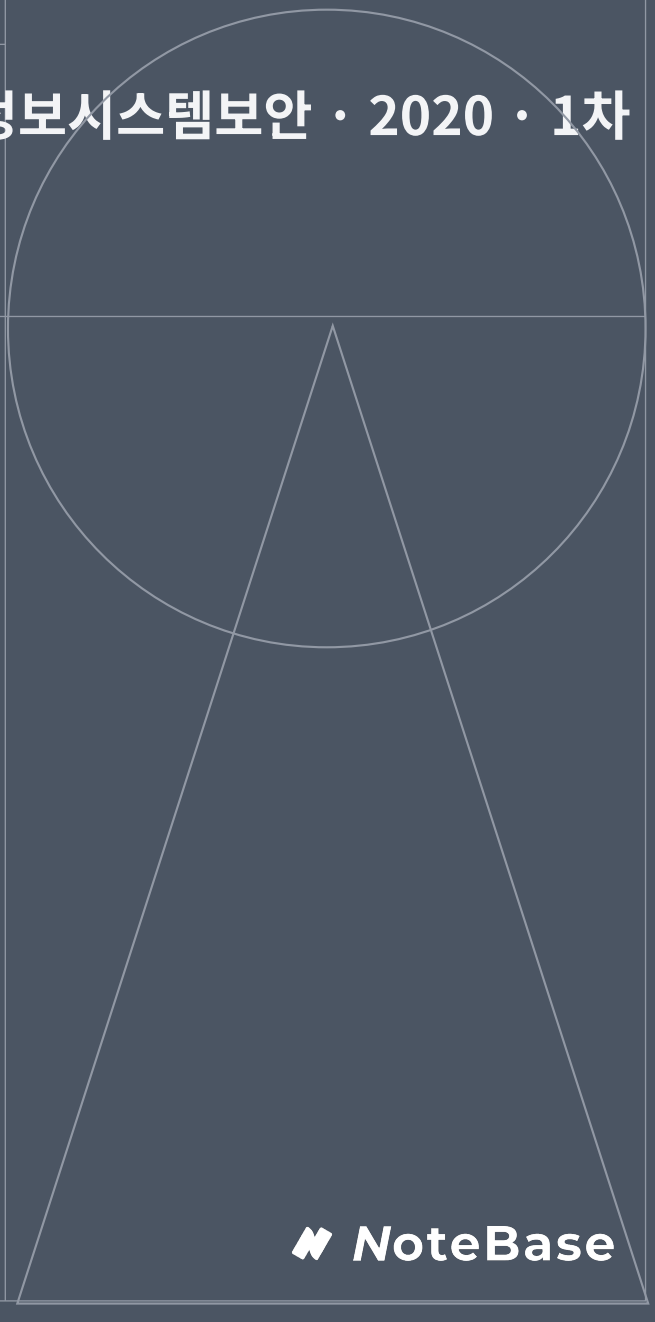
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2020 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2020 · 1차

공무원/해경/일반직 9급 · 정보시스템보안 · 2020 · 1차

문 1. 다음 중 스테가노그래피(Steganography)에 대한 설명으로 가장 옳지 않은 것은?

① 그림의 픽셀 중 일부를 저장하고 싶은 데이터로 대체하여 저장하는 방법으로 원본 그림과 대체된 그림을 육안으로 구별할 수 있다.

② 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.

③ 텍스트·이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.

④ 9.11 테러 당시 테러리스트들이 대화를 은닉하기 위해 사용한 기법이다.

정답 1번

출제 포인트

스테가노그래피의 목적이 비밀정보의 내용뿐 아니라 그 존재 자체를 드러나지 않게 숨기는 데 있다는 점을 묻는 문제이다.

핵심 개념

스테가노그래피는 비밀정보를 이미지·음성·영상·텍스트 같은 다른 매체 안에 은닉하여 정보가 있다는 사실 자체를 알아차리기 어렵게 하는 기술이다. 암호화가 정보의 내용을 해독하기 어렵게 만드는 기술이라면, 스테가노그래피는 정보의 존재를 감추는 데 초점이 있다. 이미지에서는 픽셀값의 최하위 비트처럼 변화가 눈에 잘 띄지 않는 부분을 이용할 수 있다.

선지별 해설

① X — 틀린 표현은 '원본 그림과 대체된 그림을 육안으로 구별할 수 있다'이다. 스테가노그래피는 픽셀값의 미세한 변화 등을 이용하여 은닉 전후의 차이를 육안으로 쉽게 구별하기 어렵게 하는 것이 핵심이다.
② O — 스테가노그래피는 민감한 정보의 내용만 보호하는 데 그치지 않고, 비밀정보가 존재한다는 사실 자체를 숨기는 기술이다.
③ O — 텍스트·이미지·음성·영상 등 디지털 매체에 비밀 이진 정보를 은닉할 수 있다. 이미지의 픽셀값 일부를 미세하게 바꾸는 방식이 그 예이다.
④ O — 9·11 테러와 관련하여 테러리스트들이 공개 매체 속에 대화나 정보를 숨기는 데 스테가노그래피를 사용한 사례가 대표적인 활용 사례로 소개된다.

NoteBase

오답 포인트

①의 '픽셀 일부를 대체한다'는 설명만 보고 맞다고 판단하기 쉽다. 그러나 판별 기준은 대체 여부가 아니라 그 변화가 눈에 띄는지이다. 육안으로 쉽게 구별된다면 비밀정보의 존재를 감추려는 스테가노그래피의 목적에 어긋난다.

다시 나오면 이렇게 판단

'정보의 존재를 숨긴다', '은닉 매체를 이용한다', '변형을 쉽게 알아차리기 어렵다'는 표현은 스테가노그래피의 핵심 특성에 부합한다. 반대로 은닉 전후를 쉽게 식별할 수 있다는 표현은 틀린 것으로 판단한다.

암기 포인트

암호화는 내용을 숨기고, 스테가노그래피는 존재를 숨긴다.

NoteBase

문 2. 다음 내용에 해당하는 공개키 기반 구조(PKI, Public Key Infrastructure)의 구성 요소로 옳은 것은?

· 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다.
· 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다.
· 인증서 폐기 목록(Certificate Revocation List)을 작성한다.

① 사용자
② 등록기관
③ 인증기관
④ 디렉토리

정답 3번

출제 포인트

이 문제는 공개키 기반 구조(PKI)의 구성 요소 가운데 인증서 발급·갱신·폐기와 인증서 폐기 목록(CRL) 작성을 담당하는 주체를 구별하는 문제이다.

핵심 개념

인증기관(CA)은 사용자의 공개키와 신원 정보를 결합한 인증서를 발급하고 인증서의 갱신·폐기 및 CRL 작성을 담당하는 신뢰기관이다. 등록기관(RA)은 인증서 신청자의 신원을 확인하고 등록 업무를 대행하며, 디렉토리는 인증서와 CRL을 조회할 수 있도록 저장·공개한다. 사용자는 인증서를 신청하고 발급받아 이용하는 주체이다.

선지별 해설

① X — 사용자는 인증서를 신청하고 발급받아 이용하는 주체이므로, 인증서를 발급하고 CRL을 작성하는 기관이 아니다. 틀린 표현은 '사용자'이며, 제시된 업무의 담당 주체는 '인증기관'이다.
② X — 등록기관은 사용자의 신원을 확인하고 인증서 발급 신청을 접수·등록하는 역할을 한다. 틀린 표현은 '등록기관'이며, 인증서 발급·갱신·폐기와 CRL 작성은 '인증기관'의 역할이다.
③ O — 인증기관은 공개키 인증서를 생성·발급하고, 필요하면 인증서를 갱신하거나 폐기하며, 폐기된 인증서 정보를 담은 CRL을 작성한다. 제시된 세 업무가 모두 인증기관의 역할과 일치한다.
④ X — 디렉토리는 발급된 인증서와 CRL 등을 저장하여 사용자가 조회할 수 있게 하는 저장소이다. 틀린 표현은 '디렉토리'이며, 인증서와 CRL을 생성·관리하는 주체는 '인증기관'이다.

