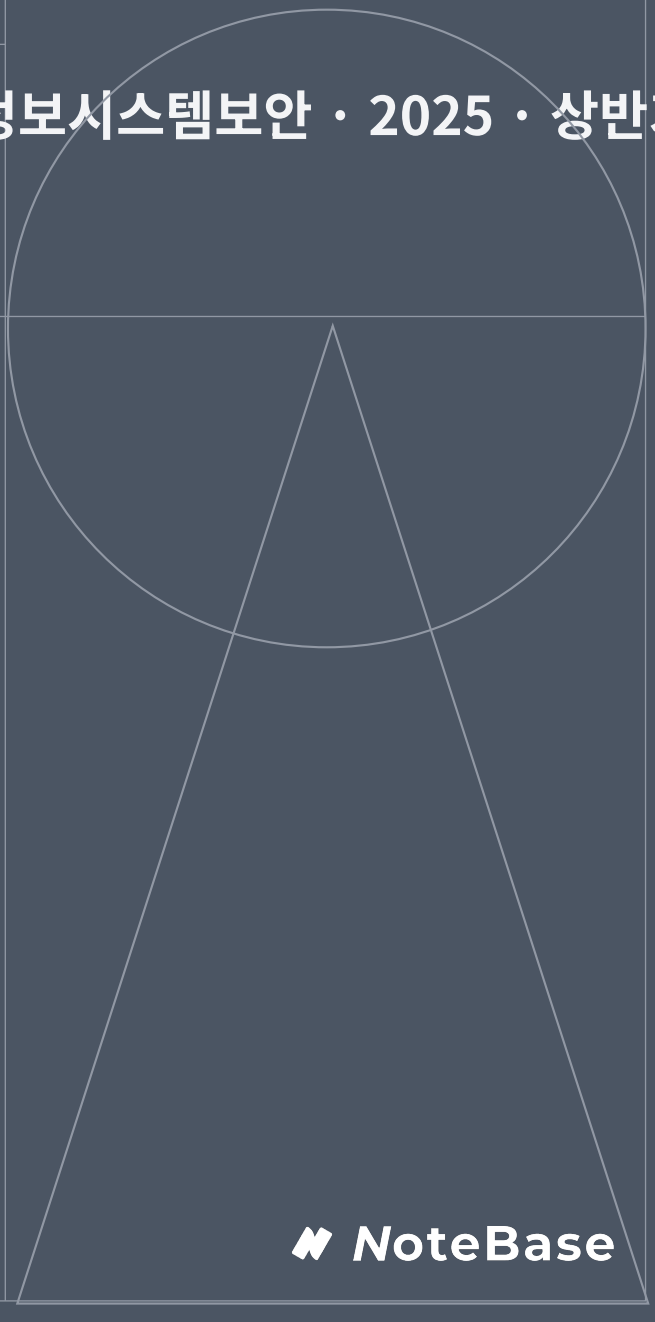
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2025 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2025 · 상반기

공무원/해경/일반직 9급 · 정보시스템보안 · 2025 · 상반기

문 1. 암호화에 대한 다음 설명 중 가장 옳지 않은 것은?

① 대칭 블록 암호화에서 한 블록의 크기는 일정 비트 길이로 설정된다.

② 대칭 블록 암호화에서 단위 블록의 크기가 커지면 보안성이 높아진다.

③ One-Time Pad의 키 크기는 64 또는 128비트 길이로 설정한다.

④ 스트림 암호에서 일부 암호문 비트가 손상되어도 에러 전파가 나타나지 않는다.

정답 3번

출제 포인트

블록 암호와 스트림 암호의 처리 방식, 그리고 One-Time Pad가 완전한 비밀성을 얻기 위한 키 조건을 구별하는 문제이다.

핵심 개념

블록 암호는 평문을 일정한 크기의 블록으로 나누어 암호화한다. 스트림 암호는 비트 또는 바이트 단위의 평문을 키 스트림과 결합해 순차적으로 암호화한다. One-Time Pad는 평문과 같은 길이의 진정한 난수 키를 단 한 번만 사용하는 암호 방식이다.

선지별 해설

① O — 대칭 블록 암호는 정해진 비트 길이의 블록을 단위로 평문을 처리하므로 한 블록의 크기는 일정하다.
② O — 블록 크기가 커지면 가능한 블록의 종류가 늘고 동일 블록의 반복이나 충돌이 나타날 가능성이 낮아져 일반적으로 암호 분석에 더 강해진다.
③ X — 틀린 표현은 '키 크기는 64 또는 128비트'이다. One-Time Pad의 키는 고정된 64비트나 128비트가 아니라 평문과 같은 길이여야 하며, 진정한 난수로 생성하여 한 번만 사용해야 한다.
④ O — 일반적인 동기식 스트림 암호에서는 암호문의 한 비트가 손상되면 복호화된 평문의 대응 비트만 잘못되고 이후 비트로 오류가 전파되지 않는다.

오답 포인트

③의 64비트와 128비트는 일반적인 블록 크기나 암호 키 길이와 혼동하게 만드는 표현이다. One-Time Pad를 판별하는 핵심은 고정 길이가 아니라 '평문과 같은 길이·진정한 난수·한 번만 사용'이다.

NoteBase

다시 나오면 이렇게 판단

블록 암호는 고정 크기 블록, 스트림 암호는 비트·바이트 단위 처리로 구분한다. One-Time Pad 선지에서는 키가 평문과 같은 길이인지, 무작위인지, 재사용하지 않는지를 차례로 확인한다.

암기 포인트

One-Time Pad의 키는 평문과 같은 길이의 난수이며 단 한 번만 사용한다.

NoteBase

문 2. 정보 보안 방법에 관한 다음 설명 중 가장 옳지 않은 것은?

① 핑거프린팅(Fingerprinting)은 디지털 콘텐츠에 판매자 정보를 삽입, 해당 콘텐츠의 판매량을 집계하기 위한 방법이다.

② 디지털 워터마킹(Digital Watermarking)은 디지털 콘텐츠에 저작정보를 추가, 권리정보를 포함하기 위한 방법이다.

③ 스테가노그래피(Steganography)는 콘텐츠에 전달하려는 정보를 은닉, 삽입하는 방법이다.

④ DRM(Digital Rights Management)은 콘텐츠의 사용에 대한 권한을 통제, 관리하기 위한 방법이다.

정답 1번

출제 포인트

디지털 콘텐츠 보호 기술인 핑거프린팅, 디지털 워터마킹, 스테가노그래피, DRM의 목적과 삽입 정보의 차이를 묻는 문제이다.

핵심 개념

핑거프린팅: 콘텐츠의 각 사본에 구매자·사용자 식별정보를 다르게 삽입하여 불법 유통이 발생했을 때 유출 경로를 추적하는 기술이다.
디지털 워터마킹: 콘텐츠에 저작권자·소유권 등의 권리정보를 삽입하여 권리를 표시하거나 진위를 확인하는 기술이다.
스테가노그래피: 전달할 비밀정보를 다른 콘텐츠 안에 숨겨 정보의 존재 자체를 알아보기 어렵게 하는 기술이다.
DRM: 디지털 콘텐츠의 접근, 이용, 복제, 배포 등의 권한을 통제하고 관리하는 기술이다.

선지별 해설

① X — 핑거프린팅에 삽입하는 핵심 정보는 '판매자 정보'가 아니라 사본을 받은 구매자·사용자의 식별정보이며, 목적도 '판매량 집계'가 아니라 불법 복제·유통 시 유출자를 식별하고 유통 경로를 추적하는 것이다. 올바르게는 '핑거프린팅은 디지털 콘텐츠에 구매자·사용자 식별정보를 삽입하여 불법 유통 경로를 추적하는 방법이다'라고 해야 한다.
② O — 디지털 워터마킹은 저작권자나 소유권 등 저작·권리정보를 콘텐츠에 삽입하여 권리 주장, 진위 확인, 불법 복제 방지 등에 활용하는 방법이다.
③ O — 스테가노그래피는 이미지·음성 등의 콘텐츠에 전달하려는 정보를 은닉하여 비밀정보가 존재한다는 사실 자체를 감추는 방법이다.
④ O — DRM은 허가된 사용자와 이용 조건에 따라 콘텐츠의 열람, 복제, 변경, 배포 등의 권한을 통제하고 관리하는 방법이다.

NoteBase

오답 포인트

①의 '판매자 정보'와 '판매량 집계'가 함정이다. 핑거프린팅은 판매 통계 기술이 아니라 구매자·사용자마다 다른 식별표지를 넣어 불법 유출의 책임 주체와 경로를 추적하는 기술이다.

