2019년 지방직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
②	④	④	②	②	③	③	④	①	④
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
②	①	②	③	①	①	②	②	④	④

문 1. 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직은?

① CISO
② CERT
③ CPPG
④ CPO

② CERT(Computer Emergency Response Team, 침해사고대응팀)에 대한 정의이다.

<오답 체크> ① CISO(Chief Information Security Officer, 정보보호최고책임자)
기업에서 정보 보안을 위한 기술적 대책과 법률 대응까지 총괄 책임을 지는 최고 임원을 지칭한다.

③ CPPG(Certified Privacy Protection General, 개인정보관리사)
한국CPO포럼에서 시행하는 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 평가하는 시험 제도이자 본 자격증을 취득한 사람을 일컫는다.

④ CPO(Chief Privacy Officer, 개인정보보호최고책임자)
개인정보의 처리에 관한 업무를 총괄해서 책임지는 자

답 ②

문 2. OECD 개인정보보호 8개 원칙 중 다음에서 설명하는 것은?

> 개인정보 침해, 누설, 도용을 방지하기 위한 물리적·조직적·기술적인 안전조치를 확보해야 한다.

① 수집 제한의 원칙(Collection Limitation Principle)
② 이용 제한의 원칙(Use Limitation Principle)
③ 정보 정확성의 원칙(Data Quality Principle)
④ 안전성 확보의 원칙(Security Safeguards Principle)

보기의 내용은 개인정보를 운영하는 과정에서 외부로 유출되지 않도록 안전하게 지킬 것을 의미하므로, ④안정성 확보의 원칙에 부합한다.

◈ OECD 개인정보보호 8원칙

① 수집 제한의 법칙(Collection Limitation Principle)
개인정보는 적법하고 공정한 방법을 통해 수집되어야 한다.

② 정보 정확성의 원칙(Data Quality Principle)
이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

③ 목적 명시의 원칙(Purpose Specification Principle)
개인정보는 수집 과정에서 수집 목적을 명시하고, 명시된 목적에 적합하게 이용되어야 한다.

④ 이용 제한의 원칙(Use Limitation Principle)
정보 주체의 동의가 있거나, 법규정이 있는 경우를 제외하고 목적 외 이용되거나 공개될 수 없다.

⑤ 안전성 확보의 원칙(Security Safeguard Principle)
개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적, 조직적, 기술적 안전 조치를 확보해야 한다.

⑥ 공개의 원칙(Openness Principle)
개인정보의 처리 및 보호를 위한 정책 및 관리자에 대한 정보는 공개되어야 한다.

⑦ 개인 참가의 원칙(Individual Participation Principle)
정보 주체의 개인정보 열람/정정/삭제 청구권은 보장되어야 한다.

⑧ 책임의 원칙(Accountability Principle)
개인정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

답 ④

문 3. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은?

① DoS 공격
② 취약한 인증 및 세션 공격
③ SQL 삽입 공격
④ CSRF 공격

④ **CSRF**(Cross-site request forgery, 크로스사이트 요청 변조)
로그인 된 피해자의 세션 쿠키를 위조하여, 피해자가 의도 않은 요청을 웹사이트로 보내 피해를 입히는 공격이다.

<오답 체크> ① **DoS**(Denial of Service, 서비스 거부 공격)은 해당 시스템의 자원을 고갈시켜 제대로 사용하지 못하게 하는 공격들을 총칭하여 이르는 용어이다.

② **취약한 인증 및 세션 공격**(Broken Authentication and Session Management)
인증 및 세션 관리와 관련된 어플리케이션 기능이 잘못 구현되어, 공격자가 암호, 키 또는 세션 토큰을 해킹하여 다른 사용자의 권한을 얻을 수 있게 되는 취약점을 말한다.

③ **SQL 삽입**(SQL 인젝션, SQL injection) 공격
클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격

답 ④

문 4. 스테가노그래피에 대한 설명으로 옳지 않은 것은?

① 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.
② 원문 데이터에 비해 더 많은 정보의 은닉이 가능하므로 암호화보다 공간효율성이 높다.
③ 텍스트.이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.
④ 고해상도 이미지 내 각 픽셀의 최하위 비트들을 변형하여 원본의 큰 손상 없이 정보를 은닉하는 방법이 있다.

▶ 스테가노그래피(steganography)는 보통의 데이터에 또 다른 정보나 데이터를 보이지 않게 삽입하는 기술이다.

② 스테가노그래피를 이용하여 정보를 은닉하는 방법은 삽입 기법과 수정 기법이 있다.
삽입 기법은 원문 데이터는 그대로 두고 은닉 정보를 덧붙여 부가하는 방식이고, 수정 기법은 원문 데이터를 눈치 채기 어려운 정도로 교묘히 수정하여 정보를 은닉하는 방식이다.
수정 기법의 경우 원문 데이터를 수정하는 방식이기 때문에 원문 데이터보다 더 많은 정보를 은닉하는 것은 불가능하며,
삽입 기법은 단순히 덧붙이는 방식이라 원문 데이터보다 더 많은 정보를 은닉하는 것도 가능은 하지만, 이 경우 데이터의 크기가 비정상적으로 증가하여 정보 은닉의 효과도 떨어지고 공간효율성도 높다고 볼 수 없다.

