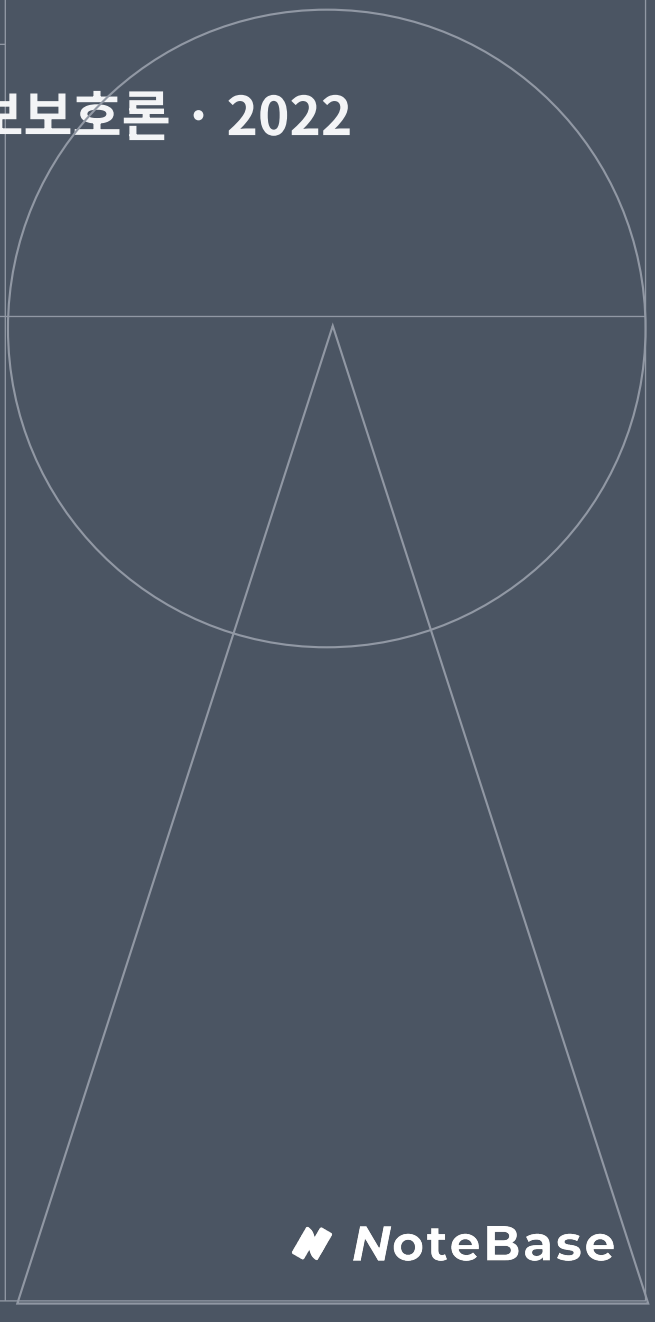
기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2022



NoteBase

기출OX 해설집

공무원/경찰/경력채용 · 정보보호론 · 2022

공무원/경찰/경력채용 · 정보보호론 · 2022

문 1. 어떤 블록 암호 모드들의 복호화 정의가 아래와 같을 때, 각각의 암호화 정의로 가장 적절한 것은? (단, C_i는 i번째 암호문, P_i는 i번째 평문, $E_K(P_i)$는 P_i를 암호화, $D_K(C_i)$는 C_i를 복호화)

복호화	$P_i = D_K(C_i) \oplus C_{i-1}$	$P_i = E_K(C_{i-1}) \oplus C_i$
암호화	㉠	㉡

① ㉠: $C_i = E_K(P_i) \oplus C_{i-1}$, ㉡: $C_i = E_K(C_{i-1}) \oplus P_i$

② ㉠: $C_i = E_K(P_i) \oplus C_{i-1}$, ㉡: $C_i = D_K(C_{i-1}) \oplus P_i$

③ ㉠: $C_i = E_K(P_i \oplus C_{i-1})$, ㉡: $C_i = E_K(C_{i-1}) \oplus P_i$

④ ㉠: $C_i = E_K(P_i \oplus C_{i-1})$, ㉡: $C_i = D_K(C_{i-1}) \oplus P_i$

정답 3번

간단한 해설

㉠은 평문과 이전 암호문을 **먼저 XOR한 뒤 암호화**하고, ㉡은 이전 암호문을 암호화한 값과 평문을 XOR한다.
같은 값을 두 번 XOR하면 원래 값으로 돌아가는 성질을 이용해 복호화 식을 변형한다.

NoteBase

계산 과정

기본 성질: XOR은 $(A \oplus B) \oplus B = A$를 만족한다. 또한 같은 키를 쓰는 암호화와 복호화는 역연산이므로 $E_K(D_K(C_i)) = C_i$이다.

㉠: 주어진 복호화 식은 $P_i = D_K(C_i) \oplus C_{i-1}$이다. 양변에 이전 암호문을 XOR하면 $P_i \oplus C_{i-1} = D_K(C_i)$가 된다. 양변에 암호화 함수 E_K를 적용하면 역함수 관계에 따라 $C_i = E_K(P_i \oplus C_{i-1})$를 얻는다. 따라서 XOR은 암호화 함수의 입력을 만드는 단계에서 수행한다. 이는 CBC 모드의 암호화 식이다.

㉡: 주어진 복호화 식은 $P_i = E_K(C_{i-1}) \oplus C_i$이다. 양변에 $E_K(C_{i-1})$를 XOR하면 같은 항이 소거되어 $C_i = E_K(C_{i-1}) \oplus P_i$를 얻는다. 암호화와 복호화 모두 이전 암호문에 암호화 함수 E_K를 적용하며, 이를 복호화 함수 D_K로 바꾸지 않는다. 이는 한 블록 단위 CFB 모드에 해당한다.

선지 연결: ㉠은 $C_i = E_K(P_i \oplus C_{i-1})$, ㉡은 $C_i = E_K(C_{i-1}) \oplus P_i$이므로 두 식이 모두 일치하는 ③이 정답이다. ①·②는 ㉠에서 XOR과 암호화의 순서를 바꾸었고, ②·④는 ㉡에서 사용할 암호화 함수를 복호화 함수로 바꾸었다.

NoteBase

문 2. ITU-T 권고안 X.800에 관한 내용 중 가장 적절하지 않은 것은?

① OSI 보안 구조인 ITU-T 권고안 X.800은 보안 요구사항을 만족하는 체계적인 접근 방법을 규정하고 있다.

② 보안 기법(Mechanism)은 보안 공격을 탐지, 예방하고 그로부터 복구하기 위한 제반 기법이다.

③ 보안 서비스는 조직의 데이터 처리 시스템 및 정보 전송에 대한 보안을 강화하기 위한 제반 서비스이며, 데이터 기밀성, 데이터 무결성, 인증, 라우팅 제어 등이 있다.

④ 보안 서비스를 제공하기 위한 보안 기법은 암호화, 데이터 무결성, 디지털서명, 트래픽 패딩, 접근제어 등이 있다.

정답 3번

간단한 해설

라우팅 제어는 보안 서비스가 아니라 보안 기법이다. 보안 정책에 따라 통신 경로를 선택하거나 회피하여 기밀성 등의 서비스를 지원한다.

