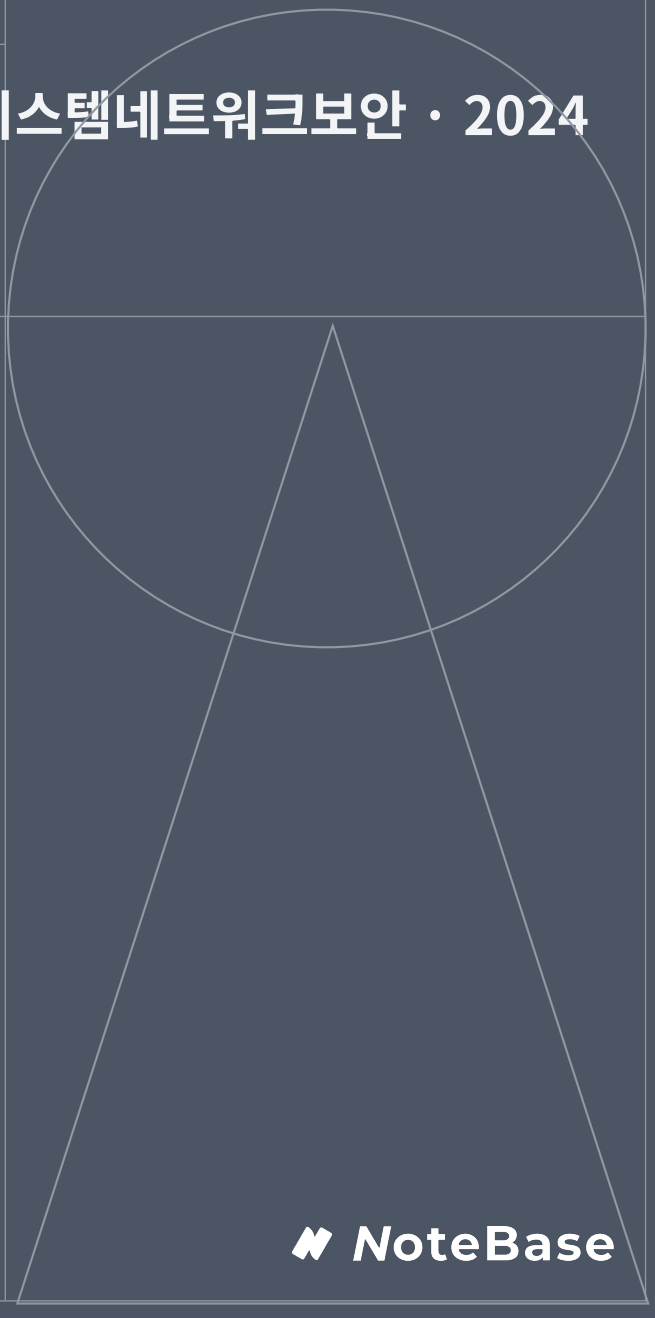
기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2024



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2024

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2024

문 1. 다음에서 설명하는 윈도우 인증 구성 요소로 가장 적절한 것은?

◯ 사용자, 그룹 계정 정보에 대한 데이터베이스를 관리한다.
◯ 사용자의 로그인 입력 정보와 데이터베이스 정보를 비교하여 일치 여부를 확인한다.

① SAM(Security Account Manager)
② SRM(Security Reference Monitor)
③ SMB(Server Message Block)
④ LSA(Local Security Authority)

정답 1번

간단한 해설

정답은 ① **SAM**이다. SAM은 로컬 사용자·그룹 계정 데이터베이스를 관리하며 로그인 인증에 필요한 계정 정보를 제공한다. 인증 절차 전반을 담당하는 LSA와 계정 정보 저장·관리 역할을 구별해야 한다.

NoteBase

대응 관계 해설

첫 번째 단서인 사용자·그룹 계정 데이터베이스 관리는 SAM에 대응한다. SAM은 로컬 컴퓨터의 사용자 계정과 그룹 등 계정 정보를 관리하며, 로컬 계정 인증에 사용하는 정보를 보관한다. 이 단서가 정답을 가르는 핵심이다.

두 번째 단서는 로그인 시 제출된 자격 증명을 저장된 계정 정보와 대조하는 과정을 가리킨다. 로컬 계정의 경우 SAM에 저장된 인증 정보를 사용하며, LSA와 인증 패키지가 이 인증 과정에 관여한다. SAM이 로그인 화면부터 모든 인증 절차를 혼자 처리한다는 뜻은 아니다.

① SAM은 두 단서를 종합했을 때 가장 적절하다. 특히 **로컬 사용자·그룹 계정 데이터베이스의 관리**라는 기능이 SAM을 직접 가리키므로 정답은 ①이다.

② SRM은 보안 참조 모니터로, 접근 토큰과 객체의 보안 정보 등을 바탕으로 보호된 자원에 대한 접근 권한을 검사하는 커널 구성 요소이다. 계정 데이터베이스를 관리하는 SAM과 역할이 다르다.

③ SMB는 네트워크에서 파일·프린터 등 자원을 공유하는 데 쓰이는 통신 프로토콜이다. 사용자·그룹 계정 데이터베이스를 관리하는 인증 구성 요소가 아니다.

④ LSA는 로컬 보안 정책과 사용자 인증 등의 보안 기능을 담당하며 인증 패키지와 협력한다. SAM을 이용하여 로컬 사용자 정보를 확인할 수 있지만, 제시문이 강조하는 계정 데이터베이스 관리의 직접적인 대응 요소는 SAM이다.

NoteBase

문 2. 다음 빈칸 (㉮) 에 들어갈 용어로 가장 적절한 것은?

(㉮)은/는 기존 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하기 위해 기존의 운영체제 내에 추가로 이식되어 사용자의 모든 접근 행위를 안전하게 통제하는 역할을 수행한다. (㉮)의 주요 요구조건은 보안 경계 내의 모든 주체와 객체를 통제할 수 있어야 하고, 프로세스, 파일 시스템, 메모리 관리, 입출력을 위한 자원을 제공해야 한다.

① 접근 제어
② 보안 커널
③ 침입 탐지
④ 사용자 인증

정답 2번

간단한 해설

운영체제 내부에서 주체와 객체 사이의 접근을 빠짐없이 통제하는 구현체는 **보안 커널**이다. 접근 제어라는 기능을 시스템의 핵심 자원 관리 경계에서 실제로 강제한다는 점이 결정적이다.

빈칸별 해설

㉮ 보안 커널: 보안 커널은 참조 모니터의 개념을 실제로 구현하여 **주체가 객체에 접근하는 모든 경로에 보안정책을 적용**하는 핵심 구성요소이다. 주체는 사용자나 프로세스, 객체는 파일·메모리·입출력 자원 등이 될 수 있다. 지문에서 운영체제 내부에 이식되어 각종 자원에 대한 접근을 통제한다는 설명은 단순한 보안 기능의 이름이 아니라 이러한 구현체를 가리킨다.

요구조건과 단서의 연결: 모든 접근을 통제하려면 검사 기능을 우회할 수 없어야 하며, 비인가 변경으로부터 보호되어야 한다. 또한 올바르게 동작하는지 검증할 수 있도록 구조가 명확해야 한다. 지문에 나온 프로세스·파일 시스템·메모리·입출력은 **운영체제의 자원 관리와 접근 통제가 맞닿는 영역**이므로 보안 커널이라는 판단을 뒷받침한다.

다른 용어와의 구별: 접근 제어는 누가 어떤 자원에 어떤 행위를 할 수 있는지 제한하는 기능·정책의 이름이다. 사용자 인증은 사용자의 신원을 확인하는 것이며, 인증되었다고 모든 자원 접근이 허용되는 것은 아니다. 침입 탐지는 공격이나 비정상 행위를 찾아내는 기능으로, 모든 접근을 운영체제 내부에서 강제 통제하는 구현체와는 역할이 다르다.

따라서 두 곳에 반복된 동일한 빈칸 ㉮에는 보안 커널이 들어가며, ②와 대응한다.

NoteBase

문 3. 보안 취약점 공격에 관한 설명으로 가장 적절한 것은?

◯ 취약점에 대해 아직 알려지지 않았을 때 이루어지는 공격이다.
◯ 취약점이 알려졌어도 패치가 발표되지 않은 시점에 이루어지는 공격이다.

① 제로데이(0-day) 공격
② 원데이(1-day) 공격
③ 투데이(2-day) 공격
④ 올데이(Olday) 공격

정답 1번

간단한 해설

정답은 ① **제로데이 공격**이다. 알려지지 않은 취약점 또는 알려졌더라도 **공식 패치가 나오기 전의 취약점**을 악용한다는 공통점이 있다.

구성 요소별 해설

첫 번째 설명은 제작사나 방어자가 아직 알지 못하는 취약점을 공격자가 먼저 악용하는 상황이다. 취약점에 대응할 공식 보안 수정이 준비되기 전에 공격한다는 점에서 **제로데이 공격**에 해당한다.

두 번째 설명은 취약점이 알려졌지만 아직 패치가 발표되지 않은 상황이다. 이 문항에서 중요한 기준은 공개 여부만이 아니라 **공식 패치가 마련되기 전의 취약한 기간을 악용한다는 점**이다. 따라서 두 설명은 모두 ① 제로데이(0-day) 공격으로 연결된다.

원데이(1-day)는 통상 이미 알려진 취약점을 악용하는 맥락에서 쓰이며, 공개된 수정 정보를 이용해 아직 패치를 적용하지 않은 시스템을 노리는 공격과 구별하여 이해한다. 투데이(2-day)와 올데이(Olday)는 제시된 두 설명에 대응하는 표준적인 명칭이 아니다. 숫자를 공격이 하루 또는 이틀 동안 지속된다는 의미로 해석해서는 안 된다.

NoteBase

문 4. 리눅스 특수 권한에 관한 설명 중 가장 적절하지 않은 것은?

① Set-UID가 부여된 파일(file-A)이 실행되는 동안에는 실행시킨 사용자의 권한이 아닌 해당 파일(file-A)의 소유자 권한으로 인식된다.

② Set-GID 권한의 표시는 그룹 허가권에 실행 권한이 없을 경우 대문자 S로 표시된다.

③ Sticky-Bit는 공유를 목적으로 파일에 설정되는 특수 권한으로서 이 권한의 표시는 other 허가권의 실행 권한 자리에 t로 표시된다.

④ 특수 권한 설정은 chmod 명령을 사용하며, 8진수 모드로 Set-UID는 4, Set-GID는 2, Sticky-Bit는 1을 갖는다.

정답 3번

간단한 해설

리눅스에서 Sticky-Bit는 공유 디렉터리에 설정하여 **다른 사용자가 소유한 파일의 삭제·이름 변경을 제한**하는 데 사용한다. 일반 파일에 설정하여 파일 공유를 허용하는 권한이라는 설명은 적절하지 않다.

선지별 해설

리눅스의 특수 권한에는 Set-UID, Set-GID, Sticky-Bit가 있다. 실행 시 적용되는 사용자·그룹 식별자와 공유 디렉터리 안의 삭제 제한은 서로 다른 기능이다.

① O: Set-UID가 정상적으로 적용되는 실행 파일을 실행하면 프로세스의 유효 사용자 ID가 그 파일 소유자의 ID로 설정된다. 따라서 실행자의 실제 사용자 ID와 별개로 **파일 소유자의 유효 권한**을 사용한다. 파일에 비트가 있다는 것만으로 모든 실행 환경에서 반드시 적용된다는 뜻은 아니며, 마운트 설정 등에 따라 무시될 수 있다.

② O: Set-GID는 권한 문자열에서 그룹 실행 권한 위치에 표시한다. 그룹 실행 권한이 함께 있으면 소문자 s이고, 실행 권한은 없으면서 Set-GID만 설정되어 있으면 대문자 S이다.

③ X: Sticky-Bit의 대표적인 용도는 일반 파일의 공유가 아니라 **공유 디렉터리 내부의 삭제·이름 변경 제한**이다. 디렉터리에 쓰기 권한이 있더라도 다른 사람 소유의 항목을 함부로 삭제하지 못하게 하며, 파일 소유자·디렉터리 소유자 또는 적절한 권한을 가진 프로세스 등이 예외가 된다. 표시는 other의 실행 권한 위치에 하며, other 실행 권한이 있으면 t, 없으면 T이다.

④ O: chmod로 특수 권한을 설정할 수 있으며, 일반 권한 세 자리 앞의 특수 권한 자리에 Set-UID는 4, Set-GID는 2, Sticky-Bit는 1을 사용한다. 따라서 전체 모드 비트 값으로는 각각 4000, 2000, 1000에 해당하며 함께 설정할 때는 해당 값을 더한다.

NoteBase

문 5. 다음 중 스니핑(Sniffing)과 관련된 공격으로 가장 적절하지 않은 것은?