오답 포인트

등록기관과 인증기관을 혼동하기 쉽다. 등록기관은 신청자의 신원을 확인하는 접수 창구이고, 인증기관은 확인 결과를 바탕으로 인증서를 실제로 발급하며 폐기 상태를 관리한다. 또한 디렉토리는 인증서와 CRL을 보관·공개할 뿐 이를 작성하는 기관이 아니다.

NoteBase

다시 나오면 이렇게 판단

‘신원 확인·등록’이면 등록기관, ‘인증서 발급·갱신·폐기 및 CRL 작성’이면 인증기관, ‘인증서·CRL 저장과 조회 제공’이면 디렉토리로 판단한다.

암기 포인트

RA는 등록, CA는 발급·폐기·CRL, 디렉토리는 저장·공개이다.

NoteBase

문 3. 웹에 관한 정보 노출, 보안 취약점, 악성 파일 및 스크립트 등을 연구하며, 10대(TOP 10) 웹 애플리케이션의 취약점을 발표하는 기관은?

① Open Web Application Security Project
② Web Application Security Working Group
③ IETF Web Security Working Group
④ World Wide Web Consortium

정답 1번

출제 포인트

웹 애플리케이션의 주요 보안 위험을 선정하여 OWASP Top 10으로 발표하는 단체가 OWASP임을 묻는 문제이다.

핵심 개념

OWASP는 소프트웨어와 애플리케이션 보안 향상을 위한 비영리·개방형 보안 공동체이다. 이 문항이 출제된 당시 OWASP의 영문 명칭은 Open Web Application Security Project였으며, 웹 애플리케이션의 핵심 보안 위험을 정리한 OWASP Top 10을 발표한다. 현재 공식 명칭은 Open Worldwide Application Security Project로 바뀌었지만 약칭 OWASP는 그대로이다.

선지별 해설

① O — Open Web Application Security Project는 문항 출제 당시 OWASP의 영문 명칭이다. OWASP는 웹 애플리케이션의 주요 보안 위험을 OWASP Top 10으로 정리하여 발표하므로 문제의 설명에 해당한다.
② X — 틀린 부분은 'Web Application Security Working Group'이다. 이는 OWASP의 정식 명칭이 아니며, 올바르게는 문항 출제 당시 명칭인 'Open Web Application Security Project'이다.
③ X — 틀린 부분은 'IETF Web Security Working Group'이다. IETF는 인터넷 기술 표준을 다루는 조직이지만 문제에서 말한 OWASP Top 10의 발표 주체는 아니다. 올바르게는 'Open Web Application Security Project(OWASP)'이다.
④ X — 틀린 부분은 'World Wide Web Consortium'이다. W3C는 웹 기술의 표준화를 담당하는 국제 공동체로, OWASP Top 10의 발표 주체가 아니다. 올바르게는 'Open Web Application Security Project(OWASP)'이다.

오답 포인트

②와 ③은 'Web', 'Application Security', 'Working Group' 같은 관련 단어를 조합하여 만든 유사 명칭이다. ④의 W3C도 웹 분야의 실제 조직이지만 웹 표준을 다루는 곳이며, 웹 애플리케이션 보안 위험 목록인 Top 10은 OWASP와 연결된다.

NoteBase

다시 나오면 이렇게 판단

문제에 ‘웹 애플리케이션 취약점’과 ‘Top 10’이 함께 나오면 OWASP를 고른다. 웹 표준은 W3C, 인터넷 표준 문서는 IETF, 웹 애플리케이션 보안 위험 Top 10은 OWASP로 구분한다.

암기 포인트

웹 앱 보안 위험 Top 10 = OWASP이다.

NoteBase

문 4. 다음은 어떤 공격에 대한 설명인가?

웹사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로 사용자로 위장한 공격자가 웹사이트에 프로그램 코드를 삽입하여 나중에 이 사이트를 방문하는 다른 사용자의 웹브라우저에서 해당 코드가 실행되도록 한다.

① HTTP 세션 탈취(Session Hijacking)

② 피싱(Phishing)

③ 클릭 탈취(Click Jacking)

④ 크로스 사이트 스크립팅(Cross-Site Scripting : XSS)

정답 4번

출제 포인트

사용자 입력값에 삽입된 악성 스크립트가 다른 사용자의 웹브라우저에서 실행되는 공격을 식별하는 문제이다.

핵심 개념

크로스 사이트 스크립팅(XSS)은 웹 애플리케이션이 사용자 입력을 적절히 검증하거나 출력 시 안전하게 처리하지 않아, 공격자가 삽입한 스크립트가 다른 사용자의 브라우저에서 실행되는 공격이다. 특히 삽입된 코드가 웹사이트에 저장되었다가 나중에 방문한 사용자에게 실행되는 형태는 저장형 XSS에 해당한다.
세션 탈취는 세션 식별자 등을 빼앗아 인증된 사용자로 가장하는 공격이고, 피싱은 위조된 메시지나 사이트로 사용자를 속여 정보를 입력하게 하는 공격이며, 클릭 탈취는 투명하거나 위장된 화면 요소를 겹쳐 사용자가 의도하지 않은 클릭을 하게 하는 공격이다.

선지별 해설

① X — HTTP 세션 탈취는 세션 쿠키나 세션 식별자를 탈취하여 피해자의 인증 상태를 가로채는 공격이다. 이 선지의 공격명은 제시문의 코드 삽입·브라우저 실행과 맞지 않으며, 올바른 대응은 크로스 사이트 스크립팅(XSS)이다.
② X — 피싱은 신뢰할 만한 주체를 사칭한 메시지나 위조 사이트로 사용자를 유인하여 계정정보 등을 입력하게 하는 공격이다. 이 선지의 공격명은 입력 검증 취약점을 이용한 스크립트 실행과 맞지 않으며, 올바른 대응은 크로스 사이트 스크립팅(XSS)이다.
③ X — 클릭 탈취는 정상 화면 위에 투명하거나 위장된 요소를 겹쳐 사용자가 의도하지 않은 버튼이나 링크를 클릭하게 하는 공격이다. 이 선지의 공격명은 악성 코드를 삽입하여 다른 사용자의 브라우저에서 실행시키는 공격과 다르며, 올바른 대응은 크로스 사이트 스크립팅(XSS)이다.
④ O — 입력을 엄밀히 검증하지 않는 취약점을 이용해 웹사이트에 코드를 삽입하고, 이후 방문자의 브라우저에서 그 코드가 실행되도록 하는 공격은 크로스 사이트 스크립팅(XSS)이다.

NoteBase

오답 포인트

XSS가 실행된 뒤 세션 쿠키가 탈취될 수도 있어 ①의 세션 탈취와 혼동하기 쉽다. 그러나 세션 탈취는 공격 결과나 후속 행위가 될 수 있고, 제시문이 직접 설명하는 공격 방식은 사용자 입력을 통한 스크립트 삽입과 다른 방문자의 브라우저에서의 실행이다.

다시 나오면 이렇게 판단

입력값에 코드 삽입과 피해자 브라우저에서의 실행이 함께 제시되면 XSS로 판단한다. 세션 식별자 탈취는 세션 탈취, 가짜 메시지·사이트를 통한 정보 유도는 피싱, 화면 요소를 겹쳐 클릭을 속이는 방식은 클릭 탈취로 구분한다.

