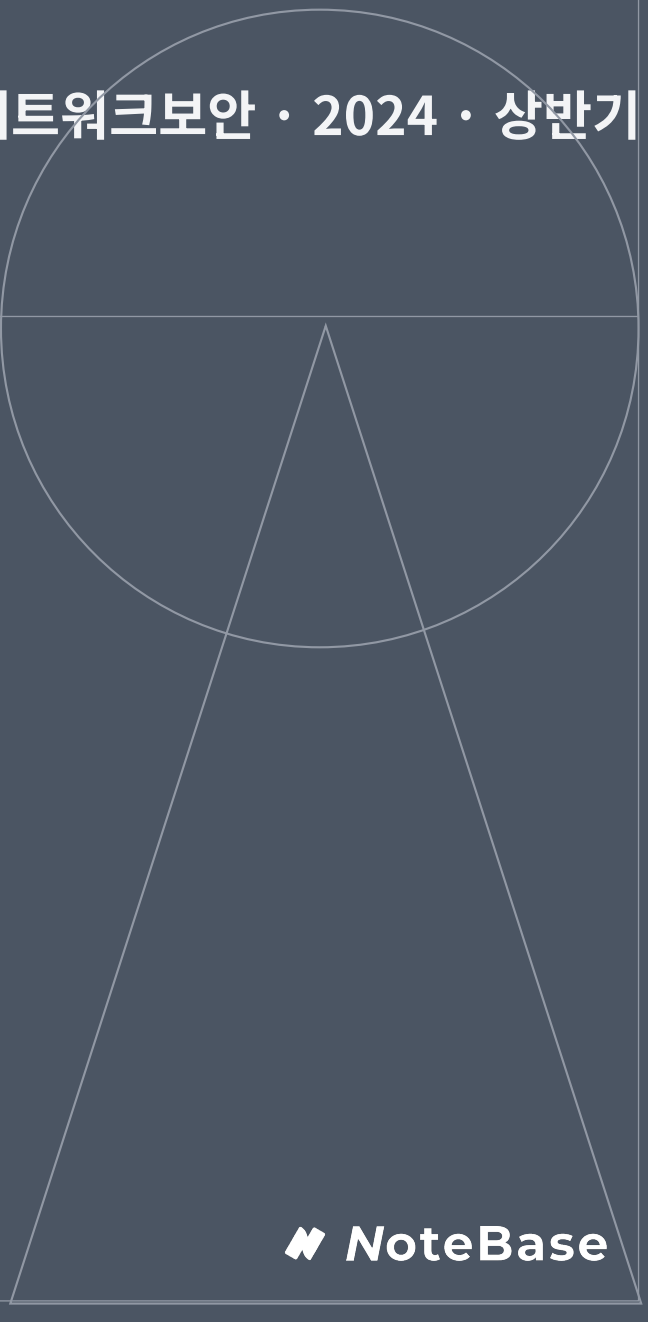
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2024 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2024 · 상반기

공무원/해경/일반직 9급 · 네트워크보안 · 2024 · 상반기

문 1. 네트워크 스위치는 기능에 따라 OSI 계층 모델에 따르는 수준이 다양하다. 다음 중 각 스위치의 최고 수준에서 제공할 수 있는 기능에 대한 설명으로 가장 옳지 않은 것은?

① L2스위치는 IP에 대하여 NAT로 주소 변환하여 패킷을 전송한다.

② L3스위치는 라우팅 경로에 따라 패킷을 전송한다.

③ L4스위치는 TCP/UDP 포트 정보에 따르는 서비스를 구분하여 패킷을 전송한다.

④ L7스위치는 패킷의 내용에 따르는 부가처리를 더하여 패킷을 전송한다.

정답 1번

출제 포인트

OSI 계층별 스위치가 패킷 전달을 판단할 때 사용하는 정보와 제공 기능을 구분하는 문제이다.

핵심 개념

L2 스위치는 데이터 링크 계층의 MAC 주소를 기준으로 프레임을 전달한다. L3 스위치는 네트워크 계층의 IP 주소와 라우팅 정보를 사용한다. L4 스위치는 전송 계층의 TCP·UDP 포트 번호 등을 이용해 서비스를 구분한다. L7 스위치는 응용 계층의 요청 내용까지 분석해 콘텐츠 기반 분배·필터링 등의 부가 처리를 할 수 있다. NAT는 IP 주소를 변환하는 네트워크 계층 기능이므로 L2 스위치의 고유 기능이 아니다.

선지별 해설

① X — 틀린 표현은 ‘L2스위치는 IP에 대하여 NAT로 주소 변환’한다는 부분이다. L2 스위치는 MAC 주소를 기준으로 프레임을 전달하며, 올바르게는 IP 주소 변환인 NAT가 L3 이상의 네트워크 계층 장비나 기능에서 수행된다고 해야 한다.
② O — L3 스위치는 IP 주소와 라우팅 테이블의 경로 정보에 따라 패킷을 목적지 네트워크로 전달한다.
③ O — L4 스위치는 TCP·UDP 포트 번호와 같은 전송 계층 정보를 이용해 웹, 메일 등 서비스를 구분하고 패킷을 분배할 수 있다.
④ O — L7 스위치는 응용 계층의 URL, 헤더, 메시지 등 패킷의 내용까지 확인하여 콘텐츠 기반 분배나 필터링 같은 부가 처리를 할 수 있다.

NoteBase

오답 포인트

①은 '스위치도 IP 패킷을 다룰 수 있다'는 사실과 'L2 스위치의 판단 기준'을 혼동하게 만든다. L2의 핵심 기준은 IP 주소가 아니라 MAC 주소이며, NAT는 단순한 L2 프레임 전달 기능이 아니다.

다시 나오면 이렇게 판단

계층 번호와 판단 정보를 연결한다. L2는 MAC 주소, L3는 IP 주소·라우팅, L4는 TCP·UDP 포트, L7은 응용 데이터의 내용으로 판단한다. 선지의 기능이 해당 계층의 정보 범위를 벗어나면 틀린 설명으로 본다.

암기 포인트

L2-MAC, L3-IP·경로, L4-포트, L7-내용이다. NAT는 L2 기능이 아니다.

NoteBase

문 2. 다음 <보기>는 어떤 형태의 공격에 대한 설명이다. 이와 관련된 내용으로 다음 중 가장 옳지 않은 것은?

<보기>
해커 A는 감염된 다수의 PC에 네트워크를 통해 특정 사이트에 대량의 패킷을 발송하는 프로그램을 다운로드 및 실행시켰으며, 이 프로그램은 특정 날짜, 시간에 어떤 사이트를 일제히 공격하였다. 사이트 관리자는 대량의 패킷 수신에 의한 사이트 마비를 감지하고, 즉시 한국인터넷진흥원에 연락하였고, DNS 싱크홀로 대처하였다.

① 싱크홀이 적용된 DNS 서버는 공격하려는 IP 요청에 대해, 싱크홀 IP 주소로 반환했다.
② 한국인터넷진흥원은 사이트에 대한 공격 접속을 회피시켰다.
③ 일반 사용자는 공격으로 인하여 사이트 접속이 느려졌으나, 접근이 가능했다.
④ 해커는 DDoS 공격을 위해 랜섬웨어를 대량 배포했다.

정답 4번

출제 포인트

다수의 감염 PC가 한 시점에 특정 서버로 대량의 패킷을 보내는 DDoS 공격과, 공격 트래픽을 우회시키는 DNS 싱크홀의 작동 원리를 묻는 문제이다.

핵심 개념

DDoS 공격은 공격자가 다수의 감염 PC를 좀비 PC로 만들어 특정 서버에 트래픽을 집중시켜 서비스를 마비시키는 분산 서비스 거부 공격이다. DNS 싱크홀은 보호 대상 도메인에 대한 DNS 응답을 원래 서버가 아닌 싱크홀 측 IP 주소로 바꾸어 트래픽을 우회시키는 대응 방식이다. 랜섬웨어는 파일이나 시스템을 암호화·잠금한 뒤 금전을 요구하는 악성코드이므로 DDoS 공격용 에이전트와 목적이 다르다.

선지별 해설

① O — DNS 싱크홀이 적용되면 보호 대상 도메인에 대한 질의에 원래 사이트의 IP 주소 대신 싱크홀 IP 주소를 응답하여 트래픽을 우회시킨다.
② O — 한국인터넷진흥원 측 싱크홀로 트래픽을 돌리면 공격 패킷이 원래 사이트에 직접 도달하는 것을 피할 수 있다.
③ O — 공격 트래픽을 싱크홀로 우회하면 원래 사이트의 마비를 줄일 수 있으므로 일반 사용자는 지연을 겪더라도 사이트에 접근할 수 있다.
④ X — 틀린 표현은 'DDoS 공격을 위해 랜섬웨어를 대량 배포했다'이다. 랜섬웨어는 데이터를 암호화하거나 시스템을 잠그고 금전을 요구하는 악성코드이다. 이 사례에서는 다수의 PC를 감염시켜 동시에 패킷을 보내게 하는 봇 또는 DDoS 공격용 악성 프로그램을 배포했다고 해야 한다.

