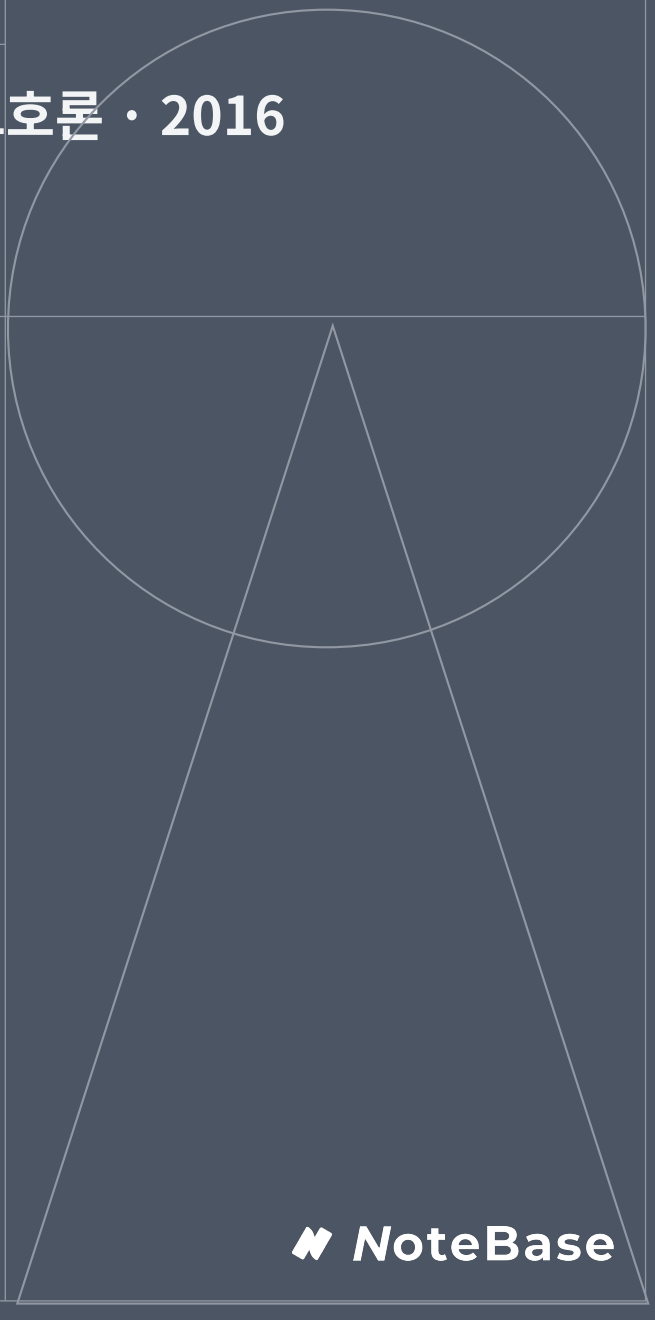
기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2016



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보보호론 · 2016

공무원/국가직/9급 · 정보보호론 · 2016

문 1. 사용자 인증에 사용되는 기술이 아닌 것은?

① Snort

② OTP(One Time Password)

③ SSO(Single Sign On)

④ 스마트 카드

정답 1번

간단한 해설

Snort는 네트워크 트래픽을 분석하여 공격을 찾아내는 **침입 탐지·방지 도구**이다. 접속한 사용자가 본인인지 확인하는 사용자 인증 기술과는 기능이 다르다.

공통 해설

사용자 인증은 접속하려는 사람이 자신이 주장하는 사용자와 일치하는지 확인하는 과정이다. 판단 기준은 **사용자의 신원을 확인하거나 그 인증 결과를 활용하는 기능**인지에 있다.

OTP는 한 번만 사용할 수 있는 비밀번호를 인증에 이용하고, 스마트 카드는 카드에 저장된 인증정보를 이용하여 사용자의 신원을 확인하는 데 쓰인다. SSO는 한 번 인증한 결과를 여러 연계 시스템에서 활용하여 반복적인 로그인을 줄인다. 따라서 이들은 인증 수단을 제공하거나 인증 결과를 연계하는 기술에 해당한다.

Snort는 네트워크 패킷을 검사하여 침입이나 공격 징후를 탐지하고, 구성에 따라 공격 트래픽을 차단한다. 확인 대상이 사용자의 신원이 아니라 **네트워크 트래픽의 공격 징후**이므로 사용자 인증 기술에 해당하지 않는다.

NoteBase

문 2. 보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은?

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자산의 잠재적인 속성으로서 위협의 이용 대상이 되는 것

① ㄱ: 위협, ㄴ: 취약점, ㄷ: 위험
② ㄱ: 위협, ㄴ: 위험, ㄷ: 취약점
③ ㄱ: 취약점, ㄴ: 위협, ㄷ: 위험
④ ㄱ: 위험, ㄴ: 위협, ㄷ: 취약점

정답 2번

간단한 해설

위협은 손실을 일으킬 수 있는 원인·행위자이고, 취약점은 위협에 이용되는 약점이다. 손실이나 부정적 영향이 생길 **가능성**을 뜻하는 것은 **위험**이다.

대응 관계 해설

ㄱ. 위협: 자산에 손실을 초래할 수 있는 사건의 잠재적인 원인이나 행위자를 뜻한다. 설명의 **'잠재적인 원인이나 행위자'**가 위협을 가리키는 단서이다. 예를 들어 시스템에 침입하려는 공격자는 위협에 해당한다.