① ARP Spoofing

② IP Spoofing

③ Switch Jamming

④ ICMP Redirect

정답 2번

간단한 해설

IP Spoofing의 핵심은 **출발지 IP 주소를 위조**하는 것이다. 주소를 속이는 것만으로 다른 호스트의 패킷이 공격자에게 전달되지는 않으므로, 통신 경로나 스위치 전달 방식을 바꾸는 나머지 기법과 구별된다.

선지별 해설

스니핑은 네트워크를 흐르는 패킷을 관찰·수집하여 통신 내용을 엿보는 것이다. 스위치 환경에서는 다른 장치의 통신이 원래 관찰 지점으로 오지 않을 수 있으므로, 공격자가 트래픽 경로나 전달 방식을 바꾸어 스니핑을 가능하게 하기도 한다.

① O: ARP Spoofing은 IP 주소와 MAC 주소의 대응 정보를 속이는 공격이다. 그 결과 다른 호스트나 게이트웨이로 가야 할 프레임이 공격자 쪽으로 전달되면 공격자가 통신 경로 중간에서 패킷을 관찰할 수 있으므로 스니핑과 관련된다.

② X: IP Spoofing은 **IP 패킷의 출발지 주소를 위조**하여 다른 호스트가 보낸 것처럼 보이게 하는 것이다. 송신자의 신원이나 주소 기반 신뢰를 속이는 것과 달리, 이것만으로 상대방의 통신이 공격자에게 전달되거나 수신 경로가 확보되지는 않는다. 다른 공격과 결합될 수는 있지만 그 자체가 스니핑을 가능하게 하는 대표적 경로 변경 기법은 아니라는 점에서 나머지와 구별된다.

③ O: Switch Jamming은 스위치의 MAC 주소 학습 테이블을 교란하거나 포화시켜 정상적인 목적지 포트 선택을 방해하는 방식이다. 장비의 동작과 보호 설정에 따라 목적지를 알 수 없는 프레임이 여러 포트로 전달되면 공격자가 다른 통신을 관찰할 기회가 생길 수 있다. 모든 스위치가 반드시 허브처럼 동작한다는 뜻은 아니다.

④ O: ICMP Redirect를 악용하면 호스트가 사용하는 다음 홉이나 경로 정보를 잘못 바꾸도록 유도할 수 있다. 호스트가 그러한 변경을 받아들여 통신이 공격자 측 경로를 거치게 되면 스니핑에 이용될 수 있다. 정상적인 경로 안내 메시지 자체와 이를 위조·악용하는 공격을 구별해야 한다.

NoteBase

문 6. TCP에 관한 설명 중 가장 적절하지 않은 것은?

① TCP 연결 설정의 주요 목적은 송수신 호스트간 데이터 전달 시 사용할 초기 순서 번호를 동기화하는 것이다.

② TCP SYN 플러딩(flooding)에 의한 서비스 거부 공격의 취약점이 있다.

③ 데이터가 오류 없이 목적지 호스트에 도착했는지 확인하기 위한 방법 중의 하나로 재전송타이머를 사용할 수 있다.

④ 목적지 호스트에서 TCP 세그먼트(segment)들을 재조합하는 과정의 취약점을 이용하여 Teardrop 공격이 가능하다.

정답 4번

간단한 해설

④가 가장 적절하지 않다. Teardrop은 TCP 세그먼트가 아니라 **IP 단편 재조립**의 취약점을 이용한다. TCP의 연결 설정, SYN 플러딩, ACK·재전송 타이머와 구별해야 한다.

선지별 해설

① (O) TCP는 연결 설정 과정의 3-way handshake를 통해 양쪽의 초기 순서 번호를 교환하고 확인한다. 양방향 바이트 흐름의 시작 번호를 서로 알게 하는 과정이며, 양쪽 호스트가 같은 초기 번호를 사용해야 한다는 뜻은 아니다.

② (O) SYN 플러딩은 연결 설정 요청을 다량 발생시켜 미완성 연결을 처리하는 서버 자원을 소모하게 하는 서비스 거부 공격이다. TCP 연결 설정 과정의 상태 유지 특성을 악용하므로, 이를 완화하는 별도의 방어가 필요하다.

③ (O) 송신 측은 보낸 데이터에 대한 확인 응답(ACK)을 기다리며 재전송 타이머를 관리한다. 제한 시간 내에 필요한 ACK를 받지 못하면 재전송하여 신뢰성 있는 전달을 지원한다. 타이머가 데이터 오류를 직접 검사하는 것은 아니며, 오류 검출에는 체크섬이 사용되고 수신 확인에는 ACK가 사용된다.

④ (X) Teardrop은 **IP 단편의 재조립 과정**에서 겹치거나 비정상적인 단편을 적절히 처리하지 못하는 취약점을 이용하는 공격이다. TCP 세그먼트의 순서 정렬·재조합을 이용하는 공격이 아니므로, IP 계층과 TCP 계층을 혼동한 설명이다.

NoteBase

문 7. 리눅스/유닉스의 주요 로그 파일 <보기 1>과 설명 <보기 2>를 가장 적절하게 연결한 것은?

<보기 1>
㉮ utmp(x) ㉯ wtmp(x)
㉰ loginlog ㉱ pacct

<보기 2>
㉠ 실패한 로그인 시도에 대한 정보를 저장하는 로그로서 기본으로 제공하지 않는다.
㉡ 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보를 저장하는 로그이다.
㉢ 사용자의 로그인, 로그아웃, 시스템 재부팅 정보를 저장하는 로그이다.
㉣ 현재 시스템에 로그인한 사용자 상태를 저장하는 로그이다.

① ㉮: ㉢, ㉯: ㉣, ㉰: ㉡, ㉱: ㉠
② ㉮: ㉢, ㉯: ㉠, ㉰: ㉣, ㉱: ㉡
③ ㉮: ㉣, ㉯: ㉡, ㉰: ㉢, ㉱: ㉠
④ ㉮: ㉣, ㉯: ㉢, ㉰: ㉠, ㉱: ㉡

정답 4번

간단한 해설

utmp(x)는 **현재 로그인 상태**를, wtmp(x)는 **로그인·로그아웃·재부팅 이력**을 저장한다. 접속 상태나 이력을 기록하는 로그와 사용자가 실행한 프로그램을 기록하는 프로세스 어카운팅 로그를 구분해야 한다.

NoteBase

대응 관계 해설

㉮ utmp(x) → ㉣: **현재 로그인한 사용자 상태**를 기록한다. 사용자가 접속하거나 종료하면 해당 상태가 갱신되므로, 과거의 접속 이력을 누적하는 wtmp(x)와 구별된다.

㉯ wtmp(x) → ㉢: 사용자의 **로그인·로그아웃과 시스템 재부팅 이력**을 기록한다. 지금 누가 접속해 있는지보다 언제 접속하고 종료했는지를 확인하는 기록이다.

㉰ loginlog → ㉠: **실패한 로그인 시도**를 기록한다. Solaris의 loginlog는 기본적으로 파일이 존재하지 않아 기록하지 않으며, 관리자가 파일을 생성하여 기록을 활성화한다. 보기의 '기본으로 제공하지 않는다'는 이러한 파일 생성 방식을 가리킨다.

㉱ → ㉡: 프로세스 어카운팅 로그는 **사용자가 실행한 프로그램 정보**를 기록한다. 어카운팅이 활성화되면 실행된 명령과 실행 사용자, CPU 사용 시간 등의 정보를 남긴다. 로그인 여부나 접속 이력만을 기록하는 로그와 달리, 시스템에서 어떤 프로그램이 실행되었는지를 확인하는 데 쓰인다.

따라서 ㉮–㉣, ㉯–㉢, ㉰–㉠, ㉱–㉡으로 연결되며, 이는 ④의 조합과 일치한다.

NoteBase

문 8. 스택 가드에서 CR(0x0d), LF(0x0a), EOF(0xff) 등을 조합해서 canary 값을 만드는 기술로 가장 적절한 것은?

① Null canary

② Return canary

③ Random canary

④ Terminator canary

정답 4번

간단한 해설

정답은 ④ **Terminator canary**이다. CR, LF 등 **입력·문자열 처리의 종료와 관련된 값들을 조합**한다는 것이 핵심 단서이다.

개념 구분

스택 가드는 보호할 스택 영역에 canary 값을 두고, 함수가 반환하기 전에 그 값이 변조되었는지 검사하는 방식으로 스택 훼손을 탐지한다. 이때 **문자열·입력 처리의 종료와 관련된 값들을 조합**하는 방식이 Terminator canary이므로 정답은 ④이다.

전통적인 설명에서는 널 바이트, CR, LF, EOF에 대응하는 값 등을 조합한다. 문자열이나 줄 입력을 처리하는 일부 함수가 특정 종료 조건에서 처리를 멈춘다는 특성을 활용한 것이다. 다만 모든 함수가 이 값들을 모두 동일하게 처리하는 것은 아니며, 문제의 EOF(0xff) 표기를 C 언어의 EOF가 언제나 문자 바이트 0xff라는 뜻으로 일반화해서는 안 된다.

Null canary는 널 값에 초점을 둔 표현이고, Random canary는 예측하기 어려운 난수값을 사용하는 방식이다. 문제처럼 여러 종료 관련 값을 조합한다는 단서는 이들과 구별된다. Return canary는 이 조합 방식을 가리키는 명칭이 아니며, 반환주소를 보호한다는 목적만 보고 선택해서는 안 된다.

NoteBase

문 9. 포트 포워딩(port forwarding)에 관한 설명 중 가장 적절한 것은?

① 일반적인 TCP 연결을 보안상 안전한 SSH(버전2) 연결로 변환하는 서비스

② 보안상 Well-known 포트 번호를 임시 포트 번호로 전환하는 절차

③ 한 포트에서 다른 포트로 메시지를 전달하는 데 사용되는 프로토콜

④ 공격 대상 호스트에서 서비스가 활성화되어 있는 포트를 찾아 연결하는 것

정답 1번

간단한 해설

①은 **SSH 포트 포워딩**을 설명한다. 일반 TCP 통신을 SSH의 암호화된 터널로 전달하는 기능이며, 단순한 포트 번호 변경이나 열린 포트 탐색과 다르다.

개념 구분

SSH 포트 포워딩의 의미: 한쪽의 지정된 포트로 들어온 TCP 연결의 데이터를 **SSH의 암호화된 통신 채널을 통해** 반대쪽으로 전달하고, 거기서 목적지 서비스로 연결하는 기능이다. 응용프로그램 자체가 암호화를 지원하지 않아도 SSH 터널 구간에서는 데이터를 보호할 수 있다. ①의 '안전한 SSH 연결로 변환'은 원래 응용프로토콜을 없애는 것이 아니라 그 통신을 SSH 터널로 운반한다는 뜻이다.

다른 선택지와의 구별: ②처럼 잘 알려진 포트 번호를 임시 포트로 바꾸는 것 자체가 정의는 아니며, 번호 변경만으로 암호화가 이루어지지도 않는다.

③의 전달 기능이라는 취지는 일부 닿아 있지만, 포트 포워딩은 그 자체가 독립된 프로토콜의 이름은 아니다.

④는 서비스가 열려 있는 포트를 찾아내는 포트 스캐닝에 관한 설명으로, 연결을 중계하는 기능과 다르다.

용어의 범위: 일반적으로 포트 포워딩에는 라우터의 주소·포트 변환처럼 SSH를 사용하지 않는 방식도 포함된다. 따라서 **모든 포트 포워딩이 암호화를 제공하는 것은 아니다**. 또한 SSH 방식에서도 암호화는 SSH 종단 사이에 적용되므로, 터널 밖의 연결까지 자동으로 보호된다고 단정할 수 없다.

이 문항의 선택지 중 SSH를 이용해 일반 TCP 통신을 안전한 채널로 전달하는 기능을 설명한 것은 ①이므로 가장 적절하다.

NoteBase

문 10. HTTP 요청 메소드에 대한 설명 중 가장 적절하지 않은 것은?

① GET : 서버가 자원을 전송해 줄 것을 요청

② PUT : 클라이언트가 서버의 URI로 자원을 전송

③ TRACE : 클라이언트와 서버간에 터널링 목적으로 사용

④ OPTIONS : 자원에 관련된 선택 사항의 정보를 요청할 때 사용

정답 3번

간단한 해설

터널을 설정하는 HTTP 메서드는 **CONNECT**이다. TRACE는 수신한 요청을 되돌려 받아 요청 전달 경로 등을 진단하는 루프백 용도이며, 터널링과 다르다.

선지별 해설

HTTP 요청 메서드는 대상 자원에 대해 클라이언트가 어떤 처리를 요구하는지를 나타낸다. 자원 조회·생성 또는 대체·진단·통신 옵션 조회의 목적을 구별한다.

① O: GET은 대상 자원의 현재 표현을 전송해 달라고 요청한다. 웹 페이지나 파일 등의 내용을 조회하는 데 사용하는 메서드이다.

② O: PUT은 요청에 담은 표현으로 지정한 URI의 대상 자원 상태를 생성하거나 대체하도록 요청한다. 단순히 데이터를 서버로 보낸다는 공통점만으로 POST와 같다고 볼 수 없으며, **지정한 대상 자원을 생성·대체**한다는 의미가 중요하다.

