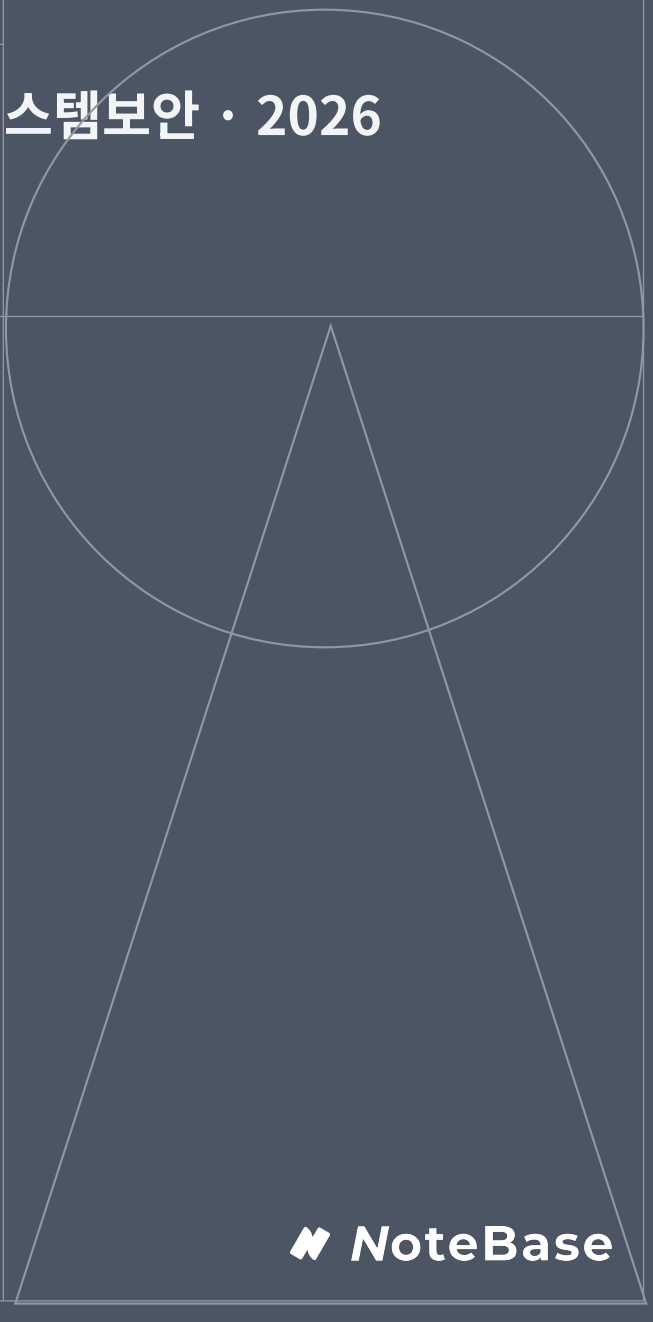
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2026



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2026

공무원/국가직/9급 · 정보시스템보안 · 2026

문 1. 보안 운영체제(Secure OS)에 대한 설명으로 옳지 않은 것은?

① 보안 커널은 접근 제어 및 감사 추적을 위한 메커니즘을 포함하고 있다.

② 패스워드의 설정 및 접근 허용의 변경 등과 같은 보안 관련 작업의 안전한 수행을 위해 안전한 경로(trusted path)를 제공한다.

③ TCB(Trusted Computing Base) 분할은 TCB를 계층화 구조로 구현하고, 각 계층은 고유의 보안 정책을 정의하기 때문에 기존의 TCB를 재사용할 수 없다.

④ 운영체제에 내재된 결함 때문에 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위해 보안 기능이 통합된 보안 커널을 추가로 이식한 운영체제이다.

정답 3번

간단한 해설

③의 '기존의 TCB를 재사용할 수 없다'는 설명이 잘못되었다. TCB 분할은 계층별로 보안 정책을 집행하도록 구성하여, **기존 TCB를 재사용하면서 보안 기능을 확장**할 수 있게 한다.

NoteBase

선지별 해설

① O: 보안 커널은 시스템의 보안 정책을 집행하는 핵심 부분이다. 접근 제어 메커니즘으로 사용자나 프로세스의 자원 접근 권한을 검사하고, **감사 추적** 메커니즘으로 접근 시도와 보안 관련 사건을 기록하여 사후에 행위를 추적할 수 있게 한다.

② O: 안전한 경로는 **사용자와 TCB 사이의 보호된 통신 경로**이다. 신뢰할 수 없는 프로그램이 이를 사칭하거나 통신에 개입하지 못하게 하여, 패스워드 설정이나 접근 권한 변경 같은 민감한 보안 작업을 실제 보안 기능과 안전하게 수행하도록 한다.

③ X: TCB는 보안 정책을 집행하는 하드웨어·펌웨어·소프트웨어 등 보호 메커니즘의 전체이다. TCB 분할은 이를 계층으로 나누어 각 계층이 맡은 보안 정책을 집행하도록 하는 방식이다. 상위 계층은 하위 계층이 제공하는 보호 기능을 이용하고 그 정책의 제약을 받으므로, **기존 TCB를 재사용하면서 새로운 계층을 추가**할 수 있다. 따라서 '재사용할 수 없다'는 '재사용할 수 있다'로 고쳐야 한다.

④ O: 보안 운영체제는 운영체제 수준에서 보안 정책을 집행하도록 보안 기능을 통합한 운영체제이다. 기존 운영체제에 **보안 커널을 이식하여 보호 기능을 강화**하는 방식으로 구현할 수 있으며, 운영체제의 취약점을 악용한 공격이나 허가받지 않은 자원 접근으로부터 시스템을 보호한다.

NoteBase

문 2. 다음에서 설명하는 접근통제 모델은?

◯ 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근 통제까지 설정하는 모델이다.
◯ 중앙 집중화된 정보 관리가 어려워서 정보에 대한 엄격한 접근 통제는 거의 불가능하다.

