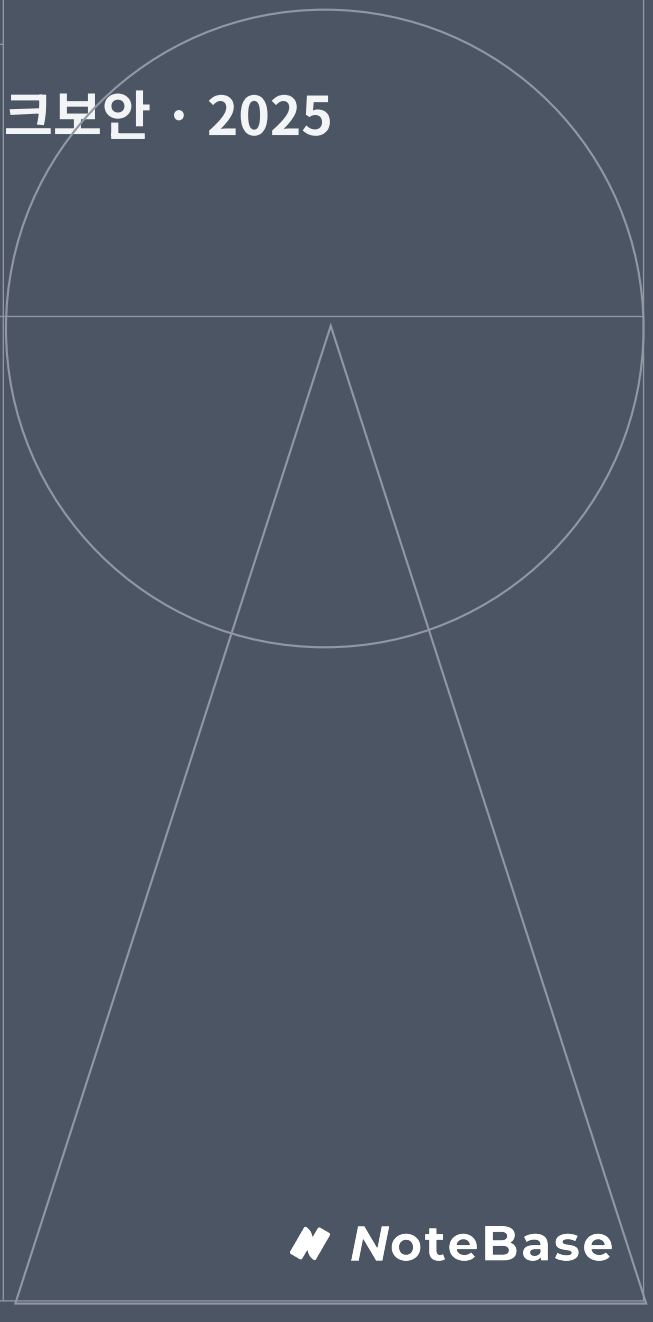
기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2025



NoteBase

기출OX 해설집

공무원/국가직/9급 · 네트워크보안 · 2025

공무원/국가직/9급 · 네트워크보안 · 2025

문 1. 정보보안 3대 요소 중 서비스 거부(Denial of Service) 공격의 침해 대상은?

① 가용성

② 기밀성

③ 무결성

④ 익명성

정답 1번

간단한 해설

서비스 거부(DoS) 공격은 정상 사용자가 서비스를 이용하지 못하게 하므로, 필요할 때 정보나 서비스를 이용할 수 있는 성질인 **가용성**을 침해한다.

개념 구분

가용성은 인가된 사용자가 필요할 때 정보와 시스템을 정상적으로 이용할 수 있는 성질이다. 서비스 거부(DoS) 공격은 과도한 요청으로 서버 자원을 소모시키거나 시스템의 동작을 방해하여 **정상적인 서비스 이용을 막는다**. 따라서 이 공격의 침해 대상은 가용성이다.

기밀성은 인가되지 않은 사람에게 정보가 공개되지 않도록 하는 성질이고, 무결성은 정보가 권한 없이 변경되거나 훼손되지 않도록 하는 성질이다. 정보가 유출되거나 변조되지 않았더라도 서버가 응답하지 않아 이용할 수 없다면 가용성이 침해된 것이다.

익명성은 행위자의 신원이 드러나지 않는 성질이다. 정보보안의 3대 요소는 **기밀성·무결성·가용성**이며, 익명성은 여기에 포함되지 않는다.

NoteBase

문 2. 네트워크에서 서버의 작동과 서버가 제공하는 서비스 존재 여부를 확인하는 것은?

① 스캐닝(scanning)

② 스미싱(SMishing)

③ 스위칭(switching)

④ 스풀링(SPOOLing)

정답 1번

간단한 해설

서버가 작동하는지, 어떤 서비스를 제공하는지 탐색하는 활동을 **스캐닝(scanning)**이라고 한다. 대상 서버나 포트의 응답을 분석하여 이러한 정보를 확인한다.

공통 해설

스캐닝은 네트워크상의 대상에 탐색 요청을 보내고 응답을 분석하여 **호스트의 동작 여부와 서비스의 존재 여부** 등을 조사하는 과정이다. 호스트 탐색으로 서버가 네트워크에서 응답하는지 확인하고, 포트·서비스 탐색으로 접속 가능한 포트와 그곳에서 제공되는 서비스를 조사한다. 예를 들어 서버의 특정 포트에 접속을 시도하고 응답을 분석하여 서비스가 제공되는지 확인하는 활동은 스캐닝에 해당한다. 문항에서 제시한 서버의 작동과 서비스 존재 여부의 확인은 이러한 탐색의 목적에 부합한다.

