2016년 서울시 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

1. 다음 중 X.509 v3 표준 인증서에 포함되지 않는 것은?

① 인증서의 버전(Version)
② 서명 알고리즘 식별자(Signature Algorithm ID)
③ 유효기간(Validity Period)
④ 디렉토리 서비스 이름(Directory Service Name)

답 ④

◈ Certificate(인증서) 구조
Version: 인증서의 버전 <--- ①
Serial Number: CA가 할당한 정수로 된 고유 번호
Signature Algorithm ID: 서명 알고리즘 식별자 <--- ②
Issuer Name: 발행자
Validity period: 유효기간 <--- ③
  Not Before: 유효기간 시작 날짜
  Not After: 유효기간 끝나는 날짜
Subject name: 소유자
Subject Public Key Info: 소유자 공개 키 정보
  Public Key Algorithm: 공개키 알고리즘
  Subject Public Key: 소유자 공개키
Issuer Unique Identifier (Optional): 발행자 고유 식별자
Subject Unique Identifier (Optional): 소유자 고유 식별자
Extensions (Optional): 확장
Certificate Signature Algorithm: 인증서 서명 알고리즘
Certificate Signature: 인증서 서명

2. 다음 중 성격이 다른 공격 유형은?

① Session Hijacking Attack
② Targa Attack
③ Ping of Death Attack
④ Smurf Attack

답 ①

①번은 사용자의 세션을 가로채어 다른 사용자로 위장해 서버에 접속하는 공격이며, 나머지 ②③④번은 서버를 마비시키는 서비스 거부 공격(DoS)이다.

① **세션 하이재킹**(Session Hijacking) 공격
시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채기 하는 공격이다.

<오답 체크> ② **Targa** 공격(Targa Attack)
IP가 정상적으로 패킷을 전송할 때 IP 단편화가 발생하게 되면 재조립 시에 정확한 조립을 위해 오프셋 값을 더하게 되어있는데, 정상적인 오프셋 값보다 더 큰 값을 더하도록 조작하여 오버플로우를 일으켜 시스템의 기능을 마비시켜 버리는 DoS 공격기법이다.

③ **Ping of Death** 공격
Icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다. 크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)화 되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

④ **Smurf** 공격(ICMP flooding)
공격대상 호스트의 IP주소로 위장된 소스 IP주소의 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상이 많은 양의 ICMP Echo 응답 패킷을 받게 만들어 시스템의 자원을 고갈시킨다.

3. Stack에 할당된 Buffer overflow Attack에 대응할 수 있는 안전한 코딩(Secure Coding) 기술의 설명으로 옳지 않은 것은?

① 프로그램이 버퍼가 저장할 수 있는 것보다 많은 데이터를 입력하지 않는다.
② 프로그램은 할당된 버퍼 경계 밖의 메모리 영역은 참조 하지 않으므로 버퍼 경계 안에서 발생될 수 있는 에러를 수정해 주면 된다.
③ gets()나 strcpy()와 같이 버퍼 오버플로우에 취약한 라이브러리 함수는 사용하지 않는다.
④ 입력에 대해서 경계 검사(Bounds Checking)를 수행해 준다.

답 ②

버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
② 오버플로우가 발생하면 버퍼 경계 밖의 메모리 영역을 참조하게 되므로 경계 밖의 에러도 수정해줘야 한다.

<오답 체크>

③④ 버퍼 오버플로우 공격에 대한 대응책으로, 오버플로우 공격에 취약한 표준 라이브러리 함수를 사용하지 않고, 버퍼 경계 검사를 수행한다.
strcpy(), strcat(), gets(), sprintf() 등의 표준 C라이브러리는 버퍼의 경계 검사를 하지 않아 오버플로우 공격에 취약하다.

4. 전자화폐(Electronic Cash)에 대한 설명으로 옳지 않은 것은?

① 전자화폐의 지불 과정에서 물품 구입 내용과 사용자 식별 정보가 어느 누구에 의해서도 연계되어서는 안 된다.
② 전자화폐는 다른 사람에게 즉시 이전할 수 있어야 한다.
③ 일정한 가치를 가지는 전자화폐는 그 가치만큼 자유롭게 분산이용이 가능해야 한다.
④ 대금 지불 시 전자화폐의 유효성 확인은 은행이 개입하여 즉시 이루어져야 한다.

