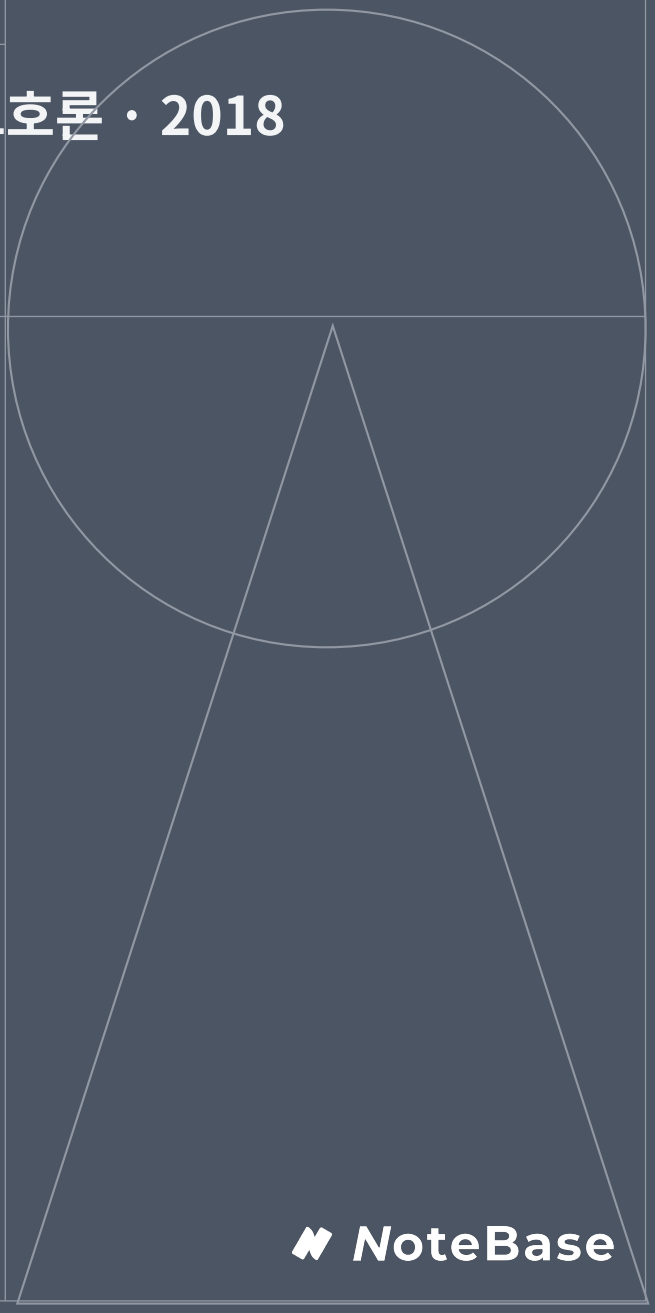
기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2018



NoteBase

기출OX 해설집

공무원/국가직/7급 · 정보보호론 · 2018

공무원/국가직/7급 · 정보보호론 · 2018

문 1. 공개키 인증서의 구조를 정의한 ITU-T 권고안은?

① X.25

② X.121

③ X.400

④ X.509

정답 4번

출제 포인트

이 문제는 ITU-T X 시리즈 권고안 가운데 공개키 인증서의 구조를 정의한 표준을 구별하는 문제이다.

핵심 개념

X.509는 공개키 기반구조에서 디지털 인증서의 형식과 인증 경로 검증 체계를 정의한 권고안이다.
X.25는 패킷교환 공중데이터망 접속을 위한 인터페이스 권고안이다.
X.121은 공중데이터망의 번호체계를 정의한 주소 지정 권고안이다.
X.400은 전자우편 중심의 메시지 처리 시스템 권고안이다.

선지별 해설

① X: X.25는 패킷교환 데이터 통신망 인터페이스에 관한 권고안이므로 인증서 구조와 무관하다. 틀린 표현은 "공개키 인증서의 구조"에 X.25를 대응시킨 부분이며, 올바르게는 "X.25는 패킷교환망 인터페이스"이다.
② X: X.121은 공중데이터망 번호체계를 정의하므로 인증서 형식을 다루지 않는다. 틀린 표현은 X.121을 인증서 표준으로 본 부분이며, 올바르게는 "X.121은 데이터망 번호체계"이다.
③ X: X.400은 메시지 처리 시스템과 전자우편 서비스 구조에 관한 권고안이다. 틀린 표현은 X.400을 인증서 구조 표준으로 본 부분이며, 올바르게는 "X.400은 메시지 처리 시스템 표준"이다.
④ O: X.509는 공개키 인증서의 구조와 인증서 검증 체계를 정의한 ITU-T 권고안이므로 옳다.

오답 포인트

X 시리즈 번호가 모두 비슷하게 보여 숫자만 보고 고르기 쉽다는 점이 함정이다. 특히 X.400은 보안 관련 문맥에서 함께 언급되기도 해 인증서 표준으로 혼동하기 쉽지만, 실제 인증서 형식은 X.509가 담당한다.

NoteBase

다시 나오면 이렇게 판단

보안 인증서, 공개키 인증서, 디지털 인증서 형식이라는 표현이 나오면 먼저 X.509를 떠올리면 된다. 번호가 비슷한 다른 X 시리즈는 네트워크 접속, 번호체계, 메시지 처리처럼 각자 담당 영역이 다르다는 기준으로 걸러낼 수 있다.

암기 포인트

X.509는 인증서, X.400은 메일, X.121은 번호, X.25는 패킷망이다.

NoteBase

문 2. ㉠, ㉡에 들어갈 정보보안 위험의 처리 방식을 바르게 연결한 것은?

(㉠)은(는) 사업 목적상 위험을 처리하는 데 들어가는 과도한 비용 또는 시간 때문에 일정 수준의 위험을 받아들이는 것으로, 그 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.
(㉡)은(는) 위험에 대한 책임을 제3자와 공유하는 것으로, 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

① ㉠: 위험 회피, ㉡: 위험 전가
② ㉠: 위험 회피, ㉡: 위험 감소
③ ㉠: 위험 수용, ㉡: 위험 전가
④ ㉠: 위험 수용, ㉡: 위험 감소

정답 3번

출제 포인트

이 문제는 정보보안 위험 처리 방식인 위험 수용, 위험 전가, 위험 회피, 위험 감소의 정의를 구분하는 문제이다.

핵심 개념

위험 수용: 위험을 없애는 비용이나 시간이 과도할 때 일정 수준의 위험을 감수하고 그 결과 책임을 조직이 부담하는 방식이다.
위험 전가: 보험, 외주, 계약 등으로 손실 부담이나 책임의 전부 또는 일부를 제3자에게 이전하는 방식이다.
위험 회피: 위험을 일으키는 업무나 활동 자체를 중단하거나 아예 수행하지 않는 방식이다.
위험 감소: 통제수단을 적용해 위험의 발생 가능성이나 영향을 낮추는 방식이다.

선지별 해설

① X: ㉠을 위험 회피라고 본 부분이 틀리다. 제시문은 비용이나 시간 문제로 위험을 받아들이는 경우이므로 위험 수용이다. ㉡의 위험 전가는 맞지만, 올바르게는 '㉠ 위험 수용, ㉡ 위험 전가'이다.
② X: ㉠과 ㉡이 모두 틀리다. ㉠은 위험을 받아들이는 위험 수용이지 활동 자체를 피하는 위험 회피가 아니다. ㉡은 제3자에게 잠재적 손실을 이전하는 위험 전가이지 통제를 통해 가능성이나 영향을 낮추는 위험 감소가 아니다. 올바르게는 '㉠ 위험 수용, ㉡ 위험 전가'이다.
③ O: ㉠은 과도한 비용이나 시간 때문에 일정 수준의 위험을 감수하므로 위험 수용이다. ㉡은 보험이나 계약으로 손실 부담을 제3자에게 이전하므로 위험 전가이다.
④ X: ㉡을 위험 감소라고 본 부분이 틀리다. 제시문은 통제 강화가 아니라 책임과 손실을 제3자와 공유하거나 이전하는 상황이므로 위험 전가이다. 올바르게는 '㉠ 위험 수용, ㉡ 위험 전가'이다.

NoteBase

오답 포인트

위험 수용과 위험 회피를 반대로 외우면 ㉠에서 흔들리기 쉽다. 또한 '보험'과 '계약'이라는 단어를 놓치면 ㉡을 위험 감소로 착각할 수 있는데, 보험은 위험을 줄이는 것이 아니라 손실 부담을 넘기는 장치이다.

다시 나오면 이렇게 판단

비용이 커서 그냥 감수한다는 표현이 나오면 위험 수용으로 본다. 보험, 계약, 외주처럼 제3자에게 손실 부담을 넘기는 표현이 나오면 위험 전가로 본다. 활동 자체를 중단하면 위험 회피이고, 통제수단으로 가능성이나 영향을 낮추면 위험 감소이다.