ㄴ. 위험: 원하지 않는 사건이 발생하여 자산에 손실이나 부정적인 영향이 생길 가능성을 뜻한다. 위협이 손실을 일으킬 수 있는 원인이라면, 위험은 **그로 인해 피해가 생길 가능성**에 초점을 둔다.

ㄷ. 취약점: 위협이 이용할 수 있는 자산의 약점이나 결함을 뜻한다. 예를 들어 추측하기 쉬운 비밀번호는 공격자가 악용할 수 있는 취약점이다. 따라서 **'위협의 이용 대상이 되는' 자산의 속성**이라는 설명이 취약점에 대응한다.

ㄱ은 위협, ㄴ은 위험, ㄷ은 취약점으로 짝지어지므로 ②의 대응과 일치한다.

NoteBase

문 3. 공개키 암호 알고리즘에 대한 설명으로 옳은 것은?

① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.

② RSA 암호 알고리즘은 적절한 시간 내에 인수가 큰 정수의 소인수분해가 어렵다는 점을 이용한 것이다.

③ 타원곡선 암호 알고리즘은 타원곡선 대수문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 긴 길이의 키를 필요로 한다.

④ ElGamal 암호 알고리즘은 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것이다.

정답 2번

간단한 해설

RSA는 큰 소수들을 곱하는 계산은 쉽지만, 그 곱을 다시 소인수분해하여 원래 소수들을 찾는 계산은 어렵다는 **소인수분해 문제의 어려움**을 이용한다.

선지별 해설

① X: 기본 Diffie-Hellman 키 교환은 두 당사자가 공통 비밀값을 만들게 하지만, **상대방의 신원을 인증하지 않는다**. 공격자가 양쪽에서 교환하는 공개값을 자신의 값으로 바꾸면 각 당사자와 따로 비밀값을 공유할 수 있으므로 중간자 공격에 취약하다. 이를 막으려면 전자서명 등으로 교환값과 상대방을 인증하는 절차를 결합해야 한다.

② O: RSA는 **큰 소인수를 가진 정수의 소인수분해가 어렵다**는 점을 이용한다. 두 큰 소수를 곱하여 공개키에 쓰이는 정수를 만드는 것은 쉽지만, 그 정수만으로 원래의 소수들을 알아내기는 어렵다. 소인수들을 알면 개인키를 구할 수 있으므로, 이 소인수분해의 어려움이 RSA의 안전성을 뒷받침한다.

③ X: 타원곡선 암호는 타원곡선 위의 점에 대한 이산로그 문제의 어려움에 기초한다. 한 점을 정해진 횟수만큼 반복해서 더한 결과는 계산할 수 있지만, 시작점과 결과점만으로 그 횟수를 알아내기는 어렵다는 뜻이다. 같은 안전성 수준을 제공할 때는 RSA보다 **더 짧은 키**를 사용할 수 있으므로, 더 긴 키가 필요하다는 부분이 잘못되었다.

④ X: 선택한 수들의 합을 구하기는 쉽지만 그 합으로부터 어떤 수들을 선택했는지 알아내기 어렵다는 설명은 **부분집합 합 문제를 이용하는 배낭 암호**에 해당한다. ElGamal은 이와 달리 이산로그 문제의 어려움에 기초한다. 기본 ElGamal에서 사용하는 모듈러 거듭제곱은 계산하기 쉽지만, 밑과 계산 결과로부터 지수를 알아내기는 어렵다는 성질을 이용한다.

NoteBase

문 4. ISO/IEC 27001의 보안 위험 관리를 위한 PDCA 모델에 대한 설명으로 옳지 않은 것은?

① IT기술과 위험 환경의 변화에 대응하기 위하여 반복되어야 하는 순환적 프로세스이다.

② Plan 단계에서는 보안 정책, 목적, 프로세스 및 절차를 수립한다.

③ Do 단계에서는 수립된 프로세스 및 절차를 구현하고 운영한다.

④ Act 단계에서는 성과를 측정하고 평가한다.

정답 4번

간단한 해설

성과를 측정하고 평가하는 것은 **Check 단계**의 역할이다. Act 단계에서는 점검 결과를 바탕으로 **시정·예방 조치를 수행하여 개선**한다.

선지별 해설

① O: PDCA는 계획·실행·점검·개선을 반복하는 관리 모형이다. IT기술과 위협이 바뀌면 기존 보안대책의 효과도 달라질 수 있으므로, 한 번 구축하고 끝내지 않고 **점검 결과를 다음 계획과 개선에 반영**한다.

② O: Plan은 정보보호 관리체계를 수립하는 단계이다. 위험을 관리하기 위해 어떤 보안 목표를 달성할지 정하고, 그 목표에 필요한 **정책·프로세스·절차를 수립**한다. 실제 운영에 앞서 운영 기준과 방법을 마련하는 것이다.

③ O: Do는 Plan에서 마련한 정책과 절차를 **실제로 구현하고 운영**하는 단계이다. 계획한 보안 통제와 업무 절차를 현장에 적용하므로, 기준을 만드는 Plan과 구별된다.

④ X: 성과를 측정하고 평가하는 것은 **Check 단계**이다. 운영 결과를 보안 정책과 목표에 비추어 점검하고 그 효과를 평가한다. Act는 이 점검 결과나 내부감사·경영검토 결과 등을 바탕으로 **시정·예방 조치를 수행하여 관리체계를 유지·개선**하는 단계이다. 따라서 선지의 'Act'를 'Check'로 고쳐야 한다.

NoteBase

문 5. 메시지의 무결성을 검증하는 데 사용되는 해시와 메시지 인증 코드(MAC)의 차이점에 대한 설명으로 옳은 것은?

