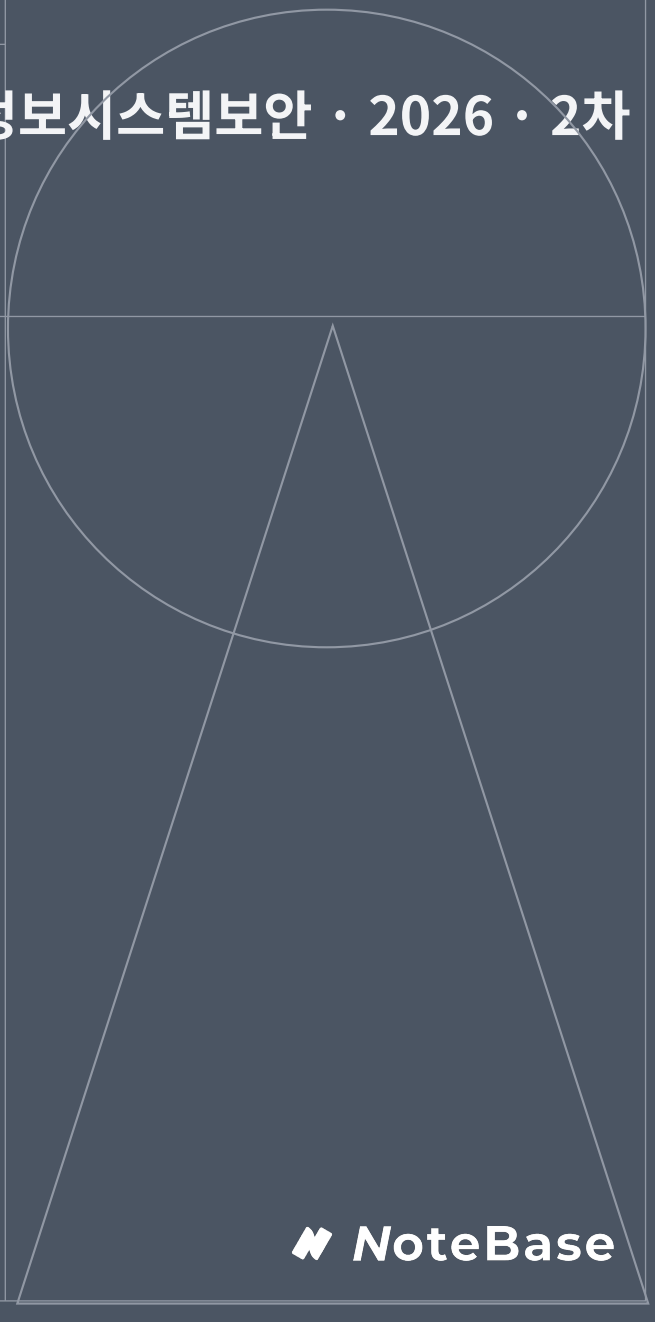
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2026 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2026 · 2차

공무원/해경/일반직 9급 · 정보시스템보안 · 2026 · 2차

문 1. 다음 중 전자서명의 요구사항으로 가장 옳지 않은 것은?

① 위조 불가

② 서명자 인증

③ 부인 방지

④ 변경 가능

정답 4번

출제 포인트

전자서명이 충족해야 하는 위조 방지, 서명자 인증, 부인 방지 및 무결성의 의미를 구별하는 문제이다.

핵심 개념

전자서명은 전자문서의 서명자를 확인하고, 서명 후 문서가 바뀌었는지를 검증하며, 서명자가 자신의 서명 행위를 부인하기 어렵게 하는 기술이다. 따라서 정당한 서명자 외에는 서명을 위조하기 어려워야 하고, 서명된 내용이 변경되면 검증에 실패해야 한다.

선지별 해설

① O — 위조 불가는 전자서명의 핵심 요구사항이다. 서명 생성에 필요한 비밀정보를 모르는 제3자가 유효한 서명을 만들어 내기 어려워야 한다.
② O — 서명자 인증은 전자서명을 검증하여 누가 서명했는지를 확인하는 성질이므로 요구사항에 해당한다.
③ O — 부인 방지는 서명자가 나중에 자신의 서명 사실을 부인하기 어렵게 하는 성질이므로 요구사항에 해당한다.
④ X — ‘변경 가능’이 틀린 표현이다. 올바르게는 ‘서명된 전자문서의 변경을 탐지할 수 있어야 한다’이다. 서명 후 내용이 변경되면 기존 전자서명의 검증이 실패해야 하므로, 변경을 허용하는 것이 요구사항은 아니다.

오답 포인트

④의 ‘변경 가능’을 전자문서 자체의 편집 가능성과 혼동하기 쉽다. 전자문서를 기술적으로 수정할 수 있더라도, 서명된 내용을 수정하면 기존 서명은 더 이상 유효하게 검증되어서는 안 된다.

NoteBase

다시 나오면 이렇게 판단

전자서명 관련 선지는 '누가 서명했는가', '위조할 수 있는가', '서명 사실을 부인할 수 있는가', '서명 후 내용 변경을 알아낼 수 있는가'를 기준으로 판단한다. 변경을 허용하거나 변경 후에도 기존 서명이 유효하다는 표현은 전자서명의 무결성 요구에 어긋난다.

암기 포인트

전자서명은 서명자 확인·위조 방지·부인 방지·변경 탐지를 보장한다.

NoteBase

문 2. 다음 중 개인정보보호위원회에서 고시한 「개인정보의 안전성 확보조치 기준」 제7조(개인정보의 암호화)에 규정된 안전한 암호 알고리즘으로 암호화하여 저장하여야 하는 개인정보로 가장 옳지 않은 것은?

① 여권번호

② 운전면허번호

③ 사원번호

④ 외국인등록번호

정답 3번

쟁점

이 문제는 「개인정보의 안전성 확보조치 기준」 제7조 제2항이 안전한 암호 알고리즘으로 암호화하여 저장하도록 열거한 이용자의 개인정보를 구별하는 문제이다.

용어 풀이

안전한 암호 알고리즘에 의한 저장 = 권한 없는 사람이 원문을 알아볼 수 없도록 검증된 암호화 방식을 적용하여 개인정보를 보관하는 것이다.

핵심 구분

제7조 제2항의 열거 대상은 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 생체인식정보이다. 사원번호는 이 열거 대상에 포함되지 않는다.

NoteBase

선지별 해설

① O
여권번호는 제7조 제2항 제2호에 열거되어 있으므로 안전한 암호 알고리즘으로 암호화하여 저장하여야 하는 개인정보에 해당한다.

② O
운전면허번호는 제7조 제2항 제3호에 열거되어 있으므로 안전한 암호 알고리즘으로 암호화하여 저장하여야 하는 개인정보에 해당한다.

③ X
사원번호는 제7조 제2항이 열거한 암호화 저장 대상에 포함되지 않는다.
틀린 표현: 사원번호가 제7조 제2항에 규정된 암호화 저장 대상이라는 부분
올바른 표현: 사원번호는 제7조 제2항의 열거 대상이 아니며,
주민등록번호·여권번호·운전면허번호·외국인등록번호·신용카드번호·계좌번호·생체인식정보가 열거되어 있다.

④ O
외국인등록번호는 제7조 제2항 제4호에 열거되어 있으므로 안전한 암호 알고리즘으로 암호화하여 저장하여야 하는 개인정보에 해당한다.

오답 포인트

③의 사원번호도 개인을 식별하는 번호라는 이유만으로 법정 열거 대상이라고 판단하기 쉽다. 그러나 이 문항은 일반적인 개인정보 여부가 아니라 제7조 제2항에 명시적으로 열거되었는지를 묻는다.

다시 나오면 이렇게 판단

암호화 저장 대상 문항에서는 먼저 제7조 제2항의 열거 목록과 선지를 대조한다. 조직이 자체적으로 부여한 사원번호와 국가·금융·생체 관련 열거정보를 구분하면 된다.

