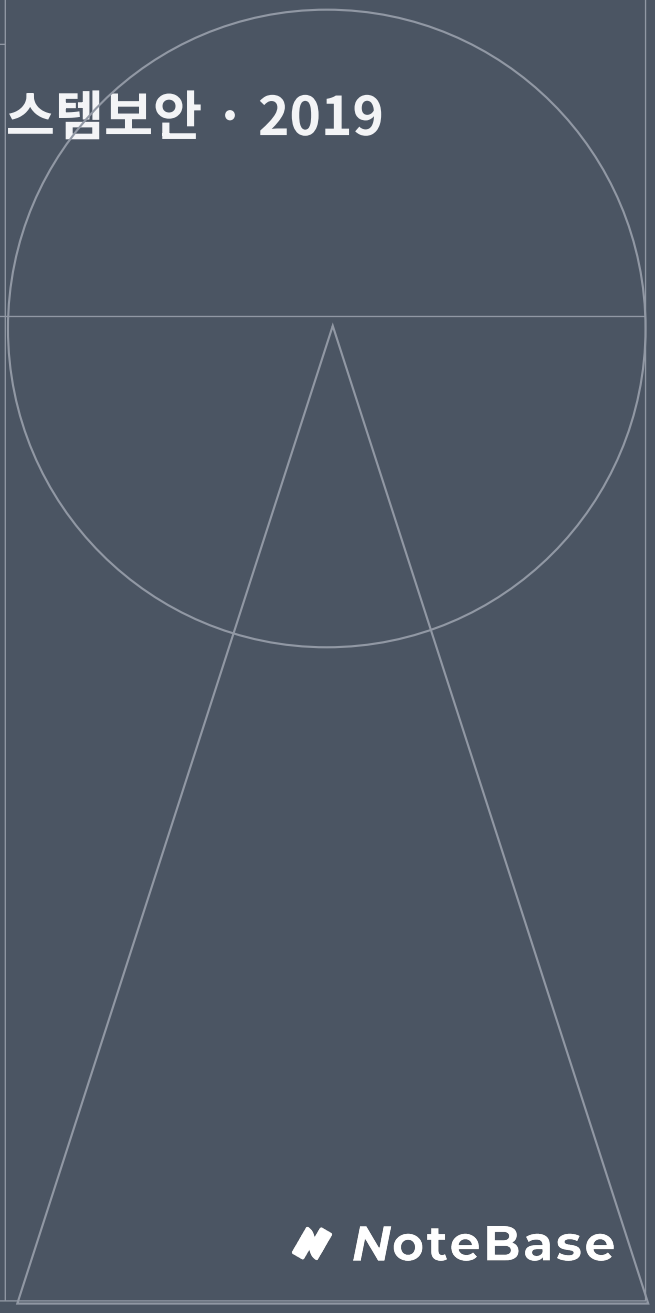
# 기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2019



NoteBase

# 기출OX 해설집

## 공무원/국가직/9급 · 정보시스템보안 · 2019

**공무원/국가직/9급 · 정보시스템보안 · 2019**

**문 1. 다음 중 HTTPS를 구성하기 위해 필요한 프로토콜만을 모두 고르면?**

ㄱ. TCP
ㄴ. SSL
ㄷ. SOAP
ㄹ. SET

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

**정답 1번**

**간단한 해설**

SSL 기반 HTTPS에서 **TCP**는 신뢰성 있는 데이터 전송을 담당하고, **SSL**은 HTTP 통신에 암호화와 무결성 보호 등의 보안 기능을 제공한다.

NoteBase

**보기별 해설**

ㄱ. TCP: SSL 기반 HTTPS에서 **신뢰성 있는 전송 통로**를 제공한다. TCP 연결 위에서 SSL이 동작하고, 그 위에서 HTTP 메시지를 주고받는다. TCP 자체가 HTTP 데이터를 암호화하는 것은 아니다.

ㄴ. SSL: HTTP와 TCP 사이에서 동작하며, **암호화·무결성 보호·상대 인증**을 위한 기능을 제공하는 보안 프로토콜이다. HTTP를 SSL 위에서 사용하는 것이 SSL 기반 HTTPS이며, SSL의 후속 프로토콜은 TLS이다.

ㄷ. SOAP: **XML 기반의 구조화된 메시지 교환**을 위한 프로토콜이다. HTTP 등을 통해 메시지를 전달할 수 있지만, HTTPS의 보안 계층을 구성하는 데 필요한 프로토콜은 아니다.

ㄹ. SET: 인터넷에서 **신용카드 결제를 보호**하기 위한 전자거래 보안 프로토콜이다. 결제 처리의 보안을 목적으로 하며, 일반적인 HTTP 통신을 HTTPS로 구성하는 데 필요한 프로토콜은 아니다.

