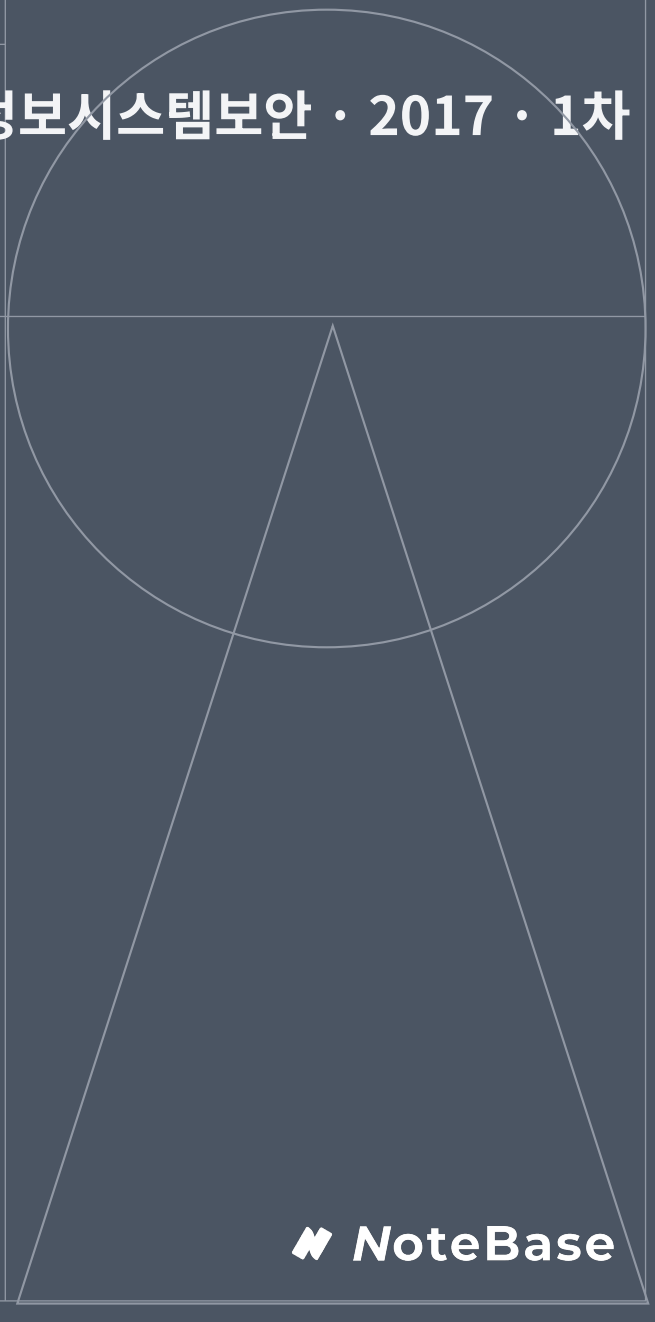
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2017 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2017 · 1차

공무원/해경/일반직 9급 · 정보시스템보안 · 2017 · 1차

문 1. 다음 지문은 데이터베이스에서 키의 유형에 대한 설명이다. 지문에 적합한 키는 무엇인가?

· 여러개의 후보키 중에서 기본키로 선정되고 남은 나머지 키를 지칭
· 기본키를 <학번>으로 선정했다면, <이름, 학과>를 지칭

① Candidate Key
② Primary Key
③ Alternate Key
④ Foreign Key

정답 3번

출제 포인트

이 문제는 후보키 중 기본키로 선택되지 않고 남은 키를 대체키(Alternate Key)라고 한다는 점을 묻는다.

핵심 개념

후보키(Candidate Key)는 한 튜플을 유일하게 식별할 수 있으면서 불필요한 속성이 없는 최소 키이다.
기본키(Primary Key)는 여러 후보키 중 대표로 선택한 키이다.
대체키(Alternate Key)는 후보키 중 기본키로 선택되지 않은 나머지 키이다.
외래키(Foreign Key)는 다른 릴레이션의 기본키 등을 참조하여 릴레이션 사이의 관계를 나타내는 키이다.
따라서 후보키가 <학번>과 <이름, 학과>이고 <학번>을 기본키로 정했다면, 선택되지 않은 <이름, 학과>는 대체키가 된다.

NoteBase

선지별 해설

① X — Candidate Key는 기본키로 선택될 수 있는 모든 후보를 통칭하므로, 기본키로 선정되고 남은 키만을 뜻하지 않는다. 틀린 표현은 'Candidate Key'이며, 올바르게는 'Alternate Key'이다.
② X — Primary Key는 후보키 중 실제로 대표 키로 선정된 키이다. 이 사례에서는 <학번>이 기본키이므로, 남은 <이름, 학과>를 가리키는 표현으로는 맞지 않는다. 틀린 표현은 'Primary Key'이며, 올바르게는 'Alternate Key'이다.
③ O — Alternate Key는 후보키 중 기본키로 채택되지 않은 나머지 키이다. <학번>을 기본키로 선정한 뒤 남은 후보키 <이름, 학과>가 이에 해당한다.
④ X — Foreign Key는 다른 릴레이션의 키를 참조하여 릴레이션 간 관계를 연결하는 속성이다. 지문에는 다른 릴레이션을 참조한다는 내용이 없다. 틀린 표현은 'Foreign Key'이며, 올바르게는 'Alternate Key'이다.

오답 포인트

'여러 후보키 중'이라는 문구만 보고 Candidate Key를 고르기 쉽다. 그러나 결정적인 표현은 '기본키로 선정되고 남은 나머지 키'이며, 이는 후보키의 하위 구분인 대체키를 뜻한다.

다시 나오면 이렇게 판단

먼저 유일성과 최소성을 만족하는 키들을 후보키로 묶는다. 그중 선택된 하나는 기본키, 선택되지 않은 나머지는 대체키로 판단한다. 다른 릴레이션의 키를 참조한다는 내용이 있을 때만 외래키로 판단한다.

암기 포인트

후보키 중 선택된 것은 기본키, 선택되지 않고 남은 것은 대체키이다.

NoteBase

문 2. 다음 설명하는 키 교환 알고리즘은 무엇인가?

1976년 미국 스탠퍼드 대학의 연구원이 개발한 것으로 공개키는 한 개의 정수와 한 개의 소수로 구성되어 있으며, 통신 직전에 통신 상대방과 공유하도록 해두고, 다른 비밀키 전용의 숫자를 통신 상대방 양쪽에서 각각 갖도록 해서, 이들과 공개키의 수치를 사용하여 공통 암호키용 수치를 산출한다.

① DES

② Diffie-Hellman

③ AES

④ SEED

정답 2번

출제 포인트

1976년 공개된 Diffie-Hellman 방식의 특징인 공개 매개변수와 각자의 비밀값을 이용한 공통 비밀키 합의를 식별하는 문제이다.

핵심 개념

Diffie-Hellman은 통신 당사자가 공개된 값과 각자 보관하는 비밀값을 이용해 같은 공유 비밀을 만드는 키 교환 방식이다. 암호문을 직접 만드는 대칭키 블록 암호가 아니라, 안전하지 않은 통신로에서 공통 키를 합의하기 위한 방식이라는 점이 핵심이다.
DES·AES·SEED는 송신자와 수신자가 같은 비밀키로 암호화와 복호화를 수행하는 대칭키 블록 암호이다.