<오답 체크> ③ 스테가노그래피의 수정 기법에 대한 설명이다.

답 ②

문 5. 다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은?

① L2TP
② SYN 플러딩
③ PPTP
④ ARP 스푸핑

② **SYN flooding**(SYN 플러딩)
TCP 3-way handshaking을 이용한 DoS공격
공격 대상 서버에 존재하지 않는 IP 주소로 위조한 무수히 많은 SYN패킷을 보낸 뒤 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격방법이다.
SYN 플러딩은 TCP를 활용하는 공격이므로 4계층에서 동작한다.

<오답 체크> ①③ L2TP와 PPTP는 2계층에서 작동하는 VPN 터널링 프로토콜이다.

④ **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.
MAC 주소를 조작하는 공격이기 때문에 2계층에서 작동한다고 봐야 한다.(ARP 프로토콜은 경우에 따라 2계층과 3계층 사이에서 작동한다고 표현하는 경우가 많으므로, 문제에 따라 융통성 있게 풀어야 한다.)

답 ②

문 6. 해시 함수의 충돌에 대한 설명으로 옳은 것은?

① 해시 함수의 입력 메시지가 길어짐에 따라 생성되는 해시 값이 길어지는 것을 의미한다.
② 서로 다른 해시 함수가 서로 다른 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
③ 동일한 해시 함수가 서로 다른 두 개의 입력 값에 대해 동일한 출력 값을 내는 것을 의미한다.
④ 동일한 해시 함수가 동일한 입력 값에 대해 다른 출력 값을 내는 것을 의미한다.

③ 해시에서의 충돌은 (동일한 해시 함수에서) 서로 다른 두 개의 메시지(입력)에 대해 같은 해시값(출력)을 갖는 것을 의미한다.
약한 충돌 내성(weak collision resistance)는 주어진 해시값과 같은 해시값을 갖는 다른 메시지를 찾을 수 없어야 하는 것이고, 강한 충돌 내성(strong collision resistance)는 출력 해시값이 같은 임의의 서로 다른 두 메시지를 찾을 수 없어야 하는 것이다.

<오답 체크> ① 해시 함수는 대부분 입력 메시지의 길이에 상관없이 동일한 길이의 해시값을 생성한다.
② 서로 다른 해시 함수라면 입력 값이 다르더라도 동일한 해시값을 출력하는 게 가능하다. 해시에서의 충돌은 같은 해시 함수로 계산하였을 때를 의미한다.
④ 동일한 해시 함수로 동일한 입력값을 계산한다면, 언제나 동일한 출력값이 나와야 한다. 이것이 보장되지 않는다면, 무결성을 위해 해시 함수를 활용하는 의미가 없다.

답 ③

문 7. 암호화 기법들에 대한 설명으로 옳지 않은 것은?

① Feistel 암호는 전치(Permutation)와 대치(Substitution)를 반복시켜 암호문에 평문의 통계적인 성질이나 암호키와의 관계가 나타나지 않도록 한다.
② Kerckhoff의 원리는 암호 해독자가 현재 사용되고 있는 암호 방식을 알고 있다고 전제한다.
③ AES는 암호키의 길이를 64비트, 128비트, 256비트 중에서 선택한다.
④ 2중 DES(Double DES) 암호 방식은 외형상으로는 DES에 비해 2배의 키 길이를 갖지만, 중간일치공격 시 키의 길이가 1비트 더 늘어난 효과밖에 얻지 못한다.

③ **AES**(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트) – 라운드 키 128비트
키 길이 128비트 – 10라운드
키 길이 192비트 – 12라운드
키 길이 256비트 – 14라운드

<오답 체크> ② 케르크호프스(Kerckhoff)의 원리는 키(key)를 제외한 시스템의 다른 모든 내용이 알려지더라도 암호체계는 안전해야 한다는 것이다. 이 말을 암호체계의 안전성은 오로지 **키의 비밀성에만 의존**해야 하며, 암호 알고리즘을을 포함한 정보를 코딩하고 전송하는 방법이 모든 사람에게 알려지더라도 암호화는 안전해야 한다는 얘기다.
이것을 확인해볼 수 있는 게 우리가 흔히 사용하는 압축 프로그램이다. zip 파일에 비밀번호를 걸어 압축할 때 우리는 알집, 반디집, 윈집 등을 이용한다. 이를 통해 zip 파일 압축 알고리즘은 서로 공유하는 공개된 알고리즘이라는 걸 알 수 있다. 하지만 암호가 걸린 zip 파일을 풀기 위해서는 비밀번호를 알지 못하면 어떤 프로그램으로도 풀 수 없다.

