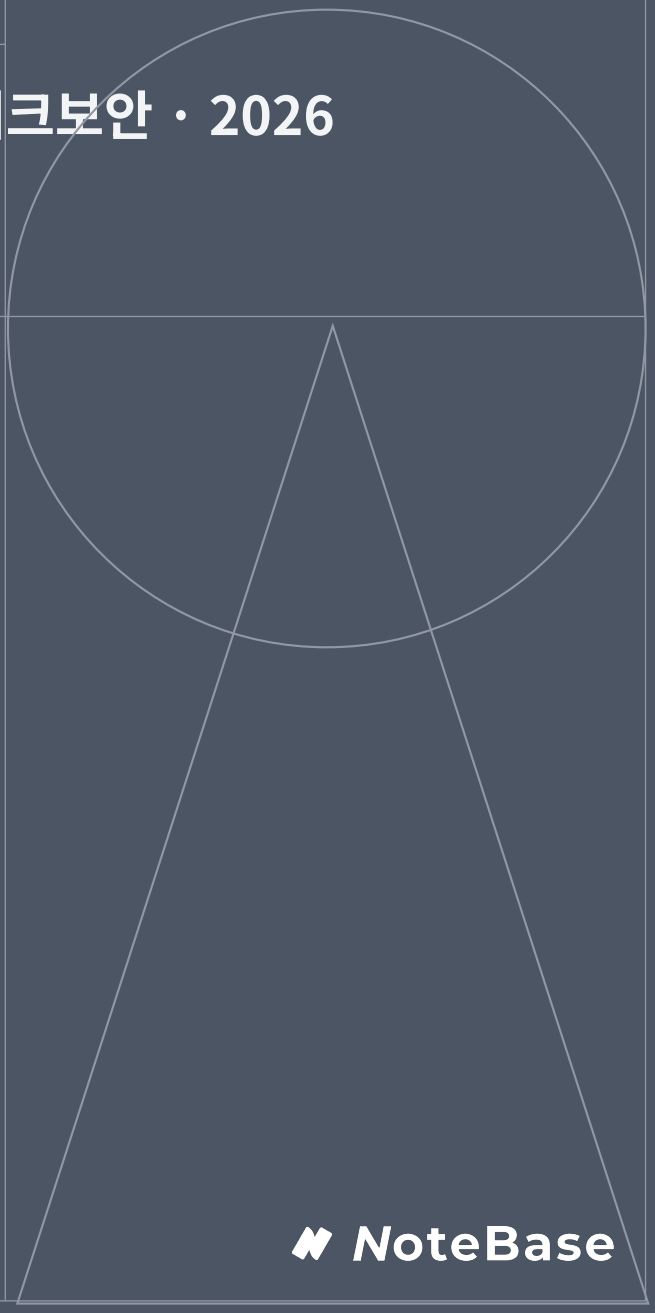
기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2026



NoteBase

기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2026

공무원/군무원/9급 · 네트워크보안 · 2026

1. TLS를 올바르게 구성했을 때 기대할 수 있는 보안 효과로 가장 적절한 것은?
   ① IP 주소 위조를 물리적으로 불가능하게 한다.
   ② 클라이언트와 서버 사이 통신의 도청, 변조, 메시지 위조 위험을 줄인다.
   ③ 모든 웹 애플리케이션 취약점을 자동 제거한다.
   ④ 서버 운영체제의 권한 상승 취약점을 자동 패치한다.

정답 2번

출제 포인트

이 문제는 TLS가 제공하는 전송 구간 보안 효과와 TLS의 보호 범위를 벗어나는 취약점을 구분하는 문제이다.

핵심 개념

TLS는 클라이언트와 서버 사이의 통신을 암호화하고, 메시지의 무결성을 확인하며, 인증서를 통해 통신 상대를 인증하는 프로토콜이다. 따라서 통신 내용의 도청·변조와 상대방 또는 메시지 위조의 위험을 줄일 수 있다. 다만 IP 계층 자체, 웹 애플리케이션 코드, 서버 운영체제의 취약점을 자동으로 제거하거나 패치하지는 않는다.

NoteBase

선지별 해설

① X
틀린 표현은 'IP 주소 위조를 물리적으로 불가능하게 한다'이다. TLS는 통신 내용을 암호화하고 인증서 검증과 무결성 확인을 제공하지만, IP 패킷의 출발지 주소를 거짓으로 꾸미는 행위 자체를 물리적으로 차단하지는 않는다. 올바르게는 'TLS는 통신 상대 인증과 무결성 검증을 통해 위조된 상대와의 통신 위험을 줄인다'이다.

② O
TLS를 올바르게 구성하면 전송 내용을 암호화하여 도청 위험을 줄이고, 무결성 검증으로 전송 중 변조를 탐지하며, 상대 인증을 통해 메시지 위조 위험도 낮춘다. 이는 TLS의 대표적인 보안 효과이다.

③ X
틀린 표현은 '모든 웹 애플리케이션 취약점을 자동 제거한다'이다. TLS는 전송 구간을 보호할 뿐 SQL 삽입, 크로스 사이트 스크립팅, 인증·인가 오류와 같은 애플리케이션 취약점을 수정하지 않는다. 올바르게는 '웹 애플리케이션 취약점은 안전한 개발, 보안 점검, 입력값 검증과 패치 등으로 별도 제거한다'이다.

④ X
틀린 표현은 '서버 운영체제의 권한 상승 취약점을 자동 패치한다'이다. TLS에는 운영체제 취약점을 탐지하거나 수정하는 기능이 없다. 올바르게는 '운영체제의 권한 상승 취약점은 보안 업데이트와 패치 관리로 해결한다'이다.

오답 포인트

'통신을 안전하게 한다'는 말을 시스템 전체의 모든 공격을 막는다는 뜻으로 확대하면 ①·③·④에 속기 쉽다. TLS가 직접 보호하는 대상은 클라이언트와 서버 사이의 전송 구간이며, 애플리케이션과 운영체제의 취약점 관리는 별도 영역이다.

다시 나오면 이렇게 판단

선지의 효과가 암호화·무결성·상대 인증에 해당하면 TLS의 기능으로 판단한다. 반대로 IP 위조의 물리적 차단, 애플리케이션 취약점 제거, 운영체제 패치처럼 다른 계층이나 시스템 관리에 속하면 TLS의 직접 효과가 아니라고 판단한다.

암기 포인트

TLS는 전송 구간의 기밀성·무결성·인증을 제공하지만, 애플리케이션과 운영체제까지 자동으로 고치지는 않는다.

NoteBase

2. S/MIME에 대한 설명으로 가장 적절하지 않은 것은?
① S/MIME은 RSA를 이용해 MIME 인터넷 전자메일 형식 표준을 보안적으로 강화시킨 것이다.
② MIME은 SMTP가 실행파일이나 2진 데이터를 전송하지 못하는 것을 개선하였다.
③ MIME 전송 부호화 방법 중 Base64 전송 부호화는 일반적으로 임의의 2진 데이터를 부호화하는데 사용한다.
④ 기능면에서 S/MIME은 PGP와 유사하지만 PGP는 메시지를 서명하고 암호화하는 기능을 제공하지 않는다.

정답 4번

출제 포인트

S/MIME과 PGP가 전자우편에 제공하는 보안 기능, MIME과 Base64의 역할을 구별하는 문제이다.

핵심 개념

S/MIME: MIME 형식의 전자우편에 공개키 암호 기술과 인증서를 적용하여 암호화와 전자서명 등의 보안 기능을 제공하는 표준이다.
MIME: SMTP의 기본적인 텍스트 전송 한계를 보완하여 다양한 문자 형식과 실행파일을 포함한 2진 첨부 데이터를 전자우편으로 전송할 수 있게 한다.
Base64: 2진 데이터를 전자우편 전송에 적합한 ASCII 문자 형태로 바꾸는 전송 부호화 방식이며, 기밀성을 제공하는 암호화 방식은 아니다.
PGP: 전자우편 메시지의 암호화와 전자서명을 모두 지원하는 보안 방식이다.

선지별 해설

① O — S/MIME은 RSA와 같은 공개키 암호 기술을 이용해 MIME 전자우편에 암호화와 전자서명 등의 보안 기능을 추가한다.
② O — MIME은 SMTP가 본래 실행파일이나 2진 데이터를 그대로 처리하기 어려운 한계를 보완하여 다양한 형식의 본문과 첨부파일을 전송할 수 있게 한다.
③ O — Base64 전송 부호화는 임의의 2진 데이터를 ASCII 문자 형태로 변환하여 전송하는 데 사용한다. 다만 이는 암호화가 아니므로 보안상 기밀성을 제공하지 않는다.
④ X — 틀린 표현은 ‘PGP는 메시지를 서명하고 암호화하는 기능을 제공하지 않는다’이다. 올바르게는 PGP도 S/MIME과 마찬가지로 메시지의 전자서명과 암호화 기능을 제공한다.

NoteBase

오답 포인트

S/MIME과 PGP가 서로 다른 전자우편 보안 체계라는 점을 기능의 차이로 오해하기 쉽다. 두 방식 모두 암호화와 전자서명을 지원한다. 또한 ③의 '부호화'를 '암호화'로 읽으면 안 된다. Base64는 전송 가능한 문자 형태로 바꾸는 방식일 뿐이다.

다시 나오면 이렇게 판단

전자우편 보안 기능을 물으면 S/MIME과 PGP는 모두 암호화와 전자서명을 지원한다고 판단한다. 전송 형식 문제를 물으면 MIME은 데이터 형식을 확장하고 Base64는 2진 데이터를 ASCII 문자 형태로 바꾼다고 구별한다.

암기 포인트

S/MIME·PGP는 암호화와 서명, MIME·Base64는 형식 확장과 전송 부호화이다.

NoteBase

3. 방화벽 로그에서 외부 IP 하나가 짧은 시간동안 22, 23, 80, 443, 445, 3389 포트로 순차 접속을 시도했다. 이에 대한 판단으로 가장 적절한 것은?
① 포트 스캔 또는 서비스 탐색 가능성이 있으므로 출발지, 빈도, 대상 포트, 성공 여부를 분석한다.
② 정상적인 웹 브라우징이다.
③ TCP 포트이므로 보안 이벤트가 아니다.
④ 443 포트가 포함되어 있으므로 모두 정상이다.

정답 1번

출제 포인트

짧은 시간에 하나의 외부 IP가 여러 서비스 포트로 연속 접속을 시도한 로그를 포트 스캔 또는 서비스 탐색의 징후로 판단할 수 있는지를 묻는 문제이다.

핵심 개념

포트 스캔은 한 호스트의 여러 포트에 접속을 시도하여 열려 있는 포트와 실행 중인 서비스를 찾아내는 탐색 행위이다. 다수의 주요 서비스 포트에 짧은 시간 동안 연속 접근한 기록은 스캔 징후가 될 수 있으므로 출발지, 시도 빈도, 대상 포트, 연결 성공 여부 등을 함께 분석해야 한다.
정상적인 웹 브라우징은 주로 웹 서비스 포트인 80과 443을 이용한다. 반면 22는 SSH, 23은 Telnet, 445는 SMB, 3389는 원격 데스크톱 서비스와 관련되므로 이 포트들까지 연속으로 접근한 행위를 단순한 웹 브라우징으로 보기 어렵다.

