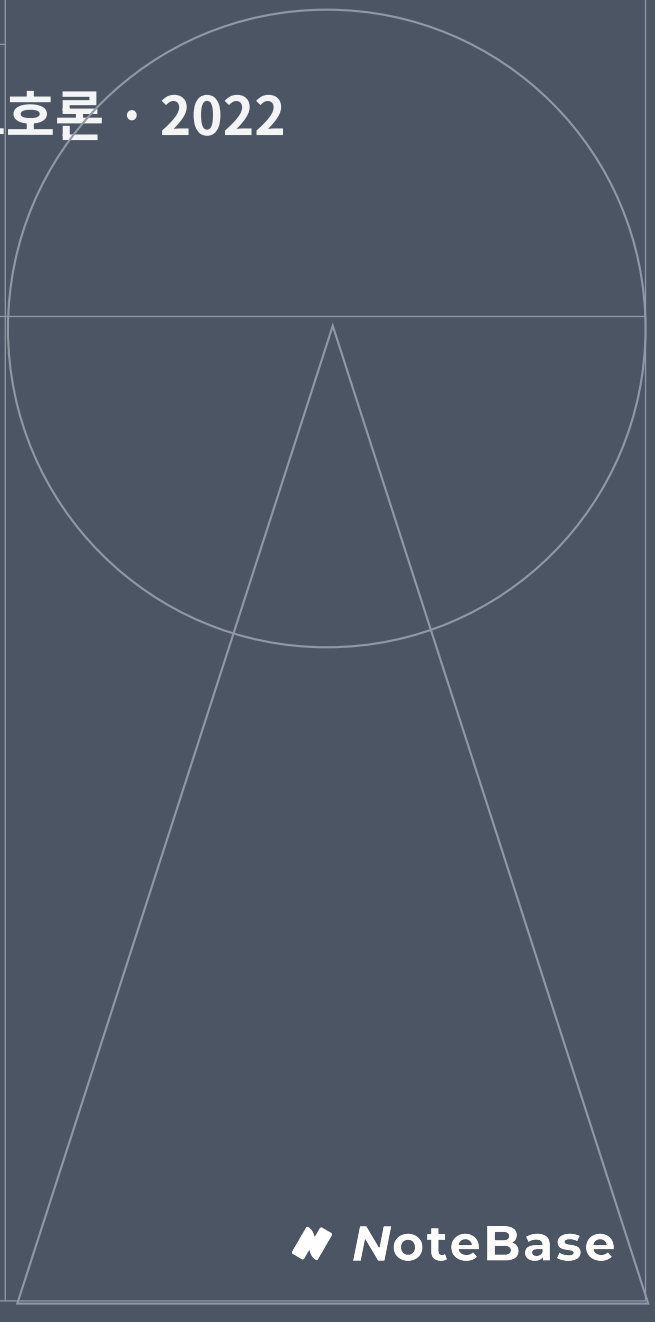
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2022



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2022

공무원/국회직/9급 · 정보보호론 · 2022

1. **방화벽의 기능으로 옳지 않은 것은?**

   ① 접근제어
   ② 로깅 및 감사 추적
   ③ 인증
   ④ 암호화
   ⑤ 시그니처 기반의 침입 탐지

정답 5번

출제 포인트

방화벽의 기본 기능과 침입 탐지 시스템(IDS)의 탐지 기능을 구분하는 문제이다.

핵심 개념

방화벽: 내부망과 외부망 사이의 통신을 보안 정책에 따라 허용하거나 차단하는 보안 장치이다. 접근제어, 사용자·접속 인증, 로그 기록과 감사 추적, VPN 연계에 의한 통신 암호화 등을 수행할 수 있다.
침입 탐지 시스템(IDS): 네트워크나 시스템의 활동을 분석하여 침입 징후를 발견하고 경보하는 시스템이다. 시그니처 기반 탐지는 알려진 공격 패턴과 일치하는지를 검사하는 대표적인 IDS 탐지 방식이다.
결정적 구분: 방화벽은 정책에 따라 통신을 통제하고, IDS는 공격의 징후를 탐지한다.

선지별 해설

① O — 접근제어는 출발지·목적지 주소, 포트, 프로토콜 등의 정책에 따라 통신을 허용하거나 차단하는 방화벽의 핵심 기능이다.
② O — 방화벽은 통신과 보안 이벤트를 로그로 남겨 사후 분석과 감사 추적에 활용할 수 있다.
③ O — 방화벽은 사용자나 접속 주체를 확인한 뒤 정책에 따라 접근을 허용하는 인증 기능을 제공할 수 있다.
④ O — 방화벽은 VPN 기능과 연계하여 외부와 주고받는 데이터를 암호화된 터널로 보호할 수 있다.
⑤ X — 틀린 표현은 '시그니처 기반의 침입 탐지'가 방화벽의 기능이라는 부분이다. 올바르게는 알려진 공격의 시그니처와 트래픽 또는 시스템 활동을 비교하여 침입을 찾아내는 IDS의 탐지 기능이다.

NoteBase

오답 포인트

방화벽과 IDS가 모두 네트워크 보안에 사용되므로 ⑤를 방화벽 기능으로 혼동하기 쉽다. 그러나 '시그니처와 비교하여 공격을 찾아낸다'는 표현은 접근 통제가 아니라 침입 탐지에 해당한다.

다시 나오면 이렇게 판단

'정책에 따라 허용·차단한다'면 방화벽, '공격 패턴이나 이상 행위를 분석하여 찾아낸다'면 IDS로 판단한다.

암기 포인트

방화벽은 통신을 통제하고, IDS는 침입을 탐지한다. 시그니처 기반 탐지는 IDS의 대표 기능이다.

NoteBase

2. 접근제어 모델에 대한 설명으로 옳지 않은 것은?

① 임의적 접근제어 기법은 자원의 소유자가 접근 주체를 결정한다.
② 강제적 접근제어 기법은 자원이 소속된 조직의 관리자가 접근권한을 결정한다.
③ 임의적 접근제어 기법은 보안 레이블을 기반으로 접근 가능 여부를 판단한다.
④ 강제적 접근제어 기법은 원래의 객체에 부여된 허가권이 복사된 객체에서도 동일하게 유지된다.
⑤ 임의적 접근제어 기법은 대부분의 운영체제에서 파일의 접근규칙을 정의할 때 활용한다.

정답 3번

출제 포인트

임의적 접근제어와 강제적 접근제어를 누가 권한을 결정하는지, 무엇을 기준으로 허용 여부를 판단하는지에 따라 구별하는 문제이다.

핵심 개념

임의적 접근제어(DAC)는 객체의 소유자가 사용자 신원 등을 기준으로 접근권한을 부여하거나 회수하는 방식이다.
강제적 접근제어(MAC)는 관리자가 정한 중앙의 보안정책에 따라 주체의 인가등급과 객체의 보안 레이블을 비교하여 접근을 통제하는 방식이다.
핵심 차이는 DAC가 소유자의 재량을 중심으로 하고, MAC가 조직의 강제된 보안정책과 보안 레이블을 중심으로 한다는 점이다.

선지별 해설

① O — 임의적 접근제어에서는 자원의 소유자가 해당 객체에 누가 접근할 수 있는지를 결정한다.
② O — 강제적 접근제어에서는 개별 소유자가 아니라 조직의 관리자 또는 중앙 보안정책이 접근권한을 결정한다.
③ X — 틀린 표현은 '임의적 접근제어 기법은 보안 레이블을 기반으로'이다. 올바르게는 강제적 접근제어 기법이 주체의 인가등급과 객체의 보안 레이블을 기반으로 접근 가능 여부를 판단한다. 임의적 접근제어는 주로 사용자 신원과 소유자가 설정한 권한을 기준으로 한다.
④ O — 강제적 접근제어에서는 객체의 보안등급과 같은 보안속성이 중앙 정책으로 관리되므로, 객체가 복사되어도 원본에 적용된 보안 제약이 복사본에 유지된다.
⑤ O — 일반적인 운영체제의 파일 권한은 파일 소유자가 사용자별 권한을 설정할 수 있으므로 임의적 접근제어의 대표적인 활용 사례이다.

NoteBase

오답 포인트

③은 '보안 레이블'이라는 강제적 접근제어의 핵심 기준을 임의적 접근제어의 특징으로 바꾸어 놓았다.
'소유자·신원·재량'과 '관리자·레이블·강제 정책'을 서로 뒤섞지 않아야 한다.

다시 나오면 이렇게 판단

권한 결정자가 객체의 소유자이면 임의적 접근제어, 중앙 관리자와 조직의 보안정책이면 강제적 접근제어로 판단한다. 보안 레이블과 인가등급의 비교가 나오면 강제적 접근제어에 해당한다.

암기 포인트

DAC는 소유자의 재량, MAC는 관리자의 정책과 보안 레이블이다.

NoteBase

3. 공격자가 자신의 공격시도나 침투 흔적을 숨기기 위해 사용하는 악의적인 프로그램의 집합 혹은 악성 프로그램은?

