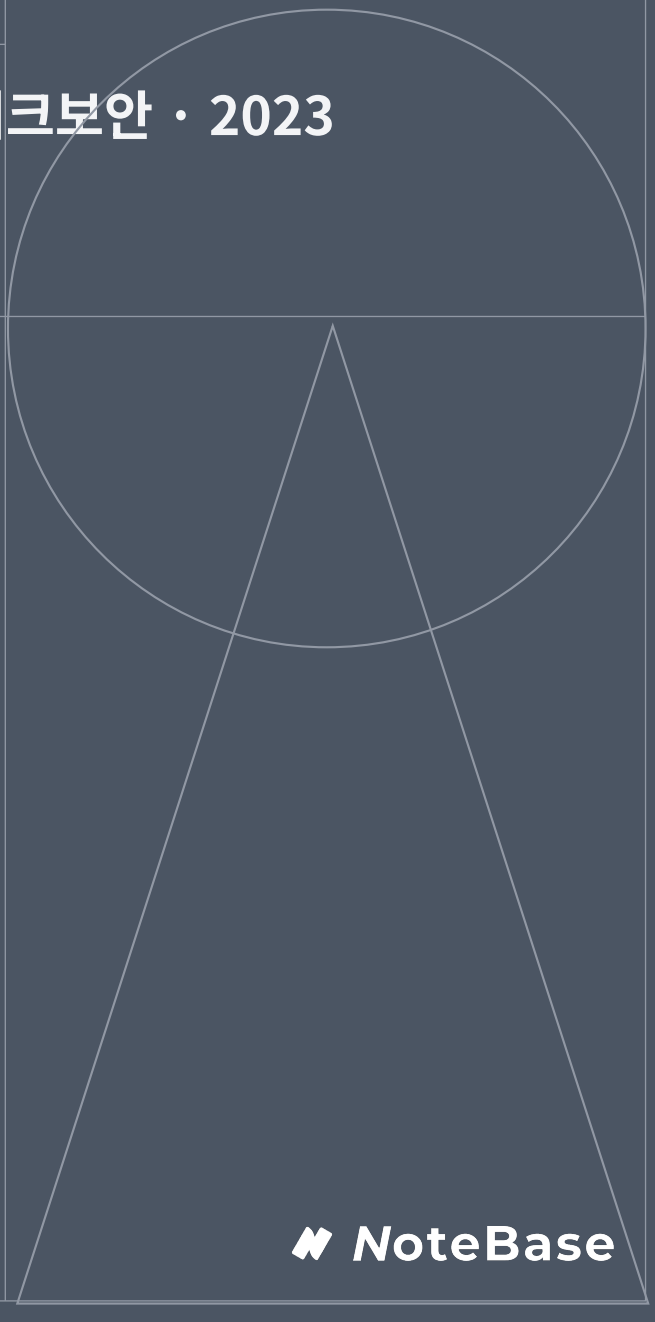
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2023



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2023

공무원/국가직/9급 · 네트워크보안 · 2023

문 1. 다음에서 설명하는 프로토콜은?

◯ 인터넷 환경에서 오류에 관한 처리를 지원한다.
◯ 네트워크 계층의 프로토콜로, 오류가 발생한 IP 패킷에 대하여 그 원인을 송신 호스트에 전달한다.
◯ 전송과정에서 문제가 발생하면 필요할 경우 라우터에 의해 이 프로토콜 메시지가 자동으로 발생한다.

① ICMP
② IGMP
③ ARP
④ FTP

정답 1번

간단한 해설

IP 패킷의 전달 과정에서 생긴 문제를 **송신 호스트에 보고**하는 것은 ICMP의 역할이다. 라우터는 필요한 경우 ICMP 메시지를 생성하여 전달 실패 등의 원인을 알린다.

공통 해설

ICMP(Internet Control Message Protocol)는 IP의 오류 보고와 제어 메시지를 담당하는 네트워크 계층 프로토콜이다. IP 패킷을 처리하던 라우터나 목적지 호스트는 문제가 발생하면 **원래 패킷을 보낸 송신 호스트**에 ICMP 메시지로 그 원인을 알릴 수 있다. 지문의 세 설명은 모두 이 오류 보고 기능을 가리킨다.

예를 들어 라우터가 목적지 네트워크로 패킷을 전달할 수 없으면, 송신 호스트에 '목적지 도달 불가' 메시지를 보낼 수 있다. 여기서 오류 처리를 지원한다는 것은 **문제를 통지한다**는 의미이며, ICMP 자체가 손실된 패킷을 재전송하거나 전달을 보장한다는 뜻은 아니다. 또한 모든 오류에 반드시 메시지가 반환되는 것은 아니므로 지문의 '필요할 경우'라는 조건에 유의한다.

NoteBase

문 2. HTTPS에 의해 암호화되지 않는 통신 요소는?

① 요청 문서 URL

② 문서의 내용

③ 포트 번호

④ HTTP 헤더의 내용

정답 3번

간단한 해설

포트 번호는 통신할 서비스를 식별하는 **전송 계층 헤더의 정보**이므로 HTTPS의 암호화 범위 밖에 있다.
HTTPS는 TLS를 통해 HTTP 메시지를 암호화한다.