암기 포인트

주민·여권·면허·외국인 + 카드·계좌 + 생체는 열거 대상이고, 사원번호는 아니다.

NoteBase

문 3. 다음 중 「개인정보 보호법」 제3조(개인정보 보호 원칙)의 내용으로 가장 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

② 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

③ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

④ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용 및 제공할 수 있다.

정답 4번

쟁점

이 문제는 「개인정보 보호법」 제3조의 개인정보 보호 원칙에 관한 문제이다. 핵심은 개인정보를 처리 목적에 필요한 범위에서만 처리해야 한다는 목적 제한 원칙을 구별하는 것이다.

용어 풀이

목적 제한 원칙은 개인정보를 명확한 처리 목적에 필요한 범위에서 적합하게 처리하고, 그 목적 밖으로 함부로 활용하지 않는 원칙이다.

핵심 구분

「개인정보 보호법」 제3조 제2항은 개인정보처리자가 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다고 규정한다. 따라서 목적 내 적합한 처리는 의무이지만 목적 외 활용은 허용이 아니라 금지이다.

NoteBase

선지별 해설

① O
개인정보의 처리 목적에 필요한 범위에서 정확성, 완전성 및 최신성이 보장되도록 하여야 한다는 내용은 제3조 제3항의 원칙에 해당한다.

② O
정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다는 내용은 제3조 제6항의 원칙에 해당한다.

③ O
법과 관계 법령상의 책임과 의무를 준수하고 실천하여 정보주체의 신뢰를 얻도록 노력하여야 한다는 내용은 제3조 제8항의 원칙에 해당한다.

④ X
처리 목적에 필요한 범위에서 적합하게 처리하여야 한다는 부분은 맞지만, 목적 외의 용도로 활용 및 제공할 수 있다고 한 부분이 틀리다.
틀린 표현: 그 목적 외의 용도로 활용 및 제공할 수 있다.
올바른 표현: 그 목적 외의 용도로 활용하여서는 아니 된다.

오답 포인트

④의 앞부분이 법조문과 같다는 이유로 뒷부분까지 옳다고 판단하기 쉽다. 그러나 제3조 제2항은 목적에 맞는 처리를 요구하는 동시에 목적 외 활용을 금지한다.

다시 나오면 이렇게 판단

개인정보 보호 원칙에서는 처리 목적의 명확성, 필요 최소한의 수집, 목적 범위 내 적합한 처리,
정확성·완전성·최신성, 안전한 관리, 권리 보장, 사생활 침해 최소화, 익명·가명 처리, 책임 준수를 확인한다.
특히 목적 외 활용을 허용하는 표현은 제3조의 원칙과 반대이므로 틀린 선지로 판단한다.

암기 포인트

목적 안에서는 적합하게 처리하고, 목적 밖에서는 활용하지 않는다.

NoteBase

문 4. 다음 중 SSO(Single Sign On)에 대한 장점으로 가장 옳지 않은 것은?

① 자원별 권한관리 편리성 증가

② 다요소 인증(MFA) 적용으로 보안성 향상

③ 중앙집중 관리를 통한 효율적 관리 기능

④ 사용자 편의성 증가

정답 1번

출제 포인트

이 문제는 SSO가 통합하는 인증과 각 자원에서 별도로 통제하는 권한 관리를 구분하는 문제이다.

핵심 개념

SSO(Single Sign-On)는 한 번의 사용자 인증으로 서로 연계된 여러 시스템이나 서비스에 다시 로그인하지 않고 접근하게 하는 방식이다. SSO의 핵심은 인증 절차의 통합이며, 사용자가 각 자원에서 무엇을 할 수 있는지를 정하는 권한 부여까지 자동으로 통합하는 것은 아니다.

선지별 해설

① X — '자원별 권한관리 편리성 증가'는 SSO의 직접적인 장점이 아니다. SSO는 여러 서비스의 로그인 인증을 통합하지만, 자원별 접근 권한은 각 서비스의 권한 정책에 따라 별도로 관리해야 한다. 올바르게는 '여러 자원에 대한 인증 절차가 통합되어 반복 로그인이 줄어든다'라고 해야 한다.
② O — 인증을 중앙의 통합 지점에서 처리하면 그 지점에 MFA를 일관되게 적용할 수 있으므로, 연계된 서비스의 인증 보안성을 높일 수 있다.
③ O — 사용자 인증을 중앙에서 관리하므로 계정과 인증 정책을 서비스마다 따로 운영할 때보다 관리가 효율적이다.
④ O — 사용자는 한 번 로그인한 뒤 연계된 여러 서비스에 접근할 수 있어 반복적인 로그인과 비밀번호 입력이 줄어든다.

오답 포인트

①의 '권한관리'를 '인증관리'와 혼동하기 쉽다. SSO가 통합하는 것은 사용자가 누구인지 확인하는 인증이며, 각 자원에서 허용되는 행위를 정하는 권한 부여는 별도의 문제이다.

다시 나오면 이렇게 판단

한 번 로그인하여 여러 서비스에 접근하는 편의성과 중앙 인증 관리는 SSO의 장점으로 판단한다. 선지가 자원별 권한 설정까지 SSO가 직접 해결한다고 하면 인증과 권한 부여를 혼동한 표현으로 판단한다.

NoteBase

암기 포인트

SSO는 로그인 인증의 통합이지, 자원별 권한 부여의 자동 통합이 아니다.

NoteBase

문 5. 다음 <보기> 중 시스템 및 서비스 보안관리에 해당하는 것은 모두 몇 개인가?

<보기>
㉠ 보안시스템 운영 ㉡ 클라우드 보안
㉢ 공개서버 보안 ㉣ 정보보안 전송
㉤ 패치관리 ㉥ 업무용 단말기기 보안

① 3개
② 4개
③ 5개
④ 6개

정답 4번

출제 포인트

시스템 및 서비스 보안관리의 세부 인증기준에 포함되는 항목을 구별하고 그 개수를 세는 문제이다.

핵심 개념

시스템 및 서비스 보안관리는 정보시스템과 서비스의 운영 과정에서 침해 위험을 줄이기 위한 기술적·관리적 보호대책 분야이다. 보기의 보안시스템 운영, 클라우드 보안, 공개서버 보안, 정보전송 보안, 패치관리, 업무용 단말기기 보안은 모두 이 분야의 세부 항목이다. 따라서 ㉠부터 ㉥까지 6개가 모두 해당한다.

선지별 해설

① X — 해당 항목은 3개가 아니라 ㉠~㉥의 6개 전부이다. 틀린 표현은 '3개'이며, 올바르게는 '6개'이다.
② X — 보안시스템 운영·클라우드 보안·공개서버 보안뿐 아니라 정보전송 보안·패치관리·업무용 단말기기 보안도 포함된다. 틀린 표현은 '4개'이며, 올바르게는 '6개'이다.
③ X — 보기에서 제외할 항목이 없으므로 5개가 아니다. 틀린 표현은 '5개'이며, 올바르게는 '6개'이다.
④ O — ㉠ 보안시스템 운영, ㉡ 클라우드 보안, ㉢ 공개서버 보안, ㉣ 정보전송 보안, ㉤ 패치관리, ㉥ 업무용 단말기기 보안이 모두 해당하므로 총 6개이다.

오답 포인트

패치관리를 시스템 및 서비스 운영관리로 잘못 분류하여 하나를 제외하면 ③의 5개를 고르기 쉽다. 패치관리는 시스템 및 서비스 보안관리의 세부 항목이라는 점이 핵심 함정이다.

NoteBase

다시 나오면 이렇게 판단

각 항목이 시스템의 안전한 운용을 위한 일반 운영 절차인지, 침해 예방을 위한 직접적인 보안 통제인지 구분한다. 보안시스템·클라우드·공개서버·정보전송·단말기·보조저장매체·패치·악성코드와 전자거래 및 핀테크 보안은 시스템 및 서비스 보안관리로 묶는다.

