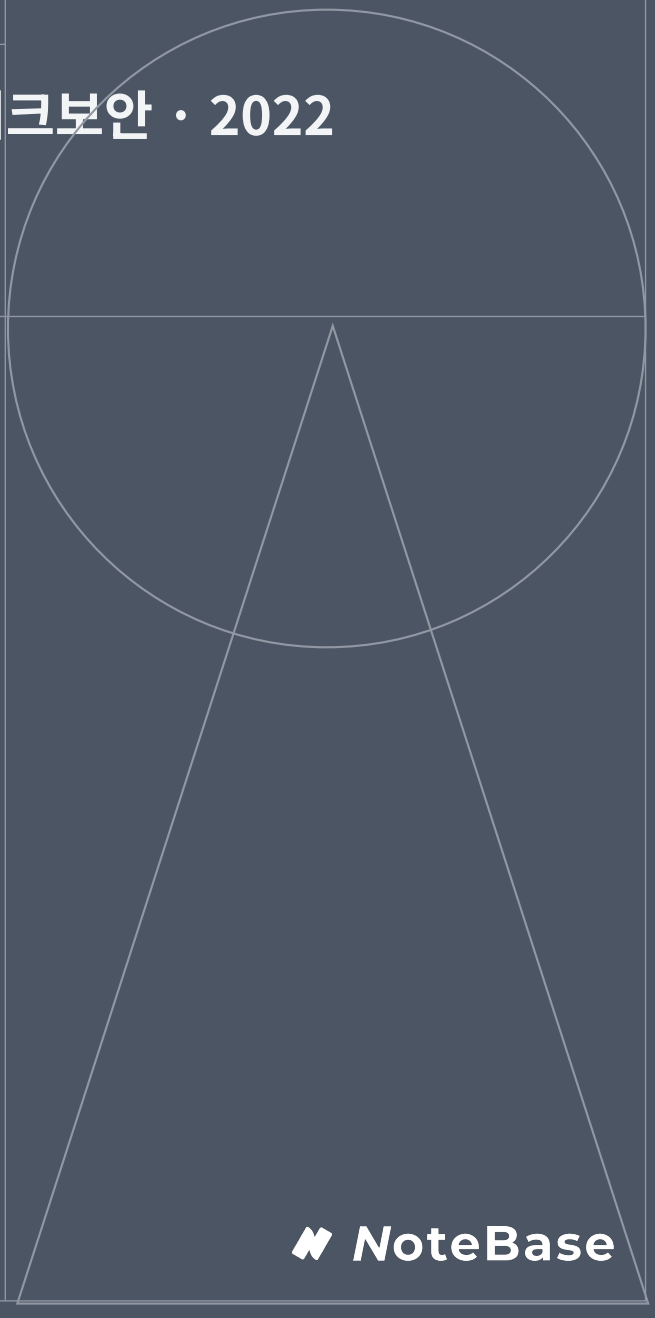
기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2022



NoteBase

기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2022

공무원/군무원/9급 · 네트워크보안 · 2022

1. 다음 중 통합보안관리시스템(Enterprise Security Management)의 특징에 대한 설명으로 가장 옳지 않은 것은?
① 공격의 효과적인 사전 탐지
② 보안 정책의 일관성 유지
③ 통합보안관리 인프라 구축
④ 침해사고에 효과적인 대응

정답 1번

출제 포인트

통합보안관리시스템(ESM)의 핵심 기능이 여러 보안 장비의 정보와 정책을 중앙에서 통합하여 관리·대응하는 것임을 이해하는 문제이다.

핵심 개념

통합보안관리시스템(ESM)은 방화벽, 침입 탐지·방지 시스템 등 여러 보안 장비에서 발생한 이벤트와 로그를 중앙에서 수집·분석하고, 보안 정책과 사고 대응을 통합 관리하는 시스템이다. 핵심 키워드는 통합 관리, 정책의 일관성, 신속한 사고 대응이다.

선지별 해설

① X — '공격의 효과적인 사전 탐지'가 부적절하다. ESM은 각 보안 장비가 생성한 이벤트와 로그를 통합·상관분석하여 이상 징후나 침해사고를 탐지하고 대응하지만, 공격 징후가 발생하기 전에 공격 자체를 미리 예측하는 시스템은 아니다. 올바르게는 '보안 이벤트의 통합 분석을 통한 이상 징후 탐지와 침해사고 대응'이라고 표현한다.
② O — 여러 보안 장비의 정책을 중앙에서 관리하므로 조직 전체에 일관된 보안 정책을 적용하고 유지할 수 있다.
③ O — 서로 다른 보안 솔루션의 로그, 이벤트, 관리 기능을 연계하여 통합보안관리 인프라를 구축할 수 있다.
④ O — 분산된 보안 정보를 한곳에서 분석하고 대응 절차를 연계하므로 침해사고를 신속하고 효과적으로 처리할 수 있다.

NoteBase

오답 포인트

①의 '사전 탐지'를 '신속한 탐지'와 혼동하기 쉽다. ESM은 이미 발생한 보안 이벤트와 이상 징후를 통합 분석하여 탐지·대응하는 데 강점이 있으며, 아무런 징후가 나타나기 전의 공격을 예측하는 기능을 핵심 특징으로 보기는 어렵다.

다시 나오면 이렇게 판단

ESM 관련 선지에서는 '중앙 집중', '로그·이벤트 통합 분석', '정책 일관성', '사고 대응'이면 핵심 특징으로 판단한다. 반면 '공격 발생 전 예측·완전 차단'처럼 ESM 자체의 기능을 지나치게 확장한 표현은 틀린 선지로 판단한다.

암기 포인트

ESM은 여러 보안 장비를 한곳에서 묶어 정책·로그·대응을 통합 관리한다.

NoteBase

2. 침입방지시스템(IPS, Intrusion Prevention System)에 대한 설명으로 가장 옳지 않은 것은?
① 침입에 대한 탐지와 차단기능을 수행한다.
② 탐지영역은 네트워크 계층과 전송계층이다.
③ 침입차단 시스템과 침입방지 시스템의 장점을 결합한 보안 시스템이다.
④ 외부로부터 유입되는 유해한 트래픽을 차단하기 위한 능동형 보안 솔루션이다.

정답 2, 3번

출제 포인트

침입방지시스템(IPS)의 탐지 범위와 구성 개념, 그리고 능동적 차단 기능을 구별하는 문제이다.

핵심 개념

IPS는 네트워크 트래픽을 실시간으로 분석하여 침입을 탐지하고 유해 트래픽을 즉시 차단하는 능동형 보안 시스템이다. 침입탐지시스템(IDS)이 탐지와 경보에 중점을 둔다면, IPS는 탐지 결과에 따라 차단까지 수행한다. 또한 IPS는 네트워크 계층과 전송계층에만 한정되지 않고 응용계층의 공격 패턴도 탐지한다.

선지별 해설

① O — IPS는 침입 징후를 탐지할 뿐 아니라 해당 트래픽을 실시간으로 차단하는 기능도 수행한다.
② X — 틀린 표현은 '탐지영역은 네트워크 계층과 전송계층이다'이다. IPS의 탐지 범위를 두 계층으로만 한정할 수 없으며, 올바르게는 네트워크·전송계층뿐 아니라 응용계층의 공격 패턴도 탐지한다고 해야 한다.
③ X — 틀린 표현은 '침입차단 시스템과 침입방지 시스템의 장점을 결합'이다. 침입방지시스템인 IPS를 다시 구성 요소로 든 순환적 설명이다. 올바르게는 침입차단시스템의 차단 기능과 침입탐지시스템(IDS)의 탐지 기능을 결합한 보안 시스템이라고 해야 한다.
④ O — IPS는 일반적으로 트래픽 경로에 인라인으로 배치되어 외부에서 들어오는 유해 트래픽을 탐지한 뒤 즉시 차단하는 능동형 보안 솔루션이다.

오답 포인트

②는 IPS의 탐지 범위를 네트워크·전송계층으로만 좁힌 점이 함정이다. ③은 '침입방지'와 '침입탐지'가 비슷해 보이지만, IPS의 결합 요소로 들어가야 할 말은 침입탐지시스템(IDS)이다.

다시 나오면 이렇게 판단

IPS 관련 선지는 '탐지만 하는가, 탐지 후 차단까지 하는가'와 '탐지 범위를 특정 하위 계층으로만 제한하는가'를 먼저 확인한다. 결합 개념을 물으면 탐지 기능은 IDS, 차단 기능은 침입차단시스템에 대응시킨다.

NoteBase

암기 포인트

IDS는 탐지·경보, IPS는 탐지·차단이다. IPS의 탐지 범위에는 응용계층도 포함된다.

NoteBase

3. 다음 중 Snort에 대한 설명으로 가장 옳은 것은?
① 실시간 트래픽분석과 IP 네트워크에서의 패킷 처리를 담당하는 공개 소스로 프로토콜 분석, 콘텐츠 검색 및 조합 작업을 할 수 있다.
② 오픈소스 웹 취약점 스캐너로 서버의 취약점을 찾아준다.
③ 비밀번호를 크래킹하는 tool로 망 패킷 스니핑, 사전 공격(dictionary attack) 등의 방법을 사용한다.
④ 수많은 해킹도구와 설명서를 포함한 모의해킹 플랫폼이다.

정답 1번

출제 포인트

Snort의 핵심 기능과 웹 취약점 스캐너, 비밀번호 크래킹 도구, 모의해킹 플랫폼의 기능을 구별하는 문제이다.

핵심 개념

Snort는 네트워크 트래픽을 실시간으로 분석하고 패킷을 검사하여 침입 징후를 탐지하는 오픈 소스 네트워크 침입 탐지·방지 도구이다. 프로토콜 분석과 콘텐츠 검색·조합이 핵심 기능이다.
웹 취약점 스캐너는 웹 서버와 웹 애플리케이션의 알려진 취약점이나 잘못된 설정을 점검한다.
비밀번호 크래킹 도구는 사전 공격, 무차별 대입 등의 방식으로 비밀번호를 추측하거나 복구한다.
모의해킹 플랫폼은 여러 보안 진단·공격 도구와 관련 문서를 묶어 제공하는 운영체제 또는 도구 모음이다.