선지별 해설

① O: X.800은 OSI 환경에서 안전한 통신을 제공하기 위한 **보안 구조**를 제시한다. 필요한 보안 서비스를 구분하고, 이를 구현하는 기법과 OSI 계층에서의 배치 관계를 설명하므로 보안 요구사항을 체계적으로 다루는 기준이 된다.

② O: 보안 기법은 **공격의 탐지·예방·복구를 실현하는 수단**이다. 보안 서비스가 제공할 보호 기능을 나타낸다면, 보안 기법은 그 기능을 실제로 구현하는 방법이다. 예를 들어 기밀성 서비스를 암호화 기법으로 구현할 수 있다.

③ X: 데이터 기밀성·데이터 무결성·인증은 보안 서비스에 해당하지만, **라우팅 제어는 보안 기법**이다. X.800의 기본 보안 서비스는 인증, 접근제어, 데이터 기밀성, 데이터 무결성, 부인방지이다. 라우팅 제어는 보안 정책에 따라 특정 네트워크·링크·중계점을 선택하거나 피하도록 경로를 제어하는 수단으로, 기밀성 등의 서비스를 지원한다.

④ O: 암호화, 데이터 무결성 기법, 디지털서명, 트래픽 패딩, 접근제어 기법은 모두 보안 서비스를 구현하는 수단이다. 암호화는 정보 노출을 막고, 무결성 기법은 변조를 탐지하며, 디지털서명은 서명자와 데이터의 진위를 검증하는 데 쓰인다. 트래픽 패딩은 더미 데이터를 넣어 트래픽 분석을 어렵게 하고, 접근제어 기법은 권한 없는 접근을 제한한다. 특히 **접근제어와 데이터 무결성은 서비스와 기법 양쪽의 명칭**으로 쓰이므로 보호 기능을 말하는지 구현 수단을 말하는지 구분해야 한다.

NoteBase

문 3. 다음 지문의 ㉠~㉣에 들어갈 값으로 가장 적절한 것은?

현재 10명이 사용하는 암호시스템을 30명이 사용할 수 있도록 확장하려면 키의 수도 증가한다. 대칭키 암호시스템을 채택할 때에는 10명일 경우 (㉠)개, 30명일 경우에는 (㉡)개가 필요하며, 확장에 추가로 필요한 키의 수는 (㉢)개이다. 반면, 공개키 암호시스템을 채택할 때 확장에 추가로 필요한 키의 수는 (㉣)개이다.

① ㉠: 45, ㉡: 435, ㉢: 390, ㉣: 40

② ㉠: 90, ㉡: 870, ㉢: 780, ㉣: 40

③ ㉠: 45, ㉡: 435, ㉢: 390, ㉣: 60

④ ㉠: 90, ㉡: 870, ㉢: 780, ㉣: 60

정답 1번

간단한 해설

대칭키는 **사용자 두 명마다 공유키 1개**를 세므로 10명일 때 45개, 30명일 때 435개이며 추가로 390개가 필요하다. 공개키 방식은 늘어난 20명에게 공개키와 개인키가 하나씩 필요하므로 추가 키는 40개이다.

계산 과정

계산 기준: 사용자 수를 n이라 하자. 모든 사용자 쌍이 서로 다른 대칭키 하나씩을 공유한다고 보면, A와 B의 키를 B와 A의 키로 다시 세면 안 되므로 키 수는 $K_s(n) = \frac{n(n-1)}{2}$개이다. 공개키 방식은 사용자마다 공개키와 개인키 한 쌍을 가진다는 기준으로 $K_p(n) = 2n$개이다. 여기서는 **키 쌍이 아니라 개별 키의 수**를 센다.

㉠: 10명에게 필요한 대칭키는 $K_s(10) = \frac{10 \times 9}{2} = 45$개이다. 두 사용자가 같은 공유키를 보유하더라도 그 키 자체는 한 개로 센다.

㉡: 30명에게 필요한 대칭키는 $K_s(30) = \frac{30 \times 29}{2} = 435$개이다. 이는 확장 이후 시스템 전체에 필요한 키 수이다.

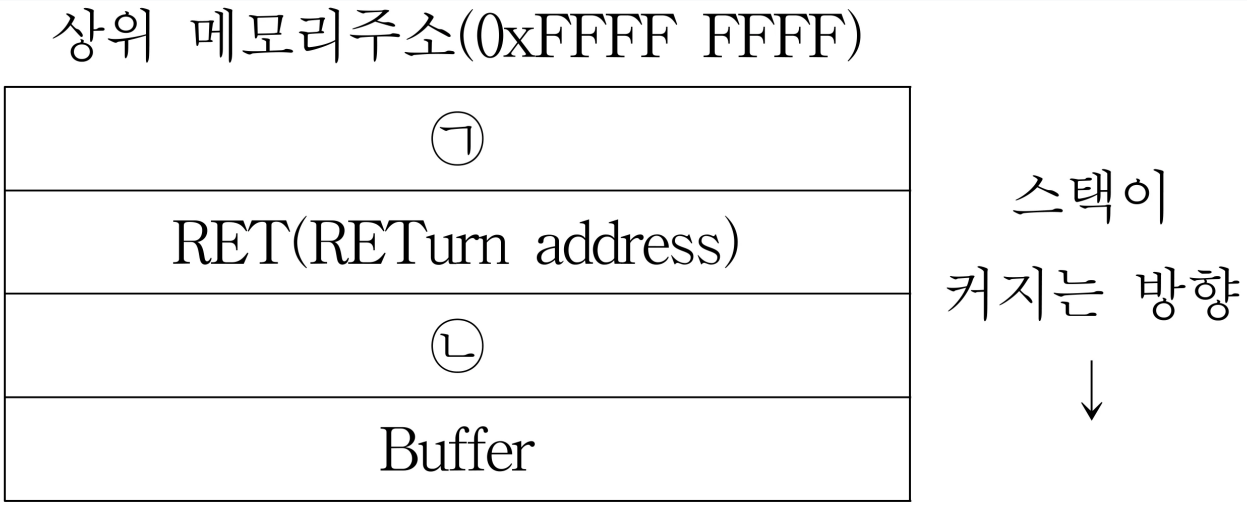
㉢: 대칭키의 추가 수는 **확장 후 총수에서 기존 총수를 뺀 값**이므로 $435 - 45 = 390$개이다. 기존 10명 사이의 45개 키는 그대로 사용할 수 있으므로 다시 추가하지 않는다.

㉣: 공개키 방식의 총 키 수는 10명일 때 $2 \times 10 = 20$개, 30명일 때 $2 \times 30 = 60$개이다. 따라서 추가 수는 $60 - 20 = 40$개이다. 새로 참여하는 20명에게 공개키·개인키 한 쌍씩, 즉 **20쌍에 해당하는 40개**가 필요하다.

따라서 ㉠ 45개, ㉡ 435개, ㉢ 390개, ㉣ 40개이므로 정답은 ①이다.

NoteBase

문 4. 스택 버퍼 오버플로우(stack buffer overflow) 공격에 대응하기 위해 스택 가드(stack guard) 방법을 사용하는 경우, 다음의 논리적 메모리에 주입하는 위치와 값이 가장 적절한 것은?