암기 포인트

시스템 및 서비스 보안관리에는
‘보안시스템·클라우드·공개서버·전자거래·정보전송·단말기·보조저장매체·패치·악성코드’가 포함된다.

NoteBase

문 6. 다음에서 설명하는 버퍼 오버플로 공격 대응 기법으로 가장 옳은 것은?

◯ 함수를 호출할 때는 스택의 ret값을 global RET Stack이라는 별도의 스택에 저장
◯ 함수를 종료할 때는 global RET Stack에 저장된 ret값과 스택의 ret값을 비교하여 일치하지 않으면 프로그램을 종료

① Stack Guard
② ASLR(Address Space Layout Randomization)
③ Stack Shield
④ Non-Executable Stack

정답 3번

출제 포인트

함수의 반환 주소를 별도의 스택에 복사해 두었다가 함수 종료 시 원래 스택의 반환 주소와 비교하는 방어 기법을 구별하는 문제이다.

핵심 개념

Stack Shield는 함수 호출 시 반환 주소를 별도의 global RET Stack에 저장하고, 함수가 끝날 때 두 반환 주소가 같은지 검사하여 변조를 탐지하는 기법이다.
Stack Guard는 반환 주소 앞에 카나리 값을 두고 그 값의 훼손 여부로 스택 버퍼 오버플로를 탐지한다.
ASLR은 코드·스택·힙 등의 메모리 배치 주소를 무작위화한다.
Non-Executable Stack은 스택 영역의 코드 실행 권한을 제거한다.

선지별 해설

① X — Stack Guard의 핵심은 반환 주소를 별도 스택에 저장하는 것이 아니라 반환 주소 앞의 카나리 값이 변조되었는지 검사하는 것이다. 틀린 연결은 '별도의 global RET Stack에 저장하고 비교'이며, 올바르게는 '카나리 값을 삽입하고 그 무결성을 검사'하는 기법이다.
② X — ASLR은 메모리상의 코드·스택·힙 등의 주소를 무작위화하여 공격자가 목표 주소를 예측하기 어렵게 한다. 틀린 연결은 '반환 주소를 별도 스택에 저장하고 비교'이며, 올바르게는 '주소 공간의 배치를 무작위화'하는 기법이다.
③ O — Stack Shield는 스택의 반환 주소를 별도의 global RET Stack에 보관한 뒤 함수 종료 시 두 값을 비교한다. 두 값이 다르면 반환 주소가 변조된 것으로 보고 프로그램을 종료하므로 지문의 설명과 일치한다.
④ X — Non-Executable Stack은 스택을 실행 불가능한 영역으로 설정하여 스택에 삽입된 공격 코드의 실행을 막는다. 틀린 연결은 '반환 주소를 별도 스택에 저장하고 비교'이며, 올바르게는 '스택 영역의 실행 권한을 제거'하는 기법이다.

NoteBase

오답 포인트

Stack Guard와 Stack Shield는 모두 반환 주소 변조 공격을 막는다는 점 때문에 혼동하기 쉽다. 이 문제의 결정적 표현은 '별도의 global RET Stack'과 '두 ret값 비교'이며, 이는 카나리를 검사하는 Stack Guard가 아니라 Stack Shield를 가리킨다.

다시 나오면 이렇게 판단

별도 반환 주소 스택과 값 비교는 Stack Shield, 카나리 값 검사는 Stack Guard, 주소 무작위화는 ASLR, 스택 실행 금지는 Non-Executable Stack으로 구분한다.

암기 포인트

Shield는 반환 주소를 따로 보관해 비교하고, Guard는 카나리로 지킨다.

NoteBase

문 7. 다음 내용에서 설명하는 것은?

◯메일로 전파되며, 감염된 시스템이 많으면 SMTP 서버의 네트워크 트래픽이 증가한다.
◯출처나 내용이 확인되지 않은 메일을 열었을 때 확산되는 경우가 많다.

① 슬래머 웜(Slammer Worm)
② 모리스 웜(Morris Worm)
③ 매스메일러 웜(Mass Mailer Worm)
④ 블래스터 웜(Blaster Worm)

정답 3번

출제 포인트

전자우편을 통해 대량 전파되고 SMTP 서버의 트래픽을 증가시키는 웜의 유형을 식별하는 문제이다.

핵심 개념

매스메일러 웜은 감염된 시스템의 주소록이나 전자우편 기능을 이용해 자신을 다수의 수신자에게 발송하며 확산하는 웜이다. 핵심 단서는 메일 전파, 출처가 불분명한 메일 또는 첨부파일의 실행, SMTP 트래픽 증가이다. 슬래머 웜은 Microsoft SQL Server의 취약점을 이용해 UDP 네트워크로 급속히 확산한다. 모리스 웜은 유닉스 계열 시스템의 여러 취약점과 취약한 계정 정보를 이용한 초기의 인터넷 웜이다. 블래스터 웜은 Windows의 DCOM RPC 취약점을 이용해 네트워크로 확산한다.

NoteBase

선지별 해설

① X
슬래머 웜은 메일을 열 때 확산되는 매스메일러형이 아니라 Microsoft SQL Server의 취약점을 이용하여 UDP로 전파되는 웜이다. 틀린 연결은 '메일 전파·SMTP 트래픽 증가 → 슬래머 웜'이며, 올바르게는 'SQL Server 취약점·UDP 기반 급속 확산 → 슬래머 웜'이다.

② X
모리스 웜은 메일 첨부파일을 대량 발송하는 유형이 아니라 유닉스 시스템의 sendmail, fingerd 등의 취약점과 취약한 계정 정보를 이용해 확산한 웜이다. 틀린 연결은 '출처 불명 메일을 열면 확산 → 모리스 웜'이며, 올바르게는 '유닉스 서비스 취약점 등을 이용한 확산 → 모리스 웜'이다.

③ O
매스메일러 웜은 전자우편을 이용해 대량으로 자신을 발송하므로 감염 시스템이 많아지면 SMTP 서버와 네트워크의 트래픽이 증가한다. 출처나 내용이 확인되지 않은 메일 또는 첨부파일을 열 때 감염·확산되기 쉽다는 설명과 일치한다.

④ X
블래스터 웜은 전자우편을 통한 대량 발송형이 아니라 Windows의 DCOM RPC 취약점을 이용해 네트워크로 전파되는 웜이다. 틀린 연결은 '메일 전파·SMTP 트래픽 증가 → 블래스터 웜'이며, 올바르게는 'Windows DCOM RPC 취약점 이용 → 블래스터 웜'이다.

오답 포인트

웜은 공통적으로 자기 복제와 네트워크 확산이 가능하므로 이름만 보면 혼동하기 쉽다. 이 문항에서는 '메일'과 'SMTP'가 결정적 단서이며, 서버 취약점을 직접 이용하는 슬래머·모리스·블래스터와 구분해야 한다.

다시 나오면 이렇게 판단

전파 매체를 먼저 확인한다. 메일·주소록·첨부파일·SMTP가 함께 제시되면 매스메일러 웜, SQL Server와 UDP가 제시되면 슬래머 웜, 유닉스의 sendmail·fingerd 등이 제시되면 모리스 웜, Windows의 DCOM RPC가 제시되면 블래스터 웜으로 판단한다.

암기 포인트

메일·SMTP는 매스메일러, SQL·UDP는 슬래머, 유닉스 취약점은 모리스, Windows RPC는 블래스터이다.

NoteBase

문 8. 다음 중 공개키에 기반하지 않는 암호화 방식은?

① RSA 암호화

② Rabin방식 암호화

③ AES 암호화

④ ECC 암호화

정답 3번

출제 포인트

공개키 암호 방식과 대칭키 암호 방식의 차이를 구별하는 문제이다.

핵심 개념

공개키 암호 방식은 공개키와 개인키라는 서로 다른 키를 사용하는 비대칭키 방식이다. RSA, Rabin, ECC가 여기에 속한다.
대칭키 암호 방식은 암호화와 복호화에 동일한 비밀키를 사용하는 방식이다. AES가 여기에 속한다.