선지별 해설

① O — 실시간 트래픽 분석과 IP 네트워크의 패킷 처리, 프로토콜 분석, 콘텐츠 검색 및 조합은 Snort의 대표 기능이다.
② X — 틀린 표현은 ‘Snort가 오픈 소스 웹 취약점 스캐너로 서버의 취약점을 찾아준다’는 부분이다. 올바르게는 웹 서버의 취약점과 설정 오류를 점검하는 도구는 Nikto와 같은 웹 취약점 스캐너이고, Snort는 네트워크 트래픽을 감시하여 침입 징후를 탐지한다.
③ X — 틀린 표현은 ‘Snort가 비밀번호를 크래킹하는 도구’라는 부분이다. 올바르게는 망 패킷 스니핑이나 사전 공격 등을 이용한 비밀번호 분석·복구는 비밀번호 크래킹 도구의 기능이고, Snort의 주된 기능은 패킷 기반 침입 탐지이다.
④ X — 틀린 표현은 ‘Snort가 수많은 해킹 도구와 설명서를 포함한 모의해킹 플랫폼’이라는 부분이다.
올바르게는 이러한 설명은 Kali Linux와 같은 모의해킹용 운영체제·플랫폼에 해당하며, Snort는 개별 네트워크 침입 탐지·방지 도구이다.

NoteBase

오답 포인트

②~④는 모두 정보보안 분야에서 사용하는 도구를 설명하지만 대상과 목적이 다르다. 특히 ③의 '패킷 스니핑'이라는 표현만 보고 Snort를 떠올리기 쉽지만, 선지 전체의 목적은 비밀번호 크래킹이므로 Snort의 설명이 아니다.

다시 나오면 이렇게 판단

도구가 무엇을 대상으로 무엇을 하는지 확인한다. 네트워크 패킷 감시·침입 탐지는 Snort, 웹 서버 취약점 점검은 웹 취약점 스캐너, 비밀번호 추측·복구는 크래킹 도구, 여러 모의해킹 도구를 묶은 환경은 모의해킹 플랫폼으로 판단한다.

암기 포인트

Snort는 패킷을 보고 침입을 탐지한다. Nikto는 웹을 점검하고, 비밀번호 크래커는 암호를 추측하며, Kali Linux는 모의해킹 도구 환경이다.

NoteBase

4. 다음 중 DoS(Denial of Service) 공격에 대한 설명으로 가장 옳지 않은 것은?
① 루트권한을 획득하는 공격이다.
② 디스크, 데이터, 시스템을 파괴하는 파괴 공격도 가능하다.
③ 공격의 원인이나 공격자를 추적하기 힘들다.
④ 매우 다양한 방법으로 공격할 수 있다.

정답 1번

출제 포인트

DoS 공격의 목적과 일반적 특징을 구분하고, 공격에 반드시 필요한 조건이 무엇인지 판단하는 문제이다.

핵심 개념

DoS(Denial of Service) 공격은 서버·네트워크·서비스의 자원을 고갈시키거나 정상 동작을 방해하여 정당한 사용자가 서비스를 이용하지 못하게 만드는 공격이다. 핵심은 가용성 침해이며, 관리자 권한인 루트 권한의 획득이 필수 조건은 아니다.

선지별 해설

① X — 틀린 표현은 '루트권한을 획득하는 공격'이다. DoS 공격은 과도한 요청 전송, 취약점 악용, 자원 고갈 등으로 서비스를 중단시키는 공격이며 루트 권한 획득을 반드시 필요로 하지 않는다. 올바르게는 '시스템이나 네트워크의 가용성을 침해하여 정상적인 서비스 이용을 방해하는 공격'이다.
② O — DoS는 단순한 접속 지연이나 자원 고갈뿐 아니라 취약점을 이용해 시스템을 비정상 종료시키거나 디스크·데이터·시스템에 손상을 일으키는 파괴적 형태로도 수행될 수 있다.
③ O — 공격자는 출발지 주소를 위조하거나 여러 경유지·다수의 공격원을 이용할 수 있으므로 공격의 실제 원인과 공격자를 추적하기 어렵다.
④ O — 대량 트래픽 유발, 서비스 요청 폭주, 프로토콜 취약점 악용, 시스템 자원 고갈 등 공격 방법이 매우 다양하다.

오답 포인트

①의 '루트권한 획득'은 시스템 침입 후 권한을 장악하는 공격과 DoS 공격을 혼동하게 만드는 표현이다. DoS의 성립 여부는 권한 탈취가 아니라 정상 사용자의 서비스 이용 가능성을 떨어뜨렸는지로 판단한다.

다시 나오면 이렇게 판단

DoS 관련 선지는 먼저 공격 목표가 기밀성·무결성·가용성 중 무엇인지 확인한다. 서비스 중단·자원 고갈·요청 폭주는 가용성 침해에 해당하며, 루트 권한 획득이나 정보 탈취를 DoS의 필수 조건이라고 하면 틀린 설명이다.

NoteBase

암기 포인트

DoS는 권한 탈취가 아니라 서비스 거부, 즉 가용성 침해이다.

NoteBase

5. 다음은 TCP header Flag에 대한 설명이다. 옳은 것을 모두 고르시오.

> ㉠ URG: TCP가 즉시 이 메시지를 상위계층 프로세스에게 전달할 수 있게 한다.
> ㉡ ACK: Acknowledgment Number가 유효함을 표시한다.
> ㉢ RST: 연결을 Reset하도록 지시하는 Flag.
> ㉣ SYN: 연결시작을 나타내기 위해 사용하는 Flag.
> ㉤ FIN: 연결을 종료하도록 지시하는 Flag.

① ㉠, ㉡, ㉢, ㉣, ㉤
② ㉡, ㉢, ㉣, ㉤
③ ㉢, ㉣, ㉤
④ ㉣, ㉤

정답 2번

출제 포인트

TCP 헤더의 URG, ACK, RST, SYN, FIN 플래그가 각각 어떤 제어 정보를 나타내는지 구분하는 문제이다.

핵심 개념

URG는 긴급 포인터(Urgent Pointer) 필드가 유효함을 나타내며, 데이터 자체를 즉시 상위 계층 프로세스에 전달한다는 뜻은 아니다. ACK는 확인 응답 번호(Acknowledgment Number) 필드가 유효함을 나타낸다. RST는 비정상적이거나 유효하지 않은 연결을 재설정하고, SYN은 연결 설정을 위한 순서 번호 동기화에, FIN은 연결 종료 의사 표시에 사용된다. 따라서 ㄱ은 틀리고 ㄴ, ㄷ, ㄹ, ㅁ은 옳다.

선지별 해설

① X — ㄱ을 포함한 것이 틀렸다. URG는 TCP가 메시지를 즉시 상위 계층 프로세스에 전달하게 하는 플래그가 아니라 긴급 포인터 필드가 유효함을 나타내는 플래그이다. 올바른 조합은 ㄴ, ㄷ, ㄹ, ㅁ이다.
② O — ㄴ의 ACK는 확인 응답 번호의 유효성을, ㄷ의 RST는 연결 재설정을, ㄹ의 SYN은 연결 시작을 위한 동기화를, ㅁ의 FIN은 연결 종료를 각각 나타내므로 모두 옳다.
③ X — 옳은 ㄴ을 빠뜨린 것이 틀렸다. ACK는 Acknowledgment Number가 유효함을 나타내므로 올바른 조합은 ㄴ, ㄷ, ㄹ, ㅁ이다.
④ X — 옳은 ㄴ과 ㄷ을 빠뜨린 것이 틀렸다. ACK는 확인 응답 번호가 유효함을 나타내고 RST는 연결 재설정을 지시하므로 올바른 조합은 ㄴ, ㄷ, ㄹ, ㅁ이다.

NoteBase

오답 포인트

ㄱ의 '즉시 상위계층 프로세스에게 전달'이라는 표현이 함정이다. URG는 즉시 전달 동작 자체가 아니라 긴급 포인터 필드의 유효성을 표시한다. 또한 조합형 문항에서는 옳은 설명을 빠뜨린 ③과 ④도 정답이 될 수 없다.

다시 나오면 이렇게 판단

각 플래그를 필드 유효성 표시와 연결 제어로 나누어 판단한다. URG·ACK는 각각 Urgent Pointer·Acknowledgment Number의 유효성을 표시하고, SYN·FIN·RST는 각각 연결 설정·종료·재설정에 대응한다.

암기 포인트

URG는 긴급 포인터, ACK는 확인 번호, SYN은 시작, FIN은 종료, RST는 재설정이다.

NoteBase

6. 다음 지문은 무엇에 대한 설명인가?

> 사용자 PC를 악성코드에 감염시켜 이용자가 인터넷 '즐겨찾기' 또는 포털사이트 검색을 통하여 금융회사 등의 정상 홈페이지 주소로 접속하여도 가짜 사이트 홈페이지로 유도되어 해커가 금융거래정보 등을 편취하는 수법

① 파밍(Pharming)
② 애드웨어(Adware)
③ 크래킹(Cracking)
④ 백도어 공격(Backdoor Attack)

정답 1번

출제 포인트

정상적인 인터넷 주소로 접속하려는 이용자를 가짜 사이트로 유도하여 금융정보를 빼내는 파밍과 다른 보안 위협의 차이를 묻는 문제이다.

핵심 개념

파밍(Pharming): 악성코드 감염이나 주소 변환 정보의 변조 등을 이용하여 사용자가 정상 주소로 접속해도 가짜 사이트로 이동하게 한 뒤 개인정보나 금융정보를 탈취하는 수법이다. / 키워드: 정상 주소 접속, 가짜 사이트 강제 유도
애드웨어(Adware): 광고를 표시하거나 광고 목적의 정보를 수집하는 프로그램이다. / 키워드: 광고 노출
크래킹(Cracking): 악의적인 목적으로 시스템·계정·보호 장치 등에 무단 침입하거나 보안을 깨뜨리는 행위이다. / 키워드: 보안 침해
백도어 공격(Backdoor Attack): 정상적인 인증 절차를 우회하여 시스템에 몰래 다시 접근할 수 있는 비밀 통로를 이용하는 공격이다. / 키워드: 우회 접근 통로

NoteBase

선지별 해설

① O — 제시문은 PC를 악성코드에 감염시키거나 정상 홈페이지 주소로 접속한 이용자를 가짜 사이트로 돌려 금융계정정보를 빼내는 수법을 설명하므로 파밍이다.
② X — 틀린 표현은 '애드웨어'이다. 애드웨어는 주로 광고를 표시하거나 광고 관련 정보를 수집하는 프로그램이며, 제시문의 수법은 올바르게는 '파밍'이다.
③ X — 틀린 표현은 '크래킹'이다. 크래킹은 악의적으로 시스템이나 계정의 보안을 깨고 무단 침입하는 행위이며, 제시문의 가짜 사이트 유도 수법은 올바르게는 '파밍'이다.
④ X — 틀린 표현은 '백도어 공격'이다. 백도어 공격은 정상 인증을 우회하는 숨은 접근 통로를 이용하는 공격이며, 제시문의 정상 주소 접속자를 가짜 사이트로 보내는 수법은 올바르게는 '파밍'이다.

