을 사용하면 안전하게 암호키를 공유할 수 있다.

③ 양자내성암호(PQC)는 양자 알고리즘을 이용하여 양자 컴퓨터에서만 동작하도록 설계된 암호이다.

④ 인수분해의 어려움에 의존하는 RSA는 쇼어(Shor) 알고리즘을 이용한 양자 컴퓨터의 공격에도 안전성을 유지할 수 있다.

정답 2번

출제 포인트

이 문제는 양자 컴퓨터 시대에 대칭키 암호, 양자 키 분배, 양자내성암호, RSA의 보안 성질을 구분하는지 묻는 문제이다.

핵심 개념

대칭키 암호인 AES는 양자 컴퓨터가 있어도 구조가 바로 무너지는 것은 아니며, 브루트포스 공격에 대한 양자 가속은 주로 그로버 알고리즘에 따른 제곱근 수준 감소로 본다.
양자 키 분배(QKD)는 양자 상태를 이용해 도청 여부를 탐지하면서 비밀키를 공유하는 방식이다.
양자내성암호(PQC)는 양자 컴퓨터의 공격에도 견디도록 설계된 고전적 암호로서, 일반 디지털 컴퓨터와 기존 네트워크에서 운용할 수 있다.
RSA는 큰 수의 인수분해 어려움에 기대는 공개키 암호인데, 충분한 양자 컴퓨터에서는 쇼어 알고리즘에 취약하다.

선지별 해설

① X: 틀린 표현은 "키 길이를 증가시켜도 더 이상 안전성을 유지할 수 없다"이다. AES는 양자 시대에도 키 길이를 늘리면 보안 여유를 높일 수 있다. 예를 들어 브루트포스 난이도는 고전적으로 2^k인데, 양자 공격에서는 대체로 $2^{k/2}$ 수준으로 약화된다고 보므로 더 긴 키가 여전히 의미가 있다. 틀린 표현 → 올바르게는 "AES는 양자 컴퓨터 앞에서도 키 길이를 늘려 보안 여유를 확보할 수 있다"이다.
② O: 양자 키 분배 프로토콜은 키 자체를 안전하게 공유하는 기술이다. 양자 상태를 측정하면 흔적이 남는 성질을 이용하므로 도청을 탐지할 수 있고, 그 결과 비밀키 공유 수단으로 사용될 수 있다.
③ X: 틀린 표현은 "양자 알고리즘을 이용하여 양자 컴퓨터에서만 동작하도록 설계된 암호"이다. PQC는 양자 컴퓨터용 암호가 아니라 양자 컴퓨터의 공격에도 버티도록 만든 고전 암호이다. 틀린 표현 → 올바르게는 "PQC는 일반 컴퓨터에서 실행되면서 양자 공격에 견디도록 설계된 암호"이다.
④ X: 틀린 표현은 "쇼어 알고리즘을 이용한 양자 컴퓨터의 공격에도 안전성을 유지할 수 있다"이다. RSA는 인수분해 문제의 어려움에 의존하는데, 쇼어 알고리즘은 이 전제를 무너뜨린다. 틀린 표현 → 올바르게는 "RSA는 충분한 양자 컴퓨터와 쇼어 알고리즘 앞에서 안전하지 않다"이다.

NoteBase

오답 포인트

③의 "양자내성"을 "양자 컴퓨터에서 쓰는 암호"로 오해하면 틀리기 쉽다. 또한 ①처럼 대칭키 암호와 ④의 RSA를 같은 수준으로 취급하면 안 된다. 양자 시대에는 공개키 암호는 구조적으로 무너질 수 있지만, 대칭키 암호는 키 길이 확대로 대응 여지가 있다.

다시 나오면 이렇게 판단

양자 시대 암호 문제는 먼저 대칭키인지 공개키인지부터 구분한다. 그다음 QKD는 "키 공유 기술", PQC는 "양자 공격에 견디는 고전 암호", RSA는 "쇼어 알고리즘에 취약"으로 분류하면 빠르게 판단할 수 있다.

암기 포인트

QKD는 키를 나누는 기술, PQC는 양자 공격을 버티는 고전 암호, RSA는 쇼어에 취약, AES는 키를 늘려 대응한다.

NoteBase

문 8. 다음 설명에 해당하는 것은?

암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상하기 위해 신뢰 컴퓨팅 그룹(Trusted Computing Group)에서 표준화한 개념이다. 기본적으로 인증된 부트(authenticated boot), 인증, 암호화 기능을 제공한다.

① TrustZone

② SIEM(Security Information & Event Management)

③ TEE(Trusted Execution Environment)

④ TPM(Trusted Platform Module)

정답 4번

출제 포인트

이 문제는 TCG가 표준화한 하드웨어 보안 모듈인 TPM과 TrustZone, TEE, SIEM의 기능 차이를 구별하는 문제이다.

핵심 개념

TPM은 TCG가 표준화한 하드웨어 기반 신뢰 루트 모듈로서 키 저장, 플랫폼 무결성 측정, 인증, 부트 검증 지원, 암호 연산을 담당한다.
TrustZone은 ARM 프로세서의 보안 확장으로 일반 영역과 보안 영역을 분리해 민감 코드를 격리 실행하는 기술이다.
TEE는 일반 운영체제와 격리된 신뢰 실행 환경 전체를 뜻하는 개념이며, TrustZone은 이를 구현하는 한 방식이 될 수 있다.
SIEM은 여러 장비의 보안 로그와 이벤트를 수집·상관분석하는 관리 체계이다.

NoteBase

선지별 해설

① X: 틀린 부분은 TrustZone을 TCG가 표준화한 하드웨어 보안 모듈처럼 본 점이다. TrustZone은 ARM 아키텍처의 하드웨어 격리 기술이지 TPM처럼 별도의 신뢰 플랫폼 모듈이 아니다. 올바르게는 ARM 기반 보안 영역 분리 기술이라고 보아야 한다.
② X: 틀린 부분은 SIEM을 인증된 부트, 인증, 암호화 기능을 제공하는 하드웨어 보안 개념으로 본 점이다. SIEM은 로그 수집, 이벤트 상관분석, 보안 관제를 위한 시스템이다. 올바르게는 보안 정보 및 이벤트 관리 체계라고 보아야 한다.
③ X: 틀린 부분은 TEE를 TCG가 표준화한 TPM과 같은 개념으로 본 점이다. TEE는 신뢰 실행 환경이라는 상위 개념이며, 안전한 실행 공간을 제공하는 것이 핵심이다. 올바르게는 격리 실행 환경을 뜻하는 실행 보안 개념이라고 보아야 한다.
④ O: TCG가 표준화했고 인증, 암호화, 부트 과정의 신뢰 확보를 지원하는 하드웨어 기반 보안 모듈이라는 설명은 TPM에 해당한다. TPM은 키를 안전하게 저장하고 플랫폼 무결성을 측정해 신뢰 부팅과 원격 인증의 기반을 제공한다.

오답 포인트

TrustZone과 TEE는 둘 다 실행 환경 격리와 관련되어 있고 TPM도 하드웨어 기반 보안이라는 점에서 함께 묶여 보이기 쉽다. 그러나 문제의 핵심 단서는 TCG 표준화와 인증된 부트·인증·암호화 기능이며, 이 조합은 TPM을 직접 가리킨다.

다시 나오면 이렇게 판단

보기 설명에서 TCG, 하드웨어 보안 모듈, 키 저장, 무결성 측정, 신뢰 부팅, 인증이 함께 나오면 TPM으로 판단한다. 실행 영역 분리나 격리 실행이 중심이면 TrustZone 또는 TEE이고, 로그 수집과 이벤트 분석이 중심이면 SIEM으로 판단한다.

암기 포인트

TPM은 신뢰 부팅과 키 보호, TrustZone은 영역 분리, TEE는 격리 실행, SIEM은 로그 분석이다.

