정보보호론(9급)

(과목코드 : 141)

2021년 군무원 채용시험 응시번호 : 성명 :

1. 응용 수준 취약점에 대한 설명으로 옳지 않은 것은?
   ① 버퍼오버플로우는 메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점이다.
   ② 크로스 사이트 스크립팅은 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다.
   ③ SSI인젝션은 조작된 XPath(XML Path) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올 수 있는 취약점이다.
   ④ SQL인젝션은 SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점이다.

2. 전자서명법에 대한 설명으로 옳지 않은 것은?
   ① “전자문서”란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
   ② 당사자 간의 약정에 따라 행해진 서명, 서명날인 또는 기명날인 방식의 전자서명은 제3의 신뢰기관이 개입하지 않았으므로 전자서명법 상 효력을 가지지 않는다.
   ③ “인증서”란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
   ④ “전자서명생성정보”란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

3. RSA 암호알고리즘을 위해 두 개의 소수가 p=3, q=11일 경우, 공개키(n)과 암호화 공개키(e=7)에 대응되는 복호용 개인키(d)로 적절한 것은?
   ① n=33, d=3 ② n=21, d=5
   ③ n=21, d=3 ④ n=33, d=5

4. Diffie-Hellman 키 공유 프로토콜에서, 공개정보인 소수 p=11, 원시원소 g=7 인 경우, 갑이 자신의 비밀키(x)를 5로, 을이 자신의 비밀키(y)를 3으로 선택했을 경우, 갑과 을이 공유하는 세션키로 옳은 것은?
   ① 10 ② 7
   ③ 8 ④ 5

5. 정보보호의 3대 요소로 옳지 않은 것은?
   ① 비인가자, 불법 침입자의 접근 제어를 통해 비밀 정보가 누출되지 않도록 보장하는 기밀성
   ② 메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 부인방지
   ③ 인가된 사용자가 적시, 적소에 필요 정보에 접근할 수 있고 사용 가능하도록 보장하는 가용성
   ④ 불법 사용자에 의해 정보 및 소프트웨어가 변경, 삭제, 생성되는 것으로부터 보호하여 원래 상태를 보존 유지하는 무결성

6. 우리나라가 개발해 국제표준화한 암호 알고리즘만으로 짝지은 것은?
   ① 블록 암호 알고리즘(SEED) - 서명 알고리즘(KCDSA)
   ② 블록 암호 알고리즘(AES) - 서명 알고리즘(RSA)
   ③ 블록 암호 알고리즘(triple DES) - 서명 알고리즘(DSA)
   ④ 블록 암호 알고리즘(ARIA) - 서명 알고리즘(ECDSA)

7. 일어날 수 있는 모든 가능한 경우에 대하여 조사하는 형태의 공격으로 적절한 것은?
   ① 전수조사 공격 ② 중간자 공격
   ③ 생일 공격 ④ 사전 공격

8. 정보보호제품 평가인증제도에 대한 설명으로 옳지 않은 것은?
① 정보보호제품의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6의 6개의 보증 등급으로 구분된다. EAL1은 최고의 평가보증등급이고, EAL6은 최저의 평가보증등급이다.
② 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.
③ 공통평가기준 1부는 정보보호시스템 보안성 평가의 원칙과 일반개념을 정의하고 평가의 일반적인 모델을 설명하는 소개부분으로, IT 보안목적을 표현하고 IT 보안요구사항을 선택·정의하며, 제품 및 시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다.
④ "보호프로파일"이라 함은, 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말하며, "보안목표명세서"라 함은 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.

