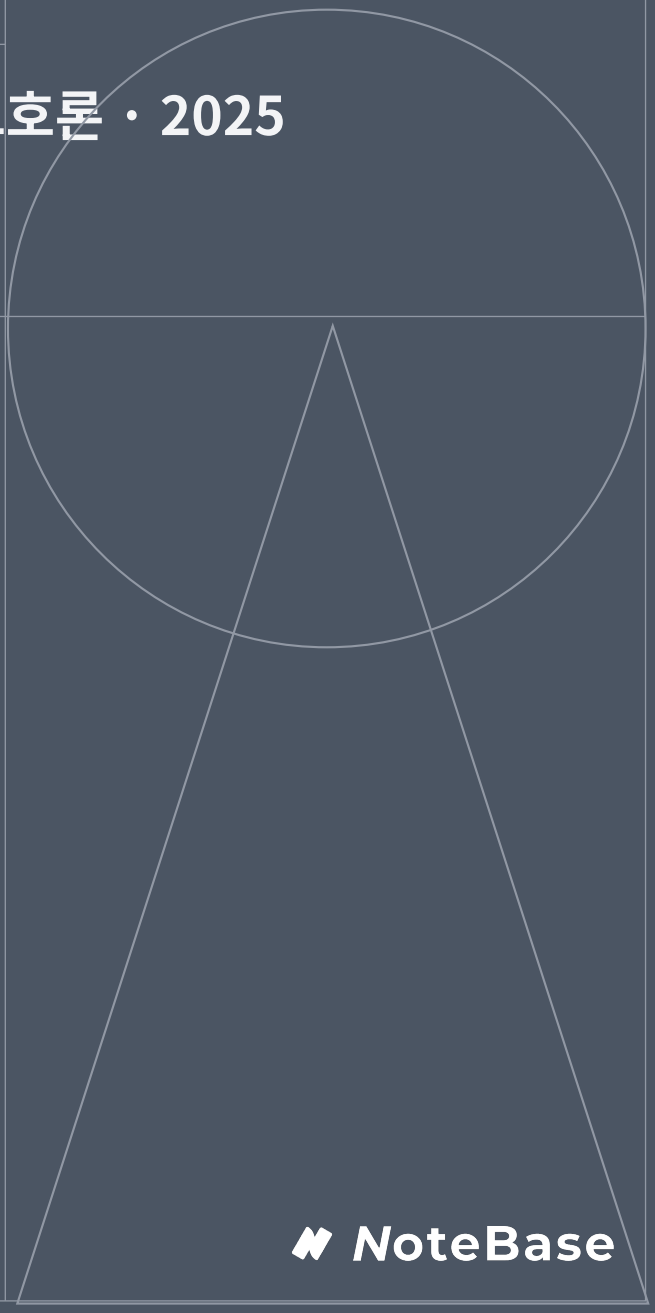
기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2025



NoteBase

기출OX 해설집

공무원/법원직/9급 · 정보보호론 · 2025

공무원/법원직/9급 · 정보보호론 · 2025

문 1. 다음 중 커버로스(Kerberos) 프로토콜에서 티켓-승인 티켓과 서비스 티켓을 구분하여 발급하는 이유로 가장 옳지 않은 것은?

① 사용자가 처음에 한 번 비밀번호로 로그인하면, 그 이후부터는 티켓-승인 티켓만을 가지고 추가 인증이 진행되도록 함으로써, 비밀번호 재사용을 막아 안전성을 높인다.

② 티켓-승인 티켓은 해당 사용자가 신원 확인을 마쳤다는 증거로, 서비스 티켓은 특정 서비스에 대해 접근 권한이 있다는 증거로 사용되어 안전성 및 유연성이 증가한다.

③ 사용자가 한 번 로그인하면, 티켓-승인 티켓으로 다양한 서비스에 추가 로그인 없이 접근할 수 있으므로 사용자 편의성이 증가한다.

④ 티켓-승인 티켓과 서비스 티켓은 각각 유효기간이 따로 설정되어 있어, 만약 서비스 티켓이 탈취되는 경우 보안 사고 대응력을 약화한다.

정답 4번

출제 포인트

커버로스에서 티켓-승인 티켓(TGT)과 서비스 티켓을 나누어 사용하는 목적이 비밀번호 노출 축소, 인증과 서비스 접근의 분리, 단일 로그인, 피해 범위 제한에 있음을 묻는 문제이다.

핵심 개념

티켓-승인 티켓(TGT): 최초 인증을 마친 사용자가 티켓 승인 서버에 특정 서비스용 티켓을 요청할 때 사용하는 티켓이다.
서비스 티켓: 사용자가 특정 서비스 서버에 접근할 때 제시하는 그 서비스 전용 티켓이다.
둘을 구분하면 최초 로그인 뒤 비밀번호를 반복해서 보내지 않으면서도 서비스별로 접근을 통제하고 티켓의 사용 범위와 유효기간을 제한할 수 있다.

NoteBase

선지별 해설

① O — 최초 인증 때 비밀번호에서 얻은 키를 이용한 뒤에는 TGT를 바탕으로 서비스 티켓을 발급받으므로, 서비스마다 비밀번호를 다시 입력하거나 전송할 필요가 줄어든다. 따라서 비밀번호 반복 사용에 따른 노출 위험을 낮춘다는 설명은 옳다.
② O — TGT는 사용자가 최초 신원 확인을 통과했음을 티켓 승인 서버에 증명하는 데 쓰이고, 서비스 티켓은 지정된 서비스에 대한 접근에 쓰인다. 인증 단계와 서비스별 접근을 분리하므로 안전성과 유연성이 높아진다.
③ O — 한 번 인증받아 TGT를 획득하면 이를 이용해 여러 서비스의 서비스 티켓을 발급받을 수 있다. 서비스마다 다시 로그인하지 않아도 되는 단일 로그인(SSO) 효과가 있으므로 사용자 편의성이 증가한다.
④ X — 틀린 표현은 '보안 사고 대응력을 약화한다'이다. 서비스 티켓은 특정 서비스와 제한된 유효기간에 묶이므로 탈취되더라도 악용 가능한 대상과 시간이 제한된다. 올바르게는 TGT와 서비스 티켓을 구분하고 각각 유효기간을 설정하면 피해 범위를 줄여 보안 사고 대응력을 강화한다고 해야 한다.

오답 포인트

④는 '티켓이 탈취될 수 있다'는 사실을 근거로 분리 발급이 보안을 약화한다고 뒤집은 선지이다. 탈취 가능성과 피해 제한 효과는 별개이며, 서비스별 티켓과 유효기간은 탈취 시 악용 범위를 제한하는 장치이다.

다시 나오면 이렇게 판단

TGT는 '서비스 티켓을 받기 위한 최초 인증의 증표', 서비스 티켓은 '특정 서비스에 제시하는 접근용 증표'로 구분한다. 비밀번호 재전송 감소, 단일 로그인, 서비스별 권한 분리, 짧은 유효기간에 따른 피해 제한은 모두 구분 발급의 장점이다.

암기 포인트

TGT로 서비스 티켓을 받고, 서비스 티켓으로 해당 서비스에 접근한다. 분리할수록 비밀번호 노출과 사고 범위가 줄어든다.

NoteBase

문 2. 보안 시스템 설계 시 참고하는 접근 제어 원칙 중 다음 <보기>에 해당하는 원칙은?

<보기>
어떤 주체가 객체에 대해서 명시적으로 접근 권한을 부여받지 않았다면, 그 주체는 객체에 대한 접근이 금지되어야 한다. 이 원칙은 또한 주체가 주어진 일을 완료하지 못하고 실패했을 때, 그 주체가 행한 변화를 초기 상태로 되돌림으로써 시스템을 안전한 상태로 유지해야 한다는 것을 의미한다.

① 직무 분리(Separation of Duties)
② 고장시 안전 초기화(Fail-Safe Default)
③ 최소 권한(Least Privilege)
④ 알 필요성(Need to Know)

정답 2번

출제 포인트

명시적으로 허용되지 않은 접근은 기본적으로 거부하고, 실패가 발생해도 시스템을 안전한 상태로 두는 고장시 안전 초기화 원칙을 다른 접근 제어 원칙과 구별하는 문제이다.

핵심 개념

고장시 안전 초기화(Fail-Safe Default)는 접근 권한의 기본값을 거부로 설정하고, 작업 실패 시에도 시스템이 안전한 상태를 유지하도록 하는 원칙이다.
직무 분리는 중요한 업무를 여러 사람이나 역할에 나누어 한 사람이 단독으로 수행하지 못하게 하는 원칙이다.
최소 권한은 주체에게 업무 수행에 꼭 필요한 최소한의 권한만 부여하는 원칙이다.
알 필요성은 업무상 필요한 정보에 한해서만 접근을 허용하는 원칙이다.

선지별 해설

① X — 직무 분리는 중요한 업무의 권한과 절차를 여러 주체에게 나누어 단독 오용을 막는 원칙이다. 보기의 '명시적으로 허용되지 않으면 접근을 금지하고 실패 시 안전한 상태로 되돌린다'를 직무 분리라고 한 부분이 틀렸으며, 올바르게는 고장시 안전 초기화이다.
② O — 명시적 허가가 없으면 접근을 거부하는 기본 거부와 실패 시 안전한 초기 상태를 유지한다는 설명은 고장시 안전 초기화에 해당한다.
③ X — 최소 권한은 업무 수행에 필요한 최소 범위의 권한만 부여하는 원칙이다. 보기의 기본 거부와 실패 시 안전 상태 유지 원칙을 최소 권한이라고 한 부분이 틀렸으며, 올바르게는 고장시 안전 초기화이다.
④ X — 알 필요성은 직무 수행에 필요한 정보만 알 수 있도록 정보 접근 범위를 제한하는 원칙이다. 보기의 기본 거부와 실패 시 안전 상태 유지 원칙을 알 필요성이라고 한 부분이 틀렸으며, 올바르게는 고장시 안전 초기화이다.

NoteBase

오답 포인트

‘권한을 받지 않으면 접근할 수 없다’는 표현만 보고 최소 권한이나 알 필요성을 고르기 쉽다. 그러나 보기에는 명시적 허가가 없을 때의 기본값이 거부라는 점과 실패 후 안전한 상태로 복귀한다는 단서가 함께 제시되어 있으므로 고장시 안전 초기화가 정답이다.

다시 나오면 이렇게 판단

‘기본적으로 거부’, ‘명시적 허가가 있어야 허용’, ‘실패하면 안전한 상태 유지·복귀’가 핵심이면 고장시 안전 초기화로 판단한다. ‘필요 최소 권한’은 최소 권한, ‘여러 사람에게 분담’은 직무 분리, ‘필요한 정보만 접근’은 알 필요성으로 구별한다.

