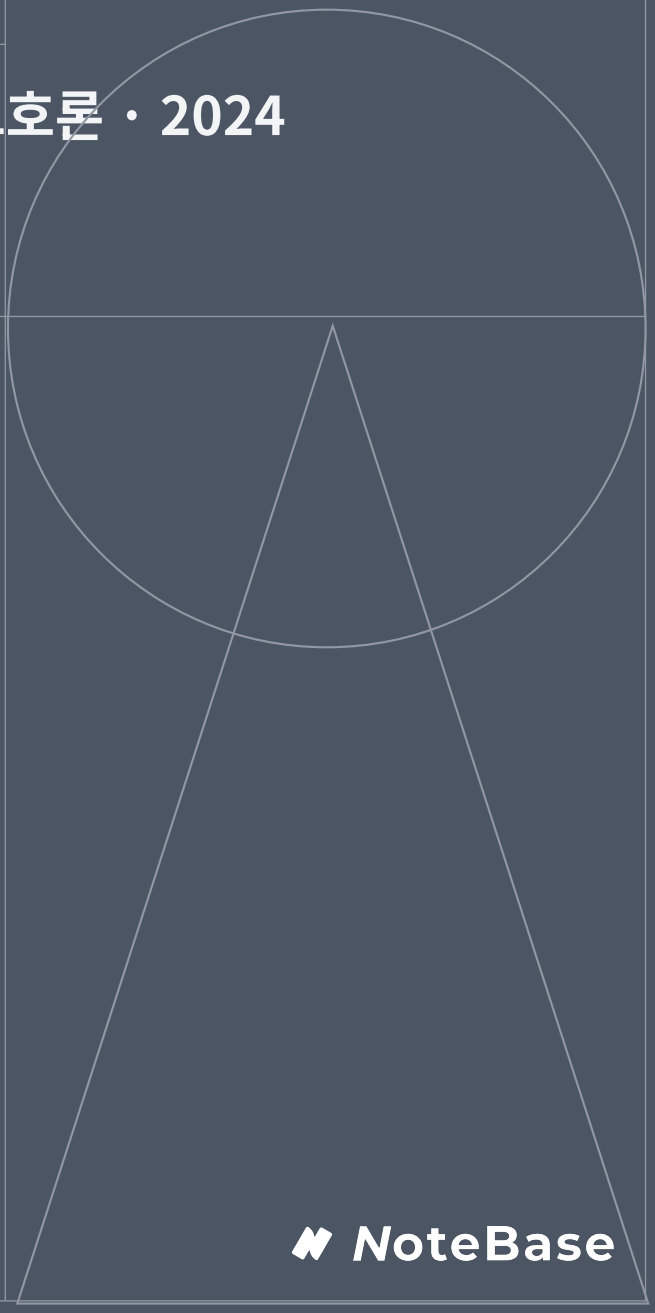
기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2024



NoteBase

기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2024

공무원/서울시/7급 · 정보보호론 · 2024

문 1. 정보 보안의 3대 요소인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 대한 설명으로 가장 옳지 않은 것은?

① 기밀성은 인가된 사용자만 정보 자산에 접근할 수 있다는 것이다.

② 무결성은 권한을 가진 사용자만 인가된 방법으로 정보를 변경할 수 있도록 하는 것이다.

③ 가용성은 인가된 사용자에게 제한된 시점에만 정보 자산에 대한 접근이 가능하도록 하는 것이다.

④ 기밀성의 대표적인 서비스로 방화벽, 암호 등이 있다.

정답 3번

출제 포인트

이 문제는 정보보안의 3대 요소인 기밀성, 무결성, 가용성의 정의와 적용 방향을 정확히 구분할 수 있는지를 묻는다.

핵심 개념

기밀성은 인가되지 않은 자에게 정보가 노출되지 않도록 하는 성질이다. 무결성은 정보가 인가되지 않은 변경 없이 정확하고 완전하게 유지되는 성질이다. 가용성은 인가된 사용자가 필요할 때 정보나 서비스를 사용할 수 있도록 하는 성질이다.

선지별 해설

1번 O: 기밀성은 인가된 사용자만 정보 자산에 접근할 수 있도록 비인가 접근을 막는 개념이므로 옳다.
2번 O: 무결성은 권한 있는 사용자만 정해진 방식으로 정보를 생성·수정·삭제할 수 있게 하여 정보의 정확성과 완전성을 지키는 것이므로 옳다.
3번 X: 틀린 표현은 "제한된 시점에만"이다. 올바르게는 "인가된 사용자가 필요한 시점에 정보 자산에 접근할 수 있도록 하는 것"이다. 가용성의 핵심은 적시에 이용 가능하게 하는 데 있다.
4번 O: 암호는 내용을 숨겨 기밀성을 보장하는 대표 수단이고, 방화벽도 비인가 접근을 차단하여 기밀성 확보에 기여하므로 옳다.

NoteBase

오답 포인트

3번의 "제한된 시점에만"이라는 표현이 함정이다. 접근을 제한하는 발상은 기밀성 쪽 표현에 가깝고, 가용성은 허용된 사용자가 필요할 때 지체 없이 이용할 수 있어야 한다는 점이 핵심이다.

다시 나오면 이렇게 판단

정보를 못 보게 하는지, 함부로 못 바꾸게 하는지, 필요할 때 쓸 수 있게 하는지를 먼저 나누면 된다. 비밀 유지이면 기밀성, 변경 방지이면 무결성, 적시 이용 보장이면 가용성이다.

암기 포인트

기밀성은 보지 못하게, 무결성은 바꾸지 못하게, 가용성은 필요할 때 쓰게 하는 것이다.

NoteBase

문 2. 블록암호의 운용 방식 중 ECB(Electric Code Book) 모드에 대한 설명으로 가장 옳지 않은 것은?

① 긴 메시지를 블록 단위로 나누어 각각을 블록암호를 이용하여 암호화하는 방법이다.

② 동일한 메시지 블록을 동일한 키로 암호화하면 동일한 암호문이 생성되기 때문에 보안 문제가 발생할 수 있다.

③ 메시지가 주어졌을 때 병렬 연산이 가능하다.

④ 메시지가 주어지기 전에 사전 계산이 가능하기 때문에, 이를 이용하여 효율을 높일 수 있다.

정답 4번

출제 포인트

이 문제는 ECB 모드의 독립적 블록 처리 특성과, 동일 블록 반복에 따른 패턴 노출 및 사전 계산 가능 모드와의 차이를 묻는다. 참고로 발문에는 ECB의 풀네임이 'Electric Code Book'으로 적혀 있으나 정확한 명칭은 'Electronic Code Book'이다.

핵심 개념

ECB는 각 평문 블록을 서로 독립적으로 같은 키로 암호화하는 방식이다. ECB의 핵심 키워드는 독립 처리와 병렬 처리 가능이다. 다만 ECB는 평문 블록이 실제로 들어와야 비로소 암호화 연산을 시작할 수 있으므로, 평문이 도착하기 전에는 미리 계산해 둘 것이 없다. 반면 메시지 입력 전 사전 계산으로 효율을 높이는 성질은 CTR이나 OFB 쪽 특징이다. CTR과 OFB는 키스트림 생성이 평문과 무관하게 키와 카운터(또는 IV)만으로 이루어지므로, 평문이 오기 전에 키스트림을 미리 만들어 두었다가 평문이 도착하면 단순 XOR만 수행하여 효율을 높일 수 있다.

선지별 해설

1번: O. ECB는 긴 메시지를 블록 단위로 나누고 각 블록을 독립적으로 블록암호에 넣어 암호화한다. 블록 사이에 이전 블록 결과를 섞지 않는다는 점이 핵심이다.
2번: O. 같은 키로 같은 평문 블록을 암호화하면 같은 암호문 블록이 나온다. 그래서 반복 패턴이 드러나 보안상 약점이 된다.
3번: O. 각 블록이 서로 독립적이므로 메시지 블록들이 주어지면 여러 블록을 동시에 암호화할 수 있다. 병렬 연산이 가능한 대표적 운용 방식이다.
4번: X. 틀린 부분은 "메시지가 주어지기 전에 사전 계산이 가능"하다는 표현이다. ECB의 암호화 입력은 평문 블록 그 자체이므로, 평문이 도착하지 않으면 넣을 입력이 없어 암호화 연산을 시작조차 할 수 없다. 즉 평문이 오기 전에 미리 계산해 둘 중간 산출물이 존재하지 않으므로 사전 계산을 통한 효율 향상은 ECB에 해당하지 않는다. 이는 평문과 무관한 키스트림을 미리 만들어 두는 CTR이나 OFB와 구분되는 지점이다.

NoteBase

오답 포인트

3번의 병렬 처리 가능성과 4번의 사전 계산 가능성을 같은 뜻으로 보면 틀린다. 병렬 처리는 평문 블록들이 모두 주어진 뒤 서로 독립이라 동시에 처리할 수 있다는 의미이고, 사전 계산은 평문이 오기 전에 미리 출력값을 준비해 둘 수 있다는 의미다. ECB는 전자에는 해당하지만 후자에는 해당하지 않는다. 평문 없이 미리 키스트림이나 출력값을 준비해 두는 구조는 CTR, OFB와 같은 키스트림 기반 모드의 특징이다.

