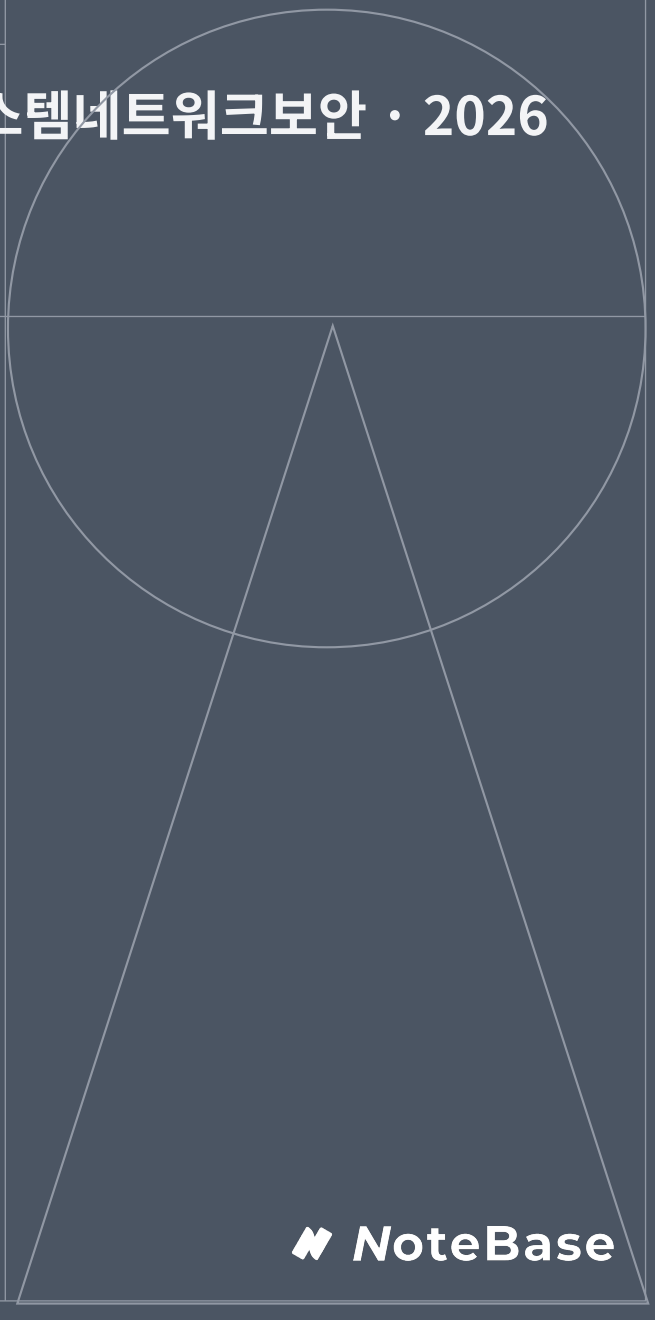
# 기출OX 해설집

공무원/경찰/경력채용 · 시스템네트워크보안 · 2026



NoteBase

# 기출OX 해설집

## 공무원/경찰/경력채용 · 시스템네트워크보안 · 2026

**공무원/경찰/경력채용 · 시스템네트워크보안 · 2026**

**문 1. 인터넷 검색 흔적, 사용자 로그인, 은행이나 신용 계좌 등의 정보를 수집하는 악성소프트웨어로 가장 적절한 것은?**

① 혹스(Hoax)

② 스턱스넷(Stuxnet)

③ 스파이웨어(Spyware)

④ 랜섬웨어(Ransomware)

**정답 3번**

**간단한 해설**

검색 기록, 로그인 정보, 금융 계좌 정보 등을 몰래 수집하는 것은 **스파이웨어**의 대표적인 기능이다. 핵심 단서는 사용자의 활동과 개인 정보를 감시·수집한다는 점이다.

**핵심 풀이**

스파이웨어는 사용자가 알아차리지 못하는 사이에 **활동 내역이나 개인 정보를 수집**하는 악성소프트웨어이다. 검색 흔적, 로그인 정보, 금융 계좌 정보처럼 사용자의 행위와 비밀 정보를 수집한다는 것이 문제의 결정적인 단서이다.

혹스는 거짓 경고나 허위 정보를 유포하여 사용자를 속이는 행위를 가리킨다.

스턱스넷은 산업 제어 시스템을 겨냥한 악성코드이며,

랜섬웨어는 파일 암호화나 접근 차단 등을 통해 복구 대가를 요구하는 것이 대표적인 특징이다. 이들은 문제에서 묻는 정보 수집 중심의 일반적인 유형명과 구별된다.

따라서 가장 적절한 것은 ③ 스파이웨어(Spyware)이다.

NoteBase

**문 2. HTTP(Hyper Text Transfer Protocol)에 관한 설명으로 가장 적절하지 않은 것은?**

① POST 방식은 HTTP Request 형태로 웹브라우저에 요청 데이터에 대한 인수를 URL(Uniform Resource Locator)을 통해 전송한다.

② 웹브라우저와 웹서버 사이에 정보를 교환하기 위한 프로토콜이다.

③ TRACE 방식은 요구 메시지의 최종 수신처까지의 루프백 검사용으로 쓰인다.

④ WWW(World Wide Web)를 위한 프로토콜로 요청과 응답의 형태를 가지고 있다.

**정답 1번**

**간단한 해설**

일반적인 폼 전송에서 **POST는 요청 본문**에 데이터를 담아 서버로 보내고, GET은 폼 인수를 URL 쿼리에 붙인다. HTTP는 요청·응답 프로토콜이며 TRACE는 요청 메시지의 루프백 검사에 사용한다.

**선지별 해설**

① X. 일반적인 HTML 폼 전송에서 POST는 처리할 데이터를 **요청 본문**에 담아 서버로 보낸다. 폼 인수를 URL의 쿼리 문자열에 붙여 전송하는 방식은 GET에 해당하므로, 선지는 POST의 전형적인 데이터 전달 방식과 요청 방향을 잘못 설명했다. 다만 POST 요청의 대상 URL에도 쿼리 문자열을 포함할 수 있으므로, POST에서는 URL 인수를 절대로 사용할 수 없다는 뜻은 아니다.

② O. HTTP는 **클라이언트와 서버 간 정보 교환**을 위한 응용 계층 프로토콜이다. 웹브라우저는 클라이언트의 대표적인 예이며 웹서버와 자원·데이터를 주고받는다.