선지별 해설

① X: 요청 문서를 가리키는 URL의 **경로와 질의 문자열**은 HTTP 요청에 담겨 TLS로 암호화된다. 따라서 요청한 문서의 구체적인 경로가 평문으로 전송되는 것은 아니다. 다만 도메인 이름은 암호화되지 않은 DNS 조회 등을 통해 드러날 수 있으므로, URL의 모든 구성 요소가 항상 숨겨진다는 뜻은 아니다.

② X: 문서의 내용은 HTTP 응답 본문에 담겨 전달되며, 이 본문도 **TLS의 암호화 대상**이다. 따라서 통신 중인 문서 내용을 암호화하지 않는다는 설명은 맞지 않는다.

③ O: 포트 번호는 전송 계층에서 통신의 종단을 식별하는 정보이다. 예를 들어 TCP 기반 HTTPS에서 목적지 포트 번호는 TCP 헤더에 들어가며, 이 헤더는 **TLS로 암호화되는 HTTP 메시지의 바깥**에 있다. 따라서 HTTPS를 사용해도 전송 계층 헤더의 포트 번호는 암호화되지 않는다.

④ X: HTTP 헤더도 HTTP 메시지의 일부이므로 본문과 함께 TLS로 암호화된다. **HTTP 헤더와 TCP 헤더**를 구별해야 한다. 쿠키나 콘텐츠 유형 등을 담는 HTTP 헤더는 암호화되지만, 포트 번호가 들어 있는 TCP 헤더는 HTTPS의 암호화 범위 밖에 있다.

NoteBase

문 3. 커버로스(Kerberos) 버전4에 대한 설명으로 옳지 않은 것은?

① MIT에서 개발되어 공공 및 상업 영역에서 사용된다.

② 신뢰하는 제3자 인증 서비스를 사용한다.

③ 클라이언트, 응용 서버, 커버로스 서버(키분배센터)로 구성된다.

④ 원격 인증에 사용하기에는 부적절하다.

정답 4번

간단한 해설

커버로스는 **원격 서비스에 접속하는 사용자를 인증**하기 위해 설계되었다. 비밀번호 자체를 네트워크로 보내는 대신 티켓과 인증자를 이용하므로, '원격 인증에 사용하기에는 부적절하다'는 설명이 잘못되었다.

선지별 해설

① O: 커버로스는 **MIT의 Athena 프로젝트**에서 개발된 네트워크 인증 체계이다. 대학·연구기관뿐 아니라 공공 및 상업 영역의 네트워크 인증에도 활용되었다.

② O: 클라이언트와 응용 서버가 함께 신뢰하는 **제3자인 키분배센터(KDC)**를 이용한다. KDC는 각 참여자와 공유하는 비밀키를 바탕으로 티켓과 세션키를 제공하고, 응용 서버는 이를 이용해 클라이언트의 신원을 확인한다.

③ O: 서비스를 요청하는 클라이언트, 서비스를 제공하는 응용 서버, 인증을 지원하는 커버로스 서버(KDC)가 기본 구성 요소이다. KDC의 기능은 **인증 서버(AS)와 티켓 발급 서버(TGS)**로 나뉜다. AS는 최초 인증에 필요한 티켓 발급 티켓(TGT)을 제공하고, TGS는 이를 바탕으로 특정 응용 서버에 제시할 서비스 티켓을 발급한다.

④ X: 커버로스는 **분산 네트워크에서 원격 인증을 제공**하기 위해 설계되었다. 클라이언트는 서비스 티켓과 세션키로 암호화한 인증자를 원격 응용 서버에 제시하고, 서버는 이를 검증해 신원을 확인한다. 따라서 '원격 인증에 사용하기에는 부적절하다'는 표현은 '원격 인증에 사용할 수 있다'로 고쳐야 한다.

NoteBase

문 4. 스니핑(sniffing) 공격에 대한 설명으로 옳은 것은?

① 네트워크 트래픽에서 데이터를 도청하는 수동적 공격이다.

② 네트워크 장비에 대량의 트래픽을 전송하여 서비스를 중단시키는 공격이다.

③ 공격자가 다른 사용자의 IP 주소를 사용하여 네트워크에 접근하는 공격이다.

④ 공격자가 특정 값을 찾아내기 위해 모든 조합을 시도하는 공격이다.

정답 1번

간단한 해설

스니핑은 네트워크를 오가는 패킷을 엿보아 정보를 얻는 **수동적 도청 공격**이다. 통신 내용을 변조하거나 서비스를 중단시키는 것이 아니라, 전송 중인 정보를 몰래 수집하여 기밀성을 침해한다.

선지별 해설

① O: 스니핑은 네트워크 트래픽을 캡처하고 분석하여 전송 중인 데이터를 도청하는 공격이다. 데이터를 바꾸지 않고 관찰하여 정보를 얻는다는 점에서 **수동적 공격**에 해당한다. 예를 들어 암호화되지 않은 통신에서 전송 내용을 읽어 내는 경우가 이에 해당한다.

② X: 대량의 트래픽을 보내 네트워크 대역폭이나 장비의 처리 자원을 소진시키는 것은 **서비스 거부(DoS) 공격**이다. 정상 사용자가 서비스를 이용하지 못하게 하여 가용성을 침해한다. 스니핑의 핵심은 서비스 중단이 아니라 통신 내용의 도청이다.

