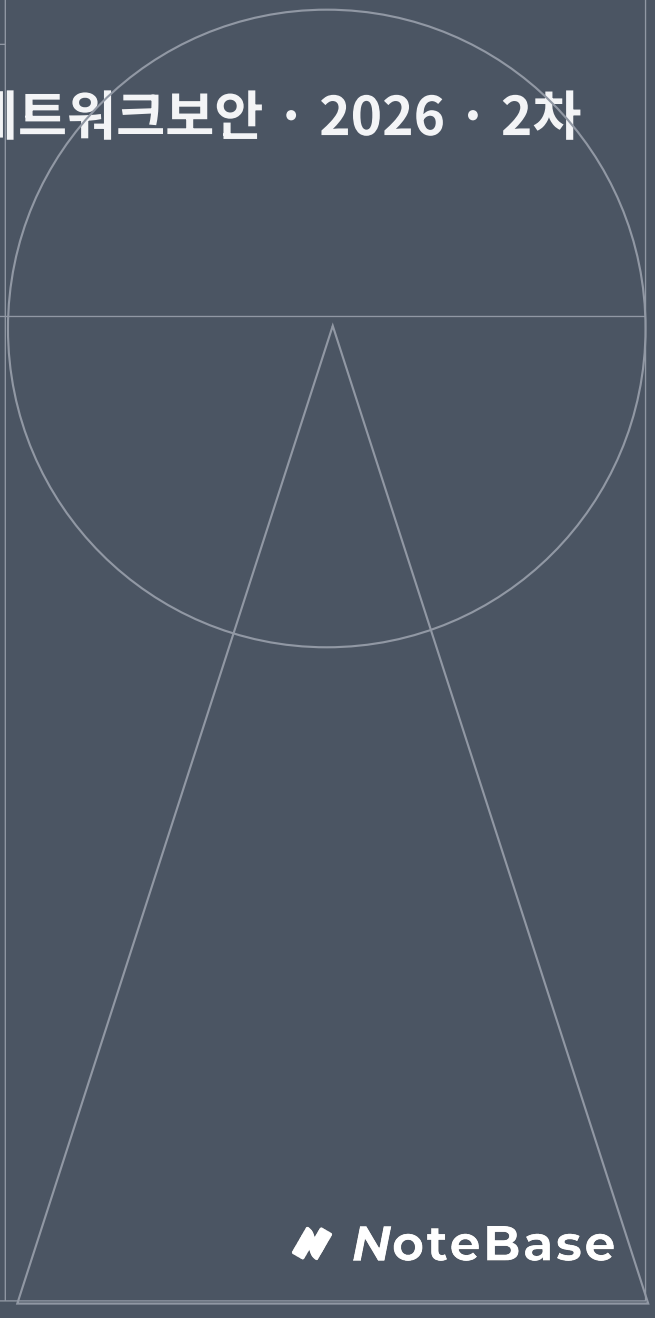
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2026 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2026 · 2차

공무원/해경/일반직 9급 · 네트워크보안 · 2026 · 2차

문 1. 다음 중 악성코드 트로이 목마의 특징으로 가장 옳지 않은 것은?

① 자기 복제

② 데이터 유출

③ 시스템 파일 파괴

④ 원격 조정

정답 1번

출제 포인트

트로이 목마가 바이러스·웜과 구별되는 핵심 특징과 감염 후 수행할 수 있는 악성 기능을 묻는 문제이다.

핵심 개념

트로이 목마는 정상적이거나 유용한 프로그램으로 위장하여 사용자의 실행을 유도한 뒤 악성 기능을 수행하는 악성코드이다. 자체 복제하여 확산하는 기능은 본질적 특징이 아니며, 감염 후 정보 탈취, 파일 훼손, 백도어 설치와 원격 제어 등을 수행할 수 있다.
트로이 목마는 위장·실행 유도가 핵심이고, 바이러스와 웜은 자기 복제·확산이 핵심이다.

선지별 해설

① X — '자기 복제'는 트로이 목마의 본질적 특징이 아니다. 올바르게는 트로이 목마는 정상 프로그램으로 위장해 실행을 유도하고, 일반적으로 스스로 복제하여 전파하지 않는다고 표현해야 한다.
② O — 트로이 목마는 저장된 개인정보나 인증정보 등을 외부로 전송하여 데이터를 유출할 수 있다.
③ O — 트로이 목마에 포함된 악성 기능은 시스템 파일을 삭제하거나 변조하여 시스템을 손상시킬 수 있다.
④ O — 트로이 목마는 백도어를 설치해 공격자가 감염된 시스템에 접속하고 원격으로 제어하도록 할 수 있다.

오답 포인트

'악성코드는 모두 스스로 복제한다'고 일반화하면 ①을 놓치기 쉽다. 자기 복제는 바이러스·웜의 대표적 성질이고, 트로이 목마의 핵심은 정상 프로그램으로의 위장과 사용자 실행 유도이다.

NoteBase

다시 나오면 이렇게 판단

선지에 '자기 복제·자동 전파'가 나오면 바이러스나 웜을 먼저 떠올리고, '정상 프로그램 위장·사용자 실행·정보 탈취·백도어·원격 제어'가 나오면 트로이 목마의 특징으로 판단한다.

암기 포인트

트로이 목마는 위장해서 침투하고 악성 기능을 수행하지만, 자기 복제가 핵심은 아니다.

NoteBase

문 2. 다음 중 서비스명과 포트가 올바르게 연결되지 않은 것은?

① POP3 over SSL - 995

② Netbios - 140

③ SNMP Manager - 162

④ FTP Data - 20

정답 2번

출제 포인트

대표적인 네트워크 서비스의 기본 포트 번호를 정확히 연결할 수 있는지를 묻는 문제이다.

핵심 개념

POP3 over SSL은 995번, NetBIOS 관련 서비스는 137~139번, SNMP 알림 수신은 162번, 능동 모드 FTP의 데이터 연결은 20번 포트를 사용한다.
NetBIOS는 이름 서비스 137번, 데이터그램 서비스 138번, 세션 서비스 139번으로 구분된다.

선지별 해설

① O — POP3 over SSL은 암호화된 POP3 통신에 TCP 995번 포트를 사용하므로 올바른 연결이다.
② X — 틀린 부분은 'Netbios - 140'이다. NetBIOS 관련 기본 포트는 이름 서비스 137번, 데이터그램 서비스 138번, 세션 서비스 139번이며 140번이 아니다.
③ O — SNMP 관리자는 에이전트가 보내는 Trap 등의 알림을 UDP 162번 포트에서 수신하므로 올바른 연결이다. 일반적인 SNMP 요청·응답에는 UDP 161번이 사용된다.
④ O — 능동 모드 FTP에서 서버가 데이터 연결에 사용하는 기본 포트는 TCP 20번이므로 올바른 연결이다. FTP 제어 연결은 TCP 21번을 사용한다.

오답 포인트

SNMP의 161번과 162번, FTP의 20번과 21번은 역할이 나뉘어 있어 혼동하기 쉽다. 그러나 ②의 140번은 NetBIOS의 연속 포트 범위인 137~139번에서 벗어난 값이다.

다시 나오면 이렇게 판단

서비스명만 외우지 않고 포트의 역할까지 함께 대조한다. SNMP는 요청·응답 161번과 알림 수신 162번, FTP는 데이터 20번과 제어 21번, NetBIOS는 137~139번으로 구분한다.

암기 포인트

POP3S 995, NetBIOS 137·138·139, SNMP Trap 162, FTP Data 20이다.

NoteBase

문 3. 다음 중 대칭키 기반 인증이 아닌 것은?

① 일회용 비밀번호(OTP) 인증

② RFID 태그와 리더간 인증

③ 무선 단말과 AP(Access Point)간 WEP키 이용

④ MAC 주소 값 인증

정답 4번

출제 포인트

인증 과정에서 송신자와 검증자가 공유한 비밀키를 사용하는 방식과, 단순 식별자 값을 확인하는 방식을 구별하는 문제이다.

핵심 개념

대칭키 기반 인증은 인증 주체와 검증자가 같은 비밀키를 공유하고, 그 키로 생성하거나 확인한 값을 이용해 정당한 사용자인지를 검증하는 방식이다. 반면 MAC 주소 인증은 단말의 MAC 주소를 허용 목록과 대조하는 식별자 기반 접근 통제이며, 공유 비밀키를 이용한 암호학적 인증이 아니다.