오답 포인트

'악성코드 감염'이라는 표현만 보고 모든 악성 프로그램이나 무단 침입 공격으로 판단하기 쉽다. 그러나 이 문항의 결정적 단서는 정상 홈페이지 주소로 접속하려는 이용자를 가짜 사이트로 유도하여 금융정보를 탈취한다는 부분이다.

다시 나오면 이렇게 판단

정상 주소를 입력하거나 정상 경로로 접속했는데 가짜 사이트로 강제 이동하면 파밍으로 판단한다. 광고 노출은 애드웨어, 보안 해제·무단 침입은 크래킹, 숨은 우회 통로를 통한 접근은 백도어 공격으로 구분한다.

암기 포인트

파밍은 '정상 주소도 가짜 사이트로', 애드웨어는 '광고', 크래킹은 '보안 깨기', 백도어는 '숨은 통로'이다.

NoteBase

7. 다음 중 표준 이더넷 프레임의 길이에 대한 설명이 가장 옳은 것은?
① 최소 프레임 길이: 64byte,
최소 데이터 길이: 48byte
② 최대 프레임 길이: 1,524byte,
최대 데이터 길이: 1,500byte
③ 최대 프레임 길이: 1,518byte,
최대 데이터 길이: 1,500byte
④ 최소 프레임 길이: 56byte,
최소 데이터 길이: 48byte

정답 3번

출제 포인트

표준 이더넷 프레임에서 헤더와 FCS가 차지하는 길이를 바탕으로 최소·최대 프레임 길이와 데이터 길이를 구분하는 문제이다.

조건 정리

프리앰블과 SFD를 제외한 표준 이더넷 프레임은 목적지 주소 6*byte*, 출발지 주소 6*byte*, 타입/길이 2*byte*, 데이터 46 ~ 1500*byte*, FCS 4*byte*로 구성된다. 따라서 데이터 이외의 고정 길이는 18*byte*이다.

사용할 공식

프레임 길이=헤더 14 byte+데이터 길이+FCS 4 byte
데이터의 최소·최대 길이에 고정 길이 18*byte*를 더하면 프레임의 최소·최대 길이를 구할 수 있다.

계산 과정

최소 프레임 길이는 14 + 46 + 4 = 64*byte*이다.
최대 프레임 길이는 14 + 1500 + 4 = 1518*byte*이다.
따라서 데이터 길이의 범위는 46 ~ 1500*byte*, 프레임 길이의 범위는 64 ~ 1518*byte*이다.

NoteBase

선지 판단

① X — 최소 프레임 길이 64*byte*는 맞지만 '최소 데이터 길이 48*byte*'가 틀렸다. 올바르게는 최소 데이터 길이가 46*byte*이다.
② X — 최대 데이터 길이 1500*byte*는 맞지만 '최대 프레임 길이 1524*byte*'가 틀렸다. 올바르게는 최대 프레임 길이가 1518*byte*이다.
③ O — 최대 데이터 1500*byte*에 헤더와 FCS의 18*byte*를 더하면 최대 프레임 길이는 1518*byte*가 된다.
④ X — '최소 프레임 길이 56*byte*, 최소 데이터 길이 48*byte*'가 모두 틀렸다. 올바르게는 최소 프레임 길이가 64*byte*, 최소 데이터 길이가 46*byte*이다.

오답 포인트

프리앰블과 SFD를 프레임 길이에 포함하거나, 헤더와 FCS의 길이를 잘못 더하면 선지의 수치에 끌리기 쉽다. 이 문항에서 프레임 길이는 프리앰블과 SFD를 제외하고 헤더 14*byte*, 데이터, FCS 4*byte*를 합한 값이다.

다시 나오면 이렇게 판단

먼저 데이터 범위가 46 ~ 1500*byte*임을 확인하고, 양 끝값에 고정 길이 18*byte*를 각각 더해 프레임 범위 64 ~ 1518*byte*를 산출한다.

암기 포인트

이더넷은 데이터 46 ~ 1500*byte*, 프레임 64 ~ 1518*byte*로 기억한다.

NoteBase

8. 다음 지문에 대한 네트워크 공격으로 가장 적절한 것은?

> 공격대상의 주소로 소스 IP 주소를 만들고 임의의 브로드캐스트 주소로 ICMP echo 패킷을 전송하여 스푸핑된 IP 호스트는 ICMP reply 패킷을 동시 다발적으로 수신하여 시스템 부하를 증가시킨다.

① Teardrop
② Land Attack
③ Syn Flooding
④ Smurf Attack

정답 4번

출제 포인트

피해자의 IP 주소로 출발지 주소를 위조한 ICMP echo 패킷을 브로드캐스트 주소로 보내 다수 호스트의 ICMP reply가 피해자에게 집중되게 하는 공격을 식별하는 문제이다.

핵심 개념

Smurf Attack은 피해자의 IP 주소로 출발지 주소를 위조한 ICMP echo 요청을 브로드캐스트 주소로 전송하여, 여러 호스트의 ICMP reply가 피해자에게 몰리게 하는 반사·증폭형 서비스 거부 공격이다.
Teardrop은 비정상적으로 겹치는 IP 단편을 보내 재조립 과정에서 장애를 일으키는 공격이다. Land Attack은 출발지와 목적지의 IP 주소 및 포트 정보를 피해자 자신으로 같게 위조하는 공격이다. SYN Flooding은 다수의 TCP SYN을 보내 연결을 완성하지 않고 반개방 연결을 누적시키는 공격이다.

NoteBase

선지별 해설

① X — Teardrop은 ICMP 브로드캐스트 반사 공격이 아니라, 겹치거나 비정상적인 IP 단편을 전송하여 수신 시스템의 패킷 재조립 과정에 장애를 일으키는 공격이다. 틀린 표현은 'Teardrop'이며, 제시문의 공격은 'Smurf Attack'이다.
② X — Land Attack은 브로드캐스트 주소로 ICMP echo를 보내는 공격이 아니라, 출발지와 목적지의 IP 주소 및 포트를 피해자 자신으로 같게 위조하여 시스템에 부하나 장애를 유발하는 공격이다. 틀린 표현은 'Land Attack'이며, 제시문의 공격은 'Smurf Attack'이다.
③ X — SYN Flooding은 ICMP reply를 피해자에게 집중시키는 공격이 아니라, TCP 3-way handshake에서 SYN 요청을 대량 전송한 뒤 연결을 완료하지 않아 반개방 연결과 대기 자원을 소진시키는 공격이다. 틀린 표현은 'Syn Flooding'이며, 제시문의 공격은 'Smurf Attack'이다.
④ O — Smurf Attack은 피해자의 주소로 출발지 IP를 위조한 ICMP echo 요청을 브로드캐스트 주소로 보내고, 브로드캐스트를 받은 여러 호스트의 ICMP reply가 피해자에게 동시에 전송되도록 한다. 제시문의 공격 구조와 정확히 일치한다.

오답 포인트

네 공격이 모두 서비스 거부를 일으킬 수 있다는 공통점만 보면 혼동하기 쉽다. 이 문항에서는 'ICMP', '출발지 IP 위조', '브로드캐스트', '다수 호스트의 reply'가 함께 제시된 점이 Smurf Attack을 가르는 결정적 단서이다.

다시 나오면 이렇게 판단

브로드캐스트 ICMP 요청에 여러 호스트가 응답하여 피해자에게 트래픽이 증폭되면 Smurf Attack으로 판단한다. IP 단편 재조립은 Teardrop, 출발지와 목적지를 피해자 자신으로 동일하게 위조하면 Land Attack, 미완료 TCP 연결을 누적시키면 SYN Flooding으로 구분한다.

암기 포인트

Smurf는 위조된 피해자 주소로 브로드캐스트 ICMP 요청을 보내 다수의 reply를 피해자에게 반사·증폭한다.

NoteBase

9. 다음 중 분산서비스 거부공격(DDoS, Distributed Denial of Service)의 공격 도구에 해당하지 않는 것은?
① Trinoo Attack
② TFN Attack
③ Targa Attack
④ Stacheldraht

정답 3번

출제 포인트

분산된 다수의 공격 시스템이 하나의 피해 시스템을 공격하는 DDoS 도구와 단일 시스템을 대상으로 하는 DoS 도구를 구별하는 문제이다.

핵심 개념

DDoS 공격 도구는 공격자가 여러 에이전트가 설치된 시스템을 제어하여 하나의 피해 시스템에 대량의 트래픽을 동시에 보내도록 구성한다. Trinoo, TFN, Stacheldraht는 대표적인 DDoS 공격 도구이고, Targa는 여러 종류의 DoS 공격을 실행하는 도구 모음이다.

선지별 해설

① O — Trinoo Attack은 다수의 에이전트를 이용해 피해 시스템에 UDP 플러딩을 가하는 대표적인 DDoS 공격 도구이다.
② O — TFN Attack은 Tribe Flood Network의 약칭으로, 여러 에이전트를 원격 제어해 다양한 플러딩 공격을 수행하는 DDoS 공격 도구이다.
③ X — Targa Attack은 여러 종류의 서비스 거부 공격을 실행하는 DoS 도구 모음으로, 대표적인 분산서비스 거부공격 도구에 해당하지 않는다. 틀린 표현은 ‘DDoS 공격 도구’이며, 올바르게는 ‘여러 DoS 공격을 실행하는 도구 모음’이다.
④ O — Stacheldraht는 여러 에이전트를 제어하여 분산 공격을 수행하는 DDoS 공격 도구이다.

오답 포인트

③의 Targa에도 ‘Attack’이라는 명칭이 붙어 있어 다른 선지와 같은 DDoS 도구로 오인하기 쉽다. 그러나 공격 도구라는 공통점보다 다수의 에이전트를 이용하는 분산 구조인지가 판단 기준이다.

