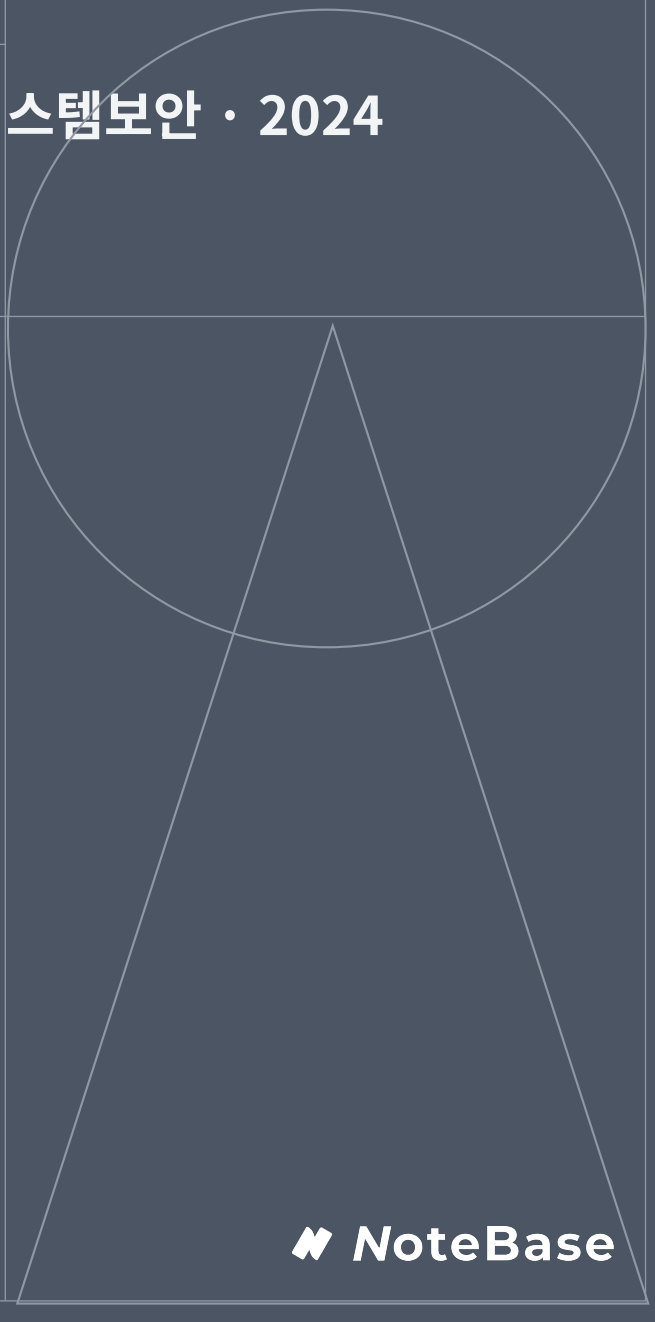
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2024



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2024

공무원/국가직/9급 · 정보시스템보안 · 2024

문 1. 유닉스 파일 시스템의 i-node 정보에 해당하지 않는 것은?

① 소유그룹

② 파일 타입

③ 파일명

④ 접근권한

정답 3번

간단한 해설

파일명은 디렉터리 항목에 저장되며, i-node에는 파일의 속성 정보가 저장된다. 디렉터리 항목이 파일명과 i-node 번호를 연결한다.

개념 구분

i-node는 파일의 속성을 관리하는 자료구조이다. 소유그룹은 그룹 ID로, 파일 타입은 일반 파일·디렉터리 등의 종류로 기록된다. 접근권한은 소유자·소유그룹·기타 사용자에게 허용되는 읽기·쓰기·실행 권한을 나타낸다. 이들은 모두 **i-node에 저장되는 속성 정보**이다.

파일명은 i-node 자체가 아니라 **디렉터리 항목에 i-node 번호와 함께** 저장된다. 예를 들어 디렉터리 항목에 'a.txt → i-node 100'이라는 연결이 있으면, 시스템은 a.txt라는 이름으로 i-node 100을 찾아 그 파일의 속성을 확인한다. 따라서 파일명은 i-node에 저장되는 정보에 해당하지 않는다.

NoteBase

문 2. PGP의 인증에 대한 설명으로 옳지 않은 것은?

① 송신자는 일방향 해시함수를 사용하여 송신 메시지의 해시 코드를 생성한다.

② 송신자가 생성한 해시 코드는 송신자의 개인키를 사용하여 암호화되며, 그 결괏값이 메시지에 포함된다.

③ 수신자는 수신한 메시지를 송신자의 공개키로 복호화하고 해시 코드를 알아낸다.

④ 디지털 서명을 생성하는 데 DSS를 사용하는 것은 허용하지 않는다.

정답 4번

간단한 해설

PGP는 디지털 서명에 RSA뿐 아니라 **DSS(디지털 서명 표준)에 따른 DSA도 사용할 수 있다**. 따라서 DSS 사용을 허용하지 않는다는 설명은 잘못되었다.

선지별 해설

① O: 송신자는 메시지에 일방향 해시함수를 적용하여 **메시지의 요약값인 해시 코드**를 만든다. 일방향이라는 것은 해시 코드만으로 원래 메시지를 복원하기가 어렵다는 뜻이다. 이 해시 코드는 디지털 서명을 생성하는 데 사용된다.

② O: 해시 코드를 송신자의 개인키로 암호화한다는 표현은 **RSA 방식의 서명 생성**을 설명한 것이다. 송신자는 자신의 개인키로 해시 코드에 대한 서명값을 만들고, 이를 메시지에 첨부하여 전송한다.