③ X: 다른 사용자의 IP 주소를 사칭하는 것은 **IP 스푸핑(IP spoofing)**이다. 패킷의 출발지 IP 주소를 위조하여 다른 호스트가 보낸 것처럼 속이는 방식이다. 송신자의 신원을 사칭하는 스푸핑과 전송 정보를 엿듣는 스니핑을 구별해야 한다.

④ X: 특정 값을 알아내려고 가능한 모든 조합을 차례로 시도하는 것은 **무차별 대입(brute force) 공격**이다. 예를 들어 비밀번호 후보를 하나씩 대입해 일치하는 값을 찾는다. 이미 전송되는 데이터를 수집하는 스니핑과 달리, 후보를 반복 시험하여 값을 알아낸다.

NoteBase

문 5. 다음에서 설명하는 기술은?

트래픽의 경로를 지정하는 제어 평면과 트래픽 전송을 수행하는 데이터 평면을 분리하여, OpenFlow 프로토콜 등을 통해 네트워크를 프로그램할 수 있다.

① BSS(Business Support System)
② OSS(Operation Support System)
③ SDN(Software Defined Networking)
④ MPLS(Multi-Protocol Label Switching)

정답 3번

간단한 해설

트래픽의 경로를 결정하는 **제어 평면과 실제 전송을 담당하는 데이터 평면을 분리**하여 소프트웨어로 네트워크를 제어하는 구조가 SDN이다. OpenFlow는 이러한 구조에서 제어 명령을 전달하는 데 쓰이는 프로토콜이다.

공통 해설

SDN(Software Defined Networking)은 **제어 기능과 데이터 전달 기능을 분리**하여 소프트웨어로 네트워크의 동작을 제어하는 기술이다. 제어 평면은 트래픽을 어떤 경로로 보낼지 결정하고, 데이터 평면은 정해진 규칙에 따라 실제 패킷을 전달한다. SDN에서는 컨트롤러가 제어 기능을 담당하고, 스위치 등의 전달 장비가 데이터 전달 기능을 수행한다.

OpenFlow는 컨트롤러와 전달 장비 사이에서 사용하는 프로토콜의 하나이다. 컨트롤러가 OpenFlow를 통해 스위치에 패킷 처리 규칙을 설정하면, 스위치는 그 규칙에 맞춰 패킷을 전달한다. 따라서 지문의 평면 분리와 OpenFlow를 통한 프로그래밍 가능성은 SDN의 구조와 작동 방식을 설명한다.

NoteBase

문 6. SSL/TLS에 대한 공격유형에 해당하지 않는 것은?

① ESP 공격

② PKI 공격

③ 레코드와 응용 데이터 프로토콜 공격

④ 핸드셰이크 프로토콜 공격

정답 1번

간단한 해설

ESP는 **IPsec의 네트워크 계층 보안 프로토콜**이다. 따라서 ESP를 대상으로 한 공격은 SSL/TLS에 대한 공격유형으로 분류하지 않는다.

선지별 해설

① X: ESP(Encapsulating Security Payload)는 IP 패킷을 보호하는 **IPsec의 보안 프로토콜**이다. 선택한 보안 설정에 따라 기밀성, 무결성, 재전송 공격 방지 등의 서비스를 제공한다. ESP 자체가 공격 기법의 이름인 것은 아니며, ESP를 대상으로 한 공격은 SSL/TLS가 아니라 IPsec에 대한 공격으로 구분한다.

② O: PKI(공개키 기반구조)는 인증서를 통해 공개키와 그 소유자의 신원을 연결하는 신뢰 기반이다. 인증서를 사용하는 SSL/TLS 통신에서는 **인증서와 상대방 신원 검증**이 인증의 근거가 된다. 검증을 생략하거나 잘못 수행하면 공격자의 인증서를 정상 서버의 것으로 받아들일 수 있으므로, 이 신뢰 기반을 노리는 PKI 공격도 SSL/TLS 관련 공격에 포함된다.

③ O: 레코드 프로토콜은 응용 데이터를 비롯한 상위 프로토콜의 메시지를 레코드로 나누어 암호화하고 무결성을 보호한다. 이때 **데이터 보호 방식의 취약점**을 이용하면 암호화된 통신에서도 비밀정보가 노출될 수 있다. 예를 들어 SSL 3.0의 CBC 패딩 처리 취약점을 이용하는 POODLE은 이러한 공격에 해당한다.

④ O: 핸드셰이크 프로토콜은 통신 시작 시 암호 알고리즘 등 보안 매개변수를 협상하고, 필요한 인증과 키 설정을 수행한다. 이 과정의 취약점을 이용하는 공격은 **인증과 키 설정 과정**을 겨냥한다. 과거 TLS의 재협상 취약점이나 트리플 핸드셰이크 공격이 이에 해당한다.

NoteBase

문 7. POP3에 대한 설명으로 옳지 않은 것은?

① POP3는 서버로부터 메일을 다운로드하는 기능을 제공한다.

② POP3 서버의 well-known 포트는 25번이다.

③ +OK 응답은 요구한 명령을 성공적으로 처리했음을 의미한다.

④ POP3 클라이언트와 서버는 명령과 응답으로 동작한다.

정답 2번

간단한 해설

②의 '25번'은 SMTP의 well-known 포트이다. POP3 서버의 well-known 포트는 **TCP 110번**이다.

