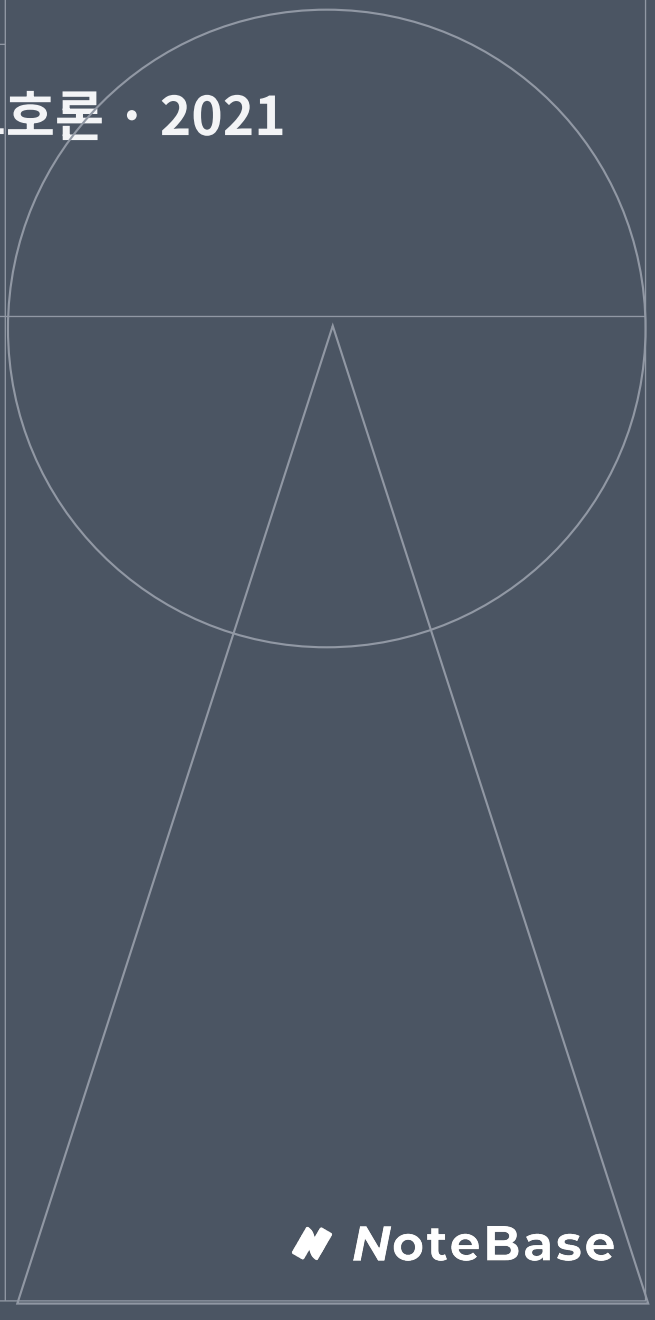
기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/서울시/7급 · 정보보호론 · 2021

공무원/서울시/7급 · 정보보호론 · 2021

문 1. 해시함수를 사용하여 변환 가능한 모든 해시값을 계산한 뒤, 이 정보를 사용하여 비밀번호를 공격하는 기법은?

① 무차별 대입(Brute-Force) 공격

② 퍼징(Fuzzing) 공격

③ 알려진 평문(Known Plaintext) 공격

④ 레인보우 테이블(Rainbow Table) 공격

정답 4번

출제 포인트

이 문제는 비밀번호 해시 공격 방식 중 사전 계산형 공격과 다른 공격 기법을 구별하는 문제이다.

핵심 개념

브루트포스 공격은 가능한 비밀번호를 하나씩 직접 대입해 찾는 방식이다.
퍼징은 비정상 입력이나 임의 입력을 넣어 프로그램 오류와 취약점을 찾는 방식이다.
알려진 평문 공격은 평문과 그에 대응하는 암호문을 알고 있을 때 키나 암호 체계를 추론하는 암호해독 방식이다.
레인보우 테이블 공격은 가능한 평문 후보의 해시값을 미리 계산한 표를 이용해 해시값에서 원문 후보를 빠르게 찾는 방식이다.

NoteBase

기출OX 해설집 · 공무원/서울시/7급 · 정보보호론 · 2021

선지별 해설

① X
무차별 대입 공격은 가능한 비밀번호를 실시간으로 하나씩 넣어 보는 방식이다.
틀린 부분은 '무차별 대입'이다. 제시문은 직접 대입이 아니라 해시값을 미리 계산해 둔 정보를 이용하는 방식이다.
올바르게는 브루트포스 공격은 사전 계산표 없이 후보를 순차 대입하는 공격이다.

② X
퍼징은 프로그램에 비정상 입력을 넣어 오동작이나 취약점을 찾는 기법이다.
틀린 부분은 '퍼징'이다. 제시문은 입력 검증 취약점 탐지가 아니라 비밀번호 해시 역추적을 설명한다.
올바르게는 퍼징은 예외 상황을 유발해 결함을 찾는 기법이다.

③ X
알려진 평문 공격은 평문과 암호문 쌍을 이미 알고 있을 때 암호키나 암호 알고리즘의 약점을 추론하는 기법이다.
틀린 부분은 '알려진 평문'이다. 제시문은 평문-암호문 쌍을 이용하는 암호해독이 아니라 해시 사전으로 비밀번호를 찾는 공격이다.
올바르게는 알려진 평문 공격은 암호화된 메시지 분석에 쓰이는 고전적 암호해독 방식이다.

④ O
레인보우 테이블 공격은 가능한 입력값들의 해시를 미리 계산해 표로 저장해 두고, 유출된 해시값과 대조하여 원문 후보를 찾는 공격이다.
문장의 '변환 가능한 모든 해시값을 계산한 뒤, 이 정보를 사용'이라는 설명과 정확히 부합한다.

오답 포인트

브루트포스 공격과 레인보우 테이블 공격은 모두 비밀번호를 찾는다는 점이 같아 헷갈리기 쉽다. 그러나 브루트포스는 그때그때 직접 대입하고, 레인보우 테이블은 해시를 미리 계산해 둔 표를 이용한다는 점이 결정적 차이이다.

다시 나오면 이렇게 판단

문장에 '미리 계산해 둔다', '표를 만들어 둔다', '해시값과 대조한다'가 나오면 레인보우 테이블 공격을 먼저 떠올리면 된다. 반대로 '하나씩 직접 시도한다'가 핵심이면 브루트포스 공격이다.

암기 포인트

브루트포스는 직접 대입, 레인보우 테이블은 미리 계산한 해시표 이용이다.

NoteBase

문 2. 블록 암호의 운용 모드에 대한 설명으로 가장 옳은 것은?

① Electronic Codebook 모드는 초기화 벡터가 필요하다.

② Cipher Feedback 모드는 재전송 공격에 취약하다고 알려져 있다.

③ Cipher Block Chaining 모드는 복호화 과정에서도 암호화 알고리즘이 사용된다.

④ Counter 모드에서 암호문의 중간 부분을 복호화하기 위해서는 해당 부분 이전의 모든 블록들을 복호화해야 한다.

정답 2번

출제 포인트

블록 암호 운용 모드별 IV 필요 여부, 복호 시 사용하는 연산, 임의 접근 가능 여부를 구별하는 문제이다.

핵심 개념

ECB는 각 블록을 서로 독립적으로 암호화하는 모드이며 IV가 필요하지 않다.
CFB는 이전 암호문과 IV를 피드백해 블록 암호를 스트림처럼 사용하는 모드이며 무결성이나 신선성을 자체적으로 보장하지 않는다.
CBC는 이전 암호문 블록과 연쇄되어 동작하는 모드이며 복호 시에는 복호 알고리즘이 필요하다.
CTR는 카운터 값을 암호화해 키스트림을 만드는 모드이므로 블록별 독립 처리와 중간 블록 임의 접근이 가능하다.

선지별 해설

1번 X: ECB 모드는 각 평문 블록을 독립적으로 처리하므로 초기화 벡터를 사용하지 않는다. 틀린 표현은 "초기화 벡터가 필요하다"이며, 올바르게는 "ECB 모드는 초기화 벡터가 필요하지 않다"이다.
2번 O: CFB 모드는 기밀성만 제공할 뿐 재전송 여부를 스스로 판별하지 못하므로 별도의 순서번호나 인증값이 없으면 이전 암호문을 다시 보내는 재전송 공격에 취약하다.
3번 X: CBC 복호는 $P_i = D_k(C_i) \oplus C_{i-1}$로 수행되므로 복호 과정에서 필요한 것은 복호 알고리즘이다. 틀린 표현은 "복호화 과정에서도 암호화 알고리즘이 사용된다"이며, 올바르게는 "CBC 모드의 복호화 과정에서는 복호 알고리즘이 사용된다"이다.
4번 X: CTR 모드는 각 블록의 카운터만 알면 해당 블록 키스트림을 바로 만들어 복호할 수 있으므로 중간 블록만 독립적으로 복호할 수 있다. 틀린 표현은 "이전의 모든 블록들을 복호화해야 한다"이며, 올바르게는 "해당 블록의 카운터 값만 알면 중간 부분도 바로 복호할 수 있다"이다.