선지별 해설

① O — 짧은 시간에 동일한 외부 IP가 여러 서비스 포트로 순차 접속을 시도한 것은 포트 스캔 또는 서비스 탐색의 전형적인 징후가 될 수 있다. 출발지, 빈도, 대상 포트, 성공 여부를 분석하여 실제 탐색 행위인지 확인하는 판단이 적절하다.
② X — 틀린 표현은 '정상적인 웹 브라우징이다'이다. 정상적인 웹 브라우징은 일반적으로 80·443 포트를 중심으로 이루어지며, 22·23·445·3389까지 연속 접근한 기록은 포트 스캔 가능성을 우선 분석해야 한다.
③ X — 틀린 표현은 'TCP 포트이므로 보안 이벤트가 아니다'이다. TCP는 통신 방식일 뿐 안전성을 보장하지 않으며, TCP 포트에 대한 반복·연속 접속 시도도 정찰이나 공격의 보안 이벤트가 될 수 있다.
④ X — 틀린 표현은 '443 포트가 포함되어 있으므로 모두 정상이다'이다. 443은 정상적인 HTTPS 통신에도 쓰이지만, 특정 정상 포트 하나가 포함되었다고 전체 접속 시도가 정상화되는 것은 아니다. 모든 대상 포트와 시간적 패턴을 종합하여 판단해야 한다.

NoteBase

오답 포인트

443이나 TCP라는 정상 통신 요소 하나만 보고 전체 로그를 정상으로 단정하는 것이 함정이다. 이 문항에서는 개별 포트의 존재보다 '동일 출발지에서 짧은 시간에 여러 서비스 포트로 연속 접속'했다는 패턴이 핵심이다.

다시 나오면 이렇게 판단

하나의 출발지가 짧은 시간에 여러 포트를 차례로 두드리면 먼저 포트 스캔 가능성을 검토한다. 그다음 출발지, 시간당 시도 횟수, 대상 포트의 종류, 연결 성공 여부와 후속 트래픽을 함께 확인하여 정상 사용과 탐색 행위를 구분한다.

암기 포인트

단일 IP·짧은 시간·다수 포트·연속 시도는 포트 스캔의 핵심 징후이다.

NoteBase

4. OSI 7계층에서 2계층(데이터링크계층)의 데이터 단위(Protocol Data Unit)로 가장 적절한 것은?
① 비트(Bits)
② 세그먼트(Segment)
③ 패킷(Packet)
④ 프레임(Frame)

정답 4번

출제 포인트

OSI 7계층에서 각 계층이 사용하는 프로토콜 데이터 단위(PDU)의 명칭을 구분하는 문제이다.

핵심 개념

프로토콜 데이터 단위(PDU)는 각 계층에서 처리하고 전달하는 데이터의 단위이다. 물리 계층은 비트, 데이터링크 계층은 프레임, 네트워크 계층은 패킷, 전송 계층은 세그먼트를 사용한다.

선지별 해설

① X — 비트(Bits)는 물리 계층의 데이터 단위이다. 틀린 표현은 '데이터링크 계층의 단위가 비트'라는 대응이며, 올바르게는 '물리 계층의 단위가 비트'이다.
② X — 세그먼트(Segment)는 전송 계층의 데이터 단위이다. 틀린 표현은 '데이터링크 계층의 단위가 세그먼트'라는 대응이며, 올바르게는 '전송 계층의 단위가 세그먼트'이다.
③ X — 패킷(Packet)은 네트워크 계층의 데이터 단위이다. 틀린 표현은 '데이터링크 계층의 단위가 패킷'이라는 대응이며, 올바르게는 '네트워크 계층의 단위가 패킷'이다.
④ O — 프레임(Frame)은 데이터링크 계층의 데이터 단위이므로 옳다.

오답 포인트

패킷과 프레임을 모두 네트워크에서 전송되는 데이터 덩어리로 생각하면 ③과 ④를 혼동하기 쉽다. 패킷은 3계층인 네트워크 계층, 프레임은 2계층인 데이터링크 계층의 단위이다.

다시 나오면 이렇게 판단

OSI 계층 번호와 PDU를 '1계층 비트, 2계층 프레임, 3계층 패킷, 4계층 세그먼트'로 대응하여 판단한다.

암기 포인트

비트(1) → 프레임(2) → 패킷(3) → 세그먼트(4)로 연결한다.

NoteBase

5. 다음에 대한 설명으로 가장 적절한 것은?

> - 이것은 메시지의 암호화 및 전자서명을 제공하고 인터넷상에서 안전한 신원 확인과 데이터 보호를 가능하게 하는 보안 프레임워크이다.
> - 이것이 되려면 인증 정보를 일원화하여 호환성을 갖춤으로써 개인이 쉽게 접근할 수 있어야 한다.
> - 신뢰를 구축하기 위해 여러 주체(PAA, PCA, CA, RA)가 트리형으로 구성하고 있다.

① 전자봉투
② DRM
③ 공개키 기반 구조
④ 커버로스

정답 3번

출제 포인트

공개키 기반 구조(PKI)의 기능과 계층적 신뢰구조를 전자봉투, DRM, 커버로스와 구별하는 문제이다.

핵심 개념

공개키 기반 구조(PKI): 인증서의 발급·검증·폐기와 공개키 관리를 통해 인터넷에서 신원 인증, 데이터 보호, 전자서명을 지원하는 보안 기반이다. PAA·PCA·CA·RA 등의 주체가 계층적 신뢰구조를 이루며 인증 정보의 표준화와 상호운용성을 뒷받침한다.
전자봉투: 데이터를 대칭키로 암호화하고 그 대칭키를 수신자의 공개키로 암호화하여 함께 전달하는 기법이다.
DRM: 디지털 콘텐츠의 접근·복제·배포 등 이용 권한을 통제하고 저작권을 보호하는 기술이다.
커버로스: 신뢰할 수 있는 키 분배 센터가 발급한 티켓을 이용하여 사용자를 인증하는 대칭키 기반 인증 방식이다.

NoteBase

선지별 해설

① X
전자봉투는 대칭키로 데이터를 암호화하고 수신자의 공개키로 그 대칭키를 암호화해 전달하는 기법이다. PAA·PCA·CA·RA가 계층적 신뢰구조를 이루는 보안 프레임워크라는 설명에는 해당하지 않는다. 틀린 표현인 '전자봉투'는 '공개키 기반 구조(PKI)'로 고쳐야 한다.

② X
DRM은 디지털 콘텐츠의 사용 권한과 복제·배포를 통제하여 저작권을 보호하는 기술이다. 인증 정보를 일원화하고 인증기관들을 계층적으로 구성하는 체계가 아니다. 틀린 표현인 'DRM'은 '공개키 기반 구조(PKI)'로 고쳐야 한다.

③ O
공개키 기반 구조(PKI)는 공개키 인증서를 중심으로 신원 인증, 암호화, 전자서명을 지원한다. 또한 PAA·PCA·CA·RA 등의 주체가 계층적 신뢰구조를 형성한다는 설명과 정확히 일치한다.

④ X
커버로스는 키 분배 센터와 티켓을 이용하는 대칭키 기반 네트워크 인증 방식이다. 공개키 인증서의 발급·검증 체계나 PAA·PCA·CA·RA의 계층구조를 뜻하지 않는다. 틀린 표현인 '커버로스'는 '공개키 기반 구조(PKI)'로 고쳐야 한다.

오답 포인트

첫 번째 설명의 '암호화'와 '전자서명'만 보면 전자봉투나 다른 보안 기술을 떠올릴 수 있다. 그러나 '인증 정보의 일원화와 상호운용성', 'PAA·PCA·CA·RA의 계층적 신뢰구조'가 PKI를 확정하는 결정적 단서이다.

다시 나오면 이렇게 판단

인증서·공개키 관리·CA와 RA·계층적 신뢰구조가 함께 제시되면 PKI로 판단한다. 콘텐츠 이용 통제는 DRM, 암호화된 대칭키의 전달은 전자봉투, 티켓과 키 분배 센터를 이용한 인증은 커버로스로 구분한다.

암기 포인트

인증서와 CA 계층은 PKI, 콘텐츠 권한은 DRM, 암호화 키 포장은 전자봉투, 티켓 인증은 커버로스이다.

NoteBase

6. 다음 Snort/Suricata 형식의 규칙이 있다. 가장 적절한 것은?

```
- alert tcp any any -> 192.168.10.0/24 80 (msg:"Suspicious URI"; content:"/admin.php"; http_uri; sid:100001;)
```

① 출발지가 내부망이고 목적지가 외부망인 패킷만 탐지한다.
② 목적지가 192.168.10.0/24의 TCP 80번이며 HTTP URI에 /admin.php가 포함된 트래픽을 경고한다.
③ 모든 UDP 패킷을 차단한다.
④ 이 규칙은 방화벽 NAT 규칙이다.

정답 2번

출제 포인트

Snort/Suricata 규칙의 헤더에서 동작·프로토콜·출발지·방향·목적지·포트를 읽고, 옵션에서 탐지 문자열과 검사 대상을 해석하는 문제이다.

핵심 개념

규칙 헤더의 alert는 일치한 트래픽에 경고를 발생시키는 동작이고, tcp는 검사할 프로토콜이다.
any any는 출발지 IP와 출발지 포트에 제한이 없다는 뜻이며, -> 뒤의 192.168.10.0/24 80은 목적지가 해당 서브넷의 TCP 80번 포트임을 뜻한다.
content:"/admin.php"와 http_uri의 조합은 HTTP URI에서 /admin.php 문자열을 찾는 조건이다. msg는 경고 메시지이고 sid는 규칙 식별자이다.

NoteBase

선지별 해설

① X
출발지는 내부망으로 지정되지 않고 any이며, 목적지는 외부망이 아니라 192.168.10.0/24로 지정되어 있다. 틀린 표현은 '출발지가 내부망이고 목적지가 외부망인 패킷만'이며, 올바르게는 '출발지 IP와 포트에 제한 없이 192.168.10.0/24의 TCP 80번 포트로 향하는 패킷을 검사한다'이다.

② O
헤더는 목적지 192.168.10.0/24의 TCP 80번 포트를 지정하고, 옵션은 HTTP URI에 /admin.php가 포함되는지를 검사한 뒤 alert 동작으로 경고한다.

③ X
헤더의 프로토콜은 udp가 아니라 tcp이고, 동작도 차단이 아니라 alert이다. 틀린 표현은 '모든 UDP 패킷을 차단한다'이며, 올바르게는 '지정된 조건에 맞는 TCP 트래픽을 탐지하여 경고한다'이다.

④ X
이 구문은 주소를 변환하는 NAT 규칙이 아니라 패킷 내용을 검사하는 Snort/Suricata 탐지 규칙이다. 틀린 표현은 '방화벽 NAT 규칙'이며, 올바르게는 'HTTP URI의 특정 문자열을 탐지하는 네트워크 보안 탐지 규칙'이다.

오답 포인트

①은 사설 IP 대역이라는 이유만으로 출발지와 목적지의 방향을 바꾸어 읽게 하고, ③은 alert를 차단 동작으로 오해하게 한다. 규칙은 왼쪽에서 오른쪽으로 읽되 alert와 tcp의 의미를 각각 분리해야 한다.

다시 나오면 이렇게 판단

헤더를 '동작-프로토콜-출발지 IP-출발지 포트-방향-목적지 IP-목적지 포트' 순서로 나눈 뒤, 괄호 안에서 content의 문자열과 http_uri의 검사 대상을 연결한다. alert는 경고이고 차단이나 NAT를 뜻하지 않는다.

암기 포인트

alert는 경고, tcp는 프로토콜, -> 오른쪽은 목적지, content + http_uri는 URI 문자열 탐지이다.