① 비바(Biba)
② 임의적 접근통제(DAC)
③ 역할기반 접근통제(RBAC)
④ 벨 라파둘라(Bell-LaPadula)

정답 2번

간단한 해설

정보 소유자가 접근 권한을 직접 설정하는 것은 임의적 접근통제(DAC)의 특징이다. 권한 결정이 소유자별로 이루어지므로 조직 전체에 통일된 접근통제 정책을 엄격하게 적용하기 어렵다.

공통 해설

임의적 접근통제(DAC)는 정보 소유자가 자신의 정보에 대해 **누구에게 어떤 접근을 허용할지 결정**하는 모델이다. 예를 들어 파일 소유자가 사용자 A에게는 읽기만, 사용자 B에게는 읽기와 수정을 허용할 수 있다. 지문의 '정보 소유자가 정보의 보안 수준을 결정하고 접근 통제까지 설정한다'는 설명은 이러한 소유자의 재량을 가리킨다.

소유자마다 접근 권한을 설정하면 권한 관리가 분산되므로, 조직 전체의 권한을 중앙에서 일관되게 관리하고 엄격한 보안 정책을 적용하기 어렵다. 둘째 설명은 이러한 관리상의 한계를 나타내며, DAC에 접근을 허용하거나 차단하는 기능 자체가 없다는 의미는 아니다.

NoteBase

문 3. 멀웨어(Malware)에 대한 설명으로 옳은 것은?

① 스파이웨어(Spyware)는 사용자 동의 없이 정보를 수집하여 전송한다.

② 트로이목마(Trojan Horse)는 시스템 자원을 암호화하여 금전을 요구하는 공격을 수행한다.

③ 바이러스(Virus)는 독립적으로 실행되며, 취약점을 이용하여 스스로 전파된다.

④ 웜(Worm)은 정상 프로그램이나 실행 가능한 부분에 자신 또는 자신의 변형을 복사하며, 다른 네트워크의 시스템으로 스스로 전파하지 못한다.

정답 1번

간단한 해설

스파이웨어는 **사용자 동의 없이 정보를 수집해 외부로 전송**하는 멀웨어이다. 정보를 몰래 빼내는 기능이 판단의 기준이다.

선지별 해설

① O: 스파이웨어는 사용자 동의 없이 개인정보나 사용 기록 등을 수집하여 외부로 전송하는 멀웨어이다. 웹 이용 기록이나 입력 정보 등을 몰래 수집할 수 있어 **정보 유출**을 일으킨다.

② X: 시스템 자원을 암호화한 뒤 복구를 대가로 금전을 요구하는 것은 **랜섬웨어**의 특징이다. 트로이목마는 정상적이거나 유용한 프로그램처럼 위장하여 악성 기능을 수행하는 멀웨어이며, 암호화와 금전 요구가 필수 특징은 아니다.

③ X: 독립적으로 실행되며 취약점 등을 이용해 스스로 전파되는 것은 웜의 특징이다. 바이러스는 **숙주 프로그램이나 실행 가능한 영역에 자신을 복제**하고, 감염된 숙주가 실행되는 과정에서 동작하므로 독립 실행을 특징으로 하는 웜과 구별된다.

④ X: 정상 프로그램이나 실행 가능한 부분에 자신 또는 변형을 복사하는 것은 바이러스의 특징이다. 웜은 독립적으로 실행되는 악성 프로그램으로, **다른 네트워크 시스템으로 스스로 전파할 수 있다**. 따라서 선지의 숙주 의존적 복제와 자가 전파 불가능이라는 설명을 모두 고쳐야 한다.

NoteBase

문 4. 다음에서 설명하는 공격은?

◯ 공격자가 특정 대상을 목표로 다양한 공격 기술을 이용해 지속적으로 공격한다.
◯ 이 공격의 사례는 제로데이 취약점을 활용한 Stuxnet이 있다.

① APT
② DDoS
③ Ransomware
④ Reverse Engineering

정답 1번

간단한 해설

특정 대상을 정해 다양한 공격 기술로 지속적으로 공격하는 특성은 **APT(지능형 지속 위협)**에 해당한다. 지문의 Stuxnet은 이러한 표적 공격의 사례이다.

공통 해설

APT(Advanced Persistent Threat, 지능형 지속 위협)는 특정 조직이나 시스템을 표적으로 삼아 다양한 기술로 침투하고, 접근을 유지하면서 목적 달성을 위해 공격을 지속하는 위협이다. 이를 식별하는 기준은 **특정 표적에 대한 지속성**이다.

지문의 '특정 대상을 목표'로 한다는 설명은 표적성을, '다양한 공격 기술을 이용해 지속적으로 공격'한다는 설명은 공격 수단의 다양성과 지속성을 나타낸다. 이 특성들이 APT의 정의와 대응한다. Stuxnet이 활용한 제로데이 취약점은 공격 수단의 한 예이며, 모든 APT가 반드시 제로데이 취약점을 이용해야 하는 것은 아니다.

NoteBase

문 5. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?

① 이상탐지(Anomaly Detection)는 시그니처(Signature) 기반 탐지라고도 한다.

② 제로데이(Zero-day) 공격에 대한 탐지는 오용탐지에 비해 이상탐지가 효율적이다.

③ 오용탐지(Misuse Detection)는 알려진 공격의 패턴을 탐지하는 방법이다.

④ 이상탐지(Anomaly Detection)는 정상적이고 평균적인 상태를 크게 벗어나는 이벤트가 발생하는 것을 탐지하는 방법이다.

정답 1번

간단한 해설

시그니처 기반 탐지는 알려진 공격 패턴과 비교하는 **오용탐지**이다. 이상탐지는 **정상 행위의 기준에서 벗어나는 정도**를 보고 의심스러운 활동을 찾는다.