NoteBase

문 9. 「개인정보 보호법」상 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우

② 시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우

③ 교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우

④ 촬영된 영상정보를 저장하지 아니하는 경우로서 개인정보보호위원회가 정하는 경우

정답 4번

쟁점

이 문제는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 예외 사유를 묻는 문제이다.
핵심은 예외 사유의 내용과 그 예외를 정하는 주체를 정확히 구별하는 것이다.

용어 풀이

고정형 영상정보처리기기란 공개된 장소 등에 지속적으로 설치되어 사람이나 사물의 영상을 촬영하는 CCTV 등의 장치를 말한다.

핵심 구분

원칙적으로 공개된 장소에는 고정형 영상정보처리기기를 임의로 설치·운영할 수 없다. 다만 범죄 예방 및 수사, 시설의 안전 및 관리와 화재 예방, 교통단속, 교통정보의 수집·분석·제공, 촬영 영상을 저장하지 않는 대통령령상 경우 등 법이 정한 예외에서는 가능하다.
이 문제의 정답을 가르는 구분은 '예외 사유의 존재'와 '그 예외를 정하는 주체'이다. 촬영된 영상정보를 저장하지 아니하는 경우의 세부 예외는 개인정보보호위원회가 아니라 대통령령이 정한다.

NoteBase

선지별 해설

① O
범죄의 예방 및 수사를 위하여 필요한 경우는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 명시적 예외에 해당한다.

② O
시설의 안전 및 관리, 화재 예방을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우도 법이 허용하는 예외이다. 선지의 핵심은 '정당한 권한을 가진 자'라는 주체 요건까지 포함되어 있다는 점이다.

③ O
교통정보의 수집·분석 및 제공을 위하여 정당한 권한을 가진 자가 설치·운영하는 경우 역시 허용된다. 교통 관련 예외는 교통단속과 교통정보의 수집·분석·제공으로 나뉘는데, 이 선지는 후자를 정확히 적었다.

④ X
촬영된 영상정보를 저장하지 아니하는 경우 자체는 예외 사유가 될 수 있다. 그러나 그 경우를 정하는 주체를 '개인정보보호위원회'라고 한 부분이 틀렸다.
틀린 표현: '개인정보보호위원회가 정하는 경우'
올바른 표현: '대통령령으로 정하는 경우'
시행령은 출입자 수, 성별, 연령대 등 통계값 또는 통계적 특성값 산출을 위해 영상을 일시적으로 처리하는 경우 등을 정하고 있다.

오답 포인트

④는 예외 사유의 방향 자체는 맞아서 쉽게 넘어가기 쉽다. 그러나 법률 문제에서는 '누가 정하는가'가 요건의 일부이므로, 대통령령 위임사항을 위원회 고시나 위원회 결정사항처럼 바꾸면 바로 오답이 된다.

다시 나오면 이렇게 판단

영상정보처리기기 설치 예외를 묻는 문제에서는 먼저 예외 사유 목록이 맞는지 확인하고, 다음으로 '정당한 권한을 가진 자', '대통령령으로 정하는 경우'처럼 주체와 위임 형식을 확인하면 된다. 내용이 비슷해 보여도 위임 주체가 바뀌면 틀린 선지로 판단된다.

암기 포인트

공개장소 CCTV 예외는 법 제25조의 열거사항이고, 저장하지 않는 예외의 세부 기준은 위원회가 아니라 대통령령이다.

NoteBase

문 10. ISMS-P 인증을 위한 '관리체계 수립 및 운영' 영역 중 하나인 '관리체계 운영'에 속하는 인증기준에 대한 설명으로 옳은 것은?

① 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.

② 선정한 보호대책을 이행계획에 따라 효과적으로 구현하고 경영진은 이행결과의 정확성과 효과성 여부를 확인하여야 한다.

③ 조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.

④ 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

정답 2번

쟁점

이 문제는 ISMS-P 인증기준 별표 7에서 1.2 위험 관리, 1.3 관리체계 운영, 1.4 관리체계 점검 및 개선의 세부 항목을 구별할 수 있는지를 묻는다.

용어 풀이

관리체계 운영은 선정된 보호대책을 실제로 구현·공유하고 운영활동을 기록·관리하는 단계이다.

핵심 구분

인증기준(제23조 관련) 별표 7에서 1.2는 정보자산 식별·현황 및 흐름분석·위험 평가·보호대책 선정을, 1.3은 보호대책 구현·보호대책 공유·운영현황 관리를, 1.4는 법적 요구사항 준수 검토·관리체계 점검·관리체계 개선을 뜻한다. 따라서 구현 여부를 묻는 ②만 1.3 관리체계 운영에 해당한다.

NoteBase

선지별 해설

① X: 이 문구는 1.2.2 현황 및 흐름분석에 해당한다. 정보서비스와 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 문서화하는 내용은 운영 단계가 아니라 위험 관리 단계의 현황 파악이다.
틀린 표현: "관리체계 운영에 속하는 기준"이라는 판단.
올바른 표현: 1.2 위험 관리의 "1.2.2 현황 및 흐름분석"에 속한다.
② O: 이 문구는 1.3.1 보호대책 구현의 내용과 일치한다. 선정한 보호대책을 이행계획에 따라 구현하고 경영진이 이행결과의 정확성과 효과성을 확인하는 것이 바로 관리체계 운영 단계이다.
③ X: 이 문구는 1.4.1 법적 요구사항 준수 검토에 해당한다. 법적 요구사항을 파악하여 규정에 반영하고 준수 여부를 지속적으로 검토하는 내용은 운영 자체가 아니라 점검 및 개선 단계의 기준이다.
틀린 표현: "관리체계 운영에 속하는 기준"이라는 판단.
올바른 표현: 1.4 관리체계 점검 및 개선의 "1.4.1 법적 요구사항 준수 검토"에 속한다.
④ X: 이 문구는 1.2.1 정보자산 식별에 해당한다. 정보자산을 식별·분류하고 중요도를 산정해 목록을 최신으로 관리하는 내용은 위험 관리의 출발점이지 관리체계 운영 기준이 아니다.
틀린 표현: "관리체계 운영에 속하는 기준"이라는 판단.
올바른 표현: 1.2 위험 관리의 "1.2.1 정보자산 식별"에 속한다.

오답 포인트

①, ③, ④는 모두 실제 운영과 가까운 표현이 들어 있어 1.3처럼 보이지만, 기준 체계상 ①과 ④는 1.2 위험 관리이고 ③은 1.4 점검 및 개선이다. 특히 "최신성 유지", "지속적 검토", "목록 관리" 같은 표현만 보고 운영 단계로 묶으면 틀리기 쉽다.

다시 나오면 이렇게 판단

문장의 동사를 기준으로 분류하면 된다. 식별·분석·평가·선정이면 1.2 위험 관리, 구현·공유·운영기록이면 1.3 관리체계 운영, 준수검토·점검·개선이면 1.4 관리체계 점검 및 개선으로 본다.

암기 포인트

1.2는 파악하고 고르는 단계, 1.3은 구현하고 굴리는 단계, 1.4는 점검하고 고치는 단계이다.

NoteBase

문 11. 재사용이 불가능하도록 매번 새로운 패스워드를 생성하는 인증 방식은?

① SSO

② OTP

③ PIN

④ RADIUS

정답 2번

출제 포인트

이 문제는 OTP와 SSO, PIN, RADIUS의 개념 차이를 구분하는 문제이다.

핵심 개념

OTP는 한 번만 사용할 수 있도록 매번 새로 생성되는 일회용 비밀번호이다. SSO는 한 번의 로그인으로 여러 시스템에 접근하는 통합 인증 방식이다. PIN은 사용자가 미리 정해 두고 반복 사용할 수 있는 개인 식별 번호이다. RADIUS는 원격 접속 환경 등에서 인증, 권한 부여, 계정을 중앙에서 처리하는 AAA 프로토콜이다.

