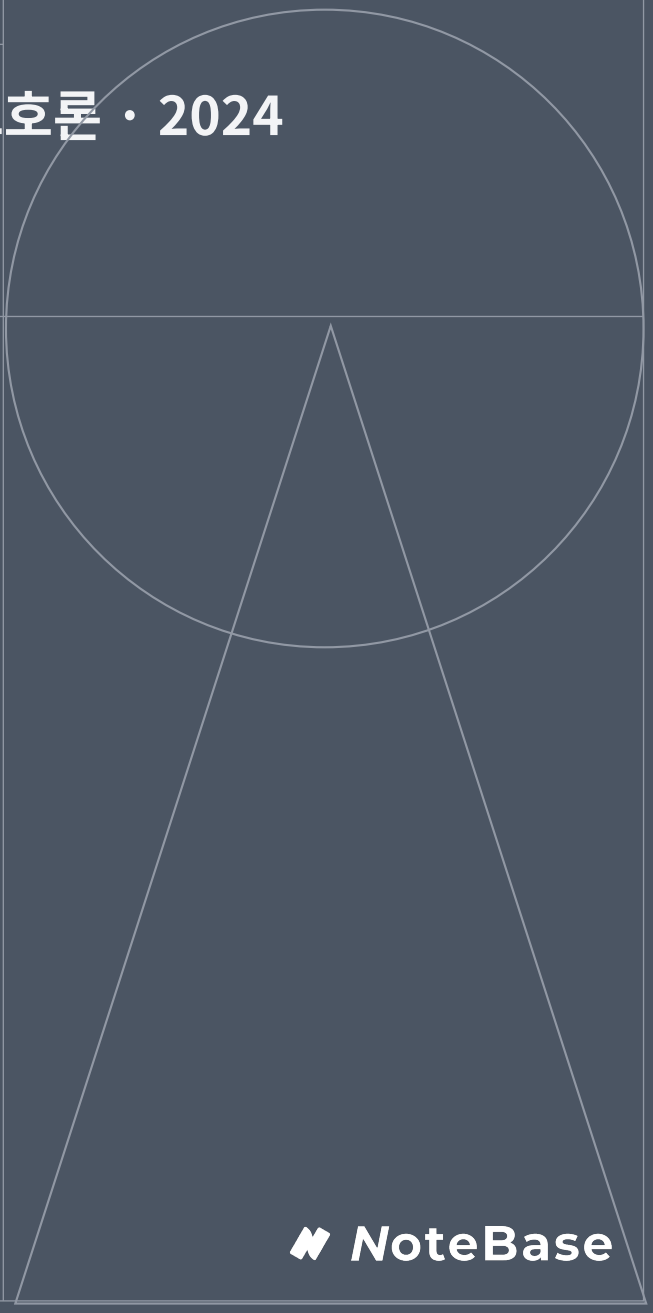
기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2024

공무원/법원직/9급 · 정보보호론 · 2024

문 1. 대표적인 블록암호인 DES, Triple DES, AES에 관한 다음 설명 중 가장 옳지 않은 것은?

① DES는 Feistel 구조를 기반으로 설계되었으며, AES는 Substitution Permutation Network 구조를 기반으로 설계가 되었다.

② Triple DES는 DES의 암호화 과정을 각각 다른 암호화 키로 3회 수행하는데, 효율을 높이기 위해 첫 번째와 두 번째 암호화 키를 동일하게 사용하도록 권장하고 있다.

③ AES의 암호화 과정은 마지막 라운드를 제외한 모든 라운드가 동일한 함수로 설계되었다.

④ AES는 안전성의 정도에 따라 키의 길이가 128, 192, 256비트를 가질 수 있으며, 키의 길이에 따라 실행하는 라운드 수가 각각 10, 12, 14라운드로 다르다.

정답 2번

출제 포인트

DES·Triple DES·AES의 구조, 키 운용 방식, AES의 라운드 구성을 구별하는 문제이다.

핵심 개념

DES는 64비트 블록을 처리하고 실질적으로 56비트 키를 사용하는 Feistel 구조의 블록암호이다.
Triple DES는 DES를 EDE, 즉 암호화-복호화-암호화 순서로 세 번 적용하며, 2키 방식에서는 첫 번째와 세 번째 단계에 같은 키를 사용한다.
AES는 128비트 블록을 처리하는 SPN 구조의 블록암호이며, 키 길이에 따라 라운드 수가 달라진다.

선지별 해설

① O — DES는 Feistel 구조이고 AES는 치환과 순열을 반복하는 SPN 구조이므로 옳다.
② X — 틀린 표현은 '암호화 과정을 각각 다른 암호화 키로 3회 수행' 및 '첫 번째와 두 번째 암호화 키를 동일하게 사용'이다. Triple DES의 대표적 처리는 암호화-복호화-암호화의 EDE 방식이며, 2키 방식은 첫 번째와 세 번째 단계에 같은 키를 사용하여 K1-K2-K1로 운용한다.
③ O — AES의 일반 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey로 구성되지만 마지막 라운드에서는 MixColumns가 제외되므로 옳다.
④ O — AES는 128·192·256비트 키를 지원하며, 각 키 길이에 따른 라운드 수는 각각 10·12·14회이므로 옳다.

NoteBase

오답 포인트

②는 '세 번 적용한다'는 점만 보고 맞는 설명처럼 느끼게 한다. 그러나 Triple DES는 단순히 서로 다른 키로 암호화를 세 번 하는 방식이 아니라 EDE 순서를 사용하며, 2키 방식에서 반복되는 키의 위치도 첫 번째와 두 번째가 아니라 첫 번째와 세 번째이다.

다시 나오면 이렇게 판단

DES는 Feistel, AES는 SPN으로 구조를 먼저 구분한다. Triple DES는 EDE와 K1-K2-K1을 확인하고, AES는 128·192·256비트 키와 10·12·14라운드의 대응 및 마지막 라운드의 MixColumns 생략을 확인한다.

암기 포인트

DES는 Feistel, AES는 SPN, 2키 Triple DES는 EDE의 K1-K2-K1, AES 키·라운드는 128-10·192-12·256-14이다.

NoteBase

문 2. 네트워크 서비스 거부 공격 기법에 관한 다음 설명 중 가장 옳지 않은 것은?

① Slowloris 공격은 HTTP 헤더 정보를 비정상적으로 조작하여 웹서버가 온전한 헤더 정보가 올 때까지 기다리게 하는 공격이다.

② Mail Bomb은 사용자에게 할당된 디스크 공간 이상의 메일을 보내어 더 이상 메일을 받을 수 없게 하는 공격이다.

③ Teardrop 공격은 UDP와 TCP 패킷의 시퀀스 넘버를 조작하여 공격 시스템에 과부하를 일으키는 공격이다.

④ Land 공격은 패킷 전송 출발지 IP 주소와 목적지 IP 주소의 값을 다르게 설정하여 공격 대상에게 패킷을 보내는 공격이다.

정답 4번

출제 포인트

서비스 거부 공격마다 자원을 고갈시키는 방식과 패킷에서 조작하는 필드가 어떻게 다른지를 구별하는 문제이다.

핵심 개념

Slowloris는 불완전한 HTTP 요청을 오래 유지하여 웹 서버의 동시 연결 자원을 소진시키는 공격이다.
Mail Bomb은 대량의 전자우편으로 수신자의 사서함 용량을 소진시키는 공격이다.
Teardrop은 서로 겹치거나 비정상적인 IP 단편 정보를 보내 재조합 과정에 장애나 과부하를 일으키는 공격이다.
LAND는 출발지와 목적지의 IP 주소를 공격 대상의 동일한 주소로 위조하여 대상 시스템이 자기 자신과 통신하게 만드는 공격이다.

선지별 해설

① O — Slowloris는 완결되지 않은 HTTP 헤더를 조금씩 보내 연결을 계속 열어 둔다. 웹 서버는 나머지 헤더를 기다리면서 연결 자원을 점유하므로 설명이 옳다.
② O — Mail Bomb은 사서함의 할당 용량을 넘을 정도로 많은 메일을 보내 저장 공간을 고갈시키고 정상 메일의 수신을 방해하므로 설명이 옳다.
③ O — Teardrop의 핵심은 UDP 또는 TCP 데이터가 실린 IP 패킷의 단편을 서로 겹치게 하거나 Fragment Offset 등 단편화 정보를 비정상적으로 조작하여 재조합 과정에 과부하나 오류를 일으키는 것이다. 이 선지의 '시퀀스 넘버'는 엄밀한 프로토콜 필드명이 아니며, 시험 문맥에서는 IP 단편의 Fragment Offset 조작을 가리킨다.
④ X — 틀린 표현은 '출발지 IP 주소와 목적지 IP 주소의 값을 다르게 설정'이다. LAND 공격은 두 IP 주소를 다르게 만드는 것이 아니라 출발지와 목적지 IP 주소를 공격 대상의 동일한 주소로 설정한다. 구현에 따라 출발지와 목적지 포트도 같게 위조하여 대상이 자기 자신에게 응답하게 만든다.

NoteBase

오답 포인트

LAND를 일반적인 IP 스푸핑처럼 출발지와 목적지를 다르게 위조하는 공격으로 착각하기 쉽다. 이 공격을 구별하는 결정적 표현은 '출발지와 목적지가 동일한 공격 대상 주소'이다. 또한 ③의 '시퀀스 넘버'는 엄밀한 프로토콜 필드명이 아니며, 시험 문맥에서는 IP 단편 재조합에 쓰이는 Fragment Offset 조작을 가리키는 표현으로 판단한다.

다시 나오면 이렇게 판단

공격명과 고갈·조작 대상을 짝지어 판단한다. Slowloris는 HTTP 연결, Mail Bomb은 사서함 용량, Teardrop은 IP 단편 재조합 정보, LAND는 출발지·목적지의 동일한 IP 주소가 핵심이다.

암기 포인트

Slowloris는 느린 미완성 헤더, Mail Bomb은 사서함 폭탄, Teardrop은 겹친 IP 조각, LAND는 출발지와 목적지가 같은 주소이다.

NoteBase

문 3. NAC(Network Access Control) 시스템에 관한 다음 설명 중 가장 옳지 않은 것은?

① 네트워크에 접근하는 접속 단말의 보안성을 검증하여 보안성을 강제화하고 접속을 통제할 수 있는 보안 인프라이다.

② 사용 단말이 내부 네트워크에 접근하기 전에 보안 정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 보안 솔루션이다.

③ NAC는 접근제어, 인증, 무결성 체크, 유해 트래픽 탐지 및 차단 기능을 제공한다.