선지별 해설

① X: 시그니처는 알려진 공격을 식별하는 패턴이다. 수집한 이벤트를 이 패턴과 대조하는 방식은 **오용탐지**이므로, '이상탐지는 시그니처 기반 탐지라고도 한다'는 설명은 두 방식을 혼동한 것이다. 이상탐지는 정상 행위의 기준을 만들고 그 기준에서 벗어난 활동을 탐지한다.

② O: 제로데이 공격은 취약점에 대한 대응이 마련되기 전에 이루어지는 공격으로, 해당 공격의 시그니처가 준비되어 있지 않을 수 있다. 오용탐지는 등록된 공격 패턴에 의존하므로 이런 공격을 놓치기 쉽다. 이상탐지는 **알려진 공격 패턴이 없어도 정상 행위와의 차이**를 이용할 수 있어 제로데이 공격 탐지에 상대적으로 유리하다. 다만 공격 행위가 정상 범위와 구별되지 않으면 탐지하지 못할 수 있다.

③ O: 오용탐지는 **알려진 공격 패턴과의 일치 여부**를 기준으로 침입을 탐지한다. 예를 들어 특정 공격에 사용되는 문자열이 시그니처로 등록되어 있다면, 수집한 트래픽에서 그 문자열을 찾아 공격을 식별한다.

④ O: 이상탐지는 정상적인 사용자의 행위나 시스템·네트워크 활동을 기준으로 삼아 **정상 범위를 크게 벗어나는 이벤트**를 탐지한다. 예를 들어 평소보다 접속 시도가 급증하면 이상 징후로 판단할 수 있다. 다만 정상적인 활동도 기준을 벗어날 수 있으므로 이상 징후가 곧 실제 공격을 뜻하는 것은 아니다.

NoteBase

문 6. 다음에서 설명하는 도구는?

웹 브라우저와 웹 서버가 통신할 때, 중간에 위치하여 웹 브라우저의 요청 메시지를 받아 웹 서버로 전송하고, 웹 서버에서 받은 응답 메시지도 웹 브라우저로 전달하는 역할을 한다. 이것을 이용하면 웹 클라이언트와 웹 서버가 교환하는 모든 데이터를 중간에서 수정이 가능하다.

① 루트킷(rootkit)

② 웹 프록시(web proxy)

③ 애드웨어(adware)

④ 포트 스캐너(port scanner)

정답 2번

간단한 해설

브라우저와 서버 사이에서 **요청과 응답을 중계**하고, 전달 전에 메시지를 수정할 수 있다는 점이 웹 프록시의 식별 단서이다.

공통 해설

웹 프록시(web proxy)는 웹 브라우저와 웹 서버 사이에서 요청과 응답을 대신 전달하는 중계 도구이다. 브라우저의 요청을 받아 서버로 보내고, 서버의 응답을 받아 다시 브라우저로 보내므로 통신 경로는 '브라우저 ↔ 웹 프록시 ↔ 서버'가 된다. 지문의 도구는 이처럼 **양방향 메시지의 전달 경로 중간에 위치**한다는 점에서 웹 프록시에 해당한다.

메시지 가로채기·수정 기능을 갖춘 웹 프록시를 사용하면, 프록시를 거치는 요청이나 응답을 전달 전에 확인하고 바꿀 수 있다. 예를 들어 브라우저가 보낸 요청의 매개변수 값을 프록시에서 수정하여 서버로 전달하면, 서버는 수정된 요청을 받는다. 지문의 데이터 수정 기능은 이러한 중계 위치를 이용한 것이다.

NoteBase

문 7. 다음과 관련된 공격은?

```
SELECT * FROM member
WHERE id = 'admin' and password = ''or''='' ;
```

① XSS

② CSRF

③ SQL Injection

④ Format String

정답 3번

간단한 해설

SQL 조건식에 **항상 참인 OR 조건**을 끼워 넣어 아이디·비밀번호 검사를 무력화하는 **SQL Injection**이다.

핵심 풀이

SQL Injection은 외부 입력이 SQL 명령의 일부로 해석되도록 하여 쿼리의 의미를 바꾸는 공격이다. 제시문의 OR 뒤에 있는 '' = ''는 빈 문자열끼리 비교하므로 항상 참이다. SQL에서는 **AND가 OR보다 먼저 결합**하므로, id = 'admin'과 password = ''를 모두 만족하는지 검사한 결과에 이 참인 조건이 OR로 연결된다. 따라서 아이디나 비밀번호의 일치 여부와 관계없이 WHERE 절 전체가 참이 되어 member 테이블의 모든 행이 조회 대상이 된다. 애플리케이션이 조회된 행의 존재만으로 로그인 성공을 판단한다면 인증을 우회할 수 있다.

공격 대상의 차이로 구분하면, XSS는 웹페이지에 삽입한 스크립트를 사용자의 브라우저에서 실행시키는 공격이고, CSRF는 사용자의 인증 상태를 이용해 원하지 않는 요청을 보내게 하는 공격이다. Format String 공격은 외부 입력이 서식 지정 문자열로 해석되는 취약점을 이용한다. 제시문은 **데이터베이스 조회 조건을 조작**하므로 SQL Injection에 해당한다.

NoteBase

문 8. 다음은 시스템의 보안 기능에 대한 설명이다. (가)~(다)에 들어갈 용어를 바르게 연결한 것은?

○ (가)는 사용자와 시스템 또는 두 시스템 간에 활성화된 접속을 관리하는 것이다.
○ (나)는 시스템 자체의 결함 때문에 발생하는 보안 문제를 체계적으로 관리하는 것이다.
○ (다)는 시스템 내부 또는 외부에서 시스템에 어떤 영향을 미쳤을 경우, 해당 사항을 기록하고 관리한다.

① (가): 로그 관리, (나): 취약점 관리, (다): 계정 관리
② (가): 로그 관리, (나): 취약점 관리, (다): 세션 관리
③ (가): 세션 관리, (나): 권한 관리, (다): 로그 관리
④ (가): 세션 관리, (나): 취약점 관리, (다): 로그 관리

정답 4번

간단한 해설

현재 활성화된 접속을 다루는 **세션 관리**와 시스템에서 일어난 일을 기록하는 **로그 관리**는 관리 대상이 다르다. 시스템 결함으로 생기는 보안 문제는 취약점 관리의 대상이다.

