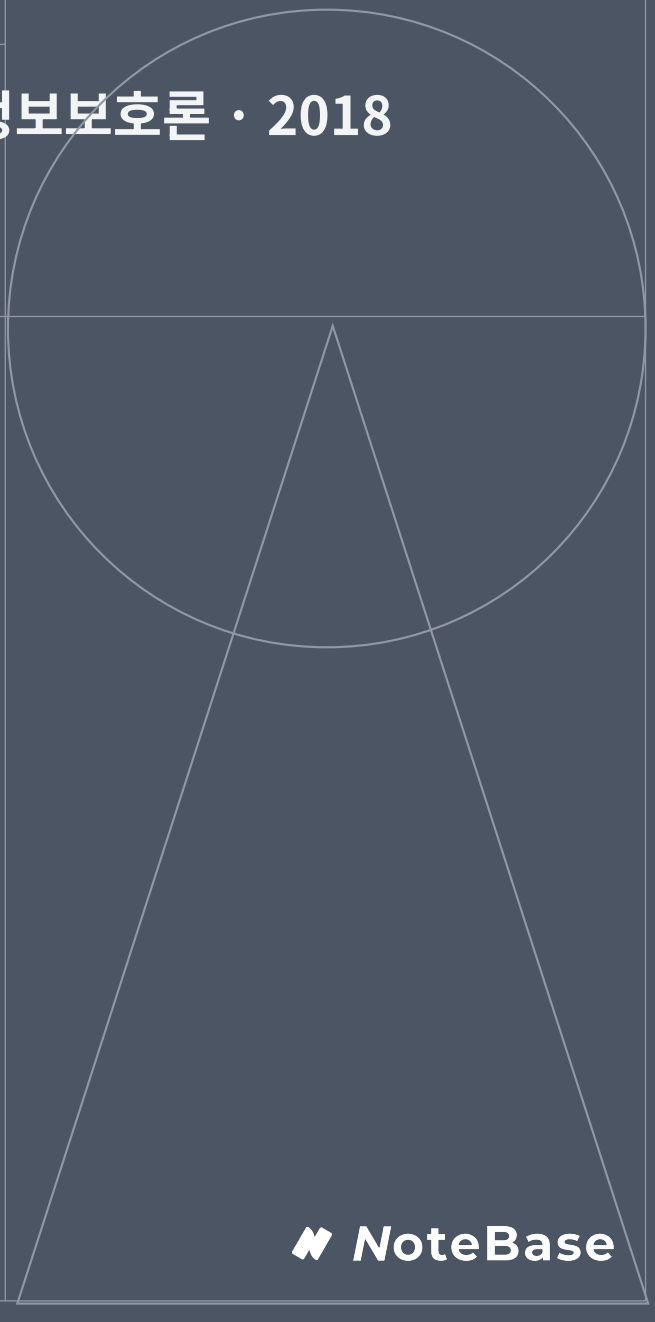
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2018

공무원/경찰/공채(경위) · 정보보호론 · 2018

문 1. 다음 지문에서 설명하는 기술과 바르게 짝지은 것은?

(가) 디지털콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
(나) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털콘텐츠에 삽입하는 기술이다.
(다) 공격자가 공격전에 공격대상에 대한 다양한 정보를 수집하는 기술이다.

① (가) 워터마킹 (나) 핑거프린팅 (다) 워터링 홀
② (가) 핑거프린팅 (나) 워터링 홀 (다) 풋프린팅
③ (가) 풋프린팅 (나) 워터마킹 (다) 핑거프린팅
④ (가) 핑거프린팅 (나) 워터마킹 (다) 풋프린팅

정답 4번

간단한 해설

구매자마다 다른 식별 정보를 넣어 유출 경로를 찾는 것은 핑거프린팅이고, 저작권 정보를 넣어 권리자를 확인하는 것은 워터마킹이다. 두 기술은 **삽입 정보가 구매자를 식별하는지, 저작권을 나타내는지**로 구분한다.

NoteBase

보기별 해설

(가) 핑거프린팅. 판매되는 복제본에 구매자별 식별 정보를 삽입하여, 불법 유통된 복제본이 발견되면 어느 구매자에게 배포한 것인지 추적한다. 지문의 **구매자 정보와 최초 배포자 추적**이 판단 단서이다.

(나) 워터마킹. 디지털콘텐츠에 저작권자나 소유권을 나타내는 정보를 삽입한다. 지문은 이용자가 알아차리지 못하고 원래 콘텐츠의 이용에 지장을 주지 않는 범위에서 정보를 넣는 비가시적 워터마킹을 설명한다. 구매자별 유출 경로보다 **저작권 정보의 표시**에 초점이 있다.

(다) 풋프린팅. 본격적인 공격에 앞서 대상 조직·시스템·네트워크에 관한 정보를 수집하여 공격 대상의 특성을 파악하는 정찰 활동이다. 선택지의 워터링 홀은 표적이 자주 방문하는 웹사이트를 침해해 방문자를 노리는 공격 방식이므로, 이 지문의 사전 정보 수집과 구분된다.

따라서 (가) 핑거프린팅, (나) 워터마킹, (다) 풋프린팅을 연결한 ④가 지문과 일치한다.

NoteBase

문 2. 암호학적 해시함수(Cryptographic Hash Function)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 어떤 입력 x에 대해 h(x)를 계산하기 어려워야 한다.

② 주어진 값 y에 대해 h(x)=y의 x 값을 찾는 계산이 어려워야 한다.

③ 생일역설(Birthday Paradox)은 충돌 저항성 공격(Collision Resistance Attack)과 관련한 수학적 분석 결과이다.

④ 입력 길이에 상관없이 고정된 길이를 출력한다.

정답 1번

간단한 해설

해시함수는 입력으로부터 해시값을 **효율적으로 계산**할 수 있어야 한다. 계산이 어려워야 하는 쪽은 주어진 해시값의 입력을 찾는 역방향이나, 같은 해시값을 갖는 서로 다른 입력을 찾는 작업이다.

선지별 해설

① X: 입력 x가 주어졌을 때 $h(x)$를 구하는 정방향 계산은 효율적으로 수행할 수 있어야 한다. 해시값을 만들 때마다 계산이 실질적으로 불가능할 정도로 어려우면 무결성 검사 등의 용도로 사용하기 어렵다. **정방향 계산의 효율성**과 역방향 탐색의 어려움을 혼동한 설명이다.

② O: 주어진 해시값 y에 대하여 $h(x) = y$를 만족하는 입력 x를 찾기 어려워야 한다는 조건은 역상 저항성이다. 여기서 목표는 '같은 결과가 나오는 아무 두 입력'이 아니라 **이미 정해진 해시값의 입력**을 찾는 것이다.

③ O: 충돌은 서로 다른 입력 x와 x'가 $h(x) = h(x')$를 만족하는 경우이다. 생일역설에 따르면 이상적인 n비트 해시에서 임의의 충돌을 찾는 데 필요한 시도 횟수는 대략 $2^{n/2}$ 규모이다. 따라서 충돌 탐색은 특정 해시값의 역상을 찾는 일반적인 전수 탐색 규모인 2^n보다 작으며, 이 차이를 분석하는 데 생일역설을 사용한다.

④ O: 통상적인 고정 출력 해시함수에서는 선택한 알고리즘의 출력 길이가 정해져 있다. 입력 데이터가 길어지거나 짧아져도 같은 알고리즘의 출력 비트수는 일정하다. 다만 **출력 길이가 같다는 것과 출력값이 같다는 것은 다르며**, 입력이 달라지면 일반적으로 해시값도 달라진다.

NoteBase

문 3. MD5(Message Digest 5)는 널리 쓰는 해시함수이며, 최종적으로 ( )비트의 해시코드를 출력한다. ( ) 안에 들어갈 적합한 숫자는 무엇인가?

① 64

② 128

③ 256

④ 512

정답 2번

간단한 해설

MD5는 입력 메시지의 길이와 관계없이 **128비트의 해시값**을 출력한다. 메시지를 나누어 처리하는 512비트 블록 크기와 구별해야 한다.

빈칸별 해설

빈칸에는 128이 들어간다. MD5는 길이가 다른 메시지를 입력받아도 **128비트로 고정된 해시값**을 출력한다. 최종 결과는 32비트 값 네 개로 구성되므로 32 × 4 = 128비트이다.

MD5가 메시지를 처리하는 블록의 크기는 512비트이며, 패딩에 덧붙이는 길이 정보는 64비트이다. 이 값들은 **최종 해시값의 길이와 다르다**. 256비트 역시 MD5의 출력 길이가 아니다.

따라서 빈칸의 수치는 128이며, ②에 해당한다.

NoteBase

문 4. 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고 이를 복호화하는 과정에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

1. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
2. Bob은 (가)를 Alice에게 전송한다.
3. Alice는 (나)를 사용하여 메시지를 암호화한다.
4. Alice는 생성된 암호문을 Bob에게 전송한다.
5. Bob은 (다)를 사용하여 암호문을 복호화한다.

① (가) Bob의 공개키 (나) Alice의 공개키 (다) Alice의 개인키

② (가) Bob의 개인키 (나) Bob의 공개키 (다) Bob의 개인키

③ (가) Bob의 개인키 (나) Alice의 공개키 (다) Alice의 개인키

④ (가) Bob의 공개키 (나) Bob의 공개키 (다) Bob의 개인키

정답 4번

간단한 해설

Bob만 메시지를 읽게 하려면 Alice는 **수신자인 Bob의 공개키로 암호화**하고, Bob은 이에 대응하는 **자신의 개인키로 복호화**한다. 따라서 Alice에게 전달할 키도 Bob의 공개키이다.

빈칸별 해설

이 과정의 목적은 Alice가 보낸 메시지의 기밀성을 보장하여 Bob만 복호화할 수 있게 하는 것이다. Bob이 만든 한 쌍의 키 중 공개키는 암호화에 사용하도록 알리고, 개인키는 Bob이 비밀로 보관한다.

(가) Bob의 공개키: Alice가 Bob에게 보낼 메시지를 암호화하려면 Bob의 공개키를 알아야 한다. 따라서 Bob은 자신의 공개키를 Alice에게 전달한다. **개인키는 다른 사람에게 전달하지 않고 비밀로 유지**해야 한다.

(나) Bob의 공개키: Alice는 메시지를 읽을 사람인 **Bob의 공개키**로 암호화한다. Alice 자신의 공개키를 사용하면 그 암호문에 대응하는 복호화 키는 Alice의 개인키가 되므로, Bob만 읽게 하려는 이 과정의 목적과 맞지 않는다.

(다) Bob의 개인키: Alice가 전송한 암호문은 Bob의 공개키로 암호화되어 있으므로, Bob은 짝이 되는 **자신의 개인키**로 원래 메시지를 복원한다. 공개키를 아는 다른 사람도 메시지를 암호화할 수는 있지만, 개인키를 모르면 정상적인 복호화를 할 수 없다.

따라서 (가)와 (나)는 Bob의 공개키, (다)는 Bob의 개인키이며, 이 대응을 제시한 ④와 일치한다.

NoteBase

문 5. 임의적 접근통제(DAC : Discretionary Access Control)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 객체(데이터)의 소유주에 의하여 접근권한 변경이 가능하다.

② 일반적으로 ACL(Access Control List)을 통해서 이루어진다.

③ 민감도 레이블(Sensitivity Label)에 따라 접근을 허용할지 결정한다.

④ ID기반 접근통제이다.

정답 3번

간단한 해설

민감도 레이블과 보안등급에 따른 접근 결정은 MAC의 특징이다. DAC는 객체 소유자 등의 재량으로 사용자별 접근권한을 설정하는 방식이다.