암기 포인트

감수하면 수용, 넘기면 전가, 끊으면 회피, 낮추면 감소이다.

NoteBase

문 3. 다음에서 설명하는 컴퓨터 시스템의 평가 기준은?

◯ 컴퓨터 시스템의 보안성을 평가하기 위해 미국 정부의 표준으로 채택된 기준이다.
◯ Rainbow 시리즈라는 미 국방부 문서 중의 하나로 오렌지 북(Orange Book)으로 불린다.
◯ 안전성과 신뢰성이 입증된 컴퓨터 시스템을 보급하기 위해 단계별 보안 평가 등급(D, C1, C2, B1, B2, B3, A1)을 분류하여 각 기관별 특성에 맞는 컴퓨터 시스템을 도입 및 운영하도록 권고하고 있다.

① TCSEC
② CC
③ CMVP
④ ITSEC

정답 1번

출제 포인트

이 문제는 TCSEC, CC, CMVP, ITSEC의 적용 대상과 평가 체계를 구별하는 문제이다.

핵심 개념

TCSEC는 미국 국방부의 컴퓨터 시스템 보안 평가 기준으로, Rainbow Series의 Orange Book이며 등급을 D, C1, C2, B1, B2, B3, A1로 구분한다.
CC는 국제 공통평가기준으로 보안 기능과 보증 요구사항을 공통 프레임으로 평가하는 기준이다.
CMVP는 암호 모듈이 기준에 맞는지를 검증하는 프로그램으로, 컴퓨터 시스템 전체 평가 기준이 아니다.
ITSEC는 유럽권 정보기술 보안 평가 기준으로, 문제의 Orange Book 등급 체계와 구별된다.

선지별 해설

① O: 제시문은 미국 정부 표준, Rainbow Series의 Orange Book, D~A1 단계 등급을 모두 말하고 있으므로 TCSEC를 가리킨다.
② X: CC는 국제 공통평가기준이므로 오렌지 북이나 D, C1, C2, B1, B2, B3, A1 등급 체계를 사용하지 않는다. 틀린 표현은 TCSEC의 특징을 CC에 대응시킨 부분이다. 올바르게는 CC는 국제 표준 기반의 공통평가기준이다.
③ X: CMVP는 암호 모듈 검증 프로그램이므로 컴퓨터 시스템 전체의 보안 등급을 분류하는 기준이 아니다. 틀린 표현은 컴퓨터 시스템 평가 기준으로 본 부분이다. 올바르게는 CMVP는 암호 모듈의 적합성을 검증하는 제도이다.
④ X: ITSEC는 유럽의 정보기술 보안 평가 기준이므로 미국 국방부의 Orange Book과 동일하지 않다. 틀린 표현은 Rainbow Series와 D~A1 등급 체계를 ITSEC에 연결한 부분이다. 올바르게는 ITSEC는 유럽권 평가 기준이다.

NoteBase

오답 포인트

CC와 ITSEC는 모두 보안 평가 기준이라 이름만 보면 헷갈리기 쉽고, CMVP도 보안 검증 제도라서 함께 섞이기 쉽다. 그러나 문제의 핵심 단서는 Orange Book과 D, C1, C2, B1, B2, B3, A1 등급이므로 TCSEC로 바로 좁혀진다.

다시 나오면 이렇게 판단

문제에서 Orange Book, Rainbow Series, 미국 국방부, D~A1 등급이 보이면 TCSEC를 먼저 판단한다. 반대로 국제 공통평가기준이면 CC, 암호 모듈 검증이면 CMVP, 유럽 평가 기준이면 ITSEC로 구분한다.

암기 포인트

TCSEC는 Orange Book, CC는 국제 공통평가기준, CMVP는 암호 모듈, ITSEC는 유럽 평가 기준이다.

NoteBase

문 4. 유닉스 시스템 명령어에 대한 설명으로 옳지 않은 것은?

① grep - 파일 내 정규 표현식을 포함한 모든 행을 검색·출력하는 명령

② mesg - 모든 로그인 사용자에게 메시지를 전송하는 명령

③ chmod - 파일이나 디렉토리의 접근 권한을 변경하는 명령

④ man - 각종 명령의 사용법을 출력하는 명령

정답 2번

출제 포인트

이 문제는 유닉스 기본 명령어의 기능을 정확히 구분하는지를 묻는 문제이다.

핵심 개념

grep은 파일에서 패턴과 일치하는 행을 찾는 검색 명령이다.
mesg는 다른 사용자가 현재 터미널에 메시지를 써 넣을 수 있는지 허용 여부를 정하는 명령이다.
chmod는 파일이나 디렉터리의 접근 권한을 변경하는 명령이다.
man은 명령어의 매뉴얼과 사용법을 보여 주는 명령이다.

선지별 해설

① O: grep은 파일 내용 중 정규 표현식과 일치하는 행을 검색하여 출력하는 명령이므로 설명이 맞다.
② X: 틀린 부분은 "모든 로그인 사용자에게 메시지를 전송"이다. mesg는 전체 사용자에게 메시지를 보내는 명령이 아니라 현재 사용자의 터미널에 대한 메시지 수신 허용 여부를 설정하는 명령이다. 모든 로그인 사용자에게 공지성 메시지를 보내는 명령은 wall이다.
③ O: chmod는 파일이나 디렉터리의 읽기, 쓰기, 실행 권한을 변경하는 명령이므로 설명이 맞다.
④ O: man은 각종 명령어의 매뉴얼 페이지를 보여 주어 사용법과 옵션을 확인하게 하는 명령이므로 설명이 맞다.

오답 포인트

mesg를 write나 wall과 혼동하면 틀리기 쉽다. 메시지 전송 명령과 메시지 수신 허용 설정 명령을 구분하지 못하도록 만든 선지이다.

다시 나오면 이렇게 판단

유닉스 명령어 문제는 명령어가 수행하는 대상이 무엇인지부터 구분하면 된다. 검색인지, 권한 변경인지, 매뉴얼 조회인지, 메시지 송수신 설정인지를 나누면 오답을 빠르게 걸러낼 수 있다.

NoteBase

암기 포인트

grep은 검색, chmod는 권한, man은 매뉴얼, mesg는 메시지 허용 설정이다.

NoteBase

문 5. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 기관의 장이 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는 기관에 해당하지 않는 것은?

① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원

② 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업

③ 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원

④ 「국가정보화 기본법」 제14조의 규정에 의한 한국정보화진흥원

정답 4번

쟁점

이 문제는 주요정보통신기반시설의 취약점 분석·평가를 관리기관의 장이 외부 기관에 맡길 수 있는 범위를 묻는 문제이다. 핵심은 정보통신기반 보호법령이 열거한 전문기관과 일반 정보화 지원기관을 구별하는 것이다.

용어 풀이

취약점 분석·평가란 주요정보통신기반시설이 해킹·악성코드·서비스 중단 같은 전자적 침해에 얼마나 취약한지를 점검하고 개선 필요사항을 찾는 절차이다.

핵심 구분

원칙적으로 취약점 분석·평가는 관리기관이 직접 전담반을 구성해 수행한다. 다만 법령이 정한 전문기관에는 위탁할 수 있다. 이 범주에는 한국인터넷진흥원, 정보공유·분석센터, 정보보호 전문서비스 기업, 한국전자통신연구원 계열 연구기관이 포함되고, 일반적인 국가정보화 추진기관이라고 해서 자동으로 포함되지는 않는다.

NoteBase

기출OX 해설집 · 공무원/국가직/7급 · 정보보호론 · 2018

선지별 해설

① O
- 한국인터넷진흥원은 정보통신기반 보호법 시행령상 취약점 분석·평가를 수행할 수 있는 대표적 전문기관에 해당한다.
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률상 설립 근거를 둔 기관이라는 점이 핵심이다.

② O
- 정보보호 전문서비스 기업은 법령상 지정된 전문기관 범주에 포함되므로 취약점 분석·평가를 위탁받을 수 있다.
- 문제의 표현처럼 정보보호산업의 진흥에 관한 법률에 따라 지정된 기업이라는 점이 맞다.

③ O
- 한국전자통신연구원 계열 연구기관도 시행령이 열거한 위탁 가능 전문기관 범주에 포함된다.
- 문제는 정부출연연구기관법상 설립 근거를 제시하고 있으므로, 열거된 전문 연구기관이라는 점에서 옳다.

④ X
- 한국정보화진흥원은 국가정보화 정책 지원기관이지만, 주요정보통신기반시설 취약점 분석·평가의 위탁 가능 기관으로 열거된 기관은 아니다.
- 틀린 표현: "국가정보화 기본법 제14조의 규정에 의한 한국정보화진흥원"
- 올바른 표현: "취약점 분석·평가를 맡길 수 있는 기관은 정보통신기반 보호법령이 열거한 전문기관이어야 하며, 한국정보화진흥원은 그 열거에 포함되지 않는다."