① 주입위치: ㉠, 값: canary

② 주입위치: ㉡, 값: canary

③ 주입위치: ㉠, 값: Global RET

④ 주입위치: ㉡, 값: Global RET

정답 2번

간단한 해설

스택 가드는 **버퍼와 반환 주소 사이에 canary를 삽입**하고 함수 반환 전에 변조 여부를 검사한다. 그림에서 두 영역 사이의 위치는 ㉡이다.

NoteBase

도식 해설

그림의 배치: 위쪽이 높은 메모리 주소이며, 위에서부터 ㉠, RET, ㉡, Buffer가 놓여 있다. 오른쪽의 아래쪽 화살표는 스택이 낮은 주소 쪽으로 커지는 방향이다. 이는 버퍼에 연속으로 데이터를 쓰다가 경계를 넘어 높은 주소 쪽의 RET를 덮어쓰는 방향과 구별해야 한다.

주입 위치: 카나리는 **Buffer와 RET 사이**에 있어야 한다. 그림에서는 이 자리가 ㉡이다. 버퍼에서 RET까지 연속으로 덮어쓰면 카나리가 먼저 손상되므로 반환 주소가 사용되기 전에 이상을 탐지할 수 있다. ㉠은 RET보다 높은 주소 쪽에 있어, 그곳까지 쓰지 않고도 RET를 손상시킬 수 있다.

주입 값: 스택 가드는 canary라는 검사값을 넣고 함수가 반환하기 전에 처음의 값과 비교한다. 값이 달라졌다면 정상 반환을 중단하여 손상된 RET가 사용되는 것을 막는다. Global RET를 넣는 것은 이 카나리 검사 방식의 설명에 해당하지 않는다.

따라서 주입 위치가 ㉡이고 값이 canary인 ②가 가장 적절하다.

NoteBase

문 5. Diffie-Hellman 키교환 알고리즘에서 소수 13과 원시근 6, 사용자 A와 B의 개인키가 각각 4, 3일 때, 공유 비밀키의 값으로 가장 적절한 것은?

① 1

② 2

③ 3

④ 4

정답 1번

간단한 해설

Diffie-Hellman의 공유 비밀키는 **상대 공개값과 자신의 개인키**로 계산한다. B의 공개값은 6^313=8이므로 A가 구하는 공유 비밀키는 8^413=1이다.

계산 과정

조건과 공식: 소수는 $p = 13$, 원시근은 $g = 6$, 개인키는 $a = 4$, $b = 3$이다. 공개값은 Y_A=g^a p, Y_B=g^b p로 계산한다. 공유 비밀키는 **상대의 공개값을 자신의 개인키만큼 거듭제곱**한 나머지이므로 K=Y_B^a p=Y_A^b p=g^ab p이다. 여기서 mod는 나눈 나머지를 뜻한다.

A의 공개값: $6^4 = 1296 = 13 \times 99 + 9$이므로 $Y_A = 9$이다. 이 값은 B에게 전달하는 공개값이며, 개인키 4나 최종 공유 비밀키와 구별한다.

B의 공개값: $6^3 = 216 = 13 \times 16 + 8$이므로 $Y_B = 8$이다. A는 이 공개값을 받아 자신의 개인키 4로 계산한다.

공유 비밀키: A가 계산하면 K=8^413이다. 큰 수를 바로 계산하는 대신 **제곱할 때마다 나머지로 줄이면** 8^2=64≡12±od13, 8^4≡12^2=144≡1±od13이므로 $K = 1$이다. B가 계산해도 $9^3 = 729 = 13 \times 56 + 1$이어서 같은 값 1을 얻는다.

따라서 공유 비밀키의 값은 1이고, 정답은 ①이다.

NoteBase

문 6. SSL/TLS에 관한 설명 중 가장 적절한 것은?

① SSL/TLS는 서버와 클라이언트 인증, 데이터 기밀성과 무결성을 제공하고, 통신을 수행할 때 URL은 “https://”로 시작한다.

② 공개키 암호 혹은 키 교환 기술을 이용하고 있기 때문에, 의사난수 생성기의 품질은 낮아도 된다.

③ 공개키가 서버로부터 오기 때문에, 클라이언트가 서버의 공개키를 하나도 가지고 있지 않아도 서버를 인증할 수 있다.

④ 종단 대 종단 보안 서비스인 SSL/TLS는 현재는 신뢰할 수 없는 프로토콜이다.

정답 1번

간단한 해설

TLS는 **상대방 인증·기밀성·무결성**을 제공하며, HTTP에 적용하면 HTTPS 웹 통신이 된다. 클라이언트 인증은 선택적이고, 서버가 보내준 공개키를 신뢰하려면 별도의 인증서·신원 검증이 필요하다.

NoteBase

선지별 해설

① O: SSL/TLS는 통신 상대의 인증, 데이터 기밀성, 무결성을 제공하는 보안 프로토콜 계열이다. **HTTP에 TLS를 적용한 웹 통신**을 HTTPS라고 하며 URL도 HTTPS 스킴을 사용한다. 서버 인증과 클라이언트 인증을 지원하지만 클라이언트 인증은 선택적이다. 따라서 이 선지는 제공 가능한 보안 기능과 HTTPS 웹 통신의 설명으로 이해해야 하며, 모든 TLS 응용이 HTTPS를 사용한다는 뜻은 아니다.

② X: 공개키 암호나 키 교환을 사용하더라도 **암호학적으로 안전한 의사난수**가 필요하다. 비밀키나 키 교환에 필요한 난수 등을 예측할 수 있으면 공격자가 비밀정보를 알아낼 수 있다. 안전한 알고리즘을 사용하는 것만으로 낮은 품질의 난수가 보완되지는 않는다.

③ X: '공개키가 서버로부터 온다'는 사실은 **그 키가 정당한 서버의 것이라는 인증 근거로 불충분**하다. 공격자도 자신의 키를 보낼 수 있으므로 인증서 기반 방식에서는 신뢰하는 CA의 공개키 등 신뢰 앵커를 바탕으로 인증서 경로와 서버 신원을 검증해야 한다. 다만 **서버 공개키를 미리 보유하지 않았다는 것 자체는 오류가 아니다**. 필요한 신뢰 정보와 검증 절차가 갖춰져 있으면 서버 인증서에서 공개키를 받아 인증할 수 있다. 이 선지의 문제는 사전 미보유가 아니라, 공개키를 받는다는 이유만으로 인증이 성립한다고 설명한 점이다.

④ X: **구식 SSL의 취약성을 TLS 전체로 일반화**한 표현이다. SSL 2.0·3.0 등 오래된 버전은 안전하지 않지만, 적절한 버전·암호 설정·인증서 검증을 사용하는 TLS까지 신뢰할 수 없다고 단정할 수는 없다. TLS는 통신 양 끝점 사이의 채널을 보호하며, 안전성은 프로토콜 버전과 구현·운영 조건을 함께 보아야 한다.

이 문항은 가장 적절한 설명을 고르므로, 위와 같은 웹 통신 문맥에서 인증·기밀성·무결성이라는 제공 기능을 설명한 ①을 선택한다.

NoteBase

문 7. 각 용어에 대한 설명으로 가장 적절하지 않은 것은?

