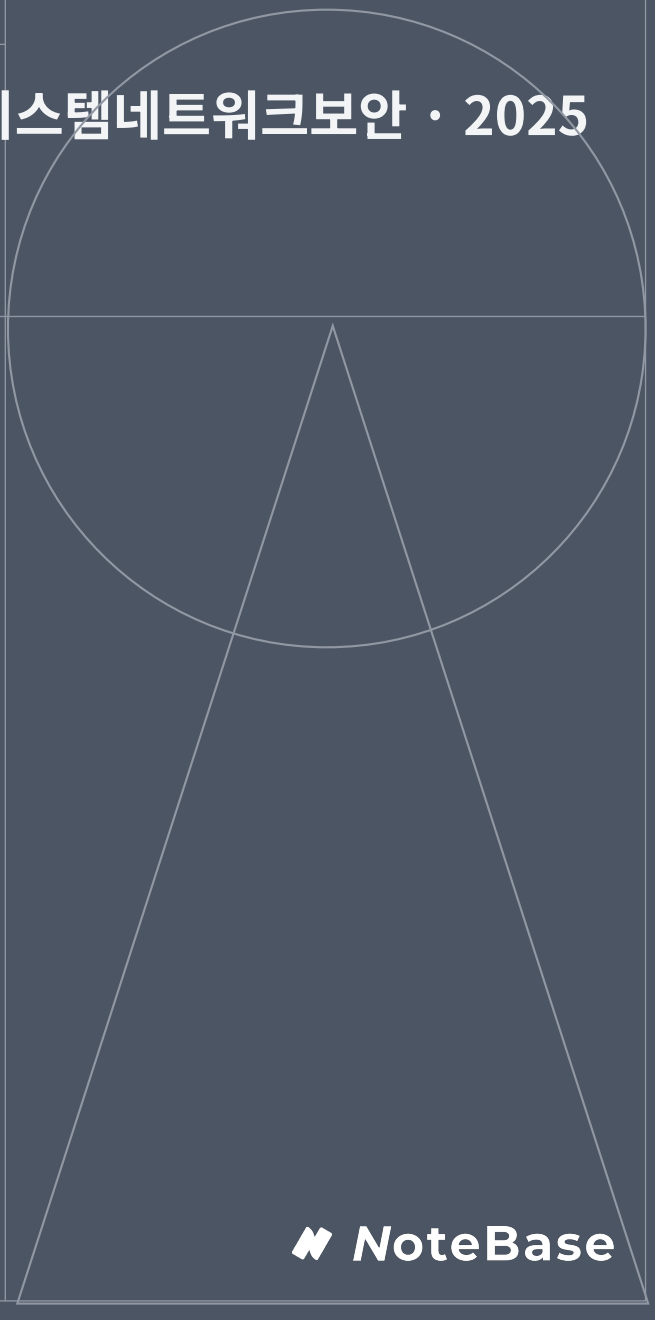
기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2025



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2025

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2025

문 1. 다음에서 설명하는 윈도우 로그로 가장 적절한 것은?

도메인 계정 사용으로 생성되고, 이 감사의 실패 이벤트 추적에서는 패스워드 크래킹 시도 등을 확인할 수 있고, 성공 이벤트 추적에서는 사후 문제를 확인할 수 있다.

① 개체 액세스 감사

② 계정 로그온 이벤트 감사

③ 로그온 이벤트 감사

④ 계정 관리 감사

정답 2번

간단한 해설

계정 로그온 이벤트 감사는 **계정 자격 증명의 인증 성공·실패**를 추적한다. 도메인 계정의 경우 인증을 처리하는 도메인 컨트롤러의 기록을 통해 반복된 인증 실패나 성공 이력을 조사할 수 있다.

NoteBase

대응 관계 해설

제시문은 도메인 계정의 인증 성공과 실패를 추적하는 **계정 로그온 이벤트 감사**에 대응한다. 이 감사는 계정 자격 증명을 검증하는 측의 사건을 기록하며, 도메인 계정 인증은 일반적으로 도메인 컨트롤러에서 처리된다.

인증 실패가 반복되면 비밀번호 추측 등 공격 시도를 의심할 단서가 된다. 다만 단순한 비밀번호 오입력도 실패를 만들 수 있으므로 **실패 하나만으로 공격을 확정할 수는 없다**. 성공 기록은 어떤 계정이 언제 인증되었는지 확인하여 사고 후 활동을 추적하는 데 활용한다.

로그온 이벤트 감사는 실제로 로그온 세션이 만들어지는 워크스테이션이나 서버의 로그온·로그오프를 추적한다. 따라서 도메인 계정으로 접속해도 해당 컴퓨터에는 로그온 이벤트가, 인증을 처리한 도메인 컨트롤러에는 계정 로그온 이벤트가 각각 생길 수 있다. 핵심 구별은 **계정 인증과 접속 세션**의 관점 차이이다.

개체 액세스 감사는 파일 등 감사 대상으로 설정된 개체에 대한 접근을 기록한다. 계정 관리 감사는 계정의 생성·삭제·변경, 그룹 구성 변경 등의 관리 작업을 기록한다. 둘 다 계정 인증 시도의 성공·실패를 직접 설명하는 범주와는 다르다.

따라서 도메인 계정의 인증 활동을 추적한다는 설명에 가장 적절한 것은 ② 계정 로그온 이벤트 감사이다.

NoteBase

문 2. 다음에서 설명하는 용어로 가장 적절한 것은?

전자상거래 당사자들의 신뢰성과 안전성을 위하여 사용자 및 판매자의 신원 인증, 거래 정보의 비밀성, 지불 데이터의 부인 방지 등의 보안 기능과 이질적인 환경에서의 상호운용성을 제공한다.

① SET
② PGP
③ OTP
④ SSO

정답 1번

간단한 해설

카드 결제 전자상거래에서 당사자 인증·거래 정보 보호·전자서명에 의한 부인 방지 등을 제공하는 프로토콜은 **SET**이다.

대응 관계 해설

전자상거래 당사자 인증: SET(Secure Electronic Transaction)은 카드 결제 거래를 안전하게 처리하기 위한 보안 프로토콜이다. 인증서를 이용하여 **카드 소지자와 판매자의 신원**을 확인하는 구조를 갖는다.

거래 정보의 비밀성: 암호화로 민감한 결제 정보를 보호한다. 또한 주문 정보와 결제 정보를 구분하고 필요한 당사자에게 전달하여 **거래 당사자별 정보 노출을 제한**한다.

지불 데이터의 부인 방지: 전자서명으로 거래 데이터의 무결성과 서명 주체를 확인하고 거래 사실을 부인하기 어렵게 한다. 주문 정보와 결제 정보의 관계를 연결하는 이중서명도 SET의 특징이다.

이질적인 환경의 상호운용성: 당사자들이 공통 프로토콜과 메시지 형식을 따르도록 하여 **서로 다른 시스템 사이의 결제 처리**를 지원한다.

PGP는 전자우편·파일의 암호화와 서명, OTP는 일회용 비밀번호, SSO는 한 번의 인증으로 여러 서비스에 접근하는 방식이다. 제시된 결제 보안 기능을 종합적으로 가리키는 것은 SET이므로 ①에 해당한다.

NoteBase

문 3. 리눅스 디렉터리의 주요 기능에 관한 설명으로 가장 적절하지 않은 것은?

① /dev : 장치 파일이 담긴 디렉터리이다.

② /opt : 추가 패키지가 설치되는 디렉터리이다.

③ /sys : 시스템의 환경설정 및 주요 설정 파일을 담고 있다.

④ /var : 시스템 운영 중에 발생하는 데이터나 로그 등 내용이 자주 바뀌는 파일이 저장된다.

정답 3번

간단한 해설

주요 시스템 설정 파일은 일반적으로 **/etc**에 둔다. /sys는 커널과 장치의 정보·속성을 노출하는 가상 파일시스템으로, 설정 파일을 보관하는 디렉터리와 구별된다.

선지별 해설

① O: /dev는 장치를 파일 인터페이스로 다루기 위한 장치 파일을 두는 디렉터리이다. 디스크 등의 블록 장치나 터미널 등의 문자 장치에 접근하는 특수 파일이 여기에 나타난다.

② O: /opt는 추가 응용 소프트웨어 패키지를 설치하는 데 사용하는 디렉터리이다. 별도로 제공되는 패키지를 전용 하위 디렉터리에 배치하는 용도로 쓰이며, 모든 리눅스 패키지가 반드시 이곳에 설치된다는 뜻은 아니다.

③ X: 시스템 전반의 주요 설정 파일을 두는 대표적 디렉터리는 **/etc**이다. /sys에는 sysfs 가상 파일시스템이 마운트되어 커널이 관리하는 장치·드라이버·커널 객체의 정보와 속성을 사용자 공간에 제공한다. 일부 속성을 통해 실행 중 설정을 조정할 수 있지만, 일반적인 시스템 설정 파일의 저장 디렉터리라는 설명과는 다르다.

④ O: /var는 시스템 운영 중 내용이나 크기가 변하는 자료를 보관한다. 대표적으로 /var/log의 로그, 메일·출력 대기열 등의 스풀 자료, 캐시와 상태 자료가 포함된다.

NoteBase

문 4. SSH에 대한 설명으로 가장 적절하지 않은 것은?

① Telnet이나 보안을 제공하지 않는 다른 원격 로그인 방식을 대체하기 위해 개발되었다.

② 원격 로그인과 X-터미널에 채택되어 사용되었으며 현재도 가장 널리 사용되는 응용 기술이다.

③ Alert 프로토콜과 Record 프로토콜을 정의하여 암호화를 한다.

④ 안전하지 않은 TCP 연결을 포트 포워딩을 사용하여 안전한 연결로 변환시킬 수 있다.

정답 3번

간단한 해설

Alert와 Record는 **SSL/TLS의 프로토콜 구성**에 해당한다. SSH는 전송계층·사용자 인증·연결 프로토콜로 구성되며 원격 로그인과 터널링을 보호한다.

선지별 해설

SSH는 안전하지 않은 네트워크 위에서 인증·기밀성·무결성을 제공하는 보안 원격접속 프로토콜이다.

① O: SSH는 Telnet이나 rlogin처럼 통신 내용과 인증정보를 충분히 보호하지 못하는 원격 로그인 방식을 대체하기 위해 개발되었다. 암호화된 채널과 호스트·사용자 인증을 통해 원격접속을 보호한다.

② O: 원격 로그인은 SSH의 대표적 용도이고, X11 포워딩을 통해 원격 그래픽 응용의 통신도 전달할 수 있다. SSH가 원격관리 분야에서 널리 사용되는 대표적 기술이라는 설명으로 이해한다. 선지의 '가장 널리'는 모든 응용기술 전체의 이용량 순위를 입증한다는 의미로 확대하지 않는다.

③ X: **Alert 프로토콜과 Record 프로토콜은 SSL/TLS의 구성요소**이다. SSH의 주요 구성은 전송계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜이다. 전송계층은 서버 인증과 암호화·무결성을 제공하고, 사용자 인증은 접속 사용자를 확인하며, 연결 프로토콜은 암호화된 통로를 여러 논리 채널로 나눈다.

