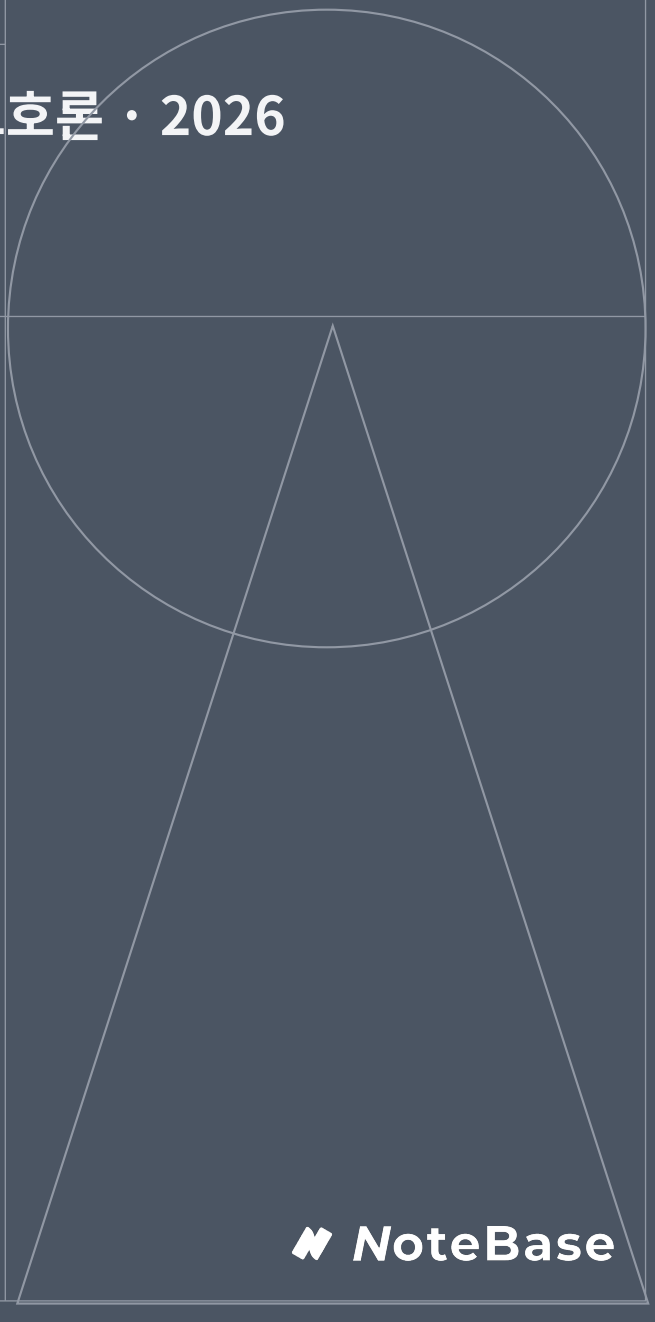
기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2026



NoteBase

기출OX 해설집

공무원/군무원/9급 · 정보보호론 · 2026

공무원/군무원/9급 · 정보보호론 · 2026

1. PKI(Public Key Infrastructure)의 구성 요소가 아닌 것은?
   ① 인증기관(CA)
   ② 등록기관(RA)
   ③ 디렉터리 서비스
   ④ 침입탐지 시스템(IDS)

정답 4번

출제 포인트

이 문제는 공개키 기반구조(PKI)를 이루는 인증서 관리 요소와 일반 보안 시스템을 구별하는 문제이다.

핵심 개념

PKI는 공개키 인증서를 발급·관리·검증하여 공개키의 소유자와 신뢰성을 확인하게 하는 체계이다.
인증기관(CA)은 인증서의 발급·갱신·폐지 등 인증서 생명주기를 관리하고 전자서명으로 인증서의 신뢰성을 보증한다.
등록기관(RA)은 신청자의 신원을 확인하고 인증서 발급·폐지 요청을 접수하여 CA에 전달한다.
디렉터리 서비스는 인증서와 인증서 폐지 정보 등을 저장·공개하여 이용자가 조회할 수 있게 한다.
침입탐지 시스템(IDS)은 네트워크나 시스템의 활동을 감시하여 침입 징후를 탐지하는 보안 시스템으로, PKI의 인증서 관리 구성 요소가 아니다.

선지별 해설

① O — 인증기관(CA)은 공개키 인증서를 발급하고 갱신·폐지하며 인증서의 신뢰성을 보증하므로 PKI의 핵심 구성 요소이다.
② O — 등록기관(RA)은 인증서 신청자의 신원을 확인하고 신청 정보를 CA에 전달하므로 PKI의 구성 요소이다.
③ O — 디렉터리 서비스는 인증서와 폐지 정보를 저장·공개하고 이용자의 조회를 지원하므로 PKI의 구성 요소이다.
④ X — 틀린 표현은 '침입탐지 시스템(IDS)이 PKI의 구성 요소'라는 분류이다. IDS는 침입 징후를 감시·탐지하는 별도의 보안 시스템이며, 올바르게는 PKI의 구성 요소가 아니다.

NoteBase

오답 포인트

IDS도 정보보호 기술이라는 이유만으로 PKI 구성 요소라고 판단하기 쉽다. 그러나 PKI 구성 요소인지는 인증서의 발급, 신원 확인, 저장·공개와 직접 관련되는지를 기준으로 구별한다.

다시 나오면 이렇게 판단

각 선지가 공개키 인증서의 발급·등록·저장·검증 과정에 직접 참여하는지 확인한다. 인증서 관리가 아니라 공격이나 침입을 탐지하는 장비·시스템이면 PKI 구성 요소에서 제외한다.

암기 포인트

PKI는 CA·RA·디렉터리, IDS는 침입 탐지이다.

2. 스팸 메일 필터링 방식 중 이메일 발신 도메인의 DNS에 등록된 IP를 검증하는 방식은?
① 베이지안 필터
② SPF(Sender Policy Framework)
③ 블랙리스트 필터
④ 콘텐츠 필터

정답 2번

출제 포인트

이 문제는 이메일 발신 도메인의 DNS에 공개된 허용 발신 IP를 대조하는 SPF와 다른 스팸 메일 필터링 방식을 구별하는 문제이다.

핵심 개념

SPF(Sender Policy Framework): 도메인 관리자가 DNS에 해당 도메인의 메일을 보낼 수 있는 서버의 IP 정보를 게시하고, 수신 서버가 실제 발신 IP와 대조하여 위조 여부를 판단하는 이메일 인증 방식이다.
베이지안 필터는 메일의 단어·특징이 스팸일 확률을 통계적으로 계산하고, 블랙리스트 필터는 차단 목록과 대조하며, 콘텐츠 필터는 제목·본문·첨부파일 등의 내용을 규칙에 따라 검사한다.

선지별 해설

① X — '베이지안 필터'가 DNS에 등록된 발신 IP를 검증한다는 부분이 틀리다. 베이지안 필터는 학습된 단어와 특징을 바탕으로 메일이 스팸일 확률을 계산하는 방식이다.
② O — SPF는 수신 서버가 발신 도메인의 DNS에 게시된 SPF 레코드를 조회하여 실제 발신 서버의 IP가 허용된 IP인지 검증하는 방식이다.
③ X — '블랙리스트 필터'가 발신 도메인의 DNS에 등록된 허용 IP를 검증한다는 부분이 틀리다. 블랙리스트 필터는 발신 IP나 도메인 등이 미리 등록된 차단 목록에 포함되는지를 확인하는 방식이다.
④ X — '콘텐츠 필터'가 DNS의 허용 발신 IP를 검증한다는 부분이 틀리다. 콘텐츠 필터는 메일의 제목·본문·첨부파일 등에 포함된 문자열이나 패턴을 분석하여 차단 여부를 판단하는 방식이다.

오답 포인트

③도 IP를 확인할 수 있어 혼동하기 쉽지만, 블랙리스트는 '차단 목록에 있는가'를 확인하고 SPF는 '발신 도메인이 DNS에 허용한 IP인가'를 확인한다는 점이 다르다.

NoteBase

다시 나오면 이렇게 판단

문제에 '발신 도메인', 'DNS', '등록된 IP', '허용된 메일 서버'가 함께 제시되면 SPF로 판단한다. 메일 내용의 통계적 확률은 베이지안, 차단 목록 대조는 블랙리스트, 제목·본문의 규칙 검사는 콘텐츠 필터로 구분한다.

암기 포인트

SPF는 DNS에 공개된 발신 허용 IP를 검사한다.

NoteBase

3. VPN(Virtual Private Network)의 주된 목적으로 가장 적절한 것은?
① 공중망에서 안전한 사설 통신 채널 구성
② 인터넷 속도 향상
③ 악성코드 차단
④ 이메일 필터링

정답 1번

출제 포인트

VPN의 주된 목적이 공중망을 이용하면서도 사설망처럼 안전한 통신 경로를 구성하는 데 있음을 묻는 문제이다.

핵심 개념

VPN(Virtual Private Network)은 인터넷 같은 공중망에서 터널링과 암호화 등을 이용하여 허가된 사용자나 네트워크 사이에 논리적으로 분리된 안전한 사설 통신 경로를 만드는 기술이다. 핵심 키워드는 공중망, 사설 통신, 터널링, 암호화이다.

선지별 해설

① O — VPN은 공중망 위에 암호화된 터널을 형성하여 사설망처럼 안전하게 통신하도록 하는 것이 주된 목적이다.
② X — 틀린 표현은 '인터넷 속도 향상'이다. VPN은 보안 통신 경로를 제공하는 기술이며 속도 향상을 목적으로 하지 않는다. 실제로는 암호화와 우회 전송에 따른 처리 부담 때문에 속도가 낮아질 수도 있다. 올바르게는 '공중망에서 안전한 사설 통신 채널 구성'이다.
③ X — 틀린 표현은 '악성코드 차단'이다. 악성코드의 탐지·차단은 백신이나 보안 솔루션의 주된 기능이며, VPN 자체의 주된 목적이 아니다. 올바르게는 '통신 데이터의 기밀성을 보호하고 안전한 접속 경로를 제공'하는 것이다.
④ X — 틀린 표현은 '이메일 필터링'이다. 스팸·피싱 메일의 분류와 차단은 이메일 보안 또는 스팸 필터의 기능이며, VPN의 주된 목적이 아니다. 올바르게는 '원격 사용자나 떨어진 네트워크를 안전하게 연결'하는 것이다.

오답 포인트

②~④는 모두 넓은 의미에서 정보통신 환경과 관련된 기능이지만 VPN의 직접적인 목적은 아니다. 특히 VPN을 사용하면 인터넷이 빨라진다는 인식과, VPN이 모든 보안 위협을 차단한다는 인식을 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

VPN 문항에서는 '공중망 위의 암호화된 터널을 통한 사설망 연결'에 해당하는지를 먼저 판단한다. 속도 향상, 악성코드 차단, 이메일 필터링처럼 다른 보안 도구의 기능은 VPN의 주된 목적에서 제외한다.