① 루트킷(Rootkit)
② 스파이웨어(Spyware)
③ 트로이 목마(Trojan Horse)
④ RAT(Remote Administration Tool)
⑤ 랜섬웨어(Ransomware)

정답 1번

출제 포인트

공격자가 자신의 침투 사실과 활동 흔적을 숨기는 데 사용하는 루트킷의 목적을 다른 악성 프로그램과 구별하는 문제이다.

핵심 개념

루트킷은 공격자가 시스템에 침투한 뒤 자신의 존재, 악성 프로세스·파일, 접근 흔적 등을 운영체제 수준에서 숨기고 권한 있는 접근을 유지하도록 돕는 악성 도구의 집합이다. 결정적 키워드는 '침투 흔적 은폐'이다.
스파이웨어는 정보 수집·감시, 트로이 목마는 정상 프로그램 위장, RAT는 원격 제어, 랜섬웨어는 암호화·잠금과 금전 요구가 핵심이다.

선지별 해설

① O — 루트킷은 공격자의 침투 흔적과 악성 활동을 숨겨 탐지를 피하고 접근을 유지하는 데 사용되므로 문제의 설명과 일치한다.
② X — 틀린 부분은 흔적 은폐 프로그램을 '스파이웨어'라고 한 것이다. 스파이웨어는 사용자의 정보나 활동을 몰래 수집·감시하는 악성 프로그램이며, 제시된 설명에 해당하는 것은 루트킷이다.
③ X — 틀린 부분은 흔적 은폐 프로그램을 '트로이 목마'라고 한 것이다. 트로이 목마는 정상적이거나 유용한 프로그램처럼 위장하여 사용자의 실행을 유도한 뒤 악성 기능을 수행하며, 제시된 설명에 해당하는 것은 루트킷이다.
④ X — 틀린 부분은 흔적 은폐 프로그램을 'RAT'라고 한 것이다. RAT는 감염된 시스템을 네트워크를 통해 원격으로 제어·관리하게 하는 도구이며, 제시된 설명에 해당하는 것은 루트킷이다.
⑤ X — 틀린 부분은 흔적 은폐 프로그램을 '랜섬웨어'라고 한 것이다. 랜섬웨어는 파일을 암호화하거나 시스템 사용을 막은 뒤 복구를 대가로 금전을 요구하며, 제시된 설명에 해당하는 것은 루트킷이다.

오답 포인트

모든 선지가 공격에 활용될 수 있다는 공통점 때문에 혼동하기 쉽다. 그러나 문제의 핵심 표현은 '공격시도나 침투 흔적을 숨기기 위해'이며, 이는 정보 탈취나 원격 제어가 아니라 은폐 기능을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

선지의 악성 프로그램을 행위 목적과 연결한다. 은폐·흔적 제거는 루트킷, 몰래 정보 수집은 스파이웨어, 정상 프로그램 위장은 트로이 목마, 원격 조종은 RAT, 암호화 후 금전 요구는 랜섬웨어로 판단한다.

암기 포인트

루트킷은 침투 흔적을 숨기고, 스파이웨어는 정보를 훔쳐보며, 트로이 목마는 위장하고, RAT는 원격 조종하며, 랜섬웨어는 잠그고 금전을 요구한다.

NoteBase

4. 공개키 기반 구조(PKI)의 특징으로 옳지 않은 것은?

① 디지털 서명의 검증
② 전송 메시지의 암호화
③ 공개키를 인증기관에 등록
④ 등록한 공개키의 암호화
⑤ 공개키와 개인키 쌍의 생성

정답 4번

출제 포인트

공개키 기반 구조(PKI)에서 공개키와 개인키의 역할, 인증기관의 기능, 디지털 서명과 암호화의 관계를 구별하는 문제이다.

핵심 개념

PKI는 공개키와 개인키, 디지털 인증서, 인증기관 등을 이용해 공개키의 소유자를 확인하고 암호화와 디지털 서명을 지원하는 체계이다. 공개키는 배포되어 암호화나 서명 검증에 사용되고, 개인키는 소유자만 비밀리에 보관하여 복호화나 서명 생성에 사용된다. 인증기관은 신원과 공개키의 결합을 확인하여 인증서를 발급한다.

선지별 해설

① O — 디지털 서명은 개인키로 생성하고 대응하는 공개키로 검증하므로, PKI는 인증서로 공개키의 소유자를 확인하여 서명 검증을 지원한다.
② O — 수신자의 공개키를 이용해 전송할 데이터나 세션 키를 암호화하고 수신자의 개인키로 복호화할 수 있으므로 기밀성을 제공한다.
③ O — 인증기관은 신원과 공개키의 대응 관계를 확인하고 그 공개키가 포함된 인증서를 발급·관리하므로, 공개키의 등록·인증은 PKI의 구성 과정에 해당한다.
④ X — 틀린 표현은 '등록한 공개키의 암호화'이다. 공개키는 공개·배포하여 사용하는 키이므로 그 자체를 비밀로 만들기 위해 암호화하는 것이 PKI의 특징이 아니다. 올바르게는 개인키를 안전하게 비밀 보관하고, 공개키는 인증서로 소유자와의 결합 및 무결성을 확인한다.
⑤ O — PKI에서는 서로 수학적으로 연관된 공개키와 개인키의 쌍을 생성하며, 두 키는 각각 암호화·검증과 복호화·서명에 사용된다.

오답 포인트

'공개키도 보안에 쓰이는 키이므로 암호화해야 한다'고 생각하기 쉽다. 그러나 공개키의 핵심은 공개와 배포이고, 보호해야 할 비밀은 개인키이다. 공개키에는 암호화가 아니라 인증서를 통한 소유자 확인과 무결성 보장이 필요하다.

NoteBase

다시 나오면 이렇게 판단

공개키는 공개·배포·암호화·서명 검증, 개인키는 비밀 보관·복호화·서명 생성으로 구분한다. 인증기관은 공개키를 숨기는 기관이 아니라 신원과 공개키의 결합을 인증하는 기관으로 판단한다.

암기 포인트

공개키는 공개하고 인증하며, 개인키는 비밀로 보호한다.

5. 솔트(Salt)에 대한 설명으로 옳지 않은 것만을 모두 고르면?

ㄱ. 패스워드 원본 뒤에 추가로 덧붙이는 랜덤 데이터이다.

ㄴ. 단방향 함수에 동일한 패스워드가 입력되어도, 같이 입력된 솔트 값의 차이를 통해 서로 다른 출력 값이 생성된다.

ㄷ. 솔트 값은 패스워드의 길이와 동일하거나, 그보다 길어야 한다.

ㄹ. 솔트 값은 단방향 함수에 패스워드와 함께 입력된 다음, 저장 공간 확보를 위해 삭제된다.

ㅁ. 솔트 값을 적용하면 패스워드의 보안성이 향상된다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
⑤ ㄹ, ㅁ

정답 4번

출제 포인트

솔트의 결합 방식과 저장 여부, 길이 조건, 보안 효과를 구분하여 옳지 않은 설명만 고르는 문제이다.

핵심 개념

솔트는 비밀번호를 해시하기 전에 비밀번호와 결합하는 무작위 값이다. 같은 비밀번호라도 서로 다른 솔트를 사용하면 해시 결과가 달라지므로 미리 계산한 해시표를 이용한 공격을 어렵게 한다. 솔트의 길이가 반드시 비밀번호 이상이어야 하는 것은 아니며, 비밀번호를 검증할 때 다시 사용해야 하므로 해시값과 함께 저장한다. 솔트는 공개되어도 되는 값이지만 사용자마다 충분히 길고 예측하기 어렵게 생성되어야 한다.

ㄱ O: 솔트는 비밀번호에 덧붙여 해시 입력을 다르게 만드는 무작위 데이터이다.

ㄴ O: 동일한 비밀번호라도 솔트가 다르면 결합된 입력이 달라져 서로 다른 해시 출력이 생성된다.

ㄷ X: 솔트 길이는 비밀번호 길이와 같거나 더 길어야 한다는 필수 조건이 없다. 올바르게는 비밀번호 길이와 무관하게 충분한 길이의 무작위 솔트를 사용한다.

ㄹ X: 솔트는 입력 후 삭제하는 값이 아니다. 올바르게는 이후 비밀번호 검증에 필요하므로 해당 비밀번호의 해시값과 함께 저장한다.

ㅁ O: 사용자마다 다른 솔트를 적용하면 동일 비밀번호의 해시값도 달라져 레인보우 테이블 등 사전 계산 공격의 효율이 낮아진다.

NoteBase

선지별 해설

① X: ㄱ은 옳고 ㄴ도 옳으므로 '옳지 않은 것'의 조합이 아니다. 올바른 조합은 ㄷ, ㄹ이다.
② X: ㄱ은 옳고 ㄷ만 옳지 않으므로 틀린 진술을 모두 고른 조합이 아니다. 올바른 조합은 ㄷ, ㄹ이다.
③ X: ㄴ은 옳고 ㄷ만 옳지 않으므로 틀린 진술을 모두 고른 조합이 아니다. 올바른 조합은 ㄷ, ㄹ이다.
④ O: ㄷ은 솔트 길이에 비밀번호 길이 이상의 필수 조건을 둔 점이 틀리고, ㄹ은 검증에 필요한 솔트를 삭제한다고 한 점이 틀리므로 옳지 않은 것만 모두 고른 조합이다.
⑤ X: ㄹ은 옳지 않지만 ㅁ은 옳으므로 옳지 않은 진술만 묶은 조합이 아니다. 올바른 조합은 ㄷ, ㄹ이다.