선지별 해설

① X
RSA 암호화는 공개키와 개인키를 사용하는 대표적인 공개키 암호 방식이다. 따라서 '공개키에 기반하지 않는다'는 조건에 해당하지 않는다. 올바르게는 'RSA는 공개키에 기반한 비대칭키 암호 방식이다'이다.

② X
Rabin 방식 암호화는 공개키와 개인키를 구분하여 사용하는 공개키 암호 방식이다. 따라서 '공개키에 기반하지 않는다'는 조건에 해당하지 않는다. 올바르게는 'Rabin 방식은 공개키에 기반한 비대칭키 암호 방식이다'이다.

③ O
AES 암호화는 하나의 비밀키를 송신자와 수신자가 공유하는 대칭키 블록 암호 방식이므로 공개키에 기반하지 않는다.

④ X
ECC 암호화는 타원곡선의 수학적 성질을 이용하는 공개키 암호 방식이다. 따라서 '공개키에 기반하지 않는다'는 조건에 해당하지 않는다. 올바르게는 'ECC는 공개키에 기반한 비대칭키 암호 방식이다'이다.

NoteBase

오답 포인트

③의 AES도 키를 사용하는 암호이므로 공개키 암호로 혼동하기 쉽다. 그러나 구분 기준은 키의 존재 여부가 아니라 암호화와 복호화에 동일한 공유 비밀키를 쓰는지, 공개키와 개인키의 쌍을 쓰는지이다.

다시 나오면 이렇게 판단

알고리즘을 대칭키와 공개키로 먼저 분류한다. AES는 대칭키이고, RSA·Rabin·ECC는 공개키 방식이므로 '공개키에 기반하지 않는 것'을 묻는 경우 AES를 선택한다.

암기 포인트

AES는 대칭키, RSA·Rabin·ECC는 공개키 방식이다.

NoteBase

문 9. 다음 중 BIOS에 대한 설명으로 가장 옳지 않은 것은?

① 하드웨어와 소프트웨어 사이에서 입출력을 중계하는 펌웨어다.

② 운영체제와 하드웨어 사이의 입출력을 담당하는 펌웨어다.

③ BIOS에 저장된 시스템 시간은 포렌식 관점에서 중요하다.

④ 전원이 공급되지 않으면 정보가 유지되지 않는다.

정답 4번

출제 포인트

BIOS의 입출력 중계 기능과 비휘발성, 그리고 BIOS 설정 정보와 시스템 시각을 유지하는 CMOS·RTC의 역할을 구분하는 문제이다.

핵심 개념

BIOS는 컴퓨터가 켜질 때 하드웨어를 초기화하고 운영체제의 부팅을 시작하며, 기본적인 입출력 서비스를 제공하는 펌웨어이다. BIOS 펌웨어는 ROM이나 플래시 메모리 같은 비휘발성 메모리에 저장되므로 주 전원이 끊겨도 코드가 사라지지 않는다. 시스템 시각과 BIOS 설정값은 보통 CMOS·RTC 회로와 보조 배터리에 의해 유지된다.

선지별 해설

① O — BIOS는 하드웨어를 제어하는 기본 입출력 서비스를 제공하므로 하드웨어와 소프트웨어 사이에서 입출력을 중계하는 펌웨어라고 볼 수 있다.
② O — 운영체제가 하드웨어를 사용할 수 있도록 기본적인 입출력 인터페이스를 제공하는 펌웨어라는 설명이다. 현대 운영체제는 부팅 뒤 장치 드라이버를 주로 사용하지만, BIOS의 기본 기능에 관한 설명으로는 타당하다.
③ O — BIOS 설정 화면에서 확인·설정하는 시스템 시각은 파일 시간 정보 등 디지털 증거의 시각을 해석하는 기준이 되므로 포렌식에서 중요하다. 실제 시각은 일반적으로 CMOS·RTC 영역에서 관리된다.
④ X — 틀린 표현은 '전원이 공급되지 않으면 정보가 유지되지 않는다'이다. BIOS 펌웨어는 비휘발성 메모리에 저장되므로 전원이 없어도 유지된다. 시스템 시각과 설정값도 주 전원이 꺼진 동안 보조 배터리로 유지되며, 그 배터리까지 방전되면 시각이나 일부 설정값이 초기화될 수 있다.

오답 포인트

④는 BIOS를 RAM과 같은 휘발성 메모리로 오인하게 만드는 선지이다. BIOS 펌웨어 자체의 저장과 CMOS·RTC 설정 정보의 배터리 유지를 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

BIOS의 기본 입출력·부팅 기능을 묻는 표현은 옳게 판단하고, 전원 차단 시 소멸 여부는 저장 매체를 확인한다.
ROM·플래시의 BIOS 코드는 비휘발성이며, 시각·설정값은 CMOS·RTC와 보조 배터리가 유지한다.

암기 포인트

BIOS 코드는 비휘발성, 시스템 시각·설정은 CMOS·RTC와 배터리이다.

NoteBase

문 10. SID(Security Identifier)는 윈도우의 각 사용자 또는 그룹을 고유하게 식별하는데 사용하는 식별번호이다. 다음 중 SID에 포함될 구성요소로 가장 옳지 않은 것은?

① 식별자 기관 값(Identifier Authority Value)

② 수정 수준(Revision Level)

③ 도메인 식별자(Domain Identifier)

④ 레지스트리 키(Registry Key)

정답 4번

출제 포인트

윈도우 SID를 이루는 필드와 SID 외부에서 사용되는 개념을 구별하는 문제이다.

핵심 개념

SID(Security Identifier)는 윈도우가 사용자·그룹 등 보안 주체를 고유하게 식별하는 값이다. 기본적으로 수정 수준, 식별자 기관 값, 하나 이상의 하위 기관 값으로 구성되며, 도메인 계정 SID에서는 하위 기관 값의 일부가 도메인 식별자를 이룬다. 마지막 하위 기관 값은 보통 해당 계정을 구별하는 RID(Relative Identifier)이다. 레지스트리 키는 윈도우 레지스트리의 데이터 저장 단위일 뿐 SID의 구성 필드가 아니다.

선지별 해설

① O — 식별자 기관 값(Identifier Authority Value)은 SID를 발급한 기관이나 권한 체계를 나타내는 기본 구성요소이다.
② O — 수정 수준(Revision Level)은 SID 형식의 버전을 나타내는 기본 구성요소이다.
③ O — 도메인 식별자(Domain Identifier)는 도메인 계정 SID에서 여러 하위 기관 값으로 표현되며, 같은 도메인에 속한 계정들이 공유하는 부분이다.
④ X — 레지스트리 키(Registry Key)는 SID의 구성요소가 아니다. 틀린 표현은 '레지스트리 키'이며, 올바르게는 SID가 수정 수준, 식별자 기관 값 및 하위 기관 값들로 구성된다고 해야 한다.

오답 포인트

SID가 레지스트리의 보안 설정이나 계정 정보와 함께 나타날 수 있다는 사실 때문에 ④의 레지스트리 키를 SID 내부 필드로 오인하기 쉽다. 저장되는 위치나 연관된 관리 수단과 식별자 자체의 구성요소는 구별해야 한다.

다시 나오면 이렇게 판단

SID 표기 구조를 '수정 수준 → 식별자 기관 값 → 하위 기관 값들'로 나누어 판단한다. 도메인 식별자와 RID는 하위 기관 값 영역에 들어가지만, 레지스트리 키는 SID를 저장하거나 참조할 수 있는 외부 저장 구조이므로 제외한다.

NoteBase

암기 포인트

SID는 수정 수준·식별자 기관·하위 기관 값으로 구성되며, 레지스트리 키는 SID 구성요소가 아니다.

NoteBase

문 11. 「국가 사이버보안 기본지침」 제76조(비밀번호 관리)에는 비밀번호 관리와 관련된 사항이 규정되어 있다. 이와 관련하여 다음 중 가장 옳지 않은 것은?