9. 정보 보안 시스템을 설계하거나 운영할 때 고려하는 요소 중 하나인 가용성을 보존하기 위해 행해지는 활동으로 옳지 않은 것은?
① 백업
② 네트워크 증설
③ 침입탐지시스템 운용
④ 전자서명

10. 디지털 포렌식 원칙에 해당하지 않는 것은?
① 정당성의 원칙
② 재현의 원칙
③ 연계보관성의 원칙
④ 무죄 추정의 원칙

11. 개인정보보호법 제3조(개인정보보호원칙)에 명시된 내용으로 옳지 않은 것은?
① 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
② 개인정보처리자는 정보주체의 동의를 받은 경우 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
③ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
④ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

12. 공개키 기반구조에 대한 설명으로 옳지 않은 것은?
① X.509 국제표준에 기반하며, 정보의 기밀성, 무결성, 인증, 부인방지 등 신뢰 서비스를 제공하는데 이용된다.
② 공개키 인증서를 발행하는 인증기관, 실체의 신원을 확인하는 등록기관, 인증서 폐지 목록을 관리하는 보관소, 최종 실체 등으로 구성된다.
③ 기업 및 기관 단위에서 사용자들에게 특정 시스템 및 애플리케이션에 접근할 수 있는 권한을 차등 부여해주는 관리 체계이다.
④ 공개키 인증서를 생성, 관리, 배포, 이용, 저장 및 폐지하기 위해 필요한 기능, 정책, 하드웨어, 소프트웨어 및 절차의 집합이다.

13. 완성된 바이너리 형태의 소프트웨어를 역으로 분석하여 원래 소스 코드의 구조를 파악하는 리버스 엔지니어링의 목적으로 옳지 않은 것은?
① 취약점 분석
② 악성코드 분석
③ 디지털 포렌식
④ 컴파일 및 링킹

14. 정보통신기반 보호에 대한 설명으로 옳지 않은 것은?

① 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 업무의 국가사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 국가안전보장과 경제사회에 미치는 피해규모 및 범위 등을 고려하여 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

② 주요정보통신기반시설 보호계획에는 주요정보통신기반시설의 취약점 분석·평가, 침해사고에 대한 예방·백업·복구대책, 보호에 관하여 필요한 사항을 포함해야 한다.

③ 정보통신기반보호위원회는 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당 분야 관리기관의 장에게 이를 지키도록 권고할 수 있다.

④ "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다.

15. 암호화에 대한 설명으로 옳지 않은 것은?

① 순서보존 암호화(Order-preserving encryption)는 원본정보의 순서와 암호값의 순서가 동일하게 유지되는 암호화 방식이다.

② 형태보존 암호화(Format-preserving encryption)는 원본 정보의 형태와 암호값의 형태가 동일하게 유지되는 암호화 방식이다.

③ 동형 암호화(Homomorphic encryption)는 암호화된 상태에서의 연산이 가능한 암호화 방식이다.

④ 일방향 암호화는 원문에 대한 암호화만 가능하며 추가정보가 있으면 암호문에 대한 복호화가 가능하다.

16. 온라인상 본인확인서비스에 대한 설명 중 옳지 않은 것은?

① "연계정보"라 함은 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위해 본인확인기관이 이용자의 주민등록번호와 본인확인기관 간 공유 비밀정보를 이용하여 생성한 정보를 말한다.

② "중복가입확인정보"라 함은 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는 데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관 간 공유비밀정보를 이용하여 생성한 정보를 말한다.

③ "공유비밀정보"라 함은 본인확인기관이 특정 이용자에 대해 동일한 중복가입확인정보와 연계정보를 생성하기 위해 공유하는 정보를 말한다.

④ 전자서명법에 따른 "전자서명인증사업자"는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"에 근거해 지정되는 본인확인기관으로 간주된다.

17. 인터넷과 같은 공중망에 터널을 형성하고 이를 통해 패킷을 캡슐화해서 전달함으로써 사설망과 같은 전용 회선처럼 사용할 수 있게 하는 기술로 적절한 것은?

① 가상 사설망　② 접근 제어
③ 회선 관리　④ 세션 관리

18. ARP Spoofing 공격에 대한 설명으로 옳지 않은 것은?

① ARP(Address Resolution Protocol)이 인증을 하지 않기 때문에 발생한다.

② 근거리 네트워크 환경에서 발생한다.

③ ARP 테이블 변경을 동적으로 관리함으로 예방할 수 있다.

