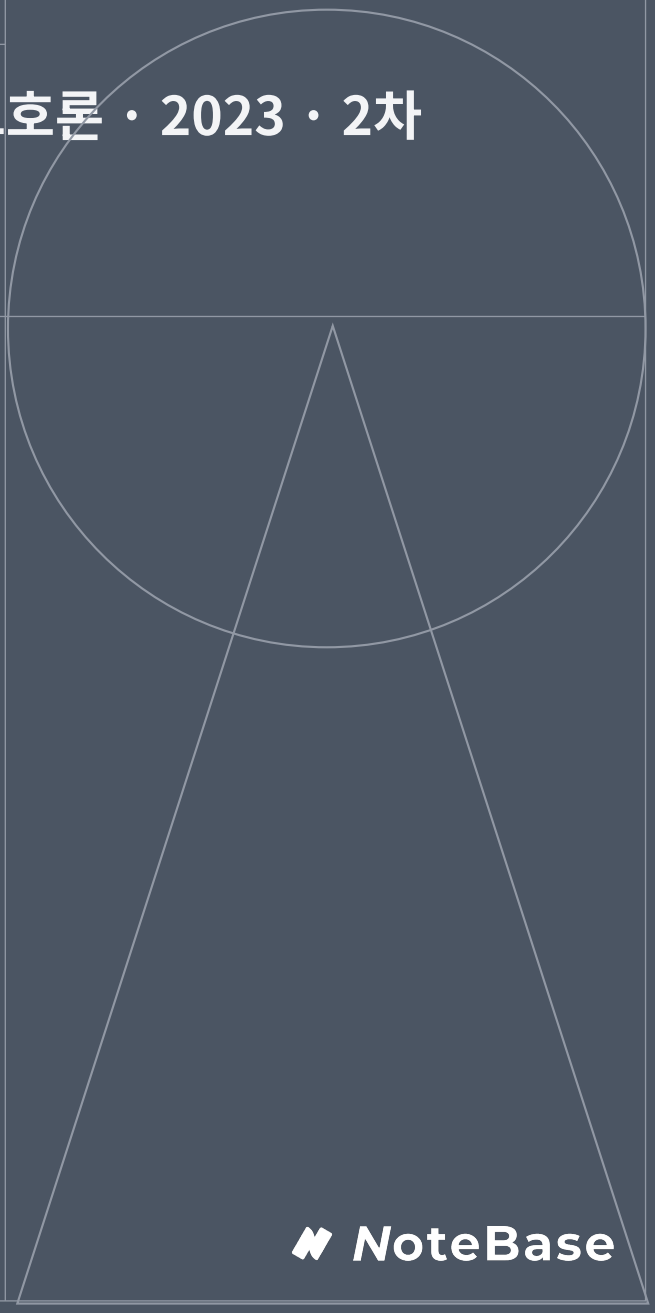
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2023 · 2차



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2023 · 2차

공무원/국가직/7급 · 정보보호론 · 2023 · 2차

문 1. 검증을 마친 시스템 사용자가 시스템 자원에 접근할 수 있도록 허락하는 과정은?

① Authentication

② Authorization

③ Audit

④ Accounting

정답 2번

출제 포인트

이 문제는 인증, 인가, 감사, 과금의 역할 차이를 구분하는 문제이다.

핵심 개념

Authentication은 사용자가 누구인지를 확인하는 인증 절차이다. 키워드는 신원 확인이다.
Authorization은 인증된 사용자에게 어떤 자원과 기능을 허용할지를 결정하는 인가 절차이다. 키워드는 권한 부여이다.
Audit는 사용자의 접근과 행위를 기록하고 추적하는 감사 절차이다. 키워드는 기록과 추적이다.
Accounting은 자원 사용량을 집계해 과금하거나 관리하는 절차이다. 키워드는 사용량 집계이다.

선지별 해설

① X: Authentication은 사용자의 신원을 확인하는 과정이므로 자원 접근을 허락하는 단계가 아니다. 틀린 표현은 접근 허락이다. 올바르게는 사용자 본인 여부를 검증하는 과정이다.
② O: Authorization은 인증이 끝난 사용자에게 시스템 자원 접근 권한을 부여하는 과정이므로 문제의 설명과 일치한다.
③ X: Audit는 누가 언제 무엇에 접근했는지를 기록하고 점검하는 기능이다. 틀린 표현은 허락하는 과정이다. 올바르게는 접근 행위를 기록하고 추적하는 과정이다.
④ X: Accounting은 자원 사용량을 측정해 과금하거나 관리하는 기능이다. 틀린 표현은 접근 허가이다. 올바르게는 사용량을 집계하는 과정이다.

NoteBase

오답 포인트

Authentication과 Authorization은 모두 접근통제 문맥에서 함께 나오므로 혼동하기 쉽다. 이 문항은 검증을 마친 사용자라는 표현으로 인증은 이미 끝났음을 먼저 제시하고, 그 다음 단계인 권한 부여를 묻게 만든 점이 함정이다.

다시 나오면 이렇게 판단

문장에서 누구인지 확인하는지, 무엇을 할 수 있게 허용하는지, 행위를 기록하는지, 사용량을 집계하는지를 먼저 구분하면 된다. 신원 확인이면 Authentication, 권한 부여이면 Authorization, 기록 추적이면 Audit, 사용량 집계이면 Accounting이다.

암기 포인트

인증은 신원 확인, 인가는 권한 부여, 감사는 기록 추적, 과금은 사용량 집계이다.

NoteBase

문 2. 도출된 위험에 대하여 보안 대책 마련을 위한 추가적인 비용의 투입이나 외부와의 연계·협력을 고려하지 않고, 잠재적 위험을 자체적으로 감수하거나 일부 시스템 기능의 사용 포기에 따른 불편함을 감수하는 방식의 위험 대처에 해당하는 것만을 모두 고르면?

ㄱ. 위험 수용
ㄴ. 위험 회피
ㄷ. 위험 감소
ㄹ. 위험 전가

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 1번

출제 포인트

이 문제는 위험 수용, 위험 회피, 위험 감소, 위험 전가의 차이를 비용 투입 여부와 외부 이전 여부로 구별할 수 있는지를 묻는다.

핵심 개념

위험 수용: 추가 통제를 더하지 않고 잔여 위험을 조직이 스스로 감수하는 방식이다. 키워드: 자체 감수.
위험 회피: 위험이 발생할 수 있는 기능이나 행위를 중단하거나 포기하여 위험 원인 자체를 피하는 방식이다. 키워드: 기능 포기.
위험 감소: 보호대책을 추가해 위험의 가능성이나 영향을 낮추는 방식이다. 키워드: 추가 비용, 통제 강화.
위험 전가: 보험, 위탁, 계약 등으로 위험 부담을 외부에 이전하는 방식이다. 키워드: 외부 연계, 협력.

선지별 해설

1번: O. ㄱ 위험 수용은 잠재적 위험을 자체적으로 감수하는 경우에 해당하고, ㄴ 위험 회피는 일부 시스템 기능의 사용을 포기해 위험을 피하는 경우에 해당한다. 문제 조건과 일치하므로 맞는 조합이다.
2번: X. ㄱ은 맞지만 ㄹ 위험 전가는 틀리다. 위험 전가는 보험 가입이나 외부 위탁처럼 외부와의 연계·협력으로 위험 부담을 넘기는 방식이다. 틀린 표현은 'ㄹ 포함'이다. 올바르게는 'ㄱ, ㄴ'이다.
3번: X. ㄴ은 맞지만 ㄷ 위험 감소는 틀리다. 위험 감소는 보안 대책을 추가해 위험 수준을 낮추는 방식이므로 문제의 '추가적인 비용의 투입을 고려하지 않고'와 어긋난다. 틀린 표현은 'ㄷ 포함'이다. 올바르게는 'ㄱ, ㄴ'이다.
4번: X. ㄷ과 ㄹ은 모두 문제 조건에 맞지 않는다. ㄷ은 추가 통제를 통한 감소이고, ㄹ은 외부 이전이므로 제시된 방식과 다르다. 틀린 표현은 'ㄷ, ㄹ'이다. 올바르게는 'ㄱ, ㄴ'이다.

NoteBase

오답 포인트

위험 수용과 위험 회피는 둘 다 적극적 보안 투자 없이 내부에서 처리한다는 점 때문에 함께 잡아야 한다. 반대로 위험 감소는 통제 강화, 위험 전가는 외부 이전이라는 키워드를 놓치면 ㄷ이나 ㄹ을 잘못 포함하게 된다.

다시 나오면 이렇게 판단

위험 대응 문제는 먼저 추가 통제가 들어가는지, 다음으로 외부에 넘기는지, 마지막으로 기능을 포기하는지를 본다. 추가 통제가 없고 스스로 감수하면 위험 수용, 기능을 중단하면 위험 회피, 통제를 강화하면 위험 감소, 외부에 넘기면 위험 전가로 판단된다.

암기 포인트

수용은 그대로 안고 가는 것이고, 회피는 아예 하지 않는 것이며, 감소는 줄이는 것이고, 전가는 남에게 넘기는 것이다.

NoteBase

문 3. 해시 충돌을 바르게 나타낸 것은? (단, 해시 함수 $h_1 \neq h_2$, 해시 입력값 $k_1 \neq k_2$)

① $h_1(k_1) = h_2(k_1)$

② $h_1(k_1) = h_1(k_2)$

③ $h_1(k_1) \neq h_1(k_2)$

④ $h_1(k_1) \neq h_2(k_2)$

정답 2번

출제 포인트

이 문제는 해시 충돌의 성립 조건인 같은 해시 함수, 서로 다른 입력, 같은 출력의 조합을 묻는 문제이다.

핵심 개념

해시 충돌은 같은 해시 함수 h에 대해 서로 다른 입력 $k_1 \neq k_2$가 같은 해시값을 내는 $h(k_1) = h(k_2)$ 상황이다. 서로 다른 함수 h_1, h_2의 출력이 우연히 같아지는 것은 일반적인 충돌 정의가 아니다.

선지별 해설

① X: $h_1(k_1) = h_2(k_1)$는 같은 입력에 서로 다른 해시 함수를 적용한 경우이다. 충돌은 함수가 하나로 고정되어 있어야 하므로 틀린 표현은 서로 다른 함수 h_1, h_2를 비교한 부분이다. 올바르게는 같은 함수에서 $k_1 \neq k_2$이면서 출력이 같아야 한다.
② O: $h_1(k_1) = h_1(k_2)$는 같은 해시 함수 h_1에 서로 다른 입력 k_1, k_2를 넣었는데 결과가 같다는 뜻이므로 해시 충돌의 정의에 정확히 맞는다.
③ X: $h_1(k_1) \neq h_1(k_2)$는 같은 함수에 서로 다른 입력을 넣었을 때 출력도 다르다는 뜻이므로 충돌이 아니다. 틀린 표현은 부등호 $\neq$이고, 충돌로 바꾸려면 등호 $=$가 되어야 한다.
④ X: $h_1(k_1) \neq h_2(k_2)$는 함수도 다르고 출력도 다르므로 충돌 여부를 나타내는 식이 아니다. 틀린 표현은 서로 다른 함수와 서로 다른 출력의 비교 자체이고, 올바르게는 같은 함수 내부에서 출력 일치를 봐야 한다.