필요한 프로토콜은 ㄱ의 TCP와 ㄴ의 SSL이며, 이는 ①의 조합에 해당한다.

NoteBase

**문 2. 웹에 관한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션의 취약점을 발표하는 기관은?**

① IETF Web Security Working Group
② Web Application Security Working Group
③ Open Web Application Security Project
④ World Wide Web Consortium

**정답 3번**

**간단한 해설**

웹 애플리케이션의 주요 보안 위험 열 가지를 정리한 **OWASP Top 10**은 OWASP가 발표하는 자료이다. 선지의 Open Web Application Security Project가 OWASP를 가리킨다.

**공통 해설**

OWASP는 웹 애플리케이션의 보안을 높이기 위해 취약점 정보와 보안 지침·도구를 공개하고 공유하는 개방형 보안 프로젝트이다. 문항에 제시된 영문 명칭은 Open Web Application Security Project이다.

대표 자료인 **OWASP Top 10**은 웹 애플리케이션에서 중요하게 다루어야 할 보안 위험 열 가지를 선정하여 설명한다. 개발자와 조직이 주요 취약점의 원인과 영향을 이해하고 예방하도록 돕는 자료이므로, 문항의 '10대 웹 애플리케이션의 취약점을 발표'한다는 설명은 OWASP의 활동에 해당한다. 여기서 열 가지는 개별 웹 애플리케이션의 수가 아니라 주요 보안 위험의 유형을 뜻한다.

NoteBase

**문 3. 다음 중 데이터 기밀성을 보장할 수 있는 프로토콜은?**

① IP

② UDP

③ Telnet

④ SSH

**정답 4번**

**간단한 해설**

SSH는 **통신 내용을 암호화**하여 전송하므로, 제3자가 데이터를 가로채더라도 내용을 알아보기 어렵게 하여 기밀성을 보호한다.

**공통 해설**

기밀성은 허가받지 않은 사람이 정보의 내용을 알 수 없도록 보호하는 성질이다. 전송 중인 데이터의 기밀성을 보호하려면, 데이터를 가로채도 원래 내용을 알아볼 수 없게 하는 **암호화**가 필요하다.

SSH는 원격 접속에 사용하는 프로토콜로, 암호화된 통신 채널을 통해 로그인 정보와 명령, 실행 결과 등을 전송한다. 따라서 전송 내용을 엿보는 도청으로부터 데이터를 보호할 수 있다. IP·UDP·Telnet은 **프로토콜 자체에 데이터 암호화 기능이 없으므로**, 이들만 사용해서는 전송 데이터의 기밀성을 보장할 수 없다.

NoteBase

**문 4. 이메일 등을 통해 진짜 사이트와 거의 동일하게 꾸민 가짜 사이트로 접속을 유도하여 개인정보를 탈취하는 공격 기법은?**

① 피싱(Phishing)

② 이블 트윈 어택(Evil Twin Attack)

③ 언팩킹(Unpacking)

④ 사이버 폭력(Cyberbullying)

**정답 1번**

**간단한 해설**

정상 사이트를 사칭한 **가짜 사이트로 유인해 개인정보를 입력하게 만드는 것**이 피싱의 핵심 수법이다.

**공통 해설**

피싱(Phishing)은 신뢰할 수 있는 기관이나 서비스를 사칭하여 사용자가 개인정보를 제공하도록 속이는 공격이다. 문항에서는 이메일 등으로 접속을 유도하고 진짜 사이트와 거의 같은 화면을 보여 주어, 사용자가 **가짜 사이트를 정상 사이트로 믿게 한다**. 사용자가 그곳에 아이디·비밀번호 등의 개인정보를 입력하면 공격자가 이를 수집할 수 있으므로, 이러한 개인정보 탈취 방식은 피싱에 해당한다.

NoteBase

**문 5. 다음은 전자우편의 암호화에 대한 설명이다. 괄호 안에 들어갈 용어는?**

( )은/는 IDEA 알고리즘과 RSA 알고리즘을 조합하여 만들었다. IDEA 알고리즘은 세션키 암호화, RSA 알고리즘은 사용자 인증을 위한 전자서명에 이용하였다. 이것의 장점으로는 구현이 쉽고, 특정 기관으로부터 인증서를 발급받지 않아도 된다는 것이다.

① PGP

② PEM

③ S/MIME

④ IMAP

**정답 1번**

**간단한 해설**

초기 PGP는 **IDEA를 이용한 대칭키 암호화와 RSA 전자서명**을 결합하였다. 공개키의 신뢰성을 사용자들이 확인하는 방식을 사용하므로 **특정 인증기관의 인증서가 필수는 아니다**.