③ X: TRACE는 요청 메시지의 응용 계층 루프백을 요청하여 최종 수신자가 받은 요청을 확인하는 진단용 메서드이다. **터널 설정은 CONNECT**의 역할이며, 대표적으로 HTTP 프록시를 통해 목적지와 터널을 연결할 때 사용한다.

④ O: OPTIONS는 대상 자원에 사용할 수 있는 통신 옵션 등의 정보를 요청한다. 서버가 제공하는 메서드 관련 정보 등 상호작용에 필요한 기능을 확인하는 데 쓰며, 자원의 본문을 가져오는 GET과 구별된다.

NoteBase

문 11. 다음 중 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

㉮ 인터넷의 라우터 보안을 위해 정적 라우팅(static routing)은 필수적으로 사용되어야 한다.
㉯ S/MIME은 X.509에 정의된 인증기관에 의해 서명된 공개키 인증서를 사용한다.
㉰ RTP(Real-time Transport Protocol)를 이용하여 VPN을 제공할 수 있다.
㉱ SSO(Single Sign On)는 효율적인 인증관리를 가능하게 한다.
㉲ LAN 카드의 ‘promiscuous’ 모드 설정은 패킷 필터링 기능을 해제하는 것이다.

① ㉮, ㉱, ㉲
② ㉯, ㉰, ㉱
③ ㉯, ㉱, ㉲
④ ㉮, ㉯, ㉰, ㉱

정답 3번

간단한 해설

정답은 ③ ㉯·㉱·㉲이다. S/MIME의 X.509 인증서, SSO의 인증 관리 효율화, promiscuous 모드의 수신 필터링 해제 설명은 옳다. **정적 라우팅은 필수가 아니며** RTP는 VPN용 프로토콜이 아니다.

NoteBase

보기별 해설

㉮ (X) 라우터 보안을 위해 **정적 라우팅을 반드시 사용해야 하는 것은 아니다**. 정적 경로는 관리자가 직접 설정하지만, 동적 라우팅에서도 지원되는 인증과 경로 필터링 등의 통제를 적용할 수 있다. 망의 규모와 운영 요구에 맞게 라우팅 방식을 선택하므로 '필수적으로'라는 단정이 틀리다.

㉯ (O) S/MIME은 전자우편의 암호화와 전자서명을 지원하며, 공개키와 소유자의 신원을 연결하기 위해 X.509 형식의 공개키 인증서를 사용한다. 인증기관의 서명을 검증하여 인증서에 대한 신뢰를 확인할 수 있다.

㉰ (X) RTP는 음성·영상과 같은 실시간 데이터를 전달하기 위한 프로토콜이다. 순서 번호와 타임스탬프 등을 제공하지만, 그 자체가 VPN을 구성하는 보안 터널 프로토콜은 아니다. VPN은 IPsec이나 TLS 기반 기술 등으로 구현할 수 있다.

㉱ (O) SSO는 한 번의 인증 결과를 활용하여 연계된 여러 서비스에 접근하도록 하여 반복 로그인을 줄이고 인증 관리를 효율화한다. 다만 인증 기능이 집중되므로 계정과 인증 기반의 보호는 여전히 중요하다.

㉲ (O) 무차별 모드인 promiscuous 모드는 네트워크 인터페이스가 자신의 MAC 주소 등을 기준으로 수신 프레임을 걸러내는 통상적인 필터링을 완화하여, 인터페이스에 도착한 다른 목적지의 프레임도 상위 계층에 전달하게 한다. 방화벽의 모든 필터를 끄거나 스위치에 흐르는 모든 트래픽을 자동으로 수신하게 한다는 뜻은 아니다.

따라서 옳은 설명은 ㉯·㉱·㉲이며 정답은 ③이다.

NoteBase

문 12. 레이스 컨디션 공격에 필요한 조건을 모두 고른 것으로 가장 적절한 것은?

㉮ 공격 대상 프로그램의 소유자는 root이어야 한다.
㉯ 공격 대상 프로그램은 Set-UID가 설정되어 있어야 한다.
㉰ 생성되는 임시 파일의 이름을 알고 있어야 한다.

① ㉮, ㉯
② ㉮, ㉰
③ ㉯, ㉰
④ ㉮, ㉯, ㉰

정답 4번

간단한 해설

root 소유 프로그램에 **Set-UID가 적용되면 소유자인 root의 권한**으로 실행된다. 임시 파일을 이용하는 전형적인 공격에서는 파일 이름을 알아내어, 프로그램의 **검사와 사용 사이**에 그 이름이 가리키는 대상을 바꾸는 방식으로 높은 권한을 악용한다.

NoteBase

보기별 해설

레이스 컨디션 공격은 공유 자원에 접근하는 작업의 실행 순서나 시점 차이를 악용한다. 보기의 root·Set-UID·임시 파일 조건은 일반 사용자가 높은 권한의 프로그램을 속여 보호된 파일에 접근하게 하는 전형적인 파일 기반 공격을 기준으로 해석한다. 이 세 조건이 모든 종류의 레이스 컨디션 공격에 공통으로 필요한 것은 아니다.

㉮ O: root 권한을 악용하는 이 전형적 상황에서는 공격 대상 실행파일의 소유자가 root이다. Set-UID는 실행파일 소유자의 권한으로 실행하게 하는 기능이므로, **소유자가 root**여야 이 방식으로 root 권한을 이용할 수 있다. 소유자가 root라는 사실만으로 일반 사용자가 실행한 프로세스가 root 권한을 얻는 것은 아니다.

㉯ O: 일반 사용자가 실행해도 프로그램 소유자의 권한을 이용하도록 하는 조건이다. **Set-UID가 적용되면 유효 사용자 ID가 실행파일 소유자의 ID로 설정**되므로, root 소유 프로그램은 root 권한으로 파일에 접근할 수 있다. 공격자는 프로그램의 파일 처리 취약점을 이용해 자신에게 없는 권한으로 작업이 수행되게 한다.

㉰ O: 임시 파일을 다른 대상으로 바꾸는 공격에서는 **프로그램이 사용할 임시 파일의 이름**을 알거나 예측할 수 있어야 한다. 예를 들어, 파일 존재 여부나 접근 권한을 검사한 뒤 실제로 열기 전에 같은 이름의 심볼릭 링크가 다른 파일을 가리키게 하면, 취약한 프로그램이 의도하지 않은 파일을 열 수 있다. 이를 위해서는 공격자가 해당 경로를 조작할 수 있고 검사와 사용 사이에 개입할 수 있어야 한다.

이처럼 root 권한으로 실행되는 프로그램과 예측 가능한 임시 파일을 이용하는 전형적 공격 상황에서는 ㉮·㉯·㉰을 함께 고른 ④에 대응한다.

NoteBase

문 13. 다음에 출력된 리눅스의 /etc/shadow 파일에 관한 설명 중 가장 적절하지 않은 것은?

```
[root@localhost ~]# tail -1 /etc/shadow

tester:$6 $1Tkc0bAR $GFtu6중략HF9tyE:16570:30:99999:7:::
       ㉮    ㉯              ㉰          ㉱
```

① ㉮: 사용자 패스워드 암호화에 사용된 MD5 해시 알고리즘을 나타낸다.

② ㉯: 해시 값을 생성할 때 사용된 솔트를 나타낸다.

③ ㉰: 사용자 패스워드에 솔트를 조합하여 해시한 암호화된 패스워드를 나타낸다.

④ ㉱: 패스워드를 바꾼 후 최소로 사용해야 되는 날짜 수를 나타낸다.

정답 1번

간단한 해설

정답은 ①이다. ㉮의 식별자 **6은 SHA-512 기반 방식**이며, MD5 기반 방식의 식별자는 1이다. ㉯는 솔트, ㉰는 해시 결과, ㉱는 최소 비밀번호 사용기간이다.

선지별 해설

① (X) ㉮의 알고리즘 식별자 6은 **SHA-512 기반의 비밀번호 해시 방식**을 나타낸다. MD5 기반 방식의 식별자는 1이므로, 이를 MD5라고 설명한 선지가 틀렸다. 알고리즘 식별자와 해시값 자체를 구별해야 한다.

② (O) ㉯는 비밀번호 해시 계산에 함께 사용한 **솔트(salt)**이다. 같은 비밀번호라도 솔트가 다르면 저장되는 해시 결과가 달라지도록 하여, 미리 계산한 해시 목록을 재사용하기 어렵게 한다. 솔트는 비밀번호 자체나 비밀 암호키가 아니다.

③ (O) ㉰는 비밀번호와 솔트 등을 입력으로 지정된 방식에 따라 계산한 해시 결과 부분이다. 선지에서는 암호화된 패스워드라고 표현했지만, 여기서는 **복호화로 원문을 되찾는 암호문이 아니라 비밀번호 검증용 해시**라는 점이 중요하다.

④ (O) ㉱의 30은 비밀번호를 변경한 뒤 다시 변경하기까지 기다려야 하는 최소 일수이다. /etc/shadow에서 마지막 변경일 다음의 최소 사용기간 필드에 해당한다. 그 뒤의 99999는 최대 사용기간, 7은 만료 전 경고기간이므로 서로 구별한다.

NoteBase

문 14. 스텔스 스캔 방법으로 가장 적절한 것을 모두 고른 것은?

㉮ TCP Open 스캔
㉯ NULL 스캔
㉰ XMAS 스캔
㉱ UDP 스캔

① ㉮, ㉯
② ㉮, ㉰
③ ㉯, ㉰
④ ㉯, ㉱

정답 3번

간단한 해설

NULL과 XMAS 스캔은 **정상적인 TCP 연결을 완성하지 않고** 플래그 설정에 따른 응답 차이를 이용한다. TCP Open 스캔은 연결을 완료하며, UDP 스캔은 UDP 포트를 조사하는 별도 방식이다.

NoteBase

보기별 해설

이 문항의 스텔스 스캔은 정상적인 TCP 연결을 완성하지 않고 비정상적인 플래그 조합 등의 응답 차이로 포트 상태를 추정하는 전형적인 기법을 뜻한다. 스텔스라는 이름이 로그나 탐지에 전혀 나타나지 않음을 보장하지는 않는다.

㉮ X: TCP Open 스캔은 3-way handshake를 완료하여 정상적인 TCP 연결을 성립시키는 방식이다. 연결 사실이 서비스에 드러나므로 이 문항의 스텔스 스캔에 해당하지 않는다.

㉯ O: NULL 스캔은 **TCP 제어 플래그를 설정하지 않은** 세그먼트에 대한 응답을 이용한다. 정상적인 연결을 완료하지 않는 전형적인 스텔스 스캔으로 분류한다.

㉰ O: XMAS 스캔은 **FIN·PSH·URG 플래그**를 함께 설정한 세그먼트를 이용한다. NULL 스캔과 마찬가지로 정상 연결을 완료하지 않고 응답 차이를 관찰한다. 다만 운영체제와 필터링 상태에 따라 결과가 달라지며 탐지될 수도 있다.

㉱ X: UDP 스캔은 UDP 응답이나 ICMP 오류 등을 이용하여 UDP 포트 상태를 조사하는 방식이다. UDP가 비연결형이라는 사실만으로 이 문항에서 묻는 TCP 플래그 기반 스텔스 스캔으로 분류하지 않는다.

따라서 해당하는 보기는 ㉯와 ㉰이며, 이를 고른 ③이 적절하다.

NoteBase

문 15. APT(Advanced Persistent Threat) 공격 단계를 예를 들어 나열한 것으로 가장 적절한 것은?

① 침입(사회공학)-운영방해(권한상승)-유출(지속적인 분석)-기밀데이터 검색(은밀한 활동)
② 침입(사회공학)-기밀데이터 검색(은밀한 활동)-운영방해(권한상승)-유출(지속적인 분석)
③ 기밀데이터 검색(은밀한 활동)-침입(사회공학)-운영방해(권한상승)-유출(지속적인 분석)
④ 기밀데이터 검색(은밀한 활동)-유출(지속적인 분석)-침입(사회공학)-운영방해(권한상승)

정답 2번

간단한 해설

제시된 예에서는 **내부 침입이 기밀데이터 검색의 전제**이고, 목표 정보의 확보가 유출보다 앞선다. 내부 검색과 통제 범위 확대를 거쳐 자료를 외부로 반출한다는 관계로 순서를 판단한다.

올바른 순서

침입(사회공학) → 기밀데이터 검색(은밀한 활동) → 운영방해(권한상승) → 유출(지속적인 분석)

침입(사회공학): 사람의 신뢰나 판단을 악용하는 사회공학적 수단 등으로 대상 조직 내부에 최초 접근점을 만드는 단계이다. 이 문항의 기밀데이터 검색은 내부에 들어간 뒤의 활동이므로 **내부 검색보다 침입이 먼저** 놓인다.