암기 포인트

Fail-Safe Default는 기본 거부와 실패 시 안전 상태 유지이다.

NoteBase

문 3. 네트워크 보안 공격의 하나인 스니핑에 관한 다음 설명 중 가장 옳지 않은 것은?

① 스니핑은 대표적인 수동적 공격의 하나로, 송신자와 수신자가 주고받는 데이터를 중간에 도청하여 실행한다.

② 스니핑을 막기 위한 방법으로는 주고받는 데이터를 암호화하는 방법이 있으며, 웹에서는 HTTPS, 이메일에서는 PGP와 S/MIME, 원격 접속에서는 SSH와 VPN을 활용할 수 있다.

③ 스니핑을 막기 위해서는 허브 대신 스위치를 사용하고 스위치의 매핑 테이블을 정적으로 설정하는 방법이 있다.

④ 스니핑을 탐지하는 방법으로 호스트 기반 탐지 도구인 ARP watch나 네트워크 기반 탐지 도구인 ifconfig를 활용하는 방법이 있다.

정답 4번

출제 포인트

스니핑의 공격 방식과 예방·탐지 수단을 구분하고, arpwatch와 ifconfig의 탐지 위치를 정확히 연결하는 문제이다.

핵심 개념

스니핑은 네트워크를 흐르는 패킷을 몰래 수집하여 그 내용을 엿보는 대표적인 수동적 공격이다. 예방에는 통신 내용의 암호화, 스위치 사용, 스위치 매핑 테이블의 정적 설정 등이 활용된다. 탐지에서는 arpwatch가 네트워크의 ARP 주소 대응 관계 변화를 감시하고, ifconfig는 개별 호스트의 네트워크 인터페이스가 무차별 모드로 동작하는지 확인하는 데 활용된다.

선지별 해설

① O — 스니핑은 송신자와 수신자 사이의 통신 데이터를 몰래 도청하는 수동적 공격이다. 데이터를 변조하거나 서비스 동작을 방해하는 것이 주된 목적이 아니다.
② O — 통신 내용을 암호화하면 패킷을 가로채더라도 평문 내용을 알아보기 어렵다. HTTPS, PGP·S/MIME, SSH·VPN은 각각 웹, 이메일, 원격 접속·통신 구간을 보호하는 수단으로 활용된다.
③ O — 허브는 수신 프레임을 여러 포트로 전달하지만 스위치는 MAC 주소 매핑에 따라 필요한 포트로 전달하므로 단순 도청 기회를 줄인다. 매핑 테이블을 정적으로 설정하면 MAC 플러딩을 이용한 스니핑도 억제할 수 있다.
④ X — 틀린 부분은 arpwatch를 호스트 기반, ifconfig를 네트워크 기반 탐지 도구로 연결한 것이다. 올바르게는 arpwatch가 네트워크의 ARP 트래픽과 주소 대응 관계 변화를 감시하는 네트워크 기반 수단이고, ifconfig가 개별 호스트에서 인터페이스의 무차별 모드 여부를 확인하는 호스트 기반 수단이다.

NoteBase

오답 포인트

④는 도구 이름 자체가 아니라 탐지 위치를 서로 뒤바꾼 선지이다. ifconfig는 해당 명령을 실행한 호스트의 인터페이스 상태를 확인하므로 네트워크 전체를 감시하는 도구로 볼 수 없다.

다시 나오면 이렇게 판단

통신 구간의 패킷·ARP 변화를 감시하면 네트워크 기반, 특정 컴퓨터의 인터페이스 상태를 확인하면 호스트 기반으로 판단한다.

암기 포인트

arpwatch는 ARP를 네트워크에서 감시하고, ifconfig는 내 호스트의 인터페이스를 확인한다.

NoteBase

문 4. 다음 중 버퍼 오버플로 공격에 대한 대응 방법 중 스택 가드에 대한 설명에 해당하는 것은?

① 스택에서 execution 권한을 제거함으로써 스택에 로드된 공격자의 공격 코드를 실행할 수 없도록 하는 기법이다.

② 스택에 있는 ret 주소를 실행 가능한 임의의 주소로 돌려 원하는 함수를 수행하게 하는 기법이다.

③ 메모리 공격을 방어하기 위하여 주소 공간 배치를 난수화하는 기법으로, 스택, 힙, 라이브러리 등 데이터 영역의 주소 등을 난수화한다.

④ 컴파일러가 프로그램의 함수를 호출할 때, ret 앞에 canary 값을 주입하고, 함수를 종료할 때 canary 값을 변조했는지 확인하는 기법이다.

정답 4번

출제 포인트

버퍼 오버플로 대응 기법인 스택 가드, 실행 불가 스택, 주소 공간 배치 난수화(ASLR)를 구별하는 문제이다.

핵심 개념

스택 가드는 함수의 반환 주소 앞에 카나리(canary) 값을 두고, 함수가 반환되기 전에 그 값의 변조 여부를 검사하여 스택 버퍼 오버플로를 탐지하는 기법이다.
실행 불가 스택(NX/DEP)은 스택의 코드 실행 권한을 제거하고, ASLR은 스택·힙·라이브러리 등의 메모리 주소 배치를 무작위화한다.

선지별 해설

① X — 스택의 실행 권한을 제거하여 스택에 주입된 공격 코드의 실행을 막는 것은 실행 불가 스택(NX/DEP)이다. 틀린 표현은 '스택 가드에 해당한다'는 취지이며, 올바르게는 '실행 불가 스택 기법이다'이다.
② X — 반환 주소(ret)를 공격자가 원하는 실행 가능 주소로 바꾸어 함수를 실행하는 것은 반환 주소를 조작하는 공격 기법이며, 스택 가드라는 방어 기법이 아니다. 틀린 표현은 '대응 방법 중 스택 가드'라는 분류이며, 올바르게는 '버퍼 오버플로를 이용한 제어 흐름 탈취 공격 기법이다'이다.
③ X — 스택·힙·라이브러리 등의 주소를 무작위화하는 것은 주소 공간 배치 난수화(ASLR)이다. 틀린 표현은 '스택 가드에 해당한다'는 취지이며, 올바르게는 'ASLR 기법이다'이다.
④ O — 컴파일러가 반환 주소 앞에 카나리 값을 넣고 함수 종료 시 그 값의 변조 여부를 확인하는 방식은 스택 가드의 핵심 원리이다.

NoteBase

오답 포인트

①, ③, ④는 모두 메모리 공격 방어와 관련되지만 방어 지점이 다르다. ①은 실행 권한, ③은 주소 예측 가능성, ④는 반환 주소 앞 카나리 값의 무결성을 다룬다. 또한 ②는 방어가 아니라 반환 주소를 조작하는 공격이라는 점이 함정이다.

다시 나오면 이렇게 판단

카나리 삽입·변조 검사는 스택 가드, 스택 실행 금지는 NX/DEP, 주소 무작위화는 ASLR, 반환 주소 변경은 제어 흐름 탈취 공격으로 판단한다.

암기 포인트

스택 가드의 표지는 '반환 주소 앞 카나리, 반환 전 변조 검사'이다.

NoteBase

문 5. CC(Common Criteria) 인증에 관한 다음 설명 중 가장 옳지 않은 것은?

① CC 인증은 정보보호 시스템의 보안 기능 요구사항과 보증 요구 사항 평가를 위해 공통으로 제공되는 국제 평가 기준이다.

② CC 인증은 사용자의 보안 요구를 표현하기 위한 공통 평가 기준 PP(Protection Profile), 특정 제품의 보안 기능을 표현한 평가 기준 자료 ST(Security Target), 인증 및 평가의 직접적인 대상 TOE(Target Of Evaluation)으로 구성된다.

③ 각 시스템은 EAL(Evaluation Assuarance Level)로 보안 수준을 평가 받는데, 이는 5단계로 구성되어 있다.

④ CC 인증 상호인정협정 회원국은 인증서 발행국과 인증서 수용국으로 나눌 수 있는데, 대한민국은 다른 국가에서 발행된 인증서를 자국에서 인정해 주는 동시에 자국 내 국제상호인증협정에 의해 공인된 평가 및 인증기관을 보유하고 있는 인증서 발행국에 속해 있다.

정답 3번

출제 포인트

CC의 목적과 PP·ST·TOE의 관계, EAL의 단계 수, 상호인정 체계를 구분하는 문제이다.

핵심 개념

CC(Common Criteria)는 정보기술 제품·시스템의 보안 기능 요구사항과 보증 요구사항을 공통 기준으로 평가하기 위한 국제 평가 기준이다.
PP(Protection Profile)는 일정한 유형의 제품에 대해 사용자의 공통 보안 요구를 구현 방식과 독립적으로 제시한 문서이다.
ST(Security Target)는 특정 TOE가 충족할 보안 요구사항과 보안 기능을 구체화한 평가 기준 문서이다.
TOE(Target of Evaluation)는 실제 평가 대상이 되는 제품 또는 시스템과 그 범위이다.
EAL(Evaluation Assurance Level)은 평가 보증 수준을 나타내며 EAL1부터 EAL7까지 7단계로 구성된다.

선지별 해설

① O — CC는 정보보호 제품·시스템의 보안 기능 요구사항과 보증 요구사항을 공통된 기준으로 평가하기 위한 국제 평가 기준이다.
② O — PP는 사용자 관점의 공통 보안 요구를, ST는 특정 제품인 TOE의 보안 요구와 기능을 표현하며, TOE는 인증·평가의 직접적인 대상이다.
③ X — 틀린 표현은 '5단계'이다. EAL은 EAL1부터 EAL7까지 7단계이며, 단계가 높을수록 더 높은 수준의 보증을 요구한다.
④ O — CC 인증 상호인정 체계에서 인증서 발행국은 다른 회원국의 인증서를 수용할 뿐 아니라 공인된 평가·인증 체계를 통해 인증서를 발행할 수 있다. 대한민국은 이러한 인증서 발행국에 해당한다.

NoteBase

오답 포인트

③의 '5단계'가 함정이다. 보안 기능의 종류나 다른 등급 체계와 혼동하지 않고 EAL1~EAL7의 7단계라는 범위를 확인해야 한다.

다시 나오면 이렇게 판단

CC 문항에서는 문서와 대상을 먼저 구분한다. 공통 사용자 요구는 PP, 특정 제품의 보안 명세는 ST, 실제 평가 대상은 TOE이며, 보증 수준은 EAL1~EAL7이다.

