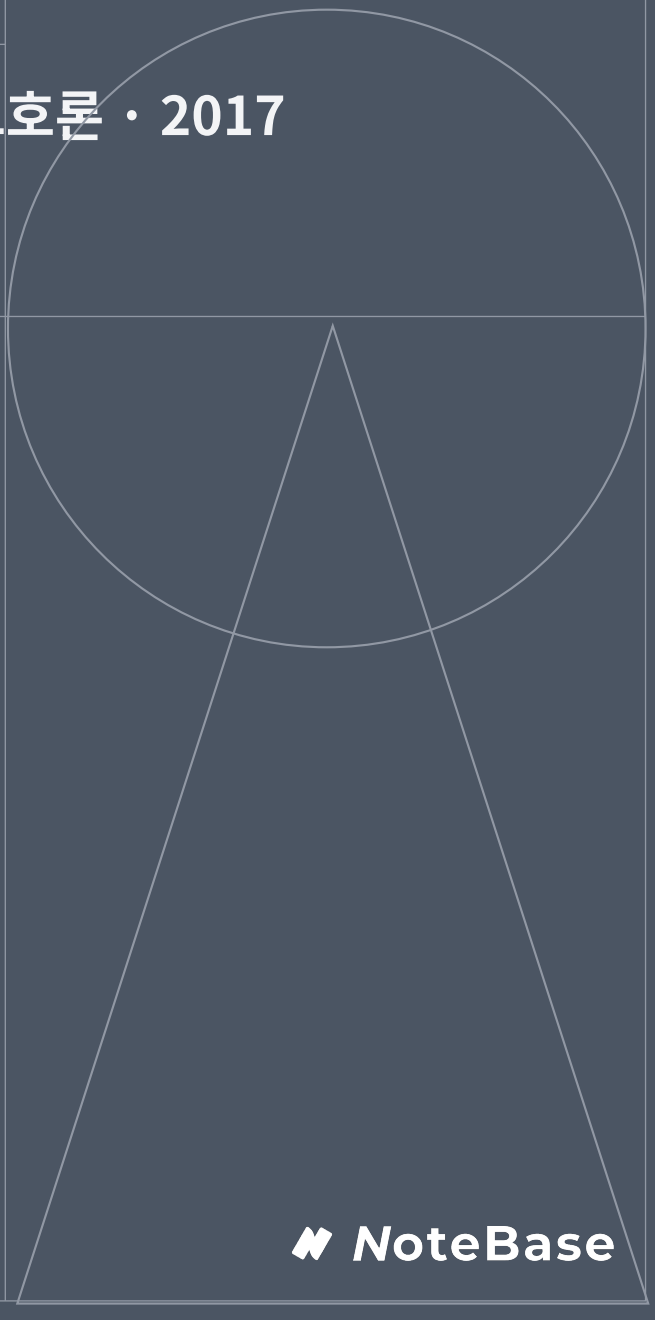
기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2017

공무원/서울시/9급 · 정보보호론 · 2017

문 1. 다음의 지문은 무엇을 설명한 것인가?

ㄱ. 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심 거래를 탐지하고 이상금융거래를 차단하는 시스템이다.
ㄴ. 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치를 할 수 있도록 지원하는 시스템이다.

① MDM
② FDS
③ MDC
④ RPO

정답 2번

간단한 해설

단말기·접속 정보와 거래 내용을 종합하여 **의심 거래를 탐지하고 대응**하는 것은 FDS의 기능이다. FDS는 보안 프로그램만으로 막지 못한 전자금융사기를 거래 분석을 통해 탐지하도록 지원한다.

공통 해설

FDS(Fraud Detection System)는 **이상금융거래 탐지시스템**이다. 전자금융거래에 이용되는 단말기 정보, 접속 정보, 거래 내용 등을 함께 분석하여 부정 사용이 의심되는 거래를 찾아내고, 거래 차단 등 필요한 조치를 지원한다. 판단의 핵심은 **여러 정보를 종합한 거래의 이상 징후 분석**이다.

ㄱ은 FDS가 분석하는 정보와 의심 거래의 탐지·차단 기능을 설명한다. ㄴ은 보안 프로그램이 방지하지 못한 전자금융사기도 거래 분석으로 탐지하여 대응을 지원한다는 역할을 설명한다. 두 설명은 모두 FDS의 기능에 해당한다.

NoteBase

문 2. 다음 중 APT(Advanced Persistent Threat) 공격에 대한 설명 중 옳지 않은 것은?

① 사회 공학적 방법을 사용한다.

② 공격대상이 명확하다.

③ 가능한 방법을 총동원한다.

④ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.

정답 4번

간단한 해설

APT 공격은 **명확한 목적과 동기**를 가지고 특정 대상을 장기간 지속적으로 공격한다. 따라서 '불분명한 목적과 동기'라는 설명은 APT의 표적성과 지속성을 잘못 설명한 것이다.

선지별 해설

① O: 사회 공학은 사람의 신뢰나 심리적 약점을 이용하여 정보 제공이나 특정 행동을 유도하는 기법이다. APT 공격자는 **특정인을 겨냥한 스피어 피싱** 등을 이용한다. 예를 들어 업무 메일로 위장한 악성 첨부파일을 보내 직원이 열도록 유도하여 침투 기회를 얻는다.