④ NAC의 접근 제어 및 인증 기능은 장치에 부여된 고유한 장치명을 기반으로 수행되며, 등록된 장치명만 네트워크에 접속할 수 있게 허용한다.

정답 4번

출제 포인트

NAC의 목적과 주요 기능, 그리고 단말 식별에 사용하는 정보를 구별하는 문제이다.

핵심 개념

NAC(Network Access Control)는 단말이 네트워크에 접속하기 전이나 접속하는 과정에서 사용자·단말의 신원과 보안 정책 준수 여부를 확인하고, 그 결과에 따라 접속을 허용·차단·격리하는 보안 체계이다. 단말 식별에는 일반적으로 MAC 주소, IP 주소, 사용자 인증 정보 등 정책에 정해진 식별 정보가 활용되며, 장치명만을 기준으로 삼지 않는다.

선지별 해설

① O — NAC는 접속 단말의 보안 상태를 점검하고, 정책을 충족하지 못한 단말의 접속을 제한하여 보안 정책을 강제하는 인프라이다.
② O — 단말이 내부 네트워크에 접근할 때 백신 설치 여부, 보안 패치 상태 등 정책 준수 여부를 검사하고 그 결과에 따라 접속을 통제한다.
③ O — NAC는 단말과 사용자의 접근 제어·인증, 보안 상태 및 무결성 점검을 수행하며, 정책에 어긋나는 트래픽이나 단말을 탐지하여 차단할 수 있다.
④ X — 틀린 표현은 '고유한 장치명을 기반으로 수행되며, 등록된 장치명만'이다. 장치명은 변경되거나 중복될 수 있으므로 NAC의 접근 제어와 인증이 장치명만을 기준으로 수행되는 것은 아니다. 올바르게는 MAC 주소, IP 주소, 사용자 인증 정보 등 정책에 정해진 식별 정보를 바탕으로 단말과 사용자를 식별하고 접속을 통제한다고 해야 한다.

오답 포인트

④의 '고유한 장치명'이라는 표현이 함정이다. 장치명은 단말을 표시하는 이름일 뿐 항상 고유하거나 신뢰할 수 있는 접근 제어 식별자가 아니며, NAC는 여러 식별 정보와 보안 상태를 종합하여 정책을 적용한다.

NoteBase

다시 나오면 이렇게 판단

NAC 선지는 '접속 전후의 신원·보안 상태 검사 → 정책에 따른 허용·차단·격리'의 흐름에 맞는지 확인한다. 특정 장치명 하나만으로 인증과 접근 제어가 이루어진다고 단정하면 틀린 설명으로 판단한다.

암기 포인트

NAC는 단말 이름 등록제가 아니라, 신원과 보안 상태를 검사하여 네트워크 접속을 통제하는 체계이다.

NoteBase

문 4. UTM(Unified Threat Management)과 ESM(Enterprise Security Management)에 관한 다음 설명 중 가장 옳지 않은 것은?

① UTM은 단일장비로 다양한 보안 기능을 하나의 장비로 통합하여 제공할 수 있다.

② UTM은 장애 발생 시 다른 보안 기능에 영향을 주지 않는다.

③ ESM은 기업과 기관의 보안 정책을 반영하고 다양한 보안 시스템을 관제, 운영, 관리함으로써 조직의 보안 목적을 효율적으로 실현하는 시스템이다.

④ ESM은 통합보안관제를 위해 구축된 다양한 보안 솔루션과 보안 장비에서 발생하는 로그와 보안 이벤트를 취합하고 이들 간에 상호 연관 분석을 함으로써 실시간 보안 위협을 파악하고 대응한다.

정답 2번

출제 포인트

UTM의 보안 기능 통합 방식과 단일 장애 지점이라는 한계, ESM의 중앙 통합관제 기능을 구분하는 문제이다.

핵심 개념

UTM: 방화벽, 침입 탐지·방지, 악성코드 차단 등 여러 보안 기능을 하나의 장비에 통합한 시스템이다. 관리가 편리하지만 장비 하나의 장애가 통합된 여러 보안 기능에 함께 영향을 줄 수 있다.
ESM: 여러 보안 장비와 솔루션의 로그·이벤트를 중앙에서 수집하고 상호 연관 분석하여 조직 전체의 보안 상태를 통합 관제·운영·관리하는 시스템이다.
UTM은 기능을 한 장비에 통합하고, ESM은 여러 장비에서 나온 보안 정보를 중앙에서 통합 관리한다.

선지별 해설

① O — UTM은 여러 보안 기능을 단일 장비에 통합하여 제공할 수 있으므로 옳다.
② X — 틀린 표현은 '장애 발생 시 다른 보안 기능에 영향을 주지 않는다'이다. 여러 기능이 한 장비에 통합되어 있으므로 장비 장애가 발생하면 다른 보안 기능도 함께 중단되거나 영향을 받을 수 있다. 올바르게는 'UTM은 단일 장비의 장애가 통합된 여러 보안 기능에 영향을 줄 수 있다'이다.
③ O — ESM은 조직의 보안 정책을 바탕으로 다양한 보안 시스템을 중앙에서 관제·운영·관리하여 보안 목적을 효율적으로 달성하는 시스템이므로 옳다.
④ O — ESM은 여러 보안 솔루션과 장비의 로그·보안 이벤트를 수집하고 상호 연관 분석하여 실시간 위협을 탐지하고 대응하므로 옳다.

오답 포인트

UTM의 '통합'이라는 장점을 기능 간 장애 격리까지 보장하는 것으로 오해하기 쉽다. ②의 '영향을 주지 않는다'는 표현이 함정이며, 한 장비에 기능이 집중될수록 장비 자체가 단일 장애 지점이 될 수 있다.

NoteBase

다시 나오면 이렇게 판단

‘여러 기능을 한 장비에 통합’하면 UTM, ‘여러 장비의 로그와 이벤트를 중앙에서 수집·연관 분석’하면 ESM으로 판단한다. UTM의 장애 관련 선지는 단일 장비 고장이 여러 통합 기능에 함께 영향을 줄 수 있는지를 확인한다.

암기 포인트

UTM은 기능 통합 장비, ESM은 로그·이벤트 통합 관제이다. UTM은 편리하지만 단일 장애 지점이 될 수 있다.

NoteBase

문 5. 크로스사이트 스크립트 공격과정을 순서대로 바르게 나열한 것은?

ㄱ. 일반 사용자 PC의 보안 취약점이 외부에 전달된다.
ㄴ. 일반 사용자가 웹서버에 접속하여 웹서버에 저장된 악성 코드를 내려받는다.
ㄷ. XSS 취약점이 있는 웹 서버에 악성코드를 업로드한다.
ㄹ. 공격자는 추가적인 보안 공격을 시작한다.
ㅁ. 일반 사용자의 PC에서 악성코드가 실행된다.

① ㄷ - ㄱ - ㄴ - ㅁ - ㄹ
② ㄷ - ㄴ - ㅁ - ㄱ - ㄹ
③ ㄷ - ㄴ - ㄱ - ㅁ - ㄹ
④ ㄷ - ㅁ - ㄱ - ㄴ - ㄹ

정답 2번

출제 포인트

저장형 크로스사이트 스크립트(XSS) 공격에서 악성 코드가 웹 서버에 저장된 뒤 사용자의 브라우저에서 실행되고, 그 결과가 공격자에게 전달되는 흐름을 묻는 문제이다.

올바른 순서

1. ㄷ — 공격자가 XSS 취약점이 있는 웹 서버에 악성 코드를 업로드한다.
2. ㄴ — 일반 사용자가 웹 서버에 접속하면서 저장된 악성 코드를 내려받는다.
3. ㅁ — 내려받은 악성 코드가 일반 사용자의 PC에서 실행된다.
4. ㄱ — 실행된 악성 코드에 의해 일반 사용자 PC의 보안 취약점 정보가 외부로 전달된다.
5. ㄹ — 공격자는 전달받은 정보를 바탕으로 추가적인 보안 공격을 시작한다.

왜 이 순서인가: 악성 코드가 실행되어야 사용자 PC의 정보가 외부로 전달될 수 있고, 공격자는 그 정보를 받은 뒤 추가 공격을 시작할 수 있기 때문이다.

NoteBase

선지별 해설

① X — ‘ㄱ - ㄴ’의 선후관계가 틀렸다. 사용자가 악성 코드를 내려받기 전에 PC의 보안 취약점 정보가 전달될 수 없다. 올바르게는 ‘ㄷ - ㄴ - ㅁ - ㄱ - ㄹ’이다.

② O — 악성 코드 업로드, 사용자 접속과 다운로드, 사용자 PC에서의 실행, 보안 취약점 정보의 외부 전달, 추가 공격의 순서가 올바르다.

③ X — ‘ㄱ - ㅁ’의 선후관계가 틀렸다. 악성 코드가 먼저 실행되어야 PC의 보안 취약점 정보가 외부로 전달된다. 올바르게는 ‘ㄷ - ㄴ - ㅁ - ㄱ - ㄹ’이다.

④ X — ‘ㅁ - ㄴ’의 선후관계가 틀렸다. 웹 서버에 저장된 악성 코드를 사용자가 먼저 내려받아야 사용자 PC에서 실행될 수 있다. 올바르게는 ‘ㄷ - ㄴ - ㅁ - ㄱ - ㄹ’이다.

오답 포인트

ㄱ의 정보 전달 시점을 악성 코드 실행 전으로 착각하기 쉽다. 이 문항에서는 다운로드가 실행보다 앞서고, 실행이 정보 전달보다 앞선다는 두 선후관계가 정답을 가른다.

다시 나오면 이렇게 판단

XSS 공격 절차는 공격 코드 삽입 → 피해자의 접속과 코드 수신 → 피해자 환경에서 코드 실행 → 정보 유출 → 후속 공격의 인과관계로 판단한다.

암기 포인트

삽입-수신-실행-유출-후속 공격의 순서이다.

NoteBase

문 6. 정보보호제품 평가·인증 제도에 관한 다음 설명 중 가장 옳지 않은 것은?

① 정보보호제품 평가 인증제도는 지능정보화 기본법 제58조 (정보보호시스템에 관한 기준 고시 등)에 근거한다

② 공통평가기준(Common Criteria, CC)는 보증의 요구를 구조화하기 위해 가장 엄격한 보증 증거인 EAL 1부터 가장 엄격하지 않은 보증 증거인 EAL 7까지 7개의 평가 보증 수준으로 보증 등급을 정의하고 있다.