① MAC는 메시지와 송·수신자만이 공유하는 비밀키를 입력받아 생성되는 반면에, 해시는 비밀키 없이 메시지로부터 만들어진다.

② 해시의 크기는 메시지 크기와 무관하게 일정하지만, MAC는 메시지와 크기가 같아야 한다.

③ 메시지 무결성 검증 시, 해시는 암호화되어 원본 메시지와 함께 수신자에게 전달되는 반면에, MAC의 경우에는 MAC로부터 원본 메시지 복호화가 가능하므로 MAC만 전송하는 것이 일반적이다.

④ 송·수신자만이 공유하는 비밀키가 있는 경우, MAC를 이용하여 메시지 무결성을 검증할 수 있으나 해시를 이용한 메시지 무결성 검증은 불가능하다.

정답 1번

간단한 해설

MAC는 메시지와 **송·수신자가 공유하는 비밀키**로 생성하지만, 일반 해시는 **비밀키 없이** 메시지로부터 생성한다. 두 방식의 핵심 차이는 비밀키의 사용 여부이다.

선지별 해설

① O: MAC는 메시지와 송·수신자가 공유하는 비밀키를 입력으로 하여 만드는 인증값이다. 수신자는 받은 메시지와 같은 비밀키로 MAC를 다시 계산하고, 전달받은 MAC와 비교하여 메시지의 무결성을 검증한다. 일반 해시는 **비밀키 없이 메시지만으로 계산**하므로 누구나 같은 메시지의 해시값을 구할 수 있다.

② X: 일반 해시의 출력 길이는 사용하는 해시 함수가 정해지면 메시지 길이와 관계없이 일정하다. MAC도 사용하는 알고리즘과 출력 길이 설정이 같다면 메시지 길이와 관계없이 일정한 길이의 인증값을 만든다. 따라서 MAC는 **메시지와 크기가 같아야 하는 것이 아니다**.

③ X: MAC는 원본 메시지를 암호화한 암호문이 아니므로 **MAC로부터 메시지를 복호화할 수 없다**. 일반적으로 메시지와 MAC를 함께 전달하고, 수신자가 메시지로 MAC를 다시 계산하여 검증한다. 또한 해시값을 암호화하여 보내는 것은 가능한 구성 방법 중 하나일 뿐, 해시를 이용할 때 항상 필요한 절차는 아니다.

④ X: 일반 해시도 **비교 기준인 원래 해시값을 신뢰할 수 있게 확보**하면, 수신한 메시지의 해시값과 비교하여 무결성을 검증할 수 있다. 공유 비밀키가 있다는 이유로 해시를 이용한 검증이 불가능해지지는 않는다. 다만 보호 없이 메시지와 해시값만 함께 보내면 공격자가 둘 다 바꿀 수 있으므로, 일반 해시만으로 악의적인 변조에 대한 무결성을 보장할 수는 없다. MAC는 비밀키를 모르는 공격자가 변조한 메시지에 맞는 유효한 인증값을 만들기 어렵게 한다.

NoteBase

문 6. DMZ(demilitarized zone)에 대한 설명으로 옳은 것만을 고른 것은?

ㄱ. 외부 네트워크에서는 DMZ에 접근할 수 없다.
ㄴ. DMZ 내에는 웹 서버, DNS 서버, 메일 서버 등이 위치할 수 있다.
ㄷ. 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.
ㄹ. DMZ는 보안 조치가 취해진 네트워크 영역으로, 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

① ㄱ, ㄷ
② ㄴ, ㄷ
③ ㄴ, ㄹ
④ ㄱ, ㄹ

정답 3번

간단한 해설

DMZ에는 **외부에 서비스를 제공하는 서버**를 두고, 방화벽 정책에 따라 외부의 접근을 허용한다. 두 방화벽으로 구성할 때는 DMZ가 **외부 방화벽과 내부 방화벽 사이**에 놓이며, 내부 사용자는 내부 방화벽을 거쳐 DMZ에 접속한다.

보기별 해설

ㄱ. X: DMZ는 외부에 공개할 서비스를 내부 네트워크와 분리하여 배치하는 영역이다. 외부 네트워크에서도 **외부 방화벽이 허용한 서비스에 접근할 수 있다**. 모든 외부 접근을 차단하는 영역이라는 설명은 잘못이다.

ㄴ. O: 외부 사용자에게 서비스를 제공하는 웹 서버, DNS 서버, 메일 서버 등을 DMZ에 배치할 수 있다. 이들을 내부 업무망과 분리하면 **공개 서버가 침해되었을 때 내부망으로 피해가 확산되는 것을 제한**할 수 있다.

ㄷ. X: 내부 방화벽과 외부 방화벽을 사용하는 구성에서 내부망과 DMZ 사이를 통제하는 장치는 **내부 방화벽**이다. 내부 사용자는 내부 방화벽을 거쳐 DMZ에 접속하며, 외부 방화벽은 외부 네트워크와 DMZ 사이의 접근을 통제한다.

ㄹ. O: 두 방화벽을 사용하는 구성은 '외부 네트워크 → 외부 방화벽 → DMZ → 내부 방화벽 → 내부 네트워크'로 나타낼 수 있다. DMZ는 **두 방화벽 사이**에 위치하고, 각 경계에서 보안 정책에 따라 통신을 통제한다.

옳은 보기는 ㄴ, ㄹ이며, ③의 조합과 일치한다.

NoteBase

문 7. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자들에게 알리고 동의를 받아야 하는 내용이 아닌 것은?