선지별 해설

DAC는 객체의 소유자 등 권한을 가진 주체가 누구에게 어떤 접근권한을 줄지 재량으로 정하는 접근통제 방식이다. 핵심은 **사용자 식별정보와 소유자의 권한 부여**이며, 보안등급에 따른 강제적 정책과 구별된다.

① O. 객체의 소유자는 자신에게 인정된 관리 권한의 범위에서 다른 사용자의 읽기·쓰기 등 접근권한을 부여하거나 변경할 수 있다. 이러한 재량성이 DAC의 특징이다.

② O. ACL은 객체별로 어떤 사용자나 그룹이 어떤 작업을 할 수 있는지 기록하는 목록이다. 객체 소유자가 이 목록의 권한을 설정하는 방식은 DAC의 대표적인 구현 방법이다. 다만 ACL이라는 자료구조 자체가 DAC에서만 사용되는 것은 아니다.

③ X. 민감도 레이블과 주체의 보안등급 등을 기준으로 접근을 강제하는 설명은 MAC(강제적 접근통제)에 해당한다. MAC에서는 일반적인 객체 소유자가 중앙의 보안정책을 임의로 변경할 수 없다. DAC의 판단 기준을 민감도 레이블이라고 한 점이 잘못되었다.

④ O. DAC는 접근을 요청한 사용자 등의 ID를 식별하고 그 사용자 또는 소속 그룹에 부여된 권한을 확인하는 방식이다. 따라서 일반적으로 ID 기반 접근통제로 설명한다.

따라서 DAC에 대한 설명으로 가장 옳지 않은 것은 ③이다.

NoteBase

문 6. 대칭키와 공개키 암호화 방식에 관한 다음 설명 중 옳은 것은 모두 몇 개인가?

가. 일반적으로 안전한 키 길이는 대칭키 방식의 키가 공개키 방식의 키보다 길다.
나. 대칭키 방식의 암호화키와 복호화키는 동일하며, 모두 비밀이다.
다. 공개키 방식의 암호화키와 복호화키는 모두 공개이다.
라. 일반적으로 암호화 속도는 대칭키 방식이 공개키 방식보다 빠르다.
마. 대칭키 방식의 알고리즘에는 AES, SEED, ECC 등이 있다.

① 2개
② 3개
③ 4개
④ 5개

정답 1번

간단한 해설

대칭키 방식은 암호화와 복호화에 **같은 비밀키**를 사용하며, 일반적으로 공개키 방식보다 빠르다. 공개키 방식에서는 공개키와 달리 개인키를 비밀로 유지해야 한다.

NoteBase

보기별 해설

가. X. 비슷한 안전성을 얻는다는 기준에서 비교하면, 일반적으로 대칭키 암호는 RSA나 ECC 같은 공개키 암호보다 짧은 키를 사용한다. 알고리즘의 수학적 구조와 알려진 공격 방법이 다르므로 **키 길이만 같다고 안전성이 같은 것은 아니다**.

나. O. 대칭키 방식은 송신자와 수신자가 같은 비밀키를 공유하여 암호화와 복호화에 사용한다. 이 키가 노출되면 제3자도 암호문을 해독할 수 있으므로 양쪽 모두 비밀로 관리해야 한다.

다. X. 공개키 방식은 공개해도 되는 공개키와 **비밀로 보관하는 개인키**를 한 쌍으로 사용한다. 기밀성을 위한 암호화에서는 수신자의 공개키로 암호화하고 수신자의 개인키로 복호화하므로, 두 키가 모두 공개되는 것은 아니다.

라. O. 대칭키 방식은 일반적으로 공개키 방식보다 연산 부담이 작아 암호화 속도가 빠르다. 따라서 많은 양의 실제 데이터를 암호화하는 데 대칭키 방식이 널리 사용된다.

마. X. AES와 SEED는 대칭키 블록 암호이지만, ECC는 **타원곡선을 이용하는 공개키 암호 기술**이다. ECC를 대칭키 알고리즘에 포함한 부분을 고쳐야 한다.

옳은 설명은 나와 라로 모두 2개이며, 이에 해당하는 선택지는 ①이다.

NoteBase

문 7. 다음 지문에서 설명하는 접근통제모델은 무엇인가?

접근통제모델 중 효율적인 업무처리(Well-formed transactions)와 직무분리(Separation of duties) 두 가지 원칙을 통해 좀 더 정교하게 무결성을 보장하는 모델이다.

① 벨-라파듈라(Bell-LaPadula)
② 비바(Biba)
③ 테이크 그랜트(Take Grant)
④ 클락-윌슨(Clark-Wilson)

정답 4번

간단한 해설

클락-윌슨 모델은 **정형화된 거래와 직무분리**를 통해 데이터 무결성을 보호한다. 단순한 무결성 등급 통제보다, 올바른 업무 절차와 역할 분담이라는 두 단서가 중요하다.

핵심 풀이

정형화된 거래: 지문의 Well-formed transactions는 단순히 업무를 빠르게 처리한다는 뜻이 아니라, **무결성을 보존하도록 검증된 절차로만 데이터를 변경**한다는 뜻이다. 사용자가 보호 데이터를 임의로 수정하지 않고, 허용된 변환 절차를 거쳐 올바른 상태에서 다른 올바른 상태로 바꾸게 한다.

직무분리: 중요한 작업의 수행과 승인·검증 등 상충하는 역할을 분리하여 **한 사람이 부정한 변경을 단독으로 완결하지 못하게** 한다. 예를 들어 거래를 입력하는 사람과 승인하는 사람을 나누면 오류나 부정행위를 견제할 수 있다.

벨-라파듈라는 주로 기밀성을 보호하기 위해 보안등급에 따른 정보 흐름을 통제한다. 지문의 상업적 거래 무결성 원칙과는 중점이 다르다.

비바도 무결성 모델이지만, 무결성 등급에 따른 접근·정보 흐름 통제가 중심이다. 따라서 '무결성'이라는 말만으로 비바를 선택하지 않고, 정형화된 거래와 직무분리라는 두 원칙을 함께 확인해야 한다.

테이크 그랜트는 권한을 취득하거나 다른 주체에게 부여하는 규칙을 통해 접근권한이 어떻게 전파되는지 설명하는 모델이다.

따라서 정형화된 거래와 직무분리를 결합해 무결성을 보장하는 모델은 클락-윌슨이며, ④에 해당한다.

NoteBase

문 8. 생체인증기술의 정확도는 부정거부율(FRR : False Rejection Rate)과 부정허용율(FAR : False Acceptance Rate)로 측정할 수 있다. 생체인증기술의 정확도에 관한 다음 설명 중 옳은 것끼리 짝지은 것은 무엇인가?

가. 사용자 편의성을 요구하는 경우 FAR이 높아지고 FRR은 낮아진다.
나. 사용자 편의성을 요구하는 경우 FRR이 높아지고 FAR은 낮아진다.
다. 보안성을 강화할 경우 FRR은 높아지고 FAR은 낮아진다.
라. 보안성을 강화할 경우 FAR은 높아지고 FRR은 낮아진다.

① 가, 다
② 가, 라
③ 나, 다
④ 나, 라

정답 1번

간단한 해설

같은 생체인증 시스템에서 판정 기준을 느슨하게 하면 본인 거부는 줄지만 타인 허용은 늘어난다. 반대로 **보안성을 위해 기준을 엄격하게 하면 FAR은 낮아지고 FRR은 높아진다**.

NoteBase

보기별 해설

FRR은 실제 본인을 타인으로 잘못 판단하여 거부하는 비율이고, FAR은 타인을 본인으로 잘못 판단하여 허용하는 비율이다. 아래 관계는 같은 인증 시스템에서 **본인으로 인정하는 임계값을 조절**하는 상황을 전제로 한다.

가. O: 사용자 편의성을 높이려면 본인이 인증에 실패하는 경우를 줄여야 한다. 판정 기준을 느슨하게 하면 본인이 통과하기 쉬워져 FRR은 낮아지지만, 타인까지 통과할 가능성이 커져 FAR은 높아진다.

나. X: FRR이 높아지면 실제 사용자가 본인인데도 거부되어 재시도해야 하는 일이 늘어난다. 따라서 이는 사용자 편의성을 높이는 방향이 아니다. 편의성을 위해 기준을 완화할 때는 **FRR이 낮아지고 FAR이 높아지는** 관계가 된다.

다. O: 보안성을 강화하려면 타인이 본인으로 통과하는 것을 줄여야 한다. 판정 기준을 엄격하게 하면 FAR은 낮아지지만, 본인의 생체정보에도 측정 오차나 변동이 있을 수 있어 일부 정상 사용자까지 거부되므로 FRR은 높아진다.

라. X: FAR이 높아진다는 것은 타인을 잘못 허용하는 경우가 늘어난다는 뜻이므로 보안성 강화와 반대이다. 보안을 위해 기준을 강화하면 **FAR은 낮아지고 FRR은 높아진다**. 알고리즘 자체를 개선하여 두 오류를 함께 줄이는 경우와, 동일 시스템에서 임계값만 바꾸는 경우는 구분해야 한다.

따라서 옳은 보기는 가와 다이며, 이를 짝지은 ①이 정답이다.

NoteBase

문 9. 다음 중 취약점 점검 도구가 아닌 것은 무엇인가?

① SARA

② NIKTO

③ TCP WRAPPER

④ NESSUS

정답 3번

간단한 해설

TCP WRAPPER는 서비스 접속의 허용·거부를 결정하는 접근통제 도구이다. 시스템의 보안상 약점을 찾아내는 취약점 점검 도구와는 목적이 다르다.

개념 구분

취약점 점검 도구는 시스템이나 서비스의 상태를 조사하여 알려진 보안 약점, 잘못된 설정 등을 찾아낸다.
접근통제 도구는 정해진 정책에 따라 누가 서비스에 접속할 수 있는지를 제한한다.

SARA: 네트워크에 연결된 호스트와 서비스를 조사하여 잠재적인 보안 취약점을 점검하는 보안 분석 도구이다. 서비스의 노출 상태와 보안상 문제를 찾아내는 데 사용되므로 취약점 점검 도구에 속한다.

NIKTO: **웹 서버를 대상으로 보안 문제를 점검**하는 도구이다. 위험한 파일이나 CGI, 오래된 서버 구성 요소, 잘못된 설정 등을 확인하므로 웹 서버 취약점 점검 도구에 해당한다.

TCP WRAPPER: 지원되는 네트워크 서비스에 들어오는 접속을 **호스트별 접근 규칙에 따라 허용하거나 거부**한다. 대표적으로 hosts.allow와 hosts.deny의 규칙을 이용한다. 접속을 통제하는 기능이 핵심이며, 시스템을 조사하여 취약점을 찾아내는 스캐너는 아니다.

NESSUS: 네트워크 호스트와 운영체제, 서비스 등을 검사하여 알려진 취약점이나 보안 설정 문제를 찾아내는 취약점 스캐너이다. 점검 결과를 통해 보완이 필요한 문제를 확인하는 데 사용된다.

따라서 취약점 점검 도구가 아닌 것은 접근통제 도구인 TCP WRAPPER이며, ③과 연결된다.

NoteBase

문 10. 윈도우 파일 시스템 NTFS(New Technology File System)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① NTFS는 기본 NTFS 보안의 공유 보안과 동일하게 Everyone 그룹에 대해서는 모든 권한이 '허용'이다.

② 기본 NTFS 보안을 변경하면 사용자마다 서로 다른 NTFS 보안을 적용시킬 수 있다.

③ 파일과 폴더에 대한 보안강화 및 접근제어가 가능하다.

④ 저용량 볼륨에 최적화되어 있다.

