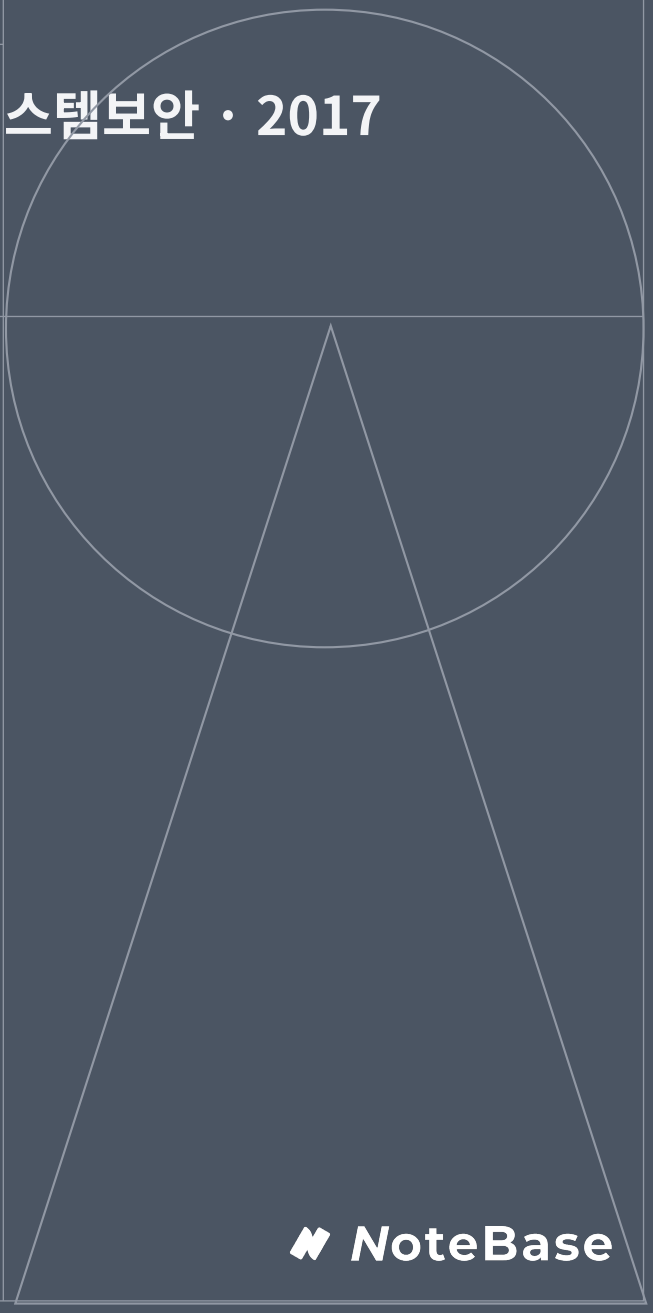
기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2017



NoteBase

기출OX 해설집

공무원/국가직/9급 · 정보시스템보안 · 2017

공무원/국가직/9급 · 정보시스템보안 · 2017

문 1. 사용자와 시스템 또는 시스템 간의 활성화된 접속을 관리하는 시스템 보안 기능은?

① 계정과 패스워드 관리

② 세션 관리

③ 파일 관리

④ 로그 관리

정답 2번

간단한 해설

사용자와 시스템 또는 시스템 사이에 유지되는 활성 접속을 세션이라 한다. 이 접속을 생성·유지·종료하는 기능이 **세션 관리**이다.

공통 해설

세션은 사용자와 시스템 또는 시스템 사이에서 접속이 성립한 뒤 유지되는 논리적인 연결 상태이다. 세션 관리는 **현재 활성화된 접속의 생성·유지·종료**를 통제하는 기능이므로, 문제에서 설명한 관리 대상과 일치한다. 계정 정보·파일·로그라는 관리 대상과 구별하여, 접속 자체를 관리한다는 점이 판단 기준이다.

예를 들어 로그인 후 서비스를 이용하는 동안 세션을 유지하고, 로그아웃하면 해당 세션을 종료한다. 일정 시간 활동이 없는 세션을 만료시키도록 설정하는 것도 방치된 접속의 악용을 줄이는 세션 관리에 해당한다.

NoteBase

문 2. 쿠키(cookie)에 대한 설명으로 옳지 않은 것은?

① 쿠키에 저장되는 내용은 각각의 웹사이트 별로 다를 수 있다.

② 쇼핑몰 사이트에서 장바구니 시스템을 이용할 때 쿠키 정보를 이용한다.

③ 쿠키는 바이러스를 스스로 전파한다.

④ 쿠키를 이용하면 사용자들의 특정 사이트 방문 여부 확인이 가능하다.

정답 3번

간단한 해설

쿠키는 브라우저에 저장되는 **데이터**이며, 스스로 실행되거나 복제되는 프로그램이 아니다. 따라서 쿠키 자체가 **바이러스를 스스로 전파하지는 않는다**.

선지별 해설

① O: 웹사이트는 서비스 목적에 따라 쿠키의 이름과 값을 정한다. 따라서 **사이트마다 저장하는 내용이 다를 수 있다**. 예를 들어 어떤 사이트는 언어 설정을, 다른 사이트는 이용자를 구별하는 식별자를 저장할 수 있다.