기밀데이터 검색(은밀한 활동): 침입 후 내부 환경을 살피며 목표가 되는 정보의 위치와 접근 조건을 파악하는 단계이다. 외부에서 수행하는 사전 정보수집과 달리, 여기서는 이미 확보한 내부 접근을 바탕으로 기밀데이터를 찾는 활동을 뜻한다.

운영방해(권한상승): 제시된 예에서는 목표 자료를 확인한 뒤 더 높은 접근권한을 확보하여 내부 자원에 대한 통제 범위를 넓히는 활동을 배치하였다. 권한상승은 **허용된 권한보다 높은 권한을 획득**하는 것이며, 그 자체가 반드시 서비스 중단을 뜻하는 것은 아니다. 실제 APT에서는 내부 탐색과 권한상승 등이 반복되거나 순서가 달라질 수 있으므로, 이 나열을 모든 공격의 고정 절차로 일반화하지 않는다.

유출(지속적인 분석): 확보한 기밀정보를 조직의 통제 범위 밖으로 반출하는 단계이다. 목표 정보를 먼저 찾아 접근·확보해야 유출할 수 있으므로, 제시된 예에서는 마지막에 놓인다. 괄호의 지속적인 분석은 장기적 공격 과정에서 대상과 정보를 계속 살핀다는 맥락이며, 유출 자체의 핵심은 **정보의 무단 외부 반출**이다.

NoteBase

문 17. 윈도우 NTFS의 디렉터리 및 파일 접근 권한 설정 규칙을 모두 고른 것으로 가장 적절한 것은?

㉮ NTFS 접근 권한은 누적되지 않는다.
㉯ 파일 접근 권한이 디렉터리 접근 권한에 우선한다.
㉰ 거부가 허용보다 우선한다.

① ㉮, ㉯
② ㉮, ㉰
③ ㉯, ㉰
④ ㉮, ㉯, ㉰

정답 3번

간단한 해설

정답은 ③ ㉯·㉰이다. NTFS의 허용 권한은 누적되므로 ㉮이 틀리다. 파일의 명시적 권한과 디렉터리에서 상속된 권한의 관계, 동일 우선순위에서의 거부 우선 규칙을 함께 구별해야 한다.

보기별 해설

㉮ (X) NTFS의 허용 권한은 누적된다. 예를 들어 사용자에게 읽기가 허용되고 소속 그룹에 쓰기가 허용되어 있다면, 다른 제한이 없는 경우 두 권한을 함께 가진다. 다만 거부 항목과 상속 관계 등도 최종 접근 판단에 반영되므로 허용 권한만 합산해 판단해서는 안 된다.

㉯ (O) 파일에 직접 설정한 접근 권한을 해당 파일의 접근 판단에 적용한다는 기본 규칙을 설명한 것이다. 특히 파일에 명시적으로 설정한 권한은 부모 디렉터리에서 상속된 권한보다 먼저 평가된다. 파일 권한과 디렉터리 권한이 언제나 별개라는 뜻이나, 파일 권한이 모든 경로 접근 제한을 무조건 없앤다는 뜻은 아니다.

㉰ (O) 같은 명시성·상속 우선순위에서 동일한 접근 권한에 허용과 거부가 충돌하면, 표준적인 접근 제어 항목 순서에서는 거부가 먼저 평가된다. 다만 **명시적 권한은 상속 권한보다 우선**하므로, 명시적 허용이 상속된 거부보다 먼저 적용될 수 있다. 따라서 이 규칙을 '모든 거부가 모든 허용에 무조건 우선한다'고 확대해서는 안 된다.

문항에서 제시한 기본 권한 규칙에 해당하는 것은 ㉯·㉰이므로 정답은 ③이다. ㉮은 '누적되지 않는다'를 '누적된다'로 고쳐야 한다.

NoteBase

문 18. 다음 설명에 관한 기술로 가장 적절한 것은?

◯ 버퍼 오버플로가 일어날 가능성이 있는지, 암호화 알고리즘에 취약점이 없는지 등을 분석할 수 있다.
◯ 소프트웨어에 버그가 발생했을 때 원인을 파악하기 위해 사용할 수 있다.
◯ 불법적인 사용자가 소프트웨어 사용 제한 기능 등을 제거하기 위해 사용할 수 있다.
◯ 공격자가 배포한 악성코드의 원리를 분석하고 대응 방안을 만들기 위해 사용할 수 있다.

① 샌드박스(Sand Box)
② 16진수 편집기
③ 리버스 쉘(Reverse Shell)
④ 리버스 엔지니어링(Reverse Engineering)

정답 4번

간단한 해설

기존 소프트웨어의 내부 구조와 동작 원리를 분석하는 기술은 리버스 엔지니어링이다. 취약점·버그·악성코드를 이해하는 데 활용되며, 사용 제한을 우회하려는 목적으로 악용될 수도 있다.

NoteBase

대응 관계 해설

리버스 엔지니어링은 이미 만들어진 소프트웨어의 코드·구조·실행 동작을 분석하여 내부 원리와 설계를 알아내는 역공학이다. 지문의 네 용도는 모두 **완성된 프로그램에서 내부 동작을 거슬러 파악**한다는 공통점을 가진다.

취약점 분석: 프로그램의 데이터 처리와 제어 흐름을 살펴 메모리 접근의 문제나 암호화 처리상의 약점을 조사할 수 있다. 다만 분석을 수행했다는 사실만으로 취약점의 존재 또는 부재가 자동으로 증명되는 것은 아니다.

버그 원인 파악: 예상과 다른 결과가 나오는 지점과 실행 흐름, 관련 데이터의 변화를 조사하여 오류의 원인을 추적한다. 특히 원래 설계 정보나 소스가 충분하지 않은 상황에서 구현으로부터 동작을 이해하는 데 도움이 된다.

사용 제한 기능 제거의 악용: 사용 제한을 판단하는 내부 동작을 이해하는 데 역공학이 악용될 수 있다는 설명이다. 역공학이라는 분석 기법 자체와 권한 없이 제한 기능을 제거하는 행위는 구별해야 하며, 이 지문은 해당 기법의 오용 가능성을 말한다.

악성코드 분석과 대응: 악성코드의 기능과 작동 조건, 외부와의 상호작용 등을 분석하여 탐지·차단·복구에 필요한 근거를 얻을 수 있다. 내부 원리를 파악한다는 점에서 역공학의 방어적 활용에 해당한다.

따라서 네 설명 전체에 대응하는 기술은 ④ 리버스 엔지니어링이다. 샌드박스는 프로그램을 격리하여 실행·관찰하는 환경이고, 16진수 편집기는 파일의 바이트를 확인·수정하는 도구이다. 둘은 분석에 활용될 수 있지만 지문 전체를 포괄하는 분석 기법의 명칭은 아니다. 리버스 쉘은 대상 시스템이 외부로 연결하여 명령 실행 통로를 형성하는 방식으로, 내부 구조를 분석하는 역공학과 다르다.

NoteBase

문 19. 다음 보안 공격들의 공통점으로 가장 적절한 것은?

SYN Flooding, Smurf, Land

① ICMP 패킷을 이용한다.
② TCP 프로토콜의 취약점을 이용한다.
③ 발신지 IP 주소를 위조한다.
④ IP 데이터그램 단편화를 이용한다.

정답 3번

간단한 해설

제시된 공격의 전형적인 형태는 **발신지 IP 주소 위조**를 이용한다. Smurf는 피해자 주소로 응답이 향하게 하고, Land는 출발지와 목적지를 피해자 자신으로 맞추며, 전통적인 SYN Flooding은 위조 주소를 이용해 연결 대기 자원을 소모시킨다.

선지별 해설

세 공격은 서비스 거부를 유발하는 방식이지만 사용하는 프로토콜과 세부 원리는 다르다. 이 문항에서는 전형적인 SYN Flooding, Smurf, Land 공격에 공통으로 활용되는 기법을 찾는다.

① X: ICMP를 이용하는 것은 Smurf의 특징이다. Smurf는 피해자의 주소를 발신지로 위조한 ICMP Echo Request에 대한 응답이 피해자에게 집중되도록 한다. SYN Flooding과 Land의 전형적인 형태는 TCP를 이용하므로 ICMP가 세 공격의 공통점은 아니다.

② X: SYN Flooding은 TCP의 연결 설정 과정에서 미완료 연결이 차지하는 자원을 소모시키며, Land는 출발지와 목적지가 같은 TCP 패킷을 처리하는 취약한 구현을 악용한다. 그러나 Smurf는 ICMP의 반사·증폭을 이용하므로 TCP 취약점 이용으로 세 공격을 모두 설명할 수 없다.

③ O: **전형적인 형태에서 발신지 IP 주소를 위조**한다. SYN Flooding은 위조한 출발지 주소로 미완료 연결을 누적시키고, Smurf는 피해자 주소로 응답을 유도하며, Land는 출발지 IP와 목적지 IP를 피해자 주소로 일치시킨다. 다만 실제 SYN Flooding은 위조하지 않은 주소를 가진 다수의 호스트로도 가능하므로, IP 위조가 모든 SYN Flooding의 필수조건이라는 뜻은 아니다.

④ X: 세 공격의 공통 원리는 IP 단편화가 아니다. 단편의 중첩이나 비정상적인 재조립 처리를 악용하는 공격과 구별해야 하며, 제시된 세 공격은 각각 연결 대기 자원 소모, 반사·증폭, 동일한 출발지·목적지 처리 문제를 이용한다.

NoteBase

문 20. 무선 네트워크 보안 취약점에 관한 설명에 부합하는 위협으로 가장 적절한 것은?

◯ 공격자가 무선 네트워크를 식별하기 위한 SSID를 모니터링하여 접속한다.
◯ 공격자가 인증절차가 없는 취약한 AP를 찾아 접속한다.
◯ MAC 필터링 기반 인증방법을 사용하는 환경에서 정상 사용자와 AP와의 통신 간 정보를 공격자가 수집하여 무선 네트워크에 접속한다.

① 도청
② DDoS
③ 불법 AP
④ 비인가 접근

정답 4번

간단한 해설

정답은 ④ **비인가 접근**이다. 세 사례 모두 무선 네트워크의 식별정보나 인증 취약점을 이용하여 **권한 없이 접속**한다는 공통점이 있다.

구성 요소별 해설

첫 번째 설명은 SSID를 알아내 네트워크를 식별한 뒤 권한 없이 접속하는 경우이다. SSID는 네트워크의 식별자이지 비밀 인증수단이 아니므로, 이를 안다는 사실이 정당한 접근 권한을 뜻하지 않는다. 다만 SSID만 알면 모든 보호된 네트워크에 접속할 수 있다는 의미는 아니다.

두 번째 설명은 인증절차가 없는 취약한 AP를 통해 승인받지 않은 사용자가 접속하는 경우이다. 핵심은 **접근통제가 부재하여 비인가자가 네트워크에 들어오는 것**이다.

세 번째 설명은 정상 통신에서 얻은 정보를 이용하여 MAC 주소 기반 접근통제의 약점을 악용하는 경우이다. MAC 필터링만으로는 강한 사용자 인증을 제공하기 어렵다는 점과 연결되며, 결과적으로 **비인가 접근**에 해당한다.

세 설명은 모두 네트워크에 권한 없이 접속한다는 공통점이 있으므로 정답은 ④이다. 도청은 통신 내용을 몰래 수집하는 행위로 일부 과정에 포함될 수 있으나 접속까지 설명하는 공통 위협은 아니다. DDoS는 다수의 공격원으로 서비스를 방해하는 것이고, 불법 AP는 승인되지 않은 AP의 설치·운영에 관한 위협으로 제시문과 구별된다.

NoteBase

문 21. 발신지 호스트(source host)에서 다른 네트워크의 목적지 호스트(destination host)로 패킷이 전달되는 과정에서 패킷 내의 각종 주소의 변화에 관한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

㉮ 2계층 스위치를 통해 전달될 때 발신지 MAC 주소와 목적지 MAC 주소는 모두 변경된다.
㉯ 라우터를 통해 전달될 때 발신지 물리주소와 목적지 물리주소는 모두 변경된다.
㉰ 라우터를 통해 전달될 때 발신지 IP 주소와 목적지 IP 주소는 그대로 유지된다.
㉱ 라우터를 통해 전달될 때 발신지 포트 주소와 목적지 포트 주소는 그대로 유지된다.

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

정답 3번

간단한 해설

정답은 ③ ㉯·㉰·㉱이다. 2계층 스위치는 MAC 주소를 유지하지만, 라우터는 다음 링크로 전달할 때 새 프레임의 MAC 주소를 설정한다. NAT 등의 변환이 없는 일반적인 라우팅에서는 **IP 주소와 포트 번호는 유지**된다.

NoteBase

보기별 해설

㉮ (X) 일반적인 2계층 스위치는 프레임의 목적지 MAC 주소를 참조하여 전달 포트를 결정한다. 프레임을 전달하면서 발신지와 목적지 MAC 주소를 자신의 주소 등으로 바꾸지 않으므로 두 주소가 모두 변경된다는 설명은 틀리다.

