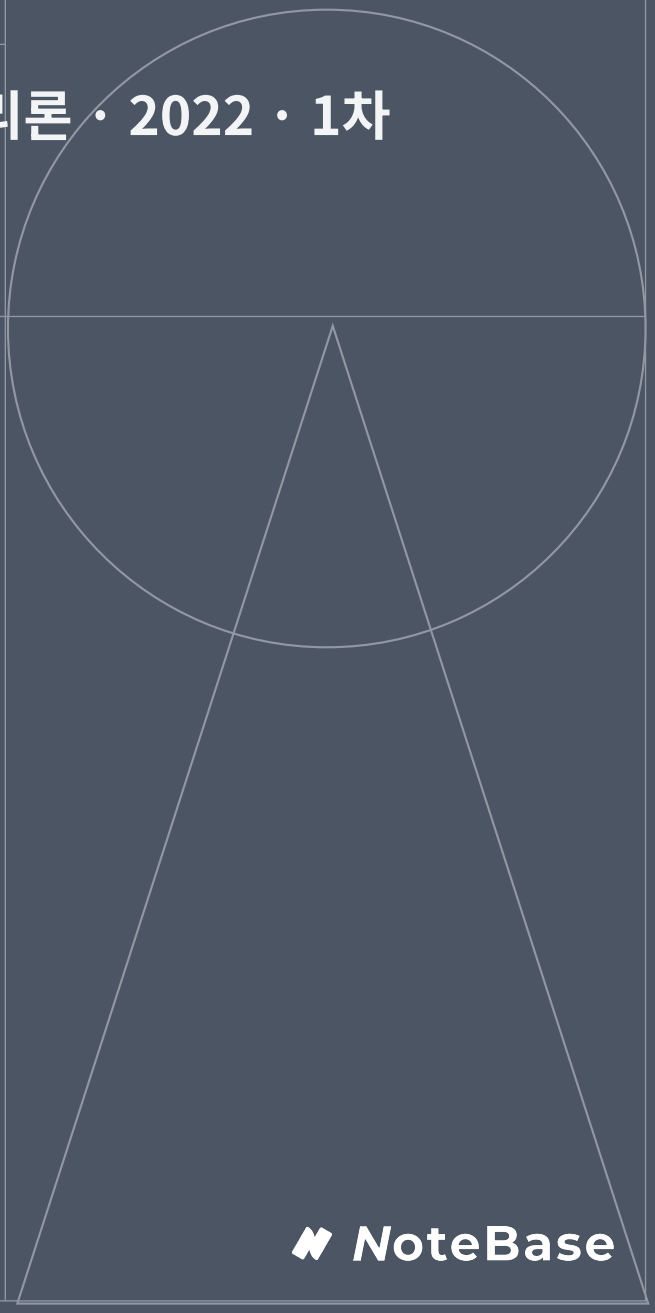
기출OX 해설집

공무원/해경/순경 · 정보관리론 · 2022 · 1차



NoteBase

기출OX 해설집

공무원/해경/순경 · 정보관리론 · 2022 · 1차

공무원/해경/순경 · 정보관리론 · 2022 · 1차

문 1. 보안 관리 대상에 대한 <보기>의 설명에서 ( )에 들어갈 용어로 다음 중 가장 옳은 것은?

<보기>
(㉠) : 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
(㉡) : 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인이나 행위자를 말한다.
(㉢) : 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.

① ㉠ 로그 ㉡ 위협 ㉢ 쿠키
② ㉠ 로그 ㉡ 위협 ㉢ 세션
③ ㉠ 백업 ㉡ 위협 ㉢ 세션
④ ㉠ 백업 ㉡ 위협 ㉢ 쿠키

정답 2번

출제 포인트

이 문제는 정보보안에서 로그, 위협, 세션의 정의를 구별할 수 있는지를 묻는 문제이다.

핵심 개념

로그: 시스템이나 네트워크에 대한 접근, 사용, 처리 결과 등 주요 활동을 시간의 흐름에 따라 기록한 정보이다. 키워드는 '활동 기록'이다.
위협: 자산에 손실이나 피해를 일으킬 수 있는 원하지 않는 사건의 잠재적 원인이나 행위자이다. 키워드는 '손실의 잠재적 원인'이다.
세션: 사용자와 시스템 또는 두 시스템 사이에 성립하여 유지되는 활성 접속이다. 키워드는 '활성화된 접속'이다.
백업은 장애나 손실에 대비하여 데이터를 별도로 복사해 두는 것이고, 쿠키는 웹사이트가 이용자의 브라우저 등에 저장하는 작은 데이터이므로 로그나 세션과 구별된다.

NoteBase

선지별 해설

① X — ㉠ 로그와 ㉡ 위협은 맞지만, ㉢의 '쿠키'가 틀렸다. 사용자와 시스템 또는 두 시스템 간의 활성화된 접속은 쿠키가 아니라 세션이다. 따라서 '㉠ 로그, ㉡ 위협, ㉢ 세션'으로 고쳐야 한다.
② O — 중요 활동의 기록은 로그, 자산 손실의 잠재적 원인이나 행위자는 위협, 활성화된 접속은 세션이므로 세 용어가 모두 정의와 일치한다.
③ X — ㉡ 위협과 ㉢ 세션은 맞지만, ㉠의 '백업'이 틀렸다. 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용의 기록은 백업이 아니라 로그이다. 따라서 '㉠ 로그, ㉡ 위협, ㉢ 세션'으로 고쳐야 한다.
④ X — ㉠의 '백업'과 ㉢의 '쿠키'가 틀렸다. ㉠은 중요 활동을 기록한 로그이고, ㉢은 활성화된 접속인 세션이다. 따라서 '㉠ 로그, ㉡ 위협, ㉢ 세션'으로 고쳐야 한다.

오답 포인트

로그·백업은 모두 데이터를 남기고, 세션·쿠키는 모두 웹 서비스 이용 과정에서 접할 수 있어 혼동하기 쉽다. 그러나 '접근 및 사용 내용의 기록'은 로그, '활성화된 접속'은 세션이라는 표현이 결정적이다.

다시 나오면 이렇게 판단

정의의 핵심 동사를 기준으로 판단한다. 활동을 '기록'하면 로그, 손실을 '초래할 잠재성'이면 위협, 접속이 '활성화되어 유지'되면 세션이다.

암기 포인트

기록은 로그, 손실의 잠재 원인은 위협, 활성 접속은 세션이다.

NoteBase

문 2. 다음 중 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 가장 옳지 않은 것은?

① 생성된 수열의 비트는 무작위로 발생한다.

② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 있어야 한다.

③ 시드(seed)라고 불리는 입력 값은 외부에 알려지지 않도록 비밀로 하여야 한다.

④ 고정값 시드(seed)를 입력받아 결정적 알고리즘을 사용하여 출력 비트열을 생성한다.

정답 2번

출제 포인트

암호학적으로 안전한 의사난수 생성기의 결정성과 예측 불가능성을 구별하는 문제이다.

핵심 개념

암호학적으로 안전한 의사난수 생성기(CSPRNG)는 시드를 입력받아 결정적 알고리즘으로 비트열을 만들지만, 시드를 모르는 공격자가 출력의 일부를 보고 나머지 출력을 계산상 실현 가능한 방법으로 예측할 수 없어야 한다. 출력은 통계적으로 무작위처럼 보여야 하며, 보안성은 시드의 충분한 엔트로피와 비밀성에 의존한다.

