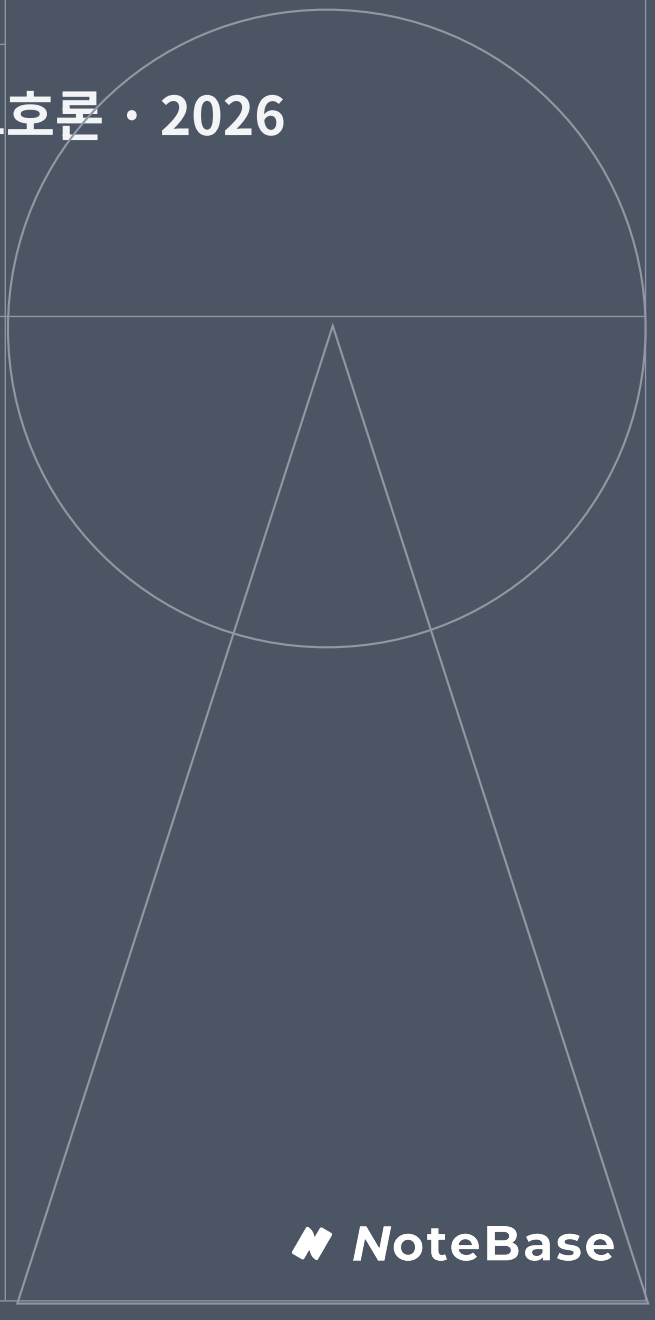
기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2026



NoteBase

기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2026

공무원/법원직/9급 · 정보보호론 · 2026

문 1. ISMS-P(정보보호 및 개인정보보호 관리체계)에 관한 다음 설명 중 가장 옳지 않은 것은?

① ISMS-P는 정보보호와 개인정보보호 관리체계를 함께 심사하는 인증제도이다.

② 관리체계의 수립·운영 등 조직적·관리적 보호 활동이 주요 평가 대상이 된다.

③ 국내에서는 KISA가 제도 안내와 심사 관련 정보를 제공한다.

④ ISMS-P는 개별 보안 제품의 기능 안전성을 시험하는 제품 인증제도이다.

정답 4번

출제 포인트

ISMS-P가 조직의 정보보호·개인정보보호 관리체계를 인증하는 제도인지, 개별 보안 제품을 시험하는 제도인지 구별하는 문제이다.

핵심 개념

ISMS-P는 조직이 정보보호와 개인정보보호를 위해 수립·운영하는 일련의 조치와 활동이 인증기준에 적합한지를 심사하는 관리체계 인증제도이다. 평가 범위에는 관리체계 수립·운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항이 포함된다. 따라서 조직의 관리체계를 평가하는 ISMS-P와 개별 보안 제품의 기능을 시험하는 제품 인증은 구별된다.

선지별 해설

① O. ISMS-P는 정보보호와 개인정보보호를 함께 포괄하는 통합 관리체계 인증이다.
② O. 관리체계의 기반 마련, 위험 관리, 운영, 점검·개선 등 조직적·관리적 보호 활동은 주요 인증기준에 포함된다. 다만 기술적·물리적 보호대책과 개인정보 처리 단계별 보호조치도 함께 평가한다.
③ O. 한국인터넷진흥원(KISA)은 ISMS-P의 법정 인증기관으로서 제도 운영, 인증 품질관리, 인증심사 및 심사원 관련 정보를 제공한다.
④ X. 틀린 표현은 '개별 보안 제품의 기능 안전성을 시험하는 제품 인증제도'이다. 올바르게는 ISMS-P는 조직의 정보보호 및 개인정보보호 관리체계가 인증기준에 적합한지를 심사하는 관리체계 인증제도이다.

NoteBase

오답 포인트

‘인증’이라는 말만 보고 ISMS-P를 제품 단위 시험·인증으로 오해하기 쉽다. 이 문항에서는 평가 대상이 개별 제품인지 조직의 관리체계인지가 결정적인 구별 기준이다.

다시 나오면 이렇게 판단

선지의 평가 대상을 먼저 확인한다. 조직의 정책·위험관리·보호대책·개인정보 처리 활동을 심사하면 ISMS-P이고, 개별 제품의 성능이나 기능을 시험한다고 하면 ISMS-P의 설명이 아니다.

암기 포인트

ISMS-P는 제품 인증이 아니라 조직의 정보보호·개인정보보호 관리체계 인증이다.

NoteBase

문 2. SSL과 TLS의 운용 및 보안성에 관한 다음 설명 중 가장 옳지 않은 것은?

① SSL 3.0은 역사적으로 통신의 기밀성, 변조 방지, 메시지 위조 방지를 목표로 설계된 프로토콜이었다.

② SSL 3.0은 더 이상 안전하다고 보기 어려우므로, 현대적 운용에서는 사용하지 않아야 한다.

③ TLS 1.3은 클라이언트와 서버 응용이 도청, 변조, 메시지 위조를 방지하도록 통신하기 위한 프로토콜이다.

④ 구형 시스템과의 호환성을 위해 TLS 접속 실패 시 SSL 3.0으로 자동 하향(fallback)하는 기능은 보안상 권장된다.

정답 4번

출제 포인트

SSL 3.0과 TLS 1.3의 보안 목표를 구분하고, 안전하지 않은 구형 프로토콜로의 하향 연결이 왜 허용되지 않는지 판단하는 문제이다.

핵심 개념

SSL 3.0: 도청, 변조, 메시지 위조를 막는 통신을 목표로 설계된 과거의 보안 프로토콜이지만, 현재는 근본적인 취약점 때문에 사용과 협상이 금지된다.
TLS 1.3: 클라이언트와 서버 사이의 통신을 도청, 변조, 메시지 위조로부터 보호하도록 설계된 현대적 전송 계층 보안 프로토콜이다.
프로토콜 하향 연결: 접속 실패를 이유로 더 낮고 취약한 버전으로 다시 연결하면 공격자가 이를 유도하는 다운그레이드 공격이 가능하므로, 적절한 버전 협상을 통해 양측이 지원하는 안전한 TLS 버전을 사용해야 한다.

선지별 해설

① O — SSL 3.0은 역사적으로 응용 프로그램의 통신에서 도청을 막아 기밀성을 확보하고, 변조와 메시지 위조를 방지하도록 설계되었다.
② O — SSL 3.0은 여러 취약점으로 인해 더 이상 안전하지 않으며, 현대적 운용에서는 사용하거나 TLS에서 SSL 3.0으로 협상해서는 안 된다.
③ O — TLS 1.3은 클라이언트와 서버 응용의 통신에서 도청, 변조, 메시지 위조를 방지하는 것을 보안 목표로 한다.
④ X — 틀린 표현은 ‘SSL 3.0으로 자동 하향하는 기능은 보안상 권장된다’이다. 자동 하향은 공격자가 더 약한 프로토콜을 선택하도록 유도하는 다운그레이드 공격의 위험을 키운다. 올바르게는 TLS 접속 실패 시 SSL 3.0으로 자동 하향하지 않고, SSL 3.0의 사용과 협상을 금지한 상태에서 양측이 지원하는 안전한 TLS 버전을 적절히 협상해야 한다.

NoteBase

오답 포인트

④의 '구형 시스템과의 호환성'은 편의성 측면에서는 그럴듯하지만, 보안 권장 사항을 뜻하지 않는다. 특히 하향 대상이 사용 금지된 SSL 3.0이므로 호환성을 이유로 자동 하향하는 판단은 성립하지 않는다.

다시 나오면 이렇게 판단

보안 프로토콜 문제에서는 먼저 해당 버전의 사용 가능 여부를 확인한다. 사용이 금지된 구형 버전이라면 호환성이나 접속 성공률을 이유로 한 자동 하향도 안전한 운용으로 볼 수 없다.

암기 포인트

SSL 3.0은 역사적 보안 목표는 있었지만 현재는 사용 금지이며, 자동 하향은 호환성 기능이 아니라 다운그레이드 위험이다.

NoteBase

문 3. IPSec의 전송 모드와 프로토콜에 관한 다음 설명 중 가장 옳지 않은 것은?

① ESP(Encapsulating Security Payload)를 사용하는 전송 모드(Transport mode)에서는 종단점 중 적어도 하나가 암호화 종단점이면 사용할 수 있다.

② 인증 헤더(Authenticated Header)를 사용하는 터널 모드(Tunnel mode)에서는 데이터의 기밀성을 보장하지 못한다.

③ AH는 IP 헤더의 변경 불가능한(immutable) 필드까지 포함하여 무결성 검사를 수행하므로, NAT 환경을 통과할 때 문제가 발생할 수 있다.

④ 전송 모드(Transport mode)에서는 원본 IP 헤더는 그대로 유지되고, IP 페이로드(상위 계층 데이터)만 보호된다.