다시 나오면 이렇게 판단

삽입 정보와 목적을 함께 본다. 사용자별 식별정보와 유출 추적이면 핑거프린팅, 저작권·소유권 표시이면 워터마킹, 비밀정보의 존재 은닉이면 스테가노그래피, 콘텐츠 이용 권한 통제이면 DRM으로 판단한다.

암기 포인트

핑거프린팅은 유출자 추적, 워터마킹은 권리 표시, 스테가노그래피는 정보 은닉, DRM은 이용 통제이다.

NoteBase

문 3. Shannon의 확산(Diffusion)과 혼돈(Confusion)에 대한 다음 <보기> 중 가장 옳은 내용을 모두 선택한 것은?

<보기>
㉠ 확산에 의하여 평문에서의 통계적 분포 성질이 암호문에도 보존된다.
㉡ 확산에 의하여 암호문에서의 통계적 분포 성질로 키값 추출이 어렵다.
㉢ 혼돈에 의하여 평문에서의 통계적 분포 성질이 암호문과 무관해진다.
㉣ 혼돈에 의하여 키값 1비트의 변화로도 암호문이 크게 달라진다.

① ㉠, ㉢
② ㉡
③ ㉡, ㉣
④ ㉣

정답 4번

출제 포인트

Shannon의 확산과 혼돈이 각각 평문의 통계적 특성과 키-암호문 관계를 어떻게 감추는지 구별하는 문제이다.

핵심 개념

확산(Diffusion): 평문의 한 비트가 여러 암호문 비트에 영향을 미치게 하여 평문의 통계적 특성이 암호문 전체에 퍼져 드러나지 않게 하는 성질이다. 키워드는 '평문 통계의 분산'이다.
혼돈(Confusion): 키와 암호문 사이의 관계를 복잡하고 비선형적으로 만들어 키를 추론하기 어렵게 하는 성질이다. 키의 작은 변화가 암호문을 크게 달라지게 하는 효과와 연결된다. 키워드는 '키 관계의 복잡화'이다.
따라서 확산은 평문과 암호문의 통계적 관계를 숨기고, 혼돈은 키와 암호문의 관계를 숨긴다.

NoteBase

선지별 해설

① X — ㉠과 ㉣은 모두 틀리다. ㉠의 '통계적 분포 성질이 암호문에도 보존된다'가 잘못되었으며, 확산은 그 통계적 성질이 암호문에 드러나지 않도록 분산시킨다. ㉣의 내용도 혼돈이 아니라 확산에 해당한다. 올바르게는 '혼돈은 키와 암호문 사이의 관계를 복잡하게 한다'이다.
② X — ㉡은 확산과 혼돈의 역할을 바꾸어 서술했다. '암호문의 통계적 분포 성질로 키값 추출이 어렵다'는 키와 암호문의 관계를 감추는 혼돈의 설명에 가깝다. 올바르게는 '확산은 평문의 통계적 특성이 암호문에 드러나지 않게 한다'이다.
③ X — ㉢은 옳지만 ㉡이 틀렸으므로 두 진술을 함께 고른 조합은 정답이 아니다. 올바른 조합은 ㉢만 포함한 것이다.
④ O — ㉢만 옳다. 혼돈은 키와 암호문의 관계를 복잡하게 하므로 키값 1비트의 변화만으로도 암호문이 크게 달라지는 성질과 연결된다.

오답 포인트

㉡과 ㉣은 확산과 혼돈의 대상을 서로 뒤바꾼 함정이다. '평문의 통계적 특성'은 확산, '키값 추론과 키-암호문 관계'는 혼돈에 대응한다. 또한 ㉠의 '보존된다'는 확산의 목적과 정반대이다.

다시 나오면 이렇게 판단

문장에 평문의 통계적 패턴을 넓게 퍼뜨린다는 내용이 나오면 확산으로 판단한다. 키와 암호문 사이의 대응을 복잡하게 하거나 키의 작은 변화가 암호문을 크게 바꾼다는 내용이 나오면 혼돈으로 판단한다.

암기 포인트

확산은 평문 통계를 흩뜨리고, 혼돈은 키와 암호문의 관계를 헷갈리게 한다.

NoteBase

문 4. 키의 대칭성에 관한 다음 설명 중 가장 옳지 않은 것은?

① 대칭키 암호화는 키의 전달 방법에 대한 보안성 유지 방안을 별도로 마련하여야 한다.

② 비대칭키 방법으로 상호간 양방향 원문 송수신이 필요할 때, 비대칭 복호화 키를 공유하고, 암호화 키를 공개하는 방법을 사용한다.

③ 대칭키 암호화는 비대칭키 암호화 방법에 비하여 처리 성능이 높다.

④ 상호간 통신 참여 구성원의 증가에 따라, 대칭키 암호화는 비대칭키 암호화에 비하여 키의 총 갯수가 점차 많아진다.

정답 2번

출제 포인트

대칭키 암호와 비대칭키 암호의 키 사용 방식, 키 관리 부담, 처리 성능의 차이를 묻는 문제이다.

핵심 개념

대칭키 암호: 암호화와 복호화에 같은 비밀키를 사용하는 방식이다. 속도가 빠르지만 통신 상대와 비밀키를 안전하게 공유해야 한다.
비대칭키 암호: 서로 수학적으로 연관된 공개키와 개인키를 사용하는 방식이다. 공개키는 배포할 수 있지만 개인키는 소유자만 보관하며 공유하지 않는다.
기밀성을 위한 전송에서는 수신자의 공개키로 암호화하고 수신자가 자신의 개인키로 복호화한다.

선지별 해설

① O — 대칭키는 송신자와 수신자가 동일한 비밀키를 사용하므로, 키가 노출되지 않도록 안전한 전달·분배 방법을 별도로 마련해야 한다.
② X — 틀린 표현은 '비대칭 복호화 키를 공유'한다는 부분이다. 복호화에 쓰는 개인키는 공유하지 않고 소유자만 보관한다. 양방향으로 기밀 통신하려면 각 참여자가 자신의 공개키만 상대에게 제공하고, 송신자는 수신자의 공개키로 암호화하며 수신자는 자신의 개인키로 복호화한다.
③ O — 대칭키 암호는 일반적으로 비대칭키 암호보다 연산이 단순하여 암호화·복호화 처리 속도가 빠르다.
④ O — 모든 참여자 쌍이 서로 다른 대칭키를 공유하면 참여자가 n명일 때 필요한 키는 $n(n-1)/2$개로 증가한다. 비대칭키 방식은 각 참여자가 자신의 키 쌍을 가지므로 참여자 수에 비례해 증가한다. 따라서 참여자가 많아질수록 대칭키 방식의 키 관리 부담이 더 빠르게 커진다.

오답 포인트

②는 공개키와 개인키의 역할을 뒤집어 개인키까지 공유한다고 표현한 것이 함정이다. '공개키는 공개, 개인키는 비공개'라는 원칙을 기준으로 판단한다.

NoteBase

다시 나오면 이렇게 판단

키를 공유한다는 설명에서는 먼저 키의 종류를 확인한다. 대칭키의 비밀키는 통신 당사자끼리 안전하게 공유하지만, 비대칭키의 공개키만 배포할 수 있고 개인키는 소유자만 보관한다. 성능은 대칭키가 빠르고, 참여자별 키 관리의 확장성은 비대칭키가 유리하다.

암기 포인트

대칭키는 같은 비밀키·빠른 처리·키 배송 문제, 비대칭키는 공개키 배포·개인키 비공개이다.

NoteBase

문 5. 다음 <보기>는 어떤 형태의 공격에 대하여 설명한 것인가?

<보기>
“A 직원이 큰 실수를 했습니다. 연말정산 시스템에 민감정보가 있어서 조심했어야 했는데, 관리 접근 암호를 집 현관문 비밀번호 숫자와 같게 한 모양입니다.
A 직원이 집을 내놓으면서 부동산에 비밀번호를 알려줬고, 해커가 부동산을 통해 번호를 알게 되었습니다.
개인정보가 외부로 유출되어 직원들이 불안해하고 있습니다.”

① 해커는 은닉 채널(Covert Channel)을 사용했다.
② 해커는 레인보우 테이블(Rainbow Table)을 사용했다.
③ 해커는 패스워드 솔트(Salt)를 사용했다.
④ 해커는 인간 기반 사회공학(Social Engineering)을 사용했다.

정답 4번

출제 포인트

이 문제는 공격자가 정보를 얻은 경로를 보고 인간 기반 사회공학 공격을 식별할 수 있는지를 묻는 문제이다.

사례 정리

핵심 사실 1: A 직원은 관리 접근 암호를 집 현관문 비밀번호와 같게 설정했다.
핵심 사실 2: A 직원은 집을 내놓으며 그 비밀번호를 부동산에 알려 주었고, 해커는 부동산을 통해 번호를 알아냈다.
판단에 중요한 조건: 해커가 암호 알고리즘이나 해시를 공격한 것이 아니라 사람 사이에 공유된 정보를 이용했다.

