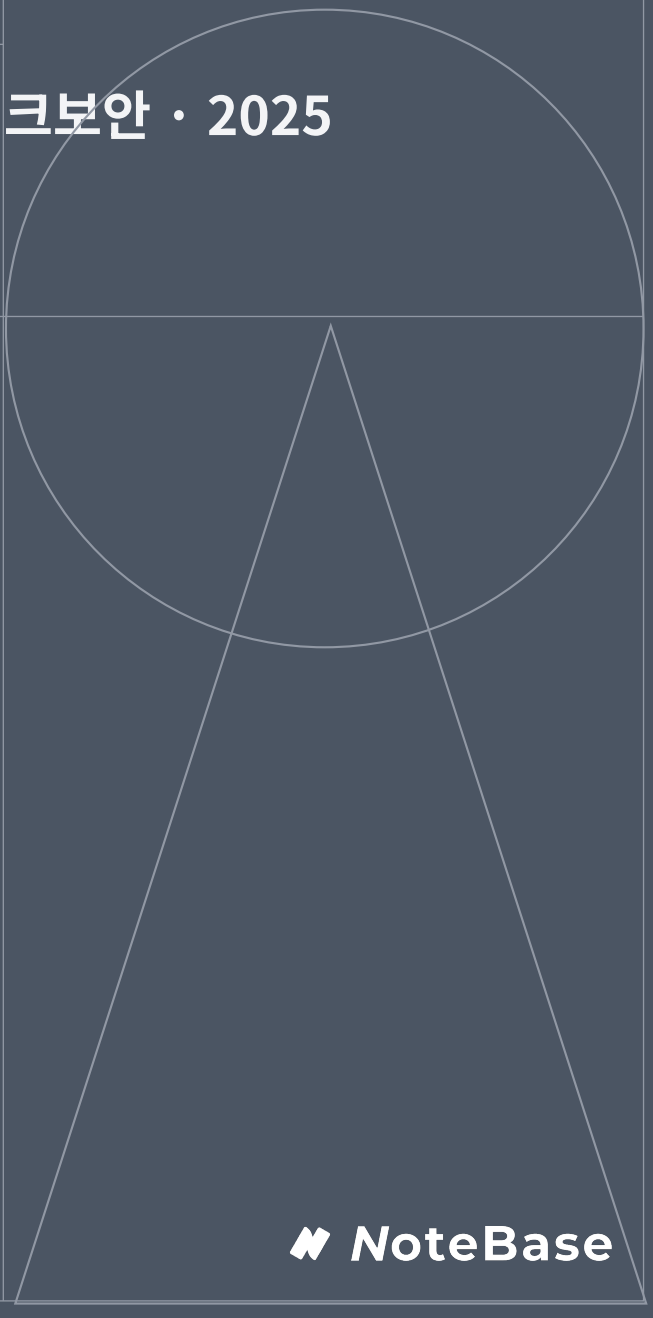
기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2025



NoteBase

기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2025

공무원/군무원/9급 · 네트워크보안 · 2025

1. 최근 사이버 공격자들이 서비스형 랜섬웨어를 활용하는 주된 이유에 대한 설명으로 가장 적절한 것은?
   ① 자체적인 랜섬웨어 개발 능력이 부족해도 쉽게 공격을 실행할 수 있기 때문이다.
   ② 암호화된 데이터의 복호화 키를 안전하게 관리하기 위해서이다.
   ③ 공격 대상 시스템의 취약점을 분석하는 시간을 단축하기 위해서이다.
   ④ 법적 추적을 피하기 위해 익명성을 강화하는 효과가 있기 때문이다.

정답 1번

출제 포인트

서비스형 랜섬웨어가 확산되는 핵심 이유인 공격의 진입장벽 완화를 이해하는지를 묻는 문제이다.

핵심 개념

서비스형 랜섬웨어(RaaS)는 개발·운영자가 랜섬웨어 도구와 공격 인프라를 서비스 형태로 제공하고, 제휴 공격자가 이를 이용해 공격한 뒤 수익을 나누는 모델이다. 제휴 공격자는 랜섬웨어를 직접 개발할 능력이 부족해도 준비된 도구를 이용할 수 있으므로 공격 참여가 쉬워진다.

NoteBase

선지별 해설

① O — RaaS는 이미 개발된 랜섬웨어와 운영 인프라를 제공하므로 자체 개발 능력이 부족한 공격자도 비교적 쉽게 공격을 실행할 수 있다.
② X — 틀린 표현은 '복호화 키를 안전하게 관리하기 위해서'이다. RaaS 활용의 주된 이유는 피해자 데이터의 복호화 키를 보호하는 것이 아니라, 공격 도구와 인프라를 빌려 기술적 진입장벽을 낮추는 데 있다.
③ X — 틀린 표현은 '공격 대상 시스템의 취약점을 분석하는 시간을 단축하기 위해서'이다. RaaS의 핵심 기능은 랜섬웨어의 제공·배포·운영 지원이며, 모든 공격 대상의 취약점 분석 시간을 자동으로 단축하는 것이 주된 활용 이유는 아니다. 올바르게는 준비된 랜섬웨어와 인프라를 이용해 개발 및 운영 부담을 줄인다고 해야 한다.
④ X — 틀린 표현은 '법적 추적을 피하기 위해 익명성을 강화하는 효과'가 주된 이유라는 부분이다. 공격자가 익명화 수단을 함께 사용할 수는 있지만, RaaS가 널리 활용되는 대표적 이유는 익명성 자체보다 비전문가도 공격에 참여할 수 있도록 도구와 서비스를 제공한다는 점이다.

오답 포인트

②의 키 관리, ③의 취약점 분석, ④의 익명성은 사이버 공격 과정에서 연관될 수 있는 요소이지만 RaaS의 본질적 확산 이유는 아니다. '서비스형'이라는 표현에서 공격 도구와 인프라의 제공, 기술 진입장벽의 하락을 찾아야 한다.

다시 나오면 이렇게 판단

RaaS의 활용 이유를 물으면 공격자가 직접 랜섬웨어를 개발해야 하는지부터 판단한다. 개발·운영자가 도구와 인프라를 제공하고 제휴 공격자가 이를 이용한다면 핵심 효과는 개발 부담 감소와 공격 진입장벽 완화이다.

암기 포인트

RaaS는 랜섬웨어의 서비스화이며, 핵심은 비전문 공격자도 참여하게 만드는 진입장벽의 하락이다.

NoteBase

2. CIDR에 대한 설명으로 가장 적절하지 않은 것은?
① IPv4의 주소 클래스를 사용하지 않는다.
② '/' 문자를 통해 네트워크 ID의 길이를 표시한다.
③ 접두어 합침을 통해 라우팅 테이블이 유지해야 하는 정보의 수를 클래스 기반 주소 지정에 비해 감소시킨다.
④ IPv6 주소 클래스 단위로 주소를 할당한다.

정답 4번

출제 포인트

CIDR의 클래스리스 주소 지정, 프리픽스 길이 표기, 경로 집약의 효과와 IPv6 주소 할당 방식을 구분하는 문제이다.

핵심 개념

CIDR(Classless Inter-Domain Routing)는 고정된 IPv4 주소 클래스 A·B·C를 사용하지 않고, 주소 뒤의 /n으로 네트워크 프리픽스의 비트 수를 나타내는 클래스리스 주소 지정·라우팅 방식이다. 연속된 여러 네트워크를 하나의 더 짧은 프리픽스로 집약할 수 있어 라우팅 테이블의 경로 수를 줄인다. IPv6도 주소 클래스 단위가 아니라 프리픽스 길이를 기준으로 주소 범위를 할당하고 경로를 표현한다.

선지별 해설

① O — CIDR는 IPv4의 고정 주소 클래스 구분을 사용하지 않고 필요한 규모에 맞는 프리픽스 길이로 네트워크를 지정한다.
② O — / 뒤의 수는 주소에서 네트워크 프리픽스로 사용하는 비트 수, 즉 네트워크 ID 부분의 길이를 나타낸다. 예를 들어 /24는 앞 24비트가 네트워크 프리픽스라는 뜻이다.
③ O — CIDR의 경로 집약은 조건을 만족하는 연속 네트워크들을 하나의 프리픽스로 광고하게 하므로, 클래스 기반 주소 지정에 비해 라우팅 테이블이 유지할 경로 정보의 수를 줄일 수 있다.
④ X — 틀린 표현은 'IPv6 주소 클래스 단위로 주소를 할당한다'이다. IPv6에는 A·B·C와 같은 주소 클래스가 없으며, 올바르게는 'IPv6 주소도 클래스 단위가 아니라 프리픽스 길이를 기준으로 할당한다'이다.

오답 포인트

'CIDR가 IPv4에서 등장했다'는 사실을 'IPv6는 클래스 단위로 할당한다'는 뜻으로 오해하기 쉽다. IPv4의 옛 클래스 체계와 IPv6의 주소 할당 방식을 섞은 ④의 표현이 함정이다.

NoteBase

다시 나오면 이렇게 판단

CIDR 선지는 '클래스 미사용', '/n은 프리픽스 비트 수', '경로 집약으로 라우팅 정보 감소'인지 확인한다. IPv6에 주소 클래스 A·B·C를 적용하는 표현은 틀린 것으로 판단한다.

암기 포인트

CIDR는 Classless, /n은 프리픽스 길이, 집약은 경로 수 감소이다. IPv6도 클래스가 아니라 프리픽스를 사용한다.

NoteBase

3. 다음 설명으로 가장 적절한 것은?

- 개별 시스템에 설치되어 해당 장비에 대한 직접적인 접근제어를 제공한다.
- OS 레벨에서 동작하며 일반적으로 SW 기반으로 구현된다.
- Windows Defender, iptables 등이 대표적이다.

① 경계형 방화벽 ② 내부 방화벽
③ 이중 방화벽 ④ 호스트 기반 방화벽

정답 4번

출제 포인트

개별 시스템에 설치되어 해당 장비의 트래픽과 접근을 직접 통제하는 방화벽 유형을 구별하는 문제이다.

핵심 개념

호스트 기반 방화벽: PC나 서버 같은 개별 시스템에 설치되어 그 시스템으로 들어오고 나가는 통신을 OS 수준에서 통제하는 방화벽이다. 키워드는 '개별 시스템 설치', 'OS 레벨', '소프트웨어 기반'이다.
경계형 방화벽: 내부망과 외부망의 경계에서 두 네트워크 사이의 트래픽을 통제한다.
내부 방화벽: 조직 내부의 네트워크 구간 사이에 설치되어 내부망을 분리하고 구간 간 이동을 통제한다.
이중 방화벽: 두 방화벽을 계층적으로 배치하여 외부망·DMZ·내부망 사이를 단계적으로 보호하는 구성이다.

