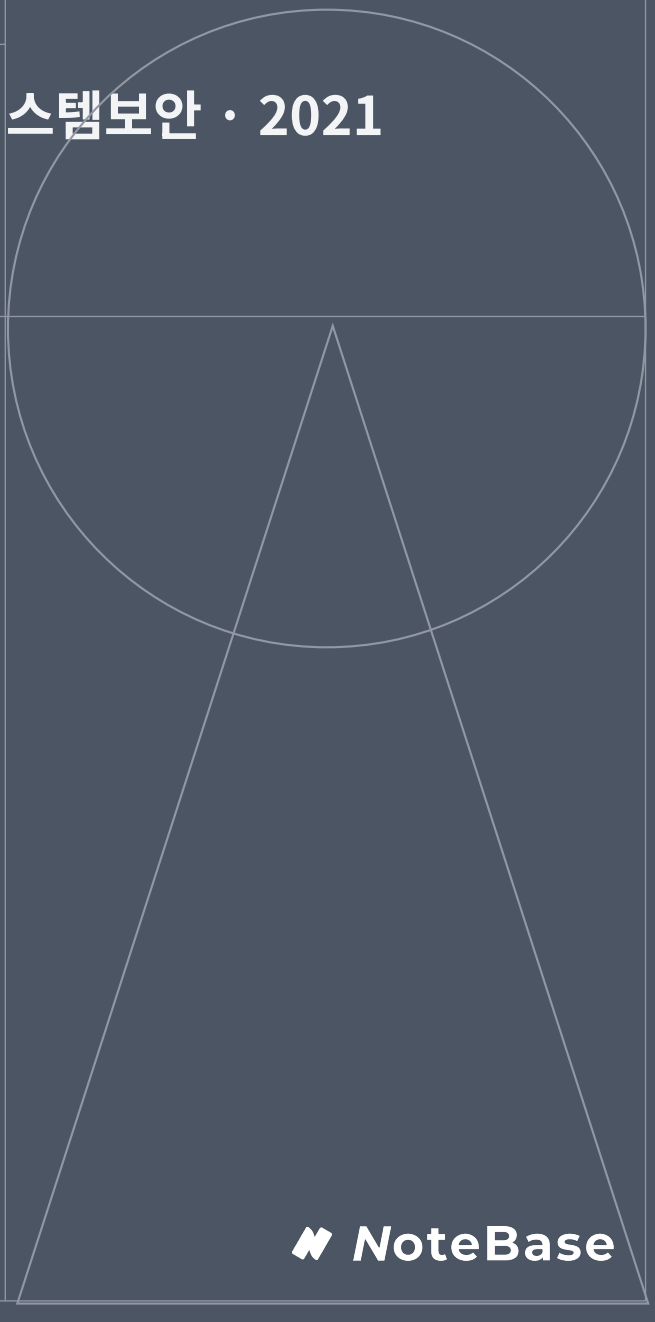
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2021



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2021

공무원/국가직/9급 · 정보시스템보안 · 2021

문 1. 다음에서 설명하는 보안시스템은?

◯ 해커를 유인해서 정보를 얻거나 잡으려고 설치하는 시스템이다.
◯ 쉽게 해킹이 가능한 것처럼 취약해 보여야 한다.
◯ 해커에게 쉽게 노출되어야 한다.
◯ 시스템의 모든 구성요소를 갖추고 있어야 한다.
◯ 시스템을 통과하는 모든 패킷을 감시해야 한다.

① 허니팟(honeypot)
② 텔넷(telnet)
③ 봇넷(botnet)
④ 샌드박스(sandbox)

정답 1번

간단한 해설

해커를 **미끼 시스템으로 유인**하여 공격 행위를 관찰하고 정보를 수집하는 것이 허니팟의 목적이다. 취약해 보이게 하고 쉽게 노출하는 것은 공격자의 접근을 유도하기 위한 것이다.

공통 해설

허니팟(honeypot)은 공격자가 침입 대상으로 여기도록 마련해 두고, 접근과 공격 행위를 관찰하여 공격 기법이나 공격자 관련 정보를 수집하는 미끼 시스템이다. 지문의 '해커를 유인해서 정보를 얻거나 잡으려고 설치한다'는 설명이 이러한 목적에 해당한다. 취약하게 보이고 쉽게 발견되도록 하는 이유도 **공격자의 접근과 공격을 유도**하기 위해서이다.

지문처럼 시스템 구성요소를 갖추는 것은 공격자가 실제 시스템으로 여기고 상호작용하도록 하기 위한 것이다. 시스템을 통과하는 모든 패킷을 감시하면 공격 과정에서 오가는 통신을 기록하고 분석할 수 있다. 이처럼 **유인한 뒤 활동을 관찰하는 목적**이 제시된 보안시스템을 허니팟으로 식별하는 기준이다.

NoteBase

문 2. 일반적인 리눅스 또는 유닉스 시스템의 디렉터리(directory)에 대한 설명으로 옳은 것은?

① /dev – 프로그램 실행 및 설치할 때 생성되는 임시 파일을 담고 있으며 임의로 삭제될 수 있다.

② /boot – 시스템 환경 설정 및 주요 설정 파일들을 담고 있다.

③ /usr/include – C 언어에서 사용되는 헤더 파일들을 담고 있다.

④ /usr – 각 계정으로 로그인할 때 이 디렉터리 밑에 자신의 홈 디렉터리가 작업 디렉터리가 된다.