④ 기지 평문 공격과 전사 공격을 이용한 중간일치공격(Meet In The Middle Attack)으로 키를 알아내고자 할 때, 1중 DES에 비해 2중 DES 키의 길이는 56비트에서 112비트로 증가하지만, 암호화에 필요한 계산은 2^{56}에서 2^{57}로 증가할 뿐이다. 이것은 키의 길이가 57비트인 암호화와 동일한 난이도로 1비트 늘어난 수준에 불과하다.

답 ③

▶ 기지 평문 공격(한 쌍의 평문과 암호문을 알고 있을 때)과 전사 공격(brute-force attack)을 이용한 중간일치공격

2중 DES는 56비트 키의 DES 암호화를 두 번 적용하는 것으로, 2×56 = 112비트의 키를 사용한다.
(이 때 암호화 키 k1, k2라 하고, 입수한 평문 M, 그에 대응하는 암호문은 C, 중간 암호문은 X라고 하자)

2중 DES의 암호화 작동 방식은
M –(k1로 암호화)-> **X** –(k2로 암호화)-> C

복호화 작동 방식은
M <-(k1로 복호화)- **X** <–(k2로 복호화)- C

1. 평문 M을 가능한 모든 키로 암호화를 하여 결과값을 테이블에 저장한다 (2^{56}번 수행) -> 결과값 테이블 1
   테이블1에 저장된 값들은 모두 평문을 1차 암호화한 중**간 암호문 X**들이다.
2. 암호문 C를 가능한 모든 키로 복호화하여 결과값을 테이블 저장한다 (2^{56}번 수행) -> 결과값 테이블 2
   테이블2에 저장된 값들은 모두 암화문을 1차 복호화한 **중간 암호 X**문들이다.
3. 테이블1에는 (M, k1, X)의 쌍, 테이블2에는 (X, k2, C)의 쌍이 들어있다. 두 테이블을 정렬·비교하여 같은 X를 가지는 키 쌍(k1, k2)을 추려낸다.
   (이 과정에서도 100번 이상의 연산이 수행되지만, 1, 2번의 연산 횟수에 비해 매우 적으므로 무시한다)
4. 추려낸 키 쌍을 이용해 실제 평문을 암호화·복호화를 수행하여 검증한다. 이로써 실제 암호화 키 k1과 k2를 알 수 있다.

이를 통해 키의 길이는 112비트이지만, 전체 $2^{56} + 2^{56} = 2^{57}$번의 암호화 연산만으로 충분하다는 것을 알 수 있다.

문 8. 디지털 포렌식에 대한 설명에서 ㉠, ㉡에 들어갈 용어는?

> (㉠) 공간은 물리적으로 파일에 할당된 공간이지만 논리적으로 사용할 수 없는 낭비 공간이기 때문에, 공격자가 의도적으로 정보를 은닉할 가능성이 있다. 또한, 이전에 저장 되었던 데이터가 남아 있을 가능성이 있어 파일 복구와 삭제된 파일의 파편 조사에 활용할 수 있다. 이 때, 디지털 포렌식의 파일 (㉡) 과정을 통해 디스크 내 비구조화된 데이터 스트림을 식별하고 의미 있는 내용을 추출할 수 있다.

㉠	㉡
① 실린더(Cylinder)	역어셈블링(Disassembling)
② MBR(Master Boot Record)	리버싱(Reversing)
③ 클러스터(Cluster)	역컴파일(Decompiling)
④ 슬랙(Slack)	카빙(Carving)

㉠ **슬랙**(Slack) 공간

물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간을 말한다. 물리적으로는 파일에 할당된 공간이지만 논리적으로는 사용할 수 없는 공간으로, 슬랙 공간에 정보를 은닉할 수 있고 파일의 복구 및 삭제된 파일의 파편조사 시 유용하게 사용할 수 있다.

램 슬랙, 드라이브 슬랙, 파일시스템 슬랙, 볼륨 슬랙 등

㉡ 카빙(Carving)

메타 데이터가 아닌 파일 자체의 바이너리 데이터(시그니처, 헤더, 푸터 등)를 이용해 디스크의 비할당 영역에서 파일을 복구하는 기법

시스템에서 파일을 삭제하면 메타 데이터만을 삭제하고 실제 데이터는 남아있는데, 이 데이터를 분석·결합하여 본래의 형태로 복구할 수 있다.

<오답 체크> ① **역어셈블링**(Dissembling)

어셈블러와 반대로, 기계어를 어셈블리어로 변환하는 것

② MBR(Master Boot Record)

주기억장치에 운영체제를 적재하기 위해 운영체계가 어디에, 어떻게 위치해 있는지를 나타내는 정보로서 디스크 첫 번째 섹터에 저장되어 있다.