암기 포인트

XSS는 입력에 스크립트를 심어 다른 사용자의 브라우저에서 실행시키는 공격이다.

NoteBase

문 5. 다음 중 Windows에서 제공하는 기본 방화벽 설명으로 가장 옳지 않은 것은?

① 연결 보안 규칙의 종류에는 격리, 인증 예외, 서버 간, 터널, 사용자 지정 등이 있다.

② 바이러스 및 웜 뿐만 아니라 스팸이나 원하지 않은 메일의 수신도 차단 할 수 있다.

③ 해커나 악성 소프트웨어가 네트워크나 인터넷을 통해 사용자 컴퓨터에 액세스하지 못하도록 방지하는 기능이다.

④ 새로운 프로그램을 차단할 때 알림을 표시할 수 있도록 설정할 수 있다.

정답 2번

출제 포인트

Windows 기본 방화벽의 네트워크 접근 통제 기능과 바이러스·스팸 차단 기능을 구별하는 문제이다.

핵심 개념

방화벽은 미리 정한 규칙에 따라 네트워크의 인바운드·아웃바운드 통신을 허용하거나 차단하는 보안 기능이다. 악성코드 파일을 탐지·제거하는 백신 기능이나 원하지 않는 메일을 걸러 내는 스팸 필터 기능과는 역할이 다르다.

선지별 해설

① O — 고급 보안이 포함된 Windows 방화벽의 연결 보안 규칙에는 격리, 인증 예외, 서버 간, 터널, 사용자 지정 유형이 있다. 이 규칙은 IPsec을 이용하는 컴퓨터 간 인증 및 연결 보호 조건을 정한다.
② X — 틀린 부분은 방화벽이 '바이러스 및 웜뿐만 아니라 스팸이나 원하지 않는 메일의 수신도 차단할 수 있다'고 한 것이다. 방화벽은 네트워크 통신을 규칙에 따라 제어하며, 바이러스·웜의 탐지와 제거는 백신이, 스팸 및 원하지 않는 메일의 차단은 메일 서비스나 스팸 필터가 담당한다.
③ O — 방화벽은 허용되지 않은 인바운드 연결과 의심스러운 네트워크 통신을 차단하여 해커나 악성 소프트웨어가 네트워크 또는 인터넷을 통해 컴퓨터에 접근하는 것을 방지하는 데 도움을 준다.
④ O — Windows 방화벽은 새로운 앱이나 프로그램의 통신을 차단했을 때 사용자에게 알림을 표시하도록 설정할 수 있다.

오답 포인트

②는 '보안 기능'이라는 공통점만으로 방화벽, 백신, 스팸 필터의 역할을 한데 묶은 선지이다. 방화벽이 악성코드의 네트워크 접근을 막는 데 도움을 줄 수 있어도 바이러스·웜 자체를 탐지·제거하거나 메일 내용을 판별하여 스팸을 거르는 기능은 아니다.

다시 나오면 이렇게 판단

통신의 허용·차단과 포트·앱·연결 규칙은 방화벽, 악성코드의 탐지·치료는 백신, 원하지 않는 메일의 분류·차단은 스팸 필터로 구분한다.

NoteBase

암기 포인트

방화벽은 통신을 거르고, 백신은 악성코드를 잡으며, 스팸 필터는 원하지 않는 메일을 거른다.

NoteBase

문 6. 「개인정보 보호법」 상 다음 업무를 수행하는 자는?

· 개인정보 보호 계획의 수립 및 시행
· 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
· 개인정보 처리와 관련한 불만의 처리 및 피해 구제
· 개인정보 유출 및 오용·남용 방지를 위한 내부통제 시스템의 구축
· 개인정보 보호 교육 계획의 수립 및 시행
· 개인정보 파일의 보호 및 관리·감독

① 개인정보 담당자
② 개인정보 보호책임자
③ 개인정보 취급자
④ 개인정보 처리자

정답 2번

쟁점

이 문제는 개인정보 보호 계획 수립, 처리 실태 조사, 불만 처리, 내부통제, 교육, 개인정보파일 관리 업무를 수행하는 법정 주체를 묻는다. 핵심은 개인정보 보호 업무를 총괄하는 개인정보 보호책임자와 실제 처리 업무를 담당하는 개인정보취급자, 개인정보처리자를 구별하는 것이다.

용어 풀이

개인정보 보호책임자는 개인정보처리자의 개인정보 처리 및 보호 업무를 총괄해서 담당하는 자이다.
개인정보취급자는 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자이고,
개인정보처리자는 업무 목적으로 개인정보파일을 운용하기 위하여 개인정보를 처리하는
공공기관·법인·단체·개인 등이다.

핵심 구분

현행 「개인정보 보호법」 제31조 제4항은 제시된 업무를 개인정보 보호책임자의 업무로 규정한다.
개인정보처리자는 개인정보 보호책임자를 지정하는 주체이고, 개인정보 보호책임자는 개인정보 처리 및 보호 업무를 총괄하는 주체이며, 개인정보취급자는 그 지휘·감독 아래 실제 개인정보 처리 업무를 담당하는 자이다.

NoteBase

선지별 해설

① X — '개인정보 담당자'는 제시된 업무의 법정 주체를 가리키는 정확한 명칭이 아니다. 틀린 표현: 개인정보 담당자. 올바른 표현: 개인정보 보호책임자.
② O — 개인정보 보호 계획의 수립·시행, 처리 실태 조사·개선, 불만 처리와 피해 구제, 내부통제시스템 구축, 보호 교육, 개인정보파일 관리·감독은 개인정보 보호책임자의 법정 업무이다.
③ X — 개인정보취급자는 개인정보처리자의 지휘·감독 아래 실제로 개인정보 처리 업무를 담당하는 자이지, 제시된 보호 업무를 총괄하는 법정 책임자가 아니다. 틀린 표현: 개인정보 취급자. 올바른 표현: 개인정보 보호책임자.
④ X — 개인정보처리자는 업무 목적으로 개인정보파일을 운용하며 개인정보를 처리하는 공공기관·법인·단체·개인 등으로서, 원칙적으로 개인정보 보호책임자를 지정하는 주체이다. 틀린 표현: 개인정보 처리자. 올바른 표현: 개인정보 보호책임자.

오답 포인트

'담당자', '취급자', '처리자'도 개인정보 업무와 관련된 말이므로 혼동하기 쉽다. 그러나 문제의 열거 사항은 단순한 실무 처리나 조직의 일반 의무가 아니라 보호 계획·조사·피해 구제·교육·감독을 아우르는 총괄 책임 업무이다.

다시 나오면 이렇게 판단

계획 수립, 실태 조사, 불만·피해 구제, 내부통제, 교육, 파일 관리·감독처럼 조직 전체의 개인정보 보호 업무가 함께 제시되면 개인정보 보호책임자로 판단한다. 지휘·감독 아래 실제 처리 업무를 하면 개인정보취급자이고, 개인정보파일을 운용하는 기관·법인·단체·개인 등은 개인정보처리자이다.

암기 포인트

처리자는 책임자를 지정하고, 책임자는 보호 업무를 총괄하며, 취급자는 지휘·감독 아래 개인정보를 처리한다.

NoteBase

문 7. 사용자 인증을 위한 접근방법으로는 사용자가 알고 있는 것, 사용자가 가지고 있는 것, 사용자 자신의 특성을 이용하는 것 등이 있다. OTP(One Time Password)에 대한 설명으로 가장 옳지 않은 것은?