**공통 해설**

PGP(Pretty Good Privacy)는 전자우편의 내용을 암호화하고 전자서명으로 발신자를 확인할 수 있게 하는 보안 방식이다. 지문은 IDEA와 RSA를 결합한 초기 PGP를 설명한다. IDEA는 메시지마다 사용하는 대칭키인 세션키로 메일 내용을 암호화하며, RSA는 발신자의 개인키로 메시지의 해시값에 전자서명을 생성하는 데 사용된다. 수신자는 발신자의 공개키로 서명을 검증하여 발신자와 내용의 변조 여부를 확인한다. 즉, **내용을 숨기는 암호화와 발신자를 확인하는 전자서명**의 역할을 나누어 결합한다.

PGP에서는 공개키의 실제 소유자를 직접 확인하거나 신뢰하는 다른 사용자의 공개키 서명을 활용하는 신뢰망(Web of Trust)을 구성할 수 있다. 따라서 **특정 인증기관에서 인증서를 발급받아야만 사용할 수 있는 것은 아니다**. 다만 인증기관의 인증서가 필수가 아니라는 것이 공개키 소유자 확인도 불필요하다는 뜻은 아니다. 이러한 암호화·전자서명과 공개키 신뢰 방식의 결합이 지문의 PGP에 해당한다.

NoteBase

**문 6. 다음 프로토콜 중 계층이 다른 것은?**

① ICMP

② POP3

③ TFTP

④ SNMP

**정답 1번**

**간단한 해설**

ICMP는 IP 통신의 오류를 보고하고 통신 상태를 진단하는 **네트워크 계층** 프로토콜이다. 전자우편 수신·파일 전송·장비 관리처럼 특정 응용 서비스를 제공하는 프로토콜과 계층이 다르다.

**선지별 해설**

① ICMP: **네트워크 계층** 프로토콜로, TCP/IP 모형에서는 인터넷 계층에 속한다. 목적지 도달 불가나 수명 초과와 같은 IP 패킷 처리상의 문제를 알리고, 에코 요청·응답으로 통신 상태를 진단하는 데 쓰인다.

② POP3: 메일 서버에 저장된 전자우편을 클라이언트가 가져오는 **응용 계층** 프로토콜이다. IP 패킷 처리 자체가 아니라 전자우편 수신이라는 서비스를 제공한다.

③ TFTP: 간단한 파일 전송 기능을 제공하는 **응용 계층** 프로토콜이다. UDP를 이용하지만, UDP 위에서 파일 전송 서비스를 제공하므로 전송 계층 프로토콜로 분류하지 않는다.

④ SNMP: 네트워크 장비의 관리 정보를 조회하거나 설정하는 **응용 계층** 프로토콜이다. 관리 대상이 네트워크 장비라는 이유로 네트워크 계층에 속하는 것은 아니다.

계층을 비교하면 ② POP3·③ TFTP·④ SNMP는 응용 계층이고, ① ICMP는 네트워크 계층이므로 ICMP의 계층이 나머지와 다르다.

NoteBase

**문 7. 다음 중 유닉스 운영체제에서 네트워크 연결에 대한 접근제어 도구는?**

① APT

② DDL

③ UTMP

④ TCPWrapper

**정답 4번**

**간단한 해설**

TCPWrapper는 접속을 요청한 **호스트와 서비스에 따라 연결을 허용하거나 거부**하는 접근제어 도구이다.

**공통 해설**

TCPWrapper는 유닉스 계열 시스템에서 클라이언트의 IP 주소나 호스트 이름을 기준으로 **네트워크 서비스에 대한 접근을 허용하거나 거부**하는 도구이다. 이 기능을 지원하는 서비스는 /etc/hosts.allow와 /etc/hosts.deny에 설정된 규칙에 따라 연결 가능 여부를 판단한다. 예를 들어 특정 호스트의 특정 서비스 접속을 거부하도록 규칙을 설정하면, 해당 호스트에서 그 서비스로 들어오는 연결을 차단할 수 있다.

NoteBase

**문 8. 웹서비스를 대상으로 하는 다양한 코드 인젝션(Code Injection) 혹은 운영체제 명령어 인젝션(OS Command Injection) 공격 등으로부터 취약점을 갖는 PHP 함수가 아닌 것은?**

① cmd
② system
③ eval
④ exec

**정답 1번**

**간단한 해설**

cmd는 **PHP의 내장 함수가 아니다**. 따라서 문제에서 묻는 PHP의 코드·명령어 실행 기능에 해당하지 않는다.