선지별 해설

① O — 일회용 비밀번호 인증의 대표 방식인 HOTP·TOTP는 사용자 측과 서버가 공유한 비밀값을 바탕으로 일회용 비밀번호를 생성하고 검증하므로 대칭키 기반 인증에 해당한다.
② O — RFID 태그와 리더 간 인증은 일반적으로 양쪽에 저장된 공유 비밀키와 대칭키 암호 연산을 이용해 정당한 태그 또는 리더인지를 확인하므로 대칭키 기반 인증에 해당한다.
③ O — WEP의 공유키 인증은 무선 단말과 AP가 같은 WEP 키를 공유하고 이를 이용해 인증 응답을 처리하므로 대칭키 기반 인증에 해당한다.
④ X — MAC 주소 값 인증은 MAC 주소라는 단말 식별자를 등록값과 비교하는 방식일 뿐 공유 비밀키를 사용하지 않는다. 틀린 표현은 이를 대칭키 기반 인증으로 보는 것이며, 올바르게는 식별자 기반의 MAC 주소 필터링 또는 접근 통제이다. 따라서 대칭키 기반 인증이 아닌 것을 묻는 이 문항의 정답이다.

오답 포인트

④에 '인증'이라는 말이 붙어 있어 암호키를 이용하는 방식처럼 보이지만, MAC 주소는 비밀키가 아니라 네트워크 인터페이스의 식별값이다. 인증이라는 명칭보다 공유 비밀키와 암호 연산의 존재 여부를 확인해야 한다.

NoteBase

다시 나오면 이렇게 판단

양쪽이 같은 비밀값을 보유하고 그 값으로 인증 코드를 생성·검증하면 대칭키 기반으로 판단한다.
주소·ID·기기번호를 등록 목록과 단순 대조하면 식별자 기반 접근 통제로 판단한다.

암기 포인트

OTP·RFID 공유키·WEP는 비밀키, MAC 주소 필터링은 식별자이다.

NoteBase

문 4. 다음 중 IPv4의 주소 할당방식으로 가장 옳지 않은 것은?

① Unicast

② Anycast

③ Broadcast

④ Multicast

정답 2번

출제 포인트

IPv4에서 사용하는 대표적인 주소 지정 방식인 유니캐스트, 브로드캐스트, 멀티캐스트를 구별하는 문제이다.

핵심 개념

Unicast는 한 송신자가 특정한 한 수신자에게 보내는 1대1 방식이다.
Broadcast는 한 송신자가 같은 브로드캐스트 도메인의 모든 호스트에게 보내는 1대전체 방식이다.
Multicast는 한 송신자가 멀티캐스트 그룹에 가입한 여러 수신자에게 보내는 1대그룹 방식이다.
Anycast는 동일한 주소를 여러 노드에 부여하고 라우팅상 가장 가까운 노드 하나로 전달하는 방식이다. 이 문제에서 묻는 IPv4의 대표적인 주소 할당방식에는 포함되지 않으며, IPv6의 주소 유형으로 분류된다.

선지별 해설

① O — Unicast는 하나의 출발지에서 특정한 하나의 목적지로 패킷을 전송하는 IPv4 주소 지정 방식이다.
② X — 틀린 표현은 'Anycast'이다. Anycast는 이 문항의 IPv4 주소 할당방식 분류에 해당하지 않는다. 올바르게는 IPv4의 대표적인 방식으로 Unicast, Broadcast, Multicast를 구분한다.
③ O — Broadcast는 같은 네트워크의 모든 호스트를 대상으로 패킷을 전송하는 IPv4 주소 지정 방식이다.
④ O — Multicast는 특정 멀티캐스트 그룹에 속한 여러 수신자에게 패킷을 전송하는 IPv4 주소 지정 방식이다.

오답 포인트

Anycast도 실제 네트워크에서 사용되므로 IPv4의 기본 주소 분류라고 착각하기 쉽다. 이 문항은 IPv4의 전통적인 세 가지 방식인 Unicast·Broadcast·Multicast와 IPv6에서 명시적으로 분류되는 Anycast를 구별하게 한다.

다시 나오면 이렇게 판단

수신 범위를 기준으로 구별한다. 한 호스트이면 Unicast, 같은 네트워크의 전체 호스트이면 Broadcast, 가입한 그룹이면 Multicast이다. 가장 가까운 노드 하나를 선택한다는 표현은 Anycast이다.

NoteBase

암기 포인트

IPv4 기본 3종은 UBM, 즉 Unicast·Broadcast·Multicast이다. IPv6는 Broadcast를 사용하지 않고 Anycast를 명시적으로 포함한다.

NoteBase

문 5. 다음 중 <보기>의 괄호 안에 들어갈 용어로 가장 옳은 것은?

<보기>
IPSec의 ㉠는 발신지 인증과 데이터 무결성 그리고 데이터 기밀성을 제공한다. 두 호스트 사이의 논리적 관계인 SA(Security Association)를 생성하기 위하여 ㉡프로토콜을 사용하여 보안상 안전한 채널을 확보한다.

① ㉠: ESP, ㉡: OSPF

② ㉠: AH, ㉡: IKE

③ ㉠: ESP, ㉡: IKE

④ ㉠: AH, ㉡: OSPF

정답 3번

출제 포인트

IPSec에서 패킷 보호를 담당하는 ESP·AH와 보안 연관(SA)의 협상·설정을 담당하는 IKE의 기능을 구별하는 문제이다.

핵심 개념

ESP(Encapsulating Security Payload)는 IP 데이터의 기밀성을 제공하며, 선택한 방식에 따라 발신지 인증과 데이터 무결성도 함께 제공하는 IPSec 보안 프로토콜이다.
AH(Authentication Header)는 발신지 인증과 데이터 무결성을 제공하지만 데이터 기밀성은 제공하지 않는다.
IKE(Internet Key Exchange)는 IPSec 통신 당사자가 보안 매개변수와 키를 협상하여 SA를 설정하도록 하는 프로토콜이다.
OSPF(Open Shortest Path First)는 최단 경로를 계산하는 링크 상태 라우팅 프로토콜로, IPSec의 SA를 생성하는 프로토콜이 아니다.

선지별 해설

① X — ㉠의 ESP는 맞지만 ㉡의 OSPF가 틀렸다. OSPF는 라우팅 프로토콜이며, SA를 설정하기 위한 키 교환·협상에는 IKE를 사용한다. 따라서 올바른 조합은 '㉠: ESP, ㉡: IKE'이다.
② X — ㉠의 AH가 틀렸다. AH는 인증과 무결성은 제공하지만 암호화를 통한 데이터 기밀성은 제공하지 않는다. 기밀성까지 제공하는 ㉠에는 ESP가 들어가며, ㉡의 IKE는 맞다. 따라서 올바른 조합은 '㉠: ESP, ㉡: IKE'이다.
③ O — ESP는 데이터 기밀성을 제공하면서 인증과 무결성 기능도 제공할 수 있고, IKE는 두 호스트 사이에서 보안 매개변수와 키를 협상하여 SA를 설정한다. 두 빈칸에 모두 부합한다.
④ X — AH는 데이터 기밀성을 제공하지 않고, OSPF는 SA 설정용 프로토콜이 아니라 라우팅 프로토콜이다. ㉠은 ESP, ㉡은 IKE로 고쳐야 한다.

NoteBase

오답 포인트

AH와 ESP가 모두 인증·무결성과 관련된다는 점 때문에 AH를 고르기 쉽지만, 지문의 결정적 표현은 '데이터 기밀성'이다. 또한 OSPF의 영문 명칭에 'Open'이 들어가더라도 키 교환이나 SA 설정과는 관계가 없다.

다시 나오면 이렇게 판단

IPSec 기능을 묻는 문항에서는 먼저 '기밀성'이 있는지 확인한다. 기밀성이 있으면 ESP, 인증·무결성만 강조되면 AH를 검토한다. 이어서 SA와 키 협상이 나오면 IKE, 경로 선택이 나오면 OSPF로 구별한다.

암기 포인트

ESP는 암호화까지, AH는 인증·무결성만, IKE는 SA와 키 협상, OSPF는 라우팅이다.

