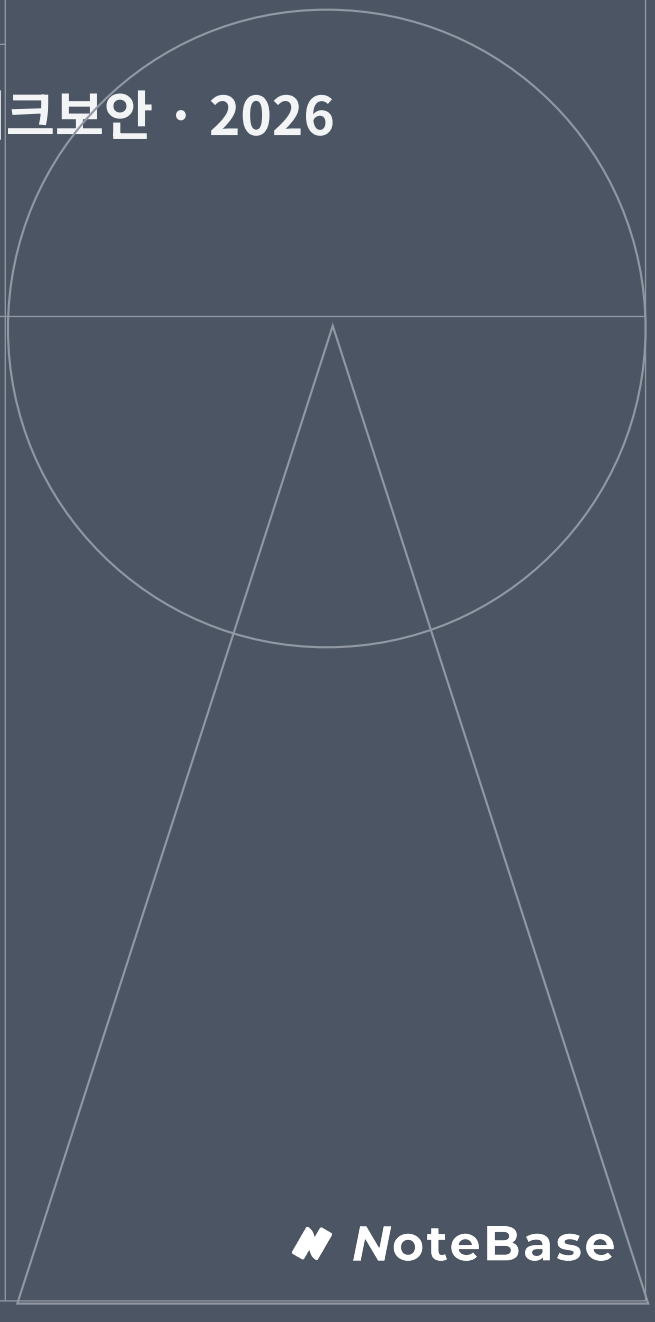
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2026



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2026

공무원/국가직/9급 · 네트워크보안 · 2026

문 1. 국내에서 개발된 대칭키 암호화 알고리즘이 아닌 것은?

① AES

② LEA

③ ARIA

④ SEED

정답 1번

간단한 해설

AES는 **벨기에 연구자들이 개발한 Rijndael**을 미국 국립표준기술연구소(NIST)가 표준으로 채택한 대칭키 암호이다. 따라서 대칭키 암호에는 해당하지만 **국내에서 개발된 알고리즘은 아니다**.

선지별 해설

네 알고리즘은 모두 암호화와 복호화에 같은 비밀키를 사용하는 대칭키 블록암호이다. 이 문항의 구별 기준은 대칭키 여부가 아니라 국내 개발 여부이다.

① X: AES는 벨기에 암호학자 Joan Daemen과 Vincent Rijmen이 개발한 Rijndael을 기반으로 NIST가 채택한 암호 표준이다. 대칭키 블록암호이지만, 국내 개발이 아니라 **국외에서 개발된 알고리즘**에 해당한다.

② O: LEA는 **국내에서 개발된 대칭키 블록암호**이다. 고속 처리가 필요한 환경과 모바일 기기 같은 경량 환경에서 기밀성을 제공하도록 설계되었다.

③ O: ARIA는 국내 학계·연구소·정부기관이 공동으로 개발한 대칭키 블록암호이다. 이름도 Academy, Research Institute, Agency의 머리글자를 따서 **학·연·관의 공동 개발**을 나타낸다.

④ O: SEED는 한국인터넷진흥원과 국내 암호전문가들이 **순수 국내기술로 개발**한 대칭키 블록암호이다. 전자상거래·금융·무선통신 등에서 중요한 정보의 기밀성을 보호하기 위해 개발되었다.

NoteBase

문 2. OSI 7계층 중 네트워크 계층에 포함되지 않는 프로토콜은?

① ARP

② UDP

③ OSPF

④ RARP

정답 2번

간단한 해설

UDP는 포트 번호로 통신할 응용 프로그램을 구분하는 **전송 계층(4계층)** 프로토콜이다. IP 주소를 이용한 전달 경로를 다루는 네트워크 계층과 역할이 다르다.

선지별 해설

이 문항은 ARP와 RARP를 주소 변환 기능에 따라 네트워크 계층 관련 프로토콜로 묶는 분류를 전제로 한다. 다만 두 프로토콜은 IP 주소와 링크 계층 주소를 연결하므로, 계층을 구분하는 기준에 따라 링크 계층 프로토콜로 설명되기도 한다. 아래 O/X는 이 문항의 분류에서 '네트워크 계층에 포함된다'는 판단을 나타낸다.

① O: ARP는 **IP 주소에 대응하는 MAC 주소**를 알아내는 주소 결정 프로토콜이다. 같은 링크에서 다음 홉으로 IP 패킷을 담은 프레임을 보내려면 그 홉의 MAC 주소가 필요하므로, IP 통신에 필요한 주소 대응을 제공한다. 이 문항에서는 이러한 역할을 네트워크 계층 관련 기능으로 분류한다.