오답 포인트

③은 CFB·OFB·CTR처럼 복호에도 암호화 알고리즘을 쓰는 모드와 CBC를 뒤섞으면 틀리기 쉽다. ④는 CBC의 연쇄 의존성을 CTR에 잘못 옮겨 놓은 함정이다.

NoteBase

다시 나오면 이렇게 판단

모드 문제는 먼저 IV 필요 여부를 보고, 다음으로 복호 시 암호화 알고리즘을 쓰는지 복호 알고리즘을 쓰는지를 가른 뒤, 마지막으로 중간 블록 임의 접근 가능 여부를 확인하면 정리가 된다.

암기 포인트

ECB는 독립, CBC는 체인, CFB는 피드백, CTR는 카운터로 랜덤 접근이 가능하다.

NoteBase

문 3. Single-Sign On을 실현하기에 적합한 기술로 가장 옳은 것은?

① DTLS

② TLS

③ OCSP

④ Kerberos

정답 4번

출제 포인트

이 문제는 Single Sign-On의 구현 방식과 전송 보안, 인증서 상태 확인 기술을 구별할 수 있는지를 묻는다.

핵심 개념

Kerberos는 티켓 기반의 네트워크 인증 프로토콜로, 한 번 인증한 뒤 여러 서비스에 재인증 없이 접근하는 SSO 구현에 적합하다.
TLS는 통신 구간을 암호화하는 전송 계층 보안 기술이다.
DTLS는 TLS를 UDP 환경에 맞게 확장한 전송 보안 기술이다.
OCSP는 인증서 폐지 상태를 온라인으로 확인하는 프로토콜이다.

선지별 해설

1번 X: DTLS는 UDP 기반 통신에서 기밀성과 무결성을 제공하는 전송 보안 기술이다. 틀린 표현은 SSO 구현 기술로 본 점이다. 올바르게는 UDP 환경의 TLS 계열 보안 프로토콜이다.
2번 X: TLS는 클라이언트와 서버 사이의 통신 구간을 보호하는 기술이다. 틀린 표현은 SSO를 실현하는 핵심 기술로 본 점이다. 올바르게는 통신 채널을 암호화하는 기술이지, 여러 서비스 간 통합 인증 자체를 담당하는 기술은 아니다.
3번 X: OCSP는 인증서가 폐지되었는지 실시간으로 조회하는 프로토콜이다. 틀린 표현은 사용자 통합 인증 기술로 본 점이다. 올바르게는 PKI 환경에서 인증서 상태를 확인하는 기술이다.
4번 O: Kerberos는 KDC가 발급한 티켓을 이용해 사용자를 인증하고, 동일한 인증 결과를 여러 서비스에서 활용할 수 있게 한다. 따라서 SSO를 실현하기에 가장 적합한 기술이다.

오답 포인트

TLS와 DTLS는 이름 때문에 인증 자체를 담당하는 것으로 오해하기 쉽고, OCSP도 인증서 관련 기술이라 인증과 혼동하기 쉽다. 이 문항의 함정은 보안 기술 전반을 모두 인증 기술처럼 보이게 배열한 점이다.

NoteBase

다시 나오면 이렇게 판단

보기마다 역할을 먼저 구분하면 된다. 통합 인증과 재사용이면 Kerberos 같은 인증 체계이고, 통신 구간 보호이면 TLS·DTLS이며, 인증서 상태 조회이면 OCSP이다.

암기 포인트

SSO는 Kerberos, 통신 암호화는 TLS·DTLS, 인증서 상태 확인은 OCSP이다.

NoteBase

문 4. 방화벽(Firewall), 침입탐지시스템(IDS) 및 침입방지시스템(IPS)에 대한 설명으로 가장 옳지 않은 것은?

① Shodan은 stateful inspection을 수행하는 2세대 방화벽의 일종이다.

② Snort는 대표적인 오픈소스 IPS이다.

③ IPtables는 linux의 패킷 필터 기반 방화벽의 규칙들을 관리하는 도구이다.

④ UFW는 linux에서 사용되는 방화벽 설정 툴이다.

정답 1번

출제 포인트

이 문제는 방화벽, IDS, IPS와 관련 도구의 역할을 구분할 수 있는지를 묻는 문제이다.

핵심 개념

방화벽은 네트워크 트래픽을 정책에 따라 허용하거나 차단하는 통제 장비이다. IDS는 침입 시도를 탐지하고 경고하는 시스템이고, IPS는 탐지 결과를 바탕으로 트래픽을 능동 차단하는 시스템이다. Shodan은 인터넷에 노출된 장비와 서비스를 검색하는 검색엔진이고, iptables는 리눅스 패킷 필터 규칙을 관리하는 도구이며, UFW는 이를 쉽게 설정하도록 돕는 프런트엔드 성격의 방화벽 설정 도구이다.

선지별 해설

① X. 틀린 부분은 "Shodan은 stateful inspection을 수행하는 2세대 방화벽의 일종"이라는 표현이다. Shodan은 방화벽이 아니라 인터넷에 공개된 서버, IoT 기기, 포트 상태 등을 수집해 검색하게 해 주는 검색엔진이다.
② O. Snort는 대표적인 오픈소스 네트워크 침입탐지 도구이며, 인라인 모드로 운용하면 IPS로도 활용할 수 있으므로 대표적 오픈소스 IPS라는 설명도 수용된다.
③ O. iptables는 리눅스 netfilter 기반에서 패킷 필터링, NAT, 포트포워딩 등의 규칙을 관리하는 명령행 도구이다.
④ O. UFW는 Uncomplicated Firewall의 약자로, 리눅스에서 방화벽 규칙을 간편하게 설정하도록 돕는 도구이다.

오답 포인트

Shodan을 보안 제품명처럼 착각하면 ①을 고르지 못한다. 이 문항은 장비형 보안통제 수단과 검색 서비스 이름을 섞어 놓아, 이름의 익숙함만으로 판단하는지를 노린 문제이다.

NoteBase

다시 나오면 이렇게 판단

선지에 나온 대상이 방화벽 장비인지, 침입탐지·차단 소프트웨어인지, 단순 검색 서비스인지부터 분류하면 된다. 제품이나 도구의 핵심 기능이 트래픽 통제인지, 탐지인지, 검색인지 한 축으로 세우면 빠르게 정오를 가를 수 있다.

암기 포인트

Shodan은 검색엔진, Snort는 IDS/IPS, iptables와 UFW는 리눅스 방화벽 관리 도구이다.

NoteBase

문 5. <보기>에서 설명하는 것으로 가장 옳은 것은?

<보기>
• 공개적으로 알려진 사이버보안 취약점을 규격화된 목록으로 만들어 식별하는 체계이다.
• 목록에는 취약점의 명칭(일련 번호 포함), 취약성 및 노출 개요, 대응 참조 사항 등이 포함된다.

① Honeypot
② CVE
③ VPN
④ UTM

정답 2번

출제 포인트

공개된 보안 취약점을 표준화된 식별 번호와 설명으로 관리하는 체계가 CVE인지 묻는 문제이다.

핵심 개념

CVE는 공개적으로 알려진 취약점과 노출 항목에 공통 식별번호를 부여해 이름, 개요, 참조 정보를 관리하는 체계이다.
Honeypot은 공격을 유인해 행위를 관찰하는 미끼 시스템이다.
VPN은 공중망 위에 암호화된 사설 통신 터널을 만드는 기술이다.
UTM은 방화벽, IDS/IPS, 안티바이러스 등을 통합한 보안 관리 장비 또는 솔루션이다.

선지별 해설

① X: Honeypot은 공격자를 유인해 침입 행위를 탐지·분석하는 미끼 시스템이다. 틀린 부분은 취약점 목록 체계로 본 점이다. 올바르게는 공격 유인 및 관찰용 시스템이다.
② O: CVE는 공개적으로 알려진 취약점에 일련번호를 부여하고 취약성 설명, 노출 개요, 참조 사항을 함께 제공하는 체계이므로 보기의 설명과 일치한다.
③ X: VPN은 Virtual Private Network로, 공중망에서 암호화 터널을 통해 사설망처럼 통신하는 기술이다. 틀린 부분은 취약점 식별 체계로 본 점이다. 올바르게는 안전한 원격 통신을 위한 가상사설망이다.
④ X: UTM은 Unified Threat Management로 여러 보안 기능을 통합 제공하는 보안 솔루션이다. 틀린 부분은 공개 취약점 목록 체계로 본 점이다. 올바르게는 통합보안관리 장비 또는 솔루션이다.