암기 포인트

VPN은 공중망을 사설망처럼 안전하게 연결하는 암호화 통신 터널이다.

NoteBase

4. XSS(Cross-Site Scripting) 공격에서 주로 이용하는 취약점으로 가장 적절한 것은?
① SQL 데이터베이스 취약점
② 웹 애플리케이션의 입력값 검증 미흡
③ 운영체제 커널 취약점
④ 네트워크 라우팅 취약점

정답 2번

출제 포인트

XSS 공격이 성립하는 핵심 원인이 웹 애플리케이션의 입력값 검증 및 출력 처리 미흡이라는 점을 묻는 문제이다.

핵심 개념

XSS는 공격자가 삽입한 악성 스크립트가 웹 페이지를 통해 다른 사용자의 브라우저에서 실행되게 하는 공격이다. 웹 애플리케이션이 외부 입력을 충분히 검증·정제하지 않거나 출력 시 문맥에 맞게 인코딩하지 않을 때 주로 발생한다.

선지별 해설

① X — SQL 데이터베이스 취약점은 XSS의 주된 이용 대상이 아니다. 이 표현은 웹 애플리케이션의 입력값 검증 미흡 및 출력 인코딩 미흡으로 고쳐야 한다. 데이터베이스 질의문 조작은 주로 SQL 삽입 공격과 관련된다.
② O — 검증되지 않은 입력값에 포함된 스크립트가 웹 페이지에 반영되면 사용자의 브라우저에서 실행될 수 있으므로 XSS가 성립한다.
③ X — 운영체제 커널 취약점은 권한 상승이나 시스템 장악 등에 이용될 수 있지만 XSS의 주된 취약점은 아니다. 운영체제 커널 취약점이라는 표현은 웹 애플리케이션의 입력값 검증 및 출력 처리 미흡으로 고쳐야 한다.
④ X — 네트워크 라우팅 취약점은 트래픽의 전달 경로나 경로 조작과 관련되며 XSS의 주된 취약점이 아니다. 네트워크 라우팅 취약점이라는 표현은 웹 애플리케이션의 입력값 검증 및 출력 처리 미흡으로 고쳐야 한다.

오답 포인트

①의 데이터베이스라는 말 때문에 웹 공격이라는 공통점만 보고 SQL 삽입과 XSS를 혼동하기 쉽다. XSS의 악성 코드는 데이터베이스가 아니라 최종적으로 사용자의 브라우저에서 실행된다는 점이 핵심이다.

다시 나오면 이렇게 판단

선지에서 스크립트 삽입과 브라우저 실행이 보이면 외부 입력 검증·정제와 출력 인코딩 여부를 확인한다. SQL 질의문 조작은 SQL 삽입, 커널 결함은 시스템 취약점, 경로 조작은 라우팅 취약점으로 구분한다.

NoteBase

암기 포인트

XSS는 입력값 검증·출력 인코딩 미흡을 틈타 브라우저에서 스크립트를 실행시키는 공격이다.

NoteBase

5. 사물인터넷(IoT) 장비를 주로 감염시키고 P2P(Peer-To-Peer) 기반의 봇넷을 구성하며, 2020년대 들어 지속해서 대량으로 탐지되고 있는 악성코드는?
① Emotet
② LokiBot
③ Mozi
④ FormBook

정답 3번

출제 포인트

IoT 장비를 주로 감염시키고 P2P 방식으로 통신하는 봇넷과 일반적인 다운로더·정보 탈취형 악성코드를 구별하는 문제이다.

핵심 개념

Mozi는 라우터·게이트웨이·DVR 등 IoT 장비의 취약점이나 약한 텔넷 암호를 이용해 확산하고, 분산 해시 테이블을 활용하여 중앙 서버 의존도가 낮은 P2P 봇넷을 구성하는 악성코드이다. 2019년 말 등장한 뒤 2020년에 IoT 봇넷 활동에서 대규모로 관측되었다.
Emotet은 다른 악성코드를 내려받아 실행시키는 기능이 중심인 모듈형 악성코드이고, LokiBot과 FormBook은 계정 정보 등 데이터를 훔치는 정보 탈취형 악성코드이다.

선지별 해설

① X — Emotet을 문제의 'IoT 장비 감염·P2P 봇넷'과 연결한 것이 틀리다. Emotet은 피싱 메일 등을 통해 유포되어 다른 악성코드를 내려받는 모듈형 다운로더로 보는 것이 정확하다.
② X — LokiBot을 문제의 'IoT 장비 감염·P2P 봇넷'과 연결한 것이 틀리다. LokiBot은 사용자 이름, 비밀번호, 암호화폐 지갑 등의 정보를 훔치는 Windows 기반 정보 탈취형 악성코드이다.
③ O — Mozi는 IoT 장비를 주로 노리고 분산 해시 테이블 기반의 P2P 통신으로 봇넷을 구성하며, 2020년 무렵 활동이 대규모로 관측된 악성코드이므로 제시된 특징과 일치한다.
④ X — FormBook을 문제의 'IoT 장비 감염·P2P 봇넷'과 연결한 것이 틀리다. FormBook은 웹 브라우저, 이메일 클라이언트, FTP 응용프로그램 등에서 정보를 훔치는 서비스형 악성코드 계열의 정보 탈취 도구로 보는 것이 정확하다.

NoteBase

오답 포인트

네 악성코드가 모두 2020년대에도 널리 언급되었고 Emotet도 봇넷을 형성할 수 있어 이름만으로 혼동하기 쉽다. 이 문항의 결정적 단서는 ‘IoT 장비를 주로 감염’, ‘P2P 기반’, ‘2020년 무렵 대량 관측’의 결합이며, 이 조합은 Mozi를 가리킨다.

다시 나오면 이렇게 판단

대상 장비와 통신 구조를 먼저 확인한다. IoT 라우터·DVR와 P2P 또는 분산 해시 테이블이 함께 제시되면 Mozi로 판단한다. 이메일 피싱과 추가 악성코드 다운로드는 Emotet, 계정·지갑 정보 탈취는 LokiBot, 브라우저·메일·FTP 정보 탈취는 FormBook으로 구별한다.

암기 포인트

Mozi = IoT + P2P, Emotet = 다운로더, LokiBot·FormBook = 정보 탈취이다.

NoteBase

6. TLS Handshake 과정에서 서버가 클라이언트에게 전송하는 것으로 가장 적절하지 않은 것은?
① 서버 인증서
② 지원하는 암호화 알고리즘 목록
③ 서버 랜덤값
④ 서버의 개인키

정답 4번

출제 포인트

TLS Handshake에서 서버가 클라이언트에게 공개·전송하는 정보와 외부에 절대 노출해서는 안 되는 비밀정보를 구분하는 문제이다.

핵심 개념

TLS Handshake는 클라이언트와 서버가 보안 통신에 사용할 방식과 키 재료를 협상하고, 인증서를 통해 서버의 신원을 확인하는 절차이다. 서버는 인증서, 클라이언트가 제시한 후보 중 선택한 암호 스위트, 서버 랜덤값 등을 전달할 수 있지만 서버의 개인키는 서버 내부에 비밀로 보관한다. 개인키 자체를 보내는 대신 개인키를 이용한 서명 등으로 개인키를 보유하고 있음을 증명한다.

선지별 해설

① O — 서버 인증서는 서버의 신원을 확인하고 서버의 공개키를 제공하기 위해 클라이언트에게 전송될 수 있다.

② O(출제 의도상) — 이 선지는 암호 알고리즘 협상 정보의 전달을 뜻하는 것으로 해석한다. 다만 프로토콜의 송신 역할을 엄밀히 구분하면, 지원하는 암호 스위트 목록은 클라이언트가 ClientHello에서 제시하고 서버는 ServerHello에서 그중 선택한 암호 스위트를 알린다. 따라서 '서버가 지원하는 목록을 보낸다'는 표현 자체는 정확하지 않지만, 이 문항은 절대 전송해서는 안 되는 개인키를 가장 부적절한 것으로 본다.

③ O — 서버 랜덤값은 클라이언트 랜덤값과 함께 세션 키를 도출하는 데 사용되는 공개적인 키 재료로서 서버가 클라이언트에게 전송한다.

④ X — '서버의 개인키'가 틀린 표현이다. 개인키가 전송되면 누구나 서버를 사칭하거나 보호된 통신을 위협할 수 있으므로 서버 내부에 비밀로 보관해야 한다. 올바르게는 서버가 개인키 자체가 아니라 서버 인증서에 포함된 공개키와 개인키로 생성한 서명 등 필요한 증명값을 전송한다.

NoteBase

오답 포인트

공개키와 개인키를 한 쌍이라는 이유로 둘 다 상대에게 보내는 것으로 혼동하기 쉽다. 인증서에 담겨 전달되는 것은 공개키이며, 개인키는 네트워크로 전송하지 않는다. 또한 ②의 표현은 엄밀하지 않다. 지원 암호 스위트 목록은 클라이언트가 보내고 서버는 그중 선택한 결과를 알린다. 이 문항은 ②를 협상 정보의 전달로 넓게 해석하고, 절대 전송해서는 안 되는 ④를 정답으로 삼은 것이다.

다시 나오면 이렇게 판단

Handshake 정보가 상대방도 알아야 하는 공개·협상 정보인지, 소유자만 보관해야 하는 비밀정보인지 구분한다. 인증서·공개키·랜덤값·협상 결과는 전달될 수 있지만 개인키는 어떤 경우에도 전달 대상이 아니다.

암기 포인트

인증서와 공개키는 전송, 개인키는 서버에 보관이다.

NoteBase

7. 과학기술정보통신부가 주무 부처로 관장하는 법률이 아닌 것은?
① 「정보통신기반 보호법」
② 「산업기술의 유출방지 및 보호에 관한 법률」
③ 「전자서명법」
④ 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」

정답 2번

쟁점

이 문제는 정보보호 관련 법률의 소관 부처를 구별하는 문제이다. 핵심은 정보통신·전자서명·클라우드 분야를 관장하는 과학기술정보통신부와 산업기술 보호를 관장하는 산업통상부를 구분하는 것이다.

용어 풀이

주무 부처는 특정 법률과 정책 분야를 중심적으로 담당하여 관련 제도를 운영하는 중앙행정기관이다.

핵심 구분

「정보통신기반 보호법」, 「전자서명법」, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」의 소관 부처는 과학기술정보통신부이다. 반면 「산업기술의 유출방지 및 보호에 관한 법률」은 산업기술과 국가핵심기술의 보호를 다루며 소관 부처는 산업통상부이다. 따라서 과학기술정보통신부가 주무 부처가 아닌 법률은 ②이다.