① 개인정보의 수집·이용 목적

② 수집하는 개인정보의 항목

③ 개인정보의 보유·이용 기간

④ 개인정보 처리의 위탁기관명

정답 4번

간단한 해설

개인정보 처리의 위탁기관명은 **수집·이용 동의 시 알릴 세 가지 사항에 포함되지 않는다**. 이 문항의 구 정보통신망법은 수집·이용 목적, 수집 항목, 보유·이용 기간을 알리도록 정했다.

공통 해설

구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조제1항은 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집할 때 **수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간**을 모두 알리고 동의를 받도록 규정했다. 목적은 '왜 수집·이용하는가', 항목은 '어떤 정보를 수집하는가', 기간은 '언제까지 보유·이용하는가'를 뜻한다.

개인정보 처리의 위탁기관명은 '어느 기관에 처리를 맡기는가'에 관한 정보로, 제22조제1항이 열거한 세 가지 고지사항에 포함되지 않는다. 이 문항은 **수집·이용 동의 시의 고지사항**을 묻고 있으므로, 처리위탁에 관한 사항과 구별해야 한다.

NoteBase

문 8. 임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?

① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 둔다.

② 주체 또는 주체가 소속되어 있는 그룹의 식별자(ID)를 근거로 객체에 대한 접근을 승인하거나 제한한다.

③ 소유권을 가진 주체가 객체에 대한 권한의 일부 또는 전부를 자신의 의지에 따라 다른 주체에게 부여한다.

④ 전통적인 UNIX 파일 접근제어에 적용되었다.

정답 1번

간단한 해설

①의 '사용자에게 주어진 역할'을 기준으로 접근을 허용하는 방식은 **역할기반접근제어(RBAC)**이다.
임의접근제어(DAC)는 **객체 소유자의 재량**으로 사용자나 그룹에 접근 권한을 부여하는 방식이다.

선지별 해설

① X: 역할에 권한을 연결하고 사용자에게 역할을 부여하여 접근을 통제하는 것은 **역할기반접근제어(RBAC)**이다. 임의접근제어(DAC)에서는 객체 소유자가 누구에게 어떤 접근 권한을 줄지 결정하며, 접근을 요청한 사용자나 그룹의 식별자를 바탕으로 허용 여부를 판단한다.

② O: DAC는 **주체 또는 소속 그룹의 식별자**를 바탕으로 접근을 통제한다. 파일 등의 객체에 설정된 권한과 접근 요청자의 사용자 ID나 그룹 ID를 대조하여 읽기·쓰기 등의 요청을 허용하거나 거부한다.

③ O: DAC의 핵심은 **소유자가 자신의 재량으로 권한을 부여**할 수 있다는 점이다. 예를 들어 파일 소유자 A가 사용자 B에게 읽기만 허용하고 쓰기는 허용하지 않을 수 있다. 이처럼 다른 주체에게 부여할 권한의 범위를 소유자가 정한다.

④ O: 전통적인 UNIX 파일 접근제어는 DAC의 대표적인 적용 사례이다. 파일의 접근 권한을 **소유자·소유 그룹·그 밖의 사용자**로 구분하여 각각 읽기·쓰기·실행 권한을 설정한다. 파일 소유자가 이 권한을 변경하여 다른 사용자의 접근을 통제할 수 있다.

NoteBase

문 9. 식별된 위험에 대처하기 위한 정보보안 위험 관리의 위험 처리 방안 중, 불편이나 기능 저하를 감수하고라도, 위험을 발생시키는 행위나 시스템 사용을 하지 않도록 조치하는 방안은?

① 위험 회피

② 위험 감소

③ 위험 수용

④ 위험 전가

정답 1번

간단한 해설

위험을 발생시키는 행위나 시스템 사용을 **하지 않도록 하는** 방안은 '위험 회피'이다. 편의나 기능을 일부 포기하더라도 해당 위험에 노출되는 원인을 없애는 방식이다.

공통 해설

위험 회피는 **위험을 발생시키는 활동을 수행하지 않거나 중단**하여 그 활동에 따른 위험에 노출되지 않도록 하는 처리 방안이다. 문제에서는 불편이나 기능 저하를 감수하면서까지 위험한 행위나 시스템 사용을 하지 않도록 조치하므로, 위험 회피에 해당한다.

구별 기준은 위험을 발생시키는 활동 자체를 계속하는지이다. 활동을 계속하면서 위험의 크기를 줄이거나, 위험을 감수하거나, 위험 부담을 다른 주체에게 넘기는 것은 활동 자체를 하지 않는 회피와 구별된다. 예를 들어 위험한 원격 접속 기능의 사용을 금지하면 그 기능의 편리함은 포기하지만, 해당 기능의 사용으로 생기는 위험은 피할 수 있다.

NoteBase

문 10. Bell-LaPadula 보안 모델의 *-속성(star property)이 규정하고 있는 것은?

① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다.

② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다.

③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다.

④ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.

정답 4번

간단한 해설

Bell-LaPadula의 *-속성은 기밀정보가 낮은 보안 수준으로 흘러가지 않도록 **하위 수준으로의 쓰기를 금지**한다. 따라서 보안 수준상 자신과 같거나 높은 객체에만 쓸 수 있다.

공통 해설

Bell-LaPadula는 정보의 기밀성을 보호하는 보안 모델이다. 사용자나 프로그램처럼 정보에 접근하는 쪽을 주체, 파일처럼 접근 대상이 되는 쪽을 객체라고 한다. *-속성은 주체가 **자신보다 낮은 보안 수준의 객체에 쓰지 못하도록** 하는 규칙으로, 'No Write Down'이라고 한다. 높은 등급의 정보를 낮은 등급의 파일에 기록하면 낮은 등급의 사용자에게도 그 정보가 노출될 수 있기 때문이다.

