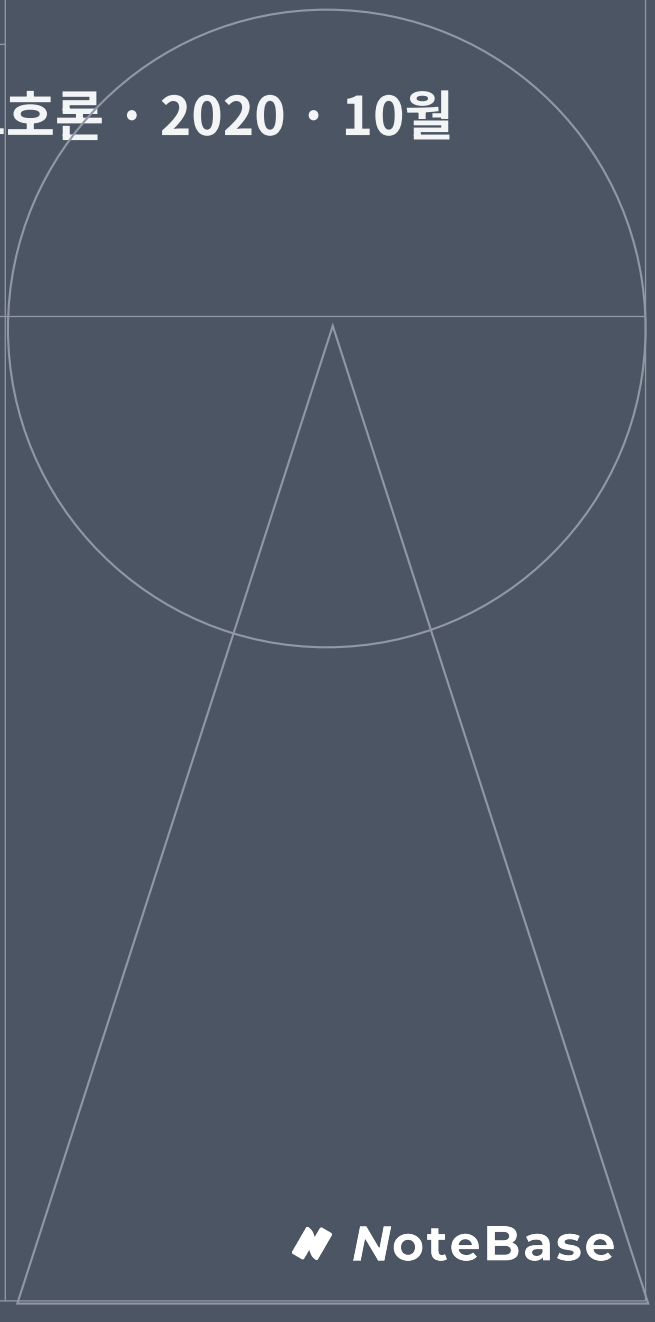
기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2020 · 10월



NoteBase

기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2020 · 10월

공무원/서울시/7급 · 정보보호론 · 2020 · 10월

문 1. 정보보안 3요소에 대한 <보기>의 설명에서 (가), (나), (다)에 들어갈 말을 옳게 짝지은 것은?

<보기>
(가)은 적절한 권한을 가진 사용자가 인가한 방법으로만 정보를 변경할 수 있도록 하는 것을 말하며 변경, 가장, 재전송 등과 같은 공격에 의해 위협받을 수 있다.
(나)은 인가된 사용자만 정보 자산에 접근할 수 있다는 것으로 일반적인 보안의 의미와 가장 가깝다. 방화벽, 암호 패스워드 등이 대표적인 예이다.
(다)은 필요한 시점에 정보 자산에 대한 접근이 가능하도록 하는 것을 말하며 DDoS와 같은 공격에 의해 위협받을 수 있다.

① (가): 무결성, (나): 가용성, (다): 기밀성
② (가): 무결성, (나): 기밀성, (다): 가용성
③ (가): 기밀성, (나): 가용성, (다): 무결성
④ (가): 기밀성, (나): 무결성, (다): 가용성

정답 2번

출제 포인트

정보보안 3요소인 무결성, 기밀성, 가용성의 정의와 대표 위협을 정확히 대응시키는지 묻는 문제이다.

핵심 개념

무결성은 인가된 방법으로만 정보가 변경되도록 보장하는 성질이며 키워드는 변경 방지, 위변조 방지이다.
기밀성은 인가된 사용자만 정보 자산에 접근할 수 있도록 하는 성질이며 키워드는 비인가 접근 차단, 접근통제이다.
가용성은 필요한 시점에 정보 자산과 서비스에 접근할 수 있도록 보장하는 성질이며 키워드는 서비스 지속, DDoS 대응이다.

NoteBase

선지별 해설

① X
(가)를 무결성으로 본 점은 맞지만, (나)를 가용성으로 둔 부분이 틀리다. '인가된 사용자만 접근'은 기밀성에 해당한다. 또한 (다)는 필요한 시점의 접근 가능성이므로 기밀성이 아니라 가용성이다.

② O
(가) 무결성, (나) 기밀성, (다) 가용성의 대응이 모두 맞다. 변경, 가장, 재전송 공격은 무결성을 해치고, 방화벽, 암호, 패스워드는 기밀성을 보장하며, DDoS는 가용성을 떨어뜨린다.

③ X
(가)를 기밀성으로 둔 부분이 틀리다. '인가한 방법으로만 정보를 변경'은 접근 자체보다 변경의 정확성을 다루므로 무결성이다. (나)도 가용성이 아니라 기밀성이다. (다)를 무결성으로 둔 것도 틀리며, 필요한 시점의 접근 가능성은 가용성이다.

④ X
(다)를 가용성으로 본 점만 맞다. 그러나 (가)는 기밀성이 아니라 무결성이고, (나)는 무결성이 아니라 기밀성이다.

오답 포인트

무결성과 기밀성을 '보호한다'는 넓은 의미로만 외우면 (가)와 (나)가 뒤바뀐다. 이 문항은 '변경을 통제하는가'와 '접근을 통제하는가'를 구분하지 못하면 쉽게 틀리도록 구성되어 있다.

다시 나오면 이렇게 판단

문장에 '변경, 위조, 재전송'이 나오면 무결성을 먼저 떠올리고, '접근 권한, 비인가 사용자 차단'이 나오면 기밀성을 본다. '필요한 시점, 서비스 지속, DDoS'가 나오면 가용성으로 판단한다.

암기 포인트

무결성은 변경, 기밀성은 접근, 가용성은 사용 가능 상태를 지키는 성질이다.

NoteBase

문 2. 블록암호 알고리즘 운영모드에 대한 설명으로 가장 옳지 않은 것은?

① CBC 모드는 현재의 평문 블록을 암호키로 암호화한 후 바로 직전의 암호블록과 XOR 연산을 수행한다.

② CFB 모드 동작에서는 평문 블록 내에 한 비트의 오류가 발생하면 모든 암호문에 영향을 미치게 된다.

③ OFB 모드는 전송 중에 비트 오류가 전파되지 않는 동기식 스트림 암호이다.

④ CTR 모드는 패딩이 필요 없고 암호화 및 복호화의 사전 준비를 할 수 있어 병렬처리가 가능하다.

정답 1번

출제 포인트

이 문제는 CBC, CFB, OFB, CTR 모드의 동작 순서와 오류 전파 특성을 구별하는 문제이다.

핵심 개념

CBC는 현재 평문 블록을 직전 암호문 블록과 XOR한 뒤 블록암호로 암호화하는 체인 방식이다.
CFB는 블록암호의 출력을 되먹임해 사용하는 자기동기식 스트림 방식으로, 입력 변화가 이후 암호문에도 연쇄 영향을 줄 수 있다.
OFB는 블록암호 출력만 계속 되먹임해 키스트림을 만드는 동기식 스트림 방식이므로 전송 중 비트 오류가 다음 비트들로 전파되지 않는다.
CTR은 카운터 값을 암호화해 키스트림을 만드는 방식이므로 패딩이 필요 없고 각 블록을 독립적으로 처리할 수 있다.

NoteBase

선지별 해설

① X
틀린 부분은 "암호화한 후 바로 직전의 암호블록과 XOR"라는 표현이다.
CBC는 평문을 먼저 직전 암호문 블록과 XOR한 뒤 그 결과를 암호화한다. 올바르게는 "현재 평문 블록을 직전 암호문 블록과 XOR한 후 암호화한다"이다.

② O
CFB는 이전 암호문이 다음 단계 입력으로 되먹임되므로 평문의 한 비트 변화가 현재 암호문뿐 아니라 이후 암호문에도 영향을 줄 수 있다. 되먹임 구조 때문에 연쇄 영향이 생긴다는 점이 핵심이다.