③ 보호 프로파일(PP)은 정보 제품이 갖추어야 할 공통적인 보안 요구사항을 모아 놓은 것이다.

④ IT보안인증사무국은 정보보호제품 평가·인증제도에 지정된 CC 인증기관이다.

정답 2번

쟁점

이 문제는 정보보호제품 평가·인증 제도의 법적 근거와 공통평가기준(CC)의 핵심 요소에 관한 문제이다. 핵심은 평가보증등급(EAL)의 숫자가 커질수록 보증 수준과 평가의 엄격성이 높아진다는 점을 구별하는 것이다.

용어 풀이

평가보증등급(EAL) = 정보보호제품의 보안기능이 요구대로 구현되었는지를 얼마나 엄격하고 깊게 평가했는지 나타내는 보증 수준이다.
보호 프로파일(PP) = 특정 제품 유형이나 사용 환경에 공통으로 필요한 보안 요구사항을 구현 방식과 독립적으로 정리한 문서이다.

핵심 구분

공통평가기준은 EAL1부터 EAL7까지 7개의 평가보증등급을 두며, EAL1은 기본적인 보증 수준이고 EAL7은 가장 높은 보증 수준이다. 등급이 높아질수록 평가의 엄격성·범위·깊이가 커지지만, 제품에 더 많은 보안기능이 있다는 뜻은 아니다. 정보보호제품 평가·인증 제도는 지능정보화 기본법 제58조와 같은 법 시행령 제51조를 근거로 운영되며, 관련 고시에 따라 IT보안인증사무국이 인증기관 역할을 수행한다.

NoteBase

선지별 해설

① O
정보보호제품 평가·인증 제도는 지능정보화 기본법 제58조와 같은 법 시행령 제51조를 법적 근거로 운영되므로 옳다.

② X
EAL의 높고 낮음을 반대로 설명했다. EAL은 숫자가 커질수록 보증 수준이 높아지므로 EAL1이 가장 기본적인 수준이고 EAL7이 가장 엄격하고 높은 수준이다.
틀린 표현: '가장 엄격한 보증 증거인 EAL1부터 가장 엄격하지 않은 보증 증거인 EAL7까지'
올바른 표현: '가장 기본적인 보증 수준인 EAL1부터 가장 엄격하고 높은 보증 수준인 EAL7까지'이다.

③ O
보호 프로파일(PP)은 특정 제품 유형이나 환경에 공통으로 요구되는 보안 요구사항을 모아 정의한 문서이므로 옳다.

④ O
IT보안인증사무국은 관련 고시에 따라 정보보호제품의 평가 결과를 인증하는 CC 인증기관 역할을 수행하므로 옳다. 평가를 직접 수행하는 CC 평가기관과 구별된다.

오답 포인트

②의 EAL 번호와 보증 수준의 방향을 뒤집은 표현이 함정이다. EAL은 숫자가 작을수록 엄격한 등급이 아니라, EAL1에서 EAL7로 갈수록 보증 수준이 높아진다. 또한 높은 EAL은 평가의 엄격성이 높다는 뜻이지 보안기능의 종류가 더 많다는 뜻은 아니다.

다시 나오면 이렇게 판단

EAL 선지는 먼저 숫자의 방향을 확인한다. EAL1은 기본 수준, EAL7은 최고 수준으로 판단한다. 이어서 평가기관은 제품을 평가하고 인증기관인 IT보안인증사무국은 평가 결과를 인증한다는 역할 구분을 적용한다.

암기 포인트

EAL은 1에서 7로 갈수록 보증이 강해진다. PP는 공통 보안 요구사항, IT보안인증사무국은 인증기관이다.

NoteBase

문 7. 윈도우 운영체제에서 사용하는 주요 그룹에 관한 다음 설명 중 가장 옳지 않은 것은?

① Administrators: 대표적인 관리자 그룹으로 윈도우 시스템의 모든 권한을 가지고 있으며, 사용 가능한 자원에 대한 권한을 설정할 수 있다.

② Power Users: 로컬 컴퓨터에서 Administrators 그룹이 가진 대부분의 권한을 가지며, 해당 컴퓨터 밖의 네트워크에서는 일반 사용자로 존재한다.

③ Users: 대부분의 사용자가 속하는 그룹으로, 네트워크를 통하여 서버나 다른 도메인 구성 요소에 로그인이 가능하다.

④ Guests: 윈도우 시스템에서 네트워크를 통하여 서버에 로그인할 수는 없으나, 서버로의 로컬 로그인은 가능하다.

정답 4번

출제 포인트

윈도우의 기본 로컬 그룹별 권한 범위와 로컬·네트워크 로그온 가능 여부를 구분하는 문제이다.

핵심 개념

Administrators는 시스템의 모든 권한을 가진 관리자 그룹이다. Power Users는 Administrators보다 제한적이지만 일반 사용자보다 넓은 로컬 관리 권한을 가진다. Users는 일반적인 작업과 네트워크 자원 이용이 가능한 표준 사용자 그룹이다. Guests는 임시·제한적 사용자를 위한 그룹으로, 서버에 로컬로 로그온할 권한은 없지만 네트워크를 통한 접근은 가능하다.

선지별 해설

① O — Administrators는 대표적인 관리자 그룹으로 시스템 전반의 권한을 가지며, 자원에 대한 접근 권한을 설정할 수 있다.
② O — Power Users는 로컬 컴퓨터에서 Administrators의 권한 대부분을 행사할 수 있지만, 다른 컴퓨터나 네트워크에서는 일반 사용자 수준으로 취급된다.
③ O — Users는 일반 사용자가 속하는 그룹으로, 네트워크를 통해 서버나 다른 도메인 구성 요소에 로그온할 수 있다.
④ X — '네트워크를 통한 서버 로그온은 불가능하고 로컬 로그온은 가능하다'는 부분이 반대로 서술되었다. Guests는 네트워크를 통해 서버에 접근할 수 있지만 서버에 로컬로 로그온할 수는 없다.

오답 포인트

④는 Guests의 제한이 적용되는 로그온 방식을 서로 뒤바꾼 선지이다. 'Guest는 제한된 계정'이라는 인상만으로 네트워크 로그온도 불가능하다고 판단하면 함정에 빠진다.

NoteBase

다시 나오면 이렇게 판단

그룹 문제에서는 먼저 권한의 크기를 Administrators, Power Users, Users, Guests 순으로 구분하고, Guests의 경우 네트워크 접근 가능과 로컬 로그온 불가를 별도로 확인한다.

암기 포인트

Guests는 네트워크 접근 가능, 서버 로컬 로그온 불가이다.

NoteBase

문 8. 네트워크 OSI(Open System Interconnection) 7계층에 관한 다음 설명 중 가장 적절한 것은?

① 데이터 링크 계층(Data Link Layer)은 실제 장치를 연결하기 위한 전기적·물리적 세부 사항을 정의한 계층이다.

② 네트워크 계층(Network Layer)은 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있게 해주는 계층이다.

③ 전송 계층(Transport Layer)은 여러 개의 노드를 거치는 경우 경로를 찾아주는 역할을 하는 계층이다.

④ 세션 계층(Session Layer)은 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공하는 계층이다.

정답 4번

출제 포인트

OSI 7계층에서 물리 계층, 데이터 링크 계층, 네트워크 계층, 전송 계층, 세션 계층의 역할을 구분하는 문제이다.

핵심 개념

물리 계층은 전기적·기계적 신호와 전송 매체 등 실제 연결 규격을 다룬다. 데이터 링크 계층은 직접 연결된 인접 노드 사이의 프레임 전송과 물리 주소, 오류 검출 등을 담당한다. 네트워크 계층은 여러 네트워크를 거쳐 목적지까지 가는 경로 선택과 패킷 전달을 담당한다. 전송 계층은 양 끝단 프로세스 사이의 종단 간 데이터 전송과 신뢰성·흐름 제어 등을 담당한다. 세션 계층은 응용 프로세스 사이의 대화 연결을 설정·유지·종료하고 통신을 관리한다.

선지별 해설

① X — '전기적·물리적 세부 사항을 정의'한다는 부분이 틀렸다. 이는 물리 계층의 역할이며, 데이터 링크 계층은 인접 노드 사이에서 프레임을 전달하고 물리 주소 지정과 오류 검출 등을 수행한다.
② X — '양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 한다'는 부분이 틀렸다. 종단 간 신뢰성 있는 데이터 전송은 전송 계층의 역할이며, 네트워크 계층은 경로 선택과 패킷 전달을 담당한다.
③ X — '여러 개의 노드를 거칠 때 경로를 찾는다'는 부분이 틀렸다. 이는 네트워크 계층의 역할이며, 전송 계층은 양 끝단 프로세스 사이의 종단 간 전송을 담당한다.
④ O — 세션 계층은 양 끝단 응용 프로세스 사이의 세션을 설정·유지·종료하며 대화와 통신을 관리하는 방법을 제공한다.

오답 포인트

1~3번은 각 계층의 역할을 한 계층씩 바꾸어 놓았다. 특히 '전기적·물리적'은 물리 계층, '경로 선택'은 네트워크 계층, '종단 간 신뢰성'은 전송 계층이라는 대응을 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

선지의 핵심 동작을 먼저 찾는다. 신호·케이블은 물리 계층, 프레임·인접 노드는 데이터 링크 계층, 경로·패킷은 네트워크 계층, 종단 간 신뢰성은 전송 계층, 대화·세션 관리는 세션 계층으로 판단한다.

암기 포인트

물리=신호, 데이터 링크=프레임, 네트워크=경로, 전송=종단 간 신뢰성, 세션=대화 관리이다.

NoteBase

문 9. 다음은 보안 기능에 대한 설명이다. 가장 올바르게 짝지어진 것은?

ㄱ. 전송된 메시지가 변경 없이 전송되었는지 확인하는 보안 기능
ㄴ. 필요할 때 언제나 메시지를 보낼 수 있도록 보장하는 보안 기능
ㄷ. 전송되는 메시지가 외부에 유출되는 것을 방지하는 보안 기능

① ㄱ: 기밀성, ㄴ: 가용성, ㄷ: 무결성
② ㄱ: 가용성, ㄴ: 무결성, ㄷ: 기밀성
③ ㄱ: 무결성, ㄴ: 기밀성, ㄷ: 가용성
④ ㄱ: 무결성, ㄴ: 가용성, ㄷ: 기밀성

정답 4번

출제 포인트

정보보호의 3요소인 기밀성·무결성·가용성을 각 설명의 핵심 표현과 정확히 연결하는 문제이다.

