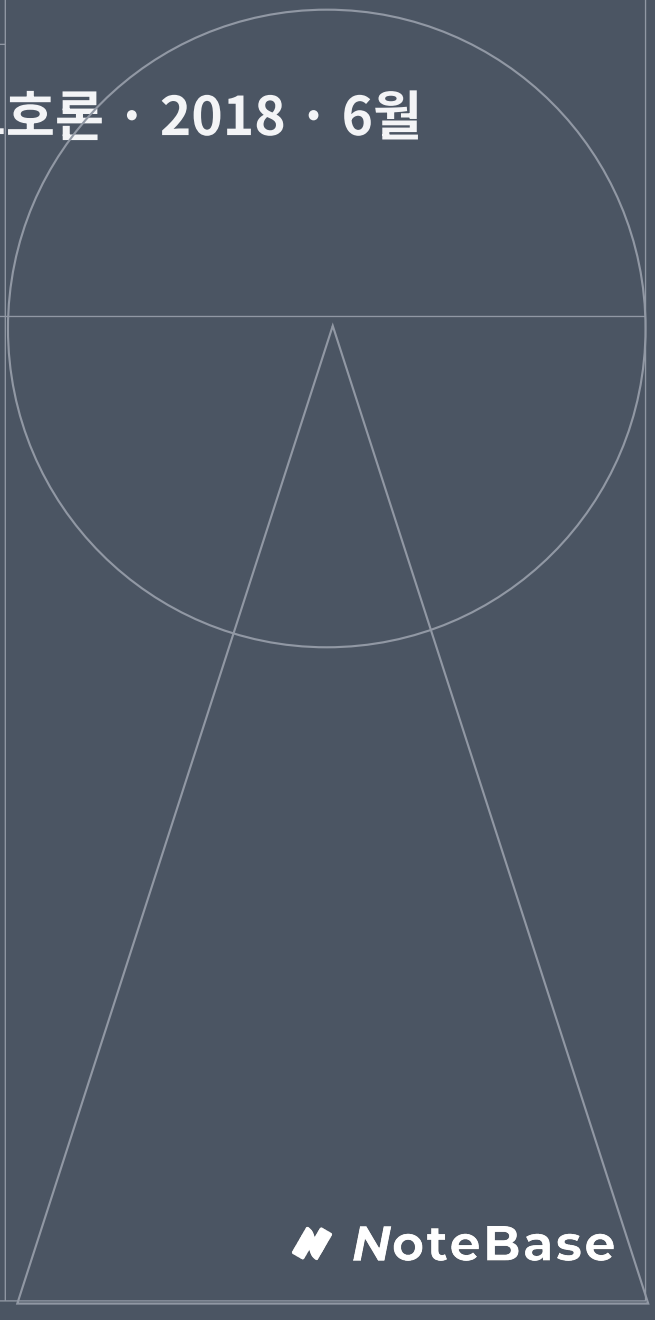
기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2018 · 6월



NoteBase

기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2018 · 6월

공무원/서울시/7급 · 정보보호론 · 2018 · 6월

문 1. 해시 알고리즘의 특징에 대한 설명으로 가장 옳은 것은?

① 해시 값이 같으면서 입력 값이 서로 다른 충돌 쌍을 찾는 것은 계산상 불가능하다.

② 고정길이의 입력 메시지를 임의 길이의 출력 값으로 압축시킨 함수이다.

③ 주어진 해시 값 y에 대해서 hash(x)=y 식을 만족하는 x를 찾는 것이 계산적으로 가능하다.

④ 메시지의 거대화 방지 및 데이터의 은닉에 사용된다.

정답 1번

출제 포인트

이 문제는 해시 함수의 기본 성질인 충돌 저항성, 역상 저항성, 그리고 입력·출력 길이 관계를 구별하는 문제이다.

핵심 개념

충돌 저항성: 서로 다른 두 입력이 같은 해시값을 갖는 쌍을 찾기 어렵다는 성질이다. 키워드는 '서로 다른 두 입력'이다.
역상 저항성: 주어진 해시값만 보고 그 값을 만드는 입력을 찾기 어렵다는 성질이다. 키워드는 '출력에서 입력 역추적'이다.
해시 함수의 길이 특성: 입력은 보통 임의 길이이고 출력은 고정 길이이다. 키워드는 '임의 길이 입력, 고정 길이 출력'이다.

선지별 해설

① O: 충돌 쌍을 찾기 어렵다는 설명은 충돌 저항성에 해당한다. 암호학적 해시 함수는 서로 다른 입력 $x \neq x'$에 대해 같은 해시값이 나오도록 만드는 쌍을 계산적으로 찾기 어렵게 설계된다.
② X: 틀린 부분은 '고정길이의 입력 메시지'와 '임의 길이의 출력 값'이다. 실제로는 임의 길이 입력을 받아 고정 길이 해시값을 출력한다.
③ X: 틀린 부분은 '계산적으로 가능하다'이다. 실제로는 주어진 해시값 y에 대해 $hash(x) = y$를 만족하는 입력 x를 찾기 어렵다는 역상 저항성이 요구된다.
④ X: 틀린 부분은 '데이터의 은닉에 사용된다'이다. 해시는 원문을 숨기는 기법이 아니라 무결성 검증, 전자서명, 비밀번호 검증 등에 사용된다. 또한 정확한 설명은 임의 길이 메시지를 고정 길이 요약값으로 변환한다는 것이지, 메시지를 은닉한다는 것이 아니다.

NoteBase

오답 포인트

②는 입력과 출력의 길이 방향을 뒤집어 놓았고, ③은 역상 저항성의 의미를 정반대로 적었다. ④는 해시를 암호화와 혼동하면 쉽게 고르게 되는 함정이다.

다시 나오면 이렇게 판단

해시 선지는 먼저 '서로 다른 두 입력을 찾는가'이면 충돌 저항성, '출력에서 입력을 찾는가'이면 역상 저항성으로 분류한다. 길이 표현은 반드시 '임의 길이 입력, 고정 길이 출력'인지 확인하면 된다.

암기 포인트

해시는 임의 길이 입력을 고정 길이로 요약하며, 계산적으로 찾기 어려운 것은 충돌과 역상이다.

NoteBase

문 2. 소프트웨어 취약점 공격에 해당하지 않는 것은?

① 버퍼 오버플로우 공격

② 힙 버퍼 오버플로우 공격

③ 크로스 사이트 스크립팅 공격

④ 웹 세션 하이재킹

정답 4번

출제 포인트

이 문제는 메모리·입력 처리 취약점을 직접 악용하는 공격과 세션 탈취 공격을 구분할 수 있는지를 묻는다.

핵심 개념

버퍼 오버플로우는 버퍼 경계를 넘겨 메모리를 덮어쓰는 구현 취약점 공격이다.
힙 버퍼 오버플로우는 힙 영역에서 발생하는 버퍼 오버플로우이다.
크로스 사이트 스크립팅은 검증·인코딩이 미흡한 웹 애플리케이션에 스크립트를 주입하는 취약점 공격이다.
웹 세션 하이재킹은 세션 ID를 탈취하거나 가로채 인증된 사용자의 세션을 빼앗는 공격이다.

선지별 해설

1번 X: 버퍼 오버플로우 공격은 배열이나 버퍼의 경계 검사 실패를 이용해 인접 메모리를 덮어쓰는 전형적인 소프트웨어 취약점 공격이다. 따라서 발문이 요구하는 '해당하지 않는 것'이 아니다.
2번 X: 힙 버퍼 오버플로우 공격은 힙 메모리 관리 취약점을 이용해 버퍼 경계를 넘는 쓰기·읽기를 유발하는 메모리 손상 공격이므로, 역시 소프트웨어 취약점 공격에 해당한다. 따라서 정답이 아니다.
3번 X: 크로스 사이트 스크립팅 공격은 입력값 검증과 출력 인코딩 미흡을 악용해 악성 스크립트를 삽입하는 웹 애플리케이션 취약점 공격으로, 웹 공격인 동시에 소프트웨어 취약점 공격에 해당한다. 따라서 정답이 아니다.
4번 O: 웹 세션 하이재킹은 인증 후 생성된 세션 식별자를 탈취하거나 가로채 사용자의 권한을 빼앗는 공격이다. 다른 세 선지가 코드·메모리·입력 처리의 구현 취약점 자체를 직접 악용하는 반면, 세션 하이재킹의 핵심은 세션 ID 탈취와 세션 관리 단계에 있다. 그러므로 구현 취약점을 직접 노리는 소프트웨어 취약점 공격에 해당하지 않는 선택지이며, 이것이 정답이다.

오답 포인트

3번의 XSS도 웹에서 일어나므로 4번의 세션 하이재킹과 같은 부류로 묶기 쉽다. 그러나 XSS는 입력 검증·출력 인코딩 미흡이라는 소프트웨어 취약점을 직접 찌르는 공격이고, 세션 하이재킹은 탈취된 세션 사용 자체가 핵심이라는 점이 다르다.

NoteBase

다시 나오면 이렇게 판단

공격 대상이 프로그램의 메모리 처리, 입력 검증, 출력 인코딩 같은 구현 취약점 자체인지 먼저 본다. 그 다음 핵심이 인증 이후의 세션 ID 탈취인지 확인하면 세션 하이재킹을 다른 취약점 공격과 구분할 수 있다.