선지별 해설

① X. SSO는 Single Sign-On으로, 한 번 인증하면 여러 서비스에 다시 로그인하지 않고 접근하는 방식이다. 틀린 표현은 "매번 새로운 패스워드"이다. 올바르게는 "한 번의 인증으로 여러 시스템을 이용하는 통합 인증 방식"이다.
② O. OTP는 One-Time Password로, 재사용이 불가능하도록 인증 시마다 새로운 비밀번호를 생성하거나 제공하는 방식이므로 발문과 일치한다.
③ X. PIN은 Personal Identification Number로, 사용자가 기억하고 반복 사용할 수 있는 고정형 비밀 번호에 가깝다. 틀린 표현은 "매번 새로운 패스워드"이다. 올바르게는 "사용자가 설정해 두고 계속 사용할 수 있는 개인 식별 번호"이다.
④ X. RADIUS는 Remote Authentication Dial-In User Service로, 중앙 인증 서버와 네트워크 장비가 인증 정보를 주고받는 프로토콜이다. 틀린 표현은 "새로운 패스워드를 생성하는 인증 방식"이다. 올바르게는 "인증과 권한 부여를 중앙에서 처리하는 AAA 프로토콜"이다.

오답 포인트

약어 자체만 보고 고르면 SSO, OTP, PIN, RADIUS가 모두 인증과 관련 있어 보이기 때문에 혼동하기 쉽다. 이 문항은 ①의 통합 인증, ③의 고정 비밀번호, ④의 인증 프로토콜을 ②의 일회용 비밀번호와 구별하는지가 핵심 함정이다.

NoteBase

다시 나오면 이렇게 판단

발문에 "재사용 불가", "매번 새로 생성", "일회용" 같은 표현이 있으면 OTP를 먼저 떠올리면 된다. 반대로 한 번 로그인으로 여러 서비스를 쓰는 것은 SSO, 고정 숫자 비밀번호는 PIN, 중앙 인증 서버 프로토콜은 RADIUS로 판단한다.

암기 포인트

OTP는 일회용, SSO는 한 번 로그인, PIN은 고정 번호, RADIUS는 중앙 인증 프로토콜이다.

NoteBase

문 12. 다음 설명의 (가), (나)에 들어갈 용어를 바르게 연결한 것은?

무선 랜 보안을 위해 WEP(Wired Equivalent Privacy)에서는 (가)를 암호화 알고리즘으로 사용하였다. 이후에 WEP 방식의 보안 취약점을 해결하기 위하여 IEEE 802.11i 표준이 만들어졌는데, 여기서는 무선 데이터의 무결성과 기밀성을 제공하기 위하여 AES를 기반으로 하는 (나)를 제안하였다.

① (가): CRC-32, (나): CCMP

② (가): CRC-32, (나): TKIP

③ (가): RC4, (나): CCMP

④ (가): RC4, (나): TKIP

정답 3번

출제 포인트

이 문제는 WEP의 암호 알고리즘과 IEEE 802.11i에서 채택한 AES 기반 보호 방식의 차이를 정확히 구별하는지를 묻는다.

핵심 개념

WEP는 무선 LAN 초기 보안 방식으로 스트림 암호인 RC4를 사용한 방식이다. CRC-32는 WEP에서 무결성 점검값으로 쓰인 것이지 암호화 알고리즘이 아니다. CCMP는 AES를 기반으로 기밀성과 무결성을 함께 제공하는 802.11i의 핵심 보호 방식이다. TKIP는 WEP의 취약점을 완화하기 위한 과도기적 방식으로 RC4를 계속 사용하며 AES 기반 방식이 아니다.

선지별 해설

1번: X. (가)를 CRC-32로 본 부분이 틀리다. CRC-32는 WEP의 무결성 확인용 ICV 계산에 쓰이는 값일 뿐 암호화 알고리즘이 아니다. 또한 (나)인 CCMP는 AES 기반이라는 점은 맞지만 (가)가 틀려서 전체 선지는 오답이다. 틀린 표현은 "CRC-32"이고, 올바르게는 "RC4"이다.
2번: X. CRC-32는 암호화 알고리즘이 아니므로 (가)가 틀리다. 또한 TKIP는 WEP 보완용 과도기 기술로 RC4를 사용하므로 AES 기반 방식이라는 설명에도 맞지 않는다. 틀린 표현은 "CRC-32"와 "AES를 기반으로 하는 TKIP"이고, 올바르게는 "RC4"와 "TKIP는 RC4 기반"이다.
3번: O. WEP는 암호화에 RC4를 사용하였다. IEEE 802.11i에서는 AES를 기반으로 한 CCMP를 도입하여 기밀성과 무결성을 강화하였다. 따라서 (가)=RC4, (나)=CCMP의 연결이 맞다.
4번: X. WEP에 RC4를 사용한 점은 맞지만, TKIP는 AES 기반 방식이 아니라 RC4 기반의 임시 보완책이다. 틀린 표현은 "AES를 기반으로 하는 TKIP"이고, 올바르게는 "AES를 기반으로 하는 방식은 CCMP"이다.

NoteBase

오답 포인트

CRC-32를 암호 알고리즘으로 착각하거나, TKIP와 CCMP를 모두 WEP 이후 보안 기술이라는 이유만으로 같은 계열로 묶으면 틀린다. 이 문제의 함정은 "AES 기반"이라는 조건이 CCMP만 가리킨다는 점이다.

다시 나오면 이렇게 판단

무선 LAN 보안 문제에서는 먼저 암호화 알고리즘인지 무결성 검사값인지부터 구분한다. 그다음 WEP는 RC4, TKIP도 RC4 계열의 보완책, CCMP만 AES 기반이라는 축으로 판단하면 된다.

암기 포인트

WEP는 RC4, WPA2의 핵심은 AES-CCMP, CRC-32는 암호가 아니라 무결성 점검값이다.

NoteBase

문 13. 다음 제시문에 해당하는 위험처리 전략은?

어떤 조직에서 시스템 로그인 패스워드의 도용을 방지하기 위하여 3가지 이상의 문자 조합으로 8글자 이상의 패스워드가 강제 설정되도록 하는 모듈을 개발·적용하려고 한다.

① 위험감소
② 위험회피
③ 위험전가
④ 위험수용

정답 1번

출제 포인트

이 문제는 위험회피·위험전가·위험수용과 구별되는 위험감소의 의미를 묻는 문제이다.

핵심 개념

위험감소는 보안통제나 보호대책을 적용해 위험의 발생 가능성이나 영향을 낮추는 전략이다. 위험회피는 위험이 생기는 활동 자체를 중단하거나 제거하는 전략이다. 위험전가는 보험, 외주, 계약 등으로 위험 부담을 제3자에게 이전하는 전략이다. 위험수용은 추가 통제를 하지 않고 현재 위험을 감내하는 전략이다.

선지별 해설

① O: 강한 패스워드 설정 모듈을 개발·적용하는 것은 로그인 비밀번호 도용 가능성을 낮추는 통제를 추가하는 것이므로 위험감소에 해당한다.
② X: 틀린 부분은 '위험회피'이다. 제시문은 로그인 사용 자체를 없애거나 해당 업무를 중단하는 것이 아니라 보안 수준을 높여 위험을 줄이는 것이므로 올바르게는 '위험감소'이다.
③ X: 틀린 부분은 '위험전가'이다. 보험 가입이나 외부 전문업체 계약처럼 위험 부담을 제3자에게 넘기는 내용이 없으므로 올바르게는 '위험감소'이다.
④ X: 틀린 부분은 '위험수용'이다. 위험수용은 추가 대책 없이 위험을 받아들이는 것인데, 제시문은 모듈을 개발·적용하는 적극적 통제를 설명하므로 올바르게는 '위험감소'이다.