① 질의응답 방식은 사용자가 직접 질의 값을 입력하면 응답 값인 OTP가 생성되어 보안성이 높다.

② OTP는 일반적으로 OTP 토큰을 이용하므로 소유에 의한 인증 기법이다.

③ 일반적으로 사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다.

④ 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

정답 3번

출제 포인트

OTP가 소유 기반 인증이라는 점과 OTP 인증의 오류 특성을 생체인증의 식별 오류와 구별하는 문제이다.

핵심 개념

OTP는 한 번만 유효한 비밀번호를 토큰이나 인증 장치가 생성하고, 서버가 그 값을 대조하여 사용자를 인증하는 방식이다.
소유 기반 인증은 사용자가 가진 토큰·카드 등을 확인하고, 생체 기반 인증은 지문·홍채처럼 사용자 자신의 특성을 측정한다. 생체인증은 측정값을 유사도에 따라 판정하므로 오거부와 오인식이 발생할 수 있지만, OTP는 생성값의 일치 여부를 확인하므로 이러한 생체정보 식별 오류와 성격이 다르다.

선지별 해설

① O — 질의응답 방식은 인증 서버가 제시한 질의값을 사용자가 토큰에 입력하고, 토큰이 그 질의값에 대응하는 일회용 응답값을 생성하는 방식이다. 질의마다 응답이 달라 재사용 공격에 강하므로 보안성이 높다.
② O — OTP는 일반적으로 사용자가 소지한 OTP 토큰이나 장치가 비밀번호를 생성하므로 소유에 의한 인증에 해당한다.
③ X — 틀린 부분은 '사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다'이다. 생체인증은 지문·홍채 등의 측정과 임계값 판정 때문에 오거부나 오인식이 발생할 수 있는 반면, OTP는 생성된 값의 일치 여부를 대조하므로 일반적으로 생체인증보다 식별 오류 발생 가능성이 높다고 볼 수 없다. 올바르게는 'OTP는 일반적으로 사용자 자신의 특성을 이용하는 생체인증보다 식별 오류 발생 가능성이 낮다'이다.
④ O — 시간 동기 방식은 토큰과 서버의 시각 동기화가 필요하고, 이벤트 동기 방식은 카운터의 재동기화가 필요할 수 있다. 또한 토큰의 발급·회수·분실 대응도 필요하므로 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

NoteBase

오답 포인트

③은 OTP 토큰의 분실이나 동기화 실패 같은 운영상 문제를 생체인증의 오거부·오인식과 같은 식별 오류로 혼동하게 만든다. 토큰 관리 부담은 ④의 내용이고, 측정값 판정에서 생기는 식별 오류는 주로 생체인증에서 문제된다.

다시 나오면 이렇게 판단

인증요소를 지식·소유·생체 특성으로 먼저 구분한 뒤, OTP는 값의 일치 여부, 생체인증은 측정값의 유사도와 임계값으로 판정한다는 차이를 적용한다. OTP의 대표적 약점은 토큰 관리와 동기화 부담이지 생체인증보다 높은 식별 오류가 아니다.

암기 포인트

OTP는 소유 기반·일회용 값 대조, 생체인증은 특성 기반·오거부와 오인식이다.

NoteBase

문 8. 다음 중 유닉스계열의 시스템에서 핵심부분인 커널(Kernel)에 대한 설명으로 가장 옳지 않은 것은?

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

정답 3번

출제 포인트

유닉스 커널의 역할과 부팅 후 상주 위치를 구별하는 문제이다.

핵심 개념

커널은 운영체제의 핵심으로서 프로세스·메모리·입출력 장치 등의 자원을 관리하고, 셸이나 프로그램의 요청을 시스템 호출을 통해 처리한다. 커널 파일은 보조기억장치에 저장되어 있다가 부팅 과정에서 주기억장치로 적재되며, 실행 중에는 주기억장치에 상주한다.

선지별 해설

① O
유닉스 시스템은 일반적으로 커널, 셸, 파일 시스템을 중심으로 구성되며, 커널은 프로세스 관리, 메모리 관리, 입출력 관리 등 핵심 기능을 수행한다.

② O
데몬은 백그라운드에서 특정 서비스를 제공하는 프로세스이다. 일반 프로세스와 마찬가지로 커널의 프로세스 관리와 스케줄링 대상이므로 커널이 그 실행을 관리한다.

③ X
틀린 표현은 '부팅될 때 가장 먼저 읽혀진다'와 '보조기억장치에 상주한다'이다. 커널보다 앞서 펌웨어와 부트 로더가 동작하며, 커널은 보조기억장치에 저장되어 있다가 부트 로더에 의해 주기억장치로 적재된 후 실행 중 주기억장치에 상주한다.

④ O
셸은 사용자 명령을 해석해 프로그램 실행 등을 요청하고, 커널은 시스템 호출을 통해 필요한 자원과 기능을 제공하므로 둘은 상호 연관되어 작업을 수행한다.

NoteBase

오답 포인트

③은 커널 파일이 보조기억장치에 저장된다는 사실과 실행 중인 커널이 주기억장치에 상주한다는 사실을 바꾸어 표현했다. 또한 부팅 과정에서 커널보다 펌웨어와 부트 로더가 먼저 동작한다는 점도 놓치기 쉽다.

다시 나오면 이렇게 판단

‘저장’과 ‘상주’를 구분한다. 커널 파일은 보조기억장치에 저장되고, 부팅 때 주기억장치로 적재되어 실행 중 주기억장치에 상주한다.

암기 포인트

커널은 디스크에 저장, 메모리에 적재·상주, 시스템 자원을 관리한다.

NoteBase

문 9. 다음 중 쿠키(Cookie)에 대한 설명으로 가장 옳지 않은 것은?

① 사용자가 웹 사이트에 접속할 때 사용자 컴퓨터에서 생성되어 해당 웹 서버에 임시 파일로 전송, 저장된다.

② 웹 사이트 접속 시 HTTP의 무상태성(Statelessness)을 보완하기 위해 사용되는 정보이다.

③ 보존기간에 따라 임시 쿠키와 영구 쿠키로 분류할 수 있다.

④ 사용자가 인식하지 못하는 사이에 사용자의 다양한 정보가 쿠키에 담겨 웹 서버로 전송될 수 있기 때문에 개인정보에 대한 피해가 발생 할 수 있다.

정답 1번

출제 포인트

쿠키가 어디에서 설정·저장되고 언제 서버로 전송되는지, 그리고 보존기간에 따라 어떻게 구분되는지를 묻는 문제이다.

핵심 개념

쿠키는 웹 서버가 브라우저에 저장하도록 설정하거나 웹 페이지의 스크립트가 생성하는 작은 정보이다. 쿠키는 기본적으로 사용자 측 브라우저에 저장되고, 이후 해당 사이트에 요청을 보낼 때 서버로 함께 전송되어 HTTP의 무상태성을 보완한다. 보존기간에 따라 브라우저 세션이 끝나면 사라지는 임시 쿠키와 지정된 만료 시점까지 남는 영구 쿠키로 구분한다.

선지별 해설

① X — '사용자 컴퓨터에서 생성되어 해당 웹 서버에 임시 파일로 전송, 저장된다'는 설명이 틀렸다. 쿠키는 일반적으로 서버의 응답으로 설정되거나 웹 페이지의 스크립트로 생성되어 사용자 측 브라우저에 저장되며, 이후 요청 시 서버로 전송된다.
② O — HTTP는 각 요청을 독립적으로 처리하는 무상태 프로토콜이므로, 쿠키를 이용하면 로그인 상태나 사용자 설정 등 이전 요청과 관련된 상태 정보를 이어 갈 수 있다.
③ O — 보존기간을 기준으로 세션 종료 시 삭제되는 임시 쿠키와 만료일을 두고 저장되는 영구 쿠키로 분류할 수 있다.
④ O — 쿠키에는 식별자, 이용 기록, 사용자 설정 등이 담길 수 있고 요청 시 서버로 전송되므로, 사용자가 충분히 인식하지 못한 상태에서 추적이나 정보 노출 등 개인정보 침해 위험이 발생할 수 있다.