① 사용된 비밀번호는 재사용하지 않는다.

② 비밀번호는 최소한 6자리 이상 문자(대/소문자, 숫자조합)로 구성된다.

③ 동일한 비밀번호를 여러 사람이 공유하여 사용하지 않는다.

④ 일반 사전에 등록된 단어의 사용을 피한다.

정답 2번

쟁점

이 문제는 「국가 사이버보안 기본지침」상 비밀번호의 생성·사용 원칙에 관한 문제이다. 핵심은 비밀번호의 최소 길이와 문자 조합 요건을 정확히 구별하는 것이다.

용어 풀이

비밀번호 복잡성은 비밀번호의 길이를 충분히 확보하고 서로 다른 종류의 문자를 섞어 추측과 무차별 대입을 어렵게 하는 기준이다.

핵심 구분

비밀번호는 숫자·문자·특수문자 등을 혼합하여 9자리 이상으로 안전하게 설정하고 정기적으로 변경·사용한다. 또한 이미 사용한 비밀번호의 재사용, 여러 사람의 동일 비밀번호 공유, 일반 사전에 등록된 단어의 사용을 피한다.

NoteBase

선지별 해설

① O
이미 사용한 비밀번호를 재사용하지 않는 것은 과거 비밀번호가 노출되었을 때 계정이 다시 침해되는 것을 막는 관리 원칙이다.

② X
비밀번호를 최소 6자리로 구성한다는 부분이 틀렸다. 길이가 짧을 뿐 아니라 특수문자 조합 요건도 빠져 있다.
틀린 표현: 최소한 6자리 이상 문자(대/소문자, 숫자조합)로 구성된다.
올바른 표현: 숫자·문자·특수문자 등을 혼합하여 9자리 이상으로 구성한다.

③ O
동일한 비밀번호를 여러 사람이 공유하면 사용자별 책임 추적이 어려워지고 한 사람에게서 유출된 비밀번호로 여러 계정이 침해될 수 있으므로 공유하지 않는다.

④ O
일반 사전에 등록된 단어는 사전 대입 공격으로 쉽게 추측될 수 있으므로 비밀번호에 사용하는 것을 피한다.

오답 포인트

②의 '6자리'와 '대문자·소문자·숫자 조합'만 보고 복잡성 기준을 충족한다고 판단하기 쉽다. 이 지침의 기준은 9자리 이상이며 특수문자도 조합 대상에 포함된다는 점이 함정이다.

다시 나오면 이렇게 판단

비밀번호 관리 선지는 길이, 문자 종류, 재사용 금지, 공유 금지, 사전 단어 회피를 차례로 확인한다. 최소 길이가 9자리보다 짧거나 문자·숫자·특수문자의 혼합 요건을 빠뜨린 선지는 틀린 것으로 판단한다.

암기 포인트

9자리 이상·숫자·문자·특수문자 혼합, 재사용·공유·사전 단어는 금지이다.

NoteBase

문 12. 다음 중 시스템 분석도구에 대한 명칭과 기능이 짝지어진 것으로 가장 옳지 않은 것은?

① chklastlog - 운영체제별 로그 변조 탐지 도구

② tripwire - 시스템 로그의 주기적 스캔 및 행위 분석 로깅 도구

③ satan - IP네트워크에 연결된 시스템의 취약점 진단 도구

④ syslogd - 시스템 로그 관리 도구

정답 2번

출제 포인트

시스템 분석·보안 도구의 명칭과 핵심 기능을 정확히 연결하는 문제이다.

핵심 개념

chklastlog는 로그인 기록의 삭제·변조 흔적을 점검하는 도구이다.
tripwire는 기준 시점의 파일·디렉터리 정보와 현재 상태를 비교하여 무결성 훼손을 탐지하는 도구이다.
SATAN은 네트워크에 연결된 시스템의 보안 취약점을 원격으로 점검하는 도구이다.
syslogd는 시스템에서 발생한 로그 메시지를 수집하고 정해진 대상에 기록·전달하는 로그 관리 데몬이다.

선지별 해설

① O — chklastlog는 로그인 관련 로그를 대조하여 삭제되거나 변조된 로그인 기록의 흔적을 탐지하므로 로그 변조 탐지 도구라는 설명이 타당하다.
② X — 틀린 부분은 tripwire를 '시스템 로그의 주기적 스캔 및 행위 분석 로깅 도구'라고 한 표현이다. tripwire는 시스템 로그의 행위를 분석하는 도구가 아니라 파일과 디렉터리의 무결성을 검사하는 도구이다. 기준 데이터베이스와 현재 파일 상태를 비교하여 변경 여부를 탐지한다.
③ O — SATAN은 IP 네트워크상의 호스트와 서비스를 조사하여 알려진 보안 취약점을 진단하는 도구이므로 연결이 옳다.
④ O — syslogd는 여러 프로그램과 커널 등이 보내는 시스템 로그 메시지를 수집하여 파일 등에 기록하거나 다른 로그 호스트로 전달하는 시스템 로그 관리 도구이다.

오답 포인트

②의 '주기적 스캔'이라는 말 때문에 tripwire가 로그 분석 도구처럼 보일 수 있다. 그러나 tripwire가 주기적으로 비교하는 대상은 행위 로그가 아니라 파일·디렉터리의 무결성 정보이다.

다시 나오면 이렇게 판단

도구가 검사하는 대상을 먼저 구분한다. 로그인 기록은 chklastlog, 파일 무결성은 tripwire, 네트워크 취약점은 SATAN, 로그 수집·기록은 syslogd에 대응한다.

NoteBase

암기 포인트

chklastlog는 로그인 로그, tripwire는 파일 무결성, SATAN은 네트워크 취약점, syslogd는 로그 관리이다.

NoteBase

문 13. 다음 중 SSL(Secure Socket Layer)에 대한 설명으로 가장 옳지 않은 것은?

① 공개키 알고리즘(X.509 인증서)을 사용한다.

② 전송계층과 응용계층 사이에서 동작하고, TCP 443 포트를 사용한다.

③ 데이터 전송시마다 매번 신원인증과 암호화를 수행한다.

④ 비밀성, 무결성, 인증을 보안기능으로 제공한다.

정답 3번

출제 포인트

SSL의 인증서 사용, 동작 계층, 기본 포트와 세션 수립 후 데이터 보호 방식을 구분하는 문제이다.

핵심 개념

SSL은 응용 프로그램과 TCP 사이에서 통신 상대 인증과 암호 매개변수 협상을 수행한 뒤 전송 데이터를 보호하는 보안 프로토콜이다. 핸드셰이크 단계에서는 X.509 인증서와 공개키 암호 기술 등을 이용해 신원을 확인하고 키를 협상하며, 이후 레코드 전송에서는 협상된 세션 키를 이용해 데이터를 암호화하고 무결성을 검증한다.

선지별 해설

① O — SSL 핸드셰이크에서는 공개키 암호 기술과 공개키를 신원에 결합한 X.509 인증서를 이용하여 서버 등의 신원을 인증하고 세션에 필요한 키를 협상한다.
② O — SSL은 응용계층 프로토콜과 TCP 사이에서 동작한다. SSL을 적용한 HTTPS의 기본 TCP 포트는 443이다.
③ X — 틀린 표현은 '데이터 전송시마다 매번 신원인증과 암호화를 수행한다'이다. 신원인증과 키 협상은 주로 세션을 수립하는 핸드셰이크 단계에서 수행하며, 세션 수립 뒤의 각 데이터 레코드는 이미 협상된 세션 키로 암호화와 무결성 보호를 수행한다.
④ O — SSL은 통신 내용의 비밀성, 변조 여부를 확인하는 무결성, 인증서를 통한 통신 상대 인증 기능을 제공한다.

오답 포인트

③은 '데이터가 전송될 때마다 보호된다'는 사실을 '매번 신원인증까지 다시 한다'로 바꾼 선지이다. 데이터 레코드마다 암호화·무결성 보호가 적용되는 것과 세션 수립 시의 신원인증을 구분해야 한다.

