

2016년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

문 1. 사용자 인증에 사용되는 기술이 아닌 것은?

- ① Snort
- ② OTP(One Time Password)
- ③ SSO(Single Sign On)
- ④ 스마트 카드

답 ①

- ① snort(스노트)는 오픈 소스이며, 실시간으로 트래픽을 분석하고 패킷을 기록하는 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)이다.
- ② OTP(One-Time Password, 일회용 비밀번호)는 한 번 생성되면 그 인증값이 임시적으로 한 번만 유효한 비밀번호 인증 방식으로, 재사용이 불가능하기 때문에 보안에 안전하다.
- ③ SSO(Single Sign-On, 통합 인증)는 한 번의 인증 과정으로 여러 컴퓨터 상의 자원을 이용 가능하게 하는 인증 시스템이다.
- ④ 스마트 카드는 단순한 정보의 저장은 물론이고 간단한 연산까지 가능한 작은 집적회로가 탑재된 카드이다.

문 2. 보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은?

- ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
- ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
- ㄷ. 자산의 잠재적인 속성으로서 위협의 이용 대상이 되는 것

	그	느	드
① 위협	취약점	위험	
② 위협	위험	취약점	
③ 취약점	위험	위험	
④ 위협	위험	취약점	

답 ②

- ㄱ. 위협(threat)은 내가 가진 자산에 해를 끼치는 요인이나 공격자
- ㄴ. 위험(risk)은 자산에 피해가 발생하는 정도와 가능성
- ㄷ. 취약점(Vulnerability)은 자신이 가진 약점으로, 위협요소는 취약점을 통해 자산에 해를 끼친다.



문 3. 공개키 암호 알고리즘에 대한 설명으로 옳은 것은?

- ① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.
- ② RSA 암호 알고리즘은 적절한 시간 내에 인수가 큰 정수의 소인수분해가 어렵다는 점을 이용한 것이다.
- ③ 타원곡선 암호 알고리즘은 타원곡선 대수문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 긴 길이의 키를 필요로 한다.
- ④ ElGamal 암호 알고리즘은 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것이다.

답 ②

- ① 디피 헬만 키 교환(Diffie-Hellman key exchange)은 두 송수신자 간 공통의 비밀키를 생성하기 위한 방법이다. 디피 헬만 방식은 중간자 공격에 취약하다.
- ③ 타원 곡선 암호(ECC)에 타원 곡선 상의 이산대수 문제에 기반한 공개키 암호화 알고리즘이다. 동일한 보안 수준에서 RSA 보다 키의 길이가 짧고 빠르다.
- ④ ElGamal 암호 알고리즘은 이산대수의 어려움에 기반한 공개키 암호 알고리즘이다. 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것은 Knapsack(배낭 문제) 암호화 방식이다.

- 대칭키 암호 알고리즘
DES, 3-DES, IDEA, AES, RC5, Skipjack, Blowfish
(국산 대칭키) SEED, HIGHT, ARIA, LEA, LSH
- 비대칭키 암호(공개키 암호) 알고리즘
RSA : 소인수분해
Rabin : 소인수분해
ElGamal : 이산대수
ECC : 타원곡선 상의 이산대수
Schnorr : 이산대수, ElGamal 에 기반, 짧은 키 길이
DSA : 이산대수, Schnorr 의 응용
DSS : 이산대수, 전자서명 전용
ECDSA : 내부적으로 타원곡선
Knapsack(배낭 문제) : 부분집합의 합을 구하는 문제 (NP-complete 문제)
KCDSA : 국산, 국내표준
ECKDSA : 국산, 내부적으로 타원곡선, 소규모, 무선

문 4. ISO/IEC 27001 의 보안 위험 관리를 위한 PDCA 모델에 대한 설명으로 옳지 않은 것은?

- ① IT 기술과 위험 환경의 변화에 대응하기 위하여 반복되어야 하는 순환적 프로세스이다.
- ② Plan 단계에서는 보안 정책, 목적, 프로세스 및 절차를 수립 한다.
- ③ Do 단계에서는 수립된 프로세스 및 절차를 구현하고 운영한다.
- ④ Act 단계에서는 성과를 측정하고 평가한다.