③ O
OFB는 암호문 자체를 다시 입력에 쓰지 않고, 내부에서 생성한 출력으로 키스트림을 이어 간다. 따라서 전송 중 암호문 한 비트 오류는 복호 시 같은 위치의 평문 한 비트에만 영향을 주고 다음 비트들로 전파되지 않는다.

④ O
CTR은 카운터를 암호화해 키스트림을 만들므로 블록 길이에 맞추기 위한 패딩이 필요 없다. 각 카운터 블록을 독립적으로 계산할 수 있어 암호화와 복호화 모두 사전 준비와 병렬 처리가 가능하다.

오답 포인트

CBC와 CFB는 모두 이전 결과가 다음 단계에 연결된다는 점 때문에 혼동하기 쉽다. 이 문항의 함정은 각 모드의 공통점이 아니라 "XOR를 언제 하느냐"와 "오류가 어디까지 전파되느냐"를 바꿔 놓는 데 있다.

다시 나오면 이렇게 판단

운영모드 문제는 먼저 입력에 무엇이 되먹임되는지, 그다음 XOR가 암호화 전인지 후인지를 본다. 이어서 암호문 1비트 오류가 다음 블록까지 번지는지, 키스트림만 계속 생성하는지를 확인하면 정오 판단이 빨라진다.

암기 포인트

CBC는 XOR 후 암호화, CFB는 암호문 되먹임, OFB는 출력 되먹임, CTR은 카운터 독립 처리이다.

NoteBase

문 3. 「개인정보 보호법」에서 규정하는 개인정보보호책임자의 업무로 가장 옳지 않은 것은?

① 개인정보 보호 계획의 수립 및 시행

② 개인정보 처리와 관련한 불만의 처리 및 피해 구제

③ 정보보호 취약점 분석·평가 및 개선

④ 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기

정답 3번

쟁점

이 문제는 개인정보보호책임자의 법정 업무를 구별하는 문제이다.
핵심은 개인정보 처리·보호에 직접 연결된 업무와 정보시스템 일반 보안업무를 구별하는 것이다.

용어 풀이

개인정보보호책임자 = 개인정보 처리에 관한 업무를 총괄하면서 개인정보 보호체계를 관리하는 책임자이다.

핵심 구분

개인정보보호책임자의 업무는 개인정보 보호 계획, 처리 실태 점검, 불만 처리, 유출 방지, 교육, 처리방침·자원 관리, 파기처럼 개인정보 처리와 직접 연결된 항목들이다.
반면 정보보호 취약점 분석·평가는 정보시스템 전반의 보안진단 표현에 가깝고, 개인정보보호책임자의 법정 업무를 그대로 적은 문구는 아니다.

NoteBase

선지별 해설

① O
개인정보 보호 계획의 수립 및 시행은 개인정보 보호체계를 운영하는 기본 업무이므로 맞다.

② O
개인정보 처리와 관련한 불만의 처리 및 피해 구제는 정보주체의 권리보호와 직접 연결되는 법정 업무이므로 맞다.

③ X
'정보보호 취약점 분석·평가'라는 표현이 틀렸다. 이는 정보시스템 전반의 보안진단 업무 표현에 가깝고, 개인정보보호책임자의 법정 업무로 열거된 항목은 아니다.
틀린 표현: 정보보호 취약점 분석·평가 및 개선
올바른 표현: 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선, 또는 개인정보 유출·오용·남용 방지를 위한 내부통제시스템의 구축·운영으로 이해하는 것이 맞다.

④ O
처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기는 개인정보의 안전한 종료관리와 직접 연결되는 업무이므로 맞다.

오답 포인트

③은 '개선'이라는 단어 때문에 그럴듯해 보이지만, 법이 말하는 것은 개인정보 처리 실태의 조사·개선이나 내부통제 구축이지 정보보호 취약점 분석·평가라는 일반 보안진단 표현이 아니다. 개인정보보호 업무와 정보보호 일반업무를 섞으면 틀리기 쉽다.

다시 나오면 이렇게 판단

개인정보보호책임자 문제는 선지의 표현이 개인정보 처리와 정보주체 보호에 직접 연결되는 법정 업무인지 먼저 본다. 계획 수립, 불만 처리, 파기처럼 조문형 표현은 맞고, 정보시스템 일반 보안진단 표현은 한 번 더 의심하는 방식으로 판단한다.

암기 포인트

개인정보보호책임자는 개인정보 처리 전 과정을 관리한다. 취약점 진단 자체보다
계획·불만처리·파기·내부통제가 핵심이다.

NoteBase

문 4. <보기>에서 SSL(Secure Sockets Layer)프로토콜이 수신된 데이터에 제공하는 서비스를 모두 고른 것은?

<보기>
ㄱ. 압축
ㄴ. 메시지 무결성
ㄷ. 기밀성
ㄹ. 단편화

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄱ, ㄴ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ

정답 4번

출제 포인트

이 문제는 SSL 레코드 프로토콜이 데이터에 제공하는 기본 서비스가 무엇인지 묻는 문제이다.

핵심 개념

압축은 전송 전에 데이터를 줄여 효율을 높이는 처리이다.
메시지 무결성은 MAC 등을 통해 전송 중 데이터가 변조되지 않았는지 확인하는 기능이다.
기밀성은 암호화를 통해 제3자가 내용을 읽지 못하게 하는 기능이다.
단편화는 상위 계층 데이터를 전송 가능한 블록으로 나누어 레코드 단위로 처리하는 기능이다.
SSL 레코드 프로토콜은 단편화, 압축, 메시지 무결성, 기밀성을 모두 제공한다.

NoteBase

선지별 해설

① X
ㄱ, ㄴ만 고른 선택지이다. SSL은 압축과 메시지 무결성만 제공하는 것이 아니라 기밀성(암호화)과 단편화도 함께 제공한다. 틀린 구성은 ㄷ, ㄹ을 빠뜨린 점이며, 올바르게는 ㄱ, ㄴ, ㄷ, ㄹ 모두이다.

② X
ㄱ, ㄷ만 고른 선택지이다. 압축과 기밀성은 맞지만 메시지 무결성과 단편화가 빠져 있다. 틀린 구성은 ㄴ, ㄹ을 제외한 점이며, 올바르게는 ㄱ, ㄴ, ㄷ, ㄹ 모두이다.

③ X
ㄱ, ㄴ, ㄹ만 고른 선택지이다. 압축, 메시지 무결성, 단편화는 맞지만 기밀성이 빠져 있다. 틀린 구성은 ㄷ을 제외한 점이며, 올바르게는 ㄱ, ㄴ, ㄷ, ㄹ 모두이다.

④ O
ㄱ 압축, ㄴ 메시지 무결성, ㄷ 기밀성, ㄹ 단편화를 모두 포함한 선택지이다. SSL 레코드 프로토콜의 대표 서비스들을 빠짐없이 고른 구성이다.

오답 포인트

SSL을 암호화와 무결성만 제공하는 프로토콜로 좁게 외우면 ㄷ이나 ㄴ만 보고 고르기 쉽다. 이 문항은 레코드 프로토콜 수준의 처리 기능인 압축과 단편화까지 함께 기억하는지를 확인하는 함정이다.

다시 나오면 이렇게 판단

SSL의 서비스 문제는 암호화만 떠올리지 않고 레코드 처리 순서를 함께 본다. 데이터를 잘라서 처리하는 단편화, 크기를 줄이는 압축, 변조 검사를 위한 무결성, 내용 보호를 위한 기밀성을 한 묶음으로 판단하면 된다.

암기 포인트

SSL 레코드 프로토콜은 자르고, 줄이고, 검사하고, 숨긴다.

NoteBase

문 5. <보기>에서 설명하는 접근 제어 모델로 가장 옳은 것은?

<보기>
시스템 자원이 얼마나 민감하고 중요한지를 나타내는 보안 레이블과 어떤 시스템 개체가 특정 자원에 접근할 수 있는지를 나타내는 보안 허가에 기반하는 접근제어 방식이다.

① 강제 접근 제어(Mandatory Access Control)
② 임의 접근 제어(Discretionary Access Control)
③ 역할 기반 접근 제어(Role-based Access Control)
④ 속성 기반 접근 제어(Attribute-based Access Control)

정답 1번

출제 포인트

이 문제는 보안 레이블과 보안 허가를 기준으로 자원 접근을 통제하는 강제 접근 제어와 다른 접근 제어 모델의 차이를 묻는 문제이다.

