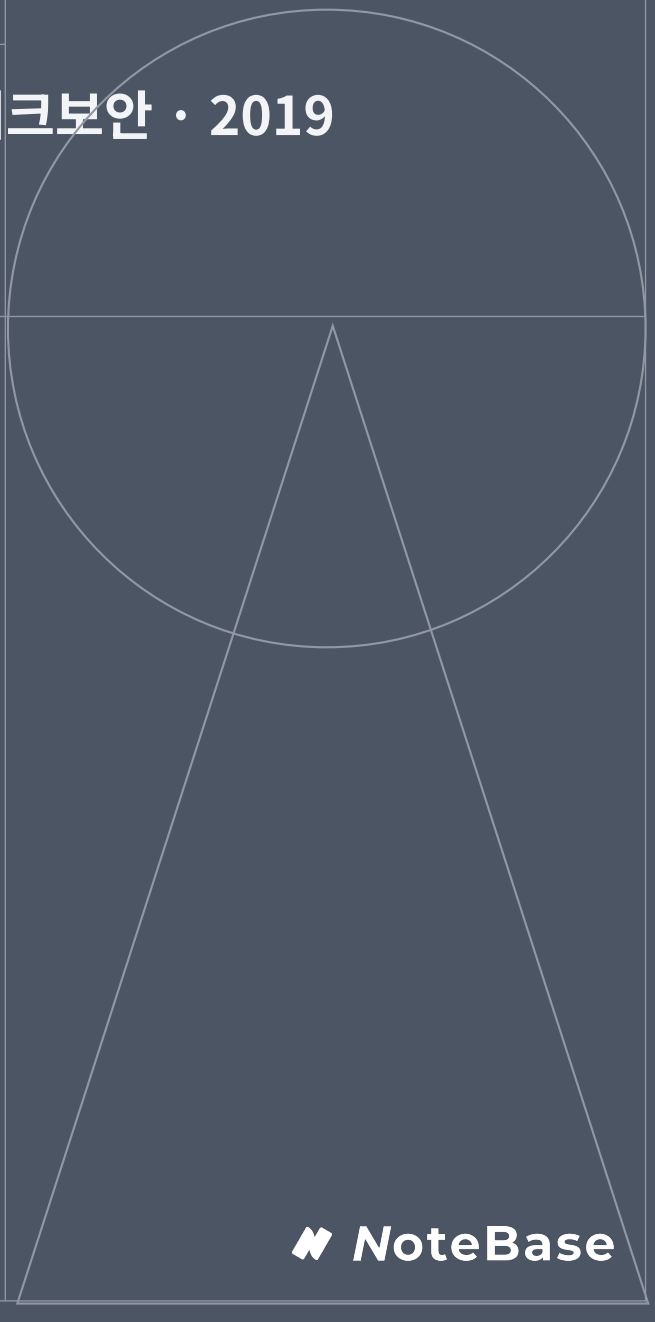
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2019



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2019

공무원/국가직/9급 · 네트워크보안 · 2019

문 1. 네트워크 관리자가 원격으로 네트워크 장비를 모니터링하고 환경 설정을 수행하고자 할 때, 네트워크 구성 요소에 의해 유지되는 변숫값을 조회하거나 변경할 수 있도록 고안된 프로토콜은?

① FTP

② NFS

③ SNMP

④ SMTP

정답 3번

간단한 해설

SNMP는 네트워크 장비가 유지하는 관리 객체의 값을 조회하거나 변경하는 프로토콜이다. 이 기능으로 원격에서 장비 상태를 감시하고 설정을 조정한다.

공통 해설

SNMP(Simple Network Management Protocol)는 네트워크 관리에 사용하는 프로토콜이다. 관리 대상 장비의 에이전트는 장비 상태와 설정을 관리 객체로 제공하며, 이러한 객체는 MIB(Management Information Base, 관리 정보 베이스)에 정의된다. 관리자는 장비의 관리 객체에 접근하여 원격 감시와 설정을 수행한다.

관리자는 **Get 요청으로 값을 조회**하고 **Set 요청으로 값을 변경**한다. 예를 들어 인터페이스의 송수신량을 조회하면 통신 상태를 감시할 수 있고, 쓰기가 허용된 인터페이스 관리 상태를 변경하면 동작 설정을 조정할 수 있다. 모든 객체를 변경할 수 있는 것은 아니며, 쓰기 가능한 객체에 대해 필요한 접근 권한이 있어야 한다. 따라서 문제의 '네트워크 구성 요소에 의해 유지되는 변숫값을 조회하거나 변경'한다는 설명은 SNMP의 관리 객체 접근 기능을 뜻한다.

NoteBase

문 2. 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격 기법은?

① 스위치 재밍

② IP 스푸핑

③ DNS 스푸핑

④ ARP 스푸핑

정답 4번

간단한 해설

ARP 스푸핑은 IP 주소에 대응하는 MAC 주소 정보를 공격자의 MAC 주소로 속여, 전송될 데이터를 공격자에게 향하게 하는 기법이다. 핵심은 **IP 주소와 MAC 주소의 대응 관계를 위조**한다는 점이다.

공통 해설

ARP는 IPv4 기반 근거리 통신망에서 통신할 상대의 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 컴퓨터는 이 대응 정보를 ARP 캐시에 저장하고, 실제 프레임을 보낼 때 목적지 MAC 주소를 정하는 데 이용한다. ARP 스푸핑은 거짓 ARP 정보를 보내 이 캐시에 **정상 상대의 IP 주소와 공격자의 MAC 주소가 연결되도록** 하는 공격이다. 이에 따라 해당 상대에게 보낼 프레임이 공격자에게 전달되어 데이터를 가로챌 수 있다.

예를 들어 피해 컴퓨터가 게이트웨이의 IP 주소에 대응하는 MAC 주소를 공격자의 것으로 저장하면, 게이트웨이로 보낼 데이터가 먼저 공격자에게 향한다. 문제의 MAC 주소 변경은 장치 자체의 물리 주소를 바꾸는 것이 아니라, **ARP 캐시에 저장된 주소 대응 정보를 속이는 것**으로 이해한다. 이 대응 관계의 위조가 주어진 공격을 ARP 스푸핑으로 식별하는 기준이다.