④ 중간자 공격 기법을 통해 이루어진다.

19. 공개된 네트워크 환경에서 통신하는 두 당사자가 공유키를 만드는 데 사용되는 Diffie-Hellman 알고리즘에 대한 설명으로 옳지 않은 것은?
① 비밀키 알고리즘의 일종이다.
② 안전을 위해 일반적으로 1024비트 이상의 큰 소수를 사용해야 한다.
③ 상대방에 대한 인증을 제공하지 않기 때문에 중간자 공격이 가능하다.
④ 안전을 위해 충분히 안전한 난수 생성 알고리즘을 사용해야 한다.

20. 미국 국방부에 의해 개발된 컴퓨터 보안 평가 방법론인 TCSEC에 대한 설명으로 옳지 않은 것은?
① 가장 낮은 평가 수준은 D이고 가장 높은 수준은 A이다.
② 운영체제에 중점을 두어 평가하기 때문에 방화벽 등에 적용하기 어렵다.
③ 기밀성, 무결성, 가용성에 대한 요구 사항을 균형적으로 다루고 있다.
④ 평가 수준별로 기능 요구 사항과 보증 요구 사항을 포함한다.

21. 개인정보 가명처리에 대한 설명으로 옳지 않은 것은?
① 가명정보는 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보이다.
② 가명정보는 처리(제공) 환경에 따라 가명정보 처리자 내부에서 활용(자체활용 또는 내부 제공·결합)하는 경우와 제3자에게 제공하는 경우로 구분할 수 있다.
③ 가명정보처리자는 가명정보 또는 추가정보의 안전한 관리를 위하여 기술적 안전조치와 관리적 안전조치를 취해야 하며, 물리적 안전조치를 취하지 않아도 무방하다.
④ 가명정보는 개인정보처리자의 정당한 처리 범위 내에서 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 처리할 수 있다.

22. 접근 권한이 시스템 전체적으로 보안 정책 및 관련 규칙에 따라 결정되기 보다는 자원의 소유자에 의해 결정되는 접근 제어 모델에 해당하는 것으로 옳은 것은?
① 강제적 접근 제어
② 임의적 접근 제어
③ 역할 기반 접근 제어
④ 규칙 기반 접근 제어

23. 윈도우를 비롯한 시스템에서 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM에 대한 설명으로 옳지 않은 것은?
① 암·복호화 및 전자서명 기능 제공
② 부팅 과정에서 인증을 통해 신뢰성 제공
③ 디바이스 및 플랫폼 인증
④ 운영체제에 의존하여 명령어가 동작함

24. 블록체인 합의 알고리즘에 대한 설명으로 옳지 않은 것은?
① 분산 시스템에서 합의란 네트워크에 존재하는 독립적인 참여자들이 동일한 블록체인 원장을 유지할 수 있도록 원장에 포함할 블록을 결정하는 방식이다.
② 분산원장 시스템에서는 다양한 합의 알고리즘들이 사용될 수 있으며, 예로는 작업증명(PoW: Proof of Work), 지분증명(PoS: Proof of Stake), 위임지분증명(DPoS: Delegated Proof of Stake) 등이 존재한다.
③ 지분 증명은 블록을 생성하는 노드가 작업(예: 특정 조건을 충족해야하는 해시 연산 등 높은 비용/자원이 필요한 작업)을 통해 스스로의 신뢰성을 증명하는 합의 방식이다.
④ 분산원장 시스템 내의 모든 노드가 일관성 있는 분산원장을 보유할 수 있도록 통신을 통해 새로운 기록의 공유, 검증 및 추가에 대한 전체의 동의를 이끌어 내는 알고리즘이다.

25. 유닉스나 리눅스 파일 설정 권한 중에서 일반 사용자가 실행 시 일시적으로 관리자(root)의 권한으로 실행되도록 함으로써 시스템의 보안에 허점을 초래할 수 있는 것으로 옳은 것은?
① SetGID ② SetUID
③ Sticky Bit ④ touch