핵심 개념

기밀성: 인가된 사람만 정보에 접근할 수 있게 하여 외부 유출을 막는 성질이다. 키워드는 '유출 방지'이다.
무결성: 정보가 권한 없이 변경되거나 훼손되지 않고 정확하게 유지되는 성질이다. 키워드는 '변경 없음'이다.
가용성: 인가된 사용자가 필요할 때 정보나 서비스를 이용할 수 있게 하는 성질이다. 키워드는 '필요할 때 언제나 이용'이다.
따라서 ㄱ은 무결성, ㄴ은 가용성, ㄷ은 기밀성에 해당한다.

선지별 해설

① X
ㄴ의 가용성만 옳다. 'ㄱ: 기밀성'과 'ㄷ: 무결성'이 틀렸으며, 올바르게는 'ㄱ: 무결성, ㄷ: 기밀성'이다.

② X
ㄷ의 기밀성만 옳다. 'ㄱ: 가용성'과 'ㄴ: 무결성'이 틀렸으며, 올바르게는 'ㄱ: 무결성, ㄴ: 가용성'이다.

③ X
ㄱ의 무결성만 옳다. 'ㄴ: 기밀성'과 'ㄷ: 가용성'이 틀렸으며, 올바르게는 'ㄴ: 가용성, ㄷ: 기밀성'이다.

④ O
메시지가 변경되지 않았는지는 무결성, 필요할 때 이용할 수 있는지는 가용성, 외부 유출 방지는 기밀성이므로 세 연결이 모두 옳다.

NoteBase

오답 포인트

‘메시지를 보낼 수 있음’을 전송 내용의 정확성과 혼동하면 ㄴ을 무결성으로 고르기 쉽다. 그러나 내용이 바뀌지 않았는지는 무결성이고, 필요할 때 서비스를 이용할 수 있는지는 가용성이다. 또한 외부 유출 방지는 기밀성이다.

다시 나오면 이렇게 판단

‘누가 볼 수 있는가’는 기밀성, ‘내용이 바뀌지 않았는가’는 무결성, ‘필요할 때 쓸 수 있는가’는 가용성으로 판단한다.

암기 포인트

유출 방지＝기밀성, 변경 방지＝무결성, 사용 보장＝가용성이다.

NoteBase

문 10. 다음 설명에 해당하는 이메일 암호화 방식은?

- 1991년 필립 짐머만에 의해 개발되었다.
- 사용자 간의 상호 인증을 통한 네트워크 구조를 통해 사용된다.
- 세션 키를 암호화하기 위하여 IDEA 알고리즘을 사용한다.
- 사용자 인증을 위한 서명으로 RSA 서명을 사용한다.

① S/MIME

② PGP

③ PEM

④ VPN

정답 2번

출제 포인트

개발자·개발 시기, 신뢰 구조, 사용 암호 알고리즘을 단서로 전자우편 보안 방식을 식별하는 문제이다.

핵심 개념

PGP(Pretty Good Privacy)는 전자우편의 기밀성·인증·무결성을 제공하는 보안 방식이다. 1991년 필립 짐머만이 개발했고, 중앙 인증기관에만 의존하지 않고 사용자들이 서로의 공개키에 서명하여 신뢰를 형성하는 신뢰망(Web of Trust)을 사용한다. 고전적 PGP에서는 IDEA가 메시지 본문을 세션 키로 대칭키 암호화하고, RSA가 세션 키 보호와 전자서명에 사용될 수 있다. 따라서 제시된 단서의 조합은 PGP를 가리킨다.

선지별 해설

① X — S/MIME은 전자우편 보안 표준이지만, X.509 인증서와 인증기관(CA)에 기초한 계층적 신뢰 구조를 사용한다. 제시문의 '필립 짐머만, 1991년, 사용자 간 상호 인증'에 해당하지 않는다. 올바르게는 이 단서들의 조합을 PGP의 특징으로 보아야 한다.
② O — PGP는 필립 짐머만이 1991년에 개발했으며, 사용자 상호 간 공개키 서명에 기반한 신뢰망을 사용한다. 또한 고전적 구성에서 IDEA와 RSA를 함께 사용하는 특징이 제시문의 단서와 일치한다.
③ X — PEM(Privacy Enhanced Mail)은 인터넷 전자우편의 보안성을 높이기 위해 설계된 별도의 표준 체계로, 제시된 PGP의 개발자와 신뢰망 구조를 뜻하지 않는다. 올바르게는 '1991년 필립 짐머만이 개발한 신뢰망 기반 방식'을 PGP라고 한다.
④ X — VPN은 공중망 위에 암호화된 가상 전용 통신 경로를 만드는 네트워크 보안 기술이며, 특정 전자우편 메시지의 암호화·서명을 위한 방식이 아니다. 올바르게는 제시된 전자우편 암호화 방식이 PGP이다.

NoteBase

오답 포인트

S/MIME과 PEM도 전자우편 보안과 관련되어 있어 혼동하기 쉽다. 이 문항에서는 특히 ‘필립 짐머만’, ‘1991년’, ‘사용자 간 상호 인증에 의한 신뢰망’이 PGP를 확정하는 단서이다. 한편 IDEA가 세션 키 자체를 암호화한다기보다, 세션 키를 이용해 메시지 데이터를 암호화한다는 점을 구분해야 한다.

다시 나오면 이렇게 판단

전자우편 보안 방식에서 사용자들이 서로의 공개키에 서명하는 신뢰망과 필립 짐머만이 함께 제시되면 PGP로 판단한다. X.509 인증기관 중심이면 S/MIME, 네트워크 구간의 암호화 터널이면 VPN으로 구분한다.

암기 포인트

PGP = 필립 짐머만 + 1991년 + 신뢰망(Web of Trust) + 전자우편 암호화·서명이다.

NoteBase

문 11. 암호학적 해시 함수에 관한 다음 설명 중 가장 옳지 않은 것은?

① 해시함수 h의 일방향성(One-wayness)은 임의의 값 y가 주어졌을 때, $h(x) = y$를 만족시키는 x값을 찾기 어려운 성질을 말한다.

② 해시함수 h의 충돌저항성(Collision resistance)은 $h(x) = h(x')$을 만족하는 서로 다른 값 x, x'을 찾기 어려운 성질을 말한다.

③ 대표적인 해시함수로는 MD5와 SHA 계열 함수를 들 수 있는데, 이 중 SHA-3는 해시 결과값의 크기로 128, 256, 384 비트 중 하나로 설정할 수 있다.

④ 비트코인에 활용되는 해시함수인 SHA-256은 SHA-2계열 해시함수의 하나로 해시 결과값의 크기가 256비트이다.

정답 3번

출제 포인트

암호학적 해시 함수의 일방향성·충돌저항성의 뜻과 SHA-3 계열의 해시 출력 길이를 구별하는 문제이다.

핵심 개념

일방향성은 해시값에서 그 해시값을 만드는 입력을 역으로 찾기 어려운 성질이다. 충돌저항성은 같은 해시값을 만드는 서로 다른 두 입력을 찾기 어려운 성질이다. SHA-3의 고정 길이 해시 함수는 SHA3-224, SHA3-256, SHA3-384, SHA3-512이며 각각 224, 256, 384, 512비트를 출력한다.

선지별 해설

① O — 임의의 해시값 y가 주어졌을 때 $h(x) = y$를 만족하는 입력 x를 찾기 어려운 성질은 일방향성, 즉 역상저항성에 해당한다.
② O — 서로 다른 두 입력 x와 x'에 대하여 $h(x) = h(x')$가 되도록 하는 쌍을 찾기 어려운 성질이 충돌저항성이다.
③ X — 틀린 표현은 '128, 256, 384비트 중 하나'이다. SHA-3의 고정 해시 출력 길이는 224, 256, 384, 512비트 중 하나이다. 128과 256은 가변 길이 출력 함수인 SHAKE128·SHAKE256의 이름에 쓰이는 보안 강도 구분이며, SHA-3의 고정 출력 길이 목록이 아니다.
④ O — SHA-256은 SHA-2 계열에 속하며 256비트의 고정 길이 해시값을 출력한다. 비트코인에서도 SHA-256이 활용된다.

오답 포인트

③은 SHA-3의 고정 길이 함수인 SHA3-224·256·384·512와 SHAKE128·256의 숫자를 섞어 놓았다. 특히 SHAKE의 128·256은 고정된 해시 출력 길이를 뜻하지 않는다는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

성질을 묻는 선지는 '주어진 해시값에서 입력 하나를 찾는가'이면 일방향성, '같은 해시값을 갖는 서로 다른 입력 두 개를 찾는가'이면 충돌저항성으로 판단한다. SHA-3의 고정 출력 길이는 224·256·384·512로 구별한다.

암기 포인트

SHA-3 고정 출력은 224·256·384·512, SHAKE는 128·256이다.

문 12. IPv4와 IPv6에 관한 다음 설명 중 가장 옳지 않은 것은?

① 기존 IPv4는 32비트 주소길이를 사용하고, IPv6는 64비트 주소 길이를 사용한다.

② IPv4는 IPSec 프로토콜을 별도로 설치해야 하지만, IPv6는 자체 지원한다.

③ IPv4는 네트워크 클래스 단위의 비순차적으로 주소를 할당하지만, IPv6는 네트워크 규모와 단말기수에 따라 순차적으로 주소를 할당한다.

④ IPv6는 헤더 내에 플로우 레이블(Flow Label) 필드를 이용하여 트래픽을 효과적으로 분류할 수 있는 기능을 제공한다.

정답 1번

출제 포인트

IPv4와 IPv6의 주소 길이, 보안 지원, 주소 할당 방식, 트래픽 분류 기능의 차이를 묻는 문제이다.

핵심 개념

IPv4는 32비트 주소를 사용하는 인터넷 프로토콜이고, IPv6는 주소 부족 문제를 보완하기 위해 128비트 주소를 사용하는 차세대 인터넷 프로토콜이다. IPv6는 확장된 주소 공간과 계층적 주소 할당, IPsec 지원, 플로우 레이블을 통한 트래픽 식별 기능을 제공한다.

선지별 해설

① X — 틀린 표현은 'IPv6는 64비트 주소 길이를 사용한다'이다. IPv6의 주소 길이는 64비트가 아니라 128비트이다. IPv4의 주소 길이가 32비트라는 부분은 옳다.
② O — IPv4에서는 IPsec을 선택적으로 추가하여 사용하지만, IPv6는 설계 단계부터 IPsec을 사용할 수 있도록 표준화된 지원 체계를 포함한다. 따라서 두 프로토콜의 보안 지원 차이를 설명한 선지이다.
③ O — IPv4의 전통적인 클래스 기반 주소 체계는 주소 공간을 비효율적이고 비연속적으로 배정하는 문제가 있었다. IPv6는 큰 주소 공간을 바탕으로 네트워크 규모와 단말 수를 고려한 계층적·순차적 주소 할당이 가능하다.
④ O — IPv6 기본 헤더의 플로우 레이블은 같은 흐름에 속하는 패킷을 식별하여 트래픽 분류와 품질 관리에 활용할 수 있다.