② O: APT는 **특정 기관·기업 등 명확한 표적**을 정하고 공격한다. 대상 조직의 정보와 보안 환경을 조사한 뒤 목적 달성에 필요한 시스템이나 정보에 접근하려 하므로, 공격대상이 명확하다는 설명이 적절하다.

③ O: APT 공격자는 목적 달성을 위해 **여러 공격 수단을 복합적으로 활용**한다. 사회 공학, 악성코드, 취약점 악용 등을 결합하고 방어 조치에 맞추어 수법을 바꾼다. '가능한 방법을 총동원한다'는 이러한 수단의 다양성을 뜻하며, 모든 공격에서 모든 기법을 반드시 사용한다는 뜻은 아니다.

④ X: APT 공격자는 정보 탈취나 업무 방해 등 **명확한 목적과 동기**를 가지고 조직적으로 활동한다. 목표 달성을 위해 대상 내부의 접근 기반을 확보하고 장기간 유지하려 하므로, '불분명한 목적과 동기'는 '명확한 목적과 동기'로 고쳐야 한다.

NoteBase

문 3. 다음 중 메시지 인증 코드(MAC : Message Authentification Code)에 대한 설명 중 옳은 것은?

① 메시지 무결성을 제공하지는 못한다.

② 비대칭키를 이용한다.

③ MAC는 가변 크기의 인증 태그를 생성한다.

④ 부인 방지를 제공하지 않는다.

정답 4번

간단한 해설

MAC는 송신자와 수신자가 **같은 비밀키를 공유**하므로 수신자도 인증 태그를 만들 수 있다. 따라서 태그만으로 송신자가 보냈다는 사실을 제3자에게 입증하는 **부인 방지는 제공하지 않는다**.

선지별 해설

① X: MAC는 **메시지 무결성을 제공한다**. 송신자가 메시지와 비밀키로 인증 태그를 생성하면, 수신자는 받은 메시지와 같은 키로 태그를 다시 계산해 전달받은 태그와 비교한다. 이 과정으로 전송 중 메시지가 변조되었는지 확인할 수 있다.

② X: MAC는 비대칭키가 아니라 **공유 비밀키를 이용하는 대칭키 방식**이다. 송신자는 이 키로 태그를 생성하고, 수신자는 같은 키로 검증한다. 송신자의 개인키와 그에 대응하는 공개키를 사용하는 전자서명과 구별된다.

③ X: MAC는 가변 길이의 메시지를 입력받아 **정해진 길이의 인증 태그**를 생성한다. 같은 알고리즘과 출력 길이 설정을 사용하면 메시지가 길어져도 태그의 길이가 함께 늘어나지는 않는다. 가변 길이인 입력 메시지와 정해진 길이인 출력 태그를 구별해야 한다.

④ O: 부인 방지는 송신자가 나중에 메시지를 보냈다는 사실을 부정하지 못하도록 입증하는 성질이다.
MAC에서는 송신자와 수신자가 비밀키를 공유하므로 **수신자도 유효한 태그를 생성할 수 있다**. 따라서 제3자는 태그만으로 두 사람 중 누가 메시지를 생성했는지 구별할 수 없어, MAC 자체는 부인 방지를 제공하지 않는다.

NoteBase

문 4. 다음 중 데이터베이스 관리자(Database Administrator)가 부여할 수 있는 SQL기반 접근권한 관리 명령어로 옳지 않은 것은?

① REVOKE

② GRANT

③ DENY

④ DROP

정답 4번

간단한 해설

DROP은 **테이블 등 데이터베이스 객체 자체를 삭제**하는 명령어이다. 사용자에게 허용할 작업을 정하는 접근권한 관리 명령어와는 구별된다.

공통 해설

접근권한 관리는 사용자나 역할이 데이터베이스 객체에 대해 어떤 작업을 할 수 있는지 정하는 것이다. 이 기준에서 GRANT는 권한을 부여하고, REVOKE는 기존의 권한 부여를 취소하며, SQL Server 등의 DENY는 권한을 명시적으로 거부한다. 모두 **객체에 대한 사용자의 권한을 설정·변경**하는 명령어이다. SQL Server에서 REVOKE는 기존의 거부 설정을 취소할 때도 사용된다.

DROP은 **데이터베이스 객체 자체를 삭제**하는 명령어로, 접근권한 관리에 해당하지 않는다. 예를 들어 DROP TABLE은 테이블의 정의와 데이터를 제거한다. 사용자의 테이블 조회 권한을 REVOKE로 회수해도 테이블 자체는 유지된다는 점에서 차이가 있다.

NoteBase

문 5. 스위칭 환경에서 스니핑(Sniffing)을 수행하기 위한 공격으로 옳지 않은 것은?

① ARP 스푸핑(Spoofing)

② ICMP 리다이렉트(Redirect)

③ 메일 봄(Mail Bomb)

④ 스위치 재밍(Switch Jamming)

정답 3번

간단한 해설

메일 봄은 대량의 전자우편으로 메일함이나 서버의 자원을 소모시키는 **서비스 거부 공격**이다. 다른 호스트의 통신을 공격자에게 유도하거나 노출시켜 엿듣게 하는 스니핑 수단과는 목적과 작동 방식이 다르다.

선지별 해설

① O: ARP 스푸핑은 거짓 ARP 정보를 보내 피해 호스트의 **IP 주소와 MAC 주소의 대응 관계를 조작**한다. 예를 들어 게이트웨이의 IP 주소에 공격자의 MAC 주소를 대응시키면, 피해 호스트가 게이트웨이로 보내려던 프레임이 공격자에게 전달된다. 공격자는 이를 수집하고 실제 게이트웨이로 중계하여 통신을 엿들을 수 있다.