③ O. TRACE는 요청 메시지에 대한 **응용 계층 루프백 검사**를 요청한다. 최종 수신자가 받은 요청을 응답으로 돌려주게 하여 요청 전달 과정의 시험·진단에 활용한다.

④ O. HTTP는 웹에서 자원을 전송하기 위한 **요청·응답** 프로토콜이다. 클라이언트가 요청을 보내면 서버가 상태와 필요한 데이터를 포함한 응답을 돌려주는 구조를 갖는다.

따라서 가장 적절하지 않은 설명은 ①이다.

NoteBase

**문 3. 다음 중 무선랜 보안 취약점에 관한 대책 방안으로 옳은 것은 모두 몇 개인가?**

㉠ 물리적 보안 및 기본 관리자 패스워드 변경
㉡ SSID 브로드캐스팅 제공
㉢ 무선랜 통신 암호화 및 인증 기술 적용
㉣ AP의 DHCP 제공

① 1개
② 2개
③ 3개
④ 4개

**정답 2번**

**간단한 해설**

무선랜의 보안 대책은 **장비·관리 계정 보호와 통신 암호화·인증**이다. SSID 알림과 DHCP 주소 배포는 네트워크 운영 기능이지, 그 자체로 취약점을 막는 보호 수단은 아니다.

**보기별 해설**

㉠ O: AP 등의 장비에 대한 **물리적 접근을 통제**하고 널리 알려진 기본 관리자 패스워드를 변경하면 무단 설정 변경과 장비 탈취 위험을 줄일 수 있다. 관리 인터페이스 보호를 위한 기본 대책이다.

㉡ X: SSID 브로드캐스팅은 주변 단말에 **무선 네트워크 이름을 알리는 기능**이다. 그 자체가 사용자 인증이나 통신 암호화를 제공하는 보안 대책은 아니다. 반대로 SSID를 숨기는 것만으로 무단 접속이 방지되는 것도 아니다.

㉢ O: 무선 통신에 **적절한 암호화와 인증**을 적용하면 도청과 비인가 접속 위험을 줄일 수 있다. 단순히 네트워크 이름을 숨기거나 주소를 수동 설정하는 것과 달리 통신과 접속 주체를 직접 보호한다.

㉣ X: AP의 DHCP 제공은 단말에 **IP 주소 등 네트워크 설정을 배포**하는 편의 기능이다. DHCP를 제공한다는 사실만으로 무선랜 취약점이 해소되거나 접속자가 인증되는 것은 아니다. DHCP 비활성화 역시 인증·암호화를 대신할 수 없다.

보안 대책에 해당하는 것은 **㉠과 ㉢, 2개**이므로 ②와 연결된다.

NoteBase

**문 4. OSI 7계층 중 ICMP Redirect 공격과 동일한 계층에서 동작하는 프로토콜로 가장 적절한 것은?**

① IPSec(IP Security)

② L2F(Layer 2 Forwarding)

③ L2TP(Layer 2 Tunneling Protocol)

④ PPTP(Point to Point Tunneling Protocol)

**정답 1번**

**간단한 해설**

ICMP Redirect는 **네트워크 계층인 3계층**의 제어 메시지와 관련된다. IP 계층에서 보안 서비스를 제공하는 IPSec도 같은 계층으로 분류한다.

**핵심 풀이**

ICMP는 IP 통신에 관한 오류 보고와 제어 정보를 전달하는 프로토콜로, OSI 대응에서는 **네트워크 계층인 3계층**으로 분류한다. ICMP Redirect는 더 적절한 다음 경로를 호스트에 알리는 메시지이며, 이를 악용해 경로 판단에 영향을 주는 공격 역시 네트워크 계층의 문제로 본다.

IPSec는 **IP 계층에서 패킷을 보호**하는 보안 프로토콜 체계이다. 따라서 ICMP Redirect와 같은 3계층에 해당한다.

L2F·L2TP·PPTP는 PPP 등 링크 계층의 트래픽을 터널로 운반하는 대표적인 2계층 터널링 기술로 분류한다. 실제로 터널을 전송할 때 IP나 UDP 등의 하위 운반 수단을 이용할 수 있지만, 그 사실만으로 이 문제의 터널링 계층 분류가 3계층으로 바뀌는 것은 아니다.

네트워크 계층에서 보안을 제공하는 기술이라는 공통점을 기준으로 고르면 ① IPSec가 해당한다.

NoteBase

**문 5. 스니핑(Sniffing)을 탐지하는 방법으로 가장 적절하지 않은 것은?**

① 의심이 가는 IP 주소에 ping을 보내 ping response가 오는지를 확인한다.

② 미리 계획된 가짜 사용자 ID와 패스워드가 사용되었는지 여부를 분석한다.

③ 테스트 대상 네트워크로 ping sweep을 보내고 들어오는 Reverse-DNS lookup을 확인한다.

④ NAT를 활용하여 외부 네트워크를 모니터링하고 DNS 주소와 IP 주소의 매핑을 감시한다.

**정답 4번**

**간단한 해설**

**NAT는 주소 변환 기능**으로, DNS 이름·IP 대응을 감시하는 스니핑 탐지 방식이 아니다. 따라서 ④가 적절하지 않다. 다른 탐지 기법 역시 특정 조건에서 얻는 단서이며 탐지를 보장하지 않는다.

**선지별 해설**

① O(조건부 탐지 기법의 축약): ping 기반 검사는 탐지용으로 **목적지 MAC 주소 등을 특수하게 설정한 프레임**과 호스트의 수신 모드 동작을 이용하여 비정상 수신 여부를 살펴보는 방식이다. 원문에는 이 조건이 생략되어 있으며, 일반적인 ping 응답만으로는 스니핑 여부를 확인할 수 없다. 또한 운영체제와 필터링 방식에 따라 결과가 달라져 응답 여부만으로 모든 스니퍼를 탐지할 수는 없다.

② O: 정상 사용자가 쓰지 않도록 미리 정한 **미끼 계정과 패스워드**를 통제된 환경의 트래픽에 노출하고, 이후 그 자격정보의 사용 시도를 관찰하면 도청이나 정보 유출을 의심할 수 있다. 다른 유출 경로도 가능하므로 사용 흔적은 조사 단서이지 스니핑만을 확정하는 증거는 아니다.

