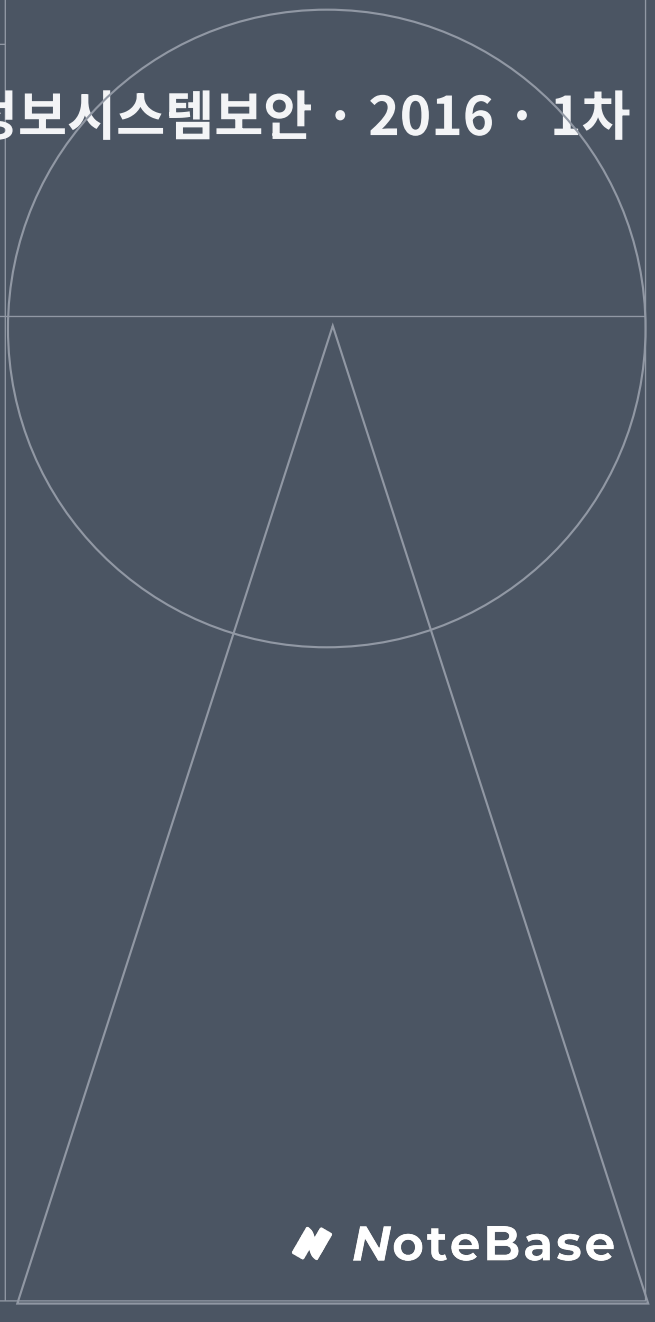
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2016 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2016 · 1차

공무원/해경/일반직 9급 · 정보시스템보안 · 2016 · 1차

문 1. 다음 중 프로세스 스케줄링을 통한 CPU 성능요소가 아닌 것은?

① CPU 이용률(Utilization)

② 시스템처리율(Throughput)

③ 대기시간(Waiting time)

④ 확장성(Expansibility)

정답 4번

출제 포인트

프로세스 스케줄링 알고리즘의 성능을 평가하는 기준과 일반적인 시스템 특성을 구별하는 문제이다.

핵심 개념

CPU 스케줄링 성능 평가는 CPU가 일한 비율, 단위 시간당 완료한 작업 수, 프로세스가 준비 큐에서 기다린 시간 등으로 판단한다. CPU 이용률과 처리율은 높을수록, 대기시간은 짧을수록 바람직하다. 확장성은 자원이나 부하가 늘어날 때 시스템이 처리 능력을 얼마나 잘 확대할 수 있는지를 뜻하는 일반적인 시스템 특성이다.

선지별 해설

① O — CPU 이용률은 전체 시간 중 CPU가 작업을 수행한 시간의 비율이므로 스케줄링 성능 평가 요소이다.
② O — 시스템 처리율은 단위 시간 동안 완료된 프로세스의 수이므로 스케줄링 성능 평가 요소이다.
③ O — 대기시간은 프로세스가 준비 큐에서 CPU 할당을 기다린 총시간이므로 스케줄링 성능 평가 요소이다.
④ X — 틀린 표현은 '확장성'이다. 확장성은 자원이나 작업 부하가 증가할 때 시스템의 처리 능력을 확대할 수 있는 성질이며, 통상적인 CPU 스케줄링 성능 평가 요소가 아니다. 올바르게는 반환시간이나 응답시간 등이 CPU 스케줄링의 대표적인 성능 평가 요소에 해당한다.

오답 포인트

④의 확장성도 넓은 의미에서는 시스템 성능과 관련되지만, 스케줄링 알고리즘이 CPU를 얼마나 효율적이고 신속하게 배분하는지를 직접 측정하는 기준은 아니다. '시스템 성능과 관련된 용어'와 'CPU 스케줄링의 평가 지표'를 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

선지가 CPU의 바쁜 정도, 완료 작업 수, 완료까지 걸린 시간, 준비 큐의 대기시간, 최초 응답까지의 시간을 직접 측정하면 스케줄링 평가 기준으로 판단한다. 시스템 규모 확대에 대한 적응 능력을 묻는 확장성은 별도의 시스템 특성으로 구별한다.

암기 포인트

CPU 스케줄링은 이용률·처리율은 높게, 반환시간·대기시간·응답시간은 짧게 평가한다. 확장성은 스케줄링의 대표 평가 기준이 아니다.

NoteBase

문 2. 다음 중 컴퓨터 바이러스의 발전단계에 대한 설명으로 가장 적절하지 않은 것은?

① 원시형 바이러스 : 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스

② 암호화 바이러스 : 바이러스 프로그램 전체 또는 일부를 암호화 시켜 저장하는 바이러스

③ 갑옷형 바이러스 : 백신 개발을 지연시키기 위해 다양한 암호화 기법을 사용하는 바이러스

④ 매크로 바이러스 : 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스

정답 1번

출제 포인트

컴퓨터 바이러스의 발전 단계별 유형을 구분하고, 각 유형의 구조와 감염 대상을 정확히 연결하는 문제이다.

핵심 개념

원시형 바이러스는 구조가 단순하고 코드의 크기가 일정하여 분석하기 쉬운 초기 형태이다. 암호화 바이러스는 바이러스 코드의 전부 또는 일부를 암호화한 형태로 저장한다. 갑옷형 바이러스는 암호화·난독화 기법 등으로 분석을 어렵게 하여 백신 개발을 지연시킨다. 매크로 바이러스는 문서 작성 프로그램 등의 매크로 기능을 이용하여 문서나 서식 파일을 감염시킨다.

선지별 해설

① X — 원시형 바이러스는 구조가 단순하고 분석하기 쉽지만, 크기가 가변적인 바이러스가 아니라 고정된 크기를 갖는 바이러스이다. 틀린 표현은 '가변 크기'이며, 올바르게는 '고정 크기'이다.
② O — 암호화 바이러스는 백신의 탐지를 어렵게 하기 위해 바이러스 프로그램의 전부 또는 일부를 암호화한 상태로 저장한다.
③ O — 갑옷형 바이러스는 다양한 암호화·난독화 기법으로 역분석을 어렵게 하여 백신 프로그램의 개발을 지연시키는 유형이다.
④ O — 매크로 바이러스는 워드프로세서나 스프레드시트처럼 매크로를 지원하는 프로그램의 문서·서식 파일을 감염시킨다.