② O: ICMP 리다이렉트는 호스트에 특정 목적지로 가는 더 적절한 다음 홉을 알려 주는 기능이다. 공격자가 이를 위조하고 피해 호스트가 받아들이면 **공격자를 다음 홉으로 사용**하도록 경로를 바꿀 수 있다. 이후 공격자를 거쳐 가는 패킷을 수집할 수 있으므로 스위칭 환경의 스니핑에 이용된다.

③ X: 메일 봄은 대량의 메일을 보내 메일함의 저장 공간이나 메일 서버의 처리 자원 등을 소모시키는 공격이다. 그 결과 정상적인 메일 이용을 어렵게 하므로 **가용성을 해치는 서비스 거부 공격**에 해당한다. 통신 경로나 스위치의 전달 동작을 조작해 다른 호스트의 패킷을 엿듣게 하는 공격은 아니다.

④ O: 스위치 재밍은 다수의 서로 다른 출발지 MAC 주소를 가진 프레임으로 스위치의 MAC 주소 테이블(CAM 테이블)을 포화시키는 방식이다. 정상적인 MAC 주소를 학습하지 못하면 **목적지 MAC 주소를 모르는 유니캐스트 프레임**이 같은 VLAN의 수신 포트를 제외한 전달 가능한 포트들로 플러딩될 수 있다. 공격자는 자신의 포트에도 전달되는 이 프레임을 수집하여 스니핑할 수 있다.

NoteBase

문 6. 다음의 지문은 무엇을 설명한 것인가?

안전한 소프트웨어 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 보안 활동이다.

① 시큐어코딩(Secure Coding)
② 스캐빈징(Scavenging)
③ 웨어하우스(Warehouse)
④ 살라미(Salami)

정답 1번

간단한 해설

소스코드의 보안 취약점을 제거하고 설계·구현 단계부터 보안을 고려하는 활동은 **시큐어코딩**이다. 개발 과정에서 취약점이 생기지 않도록 예방한다는 점이 핵심이다.

공통 해설

시큐어코딩(Secure Coding)은 안전한 소프트웨어를 만들기 위해 **개발 과정에서 보안 취약점을 예방하고 제거**하는 활동이다. 기능이 정상적으로 동작하는지만 확인하는 데 그치지 않고, 악의적인 입력이나 사용 방식에도 안전하도록 설계하고 소스코드를 작성한다.

예를 들어 외부에서 받은 입력을 그대로 처리하지 않고 허용된 형식과 길이인지 검사하도록 구현하는 것이 이에 해당한다. 지문의 취약점 제거와 보안을 고려한 설계·구현은 모두 이러한 개발 단계의 보안 활동이므로 시큐어코딩을 설명한다.

NoteBase

문 7. 다음은 TCSEC 보안등급 중 하나를 설명한 것이다. 이에 해당하는 것은?

· 각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다.
· 보안감사가 가능하며 특정 사용자의 접근을 거부할 수 있다.
· 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 이에 해당한다.

① C1
② C2
③ B1
④ B2

정답 2번

간단한 해설

계정별 로그인으로 사용자를 식별하고, **개인별 접근 통제와 보안감사**로 사용자의 행위를 추적하는 것은 C2의 특징이다. 그룹 단위의 권한 설정에 더해 특정 사용자 한 명의 접근도 제한할 수 있다.

공통 해설

TCSEC의 C2는 '통제된 접근 보호(Controlled Access Protection)' 등급이다. 임의적 접근통제를 통해 사용자나 그룹별로 파일 등의 자원에 대한 접근 권한을 설정하며, **개별 사용자 단위로 접근을 허용하거나 거부**할 수 있어야 한다. 또한 각 사용자를 식별·인증하고 보안 관련 행위를 감사기록으로 남겨, 누가 어떤 행위를 했는지 추적할 수 있게 한다. 이러한 개인별 통제와 책임추적성은 C1보다 강화된 C2의 핵심 특징이다.

지문의 '각 계정별 로그인'은 사용자 식별·인증에, '그룹 ID에 따라 통제'와 '특정 사용자의 접근을 거부'는 세분화된 접근통제에 해당한다. 여기에 **보안감사를 통한 행위 추적**까지 제시되어 있으므로, 이 설명은 C2의 통제된 접근 보호에 대응한다.

NoteBase

문 8. 다음 중 백도어(BackDoor) 공격으로 옳지 않은 것은?

① 넷버스(Netbus)

② 백오리피스(Back Orifice)

③ 무차별(Brute Force) 공격

④ 루트킷(RootKit)

정답 3번

간단한 해설

무차별 공격은 비밀번호나 암호키의 후보를 **반복 대입하여 맞는 값을 찾는 공격**이다. 정상적인 인증 절차를 우회하는 숨겨진 접근 통로인 백도어와 구별된다.

공통 해설

백도어는 **정상적인 인증 절차를 우회**하여 시스템에 접근할 수 있게 하는 숨겨진 통로이다. 이 문항에서는 이러한 통로를 제공하거나 은폐·유지하는 도구와, 비밀번호 등을 알아내려는 공격을 구별한다.

넷버스(Netbus)와 백오리피스(Back Orifice)는 대상 컴퓨터에 설치되어 공격자의 원격 접근과 제어를 가능하게 하는 백도어 도구이다.

