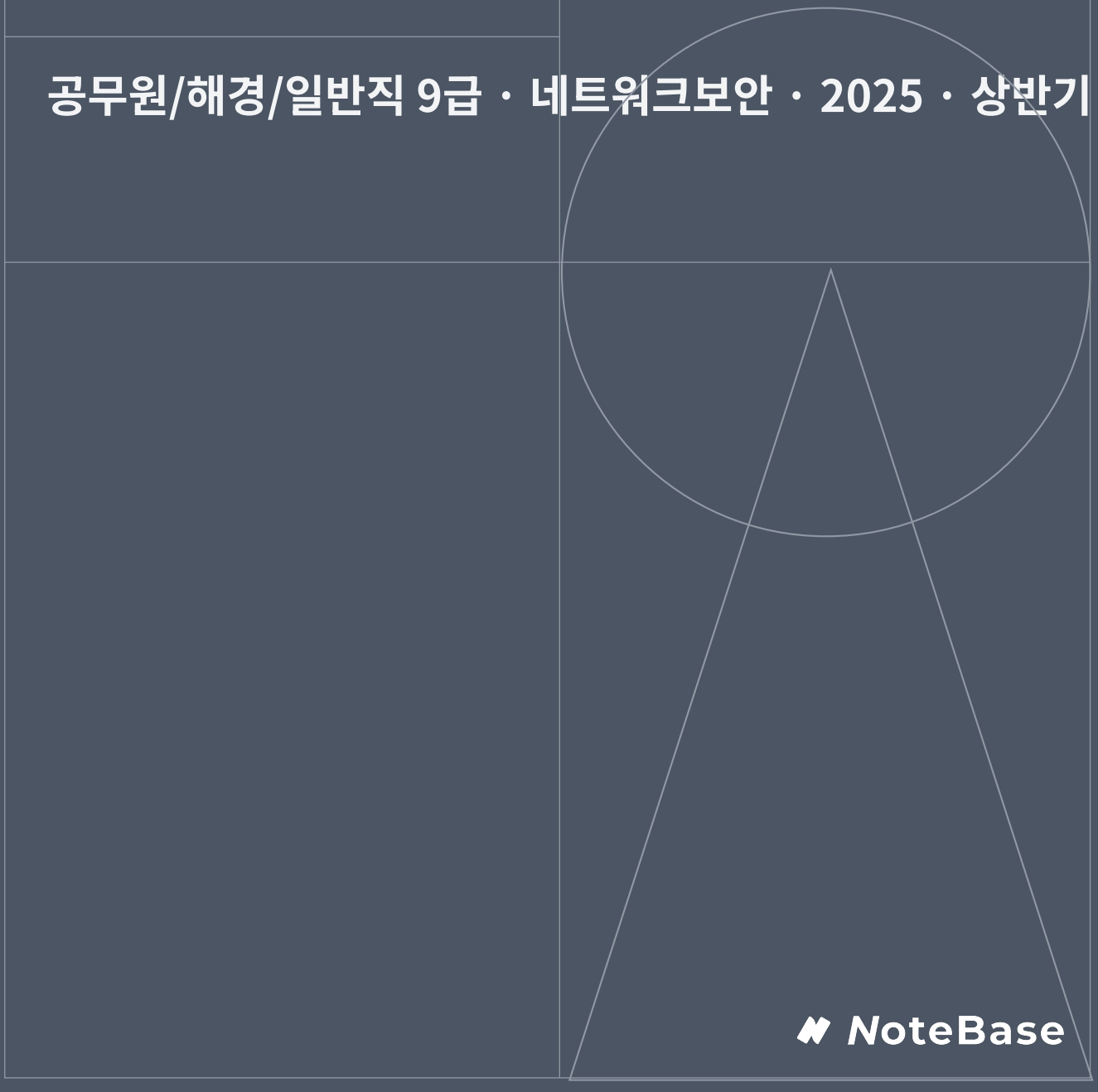
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2025 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2025 · 상반기

공무원/해경/일반직 9급 · 네트워크보안 · 2025 · 상반기

문 1. IPv4 및 IPv6에 관련된 내용으로 가장 옳지 않은 것은?

① IPv4와 IPv6는 동일 LAN에서 운영이 가능하다.

② IPv6에서 브로드캐스트는 제거되었다.

③ IPv6에서 QoS가 추가되어 응용 특성에 따른 전송이 지원된다.

④ IPv4와 IPv6 모두 보안을 위하여 IPSec 프로토콜의 추가 설치가 필요하다.

정답 4번

출제 포인트

IPv4와 IPv6의 공존 방식, 주소 전달 방식, QoS 지원 필드, IPsec 지원 구조의 차이를 묻는 문제이다.

핵심 개념

IPv4와 IPv6는 듀얼 스택 등의 전환 기술을 이용하여 같은 LAN에서 함께 운용할 수 있다. IPv6는 브로드캐스트를 사용하지 않고 멀티캐스트와 애니캐스트를 활용하며, 트래픽 클래스와 흐름 레이블을 통해 응용 흐름별 처리를 지원한다. IPsec은 두 버전에서 사용할 수 있지만, IPv4와 IPv6 모두 반드시 별도로 추가 설치해야 한다고 단정할 수는 없다.

선지별 해설

① O — 하나의 LAN에서 장비가 IPv4와 IPv6를 함께 처리하는 듀얼 스택 방식으로 두 프로토콜을 동시에 운용할 수 있다.
② O — IPv6에는 브로드캐스트 주소가 없으며, 여러 수신자에게 전달할 때 멀티캐스트 등을 사용한다.
③ O — IPv6 기본 헤더의 트래픽 클래스와 흐름 레이블은 트래픽의 우선순위와 흐름을 식별하여 응용 특성에 따른 QoS 처리를 지원한다.
④ X — 틀린 부분은 ‘IPv4와 IPv6 모두 IPSec 프로토콜의 추가 설치가 필요하다’이다. IPsec은 IPv4와 IPv6 모두에서 사용할 수 있으나, IPv6는 IPsec을 고려한 보안 확장 헤더 체계를 표준 구조에 포함하므로 두 버전 모두 별도 추가 설치가 반드시 필요하다는 설명은 옳지 않다. 올바르게는 ‘IPv4와 IPv6 모두 IPsec을 사용할 수 있으며, 실제 보안 통신에는 IPsec의 구현과 설정이 필요하다’이다.

NoteBase

오답 포인트

④는 ‘IPsec을 사용할 수 있다’와 ‘반드시 추가 설치해야 한다’를 바꾸어 놓은 선지이다. 또한 IPv6가 IPsec을 지원한다는 말은 모든 IPv6 통신이 자동으로 암호화된다는 뜻이 아니다.

다시 나오면 이렇게 판단

IPv6의 대표 변화는 브로드캐스트 제거, 멀티캐스트·애니캐스트 활용, 트래픽 클래스·흐름 레이블 지원, 확장 헤더 구조이다. 보안 선지는 ‘IPsec 지원’과 ‘항상 적용 또는 별도 설치 필수’를 구분하여 판단한다.

암기 포인트

IPv6는 브로드캐스트 없이 멀티캐스트를 쓰고, 트래픽 클래스·흐름 레이블과 IPsec 지원 구조를 갖는다.

NoteBase

문 2. 패킷 전송 프로토콜에 관련된 내용으로 가장 옳지 않은 것은?

① TCP는 연결지향 UDP는 비연결지향 프로토콜이다.

② TCP 헤더에 비해 UDP 헤더는 더 많은 필드 항목으로 구성된다.

③ TCP는 순서번호를 통해 데이터 전송 순서를 구현한다.

④ 데이터의 부분 유실을 감내할 수 있는 경우, UDP 전송방식이 더 효율적이다.

정답 2번

출제 포인트

TCP와 UDP의 연결 방식, 헤더 구조, 전송 신뢰성 및 효율성의 차이를 묻는 문제이다.

핵심 개념

TCP는 연결을 설정한 뒤 순서번호, 확인 응답, 재전송 등을 이용하여 신뢰성 있는 전송을 제공하는 연결지향 프로토콜이다. UDP는 연결 설정이나 순서·재전송 제어 없이 데이터그램을 보내는 비연결지향 프로토콜이다. TCP 헤더는 최소 20바이트이고 여러 제어 필드를 가지지만, UDP 헤더는 8바이트의 단순한 구조로 출발지 포트, 목적지 포트, 길이, 체크섬의 4개 필드로 구성된다.

선지별 해설

① O — TCP는 통신 전에 연결을 설정하는 연결지향 프로토콜이고, UDP는 연결 설정 없이 전송하는 비연결지향 프로토콜이다.
② X — 틀린 부분은 'UDP 헤더는 더 많은 필드 항목으로 구성된다'이다. 실제로는 TCP 헤더가 순서번호, 확인번호, 제어 비트 등 더 많은 필드를 가지며, UDP 헤더는 4개 필드만 가진다.
③ O — TCP는 세그먼트의 순서번호를 이용하여 수신 측에서 데이터의 순서를 확인하고 올바른 순서로 재조립한다.
④ O — 일부 데이터 유실을 허용하는 실시간 음성·영상 전송 등에서는 연결 설정, 확인 응답, 재전송 부담이 적은 UDP가 더 효율적일 수 있다.