오답 포인트

①의 '64비트'는 IPv6 주소를 구성할 때 자주 접하는 64비트 단위와 전체 주소 길이를 혼동하게 만드는 함정이다. IPv6 주소 전체는 128비트이다.

NoteBase

다시 나오면 이렇게 판단

주소 길이를 먼저 확인하면 IPv4는 32비트, IPv6는 128비트로 구분된다. 이어서 IPv6의 대표 특징인 계층적 주소 할당, IPsec 지원, 플로우 레이블을 확인한다.

암기 포인트

IPv4는 32비트, IPv6는 128비트이며, IPv6의 핵심 키워드는 IPsec·계층적 주소·플로우 레이블이다.

NoteBase

문 13. 다음 중 개인정보처리자가 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당되지 않은 것은?

① 정보주체로부터 별도의 동의를 받은 경우

② 다른 법률에 특별한 규정이 있는 경우

③ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우

④ 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우

정답 4번

쟁점

이 문제는 개인정보를 수집 목적과 다른 용도로 이용하거나 제3자에게 제공할 수 있는 예외 사유에 관한 문제이다. 핵심은 허용 사유에 해당하더라도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있으면 허용되지 않는다는 점이다.

용어 풀이

목적 외 이용·제공 = 개인정보를 처음 정한 처리 목적의 범위를 넘어 이용하거나 제3자에게 제공하는 것을 말한다.

핵심 구분

개인정보 보호법 제18조 제1항은 목적 외 이용·제공을 원칙적으로 금지한다. 다만 같은 조 제2항은 별도 동의, 다른 법률의 특별한 규정, 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우 등 열거된 사유가 있으면 예외적으로 허용한다. 이때에도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없어야 한다. 따라서 '부당하게 침해할 우려가 있는 경우'는 허용 사유가 아니라 예외적 허용을 다시 제한하는 요건이다.

선지별 해설

① O — 정보주체로부터 별도의 동의를 받은 경우는 제18조 제2항이 정한 목적 외 이용·제공의 허용 사유이다.
② O — 다른 법률에 특별한 규정이 있는 경우도 법이 정한 허용 사유이다. 단순한 내부 방침이 아니라 다른 법률의 특별한 규정이 있어야 한다.
③ O — 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우도 허용 사유이다. '공공의 필요'만으로는 부족하고 긴급성이 요구된다.
④ X — 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우에는 목적 외 이용·제공이 허용되지 않는다. 틀린 표현: '부당하게 침해할 우려가 있는 경우'. 올바른 표현: '정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없고, 제18조 제2항 각 호의 사유에 해당하는 경우'이다.

NoteBase

오답 포인트

④의 문구는 허용 사유처럼 보이지만, 실제로는 모든 허용 사유에 공통으로 붙는 제한 요건이다. ‘각 호의 사유’와 ‘부당 침해 우려가 있을 때를 제외한다’는 본문의 단서를 뒤바꾸면 틀리게 된다.

다시 나오면 이렇게 판단

먼저 별도 동의·다른 법률의 특별 규정·긴급한 공공안전 필요 등 열거된 예외 사유인지 확인하고, 다음으로 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는지 확인한다. 두 조건을 모두 충족해야 목적 외 이용·제공이 가능하다.

암기 포인트

목적 외 이용·제공은 원칙 금지, 법정 예외에 해당하고 부당 침해 우려가 없어야 허용된다.

NoteBase

문 14. VPN(Virtual Private Network)에 관한 다음 설명 중 가장 옳지 않은 것은?

① VPN은 공중망을 경유하여 데이터가 전송되더라도 외부인으로부터 안전하게 보호되도록 주소 및 라우터 체계의 비공개, 데이터 암호화, 사용자 인증 및 사용자 엑세스 권한 제한 기능을 제공한다.

② SSL VPN은 종단간 보안이 가능하며 3계층 프로토콜이다.

③ VPN에서 사용되는 암호화 프로토콜에는 PPTP, L2TP, IPSec, SSL 등이 있다.

④ VPN은 IP 패킷이 공중망을 통과할 때 사용자 간에 전용망과 같은 보안 효과를 주기 위해 터널링 프로토콜을 통해 데이터를 캡슐화하여 전송한다.

정답 2번

출제 포인트

VPN의 기본 기능과 SSL VPN이 동작하는 계층을 구별하는 문제이다. 특히 3계층에서 IP 패킷을 보호하는 IPsec VPN과 SSL/TLS를 이용하는 SSL VPN을 혼동하지 않아야 한다.

핵심 개념

VPN은 인터넷과 같은 공중망 위에 암호화·인증·접근통제·터널링을 적용하여 논리적인 사설망을 구성하는 기술이다.
IPsec VPN은 네트워크 계층인 3계층에서 IP 패킷을 보호한다. SSL VPN은 SSL/TLS를 이용하여 전송 계층 위의 응용 서비스에 안전한 접속을 제공하므로 3계층 프로토콜이라고 하지 않는다.

선지별 해설

① O — VPN은 공중망을 사용하면서도 내부 주소·라우팅 정보의 노출을 줄이고, 암호화·사용자 인증·접근 권한 통제로 통신을 보호한다.
② X — 틀린 표현은 ‘SSL VPN은 3계층 프로토콜이다’이다. SSL VPN은 SSL/TLS를 이용하여 전송 계층 위의 응용 서비스 접속을 보호하며, 3계층에서 동작하는 대표적인 VPN 기술은 IPsec이다. 따라서 종단 간 보안 통신을 제공할 수 있다는 점과 3계층 프로토콜이라는 주장은 구분해야 한다.
③ O — PPTP와 L2TP는 대표적인 터널링 프로토콜이고, IPsec과 SSL/TLS는 VPN의 보안 통신에 활용된다. 엄밀히 말하면 PPTP·L2TP 자체를 모두 암호 알고리즘으로 보는 것은 아니지만, 이 선지는 VPN 구성에 사용되는 터널링·보안 프로토콜을 열거한 것으로 옳다.
④ O — 터널링은 원래 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 공중망으로 운반하는 방식이다. 이를 통해 떨어진 사용자나 사설망 사이에 전용망과 같은 논리적 통신 경로를 만든다.

오답 포인트

②의 ‘종단간 보안이 가능’이라는 앞부분만 보고 옳다고 판단하기 쉽다. 그러나 한 선지에 여러 설명이 결합되어 있으면 모두 옳아야 하며, ‘3계층 프로토콜’이라는 뒷부분이 SSL VPN과 IPsec VPN의 계층을 뒤바꾸었다.

NoteBase

다시 나오면 이렇게 판단

VPN 프로토콜의 계층을 물으면 먼저 IP 패킷 자체를 보호하는지, 응용 서비스 접속을 SSL/TLS로 보호하는지 확인한다. IP 패킷 중심이면 IPsec과 3계층을, 웹·응용 서비스 중심이면 SSL VPN을 연결한다.

암기 포인트

IPsec은 3계층 IP 보호, SSL VPN은 SSL/TLS 기반 응용 접속 보호이다.

NoteBase

문 15. 다음 설명 중 가장 옳지 않은 것은?

① 스니핑은 네트워크 상에서 주고받은 패킷 정보를 추출하여 사용자의 정보를 탈취하거나 통신 내용을 엿보는 공격이다.

② 서버 파밍은 여러 대의 컴퓨터를 이용해 대상 웹 서버에 과도한 트래픽을 보내 서버가 기능을 못하도록 만드는 공격이다.

③ 중간자공격은 통신 중인 두 객체 사이에 중간자가 데이터를 도청하고 조작한 후 다른 쪽으로 전달하는 공격이다.

④ 피싱은 신뢰할 수 있는 객체가 보낸 메시지로 가장하여 원래 사이트와 비슷한 사이트로 접속을 유도해 정보를 부정하게 얻는 공격이다.

정답 2번

출제 포인트

스니핑, 파밍, 중간자 공격, 피싱의 수법을 구별하고 공격 명칭과 설명이 올바르게 연결되었는지를 묻는 문제이다.

핵심 개념

스니핑은 네트워크를 흐르는 패킷을 몰래 수집하여 통신 내용이나 인증 정보를 알아내는 공격이다.
파밍은 DNS 정보나 호스트 설정 등을 변조하여 사용자가 정상 주소를 입력해도 위조 사이트로 접속하게 만드는 공격이다.
중간자 공격은 통신하는 두 객체 사이에 공격자가 끼어들어 메시지를 도청하거나 변조한 뒤 전달하는 공격이다.
피싱은 신뢰할 만한 기관이나 사람을 사칭한 메시지와 위조 사이트를 이용하여 사용자가 직접 개인정보를 입력하도록 속이는 공격이다.

선지별 해설

① O — 스니핑은 네트워크상의 패킷을 가로채어 통신 내용이나 사용자 정보를 몰래 알아내는 공격이므로 옳다.
② X — 틀린 표현은 '서버 파밍'이다. 여러 대의 컴퓨터가 대상 서버에 대량의 트래픽을 보내 서비스를 마비시키는 것은 분산 서비스 거부 공격(DDoS)이다. 서버 파밍은 DNS 서버 등의 주소 정보를 변조하여 사용자를 공격자가 만든 위조 사이트로 유도하는 방식으로 설명해야 한다.
③ O — 중간자 공격은 두 통신 주체 사이에 공격자가 개입하여 데이터를 도청·변조하고 상대방에게 전달하는 공격이므로 옳다.
④ O — 피싱은 신뢰할 수 있는 주체를 사칭한 메시지로 위조 사이트 접속을 유도한 뒤 개인정보를 부정하게 얻는 공격이므로 옳다.

NoteBase

오답 포인트

②의 '여러 대의 컴퓨터', '과도한 트래픽', '서버 기능 마비'는 파밍이 아니라 DDoS를 가리키는 결정적 표현이다. 파밍의 핵심은 트래픽 폭주가 아니라 주소 정보 변조와 위조 사이트 유도이다.