루트킷(RootKit)은 악성 프로그램이나 침입 활동을 숨기는 도구 모음으로, **백도어를 은폐하고 비인가 접근을 유지**하는 데 이용될 수 있다. 루트킷의 핵심 기능은 은폐이므로 백도어 자체와 완전히 같은 뜻은 아니다.

무차별(Brute Force) 공격은 가능한 비밀번호나 암호키 후보를 반복적으로 대입하여 일치하는 값을 찾는 방식이다. 숨겨진 접근 통로를 만드는 것이 아니라 **인증정보나 암호키를 알아내는 방식**이므로 백도어 공격에 해당하지 않는다.

NoteBase

문 9. 다음 지문에서 설명하는 방화벽으로 옳은 것은?

ㄱ. 다단계 보안을 제공하기 때문에 강력한 보안을 제공한다.
ㄴ. DMZ(DeMilitarization Zone)라는 완충 지역 개념을 이용한다.
ㄷ. 설치와 관리가 어렵고 서비스 속도가 느리다는 단점이 있다.

① 베스천 호스트(Bastion host)
② 듀얼 홈드 게이트웨이(Dual homed gateway)
③ 패킷 필터링(Packet filtering)
④ 스크린드 서브넷 게이트웨이(Screened subnet gateway)

정답 4번

간단한 해설

DMZ라는 별도 완충망을 두고 외부망과 내부망 사이의 접근을 여러 단계로 통제하는 방식이 스크린드 서브넷 게이트웨이이다. DMZ의 서버가 침해되더라도 내부망으로 접근하려면 추가 보안 통제를 거쳐야 한다.

NoteBase

공통 해설

스크린드 서브넷 게이트웨이는 **외부망과 내부망 사이에 DMZ를 분리하여 두는** 방화벽 구성이다. 전형적으로 외부망 쪽과 내부망 쪽에 각각 패킷 필터링 라우터를 두고, 그 사이 DMZ에 베스천 호스트나 외부 공개용 서버를 배치한다. 외부망에서 DMZ로의 접근과 DMZ에서 내부망으로의 접근을 각각 통제한다.

ㄱ의 다단계 보안은 이러한 방어 계층을 뜻한다. 외부 공개 서버가 공격받더라도 **내부망 쪽의 별도 통제를 통과해야** 내부 시스템에 접근할 수 있으므로, 한 계층의 침해가 곧바로 내부망 침해로 이어질 위험을 줄인다.

ㄴ의 DMZ는 외부에 서비스를 제공하면서 내부망을 분리해 보호하는 완충망이다.

ㄷ은 여러 장비의 접근 규칙을 일관되게 설정하고 관리해야 하며, 통신이 여러 검사 단계를 거치면서 처리 부담과 지연이 생길 수 있다는 단점이다. 다만 **실제 서비스 속도는 장비 성능과 검사 방식에 따라 달라지므로**, 모든 구성에서 반드시 느리다는 뜻은 아니다.

베스천 호스트는 이 구조 안에 배치될 수 있는 보안 강화 호스트이고,

듀얼 홈드 게이트웨이는 두 네트워크 인터페이스를 가진 호스트를 중심으로 망을 연결·통제하는 구성이다.

패킷 필터링은 패킷의 주소·포트 등에 따라 통과 여부를 정하는 기법이다.

이들 명칭만으로는 지문의 '별도 DMZ를 둔 다단계 방어 구조'를 나타내지 않으며, 그 구조를 가리키는 명칭이 스크린드 서브넷 게이트웨이이다.

NoteBase

문 10. 포렌식의 기본 원칙 중 증거는 획득되고, 이송/분석/보관/법정 제출의 과정이 명확해야 함을 말하는 원칙은?

① 정당성의 원칙

② 재현의 원칙

③ 연계 보관성의 원칙

④ 신속성의 원칙

정답 3번

간단한 해설

증거의 획득부터 법정 제출까지 **누가 언제 증거를 취급하고 인계했는지** 추적할 수 있어야 한다는 것이 연계 보관성의 원칙이다. 증거의 관리 이력이 끊기지 않도록 기록하는 데 핵심이 있다.

공통 해설

연계 보관성의 원칙은 증거의 획득·이송·분석·보관·법정 제출에 이르는 **관리 이력을 연속적으로 기록하고 추적할 수 있어야 한다**는 원칙이다. 이를 위해 증거를 취급한 사람, 취급·인계 시각, 인계 목적 등을 기록한다. 문제의 '과정이 명확해야 한다'는 것은 이러한 증거의 이동과 취급 경로가 확인되어야 한다는 뜻이다.

예를 들어 수집자가 저장매체를 분석자에게 넘기고 분석 후 보관 담당자에게 인계했다면, 각 인계의 담당자와 시각을 기록하여 보관 경로를 이어 주어야 한다. 이 기록은 법정에 제출된 증거가 처음 획득한 증거와 어떻게 연결되는지 확인하고, 부당한 교체나 취급이 있었는지 검토하는 근거가 된다.

NoteBase

문 11. 다음 <보기>가 설명하는 접근제어방식은?

<보기>
주체나 그것이 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 자원의 소유자 혹은 관리자가 보안관리자의 개입 없이 자율적 판단에 따라 접근 권한을 다른 사용자에게 부여하는 기법이다.