정답 1번

출제 포인트

IPsec의 전송 모드와 터널 모드, 그리고 AH와 ESP가 제공하는 보안 기능의 차이를 묻는 문제이다.

핵심 개념

전송 모드는 통신 종단 간에 원본 IP 헤더를 유지하면서 그 뒤의 상위 계층 데이터를 주로 보호하는 방식이다.
이때 IPsec 보안 처리를 수행하는 종단은 통신 종단과 일치해야 한다.
터널 모드는 원본 IP 패킷 전체를 새 IP 패킷 안에 넣어 보호하므로 보안 게이트웨이 사이의 통신에도 사용할 수 있다.
AH는 출처 인증과 무결성 및 재전송 방지를 제공하지만 기밀성은 제공하지 않는다. ESP는 페이로드 암호화를 통한 기밀성을 제공하며 인증 기능도 선택적으로 제공할 수 있다.

선지별 해설

① X — 틀린 표현은 '종단점 중 적어도 하나가 암호화 종단점이면'이다. ESP 전송 모드는 IPsec 처리를 수행하는 보안 종단이 통신 종단과 일치하는 종단 간 보호에 사용하므로, 한쪽만 암호화 종단인 것으로는 충분하지 않다. 올바르게는 양쪽 통신 종단이 IPsec 보안 종단이어야 한다.
② O — AH는 인증과 무결성을 제공하지만 데이터를 암호화하지 않는다. 따라서 AH를 터널 모드로 사용하더라도 데이터의 기밀성은 보장하지 못한다.
③ O — AH의 무결성 검사는 전송 중 변하지 않아야 하는 IP 헤더 필드도 포함한다. NAT는 IP 주소 등 헤더 값을 변경하므로 수신 측의 무결성 검증이 실패할 수 있다.
④ O — 전송 모드에서는 원본 IP 헤더를 새 외부 헤더로 감싸지 않고 그대로 두며, 그 뒤의 IP 페이로드를 중심으로 보호한다. 이는 원본 IP 패킷 전체를 캡슐화하는 터널 모드와 구별된다.

NoteBase

오답 포인트

①의 '적어도 하나'가 함정이다. 전송 모드는 단순히 한쪽에 암호화 기능이 있으면 되는 방식이 아니라 통신 종단끼리 IPsec 처리를 수행하는 종단 간 방식이다. 또한 AH는 '인증'이라는 이름 때문에 암호화까지 제공한다고 착각하기 쉽지만, 기밀성은 ESP의 기능이다.

다시 나오면 이렇게 판단

먼저 모드를 구분한다. 원본 IP 헤더를 유지하고 종단 간에 보호하면 전송 모드이고, 원본 IP 패킷 전체를 새 IP 헤더로 감싸면 터널 모드이다. 다음으로 프로토콜을 구분한다. 기밀성이 필요하면 ESP이고, AH만으로는 기밀성을 제공하지 못한다. NAT가 제시되면 IP 헤더까지 무결성 검사에 포함하는 AH와의 충돌을 확인한다.

암기 포인트

전송 모드는 종단 간·원본 헤더 유지, 터널 모드는 패킷 전체 캡슐화, AH는 무결성만·ESP는 기밀성까지 제공한다.

NoteBase

문 4. 사이버 보안 모델에 관한 다음 설명 중 옳은 것을 모두 고른 것은?

ㄱ. Bell-LaPadula Model: 무결성 보호를 목적으로 하며, “No Read Down, No Write Up” 규칙을 따른다.
ㄴ. Biba Model: 기밀성 보호를 목적으로 하며, “No Read Up, No Write Down” 규칙을 따른다.
ㄷ. Clark-Wilson Model: 상업적 환경에서 무결성을 보장하기 위해 잘 정의된 트랜잭션과 직무 분리를 사용한다.
ㄹ. Chinese Wall Model: 이해 충돌(Conflict of Interest)을 방지하기 위해 경쟁사 정보 접근을 제한한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 4번

출제 포인트

대표적인 보안 모델이 보호하려는 속성과 각 모델의 핵심 규칙을 구별하는 문제이다. ㄷ과 ㄹ이 옳다.

핵심 개념

Bell-LaPadula 모델: 기밀성을 보호하며, 높은 등급의 정보를 낮은 등급으로 유출하지 않도록 ‘No Read Up, No Write Down’을 적용한다.
Biba 모델: 무결성을 보호하며, 낮은 무결성의 정보를 읽거나 높은 무결성의 대상을 오염시키는 것을 막는 ‘No Read Down, No Write Up’을 적용한다.
Clark-Wilson 모델: 상업적 환경의 무결성을 위해 잘 정의된 변환 절차와 직무 분리를 중시한다.
Chinese Wall 모델: 과거의 정보 접근 이력에 따라 경쟁 관계에 있는 조직의 정보 접근을 제한하여 이해 충돌을 방지한다.

NoteBase

선지별 해설

① X — ㄱ과 ㄴ이 모두 틀리다. ㄱ은 Bell-LaPadula의 목적과 규칙을 Biba의 것으로 바꾸어 썼고, ㄴ은 Biba의 목적과 규칙을 Bell-LaPadula의 것으로 바꾸어 썼다. 올바르게는 Bell-LaPadula가 기밀성과 'No Read Up, No Write Down', Biba가 무결성과 'No Read Down, No Write Up'을 담당한다.
② X — ㄷ은 옳지만 ㄱ이 틀리므로 옳은 것의 조합이 아니다. ㄱ의 '무결성'과 'No Read Down, No Write Up'은 Bell-LaPadula가 아니라 Biba의 특징이며, Bell-LaPadula는 기밀성을 보호한다.
③ X — ㄹ은 옳지만 ㄴ이 틀리므로 옳은 것의 조합이 아니다. ㄴ의 '기밀성'과 'No Read Up, No Write Down'은 Biba가 아니라 Bell-LaPadula의 특징이며, Biba는 무결성을 보호한다.
④ O — ㄷ과 ㄹ이 모두 옳다. Clark-Wilson은 잘 정의된 트랜잭션과 직무 분리로 상업적 무결성을 보장하고, Chinese Wall은 경쟁사 정보에 대한 접근을 제한하여 이해 충돌을 방지한다.

오답 포인트

ㄱ과 ㄴ은 두 모델의 보호 목적과 규칙을 통째로 맞바꾼 선지이다. 'Read Up'은 낮은 기밀 등급 주체가 높은 기밀 등급 정보를 읽는 것이므로 기밀성 모델인 Bell-LaPadula가 금지한다는 점이 핵심 함정이다.

다시 나오면 이렇게 판단

먼저 보호 속성을 연결한다. Bell-LaPadula는 기밀성, Biba와 Clark-Wilson은 무결성, Chinese Wall은 이해 충돌 방지이다. 그다음 Bell-LaPadula와 Biba의 읽기·쓰기 방향이 서로 반대임을 확인한다.

암기 포인트

Bell은 비밀, Biba는 무결성, Clark-Wilson은 거래·직무 분리, Chinese Wall은 경쟁사 간 정보 장벽이다.

NoteBase

문 5. 컴퓨터 보안 용어에 관한 다음 설명 중 가장 옳지 않은 것은?

① 공격자(Adversary): 공격하는 사람

② 위험(Risk): 특정 위협이 가져올 확률적으로 표현되는 예상되는 손실

③ 취약성(Vulnerability): 시스템 상의 오류나 약점

④ 위협(Threat): 시스템의 취약점을 악용하여 시도한 공격

정답 4번

출제 포인트

공격자, 위험, 취약성, 위협의 정의를 구분하고, 공격 가능성을 뜻하는 위협과 실제로 실행된 공격을 구별하는 문제이다.

핵심 개념

공격자(Adversary)는 시스템을 공격하는 주체이다.
위험(Risk)은 위협이 취약성을 악용하여 발생할 수 있는 손실의 가능성과 영향을 종합한 예상 손실이다.
취약성(Vulnerability)은 위협에 악용될 수 있는 시스템의 오류나 약점이다.
위협(Threat)은 취약성을 악용하여 피해를 일으킬 수 있는 잠재적 원인이나 가능성이고, 공격(Attack)은 그 위협을 실제 행동으로 옮긴 시도이다.

선지별 해설

① O — 공격자(Adversary)는 시스템을 공격하는 사람 등 공격의 주체를 뜻하므로 옳다.
② O — 위험(Risk)은 특정 위협이 현실화될 가능성과 그 결과로 발생할 손실을 반영한 예상 손실이므로 옳다.
③ O — 취약성(Vulnerability)은 위협이나 공격에 악용될 수 있는 시스템상의 오류 또는 약점이므로 옳다.
④ X — 틀린 표현은 '시도한 공격'이다. 이는 이미 행동으로 실행된 공격(Attack)을 설명한다. 위협(Threat)은 시스템의 취약성을 악용하여 피해를 일으킬 수 있는 잠재적 원인이나 가능성이라고 고쳐야 한다.

오답 포인트

④는 '취약점을 악용한다'는 공통 표현으로 위협과 공격을 혼동하게 한다. 아직 발생 가능한 상태이면 위협이고, 실제로 악용을 시도한 행위이면 공격이다.

다시 나오면 이렇게 판단

'약점'은 취약성, '피해를 일으킬 잠재적 가능성'은 위협, '실제로 실행한 시도'는 공격, '그로 인한 예상 손실'은 위험으로 구분한다.

NoteBase

암기 포인트

취약성은 약점, 위협은 가능성, 공격은 실행, 위험은 예상 손실이다.

NoteBase

문 6. 다음은 인터넷 웜의 고전적인 전파 모델에 관한 설명이다. 감염 속도 $dI(t)/dt$를 가장 올바르게 표현한 것은? (단, 감염된 컴퓨터는 치료되지 않는다고 가정한다)

$I(t)$: 시간 t동안 감염된 개체의 수
$S(t)$: 시간 t동안 감염에 민감한 개체의 수(취약하지만 아직 감염되지 않은 컴퓨터의 수)
b: 감염률
N: 총 컴퓨터의 수, $N = I(t) + S(t)$

① $bI(t)S(t)$

② $I(t)S(t)$

③ $bS(t)$

④ $I(t)S(t)/b$

정답 1번

출제 포인트

감염된 컴퓨터와 감염 가능성이 있는 컴퓨터의 접촉으로 새 감염이 발생할 때, 감염 속도를 결정하는 요인을 식으로 표현하는 문제이다.