오답 포인트

①은 쿠키가 네트워크를 통해 서버로 전송된다는 사실과 쿠키의 저장 위치를 뒤섞는다. 전송 대상이 서버라고 해서 쿠키 파일의 기본 저장 위치까지 서버인 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

쿠키 관련 선지는 ‘설정 주체’, ‘저장 위치’, ‘전송 시점’을 나누어 판단한다. 서버 응답이나 스크립트로 설정되고, 브라우저에 저장되며, 이후 요청에 실려 서버로 전송된다는 흐름을 기준으로 삼는다.

암기 포인트

쿠키는 브라우저에 저장되고 요청할 때 서버로 전송되며, 세션 쿠키와 영구 쿠키로 나뉜다.

NoteBase

문 10. 다음 설명에 해당하는 접근통제(Access Control) 모델은?

조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다. 사용자가 적절한 직무에 할당되고, 직무에 적합한 접근 권한이 할당된 경우에만 접근할 수 있다.

① Mandatory Access Control

② Role-Based Access Control

③ Discretionary Access Control

④ Access Control List

정답 2번

출제 포인트

사용자 개인이 아니라 직무와 역할을 기준으로 권한을 묶어 부여하는 접근통제 모델을 구별하는 문제이다.

핵심 개념

역할 기반 접근통제(RBAC)는 권한을 역할에 부여하고 사용자를 적절한 역할에 배정하여 접근을 허용하는 모델이다.
MAC는 보안 등급과 허가 등급, RBAC는 직무·역할, DAC는 객체 소유자의 재량, ACL은 객체별 접근 권한 목록을 기준으로 한다.

선지별 해설

① X — Mandatory Access Control(MAC)은 보안 정책에 따라 객체의 보안 등급과 사용자의 허가 등급을 비교해 접근을 통제한다. 틀린 부분은 직무와 직무 권한 등급을 기준으로 한다는 대응이며, 올바르게는 보안 레이블과 허가 등급을 기준으로 하는 모델이다.
② O — Role-Based Access Control(RBAC)은 직무에 대응하는 역할에 권한을 부여하고 사용자를 그 역할에 할당한다. 제시문의 '직무', '직무에 허용된 연산', '사용자의 직무 할당'이 모두 RBAC의 특징이다.
③ X — Discretionary Access Control(DAC)은 객체 소유자가 사용자의 신원 등을 기준으로 접근 권한을 재량적으로 부여하거나 회수한다. 틀린 부분은 직무를 중심으로 권한을 관리한다는 대응이며, 올바르게는 객체 소유자의 재량을 중심으로 하는 모델이다.
④ X — Access Control List(ACL)은 각 객체에 대해 어떤 사용자나 주체가 어떤 연산을 할 수 있는지를 기록한 목록이다. 틀린 부분은 ACL을 직무 기반 접근통제 모델로 본 것이며, 올바르게는 객체별 접근 권한을 열거하는 방식이다.

NoteBase

오답 포인트

‘권한 등급’이라는 표현만 보고 MAC을 고르기 쉽지만, 제시문은 보안 등급이 아니라 직무와 역할에 권한을 연결한다. 또한 ACL은 권한을 표현하는 목록이고, RBAC는 조직의 직무 변화에 맞춰 권한을 관리하는 모델이라는 점이 다르다.

다시 나오면 이렇게 판단

직무·역할에 권한을 묶고 사용자를 역할에 배정하면 RBAC, 보안 등급을 강제하면 MAC, 소유자가 권한을 정하면 DAC, 객체별 주체와 허용 연산을 나열하면 ACL로 판단한다.

암기 포인트

RBAC는 사용자→역할→권한, MAC는 등급, DAC는 소유자 재량, ACL은 객체별 권한 목록이다.

NoteBase

문 11. 다음 중 윈도우 레지스트리 키 중에서 최근 열어본 파일의 목록을 기록하고 있는 것은?

① RUN

② RecentDocs

③ Docs

④ OfficeDocs

정답 2번

출제 포인트

윈도우 레지스트리의 MRU(Most Recently Used) 아티팩트 가운데 최근 열어 본 파일 목록을 저장하는 키를 구별하는 문제이다.

핵심 개념

RecentDocs는 윈도우 탐색기에서 최근 접근한 파일과 폴더의 흔적을 기록하는 레지스트리 키이다. 파일 확장자별 하위 키가 함께 생성될 수 있어 어떤 종류의 파일을 최근 열었는지 분석하는 데 활용된다.
Run 계열 키는 로그온 때 프로그램을 자동 실행하는 용도이고, RunMRU는 실행 창에 입력한 명령의 이력을 저장하므로 RecentDocs와 구별된다.

선지별 해설

① X — RUN은 사용자가 최근 열어 본 파일 목록을 기록하는 키가 아니다. 일반적으로 Run 키는 로그온 시 자동 실행할 프로그램을 등록한다. 틀린 키 이름은 RUN이며, 최근 열어 본 파일 목록을 기록하는 키는 RecentDocs이다.
② O — RecentDocs는 최근 접근하거나 열어 본 파일·폴더의 목록을 남기는 대표적인 레지스트리 아티팩트이므로 옳다.
③ X — Docs는 최근 열어 본 파일 목록을 기록하는 표준 키 이름이 아니다. 틀린 키 이름은 Docs이며, 올바른 키 이름은 RecentDocs이다.
④ X — OfficeDocs는 윈도우 전체의 최근 파일 목록을 기록하는 표준 키 이름이 아니다. Office 프로그램의 최근 파일 이력은 응용 프로그램별 MRU 영역에서 확인하며, 이 문항이 묻는 윈도우의 일반적인 최근 문서 키는 RecentDocs이다.

오답 포인트

①의 RUN을 실행 이력인 RunMRU와 혼동하거나, ③ Docs·④ OfficeDocs처럼 파일을 연상시키는 이름을 실제 레지스트리 키로 착각하기 쉽다. 최근 파일은 RecentDocs, 실행 창 명령은 RunMRU, 로그온 자동 실행은 Run으로 구분한다.

NoteBase

다시 나오면 이렇게 판단

문제의 행위를 먼저 찾는다. ‘최근 열어 본 파일’이면 RecentDocs, ‘실행 창에 입력한 명령’이면 RunMRU, ‘로그온 때 자동 실행’이면 Run 키로 판단한다.

암기 포인트

최근 문서(Recent Documents)는 RecentDocs, 실행 명령 기록은 RunMRU, 자동 실행은 Run이다.

NoteBase

문 12. 다음 중 윈도우 “원격 데스크톱 연결” 명령어로 가장 옳은 것은?

① vnc

② mstsc

③ teamviewer

④ ftp

정답 2번

출제 포인트

Windows의 원격 데스크톱 연결 클라이언트를 실행하는 명령어와 다른 원격접속·파일전송 도구를 구별하는 문제이다.

핵심 개념

mstsc는 Microsoft Terminal Services Client의 실행 명령어로, Windows의 '원격 데스크톱 연결' 프로그램을 연다. VNC와 TeamViewer는 별도의 원격제어 방식 또는 프로그램이고, FTP는 파일 전송 프로토콜이다.