① Honeypot : 보안 위협을 사전에 대응할 목적으로 해킹 공격과 악성코드 감염을 고의로 유도함으로써 해킹 기법과 악성코드 특성과 행위를 분석하여 그에 대한 예방책을 세우도록 하는 시스템

② Bufferbloat : 데이터통신망에서 패킷 손실을 막기 위하여 버퍼의 크기를 크게 만들었지만, 이로 인하여 오히려 응답문자(ACK : acknowledgement)와 같이 작은 크기의 패킷들이 정체되어 패킷 전송이 느려지는 현상

③ Authentication, Authorization : Authentication은 사용자에 따라 적절한 접근 권한을 부여하는 것이고, Authorization은 암호를 제시함으로써 사용자를 인증하는 것

④ Grayware : 인터넷 사용자가 어쩔 수 없이 자신의 컴퓨터에 설치하도록 유도한 후(ActiveX 설치요구 등), 설치가 된 후에는 사용자의 기대와 다른 동작을 하여 시스템 성능을 악화시키거나 사용 불편을 초래하는 소프트웨어들을 총칭

정답 3번

간단한 해설

인증(Authentication)은 신원 확인, **인가(Authorization)는 접근 권한 결정**이다. 두 개념의 설명을 서로 바꾼 ③이 가장 적절하지 않다.

선지별 해설

① (O) 허니팟(Honeypot)은 공격자가 접근하도록 유인하는 미끼 시스템이다. 침입 시도와 악성코드의 동작을 관찰하여 공격 기법을 분석하고 방어 대책을 마련하는 데 활용하므로, 공격을 의도적으로 유도해 분석한다는 설명이 옳다.

② (O) 버퍼블로트(Bufferbloat)는 과도하게 쌓인 버퍼 내 패킷 때문에 **대기 지연**이 커지는 현상이다. 패킷 손실을 줄이려고 버퍼만 크게 하면 혼잡이 발생했을 때 긴 대기열이 유지되어 응답성이 나빠질 수 있다. ACK처럼 작은 패킷도 같은 대기열에 갇혀 지연되며, 이 문제는 작은 패킷에만 한정되지 않는다.

③ (X) **Authentication은 인증**으로, 비밀번호 등의 인증 수단을 검증하여 사용자가 주장하는 신원이 맞는지 확인하는 과정이다. **Authorization은 인가**로, 해당 사용자에게 어떤 자원에 대한 접근이나 작업을 허용할지 결정하는 것이다. 선지는 두 개념을 서로 바꾸어 설명했으므로 가장 적절하지 않다.

④ (O) 그레이웨어(Grayware)는 정상 프로그램과 명백한 악성 프로그램의 경계에서, 사용자가 원하지 않는 동작으로 성능 저하나 불편을 일으킬 수 있는 소프트웨어를 가리킨다. 설치를 유도한 뒤 기대와 다른 동작을 한다는 선지의 설명은 이러한 특성에 해당한다. 다만 ActiveX라는 설치 기술 자체가 그레이웨어를 뜻하는 것은 아니며, 설치 경로보다는 실제 동작을 기준으로 구별해야 한다.

NoteBase

문 8. 유클리드 알고리즘을 이용하여 2740과 1760의 최대공약수를 계산하였다. 각 위치에서의 값이 가장 적절한 것은?

q(몫)	r_1	r_2	r(나머지)
1	2740	1760	980
1	1760	㉢	780
1	980	780	200
3	780	200	㉣
1	200	180	20
㉠	180	20	0
	㉡ (최대공약수)	0	

① ㉠: 9, ㉡: 20, ㉢: 480, ㉣: 90

② ㉠: 5, ㉡: 10, ㉢: 480, ㉣: 90

③ ㉠: 5, ㉡: 10, ㉢: 980, ㉣: 180

④ ㉠: 9, ㉡: 20, ㉢: 980, ㉣: 180

정답 4번

간단한 해설

유클리드 알고리즘은 나누는 수와 나머지로 같은 계산을 반복하며, **마지막 0이 아닌 나머지**가 최대공약수이다. 표를 순서대로 계산하면 ㉠은 9, ㉡은 20, ㉢은 980, ㉣은 180이다.

NoteBase

계산 과정

계산 원리: 각 행에서 $r_1 = q \times r_2 + r$이며, 다음 행의 두 수는 현재의 r_2와 r로 바뀐다. $\gcd(r_1, r_2) = \gcd(r_2, r)$이므로 나머지가 0이 될 때까지 반복한다.

㉢ 계산: 첫 행은 $2740 = 1 \times 1760 + 980$이다. 따라서 다음 행에서 나누는 수는 980이며, $1760 = 1 \times 980 + 780$이므로 ㉢은 980이다.

㉣ 계산: 이어서 $980 = 1 \times 780 + 200$, $780 = 3 \times 200 + 180$이므로 네 번째 행의 나머지인 ㉣은 180이다.

㉠ 계산: 다음 행은 $200 = 1 \times 180 + 20$이다. 마지막 나눗셈은 $180 = 9 \times 20 + 0$이므로 그 몫인 ㉠은 9이다.

㉡ 계산: 나머지가 0이 되었을 때 마지막으로 나눈 수인 20이 최대공약수이다. 즉 $\gcd(2740, 1760) = 20$이므로 ㉡은 20이다. 종료 행의 0 자체를 최대공약수로 쓰지 않는다.

선지 연결: ㉠ 9, ㉡ 20, ㉢ 980, ㉣ 180의 조합이므로 ④가 정답이다.

NoteBase

문 9. 다음 설명에 해당하는 공격으로 가장 적절한 것은?

컴퓨터의 소프트웨어나 하드웨어 및 컴퓨터 관련 전자 제품의 버그, 보안 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 절차나 일련의 명령, 스크립트, 프로그램 또는 특정한 데이터 조각을 말하며, 이러한 것들을 사용한 공격 행위를 이르기도 한다. 주로 공격 대상 컴퓨터의 제어 권한 획득이나 서비스 거부 공격(DoS) 등을 목적으로 한다.

① Trojan Horse

② Exploit

③ Hoax

④ Bonk

정답 2번

간단한 해설

설계상 결함이나 보안 취약점을 이용해 특정 동작을 일으키는 코드·데이터·절차는 **Exploit(익스플로잇)**이다. 제어 권한 획득과 서비스 거부는 그 활용 결과에 해당한다.

개념 구분

Exploit: 핵심 단서는 **버그나 보안 취약점을 이용**하여 의도한 동작을 일으키는 절차·명령·코드·데이터라는 점이다. 취약점은 시스템에 존재하는 약점이고, 익스플로잇은 그 약점을 실제로 이용하는 수단이나 행위이다. 그 결과로 제어 권한을 얻거나 서비스를 중단시킬 수 있으므로 제시문의 목적과도 부합한다.

Trojan Horse: 정상적이거나 유용한 프로그램처럼 보이지만 내부에 악성 기능을 숨긴 프로그램이다. **정상 기능으로 위장**한다는 점이 구별 기준이다. 트로이 목마가 취약점 이용 공격과 함께 쓰일 수는 있지만, 제시문은 위장 프로그램의 정의가 아니다.

Hoax: 거짓 바이러스 경고처럼 허위 정보를 퍼뜨려 사용자를 속이거나 혼란을 일으키는 것이다. 시스템의 결함을 직접 이용하는 코드나 절차를 뜻하지 않는다.