선지별 해설

① X — 경계형 방화벽은 내부망과 외부망의 경계에서 네트워크 간 트래픽을 통제한다. 틀린 부분은 지문의 '개별 시스템에 설치'라는 특징을 경계형 방화벽으로 본 것이다. 올바르게는 '내부망과 외부망의 경계에 설치되는 방화벽'이다.
② X — 내부 방화벽은 조직 내부의 네트워크 구간이나 보안 영역 사이에 배치된다. 틀린 부분은 개별 장비의 OS에서 동작하는 방화벽을 내부 방화벽으로 본 것이다. 올바르게는 '내부망의 구간을 분리하고 구간 간 트래픽을 통제하는 방화벽'이다.
③ X — 이중 방화벽은 두 개의 방화벽을 계층적으로 배치하여 여러 경계를 단계적으로 보호하는 구성이다. 틀린 부분은 단일 개별 시스템에 설치되는 소프트웨어 방화벽을 이중 방화벽으로 본 것이다. 올바르게는 '두 방화벽을 이용해 외부망·DMZ·내부망을 단계적으로 분리하는 구성'이다.
④ O — 호스트 기반 방화벽은 각 PC나 서버에 설치되어 해당 시스템의 통신을 OS 수준에서 직접 제어한다. Windows Defender 방화벽과 iptables는 이러한 소프트웨어 기반 호스트 방화벽의 대표적인 예이다.

NoteBase

오답 포인트

‘내부에 설치된다’는 인상만으로 ② 내부 방화벽을 고르기 쉽다. 그러나 지문의 결정적 표현은 단순히 내부에 있다는 뜻이 아니라 ‘개별 시스템에 설치’되고 ‘OS 레벨에서 동작’한다는 점이다. 이는 네트워크 구간을 보호하는 내부 방화벽이 아니라 한 대의 호스트를 보호하는 방화벽을 뜻한다.

다시 나오면 이렇게 판단

설치 위치와 보호 단위를 함께 본다. 개별 PC·서버와 OS가 기준이면 호스트 기반, 내부망과 외부망의 접점이면 경계형, 내부 네트워크 구간 사이이면 내부 방화벽, 두 방화벽의 계층적 배치이면 이중 방화벽이다.

암기 포인트

한 대의 장비·OS·Windows Defender·iptables가 보이면 호스트 기반 방화벽이다.

NoteBase

4. 다음 설명의 보안 공격 기법으로 가장 적절한 것은?

> 한 사용자는 어느 블로그 댓글 입력창에 글을 작성했다. 그런데 해당 입력창에 숨겨진 악성 스크립트가 삽입되어 있었고, 사용자가 댓글을 등록하자마자 그의 브라우저에서 스크립트가 실행되어 쿠키 정보가 공격자에게 전송되었다.

① SQL 인젝션(SQL Injection)
② 사이트 간 스크립팅(Cross Site Scripting)
③ 무차별 대입 공격(Brute Force Attack)
④ 사이트 간 요청 위조(Cross Site Request Forgery)

정답 2번

출제 포인트

이 문제는 웹 입력창에 삽입된 악성 스크립트가 다른 사용자의 브라우저에서 실행되는 사례를 사이트 간 스크립팅(XSS)으로 판단할 수 있는지를 묻는 문제이다.

사례 정리

핵심 사실 1: 블로그 댓글 입력창에 악성 스크립트가 삽입되어 있었다.
핵심 사실 2: 사용자가 댓글을 등록하자 브라우저에서 그 스크립트가 실행되었다.
판단에 중요한 조건: 브라우저에서 실행된 스크립트가 쿠키 정보를 공격자에게 전송했다.

핵심 개념

사이트 간 스크립팅(XSS)은 공격자가 웹 페이지에 악성 스크립트를 삽입하여 그 페이지를 이용하는 사용자의 브라우저에서 실행되게 하는 공격이다.
적용 요건은 신뢰할 수 없는 입력이 적절히 검증·인코딩되지 않은 채 페이지에 포함되고, 피해자의 브라우저가 이를 스크립트로 해석하여 실행하는 것이다. 이 사례처럼 댓글에 저장된 스크립트가 실행되는 형태는 저장형 XSS에 해당한다.

적용 기준

공격 코드가 어디에서 실행되고 무엇을 조작하는지를 기준으로 판단한다. 사용자 브라우저에서 삽입된 스크립트가 실행되어 쿠키를 탈취했다는 점이 XSS의 결정적 특징이다.

NoteBase

선지별 해설

① X — SQL 인젝션은 검증되지 않은 입력으로 SQL 구문을 변형하여 데이터베이스를 조회·변경하는 공격이다. 이 사례는 데이터베이스 질의가 아니라 브라우저에서 악성 스크립트가 실행되었으므로 해당하지 않는다. 틀린 표현 'SQL 인젝션'은 '사이트 간 스크립팅(XSS)'으로 고쳐야 한다.
② O — 댓글 입력창에 삽입된 악성 스크립트가 사용자의 브라우저에서 실행되어 쿠키를 공격자에게 전송했으므로 사이트 간 스크립팅(XSS), 그중 저장형 XSS에 해당한다.
③ X — 무차별 대입 공격은 가능한 비밀번호나 키 값을 반복적으로 시도하여 인증 정보를 알아내는 공격이다. 이 사례에는 반복 추측이나 로그인 시도가 없다. 틀린 표현 '무차별 대입 공격'은 '사이트 간 스크립팅(XSS)'으로 고쳐야 한다.
④ X — 사이트 간 요청 위조(CSRF)는 인증된 사용자의 브라우저가 공격자가 의도한 요청을 대상 사이트에 보내도록 속이는 공격이다. 이 사례의 핵심은 원치 않는 요청 전송이 아니라 삽입된 스크립트의 실행과 쿠키 탈취이다. 틀린 표현 '사이트 간 요청 위조'는 '사이트 간 스크립팅(XSS)'으로 고쳐야 한다.

오답 포인트

쿠키가 공격자에게 전송되었다는 결과만 보고 CSRF로 혼동하기 쉽다. 그러나 이 문항의 실제 단서는 '입력창에 숨겨진 악성 스크립트'와 '브라우저에서 스크립트가 실행'되었다는 표현이다. 이는 XSS를 직접 가리킨다.

다시 나오면 이렇게 판단

브라우저에서 삽입 코드가 실행되면 XSS, 입력값이 SQL 질의를 바꾸면 SQL 인젝션, 인증값을 반복 추측하면 무차별 대입, 로그인 상태를 악용해 원치 않는 요청을 보내게 하면 CSRF로 판단한다.

암기 포인트

스크립트 실행은 XSS, SQL 조작은 SQL 인젝션, 반복 추측은 무차별 대입, 요청 강요는 CSRF이다.

NoteBase

5. ARP를 악용한 해킹처럼 동일한 네트워크에서 메시지를 몰래 가로채는 중간자 공격이 주로 발생하는 OSI 참조 모델의 계층은?
① 데이터 링크 계층 ② 네트워크 계층
③ 전송 계층 ④ 세션 계층

정답 1번

출제 포인트

ARP 스푸핑이 IP 주소와 MAC 주소의 대응 관계를 조작하여 같은 네트워크의 프레임 전달 경로를 가로채는 공격이라는 점을 묻는 문제이다.

핵심 개념

ARP는 같은 네트워크에서 목적지 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 공격자가 위조된 ARP 정보를 보내 ARP 캐시의 IP-MAC 대응 관계를 오염시키면, 피해자가 보낸 이더넷 프레임이 공격자의 MAC 주소로 전달되어 중간자 공격이 가능해진다. 따라서 ARP 스푸핑은 주로 데이터 링크 계층 공격으로 분류한다.
계층 대비: 데이터 링크 계층은 MAC 주소와 프레임 전달을 담당하고, 네트워크 계층은 IP 주소와 패킷 경로 선택을 담당하며, 전송 계층은 종단 간 데이터 전송을 담당하고, 세션 계층은 응용 프로그램 사이의 세션 설정·유지·종료를 담당한다.

선지별 해설

① O — ARP 스푸핑은 위조된 ARP 정보로 IP-MAC 대응 관계를 변조하여 이더넷 프레임의 전달 대상을 공격자의 MAC 주소로 바꾸므로 주로 데이터 링크 계층에서 발생한다.
② X — 틀린 표현은 '네트워크 계층'이다. 네트워크 계층은 IP 주소 지정과 라우팅을 담당하지만, 이 공격이 직접 조작하는 것은 ARP 캐시의 MAC 주소 대응 관계이므로 올바르게는 '데이터 링크 계층'이다.
③ X — 틀린 표현은 '전송 계층'이다. 전송 계층은 TCP·UDP를 이용한 종단 간 전송, 포트 구분, 신뢰성 등을 담당하며 ARP 스푸핑의 주된 발생 계층이 아니다. 올바르게는 '데이터 링크 계층'이다.
④ X — 틀린 표현은 '세션 계층'이다. 세션 계층은 통신 세션의 설정·유지·종료를 담당하며 ARP 캐시나 MAC 주소 대응 관계를 처리하지 않는다. 올바르게는 '데이터 링크 계층'이다.

오답 포인트

ARP가 IP 주소를 입력으로 사용하므로 ② 네트워크 계층으로 착각하기 쉽다. 그러나 공격의 직접적인 표적은 IP 주소 자체나 라우팅 경로가 아니라 같은 네트워크에서 사용하는 IP-MAC 대응 관계이며, 실제로 바뀌는 프레임의 수신 MAC 주소가 핵심이다.

NoteBase

다시 나오면 이렇게 판단

공격이 직접 변조하는 주소와 데이터 단위를 확인한다. MAC 주소·ARP 캐시·이더넷 프레임이 핵심이면 데이터 링크 계층, IP 주소·라우팅·패킷 경로가 핵심이면 네트워크 계층으로 판단한다.

암기 포인트

ARP 스푸핑은 IP-MAC 대응표를 속여 프레임을 가로채는 데이터 링크 계층 공격이다.

NoteBase

6. DNS 프로토콜의 보안 취약점을 해결하기 위해 도입된 DNSSEC이 제공하는 주요 보안 기능에 대한 설명으로 가장 적절한 것은?
① DNS 질의 및 응답 메시지 암호화
② DNS 서버 간 영역 전송 암호화
③ DNS 데이터의 무결성 및 출처 인증 보장
④ DNS 서버 자체의 가용성 보장

정답 3번

출제 포인트

DNSSEC이 DNS 데이터에 제공하는 보안 속성과 제공하지 않는 속성을 구분하는 문제이다.

