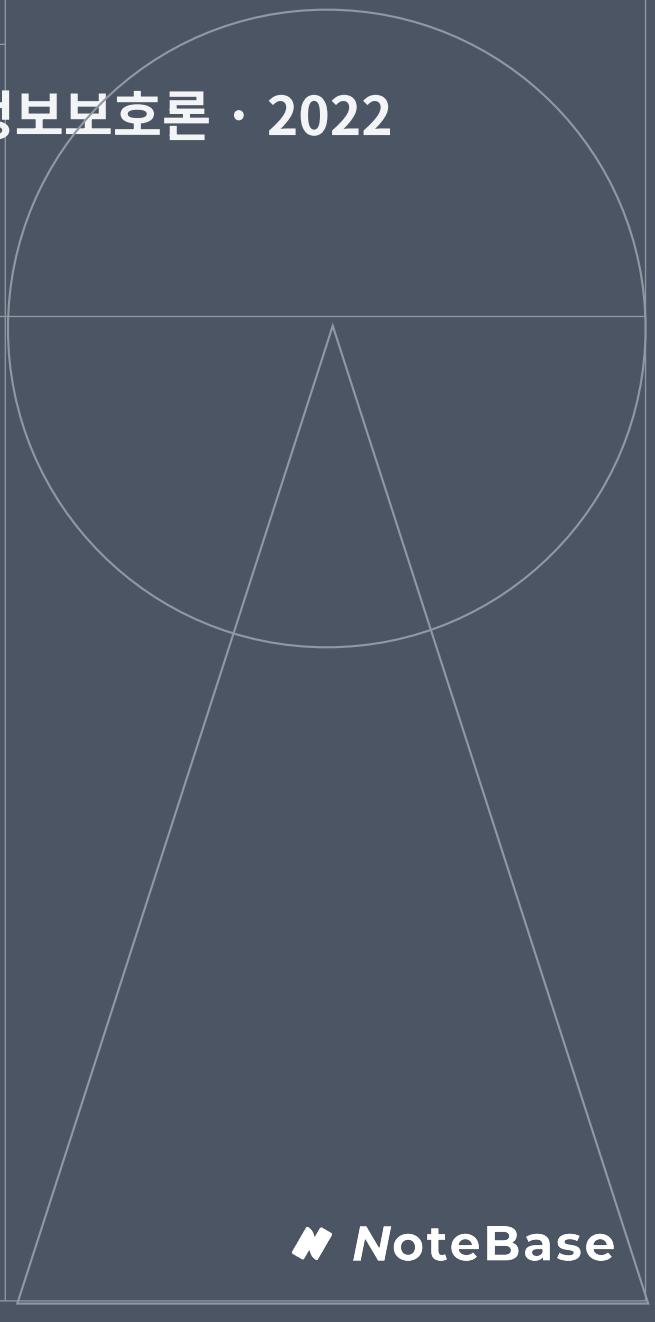
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2022



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2022

공무원/경찰/공채(경위) · 정보보호론 · 2022

문 1. 무결성(Integrity)을 위협하는 보안 공격(Security Attack)으로 가장 적절하지 않은 것은?

① 변경(Modification)

② 트래픽 분석(Traffic Analysis)

③ 부인(Repudiation)

④ 가장(Masquerading)

정답 2번

간단한 해설

트래픽 분석은 통신량·시점·상대방 등의 패턴을 관찰해 정보를 추론하는 수동적 공격으로, 주로 **기밀성**을 위협한다. 데이터를 부당하게 바꾸거나 통신 주체와 행위의 진실성을 훼손하는 공격과 구별된다.

선지별 해설

① (O) 변경은 권한 없이 메시지나 저장된 데이터의 내용을 바꾸는 공격이다. 원래 정보의 정확성과 일관성을 훼손하므로 **무결성을 직접 위협**한다.

② (X) 트래픽 분석은 메시지 내용 자체를 바꾸지 않고 통신의 양·빈도·시점·송수신자 등의 특성을 관찰하여 정보를 추론한다. 따라서 이 분류에서는 무결성 공격이 아니라 **기밀성을 위협하는 수동적 공격**이다. 통신 내용이 암호화되어 있어도 외부에 드러나는 패턴에서 정보가 노출될 수 있다.

③ (O) 부인은 실제로 메시지를 보내거나 받은 당사자가 그 행위를 하지 않았다고 주장하는 것이다. 직접적으로는 **부인방지**를 위협한다. 무결성을 정보의 부당한 변경 방지뿐 아니라 진정성과 부인방지까지 포함하는 넓은 의미로 분류하면, 부인도 무결성을 위협하는 공격에 포함된다.

④ (O) 가장은 공격자가 정당한 사용자나 통신 주체인 것처럼 신분을 속이는 공격이다. 메시지의 출처나 행위 주체의 **진정성**을 훼손하며, 정당한 사용자의 권한으로 허위 정보를 입력하거나 변경할 수도 있다. 따라서 진정성을 포함하는 무결성에 대한 위협으로 분류된다.

NoteBase

문 2. 어떤 컴퓨터가 대칭키 암호화 연산을 초당 2^{32}번 수행한다고 하자. 56비트 키를 전수조사 공격을 통해서 찾을 경우 소요되는 시간과 128비트 키로 변경할 경우 전수조사 공격으로부터 안전한지 여부에 대하여 가장 적절한 것은?

① 약 3개월 소요, 키의 크기가 128비트이면 전수공격에 안전하지 않다.

② 약 6개월 소요, 키의 크기가 128비트이면 전수공격에 안전하지 않다.

③ 약 3개월 소요, 키의 크기가 128비트이면 전수공격에 안전하다고 말할 수 있다.

④ 약 6개월 소요, 키의 크기가 128비트이면 전수공격에 안전하다고 말할 수 있다.

정답 4번

간단한 해설

56비트의 전체 키 공간을 조사하는 시간은 $2^{56}/2^{32} = 2^{24}$초로, 약 194일, 즉 **약 6개월**이다. 같은 속도에서 128비트 키의 전수조사에는 2^{96}초가 걸리므로 **주어진 전수조사 공격에 대해 계산적으로 안전**하다고 판단한다.

NoteBase

계산 과정

키 길이가 n비트이면 가능한 키는 2^n개이다. 암호화 연산 한 번으로 후보 키 하나를 시험할 수 있다고 보고, 주어진 컴퓨터의 속도로 전체 키 공간을 빠짐없이 조사하는 시간을 계산한다.

56비트 키: 전체 후보 수를 초당 시험 횟수로 나눈다.
$T_{56} = \frac{2^{56}}{2^{32}} = 2^{24} = 16{,}777{,}216$초이다.
하루는 86,400초이므로 $\frac{16{,}777{,}216}{86{,}400} \approx 194.2$일이다. 한 달을 약 30일로 보면 약 6.5개월이므로 선택지의 **약 6개월**에 해당한다.

평균 탐색시간과의 구별: 키가 균등하게 선택되고 중복 없이 탐색하다가 발견 즉시 멈추면, 평균적으로 전체 후보의 약 절반을 시험한다. 이 경우 시간은 약 2^{23}초, 즉 약 97일이어서 약 3개월이다. 이 문제의 전수조사 시간은 **전체 키 공간을 조사하는 기준**이며, 평균 발견시간과 혼동하지 않아야 한다.

128비트 키: 같은 속도가 유지되면 $T_{128} = \frac{2^{128}}{2^{32}} = 2^{96}$초이다. 1년을 365일로 환산하면 $\frac{2^{96}}{365 \times 86{,}400} \approx 2.51 \times 10^{21}$년이므로 현실적으로 실행하기 어려운 규모이다. 평균적으로 절반만 조사한다고 보아도 이 판단은 달라지지 않는다.

안전성의 범위: 가능한 키가 충분히 무작위로 선택되고 더 효율적인 취약점 공격이 없다는 전제에서, 128비트 키는 제시된 속도의 전수조사에 대해 계산적으로 안전하다. 키 길이만 늘리면 취약한 구현이나 키 유출까지 모두 막을 수 있다는 뜻은 아니다.

따라서 전체 키 공간 조사에 약 6개월이 걸리고, 128비트 키는 주어진 전수조사에 안전하다고 보는 ④와 일치한다.

NoteBase

문 3. 디지털 콘텐츠 보호에 활용되는 저작권 기술에 대한 설명으로 가장 적절하지 않은 것은?

① 디지털 워터마킹(Digital Watermarking)은 원본의 내용을 왜곡하지 않는 범위 내에서 혹은 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.

② 핑거프린팅(Fingerprinting)은 디지털 콘텐츠를 구매할 때 판매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.

③ DRM(Digital Rights Management)은 디지털 콘텐츠의 불법 복제와 유포를 막고 지적재산권 보유자의 이익과 권리를 보호해 주는 기술과 서비스를 말한다.

④ DRM(Digital Rights Management) 구성요소 중 메타데이터(Metadata)는 콘텐츠 생명주기 범위 내에서 관리되어야 할 각종 데이터의 구조 및 정보를 의미한다.

정답 2번

간단한 해설

불법 유출 경로를 추적하는 **핑거프린팅**은 판매자 정보가 아니라 **구매자나 배포본을 구별하는 정보**를 콘텐츠에 삽입한다. 불법 복제본에서 이 표식을 추출하여 어느 구매자에게 제공된 사본인지 확인하는 것이 핵심이다.

선지별 해설

① (O) 디지털 워터마킹은 콘텐츠의 이용 가치를 크게 훼손하지 않도록 저작권자나 권리 관련 정보를 콘텐츠에 삽입하는 기술이다. 삽입한 **워터마크**를 검출하여 권리 표시나 소유권 확인에 활용할 수 있다. 사용자가 쉽게 알아차리지 못하도록 삽입하는 비가시적 방식도 사용된다.

② (X) 여기서 핑거프린팅은 구매자마다 다른 식별정보를 각 배포본에 삽입하여 유출된 사본의 출처를 추적하는 기술이다. 따라서 **판매자 정보가 아니라 구매자 식별정보**로 고쳐야 한다. 동일한 판매자의 정보만 넣으면 여러 구매자 중 누구에게 제공된 사본이 유출되었는지 구별하기 어렵다.

③ (O) DRM은 디지털 콘텐츠의 권리와 이용 조건을 관리하고, 허가되지 않은 복제·이용·유포를 제한하여 권리자의 이익을 보호하는 기술과 서비스의 체계이다. 암호화, 인증, 이용권한 확인 등을 결합하여 **허용된 범위의 이용**을 관리한다.

④ (O) DRM에서 메타데이터는 콘텐츠를 생성·유통·이용하는 동안 필요한 각종 관리 정보를 구조화한 것이다. 콘텐츠 식별자, 권리자 정보, 이용 조건 등의 정보를 통해 콘텐츠와 권리를 연결하고 관리할 수 있다. 즉 콘텐츠 자체의 내용과 구별되는 **콘텐츠 관리용 데이터**이다.

NoteBase

문 4. 다음 암호화 알고리즘에 대한 설명으로 옳은 것은 모두 몇 개인가?

가. DES 알고리즘 : 64비트 평문을 64비트 암호문으로 암호화하며, 암호화와 복호화에 사용하는 키는 56비트이며 오류검출을 위해 8비트가 사용된다.
나. AES 알고리즘 : 128비트 암호화 블록으로 64, 128, 256비트의 다양한 키의 길이를 갖춘 알고리즘이다.
다. SEED 알고리즘 : 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 128비트 블록의 암호화 알고리즘이다.
라. RSA 알고리즘 : SSL 프로토콜을 가진 웹 브라우저, PGP 그리고 공개키 암호시스템에 사용된다.

① 1개
② 2개
③ 3개
④ 4개

정답 3번

간단한 해설

AES는 128비트 블록을 처리하며 키 길이는 **128·192·256비트**이다. 따라서 64비트 키를 포함한 나의 설명이 틀리고, DES의 키 구성·SEED의 개발과 블록 크기·RSA의 활용 분야에 관한 설명은 맞다.

NoteBase

보기별 해설

가. O: DES는 64비트 평문 블록을 64비트 암호문 블록으로 바꾸는 대칭키 블록 암호이다. 키는 64비트로 표현되지만 암호 연산에 실제 사용하는 유효 키는 56비트이고, 나머지 8비트는 각 바이트의 홀수 패리티를 검사하는 데 사용된다. 이 오류검출 비트는 **키의 표현에 관한 패리티 비트**이며, 암호문 전체의 무결성을 보장하는 기능을 뜻하지 않는다.

나. X: AES의 블록 크기가 128비트라는 부분은 맞지만, 키 길이에 64비트를 넣은 부분은 틀리다. AES에서 사용하는 키 길이는 **128·192·256비트**이다. 키 길이가 달라져도 AES의 블록 크기는 128비트로 일정하다.

다. O: SEED는 한국인터넷진흥원과 국내 암호 전문가들이 국내 기술로 개발한 대칭키 블록 암호이다. 128비트 블록을 처리하므로 보기의 설명과 일치한다. DES·AES·SEED는 대칭키 블록 암호라는 공통점이 있지만, 블록 크기와 키 길이는 알고리즘별로 구분해야 한다.

라. O: RSA는 서로 대응하는 공개키와 개인키를 사용하는 공개키 암호 알고리즘이다. SSL 기반 웹 통신과 PGP에서 키 전달이나 전자서명 등의 용도로 활용되어 왔으므로 활용 분야에 관한 설명은 맞다. 이때 실제 메시지 전체를 반드시 RSA로 암호화한다는 뜻은 아니며, 대칭키 암호와 함께 사용할 수 있다. 또한 SSL의 역사적 활용을 설명하는 것이지 현재의 보안 통신에 SSL 사용을 권장하는 것은 아니다.

옳은 보기는 가·다·라의 3개이므로 ③과 일치한다.

NoteBase

문 5. 다음 지문에서 설명하는 일방향 해시함수의 내용에 따른 인증 수행 방법으로 가장 적절한 것은?

일방향 해시함수를 사용하면 무결성을 확인할 수 있으나 송신자의 거짓 위장을 검출하지 못한다. 파일의 무결성을 조사함과 동시에 정당한 송신자의 것인가를 확인하는 인증을 필요로 한다.