핵심 개념

인간 기반 사회공학은 사람의 신뢰, 부주의, 권한 또는 정보 공유 과정을 이용해 비밀번호 같은 보안 정보를 얻는 공격이다. 기술적 취약점을 직접 공략했는지가 아니라 사람을 정보 획득 경로로 삼았는지가 핵심이다.

적용 기준

공격자가 관리 접근 암호를 계산하거나 복호화한 것이 아니라, 직원이 제3자에게 알려 준 번호를 그 사람을 경유해 확보했다. 따라서 사람과 정보 공유 과정의 취약성을 이용한 인간 기반 사회공학에 해당한다.

NoteBase

선지별 해설

① X — '은닉 채널을 사용했다'는 표현이 틀렸다. 은닉 채널은 보안 정책이 허용하지 않은 비정상적 통신 경로를 이용해 정보를 전달하는 방식이다. 이 사례에는 그러한 통신 경로가 없으며, 올바르게는 사람을 통해 비밀번호를 알아낸 인간 기반 사회공학을 사용했다고 해야 한다.
② X — '레인보우 테이블을 사용했다'는 표현이 틀렸다. 레인보우 테이블은 미리 계산한 해시값과 원문 후보의 대응 관계를 이용해 패스워드를 찾는 기법이다. 이 사례에는 해시값 조회나 대조가 없으며, 올바르게는 인간 기반 사회공학을 사용했다고 해야 한다.
③ X — '패스워드 솔트를 사용했다'는 표현이 틀렸다. 솔트는 패스워드를 해시할 때 임의의 값을 함께 넣어 같은 패스워드도 서로 다른 해시값이 되게 하고 레인보우 테이블 공격을 어렵게 하는 방어 기법이다. 이 사례에서 해커가 사용한 공격 기법이 아니며, 올바르게는 인간 기반 사회공학을 사용했다고 해야 한다.
④ O — 해커는 기술적으로 암호를 해독하지 않고, 직원이 부동산에 공유한 현관문 비밀번호가 관리 접근 암호와 같다는 점을 이용해 사람을 경유하여 암호를 얻었다. 이는 인간 기반 사회공학이다.

오답 포인트

비밀번호가 등장한다는 이유만으로 레인보우 테이블이나 솔트를 고르면 안 된다. ②와 ③은 해시 처리와 관련된 용어이지만, 사례의 실제 정보 획득 경로는 부동산이라는 사람을 통한 경로이다.

다시 나오면 이렇게 판단

공격 사례에서는 먼저 공격자가 정보를 어떻게 얻었는지를 확인한다. 사람의 말·신뢰·부주의·정보 공유를 이용했다면 사회공학, 해시값을 미리 계산한 표와 대조했다면 레인보우 테이블, 허용되지 않은 통신 경로로 정보를 전달했다면 은닉 채널로 판단한다.

암기 포인트

사람을 경유해 비밀번호를 얻으면 인간 기반 사회공학이다. 솔트는 공격이 아니라 해시 보안을 강화하는 값이다.

NoteBase

문 6. OTP(One-Time Password) 기기를 이용한 패스워드 인증방식에서 다음 설명 중 가장 옳은 것은?

① 이벤트(계수기) 동기화 방식은 토큰장치가 네트워크에 연결되어 계수값을 서버에 전송한다.

② 시간 동기화 방식은 토큰장치가 네트워크에 연결되어 시간 정보를 전송한다.

③ 질의응답 방식은 서버에서 요구한 질의값을 토큰에 입력하고, 나타나는 응답값을 서버에 입력하여 검증한다.

④ FRR(False Rejection Rate)값으로 오인증을 관리한다.

정답 3번

출제 포인트

OTP 생성 방식인 이벤트 동기화, 시간 동기화, 질의응답 방식의 작동 원리와 생체인증 오류율 지표를 구별하는 문제이다.

핵심 개념

이벤트 동기화 방식은 토큰과 인증 서버가 공유하는 계수기 값을 바탕으로 OTP를 생성하는 방식이다. 시간 동기화 방식은 토큰과 서버가 공유하는 시각 정보를 바탕으로 OTP를 생성하는 방식이다. 질의응답 방식은 서버가 제시한 질의값을 토큰에 넣어 응답값을 생성하고, 서버가 이를 검증하는 방식이다. 이벤트 동기화와 시간 동기화에서는 토큰이 계수값이나 시간 정보를 서버로 직접 전송하는 것이 아니라 양쪽이 동기화된 값을 각각 이용한다.

선지별 해설

① X — 틀린 표현은 '토큰장치가 네트워크에 연결되어 계수값을 서버에 전송한다'이다. 실제로는 토큰과 서버가 미리 공유·동기화한 계수기 값을 각각 이용해 OTP를 생성하고 검증하며, 토큰이 계수값을 네트워크로 직접 전송하는 방식이 아니다.
② X — 틀린 표현은 '토큰장치가 네트워크에 연결되어 시간 정보를 전송한다'이다. 실제로는 토큰의 시계와 서버의 시각을 동기화하여 같은 시간 구간에서 생성되는 OTP를 검증하며, 토큰이 시간 정보를 서버로 직접 전송하지 않는다.
③ O — 서버가 제시한 질의값을 사용자가 토큰에 입력하고, 토큰이 만든 응답값을 다시 서버에 입력하여 검증하는 절차가 질의응답 방식에 해당한다.
④ X — 틀린 표현은 'FRR값으로 오인증을 관리한다'이다. FRR은 정당한 사용자를 잘못 거부하는 오거부율로서 생체인증 시스템의 오류율 지표이다. 타인을 정당한 사용자로 잘못 받아들이는 오류 지표는 FAR이며, FRR을 OTP 기기의 오인증 관리 방식으로 보는 것은 옳지 않다.

NoteBase

오답 포인트

①과 ②는 '동기화'를 토큰이 계수값이나 시간값을 서버에 실시간 전송한다는 뜻으로 바꾼 것이 함정이다. 동기화형 OTP는 토큰과 서버가 같은 계수기 또는 시간 기준으로 각자 값을 계산한다. ④는 생체인증의 오류율 지표인 FRR을 OTP 인증의 특성처럼 섞은 선택지이다.

다시 나오면 이렇게 판단

이벤트 동기화는 계수기, 시간 동기화는 시계, 질의응답은 서버의 질의값과 토큰의 응답값을 핵심 단서로 판단한다. 토큰이 동기화 정보를 네트워크로 직접 전송한다는 표현은 배제한다.

암기 포인트

이벤트는 횟수, 시간은 시각, 질의응답은 질의값을 넣고 응답값을 돌려준다. FRR·FAR는 생체인증 오류율 지표이다.

NoteBase

문 7. 생체인증에 관련한 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ 획득성(Collectability)은 대상 특성이 정량적으로 측정 가능한지를 의미한다.
㉡ 보편성(Universality)은 측정된 특성값이 각 개인마다 구분되게 나타나는지를 의미한다.
㉢ 수용성(Acceptability)은 시간에 따라 변화하지 않는 특성이 유지되는지를 의미한다.
㉣ 성능(Performance)은 환경변화와 무관하게 높은 정확성을 지속할 수 있는가를 의미한다.

① ㉠, ㉡
② ㉠, ㉣
③ ㉡, ㉢
④ ㉢, ㉣

정답 2번

출제 포인트

생체인증 특성의 평가 기준인 획득성, 보편성, 유일성, 영속성, 수용성, 성능의 의미를 구별하는 문제이다.

핵심 개념

획득성(Collectability)은 생체 특성을 센서 등으로 정량적으로 측정할 수 있는 정도이다.
보편성(Universality)은 모든 사람이 해당 생체 특성을 보유해야 한다는 뜻이고, 사람마다 서로 구별되는 정도는 유일성(Uniqueness)이다. 시간의 흐름에도 특성이 안정적으로 유지되는 정도는 영속성(Permanence)이며, 수용성(Acceptability)은 사용자가 해당 생체정보의 수집과 인증 방식에 거부감 없이 동의하는 정도이다.
성능(Performance)은 실제 환경에서 요구되는 인식 정확도와 처리 속도 등을 달성하는 정도이다. 따라서 ㉠과 ㉣이 옳고, ㉡과 ㉢이 틀리다.