선지별 해설

① X — DES는 64비트 블록을 처리하는 대칭키 블록 암호로, 공개값과 각자의 비밀값으로 공통 키를 산출하는 키 교환 알고리즘이 아니다. 틀린 표현은 'DES'이며, 설명에 해당하는 올바른 알고리즘은 Diffie-Hellman이다.
② O — Diffie-Hellman은 1976년에 발표되었으며, 공개된 소수와 생성원 등의 매개변수 및 양측이 각각 정한 비밀값을 이용해 동일한 공유 비밀을 계산하는 키 교환 방식이다.
③ X — AES는 동일한 비밀키를 사용하는 대칭키 블록 암호 표준으로, 그 자체가 Diffie-Hellman과 같은 키 교환 알고리즘은 아니다. 틀린 표현은 'AES'이며, 올바르게는 Diffie-Hellman이다.
④ X — SEED는 국내에서 개발된 128비트 대칭키 블록 암호로, 공개 매개변수와 개인 비밀값으로 공통 키를 합의하는 방식이 아니다. 틀린 표현은 'SEED'이며, 올바르게는 Diffie-Hellman이다.

NoteBase

오답 포인트

지문에 '공통 암호키'가 나온다는 이유만으로 암호화 알고리즘인 DES·AES·SEED를 고르기 쉽다. 그러나 지문의 핵심은 데이터를 암호화하는 것이 아니라 통신 양측이 각자의 비밀값을 공개하지 않고 동일한 키를 산출한다는 데 있다.

다시 나오면 이렇게 판단

'공개된 소수·생성원', '양측의 개별 비밀값', '공통 비밀 산출'이 함께 제시되면 Diffie-Hellman 키 교환으로 판단한다. 반면 DES·AES·SEED는 이미 공유된 하나의 비밀키로 데이터를 암호화하는 대칭키 블록 암호로 구분한다.

암기 포인트

Diffie-Hellman은 키를 합의하고, DES·AES·SEED는 데이터 블록을 암호화한다.

NoteBase

문 3. 다음 중 대칭키(비밀키) 암호화 기반의 알고리즘이 아닌 것은?

① DES(Data Encryption Standard)

② ECC(Elliptic Curve Cryptosystem)

③ IDEA(International Data Encryption Algorithm)

④ AES(Advanced Encryption Standard)

정답 2번

출제 포인트

대칭키 암호와 공개키 암호를 구분하고 대표 알고리즘을 분류하는 문제이다.

핵심 개념

대칭키 암호는 암호화와 복호화에 동일한 비밀키를 사용하는 방식이며, DES·IDEA·AES가 이에 속한다. 공개키 암호는 공개키와 개인키의 서로 다른 키 쌍을 사용하며, 타원곡선의 수학적 성질을 이용하는 ECC가 이에 속한다.

선지별 해설

① X — DES는 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 블록 암호이다. 이 문항에서 DES를 '대칭키 암호가 아닌 알고리즘'으로 분류하는 것은 틀리며, 올바르게는 대칭키 암호 알고리즘이다.
② O — ECC는 타원곡선 위의 연산을 이용하는 공개키 암호 방식이다. 공개키와 개인키의 키 쌍을 사용하므로 대칭키 암호화 기반의 알고리즘이 아니다.
③ X — IDEA는 128비트 비밀키를 사용하는 대칭키 블록 암호이다. 이 문항에서 IDEA를 '대칭키 암호가 아닌 알고리즘'으로 분류하는 것은 틀리며, 올바르게는 대칭키 암호 알고리즘이다.
④ X — AES는 128비트 블록을 처리하는 대표적인 대칭키 블록 암호이다. 이 문항에서 AES를 '대칭키 암호가 아닌 알고리즘'으로 분류하는 것은 틀리며, 올바르게는 대칭키 암호 알고리즘이다.

오답 포인트

선지에 제시된 명칭이 모두 암호 알고리즘이므로 용도만 보고 고르면 혼동하기 쉽다. 이 문항의 핵심은 알고리즘의 이름이 아니라 사용하는 키의 구조이며, ECC만 공개키와 개인키의 쌍을 사용한다.

다시 나오면 이렇게 판단

알고리즘을 먼저 키 구조로 분류한다. DES·IDEA·AES는 하나의 비밀키를 공유하는 대칭키 암호이고, ECC는 공개키와 개인키를 사용하는 공개키 암호이다. 부정형 질문에서는 이 분류와 다른 하나를 정답으로 선택한다.

암기 포인트

DES·IDEA·AES는 대칭키, ECC는 공개키이다.

NoteBase

문 4. 다음 중 세마포어에 대한 설명으로 가장 옳지 않은 것은?

① 여러 개의 프로세스가 동시에 그 값을 수정하지 못한다.

② 상호배제 문제를 해결하기 위해 사용된다.

③ 세마포어에 대한 연산은 처리 중에 인터럽트 되어야 한다.

④ 다익스트라(E.J. Dijkstra)가 제안한 방법이다.

정답 3번

출제 포인트

세마포어의 목적과 세마포어 연산이 갖추어야 할 원자성을 묻는 문제이다.

핵심 개념

세마포어는 공유 자원에 접근하는 프로세스나 스레드를 제어하기 위한 동기화 도구이다. 세마포어 값은 wait(P)와 signal(V) 같은 정해진 연산으로 변경되며, 이 연산은 실행 도중 끊기지 않는 원자적 연산이어야 한다.

선지별 해설

① O — 세마포어 값의 검사와 변경은 원자적으로 수행되므로 여러 프로세스가 동시에 그 값을 수정할 수 없다.
② O — 세마포어는 임계구역에 동시에 진입할 수 있는 프로세스를 제한하므로 상호배제 문제를 해결하는 데 사용된다.
③ X — 틀린 표현은 '처리 중에 인터럽트 되어야 한다'이다. 세마포어 연산은 경쟁 상태가 발생하지 않도록 처리 중에 인터럽트되지 않는 원자적 연산이어야 한다.
④ O — 세마포어는 다익스트라(E. J. Dijkstra)가 제안한 프로세스 동기화 방법이다.

오답 포인트

③은 동시 실행을 제어하는 세마포어가 인터럽트를 활용한다는 인상을 주지만, 핵심은 반대이다. 세마포어 값을 검사하고 변경하는 도중 다른 실행 흐름이 끼어들지 않아야 한다.

다시 나오면 이렇게 판단

세마포어 연산에 '중단된다', '인터럽트된다', '동시에 수정할 수 있다'는 표현이 나오면 원자성에 어긋나는지 판단한다. 상호배제와 프로세스 동기화는 세마포어의 올바른 용도이다.

암기 포인트

세마포어는 동기화와 상호배제에 쓰이며, wait와 signal 연산은 원자적이다.

NoteBase

문 5. 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

가. MBR - 부팅 매체에 대한 기본적인 파일시스템 정보를 읽는다.
나. POST - 하드웨어 자체의 시스템에 문제가 없는지 체크한다.
다. NTLDR - 하드디스크 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며, BOOT.INI 파일의 내용을 읽는다.
라. NTDETECT.COM - 설치된 하드웨어를 검사한다.
마. NTOSKRNL.EXE - HAL.dll을 로드한다.
바. CMOS - 사용자가 설정한 기본사항을 읽어 시스템에 적용한다.

① 바-다-라-가-마-나
② 나-바-가-다-라-마
③ 나-바-다-라-가-마
④ 바-가-마-나-다-라

정답 2번

출제 포인트

이 문제는 윈도우 부팅 과정에서 하드웨어 점검과 설정 적용, 부팅 정보 확인, 운영체제 로더 실행, 하드웨어 검색, 커널 적재가 이어지는 순서를 묻는다.