오답 포인트

ㄷ의 '패스워드의 길이와 동일하거나 그보다 길어야 한다'와 ㄹ의 '저장 공간 확보를 위해 삭제된다'가 함정이다. 솔트는 비밀번호 길이에 종속되지 않으며, 비밀로 숨길 필요는 없지만 재검증을 위해 저장해야 한다.

다시 나오면 이렇게 판단

솔트 관련 선지는 세 기준으로 판단한다. 사용자마다 무작위 값을 사용하는지, 같은 비밀번호의 해시를 서로 다르게 만드는지, 검증을 위해 솔트를 해시값과 함께 보관하는지를 확인한다. 비밀번호와 같은 길이라는 조건이나 사용 후 삭제한다는 표현은 잘못된 설명이다.

암기 포인트

솔트는 '사용자마다 무작위로, 해시와 함께 저장'한다. 길이는 비밀번호 길이에 맞추는 것이 아니라 충분한 무작위성을 기준으로 한다.

NoteBase

6. 공격자가 일정 부분의 평문과 이에 대응하는 암호문을 모두 알고 있을 때 비밀키를 알아내기 위한 공격은?

① 기지 평문 공격
② 선택 암호문 공격
③ 선택 평문 공격
④ 암호문 단독 공격
⑤ 전수조사 공격

정답 1번

출제 포인트

이 문제는 공격자가 확보한 정보와 공격 과정에 따라 암호 공격을 구분하는 기준을 묻는 문제이다.

핵심 개념

기지 평문 공격은 평문의 일부와 그에 대응하는 암호문 쌍을 알고 이를 이용해 비밀키나 암호 구조를 분석하는 공격이다.
선택 평문 공격은 공격자가 고른 평문의 암호문을 얻어 분석하고, 선택 암호문 공격은 공격자가 고른 암호문의 복호화 결과를 얻어 분석한다.
암호문 단독 공격은 암호문만으로 분석하며, 전수조사 공격은 가능한 키를 모두 대입해 올바른 키를 찾는다.

선지별 해설

① O — 평문의 일부와 이에 대응하는 암호문을 알고 있으므로 기지 평문 공격에 해당한다.
② X — '선택 암호문 공격'은 공격자가 선택한 암호문의 복호화 결과를 얻을 수 있을 때의 공격이다. 문제의 조건에 맞는 올바른 표현은 '기지 평문 공격'이다.
③ X — '선택 평문 공격'은 공격자가 선택한 평문에 대응하는 암호문을 얻을 수 있을 때의 공격이다. 이미 알려진 평문·암호문 쌍을 이용한다는 조건의 올바른 표현은 '기지 평문 공격'이다.
④ X — '암호문 단독 공격'은 평문이나 키에 관한 추가 정보 없이 암호문만을 이용하는 공격이다. 평문과 대응 암호문을 함께 안다는 조건의 올바른 표현은 '기지 평문 공격'이다.
⑤ X — '전수조사 공격'은 가능한 키를 하나씩 모두 대입하는 공격이다. 알려진 평문·암호문 쌍을 분석해 키를 알아내는 공격의 올바른 표현은 '기지 평문 공격'이다.

오답 포인트

'평문을 알고 있다'는 사실만 보고 선택 평문 공격과 혼동하기 쉽다. 선택 평문 공격은 공격자가 평문을 직접 선택해 그 암호문을 얻는 반면, 기지 평문 공격은 이미 확보한 평문과 대응 암호문 쌍을 이용한다.

NoteBase

다시 나오면 이렇게 판단

공격자가 무엇을 알고 있는지와 무엇을 선택할 수 있는지를 확인한다. 알려진 평문·암호문 쌍이면 기지 평문, 평문을 선택해 암호문을 얻으면 선택 평문, 암호문을 선택해 복호문을 얻으면 선택 암호문, 암호문만 있으면 암호문 단독 공격으로 판단한다.

암기 포인트

알려진 평문+대응 암호문은 기지 평문 공격, 직접 고른 입력은 선택 공격이다.

NoteBase

7. **백도어 탐지 방법으로 옳지 않은 것은?**

① 현재 동작 중인 프로세스 및 열린 포트 확인
② SetUID 파일 검사
③ 백신 등 바이러스 탐지 툴 사용
④ 무결성 검사
⑤ 실행파일 패킹

정답 5번

출제 포인트

백도어를 탐지하는 점검 방법과 악성코드가 탐지를 피하기 위해 사용하는 은닉·분석 방해 기법을 구별하는 문제이다.

핵심 개념

백도어 탐지는 공격자가 남긴 비정상 프로세스, 열린 포트, 특수 권한 파일, 악성코드 흔적, 파일 변조 여부를 조사하는 활동이다.
실행파일 패킹은 실행파일을 압축하거나 변형해 내부 코드를 알아보기 어렵게 만드는 기법으로, 그 자체는 백도어 탐지 방법이 아니다.

선지별 해설

① O — 현재 동작 중인 프로세스와 열린 포트를 확인하면 정체불명의 프로그램이나 허가되지 않은 통신 대기 포트 등 백도어의 실행·통신 흔적을 찾을 수 있다.
② O — SetUID 파일은 일반 사용자가 파일 소유자의 권한으로 실행할 수 있으므로, 공격자가 설치한 비정상 SetUID 파일이 있는지 검사하는 것은 권한 상승형 백도어 탐지에 도움이 된다.
③ O — 백신 등 바이러스 탐지 도구는 알려진 악성코드의 서명이나 의심스러운 행위를 검사하므로 트로이목마·백도어 프로그램의 흔적을 찾는 데 사용할 수 있다.
④ O — 무결성 검사는 기준 상태의 해시 등과 현재 파일을 비교하여 시스템 파일의 무단 변경이나 백도어 삽입 흔적을 탐지한다.
⑤ X — 틀린 표현은 '백도어 탐지 방법'으로 본 '실행파일 패킹'이다. 올바르게는 실행파일 패킹은 실행 코드를 압축·변형하여 분석이나 서명 기반 탐지를 어렵게 하는 은닉·분석 방해 기법이며, 탐지 방법으로는 언패킹 후 분석이나 파일·행위 검사를 사용한다.

오답 포인트

⑤의 실행파일 패킹도 악성코드 분석 과정에서 자주 등장하므로 탐지 기술처럼 보일 수 있다. 그러나 패킹은 검사 대상 파일에 적용되는 변형 기법이고, ①~④는 시스템이나 파일에서 이상 징후를 실제로 찾아내는 점검 방법이다.

NoteBase

다시 나오면 이렇게 판단

선지가 비정상 프로세스·포트·권한·악성코드·파일 변조를 '찾는 행위'인지 확인한다. 반대로 코드를 압축·암호화·난독화하여 분석을 어렵게 한다면 탐지 방법이 아니라 회피 또는 은닉 기법으로 판단한다.

암기 포인트

프로세스·포트·SetUID·백신·무결성은 탐지, 패킹은 은닉·분석 방해이다.

NoteBase

8. 64bit 키를 사용하는 RC4 암호알고리즘을 기반으로 동작하며 IV(Initialization Vector) 헤더를 모아 분석할 경우 키가 노출되는 취약점을 갖는 무선랜 보안방식은?

① WEP
② WPA
③ WPA2
④ TKIP
⑤ CCMP

정답 1번

출제 포인트

RC4 기반 무선랜 보안 방식 중 짧은 IV를 반복 사용하고 다수의 패킷을 수집하면 비밀키가 노출될 수 있는 방식을 구별하는 문제이다.

핵심 개념

WEP: RC4로 데이터를 암호화하며, 24bit IV와 비밀키를 결합해 패킷별 RC4 키를 만든다. IV 공간이 작아 재사용이 빈번하고 특정 약한 IV가 나타나므로, 많은 패킷의 IV와 암호문을 수집·분석하면 비밀키를 추정할 수 있다.
WPA·TKIP: WEP의 취약점을 보완하기 위해 키 혼합, 더 긴 패킷 순서 값, 무결성 검사 등을 적용한다.
WPA2·CCMP: 일반적으로 RC4가 아니라 AES 기반 CCMP를 사용한다.
핵심 대비는 'WEP는 RC4·짧은 IV·키 노출 취약점, WPA는 TKIP로 보완, WPA2는 AES-CCMP'이다.

선지별 해설

① O — WEP은 64bit 키라고 부르는 구성에서 일반적으로 40bit 비밀키와 24bit IV를 결합해 RC4 키 스트림을 만든다. 짧은 IV의 반복과 약한 IV 때문에 패킷을 대량 수집하면 비밀키가 노출될 수 있으므로 문제의 설명과 일치한다.
② X — 틀린 부분은 'WPA가 제시된 64bit RC4·IV 수집형 키 노출 취약점을 갖는다'는 판단이다. 올바르게는 WPA는 WEP의 취약점을 보완하기 위해 주로 TKIP의 키 혼합과 무결성 보호를 적용한 방식이다.
③ X — 틀린 부분은 'WPA2가 RC4 기반으로 동작한다'는 판단이다. 올바르게는 WPA2는 일반적으로 AES 기반 CCMP를 사용한다.
④ X — 틀린 부분은 'TKIP 자체가 64bit WEP 방식이며 짧은 IV를 그대로 비밀키와 결합한다'는 판단이다. 올바르게는 TKIP는 RC4를 사용하지만 128bit 시간 키와 패킷별 키 혼합을 적용하여 WEP의 단순한 키 생성 방식을 보완한 WPA용 프로토콜이다.
⑤ X — 틀린 부분은 'CCMP가 RC4 기반으로 동작한다'는 판단이다. 올바르게는 CCMP는 AES의 CCM 운용 방식을 사용해 기밀성과 무결성을 제공한다.