다시 나오면 이렇게 판단

SSL의 동작을 '핸드셰이크: 인증과 키 협상'과 '레코드 전송: 협상된 키를 이용한 암호화와 무결성 보호'로 나누어 판단한다. '매 전송마다 신원인증'이라는 표현은 틀린 것으로 본다.

NoteBase

암기 포인트

SSL은 처음에 인증·키 협상, 이후에는 세션 키로 암호화·무결성 보호를 수행한다.

NoteBase

문 14. 다음은 「정보통신기반보호법」 제6조(주요정보통신기반시설보호계획의 수립 등)의 주요내용 중 일부이다. <보기>의 빈칸에 들어갈 내용으로 가장 옳은 것은?

<보기>
주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다.
1. 주요정보통신기반시설의 ( ) 분석·평가에 관한 사항
2. 주요정보통신기반시설 및 관리 정보의 ( )에 대한 예방, 백업, 복구 대책에 관한 사항
3. 그 밖에 주요정보통신기반시설의 ( )에 관하여 필요한 사항

① 시스템－보안사고－개선
② 시스템－침해사고－개선
③ 취약점－보안사고－보호
④ 취약점－침해사고－보호

정답 4번

쟁점

이 문제는 「정보통신기반 보호법」상 주요정보통신기반시설보호계획에 반드시 포함되는 사항을 묻는 문제이다. 핵심은 취약점의 분석·평가, 침해사고에 대한 대책, 시설의 보호라는 조문 용어를 정확히 연결하는 것이다.

용어 풀이

취약점 분석·평가는 주요정보통신기반시설에서 침해사고로 이어질 수 있는 약점을 찾아 그 위험을 평가하는 것이다. 침해사고는 정보통신기반시설이나 관리 정보가 공격·침입 등으로 침해되는 사고를 뜻한다.

핵심 구분

「정보통신기반 보호법」 제6조 제3항은 보호계획의 포함 사항을 ① 주요정보통신기반시설의 취약점 분석·평가, ② 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방·백업·복구 대책, ③ 그 밖에 주요정보통신기반시설의 보호에 필요한 사항으로 규정한다. 따라서 빈칸은 차례로 '취약점－침해사고－보호'이다.

NoteBase

선지별 해설

① X
첫째 빈칸의 ‘시스템’은 법문상 ‘취약점’이어야 하고, 둘째 빈칸의 ‘보안사고’는 ‘침해사고’이어야 하며, 셋째 빈칸의 ‘개선’은 ‘보호’이어야 한다.
틀린 표현: 시스템－보안사고－개선
올바른 표현: 취약점－침해사고－보호

② X
둘째 빈칸의 ‘침해사고’만 맞고, 첫째와 셋째 빈칸이 법문과 다르다.
틀린 표현: 시스템, 개선
올바른 표현: 취약점, 보호

③ X
첫째 빈칸의 ‘취약점’과 셋째 빈칸의 ‘보호’는 맞지만, 예방·백업·복구 대책의 대상은 ‘보안사고’가 아니라 ‘침해사고’이다.
틀린 표현: 보안사고
올바른 표현: 침해사고

④ O
‘취약점 분석·평가’, ‘침해사고에 대한 예방·백업·복구 대책’, ‘주요정보통신기반시설의 보호’는 모두 제6조 제3항의 문언과 일치한다.

오답 포인트

‘시스템’과 ‘보안사고’처럼 의미가 자연스러운 일반 용어를 법문의 정확한 표현으로 착각하기 쉽다. 이 문항은 문맥상 비슷한 말이 아니라 ‘취약점－침해사고－보호’라는 조문 문구를 구별하는 문제이다.

다시 나오면 이렇게 판단

보호계획의 세 항목을 약점 진단, 사고 대응, 포괄적 보호의 순서로 대응시킨다. 약점 진단은 ‘취약점 분석·평가’, 사고 대응은 ‘침해사고의 예방·백업·복구’, 마지막 포괄 항목은 ‘보호’로 판단한다.

암기 포인트

취약점을 분석하고, 침해사고에 대비하며, 기반시설을 보호한다: 취약점－침해사고－보호.

NoteBase

문 15. 다음 <보기>의 정보자산 위험처리(Risk Treatment) 활동과 그 방법이 가장 옳게 연결된 것은?

<보기>
㉠ 데이터 백업 절차를 수립하고, 방화벽 도입으로 기술적 보안통제를 적용한다.
㉡ 외부 전문기관과 보험계약을 체결하고, 위험으로 인한 손실과 책임을 분담한다.

① ㉠: 위험회피, ㉡: 위험완화
② ㉠: 위험완화, ㉡: 위험전가
③ ㉠: 위험수용, ㉡: 위험전가
④ ㉠: 위험전가, ㉡: 위험완화

정답 2번

출제 포인트

정보자산 위험처리 방법 중 위험완화와 위험전가를 활동의 내용으로 구별하는 문제이다.

핵심 개념

위험회피: 위험을 발생시키는 활동 자체를 중단하거나 제거하는 방법이다.
위험완화: 보안통제를 적용하여 위험의 발생 가능성이나 피해 규모를 낮추는 방법이다. 데이터 백업 절차와 방화벽 도입이 이에 해당한다.
위험전가: 보험이나 계약 등을 통해 위험에 따른 손실 또는 책임의 전부나 일부를 외부와 분담하는 방법이다.
위험수용: 위험 수준을 받아들이고 별도의 추가 통제 없이 감수하는 방법이다.

선지별 해설

① X — ㉠을 '위험회피', ㉡을 '위험완화'로 연결한 부분이 모두 틀렸다. 실제로 ㉠은 통제로 위험을 낮추는 위험완화이고, ㉡은 보험계약으로 손실과 책임을 분담하는 위험전가이다.
② O — ㉠의 백업 절차와 방화벽은 위험의 가능성이나 영향을 낮추므로 위험완화이고, ㉡의 외부 전문기관 및 보험계약은 손실과 책임을 외부와 분담하므로 위험전가이다.
③ X — ㉡의 위험전가는 맞지만, ㉠을 '위험수용'으로 연결한 부분이 틀렸다. ㉠은 별도 조치 없이 위험을 감수하는 것이 아니라 보안통제를 적용하므로 위험완화이다.
④ X — ㉠을 '위험전가', ㉡을 '위험완화'로 연결하여 두 개념을 서로 바꾼 것이 틀렸다. 올바르게는 ㉠이 위험완화이고 ㉡이 위험전가이다.

NoteBase

오답 포인트

‘백업’이 손실 이후의 대응처럼 보여 위험수용으로 오해하거나, 외부 기관이 보안조치를 수행한다는 이유만으로 위험완화라고 판단하기 쉽다. 그러나 ㉠은 통제의 적용으로 위험을 낮추는 활동이고, ㉡은 보험계약을 통해 손실과 책임의 부담 주체를 나누는 활동이다.

다시 나오면 이렇게 판단

활동을 없애면 회피, 통제를 추가해 가능성·영향을 낮추면 완화, 보험·계약으로 부담을 외부와 나누면 전가, 추가 조치 없이 감수하면 수용으로 판단한다.

암기 포인트

중단은 회피, 통제는 완화, 보험은 전가, 감수는 수용이다.

NoteBase

문 16. 악성코드(Malware)는 악의적인 목적을 가지고 시스템의 기밀성, 가용성, 무결성 등의 가치를 침해하는 프로그램으로 호스트에 의존 또는 독립적으로 작동된다. 다음 악성코드 중 호스트 작동유형이 다른 하나는?

① 트로이 목마(Trojan Horse)

② 바이러스(Virus)

③ 웜(Worm)

④ 논리 폭탄(Logical Bomb)

정답 3번

출제 포인트

악성코드를 호스트 프로그램에 의존하여 작동하는 유형과 스스로 실행·전파할 수 있는 독립형으로 구분하는 문제이다.