오답 포인트

패스워드 관련 조치를 보면 막연히 '아예 안 쓰는 것'처럼 느껴 ② 위험회피로 오해하기 쉽다. 그러나 문장의 핵심은 사용 중단이 아니라 강제 설정 모듈을 도입해 도용 가능성을 낮춘다는 점이다.

NoteBase

다시 나오면 이렇게 판단

보안대책을 새로 적용해 위험의 확률이나 피해를 줄이면 위험감소이다. 위험 원인을 없애면 위험회피이고, 제3자에게 부담을 넘기면 위험전가이며, 아무 조치 없이 감내하면 위험수용이다.

암기 포인트

줄이면 위험감소, 없애면 위험회피, 넘기면 위험전가, 그냥 감내하면 위험수용이다.

NoteBase

문 14. 반사형 XSS 공격에 대한 설명으로 옳은 것은?

① 악성 스크립트가 웹 서버에서 실행된다.

② 악성 스크립트는 웹 서버 측 데이터베이스에 저장된다.

③ 공격자가 보낸 악의적 링크를 사용자가 클릭하게 한다.

④ 사용자와 웹 서버 간의 신뢰 관계를 악용하여 공격자가 원하는 서버 동작을 발생시킨다.

정답 3번

출제 포인트

이 문제는 반사형 XSS의 동작 위치와 공격 성립 조건을 저장형 XSS, CSRF와 구별할 수 있는지를 묻는다.

핵심 개념

반사형 XSS는 공격자가 넣은 스크립트가 요청값에 섞여 서버 응답에 반사된 뒤 사용자 브라우저에서 실행되는 공격이다. 저장형 XSS는 악성 스크립트가 게시글·댓글 등 서버 측 저장소에 저장된 뒤 여러 사용자에게 전달되는 공격이다. CSRF는 사용자의 인증 상태를 악용하여 사용자가 의도하지 않은 서버 요청을 보내게 만드는 공격이다.

선지별 해설

1번 X: 반사형 XSS의 악성 스크립트는 웹 서버가 아니라 사용자 브라우저에서 실행된다. 틀린 표현은 "웹 서버에서 실행된다"이다. 올바르게는 "서버 응답에 포함된 스크립트가 클라이언트 브라우저에서 실행된다"이다.
2번 X: 악성 스크립트가 웹 서버 측 데이터베이스에 저장되는 형태는 저장형 XSS이다. 틀린 표현은 "데이터베이스에 저장된다"이다. 올바르게는 "반사형 XSS는 스크립트가 저장되지 않고 요청과 응답 과정에서 반사된다"이다.
3번 O: 반사형 XSS는 공격자가 조작한 URL이나 링크를 사용자에게 클릭하게 하여, 그 요청값이 서버 응답에 반사되면서 브라우저에서 스크립트가 실행되도록 유도하는 방식이 전형적이다.
4번 X: 사용자와 웹 서버 간의 신뢰 관계를 이용해 원하지 않는 서버 동작을 일으키는 설명은 CSRF에 가깝다. 틀린 표현은 "공격자가 원하는 서버 동작을 발생시킨다"이다. 올바르게는 "반사형 XSS는 사용자의 브라우저에서 스크립트를 실행시켜 쿠키 탈취나 세션 하이재킹 같은 클라이언트 측 피해를 유발한다"이다.

오답 포인트

2번의 "저장된다"는 저장형 XSS의 키워드이고, 4번의 "원하는 서버 동작"은 CSRF의 키워드이다. 반사형 XSS는 저장 여부와 서버 동작 유발 여부보다 "링크 클릭 후 응답에 반사되어 브라우저에서 실행된다"는 흐름으로 잡아야 한다.

NoteBase

다시 나오면 이렇게 판단

먼저 스크립트가 어디서 실행되는지 본다. 브라우저에서 실행되면 XSS 계열이고, 서버가 원치 않는 요청을 수행하면 CSRF 쪽이다. 그다음 스크립트가 서버에 저장되면 저장형 XSS, 저장되지 않고 요청값이 바로 응답에 반사되면 반사형 XSS로 판단된다.

암기 포인트

반사형 XSS는 링크 클릭, 저장형 XSS는 서버 저장, CSRF는 강제 요청이다.

NoteBase

문 15. ISMS-P 인증 추진체계에서 인증기관에 해당하는 것은?

① 금융보안원(FSI)

② 한국정보통신진흥협회(KAIT)

③ 한국정보통신기술협회(TTA)

④ 개인정보보호협회(OPA)

정답 1번

출제 포인트

이 문제는 ISMS-P 추진체계에서 인증기관과 심사기관의 역할 구분을 묻는 문제이다.

핵심 개념

인증기관은 인증 여부를 심의·발급·유지하는 기관이고, 심사기관은 인증심사를 수행하는 기관이다. ISMS-P 체계에서 한국인터넷진흥원(KISA)과 금융보안원(FSI)은 인증기관에 해당하고,
한국정보통신진흥협회(KAIT)·한국정보통신기술협회(TTA)·개인정보보호협회(OPA)는 심사기관에 해당한다.

선지별 해설

① O: 금융보안원(FSI)은 ISMS-P 추진체계에서 금융분야 인증심사와 인증서 발급을 담당하는 인증기관이다.
② X: 틀린 부분은 인증기관이라는 판단이다. 한국정보통신진흥협회(KAIT)는 인증기관이 아니라 인증심사를 수행하는 심사기관이다.
③ X: 틀린 부분은 인증기관이라는 판단이다. 한국정보통신기술협회(TTA)는 인증기관이 아니라 인증심사를 수행하는 심사기관이다.
④ X: 틀린 부분은 인증기관이라는 판단이다. 개인정보보호협회(OPA)는 인증기관이 아니라 인증심사를 수행하는 심사기관이다.

오답 포인트

KAIT, TTA, OPA는 실제 인증심사에 참여하는 기관이라 이름이 익숙해 인증기관으로 착각하기 쉽다. 그러나 심사를 수행하는 것과 인증서를 발급·유지하는 것은 구분되며, 이 차이를 묻는 함정이다.

다시 나오면 이렇게 판단

기관 문제가 나오면 먼저 그 기관이 인증을 최종 심의·발급하는지, 아니면 현장 인증심사를 수행하는지로 나누어 본다. 인증서 발급과 인증 유지 권한이 있으면 인증기관이고, 심사 수행 역할이면 심사기관이다.

암기 포인트

ISMS-P는 인증기관 KISA·FSI, 심사기관 KAIT·TTA·OPA로 구분한다.

NoteBase

문 16. 리눅스의 find 명령에 대한 설명으로 옳지 않은 것은?

① 명령: find / -name '*.c' 설명: 확장자가 c인 파일을 모두 찾는다.

② 명령: find / -mtime -2 설명: 최근 48시간 이내에 마지막으로 수정된 파일을 모두 찾는다.

③ 명령: find / -user user1 설명: 소유자가 user1인 파일을 모두 찾는다.

④ 명령: find / -type 4755 설명: 권한 설정이 4755로 설정된 파일을 모두 찾는다.

정답 4번

출제 포인트

이 문제는 리눅스 find 명령의 검색 조건 옵션이 무엇을 의미하는지 구별할 수 있는지를 묻는다.

핵심 개념

-name은 파일 이름 패턴으로 검색하는 옵션이다. -mtime은 수정 시각 기준의 경과 일수로 검색하는 옵션이다. -user는 소유자 이름으로 검색하는 옵션이다. -type은 파일 종류를 뜻하는 옵션이고, 권한 값 검색은 -perm으로 처리한다.