② X: UDP는 네트워크 계층이 아니라 **전송 계층(4계층)** 프로토콜이다. IP가 호스트 사이의 패킷 전달을 담당한다면, UDP는 포트 번호를 이용해 호스트 안에서 데이터를 받을 응용 프로그램을 구분한다. 비연결형으로 동작하며 UDP 자체는 재전송이나 도착 순서 보장을 제공하지 않는다.

③ O: OSPF는 라우터 사이에 링크 상태 정보를 교환하고 이를 바탕으로 최단 경로를 계산하는 **링크 상태 라우팅 프로토콜**이다. IP 패킷을 어느 경로로 전달할지 결정하는 데 쓰이므로 네트워크 계층 관련 프로토콜에 해당한다. OSPF 메시지는 TCP나 UDP를 거치지 않고 IP에 직접 실린다.

④ O: RARP는 자신의 **MAC 주소를 바탕으로 IP 주소**를 알아내는 역주소 결정 프로토콜이다. 자신의 IP 주소를 모르는 호스트가 RARP 서버에 질의하고, 서버는 미리 저장된 주소 대응 정보를 바탕으로 응답한다. ARP와 주소를 찾는 방향이 반대이며, 이 문항에서는 IP 주소 획득을 지원하는 네트워크 계층 관련 프로토콜로 분류한다.

NoteBase

문 3. (가) ~ (다)에서 설명하는 네트워크 장비를 바르게 연결한 것은?

(가) 물리 계층에서 동작하며 수신된 프레임을 모든 포트로 브로드캐스팅하는 장비
(나) 데이터 링크 계층에서 MAC 주소를 기반으로 특정 포트로 프레임을 전달하는 장비
(다) 네트워크 계층에서 네트워크 주소(IP 주소)를 확인하고 다른 네트워크와 연결하는 장비

① (가): 라우터, (나): 스위치, (다): 허브
② (가): 허브, (나): 라우터, (다): 스위치
③ (가): 스위치, (나): 허브, (다): 라우터
④ (가): 허브, (나): 스위치, (다): 라우터

정답 4번

간단한 해설

허브는 **목적지 주소를 구분하지 않고** 수신 신호를 다른 포트로 반복 전송한다. 스위치는 이와 달리 **MAC 주소에 대응하는 포트**로 프레임을 전달한다.

대응 관계 해설

(가) 허브: 물리 계층에서 동작하며, 프레임의 목적지 MAC 주소를 해석하지 않고 **수신 신호를 수신 포트를 제외한 모든 포트로 반복 전송**한다. 지문의 '모든 포트로 브로드캐스팅'은 목적지에 따라 출력 포트를 선별하지 않는 이러한 동작을 가리킨다.

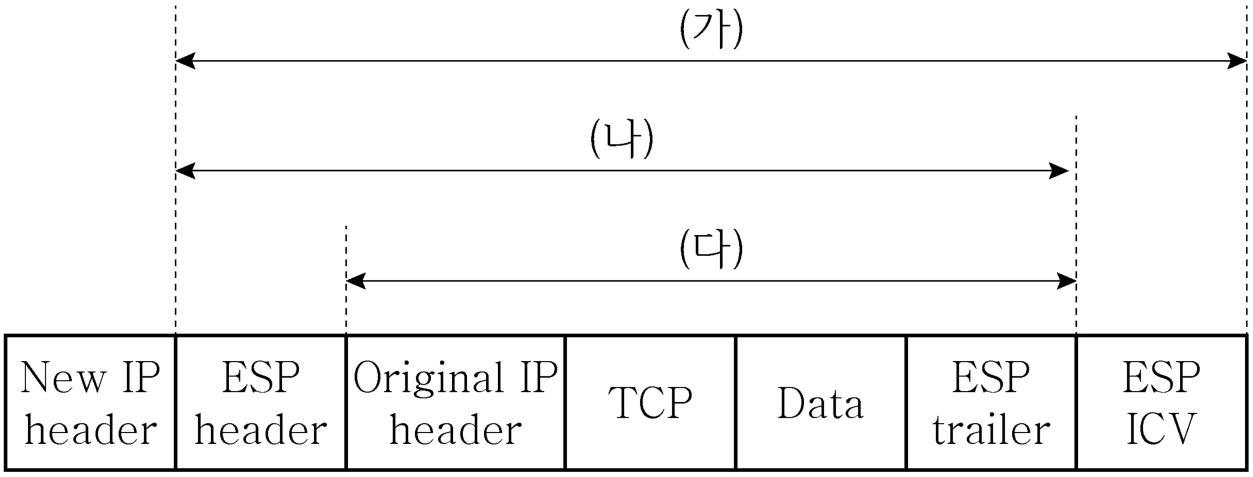
(나) 스위치: 데이터 링크 계층에서 동작하며, **목적지 MAC 주소와 포트의 대응 정보**를 이용해 프레임을 전달한다. 목적지 MAC 주소가 어느 포트에 연결되어 있는지 알고 있으면 그 포트로 전달하므로, 주소를 구분하지 않는 허브와 구별된다.

(다) 라우터: 네트워크 계층에서 동작하며, 패킷의 **목적지 IP 주소와 라우팅 테이블**을 바탕으로 전달할 경로를 결정한다. 서로 다른 네트워크를 연결하므로, 같은 네트워크에서 MAC 주소를 기준으로 프레임을 전달하는 스위치와 구별된다.

따라서 (가) 허브, (나) 스위치, (다) 라우터의 대응은 ④와 일치한다.

NoteBase

문 4. 다음 IPSec ESP(Encapsulating Security Payload)에서 터널모드의 암호화 및 인증 범위를 바르게 연결한 것은?



① 암호화 범위: (가), 인증 범위: (나)

② 암호화 범위: (가), 인증 범위: (다)

③ 암호화 범위: (다), 인증 범위: (가)

④ 암호화 범위: (다), 인증 범위: (나)

정답 4번

간단한 해설

ESP 터널모드는 **원래 IP 헤더까지 암호화**하여 내부 패킷을 보호한다. 인증은 암호화하지 않는 **ESP 헤더도 포함**하지만, 인증 결과를 담는 ESP ICV 자체는 인증 범위에서 제외한다.