다시 나오면 이렇게 판단

블록암호 운용 모드 문제에서는 먼저 블록들이 서로 독립인지, 이전 결과에 의존하는지, 평문이 오기 전에 미리 계산할 수 있는지의 세 축으로 구분하면 된다. ECB는 독립 처리와 병렬 처리에는 해당하지만 사전 계산형 모드는 아니다. 사전 계산이 가능한 것은 키스트림이 평문과 무관한 CTR, OFB 계열이다.

암기 포인트

ECB는 같은 블록이면 같은 암호문, 독립 처리라 병렬 가능, 사전 계산 특징은 키스트림이 평문과 무관한 CTR, OFB류와 연결된다.

NoteBase

문 3. 일방향 해시 함수에 대한 설명으로 가장 옳지 않은 것은?

① MD4, MD5는 128비트 길이의 해시값을 출력하며 현재는 둘 다 안전하지 않다.

② SHA-1은 180비트 길이의 해시값을 출력하며 강한 충돌 내성에 대한 취약점이 발견되어 안전하지 않다.

③ SHA-256, SHA-384, SHA-512는 각 256, 384, 512비트 길이의 해시값을 출력하며, 입력하는 메시지 길이는 SHA-256은 2^{64}비트 미만, SHA-384와 SHA-512는 2^{128}비트 미만으로 제한된다.

④ RIPEMD-160은 160비트 길이의 해시값을 출력하며, RIPEMD 함수를 수정하여 개발됐고, 비트코인에서 사용되기도 한다.

정답 2번

출제 포인트

이 문제는 대표적인 일방향 해시 함수의 출력 길이, 안전성, 그리고 허용 입력 길이를 정확히 구별할 수 있는지를 묻는다.

핵심 개념

MD4와 MD5는 128비트 해시를 내는 구형 해시 함수이고 현재는 충돌 공격에 취약하다.
SHA-1은 160비트 해시를 내지만 충돌 취약점이 확인되어 안전하다고 볼 수 없다.
SHA-256, SHA-384, SHA-512는 각각 256, 384, 512비트 해시를 내며 메시지 길이 한도는 SHA-256이 2^64비트 미만, SHA-384와 SHA-512가 2^128비트 미만이다.
RIPEMD-160은 160비트 해시를 내는 함수로, RIPEMD를 강화한 버전이며 비트코인 주소 체계에서 활용된다.

선지별 해설

1번: O. MD4와 MD5는 모두 128비트 해시값을 출력한다. 또한 둘 다 충돌 공격에 취약하여 현재는 안전한 해시 함수로 쓰기 어렵다.
2번: X. 틀린 부분은 "180비트"이다. SHA-1의 출력 길이는 180비트가 아니라 160비트이다. 뒤의 설명처럼 SHA-1은 충돌 내성 취약점이 발견되어 안전하지 않다는 판단은 맞다.
3번: O. SHA-256, SHA-384, SHA-512의 출력 길이는 이름과 같이 각각 256, 384, 512비트이다. 입력 메시지 길이 제한도 SHA-256은 2^64비트 미만, SHA-384와 SHA-512는 2^128비트 미만으로 맞다.
4번: O. RIPEMD-160은 160비트 해시를 출력하며, 기존 RIPEMD를 보강한 버전이다. 비트코인에서는 공개키 해시 등에서 SHA-256과 함께 RIPEMD-160이 사용된다.

오답 포인트

2번은 "안전하지 않다"라는 뒤 문장이 맞기 때문에 앞부분의 숫자 오류를 놓치기 쉽다. 이 문제는 알고리즘 이름과 출력 비트 수를 정확히 대응시키는지를 노린 문항이다.

NoteBase

다시 나오면 이렇게 판단

해시 함수 문제는 먼저 출력 비트 수를 확인하고, 다음으로 현재 안전성 여부와 메시지 길이 제한을 분리해서 본다. 문장 일부가 맞더라도 숫자 하나가 틀리면 전체 선지는 틀린 선지로 판단된다.

암기 포인트

MD4·MD5는 128, SHA-1은 160, SHA-256·384·512는 이름 그대로이며, SHA-1과 MD5는 현재 안전하지 않다.

NoteBase

문 4. RSA 암호 알고리즘에서 키 생성을 위해 두 개의 서로 다른 소수를 곱한 값인 $N = 7 \times 11 = 77$이 주어졌다고 할 때, 공개키로 선택할 수 있는 가장 옳은 값은?

① 3

② 5

③ 7

④ 9

정답 3번

출제 포인트

이 문제는 RSA에서 공개지수 e가 03d5(N)와 서로소여야 한다는 조건을 이용해 가능한 값을 고르는 문제이다.

조건 정리

주어진 값: $N = 7 \times 11 = 77$이다.
구해야 할 값: 공개키로 선택할 수 있는 가장 옳은 값 e이다.
주의할 조건: RSA의 공개지수 e는 1<e<03d5(N)이고 (e,03d5(N))=1이어야 한다.

사용할 공식

03d5(N)=03d5(pq)=(p-1)(q-1)
(e,03d5(N))=1
이 공식을 쓰는 이유: N이 서로 다른 두 소수 p, q의 곱으로 주어졌으므로 먼저 03d5(N)를 구한 뒤, 공개지수 e가 그 값과 서로소인지 확인해야 하기 때문이다.

계산 과정

1. $N = 7 \times 11$이므로 $p = 7$, $q = 11$이다.
2. 03d5(77)=(7-1)(11-1)=6×10=60이다.
3. 각 선택지를 60과 서로소인지 확인하면 3은 $\gcd(3, 60) = 3$, 5는 $\gcd(5, 60) = 5$, 7은 $\gcd(7, 60) = 1$, 9는 $\gcd(9, 60) = 3$이다.
4. 60과 서로소인 값은 7뿐이므로 정답은 3번이다.

NoteBase

선지 판단

1번 3: X. $\gcd(3, 60) = 3$이므로 공개지수 조건을 만족하지 못한다. 틀린 표현은 '3을 공개키로 선택할 수 있다'이고, 올바르게는 '3은 03d5(N)=60과 서로소가 아니어서 공개키로 선택할 수 없다'이다.
2번 5: X. $\gcd(5, 60) = 5$이므로 공개지수 조건을 만족하지 못한다. 틀린 표현은 '5를 공개키로 선택할 수 있다'이고, 올바르게는 '5는 60의 약수와 공약수를 가지므로 공개키로 선택할 수 없다'이다.
3번 7: O. $\gcd(7, 60) = 1$이므로 공개지수 조건을 만족한다. 7은 $1 < 7 < 60$도 만족하므로 선택 가능하다.
4번 9: X. $\gcd(9, 60) = 3$이므로 공개지수 조건을 만족하지 못한다. 틀린 표현은 '9를 공개키로 선택할 수 있다'이고, 올바르게는 '9는 60과 서로소가 아니어서 공개키로 선택할 수 없다'이다.

오답 포인트

RSA에서 N만 보고 소수 곱이라는 사실만 확인하고 바로 선택지를 고르면 틀리기 쉽다. 이 문항의 함정은 공개지수 조건이 '소수인 수를 고르는 것'이 아니라 '03d5(N)와 서로소인 수를 고르는 것'이라는 점이다. 9는 소수가 아니어서 틀린 것이 아니라 60과 공약수 3을 가지기 때문에 틀린 값이다.

다시 나오면 이렇게 판단

RSA 키 생성 문제는 먼저 $N = pq$에서 03d5(N)=(p-1)(q-1)를 구한 뒤, 후보 e에 대해 1<e<03d5(N)와 (e,03d5(N))=1을 순서대로 확인하면 된다.

암기 포인트

RSA 공개지수는 '소수인지'보다 '03d5(N)와 서로소인지'가 핵심이다.

NoteBase

문 5. 접근 제어 모델 중 하나인 비바(Biba) 모델에 대한 설명으로 가장 옳은 것은?

① 임의적 접근 제어 모델(Discretionary Access Control)에 해당한다.

② 수학적 보안 모델로 데이터의 기밀성에 초점을 맞춰 설계되었다.

③ 자신에게 허용된 보안 레벨보다 높은 보안 레벨의 문서에 대한 읽기가 허용되지 않는다.

④ 자신에게 허용된 보안 레벨보다 낮은 보안 레벨의 문서에 대한 쓰기가 허용된다.

정답 4번

출제 포인트

이 문제는 Biba 모델이 기밀성이 아니라 무결성을 보호하며, 읽기·쓰기 규칙이 Bell-LaPadula와 반대 방향이라는 점을 묻는 문제이다.

핵심 개념

Biba 모델은 데이터의 무결성을 보호하기 위한 수학적 보안 모델이다. 핵심 규칙은 no read down, no write up이다. 즉 높은 무결성 수준의 주체는 낮은 무결성 수준의 객체를 읽을 수 없고, 자신보다 높은 무결성 수준의 객체에는 쓸 수 없다. 반대로 Bell-LaPadula는 기밀성을 보호하며 no read up, no write down을 따른다.