㉯ (O) 라우터는 들어온 링크의 프레임을 벗기고 IP 패킷을 다음 링크에 맞는 새 프레임으로 캡슐화한다. 이더넷에서는 새 프레임의 발신지 MAC 주소가 라우터의 송신 인터페이스 주소가 되고, 목적지 MAC 주소는 다음 홉 장치의 주소가 된다. 따라서 링크를 넘을 때 두 물리주소가 바뀐다.

㉰ (O) 일반적인 라우팅에서는 원래 발신지와 최종 목적지를 나타내는 IP 주소가 종단 간 유지된다. 라우터가 TTL 등의 필드를 변경하더라도 발신지·목적지 IP 주소를 바꾸는 것은 아니다. 다만 NAT와 같은 주소 변환을 수행하는 경우는 예외이다.

㉱ (O) 포트 번호는 종단 호스트의 통신 프로세스를 식별하는 전송 계층 정보이므로 일반 라우터가 패킷을 중계할 때 그대로 유지된다. 포트까지 변환하는 NAPT 등의 기능이 별도로 사용되는 경우와 구별해야 한다.

따라서 일반적인 라우팅을 전제로 옳은 설명은 ㉯·㉰·㉱이며, 이를 ㉯·㉰·㉱로 표시한 ③이 정답이다.

NoteBase

문 22. 공급망 공격(Supply Chain Attack)에 대한 설명으로 가장 적절한 것은?

① 거래처 등에 위장 E-mail을 전송하여 공격자 계좌로 금전 입금을 유도한다.

② E-mail을 통해 배포된 워드 파일에 심은 매크로로 감염시킨다.

③ 침입한 컴퓨터의 공식도구나 윈도우 표준 명령어로 공격한다.

④ 패치를 배포하는 서버에 침입하여 정식 패치 등에 맬웨어(Malware)를 심는다.

정답 4번

간단한 해설

공급망 공격은 **신뢰하는 공급업체와 정상 배포 경로**를 악용한다. 패치 배포 체계를 침해하여 정식 업데이트에 악성코드를 섞으면 이를 받는 이용자에게 피해가 확산될 수 있다.

선지별 해설

① X: 거래처나 관계자를 사칭한 이메일로 공격자 계좌에 송금하도록 속이는 것은 **업무 이메일 사기(BEC)**의 전형적인 모습이다. 공급업체의 제품 제작·배포 경로를 변조하여 이용자에게 피해를 확산하는 공급망 공격과는 핵심 수단이 다르다.

② X: 이메일 첨부 문서의 악성 매크로를 통해 감염시키는 것은 **악성 문서·매크로를 이용한 공격**이다. 이 설명만으로는 소프트웨어 공급자의 개발·업데이트 경로가 침해되었다고 볼 수 없으므로 공급망 공격의 특징을 직접 설명한 것이 아니다.

③ X: 시스템에 원래 존재하는 관리 도구나 표준 명령어를 악용하는 것은 **정상 도구 악용, 즉 Living off the Land** 기법이다. 별도 악성 도구 대신 정상 기능을 사용한다는 점이 특징이며, 공급망의 신뢰 관계와 배포 경로를 침해한다는 의미와 구별된다.

④ O: 공급망 공격은 이용자가 신뢰하는 공급업체의 제품·서비스·배포 경로 등을 먼저 침해하여 최종 이용자에게 영향을 미치는 방식이다. 패치 배포 서버나 정상 업데이트를 변조하면 이용자는 **신뢰하는 업데이트 경로를 통해 악성코드를 전달**받을 수 있다. 따라서 정식 패치에 악성코드를 심는 ④가 공급망 공격을 가장 직접적으로 설명한다.

NoteBase

문 23. 80386 레지스터의 용도에 관한 설명 중 가장 적절하지 않은 것은?

① EAX : 입출력과 산술 연산에 사용한다.

② ECX : 루프가 반복되는 횟수나 좌우 방향 시프트 비트 수 저장에 사용한다.

③ EBP : 스택 세그먼트에서 현재 호출되어 사용하는 함수의 시작 주소 값 저장에 사용한다.

④ ESP : 다음 명령어의 오프셋을 저장하며, CS 레지스터와 합쳐 다음에 수행할 명령 주소를 형성한다.

정답 4번

간단한 해설

다음에 실행할 명령어의 오프셋을 보관하는 것은 **EIP**이다. **ESP는 스택 최상단 위치**를 나타내므로 명령어 포인터와 구별해야 한다.

선지별 해설

80386에서 EAX·ECX 등은 범용 레지스터이면서 특정 명령에 관례적·묵시적으로 사용된다. EBP와 ESP는 스택을 참조하는 역할을 하며, 다음 실행 위치를 가리키는 EIP와 구별된다.

① O: EAX는 누산기 역할을 하며 산술 연산의 피연산자나 결과에 사용된다. 입출력 명령에서도 전송 크기에 따라 AL·AX·EAX가 데이터 레지스터로 사용되므로 입출력과 산술 연산에 사용한다는 설명이 적절하다.

② O: ECX는 반복 횟수를 저장하는 카운터로 사용된다. 가변 시프트·회전 명령에서는 ECX의 하위 8비트인 CL이 이동할 비트 수를 지정하는 데 사용된다.

③ O: 스택 세그먼트라는 문맥에서 함수의 시작 주소는 **현재 함수의 스택 프레임 기준 위치**를 뜻하는 표현으로 이해한다. EBP를 프레임 포인터로 쓰면 매개변수와 지역변수 등을 기준 위치에 대한 오프셋으로 접근할 수 있다. EBP가 함수의 실행 코드 시작 주소를 저장한다는 뜻은 아니다.

④ X: 다음 명령어의 오프셋을 저장하는 레지스터는 **ESP가 아니라 EIP**이다. CS가 지정하는 코드 세그먼트와 EIP의 오프셋으로 실행 위치를 나타낸다. ESP는 SS가 지정하는 스택 세그먼트의 현재 최상단 오프셋을 가리키며, 스택에 값을 넣거나 꺼낼 때 변한다.

NoteBase

문 24. Codenomicon사 연구진이 발견한 OpenSSL 암호화 소프트웨어 라이브러리의 심각한 보안 취약점으로 가장 적절한 것은?

① 넷버스(Netbus)

② 스쿨버스(Schoolbus)

③ 루트킷(Rootkit)

④ 하트블리드(Heartbleed)

정답 4번

간단한 해설

하트블리드는 **OpenSSL의 하트비트 구현에서 메모리 내용이 노출되는 취약점**이다. Codenomicon 연구진이 발견한 결함이라는 단서와 일치하며, 암호 알고리즘 자체의 해독이 아니라 구현상의 경계 검사 문제이다.

핵심 풀이

하트블리드는 OpenSSL의 TLS/DTLS 하트비트 확장 구현에서 발견된 정보 노출 취약점이다. Codenomicon 연구진과 Google의 Neel Mehta가 독립적으로 발견했으며, 2014년에 공개되었다. 따라서 ‘Codenomicon’과 ‘OpenSSL 라이브러리’라는 단서가 직접 연결된다.

핵심은 **길이 검증 부족으로 허용된 데이터 범위를 넘어 메모리를 읽어 응답에 포함**할 수 있었다는 점이다. 메모리에 남아 있던 인증정보나 비밀키 등 민감한 내용이 노출될 수 있으므로 심각한 문제였다. 암호 알고리즘 자체를 수학적으로 깨뜨린 것이 아니라, 암호화 기능을 제공하는 라이브러리의 구현 결함이라는 점을 구별해야 한다.

넷버스와 스쿨버스는 원격 제어나 침입에 악용되는 프로그램의 이름으로 알려져 있으며, 이 OpenSSL 결함의 명칭이 아니다. 루트킷은 침입 흔적이나 악성 활동을 숨기고 접근을 유지하는 데 쓰이는 도구·기법을 가리키는 범주로, 특정 하트비트 구현 취약점과 다르다.

따라서 제시된 발견 주체와 대상 라이브러리에 해당하는 것은 ④ 하트블리드이다.

NoteBase

문 25. E-mail 보안 기술에 관한 설명 중 가장 적절하지 않은 것은?

① PGP는 인증서 없이 E-mail 메시지의 인증, 기밀성, 무결성 등을 제공할 수 있다.

② 메시지 송신자는 메시지에서 사용된 암호 알고리즘이나 식별자를 메시지 내에 포함할 필요가 있다.

③ 암호화와 복호화는 대칭키 알고리즘을 사용하여 수행되며 암호화된 메시지를 복호화하기 위해 필요한 비밀키는 메시지 수신자의 공개키로 암호화되어 메시지와 함께 전송된다.

④ S/MIME은 RSA 보안 기술에 기반하여 MIME의 보안 기능을 개선한 E-mail 보안 기술이다.

정답 1번

간단한 해설

정답은 ①이다. PGP는 중앙 CA의 인증서가 반드시 필요한 방식은 아니지만, **OpenPGP 공개키 인증과 인증서명**을 사용한다. 중앙 인증기관에 의존하지 않는다는 점을 인증서 자체가 없다는 뜻과 혼동하면 안 된다.

선지별 해설

① (X) PGP는 중앙 인증기관이 발급하는 X.509 인증서에 반드시 의존하지 않지만, 이를 **공개키 인증서나 키 인증 개념 자체를 사용하지 않는다**는 뜻으로 이해하면 틀리다. OpenPGP에서는 공개키와 사용자 식별정보를 결합하고 인증서명으로 그 결합을 확인하는 공개키 인증 구조를 사용한다. 이 문항은 인증서를 넓은 의미의 공개키 인증서로 보아 ①을 부적절한 설명으로 판단한다. **중앙 CA가 필수가 아니라는 것과 인증서를 전혀 사용하지 않는다는 것은 다르다**.

② (O) 수신자는 어떤 알고리즘과 방식으로 메시지가 처리되었는지 알아야 올바르게 복호화하거나 서명을 검증할 수 있다. 따라서 메시지의 관련 구조에 암호 알고리즘 식별자 등 필요한 정보를 포함한다.

③ (O) 이는 공개키를 이용해 대칭키를 전달하는 하이브리드 암호화 방식이다. 메시지 본문은 대칭키로 암호화하고, 그 대칭키인 세션키는 수신자의 공개키로 보호해 함께 보낸다. 수신자는 자신의 개인키로 세션키를 복구한 뒤 본문을 복호화한다. 여기서 전송되는 비밀키는 **수신자의 개인키가 아니라 대칭 세션키**이다.

④ (O) S/MIME은 MIME 전자우편에 전자서명과 암호화 등의 보안 기능을 제공하는 기술이다. RSA Data Security의 PKCS 계열 기술에서 출발하여 PKCS #7을 계승한 CMS 등의 형식을 활용한다. 따라서 선지의 설명은 그 기반을 나타낸 것이며, 모든 처리에 RSA 알고리즘만 사용한다는 뜻은 아니다.

NoteBase

문 26. DDoS 대응방식에 관한 설명 중 옳은 것을 모두 고른 것으로 가장 적절한 것은?

㉮ In-Line 방식은 DDoS 공격을 탐지하고 직접 차단하며 가장 많이 구축되는 방식이다.
㉯ In-Line 방식은 DDoS 대응장비에 장애가 있어도 네트워크 가용성에는 영향이 없다.
㉰ Out of Path 방식은 In-Line 방식에 비해 구축 비용이 일반적으로 많이 든다.
㉱ Out of Path 방식은 미러링 장비를 통해 복제된 패킷을 받아 DDoS 대응장비에서 분석 차단한다.

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

정답 3번

간단한 해설

정답은 ③ ㉮·㉰·㉱이다. In-Line 장비는 실제 통신 경로에 있으므로 **장애가 가용성에 영향을 줄 수 있다.** Out of Path는 경로 밖에서 트래픽을 분석하고 연동 차단 등의 방식으로 대응한다.

NoteBase

보기별 해설

㉮ (O) In-Line은 실제 통신 경로에 대응 장비를 직렬로 배치하여 통과하는 트래픽을 검사하고 공격 패킷을 직접 차단하는 방식이다. 문항에서는 이를 널리 구축되는 기본 방식으로 제시하고 있다. 다만 실제 도입 비중은 망 규모와 서비스 환경에 따라 달라질 수 있다.

㉯ (X) In-Line 장비는 실제 통신 경로 위에 있으므로 장비 장애나 처리 용량 초과가 정상 트래픽 전달에 영향을 줄 수 있다. 이중화나 우회 기능으로 위험을 줄일 수는 있지만, 그런 조건 없이 장애가 네트워크 가용성에 영향을 주지 않는다고 단정할 수 없다.

㉰ (O) 문항의 일반적인 구축 비교에서 Out of Path는 트래픽 복제·수집과 탐지 결과에 따른 차단 연동 또는 우회 처리를 위한 구성이 추가되어 비용과 구성 복잡도가 커질 수 있다. 이는 일반적 비교이며, 모든 제품과 규모에서 비용이 반드시 더 높다는 절대적인 법칙은 아니다.