NoteBase

오답 포인트

TKIP도 RC4를 사용한다는 점 때문에 ④를 고르기 쉽다. 그러나 문제의 결정적 단서는 ‘64bit 키’, ‘IV 헤더 수집’, ‘키 노출’의 결합이며, 이는 짧은 IV와 약한 키 생성 구조를 가진 WEP의 고전적 취약점을 가리킨다.

다시 나오면 이렇게 판단

RC4와 24bit IV의 반복, 약한 IV, 패킷 대량 수집에 따른 키 복구가 함께 제시되면 WEP으로 판단한다. TKIP는 RC4를 쓰더라도 키 혼합으로 WEP을 보완하고, CCMP는 AES 기반이라는 차이로 구별한다.

암기 포인트

WEP은 RC4·짧은 IV·키 노출, WPA는 TKIP, WPA2는 AES-CCMP이다.

NoteBase

9. 다음에서 설명하는 AES 운영 모드는?

○ 블록단위로 동작한다. ○ 각 블록을 병렬적으로 처리할 수 있다. ○ 블록이 독립적으로 동작하여 한 블록에서의 에러가 다른 블록에 영향을 주지 않는다.

① CTR

② OFB

③ CFB

④ CBC

⑤ ECB

정답 5번

출제 포인트

AES 블록 암호의 운영 모드 가운데 블록의 독립 처리, 병렬 처리, 오류 전파 여부를 비교하는 문제이다. 공식 채점은 이 특징들을 ECB의 대표적 특성으로 보아 ⑤를 정답으로 삼았지만, 제시된 조건만으로는 CTR도 배제하기 어렵다.

핵심 개념

ECB는 각 평문 블록을 다른 블록과 연결하지 않고 같은 키로 각각 암호화하는 모드이다. 따라서 블록별 병렬 처리가 가능하고, 한 암호문 블록의 오류가 다른 블록의 복호 결과로 전파되지 않는다. 다만 같은 평문 블록은 같은 암호문 블록이 되어 데이터의 반복 패턴이 드러날 수 있다.
CTR은 서로 다른 카운터 블록을 암호화해 만든 키 스트림과 평문을 배타적 논리합하는 방식이다. 카운터별 연산이 독립적이므로 블록별 병렬 처리가 가능하고, 암호문 오류도 다른 블록으로 전파되지 않는다. OFB와 CFB는 앞 단계의 출력이나 암호문을 되먹임하고, CBC는 앞 암호문 블록을 다음 평문 블록과 결합한다.

NoteBase

선지별 해설

① X
공식 채점에서는 CTR을 정답으로 인정하지 않았다. 그러나 CTR은 서로 다른 카운터 블록을 독립적으로 암호화하므로 병렬 처리가 가능하고, 한 암호문 블록의 전송 오류가 다른 블록의 복호 결과로 전파되지 않는다. 따라서 이미지에 제시된 세 조건만으로는 CTR을 엄밀히 배제하기 어렵고, 공식 답 ⑤는 이 특징들을 ECB의 대표적 특성으로 묶은 출제 의도에 따른 것이다.

② X
OFB는 이전 단계의 출력이 다음 키 스트림 생성에 입력되는 되먹임 구조이므로 키 스트림 생성 과정이 순차적이며 각 블록을 독립적으로 병렬 처리하는 모드가 아니다. 틀린 표현은 '각 블록을 병렬적으로 처리할 수 있다'이며, 올바르게는 '이전 출력에 의존하여 순차적으로 키 스트림을 생성한다'이다.

③ X
CFB는 앞선 암호문을 다음 처리에 되먹임하므로 블록들이 독립적으로 동작하지 않으며, 암호문 오류가 뒤의 일정 구간에도 영향을 줄 수 있다. 틀린 표현은 '블록이 독립적으로 동작하여 한 블록의 에러가 다른 블록에 영향을 주지 않는다'이며, 올바르게는 '앞선 암호문에 의존하고 오류가 뒤의 일정 구간까지 전파될 수 있다'이다.

④ X
CBC 암호화는 이전 암호문 블록을 다음 평문 블록과 결합하므로 블록을 독립적으로 처리할 수 없고 암호화의 병렬 처리도 어렵다. 또한 한 암호문 블록의 오류는 복호화할 때 해당 평문 블록과 다음 평문 블록에 영향을 준다. 틀린 대응은 'CBC'이며, 올바르게는 'ECB'이다.

⑤ O
ECB는 각 블록을 독립적으로 암호화하므로 블록 단위로 동작하고, 여러 블록을 병렬 처리할 수 있으며, 한 암호문 블록의 오류가 다른 블록의 복호 결과에 영향을 주지 않는다. 제시된 세 특징을 모두 만족한다.

오답 포인트

CTR도 카운터별 연산이 독립적이어서 병렬 처리가 가능하고 전송 오류가 다른 블록으로 전파되지 않는다. 따라서 제시된 세 조건만으로는 ①과 ⑤가 모두 부합할 수 있다. 공식 채점은 각 평문 블록을 서로 연결하지 않고 같은 블록 암호로 각각 처리하는 ECB의 대표적 특성을 묻는 의도로 ⑤를 정답으로 삼은 것으로 해석된다. ECB만을 명확히 특정하려면 동일한 평문 블록이 동일한 암호문 블록으로 변환되어 반복 패턴이 드러난다는 등의 추가 단서가 필요하다.

NoteBase

다시 나오면 이렇게 판단

블록들이 서로 독립적이고 병렬 처리가 가능하며 오류가 다른 블록으로 전파되지 않는다는 조건은 ECB뿐 아니라 CTR에도 해당할 수 있다. 동일한 평문 블록이 동일한 암호문 블록이 되거나 반복 패턴이 드러난다는 단서가 있으면 ECB이고, 카운터를 암호화해 키 스트림을 만든다는 단서가 있으면 CTR이다. 출력값을 되먹임하면 OFB, 암호문을 되먹임하면 CFB, 이전 암호문과 다음 평문을 결합하면 CBC이다.

암기 포인트

ECB는 블록별 독립 처리·병렬 처리 가능·블록 간 오류 전파 없음이다.

NoteBase

10. 암호학적 해시 알고리즘에 대한 설명으로 옳지 않은 것은?

① 해시 결과값을 이용하여 해시 입력값을 역으로 찾아내는 것은 계산상으로 불가능해야 한다.

② MD5 및 SHA-1 알고리즘은 취약점이 발견되지 않아 지금도 많이 사용되고 있다.

③ 충돌 저항성(Collision Resistance)은 동일한 출력값(해시값)을 생성하는 두 가지 입력값을 구하는 것이 계산적으로 어렵다는 것을 의미한다.

④ SHA-224은 출력의 길이가 224비트이다.

⑤ 해시 알고리즘은 어떠한 길이의 입력값이 들어오더라도 일정한 길이의 해시값을 출력한다.

정답 2번

출제 포인트

해시 함수의 일방향성·충돌 저항성·고정 길이 출력 특성과 대표 해시 알고리즘의 안전성을 구별하는 문제이다.

핵심 개념

암호학적 해시 함수는 임의 길이의 입력을 일정한 길이의 해시값으로 변환하는 함수이다. 역상 저항성은 주어진 해시값에 대응하는 입력을 찾기 어려운 성질이고, 충돌 저항성은 같은 해시값을 만드는 서로 다른 두 입력을 찾기 어려운 성질이다. MD5와 SHA-1은 충돌 취약점이 알려져 있어 보안 목적의 신규 사용에 적합하지 않다.

선지별 해설

① O — 해시값만으로 그 해시값을 만든 입력을 역으로 찾아내는 일이 계산적으로 어려워야 한다. 이는 역상 저항성에 해당한다.

② X — 틀린 표현은 '취약점이 발견되지 않아 지금도 많이 사용되고 있다'이다. MD5와 SHA-1에는 충돌 취약점이 알려져 있으므로 보안 목적에서는 사용을 피하고 SHA-2·SHA-3 계열 등 안전한 알고리즘을 사용해야 한다.

③ O — 충돌 저항성은 동일한 해시값을 출력하는 서로 다른 두 입력을 찾아내는 일이 계산적으로 어려운 성질이다.

④ O — SHA-224는 224비트 길이의 해시값을 출력한다.

⑤ O — 해시 함수는 입력 길이가 달라도 알고리즘별로 정해진 일정한 길이의 해시값을 출력한다.

오답 포인트

MD5와 SHA-1이 과거에 널리 사용되었다는 사실을 현재도 안전하다는 뜻으로 오해하기 쉽다. ②는 '많이 사용되었다'와 '취약점이 없다'를 결합해 안전성이 유지되는 것처럼 만든 선지이다.