NoteBase

문 3. 라우터 외부로 나가는 패킷의 소스 IP만을 검사하여 필터링하는 것으로, 라우터 내부의 네트워크에서 소스 IP를 위조하여 다른 네트워크를 공격하는 형태의 공격을 차단하는 필터링 기법은?

① ingress 필터링
② egress 필터링
③ black hole 필터링
④ null routing을 이용한 필터링

정답 2번

간단한 해설

egress 필터링은 내부에서 외부로 나가는 패킷을 검사한다. 소스 IP가 내부 네트워크에서 사용할 수 있는 주소 범위에 속하는지 확인하여, 외부 주소로 위조한 패킷이 다른 네트워크로 나가는 것을 차단한다.

공통 해설

egress는 네트워크를 기준으로 밖으로 나가는 방향을 뜻한다. 이 문항의 egress 필터링은 경계 라우터에서 외부로 나가는 패킷의 소스 IP, 즉 출발지 주소를 확인하고, **내부 네트워크에 허용된 출발지 주소 범위**에 속하지 않는 패킷을 버리는 방식이다. '외부로 나가는 패킷의 소스 IP 검사'라는 조건이 이 기법을 식별하는 기준이다.

예를 들어 내부 컴퓨터가 다른 네트워크의 주소를 자신의 출발지 주소처럼 적어 패킷을 보내면, 라우터는 허용 범위를 벗어난 소스 IP를 확인하여 그 패킷을 차단한다. 이로써 내부 컴퓨터가 출발지를 속여 외부를 공격하는 것을 막는다. 다만 허용된 주소 범위 안에서 이루어진 위조나 정상 출발지 주소를 사용하는 공격까지 모두 차단한다는 뜻은 아니다.

NoteBase

문 4. 전자금융거래상에서 사용되는 접속정보 및 거래정보, 단말기 정보 등을 종합적으로 분석하여 의심되는 거래를 탐지하고 이상 금융거래를 차단하는 시스템으로, 일반적인 보안 프로그램에서 방지하지 못하는 전자금융사기의 이상거래를 탐지하고 조치할 수 있는 기법은?

① STP

② ARIA

③ SARA

④ FDS

정답 4번

간단한 해설

접속정보·거래정보·단말기 정보를 함께 분석하여 의심스러운 금융거래를 탐지하고 차단하는 시스템은 **FDS(이상금융거래탐지시스템)**이다. 거래가 이루어지는 환경과 거래 패턴을 분석한다는 점이 핵심이다.

공통 해설

FDS는 Fraud Detection System의 약자로, 전자금융거래의 접속정보·거래정보·단말기 정보 등을 종합적으로 분석하여 이상금융거래를 탐지하고 차단하는 시스템이다. 판단 대상은 **거래 자체의 이상 징후**이므로, 일반적인 보안 프로그램만으로 막기 어려운 금융사기를 탐지하는 데 활용된다.

예를 들어 평소 사용하지 않던 단말기에서 짧은 시간에 반복적으로 이체가 발생하면, 접속 환경과 거래 패턴을 함께 분석하여 의심거래인지 판단할 수 있다. 문제의 '여러 정보를 종합적으로 분석하여 의심거래를 탐지하고 차단한다'는 설명은 이러한 FDS의 기능에 해당한다.

NoteBase

문 5. 사설 네트워크 용도로 사용되는 사설 IPv4 주소에 해당하는 것은?

① 10.10.20.300

② 168.10.40.11

③ 172.16.10.20

④ 192.10.20.30

정답 3번

간단한 해설

172.16.10.20은 사설 IPv4 주소 대역인 **172.16.0.0~172.31.255.255**에 포함된다. 172로 시작하는 주소 전체가 사설 주소인 것은 아니며, 두 번째 숫자가 16~31인 범위에 해당해야 한다.

선지별 해설

① X: 10.10.20.300은 마지막 숫자 300이 허용 범위를 벗어나므로 유효한 IPv4 주소가 아니다. 점으로 구분한 각 숫자는 8비트 값으로 **0~255**여야 한다. 10으로 시작하더라도 이 조건을 충족해야 사설 주소로 사용할 수 있다.

② X: 168.10.40.11은 사설 주소로 예약된 세 대역 중 어느 것에도 포함되지 않는다. 사설 주소 대역은 10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255, 192.168.0.0~192.168.255.255이다.

③ O: 172.16.10.20은 172.16.0.0~172.31.255.255에 포함되므로 사설 네트워크 용도로 사용할 수 있다. 이 대역은 첫 번째 숫자가 172이고 **두 번째 숫자가 16~31**인 범위이며, 제시된 주소의 두 번째 숫자는 16이다.

④ X: 192.10.20.30은 192.168.0.0~192.168.255.255에 포함되지 않는다. 192로 시작하는 사설 주소 대역은 **192.168로 시작**해야 하며, 제시된 주소는 두 번째 숫자가 10이므로 이 조건을 충족하지 않는다.

NoteBase

문 6. URL(Uniform Resource Locator)이 웹페이지를 정의하는 데 사용하는 식별자가 아닌 것은?

① Protocol

② Sequence Number

③ Host

④ Path

정답 2번

간단한 해설

Sequence Number는 **전송 데이터의 순서를 관리하는 번호**로, 웹 자원의 위치와 접근 방식을 나타내는 URL의 구성 요소가 아니다.

공통 해설

URL은 웹 자원의 위치와 접근 방식을 나타내는 주소이다. 일반적인 웹 URL의 기본 구조는 '프로토콜://호스트/경로'로 이해할 수 있다. Protocol은 HTTP나 HTTPS와 같은 접근 방식을, Host는 자원이 있는 서버의 이름이나 IP 주소를, Path는 그 서버에서 요청할 자원의 경로를 나타낸다. 즉, **어떤 방식으로 어느 서버의 어떤 자원에 접근하는가**를 지정한다.