답 ④

- ④ PDCA 모델
Plan(계획): 보안 정책, 목적 프로세스 및 절차 수립
Do(실행): 통제, 프로세스 및 절차 구현, 운영
Check(점검): 성과 측정, 평가, 보고
Act(처리): 검토, 유지보수, 개선

문 7. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상 정보통신 서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자들에게 알리고 동의를 받아야 하는 내용이 아닌 것은?

- ① 개인정보의 수집·이용 목적
- ② 수집하는 개인정보의 항목
- ③ 개인정보의 보유·이용 기간
- ④ 개인정보 처리의 위탁기관명

답 ④

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제 22 조(개인정보의 수집·이용 동의 등)

① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.

- 1. 개인정보의 수집·이용 목적
- 2. 수집하는 개인정보의 항목
- 3. 개인정보의 보유·이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제 1 항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

- 1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
- 2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
- 3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

④ 위탁기관에 관한 정보는 개인정보를 수집할 때가 아니라 위탁할 때 알리면 된다.

문 8. 임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?

- ① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 둔다.
- ② 주체 또는 주체가 소속되어 있는 그룹의 식별자(ID)를 근거로 객체에 대한 접근을 승인하거나 제한한다.
- ③ 소유권을 가진 주체가 객체에 대한 권한의 일부 또는 전부를 자신의 의지에 따라 다른 주체에게 부여한다.
- ④ 전통적인 UNIX 파일 접근제어에 적용되었다.

답 ①

① 역할에 따른 규칙에 기반을 두는 건 역할 기반 접근 제어(RBAC, Role Based Access Control)이다. 정보에 대한 사용자의 접근을 개별적인 신분이 아니라 조직 내 개인 역할에 따라 허용 여부를 결정하는 모델이다.

임의적 접근 제어(DAC, Discretionary Access Control(DAC)는 정보의 소유자가 보안 등급을 결정하고 이에 대한 정보의 접근제어도 설정하는 모델이다.

④ 유닉스와 윈도우는 기본적으로 개별 파일이나 폴더별로 권한을 설정하는 임의적 접근 제어 방식이다.

문 9. 식별된 위험에 대처하기 위한 정보보안 위험 관리의 위험 처리 방안 중, 불편이나 기능 저하를 감수하 고라도, 위험을 발생시키는 행위나 시스템 사용을 하 지 않도록 조치하는 방안은?

- ① 위험 회피
- ② 위험 감소
- ③ 위험 수용
- ④ 위험 전가

답 ①

- ① 위험 회피(Risk Avoidance)
위험의 정도가 크고 발생 빈도가 높을 때
위험이 존재하는 프로세스나 사업 포기하는 것
- ② 위험 감소(Risk Mitigation)
위험의 정도가 크지 않고 발생 빈도가 높을 때
위험을 감소시킬 수 있는 대책을 채택 구현, 많은 비용 소
요, 비용분석실시
- ③ 위험 수용(Risk Acceptance)
위험의 정도가 크지 않고 발생 빈도가 낮을 때
위험의 잠재 손실 비용을 감수하는 것
- ④ 위험 전가(Risk Transfer)
위험의 정도가 크고 발생 빈도가 낮을 때
보험이나 외주 등으로 잠재적 비용을 제 3 자에게 이전, 할
당

문 10. Bell-LaPadula 보안 모델의 *-속성(star property) 이 규정하고 있는 것은?

- ① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있
다.
- ② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있
다.
- ③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있
다.
- ④ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있
다.

답 ④

- ④ *-속성은 쓰기에 관한 속성으로, BLP 모델은 자신과 낮은 객체에 쓸 수 없고, 높은 객체에만 쓸 수 있다.