NoteBase

오답 포인트

④의 '랜섬웨어'도 악성코드라는 점 때문에 혼동하기 쉽다. 그러나 악성코드는 기능에 따라 구분되며, 암호화·금전 요구가 핵심인 랜섬웨어와 다수의 감염 PC를 동원해 트래픽을 집중시키는 DDoS 공격 도구는 같은 개념이 아니다.

다시 나오면 이렇게 판단

'다수의 감염 PC가 동시에 대량의 패킷 전송'이면 DDoS로 판단한다. 이어서 DNS 응답을 싱크홀 IP로 바꾸는 것은 공격 트래픽의 우회이고, 파일 암호화와 금전 요구가 나오면 랜섬웨어로 구분한다.

암기 포인트

DDoS는 좀비 PC의 트래픽 집중, DNS 싱크홀은 목적지 우회, 랜섬웨어는 암호화·금전 요구이다.

NoteBase

문 3. 다음 중 192.168.1.0과 같은 IPv4 C 클래스 네트워크를 8개의 서브넷으로 나누고, 각 서브넷에 30개의 호스트를 연결할 때 사용되는 서브넷 마스크는?

① 255.255.255.224

② 255.255.255.192

③ 255.255.255.252

④ 255.255.255.240

정답 1번

출제 포인트

C 클래스 기본 네트워크인 /24에서 8개 서브넷을 만들면서 각 서브넷에 사용 가능한 호스트 주소 30개를 확보하는 프리픽스 길이와 서브넷 마스크를 구하는 문제이다.

조건 정리

주어진 네트워크: 192.168.1.0/24
필요한 서브넷 수: 8개
서브넷별 필요한 호스트 수: 30개
주의할 조건: 각 서브넷에서 네트워크 주소와 브로드캐스트 주소를 제외해야 하므로 실제 사용 가능한 호스트 수는 전체 주소 수보다 2개 적다.

사용할 공식

서브넷 비트 수를 s, 호스트 비트 수를 h라 하면 다음 조건을 만족해야 한다.
$2^s \geq 8$
$2^h - 2 \geq 30$
IPv4 주소는 32비트이고 기본 프리픽스가 /24이므로 남은 8비트를 서브넷 비트와 호스트 비트로 나눈다.

계산 과정

1. $2^3 = 8$이므로 서브넷 비트로 3비트가 필요하다.
2. 기본 /24에서 3비트를 빌리면 프리픽스는 /27이 되고, 호스트 비트는 $32 - 27 = 5$비트가 남는다.
3. 각 서브넷의 사용 가능한 호스트 수는 $2^5 - 2 = 30$개이므로 조건을 정확히 충족한다.
4. /27은 마지막 옥텟의 상위 3비트가 1인 마스크이므로 이진수 11100000은 십진수 224이다. 따라서 서브넷 마스크는 255.255.255.224이다.

NoteBase

선지 판단

① O — 255.255.255.224는 /27이다. 8개의 서브넷을 만들고 각 서브넷에 사용 가능한 호스트 주소 30개를 제공하므로 조건에 맞는다.
② X — 255.255.255.192는 /26이다. 서브넷은 $2^2 = 4$개만 만들어지므로 8개라는 조건을 충족하지 못한다. 올바르게는 /27인 255.255.255.224이다.
③ X — 255.255.255.252는 /30이다. 서브넷별 사용 가능한 호스트 수가 $2^2 - 2 = 2$개뿐이므로 30개를 연결할 수 없다. 올바르게는 호스트 비트 5개를 남기는 /27, 즉 255.255.255.224이다.
④ X — 255.255.255.240은 /28이다. 서브넷별 사용 가능한 호스트 수가 $2^4 - 2 = 14$개이므로 30개에 부족하다. 올바르게는 /27인 255.255.255.224이다.

오답 포인트

8개 서브넷만 보고 3비트를 빌리는 계산에서 끝내거나, 호스트 주소에서 네트워크 주소와 브로드캐스트 주소 2개를 제외하지 않는 것이 함정이다. /28은 서브넷 수는 충분하지만 사용 가능한 호스트가 14개뿐이므로 두 조건을 동시에 확인해야 한다.

다시 나오면 이렇게 판단

필요한 서브넷 수로 빌릴 비트 수를 정하고, 남은 호스트 비트로 $2^h - 2$를 계산한 뒤, 두 조건을 모두 만족하는 프리픽스를 점 표기 십진수 마스크로 변환한다.

암기 포인트

/27은 서브넷 마스크 255.255.255.224이며, 서브넷 하나당 전체 주소 32개와 사용 가능한 호스트 주소 30개를 제공한다.

NoteBase

문 4. 다음 중 포트 스캔(Port Scan)에 관련된 내용으로 가장 옳지 않은 것은?

① FIN Scan, XMAS Scan, NULL Scan, ACK Scan은 로그를 남기지 않는다.

② UDP Scan에서 ICMP Port Unreachable 응답은 방화벽 탐지를 의미한다.

③ TCP 헤더를 조작하여 특수한 패킷을 만들어 열린 포트를 탐지한다.

④ 핸드셰이킹(Handshaking) 절차를 통해 열린 포트를 탐지한다.

정답 2번

출제 포인트

이 문제는 TCP·UDP 포트 스캔에서 전송하는 패킷과 응답이 뜻하는 상태를 구별하는 문제이다.

핵심 개념

TCP Connect Scan은 정상적인 3-way handshaking을 완성하여 열린 포트를 확인한다. 반면 FIN·XMAS·NULL Scan 등은 TCP 헤더의 플래그를 비정상적으로 조합한 탐사 패킷의 응답 차이로 포트 상태를 추정한다. UDP Scan에서는 대상 포트가 닫혀 있으면 일반적으로 ICMP Port Unreachable 응답이 돌아오며, 응답이 없으면 open 또는 filtered 상태일 수 있다.

선지별 해설

① O — FIN·XMAS·NULL Scan은 정상적인 TCP 연결을 완성하지 않는 스텔스 스캔이고, ACK Scan도 정상 접속용 핸드셰이크를 완성하지 않는다. 따라서 일반적인 TCP 연결 로그를 남기기 어렵다는 취지의 설명이다. 다만 실제로는 방화벽이나 IDS가 이러한 탐사 패킷 자체를 기록할 수 있다.
② X — 틀린 표현은 'ICMP Port Unreachable 응답은 방화벽 탐지를 의미한다'이다. 실제로 UDP Scan에서 이 응답은 일반적으로 해당 UDP 포트가 닫혀 있음을 의미한다. 방화벽 등에 의한 필터링은 무응답이나 통신 금지 계열의 ICMP 오류 응답 등으로 판단한다.
③ O — FIN·XMAS·NULL Scan과 같은 TCP 스캔은 TCP 헤더의 플래그를 조작한 특수 패킷을 보내고 응답의 유무나 형태를 분석하여 포트 상태를 추정한다.
④ O — TCP Connect Scan은 SYN, SYN/ACK, ACK의 3-way handshaking을 완성하여 연결이 성립하는지 확인하므로 열린 포트를 탐지할 수 있다.

오답 포인트

②는 'ICMP 응답이 왔다'는 사실을 곧바로 방화벽 탐지로 연결한 것이 함정이다. UDP Scan에서 ICMP Port Unreachable은 우선 closed의 신호이고, 오히려 응답이 없는 경우에 open과 filtered를 명확히 구별하기 어렵다.

다시 나오면 이렇게 판단

스캔별로 '무엇을 보내는가 → 어떤 응답이 오는가 → 어떤 상태로 판정하는가'를 연결한다. UDP Scan에서는 Port Unreachable이면 closed, 무응답이면 open 또는 filtered로 판단한다. TCP Connect Scan은 핸드셰이크를 완성하고, 스텔스 계열 TCP Scan은 플래그를 조작한다.

암기 포인트

UDP의 Port Unreachable은 방화벽이 아니라 closed 신호이다. Connect는 핸드셰이크, FIN·XMAS·NULL은 플래그 조작이다.

NoteBase

문 5. 다음 중 네트워크 공격에 관련된 내용으로 가장 옳지 않은 것은?

① IP 스푸핑(Spoofing)은 공격대상과 신뢰관계에 있는 시스템 주소로 공격자 IP를 위장한다.