오답 포인트

보기의 핵심 단어는 '공개적으로 알려진 취약점', '규격화된 목록', '일련 번호 포함'이다. 보안 분야 약어라는 공통점만 보고 Honeypot, VPN, UTM을 고르면 기능 중심 용어와 취약점 식별 체계를 구분하지 못한 것이다.

NoteBase

다시 나오면 이렇게 판단

선지를 볼 때 먼저 그것이 취약점 식별 체계인지, 보안 장비인지, 통신 기술인지, 공격 유인 시스템인지 범주를 나눈다. 공개 취약점에 번호를 붙여 관리한다는 설명이 나오면 CVE로 판단할 수 있다.

암기 포인트

CVE는 취약점 번호표, Honeypot은 미끼, VPN은 암호화 터널, UTM은 통합보안이다.

NoteBase

문 6. RSA에서 모듈로 연산에 사용되는 $n = 91$이고 어떤 사용자의 비밀키에 사용되는 $d = 7$이라고 할 때, 이 사용자의 공개키에 사용되는 e로 가장 옳은 것은?

① 13

② 31

③ 41

④ 존재하지 않는다.

정답 2번

출제 포인트

이 문제는 RSA에서 ed ≡ 1 ±od(n)를 만족하는 공개지수 e를 구할 수 있는지를 묻는다.

조건 정리

주어진 값: $n = 91$, $d = 7$
구해야 할 값: 공개키 지수 e
주의할 조건: n을 소인수분해해 $\varphi(n)$를 먼저 구한 뒤, d의 모듈러 역원을 찾아야 한다.

사용할 공식

공식: ed ≡ 1 ±od(n)
또한 $n = pq$이면 $\varphi(n) = (p-1)(q-1)$이다.
이 공식을 쓰는 이유: RSA에서 공개지수 e와 비밀지수 d는 $\varphi(n)$에 대해 서로 역원 관계이기 때문이다.

계산 과정

1. $91 = 7 \times 13$이므로 $p = 7$, $q = 13$이다.
2. $\varphi(91) = (7-1)(13-1) = 6 \times 12 = 72$이다.
3. 7e ≡ 1 ±od72를 만족하는 e를 찾으면 된다.
4. $7 \times 31 = 217 = 72 \times 3 + 1$이므로 $7 \cdot 31 \equiv 1 \pm od72$이다.
5. 따라서 $e = 31$이다.

NoteBase

선지별 해설

① X: $7 \times 13 = 91$이고 $91 \equiv 19 \pm \mathrm{od}72$이므로 역원이 아니다. 틀린 표현은 13이 공개지수라는 점이고, 올바르게는 $e = 31$이다.
② O: $7 \times 31 = 217$이고 $217 \equiv 1 \pm \mathrm{od}72$이므로 $d = 7$의 모듈러 역원이다. 따라서 공개키에 쓰이는 e로 옳다.
③ X: $7 \times 41 = 287$이고 $287 \equiv 71 \pm \mathrm{od}72$이므로 1이 아니다. 71은 -1에 해당하므로 거의 맞아 보이지만 역원 조건은 만족하지 않는다. 올바르게는 $e = 31$이다.
④ X: $\gcd(7, 72) = 1$이므로 7의 모듈러 역원은 반드시 존재한다. 틀린 표현은 역원이 없다는 점이고, 올바르게는 $e = 31$이 존재한다.

오답 포인트

공개지수 e를 n에 대해 역원을 구하는 것으로 착각하면 틀린다. RSA에서는 n을 소인수분해해 $\varphi(n)$를 구한 뒤, d의 역원을 $\varphi(n)$에 대해 찾아야 한다. ③처럼 -1이 나오는 값도 정답처럼 보이기 쉬운 함정이다.

다시 나오면 이렇게 판단

RSA 수치 문제는 n 소인수분해 → $\varphi(n)$ 계산 → $\mathrm{ed} \equiv 1 \pm \mathrm{od(n)}$ 확인 순서로 판단하면 된다. 마지막에는 후보값을 직접 곱해 나머지가 1인지 검산하면 된다.

암기 포인트

RSA에서 공개지수와 비밀지수는 $\varphi(n)$에 대한 역원 관계이고, $n = pq$이면 $\varphi(n) = (p-1)(q-1)$이다.

NoteBase

문 7. IPSec에 대한 설명으로 가장 옳지 않은 것은?

① IPSec은 전송모드와 터널모드로 동작할 수 있다.

② IPSec은 데이터 송신자에 대한 인증과 재전송(Replay) 공격 방지 기능을 제공할 수 있다.

③ IPSec의 키 관리 프로토콜에서는 Diffie-Hellman 기법을 개선한 Oakley 기법을 사용하여 키 교환을 수행할 수 있다.

④ IPSec은 전송 계층인 TCP 계층의 상위 계층인 세션 계층 암호화 기법이므로, 응용 프로그램에 대한 투명성(transparency)을 갖는다.

정답 4번

출제 포인트

이 문제는 IPSec의 동작 계층, 제공 기능, 키 교환 방식, 전송 모드와 터널 모드를 정확히 구별하는지를 묻는 문제이다.

핵심 개념

IPSec은 IP 계층에서 패킷 단위로 인증, 무결성, 기밀성을 제공하는 보안 프로토콜군이다.
전송 모드는 원래 IP 헤더를 유지한 채 상위 계층 데이터만 보호하고, 터널 모드는 원래 IP 패킷 전체를 새로운 IP 헤더로 감싸 보호한다.
응용 프로그램에 대한 투명성은 세션 계층에서 동작해서가 아니라 네트워크 계층에서 동작하기 때문에 생긴다.

NoteBase

선지별 해설

① O
IPSec은 전송 모드와 터널 모드를 모두 지원한다. 호스트 간 통신에서는 전송 모드, 게이트웨이 간 VPN에서는 터널 모드가 대표적으로 쓰인다.

② O
IPSec은 데이터 출처 인증과 재전송 공격 방지 기능을 제공할 수 있다. 인증 기능과 시퀀스 번호 기반의 anti-replay 기능을 통해 동일 패킷의 반복 전송 공격을 막는다.

③ O
IPSec의 키 관리에서는 Diffie-Hellman 기반의 키 교환을 사용하며, 전통적으로 IKE가 ISAKMP/Oakley 체계 위에서 동작한다고 설명한다. 따라서 Oakley 기법을 사용하여 키 교환을 수행할 수 있다는 진술은 옳다.

④ X
틀린 부분은 "TCP 계층의 상위 계층인 세션 계층 암호화 기법"이라는 표현이다. IPSec은 세션 계층 암호화가 아니라 네트워크 계층인 IP 계층에서 동작하는 보안 프로토콜군이다. 올바르게는 "IPSec은 IP 계층에서 동작하므로 응용 프로그램에 대해 비교적 투명하게 보안 기능을 제공할 수 있다."라고 고쳐야 한다.

오답 포인트

④는 "응용 프로그램에 대한 투명성"이라는 맞는 효과에 "세션 계층"이라는 틀린 계층 정보를 붙여 함정을 만든 선지이다. 효과가 맞는다고 해서 근거가 맞는 것은 아니므로, 보안 기술의 동작 계층을 따로 확인해야 한다.

다시 나오면 이렇게 판단

IPSec이 나오면 먼저 동작 계층이 IP 계층인지 확인한 뒤, 모드가 전송 모드와 터널 모드인지, 기능이 인증·무결성·기밀성·재전송 방지인지, 키 교환이 Diffie-Hellman 기반인지 순서대로 대조하면 된다.

암기 포인트

IPSec은 IP 계층에서 동작하고 전송 모드와 터널 모드를 지원하며, 키 교환은 Diffie-Hellman 기반 IKE/Oakley로 이해하면 된다.

NoteBase

문 8. 포맷 스트링(format string) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 취약한 함수를 이용한다는 점에서 버퍼 오버플로우와 공통점이 있으나, 버퍼 오버플로우 공격이 알려지기 훨씬 이전에 발견되었다.

② C 언어의 printf 함수가 대표적인 공격 대상이다.

③ %x 토큰을 적절히 활용하면 공격자는 메모리 내용을 출력하여 확인할 수 있다.

④ %n 토큰을 적절히 활용하면 공격자는 메모리의 내용을 변경할 수 있다.

정답 1번

출제 포인트

포맷 스트링 취약점에서 `%x`는 메모리 읽기, `%n`은 메모리 쓰기에 악용된다는 점과 버퍼 오버플로우와의 역사적 선후를 구별하는 문제이다.

핵심 개념

포맷 스트링 취약점은 사용자 입력이 데이터가 아니라 포맷 문자열 자체로 해석될 때 `%x`, `%s`, `%n` 같은 지정자를 통해 메모리를 읽거나 쓸 수 있는 취약점이다.
버퍼 오버플로우는 버퍼 경계를 넘는 입력으로 인접 메모리를 덮어쓰는 취약점이다.
두 취약점은 모두 메모리 안전성과 관련되지만, 악용 방식은 다르며 버퍼 오버플로우가 더 오래전부터 알려져 왔다.