NoteBase

대응 관계 해설

암호화 범위: (다). 터널모드는 원래 IP 패킷 전체를 ESP의 내부에 넣으므로, 그림의 Original IP header·TCP·Data와 ESP trailer가 암호화된다. 따라서 **Original IP header부터 ESP trailer까지**인 (다)에 해당한다. ESP header는 수신 측이 보안 연결을 식별하는 데 필요한 정보를 담으므로 암호화하지 않는다. 바깥의 New IP header도 패킷 전달에 사용되므로 암호화 범위에 포함되지 않는다.

인증 범위: (나). 인증은 데이터의 변조 여부와 출처를 확인하기 위한 것으로, 그림에서는 **ESP header부터 ESP trailer까지**를 대상으로 한다. 즉, 암호화된 내부 패킷과 트레일러뿐 아니라 암호화되지 않은 ESP header도 보호한다. ESP ICV는 이 범위에 대해 계산한 무결성 검사값을 담는 필드이므로 계산 대상에 포함하지 않는다. 따라서 ESP ICV까지 포함하는 (가)는 인증 범위가 아니며, New IP header 역시 ESP 인증 범위 밖에 있다.

암호화 범위는 (다), 인증 범위는 (나)이므로 ④의 연결과 일치한다.

NoteBase

문 5. SSLv3(Secure Sockets Layer version 3)에서 서버와 클라이언트가 서로 인증하고, 암호와 MAC 알고리즘과 암호키를 협상하는 역할을 하는 프로토콜은?

① Alert Protocol

② Record Protocol

③ Handshake Protocol

④ Change Cipher Spec Protocol

정답 3번

간단한 해설

Handshake Protocol은 통신 상대를 인증하고, 통신에 사용할 **암호화·MAC 알고리즘과 키를 설정**하는 절차를 담당한다.

개념 구분

Handshake Protocol: SSLv3에서 **상대 인증과 보안 매개변수 협상**을 담당한다. 클라이언트가 ClientHello로 지원하는 암호 스위트를 제시하면 서버는 ServerHello로 사용할 암호 스위트를 선택한다. 이를 통해 암호화·MAC 알고리즘 등을 정하고, 키 교환으로 마련한 공통 비밀값에서 통신에 필요한 암호화 키와 MAC용 비밀값을 도출한다. 클라이언트 인증은 서버가 요청하는 경우 선택적으로 수행하므로, 모든 연결에서 반드시 상호 인증하는 것은 아니다.

Change Cipher Spec Protocol: **이미 협상한 알고리즘과 키를 이후 레코드에 적용**하겠다고 알린다. 보안 조건을 정하는 Handshake와 달리, 정해진 조건을 실제 통신 상태에 반영하는 전환을 통지한다.

Record Protocol: 상위 계층의 메시지를 레코드로 나누어 담고, 현재 설정된 보안 조건에 따라 MAC과 암호화를 적용해 전송한다. 핵심 역할은 **설정된 조건에 따른 데이터 보호**이며, 인증과 알고리즘 협상 자체는 Handshake가 담당한다.

Alert Protocol: 오류의 내용과 심각도 또는 연결 종료를 상대에게 알린다. 보안 조건을 협상하는 기능과 구별된다.

NoteBase

문 6. 디지털 포렌식에서 다음에 해당하는 것은?

불법 해킹 용의자의 해킹 툴이 증거 능력을 갖추기 위해서는 같은 상황의 피해 시스템에 툴을 적용할 경우 피해 상황과 일치하는 결과가 나와야 한다.

① 재현의 원칙
② 신속성의 원칙
③ 무결성의 원칙
④ 연계 보관성의 원칙

정답 1번

간단한 해설

같은 상황의 시스템에서 해킹 툴을 실행했을 때 **실제 피해와 일치하는 결과**가 나와야 한다는 조건은 재현의 원칙을 나타낸다.

공통 해설

재현의 원칙은 **동일한 조건에서 같은 방법을 적용하면 동일한 결과를 얻을 수 있어야 한다**는 원칙이다. 이를 통해 분석 결과가 우연한 현상이나 특정 분석자의 주장에 그치지 않고 다시 확인될 수 있도록 한다.

지문에서는 실제 피해 시스템과 같은 상황을 갖춘 시스템에 용의자의 해킹 툴을 적용한다. 그 실행 결과가 실제 피해 상황과 일치하는지 확인함으로써 해당 툴로 그 피해가 재현되는지를 검증한다. 따라서 이 조건은 해킹 툴과 피해 결과의 관련성을 재현 실험으로 확인하는 재현의 원칙에 해당한다.

NoteBase

문 7. XSS 취약점 공격의 수행 단계를 순서대로 바르게 나열한 것은?

(가) 사용자 시스템에서 XSS 코드가 실행된다.
(나) 웹 서버는 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다.
(다) 사용자는 공격자가 작성해 둔 XSS 코드가 포함된 게시물을 클릭한다.
(라) 임의의 XSS 취약점이 존재하는 서버에 XSS 코드가 포함된 게시물을 작성하여 저장한다.
(마) XSS 코드가 실행된 결과는 공격자에게 전달되고 공격자는 공격을 종료한다.

① (나) → (가) → (다) → (라) → (마)
② (나) → (가) → (라) → (다) → (마)
③ (라) → (나) → (가) → (다) → (마)
④ (라) → (다) → (나) → (가) → (마)

정답 4번

간단한 해설

사용자가 게시물을 클릭하는 것은 **서버에 저장된 게시물을 요청하는 단계**이므로, 서버의 게시물 전달보다 앞선다. XSS 코드는 전달된 게시물을 처리하는 **사용자 브라우저에서 실행**된다.

NoteBase

올바른 순서

(라) → (다) → (나) → (가) → (마)

(라) 게시물 작성·저장: 공격자는 XSS 취약점이 있는 웹 서버에 악성 스크립트가 포함된 게시물을 작성하여 저장한다. 악성 코드가 서버에 저장되었다가 사용자에게 전달되는 **저장형 XSS**의 준비 단계이다.