NoteBase

문 3. 응용계층 프로토콜로 옳지 않은 것은?

① FTP(File Transfer Protocol)

② SCTP(Stream Control Transmission Protocol)

③ SMTP(Simple Mail Transfer Protocol)

④ Telnet

정답 2번

간단한 해설

SCTP는 응용 프로그램의 데이터를 전달하는 **전송계층 프로토콜**이다. 파일 전송이나 전자우편처럼 특정 응용 서비스를 위한 통신 규칙을 정하는 응용계층 프로토콜과 구별된다.

선지별 해설

① O: FTP는 클라이언트와 서버 사이의 **파일 전송**에 사용하는 응용계층 프로토콜이다. 파일을 보내거나 받기 위한 명령과 응답을 정의하며, 실제 데이터 전달에는 하위 전송계층의 TCP를 이용한다.

② X: SCTP는 응용계층이 아니라 **전송계층**에 속한다. TCP·UDP와 같은 계층에서 응용 프로그램에 데이터 전달 기능을 제공하며, 메시지 단위의 신뢰성 있는 전송을 지원한다. 특정 응용 서비스의 규칙을 정하는 대신 그 서비스가 사용하는 데이터를 운반한다.

③ O: SMTP는 **전자우편의 발송과 메일 서버 간 전달**을 위한 응용계층 프로토콜이다. 메일을 전달하는 명령과 응답을 정의하며, 전송계층의 TCP를 이용한다.

④ O: Telnet은 원격 컴퓨터에 접속하여 **터미널을 사용하는 기능**을 제공하는 응용계층 프로토콜이다. 사용자의 입력과 원격 컴퓨터의 출력을 주고받으며, 전송계층의 TCP를 이용한다.

NoteBase

문 4. IEEE 802.11 무선 랜에서 네트워크를 식별하기 위해 사용되는 것은?

① OID(Object IDentifier)

② SSID(Service Set IDentifier)

③ RFID(Radio Frequency IDentification)

④ NIDS(Network-based Intrusion Detection System)

정답 2번

간단한 해설

SSID는 IEEE 802.11 무선 랜의 **서비스 집합을 식별하는 이름**이다. 무선 네트워크를 선택할 때 표시되는 네트워크 이름이 이에 해당한다.

개념 구분

SSID(Service Set Identifier)는 IEEE 802.11 무선 랜에서 **서비스 집합을 구별하는 식별자**이다. 예를 들어 Wi-Fi 목록에 'Campus'라는 네트워크 이름이 표시된다면, 'Campus'가 해당 네트워크의 SSID이다.

OID(Object Identifier)는 **객체를 식별하는 식별자**이다. 문제는 일반적인 객체 식별자가 아니라 IEEE 802.11 무선 랜의 서비스 집합을 식별하는 명칭을 묻는다는 점에서 구별된다.

NoteBase

문 5. 한 번의 시스템 인증을 통하여 여러 정보 시스템에 재인증 절차 없이 접근할 수 있는 통합 로그인 기술은?

① DRM

② SSO

③ SET

④ PGP

정답 2번

간단한 해설

SSO(Single Sign-On)는 한 번의 인증 결과를 여러 정보 시스템에서 활용하여, 시스템마다 다시 로그인하는 절차를 줄이는 통합 로그인 기술이다.

공통 해설

SSO(Single Sign-On)는 사용자가 한 번 인증받으면, 통합 로그인에 연계된 여러 정보 시스템을 개별 로그인 없이 이용하게 하는 기술이다. 각 시스템이 **최초 인증 결과를 신뢰하여 활용**하므로 사용자에게 아이디와 비밀번호 등을 다시 입력하도록 요구하지 않는다.

예를 들어 SSO로 연계된 사내 메일과 전자결재 시스템에서는 한 번 로그인한 뒤 다른 시스템으로 이동해도 별도의 로그인 없이 이용할 수 있다. 이처럼 '한 번의 인증'과 '여러 시스템에서 재인증 생략'을 함께 충족하는 통합 로그인 기술을 묻는 설명은 SSO에 해당한다.

NoteBase

문 6. 스니핑(sniffing) 공격에 대한 보안 대책으로 옳지 않은 것은?

① 원격 접속 시 SSH 사용

② 웹 환경에서 HTTPS 사용

③ 스위치 대신 더미 허브 사용

④ 이메일 환경에서 S/MIME 사용

정답 3번

간단한 해설

더미 허브는 받은 신호를 **수신 포트를 제외한 모든 포트로 전달**하므로 다른 호스트의 통신을 엿듣기 쉽게 만든다. 스니핑 위험을 줄이려면 더미 허브 대신 스위치를 사용하고, 통신 내용을 암호화해야 한다.

선지별 해설

① O: SSH는 원격 접속 과정에서 인증 정보와 명령·응답 등의 통신 내용을 **암호화**한다. 따라서 공격자가 전송 패킷을 가로채더라도 그 내용을 평문처럼 읽기 어렵게 하므로 스니핑 대책에 해당한다.

② O: HTTPS는 HTTP 통신에 TLS를 적용하여 웹 브라우저와 서버 사이의 **전송 내용을 암호화**한다. 로그인 정보나 웹 요청·응답 내용이 전송 도중 노출되는 것을 방지한다.