㉱ (O) Out of Path 대응 체계는 실제 통신 경로 밖에서 미러링된 트래픽을 받아 분석하고, 공격이 확인되면 네트워크 장비와의 연동 차단이나 트래픽 우회·정화 등의 방식으로 대응한다. **복제 패킷을 분석하거나 폐기하는 것만으로 원래 통신 경로의 패킷이 차단되지는 않는다.** 따라서 '분석 차단'은 탐지 이후 실제 경로에 대한 대응까지 포함한 설명으로 이해해야 한다.

옳은 설명은 ㉮·㉰·㉱이며 정답은 ③이다. 핵심 오답은 통신 경로에 놓인 In-Line 장비의 장애 영향을 부정한 ㉯이다.

NoteBase

문 27. 다음 윈도우 SID 출력 내용에 관한 설명 중 가장 적절하지 않은 것은?

```
SID for WIN_2016\administrator
S-1-5-21-3927844882-394592529-3216461276-500
 ㉮   ㉯                ㉰                ㉱
```

① ㉮ : 해당 시스템이 윈도우 시스템임을 의미한다.

② ㉯ : 시스템의 사용자 계정 유형(관리자, Guest, 일반 사용자)을 나타낸다.

③ ㉰ : 시스템의 고유한 숫자로, 시스템을 설치할 때 이것의 특성을 수집하여 생성한다.

④ ㉱ : 숫자로 표현하는 각 사용자의 고유한 ID이다.

정답 2번

간단한 해설

㉯의 '5-21'은 **사용자 계정 유형을 나타내지 않는다**. '5'는 SID 발급 주체인 NT Authority를, '21'은 컴퓨터·도메인 계정 SID에 쓰이는 하위 권한 값을 뜻한다. 기본 Administrator 계정은 맨 끝의 **RID 500**으로 식별한다.

출제 포인트

윈도우 SID에서 발급 주체, 컴퓨터·도메인 식별 부분, 개별 계정의 RID가 차지하는 위치를 구분하는 문제이다.

핵심 개념

SID는 윈도우가 사용자나 그룹 등 보안 주체를 식별하는 보안 식별자이다. 같은 컴퓨터의 로컬 계정은 컴퓨터를 식별하는 앞부분을 공유하고, 마지막의 RID로 구별된다.
그림은 'S-1 / 5-21 / 3927844882-394592529-3216461276 / 500'으로 나누어 읽는다. S는 SID 문자열이라는 표시이고 1은 SID 구조의 버전이다. 5는 NT Authority, 21은 컴퓨터·도메인 계정 SID에 쓰이는 하위 권한 값이다. 가운데 세 숫자는 해당 컴퓨터·도메인을 식별하는 부분이며, 마지막 500은 그 안에서 특정 계정을 식별하는 상대 식별자이다.

NoteBase

선지별 해설

① O
문항에서는 ㉮를 윈도우 SID의 표기라는 취지로 설명한다. 다만 S-1 자체가 윈도우 운영체제의 종류나 버전을 뜻하는 것은 아니다. 정확히는 S가 SID 문자열임을, 1이 SID 구조의 버전임을 나타낸다.

② X
㉯의 '5-21'은 관리자·Guest·일반 사용자라는 계정 유형을 나타내지 않는다. 5는 NT Authority를 나타내는 식별 기관 값이고, 21은 컴퓨터·도메인 계정 SID에 쓰이는 하위 권한 값이다. 따라서 '사용자 계정 유형'은 'SID 발급 주체와 하위 권한 값'으로 고친다. 그림의 기본 Administrator 계정을 식별하는 값은 ㉱의 RID 500이다.

③ O
㉰의 세 숫자는 해당 컴퓨터·도메인을 식별하는 고유 부분이며, 로컬 컴퓨터의 경우 윈도우 설치 과정에서 생성된다. 이 문항에서는 설치 시 생성되는 시스템 식별 부분이라는 취지로 이해한다. 다만 '특성을 수집하여 생성한다'를 하드웨어 사양을 그대로 숫자로 변환한다는 뜻으로 외우지는 않는다. 기술적으로 이 부분은 생성된 96비트 난수를 세 개의 32비트 값으로 나눈 것이다.

④ O
㉱는 같은 컴퓨터·도메인 안에서 계정을 구별하는 RID이다. 그림의 500은 기본 Administrator 계정에 예약된 값이다. RID만으로 모든 컴퓨터의 사용자를 구별하는 것은 아니며, 컴퓨터·도메인 식별 부분과 결합한 전체 SID가 계정을 식별한다.

오답 포인트

그림 위에 administrator가 적혀 있다고 해서 '5-21'이 관리자 유형을 나타내는 것은 아니다. 계정을 구별하는 마지막 값과 SID 발급 주체를 나타내는 앞쪽 값을 혼동한 설명이다. 또한 S-1의 1은 윈도우 버전 번호가 아니다.

다시 나오면 이렇게 판단

SID를 앞쪽의 구조·발급 주체, 가운데의 컴퓨터·도메인 식별 부분, 맨 끝의 RID로 나누어 판단한다. 기본 Administrator 계정 여부는 마지막 RID 500으로 확인하며, RID의 고유성은 같은 컴퓨터·도메인 안에서 이해한다.

암기 포인트

S는 SID 표시, 1은 구조 버전, 5는 NT Authority, 가운데 세 숫자는 컴퓨터·도메인 식별 부분, 끝의 RID는 계정 식별이다. 기본 Administrator의 RID는 500이다.

NoteBase

문 28. 사이버 킬 체인은 사이버 공격을 프로세스 기반으로 분석하여 단계별로 가해지는 위협 요소를 파악하고 공격을 완화할 목적으로 수행되는 사이버 공격 분석 모델이다. 공격단계를 순서대로 나열한 것으로 빈칸 (㉮)~(㉲)에 가장 적절한 것은?

[공격단계]
정찰-(㉮)-(㉯)-(㉰)-(㉱)-명령&제어-실행

① ㉮: 무기화, ㉯: 설치, ㉰: 전달, ㉱: 익스플로잇

② ㉮: 무기화, ㉯: 전달, ㉰: 설치, ㉱: 익스플로잇

③ ㉮: 무기화, ㉯: 익스플로잇, ㉰: 전달, ㉱: 설치

④ ㉮: 무기화, ㉯: 전달, ㉰: 익스플로잇, ㉱: 설치

정답 4번

간단한 해설

공격 수단은 먼저 준비되어 표적에 전달되고, **취약점 악용으로 동작할 계기를 얻은 뒤 설치**된다. 따라서 전달과 익스플로잇, 설치는 서로 구별되며 그 선후관계를 바꾸지 않는다.

NoteBase

올바른 순서

정찰 → 무기화(㉮) → 전달(㉯) → 익스플로잇(㉰) → 설치(㉱) → 명령&제어 → 실행

정찰: 표적의 환경과 인적·기술적 정보를 파악한다. 이 정보는 어떤 공격 수단을 준비할지 결정하는 바탕이 된다.

무기화(㉮): 정찰 결과에 맞추어 공격에 사용할 수단을 준비한다. 준비된 공격 수단이 있어야 표적에게 보내는 전달 단계로 진행할 수 있다.

전달(㉯): 준비한 공격 수단을 표적 환경에 도달시킨다. **전달되었다는 사실만으로 취약점 악용에 성공한 것은 아니므로** 익스플로잇 단계와 구별한다.

익스플로잇(㉰): 표적에 도달한 공격 수단이 취약점 등을 악용하여 공격자의 코드가 동작할 계기를 만든다. 이 모델에서는 이러한 악용을 통해 다음의 설치가 가능해진다.

설치(㉱): 표적 시스템에 악성 구성요소 등을 설치하여 접근을 지속할 기반을 만든다. **코드 실행을 유발하는 익스플로잇과 지속적 접근 기반을 만드는 설치**를 구별한다.

명령&제어: 침해된 시스템과 공격자가 통신하며 명령을 전달할 수 있는 경로를 형성한다. 이는 이후 공격 목적을 수행하는 데 활용된다.

실행: 정보 탈취나 서비스 방해 등 공격자가 의도한 최종 목적을 수행한다. 여기서 실행은 단순히 프로그램을 처음 구동한다는 뜻이 아니라 공격 목표에 따른 행위를 가리킨다.

NoteBase

문 29. CSRF(Cross-Site Request Forgery) 공격에 관한 설명 중 가장 적절하지 않은 것은?

① HTTP GET과 HTTP POST 서비스의 차이에 따라 CSRF 공격 방법도 차이가 있다.

② 피해자가 타겟 웹 사이트로 전송되는 사이트 간 요청을 위조할 수 있는 악성 웹 페이지를 방문하여야 한다.

③ CSRF 공격이 성공하기 위해서는 피해자가 악성 웹 페이지 방문 후 타겟 웹 사이트와 세션을 확립하여야 한다.

④ 일반적인 대응책은 HTTP 요청이 자체 웹 페이지에서 오는지 아니면 제3자의 웹 페이지에서 오는지 구별하는데 도움이 되는 비밀 토큰 등을 이용하는 것이다.

정답 3번

간단한 해설

③이 가장 적절하지 않다. 전형적인 CSRF는 피해자가 대상 사이트에 **이미 인증된 상태**에서 의도하지 않은 요청을 보내게 하는 공격이다. 악성 페이지 방문 후에 새로 세션을 만들어야 하는 것은 아니다.

선지별 해설

① (O) 대상 기능이 GET과 POST 중 어떤 요청 방식을 사용하는지에 따라 요청을 유발하는 형태와 매개변수 전달 방식이 달라진다. 다만 POST를 쓴다는 사실만으로 CSRF가 방지되는 것은 아니며, 서버가 요청의 정당성을 별도로 확인해야 한다.

② (O) 문항이 전제한 전형적인 공격에서는 피해자가 공격자가 유도한 웹 페이지 등의 악성 콘텐츠에 노출되고, 그 콘텐츠가 대상 사이트로 의도하지 않은 요청을 발생시킨다. 반드시 공격자 소유의 별도 웹 사이트에서만 가능한 것은 아니며, 악성 링크나 삽입된 콘텐츠 등도 유도 경로가 될 수 있다.

③ (X) 전형적인 세션 기반 CSRF는 피해자가 대상 사이트에 **이미 로그인하여 유효한 세션을 가진 상태**에서 악성 콘텐츠에 의해 요청을 보내도록 유도한다. 브라우저가 해당 요청에 인증 정보를 자동으로 포함할 수 있다는 점을 악용하는 것이다. 악성 페이지를 방문한 후에 반드시 새로 세션을 확립해야 한다는 순서 조건은 없다.

④ (O) 서버가 예측하기 어려운 CSRF 방지 토큰을 발급하고 상태를 변경하는 요청에서 그 유효성을 검증하면, 공격자가 임의로 만든 요청과 정상적인 요청을 구별하는 데 도움이 된다. 토큰은 공격자가 알 수 없고 적절히 검증되어야 하며, 세션 쿠키가 자동으로 전송된다는 사실만으로 요청을 신뢰해서는 안 된다.

NoteBase

문 30. 리눅스 시스템에서 다음과 같은 실행 결과를 출력하는 가장 적절한 명령어는?

Filesystem	1K-blocks	Used	Avail	Use%	Mounted on
/dev/sda2	91871**	4977***	3743***	58%	/

① #mount -t

② #df -k

③ #du -k

④ #repquota -a

정답 2번

간단한 해설

정답은 ② **df -k**이다. df는 **파일시스템별 디스크 사용량과 가용 공간**을 표시하며, -k는 1024바이트 단위 출력을 지정한다.

핵심 풀이

그림에는 Filesystem, 1K-blocks, Used, Avail, Use%, Mounted on 열이 있다. 이는 **파일시스템별 전체 용량·사용량·가용량·사용률·마운트 위치**를 보여 주는 df의 출력 형식이다.

선택지의 -k 옵션은 용량을 **1024바이트 블록 단위**로 표시하도록 지정한다. 따라서 1K-blocks라는 열 제목과 일치하는 명령은 ② df -k이다. /dev/sda2 파일시스템이 루트 디렉터리 /에 마운트되어 있고 사용률이 58%임을 읽을 수 있다. 가려진 용량 숫자를 복원할 필요는 없다.

du -k는 지정한 파일이나 디렉터리가 차지하는 디스크 사용량을 집계하는 명령으로, 파일시스템 전체의 가용량을 보여 주는 df와 다르다.

mount는 파일시스템을 연결하거나 마운트 정보를 다루며 -t는 파일시스템 종류를 지정하는 옵션이다.

repquota -a는 적용 대상 파일시스템들의 사용자 디스크 할당량 정보를 보고하는 명령이므로 제시된 출력과 구별된다. 그룹 할당량을 보고하려면 -g 옵션을 지정한다.

NoteBase

문 31. 컨테이너화된 응용프로그램의 보안에 관한 설명으로 가장 적절하지 않은 것은?

① 컨테이너 안에서는 호스트의 파일 시스템 전체를 볼 수 없다.

② 컨테이너는 호스트 컴퓨터의 커널을 공유한다.

③ 컨테이너 격리는 기본적으로 VM 격리보다 강하다.