이 속성을 적용할 때는 **쓰기 연산인지, 쓰기 대상의 보안 수준이 주체 이상인지**를 확인한다. 읽을 수 있는 객체의 범위를 제시한 설명은 여기서 묻는 쓰기 제한을 설명하지 못하며, 낮은 수준의 객체에 쓰도록 허용하는 설명은 정보의 하향 유출을 막는 원칙에 어긋난다. 보안 수준을 기준으로 쓰기 대상은 자신과 같거나 높은 객체로 제한된다.

NoteBase

문 11. 버퍼 오버플로우에 대한 설명으로 옳지 않은 것은?

① 프로세스 간의 자원 경쟁을 유발하여 권한을 획득하는 기법으로 활용된다.

② C 프로그래밍 언어에서 배열에 기록되는 입력 데이터의 크기를 검사하지 않으면 발생할 수 있다.

③ 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류가 발생하게 되는 상황이다.

④ 버퍼 오버플로우 공격의 대응책 중 하나는 스택이나 힙에 삽입된 코드가 실행되지 않도록 하는 것이다.

정답 1번

간단한 해설

①의 '프로세스 간의 자원 경쟁'을 이용하는 방식은 **경쟁 조건 공격**에 해당한다. 버퍼 오버플로우는 **버퍼의 경계를 넘어 데이터를 기록**하여 인접한 메모리를 훼손하는 현상이다.

선지별 해설

① X: 여러 프로세스가 공유 자원에 접근할 때 실행 순서나 시점에 따라 결과가 달라지는 경쟁 조건을 악용하면 권한을 획득할 수 있다. 이는 **경쟁 조건 공격**의 설명이다. 버퍼 오버플로우 공격은 버퍼의 경계를 넘어 데이터를 써서 인접한 데이터나 제어 정보를 덮어쓰는 방식이다.

② O: C 언어의 배열 접근은 기본적으로 **배열 경계를 자동으로 검사하지 않는다**. 따라서 입력 크기가 배열의 용량을 넘는데도 이를 확인하지 않고 기록하면 배열 밖의 메모리까지 덮어쓸 수 있다. 예를 들어 8바이트 버퍼에 12바이트를 그대로 기록하면 버퍼의 경계를 넘는다.

③ O: 버퍼 오버플로우는 할당된 버퍼의 경계를 넘어 데이터를 기록하는 현상이다. 이때 **인접한 메모리의 내용이 덮어써져** 데이터가 손상되거나 프로그램이 비정상 종료될 수 있다. 덮어쓴 대상이 실행 흐름을 결정하는 제어 정보라면 공격자가 프로그램의 동작을 바꾸는 데 악용할 수도 있다.

④ O: 스택이나 힙의 데이터 영역을 실행 불가능하게 설정하면 공격자가 그곳에 삽입한 코드의 실행을 차단할 수 있다. 대표적으로 데이터 실행 방지(DEP)는 **데이터 영역에 삽입된 코드의 실행**을 막는다. 다만 버퍼의 경계를 넘는 쓰기 자체를 막는 기능은 아니므로, 입력 크기 검사와 함께 적용하는 방어 수단이다.

NoteBase

문 12. 침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는 데 적합한 기법은?

① 규칙 기반의 오용 탐지

② 통계적 분석에 의한 이상(anomaly) 탐지

③ 전문가 시스템을 이용한 오용 탐지

④ 시그니처 기반(signature based) 탐지

정답 2번

간단한 해설

이상 탐지는 **정상적인 활동 양상에서 벗어나는 행위**를 찾아내므로, 공격 패턴이 미리 등록되어 있지 않아도 알려지지 않은 공격을 탐지할 수 있다.

공통 해설

침입탐지 기법은 무엇을 기준으로 의심 행위를 찾아내는지에 따라 구분한다. 통계적 분석에 의한 이상 탐지는 평소의 접속 빈도나 트래픽 양 등으로 정상 활동의 통계적 기준을 만들고, 관찰된 활동이 그 기준에서 유의하게 벗어나면 침입 가능성이 있다고 판단한다. **알려진 공격 패턴과의 일치가 필요하지 않으므로** 알려지지 않은 공격을 탐지하는 데 적합하다. 다만 정상 범위에서 벗어났다는 사실이 곧 공격임을 뜻하지는 않아, 정상 활동을 공격으로 잘못 판단할 수도 있다.

규칙 기반의 오용 탐지와 전문가 시스템을 이용한 오용 탐지는 이미 알려진 공격에 관한 규칙·지식을 적용하고, 시그니처 기반 탐지는 알려진 공격의 특징적인 패턴과 관찰된 활동을 대조한다. 이들은 **미리 확보한 공격 지식이나 패턴**을 판단 기준으로 삼으므로, 그 기준에 포함되지 않은 새로운 공격을 탐지하는 데 한계가 있다.

NoteBase

문 13. 「전자서명법」상 공인인증기관이 발급한 공인인증서의 효력 소멸 또는 폐지의 사유에 해당하지 않는 것은?

① 공인인증서의 유효기간이 경과한 경우

② 가입자의 전자서명검증정보가 유출된 경우

③ 공인인증기관이 가입자의 사망 · 실종선고 또는 해산 사실을 인지한 경우

④ 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우

정답 2번

간단한 해설

전자서명검증정보는 서명을 확인하는 데 사용하는 **공개키**이므로, 그 정보가 알려졌다는 사실만으로 공인인증서를 폐지하지 않는다. 폐지 사유는 공인인증기관이 가입자의 **전자서명생성정보인 개인키의 유출 사실을 인지한 경우**이다.