답 ④

④ 전자화폐의 유효성 확인을 위해 은행이 개입할 필요가 없다.

5. Linux system의 바이너리 로그파일인 btmp(솔라리스의 경우는 loginlog 파일)를 통해 확인할 수 있는 공격은?

① Password Dictionary Attack
② SQL Injection Attack
③ Zero Day Attack
④ SYN Flooding Attack

답 ①

리눅스의 btmp 로그에는 로그인 실패 기록에 대한 정보가 포함되어 있으며, loginlog 파일에는 로그인 시 5번 이상 실패할 경우의 정보가 기록된다.

① **사전 공격**(Password Dictionary Attack)
사용자가 설정하는 대부분의 패스워드에 특정 패턴이 있음을 착안한 방법으로 패스워드로 사용할 만한 것을 사전으로 만들어놓고 이를 하나씩 대입하여 일치 여부를 확인하는 방법이다.
사전 공격은 계속 로그인을 시도하는 방식이기 때문에 로그인 실패 기록이 남게 된다.

<오답 체크> ② **SQL 삽입**(SQL 인젝션, SQL injection)
클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격하는 것이다.

③ **제로데이**(Zero Day) 공격은 운영체제나 소프트웨어의 보안 취약점에 대한 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법이다.

④ **SYN flooding**
TCP 3-way handshaking을 이용한 DoS공격으로, 공격 대상 서버에 무수히 많은 SYN패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격이다.
서버의 자원을 낭비시키고 가용성을 떨어뜨려 서비스 불능 상태에 빠뜨리는 것이 목적이다.

6. 다음 바이러스 발전 단계에 따른 분류에 대한 설명으로 옳지 않은 것은?

① 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.
② 암호화 바이러스는 바이러스 프로그램 전체 또는 일부를 암호화시켜 저장하는 바이러스이다.
③ 갑옷형 바이러스는 백신 개발을 지연시키기 위하여 다양한 암호화 기법을 사용하는 바이러스이다.
④ 매크로 바이러스는 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스이다.

답 ①

① 원시형 바이러스는 가변 크기가 아닌, 고정 크기를 갖는 단순한 바이러스이다.

- 1세대 **원시형 바이러스**(Primitive Virus)
  프로그램 구조가 단순하고 고정 크기를 가지며, 분석이 상대적으로 쉬운 바이러스
- 2세대 **암호화 바이러스**(Encryption Virus)
  백신 프로그램이 진단할 수 없도록 바이러스 프로그램의 일부 또는 대부분을 암호화시킨 바이러스
- 3세대 **은폐형 바이러스**(Stealth Virus)
  자신을 은폐하고 사용자나 백신 프로그램에 거짓 정보를 제공하기 위해서 다양한 기법을 사용하는 바이러스
  감염된 파일의 길이가 증가하지 않은 것처럼 보이게 하고, 백신 프로그램에게 감염되기 전의 내용을 보여줘 바이러스가 없는 것처럼 속인다.
- 4세대 **갑옷형 바이러스**(Armour Virus)
  백신 프로그램으로부터 숨기보다는 여러 단계의 암호화와 다양한 기법을 동원하여 바이러스 분석을 어렵게 하고 백신 프로그램 개발을 지연시키며, 암호화를 푸는 부분조차 감염될 때마다 달라진다.
- 5세대 **매크로 바이러스**(Macro virus)
  매크로 기능이 있는 MS 사 오피스 제품군(워드, 엑셀, 파워포인트)이외에 비지오(Visio), 오토캐드(AutoCAD) 등 매크로 기능이 있는 응용 소프트웨어 안에서 실행되는 바이러스

7. 공개키 기반구조(Public Key Infrastructure, PKI)를 위한 요소 시스템으로 옳지 않은 것은?

① 인증서와 인증서 폐지 목록을 공개하기 위한 디렉토리
② 사용자 신원을 확인하는 등록기관
③ 인증서 발행업무를 효율적으로 수행하기 위한 인증기관 웹 서버
④ 인증서를 발행 받는 사용자(최종 개체)

답 ③

③ 보통 공개키 기반구조의 구성요소로는 인증서, 인증기관(CA), 등록기관(RA), 저장소(디렉터리), 사용자를 말하며, 웹 서버는 포함되지 않는다.