NoteBase

다시 나오면 이렇게 판단

해시 특성은 '해시값에서 입력 찾기=역상 저항성', '같은 해시값의 서로 다른 두 입력 찾기=충돌 저항성', '임의 길이 입력에서 고정 길이 출력'으로 구분한다. MD5·SHA-1을 안전한 알고리즘이라고 설명하면 틀린 선지로 판단한다.

암기 포인트

해시는 임의 길이 입력을 고정 길이로 바꾸며, MD5·SHA-1은 충돌 취약점 때문에 보안용으로 부적합하다.

NoteBase

11. 「개인정보 보호법」 제25조에 따라 공개된 장소에서의 영상정보 처리기기 설치가 예외적으로 허용되는 경우가 아닌 것은?

① 법령에서 구체적으로 허용하고 있는 경우
② 범죄의 예방 및 수사를 위하여 필요한 경우
③ 시설안전 및 화재 예방을 위하여 필요한 경우
④ 교통단속을 위하여 필요한 경우
⑤ 통계작성·과학적 연구·공익적 기록보존 등을 위하여 필요한 경우

정답 5번

쟁점

이 문제는 공개된 장소에 고정형 영상정보처리기기를 설치·운영할 수 있는 예외 사유를 묻는 문제이다. 핵심은 「개인정보 보호법」 제25조의 설치·운영 허용 사유와 제28조의2의 가명정보 처리 목적을 구별하는 것이다.

용어 풀이

고정형 영상정보처리기기 = 일정한 공간에 설치되어 지속적 또는 주기적으로 사람이나 사물의 영상을 촬영하거나 전송하는 장치이다. 공개된 장소에서는 원칙적으로 설치·운영이 금지되고, 법률이 정한 사유가 있을 때만 예외적으로 허용된다.

핵심 구분

「개인정보 보호법」 제25조는 공개된 장소에서의 고정형 영상정보처리기기 설치·운영을 원칙적으로 금지하면서, 법령의 구체적 허용, 범죄 예방·수사, 시설 안전·관리 및 화재 예방, 교통단속, 교통정보의 수집·분석·제공 등의 경우를 예외로 둔다. 반면 통계작성·과학적 연구·공익적 기록보존 등은 제28조의2에 따른 가명정보의 처리 목적이며, 그 자체가 공개된 장소에서 기기를 설치·운영할 수 있는 제25조의 예외 사유는 아니다.

NoteBase

선지별 해설

① O
법령에서 구체적으로 허용하는 경우는 제25조가 정한 예외 사유이다.

② O
범죄의 예방 및 수사를 위하여 필요한 경우는 제25조가 정한 예외 사유이다.

③ O
시설의 안전·관리 및 화재 예방을 위하여 필요한 경우는 제25조가 정한 예외 사유이다. 현행법은 정당한 권한을 가진 자가 설치·운영하는 경우로 규정한다.

④ O
교통단속을 위하여 필요한 경우는 제25조가 정한 예외 사유이다. 현행법은 정당한 권한을 가진 자가 설치·운영하는 경우로 규정한다.

⑤ X
통계작성·과학적 연구·공익적 기록보존 등은 가명정보를 정보주체의 동의 없이 처리할 수 있는 목적에 해당할 뿐, 공개된 장소에서 고정형 영상정보처리기기를 설치·운영할 수 있는 예외 사유가 아니다.
틀린 표현: 통계작성·과학적 연구·공익적 기록보존 등을 위하여 필요한 경우에는 공개된 장소에서 영상정보처리기기를 설치할 수 있다.
올바른 표현: 개인정보처리자는 통계작성·과학적 연구·공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

오답 포인트

⑤의 문구는 개인정보 보호법에 실제로 등장하므로 설치 허용 사유처럼 보이기 쉽다. 그러나 이는 제28조의2의 가명정보 처리 목적이고, 제25조의 공개된 장소에서의 기기 설치·운영 예외와는 적용 영역이 다르다.

다시 나오면 이렇게 판단

공개된 장소의 고정형 영상정보처리기기 문제에서는 먼저 제25조의 설치 목적 목록인지 확인한다.
통계작성·과학적 연구·공익적 기록보존이라는 묶음이 보이면 가명정보 처리 특례를 떠올리고, 기기 설치 예외와 구별한다.

암기 포인트

CCTV 설치 예외는 범죄·시설·화재·교통 중심이고, 통계·연구·기록은 가명정보 처리 목적이다.

NoteBase

12. 다음은 리눅스의 /etc/passwd 파일의 일부이다. 이에 대한 설명으로 옳지 않은 것만을 모두 고르면?

```
root:x:0:0:root:/root:/bin/bash
(1)  (2) (3) (4)  (5)      (6)        (7)
```

ㄱ. (1)과 (5)는 사용자 계정에 관한 정보들로 반드시 동일한 값이어야 한다.

ㄴ. (2)는 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타낸다.

ㄷ. (3)은 사용자 번호(User ID)를 나타내며, 계정마다 다른 값을 가져야 한다.

ㄹ. 이 파일을 통해 현재 시스템에 등록된 계정 정보를 확인할 수 있다.

ㅁ. (7)은 사용자의 홈 디렉터리 정보를 나타낸다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄱ, ㅁ
④ ㄷ, ㄹ
⑤ ㄷ, ㅁ

정답 3번

출제 포인트

/etc/passwd의 7개 필드가 각각 사용자명, 암호 표시, UID, GID, 설명, 홈 디렉터리, 로그인 셸 중 무엇을 뜻하는지 구분하는 문제이다.

핵심 개념

/etc/passwd의 한 행은 콜론(:)으로 구분된 7개 필드로 구성된다. 순서는 사용자명 : 암호 표시 : UID : GID : 사용자 설명(GECOS) : 홈 디렉터리 : 로그인 셸이다. 제시된 행에서는 (1) root가 사용자명, (2) x가 shadow 파일 사용 표시, (3) 0이 UID, (4) 0이 GID, (5) root가 사용자 설명, (6) /root가 홈 디렉터리, (7) /bin/bash가 로그인 셸이다.

NoteBase

선지별 해설

① X — ㄱ은 틀리지만 ㄴ은 옳으므로, 옳지 않은 설명의 조합이 아니다. ㄱ의 '(1)과 (5)는 반드시 동일한 값'이 틀렸으며, 올바르게는 (1)은 사용자명이고 (5)는 사용자 설명 필드이므로 서로 달라도 된다. ㄴ의 x는 실제 암호문이 /etc/shadow에 저장됨을 나타낸다.
② X — ㄱ은 틀리지만 ㄷ은 옳으므로, 옳지 않은 설명의 조합이 아니다. ㄷ의 (3)은 UID이며 계정을 식별하는 번호이므로 계정별로 구별되는 값을 부여하는 것이 원칙이다.
③ O — ㄱ과 ㅁ이 모두 옳지 않은 설명이다. ㄱ에서 (1)과 (5)는 역할이 다른 필드라 반드시 같을 필요가 없다. ㅁ에서 (7)은 홈 디렉터리가 아니라 로그인 셸이며, 홈 디렉터리는 (6)의 /root이다.
④ X — ㄷ과 ㄹ은 모두 옳은 설명이므로, 옳지 않은 설명의 조합이 아니다. (3)은 UID이고, /etc/passwd에는 시스템에 등록된 사용자 계정의 기본 정보가 기록된다.
⑤ X — ㄷ은 옳고 ㅁ만 틀리므로, 둘 모두를 옳지 않은 설명으로 고른 조합이 아니다. ㅁ의 '(7)은 홈 디렉터리'가 틀렸으며, 올바르게는 (6)이 홈 디렉터리이고 (7)은 로그인 셸이다.

오답 포인트

(5)의 값도 root라서 (1)과 같은 필드라고 오인하기 쉽지만, 값이 우연히 같을 뿐 의미는 각각 사용자명과 사용자 설명으로 다르다. 또한 끝의 두 필드는 홈 디렉터리와 로그인 셸 순서이므로 /root와 /bin/bash의 역할을 바꾸어 판단하면 안 된다.

다시 나오면 이렇게 판단

콜론을 기준으로 7개 필드를 먼저 나눈 뒤 '이름-암호-UID-GID-설명-홈-셸' 순서에 맞추어 각 문장을 판단한다. 조합형에서는 ㄱ~ㅁ의 진위를 먼저 확정한 다음 보기의 조합과 대조한다.

암기 포인트

passwd 7필드는 '이름-암호-UID-GID-설명-홈-셸'이며, 마지막 두 칸은 홈 디렉터리 다음 로그인 셸이다.

NoteBase

13. 버퍼 오버플로(Buffer Overflow) 공격에 대한 설명으로 옳지 않은 것은?

① 데이터 길이에 대한 불명확한 정의를 악용한 공격이다.
② 버퍼 오버플로 공격에 취약한 함수로 strcpy, strcat, gets, scanf 등이 있다.
③ printf와 같은 함수에서 포맷스트링이 포함된 문자열을 통해 공격이 이루어진다.
④ 스택 버퍼 오버플로 공격으로 해커의 공격 코드가 실행되지 않도록, 스택 가드(Stack Guard), 스택 쉴드(Stack Shield) 등의 방어 기법이 적용될 수 있다.
⑤ 입력 데이터의 길이에 대한 정의를 포함하는 snprintf, fgets 등의 함수 사용이 권장된다.