Bonk: 비정상적인 IP 단편의 중첩과 재조립 처리의 취약점을 이용하는 서비스 거부 공격의 한 종류이다. 취약점 이용이라는 공통점은 있으나, 제시문은 특정 패킷 공격이 아니라 여러 형태의 취약점 이용 수단과 행위를 포괄하여 설명한다.

따라서 제시문에 해당하는 명칭은 ② Exploit이다.

NoteBase

문 10. '2021 국가정보보호백서'에 게재된 PKI(Public-Key Infrastructure) 공인인증기관(CA, Certification Authority)으로 지정되지 않은 곳은?

① (주)코스콤
② 한국정보인증(주)
③ (주)한국무역정보통신
④ (주)한국거래소

정답 4번

간단한 해설

2021 국가정보보호백서의 공인인증기관 명단에는 코스콤·한국정보인증·한국무역정보통신이 포함되지만, **한국거래소는 포함되지 않는다**. 따라서 정답은 ④이다.

개념 구분

판단 기준: 이 문항은 **2021 국가정보보호백서의 공인인증기관 지정 현황**을 기준으로 판단한다. 인증기관(CA)은 인증서의 발급·관리 등을 수행하는 기관이다. 금융이나 전자거래와 관련된 기관이라는 이유만으로 모두 CA에 해당하는 것은 아니다.

코스콤: 백서의 지정 현황에 포함되며, 주요 이용분야는 **온라인증권**으로 제시되어 있다. 증권거래에 쓰이는 인증서비스를 제공하는 기관이라는 점을 한국거래소와 구별해야 한다.

한국정보인증: 지정 현황에 포함되며, 주요 이용분야는 전자상거래이다. 따라서 공인인증기관으로 지정되지 않은 곳을 찾는 답에 해당하지 않는다.

한국무역정보통신: 지정 현황에 포함되며, 주요 이용분야는 전자무역이다. 백서에는 이 세 기관 외에도 금융결제원과 한국전자인증이 포함되어 총 5개 기관이 제시된다.

한국거래소: 증권·파생상품 시장의 운영을 담당하는 기관으로, 해당 백서의 **공인인증기관 명단에는 포함되지 않는다**. 코스콤의 온라인증권 인증업무와 한국거래소의 시장 운영 역할을 혼동하면 안 된다.

따라서 지정되지 않은 곳은 ④ (주)한국거래소이다.

NoteBase

문 11. IoT(Internet of Things)에 관한 설명으로 가장 적절하지 않은 것은?

① IoT 기기를 대상으로 한 악성코드는 미라이(Mirai), 다이어(Dyre) 등이 있다.

② 네트워크 카메라 제품에 관한 주요 보안 위협에는 공격 대상자의 사진, 동영상을 공격자의 서버 및 이메일로 전송하는 방법 등이 있다.

③ IoT 제품의 보안 요구사항에는 시큐어 코딩, 알려진 보안 취약점 및 취약점 제거, 안전한 소프트웨어 사용 등이 있다.

④ 안전한 IoT 사용을 위해 ARIA, SEED, EC-KCDSA 사용을 권장한다.

정답 1번

간단한 해설

미라이는 IoT 기기를 봇넷에 편입시키는 악성코드이지만, **다이어는 금융정보 탈취형 악성코드**이다. 두 가지를 모두 IoT 대상 악성코드로 분류한 ①이 가장 적절하지 않다.

선지별 해설

① (X) 미라이(Mirai)는 네트워크 카메라·공유기 등 IoT 기기를 감염시켜 봇넷을 구성하고 DDoS 공격 등에 악용하는 악성코드이다. 반면 **다이어(Dyre)는 금융정보 탈취형 악성코드**로, 주로 Windows 환경에서 인터넷뱅킹 등의 로그인 정보를 훔친다. 따라서 두 악성코드를 모두 IoT 기기 대상 악성코드로 묶은 ①이 가장 적절하지 않다.

② (O) 네트워크 카메라가 침해되면 공격자가 촬영 영상이나 사진에 접근하여 외부 서버 또는 이메일로 유출할 수 있다. 카메라 원격 제어와 무단 촬영도 사생활 침해로 이어질 수 있으므로, 사진·동영상의 외부 전송은 주요 보안 위협에 해당한다.

③ (O) IoT 제품은 개발 단계에서 시큐어 코딩으로 보안 약점이 생기는 것을 예방하고, 사용하는 소프트웨어의 알려진 취약점을 점검·제거해야 한다. 안전한 소프트웨어를 사용하고 보안 패치를 적용하는 것도 필요하다. 선지의 보안 요구사항은 취약점을 제품에 두라는 뜻이 아니라, **취약점을 찾아 제거**하여 안전성을 확보하라는 취지이다.

④ (O) IoT의 데이터를 보호하려면 안전성이 검토된 표준 암호 알고리즘을 용도에 맞게 적용해야 한다. ARIA와 SEED는 대칭키 블록암호로 데이터 암호화에, EC-KCDSA는 전자서명으로 메시지의 출처와 무결성 검증에 활용할 수 있다. 이들 알고리즘의 사용 권장은 적절하며, 실제 구현에서는 적정한 키 길이·안전한 운용 방식·키 관리도 함께 갖추어야 한다.

NoteBase

문 12. 대칭키 블록 암호 알고리즘 중 키 길이가 256bit인 것으로 가장 적절한 것은?

① RSA

② SHA-3

③ Blowfish

④ ARIA

정답 4번

출제 포인트

대칭키 블록 암호의 분류와 키 길이를 구분하는 문제이다. ARIA의 명시된 키 길이 128비트, 192비트, 256비트와 Blowfish의 가변 키 길이를 비교한다.

핵심 개념

대칭키 블록 암호는 같은 비밀키를 사용하여 일정한 크기의 데이터 블록을 암호화하고 복호화하는 방식이다. 키 길이는 비밀키의 크기이고, 블록 길이는 한 번에 처리하는 데이터의 크기이므로 서로 다르다. RSA는 공개키 암호이고, SHA-3는 해시 함수이며, Blowfish와 ARIA는 대칭키 블록 암호이다.

선지별 해설

이 문항의 O/X는 제공 답안에 따른 선택 판단을 나타내며, X가 해당 알고리즘의 모든 특성이 틀렸다는 뜻은 아니다.

① RSA — X. RSA는 공개키와 개인키를 사용하는 비대칭키 암호이다. 대칭키 블록 암호로 분류하는 것은 잘못이며, 공개키 암호로 구분해야 한다.

② SHA-3 — X. SHA-3는 입력 데이터의 해시값을 만드는 해시 함수이다. SHA3-256의 256은 해시 출력 길이이며 암호화 키 길이가 아니다. 대칭키 블록 암호가 아니라 해시 함수로 구분해야 한다.

③ Blowfish — X(제공 답안에 따른 비선택). Blowfish는 대칭키 블록 암호이며, 키 길이가 32비트부터 448비트까지 가변적이므로 256비트 키도 사용할 수 있다. 따라서 '256비트 키를 지원하지 않는다'는 설명은 틀리며, '가변 키 길이 범위에 256비트가 포함된다'가 정확하다. ARIA의 명시된 세 가지 키 길이를 연결하는 제공 답안에서는 선택하지 않지만, 발문의 조건만으로 Blowfish의 기술적 적합성을 완전히 배제할 수는 없다.