③ O: 일부 스니퍼는 관찰한 IP 주소의 이름을 표시하기 위해 **역방향 DNS 조회**를 발생시킬 수 있다. 탐지용 트래픽과 연계된 예상 밖의 조회를 관찰하면 스니퍼 존재의 단서가 된다. 이름 조회를 끈 스니퍼는 반응하지 않을 수 있고 정상 프로그램도 조회하므로, 모든 조회를 곧바로 스니핑으로 판정해서는 안 된다.

④ X: **NAT는 IP 주소를 변환하는 기능**이며, DNS의 이름·IP 주소 대응을 감시하여 스니핑을 탐지하는 기법이 아니다. DNS 조회의 발생을 이용하는 탐지 아이디어와 NAT의 주소 변환 기능을 혼동한 설명이다.

NoteBase

**문 6. 필 짐머만(Phil Zimmermann)이 독자적으로 개발한 암호화 E-mail로, 1991년에 IDEA 알고리즘과 RSA 알고리즘을 조합하여 만든 보안 프로토콜로 가장 적절한 것은?**

① PGP(Pretty Good Privacy)

② PEM(Privacy Enhanced Mail)

③ MIME(Multipurpose Internet Mail Extensions)

④ S/MIME(Secure/Multipurpose Internet Mail Extensions)

**정답 1번**

**간단한 해설**

**필 짐머만이 개발한 PGP**를 묻는 문제이다. 1991년 최초 공개라는 역사적 단서와, 전통적인 PGP 2.x의 **IDEA·RSA 혼합 암호** 구성을 구별하여 이해하면 된다.

**핵심 풀이**

개발자 **필 짐머만**과 1991년 최초 공개라는 단서는 PGP를 가리킨다. PGP는 공개키 암호와 대칭키 암호를 함께 사용하는 전자우편·파일 보안 방식이다.

전통적인 PGP 2.x에서 **IDEA는 메시지의 대칭키 암호화**에, **RSA는 세션키 보호와 전자서명**에 이용된다. 본문은 빠른 대칭키 방식으로 암호화하고, 그 암호화 키를 수신자의 공개키로 보호하는 혼합 방식이다. 다만 문제의 연혁은 압축된 설명이다. 1991년은 PGP 1.0 최초 공개 시점이며, IDEA·RSA 조합은 RFC 1991과 RFC 2440이 설명하는 PGP 2.x의 특징으로 구별해야 한다. 최초 공개 버전부터 같은 알고리즘 조합이었다고 단정하지 않는다.

① PGP(Pretty Good Privacy)는 제시된 개발자와 전통적인 혼합 암호 구성에 대응한다.

② PEM(Privacy Enhanced Mail)은 전자우편에 기밀성과 인증 등을 제공하기 위한 별도의 보안 규격이다. 짐머만이 개발한 PGP의 명칭이 아니다.

③ MIME은 다양한 문자·멀티미디어 등의 내용을 전자우편에 담기 위한 **메시지 형식 확장**이다. MIME 자체가 암호화나 전자서명을 제공하는 보안 방식은 아니다.

④ S/MIME은 MIME 메시지에 암호화와 전자서명 등의 보안 기능을 더하는 규격이다. 전자우편 보안이라는 공통점은 있지만, 문제에서 지목한 PGP와는 별개이다.

따라서 가장 적절한 것은 ① PGP이다.

NoteBase

**문 7. 방화벽(Firewall)의 기본적인 역할로 가장 적절하지 않은 것은?**

① 허용 또는 차단된 접근에 대한 기록을 유지한다.

② 통과시킬 접근과 거부할 접근에 따라 허용 또는 차단을 수행한다.

③ 한 시스템의 인증에 성공하면 다른 시스템의 접근 권한을 모두 얻을 수 있다.

④ 내부 네트워크 주소를 외부 공인 네트워크 주소로 전송 단계에서 변경하여 전달한다.

**정답 3번**

**간단한 해설**

방화벽은 **정책에 따라 통신을 허용·차단**하는 장치이다. 한 번 인증되었다고 다른 모든 시스템의 접근 권한을 자동으로 부여하는 것은 방화벽의 역할이 아니다.

**선지별 해설**

① O: 방화벽은 정책에 따라 허용하거나 차단한 통신의 **로그를 기록**할 수 있다. 이러한 기록은 접근 내역 감사, 이상 징후 확인 및 사고 분석에 활용된다.

② O: 방화벽의 핵심 역할은 보안 정책에 따른 **트래픽 접근 통제**이다. 주소, 포트, 프로토콜, 연결 상태 등의 조건을 검사하여 통과시킬 통신과 차단할 통신을 결정한다.

③ X: 한 시스템에서 인증되었다는 이유로 **다른 모든 시스템의 접근 권한**이 자동 부여되지는 않는다. 방화벽은 정책에 따라 접근을 통제한다. 한 번의 인증을 여러 서비스에서 활용하는 SSO와도 구별해야 하며, SSO 역시 각 서비스의 모든 권한을 부여한다는 뜻은 아니다.

④ O: 내부 사설 주소를 외부 공인 주소로 변환하여 전달하는 것은 **NAT(네트워크 주소 변환)**이다. 많은 방화벽 제품이 함께 제공하는 기능이므로 이 문제의 기능 분류에 포함된다. 다만 모든 방화벽의 필수 기능이거나 주소 변환 자체가 접근 통제를 대신하는 것은 아니다.

NoteBase

**문 8. 다음에서 설명하는 프로토콜로 가장 적절한 것은?**

· 논리 주소를 물리 주소와 연관시킨다.
· 송신자는 수신자의 물리 주소를 모르기 때문에 질의 패킷을 네트워크 상에서 브로드캐스트 한다.
· 응답 패킷은 질의 패킷에서 수신된 물리 주소를 사용하여 요청자에게 직접 유니캐스트 된다.

① IP(Internet Protocol)
② ARP(Address Resolution Protocol)
③ TCP(Transmission Control Protocol)
④ ICMP(Internet Control Message Protocol)

**정답 2번**

**간단한 해설**

**IPv4 주소에 대응하는 MAC 주소**를 찾고, 일반적으로 요청은 브로드캐스트하고 응답은 요청자에게 유니캐스트하는 프로토콜은 ARP이다.

**핵심 풀이**

ARP는 같은 링크에서 통신할 대상의 **IPv4 주소에 대응하는 MAC 주소**를 알아내는 프로토콜이다. 제시문의 논리 주소는 IP 주소, 물리 주소는 MAC 주소로 이해하며, 두 주소의 대응 관계를 확인한다는 것이 첫 번째 단서이다.