③ X: 더미 허브는 목적지 MAC 주소를 구별하여 전달하지 않고, 받은 신호를 수신 포트를 제외한 모든 포트로 내보낸다. 따라서 같은 허브에 연결된 공격자가 다른 호스트의 트래픽을 수집하기 쉬워진다. 대책은 **더미 허브 대신 스위치를 사용**하는 것이다. 스위치는 학습된 목적지 MAC 주소에 해당하는 유니캐스트 프레임을 해당 포트로만 전달하여 불필요한 노출을 줄인다. 다만 스위치만으로 모든 스니핑을 막을 수는 없으므로 통신 암호화도 함께 적용한다.

④ O: S/MIME는 이메일에 암호화와 전자서명 기능을 제공한다. 이 중 **암호화 기능**을 사용하면 메일 내용을 가로채더라도 복호화에 필요한 개인키 없이는 내용을 읽기 어렵게 하므로 스니핑 대책이 된다. 전자서명만 적용하는 것은 메일 내용을 숨기는 대책이 아니다.

NoteBase

문 7. 블록체인에서 보유한 자산에 대한 지분율에 비례하여 의사결정 권한을 주는 합의 알고리즘은?

① PoS(Proof of Stake)

② PoW(Proof of Work)

③ PRNG(Pseudo-Random Number Generator)

④ PBFT(Practical Byzantine Fault Tolerance)

정답 1번

간단한 해설

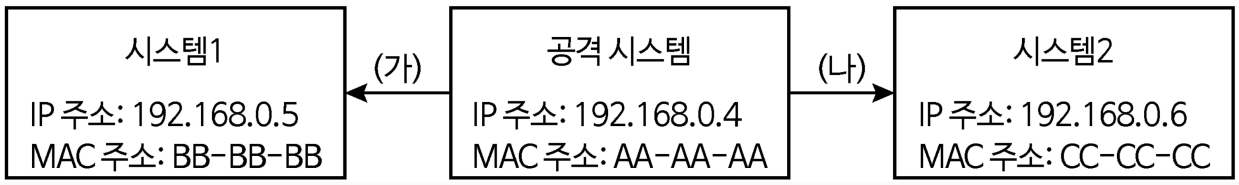
보유 자산의 **지분을 합의 참여 권한의 기준**으로 삼는 방식이 PoS(지분증명)이다.

공통 해설

PoS(Proof of Stake, 지분증명)는 **자산의 지분을 기준으로 합의 참여 권한을 배분**하는 방식이다. 여기서 Stake는 참여자가 가진 지분을 뜻하며, 합의 참여 권한은 블록 생성이나 검증 등 장부 상태를 확정하는 과정에 참여할 권한을 말한다. 문제의 '지분율에 비례하여 의사결정 권한을 준다'는 조건은 지분이 클수록 합의 과정에 더 큰 영향력을 갖게 한다는 의미이므로 PoS에 대응한다.

NoteBase

문 8. 다음 랜(LAN)에서 '공격시스템'이 ARP 스푸핑(spoofing) 공격을 위해 (가), (나)에서 수행하는 작업을 ㄱ~ㄹ에서 찾아 바르게 연결한 것은? (단, MAC 주소는 24비트로 가정한다)



ㄱ. 시스템1의 MAC 주소를 AA-AA-AA라고 알린다.

ㄴ. 시스템2의 MAC 주소를 AA-AA-AA라고 알린다.

ㄷ. 시스템1의 MAC 주소를 CC-CC-CC라고 알린다.

ㄹ. 시스템2의 MAC 주소를 BB-BB-BB라고 알린다.

① (가): ㄴ, (나): ㄱ

② (가): ㄴ, (나): ㄷ

③ (가): ㄹ, (나): ㄱ

④ (가): ㄹ, (나): ㄷ

정답 1번

간단한 해설

ARP 스푸핑은 상대방의 IP 주소에 **공격 시스템의 MAC 주소**를 대응시키도록 속이는 공격이다. 그림에서는 양쪽 시스템이 상대방의 MAC 주소를 AA-AA-AA로 인식하게 해야 한다.

NoteBase

대응 관계 해설

ARP는 같은 LAN에서 IP 주소에 대응하는 MAC 주소를 알아내는 데 사용된다. ARP 스푸핑은 거짓 주소 대응 정보를 알려 피해 시스템의 ARP 캐시를 오염시키는 공격이다. 그림에서 공격 시스템의 MAC 주소는 AA-AA-AA이므로, 상대방에게 보낼 프레임이 이 주소로 향하도록 속여야 한다.

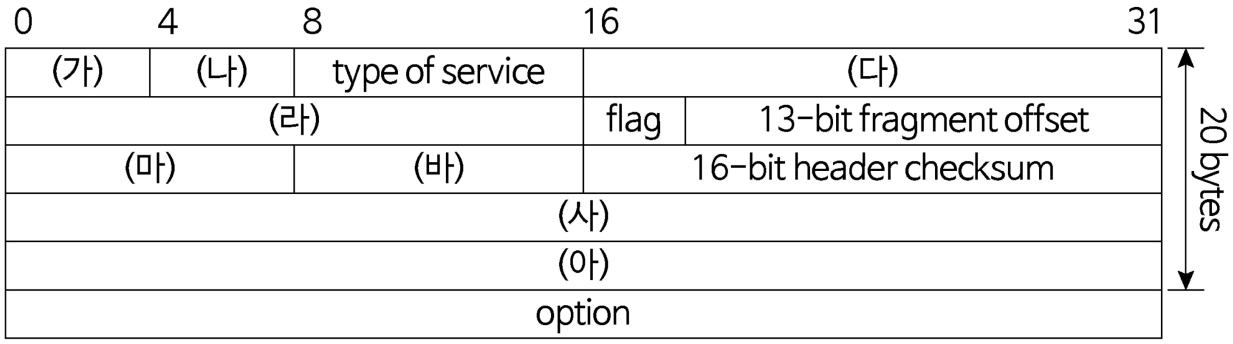
(가) → ㄴ: 화살표가 시스템1을 향하므로 시스템1에 거짓 정보를 알리는 작업이다. 시스템2의 IP 주소 192.168.0.6에 **공격 시스템의 MAC 주소 AA-AA-AA**가 대응한다고 알린다. 그러면 시스템1이 시스템2로 보낼 프레임을 공격 시스템에 보내게 된다. 시스템2의 실제 MAC 주소는 CC-CC-CC이다. ㄹ의 BB-BB-BB는 시스템1 자신의 MAC 주소이므로 공격 시스템으로 유도할 수 없다.