② O: 쿠키는 서로 분리된 웹 요청을 **같은 이용자의 요청으로 연결**하는 데 쓰인다. 예를 들어 브라우저의 쿠키에 저장된 세션 식별자로 서버의 장바구니를 찾아, 다른 페이지로 이동해도 담아 둔 상품을 유지할 수 있다. 장바구니 상품 정보 전체를 반드시 쿠키에 저장해야 하는 것은 아니다.

③ X: 쿠키는 웹사이트와 브라우저 사이에서 주고받고 저장하는 데이터이므로 **자체적인 실행·자기복제 기능이 없다**. 따라서 '바이러스를 스스로 전파한다'는 설명은 틀리다. 쿠키는 이용 상태 등을 유지하는 데 쓰이는 데이터이며, 스스로 바이러스를 전파하는 프로그램이 아니다.

④ O: 사이트가 이전 방문 때 저장한 쿠키를 이후 요청에서 받으면, 그 식별자를 이용해 **이전에 방문한 브라우저인지 확인**할 수 있다. 이는 쿠키가 유지되고 해당 사이트에 전송되는 범위에서 가능하며, 쿠키만으로 이용자의 실제 신원이나 모든 사이트의 방문 기록을 알 수 있다는 뜻은 아니다.

NoteBase

문 3. 웹 애플리케이션에 대한 보안 취약점을 이용한 공격으로 옳지 않은 것은?

① Shoulder Surfing

② Cross Site Scripting

③ SQL Injection

④ Cross Site Request Forgery

정답 1번

간단한 해설

Shoulder Surfing은 화면이나 키보드 입력을 **어깨너머로 훔쳐보아 정보를 얻는 공격**이다. 웹 애플리케이션의 프로그램상 취약점을 이용하는 공격에 해당하지 않는다.

선지별 해설

① X: Shoulder Surfing은 사용자의 화면이나 키보드 입력을 엿보아 비밀번호 등의 정보를 얻는 공격이다. 웹 애플리케이션의 취약점을 악용하는 것이 아니라 **사용자의 정보 입력·열람 장면을 관찰**하는 사회공학적 공격에 해당한다.

② O: Cross Site Scripting(XSS)은 웹 페이지에 공격자가 넣은 악성 스크립트가 **다른 사용자의 브라우저에서 실행**되도록 하는 공격이다. 웹 애플리케이션이 신뢰할 수 없는 입력을 안전하게 처리하지 않고 페이지에 포함하는 등의 취약점을 이용한다.

③ O: SQL Injection은 웹 애플리케이션의 입력값이 SQL 명령의 일부로 해석되는 취약점을 이용하여 **데이터베이스 질의를 변조**하는 공격이다. 입력 데이터와 SQL 명령을 안전하게 분리하지 않으면, 공격자가 의도한 조건이나 명령이 실행되어 정보가 유출되거나 데이터가 변경될 수 있다.

④ O: Cross Site Request Forgery(CSRF)는 로그인한 사용자의 브라우저가 **사용자가 의도하지 않은 요청을 전송**하도록 유도하는 공격이다. 쿠키 등의 인증정보가 요청에 함께 전송되는 상황에서, 웹 애플리케이션이 요청의 정당성을 충분히 검증하지 않으면 사용자의 권한으로 정보 변경 등의 처리가 이루어질 수 있다.

NoteBase

문 4. FTP 서버가 데이터를 전송할 때 목적지가 어디인지 검사하지 않는 설계상의 문제점을 이용한 FTP 공격 유형은?

① FTP Bounce 공격

② Land 공격

③ TFTP 공격

④ Smurf 공격

정답 1번

간단한 해설

FTP 서버가 클라이언트가 지정한 다른 호스트로 데이터를 보내도록 하는 기능을 악용한 것이 **FTP Bounce 공격**이다. 전송 목적지를 적절히 검사하지 않으면 공격자는 FTP 서버를 경유해 제3의 호스트에 접속하거나 데이터를 보낼 수 있다.

공통 해설

FTP는 명령을 주고받는 제어 연결과 실제 데이터를 전송하는 데이터 연결을 따로 사용한다. 능동 모드에서는 클라이언트가 PORT 명령으로 데이터 연결의 목적지 주소와 포트를 알려 주면 서버가 그 목적지로 연결한다. 이때 서버가 **제어 연결의 상대와 다른 호스트를 목적지로 지정하는 요청**까지 제한 없이 허용하면, 공격자는 서버를 제3의 호스트에 접속시키는 중계 수단으로 악용할 수 있다. 이 취약한 동작을 이용하는 공격이 FTP Bounce 공격이다.

예를 들어 공격자 A가 FTP 서버 B에 접속한 뒤 전송 목적지를 별도의 호스트 C로 지정하면, 목적지 검사가 미흡한 B는 A 대신 C로 연결하여 데이터를 보낼 수 있다. 여기서 핵심은 **공격자가 대상에 직접 연결하지 않고 FTP 서버를 경유한다**는 점이다. 문제의 '데이터 전송 목적지를 검사하지 않는 설계상의 문제점'은 바로 이러한 제3자 전송 기능의 악용을 가리킨다.

NoteBase

문 5. 웹 취약점 중 디렉터리 탐색을 차단하기 위해 사용자 입력 문자열에 필터링을 적용하는 특수 문자는?