암기 포인트

오버플로우·XSS는 구현 취약점 공격, 세션 하이재킹은 세션 탈취 공격이다.

NoteBase

문 3. 메시지 송수신 상황에서 <보기>의 조치를 취했을 경우에 지켜질 수 있는 정보보호 서비스로 옳은 것끼리 짝지어진 것은?

<보기>
송신자 앨리스는 밥에게 보낼 메시지를 먼저 자신의(앨리스) 개인키로 암호화하였다. 이렇게 암호화된 암호문을 수신자인 밥의 공개키로 한 번 더 암호화를 한 뒤에 수신자인 밥에게 보냈다.

① 무결성, 인증, 부인방지
② 기밀성, 무결성, 부인방지
③ 기밀성, 무결성, 인증, 부인방지
④ 무결성, 인증, 가용성, 부인방지

정답 3번

출제 포인트

송신자가 자신의 개인키로 먼저 처리하고 수신자의 공개키로 다시 암호화한 경우, 어떤 정보보호 서비스가 함께 확보되는지를 묻는 문제이다.

사례 정리

핵심 사실 1: 앨리스는 메시지에 자신의 개인키를 먼저 적용하였다.
핵심 사실 2: 그 결과물에 밥의 공개키를 다시 적용하여 밥에게 전송하였다.
판단에 중요한 조건: 밥은 자신의 개인키로 외부 암호를 풀고, 앨리스의 공개키로 송신자와 변조 여부를 확인할 수 있다.

핵심 개념

전자서명 성격의 개인키 처리 = 송신자 본인만 만들 수 있는 값을 붙여 송신자 인증, 무결성, 부인방지를 제공하는 방식이다.
수신자 공개키 암호화 = 대응하는 개인키를 가진 수신자만 내용을 복호화할 수 있어 기밀성을 제공하는 방식이다.

적용 기준

이 사례에서는 '누가 읽을 수 있는가'와 '누가 보냈는가'를 나누어 본다. 밥의 공개키로 한 번 더 암호화했으므로 제3자는 내용을 읽을 수 없어 기밀성이 확보된다. 앨리스의 개인키를 먼저 적용했으므로 앨리스의 공개키로 송신자 확인과 변조 여부 검사가 가능해 무결성, 인증, 부인방지가 함께 성립한다.

NoteBase

선지별 해설

① X: 무결성, 인증, 부인방지는 맞지만 기밀성이 빠졌다. 밥의 공개키로 다시 암호화했으므로 올바르게는 '기밀성, 무결성, 인증, 부인방지'가 된다.
② X: 기밀성, 무결성, 부인방지는 포함되지만 인증이 빠졌다. 앨리스의 개인키를 사용한 부분은 수신자가 앨리스의 공개키로 확인할 수 있으므로 올바르게는 '기밀성, 무결성, 인증, 부인방지'가 된다.
③ O: 밥의 공개키 암호화는 기밀성을 주고, 앨리스의 개인키 적용은 인증, 무결성, 부인방지를 준다. 따라서 네 가지 서비스가 모두 성립한다.
④ X: 가용성은 시스템이나 서비스가 필요할 때 사용할 수 있는 성질로, 이 암호화 절차만으로 확보되지 않는다. 틀린 표현은 '가용성'이며 올바르게는 '기밀성'이 들어가야 하므로 '기밀성, 무결성, 인증, 부인방지'가 된다.

오답 포인트

개인키와 공개키의 역할을 뒤섞으면 인증과 기밀성 중 하나를 빠뜨리기 쉽다. 특히 ④처럼 암호화 절차와 무관한 가용성을 끼워 넣는 선택지가 대표적인 함정이다.

다시 나오면 이렇게 판단

송신자 개인키가 먼저 나오면 서명 계열로 보고 인증, 무결성, 부인방지를 떠올린다. 여기에 수신자 공개키 암호화가 추가되면 기밀성이 더해진다고 판단한다. 가용성은 별도의 시스템 운영 관점이므로 이런 암호 절차만으로는 성립하지 않는다.

암기 포인트

송신자 개인키는 서명, 수신자 공개키는 기밀성이라는 대응으로 기억하면 된다.

NoteBase

문 4. 공인인증서에 대한 설명으로 가장 옳은 것은?

① 공인인증서는 공개키와 소유자를 연결시켜주는 전자 문서로 오늘날 사용되는 대부분의 인증서는 X.509 인증서(버전3)를 표준으로 따른다.

② 공인인증서의 기본 영역은 버전, 일련번호, 서명 알고리즘, 발급자, 주체, 주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책 등을 포함하고 있다.

③ 누구나 사용자의 인증서를 획득하고, 공개키를 획득할 수 있으며 누구나 자유롭게 인증서를 수정/발급할 수 있다.

④ 인증서 폐기 목록은 보통 폐기된 인증서에 관한 정보만 유지하는데, 이를 나쁜 목록(bad-list) 방법이라고 한다. 나쁜 목록 방법은 좋은 목록(good-list) 방법보다 안전하지만 상대적으로 용량이 매우 크다.

정답 1번

출제 포인트

이 문제는 공개키 인증서의 역할, X.509 v3 인증서의 기본 필드와 확장 필드, 인증서 폐지 목록의 의미를 구별할 수 있는지를 묻는 문제이다.

핵심 개념

공개키 인증서는 공개키가 누구의 것인지를 인증기관의 서명으로 증명하는 전자문서이다.
X.509 v3의 기본 필드는 버전, 일련번호, 서명 알고리즘 식별자, 발급자, 유효기간, 주체, 주체 공개키 정보 등이고, 주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책 등은 확장 필드이다.
CRL은 폐지된 인증서만 모아 두는 bad-list 방식이고, good-list는 유효한 인증서만 허용하는 방식이라 더 안전하지만 관리 용량이 더 커진다.

선지별 해설

① O: 공개키 인증서는 공개키와 소유자 신원을 연결하는 전자문서이며, 실무에서는 X.509 v3 형식이 대표적인 인증서 표준으로 사용된다.
② X: 틀린 부분은 '주체키 식별자, 기관 정보 액세스, 키 사용 용도, 인증서 정책 등을 기본 영역에 포함한다'는 표현이다. 실제로는 이 항목들은 X.509 v3의 확장 필드이고, 기본 필드는 버전, 일련번호, 서명 알고리즘, 발급자, 유효기간, 주체, 주체 공개키 정보 등이다.
③ X: 틀린 부분은 '누구나 자유롭게 인증서를 수정/발급할 수 있다'는 표현이다. 실제로는 사용자의 인증서와 공개키는 배포되어 누구나 열람할 수 있지만, 인증서의 발급과 서명은 신뢰된 인증기관이 수행하므로 임의 수정이나 임의 발급은 할 수 없다.
④ X: 틀린 부분은 '나쁜 목록 방법이 좋은 목록 방법보다 안전하지만 용량이 매우 크다'는 표현이다. 실제로는 CRL은 폐지된 인증서만 관리하는 bad-list라 용량이 상대적으로 작지만, 누락이나 최신성 문제 때문에 good-list보다 안전성이 낮을 수 있다. good-list가 더 안전한 대신 관리 용량이 커진다.

NoteBase

오답 포인트

②는 기본 필드와 확장 필드를 섞어 놓은 선지이고, ③은 앞부분의 '공개키와 인증서는 공개 가능하다'는 사실 때문에 뒷부분의 '임의 수정/발급 가능'이라는 오류를 놓치기 쉽다. ④는 bad-list와 good-list의 안전성, 저장 용량의 방향을 서로 뒤집어 놓은 점이 함정이다.

다시 나오면 이렇게 판단

인증서 문제는 먼저 인증서의 역할이 신원과 공개키의 연결인지 확인하고, 다음으로 필드가 기본 항목인지 확장 항목인지 구분한다. 폐지 목록이 나오면 bad-list는 폐지된 것만 막는 방식이고 good-list는 허용할 것만 남기는 방식이라는 점을 기준으로 안전성과 용량의 방향을 판단한다.

암기 포인트

인증서는 신원과 공개키를 묶는 문서이고, X.509 v3의 SKI·AIA·Key Usage·Policy는 확장 필드이며, CRL은 작지만 덜 안전한 bad-list이다.

NoteBase

문 5. 보안 등급 평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)에 대한 설명으로 가장 옳은 것은?

① E1~E6까지 6등급으로 구분한다.

② 기밀성, 무결성, 가용성을 평가한다.

③ 유럽의 신뢰성 있는 컴퓨터 시스템 평가기준이다.

④ 각 클래스별로 기능 요구사항과 보증 요구사항을 정의·포함한다.

정답 4번

출제 포인트

이 문제는 TCSEC의 등급 체계와 평가 관점, 그리고 Common Criteria 및 ITSEC와의 차이를 구분하는 문제이다.

핵심 개념

TCSEC는 미국의 신뢰 컴퓨터 시스템 평가기준으로, 주로 기밀성 중심의 보안 요구사항과 보증 요구사항을 등급별로 제시한 기준이다.
Common Criteria는 EAL1부터 EAL7까지의 평가보증등급을 사용한다.
ITSEC는 유럽의 정보기술 보안 평가기준이다.