정답 3번

출제 포인트

버퍼 오버플로와 포맷 스트링 공격을 구별하고, 경계 검사를 하지 않는 함수와 길이를 제한하는 안전한 함수 및 스택 보호 기법을 판단하는 문제이다.

핵심 개념

버퍼 오버플로: 버퍼에 할당된 크기보다 많은 데이터를 기록하여 인접 메모리나 제어 정보를 덮어쓰는 공격이다. 핵심은 입력·복사 길이에 대한 경계 검사가 없거나 잘못되었다는 점이다.
포맷 스트링 공격: 외부 입력을 printf 계열 함수의 포맷 문자열로 직접 사용하여 메모리 내용을 읽거나 변경하는 공격이다. 핵심은 데이터가 포맷 지정자로 해석된다는 점이다.
방어: 입력·출력 길이를 제한하는 함수와 스택의 반환 주소 변조를 탐지·보호하는 기법을 함께 사용한다.

선지별 해설

① O — 버퍼의 실제 크기나 허용 가능한 데이터 길이를 정확히 확인하지 않으면 경계를 넘는 쓰기가 발생할 수 있으므로 버퍼 오버플로의 원인에 해당한다.
② O — strcpy, strcat, gets 및 길이 제한 없이 문자열을 읽는 scanf는 목적지 버퍼의 경계를 넘길 수 있어 취약하다.
③ X — 틀린 표현은 ‘printf와 같은 함수에서 포맷스트링이 포함된 문자열을 통해 버퍼 오버플로 공격이 이루어진다’이다. 외부 입력을 printf 계열 함수의 포맷 문자열로 직접 넘길 때 발생하는 것은 포맷 스트링 공격이다. 올바르게는 ‘검증되지 않은 입력이 포맷 문자열로 사용되면 포맷 스트링 공격이 이루어질 수 있다’이다.
④ O — Stack Guard는 스택의 제어 정보 앞에 둔 보호값의 변조를 검사하고, Stack Shield와 같은 기법은 반환 주소를 보호하여 공격 코드로 제어가 넘어가는 것을 막는 데 사용된다.
⑤ O — snprintf는 출력할 최대 길이를 지정하고 fgets는 읽을 최대 길이를 지정하므로 버퍼 크기에 맞춰 사용하면 경계를 넘는 쓰기를 예방할 수 있다.

NoteBase

오답 포인트

③은 printf라는 함수명과 문자열 공격이라는 공통점 때문에 버퍼 오버플로처럼 보이게 만든 선지이다. 그러나 사용자의 문자열이 함수의 포맷 자체로 해석되는 취약점은 포맷 스트링 공격으로 분류한다.

다시 나오면 이렇게 판단

버퍼 용량을 넘겨 쓰는지가 핵심이면 버퍼 오버플로, 외부 입력 속 퍼센트 포맷 지정자가 해석되는지가 핵심이면 포맷 스트링 공격으로 판단한다. 함수명만 보지 않고 길이 경계 검사와 포맷 문자열 통제 여부를 확인한다.

암기 포인트

길이 초과 쓰기는 버퍼 오버플로, 입력을 포맷으로 해석하면 포맷 스트링 공격이다.

NoteBase

14. 보안 제품 평가 및 기준에 대한 설명으로 옳은 것은?

① CC는 EAL1부터 EAL6까지 6개의 등급으로 구분한다.
② ITSEC에서 최상위 레벨의 보안등급은 A1이다.
③ TCSEC은 유럽 4개국이 작성한 보안 기준이다.
④ ITSEC은 기밀성, 무결성, 가용성을 포괄하는 표준안을 제시한다.
⑤ CC 보증 등급에서 EAL4는 준정형적 설계 및 시험을 요구한다.

정답 4번

출제 포인트

CC, ITSEC, TCSEC의 개발 주체와 평가등급 체계, 그리고 보증수준별 요구사항을 구별하는 문제이다.

핵심 개념

CC(Common Criteria): 여러 국가가 공통으로 사용하는 정보보호 제품 평가기준이며, 보증수준을 EAL1부터 EAL7까지 구분한다.
ITSEC: 유럽에서 마련된 정보기술 보안 평가기준으로, 기능성과 보증을 구분하여 평가하며
기밀성·무결성·가용성과 관련된 보안 기능을 다룬다. 보증등급은 E0부터 E6까지이다.
TCSEC: 미국 국방부가 제정한 보안 평가기준이며 D, C1, C2, B1, B2, B3, A1 순으로 보증 수준이 높아진다.

선지별 해설

① X — 틀린 표현은 'EAL1부터 EAL6까지 6개의 등급'이다. CC의 보증등급은 EAL1부터 EAL7까지 모두 7개이다.
② X — 틀린 표현은 'ITSEC에서 최상의 레벨의 보안등급은 A1'이다. A1은 TCSEC의 최상위 등급이고, ITSEC의 보증등급은 E0부터 E6까지이며 최상위는 E6이다.
③ X — 틀린 표현은 'TCSEC은 유럽 4개국이 작성'이다. TCSEC은 미국 국방부가 제정한 기준이며,
영국·독일·프랑스·네덜란드 등 유럽 국가들이 공동으로 마련한 기준은 ITSEC이다.
④ O — ITSEC은 정보기술 제품과 시스템의 보안 기능 및 보증을 평가하는 기준으로서 기밀성, 무결성, 가용성과 관련된 보안 요구를 포괄한다.
⑤ X — 틀린 표현은 'EAL4는 준정형적 설계 및 시험을 요구'한다는 부분이다. EAL4는 체계적으로
설계·시험·검토된 수준이고, 준정형적으로 설계되고 시험된 수준은 EAL5이다.

오답 포인트

②는 TCSEC의 A1을 ITSEC의 등급처럼 바꾸었고, ③은 ITSEC과 TCSEC의 개발 주체를 뒤바꾸었다. 또한 ①은 CC의 마지막 등급인 EAL7을 누락했으며, ⑤는 EAL4와 EAL5의 설명을 바꾸어 제시했다.

NoteBase

다시 나오면 이렇게 판단

먼저 등급 표기를 기준별로 연결한다. CC는 EAL1~EAL7, ITSEC은 E0~E6, TCSEC은 D~A1이다. 그다음 개발 주체와 보증수준의 핵심 표현을 대조한다. CC의 EAL4는 체계적 설계·시험·검토, EAL5는 준정형적 설계·시험이다.

암기 포인트

CC는 EAL 1~7, ITSEC은 유럽·E 0~6, TCSEC은 미국·A1이 최고이다. EAL4는 체계적, EAL5는 준정형적이다.

NoteBase

15. SSL/TLS에 대한 설명으로 옳지 않은 것은?

① TCP 프로토콜 상위계층에 위치하여, TCP 프로토콜을 통해 전송하는 데이터를 안전하게 전달하는 것을 목적으로 한다.
② Heartbleed 취약점은 OpenSSL 라이브러리에서 발견된 바 있다.
③ 레코드 프로토콜은 상위계층에서 오는 데이터를 전달한다.
④ TLS 1.3에서는 더 이상 RSA를 키 교환 알고리즘으로 지원하지 않는다.
⑤ TLS 1.3은 TLS 1.2 혹은 그 이하 버전과 비교하여 Handshake 과정에서 주고받는 메시지 교환 횟수가 더 많아졌다.

정답 5번

출제 포인트

SSL/TLS의 계층상 위치, Record 프로토콜의 역할, Heartbleed, TLS 1.3의 키 교환 방식과 Handshake 단축을 구분하는 문제이다.

핵심 개념

SSL/TLS는 응용계층 데이터가 TCP를 통해 전송되기 전에 기밀성·무결성·상대 인증을 제공하는 보안 프로토콜이다.
Record 프로토콜은 상위의 Handshake·Alert·응용 데이터 등을 레코드로 만들어 보호한 뒤 하위의 TCP로 전달한다.
TLS 1.3은 정적 RSA 키 교환을 제거하고 (EC)DHE 기반 키 교환을 사용하며, Handshake 왕복 횟수를 줄여 연결 설정을 단축한다. RSA 인증서와 RSA 서명 알고리즘의 사용까지 모두 금지한 것은 아니다.

선지별 해설

① O — SSL/TLS는 TCP의 상위에서 동작하며, TCP로 전달되는 응용 데이터를 암호화하고 무결성을 보호하여 안전한 통신을 제공한다.
② O — Heartbleed는 OpenSSL의 TLS Heartbeat 확장 구현에서 길이 검증이 누락되어 메모리 내용이 노출될 수 있었던 취약점이다.
③ O — Record 프로토콜은 Handshake 메시지와 응용 데이터 등 상위에서 받은 데이터를 레코드 단위로 처리하고 보호하여 TCP에 전달한다.
④ O — TLS 1.3에서는 정적 RSA 키 교환이 제거되었으므로 RSA를 키 교환 알고리즘으로 지원하지 않는다. 다만 RSA 서명은 인증 용도로 사용할 수 있다.
⑤ X — 틀린 표현은 '메시지 교환 횟수가 더 많아졌다'이다. 올바르게는 TLS 1.3이 TLS 1.2 이하보다 Handshake의 왕복 통신을 줄였다고 해야 한다. 일반적인 최초 연결은 1-RTT로 완료되고, 재개 연결에서는 조건에 따라 0-RTT도 가능하다.