NoteBase

7. 랜섬웨어의 감염 경로로 가장 적절하지 않은 것은?
① 스팸 메일
② SNS로 유포된 URL
③ 허용된 프로그램만 실행 가능한 USB
④ 파일 공유 사이트에서 다운로드한 파일

정답 3번

출제 포인트

랜섬웨어가 피해자의 장치에 유입·실행되는 일반적인 감염 경로와, 감염을 차단하기 위한 실행 통제 수단을 구별하는 문제이다.

핵심 개념

랜섬웨어는 파일을 암호화하거나 시스템 사용을 제한한 뒤 금전을 요구하는 악성코드이다. 스팸 메일, SNS의 악성 URL, 파일 공유 사이트에서 받은 감염 파일처럼 외부의 악성 콘텐츠를 열거나 실행하는 과정이 대표적인 감염 경로이다. 반면 허용된 프로그램만 실행되도록 제한하는 방식은 악성코드 실행 가능성을 낮추는 통제 수단이다.

선지별 해설

① O — 스팸 메일의 악성 첨부파일이나 링크를 열면 랜섬웨어가 내려받아지거나 실행될 수 있으므로 대표적인 감염 경로이다.

② O — SNS에 유포된 악성 URL을 누르면 악성 파일 다운로드 페이지나 취약점을 악용하는 사이트로 연결될 수 있으므로 감염 경로가 될 수 있다.

③ X — 틀린 표현은 '허용된 프로그램만 실행 가능한 USB'를 랜섬웨어의 감염 경로로 본 부분이다. 올바르게는 허용 목록에 포함된 프로그램만 실행하도록 제한하는 USB 또는 실행 통제 환경은 승인되지 않은 랜섬웨어의 실행을 막는 보안 수단에 가깝다.

④ O — 출처나 안전성이 확인되지 않은 파일 공유 사이트의 파일에는 랜섬웨어가 포함될 수 있고, 이를 내려받아 실행하면 감염될 수 있으므로 일반적인 감염 경로이다.

NoteBase

오답 포인트

③의 ‘USB’라는 매체명만 보고 이동식 저장장치를 곧바로 감염 경로로 판단하기 쉽다. 그러나 이 선지의 결정적 표현은 ‘허용된 프로그램만 실행 가능’이며, 이는 악성코드 유입 경로가 아니라 승인되지 않은 프로그램의 실행을 제한하는 통제 기능이다.

다시 나오면 이렇게 판단

선지가 악성 파일이나 링크를 전달하는 유입 수단인지, 아니면 악성 프로그램의 실행을 제한하는 방어 수단인지 구분한다. 메일·URL·불분명한 다운로드는 감염 경로로, 허용 목록·실행 제한은 예방 통제로 판단한다.

암기 포인트

스팸·악성 URL·의심 파일은 유입 경로, 허용 프로그램만 실행은 차단 수단이다.

NoteBase

8. TLS와 같은 공개 인터넷 환경의 보안 통신에서 공개키 기반 절차와 대칭키 암호를 함께 사용하는 주된 이유로 가장 적절한 것은?
   ① 공개키 암호는 대칭키 암호보다 항상 빠르므로 대용량 데이터 암호화에만 사용한다
   ② 통신 전에 안전한 비밀키를 공유하기 어려운 환경에서 공개키 기반 인증과 키 합의 절차로 세션키를 설정하고, 이후 대칭키 암호로 데이터를 효율적으로 보호할 수 있기 때문이다.
   ③ 공개키 암호와 대칭키 암호는 항상 같은 키를 사용한다.
   ④ 대칭키 암호는 기밀성을 제공할 수 없으므로 사용하지 않는다.

정답 2번

출제 포인트

TLS와 같은 보안 통신에서 공개키 암호와 대칭키 암호를 함께 쓰는 하이브리드 방식의 목적과 두 암호 방식의 역할 차이를 묻는 문제이다.

핵심 개념

공개키 암호는 공개키와 개인키의 쌍을 이용하여 상대를 인증하거나 세션 키를 안전하게 설정하는 방식이다.
통신 전에 비밀키를 미리 공유하기 어려운 문제를 해결하는 데 유리하지만 연산 부담이 크다.
대칭키 암호는 송신자와 수신자가 같은 비밀키를 공유하여 데이터를 암호화·복호화하는 방식이다. 처리 속도가 빨라 세션 키가 설정된 뒤 실제 통신 데이터를 효율적으로 보호하는 데 적합하다.
따라서 TLS 계열의 보안 통신은 공개키 기반 절차로 인증과 키 설정을 수행하고, 이후 대칭키 암호로 본문 데이터를 보호하는 역할 분담을 사용한다.

NoteBase

선지별 해설

① X — '공개키 암호는 대칭키 암호보다 항상 빠르므로 대용량 데이터 암호화에만 사용한다'는 부분이 틀렸다. 공개키 암호는 일반적으로 대칭키 암호보다 연산 부담이 크며, 주로 인증이나 세션 키 설정에 사용한다. 대용량 데이터는 빠른 대칭키 암호로 처리한다.
② O — 공개된 네트워크에서는 통신 전에 안전한 비밀키를 미리 공유하기 어렵다. 공개키 기반 인증과 키 합의·키 설정 절차로 세션 키를 안전하게 마련한 뒤, 대칭키 암호로 실제 데이터를 빠르고 효율적으로 보호할 수 있으므로 두 방식을 함께 사용한다.
③ X — '항상 같은 키를 사용한다'는 부분이 틀렸다. 대칭키 암호는 암호화와 복호화에 같은 공유 비밀키를 사용하지만, 공개키 암호는 서로 대응하는 공개키와 개인키의 쌍을 사용한다.
④ X — '대칭키 암호는 기밀성을 제공할 수 없다'는 부분이 틀렸다. 대칭키 암호는 공유 비밀키를 모르는 제3자가 평문을 알아볼 수 없게 하므로 기밀성을 제공하며, 실제 세션 데이터 보호에 널리 사용된다.

오답 포인트

①은 공개키 암호의 '키 배포에 유리함'을 '처리 속도가 빠름'으로 바꾸었고, ③은 대칭키의 동일 키 구조를 공개키 암호에도 잘못 적용했다. ④는 대칭키 암호가 세션 데이터의 기밀성을 담당한다는 핵심 역할을 정반대로 서술했다.

다시 나오면 이렇게 판단

보안 프로토콜에서 두 암호 방식을 함께 사용하는 이유를 물으면 '공개키 기반 절차로 인증·키 설정, 대칭키 암호로 빠른 데이터 처리'라는 역할 분담을 기준으로 판단한다.

암기 포인트

공개키는 인증·키 설정, 대칭키는 빠른 본문 암호화이다.

NoteBase

9. 기관 로그인 시스템에서 5회 실패 시 계정을 24시간 동안 잠그도록 설정했다. 이후 공격자가 여러 사용자 ID에 대해 일부러 5회씩 실패 로그인을 발생시켜 업무가 중단되었다. 이에 대한 개선책으로 가장 적절한 것은?
① 계정 잠금 정책을 완전히 제거한다.
② 비밀번호 길이를 4자리로 줄인다.
③ 위험 기반 지연, 단계적 제한, CAPTCHA 또는 추가 인증, 출발지 평판, 관리자 알림을 조합한다.
④ 실패 로그를 남기지 않는다.

정답 3번

출제 포인트

이 문제는 반복 로그인 실패를 막는 계정 잠금 정책과, 그 정책이 악용되어 정상 사용자의 업무를 중단시키는 서비스 거부 위험 사이의 균형을 묻는다.

핵심 개념

계정 잠금은 일정 횟수 이상 인증에 실패한 계정의 로그인을 제한하여 비밀번호 추측 공격을 억제하는 통제이다. 그러나 고정된 실패 횟수만으로 모든 계정을 장시간 잠그면 공격자가 일부러 실패를 반복하여 정상 사용자를 차단할 수 있다. 따라서 실패 횟수, 접속 위치·기기 등 위험 신호에 따른 지연과 단계적 제한, CAPTCHA·추가 인증, 출발지 평판, 관리자 알림을 함께 적용하여 공격은 어렵게 하고 정상 사용자의 업무 중단은 줄이는 방식이 적절하다.

NoteBase

선지별 해설

① X
계정 잠금 정책을 완전히 제거하면 공격자가 횟수 제한 없이 비밀번호를 반복 추측할 수 있어 무차별 대입 공격과 비밀번호 대입 공격에 취약해진다. 틀린 표현은 '완전히 제거한다'이며, 올바르게는 잠금 기능을 유지하되 위험 기반 지연과 단계적 제한 등으로 악용 가능성을 낮춘다.

② X
비밀번호 길이를 4자리로 줄이면 가능한 비밀번호 조합과 추측 난도가 감소하여 계정 탈취 위험이 커진다. 틀린 표현은 '4자리로 줄인다'이며, 올바르게는 충분한 길이와 강도를 확보하고 반복 실패 통제를 함께 적용한다.

③ O
위험 기반 지연과 단계적 제한은 반복 실패에 대한 제재를 점차 강화하고, CAPTCHA·추가 인증은 자동화된 공격과 정상 사용자를 구분하는 데 도움을 준다. 여기에 출발지 평판과 관리자 알림을 결합하면 여러 사용자 ID를 의도적으로 잠그는 공격을 탐지·완화하면서도 정상 사용자의 장시간 일괄 잠금을 줄일 수 있다.

④ X
실패 로그를 남기지 않으면 여러 계정에서 반복되는 실패, 의심스러운 출발지, 공격 확산 여부를 탐지하고 조사하기 어렵다. 틀린 표현은 '남기지 않는다'이며, 올바르게는 실패 로그를 기록·보호·분석하고 이상 징후가 있으면 관리자에게 알린다.

오답 포인트

문제의 함정은 계정 잠금 자체를 없애면 가용성 문제가 해결된다고 생각하는 데 있다. ①은 서비스 거부의 수단은 없애지만 비밀번호 추측 방어까지 제거하고, ②와 ④도 각각 인증 강도와 탐지 능력을 약화한다. ③처럼 통제를 폐기하지 않고 위험도에 따라 강도를 조절하는 것이 핵심이다.

다시 나오면 이렇게 판단

고정 임계치 기반 장시간 잠금이 악용된 사례에서는 '잠금 폐지'가 아니라 '위험 기반·점진적 제재 + 자동화 방지 또는 추가 인증 + 로그·알림'의 조합을 우선 판단한다. 보안 통제의 개선책은 계정 탈취 방지와 정상 사용자의 가용성을 함께 보존해야 한다.

암기 포인트

잠금은 없애지 않고 정교하게 적용한다: 위험 기반, 단계적 제한, 추가 인증, 로그·알림이다.

NoteBase

10. NAT에 대한 설명으로 가장 적절한 것은?
① NAT는 주소 변환 기능이며, 접근 제어, 침입 탐지, 인증을 대체하지 못한다.
② NAT만 적용하면 내부망의 모든 보안 위협이 제거된다.
③ NAT는 암호화 프로토콜이다.
④ NAT를 사용하면 악성코드의 외부 통신이 원천적으로 불가능하다.

정답 1번

출제 포인트

NAT의 주소 변환 기능과 방화벽·침입 탐지·인증·암호화 같은 보안 기능을 구분하는 문제이다.

핵심 개념

NAT(Network Address Translation)는 패킷의 IP 주소를 공인 주소와 사설 주소 사이에서 변환하고, 방식에 따라 포트 번호도 함께 변환하는 기술이다. 내부 주소를 외부에 직접 드러내지 않는 부수적 효과는 있지만, 트래픽 허용 여부를 통제하거나 공격을 탐지하고 사용자를 인증하거나 데이터를 암호화하는 전용 보안 기술은 아니다.