NoteBase

기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2018 · 6월

선지별 해설

① X
틀린 부분은 "E1~E6"이다.
TCSEC는 E1~E6이 아니라 D, C1, C2, B1, B2, B3, A1 등의 등급 체계를 사용한다.

② X
틀린 부분은 "기밀성, 무결성, 가용성"을 평가한다는 표현이다.
TCSEC는 CIA 전반을 균형 있게 평가하는 기준이 아니라, 다단계 보안과 접근통제 등 기밀성 중심의 평가기준이다.

③ X
틀린 부분은 "유럽의"이다.
TCSEC는 유럽 기준이 아니라 미국 국방부가 제시한 신뢰 컴퓨터 시스템 평가기준이다.
유럽의 평가기준은 ITSEC로 보는 것이 맞다.

④ O
TCSEC는 각 보안 등급 또는 클래스를 나누고, 각 클래스마다 기능 요구사항과 이를 얼마나 신뢰할 수 있는지에 관한 보증 요구사항을 포함한다.
따라서 4번의 설명이 가장 옳다.

오답 포인트

①은 EAL 등급 체계를 TCSEC에 섞어 놓은 함정이다. ②는 정보보호의 일반 목적(CIA)을 보안평가기준의 성격과 혼동하게 만든 표현이다. ③은 TCSEC와 ITSEC의 지역적 출처를 바꿔 놓은 함정이다.

다시 나오면 이렇게 판단

보안평가기준 문제는 먼저 기준의 출처와 등급 체계를 확인하면 된다. EAL이 보이면 Common Criteria, 유럽 기준이면 ITSEC, D·C·B·A1 체계이면 TCSEC로 판단한다.

암기 포인트

TCSEC는 미국·기밀성 중심·D/C/B/A1, CC는 EAL, ITSEC는 유럽이다.

NoteBase

문 6. <보기>의 패킷 로그가 검출된 공격은?

<보기>
Source: 203.211.11.11
Destination: 203.211.11.11
Protocol: 6
Src Port: 21845
DST Port: 21845

① Teardrop
② Land attack
③ Ping of Death
④ SYN flooding

정답 2번

출제 포인트

이 문제는 패킷 로그에서 출발지 IP와 목적지 IP가 같고 출발지 포트와 목적지 포트도 같은 점을 보고 Land attack을 식별할 수 있는지를 묻는다.

선지별 해설

1번 X: Teardrop은 IP 단편화 조각을 겹치게 보내 재조립 오류를 유발하는 공격이다. 제시된 로그에는 단편화 오프셋이나 조각 겹침 정보가 없으므로 Teardrop으로 볼 수 없다. 틀린 표현은 공격 유형 판단이며, 올바르게는 단편화 이상이 보일 때 Teardrop을 의심한다.
2번 O: Land attack은 출발지 IP와 목적지 IP가 같고 출발지 포트와 목적지 포트도 같은 위조 패킷을 보내 대상 시스템이 자기 자신에게 응답하게 만드는 공격이다. 로그의 Source와 Destination이 모두 203.211.11.11이고 Src Port와 DST Port도 모두 21845이므로 Land attack의 전형적 형태이다.
3번 X: Ping of Death는 비정상적으로 큰 ICMP Echo 패킷으로 시스템 오류를 유발하는 공격이다. 제시된 로그의 Protocol 값 6은 TCP를 뜻하므로 ICMP 기반인 Ping of Death와 맞지 않는다. 틀린 표현은 공격 유형 판단이며, 올바르게는 ICMP oversized ping일 때 Ping of Death를 판단한다.
4번 X: SYN flooding은 다수의 TCP SYN 패킷으로 반개방 연결을 과도하게 만들어 자원을 고갈시키는 공격이다. 단일 로그에서 핵심 단서는 같은 IP와 같은 포트의 자기지향 패킷이지 대량 SYN 자체가 아니다. 틀린 표현은 공격 유형 판단이며, 올바르게는 SYN flooding은 다수의 SYN 요청과 half-open connection 누적이 관찰될 때 판단한다.

NoteBase

오답 포인트

Protocol이 6이라는 이유만으로 TCP 기반 공격 전부를 SYN flooding으로 몰아가면 틀린다. 이 문제의 함정은 프로토콜 종류보다 Source=Destination, Src Port=DST Port라는 자기지향 동일값 패턴을 먼저 보아야 한다는 점이다.

다시 나오면 이렇게 판단

패킷 로그형 문제에서는 먼저 IP와 포트의 동일 여부를 확인하고, 그다음 프로토콜 번호를 본다. 출발지와 목적지가 모두 같고 포트까지 같으면 Land attack을 우선 판단하고, ICMP 대용량이면 Ping of Death, 단편화 이상이면 Teardrop, 대량 SYN 누적이면 SYN flooding으로 구분한다.

암기 포인트

Land attack은 같은 IP, 같은 포트로 자기 자신을 향하게 만드는 공격이다.

NoteBase

문 7. 유럽의 정보보호 전문기관인 ENISA(European Network and Information Society Agency)에서 분류한 SNS 관련 보안 위협 중 <보기>에서 설명하는 것으로 가장 옳은 것은?

<보기>
• SNS를 이용한 스팸 증가
• 크로스 사이트 스크립팅 및 웜·바이러스 등에 대한 취약성 증가
• 다양하게 통합되는 SNS 포털들이 정보수집기로 이용되어 보안 취약성이 증가

① 프라이버시 보안 위협
② 네트워크 상의 보안 위협
③ ID 관련 보안 위협
④ 사회적 위협

정답 2번

출제 포인트

이 문제는 ENISA의 SNS 보안 위협 분류에서 스팸, XSS, 웜·바이러스, SNS 통합 포털을 어느 범주로 묶는지를 구별하는 문제이다.

핵심 개념

프라이버시 보안 위협은 개인정보 수집·연계·삭제 곤란처럼 사생활 침해가 중심인 위협이다.
네트워크 상의 보안 위협은 스팸, XSS, 웜·바이러스, SNS aggregator처럼 기존 네트워크·정보보안 위협이 SNS 환경에서 변형되어 나타나는 위협이다.
ID 관련 보안 위협은 피싱, 계정 침해, 프로필 도용처럼 신원과 인증정보를 노리는 위협이다.
사회적 위협은 스토킹, 괴롭힘, 기업 스파이 행위처럼 사회적 관계를 악용하는 위협이다.

NoteBase

선지별 해설

1번 X: 보기의 핵심은 SNS 스팸, 크로스 사이트 스크립팅, 웜·바이러스, SNS 포털 통합에 따른 취약성 증가이다. 이는 프라이버시 침해보다 기술적·네트워크적 공격 유형의 묶음이다. 틀린 표현은 "프라이버시 보안 위협"이다. 올바르게는 "네트워크 상의 보안 위협"이다.
2번 O: ENISA 문서에서 SN Spam, Cross Site Scripting, Viruses and Worms, SNS Aggregators는 "SNS variants of traditional network and information security threats"로 함께 분류된다. 보기의 세 항목이 이 범주를 그대로 설명하므로 맞다.
3번 X: ID 관련 보안 위협은 spear phishing, 정보유출을 노린 침투, 프로필 도용처럼 신원 사칭이나 인증정보 탈취가 중심이다. 보기에는 신원 도용보다 스팸과 악성코드, XSS, aggregator 취약성이 제시되어 있다. 틀린 표현은 "ID 관련 보안 위협"이다. 올바르게는 "네트워크 상의 보안 위협"이다.
4번 X: 사회적 위협은 stalking, bullying, corporate espionage처럼 사람 간 관계나 사회적 상호작용을 악용하는 유형이다. 보기는 사회적 괴롭힘이 아니라 기술적 취약점과 스팸 확산을 말한다. 틀린 표현은 "사회적 위협"이다. 올바르게는 "네트워크 상의 보안 위협"이다.

오답 포인트

SNS aggregator가 여러 계정의 정보를 모으므로 프라이버시 위협처럼 보이기 쉽다. 그러나 이 문항은 개별 항목의 부수 효과가 아니라 ENISA의 분류 이름을 묻는다. 스팸, XSS, 웜·바이러스가 함께 제시되면 기술적 네트워크 위협 묶음으로 판단하는 것이 맞다.

다시 나오면 이렇게 판단

선지나 보기에서 스팸, 악성코드, XSS, 포털 통합 취약점처럼 서비스 동작이나 계정·트래픽에 직접 영향을 주는 기술적 공격이 나오면 네트워크 상의 보안 위협으로 본다. 반대로 개인정보 노출이면 프라이버시, 도용·피싱이면 ID, 스토킹·괴롭힘이면 사회적 위협으로 구분한다.

암기 포인트

스팸·XSS·웜·Aggregator는 기술형이므로 네트워크, 피싱·도용은 ID, 스토킹·괴롭힘은 사회적 위협이다.

NoteBase

문 8. 정보보안의 위험 관리 과정에서 조직의 보안 요구사항에 대한 효과적인 식별 및 효율적인 위험의 감소를 실현하기 위해 세부적인 위험 분석 방법들이 존재한다. <보기>에서 설명하는 (가)에 해당하는 위험 분석 방법으로 가장 옳은 것은?

