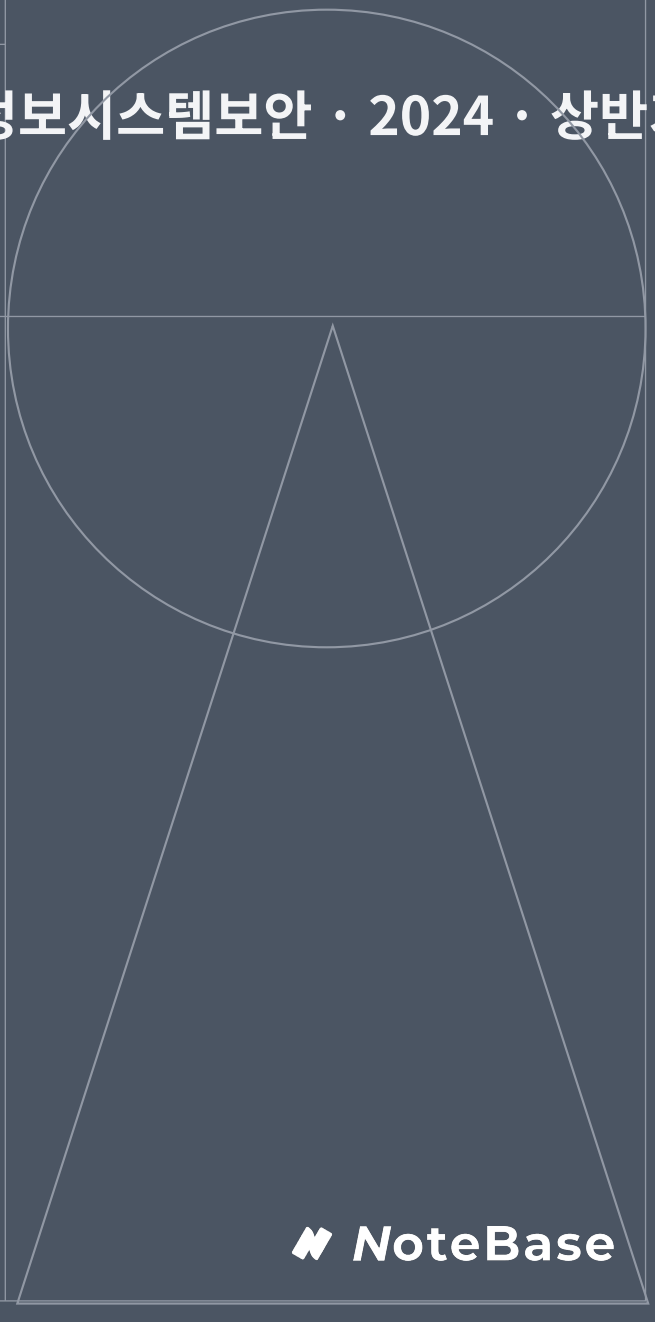
기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2024 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 정보시스템보안 · 2024 · 상반기

공무원/해경/일반직 9급 · 정보시스템보안 · 2024 · 상반기

문 1. 다음 중 암호를 찾기 위하여 가능한 모든 조합을 시도하는 공격기법으로 가장 옳은 것은?

① 무차별(Brute-force) 공격

② 사전(Dictionary) 공격

③ 스미싱(Smishing) 공격

④ 암호 추측(Password Guessing) 공격

정답 1번

출제 포인트

암호 공격 기법을 시도하는 후보의 범위와 생성 방식으로 구별하는 문제이다. 가능한 모든 문자 조합을 빠짐없이 대입하는 공격은 무차별 공격이다.

핵심 개념

무차별 공격: 정해진 문자 집합과 길이에서 만들 수 있는 모든 조합을 체계적으로 시도하는 공격이다. 키워드는 ‘모든 조합’이다.
사전 공격: 사전에 준비한 단어 목록과 그 변형을 암호 후보로 사용하는 공격이다.
스미싱 공격: 문자메시지와 피싱을 결합하여 악성 링크 접속이나 정보 입력을 유도하는 사회공학 공격이다.
암호 추측 공격: 사용자 정보나 흔한 암호 등 성공 가능성이 높아 보이는 후보를 골라 시도하는 공격이다.

선지별 해설

① O — 무차별(Brute-force) 공격은 가능한 모든 조합을 순차적·체계적으로 시도하므로 문제의 설명과 정확히 일치한다.
② X — 사전(Dictionary) 공격은 가능한 모든 조합이 아니라 미리 만든 단어 목록과 흔한 변형을 대입한다. ‘가능한 모든 조합을 시도하는 공격’은 무차별 공격으로 고쳐야 한다.
③ X — 스미싱(Smishing) 공격은 문자메시지의 링크나 안내를 이용해 악성 앱 설치 또는 정보 입력을 유도하는 공격이다. ‘가능한 모든 조합을 시도하는 공격’은 무차별 공격으로 고쳐야 한다.
④ X — 암호 추측(Password Guessing) 공격은 사용자 관련 정보나 흔한 암호처럼 가능성이 높은 후보를 선택해 추측한다. ‘가능한 모든 조합을 시도하는 공격’은 무차별 공격으로 고쳐야 한다.

NoteBase

오답 포인트

②와 ④도 여러 암호를 대입할 수 있어 ①과 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '가능한 모든 조합'이다. 제한된 단어 목록을 쓰면 사전 공격이고, 가능성 높은 후보만 골라 시도하면 암호 추측 공격이다.

다시 나오면 이렇게 판단

공격에 사용하는 후보의 범위를 확인한다. 모든 조합이면 무차별 공격, 단어 목록이면 사전 공격, 개인 정보나 흔한 암호를 바탕으로 선별한 후보이면 암호 추측 공격, 문자메시지로 링크 접속이나 정보 입력을 유도하면 스미싱 공격이다.

암기 포인트

모든 조합은 무차별, 단어 목록은 사전, 유력 후보는 추측, 문자메시지 피싱은 스미싱이다.

NoteBase

문 2. 다음 중 웜(Worm)에 대한 설명으로 가장 옳지 않은 것은?

① 시스템의 취약점을 이용해 자신을 실행시킨다.

② 자신을 복제하여 네트워크 연결을 통해 복제본을 전송한다.

③ 다른 프로그램의 한 유형인 것처럼 가장하여 활동한다.

④ 네트워크 기반 웜 방어가 가능하다.

정답 3번

출제 포인트

웜의 자기 복제·네트워크 전파 특성과 트로이목마의 위장 특성을 구별하는 문제이다.

핵심 개념

웜은 다른 프로그램에 기생하지 않고 스스로 실행·복제하면서 네트워크를 통해 전파되는 악성코드이다.
시스템이나 네트워크 서비스의 취약점을 이용해 침투할 수 있다.
트로이목마는 정상적이거나 유용한 프로그램인 것처럼 가장하여 사용자의 실행을 유도하는 악성코드이다.
웜은 '자기 복제와 네트워크 전파', 트로이목마는 '정상 프로그램으로 위장'이 핵심 구별 기준이다.

선지별 해설

① O — 웜은 운영체제나 네트워크 서비스의 취약점을 이용해 대상 시스템에 침투하고 자신을 실행시킬 수 있다.
② O — 웜은 자신을 복제하며 네트워크 연결을 통해 복제본을 다른 시스템으로 전송·확산한다.
③ X — '다른 프로그램의 한 유형인 것처럼 가장한다'는 부분이 틀렸다. 올바르게는 트로이목마가 정상적이거나 유용한 프로그램인 것처럼 위장하여 활동하며, 웜은 스스로 복제해 네트워크로 전파된다.
④ O — 네트워크 트래픽을 감시하고 웜의 시그니처, 비정상적인 연결 증가, 스캔 행위 등을 탐지·차단하는 침입 탐지·방지 시스템 등으로 네트워크 기반 방어가 가능하다.