다시 나오면 이렇게 판단

패킷을 몰래 수집하면 스니핑, 통신 사이에 끼어 도청·변조하면 중간자 공격, 주소 정보를 변조해 위조 사이트로 보내면 파밍, 사칭 메시지로 사용자를 속여 위조 사이트에 정보를 입력하게 하면 피싱, 대량 트래픽으로 서비스를 마비시키면 DDoS로 구분한다.

암기 포인트

스니핑은 엿듣기, 중간자 공격은 사이에 끼어들기, 파밍은 주소 변조, 피싱은 사칭 유인, DDoS는 트래픽 폭주이다.

NoteBase

문 16. 리눅스의 권한 설정에 관한 다음 설명 중 가장 옳지 않은 것은?

① 리눅스에서는 파일의 접근 권한에 대하여 파일을 만든 소유자 권한, 소유자가 속한 소유 그룹 권한으로만 나눠서 관리한다.

② 리눅스에서는 기본적으로 사용자 ID를 체크하여 실행 권한이 있으면 명령어를 수행한다.

③ 리눅스에서는 사용자 ID에게 실행 권한이 없으면 SetUID, SetGID, Sticky bit이 설정되어 있는지를 확인한다.

④ SetUID가 설정되어 있는 파일을 사용자가 실행하면 사용자의 권한이 아닌 소유자의 권한으로 실행한다.

정답 1번

출제 포인트

리눅스의 일반 접근 권한이 소유자, 소유 그룹, 기타 사용자로 구분된다는 점과 SetUID·SetGID·Sticky bit의 기능을 구별하는 문제이다.

핵심 개념

일반 접근 권한: 파일이나 디렉터리에 대한 읽기·쓰기·실행 권한을 소유자(user), 소유 그룹(group), 기타 사용자(others)별로 설정한다.
SetUID: 실행 파일을 실행하는 동안 그 파일 소유자의 유효 사용자 ID 권한을 적용한다.
SetGID: 실행 파일에서는 파일 소유 그룹의 유효 그룹 ID 권한을 적용하며, 디렉터리에서는 새 파일이 그 디렉터리의 그룹을 이어받게 한다.
Sticky bit: 주로 공유 디렉터리에서 파일 삭제·이름 변경을 파일 소유자, 디렉터리 소유자 또는 특권 사용자 등으로 제한한다.

선지별 해설

① X — '소유자 권한, 소유 그룹 권한으로만' 나눈다는 부분이 틀렸다. 실제로는 소유자(user), 소유 그룹(group), 기타 사용자(others)의 세 범주로 나누어 권한을 관리한다.
② O — 리눅스는 프로세스의 사용자 ID와 파일에 설정된 실행 권한을 대조하여 실행 가능 여부를 판단한다. 정확히는 유효 사용자 ID와 유효 그룹 ID 및 보조 그룹을 기준으로 해당 권한 범주의 실행 비트를 검사한다.
③ O — 이 선지는 일반 권한뿐 아니라 SetUID, SetGID, Sticky bit과 같은 특수 권한 비트도 구분하여 확인한다는 취지이다. 다만 SetUID와 SetGID는 실행이 허용된 뒤 적용될 유효 ID를 바꾸는 기능이고, Sticky bit은 주로 디렉터리의 삭제·이름 변경을 제한하므로, 특수 권한 비트가 없는 실행 권한을 새로 부여하는 것은 아니다.
④ O — 실행 권한이 있는 SetUID 파일을 실행하면 프로세스의 유효 사용자 ID가 파일 소유자의 ID로 설정되어, 실행 중에는 파일 소유자의 권한이 적용된다.

NoteBase

오답 포인트

①의 '소유자와 소유 그룹만'이라는 표현에 기타 사용자(others)가 빠져 있다. 또한 SetUID를 사용자의 모든 권한이 영구적으로 소유자 권한으로 바뀌는 기능으로 오해하기 쉽지만, 해당 실행 파일이 동작하는 동안 프로세스의 유효 사용자 ID에만 영향을 준다.

다시 나오면 이렇게 판단

일반 권한은 user-group-others의 세 범주와 read-write-execute의 세 권한을 먼저 확인한다. 그다음 특수 권한은 SetUID=소유자 유효 ID, SetGID=그룹 유효 ID 또는 디렉터리 그룹 상속, Sticky bit=공유 디렉터리 삭제 제한으로 구별한다.

암기 포인트

일반 권한은 u-g-o, 특수 권한은 SetUID=소유자, SetGID=그룹, Sticky=공유 디렉터리 삭제 제한이다.

NoteBase

문 17. 다음 중 해당 취약점에 대한 패치가 아직 나오지 않은 취약점을 이용한 공격은?

① 인젝션 공격

② 전수조사 공격

③ Slowloris 공격

④ 제로데이 공격

정답 4번

출제 포인트

패치가 아직 제공되지 않은 취약점을 이용하는 공격의 명칭을 구별하는 문제이다.

핵심 개념

제로데이 공격은 취약점이 알려졌더라도 이를 고칠 보안 패치가 아직 배포되지 않은 시점에 그 취약점을 악용하는 공격이다. 방어자가 패치를 적용할 수 있는 시간이 사실상 0일이라는 뜻에서 제로데이라고 한다.

선지별 해설

① X

인젝션 공격은 검증되지 않은 입력값에 명령어나 질의문을 삽입하여 시스템이 이를 실행하게 만드는 공격이다. 틀린 부분은 패치가 아직 나오지 않은 취약점을 이용하는 공격으로 본 점이며, 올바르게는 입력값 처리의 허점을 악용하는 공격이다.

② X

전수조사 공격은 가능한 비밀번호나 키의 후보를 하나씩 모두 대입하여 정답을 찾는 공격이다. 틀린 부분은 미패치 취약점의 악용과 연결한 점이며, 올바르게는 가능한 후보를 빠짐없이 시도하는 무차별 대입 공격이다.

③ X

Slowloris 공격은 다수의 HTTP 연결을 열고 불완전한 요청을 매우 느리게 보내 연결을 오래 유지함으로써 웹 서버의 자원을 고갈시키는 서비스 거부 공격이다. 틀린 부분은 패치가 없는 취약점을 이용한다는 점이며, 올바르게는 느린 요청으로 서버 연결 자원을 점유하는 공격이다.

④ O

제로데이 공격은 해당 취약점을 고치는 패치가 아직 나오지 않은 상태에서 그 취약점을 악용하는 공격이므로 지문의 설명에 해당한다.

NoteBase

오답 포인트

모든 공격이 시스템의 약점을 노린다는 공통점 때문에 혼동하기 쉽다. 그러나 지문의 결정적 표현은 '패치가 아직 나오지 않은 취약점'이며, 이는 공격 방식이 아니라 패치 제공 전이라는 시간적 상태를 가리키므로 제로데이 공격을 선택한다.

다시 나오면 이렇게 판단

선지에서 '미공개 취약점', '보안 패치 배포 전', '대응책이 마련되기 전'과 같은 표현이 나오면 제로데이 공격을 먼저 판단한다. 입력값에 명령을 삽입하면 인젝션, 모든 후보를 대입하면 전수조사, 느린 HTTP 연결로 자원을 점유하면 Slowloris로 구별한다.

암기 포인트

패치까지 0일, 미패치 취약점 악용은 제로데이 공격이다.

NoteBase

문 18. 다음 중 버퍼 오버플로 공격(Buffer Overflow Attack)에 취약한 함수와 가장 거리가 먼 것은?

① strcpy

② scanf

③ gets

④ printf

정답 4번

출제 포인트

이 문제는 입력·복사 과정에서 목적지 버퍼의 크기를 확인하지 않아 버퍼 오버플로를 일으킬 수 있는 C 함수와, 그 위험과 직접 관련성이 낮은 함수를 구별하는 문제이다.

핵심 개념

버퍼 오버플로는 프로그램이 확보한 버퍼의 경계를 넘어 데이터를 기록하여 인접한 메모리를 훼손하는 현상이다. strcpy와 gets는 저장할 데이터의 길이를 자체적으로 제한하지 않으며, scanf도 %s 등에 최대 입력 폭을 지정하지 않으면 목적지 배열의 크기를 넘길 수 있다. printf는 표준 출력으로 내용을 내보내는 함수이므로 이들과 같은 방식으로 입력을 버퍼에 저장하지 않는다. 다만 신뢰할 수 없는 문자열을 서식 문자열로 직접 사용하면 별도의 포맷 스트링 취약점이 생길 수 있다.

선지별 해설

① X — strcpy는 원본 문자열의 길이를 검사하지 않고 널 문자까지 목적지 버퍼에 복사하므로, 목적지 공간이 부족하면 경계를 넘어 기록한다. 따라서 '버퍼 오버플로에 취약한 함수와 가장 거리가 먼 함수'가 아니라 대표적인 취약 함수이다. 올바르게는 크기를 제한할 수 있는 방식으로 복사하고 목적지 버퍼의 용량과 널 종료를 함께 확인해야 한다.
② X — scanf는 %s와 같은 변환에서 입력 폭을 제한하지 않으면 목적지 문자 배열보다 긴 입력을 기록할 수 있다. 따라서 가장 거리가 먼 함수가 아니다. 올바르게는 서식에 배열 크기에 맞는 최대 입력 폭을 지정해야 한다.
③ X — gets는 입력 길이를 제한할 방법 없이 줄바꿈 전까지 문자를 버퍼에 저장하므로 버퍼 오버플로에 매우 취약하다. 따라서 가장 거리가 먼 함수가 아니다. 올바르게는 버퍼 크기를 인자로 받는 fgets와 같은 함수를 사용해야 한다.
④ O — printf는 데이터를 지정된 문자 배열에 입력하거나 복사하는 함수가 아니라 표준 출력으로 보내는 함수이므로, 나머지 세 함수보다 전형적인 버퍼 오버플로 위험과 거리가 멀다. printf의 대표적 보안 위험은 외부 입력을 서식 문자열로 직접 사용할 때 발생하는 포맷 스트링 취약점이다.

NoteBase

오답 포인트

printf도 보안상 잘못 사용될 수 있다는 점 때문에 혼동하기 쉽다. 그러나 이 문항은 일반적인 보안 취약점 전체가 아니라 '버퍼 경계를 넘어 쓰는 함수'를 묻는다. printf의 포맷 스트링 취약점과 strcpy·scanf·gets의 길이 미검사에 따른 버퍼 오버플로를 구분해야 한다.

다시 나오면 이렇게 판단

각 함수가 외부 데이터를 크기 제한 없이 목적지 메모리 버퍼에 기록하는지를 확인한다. 길이 제한 없는 문자열 복사·입력 함수는 버퍼 오버플로 위험군이고, 표준 출력 함수는 직접적인 위험군에서 벗어난다.