핵심 개념

DNSSEC은 DNS 응답에 전자서명을 적용하여 데이터가 변조되지 않았는지와 신뢰할 수 있는 출처에서 제공되었는지를 검증하는 기술이다. 핵심 보안 속성은 무결성과 출처 인증이며, 데이터의 기밀성이나 DNS 서버의 가용성을 보장하는 기술은 아니다.

선지별 해설

① X — ‘DNS 질의 및 응답 메시지 암호화’가 틀린 표현이다. DNSSEC은 전자서명을 통해 응답을 검증하지만 질의·응답 내용 자체를 암호화하지는 않는다. 올바르게는 ‘DNS 데이터의 무결성과 출처를 검증한다’이다.
② X — ‘DNS 서버 간 영역 전송 암호화’가 틀린 표현이다. DNSSEC의 목적은 영역 전송 경로를 암호화하는 것이 아니라 배포된 DNS 데이터의 전자서명을 검증하는 것이다. 올바르게는 ‘영역 전송 암호화는 DNSSEC의 주요 보안 기능이 아니다’이다.
③ O — DNSSEC은 서명된 DNS 레코드를 검증하여 DNS 데이터가 변조되지 않았다는 무결성과 해당 데이터가 정당한 출처에서 왔다는 출처 인증을 보장한다.
④ X — ‘DNS 서버 자체의 가용성 보장’이 틀린 표현이다. DNSSEC은 서버 장애나 서비스 거부 공격을 막아 서버를 계속 이용할 수 있게 하는 기술이 아니다. 올바르게는 ‘DNSSEC은 DNS 데이터의 무결성과 출처 인증을 제공한다’이다.

오답 포인트

‘보안’이라는 표현만 보고 암호화나 가용성까지 제공한다고 넓게 해석하기 쉽다. DNSSEC의 전자서명은 데이터의 진위와 변조 여부를 확인하지만, DNS 메시지의 내용을 숨기거나 서버의 정상 운영을 보장하지 않는다.

NoteBase

다시 나오면 이렇게 판단

DNSSEC 선지는 '전자서명으로 데이터의 무결성과 출처를 인증하는가'를 기준으로 판단한다. 질의·응답 또는 영역 전송의 암호화, 서버 가용성 보장은 DNSSEC의 핵심 기능에서 제외한다.

암기 포인트

DNSSEC은 서명으로 무결성·출처 인증을 제공하며, 암호화·가용성은 보장하지 않는다.

NoteBase

7. Advanced, Persistent, Threats는 APT를 정의하는 세 가지 핵심 요소다. 'Persistent'가 의미하는 바에 대한 설명으로 가장 적절한 것은?
① 공격자가 최신 기술을 사용하여 공격한다.
② 공격 배후에 숙련되고 목적의식이 뚜렷한 주체가 있다.
③ 공격자가 탐지를 회피하며 장기간에 걸쳐 시스템에 침입 상태를 유지한다.
④ 공격이 일회성으로 끝나지만 피해 규모가 크다.

정답 3번

출제 포인트

이 문제는 APT(Advanced Persistent Threats)의 세 핵심 요소 중 Persistent가 뜻하는 지속성의 개념을 묻는다.

핵심 개념

Advanced: 지능적이고 고도화된 공격 기법을 활용한다는 뜻이다. 반드시 최신 기술만을 사용한다는 의미는 아니다.
Persistent: 탐지를 피하면서 목표 시스템에 장기간 접근하거나 침투 상태를 유지한다는 뜻이다.
Threats: 공격 능력과 의도 및 구체적인 목적을 가진 위협 주체가 공격한다는 뜻이다.
세 요소는 각각 공격 기법의 고도성, 활동의 지속성, 위협 주체의 능력·의도를 가리킨다.

선지별 해설

① X — '최신 기술을 사용'한다는 표현은 Persistent의 의미가 아니며, Advanced도 반드시 최신 기술만을 뜻하지 않는다. 올바르게는 '공격자가 지능적이고 고도화된 공격 기법을 사용한다'라고 해야 한다.
② X — '숙련되고 목적의식이 뚜렷한 주체'는 공격 능력과 의도를 지닌 Threats의 측면을 설명한다. Persistent에 맞게 고치면 '공격자가 목표 시스템에 대한 접근과 침투 활동을 장기간 지속한다'가 된다.
③ O — 탐지를 회피하면서 장기간 시스템 침입 상태를 유지한다는 설명은 Persistent의 지속적·장기적 활동을 정확히 나타낸다.
④ X — '공격이 일회성으로 끝난다'는 부분이 Persistent와 반대이다. 올바르게는 '공격자가 탐지를 피하며 장기간 반복적으로 활동하거나 침투 상태를 유지한다'라고 해야 하며, 피해 규모의 크기는 Persistent를 판별하는 기준이 아니다.

NoteBase

오답 포인트

①의 '최신 기술', ②의 '숙련된 목적 지향적 주체'처럼 APT의 다른 요소와 관련된 표현을 Persistent의 뜻으로 혼동하기 쉽다. 또한 ④의 '피해 규모가 크다'에 끌릴 수 있지만, Persistent의 판단 기준은 피해의 크기가 아니라 공격 활동과 침투 상태의 장기적 지속 여부이다.

다시 나오면 이렇게 판단

APT의 각 단어가 묻는 판단축을 구분한다. 공격 기법의 고도성은 Advanced, 공격의 장기적 유지·반복은 Persistent, 공격 주체의 능력·의도·목적은 Threats에 해당한다. Persistent가 나오면 '장기간', '지속', '잠복', '탐지 회피', '침투 상태 유지'라는 표현을 찾는다.

암기 포인트

Advanced는 고도화, Persistent는 장기 지속, Threats는 능력과 의도를 가진 위협 주체이다.

NoteBase

8. 애플리케이션 게이트웨이에 대한 설명으로 적절하지 않은 것은?
① 응용 계층에서 동작한다.
② 프로토콜별로 Proxy Daemon이 필요하다.
③ 응용 프로그램 사용을 기록하여 사용자 및 응용 서비스 접근제어를 제공한다.
④ 처리 속도가 빠르고, 다양한 서비스에 대한 유연성을 제공한다.

정답 4번

출제 포인트

애플리케이션 게이트웨이의 동작 계층, 프로토콜별 프록시 구조, 장점과 한계를 구분하는 문제이다.

핵심 개념

애플리케이션 게이트웨이는 응용 계층에서 클라이언트와 서버 사이의 연결을 대신 중계하면서 응용 프로토콜의 내용을 검사하고 접근을 통제하는 방화벽이다. 프로토콜별 프록시를 이용하므로 세밀한 제어와 기록이 가능하지만, 처리 부담이 크고 지원할 서비스마다 별도 프록시가 필요하여 속도와 유연성에는 한계가 있다.

선지별 해설

① O — 애플리케이션 게이트웨이는 OSI 응용 계층에서 동작하며 응용 프로토콜의 명령과 데이터까지 검사할 수 있다.
② O — HTTP, FTP 등 응용 프로토콜마다 그 프로토콜을 이해하고 중계하는 Proxy Daemon이 필요하다.
③ O — 프록시를 거치는 응용 프로그램의 사용 내역을 기록할 수 있고, 사용자와 응용 서비스 단위로 세밀한 접근제어를 제공할 수 있다.
④ X — 틀린 표현은 '처리 속도가 빠르고, 다양한 서비스에 대한 유연성을 제공한다'이다. 올바르게는 응용 계층의 내용을 검사하고 중계하므로 처리 속도가 상대적으로 느리며, 서비스별 Proxy Daemon이 필요하므로 새로운 서비스에 대한 유연성이 낮다고 해야 한다.

오답 포인트

애플리케이션 게이트웨이가 세밀하고 강력한 보안을 제공한다는 장점을 성능과 유연성까지 높다는 뜻으로 확대하면 ④를 놓치기 쉽다. 정밀한 검사에는 처리 부담이 따르고, 프로토콜별 프록시 구조에는 지원 서비스의 제약이 따른다.

NoteBase

다시 나오면 이렇게 판단

‘응용 계층·프로토콜별 프록시·사용 기록·세밀한 접근제어’는 애플리케이션 게이트웨이의 특징으로 판단한다. 반대로 ‘빠른 처리·다양한 서비스에 대한 높은 유연성’은 프로토콜별 중계와 검사에 따른 한계에 어긋나는 표현으로 판단한다.

암기 포인트

애플리케이션 게이트웨이는 응용 계층에서 정밀하게 검사하지만, 프로토콜별 프록시가 필요하여 느리고 유연성이 낮다.

NoteBase

9. 보안사고 대응 절차 중 사고 상황을 문서화하고 전문 인력에게 보고한 후 신속히 조치 조직을 가동하며 관계 부서에도 공식적으로 통보하는 단계로 가장 적절한 것은?
① 사고 탐지 ② 초기 대응
③ 사고 조사 ④ 해결

정답 2번

출제 포인트

이 문제는 보안사고 대응 절차에서 상황을 문서화·보고한 뒤 대응 조직을 가동하고 관계 부서에 공식 통보하는 단계가 무엇인지 묻는다.

올바른 순서

1. 사고 탐지 — 이상 징후와 보안사고 발생 여부를 식별한다.
2. 초기 대응 — 사고 상황을 문서화하여 전문 인력에게 보고하고, 대응 조직을 신속히 가동하며, 관계 부서에 공식 통보한다.
3. 사고 조사 — 사고 원인, 침해 범위, 피해 내용과 증거를 구체적으로 분석한다.
4. 해결 — 조사 결과를 토대로 사고를 복구하고 취약점을 보완하여 재발을 방지한다.

왜 이 순서인가: 사고를 먼저 탐지해야 대응 체계를 가동할 수 있고, 초기 대응으로 상황을 통제하고 정보를 공유한 뒤에 상세 조사와 복구·개선이 이어지기 때문이다.

NoteBase

선지별 해설

① 사고 탐지 X
사고 탐지는 이상 징후를 확인하고 사고 발생 여부를 식별하는 단계이다. 제시문의 '문서화·전문 인력 보고·대응 조직 가동·관계 부서 공식 통보'는 탐지 이후의 조치이다.
틀린 표현 '사고 탐지' → 올바르게는 '초기 대응'이다.