오답 포인트

UDP가 빠르고 단순하다는 점을 헤더 필드가 더 많다는 뜻으로 뒤집은 ②가 함정이다. UDP의 효율성은 제어 필드와 신뢰성 제어 절차가 적어서 생긴다.

다시 나오면 이렇게 판단

연결 설정·순서 보장·확인 응답·재전송이 제시되면 TCP, 작은 헤더·낮은 오버헤드·일부 유실 허용이 제시되면 UDP로 판단한다. 헤더 필드 수는 TCP가 더 많다.

NoteBase

암기 포인트

TCP는 연결·순서·신뢰성, UDP는 비연결·단순 헤더·낮은 오버헤드이다.

NoteBase

문 3. 다음 네트워크 장비에 관련한 서술에서 가장 옳지 않은 것은?

① 더미 허브에 비하여 L3 스위치를 사용할 경우 패킷 충돌이 줄어든다.

② 네트워크 간 연결에서 전체 대역폭 감소를 경감하기 위해서는 브릿지 대신 라우터를 쓰는 것이 좋다.

③ 스위치는 다양한 계층 수준으로 구현한 제품이 있으며, L3 스위치부터는 패킷 전송 페이로드 데이터 내용을 분석하여 처리한다.

④ VLAN은 일부 단말을 선택하여 가상의 LAN으로 구성되도록 하는 기능이다.

정답 3번

출제 포인트

허브·브릿지·라우터·계층별 스위치·VLAN이 트래픽을 처리하는 기준과 충돌 도메인 및 브로드캐스트 도메인을 구분하는 문제이다.

핵심 개념

더미 허브는 수신 신호를 모든 포트로 내보내 하나의 충돌 도메인을 공유하게 하는 물리 계층 장비이다. 브릿지와 L2 스위치는 MAC 주소를 기준으로 프레임을 전달하고 포트별로 충돌 도메인을 나눈다. 라우터와 L3 스위치는 IP 주소 등 네트워크 계층 헤더를 기준으로 패킷을 전달하며 브로드캐스트 도메인을 구분한다. VLAN은 물리적 위치와 관계없이 선택한 포트나 단말을 논리적으로 묶어 별도의 LAN과 브로드캐스트 도메인을 구성하는 기능이다.

선지별 해설

① O — 더미 허브는 모든 단말이 하나의 충돌 도메인을 공유하지만, L3 스위치는 스위칭 포트별로 충돌 도메인을 분리하고 일반적으로 전이중 통신을 지원하므로 패킷 충돌이 줄어든다.
② O — 브릿지는 충돌 도메인을 나누지만 브로드캐스트 트래픽은 다른 세그먼트로 전달한다. 라우터는 네트워크를 서로 다른 브로드캐스트 도메인으로 분리하므로 불필요한 브로드캐스트 확산과 그에 따른 대역폭 소모를 줄일 수 있다.
③ X — 틀린 표현은 'L3 스위치부터는 패킷 전송 페이로드 데이터 내용을 분석하여 처리한다'이다. L3 스위치는 주로 IP 주소 등 네트워크 계층 헤더를 분석하여 패킷을 전달한다. 페이로드의 응용 계층 내용까지 분석하는 기능은 일반적인 L3 스위치의 기준이 아니라 L7 스위치나 심층 패킷 검사 기능에 해당한다.
④ O — VLAN은 스위치의 일부 포트나 단말을 논리적으로 묶어 하나의 가상 LAN으로 구성하는 기능이다. 같은 VLAN의 단말은 물리적으로 떨어져 있어도 같은 논리적 브로드캐스트 도메인에 속할 수 있다.

NoteBase

오답 포인트

③은 L3 스위치가 '패킷'을 처리한다는 사실을 '패킷의 페이로드 내용'을 분석한다는 뜻으로 바꾼 것이 함정이다. 계층을 판별할 때는 장비가 보는 정보가 IP 헤더인지, TCP·UDP 포트 정보인지, 응용 계층 페이로드인지 구분해야 한다.

다시 나오면 이렇게 판단

장비가 전달 판단에 사용하는 주소와 정보의 계층을 확인한다. 허브는 주소를 보지 않고 신호를 반복하며, L2 스위치는 MAC 주소, 라우터와 L3 스위치는 IP 주소를 본다. 응용 데이터의 내용 분석이 제시되면 일반적인 L3 기능이 아니라 상위 계층 장비나 심층 패킷 검사 기능인지 판단한다.

암기 포인트

허브는 하나의 충돌 도메인, 스위치는 충돌 도메인 분리, 라우터·L3 스위치는 IP 헤더 기반 전달, VLAN은 논리적 LAN 분리이다.

NoteBase

문 4. 정보통신망을 통한 침해사고가 발생하였을 때, 이에 대한 처리, 대응, 예방, 복구를 수행하는 조직은?

① PEM

② CERT

③ CCRA

④ ISMS-P

정답 2번

출제 포인트

침해사고의 처리·대응·예방·복구를 담당하는 조직인 CERT와 보안 표준·협정·인증체계를 구별하는 문제이다.

핵심 개념

CERT(Computer Emergency Response Team)는 컴퓨터·정보통신망 침해사고에 대응하는 전문 조직이다. 사고 신고 접수와 분석, 대응 지원, 피해 복구, 재발 방지 활동을 수행한다.
PEM은 전자우편 보안 기술, CCRA는 정보보호제품 평가 인증서의 국제 상호인정 협정, ISMS-P는 정보보호 및 개인정보보호 관리체계 인증 제도이다.

선지별 해설

① X — PEM(Privacy Enhanced Mail)은 전자우편의 기밀성·무결성·인증 등을 제공하기 위한 보안 규격이지 침해사고 대응 조직이 아니다. 틀린 표현은 '침해사고를 처리·대응·예방·복구하는 조직이 PEM'이라는 대응 관계이며, 올바르게는 그 조직이 CERT이다.
② O — CERT는 침해사고를 접수·분석하고 대응과 복구를 지원하며 예방 활동도 수행하는 침해사고 대응 조직이다.
③ X — CCRA(Common Criteria Recognition Arrangement)는 공통평가기준에 따른 정보보호제품 평가·인증 결과를 참여국 사이에서 상호 인정하기 위한 협정이지 침해사고 대응 조직이 아니다. 올바르게는 침해사고 대응 조직이 CERT이다.
④ X — ISMS-P는 조직의 정보보호 및 개인정보보호 관리체계를 심사·인증하는 제도이지 개별 침해사고의 처리와 복구를 수행하는 대응 조직이 아니다. 올바르게는 침해사고 대응 조직이 CERT이다.

오답 포인트

네 용어가 모두 정보보호 분야에 속하지만 성격이 다르다. 특히 ISMS-P의 '관리체계'와 CERT의 '대응 조직'을 혼동하기 쉽다. 문제의 '사고 처리·대응·복구를 수행하는 조직'이라는 표현이 CERT를 가리키는 결정적 단서이다.

NoteBase

다시 나오면 이렇게 판단

용어의 성격을 먼저 구분한다. 침해사고 대응 조직이면 CERT, 전자우편 보안이면 PEM, 평가·인증의 국제 상호인정이면 CCRA, 정보보호·개인정보보호 관리체계 인증이면 ISMS-P로 판단한다.

암기 포인트

CERT는 사고 대응팀, PEM은 메일 보안, CCRA는 인증 상호인정, ISMS-P는 관리체계 인증이다.

NoteBase

문 5. 무선랜에 관련된 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ WEP는 보안 수준이 낮아 해킹 위험이 높다.
㉡ TKIP과 CCMP 중 CCMP를 선택할 경우 상대적으로 더 위험하다.
㉢ WPA2 수준을 보다 보완하여 WPA3가 구현되었다.
㉣ 등록된 MAC 주소만 연결할 수 있도록 AP를 설정하면 보안이 충분하다.

① ㉠, ㉢
② ㉠, ㉣
③ ㉡, ㉢
④ ㉡, ㉣

정답 1번

출제 포인트

무선랜 보안 방식인 WEP·TKIP·CCMP·WPA3의 상대적 안전성과 MAC 주소 필터링의 한계를 구별하는 문제이다.

핵심 개념

WEP는 오래된 무선랜 보안 방식으로 암호화 취약점 때문에 안전성이 낮다.
TKIP은 기존 장비와의 호환성을 고려한 과도기적 방식이고, CCMP는 AES 기반으로 TKIP보다 강한 보안을 제공한다.
WPA3는 WPA2의 한계를 보완해 인증과 암호 보호를 강화한 규격이다.
MAC 주소 필터링은 허용된 장치를 제한하는 보조 수단일 뿐이며, MAC 주소 위조가 가능하므로 이것만으로 충분한 보안이 되지 않는다.

선지별 해설

① O — ㉠과 ㉢은 모두 옳다. WEP는 취약해 해킹 위험이 높고, WPA3는 WPA2의 보안 한계를 보완한 규격이다.
② X — ㉠은 옳지만 ㉣이 틀렸다. 틀린 표현은 '보안이 충분하다'이다. 올바르게는 등록된 MAC 주소만 허용하는 설정은 보조적 접근 통제 수단이며, 주소 위조가 가능하므로 별도의 강한 인증·암호화가 필요하다.
③ X — ㉢은 옳지만 ㉡이 틀렸다. 틀린 표현은 'CCMP를 선택할 경우 상대적으로 더 위험하다'이다. 올바르게는 CCMP가 TKIP보다 상대적으로 더 안전하다.
④ X — ㉡과 ㉣이 모두 틀렸다. CCMP는 TKIP보다 더 안전하며, MAC 주소 제한만으로는 충분한 보안을 확보할 수 없다.