① $

② /

③ --

④ >

정답 2번

간단한 해설

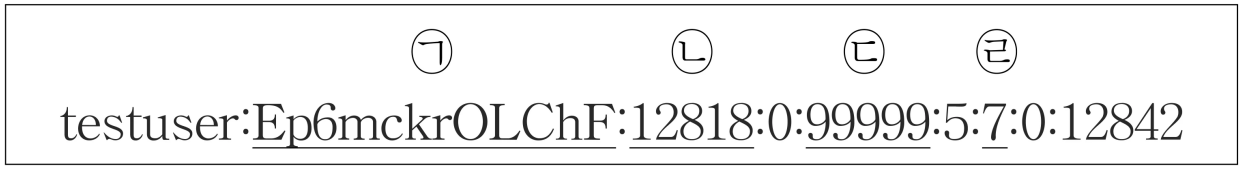
디렉터리 탐색 공격은 '../' 같은 경로 표현을 이용해 허용된 디렉터리 밖의 파일에 접근한다. 이때 **'/'는 디렉터리를 구분하는 문자**이므로 필터링 대상이 된다.

공통 해설

디렉터리 탐색은 사용자 입력을 파일 경로로 처리할 때, 공격자가 경로를 조작하여 허용된 디렉터리 밖의 파일에 접근하는 공격이다. 경로에서 **'/'는 디렉터리 구분자**이고, '..'는 상위 디렉터리를 뜻한다. 예를 들어 '../report.txt'는 상위 디렉터리에 있는 report.txt를 지정하므로, '../'를 반복하면 더 위의 디렉터리를 가리킬 수 있다. 따라서 문항에서 묻는 특수 문자는 이러한 경로 구성에 쓰이는 '/'이다.

NoteBase

문 6. 리눅스 시스템에서 /etc/shadow 파일 내용에 대한 설명으로 옳지 않은 것은?



① ㉠ - 암호화된 패스워드

② ㉡ - 최근 패스워드 바꾼 날

③ ㉢ - 현재 패스워드의 유효기간

④ ㉣ - 패스워드 만료 전 유저에게 바꿀 것을 경고하는 기간

정답 4번

간단한 해설

㉣의 7은 **패스워드 만료 후의 비활성 기간**이다. 만료 전에 변경을 경고하는 기간은 바로 앞 필드의 **5일**이다.

선지별 해설

/etc/shadow의 각 행은 콜론(:)으로 필드를 구분한다. 사용자 이름을 첫 번째 필드로 세어 각 값의 위치와 의미를 대응시킨다.

① O: ㉠은 사용자 이름 다음에 오는 두 번째 필드로, **암호화된 패스워드**를 저장한다. 일반적으로 평문 패스워드 자체가 아니라 인증에 사용하는 해시값을 담는다.

② O: ㉡의 12818은 세 번째 필드로, **마지막 패스워드 변경일**을 나타낸다. 날짜를 연월일로 직접 쓰는 대신 1970년 1월 1일을 기준으로 경과한 일수로 기록한다.

③ O: ㉢의 99999는 다섯 번째 필드로, 마지막 변경일로부터 패스워드를 사용할 수 있는 **최대 사용 일수**를 나타낸다. 이 기간이 지나면 패스워드 변경이 요구되므로, 현재 패스워드의 유효기간이라는 설명에 해당한다.

④ X: ㉣의 7은 일곱 번째 필드로, **패스워드가 만료된 뒤 로그인이 제한될 때까지의 기간**을 뜻한다. 만료 후 7일 동안 패스워드를 변경하지 않으면 로그인이 제한된다. 선지의 '만료 전 유저에게 바꿀 것을 경고하는 기간'은 여섯 번째 필드인 5에 해당하며, 만료 5일 전부터 경고한다.

NoteBase

문 7. 사용자의 계정명, 로그인한 시간, 로그아웃한 시간, 터미널 번호나 IP주소를 출력하는 유닉스 시스템 명령어는?

① last
② lastcomm
③ acctcom
④ chown

정답 1번

간단한 해설

last는 **로그인·로그아웃 이력**을 조회하는 명령어이다. 사용자 계정명, 접속 터미널이나 원격 접속지, 로그인·로그아웃 시각을 통해 누가 언제 어디서 접속했는지 확인할 수 있다.

공통 해설

last는 로그인·로그아웃 기록 파일을 읽어 **사용자별 접속 세션**을 출력한다. 세션은 한 번 로그인한 뒤 로그아웃할 때까지의 접속 단위를 뜻한다. 출력에는 계정명, 터미널, 원격 접속지의 호스트명이나 IP 주소, 로그인·로그아웃 시각과 접속 지속 시간 등이 나타난다. 따라서 발문처럼 사용자의 접속 시작과 종료, 접속 위치를 함께 확인하는 기능에 해당한다. 아직 종료되지 않은 세션은 로그아웃 시각 대신 접속 중임이 표시될 수 있다.

NoteBase

문 8. 다음에서 설명하는 보안 공격은?

유닉스 시스템에서 관리자 권한으로 실행되는 프로그램 중간에 임시 파일을 만드는 프로세스가 있을 경우 임시 파일 이름의 심볼릭 링크(Symbolic link) 파일을 생성하고, 이 프로세스 실행 중에 끼어들어 그 임시 파일을 전혀 엉뚱한 파일과 연결하여 악의적인 행동을 수행하도록 하는 공격이다.