Sequence Number는 TCP 등에서 전송 데이터의 순서를 관리하는 번호이다. 전송 과정에서 데이터의 순서를 구분하는 정보이므로, 웹 자원의 주소를 구성하는 **프로토콜·호스트·경로와는 역할이 다르다**. 따라서 URL의 구성 요소에 해당하지 않는다.

NoteBase

문 7. OSI(Open Systems Interconnection) 참조 모델과 TCP/IP 프로토콜에 대한 설명으로 옳지 않은 것은?

① OSI 참조 모델은 국제 표준 기구인 ISO가 만든 모델이며, 서로 다른 컴퓨터 간의 기능을 여러 계층으로 구분하여 계층마다 표준화된 서비스와 프로토콜을 규정하였다.

② OSI 참조 모델은 Layer 1인 최상위의 응용 계층부터 Layer 7인 최하위의 물리 계층까지 7개 계층으로 구성된다.

③ 데이터 링크 계층은 물리 계층에서 발생할 수 있는 오류를 발견하는 역할을 한다.

④ 네트워크 계층에서는 출발지부터 목적지까지 여러 링크를 경유하여 패킷을 포워드 할 수 있으며, 이때 IP 주소와 같은 논리 주소가 이용된다.

정답 2번

간단한 해설

②는 계층 번호의 방향을 거꾸로 설명했다. OSI 참조 모델에서 **1계층은 최하위 물리 계층**이고, **7계층은 최상위 응용 계층**이다.

선지별 해설

① O: OSI 참조 모델은 ISO가 서로 다른 시스템 간의 통신을 표준화하기 위해 마련한 모델이다. 통신 기능을 계층별로 나누고 각 계층의 역할과 서비스 관계를 정리하여, 서로 다른 시스템이 통신할 수 있는 **공통 기준**을 제공한다.

② X: OSI 참조 모델의 계층 번호는 **최하위 물리 계층을 1계층**으로 하여 위로 갈수록 커진다. 아래에서부터 물리(1) → 데이터 링크(2) → 네트워크(3) → 전송(4) → 세션(5) → 표현(6) → 응용(7) 순이다. 따라서 선지의 'Layer 1인 최상위의 응용 계층'은 'Layer 7인 최상위의 응용 계층'으로, 'Layer 7인 최하위의 물리 계층'은 'Layer 1인 최하위의 물리 계층'으로 고쳐야 한다.

③ O: 물리 계층에서 비트를 전송하는 동안 잡음 등으로 비트 오류가 발생할 수 있다. 데이터 링크 계층은 비트들을 프레임 단위로 다루며, CRC와 같은 오류 검출 방식을 이용하여 **전송 중 발생한 오류를 검출**한다. 오류를 검출하는 기능과 오류를 직접 정정하는 기능은 구별된다.

④ O: 네트워크 계층은 서로 다른 네트워크를 거쳐 목적지까지 패킷을 전달하는 기능을 담당한다. 라우터는 목적지 IP 주소와 같은 **논리 주소**를 바탕으로 라우팅 정보를 확인하여 다음 전달 지점을 정한다. 이 과정을 거치면서 패킷은 여러 링크를 지나 목적지로 전달될 수 있다.

NoteBase

문 8. 다음 중 HTTPS가 사용될 때 통신 간에 암호화되는 요소에 해당하는 것은?

① 요청되는 문서의 URL

② IP 헤더의 TTL 필드

③ TCP 헤더의 플래그 비트들

④ 탐색엔진

정답 1번

간단한 해설

HTTPS는 HTTP 메시지를 TLS로 암호화하므로, 요청 문서의 URL 중 **HTTP 요청에 담기는 경로와 쿼리 정보**가 보호된다. IP·TCP 헤더는 이 암호화 범위에 포함되지 않는다.

공통 해설

HTTPS는 HTTP 요청과 응답을 TLS로 보호하는 방식이다. 이때 암호화되는 것은 **TLS에 전달되는 HTTP 메시지**이며, 이를 운반하는 IP·TCP 헤더까지 함께 암호화되는 것은 아니다.

요청되는 문서의 URL 중 경로는 서버에서 어떤 자원을 요청하는지를 나타내고, 쿼리는 요청에 필요한 매개변수를 담는다. 이 정보는 HTTP 요청에 포함되므로 TLS로 암호화된다.

IP 헤더의 TTL 필드는 패킷의 수명을 제한하는 네트워크 계층 정보이다. HTTP 메시지 바깥에 있으므로 HTTPS 자체의 암호화 대상이 아니다.

TCP 헤더의 플래그 비트들은 연결 설정·종료 등 TCP 통신을 제어하는 정보이다. TLS는 TCP 위에서 동작하므로 **TCP 헤더의 플래그까지 암호화하지는 않는다**.

탐색엔진은 검색 기능을 제공하는 시스템이며, 그 자체가 HTTP 메시지 안에 실리는 데이터 항목은 아니다. 따라서 엔진 자체를 HTTPS의 암호화 요소로 볼 수 없다.

이 문항에서 암호화되는 요소는 요청 문서의 URL이다. 다만 이는 HTTP 요청에 실리는 경로·쿼리 정보가 보호된다는 의미이다. 도메인 이름은 DNS 조회나 TLS 연결 설정 과정에서 별도로 드러날 수 있고, # 뒤의 프래그먼트는 요청 대상으로 서버에 전송되지 않으므로 **URL의 모든 구성 요소가 통신 중 암호화된다는 뜻은 아니다**.

NoteBase

문 9. HTTP 메시지의 header 정보를 조작하여 서버가 header 정보를 완전히 수신할 때까지 연결을 유지하도록 하여 서버의 가용량을 소비시킴으로써 다른 사용자의 정상적인 서비스를 방해하는 공격은?