조건 정리

$I(t)$는 감염된 컴퓨터 수, $S(t)$는 아직 감염되지 않은 취약한 컴퓨터 수, b는 감염률이다. 감염된 컴퓨터는 치료되지 않으므로 $I(t)$의 감소항은 없으며, 새 감염이 생길 가능성은 감염원과 취약 개체가 만나는 조합에 비례한다.

사용할 공식

감염 속도는 다음과 같다.
$\frac{dI(t)}{dt} = bI(t)S(t)$
감염원인 $I(t)$, 감염 대상인 $S(t)$, 접촉이 실제 감염으로 이어지는 정도인 b가 모두 있어야 새 감염의 발생 속도를 나타낼 수 있다.

NoteBase

선지별 해설

① O — $bI(t)S(t)$는 감염률, 감염된 컴퓨터 수, 취약한 컴퓨터 수를 모두 반영하므로 감염 속도를 올바르게 나타낸다.
② X — $I(t)S(t)$는 감염률 b를 누락한 식이다. 올바르게는 $bI(t)S(t)$이다.
③ X — $bS(t)$는 감염원인 $I(t)$를 누락한 식이어서 감염된 컴퓨터가 많을수록 접촉 기회가 증가한다는 점을 반영하지 못한다. 올바르게는 $bI(t)S(t)$이다.
④ X — $I(t)S(t)/b$는 감염률 b를 분모에 둔 점이 틀렸다. 감염률이 커질수록 감염 속도도 커져야 하므로 올바르게는 $bI(t)S(t)$이다.

오답 포인트

핵심 함정은 세 요소 중 하나를 빼거나 감염률을 역수로 처리하는 것이다. 특히 ④처럼 b를 분모에 두면 감염률이 높을수록 감염 속도가 낮아지는 모순이 생긴다.

다시 나오면 이렇게 판단

전파 속도식을 고를 때는 감염원 $I(t)$, 감염 대상 $S(t)$, 전파 가능성 b가 모두 곱해져 있는지 확인한다. 치료가 없다는 조건은 별도의 감소항이 없다는 뜻으로 판단한다.

암기 포인트

새 감염 속도는 감염률 × 감염자 수 × 취약자 수, 즉 bIS이다.

NoteBase

문 7. 침입 탐지 시스템(Intrusion Detection System)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 감사와 로깅할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않는다.

② NIDS는 네트워크를 통한 공격을 탐지하기 위한 장비다.

③ 네트워크를 통한 공격을 탐지할 뿐만 아니라 차단을 수행한다.

④ 설치 위치와 목적에 따라 HIDS와 NIDS로 나눌 수 있다.

정답 3번

출제 포인트

침입 탐지 시스템(IDS)의 탐지 기능과 침입 방지 시스템(IPS)의 차단 기능을 구분하는 문제이다.

핵심 개념

IDS는 시스템이나 네트워크의 활동을 감시하여 침입 징후를 탐지하고 기록·경보하는 보안 시스템이다. HIDS는 개별 호스트에서 발생하는 활동을 감시하고, NIDS는 네트워크 구간의 트래픽을 감시한다. IDS는 탐지가 중심이고, IPS는 공격 트래픽의 차단까지 수행하는 것이 중심이다.

선지별 해설

① O — IDS의 감사·로깅은 통신 내용을 수동적으로 관찰하고 기록하는 방식이므로, 그 과정에서 네트워크 자원을 없애거나 데이터를 변조하지 않는다.
② O — NIDS는 네트워크 구간을 지나는 패킷과 트래픽을 감시하여 네트워크를 통한 공격을 탐지한다.
③ X — 틀린 표현은 '탐지할 뿐만 아니라 차단을 수행한다'이다. 일반적인 IDS의 핵심 기능은 침입 탐지·기록·경보이며, 공격 트래픽을 능동적으로 차단하는 기능은 IPS의 핵심 기능이다.
④ O — IDS는 설치 위치와 감시 대상에 따라 호스트 기반 IDS(HIDS)와 네트워크 기반 IDS(NIDS)로 구분할 수 있다.

오답 포인트

③은 IDS와 IPS의 기능을 바꾸어 놓은 선지이다. IDS가 탐지 후 경보를 제공하는 것과 IPS가 트래픽 경로에서 공격을 차단하는 것을 혼동하면 틀리기 쉽다.

다시 나오면 이렇게 판단

선지에 '탐지·기록·경보'가 나오면 IDS의 기능으로, '능동적 차단·방지'가 나오면 IPS의 기능으로 판단한다. 설치 위치가 개별 호스트이면 HIDS, 네트워크 구간이면 NIDS로 구분한다.

암기 포인트

IDS는 탐지, IPS는 탐지 후 차단이다. HIDS는 호스트, NIDS는 네트워크를 감시한다.

NoteBase

문 8. 접근통제(Access Control) 모델에 관한 다음 설명 중 가장 옳은 것은?

① DAC(Discretionary Access Control)에서는 시스템 관리자가 모든 권한을 강제로 부여한다.

② MAC(Mandatory Access Control)에서는 객체의 소유자가 자신의 재량으로 권한을 부여한다.

③ RBAC(Role-based Access Control)은 사용자의 역할에 권한을 부여하고, 사용자는 역할을 통해 권한을 획득한다.

④ ABAC(Attribute-based Access Control)은 역할만을 기준으로 접근을 결정한다.

정답 3번

출제 포인트

접근 권한을 누가, 어떤 기준으로 부여하는지에 따라 DAC, MAC, RBAC, ABAC를 구분하는 문제이다.

핵심 개념

DAC는 객체의 소유자가 자신의 재량으로 접근 권한을 부여하는 방식이다.
MAC는 시스템이 보안 등급과 강제 정책에 따라 접근을 통제하는 방식이다.
RBAC은 역할에 권한을 연결하고 사용자에게 역할을 배정하는 방식이다.
ABAC은 사용자·객체·행위·환경 등의 속성과 정책을 조합하여 접근을 결정하는 방식이다.

선지별 해설

① X — '시스템 관리자가 모든 권한을 강제로 부여한다'는 부분이 틀렸다. DAC에서는 객체의 소유자가 자신의 재량으로 다른 사용자에게 접근 권한을 부여하거나 회수한다.
② X — '객체의 소유자가 자신의 재량으로 권한을 부여한다'는 부분이 틀렸다. 이는 DAC의 특징이며, MAC에서는 시스템의 강제 보안 정책과 보안 등급에 따라 접근 권한이 결정된다.
③ O — RBAC은 권한을 개별 사용자에게 직접 연결하지 않고 역할에 부여하며, 사용자는 자신에게 배정된 역할을 통해 그 권한을 획득한다.
④ X — '역할만을 기준으로'라는 부분이 틀렸다. 역할을 기준으로 하는 방식은 RBAC이며, ABAC은 사용자·객체·행위·환경 등 여러 속성을 정책과 함께 평가하여 접근을 결정한다.

오답 포인트

①과 ②는 DAC와 MAC의 권한 부여 주체를 서로 바꾸어 놓았고, ④는 ABAC의 '속성'을 RBAC의 '역할'로 바꾸어 놓았다.

다시 나오면 이렇게 판단

소유자의 재량이면 DAC, 시스템의 강제 정책과 보안 등급이면 MAC, 역할이면 RBAC, 여러 속성과 정책의 조합이면 ABAC으로 판단한다.

NoteBase

암기 포인트

DAC는 소유자 재량, MAC는 강제 정책, RBAC은 역할, ABAC은 속성이다.

문 9. 정보의 무결성(Integrity)을 검증하기 위해 사용되는 해시 함수(H)의 특성 중 '제2역상 저항성(Second Preimage Resistance)'의 의미에 관한 다음 설명 중 가장 옳은 것은?

① 해시값($y = H(x)$)이 주어져 있을 때, 그 해시값을 출력하는 입력값(x)을 찾기 어렵다.

② 입력값(x)이 주어져 있을 때, 그 입력과 같은 해시값($H(y) = H(x)$)을 출력하는 다른 입력값(y)을 찾기 어렵다.

③ 입력의 작은 변화가 해시값을 크게 바꾼다.

④ 같은 해시값($H(y) = H(x)$)을 출력하는 두 개의 다른 입력값($x, y, x \neq y$)을 찾기 어렵다.

정답 2번

출제 포인트

해시 함수의 제2역상 저항성을 역상 저항성, 눈사태 효과, 충돌 저항성과 구별하는 문제이다.

핵심 개념

역상 저항성: 해시값이 주어졌을 때 그 값을 만드는 입력을 찾기 어려운 성질이다.
제2역상 저항성: 특정 입력이 주어졌을 때 그 입력과 같은 해시값을 만드는 다른 입력을 찾기 어려운 성질이다.
충돌 저항성: 입력이 미리 정해지지 않은 상태에서 같은 해시값을 만드는 서로 다른 두 입력을 찾기 어려운 성질이다.
눈사태 효과: 입력이 조금만 달라져도 해시값이 크게 달라지는 성질이다.

NoteBase

선지별 해설

① X
틀린 부분은 해시값만 주어진 상태에서 그 해시값을 출력하는 입력값을 찾기 어렵다고 한 것이다. 이는 제2역상 저항성이 아니라 역상 저항성의 설명이다. 올바르게는 '해시값 y가 주어졌을 때 $H(x) = y$인 입력 x를 찾기 어렵다'이다.

② O
입력 x가 먼저 주어졌을 때 $H(y) = H(x)$를 만족하는 다른 입력 y를 찾기 어렵다는 설명은 제2역상 저항성의 정의와 일치한다. 여기서 $y \neq x$이다.

③ X
틀린 부분은 입력의 작은 변화가 해시값을 크게 바꾼다는 설명을 제2역상 저항성으로 본 것이다. 이는 눈사태 효과의 설명이다. 올바르게는 '주어진 입력과 같은 해시값을 갖는 다른 입력을 찾기 어렵다'이다.