오답 포인트

③의 '다른 프로그램인 것처럼 가장한다'는 표현을 웜의 은닉 기능으로 오인하기 쉽다. 그러나 이 표현은 위장을 핵심으로 하는 트로이목마의 특징이고, 웜의 결정적 특징은 자기 복제와 네트워크 전파이다.

다시 나오면 이렇게 판단

선지에서 '자기 복제·네트워크 자동 전파'가 보이면 웜으로, '정상 프로그램으로 위장·사용자의 실행 유도'가 보이면 트로이목마로 판단한다.

암기 포인트

웜은 스스로 복제해 퍼지고, 트로이목마는 정상 프로그램처럼 위장한다.

NoteBase

문 3. 다음 중 윈도우를 설치할 때 기본적으로 생성되는 그룹 설명으로 가장 옳지 않은 것은?

① Users: 개개인에 할당된 사용자 환경을 직접 만들 수 있지만 시스템 서비스의 시작 및 종료 권한이 없다.

② Replicator: 도메인에 있는 파일을 복제할 수 있는 권한을 가지는 그룹이다.

③ Administrators: 도메인 지원이나 로컬 컴퓨터에 대한 모든 권한이 있다.

④ Power Users: 공용 프로그램 그룹 생성 및 컴퓨터의 시계 설정 권한은 있으나 디렉터리나 네트워크 공유 설정 권한은 없다.

정답 4번

출제 포인트

Windows를 설치할 때 기본적으로 생성되는 사용자 그룹별 권한 범위를 구별하는 문제이다.

핵심 개념

Users는 일반적인 작업을 수행하는 표준 사용자 그룹이고, Power Users는 Users보다 넓은 시스템 관리 권한을 가진 그룹이다. Replicator는 도메인의 파일 복제를 지원하는 그룹이며, Administrators는 시스템 전반을 관리하는 최고 권한 그룹이다.
그룹을 구별하는 핵심 기준은 일반 사용, 파일 복제, 전체 관리, 제한적 관리 가운데 어느 범위의 권한이 부여되는지이다.

선지별 해설

① O — Users는 각 사용자에게 할당된 개인 환경을 만들고 사용할 수 있지만, 시스템 서비스를 시작하거나 종료하는 관리 권한은 없다.
② O — Replicator는 도메인 내 파일 복제 기능을 지원하기 위해 사용되는 그룹이다.
③ O — Administrators는 로컬 컴퓨터 또는 도메인을 관리하는 데 필요한 전반적인 권한을 가진다.
④ X — 틀린 부분은 '디렉터리나 네트워크 공유 설정 권한은 없다'이다. Power Users는 공용 프로그램 그룹을 만들고 컴퓨터의 시계를 설정할 수 있을 뿐 아니라, 디렉터리를 공유하고 네트워크 공유를 생성·관리할 수도 있다.

오답 포인트

Power Users가 Administrators보다 권한이 제한된다는 사실을 '공유 설정 권한도 전혀 없다'로 확대하면 ④를 맞는 설명으로 오인하기 쉽다. 제한적 관리자 그룹이라는 말은 모든 관리 기능이 금지된다는 뜻이 아니다.

다시 나오면 이렇게 판단

그룹 이름과 핵심 기능을 연결한다. Users는 일반 사용, Replicator는 파일 복제, Administrators는 전체 관리, Power Users는 일반 사용자보다 넓은 제한적 관리 권한으로 판단한다.

NoteBase

암기 포인트

Users는 일반 사용, Replicator는 복제, Administrators는 전체 관리, Power Users는 공유 설정이 가능한 제한적 관리자이다.

NoteBase

문 4. 다음 중 윈도우 NTFS 디스크 구조에서 볼륨 및 파일시스템에 존재하는 모든 파일과 디렉터리에 대한 정보를 담고 있는 테이블로 가장 옳은 것은?

① MFT(Master File Table)

② VBR(Volume Boot Record)

③ MBR(Master Boot Record)

④ FSINFO(File System Information)

정답 1번

출제 포인트

NTFS에서 파일과 디렉터리의 메타데이터를 관리하는 MFT와 부팅·파티션·FAT32 보조 정보 구조를 구별하는 문제이다.

핵심 개념

MFT(Master File Table)는 NTFS 볼륨의 모든 파일과 디렉터리에 관한 레코드를 저장하는 핵심 메타데이터 테이블이다. 파일명, 크기, 시간 정보, 데이터의 저장 위치 같은 속성이 각 레코드에 기록된다.
VBR은 특정 볼륨의 부팅 정보, MBR은 디스크의 부팅 코드와 파티션 정보, FSINFO는 FAT32의 여유 클러스터 관련 정보를 담는다.

선지별 해설

① O — MFT는 NTFS 볼륨에 존재하는 모든 파일과 디렉터리의 메타데이터 레코드를 관리하는 테이블이므로 문제의 설명에 해당한다.
② X — 틀린 부분은 VBR을 모든 파일과 디렉터리의 정보 테이블로 본 점이다. VBR(Volume Boot Record)은 해당 볼륨의 파일시스템 매개변수와 부팅에 필요한 코드·정보를 담는 영역이다.
③ X — 틀린 부분은 MBR을 NTFS 파일·디렉터리 정보 테이블로 본 점이다. MBR(Master Boot Record)은 디스크 선두에서 부팅 코드와 파티션 테이블을 담는 구조이다.
④ X — 틀린 부분은 FSINFO를 NTFS의 전체 파일·디렉터리 정보 테이블로 본 점이다. FSINFO(File System Information)는 FAT32에서 여유 클러스터 수와 다음 여유 클러스터의 탐색 힌트 등을 저장하는 보조 구조이다.

오답 포인트

MFT, VBR, MBR, FSINFO가 모두 디스크나 파일시스템의 관리 구조라는 점이 함정이다. 문제의 핵심 표현인 ‘NTFS의 모든 파일과 디렉터리에 대한 정보’를 보면 부팅 영역이 아니라 파일별 레코드 테이블인 MFT를 선택한다.

NoteBase

다시 나오면 이렇게 판단

파일·디렉터리별 메타데이터이면 MFT, 볼륨 부팅 정보이면 VBR, 디스크 부팅과 파티션 정보이면 MBR, FAT32의 여유 클러스터 정보이면 FSINFO로 판단한다.

암기 포인트

NTFS의 파일 장부는 MFT, 볼륨 부팅은 VBR, 디스크 부팅·파티션은 MBR, FAT32 여유 공간 힌트는 FSINFO이다.

NoteBase

문 5. 다음 중 사용자 및 그룹 계정에 대한 데이터베이스를 관리하며, 사용자의 로그인 입력 정보와 데이터베이스 정보를 비교하여 인증 여부를 결정하는 윈도우 인증 구성요소로 가장 옳은 것은?

① LSA(Local Security Authority)

② SAM(Security Account Manager)

③ SRM(Security Reference Monitor)

④ NTLM(NT LAN Manager)

정답 2번

출제 포인트

윈도우 보안 구성요소 가운데 로컬 사용자·그룹 계정 데이터베이스를 담당하는 SAM과 LSA, SRM, NTLM의 역할을 구별하는 문제이다.

핵심 개념

SAM(Security Account Manager)은 로컬 사용자와 그룹의 계정 정보 및 인증에 필요한 정보를 보관·관리하는 구성요소이다. 시험에서는 로그인 시 입력된 정보와 SAM 데이터베이스의 계정 정보를 대조하여 로컬 사용자의 인증 여부를 판단하는 역할로 구분한다.
LSA는 로컬 보안 정책과 인증 절차를 관장하고, SRM은 객체 접근 권한을 검사하며, NTLM은 시도-응답 방식의 인증 프로토콜이다.

NoteBase

선지별 해설

① X
LSA(Local Security Authority)는 로컬 보안 정책을 관리하고 로그온 인증 절차를 조정하는 구성요소이다. 틀린 부분은 사용자 및 그룹 계정 데이터베이스를 관리한다는 역할을 LSA에 대응시키는 것이다. 해당 데이터베이스를 관리하는 구성요소는 SAM이다.