오답 포인트

①은 '단순하고 분석하기 쉽다'는 설명은 맞지만 '가변 크기'가 틀린 혼합형 선지이다. 가변적인 형태로 탐지를 피하는 특징을 초기의 원시형 바이러스와 혼동하면 안 된다.

다시 나오면 이렇게 판단

유형명과 핵심 표지를 연결한다. 원시형은 단순·고정 크기, 암호화형은 코드 암호화, 갑옷형은 분석 방해, 매크로형은 문서·서식 감염으로 판단한다.

NoteBase

암기 포인트

원시형은 단순·고정, 암호화형은 코드 암호화, 갑옷형은 분석 방해, 매크로형은 문서 감염이다.

NoteBase

문 3. 다음 중 인터넷 익스플로러의 인터넷 옵션에 대한 설명으로 가장 옳지 않은 것은?

① 임시 인터넷 파일 폴더에 있는 쿠키를 삭제할 수 있다.

② 임시 인터넷 파일의 폴더는 변경할 수 있으나, 할당할 디스크 공간의 크기를 변경할 수 없다.

③ 인터넷 영역에 적용할 보안 수준을 설정할 수 있다.

④ 인터넷 영역에 대한 개인정보 설정을 선택할 수 있다.

정답 2번

출제 포인트

이 문제는 Internet Explorer의 인터넷 옵션에서 임시 인터넷 파일, 보안 영역, 개인정보 설정을 각각 관리할 수 있는지를 묻는 문제이다.

핵심 개념

인터넷 옵션은 검색 기록과 임시 인터넷 파일을 관리하고, 영역별 보안 수준과 개인정보 보호 수준을 설정하는 기능이다. 임시 인터넷 파일 설정에서는 저장 폴더의 위치뿐 아니라 사용할 디스크 공간의 크기도 조정할 수 있다.

선지별 해설

① O — 인터넷 옵션의 검색 기록 삭제 기능을 이용하면 저장된 쿠키를 삭제할 수 있다.
② X — 틀린 부분은 '할당할 디스크 공간의 크기를 변경할 수 없다'이다. 임시 인터넷 파일의 저장 폴더를 변경할 수 있을 뿐 아니라, 사용할 디스크 공간의 크기도 변경할 수 있다.
③ O — 보안 탭에서 인터넷 영역을 선택하고 그 영역에 적용할 보안 수준을 설정할 수 있다.
④ O — 개인정보 탭에서 인터넷 영역의 개인정보 보호 수준을 선택하여 쿠키 처리 방식 등을 설정할 수 있다.

오답 포인트

②는 폴더 위치 변경 기능만 인정하고 디스크 공간 크기 조정 기능을 부정하는 데 함정이 있다. 두 항목은 모두 임시 인터넷 파일 설정에서 변경할 수 있다.

다시 나오면 이렇게 판단

인터넷 옵션의 기능을 '검색 기록·임시 파일 관리', '영역별 보안 수준', '개인정보·쿠키 관리'로 나누어 판단한다. 임시 인터넷 파일 설정에는 저장 위치와 디스크 공간 크기 조정이 함께 포함된다.

암기 포인트

임시 인터넷 파일은 폴더 위치도, 디스크 공간 크기도 변경할 수 있다.

NoteBase

문 4. 다음은 운영체제의 보안을 위한 분리 중에서 어떤 분리에 대한 설명인지 보기 중에서 고르시오

프로그램의 접근을 제한하여 허용된 영역 밖의 객체에 대해 접근하지 못하게 한다.

① 암호적 분리
② 물리적 분리
③ 시간적 분리
④ 논리적 분리

정답 4번

출제 포인트

운영체제의 보안 분리 방식 중 프로그램의 접근 가능 범위를 제한하는 방식을 구별하는 문제이다.

핵심 개념

논리적 분리는 운영체제의 접근 통제 기능으로 프로그램마다 허용된 객체와 주소 영역을 구분하는 방식이다.
암호적 분리는 정보를 암호화하여 올바른 키를 가진 주체만 내용을 이용하게 하는 방식이다.
물리적 분리는 서로 다른 보안 영역이 별도의 물리적 장치나 자원을 사용하게 하는 방식이다.
시간적 분리는 보안 수준이 다른 프로세스나 작업이 같은 자원을 서로 다른 시간에 사용하게 하는 방식이다.

선지별 해설

① X — 암호적 분리는 데이터 등을 암호화하여 키가 있는 주체만 내용을 이용하게 하는 방식이다. 제시문의 '프로그램의 접근을 허용된 영역으로 제한'하는 방식은 암호적 분리가 아니라 논리적 분리이다.
② X — 물리적 분리는 보안 영역별로 장치나 자원을 물리적으로 따로 두는 방식이다. 제시문처럼 운영체제의 접근 통제로 영역을 구분하는 것은 논리적 분리이다.
③ X — 시간적 분리는 같은 자원을 서로 다른 시간에 사용하도록 실행 시점을 나누는 방식이다. 제시문은 사용 시간을 나누는 것이 아니라 프로그램의 접근 가능 영역을 제한하므로 논리적 분리이다.
④ O — 논리적 분리는 운영체제가 프로그램의 접근 권한과 주소 영역을 제한하여 허용된 영역 밖의 객체에 접근하지 못하게 하는 방식이다.

오답 포인트

'분리'라는 말만 보고 물리적으로 공간을 나누는 ②를 고르기 쉽다. 그러나 제시문의 핵심 표현은 '프로그램의 접근을 제한'과 '허용된 영역 밖의 객체에 접근하지 못하게 한다'이며, 이는 접근 권한과 영역을 소프트웨어적으로 구분하는 논리적 분리이다.

NoteBase

다시 나오면 이렇게 판단

분리의 수단을 확인한다. 별도 장치·자원이면 물리적 분리, 사용 시점이 다르면 시간적 분리, 암호와 키를 사용하면 암호적 분리, 운영체제가 접근 권한이나 주소 영역을 제한하면 논리적 분리이다.

암기 포인트

장치는 물리, 시점은 시간, 키는 암호, 접근 권한과 영역은 논리이다.

NoteBase

문 5. 안티루트킷의 주요 기능이 아닌 것은 무엇인가?

① 숨긴 파일 찾기

② 수정된 레지스트리 찾기

③ 보호해제된 프로세스 탐지

④ 로그파일 수정

정답 4번

출제 포인트

안티루트킷이 루트킷의 은폐·변조 흔적을 탐지하는 방어 도구인지, 공격자가 흔적을 없애는 기능인지 구분하는 문제이다.

핵심 개념

루트킷은 파일·프로세스·레지스트리 등의 존재나 변조 흔적을 숨겨 침입 상태를 유지하는 악성 도구이다. 안티루트킷은 정상적인 시스템 정보와 실제 상태를 비교하여 이러한 은폐·변조를 찾아내고 제거하는 보안 도구이다. 로그파일을 수정하여 흔적을 지우는 행위는 탐지 기능이 아니라 공격자의 흔적 은폐 행위이다.