④ X
틀린 부분은 서로 다른 두 입력을 모두 자유롭게 찾아 같은 해시값을 만들기 어렵다고 한 것이다. 이는 제2역상 저항성이 아니라 충돌 저항성의 설명이다. 올바르게는 '특정 입력 x가 주어졌을 때 $H(y) = H(x)$인 다른 입력 y를 찾기 어렵다'이다.

오답 포인트

①, ②, ④는 모두 같은 해시값을 다루지만 공격자에게 무엇이 먼저 주어지는지가 다르다. ①은 해시값만 주어지고, ②는 특정 입력이 주어지며, ④는 두 입력 모두 정해지지 않는다.

다시 나오면 이렇게 판단

문장에서 먼저 주어진 대상을 확인한다. 해시값이 주어지면 역상 저항성, 특정 입력이 주어지면 제2역상 저항성, 아무 입력도 정해지지 않은 채 서로 다른 두 입력을 찾으면 충돌 저항성이다.

암기 포인트

해시값→입력은 역상, 입력→같은 해시의 다른 입력은 제2역상, 서로 다른 두 입력을 함께 찾는 것은 충돌이다.

NoteBase

문 10. 대칭 암호화 구조에 관한 다음 설명 중 가장 옳지 않은 것은?

① 평문(plaintext): 암호화될 데이터이며, 암호화 알고리즘의 입력값이다.

② 암호화 알고리즘: 평문을 변화시켜 암호문을 만드는 알고리즘이다.

③ 복호화 알고리즘: 암호문을 평문으로 바꾸어주는 알고리즘이다.

④ 비밀 키: 암호화 키와 복호화 키는 반드시 다른 종류이어야 한다.

정답 4번

출제 포인트

대칭 암호화 구조를 이루는 평문, 암호화 알고리즘, 암호문, 복호화 알고리즘, 비밀 키의 역할과 대칭키 방식의 핵심 특징을 묻는 문제이다.

핵심 개념

대칭 암호는 암호화와 복호화에 같은 비밀 키를 사용하거나, 한 키로부터 다른 키를 쉽게 알아낼 수 있는 방식이다. 평문은 암호화 알고리즘에 입력되어 암호문으로 변환되고, 암호문은 복호화 알고리즘과 비밀 키를 통해 다시 평문으로 복원된다.

선지별 해설

① O — 평문은 암호화하기 전의 원래 데이터이며 암호화 알고리즘의 입력값이다.
② O — 암호화 알고리즘은 평문과 암호화 키를 이용해 암호문을 생성한다.
③ O — 복호화 알고리즘은 암호문과 복호화 키를 이용해 원래의 평문을 복원한다.
④ X — 틀린 표현은 '암호화 키와 복호화 키는 반드시 다른 종류이어야 한다'이다. 대칭 암호에서는 두 키가 같거나 한 키로부터 다른 키를 쉽게 알아낼 수 있으므로, 올바르게는 '암호화 키와 복호화 키는 동일하거나 서로 쉽게 유도할 수 있는 비밀 키이어야 한다'이다.

오답 포인트

④의 '반드시 다른 종류'는 공개키 암호의 특징과 혼동하게 만드는 표현이다. 대칭 암호의 대칭성은 암호화·복호화에 사용되는 키가 같거나 서로 쉽게 관련된다는 데 있다.

다시 나오면 이렇게 판단

암호화 키와 복호화 키의 관계를 먼저 확인한다. 같은 비밀 키를 공유하거나 두 키를 쉽게 유도할 수 있으면 대칭 암호이고, 서로 다른 공개키와 개인키를 사용하며 한 키에서 다른 키를 현실적으로 구하기 어려우면 공개키 암호이다.

NoteBase

암기 포인트

대칭 암호는 공유 비밀 키, 공개키 암호는 공개키와 개인키의 쌍이다.

NoteBase

문 11. <보기>와 같은 ASP 코드에 대해서, 다음 중 SQL Injection이 성공하는 user 입력이 아닌 것은?(단, DBMS는 Microsoft SQL Server를 기준으로 한다)

< 보 기 >

```
set ok = execute( "SELECT * FROM Users
    WHERE user=' "  &  form("user")  & "
  '
    AND   pwd=' " & form("pwd") & " '" );
if not ok.EOF
    login success
else  fail;
```

① ' or 1=1 --

② ' ; DROP TABLE Users --

③ ' ; exec xp_cmdshell 'net user badguy badpwd / ADD' --

④ ' pwd=1234 --

정답 4번

출제 포인트

사용자 입력을 문자열 연결 방식의 SQL문에 직접 넣었을 때 따옴표가 닫히는지, 뒤에 유효한 조건문이나 추가 명령이 이어지는지, 나머지 구문이 주석 처리되는지를 판단하는 문제이다.

사례 정리

ASP 코드는 user와 pwd 입력을 검증하거나 매개변수화하지 않고 SQL 문자열에 직접 연결한다. 따라서 user 입력의 작은따옴표로 기존 문자열을 닫은 뒤 SQL 구문을 삽입하고, --로 원래 쿼리의 나머지를 주석 처리할 수 있다.

핵심 개념

SQL Injection은 외부 입력이 SQL문의 데이터가 아니라 명령이나 조건식의 일부로 해석되도록 만드는 공격이다. 이 사례에서 공격이 성립하려면 작은따옴표 뒤에 문법적으로 유효한 조건식 또는 추가 명령이 와야 하고, --로 뒤의 원래 구문을 주석으로 처리해야 한다.

NoteBase

적용 기준

각 user 입력을 WHERE user='입력값' 위치에 그대로 대입해 완성된 SQL문의 문법을 확인한다. 아래 O는 문제에서 요구한 'SQL Injection이 성공하는 입력이 아님'에 해당함을, X는 성공하는 입력이어서 정답이 아님을 뜻한다.

선지별 해설

① X
' or 1=1 --는 기존 문자열을 닫고 항상 참인 OR 조건을 만든 뒤 나머지 비밀번호 조건을 주석 처리하므로 인증 우회형 SQL Injection이 성립한다. 이 선지를 실패하는 입력으로 보는 것은 틀리며, 올바르게는 '항상 참 조건을 삽입해 성공하는 입력'이다.

② X
' ; DROP TABLE Users --는 기존 문자열과 첫 SELECT문을 끝낸 다음 Users 테이블 삭제 명령을 추가하고 나머지를 주석 처리하는 중첩 질의형 입력이다. 이 선지를 실패하는 입력으로 보는 것은 틀리며, 올바르게는 '추가 SQL 명령을 실행시키는 입력'이다.

③ X
' ; exec xp_cmdshell 'net user badguy badpwd / ADD' --는 첫 문장을 끝낸 뒤 xp_cmdshell 실행문을 추가하는 형태이므로 SQL Injection 구문 자체는 성립한다. 실제 운영체제 명령 실행에는 xp_cmdshell의 활성화와 실행 권한이 필요하지만, 문제의 출제 전제에서는 성공하는 공격 입력이다. 이 선지를 실패하는 입력으로 보는 것은 틀리며, 올바르게는 '추가 저장 프로시저 실행을 시도하는 입력'이다.

④ O
' pwd=1234 --를 대입하면 user='' 다음에 연결 연산자 없이 pwd=1234가 바로 이어져 SQL 문법 오류가 발생한다. 따라서 SQL Injection이 성공하는 user 입력이 아니다. 성공 가능한 조건식으로 고치려면 예를 들어 ' or 1=1 --처럼 작은따옴표 뒤에 OR 등의 연산자와 완전한 조건식을 넣어야 한다.

오답 포인트

④에도 작은따옴표와 주석 기호가 있어 공격처럼 보이지만, 따옴표를 닫는 것만으로는 부족하다. user=''와 pwd=1234 사이를 연결할 OR, AND, 세미콜론 같은 문법 요소가 없다는 점이 함정이다.

다시 나오면 이렇게 판단

입력 문자열을 실제 쿼리에 대입한 뒤 '문자열 종료 → 유효한 조건식 또는 추가 명령 → 나머지 구문의 주석 처리'가 모두 이루어지는지 순서대로 확인한다. 세 요소 중 하나라도 빠져 SQL 문법이 깨지면 해당 입력은 성공하지 않는다.

암기 포인트

SQL Injection의 기본 구조는 ‘따옴표 닫기 + 유효한 SQL 삽입 + 뒤쪽 주석 처리’이다.

NoteBase

문 12. 다음 중 문제를 수론(number theory) 문제로 변환한 후 양자 컴퓨터를 사용하여 큰 정수를 효율적으로 인수분해하도록 설계된 알고리즘은?

① 그로버 알고리즘(Grover's Algorithm)

② 쇼어 알고리즘(Shor's Algorithm)

③ 야오 법칙(Yao's Principle)

④ 확장 유클리드 알고리즘(Extended Euclidean Algorithm)

정답 2번

출제 포인트

이 문제는 대표적인 양자 알고리즘과 고전 알고리즘이 각각 해결하는 문제를 구별하는 문제이다. 큰 정수의 인수분해를 효율적으로 수행하는 양자 알고리즘은 쇼어 알고리즘이다.

핵심 개념

쇼어 알고리즘은 정수 인수분해를 위수·주기 찾기 문제로 바꾸고 양자 계산을 이용해 주기를 구하는 알고리즘이다. 큰 정수의 인수분해와 이산로그 문제를 다항 시간에 해결할 수 있어 RSA와 같은 공개키 암호에 위협이 된다.
그로버 알고리즘은 구조가 없는 탐색 공간에서 원하는 항목을 제곱근 수준의 질의 횟수로 찾는다. 야오 원리는 확률적 알고리즘의 성능 하한을 분석하는 원리이고, 확장 유클리드 알고리즘은 최대공약수와 베주 계수를 구해 모듈러 역원을 계산하는 데 쓰인다.