① Slowloris 공격

② HTTP CC 공격

③ HTTP GET Flooding 공격

④ Slow HTTP POST 공격

정답 1번

간단한 해설

서버가 **HTTP 헤더를 끝까지 받지 못한 상태**로 연결을 계속 유지하게 만드는 것이 Slowloris 공격의 특징이다. 미완성 요청을 기다리는 연결이 쌓이면서 정상 사용자를 처리할 여력이 줄어든다.

공통 해설

Slowloris는 HTTP 요청의 **헤더 전송을 완료하지 않은 채 연결을 오래 유지**하여 서버 자원을 소모시키는 서비스 거부 공격이다. 공격자는 여러 연결을 열고 헤더 일부를 조금씩 추가로 보내 서버가 나머지 헤더를 계속 기다리게 한다. 이 대기 상태의 연결이 서버의 연결 처리 용량을 차지하면 정상 사용자의 요청을 받아들이기 어려워진다. 따라서 문제의 'header 정보를 완전히 수신할 때까지 연결을 유지'한다는 설명은 Slowloris의 작동 방식에 해당한다.

구별 기준은 단순히 서비스가 느려진다는 결과가 아니라 **헤더 수신이 끝나지 않도록 만든다**는 방식이다. Slow HTTP POST는 헤더를 보낸 뒤 요청 본문을 천천히 전송하여 서버가 본문 수신을 기다리게 하므로, 문제에서 지연시키는 부분과 다르다.

NoteBase

문 10. 다음 ㉠~㉣에 들어갈 용어를 바르게 연결한 것은?

가상 사설망이라 불리는 (㉠) 기법은 접근 제어를 위해 보안서비스와 터널링 기술이 요구된다. 터널링 프로토콜로 MS에서 개발한 (㉡) 기법과 시스코에서 개발한 (㉢) 기법이 있으며, 이 둘을 결합한 형태로 (㉣) 기법이 있다.

① ㉠: VPN, ㉡: PPTP, ㉢: L2TP, ㉣: L2F

② ㉠: VPN, ㉡: PPTP, ㉢: L2F, ㉣: L2TP

③ ㉠: PPTP, ㉡: VPN, ㉢: L2TP, ㉣: L2F

④ ㉠: PPTP, ㉡: VPN, ㉢: L2F, ㉣: L2TP

정답 2번

간단한 해설

시스코에서 개발한 터널링 프로토콜은 **L2F**이고, MS의 PPTP와 L2F의 특징을 결합한 프로토콜은 **L2TP**이다.

빈칸별 해설

㉠ VPN: VPN(Virtual Private Network)은 **공중망을 이용해 논리적인 사설망을 구성**하는 기술이다. 인터넷 같은 공중망을 통신 경로로 사용하면서 터널링과 보안서비스를 적용하여 사설망처럼 이용하므로, '가상 사설망'에 들어갈 용어이다.

㉡ PPTP: PPTP(Point-to-Point Tunneling Protocol)는 **MS 등이 개발한 터널링 프로토콜**이다. PPP 프레임을 캡슐화하여 IP 네트워크를 통해 전달한다. VPN이 가상 사설망이라는 전체 기술을 가리키는 데 비해, PPTP는 이를 구현하는 데 사용하는 터널링 프로토콜이다.

㉢ L2F: L2F(Layer 2 Forwarding)는 **시스코에서 개발한 터널링 프로토콜**이다. PPP 프레임 등을 터널을 통해 전달하므로, 지문의 '시스코에서 개발한'이라는 조건에 대응한다.

㉣ L2TP: L2TP(Layer 2 Tunneling Protocol)는 **PPTP와 L2F의 특징을 결합**한 터널링 프로토콜이다. 따라서 지문의 '이 둘'은 MS의 PPTP와 시스코의 L2F를 뜻하며, 이들을 결합한 형태에 들어갈 용어는 L2TP이다.

㉠~㉣은 VPN, PPTP, L2F, L2TP로 연결되며, ②의 구성과 일치한다.

NoteBase

문 11. 데이터링크의 효율성을 위해서 다수의 디바이스가 단일 링크를 공유하여 전송해 주는 기술은?

① 변조

② 부호화

③ 암호화

④ 다중화

정답 4번

간단한 해설

여러 장치의 데이터를 **하나의 링크로 함께 전송**하도록 하는 기술이 다중화이다. 링크의 전송 자원을 나누어 사용하므로 장치마다 별도의 링크를 마련하지 않고도 통신할 수 있다.

공통 해설

다중화는 **여러 데이터 흐름이 하나의 전송 링크를 공유**하도록 결합하여 보내는 기술이다. 이 문항에서는 데이터의 표현이나 내용을 바꾸는 방식보다, 여러 장치가 한 링크의 전송 자원을 함께 사용하도록 하는 기능이 판단 기준이다. 이 기능에 해당하는 명칭은 다중화이다.

예를 들어 장치 A와 B에 서로 다른 전송 시간대를 배정하면, 두 장치가 같은 링크를 번갈아 이용하여 각자의 데이터를 보낼 수 있다. 이처럼 시간을 나누어 링크를 공유하는 방식은 시분할 다중화이다.

NoteBase

문 12. 부인 봉쇄(non-repudiation) 기능을 제공하는 기법은?

① 디지털 서명

② 트래픽 패딩

③ 접근 제어

④ CRC

정답 1번

간단한 해설

디지털 서명은 서명자의 개인키로 생성한 서명을 공개키로 검증하여, **서명 사실을 나중에 부인하지 못하도록 하는 증거**를 제공한다. 이를 부인 봉쇄 또는 부인 방지라고 한다.

공통 해설

부인 봉쇄는 어떤 행위를 한 당사자가 나중에 그 사실을 부정할 때, 이를 반박할 수 있는 증거를 제공하는 기능이다. 문서의 내용이 바뀌었는지만 확인하는 것으로는 부족하고, **누가 그 문서에 서명했는지 입증**할 수 있어야 한다.