▷ **리버싱**(Reversing) = **리버스 엔지니어링**(Reverse Engineering, 역공학)

완성된 프로그램을 역으로 분석하여 내부의 설계나 작동 원리 등을 이해하는 과정. 넓은 의미론느 이를 통해 단점을 보완하고 새로운 아이디어를 추가하는 등의 일련의 작업까지 의미한다.

③ **역컴파일링**(Decompiling)

컴파일러와 반대로, 저급 언어를 고급 언어로 변환하는 것

답 ④

문 9. 버퍼 오버플로우 공격 대응 방법 중 ASLR(Address Space Layout Randomization)에 대한 설명으로 옳은 것은?

① 함수의 복귀 주소 위조 시, 공격자가 원하는 메모리 공간의 주소를 지정하기 어렵게 한다.

② 함수의 복귀 주소와 버퍼 사이에 랜덤(Random) 값을 저장하여 해당 주소의 변조 여부를 탐지한다.

③ 스택에 있는 함수 복귀 주소를 실행 가능한 임의의 libc 영역 내 주소로 지정하여 공격자가 원하는 함수의 실행을 방해한다.

④ 함수 호출 시 복귀 주소를 특수 스택에 저장하고 종료 시 해당 스택에 저장된 값과 비교하여 공격을 탐지한다.

① **ASLR**(Address Space Layout Randomization)

메모리상의 공격을 어렵게 하기 위해 스택이나 힙, 라이브러리 등의 주소를 랜덤으로 프로세스 주소 공간에 배치함으로써 실행할 때 마다 데이터의 주소가 바뀌게 하는 방법이다.

데이터의 주소가 매번 바뀌기 때문에 공격자가 악성코드를 심어놓은 주소로 조작하는 것을 어렵게 만들어 준다.

<오답 체크> ② **Stack Guard**(스택 가드)

메모리의 특정한 위치(ret 앞)에 카나리(canary)라는 특정한 값을 집어넣어, 프로그램 실행시 해당 카나리 값이 변조되었을 경우 스택 영역이 변조되었다고 판단하여 프로그램을 종료하는 방법이다.

③ **RTL**(Return-to-Libc) 공격

버퍼 오버플로우에 대한 대응책이 아니고, 반대로 버퍼 오버플로우를 예방책을 우회하기 위한 해커의 공격법에 대한 설명이다.

먼저 버퍼 오버플로우 방어 기법 중, 스택에서 코드가 실행되지 않도록 NX-bit 비트를 설정하는 Non-Executable Stack 기법이 있다.

공격자는 이 방어 기법을 우회하기 위해 libc 표준 공용 라이브러리를 이용한다. libc 는 공용 라이브러리이기 때문에 실행이 가능한데, 공격자는 함수의 복귀 주소를 libc 내의 영역으로 지정하여 원하는 함수가 실행되도록 할 수 있다.

④ **Stack Shield**(스택 쉴드)

스택 쉴드는 프로그램 반환 주소를 안전한 공간에 복사해두고, 함수가 종료될 때 현재 스택의 리턴 반환 주소와 복사해둔 반환 주소를 비교하여 변조되었는지 확인하는 탐지 방법이다.

답 ①

문 10. 국내의 기관이나 기업이 정보 및 개인정보를 체계적으로 보호할 수 있도록 통합된 관리체계 인증제도는?

① PIPL - P
② ISMS - I
③ PIMS - I
④ ISMS - P

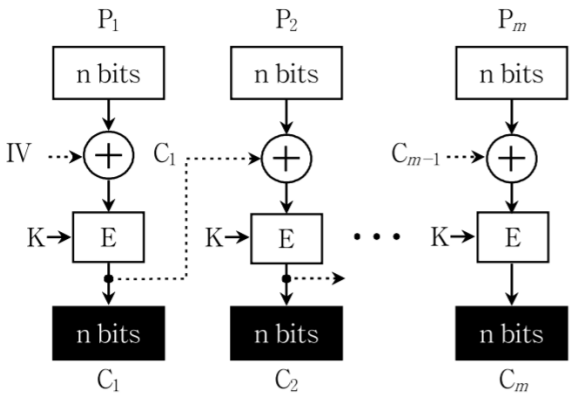
◈ **ISMS-P**(정보보호 및 개인정보보호 관리체계 인증)
기존의 ISMS와 PIMS를 통합한 것으로, 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도로, 2018년 말부터 시행되었다. 2019년 5월 삼성증권이 최초로 ISMS-P인증을 취득하였으며, 2019년 7월 16일 롯데면세점이 면세업계 최초로 취득하였다.

