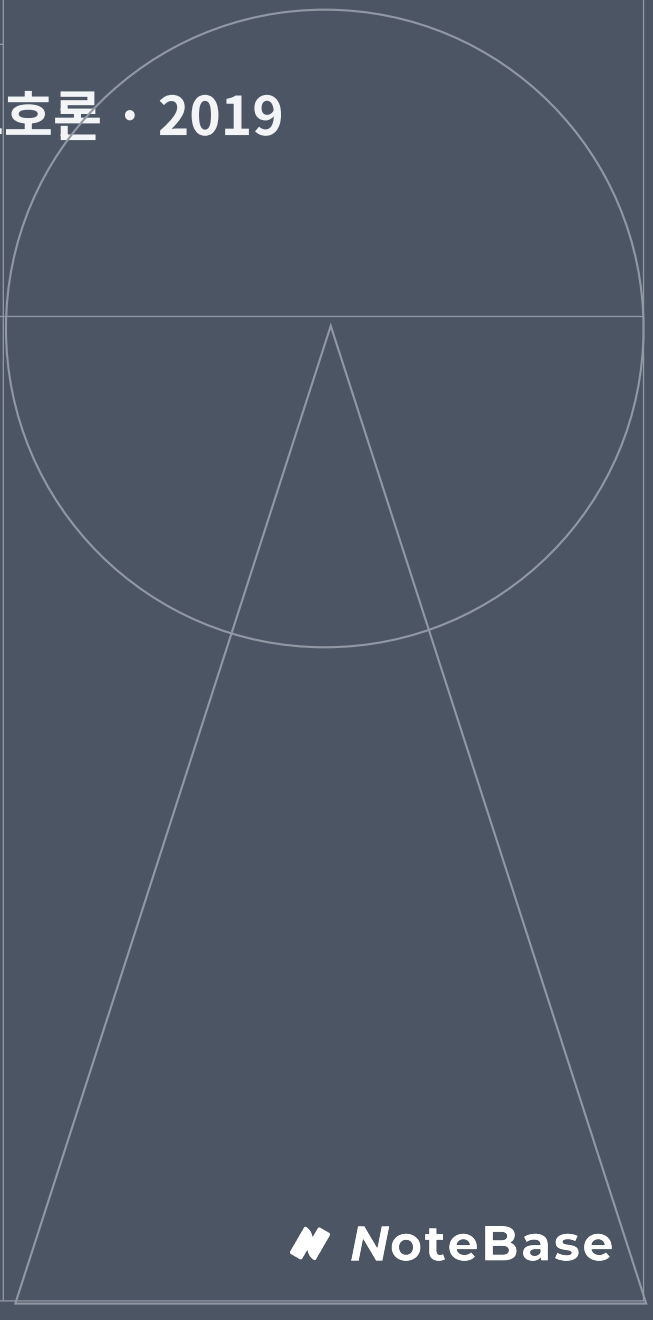
# 기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2019



NoteBase

# 기출OX 해설집

## 공무원/국회직/9급 · 정보보호론 · 2019

공무원/국회직/9급 · 정보보호론 · 2019

1. 다음 설명에서 제시하는 공격의 명칭은?

> 사용자가 특정 웹 사이트에 접속하기 위해 올바른 URL을 입력하였지만, 실제로는 해커가 만들어 놓은 웹 사이트에 접속되었다. 해커의 웹 사이트에서는 불법적으로 개인정보가 수집되고 있었다. 사용자의 컴퓨터는 공격자에게 점유되어 정상적인 URL을 입력해도 이에 해당하는 IP 주소가 공격자의 웹 서버로 연결되도록 되어 있었다.

① Pharming
② Smishing
③ QRshing
④ Phishing
⑤ SQL Injection

**정답 1번**

**출제 포인트**

이 문제는 정상적인 URL을 입력해도 공격자가 조작한 서버로 연결되는 파밍과 다른 사회공학·웹 공격의 차이를 묻는 문제이다.

**핵심 개념**

파밍(Pharming)은 DNS 정보나 호스트 설정 등을 변조하여 사용자가 정상적인 URL을 입력해도 위조 사이트로 접속하게 만드는 공격이다.
피싱(Phishing)은 공격자가 신뢰할 만한 기관이나 사람을 사칭한 메시지·사이트로 사용자를 속여 개인정보 입력이나 악성 링크 접속을 유도하는 공격이다.
스미싱(Smishing)은 문자메시지를 이용한 피싱이고, 큐알싱(QRshing)은 악성 QR 코드를 이용한 피싱이다.
SQL 인젝션은 입력값에 악의적인 SQL 구문을 삽입하여 데이터베이스를 비정상적으로 조회하거나 조작하는 공격이다.

NoteBase

### 선지별 해설

① O — Pharming은 사용자가 정상적인 URL을 입력했는데도 DNS 정보나 컴퓨터의 주소 변환 설정이 변조되어 공격자의 웹 서버로 연결되는 공격이다. 제시된 상황과 일치한다.
② X — Smishing은 문자메시지를 통해 악성 링크 접속이나 개인정보 입력을 유도하는 공격이다. 이 선지의 Smishing은 Pharming으로 고쳐야 한다.
③ X — QRshing은 악성 QR 코드를 스캔하게 하여 위조 사이트 접속이나 악성 앱 설치를 유도하는 공격이다. 이 선지의 QRshing은 Pharming으로 고쳐야 한다.
④ X — Phishing은 사칭 메시지나 위조 사이트로 사용자를 속여 개인정보를 제공하도록 유도하는 포괄적인 공격이다. 정상 URL을 입력했는데도 주소 변환 정보의 변조로 공격자 서버에 연결되는 구체적인 공격 명칭은 Pharming이다.
⑤ X — SQL Injection은 웹 입력값에 악성 SQL 구문을 삽입하여 데이터베이스의 조회·변조·삭제 등을 시도하는 공격이다. 이 선지의 SQL Injection은 Pharming으로 고쳐야 한다.

### 오답 포인트

공격자의 위조 사이트에서 개인정보를 수집한다는 결과만 보면 ④ Phishing을 고르기 쉽다. 그러나 이 문제의 결정적 표현은 '정상적인 URL을 입력해도 공격자의 웹 서버로 연결'된다는 부분이며, 이는 주소 변환 정보를 조작하는 Pharming의 특징이다.

### 다시 나오면 이렇게 판단

공격 매체와 접속 방식으로 구별한다. 정상 주소 입력 후 강제 우회는 Pharming, 사칭 메시지·사이트로 자발적 접속을 유도하면 Phishing, 문자메시지는 Smishing, QR 코드는 QRshing, 악성 SQL 구문으로 데이터베이스를 공격하면 SQL Injection이다.

### 암기 포인트

정상 주소도 가짜 사이트로 바꾸어 보내면 Pharming이다. 문자면 Smishing, QR이면 QRshing, DB 질의문을 찌르면 SQL Injection이다.

NoteBase

**2. 네트워크 보안과 관련된 다음 설명에서 ㉠, ㉡에 들어갈 용어는?**

> 네트워크 인터페이스 카드가 가지고 있는 모드 중 ( ㉠ ) 모드를 설정하여 네트워크 인터페이스 카드를 거치는 모든 데이터를 확인하는 스니핑 공격을 수행할 수 있다. 이 모드 설정을 위해서 Linux 환경에서는 ( ㉡ ) 명령어를 활용한다.

| | ㉠ | ㉡ |
|---|---|---|
| ① | non-promiscuous | netstat |
| ② | promiscuous | netstat |
| ③ | non-promiscuous | ifconfig |
| ④ | promiscuous | ifconfig |
| ⑤ | non-promiscuous | ipconfig |

**정답 4번**

**출제 포인트**

네트워크 인터페이스 카드가 자신에게 전달된 프레임만 처리하는 일반 모드와, 수신되는 모든 프레임을 받아들여 스니핑에 활용할 수 있는 promiscuous 모드를 구별하고 Linux 설정 명령어를 연결하는 문제이다.

**핵심 개념**

promiscuous 모드: 네트워크 인터페이스 카드가 목적지 MAC 주소가 자신의 주소인지와 관계없이 수신되는 프레임을 받아들이는 모드이다. 키워드는 전체 프레임 수신과 스니핑이다.
non-promiscuous 모드: 일반적인 수신 모드로, 주로 자신의 MAC 주소로 온 프레임과 브로드캐스트·관련 멀티캐스트 프레임을 처리한다.
Linux에서는 ifconfig 명령어에 promisc 옵션을 사용하여 promiscuous 모드를 설정할 수 있다. netstat은 네트워크 연결과 통계 등을 확인하는 명령어이고, ipconfig는 주로 Windows에서 IP 설정 정보를 확인하는 명령어이다.