선지별 해설

① X — vnc는 VNC 방식의 원격 화면 제어를 가리키며 Windows 기본 '원격 데스크톱 연결' 실행 명령어가 아니다. 틀린 표현은 'vnc'이고, 올바른 명령어는 'mstsc'이다.
② O — mstsc를 실행하면 Windows의 '원격 데스크톱 연결' 클라이언트가 열린다.
③ X — teamviewer는 별도로 설치하여 사용하는 원격지원·원격제어 프로그램의 이름이며 Windows 기본 '원격 데스크톱 연결' 명령어가 아니다. 틀린 표현은 'teamviewer'이고, 올바른 명령어는 'mstsc'이다.
④ X — ftp는 네트워크에서 파일을 전송하는 프로토콜 또는 그 클라이언트를 뜻하며 원격 데스크톱 화면에 접속하는 명령어가 아니다. 틀린 표현은 'ftp'이고, 올바른 명령어는 'mstsc'이다.

오답 포인트

vnc와 teamviewer도 원격으로 다른 컴퓨터를 제어할 수 있어 혼동하기 쉽다. 그러나 문항은 원격제어 도구 일반이 아니라 Windows에 내장된 '원격 데스크톱 연결'의 실행 명령어를 묻는다.

다시 나오면 이렇게 판단

문제에 Windows의 '원격 데스크톱 연결'과 '명령어'가 함께 나오면 mstsc를 선택한다. 원격제어 제품명과 파일전송 프로토콜은 구별한다.

NoteBase

암기 포인트

Windows 원격 데스크톱 연결 = mstsc

NoteBase

문 13. 다음 중 비선점(Non-preemptive) 스케쥴링 방식으로 바르게 묶인 것은?

① FCFS, SJF

② FCFS, Round Robin

③ SJF, SRT

④ SJF, Round Robin

정답 1번

출제 포인트

이 문제는 CPU 스케줄링 알고리즘이 실행 중인 프로세스의 CPU를 강제로 빼앗을 수 있는지에 따라 선점형과 비선점형을 구분하는 문제이다.

핵심 개념

비선점 스케줄링: 한 프로세스가 CPU를 할당받으면 종료되거나 대기 상태로 전환될 때까지 다른 프로세스가 CPU를 강제로 빼앗지 않는 방식이다. FCFS와 비선점형 SJF가 이에 해당한다.
선점 스케줄링: 운영체제가 실행 중인 프로세스의 CPU를 회수하여 다른 프로세스에 할당할 수 있는 방식이다. Round Robin과 SRT가 이에 해당한다.
SJF는 준비 큐에서 실행 시간이 가장 짧은 작업을 먼저 선택하는 비선점 방식이고, SRT는 남은 실행 시간이 가장 짧은 프로세스를 선택하며 새 프로세스 도착 시 선점할 수 있는 SJF의 선점형 방식이다.

선지별 해설

① O — FCFS는 도착 순서대로 실행하며 일단 CPU를 받은 프로세스를 강제로 중단시키지 않는다. SJF도 선택된 작업이 끝날 때까지 실행하는 비선점 방식이므로 둘을 바르게 묶었다.
② X — 틀린 표현은 'Round Robin'이다. Round Robin은 일정 시간 할당량이 끝나면 CPU를 회수하는 선점 방식이다. 올바르게는 'FCFS, SJF'가 비선점 방식의 묶음이다.
③ X — 틀린 표현은 'SRT'이다. SRT는 더 짧은 남은 실행 시간을 가진 프로세스가 도착하면 현재 프로세스를 선점할 수 있다. 올바르게는 'SJF, FCFS'가 비선점 방식의 묶음이다.
④ X — 틀린 표현은 'Round Robin'이다. Round Robin은 시간 할당량을 기준으로 실행 중인 프로세스를 선점한다. 올바르게는 'SJF, FCFS'가 비선점 방식의 묶음이다.

오답 포인트

SJF와 SRT를 모두 '짧은 작업 우선' 계열로만 기억하면 선점 여부를 놓치기 쉽다. 또한 Round Robin은 순환 순서로 공평하게 실행하지만, 시간 할당량 만료 시 CPU를 회수하므로 비선점 방식이 아니다.

NoteBase

다시 나오면 이렇게 판단

실행 중인 프로세스를 강제로 중단시키는 계기가 있는지를 확인한다. 시간 할당량 만료로 교체하는 Round Robin과 더 짧은 잔여 시간이 생기면 교체하는 SRT는 선점형이고, FCFS와 기본 SJF는 비선점형이다.

암기 포인트

비선점은 FCFS·SJF, 선점은 Round Robin·SRT이다.

NoteBase

문 14. 다음 중 리눅스 계정 관리 파일 /etc/shadow에서 확인할 수 있는 정보로 가장 관련 없는 것은?

① 사용자 계정 이름

② 암호화된 사용자 패스워드

③ 사용자 패스워드 최소 길이

④ 사용자 패스워드 만료일까지 남은 기간

정답 3번

출제 포인트

/etc/shadow에 저장되는 계정·패스워드 정보와 패스워드 정책 설정 정보를 구분하는 문제이다.

핵심 개념

/etc/shadow는 사용자 계정 이름, 암호화된 패스워드 정보, 패스워드를 마지막으로 변경한 날, 최소·최대 사용 기간, 만료 경고 기간, 계정 만료일 등을 콜론(:)으로 구분해 저장한다. 여기서 '최소 사용 기간'은 패스워드를 다시 변경할 수 있을 때까지의 일수이지 패스워드의 최소 문자 수가 아니다.

선지별 해설

① O — 각 레코드의 첫 번째 필드에는 사용자 계정 이름이 저장된다.
② O — 두 번째 필드에는 암호화된 사용자 패스워드 정보가 저장된다. 실제 환경에서는 패스워드 해시 또는 잠금 상태를 나타내는 값이 들어갈 수 있다.
③ X — 틀린 표현은 '사용자 패스워드 최소 길이'이다. /etc/shadow에는 패스워드의 최소 문자 수가 아니라 패스워드 변경 후 다시 변경할 수 있을 때까지의 최소 사용 기간이 일수로 저장된다. 패스워드 최소 길이는 별도의 패스워드 품질 정책에서 관리한다.
④ O — /etc/shadow에는 마지막 패스워드 변경일, 최대 사용 기간, 만료 전 경고 기간 등 만료 시점을 판단하는 정보가 저장되므로 패스워드 만료일까지 남은 기간과 관련된 정보를 확인할 수 있다.

오답 포인트

③의 '최소 길이'를 /etc/shadow의 '최소 사용 기간'과 혼동하기 쉽다. 둘 다 '최소'라는 표현을 쓰지만, 전자는 문자 수이고 후자는 패스워드 변경 간격을 뜻한다.

다시 나오면 이렇게 판단

/etc/shadow의 항목은 계정 이름, 패스워드 해시, 날짜·기간 중심의 만료 관리 정보로 판단한다. 문자 조합이나 최소 길이처럼 패스워드 품질을 정하는 항목은 별도의 정책 설정으로 구분한다.

NoteBase

암기 포인트

shadow는 해시와 날짜·기간, 최소 길이는 패스워드 품질 정책이다.

NoteBase

문 15. 다음 중 유닉스 시스템의 로그분석에 사용하는 로그 파일에 대한 설명으로 가장 옳지 않은 것은?