핵심 개념

강제 접근 제어(MAC)는 시스템이 부여한 보안 등급과 보안 허가에 따라 접근을 통제하는 방식이다. 자원의 민감도와 주체의 허가 수준이 기준이 된다.
임의 접근 제어(DAC)는 객체 소유자가 접근 권한을 정하는 방식이다. 소유자 재량과 권한 위임이 핵심이다.
역할 기반 접근 제어(RBAC)는 사용자에게 부여된 역할에 따라 권한을 묶어서 관리하는 방식이다. 직무와 역할이 기준이 된다.
속성 기반 접근 제어(ABAC)는 사용자, 자원, 환경의 여러 속성을 조합해 접근 여부를 결정하는 방식이다. 다양한 속성 정책이 기준이 된다.

NoteBase

선지별 해설

① O
보안 레이블과 보안 허가에 따라 접근을 통제한다는 설명은 강제 접근 제어의 전형적인 특징이다. 군사·기밀 등급처럼 시스템이 정한 보안 정책이 우선한다.

② X
틀린 부분은 임의 접근 제어이다.
실제로는 객체 소유자가 자신의 재량으로 접근 권한을 설정하는 방식이 임의 접근 제어이다. 보기처럼 보안 레이블과 보안 허가를 기준으로 중앙 통제하는 방식은 아니다.

③ X
틀린 부분은 역할 기반 접근 제어이다.
실제로는 사용자에게 부여된 역할에 따라 권한을 관리하는 방식이 역할 기반 접근 제어이다. 보기처럼 자원의 민감도와 주체의 보안 허가를 직접 대응시키는 모델은 아니다.

④ X
틀린 부분은 속성 기반 접근 제어이다.
실제로는 사용자 속성, 자원 속성, 시간·위치 같은 환경 속성을 함께 평가하는 방식이 속성 기반 접근 제어이다. 보기의 설명처럼 보안 등급 레이블과 허가 등급 중심으로 동작하는 모델과는 구별된다.

오답 포인트

보기의 핵심 표현은 보안 레이블과 보안 허가이다. 이 표현을 놓치면 RBAC의 역할, ABAC의 속성, DAC의 소유자 재량과 MAC의 등급 기반 통제를 서로 혼동하기 쉽다.

다시 나오면 이렇게 판단

선지나 보기에서 등급, 기밀성, 보안 레이블, 보안 허가가 나오면 먼저 MAC를 떠올리면 된다. 소유자가 정하면 DAC, 역할이 기준이면 RBAC, 여러 속성을 조합하면 ABAC로 판단할 수 있다.

암기 포인트

MAC는 레이블·허가, DAC는 소유자 재량, RBAC는 역할, ABAC는 속성 조합이다.

NoteBase

문 6. 가상사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?

① PPTP는 OSI 3계층에서 동작하는 터널링 기술이다.

② 이미 구축되어 있는 공용망을 이용하므로 추가적인 구축비용 부담이 적다.

③ 가상사설망은 응용프로그램 하단 계층에서 작동하므로 응용프로그램을 수정할 필요가 없다.

④ 정보의 기밀성을 제공하기 위해 데이터를 암호화한다.

정답 1번

출제 포인트

이 문제는 VPN의 장점과 함께 터널링 프로토콜이 동작하는 계층을 구분하는지를 묻는 문제이다.

핵심 개념

PPTP는 PPP 프레임을 터널링하는 프로토콜로 보통 2계층 기반 VPN으로 분류된다.
IPsec은 IP 패킷을 보호하므로 3계층 기반 VPN에 해당한다.
VPN은 공용망을 전용망처럼 사용하면서 암호화로 기밀성을 확보하고, 응용프로그램 아래 계층에서 동작해 기존 응용프로그램을 그대로 사용할 수 있다.

선지별 해설

① X: 틀린 부분은 "OSI 3계층"이다. PPTP는 PPP 기반 터널링으로 보통 2계층 VPN 기술로 분류되므로 3계층에서 동작하는 기술이라고 볼 수 없다. 올바르게는 "PPTP는 OSI 2계층 기반의 터널링 기술이다."이다.
② O: VPN은 이미 구축된 인터넷 같은 공용망을 이용해 논리적 사설망을 구성하므로 전용 회선을 새로 설치하는 방식보다 구축비용 부담이 작다.
③ O: VPN은 응용계층 아래에서 터널링과 암호화를 처리하므로 일반적으로 기존 응용프로그램 자체를 수정하지 않고 사용할 수 있다.
④ O: VPN은 전송 데이터를 암호화해 공용망 구간에서도 제3자가 내용을 쉽게 읽지 못하게 하므로 기밀성 제공에 기여한다.

오답 포인트

PPTP와 IPsec의 계층을 뒤바꾸는 함정이 핵심이다. PPTP는 PPP 기반 터널링, IPsec은 IP 계층 보호라는 기준으로 나누면 ①의 오류를 바로 찾을 수 있다.

다시 나오면 이렇게 판단

VPN 선지가 나오면 먼저 어떤 프로토콜이 어느 계층을 기준으로 보호하는지 본다. PPP 프레임을 터널링하면 2계층 계열, IP 패킷 자체를 보호하면 3계층 계열로 판단하면 된다.

NoteBase

암기 포인트

PPTP·L2TP는 2계층 계열, IPsec은 3계층 계열, VPN은 공용망 사용·암호화·응용프로그램 수정 불필요가 기본 특징이다.

NoteBase

문 7. 악성 소프트웨어에 대한 설명으로 가장 옳지 않은 것은?

① 트로이목마는 악성 루틴이 숨어 있는 프로그램으로, 겉보기에는 정상적인 프로그램으로 보이지만 프로그램을 실행하면 악성 코드가 실행된다.

② 스파이웨어는 특정 컴퓨터를 감염시켜 장악한 뒤 원격 조정할 수 있는 스파이 네트워크로, 해커는 파일을 검색하거나 내려 받을 수 있고 촬영이나 녹음을 지시할 수도 있다.

③ 랜섬웨어는 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성 코드이다.

④ PC의 부팅영역인 MBR을 조작하는 프로그램을 부트킷이라 한다.

정답 2번

출제 포인트

이 문제는 대표적 악성 소프트웨어의 정의와 기능을 구별할 수 있는지를 묻는 문제이다.

핵심 개념

트로이목마는 정상 프로그램처럼 보이지만 내부에 악성 기능을 숨겨 실행되게 하는 악성코드이다.
스파이웨어는 사용자 동의 없이 설치되어 사용자의 정보나 활동 내역을 몰래 수집하는 악성 프로그램이다.
랜섬웨어는 파일을 암호화하거나 시스템 사용을 제한한 뒤 금전을 요구하는 악성코드이다.
부트킷은 부팅 영역이나 부트 로더를 감염시키는 루트킷 계열 악성코드이다.

선지별 해설

1번 O: 트로이목마는 겉보기에는 정상 프로그램처럼 보이지만 실행 시 숨겨진 악성 기능이 함께 동작하는 형태이므로 설명이 맞다.
2번 X: 틀린 부분은 "스파이웨어는 특정 컴퓨터를 감염시켜 장악한 뒤 원격 조정할 수 있는 스파이 네트워크"라는 표현이다. 실제로 원격 제어, 파일 검색·다운로드, 촬영·녹음 지시는 백도어·원격제어형 트로이목마 또는 봇넷의 특징에 가깝고, 스파이웨어의 핵심은 사용자 정보의 은밀한 수집이다.
3번 O: 랜섬웨어는 문서·사진 등의 파일을 암호화한 뒤 일정 시간 내 금전 지급을 요구하고 복호화 대가를 제시하는 악성코드이므로 설명이 맞다.
4번 O: 부트킷은 PC의 부팅 과정에 관여하는 MBR이나 부트 영역을 조작해 은닉성과 지속성을 확보하는 악성코드이므로 설명이 맞다.

오답 포인트

스파이웨어를 "몰래 정보 수집"이 아니라 "감염 후 원격 조종"으로 기억하면 2번에 속기 쉽다. 출제자는 스파이웨어와 백도어·봇넷의 기능을 섞어 놓아 개념 구분이 흐려지는 지점을 노렸다.

NoteBase

다시 나오면 이렇게 판단

악성코드 문제는 먼저 주기능을 기준으로 분류하면 된다. 정상 프로그램 위장 실행이면 트로이목마, 정보 몰래 수집이면 스파이웨어, 파일 암호화 후 금전 요구이면 랜섬웨어, 부팅 영역 감염이면 부트킷으로 판단한다.

암기 포인트

스파이웨어는 수집, 백도어는 원격제어, 랜섬웨어는 암호화와 금전 요구, 부트킷은 MBR·부트영역 감염이다.

NoteBase

문 8. 리버스 엔지니어링을 어렵게 만드는 안티 리버싱 기술에 대한 설명으로 가장 옳지 않은 것은?

① 원본 프로그램을 새로운 파일에 패킹된 형태로 압축하고 암호화하여 저장한다.