선지별 해설

① O — 출력 비트열은 통계적으로 무작위한 특성을 보여야 하므로 옳다.
② X — 틀린 표현은 '다른 부분 수열로부터 추정될 수 있어야 한다'이다. 실제로는 출력의 어느 부분을 알아도 다른 부분을 현실적인 계산으로 추정할 수 없어야 한다. 예측 가능하면 암호학적으로 안전하지 않다.
③ O — 시드가 알려지면 결정적 알고리즘의 출력도 재현될 수 있으므로 시드는 공격자가 알거나 추측하지 못하도록 비밀성과 예측 불가능성을 확보해야 한다.
④ O — 의사난수 생성기는 시드를 입력받아 결정적 알고리즘으로 출력 비트열을 생성하므로, 같은 고정 시드에는 같은 출력이 생성된다. 다만 실제 보안 운용에서는 공개되거나 반복되는 시드를 사용해서는 안 된다.

오답 포인트

의사난수 생성기가 결정적이라는 사실과 출력이 공격자에게 예측 가능하다는 뜻을 혼동하기 쉽다. 내부적으로 같은 시드에서 같은 출력이 나오더라도, 시드를 모르는 공격자는 한 부분 수열로 다른 부분 수열을 예측할 수 없어야 한다.

다시 나오면 이렇게 판단

CSPRNG 선지는 '결정적 생성'과 '외부의 예측 불가능성'을 함께 확인한다. 출력 일부로 과거·미래 출력이나 다른 부분을 추정할 수 있다고 하면 보안 조건에 반하므로 틀린 설명이다.

NoteBase

암기 포인트

같은 시드에는 같은 출력, 시드를 모르면 다음 출력은 예측 불가이다.

NoteBase

문 3. 다음 중 중앙 집중형 인증 방식인 커버로스(Kerberos)에 대한 설명으로 가장 옳지 않은 것은?

① 신뢰받는 제3자인 키 배포기관이 구성원들 중간에 개입하는 방법이다.

② 커버로스는 세션키를 이용한 티켓 기반 인증 기법을 제공한다.

③ 인증 서버가 사용자에게 발급한 티켓(승인 티켓)은 유효기간 내에 재사용할 수 있다.

④ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

정답 4번

출제 포인트

이 문제는 Kerberos의 중앙 집중형 인증 구조, 티켓과 세션키의 역할, SSO 지원 여부를 묻는 문제이다.

핵심 개념

Kerberos는 신뢰받는 제3자인 키 배포 센터(KDC)가 대칭키 기반의 티켓과 세션키를 발급하여, 분산 환경에서 사용자의 신원을 확인하고 서비스 이용을 인증하는 방식이다. 사용자는 최초 인증 후 티켓을 이용해 여러 서비스에 접근할 수 있으므로 SSO를 구현할 수 있다.

선지별 해설

① O — Kerberos는 신뢰받는 제3자인 키 배포 센터(KDC)가 사용자와 서비스 사이에서 인증 정보와 키를 배포하는 중앙 집중형 인증 방식이다.
② O — Kerberos는 사용자와 서비스가 공유할 세션키를 티켓에 담아 전달하고, 이 티켓을 근거로 인증하는 티켓 기반 기법이다.
③ O — 인증 서버가 발급하는 티켓 승인 티켓(TGT)은 정해진 유효기간 동안 티켓 발급 서버에 제시하여 서비스 티켓을 요청하는 데 재사용할 수 있다.
④ X — 틀린 표현은 'SSO 시스템을 구축할 수 없다'이다. Kerberos는 최초 인증으로 얻은 티켓 승인 티켓을 이용하여 분산 시스템의 여러 서비스에 접근할 수 있으므로 SSO 시스템을 구축할 수 있다.

오답 포인트

④는 Kerberos가 중앙 집중형이라는 점을 서비스도 한곳에 모여 있어야 한다는 뜻으로 혼동하게 만든다. 중앙 집중되는 것은 인증과 키 관리이며, 실제 서비스는 분산되어 있어도 티켓을 이용한 SSO가 가능하다.

다시 나오면 이렇게 판단

Kerberos 선지는 'KDC라는 신뢰기관', '대칭키와 세션키', '티켓 기반 인증', '분산 환경의 SSO'를 핵심 기준으로 판단한다. 이 가운데 SSO가 불가능하다고 하면 틀린 설명이다.

NoteBase

암기 포인트

Kerberos는 KDC가 티켓과 세션키를 발급하며, 분산 환경에서 SSO를 지원한다.

NoteBase

문 4. 다음 중 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화 되어 있는 파일로 가장 옳은 것은?

① /etc/group
② /etc/passwd
③ /etc/shadow
④ /etc/login.defs

정답 3번

출제 포인트

이 문제는 리눅스의 계정 관련 파일 중 사용자 패스워드 해시와 패스워드 사용 기간 정보를 함께 저장하는 파일을 구별하는 문제이다.

핵심 개념

/etc/shadow는 사용자별 패스워드 해시와 마지막 변경일, 최소·최대 사용 기간, 만료 경고 기간 등의 패스워드 에이징 정보를 저장하는 파일이다. 여기서 흔히 '암호화된 패스워드'라고 표현하는 값은 원래 패스워드를 복호화해 쓰는 암호문이 아니라, 검증에 사용하는 일방향 해시값이다.
/etc/passwd는 사용자 계정의 기본 정보, /etc/group은 그룹 정보, /etc/login.defs는 로그인 및 계정 생성에 적용할 기본 설정을 담는다.

NoteBase

선지별 해설

① X
/etc/group은 그룹 이름, 그룹 식별 번호, 소속 사용자 등 그룹 정보를 저장한다. 틀린 부분은 사용자 패스워드와 그 정책을 저장하는 파일로 본 점이며, 올바르게는 그룹 정보를 저장하는 파일이다.

② X
/etc/passwd는 사용자 이름, 사용자 식별 번호, 그룹 식별 번호, 홈 디렉터리, 로그인 셸 등의 계정 기본 정보를 저장한다. 틀린 부분은 실제 패스워드 해시가 이 파일에 저장된다고 본 점이며, 일반적인 shadow 패스워드 방식에서는 패스워드 필드에 x가 표시되고 실제 해시값은 /etc/shadow에 저장된다.

③ O
/etc/shadow는 사용자 패스워드 해시와 패스워드의 변경일·최소 및 최대 사용 기간·경고 기간 등 사용자별 패스워드 에이징 정보를 함께 저장하므로 문제의 조건에 맞는다.

④ X
/etc/login.defs는 로그인, 계정 생성, 패스워드 에이징 등에 사용할 시스템 기본값을 정하는 설정 파일이다. 틀린 부분은 사용자별 패스워드 해시까지 저장한다고 본 점이며, 올바르게는 실제 사용자별 패스워드 해시는 /etc/shadow에 저장된다.

오답 포인트

/etc/login.defs에도 패스워드 사용 기간의 기본 설정이 있어 ④가 그럴듯하다. 그러나 문제는 정책 정보뿐 아니라 사용자 패스워드 해시까지 들어 있는 하나의 파일을 묻고 있으므로 /etc/shadow가 정답이다.

다시 나오면 이렇게 판단

파일을 저장 대상별로 구분한다. 사용자 기본 정보는 /etc/passwd, 그룹 정보는 /etc/group, 사용자별 패스워드 해시와 에이징 정보는 /etc/shadow, 계정·로그인 정책의 기본값은 /etc/login.defs이다.

암기 포인트

passwd는 계정표, group은 그룹표, shadow는 비밀번호 해시와 사용자별 만료 정보, login.defs는 기본 정책이다.

NoteBase

문 5. 다음 중 유닉스 로그파일에 대한 설명으로 가장 옳지 않은 것은?

① lastlog : 사용자들이 마지막으로 로그아웃한 정보를 가지고 있다.

② utmp : 현재 로그인한 사용자 정보를 가지고 있다.