NoteBase

문 6. 다음 중 TCP SYN flood 공격에 대한 설명으로 옳은 것은?

① 브로드캐스트 주소를 대상으로 하는 공격이다.

② TCP 패킷의 무결성을 떨어뜨리는 공격이다.

③ TCP 패킷의 내용을 엿보는 공격이다.

④ TCP 프로토콜의 초기 연결설정 단계에서 이루어지는 공격이다.

정답 4번

출제 포인트

TCP SYN flood가 TCP 3-way handshake의 연결 설정 절차를 악용하는 서비스 거부 공격임을 묻는 문제이다.

핵심 개념

TCP SYN flood는 다수의 SYN 패킷을 보내 서버에 반개방 연결을 대량으로 남기고, 연결 대기 큐와 같은 자원을 소진시켜 정상 사용자의 접속을 방해하는 공격이다. 핵심 키워드는 TCP 초기 연결 설정, 반개방 연결, 자원 고갈이다.

선지별 해설

① X
브로드캐스트 주소를 대상으로 트래픽을 증폭하는 것은 대표적으로 Smurf 공격의 특징이다. 틀린 표현은 ‘브로드캐스트 주소를 대상으로’이며, TCP SYN flood는 서버의 TCP 연결 대기 자원을 대상으로 다수의 SYN 패킷을 보내는 공격이다.

② X
TCP SYN flood는 TCP 패킷의 데이터나 검사 값을 변조하여 무결성을 훼손하는 공격이 아니다. 틀린 표현은 ‘TCP 패킷의 무결성을 떨어뜨리는’이며, 실제로는 미완료 연결을 누적시켜 서버의 자원을 고갈시키는 서비스 거부 공격이다.

③ X
TCP 패킷의 내용을 몰래 관찰하는 행위는 스니핑에 해당한다. 틀린 표현은 ‘TCP 패킷의 내용을 엿보는’이며, TCP SYN flood는 패킷 내용의 도청이 아니라 연결 요청의 대량 발생으로 서비스 가용성을 저해하는 공격이다.

④ O
TCP SYN flood는 TCP 3-way handshake에서 공격자가 SYN을 대량으로 보내고 연결을 정상적으로 완료하지 않는 방식으로 수행된다. 따라서 TCP 프로토콜의 초기 연결 설정 단계를 악용한다는 설명이 옳다.

NoteBase

오답 포인트

‘브로드캐스트’, ‘무결성’, ‘엿보기’는 각각 다른 공격의 표적이나 보안 속성을 나타낸다. SYN flood의 SYN은 TCP 연결을 시작하는 제어 비트이므로 도청이나 변조가 아니라 연결 대기 상태를 대량으로 만드는 가용성 공격과 연결해야 한다.

다시 나오면 이렇게 판단

공격명에 SYN이 나오면 TCP 3-way handshake의 첫 단계와 반개방 연결 누적을 먼저 떠올린다. 정상 연결을 완료하지 않아 서버 자원을 소진한다는 설명이면 SYN flood에 해당한다.

암기 포인트

SYN flood는 연결 시작만 반복하여 반개방 연결을 쌓는 가용성 공격이다.

NoteBase

문 7. 다음 중 허니팟(Honeypot)에 대한 설명으로 가장 옳지 않은 것은?

① 공격자가 가능한 오랫동안 허니팟에 머물도록 하고 그 사이에 관리자는 필요한 대응을 준비한다.

② 공격자의 행동패턴에 관한 정보를 수집한다.

③ 공격자를 유인하기 위한 시스템이므로 쉽게 노출되지 않는 곳에 두어야 한다.

④ 공격자를 중요한 시스템에 접근하지 못하게 유인한다.

정답 3번

출제 포인트

허니팟의 목적과 배치 원칙을 구분하는 문제이다.

핵심 개념

허니팟은 실제 서비스처럼 보이는 미끼 시스템을 제공하여 공격자를 유인하고, 공격 행위를 관찰·분석하며, 중요 시스템으로 향하는 공격을 분산시키는 보안 수단이다. 공격자의 접근을 끌어낼 수 있어야 하지만, 침해된 허니팟이 실제 운영망 공격의 발판이 되지 않도록 중요 시스템과 격리하고 엄격하게 감시해야 한다.

선지별 해설

① O — 공격자가 허니팟에 오래 머물면 관리자는 공격 행위를 관찰하면서 침해 범위 파악과 차단 등 필요한 대응을 준비할 시간을 확보할 수 있다.
② O — 허니팟의 핵심 목적 중 하나는 공격 기법, 침입 경로, 명령 및 행동 패턴에 관한 정보를 수집하는 것이다.
③ X — 틀린 표현은 '쉽게 노출되지 않는 곳에 두어야 한다'이다. 허니팟은 공격을 유인할 수 있도록 공격자에게 매력적이고 접근 가능한 대상으로 보이게 구성한다. 다만 실제 중요 시스템과는 격리하여 허니팟을 통한 추가 침해를 막아야 한다.
④ O — 공격자의 관심을 미끼 시스템으로 돌려 실제 중요 시스템에 대한 접근을 지연하거나 분산시키는 것이 허니팟의 기능이다.

오답 포인트

③은 '보호를 위해 격리한다'는 원칙과 '공격자에게 노출되지 않게 숨긴다'를 혼동하게 만든다. 허니팟은 공격을 유인할 수 있어야 하므로 접근 대상으로 보여야 하며, 숨기는 대상이 아니라 운영망과 논리적·물리적으로 격리할 대상이다.

다시 나오면 이렇게 판단

허니팟 선지는 유인, 관찰·정보 수집, 중요 자산 보호라는 목적에 맞는지 확인한다. 배치에 관한 선지는 '공격자에게는 미끼로 보이되 실제 운영망과는 격리한다'는 기준으로 판단한다.

NoteBase

암기 포인트

허니팟은 공격자에게는 보이는 미끼이고, 운영망과는 격리된 관찰 장치이다.

NoteBase

문 8. 다음 <보기>에서 설명하는 방화벽(Firewall)의 가장 적절한 구축형태는?

<보기>
◯ 필터링 속도가 빠르고, 비용이 적게 든다.
◯ 네트워크 계층에서 동작하므로 클라이언트와 서버에 변화가 없다.
◯ 네트워크 계층과 트랜스포트 계층에 입각한 트래픽만 방어할 수 있다.
◯ 패킷 필터링 규칙을 구성하여 검증하기 어렵다.
◯ 패킷 내의 데이터에 대한 공격을 차단하지 못한다.

① 어플리케이션 프록시(Application Proxy)
② 듀얼 홈 게이트웨이(Dual Homed Gateway)
③ 스크리닝 라우터(Screening Router)
④ 싱글 홈 게이트웨이(Single Homed Gateway)

정답 3번

출제 포인트

이 문제는 동작 계층, 처리 속도, 구축 비용, 검사 범위를 근거로 방화벽 구축 형태를 구별하는 문제이다.

핵심 개념

스크리닝 라우터는 경계 라우터에서 출발지·목적지 IP 주소, 프로토콜, 포트 등 패킷 헤더 정보를 규칙과 대조하여 통과 여부를 결정하는 패킷 필터링 방식이다. 네트워크 계층과 트랜스포트 계층 정보를 중심으로 처리하므로 빠르고 비용이 적게 들지만, 규칙 관리가 복잡해질 수 있고 응용 데이터 내부의 공격을 세밀하게 검사하기 어렵다.
어플리케이션 프록시는 응용 계층에서 클라이언트와 서버의 연결을 대신 중계하며 응용 프로토콜과 데이터 내용을 검사한다.
듀얼 홈 게이트웨이는 두 개의 네트워크 인터페이스를 가진 게이트웨이가 내부망과 외부망 사이의 직접 전달을 차단하고 중계한다. 싱글 홈 게이트웨이는 하나의 네트워크 인터페이스를 가진 배스천 호스트를 스크리닝 라우터 뒤에 두고 프록시 기능을 제공하는 구조이다.

