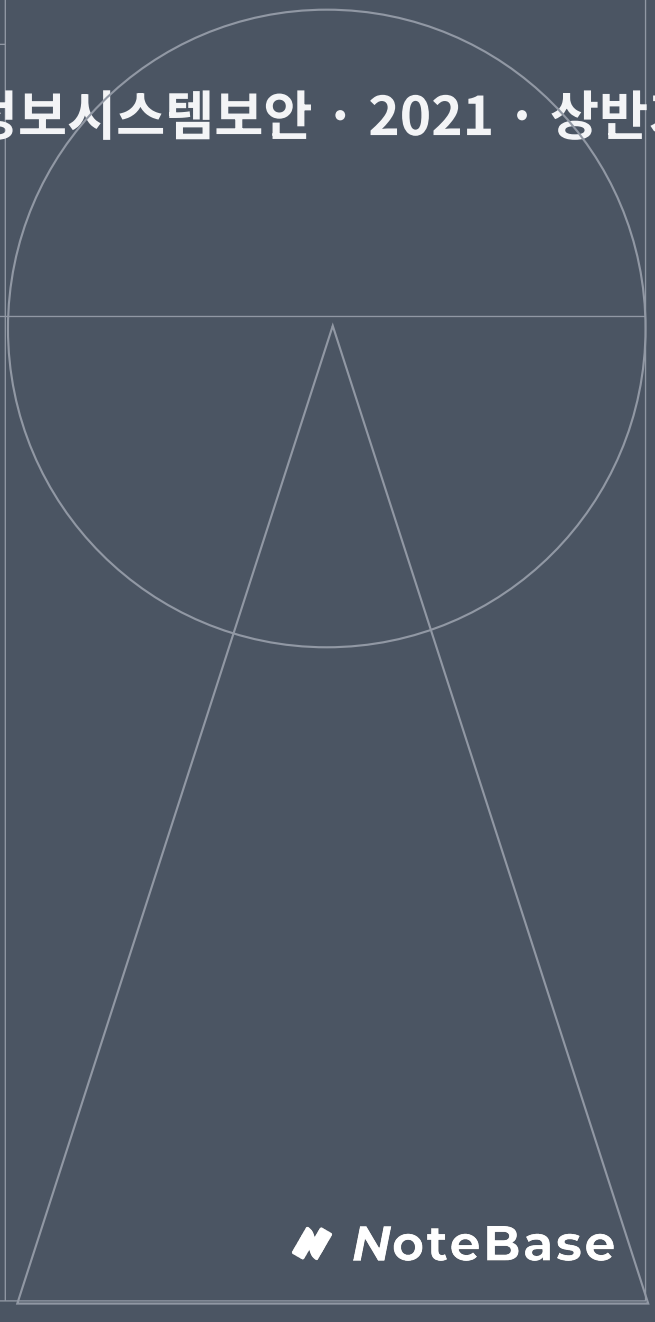
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2021 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2021 · 상반기

공무원/해경/일반직 9급 · 정보시스템보안 · 2021 · 상반기

문 1. 다음 중 디지털 포렌식의 기본 원칙에 대한 설명으로 가장 옳지 않은 것은?

① 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐 획득하여야 하며, 위법한 절차를 거쳐 획득한 증거는 증거능력이 없다.

② 재현의 원칙 : 증거는 어떤 절차를 통해 정제될 수 없으며 똑같은 환경에서 같은 결과가 한번만 나오면 된다.

③ 신속성의 원칙 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 가능한 빠르게 획득해야 한다.

④ 연계 보관성의 원칙 : 증거는 획득 후 이송/분석/보관/법정 제출의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

정답 2번

출제 포인트

디지털 증거가 법정에서 신뢰받기 위해 지켜야 하는 정당성, 재현성, 신속성, 연계 보관성의 의미를 구별하는 문제이다.

핵심 개념

정당성은 적법한 절차로 증거를 수집해야 한다는 원칙이다. 재현성은 동일한 조건과 절차를 적용하면 반복하여 동일한 결과를 얻을 수 있어야 한다는 원칙이다. 신속성은 휘발성 데이터가 사라지거나 변하기 전에 빠르게 확보해야 한다는 원칙이다. 연계 보관성은 수집부터 법정 제출까지 증거의 취급·이동·분석·보관 이력이 끊김 없이 기록되고 추적되어야 한다는 원칙이다.

NoteBase

선지별 해설

① O — 정당성의 원칙은 디지털 증거를 적법한 절차에 따라 획득해야 하며, 위법하게 수집된 증거는 증거능력이 부정될 수 있다는 내용이다.
② X — 틀린 표현은 '어떤 절차를 통해 정제될 수 없으며'와 '같은 결과가 한번만 나오면 된다'이다. 재현의 원칙은 원본의 무결성을 보존하고 분석 절차와 조건을 기록한 상태에서, 동일한 절차를 반복하면 동일한 결과가 나와야 한다는 뜻이다. 따라서 필요한 분석·처리 자체를 금지하는 원칙이 아니며, 한 번의 일치만으로 충족되지 않는다.
③ O — 메모리나 실행 중인 프로세스처럼 전원이 꺼지거나 시간이 지나면 사라질 수 있는 휘발성 정보가 있으므로 가능한 한 신속하게 증거를 확보해야 한다.
④ O — 연계 보관성의 원칙은 증거의 획득, 이송, 분석, 보관, 법정 제출 전 과정에서 누가 언제 어떻게 취급했는지를 기록하여 그 이력을 추적할 수 있게 하는 것이다.

오답 포인트

②는 재현성을 '한 번 같은 결과가 나오는 것'으로 축소하고, 증거의 정제·분석 절차가 전혀 허용되지 않는 것처럼 바꾸었다. 재현성의 핵심은 분석 금지가 아니라 동일 조건·동일 절차에 따른 반복 가능한 결과이다.

다시 나오면 이렇게 판단

적법한 수집은 정당성, 휘발 전의 빠른 확보는 신속성, 취급 이력의 연속적 기록은 연계 보관성, 동일 조건과 절차에서 반복되는 결과는 재현성으로 판단한다.

암기 포인트

정당성은 적법하게, 재현성은 반복해도 같게, 신속성은 사라지기 전에, 연계 보관성은 전 과정을 추적 가능하게 한다.

NoteBase

문 2. 다음 중 정보자산에 대한 위험분석에서 사용하는 ALE, SLE, ARO 사이의 관계로 가장 옳은 것은?

① $ALE = SLE + ARO$

② $SLE = ALE + ARO$

③ $ALE = SLE \times ARO$

④ $SLE = ARO \times ALE$

정답 3번

출제 포인트

이 문제는 연간 예상손실액 *ALE*, 단일 손실 예상액 *SLE*, 연간 발생률 *ARO*의 관계를 묻는 문제이다.

조건 정리

*SLE*는 사고가 한 번 발생했을 때의 예상손실액이고, *ARO*는 같은 사고가 1년 동안 발생할 것으로 예상되는 횟수이다. *ALE*는 해당 위험으로 인해 1년 동안 발생할 것으로 예상되는 총손실액이다.

사용할 공식

$ALE = SLE \times ARO$
한 번의 예상손실액에 연간 예상 발생횟수를 곱하면 연간 예상손실액이 되므로 이 공식을 사용한다.

선지 판단

① X — $ALE = SLE + ARO$는 금액인 *SLE*와 발생률인 *ARO*를 더하므로 성립하지 않는다. 올바르게는 $ALE = SLE \times ARO$이다.
② X — $SLE = ALE + ARO$는 변수의 관계와 연산이 모두 잘못되었다. 올바르게는 $ARO \neq 0$일 때 $SLE = ALE/ARO$이다.
③ O — 단일 손실 예상액에 연간 발생률을 곱하면 연간 예상손실액이 되므로 $ALE = SLE \times ARO$가 성립한다.
④ X — $SLE = ARO \times ALE$는 *ALE*와 *SLE*의 위치가 잘못되었다. 올바르게는 $ARO \neq 0$일 때 $SLE = ALE/ARO$이다.

오답 포인트

①과 ②는 성격이 다른 손실액과 발생률을 더하도록 만든 함정이고, ④는 곱셈 관계에서 구하려는 변수를 이항할 때 나눗셈으로 바꾸지 않은 함정이다.