② ARP 스푸핑은 공격 대상자의 MAC 주소를 공격자의 MAC 주소로 갱신시킨다.

③ ARP 리다이렉트(Redirect)는 패킷 스니핑(Sniffing)은 불가능하나, 임의 IP로 패킷 전송이 가능해진다.

④ ICMP 리다이렉트는 스니핑 시스템을 네트워크상 추가 라우터(Router)로 등록하여 패킷 스니핑을 한다.

정답 3번

출제 포인트

IP·ARP 스푸핑과 ARP·ICMP 리다이렉트가 트래픽을 속이거나 우회시키는 방식을 구별하는 문제이다.

핵심 개념

IP 스푸핑은 송신지 IP 주소를 신뢰받는 시스템의 주소처럼 위조하는 공격이다.
ARP 스푸핑은 위조된 ARP 정보를 보내 IP 주소와 MAC 주소의 대응 관계를 공격자에게 유리하게 바꾸는 공격이다.
ARP 리다이렉트는 변조된 ARP 정보를 이용해 피해자의 패킷이 공격자 시스템을 거치게 하는 방식이므로 스니핑이 가능하다.
ICMP 리다이렉트 공격은 공격자가 더 적절한 라우터인 것처럼 거짓 경로 정보를 보내 피해자의 패킷 경로를 공격자 쪽으로 바꾸는 방식이다.

선지별 해설

① O — IP 스푸핑은 공격자의 송신지 IP를 공격 대상과 신뢰 관계에 있는 시스템의 IP처럼 위장하는 공격이므로 옳다.
② O — ARP 스푸핑은 피해자의 ARP 캐시에 있는 IP-MAC 대응 정보를 위조하여, 통신 상대의 IP에 공격자의 MAC 주소가 대응되도록 갱신하는 공격이므로 옳다.
③ X — 틀린 표현은 '패킷 스니핑은 불가능'이다. ARP 리다이렉트로 피해자의 패킷을 공격자 시스템을 경유하게 만들면 패킷 스니핑이 가능하다. 올바르게는 'ARP 리다이렉트는 패킷 경로를 공격자 쪽으로 우회시켜 패킷 스니핑을 가능하게 한다'이다.
④ O — ICMP 리다이렉트 공격은 공격자 시스템을 추가 라우터처럼 인식하게 하여 피해자의 패킷을 공격자에게 우회시키고 스니핑할 수 있으므로 옳다.

오답 포인트

③은 '리다이렉트'가 단순히 임의 목적지로 패킷을 보내는 기능인 것처럼 표현하면서 핵심 결과인 스니핑 가능성을 부정한다. 트래픽이 공격자 시스템을 경유하면 공격자는 전달 중인 패킷을 관찰할 수 있다.

NoteBase

다시 나오면 이렇게 판단

스푸핑은 주소나 대응 정보를 위조하는지, 리다이렉트는 패킷의 이동 경로를 공격자 쪽으로 우회시키는지를 확인한다. 패킷이 공격자를 경유하도록 만드는 공격이라면 스니핑이 가능하다고 판단한다.

암기 포인트

IP 스푸핑은 IP 위장, ARP 스푸핑은 IP-MAC 대응 변조, 리다이렉트는 경로 우회와 스니핑이다.

NoteBase

문 6. 다음 중 네트워크를 통한 침입에 대한 대처 방안으로 가장 옳지 않은 것은?

① 방화벽(Firewall), IDS, IPS는 모두 네트워크 액세스에 대한 보안 대책이다.

② 트로이목마에 의해 방화벽 안쪽 PC가 해킹되었을 때, 방화벽은 공격에 매우 취약하다.

③ 방화벽은 패킷 내부의 전송 데이터에 대한 분석을 수행하지 않는다.

④ 가장 적극적인 차단을 실시하여 예방적 방어를 수행하는 것은 IDS이다.

정답 4번

출제 포인트

이 문제는 방화벽, IDS, IPS가 네트워크 침입에 대응하는 방식과 각 보안 대책의 한계를 구분하는 문제이다.

핵심 개념

방화벽(Firewall): 미리 정한 보안 정책에 따라 네트워크 경계에서 통신의 허용·차단을 결정하는 장치이다. 일반적인 패킷 필터링 방화벽은 주로 출발지·목적지 주소, 포트, 프로토콜 등의 헤더 정보를 기준으로 판단한다.
IDS(Intrusion Detection System): 침입 징후를 탐지하여 관리자에게 경보하는 시스템이다. 핵심은 탐지와 알림이다.
IPS(Intrusion Prevention System): 침입 징후를 탐지할 뿐 아니라 해당 트래픽을 실시간으로 차단하여 공격을 예방하는 시스템이다. 핵심은 탐지와 능동 차단이다.

선지별 해설

① O — 방화벽은 접근통제를 수행하고, IDS와 IPS는 네트워크 트래픽에서 침입 징후를 탐지하거나 차단하므로 모두 네트워크 접근·침입에 대한 보안 대책에 해당한다.
② O — 트로이목마로 내부 PC가 이미 감염되면 공격 경로가 방화벽 안쪽에 형성될 수 있다. 네트워크 경계의 통신을 통제하는 방화벽만으로는 내부에서 시작된 공격이나 허용된 연결을 악용한 공격을 막기 어렵다.
③ O — 전통적인 패킷 필터링 방화벽은 패킷 헤더의 주소, 포트, 프로토콜 등을 검사하며 전송 데이터의 구체적인 내용까지 분석하지 않는다. 따라서 이 문항의 방화벽 기능 설명으로 옳다.
④ X — 틀린 표현은 '가장 적극적인 차단을 실시하여 예방적 방어를 수행하는 것은 IDS'이다. IDS는 침입을 탐지하고 경보하는 역할이 중심이며, 탐지한 공격 트래픽을 능동적으로 차단하여 예방적 방어를 수행하는 것은 IPS이다.

오답 포인트

④는 IDS와 IPS의 공통 기능인 '탐지'를 이용해 두 개념을 바꾸어 놓았다. '적극적인 차단'과 '예방'이라는 표현은 IDS가 아니라 IPS를 가리킨다.

NoteBase

다시 나오면 이렇게 판단

‘탐지·경보’이면 IDS, ‘탐지 후 실시간 차단·예방’이면 IPS로 판단한다. 방화벽은 네트워크 경계에서 정책에 따라 통신을 허용하거나 차단하지만, 이미 내부에 들어온 악성코드에 의한 공격에는 한계가 있다.

암기 포인트

IDS는 Detect(탐지·경보), IPS는 Prevent(예방·차단)이다.

NoteBase

문 7. 다음 중 무선랜에 관련된 설명으로 가장 옳지 않은 것은?

① WPA2-PSK는 인증서버를 두고 사용자 계정과 패스워드에 기반한 암호화이다.

② TKIP과 CCMP 중 CCMP가 더 강화된 보안 프로토콜이다.

③ WEP에서 WPA, WPA2로 발전하면서, 암호 알고리즘이 점차 강화되었다.

④ CCMP는 AES 블록 암호에 기반한 프로토콜로 WPA2에 적용된다.

정답 1번

출제 포인트

WPA2의 개인용 인증 방식인 PSK와 기업용 인증 방식의 차이, 그리고 TKIP·CCMP의 보안 수준을 구분하는 문제이다.

핵심 개념

WPA2-PSK: 인증 서버 없이 무선 공유기와 단말이 미리 공유한 비밀키(패스프레이즈)를 사용하는 개인용 방식이다.
WPA2-Enterprise: 802.1X와 RADIUS 등의 인증 서버를 이용하여 사용자별 계정이나 인증서를 확인하는 기업용 방식이다.
TKIP과 CCMP: TKIP은 WPA에서 기존 WEP 장비의 취약점을 보완하기 위해 사용한 방식이고, CCMP는 AES 블록 암호를 기반으로 기밀성과 무결성을 제공하는 더 강한 방식이다.

선지별 해설

① X — '인증서버를 두고 사용자 계정과 패스워드에 기반'이라는 부분이 틀리다. WPA2-PSK는 인증 서버를 두지 않고 AP와 단말이 미리 공유한 키를 사용한다. 인증 서버에서 사용자별 자격 증명을 확인하는 것은 WPA2-Enterprise 방식이다.
② O — CCMP는 AES를 기반으로 암호화와 무결성 보호를 제공하므로, TKIP보다 강화된 보안 프로토콜이다.
③ O — WEP의 취약점을 보완하기 위해 WPA가 도입되었고, 이어 WPA2에서 AES 기반 CCMP가 채택되면서 무선랜 보안이 전반적으로 강화되었다.
④ O — CCMP는 AES 블록 암호를 사용하는 보안 프로토콜이며 WPA2에 적용된다.

