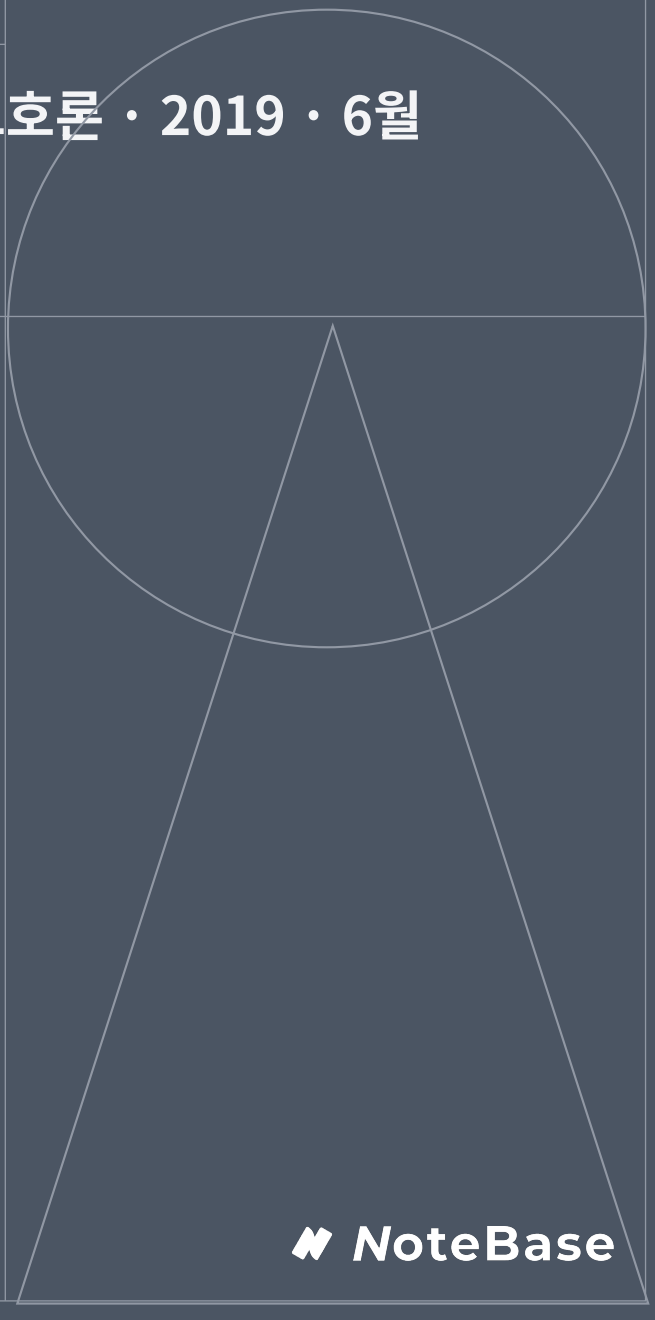
기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2019 · 6월



NoteBase

기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2019 · 6월

공무원/서울시/9급 · 정보보호론 · 2019 · 6월

문 1. 해시와 메시지 인증코드에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 순서대로 나열한 것은?

<보기>
해시와 메시지 인증코드는 공통적으로 메시지의 (㉠)을 검증할 수 있지만, 메시지 인증코드만 (㉡) 인증에 활용될 수 있다.

① ㉠: 무결성, ㉡: 상호
② ㉠: 무결성, ㉡: 서명자
③ ㉠: 비밀성, ㉡: 상호
④ ㉠: 비밀성, ㉡: 서명자

정답 1번

간단한 해설

해시와 메시지 인증코드는 메시지가 변경되었는지 확인하는 **무결성** 검증에 쓰인다. 메시지 인증코드는 **공유 비밀키**를 사용하므로 통신 당사자 간 상호 인증에도 활용할 수 있다.

빈칸별 해설

㉠ 무결성: 무결성은 메시지가 변경되지 않았음을 뜻한다. 해시는 메시지에서 해시값을 계산하고, 이를 **신뢰할 수 있는 원래 해시값**과 비교하여 변경 여부를 확인하는 데 쓰인다. 메시지 인증코드(MAC)는 메시지와 비밀키로 인증값을 생성하고, 수신자가 같은 키로 다시 계산한 값과 비교하여 무결성을 검증한다. 둘 다 메시지 내용을 암호화하여 숨기는 기능은 아니므로 비밀성을 보장하지 않는다.

㉡ 상호: MAC에서는 송신자와 수신자가 **같은 비밀키를 공유**한다. 두 당사자만 키를 알고 있다면 수신자는 MAC을 검증하여 상대방이 보낸 메시지인지 확인할 수 있다. 반대 방향으로도 메시지와 MAC을 교환·검증하는 인증 절차를 구성할 수 있으므로 상호 인증에 활용된다. 키가 없는 일반 해시는 누구나 계산할 수 있어 그 자체로 상대방을 인증하지 못한다. 한편 MAC은 수신자도 생성할 수 있으므로, 제삼자에게 특정 서명자의 작성 사실을 증명하는 전자서명의 서명자 인증·부인방지 기능과는 구별된다.

따라서 빈칸의 조합은 ㉠ 무결성, ㉡ 상호이며, 이는 ①의 구성과 일치한다.

NoteBase

문 2. 바이러스의 종류 중에서 감염될 때마다 구현된 코드의 형태가 변형되는 것은?

① Polymorphic Virus

② Signature Virus

③ Generic Decryption Virus

④ Macro Virus

정답 1번

간단한 해설

다형성 바이러스(Polymorphic Virus)는 감염될 때마다 코드의 외형을 바꾸면서도 본래의 기능은 유지한다. 이 때문에 고정된 코드 패턴만으로 탐지하기 어렵다.