NoteBase

선지별 해설

① X
- 「정보통신기반 보호법」은 주요정보통신기반시설을 전자적 침해행위로부터 보호하는 법률로, 과학기술정보통신부 소관이다.
- 틀린 판단: 과학기술정보통신부가 주무 부처인 법률이 아니다.
- 올바른 판단: 과학기술정보통신부가 주무 부처인 법률이다.

② O
- 「산업기술의 유출방지 및 보호에 관한 법률」은 산업기술과 국가핵심기술의 유출 방지·보호를 다루며, 산업통상부 소관이다. 따라서 과학기술정보통신부가 주무 부처인 법률이 아닌 것을 고르는 문제의 정답이다.

③ X
- 「전자서명법」은 전자서명의 신뢰성과 전자서명인증업무의 운영을 다루는 과학기술정보통신부 소관 법률이다.
- 틀린 판단: 과학기술정보통신부가 주무 부처인 법률이 아니다.
- 올바른 판단: 과학기술정보통신부가 주무 부처인 법률이다.

④ X
- 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」은 클라우드컴퓨팅의 발전·이용 촉진과 이용자 보호를 다루는 과학기술정보통신부 소관 법률이다.
- 틀린 판단: 과학기술정보통신부가 주무 부처인 법률이 아니다.
- 올바른 판단: 과학기술정보통신부가 주무 부처인 법률이다.

오답 포인트

법률명에 '기술'과 '보호'가 들어간다는 이유만으로 모두 과학기술정보통신부 소관이라고 판단하기 쉽다. ②의 '산업기술'은 정보통신 일반이 아니라 산업경쟁력 및 국가핵심기술 보호와 연결되므로 산업통상부 소관이라는 점이 함정이다. 또한 지문이 '아닌 것'을 묻는 부정형임을 놓치면 ①·③·④를 잘못 고를 수 있다.

다시 나오면 이렇게 판단

법률명의 핵심 정책대상을 먼저 확인한다. 정보통신기반·전자서명·클라우드는 과학기술정보통신부로 묶고, 산업기술·국가핵심기술의 유출 방지와 보호는 산업통상부로 구분한다. 마지막으로 지문의 '아닌 것'이라는 부정 표현을 확인한다.

암기 포인트

정보통신기반·전자서명·클라우드 = 과기정통부, 산업기술 유출방지 = 산업통상부이다.

NoteBase

8. 커버로스(Kerberos) 인증 프로토콜에 대한 설명으로 가장 적절하지 않은 것은?
① 티켓 기반 인증 방식을 사용한다.
② 대칭키 암호화를 기반으로 한다.
③ 공개키 인프라(PKI)만을 사용한다.
④ 단일 로그온(SSO)을 지원한다.

정답 3번

출제 포인트

Kerberos 인증의 핵심 요소인 KDC, 티켓, 대칭키 암호화, 단일 로그온의 관계를 묻는 문제이다.

핵심 개념

Kerberos는 신뢰할 수 있는 키 배포 센터(KDC)가 발급한 티켓으로 사용자의 신원을 확인하는 네트워크 인증 프로토콜이다. 기본 구조에서는 클라이언트·서버와 KDC가 공유하는 비밀키를 바탕으로 대칭키 암호화를 사용한다. 한 번 인증받은 뒤 발급된 티켓으로 여러 서비스에 접근할 수 있어 단일 로그온(SSO)을 지원한다.

선지별 해설

① O — Kerberos는 KDC가 발급한 티켓을 서비스 접근 시 제시하는 티켓 기반 인증 방식을 사용한다.

② O — Kerberos의 기본 인증 구조는 공유 비밀키를 이용한 대칭키 암호화를 기반으로 한다.

③ X — 틀린 표현은 '공개키 인프라(PKI)만을 사용한다'이다. Kerberos의 핵심은 PKI만을 사용하는 것이 아니라 KDC가 발급하는 티켓과 대칭키 암호화에 있다. 올바르게는 'Kerberos는 KDC와 대칭키 암호화를 기반으로 티켓 인증을 수행한다'이다.

④ O — 최초 인증으로 티켓 발급 티켓(TGT)을 얻으면 매번 자격 증명을 다시 입력하지 않고 여러 서비스용 티켓을 발급받을 수 있으므로 단일 로그온(SSO)을 지원한다.

오답 포인트

③의 'PKI'라는 기술 용어보다 '만을'이라는 단정이 핵심 함정이다. Kerberos에 공개키를 활용하는 확장 방식이 있을 수 있어도, Kerberos 자체의 기본 인증 구조를 PKI 전용 방식으로 설명할 수는 없다.

NoteBase

다시 나오면 이렇게 판단

Kerberos 관련 선지는 ‘KDC가 티켓을 발급한다’, ‘기본적으로 대칭키를 사용한다’, ‘TGT를 통해 SSO를 지원한다’라는 세 기준으로 판단한다. PKI만 사용하거나 공개키 암호화만을 기반으로 한다는 표현은 틀린 설명으로 판단한다.

암기 포인트

Kerberos는 KDC·대칭키·티켓·SSO이다.

NoteBase

9. 디지털 포렌식(Digital Forensics) 원칙에 대한 설명으로 옳은 것을 모두 고르면?

ㄱ. 원본 증거의 무결성을 보존하기 위해 이미지 복사본으로 분석을 수행한다.
ㄴ. 해시값을 통해 수집된 증거의 변조 여부를 검증할 수 있다.
ㄷ. 증거의 연속성(Chain Of Custody)은 증거의 취급 이력을 문서화한다.
ㄹ. 포렌식 도구로 수집한 모든 데이터는 법적 효력을 자동으로 가진다.

① ㄱ, ㄴ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ, ㄹ

정답 3번

출제 포인트

디지털 포렌식에서 원본 증거의 무결성을 보존하고, 해시값과 증거의 연속성으로 증거의 신뢰성을 입증하는 원칙을 묻는 문제이다.

핵심 개념

이미지 복사본: 저장매체의 데이터를 비트 단위로 복제한 사본으로, 원본을 직접 변경하지 않고 분석하기 위해 사용한다.
해시값: 데이터에서 계산한 고유한 요약값으로, 수집 당시와 분석 이후의 값이 같은지 비교하여 변조 여부와 무결성을 확인한다.
증거의 연속성(Chain of Custody): 증거를 누가 언제 어디서 수집·인계·보관·분석했는지 전 과정을 기록하여 증거의 동일성과 신뢰성을 뒷받침하는 관리 체계이다.
법적 효력: 포렌식 도구로 수집했다는 사실만으로 자동 발생하지 않으며, 적법한 수집 절차와 무결성·동일성·신뢰성 등이 함께 입증되어야 한다.

NoteBase

선지별 해설

① X
ㄱ과 ㄴ은 옳지만, 증거의 취급 이력을 문서화하는 ㄷ도 옳으므로 조합이 불완전하다. 틀린 부분은 옳은 진술에서 ㄷ을 제외한 점이다. 올바른 조합은 ㄱ, ㄴ, ㄷ이다.

② X
ㄴ과 ㄷ은 옳지만, 원본 증거의 변경을 방지하기 위해 이미지 복사본으로 분석하는 ㄱ도 옳으므로 조합이 불완전하다. 틀린 부분은 옳은 진술에서 ㄱ을 제외한 점이다. 올바른 조합은 ㄱ, ㄴ, ㄷ이다.

③ O
ㄱ은 원본 보존 원칙, ㄴ은 해시값을 이용한 무결성 검증, ㄷ은 증거의 연속성에 관한 설명으로 모두 옳다.

④ X
ㄹ의 '모든 데이터는 법적 효력을 자동으로 가진다'는 표현이 틀렸다. 포렌식 도구로 수집한 데이터도 수집의 적법성, 무결성, 동일성, 증거의 연속성 및 분석의 신뢰성 등이 입증되어야 증거로 인정될 수 있다. 따라서 올바른 조합은 ㄹ을 제외한 ㄱ, ㄴ, ㄷ이다.

오답 포인트

ㄹ에서 '포렌식 도구로 수집'과 '법적 효력의 자동 발생'을 같은 것으로 보는 것이 함정이다. 도구의 사용은 신뢰성 확보에 도움이 되지만, 적법한 절차와 무결성 입증을 대신하지 않는다. 또한 ㄷ의 증거의 연속성은 단순한 보관이 아니라 수집부터 분석까지 모든 취급 이력을 문서화하는 원칙이다.

다시 나오면 이렇게 판단

원본은 직접 분석하지 않고 사본을 사용하며, 해시값은 데이터의 동일성·무결성을 확인하고, 증거의 연속성은 취급 전 과정을 기록한다고 판단한다. '모든', '자동으로', '무조건'처럼 증거능력을 절대화하는 표현은 적법 절차와 신뢰성 입증 요건을 빠뜨렸는지 확인한다.

암기 포인트

원본은 보존, 분석은 이미지 사본, 무결성은 해시, 취급 이력은 증거의 연속성이다. 포렌식 수집만으로 법적 효력이 자동 발생하지 않는다.

NoteBase

10. 침입탐지 시스템(IDS)에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. 시그니처 기반 탐지는 알려진 공격 패턴과 비교하여 탐지하므로 알려지지 않은 공격(Zero-day)에 취약하다.
ㄴ. 이상 탐지(Anomaly Detection)는 정상 행위 기준을 설정하고 벗어나는 행위를 탐지하므로 오탐(False Positive)이 발생할 수 있다.
ㄷ. NIDS는 암호화된 트래픽도 복호화하여 내용 기반으로 탐지할 수 있다.
ㄹ. IDS는 탐지만 수행하며, 능동적 차단은 IPS의 역할이다.

① ㄷ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 1번

출제 포인트

이 문제는 시그니처 기반 탐지와 이상 탐지의 차이, 암호화 트래픽에 대한 NIDS의 한계, IDS와 IPS의 역할 구분을 묻는다.

핵심 개념

시그니처 기반 탐지는 알려진 공격의 특징이나 패턴과 비교하여 침입을 찾는 방식이다. 알려지지 않은 공격에는 취약하지만 일반적으로 오탐이 비교적 적다.
이상 탐지는 정상 행위의 기준선을 정하고 이를 벗어난 활동을 찾는 방식이다. 알려지지 않은 공격도 탐지할 가능성이 있지만 정상적인 변화까지 공격으로 판단하여 오탐이 발생할 수 있다.
NIDS는 네트워크 구간의 패킷과 흐름을 감시하는 시스템이다. 암호화된 페이로드는 별도의 복호화 수단이나 복호화 지점과의 연계가 없으면 내용 기반으로 검사하기 어렵다.
IDS의 중심 기능은 탐지·경고이고, IPS의 중심 기능은 트래픽 경로에서 공격을 능동적으로 차단하는 것이다.