선지별 해설

① X. 틀린 부분은 `버퍼 오버플로우 공격이 알려지기 훨씬 이전에 발견되었다`는 표현이다. 버퍼 오버플로우는 포맷 스트링 취약점보다 훨씬 오래전부터 알려진 대표적 메모리 오염 취약점이다. 올바르게는 `취약한 함수 사용이라는 공통점은 있으나, 포맷 스트링 취약점은 버퍼 오버플로우보다 뒤늦게 널리 알려졌다`가 맞다.
② O. C 언어의 `printf` 계열 함수는 사용자 입력을 포맷 문자열로 그대로 넘길 때 포맷 스트링 취약점이 발생하는 대표적 대상이다. `printf(user_input);` 같은 코드가 전형적 사례이다.
③ O. `%x`는 스택에 있는 값을 16진수로 출력하게 하므로 공격자가 메모리 내용을 읽어내는 데 악용할 수 있다. 따라서 정보 유출형 동작에 해당한다.
④ O. `%n`은 지금까지 출력한 문자 수를 지정된 주소에 기록하므로 메모리 쓰기 공격에 악용될 수 있다. 직접 임의 문자열을 쓰는 것은 아니지만, 기록값을 조절해 메모리 내용을 변경할 수 있다.

오답 포인트

①은 역사적 선후를 비틀어 놓은 선지이다. `%x`와 `%n`의 기능만 외우고 형식 문자열 취약점의 등장 배경을 놓치면 ③, ④가 익숙하다는 이유로 ①을 지나치기 쉽다.

NoteBase

다시 나오면 이렇게 판단

포맷 스트링 문제는 대표 함수가 `printf` 계열인지, 읽기 기능은 `%x` 같은 출력 지정자인지, 쓰기 기능은 `%n`인지, 그리고 버퍼 오버플로우보다 나중에 부각된 취약점인지의 네 축으로 판단하면 된다.

암기 포인트

포맷 스트링은 `printf` 계열, 읽기는 `%x`, 쓰기는 `%n`, 역사적으로는 버퍼 오버플로우 뒤에 부각된 취약점이다.

NoteBase

문 9. AES에 대한 설명으로 가장 옳은 것은?

① AES-192는 한 번의 수행으로 192비트의 평문 블록을 암호화한다.

② Daemen과 Rijmen이 설계한 Rijndael 알고리즘에 기반한다.

③ 유한체 $GF(2^{256})$ 상의 연산을 이용하여 설계되었다.

④ 치환(substitution) 및 전치(permutation) 연산을 반복하는 페이스텔(Feistel) 구조를 사용한다.

정답 2번

출제 포인트

이 문제는 AES의 기반 알고리즘, 블록 크기, 유한체 연산 단위, 내부 구조를 정확히 구별하는지를 묻는 문제이다.

핵심 개념

AES는 Rijndael을 기반으로 표준화된 대칭키 블록암호이며, 블록 크기는 키 길이와 무관하게 128비트로 고정된다.
AES의 바이트 단위 연산은 $GF(2^8)$에서 수행되고, 구조는 Feistel이 아니라 SPN(Substitution-Permutation Network)이다.

선지별 해설

① X: 틀린 부분은 "192비트의 평문 블록"이다. AES-192에서 192비트는 키 길이이고, 평문 블록 길이는 128비트이다. 올바르게는 "AES-192는 192비트 키를 사용하여 128비트 평문 블록을 암호화한다"이다.
② O: AES는 Joan Daemen과 Vincent Rijmen이 설계한 Rijndael 알고리즘을 기반으로 표준화된 블록암호이므로 옳다.
③ X: 틀린 부분은 "GF(2^256)"이다. AES는 바이트 단위 연산을 위해 $GF(2^8)$을 사용한다. 올바르게는 "유한체 $GF(2^8)$ 상의 연산을 이용하여 설계되었다"이다.
④ X: 틀린 부분은 "페이스텔(Feistel) 구조"이다. AES는 치환과 전치를 반복하는 점은 맞지만 구조 자체는 SPN이다. 올바르게는 "치환 및 전치 연산을 반복하는 SPN 구조를 사용한다"이다.

오답 포인트

AES-192의 192를 블록 길이로 착각하거나, 유한체 차수를 크게 쓰면 더 복잡해 보인다는 이유로 $GF(2^{256})$를 고르기 쉽다. 또한 "치환과 전치의 반복"이라는 표현만 보고 DES와 같은 Feistel 구조로 오인하기 쉽다.

다시 나오면 이렇게 판단

AES 계열 문제는 먼저 키 길이와 블록 길이를 분리해서 보고, 그다음 바이트 연산이 $GF(2^8)$인지와 구조가 SPN인지 확인하면 빠르게 판단할 수 있다.

NoteBase

암기 포인트

AES는 128비트 블록, Rijndael 기반, $GF(2^8)$ 연산, SPN 구조이다.

NoteBase

문 10. <보기>의 설명에 맞는 접근 제어 모델로 가장 옳은 것은?

<보기>
• 정보 소유자가 정보의 보안 수준을 결정하고 이에 대한 접근 권한도 설정할 수 있는 모델이다.
• 이 모델의 대표적인 사례로는 Linux 및 Windows 운영체제에서 파일 시스템 접근 권한을 설정하는 방법이 있다.

① 임의적 접근 제어(Discretionary Access Control) 모델
② 강제적 접근 제어(Mandatory Access Control) 모델
③ 역할기반 접근 제어(Role–Based Access Control) 모델
④ 벨–라파둘라(Bell–LaPadula) 모델

정답 1번

출제 포인트

정보 소유자가 권한을 정하는 임의적 접근 제어와, 보안 정책·역할·기밀성 규칙으로 통제하는 다른 접근 제어 모델을 구별하는 문제이다.

핵심 개념

DAC는 객체 소유자가 다른 사용자에게 읽기·쓰기·실행 권한을 부여하거나 회수할 수 있는 모델이다. 결정 차이축은 권한 결정 주체이며 키워드는 소유자 재량이다.
MAC는 시스템이 보안 등급과 정책에 따라 권한을 강제하는 모델이다. 결정 차이축은 중앙 정책 강제이며 키워드는 보안 등급과 레이블이다.
RBAC는 사용자에게 직접 권한을 주기보다 역할에 권한을 묶고 사용자를 역할에 배정하는 모델이다. 결정 차이축은 직무 역할이며 키워드는 역할 기반 할당이다.
Bell-LaPadula는 기밀성 유지를 위한 대표적 강제적 접근 제어 모델이다. 결정 차이축은 기밀성 규칙이며 키워드는 no read up, no write down이다.

NoteBase

선지별 해설

① O
정보 소유자가 보안 수준과 접근 권한을 정할 수 있다는 설명은 DAC의 핵심이다. Linux와 Windows의 파일 권한 설정도 대표적인 DAC 사례이다.
② X
틀린 부분은 보기의 설명을 강제적 접근 제어와 연결한 점이다. MAC는 객체 소유자가 임의로 권한을 정하는 방식이 아니라 시스템 정책과 보안 레이블에 따라 중앙에서 권한을 강제한다. 올바르게는 "강제적 접근 제어는 시스템이 보안 등급과 규칙에 따라 접근을 통제하는 모델"이다.
③ X
틀린 부분은 소유자 재량형 설명을 역할기반 접근 제어와 연결한 점이다. RBAC는 사용자별 재량이 아니라 역할별 권한 묶음이 기준이다. 올바르게는 "역할기반 접근 제어는 직무 역할에 권한을 할당하고 사용자를 역할에 배정하는 모델"이다.
④ X
틀린 부분은 일반적인 소유자 권한 설정 모델을 Bell-LaPadula 모델로 본 점이다. Bell-LaPadula는 기밀성 보호를 위한 MAC 계열 모델로, 상위 등급 읽기 금지와 하위 등급 쓰기 금지 같은 규칙이 핵심이다. 올바르게는 "Bell-LaPadula 모델은 기밀성 중심의 강제적 접근 제어 모델"이다.

오답 포인트

DAC와 MAC를 모두 접근 통제라는 큰 범주로만 외우면 소유자 재량인지, 시스템 정책 강제인지가 흐려진다. 이 문제는 보기의 "정보 소유자가"와 "파일 시스템 권한 설정"이라는 표현이 DAC를 직접 가리킨다는 점을 묻는다.

다시 나오면 이렇게 판단

접근 권한을 누가 결정하는지를 먼저 본다. 소유자가 정하면 DAC, 보안 등급과 중앙 정책이 강제하면 MAC, 역할이 기준이면 RBAC, 기밀성 규칙이 전면에 나오면 Bell-LaPadula로 판단할 수 있다.