(다) 사용자의 게시물 클릭: 사용자가 공격자가 작성해 둔 게시물을 클릭하면 브라우저가 서버에 해당 게시물의 내용을 요청한다. 클릭할 게시물이 먼저 저장되어 있어야 하며, 이 **요청이 서버 응답보다 먼저** 이루어진다.

(나) 서버의 게시물 전달: 웹 서버는 사용자의 요청에 응답하여 저장된 게시물의 내용을 전달한다. 이때 악성 스크립트가 안전하게 처리되지 않고 게시물에 포함된 채 전달되어, 사용자 브라우저가 공격 코드를 받게 된다.

(가) 사용자 시스템에서 코드 실행: 게시물을 받은 브라우저가 그 안의 악성 스크립트를 실행한다. 서버에 코드를 저장하는 단계와 달리, 여기서 실제 실행이 이루어지는 곳은 **사용자 브라우저**이다. 따라서 서버의 게시물 전달이 코드 실행에 앞선다.

(마) 실행 결과 전달·공격 종료: 제시된 공격 과정에서는 XSS 코드의 실행 결과가 공격자에게 전달되고 공격자는 공격을 종료한다. 전달할 결과가 생기려면 먼저 코드가 실행되어야 하므로 이 단계가 마지막에 놓인다.

NoteBase

문 8. TCP 세션 하이재킹 공격에 대한 설명으로 옳지 않은 것은?

① 공격자는 적절한 시퀀스 넘버를 얻기 위해 스니핑을 한다.

② TCP 세션 하이재킹은 공격자가 동기화 상태를 무너뜨리는 것에서 시작한다.

③ 공격자는 네트워크에서 직접 클라이언트의 세션 ID를 수정하여 새로운 세션을 생성한다.

④ 서버와 클라이언트의 통신 시에 시퀀스 넘버의 제어에 문제점이 있음을 파악하고 악용한다.

정답 3번

간단한 해설

TCP 세션 하이재킹은 **시퀀스 번호를 악용하여 이미 연결된 통신을 가로채는 공격**이다. 클라이언트의 세션 ID를 직접 수정하여 새로운 세션을 만드는 방식이 아니다.

선지별 해설

① O: 스니핑은 네트워크에서 오가는 패킷을 엿보는 것이다. 공격자는 TCP 헤더를 관찰하여 **현재 사용 중인 시퀀스 번호**와 확인응답 번호를 파악하고, 이를 위조 패킷이 기존 연결의 데이터로 받아들여지도록 만드는 데 이용한다.

② O: 동기화 교란을 이용하는 대표적인 능동형 공격에서는 먼저 **클라이언트와 서버가 관리하는 시퀀스 번호의 관계를 어긋나게** 만든다. 한쪽이 다음에 보낼 데이터의 번호와 상대가 다음에 받으리라 기대하는 번호가 맞지 않게 되면 정상 통신이 방해되고, 공격자는 각 상대가 기대하는 번호에 맞춘 위조 패킷으로 통신에 개입한다.

③ X: TCP 세션 하이재킹의 대상은 **새로 만드는 세션이 아니라 이미 성립한 TCP 연결**이다. 공격자는 정상 통신 상대를 사칭하고 적절한 시퀀스 번호 등을 갖춘 패킷을 주입하여 기존 연결을 가로챈다. TCP 헤더에는 웹 애플리케이션의 세션 ID와 같은 필드가 없으므로, 클라이언트의 세션 ID를 직접 수정한다는 설명은 TCP 연결 탈취의 원리와 다르다.

④ O: TCP의 시퀀스 번호는 전송하는 바이트의 순서를 나타내며, 수신 측은 이 번호와 수신 윈도 등을 기준으로 패킷을 처리한다. 그러나 **시퀀스 번호가 유효하다는 사실만으로 송신자의 신원이 인증되는 것은 아니다**.
공격자는 번호를 알아내거나 예측하고 통신 상대를 사칭하여 위조 데이터를 기존 연결에 끼워 넣는 데 이 점을 악용한다.

NoteBase

문 9. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

nmap 명령어의 옵션에서 (가)는 TCP SYN을 스캔하고, (나)는 스캔 결과를 상세히 출력한다.

① (가): -sS, (나): -v
② (가): -sS, (나): -A
③ (가): -sT, (나): -v
④ (가): -sT, (나): -A

정답 1번

간단한 해설

TCP SYN 스캔을 지정하는 옵션은 **-sS**이고, 출력 정보의 상세 수준을 높이는 옵션은 **-v**이다.

빈칸별 해설

(가) -sS: SYN 패킷을 보내고 응답을 분석하여 포트 상태를 판단하는 TCP SYN 스캔이다. 열린 포트에서 SYN/ACK를 받아도 **TCP 연결을 완성하지 않는** 반개방 스캔이다. 반면 -sT는 운영체제의 connect 호출을 이용하며, 열린 포트에 대해 TCP 연결을 완성하는 TCP connect 스캔이다.

(나) -v: **출력의 상세 수준을 높이는** 옵션이다. 스캔 중 열린 포트가 발견되면 바로 표시하는 등 진행 상황과 결과에 관한 정보를 더 많이 출력한다. -A는 운영체제 탐지, 서비스 버전 탐지, 기본 스크립트 스캔, 경로 추적 기능을 활성화하는 옵션이며, -v의 상세 출력 기능을 자동으로 활성화하지는 않는다.

(가)는 -sS, (나)는 -v이므로 ①의 조합과 일치한다.

NoteBase

문 10. 암호화 단계에서 현재의 평문 블록을 바로 직전의 암호 블록과 XOR한 것을 암호 알고리즘 입력으로 사용하는 블록 암호 운영 모드는?

① CFB

② CBC

③ OFB

④ CTR

정답 2번

간단한 해설

CBC는 현재 평문 블록과 직전 암호 블록을 **먼저 XOR한 뒤 암호 알고리즘에 입력**한다. 직전 암호문의 영향을 다음 블록에 이어 주는 구조이다.

핵심 풀이

CBC(Cipher Block Chaining)는 현재 평문 블록을 직전 암호 블록과 XOR하고, 그 결과를 블록 암호 알고리즘으로 암호화하여 현재 암호 블록을 만든다. 즉, **평문과의 XOR이 암호 알고리즘 적용보다 먼저** 이루어진다. 첫 평문 블록에는 직전 암호 블록이 없으므로 초기화 벡터(IV)를 대신 사용한다.