오답 포인트

①과 ④처럼 출력값의 같고 다름만 보고 충돌이라고 착각하기 쉽다. 이 문항의 함정은 출력의 일치 여부보다 먼저 같은 해시 함수인지 확인해야 한다는 점이다.

다시 나오면 이렇게 판단

충돌 식은 순서대로 같은 함수인지, 입력이 서로 다른지, 출력이 같은지를 확인하면 된다. 즉 같은 함수 1개, 다른 입력 2개, 같은 출력 1개가 동시에 성립하면 충돌이다.

NoteBase

암기 포인트

해시 충돌은 같은 함수, 다른 입력, 같은 출력이다.

NoteBase

문 4. 메시지 인증 코드(MAC)에 대한 설명으로 옳지 않은 것은?

① MAC을 사용하기 위해서는 송·수신자만의 공유 비밀키가 필요하다.

② MAC의 길이는 메시지의 길이와 같다.

③ 메시지와 함께 전달되어 메시지 무결성 검증에 이용된다.

④ 수신자는 검증을 통해 메시지가 송신자로부터 전송된 것을 확인할 수 있다.

정답 2번

출제 포인트

이 문제는 MAC의 기능과 출력 길이의 성격을 정확히 구분하는지를 묻는 문제이다.

핵심 개념

MAC는 송신자와 수신자가 공유한 비밀키로 메시지에 대해 생성하는 인증값이다.
핵심은 메시지 무결성과 메시지 인증을 제공한다는 점이며, 출력 길이는 알고리즘이 정한 고정 길이이다.
즉 메시지 길이는 가변이지만 MAC 값의 길이는 보통 일정하다.

선지별 해설

① O: MAC는 비밀키를 아는 당사자만 생성·검증할 수 있으므로 송신자와 수신자 사이의 공유 비밀키가 필요하다.
② X: 틀린 부분은 'MAC의 길이는 메시지의 길이와 같다'는 표현이다.
올바르게는 MAC의 길이는 메시지 길이와 무관하고 알고리즘이 정한 고정 길이이다.
③ O: MAC 값은 메시지와 함께 전달되어 전송 중 메시지가 변조되지 않았는지 확인하는 무결성 검증에 이용된다.
④ O: 수신자는 MAC 검증을 통해 비밀키를 아는 송신자가 만든 메시지인지 확인할 수 있으므로 메시지 인증 기능을 가진다.

오답 포인트

②는 해시값이 메시지 전체를 대표한다는 인상 때문에 길이도 메시지 길이를 따라간다고 착각하게 만든 선지이다. MAC는 메시지 전체를 입력으로 사용하지만 결과는 요약된 고정 길이 인증값이라는 점이 함정이다.

다시 나오면 이렇게 판단

MAC 문제는 먼저 '무결성·인증 제공', '공유 비밀키 사용', '출력 길이는 고정'의 세 가지 축으로 판단하면 된다.
선지에 메시지 길이와 MAC 길이를 동일시하는 표현이 나오면 바로 오답으로 판단할 수 있다.

암기 포인트

MAC는 공유키 기반 무결성·인증 값이고, 메시지는 길어져도 MAC 길이는 보통 고정이다.

NoteBase

문 5. 리눅스 파일의 접근 권한을 설정하기 위하여 다음과 같은 명령을 실행한 경우, 해당 파일에 부여된 권한을 바르게 나타낸 것은?

chmod 2755 file1

① -rwxr-xr-x

② -rwsr-xr-x

③ -rwxr-sr-x

④ -rwsr-sr-x

정답 3번

출제 포인트

이 문제는 8진수 권한 표기에서 특수 권한 비트인 setgid와 일반 권한 755를 문자열 권한으로 바꾸는 규칙을 묻는 문제이다.

핵심 개념

755는 소유자 7=rwx, 그룹 5=r-x, 기타 5=r-x를 뜻한다.
앞자리 2는 setgid를 뜻하며 그룹 실행 비트 자리에 반영된다.
그룹 실행 비트가 켜져 있으면 s로, 꺼져 있으면 S로 표시된다.

선지별 해설

① X: `-rwxr-xr-x`는 755만 반영한 표기이고 앞자리 2의 setgid가 빠져 있다.
틀린 표현은 그룹 권한 부분 `r-x`이다. 올바르게는 setgid가 반영된 `r-s`가 되어 `-rwxr-sr-x`가 된다.

② X: `-rwsr-xr-x`는 소유자 실행 비트 자리에 setuid가 반영된 형태이다.
틀린 표현은 소유자 권한 부분 `rws`이다. 올바르게는 setuid가 아니라 setgid이므로 소유자 쪽은 `rwx` 그대로이고 그룹 쪽이 `r-s`가 되어 `-rwxr-sr-x`가 된다.

③ O: `2755`는 setgid(2) + 755이므로 기본 권한 `rwxr-xr-x`에서 그룹 실행 비트 자리가 `x` 대신 `s`로 바뀐다. 따라서 `-rwxr-sr-x`가 맞다.

④ X: `-rwsr-sr-x`는 setuid와 setgid가 모두 설정된 6755에 해당한다.
틀린 표현은 소유자 권한 부분 `rws`이다. 올바르게는 setuid 없이 소유자 쪽은 `rwx`이고 전체 표기는 `-rwxr-sr-x`가 된다.

NoteBase

오답 포인트

앞자리 2를 setuid로 착각하면 ②나 ④로 흔들린다. 또 특수 권한은 실행 비트 자리에 겹쳐 표시되므로, setgid가 붙더라도 그룹 실행 비트가 살아 있으면 `s`, 실행 비트가 없으면 `S`가 된다는 점을 놓치기 쉽다.

다시 나오면 이렇게 판단

네 자리 chmod는 첫 자리에서 특수 권한을, 뒤 세 자리에서 기본 권한을 먼저 분리해 읽는다. 그다음 setuid는 소유자 실행 자리, setgid는 그룹 실행 자리, sticky bit는 기타 실행 자리에 덮어쓴다고 보면 빠르게 판단할 수 있다.

암기 포인트

4=setuid, 2=setgid, 1=sticky bit이며, 실행 비트가 있으면 s 또는 t, 없으면 S 또는 T로 표시된다.

NoteBase

문 6. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 관리기관의 장이 국가정보원장에게 우선적으로 기술적 지원을 요청하여야 하는 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설이 아닌 것은?

① 도로·철도·지하철·공항·항만 등 주요 교통시설

② 전력, 가스, 석유 등 에너지·수자원 시설

③ 금융 정보통신기반시설 등 개인정보가 저장된 정보통신기반시설

④ 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

정답 3번

쟁점

이 문제는 「정보통신기반 보호법」 제7조에서 국가정보원장에게 우선적으로 기술적 지원을 요청하여야 하는 시설과, 오히려 국가정보원장이 기술적 지원을 수행할 수 없는 시설을 구별하는 문제이다. 핵심은 우선 요청 대상의 열거와 개인정보 저장 시설에 대한 지원 금지를 구별하는 것이다.

용어 풀이

우선적 지원 요청 대상은 기술적 지원이 필요할 때 다른 기관보다 먼저 국가정보원장에게 지원을 요청하여야 하는 법정 대상 시설이다.
지원 금지 대상은 국가정보원장이 기술적 지원을 수행하여서는 아니 되는 시설이다.

핵심 구분

법 제7조제2항은 국가안전보장에 중대한 영향을 미치는 시설로서 주요 교통시설, 에너지·수자원 시설, 방송중계·국가지도통신망 시설, 원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설을 우선 요청 대상으로 열거한다. 반면 법 제7조제3항은 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대해서는 국가정보원장이 기술적 지원을 수행하여서는 아니 된다고 정한다. 즉 주요정보통신기반시설이라고 해서 모두 국가정보원 우선 요청 대상이 되는 것은 아니다.

NoteBase

선지별 해설

① O
도로·철도·지하철·공항·항만 등 주요 교통시설은 법 제7조제2항제1호의 우선 요청 대상이다. 선지의 열거가 조문과 일치하므로 옳은 설명이다.

② O
전력, 가스, 석유 등 에너지·수자원 시설은 법 제7조제2항제2호의 우선 요청 대상이다. 에너지 기반과 수자원 기반은 국가안전보장에 중대한 영향을 미치는 시설로 보아 우선 요청 대상으로 묶인다.

③ X
금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대해서는 법 제7조제3항에 따라 국가정보원장이 기술적 지원을 수행하여서는 아니 된다. 따라서 이를 국가정보원장에게 우선적으로 지원 요청하여야 하는 시설로 보는 것은 틀리다. 틀린 표현은 '우선적으로 기술적 지원을 요청하여야 하는 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설'이다. 올바른 표현은 '국가정보원장이 기술적 지원을 수행하여서는 아니 되는 제외 대상 정보통신기반시설'이다.

④ O
원자력·국방과학·첨단방위산업 관련 정부출연연구기관의 연구시설은 법 제7조제2항제4호의 우선 요청 대상이다. 국가안전보장과 직접 연결되는 연구시설이므로 우선 요청 대상으로 본다.

오답 포인트

이 문제를 틀렸다면 '주요정보통신기반시설'이라는 큰 개념과 '국가정보원장 우선 요청 대상'이라는 좁은 개념을 혼동했을 가능성이 높다. 특히 ③은 금융·개인정보 저장 시설도 중요해 보인다는 점을 이용해 우선 요청 대상으로 착각하게 만드는 함정이지만, 조문은 오히려 국가정보원장의 기술적 지원 금지 대상으로 둔다.

다시 나오면 이렇게 판단

이 유형은 먼저 조문이 우선 요청 대상을 열거하는지, 금지 대상을 따로 두는지를 나누어 본다. 교통, 에너지·수자원, 방송중계·국가지도통신망, 원자력·국방과학·첨단방위산업 연구시설은 우선 요청 대상으로 보고, 금융·개인정보 저장 시설은 지원 금지 대상으로 반대로 판단한다.

암기 포인트

국정원 우선 요청은 교에방원이고, 금융·개인정보 저장 시설은 지원 금지 대상이다.

NoteBase

문 7. AES 알고리즘의 복호화 과정에서 한 암호 블록에 대해 실행되는 처음 4개의 오퍼레이션을 첫 번째부터 네 번째까지 순서대로 바르게 나열한 것은? (단, ARK: Add Round Key, IMC: Inverse Mix Columns, ISR: Inverse Shift Rows, ISB: Inverse Substitute Bytes)

① ARK - IMC - ISR - ISB

② ARK - ISB - ISR - IMC

③ ARK - ISR - ISB - ARK

④ IMC - ISR - ISB - ARK

정답 3번

출제 포인트

이 문제는 AES 복호화에서 초기 Add Round Key 뒤에 이어지는 역라운드의 표준 수행 순서를 묻는 문제이다.