**공통 해설**

코드·명령어 인젝션은 외부 입력이 단순한 데이터로 처리되지 않고 **실행할 코드나 명령어의 일부로 해석**될 때 발생한다. 이 문제는 각 이름이 PHP에서 그러한 실행 기능을 제공하는지로 구분한다.

system()과 exec()는 전달된 운영체제 명령어를 실행하고, eval()은 전달된 문자열을 PHP 코드로 실행한다. 따라서 공격자가 조작한 입력을 적절한 검증이나 보호 처리 없이 실행 내용에 반영하면, 앞의 두 함수는 운영체제 명령어 인젝션으로, eval()은 코드 인젝션으로 이어질 수 있다. eval은 엄밀히는 함수가 아니라 PHP의 언어 구성 요소이지만, 이 문항에서는 코드 실행 기능을 함께 묻고 있다.

cmd는 **PHP가 제공하는 내장 실행 함수가 아니다**. 따라서 나머지 후보처럼 PHP의 코드·명령어 실행 기능으로 분류할 수 없다. 이는 system(), exec(), eval()을 사용하면 언제나 취약하다는 뜻이 아니라, 신뢰할 수 없는 입력이 실행 내용을 바꿀 수 있는지가 위험을 가르는 조건이라는 뜻이다.

NoteBase

**문 9. 관리자는 자신이 소유하고 있는 특정 자원에 대한 자신의 권한을 다른 사람에게 위임할 수 있다. 이를 통해 사용자들에게 주어진 권한 이외에 모든 권한을 차단할 수 있는 접근 제어 모델은?**

① 강제적 접근 제어(Mandatory Access Control)

② 임의 접근 제어(Discretionary Access Control)

③ 역할 기반 접근 제어(Role Based Access Control)

④ 속성 기반 접근 제어(Attribute Based Access Control)

**정답 2번**

**간단한 해설**

자원 소유자가 자신의 자원에 대한 접근 권한을 정하고 다른 사용자에게 부여할 수 있다는 점이 **임의 접근 제어(DAC)**의 특징이다. 허용되지 않은 접근을 차단한다는 사실보다 **소유자의 재량에 따른 권한 부여**가 모델을 구별하는 단서이다.

**공통 해설**

임의 접근 제어(DAC)는 **자원 소유자의 재량**에 따라 누가 해당 자원에 어떤 작업을 할 수 있는지 정하는 접근 제어 방식이다. 소유자는 자신에게 허용된 권한과 정책의 범위 안에서 다른 사용자에게 접근 권한을 부여할 수 있다. 문제에서 관리자가 '자신이 소유하고 있는 특정 자원'에 대한 권한을 다른 사람에게 위임한다는 설명이 이 정의에 해당한다.

예를 들어 파일 소유자 A가 사용자 B에게 읽기 권한만 부여하면 B의 읽기는 허용되지만, 별도로 쓰기 권한을 받지 않은 B의 수정 요청은 거부된다. 이처럼 소유자가 부여한 권한을 기준으로 접근을 허용하고 그 밖의 접근을 차단한다. 여기서 '임의'는 누구나 마음대로 접근한다는 뜻이 아니라 **권한 부여를 소유자의 재량으로 결정한다**는 뜻이다.

NoteBase

**문 10. 버퍼 오버플로우 공격 탐지 기법 중 스택 가드(Stack Guard)에 사용하는 기술은?**

① Full Canary

② Buffer Canary

③ Stack Canary

④ Random Canary

**정답 4번**

**간단한 해설**

스택 가드의 Random Canary는 **예측하기 어려운 난수를 카나리 값으로 사용**하여 공격자가 같은 값으로 덮어쓰는 것을 어렵게 한다. 공식 채점 답은 Random Canary이지만, 발문에 난수 조건이 없어 포괄 명칭인 Stack Canary와 범위가 겹친다.

**공통 해설**

StackGuard의 카나리 보호 방식은 스택의 버퍼와 저장된 복귀 주소 사이에 검사값을 두고, 함수가 반환되기 전에 그 값이 유지되는지 확인한다. 버퍼를 넘어 복귀 주소까지 연속해서 덮어쓰는 과정에서 카나리 값이 바뀌면 프로그램을 종료하여 변조된 주소로 복귀하는 것을 막는다.

Random Canary는 프로그램 시작 시 난수로 정한 값을 카나리로 사용하는 방식이다. 공격자가 카나리 값을 알면 같은 값을 써 넣어 검사를 피할 수 있으므로, **값을 미리 예측하기 어렵게 하는 것**이 중요하다. 다만 값이 유출되면 이 보호를 우회할 수 있어 모든 버퍼 오버플로우를 막는다는 뜻은 아니다.

Stack Canary는 스택에 배치하는 카나리의 포괄적인 명칭이며, Random Canary는 그 값을 정하는 구체적인 방식이다. 따라서 두 용어는 배타적인 관계가 아니다. StackGuard에는 문자열 종료 문자 등을 활용하는 Terminator Canary도 있어 **StackGuard가 반드시 난수 방식만 사용하는 것은 아니다**. ① Full Canary와 ② Buffer Canary는 이러한 난수 기반 방식을 나타내는 명칭이 아니다.