③ O: 송신자의 공개키로 확인하는 대상은 수신 메시지에 포함된 **디지털 서명**이다. RSA 방식에서는 서명으로부터 해시 정보를 확인하고, 수신한 메시지에 같은 해시함수를 적용하여 얻은 값과 비교한다. 두 값이 일치하는지 확인하여 메시지의 변조 여부를 검증하는 것으로, 메시지 본문 전체를 송신자의 공개키로 복호화한다는 뜻은 아니다.

④ X: PGP는 RSA뿐 아니라 **DSS에 따른 DSA를 이용한 디지털 서명도 지원한다**. 따라서 'DSS를 사용하는 것은 허용하지 않는다'는 'DSS에 따른 서명 방식도 사용할 수 있다'로 고쳐야 한다. DSA는 RSA와 달리 해시 코드를 암호화한 뒤 복호화하는 방식이 아니라, 별도의 서명 생성·검증 연산을 사용한다.

NoteBase

문 3. 사용자 및 그룹 계정 정보에 대한 데이터베이스를 관리하는 윈도 인증 구성 요소는?

① LSA

② SAM

③ SRM

④ SID

정답 2번

간단한 해설

사용자와 그룹의 계정 정보를 데이터베이스로 저장·관리하는 역할은 **SAM(Security Accounts Manager)**이 담당한다.

공통 해설

SAM(Security Accounts Manager)은 윈도에서 **로컬 사용자와 그룹의 계정 데이터베이스를 관리**하는 구성 요소이다. 로컬 사용자나 그룹을 생성·변경·삭제할 때 그 정보를 이 데이터베이스에 반영하므로, 발문에서 제시한 계정 정보의 관리 기능에 대응한다.

NoteBase

문 4. 다음에서 설명하는 웹 취약점은?

웹 애플리케이션을 구동하는 웹 서버의 보안 설정이 취약하여 발생하는 보안 설정 오류 취약점이다. 정상적인 URL 경로 중 확인 대상 디렉터리까지만 직접 접근하여 이 취약점을 점검할 수 있다.

① SQL Injection
② 디렉터리 인덱싱
③ 운영체제 명령어 실행
④ XSS(Cross Site Scripting)

정답 2번

간단한 해설

정상적인 URL에서 **디렉터리 경로까지만 접근**해 내부 파일 목록이 노출되는지 확인하는 것은 디렉터리 인덱싱 취약점의 점검 방법이다. 웹 서버의 목록 표시 설정으로 공개할 필요가 없는 파일명과 디렉터리 구조가 드러날 수 있다.

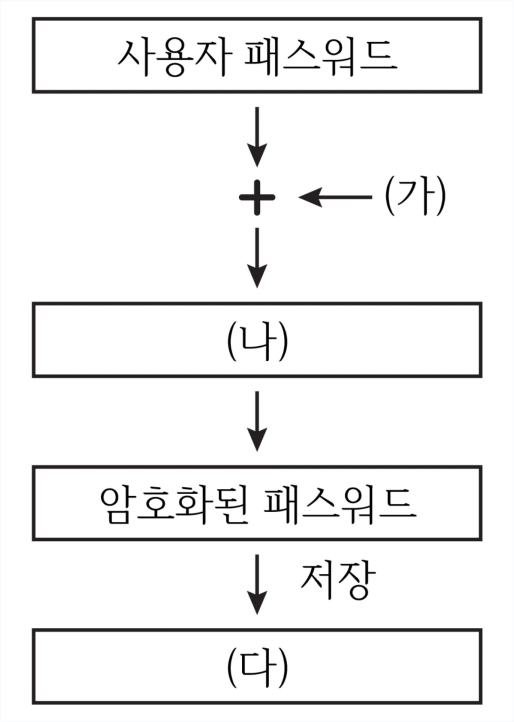
공통 해설

디렉터리 인덱싱 취약점은 웹 서버의 설정 때문에 디렉터리에 있는 파일과 하위 디렉터리의 목록이 외부에 불필요하게 노출되는 취약점이다. 일반적으로 요청한 디렉터리에 기본 문서가 없고 **디렉터리 목록 표시 기능이 활성화**되어 있으면, 서버가 목록을 자동으로 생성해 보여 줄 수 있다. 이 목록을 통해 공개할 필요가 없는 파일명과 디렉터리 구조가 알려질 수 있다.

지문의 '확인 대상 디렉터리까지만 직접 접근'한다는 것은 특정 파일을 지정하지 않고 해당 디렉터리를 요청하여 목록 노출 여부를 확인한다는 뜻이다. 따라서 웹 서버의 보안 설정 오류와 디렉터리 접근이라는 두 단서는 디렉터리 인덱싱의 발생 원인과 점검 방법에 대응한다.

NoteBase

문 5. 다음 리눅스 시스템 사용자 패스워드 저장 과정의 (가)~(다)에 들어갈 내용을 바르게 연결한 것은?



① (가): Salt, (나): RSA, (다): /etc/passwd

② (가): Salt, (나): SHA256, (다): /etc/shadow

③ (가): 암호키, (나): MD5, (다): /etc/passwd

④ (가): 암호키, (나): ARIA, (다): /etc/shadow

정답 2번

간단한 해설

패스워드에 **솔트(Salt)**를 결합하면 같은 패스워드라도 솔트가 다를 때 서로 다른 해시값으로 저장할 수 있다.
그림의 '암호화된 패스워드'는 복호화할 암호문이 아니라 **일방향 해시값**을 뜻한다.