① Fingerprinting 공격

② Race Condition 공격

③ Session Hijacking 공격

④ Heartbleed 공격

정답 2번

간단한 해설

관리자 권한 프로그램이 임시 파일에 접근하기 전에 심볼릭 링크를 조작하여 다른 파일을 처리하게 만든다.
이처럼 **프로세스의 실행 순서와 시점**을 악용하는 것이 경쟁 조건(Race Condition) 공격이다.

공통 해설

경쟁 조건(Race Condition)은 여러 프로세스나 스레드가 같은 자원에 접근할 때 **실행 순서나 시점에 따라 처리 결과가 달라지는 상황**이다. 공격자는 정상 프로그램의 작업 사이에 끼어들어 자원의 상태를 바꾸고, 프로그램이 의도하지 않은 처리를 하도록 유도한다.

심볼릭 링크는 다른 파일이나 경로를 가리키는 파일이다. 지문에서는 관리자 권한 프로그램이 사용할 임시 파일 이름에 심볼릭 링크를 만들고, 프로그램이 그 경로를 실제로 사용하는 시점에 다른 파일로 연결되도록 한다.
프로그램이 링크를 따라 접근하면 임시 파일 대신 공격자가 지정한 파일에 관리자 권한으로 작업할 수 있다.
핵심은 링크 자체가 아니라 **프로그램의 파일 접근과 공격자의 링크 조작 사이의 시간차**를 이용한다는 점이므로, 설명된 공격은 Race Condition 공격에 해당한다.

NoteBase

문 9. <보기 1>의 리눅스 패킷 필터링 요청 정책에 따른 <보기 2>의 ㉠~㉢에 들어갈 iptables의 명령어를 바르게 연결한 것은?

<보기 1>
INPUT 체인에 입력 인터페이스가 eth0이고, 도착지가 192.168.10.10이고, 프로토콜은 tcp이며, 도착 포트는 80인 패킷은 버리는 정책을 추가
<보기 2>
iptables -A INPUT -i eth0 (㉠) 192.168.10.10
(㉡) tcp (㉢) 80 -j DROP

① ㉠: --ip, ㉡: -proc, ㉢: -p

② ㉠: --ip, ㉡: -p, ㉢: --port

③ ㉠: -d, ㉡: -proc, ㉢: --dport

④ ㉠: -d, ㉡: -p, ㉢: --dport

정답 4번

간단한 해설

iptables에서 도착지 IP 주소는 **-d**, 프로토콜은 **-p**, 도착 포트는 **--dport**로 지정한다. 따라서 주소·프로토콜·포트 조건을 각각 -d 192.168.10.10, -p tcp, --dport 80으로 표현한다.

빈칸별 해설

-A INPUT은 INPUT 체인의 끝에 규칙을 추가하고, -i eth0은 입력 인터페이스를 eth0으로 제한한다. 여기에 도착지 주소·프로토콜·도착 포트 조건을 함께 지정하면, 이 조건들을 모두 만족하는 패킷이 해당 규칙과 일치할 때 -j DROP에 따라 폐기된다.

㉠ -d: 도착지 IP 주소를 지정하는 옵션이다. -d 192.168.10.10은 패킷의 **목적지 IP 주소**가 192.168.10.10이라는 조건을 나타낸다. 긴 옵션명은 --destination이며, 제시된 --ip를 쓰는 자리가 아니다.

㉡ -p: 패킷의 프로토콜을 지정하는 옵션이다. -p tcp는 **TCP 패킷**을 대상으로 한다. 긴 옵션명은 --protocol이며, -proc가 아니다. -p는 포트 번호를 지정하는 옵션과 구별해야 한다.

㉢ --dport: 도착 포트를 지정하는 옵션이다. -p tcp 뒤의 --dport 80은 TCP 패킷의 **목적지 포트가 80**이라는 조건을 나타낸다. 긴 옵션명은 --destination-port이며, 제시된 --port나 프로토콜 지정용 -p로 대신할 수 없다.

㉠ -d, ㉡ -p, ㉢ --dport의 조합은 ④와 일치한다.

NoteBase

문 10. 유닉스 시스템에 기록되는 로그파일에 대한 설명을 바르게 연결한 것은?

(가) 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보를 기록
(나) 사용자의 로그인, 로그아웃 시간과 시스템의 종료 시간, 시작 시간을 기록
(다) FTP 접속을 기록

① (가): wtmp, (나): pacct, (다): loginlog
② (가): wtmp, (나): loginlog, (다): xferlog
③ (가): pacct, (나): loginlog, (다): wtmp
④ (가): pacct, (나): wtmp, (다): xferlog

정답 4번

간단한 해설

프로그램 실행 이력을 남기는 **pacct**와 로그인·로그아웃 및 시스템 시작·종료 이력을 남기는 **wtmp**는 기록 대상이 다르다. 사용자가 접속한 시점과 접속 후 실행한 프로그램을 구분해야 한다.

대응 관계 해설

(가) pacct: 사용자가 수행한 **프로그램의 실행 정보**를 기록하는 프로세스 회계 로그이다. 프로세스 회계 기능이 활성화되어 있으면 프로세스가 종료될 때 실행 정보를 남긴다. 따라서 로그인한 사용자가 어떤 프로그램을 실행했는지를 기록한다는 설명에 대응한다.