② O
SAM(Security Account Manager)은 로컬 사용자 및 그룹 계정 데이터베이스를 관리하며, 로그인 정보와 저장된 계정 정보를 바탕으로 로컬 인증 여부를 판단하는 데 사용된다.

③ X
SRM(Security Reference Monitor)은 사용자가 객체에 접근할 때 접근 토큰과 객체의 보안 정보를 바탕으로 접근 권한을 검사하고 보안 감사를 집행하는 구성요소이다. 틀린 부분은 계정 데이터베이스 관리 기능을 SRM에 대응시킨 것이다. 올바르게는 SRM은 객체 접근 통제를 담당한다.

④ X
NTLM(NT LAN Manager)은 시도-응답 방식으로 사용자를 인증하는 인증 프로토콜이다. 틀린 부분은 NTLM을 사용자·그룹 계정 데이터베이스를 관리하는 구성요소로 본 것이다. 올바르게는 계정 데이터베이스는 SAM이 관리하고, NTLM은 인증 과정에서 사용되는 프로토콜이다.

오답 포인트

①의 LSA도 인증에 관여하므로 SAM과 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '사용자 및 그룹 계정에 대한 데이터베이스를 관리'한다는 부분이며, 이는 SAM을 가리킨다.

다시 나오면 이렇게 판단

계정 데이터베이스는 SAM, 로컬 보안 정책과 인증 절차는 LSA, 객체 접근 권한 검사는 SRM, 시도-응답 인증 방식은 NTLM으로 역할을 나누어 판단한다.

암기 포인트

SAM은 계정 저장, LSA는 보안 정책, SRM은 접근 검사, NTLM은 인증 프로토콜이다.

NoteBase

문 6. 다음 중 윈도우 운영체제의 레지스트리에 대한 설명으로 가장 옳지 않은 것은?

① 레지스트리 편집기로 레지스트리 설정을 열람, 수정, 추가, 삭제할 수 있다.

② HKEY_CLASSES_ROOT(HKCR)에는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 애플리케이션에 대한 맵핑 정보를 저장하고 있다.

③ HKEY_CURRENT_CONFIG(HKCC)에는 소프트웨어 목록과 애플리케이션 이름, 경로, 라이선스 정보 등 환경 설정 정보가 저장되어 있다.

④ HKEY_USERS(HKU)에는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.

정답 3번

출제 포인트

이 문제는 윈도우 레지스트리의 주요 루트 키가 각각 어떤 정보를 저장하는지 구별하는 문제이다.

핵심 개념

레지스트리는 윈도우와 응용 프로그램의 구성 정보를 계층적으로 저장하는 데이터베이스이다. HKCR은 파일 형식과 프로그램 연결 정보, HKU는 사용자별 프로필 설정, HKCC는 현재 사용 중인 하드웨어 프로필 정보를 다룬다. 소프트웨어의 설치·구성 정보는 주로 HKLM\SOFTWARE에 저장된다.

선지별 해설

① O
레지스트리 편집기(regedit)를 이용하면 권한이 허용된 범위에서 레지스트리 키와 값을 열람하고 수정·추가·삭제할 수 있다.

② O
HKCR은 등록된 파일 확장자와 파일 형식, 해당 파일을 열 때 사용할 프로그램의 연결 정보를 제공하므로 옳다.

③ X
틀린 표현은 HKCC에 '소프트웨어 목록과 애플리케이션 이름, 경로, 라이선스 정보 등'이 저장된다는 부분이다. HKCC에는 현재 사용 중인 하드웨어 프로필에 관한 정보가 저장되며, 시스템 전반의 소프트웨어 구성 정보는 주로 HKLM\SOFTWARE에서 관리된다.

④ O
HKU는 시스템에 로드된 사용자 프로필별 설정을 사용자 SID 아래에 저장하는 루트 키이므로, 사용자 계정별 환경 설정을 다루는 키라는 취지에서 옳다. 다만 계정·그룹의 보안 데이터 자체는 HKLM\SAM 영역과 구별된다.

NoteBase

오답 포인트

③은 ‘CURRENT_CONFIG’라는 이름 때문에 현재의 소프트웨어 환경 설정을 저장한다고 오해하게 만든다. 여기서 config는 현재 선택된 하드웨어 프로필을 뜻한다. 또한 ④의 HKU는 사용자별 설정을 담는다는 점과 계정·그룹 보안 데이터의 저장 위치를 구분해야 한다.

다시 나오면 이렇게 판단

루트 키의 이름을 저장 대상과 연결한다. CLASSES_ROOT는 파일 형식·프로그램 연결, USERS는 사용자별 프로필, CURRENT_CONFIG는 현재 하드웨어 프로필로 판단한다. 소프트웨어 설치·구성 정보가 제시되면 HKLM\SOFTWARE를 우선 검토한다.

암기 포인트

HKCR은 파일 연결, HKU는 사용자 프로필, HKCC는 현재 하드웨어 구성이다.

NoteBase

문 7. 다음 중 유닉스 디렉터리 설명으로 가장 옳은 것은?

① /dev: 프로그램 실행 및 설치 시 생성되는 임시 파일을 담고 있다.

② /home: 시스템 최상위 디렉터리이다.

③ /lib: 시스템 로그가 저장되는 디렉터리이다.

④ /etc: 시스템의 환경 설정 및 주요 설정 파일을 담고 있다.

정답 4번

출제 포인트

유닉스의 주요 디렉터리가 각각 어떤 종류의 파일을 저장하는지 구분하는 문제이다.

핵심 개념

/dev는 장치 파일, /home은 일반 사용자의 홈 디렉터리, /lib는 공유 라이브러리와 커널 모듈, /etc는 시스템 설정 파일을 두는 디렉터리이다. 시스템 로그는 일반적으로 /var/log에 저장되고, 임시 파일은 주로 /tmp에 저장된다.

선지별 해설

① X
틀린 표현은 '프로그램 실행 및 설치 시 생성되는 임시 파일'이다. /dev에는 디스크, 터미널 등 하드웨어 장치를 파일처럼 다루기 위한 장치 파일이 저장된다. 임시 파일은 일반적으로 /tmp에 저장된다.

② X
틀린 표현은 '시스템 최상위 디렉터리'이다. /home은 일반 사용자별 홈 디렉터리가 위치하는 곳이다. 시스템 최상위 디렉터리는 /이다.

③ X
틀린 표현은 '시스템 로그가 저장되는 디렉터리'이다. /lib에는 시스템 구동과 명령 실행에 필요한 공유 라이브러리와 커널 모듈 등이 저장된다. 시스템 로그는 일반적으로 /var/log에 저장된다.

④ O
/etc에는 시스템 전반의 환경 설정과 주요 설정 파일이 저장되므로 옳다.

오답 포인트

디렉터리 이름 자체보다 저장 대상의 기능을 연결해야 한다. 특히 /dev를 임시 파일 디렉터리인 /tmp와 혼동하거나, /home을 최상위 디렉터리인 /와 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

장치는 /dev, 사용자 공간은 /home, 라이브러리는 /lib, 설정은 /etc, 로그는 /var/log, 임시는 /tmp로 대응하여 판단한다.

암기 포인트

dev-장치, home-사용자, lib-라이브러리, etc-설정, var/log-로그, tmp-임시 파일이다.

NoteBase

문 8. 다음 중 생체인증의 오인식률과 오거부율에 대한 설명으로 가장 옳은 것은?

① 오인식률이 높으면 허가되어야 할 사람의 차단이 높아진다.

② 오거부율이 높으면 차단되어야 할 사람의 진입이 높아진다.

③ 오인식률과 오거부율간의 상관관계는 나타나지 않는다.

④ 보안 등급을 높여야 할 경우, 상대적으로 오거부율이 높아질 수 있다.

정답 4번

출제 포인트

생체인증의 오인식률과 오거부율이 누구를 잘못 허용하거나 거부하는지를 구별하고, 인증 기준을 엄격하게 할 때 두 비율이 어떻게 변하는지를 묻는 문제이다.