빈칸별 해설

(가) 세션 관리: 세션은 사용자와 시스템 또는 두 시스템 사이에 형성된 접속 상태를 뜻한다. 따라서 **활성화된 접속의 유지와 종료**를 다루는 설명은 세션 관리에 해당한다. 사용자 식별정보의 생성·변경·삭제를 다루는 계정 관리와는 관리 대상이 다르다.

(나) 취약점 관리: 취약점은 공격에 악용될 수 있는 시스템의 결함이나 약점이다. 이를 찾아 평가하고 보안 패치 등으로 보완하는 것이 취약점 관리이다. 여기서는 **시스템 자체의 결함**이 핵심 단서이며, 사용자가 어떤 자원에 어떤 작업을 할 수 있는지 정하는 권한 관리와 구별된다.

(다) 로그 관리: 로그는 시스템에서 발생한 사건이나 활동을 남긴 기록이다. 내부 또는 외부의 행위가 시스템에 미친 영향을 **기록하고 보관·분석**하는 설명은 로그 관리에 해당한다. 현재 접속 상태를 관리하는 세션 관리와 달리, 발생한 일을 추적할 수 있는 기록을 관리한다.

(가)는 세션 관리, (나)는 취약점 관리, (다)는 로그 관리로 연결되므로 ④의 조합과 일치한다.

NoteBase

문 9. 운영체제의 프로세스에 대한 설명으로 옳지 않은 것은?

① 프로세스는 실행 중인 프로그램이다.

② 프로세스의 상태는 준비(ready), 실행(running), 종료(terminated) 등이 있다.

③ 문맥 교환(context switch)은 한 프로세스 내에서 다른 메모리 공간을 사용해야 할 때 발생한다.

④ 프로세스를 관리하기 위한 정보는 프로세스 제어 블록(process control block)에 저장된다.

정답 3번

간단한 해설

문맥 교환은 **CPU의 실행 대상을 바꾸기 위해 실행 상태를 저장하고 복원하는 과정**이다. 한 프로세스 안에서 다른 메모리 영역을 사용한다는 이유만으로 문맥 교환이 발생하는 것은 아니다.

선지별 해설

① O: 프로세스는 **실행 중인 프로그램**이다. 저장장치에 보관된 프로그램이 명령과 데이터의 집합이라면, 프로세스는 그 프로그램이 실행되면서 메모리와 CPU 등 자원을 할당받아 동작하는 실체이다.

② O: 준비(ready)는 실행에 필요한 조건을 갖추고 **CPU 할당을 기다리는 상태**, 실행(running)은 CPU를 할당받아 명령을 수행하는 상태, 종료(terminated)는 실행을 마친 상태이다. 프로세스의 상태에는 이 밖에도 입출력 완료 등을 기다리는 대기 상태가 있다.

③ X: 문맥 교환(context switch)은 CPU가 실행하던 프로세스의 문맥을 저장하고, 다음에 실행할 프로세스의 문맥을 복원하는 과정이다. 문맥에는 프로그램 카운터와 CPU 레지스터 값 등 실행을 이어 가는 데 필요한 정보가 포함된다. 예를 들어 A에서 B로 실행 대상을 바꿀 때 A의 상태를 저장하고 B의 상태를 불러온다. 따라서 발생 기준은 **한 프로세스 안의 메모리 영역 변경이 아니라 실행 대상의 전환**이다.

④ O: 프로세스 제어 블록(PCB)은 운영체제가 **프로세스를 관리하는 데 필요한 정보를 보관하는 자료구조**이다. 프로세스 식별자, 상태, 프로그램 카운터, CPU 레지스터 값, 스케줄링 정보 등이 저장된다. 운영체제는 이 정보를 이용해 프로세스를 식별하고 실행을 관리하며, 중단된 실행을 다시 이어 갈 수 있다.

NoteBase

문 10. 다음은 리눅스의 파일 권한에 대한 설명이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

소유자가 root인 어떤 파일의 권한이 '-rwsr-xr-x'로 설정되어 있다. 이 권한에서 's'는 (가) 설정을 의미한다. 이 파일의 권한을 숫자로 표현하면 (나)이다.

① (가): SetUID, (나): 2755

② (가): SetUID, (나): 4755

③ (가): SetGID, (나): 2755

④ (가): SetGID, (나): 4755

정답 2번

간단한 해설

's'가 **소유자의 실행 권한 자리**에 있으므로 SetUID를 뜻한다. SetUID의 특수 권한 값 4와 일반 권한 rwxr-xr-x의 값 755를 결합하면 **4755**가 된다.

빈칸별 해설

(가) SetUID: '-rwsr-xr-x'에서 맨 앞의 '-'는 일반 파일을 뜻하며, 뒤의 아홉 자리는 소유자·그룹·기타 사용자의 권한을 세 자리씩 나타낸다. 's'가 소유자 권한인 'rws'의 실행 권한 자리에 있으므로 **SetUID가 설정**되어 있다. 소문자 's'는 소유자의 실행 권한도 함께 설정되어 있음을 뜻한다. SetUID가 설정된 실행 파일은 실행 시 프로세스의 유효 사용자 ID가 파일 소유자의 ID로 설정되므로, 이 파일에서는 root가 된다. SetGID는 그룹의 실행 권한 자리에 's'가 표시된다는 점에서 구별된다.

(나) 4755: 숫자 권한은 8진수로 나타내며, 특수 권한 한 자리 뒤에 소유자·그룹·기타 사용자의 권한을 차례로 붙인다. 일반 권한에서 읽기 r은 4, 쓰기 w는 2, 실행 x는 1이다. 소유자의 'rws'는 실행 권한을 포함하므로 4 + 2 + 1 = 7이고, 그룹과 기타 사용자의 'r-x'는 각각 4 + 1 = 5이다. 따라서 일반 권한은 755이다. 특수 권한 자리에서 **SetUID는 4, SetGID는 2**이므로 이 파일의 숫자 권한은 4755이다. 2755는 SetGID와 일반 권한 755를 결합한 값이다.

