1과목 : 과목 구분 없음

1. 사용자 인증에 사용되는 기술이 아닌 것은?

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

2. 보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은? (순서대로 ㄱ, ㄴ, ㄷ)

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

① 위협, 취약점, 위험
❷ 위협, 위험, 취약점
③ 취약점, 위협, 위험
④ 위험, 위협, 취약점

3. 공개키 암호 알고리즘에 대한 설명으로 옳은 것은?

① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.
❷ 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.

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

① IT기술과 위험 환경의 변화에 대응하기 위하여 반복되어야 하는 순환적 프로세스이다.
② Plan 단계에서는 보안 정책, 목적, 프로세스 및 절차를 수립한다.
③ Do 단계에서는 수립된 프로세스 및 절차를 구현하고 운영한다.
❹ Act 단계에서는 성과를 측정하고 평가한다.

5. 메시지의 무결성을 검증하는 데 사용되는 해시와 메시지 인증코드(MAC)의 차이점에 대한 설명으로 옳은 것은?

❶ MAC는 메시지와 송?수신자만이 공유하는 비밀키를 입력받아 생성되는 반면에, 해시는 비밀키 없이 메시지로부터 만들어진다.
② 해시의 크기는 메시지 크기와 무관하게 일정하지만, MAC는 메시지와 크기가 같아야 한다.
③ 메시지 무결성 검증 시, 해시는 암호화되어 원본 메시지와 함께 수신자에게 전달되는 반면에, MAC의 경우에는 MAC로부터 원본 메시지 복호화가 가능하므로 MAC만 전송하는 것이 일반적이다.
④ 송?수신자만이 공유하는 비밀키가 있는 경우, MAC를 이용하여 메시지 무결성을 검증할 수 있으나 해시를 이용한 메시지 무결성 검증은 불가능하다.

6. DMZ(demilitarized zone)에 대한 설명으로 옳은 것만을 고른 것은?

ㄱ. 외부 네트워크에서는 DMZ에 접근할 수 없다.
ㄴ. DMZ 내에는 웹 서버, DNS 서버, 메일 서버 등이 위치할 수 있다.
ㄷ. 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.
ㄹ. DMZ는 보안 조치가 취해진 네트워크 영역으로, 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

① ㄱ, ㄷ
② ㄴ, ㄷ
❸ ㄴ, ㄹ
④ ㄱ, ㄹ

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
❹ 개인정보 처리의 위탁기관명

8. 임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?

❶ 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.

9. 식별된 위험에 대처하기 위한 정보보안 위험 관리의 위험 처리 방안 중, 불편이나 기능 저하를 감수하고라도, 위험을 발생시키는 행위나 시스템 사용을 하지 않도록 조치하는 방안은?

❶ 위험 회피
② 위험 감소
③ 위험 수용
④ 위험 전가

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

① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다.
② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다.
③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다.
❹ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.

11. 버퍼 오버플로우에 대한 설명으로 옳지 않은 것은?

❶ 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.

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

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

13. [전자서명법] 상 공인인증기관이 발급한 공인인증서의 효력 소멸 또는 폐지의 사유에 해당하지 않는 것은?

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

14. 가상사설망(VPN)에 대한 설명으로 옳지 않은 것은?

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

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
❷ 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 재난으로 부터 보호하며, 정보 시스템의 시의 적절한 재개를 보장

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

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

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/MIME를 이용하면 메시지가 항상 암호화되기 때문에 S/MIME 처리 능력이 없는 수신자는 전자우편 내용을 볼 수 없다.
❹ 국제 표준 X.509 형식의 공개키 인증서를 사용한다.

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

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

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

❶ 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.

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
❹ nslookup :사용자 계정 정보 확인

1	2	3	4	5	6	7	8	9	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