NoteBase

**선지별 해설**

① X — ‘non-promiscuous’와 ‘netstat’이 모두 틀렸다. 모든 프레임을 확인하는 모드는 promiscuous 모드이며, Linux에서 이 모드를 설정할 때 사용하는 명령어는 ifconfig이다.
② X — ‘promiscuous’는 맞지만 ‘netstat’이 틀렸다. netstat은 네트워크 연결·통계 확인에 사용하며, 올바른 설정 명령어는 ifconfig이다.
③ X — ‘ifconfig’는 맞지만 ‘non-promiscuous’가 틀렸다. 스니핑을 위해 모든 수신 프레임을 받아들이는 모드는 promiscuous 모드이다.
④ O — promiscuous 모드는 네트워크 인터페이스 카드가 수신하는 프레임을 폭넓게 받아 스니핑할 수 있게 하며, Linux에서는 ifconfig 명령어로 이 모드를 설정할 수 있다.
⑤ X — ‘non-promiscuous’와 ‘ipconfig’가 모두 틀렸다. 올바른 조합은 promiscuous와 ifconfig이며, ipconfig는 주로 Windows의 IP 설정 정보를 확인하는 명령어이다.

**오답 포인트**

②는 모드 이름만 맞고 명령어가 netstat으로 바뀌어 있으며, ③은 명령어만 맞고 모드 이름이 반대로 제시되어 있다. 모든 프레임 수신은 promiscuous, Linux 설정은 ifconfig라는 두 요소를 각각 확인해야 한다.

**다시 나오면 이렇게 판단**

‘모든 데이터 확인·스니핑’이 보이면 promiscuous 모드를 선택하고, Linux에서 해당 모드를 켜는 명령어를 물으면 ifconfig의 promisc 옵션을 연결한다. 연결·통계 조회인 netstat이나 Windows IP 정보 확인인 ipconfig와 구분한다.

**암기 포인트**

전체 프레임 수신은 promiscuous, Linux 모드 설정은 ifconfig이다.

NoteBase

3. RSA 암호 시스템에서 밥이 앨리스의 공개키 (e, N)= (11, 143)을 취득하여 앨리스에게 평문 4를 암호화하여 보내고자 한다. 이때 전송되는 암호문은?

① $11^4 \mod 143$
② $4^{11} \mod 143$
③ $4^{143} \mod 11$
④ $11^{143} \mod 7$
⑤ $4^{143} \mod 7$

정답 2번

**출제 포인트**

RSA에서 수신자의 공개키와 평문을 이용해 암호문을 만드는 공식을 적용하는 문제이다.

**조건 정리**

주어진 값: 공개 지수 $e = 11$, 법 $N = 143$, 평문 $M = 4$이다.
구해야 할 값: 전송할 암호문 $C$이다.
주의할 조건: 공개키의 $e$는 지수에, $N$은 나머지 연산의 법에 넣는다.

**사용할 공식**

RSA 암호화 공식은 다음과 같다.
C=M^e N
송신자 밥이 수신자 앨리스의 공개키로 평문을 암호화하는 상황이므로 이 공식을 사용한다.

**계산 과정**

주어진 값을 공식에 대입하면 다음과 같다.
C=4^11 143
값까지 계산하면 4^8 ≡ 42 ±od143이고,
4^11=4^8·4^2·4 ≡ 42·16·4=2688 ≡ 114 ±od143
따라서 전송되는 암호문은 4^11 143, 즉 114이다.

NoteBase

### 선지 판단

① X — 11^4 143은 공개 지수 11과 평문 4를 서로 바꾸었다. 올바르게는 4^11 143이다.
② O — 평문 4를 공개 지수 11만큼 거듭제곱한 뒤 공개키의 법 143으로 나머지를 구한 4^11 143이므로 RSA 암호화 공식과 일치한다.
③ X — 4^143 11은 법 $N = 143$을 지수로, 공개 지수 $e = 11$을 법으로 잘못 배치했다. 올바르게는 4^11 143이다.
④ X — 11^143 7은 평문 4를 밑으로 사용하지 않고, 공개키의 두 값도 지수와 법에 맞게 배치하지 않았다. 올바르게는 4^11 143이다.
⑤ X — 4^143 7은 밑만 평문 4와 같을 뿐, 지수 143과 법 7이 공개키와 일치하지 않는다. 올바르게는 4^11 143이다.
계산식과 일치하는 선지는 ②이다.

### 오답 포인트

공개키를 나타내는 순서 $(e, N)$를 보고 두 수를 그대로 식의 앞뒤에 놓는 것이 함정이다. $e$는 평문의 지수이고 $N$은 나머지 연산의 법이라는 역할을 구분해야 한다.

### 다시 나오면 이렇게 판단

RSA 암호화 문제에서는 먼저 평문을 $M$, 공개키의 첫째 값을 $e$, 둘째 값을 $N$으로 대응시킨 뒤 C=M^e N에 대입한다.

### 암기 포인트

RSA 암호화는 '평문을 공개 지수만큼 거듭제곱하고 공개 모듈러스로 나눈 나머지', 즉 C=M^e N이다.

NoteBase

**4.** 다음과 같은 정보보안 요구사항이 존재할 때 필요한 정보보호 시스템들을 짝지은 것으로 옳은 것은?

> 공인 IP 주소 자원의 효율적인 관리를 위해 사설 IP와의 연계를 수행하고 조직 내부의 네트워크 구조를 외부에서 알 수 없도록 하고 싶다. 또한, 내부에서 외부로의 정보유출을 탐지하여 개인정보 및 민감 정보의 유출을 차단하고자 한다.

① NAT-VPN
② IPS-DLP
③ NAT-SSL
④ IPS-SSL
⑤ NAT-DLP

**정답 5번**

**출제 포인트**

공인 IP 주소와 사설 IP 주소의 연계 및 내부 네트워크 구조 은닉에는 NAT가, 조직 내부의 개인정보·민감정보가 외부로 유출되는 것을 탐지하고 차단하는 데에는 DLP가 적합하다는 점을 묻는 문제이다.

**핵심 개념**

NAT: 사설 IP 주소와 공인 IP 주소를 변환하여 여러 내부 단말이 공인 IP 자원을 효율적으로 사용하게 하고, 외부에서 내부 주소 체계를 직접 알기 어렵게 하는 기술이다. 키워드는 IP 주소 변환과 내부 주소 은닉이다.
DLP: 데이터의 내용과 정책을 기준으로 개인정보·기밀정보 등 중요 정보의 외부 전송을 탐지하고 차단하는 정보유출방지 기술이다. 키워드는 중요 정보 식별과 유출 통제이다.
IPS: 공격 패턴이나 비정상 트래픽을 탐지하여 침입을 차단하는 시스템이다.
VPN·SSL: 통신 구간의 기밀성과 무결성을 위해 암호화된 통신을 제공하는 기술이며, 정보 내용 자체를 판별하여 유출을 통제하는 DLP와 목적이 다르다.

NoteBase

**선지별 해설**

① X — NAT는 공인·사설 IP 연계와 내부 주소 은닉에 적합하지만, VPN은 안전한 원격 접속이나 암호화 통신망을 제공하는 기술이므로 민감정보의 외부 유출을 내용 기반으로 탐지·차단하는 요구에 맞지 않는다. 틀린 표현은 'VPN'이며, 올바르게는 'DLP'이므로 NAT-DLP가 되어야 한다.
② X — DLP는 정보유출 차단 요구에 적합하지만, IPS는 침입 공격을 탐지·차단하는 시스템으로 공인 IP와 사설 IP를 변환하지 않는다. 틀린 표현은 'IPS'이며, 올바르게는 'NAT'이므로 NAT-DLP가 되어야 한다.
③ X — NAT는 첫 번째 요구에 적합하지만, SSL은 통신 구간을 암호화하는 기술일 뿐 개인정보나 민감정보의 유출 여부를 내용 기반으로 판별하여 차단하는 기술이 아니다. 틀린 표현은 'SSL'이며, 올바르게는 'DLP'이므로 NAT-DLP가 되어야 한다.
④ X — IPS는 침입 탐지·차단용이고 SSL은 통신 암호화용이므로 두 요구사항에 각각 대응하지 못한다. 틀린 표현은 'IPS-SSL'이며, 올바르게는 'NAT-DLP'이다.
⑤ O — NAT는 공인 IP 자원의 효율적 사용과 내부 네트워크 주소 구조의 은닉을 지원하고, DLP는 개인정보·민감정보의 외부 유출을 탐지하고 차단하므로 두 요구사항에 정확히 대응한다.

**오답 포인트**

VPN과 SSL도 정보를 보호하는 기술이어서 DLP와 혼동하기 쉽다. 그러나 VPN·SSL은 전송 구간을 암호화하는 데 초점이 있고, DLP는 전송하려는 데이터의 내용과 보안 정책을 검사하여 유출을 통제한다. 또한 IPS의 '차단'은 주로 외부 공격과 침입을 대상으로 하므로 내부 중요 정보의 유출 방지와 구별해야 한다.