일반적인 이더넷 환경에서 요청자는 대상의 MAC 주소를 모르므로 ARP 요청을 **브로드캐스트**하여 같은 브로드캐스트 영역의 장치들에 묻는다. 해당 IP 주소를 가진 장치는 요청에 포함된 송신자의 MAC 주소를 이용해 응답을 요청자에게 유니캐스트로 돌려준다. 이는 제시된 질의·응답 방식과 일치한다.

목적지가 다른 네트워크에 있으면 보통 최종 목적지의 MAC 주소가 아니라 같은 링크에 있는 다음 홉 라우터의 MAC 주소를 ARP로 확인한다. ARP 요청이 라우터를 넘어 인터넷 전체로 방송되는 것은 아니다.

IP는 패킷 주소 지정과 전달, TCP는 신뢰성 있는 전송, ICMP는 오류 보고와 제어 메시지를 담당한다. IP와 MAC의 대응 및 브로드캐스트 요청·유니캐스트 응답을 설명한 선택지는 ② ARP이다.

NoteBase

**문 9. TCP에 관한 설명으로 가장 적절하지 않은 것은?**

① TCP에서의 Checksum 포함은 필수 사항이다.

② 전송되는 데이터 byte는 TCP에 의해 항상 0부터 번호가 매겨진다.

③ 세그먼트 내의 확인응답 번호 값은 수신하기를 기대하는 다음 byte의 번호를 나타낸다.

④ 세그먼트 내의 순서 번호 필드의 값은 그 세그먼트에 포함되는 첫 번째 데이터 byte의 번호를 나타낸다.

**정답 2번**

**간단한 해설**

TCP의 실제 순서 번호는 연결마다 선택한 **초기 순서 번호(ISN)**를 기준으로 진행한다. 따라서 전송 바이트에 항상 0부터 번호를 매긴다는 설명은 옳지 않다.

**선지별 해설**

① O: TCP 체크섬은 **필수**이다. 송신 측이 계산해 넣고 수신 측이 검사하며, TCP 헤더와 데이터 및 IP 의사 헤더를 계산에 사용한다.

② X: TCP는 연결 설정 시 **초기 순서 번호(ISN)**를 정하므로, 실제 전송 바이트의 번호가 항상 0에서 시작하는 것은 아니다. SYN이 순서 번호 하나를 사용하므로 첫 데이터 바이트는 ISN 다음 번호부터 시작한다. 분석 도구가 0부터 표시하는 상대 순서 번호와 실제 번호를 혼동하면 안 된다.

③ O: ACK 플래그가 설정되어 유효한 확인응답 번호는 **다음에 받기를 기대하는 순서 번호**이다. 일반적인 데이터 전송에서는 그 앞까지 연속적으로 받았음을 누적 확인하는 의미이다.

④ O: **SYN이 없는 일반 데이터 세그먼트**에서는 순서 번호 필드가 첫 데이터 바이트의 번호를 나타낸다. 다만 SYN이 설정된 세그먼트에서는 이 필드가 ISN이고, 첫 데이터 바이트는 ISN+1이므로 선지의 설명을 SYN까지 예외 없이 적용해서는 안 된다.

NoteBase

**문 10. 다음 중 TCP 세션 하이재킹(Session Hijacking)에 관한 내용으로 옳은 것만을 모두 고른 것은?**

㉠ 세션의 탈취 혹은 탈취 실패에 따라 접속 초기에 예상치 못한 세션의 리셋(Reset)을 경험한다.
㉡ 패킷의 유실과 재전송이 발생하여 서버와의 응답시간이 짧아진다.
㉢ 초기 ACK 패킷의 비율이 급격히 감소한다.
㉣ 서버와 시퀀스 넘버(Sequence Number)를 주기적으로 체크하여 동기화 상태에 빠지는지 확인한다.

① ㉠
② ㉠㉢
③ ㉢㉣
④ ㉠㉡㉣

**정답 1번**

**간단한 해설**

TCP 세션 하이재킹에서는 **비정상 리셋과 통신 상태 불일치**가 의심 징후가 될 수 있다. 재전송은 응답 지연을 늘릴 수 있고, 전형적인 비동기화 공격에서는 ACK 감소보다 반복 ACK 교환이 문제된다.

**보기별 해설**

㉠ O. 세션 탈취 과정에서 RST가 주입되거나 통신 상태가 어긋나면 **예상치 못한 연결 리셋**이 나타날 수 있다. 접속 초기의 비정상 리셋도 의심 징후가 될 수 있다는 의미이다. 모든 하이재킹에서 반드시 발생하거나, 리셋만으로 공격 성공 여부가 확정되는 것은 아니다.

㉡ X. 패킷 유실과 재전송은 기다림과 추가 전송을 유발하므로 일반적으로 **응답 지연이 증가**하는 방향으로 작용한다. 응답시간이 짧아진다는 설명은 반대이다.

㉢ X. 전형적인 비동기화 기반 세션 하이재킹에서는 양 끝의 순서 번호·확인 번호가 어긋나 **중복 ACK의 반복 교환**, 즉 ACK storm이 나타날 수 있다. 따라서 초기 ACK 비율의 급격한 감소를 일반적인 징후로 설명하는 것은 적절하지 않다. ACK storm 역시 구현과 공격 방식에 따라 나타나는 현상이지 모든 공격의 필수 조건은 아니다.

㉣ X. 순서 번호와 확인 번호의 관계를 점검하여 의심해야 할 것은 정상적인 동기화 자체가 아니라 **비동기화·상태 불일치**이다. 정상 통신에서는 양 끝의 송수신 상태가 일관되므로, 동기화 상태에 빠지는지를 공격 이상 징후로 보는 설명은 잘못되었다.

따라서 옳은 보기는 ㉠만이므로 ①이다.

NoteBase

**문 11. 조직 내의 중요 자료가 외부로 유출되는 것을 탐지하여 차단하는 방안으로 가장 적절한 것은?**

① SSO(Single Sign On)

② DLP(Data Loss Prevention)

③ MITM(Man In The Middle)

④ VPN(Virtual Private Network)

**정답 2번**

**간단한 해설**

**DLP**는 중요 정보의 사용과 이동을 감시하고, 정책에 어긋나는 외부 유출을 탐지·차단한다. 인증 통합이나 통신 경로 보호가 아니라 데이터 반출 통제가 핵심이다.

**핵심 풀이**

DLP는 조직의 중요 데이터를 식별하고 사용·저장·전송 과정을 감시하여 **허가되지 않은 정보 유출을 탐지·차단**하는 기술과 관리 방안이다. 자료의 내용이나 전송 대상 등을 정책과 비교하여 반출을 통제한다는 점이 문제의 핵심이다.