<보기>
(가)는 모든 시스템에 대하여 표준화된 보안 대책을 제시하며 체크리스트 형태로 보안 대책이 있는지 없는지를 판단하여 적용되어 있지 않은 보안대책을 적용하는 방법으로 수행하는 위험 분석 방법

① 비정형 접근법
② 복합 접근법
③ 상세위험 분석
④ 베이스라인 접근법

정답 4번

출제 포인트

이 문제는 위험 분석 방법 중 베이스라인 접근법의 정의와 다른 접근법과의 구별 기준을 묻는 문제이다.

핵심 개념

베이스라인 접근법은 모든 시스템에 공통으로 적용할 최소한의 표준 보안대책을 체크리스트 형태로 두고, 빠진 통제를 보완하는 방식이다.
상세위험 분석은 자산, 위협, 취약점을 개별적으로 식별하고 영향도와 발생 가능성을 따져 위험을 정밀 평가하는 방식이다.
비정형 접근법은 구조화된 기준표보다 전문가 경험과 직관에 크게 의존하는 방식이다.
복합 접근법은 베이스라인 같은 간이 기법과 상세위험 분석을 함께 사용하는 방식이다.

선지별 해설

① X: 비정형 접근법은 표준화된 체크리스트를 일괄 적용하는 방식이 아니라 전문가 판단과 경험에 의존하는 성격이 강하다. 틀린 부분은 '비정형 접근법'이라는 명칭이다. 올바르게는 베이스라인 접근법이다.
② X: 복합 접근법은 베이스라인 접근법과 상세위험 분석 등을 혼합해 사용하는 방식이다. 제시문처럼 모든 시스템에 공통 통제를 먼저 대입하는 단일 설명과는 다르다. 틀린 부분은 '복합 접근법'이라는 명칭이다. 올바르게는 베이스라인 접근법이다.
③ X: 상세위험 분석은 체크리스트 유무만 확인하는 수준이 아니라 자산 가치, 위협, 취약점, 손실 가능성을 세부적으로 분석한다. 틀린 부분은 '상세위험 분석'이라는 명칭이다. 올바르게는 베이스라인 접근법이다.
④ O: 베이스라인 접근법은 모든 시스템에 대해 표준화된 보안대책을 제시하고, 체크리스트로 적용 여부를 점검한 뒤 미적용 항목을 보완하는 방법이므로 제시문과 정확히 일치한다.

NoteBase

오답 포인트

출제자는 '위험 분석'이라는 말 때문에 많은 수험생이 ③ 상세위험 분석으로 끌리도록 만든다. 그러나 지문 핵심은 '모든 시스템', '표준화된 보안 대책', '체크리스트', '없는 대책을 적용'이라는 최소 보안수준 일괄 적용 구조에 있다.

다시 나오면 이렇게 판단

문장에 공통 기준, 표준 대책, 체크리스트, 최소 보안수준 같은 표현이 나오면 베이스라인 접근법을 먼저 떠올린다. 반대로 자산별 위협·취약점·영향도를 개별 산정하면 상세위험 분석으로 판단한다.

암기 포인트

베이스라인은 공통 체크리스트, 상세위험 분석은 개별 정밀분석이다.

NoteBase

문 9. 「개인정보 보호법 시행령」에서 규정한 개인정보 영향평가 대상에 대한 설명으로 가장 옳지 않은 것은?

① 5만 명 이상의 정보주체에 대한 민감 정보 또는 고유식별정보의 처리가 수반되는 개인정보파일

② 내부 또는 외부에서 구축·운용하는 다른 개인정보파일과 연계하려는 경우, 연계 결과 10만 명 이상의 정보주체에 관한 개인정보파일

③ 100만 명 이상의 정보주체에 관한 개인정보파일

④ 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우, 변경된 부분

정답 2번

쟁점

이 문제는 「개인정보 보호법 시행령」상 개인정보 영향평가 대상 기준을 구별하는 문제이다.
핵심은 정보주체 수 기준과 연계·변경의 요건을 정확히 나누는 것이다.

용어 풀이

개인정보 영향평가 = 공공기관이 대규모 개인정보파일을 구축·연계·변경할 때 개인정보 침해 위험을 사전에 분석하는 제도이다.

핵심 구분

원칙적으로 영향평가 대상은 5만 명 이상 민감정보·고유식별정보 파일, 50만 명 이상 연계 결과 파일, 100만 명 이상 일반 개인정보파일, 영향평가 후 운용체계 변경 파일로 나뉜다.
연계 기준은 10만 명이 아니라 50만 명이고, 운용체계 변경의 경우에는 변경된 부분만 영향평가 대상이 된다.

NoteBase

선지별 해설

① O
5만 명 이상의 정보주체에 대한 민감정보 또는 고유식별정보 처리가 수반되는 개인정보파일은 영향평가 대상에 해당한다.
민감정보·고유식별정보는 일반 개인정보파일보다 더 낮은 5만 명 기준을 적용한다.

② X
다른 개인정보파일과 연계하는 경우의 기준은 연계 결과 10만 명 이상이 아니라 50만 명 이상이다.
틀린 표현: "연계 결과 10만 명 이상의 정보주체"
올바른 표현: "연계 결과 50만 명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일"

③ O
100만 명 이상의 정보주체에 관한 개인정보파일은 영향평가 대상이다.
대규모 일반 개인정보파일의 기본 수치 기준이 100만 명이라는 점을 묻는 선지이다.

④ O
개인정보 검색체계 등 개인정보파일의 운용체계를 변경하는 경우에는 그 개인정보파일이 영향평가 대상이 된다.
이 경우 영향평가 범위는 변경된 부분으로 한정된다.

오답 포인트

연계 기준 수치를 10만 명으로 잘못 외우면 ②를 맞는 말처럼 보기 쉽다.
이 문제는 5만·50만·100만의 단계적 기준과 '변경된 부분만 평가'라는 예외를 함께 묻는 함정형 문항이다.

다시 나오면 이렇게 판단

개인정보 영향평가 대상은 먼저 민감정보·고유식별정보 여부를 보고 5만 명 기준을 확인한 뒤, 연계이면 50만 명, 일반 대규모 파일이면 100만 명, 이미 영향평가를 받은 시스템의 운용체계 변경이면 변경 부분만 평가 대상으로 잡으면 된다.

암기 포인트

영향평가 기준은 5만-50만-100만, 연계는 50만, 변경은 변경된 부분이다.

NoteBase

문 10. <보기>에서 설명하는 포렌식 (Forensic)의 기본 원칙에 해당하는 것으로 가장 옳은 것은?

<보기>
증거는 획득하고 난 뒤 '이송·분석·보관·법정 제출'이라는 일련의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다. 이를 만족하려면 증거를 전달하고 전달받는 데 관여한 담당자와 책임자를 명시해야 한다.

① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무결성의 원칙

정답 3번

출제 포인트

이 문제는 디지털 포렌식의 기본 원칙 중 연계 보관성의 원칙과 정당성, 재현성, 무결성을 구별할 수 있는지를 묻는 문제이다.

핵심 개념

연계 보관성의 원칙은 증거를 누가 언제 어떻게 인수·이송·보관·분석·제출했는지를 끊기지 않게 기록하여 추적 가능하게 하는 원칙이다.
정당성의 원칙은 증거 수집과 처리가 적법한 권한과 절차에 따라 이루어져야 한다는 원칙이다.
재현의 원칙은 같은 절차와 환경으로 다시 조사했을 때 같은 결과를 얻을 수 있어야 한다는 원칙이다.
무결성의 원칙은 수집된 증거가 변경·훼손되지 않은 원본 상태를 유지해야 한다는 원칙이다.

선지별 해설

① X: 틀린 부분은 이송·분석·보관·법정 제출 과정의 추적 가능성을 정당성의 원칙으로 본 점이다. 올바르게는 적법한 절차와 권한에 따라 증거를 취득·처리하는 것이 정당성의 원칙이다.
② X: 틀린 부분은 담당자와 책임자 명시, 전달 과정 추적을 재현의 원칙으로 본 점이다. 올바르게는 동일한 조건에서 같은 분석 결과를 다시 얻을 수 있어야 한다는 것이 재현의 원칙이다.
③ O: 보기의 핵심은 증거 획득 후 이송·분석·보관·법정 제출의 전 과정이 명확하고 추적 가능해야 하며, 전달자와 인수자를 특정해야 한다는 점이다. 이는 연계 보관성의 원칙에 해당한다.
④ X: 틀린 부분은 전달 과정의 기록과 책임자 명시를 무결성의 원칙으로 본 점이다. 올바르게는 증거 자체가 변조·훼손되지 않고 동일성을 유지하는 것이 무결성의 원칙이다.

NoteBase

오답 포인트

연계 보관성과 무결성은 모두 증거 보존과 관련되어 혼동되기 쉽다. 그러나 이 문항은 증거 내용의 변경 여부가 아니라 누가 전달하고 누가 인수했는지, 그 과정이 추적되는지를 묻고 있으므로 연계 보관성이 정답이다.

다시 나오면 이렇게 판단

선지에 이송, 인수인계, 담당자, 책임자, 추적 가능, 법정 제출 같은 표현이 나오면 먼저 연계 보관성을 떠올린다. 적법 절차는 정당성, 같은 결과의 반복 가능성은 재현, 변조 방지는 무결성으로 구분하면 된다.