① wtmp : 사용자 로그인, 로그아웃 정보를 기록

② sulog : su(switch user) 명령어 사용 정보를 기록

③ utmp : 시스템에 현재 로그인한 사용자의 정보를 기록

④ btmp : 로그인에 성공한 정보를 기록

정답 4번

출제 포인트

이 문제는 유닉스 로그인 관련 로그 파일인 wtmp, sulog, utmp, btmp가 각각 어떤 접속 정보를 기록하는지 구별하는 문제이다.

핵심 개념

utmp는 현재 로그인 상태, wtmp는 로그인·로그아웃 이력, btmp는 로그인 실패 이력을 기록한다. sulog는 su 명령을 이용한 사용자 전환 시도를 기록한다.

선지별 해설

① O — wtmp는 사용자의 로그인과 로그아웃 등 접속 이력을 기록하므로 옳다.
② O — sulog는 su(switch user) 명령을 사용한 사용자 전환 관련 정보를 기록하므로 옳다.
③ O — utmp는 현재 시스템에 로그인해 있는 사용자의 상태 정보를 기록하므로 옳다.
④ X — 틀린 표현은 '로그인에 성공한 정보'이다. btmp는 로그인에 실패한 시도 정보를 기록한다. 로그인 성공을 포함한 접속 이력은 wtmp에서 확인한다.

오답 포인트

wtmp와 btmp는 이름이 비슷하지만 기록 대상이 다르다. ④는 btmp를 성공 로그인 기록으로 바꾸어 제시한 것이 함정이다.

다시 나오면 이렇게 판단

'현재 접속자'는 utmp, '접속 이력'은 wtmp, '실패한 로그인'은 btmp, 'su 사용자 전환'은 sulog로 대응시켜 판단한다.

암기 포인트

utmp는 현재, wtmp는 접속 이력, btmp는 실패, sulog는 su 사용 기록이다.

NoteBase

문 16. 다음 중 데이터베이스 보안 요구사항으로 가장 옳지 않은 것은?

① 데이터 무결성 보장

② 비밀 데이터 관리 및 보호

③ 추론 보장

④ 사용자 인증

정답 3번

출제 포인트

데이터베이스 보안이 요구하는 무결성·기밀성·인증과, 민감한 정보를 알아내는 추론을 통제하는 개념을 구별하는 문제이다.

핵심 개념

데이터베이스 보안은 허가되지 않은 열람·변경·파괴를 막아 기밀성, 무결성, 가용성을 지키고 정당한 사용자인지를 확인하는 것이다.
추론 통제는 공개가 허용된 여러 데이터나 질의 결과를 결합하여 비밀 정보를 유추하지 못하도록 제한하는 것이다. 보안이 보장해야 하는 것은 추론 자체가 아니라 부당한 추론의 방지이다.

선지별 해설

① O — 데이터 무결성 보장은 데이터가 권한 없이 변경·삭제되거나 훼손되지 않고 정확성과 일관성을 유지하게 하는 데이터베이스 보안 요구사항이다.
② O — 비밀 데이터 관리 및 보호는 인가되지 않은 사용자의 접근이나 노출을 막아 기밀성을 유지하는 요구사항이다.
③ X — 틀린 표현은 '추론 보장'이다. 추론을 보장하면 공개 데이터의 조합을 통해 비밀 정보가 드러날 수 있으므로 보안 목적과 반대이다. 올바르게는 '비밀 정보에 대한 부당한 추론 방지 또는 추론 통제'이다.
④ O — 사용자 인증은 접근을 요청한 사람이 주장하는 정당한 사용자인지 확인하여 비인가 접근을 막는 보안 요구사항이다.

오답 포인트

③의 '보장'이라는 긍정적 표현 때문에 보안 기능처럼 보이지만, 데이터베이스 보안에서는 민감한 정보의 추론을 가능하게 하는 것이 아니라 이를 방지·통제해야 한다.

다시 나오면 이렇게 판단

각 표현이 정보의 보호와 정당한 이용을 강화하는지 확인한다. 무결성·기밀성·인증은 보호를 강화하지만, 비밀 정보의 추론을 '보장'하는 표현은 보호 목적에 어긋난다.

NoteBase

암기 포인트

무결성은 변조 방지, 기밀성은 노출 방지, 인증은 사용자 확인, 추론은 보장이 아니라 통제이다.

NoteBase

문 17. 해양경찰청은 4명이 사용할 수 있는 암호 시스템을 도입하려고 한다. 대칭키 암호 시스템과 공개키 암호 시스템 도입 시 필요한 키의 개수를 각각 구분하여 순서대로 나열한 것은?

① 2개, 4개

② 4개, 6개

③ 6개, 8개

④ 8개, 10개

정답 3번

출제 포인트

4명이 서로 안전하게 통신할 때 대칭키 방식의 사람 쌍별 공유키 수와 공개키 방식의 개인별 공개키·개인키 수를 구분하여 계산하는 문제이다.

조건 정리

사용자는 4명이다.
대칭키 암호 시스템에서는 통신하는 두 사람마다 서로 공유하는 비밀키 1개가 필요하다.
공개키 암호 시스템에서는 각 사용자가 공개키 1개와 개인키 1개로 이루어진 키 쌍을 가진다.

사용할 공식

사용자가 n명일 때 대칭키 수는 $\frac{n(n-1)}{2}$개이고, 공개키 시스템의 전체 키 수는 $2n$개이다.
대칭키는 두 사람의 조합마다 하나씩 필요하고, 공개키 방식은 사람마다 공개키와 개인키가 하나씩 필요하므로 이 공식을 사용한다.

계산 과정

대칭키 수: $\frac{4(4-1)}{2} = 6$개이다.
공개키 시스템의 키 수: $2 \times 4 = 8$개이다.
따라서 순서대로 6개, 8개이다.

선지 판단

① X — ‘2개, 4개’는 두 방식의 키 수를 모두 적게 센 값이다. 올바르게는 대칭키 6개, 공개키 8개이다.
② X — ‘4개, 6개’는 각 사용자에게 대칭키 1개만 배정한다고 잘못 보고, 공개키도 전체 8개가 아닌 일부만 센 값이다. 올바르게는 6개, 8개이다.
③ O — 대칭키는 사용자 두 명의 조합 수인 6개이고, 공개키 방식은 4명에게 공개키와 개인키가 각각 하나씩 필요하므로 8개이다.
④ X — ‘8개, 10개’는 두 방식의 필요한 키 수를 실제보다 각각 2개씩 많이 센 값이다. 올바르게는 6개, 8개이다.

NoteBase

오답 포인트

대칭키를 사용자 수인 4개로 세거나 공개키 방식에서 공개키만 세어 4개라고 판단하기 쉽다. 대칭키는 사람 수가 아니라 서로 통신하는 사람 쌍의 수를 세고, 공개키 방식은 개인별 공개키와 개인키를 모두 센다.

다시 나오면 이렇게 판단

사용자가 n명이면 대칭키는 서로 다른 두 사람의 조합인 $\binom{n}{2}$, 공개키 방식의 전체 키는 개인별 키 쌍을 합한 $2n$으로 판단한다.

암기 포인트

대칭키는 '사람 쌍마다 1개', 공개키 방식은 '사람마다 2개'이다.

NoteBase

문 18. 다음 중 전자서명(Digital Signature)이 제공하는 기능으로 가장 옳지 않은 것은?

① 부인 방지(Non Repudiation)

② 변경 불가(Unalterable)

③ 서명자 인증(Authentication)

④ 재사용 가능(Reusable)

정답 4번

출제 포인트

전자서명이 제공하는 서명자 인증, 무결성, 부인 방지와 전자서명의 재사용 가능 여부를 구별하는 문제이다.