(나) → ㄱ: 화살표가 시스템2를 향하므로 시스템2에 거짓 정보를 알리는 작업이다. 시스템1의 IP 주소 192.168.0.5에 **공격 시스템의 MAC 주소 AA-AA-AA**가 대응한다고 알린다. 그러면 시스템2가 시스템1로 보낼 프레임도 공격 시스템으로 향한다. 시스템1의 실제 MAC 주소는 BB-BB-BB이다. ㄷ의 CC-CC-CC는 시스템2 자신의 MAC 주소이므로 공격 시스템으로 유도할 수 없다.

따라서 (가)는 ㄴ, (나)는 ㄱ에 대응하며, 이 조합은 ①과 일치한다.

NoteBase

문 9. Land 공격을 위한 IPv4 데이터그램 헤더에서 같은 값을 저장하는 필드로만 묶인 것은?



① (가), (나)

② (다), (라)

③ (마), (바)

④ (사), (아)

정답 4번

간단한 해설

Land 공격은 **출발지 IP 주소와 목적지 IP 주소를 피해 호스트의 주소로 같게** 설정한다. 그림에서 두 주소를 저장하는 필드는 각각 (사)와 (아)이다.

도식 해설

Land 공격은 출발지 주소를 피해 호스트의 주소로 위조하여, 출발지와 목적지가 모두 피해 호스트를 가리키는 패킷을 보내는 서비스 거부 공격이다. 따라서 IPv4 헤더에서 찾아야 할 것은 **출발지 주소와 목적지 주소 필드**이다.

(사), (아): 그림에서 헤더 체크섬이 있는 행 바로 아래의 32비트 필드 (사)는 출발지 IP 주소이고, 그 아래의 32비트 필드 (아)는 목적지 IP 주소이다. Land 공격에서는 **두 필드에 같은 피해 호스트의 IP 주소**를 넣는다.

다른 표식의 구분: (가)는 버전, (나)는 IP 헤더 길이(IHL)이고, (다)는 데이터그램 전체 길이, (라)는 식별자이다. (마)는 수명(TTL), (바)는 상위 프로토콜을 나타낸다. 이들은 출발지·목적지 주소를 저장하는 필드가 아니므로, 두 값을 같게 하는 것이 Land 공격의 주소 설정 조건에 해당하지 않는다.

NoteBase

문 10. 다음에서 설명하는 취약점을 이용하는 서비스 거부 공격은?

서버는 클라이언트와 TCP 3-way 핸드셰이크(handshake) 과정을 완료하기 전에 절반-개방(half-open) 연결을 큐에 저장하는데 이 같은 큐는 한정된 용량을 가진다.

① Smurf 공격
② Teardrop 공격
③ SYN flooding 공격
④ Ping-of-death 공격

정답 3번

간단한 해설

SYN flooding 공격은 TCP 연결 요청을 대량으로 보내고 핸드셰이크를 완료하지 않아, **절반-개방 연결을 저장하는 큐**를 소진시킨다. 큐가 가득 차면 정상 사용자의 새 연결 요청을 처리하기 어려워진다.

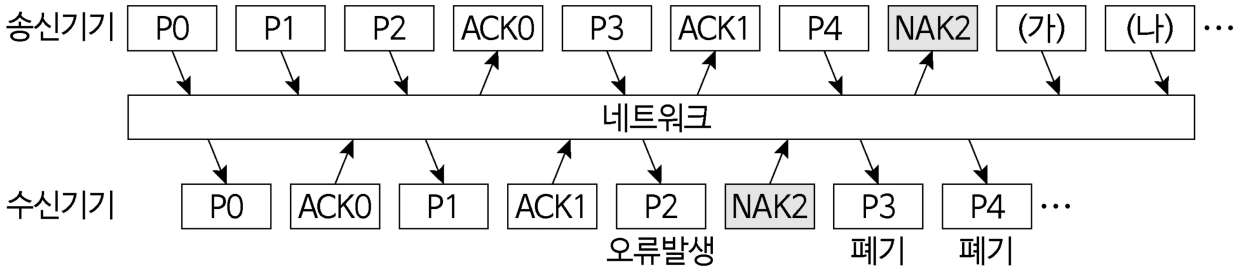
공통 해설

TCP 3-way 핸드셰이크는 클라이언트의 SYN 전송, 서버의 SYN+ACK 응답, 클라이언트의 ACK 전송으로 이루어진다. 서버가 SYN+ACK를 보낸 뒤 **마지막 ACK를 기다리는 상태**가 지문에서 말하는 절반-개방 연결이다. 이때 서버는 연결 설정에 필요한 정보를 용량이 한정된 큐에 보관한다.