핵심 개념

오인식률은 차단되어야 할 비인가자를 허가된 사람으로 잘못 판단하여 통과시키는 비율이다. 오거부율은 허가되어야 할 정당한 사용자를 비인가자로 잘못 판단하여 차단하는 비율이다. 인증 임계값을 엄격하게 하면 비인가자의 통과 가능성인 오인식률은 낮아지지만, 정당한 사용자까지 거부할 가능성인 오거부율은 높아질 수 있다.

선지별 해설

① X — '오인식률이 높으면 허가되어야 할 사람의 차단이 높아진다'는 부분이 틀렸다. 허가되어야 할 사람의 차단이 높아지는 것은 오거부율이 높은 경우이다. 오인식률이 높으면 차단되어야 할 비인가자의 잘못된 진입이 늘어난다.
② X — '오거부율이 높으면 차단되어야 할 사람의 진입이 높아진다'는 부분이 틀렸다. 차단되어야 할 사람의 진입이 높아지는 것은 오인식률이 높은 경우이다. 오거부율이 높으면 허가되어야 할 정당한 사용자의 차단이 늘어난다.
③ X — '상관관계는 나타나지 않는다'는 부분이 틀렸다. 동일한 인증 시스템에서 임계값을 조정하면 일반적으로 오인식률과 오거부율은 한쪽이 낮아질 때 다른 쪽이 높아지는 상충 관계를 보인다.
④ O — 보안 등급을 높이기 위해 인증 기준을 엄격하게 하면 비인가자의 오인식 통과는 줄어들지만 정당한 사용자도 거부될 가능성이 커지므로 오거부율이 상대적으로 높아질 수 있다.

오답 포인트

①과 ②는 오인식률과 오거부율의 대상을 서로 바꾼 선지이다. ③은 두 오류율이 독립적이라고 오해하게 하지만, 인증 임계값의 조정에 따라 두 비율은 일반적으로 상충한다.

NoteBase

다시 나오면 이렇게 판단

‘비인가자를 통과시킴’은 오인식률, ‘정당한 사용자를 차단함’은 오거부율로 구분한다. 보안 기준을 엄격하게 하면 비인가자의 통과는 줄고 정당한 사용자의 거부는 늘 수 있다고 판단한다.

암기 포인트

오인식은 비인가자를 잘못 허용하고, 오거부는 정당한 사용자를 잘못 차단한다. 보안을 엄격하게 하면 오인식률은 낮아지고 오거부율은 높아질 수 있다.

NoteBase

문 9. 다음 중 시스템 관리와 관련된 보안 기능에서 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대해 관리하는 것으로 가장 옳은 것은?

① 로그 관리

② 세션 관리

③ 권한 관리

④ 취약점 관리

정답 2번

출제 포인트

시스템 보안 관리 기능 가운데 활성화된 접속을 관리하는 기능이 무엇인지 구별하는 문제이다.

핵심 개념

세션 관리는 사용자와 시스템 사이 또는 시스템과 시스템 사이에 성립한 활성 접속의 생성, 유지, 종료 등을 통제하는 기능이다.
로그 관리는 시스템 활동 기록을 수집·보관·점검하고, 권한 관리는 사용자나 계정에 접근 권한을 부여·변경·회수한다. 취약점 관리는 보안상 약점을 발견·평가·조치한다.

선지별 해설

① X — 로그 관리는 접속 자체가 아니라 접속 기록을 포함한 시스템 활동 기록을 수집·보관·점검하는 기능이다. 틀린 표현은 '로그 관리'이며, 활성화된 접속을 관리하는 기능은 '세션 관리'이다.
② O — 세션 관리는 사용자와 시스템 또는 두 시스템 사이에 활성화된 접속 상태를 생성·유지·종료하는 기능이므로 문항의 설명과 일치한다.
③ X — 권한 관리는 사용자나 계정이 어떤 자원에 어떤 행위를 할 수 있는지를 정하는 기능이다. 틀린 표현은 '권한 관리'이며, 활성화된 접속을 관리하는 기능은 '세션 관리'이다.
④ X — 취약점 관리는 시스템의 보안상 약점을 식별·평가하고 보완하는 기능이다. 틀린 표현은 '취약점 관리'이며, 활성화된 접속을 관리하는 기능은 '세션 관리'이다.

오답 포인트

'접속'이라는 말만 보고 접속 기록인 로그나 접속 허용 범위인 권한을 고르기 쉽다. 문항은 이미 활성화된 연결 상태를 관리한다고 했으므로 핵심 단어는 '세션'이다.

다시 나오면 이렇게 판단

기록의 수집·보관은 로그, 연결 상태의 생성·유지·종료는 세션, 자원 이용 범위의 부여·회수는 권한, 보안 약점의 발견·보완은 취약점 관리로 구별한다.

NoteBase

암기 포인트

기록은 로그, 연결은 세션, 허용 범위는 권한, 약점은 취약점이다.

NoteBase

문 10. 다음 중 버퍼오버플로우(Buffer Overflow) 공격에 가장 안전한 C언어 함수로 옳은 것은?

① sscanf()

② strcat()

③ snprintf()

④ vsprintf()

정답 3번

출제 포인트

C 문자열 처리 함수가 목적지 버퍼의 크기를 제한할 수 있는지를 묻는 문제이다.

핵심 개념

버퍼 오버플로우는 프로그램이 확보한 버퍼의 경계를 넘어 데이터를 기록할 때 발생한다. snprintf()는 목적지 버퍼의 전체 크기를 인수로 받아 그 범위 안에서만 출력하므로, 제시된 함수 중 버퍼 오버플로우 방지에 가장 유리하다. 다만 크기 인수를 실제 버퍼 크기에 맞게 전달하고 반환값을 확인해야 잘림 여부도 처리할 수 있다.

선지별 해설

① X — sscanf()는 입력 문자열을 형식에 맞추어 변수에 저장하지만, %s나 %[변환에 최대 필드 폭을 지정하지 않으면 목적지 문자 배열의 크기를 넘길 수 있다. 따라서 sscanf() 자체가 가장 안전한 함수라는 표현은 틀리며, 문자열 입력에는 배열 크기에 맞는 필드 폭을 지정해야 한다.
② X — strcat()는 목적지 문자열 뒤에 원본 문자열을 붙이면서 목적지 버퍼의 남은 크기를 확인하지 않는다. 따라서 strcat()가 안전하다는 표현은 틀리며, 연결 전에 필요한 공간을 검증하고 크기를 제한하는 방식으로 처리해야 한다.
③ O — snprintf()는 버퍼 크기 인수를 받아 기록 가능한 최대 범위를 제한한다. 크기 인수를 올바르게 지정하면 제시된 함수 중 버퍼 오버플로우에 가장 안전하다.
④ X — vsprintf()는 가변 인수 목록을 형식화해 출력하지만 출력 길이를 제한하는 버퍼 크기 인수가 없다. 따라서 vsprintf()가 안전하다는 표현은 틀리며, 크기 제한 인수를 받는 vsnprintf()를 사용해야 한다.

오답 포인트

함수 이름에 n이 들어간다고 언제나 안전한 것은 아니지만, 이 문항에서는 snprintf()의 n이 목적지 버퍼의 전체 크기를 직접 제한한다는 점이 핵심이다. 특히 sscanf()는 읽기 함수처럼 보여도 폭 제한 없는 %s가 버퍼를 넘길 수 있고, vsprintf()는 출력 길이를 제한하지 않는다는 점이 함정이다.

NoteBase

다시 나오면 이렇게 판단

문자열 함수의 안전성을 비교할 때 목적지 버퍼 크기를 함수에 전달하는지와 실제 기록량을 그 크기 이하로 제한하는지를 확인한다. 이 기준에서 snprintf()는 제한 기능이 있고 strcat()와 vsprintf()는 없으며, sscanf()는 변환 지정자에 별도의 폭 제한이 필요하다.