암기 포인트

DAC는 소유자 재량, MAC는 정책 강제, RBAC는 역할 기준, Bell-LaPadula는 기밀성 규칙이다.

NoteBase

문 11. DoS공격에 대한 설명으로 가장 옳지 않은 것은?

① HTTP GET Flooding 공격: TCP 3-Way 핸드셰이킹 과정을 통해 공격 대상 시스템에 정상적으로 접속한 뒤 HTTP의 GET Method로 특정 페이지를 무한 실행한다.

② 동적 HTTP Request Flooding 공격: 요청 페이지를 변경하여 웹 페이지를 지속적으로 요청한다.

③ Slow HTTP Header DoS(Slowloris) 공격: 웹 서버에 ID 및 Password, 게시글, 첨부 파일 등을 전송할 때 사용하는 HTTP POST 메시지에서 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여 전송한다.

④ Mail Bomb: 각 사용자에게 할당된 디스크 공간 이상의 메일을 보내 더 이상 메일을 받을 수 없게 하는 공격이다.

정답 3번

출제 포인트

이 문제는 웹 기반 DoS 공격 기법의 동작 원리와 서로 비슷한 슬로우 공격 계열의 차이를 구별하는 문제이다.

핵심 개념

HTTP GET Flooding은 정상 세션을 맺은 뒤 GET 요청을 대량 반복해 서버 자원을 소모시키는 공격이다.
동적 HTTP Request Flooding은 요청 URL이나 파라미터를 계속 바꾸어 캐시 우회를 노리면서 웹 자원을 지속적으로 소모시키는 공격이다.
Slowloris는 요청 헤더를 끝까지 보내지 않고 조금씩 전송해 연결을 오래 점유하는 Slow HTTP Header DoS이다.
Mail Bomb는 사용자 메일함 용량을 초과할 만큼 메일을 보내 저장 공간을 고갈시키는 서비스 거부 공격이다.

NoteBase

선지별 해설

① O
TCP 3-way 핸드셰이킹으로 정상 연결을 맺은 뒤 HTTP GET 요청을 반복해 특정 페이지 처리 자원을 소모시키는 설명이므로 맞다.

② O
동적 HTTP Request Flooding은 요청 페이지나 파라미터를 바꾸어 지속적으로 요청함으로써 캐시 효과를 줄이고 서버 부하를 키우는 공격이므로 맞다.

③ X
틀린 부분은 "Slow HTTP Header DoS(Slowloris)"와 "HTTP POST 메시지에서 헤더의 Content-Length 필드에 임의의 큰 값을 설정"이라는 연결이다.
Slowloris는 헤더를 매우 천천히 끊어 보내 연결을 오래 붙잡는 공격이다. Content-Length를 크게 잡고 본문을 천천히 보내는 설명은 Slow HTTP POST DoS 또는 RUDY 계열로 고쳐야 한다.

④ O
Mail Bomb는 사용자에게 할당된 메일 저장 공간을 초과할 정도로 대량 메일을 보내 더 이상 메일을 수신하지 못하게 만드는 공격이므로 맞다.

오답 포인트

③은 둘 다 슬로우 공격이라는 점 때문에 Slowloris와 Slow POST 계열을 섞어 놓은 선지이다. 헤더를 천천히 보내는지, POST 본문 길이를 크게 잡고 바디를 질질 끄는지가 구별 포인트이다.

다시 나오면 이렇게 판단

웹 DoS 선지는 먼저 공격 대상이 무엇을 점유하는지 본다. GET 대량 반복이면 요청 처리 자원, 동적 요청이면 캐시 우회형 웹 부하, 헤더를 늦게 보내면 Slowloris, 큰 Content-Length와 느린 본문 전송이면 Slow POST 계열로 판단한다.

암기 포인트

Slowloris는 느린 헤더, RUDY·Slow POST는 큰 Content-Length와 느린 바디 전송이라는 구분으로 외운다.

NoteBase

문 12. ElGamal 등과 같이 이산 대수 문제를 기반으로 하는 암호화 기법에서 비밀키로 공개키를 계산할 때 원시근이 사용된다. 사용되는 소수가 13일 때, 원시근으로 사용될 수 있는 값은?

① 6

② 8

③ 10

④ 12

정답 1번

출제 포인트

이 문제는 ElGamal에서 사용하는 원시근의 조건, 즉 법 13에서 위수가 12인 생성원을 고를 수 있는지를 묻는 문제이다.

조건 정리

주어진 값: 소수 13
구해야 할 값: 법 13에서의 원시근
주의할 조건: 원시근은 $13 - 1 = 12$개의 비영 원소를 모두 생성해야 하므로 위수가 12여야 한다.

사용할 공식

법 p에서 원시근 g는 위수(order)가 $p - 1$인 원소이다. 따라서 $p = 13$이면 g^12≡1±od13이고, 12의 진약수인 2,3,4,6에 대해서는 g^d≡1±od13이어야 한다.
이 공식을 쓰는 이유는 ElGamal의 밑 g가 곱셈군 전체를 생성하는 생성원이어야 공개키 계산이 올바르게 이루어지기 때문이다.

계산 과정

1. 13의 비영 원소 개수는 12이므로 후보의 위수가 12인지 확인한다.
2. $6^2 \equiv 36 \equiv 10$, $6^3 \equiv 60 \equiv 8$, $6^4 \equiv 48 \equiv 9$, 6^6≡8^2≡64≡12±od13이므로 2,3,4,6승에서 1이 나오지 않는다. 따라서 6의 위수는 12이다.
3. $8^2 \equiv 64 \equiv 12$, 8^4≡12^2≡144≡1±od13이므로 8의 위수는 4이다.
4. $10^2 \equiv 100 \equiv 9$, $10^3 \equiv 90 \equiv 12$, 10^6≡12^2≡1±od13이므로 10의 위수는 6이다.
5. 12≡-1±od13이므로 12^2≡1±od13이고 위수는 2이다.

NoteBase

선지별 해설

① O
6은 2,3,4,6승 어디에서도 1이 되지 않고 최종적으로 6^12≡1±od13이므로 위수가 12이다. 따라서 법 13의 원시근으로 사용할 수 있다.
② X
8은 8^4≡1±od13이므로 위수가 4에 불과하다. 틀린 표현은 "원시근으로 사용될 수 있다"이고, 올바르게는 "8은 원시근이 아니라 위수가 4인 원소이다"이다.
③ X
10은 10^6≡1±od13이므로 위수가 6이다. 틀린 표현은 "원시근으로 사용될 수 있다"이고, 올바르게는 "10은 원시근이 아니라 6개의 값만 순환시키는 원소이다"이다.
④ X
12는 −1과 같아서 12^2≡1±od13이다. 틀린 표현은 "원시근으로 사용될 수 있다"이고, 올바르게는 "12는 위수가 2인 원소이므로 원시근이 아니다"이다.

오답 포인트

원시근인지 판단할 때 단순히 1이 아니거나 소수보다 작은 수라는 이유만으로 고르면 틀리기 쉽다. 이 문항의 함정은 8, 10, 12도 겉보기에는 무난한 후보처럼 보이지만 각각 위수가 4, 6, 2로 줄어든다는 점이다.

다시 나오면 이렇게 판단

소수 p에서 원시근을 묻는 문제는 먼저 $p-1$을 구한 뒤 그 약수들에 대한 거듭제곱을 검사해 위수가 $p-1$인지 확인하면 된다. 즉 $p-1$의 진약수에서 1이 한 번이라도 나오면 원시근이 아니다.

암기 포인트

원시근 판정의 핵심은 "위수 = $p-1$"이다. $p-1$의 진약수 승에서 1이 나오면 탈락이다.

NoteBase

문 13. SSL/TLS에서 레코드 프로토콜의 동작단계로 가장 옳은 것은?

① 압축 → 암호화 → MAC 추가 → 단편화

② 압축 → MAC 추가 → 암호화 → 단편화

③ 암호화 → 단편화 → 압축 → MAC 추가

④ 단편화 → 압축 → MAC 추가 → 암호화

정답 4번

출제 포인트

이 문제는 SSL/TLS 레코드 프로토콜에서 송신 측 데이터 처리 순서를 묻는 문제이다.

올바른 순서

1. 단편화 — 상위 계층에서 내려온 데이터를 레코드 단위로 나눈다.
2. 압축 — 단편화된 데이터를 필요하면 압축한다.
3. MAC 추가 — 압축된 데이터에 무결성 검사용 MAC을 붙인다.
4. 암호화 — 데이터와 MAC을 함께 암호화해 전송한다.

왜 이 순서: MAC은 압축된 평문을 기준으로 계산되고, 암호화는 그 결과물 전체를 보호하는 마지막 단계이기 때문이다.

선지별 해설

① X: 압축으로 시작하는 점과 암호화 후 MAC을 붙이는 점이 틀리다. 레코드 프로토콜은 먼저 단편화하고, MAC을 붙인 뒤 마지막에 암호화한다. 틀린 표현은 "압축 → 암호화 → MAC 추가 → 단편화"이고, 올바르게는 "단편화 → 압축 → MAC 추가 → 암호화"이다.