오답 포인트

이 문제를 틀렸다면 정보보호 전문기관과 정보화 일반 지원기관을 혼동했을 가능성이 높다. ④는 기관 이름만 보면 국가 차원의 정보화 기관이라 그럴듯하지만, 취약점 분석·평가 위탁기관은 별도 법령에서 제한적으로 열거한다는 점이 함정이다.

다시 나오면 이렇게 판단

기관 열거형 법령 문제는 먼저 해당 업무가 모든 공공기관에 넓게 열려 있는지, 아니면 시행령이 특정 전문기관만 열거하는지부터 본다. 보안 점검·인증·취약점 분석처럼 전문성이 큰 업무는 대개 열거주의로 처리되므로, 정보화 일반기관은 제외될 가능성이 높다.

암기 포인트

취약점 분석·평가 위탁은 정보화기관이 아니라 보안 전문기관 열거라는 점이 핵심이다.

NoteBase

문 6. SHA-512 알고리즘의 처리 방식에 대한 설명으로 옳지 않은 것은?

① 최대 크기가 2^{128}비트 이하인 메시지를 입력받아 512비트 메시지 다이제스트를 출력한다.

② 필요한 길이의 패딩과 128비트 블록을 추가하여 처리하려는 메시지의 전체 크기가 1,024비트의 배수가 되게 한다.

③ 8개 소수의 제곱근에서 얻은 이진수로 초기화된 512비트 버퍼를 알고리즘의 중간 값과 최종 값을 저장하는 데 사용한다.

④ 블록 단위로 메시지를 처리하는 과정은 80라운드로 이루어지며, 규칙성을 제거하기 위해 각 라운드마다 서로 다른 암호 키를 사용한다.

정답 4번

출제 포인트

이 문제는 SHA-512의 입력 한계, 패딩 방식, 초기 해시값, 라운드 상수의 성격을 구분하는 문제이다.

핵심 개념

- SHA-512: SHA-2 계열 해시 함수로 2^128비트 이하 메시지를 1024비트 블록으로 처리하여 512비트 다이제스트를 만든다.
- 패딩: 메시지 끝에 1, 0들, 128비트 길이 정보를 붙여 전체 길이를 1024비트의 배수로 맞춘다.
- 초기 해시값과 라운드 상수: 초기 해시값은 8개 소수 제곱근 소수부에서, 라운드 상수는 80개 소수 세제곱근 소수부에서 얻은 고정 공개값이다.

NoteBase

선지별 해설

① O
최대 입력 길이가 2^{128}비트 미만인 메시지를 받아 512비트 메시지 다이제스트를 출력하므로 맞는 설명이다.

② O
SHA-512는 패딩과 128비트 길이 정보를 추가하여 전체 입력 길이가 1024비트의 배수가 되게 하므로 맞는 설명이다.

③ O
초기 해시값은 8개의 64비트 워드로 이루어져 총 512비트이며, 처음 8개 소수의 제곱근 소수부에서 얻은 값으로 초기화된다. 이 값은 압축 과정의 중간 해시값과 최종 해시값 저장에 사용되므로 맞는 설명이다.

④ X
80라운드로 처리한다는 부분은 맞다. 틀린 표현은 '서로 다른 암호 키'이다. SHA-512는 대칭키 암호처럼 비밀키를 라운드마다 쓰는 구조가 아니라, 각 라운드에서 공개된 고정 상수 K_t를 사용한다. 올바르게는 '각 라운드마다 서로 다른 라운드 상수를 사용한다'이다.

오답 포인트

④는 '80라운드'라는 맞는 정보 뒤에 '암호 키'라는 낯익은 표현을 붙여 해시 함수와 블록 암호를 혼동하게 만든 선지이다. SHA-512는 키 기반 암호가 아니라 압축 함수 기반 해시이므로 비밀 키와 라운드 상수를 구분해야 한다.

다시 나오면 이렇게 판단

SHA-512가 나오면 먼저 블록 크기 1024비트, 다이제스트 512비트, 길이 필드 128비트, 라운드 수 80을 대응시켜 본다. 그다음 선지에 '암호 키'처럼 비밀값을 뜻하는 표현이 나오면 해시의 고정 상수 개념과 비교해 오답 여부를 판단한다.

암기 포인트

SHA-512는 1024비트 블록, 512비트 출력, 128비트 길이 필드, 80라운드 상수 사용 구조이다.

NoteBase

문 7. 커버로스(Kerberos) 버전 4 인증 시스템에서 클라이언트가 응용 서버에게 제시하는 티켓에 포함되는 구성요소가 아닌 것은?

① 클라이언트 ID

② 클라이언트와 응용 서버 간의 세션키

③ 인증 서버의 네트워크 주소

④ 티켓의 유효시간

정답 3번

출제 포인트

이 문제는 Kerberos 버전 4의 서비스 티켓에 실제로 들어가는 항목과 들어가지 않는 항목을 구별하는 문제이다.

핵심 개념

Kerberos 버전 4의 서비스 티켓은 응용 서버가 클라이언트를 검증할 수 있도록 클라이언트 ID, 클라이언트의 네트워크 주소, 서버와 공유할 세션키, 유효시간 등을 담는다.
인증 서버의 네트워크 주소는 티켓의 구성요소가 아니며, 인증 절차에 관여하는 별도 시스템 정보일 뿐이다.

선지별 해설

① O: 클라이언트 ID는 티켓에 포함된다. 서버는 이 식별자를 보고 어떤 사용자를 위한 티켓인지 확인한다.
② O: 클라이언트와 응용 서버 간의 세션키는 티켓의 핵심 구성요소이다. 서버는 이 키로 이후 통신을 안전하게 처리한다.
③ X: 틀린 부분은 "인증 서버의 네트워크 주소"이다. Kerberos 버전 4 티켓에는 인증 서버 주소가 아니라 클라이언트의 네트워크 주소가 포함된다.
④ O: 티켓의 유효시간은 재사용과 오남용을 막기 위해 포함된다. 일정 시간이 지나면 해당 티켓은 더 이상 쓸 수 없다.

오답 포인트

③은 '네트워크 주소'라는 표현이 같아서 클라이언트 주소와 인증 서버 주소를 서로 바꿔 외우면 틀리기 쉽다. Kerberos 티켓은 인증 서버의 위치 정보를 전달하는 문서가 아니라 서비스 이용에 필요한 인증 정보를 담는다는 점이 함정이다.

다시 나오면 이렇게 판단

Kerberos 티켓 문제는 응용 서버가 클라이언트를 검증하는 데 직접 필요한 정보만 남긴다고 보면 된다. 사용자 식별자, 클라이언트 주소, 세션키, 유효시간은 포함되고 인증 서버 자체의 주소 같은 정보는 포함되지 않는다.

NoteBase

암기 포인트

Kerberos 티켓은 '누가, 어디서, 어떤 키로, 언제까지'를 담고 인증 서버 주소는 담지 않는다.

NoteBase

문 8. 방화벽은 검사 대상이나 동작 방식에 따라 패킷 필터링, 상태 검사(stateful inspection), 응용 레벨 게이트웨이, 회선 레벨 게이트웨이로 분류할 수 있다. 상태 검사 방화벽에 대한 설명으로 옳은 것은?

① 트래픽 정보 수집이 어렵고, IP 스푸핑 공격에 대응하기 어렵다.

② 서비스별로 프록시 서버 데몬을 두어 사용자 인증과 접근 제어를 수행한다.

③ 패킷 필터링 기능을 사용하며 현재 연결 세션의 트래픽 상태와 미리 저장된 상태와의 비교를 통하여 접근을 제어한다.

④ 송·수신자 간의 직접적인 연결을 허용하지 않고, 송신자와 수신자 사이에서 프록시가 어떤 연결을 허용할지를 판단한다.

정답 3번

출제 포인트

이 문제는 상태 검사 방화벽과 패킷 필터링 방화벽, 응용 레벨 게이트웨이, 회선 레벨 게이트웨이의 동작 차이를 구분하는 문제이다.

핵심 개념

패킷 필터링 방화벽은 헤더 정보 중심으로 각 패킷을 독립적으로 검사하는 방식이다.
상태 검사 방화벽은 세션의 상태 정보를 저장해 두고 현재 패킷이 그 연결 흐름에 맞는지까지 함께 판단하는 방식이다.
응용 레벨 게이트웨이는 서비스별 프록시를 두고 응용 계층에서 명령과 인증을 통제하는 방식이다.
회선 레벨 게이트웨이는 종단 간 직접 연결을 끊고 프록시가 세션 연결 자체를 중계하는 방식이다.