공통 해설

다형성 바이러스(Polymorphic Virus)는 **감염될 때마다 코드의 형태를 변형**하는 바이러스이다. 대표적으로 바이러스 본체를 암호화하고, 새로운 감염본을 만들 때 변형 엔진으로 복호화 루틴을 바꾼다. 복호화 루틴은 암호화된 본체를 실행할 수 있도록 풀어 주는 코드이다. 이렇게 하면 같은 악성 기능을 수행하면서도 감염본마다 바이트 패턴이 달라져, 알려진 고정 패턴인 시그니처와 대조하는 탐지를 어렵게 한다. 문항의 '감염될 때마다 구현된 코드의 형태가 변형'된다는 조건은 이러한 다형성의 특징에 해당한다.

NoteBase

문 3. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?

① 오용탐지는 새로운 침입 유형에 대한 탐지가 가능하다.

② 기술적 구성요소는 정보 수집, 정보 가공 및 축약, 침입 분석 및 탐지, 보고 및 조치 단계로 이루어진다.

③ 하이브리드 기반 IDS는 호스트 기반 IDS와 네트워크 기반 IDS가 결합한 형태이다.

④ IDS는 공격 대응 및 복구, 통계적인 상황 분석 보고 기능을 제공한다.

정답 1번

간단한 해설

오용탐지는 **미리 알려진 공격 패턴**과 관찰된 활동을 대조하므로, 등록된 패턴이 없는 새로운 침입 유형은 탐지하기 어렵다. 정상적인 활동에서 벗어나는지를 살펴 새로운 공격도 탐지할 수 있는 방식은 **이상탐지**이다.

선지별 해설

① X: 오용탐지는 알려진 공격의 특징을 규칙이나 서명으로 저장하고, 수집한 정보가 그 패턴과 일치하는지 검사한다. 따라서 '새로운 침입 유형에 대한 탐지가 가능하다'는 표현은 **알려진 침입 유형을 탐지하는 데 효과적이다**로 고쳐야 한다. 이상탐지는 정상 행위의 기준에서 벗어나는 활동을 찾아내므로, 기존 공격 패턴이 없어도 새로운 공격을 탐지할 수 있다.

② O: 정보 수집 단계에서는 네트워크 패킷이나 호스트의 감사 로그 등을 모은다. 정보 가공 및 축약 단계에서는 수집 자료를 분석에 적합하게 정리하고 필요한 정보를 추린다. 침입 분석 및 탐지 단계에서 공격 여부를 판단한 뒤, 보고 및 조치 단계에서 경보를 알리고 필요한 대응으로 연결한다. 즉, **수집한 자료를 가공하여 분석하고 그 결과에 따라 조치**하는 흐름이다.

③ O: 호스트 기반 IDS는 개별 컴퓨터의 로그, 파일 및 시스템 활동 등을 살피고, 네트워크 기반 IDS는 네트워크를 흐르는 패킷과 트래픽을 살핀다. 두 방식을 결합한 하이브리드 기반 IDS는 **호스트 내부 정보와 네트워크 정보를 함께 활용**하여 각 방식의 탐지 범위를 보완한다.

④ O: IDS는 침입을 탐지하면 경보와 관련 기록을 제공하여 **공격 대응과 복구를 지원**한다. 또한 일정 기간의 탐지 기록을 집계하여 공격 유형과 발생 빈도 등 통계적인 상황 분석 보고를 제공한다. 여기서 복구 기능은 탐지 정보와 연계한 복구 지원을 포함하며, 모든 IDS가 손상된 시스템을 스스로 완전히 복원한다는 뜻은 아니다.

NoteBase

문 4. <보기>에서 블록암호 모드 중 초기 벡터(Initialization Vector)가 필요하지 않은 모드를 모두 고른 것은?

<보기>
ㄱ. CTR 모드
ㄴ. CBC 모드
ㄷ. ECB 모드

① ㄱ
② ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

정답 2번

간단한 해설

ECB는 각 평문 블록을 같은 키로 독립적으로 암호화하므로 **초기 벡터가 필요하지 않다**. 앞 블록의 암호문이나 초기 카운터 같은 별도 초기화 입력을 사용하지 않는다.

보기별 해설

ㄱ. CTR 모드: **초기 카운터 블록이 필요하다**. 카운터 블록을 암호화한 결과와 평문을 XOR하여 암호문을 만든다. 같은 키로 처리하는 모든 메시지에서 카운터 블록이 중복되지 않도록 해야 한다. 엄밀한 용어로는 CBC의 IV와 CTR의 초기 카운터를 구분하지만, 이 문항은 초기화에 필요한 별도 입력까지 포함하여 묻는 것으로 해석한다. 따라서 CTR을 초기화 값이 필요 없는 모드에 포함하지 않는다.

ㄴ. CBC 모드: 첫 평문 블록을 **IV와 XOR한 뒤 암호화**한다. 다음 블록부터는 직전 암호문 블록과 XOR하므로, 직전 암호문이 없는 첫 블록의 처리를 위해 IV가 필요하다. CBC의 IV는 예측할 수 없어야 한다.

ㄷ. ECB 모드: 각 평문 블록을 **다른 블록과 독립적으로 암호화**하므로 IV가 필요하지 않다. 같은 키에서 같은 평문 블록은 같은 암호문 블록이 되며, 이를 바꾸어 주는 초기화 입력을 사용하지 않는다.

따라서 초기 벡터가 필요하지 않은 모드는 ㄷ이며, ②의 구성에 해당한다.

NoteBase

문 5. 스트림 암호(Stream Cipher)에 대한 설명으로 가장 옳지 않은 것은?

① Key Stream Generator 출력값을 입력값(평문)과 AND 연산하여, 암호문을 얻는다.

② 절대 안전도를 갖는 암호로 OTP(One-Time Pad)가 존재한다.

③ LFSR(Linear Feedback Shift Register)로 스트림 암호를 구현할 수 있다.

④ Trivium은 현대적 스트림 암호로 알려져 있다.

정답 1번

간단한 해설

스트림 암호는 키 스트림과 평문을 **AND가 아니라 XOR** 연산하여 암호문을 만든다. 같은 키 스트림으로 암호문을 다시 XOR하면 평문을 복원할 수 있다.