② X: MAC을 암호화보다 먼저 두는 부분은 맞지만, 단편화가 맨 마지막에 오는 점이 틀리다. 단편화는 가장 먼저 수행되어야 이후 압축과 MAC, 암호화의 입력 단위가 정해진다. 틀린 표현은 "압축 → MAC 추가 → 암호화 → 단편화"이고, 올바르게는 "단편화 → 압축 → MAC 추가 → 암호화"이다.

③ X: 암호화를 첫 단계로 둔 것이 가장 큰 오류이다. 암호화는 단편화, 압축, MAC 추가가 끝난 뒤 최종 결과물에 적용된다. 틀린 표현은 "암호화 → 단편화 → 압축 → MAC 추가"이고, 올바르게는 "단편화 → 압축 → MAC 추가 → 암호화"이다.

④ O: 단편화 후 압축하고, 그 결과에 MAC을 추가한 뒤 마지막에 암호화하는 순서가 SSL/TLS 레코드 프로토콜의 전형적인 송신 처리 순서와 일치한다.

NoteBase

오답 포인트

MAC과 암호화의 선후관계를 뒤바꾸거나 단편화를 중간 단계로 착각하면 틀리기 쉽다. 이 문항은 "무결성 검사는 암호화 전에 붙이고, 암호화는 맨 마지막에 한다"는 흐름을 알고 있는지를 묻는다.

다시 나오면 이렇게 판단

절차형 보안 프로토콜 문제는 데이터 가공 순서를 입력 준비 단계, 무결성 부가 단계, 기밀성 보호 단계로 나누어 판단한다. 레코드 프로토콜에서는 레코드 단위를 먼저 만든 뒤 내용을 줄이고, 무결성 값을 붙인 다음, 마지막에 암호화하는 흐름으로 판단하면 된다.

암기 포인트

레코드 프로토콜 송신 순서는 "단편화 → 압축 → MAC → 암호화"이다.

NoteBase

문 14. 해시 함수에 대한 설명으로 가장 옳지 않은 것은?

① 160비트 길이의 해시 출력값을 갖는 SHA-1 해시 함수는 안전하지 않다고 알려져 있다.

② 키를 갖는 해시함수(Keyed Hash Function)는 메시지 인증 목적으로 사용될 수 있다.

③ 안전한 해시함수는 특정 해시값 h=H(x)를 갖는 x를 찾는 것이 어렵다는 충돌 회피성(collision resistance)을 가져야 한다.

④ NIST에서는 기존의 SHA-2와 원천적으로 다른 구조를 갖는 SHA-3(Keccak)를 표준화하였다.

정답 3번

출제 포인트

이 문제는 해시 함수의 기본 보안 성질인 충돌 회피성, 역상 저항성, 키드 해시의 용도를 구분하는 문제이다.

핵심 개념

충돌 회피성은 서로 다른 두 입력 $x \neq y$에 대해 $H(x) = H(y)$가 되도록 찾기 어려운 성질이다.
역상 저항성은 주어진 해시값 h에 대해 $H(x) = h$를 만족하는 입력 x를 찾기 어려운 성질이다.
키를 갖는 해시함수는 비밀 키를 공유한 당사자만 올바른 해시값을 만들 수 있게 하여 메시지 인증에 사용된다.

선지별 해설

① O
SHA-1은 160비트 해시 출력값을 가지며, 충돌 공격이 현실화되어 현재는 안전하지 않은 해시 함수로 본다.

② O
키를 갖는 해시함수는 대표적으로 HMAC처럼 메시지 인증 코드 구성에 쓰이며, 송신자와 수신자가 같은 비밀 키를 공유할 때 메시지 무결성과 인증에 사용할 수 있다.

③ X
틀린 부분은 "특정 해시값 $h = H(x)$를 갖는 x를 찾는 것이 어렵다"를 충돌 회피성이라고 한 표현이다.
이 설명은 충돌 회피성이 아니라 역상 저항성에 해당한다.
충돌 회피성은 같은 해시값을 만드는 서로 다른 두 입력을 찾기 어려운 성질로 고쳐야 한다.

④ O
SHA-3는 Keccak 기반으로 표준화되었고, Merkle-Damgard 구조 계열인 SHA-2와는 구조적으로 다른 스펀지 구조를 사용한다.

NoteBase

오답 포인트

충돌 회피성과 역상 저항성을 뒤바꾸는 함정이 핵심이다. "주어진 해시값에서 원문을 찾는가"를 묻으면 역상 저항성이고, "같은 해시값을 만드는 서로 다른 두 입력을 찾는가"를 묻으면 충돌 회피성이다.

다시 나오면 이렇게 판단

해시 보안 성질 문제는 먼저 대상이 한 개 입력인지, 서로 다른 두 개 입력인지 구분하면 된다. 하나의 해시값에서 원문 하나를 찾는 문제이면 역상 저항성, 두 입력의 해시를 같게 맞추는 문제이면 충돌 회피성으로 판단한다.

암기 포인트

역상 저항성은 해시값에서 원문 찾기, 충돌 회피성은 서로 다른 두 입력의 같은 해시값 찾기이다.

NoteBase

문 15. 디지털 서명에 대한 설명으로 가장 옳은 것은?

① 디지털 서명 기법에서 서명의 크기는 원본 데이터의 크기에 비례한다.

② RSA를 사용하는 경우 공개키로 서명하고 개인키로 서명을 검증한다.

③ X.509 인증서에는 공개키를 인증하기 위한 인증기관의 서명이 포함되어 있다.

④ 서명 과정에서 메시지에 해시함수를 적용하면 원본으로 복구가 불가능하므로, 해시함수는 서명에 사용하지 않는 것이 좋다.

정답 3번

출제 포인트

이 문제는 디지털 서명의 동작 원리와 X.509 인증서의 역할을 정확히 구별할 수 있는지를 묻는다.

핵심 개념

디지털 서명은 송신자가 자신의 개인키로 메시지의 해시값에 서명해 무결성과 송신자 인증을 제공하는 기술이다. 해시함수는 임의 길이의 입력을 고정 길이의 다이제스트로 바꾸는 일방향 함수이며, 서명 효율을 높이기 위해 서명 과정에 함께 사용된다.
X.509 인증서는 주체의 공개키와 신원 정보를 담고, 이를 인증기관이 자신의 서명으로 보증한 공개키 인증서이다.

선지별 해설

1번 X: 디지털 서명은 보통 원문 전체가 아니라 원문의 해시값에 대해 생성하므로 서명 크기는 원문 길이에 비례하지 않는다. 틀린 표현은 '원본 데이터의 크기에 비례한다'이다. 올바르게는 '서명 크기는 대체로 원문 크기와 무관하고 알고리즘 및 키 길이에 의해 결정된다'이다.
2번 X: RSA 서명은 개인키로 서명하고 공개키로 검증한다. 틀린 표현은 '공개키로 서명하고 개인키로 서명을 검증한다'이다. 올바르게는 '개인키로 서명하고 공개키로 검증한다'이다.
3번 O: X.509 인증서에는 대상의 공개키와 신원 정보가 담기고, 그 공개키가 맞다는 사실을 인증기관이 자신의 전자서명으로 보증한다. 따라서 인증기관의 서명이 포함된다는 설명이 옳다.
4번 X: 해시함수는 원문 복원이 불가능한 일방향 함수이기 때문에 오히려 디지털 서명에 적합하다. 원문 전체 대신 해시값에 서명하면 효율이 높아지고 검증도 가능하다. 틀린 표현은 '해시함수는 서명에 사용하지 않는 것이 좋다'이다. 올바르게는 '해시함수는 디지털 서명에서 핵심적으로 사용된다'이다.

오답 포인트

2번처럼 암호화와 서명의 키 사용 방향을 뒤바꾸거나, 4번처럼 해시함수의 일방향성을 이유로 서명에 부적합하다고 착각하면 틀리기 쉽다. 이 문제는 '원문 전체 서명'이 아니라 '해시 후 서명'이라는 기본 구조를 알고 있는지를 노린다.

NoteBase

다시 나오면 이렇게 판단

디지털 서명 문제는 먼저 '개인키로 서명, 공개키로 검증'을 확인하고, 다음으로 '원문이 아니라 해시값에 서명'하는 구조를 떠올리면 빠르게 판단할 수 있다. 인증서가 나오면 공개키를 인증기관 서명으로 보증하는 문서인지 확인하면 된다.

암기 포인트

전자서명은 개인키로 서명하고 공개키로 검증하며, X.509는 공개키를 CA 서명으로 보증한다.

NoteBase

문 16. DB 접근통제 방식 중 <보기>에서 설명하는 것은?