정답 4번

간단한 해설

NTFS는 접근제어·복구 기능과 함께 **대용량 볼륨 관리**를 지원한다. 관리용 정보의 공간 부담이 있어 저용량 볼륨에 최적화되어 있다는 설명은 잘못이다.

선지별 해설

NTFS는 파일과 폴더의 접근권한을 세밀하게 관리하고 대용량 저장장치를 지원하는 파일 시스템이다. 관리용 메타데이터와 로그 등의 공간이 필요하므로 저용량 볼륨에 최적화된 구조라고 설명하는 것은 부적절하다.

① O. 구형 윈도우의 기본 권한 설정을 설명한 것이다. 예를 들어 Windows 2000 계열의 설명에서는 NTFS 드라이브의 루트에 Everyone 그룹의 모든 권한 허용을 부여하는 기본 구성이 제시된다. 다만 실제 파일·폴더의 권한은 운영체제 버전, 상속 및 변경된 ACL에 따라 달라지므로, 모든 NTFS 파일에 언제나 모든 사용자 권한이 허용된다는 뜻으로 확대하면 안 된다.

② O. NTFS에서는 파일·폴더의 접근제어 목록(ACL)에 사용자 또는 그룹별 권한을 설정할 수 있다. 예를 들어 같은 파일에 대해 한 사용자는 읽기만, 다른 사용자는 수정까지 허용하는 식으로 권한을 달리 부여할 수 있다.

③ O. NTFS의 파일·폴더별 권한을 이용하면 읽기·쓰기·실행 등의 접근을 허용하거나 제한할 수 있다. 따라서 저장된 자료에 대한 접근제어와 보안 강화가 가능하다.

④ X. NTFS는 대용량 볼륨과 파일 관리, 접근제어 및 복구 기능 등을 지원하도록 설계되었다. 관리용 정보가 차지하는 공간적 부담이 있으므로 작은 볼륨에서 특히 효율적인 파일 시스템이라는 설명은 반대이다. '저용량 볼륨에 최적화'가 아니라 **대용량 볼륨 관리에 적합**하다고 이해해야 한다.

따라서 가장 옳지 않은 설명은 ④이다.

NoteBase

문 11. 다음 중 윈도우 레지스트리 키가 아닌 것은 무엇인가?

① HKEY_CLASSES_ROOT

② HKEY_CURRENT_USER

③ HKEY_MACHINE_SAM

④ HKEY_USERS

정답 3번

간단한 해설

HKEY_MACHINE_SAM은 윈도우가 정의한 루트 키 이름이 아니다. 시스템 전체 설정의 루트 키는 HKEY_LOCAL_MACHINE이고, SAM은 그 아래에 있는 하위 키이다.

개념 구분

선택지의 HKEY_로 시작하는 이름들은 윈도우 레지스트리의 미리 정의된 루트 키를 묻는 맥락이다. 이름 일부가 익숙하더라도 **루트 키 이름과 하위 키 경로를 합쳐 새 이름을 만들면 안 된다**.

HKEY_CLASSES_ROOT: 파일 확장자 연결과 COM 클래스 등록 등의 정보를 제공하는 루트 키이다. 일반적으로 시스템 전체의 클래스 설정과 현재 사용자의 클래스 설정을 결합한 보기를 제공한다.

HKEY_CURRENT_USER: 현재 로그인한 사용자의 환경과 응용프로그램 설정 등 사용자별 정보를 제공한다. HKEY_USERS 아래에 로드된 현재 사용자 프로필과 연결되는 루트 키이다.

HKEY_MACHINE_SAM: 미리 정의된 루트 키가 아니다. 올바른 시스템 전체 설정 루트는 HKEY_LOCAL_MACHINE이며, 보안 계정 관리 정보와 관련된 SAM의 경로는 **HKEY_LOCAL_MACHINE\SAM**이다. SAM이 존재한다는 사실이 HKEY_MACHINE_SAM이라는 루트 키를 만들어 주지는 않는다.

HKEY_USERS: 시스템에 현재 로드되어 있는 사용자 프로필별 레지스트리 정보를 포함한다. 모든 등록 계정의 프로필이 항상 전부 로드되어 있다는 뜻은 아니며, 현재 사용자의 설정에 접근하는 HKEY_CURRENT_USER와도 구별된다.

따라서 윈도우의 미리 정의된 레지스트리 루트 키가 아닌 것은 **HKEY_MACHINE_SAM인 ③**이다.

NoteBase

문 12. 리눅스 시스템 로그(log) 파일 중 계정들의 로그인 및 로그아웃에 대한 정보를 가진 파일은 무엇인가?

① wtmp
② dmesg
③ xferlog
④ btmp

정답 1번

간단한 해설

wtmp는 사용자의 로그인·로그아웃 이력을 누적 기록한다. 로그인에 실패한 시도를 기록하는 btmp와 구별해야 한다.

개념 구분

로그 파일은 이름보다 기록하는 사건의 종류로 구별한다. 이 문제의 핵심은 계정이 시스템에 접속하고 접속을 종료한 이력을 찾는 것이다.

wtmp: **로그인·로그아웃의 과거 이력**을 누적하여 기록한다. 사용자와 접속 시각 등의 정보를 바탕으로 누가 언제 접속했는지 확인할 수 있으며, 대표적으로 last 명령으로 내용을 조회한다.

dmesg: 부팅 과정의 장치 인식이나 드라이버 초기화 등 **커널 메시지**와 관련된 로그이다. dmesg 명령은 커널의 메시지 버퍼를 보여 주며, 전통적인 구성에서는 관련 부팅 메시지가 로그 파일로도 보관된다. 사용자별 로그인·로그아웃 이력을 기록하는 파일과는 용도가 다르다.

xferlog: FTP 서비스의 **파일 전송 이력**을 기록한다. 전송 시각, 파일명, 전송량, 전송 방향 등의 정보로 업로드·다운로드 활동을 확인하는 데 사용한다.

btmp: **실패한 로그인 시도**를 기록하며, 대표적으로 lastb 명령으로 조회한다. 정상적으로 로그인한 뒤 로그아웃한 접속 이력을 묻는 경우에는 wtmp를 구별하여 선택해야 한다.

따라서 계정들의 로그인 및 로그아웃 정보를 가진 파일은 wtmp이며, ①에 해당한다.

NoteBase

문 13. 리눅스 명령어에 관한 다음 설명 중 바르게 짝지은 것은 무엇인가?

(가) 파일과 디렉터리의 퍼미션(Permission) 변경
(나) 파일과 디렉터리의 소유권(Ownership) 변경
(다) 사용자 패스워드 변경
(라) 계정 생성

① (가): umask, (나): chown, (다): passwd, (라): netuser
② (가): chmod, (나): chgroup, (다): passwd, (라): useradd
③ (가): chmod, (나): chown, (다): passwd, (라): useradd
④ (가): umask, (나): chown, (다): chpwd, (라): useradd

정답 3번

간단한 해설

기존 파일의 접근권한은 **chmod**로, 소유자는 **chown**으로 바꾼다. umask는 새로 만드는 파일의 권한을 제한하는 마스크이므로 기존 파일의 권한 변경과 구분한다.

보기별 해설

(가) chmod. 파일과 디렉터리의 읽기·쓰기·실행 권한 등을 변경한다. '어떤 작업을 허용할 것인가'에 해당하는 **접근권한**을 다루는 명령이다. umask는 새 파일이나 디렉터리를 만들 때 요청된 권한에서 제외할 비트를 정하는 마스크로, 이미 있는 파일의 권한을 직접 변경하는 명령이 아니다.

(나) chown. 파일과 디렉터리의 **소유 사용자**를 변경하며, 지정 방식에 따라 소유 그룹도 함께 변경할 수 있다. 그룹만 변경하는 표준 명령은 chgrp이므로 선택지의 chgroup과 혼동하지 않아야 한다.

(다) passwd. 사용자 계정의 비밀번호를 변경하는 명령이다. 일반 사용자는 자신의 비밀번호를, 관리 권한을 가진 사용자는 다른 계정의 비밀번호도 변경할 수 있다.

(라) useradd. 새 사용자 계정을 생성한다. 계정명과 필요한 설정을 등록하며, 홈 디렉터리 생성 여부 등은 옵션과 시스템 설정에 따라 달라진다.

따라서 (가) chmod, (나) chown, (다) passwd, (라) useradd의 조합인 ③이 일치한다.

NoteBase

문 15. 정보보호 보안평가 표준 등에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① TCSEC은 보안등급을 A,B,C,D로 구분하며 네트워크를 고려하지 않은 시스템 보안평가 표준이다.

② ITSEC은 오렌지북으로 불리는 컴퓨터시스템 평가기준으로 미국방부에서 최초로 수용되었다.

③ CC(Common Criteria)는 단일화된 공통 평가기준을 제정하여 적용함으로써 시간의 절약, 평가비용의 절감 등의 효과가 있다.

④ ISMS는 BS7799를 기반으로 국내 환경에 적합하게 작성하였다.

정답 2번

간단한 해설

오렌지북은 미국의 TCSEC을 가리킨다. ITSEC은 유럽의 보안 평가기준이므로, 오렌지북과 미국 국방부의 기준이라는 설명을 ITSEC에 붙이면 두 기준을 혼동하게 된다.

선지별 해설

① O: TCSEC은 보안 수준을 D·C·B·A의 네 큰 등급으로 나누며, 각각 최소 보호·임의적 보호·강제적 보호·검증된 보호를 구분한다. 주로 단일 컴퓨터 시스템을 대상으로 한 기준이므로, 네트워크 보안에 적용하기 위한 별도의 해석 기준이 마련되었다.

② X: 미국 국방부의 평가기준으로서 **오렌지북이라 불리는 것은 TCSEC**이다. ITSEC은 유럽에서 마련한 정보기술 보안 평가기준으로, 보안 기능과 보증을 구분하여 평가한다. 두 기준의 명칭과 출처를 바꾸어 설명한 부분이 잘못되었다.

③ O: CC는 서로 다른 평가기준을 공통 기준으로 통합하여 보안 기능과 보증을 일관된 틀에서 평가하도록 한다. 공통 기준과 상호인정은 **중복 평가 부담을 줄여** 시간과 비용을 절약하는 데 기여한다.

④ O: 국내 ISMS는 BS7799 등 정보보호 관리 표준을 바탕으로 국내 환경에 맞게 구성한 정보보호 관리체계이다. 제품 하나의 보안 기능만 평가하는 것이 아니라, 조직의 정책·위험관리·보호대책·운영 등 **정보보호 관리체계 전반**을 다룬다. 국내 ISMS 인증과 BS7799 인증 자체가 동일한 제도라는 뜻은 아니다.

NoteBase

문 16. 서비스거부 공격(DoS: Denial of Service)의 유형 중 Smurf 공격에 관한 다음 설명 중 가장 옳은 것은 무엇인가?

① 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN 패킷을 전송한다.

② 출발지와 목적지의 IP주소를 동일하게 공격대상의 IP주소로 위조하여 전송한다.

③ 출발지 IP주소를 공격대상 IP주소로 위조하여 ICMP 패킷을 브로드캐스트 주소로 전송한다.

④ ICMP PING 패킷을 비정상적으로 크게 만들어 전송한다.

정답 3번

간단한 해설

Smurf 공격은 **피해자 주소로 위조한 ICMP 요청을 브로드캐스트로 보내**, 여러 호스트의 응답이 피해자에게 몰리게 하는 반사·증폭 공격이다. SYN 패킷이나 비정상적인 패킷 크기가 아니라, 다수의 ICMP 응답을 유도한다는 점이 핵심이다.