SSO는 한 번의 인증을 여러 연계 서비스에서 활용하는 방식이다.

MITM은 통신 당사자 사이에 개입하여 내용을 가로채거나 변조하는 공격이며,

VPN은 공용 네트워크 위에 논리적인 사설 통신 경로를 구성하는 기술이다. VPN의 통신 보호와 자료 반출 자체를 통제하는 DLP는 목적이 다르다.

따라서 중요 자료의 외부 유출을 탐지하고 차단하는 방안으로 가장 적절한 것은 ② DLP(Data Loss Prevention)이다.

NoteBase

**문 12. 리눅스의 파일 링크에 관한 설명으로 가장 적절하지 않은 것은?**

① 파일 링크에는 하드 링크와 심볼릭 링크가 있다.

② 파일 링크에서 파일의 i-node 번호는 ls -i 명령으로 알 수 있다.

③ 파일 링크에서 원본 파일과 하드 링크 파일 존재 확인은 ls -il 명령으로 알 수 있다.

④ 파일 링크에서 링크를 만들기 위해서는 ls 명령어를 이용하여 심볼릭 링크를 만들 수 있다.

**정답 4번**

**간단한 해설**

심볼릭 링크를 만드는 명령은 **ln -s**이다. ls는 파일 정보를 나열하는 명령이므로, ls로 심볼릭 링크를 만든다는 ④가 적절하지 않다.

**선지별 해설**

① O: **하드 링크**는 같은 파일의 i-node를 가리키는 또 다른 이름이며, **심볼릭 링크**는 대상의 경로를 담는 별도 파일이다. 하드 링크는 같은 파일시스템 안에서 생성하는 반면, 심볼릭 링크는 다른 파일시스템의 대상도 경로로 가리킬 수 있다.

② O: **ls -i**는 파일 이름과 함께 i-node 번호를 출력한다. 같은 파일시스템 안에서 두 이름이 같은 i-node 번호를 가지면 같은 파일을 가리키는 하드 링크인지 판단할 수 있다. 서로 다른 파일시스템의 i-node 번호는 같을 수 있으므로 번호만을 전역 식별자로 보아서는 안 된다.

③ O: **ls -il**은 i-node 번호와 자세한 파일 정보를 함께 보여준다. 확인 대상의 이름들을 나열하여 같은 파일시스템에서 i-node 번호가 같은지, 하드 링크 수가 얼마인지 확인할 수 있다. 다만 하드 링크에는 원본과 복사본의 기능상 우열이 없으며, 이 명령이 파일시스템 전체의 모든 하드 링크 경로를 자동 검색하는 것은 아니다.

④ X: 링크를 만드는 명령은 ls가 아니라 **ln**이다. 심볼릭 링크는 **ln -s 대상경로 링크이름**으로 생성한다. ls는 파일과 디렉터리의 정보를 나열하는 명령이므로 링크 생성 명령과 구별해야 한다.

NoteBase

**문 13. 리눅스에서 빈 파일을 새로 생성하거나 파일의 마지막 접근시간 또는 수정시간을 변경하는 명령어로 가장 적절한 것은?**

① grep
② fdisk
③ touch
④ mount

**정답 3번**

**간단한 해설**

**touch**는 파일의 접근·수정 시각을 갱신하며, 대상 파일이 없으면 기본적으로 빈 파일을 생성한다. 기존 파일의 내용을 비우는 명령은 아니다.

**핵심 풀이**

touch는 파일의 **접근 시각과 수정 시각**을 갱신하는 명령어이다. 별도 옵션이 없으면 두 시각을 현재 시각으로 바꾼다. 지정한 파일이 존재하지 않으면 기본 동작으로 빈 파일을 생성하므로, 발문에 제시된 두 기능에 모두 해당한다.

이미 존재하는 파일에 touch를 사용한다고 해서 **기존 내용이 지워지는 것은 아니다**. 기본적으로 파일의 내용은 유지한 채 시각 정보를 바꾼다. 파일이 없을 때 생성하는 기능과 기존 파일을 비우는 동작을 구별해야 한다.

grep은 입력에서 지정한 패턴과 일치하는 행 등을 찾는 명령어이고,

fdisk는 디스크의 파티션 테이블을 관리하는 도구이다.

mount는 파일시스템을 디렉터리 계층에 연결한다. 이들은 파일 시각 갱신을 주기능으로 하는 명령어가 아니다.

따라서 빈 파일 생성과 접근·수정 시각 변경을 설명한 선택지는 ③ touch이다.

NoteBase

**문 14. NAC(Network Access Control)에 관한 설명으로 가장 적절하지 않은 것은?**

① 접근제어 및 인증 기능은 일반적으로 MAC 주소를 기반으로 수행한다.

② 해커를 유인하여 정보를 얻고 해커의 행동과 공격 기법을 분석하는데 사용된다.

③ PC 및 네트워크 장치 통제를 위해 백신관리, 패치관리, 자산관리 기능을 수행한다.

④ 해킹, 웜, 유해 트래픽 탐지 및 차단을 수행한다.

**정답 2번**

**간단한 해설**

NAC의 중심은 **단말·사용자의 네트워크 접근 통제**와 보안 정책 준수 확인이다. 공격자를 유인하여 행동과 공격 기법을 분석하는 목적은 **허니팟**에 해당한다.

**선지별 해설**

① O. NAC는 접속 단말을 식별하고 정책에 따라 네트워크 접근을 허용·제한한다. **MAC 주소 기반 단말 식별·인증**은 그 구현 방식 중 하나이며, 이 문제는 그러한 일반적 단말 통제 기능을 가리킨다. 다만 모든 NAC 인증이 MAC 주소만으로 수행되는 것은 아니며, 사용자 계정·인증서·802.1X 등도 활용된다.

② X. 공격자를 유인하고 그 행동과 공격 기법을 관찰·분석하는 것은 **허니팟**의 대표적인 목적이다. NAC의 중심은 접속 단말·사용자의 신원과 보안 상태를 확인하고 접근 정책을 집행하는 것이다.

③ O. NAC는 단말의 백신 설치·갱신 상태와 패치 적용 여부를 점검하고 자산 정보를 수집하여 **보안 정책 준수 여부**에 따라 접근을 통제할 수 있다. 필요한 조치는 관리 기능이나 다른 솔루션과의 연계를 통해 수행한다. NAC 자체를 백신 엔진과 동일시하는 뜻은 아니다.