NoteBase

오답 포인트

④의 'RSA를 키 교환 알고리즘으로 지원하지 않는다'를 'RSA를 전혀 사용할 수 없다'로 확대 해석하면 혼동하기 쉽다. TLS 1.3에서 제거된 것은 정적 RSA 키 교환이며 RSA 서명은 남아 있다. ⑤는 TLS 1.3의 성능 개선 방향을 반대로 서술한 선지이다.

다시 나오면 이렇게 판단

TLS 1.3 관련 선지는 '정적 RSA 키 교환 제거, (EC)DHE 중심, Handshake 왕복 횟수 감소'의 세 기준으로 판단한다. Record 프로토콜은 상위 데이터를 보호하여 TCP로 내려보내는 계층으로 구분한다.

암기 포인트

TLS 1.3은 정적 RSA 키 교환을 빼고 Handshake를 줄였다.

NoteBase

16. 블루투스(Bluetooth) 연결을 통해 무선 기기에서 무단으로 정보에 접근하는 것을 말하며, 공격자가 OPP(OBEX Push Profile)를 사용하여 상대 기기에 있는 주소록이나 달력, 파일 등을 접근하는 공격은?

① 블루버그(Bluebug)
② 블루스나프(Bluesnarf)
③ 블루프린팅(Blueprinting)
④ 블루재킹(Bluejacking)
⑤ BIAS(Bluetooth Impersonation AttackS)

정답 2번

출제 포인트

이 문제는 블루투스 공격을 공격 행위와 사용 목적에 따라 구별하는 문제이다. OPP(OBEX Push Profile)를 이용하여 상대 기기의 주소록·달력·파일 등에 무단 접근하는 공격은 블루스나프이다.

핵심 개념

블루스나프(Bluesnarf)는 블루투스의 OBEX 관련 기능을 악용하여 상대 기기의 주소록, 달력, 파일과 같은 정보를 허가 없이 빼내는 공격이다.
블루버그(Bluebug)는 취약한 블루투스 연결을 통해 기기의 통화·메시지 등 기능을 원격으로 조작하는 공격이다.
블루프린팅(Blueprinting)은 블루투스 기기의 제조사, 모델, 지원 서비스나 프로파일 등의 특성을 수집하여 식별하는 정찰 행위이다.
블루재킹(Bluejacking)은 블루투스를 통해 원치 않는 메시지나 전자 명함 등을 보내는 행위이다.
BIAS(Bluetooth Impersonation AttackS)는 블루투스 인증 절차의 약점을 이용하여 신뢰 관계가 있는 다른 기기로 위장하는 공격이다.

NoteBase

선지별 해설

① X — 블루버그는 상대 기기의 통화·메시지 등 기능을 원격으로 조작하는 공격이다. ‘OPP를 이용한 주소록·달력·파일의 무단 접근’이라는 표현은 블루스나프로 고쳐야 한다.
② O — 블루스나프는 OPP 등 OBEX 관련 기능을 악용하여 상대 기기의 주소록·달력·파일에 무단으로 접근하거나 정보를 빼내는 공격이므로 제시된 설명과 일치한다.
③ X — 블루프린팅은 블루투스 기기의 제조사, 모델, 지원 서비스나 프로파일 등 식별 정보를 수집하는 정찰 행위이다. ‘주소록·달력·파일에 무단 접근하는 공격’은 블루스나프로 고쳐야 한다.
④ X — 블루재킹은 블루투스를 통해 원치 않는 메시지나 전자 명함 등을 보내는 행위이다. ‘상대 기기의 정보를 무단으로 빼내는 공격’은 블루스나프로 고쳐야 한다.
⑤ X — BIAS는 인증 절차의 약점을 이용하여 공격 기기가 신뢰받는 블루투스 기기인 것처럼 위장하는 공격이다. ‘OPP를 이용해 주소록·달력·파일에 무단 접근하는 공격’은 블루스나프로 고쳐야 한다.

오답 포인트

블루버그와 블루스나프는 모두 상대 기기에 무단으로 관여한다는 점 때문에 혼동하기 쉽다. 이 문항에서는 ‘주소록·달력·파일 등 정보에 접근’과 ‘OPP·OBEX’가 블루스나프를 가리키는 결정적 표현이다.

다시 나오면 이렇게 판단

정보 탈취는 블루스나프, 기기 기능의 원격 조작은 블루버그, 기기 특성 수집은 블루프린팅, 원치 않는 메시지 전송은 블루재킹, 신뢰 기기 위장은 BIAS로 판단한다.

암기 포인트

스나프는 정보 탈취, 버그는 기능 조작, 프린팅은 기기 식별, 재킹은 메시지 전송, BIAS는 기기 위장이다.

NoteBase

17. 위험분석 및 평가를 통해 도출된 위험에 대해 적절한 처리를 하고자 할 때, 접근 방법으로 옳지 않은 것은?

① 위험 수용
② 위험 감소
③ 위험 회피
④ 위험 전가
⑤ 위험 검사

정답 5번

출제 포인트

이 문제는 위험분석 및 평가 결과에 따라 선택하는 위험 처리 방법을 구분하는 문제이다.

핵심 개념

위험 처리는 식별·평가된 위험을 조직이 정한 수준으로 다루는 의사결정이다.
위험 수용은 별도의 추가 조치 없이 위험을 감수하는 방법이고, 위험 감소는 통제로 발생 가능성이나 영향을 낮추는 방법이다. 위험 회피는 위험을 일으키는 활동 자체를 중단하거나 변경하는 방법이며, 위험 전가는 보험이나 계약 등을 통해 손실 부담의 일부 또는 전부를 제3자에게 이전하는 방법이다.

선지별 해설

① O — 위험 수용은 위험 수준이 허용 범위 안에 있거나 추가 통제 비용이 기대 손실보다 큰 경우, 위험을 인지한 채 받아들이는 적절한 처리 방법이다.
② O — 위험 감소는 보안 통제를 적용하여 위험의 발생 가능성이나 발생 시 영향을 낮추는 적절한 처리 방법이다.
③ O — 위험 회피는 위험의 원인이 되는 업무·자산·기술의 사용을 중단하거나 방식을 바꾸어 해당 위험을 피하는 적절한 처리 방법이다.
④ O — 위험 전가는 보험 가입, 외주 또는 계약 등을 통해 위험으로 인한 손실 부담을 제3자와 분담하거나 이전하는 적절한 처리 방법이다.
⑤ X — 틀린 표현은 '위험 검사'이다. 위험 검사는 위험 처리 방법의 유형이 아니며, 올바르게는 위험 수용·위험 감소·위험 회피·위험 전가 가운데 평가 결과에 맞는 방법을 선택한다고 해야 한다.

오답 포인트

'검사'가 위험을 확인하거나 점검하는 활동처럼 보여 처리 방법으로 착각하기 쉽다. 그러나 위험을 분석·평가하는 활동과 평가 후 위험을 처리하는 방법은 구분되며, ⑤의 '위험 검사'는 처리 방법에 해당하지 않는다.

NoteBase

다시 나오면 이렇게 판단

위험을 그대로 감수하면 수용, 가능성이나 영향을 낮추면 감소, 원인 활동을 없애면 회피, 손실 부담을 제3자에게 넘기면 전가로 판단한다. 단순한 검사·식별·분석·평가는 위험을 파악하는 과정이지 위험 처리 방법은 아니다.

암기 포인트

위험 처리의 핵심 네 가지는 수용·감소·회피·전가이다.

NoteBase

18. SYN Flooding 공격과 ARP Spoofing 공격이 이루어지는 네트워크 OSI 계층으로 올바르게 짝지어진 것은?

	SYN Flooding 공격	ARP Spoofing 공격
①	Physical Layer	Network Layer
②	Network Layer	Transport Layer
③	Transport Layer	Data Link Layer
④	Data Link Layer	Network Layer
⑤	Network Layer	Data Link Layer

정답 3번

출제 포인트

이 문제는 SYN Flooding과 ARP Spoofing이 악용하는 프로토콜의 기능을 기준으로 공격이 이루어지는 OSI 계층을 구분하는 문제이다.

핵심 개념

SYN Flooding: TCP의 연결 설정 과정에서 SYN 요청을 대량으로 보내 서버의 대기 자원을 고갈시키는 공격이다. TCP는 전송 계층 프로토콜이므로 SYN Flooding은 전송 계층 공격이다.
ARP Spoofing: 위조된 ARP 정보를 보내 IP 주소와 MAC 주소의 대응 관계를 속이는 공격이다. ARP를 이용한 동일 네트워크 구간의 주소 대응 조작이므로 데이터 링크 계층 공격으로 분류한다.
핵심 대비: SYN·TCP는 전송 계층, ARP·MAC 주소 대응은 데이터 링크 계층이다.