암기 포인트

strcpy·gets·폭 제한 없는 scanf는 버퍼 경계 초과, printf는 주로 포맷 스트링을 주의한다.

NoteBase

문 19. 다음 중 개인정보 보호법 시행령에서 정한 고유식별정보의 범위에 포함되지 않은 것은?

① 여권번호

② 운전면허번호

③ 이메일 주소

④ 외국인등록번호

정답 3번

쟁점

이 문제는 개인정보 보호법 시행령상 고유식별정보의 범위를 묻는 문제이다. 핵심은 법령이 열거한 네 가지 정보와 일반적인 연락처 정보를 구별하는 것이다.

용어 풀이

고유식별정보는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보 가운데 대통령령으로 정한 정보이다.

핵심 구분

개인정보 보호법 시행령 제19조는 주민등록번호, 여권번호, 운전면허의 면허번호, 외국인등록번호를 고유식별정보로 열거한다. 이메일 주소는 개인정보가 될 수 있지만 이 조항이 정한 고유식별정보에는 포함되지 않는다.

NoteBase

선지별 해설

① X
여권번호는 시행령 제19조에 열거된 고유식별정보이므로 '포함되지 않은 것'이 아니다.
틀린 판단: 여권번호가 고유식별정보의 범위에 포함되지 않는다.
올바른 판단: 여권번호는 고유식별정보의 범위에 포함된다.

② X
운전면허번호는 시행령 제19조의 '운전면허의 면허번호'에 해당하므로 '포함되지 않은 것'이 아니다.
틀린 판단: 운전면허번호가 고유식별정보의 범위에 포함되지 않는다.
올바른 판단: 운전면허번호는 고유식별정보의 범위에 포함된다.

③ O
이메일 주소는 시행령 제19조가 열거한 고유식별정보가 아니므로 문제의 '포함되지 않은 것'에 해당한다.

④ X
외국인등록번호는 시행령 제19조에 열거된 고유식별정보이므로 '포함되지 않은 것'이 아니다.
틀린 판단: 외국인등록번호가 고유식별정보의 범위에 포함되지 않는다.
올바른 판단: 외국인등록번호는 고유식별정보의 범위에 포함된다.

오답 포인트

이메일 주소도 개인을 식별하는 개인정보가 될 수 있다는 점 때문에 고유식별정보로 착각하기 쉽다. 그러나 모든 개인정보가 고유식별정보인 것은 아니며, 이 문제에서는 시행령 제19조의 열거 여부로 판단한다.

다시 나오면 이렇게 판단

고유식별정보의 범위를 묻는 문제에서는 주민등록번호·여권번호·운전면허번호·외국인등록번호의 네 가지 열거 항목인지 먼저 확인한다. 이메일 주소·전화번호·주소처럼 일반적인 연락처 정보는 이 열거 항목과 구별한다.

암기 포인트

고유식별정보 네 가지는 주민등록번호·여권번호·운전면허번호·외국인등록번호이고, 이메일 주소는 제외된다.

NoteBase

문 20. 악성코드에 관한 다음 설명 중 가장 옳지 않은 것은?

① 트로이목마는 정상적인 프로그램으로 위장하여 사용자로 하여금 실행을 유도하는 악성 프로그램을 말한다.

② 바이러스는 프로그램 또는 문서에 삽입되어 감염되거나 동작한다.

③ 웜은 자체적으로 실행되면서 네트워크를 통해 자신을 복제하고 전파한다.

④ 루트킷은 바이러스나 웜과 결합하여 자동으로 설치되기 어렵다.

정답 4번

출제 포인트

트로이목마·바이러스·웜·루트킷을 실행 방식, 복제 여부, 은폐 기능으로 구분하는 문제이다.

핵심 개념

트로이목마: 정상 프로그램인 것처럼 위장해 사용자의 실행을 유도하는 악성코드이다.
바이러스: 다른 프로그램이나 문서 등에 자신의 코드를 삽입하여 감염시키고, 감염된 대상이 실행될 때 동작하는 악성코드이다.
웜: 다른 파일에 기생하지 않고 스스로 실행·복제하며 주로 네트워크를 통해 전파되는 악성코드이다.
루트킷: 공격자가 시스템의 높은 권한을 유지하면서 악성 행위와 관련 파일·프로세스 등을 숨기도록 하는 도구 또는 악성코드이다.

선지별 해설

① O — 트로이목마는 정상 프로그램으로 위장하여 사용자가 직접 설치하거나 실행하도록 속이는 방식이 핵심이다.
② O — 바이러스는 보통 실행 파일, 프로그램 또는 문서 등에 삽입되어 숙주가 실행되거나 문서가 열릴 때 감염·동작한다.
③ O — 웜은 독립적으로 실행되고 자기 자신을 복제하며, 네트워크의 취약점 등을 이용해 다른 시스템으로 전파될 수 있다.
④ X — 틀린 표현은 '바이러스나 웜과 결합하여 자동으로 설치되기 어렵다'이다. 루트킷은 다른 악성코드와 함께 유입되거나 침해 과정에서 자동으로 설치될 수 있으며, 설치 후 공격자의 권한과 악성 흔적을 숨기는 데 이용된다. 올바르게는 '루트킷은 바이러스나 웜 등 다른 악성코드와 결합해 자동으로 설치될 수 있다'이다.

오답 포인트

루트킷을 독립적인 감염·전파 유형으로만 생각하면 ④의 '설치되기 어렵다'를 지나치기 쉽다. 루트킷의 핵심은 설치 방식의 제한이 아니라 침투 후 권한 유지와 은폐 기능이다.

NoteBase

다시 나오면 이렇게 판단

사용자를 속여 실행시키면 트로이목마, 숙주 파일에 붙으면 바이러스, 스스로 복제·전파하면 웜, 권한과 악성 흔적을 숨기면 루트킷으로 판단한다.

암기 포인트

트로이목마는 위장, 바이러스는 숙주 감염, 웜은 자기 복제, 루트킷은 권한 유지와 은폐이다.

NoteBase

문 21. 보안 시스템 설계 시 참고하는 접근 제어 원칙 중 운영 체제에서 사용하는 관리자 계정에 일반적으로 적용되지 않는 원칙은?

① 직무분리

② 고장 시 안전 초기화

③ 최소권한

④ 알 필요성

정답 3번

출제 포인트

운영 체제의 관리자 계정이 갖는 포괄적 권한과 일반적인 접근 제어 원칙의 관계를 구별하는 문제이다.

핵심 개념

관리자 계정은 시스템 설정과 사용자·권한 관리를 위해 광범위한 권한을 갖는 특수 계정이다. 최소권한은 사용자나 프로세스에 업무 수행에 필요한 최소한의 권한만 부여하는 원칙이므로, 광범위한 권한을 전제로 하는 관리자 계정 자체에는 일반적으로 그대로 적용되지 않는다. 다만 실제 운영에서는 관리자 계정의 사용을 필요한 작업과 시간으로 제한하고, 평상시에는 일반 계정을 사용하는 방식으로 위험을 줄인다.

선지별 해설

① X — 직무분리는 한 사람에게 권한과 책임이 집중되지 않도록 업무를 나누는 원칙이다. 관리자 업무도 계정 관리, 감사, 보안 운영 등을 분리할 수 있으므로 '관리자 계정에는 일반적으로 적용되지 않는다'는 판단이 틀리다. 올바르게는 관리자 권한의 오용을 막기 위해 관리자 업무에도 직무분리를 적용할 수 있다.
② X — 고장 시 안전 초기화는 시스템에 장애나 오류가 생기면 접근을 허용하는 쪽이 아니라 차단하는 안전한 상태를 기본값으로 삼는 원칙이다. 관리자 인증이나 접근 제어 기능에도 적용되므로 '관리자 계정에는 일반적으로 적용되지 않는다'는 판단이 틀리다. 올바르게는 장애가 발생해도 관리자 접근을 자동 허용하지 않고 안전한 거부 상태로 처리한다.
③ O — 최소권한은 필요한 최소 권한만 부여하는 원칙이지만, 운영 체제의 관리자 계정은 시스템 전반을 관리하기 위해 본질적으로 광범위한 권한을 가진다. 따라서 제시된 원칙 가운데 관리자 계정 자체에 일반적으로 적용되지 않는 것으로 보는 것은 최소권한이다.
④ X — 알 필요성은 업무 수행에 필요한 정보에만 접근하게 하는 원칙이다. 관리자라도 담당 업무와 무관한 정보까지 항상 열람해야 하는 것은 아니므로 '관리자 계정에는 일반적으로 적용되지 않는다'는 판단이 틀리다. 올바르게는 관리자의 정보 접근도 담당 업무상 알 필요가 있는 범위로 제한할 수 있다.

NoteBase

오답 포인트

③의 관리자 계정은 권한이 크다는 사실과 관리자의 권한 사용까지 아무 제한이 없다는 주장을 혼동하기 쉽다. 이 문항은 계정 자체의 포괄적 권한 때문에 최소권한이 일반적으로 그대로 적용되지 않는다는 점을 묻지만, 실제 사용 범위와 시간은 별도로 제한할 수 있다.

다시 나오면 이렇게 판단

각 원칙이 관리자 계정의 넓은 권한 자체와 충돌하는지 판단한다. 직무분리·고장 시 안전 초기화·알 필요성은 관리자 업무나 접근 방식에도 적용할 수 있지만, 최소권한은 포괄적 권한을 가진 관리자 계정의 성격과 직접 충돌한다.

암기 포인트

관리자 계정은 포괄 권한, 일반 계정은 최소권한이다. 관리자 권한의 사용은 직무분리·안전한 기본값·알 필요성으로 통제한다.

NoteBase

문 22. SSL(Secure Socket Layer)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 암호화된 웹서핑을 가능하게 한다.

② 서버 인증, 클라이언트 인증, 암호화된 세션 기능을 제공한다.

③ SSL을 지원하는 웹사이트는 https://로 시작한다.

④ 데이터링크 계층에서 동작하는 프로토콜이다.

정답 4번

출제 포인트

SSL의 보안 기능과 동작 계층을 구별하는 문제이다.

핵심 개념

SSL은 응용 계층의 데이터를 암호화하고 통신 상대를 인증하여 안전한 통신 세션을 제공하는 보안 프로토콜이다. TCP를 이용하는 응용 프로토콜과 전송 계층 사이에서 보안 기능을 제공하므로 데이터링크 계층 프로토콜이 아니다. 오늘날에는 SSL의 후속 규격인 TLS가 같은 역할을 수행한다.