선지별 해설

① X: 다량의 SYN을 보내 연결 설정 자원을 소모시키는 SYN 플러딩 공격에 대한 설명이다. 존재하지 않는 출발지로 위조하면 서버의 SYN-ACK에 정상적인 마지막 ACK가 돌아오지 않아, 서버가 미완성 연결을 유지하는 자원이 소모될 수 있다. Smurf의 핵심인 브로드캐스트 ICMP 응답 증폭과는 다르다.

② X: 출발지와 목적지를 모두 피해자의 주소로 지정하는 것은 LAND 공격의 특징이다. 자신을 출발지로 표시한 비정상적인 패킷을 피해자에게 보내 처리상의 취약점을 악용하는 방식이며, 여러 호스트의 응답을 한곳으로 모으는 Smurf와 구별된다.

③ O: ICMP Echo Request의 출발지를 피해자의 IP 주소로 위조하여 브로드캐스트 주소로 보내면, 이를 수신하고 응답하는 여러 호스트의 Echo Reply가 피해자에게 향한다. 이때 **요청을 받은 여러 호스트가 응답량을 증폭**시키므로 피해자의 네트워크나 처리 자원을 소모시킬 수 있다. 브로드캐스트 전달 및 응답이 허용되는 환경이라는 조건이 필요하다.

④ X: 비정상적으로 큰 ICMP 패킷을 이용하는 것은 Ping of Death 공격에 대한 설명이다. 허용 크기를 넘는 패킷의 재조립·처리 과정에 있는 취약점 등을 악용하는 방식으로, 단순히 모든 큰 패킷이 공격이라는 뜻은 아니다. Smurf는 패킷 크기 이상보다 **위조된 출발지와 브로드캐스트 응답의 결합**이 구별 기준이다.

NoteBase

문 17. 리눅스에서 파일 접근권한 중 setuid나 setgid가 설정되어 있으면 보안상 위험해 질 수 있다. setuid나 setgid가 설정되어 있는 파일을 찾는 명령이 아닌 것은 무엇인가?

① find / -perm -1000 -print

② find / -perm -2000 -print

③ find / -perm -4000 -print

④ find / -perm -6000 -print

정답 1번

간단한 해설

8진수 권한 값에서 **1000은 sticky bit**, 2000은 setgid, 4000은 setuid이다. 따라서 -perm -1000은 setuid나 setgid 비트를 검사하는 조건이 아니다.

핵심 풀이

각 명령은 /부터 탐색하며, -perm은 권한 비트를 검사하고 -print는 조건에 맞는 경로를 출력한다. -perm 뒤의 값이 -mode 형태이면 **mode에 지정한 비트가 모두 설정**되어 있어야 하며, 나머지 비트의 설정 여부는 따지지 않는다. 여기의 권한 값은 8진수이다.

① find / -perm -1000 -print는 1000에 해당하는 sticky bit가 설정된 경로를 찾는다. setuid나 setgid 비트 자체를 검사하지 않는다. sticky bit와 다른 특수 비트가 함께 설정된 경로가 우연히 포함될 수는 있지만, 이 명령의 검색 기준은 sticky bit이다.

② find / -perm -2000 -print는 setgid 비트가 설정된 경로를 찾는다. setgid는 8진수 권한 값 2000에 해당한다.

③ find / -perm -4000 -print는 setuid 비트가 설정된 경로를 찾는다. setuid는 8진수 권한 값 4000에 해당한다.

④ find / -perm -6000 -print는 setuid와 setgid가 **둘 다 설정된** 경로를 찾는다. 6000은 두 비트를 함께 지정한 값이고, 앞의 -는 지정한 비트를 모두 요구한다. 따라서 둘 중 하나만 설정된 모든 경로를 찾는 조건은 아니지만, 검색 결과에는 두 특수 비트가 설정되어 있다. GNU find에서 둘 중 하나 이상을 검사하려면 -perm /6000을 사용한다.

따라서 setuid·setgid가 아닌 sticky bit를 검색 기준으로 삼은 명령은 ①이다.

NoteBase

문 18. 다음 지문에서 설명하는 프로토콜은 무엇인가?

가. TCP/IP 네트워크의 시스템이 동일 네트워크나 다른 시스템의 MAC 주소를 알고자 하는 경우에 사용한다.
나. IP 주소를 물리적인 하드웨어 주소인 MAC 주소로 변환하여 주는 프로토콜이다.

① TCP/IP
② ARP
③ RARP
④ SMTP

정답 2번

간단한 해설

알고 있는 **IPv4 주소에 대응하는 MAC 주소**를 알아내는 프로토콜은 ARP이다. MAC 주소를 바탕으로 IP 주소를 알아내는 RARP와는 변환 방향이 반대이다.

핵심 풀이

지문의 핵심은 가의 'MAC 주소를 알고자 하는 경우'와 나의 'IP 주소를 MAC 주소로 변환'이다. IPv4 패킷을 이더넷 프레임에 담아 전달하려면 같은 링크에서 다음으로 받을 장치의 MAC 주소가 필요하며, ARP가 IP 주소와 MAC 주소의 대응을 알아내는 역할을 한다.

필요한 대응 정보가 ARP 캐시에 없으면 보통 ARP 요청을 같은 링크에 브로드캐스트하고, 해당 주소에 대한 응답으로 MAC 주소를 확인한다. 목적지가 다른 네트워크에 있으면 원격 목적지의 MAC 주소를 직접 구하는 것이 아니라 **같은 링크에 있는 다음 홉 라우터의 MAC 주소**를 구한다.

RARP는 자신의 MAC 주소를 알고 있는 장치가 대응하는 IP 주소를 얻는 역방향 주소 결정 방식이다. 따라서 지문의 IP 주소에서 MAC 주소를 찾는 방향과 맞지 않는다.

TCP/IP는 인터넷 통신에 사용하는 프로토콜 체계의 이름으로, 지문이 요구하는 구체적인 주소 결정 프로토콜명이 아니다.

SMTP는 전자우편을 전송하는 응용 계층 프로토콜이므로 IP 주소와 MAC 주소의 대응을 구하는 기능과 다르다.

두 단서를 충족하는 프로토콜은 ARP이므로 ②가 해당한다.

NoteBase

문 19. 방화벽(firewall)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 패킷 필터링(Packet Filtering) 방화벽은 특정 IP, 프로토콜, 포트의 차단 및 허용을 할 수 있다.

② 패킷 필터링(Packet Filtering) 방화벽은 바이러스에 감염된 파일 전송시 분석이 불가능하다.

③ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 응용 계층에서 동작하기 때문에 다른 방식의 방화벽에 비해 처리 속도가 가장 빠르다.

④ 어플리케이션 게이트웨이(Application Gateway) 방화벽은 각 서비스별로 프록시 데몬이 존재한다.

정답 3번

간단한 해설

어플리케이션 게이트웨이는 **응용 데이터 해석과 프록시 중계**를 수행하므로 처리 부담이 생긴다. 응용 계층에서 동작한다는 이유로 다른 방식보다 속도가 가장 빠르다고 할 수 없다.

선지별 해설

① O: 패킷 필터링 방화벽은 주로 **패킷 헤더의 IP 주소·프로토콜·포트**를 규칙과 비교하여 통과 여부를 결정한다. 따라서 특정 주소나 서비스에 대한 차단·허용이 가능하다.

② O: 기본적인 패킷 필터링은 헤더 정보로 통신을 판정하므로, 전송 파일의 내용을 재구성하여 바이러스 감염 여부를 검사하는 기능은 제공하지 않는다. 파일 악성코드 분석에는 **별도의 콘텐츠 검사·악성코드 탐지 기능**이 필요하다.

③ X: 어플리케이션 게이트웨이는 응용 프로토콜의 내용과 동작을 해석하고 통신을 중계하므로 처리 부담이 커질 수 있다. **응용 계층에서 동작한다고 처리 속도가 가장 빠른 것은 아니다**. 단순한 헤더 검사보다 정밀한 통제가 가능하다는 장점과, 분석·중계에 드는 비용을 구별해야 한다.

④ O: 어플리케이션 게이트웨이는 각 서비스의 프로토콜을 이해하는 프록시를 통해 클라이언트와 서버 사이의 통신을 중계한다. 따라서 서비스별 프록시 데몬이 필요하며, 해당 서비스용 프록시가 지원되어야 그 서비스를 처리할 수 있다.

NoteBase

문 20. 침입탐지방법에 관한 다음 설명 중 ( ) 안에 들어갈 내용으로 바르게 짝지은 것은 무엇인가?

오용탐지(Misuse)는 침입패턴 정보를 데이터베이스화하고, 사용자 혹은 침입자가 네트워크 및 호스트를 사용하는 활동 기록과 비교하여 동일하면 침입으로 식별하는 것이다. 이 방법은 False Positive가 (가)는 장점이 있지만 반대로 False Negative가 (나)는 단점이 있다.

① (가) 높다 (나) 낮다
② (가) 낮다 (나) 높다
③ (가) 높다 (나) 높다
④ (가) 낮다 (나) 낮다

정답 2번

간단한 해설

오용탐지는 알려진 공격 패턴과 일치하는지를 확인하므로 **정상 활동을 공격으로 잘못 경보하는 경우는 적은 편**이다. 반면 등록되지 않은 새로운 공격을 놓치기 쉬워 False Negative가 높아질 수 있다.

빈칸별 해설

오용탐지는 알려진 공격의 특징을 시그니처로 저장하고 관찰된 활동과 대조하는 방식이다. 여기서 양성(Positive)은 침입으로 판정하는 것이고, 음성(Negative)은 침입으로 판정하지 않는 것이다. 지문은 이 방식의 전형적인 장단점을 비교한다.

(가) 낮다: False Positive는 실제로는 정상 활동인데 침입이라고 잘못 경보하는 오탐이다. 오용탐지는 알려진 공격의 구체적인 패턴을 기준으로 하므로, 패턴이 적절히 정의되어 있으면 정상 활동을 막연히 비정상으로 판단하는 경우가 비교적 적다. 따라서 빈칸에는 '낮다'가 들어간다. 다만 시그니처가 지나치게 넓거나 부정확하면 오탐이 발생할 수 있으므로, 오탐이 전혀 없다는 뜻은 아니다.

(나) 높다: False Negative는 실제 공격이 발생했는데도 이를 침입으로 식별하지 못하는 미탐이다. 새로운 공격이나 기존 패턴에서 벗어난 변형 공격은 시그니처와 일치하지 않아 놓칠 수 있다. 이 때문에 **알려지지 않은 공격에 대한 미탐 위험**이 상대적으로 커진다는 것이 오용탐지의 한계이다. 알려진 패턴의 공격까지 언제나 잘 탐지하지 못한다는 뜻은 아니다.

따라서 (가)는 낮다, (나)는 높다이며, 이 조합에 해당하는 것은 ②이다.

NoteBase

문 21. 보안 취약점 점검 도구에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① netstat은 대부분의 운영체제에 기본으로 탑재된 도구이며 네트워크 상태를 확인하기 위해 사용한다.

② tcpdump는 네트워크 패킷 출력 도구로 특정 구간의 장비 사이에서 네트워크 통신이 되는지 확인하기 위해 사용한다.

③ nmap은 포트 스캔뿐만 아니라 대상 시스템의 운영체제나 네트워크 장치 정보 등을 수집할 수 있는 보안 스캐너이다.

④ WireShark는 네트워크 패킷 생성 및 재전송 도구로 네트워크 침해사고 분석 중 확보한 패킷 파일을 시뮬레이션하기 위해 사용한다.

정답 4번

간단한 해설

Wireshark의 핵심 기능은 **패킷 수집과 프로토콜 분석**이다. 저장된 패킷을 읽어 분석하는 것과, 패킷을 네트워크에 다시 보내는 재전송은 구별된다.