암기 포인트

누가 넘겼는지는 연계 보관성이고, 안 바뀌었는지는 무결성이다.

NoteBase

문 11. <보기>에서 설명하고 있는 시스템 관련 보안으로 가장 옳은 것은?

<보기>
시스템은 계정과 패스워드 관리, 권한 관리, 접근 제어 등의 다양한 시스템 관련 보안 기능을 충분히 갖추고도 보안적인 문제가 발생할 수 있는데, 이는 컴퓨터의 하드웨어 또는 소프트웨어의 결함이나 운영체제 설계상의 허점으로 인한 것이다. 이러한 시스템 자체의 결함을 체계적으로 관리하는 통합적인 개념이다.

① 세션 관리
② 로그 관리
③ 취약점 관리
④ 패치 관리

정답 3번

출제 포인트

이 문제는 시스템의 하드웨어·소프트웨어·운영체제 결함을 통합적으로 다루는 보안 관리 개념이 무엇인지를 묻는 문제이다.

핵심 개념

세션 관리: 인증 이후 생성되는 세션의 유지·만료·탈취 방지를 다루는 관리이다. 키워드는 로그인 상태 통제이다.
로그 관리: 시스템과 사용자 행위를 기록·보관·분석하여 추적성과 이상 징후 탐지를 확보하는 관리이다. 키워드는 기록과 분석이다.
취약점 관리: 하드웨어, 소프트웨어, 운영체제의 결함이나 설계상 허점을 식별·평가·조치·추적하는 통합 관리이다. 키워드는 약점의 체계적 관리이다.
패치 관리: 알려진 취약점을 줄이기 위해 보안 업데이트나 수정 파일을 적용하는 관리이다. 키워드는 업데이트 적용이다.

NoteBase

선지별 해설

① X: '세션 관리'가 틀린 표현이다. 세션 관리는 사용자의 로그인 세션 생성, 유지, 종료, 세션 하이재킹 방지 등을 다루는 개념이다. 올바르게는 시스템 자체의 결함을 통합적으로 관리하는 '취약점 관리'여야 한다.
② X: '로그 관리'가 틀린 표현이다. 로그 관리는 이벤트와 접근 기록을 남기고 분석하는 활동으로, 사후 추적과 모니터링이 중심이다. 올바르게는 하드웨어·소프트웨어·운영체제의 허점을 체계적으로 관리하는 '취약점 관리'이다.
③ O: 보기의 핵심은 시스템 자체의 결함, 설계상 허점, 통합적 관리이다. 이는 취약점을 발견하고 평가하고 개선하는 전 과정을 포함하는 '취약점 관리'에 해당한다.
④ X: '패치 관리'가 틀린 표현이다. 패치 관리는 취약점 대응 방법 중 하나로서 수정 파일이나 업데이트를 적용하는 단계에 가깝다. 올바르게는 패치 적용까지 포괄하는 상위 개념인 '취약점 관리'이다.

오답 포인트

④ 패치 관리가 가장 강한 함정이다. 패치도 취약점을 줄이는 수단이므로 비슷해 보이지만, 패치 관리는 조치 방법의 한 부분이고 취약점 관리는 취약점 식별, 위험 평가, 우선순위 결정, 조치, 재점검까지 포함하는 더 넓은 개념이다.

다시 나오면 이렇게 판단

보기에서 '하드웨어·소프트웨어의 결함', '운영체제 설계상의 허점', '체계적·통합적 관리'가 함께 나오면 먼저 취약점 관리의 상위 개념 여부를 판단한다. 기록 중심이면 로그 관리, 로그인 상태 통제면 세션 관리, 업데이트 적용이면 패치 관리로 구분된다.

암기 포인트

결함 전체를 관리하면 취약점 관리이고, 수정 파일을 적용하면 패치 관리이다.

NoteBase

문 12. 악성코드에 대한 설명으로 가장 옳은 것은?

① 바이러스(virus)는 다른 프로그램을 감염시키지는 않지만 네트워크를 통해 자기 복제를 하며 전파된다.

② 트로이목마(Trojan horse)는 자기 복제 능력은 없으면서 정상적인 기능을 하는 프로그램 속에 숨어서 정보를 빼내거나 사용자 PC를 원격으로 제어할 수 있게 한다.

③ 애드웨어(adware)는 사용자의 브라우저를 원하지 않은 사이트로 이동시키면서 팝업창을 띄운다.

④ 드로퍼(dropper)는 사용자의 동의를 얻어 설치되었으나 프로그램 목적과 상관없이 시작 페이지 변경, 광고 노출, 과도한 리소스 사용으로 시스템 성능 저하를 가져오거나 존재하지 않는 위험을 가지고 사용자를 위협하여 결제를 유도한다.

정답 2번

출제 포인트

이 문제는 바이러스, 웜, 트로이목마, 애드웨어, 드로퍼의 핵심 차이를 구별할 수 있는지를 묻는다.

핵심 개념

바이러스는 다른 실행 파일이나 부트 영역에 기생해 감염 대상을 통해 퍼지는 악성코드이다.
웜은 숙주 파일 없이 네트워크를 통해 스스로 복제·전파되는 악성코드이다.
트로이목마는 정상 프로그램처럼 위장하지만 스스로 복제하지 않고, 내부에 악성 기능을 숨겨 정보 유출이나 원격 제어를 수행할 수 있다.
드로퍼는 다른 악성코드를 시스템에 설치시키는 전달용 악성코드이다.
애드웨어는 광고 표시를 주목적으로 하며, 공포를 조성해 결제를 유도하는 유형은 스케어웨어에 가깝다.

선지별 해설

1번 X: '다른 프로그램을 감염시키지는 않지만 네트워크를 통해 자기 복제를 하며 전파된다'는 설명은 바이러스가 아니라 웜의 특징이다. 바이러스는 다른 파일이나 프로그램에 기생해 감염을 확산한다.
2번 O: 트로이목마는 자기 복제 기능이 없고 정상 프로그램으로 가장해 숨어든 뒤 정보 탈취, 백도어 설치, 원격 제어 같은 악성 행위를 수행할 수 있다.
3번 X: '사용자의 브라우저를 원하지 않는 사이트로 이동시키면서 팝업창을 띄운다'는 표현은 브라우저 하이재커의 성격이 강하다. 애드웨어는 광고 노출이 핵심이므로 올바르게는 '광고를 표시하거나 광고성 프로그램을 설치해 수익을 노린다'라고 보는 편이 맞다.
4번 X: '사용자의 동의를 얻어 설치되었으나 ... 사용자를 위협하여 결제를 유도한다'는 설명은 드로퍼가 아니라 애드웨어나 스케어웨어의 특징에 가깝다. 드로퍼는 올바르게는 '내부에 포함한 다른 악성코드를 시스템에 설치하는 역할을 한다'라고 정리된다.

NoteBase

오답 포인트

1번은 바이러스와 웜의 차이를 뒤바꿔 놓은 함정이다. 3번과 4번은 광고 노출, 브라우저 변경, 결제 유도 같은 현상을 섞어 애드웨어, 브라우저 하이재커, 스케어웨어, 드로퍼를 혼동하게 만든다.

다시 나오면 이렇게 판단

먼저 자기 복제 여부를 본다. 다음으로 숙주 파일이 필요한지, 정상 프로그램으로 위장하는지, 다른 악성코드를 설치하는지가 각각 웜, 바이러스, 트로이목마, 드로퍼를 가르는 기준이 된다.

암기 포인트

바이러스는 감염형, 웜은 네트워크 자기복제형, 트로이목마는 위장형, 드로퍼는 설치형 악성코드이다.

NoteBase

문 13. <보기>에서 설명하는 정보 은닉 기술로 가장 옳은 것은?

<보기>
비밀 정보를 기존의 이미지 파일, 음악 파일, 동영상 파일 등에 숨겨서 전송하는 정보 은닉(information hiding) 기술의 일종이다. 이 기술은 저작권 보호보다는 정보를 은밀하게 전달하기 위한 목적이 크다.

① 워터마크(watermark)
② 스테가노그래피(steganography)
③ 스파이웨어(spyware)
④ 새도(shadow)

정답 2번

출제 포인트

이 문제는 정보 은닉 기법인 스테가노그래피와 워터마크, 스파이웨어 같은 인접 용어를 목적 기준으로 구별할 수 있는지를 묻는다.

핵심 개념

스테가노그래피는 비밀 정보를 이미지·음성·동영상 같은 매체 속에 숨겨 존재 자체를 감추며 전달하는 기술이다.
워터마크는 저작권 표시나 소유권 식별 정보를 콘텐츠에 삽입하는 기술이다.
스파이웨어는 사용자 정보를 몰래 수집하는 악성 소프트웨어이다.
섀도는 이 문맥의 정보 은닉 기술 명칭이 아니다.