NoteBase

빈칸별 해설

(가) Salt: 그림에서 사용자 패스워드에 추가되는 값은 솔트이다. 솔트는 패스워드를 해싱할 때 함께 사용하는 부가 값으로, 사용자마다 다른 솔트를 사용하면 같은 패스워드의 해시값이 같아지는 것을 막고 미리 계산한 해시값 목록의 재사용을 어렵게 한다. **솔트는 복호화에 쓰는 비밀 암호키가 아니며**, 해시값과 함께 저장할 수 있다.

(나) SHA256: 솔트와 패스워드를 입력받아 저장용 값을 만드는 단계이므로, 제시된 조합에서는 SHA-256 기반 패스워드 해싱이 해당한다. 그림의 '암호화된 패스워드'는 원문으로 되돌리는 암호문이 아니라 해시 결과를 가리킨다. 로그인할 때도 저장값을 복호화하지 않고, 입력한 패스워드에 같은 솔트와 해싱 방식을 적용하여 **저장된 해시값과 비교**한다. RSA와 ARIA는 각각 공개키 암호와 대칭키 암호로, 여기서 요구하는 일방향 해싱과 구별된다.

(다) /etc/shadow: 섀도 패스워드 방식을 사용하는 리눅스에서는 패스워드 해시와 관련 정보를 **일반 사용자의 읽기가 제한된 /etc/shadow**에 저장한다. /etc/passwd에는 사용자 이름·사용자 ID·홈 디렉터리 등의 계정 정보가 있으며, 패스워드 필드에는 실제 해시 대신 보통 'x'를 두어 /etc/shadow에 저장되어 있음을 나타낸다.

(가)는 Salt, (나)는 SHA256, (다)는 /etc/shadow로 연결되므로 ②의 조합과 일치한다.

NoteBase

문 6. x86 32bit 계열 CPU의 레지스터에 대한 설명으로 옳지 않은 것은?

① EDI는 목적지 주소 값을 저장한다.

② ECX는 반복적으로 실행되는 특정 명령에 사용된다.

③ CS는 프로그램에서 정의된 데이터, 상수, 작업 영역의 메모리 주소를 저장한다.

④ EFLAGS는 연산 결과 및 시스템의 상태와 관련된 여러 가지 플래그 값을 저장한다.

정답 3번

간단한 해설

③은 코드 영역과 데이터 영역을 혼동했다. **CS는 실행할 명령어가 있는 코드 세그먼트**를 가리키며, 프로그램의 데이터·상수·작업 영역에 대한 설명은 데이터 세그먼트를 가리키는 **DS**에 해당한다.

선지별 해설

① O: EDI는 목적지 인덱스 레지스터로, 문자열 처리 명령에서 **목적지의 위치**를 나타낸다. 32비트 주소 크기를 사용하는 문자열 복사에서는 ESI가 원본 위치를, EDI가 복사할 목적지 위치를 나타내며, EDI에는 목적지 세그먼트 안의 오프셋이 들어간다.

② O: ECX는 문자열 반복 처리나 루프에서 **반복 횟수를 세는 카운터**로 사용된다. 예를 들어 REP 접두어를 사용하는 문자열 명령은 ECX를 통해 반복 횟수를 관리한다.

③ X: CS는 **코드 세그먼트**를 가리키는 레지스터이다. 코드 세그먼트에는 실행할 명령어가 있으며, 프로그램의 데이터·상수·작업 영역을 담는 데이터 세그먼트는 DS가 가리킨다. 보호 모드에서 CS와 DS에 저장되는 값은 각 세그먼트를 식별하는 세그먼트 선택자이므로, 개별 명령어나 데이터의 전체 메모리 주소를 직접 저장한다는 뜻은 아니다.

④ O: EFLAGS는 **연산 결과를 나타내는 상태 플래그와 CPU 동작을 제어하는 플래그** 등을 저장한다. 따라서 산술·논리 연산의 결과뿐 아니라 시스템의 상태 및 제어에 관련된 정보를 함께 나타낸다.

NoteBase

문 7. 다음에서 설명하는 공격에 대한 대응 방법으로 옳지 않은 것은?

◯ 웹 서버를 기반으로 서버에 파일이 업로드되고 서버 측에서 실행되는 이러한 파일을 웹 셸(web shell)이라고 한다.
◯ 공격자는 웹 서버에 업로드된 웹 셸 파일을 원격지에서 실행하여 웹 서버를 공격할 수 있다.

① 업로드 파일에 대한 실행 금지
② 업로드 파일에 대한 위치 격리
③ 업로드 가능한 파일 형식 제한
④ 업로드 파일명에 대한 필터링 설정

정답 4번

간단한 해설

웹 셸 공격은 업로드된 악성 파일이 서버에서 실행되어 발생하므로, 파일의 유입과 실행을 제한하는 것이 핵심이다. 공식 정답은 ④이지만, **파일명 필터링도 유효한 보조 보안 조치**이므로 이를 무조건 잘못된 대응이라고 단정할 수는 없다.

NoteBase

선지별 해설

웹 셸은 서버에서 실행되어 공격자의 명령을 처리하는 악성 스크립트이다. 대응 방법은 위험한 파일의 업로드를 제한하거나, 저장된 파일에 대한 접근과 서버 측 실행을 차단하는 방향으로 마련한다.

① O: 업로드된 파일이 **서버 측 스크립트로 실행되지 않도록** 설정하면 웹 셸의 작동을 차단할 수 있다. 업로드 디렉터리에서 스크립트 처리를 금지하는 조치가 이에 해당한다. 운영체제의 실행 권한만 없애는 것과 웹 서버의 스크립트 실행을 차단하는 것은 구별된다.

② O: 업로드 파일을 웹 루트, 즉 웹에 공개되는 기본 디렉터리 밖의 별도 저장 영역에 두면 URL을 통한 직접 접근을 제한할 수 있다. 위치 격리는 **웹 요청이 업로드 파일의 실행으로 이어지는 경로**를 줄이는 조치이며, 해당 파일을 애플리케이션이 다시 불러와 실행하지 않도록 함께 통제해야 한다.