선지별 해설

이 문항은 공인인증서 제도를 규정하던 구 「전자서명법」을 기준으로 한다. 효력 소멸은 인증서의 효력이 없어지는 것이고, 폐지는 법정 사유에 따라 공인인증기관이 인증서를 더 이상 유효하게 사용할 수 없도록 하는 조치이다. 같은 법 제16조 제1항 제4호는 폐지된 공인인증서의 효력도 소멸한다고 규정한다.

① O: 구 「전자서명법」 제16조 제1항 제1호에 따라 공인인증서의 **유효기간이 경과하면 그때 효력이 소멸**한다. 이는 공인인증기관이 별도로 폐지해야만 효력이 없어지는 경우와 구별된다.

② X: 전자서명검증정보는 전자서명을 확인하는 데 쓰는 공개키이며, 구 「전자서명법」 제15조 제2항 제2호에 따라 공인인증서에 포함되는 정보이다. 따라서 검증정보가 알려졌다는 사실 자체는 효력 소멸이나 폐지의 사유가 아니다. 제18조 제1항 제4호의 폐지 사유는 공인인증기관이 가입자의 **전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우**이다. 생성정보는 서명을 만드는 개인키이므로, 유출되면 타인이 가입자를 가장하여 서명할 위험이 있다.

③ O: 구 「전자서명법」 제18조 제1항 제3호에 따라 공인인증기관이 가입자의 **사망·실종선고 또는 해산 사실을 인지하면** 공인인증서를 폐지하여야 한다. 사망·실종선고는 자연인, 해산은 법인 등에 관한 사유로서 가입자의 존속과 관련된다.

④ O: 구 「전자서명법」 제18조 제1항 제1호에 따라 **가입자 또는 그 대리인이 폐지를 신청하면** 공인인증기관은 해당 공인인증서를 폐지하여야 한다. 개인키 유출 같은 별도의 사고가 있어야만 신청할 수 있는 것은 아니다.

NoteBase

문 14. 가상사설망(VPN)에 대한 설명으로 옳지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.

② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자 인증의 보안 기능을 제공한다.

③ 네트워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.

④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동 중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

정답 3번

간단한 해설

VPN 터널링은 **OSI 4계층 프로토콜로만 구현해야 하는 것이 아니다**. IPsec처럼 네트워크 계층에서 구현할 수도 있으며, SSH는 TCP 위에서 동작하는 **응용 계층 프로토콜**이다.

선지별 해설

① O: VPN은 인터넷 같은 공중망 위에 논리적인 사설 통신망을 구성하는 기술이다. **기존 공중망을 활용**하므로 지점 사이마다 별도의 전용선을 설치·임대하는 사설망보다 일반적으로 구축비용이 저렴하다.

② O: 보안 VPN은 암호화로 통신 내용을 숨기는 **기밀성**, 전송 중 데이터의 변조 여부를 확인하는 무결성, 접속자가 허용된 사용자인지 확인하는 사용자 인증을 제공한다. 이 기능들을 통해 공중망에서도 안전하게 통신할 수 있다.

③ X: 터널링은 원래의 패킷을 다른 패킷 안에 넣는 캡슐화 등을 통해 네트워크 종단점 사이에 논리적인 통로를 만드는 기능이다. **특정 계층의 프로토콜로만 구현해야 하는 것은 아니며**, 2계층의 L2TP나 3계층의 IPsec 등으로 구현할 수 있다. 또한 SSH는 OSI 4계층 프로토콜이 아니라 TCP 위에서 동작하는 **응용 계층인 7계층의 프로토콜**이다. SSH도 포트 포워딩을 통한 터널링에 활용할 수 있으므로, 터널링 가능 여부와 OSI 계층 분류를 구별해야 한다.

④ O: 원격 접속 VPN은 회사 밖의 사용자가 인터넷을 통해 회사 내부 시스템에 안전하게 접근하도록 한다. 재택근무자나 이동 중인 직원은 **인증을 거쳐 보호된 통신 경로로 접속**하므로 사무실 밖에서도 업무에 필요한 내부 자원을 이용할 수 있다.

NoteBase

문 15. ISO/IEC 27002 보안 통제의 범주에 대한 설명으로 옳지 않은 것은?

① 보안 정책: 비즈니스 요구사항, 관련 법률 및 규정을 준수하여 관리 방향 및 정보 보안 지원을 제공

② 인적 자원 보안: 조직 내의 정보 보안 및 외부자에 의해 사용되는 정보 및 자원 관리

③ 자산 관리: 조직의 자산에 대한 적절한 보호를 성취하고 관리하며, 정보가 적절히 분류될 수 있도록 보장

④ 비즈니스 연속성 관리: 비즈니스 활동에 대한 방해에 대처하고, 중대한 비즈니스 프로세스를 정보 시스템 실패 또는 재난으로부터 보호하며, 정보 시스템의 시의 적절한 재개를 보장

정답 2번

간단한 해설

②의 설명은 **정보보호 조직** 범주에 해당한다. 인적 자원 보안은 **채용 전·재직 중·고용 종료 또는 변경 시** 사람과 관련된 보안 위험을 관리하는 범주이다.

선지별 해설

① O: 보안 정책은 업무 요구사항과 관련 법률·규정을 반영하여 **정보보안의 관리 방향과 경영진의 지원**을 제시한다. 조직이 어떤 원칙과 목표에 따라 정보를 보호할지 정하는 기준이 된다.