NoteBase

오답 포인트

㉡은 TKIP과 CCMP의 보안 수준을 반대로 서술했고, ㉣은 MAC 주소 필터링을 완전한 보안 수단처럼 과장했다. 조합형에서는 ㉡과 ㉣ 중 하나라도 포함된 선택지를 제외하면 ㉠과 ㉢을 묶은 1번만 남는다.

다시 나오면 이렇게 판단

무선랜 보안 방식은 WEP보다 WPA 계열이 강하고, TKIP보다 CCMP가 강하다는 방향으로 판단한다. MAC 주소 필터링처럼 쉽게 우회 가능한 장치 식별 방식은 단독 보안 수단이 아니라 보조 수단으로 판단한다.

암기 포인트

WEP는 취약, CCMP는 TKIP보다 강함, WPA3는 WPA2 보완, MAC 필터링은 보조 수단이다.

NoteBase

문 6. 모바일 기기 보안에 관련된 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ MDM 기능을 이용하여 분실 기기에 대한 원격감시, 관리가 가능하나 원격 기기의 자료 삭제는 어렵다.
㉡ 가상화 컨테이너 기술을 이용하여 격리 및 보안영역을 구현할 수 있다.
㉢ BYOD는 개인 기기를 이용, 업무에 사용할 수 있도록 확장하는 방법이다.
㉣ 샌드박스 기술은 응용 프로그램 간 네트워크를 통합, 연결성을 보장한다.

① ㉠, ㉢
② ㉠, ㉣
③ ㉡, ㉢
④ ㉡, ㉣

정답 3번

출제 포인트

모바일 기기 보안에서 MDM, 컨테이너 기술, BYOD, 샌드박스의 기능을 구별하고 옳은 설명의 조합을 찾는 문제이다.

핵심 개념

MDM은 조직이 모바일 기기를 원격으로 설정·감시·통제하는 관리 기술이며, 분실 시 잠금이나 업무 자료 삭제 같은 조치를 할 수 있다.
컨테이너 기술은 개인 영역과 업무 영역을 논리적으로 분리하여 업무 데이터와 앱을 격리·보호한다.
BYOD는 개인 소유 기기를 업무에 활용하도록 허용하는 방식이다.
샌드박스는 응용 프로그램을 제한되고 격리된 실행 환경에서 동작하게 하여 다른 앱이나 시스템에 미치는 영향을 줄이는 기술이다.

선지별 해설

① X — ㉠은 틀리고 ㉢은 옳으므로 옳은 내용의 조합이 아니다. ㉠의 틀린 표현은 '원격 기기의 자료 삭제는 어렵다'이다. MDM은 분실 기기의 자료를 원격으로 삭제할 수 있다.
② X — ㉠과 ㉣이 모두 틀리므로 옳은 내용의 조합이 아니다. ㉠은 MDM으로 원격 자료 삭제가 가능하다고 고쳐야 하며, ㉣은 샌드박스가 응용 프로그램을 서로 격리한다고 고쳐야 한다.
③ O — ㉡의 컨테이너 기술은 격리된 보안 영역을 구현할 수 있고, ㉢의 BYOD는 개인 기기를 업무에 활용하는 방식이므로 두 내용이 모두 옳다.
④ X — ㉡은 옳지만 ㉣은 틀리므로 옳은 내용의 조합이 아니다. ㉣의 틀린 표현은 '응용 프로그램 간 네트워크를 통합, 연결성을 보장한다'이다. 샌드박스는 응용 프로그램의 실행 환경과 권한을 격리하여 영향을 제한한다.

NoteBase

오답 포인트

㉠은 MDM을 단순 감시 도구로만 좁혀 원격 삭제 기능을 부정하고, ㉣은 격리 기술인 샌드박스를 연결성 보장 기술처럼 바꾸어 놓았다. '관리·통제'와 '격리'라는 핵심 기능을 기준으로 판단해야 한다.

다시 나오면 이렇게 판단

MDM은 기기 원격 관리, 컨테이너와 샌드박스는 격리, BYOD는 개인 기기의 업무 활용으로 연결한다. 각 보기의 기능이 이 핵심어와 일치하는지 먼저 판별한 뒤 옳은 보기의 조합을 선택한다.

암기 포인트

MDM은 원격 관리·삭제, 컨테이너는 영역 분리, BYOD는 개인 기기 업무 활용, 샌드박스는 앱 격리이다.

NoteBase

문 7. 네트워크 보안에 관련된 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ 스머프(Smurf) 공격은 L3 장치 수준에서 차단하기 어려우며 L4 장치가 필요하다.
㉡ 이메일 스푸핑(Spoofing) 공격은 L3 장치 수준에서 차단하기 어려우며 L7 장치가 필요하다.
㉢ Promiscuous 모드로 LAN카드를 설정하면 카드에 연결된 네트워크의 패킷을 모두 감청할 수 있다.
㉣ DNS 스푸핑(Spoofing)은 DNS 요청에 대해 위조된 서버의 IP로 거짓 정보를 응답하는 것으로, TCP 패킷 형태이다.

① ㉠, ㉡
② ㉡, ㉢
③ ㉢, ㉣
④ ㉠, ㉣

정답 2번

출제 포인트

스머프 공격, 이메일 스푸핑, 무차별 모드, DNS 스푸핑의 동작 계층과 패킷 특성을 구별하는 문제이다.

핵심 개념

스머프 공격은 출발지 IP를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 응답을 피해자에게 집중시키는 공격이다. 라우터의 directed broadcast 차단이나 L3 필터링으로 방어할 수 있다.
이메일 스푸핑은 발신자 주소 등 이메일 정보를 위조하는 응용 계층 공격이므로 메일 헤더와 내용을 검사하는 L7 수준의 보안 기능이 적합하다.
Promiscuous 모드는 LAN 카드가 자신의 MAC 주소로 온 프레임뿐 아니라 해당 인터페이스에 도달한 다른 프레임도 수신하도록 하는 모드이다.
DNS 스푸핑은 위조된 DNS 응답으로 피해자를 거짓 IP 주소에 연결시키는 공격이며, 일반적인 DNS 질의·응답은 UDP를 사용한다.

NoteBase

선지별 해설

① X — ㉠은 틀리고 ㉡은 옳으므로 두 내용을 모두 옳게 묶은 선택지가 아니다. ㉠의 틀린 표현은 'L3 장치 수준에서 차단하기 어려우며 L4 장치가 필요하다'이다. 실제로는 라우터에서 directed broadcast를 차단하거나 ICMP 트래픽을 필터링하는 등 L3 수준에서도 스머프 공격을 방어할 수 있다.
② O — ㉡과 ㉢이 모두 옳다. 이메일 스푸핑은 메일 헤더 등 응용 계층 정보를 확인해야 하므로 L7 장치가 적합하고, Promiscuous 모드는 네트워크 인터페이스에 도달한 프레임을 목적지 MAC 주소와 관계없이 수신하여 감청에 이용될 수 있다.
③ X — ㉢은 옳지만 ㉣은 틀리므로 옳은 내용만 묶은 선택지가 아니다. ㉣의 틀린 표현은 'TCP 패킷 형태이다'이다. 실제로 일반적인 DNS 질의·응답은 UDP 패킷 형태이며, DNS 스푸핑은 이 응답을 위조하여 거짓 IP 주소를 전달한다.
④ X — ㉠과 ㉣이 모두 틀리므로 옳은 내용으로 선택된 조합이 아니다. ㉠은 L3 수준에서도 차단할 수 있고, ㉣의 일반적인 DNS 질의·응답은 TCP가 아니라 UDP를 사용한다. 따라서 올바르게는 ㉠을 '스머프 공격은 L3 장치에서도 차단할 수 있다', ㉣을 'DNS 스푸핑은 일반적으로 위조된 UDP DNS 응답을 이용한다'로 고쳐야 한다.

오답 포인트

㉠에서는 공격이 대량 트래픽을 만든다는 점 때문에 L4 장치가 반드시 필요하다고 오해하기 쉽지만, 핵심인 IP 브로드캐스트와 ICMP는 L3에서 통제할 수 있다. ㉣에서는 DNS가 경우에 따라 TCP도 사용할 수 있다는 사실과 일반적인 DNS 질의·응답의 기본 전송 방식인 UDP를 혼동하기 쉽다.

다시 나오면 이렇게 판단

공격 이름보다 실제로 검사하거나 차단해야 하는 정보를 기준으로 판단한다. IP·ICMP·라우팅 정보는 L3, 포트·세션 정보는 L4, 이메일 헤더나 DNS 응답 내용처럼 응용 프로토콜 내부 정보는 L7에 대응시킨다. DNS 전송 방식은 일반 질의·응답이면 UDP, 큰 응답이나 영역 전송 등 예외적 상황이면 TCP가 사용될 수 있다고 구분한다.

암기 포인트

Smurf는 ICMP·브로드캐스트이므로 L3 차단, 이메일 스푸핑은 메일 내용 검사이므로 L7, Promiscuous는 도달 프레임 수신, 일반 DNS 질의는 UDP이다.