정답 3번

간단한 해설

/usr/include는 C 프로그램을 컴파일할 때 사용하는 **헤더 파일**을 저장하는 디렉터리이다. 헤더 파일에는 함수 선언이나 자료형 정의 등이 담긴다.

선지별 해설

① X: /dev는 디스크나 터미널 같은 장치에 접근하기 위한 **장치 파일**을 담는 디렉터리이다. 프로그램 실행·설치 과정에서 생성되는 임시 파일을 저장하는 곳은 /tmp이며, 그 파일은 시스템의 정리 정책 등에 따라 삭제될 수 있다.

② X: /boot는 커널 이미지와 부트로더 관련 파일 등 **부팅에 필요한 파일**을 담는 디렉터리이다. 시스템 환경 설정과 주요 설정 파일을 담는 곳은 /etc이다.

③ O: /usr/include는 C 언어에서 사용하는 **헤더 파일**을 담는 디렉터리이다. 예를 들어 stdio.h에는 printf 같은 표준 입출력 함수의 선언이 있어, 컴파일러가 소스 코드의 함수 사용을 처리하는 데 이용한다.

④ X: /usr는 사용자 명령어, 라이브러리, 공유 데이터 등 프로그램 관련 파일을 담는 디렉터리이다. 로그인할 때 작업 디렉터리가 되는 곳은 **해당 계정에 지정된 홈 디렉터리**이며, 일반 사용자의 홈 디렉터리는 보통 /home/사용자명 형태로 배치된다.

NoteBase

문 3. 데이터베이스 보안에서 웹을 이용한 SQL 인젝션 공격 방지를 위한 시큐어 코딩(secure coding) 방법으로 옳지 않은 것은?

① 주석문에 시스템 주요 정보를 사용자가 볼 수 있도록 해야 한다.

② 애플리케이션에서 데이터베이스 연결을 수행할 때 최소 권한의 계정을 사용해야 한다.

③ 외부 입력값이 삽입되는 SQL 쿼리문의 구조가 변경되지 않도록 해야 한다.

④ 외부 입력값이 삽입되는 SQL 쿼리문은 특수문자를 필터링하여 입력값 검증을 수행해야 한다.

정답 1번

간단한 해설

사용자에게 전달되는 주석문에 시스템 주요 정보를 공개하면 공격자가 내부 구조를 파악하는 데 이용할 수 있다. 민감한 정보는 주석문에서 **제거하여 외부에 노출되지 않도록** 해야 한다.

선지별 해설

SQL 인젝션은 외부 입력값이 단순한 데이터가 아니라 SQL 구문의 일부로 해석되어 쿼리의 의도나 구조를 바꾸는 공격이다. 입력값 처리와 함께 정보 노출 및 데이터베이스 접근 권한도 관리해야 한다.

① X: 사용자에게 전달되는 HTML 등의 주석문은 화면에 표시되지 않더라도 소스 보기로 확인할 수 있다. 여기에 내부 경로나 데이터베이스 접속 정보 같은 시스템 주요 정보를 넣으면 공격에 필요한 단서를 제공한다. 따라서 '사용자가 볼 수 있도록'이 아니라 **민감한 정보를 제거하여 사용자가 볼 수 없도록** 해야 한다.

② O: 데이터베이스 연결 계정에는 **업무 수행에 필요한 최소 권한만** 부여해야 한다. 예를 들어 조회만 필요한 기능에는 필요한 테이블의 조회 권한만 부여한다. 이는 SQL 인젝션이 발생하더라도 불필요한 데이터 변경이나 삭제 등으로 피해가 확대되는 것을 제한한다.

③ O: 외부 입력값 때문에 SQL 쿼리문의 구조가 바뀌면 공격자가 조건이나 명령을 삽입할 수 있다. 이를 막으려면 **SQL 구문과 입력 데이터를 분리**해야 한다. 대표적으로 매개변수화된 쿼리를 사용하여 SQL 구조를 정해 두고 입력값을 별도의 매개변수로 전달하면, 입력값이 명령이 아닌 데이터로 처리된다.

④ O: 따옴표 등 SQL 구문에 영향을 줄 수 있는 특수문자를 검사하고, 입력 항목의 용도에 맞지 않는 입력을 제한하는 것은 입력값 검증 대책이다. 다만 **특수문자 필터링만으로 모든 SQL 인젝션을 막을 수는 없다**. 허용되는 형식과 값인지 검증하고, 매개변수화된 쿼리와 함께 적용해야 한다.

NoteBase

문 4. 중요 데이터에 대한 기밀성 또는 무결성을 제공하는 보안기술 중 복호화를 위한 키가 사용되는 알고리즘은?

① SHA-256

② MD5

③ AES

④ HAS-160

정답 3번

간단한 해설

AES는 암호문을 **키를 이용해 원래 데이터로 복원**할 수 있는 대칭키 암호 알고리즘이다. 해시 알고리즘과 달리 복호화 절차가 있다.

공통 해설

복호화는 암호화된 데이터를 원래의 평문으로 되돌리는 과정이다. AES는 **암호화와 복호화에 같은 비밀키**를 사용하는 대칭키 암호 알고리즘으로, 데이터를 암호문으로 바꾸어 기밀성을 제공하고 해당 키로 다시 평문을 복원할 수 있다. 따라서 문제의 '복호화를 위한 키가 사용되는 알고리즘'에 해당한다.

SHA-256, MD5, HAS-160은 입력 데이터로부터 해시값을 만드는 해시 알고리즘이다. 해시는 원문 복원을 목적으로 하지 않는 일방향 처리이므로 **해시값을 원문으로 되돌리는 복호화 절차와 복호화 키가 없다**. 이 구별이 네 후보를 판단하는 공통 기준이다.