다시 나오면 이렇게 판단

위험분석 공식은 '한 번의 손실 × 1년의 발생횟수 = 1년의 손실' 순서로 판단한다. 따라서 $SLE \times ARO$의 결과가 *ALE*가 된다.

NoteBase

암기 포인트

연간 손실은 단일 손실에 연간 발생률을 곱한다: $ALE = SLE \times ARO$.

NoteBase

문 3. 다음 중 대칭키 암호에 대한 설명으로 가장 옳지 않은 것은?

① DES, AES는 대칭키 암호 알고리즘에 속한다.

② AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.

③ AES는 128bit 라운드 키를 사용한다.

④ 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.

정답 4번

출제 포인트

대칭키 암호와 공개키 암호의 키 사용 방식, 그리고 AES의 구조와 라운드 키 길이를 구별하는 문제이다.

핵심 개념

대칭키 암호는 송신자와 수신자가 같은 비밀키를 공유하여 암호화와 복호화에 사용하는 방식이다. DES와 AES가 대표적인 대칭키 암호이다.
공개키 암호는 서로 다른 공개키와 개인키를 한 쌍으로 사용하는 방식이다.
AES는 128비트 블록을 처리하는 SPN 구조의 대칭키 암호이며, 원래 암호키의 길이는 128비트·192비트·256비트 중 하나이지만 키 확장으로 생성되는 각 라운드 키는 128비트이다.

선지별 해설

① O — DES와 AES는 모두 암호화와 복호화에 공유 비밀키를 사용하는 대칭키 암호 알고리즘이다.
② O — AES는 바이트 치환, 행 이동, 열 혼합, 라운드 키 덧셈 등을 반복하는 SPN(Substitution-Permutation Network) 구조이다.
③ O — AES의 블록 크기는 128비트이므로 키 확장 과정에서 만들어져 각 라운드의 상태 블록과 결합되는 라운드 키도 128비트이다. 원래 암호키 자체는 128비트·192비트·256비트가 가능하다는 점과 구별된다.
④ X — 틀린 표현은 '두 개의 키 값(비밀키, 공개키)'이다. 이는 대칭키 암호가 아니라 공개키와 개인키라는 서로 다른 키 쌍을 사용하는 공개키 암호의 특징이다. 올바르게는 대칭키 암호는 송신자와 수신자가 하나의 공유 비밀키를 암호화와 복호화에 사용한다고 해야 한다.

오답 포인트

④의 '대칭적으로 존재'라는 표현 때문에 공개키와 비밀키의 쌍을 대칭키 방식으로 착각하기 쉽다. 대칭키의 '대칭'은 두 종류의 키가 짝을 이룬다는 뜻이 아니라 암호화와 복호화에서 같은 공유 비밀키를 사용한다는 뜻이다. 또한 ③의 라운드 키 128비트와 원래 암호키의 세 가지 길이를 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

같은 공유 비밀키를 쓰면 대칭키 암호, 공개키와 개인키라는 서로 다른 키 쌍을 쓰면 공개키 암호로 판단한다. AES에서는 블록과 각 라운드 키는 128비트이고, 원래 암호키는 128비트·192비트·256비트가 가능하다고 구분한다.

암기 포인트

DES·AES는 대칭키, AES는 SPN, 라운드 키는 128비트, 공개키·개인키 쌍은 비대칭키이다.

NoteBase

문 4. 다음 중 Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.

② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.

③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.

④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

정답 3번

출제 포인트

Feistel 구조의 특징과 AES가 사용하는 암호 구조를 구별하는 문제이다.

핵심 개념

Feistel 구조는 입력 블록을 좌우로 나누고 라운드 함수와 XOR 연산을 반복하여 암호화하는 대칭키 블록 암호 구조이다. 복호화는 암호화와 같은 구조를 사용하되 라운드 키의 적용 순서를 반대로 한다. AES는 Feistel 구조가 아니라 하나의 블록 전체에 대치와 치환을 반복하는 SPN 구조를 사용한다.

선지별 해설

① O — Feistel 암호의 강도에는 평문 블록의 길이, 키의 길이, 라운드 수가 중요한 영향을 미친다. 블록과 키의 크기 및 반복 횟수는 공격 난이도와 직접 관련된다.
② O — Feistel 구조는 암호화와 복호화에 같은 연산 구조를 사용할 수 있다. 다만 복호화할 때에는 라운드 키를 암호화 때와 반대 순서로 적용한다.
③ X — 틀린 표현은 ‘AES 암호 알고리즘은 Feistel 암호 방식을 사용한다’이다. 올바르게는 AES는 Feistel 구조가 아니라 SPN 구조를 사용하는 대칭키 블록 암호 알고리즘이다.
④ O — Feistel 구조는 DES와 같은 대칭키 블록 암호 알고리즘을 구성하는 데 사용되는 대표적인 구조이다.

오답 포인트

③은 AES도 대칭키 블록 암호라는 점을 이용해 ‘대칭키 블록 암호이면 Feistel 구조’라고 혼동하게 만든다. 대칭키 블록 암호라는 분류와 내부 암호 구조는 별개의 구분이며, AES의 내부 구조는 SPN이다.

다시 나오면 이렇게 판단

알고리즘의 키 방식과 내부 구조를 나누어 판단한다. DES는 Feistel 구조, AES는 SPN 구조라는 대응 관계를 먼저 확인하면 된다.

암기 포인트

DES는 Feistel, AES는 SPN이다. Feistel 복호화는 같은 구조에 라운드 키 순서만 반대로 적용한다.

NoteBase

문 5. 다음 중 KDC(Key Distribution Center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜로 가장 옳은 것은?

① Otway-Rees 프로토콜

② Needham-Schroeder 프로토콜

③ Kerberos 프로토콜

④ Diffie-Hellman 프로토콜

정답 4번

출제 포인트

이 문제는 신뢰할 수 있는 제3자인 KDC가 세션 키를 배포하는 프로토콜과, 통신 당사자가 공개된 값을 교환하여 공통 비밀값을 만드는 키 합의 프로토콜을 구별하는 문제이다.

핵심 개념

Diffie-Hellman은 두 통신 주체가 각자의 비밀값을 공개하지 않은 채 공개값을 교환하여 동일한 공유 비밀값을 계산하는 키 합의 방식이다. 이 공유 비밀값에서 대칭 세션 키를 도출할 수 있으므로 KDC가 필수적이지 않다. Otway-Rees와 대칭키 방식의 Needham-Schroeder는 신뢰할 수 있는 제3자가 세션 키 설정에 관여하며, Kerberos는 KDC의 인증 서버와 티켓 발급 서버를 이용한다.

선지별 해설

① X — Otway-Rees 프로토콜은 신뢰할 수 있는 제3의 서버가 통신 주체들을 확인하고 세션 키를 전달하는 방식이다. 틀린 부분은 ‘KDC 없이 양쪽 통신 주체가 생성한다’는 점이며, 올바르게는 ‘신뢰할 수 있는 제3의 서버가 세션 키 설정에 관여한다’이다.
② X — 이 문맥의 Needham-Schroeder 대칭키 프로토콜은 KDC가 각 주체와 공유한 장기 대칭키를 이용해 세션 키를 배포한다. 틀린 부분은 ‘KDC 없이’이며, 올바르게는 ‘KDC를 통해 세션 키를 전달받는다’이다.
③ X — Kerberos는 KDC를 중심으로 동작하며, KDC의 인증 서버와 티켓 발급 서버가 인증과 서비스 이용용 세션 키 발급에 관여한다. 틀린 부분은 ‘KDC 없이’이며, 올바르게는 ‘KDC가 티켓과 세션 키를 발급한다’이다.
④ O — Diffie-Hellman 프로토콜은 중앙의 키 배포 기관 없이 두 통신 주체가 공개값을 교환하고 각자 같은 공유 비밀값을 계산하여 대칭 세션 키를 도출할 수 있다.