선지별 해설

① O: netstat은 연결 상태, 수신 대기 포트, 네트워크 통계 등 **운영체제의 네트워크 상태**를 확인하는 도구이다. 여러 운영체제에서 기본 도구로 널리 제공되어 왔으며, 구체적인 설치 여부와 표시 항목은 운영체제·환경에 따라 달라질 수 있다.

② O: tcpdump는 관찰 가능한 네트워크 인터페이스에서 패킷을 캡처하고 내용을 출력하는 도구이다. 장비 사이에 요청·응답 패킷이 오가는지 살펴보아 통신 여부나 장애 원인을 확인할 수 있다. 관찰 가능한 구간의 트래픽을 확인한다는 점이 전제된다.

③ O: nmap은 포트 상태를 조사하는 보안 스캐너이며, 옵션과 대상의 응답에 따라 **운영체제·서비스·장치 유형** 등의 정보도 추정할 수 있다. 수집 결과의 정확성은 대상과 네트워크 환경에 영향을 받는다.

④ X: Wireshark는 네트워크 패킷을 **수집하고 해석·분석하는 도구**이다. 저장된 패킷 파일을 열어 통신 내용을 분석할 수 있지만, 그 패킷을 네트워크로 재전송하는 도구는 아니다. 확보한 패킷의 재전송에는 Tcpreplay 같은 별도의 도구를 사용한다.

NoteBase

문 22. 스위치 환경 하에서 나타나는 스니핑(Sniffing) 기법이 아닌 것은 무엇인가?

① Switch Jamming

② ARP Spoofing

③ ICMP Redirect

④ Session Hijacking

정답 4번

간단한 해설

스니핑의 핵심은 통신 내용을 엿보는 것이고, Session Hijacking의 핵심은 **정상 사용자의 세션을 탈취해 그 사용자처럼 통신하는 것**이다. 세션 탈취 과정에 스니핑이 이용될 수 있어도 두 공격의 목적과 기능은 다르다.

개념 구분

스위치는 학습한 MAC 주소에 따라 프레임을 해당 포트로 전달하므로, 다른 호스트의 유니캐스트 트래픽을 단순히 수신하는 데 제약이 있다. 스위치 환경의 스니핑 기법은 이 전달 방식을 교란하거나 경로를 바꾸어 공격자가 트래픽을 볼 수 있게 하는 데 초점이 있다.

Switch Jamming은 MAC 주소 테이블의 용량을 소진시키는 등의 방법으로 정상적인 주소 학습을 방해하는 기법이다. 목적지 포트를 알 수 없게 된 프레임이 같은 VLAN의 여러 포트로 전달되는 현상을 악용하여 도청 기회를 만든다. 모든 스위치가 무조건 허브처럼 동작한다는 뜻은 아니며, 장비 동작과 보안 설정에 따라 제한될 수 있다.

ARP Spoofing은 IP 주소와 MAC 주소의 대응 정보를 거짓으로 인식시키는 기법이다. 통신이 공격자 쪽으로 향하도록 유도하여 스위치 환경에서도 트래픽을 관찰하는 데 악용될 수 있다.

ICMP Redirect의 악용은 경로 변경 정보를 신뢰하는 호스트가 트래픽을 다른 다음 홉으로 보내도록 유도하는 방식이다. 잘못된 경로가 받아들여지면 공격자 쪽으로 흐르는 트래픽을 엿볼 수 있다.

Session Hijacking은 이미 형성된 세션의 제어권이나 인증 상태를 빼앗아 정당한 통신 당사자로 가장하는 공격이다. 단순한 **통신 내용의 관찰**을 넘어 **세션의 탈취와 무단 사용**이 핵심이다.

따라서 스위치 환경에서 트래픽을 엿보기 위한 기법과 구별되는 것은 ④ Session Hijacking이다.

NoteBase

문 23. 다음 지문은 무엇에 관한 설명인가?

무선랜을 통하여 전송되는 패킷의 각 헤더에 덧붙여지는 32바이트 길이의 고유 식별자로서, 무선장비가 BSS(Basic Service Set)에 접속할 때 암호처럼 사용한다.

① SSID(Service Set Identifier)
② WEP(Wired Equivalent Privacy)
③ MAC(Message Authentication Code)
④ RFID(Radio Frequency Identification)

정답 1번

간단한 해설

BSS에 접속할 때 사용할 무선 네트워크를 구별하는 이름은 **SSID**이다. SSID는 최대 32바이트의 식별자이며 비밀 인증 암호와는 구별된다.

개념 구분

지문의 핵심 단서는 무선랜에서 접속할 네트워크를 구별하는 식별자라는 점이다. SSID는 **무선 네트워크의 이름**에 해당하며, 단말이 원하는 서비스 집합을 식별하는 데 사용한다. BSS 접속과 32바이트라는 단서도 SSID를 가리킨다.

다만 지문의 표현은 정확한 기술적 의미와 구별해야 한다. SSID의 길이는 고정 32바이트가 아니라 **최대 32바이트**이다. SSID는 비콘·탐색·연결 요청 등의 관리 프레임에서 전달되는 정보요소이며, 모든 무선 데이터 패킷의 헤더에 반드시 붙는 것은 아니다. 또한 '암호처럼 사용한다'는 표현을 비밀 인증 암호라는 뜻으로 이해하면 안 된다. SSID는 공개될 수 있는 식별자이고, 인증·암호화에 쓰는 비밀번호나 키는 별도이다.

② WEP는 무선랜의 통신 내용을 보호하기 위해 사용된 초기 보안 방식이다. 접속할 네트워크의 이름을 뜻하는 식별자가 아니다.

③ 이 선지의 MAC은 Message Authentication Code, 즉 메시지 인증 코드이다. 비밀키를 이용해 메시지의 무결성과 인증을 확인하는 값이며, 네트워크 이름이나 장치의 MAC 주소를 뜻하지 않는다.

④ RFID는 무선 주파수를 이용하여 태그의 정보를 읽고 대상을 식별하는 기술이다. 무선랜의 서비스 집합을 구별하는 이름과는 다르다.

따라서 지문이 가리키는 개념은 ① SSID이다.

NoteBase

문 24. IPSec 프로토콜에서 AH(Authentication Header) 프로토콜이 제공하는 보안 기능이 아닌 것은 무엇인가?

① 무결성
② 인증
③ 기밀성
④ 재전송 공격방지

정답 3번

간단한 해설

AH는 데이터의 변경 여부와 출처를 확인하지만 **데이터를 암호화하지 않으므로 기밀성을 제공하지 않는다**.
무결성·데이터 출처 인증과 재전송 공격 방지는 AH가 지원하는 기능이다.

개념 구분

AH(Authentication Header)는 IP 패킷에 인증 정보를 붙여 무결성과 데이터 출처 인증을 제공하는 IPSec 프로토콜이다. 인증 정보를 붙이는 것과 본문을 암호화하여 숨기는 것은 서로 다른 기능이다.

무결성: 수신자는 인증 값을 검증하여 보호 대상 데이터가 전송 중 변경되었는지 확인할 수 있다. AH는 데이터뿐 아니라 전송 중 변하지 않는 IP 헤더 부분도 보호하지만, 경유 과정에서 값이 바뀌는 모든 헤더 필드까지 그대로 보호하는 것은 아니다.

인증: 해당 패킷이 보안 연결에서 정한 키를 사용하는 정당한 상대방에게서 왔는지 확인하는 **데이터 출처 인증**을 지원한다. 데이터의 출처를 확인하는 기능이며, 메시지 내용을 감추는 암호화와는 구별된다.

기밀성: 권한 없는 사람이 메시지 내용을 알 수 없게 하는 성질이다. AH는 **패킷 본문을 암호화하지 않으므로 기밀성을 제공하지 않는다**. IPSec에서 암호화를 통한 기밀성이 필요하면 ESP의 암호화 기능을 사용한다.

재전송 공격방지: AH의 순서 번호와 수신 측의 재전송 검사 기능을 이용하여 이미 받은 패킷이 다시 제출되는 것을 탐지하고 거부할 수 있다. 이 기능은 수신 측에서 사용하도록 선택하여 순서 번호를 검사할 때 유효하다.

따라서 AH가 제공하지 않는 보안 기능은 기밀성이며, ③과 연결된다.

NoteBase

문 25. 무선랜에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 일반적으로 유선랜에 비해 품질이 낮다.

② 인증 암호의 취약성이 있다.

③ 무선 네트워크는 외부 전자기기와의 전파간섭이 없다.

④ 물리적 특성으로 인한 도난, 불법설치, 불법도청 등의 취약성이 있다.

정답 3번

간단한 해설

무선랜은 전파를 사용하므로 **같거나 인접한 주파수 대역을 사용하는 기기의 간섭**을 받을 수 있다. 외부 전자기기의 영향이 없다는 설명은 무선 매체의 특성과 반대이다.

선지별 해설

① O: 무선랜은 거리, 장애물, 전파 간섭, 매체를 함께 사용하는 단말 수 등에 따라 신호 품질과 실제 전송률이 달라진다. 따라서 안정된 유선 연결에 비해 통신 품질의 변동이나 손실이 커지기 쉽다는 일반적인 비교이다. 모든 무선랜의 최대 속도가 모든 유선랜보다 낮다는 절대적 의미는 아니다.

② O: 인증 방식이나 암호 설정이 취약하면 비인가 접속이나 통신 내용 노출의 위험이 있다. 약한 공유 비밀번호, 오래된 보안 방식, 잘못된 설정 등이 그 예이다. 이는 인증·암호화의 취약성을 관리해야 한다는 뜻이며, 적절한 보안 방식을 사용하는 모든 무선랜이 반드시 쉽게 해독된다는 뜻은 아니다.

③ X: 무선랜은 외부 전자기기나 주변 무선 기기로부터 간섭을 받을 수 있다. 예를 들어 같은 대역을 사용하는 다른 무선랜이나 일부 블루투스 장치, 전자레인지 등이 영향을 줄 수 있다. 간섭이 생기면 오류와 재전송이 늘고 전송률이 낮아질 수 있으므로, **전파 간섭이 없다는 부분**이 틀렸다.

④ O: 무선 장비나 이동 단말의 도난, 관리자가 승인하지 않은 AP의 설치, 전파 수신을 통한 도청 등이 위협이 될 수 있다. 전파는 건물의 물리적 경계를 넘어 도달할 수 있으므로, 통신선에 직접 연결하지 않고도 신호를 관찰할 여지가 있다. 따라서 물리적 장비 관리와 함께 **인증·암호화 및 비인가 AP 관리**가 필요하다.

NoteBase

문 26. 다음 지문은 무엇에 관한 설명인가?

가. Phil Zimmermann이 개발한 대표적인 이메일 보안프로토콜이다.
나. RSA와 Diffie-Hellman 등으로 공개키 생성이 가능하다.
다. 암호 알고리즘을 이용하여 기밀성, 인증, 무결성, 부인방지 등의 기능 지원이 가능하다.

① POP3

② S/MIME

③ PEM

④ PGP

정답 4번

간단한 해설

Phil Zimmermann이 개발한 전자우편 보안 도구는 **PGP**이다. 암호화와 전자서명을 결합하여 기밀성·인증·무결성·부인방지 기능을 지원한다.

NoteBase

핵심 풀이

가. PGP는 Phil Zimmermann이 개발한 전자우편 보안 도구이다. **개발자 이름**이 다른 이메일 관련 방식과 구별하는 직접적인 단서이다.