선지별 해설

① X — ㉠은 옳지만 ㉡은 틀리다. ㉡의 '각 개인마다 구분되게 나타나는지'는 보편성이 아니라 유일성의 설명이다. 보편성은 모든 사람이 해당 생체 특성을 가지고 있다는 뜻이다. 따라서 올바른 조합은 ㉠, ㉣이다.
② O — ㉠의 획득성은 생체 특성의 정량적 측정 가능성을 뜻한다. ㉣의 성능은 환경 변화가 있더라도 높은 인식 정확도 등 요구되는 성능을 지속적으로 확보할 수 있는지를 뜻한다. 두 진술이 모두 옳다.
③ X — ㉡과 ㉢이 모두 틀리다. ㉡은 보편성이 아니라 유일성을 설명하고, ㉢의 '시간에 따라 변화하지 않는 특성이 유지되는지'는 수용성이 아니라 영속성의 설명이다. 올바른 조합은 ㉠, ㉣이다.
④ X — ㉣은 옳지만 ㉢은 틀리다. 수용성은 사용자가 생체정보의 수집과 인증 방식을 얼마나 받아들일 수 있는지를 의미하며, 시간에 따른 특성의 안정성은 영속성이다. 따라서 올바른 조합은 ㉠, ㉣이다.

NoteBase

오답 포인트

㉡은 ‘개인마다 구분’이라는 표현으로 유일성을 보편성처럼 바꾸었고, ㉢은 ‘시간에 따라 유지’라는 표현으로 영속성을 수용성처럼 바꾸었다. 서로 비슷해 보이는 평가 기준의 명칭을 뒤바꾼 것이 핵심 함정이다.

다시 나오면 이렇게 판단

모든 사람에게 있는지는 보편성, 사람마다 다른지는 유일성, 측정 가능한지는 획득성, 시간이 지나도 유지되는지는 영속성, 사용자가 받아들이는지는 수용성, 실제 인식 정확도와 처리 능력은 성능으로 구분한다.

암기 포인트

보편성은 모두 보유, 유일성은 서로 구별, 획득성은 측정 가능, 영속성은 시간에도 유지, 수용성은 사용자 수용, 성능은 정확도와 처리 능력이다.

NoteBase

문 8. 클라우드 컴퓨팅의 특징으로 가장 옳은 것은?

① 가상기계와 달리 컨테이너(Container) 기술은 호스트 운영체제(Host OS)를 공유하여 성능을 높인다.

② 클라우드의 가상기계는 구축형에 비해 고성능이다.

③ SecaaS(Security as a Service)는 클라우드 수준에서 제공하는 보안 서비스로, 가상기계의 운영체제에 설치하여 사용하여야 한다.

④ 클라우드는 처리 부하를 예상하여 필요한 자원을 정적으로 계획, 구성하여야 한다.

정답 1번

출제 포인트

가상기계와 컨테이너의 구조 차이, 클라우드 서비스의 성능 특성, SecaaS의 제공 방식, 클라우드의 탄력성을 구별하는 문제이다.

핵심 개념

가상기계는 하이퍼바이저 위에서 각각 별도의 게스트 운영체제를 실행하는 가상화 방식이다. 컨테이너는 호스트 운영체제의 커널을 공유하면서 응용 프로그램과 그 실행 환경을 격리하므로 가상기계보다 자원 오버헤드가 작다. 클라우드 컴퓨팅은 수요 변화에 맞추어 자원을 신속하고 탄력적으로 확장하거나 축소하며, SecaaS는 보안 기능을 클라우드 서비스 형태로 제공하는 방식이다.

선지별 해설

① O — 컨테이너는 각 인스턴스마다 별도의 게스트 운영체제를 두는 가상기계와 달리 호스트 운영체제의 커널을 공유한다. 따라서 운영체제 중복에 따른 오버헤드가 줄어 자원 효율과 실행 성능을 높일 수 있다.
② X — 틀린 표현은 '클라우드의 가상기계는 구축형에 비해 고성능이다'이다. 클라우드 가상기계가 온프레미스 구축형 시스템보다 본질적으로 고성능인 것은 아니며, 실제 성능은 할당된 CPU·메모리·스토리지, 가상화 오버헤드, 네트워크 환경 등에 따라 달라진다.
③ X — 틀린 표현은 '가상기계의 운영체제에 설치하여 사용하여야 한다'이다. SecaaS는 보안 기능을 클라우드 기반 서비스로 제공하는 모델이므로 반드시 각 가상기계의 운영체제에 설치해야 하는 것은 아니며, 웹·API·네트워크 연계 등의 방식으로 이용할 수 있다.
④ X — 틀린 표현은 '필요한 자원을 정적으로 계획, 구성하여야 한다'이다. 클라우드는 처리 부하의 변화에 따라 자원을 동적으로 확장하거나 축소하는 탄력성과 신속한 자원 제공을 특징으로 한다.

오답 포인트

②는 클라우드의 확장성과 자원 선택 폭을 개별 가상기계의 절대적인 고성능으로 바꾼 함정이다. ③은 서비스로 제공되는 보안 기능을 로컬 설치형 보안 소프트웨어와 혼동하게 하며, ④는 클라우드의 핵심인 동적 탄력성을 정적 용량 계획으로 뒤집는다.

NoteBase

다시 나오면 이렇게 판단

가상기계와 컨테이너는 '게스트 운영체제를 각각 두는가, 호스트 커널을 공유하는가'로 구별한다. 클라우드 관련 선지는 특정 환경의 절대적 고성능을 주장하는지, 서비스를 반드시 로컬에 설치한다고 단정하는지, 자원을 정적으로만 구성한다고 하는지를 확인한다.

암기 포인트

가상기계는 게스트 OS별 실행, 컨테이너는 호스트 커널 공유, 클라우드는 동적 탄력성, SecaaS는 보안의 서비스화이다.

NoteBase

문 9. TPM(Trusted Platform Module)에 관련된 내용으로 가장 옳지 않은 것은?

① 운영체제의 부팅이 완료된 후 응용 프로그램의 실행을 제한한다.

② 물리적인 컴퓨터 도난으로부터 데이터의 보안을 제공한다.

③ 암호화 키의 생성과 저장, 패스워드 저장, 무결성 검증 측정값의 저장, 인증서 관련 신뢰 연산 제공을 포함한다.

④ 신뢰 컴퓨팅(Trusted Computing)을 위한 핵심 요소로써 하드웨어/소프트웨어로 구성된 TPM을 필요로 한다.

정답 1번

출제 포인트

TPM의 핵심 역할인 신뢰 기반 제공·암호 키 보호·부팅 무결성 측정과 운영체제 또는 응용 프로그램이 담당하는 실행 통제를 구별하는 문제이다.

핵심 개념

TPM은 암호 키와 인증 정보 등을 안전하게 보호하고, 시스템 구성요소의 무결성 측정값을 저장하여 플랫폼이 신뢰할 수 있는 상태인지 검증하도록 돕는 보안 모듈이다. TPM은 측정과 보호의 신뢰 기반을 제공하지만, 운영체제 부팅 후 어떤 응용 프로그램의 실행을 허용하거나 차단하는 정책을 직접 집행하는 장치는 아니다.

선지별 해설

① X — '운영체제의 부팅이 완료된 후 응용 프로그램의 실행을 제한한다'는 부분이 틀렸다. 응용 프로그램 실행 제한은 운영체제의 접근 통제나 응용 프로그램 허용 목록 같은 실행 통제 기능이 담당한다. 올바르게는 TPM은 부팅 과정의 구성요소를 측정하고 그 값을 안전하게 보관하여 플랫폼 무결성 검증을 지원한다고 해야 한다.
② O — TPM에 결합하여 보호한 암호 키는 장치의 신뢰 상태가 충족될 때만 사용되도록 구성할 수 있다. 따라서 컴퓨터가 도난당해 저장장치만 분리되더라도 암호화된 데이터의 복호화를 어렵게 하여 데이터 보호에 기여한다.
③ O — TPM은 암호 키의 생성·보호·저장, 인증 정보의 보호, 플랫폼 무결성 측정값의 저장, 인증서와 관련된 신뢰 연산을 지원한다. 이는 TPM의 대표적인 보안 기능이다.
④ O — 신뢰 컴퓨팅은 TPM이 제공하는 하드웨어 기반 또는 펌웨어 기반의 신뢰점과 이를 이용하는 소프트웨어가 함께 작동하는 구조이다. TPM은 측정값과 키를 보호하는 핵심 신뢰 기반으로 사용된다.

오답 포인트

①은 TPM이 부팅 무결성 측정을 지원한다는 사실을 '부팅 후 응용 프로그램 실행을 직접 제한한다'는 기능으로 바꾸어 놓았다. 무결성 측정·키 보호와 실행 허용·차단은 서로 다른 기능이다.

NoteBase

다시 나오면 이렇게 판단

선지의 동사가 '측정한다·저장한다·키를 보호한다·신뢰 연산을 제공한다'이면 TPM의 기능에 가깝다. '응용 프로그램 실행을 직접 허용하거나 차단한다'이면 운영체제나 별도의 실행 통제 기능에 가깝다.