NoteBase

선지별 해설

① X — 어플리케이션 프록시는 응용 계층에서 연결을 대신 맺고 응용 프로토콜이나 데이터 내용을 검사하는 방식이다. 보기의 '네트워크 계층과 트랜스포트 계층의 트래픽만 방어'한다는 표현과 맞지 않는다. 올바르게는 응용 계층 검사와 세션 중계가 핵심이다.
② X — 듀얼 홈 게이트웨이는 두 개의 네트워크 인터페이스로 내부망과 외부망을 분리하고 게이트웨이를 통해 트래픽을 중계하는 구조이다. 올바르게는 단순한 패킷 헤더 필터링보다 망 분리와 프록시 중계가 핵심이다.
③ O — 스크리닝 라우터는 라우터의 패킷 필터링 규칙을 이용하여 네트워크 계층과 트랜스포트 계층의 헤더 정보를 검사한다. 처리 속도가 빠르고 비용이 적지만 규칙 구성·검증이 어렵고 패킷 데이터 내부의 공격을 차단하기 어렵다는 보기의 특징과 모두 일치한다.
④ X — 싱글 홈 게이트웨이는 하나의 네트워크 인터페이스를 가진 배스천 호스트를 스크리닝 라우터 뒤에 두고 프록시 서비스를 제공하는 구조이다. 올바르게는 보기처럼 라우터 하나가 네트워크·트랜스포트 계층의 패킷만 거르는 형태가 아니라, 스크리닝 라우터와 싱글 홈 배스천 호스트를 결합한 형태이다.

오답 포인트

'클라이언트와 서버의 변경이 없다'는 문장만 보고 모든 게이트웨이 방식에 연결하면 안 된다. 빠른 속도·낮은 비용·네트워크 및 트랜스포트 계층·패킷 필터링 규칙·데이터 내용 검사 불가가 함께 제시되면 스크리닝 라우터를 가리킨다.

다시 나오면 이렇게 판단

IP 주소·프로토콜·포트와 같은 헤더, 빠른 처리, 낮은 비용이 핵심이면 스크리닝 라우터로 판단한다. 응용 데이터 검사와 세션 중계가 핵심이면 어플리케이션 프록시, 네트워크 인터페이스의 수와 내부망·외부망 분리가 핵심이면 싱글 홈 또는 듀얼 홈 게이트웨이로 판단한다.

암기 포인트

스크리닝 라우터는 '헤더만 빠르게', 어플리케이션 프록시는 '내용까지 깊게' 검사한다.

NoteBase

문 9. 다음 중 RIP(Routing Information Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① 거리 벡터 알고리즘을 사용한다.

② 홉 수(Hop Count)가 10이 되면 도달 불가능으로 간주한다.(Route Poisoning)

③ UDP 포트 520번, 521번 사용한다.

④ 홉 수(Hop Count) 변경시 즉시 갱신한다.(Triggered Update)

정답 2번

출제 포인트

RIP의 경로 선택 방식, 최대 홉 수, 사용 포트, 경로 변화 통지 방식을 구별하는 문제이다.

핵심 개념

RIP는 목적지까지 거치는 라우터의 수인 홉 수를 거리 값으로 삼는 거리 벡터 라우팅 프로토콜이다. 최대 유효 홉 수는 15이며, 16홉은 도달 불가능을 뜻한다. RIPv1·RIPv2는 UDP 520번을 사용하고, IPv6용 RIPng는 UDP 521번을 사용한다.

선지별 해설

① O — RIP는 각 목적지까지의 거리와 다음 홉 정보를 이웃 라우터와 교환하는 거리 벡터 알고리즘을 사용한다.
② X — 틀린 표현은 '홉 수가 10이 되면 도달 불가능'이다. 실제로 RIP는 15홉까지 도달 가능한 경로로 취급하고 16홉을 무한대로 설정하여 도달 불가능으로 간주한다. 이러한 무한대 메트릭을 광고해 잘못된 경로를 제거하는 방식이 route poisoning이다.
③ O — RIPv1·RIPv2는 UDP 520번을 사용하고, RIPng는 UDP 521번을 사용하므로 RIP 계열의 포트에 관한 설명으로 옳다.
④ O — 경로의 홉 수 등 라우팅 정보가 변경되면 정기 갱신 시각을 기다리지 않고 변경 정보를 즉시 알리는 triggered update를 사용할 수 있다.

오답 포인트

②는 route poisoning이라는 용어는 맞게 제시하면서 도달 불가능의 기준을 10홉으로 바꾼 함정이다.
RIP에서는 15홉이 도달 가능한 상한이고 16홉이 도달 불가능이다.

다시 나오면 이렇게 판단

RIP 선지에서는 '거리 벡터·홉 수', '15홉까지 가능·16홉은 불가능', 'UDP 520·RIPng 521', '변경 시 triggered update'를 차례로 대조한다.

NoteBase

암기 포인트

RIP는 거리 벡터, 15홉까지 도달 가능, 16홉부터 무한대이다.

NoteBase

문 10. 다음 중 동일한 데이터가 두 개 이상의 디스크에 동시에 저장되고, 하나의 디스크에 오류가 발생해도 다른 드라이브의 동일한 데이터를 사용할 수 있는 RAID 방식은?

① RAID 0

② RAID 1

③ RAID 2

④ RAID 3

정답 2번

출제 포인트

동일한 데이터를 여러 디스크에 복제하여 장애에 대비하는 미러링 방식이 RAID 1임을 묻는 문제이다.

핵심 개념

RAID 0은 데이터를 여러 디스크에 나누어 기록하는 스트라이핑 방식으로, 속도는 높이지만 중복 저장과 장애 복구 기능이 없다.
RAID 1은 동일한 데이터를 둘 이상의 디스크에 그대로 복제하는 미러링 방식으로, 한 디스크에 장애가 발생해도 다른 디스크의 복제본을 사용할 수 있다.
RAID 2는 데이터를 비트 단위로 분산하고 해밍 코드 기반 오류 정정 정보를 사용한다.
RAID 3은 데이터를 바이트 단위로 분산하고 별도의 전용 패리티 디스크를 사용한다.

선지별 해설

① X — RAID 0은 데이터를 분산하는 스트라이핑 방식일 뿐 동일한 데이터를 복제하지 않는다. 틀린 표현은 RAID 0이며, 제시된 설명에 맞는 방식은 RAID 1이다.
② O — RAID 1은 동일한 데이터를 여러 디스크에 동시에 저장하는 미러링 방식이므로, 한 디스크가 고장 나도 다른 디스크의 동일한 데이터를 이용할 수 있다.
③ X — RAID 2는 비트 단위 스트라이핑과 해밍 코드 기반 오류 정정을 사용하는 방식이지, 동일한 데이터 사본을 저장하는 미러링 방식이 아니다. 틀린 표현은 RAID 2이며, 올바른 방식은 RAID 1이다.
④ X — RAID 3은 바이트 단위 스트라이핑과 전용 패리티 디스크를 사용하는 방식이다. 패리티로 한 디스크 장애를 복구할 수는 있지만 동일한 데이터를 별도 디스크에 그대로 저장하는 방식은 아니다. 틀린 표현은 RAID 3이며, 올바른 방식은 RAID 1이다.

오답 포인트

RAID 3도 한 디스크 장애에 대응할 수 있어 ④와 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '동일한 데이터가 두 개 이상의 디스크에 동시에 저장'된다는 것이며, 이는 패리티가 아니라 미러링을 뜻한다.

NoteBase

다시 나오면 이렇게 판단

‘동일한 데이터 복제’가 보이면 미러링인 RAID 1로 판단한다. ‘패리티’가 보이면 RAID 3·4·5·6 계열을, ‘중복성 없이 분산하여 속도 향상’이 보이면 RAID 0을 구분한다.

암기 포인트

RAID 0은 분산, RAID 1은 복제(미러링)이다.

NoteBase

문 11. 다음 중 ICMP(Internet Control Message Protocol)에 대한 설명으로 가장 옳은 것은?

① ICMP는 네트워크 진단을 위해 ping명령어 등을 사용하며, OSI 7모형의 전송계층에서 작동한다.

② ICMP 패킷 헤더에는 패킷 위변조 확인을 위해 Parity bit를 사용하는 필드를 포함한다.

③ ICMP 오류 메시지 중 시간초과(Time Exceed)는 목적지에 도달하기 전에 TTL값이 1이 되면 보내는 메시지이다.