선지별 해설

1번 X: 워터마크는 디지털 콘텐츠에 소유권 표시나 추적 정보를 넣어 저작권 보호와 출처 확인에 쓰이는 기술이다. 틀린 표현은 정보 은닉의 주목적처럼 본 부분이다. 올바르게는 저작권 보호와 식별이 중심 목적이다.
2번 O: 스테가노그래피는 비밀 정보를 다른 파일 안에 숨겨 전송하는 대표적인 정보 은닉 기술이다. 제시문의 '이미지 파일, 음악 파일, 동영상 파일 등에 숨겨서 전송'이라는 설명과 정확히 일치한다.
3번 X: 스파이웨어는 사용자의 활동이나 정보를 몰래 수집하는 악성코드이다. 틀린 표현은 정보 은닉 기술로 본 부분이다. 올바르게는 정보 은닉이 아니라 불법 수집과 감시를 수행하는 악성 소프트웨어이다.
4번 X: 섀도는 제시문의 설명에 대응하는 정보 은닉 기술 용어가 아니다. 틀린 표현은 기술 명칭으로 제시된 부분이다. 올바르게는 비밀 정보를 매체에 숨겨 전달하는 기술을 스테가노그래피라고 한다.

NoteBase

오답 포인트

워터마크도 데이터를 삽입한다는 점 때문에 스테가노그래피와 혼동하기 쉽다. 그러나 워터마크는 존재를 숨기는 것이 핵심이 아니라 저작권 표시와 추적이 핵심이라는 점에서 목적이 다르다.

다시 나오면 이렇게 판단

문장에서 비밀 정보를 파일 속에 숨겨 은밀히 전달한다고 하면 스테가노그래피를 먼저 떠올린다. 저작권 보호나 소유권 표시가 나오면 워터마크, 사용자 감시나 정보 탈취가 나오면 스파이웨어로 판단한다.

암기 포인트

스테가노그래피는 숨겨서 전달, 워터마크는 표시해서 보호, 스파이웨어는 몰래 수집이다.

NoteBase

문 14. 이메일 보안의 사실상의 표준으로 사용되고 있는 PGP (Pretty Good Privacy)에 대한 설명으로 가장 옳은 것은?

① RSA, DSA 등의 알고리즘을 사용한 디지털 서명을 통해 보낸 사람에 대한 인증과 부인방지 기능을 제공한다.

② AES, IDEA 등의 대칭키 암호화 알고리즘을 사용하여 이메일의 내용이 외부에 노출되는 것을 방지하는 기밀성은 제공하나, 이메일의 내용이 전송 중에 변경되지 않았다는 무결성은 보장하지 못한다.

③ PGP는 송신자의 대용량 이메일을 작은 메시지로 분할하지 않고 수신자에게 전송한다.

④ PGP는 이메일의 내용만 암호화하고, 첨부되는 문서는 암호화하지 못하여 다른 기법을 추가로 사용해야 한다.

정답 1번

출제 포인트

이 문제는 PGP가 제공하는 전자서명, 기밀성, 무결성, 압축, 분할, 첨부파일 보호 기능을 정확히 구별하는지 묻는 문제이다.

핵심 개념

전자서명: 송신자의 개인키로 서명하고 수신자가 공개키로 검증하여 송신자 인증과 부인방지를 제공하는 기능이다.
기밀성: 세션키와 대칭키 암호를 이용해 메일 내용을 암호화하여 제3자가 읽지 못하게 하는 기능이다.
무결성: 해시값과 서명 검증을 통해 전송 중 내용이 변조되지 않았는지 확인하는 기능이다.
압축·분할: PGP는 메시지를 압축해 효율을 높이고, 큰 메시지는 분할하여 전송한 뒤 수신 측에서 재조합할 수 있다.
첨부파일 보호: PGP는 본문만이 아니라 첨부파일까지 함께 암호화할 수 있다.

NoteBase

선지별 해설

① O
RSA, DSA 등의 공개키 알고리즘 기반 전자서명은 송신자 인증과 부인방지를 제공하므로 옳다. PGP의 핵심 기능 중 하나가 서명을 통한 인증이다.
② X
틀린 표현은 "무결성은 보장하지 못한다"이다. 올바르게는 PGP는 대칭키 암호로 기밀성을 제공할 뿐 아니라 해시와 전자서명을 통해 무결성도 확인할 수 있다.
③ X
틀린 표현은 "작은 메시지로 분할하지 않고"이다. 올바르게는 PGP는 대용량 메시지를 전송 환경에 맞게 분할하여 보낼 수 있고 수신 측에서 다시 결합할 수 있다.
④ X
틀린 표현은 "이메일의 내용만 암호화하고, 첨부되는 문서는 암호화하지 못한다"이다. 올바르게는 PGP는 본문과 첨부파일을 함께 암호화할 수 있으므로 별도 기법이 필수인 것은 아니다.

오답 포인트

②는 대칭키 암호를 쓰면 기밀성만 있고 무결성은 없다는 일반론을 PGP 전체 기능에 그대로 덧씌운 함정이다. ③은 PGP의 분할 기능을 부정했고, ④는 첨부파일 보호 범위를 본문으로만 축소해 수험생이 기능 범위를 좁게 기억했는지를 노린 선지이다.

다시 나오면 이렇게 판단

메일 보안 기술 문제가 나오면 먼저 서명 기능과 암호화 기능을 분리해 본다. 서명은 인증·부인방지·무결성 쪽이고, 암호화는 기밀성 쪽이다. 그다음 압축, 분할, 첨부파일 처리처럼 PGP의 부가 기능을 함께 확인하면 오답을 빠르게 걸러낼 수 있다.

암기 포인트

PGP는 서명으로 인증·부인방지·무결성을 확보하고, 암호화로 기밀성을 확보하며, 압축·분할·첨부파일 보호까지 지원한다.

NoteBase

문 15. <보기>에서 설명하는 시스템 공격에 해당하는 것으로 가장 옳은 것은?

<보기>
2014년 4월에 발견된 오픈 소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그로 전 세계 웹 사이트 가운데 2/3 정도가 사용하는 OpenSSL에서 발견된 치명적인 결함을 말한다. 이 공격은 주로 아이디, 비밀번호, 주민등록번호 등 개인정보와 SSL 서버 비밀키, 세션키, 쿠키 등을 탈취한다.

① 스쿨버스
② 루트킷
③ 하트블리드 공격
④ 무차별 공격

정답 3번

출제 포인트

이 문제는 OpenSSL의 heartbeat 취약점으로 서버 메모리가 유출되는 하트블리드 공격의 특징을 식별하는 문제이다.

핵심 개념

하트블리드 공격은 OpenSSL heartbeat 확장의 구현 오류를 악용하는 정보 유출 공격으로, heartbeat 요청의 페이로드 길이를 제대로 검증하지 않는 결함 때문에 서버 프로세스 메모리 일부를 과다 반환받아 읽어 온다.
스쿨버스는 보안 분야에서 널리 통용되는 표준 공격 명칭이 아니며, 보기가 설명하는 OpenSSL 메모리 누출 취약점과 무관한 오답 선지이다.
루트킷은 침입 후 존재를 숨기고 권한을 유지하기 위해 쓰이는 은닉성 악성 도구이다.
무차별 공격은 가능한 비밀번호나 키를 반복 대입하는 추측 공격이다.

NoteBase

선지별 해설

① X: 스쿨버스는 보안 분야에서 널리 통용되는 표준 공격 명칭이 아니며, 보기처럼 OpenSSL 버그로 서버 메모리에서 비밀키, 세션키, 쿠키를 읽어 내는 하트블리드 공격을 가리키는 용어가 아니다. 따라서 보기의 설명과 맞지 않는 오답이다.
② X: 루트킷은 시스템 내부에 숨어 관리자 권한 유지, 탐지 회피, 로그 은닉 등에 쓰인다. 보기의 핵심은 침투 후 은닉이 아니라 OpenSSL 취약점을 이용한 메모리 유출이다. 틀린 표현은 '루트킷'이고, 올바르게는 '은닉 도구가 아니라 취약점 기반 정보 유출 공격'이다.
③ O: 2014년 4월 공개된 OpenSSL의 치명적 결함으로 아이디, 비밀번호, 주민등록번호, 세션키, 쿠키, SSL 서버 비밀키 등이 노출될 수 있다는 설명은 하트블리드 공격의 전형적 특징과 일치한다. heartbeat 처리 오류로 메모리를 과다 반환받아 민감정보를 탈취한다.
④ X: 무차별 공격은 비밀번호나 암호키를 가능한 경우의 수대로 반복 대입하는 방식이다. 보기처럼 OpenSSL 구현 결함 하나로 정상 메모리 내용을 읽어 가는 공격이 아니다. 틀린 표현은 '무차별 공격'이고, 올바르게는 '무차별 대입이 아니라 Heartbleed 취약점 악용'이다.

오답 포인트

하트블리드는 '개인정보 탈취'만 보고 비밀번호 추측형 공격으로 오인하기 쉽다. 그러나 핵심 단서는 '2014년 4월', 'OpenSSL', '치명적 결함', '세션키·쿠키·서버 비밀키 유출'이며, 이는 추측이나 은닉이 아니라 메모리 누출 취약점이다.

다시 나오면 이렇게 판단

연도와 제품명, 유출 대상 정보를 먼저 묶어서 본다. OpenSSL에서 메모리 내용이 새어 나와 키와 쿠키가 노출된다고 하면 하트블리드로 판단하고, 비밀번호 반복 대입이면 무차별 공격, 침입 흔적 은닉이면 루트킷으로 구분한다.