① RBAC

② DAC

③ MAC

④ LBAC

정답 2번

간단한 해설

사용자나 그룹의 신원을 기준으로 접근을 제한하면서, **소유자나 관리자의 재량으로 접근 권한을 부여**하는 방식이 임의적 접근제어(DAC)이다.

공통 해설

임의적 접근제어(DAC, Discretionary Access Control)는 사용자나 그룹의 신원을 기준으로 객체에 대한 접근을 제한하며, 자원 소유자나 관리자가 자신의 판단으로 다른 사용자에게 접근 권한을 부여하는 방식이다. 여기서 '임의적'은 누구나 자유롭게 접근한다는 뜻이 아니라, **권한을 줄 대상을 소유자나 관리자의 재량으로 결정한다**는 뜻이다.

예를 들어 파일 소유자 A가 보안관리자의 개입 없이 사용자 B에게 읽기 권한을 주면, B는 부여받은 권한에 따라 그 파일을 읽을 수 있다. 보기에서도 사용자나 그룹의 신원을 기준으로 접근을 제한하고 소유자나 관리자가 자율적으로 권한을 부여하므로, 임의적 접근제어인 DAC에 해당한다.

NoteBase

문 12. 다음은 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명이다. 이들 중 옳지 않은 것은?

① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원

② 방화벽이나 게이트웨이 등에 구현

③ IP 기반의 네트워크에서만 동작

④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능함

정답 4번

간단한 해설

④의 '신규 알고리즘 적용이 불가능함'이 잘못된 설명이다. IPSec은 **특정 암호화·인증 알고리즘에 종속되지 않도록** 설계되어, 새로운 알고리즘을 추가하여 사용할 수 있다.

선지별 해설

① O: IPSec의 ESP는 IP 패킷의 보호할 데이터를 암호화하여 기밀성을 제공한다. DES-CBC, RC5, Blowfish는 과거 IPSec 규격에서 사용할 수 있도록 정의된 암호화 방식들이다. IPSec은 **하나의 암호화 알고리즘만 사용하는 구조가 아니다**.

② O: IPSec은 호스트뿐 아니라 **방화벽이나 라우터 같은 보안 게이트웨이**에도 구현할 수 있다. 보안 게이트웨이는 내부 호스트를 대신하여 외부로 나가는 IP 패킷을 보호하고, 들어오는 보호 패킷을 처리할 수 있다.

③ O: IPSec은 **IP 계층에서 IP 패킷을 보호**하는 프로토콜이므로 IP 기반 네트워크에서 동작한다. IPv4와 IPv6에 적용할 수 있으며, TCP나 UDP 등 특정 상위 계층 프로토콜에만 한정되지 않는다.

④ X: IPSec은 보안 프로토콜의 구조와 구체적인 암호화·인증 알고리즘을 분리한 모듈식 설계이다. 따라서 '신규 알고리즘 적용이 불가능함'은 **'신규 알고리즘을 추가하여 적용할 수 있음'**으로 고쳐야 한다. 다만 실제 통신에 사용하려면 양쪽 장비가 해당 알고리즘을 지원하고 사용할 방식에 합의해야 한다.

NoteBase

문 13. 다음의 지문은 RSA 알고리즘의 키생성 적용 순서를 설명한 것이다. ( )를 바르게 채운 것은?

ㄱ. 두 개의 큰 소수, p와 q를 생성한다. ($p \neq q$)
ㄴ. 두 소수를 곱하여, $n = p \cdot q$를 계산한다.
ㄷ. (㉮)을 계산한다.
ㄹ. $1 < A < \phi(n)$이면서 A, $\phi(n)$이 서로소가 되는 A를 선택한다. $A \cdot B$를 $\phi(n)$으로 나눈 나머지가 1임을 만족하는 B를 계산한다.
ㅁ. 공개키로 (㉯), 개인키로 (㉰)를 각각 이용한다.

① ㉮: $\phi(n) = (p-1)(q-1)$, ㉯: (n, A), ㉰: (n, B)
② ㉮: $\phi(n) = (p+1)(q+1)$, ㉯: (n, B), ㉰: (n, A)
③ ㉮: $\phi(n) = (p-1)(q-1)$, ㉯: (n, B), ㉰: (n, A)
④ ㉮: $\phi(n) = (p+1)(q+1)$, ㉯: (n, A), ㉰: (n, B)

정답 1번

간단한 해설

서로 다른 두 소수의 곱 $n = pq$에 대해 오일러 피 함수는 $\phi(n) = (p-1)(q-1)$이다. 먼저 선택한 **공개 지수 A**와 그에 대응하여 계산한 **개인 지수 B**를 구분하면, 공개키는 (n, A), 개인키는 (n, B)이다.

빈칸별 해설

㉮: $\phi(n) = (p-1)(q-1)$이다. 오일러 피 함수 $\phi(n)$은 1부터 n까지의 자연수 중 n과 서로소인 수의 개수이다. 소수 p에서는 p의 배수인 p만 제외하므로 $\phi(p) = p - 1$이다. p와 q는 **서로 다른 소수이므로 서로소**이고, 서로소인 두 수의 곱에 대한 피 함수 값은 각 피 함수 값의 곱이므로 $\phi(pq) = (p-1)(q-1)$이 된다. 따라서 각 소수에 1을 더하는 식은 맞지 않는다.