※ 공개키 기반구조(PKI) 구성 요소
- 인증서(Certificate)
  공개키나 공개키의 정보를 포함하는 인증서
  주로, X.509 v3 표준 형식에 기반함
- 인증 기관(CA, Certification Authority)
  공개키 인증서와 인증서 폐기목록을 생성하고 발급한다.
  공개키에 대한 공신력있는 인증기관
- 등록 기관(RA, Registration Authority)
  인증기관과 사용자 사이에서 사용자 신분 확인, 인증서 발급을 중개, 전달한다.
  신원확인, 고객데이터 유지 등 인증기관의 확인 업무를 대행하며, 사용자의 인증서 발급 요청을 등록한다.
- 저장소(Repository)
  공개된 저장소 역할 (저장 및 검색 등)
  DAP 및 LDAP 등을 이용하여 X.500 디렉토리 서비스를 제공
- 인증서 관리 시스템
- 사용자(Client)

8. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header 에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호
③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간

답 ④

④ TCP 헤더 필드는
포트 번호, 순서 번호, 확인응답/승인 번호, 헤더 길이, 제어 플래그 비트, 윈도우 크기, 검사합(체크섬), 긴급 포인터, 옵션으로 구성되어 있다.
패킷의 생성 시간은 포함되어 있지 않다.

9. 아래 <보기>의 지문은 신문에서 발췌한 기사이다. 빈칸에 들어갈 단어로 적절한 것은?

< 보 기 >

취업준비생 김다정(28)씨는 지난 5월 7일 ☐공격으로 취업을 위해 모아뒀던 학습 및 준비 자료가 모두 암호화돼 버렸다. 컴퓨터 화면에는 암호를 알려주는 대가로 100달러(약 11만 5000원)를 요구하는 문구가 떴지만, 결제해도 데이터를 되찾을 수 없다는 지인의 조언에 데이터복구 업체를 통해 일부 자료만 복구해 보기로 했다. 그런데 업체를 통해 데이터 일부를 복구한 지 하루 만인 지난 10일 또 다시 공격을 받아 컴퓨터가 먹통이 돼 버렸다.

① 하트블리드(Heart bleed)
② 랜섬웨어(Ransomware)
③ 백오리피스(Back Orifice)
④ 스턱스넷(Stuxnet)

답 ②

② **랜섬웨어**(Ransomware)
인질의 몸값을 뜻하는 ransom과 제품을 뜻하는 ware의 합성어로, 컴퓨터에 감염시켜 사용자의 파일을 암호화한 뒤 인질로 잡아 금전을 요구하는 악성 프로그램이다.

<오답 체크> ① **하트블리드**(HeartBleed)
2014년 4월 OpenSSL 1.0.1 버전에서 발견된 매우 심각한 버그
OpenSSL을 구성하고 있는 TLS/DTLS의 HeartBeat 확장규격에서 발견된 취약점으로, 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취할 수 있다.

③ **백오리피스**(Back Orifice)
원격 관리를 위하여 고안된 컴퓨터 프로그램으로, 사용자가 원격지로부터 실행중인 마이크로소프트 윈도 운영 체제를 조작 가능하게 한다.

④ **스턱스넷**(Stuxnet)
독일 지멘스사의 원격 감시 제어 시스템인 SCADA의 제어 소프트웨어 및 장비를 공격한다. 스턱스넷은 산업시설을 감시하고 파괴하는 악성 소프트웨어로는 최초이다.

10. 다음 중 Cipher Block Chaining 운용 모드의 암호화 수식을 제대로 설명한 것은? (단, P_i는 i번째 평문 블록을, C_i는 i번째 암호문 블록을 의미한다.)

① $C_i = E_k(P_i)$
② $C_i = E_k(P_i \oplus C_{i-1})$
③ $C_i = E_k(C_{i-1}) \oplus P_i$
④ $C_i = E_k(P_i) \oplus C_{i-1}$

답 ③

③ **CBC**(cipher-block chaining, 암호 블록 체인) 모드는 평문 블록을 이전 단계의 **암호문 블록과 XOR 한 후 암호화**한다. 첫 번째 평문 블록의 경우에는 초기화 벡터(IV)와 XOR 한 후 암호화한다.