선지별 해설

① O — SSL은 웹 브라우저와 웹 서버 사이에서 전달되는 데이터를 암호화하므로 암호화된 웹서핑을 가능하게 한다.
② O — SSL은 서버 인증을 기본적으로 지원하고, 설정에 따라 인증서를 이용한 클라이언트 인증도 지원하며, 협상된 세션 키로 통신 내용을 암호화한다.
③ O — HTTP 통신을 SSL/TLS로 보호할 때 URL은 http://가 아니라 https://로 시작한다.
④ X — 틀린 표현은 '데이터링크 계층에서 동작'이다. 올바르게는 SSL이 TCP를 사용하는 응용 프로토콜과 전송 계층 사이에서 보안 기능을 제공한다고 해야 한다.

오답 포인트

SSL이 네트워크 통신을 보호한다는 이유만으로 하위 계층인 데이터링크 계층의 프로토콜로 오인하기 쉽다. SSL은 특정 링크의 프레임을 보호하는 기술이 아니라 응용 데이터의 종단 간 보안 통신을 지원한다.

다시 나오면 이렇게 판단

SSL 관련 선지는 '인증·암호화·무결성·HTTPS'이면 핵심 기능에 해당하는지 확인하고, 동작 계층을 묻는 경우에는 데이터링크 계층이 아니라 TCP 위에서 응용 프로토콜을 보호한다는 점으로 판단한다.

암기 포인트

SSL/TLS는 HTTPS의 보안 통신을 담당하며, 데이터링크 계층이 아니라 TCP 위에서 응용 데이터를 보호한다.

NoteBase

문 23. 다음 중 ECC(Elliptic Curve Cryptosystem)와 RSA(Rivest Shamir Adleman) 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

① ECC는 RSA에 비해 속도가 빠르다.

② RSA는 ECC에 비해 키 길이가 짧다.

③ ECC는 RSA 대비 소형 Mobile 환경에 적합하다.

④ ECC는 WPKI(무선) 기반 구조이고, RSA는 PKI(유선) 기반 구조이다.

정답 2번

출제 포인트

이 문제는 동일한 보안강도를 기준으로 ECC와 RSA의 키 길이, 연산 효율 및 활용 환경을 비교하는 문제이다.

핵심 개념

ECC는 타원곡선 위의 이산대수 문제를 안전성의 기반으로 삼는 공개키 암호 방식이다. 비교적 짧은 키로 높은 보안강도를 제공하므로 저장 공간, 통신량, 전력 등이 제한된 환경에 유리하다.
RSA는 큰 정수의 소인수분해가 어렵다는 점을 안전성의 기반으로 삼는 공개키 암호 방식이다. ECC와 동일한 수준의 보안강도를 얻으려면 일반적으로 더 긴 키가 필요하다.
핵심 비교는 'ECC는 짧은 키', 'RSA는 상대적으로 긴 키'이다.

선지별 해설

① O — 출제에서 전제한 동일 보안강도 기준에서는 ECC가 RSA보다 짧은 키와 작은 연산 자원으로 구현될 수 있어 제한된 환경에서 효율적이고 빠르게 동작하는 것으로 비교한다. 다만 모든 구현과 모든 연산에서 언제나 빠르다는 절대적 의미는 아니다.
② X — 틀린 부분은 'RSA는 ECC에 비해 키 길이가 짧다'이다. 실제로는 동일한 보안강도를 기준으로 ECC의 키가 RSA의 키보다 짧고, RSA는 ECC보다 긴 키가 필요하다.
③ O — ECC는 짧은 키로 보안강도를 확보할 수 있어 저장 공간, 통신 대역폭, 전력 및 처리 자원이 제한된 소형 모바일 환경에 적합하다.
④ O — 전통적인 활용 환경의 비교에서는 ECC가 무선·모바일용 WPKI에 적합하고 RSA가 유선 환경의 일반 PKI에서 널리 사용되는 방식으로 구분한다. 이는 대표적인 적용 환경을 비교한 것이며, 각 알고리즘을 해당 환경에서만 사용할 수 있다는 뜻은 아니다.

오답 포인트

②는 키 길이의 우열을 정반대로 바꾼 선지이다. 알고리즘의 키 길이 숫자 자체를 단순 비교하는 것이 아니라 동일한 보안강도를 전제로 비교해야 한다. 또한 ①과 ④는 시험상 대표적 효율과 활용 환경을 묻는 표현이지 모든 구현에 대한 절대적 제한을 뜻하지 않는다.

NoteBase

다시 나오면 이렇게 판단

ECC와 RSA를 비교할 때 먼저 동일 보안강도라는 전제를 둔다. 그다음 'ECC는 더 짧은 키와 자원 절약으로 모바일·무선 환경에 유리하고, RSA는 상대적으로 더 긴 키를 사용한다'는 기준으로 선지를 판단한다.

암기 포인트

동일 보안강도에서는 ECC는 짧은 키·모바일 친화, RSA는 긴 키이다.

NoteBase

문 24. ARP 스푸핑 공격을 방지 하기 위한 방안으로 가장 옳지 않은 것은?

① 관리자가 수동으로 MAC 주소를 관리한다.

② ARP 캐쉬의 내용이 바뀌면 관리자에게 경고 메시지를 보내도록 설정한다.

③ 방화벽을 이용하여 ARP 패킷에 대해 임계값을 설정한다.

④ Snort와 같은 침입 탐지 시스템을 활용한다.

정답 3번

출제 포인트

ARP 스푸핑은 공격자가 거짓 IP-MAC 대응 정보를 보내 ARP 캐시를 오염시키는 공격이므로, 대응책이 위조된 대응 정보의 등록을 막거나 그 변조를 탐지할 수 있는지를 묻는 문제이다.

핵심 개념

ARP 스푸핑 방어의 핵심은 신뢰할 수 있는 IP-MAC 대응 관계를 고정·검증하거나 ARP 캐시의 비정상 변경을 탐지하는 데 있다. 단순히 ARP 패킷의 개수만 제한하면 대량의 ARP 패킷을 이용한 서비스 거부는 줄일 수 있지만, 적은 수의 위조 ARP 응답으로 이루어지는 캐시 오염 자체는 판별하지 못한다.

선지별 해설

① O — 관리자가 신뢰할 수 있는 IP-MAC 대응 관계를 정적 ARP 항목으로 수동 관리하면 공격자가 보낸 거짓 ARP 정보로 해당 항목이 동적으로 바뀌는 것을 막을 수 있다.

② O — ARP 캐시의 변경을 감시하고 관리자에게 경고하면 비정상적인 IP-MAC 대응 관계의 변조를 신속히 탐지하고 대응할 수 있다.

③ X — 틀린 부분은 '방화벽을 이용하여 ARP 패킷에 대해 임계값을 설정한다'는 것이다. 일반적인 방화벽의 IP 기반 필터링이나 단순 패킷 수 임계값은 ARP 응답의 IP-MAC 대응 관계가 진짜인지 확인하지 못하므로 ARP 스푸핑의 직접적인 방지책이 아니다. 올바르게는 스위치의 동적 ARP 검사와 같이 신뢰된 바인딩 정보를 기준으로 ARP 패킷을 검증하거나 정적 ARP 항목을 사용한다.

④ O — Snort와 같은 침입 탐지 시스템은 비정상적인 ARP 활동이나 IP-MAC 대응 관계의 변화를 탐지하여 ARP 스푸핑 징후를 경고할 수 있다.

NoteBase

오답 포인트

③의 '임계값'은 ARP 패킷이 지나치게 많이 발생하는 상황에는 도움이 될 수 있어 그럴듯하다. 그러나 ARP 스푸핑의 본질은 패킷 수가 아니라 거짓 IP-MAC 대응 정보이며, 소량의 위조 응답만으로도 캐시 오염이 가능하다는 점이 함정이다.

다시 나오면 이렇게 판단

대응책이 IP-MAC 대응 관계를 고정하거나 검증하는지, 또는 그 변조를 탐지하는지를 먼저 확인한다. 패킷의 양만 제한하고 대응 정보의 진위를 확인하지 않는 방법은 ARP 스푸핑의 핵심 방어책으로 보지 않는다.

암기 포인트

ARP 스푸핑은 '양'이 아니라 '거짓 대응 관계'의 문제이므로, 정적 매핑·바인딩 검증·변조 탐지가 핵심이다.

NoteBase

문 25. IPSec 프로토콜이 보안을 제공하지 못하는 계층은?

① 응용
② 전송
③ 네트워크
④ 물리

정답 4번

출제 포인트

IPsec가 동작하는 계층과 그 보안 효과가 미치는 범위를 구분하는 문제이다.

핵심 개념

IPsec는 네트워크 계층에서 IP 패킷에 기밀성, 무결성, 인증 등의 보안 서비스를 제공한다. 상위 계층인 전송 계층과 응용 계층의 데이터는 IP 패킷의 페이로드에 포함되므로 함께 보호될 수 있지만, 케이블·전파 같은 물리적 전송 매체 자체를 보호하지는 않는다.

선지별 해설

① X — '응용 계층에는 보안을 제공하지 못한다'는 판단이 틀리다. 응용 계층 데이터는 IP 패킷 안에 실리므로 IPsec에 의해 보호될 수 있다.
② X — '전송 계층에는 보안을 제공하지 못한다'는 판단이 틀리다. TCP·UDP 세그먼트는 IP 페이로드에 포함되므로 IPsec의 보호 대상이 될 수 있다.
③ X — '네트워크 계층에는 보안을 제공하지 못한다'는 판단이 틀리다. IPsec는 바로 네트워크 계층에서 IP 패킷에 보안 서비스를 제공한다.
④ O — 물리 계층은 케이블, 전파, 신호 등 실제 전송 매체와 비트 전송을 다룬다. IPsec는 물리적 매체나 신호 자체의 보안을 제공하지 못한다.

오답 포인트

IPsec가 네트워크 계층에서 동작한다는 사실을 '네트워크 계층만 보호한다'고 오해하기 쉽다. IPsec는 상위 계층 데이터를 담은 IP 패킷을 보호하지만 물리적 전송 매체까지 보호하지는 않는다.

다시 나오면 이렇게 판단

보안 프로토콜의 동작 계층과 보호되는 데이터의 범위를 나누어 판단한다. IPsec는 네트워크 계층에서 동작하며 IP 패킷에 포함된 상위 계층 데이터는 보호할 수 있지만 물리 계층 자체는 보호할 수 없다.

NoteBase

암기 포인트

IPsec는 IP 패킷을 보호하고, 물리 매체는 보호하지 않는다.

NoteBase