(나) wtmp: 사용자의 **로그인·로그아웃 이력**과 시스템의 시작·종료 이력을 누적하여 기록한다. 프로그램별 실행 내역을 기록하는 pacct와 달리, 사용자가 언제 접속하고 접속을 마쳤는지와 시스템이 언제 시작·종료되었는지를 확인하는 로그이다.

(다) xferlog: FTP 서비스의 **파일 전송 내역**을 기록하는 로그이다. 전송 시각, 접속한 원격 호스트, 파일명, 전송량 등의 정보를 남기므로 FTP 접속에 관한 (다)의 설명에 대응한다.

세 설명을 각각 pacct, wtmp, xferlog로 연결한 ④가 이 대응에 해당한다.

NoteBase

문 11. 다음에서 설명하는 공격방법은?

◯ 버퍼 오버플로우 공격과 유사하며 C언어가 생기면서부터 존재했지만, 발견에 많은 시간이 소요되었다.
◯ 데이터의 형태와 길이에 대한 불명확한 정의로 인한 공격이다.

① Reverse Telnet
② Hypervisor
③ Format String
④ RootKit

정답 3번

간단한 해설

포맷 스트링(Format String) 공격은 외부 입력을 단순한 데이터가 아니라 **서식 지정자로 해석**하게 만드는 취약점을 이용한다. C언어의 출력 함수에서 서식을 안전하게 지정하지 않으면 메모리 내용이 노출되거나 변조될 수 있다는 점이 제시문의 단서이다.

공통 해설

포맷 스트링(Format String) 공격은 printf 같은 C언어의 서식 처리 함수가 **신뢰할 수 없는 입력을 서식 문자열로 사용**할 때 발생한다. 서식 문자열은 %d, %s 등의 지정자로 자료를 어떤 형식으로 처리할지 정하는 문자열이다. 외부 입력에 포함된 지정자까지 함수가 해석하면, 의도하지 않은 메모리 내용을 읽거나 특정 조건에서 메모리를 변경하고 프로그램을 비정상 종료시킬 수 있다.

예를 들어 외부 입력을 담은 문자열 변수가 user_input일 때, printf(user_input)은 입력 자체를 서식으로 해석한다. 반면 printf("%s", user_input)은 서식을 %s로 고정하여 입력을 문자열 데이터로 출력한다.
제시문의 '데이터의 형태와 길이에 대한 불명확한 정의'는 이처럼 서식과 입력 데이터를 안전하게 구분하지 않은 문제와 연결된다. 버퍼 오버플로우는 확보한 버퍼의 경계를 넘어 데이터를 기록하는 것이 핵심인 반면, 포맷 스트링 공격은 **입력을 서식으로 잘못 해석하는 것**이 핵심이다.

NoteBase

문 12. 유닉스 시스템의 디렉터리별 역할에 대한 설명을 바르게 연결한 것은?

(가) 시스템의 환경 설정 및 주요 설정 파일을 담고 있다.
(나) 기본적으로 실행 가능한 파일을 담고 있다.
(다) 각 사용자의 작업 디렉터리를 담고 있다.

① (가): /bin, (나): /home, (다): /etc
② (가): /home, (나): /etc, (다): /bin
③ (가): /etc, (나): /bin, (다): /home
④ (가): /bin, (나): /etc, (다): /home

정답 3번

간단한 해설

시스템 설정 파일은 **/etc**, 기본 명령어의 실행 파일은 **/bin**에 둔다. **/home**은 사용자별 작업 공간인 홈 디렉터리를 모아 두는 곳이다.

대응 관계 해설

(가) /etc: **시스템의 환경 설정 파일**을 보관하는 디렉터리이다. 예를 들어 /etc/hosts에는 호스트 이름과 IP 주소의 대응 정보를 저장한다. 따라서 시스템 설정 및 주요 설정 파일이라는 설명에 대응한다.

(나) /bin: **기본 명령어의 실행 파일**을 보관하는 디렉터리이다. 파일 목록을 확인하는 ls, 파일을 복사하는 cp 등이 대표적이다. 명령어의 동작을 정하는 설정 파일과 명령어 자체의 실행 파일을 구별해야 한다.

(다) /home: **사용자별 홈 디렉터리**를 모아 두는 디렉터리이다. 예를 들어 사용자 kim의 홈 디렉터리를 /home/kim으로 두면 그 안에서 개인 파일과 작업 자료를 관리한다. 따라서 각 사용자의 작업 디렉터리를 담는다는 설명에 대응한다.

(가)는 /etc, (나)는 /bin, (다)는 /home으로 연결되므로 ③의 구성과 일치한다.

NoteBase

문 13. 윈도우즈 시스템 명령창에서 netstat -an 명령을 수행한 결과의 일부이다. 구동 중인 서비스로 옳지 않은 것은?

프로토콜	로컬주소	외부주소	상태
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

① FTP

② Telnet

③ SMTP

④ HTTP

정답 2번

간단한 해설

Telnet의 표준 TCP 포트는 **23번**이다. 제시된 LISTENING 항목에는 21·25·80번 포트만 있고 23번 포트는 없어, Telnet이 구동 중이라는 근거가 없다.

NoteBase

선지별 해설

이 문항은 서비스의 표준 TCP 포트 번호를 기준으로 해석한다. 로컬주소의 콜론 뒤 숫자는 해당 시스템의 포트 번호이고, LISTENING은 그 포트에서 연결 요청을 기다리는 상태이다. 따라서 외부주소의 0이 아니라 로컬주소의 포트 번호를 서비스와 대응시킨다.