**다시 나오면 이렇게 판단**

요구사항의 동사를 기준으로 판단한다. '사설 IP와 공인 IP의 변환·연계, 내부 주소 은닉'이면 NAT이고, '개인정보·기밀정보의 외부 유출 탐지·차단'이면 DLP이다. '침입 탐지·차단'은 IPS, '통신 구간 암호화'는 VPN 또는 SSL로 구분한다.

**암기 포인트**

주소를 바꾸고 숨기는 것은 NAT, 데이터가 새는 것을 막는 것은 DLP이다.

NoteBase

**5. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?**

① 신뢰받는 제3자인 키 배포 기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션 키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 토큰을 이용한 인증 프로토콜이다.
④ 인증 서버가 사용자에게 발급한 티켓(즉, 티켓-승인 티켓)은 유효기간 내에 재사용할 수 있다.
⑤ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

**정답 5번**

### 출제 포인트

Kerberos의 신뢰 구조, 티켓 기반 인증 방식, 티켓 재사용 범위와 SSO 지원 여부를 구별하는 문제이다.

### 핵심 개념

Kerberos는 신뢰받는 제3자인 키 배포 센터(KDC)가 발급한 티켓과 세션 키를 이용하여 네트워크상의 사용자를 인증하는 프로토콜이다.
인증 서버(AS)는 로그인 인증 후 티켓-승인 티켓(TGT)을 발급하고, 티켓 승인 서버(TGS)는 유효한 TGT를 바탕으로 각 서비스에 접근할 서비스 티켓을 발급한다. 사용자는 TGT의 유효기간 동안 매번 비밀번호를 다시 입력하지 않고 여러 서비스의 티켓을 받을 수 있으므로 SSO를 구현할 수 있다.

### 선지별 해설

① O — Kerberos는 신뢰받는 제3자인 KDC가 통신 구성원 사이에서 키와 티켓을 발급하여 인증을 중개하는 구조이다.
② O — Kerberos는 세션 키가 포함된 티켓을 이용하여 사용자와 서비스가 인증 정보를 확인하는 티켓 기반 인증 기법이다.
③ O — Kerberos의 티켓은 인증 권한을 나타내는 토큰으로 기능하므로 Kerberos는 토큰을 이용한 인증 프로토콜에 해당한다.
④ O — 인증 서버가 발급한 TGT는 유효기간 동안 TGS에 여러 서비스 티켓을 요청할 때 재사용할 수 있다. 다만 실제 서비스에 제시하는 서비스 티켓과 TGT는 구별된다.
⑤ X — 틀린 표현은 'SSO 시스템을 구축할 수 없다'이다. Kerberos는 한 번의 로그인으로 TGT를 받은 뒤 여러 네트워크 서비스의 서비스 티켓을 발급받을 수 있으므로, 분산 시스템 환경에서 SSO 시스템을 구축할 수 있다.

NoteBase

### 오답 포인트

분산 시스템에서는 인증 대상이 여러 개이므로 SSO가 불가능하다고 생각하기 쉽다. 그러나 Kerberos는 TGT를 공통 인증 기반으로 삼아 여러 서비스의 티켓을 발급하므로, 바로 그 분산 환경에서 반복 로그인을 줄이는 SSO를 지원한다.

### 다시 나오면 이렇게 판단

Kerberos 선지는 'AS가 TGT 발급 → TGT로 TGS에 서비스 티켓 요청 → 서비스 티켓으로 개별 서비스 이용'의 흐름에 맞추어 판단한다. TGT의 유효기간 내 재사용과 여러 서비스에 대한 SSO 지원은 Kerberos의 핵심 특징이다.

### 암기 포인트

Kerberos는 신뢰받는 제3자, 세션 키, 티켓, TGT 재사용, SSO로 연결한다.

NoteBase

**6. 다음 설명에서 제시하는 목적으로 활용되는 네트워크 보안 기술은?**

> 조직 내에 운영되는 다양한 정보보안 장비 및 IT 시스템들의 이벤트 로그를 수집, 분석하여 이상 징후 및 위험사항을 파악한다. 이렇게 파악된 결과를 인지하기 쉬운 형태로 가공하여 경영진에 보고하기도 한다. 이상 징후의 도출에 전문가의 경험을 활용하거나 인공지능 기술을 활용한다.

① SIEM
② DLP
③ VPN
④ NAT
⑤ IPS

**정답 1번**

**출제 포인트**

여러 보안 장비와 IT 시스템의 이벤트 로그를 통합 수집·분석하여 이상 징후를 탐지하고 보고하는 기술이 SIEM임을 묻는 문제이다.

**핵심 개념**

SIEM(Security Information and Event Management)은 다양한 시스템의 보안 정보와 이벤트 로그를 중앙에서 수집·상관분석하여 위협을 탐지하고, 결과를 시각화·보고하는 통합 보안 관리 기술이다.
DLP는 중요 정보의 유출 방지, VPN은 암호화된 사설 통신 경로 구성, NAT는 사설 주소와 공인 주소의 변환, IPS는 네트워크 침입 탐지 및 차단이 핵심이다.

**선지별 해설**

① O — SIEM은 여러 보안 장비와 IT 시스템의 이벤트 로그를 통합 수집·분석하고, 상관관계를 바탕으로 이상 징후와 위협을 탐지하며, 결과를 대시보드나 보고서로 제공한다. 제시문의 모든 핵심 기능과 일치한다.
② X — 틀린 표현은 'DLP'이다. DLP는 개인정보나 기밀정보 같은 중요 데이터가 외부로 유출되는 것을 탐지·통제하는 기술이다. 제시문에 맞는 용어는 SIEM이다.
③ X — 틀린 표현은 'VPN'이다. VPN은 공중망에서 암호화와 터널링을 이용해 사설망처럼 안전한 통신 경로를 제공하는 기술이다. 제시문에 맞는 용어는 SIEM이다.
④ X — 틀린 표현은 'NAT'이다. NAT는 내부 사설 IP 주소와 외부 공인 IP 주소를 변환하는 기술이다. 제시문에 맞는 용어는 SIEM이다.
⑤ X — 틀린 표현은 'IPS'이다. IPS는 주로 네트워크 트래픽을 검사해 침입 행위를 탐지하고 차단하는 기술이다. 여러 장비의 로그를 통합 수집·상관분석하여 시각화하고 보고하는 제시문의 기술은 SIEM이다.

NoteBase

**오답 포인트**

⑤ IPS도 이상 징후를 탐지한다는 점 때문에 혼동하기 쉽다. 그러나 '다양한 장비와 시스템의 이벤트 로그', '통합 분석', '시각화와 경영진 보고'라는 표현은 개별 트래픽을 탐지·차단하는 IPS가 아니라 SIEM을 가리킨다.

**다시 나오면 이렇게 판단**

문제에서 여러 출처의 로그를 중앙에 모아 상관분석하고 대시보드·보고서로 제공한다고 하면 SIEM으로 판단한다. 데이터 유출 통제는 DLP, 암호화 터널은 VPN, IP 주소 변환은 NAT, 침입 트래픽의 실시간 차단은 IPS로 구분한다.

**암기 포인트**

SIEM은 로그 통합·상관분석·탐지·보고, IPS는 침입 탐지·차단이다.

NoteBase

**7. 보안 프로토콜에 대한 설명으로 옳지 않은 것은?**

① 경량 프로토콜인 CoAP는 DTLS를 사용하여 보안성을 제공한다.
② 사물인터넷 프로토콜인 MQTT는 TLS 프로토콜을 사용한다.
③ TLS 프로토콜은 UDP 상에서 동작하므로 많은 인터넷 응용에서 사용된다.
④ HTTPS는 HTTP 프로토콜에 SSL/TLS를 적용한 것이다.
⑤ SSH은 TCP 프로토콜 상에서 사용되며, telnet의 안전성 보장에 사용된다.

**정답 3번**

**출제 포인트**

보안 프로토콜이 사용하는 전송 프로토콜과 TLS·DTLS의 적용 관계를 구분하는 문제이다.

**핵심 개념**

TLS는 신뢰성 있는 연결형 전송을 전제로 통신 내용을 암호화하고 무결성과 인증을 제공하는 보안 프로토콜로, 일반적으로 TCP 위에서 사용된다.
DTLS는 데이터그램 환경에 맞게 설계된 TLS 계열 프로토콜로, UDP 기반 응용에서 사용된다.
CoAP는 주로 UDP 기반의 경량 사물인터넷 프로토콜이므로 DTLS를 적용할 수 있고, MQTT는 일반적으로 TCP 기반이므로 TLS를 적용한다. HTTPS는 HTTP에 TLS를 적용한 것이며, SSH는 TCP 위에서 안전한 원격 접속을 제공한다.