CFB·OFB·CTR은 암호 알고리즘의 출력으로 만든 키스트림을 평문과 XOR하여 암호문을 만든다. 평문과의 XOR이 **암호 알고리즘 적용 후**에 이루어진다는 점에서 CBC와 구별된다. 특히 CFB도 이전 암호문을 피드백하지만, 이를 먼저 암호 알고리즘에 넣은 뒤 그 출력의 필요한 부분을 평문과 XOR한다. 따라서 '이전 암호문을 이용한다'는 단서만으로 CBC와 CFB를 구분해서는 안 된다.

NoteBase

문 11. TCP/IP 프로토콜에 대한 설명으로 옳지 않은 것은?

① SMTP는 네트워크의 두 메일 서버 간에 이메일을 송수신할 때 사용되는 프로토콜이다.

② DHCP는 네트워크의 각 노드에 IP 주소를 자동으로 할당하고 관리한다.

③ ARP를 이용하여 LAN에 연결되어 있는 다른 노드의 포트 번호를 획득할 수 있다.

④ ICMP의 송신지 억제(Source Quench) 메시지는 송신 노드에 혼잡 가능성을 알리고 전송 속도를 늦출 것을 요구한다.

정답 3번

간단한 해설

③의 '포트 번호'는 **MAC 주소**로 고쳐야 한다. ARP는 같은 LAN에서 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다.

선지별 해설

① O: SMTP는 **메일 서버 사이에서 이메일을 전송**하는 프로토콜이다. 보내는 서버가 SMTP로 메일을 전달하고 받는 서버가 이를 수신하므로, 두 메일 서버 간 송수신에 사용된다는 설명이 성립한다.

② O: DHCP는 클라이언트에 **IP 주소를 자동으로 할당**하고 그 사용을 관리하는 프로토콜이다. DHCP 서버는 주소를 일정 기간 임대하고, 클라이언트는 임대 기간을 갱신하여 계속 사용할 수 있다.

③ X: ARP는 같은 LAN에서 알고 있는 IPv4 주소에 대응하는 **MAC 주소**를 알아내는 프로토콜이다. 이 MAC 주소는 이더넷 프레임을 해당 노드로 보내는 데 필요하다. 선지의 '포트 번호'는 'MAC 주소'로 고쳐야 한다. 포트 번호는 TCP·UDP에서 통신할 응용 프로그램이나 서비스를 구분하는 데 사용하며, ARP로 알아내는 대상이 아니다.

④ O: Source Quench는 원래 라우터나 수신 호스트가 혼잡 또는 처리 용량 부족을 송신 노드에 알리고 **전송 속도를 줄이도록 요청**하기 위해 정의된 ICMP 메시지이다. 따라서 이 메시지의 본래 기능을 설명한 진술이다. 다만 현재는 RFC 6633에 따라 혼잡 제어 수단으로서의 사용이 폐기되었으므로, 현재도 사용해야 하는 방식이라는 뜻으로 이해해서는 안 된다.

NoteBase

문 12. 네트워크 공격 기술에 대한 설명으로 옳지 않은 것은?

① 랜드 공격은 패킷을 전송할 때 출발지 MAC 주소와 목적지 MAC 주소의 값을 같게 만들어서 공격 대상에게 보내는 공격이다.

② 스위치 재밍 공격은 스위치가 MAC 주소 테이블을 기반으로 패킷을 포트에 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격이다.

③ IP 스푸핑은 신뢰 관계에 있는 두 개의 호스트 사이에서 하나의 시스템을 마비시킨 후 자신이 신뢰 관계에 있는 호스트인 것처럼 속이는 공격이다.

④ HTTP GET 플러딩은 웹서버에서 처리할 수 없는 최대 성능 이상의 과도한 HTTP GET 요청을 전송함으로써 웹 서버가 자원을 모두 소비하여 정상적인 기능을 발휘하지 못하도록 하는 공격이다.

정답 1번

간단한 해설

랜드 공격은 출발지와 목적지의 **IP 주소를 공격 대상의 IP 주소로 같게** 설정하고, TCP 포트 번호도 같게 만든 패킷을 보내는 공격이다. ①의 'MAC 주소'는 'IP 주소'로 고쳐야 한다.

선지별 해설

① X: 랜드(LAND) 공격은 출발지와 목적지의 **IP 주소와 TCP 포트 번호를 각각 같게** 설정한 TCP SYN 패킷을 공격 대상에게 보내는 서비스 거부 공격이다. 출발지와 목적지 IP 주소에는 모두 공격 대상의 IP 주소를 넣는다. 이를 처리하는 데 취약한 시스템의 오동작이나 자원 소모를 유발하므로, 선지의 '출발지 MAC 주소와 목적지 MAC 주소'는 '출발지 IP 주소와 목적지 IP 주소'로 고쳐야 한다.

② O: 스위치는 MAC 주소와 포트의 대응을 저장한 MAC 주소 테이블을 이용해 프레임을 전달한다. 스위치 재밍은 서로 다른 위조 출발지 MAC 주소를 가진 프레임을 대량으로 보내 **MAC 주소 테이블을 포화**시키는 방식이 대표적이다. 새 주소를 정상적으로 학습하지 못하면 목적지 포트를 알 수 없는 프레임이 여러 포트로 전달되어, 정상적인 선택 전달 기능을 방해할 수 있다.

③ O: IP 스푸핑은 패킷의 **출발지 IP 주소를 위조하여 다른 호스트로 가장**하는 것이다. 선지는 IP 주소에 기반한 신뢰 관계를 악용하는 전형적인 공격 사례를 설명한다. 공격 대상이 신뢰하는 호스트의 응답을 마비시킨 뒤 그 호스트의 IP 주소를 사칭하면, 실제 호스트가 연결을 끊는 응답을 보내 공격을 방해하는 일을 막을 수 있다. 다만 신뢰 호스트의 마비가 모든 IP 스푸핑 공격에 필수인 것은 아니다.