NoteBase

선지별 해설

① O — ㄷ만 틀린 문장으로 고른 조합이다. ㄷ의 '암호화된 트래픽도 복호화하여 내용 기반으로 탐지할 수 있다'는 표현이 틀렸다. 올바르게는 NIDS가 별도의 복호화 수단 없이 암호화된 페이로드를 스스로 복호화하여 내용 기반으로 탐지할 수 없다고 해야 한다.
② X — ㄱ과 ㄷ을 모두 틀렸다고 한 조합이지만, ㄱ은 옳다. 시그니처 기반 탐지는 알려진 공격 패턴과 비교하므로 알려지지 않은 제로데이 공격에 취약하다. 틀린 표현은 'ㄱ, ㄷ'이며, 올바른 조합은 'ㄷ'이다.
③ X — ㄴ과 ㄷ을 모두 틀렸다고 한 조합이지만, ㄴ은 옳다. 이상 탐지는 정상 행위 기준에서 벗어난 활동을 탐지하므로 정상적인 변화도 공격으로 판단하는 오탐이 발생할 수 있다. 틀린 표현은 'ㄴ, ㄷ'이며, 올바른 조합은 'ㄷ'이다.
④ X — ㄷ과 ㄹ을 모두 틀렸다고 한 조합이지만, ㄹ은 옳다. IDS는 주로 탐지와 경고를 수행하고, 네트워크 경로에서 공격을 능동적으로 차단하는 기능은 IPS의 역할이다. 틀린 표현은 'ㄷ, ㄹ'이며, 올바른 조합은 'ㄷ'이다.

오답 포인트

ㄷ의 '복호화하여'가 핵심 함정이다. NIDS가 암호화된 트래픽의 흐름이나 메타데이터를 관찰할 수 있다는 사실과, 암호화된 페이로드를 직접 복호화하여 내용을 검사할 수 있다는 주장은 다르다. 또한 ㄹ에서는 탐지·경고를 담당하는 IDS와 능동 차단을 담당하는 IPS를 구분해야 한다.

다시 나오면 이렇게 판단

탐지 방식은 '알려진 패턴과 비교하면 시그니처', '정상 기준에서 벗어났는지 보면 이상 탐지'로 구분한다. 암호화 트래픽은 별도 복호화 조건이 제시되지 않으면 내용 검사가 어렵다고 판단하고, 탐지·경고는 IDS, 능동 차단은 IPS로 구분한다.

암기 포인트

시그니처는 알려진 공격에 강하고, 이상 탐지는 제로데이에 대응 가능하지만 오탐이 생길 수 있다. 암호화 내용은 그대로는 보이지 않으며, IDS는 탐지, IPS는 차단이다.

NoteBase

11. IPSec 프로토콜에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. AH(Authentication Header)는 데이터 무결성과 인증을 제공하지만 기밀성은 제공하지 않는다.
ㄴ. ESP(Encapsulating Security Payload)는 데이터 암호화와 인증을 모두 제공한다.
ㄷ. 전송 모드(Transport Mode)는 원본 IP 헤더를 포함한 전체 패킷을 새 패킷으로 캡슐화한다.
ㄹ. IKE(Internet Key Exchange)는 IPSec에서 보안 연결(SA) 협상에 사용된다.

① ㄷ
② ㄷ, ㄹ
③ ㄴ, ㄷ
④ ㄱ, ㄷ

정답 1번

출제 포인트

IPsec의 AH·ESP·IKE가 담당하는 기능과 전송 모드·터널 모드의 캡슐화 범위를 구분하는 문제이다.

핵심 개념

AH: IP 패킷의 무결성과 데이터 출처 인증을 제공하지만 기밀성은 제공하지 않는 IPsec 프로토콜이다.
ESP: 데이터 암호화를 통한 기밀성을 제공하고, 무결성과 출처 인증 기능도 지원하는 IPsec 프로토콜이다.
전송 모드: 원본 IP 헤더는 그대로 두고 주로 상위 계층의 페이로드를 보호한다.
터널 모드: 원본 IP 헤더를 포함한 원본 IP 패킷 전체를 캡슐화하고 새로운 외부 IP 헤더를 붙인다.
IKE: 통신 당사자가 보안 연계(SA)를 협상하고 키를 관리하도록 하는 프로토콜이다.

NoteBase

선지별 해설

① O — ㄷ만 틀렸으므로 옳은 조합이다. ㄷ의 '전송 모드는 원본 IP 헤더를 포함한 전체 패킷을 새 패킷으로 캡슐화한다'는 표현이 틀렸다. 올바르게는 터널 모드가 원본 IP 패킷 전체를 캡슐화하며, 전송 모드는 원본 IP 헤더를 유지하고 주로 페이로드를 보호한다.
② X — ㄹ은 IKE가 IPsec의 보안 연계(SA) 협상에 사용된다는 옳은 설명이므로 틀린 지문에 포함할 수 없다. 올바른 틀린 지문 조합은 ㄷ만이다.
③ X — ㄴ은 ESP가 데이터 암호화와 인증 기능을 모두 제공한다는 옳은 설명이므로 틀린 지문에 포함할 수 없다. 올바른 틀린 지문 조합은 ㄷ만이다.
④ X — ㄱ은 AH가 데이터 무결성과 인증을 제공하지만 기밀성은 제공하지 않는다는 옳은 설명이므로 틀린 지문에 포함할 수 없다. 올바른 틀린 지문 조합은 ㄷ만이다.

오답 포인트

ㄷ의 '원본 IP 헤더를 포함한 전체 패킷'이라는 문구는 터널 모드의 특징이다. 전송 모드와 터널 모드의 보호 범위를 바꾸어 제시한 것이 핵심 함정이다. 또한 AH의 인증과 ESP의 암호화·인증, IKE의 SA 협상을 서로 다른 역할로 구분해야 한다.

다시 나오면 이렇게 판단

먼저 기능별로 AH는 무결성·인증, ESP는 암호화·인증, IKE는 SA 협상으로 구분한다. 이어서 원본 IP 헤더가 유지되면 전송 모드이고, 원본 IP 패킷 전체가 새 IP 패킷 안에 들어가면 터널 모드로 판단한다.

암기 포인트

AH는 인증, ESP는 암호화까지, IKE는 SA 협상이다. 전송은 페이로드, 터널은 원본 패킷 전체를 보호한다.

NoteBase

12. 방화벽(Firewall)에 대한 설명으로 틀린 것을 모두 고르면?

ㄱ. 상태 기반 검사(Stateful Inspection) 방화벽은 TCP 연결 상태를 추적한다.
ㄴ. 방화벽은 암호화된 악성코드 내부 내용을 자동으로 탐지하고 차단한다.
ㄷ. 패킷 필터링 방화벽은 IP 주소와 포트 번호를 기반으로 트래픽을 제어한다.
ㄹ. 방화벽은 내부 사용자에 의한 모든 내부 위협을 완벽하게 차단한다.

① ㄱ, ㄷ
② ㄴ, ㄹ
③ ㄴ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

정답 2번

출제 포인트

상태 기반 검사와 패킷 필터링의 기능, 암호화된 트래픽 및 내부자 위협에 대한 방화벽의 한계를 구분하는 문제이다.

핵심 개념

상태 기반 검사 방화벽: 통신 세션의 상태 정보를 기록하고 정상적인 연결에 속한 패킷인지 판단하는 방화벽이다. TCP에서는 연결 설정·유지·종료 상태를 추적한다.
패킷 필터링 방화벽: 패킷 헤더의 출발지·목적지 IP 주소, 포트 번호, 프로토콜 등의 규칙을 기준으로 통과 여부를 결정한다.
방화벽의 한계: 암호화된 트래픽은 복호화나 별도의 SSL/TLS 검사 기능이 없으면 내부 내용을 직접 판별하기 어렵고, 내부자의 오용을 포함한 모든 내부 위협을 완벽하게 차단할 수도 없다.
따라서 ㄱ과 ㄷ은 옳고, ㄴ과 ㄹ은 틀리다.

NoteBase

선지별 해설

① X — ㄱ은 상태 기반 검사 방화벽이 TCP 연결 상태를 추적한다는 옳은 설명이므로 틀린 설명에 포함할 수 없다. 또한 실제로 틀린 ㄹ이 빠져 있다. 올바른 조합은 'ㄴ, ㄹ'이다.
② O — ㄴ은 암호화된 악성 트래픽의 내부 내용을 방화벽이 자동으로 탐지한다고 단정하여 틀리고, ㄹ은 모든 내부 위협을 완벽하게 차단한다고 단정하여 틀리다.
③ X — ㄴ과 ㄹ은 틀리지만, ㄷ은 IP 주소와 포트 번호를 기준으로 트래픽을 제어하는 패킷 필터링의 기본 기능이므로 틀린 설명에 포함할 수 없다. 올바른 조합은 'ㄴ, ㄹ'이다.
④ X — ㄴ과 ㄹ은 틀리지만, ㄱ과 ㄷ은 모두 옳은 설명이므로 네 문장을 전부 틀렸다고 볼 수 없다. 올바른 조합은 'ㄴ, ㄹ'이다.

오답 포인트

ㄴ의 '암호화된 내부 내용을 자동으로'와 ㄹ의 '모든 내부 위협을 완벽하게'가 함정이다. 방화벽에 다양한 보안 기능이 추가될 수 있어도 암호화 내용의 자동 판독이나 모든 내부자 위협의 완전 차단이 기본적으로 보장되는 것은 아니다.

다시 나오면 이렇게 판단

방화벽 기능을 묻는 문장에서는 먼저 검사 대상을 구분한다. 연결 상태 추적과 IP·포트 기반 제어는 기본 기능으로 판단하고, 암호화된 본문 자동 탐지나 모든 위협의 완전 차단처럼 별도 기능이 필요하거나 절대적인 표현은 틀릴 가능성을 검토한다.

암기 포인트

상태 기반은 연결 상태, 패킷 필터링은 IP·포트, 암호화 내용과 내부자 위협에는 한계가 있다.

NoteBase

13. 공개키 기반구조(PKI)에 대한 설명으로 옳은 것을 모두 고르면?

ㄱ. 인증기관(CA)은 공개키 인증서를 발급·관리한다.
ㄴ. 인증서 폐지 목록(CRL)은 유효기간이 만료된 인증서 목록이다.
ㄷ. 등록기관(RA)은 사용자 신원을 확인하고 인증서 발급을 요청한다.
ㄹ. OCSP는 인증서의 실시간 유효성 검증을 위한 프로토콜이다.