① ECC(Elliptic Curve Cryptography)
② MDC(Modification Detection Code)
③ MAC(Message Authentication Code)
④ PGP(Pretty Good Privacy)

정답 3번

간단한 해설

MAC(메시지 인증 코드)는 메시지와 송수신자가 공유하는 비밀키로 인증값을 만들어, 메시지의 무결성과 송신자의 정당성을 함께 확인한다. 비밀키 없이 계산하는 일반 해시값만으로는 송신자 위장을 막을 수 없다.

공통 해설

일반적인 일방향 해시함수는 같은 메시지에서 같은 해시값을 계산하므로, 신뢰할 수 있는 원래 해시값과 비교하면 파일의 변경 여부를 확인할 수 있다. 그러나 공격자가 메시지와 함께 전달되는 해시값까지 바꿀 수 있다면, 변조한 메시지의 해시값을 새로 계산해 보낼 수 있다. 따라서 **비밀키 없는 해시값만으로는 송신자를 인증할 수 없다**.

MAC(Message Authentication Code)는 **메시지와 공유 비밀키를 이용해 생성하는 인증값**이다. 송신자는 메시지에 대한 MAC을 생성해 함께 보내고, 수신자는 같은 비밀키와 받은 메시지로 MAC을 다시 계산하여 전달된 값과 비교한다. 안전한 MAC 알고리즘을 사용하고 비밀키가 노출되지 않았다면, 키를 모르는 공격자는 메시지를 바꾸더라도 그에 맞는 유효한 MAC을 만들기 어렵다. 이 원리로 메시지의 무결성과 해당 키를 가진 송신자로부터 왔다는 사실을 함께 확인한다.

지문의 '무결성을 조사함과 동시에 정당한 송신자의 것인가를 확인'한다는 요구는 이러한 MAC의 기능에 해당한다. 특히 해시함수와 비밀키를 결합해 MAC을 구현하는 대표적인 방식이 HMAC이다.

NoteBase

문 6. 다음 지문에서 설명하는 사회공학적 해킹방법으로 가장 적절한 것은?

공격자는 피해자가 가지고 있는 가치 있는 정보를 포기하도록 유도하는 사회공학의 한 형태이다. 예를 들어, 공격자가 직원에게 전화를 걸어 CEO나 정보기술팀의 권한자로 가장하여 피해자에게 자신의 존재를 확신시키고, 피해자로부터 원하는 정보를 수집한다.

① Quid Pro Quo

② Pretexting

③ Clickjacking

④ Dumpster Diving

정답 2번

간단한 해설

CEO나 정보기술팀의 권한자인 것처럼 **허위 신분과 그럴듯한 상황을 만들어 신뢰를 얻는** 것이 핵심이다. 이러한 명분으로 상대방의 정보 제공을 유도하는 방법을 프리텍스팅(Pretexting)이라고 한다.

NoteBase

대응 관계 해설

사회공학은 프로그램의 결함만을 이용하는 대신 사람의 신뢰, 권위에 대한 복종, 호의 등을 악용하여 정보를 얻거나 특정 행동을 유도하는 공격이다. 이 사례에서는 정보를 얻는 매체가 전화라는 점보다 상대를 믿게 만드는 방식이 공격을 구별하는 기준이다.

사례와 Pretexting의 대응: 프리텍스팅은 허위 신분·상황·업무상 명분을 꾸며 피해자의 경계심을 낮추는 방법이다. CEO나 정보기술팀의 권한자를 사칭하는 행위는 자신이 정보를 요구할 정당한 권한을 가진 사람이라고 믿게 만드는 장치이다. 직원은 그 **거짓 신분에 대한 신뢰** 때문에 평소 공개하지 않을 정보를 제공하게 된다.

Quid Pro Quo와의 구별: 대가나 도움을 제공하겠다고 약속하면서 그 반대급부로 정보나 접근 권한을 요구하는 방식이다. 무료 기술지원 등의 대가로 정보를 받으려는 교환 구조가 핵심이다. 이 사례에는 대가를 제시하는 조건이 없으므로, 정보기술팀을 사칭했다는 사실만으로 이를 Quid Pro Quo라고 분류할 수 없다.

Clickjacking과의 구별: 사용자가 보는 화면과 실제 클릭 대상이 달라지도록 투명한 화면 요소 등을 겹쳐, 의도하지 않은 버튼이나 링크를 누르게 하는 방식이다. 핵심은 **화면 조작을 통한 클릭의 가로채기**이며, 전화 상대방의 권한을 가장하여 정보를 얻는 사례와 다르다.

Dumpster Diving과의 구별: 버려진 문서나 저장매체 등을 뒤져 내부 정보, 계정 단서 등을 수집하는 방법이다. 정보의 획득 경로가 폐기물이라는 점이 특징이며, 상대방을 대화로 속여 스스로 정보를 제공하게 하는 사례에 해당하지 않는다.

따라서 제시된 권한자 사칭과 정보 제공 유도는 ② Pretexting에 대응한다.

NoteBase

문 7. 공개키 기반구조(PKI)의 구성요소에 대한 설명으로 가장 적절하지 않은 것은?

① 이용자 : 공개키 사용자는 메시지를 암호화해서 송신하거나 전자서명을 검증한다.

② 인증기관(CA) : 다른 인증기관(CA)과 상호인증을 제공한다.

③ 저장소 : 디렉터리를 관리하는 서버는 OCSP(Online Certificate Status Protocol)를 이용하여 X.500 디렉터리 서비스를 제공한다.

④ 인증기관(CA) : 인증서를 폐지하는 경우 인증기관은 인증서 폐지 목록(Certificate Revocation List, CRL)을 작성한다.

정답 3번

간단한 해설

OCSP는 **인증서의 폐지 상태를 온라인으로 확인하는 프로토콜**이다. X.500 계열 디렉터리 정보의 검색·접근에는 LDAP 등을 사용하므로, OCSP가 디렉터리 서비스를 제공한다는 설명은 기능을 혼동했다.

선지별 해설

① O: 공개키 암호 방식에서 송신자는 수신자의 공개키로 메시지를 암호화하고, 수신자는 대응하는 개인키로 복호화한다. 전자서명의 경우 서명자는 자신의 개인키로 서명하고 검증자는 서명자의 공개키로 검증한다. 따라서 이용자가 공개키로 수행하는 대표 기능을 바르게 설명했다. 공개키의 소유자를 믿을 수 있도록 연결하는 것이 인증서의 역할이다.

② O: 인증기관(CA)은 다른 CA에 대한 인증서를 발급하여 서로 다른 인증 영역 사이에 신뢰 경로를 형성할 수 있다. 이러한 교차인증을 통해 이용자는 다른 CA가 발급한 인증서까지 검증할 수 있다. 모든 CA가 반드시 모든 다른 CA와 상호인증한다는 의미는 아니며, 정책과 신뢰 관계에 따라 구성된다.

③ X: OCSP는 개별 인증서의 **폐지 상태를 온라인으로 질의·응답하는 프로토콜**이다. X.500 계열 디렉터리의 정보에 접근하여 인증서·CRL 등을 검색하는 데 사용하는 대표적인 프로토콜은 LDAP이며, X.500의 기본 접근 프로토콜인 DAP도 있다. 따라서 디렉터리 서비스와 OCSP의 기능을 혼동했다. OCSP의 긍정 응답만으로 인증서의 모든 유효성 검사가 끝나는 것도 아니다.

④ O: 인증기관은 인증서 폐지 정보를 CRL로 작성·발행하여 이용자가 해당 인증서를 계속 신뢰해서는 안 된다는 사실을 확인하게 한다. CRL에는 폐지된 인증서의 일련번호와 폐지 시각 등의 정보가 포함되며, 이용자는 발행자의 서명과 목록의 갱신 시점도 확인한다. 이는 CA의 일반적인 인증서 수명주기 관리 업무에 관한 설명이다.

NoteBase

문 8. 다음 지문과 같은 특징을 갖는 접근통제 모델로 가장 적절한 것은?

- 무결성 중심의 상업 환경에 적합하게 설계된 모델
- 금융자산관리 및 회계분야에 주로 사용
- 체계화된 거래를 위한 접근통제 모델
- 인가자의 부적절한 정보 변조를 방지하는 직무분리를 반영

① BIBA 모델

② BLP 모델

③ State Machine 모델

④ Clark-Wilson 모델

정답 4번

간단한 해설

상업적 데이터의 무결성을 **체계화된 거래와 직무분리**로 보호한다는 점이 Clark-Wilson 모델의 핵심이다. 단순히 무결성을 다룬다는 사실만이 아니라, 인가된 사용자도 정해진 절차와 역할 분담에 따라 데이터를 처리하게 한다는 단서를 함께 보아야 한다.

구성 요소별 해설

상업 환경의 무결성: **Clark-Wilson 모델**은 업무 데이터가 올바른 상태를 유지하도록 보호하는 데 초점을 둔다. 기밀성을 중심으로 하는 BLP 모델과 구별되며, BIBA도 무결성 모델이지만 그것만으로는 거래 절차와 직무분리라는 나머지 단서까지 설명되지 않는다.

금융·회계 업무: 잔액이나 회계 장부는 단순히 열람 권한만 통제해서는 충분하지 않다. 금액 변경이 승인된 업무 규칙에 맞게 이루어지고 처리 전후의 일관성이 유지되어야 하므로, **상업적 거래의 정확성**을 보호하는 이 모델이 적합하다.

체계화된 거래: 사용자가 보호 대상 데이터를 임의로 직접 바꾸지 못하게 하고, 검증된 **변환 절차**를 통해서만 변경하게 한다. 예를 들어 자금 이체에서는 출금과 입금이 정해진 절차로 함께 처리되어 유효한 상태에서 다른 유효한 상태로 전환되어야 한다.

직무분리: 거래의 승인·실행·검증 등 중요한 역할을 분리하여 한 사람이 권한을 악용해 부적절한 변경을 하고 이를 숨기기 어렵게 한다. 외부 비인가자뿐 아니라 **인가된 내부자의 부정행위**도 통제한다는 점이 중요하다.
이러한 거래 통제와 직무분리를 함께 제시한 모델은 ④ Clark-Wilson 모델이며, 일반적인 상태 전이의 안전성을 다루는 State Machine 모델보다 지문의 특징에 구체적으로 부합한다.

NoteBase

문 9. 사용자 인증의 내용으로 가장 적절하지 않은 것은?

① 통합 인증 체계(Single Sign On, SSO)는 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보시스템에 재인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션이다.

② 일회용 패스워드(One-Time Password, OTP)의 비동기화 방식은 시간 혹은 계수기 메커니즘을 기반으로 한다.

③ 생체인증시스템 설계 시 고려 사항으로 무결성, 속도 및 처리량, 프라이버시, 위조 저항성 등이 있다.

④ 커버로스(Kerberos)의 구성요소인 KDC(Key Distribution Center)는 키 분배 서버로 사전공격이 발생하고 있어도 알지 못한다.

정답 2번

간단한 해설

시간이나 계수기를 공통 기준으로 OTP를 생성하는 방식은 **동기화 방식**이다. 비동기 방식의 대표적인 형태는 서버의 질의값에 대한 응답으로 인증하는 방식이다.

NoteBase

선지별 해설

① O. SSO는 한 번의 사용자 인증 결과를 연동된 여러 서비스가 활용하여 **서비스마다 로그인 정보를 다시 입력하는 절차를 줄이는** 방식이다. 각 서비스는 인증 토큰이나 티켓 등을 검증하여 접근을 허용한다. 적용 범위는 SSO에 연동된 시스템이며, 세션 만료나 추가 보안 확인에 따른 재인증까지 영구적으로 없어지는 것은 아니다.

② X. 시간 또는 계수기를 기준으로 OTP를 생성하는 것은 **동기화 방식**이다. 시간 동기 방식은 사용자 장치와 서버가 같은 시간 구간을, 계수기 동기 방식은 같은 순번을 기준으로 값을 계산한다. 반면 비동기 방식은 서버가 제시하는 질의값에 대해 사용자가 비밀키 등을 이용한 응답값을 생성하는 **질의·응답 방식**을 대표적으로 사용한다.

③ O. 생체인증시스템은 생체정보와 인증 결과의 변조를 막는 무결성, 신속한 인증을 위한 처리 속도와 동시 이용자를 감당하는 처리량을 고려해야 한다. 또한 민감한 생체정보의 수집·이용·저장에 따른 프라이버시와 가짜 지문·사진 등을 이용한 **위조 시도에 대한 저항성**도 중요하다. 인증 정확도만 높고 정보 보호나 운영 성능이 부족한 시스템은 안전하게 운용하기 어렵다.

④ O. KDC는 커버로스에서 인증과 티켓·키 분배를 담당하는 신뢰 기관이다. 이 선지는 공격자가 이미 확보한 인증 교환 자료에 대해 비밀번호 후보를 자신의 장치에서 시험하는 **오프라인 사전공격**의 탐지 한계로 이해해야 한다. 개별 추측을 KDC에 보내지 않으므로 KDC는 그 추측이 진행 중이라는 사실을 직접 관찰하기 어렵다. 서버에 반복 요청을 보내는 온라인 공격은 로그나 시도 제한으로 대응할 수 있으므로, 모든 사전공격을 언제나 탐지할 수 없다는 의미로 일반화할 수는 없다.

따라서 시간·계수기 기반 OTP를 비동기화 방식으로 설명한 ②가 가장 적절하지 않다.

NoteBase

문 10. 다음 지문의 리눅스 패스워드 규칙 설정 내용으로 가장 적절하지 않은 것은?

```
#cat /etc/security/pwquality.conf
minlen = 9
lcredit = -1
ucredit = -1
dcredit = -1
ocredit = -1

#cat /etc/login.defs
PASS_MAX_DAYS 90
PASS_MIN_DAYS 1
PASS_MIN_LEN 9
PASS_WARN_AGE 7
```

① 비밀번호는 최소 9자리 이상이어야 한다.

② 비밀번호는 최대 90일 변경주기를 가지고 있다.

③ 숫자, 소문자, 대문자는 각각 하나 이상을 포함해야 한다.

④ 특수문자를 사용하기 위해서는 별도의 설정값을 포함해야 한다.

정답 4번

간단한 해설

지문에 이미 **ocredit = -1**이 있으므로 특수문자를 최소 1개 포함해야 한다. 별도의 설정을 추가해야 사용할 수 있는 것이 아니며, 음수 값은 해당 문자 종류의 **최소 포함 개수**를 뜻한다.