④ ICMP 오류 메시지 중 발신억제(Source Quench)는 통신량의 폭주로 목적지나 라우터의 버퍼가 초과되면 발생하는 메시지이다.

정답 4번

출제 포인트

ICMP의 동작 계층, 오류 검출 방식, Time Exceeded와 Source Quench의 발생 조건을 구별하는 문제이다.

핵심 개념

ICMP는 IP 통신 중 발생한 오류를 알리고 네트워크 상태를 진단하기 위한 인터넷 계층 프로토콜이다. ICMP 메시지는 Type과 Code로 종류를 구분하고 Checksum으로 오류를 검출한다. Time Exceeded는 패킷의 TTL이 감소하여 0이 되었을 때 생성되며, Source Quench는 원래 혼잡으로 처리 용량이나 버퍼가 부족할 때 송신자에게 전송률을 낮추도록 알리기 위해 정의된 메시지이다. 다만 Source Quench는 현재 표준에서는 폐기된 방식이다.

선지별 해설

① X — ping이 ICMP Echo Request와 Echo Reply를 이용하는 것은 맞지만, '전송계층에서 작동한다'는 부분이 틀렸다. ICMP는 OSI 계층 관점에서 네트워크 계층에서 동작한다.
② X — 'Parity bit를 사용하는 필드'가 틀렸다. ICMP 헤더에는 ICMP 메시지의 오류를 검출하는 Checksum 필드가 있으며, 패리티 비트 필드를 사용하는 것이 아니다.
③ X — 'TTL값이 1이 되면'이 틀렸다. 라우터가 TTL을 감소시킨 결과 0이 되면 패킷을 폐기하고 ICMP Time Exceeded 메시지를 원래 송신자에게 보낸다.
④ O — Source Quench는 본래 트래픽 폭주로 라우터의 출력 버퍼가 부족하거나 목적지 호스트가 패킷을 처리하기 어려울 때 송신 측에 전송률 감소를 요구하도록 정의된 ICMP 오류 메시지이다. 따라서 고전적인 ICMP 메시지의 기능을 설명한 선지로 옳다. 현재는 이 메시지의 생성과 처리가 폐기되었다.

오답 포인트

③은 TTL이 1인 패킷이 다음 라우터에서 감소되어 0이 되는 과정을 'TTL이 1이면 즉시 오류'라고 바꾼 함정이다.
④는 Source Quench가 현재 폐기되었다는 사실과 원래 정의된 기능을 혼동하게 만드는 선지이다. 이 문항에서는 메시지의 본래 발생 상황을 묻는다.

NoteBase

다시 나오면 이렇게 판단

ICMP 선지는 계층, 헤더 필드, 발생 조건을 차례로 확인한다. ICMP는 네트워크 계층, 무결성 확인은 Checksum, TTL 만료는 감소 결과 0, 혼잡 억제의 고전적 메시지는 Source Quench로 대응한다.

암기 포인트

ICMP는 네트워크 계층, Checksum, TTL 0이면 Time Exceeded, 혼잡 억제는 Source Quench이다.

NoteBase

문 12. 디지털 포렌식(Forensic)은 증거의 법적 효력을 위해 지켜져야 하는 원칙이 있다. 다음 중 기본원칙으로 가장 옳지 않은 것은?

① 정당성의 원칙

② 재현의 원칙

③ 연계보관성의 원칙

④ 기밀성의 원칙

정답 4번

출제 포인트

디지털 증거의 법적 증거능력과 신뢰성을 확보하기 위한 기본원칙과 일반적인 정보보안 속성을 구별하는 문제이다.

핵심 개념

정당성의 원칙: 적법한 절차와 정당한 방법으로 증거를 수집·분석해야 한다는 원칙이다.
재현의 원칙: 같은 조건과 절차를 적용하면 같은 분석 결과가 다시 나와야 한다는 원칙이다.
연계보관성의 원칙: 증거의 수집부터 분석·보관·제출까지 취급자와 이동 과정을 기록하여 증거가 바뀌지 않았음을 입증하는 원칙이다.
기밀성은 허가받지 않은 사람이 정보에 접근하지 못하게 하는 정보보안의 속성으로, 이 문항에서 묻는 디지털 포렌식 증거의 기본원칙에 해당하지 않는다.

선지별 해설

① O — 정당성의 원칙은 디지털 증거를 적법하고 정당한 절차에 따라 획득해야 한다는 기본원칙이다. 위법하거나 권한 없는 방법으로 수집하면 증거의 법적 효력이 문제 될 수 있다.
② O — 재현의 원칙은 동일한 조건과 분석 절차에서 동일한 결과가 반복되어야 한다는 기본원칙이다. 분석 결과의 객관성과 신뢰성을 검증하는 기준이 된다.
③ O — 연계보관성의 원칙은 증거를 누가 언제 어디서 어떻게 취급했는지 전 과정을 기록·관리하는 기본원칙이다. 이를 통해 수집된 증거와 법정에 제출된 증거의 동일성을 설명할 수 있다.
④ X — 틀린 표현은 '기밀성의 원칙'이다. 기밀성은 정보보안의 주요 속성이지만 디지털 포렌식 증거의 법적 효력을 위한 기본원칙으로 분류되지 않는다. 올바르게는 '무결성의 원칙'과 같이 증거가 수집 이후 변경·훼손되지 않았음을 보장하는 원칙이 기본원칙에 해당한다.

오답 포인트

기밀성이 정보보안에서 매우 중요한 속성이므로 포렌식의 기본원칙처럼 보이는 것이 함정이다. 그러나 이 문항은 정보보안의 기밀성·무결성·가용성을 묻는 것이 아니라 디지털 증거의 법적 신뢰성을 뒷받침하는 원칙을 묻는다.

NoteBase

다시 나오면 이렇게 판단

선지가 적법한 수집, 동일 결과의 재현, 증거 취급 이력의 추적, 원본과 사본의 동일성 보장에 관한 것인지 확인한다. 접근 권한 통제나 비밀 유지 자체를 뜻하는 기밀성은 일반 정보보안 속성으로 구별한다.

암기 포인트

포렌식 증거는 정당하게 수집하고, 결과가 재현되며, 보관 이력이 이어지고, 내용이 훼손되지 않아야 한다. 기밀성은 정보보안 속성이다.

NoteBase

문 13. 다음 중 근거리통신망인 이더넷(Ethernet)의 매체 접근제어 기법인 CSMA/CD의 특징으로 가장 옳지 않은 것은?

① 반송파 감지 및 충돌 검출기반 매체 접근제어

② 다중 호스트간 패킷손실이 거의 없는 제어방식

③ 논리적으로 버스(BUS) 토폴로지 형태를 구성

④ 충돌 발생시 일정시간 대기 후 재전송 제어방식

정답 2번

출제 포인트

CSMA/CD의 반송파 감지, 충돌 검출, 재전송 대기라는 동작 원리와 논리적 토폴로지의 특징을 묻는 문제이다.

핵심 개념

CSMA/CD는 여러 호스트가 하나의 공유 매체를 사용하는 반이중 이더넷에서 전송 전에 반송파를 감지하고, 전송 중 충돌이 검출되면 임의의 시간 동안 기다린 뒤 다시 전송하는 매체 접근제어 방식이다. 공유 이더넷은 물리적 배선 형태와 관계없이 논리적으로 하나의 매체를 함께 사용하는 버스형으로 동작한다.

선지별 해설

① O — CSMA/CD는 반송파를 감지한 뒤 전송하고, 전송 중 발생한 충돌을 검출하는 매체 접근제어 방식이다.
② X — 틀린 표현은 '패킷손실이 거의 없는'이다. 여러 호스트가 동시에 전송하면 충돌이 발생할 수 있으며, 충돌 검출과 재전송으로 이를 처리할 뿐 손실이 거의 없음을 보장하지 않는다. 반복 충돌로 재전송 한도를 넘으면 프레임이 폐기될 수도 있다. 올바르게는 '다중 호스트가 공유 매체에서 충돌을 감지하고 재전송하는 제어방식'이다.
③ O — 공유형 이더넷에서는 여러 장치가 하나의 충돌 도메인인 공통 매체를 공유하므로 논리적으로 버스 토폴로지를 구성한다.
④ O — 충돌이 발생하면 전송을 중단하고 이진 지수 백오프에 따라 정한 임의의 대기시간이 지난 뒤 재전송한다.