③ O: 업무에 필요한 파일 형식만 허용하면 실행 가능한 악성 스크립트의 유입을 줄일 수 있다. 확장자나 사용자가 보낸 파일 형식 정보만 믿지 않고 **실제 내용이 허용된 형식에 부합하는지**도 검증해야 한다. 형식 검증만으로 악성 내용이 모두 제거되는 것은 아니므로 실행 차단과 함께 적용한다.

④ O: 파일명에 포함된 위험한 문자나 경로 문자열을 제한하는 필터링은 의도하지 않은 위치에 파일이 저장되거나 기존 파일이 덮어써지는 위험을 줄이는 보조 대책이다. 다만 **파일명이 허용된다는 사실만으로 내용의 안전성이나 실행 차단이 보장되지는 않는다**. 또한 위험한 확장자를 검사하는 필터링까지 포함하면 ③의 파일 형식 제한과도 일부 겹친다.

공식 채점 답은 ④이다. 그러나 원문에는 파일명 필터링의 범위가 명시되어 있지 않아, 보안 원칙상 ④만 잘못된 대응이라고 단정할 근거는 부족하다. 파일명 검사만으로 웹 셸을 완전히 막을 수 없다는 한계와 파일명 검증 자체의 보안 효과는 구별된다.

NoteBase

문 8. 참조 모니터(Reference Monitor)에 대한 설명으로 옳지 않은 것은?

① 모든 주체 간 상호 접근통제를 담당하는 추상적인 기계이다.

② 참조 모니터 데이터베이스를 참조하여 접근통제를 수행한다.

③ 모든 접근 시도에 대해 시행되어야 하고 회피하는 것이 불가능해야 한다.

④ 보안 매개변수 설정 등과 같은 다른 보안 메커니즘과 데이터를 교환하면서 상호 작용을 한다.

정답 1번

간단한 해설

참조 모니터는 **주체가 객체에 접근하는 모든 시도**를 통제하는 추상적인 기계이다. '주체 간 상호 접근통제'라는 표현은 접근을 요청하는 주체와 보호 대상인 객체를 구분하지 못한 설명이다.

선지별 해설

① X: 참조 모니터는 **주체의 객체에 대한 접근**을 통제하는 추상적인 기계이다. 주체는 사용자나 프로세스처럼 접근을 요청하는 능동적 요소이고, 객체는 파일이나 데이터처럼 접근의 대상이 되는 자원이다. 따라서 '모든 주체 간 상호 접근통제'를 '주체가 객체에 접근하는 모든 시도에 대한 접근통제'로 고쳐야 한다.

② O: 참조 모니터 데이터베이스에는 접근권한과 주체·객체의 보안 속성 등 접근 판단에 필요한 정보가 저장된다. 참조 모니터는 요청한 주체, 대상 객체, 읽기·쓰기 등의 요청 연산을 이 정보와 대조하여 **접근을 허용하거나 거부**한다.

③ O: 참조 모니터는 **모든 접근 시도에서 반드시 실행**되어야 한다. 이를 완전한 중재라고 하며, 참조 모니터를 거치지 않고 객체에 접근하는 우회 경로가 없어야 한다. 일부 접근만 검사하면 검사하지 않은 경로로 보안정책을 위반할 수 있기 때문이다.

④ O: 참조 모니터는 접근권한이나 보안등급을 설정·관리하는 기능 등 다른 보안 메커니즘과 상호 작용한다. 이러한 기능이 제공하는 **보안 매개변수**를 접근 판단에 사용하므로, 접근을 검사하는 기능과 판단에 필요한 보안정보를 설정하는 기능이 연계된다.

NoteBase

문 9. (가)에 들어갈 리눅스 메일 시스템의 구성 요소는?

◯ 메일 클라이언트에서 (가)로 메일을 보낼 때와 (가)에서 (가)로 메일이 중계될 때 SMTP 프로토콜을 사용한다.
◯ 불특정 다수의 메일 전송 및 중계를 허용하면 공격자는 스팸 메일을 보내는 도구로 (가)를 악용할 수 있다.

① MTA(Message Transfer Agent)
② MDA(Mail Delivery Agent)
③ MUA(Mail User Agent)
④ MRA(Mail Relay Agent)

정답 1번

간단한 해설

MTA는 **SMTP로 메일을 전송·중계**하는 구성 요소이다. 외부인의 중계를 제한하지 않으면 공격자가 이를 스팸 발송에 악용하는 오픈 릴레이 문제가 생긴다.

빈칸별 해설

(가) MTA(Message Transfer Agent): 메일을 받아 수신자 쪽의 다른 메일 서버로 전달하는 구성 요소이다. 지문의 메일 클라이언트 → MTA, MTA → MTA 구간에서는 **SMTP를 이용하여 메일을 전송**한다. 예를 들어 발신 측 서버가 수신 측 서버로 메일을 넘길 때 MTA 간 중계가 이루어진다.

불특정 다수에게 외부 목적지로의 중계를 허용하는 상태를 **오픈 릴레이**라고 한다. 이때 공격자는 해당 MTA에 스팸 메일을 맡겨 다른 수신자들에게 전송하게 할 수 있다. 따라서 두 번째 설명도 메일 전송·중계를 담당하는 MTA의 설정과 관련된다.

MUA는 사용자가 메일을 작성하고 읽는 클라이언트이고, MDA는 수신된 메일을 사용자의 우편함에 최종 배달한다. 이와 구별하여 지문은 서버 사이의 전송·중계 기능을 묻는다.