① O: FTP의 제어 연결에는 표준 TCP **21번 포트**를 사용한다. 로컬주소가 0.0.0.0:21인 행이 LISTENING 상태이므로, 표준 포트를 기준으로 FTP 서비스가 연결을 기다리고 있음을 알 수 있다.

② X: Telnet의 표준 TCP 포트는 **23번**이다. 제시된 결과에는 23번 포트의 LISTENING 항목이 없으므로, Telnet을 구동 중인 서비스로 판단할 수 없다. 표시된 21·25·80번 포트는 각각 FTP·SMTP·HTTP에 대응한다.

③ O: SMTP의 표준 TCP 포트는 **25번**이다. 로컬주소가 0.0.0.0:25인 행이 LISTENING 상태이므로, 표준 포트를 기준으로 SMTP 서비스가 연결을 기다리고 있음을 알 수 있다.

④ O: HTTP의 표준 TCP 포트는 **80번**이다. 로컬주소가 0.0.0.0:80인 행이 LISTENING 상태이므로, 표준 포트를 기준으로 HTTP 서비스가 연결을 기다리고 있음을 알 수 있다.

NoteBase

문 14. OWASP(Open Web Application Security Project)에서 발표한 2013년 Mobile Security Project Top 10의 위협 요소로 옳지 않은 것은?

① 안전하지 않은 세션처리(Improper Session Handling)

② 취약한 권한 및 인증(Poor Authorization and Authentication)

③ 안전하지 않은 데이터 저장(InSecure Data Storage)

④ 서버 측 인젝션(Server Side Injection)

정답 4번

간단한 해설

④의 '서버 측 인젝션'은 **클라이언트 측 인젝션(Client Side Injection)**으로 고쳐야 한다. 이는 악성 입력이 모바일 앱에서 코드나 명령으로 해석되어 실행되는 위협이다.

선지별 해설

① O: 안전하지 않은 세션처리는 Top 10에 포함된다. 세션은 로그인한 사용자의 인증 상태를 이어 가는 수단이다. 세션 토큰이 노출되거나 로그아웃 후에도 서버에서 유효하게 남아 있으면 공격자가 이를 재사용하여 사용자를 사칭할 수 있다. 따라서 **세션 토큰의 보호와 적절한 만료·폐기**가 중요하다.

② O: 취약한 권한 및 인증은 Top 10에 포함된다. 인증은 **사용자가 누구인지 확인**하는 것이고, 권한 검사는 **그 사용자가 해당 작업을 수행할 수 있는지 확인**하는 것이다. 사용자 확인이 부실하거나 접근 권한을 검사하지 않으면 타인의 계정이나 허용되지 않은 기능에 접근할 수 있다.

③ O: 안전하지 않은 데이터 저장은 Top 10에 포함된다. 모바일 기기의 파일이나 데이터베이스 등에 비밀번호·개인정보 같은 민감한 정보를 충분히 보호하지 않고 저장하는 문제이다. 예를 들어 민감한 정보를 평문으로 저장하고 접근도 제한하지 않으면, 저장소에 접근한 공격자가 내용을 읽을 수 있다. 핵심은 **기기에 저장된 민감한 정보의 보호 부족**이다.

④ X: 해당 목록에 제시된 인젝션 항목은 서버 측 인젝션이 아니라 **클라이언트 측 인젝션**이다. 신뢰할 수 없는 입력이 모바일 앱 내부에서 코드나 명령으로 해석되어 실행되는 문제로, 기기 내 데이터베이스를 대상으로 한 SQL 인젝션 등이 이에 해당한다. 서버 측 인젝션도 실제 보안 위협이지만, 이 문항이 묻는 Top 10의 독립 항목 명칭과는 다르다.

NoteBase

문 15. 리눅스 시스템의 umask 값에 따라 생성된 파일의 접근 권한이 '-rw-r-----'일 때, 기본 접근 권한을 설정하는 umask 값은?

① 200

② 260

③ 026

④ 620

정답 3번

간단한 해설

일반 파일 생성 시의 권한 666에서 **그룹의 쓰기 권한과 기타 사용자의 읽기·쓰기 권한**을 제거하면 '-rw-r-----'(640)이 된다. 이때 제거할 권한을 소유자·그룹·기타 사용자 순서로 나타낸 umask 값이 026이다.

계산 과정

적용 기준: umask는 새 파일에 부여할 권한 중 **제거할 권한 비트**를 지정한다. 이 문제에서는 일반 파일을 생성할 때 통상 요청하는 권한 666(rw-rw-rw-)을 기준으로 한다. 처음부터 실행 권한이 없으므로, umask가 실행 권한을 제거하지 않더라도 실행 권한이 새로 생기지는 않는다.

접근 권한 환산: '-rw-r-----'의 맨 앞 '-'는 일반 파일을 뜻하며, 나머지는 소유자·그룹·기타 사용자의 권한이다. 읽기 r은 4, 쓰기 w는 2, 실행 x는 1로 나타내므로 소유자의 rw-는 4 + 2 = 6, 그룹의 r--는 4, 기타 사용자의 ---는 0이다. 따라서 주어진 접근 권한은 8진수 640이다.

umask 산출: 소유자는 rw-를 그대로 유지하므로 제거할 권한이 없어 0이다. 그룹은 rw-에서 **쓰기 권한 w(2)**를 제거해야 r--가 된다. 기타 사용자는 rw-에서 **읽기·쓰기 권한 rw(6)**를 모두 제거해야 ---가 된다. 이를 소유자·그룹·기타 사용자 순서로 모으면 umask는 026이다.