① ㄱ, ㄷ
② ㄱ, ㄴ, ㄹ
③ ㄱ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

정답 3번

출제 포인트

공개키 기반구조(PKI)의 구성 요소인 인증기관(CA)·등록기관(RA)과 인증서 상태 확인 수단인 CRL·OCSP의 역할을 구분하는 문제이다.

핵심 개념

CA는 공개키 인증서의 발급과 폐지 등 인증서 수명주기를 관리하는 기관이다.
RA는 인증서 신청자의 신원을 확인하고 CA에 인증서 발급을 요청하는 기관이다.
CRL은 유효기간이 남아 있더라도 폐지되어 더 이상 신뢰할 수 없는 인증서의 목록이다. 단순히 유효기간이 만료된 인증서의 목록이 아니다.
OCSP는 특정 인증서의 현재 상태를 온라인으로 조회하여 실시간으로 유효성을 확인하는 프로토콜이다.

NoteBase

선지별 해설

① X
ㄱ과 ㄷ은 옳지만 ㄹ도 옳으므로 정답 조합이 아니다. 틀린 부분은 옳은 설명인 ㄹ을 제외한 것이다. 올바른 조합은 ㄱ, ㄷ, ㄹ이다.

② X
ㄱ과 ㄹ은 옳지만 ㄴ은 틀리고 ㄷ은 옳다. 틀린 부분은 ㄴ을 포함하고 ㄷ을 제외한 것이다. 올바른 조합은 ㄱ, ㄷ, ㄹ이다.

③ O
ㄱ의 CA 발급·관리 기능, ㄷ의 RA 신원 확인 및 발급 요청 기능, ㄹ의 OCSP 실시간 인증서 상태 확인 기능이 모두 옳다.

④ X
ㄴ을 포함한 것이 틀렸다. CRL은 유효기간이 만료된 인증서 목록이 아니라 유효기간 만료 전이라도 폐지된 인증서의 목록이다. 따라서 ㄴ을 제외한 ㄱ, ㄷ, ㄹ이 올바른 조합이다.

오답 포인트

ㄴ의 '유효기간이 만료된'이라는 표현이 함정이다. 인증서는 유효기간이 지나면 자연히 효력을 잃지만, CRL은 아직 유효기간이 남았어도 키 노출 등의 사유로 폐지된 인증서를 확인하기 위한 목록이다.

다시 나오면 이렇게 판단

기관의 역할은 CA=인증서 발급·관리, RA=신원 확인·발급 요청으로 나눈다. 상태 확인 방식은 CRL=폐지 목록을 내려받아 확인, OCSP=특정 인증서의 현재 상태를 온라인으로 조회로 구분한다.

암기 포인트

CA는 발급·관리, RA는 신원 확인·요청, CRL은 폐지 목록, OCSP는 온라인 실시간 조회이다.

NoteBase

14. 해시함수 H에 대한 성질을 설명한 것으로 가장 적절한 것은?

A. 서로 다른 입력 값 x, y에 대해 H(x) = H(y)가 되는 경우를 찾기 어렵다.
B. 주어진 출력 값 y에 대해 H(x) = y를 만족하는 x를 찾기 어렵다.

① A - 제2역상저항성 B - 충돌저항성
② A - 충돌저항성 B - 일방향성
③ A - 일방향성 B - 제2역상저항성
④ A - 충돌저항성 B - 제2역상저항성

정답 2번

출제 포인트

이 문제는 해시함수의 충돌저항성, 일방향성, 제2역상저항성을 각각 어떤 공격 상황에서 요구하는지 구별하는 문제이다.

핵심 개념

충돌저항성: 공격자가 서로 다른 임의의 두 입력 x, y를 골라 $H(x) = H(y)$가 되는 쌍을 찾기 어려운 성질이다.
일방향성(역상저항성): 주어진 해시 출력값 y에 대해 $H(x) = y$를 만족하는 입력 x를 찾기 어려운 성질이다.
제2역상저항성: 특정 입력 x가 주어졌을 때 $H(x') = H(x)$를 만족하는 다른 입력 x'를 찾기 어려운 성질이다.

선지별 해설

① X — A의 '서로 다른 입력값 x, y를 찾아 같은 해시값을 만드는 경우'는 충돌저항성이고, B의 '주어진 출력값의 입력을 찾는 경우'는 일방향성이다. 올바르게는 'A-충돌저항성, B-일방향성'이다.
② O — A는 서로 다른 두 입력의 동일한 해시값을 찾기 어렵다는 충돌저항성이고, B는 출력값으로부터 입력을 역으로 찾기 어렵다는 일방향성이므로 두 연결이 모두 옳다.
③ X — A는 일방향성이 아니라 충돌저항성이고, B는 제2역상저항성이 아니라 일방향성이다. 올바르게는 'A-충돌저항성, B-일방향성'이다.
④ X — A를 충돌저항성으로 연결한 부분은 옳지만, B를 제2역상저항성으로 연결한 부분이 틀리다. 제2역상저항성은 특정 입력이 먼저 주어지고 그 입력과 해시값이 같은 다른 입력을 찾기 어려운 성질이다. 올바르게는 'A-충돌저항성, B-일방향성'이다.

NoteBase

오답 포인트

A에서 서로 다른 두 입력을 찾는다는 표현과 제2역상저항성의 '다른 입력'을 혼동하기 쉽다. 제2역상저항성은 기준 입력 하나가 먼저 주어지지만, 충돌저항성은 기준 입력 없이 같은 해시값을 갖는 두 입력의 쌍을 공격자가 찾는다는 점이 다르다.

다시 나오면 이렇게 판단

공격자에게 무엇이 주어졌는지를 먼저 본다. 출력값만 주어지면 일방향성, 특정 입력이 주어지고 같은 해시값의 다른 입력을 찾으면 제2역상저항성, 기준 입력 없이 서로 다른 두 입력의 같은 해시값을 찾으면 충돌저항성이다.

암기 포인트

출력값에서 입력 찾기=일방향성, 특정 입력의 짝 찾기=제2역상저항성, 같은 해시값의 두 입력 찾기=충돌저항성이다.

NoteBase

15. 다음은 MAC(Message Authentication Code)을 사용하는 환경을 설명한다. 이에 대한 설명으로 가장 적절하지 않은 것은?

> 어떤 시스템에서 송신자 A와 수신자 B는 비밀키 K를 공유하고 있으며, 메시지 M과 MAC 값을 함께 전송하고 있다.

① MAC 값은 보안을 위해 반드시 96비트 길이로 절단(Truncation)해야 한다.
② MAC은 메시지의 무결성과 송신자 인증을 제공할 수 있다.
③ 재전송 공격을 방지하기 위해 Nonce나 타임스탬프를 함께 사용할 수 있다.
④ 안전한 MAC 알고리즘은 K를 알지 못하면 새로운 유효한 MAC 값을 생성하기 어렵다.

정답 1번

출제 포인트

공유 비밀키를 사용하는 MAC의 보안 기능, 태그 길이, 재전송 공격 방지 방법을 구분하는 문제이다.

핵심 개념

MAC은 송신자와 수신자가 공유한 비밀키와 메시지를 입력으로 계산하는 인증값이다. 수신자는 받은 메시지로 MAC을 다시 계산하여 값이 일치하는지 확인함으로써 메시지 무결성과 데이터 출처 인증을 확인할 수 있다. MAC 태그의 길이는 알고리즘과 프로토콜의 보안 요구에 따라 정하며, 특정 길이로 항상 절단해야 하는 것은 아니다. 또한 MAC만으로는 메시지의 기밀성이나 제3자에 대한 부인방지를 제공하지 않는다.

NoteBase

선지별 해설

① X — 틀린 표현은 '반드시 96비트 길이로 절단해야 한다'이다. MAC 값은 필요에 따라 절단할 수 있지만, 태그 길이는 사용 알고리즘과 프로토콜 및 요구 보안 수준에 따라 달라진다. 올바르게는 'MAC 값은 정해진 보안 요구와 규격에 따라 적절한 길이로 사용하거나 절단할 수 있다'이다.
② O — 수신자는 공유키 K로 MAC을 다시 계산하여 전송된 MAC과 비교한다. 값이 일치하면 전송 중 메시지가 변조되지 않았다는 무결성과, 공유키를 아는 주체가 생성했다는 데이터 출처 인증을 확인할 수 있다.
③ O — Nonce나 타임스탬프를 메시지와 함께 MAC의 인증 대상에 포함하면 각 전송의 신선성을 확인할 수 있으므로, 과거의 메시지와 MAC을 그대로 다시 보내는 재전송 공격을 탐지할 수 있다.
④ O — 안전한 MAC은 비밀키 K를 모르는 공격자가 임의의 새 메시지에 대해 검증을 통과하는 유효한 MAC 값을 위조하기 어렵도록 설계된다.

오답 포인트

①은 실제로 쓰일 수 있는 태그 길이인 96비트를 모든 MAC에 적용되는 절대 규칙처럼 제시한 것이 함정이다. '사용할 수 있다'와 '반드시 해야 한다'를 구분해야 한다. 또한 ②의 송신자 인증은 공유키 보유자에 대한 데이터 출처 인증이라는 뜻이며, 공개키 서명처럼 제3자에게 송신자를 증명하는 부인방지 기능을 뜻하지 않는다.

다시 나오면 이렇게 판단

MAC 선지는 먼저 '무결성·데이터 출처 인증'을 제공하는지 확인하고, 기밀성·부인방지를 MAC 자체의 기능이라고 하면 틀린 것으로 판단한다. 재전송 방지는 Nonce·타임스탬프 같은 신선성 값이 MAC의 인증 범위에 포함되는지 확인한다. 태그 길이는 특정 수치가 보편적으로 강제되는지가 아니라 해당 규격과 보안 수준에 따라 결정되는지를 본다.

암기 포인트

MAC은 무결성·출처 인증, Nonce·타임스탬프는 신선성, 태그 길이는 규격과 보안 수준에 따라 결정된다.

NoteBase

16. TLS 1.3에 대한 설명으로 가장 적절하지 않은 것은?

① TLS 1.3에서는 Handshake 과정에서 디피-헬만 키 교환을 사용하여 전방향 안전성(Forward Secrecy)을 기본적으로 제공한다.

② TLS 1.3에서는 서버 인증 시 X.509 인증서를 사용하며, 클라이언트는 이를 검증하여 서버의 신원을 확인한다.

③ TLS 1.3에서는 RSA 키 교환 방식이 제거되었으나, RSA 기반 전자서명은 여전히 사용될 수 있다.

④ TLS 1.3에서는 Handshake 과정에서 암호화되지 않은 서버의 X.509 인증서를 클라이언트에게 전송한다.

정답 4번

출제 포인트

TLS 1.3의 키 교환, 서버 인증, 전자서명, Handshake 메시지 암호화 범위를 구분하는 문제이다.