올바른 순서

1. ARK — 암호문 블록에 마지막 라운드 키를 먼저 XOR한다.
2. ISR — 행 이동을 역방향으로 되돌려 바이트 위치를 원상복구한다.
3. ISB — 각 바이트에 역 S-Box를 적용해 치환을 되돌린다.
4. ARK — 다음 단계로 넘어가기 전에 해당 라운드 키를 다시 XOR한다.

왜 이 순서인가: AES 복호화는 먼저 키 결합을 풀고, 그다음 바이트 위치 복원과 역치환을 거친 뒤 라운드 키를 적용해야 이후 IMC가 올바른 상태값에 작동할 수 있다.

선지별 해설

① X: 틀린 부분은 "ARK - IMC - ISR - ISB"이다. 초기 ARK 다음에는 곧바로 IMC가 오지 않는다. 올바르게는 "ARK - ISR - ISB - ARK" 순서이다.

② X: 틀린 부분은 네 번째 단계가 IMC인 점이다. 표준 복호화의 처음 네 연산 안에는 두 번째 ARK가 들어가고 IMC는 그 다음 단계에 온다. 올바르게는 "ARK - ISR - ISB - ARK"이다.

③ O: 초기 Add Round Key 후에 Inverse Shift Rows, Inverse Substitute Bytes, Add Round Key가 이어지므로 처음 네 연산의 배열이 정확하다.

④ X: 틀린 부분은 첫 단계가 IMC인 점이다. AES 복호화는 IMC로 시작하지 않고 마지막 라운드 키를 적용하는 ARK로 시작한다. 올바르게는 "ARK - ISR - ISB - ARK"이다.

오답 포인트

복호화에서 IMC가 사용된다는 사실만 기억하고 IMC를 너무 앞에 배치하면 오답이 된다. 또 ISR과 ISB, ARK와 IMC의 상대적 위치를 묶어서 외우지 않으면 ①, ②처럼 중간 순서를 잘못 고르기 쉽다.

NoteBase

다시 나오면 이렇게 판단

AES 복호화 순서 문제는 "처음은 ARK, 역라운드의 핵심은 ISR -> ISB -> ARK -> IMC"의 골격으로 판단하면 된다. 보기에서 처음 네 연산을 묻는다면 IMC가 나오기 전까지를 먼저 끊어서 확인하면 된다.

암기 포인트

AES 복호화 초반은 "ARK 후 ISR-ISB-ARK"이고 IMC는 그 다음이다.

NoteBase

문 8. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3의 일부이다. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

(가)는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 (나)로 지정하고 과학기술정보통신부장관에게 신고하여야 한다.

① (가): 정보통신서비스 제공자, (나): 정보보호 최고책임자
② (가): 정보통신서비스 제공자, (나): 개인정보 보호책임자
③ (가): 개인정보처리자, (나): 정보보호 최고책임자
④ (가): 개인정보처리자, (나): 개인정보 보호책임자

정답 1번

쟁점

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3 제1항상 정보보호 최고책임자 지정·신고의 주체와 지정 대상을 구별하는 문제이다. 핵심은 정보통신서비스 제공자가 일정 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하여 과학기술정보통신부장관에게 신고한다는 점과, 개인정보 보호책임자 제도와 구별하는 점이다.

용어 풀이

정보통신서비스 제공자 = 정보통신망을 이용하여 정보를 제공하거나 그 제공을 매개하는 자이다.
정보보호 최고책임자 = 정보통신시스템 보안과 정보의 안전한 관리를 총괄하는 책임자이다.
개인정보 보호책임자 = 「개인정보 보호법」상 개인정보 처리에 관한 업무를 총괄하는 책임자이다.

핵심 구분

원칙적으로 이 조문은 정보통신서비스 제공자가 임직원을 정보보호 최고책임자로 지정하여 신고하는 제도이다. 개인정보처리자가 개인정보 보호책임자를 두는 제도와는 주체와 책임자 명칭이 다르다. 즉 정보통신망법 제45조의3 제1항의 연결은 '정보통신서비스 제공자-정보보호 최고책임자'이다.

NoteBase

선지별 해설

① O: 조문에 '정보통신서비스 제공자'가 일정 기준에 해당하는 임직원을 '정보보호 최고책임자'로 지정하고 신고한다고 되어 있으므로 정확하다.

② X: (가)는 맞지만 (나)가 틀리다. 이 조문은 개인정보 보호책임자가 아니라 정보보호 최고책임자를 지정·신고하는 규정이다.
틀린 표현: '개인정보 보호책임자'
올바른 표현: '정보보호 최고책임자'

③ X: (나)는 맞지만 (가)가 틀리다. 이 조문상 지정·신고 의무의 주체는 개인정보처리자가 아니라 정보통신서비스 제공자이다.
틀린 표현: '개인정보처리자'
올바른 표현: '정보통신서비스 제공자'

④ X: (가)와 (나)가 모두 틀리다. 개인정보처리자-개인정보 보호책임자는 「개인정보 보호법」의 연결이고, 제시된 조문은 정보통신망법상 정보통신서비스 제공자-정보보호 최고책임자에 관한 규정이다.
틀린 표현: '개인정보처리자', '개인정보 보호책임자'
올바른 표현: '정보통신서비스 제공자', '정보보호 최고책임자'

오답 포인트

이 문제를 틀렸다면 정보통신망법의 정보보호 최고책임자 제도와 개인정보 보호법의 개인정보 보호책임자 제도를 섞어서 기억했을 가능성이 높다. 출제자는 주체인 '정보통신서비스 제공자'와 책임자 명칭인 '정보보호 최고책임자'를 각각 바꾸어 혼동을 유도하였다.

다시 나오면 이렇게 판단

조문형 연결 문제는 먼저 주체와 책임자 명칭을 짝으로 확인하면 된다. 정보통신망법에서 보안 총괄 책임자를 묻는다면 '정보통신서비스 제공자-정보보호 최고책임자'를 먼저 떠올리면 정답을 빠르게 고를 수 있다.

암기 포인트

정보통신망법은 정보통신서비스 제공자와 정보보호 최고책임자를 연결하고, 개인정보 보호법은 개인정보처리자와 개인정보 보호책임자를 연결한다.

NoteBase

문 9. 리눅스에서 사용자 계정의 패스워드를 변경한 후 그 패스워드를 그대로 사용해야 할 최소 기간과 사용할 수 있는 최대 기간을 지정하기 위한 명령어와 그 명령의 실행 결과가 저장되는 파일을 바르게 연결한 것은?

① usermod /etc/passwd

② chage /etc/passwd

③ usermod /etc/shadow

④ chage /etc/shadow

정답 4번

출제 포인트

리눅스에서 패스워드 최소 사용 기간과 최대 사용 기간을 설정하는 명령과 그 정보가 저장되는 파일을 구분하는 문제이다.

핵심 개념

chage는 패스워드 에이징 정보를 설정하는 명령이다. usermod는 사용자 계정의 일반 속성을 수정하는 명령이다. /etc/passwd는 로그인명, UID, 홈 디렉터리, 셸 같은 계정 기본 정보가 저장되는 파일이고, /etc/shadow는 해시된 패스워드와 최소 사용 기간, 최대 사용 기간 같은 패스워드 에이징 정보가 저장되는 파일이다.

선지별 해설

① X: usermod는 사용자 계정 속성을 수정하는 명령이지만 패스워드 최소 사용 기간과 최대 사용 기간을 지정하는 대표 명령이 아니다. 틀린 부분은 "usermod"이다. 올바르게는 chage가 최소 기간과 최대 기간을 설정한다.
② X: chage로 패스워드 사용 기간을 설정하는 점은 맞지만 저장 파일이 틀리다. 틀린 부분은 "/etc/passwd"이다. 올바르게는 패스워드 에이징 정보가 /etc/shadow에 저장된다.
③ X: /etc/shadow는 맞지만 명령이 틀리다. 틀린 부분은 "usermod"이다. 올바르게는 chage가 최소 기간과 최대 기간을 설정한다.
④ O: chage는 패스워드 최소 사용 기간과 최대 사용 기간을 설정하는 명령이고, 그 결과인 패스워드 에이징 정보는 /etc/shadow에 저장된다.

오답 포인트

usermod도 계정 관련 명령이라 비슷해 보이지만, 이 문항은 계정 속성 일반이 아니라 패스워드 사용 기간을 묻는다. 또 /etc/passwd와 /etc/shadow를 혼동하기 쉬운데, 패스워드와 에이징 정보는 /etc/shadow에 저장된다는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

문항에 최소 사용 기간, 최대 사용 기간, 만료, 경고일 같은 패스워드 에이징 키워드가 나오면 먼저 chage와 /etc/shadow를 떠올리면 된다. 반대로 계정명, 홈 디렉터리, 기본 그룹, 로그인 셸 같은 일반 계정 속성이 나오면 usermod 계열을 검토하면 된다.

암기 포인트

패스워드 나이 정보는 chage와 /etc/shadow의 조합으로 연결된다.

NoteBase

문 10. 서비스 거부(DoS) 공격에 대한 대응 방법으로 옳지 않은 것은?

① Smurf 공격에 대응하기 위해 브로드캐스트 IP 주소로 전송되는 ICMP 패킷을 차단한다.

② Land 공격에 대응하기 위해 출발지와 목적지의 IP 주소가 동일한 패킷을 차단한다.

③ TCP SYN Flooding 공격에 대응하기 위해 서버의 TCP 연결 테이블의 크기를 감소시킨다.

④ Slowloris 공격에 대응하기 위해 특정 클라이언트로부터 전송된 일정 시간 동안의 불완전한 HTTP 요청 개수와 연결 유지 시간을 제한한다.

정답 3번

출제 포인트

이 문제는 대표적인 DoS 공격 유형별 대응 방법이 서로 어떻게 대응되는지를 구분하는 문제이다.

핵심 개념

Smurf 공격은 출발지 IP를 피해자로 위조한 뒤 브로드캐스트 주소로 ICMP Echo를 보내 다수의 응답을 피해자에게 집중시키는 반사형 DoS이다.
Land 공격은 출발지와 목적지 주소가 동일한 비정상 패킷으로 시스템 혼란을 유발하는 공격이다.
TCP SYN Flooding은 SYN만 대량 전송해 반개방 연결을 쌓아 TCP 연결 대기 큐를 고갈시키는 공격이다.
Slowloris는 HTTP 요청을 매우 느리게 끊어 보내며 연결을 오래 붙잡아 웹 서버의 동시 연결 자원을 소모시키는 공격이다.

NoteBase

선지별 해설

① O
브로드캐스트 IP로 향하는 ICMP 요청을 차단하면 Smurf 공격의 반사 증폭 경로를 줄일 수 있으므로 옳다.