선지별 해설

① X: 키 스트림 생성기의 출력과 평문은 **XOR(배타적 논리합)** 연산으로 결합한다. XOR는 두 비트가 같으면 0, 다르면 1을 출력하며, 암호문에 같은 키 스트림을 다시 XOR하면 원래 평문이 나온다. 반면 AND는 키 스트림의 비트가 0이면 평문이 0이든 1이든 결과가 0이므로, 그 결과와 키만으로 원래 비트를 구별할 수 없다.

② O: OTP는 평문과 독립적으로 생성된 균등한 진정 난수 키를 사용하고, 키를 비밀로 유지하며 **평문 길이 이상으로 확보하여 한 번만 사용**할 때 완전 비밀성을 갖는다. 이 조건에서는 암호문을 알아도 평문에 관한 추가 정보를 얻을 수 없으므로, 공격자의 계산 능력과 무관한 절대 안전도를 갖는다.

③ O: LFSR는 저장된 비트들을 이동시키면서 특정 위치의 비트들을 XOR한 값을 새 비트로 넣어 비트열을 생성하는 선형 피드백 시프트 레지스터이다. 이를 **키 스트림 생성기의 구성 요소**로 사용하여 스트림 암호를 구현할 수 있다. 다만 단일 LFSR의 출력은 선형 관계 때문에 예측될 수 있으므로, 안전한 암호를 구성하려면 비선형 결합 등의 보완이 필요하다.

④ O: Trivium은 **동기식 스트림 암호**이다. 비밀키와 초기화 벡터(IV)로 내부 상태를 초기화한 뒤, 상태를 갱신하면서 키 스트림을 생성한다. 생성한 키 스트림을 평문과 XOR하여 암호화한다.

NoteBase

문 6. <보기>에서 설명하는 DRM 구성요소는?

<보기>
DRM의 보호 범위에서 유통되는 콘텐츠의 배포 단위로서 암호화된 콘텐츠 메타 데이터, 전자서명 등의 정보로 구성되어 있다. 또한, MPEG-21 DID 규격을 따른다.

① 식별자
② 클리어링 하우스
③ 애플리케이션
④ 시큐어 컨테이너

정답 4번

간단한 해설

암호화된 콘텐츠와 메타데이터·전자서명 등을 **하나의 보호된 배포 단위**로 묶은 것이 시큐어 컨테이너이다.

공통 해설

시큐어 컨테이너는 DRM으로 보호되는 콘텐츠를 유통하기 위해 **콘텐츠와 관련 정보를 하나의 배포 단위로 묶은 구조**이다. 암호화는 콘텐츠 내용을 보호하고, 메타데이터는 콘텐츠의 속성 등을 설명하며, 전자서명은 서명된 정보의 위변조 여부와 서명자를 확인하는 데 쓰인다. 따라서 보기처럼 이러한 정보로 구성된 콘텐츠의 배포 단위를 묻는 경우에는 시큐어 컨테이너가 해당한다.

MPEG-21 DID(Digital Item Declaration)는 디지털 아이템을 이루는 **자원·메타데이터와 그 상호 관계**를 기술하는 규격이다. 보기에서 이 규격을 따른다고 한 것은 콘텐츠와 관련 정보를 일정한 구조로 표현하여 함께 유통한다는 설명을 뒷받침한다.

NoteBase

문 7. 이더넷(Ethernet)상에서 전달되는 모든 패킷(Packet)을 분석하여 사용자의 계정과 암호를 알아내는 것은?

① Nessus
② SAINT
③ Sniffing
④ IPS

정답 3번

간단한 해설

네트워크를 오가는 패킷을 가로채 내용을 분석하는 행위가 **스니핑(Sniffing)**이다. 계정과 암호가 평문으로 전송되면 수집한 패킷에서 해당 정보를 읽어낼 수 있다.

공통 해설

스니핑(Sniffing)은 네트워크에서 관찰할 수 있는 패킷을 수집하고 그 내용을 분석하는 도청 기법이다. 문제에서 이더넷으로 전달되는 패킷을 분석하여 계정과 암호를 알아낸다는 설명은 **전송 중인 통신 내용을 엿보는 행위**에 해당하므로 스니핑을 가리킨다.

계정과 암호가 암호화되지 않은 평문으로 전송되면 패킷의 데이터 부분을 분석하여 그 값을 읽을 수 있다. 다만 **암호화된 통신은 패킷을 수집하는 것만으로 계정과 암호가 바로 드러나지 않는다**. 스니핑 자체가 암호를 해독하거나 추측하는 기법을 뜻하는 것은 아니다.

NoteBase

문 8. 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화되어 있는 파일은?

① /etc/group
② /etc/passwd
③ /etc/shadow
④ /etc/login.defs

정답 3번

간단한 해설

/etc/shadow는 **사용자별 패스워드 해시값**과 최대 사용 일수·만료 전 경고 기간 같은 **패스워드 유효기간 정보**를 함께 저장한다.

공통 해설

리눅스의 shadow 패스워드 방식에서 /etc/shadow는 사용자별 패스워드 정보를 보관하는 파일이다.
패스워드는 평문이 아니라 **일방향 해시값**으로 저장되며, 문항의 '암호화되어 있는'은 이러한 보호된 저장 형태를 가리킨다. 이 파일에는 마지막 패스워드 변경일, 최대 사용 일수, 만료 전 경고 기간 등도 기록되어 사용자별 패스워드 유효기간을 관리한다.

문항은 패스워드 정책 정보뿐 아니라 **사용자 패스워드의 저장**도 함께 요구하므로 /etc/shadow에 해당한다.
/etc/login.defs에도 계정 생성 시 적용할 패스워드 유효기간 기본 설정이 있지만, 개별 사용자의 패스워드 해시값을 저장하는 파일은 아니다.