오답 포인트

‘대칭 세션 키를 사용한다’는 사실과 ‘KDC가 그 키를 배포한다’는 사실을 같은 것으로 보면 틀리기 쉽다. Diffie-Hellman은 대칭 암호 자체가 아니라, 중앙 배포자 없이 양쪽이 대칭키의 재료가 되는 공유 비밀값에 합의하는 방식이다. 또한 기본 Diffie-Hellman만으로는 상대 신원을 인증하지 못하므로 별도의 인증이 없으면 중간자 공격에 취약하지만, 이는 KDC 없는 키 합의가 가능하다는 정답 판단을 바꾸지 않는다.

NoteBase

다시 나오면 이렇게 판단

문제에 ‘KDC가 세션 키를 발급·배포한다’가 나오면 Needham-Schroeder 대칭키 방식이나 Kerberos 계열을 떠올리고, ‘공개값 교환으로 양쪽이 같은 비밀값을 계산한다’가 나오면 Diffie-Hellman으로 판단한다.

암기 포인트

KDC는 키를 배포하고, Diffie-Hellman은 양쪽이 키에 합의한다.

NoteBase

문 6. 정부는 사이버테러를 없애기 위하여 2020년 8월 「개인정보 보호법」 개정으로 100만 명 이상 이용자의 개인정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 망분리를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 가장 옳지 않은 것은?

① DMZ

② OS 커널분리

③ VDI

④ 가상화기술

정답 1번

출제 포인트

이 문제는 업무용 환경과 외부 인터넷 환경을 분리하는 망분리 기술과, 내부망과 외부망 사이에 별도의 보안 구역을 두는 DMZ를 구별하는 문제이다.

핵심 개념

망분리는 업무망과 인터넷망 사이의 직접적인 접속을 차단하는 보안 방식이다. 물리적으로 별도의 단말·망을 사용하는 물리적 망분리와, 가상화 등을 이용해 하나의 장비 안에서 환경을 분리하는 논리적 망분리가 있다. DMZ는 외부에 공개할 서버를 내부망과 외부망 사이의 별도 네트워크 구역에 배치하여 내부망을 보호하는 경계 보안 구조이다.

선지별 해설

① X — DMZ는 웹 서버 등 외부 공개 시스템을 내부망과 외부망 사이의 별도 구역에 두는 경계 보안 구조이므로, 사용자 업무 환경과 인터넷 환경을 분리하는 망분리 기술로 분류하지 않는다. 틀린 표현은 ‘DMZ를 망분리 기술로 본 것’이다. 올바른 표현은 ‘DMZ는 외부 공개 구간과 내부망 사이에 두는 완충 네트워크 구역이다’이다.
② O — OS 커널분리는 운영체제 수준에서 서로 격리된 실행 환경을 구성하므로 논리적 망분리를 구현하는 방식에 해당한다.
③ O — VDI는 서버의 가상 데스크톱에 원격 접속하게 하여 사용자 단말의 인터넷 환경과 업무 환경을 논리적으로 분리할 수 있다.
④ O — 가상화기술은 데스크톱이나 애플리케이션 등 실행 환경을 격리하여 논리적 망분리를 구현하는 기반 기술이다.

오답 포인트

DMZ에도 ‘분리된 구역’이라는 성격이 있어 망분리 기술로 착각하기 쉽다. 그러나 DMZ의 핵심은 공개 서버를 위한 경계 구역이고, 망분리의 핵심은 업무 환경과 인터넷 환경의 접속 차단이다.

NoteBase

다시 나오면 이렇게 판단

선지가 사용자 단말의 업무·인터넷 환경을 물리적 또는 논리적으로 격리하는 기술인지 확인한다. 외부 공개 서버를 내부망과 분리해 배치하는 경계 구역을 설명한다면 DMZ이다.

암기 포인트

망분리는 업무망과 인터넷망의 격리, DMZ는 외부망과 내부망 사이의 완충 구역이다.

NoteBase

문 7. 다음 중 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 가장 옳지 않은 것은?

① secure - telnet이나 ftp 등 인증과정을 거치는 모든 로그를 저장

② loginlog - 성공한 로그인에 대한 내용

③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보

④ btmp - 5번 이상 실패한 로그인 시도 정보

정답 2번

출제 포인트

유닉스·리눅스의 주요 로그 파일을 인증 성공, 인증 실패, 보안·인증 메시지, 프로세스 회계 정보로 구분하는 문제이다.

핵심 개념

secure는 보안·인증 관련 메시지를, loginlog는 반복된 로그인 실패 기록을, pacct는 프로세스 회계 정보를, btmp는 실패한 로그인 시도 정보를 저장한다. 특히 loginlog는 성공한 로그인 기록이 아니라 실패한 로그인 기록이라는 점이 핵심이다.

선지별 해설

① O

secure는 로그인 인증 등 보안·인증 관련 메시지를 기록하는 로그이다. telnet이나 FTP처럼 인증 절차를 거치는 서비스의 인증 기록을 확인하는 데 활용된다.

② X

틀린 표현은 '성공한 로그인'이다. loginlog는 성공한 로그인이 아니라 일정 횟수 이상 연속으로 실패한 로그인 시도 정보를 기록한다. 성공한 로그인 이력은 일반적으로 wtmp나 lastlog 계열에서 확인한다.

③ O

pacct는 프로세스 회계가 활성화된 시스템에서 사용자가 실행한 명령·프로세스의 실행 정보를 기록한다. 사용자 ID, 실행 명령, CPU 사용 시간 등의 회계 정보가 포함될 수 있다.

④ O

btmp는 실패한 로그인 시도 정보를 기록하는 파일이므로 로그 종류와 기록 대상의 연결이 맞다. 다만 실패 횟수 임계값은 시스템과 설정에 따라 달라질 수 있으며, btmp의 본질은 실패한 로그인 시도 자체를 기록하는 데 있다.

NoteBase

오답 포인트

②의 '성공한'이라는 단어가 함정이다. loginlog라는 이름 때문에 정상 로그인 이력으로 오해하기 쉽지만, 실제 기록 대상은 반복된 로그인 실패이다. 또한 로그인 실패 횟수 조건과 실패 로그 파일의 기본 역할을 혼동하지 않아야 한다.

다시 나오면 이렇게 판단

로그 파일명을 기록 대상과 짝지어 판단한다. secure는 보안·인증, loginlog와 btmp는 로그인 실패, pacct는 사용자가 실행한 프로세스, wtmp·lastlog는 정상 로그인 이력으로 구분한다.

암기 포인트

loginlog·btmp는 실패, pacct는 실행 프로세스, secure는 보안·인증이다.

NoteBase

문 8. 다음 <보기> 중 리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 가장 옳은 것을 모두 고른 것은?

<보기>
㉠ 재부팅 시간 정보
㉡ 사용자의 로그인/로그아웃 정보
㉢ 로그인에 실패한 사용자의 IP주소

① ㉠
② ㉠, ㉡
③ ㉡
④ ㉠, ㉡, ㉢

정답 2번

출제 포인트

리눅스의 wtmp와 btmp 로그가 각각 어떤 접속 기록을 저장하는지 구분하는 문제이다.

핵심 개념

wtmp는 시스템의 부팅·재부팅 기록과 사용자의 로그인·로그아웃 이력을 누적하여 저장하는 로그이다. 반면 btmp는 실패한 로그인 시도를 저장하므로, 로그인 실패 사용자의 접속 IP 주소는 btmp에서 확인한다.

NoteBase

선지별 해설

① X
㉠ 재부팅 시간 정보는 wtmp에서 확인할 수 있지만, ㉡ 로그인·로그아웃 정보도 확인할 수 있으므로 ㉠만 고른 것이 틀렸다. 올바르게는 ㉠과 ㉡을 함께 골라야 한다.

② O
wtmp에는 시스템 재부팅 기록과 사용자의 로그인·로그아웃 이력이 남으므로 ㉠과 ㉡이 모두 옳다.

③ X
㉡ 로그인·로그아웃 정보는 wtmp에서 확인할 수 있지만, ㉠ 재부팅 시간 정보도 확인할 수 있으므로 ㉡만 고른 것이 틀렸다. 올바르게는 ㉠과 ㉡을 함께 골라야 한다.

④ X
틀린 항목은 ㉢이다. 로그인 실패 사용자의 IP 주소는 실패한 로그인 시도를 기록하는 btmp에서 확인한다. 올바르게는 ㉠과 ㉡만 고른다.