② 초기 대응 O
사고 상황을 기록하고 전문 인력에게 보고하며, 신속하게 대응 조직을 가동하고 관계 부서에 통보하는 활동은 사고 확산을 막고 후속 조치를 준비하는 초기 대응에 해당한다.

③ 사고 조사 X
사고 조사는 원인, 침해 경로, 영향 범위, 피해 규모와 증거를 분석하는 단계이다. 제시문은 상세 원인 분석보다 보고·조직 가동·공식 통보에 초점이 있다.
틀린 표현 '사고 조사' → 올바르게는 '초기 대응'이다.

④ 해결 X
해결은 사고를 복구하고 취약점을 제거하며 재발 방지 대책을 적용하는 단계이다. 제시문에는 복구나 취약점 보완이 아니라 대응 체계의 가동과 통보가 나타난다.
틀린 표현 '해결' → 올바르게는 '초기 대응'이다.

오답 포인트

'사고 상황을 문서화한다'는 표현만 보고 사고 조사로 오인하기 쉽다. 그러나 전문 인력 보고, 대응 조직 가동, 관계 부서 공식 통보가 함께 제시되면 상세 분석 단계가 아니라 초동 조치를 수행하는 초기 대응 단계이다.

다시 나오면 이렇게 판단

절차형 문제는 활동의 핵심 동사를 기준으로 구분한다. 이상 징후 확인은 사고 탐지, 보고·조직 가동·통보는 초기 대응, 원인·범위·증거 분석은 사고 조사, 복구·보완·재발 방지는 해결로 판단한다.

암기 포인트

탐지는 발견, 초기 대응은 보고·가동·통보, 조사는 분석, 해결은 복구·보완이다.

NoteBase

10. SSH의 전송 계층 프로토콜 동작 과정으로 적절하지 않은 것은?
① 서버가 클라이언트에게 개인키를 전송하여 서버 인증
② 클라이언트와 서버 간 키 교환
③ 클라이언트와 서버가 SSH 버전 정보 교환
④ 암호화, MAC, 압축 방식 협의

정답 1번

출제 포인트

SSH 전송 계층 프로토콜에서 버전 교환, 알고리즘 협상, 키 교환과 서버 인증이 어떻게 이루어지는지를 묻는 문제이다.

올바른 순서

1. 프로토콜 버전 정보 교환 — 클라이언트와 서버가 각자의 식별 문자열을 보낸다.
2. 알고리즘 협상 — 키 교환, 서버 호스트 키, 암호화, MAC, 압축 방식을 협의한다.
3. 키 교환 및 서버 인증 — 공유 비밀을 만들고, 서버는 호스트 공개키와 개인키로 생성한 서명을 제공한다. 클라이언트는 공개키로 서명을 검증한다.
4. 새 키 적용 — 합의한 키와 알고리즘을 이후 통신에 적용한다.

왜 이 순서: 버전 확인과 알고리즘 협상이 먼저 이루어져야 양측이 공통으로 지원하는 방식으로 키 교환과 보호 통신을 수행할 수 있기 때문이다.

선지별 해설

① X — '서버가 클라이언트에게 개인키를 전송'한다는 부분이 틀리다. 개인키는 서버 밖으로 전송하지 않는다. 올바르게는 서버가 호스트 공개키와 개인키로 생성한 서명을 보내고, 클라이언트가 그 서명을 검증하여 서버를 인증한다.
② O — 클라이언트와 서버는 키 교환을 통해 공유 비밀을 만들고, 여기서 암호화와 무결성 보호에 사용할 세션 키를 도출한다.
③ O — 연결이 설정되면 양측은 SSH 프로토콜 버전 등이 포함된 식별 문자열을 서로 교환한다.
④ O — 양측은 실제 보호 통신에 앞서 사용할 암호화 알고리즘, MAC 알고리즘, 압축 방식 등을 협상한다.

오답 포인트

①은 공개키 기반 서버 인증을 '개인키 전송'으로 바꾼 함정이다. 공개키는 전달할 수 있지만 개인키는 소유자가 보관하며, 개인키로 만든 서명을 공개키로 검증한다.

NoteBase

다시 나오면 이렇게 판단

SSH 절차는 '버전 교환 → 알고리즘 협상 → 키 교환·서버 인증 → 새 키 적용'의 흐름으로 판단한다. 공개키는 전달·검증에 쓰이고 개인키는 외부로 전송하지 않는다는 원칙을 함께 적용한다.

암기 포인트

SSH 서버 인증은 '공개키와 서명은 전송, 개인키는 서버에 보관'으로 기억한다.

NoteBase

11. 침입 탐지 시스템(IDS) 중 알려진 공격 패턴을 수집하고 분류한 후 네트워크 트래픽을 검사하여 일치하는 패턴의 위협 수준을 평가하는 방식으로 가장 적절한 것은?
① 이상 탐지 기반 IDS
② 하이브리드 IDS
③ 시그니처 기반 IDS
④ 행동 분석 기반 IDS

정답 3번

출제 포인트

알려진 공격 패턴을 미리 수집·분류하고 네트워크 트래픽에서 그 패턴과의 일치 여부를 검사하는 IDS 탐지 방식을 구별하는 문제이다.

핵심 개념

시그니처 기반 IDS: 알려진 공격의 고유한 패턴이나 규칙을 시그니처로 등록한 뒤, 관찰된 트래픽과 대조하여 공격을 탐지하는 방식이다. 키워드는 '알려진 공격 패턴'과 '패턴 일치'이다.
이상 탐지 기반 IDS: 정상 상태의 통계적 특성이나 프로파일을 기준으로 삼고, 그 기준에서 크게 벗어난 활동을 이상으로 탐지하는 방식이다. 키워드는 '정상 기준'과 '편차'이다.
하이브리드 IDS: 시그니처 기반 탐지와 이상 탐지 등 둘 이상의 방식을 결합하여 각각의 장단점을 보완하는 방식이다.
행동 분석 기반 IDS: 사용자·호스트·응용 프로그램 등의 행동을 관찰하고 행동 규칙이나 프로파일을 기준으로 의심스러운 행위를 식별하는 방식이다.

선지별 해설

① X — '이상 탐지 기반 IDS'가 틀린 표현이다. 이상 탐지는 정상 행동의 기준을 만든 뒤 그 기준에서 벗어난 편차를 탐지한다. 제시문처럼 알려진 공격 패턴과 트래픽을 대조하는 방식은 시그니처 기반 IDS이다.
② X — '하이브리드 IDS'가 틀린 표현이다. 하이브리드 IDS는 시그니처 탐지와 이상 탐지 등 여러 방식을 결합한다. 제시문에는 결합 방식이 아니라 알려진 패턴의 수집·분류 및 일치 검사가 제시되어 있으므로 시그니처 기반 IDS가 올바른 표현이다.
③ O — 알려진 공격 패턴을 시그니처로 구축하고 실제 네트워크 트래픽에서 동일하거나 대응하는 패턴을 찾는 것은 시그니처 기반 IDS의 전형적인 탐지 원리이다.
④ X — '행동 분석 기반 IDS'가 틀린 표현이다. 행동 분석 기반 IDS는 사용자·호스트·응용 프로그램 등의 행위를 관찰하여 의심스러운 행동을 식별한다. 제시문처럼 이미 알려진 공격 패턴과 트래픽의 일치 여부를 검사하는 방식은 시그니처 기반 IDS이다.

NoteBase

오답 포인트

‘위협 수준을 평가한다’는 표현만 보고 행동 분석이나 하이브리드 방식으로 넓게 판단하기 쉽다. 그러나 정답을 결정하는 표현은 ‘알려진 공격 패턴을 수집·분류’하고 ‘일치하는 패턴’을 검사한다는 부분이며, 이는 시그니처 매칭을 직접 가리킨다.

다시 나오면 이렇게 판단

알려진 공격 패턴·규칙·문자열과의 일치를 찾으면 시그니처 기반, 정상 프로파일에서의 편차를 찾으면 이상 탐지 기반, 두 방식을 결합하면 하이브리드, 행위 주체의 행동을 추적·분석하면 행동 분석 기반으로 판단한다.

암기 포인트

알려진 패턴과 매칭하면 시그니처, 정상에서 벗어나면 이상 탐지이다.

NoteBase

12. CSMA/CD 방식에서 데이터 전송 중 충돌이 감지되었을 때 송신 장치가 잼 신호(Jam Signal)를 전송하는 이유로 가장 적절한 것은?
① 데이터 전송 속도를 일시적으로 높이기 위해
② 충돌에 관여된 다른 모든 장치에 충돌 발생을 확실히 알리기 위해
③ 특정 시간 동안 매체를 독점적으로 쓰기 위한 예약 신호로 사용하기 위해
④ 손상된 프레임을 즉시 복구하기 위한 정보를 포함하기 위해

정답 2번

출제 포인트

이 문제는 CSMA/CD에서 충돌을 감지한 송신 장치가 잼 신호를 보내는 목적을 묻는 문제이다.

핵심 개념

CSMA/CD는 전송 전에 매체의 사용 여부를 확인하고, 전송 중 충돌을 감지하면 전송을 중단한 뒤 임의의 대기 시간을 거쳐 재전송하는 방식이다.
잼 신호(Jam Signal)는 충돌이 발생했다는 사실을 네트워크의 관련 장치들이 확실히 인식하도록 보내는 신호이다. 잼 신호 자체가 매체를 예약하거나 손상된 프레임을 복구하는 것은 아니다.

NoteBase

선지별 해설

① X
틀린 표현은 '데이터 전송 속도를 일시적으로 높이기 위해'이다. 잼 신호는 전송 속도를 높이는 신호가 아니라 충돌 사실을 알리는 신호이다. 올바르게는 충돌을 감지한 장치가 전송을 중단하고 충돌 발생을 알리기 위해 잼 신호를 보낸다.

② O
잼 신호를 보내면 충돌에 관여한 다른 장치들도 충돌 발생을 확실히 인식하여 현재 전송을 중단하고 재전송 절차로 넘어갈 수 있다.

③ X
틀린 표현은 '매체를 독점적으로 쓰기 위한 예약 신호'이다. 잼 신호에는 매체를 특정 시간 동안 예약하는 기능이 없다. 올바르게는 충돌 사실을 알린 뒤 각 송신 장치가 임의의 대기 시간을 거쳐 다시 전송을 시도한다.

④ X
틀린 표현은 '손상된 프레임을 즉시 복구하기 위한 정보를 포함'한다는 것이다. 잼 신호는 프레임 복구 정보를 담지 않는다. 올바르게는 충돌로 손상된 프레임을 폐기하고, 송신 장치가 대기 후 프레임을 재전송한다.