오답 포인트

②는 충돌 후 재전송 기능을 '패킷손실이 거의 없음'이라는 성능 보장으로 바꾼 함정이다. CSMA/CD는 충돌을 예방하거나 무손실을 보장하는 방식이 아니라 충돌을 감지하고 백오프 후 재전송하는 방식이다.

다시 나오면 이렇게 판단

CSMA/CD 선지는 '전송 전 반송파 감지 → 전송 중 충돌 검출 → 충돌 시 임의 대기 후 재전송'의 흐름에 맞는지 확인한다. 무충돌이나 무손실을 보장한다는 표현은 틀린 것으로 판단한다.

NoteBase

암기 포인트

CSMA/CD는 듣고 전송하며, 부딪히면 감지하고 기다렸다가 다시 보낸다.

NoteBase

문 14. 다음 중 UDP Flooding 공격 대응방법으로 가장 옳지 않은 것은?

① 네트워크 트래픽 대역폭을 축소한다.

② 패킷의 크기를 기반으로 차단한다.

③ 발신자 IP별 임계치로 차단한다.

④ 미사용 프로토콜을 필터링한다.(UDP차단)

정답 1번

출제 포인트

UDP Flooding 공격의 대응은 공격 트래픽의 유입량과 특징을 식별하여 필터링하거나 전송률을 제한하는 것이 핵심이다.

핵심 개념

UDP Flooding은 다량의 UDP 패킷을 보내 네트워크 대역폭이나 시스템 처리 자원을 소진시키는 서비스 거부 공격이다. 대응 방법에는 불필요한 UDP 트래픽 차단, 패킷 특성 기반 필터링, 발신지별 임계치 적용과 전송률 제한 등이 있다.

선지별 해설

① X — '네트워크 트래픽 대역폭을 축소한다'는 표현이 틀렸다. 사용 가능한 대역폭을 줄이면 정상 트래픽까지 더 쉽게 혼잡해지므로 공격 대응이 되지 않는다. 올바르게는 공격 UDP 트래픽을 필터링하거나 전송률을 제한하고, 필요한 경우 충분한 처리 용량을 확보한다.
② O — 공격 패킷이 특정 크기 또는 반복적인 크기 분포를 보이면 그 패킷 특성을 필터 규칙으로 삼아 차단할 수 있다.
③ O — 발신자 IP별 패킷 수나 전송률에 임계치를 두고 이를 넘는 트래픽을 차단하거나 제한하는 방식은 UDP Flooding 완화에 활용된다.
④ O — 실제로 사용하지 않는 UDP 기반 프로토콜이나 포트의 트래픽을 경계 장비에서 차단하면 불필요한 공격 경로를 줄일 수 있다. UDP를 업무상 전혀 사용하지 않는 환경이라면 UDP 자체를 차단할 수도 있다.

오답 포인트

①의 '대역폭 축소'를 공격 트래픽의 '대역폭 제한'과 혼동하기 쉽다. 줄여야 하는 것은 네트워크가 사용할 수 있는 전체 대역폭이 아니라 공격으로 의심되는 UDP 트래픽의 유입률이다.

다시 나오면 이렇게 판단

대응책이 공격 트래픽만 식별·차단·제한하는지, 아니면 정상 트래픽이 사용할 자원까지 줄이는지를 구분한다. 공격 트래픽의 필터링과 전송률 제한은 대응이지만 전체 네트워크 대역폭 축소는 대응이 아니다.

NoteBase

암기 포인트

UDP Flooding 대응은 공격 UDP의 차단·필터링·전송률 제한이며, 전체 대역폭 축소가 아니다.

NoteBase

문 15. 다음 중 무선 네트워크의 안전한 사용방법에 대한 설명으로 가장 옳지 않은 것은?

① 업무용 무선AP와 방문자용 무선AP를 분리하여 접근통제한다.

② 무선AP의 비밀번호는 쉽게 예측하지 못하게 주기적으로 변경하고, 데이터는 암호화하여 전송토록 설정 관리한다.

③ 무선AP의 접근권한을 통제하고, 무선침입차단시스템(WIPS) 등을 사용해 불법적인 사용자나 AP를 차단한다.

④ 주기적인 워 드라이빙을 통해 다양한 사용자 접근을 주기적으로 분석하고, MAC주소 인증을 통해 보안을 강화한다.

정답 4번

출제 포인트

무선 네트워크의 안전한 운영 대책과 무선망 탐색 행위인 워 드라이빙을 구별하는 문제이다.

핵심 개념

안전한 무선 네트워크 운영은 업무망과 방문자망의 분리, 강한 인증, 통신 암호화, 접속 권한 통제, 비인가 단말·AP의 탐지와 차단을 결합하는 것이다.
워 드라이빙은 이동하면서 주변 무선 네트워크를 검색하여 SSID, 신호, 보안 설정 등의 정보를 수집하는 행위이다. 정상 사용자의 접근을 분석하는 일반적인 보안 운영 방법과는 다르다.
MAC 주소 인증은 주소 위조가 가능하므로 보조적인 통제 수단일 뿐, 강한 사용자 인증을 대신할 수 없다.

선지별 해설

① O — 업무용 AP와 방문자용 AP를 분리하면 방문자 단말이 업무망 자원에 직접 접근하지 못하도록 접근 범위를 나눌 수 있다.
② O — 예측하기 어려운 비밀번호를 관리하고 무선 구간의 데이터를 암호화하면 비인가 접속과 통신 내용 노출의 위험을 줄일 수 있다.
③ O — AP 접근 권한을 통제하고 WIPS로 비인가 사용자나 불법 AP를 탐지·차단하는 것은 적절한 무선망 보호 대책이다.
④ X — 틀린 표현은 '워 드라이빙을 통해 다양한 사용자 접근을 분석'한다는 부분과 MAC 주소 인증을 주된 보안 강화책처럼 제시한 부분이다. 워 드라이빙은 주변 무선망을 탐색·수집하는 행위이며, 사용자 접근은 인증·접속 로그와 WIPS 등으로 감시한다. MAC 주소는 위조될 수 있으므로 강한 인증과 암호화에 보조적으로 사용해야 한다.

NoteBase

오답 포인트

④는 '주기적 분석'과 '인증'이라는 보안 용어를 넣어 정상적인 관리 활동처럼 보이게 한다. 그러나 워 드라이빙은 사용자 접근 분석 수단이 아니며, MAC 주소만으로는 신뢰할 만한 사용자 인증을 보장하지 못한다.

다시 나오면 이렇게 판단

무선망 대책은 분리·강한 인증·암호화·권한 통제·비인가 AP 탐지에 해당하는지 확인한다. 주변 무선망을 돌아다니며 탐색하는 행위를 정상적인 사용자 접근 분석으로 설명하면 틀린 선지로 판단한다.

암기 포인트

워 드라이빙은 무선망 탐색, WIPS는 비인가 무선 접속 탐지·차단, MAC 인증은 보조 수단이다.

NoteBase

문 16. 다음 중 IDS의 침입탐지 모델인 오용탐지와 이상탐지에 대한 설명으로 가장 옳지 않은 것은?

① 오용탐지 IDS는 시그니처 기반의 탐지방식으로, 오탐발생(False Positive) 확률은 낮다.

② 이상탐지 IDS는 행위기반의 탐지방식으로, 미탐발생(False Negative) 확률은 낮다.

③ 오용탐지 IDS는 패턴과 축약된 데이터를 비교하여 일치 여부를 판단하며, 미탐발생(False Negative) 확률은 낮다.

④ 이상탐지 IDS는 사용자의 행동패턴을 분석하여 이상패턴을 탐지하는 방식으로, 오탐발생(False Positive) 확률은 높다.

정답 3번

출제 포인트

오용탐지와 이상탐지가 무엇을 기준으로 침입을 판정하는지, 그리고 각 방식에서 오탐과 미탐이 어떻게 나타나는지를 구별하는 문제이다.