NoteBase

문 5. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?

① 커버로스의 전반적인 기법은 신뢰하는 제3자 인증 서비스 방안이다.

② 커버로스 프로토콜은 인증 서버(authentication server), 티켓 발급 서버(ticket granting server) 및 사용자에게 서비스를 제공하는 다수의 서비스 서버(service server)를 사용한다.

③ 커버로스를 구성하는 개체 간에 교환되는 대부분의 메시지는 대칭키 암호화 기술로 기밀성이 보장된다.

④ 커버로스 버전 4에서 암호화된 메시지는 암호 알고리즘 식별자가 덧붙여진다. 이것은 사용자에게 DES가 아닌 다른 알고리즘을 사용할 수 있도록 한다.

정답 4번

간단한 해설

커버로스 버전 4는 **DES에 의존**한다. 암호 알고리즘 식별자를 두어 DES 이외의 알고리즘도 사용할 수 있게 한 것은 **버전 5**의 특징이다.

선지별 해설

① O: 커버로스는 사용자와 서비스 서버가 함께 신뢰하는 **제3자의 티켓을 이용해 신원을 확인**하는 인증 방식이다. 서비스 서버는 사용자가 제시한 티켓과 인증자를 검증하여 사용자의 신원을 확인한다.

② O: 인증 서버(AS)는 사용자의 최초 인증을 처리하고 티켓 발급 서버에 제시할 티켓인 TGT를 발급한다. 티켓 발급 서버(TGS)는 TGT와 인증자를 확인한 뒤 **개별 서비스 서버에 제시할 서비스 티켓**을 발급한다. 사용자는 이 서비스 티켓과 인증자를 서비스 서버에 제시하여 인증받는다.

③ O: 커버로스는 **공유 비밀키를 사용하는 대칭키 암호화**를 기본으로 한다. 티켓의 인증 정보는 해당 서버의 비밀키로, 인증자는 사용자와 서버가 공유하는 세션키로 암호화하여 보호한다. 다만 최초 티켓 요청처럼 암호화되지 않는 부분도 있으므로 모든 메시지 전체가 암호화된다는 뜻은 아니다.

④ X: 버전 4는 DES를 사용하도록 설계되어 다른 암호 알고리즘을 유연하게 선택하기 어렵다. 암호화된 데이터에 사용된 알고리즘을 나타내는 식별 필드를 두어 **DES 이외의 알고리즘도 지원하는 것은 버전 5**의 특징이다.
따라서 선지의 '커버로스 버전 4'를 '커버로스 버전 5'로 고쳐야 한다.

NoteBase

문 6. 다음 리눅스 시스템의 /etc/passwd 파일 내용에서 사용자의 권한 수준을 결정하는 항목은?

adm : x : 0 : 1 : administrator : /var/adm : /sbin/nologin

① adm

② x

③ 0

④ /sbin/nologin

정답 3번

간단한 해설

콜론으로 구분된 세 번째 항목은 **사용자 식별자(UID)**이다. 제시된 값 **0은 관리자(root) 권한**을 나타낸다.

핵심 풀이

UID와 권한: /etc/passwd의 필드는 콜론(:)으로 구분되며, 세 번째 필드가 사용자 식별자(UID)이다. 제시된 행에서는 그 값이 0이므로 슈퍼유저(root)에 해당한다. 계정명이 adm이어도 **UID가 0이면 관리자 권한**을 갖는다. 바로 뒤의 1은 기본 그룹 식별자(GID)로, UID와 구별한다.

계정명과 비밀번호 필드: 첫 번째 필드 adm은 로그인할 때 사용하는 계정명이다. 두 번째 필드 x는 **비밀번호 해시가 /etc/shadow에 저장되어 있음**을 나타내는 표시이며, 권한 수준을 나타내는 값이 아니다.

로그인 셸: 마지막 필드 /sbin/nologin은 일반적인 셸 로그인을 거부하도록 지정한 프로그램이다. 이는 **로그인 허용 여부**에 관한 설정이며, UID 0이라는 계정의 식별자나 관리자 권한 자체를 바꾸지는 않는다.

NoteBase

문 7. 리눅스 배시(bash) 셸에서 셸 변수 또는 환경 변수로 설정된 SHELL에 저장된 값을 출력하는 명령은?

① echo SHELL

② echo ‘$SHELL’

③ echo “$SHELL”

④ echo \$SHELL

정답 3번

간단한 해설

직선 큰따옴표로 묶은 echo "$SHELL"에서는 **변수 확장이 유지**되어 SHELL에 저장된 값이 출력된다. 공식 답 ③은 곡선 큰따옴표를 이 인용 방식의 표기로 해석한 것이다.

개념 구분

SHELL은 변수 이름이고, $SHELL은 그 변수의 값을 참조하는 표현이다. Bash는 변수 확장을 수행한 뒤 그 결과를 echo에 전달한다. 아래에서는 ②·③의 곡선 따옴표를 각각 직선 작은따옴표와 직선 큰따옴표를 나타낸 것으로 해석한다.

① echo SHELL: **변수 참조를 나타내는 $가 없으므로** 문자 SHELL을 출력한다. 변수 이름만 적는 것으로는 저장된 값을 가져오지 않는다.

② echo ‘$SHELL’: 직선 작은따옴표를 사용한 echo '$SHELL'은 **작은따옴표 안의 변수 확장을 막는다**. 따라서 저장된 값이 아니라 문자 $SHELL을 출력하며, 인용에 사용한 작은따옴표는 출력되지 않는다.