④ O: SSH 포트 포워딩은 일반 TCP 통신을 SSH 터널로 전달하여 SSH 양 끝 사이의 구간을 암호화해 보호할 수 있다. 다만 터널 밖의 구간이나 응용 자체의 취약점까지 자동으로 안전하게 만드는 것은 아니므로, 보호 범위는 SSH가 연결된 두 끝점 사이로 구분해야 한다.

NoteBase

문 5. 다음에서 설명하는 공격기법으로 가장 적절한 것은?

통신을 연결하는 두 사람 사이에 침입하여, 두 사람이 상대방에게 연결됐다고 생각하도록 조작하고, 공격자는 한쪽에서 전달된 정보를 도청하거나 조작한 후 다른 쪽으로 전달하는 공격기법이다.

① 부채널 공격
② 살라미 공격
③ 무차별 공격
④ 중간자 공격

정답 4번

간단한 해설

양쪽이 서로 직접 통신한다고 믿지만, 실제로는 공격자가 사이에서 정보를 받아 도청하거나 바꾸어 전달한다. 이처럼 **통신 당사자 사이에 끼어들어 상대방을 가장하는** 방식이 중간자 공격이다.

공통 해설

중간자 공격은 공격자가 두 통신 당사자 사이에 개입하여, 각각에게 자신이 원래 통신하려던 상대방인 것처럼 행동하는 공격이다. 두 사람은 서로 연결되었다고 믿지만, 실제 정보는 **공격자를 거쳐 전달**되므로 공격자가 내용을 도청하거나 변조할 수 있다. 지문의 '상대방에게 연결됐다고 생각하도록 조작'하고 '한쪽의 정보를 다른 쪽으로 전달'한다는 조건이 이 정의에 해당한다.

예를 들어 A가 B에게 보내는 메시지를 공격자가 먼저 받아 내용을 읽거나 바꾼 뒤 B에게 전달한다. B가 보내는 응답도 같은 방식으로 중계하면 양쪽은 공격자의 개입을 모른 채 통신을 이어갈 수 있다. 핵심은 단순히 정보를 엿듣는 데 그치지 않고 **양쪽 사이에서 상대방을 가장하며 통신을 중계**한다는 점이다.

NoteBase

문 6. 리눅스에서 exam이라는 파일에 SetUID를 설정하는 명령으로 가장 적절한 것은?

① chmod u+t exam

② chmod g+s exam

③ chmod 2755 exam

④ chmod 4755 exam

정답 4번

간단한 해설

특수 권한의 8진수 값에서 **4000은 SetUID**를 뜻한다. 따라서 4755는 SetUID와 일반 권한 755를 함께 지정하는 값이다.

핵심 풀이

SetUID는 실행 시 파일 소유자의 사용자 ID가 유효 사용자 ID에 적용되도록 하는 특수 권한 비트이다. 4자리 8진수 권한에서 **맨 앞의 4가 SetUID**를 뜻하며, 2는 SetGID, 1은 스티키 비트에 해당한다.

'chmod 4755 exam'은 SetUID를 설정하면서 일반 권한을 755로 정한다. 755는 소유자에게 읽기·쓰기·실행, 그룹과 기타 사용자에게 읽기·실행을 부여한다. 따라서 이 명령은 SetUID 비트만 추가하는 것이 아니라 **일반 접근 권한도 함께 지정**한다. 기존 일반 권한을 유지하면서 SetUID를 추가하는 기호 방식은 'chmod u+s exam'이다.

'chmod g+s exam'과 'chmod 2755 exam'은 소유자 사용자 ID가 아니라 그룹 ID에 관한 SetGID를 설정한다. 'u+t'의 t는 SetUID용 기호가 아니며, GNU chmod에서 u+t는 효과가 없다. 스티키 비트를 설정할 때 쓰는 +t와 SetUID를 설정하는 u+s를 혼동하지 않는다.

따라서 exam에 SetUID를 설정하는 제시된 명령은 ④ 'chmod 4755 exam'이다.

NoteBase

문 7. VPN에서 사용하는 터널링 프로토콜 중에서 가장 적절하지 않은 것은?

① L2F

② PPTP

③ L2TP

④ P2P

정답 4번

간단한 해설

P2P는 동등한 노드들이 자원을 주고받는 **통신 방식**이며 VPN 터널링 프로토콜의 이름이 아니다.
L2F·PPTP·L2TP는 터널을 통해 프레임을 전달하는 프로토콜이다.

선지별 해설

터널링은 원래의 프레임이나 패킷을 다른 프로토콜의 데이터 부분에 넣어 전달하여 논리적인 통신 경로를 만드는 기술이다. 터널링 기능과 암호화 기능은 구별해야 한다.

① O: L2F(Layer Two Forwarding)는 링크 계층 프레임을 터널을 통해 전달하는 프로토콜이다. 원격 접속 지점과 실제 사설망 접속을 처리하는 지점을 분리할 수 있어 가상 사설망의 터널링에 사용된다.

② O: PPTP(Point-to-Point Tunneling Protocol)는 PPP 프레임을 IP 네트워크를 통해 운반하는 터널링 프로토콜이다. 제어 연결과 GRE 기반 데이터 전달을 이용하며, 명칭의 'Tunneling'이 나타내듯 논리적인 터널을 구성한다.

③ O: L2TP(Layer Two Tunneling Protocol)는 L2F와 PPTP의 개념을 바탕으로 PPP 트래픽을 터널링하는 프로토콜이다. **L2TP 자체의 터널링이 데이터 암호화를 뜻하지는 않으며**, 통신 보호를 위해 IPsec과 결합할 수 있다.

④ X: P2P(Peer-to-Peer)는 참여 노드들이 서로 자원을 제공하거나 이용하는 **네트워크 구성·통신 방식**이다. 그 자체가 VPN 터널의 설정과 캡슐화 절차를 규정한 특정 터널링 프로토콜은 아니다. PPTP나 PPP와 이름을 혼동해서는 안 된다.

따라서 VPN 터널링 프로토콜로 가장 적절하지 않은 것은 ④이다.

NoteBase

문 8. 다음에서 설명하는 공격기법으로 가장 적절한 것은?

TCP 3중 연결(3-way handshaking)의 취약점과 반사 서버(라우터 등)를 이용한 공격으로, 공격자는 출발지 IP를 공격 대상의 IP로 위조하여 SYN 패킷을 다수의 반사 서버로 전송하여 응답하는 SYN-ACK 패킷을 공격 대상이 받도록 한다.

① LAND

② Port Scan

③ DRDoS

④ ARP Spoofing

정답 3번

간단한 해설

출발지 주소를 피해 대상의 주소로 위조하여 여러 서버의 응답이 그 대상에 집중되게 하는 **반사 구조**가 핵심이다. 이는 분산 반사 서비스 거부 공격인 DRDoS에 해당한다.

대응 관계 해설

출발지 IP 위조: 제시문에서는 패킷의 출발지를 공격 대상의 IP로 표시한다. 따라서 요청을 받은 서버가 응답할 주소는 실제 요청을 보낸 공격자가 아니라 **위조된 출발지인 공격 대상**이 된다.

반사 서버와 TCP 응답: TCP 연결 설정에서 SYN을 받은 서버는 SYN-ACK으로 응답한다. 제시문은 이 응답 동작을 이용하여 여러 서버가 피해 대상 쪽으로 응답을 보내게 하므로 **제3의 서버가 트래픽을 반사**하는 구조이다.

분산된 응답의 집중: 다수의 반사 서버가 보내는 SYN-ACK이 한 대상에 집중되어 통신 자원과 서비스 가용성에 부담을 준다. 이처럼 여러 반사 지점을 이용하는 서비스 거부 공격이 **DRDoS(분산 반사 서비스 거부 공격)**이다.

LAND는 출발지와 목적지 주소·포트 등을 동일하게 설정하는 공격이고, Port Scan은 서비스가 열려 있는 포트를 조사하는 행위이다. ARP Spoofing은 IP와 MAC 주소의 대응 정보를 속이는 공격이다. 제시된 분산 반사 구조에 대응하는 선택지는 ③ DRDoS이다.

NoteBase

문 9. IDS의 비정상(Anomaly) 행위 탐지에 대한 설명으로 가장 적절하지 않은 것은?

① 신경망, 통계적 방법, 특징 추출 등의 기술을 사용한다.

② 미리 학습된 사용자 패턴과 다른 경우에 침입으로 판단할 수 있다.

③ 오용(Misuse)탐지 방식보다 False Positive가 상대적으로 낮다.

④ Zero Day Attack에 대응이 가능한 방법이다.

정답 3번

간단한 해설

비정상 행위 탐지는 정상 패턴에서 벗어나는 활동을 찾으므로 알려지지 않은 공격도 탐지할 수 있다. 반면 새로운 정상 활동을 공격으로 오인하는 **False Positive가 상대적으로 높아질 수 있다**는 한계가 있다.

선지별 해설

비정상 행위 탐지는 정상 행위의 기준과 현재 행위의 차이를 이용하고, 오용 탐지는 알려진 공격의 특징이나 규칙과 현재 행위를 대조한다.

① O: 정상 행위의 특징을 추출하고 모델링하기 위해 통계적 방법이나 신경망 등을 사용할 수 있다. 접속 시간, 요청 빈도, 전송량 같은 특성을 학습하거나 분석해 정상 범위에서 크게 벗어나는지를 평가한다.

② O: 미리 형성한 정상 사용자·시스템 행위 프로파일과 다른 활동이 나타나면 침입 의심으로 판단할 수 있다. 다만 차이가 있다는 사실만으로 실제 공격이 확정되는 것은 아니므로, 임계값과 문맥을 함께 고려해야 한다.

③ X: 정상 행위도 업무 변화나 드문 작업 때문에 학습된 패턴에서 벗어날 수 있다. 따라서 비정상 탐지는 오용 탐지보다 **정상 활동을 공격으로 잘못 경보하는 False Positive가 상대적으로 높아지기 쉽다**. 실제 비율은 학습자료·임계값·운영환경에 따라 달라지지만, 일반적인 특징을 '상대적으로 낮다'고 설명한 것은 반대이다.

④ O: 알려진 공격 서명과 일치하지 않아도 정상 패턴에서 크게 벗어나면 탐지할 수 있으므로, 제로데이 공격을 발견하는 데 활용할 수 있다. 다만 모든 제로데이 공격의 탐지를 보장하거나 IDS 자체가 항상 자동 차단한다는 뜻은 아니다.

NoteBase

문 10. 다음 빈칸 (㉠), (㉡)에 들어갈 용어로 가장 적절한 것은?

80x86 시스템의 메모리 구성 요소 중 (㉠)은/는 초기화되지 않은 정적/전역 변수를 저장하며, 프로그램을 실행할 때 0이나 NULL 포인터로 초기화되는 영역이다. 그리고 (㉡)는 실행되는 머신 코드가 있는 영역으로 EIP가 다음에 실행하는 명령을 가리킨다.

① ㉠: 스택, ㉡: 텍스트 세그먼트

② ㉠: 힙, ㉡: 데이터 세그먼트

③ ㉠: BSS 세그먼트, ㉡: 텍스트 세그먼트

④ ㉠: 텍스트 세그먼트, ㉡: 데이터 세그먼트

정답 3번

간단한 해설

초기값을 명시하지 않은 전역·정적 변수는 **BSS 세그먼트**에, 실행할 기계어 명령은 **텍스트 세그먼트**에 대응한다. BSS의 변수는 초기값을 명시하지 않았어도 실행 전에 0이나 널 포인터 등으로 초기화된다.