선지별 해설

① O — NAT의 본질은 주소 변환이다. 주소 노출을 줄이는 효과가 있더라도 접근 제어, 침입 탐지, 인증 기능 자체를 제공하지 않으므로 이들을 대체할 수 없다는 설명이 적절하다.
② X — 틀린 표현은 '모든 보안 위협이 제거된다'이다. NAT만으로 악성코드, 허용된 통신을 이용한 공격, 내부자 위협 등을 막을 수 없다. 올바르게는 NAT를 방화벽, 침입 탐지·방지, 인증 등의 보안 통제와 함께 사용해야 한다.
③ X — 틀린 표현은 '암호화 프로토콜'이다. NAT는 주소 정보를 변환할 뿐 통신 내용을 암호화하지 않는다. 올바르게는 NAT는 주소 변환 기술이며, 암호화에는 TLS나 IPsec 같은 별도의 프로토콜이 필요하다.
④ X — 틀린 표현은 '외부 통신이 원천적으로 불가능하다'이다. 악성코드는 이미 허용된 외부 연결이나 내부에서 시작한 통신을 이용해 외부와 통신할 수 있다. 올바르게는 NAT만으로 악성코드의 외부 통신을 완전히 차단할 수 없으며 별도의 접근 제어와 탐지 정책이 필요하다.

오답 포인트

NAT가 내부 주소를 숨겨 주는 효과를 '완전한 보안 제공'으로 확대 해석하는 것이 함정이다. 특히 ②의 '모든', ④의 '원천적으로' 같은 절대 표현과 ③의 '암호화'는 NAT의 실제 기능 범위를 벗어난다.

NoteBase

다시 나오면 이렇게 판단

선지의 기능이 주소·포트 변환인지 먼저 확인한다. 접근 제어, 공격 탐지, 사용자 인증, 내용 암호화, 악성 통신의 완전 차단을 NAT의 고유 기능이라고 하면 틀린 설명으로 판단한다.

암기 포인트

NAT는 주소 변환이지 방화벽·IDS·인증·암호화가 아니다.

11. DES/3DES에 대한 설명으로 가장 적절하지 않은 것은?

① 3DES는 DES의 동일한 암호키를 3번 반복(암호키-암호키-암호키)한다.

② 라운드(Round)라는 암호화의 한 단계를 16회 반복한다.

③ 기본구조는 페이스텔 네트워크(Feistel Network) 또는 페이스텔 암호(Feistel Cipher)라고 한다.

④ 규격상으로 DES의 키는 총 64비트이지만 각 바이트의 마지막 1비트씩 총 8비트가 패리티비트로 사용되어 실제 암호화에 쓰이는 키 길이는 56비트이다.

정답 1번

출제 포인트

이 문제는 DES의 기본 구조와 3DES의 키 사용 방식을 구별하는 문제이다.

핵심 개념

DES: 64비트 블록을 처리하는 16라운드 페이스텔 구조의 대칭키 암호이며, 64비트 키 중 8비트는 패리티 비트이므로 실제 암호화 키 길이는 56비트이다.
3DES: DES 연산을 보통 암호화-복호화-암호화(EDE) 순서로 세 번 적용하며, 2키 방식은 K1-K2-K1, 3키 방식은 K1-K2-K3를 사용한다. 세 단계에 모두 같은 키를 쓰면 중간의 역연산이 상쇄되어 단일 DES와 같은 효과가 나므로 3DES의 보안 강화 방식이라고 할 수 없다.

NoteBase

선지별 해설

① X
틀린 표현은 'DES의 동일한 암호키를 3번 반복'한다는 부분이다. 올바르게는 3DES는 DES를 세 번 적용하되, 일반적으로 EDE 구조에서 2개의 키(K1-K2-K1) 또는 3개의 키(K1-K2-K3)를 사용한다. 동일한 키로 EDE를 수행하면 단일 DES와 같은 결과가 되어 보안 강화를 이루지 못한다.

② O
DES는 페이스텔 구조의 라운드 함수를 16회 반복하여 암호화한다.

③ O
DES의 기본 구조는 입력 블록을 좌우로 나누고 라운드마다 한쪽에 함수 연산을 적용해 결합하는 페이스텔 네트워크이며, 페이스텔 암호라고도 한다.

④ O
DES 키는 형식상 64비트이지만 8바이트 각각의 마지막 1비트가 패리티 검사용이므로 패리티 비트는 총 8비트이다. 따라서 실제 암호화에 쓰이는 유효 키 길이는 56비트이다.

오답 포인트

'3DES는 DES를 세 번 수행한다'는 사실을 '동일한 키를 세 번 쓴다'로 바꾸어 놓은 ①의 표현이 함정이다. 반복되는 것은 DES 연산이며, 보안 강화를 위해 단계별 키 조합을 구별해야 한다.

다시 나오면 이렇게 판단

DES 관련 선지에서는 16라운드, 페이스텔 구조, 형식상 64비트·유효 56비트를 먼저 확인한다. 3DES에서는 EDE 연산 순서와 2키 방식(K1-K2-K1)·3키 방식(K1-K2-K3)을 확인하고, 세 단계 모두 같은 키라는 설명은 단일 DES로 축약되므로 틀린 것으로 판단한다.

암기 포인트

DES는 16라운드·페이스텔·유효 56비트, 3DES는 EDE와 2키 또는 3키 방식이다.

NoteBase

12. 원격 근무자가 기관 내부 시스템에 접속하기 위해 VPN을 사용한다. 이에 대한 설명으로 가장 적절한 것은?

① VPN은 원격 단말의 악성코드 감염 여부와 무관하게 모든 접근을 신뢰하게 만든다.

② VPN은 방화벽 정책과 동시에 사용할 수 없다.

③ VPN을 쓰면 계정 탈취 위험은 사라진다.

④ VPN은 통신 구간 보호와 내부 접근 경로 제공에 도움을 주지만, 사용자 인증·단말 상태 점검, 접근 권한 통제와 함께 운영해야 한다.

정답 4번

출제 포인트

VPN이 보호하는 통신 구간과 VPN만으로 해결할 수 없는 단말·계정·접근권한 보안을 구분하는 문제이다.

핵심 개념

VPN은 공용망을 통해 원격 단말과 기관 내부망 사이에 암호화된 논리적 통신 경로를 만드는 기술이다. 통신 내용 보호와 안전한 접속 경로 제공에는 도움이 되지만, 원격 단말의 악성코드 감염 여부나 계정 탈취 가능성까지 자동으로 해결하지는 않는다. 따라서 방화벽, 사용자 인증, 단말 상태 점검, 최소 권한에 따른 접근 통제를 함께 적용해야 한다.

선지별 해설

① X — 틀린 표현은 '악성코드 감염 여부와 무관하게 모든 접근을 신뢰하게 만든다'이다. VPN은 통신 경로를 보호할 뿐 원격 단말 자체를 신뢰 가능한 상태로 바꾸지 않는다. 올바르게는 단말의 악성코드 감염 여부와 보안 상태를 별도로 점검하고, 안전한 단말에 필요한 범위의 접근만 허용해야 한다.

② X — 틀린 표현은 '방화벽 정책과 동시에 사용할 수 없다'이다. VPN과 방화벽은 함께 사용할 수 있으며, 방화벽 정책으로 VPN 사용자의 접속 대상·포트·서비스를 제한할 수 있다. 올바르게는 VPN과 방화벽을 상호 보완적으로 운영해야 한다.

③ X — 틀린 표현은 '계정 탈취 위험은 사라진다'이다. VPN을 사용해도 비밀번호 유출, 피싱, 인증정보 탈취 등으로 계정이 악용될 수 있다. 올바르게는 다중요소 인증과 계정 관리로 탈취 위험을 줄여야 한다.

④ O — VPN은 통신 구간을 보호하고 원격 사용자가 내부망에 접속할 수 있는 경로를 제공한다. 그러나 이것만으로 단말과 사용자를 완전히 신뢰할 수는 없으므로 사용자 인증, 단말 상태 점검, 접근권한 통제를 함께 운영해야 한다.

NoteBase

오답 포인트

VPN을 사용하면 접속 주체와 단말까지 모두 안전해진다고 과대평가하기 쉽다. 특히 ①의 '모든 접근을 신뢰', ③의 '위험은 사라진다' 같은 절대 표현이 함정이다. VPN은 통신 구간 보호 수단이지 단말 보안·계정 보안·권한 통제 전체를 대신하는 수단이 아니다.

다시 나오면 이렇게 판단

VPN 관련 선지는 먼저 보호 대상을 확인한다. '통신 구간의 기밀성·무결성 및 안전한 접속 경로'에 관한 설명이면 타당할 수 있지만, '단말을 무조건 신뢰한다', '계정 탈취가 사라진다', '방화벽과 병행할 수 없다'처럼 다른 보안 통제를 불필요하게 만든다는 설명은 틀린 것으로 판단한다.

암기 포인트

VPN은 안전한 통신 경로를 제공하지만, 단말·계정·권한까지 자동으로 안전하게 만들지는 않는다.

NoteBase

13. 침해 사고 조사에서 서버 로컬 로그가 삭제되어 원인 분석이 어렵다. 향후 재발 방지를 위한 방안으로 가장 적절한 것은?
① 로그를 남기지 않도록 설정한다.
② 중앙 로그 서버 또는 SIEM으로 전송하고, 시간 동기화와 접근 통제를 적용한다.
③ 관리자 계정으로 누구나 로그를 수정할 수 있게 한다.
④ 로그 저장 기간을 1시간으로 줄인다.

정답 2번

출제 포인트

이 문제는 침해 사고 분석에 필요한 로그의 가용성과 무결성을 확보하는 중앙 집중형 로그 관리 방안을 묻는다.

핵심 개념

중앙 집중형 로그 관리는 각 서버의 로그를 별도 로그 서버나 SIEM으로 전송하여 한곳에서 보관·분석하는 방식이다. 원본 서버가 침해되거나 로컬 로그가 삭제되어도 조사 자료를 확보하려면 로그의 원격 전송, 시간 동기화, 접근 통제, 적정 기간 보존이 함께 적용되어야 한다.

선지별 해설

① X — '로그를 남기지 않도록' 설정하면 사고 원인과 공격 경로를 확인할 증거가 사라진다. 올바르게는 보안·시스템 로그가 생성되도록 설정하고 필요한 항목을 충분히 기록해야 한다.
② O — 로그를 중앙 로그 서버 또는 SIEM으로 전송하면 로컬 로그가 삭제되어도 별도 위치의 기록을 활용할 수 있다. 시간 동기화는 여러 장비의 사건 순서를 정확히 맞추고, 접근 통제는 로그의 무단 수정·삭제를 막으므로 재발 방지 방안으로 가장 적절하다.
③ X — '관리자 계정으로 누구나' 로그를 수정하게 하면 로그의 무결성과 책임 추적성이 훼손된다. 올바르게는 최소 권한 원칙에 따라 승인된 담당자만 로그에 접근하게 하고, 수정·삭제 권한도 엄격히 제한해야 한다.
④ X — '저장 기간을 1시간으로' 줄이면 사고를 뒤늦게 발견했을 때 필요한 기록이 이미 삭제될 수 있다. 올바르게는 조직의 보안 정책과 사고 조사 필요 기간에 맞추어 충분한 보존 기간을 설정해야 한다.

오답 포인트

핵심 함정은 로그를 많이 남기는 것만으로 충분하다고 보는 데 있다. 이 문항에서는 로컬 로그 삭제가 문제이므로 별도 서버로의 중앙 전송이 필요하고, 서로 다른 장비의 기록을 연결하기 위한 시간 동기화와 로그 변조를 막는 접근 통제까지 갖추어야 한다.