공식 채점 답은 ④ Random Canary이다. 다만 원문은 난수 사용을 조건으로 제시하지 않았으므로, StackGuard의 보호 기법을 포괄적으로 가리키는 ③ Stack Canary를 기술적으로 무관한 용어라고 배제하기는 어렵다. 공식 채점은 난수 기반의 구체적인 방식을 선택한 것으로 이해되며, 발문만으로 ③과 ④를 엄밀하게 구별하는 데에는 한계가 있다.

NoteBase

**문 11. 다음 설명에 해당하는 정보보안 제품 평가는?**

◯ IT 제품의 보안성을 평가하기 위한 국제 표준
◯ 여러 과정과 기준을 통해 각 시스템은 EAL로 보안 수준을 평가
◯ 크게 3부분으로 구성되며, 제1부는 정보시스템의 보안 목적 및 요구 사항, 제2부는 보안 기능 요구 사항, 제3부는 보안 보증 요구 사항으로 구성

① TCSEC
② ITSEC
③ CC
④ ISO/IEC27001

**정답 3번**

**간단한 해설**

IT 제품의 보안 기능과 그 기능을 신뢰할 수 있는 정도를 함께 평가하고, **EAL(평가보증등급)**을 사용하는 기준은 **CC(공통평가기준)**이다. 지문의 보안 기능 요구 사항과 보안 보증 요구 사항 구분도 CC의 특징이다.

**공통 해설**

CC(Common Criteria, 공통평가기준)는 IT 제품의 보안성을 공통된 기준으로 평가하기 위한 국제 표준이다. 제품이 어떤 보안 기능을 제공해야 하는지를 정하는 '보안 기능 요구 사항'과, 그 기능이 요구대로 구현되었다고 얼마나 신뢰할 수 있는지를 확인하는 '보안 보증 요구 사항'을 구분한다.

지문에 제시된 CC의 3부 구성에서 제1부는 보안 목적과 요구 사항을 표현하는 데 필요한 개요와 일반 모형을, 제2부는 보안 기능 요구 사항을, 제3부는 보안 보증 요구 사항을 다룬다. 이처럼 **보안 기능과 보증을 구분하는 구성**이 제시된 설명을 CC에 대응시키는 근거이다.

EAL(Evaluation Assurance Level)은 CC의 보증 요구 사항을 묶어 정한 **평가보증등급**으로, EAL1부터 EAL7까지 있다. 높은 등급일수록 평가의 엄격성·범위·깊이 등에 관한 요구가 높아진다. 따라서 지문의 'EAL로 보안 수준을 평가'한다는 설명은 보안 기능을 얼마나 엄격하게 검증하여 신뢰를 확보했는지를 나타내는 것으로 이해한다.

NoteBase

**문 12. 유닉스 파일 및 디렉토리 권한 변경 명령어와 그 기능을 연결한 것으로 옳지 않은 것은?**

① chmod - 파일 및 디렉토리의 권한 변경

② chown - 파일 및 디렉토리의 소유자와 소유그룹 변경

③ chgrp - 파일 및 디렉토리의 소유그룹 변경

④ chmask - 파일 및 디렉토리 생성 시 부여되는 기본 권한 변경

**정답 4번**

**간단한 해설**

④에 제시된 기능에 해당하는 명령은 chmask가 아니라 **umask**이다. umask는 새 파일이나 디렉토리를 만들 때 부여하지 않을 권한을 마스크로 지정한다.

**선지별 해설**

① O: chmod는 파일과 디렉토리의 **읽기·쓰기·실행 권한**을 변경한다. 소유자, 소유그룹, 그 밖의 사용자에게 허용할 접근 권한을 설정하는 명령이다.

② O: chown은 파일과 디렉토리의 **소유자와 소유그룹**을 변경할 수 있다. 소유자만 지정하면 소유자를 바꾸고, '소유자:그룹' 형식으로 지정하면 두 항목을 함께 바꿀 수 있다.

③ O: chgrp는 파일과 디렉토리의 **소유그룹**을 변경한다. 소유자 자체를 바꾸는 것이 아니라 해당 파일이나 디렉토리가 속한 그룹을 바꾸는 명령이다.

④ X: 생성 시 기본 권한에 영향을 주는 명령은 chmask가 아니라 **umask**이다. umask는 생성 프로그램이 요청한 권한에서 마스크로 지정한 권한을 제외하도록 한다. chmod가 이미 존재하는 파일이나 디렉토리의 권한을 바꾸는 데 비해, umask는 이후 새로 생성되는 파일이나 디렉토리의 권한에 영향을 준다.