<보기>
네트워크 선로 상의 패킷들을 TAP 방식과 패킷 미러링 방식을 통해 분석 로깅하는 방식으로 사후 감사의 의미에 비중을 두는 보안 방식이다.

① 에이전트 방식

② 프록시 방식

③ 인라인 방식

④ 스니핑 방식

정답 4번

출제 포인트

이 문제는 DB 접근통제 방식 중 스니핑 방식의 동작 위치와 감사 중심 성격을 구별하는 문제이다.

핵심 개념

에이전트 방식은 DB 서버에 에이전트를 설치해 내부에서 질의와 접근을 수집·통제하는 방식이다.
프록시 방식은 사용자와 DB 서버 사이에 중계 장비를 두고 모든 접속을 우회시켜 통제하는 방식이다.
인라인 방식은 네트워크 경로상에 장비를 직접 위치시켜 실시간 차단과 제어를 수행하는 방식이다.
스니핑 방식은 TAP이나 포트 미러링으로 복제된 패킷을 수집·분석해 접근 내역을 감사하는 방식이다.

선지별 해설

① X: 틀린 부분은 "에이전트 방식"이다. 에이전트 방식은 DB 서버에 소프트웨어를 설치해 로그와 질의를 수집하는 구조이다. 제시문처럼 네트워크 선로에서 TAP과 패킷 미러링으로 패킷을 복제해 분석하는 방식은 스니핑 방식이다.
② X: 틀린 부분은 "프록시 방식"이다. 프록시 방식은 DB 앞단에서 접속을 반드시 거치게 하여 세션과 SQL을 중계·통제하는 방식이다. 제시문은 중계 장비를 거치는 구조가 아니라 복제된 네트워크 패킷을 사후 분석하는 설명이므로 스니핑 방식이 맞다.
③ X: 틀린 부분은 "인라인 방식"이다. 인라인 방식은 통신 경로에 직접 삽입되어 비인가 질의를 즉시 차단하는 예방 통제 성격이 강하다. 제시문은 사후 감사의 의미에 비중을 둔다고 했으므로 인라인이 아니라 스니핑 방식이다.
④ O: 스니핑 방식은 네트워크 구간에서 패킷을 복제해 수집하고 이를 분석·로깅하는 방식이다. TAP 방식과 패킷 미러링, 사후 감사 중심이라는 단서가 모두 스니핑 방식의 특징과 일치한다.

NoteBase

오답 포인트

TAP, 패킷 미러링, 사후 감사라는 단서를 놓치면 네트워크 장비를 쓴다는 이유만으로 프록시 방식이나 인라인 방식으로 혼동하기 쉽다. 이 문항은 실시간 차단인지, 중계 통제인지, 복제 패킷 감사인지를 구분하는지를 묻는다.

다시 나오면 이렇게 판단

문장에 TAP, 포트 미러링, 패킷 복제, 분석 로깅, 사후 감사가 나오면 스니핑 방식을 먼저 떠올리면 된다. 반대로 중간에서 접속을 대신 받아 주면 프록시, 통신 경로에 직접 들어가 즉시 차단하면 인라인, 서버 내부에 프로그램을 설치하면 에이전트 방식으로 판단한다.

암기 포인트

복제 패킷 감사는 스니핑, 중계 통제는 프록시, 경로 차단은 인라인, 서버 설치는 에이전트이다.

NoteBase

문 17. FTP 서버를 안전하게 운영하기 위한 방법으로 가장 좋은 것은?

① 파일과 사용자에 대한 보안을 위하여 익명(anonymous) FTP로 설정한다.

② 사용자가 본인의 홈디렉터리보다 상위 디렉터리에 접근할 수 있도록 설정한다.

③ 파일 내용이 인가되지 않은 방법으로 수정되지 않도록 Everyone 계정을 제거해야 한다.

④ 출장이나 재택근무 등을 대비하여 모든 IP주소 대역에서 접근할 수 있도록 한다.

정답 3번

출제 포인트

이 문제는 FTP 서버의 접근 통제와 파일 권한 최소화 원칙을 구분하는 문제이다.

핵심 개념

익명 FTP는 불특정 사용자의 공개 접근을 허용하는 방식이어서 사용자 식별과 접근 통제가 약하다.
FTP 보안의 기본은 사용자를 필요한 디렉터리와 필요한 권한으로만 제한하는 것이다.
파일 무결성 보호는 불필요한 쓰기 권한을 제거하여 비인가 수정 가능성을 줄이는 데 있다.
접속 허용 범위도 필요한 사용자와 필요한 IP 대역으로 최소화하는 것이 원칙이다.

선지별 해설

① X. 익명 FTP는 계정 식별 없이 접근을 허용하는 방식이므로 파일과 사용자 보안을 강화하는 설정이 아니다. 틀린 표현은 "보안을 위하여 익명 FTP로 설정한다"이다. 올바르게는 "익명 FTP는 꼭 필요한 공개 다운로드 용도에서만 제한적으로 사용하고, 일반적으로는 인증 기반 접근으로 운영한다"이다.
② X. 사용자가 홈디렉터리보다 상위 디렉터리까지 접근하면 다른 경로나 시스템 파일에 닿을 가능성이 커져 보안에 불리하다. 틀린 표현은 "상위 디렉터리에 접근할 수 있도록"이다. 올바르게는 "사용자를 자신의 홈디렉터리 이하로 제한하도록 설정한다"이다.
③ O. Everyone에 광범위한 권한이 남아 있으면 비인가 사용자가 파일을 수정할 위험이 커진다. 따라서 파일 내용이 허가되지 않은 방식으로 바뀌지 않게 하려면 Everyone에 부여된 불필요한 권한, 특히 쓰기 권한을 제거하는 방향이 맞다.
④ X. 모든 IP주소 대역에서 접근을 허용하면 공격 표면이 과도하게 넓어진다. 틀린 표현은 "모든 IP주소 대역에서 접근할 수 있도록"이다. 올바르게는 "업무상 필요한 IP 대역만 허용하거나 VPN 등으로 제한하여 접근하게 한다"이다.

오답 포인트

①과 ④는 "편의성"이나 "공개성"을 보안 강화처럼 포장한 선지이다. 익명 허용, 상위 디렉터리 허용, 전 대역 IP 개방처럼 접근 범위를 넓히는 표현이 나오면 안전한 운영과는 반대 방향일 가능성이 크다.

NoteBase

다시 나오면 이렇게 판단

FTP 보안 선지는 먼저 접근 범위를 넓히는지 줄이는지로 판단한다. 익명 허용, 디렉터리 이탈 허용, 전체 IP 개방처럼 범위를 넓히면 대체로 틀리고, 불필요한 권한 제거처럼 권한을 축소하면 맞을 가능성이 높다.

암기 포인트

FTP 보안은 공개 확대가 아니라 권한 축소이다. 익명 금지, 상위 디렉터리 차단, 전체 IP 개방 금지, Everyone의 불필요한 쓰기 권한 제거가 핵심이다.

NoteBase

문 18. 소프트웨어 보안 약점 유형에 대한 설명으로 가장 옳은 것은?

① 코드 오류: 의도하지 않은 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안 약점 (예: DNS lookup에 의존한 보안결정)

② 에러 처리: 프로그램 입력 값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안 약점 (예: SQL 삽입, XQuery 삽입, LDAP 삽입 등)

③ 시간 및 상태: 중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때, 인가되지 않은 사용자에게 데이터 누출이 가능해지는 보안 약점 (예: 잘못된 세션에 의한 데이터 또는 시스템 데이터 정보 노출 등)

④ 보안 기능: 인증, 접근제어, 암호화 등의 기능을 부적절하게 구현 시 발생할 수 있는 보안 약점 (예: 부적절한 인가, 하드코드된 암호화키 등)

정답 4번

출제 포인트

소프트웨어 보안 약점 유형의 이름과 대표 예시를 정확히 대응시키는지를 묻는 문제이다.

핵심 개념

코드 오류는 구현 로직 자체의 실수로 생기는 약점이다.
입력값 검증 및 표현 오류는 외부 입력 검증 누락이나 형식 처리 문제로 생기는 약점이다.
시간 및 상태는 경쟁 상태, 세션 상태, 처리 순서처럼 시점과 상태 관리에서 생기는 약점이다.
캡슐화 약점은 중요한 데이터나 기능을 충분히 숨기지 못해 정보 노출이 생기는 경우이다.
보안 기능 약점은 인증, 인가, 접근통제, 암호화 같은 보안 메커니즘을 잘못 구현한 경우이다.

NoteBase

선지별 해설

① X
의도하지 않은 API 사용이나 보안에 취약한 API 사용은 코드 오류보다는 API 오용 또는 안전하지 않은 API 사용에 가까운 설명이다. 틀린 표현은 "코드 오류"이다. 올바르게는 "API를 의도하지 않은 방식으로 사용하거나 안전하지 않은 API를 사용하여 발생하는 약점"이라고 고쳐야 한다.