선지별 해설

① X — 그로버 알고리즘이라는 선택이 틀렸다. 그로버 알고리즘은 비정렬·비구조화된 탐색을 약 제곱근 수준으로 가속하는 양자 탐색 알고리즘이며, 큰 정수의 효율적 인수분해 알고리즘은 쇼어 알고리즘이다.
② O — 쇼어 알고리즘은 인수분해 문제를 위수·주기 찾기 문제로 환원하고 양자 푸리에 변환 등을 이용해 큰 정수의 인수분해를 효율적으로 수행하도록 설계되었다.
③ X — 야오 법칙이라는 선택이 틀렸다. 야오 원리는 확률적 알고리즘과 입력 분포에 대한 결정적 알고리즘을 연결하여 계산 복잡도의 하한을 분석하는 원리이며, 정수 인수분해용 양자 알고리즘은 쇼어 알고리즘이다.
④ X — 확장 유클리드 알고리즘이라는 선택이 틀렸다. 확장 유클리드 알고리즘은 두 정수의 최대공약수와 베주 계수를 구하고 모듈러 역원을 계산하는 고전 알고리즘이며, 큰 정수의 인수분해를 양자적으로 가속하는 알고리즘은 쇼어 알고리즘이다.

NoteBase

오답 포인트

그로버 알고리즘도 대표적인 양자 알고리즘이라는 점 때문에 ①과 혼동하기 쉽다. 그러나 '큰 정수의 인수분해'는 쇼어, '구조 없는 탐색'은 그로버로 구분한다. 확장 유클리드 알고리즘은 RSA 계산 과정에서 모듈러 역원을 구할 때 활용될 수 있지만 인수분해 알고리즘은 아니다.

다시 나오면 이렇게 판단

문제의 핵심 작업을 먼저 확인한다. 인수분해·이산로그이면 쇼어 알고리즘, 비구조화 탐색이면 그로버 알고리즘, 최대공약수·모듈러 역원이면 확장 유클리드 알고리즘으로 판단한다.

암기 포인트

인수분해는 쇼어, 탐색은 그로버, 역원은 확장 유클리드이다.

NoteBase

문 13. 이상 탐지 기반 IDS와 시그니처 기반 IDS의 비교에 관한 다음 설명 중 가장 옳지 않은 것은?

① 시그니처 기반 IDS는 알려진 공격 패턴 DB와 일치하는 트래픽을 탐지한다.

② 이상 탐지 기반 IDS는 정상 행위의 기준선을 학습한 후 이를 벗어난 경우를 탐지한다.

③ 시그니처 기반 IDS는 제로데이 공격(미지의 공격) 탐지에 강점이 있다.

④ 이상 탐지 기반 IDS는 오탐(False Positive) 비율이 상대적으로 높다.

정답 3번

출제 포인트

이 문제는 시그니처 기반 IDS와 이상 탐지 기반 IDS의 탐지 기준, 미지 공격 탐지 가능성, 오탐 특성을 구별하는 문제이다.

핵심 개념

시그니처 기반 IDS: 알려진 공격의 특징이나 패턴을 시그니처 DB에 저장하고, 관찰한 트래픽이 그 패턴과 일치하는지를 검사하는 침입 탐지 방식이다. 알려진 공격에는 효과적이지만 시그니처가 없는 새로운 공격에는 취약하다.
이상 탐지 기반 IDS: 정상 행위의 기준선을 학습하거나 설정하고, 그 기준에서 벗어난 행위를 침입 가능성이 있는 것으로 탐지하는 방식이다. 미지의 공격도 탐지할 수 있지만 정상적인 변화까지 공격으로 판단하여 오탐이 늘어날 수 있다.
결정적인 구분은 시그니처 기반은 '알려진 공격 패턴과의 일치'를, 이상 탐지 기반은 '정상 기준선에서의 이탈'을 판단 기준으로 삼는다는 점이다.

선지별 해설

① O — 시그니처 기반 IDS는 트래픽의 특징을 알려진 공격 패턴 DB와 대조하여 일치하는 공격을 탐지한다.
② O — 이상 탐지 기반 IDS는 정상 행위의 기준선을 마련한 뒤, 이 기준을 벗어나는 비정상 행위를 탐지한다.
③ X — 틀린 표현은 '제로데이 공격(미지의 공격) 탐지에 강점이 있다'이다. 시그니처 기반 IDS는 등록된 공격 패턴이 없는 제로데이 공격을 탐지하기 어렵다. 올바르게는 이상 탐지 기반 IDS가 정상 기준선에서 벗어나는 행위를 찾아 미지의 공격 탐지에 상대적으로 강점이 있다고 해야 한다.
④ O — 이상 탐지 기반 IDS는 정상 행위의 변동도 이상으로 판단할 수 있으므로 시그니처 기반 IDS보다 오탐 비율이 상대적으로 높을 수 있다.

오답 포인트

③은 두 방식의 장점을 서로 바꾸어 놓았다. '제로데이·미지 공격'은 기존 시그니처가 없으므로 패턴 일치 방식의 강점이 아니라 정상 기준선 이탈을 보는 이상 탐지 방식의 상대적 강점이다.

NoteBase

다시 나오면 이렇게 판단

선지에서 '알려진 공격·패턴 DB·정확한 매칭'이 나오면 시그니처 기반으로, '정상 기준선·이탈·미지 공격·높은 오탐'이 나오면 이상 탐지 기반으로 판단한다.

암기 포인트

시그니처는 아는 공격을 잘 찾고, 이상 탐지는 모르는 공격도 찾지만 오탐이 많다.

NoteBase

문 14. 방화벽 유형에 관한 다음 설명 중 가장 옳은 것은?

① 패킷 필터링 방화벽(Packet Filtering Firewall)은 응용 계층 데이터까지 검사하므로 성능 오버헤드가 크다.

② 상태 기반 검사 방화벽(Stateful Inspection Firewall)은 연결 상태 테이블을 유지하여 트래픽 흐름을 동적으로 추적한다.

③ 애플리케이션 레벨 게이트웨이(Application-level Gateway)는 IP 헤더만 검사하고 응용 데이터는 검사하지 않는다.

④ 회선 레벨 게이트웨이(Circuit-level Gateway)는 각 패킷의 내용을 상세히 분석한다.

정답 2번

출제 포인트

방화벽 유형별로 검사하는 정보와 연결 상태 추적 여부를 구분하는 문제이다.

핵심 개념

패킷 필터링 방화벽은 주로 네트워크·전송 계층의 헤더 정보를 규칙과 대조하여 패킷의 통과 여부를 결정한다. 상태 기반 검사 방화벽은 연결 상태 테이블을 유지하면서 현재 패킷이 정상적인 세션 흐름에 속하는지 판단한다. 애플리케이션 레벨 게이트웨이는 응용 프로그램의 프록시로 동작하며 응용 계층의 명령과 데이터를 검사한다. 회선 레벨 게이트웨이는 세션이나 회선의 설정이 적절한지를 확인한 뒤 트래픽을 중계하며, 각 패킷의 응용 내용을 상세히 분석하지는 않는다.

선지별 해설

① X — 틀린 표현은 '응용 계층 데이터까지 검사하므로 성능 오버헤드가 크다'이다. 패킷 필터링 방화벽은 주로 출발지·목적지 IP 주소, 포트 번호, 프로토콜 같은 헤더 정보를 검사하므로 비교적 처리가 빠르고 오버헤드가 작다.
② O — 상태 기반 검사 방화벽은 연결 상태 테이블을 유지하고 패킷이 기존 연결의 정상적인 흐름에 속하는지를 동적으로 추적한다.
③ X — 틀린 표현은 'IP 헤더만 검사하고 응용 데이터는 검사하지 않는다'이다. 애플리케이션 레벨 게이트웨이는 응용 프로그램별 프록시로 동작하면서 응용 계층의 명령과 데이터를 검사한다.
④ X — 틀린 표현은 '각 패킷의 내용을 상세히 분석한다'이다. 회선 레벨 게이트웨이는 세션 설정과 연결 상태를 확인하여 트래픽을 중계하며, 각 패킷의 응용 내용을 상세히 검사하는 방식은 아니다.

오답 포인트

①과 ③은 패킷 필터링과 애플리케이션 레벨 게이트웨이의 검사 범위를 서로 뒤바꾼 선지이다. ④는 연결 자체를 확인하는 회선 레벨 게이트웨이에 패킷 내용 분석 기능을 잘못 붙였다.

NoteBase

다시 나오면 이렇게 판단

선지에서 무엇을 검사하는지 먼저 확인한다. IP 주소·포트 등 헤더이면 패킷 필터링, 연결 상태 테이블이면 상태 기반 검사, 응용 데이터이면 애플리케이션 레벨 게이트웨이, 세션·회선 설정이면 회선 레벨 게이트웨이로 판단한다.

암기 포인트

패킷 필터링은 헤더, 상태 기반 검사는 상태 테이블, 애플리케이션 게이트웨이는 응용 데이터, 회선 게이트웨이는 세션 연결을 본다.

NoteBase

문 15. SSH 프로토콜 구조에 관한 다음 설명 중 가장 옳지 않은 것은?

① SSH 사용자 인증 프로토콜은 클라이언트 사용자의 인증과 서버 호스트 키 검증을 담당하며, 서버 인증은 사용자 인증 단계에서 수행된다.

② SSH 사용자 인증 프로토콜은 전송 계층 위에서 동작하며 공개키, 패스워드, 호스트 기반 인증 등의 방법을 포함할 수 있다.

③ SSH 연결 프로토콜은 암호화된 터널 위에서 여러 논리 채널을 다중화하는 기능을 제공한다.

④ SSH 전송 계층 프로토콜은 일반적으로 TCP/IP 위에서 동작하며 서버 인증, 기밀성, 무결성을 제공한다.

정답 1번

출제 포인트

SSH를 구성하는 전송 계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜의 역할을 구별하는 문제이다.

핵심 개념

SSH 전송 계층 프로토콜은 서버 인증과 통신의 기밀성·무결성을 제공하는 기반 계층이다.
SSH 사용자 인증 프로토콜은 전송 계층 위에서 클라이언트 사용자의 신원을 서버에 인증한다.
SSH 연결 프로토콜은 인증된 암호화 연결 위에서 여러 논리 채널을 다중화한다.
핵심 구분은 '서버 호스트 인증은 전송 계층, 사용자 인증은 사용자 인증 프로토콜, 채널 다중화는 연결 프로토콜'이다.