③ echo “$SHELL”: 직선 큰따옴표를 사용한 echo "$SHELL"은 **큰따옴표 안에서도 변수 확장을 허용한다**. 확장 결과는 하나의 인수로 전달되고 인용 부호는 제거된다. 예를 들어 SHELL의 값이 /bin/bash라면 /bin/bash가 출력된다.

④ echo \$SHELL: 인용되지 않은 백슬래시는 **바로 뒤 $의 특수 기능을 제거한다**. 이에 따라 변수 확장이 일어나지 않고 문자 $SHELL이 출력된다. 백슬래시 자체는 출력되지 않는다.

표기상의 한계: 곡선 따옴표 ‘ ’와 “ ”는 Bash의 인용 문자가 아니다. 원문 그대로 입력하면 ②와 ③ 모두 $SHELL이 확장되고 곡선 따옴표도 출력에 남는다. SHELL이 /bin/bash라면 각각 ‘/bin/bash’와 “/bin/bash”가 출력된다.

따라서 공식 채점 답은 ③이며, 이는 원문의 곡선 큰따옴표를 직선 큰따옴표 인용의 표기로 읽는 해석에 따른다.

NoteBase

문 8. 일반적으로 컴퓨터를 부팅할 때 운영체제를 주기억장치에 적재하는 부트 프로그램이 저장되는 디스크 공간은?

① BIOS(Basic Input Output System)

② POST(Power On Self Test)

③ MBR(Master Boot Record)

④ CMOS(Complementary Metal Oxide Semiconductor)

정답 3번

간단한 해설

전통적인 BIOS 기반 부팅에서 부팅을 시작하는 코드는 디스크 첫 섹터의 **MBR(Master Boot Record)**에 저장된다.

공통 해설

전통적인 BIOS/MBR 부팅 방식에서 MBR은 디스크의 첫 번째 섹터에 있는 레코드로, **초기 부트 코드와 파티션 정보**를 담는다. BIOS가 MBR을 주기억장치로 읽어 그 코드를 실행하면, 후속 부트 로더로 실행이 이어져 운영체제를 주기억장치에 적재하는 과정이 진행된다. 따라서 문항의 '부트 프로그램이 저장되는 디스크 공간'은 초기 부트 코드가 기록된 MBR을 가리킨다.

NoteBase

문 9. 다음은 보안관리 도구들에 대한 설명이다. ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

○ (㉠)는(은) 파일이나 디렉터리에 접근 권한을 제어할 수 있도록 한다.
○ (㉡)는(은) 사용자를 인증하고 그 사용자의 서비스에 대한 접근을 제어하는 모듈화된 방법이다.
○ (㉢)는(은) root 권한을 획득한 침입자에게 시스템의 모든 부분이 해킹당할 수 있는 위험을 보완하기 위해 만들어졌다.

① ㉠: ACL, ㉡: NMap, ㉢: PAM
② ㉠: ACL, ㉡: PAM, ㉢: SELinux
③ ㉠: NMap, ㉡: PAM, ㉢: SELinux
④ ㉠: NMap, ㉡: ACL, ㉢: PAM

정답 2번

간단한 해설

PAM은 **사용자 인증과 서비스 접근 제어를 모듈화**하는 방식이다. SELinux는 root 권한을 빼앗겼을 때 피해가 시스템 전체로 확산되는 위험을 **강제 접근 통제**로 줄인다.

빈칸별 해설

㉠ ACL: 접근 제어 목록(Access Control List)으로, 파일이나 디렉터리에 대해 **어떤 사용자·그룹에 어떤 접근 권한을 부여할지** 지정한다. 예를 들어 특정 사용자에게 한 파일의 읽기 권한만 부여하는 식으로 접근을 제어한다.

㉡ PAM: 장착형 인증 모듈(Pluggable Authentication Modules)로, 서비스가 사용자 인증과 계정 접근 허용 여부를 **설정된 모듈을 통해 처리**하도록 한다. 서비스마다 인증 기능을 따로 구현하는 대신 필요한 모듈을 연결할 수 있으므로, 지문의 '사용자 인증'과 '모듈화된 방법'에 대응한다.

㉢ SELinux: 보안 강화 리눅스(Security-Enhanced Linux)로, 기존의 파일 소유권·권한에 따른 접근 제어에 **보안 정책에 따른 강제 접근 통제(MAC)**를 추가한다. 정책을 강제하는 상태에서는 root 권한으로 실행되는 프로세스도 해당 정책의 제한을 받으므로, 침입자가 root 권한을 얻었을 때 허용되지 않은 자원으로 피해가 확산되는 것을 제한한다.

㉠은 ACL, ㉡은 PAM, ㉢은 SELinux이므로 이 대응을 모두 제시한 조합은 ②이다.

NoteBase

문 10. XSS 취약점 공격에 대비하여 필터링해야 할 특수문자만을 모두 고르면?

ㄱ. <
ㄴ. &
ㄷ. >
ㄹ. /

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

정답 4번

간단한 해설

XSS는 입력값이 웹 페이지에서 코드로 해석되어 실행될 때 발생한다. 태그와 문자 참조를 구성하는 특수문자를 **단순한 문자로 처리**해야 하며, 종료 태그에 쓰이는 **'/'도 처리 대상**에 포함된다.

NoteBase

보기별 해설

XSS는 신뢰할 수 없는 입력이 웹 페이지에 삽입되어 사용자의 브라우저에서 공격자의 코드로 실행되는 취약점이다. 이 문항은 입력 문자가 HTML 구문으로 해석되지 않도록 처리해야 할 대상을 묻는다.