핵심 개념

전자서명은 서명자의 개인키로 메시지와 결합된 서명값을 만들고 공개키로 이를 검증하는 기술이다. 이를 통해 서명자를 확인하고, 서명 후 메시지가 변경되었는지 탐지하며, 서명 사실의 부인을 방지할 수 있다. 서명값은 특정 메시지에 종속되므로 다른 메시지의 서명으로 재사용할 수 없다.

선지별 해설

① O — 부인 방지는 전자서명의 대표 기능이다. 서명자의 개인키로 생성된 유효한 서명은 서명자가 나중에 그 서명 사실을 부인하기 어렵게 한다.
② O — 변경 불가는 서명된 메시지가 바뀌면 검증이 실패한다는 뜻이다. 즉 변경 행위 자체를 물리적으로 막는 것이 아니라 변경 여부를 탐지하여 무결성을 확인한다.
③ O — 공개키로 전자서명을 검증하면 해당 개인키를 가진 서명자가 생성한 서명인지 확인할 수 있으므로 서명자 인증 기능을 제공한다.
④ X — 틀린 표현은 '재사용 가능'이다. 전자서명은 특정 메시지의 내용과 결합되어 생성되므로 다른 메시지에 그대로 붙여 재사용하면 검증에 실패한다. 올바르게는 '다른 메시지의 서명으로 재사용할 수 없다'이다.

오답 포인트

②의 '변경 불가'를 파일 수정 자체가 불가능하다는 뜻으로 해석하면 혼동하기 쉽다. 전자서명이 보장하는 것은 변경 방지가 아니라 변경 탐지를 통한 무결성이다. 반면 ④의 '재사용 가능'은 서명값이 메시지마다 달라진다는 성질에 정면으로 어긋난다.

다시 나오면 이렇게 판단

전자서명의 기능은 '누가 서명했는가(서명자 인증)', '내용이 바뀌었는가(무결성)', '서명 사실을 부인할 수 있는가(부인 방지)'로 판단한다. 특정 메시지에 대한 서명을 다른 메시지에 옮겨 쓸 수 있다는 설명은 틀린 것으로 판단한다.

NoteBase

암기 포인트

전자서명은 인증·무결성·부인 방지를 제공하고, 서명값은 메시지에 종속되어 재사용할 수 없다.

NoteBase

문 19. 다음 중 능동적 보안 공격에 해당하는 것을 모두 고르면?

㉠ 신분위장
㉡ 도청
㉢ 메시지 변조
㉣ 트래픽 분석
㉤ 서비스 거부

① ㉠, ㉡, ㉢
② ㉠, ㉢, ㉤
③ ㉡, ㉢, ㉣
④ ㉢, ㉣, ㉤

정답 2번

출제 포인트

보안 공격이 시스템의 자원이나 데이터에 변화를 일으키는 능동적 공격인지, 정보를 몰래 관찰하기만 하는 수동적 공격인지 구분하는 문제이다.

핵심 개념

능동적 공격: 데이터의 변경, 거짓 데이터의 생성, 서비스 방해처럼 시스템의 상태나 정상 동작에 영향을 주는 공격이다. 신분위장, 메시지 변조, 서비스 거부가 해당한다.
수동적 공격: 통신 내용을 엿보거나 통신 양상을 관찰하지만 데이터나 시스템 상태를 직접 바꾸지는 않는 공격이다. 도청과 트래픽 분석이 해당한다.

NoteBase

선지별 해설

① X
㉠ 신분위장과 ㉢ 메시지 변조는 능동적 공격이지만, ㉡ 도청은 통신 내용을 몰래 획득하는 수동적 공격이다. 틀린 부분은 ㉡을 포함하고 ㉤ 서비스 거부를 빠뜨린 것이며, 올바른 조합은 ㉠, ㉢, ㉤이다.

② O
㉠ 신분위장은 공격자가 다른 주체인 것처럼 행세하는 공격이고, ㉢ 메시지 변조는 전송 내용을 변경하는 공격이며, ㉤ 서비스 거부는 정상적인 서비스 제공을 방해하는 공격이다. 세 가지 모두 시스템이나 통신의 정상 상태에 영향을 주는 능동적 공격이다.

③ X
㉢ 메시지 변조만 능동적 공격이고, ㉡ 도청과 ㉣ 트래픽 분석은 정보를 관찰하는 수동적 공격이다. 틀린 부분은 ㉡과 ㉣을 포함하고 ㉠과 ㉤을 빠뜨린 것이며, 올바른 조합은 ㉠, ㉢, ㉤이다.

④ X
㉢ 메시지 변조와 ㉤ 서비스 거부는 능동적 공격이지만, ㉣ 트래픽 분석은 통신량·빈도·상대방 등의 통신 양상을 관찰하는 수동적 공격이다. 틀린 부분은 ㉣을 포함하고 ㉠ 신분위장을 빠뜨린 것이며, 올바른 조합은 ㉠, ㉢, ㉤이다.

오답 포인트

도청과 트래픽 분석도 공격이므로 능동적 공격으로 착각하기 쉽다. 그러나 공격의 위험성이나 불법성이 아니라 데이터·시스템 상태를 직접 변화시키는지를 기준으로 구분한다.

다시 나오면 이렇게 판단

내용을 엿보거나 통신 패턴만 관찰하면 수동적 공격으로, 신원을 속이거나 메시지를 바꾸거나 서비스를 방해하면 능동적 공격으로 판단한다.

암기 포인트

관찰은 수동, 위장·변조·방해는 능동이다.

NoteBase

문 20. 리눅스 운영체제에서 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?(단, kcg.txt는 일반파일이다.)

chmod 761 kcg.txt

① -rwxr-x--x

② -rwxrw---x

③ -rwxr-x---

④ -rw-r-----

정답 2번

출제 포인트

chmod의 8진수 권한을 소유자·그룹·기타 사용자 순서의 문자 권한으로 변환하는 문제이다.

핵심 개념

읽기(r)는 4, 쓰기(w)는 2, 실행(x)은 1이며, 각 자리의 합으로 권한을 나타낸다. 7은 rwx, 6은 rw-, 1은 --x이다. 일반 파일은 맨 앞 문자가 -이므로 chmod 761 kcg.txt의 권한은 -rwxrw---x가 된다.

선지별 해설

① X

-rwxr-x--x에서 그룹 권한 r-x는 5이므로 6과 일치하지 않는다. 틀린 부분은 그룹 권한 r-x이며, 올바르게는 rw-이다.

② O

-rwxrw---x는 일반 파일(-), 소유자 7(rwx), 그룹 6(rw-), 기타 사용자 1(--x)을 정확히 나타낸다.

③ X

-rwxr-x---는 그룹 권한이 5(r-x), 기타 사용자 권한이 0(---)이므로 761이 아니다. 올바르게는 그룹을 rw-, 기타 사용자를 --x로 표시한 -rwxrw---x이다.

④ X

-rw-r-----는 소유자 6(rw-), 그룹 4(r--), 기타 사용자 0(---)을 나타내므로 640에 해당한다. 761의 올바른 표기는 -rwxrw---x이다.

NoteBase

오답 포인트

6을 r-x로 잘못 바꾸거나 마지막 1의 실행 권한 x를 빠뜨리기 쉽다. 각 숫자를 소유자·그룹·기타 사용자 순서로 따로 변환해야 한다.

다시 나오면 이렇게 판단

각 자리에서 4(r), 2(w), 1(x)를 분해한 뒤 소유자·그룹·기타 사용자 순서로 이어 붙인다. 파일 종류를 나타내는 첫 문자는 일반 파일이면 -로 적는다.

암기 포인트

4는 r, 2는 w, 1은 x이므로 761은 rwx·rw-·--x이다.

NoteBase