다시 나오면 이렇게 판단

도구 이름을 보면 먼저 Trinoo·TFN·Stacheldraht의 DDoS 도구군을 묶고, 여러 DoS 공격 기법을 모아 둔 Targa를 분리한다. 부정형 문항에서는 이 분류에 속하지 않는 Targa를 선택한다.

NoteBase

암기 포인트

DDoS 3종은 Trinoo·TFN·Stacheldraht, Targa는 DoS 도구 모음이다.

NoteBase

10. 어떤 네트워크 보안 모델은 다음 지문과 같이 5가지 원칙을 기반으로 하고 있다. 해당하는 보안 모델은 무엇인가?

> ㉠ 네트워크의 모든 사용자는 항상 위험하다고 가정
> ㉡ 외부 및 내부 위협이 네트워크에 항상 존재
> ㉢ 네트워크의 신뢰 여부를 결정할 때 네트워크의 위치는 충분하지 않음
> ㉣ 모든 디바이스, 사용자, 네트워크를 인증하고 권한 확인
> ㉤ 최대한 많은 데이터 소스를 기반으로 자동적인 정책 수립

① 경계면 보안
② 엣지 보안
③ 제로 트러스트 보안
④ 공격표면 보안

정답 3번

출제 포인트

이 문제는 네트워크 위치만으로 신뢰하지 않고 모든 접근을 지속적으로 검증하는 제로 트러스트 보안의 원칙을 구별하는 문제이다.

핵심 개념

제로 트러스트 보안은 내부와 외부를 가리지 않고 어떤 사용자·기기·접근도 미리 신뢰하지 않으며, 매 접근마다 인증·인가하고 최소 권한을 적용하는 보안 모델이다. 핵심 키워드는 '절대 신뢰하지 말고 항상 검증한다'이다.
경계면 보안은 내부와 외부의 경계를 중심으로 방화벽 등에서 침입을 차단하고, 엣지 보안은 사용자·기기·서비스와 가까운 네트워크 가장자리의 분산 지점을 보호한다. 공격표면 보안은 공격자가 악용할 수 있는 노출 지점을 식별하고 줄이며 관리하는 데 초점을 둔다.

NoteBase

선지별 해설

① X — 경계면 보안은 내부망과 외부망의 경계를 중심으로 방어하는 모델이다. 제시문처럼 모든 사용자를 잠재적 위험으로 보고 신뢰를 계속 검증하는 모델은 아니다. 틀린 연결은 '다섯 원칙 → 경계면 보안'이며, 올바르게는 '다섯 원칙 → 제로 트러스트 보안'이다.
② X — 엣지 보안은 네트워크 가장자리의 단말·서비스·분산 지점을 보호하는 데 초점을 둔다. 내부·외부를 가리지 않고 위치만으로 신뢰하지 않으며 모든 접근을 인증·인가한다는 제시문의 원칙은 제로 트러스트의 특징이다. 틀린 연결은 '다섯 원칙 → 엣지 보안'이며, 올바르게는 '다섯 원칙 → 제로 트러스트 보안'이다.
③ O — 제로 트러스트는 내부 사용자나 내부 네트워크도 자동으로 신뢰하지 않고, 사용자·기기·접근 요청을 지속적으로 인증·인가한다. 또한 다양한 상황 정보를 바탕으로 정책을 자동 적용한다는 점까지 제시문의 다섯 원칙과 일치한다.
④ X — 공격표면 보안은 외부에 노출되거나 악용될 수 있는 자산·서비스·취약 지점을 식별하고 최소화하는 데 초점을 둔다. 제시된 다섯 원칙 전체를 가리키는 보안 모델은 아니다. 틀린 연결은 '다섯 원칙 → 공격표면 보안'이며, 올바르게는 '다섯 원칙 → 제로 트러스트 보안'이다.

오답 포인트

'네트워크의 모든 사용자는 항상 위험하다'는 표현만 보고 외부 공격을 막는 경계면 보안을 고르기 쉽다. 그러나 ③의 결정적 단서는 '네트워크 위치만으로 신뢰하지 않음'과 '모든 사용자·기기·네트워크를 인증하고 권한을 확인함'이다. 이는 내부망도 자동으로 신뢰하지 않는 제로 트러스트의 원칙이다.

다시 나오면 이렇게 판단

내부·외부 구분 없이 신뢰를 전제로 하지 않고, 매 접근에서 신원·기기·권한을 검증하며, 상황 정보에 따라 정책을 적용한다는 표현이 함께 나오면 제로 트러스트로 판단한다. 경계를 세워 막는다는 표현은 경계면 보안, 네트워크 가장자리 보호는 엣지 보안, 노출 지점의 식별·축소는 공격표면 보안으로 구별한다.

암기 포인트

제로 트러스트는 '위치로 믿지 않고, 매번 검증하며, 필요한 권한만 부여한다'이다.

NoteBase

11. 다음 중 OWASP TOP 10 2021에 새롭게 포함되지 않는 웹 취약점으로 가장 적절한 것은?
① 소프트웨어 및 데이터 무결성 오류 (Software and Data Integrity Failures)
② 안전하지 않은 설계(Insecure Design)
③ 서버 측 요청 위조 (Server-Side Request Forgery)
④ Identification and Authentication Failures (식별 및 인증 오류)

정답 4번

출제 포인트

OWASP Top 10 2021에서 새로 추가된 범주와 기존 범주가 명칭·범위만 바뀐 경우를 구별하는 문제이다. 문제의 부정 표현인 '새롭게 포함되지 않는'을 정확히 확인해야 한다.

핵심 개념

OWASP Top 10은 웹 애플리케이션의 주요 보안 위험을 10개 범주로 정리한 목록이다. 2021판에서 새 범주로 제시된 항목은 '안전하지 않은 설계', '소프트웨어 및 데이터 무결성 오류', '서버 측 요청 위조'이다. 반면 '식별 및 인증 오류'는 종전의 '취약한 인증(Broken Authentication)'을 바탕으로 명칭과 범위를 조정한 범주이므로 새롭게 포함된 항목으로 보지 않는다.

선지별 해설

① X(정답 아님) — '소프트웨어 및 데이터 무결성 오류'는 신뢰할 수 없는 소프트웨어 업데이트, 중요 데이터, CI/CD 파이프라인 등의 무결성 문제를 다루는 2021판의 새 범주이다. 이 선지를 '새롭게 포함되지 않은 항목'으로 판단하면 틀리며, 올바르게는 '2021판에 새롭게 포함된 범주'이다.
② X(정답 아님) — '안전하지 않은 설계'는 설계 단계에서 필요한 보안 통제의 부재나 결함을 다루기 위해 2021판에 새롭게 포함된 범주이다. 이 선지를 '새롭게 포함되지 않은 항목'으로 판단하면 틀리며, 올바르게는 '2021판에 새롭게 포함된 범주'이다.
③ X(정답 아님) — '서버 측 요청 위조(SSRF)'는 서버가 공격자가 조작한 요청을 대신 전송하게 되는 취약점으로, 2021판에 새롭게 포함된 범주이다. 이 선지를 '새롭게 포함되지 않은 항목'으로 판단하면 틀리며, 올바르게는 '2021판에 새롭게 포함된 범주'이다.
④ O(정답) — '식별 및 인증 오류'는 완전히 새로 추가된 범주가 아니라 종전의 '취약한 인증(Broken Authentication)'이 명칭과 범위를 조정한 항목이다. 따라서 '2021판에 새롭게 포함되지 않는 항목'이라는 조건에 맞는다.

NoteBase

오답 포인트

④의 이름이 이전 판과 달라졌다는 이유만으로 새 범주라고 오인하기 쉽다. 명칭 변경과 신규 추가는 다르며, 이 문제에서는 ④가 기존 인증 관련 범주의 개편이라는 점이 함정이다.

다시 나오면 이렇게 판단

2021판의 신규 범주 세 가지인 '안전하지 않은 설계', '소프트웨어 및 데이터 무결성 오류', '서버 측 요청 위조'를 먼저 묶는다. 나머지 선지가 기존 범주의 명칭·범위 조정인지 확인하면 부정형 질문의 답을 고를 수 있다.

암기 포인트

2021 신규 3개는 설계·무결성·SSRF이고, 식별 및 인증 오류는 기존 인증 범주의 개편이다.

NoteBase

12. 기존 IP 기반 인터넷의 주소 고갈 문제를 해결하기 위해 IPv4에서 IPv6로의 전환이 이루어지고 있다.
하지만 인터넷상의 모든 시스템이 IPv4에서 IPv6로 전환하기 위해서는 상당히 많은 시간이 소요된다. 이와 같은 문제를 해결하기 위해, IETF에서 IPv4와 IPv6 시스템 사이에 문제가 없도록 전환을 돕는 전략을 사용하고 있다.
다음 중 이에 해당하지 않는 것은?
① 터널링(tunneling)
② 라우터 간청(router-solicitation)
③ 헤더 변환(header translation)
④ 이중 스택(dual stack)

정답 2번

출제 포인트

IPv4와 IPv6의 공존·전환을 지원하는 기술과 IPv6 내부에서 사용하는 제어 메시지를 구별하는 문제이다.

핵심 개념

터널링은 한 프로토콜의 패킷을 다른 프로토콜의 패킷 안에 캡슐화하여 호환되지 않는 구간을 통과시키는 방식이다.
헤더 변환은 IPv4와 IPv6 사이에서 패킷 헤더를 대응되는 형식으로 바꾸는 방식이다.
이중 스택은 하나의 시스템이 IPv4와 IPv6를 모두 구현하여 상황에 맞는 프로토콜을 사용하는 방식이다.
라우터 간청은 IPv6 호스트가 주변 라우터에 라우터 광고를 보내 달라고 요청하는 ICMPv6 이웃 탐색 메시지이다.

선지별 해설

① O — 터널링은 IPv6 패킷을 IPv4 패킷 안에 캡슐화하는 등의 방법으로 서로 다른 프로토콜 구간을 이어 주므로 전환 전략에 해당한다.
② X — '라우터 간청'은 IPv4/IPv6 전환 전략이라는 분류가 틀렸다. 올바르게는 IPv6 호스트가 라우터 광고를 신속히 받기 위해 보내는 ICMPv6 이웃 탐색 메시지이다. 따라서 '전환을 돕는 전략에 해당하지 않는 것'을 묻는 이 문항의 정답이다.
③ O — 헤더 변환은 IPv4 패킷과 IPv6 패킷 사이의 헤더 형식을 변환하여 한쪽 프로토콜만 사용하는 시스템과의 통신을 돕는 전환 전략이다.
④ O — 이중 스택은 장비가 IPv4와 IPv6를 동시에 지원하게 하여 전환 기간에 두 네트워크와 모두 통신하도록 하는 전략이다.