결과 확인: umask 026을 적용하면 소유자는 6, 그룹은 4, 기타 사용자는 0의 권한을 갖게 되어 640, 즉 '-rw-r-----'가 된다. 따라서 선택지 ③의 026이 주어진 접근 권한을 만든다.

NoteBase

문 16. 윈도우즈 시스템이 동작하기 위한 프로세스와 그에 대한 설명을 바르게 연결한 것은?

(가) Winlogon 서비스에 대한 필요한 인증 프로세스를 담당한다.
(나) 사용자 세션을 시작하는 기능을 담당한다.
(다) 사용자가 미리 지정한 시간에 작업을 실행시키는 작업 스케줄을 담당한다.

① (가): smss.exe, (나): mstask.exe, (다): lsass.exe
② (가): smss.exe, (나): lsass.exe, (다): mstask.exe
③ (가): lsass.exe, (나): mstask.exe, (다): lsass.exe
④ (가): lsass.exe, (나): smss.exe, (다): mstask.exe

정답 4번

간단한 해설

Winlogon과 연계하여 사용자를 **인증**하는 것은 lsass.exe이고, 사용자 **세션을 시작**하는 것은 smss.exe이다. 인증 정보를 확인하는 역할과 세션 실행 환경을 준비하는 역할을 구분한다.

대응 관계 해설

(가) lsass.exe: 로컬 보안 기관 하위 시스템 서비스로, Winlogon을 통한 로그온 과정에서 **사용자의 신원을 인증**하는 역할을 맡는다. 입력된 자격 증명이 유효한지 확인하는 것이므로, 세션 초기화를 담당하는 smss.exe와 구별된다.

(나) smss.exe: 세션 관리자 하위 시스템으로, **세션에 필요한 환경과 프로세스를 초기화**하여 사용자 세션을 시작한다. 세션은 사용자의 프로그램 등이 실행되는 환경이며, 이 환경을 준비하는 기능은 사용자 인증이나 예약 작업 실행과 다르다.

(다) mstask.exe: 기존 윈도우즈의 작업 스케줄러 프로세스로, 사용자가 등록한 작업을 **미리 지정한 시간에 실행**한다. 예를 들어 특정 시각에 프로그램을 실행하도록 예약했을 때 그 시간 조건에 따라 작업을 수행하는 역할이다.

(가)는 lsass.exe, (나)는 smss.exe, (다)는 mstask.exe에 대응하므로 ④의 연결과 일치한다.

NoteBase

문 17. 버퍼 오버플로우 공격의 대응방법 중 스택에서 실행 권한을 제거해 스택에 로드된 공격자의 공격 코드가 실행될 수 없도록 하는 방법은?

① Stack Guard

② Non-Executable Stack

③ Stack Shield

④ ASLR(Address Space Layout Randomization)

정답 2번

간단한 해설

Non-Executable Stack은 스택의 **실행 권한을 제거**하여, 스택에 저장된 공격 코드를 CPU가 명령어로 실행하지 못하게 한다.

공통 해설

Non-Executable Stack은 스택 메모리에 실행 불가 속성을 적용하는 방어 기법이다. 메모리의 읽기·쓰기 권한과 실행 권한은 구별되므로, 스택에 데이터를 저장할 수 있어도 그 내용을 명령어로 실행할 수 있는 것은 아니다.

버퍼 오버플로우로 공격 코드가 스택에 들어가더라도, 실행 흐름이 그 코드의 주소로 이동하면 **실행 권한 위반**이 발생하여 해당 코드의 실행이 차단된다. 문제의 핵심인 '스택에서 실행 권한을 제거'한다는 동작이 Non-Executable Stack의 정의에 해당한다. 이 기법은 스택에 주입된 코드의 실행을 막지만, 버퍼 범위를 넘는 쓰기 자체를 방지하는 것은 아니다.

NoteBase

문 18. 전자우편서비스 관련 프로토콜에 대한 설명으로 옳지 않은 것은?

① SMTP(Simple Mail Transfer Protocol)는 송신자의 메일 서버로부터 수신자의 메일 서버로 메시지 전송을 담당한다.

② MIME(Multipurpose Internet Mail Extension)은 SMTP를 확장하여 오디오, 비디오, 응용 프로그램, 기타 여러 종류의 데이터 파일을 주고받을 수 있다.

③ Secure/MIME은 MIME 데이터를 전자서명과 암호화 기술을 이용하여 암호화, 인증, 메시지 무결성, 송신처 부인방지 등을 제공한다.

④ IMAP(Internet Message Access Protocol)은 POP3와 다르게 SMTP 프로토콜을 의존하지 않고, 이메일의 원본을 서버에서 삭제한다.

정답 4번

간단한 해설

IMAP은 **메일을 서버에 보관한 채 조회·관리**하므로, 읽었다는 이유만으로 서버의 원본을 삭제하지 않는다. IMAP과 POP3는 모두 수신 메일 접근용이며, 메일 발송은 별도의 **SMTP**가 담당한다.