NoteBase

선지별 해설

① X: '트래픽 정보 수집이 어렵고, IP 스푸핑 공격에 대응하기 어렵다'는 설명은 상태 저장 없이 개별 패킷만 보는 단순 패킷 필터링 방화벽의 약점에 가깝다. 상태 검사 방화벽은 연결 상태를 추적하므로 이 설명이 그대로 맞지 않는다. 틀린 표현은 '상태 검사 방화벽'에 이 약점을 붙인 부분이며, 올바르게는 '기본적인 패킷 필터링 방화벽은 트래픽 맥락 파악이 제한적이다'이다.
② X: 서비스별 프록시 서버 데몬을 두어 사용자 인증과 접근 제어를 수행하는 것은 응용 레벨 게이트웨이의 특징이다. 상태 검사 방화벽은 프록시 데몬 중심이 아니라 세션 상태 테이블을 바탕으로 패킷 흐름을 검사한다. 틀린 표현은 '서비스별 프록시 서버 데몬'이며, 올바르게는 '응용 레벨 게이트웨이는 서비스별 프록시를 사용한다'이다.
③ O: 상태 검사 방화벽은 기본적으로 패킷 필터링 기능을 가지면서, 현재 패킷이 기존 세션의 상태 정보와 일치하는지를 확인해 접근을 통제한다. 현재 연결 세션의 트래픽 상태와 저장된 상태 정보를 비교한다는 설명이 핵심 특징에 맞다.
④ X: 송신자와 수신자 사이에 프록시가 개입해 직접 연결을 허용하지 않고 연결 여부를 판단하는 설명은 회선 레벨 게이트웨이 또는 프록시형 게이트웨이의 특징이다. 상태 검사 방화벽의 핵심은 프록시 중계가 아니라 세션 상태 추적이다. 틀린 표현은 '프록시가 어떤 연결을 허용할지를 판단한다'이며, 올바르게는 '회선 레벨 게이트웨이는 프록시가 연결을 중계한다'이다.

오답 포인트

상태 검사 방화벽은 '패킷 필터링을 확장한 형태'라는 점 때문에 ①과 ③을 함께 맞는 설명처럼 착각하기 쉽다. 그러나 ①은 상태를 보지 않는 필터링 방화벽의 한계를 말하고, ②와 ④는 각각 응용 레벨 게이트웨이와 회선 레벨 게이트웨이의 프록시 특성을 섞어 놓은 선지이다.

다시 나오면 이렇게 판단

방화벽 유형 문제는 먼저 판단 기준을 나누면 정리가 된다. 헤더 중심의 단순 검사이면 패킷 필터링, 세션 상태 추적이면 상태 검사, 서비스별 프록시이면 응용 레벨 게이트웨이, 연결 중계 프록시이면 회선 레벨 게이트웨이로 판단할 수 있다.

암기 포인트

상태 검사는 세션 상태 추적, 응용 게이트웨이는 서비스별 프록시, 회선 게이트웨이는 연결 중계이다.

NoteBase

문 9. VPN의 터널링 기능을 제공하는 L2TP(Layer 2 Tunneling Protocol)에 대한 설명으로 옳지 않은 것은?

① 데이터 링크 계층에서 터널링을 지원한다.

② PPTP(Point-to-Point Tunneling Protocol)와 L2F(Layer 2 Forwarding Protocol)의 기능을 결합한 프로토콜이다.

③ 데이터의 보안성을 높이기 위하여 IPsec과 결합하여 사용할 수 있다.

④ 패킷 인증, 암호화, 키 관리 기능을 제공한다.

정답 4번

출제 포인트

이 문제는 L2TP의 계층적 성격과 터널링 기능, 그리고 IPsec과 결합할 때의 보안 기능 분담을 구별하는 문제이다.

핵심 개념

L2TP는 2계층에서 PPP 프레임 등을 터널링하는 프로토콜이며, 핵심 기능은 터널 생성과 전달이다.
PPTP와 L2F의 기능을 반영해 만든 프로토콜로 이해할 수 있다.
IPsec은 패킷 인증, 암호화, 키 관리로 대표되는 보안 기능을 담당하므로, L2TP 자체와 구별해야 한다.

선지별 해설

① O: L2TP는 Layer 2 Tunneling Protocol이라는 이름 그대로 데이터 링크 계층의 터널링을 지원하므로 옳다.
② O: L2TP는 PPTP와 L2F의 기능을 결합한 형태로 정리하는 것이 일반적이므로 옳다.
③ O: L2TP는 자체 보안 기능이 약하므로 IPsec과 결합한 L2TP/IPsec 형태로 사용되어 기밀성과 무결성을 보완할 수 있으므로 옳다.
④ X: 틀린 부분은 "패킷 인증, 암호화, 키 관리 기능을 제공한다"는 표현이다. 실제로는 L2TP 자체가 아니라 IPsec이 패킷 인증, 암호화, 키 관리를 제공하고, L2TP는 터널링 자체를 담당한다.

오답 포인트

L2TP와 IPsec을 함께 쓰는 사례가 많아서 L2TP 자체가 암호화와 인증까지 수행한다고 섞어 외우기 쉽다. 이 문항은 터널링 프로토콜과 보안 프로토콜의 역할 분리를 묻는 함정이다.

다시 나오면 이렇게 판단

VPN 관련 선지를 보면 먼저 그 기술이 터널을 만드는지, 아니면 인증·암호화·키 관리를 담당하는지부터 나눠 판단한다. L2TP는 터널링, IPsec은 보안 기능이라는 기준으로 보면 빠르게 정리된다.

NoteBase

암기 포인트

L2TP는 터널, IPsec은 보호라는 구도로 기억하면 혼동이 줄어든다.

NoteBase

문 10. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 유출등의 통지·신고에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 (㉠) 또는 (㉡)에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자등의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

① ㉠ 과학기술정보통신부, ㉡ 한국인터넷진흥원

② ㉠ 과학기술정보통신부, ㉡ 개인정보보호위원회

③ ㉠ 방송통신위원회, ㉡ 한국인터넷진흥원

④ ㉠ 방송통신위원회, ㉡ 개인정보보호위원회

정답 3번

쟁점

이 문제는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 유출등 발생 시 신고기관을 정확히 연결할 수 있는지를 묻는 문제이다.

용어 풀이

유출등은 개인정보의 분실·도난·유출을 묶어 부르는 말이다.

핵심 구분

이용자에게는 유출 사실과 법정 사항을 통지하고, 행정기관 측 신고는 방송통신위원회 또는 한국인터넷진흥원에 한다. 한국인터넷진흥원이 신고를 받으면 그 사실을 방송통신위원회에 알리게 된다.

NoteBase

선지별 해설

1번: X. ㉠이 틀렸다. 법상 신고 상대방은 과학기술정보통신부가 아니라 방송통신위원회 또는 한국인터넷진흥원이다. 틀린 표현은 "과학기술정보통신부"이고, 올바른 표현은 "방송통신위원회"이다. ㉡ 한국인터넷진흥원은 맞는 기관이지만 ㉠이 틀려 전체는 오답이다.
2번: X. ㉠과 ㉡이 모두 틀렸다. 개인정보 유출등의 신고기관은 과학기술정보통신부나 개인정보보호위원회가 아니다. 틀린 표현은 "과학기술정보통신부"와 "개인정보보호위원회"이고, 올바른 표현은 "방송통신위원회"와 "한국인터넷진흥원"이다.
3번: O. 법 조문과 시행령의 신고 규정 모두 방송통신위원회 또는 한국인터넷진흥원을 신고 대상으로 둔다. 따라서 ㉠ 방송통신위원회, ㉡ 한국인터넷진흥원이 정확하다.
4번: X. ㉠ 방송통신위원회는 맞지만 ㉡이 틀렸다. 이 조문에서 신고기관으로 적시되는 기관은 개인정보보호위원회가 아니라 한국인터넷진흥원이다. 틀린 표현은 "개인정보보호위원회"이고, 올바른 표현은 "한국인터넷진흥원"이다.

오답 포인트

감독기관, 접수기관, 일반 개인정보 주무기관을 한꺼번에 섞으면 틀리기 쉽다. 이 문항은 이용자에 대한 통지와 국가기관에 대한 신고를 구분하고, 신고기관을 방송통신위원회 또는 한국인터넷진흥원으로 기억하는지를 노린 문제이다.

다시 나오면 이렇게 판단

개인정보 유출 조문이 나오면 먼저 이용자에게 알려야 할 5가지 사항이 무엇인지 보고, 그다음 신고 상대방이 방송통신위원회 또는 한국인터넷진흥원인지 확인하면 된다. 중앙부처 명칭이나 개인정보보호위원회가 선택지에 보이면 우선 오답 후보로 본다.

암기 포인트

유출 통지는 이용자에게 하고, 유출 신고는 방통위 또는 한국인터넷진흥원에 한다.

NoteBase

문 11. 침입차단시스템이 제공하는 주요 보안 서비스가 아닌 것은?

① 접근 통제

② 최대 권한 부여

③ 사용자 인증

④ 감사 및 로그 기능

정답 2번

출제 포인트

이 문제는 침입차단시스템의 주요 기능과 권한 관리 원칙을 구별할 수 있는지를 묻는다.