NoteBase

문 8. VPN에 관련된 다음 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ VPN 연결로 원격지 노드를 LAN으로 묶을 수 있다.
㉡ VPN의 보안 기밀 수준은 선택한 암호화 알고리즘에 따라 결정된다.
㉢ PPTP, L2F, L2TP는 2계층 수준, IPSec, SOCKS v5 프로토콜은 5계층 수준에서 연결성을 제공한다.
㉣ IPSec의 전송모드의 패킷은 터널모드 패킷에 비하여 상대적으로 더 큰 크기가 된다.

① ㉠, ㉡
② ㉡, ㉢
③ ㉢, ㉣
④ ㉠, ㉣

정답 1번

출제 포인트

VPN의 기능, 프로토콜이 동작하는 계층, IPsec 전송 모드와 터널 모드의 패킷 구조를 구분하는 문제이다.

핵심 개념

VPN은 공중망을 이용하면서 암호화와 터널링으로 사설망처럼 안전한 논리적 연결을 구성하는 기술이다.
PPTP·L2F·L2TP는 데이터 링크 계층인 2계층에서 터널링을 제공하고, IPsec은 네트워크 계층인 3계층에서 IP 패킷을 보호한다. SOCKS v5는 5계층 수준에서 연결을 중계한다.
IPsec 전송 모드는 원래 IP 헤더를 유지하고 페이로드를 보호한다. 터널 모드는 원래 IP 패킷 전체를 캡슐화하고 새 IP 헤더를 추가하므로 전송 모드보다 패킷이 더 커진다.

선지별 해설

① O — ㉠과 ㉡은 모두 옳다. VPN은 원격지 노드를 하나의 사설 LAN처럼 연결할 수 있고, 기밀성의 강도는 사용하는 암호화 알고리즘의 영향을 받는다.
② X — ㉡은 옳지만 ㉢이 틀렸다. ㉢의 잘못된 표현은 'IPSec이 5계층 수준에서 연결성을 제공한다'는 부분이다. 올바르게는 IPsec은 3계층, SOCKS v5는 5계층 수준에서 동작한다. 따라서 옳은 조합은 ㉠, ㉡이다.
③ X — ㉢과 ㉣은 모두 틀렸다. ㉢은 IPsec의 계층을 5계층으로 잘못 분류했고, ㉣은 두 모드의 패킷 크기를 반대로 설명했다. 올바르게는 IPsec은 3계층에서 동작하며, 새 IP 헤더를 추가하는 터널 모드 패킷이 전송 모드 패킷보다 상대적으로 더 크다.
④ X — ㉠은 옳지만 ㉣이 틀렸다. ㉣의 '전송 모드의 패킷이 더 크다'는 표현은 반대이다. 올바르게는 캡슐화와 새 IP 헤더가 추가되는 터널 모드의 패킷이 더 크다. 따라서 옳은 조합은 ㉠, ㉡이다.

NoteBase

오답 포인트

㉢은 SOCKS v5의 5계층 설명을 IPsec에도 함께 적용하게 만들고, ㉣은 전송 모드와 터널 모드의 오버헤드 크기를 뒤집어 놓았다. IPsec은 3계층이고 새 IP 헤더가 붙는 쪽은 터널 모드이다.

다시 나오면 이렇게 판단

프로토콜 계층은 PPTP·L2F·L2TP는 2계층, IPsec은 3계층, SOCKS v5는 5계층으로 구분한다. IPsec 모드는 새 IP 헤더의 추가 여부를 확인하여, 새 헤더가 추가되는 터널 모드의 오버헤드가 더 크다고 판단한다.

암기 포인트

터널링 2계층은 PPTP·L2F·L2TP, IP 보안 3계층은 IPsec, 5계층은 SOCKS v5이다. IPsec은 '터널 모드 = 새 IP 헤더 = 더 큰 패킷'으로 연결한다.

NoteBase

문 9. 다음 보안 장비에 관련한 <보기> 중 가장 옳은 내용으로 선택된 것은?

<보기>
㉠ 방화벽(Firewall)은 내부의 컴퓨터가 트로이 목마 등 침입에 감염되었을 때 보안성이 급격히 하락한다.
㉡ 배스천 호스트(Bastion Host)는 내부 네트워크와 인터넷 간 연결되는 유일한 경로이므로 외부에서 내부로 전송되는 모든 패킷은 이 호스트를 경유하여야만 한다.
㉢ NAT를 이용하면 외부 네트워크로부터 내부 네트워크상 기계에 대한 직접 액세스가 제한되도록 구성할 수 있다.

① ㉠, ㉡
② ㉡, ㉢
③ ㉠, ㉢
④ ㉠, ㉡, ㉢

정답 4번

출제 포인트

방화벽, 배스천 호스트, NAT가 내부 네트워크를 보호하는 방식과 각각의 한계를 구분하는 문제이다.

핵심 개념

방화벽: 네트워크 경계에서 미리 정한 보안 정책에 따라 통신을 허용하거나 차단하는 장비이다. 이미 내부 호스트가 악성코드에 감염되면 경계 통제만으로는 내부에서 발생하는 공격을 충분히 막기 어렵다.
배스천 호스트: 외부 네트워크에 노출되는 관문 역할을 하도록 보안을 강화한 호스트이다. 외부와 내부 사이의 접근을 이 호스트로 집중시켜 통제한다.
NAT: 내부 주소와 외부 주소를 변환하는 기술이다. 내부 주소를 외부에 직접 드러내지 않고, 외부에서 시작되는 임의의 직접 접속을 제한하도록 구성할 수 있다.

NoteBase

선지별 해설

① X
㉠과 ㉡은 모두 옳지만, 옳은 ㉢을 제외한 불완전한 조합이다. 올바르게는 ㉠, ㉡, ㉢을 모두 선택해야 한다.

② X
㉡과 ㉢은 모두 옳지만, 옳은 ㉠을 제외한 불완전한 조합이다. 올바르게는 ㉠, ㉡, ㉢을 모두 선택해야 한다.

③ X
㉠과 ㉢은 모두 옳지만, 옳은 ㉡을 제외한 불완전한 조합이다. 올바르게는 ㉠, ㉡, ㉢을 모두 선택해야 한다.

④ O
㉠은 내부 호스트가 침해되면 경계형 방화벽의 보호 효과가 크게 약화된다는 설명이고, ㉡은 배스천 호스트에 외부와 내부 사이의 통신 경로를 집중시키는 구성에 관한 설명이며, ㉢은 NAT로 외부에서 내부 호스트에 직접 접근하기 어렵게 구성할 수 있다는 설명이다. 세 내용이 모두 옳다.

오답 포인트

NAT를 단순한 주소 절약 기술로만 보아 ㉢을 제외하거나, 방화벽이 내부 감염까지 완전히 방어한다고 생각하여 ㉠을 제외하기 쉽다. 또한 배스천 호스트의 핵심은 외부와 내부 사이의 접근 경로를 집중해 통제하는 데 있다.

다시 나오면 이렇게 판단

각 장비의 통제 위치를 기준으로 판단한다. 방화벽은 경계의 트래픽, 배스천 호스트는 외부에 노출된 관문, NAT는 주소 변환과 외부발 직접 접근 제한에 초점을 둔다. 조합형 선지에서는 각 진술의 진위를 먼저 독립적으로 판정한 뒤 모두 포함한 조합을 찾는다.

암기 포인트

방화벽은 경계 통제, 배스천 호스트는 강화된 관문, NAT는 주소 변환과 내부 주소 은닉이다.

NoteBase

문 10. 다음 <보기>에서 설명하는 보안 기술은?

<보기>
◯ 빅데이터의 방대한 정보 속에서 단순한 로그 수집 및 분석이 아닌, 사후에 추적이 가능하도록 상관분석과 포렌식 기능을 제공하는 등 지능적 위협에 대한 조기 경고 모니터링 체계

① TMS(Threat Management System)
② SIEM(Security Information Event Management)
③ SOAR(Security Orchestration Automation and Response)
④ NGFW(Next Generation Firewall)

정답 2번

출제 포인트

방대한 보안 로그와 이벤트를 모아 상관분석하고, 포렌식과 조기 경보에 활용하는 SIEM의 핵심 기능을 식별하는 문제이다.

핵심 개념

SIEM은 여러 정보시스템과 보안장비에서 발생한 로그·보안 이벤트를 중앙에서 수집하고 서로 연관 지어 분석하여 위협을 탐지·추적하는 통합 보안관제 체계이다.
TMS는 네트워크 위협의 탐지·분석·대응을 통합 관리하고, SOAR는 보안 도구와 대응 절차를 연계·자동화하며, NGFW는 애플리케이션 식별과 침입방지 등 고급 통제 기능을 결합한 방화벽이다.

선지별 해설

① X — TMS는 여러 보안 기능을 연계하여 네트워크 위협을 통합적으로 탐지·분석·대응하는 체계이다. 틀린 표현은 'TMS'이며, 보기처럼 방대한 로그·이벤트의 상관분석과 포렌식에 초점을 둔 체계는 SIEM이다.
② O — SIEM은 다양한 출처의 로그와 이벤트를 수집·분석하고 상관관계를 찾아 지능형 위협을 조기에 탐지하며, 사고 이후 추적과 포렌식에 필요한 정보를 제공한다. 보기의 핵심어와 정확히 일치한다.
③ X — SOAR는 여러 보안 솔루션을 오케스트레이션하고 반복적인 분석·대응 절차를 플레이북으로 자동화하는 기술이다. 틀린 표현은 'SOAR'이며, 보기의 로그 상관분석·포렌식 중심 체계는 SIEM이다.
④ X — NGFW는 기존 방화벽 기능에 애플리케이션 식별·제어, 사용자 기반 정책, 침입방지 등의 기능을 결합한 차세대 방화벽이다. 틀린 표현은 'NGFW'이며, 보기의 중앙 로그 수집·상관분석·사후 추적 기능은 SIEM에 해당한다.