선지별 해설

① X — 틀린 표현은 '서버 호스트 키 검증을 담당하며, 서버 인증은 사용자 인증 단계에서 수행된다'이다. 서버 인증은 SSH 전송 계층의 키 교환 과정에서 서버 호스트 키를 이용해 수행된다. 사용자 인증 프로토콜은 그 뒤 클라이언트 사용자를 서버에 인증한다.
② O — 사용자 인증 프로토콜은 SSH 전송 계층 위에서 동작하며 공개키 인증, 패스워드 인증, 호스트 기반 인증 등의 방법을 사용할 수 있다.
③ O — 연결 프로토콜은 보호된 SSH 연결 하나에서 셸 세션, 포트 포워딩 등에 쓰이는 여러 논리 채널을 다중화한다.
④ O — 전송 계층 프로토콜은 일반적으로 TCP/IP 위에서 동작하며 서버 인증, 기밀성, 무결성을 제공한다.

오답 포인트

①은 '사용자 인증'이라는 이름 때문에 서버와 사용자에 관한 모든 인증을 이 계층이 담당한다고 착각하게 만든다. 그러나 서버 호스트 인증과 클라이언트 사용자 인증은 서로 다른 단계와 프로토콜의 역할이다.

NoteBase

다시 나오면 이렇게 판단

인증 대상을 먼저 본다. 서버의 호스트 키를 확인하면 전송 계층, 클라이언트 사용자의 신원을 확인하면 사용자 인증 프로토콜, 여러 세션과 포워딩 채널을 나누면 연결 프로토콜로 판단한다.

암기 포인트

전송은 서버·보안, 사용자 인증은 클라이언트 사용자, 연결은 채널 다중화이다.

NoteBase

문 16. 다음 중 능동적 공격(active attack)에 해당하지 않는 것은?

① 위장

② 가장

③ 메시지 위조

④ 트래픽 분석

정답 4번

출제 포인트

이 문제는 시스템이나 데이터에 변화를 일으키는 능동적 공격과 정보를 몰래 관찰하는 수동적 공격을 구별하는 문제이다.

핵심 개념

능동적 공격: 공격자가 신분이나 메시지를 조작하거나 시스템의 정상 동작을 방해하는 공격이다. 키워드는 변조·위조·개입이다.
수동적 공격: 통신 내용을 엿보거나 트래픽의 양·빈도·흐름을 관찰하여 정보를 얻는 공격이다. 키워드는 도청·관찰·분석이다.

선지별 해설

① X(정답 조건 불충족) — 위장은 공격자가 신원이나 통신 주체를 속여 정상 개체처럼 행동하는 능동적 공격이다. '능동적 공격에 해당하지 않는다'가 아니라 '능동적 공격에 해당한다'가 올바른 분류이다.
② X(정답 조건 불충족) — 가장은 공격자가 정당한 사용자나 시스템인 것처럼 행세하여 통신에 개입하는 능동적 공격이다. '능동적 공격에 해당하지 않는다'가 아니라 '능동적 공격에 해당한다'가 올바른 분류이다.
③ X(정답 조건 불충족) — 메시지 위조는 거짓 메시지를 만들거나 메시지 내용을 조작하여 데이터의 무결성에 영향을 주므로 능동적 공격이다. '능동적 공격에 해당하지 않는다'가 아니라 '능동적 공격에 해당한다'가 올바른 분류이다.
④ O — 트래픽 분석은 메시지 내용을 직접 바꾸지 않고 통신량, 빈도, 시점, 송수신 관계 등을 관찰해 정보를 추론하는 수동적 공격이다. 따라서 능동적 공격에 해당하지 않는다.

오답 포인트

'공격'이라는 말 때문에 트래픽 분석도 능동적 공격으로 보기 쉽다. 그러나 구분 기준은 공격성이 아니라 데이터나 시스템에 직접 변화를 가하는지 여부이다. 트래픽 분석은 관찰만 하므로 수동적 공격이다.

NoteBase

다시 나오면 이렇게 판단

신분·메시지·서비스를 조작하거나 방해하면 능동적 공격, 통신을 변경하지 않고 엿보거나 흐름을 분석하면 수동적 공격으로 판단한다.

암기 포인트

조작·방해는 능동, 도청·트래픽 분석은 수동이다.

NoteBase

문 17. DoS 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

① SIP Flood 공격은 IRC에 관한 공격 중 하나이다.

② Reflection 공격을 하려면 패킷 내 소스 IP 주소를 위조해야 한다.

③ Reflection 공격을 이용하면 DNS 서비스에 대한 DoS 공격이 가능하다.

④ DoS 공격은 가용성(Availability)을 떨어뜨리는 공격이다.

정답 1번

출제 포인트

DoS 공격의 유형인 SIP Flood와 Reflection 공격의 동작 원리, 그리고 DoS가 침해하는 보안 속성을 구분하는 문제이다.

핵심 개념

SIP Flood: 인터넷 전화 등에서 세션을 설정·관리하는 SIP에 다량의 요청을 보내 서비스 자원을 고갈시키는 공격이다.
Reflection 공격: 공격자가 피해자의 IP 주소로 출발지 주소를 위조해 여러 서버에 요청을 보내고, 서버의 응답이 피해자에게 향하도록 하는 반사형 DoS 공격이다.
DoS: 정상 사용자가 시스템이나 네트워크 서비스를 이용하지 못하게 하여 가용성을 침해하는 공격이다.

선지별 해설

① X — 틀린 표현은 'IRC에 관한 공격'이다. SIP Flood는 IRC 공격이 아니라 SIP를 사용하는 인터넷 전화·멀티미디어 통신 서비스에 다량의 SIP 요청을 보내는 공격이다.
② O — Reflection 공격에서는 요청 패킷의 소스 IP 주소를 피해자의 IP 주소로 위조한다. 그러면 요청을 받은 반사 서버의 응답이 공격자가 아니라 피해자에게 전달된다.
③ O — 공격자는 피해자의 IP 주소로 위조한 DNS 질의를 DNS 서버에 보내 응답이 피해자에게 집중되도록 할 수 있으므로 DNS 서비스를 반사 서버로 이용한 DoS 공격이 가능하다.
④ O — DoS 공격은 시스템이나 네트워크 자원을 고갈시켜 정상 사용자의 서비스 이용을 방해하므로 정보보호의 가용성을 떨어뜨린다.

오답 포인트

①의 'SIP'를 채팅 관련 프로토콜로 오인하면 IRC 공격으로 잘못 연결하기 쉽다. SIP는 인터넷 전화 등의 세션 설정 프로토콜이고, IRC는 인터넷 채팅 프로토콜이므로 서로 다른 서비스이다.

NoteBase

다시 나오면 이렇게 판단

공격명에 포함된 프로토콜이 어떤 서비스에 쓰이는지 먼저 확인한다. Reflection은 '피해자 IP로 출발지 위조 → 반사 서버에 요청 → 응답이 피해자에게 집중'의 흐름으로 판단하고, 서비스 이용을 막는 공격은 가용성 침해로 분류한다.

암기 포인트

SIP는 인터넷 전화 세션, IRC는 채팅, Reflection은 소스 IP 위조와 응답 반사, DoS는 가용성 침해이다.

NoteBase

문 18. 다음 중 크로스사이트 스크립팅(XSS) 공격의 근본적인 원인으로 가장 옳은 것은?

① 취약한 암호화 알고리즘 사용

② 세션 타임아웃 미설정

③ 잘못된 접근통제 설정

④ 사용자 입력값의 불충분한 검증·이스케이핑

정답 4번

출제 포인트

XSS는 신뢰할 수 없는 사용자 입력이 웹 페이지의 실행 가능한 코드로 해석되면서 발생한다는 점을 묻는 문제이다.

핵심 개념

크로스사이트 스크립팅(XSS)은 공격자가 넣은 스크립트가 다른 사용자의 브라우저에서 실행되는 웹 취약점이다. 핵심 원인은 사용자 입력을 출력 위치의 문맥에 맞게 이스케이핑하지 않거나, 위험한 입력을 적절히 검증·정제하지 않은 채 페이지에 포함하는 것이다.

선지별 해설

① X — '취약한 암호화 알고리즘 사용'은 암호문의 기밀성이나 무결성을 약화하는 원인이지 XSS의 근본 원인이 아니다. 올바르게는 사용자 입력을 웹 페이지에 반영할 때 문맥에 맞는 출력 이스케이핑과 필요한 검증·정제를 하지 않는 것이 XSS의 원인이다.

② X — '세션 타임아웃 미설정'은 세션이 불필요하게 오래 유지되는 세션 관리 문제이지 XSS를 발생시키는 원인이 아니다. 올바르게는 적절한 세션 만료 시간을 설정하는 것이 세션 관리 대책이며, XSS 방지는 신뢰할 수 없는 데이터의 안전한 처리와 출력 이스케이핑이 핵심이다.

③ X — '잘못된 접근통제 설정'은 권한이 없는 사용자가 자원이나 기능에 접근하게 되는 인가 문제이지 XSS의 근본 원인이 아니다. 올바르게는 자원별 권한을 서버에서 검사하는 것이 접근통제 대책이며, XSS는 입력값이 실행 가능한 스크립트로 해석되지 않도록 처리해야 예방할 수 있다.

④ O — 사용자 입력값을 충분히 검증·정제하지 않고 출력 문맥에 맞게 이스케이핑하지 않으면 입력된 스크립트가 브라우저에서 코드로 실행될 수 있으므로 XSS의 근본 원인에 해당한다.

오답 포인트

XSS 공격으로 세션 정보가 탈취될 수 있다는 결과 때문에 ②를 고르기 쉽다. 그러나 공격의 결과와 발생 원인은 다르다. 세션 탈취는 가능한 피해이고, 사용자 입력이 코드로 해석되게 만든 불충분한 검증·정제 및 출력 이스케이핑이 발생 원인이다.

NoteBase

다시 나오면 이렇게 판단

웹 공격의 원인을 묻는 경우 데이터가 어떤 경계를 넘어 어떻게 해석되는지를 확인한다. 신뢰할 수 없는 입력이 HTML이나 자바스크립트 문맥에서 코드로 해석되면 XSS이고, 권한 검사 실패는 접근통제 문제이며, 세션 만료 설정 실패는 세션 관리 문제이다.