(가)는 SetUID, (나)는 4755이므로 ②의 조합과 일치한다.

NoteBase

문 11. 리눅스의 보안 관리에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. 원격에서 root 계정으로 접속하는 것을 관리자가 제한한다.
ㄴ. /etc/passwd 파일의 소유자와 권한 설정을 확인한다.
ㄷ. 소유자가 없는 파일과 디렉터리를 관리자가 삭제하거나 소유자를 변경한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 4번

간단한 해설

소유자 계정이 삭제된 뒤에도 해당 계정의 파일과 디렉터리가 남을 수 있다. **불필요한 것은 삭제하고 필요한 것은 적절한 계정으로 소유자를 변경**하여 관리한다.

보기별 해설

ㄱ. O: root는 시스템 전반을 관리할 수 있는 강력한 권한을 가진 계정이다. 원격에서 root로 직접 접속할 수 있으면 계정이 탈취되었을 때 피해가 시스템 전체로 확대될 수 있다. 따라서 **root 계정의 원격 직접 접속을 제한**하는 것은 관리자 권한의 노출을 줄이는 보안 조치이다.

ㄴ. O: /etc/passwd는 사용자 이름, 사용자 식별자(UID), 홈 디렉터리, 로그인 셸 등 계정 정보를 담는 파일이다. 이 파일이 무단으로 변경되면 계정 정보가 조작될 수 있으므로 소유자가 root인지, 일반 사용자에게 쓰기 권한이 부여되어 있지 않은지 확인해야 한다. 일반 사용자의 읽기는 통상 허용되지만 **쓰기는 제한**해야 한다.

ㄷ. O: 리눅스 파일의 소유권은 사용자 식별자(UID)로 기록된다. 계정을 삭제해도 그 계정이 소유하던 파일과 디렉터리가 남아, 해당 UID에 대응하는 계정이 없는 상태가 될 수 있다. 이후 같은 UID가 다른 계정에 할당되면 그 계정이 기존 파일의 소유자로 취급될 수 있으므로, 관리자는 **불필요한 파일은 삭제하고 필요한 파일은 적절한 소유자로 변경**해야 한다.

ㄱ, ㄴ, ㄷ은 모두 적절한 리눅스 보안 관리 조치이므로, 세 보기를 모두 포함하는 ④에 해당한다.

NoteBase

문 12. 리눅스의 파일 및 디렉터리 권한에 대한 설명으로 옳지 않은 것은?

① ‘-rw-r-xr-x’을 숫자로 표현하면 655이다.

② ‘drw-r-xr-x’에서 ‘d’는 디렉터리를 의미한다.

③ ‘chmod u-w’ 명령은 소유자의 쓰기 권한을 제거한다.

④ ‘chown -R’ 명령은 소유한 모든 하위 파일의 권한을 변경한다.

정답 4번

간단한 해설

'chown -R'은 지정한 디렉터리와 그 하위 항목의 **소유자**를 재귀적으로 변경한다. 읽기·쓰기·실행 **권한을 변경하는 명령은 chmod**이다.

선지별 해설

① O: 맨 앞의 '-'는 일반 파일을 뜻하고, 뒤의 아홉 문자는 소유자·그룹·기타 사용자의 권한을 세 문자씩 나타낸다. 읽기 r은 4, 쓰기 w는 2, 실행 x는 1이며 '-'는 해당 권한이 없다는 뜻이다. 'rw-'는 4 + 2 = 6, 'r-x'는 4 + 1 = 5이므로 '-rw-r-xr-x'의 권한은 **655**로 표현한다.

② O: 권한 표시의 **첫 문자는 파일의 종류**를 나타낸다. 'drw-r-xr-x'의 첫 문자 'd'는 디렉터리라는 뜻이며, 그 뒤의 'rw-r-xr-x'가 사용자별 권한을 나타낸다.

③ O: chmod의 기호 모드에서 'u'는 파일 소유자, '-'는 권한 제거, 'w'는 쓰기 권한을 뜻한다. 따라서 'chmod u-w 파일명'은 해당 파일의 **소유자 쓰기 권한만 제거**하고, 다른 사용자 범주의 권한은 그대로 둔다.

④ X: chown은 **소유자를 변경**하는 명령이고, '-R'은 지정한 디렉터리와 그 아래의 파일·디렉터리에 재귀적으로 적용하는 옵션이다. 예를 들어 'chown -R 새소유자 디렉터리'는 지정한 디렉터리와 하위 항목의 소유자를 바꾼다. 선지의 '권한을 변경한다'는 '소유자를 변경한다'로 고쳐야 한다. 읽기·쓰기·실행 권한을 하위 항목까지 변경하려면 'chmod -R 권한값 디렉터리'를 사용한다.

NoteBase

문 13. 리눅스의 로그에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. lastlog는 가장 최근 로그인 정보의 기록으로 lastlog 명령어로 확인한다.
ㄴ. btmp는 실패한 로그인 정보를 기록한 바이너리 파일로 lastb 명령어로 확인한다.
ㄷ. boot.log는 부팅 시 동작하는 데몬 관련 정보를 기록한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 4번

간단한 해설

boot.log는 **부팅 과정의 메시지**를 기록하므로, 부팅 시 시작되는 데몬이나 서비스의 상태 정보도 포함한다. 로그인 기록과 구분하여 시스템 시작 과정의 문제를 확인하는 데 쓰인다.

보기별 해설

ㄱ. O: /var/log/lastlog는 **사용자별 가장 최근 로그인 정보**를 저장한다. lastlog 명령어는 이 파일을 읽어 사용자 이름, 접속 터미널, 마지막 로그인 시각 등을 표시한다. 전체 로그인 이력을 차례로 나열하는 기록과 달리 각 사용자의 마지막 로그인 정보를 확인하는 용도이다.