NoteBase

**문 13. OSI 각 계층 중 데이터 링크 계층에서 동작하는 프로토콜에 해당하지 않는 것은?**

① L2F

② L2TP

③ PPTP

④ IPSec

**정답 4번**

**간단한 해설**

IPSec은 IP 패킷에 보안 기능을 제공하는 **네트워크 계층(3계층)** 프로토콜이다. 데이터 링크 계층(2계층)의 프레임을 터널링하는 프로토콜과 구별된다.

**공통 해설**

이 문항의 구분 기준은 **링크 계층의 프레임을 전달하는가, IP 계층에서 보안을 제공하는가**이다. OSI 모형에서 데이터 링크 계층은 2계층이고, IP가 속하는 네트워크 계층은 3계층이다. 터널링은 원래의 데이터를 다른 프로토콜의 데이터 안에 넣어 운반하는 방식이다.

L2F·L2TP·PPTP는 PPP 등의 링크 계층 데이터를 캡슐화하여 터널로 전달하므로 2계층 터널링 프로토콜로 분류한다. 외부 운반에 IP 네트워크를 이용하더라도, 터널이 전달하는 대상이 **링크 계층 데이터**라는 점이 분류의 기준이다.

IPSec은 링크 계층 프레임을 전달하는 방식이 아니라 **IP 계층에서 패킷을 보호**하는 보안 프로토콜 모음이다. 따라서 데이터 링크 계층에 해당하지 않는 것은 IPSec이며, 그 동작 계층은 네트워크 계층이다.

NoteBase

**문 14. SMTP에 대한 설명으로 옳지 않은 것은?**

① SMTP는 실행 파일이나 2진 데이터를 텍스트 형태로 변환하여 전송한다.

② 송·수신 측이 직접 상대방을 상호 인증하는 방식을 통해 메시지를 전송한다.

③ SMTP 서버는 특정 크기 이상의 메일 메시지를 처리하지 못하고 거부한다.

④ 주로 TCP 포트 25번을 사용한다.

**정답 2번**

**간단한 해설**

SMTP는 **송신자와 수신자의 직접 상호 인증을 기본 전송 조건으로 요구하지 않는다**. 메일은 서버를 통해 전달되며, 인증이 필요하면 SMTP AUTH 같은 별도 확장을 이용한다.

**선지별 해설**

① O: 기본 SMTP는 7비트 텍스트 전송을 전제로 하므로, 실행 파일이나 2진 데이터는 MIME의 Base64 같은 방식으로 텍스트 형태로 인코딩하여 보낸다. 여기서 **데이터 변환은 MIME 인코딩의 역할**이고, SMTP는 그렇게 구성된 메일을 전송한다.

② X: SMTP는 메일을 전송·중계하는 프로토콜이며, **송신자와 수신자가 직접 서로를 인증하는 절차를 기본적으로 요구하지 않는다**. 송신 측 메일 서버에서 수신 측 메일 서버로 전달하거나 중계 서버를 거칠 수 있다. SMTP AUTH를 이용한 클라이언트와 서버 사이의 인증은 별도 확장 기능이며, 최종 송신자와 수신자의 직접 상호 인증과 구별된다.

③ O: SMTP 서버에 **최대 메시지 크기 제한이 설정되어 있으면** 그 상한을 초과하는 메일은 거부된다. SIZE 확장을 지원하는 서버는 수용 가능한 최대 크기를 미리 알릴 수도 있다. 이는 모든 SMTP 서버에 동일한 고정 한도가 있다는 뜻이 아니라, 각 서버의 설정과 자원에 따라 제한된다는 뜻이다.

④ O: SMTP는 TCP를 이용하며, **메일 서버 사이의 전송에는 통상 25번 포트**를 사용한다. 따라서 SMTP의 대표적인 포트 번호를 TCP 25번으로 설명한다.

NoteBase

**문 15. 윈도우즈 시스템 보안 아키텍처(Security Architecture)에 대한 설명으로 옳지 않은 것은?**

① SRM(Security Reference Monitor)은 로컬 컴퓨터상에서 보안을 제어함으로써, 특권 컴포넌트들과 사용자 모드에서 동작하는 서브시스템에 보안 서비스를 제공한다.

② LSA(Local Security Authority)는 사용자 모드 프로세스에서 동작하며 윈도우즈에서 로컬 보안 정책을 집행한다.

③ SAM(Security Account Manager)은 윈도우즈 운영체제에서 로컬 주체 및 그룹에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스로 보안 토큰 발급과 저장 등을 수행한다.