NoteBase

오답 포인트

‘위협 관리’, ‘자동 대응’, ‘차세대 방화벽’도 모두 보안관제와 관련되어 혼동하기 쉽다. 그러나 보기의 결정적 표현은 ‘방대한 정보’, ‘상관분석’, ‘포렌식’, ‘사후 추적’이며, 이는 SIEM을 가리킨다.

다시 나오면 이렇게 판단

로그·이벤트의 중앙 수집과 상관분석이 중심이면 SIEM, 여러 도구와 대응 절차의 자동화가 중심이면 SOAR, 네트워크 위협의 통합 탐지·대응이면 TMS, 방화벽의 애플리케이션·사용자 단위 통제가 중심이면 NGFW로 구분한다.

암기 포인트

SIEM은 로그를 모아 상관분석하고 추적하며, SOAR는 대응 절차를 연계해 자동화한다.

NoteBase

문 11. 다음 <보기>에서 포렌식의 원칙에 관련한 서술로 가장 옳게 짝지어진 것은?

<보기>
㉠ 재현의 원칙
㉡ 무결성의 원칙
㉢ 정당성의 원칙
㉣ 연계 보관성의 원칙
ⓐ 적법한 절차를 거쳐 획득한 것만이 증거력을 가짐.
ⓑ 획득 후 이송/분석/보관/법정제출과정이 명확하고 추적 가능해야 함.
ⓒ 같은 환경에서는 같은 결과가 얻어져야 함.
㉣ 수집정보는 연계보관성 및 단계과정에서의 위조, 변조가 일어나지 않아야 함.

① ㉠-ⓒ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓑ
② ㉠-ⓐ, ㉡-ⓑ, ㉢-ⓓ, ㉣-ⓒ
③ ㉠-ⓒ, ㉡-ⓓ, ㉢-ⓑ, ㉣-ⓐ
④ ㉠-ⓐ, ㉡-ⓓ, ㉢-ⓑ, ㉣-ⓒ

정답 1번

출제 포인트

디지털 포렌식 증거가 증거력을 가지기 위한 재현성·무결성·정당성·연계 보관성의 의미를 구별하는 문제이다.

핵심 개념

재현의 원칙은 같은 조건과 분석 절차에서 같은 결과가 나와야 한다는 원칙이다. 키워드는 '같은 환경·같은 결과'이다.
무결성의 원칙은 수집한 정보가 위조·변조되지 않고 원래 상태를 유지해야 한다는 원칙이다. 키워드는 '위조·변조 방지'이다.
정당성의 원칙은 증거를 적법한 절차와 정당한 방법으로 획득해야 한다는 원칙이다. 키워드는 '적법한 절차'이다.
연계 보관성의 원칙은 증거의 획득부터 이송·분석·보관·법정 제출까지 취급 과정과 담당자가 명확하고 추적 가능해야 한다는 원칙이다. 키워드는 '전 과정 추적'이다.
따라서 ㉠-ⓒ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓑ로 연결된다.

NoteBase

선지별 해설

① O — 재현은 같은 환경에서 같은 결과를 얻는 ⓒ, 무결성은 위조·변조를 막는 ⓓ, 정당성은 적법하게 획득하는 ⓐ, 연계 보관성은 취급 전 과정을 추적하는 ⓑ와 각각 연결되므로 모두 옳다.
② X — ㉠-ⓐ, ㉡-ⓑ, ㉢-ⓓ, ㉣-ⓒ라는 연결이 모두 잘못되었다. 올바르게는 ㉠-ⓒ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓑ이다.
③ X — ㉠-ⓒ와 ㉡-ⓓ는 맞지만, ㉢-ⓑ와 ㉣-ⓐ가 서로 뒤바뀌었다. 올바르게는 정당성 ㉢이 적법한 획득인 ⓐ, 연계 보관성 ㉣이 전 과정의 추적 가능성인 ⓑ와 연결된다.
④ X — ㉡-ⓓ만 맞고 ㉠-ⓐ, ㉢-ⓑ, ㉣-ⓒ는 잘못되었다. 올바르게는 재현 ㉠-ⓒ, 정당성 ㉢-ⓐ, 연계 보관성 ㉣-ⓑ이다.

오답 포인트

무결성과 연계 보관성은 모두 증거의 신뢰성과 관련되어 혼동하기 쉽다. ‘내용이 변하지 않았는가’는 무결성이고, ‘누가 언제 어떤 단계로 취급했는가를 추적할 수 있는가’는 연계 보관성이다.

다시 나오면 이렇게 판단

같은 결과는 재현, 위조·변조 방지는 무결성, 적법한 획득은 정당성, 획득부터 제출까지의 추적은 연계 보관성으로 판단한다.

암기 포인트

재현=같은 결과, 무결성=변조 없음, 정당성=적법 획득, 연계 보관성=전 과정 추적이다.

NoteBase

문 12. 다음 <보기>에서 공격형태와 이에 관련한 설명으로 가장 옳게 짝지어진 것은?

<보기>
㉠ Ping of Death
㉡ Heartbleed
㉢ Bonk, Boink
㉣ GET Flooding
ⓐ OpenSSL 패키지 최신버전 업데이트로 보안.
ⓑ 분할된 패킷을 탐지, 공격 여부를 의심, 제거.
ⓒ 응용수준의 대응방법으로 방어.
ⓓ TCP 패킷의 순서번호를 조작하는 공격방법.

① ㉠-ⓑ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓒ
② ㉠-ⓒ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓑ
③ ㉠-ⓑ, ㉡-ⓐ, ㉢-ⓓ, ㉣-ⓒ
④ ㉠-ⓑ, ㉡-ⓓ, ㉢-ⓐ, ㉣-ⓒ

정답 3번

출제 포인트

대표적인 서비스 거부 공격과 취약점 공격의 작동 특징 및 대응 방법을 정확히 연결하는 문제이다.

핵심 개념

Ping of Death는 비정상적으로 큰 IP 패킷이 재조립되도록 조각난 패킷을 보내 시스템 장애를 유발하는 공격이다. 따라서 비정상적인 분할 패킷을 탐지하고 제거하는 대응과 연결된다.
Heartbleed는 OpenSSL의 Heartbeat 확장 기능 취약점을 악용해 메모리 내용을 유출하는 공격이다. 취약점이 수정된 OpenSSL 버전으로 업데이트하는 것이 핵심 대응이다.
Bonk·Boink는 TCP 패킷의 순서번호를 비정상적으로 조작하여 시스템 장애를 유발하는 공격이다.
GET Flooding은 다량의 HTTP GET 요청으로 웹 서버의 자원을 고갈시키는 응용 계층 공격이다. 따라서 웹 응용 수준에서 비정상 요청을 식별·제한하는 방식으로 방어한다.
올바른 연결은 ㉠-ⓑ, ㉡-ⓐ, ㉢-ⓓ, ㉣-ⓒ이다.

NoteBase

선지별 해설

① X — ㉠ Ping of Death와 ⓑ의 연결은 맞지만, ㉡ Heartbleed를 ⓓ와 연결하고 ㉢ Bonk·Boink를 ⓐ와 연결한 부분이 틀리다. 올바르게는 ㉡-ⓐ, ㉢-ⓓ이므로 전체 연결은 ㉠-ⓑ, ㉡-ⓐ, ㉢-ⓓ, ㉣-ⓒ이다.
② X — ㉠ Ping of Death는 응용 수준의 GET Flooding 대응인 ⓒ가 아니라 분할 패킷 탐지·제거인 ⓑ와 연결된다. 또한 ㉡ Heartbleed는 ⓓ가 아니라 OpenSSL 업데이트인 ⓐ, ㉢ Bonk·Boink는 ⓐ가 아니라 TCP 순서번호 조작인 ⓓ, ㉣ GET Flooding은 ⓑ가 아니라 응용 수준 대응인 ⓒ와 연결된다.
③ O — Ping of Death는 분할 패킷 탐지·제거(ⓑ), Heartbleed는 OpenSSL 최신 버전 업데이트(ⓐ), Bonk·Boink는 TCP 순서번호 조작(ⓓ), GET Flooding은 응용 수준 대응(ⓒ)과 각각 정확히 연결된다.
④ X — ①과 동일한 연결로, ㉡ Heartbleed와 ㉢ Bonk·Boink의 설명을 서로 잘못 배치하였다. 올바르게는 ㉡-ⓐ, ㉢-ⓓ이므로 전체 연결은 ㉠-ⓑ, ㉡-ⓐ, ㉢-ⓓ, ㉣-ⓒ이다.

오답 포인트

ⓐ의 ‘OpenSSL’은 Heartbleed를 곧바로 가리키고, ⓒ의 ‘응용수준’은 HTTP GET 요청을 이용하는 GET Flooding과 연결된다. 이 두 연결을 먼저 확정하지 않으면 Heartbleed와 Bonk·Boink의 설명을 뒤바꾸기 쉽다. 또한 ①과 ④는 원문상 같은 내용이므로 둘 다 동일한 이유로 오답이다.