㉯: 공개키는 (n, A)이다. ㄹ에서 $1 < A < \phi(n)$이고 A와 $\phi(n)$이 서로소가 되도록 먼저 선택한 A가 **공개 지수**이다. 서로소 조건은 A에 대응하는 역원을 구할 수 있게 한다. 공개키는 공통으로 사용하는 모듈러스 n과 공개 지수 A로 구성된다.

㉰: 개인키는 (n, B)이다. B는 $A \cdot B \equiv 1 \pm od\phi(n)$을 만족하도록 계산한 **A의 모듈러 곱셈 역원**이다. 즉, A와 B를 곱한 값을 $\phi(n)$으로 나누면 나머지가 1이 된다. 이 관계를 갖는 B가 공개 지수 A에 대응하는 개인 지수이며, 암호화된 값을 복호화할 때 사용한다. 따라서 개인키는 n과 B로 구성된다.

㉮의 $\phi(n) = (p-1)(q-1)$, ㉯의 (n, A), ㉰의 (n, B)를 함께 제시한 선택지는 ①이다.

NoteBase

문 14. 스파이웨어 주요 증상으로 옳지 않은 것은?

① 웹브라우저의 홈페이지 설정이나 검색 설정을 변경, 또는 시스템 설정을 변경한다.

② 컴퓨터 키보드 입력내용이나 화면표시내용을 수집, 전송한다.

③ 운영체제나 다른 프로그램의 보안설정을 높게 변경한다.

④ 원치 않는 프로그램을 다운로드하여 설치하게 한다.

정답 3번

간단한 해설

③의 '보안설정을 높게 변경한다'는 설명이 잘못되었다. 스파이웨어는 악성 활동을 쉽게 하려고 **보안설정을 낮추거나 보안 기능을 해제**할 수 있다.

선지별 해설

① O: 웹브라우저의 홈페이지나 검색 설정을 사용자 의사와 무관하게 바꾸어 특정 사이트로 접속을 유도할 수 있다. 이처럼 **브라우저나 시스템 설정을 임의로 변경**하는 것은 스파이웨어 감염 시 나타날 수 있는 증상이다.

② O: 스파이웨어는 사용자 몰래 정보를 수집하는 프로그램이다. **키보드 입력을 기록하거나 화면 내용을 캡처**하여 외부로 전송하면 계정 정보나 개인적인 작업 내용이 유출될 수 있다.

③ X: 보안설정을 높이면 프로그램의 실행이나 정보 유출이 제한될 수 있으므로, 이를 스파이웨어의 주요 증상으로 보기는 어렵다. 스파이웨어는 자신의 활동을 방해하는 보호 기능을 피하려고 **보안설정을 낮추거나 보안 기능을 해제**할 수 있다. 따라서 '높게 변경한다'를 '낮게 변경한다'로 고쳐야 한다.

④ O: 스파이웨어는 **원치 않는 추가 프로그램을 다운로드·설치**하게 할 수 있다. 이 과정에서 광고 프로그램이나 다른 악성 프로그램이 함께 설치되어 불필요한 실행이나 추가적인 정보 수집이 발생할 수 있다.

NoteBase

문 15. 다음 설명에 해당하는 취약점 점검도구는?

어느 한 시점에서 시스템에 존재하는 특정경로 혹은 모든 파일에 관한 정보를 DB화해서 저장한 후 차후 삭제, 수정 혹은 생성된 파일에 관한 정보를 알려주는 툴이다. 이 툴은 MD5, SHA 등의 다양한 해시 함수를 제공하고 파일들에 대한 DB를 만들어 이를 통해 해커들에 의한 파일들의 변조여부를 판별하므로 관리자들이 유용하게 사용할 수 있다.

① Tripwire
② COPS(Computer Oracle and Password System)
③ Nipper
④ MBSA(Microsoft Baseline Security Analyzer)

정답 1번

간단한 해설

Tripwire는 파일 정보를 기준 DB에 저장한 뒤 현재 상태와 비교하여 **파일의 생성·삭제·수정**을 탐지하는 무결성 점검도구이다. 지문의 해시 함수와 파일 DB는 이러한 변경을 확인하기 위한 수단이다.

공통 해설

파일 무결성 점검은 파일이 기준 상태에서 달라졌는지를 확인하는 작업이다. **Tripwire**는 정상으로 확인된 시점의 점검 대상 파일에 대해 경로·속성·해시값 등의 정보를 기준 DB에 저장한다. 이후 점검할 때 현재 파일 정보를 다시 수집하여 **기준 DB와 비교**하고, 새로 생긴 파일·사라진 파일·내용이나 속성이 바뀐 파일을 보고한다. 지문의 MD5·SHA는 파일 내용으로부터 비교에 사용할 해시값을 만드는 함수이다.

예를 들어 파일 이름이 그대로여도 내용이 수정되어 해시값이 달라지면 변경을 탐지할 수 있다. 이처럼 '파일 정보의 DB 저장 → 현재 상태와 비교 → 변경 보고'라는 동작이 Tripwire를 가리키는 핵심 단서이다. 다만 정상적인 업데이트도 파일을 바꿀 수 있으므로, **변경 탐지가 곧 해킹의 확정을 뜻하지는 않는다**. 관리자는 보고된 변경이 승인된 작업에 따른 것인지 확인해야 한다.

NoteBase

문 16. 정부는 사이버테러를 없애기 위하여 2012년 8월 정보통신망법 시행령 개정으로 100만 명 이상 이용자의 개인정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 '망분리'를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 옳지 않은 것은?