④ AD(Active Directory) 서비스는 네트워크의 모든 정보를 디렉토리에 저장해 네트워크 자원을 손쉽게 찾고 접근하는 서비스를 제공한다.

**정답 3번**

**간단한 해설**

SAM은 **로컬 사용자·그룹의 계정 정보를 저장하는 데이터베이스**이며, 보안 토큰을 발급·저장하는 역할을 하지 않는다. 접근 토큰은 인증 성공 후 운영체제가 생성하여 프로세스나 스레드의 사용자 신원과 권한을 나타내는 데 사용한다.

**선지별 해설**

① O: SRM은 커널 모드에서 동작하며 로컬 컴퓨터의 자원에 대한 **접근 권한을 검사**한다. 프로세스나 스레드의 접근 토큰에 담긴 신원·권한과 대상 객체의 접근 제어 정보를 확인하여 요청한 작업을 허용할지 판단한다. 이러한 기능으로 특권 컴포넌트와 사용자 모드 서브시스템에 보안 서비스를 제공한다.

② O: LSA는 **사용자 모드의 보호된 시스템 프로세스**인 LSASS를 통해 동작하며, 사용자 인증과 로컬 보안 정책 집행을 담당한다. 로컬 계정으로 로그온할 때는 SAM의 계정 정보를 이용하여 사용자를 인증한다. 커널 모드에서 자원 접근을 검사하는 SRM과 동작 위치 및 주된 역할이 다르다.

③ X: SAM은 로컬 사용자와 그룹의 계정 정보 및 인증에 필요한 정보를 저장하는 데이터베이스이다. **보안 토큰의 발급·저장은 SAM의 기능이 아니다.** 접근 토큰은 인증 성공 후 LSA를 중심으로 한 로그온 처리 과정에서 생성되며, 사용자와 소속 그룹의 보안 식별자(SID), 특권 등을 담아 프로세스나 스레드의 보안 문맥을 나타낸다. 계정 정보를 보관하는 SAM과 실행 중 자원 접근 판단에 쓰이는 접근 토큰을 구분해야 한다.

④ O: AD는 사용자, 컴퓨터, 그룹, 프린터 등 **네트워크 객체의 정보를 디렉터리에 체계적으로 저장**하는 서비스이다. 사용자와 관리자가 이 정보를 검색하여 필요한 자원을 찾을 수 있게 하며, 인증과 접근 제어를 통해 권한이 있는 사용자가 자원에 접근하도록 지원한다.

NoteBase

**문 16. ITU-T 권고안에서 정하고 있는 인증서 표준 규격은?**

① RFC 822

② X.509

③ X.501

④ X.25

**정답 2번**

**간단한 해설**

X.509는 ITU-T가 정한 **공개키 인증서의 표준 규격**이다.

**공통 해설**

X.509는 ITU-T 권고안으로, 공개키 인증서의 형식과 인증서 검증 체계 등을 규정한다. 공개키 인증서는 **특정 주체와 그 공개키의 연결**을 증명하는 전자 문서이다. 인증서에는 주체, 공개키, 발급자, 유효기간 등의 정보와 발급자의 전자서명이 포함되며, 발급자는 이 서명을 통해 인증서 정보와 주체·공개키의 연결을 보증한다. 따라서 문항에서 묻는 인증서 표준 규격에 해당하는 명칭은 X.509이다.

NoteBase

**문 17. 다음 중 국내의 정보보호 및 개인정보보호 관리체계 인증제도에 해당하는 것은?**

① P-ISMS

② ISMS-P

③ PDCA-K

④ ISMS-K

**정답 2번**

**간단한 해설**

ISMS의 정보보호 범위에 **개인정보보호(P)**를 함께 포함한 관리체계 인증이 ISMS-P이다.

**공통 해설**

정보보호 및 개인정보보호 관리체계 인증은 조직이 수립·운영하는 정보보호·개인정보보호 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도이다. 정보보호 관리체계 인증인 ISMS와 달리, **개인정보보호까지 함께 포함한** 관리체계 인증의 공식 명칭은 ISMS-P이다. P-ISMS, PDCA-K, ISMS-K는 이 제도의 공식 명칭에 해당하지 않는다.

NoteBase

**문 18. 윈도우즈 파일 시스템에 대한 설명으로 옳지 않은 것은?**

① FAT16의 저장 가능 용량은 최대 2GB까지만 지원한다.

② FAT32 테이블의 기본 크기는 32비트이다.

③ NTFS는 윈도우 NT 버전에서 지원한다.

④ FAT32는 개별 폴더와 파일에 접근 제어를 설정할 수 있다.

**정답 4번**

**간단한 해설**

FAT32는 **개별 파일·폴더에 사용자별 접근 권한을 설정하는 기능을 지원하지 않는다**. 읽기·쓰기 등의 권한을 접근 제어 목록(ACL)으로 관리하는 것은 NTFS의 기능이다.