② O
Land 공격은 출발지와 목적지 정보가 동일한 비정상 패킷을 이용하므로 이런 패킷을 필터링하는 대응은 타당하므로 옳다.

③ X
틀린 부분은 "서버의 TCP 연결 테이블의 크기를 감소시킨다"는 표현이다.
실제로는 TCP SYN Flooding에 대비해 연결 대기 큐를 충분히 확보하고, SYN cookie 사용이나 반개방 연결 유지 시간 축소 같은 방식으로 자원 고갈을 완화한다.
연결 테이블 크기를 감소시키면 적은 수의 SYN만으로도 자원이 더 빨리 고갈되므로 대응이 아니라 취약성 확대에 가깝다.

④ O
Slowloris는 불완전한 HTTP 요청을 오래 유지해 연결을 점유하는 공격이므로, 클라이언트별 불완전 요청 수와 연결 유지 시간을 제한하는 대응은 옳다.

오답 포인트

③은 "연결 테이블 관리"라는 말만 보고 자원을 줄여 통제한다고 오해하기 쉽다. 그러나 SYN Flooding 대응의 핵심은 반개방 연결을 덜 쌓이게 하거나 더 버티게 만드는 것이지, 수용 가능한 연결 수 자체를 줄이는 것이 아니다.

다시 나오면 이렇게 판단

공격 이름을 보면 먼저 고갈되는 자원이 무엇인지 연결한다. Smurf는 ICMP 반사, Land는 동일 출발지·목적지의 비정상 패킷, SYN Flooding은 반개방 TCP 큐, Slowloris는 장시간 유지되는 불완전 HTTP 연결로 판단하면 선지의 대응 방향을 빠르게 가를 수 있다.

암기 포인트

Smurf는 ICMP 브로드캐스트 차단, Land는 동일 출발지·목적지 차단, SYN Flooding은 반개방 연결 보호, Slowloris는 느린 HTTP 연결 제한으로 정리된다.

NoteBase

문 11. 다음 설명에 해당하는 RAID 레벨은?

◯ 패리티를 생성하기 위해 XOR 연산자를 이용한 오류 정정 코드를 사용한다.
◯ 패리티 블록들은 전체 디스크 배열에 분산되어 저장된다.

① RAID 레벨 1
② RAID 레벨 3
③ RAID 레벨 4
④ RAID 레벨 5

정답 4번

출제 포인트

이 문제는 RAID 1, 3, 4, 5의 패리티 저장 방식과 스트라이핑 단위를 구별하는 문제이다.

핵심 개념

RAID 1은 동일 데이터를 그대로 복제하는 미러링 방식이다.
RAID 3은 바이트 단위 스트라이핑과 전용 패리티 디스크를 사용하는 방식이다.
RAID 4는 블록 단위 스트라이핑과 전용 패리티 디스크를 사용하는 방식이다.
RAID 5는 블록 단위 스트라이핑을 하면서 패리티 블록을 여러 디스크에 분산 저장하는 방식이다.

NoteBase

선지별 해설

① X
RAID 1은 미러링 방식이므로 패리티를 생성하지 않는다.
틀린 부분은 RAID 1이라는 표현이다.
올바르게는 동일 데이터를 두 개 이상 디스크에 복제 저장하는 RAID 1이 아니라, 패리티를 사용하는 RAID 계열을 떠올려야 한다.

② X
RAID 3은 XOR 기반 패리티를 사용할 수 있지만 패리티를 전용 디스크 하나에 둔다.
틀린 부분은 RAID 3이라는 표현이다.
올바르게는 패리티 블록이 전체 디스크 배열에 분산 저장되는 방식은 RAID 3이 아니라 RAID 5이다.

③ X
RAID 4도 블록 단위 스트라이핑과 패리티를 사용하지만 패리티 디스크가 전용으로 따로 존재한다.
틀린 부분은 RAID 4라는 표현이다.
올바르게는 전용 패리티 디스크가 아니라 패리티 블록을 각 디스크에 분산 저장하는 방식이 RAID 5이다.

④ O
RAID 5는 패리티 계산에 XOR를 사용하고, 패리티 블록을 모든 디스크에 분산 배치한다.
문제의 두 설명을 동시에 만족하는 RAID 레벨은 RAID 5이다.

오답 포인트

RAID 3, RAID 4, RAID 5가 모두 패리티를 사용한다는 점 때문에 헷갈리기 쉽다. 이 문항의 핵심 함정은 패리티 사용 여부가 아니라 패리티를 전용 디스크에 두는지, 여러 디스크에 분산하는지의 차이이다.

다시 나오면 이렇게 판단

문장에서 먼저 미러링인지 패리티 방식인지를 구분한 뒤, 패리티가 전용 디스크에 있으면 RAID 3 또는 RAID 4, 패리티가 분산 저장되면 RAID 5로 판단한다. 여기에 스트라이핑 단위가 바이트인지 블록인지까지 붙이면 RAID 3과 RAID 4도 구분된다.

암기 포인트

RAID 1은 미러링, RAID 3과 4는 전용 패리티, RAID 5는 분산 패리티이다.

NoteBase

문 12. 객체 소유자가 자율적 판단에 따라 객체에 대한 접근 권한을 제어하는 것은?

① 임의적 접근 제어(DAC)

② 강제적 접근 제어(MAC)

③ 역할 기반 접근 제어(RBAC)

④ 래티스 기반 접근 제어(Lattice Based Access Control)

정답 1번

출제 포인트

이 문제는 접근통제 모델을 객체 권한의 결정 주체로 구별하는 문제이다.

핵심 개념

DAC는 객체 소유자가 자신의 객체에 대한 접근 권한을 자율적으로 부여·변경하는 방식이다.
MAC는 시스템이 정한 보안등급과 규칙에 따라 접근을 강제로 통제하는 방식이다.
RBAC는 사용자 개인이 아니라 역할에 권한을 묶어 역할 기준으로 접근을 통제하는 방식이다.
래티스 기반 접근 제어는 보안등급의 지배관계와 격자 구조를 이용해 권한을 결정하는 방식으로, 일반적으로 MAC 계열의 모델이다.

선지별 해설

① O: 객체 소유자가 자율적으로 권한을 정하는 모델은 DAC이다. 발문의 핵심 표현인 "객체 소유자"와 "자율적 판단"이 DAC의 정의와 정확히 일치한다.
② X: 틀린 부분은 "강제적 접근 제어"이다. MAC는 소유자가 아니라 중앙 정책과 보안등급에 따라 시스템이 접근을 강제로 통제한다. 올바르게는 "시스템 정책이 보안등급에 따라 접근을 통제하는 것은 MAC이다."이다.
③ X: 틀린 부분은 "역할 기반 접근 제어"이다. RBAC는 객체 소유자의 재량이 아니라 직무나 역할에 권한을 연결해 사용자에게 역할을 부여하는 방식이다. 올바르게는 "역할에 권한을 연결해 역할 기준으로 접근을 통제하는 것은 RBAC이다."이다.
④ X: 틀린 부분은 "래티스 기반 접근 제어"이다. 래티스 기반 접근 제어는 보안등급의 상하관계와 지배관계로 접근 가능 여부를 판단한다. 올바르게는 "보안등급의 격자 구조에 따라 접근을 통제하는 것은 래티스 기반 접근 제어이다."이다.

오답 포인트

"누가 권한을 결정하는가"를 놓치면 헷갈리기 쉽다. 발문은 객체 소유자의 자율성을 묻는데, MAC와 래티스 기반 접근 제어는 시스템 정책과 보안등급이 기준이고, RBAC는 역할이 기준이라는 점에서 DAC와 다르다.

NoteBase

다시 나오면 이렇게 판단

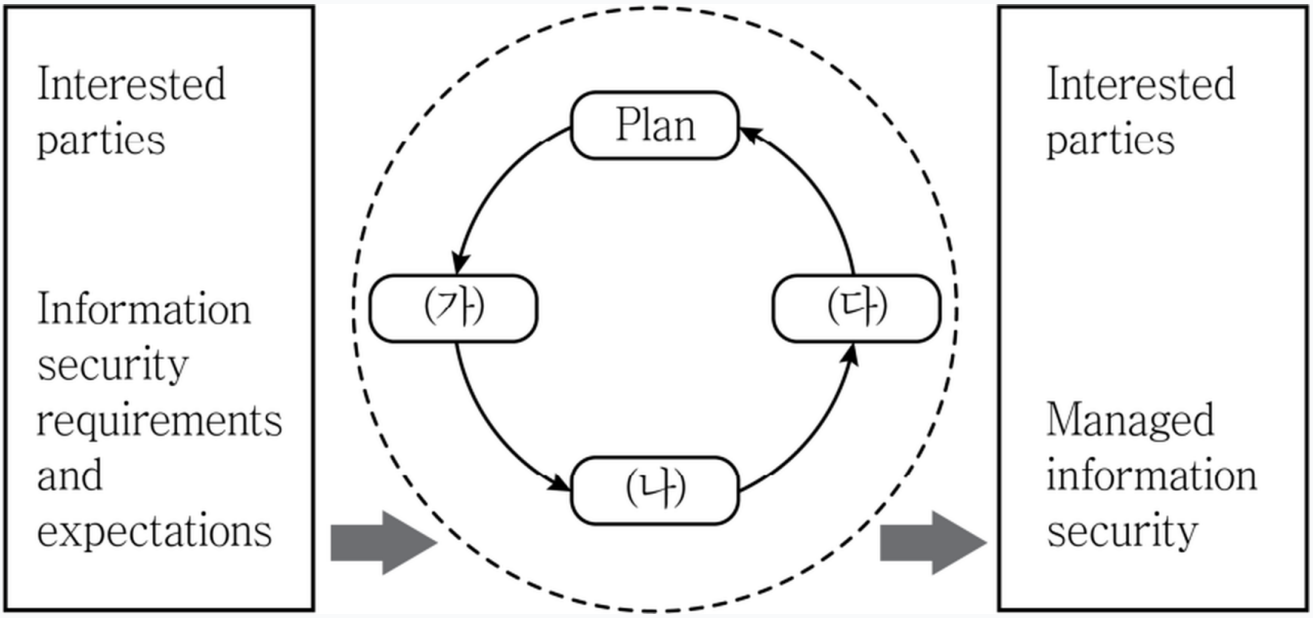
접근통제 문제는 먼저 권한 결정 주체를 본다. 소유자가 재량으로 정하면 DAC, 시스템 정책과 등급이 정하면 MAC, 역할이 정하면 RBAC로 판단하면 된다.

암기 포인트

DAC는 소유자 재량, MAC는 정책 강제, RBAC는 역할 기준이다.

NoteBase

문 13. ISO 27001 표준의 관리 체계 모델을 나타낸 다음 그림의 (가)~(다)에 들어갈 용어를 바르게 연결한 것은?