③ wtmp : 로그인과 로그아웃, 시스템 부팅 정보를 가지고 있다.

④ sulog : su(switch user) 명령어를 실행한 정보를 가지고 있다.

정답 1번

출제 포인트

유닉스의 주요 로그 파일이 기록하는 정보의 종류를 구분하는 문제이다.

핵심 개념

lastlog는 사용자별 마지막 로그인 정보를 기록한다. utmp는 현재 로그인 상태, wtmp는 로그인·로그아웃 및 시스템 부팅 이력, sulog는 su 명령의 실행 이력을 기록한다.

선지별 해설

① X — lastlog가 보관하는 것은 사용자의 마지막 로그아웃 정보가 아니라 마지막 로그인 정보이다. 틀린 표현인 '마지막으로 로그아웃한 정보'는 '마지막으로 로그인한 정보'로 고쳐야 한다.
② O — utmp는 현재 시스템에 로그인해 있는 사용자 정보를 기록하므로 현재 접속 상태를 확인할 때 이용한다.
③ O — wtmp는 사용자의 로그인과 로그아웃 이력을 누적하며 시스템 부팅 정보도 기록한다.
④ O — sulog는 사용자가 su 명령으로 다른 사용자 계정으로 전환을 시도하거나 실행한 이력을 기록한다.

오답 포인트

①의 '로그아웃'이 함정이다. lastlog의 이름에 있는 last는 마지막 접속 종료가 아니라 사용자별 마지막 로그인 시점을 뜻한다.

다시 나오면 이렇게 판단

현재 로그인 상태는 utmp, 누적된 로그인·로그아웃 및 부팅 이력은 wtmp, 사용자별 마지막 로그인은 lastlog, su 실행 이력은 sulog로 구분한다.

암기 포인트

lastlog는 마지막 로그인, utmp는 현재 접속, wtmp는 접속·종료의 누적 이력, sulog는 su 이력이다.

NoteBase

문 6. 다음 중 hwp, pdf, doc 등의 문서를 암호화하여 외부 유출 시에도 기업 내부 정보를 보호하는 것으로 가장 옳은 것은?

① DRM

② CDR

③ NFV

④ EDR

정답 1번

출제 포인트

문서 자체를 암호화하고 사용 권한을 통제하여 유출 뒤에도 내용을 보호하는 DRM과 다른 보안 기술의 차이를 묻는 문제이다.

핵심 개념

DRM(Digital Rights Management)은 문서 등 디지털 콘텐츠를 암호화하고 열람·편집·복사·출력 권한을 통제하는 기술이다.
CDR은 문서에서 악성 코드가 들어갈 수 있는 활성 콘텐츠를 제거하고 안전한 형태로 재구성하는 기술이다.
NFV는 방화벽·라우터 같은 네트워크 기능을 전용 장비가 아닌 소프트웨어로 가상화하는 기술이다.
EDR은 PC·서버 같은 단말의 위협 행위를 탐지하고 조사·대응하는 기술이다.

선지별 해설

① O — DRM은 hwp, pdf, doc 등의 문서를 암호화하고 사용자별 이용 권한을 제한하므로, 문서가 외부로 유출되어도 권한 없는 사람이 내용을 이용하지 못하게 한다.
② X — CDR이라는 표현이 틀렸다. CDR은 파일의 악성 요소를 제거한 뒤 안전한 파일로 재구성하는 기술이며, 문서를 암호화하여 유출 후에도 정보를 보호하는 기술은 DRM이다.
③ X — NFV라는 표현이 틀렸다. NFV는 네트워크 기능을 범용 서버에서 소프트웨어로 구현하는 기술이며, 문서 암호화와 권한 통제에 해당하는 기술은 DRM이다.
④ X — EDR이라는 표현이 틀렸다. EDR은 단말에서 발생하는 위협을 지속적으로 탐지하고 대응하는 기술이며, 유출된 문서의 내용을 암호화 상태로 보호하는 기술은 DRM이다.

오답 포인트

②의 CDR도 문서 보안에 쓰이므로 혼동하기 쉽다. 그러나 CDR의 핵심은 위험 요소 제거와 재구성이고, DRM의 핵심은 암호화와 이용 권한 통제이다.

NoteBase

다시 나오면 이렇게 판단

문서 암호화·열람 권한·복사 및 출력 통제가 제시되면 DRM, 문서 내 악성 요소 제거가 제시되면 CDR, 네트워크 기능의 소프트웨어화가 제시되면 NFV, 단말 위협 탐지·대응이 제시되면 EDR로 판단한다.

암기 포인트

DRM은 문서 권한 보호, CDR은 문서 위험 제거, NFV는 네트워크 기능 가상화, EDR은 단말 위협 대응이다.

NoteBase

문 7. 다음 중 개인정보영향평가 시 고려하여야 할 사항으로 가장 옳지 않은 것은?

① 처리하는 개인정보의 수

② 개인정보처리자의 인가 여부

③ 정보주체의 권리를 해할 가능성 및 그 위험 정도

④ 개인정보의 제3자 제공 여부

정답 2번

쟁점

이 문제는 개인정보 영향평가에서 법적으로 고려하여야 하는 사항에 관한 문제이다. 핵심은 개인정보의 처리 규모·제공 관계·권리 침해 위험과 개인정보처리자에 대한 인가 여부를 구별하는 것이다.

용어 풀이

개인정보 영향평가는 개인정보파일의 운용으로 발생할 수 있는 개인정보 침해 위험요인을 미리 분석하고 개선 사항을 도출하는 평가이다.

핵심 구분

현행 개인정보 보호법 제33조는 영향평가 시 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성과 그 위험 정도, 그 밖에 대통령령으로 정한 사항을 고려하도록 한다. 개인정보처리자의 인가 여부는 이 법정 고려사항에 포함되지 않는다.

NoteBase

선지별 해설

① O
처리하는 개인정보의 수는 개인정보 처리 규모와 침해 발생 시 영향을 판단하는 법정 고려사항이다.

② X
개인정보처리자의 인가 여부는 개인정보 영향평가의 법정 고려사항이 아니다.
틀린 표현: 개인정보처리자의 인가 여부
올바른 표현: 개인정보처리자의 인가 여부는 고려사항이 아니며, 개인정보의 처리 규모·제3자 제공 여부·정보주체의 권리 침해 위험 등을 고려한다.

③ O
정보주체의 권리를 해할 가능성 및 그 위험 정도는 영향평가가 분석하려는 핵심 위험이므로 법정 고려사항이다.

④ O
개인정보의 제3자 제공 여부는 개인정보의 이용 범위와 외부 확산 위험에 관계되므로 법정 고려사항이다.

오답 포인트

②의 '인가 여부'를 영향평가 수행기관의 지정 제도와 혼동하기 쉽다. 영향평가의 고려사항은 개인정보처리자에 대한 인가가 아니라 개인정보의 규모, 제공 관계, 정보주체의 권리 침해 위험에 초점이 있다.

다시 나오면 이렇게 판단

선지의 내용이 개인정보파일의 규모, 외부 제공, 정보주체의 권리 침해 위험처럼 개인정보 침해 가능성을 평가하는 요소인지 확인한다. 개인정보처리자 자체에 대한 인가 여부처럼 위험평가와 직접 관련이 없는 항목은 제외한다.

암기 포인트

영향평가 고려사항은 '개인정보의 수·제3자 제공·권리 침해 위험'이고, 개인정보처리자의 인가 여부는 아니다.

NoteBase

문 8. 다음 중 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.

② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.

③ 메시지 자체를 암호화 또는 복호화 할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.

④ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화 할 수 있다.

정답 1번

출제 포인트

하이브리드 암호 시스템이 공개키 암호로 세션키를 안전하게 전달하고, 대칭키 암호로 메시지를 빠르게 처리한다는 결합 원리를 묻는 문제이다.