핵심 개념

오용탐지는 알려진 공격의 시그니처나 패턴과 관측 데이터를 비교하여 일치하면 침입으로 판단하는 방식이다. 알려진 공격은 정확히 잡아 오탐은 적지만, 등록되지 않은 새로운 공격을 놓치기 쉬워 미탐은 많다.
이상탐지는 정상적인 사용자·시스템 행동을 기준으로 삼고, 그 기준에서 크게 벗어난 행위를 침입으로 판단하는 방식이다. 새로운 공격도 탐지할 수 있어 미탐은 적지만, 정상적인 행동 변화도 공격으로 판단할 수 있어 오탐은 많다.

선지별 해설

① O — 오용탐지는 알려진 공격 시그니처와 일치하는지를 확인하므로 정상 행위를 공격으로 잘못 판단하는 오탐(False Positive)이 비교적 적다.
② O — 이상탐지는 정상 행위에서 벗어난 패턴을 탐지하므로 알려지지 않은 공격도 포착할 수 있어 미탐(False Negative)이 비교적 적다.
③ X — 패턴과 데이터를 비교한다는 설명은 오용탐지에 해당하지만, '미탐발생(False Negative) 확률은 낮다'는 부분이 틀렸다. 오용탐지는 등록된 시그니처가 없는 새로운 공격을 놓치기 쉬우므로 미탐 확률은 높다고 고쳐야 한다.
④ O — 이상탐지는 사용자의 정상 행동패턴과 다른 행위를 탐지하며, 정상적인 행동 변화까지 침입으로 판단할 수 있으므로 오탐(False Positive)이 비교적 많다.

오답 포인트

③의 앞부분인 '패턴과 축약된 데이터를 비교'는 오용탐지의 특성과 맞기 때문에 선지 전체를 옳다고 보기 쉽다. 그러나 시그니처에 없는 공격은 잡기 어렵다는 점에서 '미탐 확률은 낮다'가 반대로 제시되었다.

NoteBase

다시 나오면 이렇게 판단

알려진 공격 패턴과의 일치 여부를 보면 오용탐지, 정상 행동에서의 이탈 여부를 보면 이상탐지로 판단한다. 이어서 오용탐지는 오탐이 낮고 미탐이 높으며, 이상탐지는 오탐이 높고 미탐이 낮다는 대응 관계를 적용한다.

암기 포인트

오용탐지는 '아는 공격만 정확히'라서 오탐은 낮고 미탐은 높다. 이상탐지는 '낯선 행동도 의심'하므로 미탐은 낮고 오탐은 높다.

NoteBase

문 17. 다음 중 VPN의 일반적인 특징에 대한 설명으로 가장 옳은 것은?

① VPN의 주요기능으로 로그분석, 인증, 암호화, 터널링이 있다.

② VPN 터널링은 출발지와 목적지 간의 데이터 무결성을 보장한다.

③ 두 개의 네트워크를 VPN으로 구성시, IPSec 프로토콜을 적용한다.

④ SSL VPN은 TCP/IP의 3계층에서 터널링을 수행하며, 두 개의 네트워크 간 안전한 자료전송을 보장한다.

정답 3번

출제 포인트

이 문제는 VPN의 핵심 기능과 IPSec VPN·SSL VPN의 동작 계층 및 용도를 구분하는 문제이다.

핵심 개념

VPN은 공중망을 이용하면서 인증, 암호화, 무결성 보호, 터널링 등을 통해 사설망처럼 안전한 통신 경로를 구성하는 기술이다.
터널링은 원래 패킷을 다른 패킷 안에 캡슐화하여 가상 통신 경로로 전달하는 방식이며, 그 자체가 암호화나 무결성 검증을 뜻하지는 않는다.
IPSec VPN은 네트워크 계층에서 IP 패킷을 보호하므로 두 네트워크를 연결하는 사이트 간 VPN에 널리 쓰인다.
SSL VPN은 TCP 위의 SSL/TLS를 이용하며 주로 원격 사용자가 웹 브라우저나 전용 클라이언트로 내부 자원에 안전하게 접속할 때 쓰인다.

선지별 해설

① X — 틀린 표현은 '로그분석'이 VPN의 주요 기능이라는 부분이다. 로그 분석은 VPN 장비의 운영·감사 기능에 해당하며, VPN 자체의 핵심 기능은 인증, 암호화, 무결성 보호, 터널링 등이다.
② X — 틀린 표현은 '터널링이 데이터 무결성을 보장한다'는 부분이다. 터널링은 패킷을 캡슐화하여 전달 경로를 만드는 기능이고, 무결성은 해시 기반 인증 등 별도의 무결성 검증 기능으로 보장한다.
③ O — 서로 떨어진 두 네트워크를 안전하게 연결하는 사이트 간 VPN에는 네트워크 계층에서 IP 패킷을 보호하는 IPSec 프로토콜이 일반적으로 적용된다.
④ X — 틀린 표현은 'SSL VPN은 TCP/IP의 3계층에서 터널링을 수행한다'는 부분이다. 네트워크 계층에서 동작하는 것은 대표적으로 IPSec VPN이며, SSL VPN은 TCP 위의 SSL/TLS를 이용하여 주로 사용자와 내부 자원 사이의 원격 접속을 보호한다.

오답 포인트

터널을 만든다는 사실과 그 안의 데이터가 무결성 보호를 받는다는 사실을 같은 기능으로 보는 것이 함정이다.
또한 네트워크 계층의 IPSec VPN과 TCP 위에서 동작하는 SSL VPN의 계층을 서로 바꾸어 제시한 ④에 주의한다.

NoteBase

다시 나오면 이렇게 판단

두 네트워크 전체를 연결하면 사이트 간 IPSec VPN, 개별 사용자의 원격 접속이면 SSL VPN을 우선 떠올린다. 터널링은 캡슐화, 암호화는 기밀성, 해시·인증은 무결성이라는 기능별 역할도 분리하여 판단한다.

암기 포인트

IPSec는 네트워크 대 네트워크, SSL VPN은 사용자 대 내부 자원, 터널링은 캡슐화이다.

NoteBase

문 18. 다음 중 수신측 개체가 송신측 개체로부터 오는 데이터의 양이나 속도를 제한하는 프로토콜의 기능으로 가장 옳은 것은?

① 연결 제어
② 오류 제어
③ 순서 제어
④ 흐름 제어

정답 4번

출제 포인트

이 문제는 통신 프로토콜의 연결 제어, 오류 제어, 순서 제어, 흐름 제어를 기능에 따라 구별하는 문제이다.

핵심 개념

흐름 제어는 수신측의 처리 능력과 버퍼 용량에 맞추어 송신측이 보내는 데이터의 양이나 전송 속도를 조절하는 기능이다.
연결 제어는 통신 연결의 설정·유지·해제를 관리하고, 오류 제어는 전송 중 발생한 오류를 검출하고 복구하며, 순서 제어는 데이터가 올바른 순서로 전달·재조립되도록 관리한다.

선지별 해설

① X — 연결 제어는 통신 연결의 설정·유지·해제를 관리하는 기능이다. 틀린 표현은 '연결 제어'이며, 제시된 기능은 '흐름 제어'이다.
② X — 오류 제어는 전송 오류를 검출하고 재전송 등의 방법으로 복구하는 기능이다. 틀린 표현은 '오류 제어'이며, 제시된 기능은 '흐름 제어'이다.
③ X — 순서 제어는 분할되어 전송된 데이터가 올바른 순서로 전달·재조립되도록 관리하는 기능이다. 틀린 표현은 '순서 제어'이며, 제시된 기능은 '흐름 제어'이다.
④ O — 흐름 제어는 수신측이 감당할 수 있는 범위에 맞추어 송신측의 데이터 양이나 전송 속도를 제한·조절하는 기능이므로 제시된 설명과 일치한다.

오답 포인트

'제어'라는 공통 표현 때문에 각 기능을 혼동하기 쉽다. 이 문항의 결정적 단서는 수신측이 송신측의 데이터 양이나 속도를 제한한다는 부분이며, 이는 오류 발생 여부나 데이터 순서가 아니라 수신 능력에 맞춘 전송량 조절을 뜻한다.

NoteBase

다시 나오면 이렇게 판단

수신측의 처리 속도·버퍼와 송신량의 균형을 묻는 경우 흐름 제어로 판단한다. 연결의 설정·해제는 연결 제어, 손상·유실의 검출과 복구는 오류 제어, 도착 순서의 보장은 순서 제어로 구별한다.