암기 포인트

TPM은 키 보호와 부팅 무결성 측정의 신뢰 기반이며, 부팅 후 프로그램 실행을 직접 통제하는 기능은 아니다.

NoteBase

문 10. 다음 <보기>는 정보보호의 목표이다. 가장 올바르게 짝지어진 것은?

<보기>
㉠ 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질.
㉡ 오직 인가된 사람, 인가된 프로세스, 인가된 시스템만이 접근해야 한다는 원칙.
㉢ 정당한 사용자가 정보시스템의 데이터 또는 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질.

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

정답 3번

출제 포인트

정보보호의 3대 목표인 무결성·기밀성·가용성의 정의를 구별하여 ㉠~㉢에 대응시키는 문제이다.

핵심 개념

무결성: 정보가 인가되지 않은 방식으로 생성·변경·삭제되지 않고 정확하고 완전한 상태를 유지하는 성질이다. 키워드는 변조·훼손 방지이다.
기밀성: 정보가 인가된 사람·프로세스·시스템에만 공개되고 접근이 허용되는 성질이다. 키워드는 비인가 접근·노출 방지이다.
가용성: 인가된 사용자가 필요할 때 정보와 자원을 지체 없이 사용할 수 있는 성질이다. 키워드는 필요할 때 사용 가능이다.
따라서 ㉠은 무결성, ㉡은 기밀성, ㉢은 가용성이다.

NoteBase

선지별 해설

① X
㉠의 '기밀성'과 ㉡의 '인증성'이 틀렸다. 불법적인 생성·변경·삭제를 막는 ㉠은 무결성이고, 인가된 주체만 접근하게 하는 ㉡은 기밀성이다. ㉢의 가용성만 옳다. 올바른 짝은 '㉠ 무결성, ㉡ 기밀성, ㉢ 가용성'이다.

② X
㉠·㉡·㉢의 대응이 모두 틀렸다. ㉠은 기밀성이 아니라 무결성, ㉡은 가용성이 아니라 기밀성, ㉢은 인증성이 아니라 가용성이다. 올바른 짝은 '㉠ 무결성, ㉡ 기밀성, ㉢ 가용성'이다.

③ O
㉠은 정보의 불법적인 생성·변경·삭제를 방지하므로 무결성이고, ㉡은 인가된 주체만 접근하도록 하므로 기밀성이며, ㉢은 정당한 사용자가 필요할 때 자원을 사용할 수 있게 하므로 가용성이다. 세 대응이 모두 옳다.

④ X
㉠의 무결성은 옳지만 ㉡의 '가용성'과 ㉢의 '기밀성'이 서로 바뀌었다. 인가된 주체만 접근하는 ㉡은 기밀성이고, 필요할 때 사용할 수 있는 ㉢은 가용성이다. 올바른 짝은 '㉠ 무결성, ㉡ 기밀성, ㉢ 가용성'이다.

오답 포인트

'인가된 사람만 접근'이라는 표현을 사용자 신원을 확인하는 인증성과 혼동하기 쉽다. 이 문장에서는 정보의 접근·노출 대상을 인가된 주체로 제한하는 목표를 묻고 있으므로 기밀성이다. 또한 '변경·삭제 방지'는 무결성, '필요할 때 사용'은 가용성으로 구별한다.

다시 나오면 이렇게 판단

변조·삭제·정확성은 무결성, 비인가 접근·노출 제한은 기밀성, 필요 시 접근·서비스 지속은 가용성으로 판단한다. 인증성은 접근하려는 주체나 정보의 출처가 진짜인지 확인하는 개념이므로 기밀성과 구별한다.

암기 포인트

변경 방지는 무결성, 공개 제한은 기밀성, 사용 보장은 가용성이다.

NoteBase

문 11. 다음 <보기> 설명에 해당하는 유형의 바이러스를 가장 옳게 짝지은 것은?

<보기>
㉠ 바이러스가 랜덤 암호화키를 생성하고 스스로 암호화한다.
㉡ 안티 바이러스 소프트웨어에 의해 탐지되지 않기 위해 자신을 감추도록 설계된 바이러스를 말한다.
㉢ 감염시킬 때마다 변형되므로 특징을 이용한 탐지가 불가능해진다.
㉣ 감염시킬 때마다 형태뿐만 아니라 행동 패턴까지 변화가 일어난다.

① ㉠: 폴리모픽 바이러스, ㉡: 메타모픽 바이러스, ㉢: 스텔스 바이러스, ㉣: 암호화된 바이러스
② ㉠: 폴리모픽 바이러스, ㉡: 암호화된 바이러스, ㉢: 메타모픽 바이러스, ㉣: 스텔스 바이러스
③ ㉠: 암호화된 바이러스, ㉡: 스텔스 바이러스, ㉢: 폴리모픽 바이러스, ㉣: 메타모픽 바이러스
④ ㉠: 암호화된 바이러스, ㉡: 스텔스 바이러스, ㉢: 메타모픽 바이러스, ㉣: 폴리모픽 바이러스

정답 3번

출제 포인트

이 문제는 암호화된 바이러스, 스텔스 바이러스, 폴리모픽 바이러스, 메타모픽 바이러스를 은폐·변형 방식에 따라 구별하는 문제이다.

핵심 개념

암호화된 바이러스는 랜덤 암호화키 등으로 바이러스 본체를 암호화하여 정적 형태를 감추는 바이러스이다.
스텔스 바이러스는 감염 사실이나 자신의 존재가 보안 프로그램에 드러나지 않도록 시스템 정보를 조작하거나 동작을 숨기는 바이러스이다.
폴리모픽 바이러스는 감염할 때마다 암호화키나 복호화 코드 등의 외형적 특징을 바꾸어 동일한 시그니처로 탐지하기 어렵게 하는 바이러스이다.
메타모픽 바이러스는 감염할 때마다 자신의 코드 구조를 재작성하여 형태뿐 아니라 명령 구성과 행동 패턴까지 달라지게 하는 바이러스이다.

NoteBase

선지별 해설

① X — ㉠을 폴리모픽 바이러스, ㉡을 메타모픽 바이러스, ㉢을 스텔스 바이러스, ㉣을 암호화된 바이러스로 연결한 부분이 모두 잘못되었다. 올바르게는 ㉠ 암호화된 바이러스, ㉡ 스텔스 바이러스, ㉢ 폴리모픽 바이러스, ㉣ 메타모픽 바이러스이다.
② X — ㉠을 폴리모픽 바이러스, ㉡을 암호화된 바이러스, ㉢을 메타모픽 바이러스, ㉣을 스텔스 바이러스로 연결한 부분이 잘못되었다. 랜덤 키로 스스로 암호화하는 ㉠은 암호화된 바이러스이고, 탐지를 피하려고 자신을 숨기는 ㉡은 스텔스 바이러스이며, 감염 때마다 변형되는 ㉢은 폴리모픽 바이러스, 형태와 행동 패턴까지 바뀌는 ㉣은 메타모픽 바이러스이다.
③ O — ㉠의 랜덤 키를 이용한 자기 암호화는 암호화된 바이러스, ㉡의 탐지 회피를 위한 은폐는 스텔스 바이러스, ㉢의 감염 때마다 이루어지는 변형은 폴리모픽 바이러스, ㉣의 형태와 행동 패턴 변화는 메타모픽 바이러스의 특징이다.
④ X — ㉠과 ㉡은 맞지만, ㉢을 메타모픽 바이러스, ㉣을 폴리모픽 바이러스로 연결한 부분이 뒤바뀌었다. 올바르게는 감염 때마다 외형적 특징이 변하는 ㉢이 폴리모픽 바이러스이고, 코드 구조와 행동 패턴까지 변하는 ㉣이 메타모픽 바이러스이다.

오답 포인트

폴리모픽과 메타모픽은 모두 감염할 때마다 모습이 달라진다는 점 때문에 혼동하기 쉽다. ㉣의 '형태뿐만 아니라 행동 패턴까지'라는 표현은 더 근본적으로 코드를 재작성하는 메타모픽 바이러스를 가리키는 결정적 단서이다.

다시 나오면 이렇게 판단

'암호화키 생성·자기 암호화'는 암호화된 바이러스, '탐지 회피를 위한 은폐'는 스텔스 바이러스, '감염 때마다 외형 변형'은 폴리모픽 바이러스, '코드 구조와 행동 패턴까지 변화'는 메타모픽 바이러스로 판단한다.

암기 포인트

암호화는 키, 스텔스는 숨김, 폴리모픽은 외형 변화, 메타모픽은 코드와 행동까지 재구성이다.

NoteBase

문 12. 윈도우즈 시스템이 동작하기 위한 프로세스와 그에 대한 설명으로 가장 옳지 않은 것은?

① mstask.exe - 사용자가 미리 지정한 시간에 작업을 실행시키는 스케줄을 담당.