빈칸별 해설

㉠ BSS 세그먼트: 명시적으로 초기값을 주지 않은 전역 변수와 정적 변수를 위한 영역이다. 이러한 정적 저장 기간의 변수는 프로그램 실행 전에 정수형은 0, 포인터형은 널 포인터 등으로 초기화된다. 따라서 **'초기화되지 않은'은 초기값을 코드에 명시하지 않았다는 뜻**이지 실행 시 임의의 쓰레기 값을 갖는다는 뜻이 아니다.

㉡ 텍스트 세그먼트: CPU가 실행하는 기계어 명령을 담는 코드 영역이다. 문제의 32비트 x86 문맥에서 EIP는 다음에 실행할 명령의 위치를 나타내는 명령 포인터이므로, 실행 코드라는 단서가 텍스트 세그먼트에 대응한다.

다른 영역과의 구별: 데이터 세그먼트는 통상 초기값이 지정된 전역·정적 데이터를 저장하며, 0으로 초기화되는 데이터는 BSS에 배치될 수 있다. 힙은 동적으로 할당하는 메모리, 스택은 함수 호출의 복귀 정보와 자동 지역 변수 등을 위한 영역이므로 두 빈칸의 설명과 다르다.

따라서 ㉠은 BSS 세그먼트, ㉡은 텍스트 세그먼트이며, 이 대응은 ③과 일치한다.

NoteBase

문 11. 다음에서 설명하는 SNS 보안 위협으로 가장 적절한 것은?

이것은 사용자를 속이는 사회공학적 공격기법이다. 공격자는 와이파이 무선 네트워크에서 Rogue AP를 이용해 사용자 정보를 가로채고, 그 정보로 SNS에 가입 후 공격 대상의 지인이나 특정 유명인으로 가장하여 악의적인 목적을 가지고 활동한다.

① 피싱

② 사이버 폭력

③ 악성 소프트웨어

④ 이블 트윈 어택

정답 4번

간단한 해설

정상적인 무선 접속점처럼 위장한 **가짜 AP**로 사용자를 속이고 정보를 가로채는 것은 이블 트윈 어택이다. 제시문은 탈취한 정보를 SNS 사칭에 이용하는 경우까지 연결하여 설명한다.

대응 관계 해설

사용자를 속이는 방식: 사회공학적 공격은 사람의 신뢰나 판단을 악용한다. 제시문은 사용자가 믿을 만한 네트워크나 인물로 착각하게 만드는 **위장과 사칭**을 공통 수단으로 제시한다.

Rogue AP를 통한 정보 가로채기: 이블 트윈 어택은 정상 무선 접속점처럼 보이는 가짜 AP로 사용자를 유인하여 정보를 가로채는 공격이다. 따라서 **신뢰할 만한 AP를 가장한 무선 접속점**이라는 단서가 명칭을 결정한다.

SNS에서의 사칭: 제시문에서는 획득한 정보를 SNS 계정에 이용하고 지인이나 유명인으로 가장하여 타인의 신뢰를 악용한다. 이는 정보 탈취 이후의 사칭 활동을 설명한 것으로, **모든 이블 트윈 공격에 반드시 SNS 가입이 필요한 것은 아니다**.

피싱은 속임수로 정보를 입력하게 하는 등의 더 넓은 기만 수법이고, 사이버 폭력은 온라인 괴롭힘 등의 행위, 악성 소프트웨어는 해로운 동작을 수행하는 프로그램이다. 가짜 AP라는 구체적 단서와 가장 잘 대응하는 선택지는 ④ 이블 트윈 어택이다.

NoteBase

문 12. 다음에서 설명하는 버퍼 오버플로 공격 대응 기법으로 가장 적절한 것은?

◯ 함수를 호출할 때는 ret를 Global RET Stack이라는 특수 스택에 저장한다.
◯ 함수를 종료할 때는 Global RET Stack에 저장된 ret 값과 스택의 ret 값을 비교하여 일치하지 않으면 프로그램을 종료시킨다.

① 스택 가드
② 스택 실드
③ ASLR
④ Non-Executable Stack

정답 2번

간단한 해설

함수의 **반환주소 자체를 Global RET Stack에 별도로 보관**한다는 것이 식별 단서이다. 카나리 값을 두는 스택 가드와 달리, 이 반환주소 보호 방식은 스택 실드에 해당한다.

대응 관계 해설

첫 번째 설명의 ret는 함수 실행 후 돌아갈 반환주소를 뜻한다. 이를 일반 실행 스택과 별도의 Global RET Stack에 복사해 두는 방식은 **스택 실드(Stack Shield)**의 특징이다.

두 번째 설명은 보관한 반환주소와 실행 스택의 반환주소를 비교해 변조 시 종료하는 검사 방식으로 제시되어 있다. 다만 실제 Stack Shield의 Global Ret Stack 방식에는 별도 보관한 주소를 원래 스택에 복원하는 구현이 있고, 비교·종료 검사는 별도의 반환주소 검사 방식과 구분되기도 한다. 따라서 비교 후 종료하는 동작이 모든 구현에 공통되는 것은 아니며, **반환주소의 별도 보관·보호**가 공통 식별 기준이다.

스택 가드는 버퍼와 제어정보 사이에 카나리 값을 두고 그 값의 변화를 검사하는 기법이다. 제시문은 카나리가 아니라 반환주소 자체를 별도 저장하므로 이와 다르다.

ASLR은 메모리 영역의 배치 주소를 무작위화하여 공격자가 주소를 예측하기 어렵게 한다.

Non-Executable Stack은 스택 영역의 데이터가 명령어로 실행되지 않도록 한다. 둘 다 반환주소를 Global RET Stack에 복사하는 방식과는 구별된다.

NoteBase

문 13. 수신한 패킷의 IPv4 헤더의 HLEN 필드에 이진수 1111_2가 저장되어 있다면 이 패킷의 헤더의 길이는 몇 byte가 가장 적절한가?

① 20byte

② 40byte

③ 50byte

④ 60byte

정답 4번

간단한 해설

HLEN은 **4바이트 단위**의 헤더 길이를 나타낸다. 이진수 1111_2는 15이므로, 헤더 길이는 $15 \times 4 =$ **60바이트**이다.

계산 과정

IPv4의 HLEN 또는 IHL 필드는 헤더 길이를 바이트 수가 아니라 **32비트 워드의 개수**로 저장한다. 32비트는 4바이트이므로 필드 값에 4를 곱해야 바이트 단위 길이가 된다.

주어진 이진수는 $1111_2 = 8 + 4 + 2 + 1 = 15$이다. 이는 헤더가 15개의 32비트 워드로 구성된다는 뜻이지, 헤더가 15바이트라는 뜻이 아니다.

따라서 헤더 길이는 $15 \times 4 = 60$바이트이다. 기본 헤더는 20바이트이지만 옵션과 패딩이 있으면 더 길어질 수 있으며, 4비트 IHL의 최대값 15에 해당하는 **최대 헤더 길이가 60바이트**이다. 이는 데이터부를 포함하는 패킷 전체 길이가 아니다.

계산 결과가 60바이트이므로 ④와 일치한다.

NoteBase

문 14. 리눅스 파일시스템에 관한 설명으로 가장 적절하지 않은 것은?

① ext 파일시스템은 Extended File System의 약자로 MFS의 기능을 확장했다.

② ext3 파일시스템은 저널링 기능을 도입하여 데이터의 복구 기능을 강화했다.

③ swap은 스왑 영역을 관리하기 위한 스왑 파일시스템이다.

④ proc는 메모리에 임시 파일을 저장하기 위한 파일시스템이며, 시스템이 재시작할 때마다 기존 내용이 없어진다.

정답 4번

간단한 해설

proc는 **프로세스·커널 상태 정보를 제공**하는 가상 파일시스템이다. 메모리에 임시 파일을 저장하는 용도는 tmpfs의 설명이며, proc와 구별해야 한다.

선지별 해설

① O: ext는 Extended File System으로, 초기 리눅스에서 사용하던 Minix 파일시스템(MFS)의 제약을 개선한 파일시스템이다. 지원 가능한 파일시스템 크기와 파일명 길이 등을 확장했다.

② O: ext3는 ext2에 **저널링 기능**을 추가했다. 변경 작업을 저널에 기록하여 비정상 종료 후 파일시스템의 일관성을 복구하는 데 활용한다. 다만 저널링이 모든 사용자 데이터의 손실을 막거나 백업을 대신한다는 뜻은 아니다.

③ O: swap은 메모리에서 내보낸 페이지를 저장하는 스왑 영역과 그 형식을 가리킨다. 전용 파티션이나 파일을 스왑 영역으로 사용할 수 있으며 가상메모리 관리에 이용된다. 여기서 '스왑 파일시스템'은 이러한 특수 영역을 가리키는 표현으로, **일반 파일·디렉터리를 저장하도록 마운트하는 파일시스템과는 다르다**.

④ X: proc는 실행 중인 **프로세스와 커널의 상태 정보를 파일 형태로 제공**하는 가상 파일시스템이다. 사용자가 임시 파일을 저장하는 용도가 아니다. 메모리 기반의 임시 파일 저장이라는 설명은 tmpfs에 해당한다. tmpfs의 내용은 재부팅하면 사라지며, 설정에 따라 일부 페이지가 스왑 공간으로 이동할 수도 있다.

따라서 proc를 임시 파일 저장용으로 설명한 ④가 가장 적절하지 않다.

NoteBase

문 15. OTP(One Time Password) 발생기의 인증방식-인증값의 연결이 가장 적절하지 않은 것은?

① S/KEY 방식 - 해시값

② 이벤트 동기화 방식 - 이벤트

③ 시간 동기화 방식 - 시간

④ 도전-응답(Challenge-response) 방식 - 난수

정답 2번

간단한 해설

이벤트 동기화 방식이 사용하는 것은 이벤트 자체가 아니라 **이벤트 발생 횟수인 카운터 값**이다. 발생기와 서버는 이 카운터를 기준으로 같은 일회용 암호를 생성·검증한다.

선지별 해설

각 연결은 OTP를 만드는 기준이나 처리 방식에 관한 것이다. 시간·난수·카운터 같은 입력값과 최종적으로 제출하는 OTP를 구별해야 한다.

① O: S/KEY는 일방향 해시 함수를 반복 적용하여 만든 해시 연쇄의 값을 일회용 암호로 사용한다. 서버는 제출된 값에 해시를 적용한 결과를 저장한 검증값과 비교하므로, 해시값이라는 연결이 적절하다.

② X: 이벤트 동기화 방식에서 동기화하는 값은 **이벤트 발생 횟수를 나타내는 카운터**이다. 버튼 조작 등의 이벤트는 카운터를 증가시키는 계기이며, 이벤트 자체를 인증값으로 사용하는 것이 아니다. 대표적인 HOTP는 공유 비밀키와 카운터를 입력으로 OTP를 생성한다.