NoteBase

선지별 해설

지문은 비밀번호의 길이·문자 구성을 정하는 pwquality.conf와 사용기간 등의 기본값을 정하는 login.defs의 설정을 제시한다. 각 설정값이 적용되는 비밀번호 규칙을 해석한다.

① O: pwquality.conf의 **minlen = 9**는 최소 길이를 9자로 정한다. 이 지문에서는 lcredit, ucredit, dcredit, ocredit가 모두 음수이므로 문자 종류별 길이 가산점을 주는 설정이 아니라 각 종류의 최소 포함 개수를 요구한다. 따라서 가산점으로 실제 길이를 줄이는 경우가 아니며, 비밀번호는 9자 이상이어야 한다. login.defs에도 PASS_MIN_LEN 9가 표시되어 있지만, PAM 기반 환경의 길이 검사에서는 지문에 제시된 pwquality 설정이 중요하다.

② O: **PASS_MAX_DAYS 90**은 비밀번호의 최대 사용기간을 90일로 정한 기본값이다. PASS_MIN_DAYS 1은 변경 후 다시 변경하기까지의 최소 간격이 1일, PASS_WARN_AGE 7은 만료 7일 전부터 경고한다는 뜻이다. 다만 login.defs의 이러한 기간 설정은 계정 생성 시 기본값으로 사용되므로, 파일의 값을 바꾼다고 기존 모든 계정의 기간이 자동으로 바뀌는 것은 아니다.

③ O: dcredit는 숫자, lcredit는 소문자, ucredit는 대문자에 관한 설정이다. 이 값이 음수이면 그 절댓값이 해당 문자 종류의 최소 개수이므로, **각각 -1은 해당 문자를 최소 1개 포함**하라는 뜻이다. 숫자·소문자·대문자 중 하나만 골라 넣는다는 의미가 아니다.

④ X: 지문에는 이미 **ocredit = -1**이 설정되어 있다. ocredit는 숫자·대문자·소문자 이외의 문자에 관한 항목이며, 여기서는 특수문자를 최소 1개 포함하도록 요구한다. 따라서 특수문자를 위해 별도의 설정값을 더 넣어야 한다는 설명은 부적절하다. 이 항목은 특수문자의 사용을 새로 허용하는 스위치가 아니라, 포함 개수에 대한 조건이다.

NoteBase

문 11. 다음 중 버퍼 오버플로우(Buffer Overflow) 대응방법으로 가장 적절하지 않은 것은?

① DLP (Data Loss Prevention)

② ASLR (Address Space Layout Randomization)

③ Stack Guard

④ Stack Shield

정답 1번

간단한 해설

DLP는 **민감한 정보의 무단 반출·유출을 탐지하고 통제**하는 기술이다. 메모리 주소를 예측하기 어렵게 하거나 반환 주소의 변조를 막는 버퍼 오버플로우 대응기법과는 보호 대상이 다르다.

선지별 해설

버퍼 오버플로우는 확보된 버퍼의 경계를 넘어 데이터를 기록하여 인접한 메모리 내용을 훼손하는 현상이다. 특히 스택의 반환 주소가 변조되면 프로그램의 실행 흐름이 공격자가 의도한 곳으로 바뀔 수 있으므로, 주소 예측을 어렵게 하거나 제어 정보의 변조를 탐지·차단하는 방어가 사용된다.

① X: DLP는 문서나 전송 데이터 등에 포함된 민감정보를 식별하고, 외부 전송·복사 등 정책에 어긋나는 유출 경로를 통제한다. **버퍼 경계 초과나 반환 주소 변조를 직접 방어하는 기술은 아니다.** 이름이 비슷한 DEP는 실행 권한이 없는 메모리 영역에서 코드가 실행되지 못하게 하여 악성 코드 실행을 완화하는 기술이므로 DLP와 구별된다.

② O: ASLR은 실행 파일·라이브러리·스택·힙 등 메모리 영역의 배치 주소를 무작위화하여 공격에 필요한 주소를 예측하기 어렵게 한다. 공격자가 알아야 할 **목표 주소의 불확실성**을 높이는 방식이다. 잘못된 메모리 쓰기 자체를 없애는 것은 아니므로 입력 길이 검증 등과 함께 사용한다.

③ O: Stack Guard는 스택의 중요한 제어 정보 앞에 카나리 값을 두고, 함수가 반환하기 전에 그 값이 훼손되었는지 검사하는 방식으로 스택 변조를 탐지한다. 버퍼를 넘친 데이터가 반환 주소까지 덮어쓰는 과정에서 카나리도 바뀌면 비정상 실행을 차단한다. 핵심은 **카나리 값의 무결성 검사**이다.

④ O: Stack Shield는 함수 호출 때 반환 주소를 별도의 저장 영역에 복사해 보관하고, 반환할 때 그 사본을 이용하여 반환 주소를 복원하거나 변조 여부를 검사하는 방식이다. 따라서 일반 스택의 반환 주소가 덮어써지더라도 그 값만 믿고 제어를 넘기지 않도록 보호한다. 카나리를 검사하는 Stack Guard와 달리 **반환 주소의 별도 사본**을 이용한다.

NoteBase

문 12. 어떤 이미지에 작은 변화를 주어 딥러닝 네트워크가 판단할 때 결정경계(Decision Boundary)를 넘겨 잘못 인식하게 만드는 방법으로, AI 알고리즘에 내재되어 있는 취약점에 의해 발생할 수 있는 공격으로 가장 적절한 것은?

① Adversarial Attack

② Side Channel Attack

③ Bluekeep

④ Deepfake

정답 1번

간단한 해설

모델이 잘못 분류하도록 이미지에 의도적인 작은 교란을 가하는 것은 **적대적 공격**이다. 사람에게는 거의 같은 이미지여도 모델의 결정경계를 넘으면 분류 결과가 바뀔 수 있다.

개념 구분

① 적대적 공격(Adversarial Attack)은 학습된 모델이 잘못 판단하도록 입력 등을 의도적으로 조작하는 공격이다. 발문은 그중 이미지를 조금 바꾸어 분류 결과를 뒤집는 적대적 예제 공격을 설명한다. '결정경계'는 모델이 서로 다른 범주로 분류하는 영역의 경계이며, 공격자는 입력이 이 경계를 넘도록 작은 교란을 가한다. 사람에게는 거의 같은 이미지로 보여도 모델의 출력은 달라질 수 있으므로, '작은 변화'와 '오인식'이라는 단서에 일치한다.

② 부채널 공격(Side Channel Attack)은 연산 시간, 소비 전력, 전자파 등 시스템 동작에서 부수적으로 드러나는 정보를 이용하여 비밀 정보를 추론하는 공격이다. 모델에 넣을 이미지를 조작해 분류 결과를 바꾸는 것이 아니라, 구현 과정에서 새어 나오는 정보를 관찰한다는 점이 다르다.

③ BlueKeep는 일부 Windows의 원격 데스크톱 서비스에서 발견된 원격 코드 실행 취약점의 이름이다. 원격 데스크톱 연결을 처리하는 소프트웨어의 취약점에 관한 것이므로 딥러닝 모델의 결정경계를 넘기는 공격과 구별된다.

④ 딥페이크(Deepfake)는 딥러닝 등을 이용해 실제처럼 보이는 영상·이미지·음성 등을 합성하거나 변조하는 기술 또는 그 결과물이다. 사람이나 시스템을 속이는 데 악용될 수 있지만, 발문처럼 입력에 작은 교란을 가해 분류 모델의 판단을 바꾸는 공격을 직접 지칭하는 용어는 아니다.

따라서 발문의 공격은 적대적 공격을 뜻하는 ①이다.

NoteBase

문 13. 다음에서 커널의 기능으로 옳은 것을 모두 고른 것은?

㉠ 동기화(Synchronization)
㉡ 프로세스간 통신(Inter Process Communication)
㉢ POST(Power On Self Test)
㉣ 메시지 전달(Message Passing)

① ㉠, ㉡, ㉢, ㉣
② ㉠, ㉡, ㉣
③ ㉡, ㉢, ㉣
④ ㉠, ㉢

정답 2번

간단한 해설

커널은 실행 중인 프로세스의 **동기화와 통신**을 지원하며 메시지 전달도 이에 포함된다. 반면 **POST**는 운영체제 실행 전에 펌웨어가 수행하는 하드웨어 초기 점검이므로 커널의 기능에 해당하지 않는다.

보기별 해설

㉠ (O) 동기화는 여러 프로세스나 스레드가 공유 자원을 사용할 때 실행 순서와 접근을 조절하는 기능이다. 커널은 세마포어·뮤텍스 등 동기화 수단과 대기·깨우기 기능을 지원하여 **경쟁 상태**를 방지하고 필요한 실행 순서를 보장하도록 돕는다.

㉡ (O) 프로세스간 통신은 서로 다른 프로세스가 데이터를 교환하고 협력할 수 있게 하는 기능이다. 커널은 공유 메모리, 파이프, 메시지 큐 등의 통신 수단을 관리하거나 필요한 기반을 제공하여 **프로세스 사이의 정보 교환**을 지원한다.

㉢ (X) POST는 전원을 켠 뒤 메모리 등 주요 하드웨어가 정상적으로 동작하는지 확인하는 자체 점검이다. 운영체제 커널이 실행되기 전의 부팅 단계에서 **BIOS·UEFI 등 펌웨어**가 담당하므로 커널 기능으로 분류하지 않는다.

㉣ (O) 메시지 전달은 프로세스가 메시지를 송신·수신하여 정보를 교환하는 방식이다. 커널은 통신 상대의 연결, 메시지 전달과 대기 처리 등을 지원한다. 이는 **프로세스간 통신의 한 방식**이므로 ㉡과 함께 옳은 항목이다.

옳은 보기는 ㉠, ㉡, ㉣이므로 ②이다.

NoteBase

문 14. 유닉스/리눅스의 파일 시스템 구조 중 I-node 블록에 대한 설명으로 가장 적절하지 않은 것은?

① 각 파일이나 디렉터리에 대한 모든 정보를 저장한다.

② 모든 파일은 반드시 하나의 아이노드(I-node) 블록을 갖는다.

③ 전체 파일 시스템에 대한 정보를 저장한다.

④ 파일의 소유자, 유형, 접근권한, 접근시간, 크기, 링크 수, 저장된 블록 주소 등의 정보를 저장한다.

정답 3번

간단한 해설

아이노드는 개별 파일이나 디렉터리의 속성과 데이터 위치를 관리한다. **전체 파일시스템의 관리 정보는 슈퍼블록**에 저장된다.

선지별 해설

① O. 이 문항에서 말하는 정보는 ④에 나열된 것처럼 **개별 파일·디렉터리의 속성과 관리 정보**를 뜻한다. 아이노드는 소유자, 접근권한, 크기, 데이터 위치 등을 관리한다. 다만 '모든 정보'를 파일명이나 파일 내용까지 전부 저장한다는 뜻으로 확대하면 부정확하다. 파일명과 아이노드 번호의 대응은 해당 이름이 속한 디렉터리 엔트리에 저장된다.

② O. 유닉스 계열 파일시스템에서 개별 파일 객체는 **하나의 아이노드 항목**으로 관리된다. 여기서 '아이노드 블록'은 파일에 대응하는 아이노드를 가리키는 표현이며, 파일마다 물리적인 디스크 블록 하나를 독점한다는 뜻은 아니다. 하나의 블록에 여러 아이노드 항목이 들어갈 수 있고, 여러 하드 링크 이름이 동일한 아이노드를 가리킬 수도 있다.

③ X. 전체 파일시스템의 블록 수, 아이노드 수, 블록 크기 등 **파일시스템 전체의 관리 정보는 슈퍼블록**에 저장된다. 아이노드는 개별 파일이나 디렉터리에 관한 정보를 담으므로, 정보를 관리하는 대상의 범위가 다르다.

④ O. 아이노드는 소유자 식별 정보, 파일 유형과 접근권한, 접근시간 등의 시간 정보, 파일 크기, 하드 링크 수 및 데이터의 저장 위치를 찾는 정보를 담는다. 이러한 항목은 **파일의 속성과 데이터 접근을 관리**하는 데 사용된다. 데이터 위치는 파일시스템 방식에 따라 블록 포인터나 익스텐트 정보 등으로 나타낼 수 있다.

따라서 슈퍼블록의 기능을 아이노드의 기능으로 설명한 ③이 가장 적절하지 않다.

NoteBase

문 15. 무선 랜 통신 암호화에 대한 설명으로 가장 적절하지 않은 것은?

① WEP는 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용되기 시작했다.

② WPA-PSK는 802.11i 보안 표준의 일부분으로 WEP 방식의 보안 문제점을 해결하기 위해 만들어졌다.

③ WEP는 RC4 암호화 알고리즘을 기본으로 사용한다.

④ WPA-1은 CCMP 암호화방식을 사용하여 WEP 방식의 취약점을 해결하기 위해 제정된 표준이다.

정답 4번

간단한 해설

WPA-1은 WEP의 취약점을 보완하는 **TKIP**를 사용한다. **AES 기반 CCMP**는 WPA2의 대표적인 암호화 방식이므로 이를 WPA-1의 방식으로 설명하면 잘못이다.

출제 포인트

WEP, WPA-1, WPA2의 암호화 방식과 PSK의 의미를 구분하는 문제이다.

핵심 개념

WEP는 무선 구간의 데이터를 암호화하는 초기 보안 방식으로 RC4를 사용한다.
WPA-1은 WEP의 취약점을 보완한 보안 방식으로 TKIP를 사용하며 TKIP도 RC4 기반이다. WPA2는 IEEE 802.11i를 반영하며 AES 기반 CCMP를 지원한다.
PSK는 접속 장치들이 미리 공유한 키로 인증하는 방식이다. 암호화 알고리즘의 이름과 구분한다.

NoteBase

선지별 해설

① O
이 문항에서는 802.11b 무선 랜에 WEP가 적용되었다는 취지로 옳게 처리한다. 다만 WEP는 초기 IEEE 802.11 표준부터 포함되었으므로 '802.11b부터'를 정확한 최초 도입 시점으로 외우지는 않는다.

② O
WPA는 IEEE 802.11i의 일부 기능을 먼저 채택하여 WEP의 보안 문제를 보완했다. WPA-PSK는 그중 사전 공유 키를 이용하는 인증 방식이다.

③ O
WEP의 기본 암호화 알고리즘은 RC4이다. RC4는 키로 생성한 암호용 비트열을 데이터와 결합하는 스트림 암호이다.