② 공격에 이용될 수 있는 코드를 최소화하기 위해 쓰레기(Garbage)코드를 모두 삭제한다.

③ 리버스 엔지니어링 수행을 위한 디버거 활동을 탐지하여 프로그램을 강제 종료한다.

④ 다단계 점프문을 섞어 코드를 치환하여 배치한다.

정답 2번

출제 포인트

이 문제는 패킹, 가비지 코드, 안티 디버깅, 제어 흐름 난독화처럼 대표적인 안티 리버싱 기법의 목적과 동작을 구별할 수 있는지를 묻는다.

핵심 개념

패킹은 실행 파일을 압축하거나 암호화한 뒤 복원 루틴과 함께 재구성하여 분석을 어렵게 하는 기법이다.
가비지 코드는 실제 기능과 무관한 명령을 끼워 넣어 분석자가 읽어야 할 양을 늘리는 난독화 기법이다.
안티 디버깅은 디버거 부착, 브레이크포인트, 실행 환경 변조를 탐지해 분석을 방해하는 기법이다.
제어 흐름 난독화는 점프와 분기를 복잡하게 섞어 코드의 실제 실행 순서를 파악하기 어렵게 만드는 기법이다.

선지별 해설

1번 O: 패킹은 원본 프로그램을 압축하거나 암호화한 형태로 다시 저장해 정적 분석을 어렵게 만든다. 실행 시에는 언패킹 과정을 거쳐 원래 코드가 메모리에서 복원된다.
2번 X: 틀린 부분은 "쓰레기(Garbage) 코드를 모두 삭제한다"는 표현이다. 가비지 코드는 삭제하는 대상이 아니라 오히려 삽입하여 분석을 혼란스럽게 만드는 난독화 요소이다. 올바르게는 "공격자나 분석자를 혼란시키기 위해 실제 기능과 무관한 가비지 코드를 삽입한다"이다.
3번 O: 안티 디버깅은 디버거 사용 여부를 탐지해 실행을 중단하거나 강제 종료하도록 만들어 리버스 엔지니어링을 방해한다.
4번 O: 다단계 점프문을 섞어 코드를 치환하여 배치하는 방식은 제어 흐름을 복잡하게 만들어 역분석자가 코드의 실제 흐름을 추적하기 어렵게 하는 난독화 기법에 해당한다.

오답 포인트

가비지 코드라는 말 때문에 불필요한 코드를 제거하는 최적화처럼 읽으면 2번에 속기 쉽다. 안티 리버싱 문맥에서 가비지 코드는 제거 대상이 아니라 분석 방해를 위해 추가하는 코드라는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

선지마다 해당 기법의 목적이 무엇인지 먼저 본다. 숨기는 기법이면 패킹, 쓸모없는 코드를 끼워 넣으면 가비지 코드, 디버거를 막으면 안티 디버깅, 실행 흐름을 꼬아 놓으면 제어 흐름 난독화로 판단할 수 있다.

암기 포인트

패킹은 숨김, 가비지 코드는 삽입, 안티 디버깅은 탐지, 제어 흐름 난독화는 점프 혼선이다.

NoteBase

문 9. 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 대칭키 암호 알고리즘은 공개키 암호 알고리즘보다 수행속도가 매우 빠르다.

② 하이브리드 암호 시스템에서 세션키는 공개키 암호화 방식을 사용해서 복호화한다.

③ 대칭키 암호 시스템에서 MAC(메시지 인증 코드)을 이용하여 기밀성과 무결성을 제공한다.

④ 타원 곡선 암호는 RSA보다 키의 비트수를 적게 하면서도 동일한 성능을 제공하는 것이 가장 큰 특징이다.

정답 3번

출제 포인트

대칭키 암호, 공개키 암호, 하이브리드 암호, MAC, 타원 곡선 암호의 역할과 차이를 정확히 구분하는 문제이다.

핵심 개념

대칭키 암호는 송수신자가 같은 비밀키로 데이터를 빠르게 암호화·복호화하는 방식이다.
공개키 암호는 공개키와 개인키를 나누어 키 교환, 전자서명, 세션키 전달에 주로 쓰는 방식이다.
하이브리드 암호는 데이터 본문은 대칭키로 처리하고, 세션키 전달만 공개키 방식으로 처리하는 결합 구조이다.
MAC은 비밀키를 이용해 메시지의 위변조 여부를 확인하는 값으로, 무결성과 인증을 지원하지만 기밀성을 직접 제공하지는 않는다.
타원 곡선 암호는 RSA보다 짧은 키 길이로도 동등한 보안 강도를 달성하는 것이 대표적 특징이다.

선지별 해설

① O 대칭키 암호는 공개키 암호보다 연산이 단순하여 일반적으로 훨씬 빠르다. 대용량 데이터 암호화에 대칭키가 쓰이는 대표 이유가 수행 속도이다.
② O 하이브리드 암호 시스템에서는 세션키를 공개키 암호 방식으로 보호한다. 세션키는 수신자의 공개키로 암호화되어 전달되고, 수신자는 자신의 개인키로 복호화하므로 문장의 취지는 맞다.
③ X 틀린 표현은 'MAC을 이용하여 기밀성과 무결성을 제공한다'이다. MAC은 메시지 인증과 무결성 검증에는 쓰이지만 내용을 숨기는 기능은 없으므로 기밀성을 제공하지 않는다. 올바르게는 '대칭키 암호는 암호화로 기밀성을 제공하고, MAC은 무결성과 인증을 제공한다'이다.
④ O 타원 곡선 암호는 RSA보다 더 짧은 키 길이로도 비슷한 보안 강도를 낼 수 있다. 이 문장은 '동일한 보안 수준을 더 작은 키로 달성한다'는 취지로 이해하면 맞는 설명이다.

오답 포인트

③은 MAC과 암호화를 하나로 섞어 놓은 점이 함정이다. 무결성 검사는 MAC의 역할이고, 기밀성은 암호화의 역할이므로 기능 축을 분리해서 보아야 한다.

NoteBase

다시 나오면 이렇게 판단

암호 문제는 먼저 기능을 셋으로 나누면 된다. 데이터 내용을 숨기면 기밀성, 위변조를 확인하면 무결성, 세션키를 안전하게 전달하면 공개키 기반 키 교환으로 정리하면 선지 판단이 빨라진다.

암기 포인트

기밀성은 암호화, 무결성은 MAC, 세션키 전달은 공개키, 대용량 본문 처리는 대칭키이다.

NoteBase

문 10. <보기>에서 2-요소 인증(Two-factor authentication) 방식에 해당하는 것을 모두 고른 것은?

<보기>
ㄱ. 정부24 사이트 사용을 위해, 보안 토큰에 저장되어 있는 공인인증서를 로딩하고 공인인증서 패스워드를 입력하여 로그인하였다.
ㄴ. OTP(one-time-password)를 인터넷 쇼핑몰 사이트에 입력하고 사용자 인증을 수행하였다.
ㄷ. ATM에서 현금을 인출하기 위해 현금카드를 ATM 기기에 꽂고 계좌 비밀번호를 입력하였다.
ㄹ. 서버실 출입문을 열기 위해서 얼굴인식과 홍채인증을 하였다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 2번

출제 포인트

이 문제는 각 사례를 지식 요소, 소유 요소, 생체 요소로 분류한 뒤 서로 다른 두 요소를 함께 쓴 경우만 2-요소 인증에 해당하는지를 묻는 문제이다.

사례 정리

ㄱ은 보안 토큰과 인증서 비밀번호를 함께 사용한 사례이다.
ㄴ은 OTP만 입력한 사례이다.
ㄷ은 현금카드와 계좌 비밀번호를 함께 사용한 사례이다.
ㄹ은 얼굴인식과 홍채인증을 함께 사용한 사례이다.

핵심 개념

2-요소 인증은 서로 다른 범주의 인증요소 두 가지를 함께 사용하는 인증이다. 대표 범주는 지식 요소(비밀번호), 소유 요소(카드·토큰), 생체 요소(지문·얼굴·홍채)이다. 같은 범주의 수단을 두 개 써도 2-요소 인증은 아니다.

적용 기준

각 사례의 인증수단을 먼저 지식, 소유, 생체 중 어디에 속하는지 나눈다. 그다음 서로 다른 범주가 정확히 두 개 결합되었는지 판단하면 된다.