핵심 개념

TLS 1.3: 통신 상대를 인증하고 세션 키를 합의하여 통신을 보호하는 프로토콜이다. 인증서 기반 Handshake에서는 (EC)DHE로 키를 합의한 뒤 서버의 Certificate와 CertificateVerify 등의 인증 메시지를 Handshake 트래픽 키로 암호화한다.
전방향 안전성: 장기 비밀키가 나중에 유출되어도 과거 세션 키와 통신 내용이 함께 노출되지 않는 성질이다.
RSA의 역할: TLS 1.3에서는 RSA로 premaster secret을 암호화하는 정적 RSA 키 교환은 제거되었지만, RSA는 인증을 위한 전자서명 알고리즘으로 사용할 수 있다.

NoteBase

선지별 해설

① O — TLS 1.3은 정적 RSA·정적 DH 키 교환을 제거하고 공개키 기반 키 교환에 일회성 (EC)DHE를 사용하여 전방향 안전성을 제공한다. 다만 PSK만 사용하는 모드는 예외적으로 전방향 안전성을 제공하지 않으므로, 선지의 '기본적으로'라는 표현이 중요하다.
② O — 인증서 기반 서버 인증에서는 서버가 X.509 인증서 체인을 보내고, 클라이언트는 인증서의 유효성·신뢰 경로·서버 이름 등을 검증하여 서버의 신원을 확인한다.
③ O — TLS 1.3에서는 RSA 키 교환 방식이 제거되었지만 RSA 자체가 없어진 것은 아니다. RSA-PSS 등 RSA 기반 전자서명은 CertificateVerify를 통한 서버 인증에 사용할 수 있다.
④ X — 틀린 표현은 '암호화되지 않은 서버의 X.509 인증서를 전송한다'이다. 올바르게는 서버의 Certificate 메시지는 ServerHello 뒤에 합의된 Handshake 트래픽 키로 암호화되어 전송된다. 따라서 가장 적절하지 않은 설명은 ④이다.

오답 포인트

③의 'RSA 키 교환 제거'를 'RSA 전면 제거'로 확대 해석하거나, TLS 1.2의 Handshake 흐름을 떠올려 ④의 인증서가 평문이라고 판단하기 쉽다. TLS 1.3에서는 키 교환 방식과 서명 알고리즘을 분리하고, ServerHello 이후의 인증 메시지가 암호화된다는 점을 구분한다.

다시 나오면 이렇게 판단

TLS 1.3 문제에서는 먼저 기능을 키 교환과 인증으로 나눈다. 정적 RSA 키 교환은 제거되었지만 RSA 서명은 가능하며, ServerHello에서 공유 키 재료가 마련된 뒤 전송되는 Certificate 등 서버 인증 메시지는 암호화된다고 판단한다.

암기 포인트

TLS 1.3은 'RSA 키 교환은 제거, RSA 서명은 가능, 서버 인증서는 암호화'로 기억한다.

NoteBase

17. DNSSEC(Domain Name System Security Extensions)에 대한 설명으로 가장 적절한 것은?
① DNSSEC은 전자서명을 이용하여 DNS 데이터의 무결성과 출처 인증을 제공한다.
② DNSSEC은 DNS 응답 데이터를 암호화하여 기밀성을 제공한다.
③ DNSSEC은 공유 비밀키를 이용하여 DNS 서버 간 인증을 수행한다.
④ DNSSEC은 DNS 질의 자체를 보호하여 스니핑을 방지한다.

정답 1번

출제 포인트

DNSSEC이 제공하는 보안 속성이 DNS 데이터의 무결성과 출처 인증이며, 기밀성이나 도청 방지는 제공하지 않는다는 점을 묻는 문제이다.

핵심 개념

DNSSEC은 DNS 레코드에 대한 전자서명과 신뢰 체인을 검증하여 응답 데이터가 위조·변조되지 않았고 정당한 출처에서 제공되었음을 확인하는 DNS 보안 확장이다.
DNSSEC: 데이터 무결성·출처 인증 / 키워드: 전자서명, 공개키 검증, 신뢰 체인
전송 구간 암호화: 질의·응답의 기밀성 보호 / 키워드: DoT, DoH
공유 비밀키 기반 DNS 메시지 인증: 서버 등 당사자 간 거래 인증 / 대표 기술: TSIG

NoteBase

선지별 해설

① O — DNSSEC은 전자서명을 검증하여 DNS 데이터의 무결성과 데이터 출처 인증을 제공한다. 따라서 가장 적절한 설명이다.
② X — 틀린 표현은 'DNS 응답 데이터를 암호화하여 기밀성을 제공한다'이다. 올바르게는 DNSSEC은 응답 데이터에 전자서명을 적용해 무결성과 출처 인증을 제공하며, 응답 내용을 암호화하지 않으므로 기밀성은 제공하지 않는다.
③ X — 틀린 표현은 '공유 비밀키를 이용하여 DNS 서버 간 인증을 수행한다'이다. 올바르게는 DNSSEC은 서명 생성에 개인키를 사용하고 검증에 공개키를 사용한다. 공유 비밀키로 DNS 메시지의 당사자 간 인증과 무결성을 제공하는 방식은 대표적으로 TSIG이다.
④ X — 틀린 표현은 'DNS 질의 자체를 보호하여 스니핑을 방지한다'이다. 올바르게는 DNSSEC은 서명된 DNS 응답 데이터의 진위와 무결성을 검증하지만 질의·응답을 암호화하지 않으므로 스니핑 자체를 막지 못한다. 전송 구간의 기밀성은 DoT나 DoH와 같은 별도 기술이 담당한다.

오답 포인트

②와 ④는 '보안'이라는 말 때문에 DNSSEC도 암호화를 제공한다고 착각하게 만든다. DNSSEC의 전자서명은 데이터가 믿을 만한 출처에서 왔고 변조되지 않았는지를 확인할 뿐, 내용을 숨기지는 않는다. ③은 DNSSEC의 공개키 기반 서명 검증을 TSIG의 공유 비밀키 방식과 혼동하게 만든다.

다시 나오면 이렇게 판단

DNSSEC 선지에서는 '전자서명·무결성·출처 인증'이면 옳은 방향이고, '응답 암호화·기밀성·스니핑 방지'이면 틀린 방향으로 판단한다. 공유 비밀키가 제시되면 DNSSEC이 아니라 TSIG와의 혼동 여부를 확인한다.

암기 포인트

DNSSEC은 서명으로 진위와 무결성을 확인하고, 암호화로 내용을 숨기지는 않는다.

NoteBase

18. 웹 보안에서 사용하는 쿠키(Cookie)의 보안 속성에 대한 설명으로 가장 적절한 것은?
① HttpOnly 속성이 설정된 쿠키는 HTTPS 연결에서만 전송된다.
② Secure 속성이 설정된 쿠키는 클라이언트 측 스크립트에서 접근할 수 없다.
③ SameSite 속성은 교차 사이트 요청에서 쿠키 전송 여부를 제어할 수 있다.
④ 쿠키는 기본적으로 암호화되어 저장되므로 별도의 보호가 필요 없다.

정답 3번

출제 포인트

쿠키의 Secure, HttpOnly, SameSite 속성이 각각 전송 경로, 스크립트 접근, 교차 사이트 요청을 어떻게 제한하는지 구분하는 문제이다.

핵심 개념

Secure: 쿠키가 HTTPS 같은 보안 연결을 통해서만 전송되도록 제한한다. / 키워드: 전송 경로
HttpOnly: 자바스크립트와 같은 클라이언트 측 스크립트가 쿠키에 접근하지 못하게 한다. / 키워드: 스크립트 접근 차단
SameSite: 교차 사이트 요청에 쿠키를 함께 보낼지를 Strict, Lax, None 등의 값으로 제어한다. / 키워드: 교차 사이트 전송
쿠키 값은 기본적으로 암호화되어 저장되는 것이 아니므로 민감정보를 그대로 담아서는 안 된다.

선지별 해설

① X — ‘HttpOnly 속성이 설정된 쿠키는 HTTPS 연결에서만 전송된다’는 표현이 틀렸다. HTTPS 연결에서만 전송되도록 하는 속성은 Secure이다. 올바르게는 ‘Secure 속성이 설정된 쿠키는 HTTPS 같은 보안 연결에서만 전송된다’이다.
② X — ‘Secure 속성이 설정된 쿠키는 클라이언트 측 스크립트에서 접근할 수 없다’는 표현이 틀렸다. 스크립트 접근을 차단하는 속성은 HttpOnly이다. 올바르게는 ‘HttpOnly 속성이 설정된 쿠키는 클라이언트 측 스크립트에서 접근할 수 없다’이다.
③ O — SameSite 속성은 교차 사이트 요청에서 쿠키를 전송할지 여부를 제어하므로 적절한 설명이다.
④ X — ‘쿠키는 기본적으로 암호화되어 저장된다’는 표현이 틀렸다. 쿠키는 기본적으로 암호화되지 않으며, Secure·HttpOnly·SameSite 등 적절한 속성과 서버 측 보호 대책을 함께 적용해야 한다.

NoteBase

오답 포인트

①과 ②는 HttpOnly와 Secure의 기능을 서로 바꾸어 제시한 함정이다. 또한 Secure는 전송 경로를 제한할 뿐 쿠키 값을 암호화하거나 스크립트 접근을 막는 속성이 아니다.

다시 나오면 이렇게 판단

속성 이름을 보호 대상과 연결해 판단한다. 통신 경로가 HTTPS인지 묻는다면 Secure, 자바스크립트 접근을 묻는다면 HttpOnly, 교차 사이트 요청의 쿠키 전송을 묻는다면 SameSite에 해당한다.

암기 포인트

Secure는 전송 경로, HttpOnly는 스크립트 접근, SameSite는 교차 사이트 전송을 통제한다.

NoteBase

19. 웹 애플리케이션에서 CSRF(Cross-Site Request Forgery) 공격에 대한 설명으로 가장 적절한 것은?
① CSRF 공격은 주로 서버 측 데이터베이스 취약점을 이용한다.
② CSRF 토큰은 예측 불가능한 값으로 생성되어야 한다.
③ CSRF 공격은 암호화된 통신(HTTPS)을 사용하면 완전히 방지된다.
④ CSRF는 사용자의 비밀번호를 직접 탈취하는 공격이다.

정답 2번

출제 포인트

CSRF 공격의 작동 원리와 CSRF 토큰, HTTPS의 방어 범위를 구분하는 문제이다.