④ X
'WPA-1은 CCMP 암호화방식을 사용'한다는 연결이 잘못이다. WPA-1의 기본 방식은 TKIP이며 AES 기반 CCMP는 WPA2에 대응한다.

오답 포인트

④의 'WEP 방식의 취약점을 해결'한다는 목적은 맞지만 암호화 방식을 CCMP로 연결한 부분이 잘못이다. 같은 보완 목적을 가진 WPA-1과 WPA2도 사용하는 방식은 구분한다.

다시 나오면 이렇게 판단

보안 방식과 암호화 방식을 먼저 연결한다. WEP는 RC4, WPA-1은 TKIP, WPA2는 AES 기반 CCMP로 구분하고 PSK는 인증에 쓰는 사전 공유 키라는 뜻으로 따로 판단한다.

암기 포인트

WEP는 RC4, WPA-1은 TKIP, WPA2는 CCMP이다. PSK는 사전 공유 키이다.

NoteBase

문 16. 블록체인(Blockchain) 기반 기술에 대한 설명으로 가장 적절하지 않은 것은?

① 분산 네트워크의 경우 블록체인 정보는 네트워크에 참여하는 노드들이 가지고 있으며 동일한 거래 내역이 분산 저장되어 관리된다.

② 암호 기술의 경우 개인 간 거래 시 생성되는 전자서명을 검증하여 거래내역이 변경되지 않았음을 입증하는데 ECDSA 전자서명 알고리즘을 이용한다.

③ 이중 거래 방지의 경우 악의적인 목적으로 동시에 두 곳 이상의 계좌로 송금하는 행위를 방지하기 위해서 총 통화량과 The Longest Chain Wins 메커니즘을 이용한다.

④ 비트코인, 모네로 등의 채굴은 대부분 지분증명(PoS, Proof of Staking) 방식을 사용한다.

정답 4번

간단한 해설

비트코인과 모네로는 채굴자의 계산 작업을 이용하는 **작업증명(PoW)** 방식이다. 맡긴 지분 등을 기준으로 검증에 참여하는 지분증명(PoS) 방식으로 설명한 부분이 틀리다.

NoteBase

선지별 해설

① O: 블록체인은 여러 참여 노드가 거래 기록을 공유·검증하고 분산된 원장으로 유지하는 구조이다. 유효한 거래 내역에 합의함으로써 특정 중앙 관리자가 유일한 원본을 보관하는 방식과 구별된다. 다만 모든 종류의 노드가 언제나 전체 기록을 똑같이 저장하는 것은 아니며, 경량 노드나 저장 공간을 줄이는 방식도 있다.

② O: 비트코인에서 대표적으로 사용되어 온 ECDSA는 타원곡선 기반 전자서명 알고리즘이다. 거래에 대한 서명을 공개키로 검증하여 정당한 개인키 보유자가 승인했는지와 서명이 보호하는 거래 정보가 바뀌지 않았는지를 확인한다. 이는 블록체인의 대표적인 암호 기술에 관한 설명이며, 모든 블록체인이나 모든 거래 형식이 반드시 ECDSA만 사용한다는 뜻은 아니다.

③ O: 여기서 '이중 거래'는 같은 자금을 서로 충돌하는 거래에서 중복 소비하려는 행위를 뜻한다. 여러 수취인에게 정상적으로 나누어 송금하는 행위 자체를 금지하는 것은 아니다. 노드는 발행·거래 금액 규칙과 이미 소비된 자금 여부를 검사하며, 유효한 체인이 갈라지면 'The Longest Chain Wins'로 요약되는 체인 선택 규칙에 따라 하나의 거래 이력에 합의한다. 비트코인에서 이는 정확히는 **누적 작업량이 가장 큰 유효 체인**을 선택한다는 뜻이다. 총 통화량을 제한하는 것만으로 이중 지불을 막는 것이 아니라, 거래 유효성 검사와 합의가 함께 작동한다.

④ X: 비트코인과 모네로의 채굴에는 **작업증명(PoW)**이 사용된다. 채굴자가 계산 작업을 수행하고 다른 노드가 그 작업 결과와 블록의 유효성을 검증한다. 지분증명(PoS, Proof of Stake)은 맡긴 지분 등을 바탕으로 검증 참여와 블록 생성 권한을 정하는 방식이므로 두 암호화폐의 채굴 방식과 다르다. 선지의 영문도 통상 'Proof of Stake'라고 표현한다.

NoteBase

문 17. 다음 지문은 VLAN(Virtual LAN)에 대한 설명이다. 빈칸에 들어갈 내용을 순서대로 나열한 것은?

VLAN이란 (㉠) 트래픽을 제한하여 불필요한 트래픽을 차단하기 위한 (㉡) LAN이다. 스위치는 허브처럼 한 포트에서 발생한 데이터를 모든 포트에 전달하지 않기 때문에 스위치에 흐르는 데이터를 분석하려면 허브와는 달리 (㉢) 기능을 사용해야 한다.

① ㉠ 멀티캐스팅 ㉡ 논리적인 ㉢ 포트미러링
② ㉠ 브로드캐스팅 ㉡ 논리적인 ㉢ 포트미러링
③ ㉠ 멀티캐스팅 ㉡ 물리적인 ㉢ 포트필터링
④ ㉠ 브로드캐스팅 ㉡ 물리적인 ㉢ 포트필터링

정답 2번

간단한 해설

VLAN은 물리적 배선을 나누는 대신 **논리적으로 브로드캐스트 전달 범위를 분리**한다. 다른 포트의 스위칭 트래픽을 분석하려면 해당 트래픽을 감시 포트로 복사하는 **포트미러링**을 사용한다.

빈칸별 해설

㉠ 브로드캐스팅: 브로드캐스팅은 같은 브로드캐스트 도메인 전체에 프레임을 전달하는 방식이다. VLAN은 **브로드캐스트 도메인을 분리**하여 한 VLAN의 브로드캐스트가 다른 VLAN으로 그대로 퍼지는 것을 막는다. 브로드캐스트 자체를 전부 없애는 것이 아니라 전달 범위를 제한한다. 특정 수신 집단을 대상으로 하는 멀티캐스팅은 이 빈칸에서 묻는 도메인 분리의 기준과 다르다.

㉡ 논리적인: VLAN은 물리적 배선이나 스위치 한 대의 경계와 별개로 장치들을 논리적으로 묶는 LAN이다. 같은 물리적 스위치의 포트도 서로 다른 VLAN에 속할 수 있으므로 **물리적 연결과 논리적 네트워크 소속**을 구분한다. 서로 다른 VLAN 사이의 통신에는 일반적으로 라우터나 3계층 스위치의 라우팅이 필요하다.

㉢ 포트미러링: 스위치는 목적지 MAC 주소를 학습한 일반 유니캐스트 프레임을 해당 포트로 전달하므로, 분석 장비를 임의의 다른 포트에 연결하는 것만으로 모든 통신을 볼 수는 없다. 포트미러링은 **선택한 포트나 VLAN의 트래픽을 복사**하여 분석 장비가 연결된 감시 포트로 보내는 기능이다. 트래픽을 허용하거나 차단하는 필터링과 구별된다. 스위치도 브로드캐스트나 목적지를 아직 모르는 유니캐스트 등은 같은 VLAN 안의 여러 포트로 전달할 수 있으므로, 지문의 비교를 '어떤 프레임도 여러 포트로 보내지 않는다'는 뜻으로 해석하지 않는다.

따라서 ㉠ 브로드캐스팅, ㉡ 논리적인, ㉢ 포트미러링의 조합인 ②와 일치한다.

NoteBase

문 18. APT(Advanced Persistent Threat) 침투 기법 중 드라이브-바이-다운로드(Drive-By-Download) 공격의 내용으로 가장 적절한 것은?

① 특정 기관의 구체적인 개인 또는 그룹을 목표로 진행되는 목표 지향적인 피싱공격이다.

② 공격자는 공격 대상이 주로 방문하는 웹사이트에 대한 정보를 사전에 파악한 후(사회공학적 기법) 제로데이 취약점을 이용해 해당 사이트에 악성코드를 심어두는 공격이다.

③ 다중 확산 메커니즘과 페이로드를 포함한 악성 소프트웨어로 목표를 오염시키는 공격이다.

④ 공격자는 사전에 USB 메모리에 악성코드를 삽입, 특정 타깃/조직의 이동 동선 상에 이를 방치한 후 누군가 이를 가져가서 내부 PC에 연결하는 순간 감염되게 하는 공격이다.

정답 3번

간단한 해설

드라이브-바이-다운로드는 웹사이트 방문 중 취약점을 악용해 **사용자 모르게 악성코드를 내려받아 감염시키는** 공격이다. 선지의 악성 소프트웨어 감염이라는 설명과 연결되지만 **다중 확산 메커니즘 자체가 필수 조건은 아니다**.

출제 포인트

APT의 침투에 쓰이는 스피어 피싱, 워터링 홀, 드라이브-바이-다운로드, 악성 USB 유인 공격의 특징을 구분한다.

핵심 개념

드라이브-바이-다운로드는 웹페이지에 접속하는 과정에서 브라우저나 플러그인의 취약점을 악용해 악성코드를 내려받고 실행하게 하는 방식이다. 사용자가 악성 파일을 의도적으로 다운로드하지 않아도 감염될 수 있다.
워터링 홀은 표적이 자주 방문하는 사이트를 미리 공격해 표적의 방문을 기다리는 방식이다. 워터링 홀 사이트에서 드라이브-바이-다운로드를 실행할 수 있으므로 두 개념은 함께 사용될 수 있다.
페이로드는 공격 과정에서 전달되어 정보 탈취 등 실제 악성 동작을 수행하는 코드나 기능을 뜻한다.

NoteBase

선지별 해설

① X
'구체적인 개인 또는 그룹을 목표로' 하는 피싱은 스피어 피싱이다. 불특정 다수에게 보내는 일반 피싱과 달리 표적을 정해 맞춤형으로 접근한다. 드라이브-바이-다운로드의 설명으로 고치려면 웹 방문 중 취약점을 통한 악성코드 다운로드와 감염을 제시해야 한다.

② X
'공격 대상이 주로 방문하는 웹사이트'를 미리 파악해 악성코드를 심는 것은 워터링 홀 공격의 설명이다. 드라이브-바이-다운로드는 그 사이트를 방문한 뒤 악성코드가 내려받아져 감염되는 기술적 과정에 초점을 둔다. 두 공격이 함께 쓰일 수 있지만 이 선지에서 직접 설명한 기법은 워터링 홀이다. 제로데이 취약점만 사용해야 하는 것은 아니다.

③ O
악성 소프트웨어와 페이로드로 목표 시스템을 감염시킨다는 점을 드라이브-바이-다운로드의 악성코드 전달·감염 과정과 연결한 설명이다. 다만 '다중 확산 메커니즘과 페이로드'는 악성 소프트웨어의 일반적 특성을 나타내는 표현이므로 이것만으로 해당 공격을 정의할 수는 없다. 정확한 구별 기준은 웹 방문을 계기로 사용자 모르게 악성코드가 내려받아지고 감염되는 과정이다.

④ X
악성코드를 넣은 USB를 표적의 이동 경로에 두어 연결하도록 유도하는 것은 USB 드롭 또는 베이팅 공격이다. 감염 경로가 이동식 저장매체이므로 웹을 통한 드라이브-바이-다운로드와 구별된다. USB를 연결하는 것만으로 모든 PC가 반드시 감염되는 것은 아니며 악성코드 실행이나 취약점 악용이 있어야 한다.

오답 포인트

②에 웹사이트와 제로데이 취약점이 등장한다고 두 기법을 같은 뜻으로 외우기 쉽다. 워터링 홀은 표적이 방문할 사이트를 고르는 전략이고 드라이브-바이-다운로드는 웹 방문 중 악성코드를 전달하는 방식이다. ③의 '다중 확산'을 드라이브-바이-다운로드의 필수 특징으로 외우는 것도 피한다.

다시 나오면 이렇게 판단

표적을 정한 피싱이면 스피어 피싱, 표적의 단골 사이트를 미리 공격하면 워터링 홀, 웹 방문 중 몰래 악성코드를 내려받아 감염시키면 드라이브-바이-다운로드, 주운 USB의 연결을 유도하면 USB 유인 공격으로 구분한다.

암기 포인트

스피어 피싱은 표적 맞춤, 워터링 홀은 단골 사이트, 드라이브-바이-다운로드는 웹 방문 중 감염, USB 드롭은 저장매체 유인이다.

NoteBase

문 19. 다음 지문에서 설명하는 내용으로 가장 적절한 것은?

고객 신용정보를 훔치기 위해 POS에 침입하는 공격이다. POS 시스템의 메모리를 검사하여 악용을 목적으로 신용카드번호 및 개인식별번호와 같은 민감 개인정보를 수집한다.

① Free-Riding Attack
② RAM-Scraping Attack
③ Ransomware
④ Side Channel Attack

정답 2번

간단한 해설

POS의 메모리를 검사하여 그 안에 노출된 카드 정보 등을 수집하는 공격은 **RAM 스크래핑**이다. 핵심은 저장 장치의 파일이나 부수적 신호가 아니라 처리 중인 메모리의 민감 정보를 직접 노린다는 점이다.

NoteBase

대응 관계 해설

지문의 'POS에 침입'은 판매 시점의 결제 처리 시스템을 공격 대상으로 삼았다는 뜻이다. '메모리를 검사'하고 '신용카드번호 및 개인식별번호와 같은 민감 개인정보를 수집'한다는 부분은, 처리 과정에서 메모리에 노출된 정보를 직접 읽어 탈취하는 방식을 가리킨다. 이 단서들이 **RAM-Scraping Attack**에 대응한다. 모든 POS가 개인식별번호를 평문으로 보관한다는 뜻은 아니며, 실제로 메모리에 접근 가능한 형태로 노출된 정보가 수집 대상이다.

② RAM-Scraping Attack은 악성코드 등이 RAM에 있는 민감한 정보를 찾아 수집하는 공격이다. 특히 POS의 결제 처리 중 일시적으로 존재하는 카드 정보가 대상이 될 수 있으므로, 지문의 공격 위치·수집 방법·목적이 모두 이 명칭과 연결된다.