오답 포인트

①은 PSK의 '패스프레이즈'와 기업용 방식의 '사용자 계정·패스워드'를 섞어 놓았다. 패스프레이즈가 등장한다고 해서 인증 서버를 사용하는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

PSK가 보이면 인증 서버 없이 미리 공유한 키를 쓰는 개인용 방식으로 판단한다. 802.1X, RADIUS, 사용자별 계정·인증서가 보이면 Enterprise 방식으로 판단한다. 암호 프로토콜의 보안 수준은 일반적으로 TKIP보다 AES 기반 CCMP가 높다.

암기 포인트

PSK는 공유키, Enterprise는 인증 서버, WPA2의 핵심 암호 프로토콜은 AES 기반 CCMP이다.

NoteBase

문 8. 다음 <보기>는 어떤 웹서버 공격에 관련된 내용을 말한 것이다. 다음 중 내용으로 알 수 있는 것으로 가장 옳지 않은 것은?

<보기>
“우리 원의 웹사이트 외주 제작자가 큰 실수를 했습니다. 게시물 업로드 폼에 GET이 쓰였고, 해커가 이를 이용해 웹서버에서 악성 스크립트를 실행시켰습니다. 그리고 그 스크립트로 웹 DB의 사용자 게시물에 다른 해킹 서버로 액세스하도록 또 다른 스크립트를 덧붙였습니다.
결국 그 해킹된 웹서버에 접속해 게시글을 읽은 민원인 PC에 랜섬웨어가 다운로드 되어서 큰 문제가 터졌습니다. 현재 웹서버 로그에 남은 해커 IP 기록을 찾았고, 추적 중입니다.”

① 해커는 CSRF, XSS, 랜섬웨어를 모두 사용했다.
② 해커는 서버와 게시물을 읽은 사용자 PC에 모두 악성 스크립트를 실행시켰다.
③ 폼의 입력란에 대한 필터링과 GET대신 POST를 이용하면 보완이 가능하다.
④ 해커는 일반 사용자 PC를 우선 해킹하고 이를 경유하여 원의 웹서버를 해킹했다.

정답 4번

출제 포인트

이 문제는 웹 공격이 CSRF에서 저장형 XSS와 랜섬웨어 유포로 이어지는 과정을 사례의 시간 순서와 공격 위치에 맞게 판단하는 문제이다.

사례 정리

핵심 사실 1: 해커가 GET 방식의 게시물 업로드 기능을 악용해 웹서버에 악성 스크립트를 실행시켰다.
핵심 사실 2: 웹 DB에 저장되는 사용자 게시물에 외부 해킹 서버로 접속하는 스크립트가 삽입되었다.
핵심 사실 3: 이후 해당 게시물을 읽은 민원인의 PC에 랜섬웨어가 다운로드되었다.
판단에 중요한 조건: 공격의 진행 방향은 웹서버와 게시물 오염이 먼저이고, 게시물을 읽은 사용자 PC의 피해가 나중이다.

핵심 개념

CSRF는 사용자의 의도와 무관하게 웹 애플리케이션에 요청을 보내도록 만드는 공격이다.
저장형 XSS는 공격자가 삽입한 스크립트가 서버의 게시물이나 DB에 저장되었다가 해당 페이지를 보는 사용자의 브라우저에서 실행되는 공격이다.
랜섬웨어는 시스템이나 파일의 이용을 제한하고 금전을 요구하는 악성코드이다.

NoteBase

적용 기준

사례의 행위를 요청 위조, 서버·DB에 스크립트 저장, 사용자 브라우저에서 스크립트 실행, 랜섬웨어 다운로드의 순서로 나누어 판단한다. 특히 최초 침해 대상과 이후 피해 대상을 뒤바꾸지 않아야 한다.

선지별 해설

① O — GET 방식의 폼 악용은 CSRF 관련 단서이고, 게시물에 스크립트를 삽입해 열람자의 브라우저에서 동작하게 한 부분은 저장형 XSS이며, 최종적으로 랜섬웨어가 다운로드되었다. 따라서 사례에는 세 공격 요소가 모두 나타난다.
② O — 해커는 먼저 웹서버 측에서 악성 스크립트를 실행하고 게시물에 다른 스크립트를 삽입했다. 이후 게시물을 읽은 사용자 PC에서는 삽입된 스크립트가 작동해 외부 해킹 서버에 접근하고 랜섬웨어 다운로드로 이어졌다. 따라서 서버와 사용자 PC 양쪽에서 악성 코드가 실행되는 흐름이다.
③ O — 게시물 입력값을 검증·필터링하면 악성 스크립트 삽입을 줄일 수 있고, 상태를 변경하는 요청을 GET 대신 POST로 처리하면 URL만으로 요청이 실행되는 위험을 줄일 수 있다. 다만 POST 사용만으로 CSRF가 완전히 차단되는 것은 아니므로 실무에서는 CSRF 토큰 등의 검증도 함께 사용한다.
④ X — 사례에서는 일반 사용자 PC를 먼저 해킹해 웹서버로 경유한 것이 아니다. 틀린 표현인 '일반 사용자 PC를 우선 해킹하고 이를 경유하여 웹서버를 해킹했다'는 '웹서버와 게시물을 먼저 공격하고, 오염된 게시물을 읽은 일반 사용자 PC에 후속 피해를 일으켰다'로 고쳐야 한다.

오답 포인트

④는 등장하는 공격 대상 자체는 모두 맞지만 공격 순서를 거꾸로 제시한다. 또한 ③의 POST는 단독으로 완전한 방어책이라는 뜻이 아니라 GET 사용에 따른 위험을 줄이는 보완책이라는 점을 구분해야 한다.

다시 나오면 이렇게 판단

웹 공격 사례는 요청을 누가 만들었는지, 악성 코드가 어디에 저장되었는지, 어디에서 실행되었는지, 최종 피해가 무엇인지의 네 단계로 나누어 시간 순서대로 판단한다.

암기 포인트

요청 위조는 CSRF, 저장된 스크립트의 브라우저 실행은 저장형 XSS, 파일·시스템을 인질로 삼는 악성코드는 랜섬웨어이다.

NoteBase

문 9. DNS는 도메인에 대한 IP 주소 변환을 수행하는 역할을 한다. 다음 중 이에 관련된 내용으로 가장 옳지 않은 것은?

① DNS 스푸핑(Spoofing)은 특정 도메인에 대해 가짜 IP 주소를 반환하는 기법이다.

② DNS 싱크홀(Sinkhole)은 방어할 도메인에 대해 공격 트래픽을 처리할 대치된 IP주소를 반환하는 방법이다.

③ DNS Cache Poisoning은 공격대상 DNS 서버에 대량의 패킷을 전송하여 동작을 정지시키고, 해킹서버를 가짜 DNS 서버로 등록시킨다.

④ DNSSEC은 전자서명을 이용해, 서명된 응답만이 등록되도록 검증 처리한다.

정답 3번

출제 포인트

DNS 스푸핑, DNS 싱크홀, DNS 캐시 포이즈닝, DNSSEC의 목적과 동작 차이를 묻는 문제이다.

핵심 개념

DNS 스푸핑은 위조된 DNS 응답으로 사용자를 가짜 IP 주소로 유도하는 공격이다.
DNS 싱크홀은 악성·위험 도메인의 질의를 방어자가 통제하는 IP 주소로 보내 공격 통신을 차단하거나 분석하는 방어 기법이다.
DNS 캐시 포이즈닝은 DNS 캐시에 위조된 도메인-IP 매핑 정보를 저장시켜 이후 질의에 잘못된 주소를 돌려주게 하는 공격이다.
DNSSEC은 DNS 데이터에 대한 전자서명을 검증하여 응답의 출처와 무결성을 확인하는 기술이다.

선지별 해설

① O — DNS 스푸핑은 특정 도메인 질의에 대해 공격자가 의도한 가짜 IP 주소를 응답하여 사용자를 위조 사이트 등으로 유도하는 기법이다.
② O — DNS 싱크홀은 악성·위험 도메인에 방어자가 관리하는 대체 IP 주소를 반환하여 해당 트래픽을 차단하거나 수집·분석하는 방법이다.
③ X — 틀린 부분은 '대량의 패킷을 전송하여 DNS 서버를 정지시키고, 해킹 서버를 가짜 DNS 서버로 등록시킨다'는 설명이다. 이는 서비스 거부 공격과 가짜 DNS 서버 운용을 섞은 표현이다. 올바르게는 공격자가 위조 DNS 응답을 주입하여 대상 DNS 서버의 캐시에 거짓 도메인-IP 매핑을 저장시키는 공격이다.
④ O — DNSSEC은 전자서명을 이용해 DNS 응답의 출처와 데이터 무결성을 검증한다. 즉 신뢰 사슬에 따라 서명을 검증함으로써 위조·변조된 응답의 수용을 막는다.