핵심 개념

CSRF(Cross-Site Request Forgery)는 공격자가 로그인된 사용자의 브라우저를 속여 사용자가 의도하지 않은 요청을 신뢰받는 웹 서비스에 보내게 하는 공격이다. 브라우저가 쿠키 등 인증 정보를 요청에 자동으로 포함한다는 점을 악용한다.
CSRF 토큰은 서버가 발급하고 요청마다 검증하는 비밀값으로, 공격자가 값을 알아내어 유효한 요청을 위조하기 어렵도록 예측 불가능하게 생성되어야 한다.
HTTPS는 전송 중인 데이터를 암호화하지만, 인증된 브라우저가 만든 원치 않는 요청 자체를 판별하지는 못한다.

NoteBase

선지별 해설

① X
틀린 표현은 '주로 서버 측 데이터베이스 취약점을 이용한다'이다. CSRF는 주로 브라우저가 쿠키 등 인증 정보를 자동으로 전송하는 특성과 서버가 요청의 정당한 출처를 충분히 검증하지 않는 점을 악용한다.

② O
CSRF 토큰은 공격자가 추측하거나 미리 구성할 수 없도록 충분히 무작위적이고 예측 불가능한 값으로 생성되어야 하며, 서버는 요청에 포함된 토큰의 유효성을 검증해야 한다.

③ X
틀린 표현은 'HTTPS를 사용하면 완전히 방지된다'이다. HTTPS는 통신 내용을 암호화하여 도청·변조를 막지만, 인증된 사용자의 브라우저에서 전송되는 위조 요청은 막지 못한다. 실제로는 CSRF 토큰 검증, SameSite 쿠키, Origin 또는 Referer 검증 등의 대책이 필요하다.

④ X
틀린 표현은 '사용자의 비밀번호를 직접 탈취하는 공격'이다. CSRF는 비밀번호를 직접 훔치는 공격이 아니라, 이미 인증된 사용자의 권한을 이용하여 비밀번호 변경·송금 같은 원치 않는 요청을 실행하게 하는 공격이다.

오답 포인트

③의 HTTPS를 만능 보안 대책으로 보는 것이 핵심 함정이다. HTTPS가 보호하는 것은 전송 경로이며, 요청이 사용자의 진짜 의사에 따른 것인지는 별도의 CSRF 방어로 확인해야 한다. ④처럼 CSRF를 피싱이나 자격 증명 탈취 공격과 혼동해서도 안 된다.

다시 나오면 이렇게 판단

선지에서 '인증된 브라우저가 원치 않는 요청을 전송한다'는 구조와 '예측 불가능한 토큰을 서버가 검증한다'는 설명을 찾으면 CSRF의 원리와 대책에 해당한다. 데이터베이스 취약점, HTTPS만으로 완전 방지, 비밀번호 직접 탈취라는 설명은 CSRF의 핵심과 다르다.

암기 포인트

CSRF는 인증 정보를 훔치는 공격이 아니라 인증된 요청을 위조하는 공격이며, 핵심 방어는 예측 불가능한 CSRF 토큰의 검증이다.

NoteBase

20. 시스템 관리자가 특정 파일에 대해 소유자만 읽기와 쓰기가 가능하도록 설정하려고 한다. 이때 사용할 수 있는 명령어로 가장 적절한 것은?
① chmod 777 file.txt
② chmod 644 file.txt
③ chmod 755 file.txt
④ chmod 600 file.txt

정답 4번

출제 포인트

이 문제는 chmod의 8진수 권한 표기에서 소유자·그룹·기타 사용자의 권한을 구분하여 설정할 수 있는지를 묻는다.

핵심 개념

chmod의 세 자리 숫자는 왼쪽부터 소유자, 그룹, 기타 사용자의 권한을 뜻한다. 각 자리에서 읽기는 4, 쓰기는 2, 실행은 1이며, 허용할 권한의 값을 더한다. 소유자에게만 읽기와 쓰기를 허용하면 소유자는 4+2=6, 그룹과 기타 사용자는 권한이 없으므로 각각 0이 되어 600이다.

선지별 해설

① X — 777은 소유자·그룹·기타 사용자 모두에게 읽기·쓰기·실행 권한을 부여한다. '소유자만 읽기와 쓰기 가능'으로 고치면 chmod 600 file.txt이다.
② X — 644는 소유자에게 읽기·쓰기 권한을 주지만 그룹과 기타 사용자에게도 읽기 권한을 준다. 그룹과 기타 사용자의 읽기 권한을 제거하면 chmod 600 file.txt이다.
③ X — 755는 소유자에게 읽기·쓰기·실행 권한을 주고 그룹과 기타 사용자에게 읽기·실행 권한을 준다. 소유자의 실행 권한과 그룹·기타 사용자의 모든 권한을 제거하면 chmod 600 file.txt이다.
④ O — 600은 소유자에게 읽기(4)와 쓰기(2) 권한만 부여하고, 그룹과 기타 사용자에게는 아무 권한도 부여하지 않으므로 요구 조건에 정확히 맞는다.

오답 포인트

②의 644도 소유자에게 읽기·쓰기를 허용하므로 맞는 것처럼 보이지만, 뒤의 44 때문에 그룹과 기타 사용자도 읽을 수 있다. 또한 '읽기와 쓰기 가능'은 실행 권한까지 허용한다는 뜻이 아니므로 소유자 자리는 7이 아니라 6이다.

NoteBase

다시 나오면 이렇게 판단

먼저 권한 대상을 소유자·그룹·기타 사용자 순서로 나누고, 각 대상에 대해 읽기 4, 쓰기 2, 실행 1을 더한다. '소유자만 읽기·쓰기'는 rw- --- ---이므로 숫자로 600이다.

암기 포인트

chmod는 소유자-그룹-기타 순서이며, r=4, w=2, x=1이다. 소유자만 rw이면 600이다.

NoteBase

21. 아래의 공격 시나리오에 대한 설명으로 가장 적절한 것은?

> 공격자는 특정 웹사이트에 악성 스크립트를 삽입하여 사용자 브라우저에서 실행되도록 하였고, 이를 통해 사용자의 세션 쿠키를 탈취하였다. 이후 탈취한 쿠키를 이용하여 정상 사용자로 가장하여 시스템에 접근하였다.

① Session Hijacking 공격으로, XSS를 통해 세션 정보를 탈취한 후 수행한 것이다.
② SQL Injection 공격으로, 데이터베이스를 조작한 것이다.
③ CSRF 공격으로, 사용자의 요청을 위조한 것이다.
④ DoS 공격으로, 시스템 자원을 고갈시킨 것이다.

정답 1번

출제 포인트

악성 스크립트로 세션 쿠키를 탈취한 뒤 정상 사용자로 가장하는 공격을 XSS와 세션 하이재킹의 연계로 식별하는 문제이다.

핵심 개념

XSS는 웹페이지에 삽입된 악성 스크립트가 사용자의 브라우저에서 실행되게 하는 공격이다.
세션 하이재킹은 탈취한 세션 식별자나 세션 쿠키를 이용해 피해자의 인증된 세션을 가로채는 공격이다.
SQL Injection은 입력값을 통해 악의적인 SQL 문을 주입하여 데이터베이스를 조회하거나 조작하는 공격이다.
CSRF는 로그인된 사용자의 브라우저가 공격자가 의도한 요청을 본인 의사와 다르게 보내도록 만드는 공격이다.
DoS는 과도한 요청이나 자원 소모를 유발하여 정상적인 서비스 이용을 방해하는 공격이다.

NoteBase

선지별 해설

① O — 악성 스크립트가 브라우저에서 실행되어 세션 쿠키를 탈취한 부분은 XSS이고, 탈취한 쿠키로 정상 사용자를 가장한 부분은 세션 하이재킹이다. 시나리오의 공격 과정과 정확히 일치한다.
② X — 틀린 부분은 'SQL Injection 공격으로 데이터베이스를 조작'했다는 표현이다. 실제로는 데이터베이스에 SQL 문을 주입한 것이 아니라 XSS로 세션 쿠키를 탈취한 뒤 세션 하이재킹을 수행한 것이다.
③ X — 틀린 부분은 'CSRF 공격으로 사용자의 요청을 위조'했다는 표현이다. 실제로는 인증된 사용자의 브라우저에 원치 않는 요청을 보내게 한 것이 아니라, 세션 쿠키를 탈취하여 피해자의 세션을 직접 가로챈 것이다.
④ X — 틀린 부분은 'DoS 공격으로 시스템 자원을 고갈'시켰다는 표현이다. 실제로는 서비스 가용성을 떨어뜨린 것이 아니라, 탈취한 세션 쿠키를 이용해 정상 사용자로 가장하여 시스템에 접근한 것이다.

오답 포인트

악성 스크립트가 등장했다는 사실만 보고 공격 전체를 XSS 하나로 끝내거나, 정상 사용자의 권한이 이용되었다는 이유만으로 CSRF와 혼동하기 쉽다. 이 시나리오에서는 XSS가 쿠키 탈취 수단이고, 탈취한 쿠키로 인증 세션을 가로챈 최종 공격이 세션 하이재킹이다.

다시 나오면 이렇게 판단

브라우저에서 악성 스크립트 실행은 XSS, 세션 쿠키 탈취 후 사용자 가장은 세션 하이재킹, 악성 SQL 문으로 DB 조작은 SQL Injection, 로그인 사용자의 의도하지 않은 요청 전송은 CSRF, 자원 고갈에 따른 서비스 장애는 DoS로 구분한다.

암기 포인트

XSS로 쿠키를 훔치고, 훔친 쿠키로 세션을 가로채면 세션 하이재킹이다.

NoteBase

22. 현재 디렉터리에 있는 파일과 하위 디렉터리 목록을 확인하는 명령어로 가장 적절한 것은?
① ls
② cd
③ pwd
④ mkdir

정답 1번

출제 포인트

현재 디렉터리의 파일과 하위 디렉터리 목록을 확인하는 명령어를 구별하는 문제이다.

핵심 개념

ls: 지정한 디렉터리의 내용을 나열하며, 경로를 생략하면 현재 디렉터리의 파일과 하위 디렉터리 목록을 보여준다.
cd: 현재 작업 디렉터리를 다른 디렉터리로 변경한다.
pwd: 현재 작업 디렉터리의 경로를 출력한다.
mkdir: 새로운 디렉터리를 생성한다.

선지별 해설

① O — ls는 디렉터리의 내용을 나열하는 명령어이므로 현재 디렉터리의 파일과 하위 디렉터리 목록을 확인할 때 사용한다.
② X — cd는 목록을 확인하는 명령어가 아니라 현재 작업 디렉터리를 변경하는 명령어이다. 올바르게는 현재 디렉터리의 목록 확인에 ls를 사용한다.
③ X — pwd는 목록을 확인하는 명령어가 아니라 현재 작업 디렉터리의 경로를 출력하는 명령어이다. 올바르게는 현재 디렉터리의 목록 확인에 ls를 사용한다.
④ X — mkdir는 목록을 확인하는 명령어가 아니라 새 디렉터리를 생성하는 명령어이다. 올바르게는 현재 디렉터리의 목록 확인에 ls를 사용한다.