NoteBase

문 9. 타원곡선 암호에 대한 설명으로 가장 옳지 않은 것은?

① 타원곡선 암호의 단점은 보안성 향상을 위하여 키 길이가 길어진다는 것이다.

② 타원곡선에서 정의된 연산은 덧셈이다.

③ 타원곡선을 이용하여 디피-헬먼(Diffie-Hellman) 키 교환을 수행할 수 있다.

④ 타원곡선은 공개키 암호에 사용된다.

정답 1번

간단한 해설

타원곡선 암호(ECC)는 RSA 등과 **동일한 보안 수준에서 더 짧은 키**를 사용할 수 있다는 장점이 있다. '보안성 향상을 위하여 키 길이가 길어진다'는 설명은 ECC의 특징적인 단점으로 볼 수 없다.

선지별 해설

① X: ECC는 RSA 같은 기존 공개키 암호와 비교할 때 **같은 보안 수준을 더 짧은 키로 제공**할 수 있다. 키가 짧으면 저장·전송에 필요한 데이터량을 줄일 수 있다. ECC에서도 목표 보안 수준을 높이면 더 긴 키가 필요할 수 있지만, 이를 ECC의 특징적인 단점이라고 한 것은 부적절하다.

② O: 타원곡선 암호의 기본 군 연산은 **곡선 위의 점 덧셈**이다. 두 점을 정해진 규칙으로 더해 다시 곡선 위의 점을 얻으며, 각 좌표를 단순히 더하는 연산은 아니다. 한 점을 반복해서 더하는 연산을 스칼라 곱이라고 한다.

③ O: 타원곡선 위에서 디피-헬먼 키 교환을 구현한 것이 **ECDH**이다. 공통 기준점 G와 각자의 비밀 정수 a, b를 사용해 공개값 aG, bG를 교환한다. 각자 받은 공개값에 자신의 비밀 정수를 곱하면 $a(bG) = b(aG) = abG$로 같은 공유점을 얻고, 이로부터 공유 비밀키를 도출할 수 있다.

④ O: ECC는 **개인키와 공개키를 구분**하는 공개키 암호 기술이다. 개인키를 비밀 정수 d로 두고, 기준점 G에 대해 공개키를 $Q = dG$로 만든다. 안전하게 선택된 곡선과 매개변수에서는 공개된 G와 Q로부터 d를 구하기 어렵다는 타원곡선 이산로그 문제의 난해성을 이용한다.

NoteBase

문 11. 「개인정보 보호법」상 주민등록번호의 처리에 대한 설명으로 가장 옳지 않은 것은?

① 개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

② 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 개인정보처리자로부터 주민등록번호를 제공받은 자는 개인정보 보호 위원회의 심의·의결을 거쳐 제공받은 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

정답 4번

간단한 해설

주민등록번호를 제공받았다고 하여 **보호위원회의 심의·의결만으로** 목적 외 이용이나 재제공을 할 수 있는 것은 아니다. 공공기관의 법정 업무 수행을 위한 예외와 개인정보를 제공받은 자의 이용·제공 제한을 구별해야 한다.

NoteBase

선지별 해설

① O: 개인정보 보호법 제24조의2제2항은 주민등록번호를 분실·도난·유출·위조·변조·훼손으로부터 보호하기 위하여 **암호화하여 안전하게 보관할 의무**를 정한다. 적법하게 수집한 주민등록번호라도 보관 과정에서 이 보호조치를 해야 한다.

② O: 선지의 행정안전부장관과 과징금 액수는 구 개인정보 보호법 제34조의2제1항에 따른 것이다. 당시에는 주민등록번호의 분실·도난·유출·위조·변조·훼손이 발생하면 행정안전부장관이 5억원 이하의 과징금을 부과·징수할 수 있었다. 다만 개인정보처리자가 제24조제3항에 따른 **안전성 확보조치를 다한 경우에는 부과 대상에서 제외**되므로, 사고 발생만으로 언제나 과징금이 부과되는 것은 아니다.

③ O: 개인정보 보호법 제24조의2제3항에 따라 인터넷 홈페이지 회원가입 단계에서는 **주민등록번호를 사용하지 않는 가입 방법**을 제공해야 한다. 법정 사유에 따라 주민등록번호 처리가 허용되는 개인정보처리자에게도 이 의무가 적용된다.

④ X: 개인정보 보호법 제19조는 개인정보를 제공받은 자의 목적 외 이용·제3자 제공을 원칙적으로 금지하고, 정보주체의 별도 동의나 다른 법률의 특별한 규정을 예외로 둔다. **보호위원회의 심의·의결은 제19조의 예외가 아니다.** 심의·의결에 관한 제18조제2항제5호는 공공기관이 다른 법률에서 정한 소관 업무를 수행하려면 목적 외 이용·제공이 필요한 경우에 적용되며, 정보주체나 제3자의 이익을 부당하게 침해할 우려도 없어야 한다. 따라서 이 규정을 제공받은 자의 일반적인 이용·제공 허용 근거로 삼을 수 없다. 또한 주민등록번호에는 제24조의2제1항의 특별한 처리 제한도 적용되므로, 일반 개인정보에 관한 별도 동의만으로 주민등록번호의 목적 외 이용·재제공까지 허용되는 것은 아니다.

NoteBase

문 12. <보기>의 설명에 해당되는 공격 유형으로 가장 적합한 것은?

<보기> SYN 패킷을 조작하여 출발지 IP 주소와 목적지 IP 주소를 일치시켜서 공격 대상에 보낸다. 이때 조작된 IP 주소는 공격 대상의 주소이다.

① Smurf Attack
② Land Attack
③ Teardrop Attack
④ Ping of Death Attack

정답 2번

간단한 해설

SYN 패킷의 **출발지와 목적지 IP 주소를 모두 공격 대상의 주소로 위조**하는 것은 Land Attack의 특징이다. 공격 대상이 자신에게서 온 연결 요청처럼 처리하도록 만드는 방식이다.