② X: 조직 내부의 정보보안을 관리하고 외부자가 접근·처리·관리하는 정보와 정보처리 설비를 보호하는 것은 **정보보호 조직** 범주의 내용이다. 인적 자원 보안은 사람에게서 발생하는 보안 위험을 줄이기 위해 채용 전, 재직 중, 고용 종료 또는 변경 시의 보안 책임과 통제를 다룬다. 채용 전 적격성 확인과 보안 책임의 명시, 재직 중 보안 인식 교육 등이 이에 해당한다.

③ O: 자산 관리는 조직의 자산을 식별하고 보호 책임을 정하여 적절한 보호 수준을 유지하는 범주이다. 정보의 민감도와 중요도 등에 따른 **정보 분류**도 포함되므로, 보호가 더 필요한 정보를 구분하여 그에 맞는 통제를 적용할 수 있다.

④ O: 비즈니스 연속성 관리는 정보 시스템의 중대한 장애나 재난으로 인한 업무 중단에 대비하고 핵심 업무를 보호하는 범주이다. 예방과 복구 대책을 마련하여 피해를 줄이고, 중단된 업무와 이를 지원하는 정보 시스템이 **필요한 시간 안에 재개**되도록 한다.

NoteBase

문 16. OWASP(The Open Web Application Security Project)에서 발표한 2013년도 10대 웹 애플리케이션 보안 위험 중 발생 빈도가 높은 상위 3개에 속하지 않는 것은?

① Injection

② Cross-Site Scripting

③ Unvalidated Redirects and Forwards

④ Broken Authentication and Session Management

정답 3번

간단한 해설

Unvalidated Redirects and Forwards는 2013년 OWASP Top 10의 **A10** 항목으로, 상위 세 항목에 포함되지 않는다.

공통 해설

2013년 OWASP Top 10의 **상위 세 항목은 A1~A3**이다. A1은 Injection(인젝션), A2는 Broken Authentication and Session Management(인증 및 세션 관리 취약점), A3는 Cross-Site Scripting(XSS, 크로스 사이트 스크립팅)이다. 따라서 이 세 명칭은 모두 문항에서 묻는 상위 3개에 속한다.

Unvalidated Redirects and Forwards(검증되지 않은 리다이렉트 및 포워드)는 같은 2013년 목록의 **A10**이다. 10대 보안 위험에는 포함되지만, 상위 3개에는 포함되지 않는다.

NoteBase

문 17. 전자우편의 보안 강화를 위한 S/MIME(Secure/Multipurpose Internet Mail Extension)에 대한 설명으로 옳은 것은?

① 메시지 다이제스트를 수신자의 공개키로 암호화하여 서명한다.

② 메시지를 대칭키로 암호화하고 이 대칭키를 발신자의 개인키로 암호화한 후 암호화된 메시지와 함께 보냄으로써 전자우편의 기밀성을 보장한다.

③ S/MIME를 이용하면 메시지가 항상 암호화되기 때문에 S/MIME 처리 능력이 없는 수신자는 전자우편 내용을 볼 수 없다.

④ 국제 표준 X.509 형식의 공개키 인증서를 사용한다.

정답 4번

간단한 해설

S/MIME는 **X.509 형식의 공개키 인증서**를 사용한다. 이 인증서는 소유자와 공개키의 연결을 증명하여 전자서명 검증이나 암호화에 사용할 공개키를 확인하는 데 쓰인다.

선지별 해설

① X: 메시지 다이제스트는 메시지에 해시함수를 적용하여 얻은 요약값이다. 전자서명은 **발신자의 개인키로 생성**하고, 수신자는 발신자의 공개키로 검증한다. 수신자의 공개키로 암호화하는 것은 발신자의 서명을 만드는 방법이 아니다.

② X: 메시지 자체를 대칭키로 암호화하는 부분은 맞지만, 그 대칭키를 암호화할 때는 발신자의 개인키가 아니라 **수신자의 공개키**를 사용한다. 수신자는 자신의 개인키로 대칭키를 복원한 뒤 메시지를 복호화한다. 발신자의 개인키로 처리하고 공개된 발신자의 공개키로 복원할 수 있게 해서는 수신자만 내용을 읽도록 하는 기밀성을 보장할 수 없다.

③ X: S/MIME는 서명과 암호화 기능을 제공하지만 메시지를 **항상 암호화하는 것은 아니다**. 암호화 없이 서명만 적용할 수도 있다. 특히 본문과 서명을 분리하는 multipart/signed 형식에서는 S/MIME 처리 기능이 없는 수신자도 본문을 읽을 수 있다. 다만 전자서명을 검증하려면 그에 필요한 처리 기능이 있어야 한다.

④ O: S/MIME는 **X.509 형식의 공개키 인증서**를 사용한다. 인증서에는 소유자 정보와 공개키 등이 담기며, 인증기관의 전자서명으로 그 연결을 증명한다. 이를 통해 발신자의 서명을 검증할 공개키나 수신자에게 보낼 메시지를 암호화하는 데 사용할 공개키를 확인한다.

NoteBase

문 18. 국내 정보보호관리체계(ISMS)의 관리 과정 5단계 중 위험 관리 단계의 통제항목에 해당하지 않는 것은?

① 위험 관리 방법 및 계획 수립

② 정보보호 대책 선정 및 이행 계획 수립

③ 정보보호 대책의 효과적 구현

④ 위험 식별 및 평가

정답 3번

간단한 해설

'정보보호 대책의 효과적 구현'은 **정보보호대책 구현 단계**의 통제항목이다. 위험관리 단계에서는 위험을 식별·평가하고, 필요한 대책을 선정하여 **이행계획을 수립**한다.