ㄴ. O: /var/log/btmp는 **실패한 로그인 시도**를 저장하는 바이너리 파일이다. 일반 텍스트 파일처럼 읽는 대신 lastb 명령어로 기록을 해석하여 실패한 로그인 내역을 확인한다.

ㄷ. O: /var/log/boot.log는 시스템 부팅 과정의 메시지를 저장한다. 부팅 시 데몬이나 서비스를 시작하면서 출력되는 **시작 상태와 오류 등의 정보**가 기록되므로, 부팅 시 동작하는 데몬 관련 정보를 기록한다는 설명에 부합한다.

ㄱ, ㄴ, ㄷ이 모두 옳으므로 이를 모두 포함한 조합은 ④이다.

NoteBase

문 14. 버퍼 오버플로 공격에 대한 설명으로 옳지 않은 것은?

① realpath()는 버퍼 오버플로에 취약한 함수이다.

② 데이터 타입(data type)에 대한 불명확한 정의로 인해 발생한다.

③ 할당된 버퍼 한계를 벗어나서 인근 메모리 위치에 데이터를 덮어쓰는 것이다.

④ 대응 방법은 스택가드, 스택쉴드, ASLR 등이 있다.

정답 2번

간단한 해설

버퍼 오버플로는 **버퍼의 크기나 경계를 제대로 검사하지 않아** 허용 범위를 넘어 데이터를 쓸 때 발생한다. 데이터 타입이 명확하게 정의되어 있어도 쓰기 길이를 제한하지 않으면 발생할 수 있다.

선지별 해설

① O: realpath()는 경로를 해석하여 절대 경로를 구하는 함수이다. 호출자가 제공하는 결과 버퍼의 크기를 인수로 받지 않으므로, **결과 경로를 담기에 부족한 버퍼**를 넘기면 버퍼 오버플로 위험이 있다. 따라서 이 선지는 버퍼 크기를 안전하게 확보하지 않은 사용에서의 위험을 뜻하며, 모든 호출이 취약하다는 뜻은 아니다. 이를 지원하는 환경에서는 결과 버퍼 인수에 NULL을 전달하여 함수가 필요한 메모리를 할당하게 할 수 있다.

② X: 버퍼 오버플로의 핵심 원인은 데이터 타입의 불명확한 정의가 아니라 **버퍼 경계나 쓰기 길이에 대한 검사 부족**이다. 예를 들어 8바이트 버퍼에 12바이트를 경계 검사 없이 쓰면 자료형이 명확해도 버퍼 밖으로 데이터가 기록된다. 따라서 '데이터 타입에 대한 불명확한 정의'는 '버퍼 크기와 쓰기 범위를 적절히 검사하지 않음'으로 고쳐야 한다.

③ O: 버퍼 오버플로는 **할당된 버퍼의 경계를 넘어 인접 메모리에 데이터를 쓰는** 현상이다. 이로 인해 다른 변수의 값이 손상되거나 프로그램이 비정상 종료될 수 있다. 스택의 복귀 주소까지 덮어쓰면 공격자가 실행 흐름을 바꾸는 데 악용할 수도 있다.

④ O: 스택가드는 스택에 카나리라는 검사값을 두고 함수가 복귀하기 전에 그 값이 변했는지 확인하여 메모리 훼손을 탐지한다. 스택쉴드는 복귀 주소의 사본을 별도 영역에 보관하여 복귀 주소를 보호한다. ASLR은 메모리 배치 주소를 무작위화하여 공격자가 목표 주소를 예측하기 어렵게 한다. 이들은 **훼손을 탐지하거나 공격 성공을 어렵게 하는** 대응 기법이며, 버퍼 경계 검사 자체를 대신하지는 않는다.

NoteBase

문 15. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?

① RSA 암호 알고리즘을 사용한다.

② 이중 서명 프로토콜을 사용한다.

③ 상점은 고객의 지불 정보(카드 번호 등)를 알 수 없다.

④ 은행은 고객의 주문 정보를 알 수 있다.

정답 4번

간단한 해설

④의 '주문 정보를 알 수 있다'는 설명은 정보 공개 대상을 잘못 연결한 것이다. SET에서 은행 측은 지불 정보를 처리하지만, **고객의 주문 내용은 알 수 없다**. 주문 정보의 해시값을 이용해 해당 주문과 지불 정보의 연결을 확인한다.

선지별 해설

① O: SET는 **공개키 암호 알고리즘인 RSA**를 사용하여 전자 서명과 암호키 전달을 수행한다. 실제 메시지 데이터의 암호화에는 대칭키 암호를 함께 사용하는 방식이다.

② O: **이중 서명**은 주문 정보와 지불 정보를 서로 연결하면서 각 수신자에게 필요한 정보만 공개하도록 하는 데 사용된다. 두 정보의 해시값을 결합한 뒤 다시 해시하여 고객의 개인키로 서명하므로, 상점과 은행은 상대방이 받는 정보의 원문을 보지 않고도 두 정보의 연결을 검증할 수 있다.

③ O: 카드 번호 등 지불 정보는 **은행 측 결제 게이트웨이만 복호화할 수 있도록** 보호된다. 상점은 암호화된 지불 정보를 전달하지만 이를 읽는 데 필요한 키를 얻을 수 없으므로 고객의 카드 번호 등을 알 수 없다.

④ X: 은행 측 결제 게이트웨이는 지불 정보를 처리하며, **고객의 주문 내용은 알 수 없다**. 주문 정보의 원문 대신 그 해시값을 받아 이중 서명을 검증하므로, 주문 내용을 공개받지 않고도 해당 주문과 지불 정보가 연결되어 있음을 확인할 수 있다.