BLP(벨 라파둘라) 모델은 기밀성을 중시한 모델
높은 보안수준의 문서 내용이 낮은 보안수준으로 흐르는
걸 방지하는 데 중점을 둔다.
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수
없다.
단순 보안 속성(Simple security property, ss-속성) – NRU(No
Read Up) 높은 등급의 데이터를 읽을 수 없다.
*-속성(Star property) – NWD(No Write Down) 낮은 등급의
데이터에 쓸 수 없다.

문 11. 버퍼 오버플로우에 대한 설명으로 옳지 않은 것은?

- ① 프로세스 간의 자원 경쟁을 유발하여 권한을 획득하는 기법으로 활용된다.
- ② C 프로그래밍 언어에서 배열에 기록되는 입력 데이터의 크기를 검사하지 않으면 발생할 수 있다.
- ③ 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류가 발생하게 되는 상황이다.
- ④ 버퍼 오버플로우 공격의 대응책 중 하나는 스택이나 힙에 삽입된 코드가 실행되지 않도록 하는 것이다.

답 ①

- ① 두 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법은 레이스 컨디션(Race Condition) 공격이다.

버퍼 오버플로우(buffer overflow) 공격은 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.

- ④ 오버 플로우가 발생하는 데이터 영역에 따라, 힙 오버플로우(heap overflow) 공격과 스택 기반 오버플로우(stack overflow)로 나뉜다.
그러므로 힙과 스택에 삽입된 코드가 실행되지 않도록 하면 방어에 도움이 된다.

문 12. 침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는 데 적합한 기법은?

- ① 규칙 기반의 오용 탐지
- ② 통계적 분석에 의한 이상(anomaly) 탐지
- ③ 전문가 시스템을 이용한 오용 탐지
- ④ 시그니처 기반(signature based) 탐지

답 ②

- ② 알려지지 않은 공격인 제로 데이 공격(zero day attack)을 탐지할 수 있는 건 이상탐지(anomaly detection)이다.

오용탐지(Misuse Detection)

= 시그니처 기반(Signature Base)

= 지식 기반(Knowledge Base)

이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지

오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능

전문가 시스템(Expert System)의 지식 DB 를 이용한 IDS Zero Day attack(제로 데이 공격)에 취약

이상탐지(Anomaly Detection IDS)

= 행위 기반(Behavior)

= 통계적 탐지(Statistical Detection)

정상 패턴을 DB 에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)

알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능

오탐율 높고, 임계치 설정이 어려움

문 13. 「전자서명법」 상 공인인증기관이 발급한 공인인증서의 효력 소멸 또는 폐지의 사유에 해당하지 않는 것은?

- ① 공인인증서의 유효기간이 경과한 경우
- ② 가입자의 전자서명검증정보가 유출된 경우
- ③ 공인인증기관이 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
- ④ 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우

답 ②

② 전자서명검증정보는 서명자의 공개키이다. 공개키는 공개된 정보이기 때문에 유출되어도 상관이 없다. 공인인증서의 폐지 사유는 전자서명생성정보(개인키)가 유출된 경우이다.

「전자서명법」

제 16 조(공인인증서의 효력의 소멸 등)

1. 공인인증서의 유효기간이 경과한 경우

- 2. 제 12 조제 1 항의 규정에 의하여 공인인증기관의 지정이 취소된 경우
- 3. 제 17 조의 규정에 의하여 공인인증서의 효력이 정지된 경우
- 4. 제 18 조의 규정에 의하여 공인인증서가 폐지된 경우

제 18 조(공인인증서의 폐지)

- 1. 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
- 2. 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
- 3. 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
- 4. 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우

문 14. 가상사설망(VPN)에 대한 설명으로 옳지 않은 것은?

- ① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.
- ② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자 인증의 보안 기능을 제공한다.
- ③ 네트워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH 와 같은 OSI 모델 4 계층의 보안 프로토콜로 구현해야 한다.
- ④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택 근무자나 이동 중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

답 ③

③ SSH(Secure Shell)은 OSI 모델 7 계층 응용 계층에서 FTP 와 telnet(원격 접속 프로토콜)을 보호하기 위한 보안 기술이다.