선지별 해설

① O: `find / -name '*.c'`는 루트 디렉터리 아래에서 이름이 `.c`로 끝나는 파일을 찾는 명령이다. 설명처럼 확장자가 c인 파일을 찾는 뜻으로 볼 수 있다.
② O: `-mtime -2`는 현재 시점에서 2일 미만 전에 수정된 파일을 뜻하므로 최근 48시간 이내에 마지막으로 수정된 파일을 찾는 설명이 맞다.
③ O: `-user user1`은 소유자가 `user1`인 파일을 찾는 조건이다. 설명과 일치한다.
④ X: 틀린 부분은 `-type 4755`이다. `-type`은 파일 종류를 `f`, `d`, `l`처럼 지정하는 옵션이므로 4755 같은 권한 값을 넣지 않는다. 권한 설정이 4755인 파일을 찾으려면 `find / -perm 4755`처럼 써야 한다.

오답 포인트

`-type`과 `-perm`을 모두 조건 옵션으로만 보고 역할을 섞으면 틀린다. 이 문항은 숫자 4755를 보고 권한 검색이라는 점을 떠올릴 수 있는지가 함정 포인트이다.

다시 나오면 이렇게 판단

find 옵션 뒤의 인자가 이름 패턴인지, 시간 조건인지, 사용자명인지, 파일 종류인지 먼저 분류한다. 숫자 권한값이 나오면 `-perm`, 파일 종류 문자가 나오면 `-type`으로 판단한다.

암기 포인트

`-name`은 이름, `-mtime`은 수정시간, `-user`는 소유자, `-type`은 종류, 권한값은 `-perm`이다.

NoteBase

문 17. DNS 스푸핑 공격에 대한 설명으로 옳지 않은 것은?

① 사용자가 악의적인 웹 사이트에 접속하도록 하는 공격이다.

② 공격자는 사용자의 DNS 질의에 대해 위조된(spoofed) 응답이 사용자에게 전달되게 한다.

③ DNS 캐시 포이즈닝(poisoning)은 위조된 DNS 응답이 로컬 DNS 서버의 캐시에 저장되므로 일정 기간 사용자에게 피해를 줄 수 있다.

④ 디지털 서명으로 DNS 데이터그램의 진위 여부를 확인할 수 있는 SSH(Secure Shell)가 DNS 캐시 포이즈닝 공격을 방지하기 위해 설계되었다.

정답 4번

출제 포인트

이 문제는 DNS 스푸핑, DNS 캐시 포이즈닝, DNSSEC의 기능을 구별할 수 있는지를 묻는 문제이다.

핵심 개념

DNS 스푸핑은 정상 도메인 이름에 대한 응답을 위조해 사용자를 다른 IP로 유도하는 공격이다. DNS 캐시 포이즈닝은 그 위조 응답이 DNS 서버나 리졸버의 캐시에 저장되어 일정 기간 계속 영향을 주는 상태이다. DNSSEC는 DNS 데이터의 무결성과 출처 진위를 디지털 서명으로 검증하는 보안 확장이다.

선지별 해설

① O: DNS 스푸핑은 사용자가 정상 사이트로 안다고 믿고 접속했는데 실제로는 공격자가 유도한 악성 웹 사이트로 연결되게 만드는 공격이다. 도메인 이름과 IP 주소의 대응관계를 속인다는 점이 핵심이다.
② O: 공격자는 사용자의 DNS 질의보다 먼저 또는 그에 맞춰 위조된 DNS 응답을 보내 사용자가 그 응답을 받게 만든다. 스푸핑의 본질이 위조된 응답 전달이라는 설명이므로 옳다.
③ O: DNS 캐시 포이즈닝은 위조된 DNS 응답이 로컬 DNS 서버나 리졸버 캐시에 남아 TTL 동안 반복적으로 잘못된 주소를 돌려주게 만드는 공격이다. 1회성 위조보다 피해가 지속된다는 점을 설명하므로 옳다.
④ X: 틀린 부분은 "SSH(Secure Shell)가 DNS 캐시 포이즈닝 공격을 방지하기 위해 설계되었다"는 표현이다. 디지털 서명으로 DNS 데이터의 진위를 확인해 캐시 포이즈닝을 완화하는 기술은 SSH가 아니라 DNSSEC이다.

오답 포인트

4번은 "디지털 서명", "진위 여부 확인"이라는 설명 자체는 DNSSEC의 특징과 맞기 때문에, 뒤에 붙은 용어가 SSH라는 점을 놓치면 맞는 선지처럼 보인다. 스푸핑과 포이즈닝의 관계도 혼동하기 쉬운데, 스푸핑은 위조 행위이고 포이즈닝은 그 결과가 캐시에 남는 상태이다.

NoteBase

다시 나오면 이렇게 판단

DNS 관련 보안 선지는 먼저 공격인지 방어기술인지를 나눈 뒤, 공격이면 위조 응답 자체인지 캐시 오염 지속인지 구분하고, 방어기술이면 디지털 서명 검증 주체가 DNSSEC인지 확인하면 된다.

암기 포인트

스푸핑은 위조 응답, 포이즈닝은 캐시 오염, 디지털 서명 검증은 DNSSEC이다.

NoteBase

문 18. 정보보호 최고책임자 또는 개인정보 보호책임자를 지정하도록 하는 근거가 되는 법률이 아닌 것은?

① 개인정보 보호법

② 전자금융거래법

③ 정보보호산업의 진흥에 관한 법률

④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정답 3번

쟁점

이 문제는 정보보호 최고책임자 또는 개인정보 보호책임자 지정 의무를 직접 두는 법률과, 정보보호 산업 진흥을 목적으로 하는 법률을 구별하는 문제이다.

용어 풀이

정보보호 최고책임자(CISO)는 조직의 정보보호 업무를 총괄하는 책임자이다.
개인정보 보호책임자(CPO)는 개인정보 처리와 보호 업무를 총괄하는 책임자이다.

핵심 구분

개인정보 보호법 제31조는 개인정보 보호책임자 지정을, 전자금융거래법 제21조의2와 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3은 정보보호최고책임자 지정을 직접 규정한다.
반면 정보보호산업의 진흥에 관한 법률은 정보보호산업의 기반 조성과 경쟁력 강화가 중심인 법률로서 정보보호 최고책임자나 개인정보 보호책임자 지정 의무를 직접 두지 않는다.

NoteBase

선지별 해설

① O
개인정보 보호법 제31조는 개인정보처리자에게 개인정보 보호책임자를 지정하도록 한다.
따라서 개인정보 보호책임자 지정의 직접 근거가 되는 법률이므로 옳은 선지이다.

② O
전자금융거래법 제21조의2는 금융회사 또는 전자금융업자에게 정보보호최고책임자를 지정하도록 한다.
전자금융업무와 정보기술부문 보안을 총괄할 책임자를 법에서 직접 요구하므로 옳은 선지이다.

③ X
정보보호산업의 진흥에 관한 법률은 정보보호산업 육성, 기반 조성, 우수기업 지정, 정보보호 공시 등 산업 진흥이 중심이다.
틀린 표현: 정보보호 최고책임자 또는 개인정보 보호책임자를 지정하도록 하는 근거가 되는 법률
올바른 표현: 정보보호산업의 진흥에 관한 법률은 정보보호 최고책임자 또는 개인정보 보호책임자 지정 의무의 직접 근거가 되지 않는 법률이다.

④ O
정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조의3은 정보통신서비스 제공자에게 정보보호 최고책임자를 지정하도록 한다.
따라서 정보보호 최고책임자 지정의 직접 근거가 되는 법률이므로 옳은 선지이다.

오답 포인트

법률명에 '정보보호'가 들어가면 모두 책임자 지정 의무를 둘 것이라고 연결하면 틀리기 쉽다. 이 문항의 함정은 '정보보호산업의 진흥에 관한 법률'처럼 산업 육성 법률과, 사업자에게 보호책임을 직접 부과하는 규제 법률을 구별하지 못하게 만드는 데 있다.