올바른 순서

1. POST(나) — 전원이 켜지면 하드웨어가 정상적으로 동작하는지 자체 점검한다.
2. CMOS(바) — 사용자가 설정한 기본 하드웨어 정보를 읽어 시스템에 적용한다.
3. MBR(가) — 부팅 매체의 부팅 정보와 파티션 정보를 확인해 운영체제 로더로 제어를 넘긴다.
4. NTLDR(다) — BOOT.INI의 부팅 구성을 읽고 윈도우 로딩을 시작한다.
5. NTDETECT.COM(라) — 설치된 하드웨어를 검색한다.
6. NTOSKRNL.EXE(마) — 윈도우 커널이 실행되며 HAL.dll 등 핵심 구성 요소를 적재한다.

왜 이 순서: 하드웨어 점검과 기본 설정이 끝나야 부팅 장치를 사용할 수 있고, 부팅 정보가 확인되어야 운영체제 로더가 실행되며, 로더가 하드웨어 정보를 수집한 뒤 커널을 적재할 수 있기 때문이다.

NoteBase

선지별 해설

① X — '바-다-라-가-마-나'는 CMOS 다음에 곧바로 NTLDR를 실행하고 POST를 마지막에 둔 부분이 틀렸다. POST는 부팅 초기에 수행되어야 하고, NTLDR보다 먼저 MBR을 거쳐야 한다. 올바르게는 '나-바-가-다-라-마'이다.
② O — POST로 하드웨어를 점검한 뒤 CMOS 설정을 적용하고, MBR에서 NTLDR로 제어를 넘긴 다음 NTDETECT.COM이 하드웨어를 검색하고 NTOSKRNL.EXE가 적재되는 순서이다.
③ X — '나-바-다-라-가-마'는 NTLDR와 NTDETECT.COM을 MBR보다 앞에 둔 부분이 틀렸다. 부팅 매체의 MBR 단계가 먼저 수행된 뒤 NTLDR와 NTDETECT.COM이 이어져야 한다. 올바르게는 '나-바-가-다-라-마'이다.
④ X — '바-가-마-나-다-라'는 POST를 MBR과 커널 적재 뒤에 둔 부분과 NTOSKRNL.EXE를 NTLDR보다 앞에 둔 부분이 틀렸다. 하드웨어 자체 점검인 POST가 먼저이고, 커널은 NTLDR 및 NTDETECT.COM 이후에 적재된다. 올바르게는 '나-바-가-다-라-마'이다.

오답 포인트

POST와 CMOS의 선후관계, MBR과 NTLDR의 선후관계를 뒤섞기 쉽다. 특히 ③은 앞부분 '나-바'가 맞지만 운영체제 로더인 NTLDR를 부팅 정보 확인 단계인 MBR보다 먼저 배치한 것이 함정이다.

다시 나오면 이렇게 판단

부팅 순서는 '하드웨어 점검 → 기본 설정 적용 → 부팅 정보 확인 → 운영체제 로더 실행 → 하드웨어 검색 → 커널 적재'의 의존관계로 판단한다.

암기 포인트

POST → CMOS → MBR → NTLDR → NTDETECT.COM → NTOSKRNL.EXE, 즉 '점검-설정-부팅 정보-로더-하드웨어 검색-커널' 순서이다.

NoteBase

문 6. 다음 괄호 안에 공통으로 들어갈 적당한 단어는?

( )은/는 하드웨어 특성으로부터 프로그램들을 격리시키고, 하드웨어와 직접적으로 상호 작동함으로써 프로그램들에게 일관된 서비스를 제공한다. ( )의 기본개념은 프로세스와 파일의 관리이다. 그밖에 입출력장치 관리, 메모리 관리 및 시스템 호출 인터페이스 등이다.

① 유틸리티(Utilities)

② 커널(Kernel)

③ 쉘(Shell)

④ 데몬(Daemon)

정답 2번

출제 포인트

하드웨어를 직접 제어하면서 프로세스·파일·입출력장치·메모리·시스템 호출을 관리하는 운영체제의 핵심 구성요소를 구별하는 문제이다.

핵심 개념

커널은 운영체제의 핵심 부분으로, 하드웨어와 직접 상호 작용하여 응용 프로그램에 일관된 자원 관리 서비스를 제공한다.
유틸리티는 시스템 관리나 특정 작업을 돕는 보조 프로그램이고, 쉘은 사용자 명령을 해석하는 인터페이스이며, 데몬은 백그라운드에서 지속적으로 서비스를 제공하는 프로세스이다.

선지별 해설

① X — 유틸리티는 파일 관리, 압축, 진단 등 특정 작업을 지원하는 보조 프로그램이다. 틀린 표현은 '유틸리티'이며, 하드웨어와 직접 상호 작용하면서 프로세스·파일·메모리 등을 관리하는 것은 커널이다.
② O — 커널은 하드웨어를 추상화하여 프로그램을 하드웨어의 세부 특성으로부터 격리하고, 프로세스·파일·입출력장치·메모리 및 시스템 호출 인터페이스를 관리한다.
③ X — 쉘은 사용자의 명령을 해석하여 운영체제에 전달하는 명령 해석기이다. 틀린 표현은 '쉘'이며, 하드웨어와 직접 상호 작용하고 핵심 자원을 관리하는 것은 커널이다.
④ X — 데몬은 사용자와 직접 상호 작용하지 않고 백그라운드에서 대기하며 특정 서비스를 제공하는 프로세스이다. 틀린 표현은 '데몬'이며, 운영체제의 중심에서 하드웨어와 자원을 관리하는 것은 커널이다.

오답 포인트

쉘과 데몬도 운영체제 환경에서 동작하므로 커널과 혼동하기 쉽다. 그러나 '하드웨어와 직접 상호 작용', '프로세스·메모리 관리', '시스템 호출 인터페이스'가 함께 제시되면 커널을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

하드웨어 제어와 핵심 자원 관리는 커널, 사용자 명령 해석은 쉘, 백그라운드 서비스는 데몬, 보조 작업 수행은 유틸리티로 구분한다.

암기 포인트

커널은 핵심 자원 관리, 쉘은 명령 해석, 데몬은 백그라운드 서비스, 유틸리티는 보조 기능이다.

NoteBase

문 7. 다음 중 오버플로우에 대한 설명 중 가장 옳지 않은 것은?

① 버퍼에 저장된 프로세스 간의 자원 경쟁을 통해 권한을 획득하여 공격하는 방법이다.

② 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀주소를 조작하는 기법을 사용한다.

③ 스택 오버플로우와 힙 오버플로우 공격이 있다.

④ 버퍼 오버플로우가 발생하면 저장된 데이터는 인접한 변수 영역 및 포인터 영역까지 침범함으로 해커가 원하는 특정코드를 실행하도록 할 수 있다.

정답 1번

출제 포인트

버퍼 오버플로우의 발생 원리와 대표 유형을 자원 경쟁에 따른 경쟁 상태 공격과 구별하는 문제이다.

핵심 개념

버퍼 오버플로우는 프로그램이 확보한 버퍼의 경계를 넘는 데이터를 기록하여 인접한 메모리 영역을 훼손하는 취약점이다. 이로 인해 제어 정보나 포인터가 변조되면 비정상 동작이나 공격자가 의도한 코드 실행으로 이어질 수 있다. 반면 경쟁 상태 공격은 여러 프로세스나 스레드가 공유 자원에 접근하는 순서와 시점의 허점을 이용한다.

선지별 해설

① X — 틀린 부분은 '프로세스 간의 자원 경쟁을 통해' 공격한다는 표현이다. 이는 공유 자원의 접근 시점이나 실행 순서를 악용하는 경쟁 상태 공격에 해당한다. 올바르게는 버퍼의 저장 용량을 초과하는 데이터를 기록하여 인접 메모리나 제어 정보를 변조하는 공격이라고 해야 한다.
② O — 특히 스택 버퍼 오버플로우에서는 버퍼의 크기를 넘는 입력이 저장된 복귀 주소까지 덮어써 프로그램의 제어 흐름을 조작할 수 있다.
③ O — 버퍼가 위치한 메모리 영역에 따라 대표적으로 스택 오버플로우와 힙 오버플로우로 구분한다.
④ O — 경계를 넘은 데이터가 인접 변수나 포인터 등 다른 메모리 영역을 침범하면 제어 흐름이 변조되어 공격자가 의도한 코드를 실행하게 할 수 있다.