① Free-Riding Attack은 필요한 대가나 기여를 하지 않으면서 타인의 자원·서비스를 무임승차하여 이용하는 공격을 뜻한다. 예를 들어 통신 서비스의 과금 규칙을 악용해 비용을 회피하는 경우가 있다. 메모리에서 카드 정보를 직접 수집하는 방식의 명칭은 아니다.

③ Ransomware는 파일을 암호화하거나 시스템 이용을 막은 뒤 복구 등의 대가로 금전을 요구하는 악성코드이다. 정보 유출을 함께 수행할 수도 있지만, 지문에는 암호화·접근 차단·몸값 요구가 없고 메모리 정보 수집이 핵심이다.

④ Side Channel Attack은 연산 시간·전력 소비·전자파 등 동작에서 부수적으로 드러나는 정보를 분석하여 비밀을 추론하는 공격이다. 메모리 내용 자체를 직접 읽어 수집하는 RAM 스크래핑과 정보 획득 경로가 다르다.

NoteBase

문 20. 다음 클라우드 컴퓨팅의 컨테이너 기술 중 ( )안에 들어갈 내용으로 가장 적절한 것은?

단일 시스템에서 여러 운영체제가 동시에 실행될 수 있도록 하는 가상화와 달리 컨테이너는 리눅스 커널의 기능인 (㉠)와(과) (㉡)을(를) 통해 서로 다른 애플리케이션 프로세스별로 공간을 격리한다.

① ㉠ cgroup ㉡ namespace

② ㉠ cgroup ㉡ dmesg

③ ㉠ pacct ㉡ dmesg

④ ㉠ wtmp ㉡ namespace

정답 1번

간단한 해설

컨테이너는 호스트 커널을 공유하면서 **cgroup으로 자원 사용을 제어**하고 **namespace로 프로세스가 보는 실행 환경을 분리**한다. 로그를 조회하거나 저장하는 도구·파일은 이 두 기능을 대신하지 못한다.

NoteBase

빈칸별 해설

지문은 별도의 게스트 운영체제를 실행하는 가상머신과, 호스트의 리눅스 커널을 공유하는 컨테이너를 대비한다. 컨테이너의 격리에는 자원 사용을 통제하는 기능과 서로 다른 실행 환경을 보이게 하는 기능이 함께 필요하다.

㉠ cgroup: 'control group'의 약자로, 프로세스를 그룹으로 묶어 CPU·메모리·입출력 등의 사용량을 관리하고 제한한다. 예를 들어 한 컨테이너가 사용할 수 있는 메모리나 CPU 몫을 정하여 다른 컨테이너의 자원을 과도하게 점유하지 않도록 한다. 핵심은 **얼마나 많은 자원을 사용할 수 있는가**의 제어이다.

㉡ namespace: 프로세스 ID, 마운트 목록, 네트워크 등 시스템 자원에 대해 프로세스 집합마다 분리된 관점을 제공한다. 따라서 컨테이너 안의 프로세스는 자신에게 속한 프로세스 목록이나 네트워크 환경 등을 독립된 것처럼 사용한다. 핵심은 **어떤 자원이 보이고 접근 가능한가**의 격리이며, CPU나 메모리 사용량 제한은 cgroup의 역할과 구별된다.

dmesg는 커널의 메시지 버퍼를 표시하는 명령으로, 부팅·장치 관련 메시지 등을 확인하는 데 사용한다. 실행 환경의 격리를 구현하는 namespace를 대신하는 기능이 아니다.

pacct는 프로세스 실행 및 자원 사용에 관한 계정 기록을 저장하는 파일이다. 사용 내역을 남기는 기록과, 프로세스 집합의 자원 사용을 실제로 제한하는 cgroup은 다르다.

wtmp는 로그인·로그아웃 등의 이력을 저장하는 파일이다. 사용자 접속 이력을 기록할 뿐 컨테이너의 자원 제어나 실행 환경 격리를 담당하지 않는다.

따라서 ㉠에는 cgroup, ㉡에는 namespace가 들어가며 ①의 조합과 일치한다.

NoteBase

문 21. 레지스트리와 관련된 내용으로 가장 적절하지 않은 것은?

① 레지스트리는 윈도우 운영체제의 하위 레벨 시스템 설정을 저장하는 데이터베이스로 다섯 가지의 루트키가 존재한다.

② 서브키 중 SAM은 윈도우 OS에서 사용자의 암호를 LM 또는 NTLM 해시 형식으로 저장하는 곳이다.

③ 루트키 중 HKLM키에 포함된 데이터는 시스템의 사용자 활동이나 사용자 계정에 대한 수정 여부를 확인할 수 있다.

④ 사고 대응자가 시스템에 연결된 USB를 발견하려면 System 레지스트리 하이브를 이용해야 한다.

정답 3번

간단한 해설

③은 사용자별 정보를 HKLM의 대표 기능으로 설명했다. HKLM은 **컴퓨터 전체의 공통 설정**을, HKCU와 HKU는 **사용자별 설정과 활동 흔적**을 확인하는 데 쓰인다.

출제 포인트

레지스트리의 루트키와 하이브를 구분하고 조사하려는 정보가 어디에 저장되는지 판단하는 문제이다.

핵심 개념

레지스트리는 윈도우의 시스템·프로그램·사용자 설정을 계층적으로 저장하는 데이터베이스이다. 루트키는 최상위 분류이고 하이브는 관련 키와 값을 묶어 파일로 저장하는 단위이다.
HKLM은 컴퓨터 전체에 적용되는 설정을 담는다. HKCU는 현재 로그인한 사용자의 설정을, HKU는 현재 로드된 사용자 프로필을 담는다. SAM 하이브는 로컬 계정 정보를, SYSTEM 하이브는 시스템 구성과 장치 정보를 담는다.

NoteBase

선지별 해설

① O: 레지스트리는 윈도우 설정을 저장하는 데이터베이스이다. 일반적으로 레지스트리 편집기에 표시되는 다섯 루트키는 HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG이다.

② O: SAM은 로컬 사용자 계정과 암호 해시를 저장한다. 선지의 'NTLM 해시'는 보통 NT 해시를 가리키는 표현이며 암호 원문을 저장한다는 뜻이 아니다. LM 해시의 저장 여부는 윈도우 버전과 보안 정책에 따라 달라진다.

③ X: 'HKLM키에 포함된 데이터'를 사용자별 활동·설정 변경을 조사하는 대표 정보로 설명한 부분이 부적절하다. HKLM은 시스템 전체의 공통 설정을 담고 사용자별 설정과 활동 흔적은 HKCU 또는 HKU의 해당 사용자 프로필에서 조사하는 것으로 고친다. 다만 계정 자체의 정보는 HKLM 아래의 SAM에도 있으므로 HKLM에 사용자 관련 정보가 전혀 없다는 뜻은 아니다.

④ O: SYSTEM 하이브에는 USB 장치의 연결 흔적이 남는다. 대표적으로 HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR에서 USB 저장장치 정보를 확인한다. 이 기록은 과거 연결 이력도 포함하므로 현재 연결 중인 장치만을 뜻하지는 않는다.

오답 포인트

③의 '사용자 활동이나 사용자 계정'이라는 표현에 끌려 HKLM을 사용자별 프로필 저장소로 판단하기 쉽다. 시스템 공통 설정, 사용자별 활동 흔적, 계정 자체 정보를 구분해야 한다.

다시 나오면 이렇게 판단

조사 대상을 먼저 구분한다. 시스템 공통 설정은 HKLM, 사용자별 설정·활동은 HKCU/HKU, 로컬 계정과 암호 해시는 SAM, USB 장치 연결 흔적은 SYSTEM에서 찾는다.

암기 포인트

HKLM은 컴퓨터 공통, HKCU/HKU는 사용자별, SAM은 계정·암호 해시, SYSTEM은 장치 정보이다.

NoteBase

문 22. 침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상사설망(VPN) 등 서로 다른 보안제품에서 발생하는 보안이벤트 정보를 한 곳으로 모으는 역할을 수행하는 보안관제시스템으로 가장 적절한 것은?

① ESM

② NMS

③ TMS

④ UTM

정답 1번

간단한 해설

ESM은 **서로 다른 보안제품의 이벤트·로그를 통합 수집하고 관리**하는 체계이다. 방화벽·IDS·VPN의 정보를 한곳에 모아 관제한다는 발문의 기능에 해당한다.

개념 구분

① ESM(Enterprise Security Management)은 서로 다른 보안 장비와 시스템의 이벤트·로그를 한곳에 수집하여 통합적으로 감시·관리하는 체계이다. 방화벽의 차단 기록, IDS의 탐지 경보, VPN의 접속 기록 등을 함께 확인하고 상관관계를 분석할 수 있다. 발문의 **이기종 보안제품에서 발생한 이벤트를 한곳으로 모은다**는 기능이 ESM의 대표적인 설명이므로 ①에 해당한다.

② NMS(Network Management System)는 라우터·스위치 등 네트워크 장비의 상태, 장애, 성능, 구성 등을 관리하는 시스템이다. 주된 관리 대상은 네트워크의 정상 동작과 운용 상태이므로, 여러 보안제품의 보안 이벤트를 통합하는 ESM과 초점이 다르다.

③ TMS(Threat Management System)는 네트워크 트래픽과 위협 정보를 분석하여 공격 징후를 탐지하고 대응하는 위협 관리 체계이다. 실제 제품에서는 로그 통합이나 장비 관리 기능이 ESM과 겹칠 수 있지만, 이 문제는 위협 분석 전반보다 '서로 다른 보안제품의 이벤트를 한곳에 수집'하는 통합보안관리의 대표 기능을 직접 묻고 있다.

④ UTM(Unified Threat Management)은 방화벽, 침입방지, 악성코드 차단, VPN 등 여러 보안 기능을 하나의 장비나 통합 플랫폼에서 제공하는 방식이다. 여러 보안 기능 자체를 한데 제공하는 UTM과, 서로 다른 보안제품이 만들어 낸 이벤트를 모아 관리하는 ESM을 구분해야 한다.

NoteBase

문 23. 호스트가 네트워크를 통해서 다른 장비로 데이터를 전송할 때 프로토콜 정보와 함께 데이터가 캡슐화(Encapsulation)된다고 정의한다. 다음 OSI 참조모델 전송층부터 물리층 사이의 각 계층에서 캡슐화되는 순서로 가장 적절한 것은?

① BIT → FRAME → PACKET → SEGMENT

② PACKET → FRAME → BIT → SEGMENT

③ SEGMENT → PACKET → BIT → FRAME

④ SEGMENT → PACKET → FRAME → BIT

정답 4번

간단한 해설

상위 계층의 데이터 단위를 하위 계층의 데이터 부분에 담고 필요한 제어 정보를 덧붙이는 흐름이다.

올바른 순서

SEGMENT → PACKET → FRAME → BIT

1. 전송층의 세그먼트(SEGMENT): 응용 계층에서 받은 데이터에 전송 계층의 제어 정보를 붙인다. 이 문제는 전송 계층의 데이터 단위를 **세그먼트**로 표현하며, 대표적으로 TCP가 이 명칭을 사용한다.

2. 네트워크층의 패킷(PACKET): 전송 계층의 데이터 단위를 데이터 부분에 담고, 목적지까지 전달하는 데 필요한 네트워크 계층 정보를 붙인다. 이 단계의 단위를 **패킷**이라고 한다.

3. 데이터링크층의 프레임(FRAME): 패킷에 해당 링크에서 전달하는 데 필요한 헤더와 트레일러 등의 제어 정보를 붙여 **프레임**을 만든다. 따라서 프레임은 패킷 다음이며 비트 전이다.

4. 물리층의 비트(BIT): 프레임을 이루는 비트들을 전기·광·무선 신호 등 물리 매체에 적합한 형태로 전송한다. 물리층에서 새로운 패킷을 만드는 것이 아니라 **비트열을 신호로 전달**하는 단계이다.

NoteBase

문 24. IP 패킷 필드의 내용으로 가장 적절하지 않은 것은?

① HL : 이 필드 값에 4를 곱한 값이 실제 헤더의 바이트 길이이다.

② Flag(DF) : DF 값이 1이면 단편화되지 않았음을 의미한다.

③ Flag(MF) : MF 값이 0이면 마지막 단편이거나 유일한 단편임을 의미한다.

④ Protocol : IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 정의하며 ICMP, IGMP, TCP, UDP, SIP가 있다.

정답 4번

간단한 해설

IPv4의 Protocol 필드는 IP 데이터 부분을 처리할 프로토콜을 식별한다. SIP는 TCP나 UDP 등을 이용하는 **응용계층 프로토콜**이므로 이 필드에서 직접 지정하는 대상이 아니다.

선지별 해설

① O. IPv4의 헤더 길이 필드인 HL 또는 IHL은 길이를 **32비트, 즉 4바이트 단위**로 나타낸다. 따라서 실제 헤더 길이는 4 × IHL바이트이다. 옵션이 없는 기본 헤더는 IHL 값이 5이므로 4 × 5 = 20바이트이다.

② O. DF가 1이면 해당 데이터그램의 **단편화를 금지**하므로, 규칙에 맞는 전달 과정에서 이를 쪼개지 않는다. 단편화 없이는 다음 네트워크로 보낼 수 없다면 그대로 단편화하는 대신 폐기한다. 원문의 '단편화되지 않았음'은 이 작동 맥락에서 이해해야 하며, DF를 과거 단편화 여부만 기록하는 상태 비트로 보아서는 안 된다. DF가 0이어도 크기가 작으면 단편화되지 않을 수 있다.

③ O. MF가 0이면 뒤에 더 이어지는 단편이 없다는 뜻이다. 따라서 **마지막 단편이거나 단편화되지 않은 데이터그램**일 수 있다. 단편화되지 않은 경우에는 단편 오프셋도 0이고, 실제로 나뉜 데이터그램의 마지막 단편은 오프셋이 0보다 크므로 두 필드를 함께 보면 구별할 수 있다.

④ X. IPv4의 Protocol 필드는 **IP 데이터 부분에 직접 실린 프로토콜**을 식별한다. ICMP는 1, IGMP는 2, TCP는 6, UDP는 17이라는 프로토콜 번호로 구별한다. 반면 SIP는 통신 세션의 생성·변경·종료를 제어하는 응용계층 프로토콜이며 TCP나 UDP 등의 전송 서비스를 이용한다. SIP 메시지를 UDP로 보냈다면 IP의 Protocol 값은 SIP가 아니라 UDP를 가리킨다.