NoteBase

선지별 해설

① X: 틀린 부분은 "ㄴ"이다. ㄱ은 보안 토큰이라는 소유 요소와 인증서 비밀번호라는 지식 요소를 함께 써서 2-요소 인증에 해당하지만, ㄴ은 OTP만 입력한 사례라 한 가지 인증수단만 제시되어 있다. 올바르게는 ㄱ, ㄷ이어야 한다.
② O: ㄱ은 소유 요소와 지식 요소의 결합이고, ㄷ은 현금카드라는 소유 요소와 계좌 비밀번호라는 지식 요소의 결합이므로 둘 다 2-요소 인증에 해당한다.
③ X: 틀린 부분은 "ㄴ"이다. ㄷ은 2-요소 인증이 맞지만 ㄴ은 OTP 단독 사용이라 2-요소 인증이 아니다. 올바르게는 ㄱ, ㄷ이다.
④ X: 틀린 부분은 "ㄴ, ㄹ"이다. ㄴ은 OTP만 제시되어 단일 요소 인증이고, ㄹ은 얼굴인식과 홍채인증이 모두 생체 요소라 같은 범주의 두 수단을 쓴 경우이다. 올바르게는 ㄱ, ㄷ이다.

오답 포인트

인증수단이 두 번 나오면 무조건 2-요소 인증이라고 오해하기 쉽다. 그러나 2-요소 인증은 수단의 개수가 아니라 범주의 개수를 본다. OTP 하나만 쓰는 경우와 생체정보 두 가지를 쓰는 경우를 모두 2-요소 인증으로 착각하면 틀린다.

다시 나오면 이렇게 판단

인증 문제는 각 수단을 지식, 소유, 생체로 먼저 분류한 뒤 서로 다른 범주 두 개가 함께 쓰였는지만 확인하면 된다. 같은 범주 두 개이거나 한 범주 하나만 제시되면 2-요소 인증이 아니다.

암기 포인트

2-요소 인증은 인증을 두 번 하는 것이 아니라 서로 다른 인증요소 두 개를 결합하는 방식이다.

NoteBase

문 11. 「개인정보의 안전성 확보조치 기준」에 대한 설명으로 가장 옳지 않은 것은?

① 개인정보취급자란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.

② 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

③ 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

④ 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 연1회 이상 점검하여야 한다.

정답 4번

쟁점

이 문제는 「개인정보의 안전성 확보조치 기준」상 개인정보취급자의 의미, 내부 관리계획 점검 주체와 주기, 접근권한 부여 원칙, 접속기록 점검 주기를 구별하는 문제이다.
핵심은 연 1회 점검 사항과 월 1회 점검 사항을 혼동하지 않는 것이다.

용어 풀이

개인정보취급자 = 개인정보처리자의 지휘·감독 아래 개인정보 처리 업무를 실제로 담당하는 자이다.
접속기록 = 개인정보처리시스템에 누가 언제 접속해 어떤 처리를 했는지를 남긴 기록이다.

핵심 구분

내부 관리계획의 이행 실태 점검은 개인정보보호책임자가 연 1회 이상 수행하는 사항이다.
반면 개인정보처리시스템의 접속기록 점검은 개인정보 오·남용이나 유출 등에 대응하기 위한 통제라서 월 1회 이상 수행하여야 한다.
접근권한은 업무 수행에 필요한 최소한의 범위에서 업무 담당자별로 차등 부여하는 것이 원칙이다.

NoteBase

선지별 해설

① O
개인정보취급자는 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자를 말한다. 임직원뿐 아니라 파견근로자, 시간제근로자 등도 포함될 수 있으므로 선지 설명이 맞다.

② O
접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태는 개인정보보호책임자가 연 1회 이상 점검·관리하여야 한다. 선지는 연간 점검 사항을 정확히 적었다.

③ O
개인정보처리시스템 접근권한은 업무 수행에 필요한 최소한의 범위로 제한하고, 업무 담당자에 따라 차등 부여하여야 한다. 최소권한 원칙과 역할별 권한 분리가 기준 내용과 일치한다.

④ X
틀린 표현은 "연1회 이상"이다. 개인정보처리시스템의 접속기록 등은 연 1회가 아니라 월 1회 이상 점검하여야 한다. 접속기록 점검은 이상 접속과 오·남용 징후를 조기에 발견하기 위한 통제이므로 점검 주기가 더 짧다. 올바른 표현은 "개인정보처리자는 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다."이다.

오답 포인트

②의 연 1회 점검과 ④의 접속기록 점검 주기를 같은 범주로 묶어 보면 오답이 된다. 내부 관리계획의 이행 실태 점검은 연 1회 이상이고, 접속기록 점검은 월 1회 이상이라는 주기 차이가 출제 포인트이다.

다시 나오면 이렇게 판단

안전성 확보조치 기준 문제에서는 먼저 주체와 통제 대상을 나눈다. 그다음 연 1회인지 월 1회인지처럼 주기를 묻는 표현이 나오면 내부 관리계획 이행 점검인지, 접속기록 상시 통제인지 구분하여 판단한다.

암기 포인트

내부 관리계획 이행 실태는 연 1회, 접속기록 점검은 월 1회이다.

NoteBase

문 12. 키 교환 알고리즘인 Diffie-Hellman 알고리즘에 대한 설명으로 가장 옳지 않은 것은?

① 이 알고리즘의 안전성은 이산대수를 계산하는 어려움에 기초한다.

② 대칭키를 공유하기 위해 사용한다.

③ 중간자 공격에 대해 강한 안전성을 가진다.

④ 실제로 키를 교환하는 것이 아니고, 공유할 키를 각자 계산하여 만들어내는 것이다.

정답 3번

출제 포인트

이 문항은 Diffie-Hellman 키 교환의 목적, 안전성 근거, 그리고 한계를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

Diffie-Hellman은 공개된 매개값과 각자의 비밀값을 이용해 같은 공유 비밀을 계산하는 키 교환 방식이다.
안전성의 핵심은 공개값만 보고 비밀 지수를 역산하기 어려운 이산대수 문제에 있다.
다만 기본 Diffie-Hellman은 상대방 인증 기능이 없어서 중간자 공격에는 취약하다.

선지별 해설

① O
이산대수 문제의 어려움에 기반한다는 설명은 맞다. 공개된 값만 보고 각자의 비밀 지수를 역으로 구하기 어렵다는 점이 안전성의 근거이다.

② O
Diffie-Hellman은 통신 당사자가 같은 대칭키 재료를 공유하도록 만드는 데 사용된다. 최종 목적은 대칭키 암호에 쓸 공유 비밀을 만드는 것이다.

③ X
틀린 부분은 "중간자 공격에 대해 강한 안정성을 가진다"는 표현이다. 기본 Diffie-Hellman은 상대방을 인증하지 않으므로 중간자 공격에 취약하다. 올바르게는 "추가적인 인증 절차가 없으면 중간자 공격에 취약하다"가 된다.

④ O
이 방식은 비밀키 자체를 전송해서 교환하는 구조가 아니다. 각자가 자신의 비밀값과 상대의 공개값을 이용해 동일한 공유 비밀을 계산해 만들어 낸다.

NoteBase

오답 포인트

수험생은 Diffie-Hellman이 널리 쓰인다는 이유만으로 ③도 안전하다고 오해하기 쉽다. 그러나 많이 쓰인다는 사실과 인증 기능 보유 여부는 별개이며, 기본형은 키 교환만 제공할 뿐 상대 신원 확인은 제공하지 않는다.

다시 나오면 이렇게 판단

Diffie-Hellman 문제가 나오면 먼저 "무엇을 하는가"와 "무엇을 못 하는가"를 나눠 본다. 공유 비밀 계산은 가능하지만, 기본형만으로는 인증이 되지 않으므로 중간자 공격 방어 문구가 나오면 틀린 선지로 판단할 수 있다.

암기 포인트

Diffie-Hellman은 공유 비밀 계산은 가능하고, 기본형만으로는 인증이 불가능하다.

NoteBase

문 13. 웹 보안 취약점에 관한 <보기>의 설명에서 (가), (나)에 들어갈 말을 옳게 짝지은 것은?

<보기>
(가) 공격은 브라우저로 전달되는 데이터에 악성 스크립트가 포함되어 개인의 브라우저에서 실행되면서 해킹을 하는 것이며, 이 공격용 악성 스크립트는 공격자가 웹 서버에 구현된 웹 어플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입을 해 놓은 것이다. 이에 대한 대응 조치로 게시물의 본문뿐만 아니라 댓글 및 검색어 입력 창 등 사용자 측에서 전달되는 모든 값에 대해서 (나)을/를 수행한다.

① (가): Cross Site Scripting, (나): 암호화
② (가): Cross Site Request Forgery, (나): 암호화
③ (가): Cross Site Request Forgery, (나): 필터링
④ (가): Cross Site Scripting, (나): 필터링

정답 4번

출제 포인트

이 문제는 XSS와 CSRF의 차이를 구분하고, XSS의 대표 대응 조치를 연결할 수 있는지를 묻는 문제이다.