SYN flooding 공격은 SYN을 대량으로 보내면서 마지막 ACK가 도착하지 않도록 하여, 연결이 완료되지 않은 요청들로 큐를 채우는 서비스 거부 공격이다. 개별 요청은 시간이 지나면 제거되지만, 새로운 요청을 계속 보내 큐를 소진시키면 정상적인 새 연결 설정이 방해된다. 따라서 지문의 '핸드셰이크 완료 전 연결 보관'과 '한정된 큐 용량'은 SYN flooding 공격을 식별하는 공통 기준이다.

NoteBase

문 11. 다음 Go-Back-N ARQ(Automatic Repeat reQuest)를 사용하는 송신기기와 수신기기 사이에 주고받은 통신 패킷 중 (가), (나)에 들어갈 내용을 바르게 연결한 것은? (단, 윈도 크기는 3이다)



① (가): P0, (나): P1

② (가): P1, (나): P2

③ (가): P2, (나): P3

④ (가): P3, (나): P4

정답 3번

간단한 해설

Go-Back-N에서는 오류가 난 패킷 뒤에 도착한 패킷도 순서대로 수신하지 못하면 폐기한다. 그림에서는 **P2부터 다시 전송**하므로 (가)는 P2, 그다음 (나)는 P3이다.

NoteBase

계산 과정

윈도 크기 3은 송신 측이 확인응답을 받지 않은 패킷을 최대 3개까지 전송할 수 있다는 뜻이다. 그림의 ACK0과 ACK1은 각각 P0과 P1의 정상 수신을 알리고, NAK2는 P2의 재전송을 요구한다.

윈도 이동: 처음에는 P0·P1·P2를 전송한다. ACK0을 받으면 P0이 확인되어 윈도 범위가 P1·P2·P3으로 이동하므로 P3을 보낼 수 있다. 이어 ACK1을 받으면 범위가 P2·P3·P4로 이동하여 P4도 전송한다. 이때 **가장 오래된 미확인 패킷은 P2**이다.

(가): 수신 측에서 P2에 오류가 발생하여 NAK2를 보낸다. Go-Back-N의 수신 측은 순서에 맞지 않게 도착한 P3과 P4를 폐기하므로, 송신 측은 **오류가 난 P2부터 미확인 패킷들을 순서대로 재전송**해야 한다. 따라서 첫 재전송 패킷인 (가)는 P2이다.

(나): P2를 재전송한 다음에는 이미 폐기된 P3을 다시 전송해야 한다. 따라서 (나)는 P3이며, 재전송 순서는 P2 → P3 → P4가 된다.

(가): P2, (나): P3이므로 ③의 연결과 일치한다.

NoteBase

문 12. SSL/TLS 프로토콜 구조에 속하지 않는 것은?

① Record Protocol

② Handshake Protocol

③ Change Cipher Spec Protocol

④ Authentication Header Protocol

정답 4번

간단한 해설

Authentication Header(AH)는 IP 패킷의 무결성과 발신자 인증을 제공하는 **IPsec의 구성 프로토콜**이다. SSL/TLS의 구성 요소에는 해당하지 않는다.

선지별 해설

① O: Record Protocol은 SSL/TLS에서 데이터를 레코드 단위로 나누어 전송하고, 설정된 암호 알고리즘과 키에 따라 **암호화와 무결성 보호**를 수행한다. 응용 데이터뿐 아니라 Handshake 등의 제어 메시지도 레코드에 담아 운반한다.

② O: Handshake Protocol은 클라이언트와 서버가 **암호 알고리즘과 키 생성에 필요한 정보를 협상**하고, 인증 방식에 따라 통신 상대를 인증하는 프로토콜이다. 여기서 마련한 보안 설정을 Record Protocol이 데이터 보호에 사용한다.

③ O: Change Cipher Spec Protocol은 SSL 및 TLS 1.2 등에서 **협상한 암호 설정을 실제 통신에 적용하도록 전환**하는 프로토콜이다. 송신자는 이 메시지를 보낸 뒤 새 설정으로 후속 레코드를 보호하고, 수신자는 이 메시지를 받으면 새 설정으로 후속 레코드를 처리한다. 암호 알고리즘 자체를 협상하는 Handshake Protocol과 역할이 다르다.

④ X: Authentication Header Protocol은 SSL/TLS가 아니라 **네트워크 계층의 IPsec**에 속한다. AH는 IP 패킷의 무결성과 데이터 발신자 인증을 제공하며, 데이터 암호화를 통한 기밀성은 제공하지 않는다. 따라서 이를 SSL/TLS의 구성 프로토콜로 분류할 수 없다.

NoteBase

문 13. 암호학적 해시 함수(cryptographic hash function)의 성질 또는 특징으로 옳지 않은 것은?

① 양방향성

② 충돌 저항성(resistance)

③ 역상(preimage) 저항성

④ 제2(second) 역상 저항성

정답 1번

간단한 해설

암호학적 해시 함수는 입력의 해시값을 계산하기는 쉽지만, 해시값으로부터 그 값을 만드는 입력을 찾기는 계산상 어렵게 하는 **일방향성**을 갖는다. 따라서 '양방향성'은 암호학적 해시 함수의 특징에 맞지 않는다.

선지별 해설

① X: 암호학적 해시 함수는 **양방향성이 아니라 일방향성**을 갖는다. 입력에서 해시값을 계산하는 것은 쉽지만, 해시값이 주어졌을 때 그 값을 만드는 입력을 찾는 것은 계산상 어려워야 한다. 암호문을 복호화하여 원문을 복원하는 것처럼 해시값을 역변환하는 기능을 제공하는 것은 아니다.

② O: 충돌 저항성은 **같은 해시값을 갖는 서로 다른 두 입력**을 찾기 계산상 어려운 성질이다. 특정 입력이나 해시값이 미리 주어질 필요 없이, 공격자가 두 입력을 모두 고를 수 있는 경우를 다룬다. 충돌이 전혀 없다는 뜻이 아니라 충돌하는 입력 쌍을 찾기 어렵다는 뜻이다.