공통 해설

Land Attack은 TCP 연결을 시작하는 SYN 패킷에서 **출발지와 목적지 주소를 모두 공격 대상 자신의 주소로 설정**하여 보내는 서비스 거부 공격이다. 출발지 주소는 보낸 쪽을, 목적지 주소는 받는 쪽을 나타내므로, 두 주소가 모두 대상의 주소이면 대상이 자기 자신에게 연결을 요청한 것처럼 보인다. 취약한 TCP/IP 구현은 이러한 비정상적인 요청을 처리하는 과정에서 서비스 장애를 일으킬 수 있다.

보기는 단순히 SYN 패킷을 많이 보낸다는 설명이 아니라, 출발지와 목적지 IP 주소를 일치시키고 그 주소를 공격 대상의 주소로 지정한다고 명시한다. 이 주소 위조 방식이 Land Attack의 정의와 일치한다.

NoteBase

문 13. TLS 및 DTLS 보안 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① TLS 프로토콜에서는 인증서(Certificate)를 사용하여 인증을 수행할 수 있다.

② DTLS 프로토콜은 MQTT 응용 계층 프로토콜의 보안에 사용될 수 있다.

③ TLS 프로토콜은 Handshake·Change Cipher Spec·Alert 프로토콜과 Record 프로토콜 등으로 구성되어 있다.

④ TCP 계층 보안을 위해 TLS가 사용되며, UDP 계층 보안을 위해 DTLS가 사용된다.

정답 2번

간단한 해설

MQTT는 일반적으로 TCP 위에서 동작하므로 통신 보안에 **TLS**를 사용한다. DTLS는 UDP 같은 데이터그램 전송을 위한 것으로, MQTT가 요구하는 **순서가 보장되는 무손실 바이트 스트림**을 자체적으로 제공하지 않는다.

선지별 해설

① O: TLS는 핸드셰이크 과정에서 **인증서에 기반한 상대방 인증**을 수행할 수 있다. 인증서는 공개키와 그 소유자의 신원을 연결하며, 인증서 검증과 해당 개인키의 소유 확인을 통해 통신 상대를 인증한다. 서버 인증에 사용할 수 있고, 클라이언트 인증서를 요청하면 클라이언트 인증에도 사용할 수 있다.

② X: MQTT는 순서가 보장되는 무손실 바이트 스트림을 요구하며, 일반적으로 TCP 위에서 동작한다. 따라서 MQTT 통신을 보호할 때는 **DTLS가 아니라 TLS**를 사용한다. DTLS는 데이터그램의 기밀성과 무결성 등을 보호하지만, 응용 데이터의 손실을 복구하거나 도착 순서를 보장하지 않으므로 MQTT에 필요한 전송 특성을 자체적으로 충족하지 못한다.

③ O: TLS 1.2의 구성에 해당한다. Record 프로토콜은 상위 메시지를 레코드 단위로 나누고 암호화·무결성 보호를 적용하여 전달한다. 그 위에서 Handshake는 **통신 상대 인증과 보안 매개변수·키 협상**을 수행하고, Change Cipher Spec은 이후 레코드에 새로 협상한 암호 설정과 키를 적용함을 알린다. Alert는 오류나 연결 종료 등의 상태를 통지한다.

④ O: TLS는 TCP와 같은 신뢰성 있는 전송 위에서 통신을 보호하고, DTLS는 UDP와 같은 **데이터그램 전송에 맞추어** 통신을 보호한다. DTLS는 데이터그램의 손실이나 순서 변경이 가능한 환경에서 보안 연결을 수립할 수 있도록 핸드셰이크 메시지의 재전송 등의 기능을 갖춘다. 여기서 TCP·UDP 계층 보안은 TCP·UDP를 이용하는 응용 통신을 보호한다는 뜻이다.

NoteBase

문 14. 무선 통신 보안 기술에 대한 설명으로 가장 옳지 않은 것은?

① 무선 네트워크 보안 기술에 사용되는 WPA2 기술은 AES/CCMP를 사용한다.

② 무선 네트워크에서는 인증 및 인가, 과금을 위해 RADIUS 프로토콜을 사용할 수 있다.

③ 무선 AP의 SSID값 노출과 MAC 주소 기반 필터링 기법은 공격의 원인이 된다.

④ 무선 네트워크 보안 기술인 WEP(Wired Equivalent Privacy) 기술은 유선 네트워크 수준의 보안성을 제공하므로 기존의 보안 취약성 문제를 극복했다.

정답 4번

간단한 해설

WEP는 유선망 수준의 보안성을 목표로 도입되었지만, **암호화와 무결성 검증의 구조적 취약점** 때문에 이를 달성하지 못했다. 따라서 기존의 보안 취약성을 극복했다는 설명은 잘못이다.

선지별 해설

① O: WPA2는 **AES 기반의 CCMP**를 사용한다. AES는 데이터를 암호화하는 알고리즘이고, CCMP는 이를 이용해 무선으로 전송하는 데이터의 기밀성과 무결성을 보호하는 프로토콜이다.

② O: RADIUS는 **인증·인가·과금 정보 관리인 AAA**를 지원하는 프로토콜이다. 인증은 사용자의 신원을 확인하고, 인가는 허용할 접근 권한을 결정하며, 과금은 접속 시간이나 전송량 등의 사용 내역을 기록하는 기능이다. 무선 네트워크에서도 AP와 RADIUS 서버를 연동해 이러한 기능을 제공할 수 있다.

③ O: SSID는 무선 네트워크를 구별하는 이름이므로 노출되면 공격자가 대상 네트워크를 파악할 수 있다. MAC 주소 기반 필터링은 허용된 단말의 주소를 등록해 접근을 제한하지만, 공격자가 무선 프레임에서 주소를 알아내고 **허용된 MAC 주소로 위조**하면 우회할 수 있다. 따라서 SSID나 MAC 주소만을 신뢰하는 접근 통제에는 공격에 악용될 수 있는 약점이 있다.