NoteBase

다시 나오면 이렇게 판단

사고 조사용 로그 대책은 '기록 생성 → 별도 위치로 중앙 전송 → 시간 동기화 → 접근 통제 → 충분한 기간 보존'의 흐름으로 판단한다. 로그를 끄거나, 누구나 수정하게 하거나, 보존 기간을 지나치게 줄이는 방안은 배제한다.

암기 포인트

로그 증거 보전의 핵심은 중앙 전송, 시간 동기화, 접근 통제, 충분한 보존이다.

NoteBase

14. IPv4 주소를 CIDR 방식으로 211.222.100.150/26인 단말기가 속한 서브 네트워크의 브로드캐스트 IP로 가장 적절한 것은?
① 211.222.100.128
② 211.222.100.223
③ 211.222.100.191
④ 211.222.100.255

정답 3번

출제 포인트

CIDR 프리픽스 /26으로 서브넷의 주소 범위를 구한 뒤, 그 범위의 마지막 주소인 브로드캐스트 IP를 찾는 문제이다.

조건 정리

주어진 IP 주소: 211.222.100.150
프리픽스 길이: /26
구해야 할 값: 해당 단말기가 속한 서브넷의 브로드캐스트 IP
주의할 조건: 브로드캐스트 주소는 해당 서브넷 범위의 마지막 주소이다.

사용할 공식

서브넷 마스크: 255.255.255.192
마지막 옥텟의 블록 크기: 256 − 192 = 64

/26은 마지막 옥텟을 64개씩 나누므로 주소 범위는 0~63, 64~127, 128~191, 192~255가 된다. 마지막 옥텟 150은 128~191 구간에 속하므로 이 구간의 마지막 주소가 브로드캐스트 주소이다.

계산 과정

1. /26의 서브넷 마스크는 255.255.255.192이다.
2. 블록 크기는 256 − 192 = 64이다.
3. 마지막 옥텟 150은 128 ≤ 150 ≤ 191이므로 네트워크 범위는 211.222.100.128~211.222.100.191이다.
4. 이 범위의 마지막 주소인 211.222.100.191이 브로드캐스트 IP이다.

NoteBase

선지 판단

① X — 211.222.100.128은 해당 /26 서브넷의 첫 주소인 네트워크 주소이다. 틀린 표현은 '브로드캐스트 IP가 211.222.100.128'이며, 올바르게는 '네트워크 IP가 211.222.100.128'이다.
② X — 211.222.100.223은 150이 속한 128~191 범위 밖의 주소이다. 틀린 표현은 '브로드캐스트 IP가 211.222.100.223'이며, 올바른 브로드캐스트 IP는 211.222.100.191이다.
③ O — 211.222.100.191은 150이 속한 128~191 범위의 마지막 주소이므로 브로드캐스트 IP이다.
④ X — 211.222.100.255는 다음 /26 서브넷인 192~255 범위의 브로드캐스트 주소이다. 틀린 표현은 '이 단말기의 서브넷 브로드캐스트 IP가 211.222.100.255'이며, 올바르게는 '211.222.100.192/26 서브넷의 브로드캐스트 IP가 211.222.100.255'이다.

계산 결과 브로드캐스트 IP는 211.222.100.191이므로 정답은 3번이다.

오답 포인트

①의 128은 서브넷의 시작점이어서 브로드캐스트 주소가 아니라 네트워크 주소이다. 또한 클래스 C 주소처럼 마지막 주소를 무조건 255로 판단하면 ④를 고르게 된다. /26에서는 마지막 옥텟을 64개 단위로 나눈 뒤, 주어진 IP가 포함된 구간의 끝값을 찾아야 한다.

다시 나오면 이렇게 판단

CIDR 문제는 서브넷 마스크 확인 → 블록 크기 계산 → 주어진 IP가 속한 범위 결정 → 범위의 첫 주소는 네트워크 주소, 마지막 주소는 브로드캐스트 주소의 순서로 판단한다.

암기 포인트

/26은 한 블록이 64개이며 경계는 0, 64, 128, 192이다. 각 블록의 끝값 63, 127, 191, 255가 브로드캐스트 주소가 된다.

NoteBase

15. IPv6에서 지원하는 주소 종류로 가장 적절하지 않은 것은?
① Unicast
② Anycast
③ Broadcast
④ Multicast

정답 3번

출제 포인트

IPv6가 지원하는 주소 지정 방식과 지원하지 않는 브로드캐스트를 구별하는 문제이다.

핵심 개념

유니캐스트(Unicast)는 하나의 인터페이스로 전달하는 일대일 방식이다.
애니캐스트(Anycast)는 같은 주소를 공유하는 여러 인터페이스 중 라우팅상 가장 가까운 하나로 전달하는 방식이다.
멀티캐스트(Multicast)는 특정 그룹에 속한 여러 인터페이스로 전달하는 방식이다.
IPv6는 유니캐스트·애니캐스트·멀티캐스트를 지원하지만 브로드캐스트(Broadcast)는 지원하지 않는다.

선지별 해설

① O — Unicast는 IPv6가 지원하는 주소 유형으로, 패킷을 특정한 하나의 인터페이스에 전달한다.
② O — Anycast는 IPv6가 지원하는 주소 유형으로, 동일한 애니캐스트 주소를 가진 인터페이스들 중 라우팅상 가장 가까운 하나에 전달한다.
③ X — Broadcast는 IPv6가 지원하는 주소 유형이 아니다. 틀린 표현은 'Broadcast'이며, 올바르게는 IPv6에서 여러 수신자에게 전달할 때 Multicast를 사용한다.
④ O — Multicast는 IPv6가 지원하는 주소 유형으로, 특정 멀티캐스트 그룹에 속한 여러 인터페이스에 전달한다.

오답 포인트

IPv4에서 사용하던 Broadcast도 IPv6에 그대로 존재한다고 생각하기 쉽다. 그러나 IPv6는 Broadcast를 없애고 그룹 전달에는 Multicast를 사용한다.

다시 나오면 이렇게 판단

IPv6 주소 유형을 묻는 경우 Unicast·Anycast·Multicast는 지원하고 Broadcast는 지원하지 않는다는 기준으로 판단한다.

NoteBase

암기 포인트

IPv6는 UAM(Unicast·Anycast·Multicast), Broadcast는 제외이다.

NoteBase

16. 침입차단 시스템에 대한 설명으로 가장 적절하지 않은 것은?

① DMZ 네트워크 구성에서 외부 침입차단 시스템은 인터넷이나 다른 WAN으로 연결되는 경계 라우터의 바로 안쪽 로컬 네트워크나 엔터프라이즈 네트워크 끝에 위치한다.

② IPSec을 침입차단 시스템 내부에서 구현할 때 침입차단 시스템은 양방향에서 암호화된 VPN 트래픽에 대해서 필터링 기능이나 접근통제, 로깅, 바이러스 스캐닝과 같은 보안기능을 수행할 수 있다.

③ VPN에서는 안전하지 않는 다른 네크워크인 인터넷을 통한 안전한 연결을 위해 하위 프로토콜 계층에서 암호와 인증을 사용한다.

④ 외부 공격으로부터 서버등을 보호해야 하기 때문에 DMZ 네트워크 구성에서 내부 침입차단 시스템은 외부 차단 시스템보다 더 엄격한 필터링 능력을 갖고 있다.

정답 2번

출제 포인트

침입차단 시스템의 배치 위치에 따라 암호화된 VPN 트래픽의 내부 내용을 검사할 수 있는지를 묻는 문제이다.
발문이 '가장 적절하지 않은 것'을 요구하므로 틀린 설명을 고른다.

핵심 개념

DMZ는 외부에 공개할 서버를 내부 네트워크와 분리하여 두는 완충 네트워크이다.
침입차단 시스템은 통과 트래픽을 정책에 따라 허용·차단하고 기록하지만, 암호화된 패킷의 내부 내용은 복호화하지 않으면 검사할 수 없다.
VPN은 인터넷과 같은 신뢰할 수 없는 네트워크를 통과할 때 암호화와 인증으로 논리적인 안전 통신 경로를 만든다.

NoteBase

선지별 해설

① O — 외부 침입차단 시스템은 인터넷이나 다른 WAN과 연결되는 경계 지점, 즉 경계 라우터의 안쪽이나 기업 네트워크의 외곽에 배치하여 외부에서 들어오는 트래픽을 우선 통제한다.

② X — 틀린 표현은 '양방향에서 암호화된 VPN 트래픽에 대해 필터링 기능이나 접근 통제, 로깅, 바이러스 스캐닝과 같은 보안 기능을 수행할 수 있다'이다. IPSec 종단 장치가 침입차단 시스템의 내부에 있으면 침입차단 시스템을 지날 때 VPN 페이로드가 아직 암호화되어 있으므로 그 내부 내용을 대상으로 한 접근 통제나 바이러스 검사를 수행할 수 없다. 올바르게는 '외부 IP 헤더와 IPSec 프로토콜을 기준으로 제한적인 허용·차단 및 연결 로깅은 할 수 있지만, VPN 트래픽의 내부 내용을 검사하려면 먼저 IPSec 트래픽을 복호화해야 한다'이다.

③ O — VPN은 인터넷처럼 안전하지 않은 공중망을 경유하더라도 하위 프로토콜 계층에서 암호화와 인증을 적용하여 데이터의 기밀성과 통신 상대의 신뢰성을 확보한다.

④ O — DMZ가 침해되더라도 내부 네트워크로 공격이 확산되지 않도록 내부 침입차단 시스템에는 외부 침입차단 시스템보다 더 엄격한 통과 정책을 적용한다.

오답 포인트

②는 'IPSec이 보안 기능을 제공한다'는 사실과 '침입차단 시스템이 암호화된 내용까지 검사할 수 있다'는 주장을 섞은 선지이다. 암호화 자체는 통신을 보호하지만, 복호화 지점보다 앞에 있는 장비에는 오히려 상세 검사를 제한한다.

다시 나오면 이렇게 판단

VPN과 침입차단 시스템의 위치 관계를 그린 뒤, 트래픽이 해당 장비를 통과하는 시점에 암호화 상태인지 복호화 상태인지 판단한다. 암호화 상태라면 외부 헤더 중심의 통제만 가능하고, 내부 데이터 검사와 바이러스 스캐닝은 복호화 이후에 가능하다.

암기 포인트

DMZ는 외부와 내부 사이의 완충 구역이고, 암호문은 복호화 전에는 내용 검사가 불가능하다.

NoteBase

17. 다음은 Ping 명령의 실행 결과이다. 이에 대한 설명으로 가장 적절하지 않은 것은?

```
Ping www.google.com [142.251.157.119] 32바이트 데이터 사용:
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=42ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=39ms TTL=114
142.251.157.119의 응답: 바이트=32 시간=40ms TTL=114

142.251.157.119에 대한 Ping 통계:
    패킷: 보냄 = 5, 받음 = 5, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 39ms, 최대 = 42ms, 평균 = 39ms
```

① 명령 프롬프트에서 'ping - t 5 www.google.com' 실행하면 된다.

② IP 패킷의 유효기간이 114이며 메시지가 5개 반복된 것은 테스트를 5회 했음을 나타낸다.

③ 서버의 FQDN(Fully Qualified Domain Name)인 www.google.com과의 사이에서 응답 테스트용 메시지를 송수신했음을 나타낸다.

④ IPv4주소 142.251.157.119로부터 응답이 있고 데이터의 크기는 32바이트, ping 테스트의 송신부터 수신까지 패킷 손실은 없음을 나타낸다.