오답 포인트

①의 '자원 경쟁'은 보안 공격이라는 공통점 때문에 버퍼 오버플로우와 혼동하기 쉽지만, 핵심 원인이 메모리 경계 초과가 아니라 실행 시점과 순서의 허점이라는 점이 다르다.

다시 나오면 이렇게 판단

선지에 용량 초과, 인접 메모리 침범, 복귀 주소·포인터 변조가 나오면 버퍼 오버플로우로 판단한다. 공유 자원, 프로세스·스레드 간 경쟁, 검사 시점과 사용 시점의 차이가 나오면 경쟁 상태로 구별한다.

NoteBase

암기 포인트

버퍼 오버플로우는 경계 초과와 메모리 침범, 경쟁 상태는 공유 자원과 실행 시점 경쟁이다.

NoteBase

문 8. 다음 중 개인 식별 방법이 아닌 것은?

① 사용자의 공개키를 이용하는 방법

② 사용자의 고유의 물리적 특성을 이용하는 방법

③ 사용자가 알고 있는 정보를 이용하는 방법

④ 사용자가 소지하고 있는 것을 이용하는 방법

정답 1번

출제 포인트

개인 식별·인증에 사용하는 세 가지 기본 요소인 지식, 소지, 생체 특성을 구별하는 문제이다.

핵심 개념

지식 기반 인증은 사용자가 알고 있는 정보로 확인하는 방식이며 비밀번호·PIN 등이 해당한다. 소지 기반 인증은 사용자가 가진 물건으로 확인하는 방식이며 보안 토큰·스마트카드 등이 해당한다. 생체 기반 인증은 지문·홍채처럼 사용자 고유의 신체적 또는 행동적 특성으로 확인하는 방식이다. 공개키 암호에서는 공개키가 누구나 알 수 있도록 공개되는 정보이므로 공개키 자체만으로 사용자를 식별하지 않으며, 사용자는 대응하는 개인키를 보유하고 있음을 전자서명 등으로 증명한다.

선지별 해설

① X — 사용자의 공개키는 공개되어도 되는 정보이므로 그 자체만으로 해당 사용자를 인증할 수 없다. 틀린 표현은 '사용자의 공개키를 이용'한다는 부분이며, 올바르게는 공개키 암호 기반 인증에서 사용자가 대응하는 개인키를 소지하고 있음을 증명하고 검증자가 공개키로 이를 확인한다고 해야 한다.
② O — 지문, 홍채, 얼굴과 같은 사용자의 고유한 물리적 특성을 이용하는 것은 생체 기반 개인 식별 방법이다.
③ O — 비밀번호나 PIN처럼 사용자만 알고 있는 정보를 이용하는 것은 지식 기반 개인 식별 방법이다.
④ O — 스마트카드나 보안 토큰처럼 사용자가 소지한 것을 이용하는 것은 소지 기반 개인 식별 방법이다.

오답 포인트

공개키가 특정 사용자와 연결되어 있다는 사실과 공개키 자체가 인증 비밀이라는 생각을 혼동하기 쉽다. 실제 인증 능력은 공개된 공개키가 아니라 그 공개키에 대응하는 개인키를 통제하고 있음을 증명하는 데서 나온다.

다시 나오면 이렇게 판단

인증 수단을 '알고 있는 것', '가지고 있는 것', '사용자 자체의 특성'으로 나눈 뒤 선지를 대조한다. 공개키 방식이 나오면 공개키 자체가 아니라 대응하는 개인키의 보유 증명이 인증의 핵심인지 확인한다.

NoteBase

암기 포인트

지식·소지·생체가 기본 인증요소이며, 공개키는 검증에 쓰이고 개인키 보유가 증명된다.

NoteBase

문 9. 게시판에 악성 스크립트를 삽입해서 쿠키, 개인정보 전송, 악성코드 다운로드 등을 수행할 수 있는 공격기법은 무엇인가?

① Web Shell

② XSS

③ 쿠키/세션 위조

④ SQL Injection

정답 2번

출제 포인트

게시판에 삽입한 악성 스크립트가 이용자의 브라우저에서 실행되는 공격을 XSS로 식별하는 문제이다.

핵심 개념

XSS(Cross-Site Scripting)는 웹 페이지에 악성 스크립트를 삽입하여 그 페이지를 열어 본 이용자의 브라우저에서 실행되게 하는 공격이다. 게시판처럼 저장된 글에 스크립트를 넣어 여러 이용자에게 실행시키는 형태는 저장형 XSS에 해당한다. 이 공격으로 쿠키·세션 정보나 개인정보가 외부로 전송되거나 악성코드 다운로드가 유도될 수 있다.

선지별 해설

① X — Web Shell은 공격자가 서버에 설치하거나 업로드한 악성 서버 측 프로그램을 통해 원격 명령을 실행하는 수단이다. 게시판에 삽입한 스크립트가 이용자의 브라우저에서 실행되는 공격이라는 표현은 Web Shell이 아니라 XSS로 고쳐야 한다.
② O — XSS는 웹 페이지에 악성 스크립트를 삽입해 이용자의 브라우저에서 실행되도록 하며, 쿠키 탈취·개인정보 전송·악성코드 다운로드 유도 등을 일으킬 수 있다.
③ X — 쿠키/세션 위조는 탈취하거나 추측한 인증 정보 등을 조작해 다른 이용자인 것처럼 인증받는 공격이다. 게시판에 악성 스크립트를 삽입하는 공격이라는 표현은 쿠키/세션 위조가 아니라 XSS로 고쳐야 한다. 쿠키 탈취는 XSS의 결과가 될 수 있지만 공격기법 자체의 이름은 다르다.
④ X — SQL Injection은 입력값에 악의적인 SQL 구문을 넣어 데이터베이스의 조회·변조·삭제나 인증 우회를 시도하는 공격이다. 게시판에 악성 스크립트를 삽입해 브라우저에서 실행시키는 공격이라는 표현은 SQL Injection이 아니라 XSS로 고쳐야 한다.

오답 포인트

문제에 쿠키가 언급되어 ③을 고르기 쉽지만, 쿠키는 공격의 결과로 탈취되는 대상이다. 공격을 구분하는 핵심은 악성 스크립트가 게시판에 삽입되고 이용자의 브라우저에서 실행된다는 점이다.

NoteBase

다시 나오면 이렇게 판단

브라우저에서 악성 스크립트가 실행되면 XSS, 서버에서 원격 명령을 실행하면 Web Shell, 인증용 쿠키나 세션 값을 조작하면 쿠키/세션 위조, 데이터베이스에 악성 SQL 구문을 전달하면 SQL Injection으로 판단한다.

암기 포인트

게시판의 악성 스크립트 → 이용자 브라우저에서 실행 → XSS이다.

NoteBase

문 10. 다음 지문 중 괄호에 들어갈 포트번호를 적절하게 나열하고 있는 것은?

· SMTP는 전자우편을 보내는 데 사용되는 기본 프로토콜로서 TCP (㉠)번 포트를 사용한다.
· POP3 데몬 포트는 TCP (㉡)번을 사용해 메일 서버에서 전자우편을 내려 받는다.

① ㉠: 25, ㉡: 100
② ㉠: 25, ㉡: 110
③ ㉠: 80, ㉡: 100
④ ㉠: 143, ㉡: 110

정답 2번

출제 포인트

전자우편 프로토콜인 SMTP와 POP3가 기본으로 사용하는 TCP 포트 번호를 구별하는 문제이다.