암기 포인트

PP는 공통 요구, ST는 특정 TOE의 명세, TOE는 평가 대상, EAL은 1~7의 7단계이다.

NoteBase

문 6. 메시지 인증 코드(Message Authentication Code)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 메시지 인증 코드는 전자서명과 함께 데이터의 무결성을 보장하기 위한 기법의 하나이다.

② 메시지 인증 코드를 설계하는 대표적인 방법으로는 해시 함수를 이용하는 HMAC과 블록암호 운용방식의 하나인 CBC 모드를 이용하는 CBC-MAC이 있다.

③ 메시지 인증 코드를 사용하기 위해서는 별도의 다른 안전한 방법으로 키를 공유해야 한다.

④ 메시지 인증 코드는 비밀키를 소유한 사람이 메시지에 대한 MAC 값을 계산하여 공개한다면, 누구나 검증이 가능하다.

정답 4번

출제 포인트

메시지 인증 코드(MAC)의 무결성·메시지 인증 기능과 공유 비밀키에 기반한 검증 범위를 묻는 문제이다.

핵심 개념

메시지 인증 코드(MAC)는 송신자와 수신자가 공유한 비밀키와 메시지를 입력하여 짧은 인증값을 만들고, 메시지의 변조 여부와 공유키를 아는 주체가 생성했는지를 확인하는 기법이다.
MAC은 공유 비밀키 방식이므로 키를 가진 당사자만 생성·검증할 수 있다. 전자서명은 서명자의 개인키로 생성하고 공개키로 누구나 검증할 수 있다는 점에서 MAC과 다르다.

선지별 해설

① O — MAC은 메시지가 전송 중 변경되지 않았는지를 확인하여 데이터 무결성을 보장하는 대표적인 인증 기법이다. 전자서명도 무결성을 검증할 수 있다.
② O — HMAC은 해시 함수와 비밀키를 결합한 MAC이고, CBC-MAC은 블록암호의 CBC 구조를 이용하여 MAC을 구성한다.
③ O — MAC의 생성자와 검증자는 같은 비밀키를 사용하므로, 통신 전에 그 키를 별도의 안전한 방법으로 공유해야 한다.
④ X — 틀린 표현은 '누구나 검증이 가능하다'이다. 실제로는 공유 비밀키를 가진 사람만 MAC 값을 계산하고 검증할 수 있다. 누구나 공개키로 검증할 수 있는 것은 공개키 기반 전자서명의 특징이다.

오답 포인트

④는 MAC 값이 공개된다는 사실과 검증 권한까지 공개된다는 사실을 혼동하게 한다. MAC 값만 보아서는 검증할 수 없고, 검증 계산에는 공유 비밀키가 필요하다.

NoteBase

다시 나오면 이렇게 판단

‘공유 비밀키’가 나오면 MAC, ‘개인키로 서명하고 공개키로 누구나 검증’하면 전자서명으로 구분한다. MAC에서 누구나 검증할 수 있다고 하면 틀린 설명이다.

암기 포인트

MAC은 비밀키를 공유한 당사자끼리 생성·검증하고, 전자서명은 공개키로 누구나 검증한다.

NoteBase

문 7. RSA 암호의 모듈러스를 두 소수 7과 11을 곱하여 $N = 7 \times 11 = 77$로 생성하였다고 할 때, 공개키 e로 선택할 수 있는 값은?

① 6

② 15

③ 23

④ 30

정답 3번

출제 포인트

RSA에서 공개 지수 e는 오일러 피 함수 $\varphi(N)$보다 작고 $\varphi(N)$과 서로소여야 한다는 조건을 적용하는 문제이다.

조건 정리

주어진 값: $p = 7, q = 11, N = pq = 77$이다.
구해야 할 값: 공개 지수 e로 선택할 수 있는 값이다.
주의할 조건: $1 < e < \varphi(N)$이고 $\gcd(e, \varphi(N)) = 1$이어야 한다.

사용할 공식

서로 다른 두 소수의 곱 $N = pq$에 대하여
$\varphi(N) = (p - 1)(q - 1)$
이다. 공개 지수 e는 $\varphi(N)$과 서로소여야 모듈러 역원인 개인 지수 d가 존재하므로 이 조건을 사용한다.

계산 과정

1. $\varphi(77) = (7 - 1)(11 - 1) = 6 \times 10 = 60$이다.
2. 따라서 후보 값마다 60과의 최대공약수를 구한다.
3. $\gcd(6, 60) = 6, \gcd(15, 60) = 15, \gcd(23, 60) = 1, \gcd(30, 60) = 30$이다.
4. 60과 서로소인 값은 23뿐이다.

NoteBase

선지 판단

① X — 6은 60의 약수이므로 $\gcd(6, 60) = 6$이다. 틀린 표현 '6' → 올바르게는 60과 서로소인 값을 선택해야 한다.
② X — 15는 60의 약수이므로 $\gcd(15, 60) = 15$이다. 틀린 표현 '15' → 올바르게는 60과 서로소인 값을 선택해야 한다.
③ O — 23은 60과 공약수가 1뿐이므로 $\gcd(23, 60) = 1$이다. 따라서 공개 지수 e로 선택할 수 있다.
④ X — 30은 60의 약수이므로 $\gcd(30, 60) = 30$이다. 틀린 표현 '30' → 올바르게는 60과 서로소인 값을 선택해야 한다.

오답 포인트

모든 후보가 60보다 작다는 사실만 확인하면 안 된다. 공개 지수는 범위 조건뿐 아니라 $\varphi(N)$과 서로소라는 조건도 충족해야 하며, ①·②·④는 모두 60과 공약수를 가진다.

다시 나오면 이렇게 판단

두 소수 p, q가 주어지면 먼저 $\varphi(N) = (p-1)(q-1)$을 계산하고, 각 후보에 대해 $1 < e < \varphi(N)$과 $\gcd(e, \varphi(N)) = 1$을 차례로 확인한다.

암기 포인트

RSA 공개 지수 e: $1 < e < \varphi(N)$, e와 $\varphi(N)$은 서로소이다.

NoteBase

문 8. KDC(Key Distribution Center)는 교환 키의 위험을 줄이기 위해 계획된 암호체계의 부분이다. 세션 키를 포함한 Ticket을 만드는 순서로 올바르게 나열한 것은?

(A) 사용자는 파일서버에 대한 접근을 요청한다.
(B) 티켓 부여 서비스는 세션 키에 포함된 새로운 티켓을 만든다.
(C) 인증 서비스는 사용자에게 시작 티켓(Initial Ticket)을 전송한다.
(D) 사용자는 하나의 세션 키를 추출하고 티켓을 파일 서버로 전송한다.
(E) 사용자는 인증 서비스에 인증한다.

① (A) - (B) - (C) - (D) - (E)
② (C) - (A) - (B) - (D) - (E)
③ (B) - (C) - (E) - (A) - (D)
④ (E) - (C) - (A) - (B) - (D)

정답 4번

출제 포인트

KDC 기반 티켓 인증에서 사용자 인증, 시작 티켓 발급, 서버 접근 요청, 서비스 티켓 생성, 서버에 티켓 제시로 이어지는 선후관계를 묻는 문제이다.

올바른 순서

1. (E) 사용자가 인증 서비스에 인증한다. — 사용자의 신원을 먼저 확인하는 단계이다.
2. (C) 인증 서비스가 사용자에게 시작 티켓을 전송한다. — 이후 티켓 부여 서비스를 이용할 수 있는 근거를 받는 단계이다.
3. (A) 사용자가 파일 서버에 대한 접근을 요청한다. — 접근할 서비스가 정해진 뒤 해당 서버용 티켓을 요청하는 단계이다.
4. (B) 티켓 부여 서비스가 세션 키를 담은 새로운 티켓을 만든다. — 사용자와 파일 서버의 통신에 사용할 서비스 티켓을 생성하는 단계이다.
5. (D) 사용자가 세션 키를 추출하고 티켓을 파일 서버로 전송한다. — 발급받은 티켓을 실제 파일 서버에 제시하는 단계이다.

왜 이 순서: 시작 티켓은 사용자 인증의 결과이고, 파일 서버용 티켓은 서버 접근 요청의 결과이므로 (E) → (C) → (A) → (B) → (D)의 의존관계가 성립한다.

NoteBase

선지별 해설

① X — (A) 파일 서버 접근 요청을 사용자 인증보다 먼저 두고, (E) 인증을 마지막에 둔 점이 틀리다. 올바르게는 먼저 (E) 인증을 거쳐 (C) 시작 티켓을 받은 뒤 (A) 접근을 요청하며, 전체 순서는 (E) → (C) → (A) → (B) → (D)이다.
② X — (C) 시작 티켓 발급을 그 전제인 (E) 사용자 인증보다 먼저 두고, (E)를 티켓 전송 뒤에 둔 점이 틀리다. 올바르게는 (E) 인증 다음에 (C) 시작 티켓 발급이 이루어진다.
③ X — (B) 서비스 티켓 생성을 인증과 파일 서버 접근 요청보다 먼저 둔 점이 틀리다. 올바르게는 (E) 인증과 (C) 시작 티켓 발급을 거쳐 (A) 접근을 요청한 다음 (B) 서비스 티켓이 생성된다.
④ O — (E) 사용자 인증 → (C) 시작 티켓 수령 → (A) 파일 서버 접근 요청 → (B) 세션 키를 담은 새 티켓 생성 → (D) 세션 키 추출 및 파일 서버에 티켓 전송의 순서가 정확하다.

오답 포인트

시작 티켓 발급과 파일 서버용 티켓 생성을 같은 단계로 보면 순서가 뒤섞이기 쉽다. (C)의 시작 티켓은 (E) 사용자 인증 뒤에 받고, (B)의 새 티켓은 (A) 파일 서버 접근 요청 뒤에 만들어진다는 점이 핵심이다.

다시 나오면 이렇게 판단

각 단계의 산출물이 다음 단계의 입력이 되는지 확인한다. 인증해야 시작 티켓을 받고, 접근을 요청해야 해당 서버용 티켓이 만들어지며, 티켓이 만들어져야 서버에 전송할 수 있다.

암기 포인트

인증 → 시작 티켓 → 서버 요청 → 서비스 티켓 → 서버 제시의 흐름으로 기억한다.

NoteBase

문 9. 다음 중 utmp 로그와 관련 있는 명령어가 아닌 것은?

① w
② history
③ whodo
④ users

정답 2번

출제 포인트

utmp에 저장되는 현재 로그인 사용자 정보를 조회하는 명령어와 셸 명령 이력을 조회하는 history를 구별하는 문제이다.