④ O. NAC는 이상 행위나 감염 징후를 자체 기능 또는 보안 시스템 연계로 파악하고 **위험 단말의 접근 차단·격리**를 수행할 수 있다. 이를 통해 해킹·웜·유해 트래픽의 확산을 억제한다. 모든 NAC가 모든 공격을 독자적으로 탐지한다는 의미는 아니다.

따라서 NAC에 관한 설명으로 가장 적절하지 않은 것은 ②이다.

NoteBase

**문 15. 다음은 umask 값에 따른 디렉터리(Directory) 권한을 나타낸 표이다. ㉠~㉣에 해당하는 것으로 가장 적절한 것은?**

| umask | 소유자 | 그룹 | 다른 사용자 |
|---|---|---|---|
| 002 | ALL | ALL | ㉠ |
| 022 | ALL | ㉡ | Read, Execution |
| 027 | ㉢ | Read, Execution | None |
| ㉣ | ALL | None | None |

① ㉠: ALL, ㉡: ALL, ㉢: Read, Execution, ㉣: 075

② ㉠: ALL, ㉡: Read, Execution, ㉢: None, ㉣: 075

③ ㉠: Read, Execution, ㉡: Read, Execution, ㉢: ALL, ㉣: 077

④ ㉠: Read, Execution, ㉡: ALL, ㉢: ALL, ㉣: 077

**정답 3번**

**간단한 해설**

디렉터리의 기본 권한 777에서 **umask가 지정한 권한을 제거**한다. 002·022·027은 각각 775·755·750을 만들며, 소유자만 모든 권한을 갖게 하는 마스크는 077이다.

NoteBase

**계산 과정**

이 표는 기본 디렉터리 권한을 777로 놓고 **umask에 지정된 권한 비트를 제거**하여 계산한다. 각 자리에서 읽기 r=4, 쓰기 w=2, 실행·탐색 x=1이며, 7은 ALL(rwx), 5는 Read, Execution(r-x), 0은 None(---)이다. 결과는 비트 연산 777 AND (NOT umask)로 구한다.

umask 002이면 777에서 다른 사용자의 쓰기 비트만 제거하여 **775**가 된다. 따라서 ㉠은 Read, Execution이다.

umask 022이면 그룹과 다른 사용자의 쓰기 비트를 제거하여 **755**가 되므로 ㉡도 Read, Execution이다.

umask 027이면 소유자는 그대로 7, 그룹은 5, 다른 사용자는 0이 되어 **750**이다. 따라서 ㉢은 ALL이다.

소유자만 ALL이고 그룹과 다른 사용자가 None이려면 결과가 700이어야 하므로, 제거할 비트인 ㉣은 **077**이다.

따라서 ㉠=Read, Execution, ㉡=Read, Execution, ㉢=ALL, ㉣=077로 ③과 일치한다. umask는 단순한 십진수 뺄셈 규칙이 아니라 권한 비트를 지우는 규칙이며, 이 표는 별도 기본 ACL 등의 효과가 없는 일반적인 디렉터리 생성 조건을 전제로 한다.

NoteBase

**문 16. 윈도우 인증에 관하여 <보기 1>의 구성요소와 <보기 2>의 설명을 가장 적절하게 연결한 것은?**

<보기 1>
(가) LSA (나) NTLM (다) SAM (라) SRM
<보기 2>
㉠ 인증 프로토콜로서 시도-응답 메커니즘을 기반으로 사용자의 컴퓨터를 인증한다.
㉡ 모든 계정의 로그인에 대한 검증과 시스템 자원 및 파일 등에 대한 접근 권한을 검사한다.
㉢ 사용자/그룹 계정 정보에 대한 데이터베이스를 관리한다.
㉣ 사용자에게 고유의 SID(Security Identifier)를 부여한다.

① (가): ㉡, (나): ㉠, (다): ㉢, (라): ㉣
② (가): ㉡, (나): ㉣, (다): ㉢, (라): ㉠
③ (가): ㉣, (나): ㉢, (다): ㉠, (라): ㉡
④ (가): ㉣, (나): ㉢, (다): ㉡, (라): ㉠

**정답 1번**

**출제 포인트**

윈도우 보안 구성요소의 역할을 구분하고, 제시된 연결 중 가장 적절한 조합을 비교하는 문제이다.

**핵심 개념**

LSA는 사용자 로그인 인증과 로컬 보안 정책을 담당하는 보안 구성요소이며, 로컬 계정과 그룹의 SID를 생성한다.
NTLM은 시도·응답 방식으로 사용자나 컴퓨터의 신원을 확인하는 인증 프로토콜이다.
SAM은 로컬 사용자·그룹 계정 정보를 저장하고 관리하는 구성요소이다.
SRM은 커널에서 시스템 객체에 대한 접근 권한을 검사하고 접근 통제를 집행하는 구성요소이다. SID를 생성하는 구성요소가 아니다.
㉡은 서로 다른 역할을 함께 기술한다. 로그인 검증은 LSA의 역할과 맞지만, 파일 등 시스템 객체의 접근 권한 검사는 SRM의 역할로 구분해야 한다.