나. PGP는 공개키·개인키 쌍을 활용하며, RSA 방식과 Diffie-Hellman 계열의 ElGamal 방식 등을 사용해 왔다. 지문의 설명은 이런 공개키 암호 기술의 지원을 가리킨다. 지원 알고리즘은 버전·구현에 따라 달라질 수 있고, 암호화용 키와 서명용 키의 역할은 구별된다.

다. 메시지 암호화는 내용을 숨겨 기밀성을 제공한다. 전자서명은 작성자를 확인하고 변경 여부를 탐지하여 인증·무결성을 제공하며 부인방지를 지원한다. 즉 **암호화와 전자서명을 결합**하여 여러 보안 기능을 제공할 수 있다.

POP3는 메일 서버에 저장된 전자우편을 가져오기 위한 프로토콜이다. 지문과 같은 종합적인 메시지 보안 방식의 명칭은 아니다.

S/MIME도 전자우편의 암호화와 서명을 지원하지만, MIME 메시지에 보안 기능을 적용하는 표준이며 Phil Zimmermann이 개발한 도구라는 단서에 해당하지 않는다.

PEM은 전자우편의 프라이버시 보호를 위해 마련된 보안 방식이다. 이메일 보안이라는 공통점만으로 고르지 않고 개발자 단서까지 함께 대조해야 한다.

따라서 지문은 PGP를 설명하며, ④에 해당한다.

NoteBase

문 27. FTP(File Transfer Protocol)에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 네트워크에서 컴퓨터 간 파일 송·수신을 위한 프로토콜이다.

② FTP는 두 개의 잘 알려진(well-known) TCP 포트를 사용한다.

③ 포트 20번은 제어 연결을 위해 사용되고, 포트 21번은 데이터 연결을 위해 사용된다.

④ FTP는 기본적으로 Active Mode와 Passive Mode를 지원한다.

정답 3번

간단한 해설

FTP의 **제어 연결은 TCP 21번**을 사용하며, 전통적인 능동 모드에서 서버 측 데이터 연결의 기본 포트는 TCP 20번이다. 두 포트의 역할을 뒤바꾼 설명이 틀렸다.

선지별 해설

① O. FTP는 네트워크를 통해 컴퓨터 사이에서 파일을 업로드하거나 다운로드하는 데 사용하는 응용 계층 프로토콜이다. 명령과 응답을 주고받는 제어 연결과 실제 내용을 옮기는 데이터 연결을 구분한다.

② O. FTP에는 전통적으로 TCP 20번과 21번이라는 두 개의 잘 알려진 포트가 정해져 있다. 다만 수동 모드에서는 별도로 정한 서버 포트로 데이터 연결을 맺으므로, 모든 FTP 통신이 언제나 두 포트만 사용한다는 뜻은 아니다.

③ X. **21번은 제어 연결, 20번은 능동 모드의 서버 측 기본 데이터 포트**이다. 제어 연결에는 로그인·파일 전송 요청 같은 명령과 응답이 흐르고, 데이터 연결에는 파일 내용이나 디렉터리 목록 등이 흐른다. 선지는 두 포트의 용도를 반대로 설명했다.

④ O. 능동 모드에서는 서버가 클라이언트 쪽으로 데이터 연결을 시작하고, 수동 모드에서는 클라이언트가 서버가 알려 준 포트로 데이터 연결을 시작한다. 두 방식의 핵심 차이는 **데이터 연결을 시작하는 쪽**이며, 제어 연결은 클라이언트가 서버에 요청한다.

제어 포트와 데이터 포트를 뒤바꾼 ③이 가장 옳지 않은 설명이다.

NoteBase

문 28. DNSSEC는 DNS(Domain Name System)가 갖고 있는 보안 취약점을 극복하기 위한 DNS 확장 표준프로토콜이다. DNSSEC이 예방할 수 있는 공격기법은 무엇인가?

① 파밍(Pharming)
② 피싱(Phishing)
③ 스미싱(Smishing)
④ 랜섬웨어(Ransomware)

정답 1번

간단한 해설

DNSSEC는 전자서명으로 DNS 응답의 출처와 무결성을 검증하여 **위조된 DNS 정보로 가짜 사이트에 연결시키는 파밍**을 방어한다. 사용자를 속이는 모든 메시지나 악성코드를 차단하는 기능은 아니다.

개념 구분

DNS는 도메인 이름에 대응하는 IP 주소 등을 알려 준다. 이 정보를 공격자가 위조하면 사용자가 정상 도메인을 입력해도 다른 서버로 연결될 수 있다. DNSSEC는 서명된 DNS 데이터의 출처와 무결성을 검증하여 이러한 위조를 탐지하는 데 사용된다.

파밍(Pharming): 정상 사이트에 접속하려는 사용자를 가짜 사이트로 돌리는 공격이다. 특히 **DNS 응답 위조나 캐시 오염을 이용하는 파밍**은 DNSSEC의 서명 검증으로 방어할 수 있다. 다만 보호 대상 도메인에 DNSSEC가 적용되고 검증이 제대로 이루어져야 하며, 사용자 컴퓨터의 다른 설정을 변조하는 모든 형태의 파밍까지 막는다는 뜻은 아니다.

피싱(Phishing): 신뢰할 만한 기관이나 사람을 사칭하여 사용자가 비밀번호 등 민감한 정보를 제공하도록 속이는 공격이다. 사용자가 공격자의 도메인으로 직접 유도되는 경우 DNS 응답 자체는 정상일 수 있으므로, **DNS 정보 검증만으로 사칭 내용까지 판별하지 못한다**.

스미싱(Smishing): 문자메시지를 이용하는 피싱이다. 문자에 담긴 사칭 내용이나 악성 링크로 사용자를 속이는 것이 핵심이므로, DNS 데이터의 무결성을 확인하는 DNSSEC가 이를 전반적으로 차단하지는 않는다.

랜섬웨어(Ransomware): 파일을 암호화하거나 시스템 접근을 제한하고 복구 대가를 요구하는 악성코드이다. DNS 응답의 위조와는 다른 공격 방식이므로, DNSSEC는 파일 암호화나 악성코드 실행을 직접 막는 기능이 아니다.

따라서 제시된 공격 중 DNSSEC가 직접 방어하는 DNS 위조와 연결되는 것은 파밍이며, ①에 해당한다.

NoteBase

문 29. 웹 서비스 공격기법에 관한 다음 설명 중 공격기법을 바르게 짝지은 것은 무엇인가?

(가) 게시판의 글에 원본과 함께 악성코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 함으로써 클라이언트의 정보를 유출하는 공격기법
(나) 공격자의 악의적인 데이터로 예상하지 못한 명령을 실행하거나 적절한 권한없이 데이터에 접근하도록 인터프리터를 속이는 공격기법
(다) 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격기법

① (가) CSRF (나) Injection (다) XSS
② (가) XSS (나) Injection (다) CSRF
③ (가) CSRF (나) XSS (다) File Upload
④ (가) XSS (나) File Upload (다) Injection

정답 2번

간단한 해설

XSS는 웹페이지에 섞인 코드가 브라우저에서 실행되는 문제이고, Injection은 입력이 명령으로 해석되는 문제이다. **사용자의 인증 상태를 악용해 원치 않는 요청을 보내게 하는 것**은 CSRF이다.

NoteBase

대응 관계 해설

세 설명은 공격자의 입력이 어디에서 어떤 역할을 하게 되는지를 기준으로 구분한다. 게시글 속 코드가 브라우저에서 실행되는지, 데이터가 인터프리터의 명령으로 해석되는지, 사용자의 인증을 이용한 요청이 발생하는지를 살펴보면 된다.

(가) XSS: 게시판에 저장된 악성 스크립트가 다른 사용자의 브라우저에서 게시글과 함께 실행되는 저장형 XSS에 해당한다. 브라우저가 해당 웹사이트의 콘텐츠로 받아들여 실행한 코드가 사용자의 정보에 접근하거나 페이지를 조작할 수 있다는 점이 핵심이다. **서버에 저장된 게시글이 전달 경로이고, 코드 실행은 클라이언트에서 일어난다**.

(나) Injection: 공격자가 넣은 데이터가 원래의 데이터 범위를 벗어나 명령이나 질의의 일부로 해석되는 공격이다. 인터프리터가 이를 정상적인 명령처럼 처리하면 개발자가 의도하지 않은 동작을 하거나 권한 없는 데이터 접근이 발생할 수 있다. SQL 인젝션이나 명령어 인젝션이 대표적이며, 공통 원인은 **데이터와 명령의 경계가 무너지는 것**이다. XSS도 넓게는 코드 삽입 공격이지만, (가)는 그중 브라우저 스크립트 실행을 구체적으로 가리킨다.

(다) CSRF: 사용자가 원하지 않은 요청을 공격자가 유도하고, 웹사이트가 사용자의 인증 쿠키 등과 함께 도착한 요청을 정상 요청으로 받아들이는 공격이다. 사용자의 권한으로 특정 동작을 실행하게 한다는 점이 핵심이며, 응답 내용을 공격자가 읽거나 사이트 안에서 스크립트를 실행해야만 성립하는 것은 아니다. XSS의 코드 실행과 구별해야 한다.

File Upload 공격은 업로드 제한이나 파일 처리의 허점을 이용해 위험한 파일을 서버에 올리는 등의 방식이다. (나)의 인터프리터 조작이나 (다)의 사용자 요청 위조를 단순히 파일 업로드로 분류할 수는 없다.

따라서 (가)는 XSS, (나)는 Injection, (다)는 CSRF이므로 ②가 정답이다.

NoteBase

문 30. 데이터베이스 보안 요구사항에 관한 다음 설명 중 가장 옳지 않은 것은 무엇인가?

① 부적절한 접근방지 - 인가된 사용자의 접근만이 허락되고 모든 접근요청은 DBMS가 검사한다.

② 추론방지 - 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 해야 하는 것을 의미한다.

③ 사용자 인증 - 별도의 엄격한 사용자 인증방식이 필요하다.

④ 다단계 보호 - 데이터에 대한 등급분류를 통하여 책임추적성을 보장한다.

정답 4번

간단한 해설

다단계 보호는 데이터와 사용자의 등급에 따른 **접근통제**를 위한 것이다. 누가 어떤 작업을 했는지 추적하는 책임추적성은 사용자 식별과 감사 기록으로 확보해야 한다.

선지별 해설

① O. 부적절한 접근방지는 사용자가 허용받지 않은 데이터나 연산에 접근하지 못하도록 하는 것이다. DBMS는 접근요청마다 사용자와 부여된 권한을 확인하여 허용 여부를 판단해야 한다. 로그인한 사용자라도 모든 데이터에 무제한으로 접근할 수 있는 것은 아니다.

② O. 추론방지는 공개가 허용된 통계 결과들을 이용해 비공개인 개별 데이터를 알아내는 일을 막는 것이다. 개별 행의 직접 조회를 차단했더라도, 여러 집계 결과를 조합해 특정 개인의 값을 추정할 수 있다면 정보가 노출될 수 있다.

③ O. 사용자 인증은 데이터베이스에 접근하려는 주체가 자신이 주장하는 사용자임을 확인하는 절차이다. 다른 사용자를 사칭한 접근을 막기 위해 충분히 엄격한 인증이 필요하다. 인증 후 어떤 데이터와 연산을 허용할지는 접근권한에 따라 별도로 판단한다.

④ X. 다단계 보호는 데이터의 민감도 등급과 사용자의 접근 허용등급 등을 비교하여 **등급에 맞는 접근통제**를 수행하는 것이다. 등급분류 자체가 누가 어떤 작업을 했는지를 밝혀 주지는 않는다. 책임추적성을 확보하려면 사용자 식별정보와 접근·변경 내역을 감사 로그 등으로 기록하고 보호해야 한다.