핵심 개념

SMTP는 전자우편을 보내거나 메일 서버 사이에서 전달할 때 사용하는 프로토콜이며 기본 TCP 포트는 25번이다.
POP3는 메일 서버에 저장된 전자우편을 클라이언트로 내려받을 때 사용하는 프로토콜이며 기본 TCP 포트는 110번이다.

선지별 해설

① X — ㉠의 SMTP 25번은 맞지만 ㉡의 POP3를 100번으로 제시한 부분이 틀리다. 올바르게는 '㉠: 25, ㉡: 110'이다.
② O — SMTP의 기본 TCP 포트는 25번이고 POP3의 기본 TCP 포트는 110번이므로 두 값이 모두 맞다.
③ X — ㉠의 SMTP를 80번, ㉡의 POP3를 100번으로 제시한 부분이 모두 틀리다. 올바르게는 '㉠: 25, ㉡: 110'이다. 80번은 일반적으로 HTTP의 기본 포트이다.
④ X — ㉠의 SMTP를 143번으로 제시한 부분이 틀리다. 올바르게는 '㉠: 25, ㉡: 110'이다. 143번은 일반적으로 IMAP의 기본 포트이며, POP3의 110번과 구별된다.

오답 포인트

메일 수신 프로토콜인 POP3와 IMAP을 혼동하면 110번과 143번을 바꾸기 쉽다. 또한 80번은 웹 통신에 쓰이는 HTTP의 기본 포트이므로 SMTP와 연결되지 않는다.

NoteBase

다시 나오면 이렇게 판단

메일 발송·전달은 SMTP 25번, 서버에서 메일을 내려받는 것은 POP3 110번으로 대응시킨다. 서버의 메일을 동기화하며 관리하는 IMAP 143번과도 구분한다.

암기 포인트

SMTP 25, POP3 110, IMAP 143이다.

NoteBase

문 11. 유닉스 파일시스템의 i-Node가 가지고 있지 않는 정보는 무엇인가?

① 파일 유형

② 파일 수정시각

③ 파일의 링크 수

④ 파일의 이름

정답 4번

출제 포인트

유닉스 파일시스템에서 i-Node에 저장되는 파일 메타데이터와 디렉터리 엔트리에 저장되는 파일 이름을 구분하는 문제이다.

핵심 개념

i-Node는 파일 유형과 권한, 소유자, 크기, 시각 정보, 링크 수, 데이터 블록 위치 등 파일의 메타데이터를 저장한다. 파일 이름은 i-Node가 아니라 디렉터리 엔트리에 i-Node 번호와 함께 저장된다. 따라서 하나의 i-Node를 가리키는 하드 링크마다 서로 다른 파일 이름을 사용할 수 있다.

선지별 해설

① X — 파일 유형은 i-Node의 모드 정보에 포함된다. 이 선지를 올바르게 고치면 '파일 유형은 i-Node가 가지고 있는 정보이다'가 된다.
② X — 파일 수정시각은 i-Node에 저장되는 시각 정보이다. 이 선지를 올바르게 고치면 '파일 수정시각은 i-Node가 가지고 있는 정보이다'가 된다.
③ X — 파일의 링크 수는 해당 i-Node를 가리키는 하드 링크의 수로서 i-Node에 저장된다. 이 선지를 올바르게 고치면 '파일의 링크 수는 i-Node가 가지고 있는 정보이다'가 된다.
④ O — 파일의 이름은 디렉터리 엔트리에 저장되고, i-Node에는 저장되지 않는다. 따라서 i-Node가 가지고 있지 않은 정보에 해당한다.

오답 포인트

파일을 식별할 때 이름을 사용한다는 일상적 관점 때문에 파일 이름도 i-Node에 들어 있다고 착각하기 쉽다. 그러나 유닉스 파일시스템은 디렉터리의 '파일 이름 → i-Node 번호' 연결과 i-Node의 파일 메타데이터를 분리한다.

NoteBase

다시 나오면 이렇게 판단

파일 이름은 디렉터리 엔트리, 파일의 속성과 데이터 위치는 i-Node라는 기준으로 판단한다. 서로 다른 이름의 하드 링크가 같은 i-Node를 가리킬 수 있다는 사실을 적용하면 파일 이름이 i-Node 정보가 아님을 바로 구별할 수 있다.

암기 포인트

이름은 디렉터리, 속성은 i-Node이다.

NoteBase

문 12. MS오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성코드는?

① 애드웨어
② 트로이 목마
③ 백도어
④ 매크로 바이러스

정답 4번

출제 포인트

응용 프로그램의 문서에 포함된 매크로·스크립트 실행 기능을 악용하는 악성코드의 종류를 구별하는 문제이다.

핵심 개념

매크로 바이러스는 워드프로세서나 스프레드시트 문서 및 서식 파일의 매크로 기능을 이용하여 실행·전파되는 악성코드이다.
애드웨어는 광고 노출, 트로이 목마는 정상 프로그램 위장, 백도어는 인증 절차를 우회하는 비밀 접근 통로가 핵심이다.

선지별 해설

① X — 애드웨어는 주로 광고를 자동으로 표시하거나 광고 목적으로 이용 정보를 수집하는 소프트웨어이다. 문서에 삽입된 스크립트 실행 환경을 악용한다는 설명에 해당하지 않으며, 올바른 용어는 매크로 바이러스이다.
② X — 트로이 목마는 유용하거나 정상적인 프로그램으로 위장하여 사용자가 실행하도록 유도한 뒤 악성 기능을 수행한다. 문서의 매크로 기능을 악용하는 악성코드라는 표현은 트로이 목마가 아니라 매크로 바이러스에 해당한다.
③ X — 백도어는 정상적인 인증·접근 통제를 우회하여 시스템에 몰래 접근할 수 있도록 만든 통로 또는 기능이다. 문서 파일의 스크립트 실행 환경을 악용하는 유형이라는 표현은 백도어가 아니라 매크로 바이러스에 해당한다.
④ O — 매크로 바이러스는 MS 오피스와 같은 응용 프로그램의 문서에 매크로 형태로 삽입되어, 문서를 열거나 특정 동작을 할 때 실행될 수 있다. 문제의 설명과 정확히 일치한다.

오답 포인트

선지들이 모두 악성 행위와 관련된 용어이지만, 문제의 결정적 단서는 '응용 프로그램의 문서 파일'과 '스크립트 형태의 실행 환경'이다. 프로그램으로 위장하는 트로이 목마나 접근 통제를 우회하는 백도어와 혼동하면 안 된다.

NoteBase

다시 나오면 이렇게 판단

문서 파일과 매크로·스크립트 실행 기능이 함께 제시되면 매크로 바이러스로 판단한다. 정상 프로그램 위장은 트로이 목마, 비밀 우회 접근은 백도어, 광고 표시는 애드웨어로 구별한다.

암기 포인트

문서 속 매크로는 매크로 바이러스, 정상 프로그램 위장은 트로이 목마, 몰래 들어가는 통로는 백도어이다.

NoteBase

문 13. 다음 지문의 괄호 안에 들어갈 용어를 순서대로 나열한 것은?

공개키 알고리즘으로 정보화 서비스와 전자서명 서비스를 제공할 때 암호화에 사용하는 키는 수신자의 ( )이고, 전자서명에서 서명 검증에 사용하는 키는 송신자의 ( )이다.

① 개인키, 개인키
② 개인키, 공개키
③ 공개키, 개인키
④ 공개키, 공개키

정답 4번

출제 포인트

공개키 암호화에서 기밀성을 확보하는 키와 전자서명을 검증하는 키가 각각 누구의 어떤 키인지 묻는 문제이다.