핵심 개념

대칭키 암호는 암호화와 복호화에 같은 비밀키를 사용하므로 처리 속도는 빠르지만, 통신 전에 그 키를 안전하게 공유하기 어렵다. 공개키 암호는 공개키와 개인키의 쌍을 사용하여 키 전달 문제를 보완하지만 대량의 메시지 처리에는 상대적으로 느리다. 하이브리드 암호 시스템은 메시지는 대칭키인 세션키로 암호화하고, 세션키는 수신자의 공개키로 암호화하여 전달함으로써 두 방식의 장점을 결합한다.

선지별 해설

① X — '대칭키 암호의 키 교환 문제가 존재한다'는 표현이 틀렸다. 하이브리드 암호 시스템은 세션키를 수신자의 공개키로 암호화해 전달하므로 대칭키 암호의 안전한 키 교환 문제를 보완한다. 올바르게는 '하이브리드 암호 시스템은 공개키 암호를 이용하여 대칭키의 키 교환 문제를 해결한다'이다.
② O — 송신자는 메시지 암호화에 사용한 대칭키인 세션키를 수신자의 공개키로 암호화하여 전달한다. 수신자의 공개키로 암호화한 세션키는 그와 짝을 이루는 수신자의 개인키로만 복호화할 수 있다.
③ O — 실제 메시지는 처리 속도가 빠른 대칭키 암호로 암호화하고 복호화한다. 공개키 암호는 주로 크기가 작은 세션키를 안전하게 전달하는 데 사용한다.
④ O — 수신자는 자신의 공개키로 암호화되어 온 세션키를 자신의 개인키로 복호화한다. 이렇게 얻은 세션키로 메시지 본문을 복호화한다.

오답 포인트

①은 대칭키 암호 자체의 약점과 하이브리드 암호 시스템의 성질을 혼동하게 한다. 대칭키 암호에는 안전한 키 공유 문제가 있지만, 하이브리드 방식은 바로 그 문제를 공개키 암호로 보완한 방식이다.

NoteBase

다시 나오면 이렇게 판단

‘무엇을 암호화하는가’를 구분한다. 메시지 본문은 빠른 대칭키로 처리하고, 그때 쓰는 세션키는 수신자의 공개키로 암호화하여 보내며 수신자의 개인키로 복호화한다.

암기 포인트

본문은 대칭키, 세션키 전달은 공개키, 세션키 복호화는 수신자의 개인키이다.

NoteBase

문 9. 다음 중 유닉스에서 파일의 속성을 검색하는 find 옵션으로 가장 옳지 않은 것은?

① mtime : 파일의 내용이 수정된 시간을 기준으로 검색한다.

② atime : 파일에 접근한 시간을 기준으로 검색한다.

③ ctime : 파일 속성, 권한, 크기가 변경된 시간을 기준으로 검색한다.

④ rtime : 파일 실행 일자를 기준으로 검색한다.

정답 4번

출제 포인트

유닉스 find 명령에서 파일의 시간 정보를 기준으로 검색하는 mtime, atime, ctime의 의미와 존재하지 않는 rtime을 구별하는 문제이다.

핵심 개념

mtime은 파일 내용이 마지막으로 수정된 시각, atime은 파일 내용에 마지막으로 접근한 시각, ctime은 권한·소유자 등 파일의 상태 정보가 마지막으로 변경된 시각을 뜻한다. 일반적인 유닉스 find에는 파일 실행 일자를 뜻하는 rtime 조건이 없다.

선지별 해설

① O — mtime은 modification time으로, 파일 내용이 수정된 시간을 기준으로 검색한다.
② O — atime은 access time으로, 파일을 읽는 등 파일 내용에 접근한 시간을 기준으로 검색한다.
③ O — ctime은 change time으로, 권한·소유자 같은 파일 상태 정보가 변경된 시간을 기준으로 검색한다. 파일 크기가 달라지는 변경도 ctime에 반영된다.
④ X — 틀린 표현은 ‘rtime : 파일 실행 일자’이다. 일반적인 유닉스 find에는 rtime이라는 시간 검색 조건이 없으며, 실행 일자를 기준으로 검색하는 표준 조건도 아니다. 올바르게는 find의 대표적인 시간 조건을 mtime, atime, ctime으로 구분한다.

오답 포인트

rtime이 run time의 약어처럼 보여 실제 조건으로 착각하기 쉽다. 또한 ctime을 creation time으로 오해하기 쉽지만, 유닉스에서 ctime은 파일 생성 시각이 아니라 파일 상태 정보의 변경 시각이다.

다시 나오면 이렇게 판단

시간 조건의 첫 글자를 기준으로 m은 내용 수정, a는 접근, c는 상태 변경으로 대응한다. 이 세 가지에 포함되지 않는 rtime 같은 표현은 실제 find 조건인지 별도로 판별한다.

NoteBase

암기 포인트

m은 modify, a는 access, c는 change이며, rtime은 없다.

NoteBase

문 10. 다음의 ㉠ ~ ㉢에 해당되는 대칭키 암호 알고리즘을 가장 옳게 나열한 것은?

<보기>
㉠ DES의 암호화 강도가 점점 약해지면서 이를 대체하기 위한 알고리즘으로 현재 미국 연방정부표준 블록 암호 알고리즘(NIST FIPS 197)으로 사용
㉡ 국내에서 민간 부분인 인터넷, 전자상거래, 무선 통신 등에서 민감 정보 및 프라이버시 보호를 위해 한국인터넷진흥원(KISA)이 주축이 되어 개발한 128/256 비트 암호키를 지원하며 IFTF 및 ISO/IEC 국제표준으로 채택된 바 있음
㉢ 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안기술연구소 주도로 경량 환경 및 하드웨어의 효율성 향상을 위해 개발된 128비트 블록 암호 알고리즘으로 128/192/256 비트 암호화키를 지원

① ㉠ AES ㉡ SEED ㉢ ARIA
② ㉠ AES ㉡ ARIA ㉢ SEED
③ ㉠ ARIA ㉡ SEED ㉢ AES
④ ㉠ ARIA ㉡ AES ㉢ SEED

정답 1번

출제 포인트

대칭키 블록 암호인 AES, SEED, ARIA를 개발 배경과 개발 주체, 지원 키 길이로 구별하는 문제이다.

핵심 개념

AES: DES를 대체하기 위해 선정된 미국 연방정부 표준 블록 암호로, 128비트 블록과 128·192·256비트 키를 사용한다.
SEED: 한국인터넷진흥원(KISA)이 주도하여 개발한 국산 블록 암호이며, 국내 민간 분야의 정보 보호와 국제표준 채택이라는 설명이 핵심 단서이다.
ARIA: 국가보안기술연구소 주도로 전자정부 등 다양한 환경에 맞게 개발한 128비트 블록 암호로, 128·192·256비트 키를 지원한다.

선지별 해설

① O — ㉠은 DES를 대체한 미국 표준 AES, ㉡은 KISA 주도로 개발된 SEED, ㉢은 국가보안기술연구소 주도로 개발된 ARIA이므로 모두 옳게 연결되었다.
② X — ㉡의 'ARIA'와 ㉢의 'SEED'가 서로 뒤바뀌었다. 올바르게는 ㉡ SEED, ㉢ ARIA이다.
③ X — ㉠의 'ARIA'와 ㉢의 'AES'가 틀렸다. 올바르게는 ㉠ AES, ㉡ SEED, ㉢ ARIA이다.
④ X — ㉠의 'ARIA', ㉡의 'AES', ㉢의 'SEED'가 모두 틀렸다. 올바르게는 ㉠ AES, ㉡ SEED, ㉢ ARIA이다.