② svchost.exe - DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스.

③ lsass.exe - 윈도우 운영체제 내에서의 보안 정책의 시행을 담당하며 시스템에 접근하려는 모든 사용자를 체크.

④ smss.exe - 윈도우 콘솔을 관장하고, 스레드를 생성/삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스.

정답 4번

출제 포인트

윈도우 핵심 프로세스의 이름과 역할을 정확히 연결하는 문제이다. 특히 smss.exe와 csrss.exe의 역할을 구별해야 한다.

핵심 개념

mstask.exe는 예약된 작업을 지정 시각에 실행하도록 관리하는 작업 스케줄러 관련 프로세스이다.
svchost.exe는 DLL 형태로 구현된 윈도우 서비스를 불러와 실행하는 공용 호스트 프로세스이다.
lsass.exe는 로컬 보안 정책의 시행과 사용자 인증 등 시스템 보안을 담당하는 프로세스이다.
smss.exe는 시스템 시작 단계에서 세션을 초기화하고 csrss.exe와 winlogon.exe 같은 핵심 프로세스의 구동을 준비하는 세션 관리자 프로세스이다.

선지별 해설

① O — mstask.exe는 사용자가 미리 설정한 시각에 예약 작업이 실행되도록 관리하는 작업 스케줄러 관련 프로세스이므로 옳다.
② O — svchost.exe는 DLL 형태로 구현된 여러 윈도우 서비스가 동작할 수 있도록 실행 환경을 제공하는 공용 호스트 프로세스이므로 옳다.
③ O — lsass.exe는 로컬 보안 정책을 시행하고 사용자의 로그온 인증과 접근 권한 확인을 담당하므로 옳다.
④ X — 틀린 부분은 smss.exe가 윈도우 콘솔을 관장하고 스레드의 생성·삭제 및 32비트 가상 MS-DOS 환경을 지원한다는 설명이다. 이 역할은 csrss.exe에 관한 설명이며, smss.exe는 시스템 세션을 초기화하고 csrss.exe와 winlogon.exe 등의 시작을 준비하는 세션 관리자 프로세스이다.

오답 포인트

④는 실제 윈도우 핵심 프로세스의 기능을 제시하되 그 이름만 smss.exe로 바꾼 선지이다. 콘솔과 스레드 관리, 가상 MS-DOS 환경 지원은 csrss.exe의 역할이고, smss.exe의 핵심어는 세션 초기화이다.

NoteBase

다시 나오면 이렇게 판단

프로세스 이름을 역할의 핵심어와 연결한다. 예약 작업은 mstask.exe, DLL 기반 서비스의 호스팅은 svchost.exe, 보안 정책과 인증은 lsass.exe, 세션 초기화는 smss.exe, 콘솔과 스레드 관리는 csrss.exe로 구분한다.

암기 포인트

mstask는 예약 작업, svchost는 서비스 호스트, lsass는 보안·인증, smss는 세션 시작, csrss는 콘솔·스레드이다.

NoteBase

문 13. 다음 <보기>의 ㉠, ㉡에 들어갈 말로 가장 옳은 것은?

<보기>
두 프로세스 간에 자원을 사용하기 위해서 경쟁하는 것을 이용한 공격은 ㉠이라 하고, 시스템 프로그램과 공격 프로그램을 경쟁 상태에 이르게 하여 시스템 프로그램 권한으로 ㉡가 Root로 설정된 파일에 접근을 가능하게 하는 방법을 말한다.

① ㉠: 힙 오버플로우 공격, ㉡: SetGID
② ㉠: 레이스 컨디션 공격, ㉡: SetUID
③ ㉠: 스택 오버플로우 공격, ㉡: Finger
④ ㉠: 코드 기반 공격, ㉡: Shadow

정답 2번

출제 포인트

두 프로세스의 실행 순서와 자원 경쟁을 악용하는 레이스 컨디션 공격과, 파일 소유자의 권한으로 프로그램을 실행하게 하는 SetUID를 연결하는 문제이다.

핵심 개념

레이스 컨디션 공격은 여러 프로세스가 같은 자원에 접근하는 시점이나 실행 순서의 틈을 악용하여 비정상적인 결과를 만드는 공격이다. 특히 검사 시점과 사용 시점 사이에 대상이 바뀌는 TOCTOU가 대표적이다.
SetUID는 실행 파일을 실행한 사용자가 그 파일 소유자의 유효 사용자 ID 권한을 갖게 하는 특수 권한이다.
따라서 Root 소유 실행 파일에 SetUID가 설정되어 있으면 프로그램은 Root 권한으로 동작할 수 있다.
SetGID는 파일 소유자의 사용자 권한이 아니라 파일 소유 그룹의 유효 그룹 ID 권한을 부여한다.

NoteBase

선지별 해설

① X — '힙 오버플로우 공격'은 힙 메모리 영역의 경계를 넘는 쓰기를 악용하는 공격이므로 자원 경쟁을 이용한다는 ㉠의 설명과 맞지 않는다. 또한 SetGID는 그룹 권한을 부여한다. 올바르게는 ㉠은 레이스 컨디션 공격, ㉡은 SetUID이다.
② O — 자원 사용의 경쟁 상태를 악용하는 것은 레이스 컨디션 공격이고, Root 소유 파일의 권한으로 실행되게 하는 특수 권한은 SetUID이므로 두 대응이 모두 옳다.
③ X — '스택 오버플로우 공격'은 스택의 버퍼 경계를 넘는 입력으로 실행 흐름 등을 훼손하는 공격이며, Finger는 사용자 정보를 조회하는 명령 또는 프로토콜이지 특수 실행 권한이 아니다. 올바르게는 ㉠은 레이스 컨디션 공격, ㉡은 SetUID이다.
④ X — '코드 기반 공격'은 자원 경쟁을 악용하는 공격의 정확한 명칭이 아니며, Shadow는 일반 사용자의 비밀번호 해시 접근을 제한하기 위한 파일 체계를 가리킬 뿐 실행 파일에 Root 소유자 권한을 부여하는 기능이 아니다. 올바르게는 ㉠은 레이스 컨디션 공격, ㉡은 SetUID이다.

오답 포인트

'경쟁'이라는 표현을 메모리 영역 공격과 혼동하거나 SetUID와 SetGID를 바꾸어 고르는 것이 함정이다. 사용자 권한은 UID, 그룹 권한은 GID로 구분해야 한다.

다시 나오면 이렇게 판단

동시 실행·공유 자원·실행 시점의 틈이 제시되면 레이스 컨디션을 먼저 판단한다. 이어서 파일 소유자의 사용자 권한으로 실행되면 SetUID, 파일 소유 그룹의 권한으로 실행되면 SetGID로 구분한다.

암기 포인트

경쟁 상태는 Race Condition, Root 소유자의 권한 실행은 SetUID이다.

NoteBase

문 14. FTP(File Transfer Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① FTP 모드에는 Active와 Passive 모드가 있다.

② TCP 포트 20은 제어 연결을 위해, 21은 데이터 연결을 위해 사용된다.

③ Passive 모드에서 데이터 전송을 하기 위해서는 1024번 이상의 포트를 사용한다.

④ 클라이언트는 FTP를 이용하여 서버의 파일을 읽고 저장할 수 있을 뿐만 아니라 파일목록을 볼 수도 있다.

정답 2번

출제 포인트

FTP가 제어 연결과 데이터 연결을 분리해 사용하는 방식, 그리고 Active 모드와 Passive 모드에서 데이터 연결을 만드는 주체와 포트를 구별하는 문제이다.

핵심 개념

FTP는 파일 전송을 위해 제어 연결과 데이터 연결을 별도로 사용하는 응용 계층 프로토콜이다. 제어 연결은 서버의 TCP 21번 포트를 사용한다. Active 모드에서는 서버가 일반적으로 TCP 20번 포트에서 클라이언트 쪽으로 데이터 연결을 시작하고, Passive 모드에서는 서버가 제시한 1024번 이상의 포트로 클라이언트가 데이터 연결을 시작한다.

선지별 해설

① O — FTP에는 데이터 연결 방식에 따라 Active 모드와 Passive 모드가 있다.
② X — '20은 제어 연결, 21은 데이터 연결'이라는 부분이 서로 뒤바뀌었다. 올바르게는 TCP 21번 포트가 제어 연결에 사용되고, Active 모드의 데이터 연결에는 서버 측 TCP 20번 포트가 사용된다.
③ O — Passive 모드에서는 서버가 1024번 이상의 포트를 열어 알리고, 클라이언트가 그 포트로 데이터 연결을 시작한다.
④ O — FTP 클라이언트는 서버에 있는 파일을 내려받거나 서버에 파일을 올릴 수 있으며, 디렉터리의 파일 목록도 조회할 수 있다.