④ X: WEP의 이름은 '유선과 동등한 프라이버시'라는 도입 목표를 나타낼 뿐, 실제로 그 수준의 보안성을 보장한다는 뜻은 아니다. WEP는 RC4 암호화에 24비트 초기화 벡터(IV)를 사용하는데, IV의 반복과 키 구성 방식의 약점 때문에 수집한 무선 트래픽으로부터 키를 복구하는 공격에 취약하다. 또한 무결성 검사에 쓰는 CRC-32는 의도적인 데이터 변조를 막는 암호학적 검증 수단이 아니다. 따라서 WEP는 **기존 취약성을 극복한 기술이 아니라 보안상 취약한 초기 무선 보안 기술**이며, 이를 보완하기 위해 WPA와 WPA2가 도입되었다.

NoteBase

문 15. 서비스 거부 공격(DoS)에 대한 설명으로 가장 옳지 않은 것은?

① 공격자가 임의로 자신의 IP 주소를 속여서 다량으로 서버에 보낸다.

② 대상 포트 번호를 확인하여 17, 135, 137번, UDP 포트 스캔이 아니면, UDP Flooding 공격으로 간주한다.

③ 헤더가 조작된 일련의 IP 패킷 조각들을 전송한다.

④ 신뢰 관계에 있는 두 시스템 사이에 공격자의 호스트를 마치 하나의 신뢰 관계에 있는 호스트인 것처럼 속인다.

정답 4번

간단한 해설

④의 신뢰 관계를 이용해 정상 호스트로 가장하는 행위는 **IP 스푸핑**이다. DoS는 시스템 자원이나 처리상의 취약점을 이용해 **정상적인 서비스 이용을 방해**하는 공격이다.

선지별 해설

① O: 출발지 IP 주소를 위조한 패킷을 대량으로 전송하는 것은 DoS에 쓰이는 방식이다. 예를 들어 SYN Flooding에서는 연결 요청을 대량으로 보내고 연결을 완료하지 않아 서버의 연결 대기 자원을 소모시킬 수 있다. 이때 **IP 주소 위조는 공격 출처를 숨기는 수단**이고, 서비스 장애를 일으키는 핵심은 서버 자원의 소모이다.

② O: 대량의 의심스러운 UDP 트래픽을 분석하면서 포트 스캔과 UDP Flooding을 구별하는 탐지 관점의 설명이다. 17·135·137번 등 목적지 포트를 확인하되, UDP 포트 스캔은 서비스나 포트의 상태를 알아보려는 행위이고 UDP Flooding은 패킷을 대량으로 보내 서버 처리 자원이나 대역폭을 소모시키는 행위이다. 다만 **특정 포트 번호이거나 스캔이 아니라는 이유만으로 공격이 확정되지는 않는다**. 정상 UDP 통신과 구별하려면 단위 시간당 패킷 수와 트래픽 양상 등을 함께 확인해야 한다.

③ O: **Teardrop 공격**의 방식이다. IP 단편 헤더의 오프셋 등 재조립에 필요한 정보를 조작하여 단편의 데이터 영역이 겹치도록 전송한다. 단편은 나뉜 IP 패킷 조각이고, 오프셋은 원래 데이터에서 그 조각의 위치를 나타낸다. 이를 제대로 처리하지 못하는 취약한 시스템은 재조립 과정에서 오류나 중단이 발생하여 서비스를 제공하지 못할 수 있다.

④ X: 신뢰하는 호스트의 IP 주소를 위조해 그 호스트에서 온 통신처럼 받아들이게 하는 **IP 스푸핑에 의한 신뢰 관계 악용**을 설명한다. IP 주소에 기반해 접근을 허용하는 시스템을 속여 권한 없는 접근을 시도하는 방식이다. 이를 DoS의 설명으로 제시한 부분이 잘못되었다. DoS는 자원 고갈이나 취약점 악용으로 정상 사용자의 서비스 이용을 방해하는 공격이다. IP 스푸핑이 DoS의 보조 수단으로 쓰일 수는 있지만, 신뢰 호스트로 가장하는 행위 자체가 서비스 거부를 뜻하지는 않는다.

NoteBase

문 16. 윈도우 운영체제에서의 레지스트리(Registry)에 대한 설명으로 가장 옳은 것은?

① 레지스트리 변화를 분석함으로써 악성코드를 탐지할 수 있다.

② 레지스트리는 운영체제가 관리하므로 사용자가 직접 조작할 수 없다.

③ 레지스트리 편집기를 열었을 때 보이는 다섯 개의 키를 하이브(Hive)라고 부른다.

④ HKEY_CURRENT_CONFIG는 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보를 저장한다.

정답 1번

간단한 해설

악성코드는 재부팅이나 로그인 뒤에도 실행되도록 **자동 실행 관련 레지스트리 값을 변경**할 수 있다. 이러한 키와 값의 변화를 분석하면 악성코드의 활동 흔적을 탐지할 수 있다.

선지별 해설

① O: 레지스트리는 운영체제와 응용 프로그램의 설정을 저장하는 계층형 데이터베이스이다. 악성코드는 실행을 지속하기 위해 자동 실행 항목을 추가하거나 수정할 수 있으므로, **레지스트리 키와 값의 생성·변경·삭제**는 악성코드 탐지의 단서가 된다. 예를 들어 로그인 시 실행할 프로그램을 지정하는 항목에 의심스러운 실행 파일이 등록되면, 그 변경과 관련 프로그램을 조사할 수 있다. 다만 정상 프로그램도 레지스트리를 변경하므로 변경 사실만으로 악성코드라고 단정하지는 않는다.

② X: 운영체제가 레지스트리를 관리하더라도 사용자의 직접 조작이 금지되는 것은 아니다. 사용자는 레지스트리 편집기 등의 도구로 **접근 권한이 허용된 키와 값을 수정**할 수 있다. 수정 가능 여부는 해당 키의 보안 설정과 사용자의 권한에 따라 달라진다.