따라서 다단계 보호를 책임추적성 보장으로 잘못 연결한 ④가 가장 옳지 않다.

NoteBase

문 31. 다음 지문은 무엇에 관한 설명인가?

가. 기기 내부에 암호화 및 복호화 그리고 전자서명을 위한 프로세스 및 연산장치가 내장되어 있어 암호화와 관련된 키의 생성 및 검증 등이 가능하다.
나. 보안토큰을 말하는 것으로 USB토큰 형태 이외에도 칩 형태, PCMCIA토큰 형태 등을 갖는다.

① OTP(One Time Password)
② TPM(Trusted Platform Module)
③ PKI(Public Key Infrastructure)
④ HSM(Hardware Security Module)

정답 4번

간단한 해설

HSM은 **장치 내부에서 암호키를 보호하고 암호 연산을 수행**하는 하드웨어 보안 모듈이다. 보안토큰의 형태보다 키 관리와 암호화·서명 기능이 핵심 단서이다.

핵심 풀이

가. HSM은 **암호키를 보호·관리하면서 내부에서 암호 연산**을 수행하는 하드웨어 보안 모듈이다. 내장된 처리 장치를 이용해 키를 생성하고, 암호화·복호화·전자서명·검증 등의 작업을 처리한다. 단순히 파일을 저장하는 매체와 구별된다.

나. 지문은 이런 기능을 제공하는 보안토큰의 구현 형태로 USB토큰·칩·PCMCIA토큰을 제시한다. 겉모양보다 **키 보호와 장치 내부 암호 연산**이라는 기능이 판단 기준이다. 일반 USB 메모리가 모두 HSM이라는 뜻은 아니다.

OTP는 인증할 때 한 번만 사용하는 비밀번호이다. 토큰 형태로 생성할 수 있어도, 지문에서 묻는 범용 암호 연산 모듈의 명칭과는 다르다.

TPM도 키 보호와 암호 연산을 지원하지만, 기기의 신뢰 기반을 제공하고 플랫폼의 무결성 측정·검증 등을 지원하는 데 초점을 둔다. 지문의 다양한 보안토큰 형태와 일반적인 암호 연산 장치 설명은 HSM을 가리킨다.

PKI는 공개키와 신원을 연결하는 인증서를 발급·관리·폐지하는 기반구조이다. 하나의 암호 연산 장치를 뜻하지 않는다.

따라서 지문은 HSM을 설명하며, ④에 해당한다.

NoteBase

문 32. 다음 지문은 무엇에 관한 설명인가?

신용카드 기반 지불시스템인 SET(Secure Electronic Transaction)에서는 상점이 카드 사용자의 계좌번호와 같은 정보를 모르게 하는 동시에, 상점에 대금을 지불하는 은행은 카드 사용자가 구매한 물건을 알지 못하지만 상점이 요구한 결제 대금이 정확한지 확인할 수 있게 하기 위해 사용하는 방식이다.

① 인증서(Certificate)

② 전자봉투(Digital Envelop)

③ 이중서명(Dual Signature)

④ 지불게이트웨이(Payment Gateway)

정답 3번

간단한 해설

이중서명은 주문정보와 지불정보를 하나의 거래로 결합하여, 상점과 은행이 각자 필요한 정보만 보면서도 두 정보의 연관성과 무결성을 확인하게 한다. 단순히 정보를 암호화하는 전자봉투와 구별된다.

NoteBase

개념 구분

SET에서는 상점에 필요한 주문정보와 은행 측에 필요한 지불정보를 구분한다. 상점에는 카드번호 등의 지불정보를 숨기고, 은행에는 구매 물품의 세부 주문정보를 숨기면서도 주문과 결제가 서로 대응한다는 사실을 검증해야 한다.

인증서(Certificate): 공개키가 누구의 것인지를 확인할 수 있게 하는 전자적 증명서이다. 거래 참여자의 신원과 공개키를 연결하는 데 사용되지만, 그 자체가 주문정보와 지불정보를 하나로 묶는 방식은 아니다.

전자봉투(Digital Envelop): 메시지를 대칭키로 암호화하고, 그 대칭키를 수신자의 공개키로 보호하여 전달하는 방식이다. SET에서 상점이 지불정보를 읽지 못하도록 숨기는 데 활용되지만, **서로 다른 두 정보의 거래상 연결을 서명으로 보장**하는 기능과는 구별된다.

이중서명(Dual Signature): 카드 사용자가 주문정보와 지불정보를 각각 해시하고, 두 해시값을 결합한 뒤 다시 해시한 값에 자신의 개인키로 서명한다. 두 문서에 별개의 서명을 두 번 하는 것이 아니라, **두 정보의 해시를 함께 묶은 하나의 서명**을 만드는 방식이다.

이중서명의 검증: 상점은 주문정보와 지불정보의 해시를, 은행 측은 지불정보와 주문정보의 해시를 이용하여 같은 서명을 검증한다. 각자는 상대방에게만 공개되는 정보의 원문을 몰라도 두 정보가 함께 서명되었는지 확인할 수 있다. 은행 측은 전달받은 지불정보와 상점의 결제 요청을 대조하여 결제 금액을 확인한다. 정보 자체의 비공개는 암호화·분리 전달과 함께 이루어지며, 서명은 두 정보의 연관성과 무결성을 보장한다.

지불게이트웨이(Payment Gateway): 상점의 결제 요청을 금융기관의 결제 처리 체계와 연결하는 중계 역할을 한다. 거래에 참여하는 구성 요소이지, 두 정보를 결합하여 서명하는 암호 기법의 이름은 아니다.

지문의 핵심인 정보의 분리 공개와 주문·지불정보의 연결 검증에 해당하는 방식은 이중서명이므로 ③과 연결된다.

NoteBase

문 33. 다음 중 전자화폐의 요구사항에 포함되지 않는 것은 무엇인가?

① 이중 사용방지(Double-Spending)

② 양도성(Transferability)

③ 온라인성(On-Line)

④ 분할성(Divisibility)

정답 3번

간단한 해설

현금과 유사한 전자화폐에서는 지급할 때마다 발행기관에 실시간으로 접속하지 않아도 되는 **오프라인성**이 중요한 설계 요구사항이다. 따라서 온라인 접속을 반드시 요구하는 온라인성이 그 요구사항인 것은 아니다.

개념 구분

이중 사용방지는 이미 지급한 동일한 전자화폐를 복제하거나 다시 사용하여 가치가 중복 지출되지 않도록 하는 성질이다. 전자 정보는 복제가 쉬우므로 중복 사용을 막거나 적발할 수 있는 통제가 필요하다.

양도성은 받은 전자화폐를 다른 사람에게 지급하는 데 다시 사용할 수 있는 성질이다. 수취자가 매번 발행기관에 반환해야만 하는 방식보다 현금처럼 유통할 수 있도록 하는 요구이다.

온라인성은 거래 때마다 발행기관 등과 실시간으로 연결하는 방식의 특성이다. 현금과 유사한 전자화폐의 요구사항으로는 오히려 **지급 시 중앙기관의 실시간 확인에 의존하지 않는 오프라인성**이 제시된다. 온라인 방식의 전자화폐가 존재하지 않는다는 뜻이 아니라, 온라인 접속이 모든 전자화폐의 필수 요건은 아니라는 의미이다.

분할성은 전자화폐의 가치를 더 작은 금액으로 나누어 필요한 만큼 지급할 수 있는 성질이다. 분할하여 지급한 금액과 남은 금액을 올바르게 관리하여 전체 가치가 늘어나지 않아야 한다.

따라서 현금과 유사한 전자화폐의 설계 요구사항에 해당하지 않는 것은 ③ 온라인성이다.

NoteBase

문 34. 다음 지문은 무엇에 관한 설명인가?

일반적인 정보검색엔진에서는 검색되지 않지만 특정한 환경의 웹 브라우저에서만 접속되어 검색되는 사이트를 가리킨다. 주로 사이버 범죄가 이루어지는 공간이다.

① 웹 쉘 (Web Shell)
② 다크 웹 (Dark Web)
③ 스턱스넷(StuxNet)
④ 고스트넷(GhostNet)

정답 2번

간단한 해설

검색엔진에 노출되지 않는다는 점에 더해 **별도의 네트워크나 전용 접속 환경이 필요하다**는 것이 다크 웹의 결정적 단서이다. 단순히 검색되지 않는 일반 웹페이지와 구별해야 한다.

NoteBase

개념 구분

다크 웹(Dark Web)은 Tor와 같은 별도의 네트워크나 접속 소프트웨어가 필요한 웹 영역을 가리킨다. 일반 검색엔진의 검색 결과에 나타나지 않는다는 점만으로 판별하지 않고, **특수한 접속 환경이 요구된다는 조건**을 함께 확인해야 한다. 익명성을 이용한 사이버범죄에 악용될 수 있지만, 다크 웹의 모든 이용이 불법이거나 범죄 전용 공간이라는 뜻은 아니다.

딥 웹(Deep Web)은 일반 검색엔진에 색인되지 않는 웹 자료를 폭넓게 가리킨다. 로그인 뒤에만 보이는 자료나 검색 양식으로 조회하는 데이터 등도 포함될 수 있으므로, 검색되지 않는다는 이유만으로 모두 다크 웹은 아니다. 다크 웹은 이 가운데 별도의 접속 환경을 요구하는 영역으로 구별한다.

웹 쉘(Web Shell): 웹 서버에서 실행되는 스크립트 등을 통해 원격으로 서버를 조작하게 하는 도구이다. 공격자가 서버에 심어 명령 실행 등의 통로로 악용할 수 있지만, 특수 브라우저로 접속하는 웹 영역의 이름은 아니다.

스턱스넷(StuxNet): 산업제어시스템을 표적으로 삼은 악성코드로 알려져 있다. 제어 설비의 동작에 영향을 주는 공격과 관련된 이름이며, 검색엔진에 노출되지 않는 사이트의 범주를 뜻하지 않는다.

고스트넷(GhostNet): 감염된 컴퓨터를 이용하여 정보를 수집한 사이버 첩보 네트워크에 붙은 이름이다. 웹에 접근하는 방식이나 웹 영역을 구분하는 일반적인 용어가 아니다.

따라서 지문의 두 접속 특성에 해당하는 것은 **다크 웹인** ②이다.

NoteBase

문 35. OECD 개인정보보안 8원칙에 포함되지 않는 것은 무엇인가?

① 이용제한의 원칙

② 정보 정확성의 원칙

③ 비공개의 원칙

④ 안전성 확보의 원칙

정답 3번

간단한 해설

OECD 8원칙에는 비공개가 아니라 **공개의 원칙**이 있다. 이는 개인정보 처리의 정책과 관행을 투명하게 알리라는 뜻이며, 개인정보 내용 자체를 무제한 공개하라는 뜻은 아니다.

개념 구분

OECD의 개인정보보호 8원칙은 수집제한, 정보의 질, 목적 명확화, 이용제한, 안전성 확보, 공개, 개인참가, 책임성의 원칙이다. 개인정보를 보호하면서도 **그 처리 방식과 정책은 투명하게 알린다**는 점이 핵심이다.

① 이용제한의 원칙은 명시된 목적과 다른 목적으로 개인정보를 이용·제공하는 것을 원칙적으로 제한한다. 정보주체의 동의나 법률상 권한이 있는 경우 등의 예외를 두며, 8원칙에 포함된다.

② 정보 정확성의 원칙은 정보의 질 원칙에 해당한다. 개인정보는 이용 목적에 관련되어야 하고, 필요한 범위에서 정확하고 완전하며 최신 상태로 유지되어야 한다.