암기 포인트

하트블리드는 OpenSSL heartbeat 오류로 메모리가 새고, 무차별 공격은 대입형이며, 루트킷은 은닉형이다.

NoteBase

문 16. 위협(Threats), 취약성(Vulnerability), 자산가치(Asset Value), 위험(Risk)의 상관관계 표현으로 가장 옳은 것은?

① 위험=자산가치/위협×취약성

② 위험=위협/취약성×자산가치

③ 위험=위협×취약성/자산가치

④ 위험=위협×취약성×자산가치

정답 4번

출제 포인트

이 문제는 정보보호 위험 산식에서 위험이 위협, 취약성, 자산가치의 곱으로 표현된다는 점을 묻는 문제이다.

조건 정리

주어진 요소: 위협, 취약성, 자산가치
구해야 할 값: 위험의 상관관계식
주의할 조건: 위험은 위협이 커질수록, 취약성이 높을수록, 자산가치가 클수록 함께 커지는 방향으로 이해한다.

사용할 공식

위험은 일반적으로 위협 × 취약성 × 자산가치로 표현한다.
이 공식을 쓰는 이유: 위협의 발생 가능성, 취약성의 노출 정도, 자산의 가치가 모두 커질수록 예상 손실과 위험 수준이 함께 커지기 때문이다.

계산 과정

1. 위험 식은 위협, 취약성, 자산가치가 증가하면 위험도 증가하는 구조여야 한다.
2. 따라서 세 요소를 모두 곱하는 형태가 기본 산식에 맞는다.
3. 보기에 있는 식들 중 이 조건을 만족하는 것은 ④뿐이다.

NoteBase

선지 판단

① X: 자산가치/위협 × 취약성은 위협이 커질수록 위험이 작아지는 구조이므로 위험 개념과 반대이다. 틀린 표현은 `/위협`이며, 올바르게는 `위협 × 취약성 × 자산가치`이다.
② X: 우변이 `위협/취약성 × 자산가치`로 취약성이 분모에 놓여, 취약성이 커질수록 위험이 작아지는 구조이므로 위험 개념과 반대이다. 틀린 표현은 `/취약성`이며, 올바르게는 `위협 × 취약성 × 자산가치`이다.
③ X: 우변이 `위협 × 취약성/자산가치`로 자산가치가 분모에 놓여, 자산가치가 커질수록 위험이 작아지는 구조이므로 위험 개념과 반대이다. 틀린 표현은 `/자산가치`이며, 올바르게는 `위협 × 취약성 × 자산가치`이다.
④ O: 위험을 `위협 × 취약성 × 자산가치`로 본 전형적인 정보보호 위험 산식과 일치하므로 옳다.

오답 포인트

보기 ①·②·③처럼 세 요소 중 하나라도 나눗셈으로 분모에 놓이면 그 요소가 커질수록 위험이 오히려 감소하는 식이 되어 위험 산식으로 부적절하다는 점을 놓치기 쉽다. 위험은 위협·취약성·자산가치를 모두 곱해야 하며, 어느 하나라도 분모에 들어가면 틀린 표현이 된다.

다시 나오면 이렇게 판단

위험 산식 문제는 먼저 각 요소가 커질 때 위험이 같은 방향으로 커지는지를 본다. 그다음 위협·취약성·자산가치 중 어느 하나라도 나눗셈으로 분모에 놓인 식은 오답으로 빠르게 걸러낼 수 있다.

암기 포인트

위험은 `위협 · 취약성 · 자산가치`의 곱으로 기억한다.

NoteBase

문 17. 컴퓨터 및 네트워크에서 서비스가 더 이상 진행되지 못하도록 하는 경우로써 <보기>에서 설명하고 있는 공격 방법으로 가장 옳은 것은?

<보기>
• 핑(ping)을 사용하여 현재 동작 중인 노드가 에코 메시지를 보내게 한다.
• 공격자가 발신주소를 공격하고자 하는 목적지의 IP주소로 위장하여 ICMP 에코 메시지를 요청하여 다량의 패킷이 목적지로 전송되도록 한다.
• 목표시스템은 과부하가 발생하여 정상적인 서비스가 불가능하게 된다.

① 스머프(smurf) 공격
② 중간자(man-in-the-middle) 공격
③ 포맷 스트링(format string) 공격
④ 프래글(fraggle) 공격

정답 1번

출제 포인트

이 문제는 ICMP echo request를 피해자 IP로 발신지 주소를 위조해 다수 호스트의 응답을 피해자에게 집중시키는 서비스 거부 공격을 식별할 수 있는지를 묻는 문제이다.

사례 정리

핵심 사실 1: 공격자는 ping을 사용해 ICMP 에코 메시지를 보낸다.
핵심 사실 2: 발신지 주소를 공격 대상의 IP 주소로 위장한다.
판단에 중요한 조건: 다수의 패킷 응답이 피해자에게 몰려 정상 서비스가 불가능해진다.

핵심 개념

스머프 공격은 ICMP echo request의 출발지 주소를 피해자 주소로 위조해 여러 시스템의 echo reply가 피해자에게 몰리게 만드는 반사형 서비스 거부 공격이다.
적용 요건은 ICMP 사용, 출발지 IP 스푸핑, 다수 응답의 집중이라는 세 요소이다.

적용 기준

이 사례에서는 공격자가 직접 대량 데이터를 보내는지보다 다수 시스템의 응답을 피해자에게 반사시켜 증폭시키는지를 본다. 핵심은 ping 기반 ICMP 요청과 피해자 IP 위조가 함께 나온다는 점이다.

NoteBase

선지별 해설

① O: 스머프 공격은 ICMP echo request를 보내면서 출발지 주소를 피해자 IP로 속여 다수 호스트의 echo reply가 피해자에게 집중되게 만든다. 제시문의 ping, ICMP, IP 위장, 과부하 유발이 모두 이에 해당한다.
② X: 중간자 공격은 통신 당사자 사이에 끼어들어 내용을 가로채거나 변조하는 공격이다. 이 선지의 틀린 표현은 '대량의 ICMP 응답으로 과부하를 유발하는 공격을 중간자 공격으로 본다'는 점이다. 올바르게는 '중간자 공격은 통신 경로를 장악해 도청·변조하는 공격'이다.
③ X: 포맷 스트링 공격은 프로그램이 사용자 입력을 서식 문자열로 잘못 처리할 때 메모리 내용을 읽거나 덮어쓰게 만드는 취약점 공격이다. 이 선지의 틀린 표현은 '네트워크 반사형 서비스 거부 공격을 포맷 스트링 공격으로 본다'는 점이다. 올바르게는 '포맷 스트링 공격은 응용프로그램의 문자열 처리 취약점을 악용하는 공격'이다.
④ X: 프래글 공격은 구조는 비슷하지만 ICMP가 아니라 UDP echo나 chargen 서비스를 이용해 반사 트래픽을 발생시키는 공격이다. 이 선지의 틀린 표현은 'ICMP ping 기반 반사 공격을 프래글 공격으로 본다'는 점이다. 올바르게는 '프래글 공격은 UDP 기반 반사형 서비스 거부 공격'이다.

오답 포인트

스머프와 프래글은 모두 반사형 서비스 거부 공격이라 혼동하기 쉽다. 이 문항의 함정은 '과부하' 자체가 아니라 어떤 프로토콜을 쓰는지를 묻는 데 있으며, ping과 ICMP가 보이면 프래글이 아니라 스머프로 판단해야 한다.

다시 나오면 이렇게 판단

서비스 거부 공격 유형 문제는 사용 프로토콜, 발신지 위조 여부, 응답이 누구에게 몰리는지를 먼저 본다. ICMP echo request와 피해자 IP 스푸핑이 함께 나오면 스머프, UDP echo·chargen이 나오면 프래글로 판단된다.

암기 포인트

ICMP 반사 증폭은 스머프이고, UDP echo·chargen 반사 증폭은 프래글이다.

NoteBase

문 18. <보기>에서 설명하고 있는 APT(Advanced Persistent Threats) 공격 기법으로 가장 옳은 것은?

<보기>
조사된 정보를 바탕으로 정보시스템, 웹 어플리케이션 등의 알려지지 않은 취약점 및 보안시스템에서 탐지되지 않는 악성코드 등을 감염시키는 것이다. 해당 취약점에 의해 악성코드에 감염된 PC는 동일한 취약점을 보유하고 있는 PC를 스캔하여 감염시킨다.

① 사전조사(Reconnaissance)
② 사회 공학(Social engineering)
③ 제로데이(Zero-day) 공격
④ 적응(Adaption)

정답 3번

출제 포인트

이 문제는 APT에서 사전조사, 사회공학, 제로데이 공격의 의미를 구분하고, 알려지지 않은 취약점 악용이라는 핵심 표현을 식별할 수 있는지를 묻는다.