NoteBase

오답 포인트

③은 DNS 캐시 포이즈닝을 DNS 서버에 대한 대량 패킷 공격과 혼동하게 만든다. 핵심은 서버를 정지시키는 것이 아니라 캐시 안의 도메인-IP 매핑을 거짓 정보로 오염시키는 데 있다.

다시 나오면 이렇게 판단

가짜 응답으로 잘못된 IP를 알려 주면 스푸핑, 캐시에 거짓 매핑을 남기면 캐시 포이즈닝, 방어자가 통제하는 주소로 보내면 싱크홀, 전자서명으로 출처와 무결성을 검증하면 DNSSEC으로 판단한다.

암기 포인트

스푸핑은 응답 위조, 포이즈닝은 캐시 오염, 싱크홀은 방어용 우회, DNSSEC은 서명 검증이다.

NoteBase

문 10. 다음 중 NAC(Network Access Control) 시스템의 기능 설명으로 가장 옳지 않은 것은?

① 접근 제어 및 접근 인증

② 백신 관리 및 패치 관리

③ 방화벽 및 IPS 통합 로그 관리

④ 유해 트래픽 탐지 및 차단

정답 3번

출제 포인트

NAC의 단말 접근 통제·보안 상태 점검 기능과 여러 보안 장비의 로그를 한곳에서 통합 관리하는 기능을 구별하는 문제이다.

핵심 개념

NAC(Network Access Control)는 네트워크에 접속하려는 사용자와 단말을 식별·인증하고, 보안 정책 준수 여부를 검사하여 접속을 허용·제한하거나 격리하는 시스템이다. 백신·패치 적용 상태 점검과 유해 트래픽에 대한 탐지·차단은 NAC의 접근 통제 과정에 포함될 수 있다. 반면 방화벽·IPS 등 서로 다른 보안 장비의 로그를 수집하여 연계 분석하고 통합 관리하는 것은 ESM이나 SIEM의 대표 기능이다.

선지별 해설

① O — NAC는 네트워크에 접근하는 사용자와 단말을 식별·인증하고 정책에 따라 접근 권한을 제어한다.
② O — NAC는 접속 단말의 백신 설치·업데이트 여부와 보안 패치 적용 상태를 점검하고, 기준을 충족하지 못한 단말의 접속을 제한하거나 치료·보완을 유도할 수 있다.
③ X — 틀린 표현은 '방화벽 및 IPS 통합 로그 관리'이다. 여러 보안 장비의 로그를 한곳에 수집하여 통합 관리·분석하는 것은 NAC보다 ESM 또는 SIEM의 대표 기능이다.
④ O — NAC는 접속 단말과 네트워크 행위를 정책에 따라 감시하여 유해하거나 비정상적인 트래픽을 탐지하고 해당 단말의 통신을 차단·격리할 수 있다.

오답 포인트

③도 네트워크 보안 기능이라는 점 때문에 NAC의 기능처럼 보이지만, 핵심어가 '통합 로그 관리'라는 데 함정이 있다. NAC의 중심은 접속 주체와 단말의 인증·상태 점검·접근 통제이고, 여러 장비의 로그 통합과 연계 분석은 ESM·SIEM의 영역이다.

다시 나오면 이렇게 판단

사용자·단말의 접속 허용 여부, 보안 상태 검사, 격리·차단에 관한 설명이면 NAC로 판단한다. 방화벽·IPS·서버 등 여러 장비에서 나온 로그의 수집·통합·상관분석이 중심이면 ESM 또는 SIEM으로 판단한다.

NoteBase

암기 포인트

NAC는 '누가 어떤 상태로 접속하는가'를 통제하고, ESM·SIEM은 '여러 장비의 로그를 모아 분석'한다.

NoteBase

문 11. 다음 중 VPN에 의해 제공되는 보안 기능으로 가장 옳지 않은 것은?

① 전송 데이터에 대해 암호화 보안 전송이 이루어진다.

② LAN에 대한 연결 허가를 통제할 수 있는 접근 제어가 제공된다.

③ 패킷을 데이터 내용에 따라 필터링하여 바이러스를 차단한다.

④ 터널링(Tunneling)을 통하여 원격지 PC를 내부망으로 연결해준다.

정답 3번

출제 포인트

VPN이 제공하는 핵심 보안 기능과 악성코드 탐지 기능을 구별하는 문제이다.

핵심 개념

VPN은 공중망을 이용하면서 인증과 암호화된 터널을 통해 사설망처럼 안전한 통신 경로를 구성하는 기술이다. VPN의 핵심은 통신 상대와 접근 권한을 확인하고 전송 데이터를 보호하는 데 있으며, 패킷의 응용 데이터 내용을 분석하여 바이러스를 탐지·차단하는 기능은 별도의 보안 솔루션 영역이다.

선지별 해설

① O — VPN은 터널을 통과하는 전송 데이터를 암호화하여 도청으로부터 기밀성을 보호할 수 있다.
② O — VPN 접속 과정에서 사용자나 장치를 인증하고 권한을 확인하므로, 허가된 주체의 내부 LAN 접속만 허용하는 접근 제어를 제공할 수 있다.
③ X — 틀린 부분은 '데이터 내용에 따라 필터링하여 바이러스를 차단한다'이다. VPN은 암호화·인증·터널링으로 통신 경로를 보호하며, 바이러스 탐지와 차단은 백신, 보안 게이트웨이, 침입방지시스템 등의 콘텐츠 검사 기능이 담당한다.
④ O — VPN의 터널링은 공중망 위에 논리적인 전용 통신 경로를 만들어 원격지 PC가 내부망에 안전하게 접속하도록 한다.

오답 포인트

③은 '보안 기능'이라는 넓은 표현을 이용해 VPN에 바이러스 차단 기능까지 포함되는 것처럼 보이게 한다. 그러나 암호화된 터널을 만드는 기능과 데이터 내용을 검사해 악성코드를 찾는 기능은 서로 다르다.

다시 나오면 이렇게 판단

선지가 인증, 접근 제어, 암호화, 무결성 보호, 터널링을 말하면 VPN의 기능으로 판단한다. 반면 바이러스 탐지, 악성코드 제거, 응용 데이터 내용 필터링을 말하면 VPN 자체의 핵심 기능이 아닌 별도 보안 기능으로 판단한다.

NoteBase

암기 포인트

VPN은 인증·암호화·터널링, 바이러스 차단은 콘텐츠 검사이다.

NoteBase

문 12. 다음 중 FDS(Fraud Detection System)에 관련된 내용으로 가장 옳지 않은 것은?

① 금융전산망 및 서버에 대한 해킹 침입을 탐지한다.

② 전자상거래에서 이상 거래를 탐지하기 위한 방법으로 사용한다.

③ 거래 발생 시 거래자 위치, 업종, 물품, 금액 등의 위험성을 평가한다.

④ 동일한 공간이 아니고, 시간적으로도 이동할 수 없는 위치에서의 거래 발생을 탐지한다.

정답 1번

출제 포인트

FDS가 탐지하는 금융·전자상거래의 이상 거래와 IDS가 탐지하는 정보시스템 침입을 구별하는 문제이다.

핵심 개념

FDS(Fraud Detection System)는 거래자의 평소 이용 패턴과 거래 정보를 분석하여 부정 사용이나 이상 거래를 탐지·차단하는 시스템이다. 반면 IDS(Intrusion Detection System)는 네트워크나 서버에서 발생하는 비인가 접근, 공격 등 침입 징후를 탐지한다. 결정적인 구별 기준은 탐지 대상이 '거래의 이상성'인지 '시스템 침입'인지이다.

선지별 해설

① X — '금융전산망 및 서버에 대한 해킹 침입을 탐지한다'는 부분이 FDS의 주된 기능에 해당하지 않는다. 이는 네트워크·서버의 침입 징후를 탐지하는 IDS에 관한 설명이다. 올바르게는 FDS가 금융 거래 정보와 이용 패턴을 분석하여 이상 거래나 부정 사용을 탐지한다고 해야 한다.
② O — FDS는 전자상거래에서 정상 패턴을 벗어난 결제나 부정 사용으로 의심되는 이상 거래를 탐지하는 데 사용된다.
③ O — 거래 시점의 거래자 위치, 업종, 물품, 금액 등 여러 정보를 결합하여 거래 위험도를 평가하는 것은 FDS의 기능이다.
④ O — 짧은 시간 안에 현실적으로 이동할 수 없는 서로 먼 위치에서 연속 거래가 발생하는 것은 이상 거래의 대표적인 징후이므로 FDS의 탐지 대상이 된다.