핵심 개념

utmp는 현재 시스템에 로그인한 사용자와 로그인 세션 정보를 기록하는 파일이다. w, whodo, users는 현재 로그인 정보를 표시하므로 utmp와 관련되지만, history는 사용자가 셸에서 실행한 명령의 이력을 표시한다.

선지별 해설

① O — w는 현재 로그인한 사용자와 각 사용자의 작업 정보를 보여 주는 명령어이므로 utmp의 로그인 세션 정보와 관련된다.
② X — history는 현재 로그인 세션을 기록한 utmp를 조회하는 명령어가 아니라 셸의 명령 실행 이력을 표시하는 명령어이다. 틀린 연결은 'history → utmp'이며, 올바르게는 'history → 셸 명령 이력'이다. 따라서 utmp 로그와 관련 없는 명령어로서 정답이다.
③ O — whodo는 현재 로그인한 사용자와 그 사용자가 실행 중인 프로세스 정보를 보여 주므로 utmp의 로그인 정보와 관련된다.
④ O — users는 현재 로그인한 사용자 이름을 출력하는 명령어이므로 utmp의 현재 로그인 정보와 관련된다.

오답 포인트

history도 사용자의 활동을 기록한다는 점 때문에 로그인 로그 명령어로 착각하기 쉽다. 그러나 기록 대상이 다르다. utmp는 현재 로그인 세션을, 셸 history는 사용자가 입력한 명령을 다룬다.

다시 나오면 이렇게 판단

명령어의 출력이 '누가 현재 로그인했는가'를 보여 주면 utmp 계열로, '어떤 명령을 실행했는가'를 보여 주면 셸 history 계열로 판단한다.

NoteBase

암기 포인트

w·whodo·users는 현재 로그인 사용자, history는 셸 명령 이력이다.

NoteBase

문 10. CVE(Common Vulnerabilities and Exposures)에 관한 다음 설명 중 가장 옳지 않은 것은?

① CVE는 미국의 비영리기관인 MITRE에서 만든 소프트웨어에서 공통으로 발생하는 잠재적인 보안 약점을 분류한 체계이다.

② 취약점 번호의 체계는 CVE-(발견년도)-(취약점 번호)의 형태로 이루어져 있다.

③ CVE에 정리된 대표적인 취약점으로는 인터넷 익스플로러의 0-Day 취약점, Apache Struts2의 RCE(Remote Code Execution) 취약점 등이 있다.

④ CVE로 체계화된 취약점들은 일반적으로 설계상의 문제이므로, 운영하는 쪽에서 자체 개선하기는 힘들며, 제조사의 공식 패치에 따라 개선할 수 있다.

정답 1번

출제 포인트

이 문제는 CVE와 CWE의 역할을 구별하는 문제이다. CVE는 공개된 개별 취약점을 식별하고 목록화하며, 공통적인 약점 유형을 분류하는 체계는 CWE이다.

핵심 개념

CVE(Common Vulnerabilities and Exposures): 특정 제품에서 공개된 개별 보안 취약점에 공통 식별자를 부여하는 체계이다.
CWE(Common Weakness Enumeration): 소프트웨어·하드웨어의 설계나 구현 등에 존재하여 취약점으로 이어질 수 있는 공통 약점 유형을 분류한 체계이다.
구별 기준은 '구체적으로 발생한 취약점 사례인가'와 '그 취약점을 낳는 일반적인 약점 유형인가'이다.

선지별 해설

① X — 틀린 표현은 '소프트웨어에서 공통으로 발생하는 잠재적인 보안 약점을 분류한 체계'이다. 이는 CVE가 아니라 CWE에 해당한다. CVE는 공개된 개별 취약점을 식별하고 목록화하는 체계이다.
② O — CVE 식별자는 CVE-YYYY-일련번호 형태로 표시되며, 일련번호 부분은 네 자리 이상이므로 번호 형식에 관한 핵심 설명은 맞다. 다만 엄밀히 YYYY는 취약점의 실제 발견일을 뜻하는 것이 아니라 CVE ID가 할당된 연도를 나타내므로, '발견년도'는 시험에서 단순화한 표현이다.
③ O — 인터넷 익스플로러의 0-Day 취약점이나 Apache Struts2의 원격 코드 실행 취약점처럼 특정 제품에서 확인되어 공개된 개별 취약점은 CVE 식별·목록화 대상이 될 수 있다.
④ O — 특정 제품의 취약점은 운영자가 소스 수준에서 직접 고치기 어려운 경우가 많으므로 제조사나 개발사가 제공하는 공식 보안 패치를 적용하는 것이 대표적인 근본 대응이다. 다만 모든 CVE가 설계 문제인 것은 아니며, 패치 전에는 설정 변경이나 기능 비활성화 같은 완화 조치도 사용할 수 있다.

NoteBase

오답 포인트

①은 CVE의 영문 명칭에 Common이 들어간다는 점을 이용해 '공통 약점의 분류'라고 바꾸었다. Common은 여러 보안 도구와 기관이 같은 개별 취약점을 동일한 식별자로 지칭한다는 취지이며, 공통 약점 유형의 분류는 CWE의 역할이다.

다시 나오면 이렇게 판단

특정 제품의 실제 취약점과 CVE-YYYY-NNNN 형식의 식별자가 나오면 CVE로 판단한다. 취약점의 원인이 되는 설계·코딩상 약점 유형과 CWE-NNN 형식이 나오면 CWE로 판단한다.

암기 포인트

CVE는 개별 취약점의 번호표, CWE는 공통 약점의 분류표이다.

NoteBase

문 11. 정보보호관리체계(ISMS)에 관한 다음 설명 중 가장 옳지 않은 것은?

① ISMS의 위험 관리 절차는 일반적으로 식별 → 분석 → 평가 → 대응의 순서로 진행된다.

② 위험 분석 단계에서는 자산, 위협, 취약점 등을 기반으로 사건이 발생할 가능성과 사건이 미치는 영향을 평가한다.

③ ISMS-P는 정보보호와 개인정보보호를 통합적으로 평가하는 국제 인증 제도이다.

④ ISO/IEC 27001은 조직의 정보보호관리체계 수립, 실행, 유지, 개선을 위한 국제 표준으로서 일반적인 정보보호를 다룬다.

정답 3번

출제 포인트

정보보호관리체계의 위험 관리 절차와 ISMS-P·ISO/IEC 27001의 성격을 구분하는 문제이다.

핵심 개념

위험 관리는 위험을 식별하고 분석·평가한 뒤 적절한 대응 방안을 정하는 과정이다.
ISMS-P는 정보보호와 개인정보보호를 통합해 심사하는 국내 인증 제도이다. 반면 ISO/IEC 27001은 조직의 정보보호관리체계에 관한 요구사항을 정한 국제 표준이다.

선지별 해설

① O — 위험 관리는 일반적으로 위험 식별, 위험 분석, 위험 평가, 위험 대응의 흐름으로 진행된다. 먼저 위험 요인을 찾아내고, 그 크기와 수용 가능성을 판단한 뒤 대응한다.
② O — 위험 분석은 자산에 대한 위협과 취약점을 살펴 위험 사건의 발생 가능성과 발생 시 영향을 파악하는 단계이다. 이 두 요소를 바탕으로 위험 수준을 판단한다.
③ X — 틀린 표현은 '국제 인증 제도'이다. ISMS-P는 정보보호 및 개인정보보호를 위한 조치와 활동이 인증기준에 적합한지를 KISA 또는 지정 인증기관이 심사·증명하는 국내 인증 제도이다. 올바르게는 'ISMS-P는 정보보호와 개인정보보호를 통합적으로 평가하는 국내 인증 제도이다'라고 해야 한다.
④ O — ISO/IEC 27001은 조직이 정보보호관리체계를 수립·실행·유지하고 지속적으로 개선하기 위한 요구사항을 규정한 국제 표준이다. 특정 산업에만 한정되지 않고 일반적인 정보보호 위험 관리를 다룬다.

오답 포인트

③은 '통합 인증'이라는 말 때문에 국제 표준으로 오인하기 쉽다. 여기서 통합은 정보보호와 개인정보보호를 하나의 인증체계로 결합했다는 뜻이며, 국제 인증이라는 뜻이 아니다. 국제 표준에 해당하는 것은 ISO/IEC 27001이다.

NoteBase

다시 나오면 이렇게 판단

명칭의 운영 주체와 적용 범위를 구분한다. ISMS-P는 국내의 정보보호·개인정보보호 통합 인증이고, ISO/IEC 27001은 국제 정보보호관리체계 표준이다. 위험 관리 순서는 식별 → 분석 → 평가 → 대응으로 판단한다.

암기 포인트

ISMS-P는 국내 통합 인증, ISO/IEC 27001은 국제 ISMS 표준이다.

NoteBase

문 12. 리눅스의 권한 설정에 관한 다음 설명 중 가장 옳지 않은 것은?

① 파일의 접근 권한을 파일을 만든 소유자 권한, 소유자가 속한 소유 그룹 권한, 그 외 사용자 권한으로 나눠서 관리한다.

② 기본적으로 명령어를 실행시킨 사용자 ID를 체크하여 실행 권한이 있으면 명령어를 수행한다.

③ 명령어를 실행시킨 사용자 ID에게 실행 권한이 없으면 SetUID, SetGID, Sticky bit가 설정되어 있는지를 확인한다.

④ Sticky bit가 설정된 디렉터리 내에서는 타인이 생성한 파일도 일반 사용자가 삭제할 수 있다.

정답 4번

출제 포인트

리눅스의 소유자·그룹·그 외 사용자 권한과 특수 권한 비트, 특히 디렉터리에 설정된 Sticky bit의 기능을 구분하는 문제이다.

핵심 개념

일반 접근 권한: 파일과 디렉터리의 읽기·쓰기·실행 권한을 소유자(user), 소유 그룹(group), 그 외 사용자(other)로 나누어 관리한다.
SetUID·SetGID: 실행 파일에 설정되면 프로세스가 각각 파일 소유자 또는 소유 그룹의 유효 권한으로 실행되게 하는 특수 권한이다.
Sticky bit: 공동 쓰기가 가능한 디렉터리에서 파일의 삭제·이름 변경을 파일 소유자, 디렉터리 소유자, 관리자 등으로 제한하여 다른 사용자의 파일을 보호하는 특수 권한이다.