NoteBase

오답 포인트

SEED와 ARIA가 모두 국내에서 개발된 블록 암호라는 점 때문에 ㉡과 ㉢을 바꾸기 쉽다. ㉡의 KISA·민간 분야·국제표준은 SEED, ㉢의 국가보안기술연구소·전자정부·다양한 환경은 ARIA를 가리킨다.

다시 나오면 이렇게 판단

먼저 'DES 대체·미국 표준'이면 AES로 확정한다. 국내 알고리즘은 'KISA·민간 분야'이면 SEED, '국가보안기술연구소·전자정부·128·192·256비트 키'이면 ARIA로 구별한다.

암기 포인트

미국 DES 대체는 AES, KISA 민간 보안은 SEED, 국가보안기술연구소 전자정부는 ARIA이다.

NoteBase

문 11. 서버 관리자가 사용할 수 있는 보안용 소프트웨어 중 그 용도가 가장 다른 것은?

① AWstats

② Nessus

③ Acunetix

④ Nmap

정답 1번

출제 포인트

서버 관련 도구를 로그 분석 도구와 보안 스캔·점검 도구로 구분하는 문제이다.

핵심 개념

AWStats는 웹·FTP·메일 서버 등의 로그를 분석하여 접속 현황과 이용 통계를 생성하는 로그 분석 도구이다. 반면 Nessus는 시스템·네트워크 취약점 점검, Acunetix는 웹 애플리케이션 취약점 점검, Nmap은 호스트·서비스·포트 탐색과 보안 점검에 사용된다. 따라서 AWStats만 주된 용도가 로그 기반 통계 분석이고, 나머지는 대상을 능동적으로 스캔하여 보안 상태를 파악하는 데 쓰인다.

선지별 해설

① O — AWStats는 서버 로그를 분석하여 방문자, 접속, 트래픽 등의 통계를 제공한다. 취약점이나 열린 포트를 직접 스캔하는 도구가 아니므로 나머지 세 도구와 용도가 가장 다르다.
② X — Nessus는 운영체제, 네트워크 장비, 서버 등의 취약점과 잘못된 설정을 스캔하는 취약점 진단 도구이다. 이 선지를 이질적 도구로 보는 판단이 틀리며, 올바르게는 보안 취약점 스캔 도구로 분류된다.
③ X — Acunetix는 웹 사이트와 웹 애플리케이션을 대상으로 SQL 삽입, 크로스 사이트 스크립팅 등의 취약점을 점검하는 웹 취약점 스캐너이다. 이 선지를 로그 통계 도구로 보는 판단이 틀리며, 올바르게는 웹 보안 점검 도구로 분류된다.
④ X — Nmap은 네트워크의 호스트, 열린 포트, 제공 서비스 등을 탐색하며 보안 감사에도 활용되는 네트워크 스캐닝 도구이다. 이 선지를 로그 분석 도구로 보는 판단이 틀리며, 올바르게는 네트워크 탐색·보안 점검 도구로 분류된다.

오답 포인트

네 도구가 모두 서버 관리에 활용될 수 있다는 공통점만 보면 구별하기 어렵다. 핵심 함정은 '보안용 소프트웨어'라는 표현에 끌려 모든 선지를 취약점 진단 도구로 보는 것이다. AWStats는 보안 대상을 직접 탐지·점검하기보다 이미 생성된 로그를 분석하여 통계를 제시한다.

NoteBase

다시 나오면 이렇게 판단

도구가 무엇을 입력으로 삼고 어떤 결과를 내는지로 구분한다. 로그를 읽어 접속 통계를 만들면 로그 분석 도구이고, 대상에 탐색 요청을 보내 포트·서비스·취약점을 찾으면 보안 스캔 도구이다.

암기 포인트

AWStats는 로그 통계, Nessus는 시스템 취약점, Acunetix는 웹 취약점, Nmap은 네트워크·포트 탐색이다.

NoteBase

문 12. 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 가장 옳지 않게 연결된 것은?

① ps, top : 특정 프로세스 정보를 숨김

② w, who : 특정 사용자의 정보를 숨김

③ ls, du : 특정 파일이나 디렉토리를 숨김

④ ifconfig : 특정 IP에서의 접속을 숨김

정답 4번

출제 포인트

이 문제는 공격자가 변조한 리눅스 시스템 명령어와 그 명령어를 통해 은닉하려는 정보를 올바르게 연결할 수 있는지를 묻는다.

핵심 개념

공격자는 시스템 명령어의 바이너리를 변조하여 관리자가 명령을 실행해도 침입 흔적이 출력되지 않게 할 수 있다. ps·top은 프로세스, w·who는 로그인 사용자와 세션, ls·du는 파일·디렉터리 관련 정보를 다룬다. 반면 ifconfig는 네트워크 인터페이스의 설정과 상태를 확인하는 명령어이며, 특정 IP와의 접속 내역을 확인하는 명령어가 아니다.

선지별 해설

① O — ps와 top은 실행 중인 프로세스 정보를 보여 주므로, 변조하면 공격자가 실행한 특정 악성 프로세스를 목록에서 숨길 수 있다.
② O — w와 who는 현재 로그인한 사용자와 세션 정보를 보여 주므로, 변조하면 공격자가 사용 중인 특정 계정이나 로그인 세션을 숨길 수 있다.
③ O — ls는 파일·디렉터리 목록을, du는 파일·디렉터리의 디스크 사용량을 보여 주므로, 변조하면 특정 파일이나 디렉터리의 존재 및 관련 사용량을 숨길 수 있다.
④ X — 틀린 표현은 ‘ifconfig로 특정 IP에서의 접속을 숨긴다’이다. ifconfig는 네트워크 인터페이스의 설정과 상태를 표시하는 명령어이다. 특정 IP와 맺은 네트워크 접속 정보를 숨기려는 목적이라면 접속 상태를 표시하는 netstat 등의 명령어 변조와 연결하는 것이 옳다.

오답 포인트

④에서 ifconfig가 IP 주소를 표시한다는 점 때문에 ‘특정 IP에서의 접속’까지 확인한다고 혼동하기 쉽다. 그러나 인터페이스에 설정된 IP 주소와 원격 IP와의 실제 접속 내역은 서로 다른 정보이다.

NoteBase

다시 나오면 이렇게 판단

각 명령어가 정상적으로 무엇을 출력하는지 먼저 대응한다. 프로세스는 ps·top, 로그인 사용자는 w·who, 파일·디렉터리는 ls·du, 네트워크 인터페이스 설정은 ifconfig, 네트워크 접속 상태는 netstat 계열로 구분한다.

암기 포인트

ps·top은 프로세스, w·who는 사용자, ls·du는 파일, ifconfig는 인터페이스이다.

NoteBase

문 13. 다음은 FTP(File Transfer Protocol) 서비스에 대한 내용을 설명한 것이다. 가장 옳지 않은 것은?

① 전송계층 프로토콜로 TCP를 사용하고 있으며, 클라이언트 서버 모델로 구성되어 있다.

② IETF에 따라 RFC 959로 정의된다.

③ 기본적으로 액티브 모드(Active mode)와 패시브 모드(Passive mode)를 지원한다.

④ 제어 연결은 21 포트를, 데이터 연결은 512 이후 포트를 사용한다.

정답 4번

출제 포인트

FTP의 전송계층 프로토콜, 표준 문서, 동작 모드, 제어·데이터 연결의 포트를 구분하는 문제이다.