오답 포인트

②는 FTP의 대표 포트 번호 20과 21을 알고 있어도 각각의 역할을 반대로 연결하게 만드는 선지이다. 특히 20번 포트는 모든 FTP 연결의 고정 데이터 포트가 아니라 Active 모드에서 서버 측 데이터 연결에 사용된다는 점도 함께 구별해야 한다.

다시 나오면 이렇게 판단

먼저 '21번은 제어 연결'로 고정한 뒤 데이터 연결 방향을 구분한다. Active 모드는 서버가 클라이언트로 연결을 시작하고, Passive 모드는 클라이언트가 서버가 알려 준 높은 번호의 포트로 연결을 시작한다.

NoteBase

암기 포인트

FTP 21번은 제어, Active의 20번은 데이터, Passive는 서버가 알려 준 높은 포트로 클라이언트가 접속한다.

NoteBase

문 15. CSRF(Cross Site Request Forgery)의 특징에 대한 설명으로 가장 옳지 않은 것은?

① 사이트에 방문하는 사용자가 정상적인 요청이 아닌 임의의 요청을 하도록 위조하는 방법이다.

② 특정 웹사이트가 사용자의 웹브라우저를 신용하는 상태를 악용하는 방법이다.

③ 기본적으로 XSS 공격과 마찬가지로 웹브라우저를 이용한 공격의 일종이다.

④ 악성 스크립트를 웹게시판에 등록하여 이를 웹페이지 방문자의 브라우저 내에서 적절한 검증 없이 실행되도록 한다.

정답 4번

출제 포인트

이 문제는 인증된 사용자의 권한을 악용해 원하지 않는 요청을 보내게 하는 CSRF와, 악성 스크립트를 피해자의 브라우저에서 실행하는 XSS의 차이를 묻는다.

핵심 개념

CSRF는 사용자가 특정 웹사이트에 로그인해 인증된 상태임을 악용하여, 공격자가 의도한 요청을 사용자의 브라우저가 해당 사이트로 보내게 하는 공격이다.
XSS는 웹페이지에 삽입된 악성 스크립트가 방문자의 브라우저에서 실행되게 하는 공격이다.
CSRF의 핵심은 '사용자 권한으로 위조된 요청 전송'이고, XSS의 핵심은 '브라우저에서 악성 스크립트 실행'이다.

NoteBase

선지별 해설

① O
CSRF는 공격자가 인증된 사용자의 브라우저를 통해 사용자가 의도하지 않은 임의의 요청을 대상 사이트에 보내게 하는 요청 위조 공격이다.

② O
대상 웹사이트가 로그인된 사용자의 브라우저에서 온 요청을 정당한 요청으로 신뢰하고 처리하는 상태를 악용한다. 브라우저가 세션 쿠키 등 인증 정보를 요청에 함께 보내는 점이 공격 성립의 기반이 된다.

③ O
CSRF와 XSS는 모두 웹브라우저를 매개로 피해자 측에서 공격 효과가 발생하는 웹 공격이다. 다만 CSRF는 위조 요청을 보내는 데 초점이 있고, XSS는 악성 스크립트를 실행하는 데 초점이 있다.

④ X
틀린 표현은 '악성 스크립트를 웹게시판에 등록하여 웹페이지 방문자의 브라우저에서 실행'한다는 부분이다. 이는 저장형 XSS의 설명이다. 올바르게는 CSRF는 인증된 사용자가 의도하지 않은 요청을 공격 대상 웹사이트로 전송하게 하여 그 사용자의 권한으로 처리되도록 하는 공격이다.

오답 포인트

④는 웹브라우저를 이용한다는 공통점 때문에 CSRF처럼 보이지만, '게시판에 악성 스크립트 등록'과 '방문자 브라우저에서 스크립트 실행'은 저장형 XSS를 가리키는 결정적 표현이다.

다시 나오면 이렇게 판단

선지에 '로그인 상태·인증 정보·사용자가 원하지 않은 요청'이 나오면 CSRF를, '악성 스크립트 삽입·브라우저에서 스크립트 실행'이 나오면 XSS를 판단한다.

암기 포인트

CSRF는 권한을 빌려 요청을 위조하고, XSS는 페이지에 심은 스크립트를 실행한다.

NoteBase

문 16. 「개인정보 보호법」상 개인정보 분쟁조정위원회에 대한 설명으로 가장 옳지 않은 것은?

① 위원장과 위촉위원의 임기는 2년으로 하되 1차에 한하여 연임할 수 있다.

② 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 국무총리령으로 정한다.

③ 개인정보에 대한 분쟁을 위하여 개인정보 분쟁조정위원회를 둔다.

④ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

정답 2번

쟁점

이 문제는 「개인정보 보호법」상 개인정보 분쟁조정위원회의 설치 목적, 위원의 임기, 의결정족수 및 운영에 관한 위임 형식을 구별하는 문제이다.

용어 풀이

의결정족수는 위원회가 회의를 열고 안건을 의결하는 데 필요한 출석 인원과 찬성 인원의 기준이다.

핵심 구분

「개인정보 보호법」 제40조는 개인정보에 관한 분쟁의 조정을 위하여 개인정보 분쟁조정위원회를 두고, 위원장과 위촉위원의 임기를 2년으로 하되 1차에 한하여 연임할 수 있도록 한다. 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결한다. 법에서 정하지 않은 위원회 운영 사항을 정하는 형식은 국무총리령이 아니라 대통령령이다.

선지별 해설

① O — 위원장과 위촉위원의 임기는 2년이며, 1차에 한하여 연임할 수 있으므로 옳다.
② X — 분쟁조정위원회 운영에 필요한 사항을 정하는 위임 형식을 '국무총리령'이라고 한 부분이 틀렸다. 틀린 표현: 국무총리령으로 정한다. 올바른 표현: 대통령령으로 정한다.
③ O — 개인정보에 관한 분쟁의 조정을 위하여 개인정보 분쟁조정위원회를 두므로 옳다.
④ O — 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결하므로 옳다.

오답 포인트

②의 '국무총리령'은 법률의 위임 형식을 바꾸어 놓은 함정이다. 설치 목적·임기·의결정족수보다 대통령령과 국무총리령의 구별을 정확히 확인해야 한다.

다시 나오면 이렇게 판단

위원회 관련 법령 문제에서는 설치 목적, 임기, 회의 정족수, 세부 운영사항의 위임 형식을 각각 분리하여 확인한다. 이 위원회의 세부 운영사항은 대통령령으로 정한다는 점으로 ②를 배제한다.

NoteBase

암기 포인트

분쟁조정위원회는 임기 2년·1차 연임, 재적 과반 출석·출석 과반 찬성, 운영은 대통령령이다.

NoteBase

문 17. AES(Advanced Encryption Standard) 암호화 라운드 수행시 마지막 라운드를 제외한 각 라운드 수행의 4단계 처리 순서로 가장 옳은 것은?

① Substitute bytes → Add round key → Mix columns → Shift rows

② Substitute bytes → Shift rows → Mix columns → Add round key

③ Mix columns → Add round key → Substitute bytes → Shift rows

④ Add round key → Mix columns → Shift rows → Substitute bytes

정답 2번

출제 포인트

이 문제는 AES 암호화에서 마지막 라운드를 제외한 일반 라운드의 네 변환 순서를 묻는 문제이다.

올바른 순서

1. Substitute bytes(SubBytes) — S-box를 이용하여 각 바이트를 비선형적으로 치환한다.
2. Shift rows(ShiftRows) — 상태 배열의 각 행을 서로 다른 크기만큼 순환 이동한다.
3. Mix columns(MixColumns) — 각 열의 바이트를 선형 변환하여 확산시킨다.
4. Add round key(AddRoundKey) — 변환된 상태에 해당 라운드 키를 XOR한다.

이 순서에서 ShiftRows가 바이트의 열 위치를 바꾼 뒤 MixColumns가 각 열을 섞어 확산하며, 마지막에 라운드 키를 결합한다. 다만 AES의 마지막 라운드에서는 MixColumns를 수행하지 않는다.

NoteBase

선지별 해설

① X
- 틀린 부분: Add round key를 Substitute bytes 바로 뒤에 두고 Mix columns를 Shift rows보다 먼저 수행한 순서가 틀렸다.
- 올바르게는: Substitute bytes → Shift rows → Mix columns → Add round key이다.

② O
- Substitute bytes → Shift rows → Mix columns → Add round key는 마지막 라운드를 제외한 AES 일반 라운드의 정확한 처리 순서이다.

③ X
- 틀린 부분: Mix columns를 첫 단계에 두고 Add round key를 Substitute bytes보다 앞에 둔 순서가 틀렸다.
- 올바르게는: Substitute bytes → Shift rows → Mix columns → Add round key이다.