핵심 개념

공개키 암호화: 송신자가 수신자의 공개키로 암호화하고, 수신자가 자신의 개인키로 복호화한다.
전자서명: 송신자가 자신의 개인키로 서명하고, 수신자가 송신자의 공개키로 서명을 검증한다.
따라서 정보의 기밀성을 위한 암호화와 서명 검증에는 모두 공개키를 사용하지만, 각 공개키의 소유자는 각각 수신자와 송신자이다.

선지별 해설

① X — 첫 번째 '개인키'와 두 번째 '개인키'가 모두 틀렸다. 암호화에는 수신자의 공개키를, 서명 검증에는 송신자의 공개키를 사용하므로 '공개키, 공개키'가 맞다.
② X — 첫 번째 '개인키'가 틀렸다. 수신자만 복호화할 수 있도록 암호화할 때는 수신자의 공개키를 사용하므로 '공개키, 공개키'가 맞다.
③ X — 두 번째 '개인키'가 틀렸다. 송신자의 개인키는 서명 생성에 사용하고, 서명 검증에는 송신자의 공개키를 사용하므로 '공개키, 공개키'가 맞다.
④ O — 정보 암호화에는 수신자의 공개키를 사용하고, 전자서명 검증에는 송신자의 공개키를 사용한다. 두 괄호 모두 공개키가 들어간다.

오답 포인트

암호화와 복호화, 서명 생성과 서명 검증의 키를 뒤바꾸는 것이 함정이다. 수신자의 개인키는 복호화에 사용하고, 송신자의 개인키는 서명 생성에 사용한다. 문제에서 묻는 단계는 암호화와 서명 검증이므로 둘 다 공개키이다.

NoteBase

다시 나오면 이렇게 판단

기밀성 문제는 '수신자 공개키로 잠그고 수신자 개인키로 연다'로 판단한다. 전자서명 문제는 '송신자 개인키로 서명하고 송신자 공개키로 검증한다'로 판단한다.

암기 포인트

암호화는 수신자 공개키, 서명 검증은 송신자 공개키이다.

NoteBase

문 14. 대칭키 암호 알고리즘과 공개키 암호 알고리즘에 대한 설명 중 가장 잘못된 것은?

① 대칭키 암호 알고리즘은 실행 속도가 빠르기 때문에 다양한 암호의 핵심함수로 사용된다.

② 공개키 암호 알고리즘은 자신만이 보관하는 비밀키를 이용하여 인증, 전자서명 등에 적용이 가능하다.

③ 대칭키 암호의 경우 키를 자주 변경해야 하는 불편함이 있다.

④ 대칭키 암호 알고리즘은 비밀키 공유를 위한 키 분배가 필요하지 않으면서도 암호화 및 복호화의 속도가 빠르다.

정답 4번

출제 포인트

대칭키 암호와 공개키 암호를 키의 구성, 처리 속도, 키 분배, 인증·전자서명 기능의 차이로 구별하는 문제이다.

핵심 개념

대칭키 암호는 송신자와 수신자가 같은 비밀키를 공유하여 암호화와 복호화를 수행하는 방식이다. 처리 속도가 빠르지만, 통신 전에 비밀키를 안전하게 전달하고 관리해야 한다.
공개키 암호는 서로 대응하는 공개키와 비밀키를 사용하는 방식이다. 일반적으로 공개키로 암호화한 정보는 비밀키로 복호화하며, 비밀키로 전자서명을 생성하고 공개키로 이를 검증할 수 있다.

선지별 해설

① O — 대칭키 암호는 공개키 암호보다 연산 부담이 작고 처리 속도가 빨라 대용량 데이터 암호화 등 여러 암호 시스템의 핵심 암호화 기능에 사용된다.
② O — 공개키 암호 방식에서는 소유자만 보관하는 비밀키로 전자서명을 생성할 수 있으며, 상대방은 공개키로 서명을 검증하여 인증과 무결성을 확인할 수 있다.
③ O — 대칭키가 노출되면 해당 키로 보호한 통신이 위험해지므로 키를 주기적으로 교체해야 하며, 상대방과 공유한 키를 함께 갱신해야 하는 관리상 불편이 있다.
④ X — 틀린 표현은 '비밀키 공유를 위한 키 분배가 필요하지 않다'이다. 대칭키 암호는 암호화와 복호화에 사용할 동일한 비밀키를 통신 당사자들이 미리 안전하게 공유해야 하므로 키 분배가 필요하다. 다만 암호화와 복호화 속도가 빠르다는 부분은 옳다.

오답 포인트

④는 대칭키 암호의 장점인 빠른 처리 속도와 단점인 키 분배 문제를 한 문장에 섞었다. 속도가 빠르다는 이유로 키 분배까지 불필요한 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

‘같은 비밀키를 공유한다’가 보이면 대칭키 암호이므로 빠른 속도와 안전한 키 분배의 필요성을 함께 판단한다.
‘공개키·비밀키 쌍’이나 ‘전자서명’이 보이면 공개키 암호의 성질을 판단한다.

암기 포인트

대칭키는 빠르지만 키 분배가 필요하고, 공개키는 키 쌍을 이용해 암호화와 전자서명을 지원한다.

NoteBase

문 15. 다음 지문의 프로그램은 주로 어떤 용도로 사용되는가?

Nmap, Hping, PortQry

① 스캔 공격
② DoS 공격
③ Sniffing 공격
④ Session Hijacking 공격

정답 1번

출제 포인트

Nmap, Hping, PortQry의 공통된 주된 용도가 네트워크 호스트·포트·서비스 탐색이라는 점을 묻는 문제이다.

핵심 개념

스캔 공격은 대상 시스템에 탐색 패킷을 보내 응답을 분석함으로써 살아 있는 호스트, 열린 포트, 제공 서비스 등의 정보를 수집하는 행위이다. Nmap은 네트워크·포트 탐색, Hping은 사용자가 구성한 TCP/IP 패킷을 이용한 응답 확인과 방화벽 시험, PortQry는 TCP·UDP 포트 상태 질의에 주로 사용된다.

선지별 해설

① O — 세 프로그램은 공통적으로 패킷을 보내고 응답이나 포트 상태를 확인하여 대상 네트워크의 호스트·포트 정보를 탐색하는 데 활용되므로 스캔 용도에 해당한다.
② X — 틀린 표현은 'DoS 공격'이다. DoS는 대량의 트래픽이나 요청으로 자원을 고갈시켜 서비스를 방해하는 공격이며, 제시된 프로그램들의 공통된 주된 용도는 포트와 호스트를 탐색하는 스캔이다.
③ X — 틀린 표현은 'Sniffing 공격'이다. Sniffing은 네트워크를 흐르는 패킷을 가로채 내용을 수집·분석하는 행위이며, 제시된 도구들은 주로 탐색 패킷을 보내 응답과 포트 상태를 확인하는 스캔 도구이다.
④ X — 틀린 표현은 'Session Hijacking 공격'이다. 세션 하이재킹은 이미 성립된 통신 세션의 식별 정보나 연결 상태를 탈취해 세션을 가로채는 공격이며, 제시된 프로그램들의 공통 용도는 네트워크 스캔이다.

오답 포인트

Hping이 임의 패킷 생성이나 부하 유발에도 악용될 수 있다는 점 때문에 ②와 혼동하기 쉽다. 그러나 세 도구를 함께 제시한 경우에는 개별 도구의 부수 기능이 아니라 공통 기능인 호스트·포트 탐색을 기준으로 판단한다.

NoteBase

다시 나오면 이렇게 판단

도구 묶음 문제에서는 각 도구가 공통으로 수행하는 동작을 찾는다. 포트 상태와 응답을 확인하면 스캔, 통신 내용을 수동으로 가로채면 스니핑, 자원을 고갈시키면 DoS, 성립된 연결을 탈취하면 세션 하이재킹으로 구분한다.