두 설명에 공통으로 들어갈 구성 요소는 MTA이며, ①의 명칭과 일치한다.

NoteBase

문 10. 보안 취약점으로 인해 실제 발생한 취약점의 등급을 매기는 공개 프레임워크는?

① CVE

② CVSS

③ CWE

④ NVD

정답 2번

간단한 해설

CVSS는 보안 취약점의 주요 특성을 평가하여 **심각도를 점수와 등급으로 나타내는** 공개 프레임워크이다.

공통 해설

CVSS(Common Vulnerability Scoring System)는 취약점의 주요 특성을 공통 기준으로 평가하여 심각도를 수치 점수로 나타내는 공개 프레임워크이다. 산출한 점수는 낮음·중간·높음·치명적 등의 등급으로 표현할 수 있으므로, 발문의 '취약점의 등급을 매기는' 기능에 해당한다.

구별 기준은 취약점의 심각도를 산정하는 평가 체계인지 여부이다. CVE는 개별 취약점의 식별, CWE는 약점 유형의 분류, NVD는 취약점 정보의 제공에 초점을 둔다. 이들과 구별하여 **심각도 산정 기준을 제공하는 체계**가 CVSS이다.

NoteBase

문 11. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

○ (가)는 컴파일러가 프로그램의 함수를 호출할 때 ret 앞에 canary 값을 주입하고, 종료할 때 canary 값을 변조했는지 확인하여 공격을 탐지한다.
○ (나) 공격은 데이터의 형태와 길이에 대한 불명확한 정의로 인한 문제점 중 데이터 형태에 대한 불명확한 정의로 인한 것이다.

① (가): 스택 실드, (나): 버퍼 오버플로
② (가): 스택 실드, (나): 포맷 스트링
③ (가): 스택 가드, (나): 버퍼 오버플로
④ (가): 스택 가드, (나): 포맷 스트링

정답 4번

간단한 해설

카나리 값의 변조 여부로 스택 손상을 탐지하는 기법은 스택 가드이다. 입력을 단순한 데이터가 아니라 **서식 지정자로 해석**하면서 발생하는 공격은 포맷 스트링 공격이다.

빈칸별 해설

(가) 스택 가드: 카나리는 스택의 버퍼와 복귀 주소 사이에 두는 검사값이다. 버퍼를 넘친 데이터가 복귀 주소까지 덮어쓰는 과정에서 카나리도 바뀌므로, 함수가 복귀하기 전에 **카나리 값이 유지되는지 검사**하여 변조를 탐지하고 실행을 중단한다. 스택 실드는 복귀 주소의 사본을 별도 영역에 보관하여 복귀 주소를 보호하는 방식이므로, 카나리를 검사한다는 단서와 구별된다.

(나) 포맷 스트링: 서식 문자열은 출력 함수 등이 데이터를 어떤 형태로 처리할지 지정하는 문자열이다. 공격자가 입력한 문자열을 서식 문자열로 사용하면, 입력 속 %x 같은 서식 지정자가 단순한 문자로 출력되지 않고 처리되어 의도하지 않은 메모리 내용이 노출될 수 있다. 따라서 지문의 **데이터 형태에 대한 불명확한 정의**는 포맷 스트링 공격에 대응한다. 버퍼 오버플로는 저장 공간의 크기를 초과하여 데이터를 기록하는 문제로, 입력 길이에 대한 검사 부족과 관련된다.

(가)에 스택 가드, (나)에 포맷 스트링을 넣는 조합이므로 ④와 연결된다.

NoteBase

문 12. 다음에서 설명하는 인증 방법은?

사용자가 많이 가입한 웹 사이트(네이버, 구글, 페이스북 등)의 사용자 가입 정보를 이용해서 다른 웹 사이트에 별도의 가입 과정 없이 단순하게 사용자 신원을 검증하는 토큰을 제공하여 제삼자 인증 서비스를 이용할 수 있게 해 준다.

① Kerberos

② OAuth

③ SSO

④ DIAMETER

정답 2번

간단한 해설

기존 웹 사이트의 계정과 연계하여 제삼자 사이트에 **토큰으로 제한된 접근 권한을 부여**하는 구조가 OAuth의 특징이다. 사용자는 기존 계정의 비밀번호를 제삼자 사이트에 직접 알려 주지 않고도 허용한 정보를 제공할 수 있다.

공통 해설

OAuth는 제삼자 애플리케이션이 사용자의 허락을 받아 자원에 접근하도록 하는 인가 체계이다. 핵심은 **사용자가 승인한 범위의 접근 권한을 토큰으로 위임**한다는 데 있다. 접근 토큰에는 허용된 접근 범위와 유효기간 등의 조건이 연결된다.

제시된 방식에서는 사용자가 기존 계정의 서비스에 로그인하고 정보 제공을 승인하면, 제삼자 사이트가 발급받은 접근 토큰으로 허용된 사용자 정보를 요청할 수 있다. 기존 계정의 비밀번호를 제삼자 사이트에 직접 전달할 필요가 없으며, 제삼자 사이트는 허용된 정보로 계정을 연계할 수 있다. 문항의 '기존 웹 사이트의 가입 정보 활용'과 '토큰을 통한 제삼자 서비스 연계'는 이러한 OAuth의 구조를 가리킨다.

인증은 사용자가 누구인지 확인하는 것이고, 인가는 어떤 자원에 접근할 수 있는지 권한을 부여하는 것이다. OAuth 자체의 핵심은 인가이므로, 접근 토큰을 곧바로 사용자 신원 증명서와 동일시해서는 안 된다. 이 문항에서는 단순히 여러 서비스를 편리하게 이용한다는 효과보다 제삼자에게 토큰으로 접근 권한을 위임한다는 구조가 식별 기준이다.