ㄱ. O: '<'는 **HTML 태그의 시작**을 나타낸다. 입력값에 포함된 이 문자가 태그의 시작으로 해석되면 공격자가 삽입한 요소나 스크립트가 페이지의 일부로 처리될 수 있으므로 필터링 대상이다.

ㄴ. O: '&'는 **HTML 문자 참조의 시작**을 나타낸다. 문자 참조는 특정 문자를 다른 표기로 나타내는 방식이므로, 입력된 '&'가 의도하지 않은 문자 참조로 해석되지 않도록 처리해야 한다.

ㄷ. O: '>'는 **HTML 태그를 닫는 구분자**이다. '<'로 시작한 태그 구문을 완성하는 데 쓰이므로, 입력값이 HTML 구문으로 해석되지 않도록 처리할 대상에 포함된다.

ㄹ. O: '/'는 **HTML 종료 태그를 구성**하는 문자이다. 종료 태그에서는 '<' 바로 뒤에 놓여 해당 요소의 끝을 표시한다. 공격자가 기존 요소를 끝내고 다른 구문을 삽입하는 데 이용할 수 있으므로 이 문항의 필터링 대상에 포함된다.

따라서 처리 대상은 ㄱ · ㄴ · ㄷ · ㄹ 모두이며, 이 조합은 ④에 해당한다. 다만 이 문자들만 일괄 삭제한다고 모든 XSS가 차단되는 것은 아니다. 실제 방어에서는 입력값을 검증하고, 출력되는 위치가 HTML 본문인지 속성인지 JavaScript인지에 따라 알맞은 인코딩을 적용해야 한다.

NoteBase

문 11. 다음에서 설명하는 악성 프로그램은?

◯ 사용자의 동의 없이 설치되어 개인이나 기업의 정보를 몰래 수집하고 제3자 또는 공격자에게 전송하는 것을 목적으로 한다.
◯ 해당 악성 프로그램에 감염되면 웹 브라우저 및 시스템 설정의 변경, 정상적인 프로그램의 설치 방해, 컴퓨터 키보드 입력 내용이나 화면 표시 내용을 수집 및 전송하는 등의 증상이 있다.

① 랜섬웨어(ransomware)
② 스파이웨어(spyware)
③ 웜(worm)
④ 봇(bot)

정답 2번

간단한 해설

사용자 몰래 정보를 수집하여 외부로 전송하는 것은 **스파이웨어**의 핵심 기능이다. 키보드 입력 내용이나 화면 표시 내용을 수집·전송한다는 설명도 이러한 정보 유출 목적에 부합한다.

공통 해설

스파이웨어(spyware)는 사용자의 동의 없이 개인이나 기업의 정보를 몰래 수집하고 제3자나 공격자에게 전달하는 악성 프로그램이다. 이 문항의 식별 기준은 **은밀한 정보 수집과 외부 전송이라는 목적**이다. 키보드 입력 내용을 기록하거나 화면 표시 내용을 수집하면 사용자가 입력하거나 열람한 정보가 노출될 수 있으며, 이를 외부로 보내는 동작은 스파이웨어의 정보 유출 기능에 해당한다. 웹 브라우저·시스템 설정 변경이나 정상적인 프로그램의 설치 방해도 제시된 감염 증상이지만, 이러한 장애 자체보다 정보를 몰래 수집·전송한다는 설명이 명칭을 결정하는 핵심 단서이다.

NoteBase

문 12. 사용자 인증 또는 메시지 인증 프로토콜에서 재전송 공격(replay attack)을 방지하기 위한 정보로 옳지 않은 것은?

① 사용자 식별자(user identifier)

② 순서 번호(sequence number)

③ 타임스탬프(timestamp)

④ 비표(nonce)

정답 1번

간단한 해설

사용자 식별자는 **누구인지를 구분하는 정보**일 뿐, 지금 받은 메시지가 과거 메시지를 다시 보낸 것인지는 구별하지 못한다. 재전송 공격을 막으려면 메시지의 **최신성이나 중복 여부를 확인할 정보**가 필요하다.

개념 구분

재전송 공격은 공격자가 이전에 정상적으로 전송된 인증 정보나 메시지를 가로채 다시 보내는 공격이다. 내용이 변조되지 않았더라도 재사용될 수 있으므로, 수신자는 메시지가 현재의 통신에 속하는지 확인해야 한다. 이때 사용하는 정보는 메시지와 함께 인증되어 공격자가 임의로 바꾸지 못해야 한다.

사용자 식별자(user identifier)는 사용자를 구별하는 값이다. 같은 사용자가 여러 번 통신할 때에도 그대로 쓰일 수 있으므로, **사용자 식별자만으로는 새 메시지와 재전송된 메시지를 구분할 수 없다**.

순서 번호(sequence number)는 메시지에 순차적으로 부여하는 번호이다. 수신자가 이미 받은 번호를 기록하고 중복된 번호를 거부하면 재전송을 탐지할 수 있다. 예를 들어 10번 메시지를 처리한 뒤 같은 10번 메시지가 다시 오면 중복으로 판단한다.

타임스탬프(timestamp)는 메시지 생성 시각을 나타낸다. 수신자는 자신의 현재 시각과 비교하여 **허용 시간 범위를 벗어난 메시지**를 거부한다. 이를 위해 송수신자의 시계 오차를 고려해야 하며, 허용 시간 안에서의 재전송까지 막으려면 이미 받은 메시지인지도 검사해야 한다.