**선지별 해설**

① O — CoAP는 자원이 제한된 사물인터넷 환경을 위한 경량 프로토콜이며, UDP 기반 CoAP 통신의 보안을 위해 DTLS를 사용할 수 있다.
② O — MQTT는 일반적으로 TCP 위에서 동작하며, 통신 기밀성·무결성 및 서버 인증 등을 위해 TLS를 사용할 수 있다.
③ X — 틀린 표현은 'TLS 프로토콜은 UDP 상에서 동작한다'이다. TLS는 일반적으로 TCP와 같은 신뢰성 있는 전송 위에서 사용되며, UDP 환경에서는 데이터그램용으로 설계된 DTLS를 사용한다. 따라서 'DTLS는 UDP 상에서 동작하여 UDP 기반 인터넷 응용의 보안에 사용된다'로 고쳐야 한다.
④ O — HTTPS는 HTTP 통신에 SSL/TLS를 적용하여 암호화와 인증 기능을 제공하는 방식이다. 현재는 보안상 TLS가 중심이 된다.
⑤ O — SSH는 TCP 기반의 안전한 원격 접속 프로토콜이며, 평문으로 정보를 주고받는 telnet을 대신하여 원격 로그인과 명령 실행의 보안을 제공한다.

NoteBase

**오답 포인트**

③은 TLS와 DTLS를 바꾸어 놓은 선지이다. 이름에 TLS가 포함된다는 이유로 DTLS와 TLS의 전송 방식을 같게 보면 안 된다. UDP에는 DTLS, 일반적인 TCP 연결에는 TLS가 대응한다.

**다시 나오면 이렇게 판단**

먼저 응용 프로토콜이 TCP 기반인지 UDP 기반인지 확인한다. TCP 기반의 HTTP·MQTT에는 TLS, UDP 기반의 CoAP에는 DTLS가 대응한다는 기준으로 판단한다. SSH는 TCP 기반의 보안 원격 접속 프로토콜로 구분한다.

**암기 포인트**

TCP에는 TLS, UDP에는 DTLS, HTTP+TLS는 HTTPS, 안전한 telnet 대체는 SSH이다.

NoteBase

**8. 블록 암호(Block Cipher) 모드에 대한 설명으로 옳지 않은 것은?**

① ECB(Electronic CodeBook) 모드는 평문 블록을 암호화한 것이 그대로 암호문 블록이 된다.

② CBC(Cipher Block Chaining) 모드는 암호화 전에 XOR 연산을 수행한다.

③ CFB(Cipher FeedBack) 모드는 평문 블록을 암호 알고리즘으로 직접 암호화한다.

④ OFB(Output FeedBack) 모드는 암호 알고리즘의 출력을 암호 알고리즘의 입력으로 피드백한다.

⑤ CTR(CounTeR) 모드는 스트림 암호의 일종으로 카운터의 값이 암호화의 입력이 된다.

**정답 3번**

**출제 포인트**

블록 암호 운용 모드인 ECB, CBC, CFB, OFB, CTR이 블록 암호의 입력을 구성하고 이전 블록이나 카운터를 이용하는 방식을 구별하는 문제이다.

**핵심 개념**

ECB는 각 평문 블록을 서로 독립적으로 암호화한다.
CBC는 평문 블록을 이전 암호문 블록과 XOR한 뒤 암호화하며, 첫 블록에는 IV를 사용한다.
CFB는 이전 암호문 블록(첫 단계에서는 IV)을 암호화한 출력과 평문을 XOR하여 암호문을 만든다.
OFB는 블록 암호의 출력을 다음 블록 암호 입력으로 되먹임하여 키 스트림을 만들고, 이를 평문과 XOR한다.
CTR은 서로 다른 카운터 값을 블록 암호에 입력하여 키 스트림을 만들고, 이를 평문과 XOR한다.

**선지별 해설**

① O — ECB에서는 각 평문 블록을 블록 암호로 직접 암호화하며, 그 결과가 해당 암호문 블록이 된다.
② O — CBC 암호화에서는 현재 평문 블록과 이전 암호문 블록을 먼저 XOR한 후 그 결과를 암호화한다. 첫 블록은 이전 암호문 대신 IV와 XOR한다.
③ X — 틀린 표현은 '평문 블록을 암호 알고리즘으로 직접 암호화한다'이다. CFB에서는 이전 암호문 블록(첫 단계에서는 IV)을 블록 암호의 암호화 함수에 입력하고, 그 출력과 현재 평문을 XOR하여 암호문을 만든다.
④ O — OFB에서는 블록 암호의 출력이 다음 암호화 연산의 입력으로 피드백된다. 이렇게 생성된 출력 키 스트림을 평문과 XOR한다.
⑤ O — CTR에서는 카운터 값을 블록 암호의 암호화 함수에 입력하여 키 스트림을 생성하고, 이를 평문과 XOR하므로 스트림 암호처럼 동작한다.

NoteBase

**오답 포인트**

③은 CFB도 평문을 사용하는 모드라는 점을 이용해 '평문을 직접 암호화한다'고 바꾼 함정이다. 평문은 블록 암호 함수의 입력이 아니라, 이전 암호문 또는 IV를 암호화해 얻은 출력과 XOR되는 대상이다.

**다시 나오면 이렇게 판단**

블록 암호 함수에 실제로 무엇이 입력되는지를 확인한다. ECB는 평문, CBC는 평문과 이전 암호문의 XOR값, CFB는 이전 암호문 또는 IV, OFB는 직전 암호화 출력, CTR은 카운터가 입력된다.

**암기 포인트**

ECB는 평문 직접, CBC는 XOR 후 암호화, CFB는 암호문 피드백, OFB는 출력 피드백, CTR은 카운터 암호화이다.

NoteBase

9. 파일을 실행시킬 때 사용자의 권한이 아닌 일시적으로 파일 소유자(특히 관리자)의 권한을 가지기 때문에 공격에 많이 사용되는 것은?

① setuid
② setgid
③ uid
④ gid
⑤ sticky bit

**정답 1번**

**출제 포인트**

실행 파일에 설정되는 특수 권한 비트인 setuid, setgid, sticky bit의 기능을 구별하는 문제이다.

**핵심 개념**

setuid: 실행 파일을 실행하는 동안 프로세스의 유효 사용자 ID를 그 파일 소유자의 사용자 ID로 설정하는 특수 권한 비트이다. 파일 소유자가 root이면 실행자가 일시적으로 root 권한을 사용할 수 있어, 취약한 setuid 프로그램은 권한 상승 공격의 표적이 된다.
setgid: 실행 파일에서는 프로세스의 유효 그룹 ID를 파일 소유 그룹의 ID로 설정한다. 디렉터리에서는 새로 생성되는 파일과 하위 디렉터리가 부모 디렉터리의 그룹을 물려받게 한다.
sticky bit: 주로 공유 디렉터리에서 파일의 소유자, 디렉터리 소유자 또는 특권 사용자만 해당 파일을 삭제하거나 이름을 바꿀 수 있게 제한한다.
UID와 GID는 각각 사용자와 그룹을 식별하는 번호이고, setuid와 setgid는 실행 시 유효 권한을 바꾸는 특수 권한 비트이다.

**선지별 해설**

① O — setuid가 설정된 실행 파일은 실행 중 파일 소유자의 유효 사용자 권한으로 동작한다. 특히 소유자가 root인 프로그램에 취약점이 있으면 일반 사용자가 관리자 권한을 얻는 공격에 악용될 수 있다.
② X — 틀린 표현은 'setgid'이다. setgid는 파일 소유자의 사용자 권한이 아니라 파일 소유 그룹의 권한으로 실행되게 한다.
③ X — 틀린 표현은 'uid'이다. UID는 사용자를 식별하는 번호일 뿐, 실행 시 파일 소유자의 권한을 부여하는 특수 권한이 아니다. 올바른 용어는 setuid이다.
④ X — 틀린 표현은 'gid'이다. GID는 그룹을 식별하는 번호일 뿐이며, 파일 소유자의 사용자 권한으로 실행시키지 않는다. 그룹 권한과 관련된 특수 비트는 setgid이고, 문제에서 묻는 파일 소유자의 사용자 권한과 관련된 것은 setuid이다.
⑤ X — 틀린 표현은 'sticky bit'이다. sticky bit는 주로 공유 디렉터리에서 다른 사용자가 소유한 파일의 삭제나 이름 변경을 제한한다. 실행 파일을 파일 소유자의 사용자 권한으로 동작시키는 것은 setuid이다.

NoteBase

**오답 포인트**

‘파일 소유자’와 ‘파일 소유 그룹’을 혼동하면 setuid와 setgid를 바꾸어 고르기 쉽다. 또한 UID·GID는 식별자이고 setuid·setgid는 특수 권한 비트라는 차이를 구별해야 한다.

**다시 나오면 이렇게 판단**

실행 중 파일 소유자의 사용자 권한이면 setuid, 파일 소유 그룹의 권한이면 setgid, 공유 디렉터리의 삭제·이름 변경 제한이면 sticky bit로 판단한다.

**암기 포인트**

setuid는 소유자(User), setgid는 소유 그룹(Group), sticky bit는 공유 디렉터리의 삭제 제한이다.

NoteBase

10. 개인정보 비식별화 조치로 볼 수 없는 것은?