암기 포인트

XSS는 '사용자 입력이 브라우저에서 코드로 실행됨'이며, 핵심 방어는 출력 문맥별 이스케이핑과 필요한 검증·정제이다.

NoteBase

문 19. 다음 중 HTTPS가 HTTP와 비교하여 추가로 제공하는 핵심 기능으로 가장 옳은 것은?

① 더 빠른 데이터 전송 속도

② 전송 계층의 암호화 및 서버 인증

③ IP 주소 은닉

④ 바이러스 침투 방지

정답 2번

출제 포인트

이 문제는 HTTPS가 일반 HTTP에 TLS를 적용함으로써 추가로 제공하는 보안 기능을 묻는다.

핵심 개념

HTTP는 웹에서 요청과 응답을 주고받는 통신 규약이지만, 그 자체로 전송 내용을 암호화하거나 서버의 신원을 인증하지 않는다.
HTTPS는 HTTP 통신에 TLS를 적용하여 통신 내용을 암호화하고, 인증서를 통해 접속한 서버의 신원을 확인하며, 전송 중 데이터 변조 여부도 검증한다. 핵심 키워드는 기밀성, 서버 인증, 무결성이다.

선지별 해설

① X — 틀린 표현은 '더 빠른 데이터 전송 속도'이다. HTTPS의 핵심 목적은 속도 향상이 아니라 통신 보호이며, 암호화와 인증 처리 때문에 HTTPS가 언제나 HTTP보다 빠르다고 할 수 없다. 올바르게는 'HTTPS는 HTTP 통신에 암호화와 인증 기능을 추가한다'이다.
② O — HTTPS는 TLS를 이용해 클라이언트와 서버 사이의 전송 내용을 암호화하고, 서버 인증서를 검증하여 접속 대상 서버의 신원을 확인한다. HTTP와 비교했을 때 추가되는 대표적인 핵심 보안 기능이다.
③ X — 틀린 표현은 'IP 주소 은닉'이다. HTTPS는 주로 HTTP 메시지의 내용을 암호화하지만, 패킷 전달에 필요한 목적지 IP 주소 자체를 숨기지는 않는다. IP 주소 은닉에는 VPN이나 프록시 같은 별도의 기술이 필요하다.
④ X — 틀린 표현은 '바이러스 침투 방지'이다. HTTPS는 통신 구간을 암호화하고 상대 서버를 인증하는 기술이지 악성코드를 탐지·차단하는 백신 기능이 아니다. 올바르게는 백신, 보안 프로그램, 콘텐츠 검사 체계 등이 악성코드 방지 역할을 담당한다.

오답 포인트

HTTPS의 자물쇠 표시를 모든 보안 문제를 해결한다는 뜻으로 확대 해석하기 쉽다. HTTPS는 통신 구간의 기밀성·무결성과 서버 인증을 제공하지만, IP 주소를 숨기거나 악성코드 감염을 자동으로 막는 기술은 아니다.

NoteBase

다시 나오면 이렇게 판단

HTTP와 HTTPS의 차이를 묻는 문항에서는 TLS가 추가하는 기능인지 확인한다. '암호화·인증서·무결성'은 HTTPS의 기능이고, '속도 보장·IP 은닉·바이러스 차단'은 별도 기술의 영역이다.

암기 포인트

HTTPS는 HTTP에 TLS를 더한 것으로, 핵심은 암호화·서버 인증·무결성이다.

NoteBase

문 20. 다음 중 사용자 인증의 수단(factor)으로 가장 옳지 않은 것은?

① 지식 기반: Something you know (예: 비밀번호, PIN)

② 소유 기반: Something you have (예: 스마트카드, 토큰)

③ 생체 기반: Something you are (예: 지문, 홍채)

④ 신뢰 기반: Something you trust (예: 인증기관)

정답 4번

출제 포인트

사용자 인증요소를 지식·소유·생체 기반으로 구분하고, 인증 기반의 신뢰 주체와 인증요소를 구별하는 문제이다.

핵심 개념

인증요소는 사용자가 자신의 신원을 증명하기 위해 제시하는 서로 다른 종류의 증거이다. 지식 기반은 사용자가 아는 것, 소유 기반은 사용자가 가진 것, 생체 기반은 사용자 자신에게 고유한 신체적 특성을 이용한다.
인증기관은 공개키 인증서를 발급·검증하는 신뢰 주체이지 사용자에게 속한 독립적인 인증요소가 아니다.

선지별 해설

① O — 비밀번호와 PIN은 사용자가 기억하고 있는 정보이므로 지식 기반(Something you know) 인증요소이다.
② O — 스마트카드와 토큰은 사용자가 실제로 소지한 매체이므로 소유 기반(Something you have) 인증요소이다.
③ O — 지문과 홍채는 사용자에게 고유한 신체적 특징이므로 생체 기반(Something you are) 인증요소이다.
④ X — 틀린 표현은 '신뢰 기반: Something you trust'를 사용자 인증요소로 분류하고 인증기관을 그 예로 든 부분이다. 올바르게는 인증기관은 인증서의 발급과 검증을 담당하는 신뢰 주체이며, 대표적인 사용자 인증요소는 지식·소유·생체 기반이다.

오답 포인트

'인증기관'에도 인증이라는 말이 들어가므로 인증요소처럼 보이지만, 인증기관은 사용자가 제시하는 증거가 아니라 공개키 기반구조에서 신뢰를 제공하는 제3자이다.

다시 나오면 이렇게 판단

선지의 대상을 사용자가 아는 정보, 사용자가 가진 물건, 사용자 자신의 신체적 특성 가운데 하나로 분류한다. 여기에 해당하지 않고 인증서를 발급하거나 신뢰관계를 보증하는 주체라면 사용자 인증요소와 구별한다.

NoteBase

암기 포인트

안다(Know)·가진다(Have)·그 자체이다(Are)는 인증요소이고, 인증기관은 신뢰 주체이다.

NoteBase

문 21. 비밀번호를 공격하는 방법에 관한 다음 설명 중 가장 옳은 것은?

① 오프라인 사전 공격은 암호화된 시스템 비밀번호 파일이 필요없다.

② 특정 계정 공격은 오프라인으로만 가능하다.

③ 잘 알려진 비밀번호를 공격하는 방법을 막기 위해서는 짧은 패스워드를 못 쓰게만 하면 된다.

④ 레인보우 테이블을 이용한 공격은 메모리가 충분할 때 효율적이다.

정답 4번

출제 포인트

이 문제는 비밀번호 공격 방식별로 필요한 정보, 공격 경로, 대응 방법, 시간-메모리 절충 관계를 구분하는 문제이다.

핵심 개념

오프라인 사전 공격: 탈취한 비밀번호 해시 등의 검증값을 대상으로 사전의 후보 비밀번호를 대입하여 일치 여부를 확인하는 공격이다.
특정 계정 공격: 하나의 특정 계정을 목표로 비밀번호 후보를 반복 대입하는 방식이며 온라인과 오프라인 모두 가능하다.
잘 알려진 비밀번호 공격: 흔히 쓰이는 비밀번호를 우선 대입하는 공격으로, 길이 제한뿐 아니라 흔한 비밀번호 차단과 시도 횟수 제한 같은 대응이 필요하다.
레인보우 테이블 공격: 미리 계산한 해시값과 후보 비밀번호의 대응 관계를 저장해 두고 조회하여 비밀번호를 찾는 시간-메모리 절충 공격이다.

선지별 해설

① X — 틀린 표현은 '암호화된 시스템 비밀번호 파일이 필요없다'이다. 오프라인 사전 공격은 공격자가 시스템과 통신하지 않고 후보를 검증해야 하므로 탈취한 비밀번호 해시 파일과 같은 검증 정보가 필요하다. 올바르게는 '오프라인 사전 공격에는 탈취한 비밀번호 해시 등의 검증 정보가 필요하다'이다.
② X — 틀린 표현은 '오프라인으로만 가능하다'이다. 특정 계정 공격은 목표 계정 하나를 정한 공격 대상의 구분이며, 로그인 화면에서 시도하는 온라인 공격과 탈취한 해시를 이용하는 오프라인 공격 모두 가능하다. 올바르게는 '특정 계정 공격은 온라인과 오프라인 모두 가능하다'이다.
③ X — 틀린 표현은 '짧은 패스워드를 못 쓰게만 하면 된다'이다. 최소 길이를 늘리는 것만으로는 길지만 흔한 비밀번호의 사용을 막지 못한다. 올바르게는 '충분한 길이를 요구하는 동시에 흔하거나 유출된 비밀번호를 차단하고, 온라인 공격에는 시도 횟수 제한이나 다중 인증 등을 함께 적용한다'이다.
④ O — 레인보우 테이블은 후보별 해시 계산 결과를 미리 저장해 두어 공격 시 계산 시간을 줄이는 방식이다. 충분한 메모리나 저장 공간이 있으면 큰 테이블을 보관하고 빠르게 조회할 수 있으므로 효율적이다.

NoteBase

오답 포인트

①은 '오프라인'이라는 말 때문에 비밀번호 파일도 필요 없다고 착각하게 하고, ②는 공격 대상인 '특정 계정'과 공격 경로인 '온라인·오프라인'을 혼동하게 한다. ③의 '~만 하면 된다'는 단일 대책을 충분조건처럼 제시한 표현이다. ④는 레인보우 테이블의 핵심인 계산 시간과 저장 공간의 교환 관계를 정확히 설명한다.

다시 나오면 이렇게 판단

공격 대상을 나타내는 말과 공격 경로를 나타내는 말을 분리해 판단한다. 오프라인 공격은 탈취한 검증 정보가 필요하고, 레인보우 테이블은 사전 계산 결과를 저장하여 공격 시 계산 시간을 줄이므로 저장 공간이 충분할수록 유리하다. '~만 하면 된다'는 표현은 다른 필수 대응이 없는지도 함께 확인한다.

암기 포인트

오프라인은 해시 필요, 특정 계정은 온·오프라인 모두 가능, 레인보우 테이블은 시간 대신 메모리를 쓴다.

NoteBase

문 22. 다음 중 주요 서비스의 기본 포트번호로 옳지 않은 것은?

① SMTP: 21

② SSH: 22

③ remote desktop: 3389

④ HTTPS: 443

정답 1번

출제 포인트

주요 네트워크 서비스와 기본 포트번호의 연결을 구별하는 문제이다.