선지별 해설

① O — 리눅스는 접근 권한을 파일 소유자, 소유 그룹, 그 외 사용자의 세 범주로 나누어 관리한다.
② O — 명령 실행 시에는 실행 주체의 유효 사용자 ID와 파일의 소유 관계 및 실행 권한 비트를 대조하여 실행 가능 여부를 판단한다.
③ O — 권한 검사에서는 명령을 실행한 사용자의 ID와 일반 실행 권한을 확인하고 파일 모드의 SetUID·SetGID·Sticky bit 같은 특수 권한 비트의 설정 상태도 확인한다. SetUID·SetGID는 실행 파일의 소유자·소유 그룹을 기준으로 프로세스의 유효 ID를 정하며, Sticky bit는 현대 리눅스에서 주로 디렉터리 안 항목의 삭제·이름 변경을 제한한다.
④ X — 틀린 표현은 '타인이 생성한 파일도 일반 사용자가 삭제할 수 있다'이다. 올바르게는 Sticky bit가 설정된 디렉터리에서는 일반 사용자가 타인이 소유한 파일을 임의로 삭제하거나 이름을 바꿀 수 없고, 원칙적으로 파일 소유자·디렉터리 소유자·관리자만 이를 할 수 있다.

NoteBase

오답 포인트

Sticky bit를 '삭제 권한을 부여하는 비트'로 반대로 이해하기 쉽다. Sticky bit는 여러 사용자가 쓰는 디렉터리에서 타인의 파일을 지우지 못하게 제한하는 보호 장치이다.

다시 나오면 이렇게 판단

SetUID는 실행 시 소유자 권한, SetGID는 실행 시 소유 그룹 권한, 디렉터리의 Sticky bit는 타인 소유 파일의 삭제·이름 변경 제한으로 연결하여 판단한다.

암기 포인트

Sticky는 붙잡아 둔다. 공동 디렉터리에서도 남의 파일은 함부로 삭제하지 못한다.

NoteBase

문 13. 블록암호 AES(Advanced Encryption Standard)에 관한 다음 설명 중 가장 옳지 않은 것은?

① AES는 128비트의 평문을 128비트의 암호문으로 암호화한다.

② AES의 키의 크기는 128, 192, 256비트 3가지로 설정이 가능하다.

③ AES는 키의 크기에 따라 12, 14, 16라운드를 갖는다.

④ 암호화 과정에서 AES의 각 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey의 순서로 수행되지만, 마지막 라운드에서는 MixColumns를 수행하지 않는다.

정답 3번

출제 포인트

AES의 블록 크기, 지원 키 길이, 키 길이별 라운드 수, 각 라운드의 변환 순서를 구별하는 문제이다.

핵심 개념

AES는 128비트 블록을 암호화하는 대칭키 블록암호이다. 키 길이는 128비트, 192비트, 256비트이고, 이에 대응하는 라운드 수는 각각 10회, 12회, 14회이다. 일반 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey로 구성되며 마지막 라운드에서는 MixColumns가 제외된다.

선지별 해설

① O — AES의 블록 크기는 키 길이와 관계없이 128비트이므로 128비트 평문 블록을 128비트 암호문 블록으로 변환한다.
② O — AES가 지원하는 키 길이는 128비트, 192비트, 256비트의 세 가지이다.
③ X — 틀린 부분은 '12, 14, 16라운드'이다. 올바르게는 키 길이 128비트, 192비트, 256비트에 따라 각각 10라운드, 12라운드, 14라운드를 수행한다.
④ O — 일반 라운드의 변환 순서는 SubBytes → ShiftRows → MixColumns → AddRoundKey이고, 마지막 라운드에서는 MixColumns를 수행하지 않는다.

오답 포인트

③은 키 길이가 64비트씩 늘어나는 것처럼 라운드 수도 단순히 2회씩 더한 뒤 시작값을 12회로 잘못 제시한 선지이다. AES의 라운드 수는 10·12·14로 기억해야 한다. 또한 128비트는 고정된 블록 크기이고 128·192·256비트는 선택 가능한 키 길이라는 점을 혼동하기 쉽다.

다시 나오면 이렇게 판단

AES 문항에서는 먼저 블록 크기 128비트와 키 길이 128·192·256비트를 분리하고, 키 길이별 라운드 수를 10·12·14로 대응시킨다. 라운드 구조를 물으면 마지막 라운드에서 MixColumns가 빠지는지를 확인한다.

NoteBase

암기 포인트

AES는 블록 128, 키 128·192·256, 라운드 10·12·14이며 마지막에는 MixColumns가 없다.

NoteBase

문 14. DES에 관한 다음 설명 중 가장 옳지 않은 것은?

① 64비트 평문을 64비트의 암호문으로 변환시키고, 16라운드 구조로 이루어져 있다.

② 라운드함수에서 특히 S-Box는 confusion을 구현하는 기능을 갖고 있다.

③ 키는 보통 패러티비트들을 포함하여 48비트로 표현하지만 실제 키길이는 56비트이다.

④ Double DES는 중간가로채기공격으로 인해 쓰이지 않는 메커니즘이다.

정답 3번

출제 포인트

DES의 블록 크기, 라운드 구조, S-Box의 기능, 키 길이와 Double DES의 취약점을 구분하는 문제이다.

핵심 개념

DES는 64비트 블록을 56비트 유효 키로 암호화하는 16라운드 페이스텔 구조의 대칭키 블록 암호이다. 외부에 표현되는 키는 패리티 비트 8개를 포함한 64비트이고, 각 라운드에 투입되는 서브키는 48비트이다. S-Box는 비선형 치환으로 혼돈(confusion)을 제공하며, Double DES는 중간 일치 공격에 취약하다.

선지별 해설

① O — DES는 64비트 평문 블록을 64비트 암호문 블록으로 변환하며 총 16라운드를 수행한다.
② O — 라운드 함수의 S-Box는 비선형 치환을 수행하여 키와 암호문 사이의 관계를 복잡하게 만드는 혼돈(confusion)을 구현한다.
③ X — 틀린 표현은 '패리티비트들을 포함하여 48비트'이다. DES 키는 패리티 비트 8개를 포함하면 64비트로 표현되고 실제 암호화에 쓰이는 유효 키 길이는 56비트이다. 48비트는 각 라운드에서 사용하는 서브키의 길이이다.
④ O — Double DES는 두 번의 DES 연산 사이에 존재하는 중간값을 양쪽에서 대조하는 중간 일치 공격에 취약하여 기대한 만큼 키 공간을 늘리지 못하므로 실용적인 강화 방식으로 쓰이지 않는다.

오답 포인트

③은 DES에 등장하는 64비트, 56비트, 48비트를 뒤섞은 선지이다. 64비트는 패리티를 포함한 키 표현 길이, 56비트는 유효 키 길이, 48비트는 라운드 서브키 길이이다.

다시 나오면 이렇게 판단

DES의 수치는 '블록 64비트, 표현 키 64비트, 유효 키 56비트, 라운드 키 48비트, 16라운드'로 역할과 함께 구분한다. S-Box는 혼돈, Double DES는 중간 일치 공격과 연결한다.

NoteBase

암기 포인트

DES는 블록 64·유효 키 56·서브키 48·16라운드이며, S-Box는 혼돈이고 Double DES는 중간 일치 공격에 취약하다.

NoteBase

문 15. 스푸핑 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

① ARP 스푸핑 공격은 MAC 주소를 속이는 것이다.

② IP 스푸핑 공격을 막기 위해 중요 접속 서버의 URL에 대한 IP를 hosts 파일에 등록하면 된다.

③ ICMP 리다이렉트 공격은 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격이다.

④ DNS 스푸핑 공격은 실제 DNS 서버보다 빠르게 공격 대상에게 DNS Response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.

정답 2번

출제 포인트

ARP·IP·ICMP 리다이렉트·DNS 스푸핑이 각각 어떤 주소나 경로 정보를 속이는지 구별하는 문제이다.

핵심 개념

스푸핑은 공격자가 주소나 신원 정보를 위조하여 자신을 정상 장치나 시스템처럼 보이게 하는 공격이다.
ARP 스푸핑은 IP 주소와 MAC 주소의 대응 관계를 조작하고, IP 스푸핑은 IP 패킷의 출발지 IP 주소를 위조한다.
ICMP 리다이렉트 공격은 거짓 경로 변경 정보를 보내 패킷의 흐름을 바꾸며, DNS 스푸핑은 도메인 이름에 잘못된 IP 주소가 대응되도록 만든다.

선지별 해설

① O — ARP 스푸핑은 위조된 ARP 정보를 보내 특정 IP 주소에 공격자의 MAC 주소가 대응되도록 ARP 캐시를 오염시키는 공격이다. 따라서 MAC 주소를 속인다는 설명은 옳다.
② X — 틀린 부분은 hosts 파일 등록을 IP 스푸핑의 대응책으로 본 것이다. hosts 파일에 도메인과 올바른 IP 주소의 대응 관계를 고정하면 DNS 질의 결과의 변조를 우회할 수 있으므로 DNS 스푸핑 대응에 해당한다. IP 스푸핑은 패킷의 출발지 IP 주소를 위조하는 공격이므로 출발지 주소 필터링, 패킷 인증 등의 방식으로 대응한다.
③ O — 공격자가 위조된 ICMP Redirect 메시지를 보내 자신을 더 적절한 라우터인 것처럼 알리면 피해 시스템의 경로가 변경되어 패킷이 공격자가 원하는 경로로 흐를 수 있다.
④ O — DNS는 같은 질의에 대해 먼저 도착한 정상 형식의 응답을 받아들일 수 있다. 공격자가 실제 DNS 서버보다 먼저 위조 응답을 보내면 피해자는 도메인을 잘못된 IP 주소로 해석하여 공격자가 유도한 웹 사이트에 접속할 수 있다.

오답 포인트

②는 URL과 IP 주소의 대응 관계가 등장하므로 IP 스푸핑처럼 보이지만, hosts 파일이 대신하는 것은 DNS의 이름 해석 기능이다. IP 주소가 문장에 있다는 이유만으로 IP 스푸핑 대응책으로 판단하면 안 된다.

다시 나오면 이렇게 판단

속이는 대상을 기준으로 구분한다. ARP는 IP-MAC 대응 관계, IP 스푸핑은 출발지 IP, ICMP Redirect는 라우팅 경로, DNS는 도메인-IP 대응 관계를 속인다.

암기 포인트

ARP는 MAC 대응, IP는 출발지 주소, Redirect는 경로, DNS는 이름과 IP의 대응을 속인다.

NoteBase

문 16. 무선 랜 프로토콜에 관한 다음 설명 중 가장 옳은 것은?

① 802.11b는 와이파이(Wi-Fi)라고 하며, WEP 방식의 보안을 구현한다.