오답 포인트

로그인 관련 기록이라는 공통점 때문에 성공한 로그인 이력과 실패한 로그인 시도를 같은 파일로 묶기 쉽다. wtmp는 정상 로그인·로그아웃과 재부팅 이력, btmp는 로그인 실패 이력이라는 차이가 핵심이다.

다시 나오면 이렇게 판단

정상 접속의 시작·종료와 시스템 재부팅은 wtmp, 실패한 로그인 시도는 btmp로 구분한다. 따라서 보기에서 로그인 실패가 나오면 wtmp 대상에서 제외한다.

암기 포인트

wtmp는 접속·종료·재부팅, btmp는 bad login인 로그인 실패이다.

NoteBase

문 9. 다음 중 스트림 암호에 대한 설명으로 가장 옳지 않은 것은?

① 통상 한 번에 1비트씩 암호화 및 복호화를 하기 때문에 하드웨어적인 shift register 방식을 많이 사용한다.

② 짧은 주기와 높은 선형 복잡도가 요구되며 주로 LFSR을 이용한다.

③ 스트림 암호는 데이터의 흐름을 순차적으로 처리해 가기 때문에 내부상태를 가지고 있다.

④ 블록 암호화 방식보다 매우 빠르지만 암호화 강도는 약하다.

정답 2번

출제 포인트

스트림 암호의 처리 방식과 안전한 키스트림이 갖추어야 할 조건을 묻는 문제이다.

핵심 개념

스트림 암호는 키와 내부상태로부터 키스트림을 생성하고, 평문을 비트 또는 바이트 단위로 순차 처리하는 암호 방식이다. 안전한 키스트림은 같은 패턴이 빨리 반복되지 않도록 주기가 길어야 하며, 적은 출력만으로 전체 수열을 예측하기 어렵도록 선형 복잡도도 높아야 한다.

선지별 해설

① O
스트림 암호는 평문을 통상 비트 단위로 연속 처리하므로 하드웨어에서는 시프트 레지스터를 이용한 키스트림 생성 구조가 많이 사용된다.

② X
틀린 표현은 '짧은 주기'이다. 주기가 짧으면 키스트림 패턴이 빨리 반복되어 분석과 예측에 취약해진다.
올바르게는 '긴 주기와 높은 선형 복잡도가 요구되며, 키스트림 생성에 LFSR 등이 이용된다'이다.

③ O
스트림 암호는 키스트림을 순차적으로 생성해야 하므로 현재 레지스터 값이나 이전 처리 결과와 같은 내부상태를 유지한다.

④ O
전통적인 교과서식 비교에서 스트림 암호는 단순한 연산으로 데이터를 연속 처리하므로 블록 암호보다 빠른 실시간 처리가 가능하지만, 키스트림 재사용이나 상태·동기 관리 오류에 민감하여 안전성 확보가 어렵다고 본다.

NoteBase

오답 포인트

②의 ‘높은 선형 복잡도’와 ‘LFSR’은 맞는 특징이어서 문장 전체를 옳다고 보기 쉽다. 그러나 키스트림의 반복을 늦추려면 필요한 것은 짧은 주기가 아니라 긴 주기이다.

다시 나오면 이렇게 판단

키스트림의 안전 조건을 묻는 선지에서는 ‘긴 주기’와 ‘높은 선형 복잡도’를 한 묶음으로 판단한다. 주기가 짧다고 하면 반복 가능성이 커지므로 틀린 설명이다.

암기 포인트

스트림 암호의 키스트림은 긴 주기, 높은 선형 복잡도가 핵심이다.

NoteBase

문 10. 다음은 정보보호 관리 체계(ISMS, Information Security Management System) 5단계 과정을 수립하려고 한다. 가장 옳은 순서는?

① 경영 조직 → 위험 관리 → 정책 수립 및 범위 설정 → 구현 → 사후관리
② 정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리
③ 정책 수립 및 범위 설정 → 경영 조직 → 구현 → 위험 관리 → 사후관리
④ 경영 조직 → 정책 수립 및 범위 설정 → 위험 관리 → 구현 → 사후관리

정답 2번

출제 포인트

이 문제는 정보보호 관리 체계를 수립할 때 정책과 범위를 정한 뒤 조직을 구성하고, 위험 평가 결과에 따라 보호 대책을 구현한 후 사후관리하는 흐름을 묻는 문제이다.

올바른 순서

1. 정책 수립 및 범위 설정 — 정보보호의 방향과 관리 체계를 적용할 업무·조직의 범위를 정한다.
2. 경영 조직 — 정해진 정책과 범위에 따라 책임, 권한 및 수행 조직을 마련한다.
3. 위험 관리 — 보호할 자산과 위협·취약점을 식별하고 위험을 분석하여 대응 방안을 정한다.
4. 구현 — 위험 관리에서 정한 보호 대책과 통제를 실제로 적용한다.
5. 사후관리 — 운영 결과를 점검하고 미흡한 부분을 보완·개선한다.

정책과 범위가 조직 구성의 기준이 되고, 위험 관리 결과가 구현할 보호 대책의 근거가 되므로 이 선후관계를 지켜야 한다.

NoteBase

선지별 해설

① X — '경영 조직 → 위험 관리 → 정책 수립 및 범위 설정'의 순서가 잘못되었다. 정책과 적용 범위를 먼저 정해야 그에 맞는 조직을 구성하고 위험을 관리할 수 있다. 올바르게는 '정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리'이다.

② O — 정책과 범위를 먼저 정하고, 수행 조직을 구성한 뒤, 위험을 관리하여 필요한 보호 대책을 구현하고 사후관리하는 정확한 순서이다.

③ X — '구현 → 위험 관리'의 선후관계가 뒤바뀌었다. 먼저 위험을 식별·분석하고 대응 방안을 정해야 그 결과에 맞는 보호 대책을 구현할 수 있다. 올바르게는 '정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리'이다.

④ X — '경영 조직 → 정책 수립 및 범위 설정'의 선후관계가 잘못되었다. 관리 체계의 방향과 적용 범위를 먼저 확정한 뒤 이를 수행할 조직과 역할을 정한다. 올바르게는 '정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리'이다.

오답 포인트

①과 ④는 경영 조직을 정책 수립보다 앞에 둔 점이 함정이고, ③은 보호 대책을 위험 분석 전에 구현하도록 순서를 바꾼 점이 함정이다. 정책이 전체 체계의 출발점이고 위험 관리가 구현의 근거라는 두 경계를 구분해야 한다.

다시 나오면 이렇게 판단

절차형 문제에서는 '방향과 범위 결정 → 수행 주체 구성 → 위험 파악과 대응 결정 → 대책 실행 → 점검과 개선'의 인과관계로 순서를 판단한다.

암기 포인트

정책·범위 → 조직 → 위험 → 구현 → 사후관리의 순서이다.

NoteBase

문 11. 다음 <보기>의 ㉠, ㉡에 들어갈 웹 공격 기법으로 가장 옳은 것은?

<보기>
(㉠)은(는) 웹 해킹으로 서버 권한을 획득한 후, 해당 서버에서 공격자의 PC로 연결하고 공격자가 직접 명령을 입력하여 개인정보 전송 등의 악의적인 행위를 하는 공격이다. 이 기법은 방화벽의 내부에서 외부로 나가는 패킷에 대한 아웃바운드 필터링을 수행하지 않는 허점을 이용한다.
(㉡)은(는) 공격자가 웹 서버의 게시판 등에 악성 스크립트를 삽입한 후, 사용자의 쿠키와 같은 개인정보를 특정 사이트로 전송하게 하거나 악성파일을 다운로드하여 실행하도록 유도하는 공격이다.

① ㉠: 디렉토리 리스팅, ㉡: 포맷 스트링

② ㉠: 디렉토리 리스팅, ㉡: XSS

③ ㉠: 리버스 텔넷, ㉡: 포맷 스트링

④ ㉠: 리버스 텔넷, ㉡: XSS

정답 4번

출제 포인트

이 문제는 공격의 연결 방향과 악성 스크립트의 실행 위치를 근거로 리버스 텔넷과 XSS를 구별하는 문제이다.