③ O: 시간 동기화 방식은 발생기와 서버가 공유하는 시간 기준을 이용한다. 시간을 일정 구간으로 나눈 값과 공유 비밀키로 OTP를 생성하여 같은 시간 구간에서 검증한다. '시간'은 생성 기준을 가리키며, 현재 시각 자체를 그대로 암호로 제출한다는 뜻은 아니다.

④ O: 도전-응답 방식에서는 서버가 난수 등의 도전값을 제시하고, 발생기는 그 값과 비밀정보를 이용하여 응답값을 만든다. 서버는 예상 응답과 비교하여 인증한다. 난수는 매번 달라지는 도전값의 대표적 형태이며, 난수 자체를 되돌려 보내는 것만으로 인증하는 것은 아니다.

NoteBase

문 16. 다음에서 설명하는 접근 통제 구현 방법으로 가장 적절한 것은?

기술적 통제라고도 불리며, 보호해야 할 정보에 접근하는 것을 제한하기 위해 사용하는 하드웨어와 소프트웨어 도구를 말한다. 특정 애플리케이션에 접근할 수 있는 사용자의 IP 주소 외에 다른 주소는 접근을 차단하는 방법이 이에 해당한다.

① 관리적 접근 통제
② 논리적 접근 통제
③ 물리적 접근 통제
④ 상대적 접근 통제

정답 2번

간단한 해설

하드웨어·소프트웨어의 규칙으로 정보 자원에 대한 접근을 제한하는 것은 **논리적 접근 통제**이다. 허용된 IP 주소만 애플리케이션에 접근하게 하는 사례가 이에 해당한다.

대응 관계 해설

기술적 통제와 도구: 논리적 접근 통제는 인증·권한 설정·접근 제어 규칙 등을 하드웨어와 소프트웨어로 구현하여 정보 시스템 이용을 제한하는 것이다. 통제 대상은 시설 출입이 아니라 **정보와 시스템 자원에 대한 전자적 접근**이다.

IP 주소에 따른 차단: 허용된 IP 주소의 요청만 통과시키고 나머지를 차단하는 것은 시스템이 주소와 규칙을 비교하여 접근 여부를 결정하는 방식이다. 따라서 **접근 제어 규칙의 기술적 집행**에 해당한다.

관리적 접근 통제는 정책·절차·교육 등으로, 물리적 접근 통제는 출입문·잠금장치·경비 등으로 접근을 통제한다. 장비를 사용한다는 사실만으로 물리적 통제가 되는 것은 아니다. 제시문의 기술적 접근 제한은 ② 논리적 접근 통제에 대응하며, 상대적 접근 통제는 이 분류의 해당 명칭이 아니다.

NoteBase

문 17. 안티 리버싱 기법으로 가장 적절하지 않은 것은?

① 언패킹

② 안티 디버깅

③ 타이밍 체크

④ 쓰레기 코드 넣기와 코드 치환

정답 1번

간단한 해설

안티 리버싱은 프로그램의 구조와 동작을 분석하기 어렵게 하는 기법이다. **언패킹은 패킹된 코드를 풀어 분석 가능한 형태로 복원**하는 작업이므로 그 자체로는 분석 방해 기법에 해당하지 않는다.

선지별 해설

코드를 숨기거나 분석 환경을 탐지하는 기법과, 분석자가 그 보호를 해제하는 작업을 구분한다.

① X: 언패킹은 압축·암호화 등으로 포장된 실행 코드를 풀어 원래 코드나 분석 가능한 실행 이미지를 얻는 과정이다. 분석을 어렵게 하는 것은 일반적으로 패킹이며, **언패킹은 그 반대 방향의 복원 작업**이다. 보호된 프로그램이 실행 중 자체적으로 압축을 푸는 경우가 있어도, 언패킹 자체를 안티 리버싱 기법으로 분류하지는 않는다.

② O: 안티 디버깅은 디버거의 존재나 디버깅 환경을 탐지하고 분석을 방해하는 기법이다. 실행 흐름을 추적하며 내부 동작을 파악하는 동적 분석을 어렵게 한다.

③ O: 타이밍 체크는 코드 구간의 실행시간 등을 확인해, 중단점이나 단계별 실행 때문에 평소와 다른 지연이 발생하는지 살피는 기법이다. 분석 환경을 의심하는 데 사용할 수 있지만, 지연만으로 디버깅 여부가 항상 정확히 판별되는 것은 아니다.

④ O: 쓰레기 코드 넣기는 실제 기능에 필요하지 않은 코드를 추가해 분석량을 늘리는 난독화 기법이다. 코드 치환은 원래와 같은 기능을 수행하는 다른 명령 조합으로 표현을 바꾸어 구조나 패턴의 식별을 어렵게 한다. 두 방법 모두 의미를 파악하는 역공학 작업을 방해할 수 있다.

NoteBase

문 18. 다음 설명에 해당하는 공격으로 가장 적절한 것은?

◯ 제어 채널과 데이터 채널을 다르게 사용하고, 데이터 채널을 생성할 때 목적지를 확인하지 않는 FTP의 취약점을 이용하여 공격한다.
◯ FTP의 능동 모드에서 클라이언트의 IP 주소, 포트 번호가 아닌 임의의 IP주소를 지정할 수 있는 기능을 이용한 공격이다.

① Bounce Attack
② Brute-Force Attack
③ Anonymous FTP Attack
④ Passive Attack

정답 1번

간단한 해설

FTP 서버가 능동 모드의 데이터 연결 목적지로 제3자 주소를 허용하면, 서버를 중계점처럼 악용할 수 있다.
이처럼 **FTP 서버를 거쳐 다른 시스템에 접속하도록 유도**하는 것이 바운스 공격이다.

NoteBase

대응 관계 해설

두 설명은 **FTP 바운스 공격**의 특징이다. FTP는 명령을 주고받는 제어 연결과 실제 파일 자료를 전달하는 데이터 연결을 별도로 사용한다. 연결이 분리되어 있다는 사실만으로 공격이 성립하는 것은 아니며, 데이터 연결의 목적지에 대한 검증이 부족한 경우가 문제이다.

능동 모드에서는 클라이언트가 알려 준 주소와 포트로 서버가 데이터 연결을 시도한다. 이때 서버가 제3자의 주소를 허용하면 **FTP 서버를 중계점으로 다른 시스템에 접속**하게 만들 수 있다. 제시문의 '클라이언트가 아닌 임의의 IP 주소 지정'이 이를 식별하는 결정적 단서이다.

Brute-Force Attack은 가능한 비밀번호나 키 후보를 반복해서 시도하는 공격이다. 이 문제의 핵심은 인증 정보를 추측하는 것이 아니라 데이터 연결의 목적지를 악용하는 데 있다.

Anonymous FTP Attack은 익명 접속을 허용하는 FTP의 접근권한이나 설정을 악용하는 경우와 관련된다. 익명 접속 기능 자체가 곧 바운스 공격을 뜻하지 않으며, 제시문의 공격은 제3자 데이터 연결 허용 여부로 구분한다.

Passive Attack은 일반적으로 통신을 변경하지 않고 도청·관찰하여 정보를 얻는 수동적 공격을 가리킨다. 제시문처럼 서버의 접속 동작을 유도하는 바운스 공격과 다르며, FTP의 수동 모드라는 접속 방식과도 같은 뜻이 아니다.

따라서 두 단서에 대응하는 것은 ① Bounce Attack이다.

NoteBase

문 19. 윈도우에서 실행되는 각 서비스에 관한 설명으로 가장 적절하지 않은 것은?

① csrss.exe : 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스이다.

② smss.exe : 사용자 세션을 시작하는 기능을 담당하는 프로세스로, winlogon, win32를 구동시킨다.

③ svchost.exe : DLL이 실행하는 프로세스의 기본 프로세스로, 한 시스템에서 svchost 프로세스를 여러 개 볼 수 있다.

④ winmgmt.exe : 윈도우 작업 관리자 자신의 프로세스이다.

정답 4번

간단한 해설

Windows 작업 관리자의 실행파일은 **taskmgr.exe**이다. winmgmt는 시스템 관리 정보를 제공하는 **WMI**와 관련되어 있으므로 작업 관리자 자체와 다르다.

NoteBase

선지별 해설

이 문항의 설명은 기존 32비트 Windows NT 계열의 프로세스 역할을 바탕으로 한다. 운영체제 버전에 따른 구현 차이와 각 프로세스의 본래 역할을 구분해야 한다.

① O: csrss.exe는 Client/Server Runtime Subsystem의 사용자 모드 프로세스이다. 기존 Windows에서 콘솔 처리, 프로세스·스레드 관련 지원 및 가상 DOS 환경의 일부 기능을 담당한다. 보기의 32비트 가상 MS-DOS 지원은 이러한 **32비트 Windows의 VDM 지원 맥락**에서 이해한다. DOS 실행 환경의 기반 실행파일은 ntvdm.exe이며, 16비트와 32비트 DOS 프로그램을 지원한다. CSRSS 자체가 DOS 실행기라는 뜻은 아니며, 이 기능을 64비트 Windows에도 일반화하면 안 된다.

② O: smss.exe는 Session Manager Subsystem으로 세션 초기화를 담당한다. 세션에 필요한 CSRSS 등 Windows 하위 시스템과 로그인 관련 프로세스를 시작한다. 보기의 win32는 이러한 Win32 하위 시스템을 가리키며, 사용자 세션에서는 winlogon.exe의 실행과 연결된다.

③ O: svchost.exe는 **DLL로 구현된 Windows 서비스를 로드하여 실행하는 호스트**이다. 서비스 그룹이나 개별 서비스가 별도 호스트에서 실행될 수 있으므로 한 시스템에 여러 svchost.exe 프로세스가 존재할 수 있다. DLL 자체가 독립 실행파일처럼 실행되는 것은 아니다.

④ X: winmgmt는 **WMI(Windows Management Instrumentation)**와 관련된 구성 요소로 시스템 관리 정보의 조회·관리를 지원한다. Windows 작업 관리자 자체의 실행파일은 **taskmgr.exe**이다. 시스템 관리 정보 제공 기능과 작업 관리자 프로그램을 혼동한 설명이다.

따라서 작업 관리자 프로세스를 잘못 연결한 ④가 가장 적절하지 않다.

NoteBase

문 20. 인터넷 계층별 보안 서비스를 제공하는 프로토콜의 연결이 가장 적절하지 않은 것은?

① 응용 계층 - MPLS

② 응용 계층 - HTTPS

③ 네트워크 계층 - IPSec

④ 데이터링크 계층 - PPTP

정답 1번

간단한 해설

MPLS는 응용 계층 보안 프로토콜이 아니라 **레이블을 이용해 패킷을 전달하는 기술**이다. 흔히 데이터링크 계층과 네트워크 계층 사이의 '2.5계층' 기술로 설명한다.

선지별 해설

프로토콜이 보호하거나 다루는 대상과, 실제 전송에 사용하는 하위 프로토콜을 구분하여 계층을 판단한다.

① X: MPLS는 패킷을 전달할 때 레이블을 붙이고 교환하는 방식이다. 데이터링크 계층과 네트워크 계층 사이의 기능으로 설명되며 **응용 계층과 연결하는 것은 잘못**이다. MPLS 기반 VPN이 트래픽을 논리적으로 분리할 수 있어도, MPLS 자체가 응용 데이터를 암호화하는 프로토콜이라는 뜻은 아니다.