④ 컨테이너 방화벽은 규칙에서 벗어난 네트워크 연결 시도를 기록하고 보고한다.

정답 3번

간단한 해설

일반적인 컨테이너는 **호스트 커널을 공유**하므로, 별도 게스트 커널을 사용하는 VM보다 기본 격리 경계가 강하다고 할 수 없다. 가벼운 실행 환경이라는 장점과 격리 강도는 구별해야 한다.

선지별 해설

① O: 일반적인 격리 구성의 컨테이너는 독립된 파일시스템 관점을 가지므로 호스트의 전체 파일시스템이 자동으로 노출되지 않는다. 다만 호스트 디렉터리를 명시적으로 공유하거나 과도한 권한을 부여하면 그 경계가 약해질 수 있다. 따라서 이 설명은 정상적인 기본 격리 상태에 관한 것이며, 어떤 설정에서도 호스트 파일에 접근할 수 없다는 절대적 보장은 아니다.

② O: 일반적인 운영체제 수준 컨테이너는 **호스트의 커널을 공유**하면서 프로세스·파일시스템·네트워크 등의 관점을 분리한다. 컨테이너마다 독립된 게스트 운영체제 커널을 실행하는 방식이 아니므로 가볍지만, 공유 커널이 보안상 공통 의존 지점이 된다.

③ X: 기본적인 격리 경계는 일반적으로 별도의 게스트 커널을 두는 VM 쪽이 더 강하다. 컨테이너는 커널을 공유하므로 커널 취약점이나 과도한 권한·마운트 설정이 다른 컨테이너 또는 호스트에 영향을 줄 위험이 있다. VM도 하이퍼바이저 취약점과 설정 오류에서 자유롭지는 않지만, 이를 이유로 컨테이너 격리가 기본적으로 더 강하다고 할 수는 없다.

④ O: 컨테이너 방화벽은 컨테이너의 네트워크 통신을 정책과 비교하여 허용되지 않은 연결을 통제하고, 위반 시도를 기록·보고하여 탐지와 대응을 돕는다. 실제 기록·알림의 범위는 제품 기능과 설정에 달려 있으므로, 컨테이너를 생성하기만 하면 모든 연결 시도가 자동 보고된다는 의미는 아니다.

NoteBase

문 32. 단편화(fragmentation)가 수행된 IP 데이터그램의 한 조각(fragment)의 필드 값들이 다음과 같을 때의 설명으로 가장 적절한 것은?

헤더 길이=5, 전체 길이=1020, 식별자(identification)=49153
플래그의 M비트=1, 단편화 오프셋=340

① 다음 조각의 단편화 오프셋은 465이다.

② 두 번째 조각이며, 다음 조각의 식별자는 49154가 된다.

③ 중간 조각이며, 다음 조각이 마지막 조각이 된다.

④ 동일한 식별자를 갖는 단편화된 조각들은 최종 목적지의 라우터에서 재조합된다.

정답 1번

간단한 해설

헤더는 20바이트이므로 조각의 데이터 부분은 1,000바이트이다. **오프셋의 8바이트 단위**를 적용하면 다음 조각의 오프셋은 $340 + \frac{1,000}{8} = 465$이다.

선지별 해설

① O: IPv4의 헤더 길이 필드는 4바이트 단위이므로 실제 헤더는 $5 \times 4 = 20$바이트이다. 전체 길이는 헤더를 포함하므로 데이터 부분은 $1,020 - 20 = 1,000$바이트이다. **단편화 오프셋은 8바이트 단위**이므로 현재 조각 바로 뒤 데이터의 오프셋은 $340 + \frac{1,000}{8} = 465$이다. 따라서 ①이 적절하다.

② X: 오프셋 340은 원래 데이터의 시작점으로부터 $340 \times 8 = 2,720$바이트 떨어진 위치에서 이 조각이 시작한다는 뜻이지, 두 번째 조각이라는 뜻은 아니다. 앞선 조각의 크기와 개수는 주어지지 않았다. 또한 동일한 원본 데이터그램의 조각은 **식별자 49153을 그대로 공유**하므로 다음 조각마다 식별자가 1씩 증가하지 않는다.

③ X: 오프셋이 0보다 크므로 첫 조각은 아니며, M 비트가 1이므로 뒤에 다른 조각이 있어 마지막 조각도 아니다. 따라서 현재가 중간 조각이라는 부분은 맞지만, **바로 다음 조각이 마지막인지는 알 수 없다**. 마지막 조각 여부는 해당 조각의 M 비트가 0인지 확인해야 한다.

④ X: IP 조각의 재조합은 일반적으로 중간 라우터나 목적지 직전 라우터가 아니라 **해당 IP 데이터그램의 최종 목적지 호스트**에서 수행한다. 재조합 대상은 식별자뿐 아니라 출발지·목적지 주소와 상위 프로토콜 등도 함께 확인하여 구분하므로, 식별자가 같다는 사실만으로 서로 다른 통신의 조각을 합치지 않는다.

NoteBase

문 33. 유닉스의 traceroute에 관한 설명 중 가장 적절하지 않은 것은?

① traceroute의 메시지는 UDP 데이터그램에 캡슐화되며 목적지 호스트에서 사용하지 않는 포트 번호를 사용한다.

② 목적지 호스트까지의 경로상에 있는 라우터들에 의해 발송되는 ICMP Time Exceeded 메시지와 ICMP Destination Unreachable 메시지를 사용한다.

③ 목적지 호스트까지의 경로상에 있는 라우터들의 개수가 n개라면 최대 (n+1)개의 ICMP 오류 보고 메시지를 수신하게 된다.

④ traceroute는 각 라우터와 목적지 호스트까지의 왕복 시간을 알기 위해 타이머를 설정한다.

정답 2번

간단한 해설

②는 두 ICMP 메시지의 발송 주체를 모두 라우터로 설명한 점이 부적절하다. 정상적인 UDP 기반 경로 추적에서 **Time Exceeded는 중간 라우터**가 보내고, 목적지 도달을 알리는 **Destination Unreachable의 Port Unreachable 응답은 목적지 호스트**가 보낸다.

NoteBase

선지별 해설

① O: 유닉스 traceroute의 전통적인 UDP 방식은 탐침 데이터를 UDP 데이터그램에 담아 목적지로 보낸다. 목적지 호스트에서 **사용하지 않는 UDP 포트**를 지정하여, 탐침이 도착하면 해당 호스트가 Port Unreachable 응답을 보내도록 한다. 이 응답으로 최종 목적지에 도달했음을 확인한다.

② X: 두 메시지 모두 경로상의 라우터가 발송한다는 부분이 잘못되었다. 탐침의 IP 헤더에 있는 TTL이 중간 라우터에서 소진되면 그 라우터가 ICMP Time Exceeded를 보낸다. 반면 탐침이 목적지 호스트까지 도달했으나 지정한 UDP 포트를 사용하는 프로그램이 없으면, **목적지 호스트가 ICMP Destination Unreachable의 코드 3인 Port Unreachable**을 보낸다. traceroute는 전자로 중간 경유지를 확인하고 후자로 목적지 도달을 확인한다.

③ O: **각 TTL 값에서 한 번씩 탐침하는 기본 모형**을 기준으로 이해한다. 경로가 일정하고 라우터가 n개라면, TTL을 1부터 n까지 늘리며 보낸 탐침에 대해 각 라우터에서 Time Exceeded 응답을 하나씩 받을 수 있다. TTL이 n+1인 탐침은 목적지에 도달하여 Port Unreachable 응답을 유도하므로, 이 모형에서는 최대 n+1개의 ICMP 오류 보고 메시지를 받는다. 다만 실제 유닉스 계열 구현은 같은 TTL로 보통 세 번 탐침하며 횟수를 변경할 수도 있다. 따라서 원문의 n+1을 모든 실제 실행에 적용되는 절대 상한으로 해석해서는 안 된다.

④ O: traceroute는 탐침을 보낸 시각부터 대응하는 ICMP 응답을 받은 시각까지의 경과 시간을 측정한다. 이 시간이 **출발지에서 해당 라우터 또는 목적지 호스트까지의 왕복 시간**이다. 타이머로 응답 대기 시간도 제한하며, 제한 시간 안에 응답이 없으면 해당 탐침의 왕복 시간을 얻지 못한 것으로 처리한다.

NoteBase

문 34. 안전한 소프트웨어 개발 운영을 목표로 하는 안전성 분석기법을 설명한 것으로 빈칸 (㉮)와 (㉯)에 가장 적절한 것은?

(㉮) : 인터페이스 및 함수 호출의 구조적 취약점 분석
(㉯) : 가상화 환경에서 직접 실행을 통해 이상 현상 분석

① ㉮: 소스코드 분석기법, ㉯: 샌드박스 분석기법
② ㉮: 시멘틱 분석기법, ㉯: 행위탐지 분석기법
③ ㉮: 샌드박스 분석기법, ㉯: 바이너리 분석기법
④ ㉮: 시멘틱 분석기법, ㉯: 샌드박스 분석기법

정답 4번

간단한 해설

정답은 ④이다. 인터페이스·함수 호출의 구조와 의미를 살피는 ㉮은 **시멘틱 분석**, 격리된 가상 환경에서 직접 실행해 이상을 관찰하는 ㉯는 **샌드박스 분석**에 해당한다.

빈칸별 해설

㉮은 시멘틱 분석기법이다. 프로그램의 의미와 동작 관계를 고려하여 인터페이스와 함수 호출 등의 구조를 분석하고, 잘못된 사용이나 연결 관계에서 생기는 취약점을 찾는다. 단순한 문자열이나 문법 형태의 확인보다 호출 관계와 의미적 일관성을 살펴본다는 점이 핵심이다.

㉯는 샌드박스 분석기법이다. 외부 시스템에 미치는 영향을 제한하는 격리된 가상 환경 등에서 프로그램을 실제 실행하고, 실행 중 나타나는 비정상 동작을 관찰한다. **'가상화 환경에서 직접 실행'**이라는 조건이 이 기법을 가리키는 결정적 단서이다.

소스코드 분석은 소스코드를 대상으로 결함을 찾는 넓은 범주이며 시멘틱 분석을 포함할 수도 있다. 그러나 ㉮의 구체적 설명에 가장 직접적으로 대응하는 명칭은 시멘틱 분석이다. 바이너리 분석은 컴파일된 실행 파일 등을 분석 대상으로 삼는다는 분류이며, ㉯의 격리 실행 환경을 직접 나타내는 명칭이 아니다.

행위탐지 분석은 실행 중의 행위를 관찰하는 데 초점을 두므로 샌드박스와 함께 활용될 수 있다. 다만 ㉯는 단순히 행위를 탐지한다는 설명을 넘어 가상화 환경에서 직접 실행하는 방식을 명시하므로 샌드박스 분석이 가장 적절하다.

따라서 ㉮ **시멘틱 분석기법,** ㉯ **샌드박스 분석기법**으로 연결한 ④가 정답이다.

NoteBase

문 35. 다음 설명에 관한 것으로 가장 적절한 것은?

◯ 외부로부터의 접근이 가능하지만 어느 정도의 보호가 필요한 시스템들이 자리 잡고 있다.
◯ 보통 웹 서버, E-mail 서버, DNS 서버 등을 둔다.
◯ 외부 방화벽은 외부 연결의 필요성과 일치되는 수준 정도의 접근 제어와 보호를 수행한다.
◯ 내부 방화벽은 내부의 서버와 워크스테이션들을 보호하기 위해 외부 방화벽보다 엄격한 필터링 규칙을 적용한다.

① 허니넷(Honey Net)
② 인트라넷(Intranet)
③ DMZ(Demilitarized Zone)
④ 응용 레벨 게이트웨이(Application-level Gateway)

정답 3번

간단한 해설

외부에 공개할 서버를 내부 업무망과 분리하고, 두 영역의 접근 통제를 달리하는 구역은 **DMZ**이다. 외부 서비스는 제공하되 내부망으로의 접근은 더 엄격히 제한한다.

NoteBase

구성 요소별 해설

DMZ는 외부에 공개할 서버를 내부 업무망과 분리하여 배치하는 네트워크 구역이다. 제시된 설명은 외부 접근을 허용하면서도 내부망으로의 접근은 더 엄격하게 통제하는 구조를 나타낸다.

외부 접근과 보호의 병행: 공개 서비스는 외부 사용자가 접속할 수 있어야 하지만 무제한 접근을 허용해서는 안 된다. DMZ에서는 서비스 제공에 필요한 통신만 허용하고 서버를 보호한다.

공개 서버의 배치: 외부에 서비스를 제공하는 웹·메일·DNS 서버 등을 DMZ에 배치할 수 있다. 공개 서버가 침해되더라도 **내부 업무망으로 직접 확산되는 위험을 줄이기 위해** 네트워크를 분리한다. 모든 웹·메일·DNS 서버가 반드시 DMZ에 있어야 한다는 뜻은 아니다.