오답 포인트

금융기관의 서버에서 운용된다는 이유만으로 ①의 해킹 침입 탐지를 FDS 기능으로 보기 쉽다. 그러나 설치·운용 장소가 아니라 분석 대상이 거래인지 네트워크 침입인지로 구분해야 한다.

다시 나오면 이렇게 판단

위치·시간·업종·물품·금액·평소 이용 패턴을 비교하면 FDS로 판단한다. 패킷, 비인가 접근, 공격 시도, 서버 침입 징후를 탐지하면 IDS로 판단한다.

NoteBase

암기 포인트

FDS는 수상한 거래, IDS는 수상한 침입을 찾는다.

NoteBase

문 13. 다음 중 OSI 계층과 전송단위의 연결로 가장 옳은 것은?

① OSI 계층: 데이터링크(Data Link), 전송단위: 세그먼트(Segment)

② OSI 계층: 응용(Application), 전송단위: 메시지(Message)

③ OSI 계층: 전송(Transport), 전송단위: 프레임(Frame)

④ OSI 계층: 네트워크(Network), 전송단위: 비트 스트림(Bit Stream)

정답 2번

출제 포인트

OSI 7계층의 각 계층에서 다루는 전송단위(PDU)를 올바르게 연결할 수 있는지를 묻는 문제이다.

핵심 개념

응용 계층은 사용자가 이용하는 네트워크 서비스의 데이터를 다루며 전송단위는 메시지 또는 데이터이다.
전송 계층은 종단 간 통신을 담당하며 전송단위는 세그먼트이다.
네트워크 계층은 논리 주소와 경로 선택을 담당하며 전송단위는 패킷이다.
데이터링크 계층은 인접 노드 사이의 전송과 오류 검출을 담당하며 전송단위는 프레임이다.
물리 계층은 전기적·광학적 신호로 비트를 전달하며 전송단위는 비트이다.

선지별 해설

① X — 데이터링크 계층의 전송단위는 세그먼트가 아니라 프레임이다. 올바른 연결은 '데이터링크(Data Link)-프레임(Frame)'이다.
② O — 응용 계층은 사용자의 응용 서비스가 생성한 메시지 또는 데이터를 다루므로 '응용(Application)-메시지(Message)'의 연결이 옳다.
③ X — 전송 계층의 전송단위는 프레임이 아니라 세그먼트이다. 올바른 연결은 '전송(Transport)-세그먼트(Segment)'이다.
④ X — 네트워크 계층의 전송단위는 비트 스트림이 아니라 패킷이다. 비트는 물리 계층의 전송단위이므로 올바른 연결은 '네트워크(Network)-패킷(Packet)'이다.

오답 포인트

①과 ③은 데이터링크 계층의 프레임과 전송 계층의 세그먼트를 서로 바꾸어 놓았고, ④는 물리 계층의 비트를 네트워크 계층에 연결한 것이 함정이다.

다시 나오면 이렇게 판단

계층 이름만 보지 않고 '응용-메시지, 전송-세그먼트, 네트워크-패킷, 데이터링크-프레임, 물리-비트'의 대응 관계를 차례로 대조한다.

NoteBase

암기 포인트

상위 계층부터 메시지-세그먼트-패킷-프레임-비트 순서로 기억한다.

NoteBase

문 14. 다음 중 TCP/UDP 설명으로 가장 옳지 않은 것은?

① UDP는 순서번호를 사용하지 않는다.

② TCP는 상당한 양의 자원을 사용하지만 UDP보다 느리다.

③ TCP는 흐름 제어와 윈도우 매커니즘이 없다.

④ UDP는 ACK를 보내지 않으며 신뢰성이 없는 프로토콜이다.

정답 3번

출제 포인트

TCP와 UDP의 연결 방식, 신뢰성 보장, 흐름 제어 및 전송 오버헤드의 차이를 묻는 문제이다.

핵심 개념

TCP는 연결을 설정한 뒤 순서 제어, 확인 응답, 재전송, 흐름 제어 등을 통해 신뢰성 있는 전송을 제공하는 프로토콜이다. UDP는 연결 설정이나 확인 응답 없이 데이터를 독립적인 데이터그램으로 전송하여 오버헤드는 작지만 전달과 순서를 보장하지 않는 프로토콜이다.
핵심 대비는 TCP가 신뢰성과 제어 기능을 제공하는 대신 처리 부담이 크고, UDP는 제어 기능을 줄여 단순하고 빠른 전송에 적합하다는 점이다.

선지별 해설

① O — UDP 헤더에는 TCP처럼 바이트의 전송 순서를 관리하는 순서번호 필드가 없다. 따라서 UDP 자체는 데이터그램의 도착 순서를 보장하지 않는다.
② O — TCP는 연결 설정, 확인 응답, 재전송, 순서 제어 등의 처리를 수행하므로 UDP보다 헤더와 상태 관리에 더 많은 자원을 사용하고 일반적으로 전송 지연과 처리 부담이 크다.
③ X — 틀린 부분은 '흐름 제어와 윈도우 메커니즘이 없다'이다. TCP에는 수신 측이 처리할 수 있는 양에 맞추어 송신량을 조절하는 흐름 제어가 있으며, 이를 위해 수신 윈도우와 슬라이딩 윈도우 메커니즘을 사용한다.
④ O — UDP는 프로토콜 자체에서 ACK를 주고받거나 손실 패킷을 재전송하지 않으므로 전달 성공을 보장하지 않는 비신뢰성 프로토콜이다.

오답 포인트

TCP의 윈도우 기능을 혼잡 제어와만 연결하면 ③을 놓치기 쉽다. TCP의 윈도우는 수신 측의 처리 능력에 맞추는 흐름 제어에도 사용되므로 '흐름 제어와 윈도우 메커니즘이 없다'는 설명은 TCP와 정반대이다.

다시 나오면 이렇게 판단

ACK, 순서번호, 재전송, 흐름 제어, 윈도우가 제시되면 TCP의 신뢰성·제어 기능으로 판단한다. 연결 설정과 ACK 없이 낮은 오버헤드로 전송한다는 설명은 UDP에 해당한다.

NoteBase

암기 포인트

TCP는 연결·ACK·순서·재전송·흐름 제어·윈도우, UDP는 무연결·무ACK·저오버헤드이다.

NoteBase

문 15. 다음 중 송신측에 데이터가 손실되고 있음을 알려서 전송을 잠시 중단하거나 전송률을 줄이도록 하는 ICMP(Internet Control Message Protocol) 메시지로 가장 옳은 것은?

① Destination Unreachable(Type 3)

② Source Quench(Type 4)

③ Redirection(Type 5)

④ Time Exceeded(Type 11)

정답 2번

출제 포인트

ICMP 오류 보고 메시지의 Type 번호와 각 메시지가 송신측에 전달하는 의미를 구별하는 문제이다.

핵심 개념

Source Quench는 혼잡이나 버퍼 부족으로 데이터그램이 손실될 수 있음을 송신측에 알리고 전송률을 낮추도록 요청하기 위해 정의되었던 ICMP 메시지이며 Type 4이다. 다만 현재는 폐기된 방식으로, 호스트는 이를 송신해서는 안 되고 TCP도 수신한 Source Quench를 무시한다.

선지별 해설

① X — Destination Unreachable(Type 3)는 목적지 네트워크·호스트·프로토콜·포트 등에 도달할 수 없음을 알리는 메시지이다. 틀린 표현은 송신측에 전송 중단이나 전송률 감소를 요구하는 메시지로 본 부분이며, 올바르게는 도달 불가 원인을 알리는 메시지이다.
② O — Source Quench(Type 4)는 원래 혼잡 등으로 데이터그램이 손실될 때 송신측에 전송률을 낮추도록 요청하는 용도로 정의되었으므로 문제의 설명에 해당한다.
③ X — Redirection(Type 5)은 호스트에게 특정 목적지로 가는 더 적절한 게이트웨이 또는 경로를 알려 주는 메시지이다. 틀린 표현은 데이터 손실에 따른 전송률 감소 요청으로 본 부분이며, 올바르게는 경로 변경을 안내하는 메시지이다.
④ X — Time Exceeded(Type 11)는 데이터그램의 TTL이 0이 되었거나 조각 재조립 제한 시간을 초과했음을 알리는 메시지이다. 틀린 표현은 혼잡에 따른 전송률 감소 요청으로 본 부분이며, 올바르게는 허용 시간이 초과되어 전달 또는 재조립이 완료되지 못했음을 알리는 메시지이다.