④ O: HTTP GET은 웹서버에 페이지나 파일 등의 자원을 요청하는 데 사용된다. HTTP GET 플러딩은 서버의 **처리 능력을 넘는 GET 요청**을 대량으로 보내는 응용 계층 서비스 거부 공격이다. 서버가 요청 처리에 CPU·메모리 등의 자원을 소모하여 정상 사용자의 요청에 제대로 응답하지 못하게 한다.

NoteBase

문 13. 스크리닝 라우터와 배스천 호스트에 대한 설명으로 옳지 않은 것은?

① 배스천 호스트는 내부 네트워크와 외부 네트워크 간의 게이트웨이 역할을 한다.

② 스크리닝 라우터는 배스천 호스트에 비하여 통과하거나 거절당한 패킷의 기록을 관리하기 쉽다.

③ 스크리닝 라우터는 네트워크 계층과 전송 계층에서 동작하는 프로토콜인 IP, TCP 또는 UDP의 헤더에 포함된 내용을 분석한다.

④ 배스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

정답 2번

간단한 해설

②의 '기록을 관리하기 쉽다'는 비교가 반대이다. 스크리닝 라우터는 주로 패킷 헤더로 통과 여부를 판단하므로, 호스트의 기록·감사 기능을 활용하는 **배스천 호스트가 접속 기록을 관리하기에 더 유리하다**.

선지별 해설

① O: 배스천 호스트는 외부 공격에 견디도록 보안을 강화한 호스트이다. 방화벽 구성에서 프록시 등의 기능으로 내부망과 외부망 사이의 통신을 중계하고 접근을 통제하는 **게이트웨이 역할**을 한다.

② X: 전통적인 스크리닝 라우터는 헤더에 설정된 조건으로 패킷을 허용하거나 차단하는 데 중점을 두어 기록·감사 기능이 제한적이다. 배스천 호스트는 운영체제와 프록시의 기능을 이용해 접속과 처리 내역을 상세히 기록할 수 있으므로, **배스천 호스트가 기록 관리에 더 유리하다**. 스크리닝 라우터가 전혀 기록할 수 없다는 뜻은 아니다.

③ O: 스크리닝 라우터는 **네트워크 계층과 전송 계층의 헤더 정보**를 필터링 기준으로 사용한다. IP 헤더의 출발지·목적지 주소와 프로토콜 정보, TCP·UDP 헤더의 포트 번호 등을 규칙과 대조하여 패킷의 통과 여부를 결정한다.

④ O: 배스천 호스트에 내부망 보호를 의존하는 구성에서는 이 호스트의 보안 기능이 손상되면 인증과 접근통제를 신뢰할 수 없게 된다. 공격자가 호스트를 장악하여 내부망 침입의 발판으로 삼을 수 있으므로, **해당 호스트에 의존한 보호가 무너진다**는 의미이다.

NoteBase

문 14. ICMP 리다이렉트 공격이 성공했을 경우의 상황으로 옳은 것은?

① 호스트의 ARP 캐시가 업데이트된다.

② 특정 호스트의 MAC 주소가 도용된다.

③ 스위치의 주소 테이블이 가득 차게 된다.

④ 호스트의 라우팅 테이블 정보가 업데이트된다.

정답 4번

간단한 해설

ICMP 리다이렉트는 호스트에 목적지로 가는 다음 게이트웨이를 알려 주는 메시지이다. 위조된 메시지를 호스트가 받아들이면 **라우팅 테이블의 경로 정보**가 공격자가 지정한 방향으로 바뀐다.

선지별 해설

① X: ARP 캐시는 IP 주소와 MAC 주소의 대응을 저장한다. 이를 거짓 대응으로 바꾸는 대표적인 공격은 **ARP 스푸핑**이다. ICMP 리다이렉트 공격이 직접 변경하는 것은 이 주소 대응이 아니라 목적지로 가는 경로 정보이다.

② X: 다른 호스트의 MAC 주소를 도용하는 것은 **MAC 스푸핑**이다. ICMP 리다이렉트 공격은 MAC 주소를 도용하는 대신, 위조된 경로 변경 메시지를 이용해 호스트가 패킷을 보낼 다음 게이트웨이를 바꾼다.

③ X: 스위치가 출발지 MAC 주소와 포트의 대응을 학습한다는 점을 악용하여, 수많은 가짜 MAC 주소로 주소 테이블을 채우는 것은 **MAC 플러딩**이다. ICMP 리다이렉트 공격의 대상은 스위치의 주소 테이블 용량이 아니라 호스트의 라우팅 정보이다.

④ O: ICMP 리다이렉트는 라우터가 호스트에 특정 목적지로 보낼 때 사용할 더 적절한 게이트웨이를 알려 주는 기능이다. 공격자가 정상 라우터를 사칭한 메시지를 보내고 호스트가 이를 받아들이면, 해당 목적지의 **다음 게이트웨이 정보가 변경**된다. 예를 들어 정상 게이트웨이로 보내던 패킷을 공격자가 지정한 장비로 보내도록 라우팅 테이블 정보가 업데이트된다.

NoteBase

문 15. 프로토콜별 통계 현황을 출력하는 netstat 명령어 옵션은?

① -i

② -p

③ -r

④ -s

정답 4번

간단한 해설

netstat의 **-s** 옵션은 TCP·UDP 등 **프로토콜별 통계**를 출력한다. 네트워크 인터페이스별 현황을 보여 주는 -i와 구분한다.

개념 구분

-s: 프로토콜별 통계를 출력하는 옵션이다. netstat -s를 실행하면 TCP·UDP·IP·ICMP 등의 통계를 프로토콜별로 나누어 확인할 수 있다. 문제의 '프로토콜별 통계 현황'은 **-s의 통계 출력 기능**을 가리킨다.

-i: 네트워크 인터페이스 목록과 송수신·오류 등의 통계를 출력한다. 통계를 묶는 기준이 **프로토콜이 아니라 인터페이스**라는 점에서 -s와 다르다.

-p: Linux의 net-tools에서는 소켓을 사용하는 프로세스의 PID와 프로그램 이름을 표시한다. 프로토콜별 통계를 출력하는 옵션과 구분한다.