비표(nonce)는 한 번만 사용하는 값이다. 인증할 때마다 새로운 비표를 제시하고 응답이 그 값에 결합되어 있는지 확인하면, 과거 비표로 만든 응답은 현재 인증에 사용할 수 없다. 핵심은 **같은 비표를 재사용하지 않는 것**이다.

NoteBase

문 13. 데이터베이스 명령어는 DDL, DML, DCL 등으로 구분된다. 다음 중 DCL에 해당되는 명령어는?

① DROP

② UPDATE

③ SELECT

④ GRANT

정답 4번

간단한 해설

DCL은 데이터베이스에 대한 **사용 권한을 제어**하는 명령어이다. GRANT는 사용자에게 테이블 조회 등의 권한을 부여한다.

구성 요소별 해설

DROP → DDL: 테이블 같은 데이터베이스 객체를 삭제한다. 저장된 행의 값을 바꾸는 것이 아니라 **객체 자체를 제거**하므로 데이터 정의어인 DDL에 속한다.

UPDATE → DML: 테이블에 저장된 행의 열 값을 수정한다. 테이블의 구조나 사용자 권한이 아니라 **저장된 데이터의 내용**을 다루므로 데이터 조작어인 DML에 속한다.

SELECT → DML: 테이블에서 조건에 맞는 데이터를 조회한다. 데이터를 변경하지 않더라도 저장된 데이터를 검색하는 연산이므로, 이 문항의 DDL·DML·DCL 구분에서는 DML에 속한다.

GRANT → DCL: 사용자에게 데이터베이스 객체에 대한 접근·사용 권한을 부여한다. 예를 들어 특정 테이블을 조회할 권한을 주는 것은 데이터를 직접 조회하는 SELECT와 달리 **조회할 수 있는 권한을 설정**하는 작업이다.

따라서 DCL에 해당하는 명령어는 권한을 부여하는 GRANT이며, ④와 대응한다.

NoteBase

문 14. FTP 클라이언트에서 사용하는 명령어에 대한 설명으로 옳지 않은 것은?

① lcd - 지역 호스트의 작업 디렉터리를 변경한다.

② more - 여러 개의 파일들을 원격 호스트에서 지역 호스트로 가져온다.

③ hash - 파일이 전송되는 진행 상황을 알려주도록 설정한다.

④ bin - 전송 모드를 바이너리 모드로 설정한다.

정답 2번

간단한 해설

원격 호스트의 여러 파일을 지역 호스트로 가져오는 명령어는 more가 아니라 **mget**이다. mget에 가져올 파일들을 지정하면 여러 파일을 내려받을 수 있다.

선지별 해설

① O: lcd는 FTP 클라이언트를 실행한 **지역 호스트의 작업 디렉터리**를 변경한다. 원격 서버의 디렉터리를 바꾸는 명령이 아니라, 지역 컴퓨터에서 파일을 읽거나 저장할 기준 위치를 바꾸는 명령이다.

② X: 여러 파일을 원격 호스트에서 지역 호스트로 가져오는 명령은 **mget**이다. 예를 들어 'mget a.exe b.exe'는 원격 서버의 두 파일을 지역 컴퓨터로 가져온다. 따라서 선지의 'more'를 'mget'으로 고쳐야 한다.

③ O: hash는 파일을 전송할 때 데이터 블록이 전송될 때마다 **# 기호를 출력**하는 기능을 켜거나 끈다. 이 기능을 켜면 기호가 출력되는 모습을 통해 전송이 진행 중임을 확인할 수 있다.

④ O: bin은 binary의 축약형으로, 파일 전송 형식을 **바이너리 모드**로 설정한다. 문자나 줄바꿈 형식을 변환하지 않고 파일의 바이트를 그대로 전송하므로 실행 파일 등 원래 데이터를 보존해야 하는 파일의 전송에 사용한다.

NoteBase

문 15. 시스템 관리자가 윈도우즈 시스템에서 동작 중인 프로세스를 인지하고 있으면 웜, 바이러스 등에 대응하는 데 용이하다. 윈도우즈 기본 프로세스에 대한 설명으로 옳지 않은 것은?

① csrss.exe - 윈도우즈 콘솔을 관장하고 스레드를 생성 및 삭제하는 기능을 담당한다.

② svchost.exe - 시스템 서비스를 제어(시작 및 정지)하고 서비스 간에 상호작용하는 기능을 담당한다.

③ lsass.exe - winlogon 서비스에 필요한 인증 기능을 담당한다.

④ smss.exe - 사용자 세션을 시작하는 기능을 담당한다.

정답 2번

간단한 해설

서비스의 시작·정지를 관리하는 것은 **services.exe의 서비스 제어 관리자(SCM)**이다. svchost.exe는 **DLL 형태의 서비스를 불러와 실행하는 호스트 프로세스**이다.

선지별 해설

① O: csrss.exe는 Win32 하위 시스템의 사용자 모드 부분을 담당하는 클라이언트/서버 런타임 프로세스이다. 전통적인 Windows 구조에서 **콘솔 처리와 스레드 생성·삭제**를 담당한다.

② X: 서비스의 시작·정지 요청을 처리하고 서비스 상태를 관리하는 주체는 **services.exe의 서비스 제어 관리자(SCM)**이다. svchost.exe는 **DLL 형태의 서비스를 불러와 실행하는 호스트 프로세스**이다. 서비스 제어 기능과 서비스를 실행하는 호스트의 역할을 혼동한 설명이다.