오답 포인트

잼 신호를 제어 정보나 복구 정보로 오해하기 쉽다. 특히 ③의 '예약'과 ④의 '복구 정보'는 잼 신호에 없는 기능이다. 잼 신호의 직접적인 역할은 오직 충돌 발생을 확실히 알리는 것이다.

다시 나오면 이렇게 판단

CSMA/CD에서 충돌 이후의 흐름을 '충돌 감지 → 잼 신호로 충돌 통보 → 전송 중단 → 임의 시간 대기 → 재전송'으로 판단한다. 잼 신호의 목적을 묻는 경우에는 '충돌 통보'에 해당하는 선지를 고른다.

암기 포인트

잼 신호는 속도 향상·매체 예약·프레임 복구가 아니라 충돌 통보를 위한 신호이다.

NoteBase

13. 포트 미러링에 대한 설명으로 가장 적절한 것은?
① 네트워크 속도를 증가시킨다.
② 특정 포트의 트래픽을 복사하여 다른 포트로 전달한다.
③ 트래픽 모니터링과 암호화를 통해 기밀성을 제공한다.
④ 여러 포트에서 유입되는 트래픽을 모아 보관하는 것이 목적이다.

정답 2번

출제 포인트

포트 미러링의 목적과 동작 방식을 구별하는 문제이다.

핵심 개념

포트 미러링은 스위치가 특정 포트나 VLAN을 지나는 트래픽의 복사본을 지정된 다른 포트로 보내 분석 장비가 이를 관찰할 수 있게 하는 기능이다. 핵심 키워드는 '트래픽 복사'와 '모니터링 포트로 전달'이다. 포트 미러링 자체가 속도 향상, 암호화 또는 장기 보관을 수행하는 것은 아니다.

선지별 해설

① X — '네트워크 속도를 증가시킨다'는 표현이 틀리다. 포트 미러링은 통신 속도를 높이는 기술이 아니라 트래픽을 관찰하기 위해 복사본을 만드는 기능이다. 올바르게는 '네트워크 트래픽의 분석과 장애·보안 모니터링을 지원한다'이다.

② O — 특정 포트의 트래픽을 복사하여 지정된 다른 포트로 전달하는 것은 포트 미러링의 기본 동작이다. 전달된 복사본은 패킷 분석기나 침입 탐지 장비 등이 모니터링하는 데 사용된다.

③ X — '암호화를 통해 기밀성을 제공한다'는 표현이 틀리다. 포트 미러링은 트래픽을 복사해 관찰하게 할 뿐 암호화 기능을 제공하지 않는다. 올바르게는 '트래픽 모니터링과 분석을 위해 패킷의 복사본을 제공한다'이다.

④ X — '여러 포트에서 유입되는 트래픽을 모아 보관하는 것이 목적'이라는 표현이 틀리다. 포트 미러링의 직접적인 목적은 선택한 트래픽의 복사본을 모니터링 포트로 전달하는 것이며, 저장이 필요하면 연결된 분석 장비가 별도로 수행한다. 올바르게는 '선택한 포트나 VLAN의 트래픽을 복사하여 분석 장비가 연결된 포트로 전달하는 것이 목적이다'이다.

NoteBase

오답 포인트

‘미러링’의 복사 기능을 성능 향상이나 데이터 백업으로 오해하기 쉽다. 이 문항에서는 ②의 ‘복사하여 다른 포트로 전달’이 정의에 정확히 대응하며, ④의 ‘보관’은 포트 미러링 자체의 기능이 아니다.

다시 나오면 이렇게 판단

선지에서 원본 트래픽의 복사본을 지정된 모니터링 포트로 전달한다고 설명하면 포트 미러링에 해당한다. 속도 증가, 암호화, 저장을 핵심 기능으로 제시하면 다른 기능을 섞은 설명으로 판단한다.

암기 포인트

포트 미러링은 ‘복사해서 분석 포트로 전달’이다.

NoteBase

14. 패스워드 크래킹에 대한 설명으로 가장 적절하지 않은 것은?
① 사전 공격은 패스워드 크래킹의 소요 시간을 감소시킬 수 있다.
② 패스워드 입력 실패 횟수에 제한이 없고 충분한 시간이 주어지면 무작위 대입 공격으로 패스워드를 알아낼 수 있다.
③ 충분한 길이의 패스워드는 이론적으로 패스워드 크래킹이 불가능하다.
④ John the Ripper는 패스워드 크래킹 도구이다.

정답 3번

출제 포인트

패스워드 크래킹 기법의 원리와 패스워드 길이가 공격 가능성 및 현실적인 소요 시간에 미치는 영향을 묻는 문제이다.

핵심 개념

패스워드 크래킹은 사전의 후보 단어나 가능한 문자열을 대입하여 패스워드를 찾아내는 공격이다.
사전 공격은 미리 준비한 후보 목록을 사용하므로 무작정 모든 문자열을 시험하는 것보다 탐색 범위를 줄일 수 있다.
무작위 대입 공격은 가능한 후보를 반복해서 시험하는 방식이며, 시도 제한이 없고 충분한 시간이 주어지면 유한한 패스워드 공간에서 정답을 찾을 수 있다.
패스워드가 길어지면 가능한 조합 수가 급격히 늘어 공격이 현실적으로 어려워지지만, 이론적으로 불가능해지는 것은 아니다.

NoteBase

선지별 해설

① O
사전 공격은 자주 쓰는 단어와 패스워드 후보를 미리 모아 대입하므로 탐색해야 할 후보를 줄여 크래킹 시간을 단축할 수 있다.

② O
입력 실패 횟수에 제한이 없고 충분한 시간이 주어지면 후보를 계속 대입할 수 있으므로 유한한 후보 공간 안의 패스워드를 찾아낼 수 있다.

③ X
틀린 표현은 '충분한 길이의 패스워드는 이론적으로 패스워드 크래킹이 불가능하다'이다. 올바르게는 패스워드가 길수록 후보 조합 수가 커져 크래킹이 현실적으로 매우 어려워질 수 있지만, 가능한 후보 공간이 유한한 이상 이론적으로 크래킹이 불가능한 것은 아니다.

④ O
John the Ripper는 사전 공격, 무차별 대입 등으로 패스워드를 분석하는 대표적인 패스워드 크래킹 도구이다.

오답 포인트

③의 '현실적으로 매우 어렵다'를 '이론적으로 불가능하다'로 바꾼 표현이 함정이다. 패스워드 길이는 공격에 필요한 계산량과 시간을 늘리지만 공격 가능성 자체를 없애지는 않는다.

다시 나오면 이렇게 판단

패스워드 보안 문항에서는 '불가능'이라는 단정 표현을 먼저 확인한다. 후보 공간이 유한하면 전수 대입은 이론적으로 가능하고, 길이와 복잡성은 그 소요 시간을 늘려 현실적 실행 가능성을 낮춘다고 판단한다.

암기 포인트

긴 패스워드는 크래킹을 불가능하게 만드는 것이 아니라 필요한 조합 수와 시간을 크게 늘린다.

NoteBase

15. 시스템 및 네트워크 모니터링에 대한 설명으로 가장 적절하지 않은 것은?

① 서버나 네트워크 장비의 성능에 영향을 줄 수 있는 시스템 상태를 사전에 감지하기 위해 수행하는 것을 리소스 모니터링이라고 한다.

② 서버나 네트워크 장비가 정상적으로 작동하는지 확인하기 위해 네트워크 트래픽 흐름과 병목 발생 여부를 감시하는 것을 트래픽 모니터링이라고 한다.

③ 웹 서버나 애플리케이션 서버의 상태를 주기적으로 점검하여 정상 동작 여부를 확인하는 것을 헬스 체크라고 한다.

④ ping이나 HTTP 요청을 외부에서 보내 응답 상태를 확인하는 방식은 일반적으로 내부 모니터링이라고 한다.

정답 4번

출제 포인트

시스템·네트워크 모니터링 방식의 목적과 관측 위치를 구분하는 문제이다. 특히 요청을 보내는 지점이 내부인지 외부인지에 따라 내부 모니터링과 외부 모니터링을 구별해야 한다.

핵심 개념

리소스 모니터링: CPU, 메모리, 디스크 등 시스템 자원의 사용량과 상태를 관찰하여 성능 저하나 장애 징후를 파악하는 방식이다.
트래픽 모니터링: 네트워크의 트래픽 흐름, 통신량, 지연 및 병목 등을 관찰하여 네트워크 상태를 확인하는 방식이다.
헬스 체크: 서버나 애플리케이션에 주기적으로 점검 요청을 보내 정상 응답 여부를 확인하는 방식이다.
내부 모니터링은 내부 시스템이나 에이전트의 관점에서 상태를 수집하고, 외부 모니터링은 외부 관측 지점에서 ping이나 HTTP 요청 등을 보내 실제 접근성과 응답 상태를 확인한다.

NoteBase

선지별 해설

① O — 서버나 네트워크 장비의 자원 상태를 관찰하여 성능에 영향을 줄 수 있는 이상 징후를 미리 파악하는 것은 리소스 모니터링에 해당한다.
② O — 네트워크 트래픽의 흐름을 관찰하고 병목 발생 여부를 확인하는 것은 트래픽 모니터링에 해당한다.
③ O — 웹 서버나 애플리케이션 서버에 주기적으로 점검 요청을 보내 정상 응답과 동작 여부를 확인하는 것은 헬스 체크에 해당한다.
④ X — 틀린 표현은 '외부에서 보내'는 방식이 '내부 모니터링'이라는 부분이다. 외부 관측 지점에서 ping이나 HTTP 요청을 보내 응답 상태를 확인하는 방식은 외부 모니터링이다. 내부 모니터링은 내부 시스템이나 에이전트가 자원·프로세스·로그 등의 상태를 수집하는 방식이다.

오답 포인트

④에서 ping과 HTTP라는 점검 수단만 보고 내부 모니터링으로 판단하기 쉽다. 분류 기준은 도구의 이름이 아니라 관측 위치이다. 외부에서 요청을 보내 서비스의 접근성과 응답을 확인하면 외부 모니터링이다.

다시 나오면 이렇게 판단

각 설명에서 무엇을 관찰하는지와 어디에서 관찰하는지를 함께 확인한다. 자원 사용량은 리소스 모니터링, 네트워크 흐름과 병목은 트래픽 모니터링, 주기적 정상 응답 확인은 헬스 체크로 판단한다. 외부 지점에서 서비스에 요청을 보내 확인하면 외부 모니터링으로 판단한다.