오답 포인트

cd와 pwd도 디렉터리와 관련된 명령어이지만 기능이 다르다. '목록을 확인'한다는 표현은 디렉터리 이동이나 현재 경로 출력이 아니라 내용 나열을 뜻하므로 ls에 대응한다.

NoteBase

다시 나오면 이렇게 판단

문제의 동사를 기준으로 구별한다. 목록 나열은 ls, 디렉터리 이동은 cd, 현재 경로 출력은 pwd, 디렉터리 생성은 mkdir이다.

암기 포인트

ls는 list, cd는 change directory, pwd는 print working directory, mkdir는 make directory이다.

NoteBase

23. 공급망 공격(Supply Chain Attack)에 대한 설명으로 가장 적절한 것은?

① 공격자가 직접 사용자 컴퓨터를 해킹하여 데이터를 탈취하는 공격이다.

② 신뢰된 소프트웨어나 업데이트 경로를 악용하여 악성코드를 배포하는 공격이다.

③ 네트워크 트래픽을 가로채어 정보를 수집하는 공격이다.

④ 사용자에게 이메일을 보내 비밀번호를 입력하게 하는 공격이다.

정답 2번

출제 포인트

공급망 공격이 최종 사용자를 직접 공격하는 방식이 아니라, 신뢰받는 공급업체·소프트웨어·업데이트 경로를 먼저 침해하여 악성코드를 전달하는 공격임을 구별하는 문제이다.

핵심 개념

공급망 공격: 제품이나 서비스가 사용자에게 전달되는 공급 과정의 신뢰 관계를 악용하는 공격이다. 소프트웨어 공급업체, 개발·배포 시스템, 라이브러리 또는 정상 업데이트에 악성코드를 삽입해 다수의 최종 사용자에게 전파할 수 있다.

핵심 구별축은 '사용자를 직접 노리는가'가 아니라 '신뢰된 공급·업데이트 경로를 우회 통로로 이용하는가'이다.

NoteBase

선지별 해설

① X
공격자가 사용자 컴퓨터를 직접 해킹해 데이터를 빼내는 것은 직접 침해와 정보 유출에 대한 설명이다. 틀린 표현은 '직접 사용자 컴퓨터를 해킹'이다. 공급망 공격은 올바르게는 신뢰받는 공급업체나 소프트웨어 배포 경로를 먼저 침해해 사용자에게 악성코드를 전달하는 공격이다.

② O
신뢰된 소프트웨어나 정상 업데이트 경로에 악성코드를 삽입·배포하는 것은 공급망의 신뢰를 악용하는 전형적인 공급망 공격이다.

③ X
네트워크 트래픽을 가로채 정보를 수집하는 것은 스니핑 또는 도청형 공격에 해당한다. 틀린 표현은 이를 공급망 공격으로 본 부분이다. 올바르게는 공급망 공격은 공급업체나 개발·업데이트 경로를 침해해 악성코드를 유통하는 공격이다.

④ X
이메일로 사용자를 속여 비밀번호를 입력하게 하는 것은 피싱을 통한 자격 증명 탈취이다. 틀린 표현은 이를 공급망 공격으로 본 부분이다. 올바르게는 공급망 공격은 사용자를 직접 속이는 대신 신뢰된 제품·서비스의 공급 경로를 악용한다.

오답 포인트

①의 직접 해킹, ③의 트래픽 가로채기, ④의 피싱도 모두 정보보호 공격이지만 공급망 공격은 아니다. 공격의 결과가 악성코드 감염이나 정보 유출이라는 점보다, 악성코드가 '신뢰된 공급·업데이트 경로'를 통해 전달되는지를 기준으로 판단해야 한다.

다시 나오면 이렇게 판단

선지에서 공급업체, 개발 환경, 외부 라이브러리, 정상 소프트웨어, 업데이트 서버, 배포 경로와 같은 중간 신뢰 지점이 침해되었는지 확인한다. 이런 중간 경로를 거쳐 최종 사용자에게 피해가 확산되면 공급망 공격으로 판단한다.

암기 포인트

공급망 공격은 '사용자 직접 공격'이 아니라 '신뢰된 공급 경로를 먼저 오염시키는 공격'이다.

NoteBase

24. 「개인정보 보호법 시행령」에 따라 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용 또는 제공하려는 경우 고려해야 하는 사항으로 가장 적절하지 않은 것은?

① 당초 수집 목적과 관련성이 있는지 여부
② 정보주체의 이익을 부당하게 침해하는지 여부
③ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부
④ 익명정보가 다른 정보와 결합하여 개인을 식별할 수 있는지 여부

정답 4번

쟁점

이 문제는 개인정보처리자가 정보주체의 동의 없이 개인정보를 추가로 이용하거나 제공할 때 고려해야 하는 사항에 관한 문제이다. 핵심은 시행령에 열거된 네 가지 고려사항과 그 밖의 개념을 구별하는 것이다.

용어 풀이

개인정보의 추가적인 이용·제공은 이미 수집한 개인정보를 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체의 별도 동의 없이 이용하거나 제공하는 것을 말한다.

핵심 구분

「개인정보 보호법 시행령」 제14조의2 제1항은 ① 당초 수집 목적과의 관련성, ② 개인정보를 수집한 정황 또는 처리 관행에 비추어 본 추가 이용·제공의 예측 가능성, ③ 정보주체의 이익을 부당하게 침해하는지 여부, ④ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치 여부를 고려하도록 한다. 익명정보가 다른 정보와 결합되어 개인을 식별할 수 있는지는 이 조항에 열거된 고려사항이 아니다.

NoteBase

선지별 해설

① O
- 당초 수집 목적과 관련성이 있는지 여부는 시행령이 명시한 고려사항이다.

② O
- 정보주체의 이익을 부당하게 침해하는지 여부는 시행령이 명시한 고려사항이다.

③ O
- 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부는 시행령이 명시한 고려사항이다.

④ X
- 익명정보가 다른 정보와 결합되어 개인을 식별할 수 있는지 여부는 시행령 제14조의2 제1항의 고려사항이 아니다.
- 틀린 표현: 익명정보가 다른 정보와 결합하여 개인을 식별할 수 있는지 여부
- 올바른 표현: 개인정보를 수집한 정황 또는 처리 관행에 비추어 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부

오답 포인트

④의 '다른 정보와 결합하여 개인을 식별할 수 있는지'는 개인정보의 식별 가능성과 관련된 표현이어서 그럴듯하지만, 동의 없는 추가 이용·제공의 네 가지 고려사항에는 들어 있지 않다. 이 문항은 빠진 법정 고려사항인 '예측 가능성' 대신 식별 가능성 문구를 끼워 넣은 것이 함정이다.

다시 나오면 이렇게 판단

동의 없는 추가 이용·제공 문제에서는 '목적 관련성 → 예측 가능성 → 부당한 이익 침해 여부 → 가명처리·암호화 등 안전조치'의 네 항목과 선지를 대조한다. 이 네 항목 밖의 식별 가능성 문구는 별개의 개념으로 판단한다.

암기 포인트

추가 이용·제공의 네 기준은 '관련성·예측 가능성·이익 침해·안전조치'이다.

NoteBase

25. 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 분야에 대한 설명으로 가장 적절하지 않은 것은?

① 위험관리는 조직이 자산, 위협, 취약점을 식별하고 위험을 평가·처리하는 과정을 포함한다.

② 접근통제는 사용자 인증, 권한 관리, 접근기록 등을 통해 시스템 접근을 통제하는 것을 포함한다.

③ 암호화 적용은 모든 정보 자산에 대해 반드시 동일한 암호 알고리즘을 적용하도록 요구한다.

④ 시스템 및 서비스 운영관리는 이상 행위를 탐지하고 대응하기 위한 기록 및 분석 활동을 포함한다.

정답 3번

출제 포인트

ISMS-P 보호대책에서 위험관리, 접근통제, 암호화, 시스템 및 서비스 운영관리의 목적과 적용 원칙을 구별하는 문제이다.

핵심 개념

위험관리는 정보자산과 위협·취약점을 식별하고 위험을 평가한 뒤 적절한 처리 방안을 정하는 과정이다.
접근통제는 인증, 권한 부여·관리, 접근기록 등을 통해 허가된 사용자만 시스템과 정보에 접근하도록 제한하는 활동이다.
암호화는 중요도, 법적 요구, 위험 수준, 처리 환경 등을 고려해 대상과 방식 및 안전한 알고리즘을 정하여 적용하는 보호수단이다. 모든 정보자산에 하나의 암호 알고리즘을 획일적으로 적용하는 것이 아니다.
시스템 및 서비스 운영관리는 로그와 이상 징후의 분석·대응 등 운영 중 발생하는 보안 위험을 지속적으로 통제하는 활동이다.

NoteBase

선지별 해설

① O — 위험관리는 조직의 정보자산, 위협, 취약점을 식별하고 위험의 크기를 평가한 후 회피·감소·전가·수용 등의 방식으로 처리하는 과정을 포함한다.
② O — 접근통제에는 사용자 인증, 권한의 부여·변경·말소, 접근기록의 생성·점검 등이 포함되며 이를 통해 시스템 접근을 통제한다.
③ X — 틀린 표현은 '모든 정보 자산'과 '반드시 동일한 암호 알고리즘'이다. 올바르게는 보호할 정보의 중요도와 위험, 법적 요구, 시스템 환경을 고려하여 암호화 대상을 정하고 목적에 적합한 안전한 암호 알고리즘과 키 관리 방식을 적용한다.
④ O — 시스템 및 서비스의 운영 과정에서는 로그와 이상 행위를 기록·분석하고 보안사고 징후를 탐지하여 대응하는 활동이 필요하다.

오답 포인트

③은 '암호화는 중요하다'는 맞는 취지에 '모든 자산'과 '동일한 알고리즘'이라는 획일적 요구를 섞었다. ISMS-P 보호대책은 자산의 중요도와 위험에 맞춘 차등 적용을 전제로 하므로 '모든', '반드시', '동일한'과 같은 절대 표현을 주의해야 한다.

다시 나오면 이렇게 판단

각 선지가 통제의 목적에 맞는지 먼저 확인하고, 보안조치를 모든 자산에 같은 방식으로 적용한다고 단정하는 표현은 위험 기반의 차등 적용 원칙에 어긋나는지 판단한다.

암기 포인트

위험은 식별·평가·처리, 접근은 인증·권한·기록, 암호화는 중요도와 위험에 맞게 차등 적용, 운영은 기록·탐지·대응으로 정리된다.

NoteBase