① DMZ

② OS 커널분리

③ VDI

④ 가상화기술

정답 1번

간단한 해설

DMZ는 웹·메일 서버처럼 외부에 공개할 서버를 두는 **경계 네트워크 구간**이다. 그 자체가 사용자의 **업무용 환경과 인터넷용 환경을 분리하는 기술은 아니다**.

선지별 해설

이 문항에서 망분리는 외부 인터넷을 통한 침입과 정보 유출을 막기 위해 업무망과 인터넷망의 사용 환경을 물리적 또는 논리적으로 격리하는 것을 뜻한다.

① X: DMZ는 내부망과 외부망 사이에 마련하는 **외부 서비스용 네트워크 구간**이다. 공개 웹 서버 등을 이 구간에 두고 방화벽으로 내부망 접근을 통제한다. 내부망 보호에 활용되지만, DMZ를 구성하는 것만으로 사용자의 업무용 환경과 인터넷용 환경이 분리되지는 않는다. 따라서 이 문항의 망분리 구현 기술에 해당하지 않는다.

② O: OS 커널분리는 하나의 PC에서 **업무용과 인터넷용 운영체제 환경을 분리**하여 각 환경이 해당 망을 이용하도록 하는 논리적 망분리 방식이다. 운영체제의 핵심 기능을 담당하는 커널 수준에서 실행 환경을 구분하여 두 영역 사이의 간섭을 제한한다.

③ O: VDI는 서버에 가상 데스크톱을 만들고 사용자가 단말에서 원격으로 접속하여 이용하는 기술이다. 이를 이용해 **인터넷용 가상 데스크톱과 업무용 환경을 격리**하면 논리적 망분리를 구현할 수 있다. 예를 들어 업무는 내부망 환경에서 처리하고 인터넷 접속은 별도의 가상 데스크톱에서 수행하도록 구성한다.

④ O: 가상화기술은 하나의 물리적 장비에 서로 구분되는 가상 실행 환경을 만드는 기술이다. 업무용 환경과 인터넷용 환경을 각각 구성하고 **네트워크 연결과 자원 접근을 분리·통제**하여 논리적 망분리를 구현하는 데 사용한다. 가상 환경을 만들기만 하는 것이 아니라 두 영역 사이의 접근이 통제되도록 구성해야 한다.

NoteBase

문 17. 다음 지문에서 설명하는 것은?

☒ 국내의 학계, 연구소, 정부 기관이 공동으로 개발한 블록 암호이다.
☒ 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.

① ARIA
② CAST
③ IDEA
④ LOKI

정답 1번

간단한 해설

국내 학계·연구소·정부 기관이 공동 개발하고 **Involutional SPN 구조**를 채택한 범용 블록 암호는 ARIA이다. 경량 환경과 하드웨어 구현에 적합하도록 설계되었다.

공통 해설

ARIA는 국내 학계·연구소·정부 기관이 공동 개발한 범용 블록 암호이다. 이름은 Academy(학계), Research Institute(연구소), Agency(정부 기관)에서 따왔다. 따라서 지문의 **국내 학·연·관 공동 개발**라는 단서는 ARIA의 개발 배경과 대응한다.

구조상의 단서는 **Involutional SPN**이다. SPN은 치환과 순열·확산을 반복하여 데이터를 변환하는 구조이며, ARIA의 확산 변환은 같은 변환을 두 번 적용하면 원래 입력으로 돌아오는 성질을 갖는다. 암호화와 복호화는 라운드 키를 달리하여 같은 처리 구조를 사용할 수 있어 구현을 공유하기에 유리하다. 이 구조와 경량 환경·하드웨어 구현에 대한 최적화라는 조건까지 함께 만족하는 명칭이 ARIA이다.

NoteBase

문 18. 리눅스 커널 보안 설정 방법으로 옳지 않은 것은?

① 핑(ping) 요청을 응답하지 않게 설정한다.

② 싱크 어택(SYNC Attack) 공격을 막기 위해 백로그 큐를 줄인다.

③ IP 스푸핑된 패킷을 로그에 기록한다.

④ 연결 종료 시간을 줄인다.

정답 2번

간단한 해설

백로그 큐는 연결이 아직 완성되지 않은 TCP 요청을 보관한다. 이를 **줄이면 큐가 더 쉽게 가득 차** 정상 요청까지 거부될 수 있으므로, 공격 대응을 위해서는 자원 여건에 맞게 **큐 크기를 늘리는** 방향으로 조정한다.

선지별 해설

① O: ping은 ICMP Echo 요청과 응답으로 호스트의 응답 여부를 확인한다. icmp_echo_ignore_all을 1로 설정하면 **Echo 요청에 응답하지 않게** 하여 ping을 통한 탐색을 제한할 수 있다. 다만 다른 방식의 탐색까지 모두 막는 것은 아니다.

② X: TCP SYN 플러딩은 연결 요청을 대량으로 보내고 연결을 완성하지 않아, 미완료 요청을 보관하는 백로그 큐를 소진시키는 공격이다. 큐를 줄이면 정상 요청을 수용할 여유도 줄어 서비스 거부가 더 쉽게 발생한다. 따라서 '백로그 큐를 줄인다'는 **자원 여건에 맞게 백로그 큐를 늘린다**로 고쳐야 한다. 관련 설정은 tcp_max_syn_backlog이며, SYN 쿠키도 공격 완화에 활용한다.