암기 포인트

양·속도는 흐름, 손상·유실은 오류, 앞뒤 순서는 순서, 연결의 시작과 끝은 연결 제어이다.

NoteBase

문 19. 재해복구 시스템 유형 중 다음의 설명에 가장 부합하는 것은?

◯ 주 센터와 동일한 수준의 정보기술 자원을 원격지에 구축하여 대기(Active-Standby)
◯ 복구목표시간(RTO)은 1시간
◯ 신속한 업무재개 및 데이터의 업데이트가 많은 경우에 적합
◯ 주 센터 재해시 원격지 시스템을 운영(Active) 상태로 전환

① Hot Site
② Mirror Site
③ Warm Site
④ Cold Site

정답 1번

출제 포인트

재해복구 사이트를 시스템의 준비 수준, 운영 방식, 복구 속도로 구분하는 문제이다. 동일 수준의 자원을 갖춘 대기 센터를 재해 시 가동하고 RTO가 1시간이라는 조건은 Hot Site에 해당한다.

핵심 개념

Hot Site: 주 센터와 유사한 수준의 시스템을 원격지에 미리 구축하고 대기 상태로 유지하다가 재해 시 신속히 전환하는 방식이다. 키워드는 Active-Standby와 짧은 RTO이다.
Mirror Site: 주 센터의 시스템과 데이터를 원격지에서 실시간으로 동기화하며 양쪽을 가동 상태로 유지해 즉시 또는 거의 즉시 서비스를 이어 가는 방식이다. 키워드는 Active-Active와 실시간 동기화이다.
Warm Site: 일부 장비와 설비를 갖추고 데이터 백업을 보관하지만, 복구 시 추가 설치와 데이터 복원이 필요한 방식이다.
Cold Site: 전력·통신·공간 등 기본 시설 위주로 확보하고 시스템과 데이터를 재해 후 마련하는 방식이다.

NoteBase

선지별 해설

① O — Hot Site는 주 센터와 유사한 수준의 정보기술 자원을 원격지에 구축해 Active-Standby로 대기시키고, 재해 시 원격지 시스템을 Active 상태로 전환하여 짧은 시간 안에 업무를 재개하는 방식이다. 제시된 RTO 1시간과도 부합한다.
② X — Mirror Site가 아니라 Hot Site이다. Mirror Site는 단순 대기 후 전환하는 Active-Standby가 아니라 주 센터와 원격지를 모두 가동하는 Active-Active와 실시간 데이터 동기화를 통해 복구 중단을 최소화하는 방식이다.
③ X — Warm Site가 아니라 Hot Site이다. Warm Site는 일부 자원만 사전 구축하므로 재해 후 장비 구성과 데이터 복원 절차가 더 필요하며, 동일 수준의 자원을 즉시 전환하는 방식보다 복구가 느리다.
④ X — Cold Site가 아니라 Hot Site이다. Cold Site는 원격지의 공간·전력·통신 같은 기반 시설을 중심으로 준비하고, 재해 발생 후 시스템 설치와 데이터 복원을 진행하므로 RTO 1시간의 신속한 전환에 적합하지 않다.

오답 포인트

‘주 센터와 동일한 수준의 자원’과 ‘데이터 업데이트가 많은 경우’만 보면 Mirror Site로 오인하기 쉽다. 그러나 이 문항의 결정적 표현은 ‘대기(Active-Standby)’와 ‘재해 시 Active 상태로 전환’이다. Mirror Site의 핵심은 Active-Active와 실시간 동기화이고, Hot Site의 핵심은 미리 준비된 대기 시스템으로의 신속한 전환이다.

다시 나오면 이렇게 판단

운영 상태를 먼저 확인한다. Active-Active·실시간 동기화이면 Mirror Site, Active-Standby·신속 전환이면 Hot Site, 일부 장비만 준비되어 추가 복원이 필요하면 Warm Site, 기반 시설만 준비되어 있으면 Cold Site로 판단한다.

암기 포인트

Mirror는 양쪽이 함께 Active, Hot은 준비된 시스템이 Standby, Warm은 일부 준비, Cold는 장소와 기반 시설 중심이다.

NoteBase

문 20. 다음 중 ISO/IEC15408 국제보안표준 CC(공통기준)에 대한 설명으로 가장 옳은 것은?

① EAL은 보증요구와 관련된 컴포넌트로 보증수준을 7개의 등급으로 나누고(EAL7~EAL1), EAL1은 부적합으로 분류한다.

② TOE는 CC평가 대상이 되는 시스템으로, 요구되는 보안 해결책을 제공하기 위해 제안된 제품이다.

③ PP는 보호 프로파일로, 요구되는 보안 해결책을 충족하는 보안 기능과 보증 매커니즘을 담은 공급업체 설명문서이다.

④ ST는 보안목표 명세서로, 갖추어야 할 공통적인 보안 요구사항을 모아 놓은 것으로, 패키지, EAL, 기능 및 보증요구 컴포넌트 등의 집합으로 구성된다.

정답 2번

출제 포인트

이 문제는 CC에서 평가 대상인 TOE와 보안 요구사항 문서인 PP·ST, 그리고 보증 수준인 EAL을 구별하는 문제이다.

핵심 개념

TOE(Target of Evaluation)는 CC 평가를 받는 제품 또는 시스템이다.
PP(Protection Profile)는 특정 제품의 구현과 독립적으로 일정 유형의 TOE에 필요한 보안 요구사항을 제시하는 문서이다.
ST(Security Target)는 특정 TOE가 충족하겠다고 제시하는 보안 요구사항과 보안 기능을 기술한 평가 기준 문서이다.
EAL(Evaluation Assurance Level)은 보증 요구 컴포넌트들을 묶은 보증 패키지이며, EAL1부터 EAL7까지 단계가 높아질수록 평가의 엄격성과 보증 수준이 높아진다.

NoteBase

선지별 해설

① X — EAL은 하나의 보증요구 컴포넌트가 아니라 보증요구 컴포넌트들을 조합한 보증 패키지이다. 또한 EAL1은 부적합 등급이 아니라 가장 낮은 단계의 보증 수준으로서 기능 시험을 중심으로 평가하는 등급이다. 따라서 '컴포넌트'와 'EAL1은 부적합'이라는 표현을 각각 '보증 패키지'와 'EAL1은 최저 보증 등급'으로 고쳐야 한다.
② O — TOE는 Target of Evaluation의 약자로, CC에 따라 보안성을 평가하는 대상 제품 또는 시스템을 뜻한다. 요구되는 보안 문제에 대응할 보안 기능을 제공하는 평가 대상이라는 설명이 맞다.
③ X — PP는 공급업체가 특정 제품의 보안 기능과 보증 메커니즘을 설명하는 문서가 아니다. PP는 사용자 관점에서 특정 유형의 TOE에 요구되는 보안 기능 요구사항과 보증 요구사항을 구현 독립적으로 제시하는 문서이다. 특정 TOE에 관한 공급업체의 보안 주장은 ST에 기술된다.
④ X — ST를 '공통적인 보안 요구사항'을 모아 놓은 문서라고 한 부분이 틀렸다. 공통 유형의 TOE에 대한 구현 독립적 요구사항은 PP에 해당하며, ST는 식별된 특정 TOE에 적용되는 보안 요구사항과 TOE 요약 명세 등을 제시한다. ST가 단순히 패키지·EAL·기능 및 보증요구 컴포넌트의 집합으로 정의되는 것도 아니다.

오답 포인트

③과 ④는 PP와 ST의 역할을 서로 섞은 선지이다. '공통 유형·구현 독립'이면 PP이고, '특정 TOE·평가 기준·공급업체의 보안 주장'이면 ST이다. ①에서는 EAL1을 낮은 보증 수준과 부적합 판정으로 혼동하기 쉽지만, EAL1도 정식 보증 등급이다.

다시 나오면 이렇게 판단

평가받는 대상이면 TOE, 특정 제품과 무관한 공통 요구사항이면 PP, 특정 TOE가 충족할 요구사항을 적은 문서이면 ST, 보증 평가의 단계이면 EAL로 판단한다.

암기 포인트

TOE는 평가 대상, PP는 제품군의 공통 요구, ST는 특정 제품의 보안 목표, EAL은 1부터 7까지의 보증 수준이다.

NoteBase