NoteBase

문 16. 구글 검색 명령어(Google search operator)에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. “site:”는 특정 사이트를 선택하여 검색한다.
ㄴ. “url:”은 페이지의 URL에 검색하려는 문자가 포함된 사이트를 검색한다.
ㄷ. “title:”은 페이지의 제목에 검색하려는 문자가 포함된 사이트를 검색한다.
ㄹ. “filetype:”은 특정 파일타입만 검색한다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 2번

간단한 해설

페이지의 URL에 특정 단어가 포함되도록 검색하려면 **inurl:**을, 제목에 포함되도록 검색하려면 **intitle:**을 사용한다. ㄴ과 ㄷ은 각각 'url:', 'title:'로 연산자 이름을 잘못 제시했다.

보기별 해설

ㄱ. O: site:는 검색 결과를 **지정한 사이트나 도메인으로 제한**하는 연산자이다. 특정 사이트 안에서 검색어와 관련된 페이지를 찾을 때 사용한다.

ㄴ. X: 페이지의 URL에 특정 검색어가 포함된 결과를 찾는 연산자는 'url:'이 아니라 **inurl:**이다. 예를 들어 'inurl:login'은 URL에 login이라는 단어가 포함된 페이지를 찾는 검색식이다.

ㄷ. X: 페이지의 제목에 특정 검색어가 포함된 결과를 찾는 연산자는 'title:'이 아니라 **intitle:**이다. inurl:이 검색어의 포함 위치를 URL로 제한한다면, intitle:은 제목으로 제한한다.

ㄹ. O: filetype:은 검색 결과를 **특정 파일 형식으로 제한**하는 연산자이다. 예를 들어 '보안 filetype:pdf'는 보안과 관련된 검색 결과 중 PDF 형식의 자료를 찾는 검색식이다.

옳은 보기는 ㄱ과 ㄹ이므로, 이 조합에 해당하는 선택지는 ②이다.

NoteBase

문 17. 시스템 관리에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. OWASP-ZAP는 웹 취약점 점검 시 사용하는 도구이다.
ㄴ. 데이터베이스 REVOKE문은 허가된 권한을 취소하는 명령어이다.
ㄷ. 리눅스 chage는 사용자 계정의 패스워드 에이징(aging) 정보를 변경하는 명령어이다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 4번

간단한 해설

chage의 패스워드 에이징은 **암호의 유효기간과 변경 주기**를 관리하는 기능이다. 암호 문자열을 새로 정하는 것과 달리, 사용자가 언제 암호를 바꾸어야 하는지를 설정한다.

보기별 해설

ㄱ. O: OWASP-ZAP는 **웹 애플리케이션의 취약점**을 점검하는 도구이다. 웹 요청과 응답을 분석하고 자동 스캔 등을 수행하여 보안상 취약한 부분을 찾는 데 사용한다.

ㄴ. O: REVOKE는 사용자나 역할에 **이미 부여한 권한을 취소**하는 SQL 명령어이다. 권한을 부여하는 GRANT와 구별하며, 테이블 조회 권한처럼 데이터베이스 객체에 대한 접근 권한을 회수할 때 사용한다.

ㄷ. O: 리눅스의 chage는 사용자 계정의 **패스워드 에이징 정보**를 변경하는 명령어이다. 마지막 암호 변경일, 암호 변경 사이의 최소 일수, 암호의 최대 사용 일수 등을 설정하여 암호를 언제 변경해야 하는지 관리한다.

ㄱ, ㄴ, ㄷ이 모두 옳으므로 세 보기를 모두 포함한 ④에 해당한다.

NoteBase

문 18. PGP와 S/MIME에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. PGP에서 전자 서명을 위해 DSS 또는 RSA를 사용한다.
ㄴ. PGP에서 타임스탬프, KeyID, 공개키, 암호화된 개인키, 인증서, 사용자 ID는 개인키 링에 포함되어 있다.
ㄷ. S/MIME에서 봉인된 데이터(enveloped data)는 메시지의 비밀성을 제공하기 위해 사용된다.
ㄹ. S/MIME에서 키 관리는 X.509와 PGP에서 사용되는 키 관리의 조합 방법을 사용한다.

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄱ, ㄷ, ㄹ
④ ㄴ, ㄷ, ㄹ

정답 3번

간단한 해설

PGP 개인키 링은 **사용자 자신의 키 쌍을 관리**하는 자료구조이며, 인증서는 그 기본 구성 항목에 포함되지 않는다. S/MIME의 키 관리에서는 **X.509 인증기관의 서명과 사용자의 로컬 신뢰 관리**가 함께 쓰인다.

NoteBase

보기별 해설

ㄱ. O: PGP는 전자 서명에 DSS의 서명 알고리즘인 **DSA 또는 RSA**를 사용한다. 송신자는 메시지의 해시값에 자신의 개인키로 서명하고, 수신자는 송신자의 공개키로 이를 검증하여 메시지의 무결성과 송신자 인증을 확인한다.

ㄴ. X: 개인키 링은 사용자 자신이 소유한 공개키·개인키 쌍을 저장한다. 기본 항목은 타임스탬프, KeyID, 공개키, 암호화된 개인키, 사용자 ID이며, 보기의 **'인증서'를 제외해야 한다**. 타임스탬프는 키 쌍의 생성 시각을, KeyID는 키를 식별하는 값을 나타낸다. 개인키는 유출에 대비하여 암호화한 상태로 보관한다.

ㄷ. O: 봉인된 데이터는 **암호화된 메시지와 보호된 세션키 정보**를 담아 비밀성을 제공한다. 메시지 본문은 대칭키인 세션키로 암호화하며, 수신자는 자신에게 제공된 키 정보를 이용해 세션키를 복구한 뒤 본문을 복호화한다.

ㄹ. O: S/MIME는 X.509 공개키 인증서를 사용하며, 인증기관이 인증서에 서명한다. 동시에 사용자나 관리자가 각 클라이언트에서 신뢰할 키 목록과 인증서 폐지 목록 등을 관리한다. 따라서 **인증기관을 통한 인증과 로컬 신뢰 관리의 결합**이라는 측면에서 X.509의 계층적 인증 방식과 PGP의 사용자 중심 신뢰 방식을 조합한 것으로 설명한다.