정답 1번

출제 포인트

이 문제는 Windows Ping 실행 결과에서 실행 횟수, 응답 주소, 데이터 크기, TTL, 패킷 손실 정보를 읽고 명령 옵션의 의미와 대조하는 문제이다.

자료 읽는 순서

1. 첫 줄에서 대상 도메인 www.google.com, 변환된 IPv4 주소 142.251.157.119, 데이터 크기 32바이트를 확인한다.
2. 응답 줄에서 응답 횟수 5회와 각 응답의 TTL=114를 확인한다.
3. Ping 통계에서 보냄 5, 받음 5, 손실 0을 확인한 뒤 각 선지의 명령 옵션 및 해석과 대조한다.

핵심 근거

화면에는 응답이 5회 표시되고 통계에도 보냄 5, 받음 5로 나타난다. Windows Ping에서 전송 횟수를 5회로 지정하는 옵션은 -n 5이다. -t는 횟수를 지정하는 옵션이 아니라 사용자가 중단할 때까지 계속 Ping을 보내는 옵션이다.

NoteBase

선지별 해설

① X
- 첫 줄과 통계에는 5회 실행 결과가 제시되어 있지만, Windows 명령에서 -t는 반복 횟수 5회를 지정하지 않는다. 틀린 표현인 'ping -t 5 www.google.com'은 'ping -n 5 www.google.com'으로 고쳐야 한다.

② O
- 각 응답 줄에 TTL=114가 반복되고, 응답 줄이 5개이며 통계에도 보냄 5, 받음 5가 표시된다. 따라서 화면에 나타난 TTL 값은 114이고 테스트 결과는 5회이다.

③ O
- 첫 줄의 'Ping www.google.com [142.251.157.119]'는 FQDN인 www.google.com이 IPv4 주소로 해석되었음을 보여 주며, 이어지는 5개의 응답 줄은 해당 대상과 ICMP 응답 메시지를 주고받은 결과이다.

④ O
- 각 응답 줄에는 142.251.157.119의 응답과 바이트=32가 표시된다. 통계에는 보냄 5, 받음 5, 손실 0(0% 손실)이 나타나므로 송신부터 수신까지 패킷 손실이 없다.

오답 포인트

①의 숫자 5만 보고 -t를 5회 반복 옵션으로 오해하기 쉽다. 화면의 5회 실행 결과와 명령 옵션은 따로 판단해야 하며, Windows에서는 횟수 지정이 -n이고 -t는 중단할 때까지 계속 실행한다.

다시 나오면 이렇게 판단

Ping 결과 문제에서는 먼저 대상 주소, 바이트, 시간, TTL을 응답 줄에서 읽고, 보냄·받음·손실은 통계에서 확인한다. 그다음 Windows 옵션에서 -n은 횟수 지정, -t는 계속 실행이라는 구분을 적용한다.

암기 포인트

Windows Ping은 -n이 횟수, -t가 계속 실행이다. 보냄=받음이면 손실은 0%이다.

NoteBase

18. 2.4GHz 대역과 5GHz 대역 2개의 채널을 지원하며, 최대 600Mbps까지의 속도까지 지원하는 무선랜 표준에 대한 설명으로 가장 적절한 것은?
① 802.11a
② 802.11b
③ 802.11g
④ 802.11n

정답 4번

출제 포인트

무선랜 규격별 지원 주파수 대역과 최대 전송속도를 구분하는 문제이다.

핵심 개념

802.11a는 5*GHz* 대역에서 최대 54*Mbps*를 지원한다.
802.11b는 2.4*GHz* 대역에서 최대 11*Mbps*를 지원한다.
802.11g는 2.4*GHz* 대역에서 최대 54*Mbps*를 지원한다.
802.11n은 2.4*GHz*와 5*GHz* 대역을 모두 사용할 수 있고, MIMO와 채널 결합 등을 통해 이론상 최대 600*Mbps*를 지원한다.

선지별 해설

① X — 802.11a는 5*GHz* 대역만 사용하며 최대 속도도 54*Mbps*이다. 틀린 표현인 '두 대역 지원 및 최대 600*Mbps*'는 '5*GHz* 대역 지원 및 최대 54*Mbps*'로 고쳐야 한다.
② X — 802.11b는 2.4*GHz* 대역만 사용하며 최대 속도는 11*Mbps*이다. 틀린 표현인 '두 대역 지원 및 최대 600*Mbps*'는 '2.4*GHz* 대역 지원 및 최대 11*Mbps*'로 고쳐야 한다.
③ X — 802.11g는 2.4*GHz* 대역만 사용하며 최대 속도는 54*Mbps*이다. 틀린 표현인 '두 대역 지원 및 최대 600*Mbps*'는 '2.4*GHz* 대역 지원 및 최대 54*Mbps*'로 고쳐야 한다.
④ O — 802.11n은 2.4*GHz*와 5*GHz* 대역을 모두 지원하며 이론상 최대 600*Mbps*까지 지원하므로 제시된 조건과 일치한다.

오답 포인트

802.11a도 5*GHz* 대역을 사용하므로 ①을 고르기 쉽지만, 2.4*GHz* 대역을 함께 지원하지 않고 최대 속도도 54*Mbps*이다. 두 대역 지원과 최대 600*Mbps*라는 조건을 동시에 만족하는 규격은 802.11n이다.

NoteBase

다시 나오면 이렇게 판단

먼저 주파수 대역을 확인하고 다음으로 최대 속도를 대조한다. ‘2.4*GHz*와 5*GHz* 모두 지원’ 및 ‘최대 600*Mbps*’가 함께 제시되면 802.11n으로 판단한다.

암기 포인트

a는 5*GHz*·54*Mbps*, b는 2.4*GHz*·11*Mbps*, g는 2.4*GHz*·54*Mbps*, n은 두 대역·최대 600*Mbps*이다.

NoteBase

19. 기관 내부 사용자가 정상 도메인을 입력했는데 악성 사이트로 이동했다. 내부 DNS 캐시가 오염되었을 가능성이 있다. 이에 대한 대응으로 가장 적절한 것은?

① DNS는 UDP를 사용하므로 보안 검토 대상이 아니다.

② DNSSEC 검증, 신뢰 가능한 재귀 DNS 사용, 캐시 무결성 점검, 의심 레코드 삭제 및 로그 분석을 수행한다.

③ 사용자 브라우저 캐시만 삭제하면 충분하다.

④ TLS 인증서 검증은 DNS와 무관하므로 확인할 필요가 없다.

정답 2번

출제 포인트

이 문제는 DNS 캐시 오염이 의심될 때의 적절한 대응과 관련 보안 통제의 역할을 묻는 문제이다.

핵심 개념

DNS 캐시 오염은 공격자가 변조된 DNS 응답을 캐시에 저장하게 하여 정상 도메인을 악성 IP 주소로 연결시키는 공격이다.
DNSSEC은 DNS 응답에 대한 디지털 서명을 검증하여 데이터의 출처 인증과 무결성을 확인한다.
대응의 핵심은 오염 범위를 확인하고, 신뢰 가능한 재귀 DNS를 사용하며, 의심 레코드를 제거하고 로그를 분석하는 것이다. 브라우저 캐시 삭제만으로는 운영체제·내부 DNS 서버·재귀 DNS의 캐시 오염을 해결할 수 없다.

NoteBase

선지별 해설

① X
DNS가 주로 UDP를 사용한다는 사실은 보안 검토 대상에서 제외할 근거가 아니다. UDP 기반 DNS도 응답 위조와 캐시 오염의 대상이 된다. 틀린 표현은 '보안 검토 대상이 아니다'이며, 올바르게는 DNS 캐시와 응답의 무결성을 반드시 점검해야 한다.

② O
DNSSEC 검증으로 서명된 DNS 데이터의 무결성과 출처를 확인하고, 신뢰 가능한 재귀 DNS를 사용하며, 캐시 무결성을 점검하고 의심 레코드를 삭제한 뒤 로그를 분석하는 것은 오염 확인·제거·원인 추적을 함께 수행하는 적절한 대응이다.

③ X
사용자 브라우저 캐시만 삭제하면 브라우저 외부의 운영체제 DNS 캐시, 내부 DNS 서버 캐시 또는 재귀 DNS 캐시에 남은 오염을 제거하지 못한다. 틀린 표현은 '브라우저 캐시만 삭제하면 충분하다'이며, 올바르게는 DNS 캐시 계층 전반을 점검하고 오염된 레코드를 제거해야 한다.

④ X
DNS와 TLS는 별도 계층의 기술이지만, DNS 오염으로 악성 사이트에 연결되었을 때 TLS 인증서 검증은 접속 대상의 신원을 확인하고 부정한 인증서를 탐지하는 중요한 방어 수단이다. 틀린 표현은 'DNS와 무관하므로 확인할 필요가 없다'이며, 올바르게는 TLS 인증서의 유효성, 도메인 일치 여부와 신뢰 체인을 확인해야 한다.

오답 포인트

③처럼 눈앞의 브라우저만 초기화하면 해결된다고 생각하거나, ④처럼 DNS와 TLS가 서로 다른 기술이라는 이유로 인증서 검증까지 무관하다고 판단하기 쉽다. 그러나 DNS 캐시는 여러 계층에 존재하며, TLS 인증서 검증은 잘못된 목적지로 유도된 뒤에도 서버 신원을 확인하는 별도의 방어선이다.

다시 나오면 이렇게 판단

DNS 캐시 오염 대응 선지는 '검증, 범위 확인, 제거, 추적'의 네 요소로 판단한다. DNSSEC 등으로 응답을 검증하고, 브라우저에 한정하지 않고 캐시 계층 전체를 확인하며, 의심 레코드를 제거하고, 로그로 유입 경로와 영향을 추적하는 대책이 적절하다.

암기 포인트

DNS 오염 대응은 'DNSSEC 검증 → 캐시 전반 점검·삭제 → 로그 추적'이며, TLS 인증서 검증도 별도의 방어선이다.

20. 사용자가 공공기관 사이트 접속 중 브라우저에서 “인증서 이름이 사이트 주소와 일치하지 않음” 경고를 보았다. 이에 대한 보안 판단으로 가장 적절한 것은?
① 암호화는 적용되므로 경고를 무시해도 된다.
② 서버 인증서의 주체 이름 또는 SAN(Subject Alternative Name)과 접속 도메인이 맞지 않아 서버 인증이 실패한 상황일 수 있으며, 중간자 공격 가능성도 고려해야 한다.
③ HTTPS는 인증서 검증을 수행하지 않는다.
④ 인증서 경고는 네트워크 속도 문제만 의미한다.

정답 2번

출제 포인트

이 문제는 HTTPS 접속 시 서버 인증서의 도메인 이름 검증이 서버 신원 확인과 중간자 공격 방지에 어떤 역할을 하는지 묻는 문제이다.

핵심 개념

HTTPS는 TLS를 이용하여 통신을 암호화하고, 브라우저는 인증서의 유효성·신뢰 경로와 함께 인증서에 표시된 호스트 이름이 접속한 도메인과 일치하는지 확인한다.
도메인 이름 불일치는 인증서가 접속하려는 서버용으로 발급된 것이 아닐 수 있음을 뜻한다. 따라서 서버 신원을 신뢰할 수 없으며, 잘못 설정된 인증서뿐 아니라 공격자가 다른 인증서를 제시하는 중간자 공격 가능성도 고려해야 한다.