암기 포인트

Nmap·Hping·PortQry의 공통어는 '탐색 패킷과 포트 확인', 즉 스캔이다.

NoteBase

문 16. 메시지에 대한 불법적인 공격자의 위협에는 수동적 공격과 능동적 공격이 있는데 다음 중 가장 올바르게 짝지어진 것은?

① 수동적 공격 - 삽입 공격

② 수동적 공격 - 재생 공격

③ 능동적 공격 - 메시지 변조

④ 능동적 공격 - 트래픽 분석

정답 3번

출제 포인트

이 문제는 공격자가 메시지나 시스템 자원에 변화를 일으키는지를 기준으로 수동적 공격과 능동적 공격을 구분하는 문제이다.

핵심 개념

수동적 공격은 통신 내용을 엿듣거나 통신량·송수신 관계를 관찰하여 정보를 얻지만 데이터 자체에는 변화를 가하지 않는 공격이다. 대표 유형은 메시지 내용 공개와 트래픽 분석이다.
능동적 공격은 메시지를 삽입·삭제·변조하거나 과거 메시지를 다시 보내는 등 데이터나 시스템 동작에 변화를 일으키는 공격이다. 대표 유형은 가장, 재생, 메시지 변조, 서비스 거부이다.

선지별 해설

① X — 삽입 공격은 공격자가 새로운 메시지나 데이터를 통신 과정에 끼워 넣어 내용을 변화시키므로 능동적 공격이다. 틀린 표현은 '수동적 공격'이며, 올바르게는 '능동적 공격 - 삽입 공격'이다.
② X — 재생 공격은 이전에 전송된 정상 메시지를 가로챈 뒤 다시 전송하여 인증이나 거래 절차에 영향을 주므로 능동적 공격이다. 틀린 표현은 '수동적 공격'이며, 올바르게는 '능동적 공격 - 재생 공격'이다.
③ O — 메시지 변조는 전송 중인 메시지의 내용, 순서 또는 일부를 바꾸는 행위로 데이터에 직접 변화를 일으키므로 능동적 공격이다.
④ X — 트래픽 분석은 메시지 내용을 해독하지 못하더라도 통신량, 빈도, 시점, 송수신 관계 등을 관찰하여 정보를 추론하는 수동적 공격이다. 틀린 표현은 '능동적 공격'이며, 올바르게는 '수동적 공격 - 트래픽 분석'이다.

오답 포인트

'도청처럼 몰래 수행되는가'가 아니라 데이터나 시스템 상태를 실제로 바꾸는가가 구분 기준이다. 재생 공격은 과거 메시지를 그대로 보낼 뿐 내용을 고치지 않을 수 있지만, 메시지를 다시 주입하여 통신 절차에 영향을 주므로 능동적 공격이다.

NoteBase

다시 나오면 이렇게 판단

관찰·도청·분석에 그치면 수동적 공격으로, 삽입·재전송·변조·방해처럼 통신 내용이나 시스템 동작에 영향을 주면 능동적 공격으로 판단한다.

암기 포인트

수동은 엿보기와 분석, 능동은 넣기·다시 보내기·바꾸기·막기이다.

NoteBase

문 17. 다음 중 커버로스(Kerberos)에서 재전송 공격을 막기 위해 사용하는 것은 무엇인가?

① 인증정보

② 쿠키

③ 타임스탬프

④ 세션키

정답 3번

출제 포인트

이 문제는 Kerberos가 이미 전송된 인증 메시지를 공격자가 가로채 다시 보내는 재전송 공격을 어떤 정보로 탐지하는지 묻는다.

핵심 개념

Kerberos는 인증자(authenticator)에 타임스탬프를 포함하고 서버가 허용된 시간 범위와 재사용 여부를 확인하여 메시지의 신선성(freshness)을 검증한다. 오래되었거나 이미 사용된 타임스탬프의 인증 요청은 거부되므로 재전송 공격을 막을 수 있다. 이를 위해 클라이언트와 서버의 시계 동기화가 중요하다.

선지별 해설

① X — 인증정보는 사용자나 주체의 신원을 확인하는 데 쓰이는 정보를 넓게 가리킬 뿐, 재전송 여부를 판별하는 구체적인 수단이 아니다. 틀린 표현은 '인증정보'이며, 올바르게는 인증자에 포함된 '타임스탬프'를 사용한다.
② X — 쿠키는 주로 웹 환경에서 클라이언트의 상태나 세션 식별 정보를 저장하는 수단이며, Kerberos의 재전송 방지 수단이 아니다. 틀린 표현은 '쿠키'이며, 올바르게는 '타임스탬프'이다.
③ O — Kerberos는 인증자에 포함된 타임스탬프를 검사하여 허용 시간 범위를 벗어나거나 이미 처리된 인증 요청을 거부하므로 재전송 공격을 방지한다.
④ X — 세션키는 통신 당사자가 안전한 세션을 위해 공유하는 암호키로, 메시지의 기밀성과 인증에 활용되지만 그 자체만으로 과거 메시지의 재전송 여부를 판별하지는 못한다. 틀린 표현은 '세션키'이며, 재전송 방지에 직접 사용하는 것은 '타임스탬프'이다.

오답 포인트

세션키도 Kerberos의 핵심 요소이므로 ④를 고르기 쉽다. 그러나 재전송 공격의 판단 기준은 암호화 여부가 아니라 요청이 지금 생성된 것인지에 관한 신선성이며, 이를 제공하는 정보가 타임스탬프이다.

다시 나오면 이렇게 판단

Kerberos에서 공격 유형과 방어 수단을 연결한다. 도청·내용 노출에는 암호화와 세션키가 관련되고, 과거 인증 메시지의 재사용에는 시간의 신선성을 확인하는 타임스탬프가 관련된다.

NoteBase

암기 포인트

Kerberos 재전송 방지 = 인증자의 타임스탬프 + 시계 동기화이다.

NoteBase

문 18. 다음에서 설명하는 것은 무엇인가?

재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식이다. 구축 및 유지비용이 저렴하나 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요된다.

① 중복 사이트

② 핫(Hot) 사이트

③ 웜(Warm) 사이트

④ 콜드(Cold) 사이트

정답 3번

출제 포인트

재해복구센터가 보유한 정보기술자원의 범위와 복구 소요 시간으로 중복·핫·웜·콜드 사이트를 구별하는 문제이다. 중요 자원만 부분적으로 갖추고 완전한 복구까지 다소 시간이 걸린다는 표현이 웜 사이트의 핵심이다.

핵심 개념

중복 사이트: 주센터의 시스템과 데이터를 동일하게 복제하여 주센터 장애 시에도 업무를 거의 연속적으로 이어갈 수 있는 방식이다.
핫 사이트: 주센터와 같은 수준의 정보기술자원을 갖추고 데이터를 최신 상태에 가깝게 유지하여 신속하게 복구하는 방식이다.
웜 사이트: 중요성이 높은 정보기술자원만 부분적으로 갖추어 비용을 줄이는 대신 초기 복구가 완전하지 않고 완전 복구까지 시간이 필요한 방식이다.
콜드 사이트: 전력·통신·공간 같은 기본 시설을 마련하지만 정보기술자원은 즉시 운영할 수준으로 갖추지 않아 복구에 가장 긴 시간이 필요한 방식이다.