⇨ 정책기관: 과학기술정보통신부, 방송통신위원회, 행정안전부
⇨ 인증기관: 한국인터넷증흥원(KISA) (+ 금융보안원 신규 지정)

답 ④

구분		통합인증	분야(인증기준 개수)
ISMS-P	ISMS	1 관리체계 수립 및 운영(16)	1.1 관리체계 기반 마련(6) 1.2 위험관리(4) 1.3 관리체계 운영(3) 1.4 관리체계 점검 및 개선(3)
		2 보호대책 요구사항(64)	2.1 정책, 조직, 자산 관리(3) 2.2 인적보안(6) 2.3 외부자 보안(4) 2.4 물리보안(7) 2.5 인증 및 권한 관리(6) 2.6 접근통제(7) 2.7 암호화 적용(2) 2.8 정보시스템 도입 및 개발 보안(6) 2.9 시스템 및 서비스 운영관리(7) 2.10 시스템 및 서비스 보안관리(9) 2.11 사고 예방 및 대응(5) 2.12 재해복구(2)
	-	3 개인정보 처리단계별 요구사항(22)	3.1 개인정보 수집 시 보호조치(7) 3.2 개인정보 보유 및 이용 시 보호조치(5) 3.3 개인정보 제공 시 보호조치(3) 3.4 개인정보 파기 시 보호조치(4) 3.5 정보주체 권리보호(3)

문 11. 다음의 블록 암호 운용 모드는?



E: 암호화 K: 암호화 키
$P_1, P_2, \ldots, P_m$: 평문 블록
$C_1, C_2, \ldots, C_m$: 암호 블록
IV: 초기화 벡터 ⊕ : XOR

① 전자 코드북 모드(Electronic Code Book Mode)
② 암호 블록 연결 모드(Cipher Block Chaining Mode)
③ 암호 피드백 모드(Cipher Feedback Mode)
④ 출력 피드백 모드(Output Feedback Mode)

그림을 보면 이전 단계의 암호문 블록과 다음 단계의 평문 블록을 먼저 XOR 한 다음에 암호화하고 있다. 이것은 CBC 모드 방식이다.

답 ②

◈ **ECB**(electronic codebook, 전자 코드북) 모드
가장 간단한 구조로, 암호화하려는 메시지를 여러 블록으로 나누어 각각 암호화하는 방식이다.

◈ **CBC**(cipher-block chaining, 암호 블록 체인) 모드
평문 블록을 이전 단계의 암호문 블록과 XOR 한 후 암호화한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.
초기화 벡터가 같은 경우 출력 결과가 같기 때문에, 매 암호화마다 다른 초기화 벡터를 사용해야 한다.

◈ **CFB**(cipher feedback, 암호 피드백) 모드
CBC의 변형으로, 이전 단계의 암호문 블록을 암호화한 후 현재의 평문 블록과 XOR 한다.
첫 번째 평문 블록의 경우에는 초기화 벡터(IV)를 암호화한 것과 XOR 한다.

◈ **OFB**(output feedback, 출력 피드백) 모드
초기화 벡터(IV)를 매 단계마다 암호화해가며 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

◈ **CTR**(Counter, 카운터) 모드
1씩 증가하는 카운터 값을 암호화하여 스트림 암호를 생성한 후, 생성한 스트림 암호와 평문 블록을 XOR하여 암호문 블록을 생성한다.

문 12. 무결성을 위협하는 공격이 아닌 것은?

① 스누핑 공격(Snooping Attack)
② 메시지 변조 공격(Message Modification Attack)
③ 위장 공격(Masquerading Attack)
④ 재전송 공격(Replay Attack)

① **스누핑**(snooping)
네트워크 상에 떠도는 중요 정보들을 몰래 획득하는 행위. 소극적 공격 및 기밀성을 위협하는 공격에 해당한다.
스니핑(sniffing)과의 차이점은 스니핑은 다른 사람들 사이에 오가는 패킷을 중간에서 엿듣는 것이라면, 스누핑은 네트워크 상에 남아있는 공격 대상자의 활동 내역 및 흔적들을 탐색하는 것이다. 스니핑이 상대방 차에 도청장치를 심는 것이라면, 스니핑은 미행하고 뒷조사를 하는 것이다.

<오답 체크> ②③④는 모두 적극적 공격 및 무결성을 위협하는 공격에 해당한다.

답 ①

문 13. 다음에서 설명하는 접근 제어 모델은?

> 군사용 보안구조의 요구사항을 충족시키기 위해 개발된 최초의 수학적 모델로 알려져 있다. 불법적 파괴나 변조보다는 정보의 기밀성 유지에 초점을 두고 있다. '상위레벨 읽기금지 정책(No-Read-Up Policy)'을 통해 인가받은 비밀 등급이 낮은 주체는 높은 보안 등급의 정보를 열람할 수 없다. 또한, 인가받은 비밀 등급 이하의 정보 수정을 금지하는 '하위레벨 쓰기금지 정책(No-Write-Down Policy)'을 통해 비밀 정보의 유출을 차단한다.

① DAC(Discretionary Access Control) 모델
② Bell-LaPadula 모델
③ Biba 모델
④ RBAC(Role-Based Access Control) 모델

최초의 수학적 모델로서 기밀성에 초점을 둔 모델은 벨 라파듈라(BLP, Bell-LaPadula) 모델이다.