② O: HTTPS는 HTTP 통신을 TLS로 보호하는 방식으로, 웹 응용의 안전한 통신과 연결된다. 따라서 응용 계층 서비스인 HTTP의 보안 방식으로 분류하는 연결은 적절하다. 이때 암호화·인증 등의 실제 보호 기능은 하위의 TLS가 담당한다.

③ O: IPsec은 IP 계층에서 보안 서비스를 제공한다. 설정과 사용 프로토콜에 따라 IP 패킷에 인증·무결성·기밀성 등을 제공하므로 네트워크 계층과의 연결이 적절하다.

④ O: PPTP는 데이터링크 계층의 PPP 트래픽을 IP 네트워크를 통해 터널링하는 방식으로, 2계층 터널링 프로토콜로 분류한다. 따라서 데이터링크 계층과의 연결은 적절하다. 이는 PPTP가 독립적으로 모든 암호화 기능을 제공하거나 현재의 안전한 VPN 선택임을 뜻하지 않으며, 터널링 계층의 분류와 보안성 평가는 구별해야 한다.

NoteBase

문 21. 다음에서 침입차단 시스템 구현 유형과 명칭의 연결이 가장 적절한 것은?

가. 접근통제, 로그 관리 등의 기능을 지원할 수 있으나 처리 속도가 상대적으로 느리다.
나. OSI 전 계층에서 패킷의 콘텐츠를 해석하여 침입차단을 수행한다.
다. 3계층과 4계층에서 동작하며 IP 프로토콜과 포트를 차단 및 허용할 수 있다.

① 가: 애플리케이션 게이트웨이, 나: 패킷 필터링, 다: 상태기반 패킷 검사
② 가: 애플리케이션 게이트웨이, 나: 상태기반 패킷 검사, 다: 패킷 필터링
③ 가: 회선 게이트웨이, 나: 데이터그램 필터링, 다: 상태기반 패킷 검사
④ 가: 회선 게이트웨이, 나: 상태기반 패킷 검사, 다: 데이터그램 필터링

정답 2번

간단한 해설

응용 요청의 해석·중계는 애플리케이션 게이트웨이, 통신 상태와 문맥을 이용하는 검사는 상태기반 패킷 검사에 해당한다. IP·프로토콜·포트로 허용 여부를 정하는 것은 **패킷 필터링**이다.

대응 관계 해설

가. 애플리케이션 게이트웨이: 응용 서비스의 프록시로 동작하여 애플리케이션 수준의 요청을 확인하고 접근 통제와 상세 로그를 제공한다. **응용 프로토콜을 해석하고 중계하는 처리**가 추가되어 단순 패킷 필터보다 상대적으로 느릴 수 있다. 회선 게이트웨이는 주로 연결·세션의 성립을 중계하는 방식이다.

나. 상태기반 패킷 검사: 개별 패킷의 헤더만 보는 것이 아니라 **이전 통신에서 얻은 상태와 현재 패킷의 문맥**을 함께 이용한다. 제시문은 여러 계층에서 얻은 통신·응용 정보를 분석하는 Stateful Inspection의 확장된 설명에 해당한다. 모든 구현이 언제나 모든 계층의 내용을 완전히 해석한다는 뜻은 아니다.

다. 패킷 필터링: 주로 네트워크 계층의 IP 주소·프로토콜 정보와 전송 계층의 포트 번호 등을 규칙과 비교한다. 따라서 **3·4계층의 헤더 정보에 따른 허용·차단**이라는 단서가 패킷 필터링에 대응한다.

가–애플리케이션 게이트웨이, 나–상태기반 패킷 검사, 다–패킷 필터링의 연결이므로 ②에 해당한다.

NoteBase

문 22. IPv4 헤더 필드 중에서 라우터를 통과하면서 값이 변경되는 필드로 가장 적절한 것은?

① Protocol

② TTL

③ Source Address

④ Version

정답 2번

간단한 해설

라우터는 패킷을 전달할 때 **TTL을 감소**시켜 패킷이 무한히 순환하는 것을 막는다. 감소한 TTL이 0이면 패킷을 더 전달하지 않는다.

선지별 해설

여기서 O/X는 일반적인 IPv4 라우팅에서 전달할 때마다 값이 바뀌는 필드인지에 대한 판단이다.

① X: Protocol은 IPv4 데이터 부분에 들어 있는 상위 프로토콜을 식별한다. 예를 들어 TCP와 UDP를 구별하며, 일반적인 라우팅 과정에서 홉마다 바뀌는 필드는 아니다.

② O: TTL(Time To Live)은 패킷이 네트워크에서 무한히 순환하지 않도록 수명을 제한한다. 라우터가 패킷을 전달할 때 **TTL을 최소 1 감소**시키며, 감소 결과가 0이면 더 전달하지 않고 폐기한다. 일반적으로 홉 수의 한계처럼 작동한다.

③ X: Source Address는 최초 송신자의 IPv4 주소이며, 일반적인 IP 라우팅만으로는 라우터를 지날 때마다 변경되지 않는다. NAT가 적용되면 주소가 변환될 수 있지만, 이는 주소 변환 기능에 의한 것이지 모든 라우터 통과에 공통된 동작은 아니다.

④ X: Version은 사용하는 IP 버전을 표시하며 IPv4 패킷에서는 4이다. 라우터가 IPv4 패킷을 전달한다고 해서 이 값이 홉마다 바뀌거나 자동으로 IPv6로 변하는 것은 아니다.

NoteBase

문 23. 다음 중 망 분리에 관한 설명에 해당하는 레벨의 연결이 가장 적절한 것은?

가. 망 분리를 통해 업무 프로세스를 재정립하여 인터넷망에 있어야 하는 시스템과 업무망에 있어야 하는 시스템을 분리한다.
나. 인터넷 사용 PC와 업무용 PC를 분리하여 운영한다.
다. 인터넷 접속망과 업무용 망이 분리되어 있다.

① 가: 단말 레벨, 나: 업무 레벨, 다: 네트워크 레벨
② 가: 네트워크 레벨, 나: 단말 레벨, 다: 업무 레벨
③ 가: 업무 레벨, 나: 단말 레벨, 다: 네트워크 레벨
④ 가: 업무 레벨, 나: 네트워크 레벨, 다: 단말 레벨

정답 3번

간단한 해설

업무 프로세스와 시스템 배치를 구분하는 것은 **업무 레벨**, 사용 PC를 나누는 것은 **단말 레벨**, 접속망을 나누는 것은 **네트워크 레벨**이다.

대응 관계 해설

가. 업무 레벨이다. 업무 프로세스를 재정립하고 각 시스템이 인터넷망과 업무망 중 어디에 있어야 하는지 정하는 것은 **업무의 성격과 처리 흐름**에 따라 분리 범위를 정하는 일이다. 단순히 장비를 나누기 전에 업무와 시스템의 배치를 설계하는 관점이다.

나. 단말 레벨이다. 인터넷 사용 PC와 업무용 PC를 구분하여 운영한다는 설명은 **사용자가 직접 사용하는 단말**을 분리하는 관점이다. 여기서는 분리 대상이 PC로 명시되어 있으므로 네트워크 연결 자체를 나누는 설명과 구별된다.

다. 네트워크 레벨이다. 인터넷 접속망과 업무용 망이 구분되어 있다는 설명은 **통신 경로와 네트워크 영역**을 분리하는 관점이다. 어떤 업무를 어디에 배치할지 정하는 업무 레벨이나 사용 PC를 나누는 단말 레벨과 초점이 다르다.

따라서 가는 업무 레벨, 나는 단말 레벨, 다는 네트워크 레벨로 연결되므로 ③과 일치한다.

NoteBase

문 24. 다음에서 설명하는 용어로 가장 적절한 것은?

◯ 신뢰 컴퓨팅을 위한 하드웨어/소프트웨어 방법에서 핵심이 되는 하드웨어 모듈이다.
◯ 이것은 하드웨어 칩으로 구현하는 것이 일반적이나 소프트웨어로 구현하기도 하며, 암호화 키의 생성과 저장, 패스워드의 저장, 디지털 인증서 관련 신뢰 연산 등이 제공된다.

① TCB
② TPM
③ 보안 커널
④ 참조 모니터

정답 2번

간단한 해설

암호키를 생성·보호하고 플랫폼의 신뢰를 뒷받침하는 **보안 모듈**이라는 점이 핵심이다. 이는 신뢰 플랫폼 모듈인 TPM이며, 시스템의 모든 보호요소를 통칭하는 TCB와 다르다.

대응 관계 해설

‘신뢰 컴퓨팅의 핵심 모듈’과 ‘암호화 키의 생성·저장 및 신뢰 연산’이라는 단서는 **TPM(Trusted Platform Module)**에 대응한다. TPM은 키 보호와 암호 연산, 플랫폼 측정값의 보관 및 증명 등을 지원해 신뢰의 기반을 제공한다.

TPM은 독립된 보안 칩으로 구현될 수 있고, 펌웨어나 가상화 환경의 소프트웨어 구현 형태도 있다. 구현 형태에 따라 격리와 변조 저항성 등 보호 수준은 달라지므로, 모두 동일한 하드웨어 보호를 제공한다고 보아서는 안 된다. 제시문의 패스워드 저장이나 인증서 관련 연산은 인증 비밀과 키를 보호해 인증을 지원한다는 맥락이며, 모든 비밀번호를 평문으로 저장한다는 뜻은 아니다.

TCB(Trusted Computing Base)는 시스템의 보안정책을 집행하는 데 관여하는 하드웨어·펌웨어·소프트웨어 보호요소의 전체 집합이다. 특정 암호 모듈 하나를 지칭하는 TPM보다 넓은 개념이다.

참조 모니터는 주체의 객체 접근을 보안정책에 따라 검사하는 추상적 접근통제 개념이다. 보안 커널은 이 참조 모니터 개념을 실제로 구현하는 TCB의 핵심 요소를 뜻한다. 따라서 둘 모두 제시문의 암호키 생성·저장 모듈이라는 설명과 직접 대응하지 않는다.

NoteBase

문 25. 다음에서 설명하는 무결성 점검 도구로 가장 적절한 것은?

○ 유닉스/리눅스 환경에서 파일시스템 무결성을 점검하는 대표적인 도구로 오픈 소스 버전과 상용 버전이 있다.
○ MD5, SHA 등의 다양한 해시 함수를 지원하고, 파일 및 디렉터리의 해시값을 생성하여 데이터베이스를 만들어 이를 통해 공격자들에 의한 파일들의 변조 여부를 판별한다.

① Nmap
② Nessus
③ Tripwire
④ SATAN

정답 3번

간단한 해설

파일의 해시와 속성을 기준 데이터베이스에 저장하고 현재 값과 비교하여 변경을 탐지하는 도구는 **Tripwire**이다.

대응 관계 해설

파일시스템 무결성 점검: Tripwire는 파일과 디렉터리의 상태 변화를 감시하는 도구이며 오픈 소스 계열과 상용 제품이 있다. 네트워크의 열린 포트를 찾는 것이 아니라 **관리 대상 파일의 기준 상태와 현재 상태**를 비교한다.