핵심 개념

침입차단시스템은 네트워크 경계에서 접근을 통제하고 인증 연동, 감사 및 로그 기록으로 보안을 강화하는 시스템이다.
권한 관리는 필요한 범위만 주는 최소 권한 원칙이 핵심이며, 최대 권한 부여는 보안 원칙에 어긋난다.

선지별 해설

1번: O. 접근 통제는 침입차단시스템의 대표 기능이다. 허용된 트래픽만 통과시키고 비인가 접근을 차단한다.
2번: X. 틀린 부분은 "최대 권한 부여"이다. 실제로는 사용자나 프로세스에 업무 수행에 필요한 범위만 주는 최소 권한 부여가 보안 원칙이다.
3번: O. 사용자 인증은 침입차단시스템이 연계하거나 제공할 수 있는 기본 보안 서비스에 해당한다. 정당한 사용자 여부를 확인해 접근 통제의 전제가 된다.
4번: O. 감사 및 로그 기능은 접속 시도와 차단 내역을 기록해 사후 추적과 보안 점검에 활용되는 주요 기능이다.

오답 포인트

접근 통제와 권한 부여를 함께 보다가 2번의 "최대"라는 표현을 놓치기 쉽다. 보안 시스템은 권한을 넓게 주는 것이 아니라 필요한 만큼만 제한해서 부여한다는 원칙을 떠올려야 한다.

다시 나오면 이렇게 판단

보안 서비스 문제에서는 인증, 접근 통제, 감사처럼 통제를 강화하는 기능인지 먼저 본다. 권한 부여가 나오면 최대 권한이 아니라 최소 권한 원칙인지 확인하면 정답을 가를 수 있다.

암기 포인트

침입차단시스템은 접근 통제와 로그 기록, 권한 관리는 최소 권한이 핵심이다.

NoteBase

문 12. ㉠, ㉡에 들어갈 네트워크 보안 공격을 바르게 연결한 것은?

(㉠)은(는) TCP 연결 설정을 위한 3-way handshaking 과정에서 half-open 연결 시도가 가능하다는 취약성을 이용하는 공격 방식이다.
(㉡)은(는) 서버와 클라이언트가 TCP 통신을 하고 있을 때, RST 패킷을 보내고 시퀀스 넘버 등을 조작하여 연결을 가로채는 공격 방식이다.

① ㉠: SYN 플러딩, ㉡: IP 스푸핑
② ㉠: SYN 플러딩, ㉡: 세션 하이재킹
③ ㉠: ARP 스푸핑, ㉡: IP 스푸핑
④ ㉠: ARP 스푸핑, ㉡: 세션 하이재킹

정답 2번

출제 포인트

이 문제는 SYN 플러딩, 세션 하이재킹, IP 스푸핑, ARP 스푸핑의 정의와 적용 지점을 구분하는 문제이다.

핵심 개념

SYN 플러딩: TCP 3-way handshaking 과정에서 SYN 요청을 대량으로 보내 half-open 연결을 쌓아 자원을 고갈시키는 서비스 거부 공격이다. 키워드는 half-open, 연결 대기 큐, 3-way handshaking이다.
세션 하이재킹: 이미 성립된 TCP 세션에서 시퀀스 번호 등을 조작해 통신 흐름을 탈취하거나 끼어드는 공격이다. 키워드는 established session, sequence number, RST 삽입이다.
IP 스푸핑: 출발지 IP 주소를 속여 다른 호스트인 것처럼 보이게 하는 주소 위조 기법이다. 키워드는 source IP forgery이다.
ARP 스푸핑: LAN 환경에서 ARP 응답을 위조해 IP와 MAC 주소 매핑을 속이는 공격이다. 키워드는 ARP cache poisoning이다.

NoteBase

선지별 해설

① X: ㄱ의 SYN 플러딩은 맞지만 ㄴ의 IP 스푸핑이 틀리다. IP 스푸핑은 출발지 IP를 위조하는 기법일 뿐, 이미 성립한 TCP 연결에서 RST 패킷과 시퀀스 번호를 조작해 세션을 가로채는 공격을 뜻하지는 않는다. 틀린 표현은 'IP 스푸핑'이고, 올바르게는 '세션 하이재킹'이다.
② O: ㄱ은 TCP 3-way handshaking의 half-open 상태를 악용하는 SYN 플러딩이고, ㄴ은 TCP 통신 중 RST 패킷과 시퀀스 번호 조작으로 연결을 탈취하는 세션 하이재킹이다. 두 설명이 각각의 공격 특징과 정확히 대응한다.
③ X: ㄱ의 ARP 스푸핑이 틀리다. ARP 스푸핑은 ARP 캐시를 오염시켜 같은 네트워크 내에서 트래픽을 우회시키는 공격이므로 TCP 3-way handshaking의 half-open 연결과는 관련이 없다. 틀린 표현은 'ARP 스푸핑'이고, 올바르게는 'SYN 플러딩'이다. ㄴ의 IP 스푸핑도 위 설명과 같이 세션 탈취 공격의 직접 명칭이 아니므로 부정확하다.
④ X: ㄴ의 세션 하이재킹은 맞지만 ㄱ의 ARP 스푸핑이 틀리다. half-open 연결 시도를 이용하는 공격은 ARP 스푸핑이 아니라 SYN 플러딩이다. 틀린 표현은 'ARP 스푸핑'이고, 올바르게는 'SYN 플러딩'이다.

오답 포인트

SYN 플러딩과 IP 스푸핑이 함께 언급되는 경우가 있어 둘을 같은 공격처럼 섞기 쉽다는 점이 함정이다. 이 문항은 공격이 일어나는 계층과 핵심 동작을 묻는다. half-open 연결을 쌓으면 SYN 플러딩이고, 주소를 속이면 IP 스푸핑이며, ARP 캐시를 속이면 ARP 스푸핑이고, 이미 열린 TCP 세션의 시퀀스 흐름을 탈취하면 세션 하이재킹이다.

다시 나오면 이렇게 판단

문장에 3-way handshaking, half-open, 연결 대기 자원 고갈이 보이면 SYN 플러딩으로 판단한다. 문장에 통신 중인 TCP 세션, 시퀀스 번호 조작, RST 삽입, 연결 탈취가 보이면 세션 하이재킹으로 판단한다. 주소 위조인지, ARP 매핑 위조인지, 이미 열린 세션 탈취인지를 먼저 구분하면 오답을 줄일 수 있다.

암기 포인트

half-open은 SYN 플러딩, 열린 TCP 세션 탈취는 세션 하이재킹, 출발지 주소 위조는 IP 스푸핑, ARP 매핑 위조는 ARP 스푸핑이다.

NoteBase

문 13. 다음에서 설명하는 암호 알고리즘은?

◯ Koblitz와 Miller가 제안한 것이다.
◯ RSA보다 키의 길이를 작게 하면서도 대등한 보안성을 제공한다.
◯ 전자서명이나 키 교환에 활용될 수 있다.
◯ 메모리와 처리능력이 제한된 분야에 효율적이다.

① ElGamal
② ECC(Elliptic Curve Cryptography)
③ Rabin
④ WHIRLPOOL

정답 2번

출제 포인트

이 문제는 ECC의 대표 특징을 다른 공개키 암호 및 해시 함수와 구별할 수 있는지를 묻는다.

핵심 개념

ECC: 타원곡선 위의 이산로그 문제를 기반으로 하는 공개키 암호 계열이다. 키워드가 Koblitz, Miller, 짧은 키, 전자서명, 키 교환이다.
ElGamal: 이산로그 문제 기반의 공개키 암호이지만 타원곡선 자체를 기본 전제로 한 전통적 ElGamal과는 구별된다.
Rabin: 큰 합성수 n에 대한 제곱근 계산의 어려움을 이용하는 공개키 암호이다.
WHIRLPOOL: 무결성 검증용 해시 함수로, 공개키 암호나 키 교환 방식이 아니다.

선지별 해설

1번 X: ElGamal은 이산로그 기반 공개키 암호이지만 제안자가 Koblitz와 Miller가 아니다. 틀린 표현은 'Koblitz와 Miller가 제안'에 대응시키는 부분이다. 올바르게는 ElGamal은 Taher Elgamal이 제안한 방식이다.
2번 O: ECC는 Koblitz와 Miller가 제안한 타원곡선 암호로, RSA보다 짧은 키 길이로도 비슷한 수준의 보안성을 제공한다. 또한 ECDSA 같은 전자서명, ECDH 같은 키 교환에 활용되고 경량 환경에도 비교적 유리하다.
3번 X: Rabin은 공개키 암호이지만 문제의 설명처럼 짧은 키로 같은 보안성을 주는 타원곡선 암호가 아니다. 틀린 표현은 'RSA보다 키 길이를 작게 하면서도 대등한 보안성'과 'Koblitz와 Miller'에 대응시키는 부분이다. 올바르게는 Rabin은 제곱근 문제 기반 공개키 암호이다.
4번 X: WHIRLPOOL은 해시 함수이므로 전자서명이나 키 교환 알고리즘 자체가 아니다. 틀린 표현은 공개키 암호의 특징을 해시 함수에 연결한 부분이다. 올바르게는 WHIRLPOOL은 메시지 다이제스트를 생성하는 해시 함수이다.