계층별 보안 프로토콜

- PPTP - 2 계층
- L2F - 2 계층
- L2TP - 2 계층
- IPSec - 3 계층
- SSL/TLS - 4 계층
- SOCKSv5 - 5 계층
- SSH(Secure Shell) - 7 계층(telnet 이나 FTP 를 암호화)

문 15. ISO/IEC 27002 보안 통제의 범주에 대한 설명으로 옳지 않은 것은?

- ① 보안 정책: 비즈니스 요구사항, 관련 법률 및 규정을 준수하여 관리 방향 및 정보 보안 지원을 제공
- ② 인적 자원 보안: 조직 내의 정보 보안 및 외부자에 의해 사용되는 정보 및 자원 관리
- ③ 자산 관리: 조직의 자산에 대한 적절한 보호를 성취하고 관리하며, 정보가 적절히 분류될 수 있도록 보장
- ④ 비즈니스 연속성 관리: 비즈니스 활동에 대한 방해에 대처하고, 중대한 비즈니스 프로세스를 정보 시스템 실패 또는 재난으로부터 보호하며, 정보 시스템의 시의 적절한 재개를 보장

답 ②

② K-ISMS 2.0 의 외부자 보안 통제에 대한 설명이다.

ISO/IEC 27002 의 인적 자원 보안: 고용 전, 고용 중, 고용 종료 및 직무 변경에 대한 통제

문 16. OWASP(The Open Web Application Security Project)에서 발표한 2013 년도 10 대 웹 애플리케이션 보안 위험 중 발생 빈도가 높은 상위 3 개에 속하지 않는 것은?

- ① Injection
- ② Cross-Site Scripting
- ③ Unvalidated Redirects and Forwards
- ④ Broken Authentication and Session Management

답 ③

OWASP TOP 10 2013

- A1 인젝션(Injection)
- A2 인증 및 세션 관리 취약점
(Broken Authentication and Session Management)
- A3 크로스 사이트 스크립팅(XSS, Cross Site Scripting)
- A4 안전하지 않은 객체 참조
(Insecure Direct Object Reference)
- A5 보안상 잘못된 구성(Security Misconfiguration)
- A6 민감한 데이터 노출(Sensitive Data Exposure)
- A7 기능 수준 접근 통제 누락
(Missing Function Level Access Control)
- A8 크로스 사이트 요청 변조
(CSRF, Cross Site Request Forgery)
- A9 알려진 취약점이 있는 컴포넌트 사용
(Using Components with Known Vulnerabilities)
- A10 검증되지 않은 리다이렉트 및 포워드
(Unvalidated Redirects and Forwards)

문 17. 전자우편의 보안 강화를 위한 S/MIME(Secure/Multipurpose Internet Mail Extension)에 대한 설명으로 옳은 것은?

- ① 메시지 다이제스트를 수신자의 공개키로 암호화하여 서명한다.
- ② 메시지를 대칭키로 암호화하고 이 대칭키를 발신자의 개인키로 암호화한 후 암호화된 메시지와 함께 보냄으로써 전자우편의 기밀성을 보장한다.
- ③ S/MIME 를 이용하면 메시지가 항상 암호화되기 때문에 S/MIME 처리 능력이 없는 수신자는 전자우편 내용을 볼 수 없다.
- ④ 국제 표준 X.509 형식의 공개키 인증서를 사용한다.

답 ④

S/MIME(Secure/Multipurpose Internet Mail Extension)는 MIME를 보호하기 위한 보안 기술로, RSA 이용하고 인증기관 필요로 한다.(X.509 v3 인증서)

- ① 서명을 생성할 때 수신자의 개인키로 암호화하고, 서명을 검증할 때 수신자의 공개키로 복호화한다.
- ② 메시지를 대칭키(세션키)로 암호화하는데, 이 세션키는 수신자의 공개키로 암호화해야, 개인키를 가진 수신자만 복호화할 수 있다.
세션키를 발신자의 개인키로 암호화할 경우, 발신자의 공개키를 가진 모두가 세션키를 획득할 수 있다.
- ③ S/MIME 를 사용하는 용도에 따라 메시지를 암호화할 수도, 암호화하지 않을 수도 있다.
메시지를 암호화하지 않는(Multipart/signed) 방식일 경우, S/MIME 처리 능력이 없는 수신자도 메시지의 내용을 볼 수는 있다.(단, 서명을 검증할 수는 없다)

문 18. 국내 정보보호관리체계(ISMS)의 관리 과정 5 단계 중 위험 관리 단계의 통제항목에 해당하지 않는 것은?