③ O: 역상 저항성은 **해시값이 주어졌을 때** 그 해시값을 만드는 입력을 찾기 계산상 어려운 성질이다. 찾으려는 대상은 주어진 해시값에 대응하는 입력이며, 반드시 실제로 사용된 원래 입력과 같아야 하는 것은 아니다.

④ O: 제2 역상 저항성은 **하나의 입력이 주어졌을 때** 그 입력과 다르면서 해시값은 같은 다른 입력을 찾기 계산상 어려운 성질이다. 충돌 저항성과 달리 두 입력 중 하나가 이미 정해져 있다는 점이 구별된다.

NoteBase

문 14. 다음에서 설명하는 공격을 막는 방법으로 옳지 않은 것은?

공격자가 몰래 보관해둔 기존의 정상적인 MAC(Message Authentication Code) 값을 재사용하여 전송하는 공격이다.

① 비표(nonce) 사용
② 리다이렉션(redirection) 사용
③ 타임스탬프(timestamp) 사용
④ 순서 번호(sequence number) 사용

정답 2번

간단한 해설

리다이렉션은 통신을 다른 위치로 보내는 기능일 뿐, 수신한 인증 정보가 **과거에 사용된 것인지 판별하지 못한다**. 재전송 공격을 막으려면 MAC으로 보호한 비표·타임스탬프·순서 번호 등을 검사하여 메시지의 최신성이나 중복 여부를 확인해야 한다.

NoteBase

선지별 해설

제시문은 정상적인 메시지와 MAC을 가로채 보관했다가 다시 보내는 재전송 공격을 설명한다. MAC은 메시지의 출처와 무결성을 확인하는 수단이지만, 과거의 메시지를 그대로 다시 보내면 MAC 검증을 통과할 수 있다. 따라서 최신성이나 중복 여부를 확인할 정보를 메시지와 함께 MAC으로 보호하고, 수신 측에서 그 정보의 유효성도 검사해야 한다.

① O: 비표(nonce)는 인증 과정에서 한 번만 사용하는 값이다. 예를 들어 수신자가 매번 새로운 비표를 보내고 송신자가 이를 포함한 응답의 MAC을 생성하게 하면, 과거 응답에는 현재 요구한 비표가 들어 있지 않다. 수신자가 **현재 비표와의 일치 여부**를 검사하여 과거 응답의 재사용을 거부할 수 있다.

② X: 리다이렉션(redirection)은 요청이나 통신을 다른 위치로 보내는 기능이다. 목적지를 바꾸는 것만으로는 **메시지의 최신성이나 중복 여부를 확인할 수 없다**. 재전송을 막으려면 비표·타임스탬프·순서 번호 등의 정보를 MAC으로 보호하고, 수신자가 이를 검사하여 과거 메시지를 거부하도록 해야 한다.

③ O: 타임스탬프(timestamp)는 메시지가 생성되거나 전송된 시각을 나타낸다. 수신자는 자신의 시각과 비교하여 **허용 시간 범위를 벗어난 메시지**를 거부할 수 있다. 이를 위해 송수신 측의 시각이 적절히 동기화되어야 하며, 허용 시간 안의 재전송까지 막으려면 이미 수신한 메시지를 기록하는 등의 중복 검사도 필요하다.

④ O: 순서 번호(sequence number)는 메시지마다 번호를 부여하여 전송 순서와 중복 여부를 확인하게 한다. 수신자는 **이미 처리한 번호가 다시 나타나는지**를 검사하여 재전송을 거부할 수 있다. 예를 들어 처리한 번호가 다시 들어오면 MAC이 유효하더라도 같은 메시지의 반복으로 판단하여 수락하지 않는다.

NoteBase

문 15. 다음 SSH의 전송 계층 프로토콜 작업을 순서대로 나열한 것은?

(가) 서비스 요청(service request)
(나) 키 교환 종료(end of key exchange)
(다) 알고리즘 협상(algorithm negotiation)
(라) 식별 문자열 교환(identification string exchange)

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

정답 4번

간단한 해설

SSH는 사용할 보안 알고리즘을 먼저 합의하고, 그 방식에 따라 키 교환을 마친 뒤 상위 서비스를 요청한다.
따라서 **알고리즘 협상은 키 교환 종료보다 앞서고**, **서비스 요청은 키 교환 뒤**에 이루어진다.

올바른 순서

(라) → (다) → (나) → (가)

(라) 식별 문자열 교환: 연결이 성립하면 양측은 SSH 프로토콜 버전과 소프트웨어 버전이 담긴 문자열을 교환한다. 서로 사용할 프로토콜을 확인한 뒤 키 교환 절차로 진행한다.

(다) 알고리즘 협상: 양측이 지원하는 알고리즘 목록을 교환하여 키 교환 방식, 암호화 방식, 무결성 보호 방식 등을 합의한다. **키 교환에 사용할 방식부터 정해야** 그 방식에 따라 키 교환을 수행할 수 있다.

(나) 키 교환 종료: 협상한 방식으로 키 교환을 수행한 뒤 양측이 SSH_MSG_NEWKEYS 메시지를 보내 키 교환을 끝낸다. 이 메시지 이후에 보내는 메시지부터 **새 키와 알고리즘을 적용**한다.