NoteBase

오답 포인트

전자서명과 키 교환에 쓰인다는 문장만 보고 ElGamal 같은 공개키 암호를 고르기 쉽다. 그러나 이 문항의 결정 단서는 'Koblitz와 Miller', 'RSA보다 짧은 키', '제한된 메모리와 처리능력에 효율적'이라는 타원곡선 암호의 묶음 특징이다.

다시 나오면 이렇게 판단

제안자와 보안성 대비 키 길이를 먼저 본다. Koblitz와 Miller, 짧은 키, ECDSA, ECDH, 경량 환경이 함께 나오면 ECC로 판단한다. 해시 함수인지 공개키 암호인지부터 가르면 WHIRLPOOL 같은 선택지는 바로 제외된다.

암기 포인트

ECC는 Koblitz·Miller, 짧은 키, 전자서명과 키 교환이다. WHIRLPOOL은 해시 함수이다.

NoteBase

문 14. ㉠, ㉡에 들어갈 웹 공격 기법을 바르게 연결한 것은?

(㉠)은(는) 웹 해킹으로 서버 권한을 획득한 후, 해당 서버에서 공격자의 PC로 연결하고 공격자가 직접 명령을 입력하여 개인정보 전송 등의 악의적인 행위를 하는 공격이다. 이 기법은 방화벽의 내부에서 외부로 나가는 패킷에 대한 아웃바운드 필터링을 수행하지 않는 허점을 이용한다.
(㉡)은(는) 공격자가 웹 서버의 게시판 등에 악성 스크립트를 삽입한 후, 사용자의 쿠키와 같은 개인정보를 특정 사이트로 전송하게 하거나 악성파일을 다운로드하여 실행하도록 유도하는 공격이다.

① (㉠): 디렉토리 리스팅, (㉡): 포맷 스트링
② (㉠): 디렉토리 리스팅, (㉡): XSS
③ (㉠): 리버스 텔넷, (㉡): 포맷 스트링
④ (㉠): 리버스 텔넷, (㉡): XSS

정답 4번

출제 포인트

이 문제는 리버스 텔넷과 XSS의 핵심 특징을 설명문으로 구별할 수 있는지를 묻는 문제이다.

핵심 개념

리버스 텔넷: 침해된 서버가 공격자 PC로 역방향 접속을 맺게 하여 공격자가 서버 내부에서 직접 명령을 내리게 하는 기법이다. 키워드는 서버 권한 획득 후 내부에서 외부로 나가는 역접속이다.
XSS: 웹 페이지에 악성 스크립트를 삽입해 사용자의 브라우저에서 실행되게 함으로써 쿠키 탈취, 정보 유출, 악성 행위 유도를 일으키는 공격이다. 키워드는 스크립트 삽입과 사용자 브라우저 실행이다.
디렉토리 리스팅: 웹 서버 설정 미흡으로 디렉터리 목록이 노출되는 취약점이다.
포맷 스트링: 형식 지정 문자열 처리 취약점을 악용해 메모리 내용을 읽거나 변조하는 공격이다.

NoteBase

선지별 해설

① X
틀린 부분은 ㉠을 디렉토리 리스팅으로, ㉡을 포맷 스트링으로 본 점이다. ㉠의 설명은 서버 권한 획득 뒤 서버가 공격자에게 역접속해 명령을 받는 형태이므로 리버스 텔넷이다. 디렉토리 리스팅은 파일 목록 노출 취약점일 뿐 원격 명령 수행과 관련이 없다. ㉡도 게시판 등에 악성 스크립트를 삽입해 쿠키를 탈취하는 설명이므로 XSS가 맞다. 올바르게는 ㉠은 리버스 텔넷, ㉡은 XSS이다.

② X
㉡을 XSS로 본 점은 맞지만 ㉠이 틀렸다. ㉠의 핵심은 방화벽이 내부에서 외부로 나가는 연결을 허용하는 점을 이용해 침해 서버가 공격자 PC로 연결을 맺는다는 데 있으므로 리버스 텔넷이다. 디렉토리 리스팅은 디렉터리 열람 노출 문제이므로 설명과 맞지 않는다. 올바르게는 ㉠은 리버스 텔넷이다.

③ X
㉠은 리버스 텔넷으로 맞다. 그러나 틀린 부분은 ㉡을 포맷 스트링으로 본 점이다. ㉡의 핵심은 악성 스크립트 삽입 후 사용자의 브라우저에서 실행되어 쿠키 탈취나 악성 행위 유도가 일어나는 것이므로 XSS이다. 포맷 스트링은 메모리 처리 취약점 악용 공격이어서 설명과 맞지 않는다. 올바르게는 ㉡은 XSS이다.

④ O
㉠은 서버가 공격자에게 역접속해 명령을 받는 리버스 텔넷이고, ㉡은 악성 스크립트 삽입으로 사용자 정보를 탈취하는 XSS이므로 두 설명을 모두 정확히 연결했다.

오답 포인트

㉠에서 '서버 권한 획득 후 공격자 PC로 연결'이라는 표현을 놓치면 단순 정보 노출형 취약점인 디렉토리 리스팅과 혼동하기 쉽다. ㉡에서는 '악성 스크립트 삽입'과 '쿠키 전송'이라는 문구가 XSS의 결정적 단서인데, 이를 메모리 취약점인 포맷 스트링과 섞으면 오답이 된다.

다시 나오면 이렇게 판단

설명문에서 먼저 행위를 본다. 침해된 서버가 외부 공격자에게 역방향으로 붙어 명령을 받으면 리버스 텔넷이다. 웹 페이지에 스크립트가 삽입되고 그 스크립트가 사용자 브라우저에서 실행되면 XSS이다. 파일 목록 노출이면 디렉토리 리스팅이고, 형식 지정 문자열 악용이면 포맷 스트링이다.

암기 포인트

역접속이면 리버스 텔넷, 스크립트 삽입과 쿠키 탈취면 XSS이다.

NoteBase

문 15. IEEE 802.11i에서 정의된 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol)에 대한 설명으로 옳지 않은 것은?

① 기존의 WEP(Wired Equivalent Privacy) 보안 구현 장치에서 소프트웨어적으로 동작할 수 있도록 고안되었다.

② CBC(Cipher Block Chaining)-MAC를 사용하여 메시지 무결성을 제공한다.

③ AES(Advanced Encryption Standard)의 CTR 블록 암호 모드를 사용한다.

④ WPA2(Wi-Fi Protected Access 2)에서 사용하는 보안 기술이다.

정답 1번

출제 포인트

이 문제는 CCMP와 TKIP의 역할 차이, 그리고 CCMP를 구성하는 AES-CTR과 CBC-MAC의 조합을 정확히 구별하는지를 묻는 문제이다.

핵심 개념

CCMP는 AES 기반의 무선 LAN 보안 방식으로, 기밀성은 CTR 모드가 담당하고 무결성 및 인증은 CBC-MAC이 담당한다.
TKIP는 기존 WEP 하드웨어를 최대한 활용하도록 과도기적으로 설계된 방식이고, CCMP는 그와 달리 AES를 사용하는 보다 강한 보안 방식이다.
따라서 '기존 WEP 장치에서 소프트웨어적으로 동작'이라는 설명은 TKIP의 성격에 가깝고 CCMP의 설명으로는 맞지 않는다.

NoteBase

선지별 해설

① X
기존 WEP 보안 구현 장치에서 소프트웨어적으로 동작하도록 고안된 것은 CCMP가 아니라 주로 TKIP의 설계 취지이다.
틀린 부분은 '기존의 WEP 보안 구현 장치에서 소프트웨어적으로 동작'이다.
올바르게는 'CCMP는 AES를 기반으로 하는 802.11i/WPA2 보안 방식이다.'라고 고쳐야 한다.

② O
CCMP의 CCM은 Counter Mode와 CBC-MAC을 결합한 구조이다.
이 중 CBC-MAC은 메시지 무결성과 인증을 제공하므로 설명이 맞다.

③ O
CCMP는 AES를 사용하며, 데이터 기밀성 제공에는 CTR 모드를 사용한다.
따라서 AES의 CTR 블록 암호 모드를 사용한다는 설명은 맞다.

④ O
CCMP는 WPA2에서 사용하는 대표적인 보안 기술이다.
WPA2는 AES 기반 CCMP를 표준 보안 방식으로 채택하므로 설명이 맞다.

오답 포인트

수험생이 가장 많이 헷갈리는 지점은 TKIP와 CCMP를 모두 802.11i 계열 무선 보안 기술로만 묶어 두고, 하드웨어 호환성까지 같은 성격으로 기억하는 점이다. ①은 바로 그 혼동을 노린 선지이다.