NoteBase

오답 포인트

②의 영어 표현에 네트워크 용어가 들어 있어 전환 기술처럼 보이는 점이 함정이다. 라우터 간청은 IPv4와 IPv6 사이를 연결하거나 변환하는 기술이 아니라 IPv6에서 라우터 정보를 얻기 위한 메시지이다.

다시 나오면 이렇게 판단

두 프로토콜을 함께 운용하는가, 캡슐화하는가, 서로 변환하는가를 먼저 확인한다. 이에 해당하면 전환 기술이고, IPv6 안에서 라우터 발견이나 주소 설정을 수행하는 메시지라면 전환 기술이 아니다.

암기 포인트

전환은 이중 스택·터널링·변환이고, 라우터 간청은 IPv6의 라우터 발견 메시지이다.

NoteBase

13. ICMP는 발신지 IP주소를 사용하여 오류 메시지를 데이터그램의 발신지로 보낸다. 오류 보고 과정을 단순화하기 위해 ICMP 보고 메시지가 따르는 규칙으로 가장 옳지 않은 것은?
① 현재 호스트(this host) 또는 루프백(loopback)과 같은 특수주소를 가지는 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않는다.
② 처음 단편이 아닌 단편화된 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않는다.
③ 어떤 ICMP 오류 메시지도 ICMP 오류 메시지를 전달하는 데이터그램의 응답으로 생성되지 않는다.
④ 어떤 ICMP 오류 메시지도 유니캐스트 주소를 가진 데이터그램을 위해서 생성되지 않는다.

정답 4번

출제 포인트

ICMP 오류 메시지를 새로 생성하지 않는 경우와 일반적인 유니캐스트 데이터그램에 대해 오류를 보고할 수 있는 경우를 구별하는 문제이다.

핵심 개념

ICMP 오류 메시지는 IP 데이터그램의 처리·전달 중 발생한 문제를 원래 발신지에 알리는 제어 메시지이다. 다만 오류 보고가 연쇄적으로 반복되거나 여러 호스트가 동시에 응답하는 상황을 막기 위해 ICMP 오류 메시지에 대한 응답, 첫 단편이 아닌 단편, 브로드캐스트·멀티캐스트와 같은 비유니캐스트 데이터그램, 발신지를 특정할 수 없는 특수 출발지 주소에 대해서는 새 ICMP 오류 메시지를 생성하지 않는다.

NoteBase

선지별 해설

① O — 현재 호스트(this host)나 루프백(loopback)과 같은 특수 출발지 주소는 정상적인 원격 발신지를 나타내지 않으므로 ICMP 오류 메시지를 돌려보내지 않는다.
② O — 첫 단편이 아닌 후속 단편에는 원래 데이터그램의 상위 계층 헤더가 없을 수 있으므로 ICMP 오류 메시지를 생성하지 않는다.
③ O — ICMP 오류 메시지를 전달하던 데이터그램에 다시 ICMP 오류 메시지로 응답하면 오류 보고가 연쇄적으로 발생할 수 있으므로 생성하지 않는다.
④ X — 틀린 표현은 '유니캐스트 주소를 가진 데이터그램'이다. 일반적인 유니캐스트 데이터그램의 오류는 발신지에 ICMP로 보고할 수 있다. 올바르게는 '브로드캐스트나 멀티캐스트와 같은 비유니캐스트 주소를 가진 데이터그램에 대해서는 ICMP 오류 메시지를 생성하지 않는다'이다.

오답 포인트

④의 '유니캐스트'를 오류 메시지의 전송 방식과 혼동하기 쉽다. ICMP 오류 메시지는 특정 발신지에 돌려보내는 것이 원칙이므로 유니캐스트는 일반적인 오류 보고 대상이고, 응답 폭주 위험이 있는 브로드캐스트·멀티캐스트가 억제 대상이다.

다시 나오면 이렇게 판단

오류에 대한 오류인지, 후속 단편인지, 다수에게 전달되는 비유니캐스트인지, 정상적인 발신지를 특정할 수 없는 특수 주소인지 차례로 확인한다. 이에 해당하면 ICMP 오류 생성을 억제하고, 정상적인 유니캐스트 데이터그램이라는 이유만으로는 억제하지 않는다.

암기 포인트

ICMP 오류 억제는 '오류에 오류 금지, 후속 단편 금지, 비유니캐스트 금지, 특수 출발지 금지'이다.

NoteBase

14. 다음 중 IPSec의 전송모드에 대한 설명으로 가장 옳은 것은?
① IP패킷 전체를 보호한다.
② IP헤더를 보호하지 않으며 전송층에서 발송한 정보만 보호한다.
③ IP패킷 전체를 보호한 후에 새로운 IP헤더를 추가한다.
④ 전송층에서 온 정보에 IP헤더만 추가하고 IPSec헤더를 나중에 추가한다.

정답 2번

출제 포인트

IPSec의 전송모드와 터널모드를 보호 범위와 IP 헤더 처리 방식으로 구분하는 문제이다.

핵심 개념

전송모드: 원래 IP 헤더는 유지하고 그 뒤의 전송계층 페이로드를 보호하는 방식이다. 키워드는 '원래 IP 헤더 유지, 페이로드 보호'이다.
터널모드: 원래 IP 패킷 전체를 보호 대상으로 캡슐화하고 바깥에 새로운 IP 헤더를 붙이는 방식이다. 키워드는 '패킷 전체 캡슐화, 새 IP 헤더 추가'이다.

선지별 해설

① X — 'IP패킷 전체를 보호한다'는 부분이 틀렸다. 전송모드는 원래 IP 헤더를 유지한 채 그 뒤의 페이로드를 보호하며, IP 패킷 전체를 캡슐화해 보호하는 것은 터널모드이다.
② O — 전송모드는 원래 IP 헤더를 새로 캡슐화해 보호 범위에 넣지 않고, 그 뒤의 전송계층 페이로드를 보호한다. 전송모드의 보호 범위를 가장 알맞게 설명한다.
③ X — 'IP패킷 전체를 보호한 후 새로운 IP헤더를 추가한다'는 설명은 전송모드가 아니라 터널모드이다. 전송모드는 원래 IP 헤더를 유지하고 그 뒤에 IPSec 헤더를 삽입해 페이로드를 보호한다.
④ X — 'IP헤더만 추가하고 IPSec헤더를 나중에 추가한다'는 순서가 틀렸다. 전송모드의 기본 구조는 원래 IP 헤더 뒤에 IPSec 헤더가 놓이고, 그 뒤에 보호되는 전송계층 페이로드가 이어지는 형태이다.

오답 포인트

①과 ③은 터널모드의 특징인 'IP 패킷 전체 보호'와 '새 IP 헤더 추가'를 전송모드의 특징처럼 제시한 함정이다.
④는 헤더의 배치 순서를 뒤섞은 선택지이다.

NoteBase

다시 나오면 이렇게 판단

원래 IP 헤더를 유지하고 페이로드를 보호하면 전송모드이고, 원래 IP 패킷 전체를 캡슐화한 뒤 새 IP 헤더를 붙이면 터널모드로 판단한다.

암기 포인트

전송모드는 원래 IP 헤더 유지, 터널모드는 패킷 전체 캡슐화와 새 IP 헤더 추가이다.

NoteBase

15. 다음 중 전자우편용 보안서비스인 S/MIME (Secure/Multiple Internet Mail Extension) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?
① MIME 프로토콜에 보안성을 강화한 프로토콜이다.
② ASCII 코드로된 메시지만 전송할 수 있다.
③ MIME에 기밀성과 무결성 같은 보안서비스를 위해 암호메시지구문(CMS, Cryptography Message Syntax)을 정의한다.
④ 암호알고리즘으로는 대칭암호와 비대칭암호를 모두 사용할 수 있다.

정답 2번

출제 포인트

이 문제는 MIME의 메시지 표현 기능과 S/MIME의 보안 기능을 구분할 수 있는지를 묻는다.

핵심 개념

MIME은 전자우편에서 비ASCII 문자, 이미지, 오디오 등 다양한 형식의 데이터를 전송할 수 있도록 메시지 형식과 인코딩 방식을 확장한 표준이다.
S/MIME은 MIME 형식의 메시지에 전자서명과 암호화를 적용하여 무결성, 송신자 인증, 부인방지, 기밀성 등의 보안 기능을 제공하는 규격이다.
CMS는 암호화·전자서명된 메시지의 구문을 정의하며, 대칭키 암호는 주로 본문 암호화에, 공개키 암호는 세션키 전달이나 전자서명에 사용된다.

선지별 해설

① O — S/MIME은 MIME 메시지에 암호화와 전자서명 기능을 추가하여 전자우편의 보안성을 강화한 프로토콜이다.
② X — 틀린 표현은 ‘ASCII 코드로 된 메시지만 전송할 수 있다’이다. 올바르게는 MIME이 비ASCII 문자와 이미지·오디오 같은 바이너리 데이터도 전송할 수 있도록 적절한 형식으로 표현하고 인코딩한다.
③ O — S/MIME은 기밀성과 무결성 등의 보안 서비스를 구현하기 위해 CMS를 사용하며, CMS는 암호화 또는 전자서명된 메시지의 구문을 정의한다.
④ O — S/MIME에서는 대칭키 암호와 비대칭키 암호를 모두 사용할 수 있다. 일반적으로 대칭키 암호는 메시지 본문을 효율적으로 암호화하고, 비대칭키 암호는 세션키 전달과 전자서명에 활용된다.

NoteBase

오답 포인트

②는 초기 전자우편 전송 체계가 주로 ASCII 기반이었다는 사실을 MIME 자체의 한계로 바꾸어 놓았다. MIME은 오히려 그 한계를 보완하여 비ASCII 문자와 다양한 멀티미디어 데이터를 전송할 수 있게 한 표준이다.

다시 나오면 이렇게 판단

MIME은 '다양한 콘텐츠의 표현과 전송', S/MIME은 'MIME 콘텐츠의 암호화와 전자서명'으로 구분한다.
'MIME은 ASCII만 전송한다'는 표현이 나오면 MIME의 도입 목적과 반대이므로 틀린 설명으로 판단한다.

암기 포인트

MIME은 형식 확장, S/MIME은 보안 확장이다.