(가) 서비스 요청: 키 교환을 마친 뒤 클라이언트가 SSH_MSG_SERVICE_REQUEST 메시지로 사용할 상위 서비스를 요청한다. 예를 들어 사용자 인증 서비스인 'ssh-userauth'를 요청할 수 있다. 상위 서비스를 이용하기 전에 전송 계층의 보안 설정이 마련되어야 하므로 이 단계가 뒤에 온다.

NoteBase

문 16. CIDR(Classless Inter-Domain Routing)에 대한 설명으로 옳지 않은 것은?

① IP 주소 고갈 문제를 해결하기 위해 도입되었다.

② IP 주소를 클래스 구분 없이 지정할 수 있게 해 준다.

③ IPv4 주소체계에서만 지원하며, IPv6 주소체계에서는 지원하지 않는다.

④ 슬래시(slash, '/')를 사용하여 네트워크 프리픽스(prefix)의 길이를 표시한다.

정답 3번

간단한 해설

③의 'IPv6 주소체계에서는 지원하지 않는다'는 설명이 틀렸다. IPv6에서도 **클래스 구분 없이 프리픽스 길이로 주소 범위를 나타내는 방식**을 사용한다.

선지별 해설

① O: CIDR은 클래스별로 정해진 크기의 주소 블록을 할당하면서 생기는 낭비를 줄이기 위해 도입되었다. 필요한 규모에 맞추어 주소 블록을 할당하여 **IPv4 주소 고갈을 늦추는** 데 기여한다. 주소 자체의 비트 수를 늘려 고갈 문제를 근본적으로 없애는 방식은 아니다.

② O: 기존 클래스 방식은 A·B·C 클래스에 따라 기본 네트워크 부분의 길이가 정해져 있었다. CIDR은 이러한 **클래스 경계에 얽매이지 않고** 프리픽스 길이를 지정한다. 따라서 주소 블록의 크기를 더 세밀하게 정하여 할당할 수 있다.

③ X: CIDR은 IPv4의 주소 할당과 라우팅 문제를 완화하기 위해 도입되었지만, 클래스 없이 프리픽스를 사용하는 원리가 IPv4에만 한정되는 것은 아니다. **IPv6에서도 프리픽스 길이를 지정하고 공통 프리픽스를 기준으로 경로를 집약**한다. 따라서 'IPv6 주소체계에서는 지원하지 않는다'는 'IPv6에서도 클래스 없는 프리픽스 기반 주소 지정과 경로 집약을 사용한다'로 고친다.

④ O: 주소 뒤에 '/'와 숫자를 붙여 **주소의 맨 앞에서부터 프리픽스에 해당하는 비트 수**를 표시한다. 예를 들어 IPv4의 192.168.1.0/24는 앞의 24비트가 네트워크 프리픽스임을 뜻한다. IPv6의 2001:db8:1::/64도 같은 방식으로 앞의 64비트가 프리픽스임을 나타낸다.

NoteBase

문 17. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

(가) 랜(LAN) 통신 보안을 위해, (나)는 RC4 암호화 알고리즘을 기본으로 사용하며, 암호화 과정에서 24비트의 IV(Initial Vector)를 사용한다.

① (가): 무선, (나): WEP(Wired Equivalent Privacy)

② (가): 무선, (나): WPA2(Wi-Fi Protected Access 2)

③ (가): 유선, (나): WEP

④ (가): 유선, (나): WPA2

정답 1번

간단한 해설

RC4와 **24비트 IV**를 함께 사용하는 것은 무선 LAN 보안 방식인 WEP의 특징이다. WEP의 'Wired Equivalent'는 유선용이라는 뜻이 아니라 **유선에 준하는 기밀성**을 목표로 한다는 뜻이다.

빈칸별 해설

(가) 무선: WEP(Wired Equivalent Privacy)는 **무선 LAN의 통신 내용**을 보호하기 위해 도입된 보안 방식이다. 명칭에 'Wired'가 포함되어 있지만 적용 대상이 유선 LAN이라는 뜻은 아니다. 무선 통신에서도 유선 통신에 준하는 기밀성을 제공한다는 취지의 이름이다.

(나) WEP: WEP는 스트림 암호인 RC4를 사용하며, **24비트 IV와 공유 비밀키를 결합**하여 RC4에 입력한다. IV는 초기화 벡터로, 같은 비밀키를 사용하더라도 암호화에 쓰이는 키스트림을 달리하기 위해 사용하는 값이다. 따라서 'RC4 사용'과 '24비트 IV 사용'이라는 두 조건이 WEP를 가리킨다. WPA2의 핵심 암호 방식은 AES 기반의 CCMP이므로 지문의 특징과 구별된다.

(가)에 무선, (나)에 WEP를 넣은 조합은 ①이다.

NoteBase

문 18. VPN(Virtual Private Network)에 대한 설명으로 옳지 않은 것은?

① VPN 구현을 위해 터널링 기술을 사용한다.

② 기밀성을 제공하기 위해 암호화 기술을 사용한다.

③ VPN 구현을 위해 PPTP, L2TP 등을 사용할 수 있다.

④ SSL VPN은 SA(Security Association)를 생성하기 위해 IKE(Internet Key Exchange)를 사용한다.

정답 4번

간단한 해설

IKE를 이용한 SA 설정은 **IPsec VPN**의 동작이다. SSL VPN은 **SSL/TLS 핸드셰이크**를 통해 암호화 통신에 필요한 알고리즘과 키를 설정한다.

선지별 해설

① O: VPN은 공중망 위에 논리적인 사설 통신 경로를 만들기 위해 터널링을 사용한다. 터널링은 **원래 패킷을 다른 프로토콜의 패킷 안에 캡슐화**하여 보내고, 터널 끝에서 이를 꺼내는 방식이다.