④ X
- 틀린 부분: Add round key를 첫 단계에 두고 Substitute bytes를 마지막 단계에 둔 순서가 틀렸다.
- 올바르게는: Substitute bytes → Shift rows → Mix columns → Add round key이다.

오답 포인트

암호화 시작 전에 수행하는 최초 AddRoundKey와 각 일반 라운드의 마지막 단계인 AddRoundKey를 혼동하기 쉽다. 또한 ShiftRows가 먼저 바이트의 위치를 바꾸고, 그다음 MixColumns가 열 단위로 섞는다는 선후관계가 핵심 함정이다.

다시 나오면 이렇게 판단

AES 일반 라운드는 바이트 치환 → 행 이동 → 열 혼합 → 라운드 키 결합의 흐름으로 판단한다. 마지막 라운드인지도 함께 확인하며, 마지막 라운드이면 MixColumns가 빠진다.

암기 포인트

일반 라운드는 대행열키(SubBytes → ShiftRows → MixColumns → AddRoundKey), 마지막 라운드는 열 혼합 생략이다.

NoteBase

문 18. 다음 중 Unix와 관련된 설명으로 가장 옳지 않은 것은?

① /etc/passwd : 사용자 기본 정보 파일을 저장하고 있음.

② /etc/group : 그룹 기본 정보 파일을 저장하고 있음.

③ /var : 프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있음.

④ /etc/login.defs : 사용자 계정 설정과 관련된 기본값을 정의한 파일.

정답 3번

출제 포인트

Unix 계열 시스템에서 주요 계정 정보 파일과 디렉터리의 용도를 구별하는 문제이다.

핵심 개념

/etc는 시스템 전반의 설정 파일이 주로 위치하는 디렉터리이다. /var는 로그, 스풀, 캐시처럼 시스템 운용 중 내용이 계속 변하는 가변 데이터를 저장하는 디렉터리이고, 일반적인 임시 파일은 주로 /tmp에 저장한다.

선지별 해설

① O — /etc/passwd에는 로그인 이름, 사용자 ID, 그룹 ID, 홈 디렉터리, 로그인 셸 등 사용자 계정의 기본 정보가 저장된다. 일반적인 비밀번호 해시 자체는 /etc/shadow에 저장된다.
② O — /etc/group에는 그룹 이름, 그룹 ID, 그룹 구성원 등 그룹의 기본 정보가 저장된다.
③ X — 틀린 부분은 '프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있음'이다. /var에는 로그, 메일·인쇄 스풀, 캐시 등 운용 중 변하는 데이터가 저장되며, 일반적인 임시 파일을 저장하는 대표 디렉터리는 /tmp이다.
④ O — /etc/login.defs는 사용자 계정 생성과 로그인에 적용되는 비밀번호 만료 기간, UID·GID 범위 등의 기본값을 정의하는 설정 파일이다.

오답 포인트

③은 프로그램 동작 중 생성된다는 공통점 때문에 가변 데이터와 임시 파일을 혼동하게 한다. /var의 var는 variable data를 뜻하고, 임시 파일의 대표 위치는 /tmp이다.

다시 나오면 이렇게 판단

경로의 핵심 기능으로 판단한다. /etc는 설정, /var는 계속 변하는 운용 데이터, /tmp는 임시 파일로 구분한다.

암기 포인트

/etc는 설정, /var는 가변 데이터, /tmp는 임시 파일이다.

NoteBase

문 19. 다음 <보기> 빈칸에 들어갈 용어를 가장 바르게 나열한 것은?

<보기>
○ ㉠는 공개적으로 알려진 소프트웨어의 보안 취약점을 가리키는 고유 표기를 의미한다.
○ 취약점명은 ㉠-㉡-㉢ 형식으로 구성되어 있다.

① ㉠: CVE, ㉡: 연도, ㉢: 일련번호
② ㉠: CVSS, ㉡: 연도, ㉢: 일련번호
③ ㉠: CVE, ㉡: 일련번호, ㉢: 소프트웨어버전
④ ㉠: CWE, ㉡: 일련번호, ㉢: 소프트웨어버전

정답 1번

출제 포인트

공개된 소프트웨어 보안 취약점의 고유 식별자인 CVE와 그 식별자 형식인 CVE-연도-일련번호를 구별하는 문제이다.

핵심 개념

CVE(Common Vulnerabilities and Exposures)는 공개적으로 알려진 개별 보안 취약점에 부여하는 고유 식별 체계이다. CVE 식별자는 'CVE-연도-일련번호' 형식으로 구성된다.
CVSS(Common Vulnerability Scoring System)는 취약점의 심각도를 점수로 평가하는 체계이고, CWE(Common Weakness Enumeration)는 취약점의 원인이 될 수 있는 소프트웨어·하드웨어 약점 유형을 분류하는 체계이다.

선지별 해설

① O — ㉠ CVE, ㉡ 연도, ㉢ 일련번호를 넣으면 'CVE-연도-일련번호'가 되어 CVE 식별자의 구성과 정확히 일치한다.
② X — 틀린 표현은 ㉠의 'CVSS'이다. CVSS는 취약점의 심각도를 점수화하는 체계이며 고유 취약점명의 접두어가 아니다. 올바르게는 'CVE-연도-일련번호'이다.
③ X — 틀린 표현은 ㉡의 '일련번호'와 ㉢의 '소프트웨어버전'이다. CVE 뒤에는 먼저 연도가 오고, 마지막에는 소프트웨어 버전이 아니라 일련번호가 온다. 올바르게는 ㉡ 연도, ㉢ 일련번호이다.
④ X — 틀린 표현은 ㉠의 'CWE'와 ㉢의 '소프트웨어버전'이다. CWE는 약점 유형을 분류하는 식별 체계이며, 보기에서 묻는 개별 공개 취약점 표기는 'CVE-연도-일련번호'이다. 올바르게는 ㉠ CVE, ㉡ 연도, ㉢ 일련번호이다.

NoteBase

오답 포인트

②는 CVSS가 보안 취약점과 관련된 용어라는 점을 이용한 함정이고, ④는 CVE와 CWE의 영문 약어가 비슷하다는 점을 이용한 함정이다. 또한 ③은 CVE 식별자에 제품의 소프트웨어 버전이 직접 포함된다고 착각하게 만든다.

다시 나오면 이렇게 판단

문제에서 '공개된 개별 취약점의 고유 표기'를 물으면 CVE를 선택하고, 식별자 구성은 접두어 CVE 다음에 연도와 일련번호가 차례로 온다고 판단한다. 심각도 점수는 CVSS, 약점 유형 분류는 CWE로 구별한다.

암기 포인트

CVE는 취약점 번호, CVSS는 심각도 점수, CWE는 약점 유형이며, CVE 표기는 'CVE-연도-일련번호'이다.

NoteBase

문 20. 검색엔진이 사이트를 수집하기 위해 사용하는 크롤러(Crawler)에 대하여 사이트의 수집·허용 여부를 표시하는 파일은?

① access.conf

② httpd.conf

③ robots.txt

④ crawler.txt

정답 3번

출제 포인트

검색엔진 크롤러에게 사이트의 수집 허용·제한 범위를 알리는 표준 파일명을 구별하는 문제이다.

핵심 개념

robots.txt는 웹사이트의 루트 경로에 두고 User-agent, Disallow, Allow 등의 지시어로 크롤러가 수집할 수 있는 경로를 알리는 파일이다. 이는 협조하는 크롤러에 대한 수집 지침이지, 서버 차원의 강제 접근 통제 수단은 아니다.

선지별 해설

① X — access.conf는 검색엔진 크롤러의 수집 허용 여부를 표시하는 표준 파일명이 아니다. 틀린 파일명이며, 올바르게는 robots.txt이다.
② X — httpd.conf는 Apache HTTP Server의 주 설정 파일로 서버 동작과 모듈 등을 설정한다. 크롤러 수집 정책을 표시하는 파일은 robots.txt이다.
③ O — robots.txt는 크롤러별로 수집을 허용하거나 제한할 경로를 표시하는 표준 파일이다.
④ X — crawler.txt는 크롤러 수집 정책을 알리는 표준 파일명이 아니다. 틀린 파일명이며, 올바르게는 robots.txt이다.

오답 포인트

파일명에 access나 crawler가 들어 있다는 이유만으로 ① 또는 ④를 고르기 쉽다. 이 문제는 기능을 연상해 만든 이름이 아니라 실제 표준 파일명 robots.txt를 묻는다.

다시 나오면 이렇게 판단

검색엔진·크롤러와 수집 허용 또는 제한이 함께 제시되면 robots.txt를 찾는다. 웹 서버 자체의 설정 파일과 크롤러에게 제공하는 수집 지침 파일을 구분한다.

NoteBase

암기 포인트

로봇의 수집 규칙은 robots.txt이다.

NoteBase