선지별 해설

① O — 숨긴 파일 찾기는 파일 시스템에 존재하지만 일반 조회에서 보이지 않도록 은폐된 파일을 탐지하는 기능이므로 안티루트킷의 주요 기능이다.
② O — 수정된 레지스트리 찾기는 루트킷이 자동 실행이나 은폐를 위해 바꾼 레지스트리 항목과 비정상 흔적을 탐지하는 기능이므로 안티루트킷의 주요 기능이다.
③ O — 보호해제된 프로세스 탐지는 프로세스의 보호 상태가 비정상적으로 변경되거나 정상적인 조회 결과에서 감춰진 이상을 찾아내는 기능이므로 안티루트킷의 탐지 범위에 해당한다.
④ X — 틀린 표현은 '로그파일 수정'이다. 로그파일을 수정하거나 삭제하여 침입 흔적을 감추는 것은 루트킷 등 공격 도구가 수행할 수 있는 행위이다. 올바르게는 안티루트킷이 로그와 시스템 상태의 이상 징후를 검사하여 루트킷을 탐지한다고 해야 한다.

오답 포인트

④의 '로그파일'이라는 보안 관련 대상만 보고 탐지 기능으로 오인하기 쉽다. 그러나 동사가 '탐지·검사'가 아니라 '수정'이므로 방어 도구의 기능이 아니라 공격 흔적을 은폐하는 행위이다.

다시 나오면 이렇게 판단

파일·레지스트리·프로세스의 숨김이나 변조를 찾아내는 행위는 안티루트킷 기능으로 판단한다. 반대로 로그를 수정·삭제하여 흔적을 없애는 행위는 루트킷 또는 공격자의 기능으로 판단한다.

NoteBase

암기 포인트

안티루트킷은 은폐·변조를 찾고, 루트킷은 흔적을 숨긴다.

NoteBase

문 6. 다음은 정보 보호의 목표 중 하나를 설명하는 것이다. 괄호안에 들어갈 적당한 말을 보기에서 고르시오

(____)은 정보의 내용이 불법적으로 변경되거나 삭제되지 않고 완전한 일치성을 유지하여 본래의 목적대로 사용되는 성질을 의미한다.

① 기밀성
② 인증성
③ 무결성
④ 가용성

정답 3번

출제 포인트

정보 보호의 목표인 기밀성·인증성·무결성·가용성을 정의의 핵심어로 구별하는 문제이다. 지문의 '불법적으로 변경되거나 삭제되지 않음'과 '완전한 일치성'은 무결성을 가리킨다.

핵심 개념

기밀성은 허가받지 않은 사람이 정보에 접근하거나 내용을 알지 못하게 하는 성질이다.
인증성은 사용자나 정보의 출처가 주장된 대상과 실제로 일치함을 확인할 수 있는 성질이다.
무결성은 정보가 허가 없이 변경·삭제되지 않고 정확성과 완전성을 유지하는 성질이다.
가용성은 허가받은 사용자가 필요할 때 정보와 시스템을 이용할 수 있는 성질이다.

선지별 해설

① X — 기밀성은 정보의 무단 열람이나 노출을 막는 성질이다. 지문의 '변경되거나 삭제되지 않고 완전한 일치성을 유지'한다는 설명은 기밀성이 아니라 무결성으로 고쳐야 한다.
② X — 인증성은 사용자·시스템·정보 출처의 신원이 진짜인지 확인하는 성질이다. 지문의 설명에 해당하는 말은 인증성이 아니라 무결성이다.
③ O — 무결성은 정보가 불법적으로 변경되거나 삭제되지 않고 정확하고 완전한 상태를 유지하는 성질이므로 지문의 정의와 일치한다.
④ X — 가용성은 허가받은 사용자가 필요한 시점에 정보나 시스템을 사용할 수 있는 성질이다. 지문의 설명에 해당하는 말은 가용성이 아니라 무결성이다.

오답 포인트

정보를 '보호한다'는 공통점만 보고 기밀성을 고르기 쉽다. 그러나 무단 열람·노출은 기밀성, 무단 변경·삭제는 무결성, 필요할 때의 이용은 가용성으로 구분한다.

NoteBase

다시 나오면 이렇게 판단

정의의 동사를 기준으로 판단한다. ‘보지 못하게 한다’는 기밀성, ‘바꾸지 못하게 한다’는 무결성, ‘필요할 때 쓰게 한다’는 가용성, ‘누구인지 또는 출처가 맞는지 확인한다’는 인증성이다.

암기 포인트

기밀성은 노출 방지, 무결성은 변경 방지, 가용성은 사용 보장, 인증성은 신원·출처 확인이다.

NoteBase

문 7. 다음은 트로이목마의 특징에 대한 설명이다. 성격이 가장 다른 하나는?

① 원격조정

② 시스템 파일 파괴

③ 자기복제

④ 데이터 유출

정답 3번

출제 포인트

트로이목마가 수행할 수 있는 악성 행위와 트로이목마 자체의 전파 특성을 구별하는 문제이다.

핵심 개념

트로이목마는 정상 프로그램으로 위장하여 사용자가 실행하도록 유도한 뒤 악성 기능을 수행하는 악성코드이다. 원격조정, 파일 파괴, 정보 유출 등을 수행할 수 있지만 바이러스나 웜과 달리 자기복제 기능을 본질적 특징으로 하지 않는다.

선지별 해설

① O — 원격조정은 트로이목마가 공격자에게 감염 시스템의 제어 권한을 제공하여 수행할 수 있는 대표적인 악성 기능이다.
② O — 시스템 파일을 삭제하거나 변조하여 시스템을 손상시키는 기능도 트로이목마의 악성 동작에 해당할 수 있다.
③ X — 틀린 표현은 '자기복제'이다. 트로이목마는 스스로 복제하여 전파되는 악성코드가 아니며, 올바르게는 정상 프로그램으로 위장하여 사용자의 실행 등을 통해 침투한다고 해야 한다. 자기복제는 바이러스나 웜을 구별하는 대표적 특성이다.
④ O — 저장된 개인정보나 인증정보 등을 외부로 빼내는 데이터 유출은 트로이목마가 수행할 수 있는 악성 기능이다.

오답 포인트

트로이목마도 악성코드라는 이유만으로 모든 악성코드의 공통 기능처럼 자기복제를 한다고 생각하기 쉽다. 그러나 ①·②·④는 감염 후 수행할 수 있는 공격 기능이고, ③은 전파 방식에 관한 설명이어서 성격이 다르다.

다시 나오면 이렇게 판단

선지가 감염 후의 악성 행위인지 전파 방식인지 먼저 나눈다. 위장·사용자 실행은 트로이목마, 자기복제·자동 전파는 바이러스나 웜의 특징으로 판단한다.

NoteBase

암기 포인트

트로이목마는 위장하여 침투하고 악성 기능을 수행하지만 스스로 복제하지 않는다.

NoteBase

문 8. 다음 중 시스템의 취약점 점검을 위하여 이용할 수 있는 도구가 아닌 것은?

① SATAN

② SAINT

③ nessus

④ Tripwire

정답 4번

출제 포인트

시스템·네트워크의 알려진 취약점을 탐지하는 취약점 스캐너와 파일 변경 여부를 감시하는 무결성 점검 도구를 구별하는 문제이다.