디지털 서명에서는 메시지와 서명자의 개인키를 이용하여 서명을 생성하고, 대응하는 공개키로 이를 검증한다. 개인키가 안전하게 관리되고 공개키와 서명자의 신원 연결이 확인되면, 제3자도 서명을 검증하여 해당 서명자의 서명 사실을 확인할 수 있다. 이처럼 서명자와 메시지를 연결하는 검증 가능한 증거가 부인 봉쇄의 근거가 된다.

트래픽 패딩, 접근 제어, CRC는 이러한 **서명자와 메시지를 연결하는 서명 증거를 제공하지 않는다**. 따라서 부인 봉쇄 기능을 제공하는 기법으로는 디지털 서명이 해당한다.

NoteBase

문 13. 공중 무선랜의 공격에 대한 대응 기법이 아닌 것은?

① 폐쇄 시스템 운영

② MAC 주소 인증

③ SSID 설정을 통한 접속 제한

④ WEP/WPA 키 크래킹

정답 4번

간단한 해설

WEP/WPA 키 크래킹은 무선랜의 암호 키나 비밀번호를 알아내어 보안을 깨뜨리는 **공격 기법**이다. 접속을 제한하거나 통신을 보호하는 대응 기법과 구별해야 한다.

선지별 해설

① O: 폐쇄 시스템 운영은 **SSID 숨김** 기능을 이용하여 무선랜 이름이 일반적인 검색 목록에 드러나지 않도록 하는 방식이다. 무선랜의 노출을 줄이려는 설정이지만, 통신 프레임을 분석하면 SSID를 알아낼 수 있으므로 이것만으로 침입을 막을 수는 없다.

② O: MAC 주소 인증은 접속하려는 단말의 MAC 주소를 허용 목록과 대조하여 **등록된 주소의 단말만 접속을 허용**하는 방식이다. 다만 MAC 주소를 위조하면 우회할 수 있으므로 강력한 사용자 인증이나 통신 암호화를 대신하지는 못한다.

③ O: SSID는 무선랜을 구별하는 네트워크 이름이다. SSID 설정을 통한 접속 제한은 단말이 지정된 SSID를 사용하도록 하여 무분별한 접속을 줄이려는 기본 설정으로, 이 문항에서는 대응 기법에 포함된다. 다만 **SSID 자체는 비밀 인증정보가 아니므로** 그 이름을 설정하거나 숨기는 것만으로 안전한 인증이 이루어지는 것은 아니다.

④ X: WEP/WPA 키 크래킹은 암호 키나 비밀번호를 추정·복구하여 무선랜의 보호를 무력화하려는 **공격 기법**이다. WEP/WPA를 이용한 통신 보호와 그 키를 깨뜨리는 행위는 구별해야 한다. 대응 기법은 키 크래킹이 아니라 안전한 인증·암호화 설정으로 비인가 접속과 도청을 막는 것이다.

NoteBase

문 14. 방화벽 내에서 내부 사설 IP 주소를 가진 클라이언트가 외부로 접속하는 단계를 순서대로 바르게 나열한 것은?

ㄱ. 원격지 서버가 방화벽이 보낸 패킷에 대한 응답 패킷을 보낸다.
ㄴ. 클라이언트는 내부 IP 주소를 출발지 주소로, 접속하고자 하는 외부 IP 주소를 목적지 주소로 하는 패킷을 생성하여 방화벽으로 보낸다.
ㄷ. 방화벽은 Normal NAT 규칙에 따라 패킷의 출발지 주소를 미리 설정되어 있는 방화벽 IP 주소로 바꾸어 원격지 서버에 전송한다.
ㄹ. 방화벽은 Normal NAT 규칙에 따라 목적지 주소를 처음 접속을 시도한 클라이언트의 내부 IP 주소로 바꾼 후, 클라이언트로 전송한다.

① ㄴ → ㄷ → ㄱ → ㄹ

② ㄴ → ㄹ → ㄱ → ㄷ

③ ㄷ → ㄱ → ㄴ → ㄹ

④ ㄷ → ㄹ → ㄴ → ㄱ

정답 1번

간단한 해설

외부로 나가는 요청 패킷은 방화벽에서 **출발지 주소**가 변환되고, 돌아오는 응답 패킷은 **목적지 주소**가 원래 클라이언트의 내부 IP 주소로 변환된다. 서버의 응답은 방화벽이 요청을 외부로 전달한 뒤에 이루어진다.

NoteBase

올바른 순서

ㄴ → ㄷ → ㄱ → ㄹ

ㄴ. 클라이언트의 요청: 클라이언트가 자신의 내부 사설 IP 주소를 출발지로, 접속할 외부 서버의 IP 주소를 목적지로 하는 패킷을 생성하여 방화벽으로 보낸다. 방화벽이 변환할 요청 패킷이 먼저 도착해야 하므로 이 단계가 출발점이다.

ㄷ. 요청 패킷의 주소 변환: 방화벽은 Normal NAT 규칙에 따라 **출발지 주소를 미리 설정된 방화벽 IP 주소로 바꾼다**. 목적지는 외부 서버로 유지하여 전송하므로, 서버는 클라이언트의 내부 주소 대신 변환된 방화벽 주소를 출발지로 보게 된다.

ㄱ. 외부 서버의 응답: 서버는 방화벽이 전달한 요청을 받은 뒤 응답 패킷을 보낸다. 이 응답의 **목적지는 요청에서 출발지로 보였던 방화벽 IP 주소**이므로, 응답은 먼저 방화벽으로 돌아온다.

ㄹ. 응답 패킷의 주소 복원: 방화벽은 앞서 이루어진 주소 변환에 대응하여 응답 패킷의 **목적지 주소를 원래 클라이언트의 내부 IP 주소로 바꾼다**. 그 뒤 클라이언트에 전달하므로, 이 단계는 서버의 응답이 방화벽에 도착한 후에 이루어진다.

NoteBase

문 15. 스니핑을 수행하는 스니퍼(sniffer)를 탐지하는 방법에 대한 설명으로 옳지 않은 것은?