따라서 SIP를 IP의 Protocol 필드가 직접 식별하는 프로토콜에 포함한 ④가 가장 적절하지 않다.

NoteBase

문 25. 다음 버퍼오버플로우(Buffer Oveflow) 공격의 대응책 중 하나인 안전한 코딩 기법들에서 사용을 자제해야 하는 함수는 모두 몇 개인가?

가. strcpy() 나. gets()
다. vsnprintf() 라. scanf()
마. fgets() 바. strcat()

① 3개
② 4개
③ 5개
④ 6개

정답 2번

간단한 해설

strcpy(), gets(), strcat()는 대상 버퍼의 크기에 맞추어 처리 길이를 자동 제한하지 않는다. scanf()도 **문자열 입력 폭을 제한하지 않으면** 버퍼를 넘길 수 있으므로 사용 자제 대상이며, 길이 인자를 받는 함수도 **실제 버퍼 크기를 정확히 지정**해야 한다.

NoteBase

보기별 해설

버퍼 오버플로우를 막으려면 기록할 데이터와 문자열 끝의 널 문자까지 들어갈 공간이 있는지 확인해야 한다. 이 문제는 길이 제한 없이 사용하기 쉬운 함수와, 크기 인자를 통해 처리 범위를 제한할 수 있는 함수를 구별한다.

가. strcpy() — 사용 자제 대상: 원본 문자열을 끝의 널 문자까지 목적지에 복사하지만 목적지 버퍼의 용량을 인자로 받지 않는다. 원본이 더 길면 경계를 넘어 쓸 수 있으므로, 복사 전에 필요한 공간을 검증하거나 용량을 지정할 수 있는 적절한 대안을 사용해야 한다.

나. gets() — 사용 자제 대상: 입력을 읽을 때 대상 버퍼의 크기를 전달할 방법이 없어 입력 길이를 안전하게 제한할 수 없다. **긴 입력 자체가 버퍼 초과로 이어질 수 있는** 함수이므로 사용하지 않고, 크기를 지정하는 fgets() 등으로 대체한다.

다. vsnprintf() — 크기 제한 가능: 가변인자 목록을 받아 형식에 맞춘 문자열을 만들되, 전달한 크기 안에 결과를 기록한다. 크기가 양수이면 널 문자 공간도 포함하여 제한하므로 무제한 문자열 출력보다 안전하게 사용할 수 있다. 다만 **실제 용량보다 큰 크기를 전달하면 안 되며**, 반환값으로 오류와 출력 잘림 여부를 확인해야 한다.

라. scanf() — 사용 자제 대상: '%s' 등으로 문자열을 받을 때 필드 폭을 지정하지 않으면 입력 길이가 버퍼 용량을 초과할 수 있다. 목적지 용량을 자동으로 알아내는 함수가 아니므로, 문자열 입력은 fgets() 등으로 제한한 뒤 해석하거나 널 문자 공간을 남긴 적절한 필드 폭을 지정해야 한다. 모든 scanf() 호출이 반드시 오버플로우를 일으킨다는 뜻은 아니다.

마. fgets() — 크기 제한 가능: 지정한 크기보다 한 글자 적은 수까지 입력을 저장하고, 성공적으로 읽은 문자열 끝에 널 문자를 붙인다. 실제 버퍼 용량을 정확히 지정하면 읽는 길이를 제한할 수 있다. 반환값과 줄바꿈 포함 여부를 확인하여 오류나 한 줄이 다 읽히지 않은 경우도 처리해야 한다.

바. strcat() — 사용 자제 대상: 목적지 문자열의 끝에 원본 문자열을 이어 붙이지만 목적지 전체 용량을 인자로 받지 않는다. **기존 문자열과 추가 문자열 및 널 문자의 공간**을 모두 확보해야 하며, 이를 검사하지 않으면 버퍼 경계를 넘는다.

사용을 자제할 함수는 가·나·라·바의 4개이므로 ②와 일치한다.

NoteBase

문 26. OSI 7계층 중 데이터의 압축과 암호화 기능을 수행하는 계층으로 가장 적절한 것은?

① 3계층(Network Layer)

② 4계층(Transport Layer)

③ 5계층(Session Layer)

④ 6계층(Presentation Layer)

정답 4번

간단한 해설

OSI 참조모형에서 데이터의 압축·암호화와 표현 형식 변환은 **6계층인 표현 계층**의 대표 기능이다.

개념 구분

④ 6계층인 표현 계층(Presentation Layer)은 서로 다른 시스템이 교환하는 데이터의 표현 형식을 맞추는 역할을 한다. 문자 코드나 자료 형식의 변환, 압축·압축 해제, 암호화·복호화 등이 대표 기능이다. 따라서 '데이터의 압축과 암호화'라는 발문의 단서는 **표현 계층**과 연결된다.

① 3계층인 네트워크 계층(Network Layer)은 논리적 주소와 경로 선택을 바탕으로 패킷을 목적지 네트워크까지 전달하는 역할을 한다. 데이터의 표현 형식을 변환하는 일보다 어느 경로로 전달할지를 다룬다.

② 4계층인 전송 계층(Transport Layer)은 송신 측과 수신 측 사이의 종단 간 데이터 전달을 담당한다. 전송 단위의 분할·재조립, 흐름 제어, 오류 복구 등의 기능을 제공할 수 있으며 구체적인 보장 수준은 프로토콜에 따라 다르다. 발문이 묻는 압축·암호화의 대표 분류와는 구별된다.

③ 5계층인 세션 계층(Session Layer)은 응용 간 대화 연결의 설정·관리·종료와 대화 제어·동기화를 담당한다. 연결된 대화를 어떻게 진행하고 관리할지가 중심이며, 데이터의 표현 형식 자체를 바꾸는 계층은 6계층이다.

이 구분은 OSI 참조모형에서 기능을 분류한 것이다. 실제 시스템에서는 암호화가 여러 계층의 프로토콜에 구현될 수 있으므로, 모든 암호화가 반드시 6계층에서만 수행된다는 뜻은 아니다.

NoteBase

문 27. 침입탐지시스템(IDS) 중 NIDS의 내용으로 가장 적절하지 않은 것은?

① 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고, 어떤 작업을 했는지에 대한 기록을 남기고 추적한다.

② 감사와 로깅을 할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않는다.

③ IP 주소를 소유하지 않기 때문에 해커의 직접적인 공격은 거의 완벽하게 방어할 수 있고 존재 사실도 숨길 수 있다.

④ 네트워크에서 하나의 독립된 시스템으로 운영되며, 스위칭 환경에서 NIDS를 설치하려면 다른 부가 장비가 필요하다.

정답 1번

간단한 해설

사용자 계정별 접근과 작업 이력을 운영체제의 감사 기록 등을 통해 추적하는 설명은 호스트 기반 IDS인 **HIDS**에 해당한다. NIDS는 네트워크 구간의 트래픽을 관찰·분석하여 침입 징후를 탐지하는 방식이다.

선지별 해설

① (X) 호스트의 운영체제에 설정된 사용자 계정과 감사 로그를 바탕으로 접근·작업 이력을 분석하는 것은 **HIDS**의 특징이다. NIDS의 기본 분석 대상은 네트워크 패킷과 통신 흐름이므로, 이 설명의 대상은 NIDS가 아니라 HIDS로 고쳐야 한다.

② (O) 수동 감시형 NIDS는 정상 트래픽의 사본을 받아 분석하므로, 감사와 기록을 위해 원래의 통신 데이터를 변경하거나 통신 경로를 직접 차단하지 않는다는 장점이 있다. 다만 이는 **수동적 관찰**의 특성을 말하며, 센서의 처리·저장 자원이나 미러링에 필요한 스위치 자원이 전혀 소모되지 않는다는 뜻은 아니다.

③ (O) 감시용 인터페이스에 IP 주소를 부여하지 않는 **스텔스 구성**에서는 다른 호스트가 그 인터페이스로 직접 연결하기 어려워 센서 노출과 직접 공격의 위험이 줄어든다. 선지는 이 구성의 장점을 설명한다. 다만 관리용 인터페이스에는 IP 주소가 있을 수 있고, 분석 소프트웨어의 취약점도 존재할 수 있으므로 모든 공격을 완벽히 막는다는 보장으로 해석해서는 안 된다.

④ (O) NIDS 센서는 감시 대상 호스트와 별개로 네트워크 트래픽을 수집한다. 스위칭 환경에서는 일반 포트만 연결해 다른 포트의 통신을 모두 볼 수 없으므로 **포트 미러링이나 네트워크 TAP**처럼 트래픽 사본을 센서에 전달하는 구성이 필요하다. 스위치가 미러링을 지원하면 그 기능을 사용할 수 있어 반드시 별도의 장비를 추가 구매해야 한다는 의미는 아니다.

NoteBase

문 28. 네트워크 기반 공격 중 BONK 공격에 대한 내용으로 가장 적절한 것은?

① ICMP 패킷을 일반 패킷보다 훨씬 큰 크기로 보내어 네트워크를 통해 공격 대상에 전달되는 동안 패킷 하나가 ICMP 패킷 여러 개로 분할되게 하여 공격 대상 시스템에 과부하를 일으키는 공격이다.

② TCP의 구조적인 문제를 이용하는 공격으로, SYN 패킷만을 보내어 각 서버의 동시 가용 사용자 수를 점유하여 다른 사용자가 서버를 사용할 수 없게 만드는 공격이다.

③ 패킷을 프래그먼트하여 전송할 때 패킷을 조작하여 결과적으로 공격 대상 시스템의 부하를 증가시키는 공격이다.

④ 출발지 주소와 도착지 주소가 같은 TCP 패킷을 공격 대상 시스템에 보내 가용 사용자 수를 점유하여 시스템 부하를 증가시키는 공격이다.

정답 3번

간단한 해설

BONK는 **IP 단편의 오프셋 등 재조립 정보를 비정상적으로 조작**하여 수신 시스템의 처리 결함을 이용하는 공격이다. 단순한 대량 연결 요청보다 패킷 단편을 조작한다는 점이 판단 기준이다.

개념 구분

BONK: **IP 단편의 위치 정보를 비정상적으로 조작**하여 수신 측의 재조립 처리 결함을 이용하는 서비스 거부 공격이다. 단편의 위치를 나타내는 오프셋 등이 정상적으로 맞지 않으면, 이를 제대로 검사하지 못하는 취약한 시스템에서 처리 오류나 부하가 발생할 수 있다. 정상적인 패킷 단편화 자체가 공격인 것은 아니다.

Ping of Death: ①이 설명하려는 공격이다. 비정상적으로 큰 ICMP 패킷을 IP 단편으로 나누어 전달하고 재조립 과정의 취약점을 이용한다. 대표적으로 재조립한 IP 패킷 크기가 허용 한도를 넘도록 만드는 방식이다. 단순히 정상 패킷이 여러 조각으로 나뉘었다는 사실만으로 성립하지 않는다.

SYN Flooding: ②에 해당한다. TCP 연결 설정을 시작하는 SYN 요청을 대량으로 보내고 연결을 완료하지 않아, 서버에 **반개방 연결 상태가 누적**되도록 한다. 연결 대기 자원이 소진되면 정상 이용자의 연결 요청을 처리하기 어려워진다.

LAND: ④에 해당한다. 출발지와 목적지 IP 주소를 모두 공격 대상의 주소로 위조한 TCP 패킷을 보내, 취약한 시스템이 자기 자신을 상대하는 비정상적인 연결을 처리하게 만드는 공격이다.

따라서 단편화된 패킷을 조작하여 재조립 과정에 문제를 일으키는 BONK의 특징에 부합하는 것은 ③이다.

NoteBase

문 29. Google Dork에 대한 설명으로 가장 적절하지 않은 것은?

① Google Dork은 구글을 이용한 해킹을 말한다.

② 구글검색엔진에서 “cache: police.ac.kr”로 검색할 경우, 해당 도메인의 캐시된 정보를 보여준다.

③ 구글검색엔진에서 “inurl: admin”로 검색할 경우, URL에 admin 단어가 들어가 있는 웹페이지를 보여준다.

④ 구글검색엔진에서 “site: police.ac.kr”로 검색할 경우, 서브도메인을 제외한 모든 도메인 리스트를 보여준다.

정답 4번

간단한 해설

site:은 검색 결과를 지정한 도메인 범위로 제한하며 **하위 도메인도 포함할 수 있다**. 서브도메인을 제외한 전체 도메인 목록을 보여주는 연산자는 아니다.

NoteBase

선지별 해설

이 문항은 2022년 당시 검색 연산자의 기능을 기준으로 판단한다. 원문의 검색식에는 콜론 뒤 공백이 보이지만, 실제 연산자 구문은 site:police.ac.kr처럼 **콜론과 검색값을 붙여 쓰는** 형식이다.

① O. Google Dork은 구글의 검색 연산자와 조건을 활용해 웹에 노출된 정보나 취약점의 단서를 찾는 기법을 뜻하며, 구글 해킹이라고도 부른다. 핵심은 **검색엔진에 수집된 정보를 정교하게 조회**하는 것이다. 검색만으로 인증을 우회하거나 시스템에 침입하는 기능이 생기는 것은 아니며, 정보 노출 점검에도 활용될 수 있다.

② O. 당시 cache: 연산자는 지정한 웹페이지에 대해 구글이 보관한 **캐시 사본**을 확인하는 기능이었다. 따라서 제시된 주소의 저장된 사본이 있다면 이를 볼 수 있었으며, 해당 도메인의 모든 페이지나 실시간 정보를 빠짐없이 보여주는 기능은 아니었다. 현재는 이 연산자가 폐지되었고, 구글은 2024년 9월 공식 변경기록에서 더 이상 동작하지 않는다고 밝혔다.

③ O. inurl:은 검색어의 위치를 **웹페이지의 URL**로 제한하는 연산자이다. inurl:admin은 URL에 admin이라는 단어가 포함된 검색 결과를 찾는 기능을 뜻한다. 본문이나 제목에만 그 단어가 있다는 조건과는 다르며, 검색 결과로 나타난다는 사실이 관리자 접근 권한을 제공하지는 않는다.

④ X. site:은 검색 결과를 **지정한 사이트·도메인 범위로 제한**한다. police.ac.kr처럼 도메인을 지정하면 그 도메인의 페이지뿐 아니라 하위 도메인의 페이지도 검색 대상에 포함될 수 있다. 따라서 서브도메인을 제외하거나 모든 도메인의 목록을 나열한다는 설명은 기능과 다르다. 또한 검색 결과는 색인과 검색 제공 범위의 영향을 받으므로 해당 사이트의 모든 URL을 빠짐없이 나열한다고 보장하지 않는다.