핵심 개념

포트번호는 전송 계층에서 응용 서비스를 구분하는 번호이다. 대표적인 기본 포트는 FTP 제어 연결 21, SSH 22, SMTP 25, HTTPS 443, 원격 데스크톱 프로토콜(RDP) 3389이다.

선지별 해설

① X — ‘SMTP: 21’이 틀린 표현이다. SMTP의 기본 포트는 25이고, 21은 FTP의 제어 연결에 사용하는 기본 포트이다.
② O — SSH의 기본 포트는 22이다. SSH는 원격 시스템에 암호화된 접속을 제공한다.
③ O — 원격 데스크톱 프로토콜(RDP)의 기본 포트는 3389이다.
④ O — HTTPS의 기본 포트는 443이다. HTTPS는 TLS로 보호되는 웹 통신에 사용된다.

오답 포인트

1번의 21은 널리 쓰이는 포트번호이지만 SMTP가 아니라 FTP 제어 연결의 번호이다. 서로 가까운 21·22·25를 서비스명과 바꾸어 연결하는 함정에 주의한다.

다시 나오면 이렇게 판단

서비스명과 기본 포트를 한 쌍으로 대조한다. SMTP는 25, SSH는 22, RDP는 3389, HTTPS는 443으로 판단한다.

암기 포인트

FTP 21, SSH 22, SMTP 25, HTTPS 443, RDP 3389이다.

NoteBase

문 23. 다음 중 디지털 서명(Digital Signature)이 제공하는 보안 서비스가 아닌 것은?

① 기밀성(Confidentiality)

② 서명자 인증(Authentication)

③ 부인방지(Non-repudiation)

④ 무결성(Integrity)

정답 1번

출제 포인트

디지털 서명이 제공하는 서명자 인증, 무결성, 부인방지와 암호화가 제공하는 기밀성을 구별하는 문제이다.

핵심 개념

디지털 서명은 메시지의 해시값에 서명자의 개인키로 서명하고 공개키로 이를 검증하여 서명자와 메시지의 변경 여부를 확인하는 기술이다. 따라서 서명자 인증, 무결성, 부인방지를 제공하지만 메시지 내용을 숨기는 기밀성은 그 자체로 제공하지 않는다. 기밀성이 필요하면 메시지를 별도로 암호화해야 한다.

선지별 해설

① X — 기밀성은 디지털 서명 자체가 제공하는 서비스가 아니다. 틀린 표현은 '기밀성'이며, 올바르게는 수신자의 공개키나 대칭키 등으로 메시지를 암호화해야 기밀성이 제공된다.
② O — 공개키로 서명을 검증하면 해당 개인키를 가진 서명자가 생성한 서명인지 확인할 수 있으므로 서명자 인증을 제공한다.
③ O — 서명자가 자신의 개인키로 생성한 서명은 서명 사실을 사후에 부인하기 어렵게 하므로 부인방지를 제공한다.
④ O — 수신 측에서 다시 계산한 메시지의 해시값과 서명 검증 결과가 맞지 않으면 변경 사실을 알 수 있으므로 무결성을 제공한다.

오답 포인트

①의 '기밀성'을 공개키 암호 기술 전반의 기능으로 보고 디지털 서명의 기능과 혼동하기 쉽다. 디지털 서명은 내용을 숨기는 기술이 아니라 서명자와 위변조 여부를 확인하는 기술이다.

다시 나오면 이렇게 판단

'누가 보냈는가, 바뀌었는가, 나중에 부인할 수 있는가'는 디지털 서명으로 판단하고, '내용이 보이지 않는가'는 암호화로 판단한다.

NoteBase

암기 포인트

서명은 인증·무결성·부인방지, 암호화는 기밀성이다.

NoteBase

문 24. 다음 중 항상 모든 가능한 평문이 모든 가능한 암호문으로 동일한 확률로 매핑되어 완벽한 비밀성을 보장하는 기법은?

① 디피-헬만 키 교환

② RSA

③ OTP (One-Time Pad)

④ 트리플 DES

정답 3번

출제 포인트

완벽한 비밀성은 암호문을 관찰해도 평문에 관한 정보가 전혀 늘어나지 않는 정보이론적 안전성을 뜻한다. 이 성질을 보장하는 기법을 구별하는 문제이다.

핵심 개념

OTP(One-Time Pad)는 평문과 길이가 같은 진정한 무작위 키를 비밀리에 공유하고, 그 키를 단 한 번만 사용하는 암호 기법이다. 이 조건을 모두 지키면 하나의 암호문에 대해 가능한 각 평문이 동일한 가능성을 가지므로 계산 능력과 관계없이 완벽한 비밀성이 성립한다. 반면 디피-헬만, RSA, 트리플 DES의 안전성은 공격자의 계산 능력과 계산 문제의 어려움에 의존한다.

선지별 해설

① X — 디피-헬만 키 교환은 통신 당사자가 공통 비밀값을 합의하는 방식이며, 그 자체가 모든 평문을 모든 암호문에 같은 확률로 대응시키는 완전 비밀 암호는 아니다. 틀린 표현은 '디피-헬만 키 교환'이며, 올바르게는 '이산로그 문제의 계산적 어려움에 기반한 키 합의 방식'이다.
② X — RSA는 정수 인수분해의 계산적 어려움에 기반한 공개키 암호 방식이므로 정보이론적 완벽한 비밀성을 보장하지 않는다. 틀린 표현은 'RSA'이며, 올바르게는 '계산적 안전성을 제공하는 공개키 암호 방식'이다.
③ O — OTP는 평문과 같은 길이의 진정한 무작위 키를 한 번만 사용하고 비밀로 유지할 때, 관찰된 암호문으로 평문을 더 유리하게 추정할 수 없으므로 완벽한 비밀성을 보장한다.
④ X — 트리플 DES는 DES 연산을 세 번 적용하는 대칭키 블록 암호로, 유한한 키 공간과 계산량에 의존하는 계산적 안전성을 제공할 뿐 완벽한 비밀성을 보장하지 않는다. 틀린 표현은 '트리플 DES'이며, 올바르게는 '계산적 안전성을 목표로 하는 대칭키 블록 암호'이다.

오답 포인트

'현실적으로 강한 암호'와 '완벽한 비밀성을 수학적으로 보장하는 암호'를 혼동하기 쉽다. ①·②·④는 널리 쓰이는 암호 기술이지만 계산적 안전성을 제공하며, 완벽한 비밀성은 엄격한 키 조건을 충족한 ③의 OTP에만 해당한다.

NoteBase

다시 나오면 이렇게 판단

‘모든 가능한 평문’, ‘동일한 확률’, ‘완벽한 비밀성’이 함께 제시되면 정보이론적 안전성을 묻는 것으로 판단한다. 평문과 같은 길이의 진정한 무작위 키를 한 번만 쓰는지 확인하면 OTP를 선택할 수 있다.

암기 포인트

OTP의 완벽한 비밀성 조건은 ‘평문과 같은 길이, 진정한 무작위, 비밀 공유, 단 한 번 사용’이다.

NoteBase

문 25. 분산서비스거부(DDoS) 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

① 정보보안의 3요소 중 가용성이 훼손된다.

② 일반 DoS와 달리 여러 호스트 또는 봇넷을 이용해 공격 트래픽을 분산·증폭시키는 경우가 많다.

③ UDP에서는 DDoS 공격이 성립하지 않는다.

④ 서버 메모리 증설만으로는 대역폭, CPU, 애플리케이션 처리량 등을 겨냥한 DDoS 공격을 충분히 방어하기 어렵다.

정답 3번

출제 포인트

DDoS 공격의 분산성, 가용성 침해, UDP 기반 공격 가능성 및 자원 증설의 방어 한계를 구분하는 문제이다.

핵심 개념

DoS는 서비스가 정상 요청을 처리하지 못하도록 자원을 소진시키는 공격이다. DDoS는 여러 공격 출발지나 봇넷 등을 이용해 이를 분산 수행하는 형태이며, 네트워크 대역폭·서버 자원·애플리케이션 처리 능력 등 다양한 지점을 소진시킬 수 있다. UDP도 플러드 공격이나 반사·증폭 공격에 이용될 수 있다.

선지별 해설

① O — DDoS는 정상 사용자가 서비스를 이용하지 못하게 하므로 정보보안의 3요소인 기밀성·무결성·가용성 중 가용성을 훼손한다.
② O — DDoS는 다수의 감염 호스트로 구성된 봇넷 등에서 동시에 트래픽을 보내 공격원을 분산하며, 반사·증폭 기법을 함께 사용하는 경우도 많다.
③ X — 틀린 표현은 ‘UDP에서는 DDoS 공격이 성립하지 않는다’이다. 올바르게는 UDP에서도 대량 패킷을 보내는 UDP 플러드나, 출발지 주소를 위조해 응답 트래픽을 피해자에게 집중시키는 반사·증폭 방식의 DDoS 공격이 성립한다.
④ O — DDoS는 메모리뿐 아니라 회선 대역폭, CPU, 연결 상태, 애플리케이션 처리량 등 여러 자원을 고갈시킬 수 있으므로 서버 메모리만 늘리는 것으로는 충분히 방어하기 어렵다.

오답 포인트

③은 UDP가 비연결형이라는 특성을 ‘서비스 거부 공격이 불가능하다’는 뜻으로 바꾼 함정이다. 연결 설정이 없어도 패킷 폭주로 대역폭과 처리 자원을 소진시킬 수 있으며, 오히려 출발지 주소 위조가 쉬워 반사·증폭 공격에 악용될 수 있다.

NoteBase

다시 나오면 이렇게 판단

DDoS 선지는 먼저 공격 대상 자원이 무엇인지 확인한다. 정상 서비스 이용을 막으면 가용성 침해이고, UDP의 비연결성은 공격 불가능의 근거가 아니며, 한 종류의 서버 자원만 증설하는 대책은 다른 병목을 겨냥한 공격까지 막지 못한다.

암기 포인트

DDoS는 분산된 공격원으로 가용성을 해치며, UDP에서도 가능하고 메모리 증설만으로는 막을 수 없다.

NoteBase