NoteBase

16. 다음 중 SSL/TLS에서 사용하는 4가지 프로토콜을 나열한 것으로 가장 옳은 것은?

① Authentication Header, ClientKeyExchange, Peer Certificate, Alert
② Authentication Header, SessionID, Handshake, Peer Certificate
③ SessionID, Record, ClientkeyExchange, ChangeCipherSpec
④ Record, Handshake, ChangeCipherSpec, Alert

정답 4번

출제 포인트

SSL/TLS를 구성하는 프로토콜과 핸드셰이크 과정에서 쓰이는 개별 메시지·필드를 구별하는 문제이다.

핵심 개념

SSL/TLS의 주요 프로토콜은 Record, Handshake, ChangeCipherSpec, Alert이다. Record는 데이터를 레코드 단위로 처리·보호하고, Handshake는 보안 매개변수 협상과 인증 및 키 교환을 수행한다. ChangeCipherSpec은 협상된 암호 사양을 이후 통신에 적용한다는 전환을 알리고, Alert는 오류나 연결 종료 등의 상태를 전달한다. 반면 ClientKeyExchange는 Handshake 프로토콜의 메시지이고, SessionID는 세션을 식별하는 필드이며, Peer Certificate는 상대방의 인증서이다. Authentication Header는 SSL/TLS가 아니라 IPsec에서 사용하는 프로토콜이다.

선지별 해설

① X — Alert만 SSL/TLS의 주요 프로토콜에 해당한다. Authentication Header는 IPsec 프로토콜이고, ClientKeyExchange는 Handshake 메시지이며, Peer Certificate는 상대방 인증서이다. 올바르게는 Record, Handshake, ChangeCipherSpec, Alert이다.
② X — Handshake만 SSL/TLS의 주요 프로토콜에 해당한다. Authentication Header는 IPsec 프로토콜이고, SessionID는 세션 식별 필드이며, Peer Certificate는 상대방 인증서이다. 올바르게는 Record, Handshake, ChangeCipherSpec, Alert이다.
③ X — Record와 ChangeCipherSpec은 SSL/TLS의 주요 프로토콜이지만, SessionID는 필드이고 ClientKeyExchange는 Handshake 메시지이다. 올바르게는 Record, Handshake, ChangeCipherSpec, Alert이다.
④ O — Record, Handshake, ChangeCipherSpec, Alert는 모두 SSL/TLS에서 사용하는 주요 프로토콜이다.

NoteBase

오답 포인트

ClientKeyExchange, SessionID, Peer Certificate도 SSL/TLS 통신에서 등장하므로 모두 독립된 프로토콜처럼 보이게 만든 것이 함정이다. 이들은 각각 Handshake 메시지, 세션 식별 필드, 인증서라는 점에서 프로토콜 계층의 네 구성요소와 구별된다.

다시 나오면 이렇게 판단

보기의 용어를 프로토콜, 메시지, 필드, 인증서로 먼저 분류한다. 네 프로토콜인 Record·Handshake·ChangeCipherSpec·Alert만 모인 보기를 정답으로 판단한다.

암기 포인트

SSL/TLS의 네 프로토콜은 레코드-핸드셰이크-암호사양변경-경고, 즉 Record-Handshake-ChangeCipherSpec-Alert이다.

NoteBase

17. 데이터를 전용선(leased line)으로 전송하면 보안적 측면이나 속도면에서 좋지만 회선 사용료가 고가이며, 미사용 시간이 길어 대역폭 낭비가 발생할 수 있다. 다음 중 대안으로 가장 적합한 기술은 무엇인가?
① OSPF(Open Shortest Path First)
② EIGRP(Enhanced Interior Gateway Routing Protocol)
③ 가상사설망(VPN, Virtual Private Network)
④ 가상랜(VLAN, Virtual LAN)

정답 3번

출제 포인트

전용선의 보안성과 통신 기능을 유지하면서 높은 회선 사용료와 긴 미사용 시간이라는 단점을 줄일 수 있는 대체 기술을 구별하는 문제이다.

핵심 개념

전용선은 두 지점을 전용 회선으로 상시 연결하여 안정성과 보안성이 높지만 비용이 크다. VPN은 인터넷과 같은 공용망 위에 인증·암호화된 가상 통신 경로를 구성하여 전용망과 유사한 사설 통신 환경을 제공한다. OSPF와 EIGRP는 네트워크 내부의 경로를 정하는 라우팅 프로토콜이고, VLAN은 하나의 물리적 LAN을 논리적으로 분리하는 기술이다.

선지별 해설

① X — OSPF는 링크 상태 정보를 이용해 최단 경로를 계산하는 내부 게이트웨이 라우팅 프로토콜이다. 틀린 부분은 OSPF를 전용선의 대안으로 본 점이며, 올바르게는 OSPF는 패킷의 전달 경로를 결정하는 기술이다.
② X — EIGRP는 메트릭을 바탕으로 네트워크 내부의 최적 경로를 선택하는 라우팅 프로토콜이다. 틀린 부분은 EIGRP를 회선 비용 절감용 전용망 대체 기술로 본 점이며, 올바르게는 EIGRP는 라우터 사이에서 경로 정보를 교환하는 기술이다.
③ O — VPN은 공용망을 이용하되 인증과 암호화로 보호되는 가상 터널을 구성한다. 별도의 전용 회선을 계속 임차하지 않고도 지점 간 사설 통신을 구현할 수 있으므로 제시된 문제의 가장 적합한 대안이다.
④ X — VLAN은 스위치 기반 LAN을 논리적인 브로드캐스트 도메인으로 나누어 망을 분리하는 기술이다. 틀린 부분은 VLAN을 원격 지점 간 전용선의 대안으로 본 점이며, 올바르게는 VLAN은 주로 동일한 LAN 환경에서 논리적 네트워크 분리와 트래픽 관리를 수행한다.

NoteBase

오답 포인트

OSPF·EIGRP·VPN·VLAN이 모두 네트워크 기술이라는 점이 함정이다. 그러나 ①·②는 경로 선택, ④는 LAN의 논리적 분리 기술이고, ③만 공용망을 이용해 전용망과 유사한 지점 간 보안 통신을 구성한다.

다시 나오면 이렇게 판단

전용선의 대안을 묻는 경우에는 원격 지점 간 연결, 보안 통신, 비용 절감의 세 조건을 함께 확인한다. 공용망 위에 암호화된 사설 통신 경로를 만드는 기술이면 VPN으로 판단한다.

암기 포인트

OSPF·EIGRP는 경로 선택, VLAN은 LAN 분리, VPN은 공용망 위의 가상 사설망이다.

NoteBase

18. 다음 중 HTTPS를 활성화 하면 데이터는 대칭암호 시스템으로 전송하게 되는데 송신자와 수신자가 이 대칭키를 공유하는 안전한 방법에 대한 설명으로 가장 옳지 않은 것은?
① 공개키 암호화 방식으로 대칭키를 공유한다.
② 송신자인 브라우저는 서버의 공개키로 대칭키를 암호화해서 서버로 송신한다.
③ 송신자와 수신자가 확보한 공유 대칭키로 메시지를 암호화하여 상호 간에 전송한다.
④ 서버는 인증기관의 공개키로 송신자가 보내준 공인인증서를 복호화하여 대칭키를 확보한다.

정답 4번

출제 포인트

HTTPS에서 공개키 암호가 담당하는 서버 인증·키 교환과 대칭키 암호가 담당하는 실제 데이터 암호화를 구분하는 문제이다.

핵심 개념

공개키 암호 방식: 서로 미리 비밀키를 공유하지 않아도 서버 인증과 세션키 수립을 안전하게 수행하도록 돕는 방식이다.
대칭키 암호 방식: 송신자와 수신자가 같은 세션키를 사용하여 실제 통신 데이터를 빠르게 암호화·복호화하는 방식이다.
공인인증서: 서버의 신원과 서버 공개키를 인증기관의 전자서명으로 연결한 문서이다. 인증서는 대칭키를 담아 서버에 전달하는 수단이 아니다.

선지별 해설

① O — HTTPS는 공개키 암호 기술을 이용하여 통신 상대를 인증하고 안전하게 대칭형 세션키를 수립한 뒤, 실제 데이터 통신에는 그 대칭키를 사용한다.
② O — 문항이 전제한 전통적인 RSA 키 교환 모형에서는 브라우저가 서버 인증서에서 얻은 서버 공개키로 키 재료를 암호화하여 서버에 보내고, 서버만 자신의 개인키로 이를 처리할 수 있다. 따라서 대칭키를 안전하게 공유하는 설명에 해당한다.
③ O — 송신자와 수신자가 확보한 동일한 세션 대칭키로 이후 메시지를 암호화하여 주고받는 것은 HTTPS의 하이브리드 암호 방식에 부합한다.
④ X — 틀린 표현은 '서버가 인증기관의 공개키로 인증서를 복호화하여 대칭키를 확보한다'이다. 올바르게는 브라우저가 인증기관의 공개키를 이용해 서버 인증서의 전자서명을 검증하고 서버의 신원과 공개키를 확인하며, 세션 대칭키는 별도의 키 교환 절차를 통해 수립한다. 서버 인증서에서 대칭키를 복호화해 얻는 것이 아니다.

NoteBase

오답 포인트

④는 ‘인증기관의 공개키’, ‘서버 인증서’, ‘대칭키’라는 관련 용어를 한 문장에 섞어 놓았다. 인증기관의 공개키는 인증서의 전자서명을 검증하는 데 쓰이며, 인증서 자체를 복호화하여 세션 대칭키를 꺼내는 데 쓰이지 않는다.

다시 나오면 이렇게 판단

인증기관의 공개키가 나오면 먼저 인증서 서명 검증을 떠올리고, 서버 공개키·개인키가 나오면 서버 인증과 키 교환을, 공유된 대칭키가 나오면 실제 데이터 암호화를 판단한다. 인증서에서 대칭키를 직접 얻는다는 설명은 틀린 것으로 본다.

암기 포인트

CA 공개키는 인증서 검증, 서버 키 쌍은 인증·키 교환, 세션 대칭키는 데이터 암호화에 사용된다.

NoteBase

19. 다음 중 커버로스(Kerberos)에 대한 설명으로 가장 옳은 것은?

① 네트워크 그룹을 이동시켜야 할 때 물리적 장비를 옮기는 과정 없이 스위치 설정만으로 조정할 수 있게 하는 서비스이다.