③ 비공개의 원칙은 8원칙의 명칭이 아니다. 해당하는 원칙은 **공개의 원칙**으로, 개인정보의 처리 관행·정책, 보유 사실과 성격, 주요 이용 목적, 관리 주체 등을 알 수 있게 하는 것이다. 개인정보의 내용 자체를 누구에게나 공개하라는 뜻은 아니다.

④ 안전성 확보의 원칙은 분실, 무단 접근, 훼손, 부당한 이용·변경·공개 등의 위험으로부터 개인정보를 합리적인 보안조치로 보호하도록 한다.

따라서 8원칙에 포함되지 않는 것은 ③ 비공개의 원칙이다.

NoteBase

문 36. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조(벌칙) 내용이 아닌 것은 모두 몇 개인가?

가. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.
나. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.
다. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 다른 사람을 모욕한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
라. 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 사자의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 3천만원 이하의 벌금에 처한다.

① 1개
② 2개
③ 3개
④ 4개

정답 2번

간단한 해설

제70조는 정보통신망에서 사실 또는 거짓의 사실을 드러내어 다른 사람의 명예를 훼손하는 행위를 규정한다. 모욕과 사자명예훼손은 형법의 별도 조항과 구별해야 한다.

NoteBase

보기별 해설

2018년 시험 당시의 규정을 기준으로 판단한다.

가. (O) **사실을 드러낸 명예훼손**은 제70조 제1항의 내용이다. 비방할 목적으로 정보통신망을 이용해 공공연하게 다른 사람의 명예를 훼손한 경우, 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. 제시된 요건과 법정형이 일치한다.

나. (O) **거짓의 사실을 드러낸 명예훼손**은 제70조 제2항의 내용이다. 비방 목적·정보통신망 이용·공연성이라는 요건 아래, 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다. 사실을 드러낸 경우보다 무겁게 처벌한다.

다. (X) **모욕**은 제70조에 규정된 범죄가 아니다. 공연히 사람을 모욕하는 행위는 형법 제311조의 모욕죄로 다루며, 당시 법정형은 **1년 이하의 징역이나 금고 또는 200만원 이하의 벌금**이다. 지문의 2년·500만원도 잘못되었다.

라. (X) **사자명예훼손** 역시 제70조의 내용이 아니다. 공연히 허위의 사실을 적시하여 사자의 명예를 훼손하는 행위는 형법 제308조에 규정되어 있으며, 당시 법정형은 **2년 이하의 징역이나 금고 또는 500만원 이하의 벌금**이다. 지문의 3년·3천만원은 이에 맞지 않는다.

따라서 제70조의 내용이 아닌 것은 다·라의 2개이므로 ②이다.

NoteBase

문 37. 「전자서명법」 제21조(전자서명생성정보의 관리) 제4항의 내용 중 ( ) 안에 들어갈 단어로 바르게 짝지은 것은 무엇인가?

공인인증기관은 자신이 이용하는 전자서명(가)정보를 안전하게 보관·관리하여야 한다. 이 경우 당해 전자서명(나)정보가 분실·훼손 또는 도난·유출되거나 훼손될 수 있는 위험을 인지한 때에는 지체없이 그 사실을 (다)에(게) 통보하고 인증업무의 안전성과 신뢰성을 확보할 수 있는 대책을 마련하여야 한다.

① (가) 생성 (나) 생성 (다) 인터넷진흥원
② (가) 검증 (나) 생성 (다) 인터넷진흥원
③ (가) 생성 (나) 생성 (다) 이용자
④ (가) 생성 (나) 검증 (다) 이용자

정답 1번

간단한 해설

안전하게 보관하고 유출 위험에 대응해야 하는 대상은 **전자서명을 만드는 생성정보**이다. 당시 조문은 공인인증기관이 이 정보의 위험을 인지하면 **인터넷진흥원에 지체 없이 통보**하도록 규정하였다.

빈칸별 해설

지문은 구 「전자서명법」의 공인인증기관에 관한 규정이다. 공인인증기관이 자신이 사용하는 전자서명생성정보를 보호하고, 그 정보에 사고나 위험이 생기면 통보와 대책 마련을 하도록 한 내용을 묻는다.

(가) 생성: 전자서명생성정보는 **전자서명을 만드는 데 사용하는 정보**이며, 공개키 방식에서는 서명자의 개인키에 해당한다. 이 정보가 유출되면 타인이 그 기관을 가장하여 서명을 만들 위험이 있으므로 안전하게 보관·관리해야 한다. 서명이 유효한지 확인하는 데 쓰는 전자서명검증정보와 구별된다.

(나) 생성: 앞 문장에서 안전하게 보관·관리하도록 한 바로 그 **전자서명생성정보**를 다시 가리킨다. 그 정보의 분실·훼손·도난·유출 또는 훼손될 수 있는 위험을 인지한 경우에 후속 조치 의무가 생긴다. 두 번째 빈칸도 검증이 아니라 생성이다.

(다) 인터넷진흥원: 당시 제21조 제4항은 이러한 사실을 **지체 없이 인터넷진흥원에 통보**하고, 인증업무의 안전성과 신뢰성을 확보할 대책을 마련하도록 하였다. 따라서 이 조항에서 정한 통보 상대방은 이용자가 아니라 인터넷진흥원이다. 가입자 개인의 문제와 공인인증기관 자신의 생성정보에 관한 의무를 혼동하지 않아야 한다.

따라서 (가) 생성, (나) 생성, (다) 인터넷진흥원의 조합이므로 ①과 일치한다.

NoteBase

문 38. 다음 지문은 무엇에 관한 설명인가?

가. 자신에게 불리한 증거자료를 사전에 차단하려는 활동이나 기술
나. 데이터 복구 회피기법
다. 데이터 은닉(Steganography)

① Anti Forensic
② Digital Forensic
③ Root Kit
④ Stealth Scan

정답 1번

간단한 해설

지문의 공통 목적은 **증거의 발견·복구·분석을 어렵게 하는 것**이다. 이러한 활동과 기술을 포괄하는 개념이 안티 포렌식(Anti Forensic)이다.

NoteBase

핵심 풀이

안티 포렌식은 디지털 증거의 수집·복구·분석을 방해하거나 증거의 유용성을 떨어뜨리는 활동과 기술을 말한다. 특정 프로그램 하나의 이름이 아니라, **포렌식 조사를 어렵게 한다는 목적**으로 묶은 범주이다.

가. 불리한 증거자료를 사전에 차단하려는 활동: 증거가 남지 않게 하거나, 이미 남은 자료를 찾고 해석하기 어렵게 만드는 방향이다. 증거를 확보하여 사실관계를 밝히는 포렌식과 반대되는 목적이므로 안티 포렌식의 정의에 해당한다.

나. 데이터 복구 회피기법: 삭제되거나 제거된 자료를 조사자가 다시 확보하기 어렵게 만드는 접근이다. 복구를 통해 증거를 확보하는 절차를 방해하므로 안티 포렌식의 한 범주로 볼 수 있다.

다. 데이터 은닉(Steganography): 다른 데이터나 매체 안에 정보를 숨겨 그 정보의 존재를 알아보기 어렵게 하는 기술이다. 지문에서는 증거를 감추어 발견과 분석을 방해하는 용도로 제시되므로 안티 포렌식의 예에 해당한다. 다만 데이터 은닉 기술 자체의 모든 사용이 불법이거나 증거인멸인 것은 아니다.

Digital Forensic: 디지털 자료를 적절히 수집·보존하고 분석하여 사건의 사실관계를 확인하는 활동이다. 지문의 증거 확보 방해와는 목적이 반대이다.

Root Kit: 시스템에서 특정 기능이나 존재를 숨기거나 권한을 유지하는 데 쓰이는 도구 모음이다. 은닉 기능이 조사 방해에 활용될 수는 있지만, 가~다 전체의 활동을 포괄하는 상위 개념은 아니다.

Stealth Scan: 탐지를 피하거나 탐지 가능성을 줄이면서 시스템의 서비스·포트 등을 조사하려는 스캔 방식을 가리킨다. 정보 수집 과정의 은밀성에 관한 개념으로, 데이터 복구 회피와 증거 은닉 전반을 뜻하지 않는다.

따라서 세 내용을 포괄하는 것은 **Anti Forensic인 ①**이다.

NoteBase

문 39. 1998년 Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어인 엔케이스(EnCase) 고유의 포렌식 디스크 이미지 파일형식은 무엇인가?

① FTK

② dd

③ SHA

④ E01

정답 4번

간단한 해설

EnCase에서 디스크 증거를 파일로 보관하는 대표적인 형식은 **E01**이다. 획득한 디스크 데이터를 압축하거나 여러 파일로 나누어 저장하는 증거 이미지 형식이다.

개념 구분

E01은 EnCase에서 사용하는 포렌식 증거 이미지 파일 형식이다. 저장매체에서 획득한 데이터를 증거 이미지로 보관하며 압축과 분할 저장을 지원한다. 이 문제는 분석 프로그램 자체가 아니라 **증거 데이터를 담는 이미지 형식**을 묻는다.

FTK(Forensic Toolkit)는 디지털 증거를 분석하는 포렌식 소프트웨어의 이름이다. 도구가 어떤 이미지 형식을 지원하는지와 도구 자체의 이름은 구별해야 한다.

dd는 데이터를 복제하는 명령어이며, 포렌식에서는 보통 저장매체의 내용을 연속된 바이트로 복사한 원시 이미지와 관련해 쓰이는 명칭이다. EnCase의 E01 형식과는 다르다.

SHA(Secure Hash Algorithm)는 데이터의 해시값을 계산하는 알고리즘 계열이다. 증거의 변경 여부를 점검하는 데 사용할 수 있지만 디스크 이미지 파일 형식은 아니다.

따라서 EnCase의 증거 이미지 형식에 해당하는 것은 ④ E01이다.

NoteBase

문 40. 다음 지문에서 설명하는 디지털포렌식의 원칙은 무엇인가?

증거는 획득하고 난 뒤 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무결성의 원칙

정답 3번

간단한 해설

증거를 누가 취급하고 어디로 이송·보관했는지 **전 과정을 추적할 수 있게 기록**하는 것이 연계 보관성의 원칙이다. 증거 내용의 변경 여부를 확인하는 무결성과 구별해야 한다.

개념 구분

지문의 핵심은 증거를 획득한 뒤 이송·분석·보관·법정 제출에 이르는 **취급 이력을 이어서 추적할 수 있어야 한다**는 점이다. 이는 연계 보관성, 즉 Chain of Custody의 원칙이다.

① 정당성의 원칙은 증거의 수집과 분석 등이 적법하고 정당한 권한·절차에 따라 이루어져야 한다는 뜻이다. 누가 어떤 경로로 증거를 인계받았는지를 이어서 기록하는 원칙과는 구별된다.

② 재현의 원칙은 같은 증거에 대해 동일한 조건과 검증된 절차를 적용했을 때 분석 결과를 다시 확인할 수 있어야 한다는 뜻이다. 분석의 재현 가능성에 초점이 있다.

③ 연계 보관성의 원칙은 증거의 수집자와 취급자, 인계·인수 일시, 보관 장소, 이송 목적 등 관리 이력을 연결해 남기는 것이다. 이를 통해 획득한 증거가 어떤 과정을 거쳐 제출되었는지 확인할 수 있으므로 지문과 일치한다.

④ 무결성의 원칙은 증거의 내용이 임의로 변경되거나 훼손되지 않았음을 보장하는 것이다. 해시값 비교 등은 내용의 동일성을 확인하는 수단이지만, 그것만으로 모든 인계·보관 이력이 설명되는 것은 아니다.

따라서 지문에서 설명하는 원칙은 ③ 연계 보관성의 원칙이다.

NoteBase