핵심 개념

취약점 스캐너는 대상 시스템이나 네트워크를 검사하여 알려진 보안 취약점과 잘못된 설정을 찾아내는 도구이다. SATAN, SAINT, Nessus는 취약점 점검 도구에 해당한다. Tripwire는 중요 파일의 기준 상태와 현재 상태를 비교하여 무단 변경을 탐지하는 파일 무결성 점검 도구이다.

선지별 해설

① O — SATAN은 네트워크에 연결된 시스템을 검사하여 알려진 취약점과 보안상 약점을 찾는 취약점 분석 도구이다.
② O — SAINT는 네트워크와 호스트의 보안 취약점을 탐지·분석하는 취약점 점검 도구이다.
③ O — Nessus는 호스트와 네트워크 서비스를 검사하여 알려진 취약점과 잘못된 설정을 탐지하는 취약점 스캐너이다.
④ X — Tripwire를 취약점 스캐너로 보는 부분이 틀렸다. 올바르게는 Tripwire는 중요 파일의 해시 등 기준 정보를 저장해 두고 이후의 변경을 탐지하는 파일 무결성 점검 도구이다.

오답 포인트

Tripwire도 보안 점검에 쓰인다는 점 때문에 취약점 스캐너로 혼동하기 쉽다. 그러나 SATAN·SAINT·Nessus는 알려진 취약점을 찾아내고, Tripwire는 파일이 기준 상태에서 변경되었는지를 확인한다.

다시 나오면 이렇게 판단

도구가 네트워크·서비스의 알려진 약점을 탐색하면 취약점 스캐너이고, 파일의 해시나 기준 상태를 비교해 변조를 찾으면 무결성 점검 도구로 판단한다.

NoteBase

암기 포인트

SATAN·SAINT·Nessus는 취약점 스캔, Tripwire는 파일 변경 탐지이다.

NoteBase

문 9. 윈도우(Windows) 2008 서버에서의 로그 관리는 이벤트 뷰어라는 관리 도구를 사용한다. 다음에 설명하는 이벤트는 무엇인가?

· 파일이나 다른 개체 만들기, 열기, 삭제 등의 리스트 사용과 관련된 이벤트이다.
· 로그인 시도 및 잘못된 로그인 시도 이벤트이며 이벤트 유형은 관리자가 지정한다.

① 응용(Application) 프로그램 로그
② 보안(Security) 로그
③ 시스템(System) 로그
④ 리소스(Resource) 로그

정답 2번

출제 포인트

이 문제는 Windows 이벤트 로그 가운데 파일·개체 접근과 로그온 시도 같은 감사 이벤트가 기록되는 로그를 구별하는 문제이다.

핵심 개념

보안 로그는 감사 정책에 따라 로그온 성공·실패, 파일이나 다른 개체에 대한 접근 등 보안 관련 사건을 기록한다. 응용 프로그램 로그는 응용 프로그램이 발생시킨 사건을, 시스템 로그는 운영체제 구성 요소·서비스·드라이버가 발생시킨 사건을 주로 기록한다.

선지별 해설

① X — 응용 프로그램 로그는 응용 프로그램이 기록하는 오류·경고·정보 등의 이벤트를 담는다. 파일·개체 접근과 로그온 시도에 관한 감사 이벤트라는 설명은 응용 프로그램 로그가 아니라 보안 로그에 해당한다.
② O — 보안 로그에는 관리자가 설정한 감사 정책에 따라 개체 접근과 로그온 성공·실패 같은 보안 감사 이벤트가 기록된다. 제시된 두 설명이 모두 이에 해당한다.
③ X — 시스템 로그는 운영체제 구성 요소, 장치 드라이버, 시스템 서비스에서 발생한 이벤트를 주로 담는다. 제시된 감사 이벤트는 시스템 로그가 아니라 보안 로그에 해당한다.
④ X — 리소스 로그는 제시된 파일·개체 접근 및 로그온 감사 이벤트를 분류하는 기본 로그가 아니다. 이러한 이벤트의 올바른 분류는 보안 로그이다.

오답 포인트

파일을 열거나 삭제하는 행위가 시스템 동작처럼 보여 시스템 로그로 착각하기 쉽다. 그러나 문제의 핵심 표현은 '개체 사용'과 '로그인 시도'이며, 둘 다 관리자가 감사 대상으로 설정하는 보안 사건이다.

NoteBase

다시 나오면 이렇게 판단

로그온 성공·실패, 계정 사용, 권한 사용, 파일·개체 접근처럼 '누가 무엇에 접근했는가'를 감사하는 내용이면 보안 로그로 판단한다. 응용 프로그램 자체의 오류는 응용 프로그램 로그, 운영체제 구성 요소·드라이버·서비스의 동작 문제는 시스템 로그로 구분한다.

암기 포인트

로그온·계정·권한·개체 접근 감사는 보안 로그이다.

NoteBase

문 10. 유닉스(Unix)의 로그 파일과 기록되는 내용을 바르게 연결한 것은?

ㄱ. history- 명령창에 실행했던 명령 내역
ㄴ. sulog- su 명령어 사용 내역
ㄷ. xferlog- 실패한 로그인 시도 내역
ㄹ. loginlog- FTP 파일 전송 내역

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 1번

출제 포인트

유닉스 로그의 이름과 각 로그에 기록되는 사건을 정확히 연결하는 문제이다.

핵심 개념

history는 명령창에서 실행한 명령의 내역을 보여 준다. sulog는 su 명령을 이용한 사용자 전환 내역을 기록한다. xferlog는 FTP 등의 파일 전송 내역을 기록하고, loginlog는 실패한 로그인 시도 내역을 기록한다. 따라서 ㄱ과 ㄴ은 옳고, ㄷ과 ㄹ은 기록 내용이 서로 뒤바뀌어 있다.

선지별 해설

① O — ㄱ의 history는 실행 명령 내역, ㄴ의 sulog는 su 명령 사용 내역과 연결되므로 둘 다 옳다.
② X — ㄱ은 옳지만 ㄷ의 'xferlog-실패한 로그인 시도 내역'이 틀리다. xferlog는 파일 전송 내역을 기록하며, 실패한 로그인 시도 내역은 loginlog에 기록된다. 올바른 조합은 ㄱ, ㄴ이다.
③ X — ㄴ은 옳지만 ㄷ이 틀리다. xferlog는 실패한 로그인 시도가 아니라 파일 전송 내역을 기록한다. 올바른 조합은 ㄱ, ㄴ이다.
④ X — ㄷ과 ㄹ의 기록 내용이 서로 바뀌어 모두 틀리다. 올바르게는 xferlog가 파일 전송 내역을, loginlog가 실패한 로그인 시도 내역을 기록한다. 올바른 조합은 ㄱ, ㄴ이다.

오답 포인트

xferlog와 loginlog의 용도를 반대로 연결한 ㄷ · ㄹ이 함정이다. xfer는 transfer를 뜻하므로 파일 전송과 연결되고, loginlog는 로그인 실패 기록과 연결된다.

NoteBase

다시 나오면 이렇게 판단

로그 이름의 핵심 단어를 기록 대상과 연결한다. history는 명령 이력, su는 사용자 전환, xfer는 파일 전송, login은 로그인 시도로 판단한다.

암기 포인트

history-명령 이력, sulog-su 사용, xferlog-파일 전송, loginlog-로그인 실패이다.

NoteBase

문 11. 다음 중 윈도우 파일시스템에 대한 설명으로 맞지 않는 것은?