암기 포인트

자원은 리소스, 흐름은 트래픽, 주기적 응답은 헬스 체크, 밖에서 확인하면 외부 모니터링이다.

NoteBase

16. 이더넷을 통해 데이터를 전송할 때 이더넷 프레임의 헤더에 포함되지 않는 항목으로 가장 적절한 것은?
① 목적지(Destination) 이더넷 주소
② 발신지(Source) 이더넷 주소
③ 이더넷 유형(Type)
④ 체크섬(Checksum)

정답 4번

출제 포인트

이 문제는 이더넷 프레임에서 헤더에 속하는 필드와 프레임 끝의 트레일러에 속하는 필드를 구분하는 문제이다.

핵심 개념

이더넷 프레임의 헤더는 목적지 주소, 발신지 주소, 유형/길이 등의 제어 정보를 담는다. 체크섬 역할을 하는 FCS(Frame Check Sequence)는 전송 오류를 검출하기 위한 값으로, 헤더가 아니라 프레임의 맨 끝에 붙는 트레일러 필드이다.

선지별 해설

① X
목적지(Destination) 이더넷 주소는 수신 장치를 식별하는 헤더 필드이다. 틀린 판단은 목적지 주소가 헤더에 포함되지 않는다는 것이며, 올바르게는 목적지 주소가 이더넷 헤더에 포함된다.

② X
발신지(Source) 이더넷 주소는 송신 장치를 식별하는 헤더 필드이다. 틀린 판단은 발신지 주소가 헤더에 포함되지 않는다는 것이며, 올바르게는 발신지 주소가 이더넷 헤더에 포함된다.

③ X
이더넷 유형(Type)은 상위 계층 프로토콜의 종류를 나타내는 헤더 필드이다. 틀린 판단은 유형 필드가 헤더에 포함되지 않는다는 것이며, 올바르게는 유형 필드가 이더넷 헤더에 포함된다.

④ O
체크섬에 해당하는 FCS는 프레임 전송 중 발생한 오류를 검출하는 값이다. 이 값은 헤더가 아니라 데이터 뒤, 즉 이더넷 프레임의 끝에 위치하는 트레일러 필드이므로 문제의 조건에 맞는다.

NoteBase

오답 포인트

체크섬도 프레임을 제어하는 정보이므로 헤더에 있을 것이라고 생각하기 쉽다. 그러나 이더넷에서는 목적지 주소·발신지 주소·유형은 앞부분의 헤더에 있고, FCS는 프레임 전체의 오류를 검사하도록 끝부분에 배치된다.

다시 나오면 이렇게 판단

필드의 위치를 기준으로 판단한다. 수신자·송신자·상위 프로토콜을 알리는 정보는 헤더에 있고, 전송이 끝난 뒤 프레임의 오류를 검사하는 FCS는 트레일러에 있다.

암기 포인트

주소와 유형은 앞의 헤더, 오류 검사용 FCS는 뒤의 트레일러이다.

NoteBase

17. 클라우드 환경에서 발생할 수 있는 여러 보안 위협 중 가장 적절하지 않은 것은?
① 시스템 취약점(System Vulnerabilities)
② 잘못된 설정(Misconfiguration)
③ 서버과열로 인한 성능저하(Server Overheating)
④ APT(Advanced Persistent Threats)

정답 3번

출제 포인트

클라우드 환경의 보안 위협과 단순한 장비 운용·환경 문제를 구별하는 문제이다.

핵심 개념

클라우드 보안 위협은 시스템의 기밀성·무결성·가용성을 침해할 수 있는 취약점, 설정 오류, 공격 행위 등을 말한다.
시스템 취약점은 소프트웨어나 시스템의 약점이고, 잘못된 설정은 접근 권한·공개 범위·보안 기능 등을 부적절하게 구성한 상태이며, APT는 특정 대상을 장기간 은밀하게 공격하는 지능형 지속 위협이다.
서버 과열은 냉각 불량 등으로 발생하는 물리적·운영상 장애 요인에 가깝고, 나머지 세 항목과 같은 대표적 사이버 보안 위협으로 분류하기에는 가장 적절하지 않다.

선지별 해설

① O — 시스템 취약점은 공격자가 악용하여 권한 탈취, 정보 유출, 서비스 침해를 일으킬 수 있으므로 대표적인 보안 위험 요인이다.
② O — 잘못된 설정은 저장소 공개, 과도한 접근 권한, 보안 기능 비활성화 등을 초래할 수 있으므로 클라우드 환경의 주요 보안 위협이다.
③ X — '서버 과열로 인한 성능저하'는 냉각·전원·장비 관리와 관련된 물리적·운영상 장애 요인이다. 틀린 표현을 보안 위협에 맞게 고치면 '서비스 거부 공격으로 인한 가용성 저하'와 같은 사이버 공격이어야 한다.
④ O — APT는 특정 조직이나 시스템에 장기간 침투하여 정보를 탈취하거나 시스템을 훼손하는 공격이므로 클라우드에서도 고려해야 할 보안 위협이다.

오답 포인트

③도 서비스 가용성을 낮추므로 넓은 의미에서는 물리적·환경적 보안 위험에 포함될 수 있다. 다만 선지 비교와 출제 의도상 ①·②·④는 공격자가 악용하는 취약점, 보안 설정 오류, 공격 행위라는 전형적인 사이버 보안 위협인 반면, ③은 공격과 직접 관련되지 않은 장비의 열 관리 문제이므로 가장 적절하지 않다.

NoteBase

다시 나오면 이렇게 판단

각 선지가 공격자의 행위, 악용 가능한 시스템 약점, 보안 설정 오류에 해당하는지 먼저 확인한다. 냉각 불량이나 과열처럼 공격과 직접 관련되지 않은 장비 운용 문제는 별도의 물리적·운영상 장애 요인으로 판단한다.

암기 포인트

취약점·오설정·APT는 보안 위협, 서버 과열은 운용·환경 문제이다.

NoteBase

18. 방화벽에서 정책이 적용될 때 네트워크 트래픽이 특정 규칙에 따라 허용되거나 차단되는 과정에 대한 설명으로 가장 적절한 것은?
① 가장 마지막에 설정된 규칙이 우선 적용된다.
② 트래픽 정보와 가장 많이 일치하는 규칙이 적용된다.
③ 룰셋의 위에서부터 순서대로 규칙을 평가하며 가장 먼저 일치하는 규칙의 액션이 적용된다.
④ 설정된 모든 규칙을 동시에 평가하여 최종 액션을 결정한다.

정답 3번

출제 포인트

이 문제는 방화벽 룰셋의 규칙 평가 순서와 첫 일치 우선 원리를 묻는 문제이다.

올바른 순서

1. 룰셋의 맨 위 규칙부터 트래픽의 조건과 일치하는지 확인한다.
2. 일치하지 않으면 바로 다음 규칙을 평가한다.
3. 처음으로 일치한 규칙을 만나면 그 규칙의 허용 또는 차단 액션을 적용하고 평가를 종료한다.
4. 끝까지 일치하는 규칙이 없으면 방화벽에 설정된 기본 정책에 따른다.

왜 이 순서: 먼저 일치한 규칙에서 처리가 끝나므로 같은 트래픽과 겹치는 아래쪽 규칙은 평가 결과에 영향을 주지 못한다.

선지별 해설

① X — '가장 마지막에 설정된 규칙'이 우선되는 것이 아니다. 올바르게는 룰셋의 위에서부터 평가하여 가장 먼저 일치한 규칙이 우선 적용된다.
② X — 트래픽 정보와 일치하는 조건의 수를 세어 가장 많이 일치하는 규칙을 고르는 방식이 아니다. 올바르게는 각 규칙의 조건 충족 여부를 순서대로 확인하고, 처음으로 일치한 규칙의 액션을 적용한다.
③ O — 룰셋의 위에서부터 규칙을 순서대로 평가하며, 가장 먼저 일치하는 규칙의 허용 또는 차단 액션이 적용된다.
④ X — 모든 규칙을 동시에 평가하여 최종 액션을 결정하지 않는다. 올바르게는 위에서 아래로 순차 평가하고 첫 일치 규칙에서 액션을 확정한다.

오답 포인트

②의 '가장 많이 일치'와 ④의 '모든 규칙을 동시에 평가'는 규칙의 구체성이나 조건 수가 우선순위를 정한다고 오해하게 만든다. 실제 우선순위는 규칙이 놓인 순서이며, 먼저 일치한 규칙이 아래 규칙을 가린다.

NoteBase

다시 나오면 이렇게 판단

방화벽 룰셋 문제에서는 위에서 아래로 조건 확인 → 첫 일치 규칙의 액션 적용 → 평가 종료의 흐름으로 판단한다. 규칙이 겹치면 더 위에 있는 규칙의 결과를 먼저 확인한다.

암기 포인트

위에서 아래로, 첫 일치에서 종료한다.

NoteBase

19. 네트워크 보안 위협에 대한 설명으로 가장 적절하지 않은 것은?
① 악성코드: 바이러스, 웜 등 시스템에 피해를 주거나 정보를 탈취하는 해로운 소프트웨어
② 제로데이 공격: 아직 공개되지 않은 보안 취약점을 악용해 공격하는 것으로 기존 보안 시스템이 탐지하기 어려움
③ 권한 상승: 공격자가 일반 사용자 권한을 탈취한 후 관리자 수준의 권한으로 상승시켜 시스템을 제어함
④ DDoS: 조직 내부자가 시스템에 접근해 데이터를 탈취하거나 오용하는 내부자 위협

정답 4번

출제 포인트

이 문제는 악성코드, 제로데이 공격, 권한 상승, DDoS의 정의를 구별하고, 내부자 위협을 DDoS로 잘못 설명한 선지를 찾는 문제이다.

핵심 개념

악성코드: 시스템에 피해를 주거나 정보를 탈취하도록 만들어진 해로운 소프트웨어이다.
제로데이 공격: 아직 공개되지 않았거나 보안 패치가 마련되지 않은 취약점을 악용하는 공격이다.
권한 상승: 공격자가 취약점 등을 이용해 현재보다 높은 권한을 획득하는 행위이다.
DDoS: 여러 분산된 시스템에서 대량의 트래픽이나 요청을 보내 대상의 자원을 소진시키고 정상적인 서비스 이용을 방해하는 분산 서비스 거부 공격이다.
내부자 위협: 조직 내부의 권한을 가진 사람이 고의 또는 실수로 정보나 시스템에 피해를 주는 위협이다.