① (가): Check, (나): Act, (다): Do

② (가): Check, (나): Do, (다): Act

③ (가): Do, (나): Act, (다): Check

④ (가): Do, (나): Check, (다): Act

정답 4번

출제 포인트

이 문제는 ISO 27001 관리체계의 PDCA 순서와 각 단계의 위치를 정확히 연결하는지를 묻는 문제이다.

올바른 순서

PDCA는 Plan → Do → Check → Act의 순서이다. 따라서 그림에서 Plan 다음 단계인 (가)는 Do이고, 그다음 단계인 (나)는 Check이며, 마지막으로 Plan으로 다시 이어지는 (다)는 Act이다. 실행 결과를 먼저 점검한 뒤 그 점검 결과를 반영해 개선 조치를 하는 흐름이므로 Do와 Check, Act의 선후관계가 바뀌면 틀리게 된다.

선지 1

① X. (가)를 Check, (나)를 Act, (다)를 Do로 둔 점이 틀렸다. Plan 다음에는 실행 단계인 Do가 와야 하고, Act는 점검 이후의 개선 단계이므로 중간에 올 수 없다. 올바르게는 (가)=Do, (나)=Check, (다)=Act이다.

NoteBase

선지 2

② X. (가)를 Check로 둔 점이 먼저 틀렸다. PDCA는 계획을 세운 뒤 바로 실행하고, 실행 결과를 점검한 다음 개선한다. 올바르게는 (가)=Do, (나)=Check, (다)=Act이다.

선지 3

③ X. (가)=Do는 맞지만 (나)를 Act, (다)를 Check로 바꿔 놓아 Check와 Act의 순서를 뒤집었다. 점검 없이 바로 개선할 수 없으므로 Check가 Act보다 앞선다. 올바르게는 (가)=Do, (나)=Check, (다)=Act이다.

선지 4

④ O. PDCA의 순서를 그대로 적용하면 (가)=Do, (나)=Check, (다)=Act가 되어 그림의 흐름과 정확히 일치한다.

오답 포인트

수험생은 Plan 다음에 바로 Check가 온다고 착각하거나 Check와 Act를 비슷한 사후 단계로 묶어 순서를 바꾸기 쉽다. 그러나 Check는 실행 결과를 점검하는 단계이고 Act는 점검 결과를 반영해 시정·개선하는 단계이므로 Check 다음에 Act가 와야 한다.

다시 나오면 이렇게 판단

PDCA 문제는 계획을 세운 뒤 바로 실행하고, 실행한 내용을 점검한 뒤, 그 결과를 반영해 개선하는 흐름으로 판단하면 된다. 즉 Plan 다음은 Do, Do 다음은 Check, Check 다음은 Act로 고정해서 보면 된다.

암기 포인트

PDCA는 계획-실행-점검-개선의 순서이므로 P-D-C-A로 외우면 된다.

NoteBase

문 14. 네트워크 환경에서의 재전송(replay) 공격을 방지하기 위한 수단이 아닌 것은?

① 시퀀스 번호

② 타임 스탬프

③ 비표(nonce)

④ 샌드박스

정답 4번

출제 포인트

이 문제는 재전송 공격을 막는 수단과 무관한 개념을 구별할 수 있는지를 묻는다.

핵심 개념

시퀀스 번호는 메시지의 순서를 매겨 중복 전송이나 재전송 여부를 판별하는 값이다.
타임 스탬프는 메시지가 생성된 시각을 넣어 허용 시간 범위를 벗어난 재전송을 걸러내는 값이다.
비표는 한 번만 사용하는 난수로, 이전에 사용한 값을 다시 보내는 공격을 막는 데 쓰인다.
샌드박스는 의심스러운 코드나 프로그램을 격리된 환경에서 실행해 행위를 분석하는 기술로, 재전송 공격 방지 기법과는 성격이 다르다.

선지별 해설

1번 O: 시퀀스 번호는 패킷이나 메시지의 순번을 확인해 이미 처리한 번호의 재도착을 탐지할 수 있으므로 재전송 공격 방지 수단이 된다.
2번 O: 타임 스탬프는 메시지의 신선도를 확인하는 대표적 방법이므로 오래된 메시지를 다시 보내는 재전송 공격을 막는 데 사용된다.
3번 O: 비표(nonce)는 한 번만 사용하는 임의값이므로 응답이 이전 세션 값과 재사용되는지를 확인해 재전송 공격을 방지한다.
4번 X: 틀린 부분은 '샌드박스'이다. 샌드박스는 악성 코드 분석이나 실행 격리 기술이지 재전송 공격을 막기 위한 신선도 검증 수단이 아니다. 올바르게는 시퀀스 번호, 타임 스탬프, 비표와 같은 값이 재전송 공격 방지 수단이다.

오답 포인트

샌드박스도 보안 기술이므로 공격 방지 수단처럼 보이지만, 이 문제의 기준은 메시지의 중복 여부나 신선도를 검증하느냐이다. 보안 일반 기술과 재전송 방지 전용 기법을 섞으면 틀리기 쉽다.

NoteBase

다시 나오면 이렇게 판단

재전송 공격 방지 문제는 메시지에 고유값이나 시간 정보를 넣어 이전 메시지의 재사용을 막는 장치인지를 먼저 본다. 순번, 시간, 일회성 난수이면 재전송 방지 쪽이고, 실행 격리나 탐지 분석이면 다른 보안 기술일 가능성이 크다.

암기 포인트

재전송 방지는 순번, 시간, 일회성 값이고, 샌드박스는 격리 실행 기술이다.

NoteBase

문 15. 송신자 측에서 SSL Record 프로토콜이 수행되는 순서를 바르게 나열한 것은?

① 단편화 - 암호화 - MAC 추가 - 압축

② 단편화 - 압축 - MAC 추가 - 암호화

③ 단편화 - MAC 추가 - 암호화 - 압축

④ 압축 - MAC 추가 - 암호화 - 단편화

정답 2번

출제 포인트

이 문제는 SSL Record 프로토콜의 송신 측 처리 순서에서 각 단계의 선후관계를 정확히 구별하는지를 묻는 문제이다.

올바른 순서

1. 단편화 - 상위 계층에서 내려온 데이터를 레코드 단위로 나누는 단계이다.
2. 압축 - 단편화된 데이터를 필요하면 압축하는 단계이다.
3. MAC 추가 - 압축된 데이터의 무결성 검증값을 붙이는 단계이다.
4. 암호화 - MAC이 붙은 레코드 전체를 암호화하는 단계이다.

왜 이 순서인가: MAC은 평문 또는 압축 결과를 기준으로 계산되어야 하고, 암호화는 그 결과 전체를 보호하는 마지막 단계이기 때문이다.

선지별 해설

① X: '암호화 - MAC 추가'의 순서가 틀렸다. MAC을 먼저 붙여야 수신자가 복호화 후 무결성을 검증할 수 있다. 올바르게는 '단편화 - 압축 - MAC 추가 - 암호화'이다.

② O: 단편화 뒤 압축을 하고, 그 결과에 MAC을 추가한 다음 마지막에 암호화하므로 송신 측 SSL Record 처리 순서와 일치한다.

③ X: 'MAC 추가 - 암호화 - 압축'의 순서가 틀렸다. 압축은 암호화 전에 끝나야 하며, 암호문 상태에서 다시 압축하지 않는다. 올바르게는 '단편화 - 압축 - MAC 추가 - 암호화'이다.

④ X: 시작 단계가 틀렸다. 압축은 레코드로 단편화된 뒤 적용되므로 '압축 - ... - 단편화' 순서는 성립하지 않는다. 올바르게는 '단편화 - 압축 - MAC 추가 - 암호화'이다.

오답 포인트

압축, MAC 추가, 암호화를 한 묶음으로 외우면 'MAC을 암호화 뒤에 붙인다'거나 '압축을 맨 앞에 둔다'는 식으로 선후관계를 뒤집기 쉽다. 이 문항의 함정은 MAC이 암호문에 붙는다고 착각하거나, 수신 측 역순 절차를 송신 측 순서에 섞는 데 있다.

NoteBase

다시 나오면 이렇게 판단

절차형 문제는 입력 가공 단계가 먼저 오고, 무결성 부가가 그다음 오며, 기밀성 보호가 마지막에 온다는 흐름으로 판단한다. SSL Record 송신 측은 '나눈다 -> 줄인다 -> 검증값을 붙인다 -> 숨긴다'의 순서로 정리할 수 있다.

암기 포인트

SSL Record 송신 순서는 단편화 -> 압축 -> MAC 추가 -> 암호화이다.

NoteBase

문 16. 「개인정보 보호법」상의 개인정보 보호 인증과 관련한 다음 설명의 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

개인정보 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 「개인정보 보호법」에 부합하는지 등에 관하여 인증할 수 있다. 인증의 유효기간은 (가)으로 하며, 인증의 실효성 유지를 위하여 (나) 사후관리를 실시하여야 한다.

① (가): 2년, (나): 연 1회 이상
② (가): 2년, (나): 연 2회 이상
③ (가): 3년, (나): 연 1회 이상
④ (가): 3년, (나): 연 2회 이상

정답 3번

쟁점

이 문제는 「개인정보 보호법」상 개인정보 보호 인증의 유효기간과 사후관리 주기를 정확히 구별하는지 묻는다.

용어 풀이

개인정보 보호 인증은 개인정보처리자의 개인정보 처리 및 보호 조치가 「개인정보 보호법」에 부합하는지를 개인정보 보호위원회가 인증하는 제도이다.

핵심 구분

「개인정보 보호법」 제32조의2에 따르면 인증의 유효기간은 3년이다. 또한 인증의 실효성 유지를 위한 사후관리는 연 1회 이상 실시한다. 따라서 숫자 조합은 '3년'과 '연 1회 이상'이 맞다.

선지별 해설

1번: X. 사후관리 주기인 '연 1회 이상'은 맞지만 유효기간이 틀렸다. 법은 인증의 유효기간을 3년으로 정한다. 틀린 표현은 '2년'이고, 올바른 표현은 '3년'이다.
2번: X. 유효기간과 사후관리 횟수가 모두 틀렸다. 법은 유효기간을 3년으로, 사후관리를 연 1회 이상으로 정한다. 틀린 표현은 '2년, 연 2회 이상'이고, 올바른 표현은 '3년, 연 1회 이상'이다.
3번: O. 인증의 유효기간 3년과 사후관리 연 1회 이상이 모두 법 조문과 일치한다.
4번: X. 유효기간 3년은 맞지만 사후관리 횟수가 틀렸다. 법은 연 2회 이상이 아니라 연 1회 이상 사후관리를 실시하도록 한다. 틀린 표현은 '연 2회 이상'이고, 올바른 표현은 '연 1회 이상'이다.

NoteBase

오답 포인트

이 문제는 기간과 빈도를 한 묶음으로 암기하지 않았을 때 흔들리기 쉽다. 특히 '사후관리'라는 말 때문에 연 2회 이상처럼 더 엄격한 숫자를 떠올리면 4번으로 오답을 고르기 쉽다.