② 네트워크를 구성하는 LAN 내의 장비 간에 원활한 패킷 전송을 위한 서비스이다.

③ 네트워크상에서 키를 분배하고 사용자를 인증하는 서비스이다.

④ 네트워크 내의 데이터 무결성을 보장하기 위한 해시함수 중의 하나이다.

정답 3번

출제 포인트

이 문제는 커버로스의 핵심 기능인 키 분배와 사용자·서비스 인증을 다른 네트워크 기술의 기능과 구별하는 문제이다.

핵심 개념

커버로스(Kerberos)는 신뢰할 수 있는 인증 서버가 대칭키 기반의 티켓과 세션 키를 발급하여 네트워크 사용자와 서비스를 인증하는 프로토콜이다. 비밀번호를 네트워크로 직접 반복 전송하지 않고 티켓을 이용한다는 점이 핵심이다.

NoteBase

선지별 해설

① X
틀린 표현은 '물리적 장비를 옮기는 과정 없이 스위치 설정만으로 네트워크 그룹을 이동시킨다'는 기능을 커버로스의 기능으로 본 부분이다. 이는 논리적으로 네트워크를 분할하고 포트의 소속을 바꾸는 VLAN의 설명이며, 커버로스는 사용자와 서비스를 인증한다.

② X
틀린 표현은 'LAN 내 장비 간의 원활한 패킷 전송을 위한 서비스'이다. LAN에서 프레임을 전달하는 기능은 이더넷과 스위칭 기술에 해당하며, 커버로스는 패킷 전달이 아니라 티켓 기반 인증과 키 분배를 담당한다.

③ O
커버로스는 키 분배 센터를 중심으로 티켓과 세션 키를 제공하고, 이를 이용하여 사용자와 네트워크 서비스를 인증한다. 커버로스의 핵심 목적을 정확히 설명한 선지이다.

④ X
틀린 표현은 커버로스를 '데이터 무결성을 보장하기 위한 해시함수'라고 한 부분이다. 해시함수는 입력 데이터의 해시값을 계산하여 변조 여부를 확인하는 데 이용되지만, 커버로스는 해시함수가 아니라 티켓 기반 네트워크 인증 프로토콜이다.

오답 포인트

①의 VLAN, ②의 LAN 스위칭, ④의 해시함수는 모두 네트워크·보안 분야의 용어이지만 기능이 서로 다르다. 커버로스의 식별어는 '티켓', '키 분배', '인증'이다.

다시 나오면 이렇게 판단

선지에서 인증 서버, 티켓, 세션 키, 사용자·서비스 인증이 함께 제시되면 커버로스로 판단한다. 논리적 네트워크 분리는 VLAN, 프레임 전달은 스위칭, 데이터 변조 확인은 해시함수로 구별한다.

암기 포인트

커버로스는 '티켓으로 인증하고 세션 키를 나누는 프로토콜'이다.

NoteBase

20. 다음 중 네트워크 접근에서 서버에 접근하는 요청으로부터 보안을 강화하는 방법에 대한 설명으로 가장 거리가 먼 것은?

① DNS 서버를 활용해 접근 제어를 강화하는 방식으로 IP주소를 할당한다.

② 가상랜(VLAN)을 활용해 접근 요청자에 대한 보안요구 사항에 따라 어떤 가상랜에 접근을 허가할지 결정한다.

③ 침입차단시스템(Firewall)을 이용해 네트워크 내부와 외부 사이의 트래픽을 허가하거나 거절하는 방식으로 접근을 강화한다.

④ IEEE 802.1X의 확장인증 프로토콜로 인증 절차를 수행한다.

정답 1번

출제 포인트

서버 접근 요청의 보안을 강화하는 접근통제 기술과 DNS·DHCP·VLAN·방화벽·IEEE 802.1X의 역할을 구별하는 문제이다.

핵심 개념

DNS는 도메인 이름과 IP 주소를 대응시키는 이름 해석 서비스이며, IP 주소를 자동으로 할당하는 기능은 DHCP가 담당한다.
VLAN은 하나의 물리적 네트워크를 논리적으로 분리하여 사용자나 보안 정책에 따라 통신 범위를 나눌 수 있다.
방화벽은 정해진 보안 정책에 따라 네트워크 사이의 트래픽을 허용하거나 차단한다.
IEEE 802.1X는 네트워크 접속 전에 사용자나 단말을 인증하는 포트 기반 네트워크 접근통제 기술이다.

NoteBase

선지별 해설

① X — 틀린 표현은 'DNS 서버를 활용해 접근 제어를 강화하는 방식으로 IP 주소를 할당한다'이다. DNS는 이름을 IP 주소로 해석하는 서비스이지 IP 주소를 할당하는 접근통제 기술이 아니다. 올바르게는 DHCP 서버가 단말에 IP 주소를 자동으로 할당하며, 별도의 인증·접근통제 기술이 접속 권한을 판단한다. 따라서 보안 강화 방법에 대한 설명으로 가장 거리가 멀다.
② O — VLAN을 이용하면 사용자의 소속이나 보안 요구 수준에 따라 논리적 네트워크를 분리하고, 허용된 VLAN에만 접속하도록 정책을 적용할 수 있다.
③ O — 방화벽은 내부망과 외부망 사이를 지나는 트래픽을 규칙에 따라 허용하거나 거부하므로 대표적인 네트워크 접근통제 수단이다.
④ O — IEEE 802.1X는 EAP 기반 인증 절차를 이용하여 인증된 사용자나 단말에만 네트워크 접속을 허용하는 방식이므로 접근 보안을 강화한다.

오답 포인트

①의 'IP 주소'라는 표현만 보고 DNS를 연상하기 쉽지만, DNS는 주소를 배정하지 않고 이름을 주소로 변환한다. IP 주소 자동 할당은 DHCP의 역할이라는 구분이 핵심이다.

다시 나오면 이렇게 판단

각 기술의 핵심 동사를 확인한다. DNS는 이름을 해석하고, DHCP는 IP 주소를 할당하며, VLAN은 망을 논리적으로 분리하고, 방화벽은 트래픽을 허용·차단하며, IEEE 802.1X는 접속 전에 인증한다.

암기 포인트

DNS는 이름 해석, DHCP는 IP 할당, VLAN은 논리적 분리, 방화벽은 트래픽 통제, 802.1X는 접속 인증이다.

NoteBase

21. 다음 중 네트워크 명령어 traceroute에 대한 설명으로 가장 옳지 않은 것은?
① 지정한 호스트까지의 경로를 조사한다.
② 네트워크 장애 시, 어느 라우터에 문제가 발생했는지 확인한다.
③ TCP 시간초과 메시지 및 TCP 포트 도달 불가 오류 메시지를 이용해 구현한다.
④ Windows 명령어는 tracert이고, Linux 명령어는 traceroute이다.

정답 3번

출제 포인트

traceroute의 용도와 동작 원리, 운영체제별 명령어 이름을 구분하는 문제이다.

핵심 개념

traceroute는 패킷의 TTL을 단계적으로 증가시키면서 각 홉의 라우터가 보내는 ICMP 시간 초과 메시지 등을 수집하여 목적지까지의 경로를 확인하는 명령어이다. 핵심 구분은 경로 추적에 활용되는 오류·응답 메시지가 TCP가 아니라 ICMP라는 점이다.

선지별 해설

① O — traceroute는 지정한 목적지 호스트까지 패킷이 거치는 라우터, 즉 홉의 경로를 조사한다.

② O — 각 홉의 응답과 응답이 끊기는 위치를 확인할 수 있으므로 네트워크 장애가 의심되는 라우터 구간을 파악하는 데 활용한다.

③ X — 틀린 표현은 'TCP 시간초과 메시지 및 TCP 포트 도달 불가 오류 메시지'이다. traceroute는 TTL 만료 시 라우터가 보내는 ICMP 시간 초과 메시지와 목적지 측의 ICMP 도달 불가 메시지 또는 ICMP 응답 등을 이용하여 경로를 확인한다. 따라서 'ICMP 메시지를 이용해 구현한다'로 고쳐야 한다.

④ O — Windows에서는 tracert, Linux를 비롯한 유닉스 계열에서는 traceroute라는 명령어를 사용한다.

오답 포인트

③은 탐색용 패킷의 전송 방식이나 포트라는 말에 끌려 응답 메시지까지 TCP라고 착각하게 만든다. 경로 중간 라우터의 TTL 만료 통지는 ICMP 메시지라는 점이 판단의 핵심이다.

NoteBase

다시 나오면 이렇게 판단

traceroute 선지는 ‘TTL을 단계적으로 증가시킨다 → 각 라우터가 ICMP 시간 초과 메시지를 보낸다 → 홉별 경로가 드러난다’의 흐름으로 판단한다. 명령어 이름은 Windows의 tracert와 Linux의 traceroute로 구분한다.

암기 포인트

traceroute는 TTL과 ICMP로 홉을 추적하며, Windows 명령어는 tracert이다.

NoteBase

22. 다음 중 HTTPS를 사용해서 암호화하는 통신 요소를 나열한 것에서 가장 옳지 않은 것은?
① 서버의 공개키 인증서
② 브라우저와 서버 간의 쿠키
③ HTTP 헤더 내용
④ 요청한 URL

정답 1번

출제 포인트

HTTPS에서 암호화되는 HTTP 요청·응답 데이터와 공개를 전제로 교환되는 서버 인증서를 구분하는 문제이다.

핵심 개념

HTTPS는 HTTP 메시지를 TLS로 보호하여 브라우저와 서버 사이에서 전송되는 요청·응답의 내용을 암호화한다. 따라서 쿠키, HTTP 헤더, URL의 경로와 질의 문자열은 보호 대상이다. 반면 서버의 공개키 인증서는 서버의 신원과 공개키를 전달하기 위한 공개 정보이므로 비밀로 숨겨야 하는 HTTP 데이터에 해당하지 않는다.

선지별 해설

① X — 서버의 공개키 인증서는 서버의 신원과 공개키를 클라이언트에 알리기 위한 공개 정보이다. ‘HTTPS로 암호화되는 통신 요소’라는 표현이 틀렸으며, 올바르게는 ‘서버 인증서는 TLS 연결에서 서버 인증과 키 교환에 사용되는 공개 정보’이다.
② O — 브라우저가 서버에 보내는 쿠키는 HTTP 요청 헤더에 포함되므로 HTTPS 연결에서는 TLS로 암호화되어 전송된다.
③ O — 요청·응답 헤더를 포함한 HTTP 메시지 내용은 HTTPS의 TLS 보호 대상이다.
④ O — 요청한 URL 가운데 경로와 질의 문자열은 HTTP 요청에 포함되므로 암호화된다. 다만 접속 대상의 도메인 정보까지 언제나 모두 숨겨진다는 뜻은 아니다.