② O: 기밀성은 권한 없는 사람이 통신 내용을 알아볼 수 없게 하는 성질이다. VPN은 전송 데이터를 **암호화**하여 공중망에서 데이터가 도청되더라도 내용을 쉽게 읽을 수 없도록 한다.

③ O: PPTP와 L2TP는 PPP 패킷을 다른 네트워크를 통해 운반하는 터널링 프로토콜로, VPN 구현에 사용할 수 있다. 다만 **L2TP 자체는 사용자 데이터의 암호화를 제공하지 않으므로**, 기밀성을 확보할 때는 IPsec 등과 결합한다.

④ X: IKE는 **IPsec VPN에서 SA를 설정하고 관리**하는 데 사용하는 키 교환 프로토콜이다. SA는 통신에 적용할 보안 알고리즘과 키 등의 보안 설정 정보를 나타낸다. SSL VPN은 IKE로 IPsec SA를 만드는 방식이 아니라, SSL/TLS 핸드셰이크로 통신 상대를 인증하고 암호 알고리즘과 키를 설정하여 통신을 보호한다.

NoteBase

문 19. SNMP(Simple Network Management Protocol)에 대한 설명으로 옳지 않은 것은?

① 네트워크 관리에 필요한 정보를 주고받기 위해 사용한다.

② 하위 계층 프로토콜로 UDP를 사용한다.

③ 에이전트(agent)는 비정상적인 상황에 대한 경고 메시지를 관리자(manager)에게 보낼 수 있다.

④ 관리자는 에이전트로부터 정보를 가져올 수 있으나, 에이전트에 있는 정보를 설정할 수 없다.

정답 4번

간단한 해설

④의 '정보를 설정할 수 없다'는 설명이 잘못되었다. SNMP 관리자는 조회뿐 아니라 **Set 요청으로 쓰기가 허용된 관리 객체의 값을 설정**할 수 있다.

선지별 해설

① O: SNMP는 네트워크 장비의 상태를 감시하고 제어하는 데 필요한 관리 정보를 교환하는 응용 계층 프로토콜이다. 관리자는 장비의 에이전트와 통신하여 상태 정보를 조회하거나 설정을 변경한다.

② O: SNMP는 일반적으로 하위 전송 계층 프로토콜로 **UDP**를 사용한다. SNMP의 조회·설정 요청과 응답 등의 메시지는 UDP 데이터그램에 담겨 전달된다.

③ O: 에이전트는 통신 연결의 장애 등 특정 사건이 발생하면 **관리자의 요청 없이 Trap 메시지**를 보내 이를 알릴 수 있다. 이는 관리자가 먼저 요청하여 정보를 조회하는 방식과 구별된다.

④ X: 관리자는 Get 요청으로 에이전트의 관리 정보를 조회할 수 있으며, Set 요청으로 관리 정보 베이스(MIB)에 정의된 관리 객체의 값을 설정할 수도 있다. 다만 **쓰기 가능한 객체이고 관리자에게 쓰기 권한이 있어야** 한다. 따라서 '정보를 설정할 수 없다'는 '허용된 관리 객체의 값을 설정할 수 있다'로 고쳐야 한다.

NoteBase

문 20. 터널 모드로 동작하는 IPSec의 ESP(Encapsulating Security Payload) 프로토콜에서 사용하는 다음 패킷의 구조 (가) ~ (다)에 들어갈 내용을 바르게 연결한 것은? (단, 패킷의 버전은 IPv4이다)



① (가): ESP 헤더, (나): 기존 IP 헤더, (다): 새 IP 헤더

② (가): ESP 헤더, (나): 새 IP 헤더, (다): 기존 IP 헤더

③ (가): 새 IP 헤더, (나): 기존 IP 헤더, (다): ESP 헤더

④ (가): 새 IP 헤더, (나): ESP 헤더, (다): 기존 IP 헤더

정답 4번

간단한 해설

터널 모드에서는 **기존 IP 패킷 전체를 ESP로 캡슐화**하고, 그 바깥에 전송용 새 IP 헤더를 붙인다. 따라서 기존 IP 헤더는 TCP 바로 앞에 남고, ESP 헤더는 새 IP 헤더와 기존 IP 헤더 사이에 놓인다.

빈칸별 해설

ESP 터널 모드는 기존 IP 헤더·TCP 헤더·데이터를 하나의 내부 IP 패킷으로 감싼다. 그림의 (가)~(다)는 이 내부 패킷과 새로 붙는 외부 헤더의 위치를 구분하여 채운다.

(가) 새 IP 헤더: 터널 구간에서 패킷을 전달하기 위한 **외부 IP 헤더**이다. 터널 양 끝의 IPsec 장비 주소를 담아 라우팅에 사용되므로 가장 바깥인 맨 앞에 놓인다.

(나) ESP 헤더: 새 IP 헤더 뒤이자 **기존 IP 패킷 앞**에 놓인다. 수신 측이 적용할 보안 연결을 식별하는 SPI와 재전송 공격 방지에 사용하는 순서 번호를 담는다.

(다) 기존 IP 헤더: 원래 통신의 출발지·목적지 주소를 담는 **내부 IP 헤더**이다. 기존 패킷이 통째로 캡슐화되므로 TCP 바로 앞의 위치를 유지한다. 기밀성을 제공하는 암호화를 적용하면 이 헤더도 TCP 헤더·데이터와 함께 암호화된다.

따라서 (가)는 새 IP 헤더, (나)는 ESP 헤더, (다)는 기존 IP 헤더로 연결되며, 이 조합은 ④와 일치한다.

NoteBase