핵심 개념

FTP는 클라이언트와 서버 사이에서 파일을 전송하는 응용계층 프로토콜로, TCP 기반의 제어 연결과 데이터 연결을 별도로 사용한다. 제어 연결은 서버의 TCP 21번 포트를 사용하며, 액티브 모드의 기본 데이터 연결은 서버의 TCP 20번 포트에서 시작한다. 패시브 모드에서는 서버가 데이터 연결에 사용할 포트를 동적으로 정하여 클라이언트에 알린다.

선지별 해설

① O — FTP는 신뢰성 있는 전송을 위해 전송계층에서 TCP를 사용하며, FTP 클라이언트가 FTP 서버에 접속하는 클라이언트·서버 구조로 동작한다.
② O — FTP의 기본 명세는 RFC 959에 규정되어 있다.
③ O — FTP는 데이터 연결을 누가 시작하는지에 따라 액티브 모드와 패시브 모드를 지원한다. 액티브 모드에서는 서버가 클라이언트 쪽으로 데이터 연결을 시작하고, 패시브 모드에서는 클라이언트가 서버가 알려 준 포트로 데이터 연결을 시작한다.
④ X — 틀린 부분은 '데이터 연결은 512 이후 포트를 사용한다'이다. 올바르게는 제어 연결에 서버의 TCP 21번 포트를 사용하고, 액티브 모드의 기본 데이터 연결에는 서버의 TCP 20번 포트를 사용한다. 패시브 모드의 데이터 포트는 서버가 동적으로 정하여 알려 주므로 512 이후로 고정되지 않는다.

오답 포인트

④는 제어 연결의 21번 포트는 맞게 제시한 뒤 데이터 연결 포트만 '512 이후'로 바꾸어 혼동을 유도한다. FTP의 기본 포트는 제어 21번, 액티브 데이터 20번으로 구분한다.

다시 나오면 이렇게 판단

FTP 선지에서는 먼저 TCP 기반인지와 제어·데이터 연결이 분리되는지를 확인하고, 포트가 나오면 '제어 21번, 액티브 데이터 20번, 패시브 데이터 포트는 동적 지정'의 기준으로 판단한다.

NoteBase

암기 포인트

FTP는 TCP, 제어는 21번, 액티브 데이터는 20번이다.

문 14. 다음 중 블록 암호 알고리즘의 종류가 아닌 것은?

① RC5

② DES

③ MD5

④ IDEA

정답 3번

출제 포인트

이 문제는 블록 암호와 해시 함수의 용도를 구별하는 문제이다.

핵심 개념

블록 암호는 일정한 길이의 평문 블록을 비밀키로 암호화하고 복호화하는 대칭키 암호 방식이다. RC5, DES, IDEA가 이에 해당한다.
해시 함수는 임의 길이의 입력을 고정 길이의 해시값으로 변환하는 일방향 함수이다. MD5가 이에 해당하며, 암호문을 다시 평문으로 복호화하는 블록 암호가 아니다.

선지별 해설

① O — RC5는 비밀키를 이용하여 고정 크기 블록을 암호화하는 대칭키 블록 암호 알고리즘이다.
② O — DES는 64비트 블록을 처리하는 대표적인 대칭키 블록 암호 알고리즘이다.
③ X — 틀린 분류는 ‘MD5가 블록 암호 알고리즘이다’라는 것이다. MD5는 입력 데이터의 해시값을 만드는 암호학적 해시 함수이며, 올바르게는 블록 암호 알고리즘이 아닌 해시 알고리즘으로 분류한다.
④ O — IDEA는 64비트 블록을 처리하는 대칭키 블록 암호 알고리즘이다.

오답 포인트

MD5에도 ‘암호학적’이라는 표현이 붙기 때문에 암호화 알고리즘으로 혼동하기 쉽다. 그러나 MD5는 키로 암호화·복호화하는 방식이 아니라 데이터의 해시값을 만드는 함수이다.

다시 나오면 이렇게 판단

알고리즘이 비밀키로 평문을 암호문으로 바꾸고 다시 복호화하면 블록 암호로, 입력의 요약값인 해시값을 일방향으로 만들면 해시 함수로 판단한다.

암기 포인트

RC5·DES·IDEA는 블록 암호, MD5는 해시 함수이다.

NoteBase

문 15. 다음은 윈도우 부팅 순서이다. 가장 옳게 나열한 것은?

<보기>
㉠ MBR - 부팅 매체에 대한 기본적인 파일 시스템 정보가 들어 있는 MBR 정보를 읽는다.
㉡ POST - 하드웨어 자체가 시스템에 문제가 없는지 기본적인 사항을 체크하는 과정
㉢ NTLDR - 하드디스크의 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며 boot.ini 파일의 내용을 읽는다.
㉣ NTDETECT.com - 설치된 하드웨어를 검사한다.
㉤ ntoskrnl.exe - HAL.dll을 로드한다.
㉥ CMOS - 사용자가 설정한 기본 사항을 읽어 시스템에 적용한다.

① ㉥ - ㉢ - ㉣ - ㉠ - ㉤ - ㉡
② ㉡ - ㉥ - ㉢ - ㉣ - ㉠ - ㉤
③ ㉡ - ㉥ - ㉠ - ㉢ - ㉣ - ㉤
④ ㉥ - ㉠ - ㉤ - ㉡ - ㉢ - ㉣

정답 3번

출제 포인트

윈도우 부팅 과정에서 하드웨어 점검과 기본 설정 적용, 부팅 디스크 탐색, 운영체제 로더 실행, 하드웨어 검색, 커널 적재가 어떤 순서로 진행되는지를 묻는 문제이다.

올바른 순서

㉡ POST → ㉥ CMOS → ㉠ MBR → ㉢ NTLDR → ㉣ NTDETECT.com → ㉤ ntoskrnl.exe

1. POST — 부팅을 시작하면서 하드웨어의 기본 이상 유무를 점검한다.
2. CMOS — 사용자가 설정한 시스템의 기본 사항을 읽어 적용한다.
3. MBR — 부팅 매체의 MBR 정보를 읽어 부팅할 파티션을 찾는다.
4. NTLDR — 부팅 파티션에서 실행되어 boot.ini의 내용을 읽고 윈도우 부팅을 진행한다.
5. NTDETECT.com — 설치된 하드웨어를 검색한다.
6. ntoskrnl.exe — 윈도우 커널이 실행되며 HAL.dll을 로드한다.

이 순서인 이유는 기본 하드웨어 점검과 설정 적용이 끝나야 부팅 디스크의 MBR을 읽을 수 있고, MBR이 부팅 파티션의 NTLDR로 제어를 넘겨야 하드웨어 검색과 커널 적재가 이어지기 때문이다.

NoteBase

선지별 해설

① X — ㉥ CMOS로 시작하고 ㉡ POST를 마지막에 둔 것이 잘못이다. 하드웨어 기본 점검인 POST가 먼저 이루어진 뒤 CMOS 설정을 적용한다. 올바르게는 ㉡ → ㉥ → ㉠ → ㉢ → ㉣ → ㉤이다.

② X — ㉠ MBR을 ㉢ NTLDR와 ㉣ NTDETECT.com 뒤에 둔 것이 잘못이다. MBR을 먼저 읽어 부팅 파티션의 NTLDR로 제어를 넘긴 뒤 NTDETECT.com이 하드웨어를 검색한다. 올바르게는 ㉡ → ㉥ → ㉠ → ㉢ → ㉣ → ㉤이다.

③ O — POST로 하드웨어를 점검하고 CMOS 설정을 적용한 다음, MBR → NTLDR → NTDETECT.com → ntoskrnl.exe의 순서로 진행하므로 옳다.

④ X — ㉡ POST를 ㉤ ntoskrnl.exe 뒤에 둔 것이 잘못이다. POST는 운영체제 커널이 적재되기 전, 부팅 초기에 수행되는 하드웨어 점검이다. 올바르게는 ㉡ → ㉥ → ㉠ → ㉢ → ㉣ → ㉤이다.