해시값과 기준 데이터베이스: 신뢰할 수 있는 시점의 파일 해시와 권한·소유자 등의 속성을 기준 데이터베이스에 보관하고, 이후 검사에서 다시 얻은 값과 대조한다. **기준값과의 차이**로 변경을 탐지하되, 정상 업데이트인지 공격자의 변조인지는 승인된 변경 내역 등과 함께 판단해야 한다.

Nmap은 네트워크 호스트와 포트·서비스 탐색, Nessus와 SATAN은 취약점 점검에 초점을 둔다. 해시 기반의 파일 무결성 비교라는 설명에 대응하는 선택지는 ③ Tripwire이다.

NoteBase

문 26. OSPF 라우팅 프로토콜에 사용되는 알고리즘으로 가장 적절한 것은?

① Dijkstra 알고리즘

② Greedy 알고리즘

③ Distance Vector 알고리즘

④ Euclidean 알고리즘

정답 1번

간단한 해설

OSPF는 링크 상태 정보로 구성한 그래프에서 자신을 기준으로 최단 경로 트리를 계산한다. 이때 사용하는 구체적인 SPF 알고리즘이 **Dijkstra 알고리즘**이다.

핵심 풀이

OSPF는 링크 상태 라우팅 프로토콜이다. 라우터는 영역의 링크 상태 정보를 바탕으로 네트워크 그래프를 구성하고, **자신을 출발점으로 하는 최단 경로 트리**를 계산한다. 이 SPF 계산에 사용되는 대표적인 구체적 알고리즘이 Dijkstra 알고리즘이다.

Dijkstra 알고리즘은 비음수 링크 비용을 전제로, 현재까지 확인된 후보 중 출발점으로부터의 비용이 가장 작은 정점을 차례로 확정하고 인접 정점의 경로 비용을 갱신한다. 여기서 최단 경로는 단순한 지리적 거리나 홉 수가 아니라 **링크 비용의 합이 최소인 경로**를 뜻한다.

Greedy는 매 단계에서 현재 최선의 선택을 하는 탐욕적 설계 전략을 가리킨다. Dijkstra도 이 전략에 속하지만, OSPF가 사용하는 알고리즘을 구체적으로 묻는 문항에서는 Dijkstra가 더 정확한 답이다.

Distance Vector는 이웃 라우터가 알려 준 목적지까지의 거리 정보를 이용하여 경로를 갱신하는 방식으로, 링크 상태 정보를 바탕으로 SPF를 계산하는 OSPF와 구별된다.

Euclidean 알고리즘은 최대공약수를 구하는 유클리드 알고리즘으로, OSPF의 경로 계산 알고리즘이 아니다.

따라서 가장 적절한 것은 ① Dijkstra 알고리즘이다.

NoteBase

문 27. IPSec에 대한 설명으로 가장 적절하지 않은 것은?

① 보안 서비스가 제공되는 방식에는 전송 모드와 터널 모드가 존재한다.

② AH는 암호화를, ESP는 인증과 무결성 기능을 제공한다.

③ 암호화 기술을 이용하여 IP 패킷 단위로 데이터 변조 방지 및 은닉 기능을 제공한다.

④ 터널 모드는 IP 헤더를 포함한 기존 전체 패킷 앞에 새로운 IPSec 헤더 정보가 추가된다.

정답 2번

간단한 해설

AH는 인증·무결성을 제공하지만 **데이터 암호화는 제공하지 않는다**. ESP는 기밀성을 위한 암호화와 함께 인증·무결성도 제공할 수 있다.

선지별 해설

① O: IPSec은 전송 모드와 터널 모드로 적용할 수 있다. 전송 모드는 원래 IP 헤더를 유지하면서 그 뒤에 보안 헤더를 넣고, 터널 모드는 원래 IP 패킷 전체를 새로운 IP 패킷 안에 캡슐화한다.

② X: AH(Authentication Header)는 데이터 출처 인증과 무결성 등을 제공하지만 **기밀성을 위한 데이터 암호화는 제공하지 않는다**. ESP(Encapsulating Security Payload)는 암호화에 의한 기밀성과 함께 인증·무결성을 제공할 수 있다. 따라서 ESP가 인증·무결성을 제공한다는 부분 자체가 틀린 것이 아니라, AH가 암호화를 한다는 설명이 오류이다. 실제 ESP의 보안 서비스 조합은 설정에 따라 달라진다.

③ O: IPSec은 네트워크 계층에서 IP 패킷을 보호한다. 인증·무결성 기능은 데이터 변조를 탐지하여 변조된 패킷을 거부하게 하고, 기밀성 기능은 암호화로 내용을 숨긴다. 여기서 암호 기술은 이들 기능을 포괄하며, **암호화만으로 무결성이 자동 보장되는 것은 아니다**.

④ O: 터널 모드에서는 기존 IP 헤더와 데이터를 합친 원래 IP 패킷이 내부 패킷이 된다. 그 앞에 AH 또는 ESP 보안 헤더가 붙고, 바깥쪽에는 **터널 구간 전달을 위한 새로운 IP 헤더**도 추가된다. 즉 원래 IP 헤더를 버리는 것이 아니라 내부에 포함한 채 새 패킷으로 감싼다.

따라서 AH에 암호화 기능을 잘못 부여한 ②가 가장 적절하지 않다.

NoteBase

문 28. WEP 인증에 대한 설명으로 가장 적절하지 않은 것은?

① RC4 대칭형 암호화 알고리즘을 사용하며 24bit의 IV를 결합하여 공유 비밀키를 생성한다.

② IEEE 802.11b의 표준인 스트림 암호화 기법을 사용한다.

③ 정적 키를 사용하기 때문에 무작위 공격에 취약하다.

④ AP는 인증 요청을 받으면 임의로 생성한 인증용 문자열을 암호화키로 암호화하여 클라이언트에 전송한다.

정답 4번

간단한 해설

WEP 공유키 인증에서는 AP가 도전 문자열을 **평문으로 보내고, 클라이언트가 암호화하여 응답**한다. AP가 최초 문자열부터 암호화해 전송하는 절차가 아니다.

선지별 해설

① O: WEP는 대칭형 스트림 암호인 RC4를 사용하며, 미리 공유한 비밀키에 24비트 초기화 벡터(IV)를 연결하여 RC4의 입력 키를 구성한다. 예를 들어 40비트 비밀키와 24비트 IV를 합치면 64비트 입력이 된다. 선지의 키 생성은 이 결합을 가리키며, **IV 자체가 비밀이거나 새로운 장기 공유키를 합의한다는 뜻은 아니다**.

② O: WEP는 IEEE 802.11 계열 무선랜에서 사용된 보안 방식이며, 802.11b 환경에서도 RC4 스트림 암호를 사용하였다. RC4로 만든 키 스트림과 평문을 결합해 암호화하는 방식이다.

③ O: 기본적인 WEP 운용은 정적으로 공유한 비밀키를 반복 사용한다. 키가 바뀌지 않으면 장기간 자료를 모아 키 후보를 시험할 수 있으며, 짧은 IV의 반복과 RC4 키 구성의 약점도 공격에 악용된다. 정적 키만이 유일한 취약 원인은 아니다.

④ X: 공유키 인증에서 AP는 임의의 인증용 문자열을 먼저 **평문으로** 클라이언트에 보낸다. 클라이언트가 그 문자열을 공유한 WEP 키로 암호화하여 돌려보내면 AP가 복호화한 결과를 원래 문자열과 비교한다. 처음 도전 문자열을 AP가 암호화해 보내는 것으로 설명한 점이 잘못되었다.

NoteBase

문 29. 다음에서 설명하는 블루투스 공격으로 가장 적절한 것은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다. 공격자는 블루투스 장치끼리 인증 없이 간편하게 정보를 교환하도록 개발된 OPP(Obex Push Profile) 기능을 이용하여 블루투스 장치에 있는 주소록이나 달력 등의 내용을 요청하여 열람하거나 취약한 장치의 파일에 접근할 수 있다.

① 블루스나핑
② 블루프린팅
③ 블루버깅
④ 블루재킹

정답 1번

간단한 해설

블루투스 취약점을 악용해 주소록·달력 등 저장된 정보를 **사용자 허락 없이 가져오는** 공격이 블루스나핑이다. 지문에서 파일을 요청하여 열람한다는 점이 정보 탈취를 가리킨다.

공통 해설

블루스나핑은 블루투스 연결을 통해 상대 장치에 저장된 정보를 무단으로 읽거나 가져오는 공격이다. 지문의 '주소록이나 달력 등의 내용을 요청하여 열람'한다는 설명은 **저장된 정보의 무단 취득**에 해당하므로 블루스나핑과 대응한다.

지문의 OPP는 명함 등 객체를 간편하게 교환하는 기능과 관련된다. 블루스나핑에서는 이 서비스에 접속한 뒤 파일을 요청하는 OBEX GET을 보내 주소록이나 달력 파일을 가져올 수 있다. 이는 **파일 접근을 제대로 제한하지 못하는 취약한 구현**을 악용하는 것이다. 인증 없이 서비스에 접속할 수 있다는 사실만으로 모든 장치에서 임의 파일을 읽을 수 있는 것은 아니다.

NoteBase

문 30. 다음에서 설명하는 보안 기술로 가장 적절한 것은?

기업과 기관의 보안 정책을 반영하고, 다양한 네트워크 보안 제품의 인터페이스를 표준화하여 중앙 통합 관리, 침입 종합 대응, 통합 모니터링 등을 효율적으로 구현한 지능형 보안 관리 시스템이다.

① IDS
② ESM
③ NAC
④ IPS

정답 2번

간단한 해설

서로 다른 보안 제품을 연계하여 중앙 관리·통합 모니터링·종합 대응을 제공하는 것은 **ESM(통합 보안 관리)**이다.

대응 관계 해설

보안 정책과 이기종 제품 연계: ESM(Enterprise Security Management)은 서로 다른 보안 제품에서 발생하는 정보와 관리 기능을 통합하여 조직의 보안 정책에 맞게 운영하는 시스템이다. **여러 보안 제품의 연계와 통합 관리**가 핵심이다.

중앙 관리와 통합 모니터링: 장비별로 흩어진 상태·로그·이벤트를 중앙에서 수집하고 확인하므로 전체 보안 상황을 일관되게 파악할 수 있다. 단일 장비의 침입 탐지 기능과 달리 **조직 전체의 보안 운영을 한곳에서 관리**한다.

침입 종합 대응: 여러 장비에서 얻은 보안 이벤트를 함께 분석하여 위협을 파악하고 대응을 연계한다. 개별 경보를 따로 보는 데 그치지 않고 **장비 간 정보의 관련성**을 이용하는 것이다.

IDS는 침입 탐지·경보, IPS는 침입 탐지에 따른 차단, NAC는 사용자·단말의 네트워크 접근 통제에 초점을 둔다. 제시된 이기종 보안 제품의 중앙 통합 관리에 대응하는 선택지는 ② ESM이다.

NoteBase

문 31. 유닉스/리눅스 시스템 로그 설정(/etc/syslog.conf)에서 사용하는 메시지 우선순위 중 낮은 것부터 높은 것 순으로 가장 적절한 것은?