오답 포인트

①의 Destination Unreachable는 데이터그램 손실과 관련될 수 있지만 송신 속도를 줄이라는 메시지는 아니다. 문제의 핵심 표현인 '전송률을 줄이도록 한다'와 직접 연결되는 것은 ② Source Quench이다.

NoteBase

다시 나오면 이렇게 판단

ICMP 메시지를 기능어로 대응한다. 도달 불가이면 Type 3, 혼잡 완화를 위한 송신 속도 감소 요청이면 Type 4, 더 나은 경로 안내이면 Type 5, TTL 또는 재조립 시간 초과이면 Type 11이다.

암기 포인트

3 도달 불가, 4 속도 억제, 5 경로 변경, 11 시간 초과로 연결한다.

NoteBase

문 16. 다음 <보기>에서 설명하는 라우팅 프로토콜로 가장 옳은 것은?

<보기>
◯ 인트라 도메인 라우팅 프로토콜이다.
◯ 링크 상태 라우팅 프로토콜을 기반으로 한다.
◯ 논리적 백본(Backbone)을 사용하며 영역(Area)과 연결한다.

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

정답 4번

출제 포인트

이 문제는 라우팅 프로토콜을 적용 범위와 경로 계산 방식으로 구별하는 문제이다. 보기의 핵심은 인트라 도메인, 링크 상태, 백본 영역과 일반 영역의 연결이다.

핵심 개념

OSPF는 하나의 자율 시스템 내부에서 사용하는 링크 상태 기반의 내부 게이트웨이 프로토콜이다. 네트워크를 여러 영역으로 나누고, 모든 일반 영역이 논리적 백본인 Area 0을 통해 연결되도록 구성한다.
RIP와 IGRP는 내부 게이트웨이 프로토콜이지만 거리 벡터 계열이므로 링크 상태 방식과 영역·백본 구조라는 조건에 맞지 않는다. BGP는 자율 시스템 사이에서 경로 정보를 교환하는 경로 벡터 기반의 외부 게이트웨이 프로토콜이다.

선지별 해설

① X — RIP는 자율 시스템 내부에서 쓰이지만 거리 벡터 기반이며, Area 0을 중심으로 영역을 연결하는 구조를 사용하지 않는다. 틀린 대응은 RIP이며, 보기의 설명에 맞는 프로토콜은 OSPF이다.
② X — IGRP는 시스코가 개발한 거리 벡터 기반의 내부 게이트웨이 프로토콜이다. 링크 상태와 백본 영역을 사용하는 프로토콜이라는 설명으로 고치면 OSPF가 된다.
③ X — BGP는 서로 다른 자율 시스템 사이의 라우팅에 사용하는 경로 벡터 기반 프로토콜이다. 인트라 도메인의 링크 상태 프로토콜이라는 설명에 맞게 고치면 OSPF이다.
④ O — OSPF는 인트라 도메인에서 사용하는 링크 상태 라우팅 프로토콜이며, Area 0을 논리적 백본으로 두고 다른 영역을 연결한다. 보기의 세 조건을 모두 충족한다.

NoteBase

오답 포인트

RIP와 IGRP도 인트라 도메인 프로토콜이라는 점만 보고 고르면 틀리기 쉽다. 이 문항의 결정적 표현은 '링크 상태'와 '백본·영역'이며, 두 표현이 함께 나오면 OSPF를 가리킨다.

다시 나오면 이렇게 판단

먼저 적용 범위가 자율 시스템 내부인지 외부인지 구분하고, 다음으로 거리 벡터·링크 상태·경로 벡터 중 어떤 방식인지 확인한다. 내부망에서 링크 상태와 Area 0이 함께 제시되면 OSPF로 판단한다.

암기 포인트

OSPF는 내부·링크 상태·Area 0, RIP와 IGRP는 내부·거리 벡터, BGP는 외부·경로 벡터이다.

NoteBase

문 17. 라우터 텔넷 관리 접근통제를 위해 <보기>와 같이 access-list를 설정하였다. 다음 중 적용하는 방법으로 가장 옳은 것은?

<보기>
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#access-list 1 deny any
-생략-

① Router(config-if)#ip access-group 1 in
② Router(config)#ip access-group 1 in
③ Router(config-con)#access-class 1 in
④ Router(config-line)#access-class 1 in

정답 4번

출제 포인트

표준 ACL을 일반 인터페이스 트래픽에 적용하는 ip access-group 명령과 텔넷 등 원격 관리 접속을 제한하는 access-class 명령의 적용 위치를 구별하는 문제이다.

핵심 개념

ip access-group은 라우터 인터페이스를 통과하는 패킷을 필터링하며 인터페이스 설정 모드에서 사용한다. access-class는 라우터의 VTY 가상 터미널에 들어오는 원격 관리 접속을 제한하며 라인 설정 모드에서 사용한다. 따라서 텔넷 접근통제에는 line vty 설정으로 들어간 뒤 access-class 1 in을 적용한다.

NoteBase

선지별 해설

① X
Router(config-if)#ip access-group 1 in은 해당 인터페이스로 유입되는 일반 IP 패킷에 ACL 1을 적용하는 명령이다. 텔넷 관리 접속 자체를 VTY에서 제한하는 명령이 아니다. 틀린 표현은 ip access-group이며, 올바르게는 VTY 라인 설정 모드에서 access-class 1 in을 사용한다.

② X
ip access-group은 전역 설정 모드(config)가 아니라 인터페이스 설정 모드(config-if)에서 사용하는 명령이다. 또한 이 문항의 목적은 VTY 텔넷 접근통제이므로, 올바르게는 Router(config-line)#access-class 1 in을 사용한다.

③ X
텔넷은 콘솔이 아니라 VTY 가상 터미널을 통한 원격 접속이다. 또한 적용 프롬프트도 config-con이 아니라 line vty 진입 후의 config-line이어야 한다. 올바르게는 Router(config-line)#access-class 1 in이다.

④ O
Router(config-line)#access-class 1 in은 VTY 라인으로 들어오는 접속의 출발지 주소를 ACL 1로 검사한다. 따라서 192.168.1.0/24에서 오는 텔넷 관리 접속만 허용하려는 설정에 맞는다.

오답 포인트

①의 ip access-group도 ACL을 적용하는 명령이어서 혼동하기 쉽다. 그러나 인터페이스를 통과하는 트래픽은 ip access-group, 라우터 자신에 대한 VTY 원격 접속은 access-class로 구별한다. ③은 access-class라는 명령어는 맞지만 텔넷의 적용 대상과 설정 모드를 잘못 제시했다.

다시 나오면 이렇게 판단

문제의 통제 대상이 라우터를 통과하는 패킷인지 라우터 자체의 원격 관리 접속인지 먼저 구별한다. 전자는 인터페이스의 ip access-group, 후자는 VTY 라인의 access-class를 선택한다.

암기 포인트

통과 트래픽은 인터페이스의 ip access-group, 텔넷·SSH 관리 접속은 VTY 라인의 access-class이다.

NoteBase

문 18. 다음 중 VPN 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① IPSec의 ESP는 암호화, AH는 인증기능을 제공한다.

② IPSec의 전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다.

③ PPP를 기반으로 마이크로소프트가 제안한 프로토콜은 PPTP이다.

④ PPTP, L2TP, L2F는 2계층 프로토콜이다.

정답 2번

출제 포인트

IPSec의 전송 모드와 터널 모드의 차이, 그리고 대표적인 2계층 VPN 터널링 프로토콜의 특징을 구별하는 문제이다.

핵심 개념

IPSec는 IP 계층에서 패킷을 보호하는 기술이다. AH는 데이터 무결성과 송신자 인증을 제공하지만 암호화에 의한 기밀성은 제공하지 않고, ESP는 주로 암호화에 의한 기밀성을 제공하며 무결성과 인증 기능도 함께 제공할 수 있다.
전송 모드는 원래 IP 헤더를 유지한 채 그 뒤의 상위 계층 데이터 부분을 보호한다. 터널 모드는 원래 IP 패킷 전체를 캡슐화하고 새로운 외부 IP 헤더를 붙인다.
PPTP, L2TP, L2F는 PPP 프레임을 운반하는 2계층 터널링 프로토콜 계열이다.

선지별 해설

① O — ESP는 대표적으로 암호화를 통한 기밀성을 제공하고, AH는 데이터 무결성과 송신자 인증을 제공하므로 옳다. 다만 ESP도 선택적으로 무결성과 인증 기능을 제공할 수 있다.
② X — 틀린 부분은 '전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다'이다. 전송 모드는 원래 IP 헤더를 그대로 사용하며, 새로운 외부 IP 헤더를 추가하는 것은 터널 모드이다.
③ O — PPTP는 PPP를 기반으로 하여 마이크로소프트가 제안한 터널링 프로토콜이므로 옳다. PPP 프레임을 IP 네트워크를 통해 전달할 수 있도록 캡슐화한다.
④ O — PPTP, L2TP, L2F는 모두 데이터링크 계층의 프레임을 터널링하는 2계층 프로토콜로 분류되므로 옳다.