선지별 해설

① O: POP3는 서버의 메일함에 저장된 메일을 **클라이언트로 내려받는** 프로토콜이다. 클라이언트가 RETR 명령으로 특정 메일을 요청하면 서버가 해당 메일의 내용을 전송한다.

② X: POP3 서버의 well-known 포트는 **TCP 110번**이다. 선지의 '25번'은 메일 전송에 사용하는 SMTP의 well-known 포트이므로, '110번'으로 고쳐야 한다.

③ O: +OK는 서버가 명령을 성공적으로 처리했음을 나타내는 **긍정 응답**이다. 명령 처리에 실패한 경우에는 -ERR로 응답한다.

④ O: POP3는 **클라이언트의 명령과 서버의 응답**을 주고받는 방식으로 동작한다. 클라이언트가 메일 목록 조회나 메일 가져오기 등의 명령을 보내면, 서버가 처리 결과와 필요한 데이터를 돌려준다.

NoteBase

문 8. IPv4 데이터그램 형식에 대한 설명으로 옳지 않은 것은?

① ‘Flags’는 단편화(fragmentation)와 관련이 있는 필드이다.

② ‘Time To Live’는 데이터그램이 방문할 수 있는 최대 라우터의 수를 나타내는 필드이다.

③ ‘Total Length’는 헤더를 제외한 IP 데이터그램의 길이를 나타내는 필드이다.

④ ‘Protocol’은 IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 나타내는 필드이다.

정답 3번

간단한 해설

③의 '헤더를 제외한'이 잘못된 표현이다. IPv4의 Total Length는 **헤더와 데이터를 모두 포함한 전체 길이**를 바이트 단위로 나타낸다.

선지별 해설

① O: Flags는 **단편화 허용 여부와 후속 단편의 존재 여부**를 나타낸다. DF가 1이면 단편화를 금지하고, MF가 1이면 뒤에 이어지는 단편이 있음을 뜻한다.

② O: Time To Live(TTL)는 데이터그램이 네트워크에서 무한히 순환하지 않도록 수명을 제한한다. 라우터가 전달할 때마다 **최소 1씩 감소**하고, 감소한 값이 0이 되면 데이터그램을 폐기하므로 실질적으로 거칠 수 있는 라우터의 수, 즉 홉 수의 상한으로 작용한다. 원래는 초 단위의 수명 제한으로 정의되었지만, 이 문항은 이러한 홉 수 제한 기능을 설명한 것이다.

③ X: Total Length는 헤더를 제외한 데이터 길이가 아니라 **IPv4 헤더와 데이터를 합한 전체 길이**를 바이트 단위로 나타낸다. 예를 들어 헤더가 20바이트이고 데이터가 1,000바이트이면 Total Length는 1,020바이트이다. 헤더만의 길이는 별도의 IHL(Internet Header Length) 필드로 나타낸다.

④ O: Protocol은 IP 데이터 부분에 실린 **상위 계층 프로토콜의 종류**를 나타낸다. 수신 측은 이 필드를 보고 IP에서 꺼낸 데이터를 TCP나 UDP 등 해당 프로토콜에 전달한다.

NoteBase

문 9. 다음에서 설명하는 네트워크 관리 기능은?

◯ 가능한 한 효과적인 실행을 보장하기 위하여 네트워크를 감시하고 제어한다.
◯ 통계 정보를 수집하고, 시스템 상태 이력 기록을 유지·검사하며, 시스템 성능을 측정하고, 지연 시간과 대역폭 사용률, 패킷 처리율 등을 단계별 또는 시간별로 관리한다.

① 장애 관리
② 구성 관리
③ 성능 관리
④ 보안 관리

정답 3번

간단한 해설

지연 시간·대역폭 사용률·패킷 처리율은 네트워크의 동작 효율을 나타내는 지표이다. 이 지표를 측정하고 이력을 분석해 효율적인 동작을 유지하는 기능이 **성능 관리**이다.

공통 해설

성능 관리는 네트워크가 얼마나 효율적으로 동작하는지를 측정·평가하고, 필요한 제어를 통해 적절한 성능을 유지하는 기능이다. 관리 기능을 식별하는 기준은 **무엇을 측정하고 관리하는가**이며, 제시문에서는 네트워크의 동작 효율을 나타내는 성능 지표가 그 대상이다.

지연 시간은 데이터 전달에 걸리는 시간, 대역폭 사용률은 사용 가능한 대역폭 중 실제 사용하는 비율, 패킷 처리율은 단위 시간에 처리하는 패킷 수를 나타낸다. 이러한 지표의 통계를 수집하고 시스템 상태 이력을 유지·검사하면 구간별·시간별 성능 변화와 비효율이 나타나는 지점을 파악할 수 있다. 이처럼 성능을 측정하면서 네트워크를 감시·제어한다는 설명은 성능 관리에 해당한다.

NoteBase

문 10. 공개키 기반 구조 X.509(PKIX) 모델에서 종단 개체(end entity)와 인증 기관(certificate authority) 간의 관리 기능에 해당하지 않는 것은?

① 등록(registration)

② 키 쌍 복구(key pair recovery)

③ 키 쌍 갱신(key pair update)

④ 교차 인증(cross-certification)

정답 4번

간단한 해설

교차 인증은 한 인증 기관이 다른 인증 기관의 공개키에 인증서를 발급하는 **인증 기관 간의 관리 기능**이다. 종단 개체와 인증 기관 사이의 관리 기능에는 해당하지 않는다.