핵심 개념

리버스 텔넷: 공격자가 장악한 서버가 공격자의 PC로 역방향 연결을 맺고, 공격자가 그 연결을 통해 서버에 명령을 내리는 공격이다. 내부에서 외부로 나가는 통신이 허용된 환경을 악용한다.
XSS: 공격자가 웹 페이지나 게시판에 악성 스크립트를 삽입하여, 해당 페이지를 열어 본 사용자의 브라우저에서 스크립트가 실행되게 하는 공격이다. 쿠키 등 개인정보 탈취나 악성 동작 유도에 이용될 수 있다.
디렉토리 리스팅은 웹 서버의 디렉터리와 파일 목록이 노출되는 취약점이고, 포맷 스트링 공격은 입력값이 서식 문자열로 부적절하게 처리되는 취약점을 악용하는 공격이다.

NoteBase

선지별 해설

① X
㉠과 ㉡이 모두 틀렸다. 서버가 공격자의 PC로 연결되어 공격자가 명령을 입력하는 ㉠은 디렉토리 리스팅이 아니라 리버스 텔넷이고, 게시판의 악성 스크립트가 사용자 측에서 실행되는 ㉡은 포맷 스트링이 아니라 XSS이다.

② X
㉡의 XSS는 맞지만 ㉠의 '디렉토리 리스팅'이 틀렸다. ㉠은 장악한 서버가 외부의 공격자 PC로 역접속하는 리버스 텔넷이다.

③ X
㉠의 리버스 텔넷은 맞지만 ㉡의 '포맷 스트링'이 틀렸다. ㉡은 웹 페이지에 삽입된 악성 스크립트가 사용자의 브라우저에서 실행되는 XSS이다.

④ O
㉠은 서버에서 공격자 PC로 역방향 연결을 맺는 리버스 텔넷이고, ㉡은 게시판 등에 삽입한 악성 스크립트를 사용자의 브라우저에서 실행시키는 XSS이므로 두 대응이 모두 옳다.

오답 포인트

㉠의 '서버 권한 획득'이라는 표현만 보고 서버 내부의 파일 목록 노출과 혼동하거나, ㉡의 '악성 문자열 삽입'만 보고 포맷 스트링 공격으로 오인하기 쉽다. ㉠은 내부 서버에서 공격자에게 나가는 역접속, ㉡은 웹 페이지를 본 사용자의 브라우저에서 실행되는 스크립트가 결정적 단서이다.

다시 나오면 이렇게 판단

장악된 시스템이 공격자 쪽으로 연결하고 그 통로로 명령을 받으면 리버스 텔넷으로 판단한다. 게시판이나 웹 페이지에 삽입된 스크립트가 방문자의 브라우저에서 실행되어 쿠키 탈취 등의 피해를 일으키면 XSS로 판단한다.

암기 포인트

서버가 공격자에게 역접속하면 리버스 텔넷, 웹 페이지의 스크립트가 사용자 브라우저에서 실행되면 XSS이다.

NoteBase

문 12. 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec(IP Security Protocol)에 대한 설명 중 가장 옳지 않은 것은?

① 네트워크 계층의 보안을 위하여 인증 헤더(AH, Authentication Header) 프로토콜과 ESP(Encapsulating Security Payload) 프로토콜을 사용하여 보안연계(SA, Security Association) 서비스를 제공한다.

② 강력한 암호화와 인증 방식을 가지며, 두 컴퓨터 사이의 터널화 된 통신을 가능하도록 한다.

③ 비연결 무결성은 메시지가 위·변조되지 않았음을 보장해준다.

④ ESP 프로토콜은 암호화를 지원하지 않으며 AH 프로토콜만 암호화를 지원한다.

정답 4번

출제 포인트

IPSec의 구성 프로토콜인 AH와 ESP가 제공하는 보안 기능의 차이를 묻는 문제이다.

핵심 개념

IPSec는 IP 계층에서 통신의 기밀성, 무결성, 출처 인증 등을 제공하는 보안 프로토콜 체계이다.
AH는 데이터의 무결성과 출처 인증을 제공하지만 암호화를 통한 기밀성은 제공하지 않는다. ESP는 데이터 암호화를 통한 기밀성을 제공하며, 설정에 따라 무결성과 출처 인증도 제공할 수 있다.
SA는 통신에 적용할 보안 프로토콜, 알고리즘, 키 등의 보안 매개변수를 정한 단방향 논리적 연결이다.

선지별 해설

① O — IPSec는 네트워크 계층에서 AH와 ESP를 사용하며, 통신 당사자는 SA에 정해진 보안 매개변수에 따라 보호 서비스를 적용한다.
② O — IPSec는 암호화와 인증 기능을 제공하며, 터널 모드에서는 기존 IP 패킷 전체를 새 IP 패킷 안에 캡슐화하여 두 보안 종단 사이의 터널 통신을 구현할 수 있다.
③ O — 비연결형 무결성은 각 IP 패킷이 전송 중 위조되거나 변조되지 않았는지를 검증하는 기능이다.
④ X — 틀린 표현은 'ESP 프로토콜은 암호화를 지원하지 않으며 AH 프로토콜만 암호화를 지원한다'이다. 올바르게는 ESP가 암호화를 통한 기밀성을 지원하고, AH는 암호화를 지원하지 않으며 무결성과 출처 인증을 제공한다.

오답 포인트

④는 AH와 ESP의 기능을 정확히 뒤바꾼 선지이다. AH의 'Authentication'이라는 이름 때문에 강한 보안 기능 전반을 제공한다고 오해하기 쉽지만, 암호화와 기밀성의 핵심은 ESP이다.

NoteBase

다시 나오면 이렇게 판단

선지에 암호화 또는 기밀성이 나오면 ESP에 연결한다. AH는 무결성과 출처 인증, ESP는 기밀성을 중심으로 판단하면 두 프로토콜을 구별할 수 있다.

암기 포인트

AH는 인증·무결성, ESP는 암호화·기밀성이다.

NoteBase

문 13. 다음 <보기>의 접근 제어 정책으로 가장 옳은 것은 무엇인가?

<보기>
◯ 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근 통제 정보가 복사된 객체로 전달되지 않는다.
◯ 특정 객체에 대해 특정 주체가 다른 주체에 대해 임의적으로 접근 제어가 가능하여 매우 유연한 접근 제어 서비스를 제공할 수 있다.

① Access Control List
② RBAC
③ DAC
④ MAC

정답 3번

출제 포인트

객체 소유자가 접근 권한을 자율적으로 부여·변경할 수 있고, 정보가 복사될 때 원래 객체의 접근 통제 정보가 함께 전달되지 않는 정책이 임의적 접근 통제(DAC)임을 구별하는 문제이다.

핵심 개념

DAC(임의적 접근 통제)는 객체의 소유자가 다른 주체의 접근 권한을 임의로 부여하거나 회수하는 정책이다. 유연성이 높지만, 객체의 내용이 다른 객체로 복사될 때 원래의 접근 통제 정보가 자동으로 따라가지 않아 정보 흐름을 강제하기 어렵다.
MAC(강제적 접근 통제)는 보안 등급과 허가 등 중앙의 강제 정책에 따라 접근을 결정하므로 개별 주체가 권한을 임의로 바꿀 수 없다.
RBAC(역할 기반 접근 통제)는 사용자에게 직접 권한을 주기보다 역할에 권한을 연결하고 사용자를 역할에 배정한다.
ACL(접근 제어 목록)은 객체별로 어떤 주체가 어떤 권한을 갖는지 기록한 목록으로, 접근 통제를 구현하는 자료 구조이다.

NoteBase

선지별 해설

① X — Access Control List는 객체를 기준으로 주체별 허용 권한을 기록한 목록이다. 틀린 부분은 이를 <보기>의 접근 제어 정책 자체로 본 점이며, 올바른 정책 명칭은 DAC이다. ACL은 DAC를 구현하는 데 사용될 수 있지만 DAC와 같은 정책 분류명은 아니다.
② X — RBAC는 권한을 역할에 부여하고 사용자를 역할에 배정하는 정책이다. 틀린 부분은 객체 소유자가 다른 주체의 권한을 임의로 정한다는 특징과 연결한 점이며, 이는 RBAC가 아니라 DAC의 특징이다.
③ O — DAC는 객체 소유자가 접근 권한을 자율적으로 부여·변경하므로 유연하다. 또한 정보가 다른 객체로 복사될 때 원래 객체의 접근 통제 정보가 자동 승계되지 않는다는 <보기>의 설명과도 일치한다.
④ X — MAC는 보안 등급과 허가 등 중앙에서 정한 규칙을 모든 주체에게 강제하는 정책이다. 틀린 부분은 특정 주체가 다른 주체의 접근을 임의로 제어할 수 있다고 본 점이며, MAC에서는 개별 주체가 권한을 임의로 변경할 수 없다.