오답 포인트

POST와 CMOS의 앞뒤를 혼동하거나, MBR을 NTLDR 뒤의 단계로 생각하기 쉽다. 특히 ②는 시작 두 단계가 맞지만 MBR을 뒤로 보낸 함정이다. MBR이 먼저 부팅 파티션의 로더인 NTLDR로 제어를 넘긴다는 선후관계가 핵심이다.

다시 나오면 이렇게 판단

부팅 순서는 '하드웨어 점검 → 기본 설정 적용 → 부팅 디스크 정보 확인 → 운영체제 로더 실행 → 하드웨어 검색 → 커널 적재'의 흐름으로 판단한다. 각 단계의 산출물이 다음 단계의 입력이 되는지를 확인하면 순서를 정할 수 있다.

암기 포인트

POST–CMOS–MBR–NTLDR–NTDETECT–커널 순서로 기억한다.

NoteBase

문 16. '사이버위기경보'의 등급 중 복수 정보통신서비스 제공자(ISP) 망에 장애 또는 마비가 발생하였을 경우, 발령하는 경보의 단계는 무엇인가?

① 심각 단계
② 경계 단계
③ 주의 단계
④ 관심 단계

정답 2번

출제 포인트

사이버위기경보의 각 단계와 정보통신망 장애 범위를 연결하는 문제이다.

핵심 개념

관심은 위기징후 감시를 강화하는 단계이고, 주의는 일부 정보통신망·정보시스템의 장애 등에 협조 체제를 가동하는 단계이다. 경계는 복수 정보통신서비스제공자(ISP)망·기간통신망의 장애 또는 마비 등에 즉각대응 태세로 돌입하는 단계이며, 심각은 국가 차원의 주요 정보통신망·정보시스템 장애 또는 마비 등에 대응역량을 총동원하는 단계이다.

선지별 해설

① X — 심각 단계는 국가 차원의 주요 정보통신망 및 정보시스템에 장애 또는 마비가 발생하거나 사고가 전국적·대규모로 발생한 경우에 해당한다. '심각 단계'가 아니라 '경계 단계'가 올바르다.
② O — 복수 정보통신서비스제공자(ISP)망·기간통신망에 장애 또는 마비가 발생한 경우는 경계 단계의 판단 기준에 해당한다.
③ X — 주의 단계는 일부 정보통신망 및 정보시스템의 장애나 사고가 다수 기관으로 확산될 가능성이 증가한 경우에 해당한다. '주의 단계'가 아니라 '경계 단계'가 올바르다.
④ X — 관심 단계는 위기징후의 활동 수준이 낮지만 피해 발생 가능성이나 국내 유입 우려 등이 나타나 감시를 강화하는 단계이다. '관심 단계'가 아니라 '경계 단계'가 올바르다.

오답 포인트

'마비'라는 표현만 보고 최고 단계인 심각을 고르기 쉽다. 이 문항에서는 장애 범위가 '복수 ISP망'이므로 경계이고, '국가 차원의 주요 정보통신망' 또는 '전국적·대규모 피해'까지 이르면 심각이다.

다시 나오면 이렇게 판단

장애 범위를 기준으로 구분한다. 일부 망은 주의, 복수 ISP망·기간통신망은 경계, 국가 차원의 주요 망이나 전국적·대규모 피해는 심각으로 판단한다.

NoteBase

암기 포인트

일부는 주의, 복수 ISP는 경계, 국가 차원은 심각이다.

NoteBase

문 17. 다음 중 전자우편 보안기술 PGP의 기능으로 가장 옳지 않은 것은?

① 전자서명

② 암호화

③ 생체인증

④ 무결성

정답 3번

출제 포인트

이 문제는 전자우편 보안기술인 PGP가 제공하는 기밀성·인증·무결성 기능과 PGP의 기능이 아닌 생체인증을 구별하는 문제이다.

핵심 개념

PGP(Pretty Good Privacy)는 전자우편의 내용을 암호화하고 전자서명을 적용하여 기밀성, 송신자 인증, 무결성을 제공하는 보안기술이다. 생체인증은 지문·홍채·얼굴 등 개인의 신체적 또는 행동적 특징으로 사용자를 확인하는 별도의 인증 방식이다.

선지별 해설

① O — PGP는 공개키 암호기술을 이용한 전자서명으로 송신자를 인증하고 메시지의 위조 여부를 확인할 수 있다.
② O — PGP는 메시지를 암호화하여 권한이 없는 사람이 전자우편 내용을 읽지 못하게 하는 기밀성을 제공한다.
③ X — '생체인증'은 PGP의 기능이 아니다. 올바르게는 PGP가 전자서명과 암호화를 이용하여 송신자 인증을 제공한다고 표현해야 한다.
④ O — PGP의 전자서명 과정에서는 메시지의 해시값을 활용하므로, 전송 중 내용이 변경되었는지를 확인하여 무결성을 검증할 수 있다.

오답 포인트

③의 '생체인증'도 보안기술이므로 PGP의 기능처럼 보이는 것이 함정이다. PGP는 전자우편 메시지를 암호화하고 전자서명하는 기술이며, 지문·홍채·얼굴을 인식하는 기능은 포함하지 않는다.

다시 나오면 이렇게 판단

PGP의 기능 여부는 전자우편 메시지 자체를 보호하는 기능인지로 판단한다. 암호화는 기밀성, 전자서명은 송신자 인증과 무결성에 연결되고, 생체정보로 사람을 식별하는 기능은 PGP에서 제외된다.

NoteBase

암기 포인트

PGP는 암호화·전자서명·무결성, 생체인증은 별도 방식이다.

NoteBase

문 18. 다음의 접근통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것은?

<보기>
㉠ 벨라파듈라(Bell-LaPadula) 모델
㉡ 비바(Biba) 모델
㉢ 클락 윌슨(Clark-Wilson) 모델

① ㉠
② ㉡
③ ㉠ ㉡
④ ㉡ ㉢

정답 4번

출제 포인트

벨라파듈라 모델은 기밀성을, 비바 모델과 클락 윌슨 모델은 무결성을 보장하기 위한 접근통제 모델이라는 차이를 묻는 문제이다.

핵심 개념

벨라파듈라 모델: 정보가 권한 없는 주체에게 유출되지 않도록 기밀성을 보호하는 모델이다. 핵심 규칙은 상위 보안등급 정보의 읽기를 금지하고 하위 보안등급으로의 쓰기를 금지하는 것이다.
비바 모델: 정보가 부적절하게 변경되는 것을 막아 무결성을 보호하는 모델이다. 낮은 무결성 등급의 정보를 읽지 못하게 하고 높은 무결성 등급으로 쓰지 못하게 한다.
클락 윌슨 모델: 잘 형성된 거래와 직무 분리를 통해 상업적 정보시스템의 무결성을 보호하는 모델이다.

선지별 해설

① X — ㉠ 벨라파듈라 모델은 무결성이 아니라 기밀성을 보장하기 위한 모델이다. 올바르게는 무결성 모델로 ㉡ 비바 모델과 ㉢ 클락 윌슨 모델을 골라야 한다.
② X — ㉡ 비바 모델은 무결성 모델이지만, ㉢ 클락 윌슨 모델도 무결성 모델이므로 '㉡만' 고른 것은 불완전하다. 올바르게는 ㉡과 ㉢을 모두 골라야 한다.
③ X — ㉠ 벨라파듈라 모델을 무결성 모델에 포함한 부분과 ㉢ 클락 윌슨 모델을 제외한 부분이 틀렸다. 올바른 조합은 ㉡ 비바 모델과 ㉢ 클락 윌슨 모델이다.
④ O — ㉡ 비바 모델과 ㉢ 클락 윌슨 모델은 모두 정보의 부적절한 변경을 방지하여 무결성을 보장하기 위한 모델이다.