다시 나오면 이렇게 판단

제품명이나 프로토콜 계층을 단서로 먼저 고정한다. OpenSSL은 Heartbleed, HTTP GET은 응용 계층의 GET Flooding, IP 분할·재조립은 Ping of Death, TCP 순서번호 조작은 Bonk·Boink에 대응한다.

암기 포인트

Ping of Death=IP 분할, Heartbleed=OpenSSL, Bonk·Boink=TCP 순서번호, GET Flooding=HTTP 응용 계층이다.

NoteBase

문 13. ARP(Address Resolution Protocol)에 관한 설명 중 가장 옳지 않은 것은?

① ARP 패킷은 데이터링크 프레임에 캡슐화된다.

② 호스트의 ARP 테이블을 정적으로 유지하면 ARP 스푸핑(Spoofing) 공격을 막을 수 있다.

③ ARP는 MAC 주소에 대응되는 IP 주소를 구할 때 사용되는 프로토콜이다.

④ ARP 패킷에는 발신자와 해당 수신자의 물리 주소와 논리주소가 포함된다.

정답 3번

출제 포인트

ARP의 주소 변환 방향과 ARP 패킷의 전달 방식·구성 필드·보안 대책을 구별하는 문제이다.

핵심 개념

ARP는 같은 네트워크에서 통신할 대상의 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 주소 변환 방향은 'IP 주소 → MAC 주소'이다. 반대 방향인 'MAC 주소 → IP 주소'는 ARP의 기능이 아니며, 전통적으로 RARP가 담당한다.

선지별 해설

① O

ARP 메시지는 네트워크 계층의 IP 패킷 안에 들어가는 것이 아니라 이더넷과 같은 데이터링크 계층 프레임의 페이로드로 직접 캡슐화되어 전달된다.

② O

ARP 테이블의 IP 주소와 MAC 주소 대응 관계를 정적으로 고정하면 위조된 ARP 응답이 그 대응 관계를 바꾸는 것을 차단할 수 있으므로 ARP 스푸핑 방지 방법이 된다.

③ X

틀린 표현은 'MAC 주소에 대응되는 IP 주소'이다. 올바르게는 ARP는 'IP 주소에 대응되는 MAC 주소'를 구할 때 사용하는 프로토콜이다. MAC 주소로 IP 주소를 구하는 반대 방향은 전통적으로 RARP의 기능이다.

④ O

ARP 패킷에는 송신자의 물리 주소와 논리 주소, 대상의 물리 주소와 논리 주소를 담는 필드가 있다. ARP 요청에서는 대상의 물리 주소를 아직 모르므로 해당 필드가 미확정 값으로 채워지지만 필드 자체는 포함된다.

NoteBase

오답 포인트

③은 ARP의 주소 변환 방향을 정확히 뒤집어 제시한 함정이다. '주소를 알아내는 출발점이 IP인지 MAC인지'를 확인해야 한다.

다시 나오면 이렇게 판단

ARP가 나오면 먼저 '알고 있는 IP 주소로 목적지 MAC 주소를 찾는다'는 방향을 확정한 뒤, 데이터링크 프레임에 직접 실린다는 점과 송신자·대상의 물리 주소 및 논리 주소 필드를 함께 확인한다.

암기 포인트

ARP는 IP → MAC, RARP는 MAC → IP이다.

NoteBase

문 14. 다음 <보기>의 설명에 해당하는 라우팅 프로토콜은 무엇인가?

<보기>
◯ 모든 라우터가 동일한 네트워크 토폴로지 데이터베이스를 기반으로 경로를 계산한다.
◯ 거리 벡터가 아닌 링크 상태를 활용하는 자율 시스템 도메인 내의 라우팅 프로토콜이다.

① IGRP(Interior Gateway Routing Protocol)
② RIP(Routing Information Protocol)
③ BGP(Border Gateway Protocol)
④ OSPF(Open Shortest Path First)

정답 4번

출제 포인트

이 문제는 라우팅 프로토콜을 경로 정보 표현 방식과 적용 범위로 구별하는 문제이다. 동일 영역의 라우터들이 링크 상태 데이터베이스를 공유하고 각자 최단 경로를 계산한다는 설명은 OSPF에 해당한다.

핵심 개념

OSPF는 자율 시스템 내부에서 사용하는 링크 상태 라우팅 프로토콜이다. 각 라우터는 링크 상태 정보를 교환하여 같은 영역의 링크 상태 데이터베이스를 구성하고, SPF 알고리즘으로 최단 경로를 계산한다.
IGRP와 RIP는 거리 벡터 계열이고, BGP는 자율 시스템 사이의 경로를 교환하는 경로 벡터 프로토콜이다.

선지별 해설

① X — IGRP는 거리 벡터 방식의 내부 게이트웨이 라우팅 프로토콜이므로 링크 상태 데이터베이스를 기반으로 경로를 계산한다는 설명과 맞지 않는다. 틀린 대응은 'IGRP'이며, 올바르게는 'OSPF'이다.
② X — RIP는 홉 수를 메트릭으로 사용하는 거리 벡터 방식이므로 보기의 '거리 벡터가 아닌 링크 상태'라는 조건과 반대이다. 틀린 대응은 'RIP'이며, 올바르게는 'OSPF'이다.
③ X — BGP는 주로 서로 다른 자율 시스템 사이에서 경로 정보를 교환하는 경로 벡터 프로토콜이므로 자율 시스템 도메인 내부의 링크 상태 프로토콜이라는 설명과 맞지 않는다. 틀린 대응은 'BGP'이며, 올바르게는 'OSPF'이다.
④ O — OSPF는 자율 시스템 내부에서 링크 상태 정보를 교환하고, 동일 영역의 라우터들이 링크 상태 데이터베이스를 바탕으로 최단 경로를 계산하는 프로토콜이다.

오답 포인트

'내부 게이트웨이 프로토콜'이라는 공통점만 보고 IGRP나 RIP를 고르는 것이 함정이다. 결정적인 표현은 '거리 벡터가 아닌 링크 상태'와 '네트워크 토폴로지 데이터베이스'이며, 이 두 표현은 OSPF를 가리킨다.

NoteBase

다시 나오면 이렇게 판단

토폴로지 데이터베이스·링크 상태·SPF가 제시되면 OSPF, 홉 수·거리 벡터가 제시되면 RIP, 자율 시스템 간 경로 교환·경로 벡터가 제시되면 BGP로 판단한다.

암기 포인트

OSPF는 링크 상태와 SPF, RIP는 거리 벡터와 홉 수, BGP는 자율 시스템 간 경로 벡터이다.

NoteBase

문 15. 다음 <보기> 설명에 해당하는 용어를 바르게 나열한 것은?

<보기>
㉠ 블루투스 공격장치의 검색 활동을 뜻한다.
㉡ 블루투스의 취약점을 이용하여 기기의 정보에 접근하는 공격이다.
㉢ 블루투스 장비간의 취약한 연결 관리를 악용한 공격이다.
㉣ 블루투스를 이용해 스팸처럼 명함을 익명으로 퍼트리는 것이다.

① ㉠: 블루재킹, ㉡: 블루스나핑, ㉢: 블루프린팅, ㉣: 블루버깅
② ㉠: 블루프린팅, ㉡: 블루버깅, ㉢: 블루스나핑, ㉣: 블루재킹
③ ㉠: 블루프린팅, ㉡: 블루스나핑, ㉢: 블루버깅, ㉣: 블루재킹
④ ㉠: 블루재킹, ㉡: 블루버깅, ㉢: 블루프린팅, ㉣: 블루스나핑

정답 3번

출제 포인트

블루투스 공격 유형을 공격 행위의 목적과 방식에 따라 구별하는 문제이다.

핵심 개념

블루프린팅: 주변 블루투스 장치를 검색하고 장치 정보를 수집하는 활동이다. 키워드는 장치 검색·정보 수집이다.
블루스나핑: 블루투스의 취약점을 이용해 주소록·메시지·파일 등 기기 정보에 무단 접근하는 공격이다. 키워드는 정보 탈취이다.
블루버깅: 취약한 블루투스 연결 관리를 악용해 대상 기기를 제어하거나 기능을 무단 사용하는 공격이다. 키워드는 기기 제어이다.
블루재킹: 블루투스로 익명 메시지나 전자 명함을 원치 않는 상대에게 보내는 행위이다. 키워드는 스팸성 전송이다.

NoteBase

선지별 해설

① X — ㉠의 장치 검색은 블루재킹이 아니라 블루프린팅이고, ㉢의 연결 관리 악용은 블루프린팅이 아니라 블루버깅이며, ㉣의 익명 명함 전송은 블루버깅이 아니라 블루재킹이다. ㉡의 블루스나핑만 맞다. 올바른 배열은 ㉠ 블루프린팅, ㉡ 블루스나핑, ㉢ 블루버깅, ㉣ 블루재킹이다.
② X — ㉡의 기기 정보 접근은 블루버깅이 아니라 블루스나핑이고, ㉢의 연결 관리 악용은 블루스나핑이 아니라 블루버깅이다. ㉠의 블루프린팅과 ㉣의 블루재킹은 맞다. 올바른 배열은 ㉠ 블루프린팅, ㉡ 블루스나핑, ㉢ 블루버깅, ㉣ 블루재킹이다.
③ O — 장치 검색은 블루프린팅, 기기 정보 무단 접근은 블루스나핑, 취약한 연결 관리 악용은 블루버깅, 익명 명함 전송은 블루재킹에 각각 해당한다.
④ X — ㉠의 장치 검색은 블루재킹이 아니라 블루프린팅이고, ㉡의 정보 접근은 블루버깅이 아니라 블루스나핑이며, ㉢의 연결 관리 악용은 블루프린팅이 아니라 블루버깅이고, ㉣의 익명 명함 전송은 블루스나핑이 아니라 블루재킹이다. 올바른 배열은 ㉠ 블루프린팅, ㉡ 블루스나핑, ㉢ 블루버깅, ㉣ 블루재킹이다.