핵심 개념

XSS는 웹 페이지에 삽입된 악성 스크립트가 피해자의 브라우저에서 실행되는 공격이다. 결정 차이축은 스크립트 삽입과 브라우저 실행이다. 키워드는 스크립트 실행, 입력값 검증, 필터링이다.
CSRF는 사용자가 의도하지 않은 요청을 서버에 보내게 만들어 서버 측 행위를 유발하는 공격이다. 결정 차이축은 요청 위조와 사용자 세션 악용이다. 키워드는 요청 위조, 세션, 토큰이다.
암호화는 데이터를 읽지 못하게 보호하는 기법이지, 삽입된 스크립트 자체를 제거하는 XSS 대응 조치는 아니다.

선지별 해설

① X이다. (가)는 브라우저로 전달된 악성 스크립트가 사용자 브라우저에서 실행된다고 설명하므로 XSS가 맞다. 그러나 (나)의 암호화는 XSS 대응으로 적절하지 않다. 틀린 표현은 "암호화"이다. 실제로는 사용자 입력값에 대한 필터링이나 출력 시 스크립트가 실행되지 않도록 처리하는 방식이 맞다.
② X이다. 틀린 부분은 (가)의 "Cross Site Request Forgery"이다. 제시문은 위조 요청 전송이 아니라 악성 스크립트 삽입과 브라우저 실행을 설명하므로 CSRF가 아니라 XSS이다. (나)의 암호화도 XSS 대응으로는 맞지 않다.
③ X이다. (나)의 필터링은 XSS 대응으로 맞는 방향이다. 그러나 틀린 부분은 (가)의 "Cross Site Request Forgery"이다. 실제로는 XSS이므로 올바른 짝은 "Cross Site Scripting - 필터링"이다.
④ O이다. 악성 스크립트가 브라우저로 전달되어 사용자 브라우저에서 실행된다는 설명은 XSS이다. 이에 대한 대응으로 사용자 입력값을 필터링하여 스크립트 삽입 가능성을 줄이는 조치가 맞으므로 옳은 짝이다.

NoteBase

오답 포인트

CSRF와 XSS를 모두 "웹 공격"으로만 기억하면 ③처럼 필터링이 보이는 순간 CSRF를 고르기 쉽다. 이 문항의 핵심 함정은 대응 기법보다 먼저 공격의 작동 방식이 스크립트 실행인지 요청 위조인지를 구분하지 못하게 만드는 데 있다.

다시 나오면 이렇게 판단

선지 판단에서는 먼저 공격 결과가 브라우저에서 스크립트 실행인지, 서버에 위조 요청 전송인지부터 본다. 브라우저에서 악성 스크립트가 실행되면 XSS이고, 사용자의 권한으로 원치 않는 요청이 전송되면 CSRF로 판단한다.

암기 포인트

XSS는 스크립트 실행, CSRF는 요청 위조이다. XSS 대응은 입력값 필터링과 스크립트 실행 차단이다.

NoteBase

문 14. <보기>에서 설명하는 네트워크 공격으로 가장 옳은 것은?

<보기>
ICMP 패킷을 일반보다 훨씬 큰 65,500바이트의 크기로 전송하여, 하나의 패킷이 네트워크를 통해 공격 대상에게 전달되는 동안 여러 개의 ICMP 패킷으로 나누어져 시스템에 과부하를 일으키게 한다.

① Ping of Death 공격

② TearDrop 공격

③ Land 공격

④ Smurf 공격

정답 1번

출제 포인트

이 문제는 비정상적으로 큰 ICMP 패킷을 보내 시스템에 과부하를 일으키는 Ping of Death와 다른 대표적 네트워크 공격을 구별하는 문제이다.

핵심 개념

Ping of Death는 비정상적으로 큰 ICMP 패킷을 보내 단편화와 재조립 과정에서 오류나 과부하를 유발하는 공격이다.
TearDrop은 조작된 IP 단편의 오프셋 중첩으로 재조립 오류를 일으키는 공격이다.
Land는 출발지와 목적지의 IP 주소와 포트 번호를 동일하게 꾸며 자기 자신에게 응답하게 만드는 공격이다.
Smurf는 출발지 주소를 피해자로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답이 피해자에게 몰리게 하는 증폭형 공격이다.

NoteBase

선지별 해설

① O
제시문은 매우 큰 ICMP 패킷을 전송해 전송 중 여러 조각으로 나뉘고, 대상 시스템에 과부하를 일으키는 공격을 설명한다. 이는 Ping of Death의 전형적인 설명과 일치한다.
② X
틀린 부분은 "TearDrop"이다.
TearDrop은 큰 ICMP 패킷 자체가 아니라 비정상적으로 겹치게 만든 IP 단편 정보로 재조립 오류를 유발하는 공격이다. 올바르게는 "조작된 단편 오프셋으로 재조립 오류를 노리는 공격은 TearDrop이다"가 된다.
③ X
틀린 부분은 "Land"이다.
Land는 출발지와 목적지 주소 및 포트를 같게 만들어 대상이 자기 자신과 통신하는 것처럼 보이게 하는 공격이다. 올바르게는 "출발지와 목적지 정보를 동일하게 조작하는 공격은 Land이다"가 된다.
④ X
틀린 부분은 "Smurf"이다.
Smurf는 브로드캐스트 네트워크의 다수 호스트가 피해자에게 ICMP 응답을 보내게 만드는 반사·증폭형 공격이다. 올바르게는 "브로드캐스트와 출발지 주소 위조를 이용해 다수 응답을 피해자에게 집중시키는 공격은 Smurf이다"가 된다.

오답 포인트

ICMP가 보인다고 해서 모두 Smurf로, 단편화가 보인다고 해서 모두 TearDrop으로 연결하면 오답이 된다. 이 문항의 핵심은 "매우 큰 ICMP 패킷 자체"가 원인이라는 점이며, 브로드캐스트 증폭이나 단편 오프셋 조작은 제시되지 않았다.

다시 나오면 이렇게 판단

문장에서 먼저 공격의 핵심 동작을 잡으면 된다. 큰 ICMP 패킷과 시스템 과부하는 Ping of Death, 단편 오프셋 중첩은 TearDrop, 출발지와 목적지 동일은 Land, 브로드캐스트 반사 증폭은 Smurf로 판단한다.

암기 포인트

Ping of Death는 큰 ICMP, TearDrop은 단편 오프셋, Land는 자기 자신, Smurf는 브로드캐스트 증폭이다.

NoteBase

문 15. S/MIME에 대한 설명으로 가장 옳지 않은 것은?

① 보안 기능을 제공하는 전자 우편 시스템이며 X.509 인증서를 지원한다.

② 메시지 기밀성, 메시지 무결성, 부인 방지 서비스 등을 제공한다.

③ DSA 알고리즘을 사용하여 봉인된 데이터(Enveloped Data)를 생성한다.

④ 순수한 서명 데이터(Clear-Signed Data)에는 내용에 대한 전자서명이 들어있다.

정답 3번

출제 포인트

이 문제는 S/MIME가 제공하는 보안 기능과 Signed Data, Enveloped Data, Clear-Signed Data의 역할 차이를 묻는 문제이다.

핵심 개념

S/MIME는 MIME 전자우편에 전자서명과 암호화 기능을 추가하여 기밀성, 무결성, 송신자 인증, 부인 방지를 제공하는 전자우편 보안 표준이다.
Enveloped Data는 메시지 내용을 암호화한 형식으로, 대칭키로 본문을 암호화하고 그 대칭키를 수신자의 공개키로 보호한다.
Clear-Signed Data는 원문을 읽을 수 있게 둔 상태에서 그 내용에 대한 전자서명을 함께 제공하는 형식이다.
DSA는 전자서명용 알고리즘이며 메시지 암호화나 Enveloped Data 생성용 알고리즘이 아니다.

NoteBase

선지별 해설

① O
S/MIME는 보안 전자우편 시스템이며 공개키 인증서 체계로 X.509 인증서를 사용한다.

② O
S/MIME는 메시지 암호화를 통한 기밀성, 전자서명을 통한 무결성과 송신자 인증, 그리고 그에 따른 부인 방지 서비스를 제공한다.

③ X
틀린 부분은 "DSA 알고리즘을 사용하여 봉인된 데이터(Enveloped Data)를 생성한다"이다.
DSA는 전자서명 생성과 검증에 쓰이는 알고리즘이다.
올바르게는 "Enveloped Data는 메시지 암호화를 위한 형식이며, 대칭키와 수신자의 공개키를 이용해 생성한다"가 맞다.

④ O
Clear-Signed Data는 원문 내용을 그대로 볼 수 있으면서 그 내용에 대한 전자서명을 함께 제공하는 형식이므로 설명이 맞다.