선지별 해설

① X: 틀린 부분은 '임의적 접근 제어 모델(DAC)'이다. Biba는 사용자의 재량으로 권한을 부여하는 DAC가 아니라 무결성 보장을 위한 다단계 보안 모델이다.
② X: 틀린 부분은 '기밀성에 초점을 맞춰'이다. Biba는 기밀성이 아니라 무결성에 초점을 맞춘 모델이다. 기밀성 중심 모델은 Bell-LaPadula이다.
③ X: 틀린 부분은 '높은 보안 레벨의 문서에 대한 읽기가 허용되지 않는다'이다. Biba에서는 자신보다 낮은 무결성 수준의 문서를 읽지 못한다. 높은 수준 읽기 금지는 Bell-LaPadula의 no read up에 해당한다.
④ O: Biba의 규칙은 no write up이므로 자신보다 높은 무결성 수준에는 쓸 수 없고, 낮은 무결성 수준의 문서에 대한 쓰기는 허용된다.

오답 포인트

Biba와 Bell-LaPadula를 둘 다 보안 레벨 모델로만 외우면 방향을 뒤집기 쉽다. ②는 기밀성과 무결성을 바꾸어 놓은 함정이고, ③은 Bell-LaPadula의 no read up을 Biba에 끼워 넣은 함정이다.

다시 나오면 이렇게 판단

먼저 보호 대상이 기밀성인지 무결성인지 구분한다. 기밀성이면 Bell-LaPadula로 보고 no read up, no write down을 적용한다. 무결성이면 Biba로 보고 no read down, no write up을 적용하면 된다.

NoteBase

암기 포인트

Bell-LaPadula는 no read up, no write down이고, Biba는 no read down, no write up이다.

NoteBase

문 6. 버퍼 오버플로 공격에 대한 대응책 중 스택 실드에 대한 설명으로 가장 옳은 것은?

① 스택에서 실행 권한을 제거하여 스택에 로드된 공격자의 공격 코드를 실행하지 못하도록 한다.

② 컴파일러가 프로그램의 함수를 호출할 때 ret 앞에 canary값을 주입하고, 종료할 때 canary값의 변조 여부를 확인한다.

③ 함수를 호출할 때 ret값을 Global RET Stack이라는 특수 스택에 저장한 뒤, 함수를 종료할 때 Global RET Stack에 저장된 ret값과 스택의 ret값을 비교한다.

④ 스택, 힙, 라이브러리 등 데이터 영역의 주소를 난수화한다.

정답 3번

출제 포인트

이 문제는 버퍼 오버플로 대응기법 중 스택 실드(StackShield)에 대한 설명으로 가장 옳은 것을 고르는 문항이다. 즉 네 선지 가운데 StackShield의 동작을 정확히 설명한 하나를 찾아야 하며, 나머지는 NX(비실행 스택), 스택 카나리, ASLR 등 다른 기법을 설명한 선지이다.

핵심 개념

StackShield는 함수 호출 시 복귀주소(ret)를 Global RET Stack이라는 별도의 안전한 영역에 저장해 두었다가, 함수가 종료될 때 그 저장값과 스택상의 ret값을 대조해 복귀주소 변조를 탐지·복원하는 기법이다. NX는 스택에 실행 권한을 주지 않아 주입된 셸코드의 실행을 막는 기법이다. 스택 카나리는 지역변수와 복귀주소 사이에 검사용 카나리 값을 두고 함수 종료 시 그 값의 변조 여부로 오버플로를 탐지하는 기법이다. ASLR은 스택, 힙, 라이브러리 등 메모리 영역의 배치를 무작위화해 주소 예측을 어렵게 만드는 기법이다.

선지별 해설

1번: X. 스택에서 실행 권한을 제거해 적재된 공격 코드가 실행되지 못하게 한다는 설명은 NX(비실행 스택, DEP)에 대한 것이므로 StackShield 설명으로 옳지 않다.
2번: X. 함수를 호출할 때 ret 앞에 canary 값을 주입하고 종료 시 그 변조 여부를 확인한다는 설명은 스택 카나리에 대한 것이므로 StackShield 설명으로 옳지 않다.
3번: O. 함수를 호출할 때 ret값을 Global RET Stack이라는 별도의 특수 스택에 저장해 두었다가, 함수 종료 시 Global RET Stack에 저장된 ret값과 스택의 ret값을 대조한다는 설명이 바로 StackShield의 동작이므로 가장 옳다.
4번: X. 스택, 힙, 라이브러리 등 데이터 영역의 주소를 난수화한다는 설명은 ASLR에 대한 것이므로 StackShield 설명으로 옳지 않다.

NoteBase

오답 포인트

발문이 '가장 옳지 않은 것'이 아니라 '스택 실드에 대한 설명으로 가장 옳은 것'을 묻는 점을 놓치면 정답을 거꾸로 고르기 쉽다. ①·②·④는 각각 NX, 스택 카나리, ASLR을 정확히 설명한 옳은 문장이지만 StackShield의 설명은 아니므로 이 문항에서는 정답이 되지 못한다. StackShield의 식별 표지는 Global RET Stack에 ret값을 별도 보관한다는 부분이다.

다시 나오면 이렇게 판단

버퍼 오버플로 대응기법 문제는 먼저 발문이 특정 기법의 설명을 고르라는 것인지부터 확인하고, 각 선지가 어느 기법을 설명하는지 매칭하면 된다. 실행 자체를 막으면 NX, 변조 감지용 값을 두면 카나리, 복귀주소를 별도 스택에 보관·대조하면 StackShield, 주소를 난수화하면 ASLR이다. 이 문항은 StackShield를 물었으므로 Global RET Stack을 언급한 선지가 정답이다.

암기 포인트

NX는 실행 차단, 카나리는 변조 탐지, StackShield는 Global RET Stack에 복귀주소 별도 보관·대조, ASLR은 주소 난수화이다.

NoteBase

문 7. 리눅스/유닉스 시스템에서 SetUID에 대한 설명으로 가장 옳지 않은 것은?

① 시스템에 로그인한 계정은 일반적으로 시스템으로부터 처음 부여받은 RUID(Real UID)와 EUID(Effective UID)의 값이 동일하지만, SetUID 비트를 가진 프로그램을 실행하면 잠시 일치하지 않는 상태가 발생한다.

② /usr/bin/passwd 파일에 SetUID가 설정되면 파일 소유주가 root이기 때문에, 이 파일이 실행되는 프로세스는 실행 시간 동안 root 권한을 갖는다.

③ 'find / -user root -perm /4000'과 같은 find 명령을 사용하면 SetUID가 설정된 파일들을 검색할 수 있다.

④ /usr/bin/passwd 파일에 SetUID가 설정되면 권한은 2755(rws r-x r-x)이다.

정답 4번

출제 포인트

이 문제는 리눅스/유닉스의 SetUID 동작 원리와 권한 표기에서 SetUID와 SetGID 비트를 구별할 수 있는지를 묻는 문제이다.

핵심 개념

RUID는 원래 로그인한 실제 사용자 ID이고, EUID는 현재 프로세스가 권한 판정에 사용하는 사용자 ID이다. SetUID는 실행 파일 소유자의 UID로 EUID를 바꾸는 비트이고, 권한 숫자로는 4000이 더해진다. SetGID는 그룹 기준으로 동작하는 비트이며 권한 숫자로는 2000이 더해진다.

선지별 해설

1번: O. 일반적으로 로그인 직후에는 RUID와 EUID가 같다. 그러나 SetUID가 설정된 실행 파일을 실행하면 RUID는 로그인 사용자로 유지되고 EUID만 파일 소유자 UID로 바뀔 수 있으므로 두 값이 일치하지 않는 상태가 생긴다.
2번: O. /usr/bin/passwd가 root 소유의 SetUID 파일이면 실행 중인 프로세스의 EUID가 root가 되어 비밀번호 변경에 필요한 권한을 행사할 수 있다.
3번: O. `find / -user root -perm /4000`는 root가 소유하면서 SetUID 비트가 설정된 파일을 찾는 데 사용하는 전형적인 명령 형태이다. `/4000`은 4000 비트가 포함된 파일을 찾는 의미이다.
4번: X. 틀린 부분은 `2755`이다. SetUID는 4000 비트이므로 /usr/bin/passwd의 전형적인 권한 표기는 `4755(rwsr-xr-x)`이다. `2755`는 SetGID 비트가 설정된 경우에 해당하므로 SetUID 설명으로는 맞지 않는다.

오답 포인트

SetUID와 SetGID를 모두 특수권한으로만 묶어서 외우면 4000과 2000을 뒤바꾸기 쉽다. 이 문제의 함정은 4번의 `rwsr-xr-x` 문자열은 맞아 보이는데 숫자 표기만 `2755`로 바꿔 놓았다는 점이다.

NoteBase

다시 나오면 이렇게 판단

특수권한 문제는 먼저 무엇이 바뀌는지부터 본다. 사용자 권한이 바뀌면 SetUID 4000, 그룹 권한이 바뀌면 SetGID 2000으로 판단하고, 문자 표기와 숫자 표기가 서로 일치하는지도 함께 확인한다.

암기 포인트

SetUID는 사용자 4000, SetGID는 그룹 2000, `rwsr-xr-x`는 4755이다.