다시 나오면 이렇게 판단

법령형 숫자 문제는 조문에서 주체, 유효기간, 실시 빈도를 분리해서 확인하면 된다. 이 문항에서는 '유효기간 3년'과 '사후관리 연 1회 이상'을 각각 대조하면 바로 정답이 정리된다.

암기 포인트

개인정보 보호 인증은 3년 유효, 사후관리는 연 1회 이상이다.

NoteBase

문 17. Snort에 대한 설명으로 옳지 않은 것은?

① 오픈 소스 네트워크 기반 침입 탐지 시스템으로 개발되었다.

② 수집된 트래픽을 정상행위 프로파일과 비교하여 침입을 탐지한다.

③ 패킷의 삭제, 기록 그리고 침입 경고 생성 등의 기능을 제공한다.

④ 관리자가 정의한 침입탐지 규칙을 적용할 수 있다.

정답 2번

출제 포인트

이 문제는 Snort의 탐지 방식과 기능을 알고, 시그니처 기반 침입탐지와 이상기반 침입탐지를 구별할 수 있는지를 묻는다.

핵심 개념

Snort는 미리 정의한 규칙과 시그니처로 패킷을 검사하는 오픈 소스 네트워크 기반 IDS/IPS이다. 반면 이상기반 탐지는 정상 행위 프로파일에서 벗어나는 패턴을 찾아내는 방식이다.

선지별 해설

1번 O: Snort는 대표적인 오픈 소스 네트워크 기반 침입 탐지 시스템으로 시작한 도구이므로 옳다.
2번 X: 틀린 부분은 "정상행위 프로파일과 비교"이다. 이는 이상기반 침입탐지의 설명이며, Snort는 실제로는 미리 정의한 룰과 시그니처를 패킷과 비교하여 침입을 탐지한다.
3번 O: Snort는 패킷을 기록하고 경고를 생성하며, 인라인 모드에서는 악성 패킷을 드롭하는 기능도 제공하므로 옳다.
4번 O: Snort는 관리자가 규칙 파일을 작성하거나 수정하여 침입탐지 규칙을 적용할 수 있으므로 옳다.

오답 포인트

Snort도 네트워크 트래픽을 분석하므로 이상기반 시스템과 헷갈리기 쉽다. 이 문항에서는 2번의 "정상행위 프로파일"이라는 표현이 이상기반 탐지의 핵심 단서이다.

다시 나오면 이렇게 판단

문장에 룰, 시그니처, 관리자 정의 규칙, 로그, 경고, 패킷 드롭이 나오면 Snort 같은 시그니처 기반 IDS/IPS를 떠올리면 된다. 반대로 정상 프로파일과의 편차 비교가 나오면 이상기반 탐지로 판단한다.

암기 포인트

Snort는 오픈 소스 NIDS/IPS이며 룰·시그니처 기반이고, 정상 프로파일 비교는 이상기반 탐지이다.

NoteBase

문 18. 다음 설명에 해당하는 웹 보안 공격은?

사용자가 인지하지 못한 사이에 웹 서버가 신뢰하는 사용자의 웹 브라우저로부터 공격자가 의도한 명령이 웹 서버에 전달되어 사용자의 권한으로 실행되도록 한다.

① 저장형 XSS
② 반사형 XSS
③ XXE(XML eXternal Entity)
④ CSRF

정답 4번

출제 포인트

이 문제는 사용자의 인증 상태를 악용해 서버로 원치 않는 요청을 보내는 CSRF와 XSS, XXE의 차이를 묻는 문제이다.

핵심 개념

CSRF는 로그인된 사용자의 브라우저가 자동으로 보내는 세션 쿠키를 악용하여 서버에 요청을 위조하는 공격이다.
XSS는 브라우저에서 악성 스크립트가 실행되도록 만들어 사용자 세션 탈취나 화면 변조를 일으키는 공격이다.
XXE는 XML 파서의 외부 엔티티 처리 기능을 악용하여 서버 내부 파일 조회나 내부망 접근을 시도하는 서버 측 공격이다.

NoteBase

선지별 해설

① X
저장형 XSS는 악성 스크립트가 게시판이나 댓글 등에 저장되었다가 이후 다른 사용자의 브라우저에서 실행되는 공격이다. 틀린 부분은 '공격자가 의도한 명령이 웹 서버에 전달되어 사용자의 권한으로 실행'된다는 점에 저장형 XSS를 대응시킨 것이다. 저장형 XSS로 고치려면 '악성 스크립트가 서버에 저장되어 사용자의 브라우저에서 실행된다'로 바뀌어야 한다.

② X
반사형 XSS는 공격용 입력값이 서버 응답에 즉시 반사되어 브라우저에서 스크립트가 실행되는 공격이다. 틀린 부분은 '웹 서버가 신뢰하는 사용자의 웹 브라우저로부터 명령이 전달된다'는 설명을 반사형 XSS로 본 점이다. 반사형 XSS로 고치려면 '조작된 링크나 요청의 입력값이 응답에 반사되어 브라우저에서 실행된다'로 바뀌어야 한다.

③ X
XXE는 XML eXternal Entity 취약점을 이용해 XML 파서가 외부 엔티티를 처리하게 만드는 공격이다. 틀린 부분은 사용자 브라우저의 인증 상태를 이용한 요청 위조를 XXE로 본 점이다. XXE로 고치려면 '취약한 XML 파서가 외부 엔티티를 해석하여 서버 내부 자원에 접근한다'로 바뀌어야 한다.

④ O
CSRF는 사용자가 인지하지 못하는 사이 공격자가 만든 요청이 사용자의 브라우저를 통해 서버로 전송되고, 서버가 기존 세션 쿠키를 신뢰하여 정상 사용자 요청처럼 처리하는 공격이다. 제시문의 '사용자가 인지하지 못한 사이', '웹 서버가 신뢰하는 사용자의 웹 브라우저', '사용자의 권한으로 실행'이 모두 CSRF의 핵심 특징과 일치한다.

오답 포인트

XSS와 CSRF는 모두 브라우저가 매개가 되므로 혼동하기 쉽지만, XSS의 핵심은 브라우저에서 스크립트가 실행된다는 점이고 CSRF의 핵심은 로그인된 사용자의 권한으로 요청이 위조된다는 점이다. 제시문에 '스크립트 실행'이 아니라 '사용자의 권한으로 실행'이 나오면 CSRF 쪽으로 판단이 기운다.

다시 나오면 이렇게 판단

문장에 사용자 모르게 요청이 전송되고 서버가 세션이나 쿠키를 믿어 처리한다는 흐름이 보이면 CSRF이다. 브라우저 스크립트 실행이면 XSS, XML 외부 엔티티 처리면 XXE로 구분한다.

암기 포인트

CSRF는 요청 위조, XSS는 스크립트 실행, XXE는 XML 외부 엔티티 악용이다.

NoteBase

문 19. TCP 세션 하이재킹 공격에 대한 다음 설명의 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

◯ 공격자는 클라이언트와 서버의 TCP 연결 상태를 스니핑한다.◯ 공격자는 세션이 완전히 끊어지지 않는 범위에서 서버에게 (가) 세그먼트를 보내어 서버를 잠시 Closed 상태로 만든다.◯ 공격자는 조작된 (나) 번호로 서버와 새로운 TCP 연결을 설정한다.◯ 결과적으로 공격자는 세션을 탈취하고 인증을 회피할 수 있게 된다.

① (가): FIN, (나): Sequence

② (가): FIN, (나): Acknowledgment

③ (가): RST, (나): Sequence

④ (가): RST, (나): Acknowledgment

정답 3번

출제 포인트

이 문제는 TCP 세션 하이재킹에서 연결을 즉시 끊는 제어 세그먼트와 세션 탈취에 핵심이 되는 번호가 무엇인지를 묻는 문제이다.

핵심 개념

RST는 현재 TCP 연결을 즉시 재설정하여 상대를 Closed 상태로 보내는 제어 세그먼트이다.
FIN은 정상 종료 절차를 시작하는 세그먼트이므로 즉시 강제 종료와는 성격이 다르다.
Sequence number는 TCP 바이트 흐름의 순서를 나타내는 번호로, 세션 하이재킹에서는 이 값을 맞추거나 조작해야 상대가 위조 세그먼트를 정상 데이터로 받아들인다.
Acknowledgment number는 상대가 다음에 받기를 기대하는 바이트 위치를 알리는 확인 번호이므로, 세션 탈취의 핵심 용어로 단독 지목되기 어렵다.

NoteBase

선지별 해설

① X
(가)를 FIN으로 둔 점이 틀리다. FIN은 정상적인 연결 종료를 요청하는 것이므로 서버를 즉시 Closed 상태로 보내는 공격용 세그먼트와 맞지 않는다. (나)의 Sequence는 세션 탈취 관점에서 맞는 방향이지만, 올바른 연결은 RST-Sequence이다.

② X
(가)를 FIN으로 둔 점이 틀리고, (나)를 Acknowledgment로 둔 점도 틀리다. 즉시 연결을 재설정하는 것은 RST이며, 세션 하이재킹에서 핵심은 위조 패킷이 받아들여지도록 Sequence number를 맞추는 것이다. 올바르게는 RST-Sequence이다.

③ O
RST는 연결을 강제로 재설정하여 서버 쪽 세션을 끊거나 비정상 종료 상태로 만들 때 사용하는 제어 세그먼트이다. 이후 공격자는 스니핑으로 파악한 흐름을 바탕으로 조작된 Sequence number를 사용해 서버가 정상 세션의 연속으로 오인하도록 만들 수 있으므로 연결이 맞다.

④ X
(가)의 RST는 맞지만, (나)의 Acknowledgment가 틀리다. 확인 번호만 바꾼다고 세션 탈취가 성립하는 것이 아니라, 서버가 받아들일 데이터 흐름 위치인 Sequence number를 맞춰야 한다. 올바르게는 RST-Sequence이다.

오답 포인트

FIN과 RST를 모두 종료 관련 세그먼트로만 외우면 ①, ②에 흔들리기 쉽다. 이 문항의 함정은 종료의 방식이 아니라 즉시 강제 종료인지 정상 종료 절차인지의 차이이다. 또한 Acknowledgment와 Sequence를 함께 보다가 확인 번호가 더 익숙하다는 이유로 ④를 고르기 쉽지만, 세션 탈취의 핵심은 데이터 흐름 순서를 속이는 Sequence number이다.

다시 나오면 이렇게 판단

문장에 즉시 종료, 강제 재설정, Closed 상태가 나오면 먼저 RST를 떠올리면 된다. 반대로 정상 종료 절차, 종료 요청, half-close가 나오면 FIN 가능성을 본다. 세션 하이재킹 문항에서는 공격자가 상대에게 정상 패킷처럼 보이게 해야 하므로 우선 Sequence number 관련 설명인지 확인하면 된다.

암기 포인트

RST는 강제 리셋, FIN은 정상 종료, 하이재킹의 핵심 번호는 Sequence이다.