옳은 보기는 ㄱ, ㄷ, ㄹ이며, 이 조합은 ③에 해당한다.

NoteBase

문 19. 다음은 HTTP 버전 1.1에서 정의된 요청 메서드에 대한 설명이다. (가) ~ (라)에 들어갈 내용을 바르게 연결한 것은?

◯ 게시판 등에서 파일 업로드는 (가) 방식으로 할 수 있다.
이는 (나) 방식과 달리 보내려는 데이터가 URL을 통해 노출되지 않기 때문에 최소한의 보안성은 갖추고 있다.
◯ 일반적으로 게시판의 목록이나 글 보기 화면은 접근 자유도를 부여하기 위해 (다) 방식을 사용하고, 게시글을 저장·수정·삭제하거나 대용량 데이터를 전송할 때는 (라) 방식을 사용한다.

① (가): POST, (나): GET, (다): GET, (라): POST
② (가): POST, (나): GET, (다): POST, (라): GET
③ (가): GET, (나): POST, (다): GET, (라): POST
④ (가): GET, (나): POST, (다): POST, (라): GET

정답 1번

간단한 해설

GET은 게시판의 목록이나 글을 **조회**할 때, POST는 파일이나 게시글 데이터를 **요청 본문에 담아 전송**할 때 사용한다. POST가 전송 데이터를 URL에 드러내지 않는다는 것은 데이터 자체를 암호화한다는 뜻은 아니다.

NoteBase

빈칸별 해설

(가) POST: 파일 업로드는 파일 데이터를 서버로 보내는 작업이다. 일반적인 HTML 폼에서는 POST를 사용하고 multipart/form-data 형식으로 파일과 다른 입력값을 **요청 본문에 담아** 전송한다.

(나) GET: GET 방식으로 폼을 제출하면 입력값이 **URL의 쿼리 문자열**에 포함되어 주소 표시줄이나 URL 기록을 통해 노출될 수 있다. POST로 본문에 담아 보내는 데이터는 이런 URL 노출을 피한다. 다만 POST 자체에는 암호화 기능이 없으므로, 전송 중 기밀성을 보호하려면 HTTPS가 필요하다. 지문의 '최소한의 보안성'은 URL에 데이터를 드러내지 않는다는 제한된 의미이다.

(다) GET: GET은 지정한 자원의 정보를 가져오는 메서드이므로, 서버의 게시글을 변경하지 않고 **목록이나 글 내용을 조회**하는 데 적합하다. 조회 조건이나 글 번호를 URL에 넣으면 해당 주소를 링크로 공유하거나 북마크하여 같은 화면에 다시 접근할 수 있다. 여기서 접근 자유도는 주소를 통한 접근 편의성이며, 인증이나 접근 권한 검사가 불필요하다는 뜻은 아니다.

(라) POST: 문항의 일반적인 게시판에서는 저장·수정·삭제 요청을 서버의 처리 프로그램에 보내기 위해 POST를 사용한다. 이는 단순 조회와 달리 **서버의 데이터 상태를 변경하는 처리**이다. 또한 대용량 데이터는 URL에 넣기보다 요청 본문으로 전송하는 것이 적합하다. 다만 POST라고 전송량이 무제한인 것은 아니며 서버 등의 요청 본문 크기 제한은 적용된다.

(가) POST, (나) GET, (다) GET, (라) POST의 조합이므로 ①의 연결과 일치한다.

NoteBase

문 20. 다음은 리눅스의 /etc/shadow 파일 구조이다. 각 항목에 대한 설명으로 옳은 것만을 모두 고르면?

anthony:6L9~중략~ruKuT0:18365:(가):(나):(다):(라)::
ㄱ. (가) 값이 0이면 패스워드를 즉시 변경할 수 있다.
ㄴ. (나)는 패스워드를 변경하지 않고 사용 가능한 최대 일수이다.
ㄷ. (다)는 패스워드가 만료되기 전에 경고를 시작하는 일수이다.
ㄹ. (라)는 사용자 계정이 만료되는 날이다.

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄱ, ㄴ, ㄷ
④ ㄴ, ㄷ, ㄹ

정답 3번

간단한 해설

(라)는 계정이 만료되는 날짜가 아니라 **패스워드 만료 후 로그인이 차단되기까지의 유예 일수**이다. 계정 만료일은 그다음인 여덟 번째 필드에 기록한다.

NoteBase

보기별 해설

각 항목은 콜론(:)으로 구분한다. anthony는 사용자명, 다음 항목은 패스워드 해시, 18365는 마지막 패스워드 변경일을 나타낸다. 따라서 (가)~(라)는 차례로 네 번째부터 일곱 번째 필드이다.

ㄱ. O: (가)는 네 번째 필드로, 패스워드를 변경한 뒤 다시 변경할 수 있을 때까지 기다려야 하는 최소 일수이다. 값이 0이면 **최소 대기 기간이 없으므로** 패스워드를 즉시 다시 변경할 수 있다.

ㄴ. O: (나)는 다섯 번째 필드로, 마지막 변경 후 패스워드를 그대로 사용할 수 있는 **최대 일수**이다. 이 기간이 지나면 패스워드가 만료되어 변경을 요구받는다.

ㄷ. O: (다)는 여섯 번째 필드로, 패스워드가 만료되기 **며칠 전부터 경고할지**를 정한다. 예를 들어 값이 7이면 만료 7일 전부터 사용자에게 만료 경고를 표시한다.

ㄹ. X: (라)는 일곱 번째 필드로, **패스워드 만료 후의 비활성 기간**을 일수로 지정한다. 만료 후 이 기간 안에 로그인하면 패스워드를 변경해야 하며, 변경하지 않은 채 기간까지 지나면 로그인이 차단된다. 사용자 계정 자체의 만료일은 여덟 번째 필드에 기록하며, 1970년 1월 1일부터 경과한 일수로 나타낸다.

옳은 보기는 ㄱ, ㄴ, ㄷ이며, 이 조합은 ③에 해당한다.

NoteBase