오답 포인트

블루프린팅과 블루재킹을 모두 주변 장치와 관련된 행위로 묶거나, 블루스나핑과 블루버깅을 모두 침입 공격으로만 기억하면 배열을 바꾸기 쉽다. 이 문제에서는 검색, 정보 접근, 연결 악용·제어, 명함 전송이라는 행위의 목적을 구분해야 한다.

다시 나오면 이렇게 판단

검색·장치 식별이면 블루프린팅, 정보 탈취이면 블루스나핑, 기기 제어이면 블루버깅, 메시지·명함 전송이면 블루재킹으로 판단한다.

암기 포인트

프린팅은 검색, 스나핑은 정보 탈취, 버깅은 제어, 재킹은 메시지 전송이다.

NoteBase

문 16. 다음 중 라우터가 송신 측 노드에 적합하지 않은 경로로 설정되어 있을 경우 해당 노드에 대한 최적화된 경로를 다시 지정해주는 ICMP(Internet Control Message Protocol) 메시지로 가장 옳은 것은?

① Time Exceed

② Redirection

③ Destination Unreachable

④ Source Quench

정답 2번

출제 포인트

이 문제는 라우터가 호스트에게 더 적절한 다음 홉 경로를 알려 주는 ICMP Redirect 메시지를 다른 ICMP 오류·제어 메시지와 구별하는 문제이다.

핵심 개념

ICMP Redirect는 호스트가 선택한 다음 홉보다 더 적절한 라우터가 있을 때, 현재 라우터가 그 호스트에게 더 나은 경로를 알려 주는 메시지이다. 선지의 Redirection은 이 Redirect 기능을 가리킨다.
Time Exceeded는 패킷의 TTL 만료 등을, Destination Unreachable은 목적지 도달 불가를, Source Quench는 송신 속도 억제를 요청하던 혼잡 제어를 나타낸다.

선지별 해설

① X — Time Exceeded는 패킷의 TTL이 0이 되었거나 조각 재조립 시간이 초과되었을 때 시간 초과를 알리는 메시지이다. 틀린 표현은 '최적화된 경로를 다시 지정'하는 기능으로 본 부분이며, 올바르게는 전송 시간 한계 초과를 통지하는 메시지이다.
② O — Redirection은 ICMP Redirect를 뜻한다. 라우터가 송신 호스트에게 동일 목적지에 대해 더 적절한 다음 홉 라우터를 알려 주므로 문제의 설명과 일치한다.
③ X — Destination Unreachable은 네트워크·호스트·포트 등에 도달할 수 없어 패킷을 전달하지 못했음을 알리는 메시지이다. 틀린 표현은 이를 경로 최적화 메시지로 본 부분이며, 올바르게는 목적지 도달 불가를 통지하는 메시지이다.
④ X — Source Quench는 혼잡 상황에서 송신 측에 전송량을 줄이도록 요청하던 메시지이다. 틀린 표현은 이를 더 나은 경로를 지정하는 메시지로 본 부분이며, 올바르게는 송신 속도 억제를 요청하던 메시지이다.

오답 포인트

라우팅 과정에서 문제가 생겼다는 공통점만 보고 Destination Unreachable을 고르기 쉽다. 그러나 문제의 핵심 표현은 '최적화된 경로를 다시 지정'이며, 이는 전달 실패 통지가 아니라 더 나은 다음 홉을 알려 주는 Redirect에 해당한다.

NoteBase

다시 나오면 이렇게 판단

‘더 좋은 라우터·다음 홉·경로 변경 안내’가 나오면 Redirect, ‘TTL 만료’는 Time Exceeded, ‘전달 불가’는 Destination Unreachable, ‘송신량 감소 요청’은 Source Quench로 구별한다.

암기 포인트

Redirect는 경로 수정, Time Exceeded는 시간 초과, Destination Unreachable은 도달 불가, Source Quench는 속도 억제이다.

NoteBase

문 17. SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① TCP/IP 프로토콜을 사용하는 인터넷에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

② 에이전트는 Trap 메시지를 관리자에 보냄으로써 비정상적인 상황을 경고할 수 있다.

③ SMI는 객체의 이름을 붙이고 유형을 정의하며, 부호화하는 등의 일반적인 규칙을 정의한다.

④ SMI는 공통된 정보 표현방식을 규정해서 장비간 통신이 이루어질 수 있도록 하며 객체의 유형과 연결에 관여한다.

정답 4번

출제 포인트

SNMP의 통신 방식과 포트 번호, Trap의 기능, SMI가 정하는 관리 정보의 표현 규칙을 구분하는 문제이다.

핵심 개념

SNMP는 TCP/IP 네트워크의 장치를 감시하고 관리하기 위한 응용 계층 프로토콜이다. 관리자는 에이전트의 관리 정보를 조회·변경하고, 에이전트는 중요한 사건을 Trap으로 알릴 수 있다.
SMI(Structure of Management Information)는 관리 객체의 이름, 자료형과 표현 형식, 부호화 규칙을 정한다. MIB는 이러한 규칙에 따라 정의된 관리 객체들의 집합이며, 관리자와 에이전트 사이의 실제 메시지 교환은 SNMP가 담당한다.

선지별 해설

① O — SNMP는 TCP/IP 기반 네트워크 장치를 관리하는 프로토콜이며, 일반적으로 UDP 161번은 요청·응답에, UDP 162번은 Trap·Inform 알림 수신에 사용된다.
② O — 에이전트는 장애나 상태 변화 같은 사건이 발생하면 관리자의 요청을 기다리지 않고 Trap 메시지를 보내 비정상 상황을 알릴 수 있다.
③ O — SMI는 관리 객체에 이름을 부여하는 방식, 객체의 자료형과 표현 형식, 전송 시 부호화에 관한 공통 규칙을 정의한다.
④ X — 틀린 부분은 SMI가 '장비 간 통신이 이루어지도록 하며 객체의 유형과 연결에 관여한다'고 한 부분이다. SMI의 핵심 역할은 관리 객체의 이름·자료형·표현 형식·부호화 규칙을 정의하는 것이며, 관리자와 에이전트 사이의 메시지 교환은 SNMP가 담당한다. 올바르게는 'SMI는 관리 객체의 이름, 자료형과 표현 형식, 부호화에 관한 일반 규칙을 정의한다'라고 해야 한다.

NoteBase

오답 포인트

④는 '공통된 정보 표현방식'이라는 그럴듯한 표현 뒤에 SMI의 역할이 아닌 장비 간 통신과 객체의 연결을 섞어 놓았다. ③처럼 이름·자료형·부호화 규칙을 제시하면 SMI이고, 실제 요청·응답·알림 메시지의 교환을 말하면 SNMP이다.

다시 나오면 이렇게 판단

포트와 메시지 교환은 SNMP, 관리 객체를 기술하는 문법과 규칙은 SMI, 그 규칙에 따라 정의된 관리 객체의 집합은 MIB로 구분한다.

암기 포인트

SNMP는 통신, SMI는 표현 규칙, MIB는 관리 객체 모음이다. UDP 161은 조회·응답, UDP 162는 Trap·Inform이다.

NoteBase

문 18. 다음 <보기>는 보안을 위해 필요로 하는 기능 요구 사항에 대하여 제시한 것이다. 괄호 안 내용으로 가장 옳은 것은?

<보기>
“우리 원에서 대외 홈페이지를 열기로 했습니다. 그런데 민원인이 인터넷으로 접속할 수 있어야 하니 보안장비를 구입해야 합니다. 사용자 게시판도 구축해야 하고, 민원 게시물도 업로드 할 수 있도록 해야 하니 필요한 장비는 ( ) 입니다.”

① 네트워크 방화벽
② 게이트웨이
③ 웹 방화벽
④ 침입탐지 시스템

정답 3번

출제 포인트

인터넷에 공개되는 홈페이지의 게시판·파일 업로드 기능을 보호할 때 웹 애플리케이션 계층의 공격을 점검하고 차단하는 장비를 구별하는 문제이다.

핵심 개념

웹 방화벽(WAF)은 웹 서버 앞에서 HTTP·HTTPS 요청 내용을 검사하여 SQL 삽입, 크로스 사이트 스크립팅(XSS), 악성 파일 업로드 등 웹 애플리케이션 대상 공격을 탐지·차단하는 보안장비이다.
네트워크 방화벽은 주로 출발지·목적지 IP 주소, 포트, 프로토콜 등 네트워크 통신 정책에 따라 트래픽을 허용하거나 차단한다. 침입탐지 시스템(IDS)은 공격 징후를 탐지하고 경보하는 것이 주된 기능이며, 게이트웨이는 서로 다른 네트워크나 프로토콜 사이의 통신을 중계한다.