NoteBase

문 13. 클라우드 서비스 및 보안에 대한 설명으로 옳지 않은 것은?

① 클라우드 환경에서의 서비스 모델은 IaaS, PaaS, SaaS로 구분할 수 있다.

② 한국인터넷진흥원(KISA)에서는 클라우드 서비스의 보안성 강화를 위해 '클라우드 서비스 보안인증'을 시행하고 있다.

③ 대부분의 취약점은 전통적인 IT 환경의 보안 취약점과 유사하여 기존의 보안시스템을 최대한 활용하여 방어하는 것만으로도 충분하다.

④ CSA(Cloud Security Alliance)에서는 심각한 클라우드 보안 위협에 대해 공유하고 있다.

정답 3번

간단한 해설

③의 '기존의 보안시스템을 최대한 활용하여 방어하는 것만으로도 충분하다'는 설명이 잘못되었다.
클라우드에서는 **자원 공유·가상화·관리 API에 따른 위험**도 고려하여 이용자 간 격리, 접근권한 관리 등 환경에 맞는 보안대책을 추가해야 한다.

선지별 해설

① O: 클라우드 서비스는 **제공하는 기능의 범위**에 따라 IaaS, PaaS, SaaS로 구분한다. IaaS는 서버·저장공간·네트워크 같은 인프라를, PaaS는 애플리케이션 개발·실행에 필요한 플랫폼을, SaaS는 완성된 소프트웨어의 이용 기능을 제공한다.

② O: 한국인터넷진흥원(KISA)은 클라우드서비스 보안인증제(CSAP)를 운영한다. 클라우드 서비스가 **보안인증기준을 충족하는지 평가·인증**하여 서비스의 보안 수준과 신뢰성을 높이는 제도이다.

③ X: 기존 IT 환경과 공통되는 취약점이 있더라도 **기존 보안시스템을 활용하는 것만으로 충분하지는 않다**. 여러 이용자가 자원을 공유하는 구조에서는 이용자 간 격리가 중요하고, 가상화 계층과 서비스 관리 API도 보호해야 한다. 예를 들어 외부 침입을 차단하더라도 저장공간의 공개 설정이나 계정의 과도한 권한이 남아 있으면 데이터가 노출될 수 있다. 따라서 기존 대책과 함께 가상화 환경 보호, 접근권한·설정 점검, API 보안 등 클라우드 특성에 맞는 통제가 필요하다.

④ O: CSA(Cloud Security Alliance)는 클라우드 보안 위협을 조사하여 **주요 위협과 대응방안**을 보고서 등으로 공유한다. 설정 오류, 부적절한 접근권한 관리, 안전하지 않은 인터페이스와 API 등이 이러한 위협에 포함된다.

NoteBase

문 14. 신뢰 플랫폼 모듈(Trusted Platform Module)의 구성 요소로 옳지 않은 것은?

① 난수 발생기

② 암복호화 엔진

③ RSA 키 발생기

④ MD5 해시값 생성기

정답 4번

간단한 해설

TPM에는 해시 연산 기능이 있으며, TPM 1.2의 기본 해시 엔진은 **MD5가 아니라 SHA-1**이다. 따라서 MD5 해시값 생성기는 해당 기본 구성 요소에 포함되지 않는다.

개념 구분

TPM은 암호키를 보호하고 플랫폼의 무결성 확인을 지원하는 보안 모듈이다. 난수 생성, 키 생성, 암복호화, 해시 연산은 서로 구별되는 기능이다.

① 난수 발생기: 키 생성과 인증 등에 필요한 **예측하기 어려운 난수**를 제공한다. TPM의 기본 구성 요소에 해당한다.

② 암복호화 엔진: 암호키를 이용하여 암호화·복호화 연산을 수행한다. TPM 1.2는 RSA 암호 연산을 지원하며, 이는 **키 자체를 생성하는 기능과 구별**된다.

③ RSA 키 발생기: RSA 연산에 사용할 **공개키와 개인키의 쌍을 생성**한다. 생성된 키로 암호 연산을 수행하는 암복호화 엔진과 역할이 다르며, TPM의 구성에 포함된다.

④ MD5 해시값 생성기: 해시는 입력 데이터의 요약값을 계산하는 기능이다. TPM 1.2의 기본 구성에는 **SHA-1 해시 엔진**이 들어가므로, MD5 해시값 생성기는 이 구성에 해당하지 않는다. 해시 기능의 존재가 아니라 알고리즘 명칭이 잘못된 것이다.

따라서 구성 요소로 옳지 않은 것은 ④ MD5 해시값 생성기이다.

NoteBase

문 15. syslogd 데몬에서 사용하는 다음 메시지 중 우선순위가 가장 높은 것은?

① alert

② crit

③ err

④ debug

정답 1번

간단한 해설

alert는 **즉시 조치가 필요한 상황**을 나타내며, 심각한 상태를 뜻하는 crit보다 우선순위가 높다. syslog의 심각도 등급은 **숫자가 작을수록 우선순위가 높다**.

선지별 해설

syslogd의 메시지는 심각도에 따라 우선순위를 구분하며, 심각도 등급의 숫자가 작을수록 더 긴급하고 우선순위가 높다. 각 메시지의 등급과 의미를 같은 기준으로 비교하면 다음과 같다.

① alert: 심각도 등급은 1로, **즉시 조치가 필요한 상황**을 나타낸다. crit보다 긴급한 수준이므로 제시된 네 메시지 중 우선순위가 가장 높다.

② crit: 심각도 등급은 2로, **심각한 상태**를 나타낸다. err보다 우선순위가 높지만, 즉시 조치가 필요한 alert보다는 낮다.