가. Notice
나. Alert
다. Error
라. Critical

① 가 < 나 < 다 < 라
② 가 < 다 < 라 < 나
③ 다 < 가 < 라 < 나
④ 다 < 나 < 가 < 라

정답 2번

간단한 해설

syslog의 심각도 코드는 **숫자가 작을수록 중요도가 높다**. 정상 상태의 중요한 알림보다 오류·중대 오류가 더 심각하며, 즉각 조치가 필요한 Alert는 이들보다 우선순위가 높다.

올바른 순서

가 → 다 → 라 → 나

가. Notice는 정상 상태이지만 주목할 만한 사건을 뜻하며, 심각도 숫자 코드는 5이다. 제시된 네 수준 중 가장 낮다. syslog의 심각도 코드는 **숫자가 작을수록 중요도가 높다**는 점에 유의하여 순서를 판단한다.

다. Error는 오류가 발생한 상태를 뜻하며, 코드는 3이다. 정상 범주의 중요한 알림인 Notice보다 중요도가 높다. 전체 심각도 체계에서는 Notice와 Error 사이에 Warning이 있지만, 이 문항의 보기에는 제시되어 있지 않다.

라. Critical은 중대한 오류나 심각한 상태를 뜻하며, 코드는 2이다. 일반적인 오류 수준인 Error보다 높은 우선순위로 취급한다.

나. Alert는 **즉각적인 조치가 필요한 상태**를 뜻하며, 코드는 1이다. Critical보다 중요도가 높아 제시된 네 수준 중 마지막에 위치한다. 전체 체계의 최상위인 Emergency는 코드 0이지만 이 문항의 보기에는 없다.

NoteBase

문 32. 다음 중 인터넷 전송계층 프로토콜인 TCP에서 사용되는 용어로 가장 적절하지 않은 것은?

① Process-to-Process Service

② Port number

③ Segment

④ Datagram

정답 4번

간단한 해설

TCP의 프로토콜 데이터 단위는 **세그먼트(Segment)**이다. 데이터그램(Datagram)은 보통 UDP나 IP의 데이터 단위를 가리키므로 TCP 자체의 단위와 구별한다.

선지별 해설

TCP는 전송계층에서 응용 프로세스 사이에 신뢰성 있는 바이트 스트림 전달을 제공한다. TCP의 서비스·주소·전송단위를 구분하여 살펴본다.

① O: Process-to-Process Service는 통신 양 끝 호스트에서 실행되는 응용 프로세스 사이에 전달 서비스를 제공한다는 의미이다. TCP는 단순히 호스트까지만 전달하는 IP의 역할 위에서 특정 응용의 통신을 지원한다.

② O: Port number는 한 호스트 안에서 통신 종단점을 구별하는 데 사용한다. TCP 헤더에는 출발지 포트와 목적지 포트가 있으며, IP 주소 등과 함께 연결 및 응용 전달 대상을 식별한다.

③ O: Segment는 TCP 헤더와 데이터를 포함하는 **TCP의 프로토콜 데이터 단위**이다. TCP는 응용의 바이트 스트림을 세그먼트로 전송하고, 수신 측에서는 순서와 재전송 등을 처리하여 스트림을 제공한다.

④ X: Datagram은 통상 UDP 데이터그램이나 IP 데이터그램을 설명할 때 사용하는 용어이다. TCP 자체의 데이터 단위는 세그먼트이므로 보기 중 가장 적절하지 않다. 다만 TCP 세그먼트가 하위 IP 데이터그램에 실려 전달될 수 있다는 사실까지 부정하는 것은 아니다.

NoteBase

문 33. 다음에서 설명하는 접근 통제 유형으로 가장 적절한 것은?

이것은 사용자 권한에 종속되지 않고, 민감하거나 중요한 자원에 대한 접근과 관련된 것이다. 예를 들면 일반 사용자가 관리자 권한을 전부 획득하지 못했더라도 관리자만 접근할 수 있는 메뉴에 접근하는 경우를 말한다.

① 수직적 접근 통제
② 수평적 접근 통제
③ 비즈니스 로직 접근 통제
④ 강제적 접근 통제

정답 3번

간단한 해설

사용자의 포괄적인 권한 수준만으로 판단하지 않고 **민감한 자원이나 개별 업무 기능에 대한 접근**을 통제하는 것이 비즈니스 로직 접근 통제이다. 지문은 관리자 권한 전체를 얻지 않은 상태에서도 관리자 메뉴에 접근하는 사례로 이를 설명한다.

개념 구분

비즈니스 로직 접근 통제: 애플리케이션의 업무 규칙에 따라 특정 기능이나 중요 자원에 접근할 수 있는지를 검사한다. 지문의 '사용자 권한에 종속되지 않고'는 권한 검사를 생략한다는 뜻이 아니라, **포괄적인 권한 수준과 별개로 개별 기능의 접근 허용 여부를 확인**한다는 취지이다. 일반 사용자가 관리자 권한 전체를 얻지 못했어도 관리자 메뉴에 들어갈 수 있다면, 그 메뉴에 필요한 접근 통제가 제대로 이루어지지 않은 것이다.

수직적 접근 통제: 관리자와 일반 사용자처럼 **권한 수준이 다른 사용자 집단**이 이용할 수 있는 기능을 구분한다. 일반 사용자의 관리자 메뉴 접근은 수직적 접근 통제 위반으로도 볼 수 있다. 다만 이 문항은 권한 수준 자체보다 민감한 자원과 개별 업무 기능에 대한 접근을 강조하므로 비즈니스 로직 접근 통제라는 설명에 대응한다. 수직적 접근 통제 위반이 반드시 관리자 권한 전체의 획득을 뜻하는 것은 아니다.

수평적 접근 통제: **같은 권한 수준에 있는 사용자 사이**에서 서로의 자원에 접근하지 못하도록 제한한다. 자신의 계좌만 조회할 수 있고 다른 사용자의 계좌는 조회할 수 없도록 하는 경우가 이에 해당한다. 지문은 동등한 사용자 사이의 자원 구분을 설명하지 않는다.

강제적 접근 통제: 시스템이 정한 보안 정책에 따라 접근을 강제하며, 대표적으로 **자원의 보안 등급과 사용자의 인가 등급**을 기준으로 허용 여부를 결정한다. 지문에는 이러한 등급에 따른 접근 판단이 제시되어 있지 않다.

NoteBase

문 34. 다음에서 설명하는 소스코드 취약점으로 가장 적절한 것은?

개발 단계에서 사용자의 권한에 대한 검증을 적절하게 수행하지 않았을 때 주로 발생하는 취약점이다. 이것이 취약할 경우, 공격자는 매개변수 조작이나 강제 브라우저 접근 등을 통해 다른 사용자나 상위 관리자의 정보를 볼 수도 있다.

① 위험한 형식의 파일 업로드 취약점

② 디렉터리 경로 조작 취약점

③ 코드 내 중요 정보 노출 취약점

④ 세션 처리 및 접근 통제 취약점

정답 4번

간단한 해설

요청한 사용자가 해당 정보에 접근할 권한이 있는지 확인하지 않으면 **다른 사용자나 관리자의 정보에 대한 무단 접근**이 가능해진다. 이는 세션의 사용자 신원과 접근 권한을 올바르게 확인하지 않는 접근 통제 문제이다.

대응 관계 해설

권한 검증 누락 → 세션 처리 및 접근 통제 취약점: 서버는 현재 세션의 사용자가 요청한 정보나 기능에 접근할 권한이 있는지 확인해야 한다. 보기에서는 이 검사가 부족해 다른 사용자나 관리자의 정보에 접근할 수 있으므로, 핵심은 **인증된 사용자의 요청이라도 대상별 권한을 검증하지 않은 것**이다.

접근 범위의 구별: 다른 일반 사용자의 정보에 접근하는 것은 수평적 권한 침해이고, 관리자처럼 더 높은 권한의 기능·정보에 접근하는 것은 수직적 권한 침해이다. 화면의 메뉴나 링크를 숨기는 것만으로는 서버의 접근 통제를 대신할 수 없으며, 매 요청마다 세션의 신원과 접근 권한을 검증해야 한다.

다른 취약점과의 구별: 위험한 형식의 파일 업로드는 허용해서는 안 되는 파일을 받아들이는 문제이고, 디렉터리 경로 조작은 입력된 경로를 적절히 제한하지 않아 허용 범위 밖의 파일에 접근하는 문제이다. 코드 내 중요 정보 노출은 소스코드에 비밀번호·키 같은 민감정보를 포함하는 문제이다. 보기의 직접적인 단서는 파일 형식·경로·코드 내 비밀이 아니라 사용자 권한의 검증 누락이다.

따라서 이 설명에 대응하는 것은 세션 처리 및 접근 통제 취약점이며, ④와 일치한다.

NoteBase

문 35. 다음 빈칸 (㉠), (㉡)에 들어갈 용어로 가장 적절한 것은?

패스워드는 해시와 암호화 알고리즘으로 변경하여 저장하지만, 해시값이나 암호문은 동일한 결과만으로도 패스워드를 노출하는 단점이 있다. 따라서, (㉠)는 이런 상황을 막기 위해 패스워드 해시와 암호화에 사용하는 첨가물의 일종으로 운영 체제별로 다양한 알고리즘이 존재한다. 패스워드 크래킹 방법 중 패스워드에 사용할 수 있는 문자열 범위를 정하고, 그 범위 안에서 생성 가능한 모든 패스워드를 생성하여 입력해 보는 방법이 (㉡)이다.

① ㉠: Salt ㉡: 사전 대입 공격

② ㉠: Salt ㉡: 무차별 대입 공격

③ ㉠: S/Key ㉡: 무차별 대입 공격

④ ㉠: S/Key ㉡: 사전 대입 공격

정답 2번

간단한 해설

같은 패스워드의 저장 결과가 달라지도록 함께 사용하는 값은 **Salt**이다. 정해진 범위의 모든 후보를 시도하는 방식은 **무차별 대입 공격**이다.

빈칸별 해설

㉠ Salt: 솔트는 패스워드로 해시값 등을 계산할 때 함께 사용하는 별도의 값이다. 같은 패스워드라도 **서로 다른 솔트를 사용하면 저장 결과가 달라지게** 하여 동일 패스워드의 직접 비교와 미리 계산한 해시 목록의 재사용을 어렵게 한다. 해시값이 같다는 사실만으로 원문 패스워드가 즉시 드러나는 것은 아니지만, 비교·추측 공격의 단서가 될 수 있다. S/Key는 일회용 패스워드 인증 방식으로 솔트와 다르다.

㉡ 무차별 대입 공격: 정한 문자 집합과 길이 등의 범위에서 **가능한 후보를 빠짐없이 생성하여 시도**하는 방식이다. 자주 쓰이는 단어·패스워드 목록을 우선 대입하는 사전 대입 공격과 구별된다. 솔트는 미리 만든 해시 목록의 공통 사용을 어렵게 하지만 개별 후보를 시험하는 공격 자체를 불가능하게 하지는 않는다.

㉠은 Salt, ㉡은 무차별 대입 공격이므로 ②에 해당한다.

NoteBase

문 36. 다음 중 SIEM에 대한 설명으로 가장 적절하지 않은 것은?

① 보안솔루션 위주의 로그를 수집하고 통합한다.