① NTFS는 윈도우 NT/2000/2003의 전용파일시스템이다.

② FAT16은 고용량 하드디스크를 지원한다.

③ NTFS는 자체적인 보안을 설정할 수 있다.

④ NTFS는 파일정보를 MFT(Master File Table)에 저장한다.

정답 2번

출제 포인트

윈도우 파일 시스템인 FAT16과 NTFS의 저장 용량, 보안 기능, 파일 관리 구조를 구분하는 문제이다.

핵심 개념

FAT16은 파일 할당 테이블의 항목을 16비트로 관리하는 구형 파일 시스템으로, 표현할 수 있는 클러스터 수가 적어 대용량 저장 장치 지원에 한계가 있다.
NTFS는 윈도우 NT 계열을 위해 설계된 파일 시스템으로, 파일·폴더별 접근 권한과 같은 보안 기능을 제공하며 파일 정보를 MFT에 기록한다.

선지별 해설

① O — NTFS는 윈도우 NT 계열을 위해 설계되어 Windows NT·2000·2003에서 사용하는 대표적인 파일 시스템이다.
② X — 틀린 표현은 'FAT16은 고용량 하드디스크를 지원한다'이다. FAT16은 클러스터 수와 볼륨 크기에 제약이 있어 고용량 하드디스크 지원에 한계가 있으며, 올바르게는 FAT32나 NTFS가 FAT16보다 대용량 저장 장치에 적합하다.
③ O — NTFS는 파일과 폴더에 사용자별 접근 권한을 지정할 수 있으므로 파일 시스템 자체에서 보안을 설정할 수 있다.
④ O — NTFS는 파일명, 크기, 위치, 시간 정보, 권한 등의 파일 정보를 MFT(Master File Table)에 저장하여 관리한다.

오답 포인트

FAT16도 하드디스크에서 사용할 수 있다는 사실을 '고용량 하드디스크를 충분히 지원한다'는 뜻으로 확대하면 ②를 놓치기 쉽다. 핵심은 FAT16의 16비트 클러스터 주소 체계가 볼륨 크기를 제한한다는 점이다.

다시 나오면 이렇게 판단

용량 관련 선지는 FAT16의 제한 여부를 먼저 보고, 보안과 파일 정보 관리 관련 선지는 NTFS의 접근 권한 기능과 MFT를 기준으로 판단한다.

NoteBase

암기 포인트

FAT16은 용량 제약, NTFS는 보안 설정과 MFT이다.

NoteBase

문 12. 다음은 데이터베이스 보안에 대한 설명이다. 보기 중에서 옳지 않은 것은?

① 데이터베이스에 대한 모든 접근에 대한 감사기록이 생성되어야 한다.

② 인가되지 않은 사용자에 의한 데이터의 변경과 파괴와 시스템 오류로부터 데이터베이스를 보호해야한다.

③ 기밀성과 무결성을 보장하기 위해 데이터에 대한 등급 분류는 필요없다.

④ 데이터베이스의 물리적 보호는 자연재해나 컴퓨터 시스템에 손상을 주는 위험으로부터 데이터베이스를 보호하는 것을 의미한다.

정답 3번

출제 포인트

데이터베이스 보안의 주요 통제인 접근 감사, 무결성·가용성 보호, 데이터 등급 분류, 물리적 보호의 의미를 구분하는 문제이다.

핵심 개념

데이터베이스 보안은 데이터의 기밀성·무결성·가용성을 지키기 위해 접근을 통제하고 기록하며, 데이터의 중요도에 맞는 보호 수준을 적용하고, 재해나 시스템 손상에도 대비하는 활동이다.
접근 감사는 누가 언제 어떤 데이터에 접근했는지 추적하는 통제이고, 데이터 등급 분류는 중요도와 민감도에 따라 접근 권한과 보호 수준을 달리 정하는 기초이다. 물리적 보호는 자연재해, 화재, 정전, 장비 손상 등 물리적 위험으로부터 데이터베이스 시스템을 지키는 통제이다.

선지별 해설

① O — 데이터베이스에 대한 접근 기록을 생성하면 사용자와 작업 내용을 추적할 수 있으므로 부정 접근 탐지와 사후 책임 확인에 활용된다. 따라서 접근 감사기록은 데이터베이스 보안의 기본 통제에 해당한다.
② O — 비인가 사용자의 데이터 변경·파괴는 무결성과 가용성을 침해하며, 시스템 오류도 데이터 손상이나 서비스 중단을 일으킬 수 있다. 데이터베이스는 접근 통제, 백업·복구 등의 수단으로 이러한 위험으로부터 보호되어야 한다.
③ X — 틀린 표현은 '데이터에 대한 등급 분류는 필요없다'이다. 올바르게는 기밀성과 무결성을 보장하기 위해 데이터의 중요도와 민감도에 따라 등급을 분류하고, 등급별로 접근 권한과 보호 수준을 적용해야 한다.
④ O — 물리적 보호는 자연재해나 화재, 정전, 장비 훼손처럼 컴퓨터 시스템에 물리적 손상을 줄 수 있는 위험으로부터 데이터베이스와 관련 설비를 보호하는 것을 의미한다.

오답 포인트

③은 '등급 분류'가 단순한 관리 편의라고 오인하게 만드는 선지이다. 등급 분류는 데이터의 민감도에 맞춰 접근 범위와 보호 강도를 정하는 출발점이므로, 기밀성과 무결성을 위한 보안 통제에서 제외할 수 없다.

NoteBase

다시 나오면 이렇게 판단

선지의 통제가 어떤 위험을 줄이는지 연결한다. 접근 기록은 추적성과 책임성, 비인가 변경 방지는 무결성, 백업·복구는 가용성, 등급 분류는 차등 접근 통제, 물리적 보호는 재해·설비 손상 대응에 해당한다.

암기 포인트

데이터는 등급별로 통제하고, 접근은 기록하며, 변경·파괴와 물리적 위험에는 보호·복구로 대비한다.

NoteBase

문 13. 공개키 시스템에 대한 설명으로 옳지 않은 것은?

① 암호와 해독에 다른 키를 사용한다.

② 키 분배가 비밀키 시스템보다 어렵다.

③ 해독키는 당사자만 알고 있다.

④ 암호키는 공개되어 있어 누구나 사용할 수 있다.

정답 2번

출제 포인트

공개키 암호 시스템에서 공개키와 개인키의 역할, 그리고 대칭키 암호 시스템과 비교한 키 분배의 특징을 묻는 문제이다.

핵심 개념

공개키 암호 시스템은 서로 수학적으로 연관된 공개키와 개인키를 사용하는 비대칭키 방식이다. 기밀성을 위한 암호화에서는 누구나 공개키로 암호화할 수 있지만, 그 공개키에 대응하는 개인키를 가진 사람만 복호화할 수 있다. 대칭키 방식과 달리 비밀키 자체를 상대방에게 안전하게 전달할 필요가 없어 키 분배가 더 쉽다.