NoteBase

선지별 해설

① X — 네트워크 방화벽은 주로 IP 주소·포트·프로토콜을 기준으로 접근을 통제하므로, 게시판 입력값이나 업로드 요청처럼 웹 애플리케이션의 내용을 보호한다는 요구에 가장 직접적으로 대응하지 않는다. 틀린 부분은 '네트워크 방화벽'이며, 이 요구에 가장 알맞은 장비는 웹 방화벽이다.
② X — 게이트웨이는 서로 다른 네트워크 또는 프로토콜 사이의 통신을 연결·변환하는 장비이지, 홈페이지 게시판과 파일 업로드 기능을 웹 공격으로부터 보호하는 전용 보안장비가 아니다. 틀린 부분은 '게이트웨이'이며, 올바른 장비는 웹 방화벽이다.
③ O — 웹 방화벽은 홈페이지로 들어오는 HTTP·HTTPS 요청을 애플리케이션 계층에서 검사하므로, 사용자 게시판과 파일 업로드 기능을 악용하는 웹 공격에 대응하기에 가장 적합하다.
④ X — 침입탐지 시스템은 의심스러운 행위를 탐지하여 경보하는 장비로, 웹 요청을 앞단에서 검사하고 차단하는 웹 방화벽과 주된 역할이 다르다. 틀린 부분은 '침입탐지 시스템'이며, 게시판·업로드 기능을 직접 보호하는 장비로는 웹 방화벽이 적합하다.

오답 포인트

'인터넷에 공개하므로 방화벽이 필요하다'는 표현만 보고 ①을 고르기 쉽다. 그러나 게시판과 파일 업로드라는 구체적 기능은 웹 요청의 내용을 악용하는 공격 가능성을 뜻하므로, 일반적인 네트워크 접근 통제보다 웹 애플리케이션 보호가 핵심이다.

다시 나오면 이렇게 판단

IP·포트 기반의 통신 허용·차단이면 네트워크 방화벽, HTTP·HTTPS 요청과 웹 입력값 보호이면 웹 방화벽, 공격 징후의 탐지·경보이면 침입탐지 시스템, 이기종 네트워크의 연결·변환이면 게이트웨이로 판단한다.

암기 포인트

게시판·로그인·파일 업로드처럼 웹 기능을 보호하는 장비는 웹 방화벽(WAF)이다.

NoteBase

문 19. 203.230.15.0과 같은 IPv4의 C클래스 네트워크를 30개의 서브넷으로 나누고, 각각의 서브넷에는 5개의 호스트를 연결하려고 한다. 30개의 서브넷에서 사용되는 서브넷 마스크는?

① 255.255.255.192

② 255.255.255.248

③ 255.255.255.240

④ 255.255.255.224

정답 2번

출제 포인트

C클래스의 기본 프리픽스 /24에서 서브넷 수와 서브넷당 사용 가능한 호스트 수를 모두 만족하도록 네트워크 비트와 호스트 비트를 배분하는 문제이다.

조건 정리

주어진 네트워크: 203.230.15.0/24
필요한 서브넷 수: 30개
서브넷마다 필요한 호스트 수: 5개
호스트 주소에서는 네트워크 주소와 브로드캐스트 주소를 사용할 수 없으므로 2개를 제외한다.

사용할 공식

서브넷 비트를 s, 호스트 비트를 h라고 하면 필요한 조건은 $2^s \geq 30$, $2^h - 2 \geq 5$이다.
기본 호스트부가 8비트인 /24 네트워크를 서브넷팅하므로 $s + h = 8$이다. 이 식을 쓰면 필요한 서브넷 수와 각 서브넷의 사용 가능한 호스트 수를 동시에 확인할 수 있다.

계산 과정

1. $2^4 = 16 < 30$, 2^5=32≥30이므로 서브넷 비트는 5비트가 필요하다.
2. 호스트 비트는 $8 - 5 = 3$비트가 남고, 각 서브넷에서 사용할 수 있는 호스트 수는 $2^3 - 2 = 6$개이므로 5개를 연결할 수 있다.
3. 새 프리픽스 길이는 $24 + 5 = 29$, 즉 /29이다. 마지막 옥텟의 앞 5비트가 1이므로 이진수 11111000은 십진수 248이다. 따라서 서브넷 마스크는 255.255.255.248이다.

NoteBase

선지 판단

① X — 255.255.255.192는 /26으로, /24에서 2비트만 빌려 4개 서브넷만 만든다. 30개 서브넷을 만들 수 없으며, 올바르게는 /29인 255.255.255.248이다.
② O — 255.255.255.248은 /29이다. 서브넷 비트 5개로 32개 서브넷을 만들고, 남은 호스트 비트 3개로 각 서브넷에서 6개의 호스트 주소를 사용할 수 있으므로 두 조건을 모두 만족한다.
③ X — 255.255.255.240은 /28로, /24에서 4비트를 빌려 16개 서브넷만 만든다. 호스트 수는 충분하지만 서브넷 수가 부족하며, 올바르게는 255.255.255.248이다.
④ X — 255.255.255.224는 /27로, /24에서 3비트를 빌려 8개 서브넷만 만든다. 30은 이 마스크에서 서브넷 수가 아니라 각 서브넷의 사용 가능한 호스트 수 $2^5 - 2 = 30$이며, 올바르게는 255.255.255.248이다.

오답 포인트

④의 /27은 사용 가능한 호스트가 30개라는 점을 이용한 함정이다. 문제에서 요구하는 것은 서브넷 30개와 서브넷당 호스트 5개이므로 두 수의 자리를 바꾸면 안 된다. 또한 호스트 수를 셀 때는 네트워크 주소와 브로드캐스트 주소를 제외한다.

다시 나오면 이렇게 판단

먼저 2^s로 필요한 서브넷 비트를 정하고, 남은 호스트 비트에 대해 $2^h - 2$가 필요한 호스트 수 이상인지 검산한다. 마지막으로 새 프리픽스를 점 표기 서브넷 마스크로 변환한다.

암기 포인트

/29는 블록 크기 8, 주소 8개, 사용 가능한 호스트 6개이다. 255에서 블록 크기 8을 빼면 마지막 옥텟은 248이 된다.

NoteBase

문 20. 스위치의 MAC Address Table 버퍼를 오버플로우 시켜서 스위치가 허브처럼 동작하게 강제적으로 만드는 기법은?

① 스위치 Jamming
② ICMP Redirect
③ ARP Spoofing
④ ARP Redirect

정답 1번

출제 포인트

스위치의 MAC 주소 테이블을 고갈시켜 프레임을 여러 포트로 플러딩하게 만드는 공격 기법을 구별하는 문제이다.

핵심 개념

스위치 재밍(Switch Jamming)은 대량의 위조 출발지 MAC 주소를 스위치에 학습시켜 MAC 주소 테이블을 넘치게 하는 공격이며, MAC 플러딩 또는 CAM 테이블 오버플로 공격이라고도 한다. 테이블이 정상적으로 목적지 MAC 주소와 포트의 대응 관계를 유지하지 못하면 스위치는 목적지 포트를 특정할 수 없는 프레임을 여러 포트로 플러딩하므로 허브처럼 동작하는 효과가 나타난다.
ICMP Redirect는 라우터가 호스트에게 더 적절한 다음 홉을 알려 주는 ICMP 메시지이고, ARP 스푸핑은 위조 ARP 메시지로 IP 주소와 MAC 주소의 대응 관계를 속이는 공격이다.

선지별 해설

① O — 스위치 재밍은 다수의 위조 MAC 주소를 학습시켜 MAC 주소 테이블을 오버플로시키고, 스위치가 프레임을 플러딩하도록 만드는 기법이다.
② X — 틀린 표현은 'ICMP Redirect'이다. ICMP Redirect는 더 적절한 경로 또는 게이트웨이를 알리는 메시지이며, MAC 주소 테이블 오버플로 공격은 '스위치 재밍(MAC 플러딩)'이다.
③ X — 틀린 표현은 'ARP Spoofing'이다. ARP 스푸핑은 위조된 ARP 정보를 이용해 IP 주소와 MAC 주소의 대응 관계를 변조하는 공격이며, MAC 주소 테이블을 넘치게 하는 기법은 '스위치 재밍'이다.
④ X — 틀린 표현은 'ARP Redirect'이다. 이 문항에서 설명한 공격의 정확한 명칭은 '스위치 재밍(MAC 플러딩 또는 CAM 테이블 오버플로)'이며, ARP를 속여 통신 경로를 공격자 쪽으로 유도하는 행위는 일반적으로 ARP 스푸핑으로 구분한다.

오답 포인트

'트래픽을 공격자 쪽으로 유도한다'는 결과만 보고 ICMP Redirect나 ARP 스푸핑을 고르기 쉽다. 그러나 문제의 결정적 표현은 'MAC Address Table 버퍼 오버플로'와 '허브처럼 동작'이며, 이는 스위치 재밍의 특징이다.

NoteBase

다시 나오면 이렇게 판단

MAC 주소 테이블·CAM 테이블의 용량 고갈과 프레임 플러딩이 함께 제시되면 스위치 재밍을 선택한다. IP-MAC 대응 관계 변조는 ARP 스푸핑, 더 나은 게이트웨이 통지는 ICMP Redirect로 구별한다.

암기 포인트

MAC 테이블을 채워 허브처럼 만들면 스위치 재밍, IP-MAC 대응을 속이면 ARP 스푸핑이다.

NoteBase