NoteBase

오답 포인트

②는 대표적인 무결성 모델인 비바만 제시하여 정답처럼 보이게 하지만, 거래의 적정성과 직무 분리로 무결성을 보장하는 클락 윌슨도 포함해야 한다. 벨라파듈라는 기밀성 모델이라는 점도 함께 구별해야 한다.

다시 나오면 이렇게 판단

보안 모델의 보호 목표를 먼저 분류한다. 기밀성은 벨라파듈라, 무결성은 비바와 클락 윌슨으로 대응시키고, 복수 선택형에서는 같은 목표에 속하는 모델이 빠지지 않았는지 확인한다.

암기 포인트

기밀성은 벨라파듈라, 무결성은 비바·클락 윌슨이다.

NoteBase

문 19. 다음에서 설명하는 키의 종류는 무엇인가?

<보기>
㉠ 반복적으로 사용하는 대표키로 안전한 보관이 필요하다.
㉡ 한번만 사용하는 키로 사용이 종료되면 폐기되는 키이다.
㉢ 비대칭 암호시스템에서 전자서명용 검증키이고, 평문데이터의 암호화용으로 사용한다.

① ㉠: 대칭키, ㉡: 세션키, ㉢: 개인키
② ㉠: 세션키, ㉡: 대칭키, ㉢: 공개키
③ ㉠: 마스터키, ㉡: 세션키, ㉢: 공개키
④ ㉠: 세션키, ㉡: 마스터키, ㉢: 개인키

정답 3번

출제 포인트

마스터키·세션키·공개키를 사용 기간과 비대칭 암호시스템에서의 기능으로 구별하는 문제이다.

핵심 개념

마스터키: 반복적으로 사용되는 상위 핵심키이므로 장기간 안전하게 보관해야 한다.
세션키: 한 번의 통신 세션에서 임시로 사용하고 세션이 끝나면 폐기하는 키이다.
공개키: 비대칭 암호시스템에서 공개하는 키로, 개인키로 만든 전자서명을 검증하고 수신자에게 보낼 평문을 암호화하는 데 사용한다.
개인키: 소유자만 비밀로 보관하며 전자서명을 생성하고, 대응하는 공개키로 암호화된 데이터를 복호화하는 데 사용한다.
대칭키는 암호화와 복호화에 같은 키를 사용하는 키의 방식·범주이므로, 반복 사용 여부만으로 마스터키와 동일시할 수 없다.

NoteBase

선지별 해설

① X
㉠을 대칭키, ㉢을 개인키라고 한 부분이 틀렸다. 반복적으로 사용하는 대표키는 마스터키이고, 전자서명 검증과 평문 암호화에 사용하는 키는 공개키이다. 따라서 올바른 배열은 '㉠ 마스터키, ㉡ 세션키, ㉢ 공개키'이다.

② X
㉠과 ㉡을 서로 잘못 대응시켰다. 반복적으로 사용하여 안전한 보관이 필요한 ㉠은 마스터키이고, 한 번만 사용한 뒤 폐기하는 ㉡은 세션키이다. ㉢을 공개키라고 한 부분만 옳다.

③ O
㉠은 반복 사용되는 마스터키, ㉡은 일회성 통신에 쓰고 폐기하는 세션키, ㉢은 전자서명 검증과 평문 암호화에 쓰는 공개키이므로 세 설명이 모두 정확히 대응한다.

④ X
㉠·㉡·㉢의 대응이 모두 틀렸다. ㉠은 세션키가 아니라 마스터키, ㉡은 마스터키가 아니라 세션키, ㉢은 개인키가 아니라 공개키이다.

오답 포인트

'대표키'라는 표현을 넓은 범주인 대칭키로 오인하거나, 전자서명 생성과 검증의 키를 뒤바꾸기 쉽다. 전자서명은 개인키로 생성하고 공개키로 검증하며, 기밀성 확보를 위한 암호화는 수신자의 공개키로 하고 개인키로 복호화한다.

다시 나오면 이렇게 판단

먼저 사용 기간을 본다. 반복적으로 쓰며 안전하게 보관하는 상위 키는 마스터키이고, 한 세션에서만 쓰고 폐기하는 키는 세션키이다. 비대칭키는 기능을 본다. 서명 검증과 평문 암호화는 공개키, 서명 생성과 암호문 복호화는 개인키이다.

암기 포인트

마스터키는 반복·보관, 세션키는 일회·폐기, 공개키는 서명 검증·암호화이다.

NoteBase

문 20. 해킹 수단과 그 공격 방법에 대한 설명으로 가장 옳지 않은 것은?

① Ransomware : 파일을 암호화한 후 복호화를 조건으로 금전을 요구함

② Rootkit : 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴

③ SQL Injection : 데이터베이스에 질의어를 변조하여 공격함

④ Cross-site Scripting : 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

정답 2번

출제 포인트

이 문제는 대표적인 해킹·공격 수단의 명칭과 실제 공격 방법이 올바르게 연결되었는지를 묻는다.

핵심 개념

랜섬웨어는 파일이나 시스템을 암호화·잠금한 뒤 복구를 대가로 금전을 요구하는 악성 프로그램이다.
루트킷은 공격자가 시스템에서 자신의 존재나 악성 행위를 숨기고 높은 권한의 접근을 유지하도록 하는 도구 또는 악성 코드이다.
SQL 인젝션은 입력값에 악의적인 SQL 구문을 넣어 데이터베이스 질의를 변조하는 공격이다.
크로스 사이트 스크립팅(XSS)은 웹 페이지에 악성 스크립트를 삽입하여 다른 사용자의 브라우저에서 실행되게 하는 공격이다.

선지별 해설

① O — 랜섬웨어는 파일을 암호화하거나 시스템을 잠근 뒤 복호화·복구를 조건으로 금전을 요구한다.
② X — '스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킨다'는 설명은 루트킷이 아니라 스택 기반 버퍼 오버플로 공격에 해당한다. 올바르게는 루트킷은 공격자의 존재와 악성 행위를 숨기고 관리자 권한 등의 접근을 지속하도록 한다.
③ O — SQL 인젝션은 사용자 입력을 통해 SQL 질의문의 구조나 의미를 변조하여 데이터베이스를 비정상적으로 조회·변경하게 한다.
④ O — 크로스 사이트 스크립팅은 웹 페이지에 악성 스크립트를 삽입하고 이를 이용자의 브라우저에서 실행시켜 쿠키나 세션 정보 등을 탈취할 수 있는 공격이다.

오답 포인트

②는 악성 코드를 은닉하는 루트킷과 메모리의 버퍼 크기를 초과해 데이터를 쓰는 버퍼 오버플로를 바꾸어 연결한 선지이다. '스택', '할당된 버퍼보다 큰 코드'가 보이면 버퍼 오버플로를 떠올리는 것이 핵심이다.

NoteBase

다시 나오면 이렇게 판단

공격 명칭을 목적과 수단으로 구분한다. 금전 요구는 랜섬웨어, 은닉·권한 유지는 루트킷, SQL 질의 변조는 SQL 인젝션, 브라우저에서의 악성 스크립트 실행은 XSS, 버퍼 크기 초과 입력은 버퍼 오버플로에 대응한다.

암기 포인트

랜섬웨어는 암호화와 금전 요구, 루트킷은 은닉과 권한 유지, SQL 인젝션은 질의 변조, XSS는 브라우저 스크립트 실행, 버퍼 오버플로는 메모리 범위 초과이다.

NoteBase