① 가명 처리
② 총계 처리
③ 데이터 값 삭제
④ 범주화 수행
⑤ 공개키 암호 기반 서명값 생성

**정답 5번**

**출제 포인트**

개인정보에서 개인을 알아볼 가능성을 낮추는 비식별화 조치와, 데이터의 무결성·서명자 확인을 위한 전자서명 기술을 구별하는 문제이다.

**핵심 개념**

개인정보 비식별화는 식별자를 바꾸거나, 정보를 요약·삭제·일반화하여 특정 개인을 알아보기 어렵게 만드는 처리이다.
가명 처리는 식별자를 다른 값으로 대체하고, 총계 처리는 개별 값을 합계·평균 등 집계값으로 바꾸며, 데이터 값 삭제는 식별에 기여하는 값을 제거하고, 범주화는 구체적인 값을 더 넓은 구간이나 범주로 일반화한다.
전자서명은 데이터의 무결성과 서명자 확인 등을 위한 기술로서, 그 자체가 개인정보의 식별 가능성을 낮추는 조치는 아니다.

**선지별 해설**

① O — 가명 처리는 성명이나 식별번호 같은 식별자를 다른 값으로 대체하여 원래 개인을 곧바로 알아보기 어렵게 하므로 비식별화 조치로 볼 수 있다.
② O — 총계 처리는 개별 정보를 합계·평균·빈도와 같은 집계 형태로 제시하여 개인 단위 정보의 노출을 줄이므로 비식별화 조치로 볼 수 있다.
③ O — 데이터 값 삭제는 개인을 식별할 수 있거나 식별 가능성을 높이는 값을 제거하는 방식이므로 비식별화 조치로 볼 수 있다.
④ O — 범주화는 나이 27세를 20대로 바꾸는 것처럼 구체적인 값을 더 넓은 범주로 일반화하여 식별 가능성을 낮추므로 비식별화 조치로 볼 수 있다.
⑤ X — 틀린 표현은 '공개키 암호 기반 서명값 생성'이다. 이는 전자서명을 만들어 데이터의 무결성과 서명자 확인 등을 제공하는 기술이다. 올바르게는 개인정보 비식별화 조치가 아니라 전자서명 조치라고 해야 한다.

**오답 포인트**

⑤에는 '암호'라는 보안 용어가 들어 있어 비식별화처럼 보이지만, 서명값 생성은 개인정보를 숨기거나 일반화하는 처리가 아니다. 보안 기술이라는 공통점만 보고 비식별화 조치로 판단하면 안 된다.

NoteBase

**다시 나오면 이렇게 판단**

해당 처리가 개인을 알아볼 수 있는 정보의 구체성이나 연결 가능성을 실제로 낮추는지 확인한다.
대체·집계·삭제·범주화는 비식별화에 해당하지만, 서명 생성은 무결성과 서명자 확인을 위한 기능이므로 구분한다.

**암기 포인트**

비식별화는 대체·집계·삭제·범주화, 전자서명은 무결성·서명자 확인이다.

NoteBase

11. TCP/IP 기반의 네트워크에서 목적지 호스트까지의 경로를 파악하기 위해서 데이터그램의 TTL 값과 ICMP Time Exceeded 메시지를 기반으로 동작되는 도구는?

① ipconfig
② traceroute
③ nslookup
④ netstat
⑤ telnet

**정답 2번**

**출제 포인트**

이 문제는 TTL을 단계적으로 증가시키고 ICMP Time Exceeded 메시지를 이용해 목적지까지 거치는 라우터를 확인하는 경로 추적 도구를 묻는다.

**핵심 개념**

traceroute는 TTL이 1, 2, 3, …인 데이터그램을 차례로 보내고, 각 라우터에서 TTL이 0이 될 때 돌아오는 ICMP Time Exceeded 메시지를 이용해 홉별 경로를 알아내는 도구이다.
ipconfig는 호스트의 IP 설정 확인, nslookup은 DNS 조회, netstat은 네트워크 연결과 통계 확인, telnet은 원격 접속 또는 TCP 서비스 연결 확인에 사용된다.

**선지별 해설**

① X — ipconfig는 로컬 호스트의 IP 주소, 서브넷 마스크, 기본 게이트웨이 등 TCP/IP 설정을 확인하는 명령이다. 목적지까지의 경로를 추적하는 도구는 traceroute이다.
② O — traceroute는 데이터그램의 TTL을 순차적으로 늘려 전송하고, 중간 라우터가 보내는 ICMP Time Exceeded 메시지로 각 홉을 파악한다.
③ X — nslookup은 도메인 이름과 IP 주소 등 DNS 정보를 조회하는 도구이다. TTL과 ICMP 응답으로 경로를 파악하는 도구는 traceroute이다.
④ X — netstat은 현재 네트워크 연결, 수신 대기 포트, 라우팅 정보, 프로토콜 통계 등을 확인하는 도구이다. 목적지까지의 홉별 경로를 확인하는 도구는 traceroute이다.
⑤ X — telnet은 원격 터미널 접속이나 특정 TCP 포트의 연결 가능 여부 확인에 쓰인다. TTL과 ICMP Time Exceeded 메시지를 이용한 경로 추적에는 traceroute를 사용한다.

**오답 포인트**

선지들은 모두 네트워크 관련 명령이지만 기능이 다르다. 문제의 결정적 표현은 ‘TTL 값’과 ‘ICMP Time Exceeded’이며, 이는 단순한 IP 설정·DNS 조회·연결 상태 확인이 아니라 홉별 경로 추적을 뜻한다.

NoteBase

**다시 나오면 이렇게 판단**

TTL을 1부터 증가시키며 중간 라우터의 ICMP Time Exceeded 응답을 수집한다는 설명이 나오면 traceroute로 판단한다.

**암기 포인트**

TTL + ICMP Time Exceeded + 홉별 경로 = traceroute이다.

NoteBase

**12. 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 옳지 않은 것은?**

① 물리적 망분리와 논리적 망분리 기법이 존재한다.
② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.
③ 논리적 망분리 기법으로는 SBC 및 CBC 기반의 망분리 기법이 존재한다.
④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.
⑤ 데이터 다이오드 기반 데이터 일방향성을 이용하여 망분리 실현이 가능하다.

**정답 4번**

**출제 포인트**

망분리의 물리적 방식과 논리적 방식, 그리고 각 방식에 사용되는 기술을 구분하는 문제이다.

**핵심 개념**

물리적 망분리: 업무망과 인터넷망을 별도의 단말·네트워크로 분리하여 물리적인 접속 경로를 차단하는 방식이다. 다만 USB 같은 이동식 저장 매체를 통한 악성 코드 유입 가능성까지 자동으로 없어지는 것은 아니다.
논리적 망분리: 하나의 물리적 환경에서 가상화 등의 기술로 업무 영역과 인터넷 영역을 논리적으로 격리하는 방식이다. SBC·CBC, 애플리케이션 가상화, 데스크톱 가상화 등이 여기에 해당한다.
데이터 다이오드: 데이터가 한 방향으로만 흐르게 하는 장치로, 망 사이의 역방향 접근을 차단하면서 필요한 데이터 전달을 허용한다.

**선지별 해설**

① O — 망분리는 구현 방식에 따라 별도의 장비와 회선을 사용하는 물리적 망분리와 가상화 기술로 영역을 격리하는 논리적 망분리로 구분한다.
② O — 물리적으로 망을 분리해도 감염된 USB 등 저장 매체를 두 망에서 사용하면 악성 코드가 반입될 수 있다.
③ O — SBC는 서버에서 실행 환경을 제공하는 방식이고, CBC는 클라이언트 단말에 분리된 실행 환경을 구성하는 방식으로서 모두 논리적 망분리에 활용된다.
④ X — 틀린 표현은 '물리적 망분리 실현'이다. 애플리케이션 가상화와 데스크톱 가상화는 가상화된 실행 환경을 이용해 영역을 격리하므로 논리적 망분리를 실현하는 기술이다.
⑤ O — 데이터 다이오드는 통신 방향을 한쪽으로 제한하여 반대 방향의 접근과 정보 흐름을 차단하므로 물리적으로 분리된 망 사이의 안전한 단방향 연계에 활용할 수 있다.

NoteBase

### 오답 포인트

④는 가상화 기술이 강한 격리 효과를 제공한다는 점을 '물리적' 분리로 바꾸어 놓았다. 격리 효과의 강도가 아니라 실제 망과 장비를 따로 두는지, 같은 물리 환경을 가상화하여 나누는지를 기준으로 판단해야 한다.

### 다시 나오면 이렇게 판단

별도 단말·회선·장비로 접속 경로 자체를 나누면 물리적 망분리이고, 서버·클라이언트·애플리케이션·데스크톱 가상화로 실행 영역을 나누면 논리적 망분리이다.

### 암기 포인트

별도 장비와 회선은 물리적 망분리, 가상화는 논리적 망분리, 데이터 다이오드는 단방향 전송이다.