선지별 해설

① O — 악성코드는 바이러스·웜처럼 시스템에 피해를 주거나 정보를 탈취하는 해로운 소프트웨어를 뜻하므로 적절한 설명이다.
② O — 제로데이 공격은 아직 공개되지 않았거나 패치되지 않은 취약점을 악용하므로 기존 탐지·방어 체계가 즉시 대응하기 어려울 수 있다.
③ O — 일반 사용자 권한을 획득한 뒤 관리자 수준의 더 높은 권한을 얻는 행위는 권한 상승에 해당하므로 적절한 설명이다.
④ X — 틀린 표현은 'DDoS'이다. 제시된 내용은 조직 내부자가 접근 권한을 악용해 데이터를 탈취하거나 오용하는 내부자 위협이다. 올바르게는 DDoS를 '여러 분산된 시스템이 대량의 트래픽이나 요청을 보내 대상 서비스의 가용성을 떨어뜨리는 공격'이라고 설명해야 한다.

NoteBase

오답 포인트

④는 실제로 존재하는 보안 위협의 설명을 붙여 놓았기 때문에 그럴듯해 보인다. 그러나 '조직 내부자'와 '데이터 탈취·오용'은 내부자 위협의 단서이고, DDoS의 핵심 단서는 '분산된 다수의 공격원', '대량 요청', '서비스 가용성 저하'이다.

다시 나오면 이렇게 판단

공격 주체와 침해 대상부터 구분한다. 내부 권한자가 정보를 탈취·오용하면 내부자 위협이고, 여러 시스템이 트래픽을 집중시켜 서비스를 마비시키면 DDoS이며, 낮은 권한에서 높은 권한을 얻으면 권한 상승이다.

암기 포인트

DDoS는 '분산·대량 요청·서비스 마비', 내부자 위협은 '내부 권한·정보 탈취 또는 오용'이다.

NoteBase

20. VPN의 구성에 필요한 기능으로 가장 적절하지 않은 것은?
① 인증: 사용자나 장치의 신원을 검증하여 안전한 접근을 보장하는 기능
② 백업: 시스템 장애나 데이터 손실을 대비해 데이터를 복사해두는 기능
③ 터널링: 공용 네트워크상에서 사설 네트워크처럼 데이터를 주고받기 위한 가상 연결 생성 기능
④ 암호화: 전송 중인 데이터를 보호하기 위해 내용을 암호화하는 보안 기능

정답 2번

출제 포인트

VPN을 구성하는 보안·통신 기능과 일반적인 데이터 보호 기능을 구별하는 문제이다.

핵심 개념

VPN은 공용 네트워크를 이용하면서도 사설 네트워크처럼 안전하게 통신하도록 가상의 보호된 연결을 만드는 기술이다.
인증은 접속 주체의 신원을 확인하고, 터널링은 데이터를 가상 통신 경로로 전달하며, 암호화는 전송 내용을 알아볼 수 없게 보호한다. 반면 백업은 장애나 손실에 대비해 데이터의 복사본을 별도로 보관하는 복구 수단이다.

선지별 해설

① O — 인증은 사용자나 장치의 신원을 검증하여 허가된 주체만 VPN에 접속하도록 하는 기능이므로 적절하다.
② X — '데이터를 복사해두는 기능'은 백업의 설명이며 VPN 구성에 필요한 핵심 기능이 아니다. 올바르게는 백업은 시스템 장애나 데이터 손실에 대비하는 별도의 데이터 보호·복구 기능이다.
③ O — 터널링은 공용 네트워크 위에 가상의 통신 경로를 만들어 사설 네트워크처럼 데이터를 주고받게 하는 기능이므로 적절하다.
④ O — 암호화는 전송 중인 데이터를 제3자가 읽기 어렵게 변환하여 기밀성을 보호하는 기능이므로 적절하다.

오답 포인트

②의 백업도 넓은 의미에서는 보안과 관련되어 보여 혼동하기 쉽다. 그러나 VPN의 목적은 안전한 원격 통신 경로를 만드는 것이며, 데이터 복사본을 보관하는 백업은 통신 경로를 구성하는 기능이 아니다.

NoteBase

다시 나오면 이렇게 판단

선지가 접속 주체 확인, 가상 통신 경로 형성, 전송 내용 보호에 관한 것이면 VPN 기능으로 판단한다. 장애 이후의 복구를 위해 데이터를 복사·보관하는 기능이면 백업으로 구분한다.

암기 포인트

VPN은 인증·터널링·암호화로 안전한 통신을 만들고, 백업은 손실에 대비해 데이터를 복사한다.

NoteBase

21. TLS와 프로토콜의 연동 목적으로 적절하지 않은 것은?
① HTTPS는 HTTP에 TLS를 적용하여 웹사이트 상의 보안 통신을 지원한다.
② FTPS는 FTP에 TLS를 적용하여 보안 파일 전송을 지원한다.
③ SMTPS는 SMTP에 TLS를 적용하여 이메일 보안을 지원한다.
④ IMAPS는 IMAP에 TLS를 적용하여 인증서 기반의 부인 방지를 지원한다.

정답 4번

출제 포인트

이 문제는 TLS를 응용 프로토콜에 적용한 보안 프로토콜의 명칭과 TLS가 제공하는 보안 목적을 구분하는 문제이다.

핵심 개념

TLS는 통신 구간의 기밀성, 무결성, 상대방 인증을 제공하는 보안 프로토콜이다. HTTPS, FTPS, SMTPS, IMAPS는 각각 HTTP, FTP, SMTP, IMAP에 TLS를 적용한 형태이다. 다만 TLS의 인증서 기반 인증은 통신 상대의 신원을 확인하는 기능이며, 메시지를 보낸 사실을 제3자에게 증명하는 부인 방지와는 구별된다.

선지별 해설

① O — HTTPS는 HTTP 통신에 TLS를 적용하여 웹 구간의 기밀성·무결성 및 서버 인증 등을 제공하므로 적절하다.

② O — FTPS는 FTP에 TLS를 적용하여 인증 정보와 파일 전송 구간을 보호하므로 적절하다.

③ O — SMTPS는 SMTP 통신에 TLS를 적용하여 이메일 전송 구간의 기밀성·무결성과 서버 인증 등을 제공하므로 적절하다.

④ X — 틀린 표현은 '인증서 기반의 부인 방지'이다. 인증서는 TLS에서 상대방 인증에 사용되지만, TLS 자체가 메시지 내용이나 전송 행위에 대한 부인 방지를 보장하지는 않는다. 올바르게는 'IMAPS는 IMAP에 TLS를 적용하여 이메일 접근 구간의 기밀성·무결성과 서버 인증을 지원한다'이다.

NoteBase

오답 포인트

④의 '인증서 기반'이라는 말 때문에 전자서명과 부인 방지를 떠올리기 쉽다. 그러나 TLS 인증서는 통신 상대를 인증하는 데 쓰이며, 메시지 자체에 대한 부인 방지는 별도의 전자서명과 같은 수단으로 확보한다.

다시 나오면 이렇게 판단

프로토콜명 끝의 S가 원래 응용 프로토콜에 TLS를 적용한 형태인지 먼저 확인한다. 이어 TLS의 목적은 기밀성·무결성·인증이고, 부인 방지는 메시지에 대한 전자서명의 영역이라는 기준으로 판단한다.

암기 포인트

HTTPS·FTPS·SMTPS·IMAPS는 TLS 적용, TLS 인증서는 인증, 부인 방지는 메시지 전자서명이다.

NoteBase

22. A와 B가 비대칭키 암호화를 이용하여 통신하는 과정에서 발생할 수 있는 문제점으로 가장 적절한 것은?

1. A는 통신을 시작하기 전에 자신의 공개키와 개인키로 구성된 쌍을 생성한다.
2. A는 자신의 공개키를 사용하여 메시지를 암호화한다.
3. A는 암호화된 메시지를 B에게 전송한다.
4. B는 해당 메시지를 복호화하기 위해 A의 개인키를 요청한다.

① B는 A의 개인키를 받을 수 없기 때문에 A의 공개키로 암호화된 메시지를 복호화할 수 없다.
② B뿐만 아니라 공격자 C 또한 A의 개인키를 입수하여 암호화된 메시지를 복호화할 수 있다.
③ 공격자 C가 자신의 개인키를 생성하여 A의 공개키로 암호화된 메시지를 복호화할 수 있다.
④ 공격자 C가 B의 공개키를 확보하여 A의 공개키로 암호화된 메시지를 복호화할 수 있다.

정답 1번

출제 포인트

비대칭키 암호화에서 암호화에 사용한 공개키와 복호화에 필요한 개인키의 대응 관계를 묻는 문제이다.

핵심 개념

비대칭키 암호화는 서로 한 쌍인 공개키와 개인키를 사용한다. 수신자만 평문을 읽게 하려면 송신자가 수신자의 공개키로 암호화하고, 수신자가 자신의 개인키로 복호화한다. 개인키는 소유자만 비밀로 보관하며 다른 사람에게 전달하지 않는다.

이 상황에서는 A가 자신의 공개키로 암호화했으므로 복호화에 필요한 키는 A의 개인키이다. B가 자신의 개인키로 복호화할 수 있도록 하려면 처음부터 B의 공개키로 암호화해야 한다.

NoteBase

선지별 해설

① O — A의 공개키로 암호화한 메시지는 그 공개키와 한 쌍인 A의 개인키로 복호화한다. 그러나 A의 개인키는 외부에 제공해서는 안 되므로 B는 정상적인 키 관리 아래에서 이를 받을 수 없고 메시지를 복호화할 수 없다.
② X — '공격자 C 또한 A의 개인키를 입수한다'는 부분이 제시된 절차에서 당연히 성립하지 않는다. 개인키는 A만 비밀로 보관해야 하며, C가 A의 개인키를 탈취한 경우에만 암호문을 복호화할 수 있다. 올바르게는 'A의 개인키가 유출되지 않는 한 C는 A의 공개키로 암호화된 메시지를 복호화할 수 없다'이다.
③ X — 'C가 자신의 개인키로 복호화할 수 있다'는 부분이 틀리다. C의 개인키는 C의 공개키와 한 쌍일 뿐 A의 공개키와 대응하지 않는다. 올바르게는 'A의 공개키로 암호화한 메시지는 A의 개인키로만 복호화할 수 있다'이다.
④ X — 'B의 공개키로 복호화할 수 있다'는 부분이 틀리다. 공개키는 이 문맥에서 암호화에 사용하며, B의 공개키는 A의 공개키와 한 쌍도 아니다. 올바르게는 'B가 메시지를 복호화하게 하려면 A가 B의 공개키로 암호화하고 B가 자신의 개인키로 복호화해야 한다'이다.