<오답 체크> ① ECB(electronic codebook, 전자 코드북) 모드
블록으로 나누어 각각 암호화하는 방식

③ CFB(cipher feedback, 암호 피드백) 모드
이전 단계의 **암호문 블록을 암호화한 후 현재의 평문 블록과 XOR**한다.

④ 현재의 평문 블록을 암호화한 후 이전 단계의 암호문 블록과 XOR하는 수식인데, 존재하지 않는 방식이다.
③번의 CFB 모드와 혼동하도록 만든 수식이다.

문 11. 보안 공격에 대한 설명으로 옳지 않은 것은? 11. 공통평가기준(Common Criteria, CC)에 대한 설명 중 옳지 않은 것은?

① 보호프로파일(Protection Profile)과 보안목표명세서(Security Target) 중 제품군에 대한 요구사항 중심으로 기술되어 있는 것은 보안목표명세서(Security Target)이다.
② 평가대상에는 EAL 1에서 EAL 7까지 보증등급을 부여할 수 있다.
③ CC의 개발은 오렌지북이라는 기준서를 근간으로 하였다.
④ CC의 요구사항은 class, family, component로 분류한다.

답 ①

① 제품군에 대한 요구사항을 기술한 것은 보호프로파일(PP, Protection Profile)이다.
보안목표명세서(ST, Security Target)은 특정 제품에 대한 보안 명세를 정의한 것이다. ST는 PP를 포함한다.

<오답 체크> ④ CC에서는 보안 요구를 기능과 보증이라는 2개의 측면으로 나누어 정의한다.
각 기능 및 보증 요구는 사용자로 하여금 원하는 보안 요구사항을 쉽게 활용할 수 있도록 class family component라는 형식의 계층적인 구조를 갖도록 정의되어 있다.
보안 기능요구는 9개의 class, 76개의 family, 184개의 component들로 구성
보증요구는 전체가 7개의 class, 25개의 family, 72개의 component들로 구성
PP 및 ST 평가 그림 보안 평가 일반 모델 기준은 2개의 class, 8개의 family, 8개의 component들로 구성

12. 에서 설명하는 암호화 알고리즘으로 옳은 것은?

< 보 기 >
· Ron Rivest가 1987년에 RSA Security에 있으면서 설계한 스트림 암호이다.
· 바이트 단위로 작동되도록 만들어진 다양한 크기의 키를 사용 한다.
· 사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.
·하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.

① RC5 ② SEED
③ SKIPJACK ④ RC4

답 ④

④ **RC4** 알고리즘에 대한 설명이다.
RC4는 로널드 라이베스트(Ron Rivest)가 만든 스트림 암호로, 전송 계층 보안(TLS)이나 WEP등의 여러 프로토콜에 사용되어 왔지만, 현재는 여러 연구를 통해 취약한 것으로 밝혀져 사용을 권장하지 않는다.

RC4(Rivest Cipher 4) 알고리즘의 특징
- 1987년 RSA Security 에서 Ron Rivest가 설계한 스트림 암호
- 바이트 단위로 작동됨, 다양한 크기의 키(1~256byte)를 사용 1994년 9월 익명의 제보자가 인터넷의 사이버 펑크 익명 리메일러 목록에 RC4 알고리즘을 올림
- 알고리즘은 랜덤치에 기초해서 만들어짐, 스트림의 주기는 10^{100}보다 큼
- 하나의 바이트를 출력하기 위해 8에서 16번의 연산이 필요
- SSL/TLS, WEP(Wired Equivalent Privacy), WPA(WiFi Protocol Access) 프로토콜에 응용

<오답 체크> ① RC5(Rivest Cipher 5)
RC5 역시 RC4와 마찬가지로 RSA Security사의 Ronald Rivest에 의해 1994년 고안된 블록 방식의 알고리즘이다.
키, 블록, 라운드까지 다양한 크기를 갖는 알고리즘
블록의 크기는 32, 64, 128 비트
키의 크기는 0에서 2040 비트까지 가변적
라운드 수는 0에서 255까지 가변적

② **SEED** : 한국정보보호진흥원(KISA)에서 개발
128비트 블록, 128 또는 256비트 키 길이
페이스텔 구조 16라운드
국내 전자상거래에 이용

③ **Skipjack** : 미국 NSA에서 1993년 발표
알고리즘 자체는 비밀
64비트의 블록, 80비트의 키 길이, 32라운드
일종의 스마트 카드인 클리퍼 칩에 적용하기 용이

13. 다음 중 Spoofing 공격에 대한 설명으로 옳지 않은 것은?