오답 포인트

②는 전송 모드와 터널 모드의 헤더 구성을 뒤바꾼 선지이다. '새로운 IP 헤더 추가'라는 표현은 원래 패킷 전체를 감싸는 터널 모드의 특징이다. 또한 ①은 ESP를 암호화 전용으로 단정한 문장이 아니라 대표 기능을 대비한 문장이므로 옳게 판단한다.

NoteBase

다시 나오면 이렇게 판단

IPSec 모드는 새 외부 IP 헤더의 유무로 구별한다. 원래 IP 헤더를 유지하면 전송 모드이고, 원래 IP 패킷 전체를 캡슐화한 뒤 새 IP 헤더를 붙이면 터널 모드이다. 프로토콜 계층을 물으면 PPP 프레임을 터널링하는 PPTP·L2TP·L2F는 2계층으로 판단한다.

암기 포인트

전송 모드는 원래 헤더 유지, 터널 모드는 새 외부 헤더 추가이다. AH는 인증·무결성, ESP는 암호화·기밀성이 핵심이다.

NoteBase

문 19. 다음 중 윈도우 또는 리눅스 네트워크 기반 프로그램 설명으로 가장 옳지 않은 것은?

① ipconfig /all 명령으로 컴퓨터의 IP주소, 서브넷 마스크, 기본 게이트웨이 정보를 출력하지만 물리적 주소는 확인할 수 없다.

② ping 명령은 원격 호스트가 정상적으로 운영되고 있는지를 확인하며 ICMP Echo Reply와 ICMP Echo Request를 사용한다.

③ traceroute 명령 실행결과에서 응답시간이 '*'로 표시되는 경우는 보안상의 이유로 차단되었거나 실제 해당 구간에 문제가 발생한 경우로 볼 수 있다.

④ netstat 명령은 TCP/IP 프로토콜 진단 시 다양하게 사용하며 프로토콜, 로컬 주소, 외부 주소, 상태 정보를 출력한다.

정답 1번

출제 포인트

이 문제는 ipconfig, ping, traceroute, netstat 등 네트워크 진단 명령의 기능과 출력 정보를 구별하는 문제이다.

핵심 개념

ipconfig /all은 Windows에서 IP 설정의 상세 정보와 네트워크 어댑터의 물리적 주소(MAC 주소)를 함께 확인하는 명령이다. ping은 ICMP Echo 메시지로 대상 호스트의 응답 여부를 확인하고, traceroute는 목적지까지 거치는 경로와 각 구간의 응답을 추적하며, netstat는 연결·수신 대기 상태와 주소 등의 네트워크 상태를 보여 준다.

선지별 해설

① X — 틀린 표현은 '물리적 주소는 확인할 수 없다'이다. ipconfig /all의 출력에는 IP 주소, 서브넷 마스크, 기본 게이트웨이뿐 아니라 네트워크 어댑터의 물리적 주소(MAC 주소)도 포함된다. 올바르게는 'ipconfig /all 명령으로 물리적 주소도 확인할 수 있다'이다.
② O — ping은 대상 호스트로 ICMP Echo Request를 보내고 ICMP Echo Reply가 돌아오는지를 확인하여 통신 가능 여부와 응답 상태를 진단한다.
③ O — traceroute 실행 결과의 '*'는 제한 시간 안에 응답을 받지 못했다는 뜻이다. 방화벽이나 라우터가 응답을 차단한 경우 또는 해당 구간의 장애·손실 등으로 응답이 오지 않은 경우에 나타날 수 있다.
④ O — netstat는 TCP/IP 연결 상태를 진단하는 명령으로, 대표적으로 프로토콜, 로컬 주소, 외부 주소, 연결 상태 정보를 출력한다.

NoteBase

오답 포인트

①은 ipconfig의 기본 출력과 ipconfig /all의 상세 출력을 혼동하게 만든다. /all 옵션을 붙이면 어댑터의 물리적 주소까지 표시된다는 점이 함정이다. 또한 traceroute의 '*'는 곧바로 특정 구간의 고장을 확정하는 표시가 아니라 응답 시간 초과를 나타낸다.

다시 나오면 이렇게 판단

명령마다 확인 대상을 연결해 판단한다. ipconfig /all은 상세 IP·어댑터 설정, ping은 ICMP 응답 여부, traceroute는 경로별 응답, netstat는 연결과 포트 상태를 확인한다.

암기 포인트

ipconfig /all은 IP 설정과 MAC 주소, ping은 생존 응답, traceroute는 경로, netstat는 연결 상태이다.

NoteBase

문 20. 다음 중 네트워크 기반 보안위협에 대한 설명으로 가장 옳지 않은 것은?

① SYN Flooding 공격은 TCP의 3-way Handshake 취약점을 이용한 공격이다.

② Smurf 공격은 출발지와 목적지의 IP 주소를 공격대상의 IP 주소로 변조하여 전송하며, 자신에게 응답하는 과정을 반복하게 하여 과부하를 유발하는 공격이다.

③ Teardrop 공격을 받을 경우 네트워크 연결이 끊어지거나 블루 스크린 오류화면을 출력하고 시스템이 정지된다.

④ Ping of Death 공격은 아주 작은 조각(Fragment)의 ICMP Ping 패킷을 처리하게 하여 공격 대상 시스템의 성능저하 및 마비를 일으키는 공격이다.

정답 2번

출제 포인트

대표적인 네트워크 기반 서비스 거부 공격이 악용하는 프로토콜의 취약점과 패킷 처리 방식을 구별하는 문제이다.

핵심 개념

SYN Flooding은 TCP 연결 요청만 대량으로 보내 반쯤 열린 연결을 누적시키는 공격이다.
Smurf는 피해자의 IP 주소를 출발지로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답이 피해자에게 집중되게 하는 반사·증폭 공격이다.
Teardrop은 서로 겹치거나 비정상적인 IP 조각을 보내 재조립 과정에서 장애를 일으키는 공격이다.
Ping of Death는 정상 허용 크기를 넘는 ICMP 패킷을 여러 조각으로 보내 재조립 과정에서 시스템 장애를 유발하는 공격이다.

선지별 해설

① O — SYN Flooding은 TCP의 3-way Handshake 과정에서 SYN을 받은 서버가 연결 상태와 자원을 확보한 채 마지막 ACK를 기다리는 점을 악용한다.
② X — 틀린 부분은 '출발지와 목적지의 IP 주소를 모두 공격 대상의 IP 주소로 변조한다'는 설명이다. 실제로는 출발지 IP 주소를 피해자의 주소로 위조하고, 목적지 IP 주소에는 브로드캐스트 주소를 사용하여 여러 호스트의 ICMP Echo Reply가 피해자에게 집중되게 한다.
③ O — Teardrop은 조각의 오프셋을 겹치게 하는 등 비정상적인 IP 단편을 보내 재조립 오류를 일으킨다. 취약한 시스템에서는 연결 중단, 블루 스크린 또는 시스템 정지가 발생할 수 있다.
④ O — Ping of Death는 허용 크기를 초과하는 ICMP Echo 패킷을 작은 조각들로 나누어 보내고, 피해 시스템이 이를 재조립·처리할 때 성능 저하나 마비가 발생하게 한다. 여기서 핵심은 조각 하나의 크기가 아니라 재조립된 전체 패킷이 허용 크기를 초과한다는 점이다.

NoteBase

오답 포인트

②는 Smurf의 '피해자 주소로 출발지 위조'와 '브로드캐스트 주소로 전송'을 모두 피해자 주소로 바꾸어 놓은 함정이다. ④의 '아주 작은 조각'만 보고 틀렸다고 판단하기 쉽지만, Ping of Death의 판단 기준은 조각들이 재조립된 전체 ICMP 패킷의 비정상적인 크기이다.

다시 나오면 이렇게 판단

공격별 핵심 처리 단계를 확인한다. SYN Flooding은 미완료 TCP 연결, Smurf는 피해자 출발지 위조와 브로드캐스트 반사, Teardrop은 조각 오프셋 중첩, Ping of Death는 재조립 후 크기 초과로 구별한다.

암기 포인트

SYN은 반쪽 연결, Smurf는 브로드캐스트 반사, Teardrop은 조각 중첩, Ping of Death는 초대형 Ping의 재조립이다.

NoteBase