암기 포인트

형식 출력의 버퍼 보호는 크기 제한이 있는 snprintf(), 가변 인수형에서는 vsnprintf()이다.

NoteBase

문 11. 다음 중 정보보호에서 무결성에 대한 설명으로 가장 옳은 것은?

① 정보의 내용이 임의적으로 생성, 변경, 삭제되지 않도록 보호된다.

② 정보에 대한 필요성이 요구될 때, 신속하게 액세스할 수 있다.

③ 정보에 대한 변형이 용이하여 추가 정보의 가공이 간편하다.

④ 인가된 사람만이 정보를 액세스 할 수 있다.

정답 1번

출제 포인트

정보보호의 3요소인 기밀성, 무결성, 가용성의 정의를 구별하는 문제이다.

핵심 개념

무결성은 정보가 인가되지 않거나 임의적인 방식으로 생성·변경·삭제되지 않고 정확하고 완전한 상태로 유지되는 성질이다.
기밀성은 인가된 사람만 정보에 접근할 수 있게 하는 성질이고, 가용성은 인가된 사용자가 필요할 때 정보와 시스템을 사용할 수 있게 하는 성질이다.

선지별 해설

① O — 정보가 임의적으로 생성·변경·삭제되지 않도록 보호한다는 설명은 정보의 정확성과 완전성을 지키는 무결성에 해당한다.
② X — 틀린 표현은 이를 무결성의 설명으로 본 부분이다. 필요할 때 신속하게 접근할 수 있다는 것은 가용성이다. 올바르게는 '인가된 사용자가 필요한 때 정보와 시스템에 접근하여 사용할 수 있다'이다.
③ X — 틀린 표현은 '정보에 대한 변형이 용이하다'이다. 변형의 편의성은 정보보호의 무결성을 뜻하지 않는다. 올바르게는 '정보가 인가되지 않거나 임의적인 방식으로 변경·삭제되지 않고 정확하고 완전하게 유지된다'이다.
④ X — 틀린 표현은 이를 무결성의 설명으로 본 부분이다. 인가된 사람만 정보에 접근할 수 있다는 것은 기밀성이다. 올바르게는 '정보는 인가된 사람에게만 공개되고 접근이 허용된다'이다.

오답 포인트

②의 '필요할 때 접근'은 가용성, ④의 '인가된 사람만 접근'은 기밀성이다. 접근이라는 공통 표현만 보고 판단하면 두 개념을 무결성과 혼동하기 쉽다. ③의 '변형이 용이'는 무결성과 반대로 정보의 임의 변경을 허용하는 취지이므로 오답이다.

다시 나오면 이렇게 판단

변경·삭제 방지와 정확성·완전성은 무결성, 허가된 사람만 접근은 기밀성, 필요할 때 사용 가능은 가용성으로 구별한다.

NoteBase

암기 포인트

기밀성은 허가된 사람만, 무결성은 변조 없이 정확하게, 가용성은 필요할 때 사용 가능이다.

NoteBase

문 12. 다음 중 디지털 컨텐츠의 보호에 관련된 설명으로 가장 옳지 않은 것은?

① 스테가노그래피(Steganography)는 공개된 컨텐츠에 기밀 메시지를 은폐, 전달하기 위한 방법이다.

② 디지털 워터마킹은 디지털 컨텐츠에 저작권 데이터를 부가, 컨텐츠 권리에 대한 행사를 위한 방법이다.

③ 핑거프린팅은 컨텐츠의 배포 경로에 따른 구매자를 추적하기 위한 목적으로, 컨텐츠에 따라 구분되는 정보가 부가된 방법이다.

④ DRM은 컨텐츠에 대한 구매자의 익명성을 보장, 구매자에 대한 역추적을 막으려는 방법이다.

정답 4번

출제 포인트

디지털 콘텐츠 보호 기술인 스테가노그래피, 디지털 워터마킹, 핑거프린팅, DRM의 목적과 기능을 구별하는 문제이다.

핵심 개념

스테가노그래피: 공개된 이미지·음성 등의 매체 안에 비밀 메시지를 숨겨 메시지의 존재 자체를 알아보기 어렵게 하는 기술이다. / 키워드: 기밀 메시지 은폐
디지털 워터마킹: 디지털 콘텐츠에 저작권자나 소유권 정보를 삽입하여 권리 주장과 불법 복제 확인 등에 활용하는 기술이다. / 키워드: 저작권 정보
핑거프린팅: 배포되는 콘텐츠 사본마다 구매자나 수신자를 식별할 수 있는 정보를 삽입하여 유출자를 추적하는 기술이다. / 키워드: 구매자별 식별·추적
DRM: 암호화와 이용 권한·라이선스 관리를 통해 디지털 콘텐츠의 접근, 복제, 사용 및 배포를 통제하는 기술이다. / 키워드: 사용 권한 통제

선지별 해설

① O — 스테가노그래피는 겉으로 공개된 콘텐츠에 기밀 메시지를 숨겨 전달하는 방법이므로 옳다.
② O — 디지털 워터마킹은 콘텐츠에 저작권·소유권 정보를 삽입하여 권리 주장과 불법 이용 확인에 활용하므로 옳다.
③ O — 핑거프린팅은 배포 사본에 구매자별로 구분되는 식별 정보를 넣어 불법 유출이 발생했을 때 구매자나 배포 경로를 추적하는 방법이므로 옳다.
④ X — 틀린 표현은 '구매자의 익명성을 보장, 구매자에 대한 역추적을 막으려는 방법'이다. DRM은 구매자의 익명성을 보장하는 기술이 아니라 콘텐츠의 접근·복제·사용·배포 권한을 통제하여 저작권자의 권리를 보호하는 기술이다.

NoteBase

오답 포인트

④는 DRM을 프라이버시 보호 기술처럼 설명한 것이 함정이다. DRM의 중심 목적은 구매자의 익명성 보장이 아니라 권리자가 정한 이용 조건과 권한을 기술적으로 집행하는 데 있다.

다시 나오면 이렇게 판단

숨기는 대상과 통제 대상을 기준으로 구별한다. 메시지의 존재를 숨기면 스테가노그래피, 저작권 정보를 넣으면 워터마킹, 구매자별 정보를 넣어 유출자를 찾으면 핑거프린팅, 콘텐츠 이용 권한을 통제하면 DRM이다.

암기 포인트

스테가노그래피는 메시지 은폐, 워터마킹은 저작권 표시, 핑거프린팅은 구매자 추적, DRM은 이용 권한 통제이다.

NoteBase

문 13. 다음 중 유닉스 시스템의 로그 파일에서 FTP 파일을 전송한 날짜와 시간, 접근 시스템의 IP를 확인할 수 있는 것으로 가장 옳은 것은?

① xferlog

② utmp

③ wtmp

④ pacct

정답 1번

출제 포인트

유닉스 시스템의 주요 로그 파일이 각각 어떤 활동을 기록하는지 구별하는 문제이다. FTP 파일 전송 시각과 원격 시스템의 IP 주소는 xferlog에서 확인한다.

핵심 개념

xferlog: FTP를 통한 파일 송수신 내역을 기록하는 로그이다. 전송 날짜와 시간, 원격 호스트, 전송 파일 등의 정보가 핵심이다.
utmp: 현재 시스템에 로그인해 있는 사용자의 세션 정보를 기록한다.
wtmp: 사용자의 로그인·로그아웃과 시스템 부팅·종료 등의 이력을 누적하여 기록한다.
pacct: 프로세스 계정 정보를 기록하며, 실행된 명령과 프로세스의 자원 사용 내역 등을 확인하는 데 쓰인다.