③ O: lsass.exe는 로컬 보안 권한 하위 시스템 서비스로, **사용자 인증**을 담당한다. winlogon.exe를 통해 전달된 로그인 자격 증명을 인증하는 등 로그온 과정에 필요한 보안 기능을 수행한다.

④ O: smss.exe는 **세션 관리자**로, 사용자 세션을 생성하고 초기화한다. 세션은 사용자별 실행 환경을 구분하는 단위이며, smss.exe는 세션에 필요한 시스템 프로세스가 실행되도록 준비한다.

NoteBase

문 16. 다음에서 설명하는 웹 취약점은?

◯ OWASP에서 2017년에 발표한 웹 관련 주요 10대 취약점 중 하나이다.
◯ 이 취약점은 인증된 사용자가 수행할 수 있는 것에 대한 제한이 제대로 적용되지 않는다는 것이다.
◯ 공격자는 다른 사용자의 계정 접근, 민감한 파일 보기, 다른 사용자의 데이터 수정, 접근 권한 변경 등의 불법 행위가 가능하다.

① Broken Authentication
② Broken Access Control
③ Insufficient Logging & Monitoring
④ Sensitive Data Exposure

정답 2번

간단한 해설

이미 인증된 사용자라도 **허용된 권한을 벗어난 행위**는 제한되어야 한다. 이 제한이 제대로 적용되지 않아 다른 사용자의 데이터나 기능에 접근할 수 있는 취약점이 접근 통제 실패(Broken Access Control)이다.

공통 해설

접근 통제는 사용자의 권한에 따라 이용할 수 있는 자원과 수행할 수 있는 행위를 제한하는 것이다. OWASP Top 10 2017의 접근 통제 실패(Broken Access Control)는 이 제한이 제대로 적용되지 않아 권한 밖의 정보나 기능을 이용할 수 있는 취약점이다. 인증이 사용자의 신원을 확인하는 것이라면, 접근 통제는 **그 사용자가 해당 행위를 할 권한이 있는지**를 확인하고 제한한다. 따라서 로그인에 성공했더라도 모든 계정·파일·기능에 접근할 수 있는 것은 아니다.

지문의 핵심은 '인증된 사용자'에게도 적용되어야 할 행위 제한이 작동하지 않는다는 점이다. 다른 사용자의 계정이나 민감한 파일에 접근하거나, 다른 사용자의 데이터를 수정하거나, 접근 권한을 변경하는 행위는 모두 허용된 권한의 범위를 벗어나는 사례이다. 이를 막지 못하는 공통 원인이 접근 통제 실패이다.

NoteBase

문 17. S/MIME에서 사용되는 기술만을 모두 고르면?

ㄱ. RSA
ㄴ. SHA-1
ㄷ. DSS
ㄹ. EAP

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄴ, ㄷ, ㄹ

정답 3번

간단한 해설

S/MIME는 메시지 암호화와 전자서명을 통해 전자우편을 보호한다. **EAP는 네트워크 접속 인증을 위한 프레임워크**이므로 S/MIME의 암호화·서명 기술에 해당하지 않는다.

NoteBase

보기별 해설

S/MIME는 MIME 형식의 전자우편에 암호화와 전자서명 기능을 제공한다. 이 문항은 SHA-1과 DSA 기반 서명을 지원하던 S/MIME 3.1의 기술 구성을 기준으로 판단한다.

ㄱ. O: RSA는 공개키 암호 기술로, S/MIME에서 **메시지 암호화에 사용한 대칭키를 보호**하거나 전자서명을 생성·검증하는 데 사용한다. 메시지 본문 전체를 RSA로 암호화하는 방식과는 구별한다.

ㄴ. O: SHA-1은 해시 함수로, 메시지를 입력받아 **전자서명에 사용할 메시지 다이제스트**를 만든다. 수신자는 메시지의 다이제스트를 계산하고 서명을 검증하여 변조 여부를 확인한다. SHA-1 자체가 메시지를 암호화하는 것은 아니다.

ㄷ. O: DSS는 전자서명 표준이다. 이 문항의 DSS는 DSA 기반 전자서명 기술을 가리키며, S/MIME에서 서명자의 인증과 메시지 무결성 확인에 사용된다. **전자서명 기술**이므로 메시지 내용을 감추는 암호화 기술과 역할이 다르다.

ㄹ. X: EAP는 여러 인증 방식을 수용하는 확장 가능 인증 프레임워크로, PPP나 IEEE 802 계열 네트워크의 **접속 인증**에 사용한다. S/MIME에서 메시지를 암호화하거나 전자서명하는 기술에는 해당하지 않는다.

S/MIME에 사용되는 기술은 ㄱ, ㄴ, ㄷ이므로 ③의 조합에 해당한다.

NoteBase

문 18. PGP 시스템에서 제공하는 기능에 대한 구현 기술로 옳지 않은 것은?

① 키 교환 - HDLC

② 전자 서명 - RSA

③ 메시지 암호화 - Triple DES

④ 메시지 압축 - ZIP

정답 1번

간단한 해설

HDLC는 **데이터 링크 계층의 통신 제어 프로토콜**로, PGP의 키 교환 기술이 아니다. PGP는 메시지 암호화에 쓴 세션 키를 **수신자의 공개키로 암호화**하여 전달하며, 여기에 RSA 같은 공개키 암호 기술을 사용한다.

선지별 해설

① X: HDLC는 데이터 링크 계층에서 프레임을 구성하고 전송을 제어하는 프로토콜이다. PGP의 키 전달에는 HDLC가 아니라 **RSA 같은 공개키 암호 기술**을 사용한다. 송신자는 메시지 암호화용 세션 키를 수신자의 공개키로 암호화해 보내고, 수신자는 자신의 개인키로 이를 복호화하여 세션 키를 얻는다.