② **벨 라파듈라**(BLP, Bell-LaPadula) 모델
기밀성을 중시한 모델
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star(*) 속성 – NWD(No Write Down)

<오답 체크> ① **DAC**(Discretionary Access Contro, 임의적 접근 제어)
정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

③ **비바**(Biba) 모델
무결성을 중시한 모델
높은 등급의 데이터에 쓸 수 없고, 낮은 등급의 데이터를 읽을 수 없다.
단순 무결성 속성 - NRD(No Read Down)
무결성 star(*) 속성 - NWU(No Write Up)

④ **RBAC**(Role Based Access Control, 역할 기반 접근 제어)
정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

답 ②

문 14. 유럽의 일반개인정보보호법(GDPR)에 대한 설명으로 옳은 것은?

① EU 회원국들 간 개인정보의 자유로운 이동을 금지하기 위한 목적을 갖는다.
② 그 자체로는 EU의 모든 회원국에게 직접적인 법적 구속력을 갖지 않는다.
③ 중요한 사항 위반 시 직전 회계연도의 전 세계 매출액 4 % 또는 2천만 유로 중 높은 금액이 최대한도 부과 금액이다.
④ 만 19세 미만 미성년자의 개인정보 수집 시 친권자의 동의를 얻어야 한다.

③ 일반적 사항 위반 시 전 세계 **매출액 2% 또는 1천만 유로** 중 높은 금액
중요한 사항 위반 시 전 세계 **매출액 4% 또는 2천만 유로** 중 높은 금액

<오답 체크> ① EU 회원국 전체에 동일하게 강화된 개인정보 보호 제도를 마련함으로써, 회원국들 간 보다 자유롭게 정보를 이동하고, 제3국 및 국제기구로 보다 쉽게 개인정보를 이전하기 위한 목적으로 마련되었다.

② GDPR은 모든 회원국이 의무적으로 준수해야 하는 강행규정이므로 그 자체로 법적 구속력을 갖는다.

④ **만 16세** 미만의 아동에게 온라인 서비스 제공 시 친권자의 동의를 얻어야 하며, 각 회원국이 법률로 **만 13세** 미만까지 규정을 낮추는 것이 가능하다.

답 ③

◈ GDPR(General Data Protection Regulation)
2018년 5월 25일부터 시행된 EU(유럽연합)의 개인정보보호 법령이며, 유럽 연합(EU)내의 개인정보 보호를 강화하고 회원국간 자유로운 이동을 보장하는 내용을 포함하는 규제이다. 동 법령 위반시 과징금 등 행정처분이 부과될 수 있어 EU와 거래하는 우리나라 기업도 이 법에 위반되지 않도록 주의할 필요가 있다.

▷▶ 주요 변화
→ 이전 EU 지침은 권과 차원의 규정인 데 반해, GDPR은 모든 회원국이 의무적으로 준수해야 하는 강행규정이다. 위반 시 과징금 부과
→ EU 내 사업장을 운영하는 기업뿐만 아니라 전자상개래 등을 통해 해외에서 EU 주민의 개인정보를 처리하는 기업에도 적용
→ 개인정보책임자(DPO) 지정 등 기업의 책임성을 강화하는 내용과 정보이동권 등 정보주체의 권리를 강화하는 내용이 추가

▷▶ 아래 어느 하나에 해당하는 기업으로서 EU 주민의 개인정보를 처리하는 경우에는 한국기업도 적용 대상임
→ EU에 사업장을 운영하는 기업(지점, 판매소, 영업소 등)
→ EU 지역에 사업장은 없지만, 인터넷 홈페이지를 통해 EU에 거주하는 주민에게 물품·서비스를 제공하는 기업
예) 현지어로 마케팅 활동을 하거나 현지 통화로 결제하는 경우
→ EU 주민의 행동을 모니터 하는 기업

▷▶ 특히 아래에 해당하는 기업은 특별한 주의를 요함
→ EU 주민의 민감한 정보(건강, 유전자, 범죄경력 등)를 처리하거나, 아동의 정보를 처리하는 기업
→ 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링을 하는 기업 (예 : CCTV)

▷▶ GDPR에 따른 기업의 책임강화
→ 처리제한권(신설)
정보주체는 본인에 관한 개인정보의 처리를 차단하거나 제한을 요구할 권리를 가짐
→ 정보이동권(신설)
정보주체는 본인의 개인정보를 본인 또는 다른 사업자에게 전송토록 요구할 권리를 가짐
→ 삭제권(강화)
정보주체는 본인에 관한 개인정보 삭제를 요구할 권리를 가짐
→ 프로파일링 거부권 (강화)
정보주체는 본인에게 중대한 영향을 미치는 사안에 대해 프로파일링 등 자동화된 처리에 의한 결정을 반대할 권리를 가짐

▷▶ 법 위반시 과징금 수준
→ 일반적 위반 사항(대리인 미지정 위반 등)
전 세계 매출액 2% 또는 1천만 유로(약 125억원) 중 높은 금액
→ 중요한 위반 사항(국외 이전 규정 위반 등)
전 세계 매출액 4% 또는 2천만 유로(약 250억원) 중 높은 금액

문 15. IPsec의 캡슐화 보안 페이로드(ESP) 헤더에서 암호화되는 필드가 아닌 것은?