④ ARIA — O. ARIA는 대칭키 블록 암호이며 키 길이가 128비트, 192비트, 256비트로 구분된다. 256비트 키를 사용하는 유형이 명시되어 있으므로 발문과 직접 연결되는 선택이다. 블록 길이는 128비트이므로 256비트 키 길이와 혼동하지 않는다.

NoteBase

오답 포인트

SHA3-256의 출력 길이를 키 길이로 오인하거나, Blowfish가 256비트 키를 지원하지 않는다고 외우기 쉽다. ARIA의 키 길이는 세 가지로 명시되고 Blowfish는 가변 길이라는 차이가 있지만, 그 차이만으로 Blowfish의 256비트 키 사용이 불가능해지는 것은 아니다. 이 발문은 최대 키 길이를 묻지 않는다.

다시 나오면 이렇게 판단

먼저 공개키 암호, 해시 함수, 대칭키 블록 암호를 구분한다. 다음으로 키 길이와 블록 길이를 따로 확인하고, 명시된 키 길이 유형과 가변 키 길이 범위를 비교한다. 이 문항은 ARIA의 256비트 키 유형을 연결하는 제공 답안으로 학습하되, 256비트 키를 사용할 수 있다는 조건만으로는 Blowfish도 해당한다는 점을 함께 유지한다.

암기 포인트

RSA는 공개키, SHA-3는 해시이다. ARIA의 키는 128비트, 192비트, 256비트이고, Blowfish의 키는 32~448비트로 가변적이다. Blowfish도 256비트 키를 지원한다.

NoteBase

문 13. 매스메일러형 웜 바이러스에 관한 설명으로 가장 적절하지 않은 것은?

① SMTP 서버의 네트워크 트래픽을 증가시킨다.

② 버퍼오버플로우나 포맷 스트링과 같은 취약점을 이용하여 확산 및 공격한다.

③ 매스메일러형 웜 바이러스에는 베이글, 넷스카이, 소빅 등이 있다.

④ 매스메일러형 바이러스는 내부 교육을 통해 충분히 예방할 수 있다.

정답 2번

간단한 해설

매스메일러형 웜의 대표적인 전파 방식은 **악성 메일의 대량 발송**과 첨부파일 실행 유도이다. 버퍼 오버플로우·포맷 스트링 취약점을 직접 공략하는 방식은 네트워크 공격형 웜의 특징과 연결된다.

선지별 해설

① O. 감염된 컴퓨터에서 메일 주소를 수집하고 악성 첨부파일을 여러 주소로 보내므로 SMTP 통신량이 증가한다. 대량의 메일 송수신은 메일 서버와 네트워크에 부하를 줄 수 있다.

② X. 버퍼 오버플로우나 포맷 스트링 등 소프트웨어 취약점을 직접 이용해 확산하는 것은 네트워크 공격형 웜의 전형적인 방식이다. 매스메일러형 웜의 대표적 특징은 메일로 자신을 대량 전송하고 사용자가 첨부파일을 실행하도록 유도하는 것이다. 따라서 취약점 공격 방식을 이 유형의 주된 전파 특성으로 제시한 ②가 가장 적절하지 않다. 다만 복합적인 전파 기능을 지닌 변종까지 취약점을 전혀 이용하지 않는다고 단정할 수는 없다.

③ O. 베이글(Bagle), 넷스카이(Netsky), 소빅(Sobig)은 이메일을 대량 발송하여 전파되는 매스메일러형 웜의 대표적 사례이다. 변종에 따라 공유 폴더나 다른 경로를 이용하는 기능이 추가될 수 있으나, 이메일 전파라는 분류상의 공통점은 유지된다.

④ O. 출처가 불분명하거나 예상하지 못한 첨부파일을 실행하지 않도록 교육하면 사용자 실행을 이용하는 감염 경로를 줄일 수 있다. 이 문항에서는 이러한 내부 교육의 예방 효과를 설명하는 선지이다. 다만 원문의 '충분히 예방'이 교육만으로 모든 감염을 막는다는 보장을 뜻하는 것은 아니며, 실제 방어에는 백신·메일 필터링·보안 업데이트 등도 함께 필요하다.

NoteBase

문 14. 다음에서 Elgamal 암호화 방식에 관한 설명으로 올바르게 짝지어진 것은?

㉠ RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 짧은 길이의 키를 필요로 한다.
㉡ 이산대수에 근거해서 만든 시스템이다.
㉢ 암호화와 디지털 서명 알고리즘을 모두 지원한다.
㉣ Rabin, ECC 알고리즘과 비교할 때 가장 빠르다.

① ㉠㉢
② ㉠㉣
③ ㉡㉢
④ ㉡㉣

정답 3번

간단한 해설

ElGamal은 **이산대수 문제를 바탕**으로 하며, 암호화 방식과 디지털 서명 방식을 모두 갖는다. RSA보다 짧은 키가 대표적인 장점이라는 설명과 조건 없는 속도 우위 주장은 맞지 않는다.

NoteBase

보기별 해설

여기서는 통상적인 유한체 기반 ElGamal의 특성을 판단한다.

㉠ X: 같은 안전성을 위해 RSA보다 훨씬 짧은 키를 쓰는 대표적인 방식은 **ECC**이다. 유한체 기반 ElGamal은 RSA와 비교할 때 비슷한 규모의 큰 정수 매개변수를 필요로 하므로, 짧은 키가 특징이라는 설명은 맞지 않는다. 키를 구성하는 값과 저장 형식이 다르므로 전체 공개키 파일의 길이까지 같다는 뜻은 아니다.

㉡ O: **이산대수 문제의 어려움**을 바탕으로 설계된 공개키 방식이다. 예를 들어 공개값이 y=g^x p일 때, 큰 소수 p와 적절한 생성원 g, 공개값 y로부터 비밀 지수 x를 구하기 어렵다는 성질을 이용한다.

㉢ O: ElGamal에는 메시지의 기밀성을 위한 암호화 방식과, 서명자의 인증 및 메시지 무결성을 확인하기 위한 디지털 서명 방식이 모두 있다. **암호화 절차와 서명 절차는 별개**이며, 암호문을 만들었다는 것만으로 서명까지 제공되는 것은 아니다.

㉣ X: ElGamal이 Rabin과 ECC보다 언제나 가장 빠르다고 할 수 없다. 기본 ElGamal 암호화에는 두 번의 모듈러 거듭제곱이 필요하며, 처리 속도는 암호화·복호화·서명·검증 중 무엇을 비교하는지, 매개변수 크기와 구현 환경이 어떤지에 따라 달라진다. 따라서 조건 없이 가장 빠르다고 일반화한 부분을 고쳐야 한다.

따라서 옳은 설명은 ㉡과 ㉢이며, 이를 짝지은 선택지는 ③이다.

NoteBase

문 15. 정보시스템 및 네트워크의 취약점 분석도구로 가장 적절하지 않은 것은?

① Nipper

② COPS(Computer Oracle and Password System)

③ Nessus

④ BotSnipper

정답 4번

간단한 해설

Nipper·COPS·Nessus는 **설정 오류나 보안상 약점을 점검**하는 취약점 분석도구이다. 봇넷 통신 탐지와 취약점 진단을 구별하는 이 문항의 답은 ④이다.