NoteBase

13. 다음 설명에서 제시하고 있는 공격기법과 연관된 네트워크 프로토콜은?

> 중간자(MITM: Man-In-The-Middle) 공격의 일종으로 같은 네트워크에 설치된 컴퓨터에 "피해 대상 IP 주소를 소유한 컴퓨터의 MAC 주소"를 "공격자의 MAC 주소"로 대체하는 공격을 수행한다. "피해 대상 컴퓨터"로 전달되는 메시지는 "공격자 컴퓨터"를 통해서 "피해 대상 컴퓨터"에 전달된다.

① TCP
② IP
③ ARP
④ ICMP
⑤ HTTP

**정답 3번**

**출제 포인트**

같은 네트워크에서 IP 주소와 MAC 주소의 대응 관계를 위조하여 통신을 가로채는 ARP 스푸핑의 원리를 묻는 문제이다.

**핵심 개념**

ARP(Address Resolution Protocol)는 같은 네트워크에서 목적지의 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다.
ARP 스푸핑 또는 ARP 캐시 포이즈닝은 위조된 ARP 정보를 보내 피해자의 ARP 캐시에 피해 대상 IP 주소와 공격자의 MAC 주소가 연결되도록 만든다. 그 결과 피해자가 보낸 프레임이 공격자에게 먼저 전달되고, 공격자가 이를 다시 실제 목적지로 중계하면 중간자 공격이 성립한다.

NoteBase

### 선지별 해설

① X — TCP는 연결 지향적이고 신뢰성 있는 전송을 제공하는 전송 계층 프로토콜이다. IP 주소와 MAC 주소의 대응 관계를 위조하는 프로토콜은 TCP가 아니라 ARP이다.
② X — IP는 논리 주소를 사용하여 패킷을 전달하고 경로를 선택하는 네트워크 계층 프로토콜이다. 제시된 공격은 IP 자체를 변조하는 공격이 아니라 ARP의 IP–MAC 주소 대응 정보를 위조하는 공격이다.
③ O — ARP는 같은 네트워크에서 IP 주소를 MAC 주소로 해석한다. 공격자가 위조된 ARP 정보를 주입하여 피해 대상 IP 주소에 공격자의 MAC 주소가 대응되게 만드는 수법은 ARP 스푸핑이며, 이를 이용해 트래픽을 공격자 컴퓨터를 거쳐 전달할 수 있다.
④ X — ICMP는 IP 통신 과정의 오류 보고와 진단 등에 사용되는 네트워크 계층 제어 프로토콜이다. 제시된 MAC 주소 대체 공격과 관련된 프로토콜은 ICMP가 아니라 ARP이다.
⑤ X — HTTP는 웹에서 요청과 응답을 주고받는 응용 계층 프로토콜이다. 같은 네트워크의 IP–MAC 주소 대응을 조작하는 공격은 HTTP가 아니라 ARP를 악용한다.

### 오답 포인트

설명에 IP 주소가 등장하므로 ② IP를 고르기 쉽지만, 결정적 표현은 'IP 주소를 소유한 컴퓨터의 MAC 주소를 공격자의 MAC 주소로 대체한다'는 부분이다. IP 주소와 MAC 주소를 연결하는 프로토콜은 ARP이므로 정답은 ③이다.

### 다시 나오면 이렇게 판단

동일 네트워크에서 특정 IP 주소에 대응하는 MAC 주소를 속이거나 ARP 캐시를 오염시켜 트래픽을 우회시키는 설명이면 ARP 스푸핑으로 판단한다.

### 암기 포인트

IP–MAC 주소 대응은 ARP, 그 대응 관계의 위조는 ARP 스푸핑이다.

NoteBase

14. 전문가의 경험과 지식을 활용하여 빠르게 진행되는 위험 분석 접근법은?

① 비정형 접근법(Informal Approach)
② 상세 위험 분석 접근법(Detailed Risk Analysis)
③ 기준 접근법(Baseline Approach)
④ 수학 공식 접근법(Math Formula Approach)
⑤ 단위 접근법(Unit Approach)

**정답 1번**

**출제 포인트**

위험 분석 접근법을 구분하고, 전문가의 경험과 지식을 활용해 신속하게 판단한다는 단서가 비정형 접근법을 뜻함을 묻는 문제이다.

**핵심 개념**

비정형 접근법은 정형화된 분석 절차나 계산보다 전문가의 경험과 직관을 활용하여 위험을 빠르게 식별·평가하는 방법이다.
상세 위험 분석 접근법은 자산·위협·취약성 등을 체계적으로 상세 분석하는 방법이다.
기준 접근법은 조직에 미리 정해진 표준 보안 수준과 통제 기준을 적용하는 방법이다.
복합 접근법은 기준 접근법 등으로 우선순위를 정한 뒤 중요한 영역에 상세 분석을 결합하는 방법이다.

**선지별 해설**

① O — 비정형 접근법은 전문가의 경험과 지식을 바탕으로 복잡한 정량 계산 없이 신속하게 위험을 분석하므로 문제의 설명과 일치한다.
② X — '상세 위험 분석 접근법'은 자산 가치, 위협, 취약성, 발생 가능성, 영향 등을 구체적으로 분석하므로 일반적으로 시간과 비용이 많이 든다. 올바르게는 '전문가의 경험과 지식을 활용하여 빠르게 진행하는 접근법은 비정형 접근법이다'라고 해야 한다.
③ X — '기준 접근법'은 정해진 표준 보안 수준이나 통제 기준을 일괄 적용하는 방식이다. 신속할 수는 있지만 문제에서 강조한 전문가의 경험과 지식에 따른 판단 방식은 아니다. 올바르게는 '기준 접근법은 미리 설정된 보안 기준을 적용하는 방식이다'라고 해야 한다.
④ X — '수학 공식 접근법'은 대표적인 위험 분석 접근법의 독립된 분류가 아니다. 수치와 공식을 활용하는 것은 정량적 위험 분석의 기법이 될 수 있다. 올바르게는 '전문가의 경험과 지식으로 신속하게 분석하는 방식은 비정형 접근법이다'라고 해야 한다.
⑤ X — '단위 접근법'은 대표적인 위험 분석 접근법의 독립된 분류가 아니다. 여러 방법을 함께 사용하는 대표적 분류는 복합 접근법이다. 올바르게는 '기준 적용과 상세 분석 등을 결합하는 방식은 복합 접근법이다'라고 해야 한다.

NoteBase

**오답 포인트**

③ 기준 접근법도 비교적 빠르게 적용할 수 있어 혼동하기 쉽다. 그러나 기준 접근법의 핵심은 '표준·기준의 적용'이고, ① 비정형 접근법의 핵심은 '전문가의 경험·지식·직관'이다.

**다시 나오면 이렇게 판단**

문제의 단서를 방법과 연결한다. '전문가 경험·직관, 신속한 판단'이면 비정형 접근법, '표준 보안 수준'이면 기준 접근법, '자산·위협·취약성의 세부 분석'이면 상세 위험 분석 접근법, '여러 방식의 결합'이면 복합 접근법으로 판단한다.

**암기 포인트**

경험은 비정형, 표준은 기준, 정밀 분석은 상세, 조합은 복합이다.

NoteBase

**15. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?**

① 사용할 수 있는 대칭 암호 알고리즘에는 IDEA, CAST, 트리플 DES 등이 있다.
② 공개키의 취소 증명서를 발행할 수 있다.
③ 데이터의 압축은 ZIP 형식을 사용한다.
④ RSA, MD5 등의 알고리즘을 이용하여 전자서명을 한다.
⑤ 한 명의 사용자는 다수의 공개키/개인키 쌍을 사용할 수 없다.

**정답 5번**

### 출제 포인트

이 문제는 PGP가 제공하는 암호화·전자서명·압축·키 관리 기능을 정확히 구분하는 문제이다.

### 핵심 개념

PGP는 전자우편과 파일을 보호하기 위해 대칭키 암호화, 공개키 암호화, 해시 기반 전자서명, 데이터 압축을 결합한 보안 방식이다. 사용자는 키 링을 통해 여러 공개키와 개인키 쌍을 관리할 수 있으며, 공개키가 더 이상 안전하지 않을 때를 대비한 키 취소 기능도 제공한다.

### 선지별 해설

① O — PGP는 메시지 본문을 빠르게 암호화하기 위한 대칭 암호 알고리즘으로 IDEA, CAST, 트리플 DES 등을 사용할 수 있다.

② O — PGP에서는 개인키가 노출되거나 더 이상 키를 사용하지 않을 때 해당 공개키의 효력을 취소하도록 공개키 취소 증명서를 발행할 수 있다.

③ O — PGP는 암호화 전에 데이터의 크기를 줄이고 중복 패턴을 제거하기 위해 ZIP 방식으로 데이터를 압축할 수 있다.