오답 포인트

①의 ACL은 DAC 환경에서 권한을 표현하는 수단으로 자주 사용되므로 정책인 DAC와 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '특정 주체가 다른 주체에 대해 임의적으로 접근 제어'한다는 부분이며, 이는 DAC를 직접 가리킨다.

다시 나오면 이렇게 판단

소유자의 자율적 권한 부여는 DAC, 보안 등급에 따른 중앙의 강제는 MAC, 역할을 통한 권한 배정은 RBAC, 객체별 주체·권한 목록은 ACL로 구별한다.

암기 포인트

소유자 재량은 DAC, 등급 강제는 MAC, 역할 중심은 RBAC, 객체별 권한표는 ACL이다.

NoteBase

문 14. 다음 <보기>에서 설명하는 블록암호 운용 모드는?

<보기>
◯ 암·복호화 모두 병렬 처리가 가능하다.
◯ 블록 암호 알고리즘의 암호화 로직만 사용한다.
◯ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① CTR
② CFB
③ CBC
④ ECB

정답 1번

출제 포인트

이 문제는 블록암호 운용 모드 가운데 암·복호화의 병렬 처리 가능 여부, 암호화 로직만 사용하는지, 암호문 비트 오류가 평문에 전파되는 범위를 함께 비교하는 문제이다.

핵심 개념

CTR은 카운터 값을 블록암호의 암호화 함수에 넣어 키 스트림을 만들고, 이를 평문 또는 암호문과 XOR하는 방식이다. 각 카운터 블록을 독립적으로 처리하므로 암·복호화 모두 병렬 처리가 가능하고 암호화 로직만 사용한다. 또한 전송 중 암호문 한 비트가 바뀌면 복호화된 평문의 대응하는 한 비트만 바뀐다.
CFB는 앞선 암호문을 다음 처리에 되먹임하고, CBC는 앞선 암호문 블록과 연계하여 처리한다. ECB는 각 블록을 독립적으로 처리하지만 복호화에는 블록암호의 복호화 로직이 필요하다.

선지별 해설

① O — CTR은 카운터별 키 스트림을 독립적으로 생성하므로 암·복호화 병렬 처리가 가능하고 암호화 로직만 사용한다. 암호문 한 비트 오류도 평문의 대응 비트 하나에만 영향을 주므로 보기의 세 조건을 모두 만족한다.
② X — CFB라는 선택이 틀렸다. CFB는 앞선 암호문을 되먹임하므로 암호화 처리를 병렬화할 수 없고, 암호문 비트 오류가 이후 처리 구간에도 전파될 수 있다. 올바르게는 보기의 모드는 CTR이다.
③ X — CBC라는 선택이 틀렸다. CBC 암호화는 앞선 암호문 블록에 의존하여 순차적으로 이루어지며, 복호화에는 블록암호의 복호화 로직이 사용된다. 암호문 한 비트 오류는 해당 평문 블록을 광범위하게 훼손하고 다음 평문 블록의 대응 비트에도 영향을 준다. 올바르게는 보기의 모드는 CTR이다.
④ X — ECB라는 선택이 틀렸다. ECB는 블록별 병렬 처리가 가능하지만 복호화할 때 블록암호의 복호화 로직이 필요하며, 암호문 한 비트 오류가 복호화된 평문의 한 비트에만 제한된다고 볼 수 없다. 올바르게는 보기의 모드는 CTR이다.

NoteBase

오답 포인트

ECB도 블록을 독립적으로 처리하므로 병렬 처리만 보면 CTR과 혼동하기 쉽다. 그러나 '암호화 로직만 사용'과 '한 비트 오류가 평문의 한 비트에만 영향'까지 동시에 성립하는지가 결정적인 구분 기준이다.

다시 나오면 이렇게 판단

카운터, 암·복호화 병렬 처리, 암호화 함수만 사용, 비트 오류의 일대일 대응이 함께 제시되면 CTR로 판단한다. 앞선 암호문이나 블록을 되먹임한다면 CFB 또는 CBC이므로 병렬 처리와 오류 전파 범위를 다시 확인한다.

암기 포인트

CTR은 카운터를 암호화해 키 스트림을 만들며, 양방향 병렬 처리·암호화 로직만 사용·비트 오류 일대일 대응이 핵심이다.

NoteBase

문 15. 다음 <보기>에서 설명하는 기법으로 가장 옳은 것은?

<보기>
높은 등급의 인가를 가진 주체가 낮은 등급의 인가를 가진 주체에게 정보를 보내는 방법으로 비밀정보를 다른 사람이 알지 못하게 전달하는 방법이다.

① 터널링
② 은닉채널
③ 송신채널
④ 이중채널

정답 2번

출제 포인트

보안 정책이 허용하지 않은 정보 전달 경로인 은닉채널의 정의를 식별하는 문제이다.

핵심 개념

은닉채널은 정상적인 통신용으로 허가된 경로가 아닌 수단을 이용하여 보안 정책을 우회하고 정보를 전달하는 경로이다. 높은 보안 등급의 주체가 낮은 등급의 주체에게 비밀정보를 몰래 전달하는 상황이 대표적이다.
은닉채널은 자원의 상태에 정보를 담는 저장 은닉채널과 작업 시간이나 사건 발생 간격을 이용하는 타이밍 은닉채널로 구분할 수 있다.

선지별 해설

① X — 터널링은 한 통신 프로토콜의 데이터를 다른 프로토콜의 패킷 안에 캡슐화하여 전달하는 기법이다. 높은 등급에서 낮은 등급으로 보안 정책을 우회하여 비밀정보를 보내는 경로를 뜻하지 않는다. 틀린 표현은 '터널링'이며, 올바르게는 '은닉채널'이다.
② O — 은닉채널은 보안 정책상 허용되지 않은 경로를 이용하여 비밀정보를 은밀하게 전달한다. 보기의 높은 등급 주체에서 낮은 등급 주체로의 비밀정보 전달이 이에 해당한다.
③ X — 송신채널은 정보를 보내는 일반적인 통신 경로를 가리킬 뿐, 보안 통제를 우회하는 비밀 전달 기법의 명칭이 아니다. 틀린 표현은 '송신채널'이며, 올바르게는 '은닉채널'이다.
④ X — 이중채널은 보기에서 설명한 보안 정책 우회형 정보 유출 경로의 명칭이 아니다. 두 채널을 사용한다는 사실만으로 높은 등급의 정보를 낮은 등급으로 몰래 전달하는 개념이 성립하지 않는다. 틀린 표현은 '이중채널'이며, 올바르게는 '은닉채널'이다.

NoteBase

오답 포인트

‘다른 사람이 알지 못하게 전달한다’는 표현만 보고 데이터를 감싸는 터널링을 고르기 쉽다. 그러나 핵심 단서는 ‘높은 등급에서 낮은 등급으로’와 ‘비밀정보를 은밀하게 전달’한다는 점이며, 이는 보안 정책을 우회하는 은닉채널을 가리킨다.

다시 나오면 이렇게 판단

허가되지 않은 경로, 상위 등급에서 하위 등급으로의 비밀정보 전달, 자원 상태나 시간 간격을 이용한 정보 전달이 제시되면 은닉채널로 판단한다. 다른 프로토콜 안에 패킷을 넣어 전송한다는 설명이면 터널링으로 구분한다.

암기 포인트

보안 정책을 몰래 우회하는 길은 은닉채널, 프로토콜 안에 다른 프로토콜을 넣는 것은 터널링이다.

NoteBase

문 16. 다음 <보기>는 사이버 침해사고 대응절차에 대한 설명이다. 침해사고 대응 1단계부터 6단계까지 순서를 가장 옳게 나열한 것은?