오답 포인트

③은 전자서명 알고리즘과 암호화용 데이터 형식을 뒤섞은 선지이다. DSA는 서명용이고, Enveloped Data는 암호화용 구조이므로 서명과 암호화의 역할을 바꿔 읽으면 오답이 된다.

다시 나오면 이렇게 판단

S/MIME 선지는 먼저 전자서명인지 암호화인지부터 구분하면 된다. 서명은 무결성·인증·부인 방지와 연결되고, Enveloped Data는 기밀성을 위한 암호화 구조이므로 서명 알고리즘이 나오면 Signed Data 계열인지 먼저 확인한다.

암기 포인트

S/MIME에서 DSA는 서명, Enveloped Data는 암호화, Clear-Signed Data는 원문 공개+서명 형식이다.

NoteBase

문 16. <보기>에서 설명하는 블루투스 보안 위협으로 가장 옳은 것은?

<보기>
블루투스 장치는 장치 간 종류(전화통화, 키보드 입력, 마우스 입력 등) 식별을 위해 서비스 발견 프로토콜(SDP)을 보내고 받는다. 이 서비스 발견 프로토콜을 이용해 공격자는 공격이 가능한 블루투스 장치를 검색하고 모델을 확인할 수 있다.

① 블루프린팅
② 블루스나프
③ 블루버그
④ 블루재킹

정답 1번

출제 포인트

블루투스 공격 유형 중 서비스 발견 프로토콜(SDP)로 장치 종류와 모델 정보를 수집하는 공격을 구별하는 문제이다.

핵심 개념

블루프린팅은 SDP 등을 이용해 주변 블루투스 장치의 종류, 서비스, 모델 정보를 파악하는 정보수집 단계의 공격이다.
블루스나프는 인증이 허술한 장치에서 연락처, 일정, 파일 같은 데이터를 무단으로 읽어 가는 정보탈취 공격이다.
블루버그는 장치를 원격 제어하여 통화, 문자 전송, 명령 실행 등을 하게 만드는 권한탈취 공격이다.
블루재킹은 근거리 장치에 원치 않는 메시지나 명함을 보내는 장난성 메시지 전송이다.

선지별 해설

① O - 보기는 SDP를 주고받는 과정에서 공격 가능한 블루투스 장치를 검색하고 모델을 확인한다고 했으므로 사전 정보수집인 블루프린팅에 해당한다.
② X - 틀린 부분은 "블루스나프"이다. 블루스나프는 장치 검색이 아니라 연락처, 일정, 파일 같은 데이터를 무단으로 읽어 가는 공격이다. 올바르게는 데이터 탈취가 목적이면 블루스나프이다.
③ X - 틀린 부분은 "블루버그"이다. 블루버그는 취약한 장치를 원격 조종하여 통화, 문자 전송, 명령 실행 등을 하게 만드는 공격이다. 올바르게는 장치 제어권 탈취가 목적이면 블루버그이다.
④ X - 틀린 부분은 "블루재킹"이다. 블루재킹은 근거리 장치로 원치 않는 메시지나 명함을 보내는 행위이지 SDP로 모델을 식별하는 공격이 아니다. 올바르게는 메시지 발송이 목적이면 블루재킹이다.

NoteBase

오답 포인트

"서비스 발견", "검색", "모델 확인"이라는 표현을 보고 블루투스 공격 일반으로만 묶으면 헷갈릴 수 있다. 이 문항은 실제 피해 행위보다 먼저 수행되는 정보수집 단계인지, 데이터 탈취·제어권 탈취·메시지 전송 단계인지를 구분하는지가 핵심이다.

다시 나오면 이렇게 판단

보기에서 SDP, 장치 종류, 서비스, 모델 식별처럼 주변 장치 탐색 키워드가 나오면 블루프린팅으로 판단한다. 반대로 데이터 탈취는 블루스나프, 원격 제어는 블루버그, 메시지 전송은 블루재킹으로 나눈다.

암기 포인트

블루프린팅은 찾기, 블루스나프는 훔치기, 블루버그는 조종하기, 블루재킹은 보내기이다.

NoteBase

문 17. X.509는 공개키 암호의 사용과 디지털 서명을 기반으로 한다. X.509 디지털 인증서의 구조에 포함된 것이 아닌 것은?

① 발행자 유일 식별자(Issuer Unique Identifier)

② 발행자 공개키 정보(Issuer Public Key Information)

③ 유효기간(Period of Validity)

④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

정답 2번

출제 포인트

이 문제는 X.509 디지털 인증서의 기본 구성 요소와 발행자, 주체, 공개키의 소속 관계를 구별할 수 있는지를 묻는다.

핵심 개념

발행자(issuer)는 인증서를 서명하여 보증하는 주체이고, 주체(subject)는 인증서의 대상이 되는 주체이다.
X.509 인증서는 주체의 공개키와 발행자 정보, 유효기간, 서명 알고리즘 등의 메타데이터를 담는다.
공개키의 소속이 누구인지가 핵심 차이축이며, 인증서 안에 들어가는 것은 발행자 공개키가 아니라 주체 공개키이다.

선지별 해설

1번 O: 발행자 유일 식별자(Issuer Unique Identifier)는 X.509 인증서 구조에 포함될 수 있는 필드이다. 모든 인증서에 항상 쓰이는 필수 필드는 아니지만 구조상 정의된 항목이므로 옳다.
2번 X: 틀린 표현은 "발행자 공개키 정보"이다. X.509 인증서에 들어가는 것은 발행자의 공개키가 아니라 인증 대상인 주체의 공개키 정보이다. 올바르게는 "주체 공개키 정보(Subject Public Key Information)"이다.
3번 O: 유효기간(Validity)은 인증서가 언제부터 언제까지 유효한지를 나타내는 기본 항목이다. 일반적으로 notBefore와 notAfter로 표현되므로 옳다.
4번 O: 서명 알고리즘 식별자(Signature Algorithm Identifier)는 인증서에 사용된 서명 방식이 무엇인지를 나타내는 항목이다. 인증서 검증에 필요한 정보이므로 구조에 포함된다.

오답 포인트

발행자가 인증서에 서명한다는 사실 때문에 공개키도 발행자의 것이라고 섞어 생각하면 2번에 끌리기 쉽다.
인증서는 발행자가 주체의 공개키를 보증하는 문서라는 점을 놓치면 틀린다.

NoteBase

다시 나오면 이렇게 판단

X.509 선지를 보면 먼저 인증서가 누구의 공개키를 담는 문서인지를 확인한다. 그다음 발행자 정보, 주체 정보, 유효기간, 서명 알고리즘처럼 보증에 필요한 메타데이터와 공개키의 소속을 분리해서 판단한다.

암기 포인트

인증서는 주체 공개키를 담고, 발행자는 서명으로 이를 보증한다.

NoteBase

문 18. <보기>의 (가)~(라)에 들어갈 용어를 바르게 연결한 것은?

<보기>
IEEE 802.11i 표준은 무선랜 사용자 보호를 위해서 사용자 인증 방식, 키 교환 방식 및 향상된 무선구간 암호 알고리즘을 정의하고 있다. 무선구간에서 전송되는 데이터를 보호하기 위한 방법으로 (가)의 취약성을 해결한 (나) 방식과 AES 암호 알고리즘을 사용하는 (다) 방식을 지원한다. (나) 방식은 암호키가 각 데이터프레임마다 변경되도록 만들고 메시지 무결성을 보장하기 위해 (라)을 프레임에 포함시킴으로써 (가)의 보안 취약성을 해결하였다.

① (가): WEP, (나): TKIP, (다): CCMP, (라): MIC
② (가): WAP, (나): TKIP, (다): CCMP, (라): MAC
③ (가): WEP, (나): CCMP, (다): TKIP, (라): MAC
④ (가): WAP, (나): CCMP, (다): TKIP, (라): MIC

정답 1번

출제 포인트

이 문제는 IEEE 802.11i에서 WEP, TKIP, CCMP, MIC의 역할 차이를 정확히 연결할 수 있는지를 묻는 문제이다.

핵심 개념

WEP는 초기 무선 LAN 보안 방식으로 키 재사용과 무결성 보호 취약점이 큰 방식이다.
TKIP는 WEP의 하드웨어를 최대한 활용하면서 패킷마다 다른 키를 쓰고 MIC를 추가해 WEP의 약점을 보완한 과도기적 보호 방식이다.
CCMP는 AES를 사용하는 802.11i의 본격적인 무선 구간 보호 방식이다.
MIC는 TKIP에서 메시지 무결성 강화를 위해 추가한 코드이며, 이 문제의 구별 축은 WEP의 보완 방식이 TKIP인지, AES 사용 방식이 CCMP인지, 무결성 보호 요소가 MIC인지이다.