② 802.11a는 802.11b의 속도를 개선한 프로토콜로, 802.11b와 호환되지만 네트워크 공유 시 데이터 처리의 효율이 현격히 떨어진다.

③ 802.11i는 여러 안테나를 사용하는 다중입력/다중출력(MIMO) 기술로 대역폭을 최소화하고 최대 속도는 600Mbps이다.

④ 802.11ac는 최대속도 7Gbps이고, 기존 2.5GHz/5GHz 대신 60GHz 대역을 사용하여 전송하는 방식이며, 대용량 데이터나 높은 비트레이트 동영상 스트리밍에 적합하다.

정답 1번

출제 포인트

IEEE 802.11 무선 LAN 규격별 주파수 대역, 전송 속도, 호환성, 보안 기술을 구별하는 문제이다.

핵심 개념

802.11b: 2.4GHz 대역을 사용하며 최대 11Mbps를 지원하는 초기 Wi-Fi 규격이다. WEP 보안 방식을 지원한다.
802.11a: 5GHz 대역에서 최대 54Mbps를 지원하며, 주파수 대역이 다른 802.11b와 직접 호환되지 않는다.
802.11i: 무선 LAN 보안을 강화한 규격으로, AES 기반 CCMP를 사용하는 WPA2의 기술적 토대이다.
802.11n: MIMO와 채널 결합을 사용하며 이론상 최대 600Mbps를 지원한다.
802.11ac: 5GHz 대역에서 넓은 채널과 다중 사용자 MIMO 등을 이용하는 고속 규격이다. 60GHz 대역 규격은 802.11ad이다.

선지별 해설

① O — 802.11b는 초기 Wi-Fi 규격으로 WEP 보안 방식을 지원하므로 이 문항에서 가장 옳은 설명이다.
② X — 틀린 표현은 '802.11b와 호환된다'이다. 802.11a는 5GHz, 802.11b는 2.4GHz 대역을 사용하므로 서로 직접 호환되지 않는다. 혼합 운용 시 저속 단말 때문에 효율이 떨어질 수 있다는 설명은 802.11b와 호환되는 802.11g의 특성과 관련된다.
③ X — 틀린 표현은 '802.11i는 MIMO 기술이며 최대 속도는 600Mbps'이다. 802.11i는 WPA2와 관련된 보안 강화 규격이다. MIMO를 사용하고 이론상 최대 600Mbps를 지원하는 규격은 802.11n이다.
④ X — 틀린 표현은 '802.11ac가 60GHz 대역을 사용한다'이다. 802.11ac는 5GHz 대역을 사용하며 이론상 최고 속도는 약 6.9Gbps이다. 60GHz 대역을 사용하는 규격은 802.11ad이고, 기존 무선 LAN 대역은 2.5GHz가 아니라 2.4GHz와 5GHz이다.

NoteBase

오답 포인트

③은 802.11n의 MIMO·600Mbps 특징을 보안 규격인 802.11i에 붙였고, ④는 802.11ac의 고속 전송 특징에 802.11ad의 60GHz 대역을 섞었다. 서로 다른 규격의 일부 특징을 결합한 선지를 주의해야 한다.

다시 나오면 이렇게 판단

규격을 '주파수 대역-핵심 기술-최대 속도-보안'의 네 축으로 나누어 판단한다. i는 보안, n은 MIMO·600Mbps, ac는 5GHz 고속화, ad는 60GHz로 연결하면 혼합 선지를 구별할 수 있다.

암기 포인트

i는 보안, n은 MIMO·600Mbps, ac는 5GHz, ad는 60GHz이다.

NoteBase

문 17. 다음 중 주로 시스템 자원(예: 메모리, CPU, 디스크 등)이나 네트워크 대역폭을 빠르게 소모시켜 과부하를 일으키는 것을 목표로 하지 않고, 서버의 동시 연결 수를 소진시켜 정상 사용자가 접속하지 못하게 만드는 것을 목표로 하는 공격은?

① HTTP Get Flooding 공격

② Slowloris 공격

③ Ping of Death 공격

④ Smurf 공격

정답 2번

출제 포인트

대량 트래픽으로 자원을 빠르게 소모하는 공격과 불완전한 HTTP 연결을 오래 유지하여 서버의 동시 연결 수를 소진하는 공격을 구별하는 문제이다.

핵심 개념

Slowloris는 HTTP 요청 헤더를 완성하지 않은 채 조금씩 전송하여 여러 연결을 장시간 유지하고, 서버가 수용할 수 있는 동시 연결을 소진시키는 저속 애플리케이션 계층 DoS 공격이다.
HTTP GET Flooding은 다량의 정상 형태 GET 요청을 보내 처리 자원을 소모시키고, Ping of Death는 비정상적으로 큰 ICMP 패킷의 재조립 과정에서 장애를 유발하며, Smurf는 브로드캐스트와 출발지 주소 위조를 이용해 ICMP 응답 트래픽을 피해자에게 증폭·집중시킨다.

선지별 해설

① X — HTTP GET Flooding 공격은 많은 GET 요청을 집중시켜 서버의 처리 능력과 네트워크 자원을 소모시키는 공격이다. 틀린 연결은 '동시 연결 수를 불완전한 요청으로 소진한다'는 특징이며, 올바르게는 Slowloris의 특징이다.
② O — Slowloris 공격은 완성되지 않은 HTTP 요청을 다수 열어 둔 채 연결을 오래 유지함으로써 서버의 동시 연결 한도를 소진하여 정상 사용자의 접속을 막는다.
③ X — Ping of Death 공격은 허용 크기를 넘는 비정상 ICMP 패킷을 조각내 전송하고, 대상이 이를 재조립할 때 오류나 장애를 일으키는 공격이다. 동시 HTTP 연결을 장시간 점유하는 공격이 아니라 Slowloris가 이에 해당한다.
④ X — Smurf 공격은 피해자의 IP 주소를 출발지로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답을 피해자에게 집중시키는 증폭 공격이다. 동시 연결 수 소진이 아니라 증폭된 응답 트래픽으로 대역폭과 자원을 고갈시키는 방식이다.

NoteBase

오답 포인트

모두 서비스 거부 공격이지만 공격 수단이 다르다. 특히 '빠르게 자원을 소모시키지 않고', '동시 연결 수를 소진한다'는 문구가 Slowloris를 가리킨다. GET Flooding의 대량 요청과 Slowloris의 느리고 불완전한 요청을 혼동하기 쉽다.

다시 나오면 이렇게 판단

불완전한 HTTP 요청을 천천히 보내 연결을 오래 붙잡으면 Slowloris, 대량 GET 요청이면 HTTP GET Flooding, 비정상 대형 ICMP 패킷이면 Ping of Death, 브로드캐스트를 이용한 ICMP 증폭이면 Smurf로 판단한다.

암기 포인트

Slowloris는 '느리게 요청하고, 연결은 오래 점유한다'로 기억한다.

NoteBase

문 18. 포맷 스트링 공격에 관한 다음 설명 중 가장 옳지 않은 것은?

① 포맷 지정자를 악용하여 메모리 내용을 유출하거나 조작하는 공격 방법이다.

② C언어 계열에서 printf()와 같은 출력 함수에 사용자 입력을 포맷 문자열로 직접 전달할 때 발생할 수 있다.

③ 컴파일 시점에 발생하며, 실행 시에는 영향을 미치지 않는다.

④ 공격을 방지하기 위해서는 사용자 입력을 포맷 문자열로 받지 않고, 명시적인 서식 지정자를 사용하도록 한다.

정답 3번

출제 포인트

포맷 스트링 취약점의 발생 조건과 실행 시 영향, 안전한 출력 함수 사용법을 묻는 문제이다.

핵심 개념

포맷 스트링 공격은 외부 입력이 출력 함수의 서식 문자열로 해석될 때 공격자가 포맷 지정자를 이용하여 메모리를 읽거나 쓸 수 있는 공격이다. 핵심은 사용자 입력을 데이터가 아니라 서식 문자열로 직접 전달하는 데 있다. 예를 들어 printf(user_input) 대신 printf("%s", user_input)처럼 서식을 고정하고 사용자 입력은 인수로 전달해야 한다.

선지별 해설

① O — 포맷 지정자는 함수가 추가 인수를 읽거나 특정 위치에 값을 기록하도록 지시할 수 있으므로, 이를 악용하면 메모리 정보 유출이나 메모리 조작이 가능하다.
② O — C언어 계열에서 printf(user_input)처럼 신뢰할 수 없는 입력을 포맷 문자열 자리에 직접 넣으면 입력 속의 포맷 지정자가 실행되어 취약점이 발생할 수 있다.
③ X — 틀린 표현은 '컴파일 시점에 발생하며, 실행 시에는 영향을 미치지 않는다'이다. 실제로는 프로그램 실행 중 출력 함수가 공격자의 포맷 문자열을 해석할 때 발생하며, 정보 유출·메모리 변조·비정상 종료 등의 영향을 줄 수 있다.
④ O — printf("%s", user_input)처럼 명시적인 서식 지정자를 사용하고 사용자 입력을 데이터 인수로 전달하면 입력 자체가 포맷 문자열로 해석되는 것을 막을 수 있다.

오답 포인트

③은 소스 코드에 위험한 함수 호출 방식이 작성되어 있다는 점과 취약점이 실제로 발현되는 시점을 혼동하게 만든다. 취약한 코드는 컴파일될 수 있지만, 공격은 실행 시 출력 함수가 악성 포맷 지정자를 해석하면서 성립한다.

NoteBase

다시 나오면 이렇게 판단

출력 함수의 첫 번째 인수가 고정된 서식 문자열인지 확인한다. 외부 입력이 그 자리에 직접 들어가면 포맷 스트링 취약점이고, 고정 서식의 데이터 인수로 들어가면 입력이 포맷 지정자로 해석되지 않는다.

암기 포인트

포맷 스트링 공격은 실행 시 발생한다. 서식은 고정하고 입력은 데이터로 전달한다.

NoteBase

문 19. 다음 LLM(Large Language Model, 대형언어모델)에 대한 공격 중 기존 LLM의 콘텐츠 제한 정책을 우회하는 프롬프트를 생성하여 LLM이 의도하지 않은 작업을 실행하도록 유도하는 공격은?

① 프롬프트 인젝션(Prompt Injection)
② 부적절한 출력 처리(Improper Output Handling)
③ 시스템 프롬프트 노출(System Prompt Leakage)
④ 허위 정보(Misinformation)

정답 1번

출제 포인트

콘텐츠 제한을 우회하는 악성 프롬프트로 LLM의 지시 체계를 교란하는 공격과, 출력 처리·정보 노출·허위 정보 문제를 구별하는 문항이다.