<보기>
㉠ 침해사고의 인식 및 신고
㉡ 긴급조치
㉢ 침해사고 결과 분석 및 보고서 작성
㉣ 분석
㉤ 재발방지 조치
㉥ 침해사고 분석 및 대응 결과 승인

① ㉠-㉡-㉣-㉤-㉢-㉥
② ㉠-㉡-㉢-㉣-㉤-㉥
③ ㉠-㉡-㉢-㉤-㉥-㉣
④ ㉢-㉣-㉤-㉥-㉡-㉠

정답 1번

출제 포인트

사이버 침해사고 대응이 사고 인지와 신고에서 시작하여 긴급조치, 분석, 재발방지, 결과 정리, 승인으로 마무리되는 절차를 묻는 문제이다.

올바른 순서

1단계 ㉠ 침해사고의 인식 및 신고 — 침해 정황을 확인하고 대응 절차를 시작한다.
2단계 ㉡ 긴급조치 — 피해 확산을 막기 위한 즉시 조치를 한다.
3단계 ㉣ 분석 — 사고 원인, 침해 범위, 영향을 분석한다.
4단계 ㉤ 재발방지 조치 — 분석 결과를 바탕으로 취약점을 보완한다.
5단계 ㉢ 침해사고 결과 분석 및 보고서 작성 — 대응과 재발방지 결과를 종합하여 문서화한다.
6단계 ㉥ 침해사고 분석 및 대응 결과 승인 — 작성된 결과를 최종 검토하고 승인한다.

올바른 순서는 ㉠-㉡-㉣-㉤-㉢-㉥이다. 긴급조치 후의 원인 분석이 재발방지 조치의 근거가 되고, 조치 결과가 정리된 뒤에 보고서를 작성하여 최종 승인을 받기 때문이다.

NoteBase

선지별 해설

① O — ㉠ 인식·신고 → ㉡ 긴급조치 → ㉣ 분석 → ㉤ 재발방지 조치 → ㉢ 결과 분석·보고서 작성 → ㉥ 승인으로 이어지는 올바른 순서이다.

② X — ㉢ 결과 분석 및 보고서 작성을 ㉣ 분석과 ㉤ 재발방지 조치보다 앞에 둔 부분이 틀렸다. 보고서는 사고 분석과 재발방지 조치의 결과까지 종합해야 한다. 올바르게는 ㉠-㉡-㉣-㉤-㉢-㉥이다.

③ X — ㉢ 결과 분석 및 보고서 작성과 ㉥ 승인을 ㉣ 분석보다 앞에 둔 부분이 틀렸다. 분석과 재발방지 조치를 마친 뒤 보고서를 작성하고 마지막에 승인해야 한다. 올바르게는 ㉠-㉡-㉣-㉤-㉢-㉥이다.

④ X — ㉢ 결과 분석 및 보고서 작성으로 시작하고 ㉠ 인식 및 신고를 마지막에 둔 부분이 틀렸다. 사고를 먼저 인식·신고해야 긴급조치와 후속 분석이 시작될 수 있다. 올바르게는 ㉠-㉡-㉣-㉤-㉢-㉥이다.

오답 포인트

㉣의 '분석'과 ㉢의 '결과 분석 및 보고서 작성'을 같은 단계처럼 보는 것이 함정이다. ㉣은 원인과 범위를 파악하는 실무 분석이고, ㉢은 분석과 재발방지 조치가 끝난 뒤 전체 대응 결과를 종합하여 보고서로 만드는 단계이다.

다시 나오면 이렇게 판단

절차형 문항은 '사고 발견 → 확산 차단 → 원인 분석 → 재발 방지 → 결과 문서화 → 최종 승인'의 의존관계로 판단한다. 앞 단계의 산출물이 뒤 단계의 입력이 되는지를 확인하면 순서를 구분할 수 있다.

암기 포인트

인식·신고 → 긴급조치 → 분석 → 재발방지 → 보고서 → 승인으로 기억한다.

NoteBase

문 17. 다음 중 커버로스(Kerberose)에 대한 설명으로 가장 옳지 않은 것은?

① 커버로스는 모든 사용자의 패스워드를 알고 있고, 중앙집중식 데이터베이스에 그 패스워드를 저장하고 있는 인증 서버를 이용한다.

② 커버로스는 사용자에게 동일한 계정 정보로 여러가지 서비스를 받을 수 있게 한다.

③ 커버로스는 패스워드 사전공격(Dictionary Attack)에 강하다.

④ 대칭키를 사용하여 도청으로부터 보호한다.

정답 3번

출제 포인트

Kerberos의 중앙 집중식 인증 구조, 통합 인증 기능, 대칭키 사용 방식, 패스워드 추측 공격에 대한 취약성을 구별하는 문제이다.

핵심 개념

Kerberos는 신뢰할 수 있는 키 분배 센터(KDC)가 티켓과 세션키를 발급하여 네트워크상의 사용자와 서비스를 인증하는 대칭키 기반 인증 프로토콜이다. 사용자는 처음 인증한 뒤 발급받은 티켓을 이용해 여러 서비스에 접근할 수 있으므로 통합 인증(SSO)이 가능하다. 다만 사용자의 장기 비밀키가 패스워드에서 만들어지는 구조에서는 약한 패스워드를 사용하면 획득한 인증 응답을 대상으로 오프라인 사전 대입을 시도할 수 있다.

선지별 해설

① O — 전통적인 Kerberos 설명에서 인증 서버는 각 사용자와 공유하는 패스워드 기반의 장기 비밀정보를 중앙 데이터베이스에서 관리한다. 이를 이용해 사용자의 초기 인증을 처리한다.
② O — 최초 인증 후 티켓 발급 티켓(TGT)을 받은 사용자는 패스워드를 서비스마다 다시 제출하지 않고 여러 서비스의 서비스 티켓을 발급받을 수 있다. 따라서 동일한 계정 정보로 여러 서비스를 이용하는 통합 인증이 가능하다.
③ X — 틀린 표현은 '패스워드 사전공격에 강하다'이다. 사용자의 키가 패스워드에서 유도되므로 패스워드가 약하면 공격자가 획득한 인증 응답을 후보 패스워드로 복호화해 보는 오프라인 사전공격에 취약할 수 있다. 올바르게는 'Kerberos는 약한 패스워드를 사용할 경우 패스워드 사전공격에 취약할 수 있다'이다.
④ O — Kerberos는 대칭키 암호 방식으로 티켓과 인증 정보를 보호하고, 인증된 당사자에게 세션키를 전달하므로 인증 과정에서 비밀정보가 평문으로 노출되는 것을 막는다.

오답 포인트

패스워드 자체를 네트워크로 직접 전송하지 않는다는 사실을 '패스워드 추측 공격에도 강하다'고 확대 해석하기 쉽다. ③의 함정은 전송 중 패스워드 노출 방지와 약한 패스워드에 대한 오프라인 사전 대입 가능성을 혼동하게 하는 데 있다.

NoteBase

다시 나오면 이렇게 판단

Kerberos 선지는 ‘KDC 중심 구조’, ‘티켓을 이용한 SSO’, ‘대칭키 기반’이면 기본 특징으로 판단한다. 반면 ‘패스워드 사전공격에 강하다’처럼 약한 패스워드 문제까지 해결한다고 단정하면 틀린 설명으로 판단한다.

암기 포인트

Kerberos는 KDC·티켓·대칭키·SSO가 핵심이며, 약한 패스워드의 사전공격 위험은 남는다.

NoteBase

문 18. 암호 해독자가 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법이며, 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 공격방법은 무엇인가?

① KPA

② CPA

③ COA

④ CCA

정답 1번

출제 포인트

평문과 암호문의 확보 방식에 따라 KPA, CPA, COA, CCA를 구별하는 문제이다. 일정량의 평문과 그에 대응하는 암호문을 이미 알고 이를 이용해 키나 다른 평문을 추정하는 공격은 알려진 평문 공격(KPA)이다.

핵심 개념

KPA(Known Plaintext Attack): 공격자가 평문과 그에 대응하는 암호문의 쌍을 알고 분석하는 알려진 평문 공격이다.
CPA(Chosen Plaintext Attack): 공격자가 원하는 평문을 선택하고 그 암호문을 얻어 분석하는 선택 평문 공격이다.
COA(Ciphertext-Only Attack): 공격자가 암호문만 가진 상태에서 평문이나 키를 추정하는 암호문 단독 공격이다.
CCA(Chosen Ciphertext Attack): 공격자가 선택한 암호문에 대응하는 평문을 얻어 분석하는 선택 암호문 공격이다.