NoteBase

문 8. 디지털 서명에 대한 설명으로 가장 옳은 것은?

① 문서의 기밀성을 위한 기술이다.

② 문서의 크기가 크면 문서의 해시값에 서명한다.

③ 문서의 전송자가 누구인지는 알아낼 수 없다.

④ 공개키 방식일 경우, 공개키로 서명하고 비밀키로 검증한다.

정답 2번

출제 포인트

이 문제는 디지털 서명이 기밀성이 아니라 인증, 무결성, 부인방지를 제공하며 실제 서명 대상은 원문이 아니라 해시값인 경우가 많다는 점을 묻는다.

핵심 개념

디지털 서명은 송신자가 자신의 개인키로 메시지의 해시값에 서명해 작성자 확인, 메시지 무결성, 부인방지를 확보하는 기술이다. 공개키 방식에서는 개인키로 서명하고 공개키로 검증한다.

선지별 해설

1번 X: 디지털 서명의 핵심 기능은 기밀성이 아니라 인증, 무결성, 부인방지이다. 틀린 표현은 "기밀성"이다. 올바르게는 "문서의 작성자 확인과 무결성 검증을 위한 기술이다"이다.
2번 O: 문서가 크면 원문 전체에 직접 서명하기보다 해시 함수를 적용한 해시값에 서명한다. 계산량을 줄이면서 원문 변경 여부도 함께 검증할 수 있다.
3번 X: 디지털 서명은 서명 검증을 통해 누가 서명했는지 확인할 수 있다. 틀린 표현은 "알아낼 수 없다"이다. 올바르게는 "서명자의 공개키를 통해 전송자 또는 서명자를 확인할 수 있다"이다.
4번 X: 공개키 방식의 디지털 서명은 개인키로 서명하고 공개키로 검증한다. 틀린 표현은 "공개키로 서명하고 비밀키로 검증한다"이다. 올바르게는 "비밀키로 서명하고 공개키로 검증한다"이다.

오답 포인트

암호화와 전자서명을 같은 기능으로 섞으면 틀린다. 기밀성은 주로 암호화의 기능이고, 디지털 서명은 서명 주체 확인과 무결성 검증을 담당한다. 또한 공개키 암호에서 서명과 검증의 키 방향을 거꾸로 외우기 쉽다.

다시 나오면 이렇게 판단

선지를 보면 먼저 디지털 서명이 보장하는 성질이 기밀성인지 인증·무결성·부인방지인지 구분하고, 다음으로 서명과 검증에 쓰는 키의 방향이 개인키에서 공개키로 이어지는지 확인하면 된다.

NoteBase

암기 포인트

디지털 서명은 해시값에 개인키로 서명하고 공개키로 검증하며, 기밀성이 아니라 인증·무결성·부인방지를 담당한다.

NoteBase

문 9. 미국 NIST에서 추진 중인 양자내성암호(Post-Quantum Cryptography)에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

<보기>
ㄱ. 양자내성암호는 양자 컴퓨팅 환경에서 안전하게 암호 기술을 이용할 수 있도록 하는 새로운 공개키 암호이다.
ㄴ. 1996년 그루버(Grover)는 양자 컴퓨팅을 이용한 연산으로 RSA 암호의 안전성 기반 문제인 인수분해 문제를 이론적으로 해독할 수 있는 알고리즘을 개발하였다.
ㄷ. NIST는 양자내성암호화 알고리즘 표준으로 2022년에 FALCON, SPHINCS+, CRYSTALS-KYBER, CRYSTALS-DILITHIUM을 선정하였다.
ㄹ. ECDSA는 양자 컴퓨팅을 이용한 연산으로도 해독이 불가능하여 안전하게 사용할 수 있다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

정답 1번

출제 포인트

이 문제는 양자내성암호의 의미, Shor 알고리즘과 Grover 알고리즘의 차이, NIST의 2022년 PQC 선정 결과를 구별할 수 있는지를 묻는다.

핵심 개념

양자내성암호는 양자컴퓨터 공격에도 안전하도록 설계된 공개키 암호 계열이다. Shor 알고리즘은 인수분해와 이산대수 문제를 효율적으로 풀어 RSA와 ECC 계열을 위협하고, Grover 알고리즘은 무차별 대입 탐색을 제곱근 수준으로 빠르게 한다. NIST는 2022년에 CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, SPHINCS+를 표준화 대상으로 선정하였다.

NoteBase

선지별 해설

1번 O: ㄱ과 ㄷ만 옳으므로 정답이다. ㄱ의 양자내성암호는 양자컴퓨팅 환경에서도 안전성을 목표로 하는 새로운 공개키 암호라는 설명이 맞다. ㄷ도 NIST가 2022년에 CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, SPHINCS+를 첫 표준화 대상으로 선정하였으므로 맞다.
2번 X: ㄱ은 옳지만 ㄹ이 틀려서 오답이다. 틀린 표현은 "ECDSA는 양자 컴퓨팅을 이용한 연산으로도 해독이 불가능하여 안전하게 사용할 수 있다"이다. 올바르게는 ECDSA는 타원곡선 이산대수 문제에 의존하므로 충분한 양자컴퓨터와 Shor 알고리즘이 가능해지면 안전하지 않다.
3번 X: ㄷ은 옳지만 ㄴ이 틀려서 오답이다. 틀린 표현은 "1996년 그로버는 ... RSA 암호의 안전성 기반 문제인 인수분해 문제를 이론적으로 해독"이다. 올바르게는 RSA의 인수분해와 ECC의 이산대수 문제를 효율적으로 푸는 알고리즘은 1994년 Shor 알고리즘이고, 1996년 Grover 알고리즘은 무차별 대입 탐색을 제곱근 수준으로 가속한다.
4번 X: ㄴ과 ㄹ이 모두 틀려서 오답이다. ㄴ은 Grover와 Shor의 역할을 뒤바꾼 설명이고, ㄹ은 ECDSA가 양자공격에도 안전하다고 잘못 서술하였다. 올바르게는 인수분해·이산대수 계열 공개키 암호는 양자환경에서 대체가 필요하다.

오답 포인트

출제자는 Grover와 Shor를 바꿔 적어 놓고, ECDSA를 양자환경에서도 안전한 것처럼 섞어 놓았다. "인수분해를 푸는 알고리즘이 누구인가"와 "ECC 계열이 양자공격에 안전한가"를 따로 분리하지 않으면 ㄴ, ㄹ을 함께 맞다고 보기 쉽다.

다시 나오면 이렇게 판단

양자암호 관련 선지는 먼저 공격 대상이 공개키인지 대칭키인지 구분한다. 공개키의 인수분해·이산대수 문제를 깨는 것은 Shor, 무차별 대입 탐색을 빠르게 하는 것은 Grover로 판단하면 대부분 정리된다. 이후 NIST 선정 알고리즘이 KYBER, DILITHIUM, FALCON, SPHINCS+인지 확인하면 된다.

암기 포인트

Shor는 RSA·ECC를 깨고, Grover는 탐색만 빠르게 하며, NIST 2022 선정 4종은 KYBER·DILITHIUM·FALCON·SPHINCS+이다.

문 10. 스니핑(sniffing) 공격의 보안 대책과 이에 대한 설명으로 가장 옳지 않은 것은?

① Ping을 이용한 스니퍼 탐지 - 네트워크에 존재하지 않는 MAC 주소로 위장하여 스니퍼로 의심되는 호스트에 ping을 보냈을 때, ping에 대한 응답이 오는 경우 스니퍼로 탐지할 수 있다.

② ARP를 이용한 스니퍼 탐지 - 스니퍼로 의심되는 호스트에게 위조된 ARP Request를 보냈을 때, ARP Response가 오면 해당 호스트가 프리미스큐어스(promiscuous) 모드로 설정된 것이기 때문에 스니퍼로 탐지할 수 있다.

③ DNS를 이용한 스니퍼 탐지 - 스니핑 프로그램은 일반적으로 DNS에 대한 이름을 해석하기 위해 Reverse-DNS lookup을 수행하기 때문에, 의심되는 호스트에게 ping sweep을 보내고, 들어오는 Reverse-DNS lookup을 감시하여 스니퍼를 탐지한다.

④ 유인을 이용한 스니퍼 탐지 - MAC 주소와 IP 주소의 매칭 값을 저장하고 ARP 트래픽을 모니터링하여 이 매칭 값을 변하게 하는 패킷이 탐지되면, 위조된 ARP를 사용하는 스니퍼로 탐지한다.

정답 4번

출제 포인트

이 문제는 스니퍼 탐지 기법과 ARP 스푸핑 탐지를 구별하는지를 묻는 문제이다.

핵심 개념

스니퍼 탐지는 프러미스큐어스 모드에서 나타나는 비정상 반응이나 이름 해석 흔적을 이용해 의심 호스트를 찾는 방식이다. Ping 기법은 잘못된 MAC으로 보낸 ICMP에 대한 응답 여부를 보고, ARP 기법은 일반 호스트라면 처리하지 않을 ARP 요청에 대한 반응을 본다. DNS 기법은 캡처한 주소를 이름으로 바꾸는 과정에서 발생할 수 있는 Reverse-DNS lookup 흔적을 본다. 반면 IP-MAC 매핑 변조를 감시하는 것은 스니퍼 자체 탐지라기보다 ARP 스푸핑 탐지에 가깝다.