다시 나오면 이렇게 판단

책임자 지정 근거를 묻는 문제에서는 먼저 법이 누구에게 어떤 책임자를 지정하라고 직접 명령하는지 본다. 적용 대상 사업자나 개인정보처리자를 정하고 '지정하여야 한다'는 구조가 보이면 지정 근거 법률이고, 산업 진흥이나 지원이 중심이면 직접 근거가 아닌 경우가 많다.

암기 포인트

책임자 지정은 보호의무 법률에서 직접 나오고, 산업진흥법은 지정 의무의 근거가 아니다.

NoteBase

문 19. 리눅스 /etc/group 파일의 4개 필드에 대한 설명으로 옳지 않은 것은?

① 첫 번째 필드는 그룹의 이름을 나타낸다. groupadd 명령을 이용하여 새로운 그룹을 생성할 수 있다.

② 두 번째 필드는 그룹 패스워드를 나타내는 부분이지만 /etc/gshadow 파일에서 별도 관리하는 경우에는 'x'로만 표기된다.

③ 세 번째 필드는 리눅스에서 그룹에 부여한 번호로 그룹 생성 이후에는 변경할 수 없다.

④ 네 번째 필드에 해당 그룹에 속한 사용자의 로그인 ID가 기록된다.

정답 3번

출제 포인트

이 문제는 /etc/group의 필드 순서와 각 필드의 의미, 특히 세 번째 필드인 GID의 성격을 정확히 구분하는지를 묻는 문제이다.

핵심 개념

/etc/group의 기본 형식은 이름:암호표시값:GID:멤버목록이다. 첫 번째 필드는 그룹명, 두 번째 필드는 그룹 암호 또는 그 대체 표시값, 세 번째 필드는 그룹 식별 번호인 GID, 네 번째 필드는 그 그룹에 명시적으로 속한 사용자 계정 목록이다.

선지별 해설

① O. 첫 번째 필드는 그룹의 이름이다. `groupadd` 명령은 새 그룹을 만들면서 이 그룹명 항목을 /etc/group에 추가한다.
② O. 두 번째 필드는 그룹 패스워드 자리이다. 실제 암호 정보를 /etc/gshadow에서 별도로 관리하면 /etc/group에는 `x`만 표시된다.
③ X. 틀린 부분은 "그룹 생성 이후에는 변경할 수 없다"는 표현이다. 세 번째 필드는 그룹에 부여된 번호인 GID이지만 고정 불변 값은 아니다. `groupmod -g` 같은 관리 명령으로 변경할 수 있다. 올바르게는 "세 번째 필드는 그룹 GID이며 필요에 따라 변경할 수 있다"이다.
④ O. 네 번째 필드는 해당 그룹의 멤버 사용자 로그인 ID를 쉼표로 기록하는 자리이다. 즉 그룹 구성원 목록을 저장하는 필드이다.

오답 포인트

③은 숫자 식별자라는 이유만으로 한 번 정해지면 바뀌지 않는다고 착각하게 만드는 선지이다. 이 파일의 필드는 불변 속성이 아니라 관리 대상 정보이므로, 이름과 GID 모두 관리자 명령으로 수정될 수 있다는 점이 함정의 핵심이다.

NoteBase

다시 나오면 이렇게 판단

/etc/group 문제는 먼저 필드 순서를 이름-암호표시값-GID-멤버목록으로 고정해 두고, 선지에 "변경 불가" 같은 단정 표현이 나오면 실제 관리 명령으로 수정 가능한지부터 판단하면 된다.

암기 포인트

/etc/group = 이름 : 암호표시값 : GID : 멤버목록이다.

NoteBase

문 20. 「정보통신기반 보호법」의 내용으로 옳지 않은 것은?

① 「정보통신기반 보호법」은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

② 과학기술정보통신부장관과 국가정보원장등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다.

③ 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설인 도로·철도·지하철·공항·항만 등 주요 교통시설에 대한 관리기관의 장이 「정보통신기반 보호법」 제7조제1항에 따라 기술적 지원을 요청하는 경우 과학기술정보통신부장관에게 우선적으로 그 지원을 요청하여야 한다.

④ 중앙행정기관의 장은 새로운 형태의 전자적 침해행위로부터 주요정보통신기반시설을 보호하기 위하여 필요한 경우이거나, 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요한 경우에 해당 관리기관의 장에게 주요정보통신기반시설의 취약점을 분석·평가하도록 명령할 수 있다.

정답 3번

쟁점

이 문제는 주요정보통신기반시설 보호지원, 지정 권고, 취약점 분석·평가 명령의 주체와 요건을 정확히 구별하는 문제이다.

용어 풀이

주요정보통신기반시설은 전자적 침해행위로 기능이 마비될 경우 국가안전보장과 국민생활에 큰 피해를 줄 수 있어 법에 따라 보호되는 정보통신기반시설이다.

핵심 구분

일반적인 기술적 지원 요청은 과학기술정보통신부장관과 국가정보원장등 또는 전문기관의 장에게 할 수 있다. 다만 국가안전보장에 중대한 영향을 미치는 주요 교통시설 등은 국가정보원장에게 우선적으로 요청하여야 한다. 또한 특정 시설을 주요정보통신기반시설로 지정할 필요가 있으면 과학기술정보통신부장관과 국가정보원장등이 중앙행정기관의 장에게 지정 권고를 할 수 있고, 새로운 전자적 침해행위나 중대한 변화가 있으면 중앙행정기관의 장이 취약점 분석·평가를 명령할 수 있다.

NoteBase

선지별 해설

① O
- 법의 목적 조항과 같다. 전자적 침해행위에 대비하여 주요정보통신기반시설 보호대책을 수립·시행하고, 시설의 안정적 운용을 통해 국가의 안전과 국민생활의 안정을 보장하는 것이 목적이다.

② O
- 주요정보통신기반시설 지정 권고에 관한 조문과 같다. 과학기술정보통신부장관과 국가정보원장등은 특정 시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하면 중앙행정기관의 장에게 지정 권고를 할 수 있다.

③ X
- 국가안전보장에 중대한 영향을 미치는 도로·철도·지하철·공항·항만 등 주요 교통시설의 관리기관이 기술적 지원을 요청하는 경우에는 국가정보원장에게 우선적으로 요청하여야 한다.
- 틀린 표현: "과학기술정보통신부장관에게 우선적으로 그 지원을 요청하여야 한다"
- 올바른 표현: "국가정보원장에게 우선적으로 그 지원을 요청하여야 한다"

④ O
- 중앙행정기관의 장은 새로운 형태의 전자적 침해행위에 대응할 필요가 있거나 주요정보통신기반시설에 중대한 변화가 생겨 별도의 취약점 분석·평가가 필요하면 해당 관리기관의 장에게 취약점 분석·평가를 명령할 수 있다.

오답 포인트

③은 기술적 지원의 우선 요청 상대를 바꿔 놓은 함정이다. 제7조 제1항의 일반 규정만 기억하면 과학기술정보통신부장관도 요청 대상이라고 생각하기 쉽지만, 주요 교통시설 등 국가안전보장에 중대한 영향을 미치는 시설은 제7조 제2항에 따라 국가정보원장 우선 요청이 적용된다.

다시 나오면 이렇게 판단

정보통신기반 보호법 문제는 먼저 행위 주체를 확인하고, 그다음 일반 규정인지 국가안전보장 관련 예외 규정인지를 구분하면 된다. 특히 "우선적으로", "권고할 수 있다", "명령할 수 있다" 같은 표현은 주체와 재량 여부를 함께 본다.

암기 포인트

지정은 권고, 변화는 평가 명령, 국가안보 영향 교통시설 지원은 국정원 우선이다.