**선지별 해설**

① O: FAT16의 최대 볼륨 크기는 일반적으로 **2GB**로 설명한다. 이는 MS-DOS 등에서 사용하는 FAT16의 한계에 해당한다. 다만 Windows NT에서는 64KB 클러스터를 사용하여 최대 4GB 볼륨도 지원하므로, '모든 운영체제에서 반드시 2GB까지만 가능하다'는 뜻으로 일반화해서는 안 된다.

② O: FAT32는 파일 할당 테이블의 **각 항목을 32비트**로 저장한다. 파일 할당 테이블은 파일이 차지하는 클러스터의 연결 관계 등을 기록한다. 선지의 32비트는 테이블 전체의 크기가 아니라 항목 하나의 기본 크기를 뜻한다.

③ O: NTFS는 **Windows NT 계열에서 지원하는 파일 시스템**이다. Windows NT의 보안 모델을 지원하며, 파일과 폴더에 대한 권한을 관리할 수 있다.

④ X: FAT32 자체에는 개별 파일·폴더의 사용자별 접근 권한을 저장하고 관리하는 기능이 없다. 이 설명의 'FAT32'를 **NTFS**로 고쳐야 한다. NTFS는 접근 제어 목록(ACL)을 이용하여 사용자나 그룹에 읽기·쓰기 등의 권한을 부여하거나 거부한다. 예를 들어 같은 파일에 대해 A에게는 읽기만 허용하고 B에게는 수정을 허용할 수 있다.

NoteBase

**문 19. SSL 레코드 프로토콜의 처리과정 기법에 해당하지 않는 것은?**

① 압축(Compression)

② 메시지 인증 코드(Message Authentication Code)

③ 정규화(Normalization)

④ 단편화(Fragmentation)

**정답 3번**

**간단한 해설**

SSL 레코드 프로토콜은 데이터를 단편화하고, 필요에 따라 압축한 뒤 메시지 인증 코드(MAC)를 붙이고 암호화한다. **정규화는 이 처리과정에 포함되지 않는다.**

**공통 해설**

SSL 레코드 프로토콜은 상위 계층에서 받은 데이터를 전송 가능한 레코드로 만들고 보호하는 규칙이다. 송신할 때 데이터를 작은 블록으로 나누는 단편화를 수행하고, 협상된 방식에 따라 선택적으로 압축한다. 이어서 비밀키를 사용하는 메시지 인증 코드(MAC)를 계산해 붙이고 암호화하여 전송한다. MAC는 수신 측에서 데이터의 변조 여부와 메시지의 인증을 확인하는 데 쓰이며, 암호화는 데이터 내용을 보호한다.

따라서 압축·메시지 인증 코드·단편화는 모두 SSL 레코드 처리에 해당한다. 압축 방식으로 무압축이 선택될 수 있어도 압축은 프로토콜이 정의한 처리에 속한다. **정규화(Normalization)는 이 레코드 처리에 포함되지 않는다.**

NoteBase

**문 20. 다음 설명에 해당하는 블루투스 공격 방식은?**

블루투스 공격 장치를 검색하는 활동을 의미한다. 공격자는 블루투스의 서비스 발견 프로토콜(SDP)을 이용해 공격이 가능한 블루투스 장치의 종류(예, 전화 통화, 키보드 입력, 마우스 입력 등)를 검색하고 모델을 확인할 수 있다.

① 블루스나프(Bluesnarf)

② 블루버그(Bluebug)

③ 블루프린팅(Blueprinting)

④ 블루재킹(Bluejacking)

**정답 3번**

**간단한 해설**

SDP로 제공 서비스를 조사하여 블루투스 장치의 종류와 모델을 식별하는 기법은 **블루프린팅(Blueprinting)**이다. 핵심은 공격 대상 장치의 특징을 알아내는 정보 수집에 있다.

**공통 해설**

블루프린팅은 블루투스 장치가 외부에 드러내는 특징을 분석하여 장치의 종류나 모델 등을 알아내는 식별 기법이다. SDP(서비스 발견 프로토콜)는 다른 블루투스 장치가 어떤 서비스를 제공하는지 조회하는 데 쓰인다. 이때 얻은 서비스 기록의 구성과 속성을 장치의 특징으로 활용하면 모델을 구별하는 단서가 된다.

지문에서는 전화 통화·키보드 입력·마우스 입력 등의 서비스를 검색하고 모델을 확인한다. 이는 **제공 서비스 정보를 이용한 장치 식별**이므로 블루프린팅에 해당한다. 이렇게 수집한 정보는 공격 가능한 장치를 찾는 데 활용될 수 있다.

NoteBase