③ err: 심각도 등급은 3으로, **오류 상태**를 나타낸다. crit보다 심각도가 낮으며, 디버깅 정보를 나타내는 debug보다는 우선순위가 높다.

④ debug: 심각도 등급은 7로, 프로그램의 동작을 추적하거나 문제를 분석하기 위한 **디버깅 정보**를 나타낸다. syslog의 심각도 등급 중 우선순위가 가장 낮다.

우선순위는 alert > crit > err > debug 순이므로, 제시된 메시지 중에서는 ① alert가 가장 높다.

NoteBase

문 16. 웹 취약점에 대한 설명으로 옳지 않은 것은?

① 입력 값에 대한 특수문자 검증을 통해 XSS 공격에 대응할 수 있다.

② 리버스 텔넷은 방화벽의 아웃바운드 정책에서 별다른 필터링을 수행하지 않는 허점을 이용한다.

③ 취약점이 있는 컴포넌트, 라이브러리, 프레임워크 및 다른 소프트웨어 모듈이 악용되는 경우 데이터에 손실을 발생시킬 수 있다.

④ CSRF는 사용자의 브라우저로 전달되는 데이터에 악성코드가 포함되어 브라우저에서 실행되면서 공격하는 기법이다.

정답 4번

간단한 해설

④의 '브라우저로 전달된 악성코드가 실행된다'는 설명은 **XSS**에 해당한다. **CSRF**는 인증된 사용자의 브라우저가 사용자의 의사와 무관한 요청을 신뢰하는 사이트에 보내도록 유도하는 공격이다.

선지별 해설

① O: XSS는 웹 페이지에 포함된 악성 스크립트가 사용자의 브라우저에서 실행되는 공격이다. 입력 값의 특수문자를 검증하여 위험한 입력을 제한하는 것은 대응 수단이 될 수 있다. 다만 특수문자 검사만으로 모든 XSS를 막을 수 있는 것은 아니므로, 데이터가 삽입되는 위치에 맞는 **출력 인코딩** 등도 적용하여 입력이 실행 코드로 해석되지 않게 해야 한다.

② O: 리버스 텔넷은 공격 대상 시스템에서 외부의 공격자 쪽으로 연결을 시작하게 하여 원격 제어 통로를 만드는 방식이다. 외부에서 내부로 들어오는 접속을 차단하더라도, **내부에서 외부로 나가는 연결을 제한하지 않으면** 이런 통로가 만들어질 수 있다. 따라서 인바운드뿐 아니라 아웃바운드 통신도 필요한 대상과 포트로 제한해야 한다.

③ O: 라이브러리나 프레임워크 같은 구성 요소의 취약점은 이를 사용하는 애플리케이션의 취약점이 될 수 있다. 공격자가 해당 취약점을 악용하면 구성 요소가 가진 권한과 취약점의 성격에 따라 **데이터 손실이나 서버 장악**으로 이어질 수 있다. 따라서 사용 중인 구성 요소와 버전을 관리하고 보안 패치를 적용해야 한다.

④ X: 브라우저에 전달된 데이터에 악성 스크립트가 포함되어 실행되는 것은 **XSS**의 설명이다. CSRF는 사이트가 사용자의 인증 상태를 신뢰하는 점을 이용하여 **사용자가 의도하지 않은 요청을 보내게 하는** 공격이다. 예를 들어 로그인 상태의 브라우저가 세션 쿠키를 함께 보내는 상황에서, 공격자가 유도한 정보 변경 요청을 서버가 정상적인 사용자 요청으로 받아들이면 피해가 발생할 수 있다. CSRF는 대상 사이트에 악성 스크립트를 삽입하여 실행시키는 취약점이 없어도 성립할 수 있다.

NoteBase

문 17. 리눅스 bash shell의 환경 변수에 대한 설명으로 옳은 것은?

① TERM은 접속 호스트 이름을 나타낸다.

② SHELL은 서브 셸을 사용할 때 서브 셸을 의미한다.

③ PATH는 명령을 탐색할 경로를 의미한다.

④ PWD는 현재 사용 중인 패스워드의 위치를 나타낸다.

정답 3번

간단한 해설

PATH는 명령으로 실행할 파일을 찾을 때 사용할 **디렉터리 목록**이다. 여러 경로를 콜론(:)으로 구분하여 저장하며, 셸은 이 목록을 명령 탐색에 사용한다.

선지별 해설

① X: TERM은 접속한 호스트의 이름이 아니라 **사용 중인 터미널의 종류**를 나타낸다. 프로그램은 이 값을 바탕으로 터미널에 맞는 화면 제어 방식을 선택한다.

② X: SHELL은 **셸 실행 파일의 전체 경로**를 담는 변수로, 일반적으로 사용자의 로그인 셸 경로를 나타낸다. 서브 셸을 사용한다고 해서 그 서브 셸을 가리키도록 자동으로 바뀌는 변수는 아니다.

③ O: PATH는 셸이 명령의 실행 파일을 찾을 때 탐색할 **디렉터리 목록**을 담는다. 경로들은 콜론(:)으로 구분하며, 외부 명령을 경로 없이 입력하여 파일을 탐색할 때 목록의 앞쪽 디렉터리부터 확인한다.

④ X: PWD는 패스워드의 위치가 아니라 **현재 작업 디렉터리의 경로**를 나타낸다. 셸에서 cd 명령으로 작업 디렉터리를 바꾸면 PWD도 그 디렉터리의 경로로 갱신된다.

NoteBase

문 18. 다음에서 설명하는 공격을 수행할 수 있는 도구로 옳지 않은 것은?