-r: 목적지와 게이트웨이 등 패킷 전달 경로를 확인하는 라우팅 테이블을 출력한다. 프로토콜의 처리 통계가 아니라 경로 정보를 확인하는 옵션이다.

NoteBase

문 16. IP에 대한 설명으로 옳지 않은 것은?

① IPv4에서 192.168.0.0은 사설 주소 영역에 해당된다.

② IPv4에서 IP 데이터그램의 최대 길이는 65,535바이트이다.

③ IPv6에서 주소 FCBB:0000:0000:0000:0000:0000:1ABC:BBCB는 FCBB:0:0:0:0:0:1ABC:BBCB으로 축약할 수 있다.

④ IPv6에서 홉 제한은 패킷이 라우터에 의해 중개될 때마다 1씩 증가하여 128을 넘는 순간 패킷을 폐기한다.

정답 4번

간단한 해설

IPv6의 홉 제한은 라우터가 패킷을 전달할 때마다 **1씩 감소**하며, **0이면 더 전달하지 않고 폐기**한다. 128을 넘는지를 폐기 기준으로 삼지 않는다.

선지별 해설

① O: IPv4의 사설 주소 범위 중 하나는 **192.168.0.0~192.168.255.255**이다. 192.168.0.0은 이 범위에 포함되므로 사설 주소 영역에 해당한다.

② O: IPv4 헤더의 전체 길이(Total Length) 필드는 16비트이며, 바이트 단위로 **헤더와 데이터를 합한 길이**를 나타낸다. 이 필드로 표현할 수 있는 최댓값이 65,535이므로 IPv4 데이터그램의 최대 길이는 65,535바이트이다.

③ O: IPv6 주소에서는 각 16비트 블록의 **앞쪽 0을 생략**할 수 있으며, 0000인 블록은 0 하나로 쓸 수 있다. 따라서 다섯 개의 0000 블록을 각각 0으로 바꾼 FCBB:0:0:0:0:0:1ABC:BBCB는 원래 주소와 같은 주소를 나타낸다.

④ X: 홉 제한(Hop Limit)은 패킷이 라우팅 루프에서 무한히 순환하는 것을 막기 위해 전달 횟수를 제한하는 필드이다. 라우터는 패킷을 전달할 때 이 값을 **1씩 감소**시키며, 수신 시 이미 0이거나 감소한 결과가 0이면 패킷을 폐기한다. 따라서 '1씩 증가하여 128을 넘는 순간'은 **1씩 감소하여 0이 되는 때**로 고쳐야 한다.

NoteBase

문 17. 『OWASP Top 10 for LLM Applications 2025』에서 정의한 「LLM03:2025 공급망」에 대한 항목에 해당하지 않는 것은?

① 타사 모델을 선택할 때는 포괄적인 AI 레드팀 및 평가를 수행한다.

② 취약하거나 오래된 구성 요소를 완화하기 위해 패치 정책을 구현한다.

③ 모델이 의도하지 않은 데이터 소스에 접근하는 것을 방지하기 위해 인프라를 충분히 제어해야 한다.

④ 협업 모델 개발 환경에 대한 엄격한 모니터링 및 감사 관행을 구현하여 남용을 방지하고 신속하게 탐지한다.

정답 3번

간단한 해설

③의 '의도하지 않은 데이터 소스에 대한 접근 방지'는 **LLM04:2025 데이터 및 모델 오염**의 완화책이다.
검증되지 않거나 악의적으로 조작된 데이터가 유입되어 모델의 출력이 왜곡되는 것을 막기 위한 조치이다.

선지별 해설

LLM03:2025 공급망은 외부에서 도입하는 모델·데이터·소프트웨어 구성 요소와 개발·배포 과정의 취약점으로 인해 무결성과 보안이 훼손되는 위험을 다룬다.

① O: 타사 모델에는 숨겨진 취약점이나 백도어가 있을 수 있으므로, 도입 전에 **AI 레드팀 및 평가**를 수행하는 것은 공급망 위험 완화책이다. 레드팀은 공격자 관점에서 모델을 시험하는 활동이며, 공개된 평가 점수만 믿지 않고 실제 사용 목적에 맞게 안전성을 확인한다.

② O: 취약하거나 오래된 라이브러리 등 구성 요소는 공격의 통로가 될 수 있다. **패치 정책**을 마련하여 취약점을 보완하고, 유지보수되는 API와 모델 버전을 사용하는 것은 공급망 위험을 줄이는 조치이다.

③ X: 의도하지 않은 데이터 소스에 접근하지 못하도록 인프라를 통제하는 조치는 **LLM04:2025 데이터 및 모델 오염**의 예방·완화 전략에 해당한다. 데이터 오염은 학습·미세조정·임베딩 등에 쓰이는 데이터가 조작되어 모델에 편향이나 백도어 등이 생기는 위험이다. 이 조치는 안전하지 않은 데이터의 유입을 제한하는 데 초점이 있으므로, 문제에서 묻는 LLM03:2025 공급망의 항목으로 분류한 것이 잘못이다.

④ O: 여러 참여자가 모델을 병합하거나 변환하는 협업 환경에서는 개발 과정이 악용되어 모델에 악성 요소가 유입될 수 있다. 따라서 협업 모델 개발 환경을 **엄격하게 모니터링하고 감사**하여 남용을 예방하고 신속하게 탐지하는 것은 공급망 위험 완화책이다.

NoteBase

문 18. SNMP(Simple Network Management Protocol) version 1에서 매니저와 에이전트 간의 통신에 사용되는 메시지에 대한 설명으로 옳지 않은 것은?

① trap 메시지를 이용하여 매니저가 에이전트에게 특정 상황 발생을 알린다.

② setRequest 메시지를 이용하여 매니저가 특정 변숫값의 변경을 요청한다.

③ getResponse 메시지를 이용하여 에이전트가 매니저의 요청에 해당하는 변숫값을 전송한다.

④ getRequest 메시지를 이용하여 매니저가 변숫값을 읽어올 수 있다.

정답 1번

간단한 해설

trap은 **에이전트가 매니저에게** 특정 상황의 발생을 알리는 메시지이다. ①은 통지의 송신자와 수신자를 반대로 설명했다.