선지별 해설

① O: 등록은 종단 개체가 인증서를 발급받기 전에 **인증 기관이나 등록 기관에 자신의 신원을 알리고 확인받는** 절차이다. 이 절차를 거쳐 인증 기관은 해당 종단 개체의 공개키에 대한 인증서를 발급할 수 있다.

② O: 키 쌍 복구는 종단 개체가 키 자료를 잃었을 때 **미리 백업해 둔 키 자료를 되찾는** 기능이다. 예를 들어 복호화용 개인키를 인증 기관이나 관련 백업 시스템에 보관해 두었다면 이를 복구하여 기존 암호문을 다시 복호화할 수 있다. 백업 없이 분실한 개인키를 공개키에서 계산해 내는 기능은 아니다.

③ O: 키 쌍 갱신은 종단 개체의 기존 공개키·개인키 쌍을 **새 키 쌍으로 교체**하고, 새 공개키에 대한 인증서를 발급받는 기능이다. 같은 키를 그대로 두고 인증서의 유효기간만 연장하는 것과 구별된다.

④ X: 교차 인증은 **한 인증 기관이 다른 인증 기관에 인증서를 발급**하여 인증 기관 사이의 신뢰 관계를 형성하는 기능이다. 따라서 이를 종단 개체와 인증 기관 사이의 기능으로 분류하면 안 되며, 인증 기관과 인증 기관 사이의 관리 기능으로 구분해야 한다.

NoteBase

문 11. SMS에 포함된 URL을 클릭하면 악성 앱이 설치되는 스미싱을 예방하는 방법으로 옳지 않은 것은?

① 보호되지 않는 무선 공유기의 사용을 금지한다.

② 스마트폰 환경 설정에서 알 수 없는 출처 앱 설치 기능을 허용한다.

③ 모바일 백신을 설치하여 스마트폰의 보안 상태를 주기적으로 점검한다.

④ 스마트폰 운영체제를 항상 최신 버전으로 업데이트하여 보안상 취약점이 없도록 관리한다.

정답 2번

간단한 해설

알 수 없는 출처의 앱 설치를 허용하면 문자메시지의 링크로 내려받은 악성 앱이 설치될 위험이 커진다. 예방하려면 해당 설치 기능을 **허용하지 않고 차단**해야 한다.

선지별 해설

① O: 보호되지 않는 무선 공유기는 통신 내용의 도청이나 악성 사이트로의 유도 등에 악용될 수 있다. 이런 공유기의 사용을 피하는 것은 **접속 경로의 위험을 줄이는** 스마트폰 보안 조치이다. 다만 이것만으로 문자메시지를 통한 악성 앱 설치까지 차단되는 것은 아니다.

② X: '알 수 없는 출처 앱 설치 기능을 허용한다'는 설정은 공식 앱 마켓 외의 경로로 받은 앱도 설치할 수 있게 하므로 악성 앱의 유입 위험을 높인다. 스미싱을 예방하려면 **알 수 없는 출처의 앱 설치를 차단**하고, 출처가 확인되지 않은 문자메시지의 URL을 누르지 않아야 한다.

③ O: 모바일 백신은 악성 앱 등을 탐지하여 감염을 예방하거나 발견하는 데 도움을 준다. 설치 후 **주기적으로 보안 상태를 점검**하고 백신도 업데이트하면 악성 앱에 대응하는 데 도움이 된다.

④ O: 운영체제 업데이트에는 발견된 보안 취약점을 보완하는 패치가 포함될 수 있다. 최신 버전을 유지하면 **알려진 취약점을 악용한 공격 위험**을 줄일 수 있다. 다만 최신 버전이라는 이유만으로 모든 취약점이 없어지거나 악성 앱 설치가 완전히 방지되는 것은 아니다.

NoteBase

문 12. 다음에서 설명하는 보안 기술은?

◯ 사전에 수립한 규칙에 따라 패킷을 차단 또는 허용한다.
◯ 접근 제어가 가장 기본적이고 중요한 기능이다.
◯ 구현 방식에 따라 패킷 필터링과 프록시 방식 등이 있다.

① SSO
② VLAN
③ DLP
④ Firewall

정답 4번

간단한 해설

사전에 정한 규칙에 따라 패킷을 허용하거나 차단하는 것은 **방화벽(Firewall)**의 접근 제어 기능이다. 패킷 필터링과 프록시는 이를 구현하는 방식이다.

공통 해설

방화벽(Firewall)은 네트워크 사이를 오가는 트래픽에 보안 정책을 적용하여 **허용된 통신은 통과시키고 허용되지 않은 통신은 차단**하는 보안 기술이다. 여기서 접근 제어란 어떤 통신을 허용할지 미리 규칙으로 정하고, 실제 통신이 그 규칙에 맞는지 검사하는 것을 뜻한다.

패킷 필터링 방식은 출발지·목적지 IP 주소, 포트 번호, 프로토콜 등의 정보를 규칙과 비교하여 패킷의 통과 여부를 결정한다. 프록시 방식은 클라이언트와 서버 사이에서 통신을 대신 처리하며 보안 정책에 따라 요청을 허용하거나 차단한다. 따라서 지문의 규칙 기반 패킷 제어, 접근 제어 기능, 패킷 필터링·프록시 구현 방식은 모두 방화벽을 가리키는 단서이다.