- ① 위험 관리 방법 및 계획 수립
- ② 정보보호 대책 선정 및 이행 계획 수립
- ③ 정보보호 대책의 효과적 구현
- ④ 위험 식별 및 평가

답 ③

③ 정보보호대책 구현 단계에 해당한다.

국내 정보보호관리체계(ISMS)

기업이 주요 정보자산을 보호하기 위해 수립·관리·운영하는 정보보호 관리체계가 인증기준에 적합한지를 심사하여 인증을 부여하는 제도

국내 정보보호관리체계(ISMS)의 관리 과정

관리과정	요구사항
정보보호정책 수립 및 범위설정	- 상위 수준의 정보보호정책 수립 - 정보보호 관리체계 범위 설정
경영진 책임 및 조직구성	- 경영진 참여 - 정보보호조직 구성 및 자원 할당
위험관리	- 위험관리 방법 및 계획 수립 - 위험 식별 및 평가 - 정보보호대책 선정 - 이행 계획 수립
정보보호대책 구현	- 정보보호 대책의 효과적 구현 - 내부 공유 및 교육
사후관리	- 법적 요구사항 준수 검토 - 정보보호 관리체계 운영현황 관리 - 내부감사

문 19. 공개키 기반 전자서명에서 메시지에 서명하지 않고 메시지의 해시값과 같은 메시지 다이제스트에 서명하는 이유는?

- ① 공개키 암호화에 따른 성능 저하를 극복하기 위한 것이다.
- ② 서명자의 공개키를 쉽게 찾을 수 있도록 하기 위한 것이다.
- ③ 서명 재사용을 위한 것이다.
- ④ 원본 메시지가 없어도 서명을 검증할 수 있도록 하기 위한 것이다.

답 ①

- ① 공개키 방식은 대칭키(비밀키) 방식에 비해 키의 길이가 길고 속도가 느리다.
그래서 길이가 긴 원본 메시지에 서명을 하지 않고, 길이가 짧은 해시값에 서명을 한다.
- ② 공개키를 찾는 것과 상관이 없다.
- ③ 전자서명에 사용된 서명은 절대 재사용되어서는 안 된다.
개인키의 소유자라 하더라도 문서를 전송할 때마다 새로운 서명을 생성해야 한다.
- ④ 문제에서는 메시지가 아닌 메시지의 해시값에 서명을 하는 경우를 물어봤는데, 전자서명을 검증하기 위해서 수신자는 원본 메시지에서 해시값을 구해 송신자가 보낸 해시 값과 비교하는 과정이 필요하다.
따라서 원본 메시지가 없으면 해시값을 검증할 수 없다.
만일 메시지에 직접 서명을 하는 경우라면, 원본 메시지가 필요 없지만 서명 생성 및 검증에 시간이 오래 소요된다.

문 20. 윈도우즈에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 옳지 않은 것은?

- ① route : 라우팅 테이블의 정보 확인
- ② netstat : 연결 포트 등의 네트워크 상태 정보 확인
- ③ tracert : 네트워크 목적지까지의 경로 정보 확인
- ④ nslookup : 사용자 계정 정보 확인

답 ④

- ④ nslookup 은 'name server lookup'의 약자로, 도메인 네임과 IP 주소의 매핑 정보를 조회하는 명령어이다. 서버의 네트워크가 제대로 설정되었는지 확인하는 용도로도 사용된다. 사용자의 계정정보를 확인하는 명령어는 finger 명령어이다.