NoteBase

문 20. 다음은 사용자 A와 B가 Diffie-Hellman 키 교환 프로토콜을 이용하여 비밀키를 공유하려고 하는데 D에 의한 중간자 공격이 발생한 과정을 순서대로 나타낸 것이다. 이 결과로 A가 얻은 비밀키와 B가 얻은 비밀키를 바르게 연결한 것은? (단, 사전에 A와 B는 공개된 소수 q와 원시근 α를 이용하여 각자 자신의 개인키로 X_A와 X_B를 생성하고 자신의 공개키로 Y_A와 Y_B를 각각 산출한다)

◯ D는 임의 개인키 X_{D1}과 X_{D2}를 생성하고 이에 대응하는 공개키 Y_{D1}과 Y_{D2}를 계산한다.
◯ A가 Y_A를 B에게 전송한다.
◯ D는 Y_A를 가로채고 대신에 Y_{D1}을 B에게 전송한다.
◯ B는 Y_{D1}을 받고 A에게 Y_B를 전송한다.
◯ D는 Y_B를 가로채고 대신에 Y_{D2}를 A에게 전송한다.
◯ A가 Y_{D2}를 받는다.

① A의 비밀키: (Y_A)^X_D1 q, B의 비밀키: (Y_B)^X_D2 q
② A의 비밀키: (Y_B)^X_D2 q, B의 비밀키: (Y_A)^X_D1 q
③ A의 비밀키: (Y_A)^X_D2 q, B의 비밀키: (Y_B)^X_D1 q
④ A의 비밀키: (Y_B)^X_D1 q, B의 비밀키: (Y_A)^X_D2 q

정답 3번

출제 포인트

이 문제는 Diffie-Hellman 중간자 공격에서 각 사용자가 실제로 받은 공개키와 자신의 개인키를 결합해 어떤 비밀키를 계산하는지를 묻는 문제이다.

올바른 순서

1. A가 자신의 공개키 Y_A를 전송하나 D가 이를 가로채고 B에게는 Y_{D1}을 보낸다.
2. B는 자신이 실제로 받은 Y_{D1}과 자신의 개인키 X_B로 비밀키를 계산하므로 (Y_D1)^X_B ≡ (Y_B)^X_D1 ±od q가 된다.
3. B가 자신의 공개키 Y_B를 전송하나 D가 이를 가로채고 A에게는 Y_{D2}를 보낸다.
4. A는 자신이 실제로 받은 Y_{D2}와 자신의 개인키 X_A로 비밀키를 계산하므로 (Y_D2)^X_A ≡ (Y_A)^X_D2 ±od q가 된다.

왜 이 순서인가: DH 비밀키는 항상 받은 공개키를 자신의 개인키로 거듭제곱해 계산하므로, D가 바꿔치기한 공개키가 각 사용자의 계산식을 결정한다.

NoteBase

선지별 해설

① X
틀린 이유: A의 비밀키를 $(Y_A)^{X_{D1}}$로 두면 A가 받은 공개키가 아니라 자신의 공개키 Y_A를 사용한 셈이 되고, B의 비밀키를 $(Y_B)^{X_{D2}}$로 두면 B가 받은 Y_{D1}이 아니라 자신의 공개키 Y_B를 사용한 셈이 된다.
올바르게는: A의 비밀키는 (Y_D2)^X_A ≡ (Y_A)^X_D2 ±od q, B의 비밀키는 (Y_D1)^X_B ≡ (Y_B)^X_D1 ±od q이다.

② X
틀린 이유: A는 Y_B를 직접 받지 못하고 Y_{D2}를 받으므로 $(Y_B)^{X_{D2}}$는 A의 계산식이 아니다. B도 Y_A를 받지 못하고 Y_{D1}을 받으므로 $(Y_A)^{X_{D1}}$는 B의 계산식이 아니다.
올바르게는: A는 받은 Y_{D2}와 X_A를, B는 받은 Y_{D1}과 X_B를 결합한다.

③ O
맞는 이유: A가 계산하는 값은 $(Y_{D2})^{X_A}$이고 이는 $Y_{D2} = \alpha^{X_{D2}}$, $Y_A = \alpha^{X_A}$이므로 $(Y_A)^{X_{D2}}$와 동치이다. B가 계산하는 값도 $(Y_{D1})^{X_B}$이며 이는 $(Y_B)^{X_{D1}}$와 동치이므로 ③의 연결이 맞다.

④ X
틀린 이유: A의 비밀키를 $(Y_B)^{X_{D1}}$로 두면 A가 실제로 받지 않은 Y_B를 사용한 셈이고, B의 비밀키를 $(Y_A)^{X_{D2}}$로 두면 B가 실제로 받지 않은 Y_A를 사용한 셈이다. 양쪽 모두 받은 공개키의 방향이 뒤바뀌었다.
올바르게는: A 쪽은 $(Y_A)^{X_{D2}}$, B 쪽은 $(Y_B)^{X_{D1}}$로 연결해야 한다.

오답 포인트

함정은 두 가지이다. 첫째, 중간자 공격에서는 원래 상대 공개키가 아니라 실제 수신 공개키를 써야 하는데 이를 놓치면 ②나 ④처럼 원래 공개키 Y_A, Y_B를 그대로 대입하게 된다. 둘째, $(Y_{D2})^{X_A}$를 $(Y_A)^{X_{D2}}$로 바꿔 쓸 수 있다는 동치 관계를 놓치면 ③을 틀린 식처럼 오해하게 된다.

다시 나오면 이렇게 판단

DH 변형 문제는 각 사용자 기준으로 실제로 받은 공개키가 무엇인지 먼저 표시한 뒤, 그 값을 자신의 개인키로 거듭제곱한다고 판단하면 된다. 그 다음에만 $Y = \alpha^X$ 관계를 이용해 동치식으로 변형하면 선지의 형태가 달라도 정답을 가를 수 있다.

암기 포인트

중간자 공격의 비밀키는 '내 개인키 + 내가 실제로 받은 공개키'의 조합이다. A는 Y_{D2}, B는 Y_{D1}을 받는다고 기억하면 된다.

NoteBase

문 21. IEEE 802.11i에서 사용하는 CCMP에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. 무선 단말과 AP 사이 구간에서의 데이터 기밀성과 무결성을 위해 동일한 128비트 키가 사용된다.
ㄴ. Michael 알고리즘에 의한 MIC(Message Integrity Code)를 추가하여 무결성을 제공한다.
ㄷ. 데이터 암호화를 위해 AES 암호 알고리즘과 CBC 블록 암호 운용 모드를 사용한다.
ㄹ. CBC 블록 암호 운용 모드를 이용한 암호 기반의 MAC을 이용한다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 2번

출제 포인트

이 문제는 CCMP의 구성요소를 TKIP의 Michael, 그리고 CBC 운용모드와 구별할 수 있는지를 묻는다.

핵심 개념

CCMP는 IEEE 802.11i에서 사용하는 보호 방식으로, AES 128비트 키를 기반으로 기밀성은 Counter Mode로, 무결성과 인증은 CBC-MAC으로 제공한다.
TKIP의 Michael은 무결성 검사용 MIC 알고리즘이지만 CCMP의 구성요소는 아니다.
CBC는 블록 암호 운용모드의 한 종류이지만, CCMP의 데이터 암호화는 CBC가 아니라 Counter Mode를 사용한다.

선지별 해설

1번: X. ㄱ은 옳고 ㄷ은 틀리므로 조합이 맞지 않는다. ㄱ은 CCMP가 동일한 128비트 AES 키를 바탕으로 기밀성과 무결성 보호에 사용된다는 설명으로 볼 수 있다. 반면 ㄷ의 틀린 부분은 "CBC 블록 암호 운용 모드"이다. 실제로는 데이터 암호화에 Counter Mode를 사용한다.
2번: O. ㄱ과 ㄹ이 모두 옳다. ㄹ은 CCMP가 CBC-MAC을 사용해 무결성과 메시지 인증을 제공한다는 설명으로 정확하다.
3번: X. ㄴ과 ㄷ이 모두 틀리다. ㄴ의 틀린 부분은 "Michael 알고리즘"이다. 실제로는 Michael MIC가 아니라 AES 기반 CBC-MAC을 사용한다. ㄷ도 암호화 모드를 CBC라고 한 점이 틀렸고, 올바르게는 Counter Mode이다.
4번: X. ㄹ은 옳지만 ㄴ이 틀리므로 조합이 맞지 않는다. CCMP의 무결성 보호는 Michael이 아니라 CBC-MAC이다.

NoteBase

오답 포인트

TKIP의 Michael과 CCMP의 CBC-MAC을 섞어 기억하면 ㄴ을 맞는 설명처럼 보기 쉽다. 또 CCMP라는 이름에 CBC가 들어가므로 암호화도 CBC로 한다고 오해하기 쉬운데, CBC는 MAC 쪽이고 암호화는 Counter Mode이다.

다시 나오면 이렇게 판단

무선 LAN 보안 문제에서는 먼저 방식 이름을 구성요소로 분해해 판단한다. CCMP는 Counter Mode와 CBC-MAC의 결합이고, TKIP는 Michael을 사용한다는 축으로 보면 선지의 진위를 빠르게 가를 수 있다.

암기 포인트

CCMP는 AES 기반 Counter Mode + CBC-MAC, Michael은 TKIP이다.

NoteBase

문 22. TCP 프로토콜의 보안 관련 특징에 대한 설명으로 옳지 않은 것은?

① 포트 번호를 활용하여 응용에 대한 접근통제 정책을 설정할 수 있다.

② SYN Flooding은 3-way handshaking 동작 절차를 악용한 공격이다.

③ TCP 포트 스캐닝을 통해 동작 중인 서비스를 확인할 수 있다.

④ TCP 헤더의 체크섬을 이용하여 전송 중에 발생한 데이터의 위·변조를 탐지할 수 있다.

정답 4번

출제 포인트

이 문제는 TCP의 기본 기능과 보안상 한계를 구분할 수 있는지를 묻는 문제이다.

핵심 개념

포트 번호는 서비스 식별자이므로 접근통제 정책의 기준으로 활용될 수 있다.
3-way handshaking은 TCP 연결 설정 절차이므로 SYN Flooding의 표적이 된다.
TCP 포트 스캐닝은 열려 있는 포트를 확인하여 동작 중인 서비스 존재를 추정하는 기법이다.
TCP 체크섬은 전송 중 우발적 오류를 검출하는 기능일 뿐, 암호학적 무결성 검증 수단은 아니다.

선지별 해설

① O
포트 번호는 HTTP 80, HTTPS 443처럼 서비스와 결부되므로 방화벽이나 ACL에서 특정 응용 서비스에 대한 접근통제 기준으로 사용할 수 있다.

② O
SYN Flooding은 TCP의 3-way handshaking에서 서버가 반개방 연결 상태를 유지하는 점을 악용하는 공격이다.

③ O
TCP 포트 스캐닝은 대상 호스트의 포트 개방 여부를 확인하여 어떤 서비스가 동작 중인지 파악하는 데 쓰인다.