선지별 해설

① O — 공개키 암호 시스템은 암호화에 공개키를, 복호화에 그와 다른 개인키를 사용하므로 암호와 해독에 서로 다른 키를 사용한다.
② X — 틀린 표현은 '키 분배가 비밀키 시스템보다 어렵다'이다. 공개키는 공개해 배포할 수 있으므로, 동일한 비밀키를 안전하게 공유해야 하는 비밀키 시스템보다 키 분배가 쉽다.
③ O — 기밀성을 위한 공개키 암호에서는 복호화에 쓰는 개인키를 소유자만 비밀로 보관한다.
④ O — 암호화에 쓰는 공개키는 공개되어 있으므로 누구나 받아서 해당 수신자에게 보낼 데이터를 암호화하는 데 사용할 수 있다.

오답 포인트

공개키 방식은 키가 두 개라서 키 관리 구조는 복잡해 보이지만, 공개키를 비밀리에 전달할 필요가 없다는 점 때문에 상대방과 비밀키를 미리 공유하는 문제는 오히려 줄어든다. ②의 '어렵다'가 반대로 제시된 함정이다.

다시 나오면 이렇게 판단

기밀성 기준으로 '공개키로 암호화, 개인키로 복호화'를 먼저 대응시킨다. 이어서 공개키는 공개 배포가 가능하므로 대칭키 방식보다 키 분배가 쉽다고 판단한다.

NoteBase

암기 포인트

공개키는 배포하고 개인키는 보관한다. 공개키 방식은 서로 다른 두 키를 사용하며 비밀키 사전 공유 부담이 작다.

NoteBase

문 14. 유닉스 계열의 시스템에서 핵심부분인 커널(Kernel)에 대한 설명으로 옳지 않은 것은?

① 유닉스 시스템의 구성은 커널(Kernel), 셸(Shell), 파일시스템(File System)으로 구성되며, 커널은 프로세스 관리, 메모리 관리, 입출력 관리를 수행한다.

② 커널(Kernel)은 데몬(Daemon) 프로세스를 실행하고 관리한다.

③ 유닉스계열의 시스템이 부팅될 때 가장 먼저 읽혀지는 핵심 부분으로 보조기억장치에 상주한다.

④ 커널(Kernel)은 셸(Shell)과 상호 연관되며 작업을 수행한다.

정답 3번

출제 포인트

이 문제는 유닉스 커널의 역할과 커널이 실행 중 상주하는 기억장치의 구분을 묻는 문제이다.

핵심 개념

커널은 운영체제의 핵심으로서 프로세스, 메모리, 입출력 장치 등 시스템 자원을 관리한다. 셸은 사용자 명령을 해석하여 커널의 기능을 요청하는 사용자 인터페이스이다. 커널 파일은 평소 보조기억장치에 저장되어 있지만, 부팅 과정에서 주기억장치로 적재되어 실행 중 상주한다.

선지별 해설

① O — 유닉스 시스템은 일반적으로 커널, 셸, 파일 시스템을 중심으로 구성되며, 커널은 프로세스 관리, 메모리 관리, 입출력 관리를 담당한다.
② O — 데몬은 백그라운드에서 동작하는 프로세스이다. 커널은 다른 프로세스와 마찬가지로 데몬에 CPU와 메모리 등의 자원을 배분하고 실행을 관리한다. 다만 개별 데몬의 시작·종료 같은 서비스 관리는 보통 init 또는 systemd와 같은 사용자 공간의 초기화·서비스 관리 프로세스가 담당한다.
③ X — 틀린 부분은 커널이 '보조기억장치에 상주한다'는 표현이다. 커널 파일은 보조기억장치에 저장되어 있다가 부팅 과정에서 주기억장치로 적재되며, 시스템이 동작하는 동안 주기억장치에 상주한다.
④ O — 셸은 사용자의 명령을 해석하고 시스템 호출 등을 통해 커널에 작업 수행을 요청하므로 커널과 상호 연관되어 동작한다.

오답 포인트

③은 '저장'과 '상주'를 바꾸어 놓았다. 커널 파일이 부팅 전 보조기억장치에 저장된다는 사실 때문에 보조기억장치에 상주한다고 판단하기 쉽지만, 실행 중인 커널의 상주 위치는 주기억장치이다.

다시 나오면 이렇게 판단

운영체제 구성 요소 문제에서는 저장 위치와 실행 위치를 구분한다. 보조기억장치에는 커널 파일이 저장되고, 부팅 시 적재된 커널은 주기억장치에 상주하면서 자원을 관리한다.

NoteBase

암기 포인트

커널 파일은 보조기억장치에 저장, 실행 중 커널은 주기억장치에 상주한다.

NoteBase

문 15. 다음 중 파일에 대한 부적절한 접근으로부터 보호하기 위한 방법이 아닌 것은?

① 접근제어 행렬(Access control matrix)

② 파일 압축(Compression)

③ 파일의 명명법(Naming)

④ 암호화(Encryption)

정답 2번

출제 포인트

파일의 무단 접근이나 내용 노출을 막는 보호 기법과, 파일의 저장 용량을 줄이는 처리 기법을 구분하는 문제이다.

핵심 개념

파일 보호는 누가 어떤 파일에 어떤 작업을 할 수 있는지 제한하거나, 파일 내용을 권한 없는 사람이 알아보지 못하게 하는 것이다. 접근제어 행렬은 주체별 접근 권한을 정하고, 명명법은 파일을 식별·지정하는 과정에 보호 요소를 둘 수 있으며, 암호화는 파일 내용을 해독할 수 없게 한다. 반면 압축은 데이터 표현을 줄여 저장 공간이나 전송량을 절약하는 기법이다.

선지별 해설

① O — 접근제어 행렬은 사용자·프로세스 같은 주체가 파일 같은 객체에 대해 읽기, 쓰기, 실행 등의 권한을 갖는지를 정하므로 부적절한 접근을 통제하는 방법이다.
② X — 파일 압축은 파일의 데이터량을 줄이는 방법일 뿐 접근 권한을 제한하거나 내용을 비밀로 만드는 보호 방법이 아니다. 틀린 표현은 '파일에 대한 부적절한 접근으로부터 보호하기 위한 방법'이며, 올바르게는 '저장 공간이나 전송량을 줄이기 위한 방법'이다. 따라서 문제에서 묻는 '아닌 것'에 해당한다.
③ O — 파일 명명법은 파일을 이름으로 식별하고 지정하는 방식을 이용하는 기초적인 보호 방법이다. 다만 이름이 알려지면 우회될 수 있으므로 접근제어보다 약한 수단이다.
④ O — 암호화는 적절한 키가 없는 사용자가 파일을 얻더라도 내용을 알아볼 수 없게 하므로 정보 노출을 방지하는 보호 방법이다.

오답 포인트

압축 파일에 비밀번호를 설정하는 기능과 압축 자체를 혼동하기 쉽다. 비밀번호나 암호화가 결합되면 보호 기능이 생기지만, 압축의 본래 목적은 데이터 크기 감소이므로 압축만으로는 무단 접근을 막지 못한다.

다시 나오면 이렇게 판단

각 기법이 권한 제한, 접근 대상의 식별·지정, 내용 은닉 가운데 하나를 수행하는지 확인한다. 단지 파일 크기만 줄이는 기법이면 접근 보호 수단으로 보지 않는다.

NoteBase

암기 포인트

접근제어·명명·암호화는 보호, 압축은 용량 절감이다.

NoteBase

문 16. C언어로 작성된 응용프로그램에서 버퍼 오버플로우 취약점의 발생을 방지하기 위해 사용이 권고되는 함수에 해당되지 않는 것은?