개념 구분

판단 기준: 취약점 분석도구는 시스템이나 네트워크의 설정, 권한, 소프트웨어 등을 점검하여 **공격에 악용될 수 있는 보안상 약점**을 찾는다. 네트워크에서 이미 나타나는 악성 통신을 탐지하는 도구와 주된 목적을 구별해야 한다.

Nipper: 라우터·스위치·방화벽 등 네트워크 장비의 **설정 정보를 분석**하여 잘못된 보안 설정과 취약한 구성을 찾아낸다. 따라서 네트워크 취약점 분석에 사용하는 도구이다.

COPS: 유닉스 시스템의 파일 권한, 취약한 패스워드, SUID 프로그램 등 잠재적 보안 문제를 점검하는 도구 모음이다. 시스템 내부의 설정과 권한을 살펴보는 **호스트 중심의 보안 점검**에 해당한다.

Nessus: 운영체제·서비스·응용프로그램의 알려진 취약점, 누락된 보안 패치와 잘못된 설정 등을 검사하는 취약점 스캐너이다. 네트워크로 접근 가능한 시스템의 보안상 약점을 진단하는 데 사용한다.

BotSnipper: 원문 표기는 BotSnipper이지만, 관련 원 논문에 제시된 도구명은 **BotSniffer**이다. 문맥상 이 봇넷 탐지 도구를 가리킨 것으로 해석되며, 두 철자가 공식 별칭이라는 뜻은 아니다. BotSniffer는 네트워크 트래픽의 상관성과 유사성을 분석하여 **봇넷의 명령·제어(C&C) 통신**을 탐지한다. 이는 설정 오류나 소프트웨어 약점을 찾는 일반적인 취약점 진단과 주된 목적이 다르다.

따라서 이 문항에서 가장 적절하지 않은 것은 ④ BotSnipper이다.

NoteBase

문 16. 다음 설명에 해당하는 공격유형으로 가장 적절한 것은?

· 사용자가 인증한 세션이 특정 동작을 수행하여도 계속 유지되어 정상적인 요청과 비정상적인 요청을 구분하지 못하는 점을 악용하는 공격이다.
· 사용자의 브라우저 내에서 서버가 유지하고 있는 신뢰를 이용해서 웹 서버를 공격하며 악성 스크립트를 서버에 요청한다는 특징이 있다.
· 데이터 등록·변경의 기능이 있는 페이지에서 동일 요청으로 매회 등록 및 변경 기능이 정상적으로 수행이 되면 이 공격에 취약할 가능성이 있다.

① Session Hijacking
② CSRF
③ SQL Injection
④ XSS

정답 2번

간단한 해설

서버가 인증된 사용자 브라우저를 신뢰한다는 점을 악용하여, 사용자가 의도하지 않은 등록·변경 요청을 보내게 하는 공격은 CSRF이다. 공격자가 세션을 직접 탈취하는 것이 아니라 기존 인증 상태를 이용한다.

NoteBase

핵심 풀이

CSRF(사이트 간 요청 위조)는 **인증된 사용자의 브라우저가 원하지 않는 요청을 보내도록 유도**하는 공격이다. 브라우저가 해당 사이트의 세션 쿠키 등을 요청에 실어 보내면, 방어가 없는 서버는 로그인된 사용자의 요청이라는 사실만 확인하고 사용자가 실제로 의도한 동작인지 구별하지 못한다. 지문의 '인증한 세션'과 '서버가 유지하고 있는 신뢰'가 이 구조를 가리킨다.

지문의 악성 스크립트 관련 표현은 공격자가 사용자의 브라우저에서 서버로 위조 요청을 보내도록 유도하는 것으로 이해한다. 핵심은 **사용자의 인증 상태를 이용한 요청 위조**이며, 악성 스크립트를 서버가 실행해야 성립하는 공격은 아니다. 링크나 폼을 통해 유도할 수도 있다.

데이터 등록·변경은 서버의 상태를 바꾸는 기능이므로 CSRF의 주요 대상이다. 요청의 정당성을 별도로 검증하지 않으면 공격자가 유도한 요청도 처리될 수 있다. 다만 **같은 요청이 반복 처리된다는 사실만으로 취약성이 확정되지는 않는다**. 세션별 CSRF 토큰을 사용하는 정상 구현도 있으므로 토큰 검증 등 방어 여부와 외부에서 위조 요청을 유도할 수 있는지를 함께 보아야 한다.

Session Hijacking은 세션 식별자 등을 탈취하거나 확보하여 **세션 자체를 가로채는 공격**이다. CSRF는 공격자가 세션 값을 직접 알아내지 않고도 피해자 브라우저의 기존 인증 상태를 이용할 수 있다는 점에서 구별된다.

SQL Injection은 입력값이 데이터베이스 질의문의 구조나 의미를 바꾸도록 악용하는 공격이다. 지문에는 SQL 질의문에 대한 입력 조작이 아니라 **인증된 브라우저를 이용한 요청**이 제시되어 있다.

XSS는 신뢰하는 웹 사이트의 문맥에서 **공격자의 스크립트를 사용자 브라우저에 실행**시키는 공격이다. 스크립트라는 단어가 있다고 반드시 XSS인 것은 아니다. 이 지문에서는 서버가 사용자 브라우저의 인증을 신뢰한다는 점과 등록·변경 요청을 악용한다는 점이 결정적이다.

따라서 설명에 해당하는 공격 유형은 ② CSRF이다.

NoteBase

문 17. 다음에서 설명하는 웹 공격에 해당하는 용어가 올바르게 짝지어진 것은?

㉠ 해커가 웹사이트 화면을 원하는 화면으로 바꾸어 해킹 성공을 알리는 공격으로써 공격자가 자신의 존재감을 알리는 목적으로 활용
㉡ 클라이언트의 명령을 서버에서 실행시켜주는 프로그램으로, 공격자가 악의적인 목적을 가지고 웹서버에서 임의의 명령을 실행할 수 있도록 제작한 프로그램
㉢ 웹 표적으로 삼은 특정 집단이 자주 이용하는 웹사이트를 감염시키고, 피해 대상이 그 웹사이트를 방문할 때까지 기다리는 웹 기반 공격

① ㉠: 인젝터, ㉡: 워터링 홀, ㉢: 웹 쉘
② ㉠: 디페이스, ㉡: 웹 쉘, ㉢: 워터링 홀
③ ㉠: 인젝터, ㉡: 웹 쉘, ㉢: 워터링 홀
④ ㉠: 디페이스, ㉡: 워터링 홀, ㉢: 웹 쉘

정답 2번

간단한 해설

웹 화면의 변조는 **디페이스**, 웹서버에서 명령을 실행하는 프로그램은 **웹 쉘**, 표적이 자주 찾는 사이트를 감염시켜 기다리는 공격은 **워터링 홀**이다.

대응 관계 해설

㉠ 디페이스(Defacement): 웹사이트의 정상 화면을 공격자가 원하는 문구나 그림으로 바꾸는 공격이다. 화면 변조를 통해 침입 사실을 과시하거나 자신의 주장을 드러낸다는 점이 단서이다. 코드 주입 도구를 뜻하는 인젝터가 아니라, 웹 화면을 훼손·변조하는 공격의 명칭을 묻는다.