NoteBase

선지별 해설

① X
암호화가 적용되더라도 통신 상대의 신원이 확인되지 않으면 공격자와 암호화된 연결을 맺을 수 있으므로 경고를 무시해서는 안 된다. 틀린 표현은 '경고를 무시해도 된다'이다. 올바르게는 암호화 여부와 별개로 인증서의 도메인 일치 여부를 확인하고, 불일치 경고가 발생한 연결은 중단해야 한다.

② O
서버 인증서의 주체 이름 또는 SAN에 표시된 이름과 접속 도메인이 일치하지 않으면 해당 서버의 신원을 정상적으로 확인할 수 없다. 이는 단순한 인증서 설정 오류일 수도 있지만 다른 인증서를 제시하는 중간자 공격의 징후일 수도 있으므로 경고를 심각하게 보아야 한다.

③ X
HTTPS는 TLS 연결 과정에서 인증서의 신뢰성과 접속 호스트 이름의 일치 여부를 검증하여 서버를 인증한다. 틀린 표현은 '인증서 검증을 수행하지 않는다'이다. 올바르게는 HTTPS는 인증서 검증을 수행하며, 검증 실패 시 브라우저가 보안 경고를 표시한다.

④ X
인증서 경고는 네트워크 속도 문제가 아니라 서버 신원과 연결의 안전성을 확인하지 못했다는 보안 문제를 의미한다. 틀린 표현은 '네트워크 속도 문제만 의미한다'이다. 올바르게는 인증서 경고는 인증서 만료, 신뢰되지 않는 발급자, 도메인 불일치 등 인증서 검증 실패를 의미한다.

오답 포인트

①의 '암호화됨'과 '상대방의 신원이 확인됨'을 같은 의미로 보는 것이 핵심 함정이다. 암호화는 전송 내용을 보호하지만, 인증서 검증이 실패하면 그 암호화된 연결의 상대가 공격자일 가능성을 배제할 수 없다.

다시 나오면 이렇게 판단

인증서 경고 문제에서는 먼저 유효기간, 발급자 신뢰, 도메인 이름 일치 여부를 구분한다. 접속 도메인과 인증서 이름이 다르면 서버 인증 실패로 판단하고, 단순 속도 문제가 아니라 잘못된 설정이나 중간자 공격 가능성을 검토한다.

암기 포인트

HTTPS의 암호화는 내용 보호, 인증서의 이름 검증은 서버 신원 확인이다. 도메인 불일치는 서버 인증 실패 신호이다.

NoteBase

21. 내부 업무 시스템에서 일반 사용자가 다음 URL의 숫자만 바꾸어 다른 부서 문서를 조회할 수 있었다. 개발팀은 "로그인한 사용자만 접근 가능하므로 인증 문제는 없다"고 주장한다. 판단으로 가장 적절한 것은?

- https://intra.example/doc/1001
- https://intra.example/doc/1002

① 인증이 성공했으므로 보안 취약점이 아니다.
② TLS가 적용되어 있으면 문서 번호 변경 공격은 방지된다.
③ 인증과 인가는 다르며, 객체 단위 권한 검증이 서버 측에서 수행되지 않은 접근제어 실패로 보아야 한다.
④ URL을 복잡하게 만들면 서버 측 권한 검사는 생략할 수 있다.

정답 3번

출제 포인트

이 문제는 로그인 여부를 확인하는 인증과, 특정 문서 객체에 접근할 권한이 있는지를 확인하는 인가를 구분하고 객체 단위 접근통제 실패를 판단하는 문제이다.

사례 정리

핵심 사실 1: 일반 사용자가 URL의 문서 번호를 1001에서 1002로 바꾸어 다른 부서 문서를 조회할 수 있었다.
핵심 사실 2: 개발팀은 로그인한 사용자만 접근할 수 있다는 점을 근거로 인증에는 문제가 없다고 주장한다.
판단에 중요한 조건: 로그인 성공 후에도 서버가 요청된 각 문서에 대한 사용자의 열람 권한을 별도로 검사했는지가 핵심이다.

핵심 개념

인증은 사용자가 누구인지 확인하는 절차이고, 인가는 인증된 사용자가 특정 자원에 대해 허용된 행위를 할 수 있는지 확인하는 절차이다.
객체 단위 접근통제는 문서 번호와 같은 객체 식별자가 요청될 때마다 서버가 해당 사용자의 그 객체에 대한 권한을 검증하는 것이다. 이 검사가 없으면 식별자를 바꾸어 다른 객체에 접근하는 객체 직접 참조 취약점이 발생할 수 있다.

NoteBase

적용 기준

URL에 포함된 문서 번호는 클라이언트가 임의로 변경할 수 있는 입력값이다. 따라서 서버는 로그인 여부만 확인해서는 안 되고, 매 요청마다 현재 사용자가 그 문서를 열람할 권한이 있는지 객체 단위로 검사해야 한다.

선지별 해설

① X
인증이 성공했다는 사실은 사용자의 신원만 확인되었다는 뜻이며, 모든 문서에 대한 접근 권한까지 부여되었다는 뜻은 아니다. '보안 취약점이 아니다'가 틀린 표현이다. 올바르게는 인증 후에도 각 문서에 대한 인가 검사가 없으므로 접근통제 취약점이다.

② X
TLS는 통신 구간의 기밀성과 무결성을 보호하지만, 로그인한 사용자가 URL의 문서 번호를 바꾸어 보내는 행위나 서버의 잘못된 권한 판단을 막지 못한다. '문서 번호 변경 공격은 방지된다'가 틀린 표현이다. 올바르게는 TLS 적용 여부와 별개로 서버가 객체 단위 권한을 검사해야 한다.

③ O
인증과 인가는 서로 다른 통제이다. 서버가 사용자의 신원은 확인했더라도 요청한 문서 객체에 대한 열람 권한을 검사하지 않았다면 객체 단위 접근제어 실패로 보아야 한다.

④ X
URL을 복잡하게 만드는 것은 식별자를 추측하기 어렵게 할 뿐 권한 검사를 대신하지 못한다. '서버 측 권한 검사는 생략할 수 있다'가 틀린 표현이다. 올바르게는 URL의 형태나 복잡성과 관계없이 서버가 요청된 객체에 대한 권한을 검사해야 한다.

오답 포인트

출제자가 노린 함정은 '로그인했다'는 사실을 '모든 문서에 접근할 권한이 있다'는 뜻으로 오해하게 만드는 데 있다. 또한 TLS나 복잡한 URL은 각각 전송 보호와 추측 난이도에 관한 수단일 뿐, 서버 측 인가를 대체하지 못한다.

다시 나오면 이렇게 판단

URL, 경로, 매개변수의 객체 식별자만 바꾸어 다른 사용자의 자료를 볼 수 있는 사례에서는 먼저 서버가 '이 사용자가 이 객체에 접근할 권한이 있는가'를 매 요청마다 검사하는지 판단한다. 로그인만 확인하고 객체별 권한을 확인하지 않으면 인가 실패이다.

NoteBase

암기 포인트

인증은 '누구인가', 인가는 '무엇을 할 수 있는가'이며, 객체 번호는 숨기는 것이 아니라 서버에서 권한을 검사한다.

NoteBase

22. 악성코드와 그에 대한 설명으로 가장 적절하지 않은 것은?

① 웜 : 사용자 컴퓨터에 침입하여 파일을 암호화하고 해제를 위해 대가를 요구하는 프로그램

② 바이러스 : 사용자 컴퓨터에 몰래 실행 가능한 부분을 변형하고 복제하는 프로그램

③ 트로이 목마 : 트로이 목마가 직접 컴퓨터에 영향을 주기보다는 악의적인 공격자가 해당 프로그램을 이용하여 사용자의 컴퓨터를 조종할 수 있는 방식

④ 악성 자바 코드 : 웹 사이트의 동적 구현을 위한 자바 애플릿이 악의적인 기능으로 동작하도록 만든 코드

정답 1번

출제 포인트

웜, 바이러스, 트로이 목마, 악성 자바 코드의 정의와 공격 방식을 구별하는 문제이다.

핵심 개념

웜은 다른 실행 파일에 기생하지 않고 스스로 복제하여 주로 네트워크를 통해 확산하는 악성코드이다.
바이러스는 다른 프로그램이나 파일의 실행 가능한 부분에 감염되어 자신의 코드를 복제·전파하는 악성코드이다.
트로이 목마는 정상 프로그램처럼 위장하여 실행된 뒤 정보 탈취나 원격 조종 같은 악성 기능을 수행하는 프로그램이다.
랜섬웨어는 파일을 암호화하거나 시스템 사용을 막고 복구 대가를 요구하는 악성코드이다.
악성 자바 코드는 웹의 동적 기능에 사용되는 자바 애플릿 등이 악의적인 기능을 수행하도록 작성되거나 변조된 코드이다.

NoteBase

선지별 해설

① X
파일을 암호화하고 해제를 대가로 금전을 요구한다는 설명은 웜이 아니라 랜섬웨어의 특징이다. 틀린 표현은 '웜'이다. 올바르게는 '랜섬웨어는 사용자 컴퓨터에 침입하여 파일을 암호화하고 복구 또는 해제를 대가로 금전을 요구하는 악성코드'이다. 웜은 스스로 복제하면서 네트워크를 통해 빠르게 확산하는 악성코드이다.

② O
바이러스는 프로그램이나 파일의 실행 가능한 부분에 자신의 코드를 삽입하거나 변형하고, 감염 대상을 통해 자신을 복제·전파한다. 사용자 모르게 실행될 수 있다는 설명도 바이러스의 작동 특성과 부합한다.

③ O
트로이 목마는 정상 프로그램처럼 위장하여 사용자가 실행하게 만들고, 실행된 뒤 공격자가 피해 컴퓨터를 원격 조종하거나 정보를 빼내는 데 이용될 수 있다. 스스로 복제·확산하는 것이 핵심인 웜과 구별된다.

④ O
웹 사이트의 동적 기능을 구현하는 자바 애플릿 등이 악의적인 기능을 수행하도록 만들어진 코드는 악성 자바 코드에 해당한다.

오답 포인트

①의 '침입하여 파일을 암호화'와 '해제를 위해 대가를 요구'는 랜섬웨어를 가리키는 결정적 표현이다.
악성코드라는 공통점만 보고 이를 웜의 설명으로 받아들이면 틀린다.

다시 나오면 이렇게 판단

자기 복제·네트워크 확산이면 웜, 다른 파일에 감염·기생하면 바이러스, 정상 프로그램 위장·원격 조종이면 트로이 목마, 암호화·금전 요구이면 랜섬웨어로 구별한다.

암기 포인트

웜은 스스로 퍼지고, 바이러스는 파일에 붙고, 트로이 목마는 위장하며, 랜섬웨어는 잠그고 돈을 요구한다.

NoteBase

23. Ping Of Death 공격에 대한 설명으로 가장 적절하지 않은 것은?
① 네트워크 연결 상태를 점검하기 위한 Ping 명령을 이용한 공격방법이다.
② 수신자는 대량의 패킷을 한꺼번에 받게 되어 네트워크가 마비된다.
③ Ping 명령과 함께 가능한 긴 패킷을 같이 보내는 방법이다.
④ 누락된 패킷에 대해서는 계속적으로 재전송을 요구한다.

정답 4번

출제 포인트

Ping of Death가 비정상적으로 큰 ICMP Echo 패킷과 IP 단편 재조립을 악용하는 공격이라는 점과, 전송 계층의 재전송 방식이 아니라는 점을 묻는 문제이다.