① strncat( )
② sscanf( )
③ snprintf( )
④ strncpy( )

정답 2번

출제 포인트

버퍼 오버플로를 줄이기 위해 쓰기 길이를 제한할 수 있는 C 문자열 처리 함수와 그렇지 않은 함수를 구별하는 문제이다.

핵심 개념

strncat, snprintf, strncpy는 처리할 최대 길이나 출력 버퍼 크기를 인수로 지정할 수 있는 함수이다. 반면 sscanf는 문자열에서 형식에 맞는 값을 읽는 입력 변환 함수이며, 함수 자체가 목적지 버퍼의 크기를 인수로 받지 않는다. 특히 %s 변환에 최대 필드 폭을 지정하지 않으면 목적지 문자 배열을 넘어서 쓸 수 있다.

선지별 해설

① X — strncat은 덧붙일 문자의 최대 개수를 지정할 수 있으므로 무제한 strcat보다 버퍼 경계를 관리하기에 적합하다. 이 선지는 '권고되는 함수에 해당되지 않는다'가 아니라 '길이 값을 올바르게 계산해 사용하는 경우 권고되는 함수에 해당한다'로 고쳐야 한다.
② O — sscanf는 목적지 버퍼의 크기를 별도 인수로 받지 않는다. %s 등에 필드 폭을 지정하지 않으면 입력 길이를 제한하지 못하므로, 제시된 함수 중 버퍼 오버플로 방지를 위해 권고되는 함수에 해당하지 않는다.
③ X — snprintf는 출력 버퍼의 전체 크기를 지정하여 그 범위 안에서 서식 문자열을 기록하므로 무제한 sprintf보다 안전하다. 이 선지는 '권고되는 함수에 해당되지 않는다'가 아니라 '버퍼 크기를 정확히 지정해 사용하는 경우 권고되는 함수에 해당한다'로 고쳐야 한다.
④ X — strncpy는 복사할 최대 문자 수를 지정할 수 있으므로 무제한 strcpy보다 버퍼 경계를 관리하기에 적합하다. 이 선지는 '권고되는 함수에 해당되지 않는다'가 아니라 '복사 길이와 문자열 종료를 함께 관리하는 경우 권고되는 함수에 해당한다'로 고쳐야 한다. 다만 원본 문자열 길이가 지정 길이 이상이면 널 종료 문자가 붙지 않을 수 있다.

NoteBase

오답 포인트

sscanf도 서식 문자열을 사용하므로 snprintf와 비슷하게 안전해 보이는 점이 함정이다. snprintf의 크기 인수는 출력 버퍼 전체의 상한을 직접 정하지만, sscanf의 %s 입력 길이는 서식에 필드 폭을 따로 적어야 제한된다.

다시 나오면 이렇게 판단

함수 이름에 n이 있는지만 보지 않고, 목적지에 기록할 수 있는 양을 크기 인수로 제한하는지 확인한다. strncat·snprintf·strncpy는 길이 또는 크기 인수가 있고, sscanf는 목적지 버퍼 크기 인수가 없으므로 구별된다.

암기 포인트

문자열 쓰기는 경계 길이를 전달하는 함수가 기본이고, sscanf의 %s는 필드 폭이 없으면 경계가 없다.

NoteBase

문 17. 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 무작위 문자열을 추가한다. 이렇게 추가되는 문자열을 무엇이라 하는가?

① Nonce
② Plaintext
③ Salt
④ Cipher

정답 3번

출제 포인트

패스워드 해시를 만들 때 원래 패스워드에 덧붙이는 무작위 문자열의 명칭과 역할을 묻는 문제이다.

핵심 개념

Salt는 패스워드를 해시하기 전에 각 패스워드에 고유하게 덧붙이는 무작위 값이다. 같은 패스워드라도 서로 다른 해시가 나오게 하며, 미리 계산한 해시 목록인 레인보 테이블을 이용한 공격의 효율을 낮춘다. Salt 자체를 비밀로 유지하는 것이 핵심은 아니며, 일반적으로 해시값과 함께 저장할 수 있다.

선지별 해설

① X — Nonce는 통신이나 암호 프로토콜에서 한 번만 사용하여 메시지의 신선성이나 고유성을 확보하는 값이다. 틀린 표현은 ‘Nonce’이며, 패스워드 해시에 추가하는 무작위 문자열은 Salt이다.
② X — Plaintext는 암호화되거나 해시되기 전의 원래 데이터인 평문이다. 틀린 표현은 ‘Plaintext’이며, 문제의 무작위 추가 문자열은 Salt이다.
③ O — Salt는 패스워드를 해시하기 전에 추가하는 무작위 문자열이다. 동일한 패스워드의 해시값이 항상 같아지는 현상을 막고 사전 계산 공격을 어렵게 한다.
④ X — Cipher는 평문과 암호문을 변환하는 암호 알고리즘을 뜻한다. 틀린 표현은 ‘Cipher’이며, 패스워드 해시에 덧붙이는 값은 Salt이다.

오답 포인트

Nonce와 Salt가 모두 무작위성이나 고유성을 위해 쓰일 수 있어 혼동하기 쉽다. 이 문항의 결정적 표현은 ‘패스워드를 저장할 때 해시에 추가’이며, 이에 대응하는 용어는 Salt이다.

다시 나오면 이렇게 판단

패스워드 해시 앞에 고유한 값을 덧붙인다는 설명이면 Salt로 판단한다. 프로토콜에서 한 번만 쓰는 값이면 Nonce, 가공 전 원본이면 Plaintext, 암호화·복호화 방식이면 Cipher로 구분한다.

NoteBase

암기 포인트

패스워드 해시에 뿌리는 소금은 Salt이다.

NoteBase

문 18. 다음의 보기는 웹 방화벽의 주요 기능에 대한 설명이다. 보기 중에서 틀린 것을 고르시오.

① 웹 방화벽은 URL 단위의 탐지 기능을 가지며 파일 업로드 제어기능과 파일 검사 기능을 가질 수 있다.

② 클라이언트가 보낸 요청을 검사하여 악의적인 요청과 침입을 검사하고 차단하는 기능을 가진다.

③ 웹 방화벽은 HTTP 헤더 데이터를 이용하여 사용자의 요청을 분석하는 기능을 위해 분석용 키(Key)를 가진다.

④ 웹 방화벽은 URL 및 서버 정보 위장 기능을 제공하여 사용자에게 실제 서버의 위치와 서버 정보를 숨기는 기능을 가진다.

정답 3번

출제 포인트

웹 방화벽의 요청 검사·차단, 업로드 파일 통제, 서버 정보 은닉 기능과 HTTP 메시지 분석 방식을 구별하는 문제이다.

핵심 개념

웹 방화벽(WAF)은 웹 애플리케이션 앞에서 HTTP/HTTPS 요청과 응답을 검사하고, 공격 패턴이나 보안 정책에 위배되는 트래픽을 탐지·차단하는 보안 장비 또는 소프트웨어이다. 검사 대상에는 URL, HTTP 헤더, 쿠키, 매개변수, 메시지 본문 등이 포함될 수 있으며, 탐지는 규칙·정책·시그니처 등을 기준으로 이루어진다.