선지별 해설

① O — KPA는 평문 P와 그에 대응하는 암호문 C를 알고 둘의 관계에서 키 K나 다른 평문을 추정하는 공격이므로 지문의 조건과 일치한다.
② X — CPA라는 공격 유형 지정이 틀렸다. CPA는 공격자가 분석할 평문을 직접 선택하고 그 암호문을 얻는 공격이며, 지문처럼 이미 알려진 평문·암호문 쌍을 이용하는 공격은 KPA이다.
③ X — COA라는 공격 유형 지정이 틀렸다. COA는 평문을 알지 못하고 암호문만으로 분석하는 공격이며, 평문 P와 암호문 C를 함께 아는 경우는 KPA이다.
④ X — CCA라는 공격 유형 지정이 틀렸다. CCA는 공격자가 암호문을 선택하고 그에 대응하는 평문을 얻어 분석하는 공격이며, 알려진 평문·암호문 쌍을 이용하는 경우는 KPA이다.

NoteBase

오답 포인트

CPA와 KPA는 모두 평문과 암호문의 관계를 이용하지만, 평문을 공격자가 임의로 선택할 수 있으면 CPA이고 이미 확보된 대응 쌍을 알고만 있으면 KPA이다. 지문의 '일정량의 평문에 대응하는 암호문을 알고 있는 상태'가 KPA를 가리키는 결정적 표현이다.

다시 나오면 이렇게 판단

공격자에게 주어진 정보를 기준으로 판단한다. 암호문만 있으면 COA, 알려진 평문·암호문 쌍이 있으면 KPA, 평문을 선택해 암호문을 얻으면 CPA, 암호문을 선택해 평문을 얻으면 CCA이다.

암기 포인트

Known은 알려진 평문 쌍, Chosen은 공격자가 입력을 선택한다. P를 선택하면 CPA, C를 선택하면 CCA이다.

NoteBase

문 19. 다음 중 위험(Risk)에 대한 정의 및 구성요소에 대한 내용으로 가장 옳지 않은 것은?

① 위험이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 말한다.

② 위험은 자산, 위협, 취약성으로 표현한다.

③ 위험은 손실을 끼치는 사건 발생 가능성에는 비례하나 발생 손실의 정도에 반비례한다.

④ 위협 주체가 취약점을 활용할 수 있는 가능성과 그와 관련된 비즈니스 영향을 가리킨다.

정답 3번

출제 포인트

위험의 의미와 위험을 결정하는 자산·위협·취약성, 사건 발생 가능성·손실 영향의 관계를 묻는 문제이다.

핵심 개념

위험은 위협이 자산의 취약성을 이용하여 손실이나 부정적 영향을 일으킬 가능성과 그 영향의 크기를 함께 고려한 개념이다. 일반적으로 사건 발생 가능성이 높을수록, 발생했을 때의 손실이 클수록 위험도 커진다. 자산은 보호할 가치가 있는 대상, 위협은 자산에 손해를 일으킬 수 있는 원인, 취약성은 위협에 악용될 수 있는 약점이다.

선지별 해설

① O — 위험은 원하지 않는 사건이 발생하여 손실이나 부정적 영향을 초래할 가능성을 뜻하므로 옳다.
② O — 정보보안 위험은 보호 대상인 자산, 자산에 손해를 줄 수 있는 위협, 위협이 악용하는 취약성의 관계로 표현할 수 있으므로 옳다.
③ X — 틀린 부분은 '발생 손실의 정도에 반비례한다'이다. 실제로 위험은 사건 발생 가능성뿐 아니라 손실 또는 영향의 정도에도 비례하므로, 손실 규모가 커질수록 위험도 커진다.
④ O — 위협 주체가 취약점을 이용할 가능성과 그 결과 발생하는 비즈니스 영향을 함께 고려한다는 설명이므로 옳다.

오답 포인트

③은 발생 가능성과 손실 정도의 방향을 다르게 써서 혼동을 유도한다. 손실이 클수록 위험이 작아지는 것이 아니라, 발생 가능성과 손실 영향 중 어느 하나가 커져도 위험은 커진다.

다시 나오면 이렇게 판단

위험 관련 선지는 '발생 가능성'과 '영향 또는 손실의 크기'가 모두 위험과 같은 방향으로 움직이는지 확인한다. 자산·위협·취약성의 관계를 묻는 경우에는 보호 대상, 손해 원인, 악용 가능한 약점으로 각각 대응한다.

암기 포인트

위험은 가능성과 영향이 클수록 커지며, 위협은 취약성을 이용해 자산에 손실을 준다.

NoteBase

문 20. 다음 중 위험분석 방법에 대한 설명으로 가장 옳지 않은 것은?

① 과거자료 분석법 : 과거 자료가 많을수록 분석의 정확도가 높아진다. 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며 과거의 사건 중 발생 빈도가 낮은 자료에 대해서는 적용이 어렵다.

② 확률분포법 : 미지의 사건을 추정하는데 사용되는 방법이다. 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다. (정확성이 낮다)

③ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.

④ 순위 결정법 : 시스템에 관한 전문적인 지식을 갖춘 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.

정답 4번

출제 포인트

정량적·정성적 위험분석 기법의 정의를 구별하고, 전문가 집단의 판단을 활용하는 델파이법과 위험 항목의 우선순위를 정하는 순위 결정법을 구분하는 문제이다.

핵심 개념

과거자료 분석법은 과거의 위험 발생 기록을 바탕으로 미래 위험을 추정하는 정량적 기법이다.
확률분포법은 자료의 확률적 편차를 이용해 미지의 사건에 대한 최저·보통·최고 수준의 위험을 추정하는 정량적 기법이다.
시나리오법은 일정한 조건과 상황을 가정하고 발생 가능한 결과를 추론하는 정성적 기법이다.
델파이법은 전문가 집단의 지식과 판단을 모아 위험을 분석·평가하는 정성적 기법이고, 순위 결정법은 비교우위 순위결정표 등을 이용해 위험 항목의 서술적 우선순위를 정하는 정성적 기법이다.

선지별 해설

① O — 과거자료 분석법은 축적된 사례가 많을수록 발생 빈도와 손실 규모를 더 신뢰성 있게 추정할 수 있다. 과거의 경향이 미래에도 이어진다는 전제가 필요하므로 발생 빈도가 낮거나 과거 사례가 부족한 위험에는 적용하기 어렵다.
② O — 확률분포법은 미지의 사건을 확률적·통계적 편차로 추정하여 최저·보통·최고 위험 수준을 예측한다. 추정에 의존하므로 정확성이 낮을 수 있다는 설명도 이 기법의 한계에 해당한다.
③ O — 시나리오법은 사건이 예상대로만 전개되지 않을 수 있음을 전제로 일정한 조건에서 가능한 위험 결과를 추론하는 방법이다.
④ X — 틀린 표현은 '순위 결정법'이다. 전문가 집단을 구성해 전문지식과 판단을 모아 위협과 취약성을 분석·평가하는 설명은 델파이법에 해당한다. 순위 결정법은 위험 항목을 서로 비교하여 순위결정표 등에 서술적 우선순위를 정하는 방법이다.

NoteBase

오답 포인트

④는 전문가가 위험을 평가한다는 점 때문에 순위 결정법처럼 보이게 만든 선지이다. 그러나 전문가 집단의 지식과 판단을 모으는 것은 델파이법이고, 위험 항목 자체를 비교하여 우선순위를 매기는 것이 순위 결정법이다.

다시 나오면 이렇게 판단

'과거 기록'이면 과거자료 분석법, '최저·보통·최고의 확률적 추정'이면 확률분포법, '가정한 상황의 가능한 결과'이면 시나리오법, '전문가 집단의 판단'이면 델파이법, '위험 항목의 비교와 우선순위'이면 순위 결정법으로 판별한다.

암기 포인트

전문가 판단은 델파이, 위험 순위는 순위 결정이다.

NoteBase