핵심 개념

프롬프트 인젝션은 공격자가 조작한 입력을 이용하여 LLM이 원래의 지시나 제한을 무시하고 의도하지 않은 응답 또는 작업을 수행하도록 유도하는 공격이다. 콘텐츠 제한 정책을 우회하도록 만든 프롬프트는 이 개념에 해당한다.
부적절한 출력 처리는 LLM이 생성한 출력을 후속 시스템이 충분히 검증하거나 정제하지 않고 사용하는 문제이다. 시스템 프롬프트 노출은 모델의 내부 지시문이 외부에 드러나는 문제이고, 허위 정보는 모델이 사실과 다른 내용을 생성하는 문제이다.

선지별 해설

① O — 프롬프트 인젝션은 조작된 프롬프트로 기존 지시나 콘텐츠 제한을 우회하여 LLM이 의도하지 않은 작업을 수행하게 만드는 공격이므로 지문의 설명과 일치한다.
② X — 틀린 부분은 '부적절한 출력 처리'이다. 이는 공격 프롬프트로 모델의 제한을 우회하는 것이 아니라, LLM의 출력을 검증·정제하지 않은 채 후속 코드나 시스템에서 사용하여 문제가 발생하는 취약점이다. 올바르게는 지문의 공격을 '프롬프트 인젝션'이라고 한다.
③ X — 틀린 부분은 '시스템 프롬프트 노출'이다. 이는 LLM에 설정된 내부 지시문이나 비공개 설정 내용이 사용자에게 드러나는 현상이다. 올바르게는 제한 우회 프롬프트로 의도하지 않은 작업을 유도하는 공격을 '프롬프트 인젝션'이라고 한다.
④ X — 틀린 부분은 '허위 정보'이다. 이는 LLM이 사실과 다르거나 근거가 부족한 내용을 생성하는 문제이다. 올바르게는 악성 입력으로 모델의 지시와 제한을 우회하는 공격을 '프롬프트 인젝션'이라고 한다.

NoteBase

오답 포인트

‘의도하지 않은 결과’라는 공통점만 보고 출력 처리 문제나 허위 정보로 판단하기 쉽다. 이 문항의 결정적 표현은 ‘콘텐츠 제한 정책을 우회하는 프롬프트를 생성’한다는 부분이며, 공격 수단이 프롬프트 자체이므로 프롬프트 인젝션이다.

다시 나오면 이렇게 판단

공격이 어디에 작용하는지 구분한다. 입력 프롬프트가 지시를 교란하면 프롬프트 인젝션, 생성된 출력의 검증·정제가 부족하면 부적절한 출력 처리, 내부 지시문이 드러나면 시스템 프롬프트 노출, 사실과 다른 내용이 생성되면 허위 정보이다.

암기 포인트

입력으로 지시를 교란하면 인젝션, 출력 검증이 부족하면 부적절한 출력 처리, 내부 지시가 보이면 시스템 프롬프트 노출이다.

NoteBase

문 20. 호스트 기반 침입탐지 시스템(HIDS, Host-based Intrusion Detection System)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 특정 호스트의 로그, 파일 무결성, 시스템 콜 등을 분석하여 침입 여부를 탐지한다.

② 개별 시스템에 설치하므로, 네트워크 전체의 트래픽 흐름을 중앙에서 분석하는 데 효과적이다.

③ 루트킷 탐지, 파일 변경 감시, 비정상 프로세스 탐지 등에 효과적이다.

④ 운영체제에 가까운 수준에서 동작하며, 내부자의 이상 행위 탐지에 유리하다.

정답 2번

출제 포인트

이 문제는 개별 호스트의 내부 활동을 감시하는 HIDS와 네트워크 구간의 트래픽을 감시하는 NIDS의 탐지 범위를 구별하는 문제이다.

핵심 개념

HIDS는 서버나 PC 같은 개별 호스트에 설치되어 그 호스트의 로그, 파일, 프로세스, 시스템 콜 등 내부 활동을 분석하는 침입탐지 시스템이다.
HIDS는 호스트 내부 정보가 핵심이고, NIDS는 네트워크 구간을 지나는 패킷과 트래픽 흐름이 핵심이다.

선지별 해설

① O — 특정 호스트의 로그와 파일 무결성, 시스템 콜은 HIDS가 수집·분석하는 대표적인 호스트 내부 정보이다.
② X — 틀린 부분은 '네트워크 전체의 트래픽 흐름을 중앙에서 분석하는 데 효과적이다'이다. HIDS는 개별 호스트의 내부 활동 분석에 적합하며, 네트워크 전체의 트래픽을 중앙에서 분석하는 역할은 주로 NIDS가 수행한다.
③ O — HIDS는 호스트 내부의 파일 변경, 비정상 프로세스와 시스템 상태를 관찰할 수 있으므로 루트킷 징후나 무단 변경 탐지에 효과적이다.
④ O — HIDS는 운영체제와 호스트 내부의 세부 행위를 관찰하므로 네트워크 트래픽만으로 드러나기 어려운 내부자의 비정상 행위를 탐지하는 데 유리하다.

오답 포인트

②는 '개별 시스템에 설치한다'는 앞부분은 맞지만, 뒤에서 NIDS의 기능인 네트워크 전체 트래픽 분석을 HIDS의 특징처럼 연결한 선지이다. 한 선지 안에서 앞부분과 뒷부분의 개념이 바뀌는 점이 함정이다.

다시 나오면 이렇게 판단

로그·파일·프로세스·시스템 콜처럼 호스트 안에서 발생하는 정보이면 HIDS로, 패킷·세션·네트워크 구간의 전체 트래픽이면 NIDS로 판단한다.

NoteBase

암기 포인트

HIDS는 호스트 내부, NIDS는 네트워크 흐름이다.

NoteBase

문 21. 서비스거부공격(DoS)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 분산서비스공격(DDoS)도 DoS공격의 일종이다.

② Boink, Bonk 공격은 프로토콜의 오류 제어 로직을 악용하여 시스템자원을 고갈시키는 방식이다.

③ TearDrop 공격은 패킷 전송 시 출발지 IP 주소와 목적지 IP 주소를 동일하게 만들어 공격 대상에게 보내는 공격이다.

④ 라우터에서 다이렉트 브로드캐스트를 막는 형태로 Smurf 공격에 대응할 수 있다.

정답 3번

출제 포인트

DoS 공격의 대표 유형별 공격 원리와 대응 방법을 구별하는 문제이다.

핵심 개념

DoS는 시스템이나 네트워크의 자원을 고갈시켜 정상 사용자의 서비스 이용을 방해하는 공격이다.
DDoS는 여러 공격원이 동시에 수행하는 분산형 DoS이고, TearDrop은 IP 조각의 오프셋을 조작하여 재조립 오류를 일으키는 공격이다.
Land는 출발지 IP 주소와 목적지 IP 주소를 공격 대상의 주소로 동일하게 설정하는 공격이며, Smurf는 피해자의 주소로 출발지를 위조한 ICMP 요청을 브로드캐스트 주소에 보내 응답을 피해자에게 집중시키는 공격이다.

선지별 해설

① O
DDoS는 다수의 분산된 공격원이 공격 대상의 자원을 고갈시키는 방식이므로 DoS 공격의 일종이다.

② O
Boink와 Bonk는 비정상적으로 조작된 패킷 조각을 보내 프로토콜의 오류 처리·재조립 과정에 부담을 주고 시스템 자원을 고갈시키는 DoS 공격이다.

③ X
틀린 표현은 ‘TearDrop 공격은 출발지 IP 주소와 목적지 IP 주소를 동일하게 만든다’이다. 이는 Land 공격의 방식이다. 올바르게는 TearDrop 공격은 IP 단편의 오프셋 값을 조작하여 조각들이 겹치게 하고, 패킷 재조립 과정에서 오류나 자원 고갈을 일으키는 공격이다.

④ O
Smurf 공격은 IP 다이렉트 브로드캐스트를 증폭 수단으로 이용한다. 라우터에서 다이렉트 브로드캐스트 전달을 차단하면 외부의 요청이 내부 전체 호스트로 확산되는 것을 막을 수 있다.

NoteBase

오답 포인트

③은 TearDrop과 Land의 공격 원리를 바꾸어 제시한 선지이다. ‘출발지와 목적지 IP 주소가 동일’하면 Land이고, ‘IP 조각의 오프셋 조작과 중첩’이면 TearDrop이다.

다시 나오면 이렇게 판단

공격 이름을 패킷의 어느 필드를 어떻게 조작하는지와 연결한다. IP 주소를 동일하게 설정하면 Land, 단편 오프셋을 조작하면 TearDrop, 브로드캐스트와 ICMP 응답을 증폭하면 Smurf로 판단한다.

암기 포인트

Land는 같은 IP 주소, TearDrop은 겹치는 조각, Smurf는 브로드캐스트 증폭이다.

NoteBase

문 22. 위험관리에 관한 다음 설명 중 가장 옳은 것은?

① 위험에는 인위적 위험과 자연적 위험이 존재하며, 인위적 위험에는 고의적 위험과 우발적 위험이 있다.

② 위험분석에서 연간손실예상액(ALE)는 어떤 위험이 한 번 발생했을 때 예상되는 손실을 의미하며, 1회손실예상액(SLE)과 연간발생빈도(ARO)의 합으로 구할 수 있다.

③ 영향이란 보안사고가 자산에 미치는 원인을 말한다.

④ 취약성 분석은 환경과 기존의 보안대책을 고려하여 현존하는 위험의 공격대상이 될 수 있는 자산의 강점을 검사하는 것이다.

정답 1번

출제 포인트

위험의 분류와 위험분석의 핵심 용어인 ALE, SLE, ARO, 영향, 취약성의 뜻을 구별하는 문제이다.

핵심 개념

위험은 발생 원인에 따라 자연적 위험과 인위적 위험으로 나눌 수 있고, 인위적 위험은 행위자의 의도 여부에 따라 고의적 위험과 우발적 위험으로 구분한다.
SLE는 사고가 한 번 발생했을 때의 예상 손실액이고, ARO는 그 사고의 연간 예상 발생 횟수이며, ALE는 1년 동안 예상되는 손실액이다. 관계식은 $ALE = SLE \times ARO$이다.
영향은 보안사고가 자산에 초래하는 결과이고, 취약성은 위협이 악용할 수 있는 자산이나 보호대책의 약점이다.