다시 나오면 이렇게 판단

무선 LAN 보안 문제에서 '기존 WEP 장비와의 호환'이 나오면 먼저 TKIP를 떠올리고, 'AES + CTR + CBC-MAC' 조합이 나오면 CCMP로 판단하면 된다. WPA2와 연결되면 CCMP 가능성이 매우 높다.

암기 포인트

TKIP는 WEP 호환 보완책, CCMP는 AES 기반 WPA2 표준 보안 방식이다.

NoteBase

문 16. 전자우편 보안을 위한 PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 전자우편 메시지의 인증과 기밀성 제공을 위한 것으로 필 짐머만(Phil Zimmermann)이 고안하였다.

② 메시지 발송 시 메시지에 대한 서명, 압축, 암호화 순으로 처리할 수 있다.

③ 임의의 사용자는 여러 개의 공개 · 개인키 쌍을 가질 수 있도록 하고 있다.

④ 메시지 암호화를 위한 일회용 세션키를 사용하지 않기 때문에 공유 비밀키를 교환하기 위한 절차가 필요하다.

정답 4번

출제 포인트

이 문제는 PGP의 하이브리드 암호 방식과 메시지 처리 절차를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

PGP는 공개키암호와 대칭키암호를 함께 쓰는 전자우편 보안 방식이다. 결정 차이축은 본문을 무엇으로 암호화하고, 그 키를 어떻게 전달하는가에 있다. 키워드는 세션키, 공개키암호, 전자서명이다.
전자서명은 송신자 인증과 무결성 확인을 위한 기능이고, 메시지 암호화는 기밀성 확보를 위한 기능이다. PGP는 메시지마다 일회용 세션키를 만들어 본문을 빠르게 암호화하고, 그 세션키를 수신자의 공개키로 보호한다.

NoteBase

선지별 해설

① O
필 짐머만이 전자우편의 기밀성과 인증을 위해 PGP를 고안한 설명이므로 맞다. PGP는 전자서명으로 인증과 무결성을, 암호화로 기밀성을 제공한다.

② O
PGP는 메시지 발송 시 보통 서명 후 압축 후 암호화 순으로 처리할 수 있다. 서명을 먼저 하면 서명값까지 함께 압축되고 이후 암호화되어 보호된다.

③ O
PGP는 키링 구조를 사용하므로 한 사용자가 여러 공개키·개인키 쌍을 운용할 수 있다. 키 갱신이나 용도 분리를 위해 복수의 키 쌍을 둘 수 있다는 설명과 맞다.

④ X
틀린 부분은 '일회용 세션키를 사용하지 않기 때문에'와 '공유 비밀키를 교환하기 위한 절차가 필요하다'는 표현이다.
실제로는 PGP가 메시지마다 일회용 세션키를 생성해 본문을 대칭키로 암호화하고, 그 세션키를 수신자의 공개키로 암호화해 전달한다. 올바르게는 'PGP는 일회용 세션키를 사용하므로 사전에 공유 비밀키를 직접 교환하는 절차가 필수는 아니다'라고 고쳐야 한다.

오답 포인트

④는 PGP를 순수한 대칭키 방식처럼 바꿔 말한 함정이다. 수험생이 '암호화'만 보고 공유 비밀키 교환이 필요하다고 연결하면 틀리기 쉽다. PGP의 핵심은 대칭키로 본문을 암호화하되 그 대칭키를 공개키로 안전하게 전달하는 하이브리드 구조라는 점이다.

다시 나오면 이렇게 판단

전자우편 보안 기술 문제가 나오면 본문 암호화 수단, 세션키 사용 여부, 세션키 전달 방식을 먼저 본다. '세션키를 사용하지 않는다'거나 '공유 비밀키를 미리 교환해야 한다'처럼 순수 대칭키 방식으로 설명하면 PGP와 어긋난다고 판단할 수 있다.

암기 포인트

PGP는 서명 후 압축 후 암호화 구조이며, 본문은 세션키로 암호화하고 세션키는 공개키로 보호한다.

NoteBase

문 17. 스트림 암호에 대한 설명으로 옳은 것은?

① 대표적인 스트림 암호 방식인 RC4는 다양한 키 길이를 갖도록 설계된 바이트 기반의 알고리즘이다.

② 안전성은 키열(key stream)을 생성하는 의사 난수 생성기의 안전성에 반비례한다.

③ 블록 암호와 달리 구현이 어렵고 속도가 느린 단점이 있다.

④ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다.

정답 1번

출제 포인트

이 문제는 스트림 암호의 기본 구조, 키열의 안전 조건, 블록 암호와의 일반적 차이를 정확히 구분하는지를 묻는 문제이다.

핵심 개념

스트림 암호: 평문을 비트 또는 바이트 단위로 처리하면서 생성된 키열과 결합해 암복호화하는 방식이다. 결정 차이축: 고정 블록 처리인지 연속 키열 처리인지이다. 키워드: 키열, 순차 처리, 바이트/비트 단위
블록 암호: 평문을 일정한 길이의 블록으로 나누어 각 블록을 변환하는 방식이다. 결정 차이축: 처리 단위와 연산 구조가 다르다. 키워드: 블록 단위, 라운드 연산, 운용 모드
키열 안전성: 스트림 암호의 안전성은 키열이 얼마나 예측 불가능하고 반복 주기가 긴지에 좌우된다. 결정 차이축: 의사 난수 생성기의 품질이다. 키워드: 예측 불가성, 긴 주기, 난수성

선지별 해설

① O: RC4는 바이트 단위로 동작하는 대표적인 스트림 암호이며 가변 키 길이를 사용할 수 있도록 설계되었다. 선지의 핵심인 바이트 기반, 다양한 키 길이 지원이라는 설명이 맞다.
② X: 틀린 부분은 "안전성에 반비례한다"는 표현이다. 스트림 암호의 안전성은 키열을 만드는 의사 난수 생성기의 안전성에 비례한다. 생성기가 예측 가능하면 키열도 예측 가능해져 암호가 약해진다.
③ X: 틀린 부분은 "구현이 어렵고 속도가 느린"이라는 표현이다. 실제로는 스트림 암호가 블록 암호보다 구조가 단순하여 구현이 비교적 쉽고, 실시간 처리에서 빠른 편인 경우가 많다.
④ X: 틀린 부분은 "반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다"는 표현이다. 실제로는 키열의 반복 주기가 짧을수록 같은 패턴이 다시 나타나 분석이 쉬워지므로 더 취약해진다. 주기는 길수록 안전에 유리하다.

오답 포인트

이 문항은 스트림 암호의 장단점을 블록 암호와 반대로 바꾸거나, 키열 주기와 안전성의 관계를 뒤집어 놓는 방식으로 함정을 만든다. 특히 ②의 "반비례"와 ④의 "짧을수록" 같은 방향 표현을 놓치면 틀리기 쉽다.

NoteBase

다시 나오면 이렇게 판단

스트림 암호 문제는 먼저 키열의 품질과 주기부터 본다. 키열이 예측 불가능하고 주기가 길수록 안전하다는 점을 기준으로 선지를 판단하면 방향을 뒤집은 오답을 빠르게 걸러낼 수 있다. 블록 암호와 비교할 때는 처리 단위가 연속 키열인지 고정 블록인지도 함께 확인한다.

암기 포인트

스트림 암호는 키열이 생명이며, 키열은 예측 불가하고 주기가 길어야 한다. 스트림 암호는 보통 연속 처리에 유리하고 구현이 가벼운 편이다.

NoteBase

문 18. 「개인정보의 안전성 확보조치 기준」상 개인정보처리자가 개인정보를 암호화할 때 준수해야 할 사항으로 옳지 않은 것은?

① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어를 사용하여서는 아니 된다.

정답 4번

쟁점

이 문제는 「개인정보의 안전성 확보조치 기준」상 암호화 대상 정보와 전송·저장 상황별 암호화 의무를 구별하는 문제이다.

용어 풀이

고유식별정보는 주민등록번호처럼 개인을 직접 식별할 수 있는 정보이다. 일방향 암호화는 저장된 비밀번호를 다시 평문으로 복원할 수 없도록 처리하는 방식이다.

핵심 구분

전송 단계에서는 고유식별정보, 비밀번호, 바이오정보를 암호화한다. 저장 단계에서는 비밀번호와 바이오정보를 암호화하여 저장하고, 비밀번호는 복호화되지 않도록 일방향 암호화를 적용한다. 업무용 컴퓨터나 모바일 기기에 고유식별정보를 저장하는 경우에는 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘으로 암호화한 후 저장한다.