④ O — PGP의 전자서명은 메시지의 해시값을 구한 뒤 이를 송신자의 개인키로 처리하는 방식이며, 전통적인 PGP에서는 MD5로 해시값을 만들고 RSA로 서명하는 조합을 사용할 수 있다.

⑤ X — 틀린 표현은 '한 명의 사용자는 다수의 공개키/개인키 쌍을 사용할 수 없다'이다. 올바르게는 한 명의 사용자가 용도나 사용 시기가 다른 여러 공개키/개인키 쌍을 보유하고 키 링으로 관리할 수 있다.

NoteBase

### 오답 포인트

PGP가 사용자마다 공개키와 개인키를 하나씩만 허용한다고 오해하기 쉽다. PGP의 키 링은 여러 사람의 공개키뿐 아니라 한 사용자가 보유한 복수의 키 쌍도 관리할 수 있으므로, ⑤의 '다수의 키 쌍을 사용할 수 없다'가 실제 함정이다.

### 다시 나오면 이렇게 판단

PGP 선지는 기능별로 구분한다. 본문 암호화는 대칭키, 세션 키 전달은 공개키, 전자서명은 해시와 개인키, 용량 감소는 압축, 여러 키와 취소 정보의 관리는 키 링과 취소 증명서에 대응하는지 확인한다.

### 암기 포인트

PGP는 압축·대칭키 암호화·공개키 보호·전자서명을 결합하며, 사용자 한 명도 여러 키 쌍을 관리할 수 있다.

NoteBase

**16. 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?**

① 메시지 자체를 암호화 또는 복호화할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.
② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.
③ 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.
④ 공개키 알고리즘을 사용하여 공개키와 개인키를 생성하고, 공개키를 상대방에게 전달한다.
⑤ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화할 수 있다.

**정답 3번**

**출제 포인트**

이 문제는 하이브리드 암호 시스템에서 대칭키와 공개키 암호가 각각 맡는 역할과 세션키 전달 과정을 묻는 문제이다.

**핵심 개념**

대칭키 암호는 송신자와 수신자가 같은 비밀키를 사용하여 데이터를 빠르게 암호화·복호화하는 방식이다. 공개키 암호는 공개키와 개인키의 쌍을 사용하며, 공개키로 암호화한 정보는 그에 대응하는 개인키로 복호화한다. 하이브리드 암호 시스템은 메시지 본문은 일회성 대칭키인 세션키로 처리하고, 세션키는 수신자의 공개키로 암호화하여 전달한다. 따라서 대칭키 암호의 빠른 처리 속도와 공개키 암호의 안전한 키 전달 장점을 결합한다.

**선지별 해설**

① O — 메시지 자체는 처리 속도가 빠른 대칭키 암호로 암호화하고 복호화한다. 대용량 데이터 전체에 상대적으로 느린 공개키 연산을 적용하지 않는 것이 하이브리드 방식의 핵심이다.
② O — 메시지 암호화에 사용한 대칭키인 세션키는 수신자의 공개키로 암호화하여 전달한다. 그러면 해당 공개키에 대응하는 개인키를 가진 수신자만 세션키를 복원할 수 있다.
③ X — 틀린 표현은 '대칭키 암호의 키 교환 문제가 존재한다'이다. 하이브리드 암호 시스템은 대칭키를 그대로 공유하지 않고 수신자의 공개키로 암호화해 전달함으로써 대칭키의 안전한 사전 공유·전달 문제를 해결한다. 다만 수신자의 공개키가 진짜인지 확인하는 인증 문제는 별도로 관리한다.
④ O — 공개키 암호 사용자는 공개키와 개인키의 쌍을 생성하고 공개키를 상대방에게 제공할 수 있다. 개인키는 소유자가 비밀로 보관하며 상대방에게 전달하지 않는다.
⑤ O — 수신자의 공개키로 암호화된 세션키는 그 공개키와 짝을 이루는 수신자의 개인키로 복호화할 수 있다. 복원한 세션키로 메시지 본문을 복호화한다.

NoteBase

**오답 포인트**

③은 하이브리드 암호 시스템에도 공개키의 진위를 확인하는 인증 문제가 남을 수 있다는 사실을 대칭키의 키 교환 문제와 혼동하게 만든다. 하이브리드 방식이 직접 보완하는 것은 대칭키를 상대방에게 안전하게 전달하는 문제이므로, ③처럼 그 문제가 그대로 존재한다고 하면 옳지 않다.

**다시 나오면 이렇게 판단**

‘본문은 대칭키, 세션키는 수신자의 공개키로 암호화, 수신자는 자신의 개인키로 세션키 복호화’의 흐름을 기준으로 각 선지를 판단한다. 공개키는 배포하고 개인키는 소유자가 비밀로 보관한다.

**암기 포인트**

본문은 빠른 대칭키, 세션키는 수신자의 공개키, 세션키 복호화는 수신자의 개인키이다.

NoteBase

17. <보기>에서 XSS 공격을 수행하는 과정을 나타낸 설명 중 옳지 않은 것은?

<보 기>

ㄱ. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.

ㄴ. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.

ㄷ. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.

ㄹ. 웹 서버에서 XSS 코드가 실행된다.

ㅁ. 공격 결과가 공격자에게 전달된다.

① ㄱ

② ㄴ

③ ㄷ

④ ㄹ

⑤ ㅁ

**정답 4번**

**출제 포인트**

저장형 XSS 공격에서 악성 스크립트가 저장·전달·실행되는 위치를 구분하는 문제이다.

**핵심 개념**

저장형 XSS는 공격자가 게시글 등에 삽입한 악성 스크립트가 웹 서버에 저장되었다가, 다른 사용자가 해당 콘텐츠를 조회할 때 사용자의 웹 브라우저에서 실행되는 공격이다.
핵심 구분은 '저장·전달은 웹 서버, 실행은 사용자 브라우저'이다.

NoteBase

### 선지별 해설

① O
공격자는 악성 XSS 코드를 포함한 게시글을 작성하여 웹 서버에 저장한다. 저장형 XSS의 첫 단계에 해당한다.

② O
웹 사용자가 공격자가 작성한 게시글에 접근하면 저장된 악성 스크립트가 포함된 콘텐츠를 요청하게 된다.

③ O
웹 서버는 저장된 게시글과 그 안의 XSS 코드를 사용자에게 응답으로 전달한다.

④ X
틀린 표현은 '웹 서버에서 XSS 코드가 실행된다'이다. 올바르게는 웹 서버가 XSS 코드를 포함한 콘텐츠를 전달하고, 그 코드는 해당 콘텐츠를 받은 사용자의 웹 브라우저에서 실행된다.

⑤ O
사용자 브라우저에서 실행된 악성 스크립트는 탈취한 세션 정보 등의 공격 결과를 공격자에게 전송할 수 있다.

### 오답 포인트

③의 '웹 서버에서 사용자에게 전달된다'와 ④의 '웹 서버에서 실행된다'를 혼동하기 쉽다. 웹 서버는 저장된 코드를 전달하지만, XSS 코드의 실행 주체는 피해 사용자의 웹 브라우저이다.

### 다시 나오면 이렇게 판단

XSS 공격의 각 단계를 볼 때 저장 위치, 전달 주체, 실행 위치를 나누어 판단한다. 저장형 XSS는 서버에 저장되고 서버를 통해 전달되지만, 악성 스크립트는 클라이언트인 사용자의 브라우저에서 실행된다.

### 암기 포인트

저장형 XSS는 서버에 저장, 브라우저에서 실행이다.

NoteBase

**18. CEK(Contents Encrypting Key)와 KEK(Key Encrypting Key)에 대한 설명으로 옳지 않은 것은?**

① KEK를 이용하여 지켜야 할 키의 개수를 줄일 수 있다.
② 통상적으로 CEK에는 세션 키(Session Key)가, KEK에는 마스터 키(Master Key)가 사용된다.
③ 암호문과 KEK만 있다면 원래의 콘텐츠를 알 수 있다.
④ KEK를 이용하여 CEK를 암호화한다.
⑤ KEK의 기밀성을 유지하기 위하여 PBE(Password Based Encryption)를 이용하기도 한다.

**정답 3번**

**출제 포인트**

이 문제는 콘텐츠를 직접 암호화하는 CEK와 CEK를 보호하는 KEK의 역할 차이를 묻는 문제이다.

**핵심 개념**

CEK(Contents Encrypting Key)는 실제 콘텐츠를 암호화·복호화하는 키이며, 보통 세션별로 생성되는 세션 키이다.
KEK(Key Encrypting Key)는 CEK와 같은 다른 키를 암호화하여 보호하는 키이며, 여러 CEK를 관리하는 상위 키 또는 마스터 키의 역할을 한다.
핵심 흐름은 ‘KEK로 CEK를 복호화한 뒤, CEK로 콘텐츠를 복호화한다’이다.