핵심 개념

호스트 의존형 악성코드는 다른 프로그램이나 코드에 포함되거나 결합되어 실행된다. 반면 웜은 독립적으로 실행되며 네트워크를 통해 자기 자신을 복제·전파한다. 이 분류에서는 트로이 목마, 바이러스, 논리 폭탄은 호스트 의존형이고 웜은 독립형이다.

선지별 해설

① X — 트로이 목마는 정상적이거나 유용한 기능을 가장한 프로그램에 악의적 기능을 숨겨 사용자가 실행하게 하는 호스트 의존형으로 분류된다. 독립형이 아니라 호스트 의존형이다.
② X — 바이러스는 실행 파일이나 문서 매크로 같은 숙주에 자신의 코드를 삽입하고 숙주가 실행될 때 증식하므로 호스트 의존형이다. 독립형이 아니라 호스트 의존형이다.
③ O — 웜은 별도의 숙주 프로그램에 붙지 않고 스스로 실행되며, 네트워크의 다른 시스템으로 자기 자신을 복제·전파하는 독립형 악성코드이다.
④ X — 논리 폭탄은 프로그램 내부에 숨겨져 있다가 특정 날짜나 조건이 충족되면 악성 동작을 수행하므로 호스트 의존형이다. 독립형이 아니라 호스트 의존형이다.

오답 포인트

트로이 목마도 하나의 실행 파일처럼 보일 수 있어 웜과 같은 독립형으로 오인하기 쉽다. 이 문항의 분류 기준은 파일의 겉모양이 아니라 다른 프로그램에 악성 기능을 숨기거나 결합해 작동하는지, 또는 스스로 복제·전파하는지이다.

NoteBase

다시 나오면 이렇게 판단

숙주 코드에 삽입되거나 프로그램 속에 숨겨져 작동하면 호스트 의존형으로, 숙주 없이 스스로 실행되고 네트워크로 자기 복제하면 독립형으로 판단한다.

암기 포인트

바이러스는 숙주에 붙고, 논리 폭탄은 조건을 기다리며, 웜은 혼자 퍼진다.

NoteBase

문 17. 시스템 보안위협 중 하나인 루트킷(Rootkit)은 시스템에 설치되어 있으면서 존재의 흔적을 최대한 숨기고 지속적으로 시스템에 위해를 가하는 프로그램이다. 이의 핵심 기능으로 보기 가장 어려운 것은?

① 프로세스/스레드 감추기

② 레지스트리/서비스 감추기

③ 파일 암호화

④ 스니핑 및 시스템 제어

정답 3번

출제 포인트

루트킷의 핵심 기능인 은닉·지속성 유지·시스템 제어와 파일 암호화 기능을 구별하는 문제이다.

핵심 개념

루트킷은 공격자가 침해한 시스템에서 높은 권한과 접근을 유지하면서 악성 행위와 자신의 존재를 숨기도록 만든 도구 또는 프로그램의 집합이다. 핵심 키워드는 은닉, 지속성, 권한 유지, 원격 제어이다. 반면 파일 암호화는 주로 데이터를 사용할 수 없게 만들어 금전을 요구하는 랜섬웨어의 대표 기능이다.

선지별 해설

① O — 프로세스와 스레드를 감추면 실행 중인 악성 코드가 일반적인 시스템 조회 도구에 드러나지 않게 할 수 있으므로 루트킷의 대표적인 은닉 기능이다.
② O — 레지스트리 항목과 서비스를 감추면 악성 코드의 자동 실행 설정과 지속적으로 동작하는 구성요소의 흔적을 숨길 수 있으므로 루트킷의 핵심 기능에 해당한다.
③ X — 틀린 표현은 '파일 암호화'이다. 파일 내용을 암호화하여 사용하지 못하게 만드는 것은 랜섬웨어의 대표적인 기능이며, 루트킷의 핵심은 파일 암호화가 아니라 파일·디렉터리나 악성 구성요소를 감추는 은닉이다.
④ O — 네트워크 트래픽을 스니핑하여 정보를 수집하고 공격자가 시스템을 계속 제어할 수 있게 하는 것은 침해 후 접근과 통제 권한을 유지하려는 루트킷의 기능에 부합한다.

오답 포인트

③의 '파일 암호화'를 '파일 감추기'와 혼동하기 쉽다. 루트킷은 흔적을 보이지 않게 하는 은닉에 초점이 있고, 랜섬웨어는 파일 내용을 사용할 수 없게 하는 암호화에 초점이 있다.

다시 나오면 이렇게 판단

선지가 프로세스·서비스·레지스트리·파일 등의 존재를 숨기거나 공격자의 접근과 제어를 유지하는 기능이면 루트킷과 연결한다. 데이터를 암호화하여 이용을 막고 대가를 요구하는 기능이면 랜섬웨어와 연결한다.

NoteBase

암기 포인트

루트킷은 숨기고 지배하며, 랜섬웨어는 암호화하고 요구한다.

NoteBase

문 18. APT(Advanced Persistent Threat) 공격을 완성하기 위한 시나리오 구성시, 다음 중 특정 대상을 목표로 하는 활동으로 보기 가장 어려운 것은?

① 사회공학(Social Engineering)공격

② 스피어피싱(Spear Phishing)

③ 제로데이(Zero-day)공격

④ 역공학(Reverse Engineering)

정답 4번

출제 포인트

APT 공격 시나리오에서 특정 조직이나 개인을 겨냥하는 공격 활동과, 악성코드·프로그램의 구조를 분석하는 기술을 구별하는 문제이다.

핵심 개념

APT는 특정 목표에 장기간 잠복하며 단계적으로 침투하는 지능형 지속 공격이다. 사회공학과 스피어피싱은 표적의 사람·관계·업무 정보를 이용할 수 있고, 제로데이 공격은 표적 환경의 미공개 취약점을 침투에 활용할 수 있다. 반면 역공학은 프로그램의 동작과 구조를 분석하는 기법으로, 그 자체가 특정 대상을 겨냥하는 공격 활동을 뜻하지 않는다.

NoteBase

선지별 해설

① X
사회공학 공격은 표적 조직의 구성원, 업무 관계, 심리적 약점 등을 이용하여 정보 제공이나 악성 행위를 유도할 수 있으므로 특정 대상을 목표로 하는 활동이 될 수 있다. '특정 대상을 목표로 보기 어렵다'가 아니라, 표적 정보를 활용해 맞춤형으로 수행될 수 있는 공격이다.

② X
스피어피싱은 불특정 다수에게 보내는 일반 피싱과 달리 특정 개인이나 조직을 정하여 메시지를 정교하게 꾸미는 표적형 피싱이다. 따라서 특정 대상을 목표로 보기 어려운 활동이 아니라 대표적인 표적 공격 활동이다.

③ X
제로데이 공격은 보안 패치가 마련되기 전의 알려지지 않은 취약점을 악용하는 공격이다. APT에서는 표적이 사용하는 운영체제나 응용 프로그램의 취약점을 골라 침투할 수 있으므로 특정 대상을 겨냥한 시나리오에 포함될 수 있다. '특정 대상을 목표로 보기 어렵다'가 아니라, 표적 환경에 맞추어 활용될 수 있는 공격 수단이다.

④ O
역공학은 완성된 프로그램이나 악성코드를 분석하여 내부 구조와 동작 원리를 파악하는 기술이다. 공격 준비에 이용될 가능성은 있지만, 개념 자체는 특정 개인이나 조직을 직접 겨냥하는 공격 활동이 아니므로 네 항목 중 특정 대상 지향성이 가장 약하다.

오답 포인트

③의 제로데이는 '취약점이 불특정하다'는 뜻이 아니다. 공개되지 않았거나 패치가 없는 취약점이라는 뜻이므로 표적 시스템에 맞추어 사용할 수 있다. ④도 공격에 활용될 수 있다는 이유만으로 표적 공격 자체와 동일시하면 안 된다.