③ X: 레지스트리 편집기의 최상위에 보이는 다섯 개의 키는 **루트 키 또는 미리 정의된 키**이다. 하이브는 관련 키·하위 키·값이 지원 파일과 함께 관리되는 논리적 묶음이므로, 화면의 최상위 키 다섯 개와 일대일로 대응하는 개념이 아니다. 예를 들어 HKEY_LOCAL_MACHINE 아래의 SOFTWARE와 SYSTEM은 각각 별도의 하이브에 해당한다.

④ X: HKEY_CURRENT_CONFIG는 **현재 사용 중인 하드웨어 프로필 정보**를 제공한다. 로그인한 사용자의 바탕 화면, 환경 변수, 응용 프로그램 설정 등 사용자별 구성 정보에 해당하는 키는 HKEY_CURRENT_USER이다. 선지는 하드웨어 구성 정보와 현재 사용자 정보를 혼동했다.

NoteBase

문 17. 침입차단시스템에 대한 설명으로 가장 옳은 것은?

① 스크린드 서브넷 구조(Screened Subnet Architecture)는 DMZ와 같은 완충 지역을 포함하며 구축 비용이 저렴하다.

② 스크리닝 라우터 구조(Screening Router Architecture)는 패킷을 필터링하도록 구성되므로 구조가 간단하고 인증 기능도 제공할 수 있다.

③ 이중 네트워크 호스트 구조(Dual-homed Host Architecture)는 내부 네트워크를 숨기지만, 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.

④ 스크린드 호스트 게이트웨이 구조(Screened Host Gateway Architecture)는 서비스 속도가 느리지만, 베스천 호스트에 대한 침입이 있어도 내부 네트워크를 보호할 수 있다.

정답 3번

간단한 해설

이중 네트워크 호스트는 내부망과 외부망 사이의 **직접적인 패킷 전달을 차단**하고 베스천 호스트의 프록시를 통해 통신하게 하여 내부망을 숨긴다. 그러나 **베스천 호스트가 장악되면** 이 차단 기능을 우회하거나 내부망을 공격할 수 있어 보호가 무너진다.

NoteBase

선지별 해설

① X: 스크린드 서브넷 구조는 외부망과 내부망 사이에 **DMZ라는 별도의 완충망**을 두고, 그 안에 베스천 호스트나 공개 서버를 배치한다. 전형적으로 외부·내부 라우터와 베스천 호스트 등을 사용하므로 구성이 복잡하고 구축 비용이 높다. 따라서 DMZ를 포함한다는 부분은 맞지만, 구축 비용이 저렴하다는 부분은 틀리다.

② X: 스크리닝 라우터 구조는 출발지·목적지 IP 주소, 포트 번호 등 패킷 헤더 정보를 기준으로 통신을 허용하거나 차단하므로 구조가 간단하다. 그러나 이러한 **패킷 필터링 자체는 사용자 인증을 제공하지 못한다**. 주소나 포트에 따른 접근 통제와 사용자의 신원을 확인하는 인증은 구별해야 한다.

③ O: 이중 네트워크 호스트 구조는 내부망과 외부망에 연결된 두 네트워크 인터페이스를 갖는 베스천 호스트를 사용한다. 호스트의 IP 포워딩을 끄고 프록시가 통신을 중계하게 하므로 외부에서 내부 시스템에 직접 접근하지 못하고 내부망을 숨길 수 있다. 다만 **보호가 베스천 호스트에 의존**하므로, 공격자가 이를 장악하여 IP 포워딩을 다시 켜거나 내부망으로 공격을 보내면 내부망을 보호할 수 없다.

④ X: 스크린드 호스트 게이트웨이 구조는 스크리닝 라우터와 베스천 호스트를 결합한다. 프록시가 처리하는 서비스는 중계 과정에서 지연이 생길 수 있지만, 베스천 호스트가 침해되어도 내부망을 보호할 수 있다는 설명은 틀리다. 기본 구조에서는 베스천 호스트가 **내부 호스트와 같은 망에 위치**하므로, 이를 장악한 공격자가 내부 호스트를 공격할 수 있다. 베스천 호스트를 별도의 DMZ에 두고 내부망과 추가로 분리하는 것은 스크린드 서브넷 구조이다.

NoteBase

문 18. 최근 알려진 Meltdown 보안 취약점에 대한 설명으로 가장 옳은 것은?

① CPU가 사용하는 소비 전력 패턴을 사용하여 중요한 키 값이 유출되는 보안 취약점이다.

② CPU의 특정 명령어가 실행될 때 소요되는 시간을 측정하여 해당 명령어와 주요한 키 값이 유출될 수 있는 보안 취약점이다.

③ SSL 설정 시 CPU 실행에 영향을 미쳐 CPU 과열로 인해 오류를 유발하는 보안 취약점이다.

④ CPU를 고속화하기 위해 사용된 비순차적 명령어 처리(Out-of-Order Execution) 기술을 악용한 보안 취약점이다.

정답 4번

간단한 해설

Meltdown은 CPU의 **비순차적 명령어 처리** 과정에서 접근 권한이 없는 메모리의 정보가 일시적으로 사용되는 점을 악용한다. 이때 남은 캐시 흔적을 분석하면 보호된 정보를 알아낼 수 있다.

선지별 해설

① X: 소비 전력 패턴으로 암호키를 추정하는 것은 **전력 분석 공격**에 해당한다. 연산이나 처리 데이터에 따라 전력 소비가 달라지는 점을 이용한다. Meltdown은 전력 측정이 아니라 비순차 실행 중 발생하는 메모리 접근과 캐시 흔적을 악용한다.

② X: 연산에 걸리는 시간의 차이로 비밀키를 추정하는 일반적인 **타이밍 공격**을 설명한 것이다. Meltdown에서도 캐시 접근 시간을 측정할 수 있지만, 단순히 특정 명령어의 실행 시간을 재는 것이 핵심은 아니다. 접근 권한이 없는 데이터가 비순차 실행 중 일시적으로 사용되고 캐시에 흔적을 남기는 점이 핵심이다.