NoteBase

선지별 해설

① O
(가)는 WEP가 맞다. 802.11i는 WEP의 취약성을 보완하기 위해 TKIP를 두었고, AES를 사용하는 방식은 CCMP이다. 또한 TKIP는 프레임마다 키를 바꾸고 무결성 검사용 MIC를 포함하므로 연결이 모두 맞다.

② X
틀린 부분은 (가)의 "WAP"과 (라)의 "MAC"이다. 이 문맥에서 취약한 기존 무선 보안 방식은 WAP가 아니라 WEP이다. 또한 TKIP가 프레임에 포함시키는 무결성 보호 요소는 일반 용어인 MAC으로 적지 않고 MIC로 본다. 올바르게는 WEP-TKIP-CCMP-MIC의 연결이다.

③ X
틀린 부분은 (나)의 "CCMP", (다)의 "TKIP", (라)의 "MAC"이다. WEP의 취약성을 보완한 과도기 방식은 CCMP가 아니라 TKIP이다. AES를 사용하는 방식은 TKIP가 아니라 CCMP이다. 무결성 보강 요소도 MAC이 아니라 MIC이다.

④ X
틀린 부분은 (가)의 "WAP"과 (나)의 "CCMP", (다)의 "TKIP"이다. 기존 취약 방식은 WAP가 아니라 WEP이고, WEP 보완 방식은 CCMP가 아니라 TKIP이며, AES 사용 방식은 TKIP가 아니라 CCMP이다. MIC만 맞고 나머지 연결이 틀리다.

오답 포인트

TKIP와 CCMP를 둘 다 802.11i 보안 방식으로만 외우면 서로 자리를 바꿔 적기 쉽다. 이 문제는 "WEP 보완용 과도기 방식은 TKIP", "AES 사용 방식은 CCMP"라는 역할 구분과 "무결성 검사는 MIC"를 동시에 묻는 함정이다.

다시 나오면 이렇게 판단

먼저 기준이 되는 낡은 방식이 WEP인지 확인한 다음, 그 약점을 임시로 보완한 방식은 TKIP, AES 기반의 정식 강화 방식은 CCMP로 분리하면 된다. 마지막으로 TKIP의 무결성 키워드는 MIC인지 확인하면 정답을 고를 수 있다.

암기 포인트

WEP는 취약, TKIP는 WEP 보완, CCMP는 AES, MIC는 TKIP 무결성이다.

NoteBase

문 19. 보안 등급 평가 기준인 TCSEC에 대한 설명으로 가장 옳지 않은 것은?

① 보안 요구조건을 명세화하고 평가 기준을 정의하기 위한 ISO 표준이다.

② B3 보안단계에서는 운영체제에서 보안에 불필요한 부분을 모두 제거하고 모듈에 따른 분석 및 테스트가 가능하다.

③ C2 보안단계에서는 보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있다.

④ B1 보안단계에서는 시스템 내에 보안 정책을 적용할 수 있고, 각 데이터에 대해 보안 레벨 설정이 가능하다.

정답 1번

출제 포인트

TCSEC의 성격과 보안 등급 C2, B1, B3의 핵심 특징을 구분하는 문제이다.

핵심 개념

TCSEC는 미국 국방부가 제시한 신뢰 컴퓨터 시스템 평가 기준으로 보안 등급 체계를 정의한 기준이다.
C2는 사용자별 접근통제와 감사 추적이 가능한 단계이다.
B1은 보안 라벨을 이용해 주체와 객체에 보안 등급을 부여하는 단계이다.
B3는 보안 기능을 구조화하고 불필요한 요소를 최소화하여 분석과 시험이 가능해야 하는 단계이다.

선지별 해설

① X
틀린 부분은 "ISO 표준"이다.
TCSEC는 ISO 표준이 아니라 미국 국방부(DoD)의 보안 평가 기준이다.
"보안 요구조건을 명세화하고 평가 기준을 정의한 미국 국방부 기준이다"로 고치면 맞다.

② O
B3 단계는 보안 메커니즘을 단순하고 구조적으로 설계하여 분석과 테스트가 가능해야 한다.
따라서 보안에 불필요한 부분을 제거하고 모듈 단위 분석 및 테스트가 가능하다는 설명은 맞다.

③ O
C2 단계는 감사 기능을 갖추고 사용자 단위의 임의적 접근통제를 수행한다.
따라서 특정 사용자의 접근을 거부할 수 있다는 설명은 맞다.

④ O
B1 단계는 라벨 기반 보안 정책을 적용하여 객체별 보안 등급을 부여한다.
따라서 각 데이터에 대해 보안 레벨을 설정할 수 있다는 설명은 맞다.

NoteBase

오답 포인트

TCSEC를 국제표준으로 바꾸어 Common Criteria나 ISO 계열 기준과 혼동하게 만드는 점이 함정이다. 등급 구분도 C2는 감사, B1은 라벨, B3는 구조화된 보안 설계라는 축으로 나누어 보아야 한다.

다시 나오면 이렇게 판단

TCSEC 문제는 먼저 기준의 출처가 미국 국방부인지 확인하고, 그다음 C2는 감사와 사용자별 접근통제, B1은 보안 라벨, B3는 구조화된 TCB와 시험 가능성으로 판단하면 된다.

암기 포인트

TCSEC는 DoD 기준, C2는 감사, B1은 라벨, B3는 구조화이다.

NoteBase

문 20. <보기>에서 디지털 포렌식 절차를 순서대로 바르게 나열한 것은?

<보기>
ㄱ. 보고서 작성
ㄴ. 사전준비
ㄷ. 보관 및 이송
ㄹ. 증거수집
ㅁ. 분석 및 조사

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

정답 3번

출제 포인트

이 문제는 디지털 포렌식의 기본 절차에서 사전준비, 증거수집, 보관 및 이송, 분석 및 조사, 보고서 작성의 선후관계를 묻는 문제이다.

올바른 순서

1. 사전준비 — 포렌식 대상, 장비, 인력, 절차를 미리 준비하는 단계이다.
2. 증거수집 — 디지털 증거를 원본 훼손 없이 확보하는 단계이다.
3. 보관 및 이송 — 수집한 증거를 무결성이 유지되도록 보관하고 필요한 장소로 이송하는 단계이다.
4. 분석 및 조사 — 확보된 증거를 해석하여 사실관계를 확인하는 단계이다.
5. 보고서 작성 — 조사 결과와 분석 내용을 문서로 정리하는 단계이다.

왜 이 순서: 분석 및 조사는 먼저 확보되고 보관된 증거를 입력으로 하므로, 증거수집과 보관 및 이송이 선행되어야 한다.

NoteBase

선지별 해설

① X
증거수집 뒤에 바로 분석 및 조사를 두었기 때문에 틀리다. 수집한 증거는 먼저 보관 및 이송 과정을 거쳐 무결성과 연계보관성이 유지된 상태가 되어야 분석할 수 있다.
틀린 표현: ㄴ → ㄹ → ㅁ → ㄷ → ㄱ
올바르게는: ㄴ → ㄹ → ㄷ → ㅁ → ㄱ

② X
분석 및 조사를 증거수집보다 먼저 두었기 때문에 틀리다. 분석은 확보된 증거가 있어야 가능한 후행 단계이다.
틀린 표현: ㄴ → ㅁ → ㄹ → ㄷ → ㄱ
올바르게는: ㄴ → ㄹ → ㄷ → ㅁ → ㄱ

③ O
사전준비 후 증거수집을 하고, 확보한 증거를 보관 및 이송한 다음 분석 및 조사를 수행하고 마지막에 보고서를 작성하므로 올바른 순서이다.

④ X
분석 및 조사를 증거수집보다 먼저 두고, 보관 및 이송도 증거수집보다 앞에 두었기 때문에 틀리다. 보관 및 이송과 분석은 모두 증거를 수집한 뒤에 이어지는 단계이다.
틀린 표현: ㄴ → ㅁ → ㄷ → ㄹ → ㄱ
올바르게는: ㄴ → ㄹ → ㄷ → ㅁ → ㄱ

오답 포인트

증거수집과 분석 및 조사를 바로 연결해서 외우면 보관 및 이송 단계를 빠뜨리기 쉽다. 이 문항의 함정은 분석 전에 증거의 보관과 이송이 먼저 이루어져야 한다는 점이다.

다시 나오면 이렇게 판단

절차형 문제는 준비 단계, 확보 단계, 보존 단계, 해석 단계, 문서화 단계의 흐름으로 판단한다. 뒤 단계가 앞 단계의 산출물을 필요로 하는지를 보면 순서를 안정적으로 정할 수 있다.

암기 포인트

포렌식 절차는 준비 → 수집 → 보관·이송 → 분석 → 보고의 흐름이다.

NoteBase