외부 방화벽의 역할: 인터넷에서 DMZ의 공개 서비스로 들어오는 통신을 필요한 범위에서 허용한다. 외부 접속을 지원해야 한다는 요구에 맞추어 접근 제어를 적용한다.

내부 방화벽의 역할: DMZ와 내부망 사이의 통신을 더 엄격하게 제한하여 내부 서버와 워크스테이션을 보호한다. **DMZ에 접근할 수 있다고 내부망 접근까지 허용되는 것은 아니다.**

따라서 네 설명이 함께 가리키는 것은 DMZ인 ③이다. 허니넷은 공격을 관찰하기 위한 유인용 네트워크, 인트라넷은 조직 내부용 네트워크, 응용 레벨 게이트웨이는 응용 계층에서 통신을 중계·검사하는 보안 기능으로 구별된다.

NoteBase

문 36. 비즈니스 스캠(SCAM)은 E-mail을 해킹하여 거래 결제 시점에 바이어에게 결제 은행이 변경되었다는 E-mail을 송부하고 결제 대금을 가로채는 수법이다. 공격 절차를 나열한 것으로 가장 적절한 것은?

① E-mail 스푸핑 - 스팸 메일로 감염 - 유사 E-mail 생성 - MITM(중간자) 공격

② 스팸 메일로 감염 - 유사 E-mail 생성 - MITM(중간자) 공격 - E-mail 스푸핑

③ 스팸 메일로 감염 - MITM(중간자) 공격 - E-mail 스푸핑 - 유사 E-mail 생성

④ 유사 E-mail 생성 - MITM(중간자) 공격 - 스팸 메일로 감염 - E-mail 스푸핑

정답 2번

간단한 해설

이 사례는 거래정보 침해와 사칭 수단 마련 뒤에 교신에 개입하고, **마지막에 거래처를 가장한 결제정보 변경 안내**로 피해를 일으키는 흐름이다. 사칭 수단의 준비와 그 수단을 이용한 허위 안내 발송을 구별해야 한다.

올바른 순서

스팸 메일로 감염 → 유사 E-mail 생성 → MITM(중간자) 공격 → E-mail 스푸핑

스팸 메일로 감염: 이 문항이 전제한 사례에서는 악성 메일로 인한 침해가 거래정보 노출의 출발점이다. 이메일과 관련 정보에 대한 비인가 접근이 생기면 이후 거래 당사자를 사칭하고 통신에 개입하는 데 필요한 맥락이 노출될 수 있다. 모든 비즈니스 이메일 사기가 반드시 악성코드 감염으로 시작한다는 뜻은 아니다.

유사 E-mail 생성: 정상 거래 당사자의 주소와 혼동하기 쉬운 사칭용 주소가 마련되는 단계이다. 여기서 말하는 유사 이메일은 그 사칭 수단의 준비를 뜻하며, 뒤의 허위 결제 안내 발송 자체와 구별된다.

MITM(중간자) 공격: 거래 당사자 사이의 이메일 교신에 공격자가 끼어들어 거래 흐름을 파악하거나 통신을 왜곡하는 단계이다. 이 문항에서는 이를 넓은 의미의 중간자 개입으로 사용하며, 반드시 특정 네트워크 프로토콜의 중간자 기법을 뜻하는 것은 아니다. 교신과 결제 맥락에 대한 개입이 뒤의 허위 안내를 믿게 만드는 배경이 된다.

E-mail 스푸핑: 마지막으로 정상 거래처가 보낸 것처럼 위장한 결제정보 변경 안내가 제시되는 단계이다. 앞서 마련된 사칭 수단과 거래 맥락을 이용해 수신자가 잘못된 결제 지시를 신뢰하도록 하는 것이 피해의 직접 계기가 된다. 결제정보 변경을 이메일 내용만으로 신뢰하지 않고 기존에 확인된 별도 연락 경로로 검증해야 하는 이유가 여기에 있다.

NoteBase

문 37. 다음에서 설명하는 DEP(Data Execution Prevention) 우회 방법으로 가장 적절한 것은?

◯ DEP를 우회하기 위해 사용되는 함수들은 메모리와 관련된 함수이며, 이러한 함수를 호출하기 위해서는 쉘코드 주소, 크기 등 적절한 인자값이 필요하다. 이러한 인자값을 구성하고 함수를 호출하기 위해서 사용되는 기술이다.
◯ RET로 끝나는 명령 조각들인 가젯(Gadget)의 체인(Chain)을 만들어서 원하는 코드 조각들을 여러 번 실행하게 된다.

① ROP
② RTL
③ ASLR
④ DEP 비활성화

정답 1번

간단한 해설

RET로 끝나는 명령 조각인 가젯을 체인으로 연결해 실행하는 방식은 ROP(Return-Oriented Programming)이다. 기존 실행 코드를 재사용하여 필요한 인자값을 구성하고 메모리 관련 함수를 호출할 수 있다.

공통 해설

ROP(Return-Oriented Programming)는 이미 실행 가능한 메모리에 있는 짧은 명령 조각인 가젯을 연결하여 원하는 동작을 수행하는 코드 재사용 기술이다. 지문의 핵심은 **RET로 끝나는 가젯들을 체인으로 실행한다**는 점이다. 한 가젯의 RET가 다음 가젯으로 실행을 넘기므로, 여러 조각의 동작을 이어 붙여 함수 호출에 필요한 인자값 등을 구성할 수 있다.

DEP는 실행 권한이 없는 데이터 영역의 코드 실행을 막는다. ROP는 그 영역에 넣은 쉘코드를 처음부터 직접 실행하는 대신 기존의 실행 가능한 코드를 이용한다. 지문에서는 이 가젯 체인으로 쉘코드 주소와 크기 등의 인자를 준비하고 메모리 관련 함수를 호출하여 DEP를 우회하는 과정을 설명한다.

RTL(Return-to-Libc)은 기존 라이브러리 함수로 실행을 돌리는 방식이지만, 지문처럼 **짧은 명령 조각들을 연결하는 방식**을 가리키는 명칭은 ROP이다. ASLR이나 DEP 비활성화도 이 가젯 체인 실행 기법의 명칭에 해당하지 않는다.

NoteBase

문 38. iptables 명령어에서 체인에 설정된 정책정보를 모두 제거하는 옵션으로 가장 적절한 것은?

① iptables -L

② iptables -nL

③ iptables -vL

④ iptables -F

정답 4번

간단한 해설

정답은 ④이다. **-F(flush)**는 체인에 등록된 규칙을 모두 비운다. -L, -nL, -vL은 표시 방식에 차이가 있는 조회 명령이다.

핵심 풀이

④ iptables -F의 -F는 flush를 뜻하며, **체인에 등록된 규칙을 모두 삭제**하는 명령이다. 체인을 지정하면 그 체인의 규칙을 비우고, 제시된 명령처럼 체인을 생략하면 선택된 테이블의 모든 체인에 적용된다. -t를 생략했으므로 기본 대상은 filter 테이블이다.

① -L은 규칙 목록을 조회한다.

② -nL은 -n과 -L을 함께 사용하여 주소와 포트 등을 숫자로 표시하면서 목록을 조회한다.

③ -vL은 -v와 -L을 함께 사용하여 패킷·바이트 카운터 등 자세한 정보를 포함해 조회한다. 세 명령 모두 규칙을 제거하는 기능과는 다르다.

문제의 '정책정보 제거'는 체인에 추가된 규칙을 비우는 의미로 이해해야 한다. **-F는 기본 정책 자체를 변경하거나 체인을 삭제하는 명령이 아니다.** 기본 체인의 ACCEPT·DROP 정책을 설정하는 -P, 체인을 삭제하는 -X와 구별한다.

NoteBase

문 39. IPSec의 전송모드(transport mode)에 관한 설명 중 가장 적절하지 않은 것은?

① 일반적으로 데이터를 호스트-대-호스트로 보호할 때 사용한다.

② 전송모드의 IPSec 헤더와 트레일러는 데이터링크(이더넷) 프레임에 직접 캡슐화된다.

③ 송신 호스트는 전송계층으로부터 전달된 페이로드만 보호한다.

④ 터널 모드(tunnel mode)와는 다르게 하나의 IP 헤더만 생성하여 사용한다.

정답 2번

간단한 해설

IPSec 전송모드에서도 **IP 헤더는 유지**되며, 보안 헤더는 IP 헤더 다음에 위치한다. IPSec 정보를 IP 계층 없이 이더넷 프레임에 직접 넣는 방식이 아니다.

선지별 해설

전송모드는 기존 IP 헤더를 유지하면서 주로 그 뒤의 상위 계층 내용을 보호한다. 반면 터널 모드는 원래 IP 패킷을 내부에 넣고 바깥쪽 IP 헤더를 추가한다. 실제 보호 범위는 AH와 ESP에 따라 차이가 있다.

① O: 전송모드는 일반적으로 통신하는 두 호스트가 직접 보안 처리를 수행하는 호스트 간 보호에 사용된다. 중간의 보안 게이트웨이 사이에서 내부 네트워크의 패킷을 감싸는 대표적인 터널 모드 용도와 구별된다.

② X: 전송모드에서는 **IP 헤더 뒤에 IPSec 보안 헤더**가 들어간다. ESP를 예로 들면 IP 헤더, ESP 헤더, 보호되는 상위 계층 내용과 ESP 트레일러 등의 순서로 구성되며, 이 IP 패킷이 다시 링크 계층 프레임에 실린다. IP 헤더를 거치지 않고 보안 헤더·트레일러만 이더넷에 직접 캡슐화한다는 설명은 적절하지 않다.

③ O: 문항에서 헤더·트레일러를 함께 언급하는 ESP 전송모드의 전형적 설명으로 보면, 원래 IP 헤더가 아니라 그 뒤의 상위 계층 페이로드를 보호한다. 여기서 IP 페이로드에는 TCP·UDP 헤더와 데이터 등이 포함된다. 다만 **AH의 인증은 IP 헤더의 일부 필드까지 포함**하므로, 모든 IPSec 전송모드에서 IP 헤더는 어떤 보호도 받지 않는다는 절대적 의미로 일반화해서는 안 된다.

④ O: 전송모드는 원래 IP 헤더를 이용하며, 터널 모드처럼 원래 IP 패킷 바깥에 별도의 IP 헤더를 추가하지 않는다. 따라서 기본적인 전송모드 구조는 하나의 IP 헤더를 갖는 것으로 설명한다.

NoteBase

문 40. 사회공학적 공격 흐름에서 단계별 공격방법으로 가장 적절한 것은?

[공격흐름]
정보수집단계(㉮) - 관계형성단계(㉯) - 공격단계(㉰) - 실행단계(㉱)

① ㉮: 인터넷, ㉯: 인물 위장, ㉰: 감정에 호소, ㉱: 도덕적 의무감 유발
② ㉮: 인터넷, ㉯: 인물 위장, ㉰: 도덕적 의무감 유발, ㉱: 감정에 호소
③ ㉮: 인물 위장, ㉯: 감정에 호소, ㉰: 인터넷, ㉱: 도덕적 의무감 유발
④ ㉮: 인물 위장, ㉯: 인터넷, ㉰: 도덕적 의무감 유발, ㉱: 감정에 호소

정답 1번

간단한 해설

정답은 ①이다. 제시된 흐름에서는 정보수집에 인터넷, 관계형성에 인물 위장, 공격에 감정 호소, 실행에 도덕적 의무감 유발을 연결한다. 핵심은 **정보 수집에서 신뢰 형성·심리적 압박·행동 유도로 이어지는 흐름**이다.

빈칸별 해설

㉮ 정보수집단계는 인터넷에 대응한다. 조직의 공개 자료나 인터넷에 노출된 정보를 통해 대상과 업무 환경을 파악하는 단계이다. 이 단계의 특징은 상대에게 행동을 요구하기 전에 관련 정보를 모은다는 점이다.

㉯ 관계형성단계는 인물 위장에 대응한다. 공격자가 상대가 신뢰할 만한 관계자처럼 신분을 꾸며 접촉하고 신뢰 관계를 형성하려는 단계이다. 신분을 주장한다는 사실만으로 믿지 않고 별도 경로로 확인해야 하는 이유가 된다.

㉰ 공격단계는 감정에 호소에 대응한다. 형성된 관계를 바탕으로 동정심·불안·긴박감 등의 심리적 반응을 유발하여 경계와 판단을 약화시키는 단계로 설명한다.

㉱ 실행단계는 도덕적 의무감 유발에 대응한다. 상대가 요청을 따라야 할 의무나 책임이 있다고 느끼도록 하여 실제 행동으로 이어지게 하는 단계로 설명한다. 정당한 업무 요청인지는 감정이나 압박이 아니라 확인된 절차에 따라 판단해야 한다.

문항의 단계별 연결은 **인터넷 → 인물 위장 → 감정에 호소 → 도덕적 의무감 유발**이므로 정답은 ①이다. 실제 공격에서는 이러한 심리 기법이 겹치거나 여러 단계에서 반복될 수 있으므로, 각 수단이 오직 한 단계에서만 사용된다는 뜻은 아니다.

NoteBase