① ARP Spoofing : MAC주소를 속임으로써 통신 흐름을 왜곡시킨다.
② IP Spoofing : 다른이가 쓰는 IP를 강탈해 특정 권한을 획득한다.
③ DNS Spoofing : 공격대상이 잘못된 IP주소로 웹 접속을 하도록 유도하는 공격이다.
④ ICMP Redirect : 공격자가 클라이언트의 IP주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근한다.

답 ④

④ IP Spoofing에 대한 설명이다.
ICMP Redirect(ICMP 리다이렉트는 공격자가 공격 대상에게 ICMP 리다이렉트 메시지를 보내, 자신이 공격 대상의 게이트웨이 역할을 하게 만드는 공격이다.
그러면 공격 대상이 보내는 메시지는 게이트웨이인 공격자를 통하게 되므로 스니핑이 가능해진다.

<오답 체크> ① **ARP Spoofing**
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격이다.

② **IP Spoofing**
단말 사이가 IP 주소 기반의 트러스트 관계일 경우 인증 절차를 생략한다는 취약점을 이용한 공격으로, 공격자가 자신의 IP를 다른 사람의 IP로 속여 다른 사람 행세를 하는 것이다.

③ **DNS Spoofing**공격
공격 대상자가 접속하려는 URL 주소 이름을 요청할 때, 거짓 IP주소를 반환하여 사용자가 의도하지 않은 주소로 접근하게 만드는 공격이다.
DNS 스푸핑을 하는 방법에는 스니핑을 통해 DNS 서버보다 빨리 거짓 응답을 사용자에게 전달하는 방법, 대상자의 PC에 저장된 host파일을 수정하는 방법, DNS 서버 가진 IP 주소 자체를 변조시키는 방법 등이 있다.

14. 다음 중 ISMS(Information Security Management System) 의 각 단계에 대한 설명으로 옳은 것은?

① 계획 : ISMS 모니터링과 검토
② 조치 : ISMS 관리와 개선
③ 수행 : ISMS 수립
④ 점검 : ISMS 구현과 운영

답 ②

② 조치 단계에서는 보고된 결과를 바탕으로 유지보수 및 개선을 한다.

<오답 체크> ① 계획 단계에서는 보안 정책과 절차를 수립한다.
③ 수행 단계에서는 프로세스 및 절차를 구현하고 운영한다.
④ 점검 단계에서는 성과를 측정·평가하고 보고한다.

15. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳은 것은 무엇인가?

① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.
② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.
③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션 통신을 한다.
④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.

답 ③

③ 커버로스는 대칭키를 사용한다.
커버로스 버전4는 DES 알고리즘 사용
커버로스 버전5는 DES 이외의 다른 알고리즘도 사용

<오답 체크> ① 클라이언트는 한 번 티켓을 발급받으면 해당 티켓이 유효한 기간에는 계속 서비스를 이용할 수 있다.
② 커버로스는 사용자와 서버, 키 분배 센터(KDC)로 구성되어 있다. 키 분배 센터를 통해 키 교환을 하기 때문에 별도의 프로토콜이 필요없다.
④ 서비스 티켓도 암호화된 상태로 전송되기 때문에 공격자가 암호화키를 모르면 사용할 수 없다.

16. 다음 중 시스템 내부의 트로이목마 프로그램을 감지하기 위한 도구로 가장 적절한 것은?

① Saint ② Snort
③ Nmap ④ Tripwire

답 ④

④ **Tripwire**(트립와이어)
시스템의 특정한 파일의 변화를 모니터링하고 알림을 해주는 무결성 확인 도구이다.
바이러스나 트로이 목마 등 악성 코드로 인한 변조 상태를 점검할 수 있다.