선지별 해설

① X — 'SYN Flooding 공격-Physical Layer'와 'ARP Spoofing 공격-Network Layer'가 모두 틀리다. 올바르게는 SYN Flooding은 Transport Layer, ARP Spoofing은 Data Link Layer이다.
② X — 'SYN Flooding 공격-Network Layer'와 'ARP Spoofing 공격-Transport Layer'가 모두 틀리다. 올바르게는 각각 Transport Layer와 Data Link Layer이다.
③ O — SYN Flooding은 TCP 연결 설정을 악용하므로 Transport Layer이고, ARP Spoofing은 IP-MAC 주소 대응 관계를 조작하므로 Data Link Layer이다.
④ X — 'SYN Flooding 공격-Data Link Layer'와 'ARP Spoofing 공격-Network Layer'가 모두 틀리다. 올바르게는 각각 Transport Layer와 Data Link Layer이다.
⑤ X — 'SYN Flooding 공격-Network Layer'가 틀리다. 올바르게는 SYN Flooding은 Transport Layer이다. ARP Spoofing을 Data Link Layer로 짝지은 부분은 맞다.

NoteBase

오답 포인트

ARP가 IP 주소를 다루기 때문에 Network Layer로 착각하기 쉽다. 그러나 이 문항에서는 IP 주소에 대응하는 MAC 주소 정보를 위조한다는 점을 기준으로 ARP Spoofing을 Data Link Layer로 분류한다. 또한 SYN Flooding은 패킷을 전송한다는 막연한 이미지가 아니라 TCP의 SYN 연결 절차를 악용한다는 점에서 Transport Layer이다.

다시 나오면 이렇게 판단

공격 이름에 포함된 프로토콜과 핵심 식별자를 먼저 찾는다. TCP의 SYN·ACK·포트·연결 설정은 Transport Layer, MAC 주소·프레임·ARP를 통한 주소 대응 조작은 Data Link Layer로 판단한다.

암기 포인트

SYN은 TCP이므로 전송 계층, ARP Spoofing은 MAC 주소 대응을 속이므로 데이터 링크 계층이다.

NoteBase

19. 공개키 암호방식의 성능문제와 대칭키 암호방식의 키 관리 문제를 상호 보완하여 하이브리드 암호화 환경을 구축하고자 한다. <보기>의 ㉠, ㉡에 해당하는 알고리즘으로 올바르게 짝지어진 것은?

<보 기>

㉠ 키 생성 및 교환을 위한 알고리즘
㉡ 데이터 암호화 알고리즘

	㉠	㉡
①	SHA	RSA
②	RSA	AES
③	AES	SHA
④	SEED	RSA
⑤	RSA	SHA

정답 2번

출제 포인트

하이브리드 암호화에서 비대칭키 암호가 키 생성·교환을 지원하고, 대칭키 암호가 실제 데이터를 빠르게 암호화한다는 역할 분담을 묻는 문제이다.

핵심 개념

RSA: 공개키와 개인키를 사용하는 비대칭키 암호 알고리즘으로, 하이브리드 환경에서 데이터 암호화에 사용할 대칭키를 안전하게 전달하는 데 활용된다.
AES: 동일한 비밀키로 암호화와 복호화를 수행하는 대칭키 블록 암호 알고리즘으로, 대용량 데이터를 빠르게 암호화하는 데 적합하다.
SHA: 입력값을 고정 길이 해시값으로 바꾸는 해시 함수이며, 복호화가 전제되는 데이터 암호 알고리즘이 아니다.
SEED: 대칭키 블록 암호 알고리즘이므로 데이터 암호화에는 사용할 수 있지만 공개키 기반의 키 교환 알고리즘은 아니다.
핵심 대비: RSA는 대칭키의 안전한 전달, AES는 실제 데이터의 고속 암호화를 담당한다.

NoteBase

선지별 해설

① X — ㉠의 SHA가 틀렸다. SHA는 해시 함수이므로 키 생성 및 교환을 위한 알고리즘이 아니다. 또한 ㉡에는 하이브리드 환경의 데이터 암호화용 대칭키 알고리즘이 와야 한다. 올바른 조합은 ㉠ RSA, ㉡ AES이다.
② O — RSA로 데이터 암호화에 사용할 대칭키를 안전하게 전달하고, AES로 실제 데이터를 빠르게 암호화하므로 하이브리드 암호화의 역할 분담에 맞는다.
③ X — ㉠의 AES와 ㉡의 SHA가 모두 틀렸다. AES는 대칭키 암호라서 공개키 기반의 키 교환 역할에 해당하지 않고, SHA는 해시 함수라서 데이터 암호화 알고리즘이 아니다. 올바르게는 ㉠ RSA, ㉡ AES이다.
④ X — ㉠의 SEED와 ㉡의 RSA가 역할에 맞지 않는다. SEED는 대칭키 블록 암호이므로 키 교환용 비대칭키 알고리즘이 아니며, RSA는 대용량 데이터 암호화보다 대칭키 전달에 적합하다. 올바르게는 ㉠ RSA, ㉡ AES이다.
⑤ X — ㉠의 RSA는 맞지만 ㉡의 SHA가 틀렸다. SHA는 무결성 확인 등에 쓰이는 해시 함수이지 복호화 가능한 데이터 암호 알고리즘이 아니다. ㉡은 AES가 되어야 한다.

오답 포인트

RSA도 데이터를 암호화할 수 있다는 점만 보고 ④를 고르거나, SHA를 암호 알고리즘이라는 넓은 범주만으로 보고 ①·③·⑤를 고르기 쉽다. 문제는 각 알고리즘의 존재 여부가 아니라 하이브리드 환경에서 맡는 역할을 묻는다. 키 전달은 RSA, 실제 데이터 암호화는 AES로 구분한다.

다시 나오면 이렇게 판단

먼저 빈칸의 역할을 확인한다. 키 교환·키 전달이면 공개키 방식인 RSA를, 대용량 데이터 암호화이면 빠른 대칭키 방식인 AES를 대응시킨다. SHA가 나오면 암호화·복호화가 아니라 일방향 해시 기능으로 판단한다.

암기 포인트

하이브리드 암호화는 RSA로 키를 전달하고 AES로 데이터를 암호화한다. SHA는 해시, SEED는 대칭키 블록 암호이다.

NoteBase

20. 사용자가 일시적으로 파일 소유자의 권한으로 특정 기능을 실행하고자 할 때, 사용 가능한 명령어로 옳은 것은?

① chmod u+rw testfile
② chmod 666 testfile
③ chmod o+r testfile
④ chmod 4755 testfile
⑤ chmod g+w testfile

정답 4번

출제 포인트

이 문제는 파일을 실행할 때 실행 사용자 대신 파일 소유자의 권한을 일시적으로 적용하는 SetUID의 설정 방법을 묻는다.

핵심 개념

SetUID는 실행 파일에 설정하는 특수 권한으로, 해당 파일이 실행되는 동안 프로세스의 유효 사용자 ID를 파일 소유자의 ID로 바꾼다. 숫자 모드에서 SetUID 비트는 맨 앞자리 4로 표시하므로 chmod 4755 testfile은 SetUID를 설정하고 소유자에게 rwx, 그룹과 기타 사용자에게 r-x 권한을 부여한다.

선지별 해설

① X — chmod u+rw testfile은 소유자에게 읽기(r)와 쓰기(w) 권한만 추가한다. 틀린 표현은 u+rw이며, 올바르게는 소유자 실행 시 소유자 권한을 적용하려면 u+s로 SetUID를 설정해야 한다.
② X — chmod 666 testfile은 소유자·그룹·기타 사용자에게 읽기와 쓰기 권한만 부여하며 실행 권한과 SetUID 비트가 없다. 올바르게는 SetUID를 포함한 4755와 같은 모드를 사용해야 한다.
③ X — chmod o+r testfile은 기타 사용자에게 읽기 권한만 추가한다. 틀린 표현은 o+r이며, 올바르게는 SetUID 설정에 u+s 또는 숫자 모드의 선행값 4를 사용해야 한다.
④ O — chmod 4755 testfile의 첫 자리 4는 SetUID 비트이고, 뒤의 755는 소유자 rwx와 그룹·기타 사용자 r-x를 뜻한다. 따라서 실행 시 파일 소유자의 권한을 일시적으로 사용할 수 있다.
⑤ X — chmod g+w testfile은 그룹에 쓰기 권한만 추가한다. 틀린 표현은 g+w이며, 올바르게는 파일 소유자의 권한으로 실행하려면 u+s로 SetUID를 설정해야 한다.

오답 포인트

①·②·③·⑤는 일반 읽기·쓰기 권한만 변경한다. 문제의 '파일 소유자의 권한으로 실행'은 소유자에게 rw 권한을 더 주는 것이 아니라 특수 권한 SetUID를 설정하라는 뜻이다.

NoteBase

다시 나오면 이렇게 판단

실행 중 파일 소유자의 권한을 사용한다는 표현이 나오면 SetUID를 찾는다. 기호 모드는 u+s, 숫자 모드는 일반 권한 세 자리 앞에 4를 붙이는 방식으로 판단한다.

암기 포인트

SetUID는 소유자 권한으로 실행하며, u+s 또는 숫자 모드의 앞자리 4로 설정한다.