② X
SQL 삽입, XQuery 삽입, LDAP 삽입은 입력값 검증 누락과 해석 오류가 핵심이므로 에러 처리 유형의 대표 예시가 아니다. 틀린 표현은 "에러 처리"이다. 올바르게는 "입력값 검증 및 표현 오류로 인해 발생할 수 있는 보안 약점"이라고 고쳐야 한다.

③ X
중요한 데이터나 기능을 불충분하게 캡슐화하여 정보가 노출되는 문제는 시간 및 상태가 아니라 캡슐화 약점 설명이다. 틀린 표현은 "시간 및 상태"이다. 올바르게는 "중요한 데이터 또는 기능성을 불충분하게 캡슐화하였을 때 발생하는 정보 노출 약점"이라고 고쳐야 한다.

④ O
인증, 접근제어, 암호화 기능을 부적절하게 구현하여 발생하는 약점이라는 설명이 정확하다. 부적절한 인가와 하드코드된 암호화키는 보안 기능 약점의 대표 예시이다.

오답 포인트

유형명과 예시를 서로 바꿔 놓은 선지를 구분해야 한다. ②는 삽입 공격 예시만 보면 입력 검증 문제라는 점이 바로 보여야 하고, ③은 "세션"이라는 단어에 끌리지 말고 설명의 핵심이 정보 은닉 실패인지 상태 관리 실패인지를 봐야 한다.

다시 나오면 이렇게 판단

유형명을 먼저 믿지 않고 예시를 먼저 분류하면 된다. 삽입 공격이면 입력 검증, 인증·인가·암호화면 보안 기능, 경쟁 상태나 처리 순서면 시간 및 상태, 정보 노출과 은닉 실패면 캡슐화로 판단한다.

암기 포인트

삽입은 입력 검증, 인증·인가·암호화는 보안 기능, 정보 노출은 캡슐화, 경쟁 상태는 시간 및 상태이다.

NoteBase

문 19. <보기>의 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제2조 발췌문에서 (가)에 들어갈 기관은?

<보기>
“정보보호 및 개인정보보호 관리체계 인증”이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 (가) 또는 인증기관이 증명하는 것을 말한다.

① 국가정보원
② 한국인터넷진흥원
③ 개인정보 보호위원회
④ 과학기술정보통신부

정답 2번

쟁점

이 문제는 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제2조의 정의규정에서 인증기준 적합성을 증명하는 주체를 구별할 수 있는지를 묻는다.

용어 풀이

정보보호 및 개인정보보호 관리체계 인증(ISMS-P)은 조직의 정보보호 및 개인정보보호를 위한 조치와 활동이 인증기준에 맞는지를 한국인터넷진흥원 또는 인증기관이 증명하는 제도이다.

핵심 구분

제2조 발췌문의 핵심은 정책·감독 기관과 인증 적합성 증명 기관을 구별하는 데 있다. 정의규정에서 적합함을 증명하는 주체는 한국인터넷진흥원 또는 인증기관이고, 과학기술정보통신부와 개인정보보호위원회는 제도 운영·정책 측면의 기관이며 국가정보원은 이 정의규정의 주체가 아니다.

선지별 해설

1번 X: 국가정보원은 이 고시 제2조의 인증 정의에서 적합성을 증명하는 주체로 적혀 있지 않다. 틀린 표현은 '국가정보원'이고, 올바르게는 '한국인터넷진흥원'이다.
2번 O: 제2조 발췌문은 인증신청인의 조치와 활동이 인증기준에 적합함을 '한국인터넷진흥원 또는 인증기관'이 증명한다고 정의한다. 따라서 (가)는 한국인터넷진흥원이다.
3번 X: 개인정보보호위원회는 개인정보 정책과 제도 측면의 기관이지만, 발췌된 정의규정의 빈칸에 들어가는 적합성 증명 주체는 아니다. 틀린 표현은 '개인정보보호위원회'이고, 올바르게는 '한국인터넷진흥원'이다.
4번 X: 과학기술정보통신부도 제도 관련 정책·지정 주체에 해당하지만, 제2조 정의에서 적합성을 증명하는 기관명으로 들어가지는 않는다. 틀린 표현은 '과학기술정보통신부'이고, 올바르게는 '한국인터넷진흥원'이다.

NoteBase

오답 포인트

정책·감독 기관과 실제 인증 적합성을 증명하는 기관을 같은 층위로 외우면 틀리기 쉽다. 이 문항은 '누가 제도를 관장하는가'가 아니라 '누가 적합함을 증명하는가'를 묻는 정의규정 문제이다.

다시 나오면 이렇게 판단

정의규정 빈칸 문제는 문장 속 동사를 먼저 본다. 여기서는 '증명하는' 주체를 묻고 있으므로 정책기관이 아니라 인증 실행 주체를 찾으면 된다.

암기 포인트

ISMS-P 정의규정의 증명 주체는 한국인터넷진흥원 또는 인증기관이다.

NoteBase

문 20. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 대한 설명으로 가장 옳지 않은 것은?

① 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 “접근권한”이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한이 아닌 경우에는 접근권한 허용에 대하여 동의하지 아니할 수 있다는 사실을 이용자에게 알리고 이용자의 동의를 받아야 한다.

② 정보통신서비스 제공자는 해당 서비스를 제공하기 위하여 이용자의 이동통신단말장치 내에 저장되어 있는 정보 및 이동통신단말장치에 설치된 기능에 대하여 접근할 수 있는 권한(이하 “접근권한”이라 한다)이 필요한 경우, 이 접근권한이 해당 서비스를 제공하기 위하여 반드시 필요한 접근권한인 경우에도 접근권한이 필요한 이유를 이용자에게 알리고 이용자의 동의를 받아야 한다.

③ 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 「전자상거래 등에서의 소비자보호에 관한 법률」로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

④ 과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 침해사고에 대한 긴급조치를 수행할 수 있다.

정답 3번

쟁점

이 문제는 접근권한 동의 규정과 정보보호 최고책임자 지정·신고 제도의 원칙과 예외를 정확히 구별할 수 있는지를 묻는다.

용어 풀이

접근권한은 앱 서비스 제공을 위해 이동통신단말장치의 저장정보나 기능에 접근할 수 있는 권한이다.
정보보호 최고책임자는 정보통신시스템 보안과 정보의 안전한 관리를 총괄하는 책임자이다.

핵심 구분

반드시 필요한 접근권한과 선택 접근권한은 모두 고지와 동의가 필요하다. 다만 선택 접근권한은 거부 가능 사실까지 추가로 알려야 한다.
정보보호 최고책임자는 원칙적으로 지정하고 신고하여야 한다. 다만 일정 기준에 해당하는 사업자는 지정의무가 아니라 신고의무에 대해서만 예외가 인정된다.

NoteBase

선지별 해설

① O: 반드시 필요하지 않은 접근권한은 이용자가 동의하지 않을 수 있다는 사실까지 알려야 하므로 옳다. 선택 접근권한에서는 거부 가능 고지가 추가된다.
② O: 반드시 필요한 접근권한도 필요한 이유를 알리고 이용자의 동의를 받아야 하므로 옳다. 차이는 거부 가능 사실 고지의 필요 여부이지, 동의 자체가 불필요하다는 뜻이 아니다.
③ X: 두 부분이 틀렸다. 첫째, 기준은 「전자상거래 등에서의 소비자보호에 관한 법률」이 아니라 대통령령으로 정하는 기준이다. 둘째, 예외가 인정되는 것은 정보보호 최고책임자를 지정하지 않는 것이 아니라 과학기술정보통신부장관에게 신고하지 않는 것이다. 틀린 표현은 "「전자상거래 등에서의 소비자보호에 관한 법률」로 정하는 기준", "지정하지 아니할 수 있다"이고, 올바른 표현은 "대통령령으로 정하는 기준", "신고하지 아니할 수 있다"이다.
④ O: 과학기술정보통신부장관은 침해사고 대응 업무의 하나로 침해사고에 대한 긴급조치를 수행할 수 있으므로 옳다.

오답 포인트

3번은 예외의 대상이 지정인지 신고인지를 바꿔 놓고, 기준의 근거도 전자상거래법으로 바꾸어 놓은 선지이다. 법령형 문제에서는 "할 수 있다" 앞의 행위가 무엇인지와 기준의 근거 규범이 무엇인지를 함께 확인해야 한다.

다시 나오면 이렇게 판단

법령 선지는 주체, 의무 내용, 예외 대상, 근거 규범을 순서대로 확인하면 된다. 특히 "지정"과 "신고", "반드시 필요한 권한"과 "반드시 필요하지 않은 권한"처럼 비슷한 표현의 교체 여부를 먼저 본다.

암기 포인트

선택 접근권한은 거부 가능 사실까지 고지한다. 정보보호 최고책임자는 지정이 원칙이고 일정 기준 사업자에게는 신고 예외가 붙는다.

NoteBase