NoteBase

문 13. 다음에 기술된 IEEE 802.11i RSN의 동작 단계를 순서대로 나열한 것은?

(가) 인증(authentication)
(나) 탐색(discovery)
(다) 안전 데이터 전송(protected data transfer)
(라) 키 생성 및 분배(key generation and distribution)

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

정답 3번

간단한 해설

통신할 AP와 보안 방식을 먼저 정해야 인증을 진행할 수 있다. 또한 **인증 후 데이터 보호용 키를 설정**해야 그 키로 데이터를 안전하게 전송할 수 있다.

올바른 순서

(나) → (가) → (라) → (다)

(나) 탐색: 무선 단말이 접속할 액세스 포인트(AP)를 찾고, AP가 알리는 보안 기능을 확인하여 사용할 인증 방식과 암호화 방식 등을 선택한다. **접속 대상과 보안 방식을 정한 뒤** 그에 맞는 인증 절차를 진행한다.

(가) 인증: 탐색 단계에서 선택한 인증 방식에 따라 통신 주체의 신원을 확인한다. 데이터 보호용 키를 설정하기에 앞서 **통신 상대가 정당한지 확인**하는 단계이다.

(라) 키 생성 및 분배: 인증 절차를 거친 뒤 실제 데이터 보호에 사용할 암호키를 생성·분배하고 무선 단말과 AP에 설정한다. 양쪽이 데이터를 암호화하고 검증하려면 **데이터 전송 전에 필요한 키가 준비**되어야 한다.

(다) 안전 데이터 전송: 앞 단계에서 정한 보안 방식과 설정한 키를 이용하여 무선 단말과 AP 사이의 데이터를 보호한다. 이때 암호화와 무결성 검증으로 데이터의 노출과 변조에 대응하므로, 키 설정을 마친 뒤 수행한다.

NoteBase

문 14. SNMP에서 관리 대상 장치 내부 객체들에 대한 정보 저장소를 나타내는 용어는?

① MIB

② Community

③ PDU

④ Agent

정답 1번

간단한 해설

SNMP에서 관리 대상 장치의 객체 정보를 체계적으로 모아 둔 저장소를 **MIB(Management Information Base)**라고 한다.

공통 해설

MIB(Management Information Base, 관리 정보 베이스)는 SNMP로 관리하는 객체들의 정보를 모아 놓은 **논리적 정보 저장소**이다. 장치의 상태나 통신량처럼 관리에 필요한 정보를 객체로 표현하며, 관리자는 SNMP를 통해 해당 객체의 값을 조회한다. 예를 들어 장치의 네트워크 인터페이스 상태를 확인할 때는 그 상태를 나타내는 관리 객체의 값을 읽는다. 문제에서 묻는 '관리 대상 장치 내부 객체들에 대한 정보 저장소'는 이러한 관리 정보의 집합인 MIB를 뜻한다.

NoteBase

문 15. 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격은?

① DNS 스푸핑 공격

② E-mail 스푸핑 공격

③ IP 스푸핑 공격

④ ICMP 리다이렉트 공격

정답 4번

간단한 해설

ICMP 리다이렉트는 호스트에 **패킷을 보낼 다음 라우터의 변경**을 알리는 메시지이다. 이를 위조하여 패킷이 스니핑 시스템을 거치도록 유도하는 것이 ICMP 리다이렉트 공격이다.

공통 해설

ICMP 리다이렉트는 라우터가 호스트에 특정 목적지로 패킷을 보낼 때 사용할 더 적절한 다음 라우터를 알려 주는 기능이다. 여기서 다음 홉은 목적지까지 가는 경로에서 패킷을 바로 넘겨줄 대상을 뜻한다. 호스트는 유효한 리다이렉트 메시지를 받아 해당 목적지의 다음 홉 정보를 갱신한다.

ICMP 리다이렉트 공격은 이 기능을 악용하여 정상 라우터가 보낸 것처럼 거짓 메시지를 보내고, **스니핑 시스템을 다음 홉으로 지정**한다. 피해 호스트가 그 안내를 받아들이면 해당 목적지로 보내는 패킷이 스니핑 시스템을 거치게 되어 도청할 기회가 생긴다. 문항의 '또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는' 동작이 이 방식에 해당한다.

후보를 구별하는 기준은 **경로 안내 메시지로 다음 홉을 바꾸는가**이다. DNS 응답, 메일 발신자 또는 IP 출발지 주소를 위장한다는 사실만으로는 문항의 라우터 변경 안내를 설명할 수 없다.

NoteBase

문 16. 다음과 같이 각 문자에 숫자를 배정할 때, 시저 암호 치환식 C=(P+3) 26을 활용하여 평문 STUDY를 암호화한 것은? (단, 치환식에서 C는 암호문, P는 평문이다)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

① VWXGB

② UVWFA

③ TUVEZ

④ VWXFN

정답 1번

간단한 해설

각 문자에 배정된 숫자에 **3을 더하고 26으로 나눈 나머지**를 다시 문자로 바꾼다. STUDY는 VWXGB로 변하며, 특히 Y는 24 + 3 = 27에서 나머지 1에 해당하는 B가 된다.