② O: RSA는 PGP의 전자 서명을 구현하는 데 사용할 수 있다. 송신자는 메시지의 해시값을 바탕으로 **자신의 개인키로 서명**하고, 수신자는 송신자의 공개키로 서명을 검증한다. 이를 통해 메시지가 변조되었는지와 해당 개인키 보유자가 서명했는지를 확인한다.

③ O: Triple DES는 PGP에서 메시지 내용을 암호화하는 데 사용하는 **대칭키 암호 알고리즘**이다. 메시지 본문은 세션 키로 암호화하며, 이 세션 키를 수신자에게 안전하게 전달하는 공개키 암호의 역할과 구분된다.

④ O: ZIP은 PGP의 메시지 압축에 사용하는 기술이다. **암호화 전에 메시지를 압축**하여 데이터의 중복을 줄이고 전송할 크기를 줄일 수 있다. 수신자는 복호화한 뒤 압축을 풀어 원래 메시지를 복원한다.

NoteBase

문 19. 아파치 웹 서버의 httpd.conf 파일의 주요 설정에 대한 설명으로 옳지 않은 것은?

① ServerTokens – 웹 서버, OS, 모듈 등의 정보 레벨을 지정한다.

② User/Group – 모듈 활성화 여부를 지정한다.

③ DocumentRoot – 웹 서버가 공개하는 디렉터리 트리에서 최상위 디렉터리를 지정한다.

④ UserDir – 일반 사용자의 공개 디렉터리를 지정한다.

정답 2번

간단한 해설

User와 Group은 모듈 활성화 여부가 아니라 요청을 처리하는 프로세스의 **사용자 계정과 그룹**을 지정한다. 동적 모듈을 불러와 활성 모듈 목록에 추가하는 지시어는 **LoadModule**이다.

선지별 해설

① O: ServerTokens는 HTTP 응답의 Server 헤더에 포함할 **서버 정보의 공개 범위**를 지정한다. 설정 수준에 따라 Apache의 제품명만 표시하거나 버전, 운영체제, 모듈 정보까지 표시할 수 있다.

② X: User는 클라이언트 요청을 처리하는 프로세스의 사용자 계정을, Group은 그룹을 지정한다. 즉, 어떤 사용자·그룹 권한으로 요청을 처리할지를 정하는 설정이다. '모듈 활성화 여부를 지정한다'는 설명은 **요청 처리 프로세스의 사용자 계정과 그룹을 지정한다**로 고쳐야 한다. 동적 모듈을 불러와 활성 모듈 목록에 추가하는 데에는 LoadModule을 사용한다.

③ O: DocumentRoot는 웹에서 제공할 기본 문서 트리의 **최상위 디렉터리**를 지정한다. 별도의 경로 매핑이 없다면 요청 경로를 이 디렉터리 뒤에 붙여 파일을 찾는다. 예를 들어 DocumentRoot가 '/var/www/html'이면 '/index.html' 요청은 '/var/www/html/index.html'에 대응한다.

④ O: UserDir는 **사용자별 웹 공개 디렉터리**를 지정한다. 예를 들어 'UserDir public_html'로 설정하면 '/~사용자명/' 형태의 요청을 해당 사용자의 홈 디렉터리 아래 public_html에 연결한다. User가 요청 처리 프로세스의 계정을 정하는 것과 달리, UserDir는 사용자별 콘텐츠의 위치를 정한다.

NoteBase

문 20. 다음에서 설명하는 무선 랜 보안기술 ㉠, ㉡을 바르게 연결한 것은?

○ (㉠)는(은) 사전에 공유된 비밀키를 사용하며 RC4 스트림 암호화 알고리즘과 24비트 초기화 벡터를 사용한다.
○ (㉡)는(은) 사전에 공유된 비밀키를 사용하거나 별도의 인증 서버를 이용하며 TKIP 기법을 통해 암호화 기능을 제공한다.

① ㉠: WAP, ㉡: WPA
② ㉠: WPA, ㉡: WAP
③ ㉠: WPA, ㉡: WEP
④ ㉠: WEP, ㉡: WPA

정답 4번

간단한 해설

RC4와 **24비트 초기화 벡터**를 함께 사용하는 방식은 WEP이다. 사전 공유키 방식 또는 인증 서버를 이용하는 방식을 지원하고 **TKIP**로 암호화를 제공하는 기술은 WPA이다.

빈칸별 해설

㉠ WEP: WEP는 사전에 공유한 비밀키와 **24비트 초기화 벡터(IV)**를 결합하여 RC4 암호화에 사용할 키를 구성한다. IV는 RC4 키 스트림을 초기화하는 데 쓰이는 값이다. 따라서 ㉠의 RC4와 24비트 IV라는 조건은 WEP에 해당한다.

㉡ WPA: WPA는 사전 공유키를 사용하는 개인용 방식과 **별도의 인증 서버를 이용하는 기업용 방식**을 지원한다. TKIP는 RC4를 바탕으로 패킷별 키 혼합 등을 적용하여 WEP의 취약점을 보완하는 기법이다. RC4 사용 자체는 두 기술의 공통점이므로, ㉡에서는 TKIP를 사용한다는 조건이 WPA를 식별하는 단서이다.

㉠은 WEP, ㉡은 WPA이므로 이 대응을 제시한 ④와 일치한다.

NoteBase