선지별 해설

① O — 웹 방화벽은 URL별로 접근이나 공격 여부를 탐지할 수 있고, 업로드 파일의 형식·크기 등을 통제하거나 악성 파일 여부를 검사하는 기능도 제공할 수 있다.
② O — 클라이언트의 HTTP/HTTPS 요청을 분석하여 SQL 삽입, 크로스 사이트 스크립팅 등 악의적인 요청을 탐지하고 정책에 따라 차단하는 것이 웹 방화벽의 핵심 기능이다.
③ X — 틀린 부분은 HTTP 헤더 데이터를 이용한 요청 분석을 위해 별도의 '분석용 키(Key)'를 가진다는 표현이다. HTTP 헤더는 URL, 쿠키, 매개변수, 본문 등과 함께 검사되는 HTTP 메시지의 구성 요소이며, 웹 방화벽은 보안 규칙·정책·시그니처 등을 기준으로 요청을 분석한다. 올바르게는 '웹 방화벽은 HTTP 헤더를 포함한 HTTP 요청의 여러 구성 요소를 보안 정책에 따라 분석한다'이다.
④ O — 웹 방화벽을 역방향 프록시 방식으로 배치하면 외부에는 웹 방화벽의 주소가 노출되고 실제 웹 서버의 위치나 서버 식별 정보는 감출 수 있다. URL 변환이나 응답 헤더의 서버 정보 제거·변경도 이러한 정보 은닉에 해당한다.

NoteBase

오답 포인트

③은 'HTTP 헤더를 분석한다'는 앞부분은 타당하지만, 이를 위해 웹 방화벽이 '분석용 키'를 가진다고 연결한 부분이 잘못되었다. 암호화에 쓰는 키나 URL의 키-값 매개변수와 웹 방화벽의 탐지 기준인 규칙·정책·시그니처를 혼동하면 오답을 고르기 쉽다.

다시 나오면 이렇게 판단

웹 방화벽의 기능은 웹 요청·응답의 검사와 차단, URL·업로드 통제, 웹 서버 정보 은닉을 중심으로 판단한다. HTTP 구성 요소를 검사한다는 설명과, 존재하지 않는 별도 분석 수단을 필수 기능처럼 붙인 설명을 구분한다.

암기 포인트

웹 방화벽은 HTTP의 URL·헤더·쿠키·본문을 규칙과 정책으로 검사하며, '분석용 키'로 분석하는 장비가 아니다.

NoteBase

문 19. 다음 중 전자서명의 특징으로 합법적인 서명자만이 전자서명을 생성할 수 있어야 하는 특징은 무엇인가?

① 서명자 인증
② 부인불가
③ 변경불가
④ 위조불가

정답 4번

출제 포인트

전자서명의 여러 특징 가운데 '합법적인 서명자만 서명을 생성할 수 있음'이 위조불가에 해당함을 구별하는 문제이다.

핵심 개념

위조불가는 정당한 서명자 이외의 사람이 유효한 전자서명을 만들어 낼 수 없어야 한다는 성질이다.
서명자 인증은 전자서명의 생성자가 누구인지 확인하는 성질이고, 부인불가는 서명자가 나중에 서명 사실을 부인할 수 없게 하는 성질이며, 변경불가는 서명 후 문서가 변조되면 이를 검출할 수 있게 하는 성질이다.

선지별 해설

① X — 서명자 인증은 전자서명을 검증하여 서명자의 신원을 확인하는 성질이다. '합법적인 서명자만 전자서명을 생성할 수 있음'에 해당하는 표현은 서명자 인증이 아니라 위조불가이다.
② X — 부인불가는 서명자가 사후에 자신이 서명한 사실을 부인하지 못하게 하는 성질이다. 문제의 설명은 부인불가가 아니라 위조불가이다.
③ X — 변경불가는 서명된 문서의 내용이 사후에 바뀌면 서명 검증을 통해 그 변경을 알아낼 수 있는 성질이다. 문제의 설명은 변경불가가 아니라 위조불가이다.
④ O — 위조불가는 정당한 서명자만 유효한 전자서명을 생성할 수 있고 제3자는 이를 위조할 수 없어야 한다는 성질이므로 제시된 설명과 일치한다.

오답 포인트

'합법적인 서명자'라는 말 때문에 ① 서명자 인증을 고르기 쉽다. 그러나 신원을 확인하는 것은 인증이고, 다른 사람이 유효한 서명을 만들지 못하게 하는 것은 위조불가이다.

다시 나오면 이렇게 판단

문장의 동사를 기준으로 구별한다. '누구인지 확인'은 서명자 인증, '나중에 부인하지 못함'은 부인불가, '내용 변경을 검출'은 변경불가, '제3자가 만들어 내지 못함'은 위조불가이다.

NoteBase

암기 포인트

확인은 인증, 부인은 부인불가, 변조 검출은 변경불가, 가짜 서명 방지는 위조불가이다.

NoteBase

문 20. 디지털 증거의 법적 효력을 인정받기 위해 포렌식 과정에서 지켜야 하는 원칙이 아닌 것은?

① 정당성의 원칙

② 무결성의 원칙

③ 재현의 원칙

④ 연계추적불가능의 원칙

정답 4번

출제 포인트

이 문제는 디지털 증거가 법적 증거로 인정되기 위해 수집·분석·보관 과정에서 지켜야 하는 기본 원칙을 구별하는 문제이다.

핵심 개념

정당성은 적법하고 정당한 절차와 권한에 따라 증거를 획득해야 한다는 원칙이다. 무결성은 증거가 수집된 뒤 변경·훼손되지 않았음을 보장해야 한다는 원칙이다. 재현성은 동일한 조건과 절차로 분석하면 같은 결과를 얻을 수 있어야 한다는 원칙이다. 연계보관성은 증거의 수집부터 제출까지 취급자·시점·이동·처리 내역을 계속 기록하여 추적 가능하게 해야 한다는 원칙이다.

선지별 해설

① O — 정당성의 원칙은 디지털 증거를 적법한 권한과 절차에 따라 수집해야 한다는 것으로, 법적 효력을 뒷받침하는 원칙이다.
② O — 무결성의 원칙은 수집한 디지털 증거가 변경되거나 훼손되지 않았음을 해시값 비교 등의 방법으로 확인할 수 있어야 한다는 원칙이다.
③ O — 재현의 원칙은 같은 조건과 절차로 다시 분석했을 때 동일한 결과가 나와야 한다는 뜻이며, 일반적으로 재현성의 원칙이라고 한다.
④ X — 틀린 표현은 '연계추적불가능'이다. 디지털 증거는 누가 언제 수집·이관·보관·분석했는지 추적할 수 있어야 하므로, 올바른 원칙은 연계보관성의 원칙 또는 연계추적성의 원칙이다.

오답 포인트

④는 '연계'라는 익숙한 말 때문에 실제 원칙처럼 보이지만, 핵심은 '추적불가능'이라는 부정 표현이다. 증거의 취급 이력이 끊기거나 추적되지 않으면 동일성과 무결성을 입증하기 어렵다.

NoteBase

다시 나오면 이렇게 판단

포렌식 원칙은 적법하게 수집하고, 변조되지 않게 보존하며, 같은 결과를 재현하고, 취급 과정을 처음부터 끝까지 추적할 수 있게 하는 방향이어야 한다. 이 방향을 거스르는 '불가능', '기록하지 않음', '변경 허용'과 같은 표현은 틀린 선지로 판단한다.

암기 포인트

정당하게 수집하고, 무결하게 보존하며, 재현할 수 있고, 이력을 끝까지 추적한다.

NoteBase