선지별 해설

① O — xferlog는 FTP 파일 전송 기록을 남기므로 전송 날짜와 시간, 접근한 원격 시스템의 IP 주소를 확인할 수 있다.
② X — utmp는 FTP 전송 내역이 아니라 현재 로그인 중인 사용자와 터미널 등의 세션 정보를 기록한다. 틀린 표현은 ‘FTP 파일을 전송한 날짜와 시간, 접근 시스템의 IP를 확인’한다는 부분이며, 올바르게는 ‘현재 로그인한 사용자의 세션 정보를 확인’한다고 해야 한다.
③ X — wtmp는 FTP 전송 전용 로그가 아니라 로그인·로그아웃 및 시스템 부팅·종료 이력을 누적한 로그이다. 틀린 표현은 ‘FTP 파일 전송 정보를 확인’한다는 부분이며, 올바르게는 ‘사용자의 로그인·로그아웃 이력을 확인’한다고 해야 한다.
④ X — pacct는 FTP 전송 내역이 아니라 실행된 프로세스에 관한 계정 정보를 기록한다. 틀린 표현은 ‘FTP 파일 전송 정보를 확인’한다는 부분이며, 올바르게는 ‘실행된 명령과 프로세스의 자원 사용 내역을 확인’한다고 해야 한다.

NoteBase

오답 포인트

utmp와 wtmp는 이름이 비슷하지만 utmp는 현재 로그인 상태, wtmp는 로그인·로그아웃의 누적 이력이다. 문제의 결정적 표현은 ‘FTP 파일 전송’이므로 사용자 접속 로그가 아니라 xferlog를 선택한다.

다시 나오면 이렇게 판단

파일 전송은 xferlog, 현재 로그인 사용자는 utmp, 로그인·로그아웃 이력은 wtmp, 실행 프로세스의 계정 정보는 pacct로 연결하여 판단한다.

암기 포인트

xfer는 전송, u는 현재 사용자, w는 접속 이력, pacct는 프로세스 계정이다.

NoteBase

문 14. 다음 중 암호화 알고리즘에서 키의 공개 또는 비공개 형태가 동일하게 짝지어진 것으로 가장 옳은 것은?

① AES, RSA

② RSA, ECC

③ DES, RSA

④ AES, ECC

정답 2번

출제 포인트

AES·DES가 비밀키(대칭키) 암호 알고리즘이고 RSA·ECC가 공개키(비대칭키) 암호 알고리즘이라는 분류를 묻는 문제이다.

핵심 개념

비밀키 암호: 암호화와 복호화에 동일한 비밀키를 사용하는 방식이며 AES와 DES가 해당한다.
공개키 암호: 공개키와 개인키라는 서로 다른 키의 쌍을 사용하는 방식이며 RSA와 ECC가 해당한다.

선지별 해설

① X — AES는 비밀키 암호이지만 RSA는 공개키 암호이므로 키 형태가 다르다. 동일한 형태끼리 짝지으려면 'AES, RSA'가 아니라 'AES, DES'가 되어야 한다.
② O — RSA와 ECC는 모두 공개키와 개인키의 쌍을 사용하는 공개키 암호 알고리즘이다.
③ X — DES는 비밀키 암호이지만 RSA는 공개키 암호이므로 키 형태가 다르다. 동일한 형태끼리 짝지으려면 'DES, RSA'가 아니라 'DES, AES'가 되어야 한다.
④ X — AES는 비밀키 암호이지만 ECC는 공개키 암호이므로 키 형태가 다르다. 동일한 형태끼리 짝지으려면 'AES, ECC'가 아니라 'AES, DES'가 되어야 한다.

오답 포인트

RSA와 ECC도 각각 개인키를 사용한다는 점 때문에 '비공개 형태'로 오해하기 쉽다. 분류 기준은 개인키의 존재 여부가 아니라 하나의 비밀키를 공유하는지, 공개키와 개인키의 쌍을 사용하는지이다.

다시 나오면 이렇게 판단

알고리즘을 AES·DES와 RSA·ECC의 두 묶음으로 먼저 나눈다. 앞의 묶음은 비밀키 암호이고 뒤의 묶음은 공개키 암호이므로, 같은 묶음 안에서 짝지어진 선지를 고른다.

암기 포인트

AES·DES는 비밀키, RSA·ECC는 공개키이다.

NoteBase

문 15. 다음 중 암호 분석가가 취득한 정보를 이용한 암호 분석으로 가장 옳지 않은 것은? (단, 사용된 키는 변하지 않는다고 가정한다.)

① 암호 알고리즘, 해독할 암호문을 취득하였다면, 암호문 단독(Ciphertext Only) 방법으로 공격한다.

② 암호 알고리즘, 해독할 암호문, 임의의 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문을 알고 있다면, 기지 평문(Known Plaintext) 방법으로 공격한다.

③ 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문을 얻을 수 있다면, 선택 평문(Chosen Plaintext) 방법으로 공격한다.

④ 암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 수정된 평문, 암호문에 사용된 키로 생성한 각각의 암호문을 알고 있다면, 선택 암호문(Chosen Ciphertext) 방법으로 공격한다.

정답 4번

출제 포인트

암호 분석가가 확보하거나 선택할 수 있는 평문·암호문의 종류에 따라 암호문 단독 공격, 기지 평문 공격, 선택 평문 공격, 선택 암호문 공격을 구별하는 문제이다.

핵심 개념

암호문 단독 공격: 암호 알고리즘과 암호문만을 이용하여 평문이나 키를 추정하는 공격이다.
기지 평문 공격: 공격자가 이미 알고 있는 평문과 그에 대응하는 암호문 쌍을 이용하는 공격이다.
선택 평문 공격: 공격자가 원하는 평문을 선택하고, 같은 키로 암호화된 대응 암호문을 얻어 분석하는 공격이다.
선택 암호문 공격: 공격자가 원하는 암호문을 선택하고, 그에 대응하는 복호 평문을 얻어 분석하는 공격이다.
구별 기준은 공격자가 선택하는 대상과 그 결과로 얻는 정보이다. 평문을 선택하여 암호문을 얻으면 선택 평문 공격이고, 암호문을 선택하여 평문을 얻으면 선택 암호문 공격이다.

NoteBase

선지별 해설

① O
암호 알고리즘과 해독 대상 암호문만 확보한 상황이므로 암호문 단독 공격에 해당한다.

② O
어떤 평문과 그 평문을 동일한 키로 암호화한 대응 암호문을 이미 알고 있으므로 기지 평문 공격에 해당한다. 여기서 평문은 공격자가 암호화를 요청하여 선택한 것이 아니라 이미 알려진 평문이다.

③ O
암호 분석가가 평문을 선택하고 그 평문을 동일한 키로 암호화한 암호문을 얻을 수 있으므로 선택 평문 공격에 해당한다.

④ X
틀린 표현은 '선택 암호문 방법'이다. 공격자가 평문과 수정된 평문을 선택한 뒤 각각의 대응 암호문을 얻는 것은 선택 평문 공격의 형태이며, 관련 평문 쌍과 암호문 쌍의 차이를 이용하면 차분 암호 분석에 활용할 수 있다. 선택 암호문 공격이라고 하려면 공격자가 암호문을 선택하고 그에 대응하는 복호 평문을 얻을 수 있어야 한다.

오답 포인트

④에는 '수정된 평문'과 '각각의 암호문'이 제시되어 있어 복잡해 보이지만, 공격자가 선택한 대상은 여전히 평문이다. 선택한 입력이 평문인데 이를 선택 암호문 공격으로 부른 부분이 함정이다.

다시 나오면 이렇게 판단

공격자가 무엇을 선택하고 무엇을 돌려받는지를 확인한다. 평문을 선택하고 암호문을 얻으면 선택 평문 공격, 암호문을 선택하고 복호 평문을 얻으면 선택 암호문 공격으로 판단한다. 이미 알려진 평문·암호문 쌍만 이용하면 기지 평문 공격이다.

암기 포인트

평문 선택→암호문 획득은 선택 평문, 암호문 선택→평문 획득은 선택 암호문이다.

NoteBase

문 16. 다음 중 생체인증 기술의 평가 요건으로 가장 옳지 않은 것은?