NoteBase

### 선지별 해설

아래 O/X는 제공된 정답에 따른 선택 판단이다. O가 해당 선지의 모든 연결이 기술적으로 참이라는 뜻은 아니다.
① O: LSA–㉡은 로그인 검증 부분이 맞고, NTLM–㉠과 SAM–㉢은 각각 시도·응답 인증과 계정 데이터베이스 관리라는 역할에 맞는다. 네 선지 중 NTLM–㉠과 SAM–㉢을 모두 유지하면서 LSA의 로그인 검증 역할도 반영하는 조합은 ①뿐이므로 상대적으로 가장 적절하다. 다만 SRM–㉣은 틀린 연결이다. 로컬 계정의 SID는 LSA가 생성하며, SRM은 생성된 SID 등이 포함된 보안 정보를 이용해 접근 권한을 검사한다. LSA–㉡도 자원 접근 검사까지 모두 LSA가 수행한다는 설명으로 받아들이면 부정확하다.
② X: LSA–㉡은 ①과 마찬가지로 로그인 검증 부분이 맞고 접근 검사 부분에는 한계가 있으며, SAM–㉢은 맞는다. 그러나 NTLM–㉣과 SRM–㉠은 틀리다. NTLM은 SID 부여가 아니라 ㉠의 시도·응답 인증에 연결해야 하고, SRM은 인증 프로토콜이 아니라 시스템 객체의 접근 권한 검사에 연결해야 한다. ㉣의 로컬 계정 SID 생성은 LSA의 역할이다. ①과 공통된 연결을 유지하면서 명확한 NTLM–㉠ 연결까지 잃으므로 ①보다 적절하지 않다.
③ X: LSA–㉣은 로컬 계정 SID 생성이라는 범위에서 맞는다. SRM–㉡도 자원·파일 접근 검사 부분은 맞지만, 로그인 검증까지 SRM이 담당한다는 뜻으로는 틀리다. NTLM–㉢과 SAM–㉠은 역할을 뒤바꾼 잘못된 연결이다. 계정 데이터베이스 관리는 SAM–㉢으로, 시도·응답 인증은 NTLM–㉠으로 고쳐야 한다. LSA와 SRM에 관한 타당한 부분이 있어도 두 핵심 연결을 모두 틀리므로 ①보다 적절하지 않다.
④ X: LSA–㉣은 로컬 계정 SID 생성이라는 범위에서 맞는다. NTLM–㉢, SAM–㉡, SRM–㉠은 틀린 연결이다. NTLM은 ㉠의 시도·응답 인증, SAM은 ㉢의 계정 데이터베이스 관리에 연결해야 한다. SAM의 계정 정보가 로그인 검증에 활용되더라도 SAM이 ㉡의 로그인 검증과 자원 접근 검사 전체를 담당하는 것은 아니다. ㉡의 로그인 검증은 LSA, 자원 접근 검사는 SRM으로 구분하며, SRM을 ㉠의 인증 프로토콜에 연결해서도 안 된다.

### 오답 포인트

①을 선택했다는 이유로 SRM이 SID를 부여한다고 외우는 것이 가장 큰 함정이다. ①에는 잘못된 연결이 남아 있고, ㉡도 LSA와 SRM의 역할을 섞어 기술한다. 반대로 ③·④의 LSA–㉣은 로컬 계정에 대해서는 타당하므로, 그 연결 자체를 오답 이유로 삼으면 안 된다.

### 다시 나오면 이렇게 판단

시도·응답 인증은 NTLM, 계정 데이터베이스 관리는 SAM으로 먼저 연결한다. 이 문항에서는 두 연결을 모두 만족하는 조합이 ①뿐이라는 점으로 상대적 적절성을 판단한다. 이어 로그인 검증과 로컬 SID 생성은 LSA, 시스템 객체 접근 검사는 SRM으로 구분하여 선택 판단과 개별 설명의 사실 여부를 따로 확인한다.

### 암기 포인트

NTLM은 인증 방식, SAM은 계정 저장, LSA는 로그인 인증과 로컬 SID 생성, SRM은 접근 검사이다.

NoteBase

**문 17. 유닉스/리눅스 파일시스템에 관한 설명으로 가장 적절하지 않은 것은?**

① 파일시스템의 구조는 부트블록, 슈퍼블록, i-node 리스트, 데이터 블록 등으로 구성된다.

② 부트블록은 파일 시스템 시작부에 위치하고 일반적으로 첫 번째 섹터를 차지한다.

③ 슈퍼블록은 데이터를 블록 단위로 관리하며, 각 블록은 파일 데이터를 저장하거나 파일 시스템의 내부 구조를 유지하는데 사용된다.

④ 각 파일과 디렉터리는 i-node라는 데이터 구조로 표현되며, i-node는 파일의 메타데이터를 저장하고 데이터 블록에 대한 포인터를 가지고 있다.

**정답 3번**

**간단한 해설**

**슈퍼블록은 파일시스템 전체의 관리 메타데이터**를 저장한다. 일반적인 블록 구성과 데이터 저장을 슈퍼블록의 역할로 설명한 ③이 가장 적절하지 않다.

**선지별 해설**

① O: 전통적인 유닉스 파일시스템의 개념적 배치는 **부트블록·슈퍼블록·i-node 영역·데이터 영역**으로 설명한다. 실제 리눅스 파일시스템에는 블록 그룹, 비트맵, 저널 등 추가 구조가 있을 수 있으므로 모든 구현의 물리 배치가 이 네 영역으로만 고정된다는 뜻은 아니다.

② O: 전통적인 설명에서 부트블록은 **파일시스템 또는 해당 볼륨의 시작 부분에 마련된 부팅용 영역**이며, 첫 섹터의 부트 코드와 연결하여 설명한다. 다만 부트 영역의 실제 크기와 배치는 파일시스템·디스크 형식에 따라 달라지므로 모든 현대 파일시스템에서 정확히 한 섹터만 차지한다는 일반 법칙은 아니다.

③ X: 이 설명은 저장 공간을 블록으로 나누어 파일 내용이나 내부 구조에 사용하는 **파일시스템의 일반적인 블록 구성**에 관한 설명이다. 슈퍼블록의 핵심 역할은 파일시스템의 크기, 블록 수, i-node 수, 사용 가능한 공간과 상태 등 **파일시스템 전체를 관리하는 메타데이터**를 보관하는 것이다. 슈퍼블록을 파일 데이터가 저장되는 블록 영역 전체와 혼동해서는 안 된다.

④ O: i-node는 파일이나 디렉터리의 **종류·권한·소유자·크기·시간 등의 메타데이터**와 데이터 위치를 찾는 정보를 보관한다. 전통적인 방식은 직접·간접 블록 포인터를 사용하며, 구현에 따라 익스텐트 등 다른 블록 매핑 방식도 사용한다.

NoteBase

**문 18. 프로세스에 관한 설명으로 가장 적절하지 않은 것은?**

① 프로세스는 프로그램이 실행되어 메모리에 적재된 상태를 의미한다.

② 프로세스 실행상태는 프로세스에게 중앙처리장치가 할당된 상태이다.

③ 프로세스 메모리 구조는 코드 영역, 데이터 영역, 스택(stack) 영역, 힙(heap) 영역으로 구성되어 있다.

④ 프로세스 완료상태는 프로세스가 중앙처리장치에 할당되기를 기다리는 상태이다.

**정답 4번**

**간단한 해설**

CPU를 할당받기를 기다리는 것은 **준비 상태**이다. 완료 상태는 실행이 끝난 상태이므로 두 상태를 바꾸어 설명한 부분이 잘못되었다.