① SPI(Security Parameter Index)
② Payload Data
③ Padding
④ Next Header

ESP 헤더에서 암호화되는 필드는 Payload Data, Padding, Pad Length, Next Header이다.

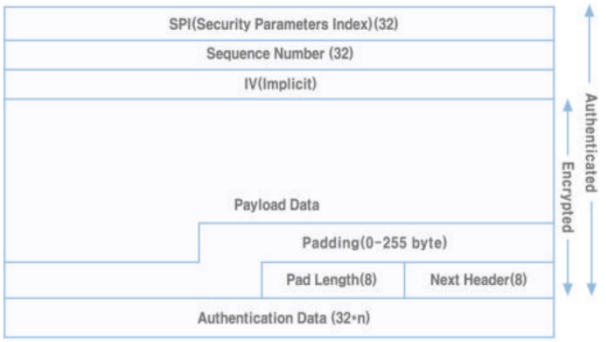
① SPI(Security Parameter Index) 필드
임의의 32비트 값으로, 목적지 IP 주소와 함께 쓰여서 사용할 SA(Security Association)를 결정하는 역할을 한다.

<오답 체크> ② Payload Data 필드
Next Header 필드가 설명하는 가변길이의 필드이다.

③ Padding필드
암호화 연산을 수행하기 위해 또는 실제 데이터의 길이를 숨기기 위해, 전체 데이터 길이가 블록 크기의 정수배가 되도록 추가하는 비트열이다.

④ Next Header 필드
8비트의 길이로, ESP 헤더 다음에 나오는 페이로드(payload)의 종류를 나타낸다.

▶ ESP 헤더 구조



답 ①

문 16. SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 서버와 클라이언트 간 양방향 통신에 동일한 암호화 키를 사용한다.
② 웹 서비스 이외에 다른 응용 프로그램에도 적용할 수 있다.
③ 단편화, 압축, MAC 추가, 암호화, SSL 레코드 헤더 추가의 과정으로 이루어진다.
④ 암호화 기능을 사용하면 주고받는 데이터가 인터넷 상에서 도청되는 위험성을 줄일 수 있다.

① 일반적인 단방향 SSL 프로토콜은 서버의 공개키만 사용하여 클라이언트는 서버를 검증하지만, 서버는 클라이언트를 검증하지 않는 문제가 있다.
이러한 불균형을 해소하기 위해, 서버와 클라이언트가 서로의 공개키를 검증하여 핸드셰이킹을 완료하는 것을 **양방향 SSL** 프로토콜이라고 한다.
다만, 이 문제는 '양방향 통신에 사용한다'는 표현이 명확하지 않은 문제가 있다. 여기서 양방향 통신이라는 말이 핸드셰이킹 과정을 의미하는 것인지 서로 데이터를 주고 받는 것을 의미하는 건지 애매하기 때문이다.
SSL 환경에서 실제 데이터를 주고 받는 과정에서는 대칭키(세션키)를 사용하기 때문이다.

<오답 체크> ③ 레코드 프로토콜(SSL Record Protocol) 작동
- 데이터를 동일한 크기의 블록으로 단편화(Fragmentation)
- 각 블록을 압축(Compression)
- 각 블록마다 MAC(Message Authentication Code) 생성
- 각 블록+MAC를 암호화(Encryption)
- SSL Record Protocol 헤더 추가

답 ①

문 17. KCMVP에 대한 설명으로 옳은 것은?

① 보안 기능을 만족하는 신뢰도 인증 기준으로 EAL1 부터 EAL7까지의 등급이 있다.
② 암호 알고리즘이 구현된 프로그램 모듈의 안전성과 구현 적합성을 검증하는 제도이다.
③ 개인정보 보호활동을 체계적.지속적으로 수행하기 위한 관리체계의 구축과 이행 여부를 평가한다.
④ 조직의 정보자산을 효과적으로 보호하고 있는지 평가하여 일정 수준 이상의 기업에 인증을 부여한다.

▶ KCMVP(Korea Cryptographic Module Validation Program, 한국 암호화 모듈 검증 제도)
암호모듈의 안전성과 구현 적합성을 검증하는 제도
시험·평가 기관(전문기관)으로는 한국인터넷진흥원과 국가보안기술연구소가 지정되어 있으며, 국가정보원이 검증하고 있다.