공통 해설

문제에서 제시한 ISMS 5단계 체계에서 위험관리는 위험을 파악하고 수용 가능한 수준으로 줄이기 위한 대책과 실행계획을 정하는 과정이다. 따라서 위험관리 방법과 수행계획을 정하는 '위험 관리 방법 및 계획 수립', 보호할 정보자산의 위협·취약성과 위험수준을 파악하는 '위험 식별 및 평가', 평가 결과에 따라 보호대책과 구현 우선순위·일정·담당자·예산 등을 정하는 '정보보호 대책 선정 및 이행 계획 수립'이 여기에 포함된다. 대책을 실제 적용할 방법과 일정을 정하는 **이행계획 수립까지 위험관리**에 속한다.

'정보보호 대책의 효과적 구현'은 수립된 이행계획에 따라 보호대책을 실제 적용하는 활동이므로 **정보보호대책 구현 단계**에 속한다. 이 단계에서는 경영진이 이행 결과의 정확성과 효과성도 확인한다. 즉, 위험관리에서 결정한 대책을 실제로 실행한다는 점에서 위험관리 단계의 통제항목과 구별된다.

NoteBase

문 19. 공개키 기반 전자서명에서 메시지에 서명하지 않고 메시지의 해시값과 같은 메시지 다이제스트에 서명하는 이유는?

① 공개키 암호화에 따른 성능 저하를 극복하기 위한 것이다.

② 서명자의 공개키를 쉽게 찾을 수 있도록 하기 위한 것이다.

③ 서명 재사용을 위한 것이다.

④ 원본 메시지가 없어도 서명을 검증할 수 있도록 하기 위한 것이다.

정답 1번

간단한 해설

공개키 방식의 서명 연산은 계산 부담이 크므로, 긴 메시지를 직접 처리하는 대신 **짧고 고정된 길이의 해시값**에 서명하여 처리 효율을 높인다. 해시는 메시지 전체를 빠르게 처리하면서 비용이 큰 서명 연산에 입력할 데이터의 양을 줄여 준다.

선지별 해설

① O: 공개키 암호 방식의 연산은 해시 연산보다 계산 부담이 크다. 메시지를 해시함수로 처리하여 고정 길이의 다이제스트를 만든 뒤 여기에 서명하면, 긴 메시지 전체에 비용이 큰 연산을 적용하는 부담을 줄일 수 있다. 따라서 다이제스트에 서명하는 것은 **서명 처리의 효율을 높이기 위한 것**이다. 이때 서명은 서명자의 개인키로 생성하고 공개키로 검증한다.

② X: 해시함수는 메시지를 다이제스트로 바꾸는 기능을 하며, 서명자의 공개키를 찾아 주지는 않는다. 공개키의 입수와 소유자 확인에는 **인증서 등 공개키를 배포하고 인증하는 수단**을 이용한다. 다이제스트에 서명하는 이유는 공개키 검색의 편의가 아니라 연산 부담을 줄이는 데 있다.

③ X: 서명은 해당 메시지의 다이제스트에 연결되므로, 다른 다이제스트를 가진 메시지에 기존 서명을 그대로 적용하면 검증을 통과하지 못한다. 다이제스트에 서명하는 목적은 **서명을 다른 메시지에 재사용하는 것이 아니라** 메시지에 대한 서명을 효율적으로 생성하고 검증하는 데 있다.

④ X: 특정 메시지에 대한 서명을 검증하려면 그 메시지와 서명이 대응하는지 확인해야 한다. 일반적인 검증자는 **받은 메시지의 해시값을 다시 계산**하고 서명자의 공개키를 이용하여 서명을 검증한다. 다이제스트에 서명한다고 원본 메시지 없이 그 내용의 변조 여부까지 확인할 수 있는 것은 아니다.

NoteBase

문 20. 윈도우즈에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 옳지 않은 것은?

① route : 라우팅 테이블의 정보 확인

② netstat : 연결 포트 등의 네트워크 상태 정보 확인

③ tracert : 네트워크 목적지까지의 경로 정보 확인

④ nslookup : 사용자 계정 정보 확인

정답 4번

간단한 해설

nslookup은 사용자 계정이 아니라 **DNS 정보**를 조회하는 명령어이다. 도메인 이름에 대응하는 IP 주소 등을 확인할 때 사용한다.

선지별 해설

① O: route는 컴퓨터의 **IP 라우팅 테이블**을 확인하거나 수정하는 명령어이다. route print로 목적지 네트워크, 게이트웨이 등 경로 선택에 쓰이는 정보를 확인할 수 있다.

② O: netstat는 **활성 연결과 포트 등 네트워크 상태**를 확인하는 명령어이다. TCP 연결의 로컬·원격 주소와 포트 번호, 연결 상태 등을 표시하며, -a 옵션을 사용하면 연결을 기다리는 포트도 확인할 수 있다.

③ O: tracert는 **목적지까지 거치는 경로**를 추적하는 명령어이다. 패킷의 TTL 값을 차례로 늘려 보내고 중간 라우터의 응답을 이용하여 경로 정보를 확인한다. route가 로컬 라우팅 테이블을 조회하는 것과 구별된다.

④ X: nslookup은 **DNS 서버에 질의하여 도메인 이름과 IP 주소 등 DNS 정보**를 조회하는 명령어이다. 예를 들어 도메인 이름을 지정하면 그 이름에 대응하는 IP 주소를 확인할 수 있다. 따라서 '사용자 계정 정보 확인'은 'DNS 정보 확인'으로 고쳐야 한다.

NoteBase