<오답 체크> ① **SAINT**(Security Administrators's Integrated Network Tool)는 미국의 보안컨설팅업체 World Wide DIGITAL SECURITY, Inc. 에서 1998년 6월에 개발한 시스템 관리자용 네트워크 진단도구로, SATAN을 기반으로 개발되었다.
② **snort**(스노트)는 오픈 소스이며, 실시간으로 트래픽을 분석하고 패킷을 기록하는 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)이다.
③ **snort**(스노트)
고든 라이언에 의해 개발된 네트워크 스캐닝 도구로, 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지한다.
TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용

17. ROT13 암호로 info 를 암호화한 결과는?

① jvxv ② foin
③ vasb ④ klmd

답 ③

③ ROT13(Rotate by 13)은 단순한 카이사르 암호의 일종으로 영어 알파벳을 13글자씩 밀어서 만든다.
예를 들어 알파벳 9번째 문자인 i를 ROT13을 이용해 암호화하면,
9 + 13 = 22
22번째 문자인 v가 된다.
14번째 문자인 n을 암호화하면 27번째 문자가 되는데,
27 mod 26 = 1
1번째 문자인 a가 된다.
마찬가지로 f -> s, o -> b가 된다.

18. 무선랜에서의 인증 방식에 대한 설명 중 옳지 않은 것은?

① WPA 방식은 48비트 길이의 초기벡터(Ⅳ)를 사용한다.
② WPA2 방식은 AES 암호화 알고리즘을 사용하여 좀 더 강력한 보안을 제공한다.
③ WEP 방식은 DES 암호화 방식을 이용한다.
④ WEP 방식은 공격에 취약하며 보안성이 약하다.

답 ③

③ WEP 방식은 암호화에 RC4 알고리즘을 이용한다.

- **WEP** 방식: 암호화를 위해 RC4 사용하며(암호키 계속 사용), 암호화와 인증에 동일한 키를 사용
- **WPA** 방식: RC4-TKIP를 통한 암호화(암호키 주기적인 변경), EAP를 통한 사용자 인증
  48비트 길이의 초기벡터(IV) 사용
- **WPA2** 방식: AES-CCMP 사용, EAP를 통한 사용자 인증

19. 다음 중 ISO 27001의 통제 영역별 주요 내용으로 옳은 것은?

① 정보보안 조직: 정보보호에 대한 경영진의 방향성 및 지원을 제공
② 인적 자원 보안 : 정보에 대한 접근을 통제
③ 정보보안 사고 관리: 사업장의 비인가된 접근 및 방해 요인을 예방
④ 통신 및 운영 관리: 정보처리시설의 정확하고 안전한 운영을 보장

답 ④

<오답 체크> ① 정보보안 정책에 대한 설명이다.
정보보안 조직은 보안을 효과적으로 관리하기 위한 보안 조직 구성 및 책임과 역할에 대한 규명
② 접근 통제에 대한 설명이다.
인적 자원 보안은 사람의 실수나 부정 행위로 인한 위험을 감소시키기 위한 대응 방안 확인
③ 물리적.환경적 보안에 대한 설명이다.
정보보안 사고 관리는 보안 사고와 취약점이 정해진 시기 내에 적절하게 수정되고 보고가 이루어지는지 여부 확인

20. 「개인정보보호법」에 따르면 주민등록번호를 처리하기 위해서는 법에서 정하는 바에 따라야 하는데, 그에 대한 내용 중 옳지 않은 것은?

① 주민등록번호 처리는 원칙적으로 금지되고 예외적인 경우에만 허용한다.
② 주민등록번호는 암호화 조치를 통해 보관해야 한다.
③ 개인정보처리자는 법령에서 주민등록번호의 처리를 허용한 경우에도 주민등록번호를 사용하지 않는 인터넷 회원 가입 방법을 정보주체에게 제공해야 한다.
④ 기 보유한 주민등록번호는 수집 시 동의 받은 보유기간까지만 보유하고 이후에는 즉시 폐기해야 한다.

답 ④

④ 개인정보 처리 동의를 받고 보유기간이 지나지 않았더라도, 개인정보가 불필요하게 되었을 때에는 지체 없이 파기하여야 한다.

제21조(개인정보의 파기) 1항
개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

① **제24조의2**(주민등록번호 처리의 제한) 1항
개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

② **제24조의2**(주민등록번호 처리의 제한) 2항
개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

③ **제24조의2**(주민등록번호 처리의 제한) 3항
개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.