① 보편성은 일반적인 사람이 가지고 있는 보편적인 특성을 의미한다.

② 지속성은 시간의 흐름에 따라 변하지 않는 특성을 지속함을 의미한다.

③ 획득성은 악의적인 방법으로 복제하기 어려운 성질인가를 의미한다.

④ 수용성은 사용자의 거부감이 없는 성질인가를 의미한다.

정답 3번

출제 포인트

생체인증 특성의 평가 요건인 보편성, 지속성, 획득성, 수용성의 의미를 구별하는 문제이다.

핵심 개념

보편성은 대부분의 사람이 해당 생체 특성을 가지고 있어야 한다는 성질이다. 지속성은 그 특성이 시간의 흐름에도 충분히 안정적으로 유지되어야 한다는 성질이다. 획득성은 생체 특성을 센서로 측정하여 정량적인 데이터로 수집할 수 있어야 한다는 성질이다. 수용성은 사용자가 생체정보의 측정과 인증 절차를 거부감 없이 받아들일 수 있어야 한다는 성질이다. 위조하거나 시스템을 속이기 어려운지는 획득성이 아니라 위조·기만에 대한 저항성과 관련된다.

선지별 해설

① O — 보편성은 인증 대상이 되는 일반적인 사람들에게 해당 생체 특성이 널리 존재하는지를 뜻한다.
② O — 지속성은 생체 특성이 시간의 경과에 따라 쉽게 변하지 않고 유지되는지를 뜻한다.
③ X — 틀린 부분은 '악의적인 방법으로 복제하기 어려운 성질'이 획득성이라는 설명이다. 획득성은 생체 특성을 센서로 측정하고 데이터로 수집할 수 있는 성질이며, 복제나 기만의 어려움은 위조·기만에 대한 저항성과 관련된다.
④ O — 수용성은 생체정보를 제공하고 인증받는 방식에 대해 사용자가 느끼는 거부감이 적은지를 뜻한다.

오답 포인트

③의 '획득'이라는 말을 공격자가 생체정보를 복제하여 얻는다는 뜻으로 오해하기 쉽다. 여기서 획득성은 인증 시스템이 생체 특성을 측정·수집할 수 있다는 의미이다.

다시 나오면 이렇게 판단

평가 요건을 묻는 경우 보편성은 존재 여부, 지속성은 시간에 따른 안정성, 획득성은 측정·수집 가능성, 수용성은 사용자의 거부감 여부로 대응시킨다. 복제나 속임수에 대한 내용은 위조·기만 저항성으로 구분한다.

NoteBase

암기 포인트

보편성은 모두에게, 지속성은 오래도록, 획득성은 측정 가능, 수용성은 거부감 없음이다.

NoteBase

문 17. 다음 중 해시함수의 성질에 관련된 것으로 가장 옳지 않은 것은?

① 데이터에 대해 해시함수를 적용한 결과는 원 데이터에 나타나는 단어 빈도에 따라 불균일한 분포로 나타난다.

② 역상 저항성이란 해시함수를 적용한 결과로 원 데이터를 계산상 찾아내기 어려운 것이다.

③ 약한 충돌 저항성은 해시함수를 적용한 결과로 동일한 해시 결과값을 갖는 데이터를 계산상 찾아내기 어려운 것이다.

④ 강한 충돌 저항성은 해시함수를 적용한 결과가 같은 값이 되는 원 데이터쌍을 찾는 것이 계산상 찾아내기 어려운 것이다.

정답 1번

출제 포인트

암호학적 해시함수의 출력 분포와 역상 저항성·약한 충돌 저항성·강한 충돌 저항성의 구별을 묻는 문제이다.

핵심 개념

암호학적 해시함수는 임의 길이의 데이터를 고정 길이의 해시값으로 변환하며, 입력의 통계적 특징과 뚜렷한 상관관계가 없도록 해시값을 전체 출력 공간에 고르게 분산시키는 성질이 요구된다.
역상 저항성: 주어진 해시값으로부터 그 해시값을 만드는 원 데이터를 찾기 어려운 성질이다.
약한 충돌 저항성(제2역상 저항성): 주어진 원 데이터와 같은 해시값을 갖는 다른 데이터를 찾기 어려운 성질이다.
강한 충돌 저항성: 같은 해시값을 갖는 서로 다른 임의의 데이터쌍을 찾기 어려운 성질이다.

선지별 해설

① X — 틀린 표현은 '원 데이터에 나타나는 단어 빈도에 따라 불균일한 분포'이다. 올바르게는 입력 데이터의 단어 빈도 같은 통계적 특징과 관계없이 해시값이 전체 출력 공간에 고르게 분포하도록 설계된다. 따라서 이 선지가 가장 옳지 않다.
② O — 역상 저항성은 해시값이 주어졌을 때 그 값을 만드는 원 데이터를 계산상 찾아내기 어려운 성질이다.
③ O — 약한 충돌 저항성은 특정 원 데이터가 주어졌을 때 이와 동일한 해시값을 갖는 다른 데이터를 계산상 찾기 어려운 성질이다. '주어진 원 데이터'를 기준으로 다른 데이터를 찾는다는 점이 핵심이다.
④ O — 강한 충돌 저항성은 해시값이 같은 서로 다른 원 데이터쌍을 임의로 찾는 것이 계산상 어려운 성질이다.

오답 포인트

입력 문서의 단어 빈도와 해시 출력의 분포를 연결하는 ①의 표현이 함정이다. 암호학적 해시함수의 출력은 입력의 빈도 특성을 그대로 반영하지 않는다. 또한 ③은 특정 원 데이터가 먼저 주어지고, ④는 조건 없이 충돌하는 데이터쌍을 찾는다는 차이가 있다.

NoteBase

다시 나오면 이렇게 판단

무엇이 먼저 주어지는지를 확인한다. 해시값이 주어지면 역상 저항성, 특정 원 데이터가 주어지면 약한 충돌 저항성, 아무 데이터도 정해지지 않은 상태에서 같은 해시값의 데이터쌍을 찾으면 강한 충돌 저항성이다. 출력 분포는 입력의 빈도와 무관하게 고른지가 판단 기준이다.

암기 포인트

해시값→원 데이터는 역상, 원 데이터→같은 해시의 다른 데이터는 약한 충돌, 같은 해시의 임의 데이터쌍은 강한 충돌이다.

NoteBase

문 18. 다음 중 공개키 기반 구조(PKI)에 관한 내용으로 가장 옳지 않은 것은?

① 정책승인기관(PAA)은 PKI의 전반적인 정책과 절차를 생성하고 루트 CA 역할을 수행한다.

② 정책인증기관(PCA)은 인증기관과 먼 사용자를 위하여 인증기관 대신 인증서 신청의 신분과 소속을 확인한다.

③ 저장소는 인증서와 사용자 관련정보, 인증서, 인증서 취소 목록을 저장, 검색하는 장소이다.

④ 인증기관(CA)은 공개키 인증서를 발급, 취소하며, 인증서/인증서 취소 목록을 관리한다.

정답 2번

출제 포인트

공개키 기반 구조(PKI)를 구성하는 정책승인기관(PAA), 정책인증기관(PCA), 등록기관(RA), 인증기관(CA), 저장소의 역할을 구별하는 문제이다.

핵심 개념

PAA는 PKI의 최상위 정책을 정하고 전체 신뢰체계의 기준을 승인하는 기관이다.
PCA는 PAA의 정책 아래에서 인증기관의 정책을 승인·관리하고 인증기관을 인증하는 정책 관리 기관이다.
RA는 인증서 신청자의 신원과 소속을 확인하여 CA의 등록 업무를 대행하는 기관이다.
CA는 공개키 인증서를 발급·취소하고 인증서와 인증서 취소 목록을 관리하는 기관이다.
저장소는 인증서, 인증서 취소 목록 및 관련 정보를 저장하고 이용자가 검색할 수 있게 하는 공개 디렉터리이다.