NoteBase

선지별 해설

① O. Ping을 이용한 스니퍼 탐지는 존재하지 않는 MAC 주소로 위장한 뒤 ICMP Echo를 보내고 응답 여부를 보는 방식으로 설명할 수 있다. 정상 NIC는 자기 MAC이 아닌 프레임을 버리지만 프러미스큐어스 모드의 호스트는 이를 상위 계층으로 넘겨 응답할 수 있다.
② O. ARP를 이용한 스니퍼 탐지는 비정상적인 ARP Request에 대한 응답 여부로 프러미스큐어스 모드 여부를 추정하는 방식이다. 핵심은 일반 호스트가 무시할 프레임에 반응하는지를 보는 데 있다.
③ O. DNS를 이용한 스니퍼 탐지는 스니핑 프로그램이 캡처한 IP 주소를 이름으로 해석하려고 Reverse-DNS lookup을 수행할 수 있다는 점을 이용한다. 의심 호스트에 트래픽을 흘린 뒤 역방향 DNS 질의가 들어오는지를 감시하는 설명은 타당하다.
④ X. 틀린 부분은 'MAC 주소와 IP 주소의 매칭 값을 저장하고 ARP 트래픽을 모니터링하여 이 매칭 값을 변하게 하는 패킷이 탐지되면, 위조된 ARP를 사용하는 스니퍼로 탐지한다'는 부분이다. 이것은 프러미스큐어스 모드의 스니퍼 탐지라기보다 ARP 캐시 변조를 이용한 ARP 스푸핑 또는 MITM 공격 탐지에 가깝다. 올바르게는 유인을 이용한 스니퍼 탐지는 미끼 계정 정보나 유인용 트래픽을 흘려보내고 이를 엿듣거나 악용하는 행위가 나타나는지로 스니퍼 사용 여부를 간접 확인하는 방식으로 본다.

오답 포인트

④는 앞부분에 '스니퍼 탐지'라고 적혀 있어 그럴듯하지만 실제 설명은 IP-MAC 매핑 변조 감시이다. 스니퍼 탐지는 수신·해석 흔적을 찾는 것이고, ARP 스푸핑 탐지는 주소 매핑 변조를 찾는 것이라는 차이를 놓치면 틀리기 쉽다.

다시 나오면 이렇게 판단

선지가 프러미스큐어스 모드의 비정상 반응, Reverse-DNS 조회 같은 수동적 도청 흔적을 말하면 스니퍼 탐지로 본다. 반대로 IP-MAC 매핑 변경, 위조 ARP 전파처럼 능동적 변조 흔적을 말하면 ARP 스푸핑 탐지로 구분한다.

암기 포인트

스니퍼 탐지는 반응과 조회 흔적, ARP 스푸핑 탐지는 매핑 변조 흔적이다.

NoteBase

문 11. SSH(Secure Shell)에 대한 설명으로 가장 옳은 것은?

① 서버에서는 기본적으로 80번 포트를 이용한다.

② 익명 계정을 이용하여 누구나 접속할 수 있다.

③ 포트 포워딩 기술을 이용하여 보안 수준이 낮은 환경에서도 안전하게 연결할 수 있다.

④ 원격 컴퓨터에 접속하기 위한 기술로, 보안 문제 때문에 SSH 대신 telnet을 사용할 것을 권장하고 있다.

정답 3번

출제 포인트

이 문제는 SSH의 기본 포트, 인증 방식, 암호화된 원격 접속 기능과 포트 포워딩의 의미를 정확히 구별할 수 있는지를 묻는다.

핵심 개념

SSH는 원격 접속과 명령 실행, 파일 전송, 터널링을 암호화하여 제공하는 프로토콜이다. telnet은 원격 접속은 가능하지만 통신 내용이 평문으로 전달된다. SSH 포트 포워딩은 특정 트래픽을 SSH 암호화 채널로 우회시켜 더 안전하게 전달하는 기능이다.

선지별 해설

1번: X. 틀린 부분은 "80번 포트"이다. SSH 서버의 기본 포트는 22번이다. 올바르게는 "서버에서는 기본적으로 22번 포트를 이용한다."이다.
2번: X. 틀린 부분은 "익명 계정을 이용하여 누구나 접속"이다. SSH는 일반적으로 유효한 계정과 비밀번호 또는 공개키 기반 인증이 필요하다. 올바르게는 "인증된 사용자만 접속할 수 있다."이다.
3번: O. SSH의 포트 포워딩은 SSH 터널을 통해 트래픽을 암호화하여 전달하는 기능이다. 따라서 보안이 약한 구간이나 내부 서비스 접속 상황에서도 더 안전한 통신 경로를 만들 수 있다.
4번: X. 틀린 부분은 "SSH 대신 telnet을 사용할 것을 권장"이다. telnet은 암호화를 제공하지 않아 계정과 명령이 평문으로 노출될 수 있으므로, 원격 접속에는 telnet보다 SSH를 사용하는 것이 일반적이다. 올바르게는 "보안 문제 때문에 telnet 대신 SSH를 사용하는 것이 권장된다."이다.

오답 포인트

원격 접속 프로토콜이라는 공통점만 보고 SSH와 telnet을 같은 수준의 기술로 보면 틀린다. 특히 1번의 80번 포트는 HTTP의 대표 포트이고, 4번은 telnet과 SSH의 보안성을 뒤집어 놓은 함정이다.

다시 나오면 이렇게 판단

원격 접속 문제는 먼저 기본 포트와 암호화 여부를 확인하고, 다음으로 인증 방식과 터널링 기능을 본다. 평문 전송이면 telnet 계열, 암호화와 포트 포워딩이 나오면 SSH로 판단할 수 있다.

NoteBase

암기 포인트

SSH는 22번 포트, 암호화, 인증, 터널링이고 telnet은 평문 원격 접속이다.

NoteBase

문 12. 작업 증명(Proof of Work) 기반의 블록체인에서 블록을 블록체인 네트워크에 추가하는 행위는?

① 분산 원장(distributed ledger)

② 블로킹(blocking)

③ 트랜잭션(transaction)

④ 채굴(mining)

정답 4번

출제 포인트

이 문제는 작업 증명 기반 블록체인에서 블록을 새로 생성해 체인에 추가하는 행위와 관련 용어를 구별하는지를 묻는다.

핵심 개념

분산 원장은 여러 참여자가 동일한 거래 기록을 공유하는 장부이다. 트랜잭션은 장부에 기록될 개별 거래 데이터이다. 채굴은 작업 증명에서 해시 계산을 통해 유효한 블록을 만들어 체인에 추가하는 행위이다. 블로킹은 일반적으로 접근이나 처리를 막는 뜻이며 블록 추가 행위를 가리키지 않는다.

선지별 해설

1번 X: 분산 원장은 블록체인이 유지하는 공유 장부 자체를 뜻한다. 틀린 표현은 "블록을 블록체인 네트워크에 추가하는 행위"에 분산 원장을 대응시킨 점이다. 올바르게는 분산 원장은 결과로 유지되는 기록 체계이다.
2번 X: 블로킹은 차단이나 막음을 뜻하는 일반 용어이다. 틀린 표현은 블로킹을 블록 생성 행위처럼 본 점이다. 올바르게는 작업 증명에서 블록을 추가하는 행위는 채굴이다.
3번 X: 트랜잭션은 송금이나 실행 요청 같은 개별 거래 단위이다. 틀린 표현은 거래 데이터 자체를 블록 추가 행위로 본 점이다. 올바르게는 여러 트랜잭션이 검증되어 블록에 담기고, 그 블록을 추가하는 과정이 채굴이다.
4번 O: 작업 증명 기반 블록체인에서 연산 경쟁을 통해 유효한 블록을 만들고 체인에 연결하는 과정을 채굴이라고 한다.

오답 포인트

분산 원장과 트랜잭션은 블록체인의 구성 요소이지만, 발문은 구성 요소가 아니라 "블록을 추가하는 행위"를 묻는다. 명사 자체가 무엇을 뜻하는지보다 장부인지, 거래 데이터인지, 행위인지의 층위를 구분하지 못하면 오답으로 이어진다.

다시 나오면 이렇게 판단

발문이 기록 매체를 묻는지, 개별 거래를 묻는지, 네트워크에 블록을 붙이는 절차를 묻는지부터 구분한다. 작업 증명에서 새 블록을 만들어 연결하는 동작이 나오면 채굴로 판단한다.

NoteBase

암기 포인트

분산 원장은 장부, 트랜잭션은 거래 1건, 채굴은 작업 증명 기반 블록 추가 행위이다.

NoteBase

문 13. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

① XSS 공격 유형 중 Stored XSS는 게시판 또는 자료실과 같이 사용자가 글을 저장하는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 기법이다.

② XSS 취약점을 확인할 수 있는 예제 코드는 SELECT name FROM sysobjects WHERE xtype = ‘U’와 같다.

③ 크로스 사이트 요청 변조 공격인 CSRF 공격은 피해자가 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 리퀘스트를 보내도록 하는 기법이다.