NoteBase

문 21. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」상 클라우드컴퓨팅서비스 제공자가 즉시 그 사실을 과학기술정보통신부장관에게 알려야 하는 경우는?

① 이용자 정보가 유출된 때

② 클라우드컴퓨팅 사업의 수요가 대규모로 발생한 때

③ 사전예고 없이 당사자 간 계약으로 정하였거나 대통령령으로 정하는 기간 이상 서비스 중단이 발생한 때

④ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생한 때

정답 1번

쟁점

이 문제는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」상 클라우드컴퓨팅서비스 제공자의 통지의무 중 과학기술정보통신부장관에게 즉시 알려야 하는 사유를 묻는 문제이다. 핵심은 이용자에게 지체 없이 알려야 하는 사유와 장관에게 즉시 알려야 하는 사유를 구별하는 데 있다.

용어 풀이

침해사고는 해킹, 악성프로그램 유포, 서비스 공격 등으로 정보통신망이나 관련 시스템의 안전성이 침해된 사고를 뜻한다. 이용자 정보 유출은 이용자 정보가 권한 없는 자에게 넘어가거나 공개된 상태를 뜻한다.

핵심 구분

법은 침해사고 발생, 이용자 정보 유출, 사전예고 없는 일정 기간 이상 서비스 중단을 우선 해당 이용자에게 지체 없이 알려야 하는 사유로 규정한다. 그중 과학기술정보통신부장관에게 즉시 알려야 하는 경우는 이용자 정보가 유출된 때만 별도로 정하고 있다. 즉, 제25조는 이용자 통지와 장관 즉시 통지를 분리하고, 장관 즉시 통지는 이용자 정보 유출에 한정한다.

NoteBase

선지별 해설

① O: 이용자 정보가 유출된 때는 해당 이용자에게 알릴 뿐 아니라 과학기술정보통신부장관에게도 즉시 알려야 하는 경우이다. 장관 즉시 통지의 직접 대상이 되는 유일한 사유이므로 옳다.
② X: 클라우드컴퓨팅 사업의 수요가 대규모로 발생한 때는 법이 정한 통지사유가 아니다. 틀린 표현은 "클라우드컴퓨팅 사업의 수요가 대규모로 발생한 때"이다. 올바르게는 침해사고 발생, 이용자 정보 유출, 사전예고 없는 일정 기간 이상 서비스 중단이 법정 통지사유이다.
③ X: 사전예고 없이 당사자 간 계약 또는 대통령령으로 정한 기간 이상 서비스 중단이 발생한 때는 해당 이용자에게 지체 없이 알려야 하는 사유이다. 장관에게 즉시 알려야 하는 사유는 아니다. 틀린 표현은 "즉시 그 사실을 과학기술정보통신부장관에게 알려야 하는 경우"이다. 올바르게는 해당 이용자에게 지체 없이 알려야 한다.
④ X: 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생한 때도 이용자 통지 사유에는 해당하지만, 장관 즉시 통지 사유에는 해당하지 않는다. 틀린 표현은 "과학기술정보통신부장관에게 알려야 하는 경우"에 포함된다는 전제이다. 올바르게는 침해사고 발생은 해당 이용자에게 지체 없이 알려야 하는 경우이다.

오답 포인트

이 문제를 틀렸다면 제25조 제1항의 이용자 통지 사유와 제2항의 장관 즉시 통지 사유를 한 덩어리로 외웠을 가능성이 높다. ③과 ④는 실제 법정 사유이므로 눈에 익숙하지만, 통지 상대방이 이용자인지 장관인지에서 답이 갈린다.

다시 나오면 이렇게 판단

법령 문제에서 "누구에게 알려야 하는가"를 묻는 경우에는 먼저 통지사유 자체가 맞는지 확인하고, 다음으로 통지 상대방이 이용자인지 감독기관인지 분리해서 본다. 이 조문에서는 장관 즉시 통지가 붙는 것은 이용자 정보 유출 하나뿐이다.

암기 포인트

클라우드법 제25조는 셋은 이용자 통지, 그중 정보유출만 장관 즉시 통지로 정리된다.

NoteBase

문 22. 패킷 필터링 방화벽에서는 포트 번호를 사용하여 특정 서비스를 허용하거나 차단하는 필터링 규칙을 적용한다. 서비스 명과 포트 번호가 옳게 짝지어지지 않은 것은?

① DNS - 161

② FTP(제어) - 21

③ HTTPS - 443

④ SMTP - 25

정답 1번

출제 포인트

이 문제는 대표적인 인터넷 서비스와 well-known port 번호의 기본 대응 관계를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

DNS는 도메인 이름을 IP 주소로 변환하는 이름 해석 서비스로 기본 포트는 53이다. FTP(제어)는 파일 전송 세션의 제어 채널로 21번 포트를 사용한다. HTTPS는 TLS로 보호된 웹 서비스로 443번 포트를 사용한다. SMTP는 메일 전송 프로토콜로 25번 포트를 사용한다. 161번 포트는 DNS가 아니라 SNMP에 대응한다.

선지별 해설

① X: 틀린 부분은 "DNS - 161"이다. DNS의 대표 포트 번호는 53이며, 161은 SNMP 포트이다.
② O: FTP의 제어 연결은 서버의 21번 포트를 사용하므로 올바른 짝이다.
③ O: HTTPS는 암호화된 웹 서비스에 사용되며 대표 포트 번호는 443이므로 올바른 짝이다.
④ O: SMTP는 전자우편 전송 프로토콜로 25번 포트를 사용하므로 올바른 짝이다.

오답 포인트

DNS와 SNMP의 포트 번호를 뒤바꾸는 함정이다. 특히 161은 자주 보이는 관리용 포트이므로 숫자만 보고 익숙한 서비스와 성급히 연결하면 오답이 된다.

다시 나오면 이렇게 판단

서비스-포트 대응 문제는 먼저 자주 출제되는 기본 포트부터 확인하면 된다. DNS는 53, FTP 제어는 21, HTTPS는 443, SMTP는 25처럼 표준 포트를 기준으로 선지를 하나씩 대조하면 판단할 수 있다.

암기 포인트

DNS 53, FTP 제어 21, HTTPS 443, SMTP 25, SNMP 161로 정리된다.

NoteBase

문 23. IPSec ESP(Encapsulating Security Payload)의 패킷 포맷에 대한 설명으로 옳지 않은 것은?

① 32비트의 보안 매개변수 색인(security parameter index) 필드에는 같은 보안연관(security association)에 속하는 각 패킷에 대해 서로 다른 보안 매개변수 색인값이 주어진다.

② 32비트의 순서 번호(sequence number) 필드에는 데이터그램의 순서를 나타내는 카운터 값이 저장된다.

③ 8비트의 다음 헤더(next header) 필드는 IP 데이터그램에 의해 전달되는 페이로드의 데이터 유형을 나타낸다.

④ ICV(Integrity Check Value) 필드에는 IP 헤더와 ICV를 제외한 전체 패킷에 대해 계산한 인증 데이터가 저장된다.

정답 1번

출제 포인트

이 문제는 ESP 패킷 포맷에서 SPI, Sequence Number, Next Header, ICV가 각각 무엇을 의미하는지를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

SPI는 수신 측이 들어온 ESP 패킷이 어떤 보안연관(SA)에 속하는지 식별하는 32비트 값이다. Sequence Number는 같은 SA 안에서 패킷마다 1씩 증가하는 카운터 값이다. Next Header는 Payload Data에 들어 있는 다음 상위 데이터의 유형을 나타내는 8비트 필드이다. ICV는 ESP 헤더, 페이로드, ESP 트레일러를 대상으로 계산되는 무결성 검증 값이다.