선지별 해설

① O: SMTP는 전자우편을 보내고 중계하는 프로토콜로, **송신 측 메일 서버에서 수신 측 메일 서버로 메시지를 전송**한다. 수신자의 단말이 서버에 도착한 메일을 조회하는 역할은 IMAP이나 POP3가 담당한다.

② O: MIME은 문자 중심의 전자우편 메시지 형식을 확장하여 오디오·비디오·응용 프로그램 파일 등 **다양한 형식의 데이터를 메일에 담을 수 있게** 한다. 데이터의 종류와 인코딩 방식을 표시하여 수신 측이 내용을 해석할 수 있게 하며, 이렇게 구성한 메시지는 SMTP로 전송할 수 있다. 즉, MIME은 메시지의 표현 형식을, SMTP는 전송을 담당한다.

③ O: S/MIME은 MIME 데이터에 전자서명과 암호화를 적용하는 보안 방식이다. **전자서명은 송신자 인증·메시지 무결성·송신 사실의 부인방지**를 지원하고, 암호화는 허가받지 않은 사람이 내용을 읽지 못하도록 기밀성을 제공한다. 메시지 변조 여부를 확인하는 기능과 내용을 숨기는 기능을 구분해야 한다.

④ X: IMAP은 **서버에 메일을 보관한 채 조회하고 관리**하는 프로토콜이다. 메일을 읽었다고 원본이 자동으로 삭제되는 것이 아니며, 삭제하려면 별도의 삭제 동작이 필요하다. POP3는 메일을 내려받는 방식이 중심이고 서버의 메일을 삭제하거나 설정에 따라 남겨 둘 수 있다. 또한 IMAP과 POP3는 모두 수신 메일 접근을 담당하고, 발송은 별도의 SMTP가 담당하므로 'POP3와 다르게 SMTP 프로토콜을 의존하지 않는다'는 구분도 적절하지 않다.

NoteBase

문 19. 디지털 포렌식에서 데이터베이스에 있는 대량의 숫자 정보의 무결성 및 정확성을 확인하기 위해 수행하는 분석 방법은?

① 스니퍼 운용

② MRTG(Multi Router Traffic Grapher)

③ CAATs(Computer Assisted Auditing Techniques)

④ 네트워크 로그 서버 분석

정답 3번

간단한 해설

CAATs는 컴퓨터를 이용해 대량의 자료를 분석하는 감사 기법이다. 데이터베이스의 숫자 정보를 재계산·대조하여 **오류와 불일치**를 찾아 무결성과 정확성을 점검한다.

공통 해설

CAATs(Computer Assisted Auditing Techniques)는 **컴퓨터 지원 감사 기법**으로, 감사용 소프트웨어 등을 이용해 전산 자료를 추출하고 분석한다. 대량의 숫자 자료에 재계산, 합계 대조, 중복·누락 검사 등을 적용하여 값이 정확하고 서로 일관되는지 확인한다. 예를 들어 거래별 수량과 단가로 금액을 다시 계산한 뒤 저장된 금액과 비교하면, 계산 결과가 일치하지 않는 기록을 찾아낼 수 있다.

문항의 판단 기준은 **데이터베이스에 저장된 수치 자체를 검사하는가**이다. CAATs는 이러한 자료 검증에 해당한다. 스니퍼 운용·MRTG·네트워크 로그 서버 분석처럼 통신이나 네트워크 활동을 관찰하는 방법만으로는 저장된 수치의 재계산과 대조를 대신할 수 없다.

NoteBase

문 20. Cross Site Scripting(XSS) 공격유형에 해당하지 않는 것은?

① Reflash XSS 공격

② Reflected XSS 공격

③ DOM(Document Object Model) 기반 XSS 공격

④ Stored XSS 공격

정답 1번

간단한 해설

'Reflash XSS'는 **일반적으로 인정되는 XSS 공격유형 명칭이 아니다**. XSS의 대표적인 유형에는 반사형(Reflected), 저장형(Stored), DOM 기반 공격이 있다.

선지별 해설

XSS는 웹페이지에 공격자가 주입한 악성 스크립트가 사용자의 브라우저에서 실행되도록 하는 공격이다.

① X: Reflash XSS는 일반적으로 인정되는 XSS 공격유형 명칭이 아니다. 대표적인 유형으로는 **Reflected XSS, Stored XSS, DOM 기반 XSS**가 있다.

② O: Reflected XSS는 반사형 XSS이다. 요청에 포함된 악성 입력이 안전하게 처리되지 않은 채 **응답에 반영되어** 사용자의 브라우저에서 실행되는 방식이다. 예를 들어 악성 스크립트가 포함된 검색어를 검색 결과 페이지에 그대로 출력하면 발생할 수 있다.

③ O: DOM 기반 XSS는 브라우저에서 실행되는 **클라이언트 측 스크립트가 입력을 안전하지 않게 처리**하여 발생한다. DOM은 웹 문서의 구조를 객체로 표현한 것이며, URL 등의 공격자 입력을 DOM에 삽입하는 과정에서 악성 스크립트가 실행될 수 있다.

④ O: Stored XSS는 저장형 XSS이다. 악성 입력이 게시글·댓글·데이터베이스 등에 **저장된 뒤**, 이를 조회하는 사용자의 브라우저에서 실행되는 방식이다. 요청의 입력을 곧바로 되돌려 주는 반사형과 달리, 저장된 악성 내용이 이후 조회 때 전달된다는 점이 특징이다.

NoteBase