계산 과정

문자표는 A부터 Z까지 0~25를 배정한다. 평문 문자의 숫자를 P, 암호문 문자의 숫자를 C로 두면, 주어진 치환식은 C=(P+3) 26이다. 각 숫자에 3을 더한 뒤 **26으로 나눈 나머지**를 구하므로, 결과가 26 이상이면 다시 문자표의 처음으로 돌아간다.

S: 문자표에서 S는 18이다. 18 + 3 = 21이고, 21은 26보다 작으므로 나머지도 21이다. 21에 해당하는 문자는 V이다.

T: 문자표에서 T는 19이다. 19 + 3 = 22이고, 나머지 22에 해당하는 문자는 W이다.

U: 문자표에서 U는 20이다. 20 + 3 = 23이고, 나머지 23에 해당하는 문자는 X이다.

D: 문자표에서 D는 3이다. 3 + 3 = 6이고, 나머지 6에 해당하는 문자는 G이다.

Y: 문자표에서 Y는 24이다. 24 + 3 = 27이며, 27을 26으로 나눈 나머지는 1이다. **27을 그대로 쓰지 않고 나머지 1로 바꾸므로** Y는 B로 치환된다.

원래 문자 순서대로 치환 결과를 연결하면 VWXGB가 되며, 이는 ①의 암호문과 일치한다.

NoteBase

문 17. SSL Handshake 프로토콜의 2단계 '서버 인증과 키 교환(server authentication and key exchange)'에서 인증서(certificate) 메시지가 사용되지 않는 기법은?

① RSA 기법

② Anonymous DH 기법

③ Ephermeral DH 기법

④ Fixed DH 기법

정답 2번

간단한 해설

Anonymous DH는 **서버의 신원을 인증하지 않고** DH 공개값을 교환하여 공통 비밀값을 만드는 방식이다. 따라서 서버 인증을 위한 certificate 메시지를 사용하지 않는다.

선지별 해설

① X: RSA 키 교환에서는 **서버의 RSA 공개키가 담긴 인증서**를 사용한다. 클라이언트는 서버 인증서를 검증한 뒤, 서버 공개키로 사전 마스터 비밀값을 암호화하여 전달한다. 따라서 인증서 메시지를 사용하지 않는 기법에 해당하지 않는다.

② O: Anonymous DH는 **인증 없이 DH 키 교환**을 수행한다. 서버는 인증서 대신 서버 키 교환 메시지로 DH 공개값 등을 전달하고, 클라이언트도 자신의 DH 공개값을 전달하여 공통 비밀값을 계산한다. 서버 신원을 확인하는 인증서 메시지는 사용하지 않는다.

③ X: 임시 DH는 연결에 사용할 임시 DH 키를 생성하지만, **임시 키 사용이 인증 생략을 뜻하지는 않는다**. 서버는 임시 DH 매개변수에 자신의 개인키로 서명하고, 클라이언트는 서버 인증서의 공개키로 그 서명을 검증한다. 따라서 서버 인증서 메시지가 필요하다.

④ X: Fixed DH는 **고정 DH 공개키와 매개변수를 서버 인증서에 포함**하여 전달한다. 클라이언트는 인증서를 검증하여 해당 공개키가 서버의 것임을 확인한다. 이 경우 생략되는 것은 별도의 서버 키 교환 메시지이며, 인증서 메시지는 사용한다.

NoteBase

문 18. 전자 서명(digital signature)에 대한 설명으로 옳지 않은 것은?

① 서명된 문서는 기밀성이 보장된다.

② 서명된 문서는 데이터가 변조되지 않았음을 보장하는 무결성을 만족한다.

③ 한 번 생성된 서명을 다른 문서의 서명으로 사용할 수 없다.

④ 전자 서명과 관련된 표준으로 DSS가 있다.

정답 1번

간단한 해설

전자 서명은 문서의 변조 여부와 서명자를 확인하는 수단으로, **서명만으로 기밀성이 보장되지는 않는다**. 문서 내용을 다른 사람이 읽지 못하게 하려면 암호화 등의 별도 보호가 필요하다.

선지별 해설

① X: 기밀성은 허가받지 않은 사람이 정보 내용을 알 수 없게 하는 성질이다. 전자 서명은 문서 내용의 공개를 막는 기능이 없으므로, **서명만으로 기밀성을 보장하지 않는다**. 서명된 문서도 평문으로 전달하면 내용을 읽을 수 있으며, 기밀성을 확보하려면 암호화 등의 별도 보호가 필요하다.

② O: 전자 서명은 **서명 이후 문서가 변조되었는지 검증**할 수 있게 하여 무결성을 제공한다. 서명자는 문서의 해시값을 바탕으로 개인키로 서명을 생성하고, 수신자는 해당 문서와 서명자의 공개키를 이용해 서명을 검증한다. 안전한 서명 방식에서는 문서 내용이 바뀌면 기존 서명의 검증이 실패하므로 변조를 탐지할 수 있다.

③ O: 전자 서명은 **서명 대상 문서의 내용에 종속**된다. 다른 내용의 문서에 기존 서명을 옮겨 붙여도 그 문서의 유효한 서명으로 검증되지 않도록 설계된다. 따라서 한 문서에 생성한 서명을 다른 문서의 서명으로 재사용할 수 없다.