오답 포인트

④처럼 B의 키라는 이유만으로 복호화할 수 있다고 판단하거나, ②처럼 개인키 탈취 가능성을 정상적인 통신 절차의 필연적 결과로 보는 것이 함정이다. 복호화 가능 여부는 키의 소유자 이름만이 아니라 암호화에 사용된 공개키와 정확히 한 쌍인 개인키인지로 판단한다.

다시 나오면 이렇게 판단

먼저 누구의 공개키로 암호화했는지 확인한 뒤, 같은 사람의 개인키가 복호화 키인지 연결한다. 기밀성을 위한 통신에서는 '수신자의 공개키로 암호화 → 수신자의 개인키로 복호화' 구조가 되어야 한다.

암기 포인트

수신자 공개키로 잠그고, 수신자 개인키로 연다. 개인키는 공유하지 않는다.

NoteBase

23. 공개키 기반 구조(PKI)의 구성요소로 가장 적절하지 않은 것은?
① 인증기관(Certificate Authority)
② TGS(Ticket Granting Server)
③ 디지털 인증서(Digital Certificate)
④ 등록기관(Registration Authority)

정답 2번

출제 포인트

공개키 기반 구조(PKI)의 구성요소와 Kerberos 인증 시스템의 구성요소를 구별하는 문제이다.

핵심 개념

PKI는 공개키와 디지털 인증서를 이용하여 통신 주체의 신원과 공개키의 관계를 신뢰할 수 있게 관리하는 체계이다.
인증기관(CA)은 디지털 인증서를 발급·관리하고, 등록기관(RA)은 인증서 신청자의 신원을 확인하여 CA의 업무를 지원하며, 디지털 인증서는 소유자의 신원 정보와 공개키를 결합한 전자 문서이다.
TGS는 Kerberos에서 서비스 이용에 필요한 서비스 티켓을 발급하는 서버이므로 PKI의 구성요소가 아니다.

선지별 해설

① O — 인증기관(CA)은 공개키 소유자의 신원을 보증하는 디지털 인증서를 발급·관리하므로 PKI의 구성요소이다.
② X — 틀린 표현은 'TGS(Ticket Granting Server)가 PKI의 구성요소'라는 부분이다. TGS는 Kerberos 인증 시스템에서 서비스 티켓을 발급하는 구성요소이며, 올바르게는 PKI의 구성요소가 아니다.
③ O — 디지털 인증서는 인증서 소유자의 신원 정보와 공개키를 연결하여 CA가 전자서명한 문서로서 PKI에서 신뢰 관계를 형성하는 핵심 요소이다.
④ O — 등록기관(RA)은 인증서 발급 신청자의 신원을 확인하고 등록 절차를 수행하여 CA를 지원하므로 PKI의 구성요소이다.

오답 포인트

TGS도 인증과 관련된 서버이므로 PKI 구성요소로 혼동하기 쉽다. 그러나 '티켓'은 Kerberos의 핵심 용어이고, PKI의 핵심 용어는 '공개키·디지털 인증서·CA·RA'이다.

다시 나오면 이렇게 판단

선지에 인증서 발급·신원 등록·공개키 보증이 나오면 PKI로 판단하고, 티켓 발급이나 TGT·TGS가 나오면 Kerberos로 판단한다.

NoteBase

암기 포인트

PKI는 인증서(CA·RA), Kerberos는 티켓(TGS)으로 구별한다.

NoteBase

24. RIPEMD-160, TIGER와 같이 데이터의 변조 여부를 확인하기 위한 무결성 검증 방식으로 가장 적절한 것은?
① 해시함수(Hash Function) 방식
② 비대칭키(Asymmetric Key) 방식
③ 대칭키(Symmetric Key) 방식
④ 공개키(Public Key Encryption) 방식

정답 1번

출제 포인트

이 문제는 RIPEMD-160과 TIGER가 암호학적 해시함수이며, 해시값을 비교하여 데이터의 변조 여부를 확인한다는 점을 묻는 문제이다.

핵심 개념

해시함수: 임의 길이의 데이터를 고정 길이의 해시값으로 변환하는 단방향 함수이다. 원본 데이터의 해시값과 수신한 데이터의 해시값이 다르면 전송·보관 과정에서 데이터가 변경되었음을 알 수 있다.
대칭키 암호: 송신자와 수신자가 같은 비밀키로 암호화와 복호화를 수행하는 방식이다.
비대칭키 암호: 서로 다른 공개키와 개인키를 사용하는 방식이며, 공개키 암호 방식이라고도 한다.

선지별 해설

① O — RIPEMD-160과 TIGER는 모두 암호학적 해시함수이다. 데이터에서 해시값을 생성하고 이를 비교하면 변조 여부를 확인할 수 있으므로 무결성 검증에 적절하다.
② X — 틀린 표현은 '비대칭키 방식'이다. 비대칭키 방식은 공개키와 개인키의 쌍을 이용하는 암호 방식이며, RIPEMD-160과 TIGER는 키 쌍을 사용하는 암호가 아니라 해시함수이다. 올바르게는 '해시함수 방식'이다.
③ X — 틀린 표현은 '대칭키 방식'이다. 대칭키 방식은 동일한 비밀키로 암호화와 복호화를 수행하지만, RIPEMD-160과 TIGER는 암호화·복호화용 비밀키를 사용하는 방식이 아니다. 올바르게는 '해시함수 방식'이다.
④ X — 틀린 표현은 '공개키 암호 방식'이다. 공개키 암호는 비대칭키 암호의 한 형태로 공개키와 개인키를 사용하지만, RIPEMD-160과 TIGER는 공개키 암호 알고리즘이 아니다. 올바르게는 '해시함수 방식'이다.

오답 포인트

②의 비대칭키 방식과 ④의 공개키 암호 방식은 사실상 같은 계열의 용어이지만, 어느 쪽도 RIPEMD-160과 TIGER의 분류가 아니다. 암호화는 주로 기밀성을 확보하고, 해시는 데이터의 지문에 해당하는 해시값을 비교하여 무결성을 확인한다는 차이가 핵심이다.

NoteBase

다시 나오면 이렇게 판단

알고리즘 이름이 RIPEMD, TIGER, SHA처럼 해시 계열이고 변조 여부나 무결성 확인을 묻는다면 해시함수와 해시값 비교를 연결한다. 암호화와 복호화 또는 공개키와 개인키가 제시될 때만 대칭키·비대칭키 방식을 검토한다.

암기 포인트

RIPEMD-160·TIGER는 해시함수, 변조 확인은 해시값 비교이다.

NoteBase

25. traceroute 명령이 경로를 단계별로 파악하기 위해 사용하는 IP 헤더 필드와 ICMP 메시지로 가장 적절한 것은?

① IP 헤더 필드: Fragment Offset,
ICMP 메시지: Destination Unreachable

② IP 헤더 필드: Differentiated Services Field,
ICMP 메시지: Echo Reply

③ IP 헤더 필드: Time To Live(TTL),
ICMP 메시지: Time Exceeded

④ IP 헤더 필드: Protocol,
ICMP 메시지: Redirect

정답 3번

출제 포인트

traceroute가 각 라우터를 경유하는 경로를 알아내기 위해 조절하는 IPv4 헤더 필드와, 중간 라우터가 그에 응답하여 보내는 ICMP 메시지의 조합을 묻는 문제이다.

핵심 개념

TTL(Time To Live)은 패킷이 통과할 수 있는 홉 수를 제한하는 IPv4 헤더 필드이다. 라우터는 패킷을 전달할 때마다 TTL을 1씩 줄이며, TTL이 0이 되면 패킷을 폐기하고 송신지에 ICMP Time Exceeded 메시지를 보낸다. traceroute는 탐사 패킷의 TTL을 1, 2, 3처럼 단계적으로 증가시키고 각 단계에서 돌아온 ICMP Time Exceeded 메시지의 송신 주소를 확인하여 경유 라우터를 차례대로 알아낸다.

NoteBase

선지별 해설

① X
Fragment Offset은 단편화된 조각이 원래 데이터에서 놓일 위치를 나타내므로 경유 단계의 제한값이 아니다. Destination Unreachable은 목적지·네트워크·포트 등에 도달할 수 없음을 알리는 메시지이며, 중간 홉의 TTL 만료를 알리는 메시지가 아니다. 틀린 조합은 'Fragment Offset, Destination Unreachable'이며, 올바르게는 'TTL, Time Exceeded'이다.

② X
Differentiated Services Field는 트래픽의 서비스 품질과 전달 처리 방식을 표시하는 필드이므로 홉을 단계별로 제한하지 않는다. Echo Reply는 ICMP Echo Request에 대한 응답으로 주로 최종 목적지의 도달을 확인하는 데 쓰이며, 중간 라우터의 TTL 만료 응답이 아니다. 틀린 조합은 'Differentiated Services Field, Echo Reply'이며, 올바르게는 'TTL, Time Exceeded'이다.

③ O
traceroute는 TTL을 단계적으로 증가시킨 탐사 패킷을 보내고, 각 중간 라우터가 TTL 만료 시 반환하는 ICMP Time Exceeded 메시지를 이용하여 경로를 홉별로 파악한다.

④ X
Protocol 필드는 IP 페이로드에 실린 상위 계층 프로토콜의 종류를 나타내므로 경유 단계를 제어하지 않는다. ICMP Redirect는 더 적절한 다음 홉이나 게이트웨이를 알려 주는 메시지로, TTL 만료를 알리는 메시지가 아니다. 틀린 조합은 'Protocol, Redirect'이며, 올바르게는 'TTL, Time Exceeded'이다.

오답 포인트

Destination Unreachable이나 Echo Reply도 traceroute 구현에 따라 최종 목적지에 도달했음을 확인하는 응답으로 나타날 수 있어 혼동하기 쉽다. 그러나 경유 라우터를 한 단계씩 드러내는 핵심 조합은 TTL과 ICMP Time Exceeded이다.

다시 나오면 이렇게 판단

'홉별 경로 추적'이 보이면 먼저 TTL을 떠올리고, 라우터에서 TTL이 0이 될 때의 응답인 ICMP Time Exceeded를 연결한다.

암기 포인트

TTL은 홉을 제한하고, TTL 만료는 Time Exceeded를 부른다.

NoteBase