**선지별 해설**

① O: 프로세스는 실행 중인 프로그램의 인스턴스이다. 실행에 필요한 코드와 데이터가 메모리에 배치되고 실행 문맥과 자원이 관리된다는 의미이다. 단순히 디스크에 저장된 프로그램 파일과 구별되며, 실행 중이라는 말이 매 순간 CPU를 점유한다는 뜻은 아니다.

② O: 실행 상태는 **CPU를 할당받아 명령을 수행하는 상태**이다. 실행할 준비는 되어 있지만 CPU 배정을 기다리는 준비 상태와 다르다.

③ O: 전형적인 프로세스 주소 공간은 명령어를 담는 코드 영역, 전역·정적 변수 등을 담는 데이터 영역, 함수 호출과 지역 변수 등에 쓰이는 스택, 동적 메모리 할당에 쓰이는 힙으로 구분한다. 이는 기본적인 구조 설명이며 실제 주소 공간에는 공유 라이브러리나 메모리 매핑 영역 등이 더 포함될 수 있다.

④ X: CPU를 할당받기를 기다리는 상태는 **준비 상태**이다. 완료 또는 종료 상태는 프로세스의 실행이 끝난 상태이다. 또한 입출력 완료나 특정 사건을 기다리는 대기 상태와 CPU 배정을 기다리는 준비 상태도 구별해야 한다.

NoteBase

**문 19. CPU 스케줄링에서 <보기 1>의 상태에 따른 <보기 2>의 평균 대기 시간으로 가장 적절한 것은?**

<보기 1>

| 프로세스 | 도착시간(ms) | 실행시간(ms) |
|---|---|---|
| P1 | 0 | 30 |
| P2 | 3 | 18 |
| P3 | 6 | 12 |

<보기 2>

(가) FCFS(First Come First Served) 방식의 평균 대기시간
(나) 비선점형 SJF(Shortest Job First) 방식의 평균 대기시간

① (가): 20, (나): 21

② (가): 20, (나): 30

③ (가): 23, (나): 21

④ (가): 23, (나): 30

**정답 3번**

**간단한 해설**

FCFS는 P1→P2→P3, 비선점형 SJF는 P1→P3→P2 순으로 실행한다. **시작시간에서 도착시간을 빼서** 평균 대기시간을 구하면 각각 23 ms와 21 ms이다.

NoteBase

**계산 과정**

주어진 도착시간과 실행시간은 각각 P1이 (0, 30), P2가 (3, 18), P3가 (6, 12)이며 단위는 모두 ms이다. 비선점형에서는 실행을 시작한 프로세스가 완료될 때까지 CPU를 유지하므로, 각 프로세스의 **대기시간 = 실행 시작시간 − 도착시간**으로 계산한다.

(가) FCFS는 **도착 순서**대로 처리한다. 실행 구간은 P1: 0~30, P2: 30~48, P3: 48~60이다. 대기시간은 P1이 0−0=0 ms, P2가 30−3=27 ms, P3가 48−6=42 ms이므로 평균은 $(0 + 27 + 42)/3 = 23$ ms이다.

(나) 비선점형 SJF는 CPU가 비었을 때 **이미 도착한 프로세스 중 실행시간이 가장 짧은 것**을 고른다. 시각 0에는 P1만 도착했으므로 P1을 먼저 실행하고, 이후 더 짧은 작업이 도착해도 중단하지 않는다. 시각 30에는 P2와 P3가 모두 대기 중이므로 실행시간 12 ms인 P3를 먼저, 18 ms인 P2를 나중에 실행한다.

SJF의 실행 구간은 P1: 0~30, P3: 30~42, P2: 42~60이다. 대기시간은 P1이 0 ms, P3가 30−6=24 ms, P2가 42−3=39 ms이므로 평균은 $(0 + 24 + 39)/3 = 21$ ms이다.

따라서 (가) 23 ms, (나) 21 ms에 해당하는 ③이다.

NoteBase

**문 20. 다음의 패킷 필터링 규칙에 관한 설명으로 가장 적절하지 않은 것은? (단, 내부 메일 서버는 192.168.1.11, 내부 FTP 서버는 192.168.1.12이고, 외부 DNS 서버는 10.10.10.20, 외부 메일 서버는 10.10.10.21이다)**

| No | From | Service | To | Action |
|---|---|---|---|---|
| 1 | Any | 80 | Any | Allow |
| 2 | Any | 21 | 192.168.1.12 | Allow |
| 3 | External | 111 | Internal | Deny |
| 4 | 192.168.1.11 | 25 | 10.10.10.21 | Allow |
| 5 | 192.168.1.11 | 143 | 10.10.10.21 | Allow |
| 6 | Internal | 53 | 10.10.10.20 | Deny |
| 7 | Any | Any | Any | Deny |

① 내부에서 외부로의 DNS 접근을 거부한다.

② 내부 서버에서 외부 서버로 전송하는 SMTP 패킷을 허용한다.

③ 내부 서버에서 외부 서버로의 IMAP 접근을 허용한다.

④ 이들 규칙에 해당하지 않는 패킷은 모두 허용한다.

**정답 4번**

**간단한 해설**

마지막 규칙은 출발지·서비스·목적지가 모두 Any이고 동작은 **Deny**이다. 앞선 규칙에 일치하지 않는 패킷은 이 규칙에 따라 모두 차단된다.

NoteBase

**선지별 해설**

① O: DNS의 기본 서비스 포트는 **53번**이다. 규칙 6은 출발지가 Internal이고 목적지가 외부 DNS 서버 10.10.10.20인 53번 포트 접근을 Deny로 처리한다. 따라서 내부에서 해당 외부 DNS 서버로의 접근을 거부한다.

② O: SMTP의 기본 서비스 포트는 **25번**이다. 규칙 4에서 내부 메일 서버 192.168.1.11이 외부 메일 서버 10.10.10.21로 보내는 25번 포트 통신을 Allow로 설정했으므로 허용된다.

③ O: IMAP의 기본 서비스 포트는 **143번**이다. 규칙 5가 내부 메일 서버 192.168.1.11에서 외부 메일 서버 10.10.10.21로의 143번 포트 통신을 Allow로 처리하므로, 제시된 서버 사이의 IMAP 접근은 허용된다.

④ X: 앞선 규칙에 해당하지 않는 패킷은 마지막 규칙 7의 **Any–Any–Any–Deny**에 의해 모두 차단된다. 즉, 허용 규칙에 명시되지 않은 통신을 기본적으로 거부하는 정책이며, 모두 허용한다는 설명은 반대이다.

NoteBase