NoteBase

선지별 해설

① X — 중복 사이트는 주센터의 시스템과 데이터를 동일하게 복제하여 업무 연속성을 매우 높이는 방식이므로, 중요 자원만 부분적으로 보유한다는 지문과 맞지 않는다. 틀린 대응은 '중복 사이트'이며, 올바르게는 '웜 사이트'이다.
② X — 핫 사이트는 주센터와 같은 수준의 정보기술자원을 갖추어 신속한 복구가 가능하므로, 초기 복구가 불완전하고 완전 복구까지 다소 시간이 걸린다는 지문과 맞지 않는다. 틀린 대응은 '핫 사이트'이며, 올바르게는 '웜 사이트'이다.
③ O — 웜 사이트는 중요성이 높은 정보기술자원만 부분적으로 보유한다. 구축·유지비용은 비교적 낮지만 완전한 복구까지 다소 시간이 걸리므로 지문의 설명과 정확히 일치한다.
④ X — 콜드 사이트는 기본 시설 중심으로 준비하고 정보기술자원을 즉시 운영할 수준으로 갖추지 않는 방식이다. 지문처럼 중요 정보기술자원을 부분적으로 보유하는 방식은 콜드 사이트가 아니라 웜 사이트이다. 틀린 대응은 '콜드 사이트'이며, 올바르게는 '웜 사이트'이다.

오답 포인트

'구축 및 유지비용이 저렴하다'만 보고 가장 저렴한 콜드 사이트를 고르기 쉽다. 그러나 지문에는 중요 정보기술자원을 '부분적으로 보유'한다고 되어 있으므로 장비 준비 수준이 콜드보다 높은 웜 사이트이다.

다시 나오면 이렇게 판단

정보기술자원의 준비 정도를 먼저 확인한다. 동일 복제는 중복 사이트, 동일 수준의 자원과 신속 복구는 핫 사이트, 중요 자원의 부분 보유와 다소 긴 복구는 웜 사이트, 기본 시설 중심의 준비와 가장 긴 복구는 콜드 사이트로 판단한다.

암기 포인트

웜은 중요 자원만 부분 준비한다. 비용은 낮아지지만 완전 복구에는 시간이 걸린다.

NoteBase

문 19. FTP 연결 방식과 관련된 다음 설명 중 가장 옳지 않은 것은?

① FTP 모드에는 active와 passive 모드가 있다.

② FTP 클라이언트에서 FTP 서버 방향으로 데이터 연결을 개시하는 것이 active 모드이다.

③ active 모드를 사용할지 passive 모드를 사용할지 결정하는 것은 FTP 클라이언트이다.

④ passive 모드에서 데이터 전송을 위해서는 서버와 클라이언트 모두 1024번 이후의 포트를 사용한다.

정답 2번

출제 포인트

FTP의 active 모드와 passive 모드를 데이터 연결의 개시 주체와 사용 포트로 구분하는 문제이다.

핵심 개념

FTP는 명령을 주고받는 제어 연결과 파일·목록을 주고받는 데이터 연결을 별도로 사용한다.
active 모드: 서버가 클라이언트 쪽으로 데이터 연결을 개시한다. 전통적으로 서버는 데이터 연결에 20번 포트를 사용하고, 클라이언트는 1024번 이후의 포트를 연다.
passive 모드: 클라이언트가 서버 쪽으로 데이터 연결을 개시한다. 서버와 클라이언트 모두 데이터 연결에 1024번 이후의 포트를 사용한다.

선지별 해설

① O — FTP의 데이터 연결 방식에는 active 모드와 passive 모드가 있다.
② X — 틀린 부분은 'FTP 클라이언트에서 FTP 서버 방향으로 데이터 연결을 개시하는 것이 active 모드'라는 표현이다. 실제로 클라이언트가 서버 방향으로 데이터 연결을 개시하는 방식은 passive 모드이며, active 모드에서는 서버가 클라이언트 방향으로 데이터 연결을 개시한다.
③ O — 클라이언트가 active 모드에 해당하는 PORT 명령 또는 passive 모드에 해당하는 PASV 명령을 선택하여 보내므로 사용할 모드를 결정하는 쪽은 클라이언트이다.
④ O — passive 모드에서는 클라이언트가 자신의 1024번 이후 포트에서 서버가 지정한 1024번 이후 포트로 데이터 연결을 개시한다.

오답 포인트

②는 제어 연결의 방향과 데이터 연결의 방향을 혼동하게 만든다. FTP 제어 연결은 두 모드 모두 클라이언트가 서버의 21번 포트로 시작하지만, 모드를 구분하는 기준은 별도의 데이터 연결을 누가 시작하는지이다.

다시 나오면 이렇게 판단

데이터 연결의 화살표만 확인한다. 서버에서 클라이언트 방향이면 active 모드이고, 클라이언트에서 서버 방향이면 passive 모드이다.

NoteBase

암기 포인트

active는 서버가 데이터 연결을 개시하고, passive는 클라이언트가 데이터 연결을 개시한다.

NoteBase

문 20. 침입을 당했을 때 로그파일을 비롯한 여러 파일의 환경설정이나 접근권한, 일부 파일이 변조나 삭제가 된다. 시스템이 변조되기 전에 헤더 값의 checksum을 저장하는 파일의 변조, 삭제 시 원래의 파일과 비교 대조할 수 있는 피해 분석 도구는?

① snort

② tcpdump

③ netstat

④ tripwire

정답 4번

출제 포인트

침입 전 파일의 기준 정보와 침입 후 상태를 비교하여 파일 변조·삭제를 탐지하는 파일 무결성 점검 도구를 묻는 문제이다.

핵심 개념

Tripwire는 정상 상태의 파일 해시값과 속성 정보를 기준 데이터베이스에 저장한 뒤 현재 상태와 비교하여 파일의 변경·변조·삭제를 탐지하는 파일 무결성 점검 도구이다.
Snort는 네트워크 트래픽을 규칙과 대조해 침입을 탐지하는 도구이고, tcpdump는 패킷을 수집·출력하는 도구이며, netstat는 네트워크 연결과 통계 정보를 확인하는 도구이다.

선지별 해설

① X — snort는 네트워크 패킷을 분석하여 침입 징후를 탐지하는 네트워크 침입 탐지 도구이다. 파일의 기준 checksum과 현재 파일을 비교하는 도구라는 표현은 틀리며, 올바른 도구는 tripwire이다.
② X — tcpdump는 네트워크 인터페이스를 지나는 패킷을 캡처하고 내용을 확인하는 도구이다. 파일 변조·삭제를 기준값과 대조하는 도구라는 표현은 틀리며, 올바른 도구는 tripwire이다.
③ X — netstat는 활성 네트워크 연결, 수신 대기 포트, 라우팅 및 인터페이스 통계 등을 확인하는 도구이다. 파일 무결성을 검사하는 도구라는 표현은 틀리며, 올바른 도구는 tripwire이다.
④ O — tripwire는 파일의 정상 상태에서 해시값과 속성 정보를 저장하고, 이후 상태와 비교하여 변조나 삭제 여부를 확인하므로 문제의 피해 분석 목적에 부합한다.

오답 포인트

침입 탐지·분석에 쓰이는 보안 도구라는 공통점만 보고 snort나 tcpdump를 고르기 쉽다. 문제의 결정적 표현은 '시스템 변조 전 checksum 저장'과 '원래 파일과 비교 대조'이며, 이는 네트워크 패킷 분석이 아니라 파일 무결성 검사 기능이다.

NoteBase

다시 나오면 이렇게 판단

기준 해시값을 저장한 뒤 파일의 변경 여부를 비교하면 tripwire, 탐지 규칙으로 네트워크 침입을 감시하면 snort, 패킷 자체를 캡처하면 tcpdump, 현재 연결·포트 상태를 확인하면 netstat로 구분한다.

암기 포인트

파일 무결성은 tripwire, 침입 탐지는 snort, 패킷 캡처는 tcpdump, 연결 상태는 netstat이다.

NoteBase