④ X
틀린 부분은 "데이터의 위·변조를 탐지"이다.
TCP 체크섬은 전송 과정의 우발적 비트 오류를 검출하는 용도이다. 악의적 위·변조 방지는 암호학적 무결성 검증이 필요하므로, 올바르게는 "TCP 체크섬으로 전송 오류를 검출할 수 있다"라고 이해해야 한다.

NoteBase

오답 포인트

체크섬이 무결성과 관련된다는 말만 보고 보안 기능으로 일반화하기 쉽다. 이 문항은 오류 검출과 위·변조 방지를 의도적으로 섞어 TCP의 기능과 암호학적 무결성 보호를 혼동하게 만든다.

다시 나오면 이렇게 판단

TCP의 보안 관련 선지는 먼저 그것이 서비스 식별, 연결 설정, 서비스 탐지, 오류 검출 중 어느 기능인지 분류하면 판단이 쉬워진다. 체크섬이 나오면 우발적 오류 검출인지, 암호학적 무결성 보장인지부터 구분한다.

암기 포인트

포트는 접근통제, SYN은 연결설정, 스캐닝은 서비스 탐지, 체크섬은 오류 검출이다.

NoteBase

문 23. SEED 128 알고리즘에 대한 설명으로 옳지 않은 것은?

① 1999년 2월 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 128비트 블록 암호 알고리즘이다.

② 전체 구조는 SPN 구조로 이루어져 있으며, 128비트의 평문 블록과 128비트 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트의 암호문을 출력한다.

③ 128비트 암호키를 64비트씩 좌우로 나누어 처리해서 얻어진 4개의 워드에 대해 간단한 산술연산과 G 함수를 적용하여 라운드 키를 생성한다.

④ 1999년 9월 정보통신단체표준(TTA)으로 제정되었으며, 2005년에는 국제 표준화 기구인 ISO/IEC와 IETF로부터 암호화 표준 알고리즘으로 인정받았다.

정답 2번

출제 포인트

이 문제는 SEED 128의 전체 암호 구조, 키 스케줄 방식, 표준화 이력을 구분하는 문제이다.

핵심 개념

SEED 128은 128비트 블록과 128비트 키를 사용하는 국산 대칭키 블록 암호이다. 전체 구조는 SPN이 아니라 16라운드 Feistel 구조이며, 키 스케줄은 128비트 키를 네 개의 32비트 워드로 나누어 G 함수와 모듈러 덧셈·뺄셈, 순환이동을 이용해 라운드 키를 생성한다.

NoteBase

선지별 해설

① O
SEED는 국산 128비트 블록 암호로 소개되며, 개발 배경과 국내 기술 기반 설명도 맞는 방향이다. 핵심은 SEED가 국내에서 개발된 128비트 블록 암호라는 점이다.

② X
틀린 표현은 "SPN 구조"이다.
SEED 128의 전체 구조는 SPN이 아니라 16라운드 Feistel 구조이다. 128비트 평문 블록과 128비트 키를 사용한다는 부분과 16라운드를 거친다는 부분은 맞지만, 구조를 SPN으로 적은 것이 오답이다.

③ O
SEED의 키 스케줄은 128비트 키를 네 개의 32비트 워드로 나누고, 이를 좌우 64비트 단위와 연결해 순환이동시키면서 G 함수와 산술연산으로 각 라운드의 서브키를 만든다. 따라서 라운드 키 생성 방식에 대한 설명으로 볼 수 있다.

④ O
SEED는 1999년 9월 TTA 표준으로 제정되었고, 2005년에는 ISO/IEC와 IETF RFC를 통해 국제 표준 계열에 포함되었다. 표준화 이력을 묻는 설명으로 맞다.

오답 포인트

AES가 대표적인 SPN 구조이기 때문에 블록 크기와 라운드 수만 보고 SEED도 SPN으로 착각하기 쉽다. 이 문항은 ②에서 블록 크기 128비트, 키 길이 128비트, 16라운드라는 맞는 정보를 섞어 두고 구조만 바꿔 놓은 함정을 쓴 문제이다.

다시 나오면 이렇게 판단

국산 블록 암호 문제에서 SEED가 나오면 먼저 "16라운드 Feistel"인지 확인하면 된다. 선지에 SPN이 나오면 AES류 특징과 뒤섞은 오답일 가능성이 높고, 키 스케줄은 G 함수와 회전, 모듈러 연산으로 서브키를 만든다는 점을 함께 대조하면 된다.

암기 포인트

SEED는 128비트 블록·128비트 키·16라운드 Feistel 구조이다.

NoteBase

문 24. ISMS-P 인증기준의 개인정보 처리 단계별 요구사항으로 옳지 않은 것은?

① 인증 및 권한관리

② 개인정보 수집 시 보호조치

③ 개인정보 보유 및 이용 시 보호조치

④ 정보주체 권리보호

정답 1번

쟁점

이 문제는 ISMS-P 인증기준에서 개인정보 처리단계별 요구사항에 속하는 항목과 보호대책 요구사항에 속하는 항목을 구별하는 문제이다.

용어 풀이

개인정보 처리단계별 요구사항은 수집, 보유 및 이용, 제공, 파기, 정보주체 권리보호처럼 개인정보 처리 흐름에 따라 배치된 기준이다.
보호대책 요구사항은 인증 및 권한 관리, 접근통제, 암호화처럼 정보보호 통제 영역별로 배치된 기준이다.

핵심 구분

개인정보 처리단계별 요구사항은 3.1 개인정보 수집 시 보호조치, 3.2 개인정보 보유 및 이용 시 보호조치, 3.3 개인정보 제공 시 보호조치, 3.4 개인정보 파기 시 보호조치, 3.5 정보주체 권리보호로 구성된다.
반면 인증 및 권한 관리는 개인정보 처리단계별 요구사항이 아니라 2.5 보호대책 요구사항에 속한다.

선지별 해설

1번: X. 인증 및 권한 관리는 개인정보 처리 단계별 요구사항이 아니라 보호대책 요구사항의 세부 항목이다.
틀린 표현: 인증 및 권한관리
올바른 표현: 인증 및 권한관리는 2.5 보호대책 요구사항이다.
2번: O. 개인정보 수집 시 보호조치는 개인정보를 처음 수집하는 단계에서의 요구사항이므로 개인정보 처리단계별 요구사항에 해당한다.
3번: O. 개인정보 보유 및 이용 시 보호조치는 수집 후 보유·이용 단계의 요구사항이므로 개인정보 처리단계별 요구사항에 해당한다.
4번: O. 정보주체 권리보호는 개인정보 처리단계별 요구사항의 한 축으로, 열람·정정·삭제 등 정보주체 권리 보장과 관련된 기준이다.

NoteBase

오답 포인트

1번의 인증 및 권한관리는 이름에 개인정보가 직접 들어가지 않아 처리단계 항목처럼 보일 수 있으나, 실제로는 접근통제와 유사한 보안통제 묶음이다. 처리 흐름 기준인지 통제 영역 기준인지를 구분하지 않으면 틀리기 쉽다.

다시 나오면 이렇게 판단

선지의 표현이 수집·보유 및 이용·제공·파기·정보주체 권리처럼 처리 흐름을 나타내면 3번대 개인정보 처리단계별 요구사항으로 본다. 인증, 접근통제, 암호화처럼 보안통제 수단을 나타내면 2번대 보호대책 요구사항으로 판단한다.

암기 포인트

3번대는 개인정보 처리 흐름, 2번대는 보안통제 영역이라는 구분으로 외우면 된다.

NoteBase

문 25. 다음은 쿠키(Cookie)의 일반적인 생성 및 저장 과정을 순서대로 나타낸 것이다. 이 과정 이후에 클라이언트가 다시 서버에 요청을 보낼 때, HTTP 메시지에 포함되는 것은?

◯ 서버가 클라이언트로부터 요청을 받으면 서버는 클라이언트에 관한 정보를 파일이나 문자열로 저장한다.
◯ 서버는 클라이언트에게 보내는 응답에 쿠키를 포함한다.
◯ 클라이언트가 응답을 받으면 브라우저는 쿠키를 도메인 서버 이름으로 정렬되는 쿠키 디렉터리에 저장한다.

① 요청 라인의 Set-Cookie
② 헤더 라인의 Set-Cookie
③ 요청 라인의 Cookie
④ 헤더 라인의 Cookie

정답 4번

출제 포인트

이 문제는 쿠키가 최초 발급될 때의 `Set-Cookie`와 이후 재요청 시 실려 가는 `Cookie`의 위치를 구분하는 문제이다.

핵심 개념

쿠키는 서버가 응답 헤더의 `Set-Cookie`로 내려보내고, 브라우저가 이를 저장한 뒤 같은 도메인에 다시 요청할 때 요청 헤더의 `Cookie`로 보낸다. 요청 라인은 메서드, 요청 URI, HTTP 버전으로 구성되므로 쿠키가 들어가지 않는다.

선지별 해설

① X: `Set-Cookie`는 서버가 쿠키를 설정할 때 사용하는 응답 헤더이다. 이후 클라이언트의 재요청 메시지에는 실리지 않으므로 틀린 표현은 `요청 라인`과 `Set-Cookie`이다. 올바르게는 `응답 헤더의 Set-Cookie`이다.
② X: 헤더 라인이라는 위치 자체는 맞지만, 문제는 클라이언트가 다시 서버에 요청할 때 포함되는 항목을 묻는다. 틀린 표현은 `Set-Cookie`이다. 올바르게는 `헤더 라인의 Cookie`이다.
③ X: 재요청 때 브라우저가 보내는 값이 `Cookie`인 점은 맞다. 다만 요청 라인은 `GET /path HTTP/1.1`처럼 시작줄만 포함하므로 쿠키가 들어가지 않는다. 틀린 표현은 `요청 라인`이다. 올바르게는 `헤더 라인의 Cookie`이다.
④ O: 저장된 쿠키는 이후 같은 서버로 요청할 때 요청 헤더의 `Cookie` 필드에 포함된다. 따라서 HTTP 메시지에 포함되는 위치와 이름을 모두 맞춘 선택지는 ④이다.

NoteBase

오답 포인트

③은 이름 `Cookie`만 맞고 위치를 `요청 라인`으로 바꿔 놓은 함정이다. ②는 헤더라는 위치는 맞지만 발급 단계의 `Set-Cookie`를 재전송 단계에도 그대로 적용하도록 유도한다.

다시 나오면 이렇게 판단

쿠키 문제는 먼저 발급 단계인지 재요청 단계인지를 구분하면 된다. 서버가 브라우저에 심어 줄 때는 `Set-Cookie`, 브라우저가 다시 보낼 때는 `Cookie`이며, 둘 다 헤더 필드이지 요청 라인은 아니다.

암기 포인트

`Set-Cookie`는 서버 응답, `Cookie`는 클라이언트 요청, 쿠키 위치는 항상 헤더이다.

NoteBase