선지별 해설

SNMP에서 매니저는 네트워크 장비의 상태를 감시하고 제어하며, 에이전트는 관리 대상 장비에서 요청을 처리하고 사건 발생을 알린다. 관리 변수는 장비의 상태나 설정을 나타내는 관리 정보이다.

① X: trap은 **에이전트가 매니저에게 자발적으로 보내는 통지**이다. 예를 들어 에이전트는 통신 링크의 장애를 감지하면 linkDown trap으로 알릴 수 있다. 따라서 '매니저가 에이전트에게'를 '에이전트가 매니저에게'로 고쳐야 한다.

② O: setRequest는 매니저가 에이전트에게 **관리 변수의 값 변경**을 요청하는 메시지이다. 매니저는 변경할 변수와 새 값을 지정하며, 실제 변경은 해당 변수가 쓰기 가능하고 요청한 값이 허용되는 등의 조건을 충족해야 한다.

③ O: getResponse는 에이전트가 매니저의 요청에 응답하는 메시지이다. 조회가 성공하면 요청받은 변수의 이름과 값을 담아 전송한다. SNMP version 1에서는 **조회 요청뿐 아니라 변경 요청에도** getResponse로 처리 결과를 알린다.

④ O: getRequest는 매니저가 에이전트에게 **지정한 관리 변수의 값 조회**를 요청하는 메시지이다. 매니저가 읽을 변수를 지정하면 에이전트가 getResponse에 그 값을 담아 응답하므로, 매니저는 이를 통해 변숫값을 읽어올 수 있다.

NoteBase

문 19. CIDR 방식으로 표현한 203.237.10.0/25에 대한 설명으로 옳은 것은?

① 203.237.10.128은 브로드캐스트 주소이다.

② 3개의 서브넷을 만들 수 있다.

③ 서브넷 마스크는 255.255.255.128이다.

④ 서브넷의 호스트 가용 IP 주소는 124개이다.

정답 3번

간단한 해설

/25는 IPv4 주소의 앞 25비트를 네트워크 부분으로 사용한다는 뜻이다. 서브넷 마스크는 1이 25개 연속된 형태이므로 **255.255.255.128**이다.

선지별 해설

IPv4 주소는 32비트이며, /25는 앞 25비트가 네트워크 부분이고 나머지 7비트가 호스트 부분임을 뜻한다. 203.237.10.0/25의 주소 범위는 203.237.10.0부터 203.237.10.127까지이다.

① X: 브로드캐스트 주소는 호스트 비트를 모두 1로 설정한 주소이므로 **203.237.10.127**이다. 203.237.10.128은 다음 /25 블록인 203.237.10.128/25의 네트워크 주소이다.

② X: 같은 크기의 서브넷으로 나눌 때 그 개수는 **분할 전 네트워크의 접두사 길이**에 따라 달라지므로, /25라는 정보만으로 3개라고 할 수 없다. 예를 들어 203.237.10.0/24를 /25로 나누면 네트워크 비트가 1개 늘어나므로 $2^{25-24} = 2$개의 서브넷이 만들어진다. 두 서브넷은 203.237.10.0/25와 203.237.10.128/25이다.

③ O: 서브넷 마스크는 네트워크 부분을 1, 호스트 부분을 0으로 표시한다. 앞 24비트는 1이므로 처음 세 옥텟은 각각 255이고, 마지막 옥텟은 **10000000**이므로 십진수로 128이다. 따라서 /25의 서브넷 마스크는 255.255.255.128이다.

④ X: 호스트 부분이 7비트이므로 이 블록의 전체 주소 수는 $2^7 = 128$개이다. 일반적인 IPv4 서브넷에서는 호스트 비트가 모두 0인 네트워크 주소와 모두 1인 브로드캐스트 주소를 호스트에 할당하지 않는다. 따라서 가용 호스트 주소는 **두 주소를 제외한 126개**이며, 범위는 203.237.10.1부터 203.237.10.126까지이다.

NoteBase

문 20. X.509 버전 3 인증서의 확장 필드에 대한 설명으로 옳지 않은 것은?

① Basic Constraints: 인증 주체가 CA인지를 식별한다.

② Authority Key Identifier: 인증서를 서명하는 데 사용하는 공개 키를 식별한다.

③ Key Usage: 인증서에 있는 암호화, 서명, 인증서 서명과 같은 키의 목적을 정의한다.

④ Subject Alternative Name: 인증서의 발급자에 대한 다양한 대체 이름을 제공하는 역할을 한다.

정답 4번

간단한 해설

Subject Alternative Name은 발급자가 아니라 **인증서 주체의 대체 이름**을 제공한다. 발급자의 대체 이름을 나타내는 확장 필드는 Issuer Alternative Name이다.

선지별 해설

① O: Basic Constraints는 인증서 주체가 인증기관(CA)인지 나타낸다. **cA 값이 TRUE**이면 인증서 주체가 CA임을 뜻하며, 이 확장에는 인증 경로의 길이를 제한하는 정보도 포함될 수 있다.

② O: Authority Key Identifier는 **인증서 서명자의 공개 키**를 식별한다. 정확히는 인증서 서명에 사용한 개인 키에 대응하는 공개 키를 가리킨다. 실제 서명은 개인 키로 생성하고, 그 서명을 검증할 때 공개 키를 사용한다. 발급자가 여러 서명 키를 보유한 경우 어떤 키에 대응하는 서명인지 구별하는 데 도움이 된다.

③ O: Key Usage는 인증서에 포함된 **키의 허용 용도**를 정의한다. 암호화, 전자서명, 인증서 서명 등 용도를 비트로 구분하여 표시하므로, 키를 사용할 수 있는 목적을 제한할 수 있다.

④ X: Subject Alternative Name은 인증서를 발급한 기관이 아니라 **인증서 주체**의 대체 이름을 제공한다. DNS 이름, IP 주소, 전자우편 주소 등을 주체의 식별 정보로 담을 수 있다. 선지의 '발급자'를 '주체'로 고쳐야 하며, 발급자의 대체 이름은 Issuer Alternative Name으로 나타낸다.

NoteBase