④ O: DSS는 **Digital Signature Standard**의 약자로, 미국 국립표준기술연구소(NIST)의 전자 서명 표준이다. 전자 서명을 생성하고 검증하는 알고리즘을 규정한다.

NoteBase

문 19. NAC(Network Access Control) 시스템에 대한 설명으로 옳지 않은 것은?

① ARP 방식은 차단하려는 단말에 ARP 스푸핑 패킷을 보내 네트워크 접근을 제어한다.

② 802.1x 방식은 802.1x RADIUS 서버와 802.1x를 지원하는 스위치가 필요하다.

③ 소프트웨어 에이전트 설치 방식은 네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치할 필요는 없다.

④ VLAN 방식은 인가받지 않은 클라이언트가 인가된 클라이언트와는 다른 별도의 VLAN으로 격리된다.

정답 3번

간단한 해설

소프트웨어 에이전트 설치 방식은 **접속하려는 각 클라이언트에 에이전트를 설치**하여 보안 상태를 점검하고 정책을 적용한다. 따라서 모든 클라이언트에 설치할 필요가 없다는 설명은 이 방식의 전제에 어긋난다.

선지별 해설

① O: ARP 방식은 차단할 단말에 ARP 스푸핑 패킷을 보내 **IP 주소와 MAC 주소의 대응 정보를 거짓으로 알리는** 방식이다. 단말의 트래픽을 통제 장비로 향하게 한 뒤 폐기하는 등의 방법으로 정상적인 네트워크 접근을 차단한다.

② O: 802.1X 방식은 **인증 결과에 따라 스위치 포트의 접근을 제어**한다. 802.1X를 지원하는 스위치가 클라이언트와 인증 서버 사이의 인증 메시지를 중계하고, RADIUS 서버가 인증을 수행한다. 따라서 이 구성을 위해서는 802.1X 지원 스위치와 RADIUS 인증 서버가 필요하다.

③ X: 소프트웨어 에이전트 설치 방식은 클라이언트에 설치된 프로그램이 보안 상태를 수집·보고하고 단말에 보안 정책을 적용하는 방식이다. 에이전트가 없는 단말에서는 해당 프로그램을 통한 상태 점검과 제어를 수행할 수 없으므로, 이 방식으로 관리할 **모든 클라이언트에 에이전트를 설치해야 한다**. 선지의 '설치할 필요는 없다'는 '설치해야 한다'로 고친다.

④ O: VLAN 방식은 인가받지 않은 클라이언트를 **인가된 클라이언트와 다른 VLAN으로 격리**한다. VLAN은 네트워크를 논리적으로 나누는 기능이므로, 격리 VLAN에서 업무 VLAN으로의 통신을 제한하여 내부 자원에 대한 접근을 통제한다.

NoteBase

문 20. IPSec에 대한 설명으로 옳지 않은 것은?

① 네트워크 계층에서 동작하는 보안 프로토콜이다.

② 트래픽을 암호화하고, 무결성을 보장하며, 인증을 제공한다.

③ 전송 모드와 터널 모드가 있다.

④ IPSec에서 AH 프로토콜은 페이로드 데이터를 암호화한다.

정답 4번

간단한 해설

AH는 데이터의 **무결성과 송신 출처 인증**을 제공하지만 **암호화는 제공하지 않는다**. IPSec에서 페이로드를 암호화하여 기밀성을 제공하는 프로토콜은 ESP이다.

선지별 해설

① O: IPSec은 **네트워크 계층인 IP 계층**에서 IP 패킷을 보호하는 보안 프로토콜 체계이다. 따라서 TCP·UDP 등 IP 위에서 동작하는 여러 상위 프로토콜의 트래픽에 보안 서비스를 적용할 수 있다.

② O: IPSec은 암호화를 통한 기밀성, 데이터의 변조 여부를 확인하는 무결성, 데이터가 정당한 송신 출처에서 왔는지 확인하는 인증을 제공할 수 있다. 다만 **실제 제공되는 서비스는 사용하는 프로토콜과 설정에 따라 달라진다**. AH는 무결성과 송신 출처 인증을 제공하고, ESP는 암호화를 통한 기밀성도 제공할 수 있다.

③ O: IPSec에는 **전송 모드와 터널 모드**가 있다. 전송 모드는 기존 IP 헤더를 유지하면서 상위 계층 데이터를 보호하며, AH를 사용하면 IP 헤더의 일부 필드도 인증 범위에 포함된다. 터널 모드는 원래 IP 패킷 전체를 새 IP 패킷 안에 넣고 외부 IP 헤더를 덧붙여 전송하므로, 내부 IP 헤더까지 보호 대상에 포함할 수 있다.

④ X: AH는 인증 정보를 이용해 데이터의 변조 여부와 송신 출처를 확인하지만, **페이로드 데이터를 암호화하지 않는다**. 따라서 'AH 프로토콜은 페이로드 데이터를 암호화한다'는 'ESP 프로토콜은 암호화를 사용하여 페이로드 데이터의 기밀성을 제공할 수 있다'로 고쳐야 한다. 인증은 데이터의 출처와 변조 여부를 확인하는 기능이고, 암호화는 데이터 내용을 알아볼 수 없게 만드는 기능이다.

NoteBase