① 로컬 네트워크에 존재하지 않는 주소로 위장하여 ping(ICMP Echo Request)을 보냈을 때, ICMP Echo Reply를 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.

② FIN 패킷을 보냈을 때, RST 패킷을 받으면 해당 호스트는 스니퍼임을 추측할 수 있다.

③ 특정 호스트에서 promiscuous mode의 설정 여부를 확인하면 스니퍼임을 추측할 수 있다.

④ ARP 트래픽을 모니터링하는 ARP watch를 이용하여 스니퍼임을 추측할 수 있다.

정답 2번

간단한 해설

FIN 패킷에 대한 **RST 응답은 스니핑의 증거가 아니다**. TCP 동작 규칙을 따르는 호스트에서는 닫힌 포트도 FIN 패킷에 RST로 응답하므로, 이 반응은 **포트 상태를 확인하는 FIN 스캔**에 이용된다.

선지별 해설

① O: ping을 이용한 탐지는 대상 호스트의 IP 주소는 유지하면서 **목적지 MAC 주소를 로컬 네트워크에 없는 주소로 설정**하는 방식이다. 일반적인 네트워크 카드는 자신에게 온 프레임이 아니므로 버리지만, 무차별 모드에서 이를 받아 운영체제가 ICMP Echo Request를 처리하면 Echo Reply가 돌아올 수 있다. 이러한 응답을 스니퍼 의심 단서로 삼는다. 다만 운영체제와 드라이버의 처리 방식에 따라 탐지 가능 여부가 달라진다.

② X: FIN 패킷에 대한 RST 응답은 스니퍼의 특징이 아니라 **포트 상태를 확인하는 단서**이다. FIN 스캔에서 TCP 동작 규칙을 따르는 호스트의 닫힌 포트는 RST로 응답하므로, 스니핑하지 않는 호스트에서도 같은 반응이 나타난다. 따라서 'RST 패킷을 받으면 스니퍼임을 추측할 수 있다'는 설명은 'RST 응답을 이용해 포트가 닫혀 있는지 판단할 수 있다'로 고쳐야 한다.

③ O: promiscuous mode는 네트워크 인터페이스에 도달한 프레임을 **목적지 MAC 주소가 자신의 주소인지에 관계없이 수신**하는 무차별 모드이다. 다른 호스트의 트래픽을 수집하는 스니퍼가 이 모드를 사용할 수 있으므로 설정 여부가 탐지 단서가 된다. 정상적인 네트워크 분석 도구도 이 모드를 사용하므로 설정만으로 악성 스니핑을 확정할 수는 없다.

④ O: ARP watch는 ARP 트래픽을 관찰하여 **IP 주소와 MAC 주소의 대응 관계 변화**를 기록하고 알리는 도구이다. ARP 스푸핑으로 다른 호스트의 트래픽을 자신에게 유도하는 스니핑에서는 이 대응 관계가 바뀔 수 있으므로, 이를 통해 의심 징후를 찾을 수 있다. ARP 정보를 바꾸지 않고 트래픽을 수집하는 수동적 스니퍼까지 모두 탐지하는 것은 아니다.

NoteBase

문 16. IPSec에 대한 설명으로 옳지 않은 것은?

① IPSec을 침입차단시스템이나 라우터에서 구현할 경우 경계를 통과하는 모든 트래픽에 적용할 수 있는 강한 보안성을 제공하기 때문에 회사나 작업그룹 사이의 트래픽 보안을 위해 특별한 처리를 할 필요가 없다.

② IPSec은 전송계층(TCP와 UDP)의 아래에 있으며 응용 프로그램에는 투명하다. 침입차단시스템이나 라우터에서 IPSec이 작동되고 있을 때는 서버 시스템과 사용자 시스템의 소프트웨어를 바꿀 필요가 없다.

③ 만약 외부로부터의 모든 트래픽이 IP를 사용해야만 한다면 침입차단시스템에서의 IPSec은 우회하는 트래픽을 차단할 수 없으며, 개별적인 사용자가 보안이 필요하다면 IPSec은 그 사용자에게 보안을 제공할 수 없다.

④ IPSec은 종단 사용자에게 투명하게 할 수 있다. 따라서 번거롭게 사용자에게 보안 메커니즘을 훈련시키거나, 개별 기반으로 키를 발급하거나, 사용자가 근무를 그만두고 떠날 때 키를 취소할 필요가 없다.

정답 3번

간단한 해설

외부 IP 트래픽이 침입차단시스템을 통해서만 들어오도록 구성하면 **IPSec 보안 처리를 우회하지 못하게 할 수 있다**. 또한 IPSec은 원격 근무자처럼 **개별 사용자에게도 보안을 제공**할 수 있다.

NoteBase

선지별 해설

① O: IPSec을 침입차단시스템이나 라우터에 구현하면 **경계를 통과하는 IP 트래픽을 한곳에서 보호**할 수 있다. 회사나 작업그룹 간 통신을 게이트웨이가 보안 정책에 따라 처리하므로, 내부의 각 응용 프로그램에 별도의 보안 처리를 추가하지 않고도 해당 통신을 보호할 수 있다. 보안 처리가 전혀 없다는 뜻이 아니라 게이트웨이가 그 처리를 맡는다는 뜻이다.

② O: IPSec은 TCP·UDP가 동작하는 전송계층보다 아래인 **IP 계층에서 보안을 제공**한다. 따라서 응용 프로그램이 보안 처리를 직접 수행하지 않아도 된다. 특히 침입차단시스템이나 라우터에서 IPSec을 처리하는 구성에서는 내부 서버와 사용자 시스템의 소프트웨어를 바꿀 필요가 없다.