다시 나오면 이렇게 판단

각 용어가 누구를 겨냥하는 공격 방식인지, 아니면 프로그램을 분석하는 기술인지 구분한다. 표적의 사람·메시지·시스템에 직접 적용하는 수단은 표적 활동으로 보고, 대상 프로그램의 구조를 알아내는 분석 기법은 별도로 판단한다.

암기 포인트

스피어피싱은 표적형 공격이고, 역공학은 구조·동작 분석 기법이다.

NoteBase

문 19. 다음 중 블록체인의 기반기술과 특징에 대한 설명으로 가장 옳은 것은?

① 블록체인은 노드들이 동일한 거래 내역을 분산으로 저장하며, 생성된 거래는 당사자 간 유니캐스트(Unicast)로 전송

② 블록체인은 블록암호화 방식을 사용하며, 무결성 검증을 위해 ECDSA 전자서명 알고리즘을 사용

③ 블록체인은 이중거래 방지를 위해, 포크(Fork) 발생시 다음 블록을 먼저 생성하여 길이가 긴 블록을 옳은 것으로 판단

④ 블록체인은 새로 만든 블록을 앞 블록과 연결성 검증을 위해 작업증명(PoW)을 수행하며, 이에 추가적인 무결성 강화를 위해 지분증명(PoS)이란 개념을 사용

정답 3번

출제 포인트

블록체인의 거래 전파 방식, 암호기술, 포크 해결 원리, 합의 알고리즘의 역할을 구분하는 문제이다.

핵심 개념

블록체인은 여러 노드가 거래 기록을 공유하고, 각 블록을 앞 블록의 해시값과 연결하여 기록의 위변조를 어렵게 만드는 분산원장이다.
거래는 참여 노드들에 전파되며, 전자서명은 거래 주체와 거래의 진위를 확인하는 데 사용된다.
작업증명(PoW)과 지분증명(PoS)은 블록 생성자와 유효한 체인을 정하는 서로 다른 합의 방식이다.

선지별 해설

① X — 틀린 표현은 '당사자 간 유니캐스트로 전송'이다. 블록체인 거래는 특정 두 당사자 사이에서만 전송되는 것이 아니라 네트워크의 여러 노드로 전파되어 검증·공유된다. 올바르게는 '거래는 P2P 네트워크를 통해 참여 노드들에 전파된다'이다.
② X — 틀린 표현은 '블록암호화 방식을 사용'이다. 블록체인은 블록 전체를 블록암호로 암호화하여 연결하는 것이 아니라 암호학적 해시로 앞 블록과 연결하고 무결성을 확인한다. ECDSA는 일부 블록체인에서 거래의 전자서명에 사용된다. 올바르게는 '블록 연결과 무결성에는 해시를, 거래 인증에는 전자서명을 사용한다'이다.
③ O — 작업증명형 블록체인에서는 포크가 생기면 노드들이 유효한 체인 중 누적 작업량이 가장 큰 체인을 정당한 체인으로 선택한다. 통상 다음 블록이 먼저 이어져 더 길어진 체인이 채택되므로 이중거래를 억제한다.
④ X — 틀린 표현은 '연결성 검증을 위해 작업증명을 수행'하고 '추가적인 무결성 강화를 위해 지분증명을 사용'한다는 부분이다. 블록 간 연결은 앞 블록의 해시값으로 확인하며, PoW와 PoS는 함께 덧붙이는 기술이 아니라 블록 생성과 합의를 위한 대안적 방식이다. 올바르게는 '블록은 해시로 연결되고, 네트워크는 PoW 또는 PoS 같은 합의 방식을 사용한다'이다.

NoteBase

오답 포인트

②는 전자서명 알고리즘이 등장한다는 이유만으로 전체 문장을 옳다고 판단하기 쉽다. 그러나 블록의 연결·무결성을 담당하는 핵심은 블록암호가 아니라 해시이다. ④는 PoW와 PoS를 누적 적용하는 기술로 섞어 놓았지만, 두 방식은 서로 다른 합의 방식이다.

다시 나오면 이렇게 판단

거래 전파는 P2P 네트워크, 블록 연결은 해시, 거래 인증은 전자서명, 체인 선택은 합의 규칙으로 나누어 판단한다. PoW와 PoS가 동시에 무결성을 강화한다고 서술하면 역할을 혼동한 것으로 판단한다.

암기 포인트

거래는 전파, 블록은 해시로 연결, 서명은 인증, PoW·PoS는 합의 방식이다.

NoteBase

문 20. 다음 <보기>의 괄호안에 들어갈 내용으로 가장 옳은 것은?

<보기>
포렌식 관점에서 파일 시스템은 매우 중요하다고 볼 수 있다. 특히 ( )는 파일 디렉터리 및 메타 정보까지 파일 형태로 관리하므로 파일과 디렉터리를 분석하여 정보를 알아내는데 유용하다.

① NTFS
② GPT
③ FAT
④ MBR

정답 1번

출제 포인트

이 문제는 파일과 디렉터리뿐 아니라 파일 시스템의 메타데이터도 파일 형태로 관리하는 NTFS의 구조적 특징을 묻는다.

핵심 개념

NTFS(New Technology File System)는 파일과 디렉터리의 정보를 MFT(Master File Table)에 레코드로 기록하고, MFT·할당 상태·로그 같은 파일 시스템 메타데이터도 특수한 메타데이터 파일로 관리하는 파일 시스템이다. GPT와 MBR은 디스크의 파티션 구성 정보를 기록하는 방식이며, FAT는 파일의 데이터 클러스터 연결 관계를 파일 할당 테이블로 관리하는 파일 시스템이다.

선지별 해설

① O — NTFS는 일반 파일과 디렉터리의 속성을 MFT에 기록하며, MFT 자체를 비롯한 주요 메타데이터도 파일 형태로 다룬다. 따라서 괄호에 들어갈 말로 옳다.
② X — GPT는 디스크 파티션의 위치와 크기 등을 기록하는 파티션 테이블 형식이지, 파일과 디렉터리 및 메타데이터를 파일 형태로 관리하는 파일 시스템이 아니다. 틀린 표현은 ‘GPT가 해당 파일 시스템이다’라는 취지이며, 올바르게는 ‘GPT는 파티션 구성 방식이다’이다.
③ X — FAT는 파일 시스템이지만 파일의 클러스터 연결 정보를 파일 할당 테이블에 기록하는 구조이며, NTFS처럼 주요 메타데이터 전반을 특수 파일로 관리한다는 설명의 대상이 아니다. 틀린 표현은 ‘FAT가 메타 정보까지 파일 형태로 관리한다’는 취지이며, 올바르게는 ‘FAT는 파일 할당 테이블을 중심으로 클러스터 연결을 관리한다’이다.
④ X — MBR은 부팅 코드와 파티션 정보를 담는 디스크 파티션 구성 형식이지 파일 시스템이 아니다. 틀린 표현은 ‘MBR이 해당 파일 시스템이다’라는 취지이며, 올바르게는 ‘MBR은 전통적인 파티션 구성 방식이다’이다.

NoteBase

오답 포인트

GPT와 MBR은 저장장치에서 자주 접하는 용어이지만 파일 시스템이 아니라 파티션 구성 방식이다. 또한 FAT도 파일 시스템이라는 점만 보고 고르면 안 되며, '메타데이터까지 파일 형태로 관리'라는 문구를 NTFS의 MFT 및 메타데이터 파일 구조와 연결해야 한다.

다시 나오면 이렇게 판단

먼저 후보가 파일 시스템인지 파티션 구성 방식인지 구분한다. 이어서 MFT, 메타데이터 파일, 저널링 같은 단서가 나오면 NTFS를 선택하고, 파일 할당 테이블과 클러스터 체인 단서가 나오면 FAT를 선택한다.

암기 포인트

NTFS는 MFT와 메타데이터 파일, FAT는 파일 할당 테이블, GPT·MBR은 파티션 구성 방식이다.

NoteBase