④ XSS 공격 유형 중 Reflected XSS는 웹 애플리케이션에 스크립트를 저장하는 것이 아니라 URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법이다.

정답 2번

출제 포인트

이 문제는 Stored XSS, Reflected XSS, CSRF, SQL Injection의 구별 기준을 묻는 문제이다.

핵심 개념

Stored XSS는 악성 스크립트가 서버에 저장되었다가 이후 다른 사용자에게 전달되는 공격이다. Reflected XSS는 요청값에 포함된 스크립트가 서버 응답에 즉시 반사되어 실행되는 공격이다. CSRF는 피해자의 인증 상태를 이용해 원하지 않는 요청을 보내게 만드는 공격이다. SQL Injection은 입력값에 SQL 구문을 삽입해 데이터베이스 질의를 변조하는 공격이다.

선지별 해설

① O: Stored XSS는 게시판, 댓글, 자료실처럼 입력 내용이 서버에 저장되는 기능에서 악성 스크립트를 심어 두었다가 이후 방문자 브라우저에서 실행되게 만드는 방식이다. 선지의 설명은 Stored XSS의 저장형 특성을 정확히 설명한다.

② X: 틀린 부분은 "SELECT name FROM sysobjects WHERE xtype = 'U'"를 XSS 취약점 확인 코드라고 한 표현이다. 이 구문은 데이터베이스의 테이블 정보를 조회하는 SQL 문으로, 브라우저에서 실행되는 스크립트가 아니라 SQL Injection 계열에서 볼 수 있는 예시이다. 올바르게는 XSS 취약점 예시는 `` `<script>alert('XSS')</script>` `` 처럼 HTML이나 JavaScript 코드가 입력되어 브라우저에서 실행되는 형태이다.

③ O: CSRF는 피해자가 인지하지 못한 상태에서 이미 로그인된 브라우저가 특정 사이트로 요청을 보내게 만드는 공격이다. 선지의 설명은 CSRF의 본질인 인증 세션 악용과 강제 요청 전송을 정확히 설명한다.

④ O: Reflected XSS는 악성 스크립트가 서버에 저장되지 않고 URL 파라미터나 검색어 같은 요청 입력값에 포함되었다가 응답에 즉시 반영되어 실행되는 공격이다. 선지의 설명은 Stored XSS와 대비되는 반사형 XSS의 특징을 정확히 설명한다.

NoteBase

오답 포인트

입력값을 악용한다는 공통점 때문에 XSS와 SQL Injection을 같은 계열로 착각하기 쉽다. 그러나 XSS는 브라우저에서 스크립트가 실행되고, SQL Injection은 데이터베이스 질의가 변조된다는 점이 결정적인 차이이다.

다시 나오면 이렇게 판단

먼저 입력값이 어디에서 실행되는지를 본다. 브라우저에서 스크립트가 실행되면 XSS이고, 데이터베이스 질의가 바뀌면 SQL Injection이다. 그다음 XSS라면 서버 저장 여부를 기준으로 저장되면 Stored XSS, 즉시 응답에 반사되면 Reflected XSS로 구분한다. 로그인된 사용자의 권한으로 원치 않는 요청을 보내게 하면 CSRF이다.

암기 포인트

브라우저 실행은 XSS, DB 질의 변조는 SQL Injection, 저장되면 Stored, 즉시 반사되면 Reflected, 요청 강제는 CSRF이다.

NoteBase

문 14. 시스템에 침투하기 위한 일반적인 웹 해킹 과정의 순서로 가장 옳은 것은?

① 공격 대상 선정 → 정보 수집 → 취약점 분석 → 공격

② 정보 수집 → 공격 대상 선정 → 취약점 분석 → 공격

③ 공격 대상 선정 → 취약점 분석 → 공격 → 정보 수집

④ 취약점 분석 → 공격 대상 선정 → 정보 수집 → 공격

정답 1번

출제 포인트

이 문제는 일반적인 웹 해킹 절차에서 대상 선정, 정보 수집, 취약점 분석, 공격의 선후관계를 구별할 수 있는지를 묻는다.

올바른 순서

1. 공격 대상 선정 - 어떤 시스템을 공격할지 정한다.
2. 정보 수집 - 선정된 대상의 서비스, 포트, 구조, 계정 정책 등을 파악한다.
3. 취약점 분석 - 수집한 정보를 바탕으로 악용 가능한 약점을 찾는다.
4. 공격 - 확인된 취약점을 실제로 이용한다.

왜 이 순서인가: 취약점 분석은 대상에 대한 정보가 수집되어 있어야 가능하고, 공격은 분석으로 확인된 취약점을 전제로 한다.

선지별 해설

1번: O. 공격 대상을 먼저 정한 뒤 그 대상의 정보를 수집하고, 수집된 정보를 바탕으로 취약점을 분석한 다음 실제 공격을 수행하므로 일반적인 순서에 맞다.

2번: X. 틀린 부분은 '정보 수집 → 공격 대상 선정'이다. 일반적인 절차에서는 먼저 공격 대상을 정하고 그 대상에 대해 정보를 수집한다. 올바르게는 '공격 대상 선정 → 정보 수집 → 취약점 분석 → 공격'이다.

3번: X. 틀린 부분은 '공격 대상 선정 → 취약점 분석 → 공격 → 정보 수집'이다. 취약점 분석은 정보 수집 뒤에 와야 하고, 정보 수집이 공격 뒤로 가면 분석의 근거가 사라진다. 올바르게는 '공격 대상 선정 → 정보 수집 → 취약점 분석 → 공격'이다.

4번: X. 틀린 부분은 '취약점 분석 → 공격 대상 선정'이다. 취약점 분석은 선정된 대상에 대한 정보가 있어야 가능하므로 시작 단계가 될 수 없다. 올바르게는 '공격 대상 선정 → 정보 수집 → 취약점 분석 → 공격'이다.

오답 포인트

정보 수집과 공격 대상 선정을 같은 단계처럼 보거나, 취약점 분석을 정보 수집 없이 독립적으로 할 수 있다고 생각하면 선후관계를 뒤바꾸기 쉽다.

NoteBase

다시 나오면 이렇게 판단

절차형 문제는 먼저 대상을 정하고, 그 대상의 정보를 모으고, 그 정보로 약점을 찾은 뒤, 마지막에 약점을 이용하는 흐름으로 판단하면 된다.

암기 포인트

선정 → 수집 → 분석 → 공격의 흐름이다.

NoteBase

문 15. HTTPS(HTTP over Secure Socket Layer)에 대한 설명으로 가장 옳지 않은 것은?

① 요청 문서의 URL과 문서 내용, HTTP 헤더 내용, 폼 요소 내용은 암호화되지만 쿠키는 암호화되지 않는다.

② HTTPS 연결이 명시되면 포트번호는 기본적으로 443번이 사용되고 SSL이 호출된다.

③ HTTPS를 사용하는 웹 페이지의 URI는 http:// 대신 https://로 시작한다.

④ 1994년에 넷스케이프사에서 HTTPS를 개발하였다.

정답 1번

출제 포인트

이 문제는 HTTPS가 무엇을 암호화하며 어떤 전송 보안 계층 위에서 동작하는지를 묻는다.

핵심 개념

HTTPS는 HTTP를 SSL/TLS 위에서 전달하여 전송 구간의 기밀성과 무결성을 확보하는 방식이다. 시험 포인트는 HTTP 메시지에 포함된 데이터가 보호 대상인지, 기본 포트와 스킴 표기가 무엇인지를 구별하는 데 있다.

선지별 해설

1번(X): 틀린 부분은 '쿠키는 암호화되지 않는다'는 표현이다. HTTPS에서는 쿠키도 HTTP 헤더의 일부이므로 전송 중 함께 암호화된다. 올바르게는 '쿠키를 포함한 HTTP 헤더와 본문 데이터는 TLS로 보호된다'이다.
2번(O): HTTPS는 기본적으로 443번 포트를 사용한다. 선지의 'SSL'은 전통적 표현이며 현재 표준 명칭은 TLS이지만, HTTPS가 SSL/TLS 계층 위에서 동작한다는 취지는 맞다.
3번(O): HTTPS를 사용하는 웹 페이지의 URI는 일반적으로 https://로 시작한다. 이는 HTTP의 http://와 구별되는 가장 기본적인 표기이다.
4번(O): HTTPS는 1990년대 중반 넷스케이프가 SSL과 함께 보급한 기술로 보는 것이 맞다. 시험에서는 1994년 넷스케이프 개발로 정리하는 서술을 옳은 설명으로 본다.

오답 포인트

쿠키를 브라우저 저장정보로만 떠올리면 전송 구간 보호 대상에서 빠진다고 착각하기 쉽다. 이 문항은 쿠키도 HTTP 헤더에 실려 함께 전송된다는 점을 놓치게 만드는 함정을 둔 문제이다.

다시 나오면 이렇게 판단

웹 보안 프로토콜 문제는 먼저 HTTP 메시지에 실제로 실려 가는 항목인지 확인한다. 요청·응답 헤더, 쿠키, 본문처럼 메시지에 포함되는 것은 HTTPS에서 함께 보호되고, 포트 번호와 URI 스킴을 이어서 판단하면 된다.