핵심 개념

사전조사: 공격 전에 대상의 시스템, 조직, 인물 정보를 수집하는 단계이다. 키워드는 정보수집이다.
사회공학: 사람을 속여 계정, 파일, 권한을 넘기게 만드는 기법이다. 키워드는 인간 심리 악용이다.
제로데이 공격: 아직 공개되거나 패치되지 않은 취약점을 이용해 침투하는 공격이다. 키워드는 미공개 취약점 악용이다.
적응: 보안 환경 변화에 맞춰 공격 방식을 바꾸는 일반 표현일 수는 있으나, 알려지지 않은 취약점 악용을 직접 가리키는 표준 공격명은 아니다.

NoteBase

선지별 해설

1번 X: 사전조사는 공격 전에 표적의 네트워크, 시스템, 사용자 정보를 수집하는 단계이다. 제시문은 이미 조사된 정보를 바탕으로 알려지지 않은 취약점을 실제로 악용해 감염시키는 단계이므로 맞지 않는다. 틀린 표현은 사전조사이다. 올바르게는 미공개 취약점을 악용하는 제로데이 공격이다.
2번 X: 사회공학은 피싱, 사칭, 유인처럼 사람을 속여 정보를 빼내거나 실행을 유도하는 기법이다. 제시문은 사람을 속이는 과정이 아니라 시스템의 알려지지 않은 취약점과 미탐지 악성코드 감염을 설명하므로 맞지 않는다. 틀린 표현은 사회공학이다. 올바르게는 취약점 악용형 제로데이 공격이다.
3번 O: 제로데이 공격은 아직 알려지지 않았거나 패치되지 않은 취약점을 이용하므로 보안시스템에서 탐지되지 않을 가능성이 크다. 제시문의 알려지지 않은 취약점, 탐지되지 않는 악성코드, 동일 취약점을 가진 PC로의 확산이라는 설명과 가장 잘 맞는다.
4번 X: 적응은 공격자가 방어 환경에 맞춰 수법을 바꾸는 일반적 설명일 뿐, 제시문처럼 알려지지 않은 취약점을 이용해 감염을 시작하는 공격명을 뜻하지 않는다. 틀린 표현은 적응이다. 올바르게는 제로데이 취약점을 악용한 공격이다.

오답 포인트

제시문 첫머리의 조사된 정보를 보고 1번 사전조사로 끌려가기 쉽다. 그러나 정답을 가르는 표현은 조사된 정보를 바탕으로 이후 무엇을 했는지이며, 핵심은 알려지지 않은 취약점과 탐지되지 않는 악성코드 감염이다.

다시 나오면 이렇게 판단

선지를 볼 때 먼저 공격의 대상이 사람인지 시스템인지 구분한다. 다음으로 정보수집 단계인지 실제 취약점 악용 단계인지 나눈다. 마지막으로 알려지지 않은 취약점이나 미패치 취약점이라는 표현이 나오면 제로데이 공격을 우선 판단한다.

암기 포인트

사전조사는 수집, 사회공학은 사람 기만, 제로데이는 미공개 취약점 악용이다.

NoteBase

문 19. 전자정부 소프트웨어 개발 시 비밀번호를 설계할 때 고려해야 할 사항으로 가장 옳지 않은 것은?

① 패스워드를 설정할 때 한국인터넷진흥원 『암호이용안내서』의 패스워드 설정규칙을 적용해야 한다.

② 패스워드 저장 시 솔트(salt)가 적용된 안전한 해시함수를 사용해야 하며 해시함수 실행은 클라이언트에서 해야 한다.

③ 네트워크를 통해 패스워드를 전송하는 경우 반드시 패스워드를 암호화하거나 암호화된 통신 채널을 이용해야 한다.

④ 패스워드 재설정·변경 시 안전하게 변경할 수 있는 규칙을 정의해서 적용해야 한다.

정답 2번

출제 포인트

이 문제는 비밀번호 설계에서 설정 규칙, 저장 방식, 전송 보호, 재설정 절차를 구분하고 특히 저장용 해시의 적용 위치를 판단하는 문제이다.

핵심 개념

비밀번호 설정 규칙은 추측 저항성을 높이기 위한 길이·복잡도·금지어 기준이다.
비밀번호 저장 보호는 서버 측 저장값을 솔트와 함께 일방향 해시로 보관해 원문 노출을 막는 방식이다.
비밀번호 전송 보호는 평문 전송을 막기 위해 TLS 같은 암호화 통신 채널이나 별도 암호화를 적용하는 것이다.
비밀번호 재설정 보호는 본인 확인과 안전한 변경 절차를 통해 계정 탈취를 막는 규칙이다.

NoteBase

기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2018 · 6월

선지별 해설

① O
한국인터넷진흥원 안내서의 패스워드 설정규칙을 반영해 길이, 조합, 유추 가능한 문자열 제한 등을 두는 것은 전자정부 서비스의 기본적인 비밀번호 정책에 해당하므로 옳다.

② X
앞부분의 "솔트가 적용된 안전한 해시함수"는 맞는 설명이지만, "해시함수 실행은 클라이언트에서 해야 한다"는 표현이 틀렸다.
비밀번호 저장 보호의 핵심은 서버가 저장 시점에 비밀번호를 솔트와 함께 일방향 해시로 처리하는 것이다.
클라이언트 측 해시는 부가 보호수단이 될 수는 있어도 저장 보안의 기준 위치가 아니며, 그것만으로는 재전송 공격이나 서버 저장 보호를 대신하지 못한다.
틀린 표현 → "해시함수 실행은 클라이언트에서 해야 한다"
올바르게는 서버 측에서 솔트와 함께 해시하여 저장해야 한다.

③ O
네트워크로 비밀번호를 보낼 때 평문 전송을 막고 암호화된 통신 채널을 이용하는 것은 필수적인 보호 조치이므로 옳다.

④ O
비밀번호 재설정·변경 과정은 본인 확인, 일회성 토큰, 유효시간, 재사용 제한 등 안전한 절차를 정의해 적용해야 하므로 옳다.

오답 포인트

②는 "솔트 적용 해시"라는 맞는 표현 뒤에 "클라이언트에서 해시를 실행해야 한다"는 문장을 붙여 저장 보안과 전송 보안을 섞어 놓은 점이 함정이다. 수험생이 솔트와 해시라는 키워드만 보고 전체 문장을 맞는 것으로 오인하기 쉽다.

다시 나오면 이렇게 판단

비밀번호 문항은 설정, 저장, 전송, 재설정의 단계로 먼저 나눈 뒤 판단하면 된다. 저장을 묻으면 서버 측 솔트 해시를 떠올리고, 전송을 묻으면 암호화 채널 사용 여부를 확인하면 된다.

암기 포인트

비밀번호는 설정 규칙, 저장은 서버 솔트 해시, 전송은 암호화 채널, 변경은 안전한 재설정 절차로 정리된다.

NoteBase

문 20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 정한 정보보호 최고책임자의 업무로 규정되지 않은 것은?

① 침해사고 대응

② 침해사고 정보 전파

③ 정보보호 사전보안성 검토

④ 정보보호 취약점 분석 및 개선

정답 2번

쟁점

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보보호 최고책임자의 법정 업무 범위를 묻는 문제이다. 핵심은 법에 열거된 업무와 법에 없는 표현을 구별하는 것이다.

용어 풀이

정보보호 최고책임자 = 조직의 정보보호 업무를 총괄하는 책임자이다.

핵심 구분

법은 정보보호 최고책임자의 업무로 정보보호 취약점 분석·평가 및 개선, 침해사고의 예방 및 대응, 정보보호 사전 보안성 검토 등을 열거한다. 반면 침해사고 정보를 다른 곳에 전파하는 업무는 해당 조항의 직접적인 열거 사항이 아니다.

NoteBase

선지별 해설

① O
- 법정 업무에는 침해사고의 예방 및 대응이 포함되므로, 선택지의 '침해사고 대응'은 그 취지를 반영한 표현이다.

② X
- 법정 업무 조항은 침해사고의 예방 및 대응을 규정하지만, '침해사고 정보 전파' 자체를 정보보호 최고책임자의 업무로 직접 열거하지는 않는다.
- 틀린 표현: 침해사고 정보 전파
- 올바른 표현: 침해사고의 예방 및 대응

③ O
- 정보보호 사전 보안성 검토는 정보보호 최고책임자의 업무로 열거된 사항이다. 신규 시스템이나 서비스 도입 전에 보안 위험을 점검하는 업무에 해당한다.

④ O
- 정보보호 취약점 분석 및 개선은 법정 업무에 해당한다. 조문상으로는 취약점 분석·평가 및 개선으로 규정되어 있어 위험을 찾고 보완하는 업무를 뜻한다.

오답 포인트

②는 '침해사고 대응'과 비슷한 말처럼 보이지만, 법이 열거한 문구는 '예방 및 대응'이지 '정보 전파'가 아니다. 비슷한 보안 실무 용어를 법정 업무 명칭으로 착각하면 오답이 된다.

다시 나오면 이렇게 판단

법령형 문제에서 업무 범위를 묻는 경우에는 실무상 관련 있는지보다 조문이 어떤 행위를 직접 열거하는지를 먼저 본다. 비슷한 표현이 보여도 조문 문구와 일치하는지로 최종 판단한다.

암기 포인트

CISO 업무는 취약점 분석·개선, 침해사고 예방·대응, 사전 보안성 검토이고, 정보 전파는 직접 열거 사항이 아니다.

NoteBase