③ O: IP 스푸핑은 패킷의 출발지 IP 주소를 위조하는 것이다. log_martians를 활성화하면 비정상적인 주소를 가진 패킷을 커널 로그에 남겨 **위조 의심 트래픽의 탐지와 분석**에 활용할 수 있다. 다만 모든 위조 패킷을 식별하는 기능은 아니다.

④ O: 종료 과정에서 불필요하게 오래 남는 연결의 대기시간을 줄이면 자원 점유를 완화할 수 있다. tcp_fin_timeout은 **애플리케이션의 참조가 끊긴 FIN_WAIT_2 연결**의 유지시간을 제한한다. 이 시간을 줄이면 해당 연결의 자원을 더 빨리 회수할 수 있다.

NoteBase

문 19. 다음 중 XSS(Cross-Site Scripting) 공격에서 불가능한 공격은?

① 서버에 대한 서비스 거부(Denial of Service) 공격

② 쿠키를 이용한 사용자 컴퓨터 파일 삭제

③ 공격대상에 대한 쿠키 정보 획득

④ 공격대상에 대한 피싱 공격

정답 2번

간단한 해설

쿠키는 웹사이트가 브라우저에 저장하는 데이터이며, 그 자체로 사용자 컴퓨터의 파일을 삭제하는 명령을 실행하지 않는다. XSS로 스크립트를 실행하더라도 일반적인 브라우저 보안 환경에서는 **임의의 로컬 파일을 삭제할 권한이 없다**.

선지별 해설

XSS는 웹페이지에 악성 스크립트를 삽입하여, 그 페이지를 보는 사용자의 브라우저에서 실행되게 하는 공격이다. 공격의 가능 범위는 브라우저와 해당 웹사이트에 부여된 권한의 제한을 받는다.

① O: XSS로 삽입한 스크립트가 여러 사용자의 브라우저에서 서버로 반복 요청을 보내게 할 수 있다. 요청이 충분히 누적되어 서버의 처리 능력을 넘으면 정상적인 서비스 제공이 어려워지는 **서비스 거부 공격**으로 이어질 수 있다. 스크립트가 실행되는 곳은 브라우저이지만, 그 요청으로 부하를 받는 대상은 서버이다.

② X: 쿠키는 세션 식별자나 설정값 등을 담는 데이터이며, 파일 삭제 명령을 실행하는 프로그램이 아니다. 또한 일반적인 브라우저의 스크립트는 보안 제한을 받아 **사용자 컴퓨터의 임의 파일을 직접 삭제할 수 없다**. 따라서 쿠키를 탈취하거나 조작하는 것과 사용자 컴퓨터의 파일을 삭제하는 것은 구별해야 한다.

③ O: XSS는 공격자가 삽입한 스크립트를 피해자의 브라우저에서 해당 웹사이트의 권한으로 실행하게 한다. 이 스크립트는 **자바스크립트에서 접근 가능한 쿠키**를 읽어 공격자에게 전송할 수 있다. 다만 HttpOnly 속성이 설정된 쿠키의 값은 자바스크립트로 직접 읽을 수 없으므로, 모든 쿠키가 항상 탈취되는 것은 아니다.

④ O: XSS로 웹페이지의 내용을 바꾸어 가짜 로그인 입력란을 표시하거나 사용자를 위조 사이트로 이동시킬 수 있다. 사용자가 정상 사이트의 화면으로 믿고 계정 정보 등을 입력하게 만들면 **피싱 공격**이 성립한다.

NoteBase

문 20. “「전자서명법」 제15조(공인인증서발급) 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다.”라는 조문에서 공인인증서에 포함되지 않는 것은?

① 가입자의 전자서명검증정보

② 가입자와 공인인증기관이 이용하는 전자서명 방식

③ 공인인증서의 재발급 고유번호

④ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항

정답 3번

간단한 해설

③의 '재발급 고유번호'는 구 「전자서명법」이 정한 공인인증서 기재사항이 아니다. 법에서 요구한 것은 인증서를 식별하는 **공인인증서의 일련번호**이다.

선지별 해설

이 문항은 공인인증서 제도를 규정하던 구 「전자서명법」 제15조제2항의 기재사항을 기준으로 판단한다.

① O: 구 「전자서명법」 제15조제2항제2호는 가입자의 전자서명검증정보를 기재사항으로 정했다. 이는 가입자가 한 **전자서명을 검증하는 데 사용하는 정보**이므로 인증서에 포함된다.

② O: 같은 항 제3호는 가입자와 공인인증기관이 이용하는 전자서명 방식을 기재사항으로 정했다. 서명을 확인하려면 어떤 방식으로 생성된 서명인지 알아야 하므로 **가입자와 공인인증기관의 전자서명 방식**이 포함된다.

③ X: 같은 항 제4호가 정한 기재사항은 **공인인증서의 일련번호**이다. 일련번호는 발급된 인증서를 식별하기 위한 번호이다. 선지의 '재발급 고유번호'는 법정 기재사항이 아니며, 이를 '공인인증서의 일련번호'로 고쳐야 한다.

④ O: 같은 항 제7호는 공인인증서의 **이용범위 또는 용도를 제한하는 경우** 그 제한에 관한 사항을 포함하도록 했다. 인증서 이용자가 허용된 범위와 용도를 확인할 수 있게 하는 정보이며, 제한이 있다는 조건을 전제로 하는 기재사항이다.

NoteBase