따라서 site: 연산자의 검색 범위와 결과를 잘못 설명한 ④가 가장 적절하지 않다.

NoteBase

문 30. 다음은 디지털 포렌식에 있어서 전자적 증거의 분석 기술에 대한 설명이다. 아래의 설명으로 가장 적절한 것은?

저장매체 또는 하드디스크 이미지의 내부구조와 파일시스템을 확인하고 파일시스템 내부에 존재하는 파일에 대응되는 응용 프로그램 구동 없이 쉽고 빠르게 분석할 수 있는 기법이다. 복제한 이미지를 사용자가 수동으로 마운팅하여 열람할 필요가 없어 분석 시간을 줄일 수 있다. 대표적인 도구로는 EnCase, FTK, FinalForensic 등이 있다.

① 디스크 브라우징(Disk Browsing) 기술

② 데이터 뷰잉(Data Viewing) 기술

③ 검색 기술

④ Time Line 분석

정답 1번

간단한 해설

핵심 단서는 개별 문서의 내용이 아니라 **디스크 이미지의 내부 구조와 파일시스템을 직접 탐색**한다는 점이다. 이미지를 운영체제에 수동으로 마운트하지 않고 파일·디렉터리 구조를 확인하는 기능은 디스크 브라우징에 해당한다.

NoteBase

대응 관계 해설

디지털 포렌식에서 디스크 이미지는 저장매체의 내용을 분석용으로 복제한 자료이다. 분석 기법은 이 이미지의 구조를 탐색하는지, 개별 파일 내용을 표시하는지, 조건에 맞는 자료를 찾는지, 시간 관계를 재구성하는지에 따라 구별할 수 있다.

지문과 디스크 브라우징의 대응: 디스크 브라우징은 도구가 지원하는 디스크·파티션·파일시스템 구조를 해석하여 파일과 디렉터리를 탐색하게 하는 기능이다. 도구가 이미지 내부를 직접 읽으므로 사용자가 이미지를 별도 드라이브로 수동 마운트하지 않아도 구조와 파일 목록 등을 확인할 수 있다. 지문의 **'내부구조와 파일시스템을 확인'**한다는 설명이 결정적인 단서이다. 내장 보기 기능을 함께 제공하면 각 파일의 원래 응용 프로그램을 실행하지 않고 내용도 확인할 수 있다.

데이터 뷰잉과의 구별: 데이터 뷰잉은 선택한 파일이나 데이터를 문자, 16진수, 그림 등의 형태로 표시하여 그 내용을 읽고 해석하는 데 중점을 둔다. 원래 응용 프로그램 없이 내용을 볼 수 있다는 점은 겹치지만, 지문 전체는 개별 파일의 표시보다 **이미지의 파일시스템을 탐색하는 기능**을 설명한다.

검색 기술과의 구별: 검색은 키워드·파일명·특정 패턴 등 조건에 맞는 자료를 찾아 분석 대상을 좁히는 방법이다. 이미지 구조를 전체적으로 열람하는 기능과 달리, 찾으려는 조건과 일치하는 자료를 추출하는 것이 중심이다.

Time Line 분석과의 구별: 파일의 생성·수정·접근 시각이나 각종 로그의 시간을 모아 사건의 발생 순서와 활동의 연관성을 재구성한다. 파일시스템을 볼 수 있는가보다 **언제 어떤 활동이 일어났는가**를 분석하는 데 초점이 있다.

EnCase, FTK, FinalForensic은 지문에 제시된 분석 도구의 예이다. 통합 도구에는 여러 분석 기능이 함께 포함될 수 있으므로 도구 이름만이 아니라 설명된 기능을 기준으로 대응시키며, 이 지문은 ① 디스크 브라우징 기술에 해당한다.

NoteBase

문 31. 다음 지문에서 ㉠에 들어갈 내용으로 가장 적절한 것은?

스위치는 하나의 포트에서 여러 MAC 주소를 학습할 수 있도록 구현되어 있다. MAC 주소 테이블이 가득 차서 더 이상 MAC 주소를 학습할 수 없을 때, 그 뒤에 들어오는 모든 Frame들은 Flooding되면서 마치 허브처럼 동작 될 수 있다. 위와 같은 공격기법을 MAC Flooding 공격이라고 한다. 이때 (㉠)를 설정하면 하나의 포트에 학습할 MAC 주소를 제한할 수 있어, 이런 공격을 방어할 수 있다. MIMT(중간자공격)에 있어서도 이 기능을 사용하면, MAC 주소를 변형하여 다른 디바이스 통신 사이에 끼어드는 ARP Spoofing도 허가된 MAC 주소로만 접속하게 제한할 수 있다.

① 포트시큐리티

② 포트포워딩

③ 포트필터링

④ 포트미러링

정답 1번

간단한 해설

포트시큐리티는 스위치 포트에서 **허용할 MAC 주소와 학습 가능한 주소 수를 제한**하여 MAC 플러딩 공격을 방어한다. 허용 MAC 제한만으로 모든 ARP 스푸핑까지 완전히 막는 것은 아니다.

NoteBase

빈칸별 해설

㉠에는 '포트시큐리티'가 들어간다. 스위치는 프레임의 출발지 MAC 주소와 들어온 포트를 연결해 학습한다. 공격자가 하나의 포트에서 다수의 허위 출발지 MAC 주소를 보내면 주소 테이블을 소진시킬 수 있다. 포트시큐리티는 **포트에서 허용할 MAC 주소와 학습 가능한 주소 수**를 제한하여 이러한 주소 테이블 오염·소진을 완화한다. 제한 위반 시 프레임을 버리거나 포트를 차단하는 등 설정에 따른 조치를 취한다.

지문의 '허브처럼 동작'한다는 표현은 목적지 MAC 주소를 학습하지 못한 프레임이 여러 포트로 전달되어 도청 위험이 커질 수 있다는 뜻이다. 실제 플러딩 여부와 범위는 스위치의 구현·설정과 목적지 주소의 학습 상태에 따라 달라지므로, 테이블이 찼다는 이유만으로 모든 프레임이 언제나 모든 포트에 전송된다고 단정할 수는 없다.

지문의 ARP 스푸핑 관련 설명은 허용하지 않은 MAC 주소를 사용하는 장치의 접속을 제한한다는 범위에서 이해한다. 포트시큐리티만으로 ARP 메시지 속 IP–MAC 대응 관계가 모두 검증되는 것은 아니다. 허용된 MAC 주소를 악용한 위조까지 막으려면 동적 ARP 검사(DAI)처럼 ARP 대응 관계를 확인하는 별도 대책이 필요할 수 있다.

② 포트포워딩은 특정 주소·포트로 들어온 통신을 다른 목적지 주소·포트로 전달하도록 연결하는 기능이다. 스위치 포트의 MAC 주소 학습 개수를 제한하는 기능과 다르다.

③ 포트필터링은 보통 TCP·UDP 포트 번호 등 정해진 기준에 따라 통신을 허용하거나 차단하는 기능이다. 빈칸이 요구하는 '한 스위치 포트에 허용되는 MAC 주소 수의 제한'과는 기준이 다르다.

④ 포트미러링은 관찰 대상 포트의 트래픽 복사본을 분석용 포트로 보내는 기능이다. 모니터링·분석을 위한 복사 기능이므로 MAC 주소 테이블 소진을 직접 방지하는 설정이 아니다.

따라서 ㉠의 기능에 대응하는 선택지는 ①이다.

NoteBase

문 32. SQL Injection 공격에 대한 설명으로 가장 적절하지 않은 것은?

① 공격자가 입력값을 조작하여 원하는 SQL 구문을 실행하는 기법이다.

② 잠재적인 SQL 구문의 구조를 확인한 후에 적절히 실행되는 문자들의 결합을 찾을 때까지 입력값을 조작하는 방법으로 공격이 수행된다.

③ 공격자가 SQL 기반 게시판 등에 게시글과 함께 공격코드를 삽입하여 공격코드를 실행하도록 한 후 클라이언트의 정보를 유출하는 공격기법도 있다.

④ 부적절한 입력값을 전달하여 에러를 발생시켜 SQL 구문을 확인하고 이에 대한 취약점을 공격하는 기법이다.

정답 3번

간단한 해설

게시글에 삽입한 스크립트를 다른 사용자의 **브라우저에서 실행**하여 정보를 유출하는 것은 저장형 **XSS**의 전형적인 방식이다. SQL Injection은 입력이 데이터베이스의 SQL 명령 구조를 바꾸어 서버 측 질의 실행에 영향을 주는 공격이라는 점에서 구별된다.

선지별 해설

① (O) SQL Injection은 외부 입력이 단순한 데이터로 처리되지 않고 **SQL 명령의 일부로 해석**되는 취약점을 이용한다. 그 결과 원래 의도한 조회 조건이나 명령의 의미가 달라져 권한 없는 조회·수정 등이 발생할 수 있다.

② (O) 공격자는 애플리케이션이 입력을 어떤 SQL 문맥에 결합하는지 추론하고 입력에 따른 반응을 비교하여 취약한 구조를 찾을 수 있다. 핵심은 입력이 쿼리의 **문법이나 실행 의미를 바꾸는지** 확인하는 것이다. 다만 모든 공격에서 전체 SQL 원문을 먼저 알아야 하는 것은 아니다.

③ (X) 게시판에 악성 스크립트를 저장한 뒤 게시글을 보는 사용자의 브라우저에서 실행되게 하여 정보를 유출하는 설명은 **저장형 XSS**에 해당한다. 게시판이 SQL 데이터베이스를 사용한다는 사실만으로 SQL Injection이 되는 것은 아니다. 구별 기준은 데이터베이스 질의를 변조하는지, 사용자 브라우저에서 스크립트를 실행시키는지이다.

④ (O) 부적절한 입력에 대해 자세한 오류 메시지가 노출되면 SQL 구문의 구조나 데이터베이스 관련 정보가 드러날 수 있다. 이를 단서로 취약점을 확인하는 것은 **오류 기반 SQL Injection**에서 활용되는 방식이다. 오류를 숨기는 것만으로 취약점이 없어지는 것은 아니며, 오류 메시지 없이 반응 차이를 이용하는 방식도 있다.

NoteBase

문 33. 재해복구 시스템 유형별 내용으로 가장 적절하지 않은 것은?

① 미러 사이트 : 주 센터와 동일한 수준의 정보기술 지원을 원격지에 구축하고, 실시간 동시 서비스를 제공

② 핫 사이트 : 중요성이 높은 정보기술 지원만 부분적으로 재해복구센터에 보유하고 서비스 제공 데이터는 동기적 또는 비동기적 방식의 실시간 미러링을 통하여 최신상태 유지

③ 웜 사이트 : 데이터를 주기적(수 시간~1일)으로 백업하고 구축 및 유지비용이 핫 사이트에 비해 저렴

④ 콜드 사이트 : 데이터만 원격지에 보관하고 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보

정답 2번

간단한 해설

핫 사이트는 신속한 업무 인계를 위해 필요한 정보자원을 갖추고 데이터를 최신 상태로 유지한다. **중요한 자원만 부분적으로 보유하는 것은 웜 사이트의 특징**이므로 ②의 앞부분이 부적절하다.

선지별 해설

① O: 미러 사이트는 주 센터와 같은 수준의 시스템을 원격지에 갖추고 데이터를 실시간으로 반영하며, 양쪽에서 서비스를 동시에 제공하는 방식이다. 주 센터에 장애가 생겨도 서비스를 이어갈 수 있도록 **이중화된 운영 환경**을 유지하므로 비용이 높다.

② X: **중요한 정보자원만 부분적으로 보유**한다는 부분은 웜 사이트의 특징이다. 핫 사이트는 주 센터의 업무를 신속히 인계할 수 있도록 필요한 정보자원을 갖추고 데이터를 최신 상태로 유지하는 방식이다. 실시간 미러링에 관한 뒷부분은 핫 사이트의 특징에 부합하지만, 부분적인 자원 보유라는 앞부분을 옳게 만들지는 않는다. 미러 사이트와 구분하는 이 문항의 분류에서는 평상시 대기하다가 재해 발생 시 서비스를 전환한다.

③ O: 웜 사이트는 필요한 정보자원의 일부를 미리 준비하고, 주기적으로 백업한 데이터를 이용하여 서비스를 복구한다. 문항의 수 시간~1일은 주기적 백업의 예이며 모든 환경에 고정된 필수 간격은 아니다. 자원을 상시 완비하고 데이터를 최신 상태로 유지하는 핫 사이트보다 비용이 낮지만, 부족한 자원 준비와 데이터 복원에 시간이 더 필요하다.

④ O: 콜드 사이트는 원격지에 백업 데이터를 보관하고 복구 장소 등 최소 기반만 준비하는 방식이다. 서비스에 필요한 장비·소프트웨어를 충분히 확보하지 않은 상태이므로 재해 후 이를 조달·설치하고 데이터를 복원해야 한다. 유지비는 낮지만 **서비스 재개까지 걸리는 시간이 길다**.

NoteBase

문 34. 소프트웨어 안전(safety)에 대한 내용으로 가장 적절하지 않은 것은?

① 기능 동작 오류, 데이터 처리 오류, 소스코드 오류에 대한 장애 관련 위험원을 식별해야 한다.

② 소프트웨어가 동작하는 시스템으로 인해 인명피해, 시스템, 재산 등에 손실을 줄 수 있는 소프트웨어 위험요소를 확인 및 관련하여 위험이 수용 가능한 수준 이하로 유지하는 것이 소프트웨어 안전 진단의 목표이다.

③ 국내 소프트웨어 안전의 법적 근거는 준비 중이며, 안전진단 범위는 항공기, 기차 및 원자력 시스템들이고, 향후 자율주행차, 드론 등이 포함된다.

④ 미국, 유럽은 항공우주, 국방, 철도, 원자력에 대한 소프트웨어 안전을 위한 규정이 존재한다.

정답 3번

①

기능 오동작·데이터 처리 오류·소스코드 결함은 안전기능을 무력화하거나 사고로 이어질 수 있으므로, **각 오류에서 발생할 수 있는 장애와 위험원을 식별**해야 한다.