NoteBase

선지별 해설

1번: O. 고유식별정보, 비밀번호, 바이오정보를 정보통신망으로 송신하거나 보조저장매체 등으로 전달하는 경우에는 암호화가 요구된다. 선지는 전송·전달 상황의 암호화 의무를 그대로 설명한 것이다.
2번: O. 비밀번호와 바이오정보는 암호화하여 저장하여야 하고, 특히 비밀번호는 다시 풀 수 없도록 일방향 암호화로 저장하여야 한다. 선지는 저장 단계의 암호화 방식까지 정확히 적었다.
3번: O. 인터넷 구간과 인터넷 구간 및 내부망 사이의 중간 지점인 DMZ에 고유식별정보를 저장하는 경우에는 암호화가 필요하다. 선지는 고유식별정보의 저장 위치에 따른 추가 보호의무를 올바르게 설명한 것이다.
4번: X. 틀린 표현은 '상용 암호화 소프트웨어를 사용하여서는 아니 된다'이다. 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우에는 오히려 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

오답 포인트

4번은 금지 문구로 방향을 뒤집은 선지이다. '사용하여서는 아니 된다'라는 부정 표현에 끌리면 틀리기 쉽고, 실제 기준은 상용 암호화 소프트웨어 사용을 배제하는 것이 아니라 암호화 수단으로 허용한다는 점이 함정이다.

다시 나오면 이렇게 판단

먼저 대상 정보가 고유식별정보인지, 비밀번호인지, 바이오정보인지 구분한다. 다음으로 전송인지 저장인지, 일반 저장인지 DMZ·업무용 기기 저장인지 상황을 나눈다. 마지막으로 의무가 암호화인지, 일방향 암호화인지, 허용되는 암호화 수단이 무엇인지 확인하면 정답을 가를 수 있다.

암기 포인트

전송은 암호화, 비밀번호 저장은 일방향 암호화, 업무용 기기 고유식별정보 저장은 상용 암호화 소프트웨어도 허용된다.

NoteBase

문 19. RSA 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① 대표적인 비대칭 암호 알고리즘으로, 널리 사용되고 있다.

② 공개키 $\{e, n\}$이 주어지면 지수 및 모듈러 연산을 통해 n과 무관한 임의 크기의 평문 블록을 하나의 암호문 블록으로 암호화할 수 있다.

③ 공개키 $\{e, n\}$의 n을 소인수분해할 수 있으면 개인키 $\{d, n\}$의 d를 알아낼 수 있다.

④ 일반적으로 키의 길이가 길수록 안전성은 높아지지만 알고리즘 수행시간은 길어진다.

정답 2번

출제 포인트

이 문제는 RSA가 비대칭 공개키 암호라는 점과 평문 블록 크기가 모듈러스 n에 의해 제한된다는 점을 정확히 구분하는지를 묻는 문제이다.

핵심 개념

비대칭 암호는 공개키와 개인키를 서로 다르게 사용하는 암호 방식이다.
RSA는 공개키 (e, n), 개인키 (d, n)를 사용하는 대표적 공개키 암호이며, 평문은 $0 \le m < n$ 범위의 정수로 표현되어야 하므로 한 번에 암호화할 수 있는 블록 크기는 n과 무관하지 않다.

NoteBase

선지별 해설

① O
RSA는 가장 대표적인 공개키 기반 비대칭 암호 알고리즘 중 하나이며, 키 교환·전자서명·인증서 체계 등에서 널리 사용되어 왔다.

② X
틀린 부분은 "n과 무관한 임의 크기의 평문 블록"이라는 표현이다.
RSA에서 평문 블록은 모듈러스 n보다 작은 값으로 표현되어야 하므로 블록 크기는 n의 크기와 패딩 방식에 의해 제한된다.
올바르게는 "공개키 (e, n)가 주어지면 n보다 작은 범위로 표현된 평문 블록을 모듈러 지수 연산으로 암호화할 수 있다"이다.

③ O
공개키의 n을 소인수분해하여 p, q를 구하면 $\varphi(n) = (p-1)(q-1)$를 계산할 수 있고, 이어서 $ed \equiv 1 \pm od(n)$를 만족하는 d를 구할 수 있다. 따라서 n의 소인수분해 가능성은 RSA 안전성과 직접 연결된다.

④ O
RSA는 일반적으로 키 길이가 길수록 소인수분해 공격에 대한 저항성이 커지지만, 큰 정수에 대한 모듈러 거듭제곱 연산 비용이 증가하므로 암호화·복호화·서명 연산 시간이 길어진다.

오답 포인트

②는 RSA가 모듈러 지수 연산을 사용한다는 사실만 맞게 제시한 뒤, 평문 블록 크기 제한이 없다는 식으로 과장한 선지이다. 수험생이 "공개키 암호는 큰 데이터를 다룬다"는 막연한 인상만으로 보면 속기 쉽지만, RSA 평문은 항상 n보다 작은 정수 범위로 들어가야 한다.

다시 나오면 이렇게 판단

RSA 관련 선지는 먼저 공개키 암호인지, 다음으로 평문이 n보다 작은 값으로 표현되어야 하는지를 확인하면 된다. 선지에 "임의 크기", "제한 없이", "n과 무관하게" 같은 표현이 나오면 블록 크기 제한을 위반하는지부터 점검하면 된다.

암기 포인트

RSA는 공개키 암호이고, 평문 블록은 항상 n보다 작아야 한다.

NoteBase

문 20. 중간 시스템(reflector)을 이용해서 서비스 거부(DoS)를 발생시키는 반사(reflection) DDoS 공격에 대한 설명으로 옳지 않은 것은?

① 공격 대상의 주소를 시작 주소로 갖는 패킷을 중간 시스템에 보낸다.

② 중간 시스템으로 네트워크 연결이 좋은 고용량의 네트워크 서버나 라우터가 이용될 수도 있다.

③ 사전에 중간 시스템 내부에 공격자의 명령 수행을 위한 비정상 프로그램이 작동하도록 해야 한다.

④ 중간 시스템이 요청 메시지에 대해서 큰 응답 메시지를 생성하는 서비스를 이용하면 공격 대상 시스템에 더 많은 피해를 줄 수 있다.

정답 3번

출제 포인트

이 문제는 반사 DDoS의 성립 조건과 증폭형 반사 공격의 특징, 그리고 봇넷형 DDoS와의 차이를 구별하는 문제이다.

핵심 개념

반사 DDoS는 공격자가 출발지 IP를 피해자 주소로 위조하여 제3의 시스템이 피해자에게 응답을 보내게 만드는 공격이다.
증폭 DDoS는 작은 요청에 대해 큰 응답을 돌려주는 서비스를 이용해 피해자에게 가는 트래픽 양을 더 키우는 방식이다.
봇넷형 DDoS는 미리 악성코드에 감염된 좀비 PC나 서버가 직접 공격 트래픽을 보내는 방식이므로, 반사 DDoS의 중간 시스템과는 성립 조건이 다르다.

NoteBase

선지별 해설

① O
공격자는 피해자의 IP 주소를 출발지 주소로 위조한 요청 패킷을 중간 시스템에 보낸다. 그러면 중간 시스템의 응답이 공격자 대신 피해자에게 돌아가므로 반사 공격의 기본 구조에 맞다.

② O
반사에 이용되는 중간 시스템은 외부와 연결이 좋고 대역폭이 큰 서버나 라우터일수록 더 많은 응답 트래픽을 보낼 수 있다. 따라서 고용량 네트워크 자원이 반사원으로 이용될 수 있다는 설명은 맞다.

③ X
틀린 부분은 "사전에 중간 시스템 내부에 공격자의 명령 수행을 위한 비정상 프로그램이 작동하도록 해야 한다"는 표현이다. 반사 DDoS의 중간 시스템은 반드시 악성코드에 감염되어 있을 필요가 없고, 정상적으로 동작하는 공개 서비스가 응답만 해도 반사에 이용될 수 있다. 올바르게는 "출발지 주소를 피해자로 위조한 요청에 대해 중간 시스템이 피해자에게 응답하도록 만들면 된다"이다.

④ O
중간 시스템이 작은 요청보다 훨씬 큰 응답을 생성하는 서비스라면 피해자에게 전달되는 트래픽이 증폭된다. 이는 DNS, NTP 같은 증폭형 반사 공격의 핵심 원리이므로 맞는 설명이다.

오답 포인트

3번은 반사 DDoS를 봇넷형 DDoS와 섞어 놓은 선지이다. "중간 시스템 내부의 비정상 프로그램"이라는 표현이 나오면 감염된 좀비를 이용하는 직접 공격인지, 정상 서비스의 응답을 이용하는 반사 공격인지를 먼저 갈라서 보아야 한다.

다시 나오면 이렇게 판단

반사 공격 문제는 먼저 출발지 IP 위조가 있는지, 다음으로 제3자가 피해자에게 응답하는 구조인지, 마지막으로 중간 시스템이 감염된 좀비인지 정상 응답 서버인지를 확인하면 된다. 감염이 필수라고 하면 반사 DDoS보다는 봇넷형 DDoS 설명일 가능성이 크다.

암기 포인트

반사 DDoS는 "위조한 출발지, 정상 중간 시스템의 응답"이고, 봇넷 DDoS는 "감염된 좀비의 직접 전송"이다.

NoteBase