선지별 해설

① O — 위험에는 자연현상에서 비롯되는 자연적 위험과 사람의 행위에서 비롯되는 인위적 위험이 있다. 인위적 위험은 해킹처럼 의도적으로 일으키는 고의적 위험과 실수·오조작처럼 의도하지 않은 우발적 위험으로 구분할 수 있다.
② X — '한 번 발생했을 때 예상되는 손실'과 'SLE와 ARO의 합'이 틀린 표현이다. 한 번의 사고로 예상되는 손실은 SLE이고, 연간손실예상액은 SLE와 ARO를 곱한 $ALE = SLE \times ARO$로 구한다.
③ X — '자산에 미치는 원인'이 틀린 표현이다. 영향은 보안사고가 자산의 가치, 업무, 기밀성·무결성·가용성 등에 미치는 결과 또는 피해를 말한다.
④ X — '자산의 강점'이 틀린 표현이다. 취약성 분석은 환경과 기존 보안대책을 고려하여 위협이 악용할 수 있는 자산이나 보호대책의 약점을 찾아 평가하는 것이다.

오답 포인트

②는 SLE와 ALE의 정의를 바꾸고 곱셈식을 합으로 바꾼 이중 함정이다. ③은 영향이라는 결과를 원인으로, ④는 취약성이라는 약점을 강점으로 뒤집었다.

NoteBase

다시 나오면 이렇게 판단

위험관리 용어는 '원인-약점-결과-손실액'의 역할을 나누어 판단한다. 위협은 사고를 일으킬 수 있는 원인, 취약성은 악용 가능한 약점, 영향은 사고의 결과이며, 연간 손실은 1회 손실에 연간 발생빈도를 곱한 값이다.

암기 포인트

인위적 위험은 고의·우발, 취약성은 약점, 영향은 결과, ALE는 SLE×ARO이다.

NoteBase

문 23. SYN Flood에 관한 다음 설명 중 가장 옳은 것은?

① 네트워크를 통해 데이터를 주고받기 위해 세워진 프로토콜의 허점을 이용한 DoS 공격방식 중 하나이다.

② TCP/IP의 취약성을 이용한 서비스 거부 공격 방식 중 하나로 SYN 공격은 대상시스템에 간헐적인 SYN 패킷을 보내는 공격이다.

③ 공격을 막는 근본적인 방법은 존재하지 않으나, 백 로그 큐를 줄이고 대기 상태를 늘리는 방법으로 해결할 수 있다.

④ 해당 공격이 외부의 정당한 접속을 방해하는 것은 아니다.

정답 1번

출제 포인트

TCP 3-way handshake의 연결 대기 구조를 악용하는 SYN Flood의 원리와 대응 방향을 묻는 문제이다.

핵심 개념

SYN Flood는 공격자가 다량의 SYN 패킷을 보내고 연결 설정을 완료하지 않아 서버의 반개방 연결 자원과 백로그 큐를 소진시키는 서비스 거부 공격이다. 정상적인 TCP 연결은 SYN → SYN/ACK → ACK의 3단계를 완료하지만, SYN Flood에서는 마지막 ACK가 오지 않아 서버가 SYN_RECEIVED 상태로 응답을 기다리게 된다.

선지별 해설

① O — TCP 연결 설정 프로토콜의 동작 특성, 즉 SYN 요청을 받으면 서버가 연결 정보를 일정 시간 보관하는 점을 악용하는 DoS 공격이므로 옳다.
② X — 틀린 표현은 '간헐적인 SYN 패킷'이다. 실제로는 대상 시스템의 연결 대기 자원을 고갈시키기 위해 다량의 SYN 패킷을 집중적으로 보내고 연결을 완료하지 않는 공격이다.
③ X — 틀린 표현은 '백로그 큐를 줄이고 대기 상태를 늘리는'이다. 실제 대응 방향은 백로그 큐의 수용량을 늘리고 반개방 연결의 대기 시간을 줄이는 것이며, SYN cookie나 비정상 SYN 트래픽 차단도 활용할 수 있다.
④ X — 틀린 표현은 '외부의 정당한 접속을 방해하는 것은 아니다'이다. SYN Flood는 반개방 연결로 서버의 대기 자원을 소진시켜 정상 사용자의 새 연결을 받아들이지 못하게 한다.

오답 포인트

②의 '간헐적', ③의 '큐를 줄이고 대기를 늘림', ④의 '정상 접속을 방해하지 않음'은 모두 공격의 자원 고갈 원리와 반대되는 표현이다. 특히 ③은 대응 방향을 정확히 거꾸로 제시한 함정이다.

NoteBase

다시 나오면 이렇게 판단

SYN Flood 선지는 '다량의 SYN 전송 → 마지막 ACK 미전송 → 반개방 연결 누적 → 백로그 큐 고갈 → 정상 접속 방해'의 흐름과 일치하는지 판단한다. 방어책은 반개방 연결이 오래·많이 쌓이지 않도록 하는 방향인지 확인한다.

암기 포인트

SYN은 보내고 ACK는 끝내지 않는다. 그 결과 반개방 연결이 쌓여 정상 접속이 막힌다.

NoteBase

문 24. 다음 대칭키 알고리즘 운영 모드 중에서 평문을 블록 단위로 나누고, 각 블록이 독립적으로 암호화되기 때문에 패턴 노출 등 보안성이 약한 운영 모드에 해당하는 것은?

① ECB

② CTR

③ CFB

④ OFB

정답 1번

출제 포인트

평문 블록을 서로 연계하지 않고 독립적으로 암호화하여 동일한 평문 블록의 패턴이 드러나는 운용 모드를 구별하는 문제이다.

핵심 개념

ECB는 각 평문 블록을 같은 키로 독립 암호화하는 모드이다. 같은 평문 블록은 같은 암호문 블록이 되므로 반복 패턴이 노출될 수 있다.
CTR은 서로 다른 카운터 값을 암호화하여 만든 키스트림과 평문을 XOR하는 모드이다.
CFB는 앞에서 생성된 암호문 블록을 다음 암호화 입력에 되먹임하는 모드이다.
OFB는 암호 알고리즘의 이전 출력값을 다음 입력에 되먹임하여 키스트림을 만드는 모드이다.

선지별 해설

① O — ECB는 평문 블록을 각각 독립적으로 암호화한다. 따라서 같은 평문 블록이 반복되면 같은 암호문 블록이 반복되어 원문의 구조나 패턴이 드러날 수 있다.
② X — 이 특징에 해당하는 모드가 CTR이라는 판단이 틀리다. CTR은 블록마다 서로 다른 카운터 값을 암호화해 키스트림을 만들고 이를 평문과 XOR하므로, 카운터를 중복 사용하지 않으면 같은 평문 블록도 위치에 따라 다른 암호문이 된다.
③ X — 이 특징에 해당하는 모드가 CFB라는 판단이 틀리다. CFB는 이전 암호문을 다음 단계에 되먹임하므로 각 블록을 서로 무관하게 직접 암호화하는 ECB 방식이 아니다.
④ X — 이 특징에 해당하는 모드가 OFB라는 판단이 틀리다. OFB는 이전 암호 알고리즘 출력값을 되먹임하여 키스트림을 만들고 평문과 XOR하는 방식이며, 평문 블록 자체를 독립적으로 직접 암호화하는 ECB 방식이 아니다.

NoteBase

오답 포인트

CTR도 블록별 처리가 가능하다는 점 때문에 ECB와 혼동하기 쉽다. 그러나 판단 기준은 병렬 처리 가능 여부가 아니라 동일한 평문 블록이 동일한 암호문 블록으로 그대로 대응하는지이다. 이런 결정적 패턴 노출은 ECB의 약점이다.

다시 나오면 이렇게 판단

문제에서 '블록 간 연계 없음', '각 블록 독립 암호화', '동일 평문은 동일 암호문', '패턴 노출'이 함께 제시되면 ECB로 판단한다. 카운터는 CTR, 암호문 되먹임은 CFB, 출력값 되먹임은 OFB로 구별한다.

암기 포인트

ECB는 블록을 따로 암호화하므로 같은 평문은 같은 암호문이 되고 패턴이 보인다.

NoteBase

문 25. 다음 중 IPSec의 구성 요소가 아닌 것은?

① 키 교환 및 관리(Key Exchange & Management)

② 보안 연계(Security Association)

③ 에이전트 보안(Agent Security)

④ 보안 프로토콜(Security Protocol)

정답 3번

출제 포인트

IPsec을 이루는 보안 프로토콜, 보안 연계, 키 관리 요소를 구별하는 문제이다.

핵심 개념

IPsec은 IP 계층에서 통신을 보호하는 보안 체계이다. AH·ESP와 같은 보안 프로토콜이 실제 보호 기능을 제공하고, 보안 연계(SA)가 통신에 적용할 보안 매개변수를 정하며, 키 교환 및 관리 기능이 필요한 키와 SA 설정을 지원한다. 에이전트 보안은 이러한 IPsec의 구성요소에 해당하지 않는다.

선지별 해설

① O — 키 교환 및 관리는 통신 당사자가 암호 키를 교환하고 IPsec 보안 연계를 설정·관리하도록 지원하므로 IPsec의 구성요소이다.
② O — 보안 연계(Security Association)는 사용할 보안 프로토콜, 알고리즘, 키 등의 보안 매개변수를 정하는 단방향 논리적 연결이므로 IPsec의 핵심 구성요소이다.
③ X — 에이전트 보안(Agent Security)은 IPsec의 구성요소가 아니다. 틀린 표현은 '에이전트 보안'이며, IPsec의 구성요소로는 보안 프로토콜, 보안 연계, 키 교환 및 관리 등이 제시된다.
④ O — 보안 프로토콜은 IP 패킷에 인증·무결성 또는 기밀성 보호를 적용하며, 대표적으로 AH와 ESP가 있으므로 IPsec의 구성요소이다.

오답 포인트

③의 '에이전트 보안'은 보안과 관련된 일반적인 표현처럼 보이지만 IPsec 구조의 표준 구성요소 명칭이 아니다. 반면 키 관리, SA, AH·ESP 보안 프로토콜은 서로 역할이 다르면서도 모두 IPsec 체계를 구성한다.

다시 나오면 이렇게 판단

IPsec 구성요소를 묻는 경우 '어떻게 보호하는가'는 AH·ESP, '어떤 조건으로 보호하는가'는 SA, '키와 SA를 어떻게 마련하는가'는 키 교환·관리로 연결한다. 이 세 역할에 들어맞지 않는 용어를 비구성요소로 판단한다.

NoteBase

암기 포인트

IPsec은 보안 프로토콜(AH·ESP) + 보안 연계(SA) + 키 관리이다. 에이전트 보안은 제외된다.

NoteBase