핵심 개념

Ping of Death는 허용 한도를 넘는 비정상적인 크기의 ICMP Echo 패킷을 여러 IP 단편으로 보내고, 수신 측이 이를 재조립하는 과정에서 오류·과부하·시스템 장애를 일으키게 하는 공격이다.
Ping 명령은 원래 ICMP Echo Request와 Echo Reply를 이용해 상대 호스트의 도달 가능성과 연결 상태를 확인한다. ICMP Echo 자체는 TCP처럼 누락된 패킷의 재전송을 계속 요구하는 방식이 아니다.

선지별 해설

① O — Ping of Death는 네트워크 연결 상태를 점검하는 Ping의 ICMP Echo 기능을 악용하는 공격이므로 적절한 설명이다.
② O — 공격자가 만든 비정상적으로 큰 패킷은 여러 단편으로 전송되며, 수신 측이 많은 단편을 받아 재조립하는 과정에서 과부하나 오류가 발생해 시스템 또는 네트워크 서비스가 마비될 수 있으므로 적절한 설명이다.
③ O — 일반적인 허용 크기를 넘는 매우 긴 ICMP Echo 패킷을 만들어 단편화된 상태로 보내는 것이 이 공격의 핵심이므로 적절한 설명이다.
④ X — 틀린 표현은 '누락된 패킷에 대해서는 계속적으로 재전송을 요구한다'이다. 올바르게는 Ping of Death는 누락 패킷의 재전송을 반복시키는 공격이 아니라, 비정상적으로 큰 ICMP Echo 패킷의 단편화와 수신 측 재조립 취약점을 악용하는 공격이다.

NoteBase

오답 포인트

④의 '재전송'이라는 표현을 Ping의 반복 전송과 혼동하기 쉽다. 그러나 Ping of Death의 판단 기준은 반복적인 재전송 요구가 아니라 크기 한도를 넘는 패킷과 단편 재조립이다. 대량의 정상 Ping을 계속 보내 자원을 소진시키는 Ping Flood와도 구별해야 한다.

다시 나오면 이렇게 판단

선지에 '비정상적으로 큰 ICMP 패킷', 'IP 단편화', '재조립 과정의 오류'가 나오면 Ping of Death로 판단한다. '다량의 정상 Ping을 반복 전송'하면 Ping Flood이고, '누락 패킷의 계속적인 재전송 요구'는 Ping of Death의 핵심 원리가 아니다.

암기 포인트

Ping of Death는 큰 Ping을 쪼개 보내 재조립 단계에서 장애를 일으키는 공격이다. 핵심은 재전송이 아니라 초과 크기와 단편 재조립이다.

NoteBase

24. AES의 운영 모드에 대한 설명으로 가장 적절하지 않은 것은?

① OFB 모드는 블록을 암호화할 때마다 1씩 증가하는 카운터를 암호화 한 후에 XOR 연산으로 암호문을 만들며 암호화와 복호화가 동일하며 병렬로 처리할 수 있다.

② CBC 모드는 블록 운영 모드 중 보안성이 우수하며 블록 단위로 동작하므로 평문과 암호문의 길이가 다르다. 각 블록은 이전 암호문과 XOR 연산 후 암호화되며 첫 번째 암호문을 위해 IV가 필요하다.

③ CFB 모드는 스트림 암호처럼 동작하며 평문과 암호문의 길이가 같고 최초의 키 생성 버퍼로 IV가 필요하다. 암호화는 순차적으로 처리하지만 복호화는 병렬로 처리할 수 있다.

④ ECB 모드는 블록 단위로 순차적으로 암호화하는 가장 단순한 모드이며 블록 단위로 동작하기 때문에 평문과 암호문의 길이가 다르다. 각 블록이 독립적으로 동작하므로 한 블록에서 에러가 발생해도 다른 블록에 영향을 주지 않는다. 다만, 하나의 블록만 해독하면 나머지 블록도 해독되는 단점이 있다.

정답 1번

출제 포인트

AES의 ECB·CBC·CFB·OFB 운용 모드에서 블록 간 의존성, IV 사용, 병렬 처리 가능 여부를 구별하는 문제이다.

NoteBase

핵심 개념

ECB는 각 평문 블록을 서로 독립적으로 암호화하는 모드이다. 구조가 단순하고 병렬 처리가 가능하지만 동일한 평문 블록이 동일한 암호문 블록이 되어 패턴이 드러난다.
CBC는 현재 평문 블록을 직전 암호문 블록과 XOR한 뒤 암호화하는 모드이다. 첫 블록에는 IV가 필요하고 암호화는 앞 블록에 의존한다.
CFB는 이전 암호화 출력을 이용해 키 스트림을 만들고 평문과 XOR하는 스트림형 운용 모드이다. 암호화는 순차적이지만 복호화는 여러 블록을 병렬 처리할 수 있다.
OFB는 이전 출력 블록을 다시 암호화하여 키 스트림을 만들고 평문·암호문과 XOR하는 스트림형 운용 모드이다. 카운터를 증가시키는 방식은 OFB가 아니라 CTR의 특징이며, OFB의 키 스트림 생성은 앞 출력에 의존하므로 병렬화할 수 없다.

선지별 해설

① X — 틀린 표현은 '1씩 증가하는 카운터'와 '병렬로 처리할 수 있다'이다. OFB는 카운터가 아니라 직전 출력 블록을 다음 블록 암호화의 입력으로 사용한다. 암호화와 복호화에서 같은 키 스트림을 XOR하는 점은 맞지만, 키 스트림 블록이 연쇄적으로 생성되므로 병렬 처리는 할 수 없다. 올바르게는 'CTR 모드는 증가하는 카운터를 암호화하며 병렬 처리가 가능하고, OFB는 직전 출력을 피드백하므로 순차적으로 처리한다'이다.
② O — CBC는 현재 평문 블록과 직전 암호문 블록을 XOR한 뒤 암호화하고, 첫 블록에는 직전 암호문이 없으므로 IV를 사용한다. 블록 암호이므로 평문 길이가 블록 크기의 배수가 아니면 패딩이 추가되어 암호문 길이가 달라질 수 있다.
③ O — CFB는 블록 암호를 스트림 암호처럼 사용하므로 평문과 암호문의 길이가 같고, 최초 키 스트림 생성을 위해 IV가 필요하다. 암호화는 이전 암호문이 필요해 순차적으로 진행되지만, 복호화에서는 필요한 이전 암호문 블록들이 이미 주어져 있어 병렬 처리가 가능하다.
④ X — ECB에서 각 블록은 서로 독립적으로 암호화되므로 한 블록의 오류가 다른 블록의 복호화에 전파되지 않는다는 설명은 맞다. 그러나 한 블록을 해독했다는 사실만으로 나머지 블록까지 해독할 수 있는 것은 아니다. ECB의 실제 보안상 약점은 동일한 평문 블록이 동일한 암호문 블록으로 나타나 반복 패턴이 노출된다는 점이다. 따라서 공식 정답은 ①로 제시되어 있으나, ④의 마지막 문장도 ECB의 블록 독립성과 양립하지 않아 문항에 복수 오답 가능성이 있다.

오답 포인트

①은 OFB와 CTR의 특징을 섞어 놓았다. 두 모드 모두 키 스트림과 XOR하고 암호화·복호화 연산이 같은 형태이지만, CTR만 독립적인 카운터 블록을 사용하여 병렬 처리가 가능하다. OFB는 직전 출력의 피드백 때문에 순차적이다.

NoteBase

다시 나오면 이렇게 판단

먼저 다음 입력이 무엇인지 확인한다. 직전 암호문이면 CBC·CFB, 직전 출력이면 OFB, 증가하는 카운터이면 CTR, 블록 간 연결이 없으면 ECB이다. 이어서 앞 블록 의존성이 있으면 암호화 병렬 처리가 어렵고, 독립 입력인 ECB·CTR은 병렬 처리가 가능하다고 판단한다.

암기 포인트

ECB는 독립, CBC는 직전 암호문과 XOR, CFB는 암호문 피드백, OFB는 출력 피드백, CTR은 카운터이다.

NoteBase

25. 관리자가 다음 순서로 방화벽 규칙을 적용했다. 장비는 위에서 아래로 첫 번째 일치 규칙을 적용한다. 203.0.113.5에서 서버 SSH 접속을 시도할 때 결과와 개선책으로 가장 적절한 것은?

```
- allow tcp any any -> server 22
- deny tcp 203.0.113.0/24 any -> server 22
- allow tcp 10.10.0.0/16 any -> server 22
- 기본 정책 deny
```

① 1번 규칙에 먼저 일치하여 허용되므로, 차단 또는 세부 허용 규칙을 더 위에 두고 광범위 허용 규칙을 제거해야 한다.
② 2번 규칙에 의해 차단되며 개선이 필요없다.
③ 기본 정책 deny에 의해 차단된다.
④ 3번 규칙 때문에 허용된다.

정답 1번

출제 포인트

방화벽이 규칙을 위에서 아래로 검사하고, 가장 먼저 일치한 규칙의 동작을 적용한 뒤 검사를 끝낸다는 점을 묻는 문제이다.

핵심 개념

첫 번째 일치 규칙: 패킷과 일치하는 규칙을 위에서부터 찾으며, 처음 일치한 규칙이 허용이면 뒤의 차단 규칙은 검사하지 않는다.
규칙 섀도잉: 앞의 넓은 범위 규칙 때문에 뒤의 더 구체적인 규칙이 적용될 기회를 잃는 현상이다.
이 문제에서는 1번 규칙이 모든 출발지의 서버 SSH 접속을 허용하므로, 203.0.113.5의 접속도 1번 규칙에서 즉시 허용된다. 203.0.113.5가 203.0.113.0/24에 속하더라도 2번 규칙까지 내려가지 않는다.

NoteBase

선지별 해설

① O — 203.0.113.5에서 서버의 22번 포트로 향하는 TCP 접속은 1번의 광범위 허용 규칙과 먼저 일치하므로 허용된다. 의도대로 통제하려면 차단 규칙이나 필요한 세부 허용 규칙을 광범위 허용 규칙보다 위에 배치하고, 불필요한 광범위 허용 규칙은 제거해야 한다.
② X — 틀린 표현은 '2번 규칙에 의해 차단되면'이다. 실제로는 1번 규칙에서 이미 허용되어 2번 규칙이 평가되지 않으므로 개선이 필요하다. 203.0.113.0/24를 차단하려면 해당 차단 규칙을 광범위 허용 규칙보다 위에 두거나 광범위 허용 규칙을 제거해야 한다.
③ X — 틀린 표현은 '기본 정책 deny에 의해 차단된다'이다. 실제로는 1번 규칙과 일치하여 허용되며, 기본 정책은 앞선 어떤 규칙과도 일치하지 않을 때만 적용된다.
④ X — 틀린 표현은 '3번 규칙 때문에 허용된다'이다. 실제로 203.0.113.5는 10.10.0.0/16에 속하지 않으며, 이 접속은 그보다 앞선 1번 규칙 때문에 허용된다.

오답 포인트

203.0.113.5가 203.0.113.0/24에 포함된다는 사실만 보고 2번 규칙을 선택하기 쉽다. 그러나 주소 범위의 일치 여부보다 규칙의 평가 순서가 먼저이며, 1번 규칙이 뒤의 2번과 3번 규칙을 가린다.

다시 나오면 이렇게 판단

출발지, 목적지, 프로토콜, 포트를 확인한 뒤 규칙을 반드시 위에서 아래로 대입한다. 처음 일치한 규칙을 찾는 즉시 허용 또는 차단을 확정하고, 끝까지 일치하는 규칙이 없을 때만 기본 정책을 적용한다.

암기 포인트

방화벽 규칙은 위에서부터 첫 일치가 승리하며, 앞의 광범위 허용은 뒤의 세부 차단을 가린다.

NoteBase