③ X: Meltdown은 **SSL 설정이나 CPU 과열로 인한 오류가 원인이 아니다**. 취약한 CPU가 비순차 실행 중 보호된 메모리의 데이터를 일시적으로 사용하면서 정보가 노출되는 취약점이다.

④ O: 비순차적 명령어 처리는 CPU가 명령어를 프로그램 순서대로만 실행하지 않고, 필요한 자원이 준비된 명령어를 먼저 실행하여 성능을 높이는 기술이다. Meltdown은 이 과정에서 접근 권한이 없는 메모리의 데이터를 일시적으로 읽고, 그 값에 따라 캐시 상태가 달라지는 점을 악용한다. 권한 위반으로 명령어의 실행 결과가 폐기되어도 **캐시에 남은 흔적**은 유지될 수 있어, 캐시 접근 시간의 차이로 보호된 데이터 값을 추정할 수 있다.

NoteBase

문 19. <보기>는 TCSEC(Trusted Computer System Evaluation Criteria)에 의하여 보안 등급을 평가할 때 만족해야 할 요건들에 대한 설명이다. 보안 등급이 높은 것부터 순서대로 나열된 것은?

<보기>
ㄱ. 강제적 접근 제어가 구현되어야 한다.
ㄴ. 정형화된 보안 정책을 일정하게 유지하여야 한다.
ㄷ. 사용자가 자신의 파일에 대한 접근 권한을 설정할 수 있어야 한다.

① ㄱ - ㄴ - ㄷ
② ㄱ - ㄷ - ㄴ
③ ㄴ - ㄱ - ㄷ
④ ㄴ - ㄷ - ㄱ

정답 3번

간단한 해설

강제적 접근 제어의 구현보다 보안 정책을 **정형 모델로 표현하고 그 일관성을 입증**하는 요건이 더 높은 등급에서 요구된다. 상위 등급은 하위 등급의 보안 기능을 포함하므로, 각 요건이 처음 요구되는 최소 등급을 기준으로 비교한다.

올바른 순서

ㄴ → ㄱ → ㄷ

ㄴ. 정형화된 보안 정책의 유지: **B2 등급부터** 보안 정책을 명확한 수학적 규칙으로 표현한 정형 모델을 유지하고, 그 모델이 공리와 일관됨을 입증해야 한다. 단순히 접근을 통제하는 기능을 갖추는 데서 나아가, 통제의 근거가 되는 정책 모델의 일관성까지 요구하므로 B1보다 높은 수준이다.

ㄱ. 강제적 접근 제어: **B1 등급부터** 요구된다. 시스템이 사용자와 파일 등에 부여된 보안 등급·범주를 바탕으로 접근을 통제한다. 사용자가 파일 공유를 허용하더라도 시스템의 강제적 보안 정책에 어긋나는 접근은 허용되지 않는다. B1은 C2의 보안 기능에 이러한 강제적 접근 제어 등을 추가한 등급이다.

ㄷ. 사용자의 파일 접근 권한 설정: **C1 등급부터** 요구되는 임의적 접근 제어에 해당한다. 사용자가 자신의 파일을 누구와 공유할지 정할 수 있다는 뜻이다. 상위 등급에서도 이 기능은 유지되지만, 이 요건 자체가 처음 요구되는 등급은 C1이므로 세 요건 중 가장 낮다.

NoteBase

문 20. 정보보호 및 개인정보보호 관리체계인증(ISMS-P)에 대한 설명으로 가장 옳지 않은 것은?

① 정보보호 관리체계 인증만 선택적으로 받을 수 있다.

② 개인정보 제공 시뿐만 아니라 파기 시의 보호조치도 포함한다.

③ 위험 관리 분야의 인증기준은 보호대책 요구사항 영역에서 규정한다.

④ 관리체계 수립 및 운영 영역은 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행되는지 평가한다.

정답 3번

간단한 해설

위험 관리 분야의 인증기준은 '보호대책 요구사항'이 아니라 **'관리체계 수립 및 운영' 영역**에 속한다. 위험을 평가하고 그 결과에 따라 보호대책을 선정하는 관리 과정이다.

선지별 해설

① O: 통합된 인증제도에서도 **정보보호 관리체계(ISMS) 인증만 선택**하여 받을 수 있다. ISMS에는 '관리체계 수립 및 운영'과 '보호대책 요구사항'이 적용되며, ISMS-P에는 여기에 '개인정보 처리 단계별 요구사항'이 추가된다. ISMS만 취득한 것을 ISMS-P 취득으로 보는 것은 아니다.

② O: ISMS-P의 '개인정보 처리 단계별 요구사항'은 수집, 보유 및 이용, 제공, 파기와 정보주체 권리보호를 다룬다. 따라서 개인정보를 외부에 제공할 때뿐 아니라 **파기할 때의 보호조치**도 심사 대상에 포함된다.

③ X: 위험 관리는 **'관리체계 수립 및 운영' 영역의 1.2 위험 관리**에 해당한다. 정보자산을 식별하고 처리 현황과 흐름을 분석하여 위험을 평가하고, 그 결과에 따라 보호대책을 선정하는 과정이다. '보호대책 요구사항' 영역은 접근통제, 암호화, 물리 보안 등 구체적인 보호대책의 기준을 정하므로 두 영역을 구별해야 한다.

④ O: '관리체계 수립 및 운영'은 계획(Plan), 실행(Do), 점검(Check), 개선(Act)의 순환에 따라 운영되는지를 평가한다. 관리체계의 기반을 마련하고 위험을 평가하여 계획을 세운 뒤 대책을 실행하며, 운영 결과를 점검하고 문제점을 개선한다. **점검·개선 결과를 다음 계획과 운영에 반영**하므로 일회성 구축으로 끝나지 않고 지속적이고 반복적으로 수행된다.

NoteBase