③ X: 외부 트래픽이 모두 IP를 사용하고 침입차단시스템이 외부에서 들어오는 유일한 경로라면, 모든 외부 패킷에 보안 정책을 적용할 수 있다. 이때 IPSec 보호가 필요한데 보호되지 않은 패킷은 폐기하도록 하여 **보안 처리를 우회하는 트래픽을 차단**할 수 있다. 또한 원격 근무자의 단말과 회사 게이트웨이 사이에 IPSec 연결을 구성하는 등 **개별 사용자에게도 보안을 제공**할 수 있다. 따라서 '차단할 수 없으며'와 '그 사용자에게 보안을 제공할 수 없다'는 두 표현 모두 잘못되었다.

④ O: 게이트웨이가 IPSec 보안 처리를 담당하면 사용자는 이를 의식하지 않고 통신할 수 있다. 이런 구성에서는 사용자에게 보안 메커니즘을 따로 교육하거나 사용자마다 IPSec용 키를 발급하고 퇴사 때 회수하는 절차를 두지 않을 수 있다. 이는 **사용자별 키 관리를 요구하지 않는 구성도 가능**하다는 뜻이며, 게이트웨이 사이의 통신에 필요한 키 관리까지 없어진다는 뜻은 아니다.

NoteBase

문 17. 전송계층에 적용되는 SSL(또는 TLS) 보안 프로토콜에 대한 설명으로 옳은 것은?

① Authentication Header 프로토콜은 발신지 호스트를 인증하고 페이로드의 무결성을 보장하기 위하여 설계되었다.

② Alert 프로토콜은 암호화 또는 암호화/인증의 결합을 제공하기 위해 사용되는 캡슐화 헤드와 트레일러로 구성된다.

③ Change Cipher Spec 프로토콜은 연결에서 사용될 암호화 그룹을 갱신하는 프로토콜이다.

④ Handshake 프로토콜은 응용데이터가 전송된 후에 사용되며, 서버와 클라이언트 간의 상호인증, 그리고 암호와 MAC 알고리즘을 협상하지만, 보안 프로토콜로 송신되는 데이터를 보호하기 위한 암호화 키들은 협상하지 않는다.

정답 3번

간단한 해설

Change Cipher Spec은 Handshake에서 협상한 암호 명세와 키를 **이후 레코드에 적용하도록 전환**한다. 암호 방식을 새로 협상하는 과정과 협상된 설정을 실제로 적용하는 과정을 구분해야 한다.

선지별 해설

① X: Authentication Header(AH)는 데이터 출처 인증과 무결성을 제공하지만, **SSL/TLS가 아닌 IPsec의 프로토콜**이다. 따라서 AH의 기능 설명 자체는 맞더라도 SSL/TLS 보안 프로토콜을 묻는 이 문항에는 해당하지 않는다.

② X: 캡슐화 헤더와 트레일러를 사용하여 암호화 또는 암호화와 인증의 결합을 제공하는 것은 IPsec의 **ESP(Encapsulating Security Payload)**에 관한 설명이다. SSL/TLS의 Alert 프로토콜은 오류의 종류와 심각도, 연결 종료 등의 상태를 상대방에게 알린다.

③ O: 이 문항에서 다루는 SSL/TLS 구조에서 Change Cipher Spec은 협상해 둔 암호 명세와 키를 **대기 상태에서 현재 적용 상태로 전환**한다. 선지의 '암호화 그룹을 갱신'은 연결에 적용할 암호 설정을 전환한다는 의미이다. 암호 명세와 키에 관한 협상은 Handshake가 담당하고, Change Cipher Spec 이후의 레코드부터 새 설정으로 보호한다.

④ X: 최초 Handshake는 **응용데이터를 전송하기 전에** 수행한다. 암호 및 MAC 알고리즘을 협상하고, 키 교환을 통해 공유 비밀을 확립하여 데이터 보호에 사용할 키를 생성할 수 있게 한다. 따라서 '전송된 후에 사용'과 '암호화 키들은 협상하지 않는다'는 설명을 고쳐야 한다. 인증 방식에 따라 서버 인증과 선택적인 클라이언트 인증도 수행하므로, 상호인증이 항상 필수인 것은 아니다.

NoteBase

문 18. TCP session hijacking 공격에 대한 설명으로 옳지 않은 것은?

① 이 공격 기법에 대한 대응 방안으로 데이터를 암호화하여 전송하는 방식을 사용한다.

② 이 공격은 클라이언트와 서버가 통신할 때 사용되는 TCP의 sequence number를 이용한 공격이다.

③ 이 공격을 성공적으로 수행하기 위해서는 ARP 스푸핑과 같은 추가적인 공격 기술이 필요하다.

④ 세션 성립은 일반적으로 인증 성립을 의미하며, 인증이 성립된 후에는 이 공격을 막을 수 있다.

정답 4번

간단한 해설

④의 '인증이 성립된 후에는 이 공격을 막을 수 있다'는 설명이 잘못되었다. TCP 세션 하이재킹은 **이미 인증된 사용자의 연결을 탈취**하여 그 사용자로 가장할 수 있으므로, 최초 인증만으로는 막을 수 없다.

선지별 해설

① O: SSH나 IPsec처럼 **암호화와 무결성 보호**를 제공하는 통신 방식을 사용하면 데이터 도청과 위조 데이터 삽입에 대응할 수 있다. 단순히 내용만 암호화하는 것과 전송 데이터의 위조 여부까지 검증하는 것은 구별해야 한다.

② O: TCP의 sequence number는 전송하는 바이트의 순서를 나타내며, 수신 측은 이를 이용해 데이터의 순서와 수신 가능 범위를 확인한다. 공격자는 **기존 연결에 맞는 순서번호**를 알아내거나 추측하여 위조 패킷이 정상 통신의 일부로 받아들여지도록 한다.

③ O: 기존 연결을 가로채려면 패킷 정보를 얻거나 정상 호스트로 가장하는 추가 기법을 결합한다. ARP 스푸핑은 같은 LAN에서 IP 주소와 MAC 주소의 대응을 속여 **통신이 공격자를 거치게 하는** 데 이용할 수 있다. 다만 ARP 스푸핑은 이러한 기법의 예이며, 모든 TCP 세션 하이재킹에 반드시 필요한 특정 기법은 아니다.