② 사용자, IP, Port, Application 등의 단위로 분석이 가능하고, APT 공격 및 알려지지 않은 패턴에 대한 분석이 가능하다.

③ MapReduce, indexing 등을 사용하며 고성능의 데이터 분석이 가능하다.

④ 수집하는 정보는 보안시스템, 보안소프트웨어, 네트워크 장비에 대한 로그, 이벤트, 웹로그 등을 대상으로 한다.

정답 1번

간단한 해설

SIEM은 보안장비의 경보만 모으는 데 그치지 않고 **서버·네트워크·응용 등 다양한 출처의 로그를 통합·상관분석**한다. 이를 보안솔루션 위주의 수집으로 한정한 설명이 가장 부적절하다.

선지별 해설

SIEM은 보안 정보 및 이벤트 관리 체계로, 여러 시스템에서 수집한 로그와 이벤트를 연결해 위협을 탐지하고 조사하는 데 활용한다.

① X: SIEM의 특징은 보안솔루션 로그에 국한되지 않는 **광범위한 데이터 수집과 통합 분석**이다. 보안장비 중심의 이벤트 통합관리와 구별할 때, SIEM은 서버·응용·네트워크·사용자 활동 등으로 분석 범위를 넓힌다. 따라서 보안솔루션 위주라고만 설명하면 SIEM의 핵심적인 확장성을 제대로 나타내지 못한다.

② O: 수집한 로그를 사용자, IP, 포트, 응용 등과 연결하여 분석할 수 있다. 여러 단계에 걸친 흔적의 상관관계나 비정상 행위를 분석하면 APT나 알려지지 않은 공격 패턴의 조사에도 활용할 수 있다. 다만 모든 SIEM이 모든 미지의 공격을 자동으로 찾아낸다는 의미는 아니다.

③ O: 대용량 데이터 처리를 위해 분산처리나 인덱싱 등의 기술을 활용할 수 있다. MapReduce는 이러한 분산 분석 방식의 예이며, 인덱싱은 검색 범위를 줄이는 데 도움이 된다. 특정 구현 기술의 사용 여부와 성능은 제품·구성에 따라 달라지므로 모든 SIEM에 동일한 구현이 필수인 것은 아니다.

④ O: 보안시스템과 보안소프트웨어의 이벤트뿐 아니라 네트워크 장비의 로그, 웹로그 등도 수집 대상이 될 수 있다. 출처가 다른 정보를 정규화하고 서로 연계해 분석한다는 점이 SIEM의 중요한 기능이다.

NoteBase

문 37. 다음에 출력된 내용의 밑줄 친 ㉠에 대한 설명으로 가장 적절한 것은?

[root@localhost ~]#crontab -l
- 생략 -
1 1 1 * * /home/cron.sh
㉠

① 매주 일요일 새벽 1시 1분에 cron.sh를 실행
② 매주 월요일 새벽 1시 1분에 cron.sh를 실행
③ 매월 1일 새벽 1시 1분에 cron.sh를 실행
④ 매일 새벽 1시 1분에 cron.sh를 실행

정답 3번

간단한 해설

crontab의 시간 필드는 분·시·일·월·요일 순서이다. 세 번째 값 1이 **매월 1일**을 지정하므로 매월 1일 새벽 1시 1분에 실행한다.

핵심 풀이

사용자 crontab의 시간 필드는 왼쪽부터 '분, 시, 일, 월, 요일' 순서이다. 그 뒤에는 실행할 명령이 온다. crontab -l은 현재 등록된 작업을 표시하는 명령이다.

밑줄 친 '1 1 1 * * /home/cron.sh'에서 첫 번째 1은 1분, 두 번째 1은 1시, 세 번째 1은 **매월 1일**을 뜻한다. 네 번째와 다섯 번째의 *는 각각 월과 요일을 제한하지 않는다는 뜻이다. 따라서 어느 요일이든 매월 1일 새벽 1시 1분에 /home/cron.sh를 실행한다.

요일은 세 번째가 아니라 다섯 번째 필드이므로 일요일이나 월요일마다 실행하는 설정이 아니다. 매일 실행하려면 일 필드도 *여야 하지만 여기서는 1로 지정되어 있다.

따라서 해당 설정을 설명한 선택지는 ③이다.

NoteBase

문 38. 다음에서 설명하는 이메일 보안 기술로 가장 적절한 것은?

IETF의 작업 그룹에서 개발한 전자우편 보안 기술이며, RFC 3370, 3850 등에 정의되어 있다. 전자우편에 대한 무결성, 부인 불가, 암호화, 인증 등의 기능 제공을 위해 다양한 암호 알고리즘이 사용된다.

① PGP

② PEM

③ S/MIME

④ Mail-Safe

정답 3번

간단한 해설

RFC 3850은 S/MIME의 인증서 처리를 규정한다. S/MIME는 전자우편에 서명과 암호화를 적용하고, 인증서 기반으로 인증·무결성·기밀성 등의 보안 기능을 제공한다.

대응 관계 해설

제시된 기술은 **S/MIME**이다. S/MIME는 MIME 형식의 전자우편 메시지에 전자서명과 암호화 등 보안 기능을 적용하는 기술이다. X.509 인증서를 이용하여 공개키와 주체의 관계를 확인하며, 암호 메시지 구문인 CMS를 활용한다.

문항에 제시된 **RFC 3850은 S/MIME 3.1의 인증서 처리**를 규정한 문서이다. RFC 3370은 CMS에 사용하는 암호 알고리즘에 관한 문서로, S/MIME의 암호 처리와 연결된다. 이 RFC 식별자가 선택지를 가르는 직접적인 근거이며, 해당 문서들이 최신 버전이라는 뜻은 아니다.

암호화는 메시지 내용을 허가되지 않은 사람이 읽지 못하도록 하여 기밀성을 제공한다. 전자서명은 메시지 변경 여부의 확인과 서명자 인증을 지원하며, 적절한 키 관리와 인증서 검증 아래 **부인 방지를 뒷받침하는 증거**가 된다. 암호화만으로 무결성·인증·부인 방지가 모두 자동 제공되는 것은 아니다.

PGP도 서명과 암호화를 제공하는 전자우편 보안 기술이지만, 제시된 RFC의 S/MIME 인증서 처리 규격과는 구별된다. PEM은 Privacy Enhanced Mail이라는 별도의 전자우편 보안 기술이며, Mail-Safe 역시 제시된 RFC 3850의 규격명이 아니다. 단순히 이메일 보안 기능이 있다는 공통점보다 특정 표준 문서와의 대응으로 판별해야 한다.

따라서 설명에 대응하는 것은 ③ S/MIME이다.

NoteBase

문 39. 다음에서 설명하는 SNMP의 구성 요소로 가장 적절한 것은?

이것은 관리할 개체의 집합이며, 관리자가 조회하거나 설정할 수 있는 개체들의 데이터베이스이고, 개체별로 트리 형식 구조를 이룬다. 관리될 각 개체를 위해 객체의 수를 결정하고, 이들을 정의된 규칙에 따라 이름을 붙이며, 각 객체에 유형을 연결한다.

① MIB

② SMI

③ OID

④ EGP

정답 1번

간단한 해설

SNMP에서 조회·설정할 관리 객체를 모아 계층적으로 정의한 관리 정보 베이스는 **MIB**이다. SMI는 객체를 정의하는 규칙, OID는 객체의 식별자이다.

대응 관계 해설

관리 개체의 집합: MIB(Management Information Base)는 네트워크 관리에 필요한 객체와 그 정보를 체계적으로 표현한 관리 정보 베이스이다. 관리자는 SNMP를 통해 객체의 값을 조회하거나 쓰기 권한이 있는 값을 설정하므로 **관리 대상 객체들의 논리적 데이터베이스**라는 설명에 대응한다.

트리 구조와 이름: 관리 객체는 계층적인 이름 공간에서 식별되며 각각 OID(Object Identifier)로 구분된다. **MIB는 객체들의 집합이고 OID는 객체를 식별하는 이름**이므로 둘은 같은 개념이 아니다.

객체 정의와 유형: MIB에는 관리할 객체를 선정하고 이름·자료형·접근 특성 등을 정의한다. 이 정의에 사용하는 공통 규칙과 표현 체계는 **SMI(Structure of Management Information)**가 제공한다. 규칙 자체인 SMI와 그 규칙에 따라 정의된 관리 정보인 MIB를 구별한다.

EGP는 자율 시스템 사이의 라우팅과 관련된 프로토콜 명칭이며 관리 객체의 데이터베이스가 아니다.

제시문의 핵심인 관리 개체의 집합에 대응하는 선택지는 ① MIB이다.

NoteBase

문 40. 다음에서 설명하는 악성코드로 가장 적절한 것은?

◯ 전파할 때 과다한 TCP/135, 445 트래픽이 발생한다.
◯ windows, windows/system32, winnt, winnt/system32 폴더에 svchost.exe 파일을 설치하고, 공격 성공 후 UDP/5599 등의 특정 포트를 열어 외부와 통신한다.
◯ 대표적으로 아고봇, 웰치아, 블래스터 등이 있다.

① 백도어
② 스파이웨어
③ 익스플로잇
④ 시스템 공격형 웜

정답 4번

간단한 해설

시스템 공격형 웜은 **네트워크 서비스의 취약점 등을 이용해 스스로 복제·전파**된다. 과도한 전파 트래픽과 아고봇·웰치아·블래스터라는 사례가 이 분류를 가리킨다.

NoteBase

대응 관계 해설

네트워크 전파 → 시스템 공격형 웜: 웜은 스스로 복제하여 다른 시스템으로 전파되는 악성코드이다. 보기의 TCP/135·445 트래픽 증가는 Windows 네트워크 서비스가 제공되는 시스템을 탐색하고 취약점을 이용하여 전파하는 행위의 단서이다. 핵심은 **시스템의 취약점을 이용한 자기 복제와 전파**이다.

파일 설치와 외부 통신: 제시된 폴더에 실행 파일을 설치하고 특정 포트를 열어 통신하는 것은 감염 후 실행과 외부 명령·자료 교환 등의 행위를 설명한다. 다만 정상 Windows에도 svchost.exe가 있으므로 파일명만으로 악성 여부를 단정할 수 없고, 설치 경로·동작·전파 행위를 함께 보아야 한다. 모든 웜이 같은 파일명이나 UDP/5599를 사용하는 것은 아니다.

대표 사례의 대응: 아고봇·웰치아·블래스터는 네트워크를 통해 전파되는 웜의 사례이다. 세부 공격 서비스나 통신 포트는 종류와 변종에 따라 다르지만, 시스템 취약점 등을 이용해 다른 컴퓨터로 확산한다는 공통 특징이 제시된 분류를 뒷받침한다.

다른 명칭과의 구별: 백도어는 정상 인증을 우회하여 접근하는 통로나 기능, 스파이웨어는 정보 수집·유출을 주목적으로 하는 악성 프로그램을 뜻한다. 익스플로잇은 취약점을 실제로 이용하는 코드나 기법이다. 웜이 백도어 기능이나 익스플로잇을 포함할 수는 있지만, 보기 전체의 자기 전파와 사례들을 포괄하는 명칭은 시스템 공격형 웜이다.

따라서 제시된 설명은 시스템 공격형 웜에 대응하며, ④와 일치한다.

NoteBase