오답 포인트

‘HTTPS를 사용하면 접속과 관련된 모든 정보가 비공개가 된다’고 생각하기 쉽다. 이 문항에서는 공개를 전제로 한 서버 인증서와 TLS 내부에서 전달되는 HTTP 데이터인 쿠키·헤더·URL 경로를 구분해야 한다.

다시 나오면 이렇게 판단

HTTP 요청·응답 안에 들어가는 쿠키, 헤더, URL 경로는 암호화 대상으로 판단한다. 서버의 신원을 확인하도록 제시되는 공개키 인증서는 공개 정보로 판단한다.

NoteBase

암기 포인트

HTTPS는 HTTP 내용은 숨기고, 서버 인증서는 신원 확인을 위해 제시한다.

NoteBase

23. 다음 중 침입탐지시스템에 활용하는 기법으로 임계값 탐지와 프로파일 기반 변형 탐지를 활용하는 탐지 방법을 가장 적절하게 설명한 것은?
① 규칙기반 탐지(Rule-based Detection)
② 통계적 변형 탐지(Statistical Anomaly Detection)
③ 감사 기록 탐지(Audit Record Detection)
④ 분산 침입 탐지(Distributed Intrusion Detection)

정답 2번

출제 포인트

침입 탐지 기법 가운데 임계값 탐지와 프로파일 기반 변형 탐지를 사용하는 방식을 구별하는 문제이다.

핵심 개념

통계적 변형 탐지는 정상 활동의 통계적 기준이나 프로파일을 만들고, 실제 활동이 그 기준에서 벗어나는 정도를 이용해 이상을 탐지하는 방식이다. 임계값 탐지는 일정 기간의 사건 횟수나 값이 설정된 한계를 넘는지를 보고, 프로파일 기반 탐지는 정상 행동 프로파일과 현재 행동의 차이를 비교한다. 반면 규칙 기반 탐지는 알려진 공격의 규칙·패턴과 일치하는지를 판단한다.

선지별 해설

① X — 규칙 기반 탐지는 알려진 공격의 규칙이나 시그니처와 관측된 행위를 대조하는 방식이다. 틀린 표현은 '규칙 기반 탐지'이며, 임계값 탐지와 프로파일 기반 변형 탐지를 활용하는 방식은 '통계적 변형 탐지'이다.
② O — 통계적 변형 탐지는 임계값을 초과하는 비정상 활동을 찾거나 정상 프로파일과 다른 행동을 탐지하므로 문제의 설명과 일치한다.
③ X — 감사 기록은 시스템 활동을 남긴 기록으로서 침입 탐지의 분석 자료가 될 수 있지만, 임계값 탐지와 프로파일 기반 변형 탐지를 포괄하는 분석 방식의 명칭은 아니다. 틀린 표현은 '감사 기록 탐지'이며, 올바른 표현은 '통계적 변형 탐지'이다.
④ X — 분산 침입 탐지는 여러 호스트나 네트워크의 탐지 정보를 모아 협력적으로 분석하는 배치·구성 방식이다. 틀린 표현은 '분산 침입 탐지'이며, 제시된 두 탐지 기법을 활용하는 분석 방식은 '통계적 변형 탐지'이다.

오답 포인트

'감사 기록'은 분석에 쓰이는 자료이고 '분산'은 탐지 시스템의 구성 방식이라는 점을 놓치면 탐지 원리를 나타내는 용어와 혼동하기 쉽다. 이 문항에서는 '임계값'과 '정상 프로파일에서의 이탈'이 통계적 변형 탐지의 결정적 단서이다.

NoteBase

다시 나오면 이렇게 판단

임계값·평균·빈도·정상 프로파일과의 편차가 제시되면 통계적 변형 탐지로 판단한다. 알려진 공격 패턴·시그니처와의 일치가 제시되면 규칙 기반 탐지로 판단한다.

암기 포인트

임계값·프로파일 이탈은 통계적 변형 탐지, 알려진 공격 패턴 대조는 규칙 기반 탐지이다.

NoteBase

24. 다음 중 침입차단시스템의 유형으로 가장 옳지 않은 것은?
① 패킷-필터링 침입차단시스템 (Packet-Filtering Firewall)
② 스테이트풀 검사 침입차단시스템 (Stateful Packet Inspection Firewall)
③ 회선-레벨 게이트웨이 (Circuit-Level Gateway)
④ 하이재킹 침입차단시스템(Hijacking Firewall)

정답 4번

출제 포인트

대표적인 침입차단시스템의 유형과 공격 기법을 구별하는 문제이다.

핵심 개념

패킷 필터링 침입차단시스템은 개별 패킷의 출발지·목적지 주소, 포트, 프로토콜 등 헤더 정보를 규칙과 비교해 통과 여부를 결정한다.
스테이트풀 검사 침입차단시스템은 연결 상태와 세션 정보를 추적하면서 패킷이 정상적인 통신 흐름에 속하는지 검사한다.
회선 레벨 게이트웨이는 세션의 연결 설정과 회선 상태를 확인하고 내부망과 외부망 사이의 연결을 중계한다.
하이재킹은 정상 세션이나 통신을 가로채는 공격 기법이며, 표준적인 침입차단시스템 유형이 아니다.

선지별 해설

① O — 패킷 필터링 침입차단시스템은 패킷 헤더의 주소·포트·프로토콜 등을 규칙에 따라 검사하는 대표적인 침입차단시스템 유형이다.
② O — 스테이트풀 검사 침입차단시스템은 연결 상태표를 유지하고 세션의 상태를 고려해 패킷을 허용하거나 차단하는 유형이다.
③ O — 회선 레벨 게이트웨이는 전송계층의 세션 연결을 확인하고 연결을 중계하는 침입차단시스템 유형이다.
④ X — 틀린 표현은 '하이재킹 침입차단시스템'이다. 하이재킹은 세션이나 통신을 가로채는 공격 기법이며, 올바르게는 침입차단시스템의 유형이 아니라 침입차단시스템 등이 방어해야 할 공격 기법이라고 해야 한다.

오답 포인트

④는 보안 용어인 '하이재킹' 뒤에 '침입차단시스템'을 붙여 실제 방화벽 유형처럼 보이게 한 함정이다. 보안과 관련된 용어라고 해서 모두 보안 장비의 분류가 되는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

각 용어가 트래픽을 검사·중계하는 방어 장비의 방식인지, 세션을 탈취하는 공격 행위인지 먼저 구분한다. 패킷 필터링·상태 추적·회선 중계는 방화벽의 검사 방식이고, 하이재킹은 공격 방식이다.

암기 포인트

필터링·스테이트풀·게이트웨이는 방화벽 유형이고, 하이재킹은 공격 기법이다.

NoteBase

25. 다음 중 TCP 헤더의 Control Flag 필드에 대한 설명으로 가장 옳지 않은 것은?

① 플래그 비트 중 SYN만 전송해 대상 서버에서 SYN+ACK로 응답하는 경우 포트가 오픈 상태로 있는 것을 판단할 수 있다.

② FIN 플래그만 전송하면 대상 포트가 닫혀있는 경우 RST 플래그가 세팅된 패킷이 수신된다.

③ 플래그 하위 비트 6개를 모두 0으로 전송하면 대상 포트가 닫혀있는 경우 PSH 플래그가 세팅된 패킷이 수신된다.

④ 플래그 하위 비트 6개를 모두 1로 전송하면 대상 포트가 닫혀있는 경우 RST 플래그가 세팅된 패킷이 수신된다.

정답 3번

출제 포인트

TCP Control Flag의 조합으로 포트의 개방 여부를 판단할 때, 열린 포트와 닫힌 포트가 어떤 플래그로 응답하는지를 묻는 문제이다.

핵심 개념

SYN은 연결 설정을 요청하는 플래그이고, SYN+ACK는 그 요청을 받아들였다는 응답이다. FIN은 연결 종료를 뜻하며, RST는 존재하지 않거나 비정상인 연결을 즉시 거부·초기화할 때 사용된다. PSH는 수신 데이터를 응용 프로그램에 신속히 전달하도록 요구하는 플래그이지, 닫힌 포트를 알리는 응답 플래그가 아니다.
플래그를 모두 0으로 보내는 방식은 NULL 탐사이며, 닫힌 포트는 일반적으로 RST가 설정된 패킷으로 응답한다.

선지별 해설

① O — SYN만 보낸 뒤 SYN+ACK를 받으면 상대가 연결 요청을 수락한 것이므로 대상 포트가 열린 상태라고 판단할 수 있다.
② O — 닫힌 포트에 FIN 탐사를 보내면 해당 연결을 처리할 수 없으므로 RST가 설정된 응답 패킷이 돌아온다.
③ X — 플래그 하위 6비트를 모두 0으로 보내는 것은 NULL 탐사이다. 닫힌 포트가 보내는 응답은 PSH가 아니라 RST가 설정된 패킷이다. 틀린 표현인 'PSH 플래그가 세팅된 패킷'은 'RST 플래그가 세팅된 패킷'으로 고쳐야 한다.
④ O — 플래그 하위 6비트를 모두 1로 만든 비정상적인 플래그 조합을 닫힌 포트로 보내면, 닫힌 포트는 연결을 거부하는 RST가 설정된 패킷으로 응답한다.

NoteBase

오답 포인트

③은 NULL 탐사의 응답 플래그를 PSH로 바꾸어 놓은 것이 함정이다. PSH는 데이터 전달을 재촉하는 기능이고, 닫힌 포트임을 나타내는 대표적인 거부 응답은 RST이다.

다시 나오면 이렇게 판단

먼저 SYN에 대한 SYN+ACK는 열린 포트의 신호로 판단한다. 그 밖의 비정상 플래그 탐사에서는 닫힌 포트가 RST로 응답하는지를 확인하고, PSH는 포트 폐쇄 통보용 플래그가 아니라는 점으로 선지를 판별한다.

암기 포인트

SYN→SYN+ACK는 포트 열림, 비정상 탐사→RST는 포트 닫힘, PSH는 데이터 즉시 전달이다.

NoteBase