④ X: 사용자 인증은 접속한 사용자의 신원을 확인하는 절차이고, 세션 하이재킹은 그 후 유지되는 연결을 탈취하여 정상 사용자로 가장하는 공격이다. 따라서 **인증이 끝난 뒤에도 공격이 가능**하며, 통신 중인 데이터와 패킷을 계속 보호해야 한다. 또한 TCP의 3-way handshake로 연결이 성립했다는 사실 자체가 사용자 인증의 완료를 뜻하지는 않는다.

NoteBase

문 19. 네트워크 공격 기법에 대한 설명으로 옳지 않은 것은?

① 서비스 거부 공격은 대상 시스템의 서비스를 중단시키기 위해 공격하는 기법이다.

② 중간자 공격(man-in-the middle attack)은 두 컴퓨터의 통신 중간에 위치하는 공격 기법이다.

③ DDoS 공격은 일반적으로 공격을 증폭시키는 중간자가 사용되는 공격 기법이다.

④ CSRF 공격은 메일 서버를 요청하지 않은 이메일로 공격하는 기법이다.

정답 4번

간단한 해설

메일 서버에 요청하지 않은 이메일을 보내는 것은 CSRF의 설명이 아니다. CSRF는 **인증된 사용자의 브라우저를 악용해 원치 않는 웹 요청**을 보내게 하는 공격이다.

선지별 해설

① O: 서비스 거부(DoS) 공격은 시스템 자원이나 네트워크 대역폭을 소진시키는 등의 방법으로 **정상적인 서비스 이용을 방해**한다. 과도한 요청으로 서버가 정상 사용자의 요청에 응답하지 못하게 하는 것이 대표적인 예이다.

② O: 중간자 공격은 **두 통신 당사자 사이에 개입**하여 주고받는 정보를 가로채거나 변조하는 공격이다. 양쪽이 서로 직접 통신한다고 믿는 동안 공격자가 통신을 중계하며 내용을 엿보거나 바꿀 수 있다.

③ O: 분산 서비스 거부(DDoS) 공격은 여러 시스템에서 한 대상을 함께 공격하여 서비스 이용을 방해한다. 공격자는 흔히 감염된 다수의 기기를 중간 시스템으로 이용해 전체 공격 규모를 키운다. 반사·증폭형 공격에서는 제3의 서버가 피해자에게 더 큰 응답을 보내도록 하기도 한다. 여기서 중간자는 ②처럼 통신을 가로채는 공격자가 아니라 **공격에 동원되거나 악용되는 중간 시스템**을 뜻한다. 다만 요청보다 큰 응답을 유발하는 트래픽 증폭이 모든 DDoS의 필수 조건인 것은 아니다.

④ X: CSRF는 사이트가 사용자의 인증 정보를 신뢰하는 점을 악용하는 요청 위조 공격이다. 예를 들어 로그인한 사용자가 공격자가 만든 페이지를 열었을 때, 취약한 사이트로 이메일 주소 변경 요청이 사용자의 인증 정보와 함께 전송되게 할 수 있다. 핵심은 **사용자가 의도하지 않은 동작을 사용자 권한으로 실행**하게 하는 것이다. 요청하지 않은 이메일을 보내는 것은 스팸 메일 전송에 해당하며, 대량의 이메일로 메일 서버의 서비스를 방해하는 공격은 메일 폭탄 공격으로 구분한다.

NoteBase

문 20. 203.230.15.0과 같은 IPv4의 C 클래스 네트워크를 30개의 서브넷으로 나누고, 각각의 서브넷에는 5개의 호스트를 연결하려고 한다. 30개의 서브넷 대부분에서 사용되는 서브넷 마스크는?

① 255.255.255.224

② 255.255.255.240

③ 255.255.255.248

④ 255.255.255.252

정답 3번

간단한 해설

호스트 5개를 연결하려면 네트워크 주소와 브로드캐스트 주소를 제외하고도 주소가 남아야 하므로 **호스트부 3비트**가 필요하다. C 클래스의 호스트부 8비트 중 나머지 5비트를 서브넷 구분에 쓰면 $2^5 = 32$개의 서브넷을 확보할 수 있으며, 이에 대응하는 마스크는 **255.255.255.248**이다.

계산 과정

기준 네트워크: C 클래스 네트워크의 기본 마스크는 255.255.255.0이며, 네트워크부는 24비트, 호스트부는 8비트이다. 이 호스트부의 일부를 서브넷 구분에 사용하고 나머지를 각 서브넷의 호스트 주소에 사용한다.

서브넷 수: 서브넷 구분에 사용하는 비트를 s라고 하면 같은 크기의 서브넷을 2^s개 만들 수 있다. $2^4 = 16 < 30$이고 $2^5 = 32 \geq 30$이므로, 30개의 서브넷을 확보하려면 **최소 5비트**가 필요하다.

호스트 수: 서브넷 구분에 5비트를 사용하면 호스트부는 $8 - 5 = 3$비트이다. 일반적인 IPv4 서브넷에서는 호스트부가 모두 0인 주소는 네트워크 주소, 모두 1인 주소는 브로드캐스트 주소이므로 **호스트에 할당할 수 있는 주소는 2개를 제외**한다. 따라서 서브넷당 사용 가능한 호스트 주소는 $2^3 - 2 = 6$개로, 호스트 5개를 연결할 수 있다. 호스트부를 2비트만 남기면 $2^2 - 2 = 2$개여서 부족하다.

마스크 변환: 서브넷 마스크는 네트워크부와 서브넷 구분 비트를 1로, 호스트부를 0으로 표시한다. 앞의 24비트에 서브넷 구분용 5비트를 더하므로 마스크 길이는 29비트(/29)이다. 마지막 옥텟은 이진수 11111000이며, 십진수로는 128 + 64 + 32 + 16 + 8 = 248이다. 따라서 마스크는 **255.255.255.248**이며, ③의 값과 일치한다.

NoteBase