②

인명·시스템·재산에 피해를 줄 위험요소를 찾아 평가하고, 필요한 안전기능과 통제수단으로 **위험을 수용 가능한 수준 이하로 유지**하는 것이 소프트웨어 안전 진단의 목표이다.

③

국내에는 과학기술정보통신부장관이 **소프트웨어안전 확보 지침을 정하여 고시하도록 하는 법적 근거가 이미 마련되어 있다**. 법적 근거가 준비 중이라는 부분이 틀리다.

소프트웨어 진흥법 제30조(소프트웨어안전 확보)
② 과학기술정보통신부장관은 다음 각 호의 사항을 포함하는 소프트웨어안전 확보를 위한 지침을 정하여 고시하여야 한다.
1. 소프트웨어안전 관련 위험 분석
2. 소프트웨어안전 확보를 위한 설계 및 구현 방법
3. 소프트웨어안전 검증 방법
4. 운영 단계의 소프트웨어안전 확보 방안
5. 그 밖에 소프트웨어안전 확보에 필요하다고 인정되는 사항

④

미국과 유럽은 **항공우주·국방·철도·원자력 등 안전이 중요한 분야에 소프트웨어 안전 기준을 운영**한다. 항공 소프트웨어의 DO-178C처럼 개발·검증·인증 과정에서 안전성을 확인하는 기준이 대표적이다.

NoteBase

문 35. 데이터베이스 암호화 방법의 내용으로 가장 적절하지 않은 것은?

① Hybrid 방식은 Plug-In 방식의 단점인 배치 업무의 성능 저하를 보완하기 위해 API 방식을 이용하는 구성이다.

② Plug-In 방식은 암·복호화 모듈을 DB 서버 내에 설치하고 이곳에서 암·복호화를 수행하는 구조이다.

③ API 방식은 암·복호화 모듈을 애플리케이션 서버 내에 설치하고 이곳에서 암·복호화를 수행하는 구조로 애플리케이션의 수정을 동반한다.

④ 파일 암호화 방식은 DBMS에 추가 기능으로 제공되는 암호화 기능을 이용하여 DB 내부에서 데이터 파일 저장 시 암호화한다.

정답 4번

간단한 해설

DBMS가 자체 기능으로 데이터 파일을 저장할 때 암호화하고 읽을 때 자동 복호화하는 방식은 **TDE**이다. 파일 암호화 방식은 이와 구별하여 **운영체제·파일시스템 계층에서 파일을 암호화**하는 방식이다.

NoteBase

선지별 해설

데이터베이스 암호화 방식은 암·복호화를 어느 계층에서 수행하는지에 따라 구별한다. 애플리케이션의 명시적 호출, DB 서버의 별도 모듈, DBMS의 자체 저장 기능, 운영체제의 파일 처리 계층은 서로 다른 적용 위치이다.

① O: Hybrid 방식은 API와 Plug-In 방식을 함께 사용한다. 많은 데이터를 일괄 처리하는 배치 업무에서 DB 서버의 암·복호화 부담이 커지면, 해당 처리에 API 방식을 적용하여 애플리케이션 측에서 암·복호화를 수행하게 할 수 있다. 이처럼 **업무 특성에 따라 두 방식의 처리 위치를 나누어** Plug-In의 성능 부담을 보완한다. 실제 성능 개선 정도는 업무량과 구현에 따라 달라진다.

② O: Plug-In 방식은 DB 서버에 암·복호화 모듈을 설치하여 DB 내부 처리 과정에서 이를 호출하는 구조이다. 암·복호화 작업이 DB 서버에서 수행되므로 데이터 처리와 연계하기 쉽지만 그만큼 DB 서버의 자원을 사용한다. 외부 모듈을 붙이는 방식이라는 점에서 DBMS가 자체적으로 제공하는 TDE 기능과 구별된다.

③ O: API 방식은 애플리케이션 서버의 암·복호화 라이브러리나 인터페이스를 호출하여 데이터를 처리한다. 애플리케이션이 저장 전 암호화와 조회 후 복호화 시점을 제어하므로, 해당 **암·복호화 호출을 넣는 프로그램 수정**이 필요하다. DB 서버에 집중될 암호 연산을 애플리케이션 측으로 옮길 수 있다.

④ X: 선지의 설명은 **DBMS 자체 암호화인 TDE**에 해당한다. TDE는 DBMS가 데이터 파일을 디스크에 쓸 때 암호화하고 메모리로 읽어 올 때 복호화하여 애플리케이션의 개별 암호화 호출 없이 저장 데이터를 보호한다. 이에 비해 이 문항에서 구분하는 파일 암호화 방식은 운영체제·파일시스템 계층에서 파일의 입출력을 암호화하며, DB 파일 외의 일반 문서·이미지 등에도 적용할 수 있다. 구별 기준은 파일이 암호화된다는 결과 자체가 아니라 **암호화를 수행하는 계층**이다.

NoteBase

문 36. 「개인정보 보호법」상 개인정보 유출 시 개인정보처리자가 정보주체에게 알려야 할 사항으로 다음 보기에 가장 적절한 것은?

제34조(개인정보 유출 통지 등)
① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.
1. 유출된 (㉠)
2. (㉡)과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

① ㉠ 개인정보의 위탁 현황 ㉡ 개인정보 보관 기간
② ㉠ 정보저장매체 ㉡ 개인정보의 위탁 현황
③ ㉠ 개인정보의 항목 ㉡ 유출된 시점
④ ㉠ 정보저장매체 ㉡ 개인정보 보관 기간

정답 3번

①
개인정보 유출 시 정보주체에게 알려야 할 사항에는 **유출된 개인정보의 항목**이 포함된다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
1. 유출등이 된 개인정보의 항목

②
개인정보처리자는 정보주체에게 **유출등이 된 시점과 그 경위**를 알려야 한다.

개인정보 보호법 제34조(개인정보 유출등의 통지 · 신고)
① 개인정보처리자는 개인정보가 유출등이 되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만, 정보주체의 연락처를 알 수 없는 경우 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다. <개정 2023.3.14, 2026.3.10>
2. 유출등이 된 시점과 그 경위

NoteBase

문 37. 정보보호 관리체계(ISMS)에서는 정보보호 정책과 목적에 부합하도록 위험분석을 통해 위험을 허용 가능한 수준으로 관리한다. 이때 위험처리 방식으로 가장 적절하지 않은 것은?

① 수용
② 삭제
③ 회피
④ 전가

정답 2번

간단한 해설

삭제는 데이터를 없애는 개별 조치일 수 있지만, ISMS의 **위험처리 전략 명칭에 해당하지 않는다**. 보호대책을 적용해 위험을 줄이는 전략은 위험감소라고 한다.

선지별 해설

① O. 위험수용은 위험을 평가한 뒤 조직의 수용 기준과 대응 비용 등을 고려하여 **그 위험과 예상 손실을 감수하기로 결정**하는 방식이다. 위험을 몰라서 방치하는 것과는 다르며, 수용의 근거와 승인 절차가 필요하다. 환경이 바뀌면 수용했던 위험도 다시 평가해야 한다.

② X. 삭제는 이 문항에서 구분하는 **위험처리 전략의 독립적인 명칭이 아니다**. 통상적인 분류에는 수용·감소·회피·전가가 있다. 접근통제나 보안 패치 등의 보호대책을 적용해 발생 가능성이나 피해 규모를 낮추는 것은 위험감소이다. 데이터 삭제 자체가 보호조치로 사용될 수는 있지만, 그것만으로 별도의 위험처리 유형인 '삭제'가 성립하는 것은 아니다.

③ O. 위험회피는 위험을 발생시키는 **활동·절차·사업을 수행하지 않거나 중단**하는 방식이다. 예를 들어 위험을 감수하기 어려운 부가 서비스를 아예 제공하지 않는 경우가 해당한다. 활동을 유지하면서 보안대책을 강화하는 위험감소와 구별된다.

④ O. 위험전가는 보험이나 계약 등을 통해 위험에서 생기는 **손실 부담을 제3자에게 이전하거나 배분**하는 방식이다. 예를 들어 보험으로 사고에 따른 일정한 경제적 손실을 보전받도록 하는 경우이다. 전가하더라도 사고 발생 가능성이나 조직이 부담하는 모든 책임이 저절로 없어지는 것은 아니다.

따라서 위험처리 방식의 명칭으로 가장 적절하지 않은 것은 ② 삭제이다.

NoteBase

문 38. 인터넷 뱅킹 시스템의 위험요소로 바르게 연결되지 않은 것은?

① 클라이언트 보안에서의 위협요소 - Virus, Trojan Horse

② 서버보안에서의 위협요소 - Unix/NT Security Holes, Improper Administration

③ 거래처리 보안에서의 위협요소 - Poor Programming, Weak Authentication

④ 내부적인 보안에서의 위협요소 - Virus & Trojan Horse, Unix/NT Security Holes, Improper Administration

정답 3번

간단한 해설

이 문제의 영역별 분류에서 부실한 프로그래밍과 취약한 인증은 **애플리케이션 보안**의 위험요소이다. 거래처리 보안의 대표 위험은 서버 위장과 취약한 암호화이므로 두 영역의 연결을 구분해야 한다.

선지별 해설

이 문제는 인터넷 뱅킹의 위험을 클라이언트·거래처리·서버·애플리케이션·내부 시스템이라는 영역별로 나눈 분류를 묻는다. 한 취약점이 다른 영역에도 피해를 줄 수 있다는 사실과, 이 분류에서 그 취약점을 어디에 배치하는지는 구별한다.

① O: 클라이언트는 이용자가 인터넷 뱅킹에 접속하는 단말 환경이다. 바이러스는 파일이나 프로그램을 감염시켜 정상 동작과 정보를 훼손할 수 있고, 트로이 목마는 정상 프로그램처럼 가장해 정보 탈취나 원격 조작 등의 악성 기능을 수행한다. 둘 다 이용자 단말의 보안을 위협하므로 연결이 맞다.

② O: 서버보안에서는 Unix·Windows NT 같은 운영체제의 보안 취약점과 부적절한 운영·관리가 위험요소가 된다. 예를 들어 취약점 패치 누락이나 과도한 권한 부여는 서버 침입과 정보 유출의 원인이 될 수 있다. 선지의 운영체제 이름은 분류에 사용된 예시이며 서버 위험이 이 두 운영체제에만 한정된다는 뜻은 아니다.

③ X: Poor Programming은 부실한 프로그램 구현, Weak Authentication은 취약한 인증을 뜻한다. 이 문제의 분류에서 둘은 **애플리케이션 보안**의 위험요소이다. 거래처리 보안에 대응하는 대표 위험은 서버 위장(Server spoof)과 취약한 암호화(Weak encryption)로, 거래 상대를 속이거나 거래 정보의 보호를 약화시키는 문제이다. 따라서 애플리케이션 보안의 위험요소를 거래처리 보안에 연결한 점이 틀리다. 부실한 구현이나 약한 인증이 실제 거래의 안전성과 무관하다는 의미는 아니다.

④ O: 내부 시스템에서도 바이러스·트로이 목마 감염, 운영체제 취약점, 부적절한 관리가 정보 유출이나 시스템 침해로 이어질 수 있다. 따라서 제시된 항목들은 내부적인 보안의 위험요소로 연결할 수 있다. 여기서 '내부적인 보안'은 내부자가 고의로 저지르는 행위만을 뜻하지 않고 조직 내부 환경의 보안도 포함한다.

NoteBase

문 39. 운영체제에서 보안에 불필요한 부분을 모두 제거하여 모듈에 따른 분석 및 테스트가 가능한 TCSEC의 단계별 보안수준으로 가장 적절한 것은?

① B1

② B2

③ B3

④ C1

정답 3번

간단한 해설

B3(보안 영역)은 보안정책 집행에 불필요한 코드를 신뢰 컴퓨팅 기반에서 제외하고 복잡성을 줄여, 분석과 시험이 가능하도록 구성하는 수준이다. 단순한 모듈화라는 단서보다 **보안 핵심의 최소화**에 초점을 맞추어 판단한다.

개념 구분

핵심 기준: **B3**에서는 신뢰 컴퓨팅 기반(TCB)이 모든 접근을 중재하고 변조로부터 보호되며, 충분히 작고 단순하여 분석과 시험을 받을 수 있어야 한다. 이를 위해 보안정책 집행에 필요하지 않은 코드를 TCB에서 제외하고 복잡성을 최소화한다.

발문의 의미: '보안에 불필요한 부분을 제거한다'는 것은 운영체제의 모든 일반 기능을 없앤다는 뜻이 아니라, **보안을 신뢰해야 하는 핵심 부분**에 불필요한 기능을 포함하지 않는다는 뜻이다. 잘 정의된 인터페이스를 가진 모듈로 구성하면 각 부분의 동작과 상호작용을 검토하기 쉬워진다.

인접 등급과의 구별: **B2**도 구조화와 모듈화를 요구하지만, 발문처럼 보안정책에 불필요한 코드를 배제하고 핵심의 복잡성을 최소화하여 분석·시험 가능성을 높이는 기준은 B3의 특징이다. B1은 보안표지와 강제적 접근통제, C1은 재량적 접근통제 중심의 보호 수준이므로 이 기준에 해당하지 않는다.

NoteBase

문 40. 다음 「정보통신기반 보호법」 제9조(취약점의 분석·평가)에서 ( ) 안에 들어갈 내용으로 가장 적절한 것은?

(㉠)은(는) 관계중앙행정기관의 장 및 (㉡)과(와) 협의하여 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.

① ㉠ 행정안전부장관 ㉡ 국가정보원장
② ㉠ 방송통신위원장 ㉡ 행정안전부장관
③ ㉠ 한국인터넷진흥원장 ㉡ 행정안전부장관
④ ㉠ 과학기술정보통신부장관 ㉡ 국가정보원장

정답 4번

공통 해설

취약점 분석·평가 기준은 **과학기술정보통신부장관이 관계중앙행정기관의 장 및 국가정보원장과 협의하여 정한다**. 정한 기준은 **관계중앙행정기관의 장에게 통보**해야 한다.

정보통신기반 보호법 제9조(취약점의 분석 · 평가)
⑤과학기술정보통신부장관은 관계중앙행정기관의 장 및 국가정보원장과 협의하여 제1항 및 제2항에 따른 취약점 분석 · 평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다. <개정 2008.2.29, 2013.3.23, 2017.7.26, 2019.12.10>

NoteBase