선지별 해설

① X. SPI는 패킷마다 바뀌는 번호가 아니라 해당 패킷이 속한 SA를 식별하는 값이다. 같은 SA에 속한 패킷은 같은 SPI를 사용한다. 틀린 표현은 "같은 보안연관에 속하는 각 패킷에 대해 서로 다른 보안 매개변수 색인값이 주어진다"이다. 올바르게는 "서로 다른 보안연관을 식별하기 위해 SA마다 SPI가 할당된다"이다.
② O. Sequence Number는 32비트 카운터로, 같은 SA에서 전송되는 패킷마다 1씩 증가한다. 재전송 공격 방지 기능과 연계되는 필드이므로 데이터그램 순서를 나타내는 카운터 값이라는 설명이 맞다.
③ O. Next Header는 8비트 필드로, Payload Data에 어떤 데이터가 들어 있는지를 식별한다. 예를 들어 IPv4, IPv6, TCP 등 다음에 오는 데이터 유형을 나타내므로 설명이 맞다.
④ O. ICV는 ESP의 무결성 검증 값으로, 외부 IP 헤더와 ICV 필드 자체를 제외한 ESP 보호 대상 부분에 대해 계산된다. 따라서 IP 헤더와 ICV를 제외한 전체 ESP 패킷 부분에 대한 인증 데이터라는 설명은 맞다.

오답 포인트

SPI와 Sequence Number를 둘 다 32비트 필드라는 이유만으로 같은 역할로 혼동하기 쉽다. SPI는 SA 식별자이고, Sequence Number는 같은 SA 내부에서 패킷 순서를 세는 증가 카운터라는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

ESP 필드 문제가 나오면 먼저 "이 값이 SA를 구분하는가, 같은 SA 안에서 패킷 순서를 세는가, 페이로드 종류를 가리키는가, 무결성 검증값인가"로 역할을 나누어 판단하면 된다. SA 식별이면 SPI, 순차 카운터이면 Sequence Number, 다음 데이터 유형이면 Next Header, 인증값이면 ICV이다.

암기 포인트

SPI는 SA 이름표, Sequence Number는 패킷 번호표, Next Header는 다음 데이터 표지, ICV는 무결성 검증값이다.

NoteBase

문 24. OAEP(Optimal Asymmetric Encryption Padding)에 대한 설명으로 옳지 않은 것은?

① 동일한 메시지에 대하여 OAEP 패딩 결과는 항상 동일하다.

② OAEP는 RSA 암호의 안전성을 높이기 위한 메시지 패딩 규격이다.

③ OAEP 패딩을 적용한 RSA에서는 수신자가 암호문의 변조 여부를 확인할 수 있다.

④ OAEP 패딩을 적용한 RSA에서는 동일한 메시지와 동일한 공개키를 사용해도 생성된 암호문이 달라질 수 있다.

정답 1번

출제 포인트

이 문제는 OAEP의 핵심 성질인 확률적 패딩, RSA 보안성 보강, 복호 시 패딩 검증 기능을 구분하는지를 묻는 문제이다.

핵심 개념

OAEP는 RSA에 적용하는 확률적 패딩 방식으로, 평문에 난수를 섞어 매번 다른 패딩 결과를 만들고 복호 시 패딩 구조가 맞는지도 함께 검사한다. 교과서식 RSA는 같은 메시지를 같은 공개키로 암호화하면 결과가 고정되지만, OAEP를 적용한 RSA는 난수 시드 때문에 결과가 달라질 수 있다.

선지별 해설

① X. 틀린 부분은 "항상 동일하다"이다. OAEP는 난수 시드를 사용하는 확률적 패딩이므로 동일한 메시지라도 매번 패딩 결과가 달라질 수 있다. 올바르게는 "동일한 메시지에 대해서도 OAEP 패딩 결과는 달라질 수 있다"이다.
② O. OAEP는 RSA의 결정론적 약점을 줄이고 선택암호문 공격에 대한 안전성을 높이기 위해 사용하는 대표적인 메시지 패딩 규격이다.
③ O. OAEP를 적용한 RSA는 복호 과정에서 패딩 구조와 해시 일치 여부를 검사하므로, 정상 형식이 아닌 암호문은 복호 실패로 처리되어 변조나 손상을 감지할 수 있다. 다만 이것은 전자서명처럼 송신자 신원을 증명하는 기능과는 다르다.
④ O. OAEP는 난수를 포함하므로 동일한 메시지와 동일한 공개키를 사용해도 생성되는 암호문이 달라질 수 있다. 이것이 교과서식 RSA와 구별되는 중요한 성질이다.

오답 포인트

①의 "항상 동일하다"와 ④의 "달라질 수 있다"를 뒤집어 읽으면 쉽게 틀린다. OAEP의 본질은 확률적 패딩이라는 점이므로, 같은 입력이라도 결과가 고정되지 않는다는 성질을 먼저 떠올려야 한다.

NoteBase

다시 나오면 이렇게 판단

RSA 패딩 문제에서 같은 메시지의 암호화 결과가 매번 같다고 서술하면 먼저 교과서식 RSA인지, OAEP처럼 난수를 넣는 확률적 패딩인지부터 구분한다. 난수가 들어가면 같은 평문과 같은 공개키라도 결과가 달라질 수 있다고 판단한다.

암기 포인트

OAEP는 난수를 넣는 RSA 패딩이므로 같은 평문도 결과가 고정되지 않는다.

NoteBase

문 25. HTTP 버전 1.1 GET 요청 메시지의 헤더 라인에 대한 설명으로 옳지 않은 것은?

① Accept: 클라이언트가 수용할 수 있는 매체의 형식

② Cookie: 서버에게 반환하는 쿠키 정보

③ Server: 서버의 URL 정보

④ User-Agent: 클라이언트 프로그램(브라우저 등) 정보

정답 3번

출제 포인트

이 문제는 HTTP/1.1 요청 헤더와 응답 헤더의 역할을 구분할 수 있는지를 묻는다.

핵심 개념

Accept는 클라이언트가 받아들일 수 있는 미디어 타입을 알리는 요청 헤더이다. Cookie는 브라우저가 저장한 쿠키 값을 서버에 다시 보내는 요청 헤더이다. User-Agent는 클라이언트 프로그램의 종류와 버전 정보를 나타내는 요청 헤더이다. Host는 요청 대상 서버의 도메인명과 포트 정보를 담는 요청 헤더이고, Server는 응답을 보낸 서버 소프트웨어 정보를 나타내는 응답 헤더이다.

선지별 해설

① O: Accept 헤더는 클라이언트가 수용 가능한 표현 형식(MIME 타입)을 서버에 알리는 요청 헤더이므로 옳다.
② O: Cookie 헤더는 서버가 Set-Cookie로 내려준 값을 클라이언트가 이후 요청에서 다시 보내는 정보이므로 옳다.
③ X: 틀린 부분은 "Server: 서버의 URL 정보"이다. Server 헤더는 URL을 담는 요청 헤더가 아니라 서버 소프트웨어 정보를 나타내는 응답 헤더이다. 요청 대상 서버의 주소 정보는 Host 헤더에 들어간다.
④ O: User-Agent 헤더는 브라우저 등 클라이언트 프로그램의 종류와 버전 정보를 나타내므로 옳다.

오답 포인트

③은 서버와 관련된 이름만 보고 맞다고 판단하기 쉽다. 그러나 요청에서 서버 주소를 지정하는 헤더는 Host이고, Server는 응답에서 서버 프로그램 정보를 알릴 때 사용된다는 점이 함정이다.

다시 나오면 이렇게 판단

헤더 이름을 보면 먼저 요청 헤더인지 응답 헤더인지부터 구분한다. 그다음 수용 형식은 Accept, 쿠키 반환은 Cookie, 클라이언트 식별은 User-Agent, 서버 주소 지정은 Host로 연결하면 판단이 안정된다.

암기 포인트

요청의 서버 주소는 Host이고, 응답의 서버 정보는 Server이다.

NoteBase