NoteBase

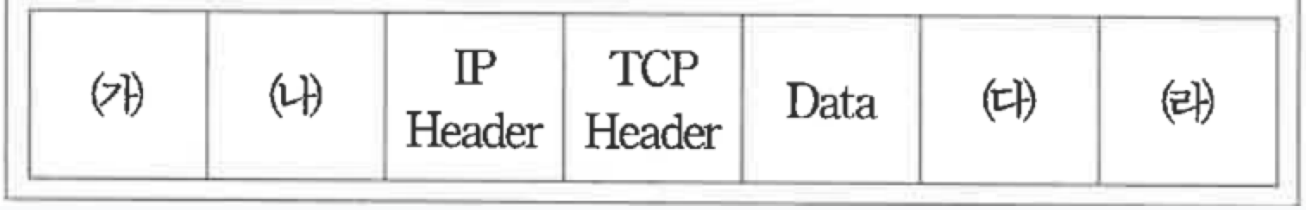
암기 포인트

HTTPS는 443, 스킴은 https, 쿠키도 헤더라서 함께 암호화된다.

NoteBase

문 16. <보기>는 IPv4 패킷에 대해서 IPSec 터널 모드의 ESP(Encapsulation Security Payload) 프로토콜을 적용한 결과이다. (가) ~ (라)에 들어갈 항목들을 가장 옳게 짝지은 것은?

<보기>



① (가): New IP Header, (나): ESP Header, (다): ESP Trailer, (라): ESP Authentication

② (가): ESP Header, (나): New IP Header, (다): ESP Authentication, (라): ESP Trailer

③ (가): New IP Header, (나): ESP Header, (다): ESP Authentication, (라): ESP Trailer

④ (가): ESP Header, (나): New IP Header, (다): ESP Trailer, (라): ESP Authentication

정답 1번

출제 포인트

이 문제는 IPSec ESP 터널 모드에서 New IP Header, ESP Header, ESP Trailer, ESP Authentication의 배치 순서를 묻는 문제이다.

선지별 해설

① O: (가)는 New IP Header, (나)는 ESP Header, (다)는 ESP Trailer, (라)는 ESP Authentication이다. 터널 모드의 전체 순서는 New IP Header -> ESP Header -> 원래 IP Header -> TCP Header -> Data -> ESP Trailer -> ESP Authentication이다.

② X: 'ESP Header'와 'New IP Header'의 위치를 바꾼 점이 틀렸다. 올바르게는 가장 바깥이 New IP Header이고 그 다음이 ESP Header이다. 또한 (다)는 ESP Authentication이 아니라 ESP Trailer이고, (라)는 ESP Trailer가 아니라 ESP Authentication이다.

③ X: (가)와 (나)는 맞지만 뒤쪽 두 항목을 서로 바꾼 점이 틀렸다. 올바르게는 Data 뒤에 ESP Trailer가 먼저 오고, 맨 끝에 ESP Authentication이 온다.

④ X: 앞쪽의 'ESP Header'와 'New IP Header' 위치가 서로 바뀌었고, 뒤쪽의 'ESP Trailer'와 'ESP Authentication' 위치도 서로 바뀌었다. 올바르게는 (가)=New IP Header, (나)=ESP Header, (다)=ESP Trailer, (라)=ESP Authentication이다.

NoteBase

오답 포인트

수험생은 터널 모드와 전송 모드를 혼동하거나, ESP Trailer와 ESP Authentication의 앞뒤를 바꾸어 기억해서 틀리기 쉽다. 이 문항은 원래 IP Header가 ESP 내부에 들어간다는 점과 맨 바깥에 New IP Header가 추가된다는 점을 동시에 확인하는 함정이다.

다시 나오면 이렇게 판단

먼저 원래 IP Header가 보호 대상 내부에 들어가는지 본다. 원래 IP Header까지 내부에 있으면 터널 모드이고, 순서는 New IP Header -> ESP Header -> 원래 IP 패킷 -> ESP Trailer -> ESP Authentication으로 판단된다.

암기 포인트

ESP 터널 모드는 새 IP로 한 번 더 감싸고, 뒤쪽은 Trailer 다음 Authentication 순서이다.

NoteBase

문 17. 디지털 포렌식 수행 절차에 대한 설명으로 가장 옳지 않은 것은?

① 수사 준비 - 디지털 기기의 데이터 수집 및 분석을 위한 장비와 툴을 확보하고 적절한 법적 절차를 거쳐 피의자 또는 수사 대상에 접근한다.

② 증거물 획득 - 디지털 포렌식 수사 현장에서 증거를 획득하는 사람과 그 과정에서 위법 여부의 존재 유무를 감독하는 사람, 인증하는 사람의 참관하에 증거를 획득한다.

③ 분석 및 조사 - 현장에서 획득된 증거인 원본을 다양한 디지털 포렌식 도구를 사용하여 조사 및 분석한다.

④ 보고서 작성 - 분석에 사용한 증거 데이터, 분석 및 조사 과정에서 증거 수집을 위해 문서화한 무결성과 관련된 정보 등을 보고서로 작성한다.

정답 3번

출제 포인트

이 문제는 디지털 포렌식 절차에서 각 단계의 역할과 단계별 산출물을 구분할 수 있는지를 묻는다.

올바른 순서

1. 수사 준비 - 장비와 도구를 확보하고 영장 등 필요한 법적 절차를 갖춘 뒤 대상에 접근하는 단계이다.
2. 증거물 획득 - 현장에서 디지털 증거를 수집하고 무결성 보존과 입회 절차를 관리하는 단계이다.
3. 분석 및 조사 - 수집한 증거의 사본이나 이미지 파일을 대상으로 내용을 해석하고 사실관계를 재구성하는 단계이다.
4. 보고서 작성 - 수집, 분석, 무결성 확인, 절차 기록을 정리해 증거능력을 설명하는 단계이다.

왜 이 순서인가: 현장에서 확보한 증거가 있어야 분석이 가능하고, 분석 결과가 정리되어야 최종 보고서를 작성할 수 있다.

선지별 해설

1번: O. 수사 준비 단계는 포렌식 장비와 도구를 준비하고 영장 등 적법 절차를 갖춘 뒤 대상 시스템에 접근하는 단계이므로 설명이 맞다.

2번: O. 증거물 획득 단계는 현장에서 증거를 수집하면서 누가 수집했고 누가 입회·확인했는지를 남겨 연계보관성을 확보해야 하므로 설명이 타당하다.

3번: X. 틀린 표현은 "현장에서 획득된 증거인 원본을 ... 조사 및 분석한다"이다. 올바르게는 원본은 보존하고, 이미징한 사본이나 복제본을 디지털 포렌식 도구로 분석한다. 원본을 직접 분석 대상으로 쓰면 무결성 훼손 위험이 커진다.

4번: O. 보고서 작성 단계는 사용한 증거 데이터, 분석 과정, 무결성 관련 기록과 결과를 문서화하는 단계이므로 설명이 맞다.

NoteBase

오답 포인트

분석 단계에서 포렌식 도구를 사용한다는 문장만 보고 3번을 맞는 설명으로 보기 쉽다. 그러나 포렌식의 핵심 함정은 도구 사용 여부가 아니라 원본 보존 원칙이며, "원본을 분석한다"라는 표현이 틀린 지점이다.

다시 나오면 이렇게 판단

절차형 문제는 각 단계의 입력물과 산출물을 연결해 판단한다. 현장에서 수집한 증거는 먼저 보존되고, 분석은 그 복제본으로 수행되며, 마지막에 분석 결과와 무결성 기록이 보고서로 정리된다는 흐름을 확인하면 된다.

암기 포인트

디지털 포렌식은 원본 보존, 사본 분석, 결과 보고의 흐름으로 정리된다.

NoteBase

문 18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3에서 정의하고 있는 정보보호 최고책임자가 총괄하는 업무로 가장 옳지 않은 것은?

① 정보보호 실태와 관행의 정기적인 감사 및 개선

② 정보보호 위험의 식별 평가 및 정보보호 대책 마련

③ 개인정보 보호 교육 계획의 수립 및 시행

④ 정보보호 계획의 수립 · 시행 및 개선

정답 3번

쟁점

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보보호 최고책임자가 총괄하는 법정 업무의 범위를 정확한 문언으로 구별하는 문제이다.

용어 풀이

정보보호 최고책임자는 정보통신서비스 제공자의 정보보호 계획, 감사, 위험 식별·평가, 대책 마련, 교육·모의훈련을 총괄하는 책임자이다.

핵심 구분

정보보호 최고책임자의 본래 총괄 업무는 정보보호 계획의 수립·시행·개선, 정보보호 실태와 관행의 정기적 감사 및 개선, 정보보호 위험의 식별·평가 및 대책 마련, 정보보호 교육과 모의 훈련 계획의 수립 및 시행이다. 반면 개인정보 보호책임자의 업무는 별도로 겸할 수 있는 업무일 수는 있어도, 정보보호 최고책임자가 총괄하는 업무 자체의 조문 문언은 아니다.