<오답 체크> ① **CC**(Common Criteria, 국제공통평가기준)
국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준
보안 등급 분류: EAL7 ~ EAL1

③ **PIMS**(개인정보보호 관리체계인증)
개인정보를 보호하는 것에 중점을 두어, 기관 및 기업이 개인정보보호 관리체계를 갖추고 체계적·지속적으로 보호 업무를 수행하는지에 대해 객관적으로 심사하여 기준 만족 시 인증을 부여하는 제도

④ **ISMS**(정보보호관리체계인증)
기업이 주요 정보자산을 보호하기 위해 수립 · 관리 · 운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도

답 ②

문 18. 「개인정보 보호법」상 개인정보 분쟁조정위원회에 대한 설명으로 옳지 않은 것은?

① 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다.
② 위원장은 행정안전부·방송통신위원회·금융위원회 및 개인정보보호위원회의 고위공무원단에 속하는 일반직공무원 중에서 위촉한다.
③ 분쟁조정위원회는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
④ 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

② **제40조**(설치 및 구성) ④항
위원장은 위원 중에서 **공무원이 아닌 사람**으로 보호위원회 위원장이 위촉한다.

<오답 체크> ① **제40조**(설치 및 구성) ②항
③ **제40조**(설치 및 구성) ⑦항
④ **제41조**(위원의 신분보장)

답 ②

제40조(설치 및 구성)
① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.
② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.
③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.
1. 개인정보 보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보 보호업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사 · 검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람
④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 위촉한다.
⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.
⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.
⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.
⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

제41조(위원의 신분보장)
위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

문 19. 전자화폐 및 가상화폐에 대한 설명으로 옳지 않은 것은?

① 전자화폐는 전자적 매체에 화폐의 가치를 저장한 후 물품 및 서비스 구매 시 활용하는 결제 수단이며, 가상화폐는 전자화폐의 일종으로 볼 수 있다.
② 전자화폐는 발행, 사용, 교환 등의 절차에 관하여 법률에서 규정하고 있으나, 가상화폐는 별도로 규정하고 있지 않다.
③ 가상화폐인 비트코인은 분산원장기술로 알려진 블록체인을 이용한다.
④ 가상화폐인 비트코인은 전자화폐와 마찬가지로 이중지불(Double Spending)문제가 발생하지 않는다.

④ 가상화폐와 전자화폐 모두 이중지불 문제는 존재한다.

특히 전자화폐는 거래 중간에 신뢰성 있는 기관(은행)이 개입하기 때문에 이중지불이 발생할 가능성을 현저히 낮출 수 있으나, 중개기관 없이 당사자간 1대1로 거래하는 가상화폐의 경우 이중지불 문제는 매우 주요한 이슈이다.

작년 캐나다 중앙은행은 블록체인 네트워크의 이중지불 문제는 현실성이 없다는 결과를 발표하였지만, 올해 초 최소 5개의 가상화폐에서 이중지불 사이버 범죄가 발생하였다.

51% 공격(51% attack)을 이용한 범죄였는데, 사이버 범죄 조직이 대규모 집단을 구성하여 블록체인의 전체 노드 중 50%를 초과하는 해시 연산력을 확보하여, 다른 정상적인 노드들보다 따른 속도로 신규 블록을 생성하여 거래 정보를 조작함으로써 이익을 얻는 공격이다. 이는 주로 네트워크 참여자의 수가 많지 않은 신생 가상화폐들을 대상으로 한다.

<오답 체크> ① 전자화폐는 IC카드 또는 네트워크에 연결된 컴퓨터에 은행예금이나 돈 등이 전자적 방법으로 저장되어 현금을 대체하는 전자 지급 수단을 말한다. 엄밀히 말하면 실물 화폐를 전자적인 방법으로 주고 받는 것이다.

가상화폐는 컴퓨터 등에 정보 형태로 남아 실물 없이 사이버상으로만 거래되는 화폐로, 전자화폐의 일종으로 본다.

② 전자화폐는 역사가 오래 되었고 널리 통용되는 만큼 진작부터 법률이 마련되어 왔다. 우리나라는 「전자금융거래법」에 규정되어 있다. 반면 가상화폐는 아직 제대로 된 별도의 규정이 마련되어 있지 않다.

답 ④

문 20. X.509 인증서(버전 3)의 확장(Extensions) 영역에 포함되지 않는 항목은?

① 인증서 정책(Certificate Policies)
② 기관 키 식별자(Authority Key Identifier)
③ 키 용도(Key Usage)
④ 서명 알고리즘 식별자(Signature Algorithm Identifier)

◈ 인증서의 기본 영역
(1) 버전 (2) 일련번호
(3) 서명 알고리즘 (4) 발급자
(5) 유효기간 (6) 주체
(7) 공개키

◈ 인증서의 확장 영역
(1) 기관 키 식별자 (2) 주체 키 식별자
(3) 주체 대체 이름 (4) CRL 배포 지점
(5) 기관 정보 액세스 (6) 키 사용 용도
(7) 인증서 정책 (8) 손도장 알고리즘
(9) 손도장

답 ④