관리자 인증 등 정상적인 절차를 거치지 않고 시스템에 접근하기 위해 제작된 프로그램으로, 원격지에서 공격자가 몰래 정보를 수집하거나 시스템의 특정 명령을 수행하고 재구성할 수 있도록 통제한다.

① Netbus
② Schoolbus
③ Nessus
④ Back Orifice

정답 3번

간단한 해설

Nessus는 시스템의 보안상 약점을 찾아내는 **취약점 점검 도구**이다. 제시문의 정상적인 인증 절차를 우회한 정보 수집과 명령 실행은 **백도어를 이용한 원격 제어**에 해당한다.

개념 구분

제시문의 핵심 단서는 '정상적인 절차를 거치지 않고 시스템에 접근'하여 '원격지에서 명령을 수행'한다는 점이다. 백도어는 정상적인 인증 절차를 우회하여 시스템에 접근할 수 있게 하는 통로이다. Netbus, Schoolbus, Back Orifice는 이러한 **백도어 기능을 이용해 원격 제어**를 수행할 수 있는 도구로, 공격자가 대상 시스템의 정보를 수집하거나 명령을 실행하는 데 악용된다.

Nessus는 운영체제나 서비스의 알려진 취약점, 누락된 보안 패치, 잘못된 설정 등을 검사하는 **취약점 스캐너**이다. 검사 결과로 보안상 약점과 보완할 사항을 파악하게 하므로, 제시문처럼 백도어를 통해 대상 시스템을 몰래 통제하는 도구와 구분된다.

NoteBase

문 19. 윈도 운영체제의 감사 정책에 대한 설명으로 옳지 않은 것은?

① 권한 사용은 관리자 권한이 필요한 작업을 수행할 때 감사한다.

② 계정 로그온 이벤트는 로컬 계정에 접근할 때 생성되는 이벤트를 감사한다.

③ 개체 액세스는 파일, 디렉터리, 레지스트리 키, 프린터와 같은 개체에 접근 시도나 속성 변경 등을 감사한다.

④ 계정 관리는 신규 사용자 및 그룹 추가, 기존 사용자 그룹 변경, 사용자 활성화 및 비활성화, 계정 패스워드 변경 등을 감사한다.

정답 2번

간단한 해설

②는 계정 인증과 해당 컴퓨터의 로그온을 혼동한 설명이다. **계정 로그온 이벤트**는 계정의 자격 증명 검증을 감사하며, 도메인 계정 인증은 도메인 컨트롤러에 기록된다.

선지별 해설

① O: 권한 사용 감사는 사용자에게 부여된 **특권을 행사하는 행위**를 추적한다. 관리자 권한이 필요한 시스템 작업에서 특권을 사용하는 경우가 이에 해당한다. 관리자 계정으로 로그인했다는 사실 자체와 작업 중 특권을 사용했다는 사실은 구별한다.

② X: 계정 로그온 이벤트를 '로컬 계정에 접근할 때 생성되는 이벤트'로 설명하면 로그온 이벤트와의 차이를 제대로 나타내지 못한다. 계정 로그온 감사의 기준은 **계정의 자격 증명 검증**이다. 도메인 계정은 이를 인증하는 도메인 컨트롤러에 계정 로그온 이벤트가 기록된다. 반면 로그온 이벤트는 사용자가 실제로 로그온하는 컴퓨터에서 세션의 생성·종료 등을 추적한다. 예를 들어 도메인 계정으로 업무용 PC에 로그인하면 계정 인증 기록은 도메인 컨트롤러에, 해당 PC의 로그온 기록은 PC에 남는다. 다만 로컬 계정을 로컬 컴퓨터가 인증할 때에도 계정 로그온 이벤트가 생성될 수 있으므로, 계정 로그온을 도메인 계정에만 한정해서는 안 된다.

③ O: 개체 액세스 감사는 파일, 디렉터리, 레지스트리 키, 프린터 같은 자원에 대한 접근 시도와 변경 작업을 추적한다. 실제 기록을 남기려면 감사 정책뿐 아니라 **대상 개체의 감사 조건**도 설정해야 한다. 시스템 액세스 제어 목록(SACL)에 감사할 사용자·작업·성공 또는 실패 조건을 지정하면, 그 조건에 해당하는 접근이 감사된다.

④ O: 계정 관리 감사는 **사용자·그룹 및 계정 설정의 변경**을 추적한다. 사용자와 그룹의 생성·변경·삭제, 그룹 구성원 추가·제거, 사용자 계정의 활성화·비활성화, 암호 설정·변경 등이 대상이다. 계정으로 로그인하는 행위와 계정 자체를 관리하는 행위를 구별한다.

NoteBase

문 20. 안티 리버싱 기법으로 프로그램의 실행 코드나 데이터를 압축 및 암호화하여 저장하는 기술은?

① 패킹
② 디컴파일
③ 시큐어 코딩
④ 안티 디버깅

정답 1번

간단한 해설

실행 코드나 데이터를 **압축·암호화한 형태로 저장**하여 원래 내용을 쉽게 분석하지 못하게 하는 것이 패킹이다.

공통 해설

패킹은 프로그램의 실행 코드나 데이터를 압축하거나 암호화하여 저장하는 기술이다. 핵심은 **저장된 코드·데이터의 형태를 바꾸어 원래 내용을 감추는 것**이며, 질문의 '압축 및 암호화하여 저장'이라는 설명이 이 정의에 해당한다.

패킹된 프로그램은 일반적으로 실행 과정에서 필요한 코드를 메모리에 풀거나 복호화한 뒤 실행한다. 따라서 저장된 실행 파일만 살펴보는 정적 분석에서는 원래 코드와 데이터를 바로 파악하기 어려워지므로, 역공학을 어렵게 하는 안티 리버싱 기법으로 사용된다.

NoteBase