선지별 해설

① O: 법은 정보보호 최고책임자가 '정보보호 실태와 관행의 정기적인 감사 및 개선' 업무를 총괄한다고 규정한다. 선지 문언이 조문과 일치한다.
② O: 법은 '정보보호 위험의 식별 평가 및 정보보호 대책 마련'을 총괄 업무로 둔다. 위험 식별·평가와 대책 마련을 함께 보는 조문 내용과 같다.
③ X: 틀린 이유는 '개인정보 보호 교육 계획의 수립 및 시행'이라는 표현 때문이다. 법이 정한 총괄 업무는 '정보보호 교육과 모의 훈련 계획의 수립 및 시행'이다. 틀린 표현은 '개인정보 보호 교육 계획'이고, 올바른 표현은 '정보보호 교육과 모의 훈련 계획'이다. 개인정보 보호책임자의 업무를 겸할 수 있는지와, 정보보호 최고책임자의 총괄 업무 문언은 구별해야 한다.
④ O: 법은 '정보보호 계획의 수립·시행 및 개선'을 총괄 업무로 규정한다. 선지가 그대로 옮긴 내용이므로 옳다.

NoteBase

오답 포인트

이 문항은 '정보보호'와 '개인정보 보호'를 일부러 비슷하게 배치해 혼동을 유도한다. 특히 ③은 교육이라는 큰 틀만 보고 넘어가면 맞는 것처럼 보이지만, 실제 조문은 '정보보호 교육과 모의 훈련'까지 포함한다는 점이 함정이다.

다시 나오면 이렇게 판단

정보보호 최고책임자 문제는 먼저 조문상 총괄 업무인지, 겸할 수 있는 다른 법정 업무인지부터 구분하면 된다. 총괄 업무는 정보보호 계획, 감사, 위험 식별·평가와 대책, 교육·모의훈련으로 정리되고, 개인정보 보호 관련 표현이 나오면 별도 업무와의 구별을 먼저 본다.

암기 포인트

CISO 총괄 업무는 계획·감사·위험대책·교육훈련이고, '개인정보 보호 교육' 자체 문언은 아니다.

NoteBase

문 19. 정보보호 및 개인정보보호 관리체계 인증 기준의 보호 대책 요구사항 분야와 항목이 바르게 짝지어진 것으로 옳지 않은 것은?

① 분야: 정보시스템 도입 및 개발 보안, 항목: 운영환경 이관

② 분야: 접근 통제, 항목: 접근권한 검토

③ 분야: 시스템 및 서비스 보안관리, 항목: 정보전송 보안

④ 분야: 시스템 및 서비스 운영관리, 항목: 정보자산의 재사용 및 폐기

정답 2번

출제 포인트

이 문제는 ISMS-P 보호대책 요구사항에서 상위 분야와 세부 항목의 소속 관계를 정확히 매칭할 수 있는지를 묻는다.

핵심 개념

보호대책 요구사항은 상위 분야 아래에 세부 항목이 배치된다. 2.5 인증 및 권한관리는 사용자 인증, 비밀번호 관리, 특수 계정 및 권한관리, 접근권한 검토처럼 계정과 권한의 적정성을 다루고, 2.6 접근통제는 네트워크 접근, 정보시스템 접근, 데이터베이스 접근, 원격접근 통제처럼 접근 경로 자체의 통제를 다룬다.

선지별 해설

1번 O: 운영환경 이관은 2.8 정보시스템 도입 및 개발 보안의 세부 항목 2.8.6에 해당하므로 짝이 맞다.
2번 X: 틀린 부분은 '접근 통제'이다. 접근권한 검토는 2.5 인증 및 권한관리의 세부 항목 2.5.6이므로, 올바르게는 '인증 및 권한관리 - 접근권한 검토'이다.
3번 O: 정보전송 보안은 2.10 시스템 및 서비스 보안관리의 세부 항목 2.10.5이므로 짝이 맞다.
4번 O: 정보자산의 재사용 및 폐기는 2.9 시스템 및 서비스 운영관리의 세부 항목 2.9.7이므로 짝이 맞다.

오답 포인트

접근권한 검토는 이름에 '접근'이 들어가므로 2.6 접근통제로 착각하기 쉽다. 그러나 이 항목의 초점은 네트워크나 시스템 진입 경로의 차단이 아니라 계정과 권한의 부여·변경·삭제 이력 및 적정성 검토라는 점이다.

다시 나오면 이렇게 판단

선지에 권한의 부여·변경·삭제·검토가 나오면 2.5 인증 및 권한관리로 본다. 네트워크, 시스템, 데이터베이스, 원격접속처럼 접근 경로를 통제하면 2.6 접근통제로 본다. 운영환경 이관은 2.8, 정보자산 재사용·폐기는 2.9, 정보전송 보안은 2.10으로 연결한다.

NoteBase

암기 포인트

권한 검토는 2.5, 접근 경로 통제는 2.6, 운영 이관은 2.8, 자산 폐기는 2.9, 전송 보안은 2.10이다.

NoteBase

문 20. <보기>에서 CC(Common Criteria: 공통평가기준)에 대한 설명으로 옳은 것을 모두 고른 것은?

<보기>
ㄱ. CC는 IT 제품의 보안성을 평가하기 위한 국제표준(ISO)으로 국가 간 평가결과를 상호인정하기 위해 미국, 유럽 등 여러 국가의 평가기준을 참조하여 개발한 단일화된 평가기준이다.
ㄴ. CC는 적용범위가 IT 제품에만 한정되지 않으므로 TOE(Target of Evaluation)라는 용어를 사용하며, TOE의 예시로 응용 소프트웨어, 운영체제 + 운영소프트웨어, 스마트카드 IC칩 등이 있다.
ㄷ. 보안목표명세서(Security Target)는 사용자의 보안요구를 표현하기 위해 CC를 준용하여 작성된 것으로 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구사항 집합이다.
ㄹ. 보호프로파일(Protection Profile)은 개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC를 준용하여 작성한 것으로 제품 평가를 위한 기초자료로 사용된다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

정답 1번

출제 포인트

이 문제는 CC에서 TOE, ST, PP의 개념과 작성 주체 및 용도를 정확히 구별할 수 있는지를 묻는다.

핵심 개념

CC는 IT 제품의 보안성을 평가하기 위한 국제 공통평가기준이다.
TOE는 평가 대상 전체를 뜻하며 하드웨어, 소프트웨어, 펌웨어 또는 그 조합이 될 수 있다.
ST는 특정 TOE에 대해 개발자나 공급자가 작성하는 보안목표 명세서로, 그 TOE가 어떤 보안기능과 보안요구사항을 갖는지를 기술한다.
PP는 특정 구현에 종속되지 않는 사용자 측 보안요구사항 문서로, 유사한 TOE 범주에 공통으로 요구되는 보안요구를 정의한다.

NoteBase

선지별 해설

1번 O: ㄱ, ㄴ이 모두 옳으므로 정답이다. ㄱ은 CC가 여러 국가의 평가기준을 통합해 만든 국제 공통평가기준이라는 설명으로 맞다. ㄴ도 TOE가 단일 제품명만이 아니라 평가 대상 전체를 뜻하므로 응용 소프트웨어, 운영체제와 운영소프트웨어의 결합, 스마트카드 IC칩 같은 다양한 형태가 될 수 있다는 점에서 맞다.
2번 X: ㄷ이 틀렸으므로 오답이다. 틀린 부분은 "사용자의 보안 요구를 표현"과 "보안요구사항 집합"을 ST의 설명으로 제시한 점이다. 올바르게는 ST는 특정 TOE에 대해 개발자나 공급자가 작성하는 보안목표 명세서이고, 사용자 측의 공통 보안요구를 정의하는 문서는 PP이다.
3번 X: ㄹ이 틀렸으므로 오답이다. 틀린 부분은 "개발자가 특정 IT 제품의 보안기능을 표현하기 위해 작성"했다는 점과 "제품 평가를 위한 기초자료"라는 점을 PP의 설명으로 제시한 것이다. 올바르게는 PP는 특정 제품이 아닌 TOE 유형에 대한 구현 독립적 보안요구를 정의하는 문서이고, 특정 제품 평가의 직접 기초자료는 ST이다.
4번 X: ㄷ과 ㄹ이 모두 틀렸으므로 오답이다. ㄷ은 ST와 PP의 역할을 바꾸어 설명했고, ㄹ은 PP를 특정 제품용 문서처럼 설명해 ST의 역할과 혼동했다.

오답 포인트

ST와 PP를 모두 "보안요구를 적는 문서"로만 기억하면 주체와 대상 범위를 놓치기 쉽다. 이 문항은 ㄷ에서 사용자 요구 문서인 PP의 성격을 ST에 붙이고, ㄹ에서 특정 TOE용 문서인 ST의 성격을 PP에 붙여 혼동을 유도했다.

다시 나오면 이렇게 판단

CC 문서가 나오면 먼저 문서의 대상이 특정 TOE인지, 특정 TOE 범주 전체인지부터 본다. 특정 제품 평가용 문서이면 ST이고, 구현 독립적인 공통 요구 문서이면 PP이다. 그다음 TOE가 평가 대상 전체를 뜻하는지 확인하면 선택지 판단이 정리된다.

암기 포인트

ST는 특정 TOE, PP는 TOE 유형 전체, TOE는 평가대상, CC는 공통평가기준이다.

NoteBase