**선지별 해설**

① O — 하나의 KEK로 여러 CEK를 보호할 수 있으므로, 콘텐츠마다 생성되는 CEK를 모두 별도로 안전하게 보관해야 하는 부담을 줄일 수 있다.
② O — CEK는 통상 세션 키로 사용되어 실제 데이터를 암호화하고, KEK는 여러 CEK를 보호하는 마스터 키로 사용된다.
③ X — 틀린 표현은 ‘암호문과 KEK만 있다면 원래의 콘텐츠를 알 수 있다’이다. KEK는 콘텐츠를 직접 복호화하는 키가 아니라 CEK를 복호화하는 키이므로, 콘텐츠 복호화에는 KEK로 얻은 CEK가 필요하다.
올바르게는 ‘암호문, KEK, 그리고 KEK로 보호된 CEK가 있어야 CEK를 복원한 뒤 원래 콘텐츠를 알 수 있다’이다.
④ O — KEK의 핵심 용도는 CEK를 암호화하여 안전하게 저장하거나 전달하는 것이다.
⑤ O — 비밀번호 기반 암호화(PBE)를 이용하면 비밀번호에서 유도한 키로 KEK를 암호화하여 저장하는 방식 등으로 KEK의 기밀성을 보호할 수 있다.

NoteBase

**오답 포인트**

③은 KEK가 CEK를 보호한다는 사실을 KEK가 콘텐츠를 직접 복호화한다는 의미로 바꾼 선지이다. KEK와 CEK의 보호 대상이 서로 다르다는 점을 구분해야 한다.

**다시 나오면 이렇게 판단**

어떤 키가 무엇을 암호화하는지 확인한다. 콘텐츠를 직접 암호화하면 CEK이고, CEK를 암호화하면 KEK이다. 복호화는 KEK로 CEK를 먼저 복원하고 그 CEK로 콘텐츠를 복원하는 순서로 판단한다.

**암기 포인트**

CEK는 콘텐츠를 잠그고, KEK는 CEK를 잠근다.

NoteBase

19. '개인정보의 안전성 확보 조치 기준' 고시에서 5만 명의 고유식별정보를 공공기관의 내부망에 저장할 경우, 해당 고유식별정보의 암호화 의무 여부를 결정하기 위해 필요한 조치에 해당하는 용어는?

① ISMS
② 취약점 점검
③ 침투 테스트
④ 개인정보 영향평가
⑤ 자산 평가

**정답 4번**

**쟁점**

이 문제는 공공기관이 내부망에 고유식별정보를 저장할 때 암호화의 적용 여부와 범위를 정하는 근거에 관한 문제이다. 핵심은 5만 명 이상의 고유식별정보를 처리하는 공공기관이 개인정보 영향평가 대상에 해당한다는 점이다.

**용어 풀이**

개인정보 영향평가는 개인정보파일을 운용하면서 생길 수 있는 개인정보 침해 위험요인을 분석하고 개선방안을 마련하는 평가이다.

**핵심 구분**

「개인정보의 안전성 확보조치 기준」 제7조 제3항 제2호는 내부망에 고유식별정보를 저장하는 경우 암호화를 원칙으로 하되, 주민등록번호 외의 고유식별정보는 정해진 기준에 따라 암호화의 적용 여부와 범위를 정할 수 있도록 한다. 개인정보 영향평가 대상 공공기관은 해당 영향평가 결과를 기준으로 삼는다. 또한 「개인정보 보호법 시행령」 제35조 제1호에 따르면 5만 명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 공공기관의 개인정보파일은 개인정보 영향평가 대상이다. 따라서 이 사안에서 필요한 조치는 개인정보 영향평가이다.

NoteBase

**선지별 해설**

① X
- ISMS는 정보보호 관리체계가 적절히 수립·운영되는지를 인증하는 제도이므로, 이 사안에서 암호화 적용 여부를 정하는 법정 평가가 아니다.
- 틀린 표현: ISMS
- 올바른 표현: 개인정보 영향평가

② X
- 취약점 점검은 시스템의 보안 취약점을 찾아내는 기술적 점검이므로, 영향평가 대상 공공기관의 암호화 적용 여부를 결정하는 조치가 아니다.
- 틀린 표현: 취약점 점검
- 올바른 표현: 개인정보 영향평가

③ X
- 침투 테스트는 실제 공격과 유사한 방식으로 시스템의 침투 가능성을 시험하는 보안 활동이므로, 고시가 정한 판단 근거가 아니다.
- 틀린 표현: 침투 테스트
- 올바른 표현: 개인정보 영향평가

④ O
- 5만 명 이상의 고유식별정보를 처리하는 공공기관은 개인정보 영향평가 대상이며, 내부망 저장 시 암호화의 적용 여부와 범위는 해당 개인정보 영향평가 결과에 따라 정할 수 있다.

⑤ X
- 자산 평가는 정보자산의 중요도나 가치를 산정하는 활동일 뿐, 이 사안에서 고시가 요구하는 암호화 판단 조치가 아니다.
- 틀린 표현: 자산 평가
- 올바른 표현: 개인정보 영향평가

**오답 포인트**

ISMS, 취약점 점검, 침투 테스트, 자산 평가는 모두 정보보호 분야의 활동이지만, 문제는 일반적인 보안 활동이 아니라 공공기관의 개인정보파일에 적용되는 고시상 판단 근거를 묻는다. 특히 '공공기관', '5만 명', '고유식별정보'가 개인정보 영향평가를 가리키는 핵심 표현이다.

NoteBase

**다시 나오면 이렇게 판단**

공공기관이 5만 명 이상의 민감정보 또는 고유식별정보를 처리한다는 조건이 보이면 먼저 개인정보 영향평가 대상을 떠올린다. 이어 내부망 암호화 여부를 묻는 경우에는 해당 개인정보 영향평가 결과가 판단 기준임을 연결한다.

**암기 포인트**

공공기관·5만 명·민감정보 또는 고유식별정보는 개인정보 영향평가로 연결한다.

NoteBase

**20. 「개인정보 보호법」 제38조 권리행사의 방법 및 절차에 대한 설명으로 옳지 않은 것은?**

① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지 등의 요구(이하 "열람등요구"라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.

② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 없다.

③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.

④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

**정답 2번**

### 쟁점

이 문제는 「개인정보 보호법」 제38조가 정한 열람등요구의 대리 행사, 만 14세 미만 아동의 법정대리인 권한, 비용 청구 및 이의제기 절차에 관한 문제이다. 핵심은 법정대리인이 아동의 권리를 행사할 수 있는지와 개인정보처리자가 마련하여야 하는 절차를 구별하는 것이다.

### 용어 풀이

열람등요구는 정보주체가 자신의 개인정보에 관하여 열람, 정정·삭제 또는 처리정지를 요구하는 권리 행사이다. 법정대리인은 법률에 따라 미성년자 등을 대신하여 권리를 행사하는 사람이다.

### 핵심 구분

「개인정보 보호법」 제38조에 따르면 정보주체는 정해진 방법과 절차에 따라 대리인을 통하여 열람등요구를 할 수 있다. 특히 만 14세 미만 아동의 법정대리인은 그 아동을 대신하여 개인정보처리자에게 열람등요구를 할 수 있다. 개인정보처리자는 대통령령에 따라 수수료와 사본 우송료를 청구할 수 있고, 요구 방법·절차의 공개와 거절 등 조치에 대한 이의제기 절차의 마련·안내 의무를 부담한다.

NoteBase

### 선지별 해설

① O
정보주체는 대통령령으로 정하는 방법과 절차에 따라 대리인에게 열람등요구를 하게 할 수 있다.

② X
만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보에 관한 열람등요구를 할 수 있으므로, '할 수 없다'가 틀렸다.
틀린 표현: 법정대리인은 열람등요구를 할 수 없다.
올바른 표현: 법정대리인은 그 아동의 개인정보에 관한 열람등요구를 할 수 있다.

③ O
개인정보처리자는 대통령령에 따라 열람등요구에 필요한 실비 범위의 수수료와 우송료를 청구할 수 있다.
우송료는 사본의 우송을 청구하는 경우에 한한다.

④ O
개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ O
개인정보처리자는 열람등요구의 거절 등 조치에 불복하는 정보주체가 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

### 오답 포인트

②의 '할 수 없다'는 만 14세 미만 아동이 직접 권리를 행사하기 어렵다는 점을 법정대리인도 행사할 수 없다는 뜻으로 바꾼 함정이다. 법은 오히려 법정대리인에게 그 아동의 열람등요구를 행사할 권한을 명시한다.

### 다시 나오면 이렇게 판단

제38조 문제에서는 먼저 권리 행사 주체를 확인한다. 정보주체는 대리인을 통하여 요구할 수 있고, 만 14세 미만 아동은 법정대리인이 대신 요구할 수 있다. 이어 비용 청구는 '할 수 있다', 방법·절차의 공개와 이의제기 절차의 마련·안내는 '하여야 한다'로 구분한다.

### 암기 포인트

14세 미만은 법정대리인이 요구할 수 있고, 처리자는 절차를 공개하며 이의제기 절차를 안내하여야 한다.

NoteBase