선지별 해설

① O — PAA는 PKI 전반의 정책과 절차를 수립·승인하고 최상위 신뢰점인 루트 CA의 역할을 수행한다.
② X — 틀린 표현은 '정책인증기관(PCA)'이다. 인증서 신청자의 신원과 소속을 확인하여 CA의 등록 업무를 대신하는 기관은 등록기관(RA)이다. PCA는 인증기관의 정책을 승인·관리하고 인증기관을 인증한다.
③ O — 저장소는 인증서, 인증서 취소 목록과 이용자 관련 정보를 보관하고 이를 검색·조회할 수 있게 한다.
④ O — CA는 공개키 인증서를 발급하고 필요하면 취소하며, 인증서와 인증서 취소 목록을 관리·공표한다.

오답 포인트

②는 PCA와 RA의 역할을 바꾸어 놓았다. '정책을 관리하고 CA를 인증'하면 PCA이고, '신청자의 신원·소속을 확인'하면 RA이다.

다시 나오면 이렇게 판단

정책의 최상위 승인·루트 역할은 PAA, CA의 정책 인증·관리는 PCA, 신청자 신원 확인은 RA, 인증서 발급·취소는 CA, 인증서와 취소 목록의 저장·검색은 저장소로 구분한다.

NoteBase

암기 포인트

PAA는 최상위 정책, PCA는 CA 정책, RA는 신청자 확인, CA는 인증서 발급·취소, 저장소는 보관·검색이다.

NoteBase

문 19. 다음 중 난수에 관련된 것으로 가장 옳게 설명한 것은?

① 무작위성, 예측 불가능성, 재현 불가능성, 복제 유지성이 난수의 성질이다.

② 생성된 난수는 가능한 범위 전체 중 중앙값에 높은 빈도로 나타난다.

③ 의사난수에서 종자(Seed)값이 유출될 경우 예측 가능해진다.

④ 어떤 순간에 생성한 난수값에 의하여 다음 생성될 난수 값이 결정된다.

정답 3번

출제 포인트

난수의 통계적 성질과 결정적 알고리즘으로 생성되는 의사난수의 예측 가능성을 구별하는 문제이다.

핵심 개념

난수는 각 값이 편향되지 않게 나타나고 앞선 값으로 다음 값을 예측하기 어려워야 하는 수열이다. 핵심 성질은 균일성과 독립성이다.
의사난수는 결정적 알고리즘이 종자(Seed)를 초기값으로 사용하여 만드는 수열이다. 같은 알고리즘에 같은 종자를 넣으면 같은 수열이 재현되므로, 종자가 유출되면 이후의 값도 예측될 수 있다.

선지별 해설

① X — 난수의 일반적인 핵심 성질은 균일성과 독립성이고, 보안 목적에서는 예측 불가능성도 요구된다. 틀린 표현은 '복제 유지성'이다. 올바르게는 의사난수가 같은 종자에서 같은 수열을 재현할 수 있다고 해야 한다.
② X — 생성값이 중앙값 부근에 더 자주 나타나면 편향된 분포이다. 틀린 표현은 '중앙값에 높은 빈도로 나타난다'이다. 올바르게는 각 값 또는 각 비트가 가능한 범위에서 특정 값에 치우치지 않고 균일하게 나타나야 한다.
③ O — 의사난수 생성기는 종자와 알고리즘에 따라 수열이 결정된다. 따라서 알고리즘이 알려진 상태에서 종자가 유출되면 같은 수열을 재현하여 값을 예측할 수 있다.
④ X — 독립적인 난수에서는 앞서 생성된 난수값 자체가 다음 난수값을 결정하지 않는다. 틀린 표현은 '생성한 난수값에 의하여 다음 값이 결정된다'이다. 의사난수의 다음 값은 단순히 직전 출력값 때문이라기보다 생성기의 내부 상태와 알고리즘에 의해 결정된다고 고쳐야 한다.

오답 포인트

의사난수가 결정적이라는 사실을 '직전 출력값이 다음 출력값을 직접 결정한다'는 뜻으로 바꾸면 안 된다. 결정의 기준은 외부에 보이는 직전 난수값이 아니라 종자에서 시작해 갱신되는 내부 상태와 생성 알고리즘이다.

NoteBase

다시 나오면 이렇게 판단

난수의 품질은 값의 편향 여부와 값들 사이의 독립성으로 판단하고, 의사난수의 보안은 종자나 내부 상태가 노출되었을 때 수열을 재현·예측할 수 있는지로 판단한다.

암기 포인트

난수는 균일·독립, 의사난수는 같은 종자이면 같은 수열이다.

NoteBase

문 20. 다음 중 Diffie-Hellman 키 교환 알고리즘에 관련된 내용으로 가장 옳지 않은 것은?

① 공개키 암호화 방식에 대한 알고리즘이다.

② 중간자 공격 방법에 대해 강하다.

③ 유한체상의 이산대수 문제 해결의 어려움에 기반한다.

④ 공개키는 평문을 암호화하기 위해 사용되는 키로써 배포 가능하다.

정답 2번

출제 포인트

Diffie-Hellman 키 교환의 목적, 수학적 기반, 공개값의 성격과 중간자 공격 취약성을 구별하는 문제이다.

핵심 개념

Diffie-Hellman은 공개된 통신로에서 두 참여자가 같은 공유 비밀을 합의하도록 하는 공개키 기반의 키 교환 알고리즘이다. 유한체에서의 이산대수 문제를 풀기 어렵다는 성질에 안전성의 기반을 두지만, 기본 방식 자체는 상대방의 신원을 인증하지 않는다. 따라서 공격자가 양쪽 사이에서 각각 별도의 키를 합의하는 중간자 공격을 막으려면 인증서, 전자서명 등의 인증 수단을 함께 사용해야 한다.

선지별 해설

① O — Diffie-Hellman은 공개키 암호 기술에 속하는 키 교환 알고리즘이다. 엄밀히 말하면 메시지를 직접 암호화하는 알고리즘이 아니라, 암호화에 사용할 공유 비밀키를 합의하는 알고리즘이다.
② X — 틀린 표현은 '중간자 공격 방법에 대해 강하다'이다. 인증 기능이 없는 기본 Diffie-Hellman은 공격자가 두 당사자 사이에 끼어 각 당사자와 따로 키를 교환하는 중간자 공격에 취약하다. 올바르게는 '인증서나 전자서명 등으로 상대방을 인증하지 않은 Diffie-Hellman은 중간자 공격에 취약하다'이다.
③ O — 고전적인 유한체 기반 Diffie-Hellman의 안전성은 유한체의 곱셈군에서 이산대수를 계산하기 어렵다는 점에 기반한다. 공개된 값만으로 비밀 지수를 현실적인 시간 안에 구하기 어렵다는 성질을 이용한다.
④ O — 공개키 방식에서는 공개키를 다른 사람에게 배포할 수 있고, 일반적인 공개키 암호에서는 수신자의 공개키가 평문 암호화에 사용된다. Diffie-Hellman에서는 배포된 공개값을 평문에 직접 적용하기보다 상대방과 공유 비밀을 계산하는 데 사용한다.

오답 포인트

공격자가 비밀 지수를 계산하기 어렵다는 사실과 통신 상대의 신원이 보장된다는 사실을 혼동하기 쉽다.
이산대수 문제의 어려움은 도청만으로 비밀을 알아내는 것을 어렵게 하지만, 기본 Diffie-Hellman에 상대 인증 기능을 부여하지는 않는다.

NoteBase

다시 나오면 이렇게 판단

Diffie-Hellman 관련 선지는 '키 교환', '이산대수 문제', '상대 인증 여부'를 차례로 확인한다. 키 교환과 이산대수 기반은 맞는 특징이고, 별도의 인증 없이 중간자 공격에 강하다는 설명은 틀린 설명이다.

암기 포인트

Diffie-Hellman은 키는 합의하지만 상대방의 신원까지 인증하지는 않는다. 기본 DH는 중간자 공격에 취약하다.

NoteBase