㉡ 웹 쉘(Web Shell): 공격자가 웹 요청 등으로 명령을 전달하면 웹서버 쪽에서 이를 실행하게 하는 악성 프로그램이다. 서버의 명령 실행이나 파일 조작 등 원격 제어 수단으로 이용될 수 있다. 핵심은 방문자를 기다리는 것이 아니라 서버에 명령을 실행시키는 기능이다.

㉢ 워터링 홀(Watering Hole): 특정 표적 집단이 자주 방문하는 웹사이트를 먼저 침해하고, 표적이 그 사이트를 방문할 때 감염시키려는 공격이다. 표적의 방문 습관을 이용해 경유지를 미리 오염시키고 기다린다는 점에서 웹 쉘과 구별된다.

선지 연결: ㉠ 디페이스, ㉡ 웹 쉘, ㉢ 워터링 홀이므로 ②가 정답이다. ①·③은 ㉠을 인젝터로 잘못 연결했고, ①·④는 웹 쉘과 워터링 홀의 설명을 서로 바꾸었다.

NoteBase

문 18. 생체 인증 기법 중 신체학적 특성을 이용한 인증으로 가장 적절하지 않은 것은?

① 지문

② 얼굴

③ 홍채

④ 걸음걸이

정답 4번

간단한 해설

걸음걸이는 걷는 방식과 움직임의 패턴을 이용하는 **행동학적 특성**이다. 지문·얼굴·홍채는 신체의 형태나 구조를 이용하는 특성으로 분류한다.

개념 구분

신체학적 특성: 몸의 형태나 구조에서 얻는 특징을 이용한다. 지문은 손가락 피부의 융선 무늬, 얼굴은 눈·코·입 등 얼굴의 형태와 배치, 홍채는 동공 주변 홍채의 무늬를 이용하므로 이 범주에 속한다.

행동학적 특성: 사람이 어떤 동작을 수행할 때 나타나는 패턴을 이용한다. 걸음걸이는 걷는 리듬과 보폭, 팔다리 움직임 같은 **보행 동작의 패턴**을 분석하므로 행동학적 특성으로 분류한다. 신체 구조의 영향을 받더라도, 인증에서 관찰하는 주된 대상이 걷는 행동이라는 점으로 구별한다.

따라서 신체학적 특성을 이용한 인증으로 가장 적절하지 않은 것은 ④ 걸음걸이이다.

NoteBase

문 19. CSA(Cloud Security Alliance)에서 2019년에 발표한 클라우드 환경에서의 위협, 리스크 및 취약점에 관한 11대 보안 위협 요인에 포함되지 않은 것은?

① 계정 하이재킹

② 데이터 유출

③ 클라우드 서비스 남용 및 악용

④ 가상화 취약점

정답 4번

간단한 해설

CSA의 **2019년 11대 위협**에는 계정 하이재킹, 데이터 유출, 클라우드 서비스 남용 및 악용이 포함된다. 가상화 계층과 관련된 공유 기술 취약점은 이 목록에서 제외되었으므로 정답은 ④이다.

핵심 풀이

판단 기준은 일반적인 클라우드 보안 위험의 존재 여부가 아니라, **CSA가 2019년에 선정한 11대 위협 목록**에 포함되는지이다. 이 목록은 「Egregious Eleven」으로 발표되었다.

제시된 항목 중 ① 계정 하이재킹은 계정 탈취, ② 데이터 유출은 허가되지 않은 정보 노출, ③ 클라우드 서비스 남용 및 악용은 클라우드 자원을 악의적인 활동에 이용하는 위협을 뜻한다. 이 세 항목은 모두 2019년 목록에 포함된다.

④ 가상화 취약점은 여러 사용자가 자원을 공유하는 가상 인프라의 기술적 결함과 관련된다. 이러한 공유 기술 취약점은 이전 보고서에서 다루었지만, **2019년 11대 위협에서는 제외**되었다. 따라서 정답은 ④ 가상화 취약점이다. 이는 가상화 취약점이 실제로 존재하지 않거나 안전하다는 뜻이 아니라, 해당 연도의 상위 11개 항목으로 선정되지 않았다는 뜻이다.

NoteBase

문 20. 다음에서 설명하는 전자우편 보안 프로토콜의 특징이 올바르게 짝지어진 것은?

㉠ S/MIME 보안 서비스에는 메시지에 대한 송신 사실 부인 방지가 포함되지 않는다.
㉡ PGP는 기밀성, 메시지 인증, 사용자 인증, 송신 부인방지, 단편화와 재조립에 대한 보안 기능을 지원한다.
㉢ PEM은 IETF가 채택한 인터넷 표준 프로토콜로 다소 구현이 복잡하고 높은 보안성을 가지고 있지만, 현재는 많이 사용하지 않고 있다.
㉣ PGP는 IDEA, 3DES로 메시지를 암호화하여 전송하고, S/MIME은 AES 128bit로 메시지를 암호화하고 압축하여 전송한다.

① ㉡㉢㉣
② ㉠㉢
③ ㉡㉢
④ ㉠㉡㉢㉣

정답 1번

간단한 해설

S/MIME은 전자서명으로 **송신 부인 방지를 제공**하므로 ㉠이 틀리다. PGP의 보안·전송 기능, PEM의 특징, PGP와 S/MIME의 지원 알고리즘 및 압축 기능에 관한 ㉡·㉢·㉣을 고르면 된다.

NoteBase

보기별 해설

㉠ X: S/MIME은 전자서명을 통해 발신자 인증과 메시지 무결성뿐 아니라 **송신 사실의 부인 방지**를 제공한다. 따라서 부인 방지가 포함되지 않는다는 부분을 포함된다고 고쳐야 한다. 메시지 암호화는 이와 구별되는 기밀성 기능이다.

㉡ O: PGP는 메시지 암호화로 기밀성을, 전자서명 검증으로 메시지의 무결성과 발신자 인증 및 송신 부인 방지를 지원한다. 긴 메시지를 나누어 보내고 수신 측에서 합치는 **단편화·재조립** 기능도 지원한다. 다만 단편화·재조립 자체는 암호학적 보안 속성이 아니라 전자우편 전송을 위한 부가 기능이다.

㉢ O: PEM은 IETF에서 표준화한 초기 전자우편 보안 프로토콜로, 암호화와 인증을 이용해 기밀성·무결성·송신 부인 방지를 제공하도록 설계되었다. **계층적 인증서·키 관리 체계**를 운영해야 하므로 구축이 복잡하며, 전자우편 보안 프로토콜로는 널리 보급되지 않았다. 여기서 높은 보안성이란 이러한 보호 기능을 갖추었다는 역사적 설명이지, 과거 암호 알고리즘의 현재 안전성을 일괄 보장한다는 뜻은 아니다.

㉣ O: PGP의 전통적 메시지 암호화 방식에는 IDEA와 3DES가 있고, S/MIME 3.2는 AES-128 암호화와 메시지 압축 기능을 지원한다. 이 보기는 **지원하는 알고리즘과 기능**을 연결한 설명으로 이해한다. PGP가 IDEA·3DES만 쓰거나 S/MIME이 AES-128만 쓰는 것은 아니며, S/MIME의 압축도 모든 메시지에 필수로 적용되는 절차는 아니다. 암호화와 압축의 적용 순서가 하나로 고정된다는 뜻도 아니다.

따라서 해당 특징에 부합하는 보기는 ㉡·㉢·㉣이며, 정답은 ①이다.

NoteBase