정보보호론

문 1. 서비스 거부 공격 방법이 아닌 것은?
① ARP spoofing
② Smurf
③ SYN flooding
④ UDP flooding

문 2. MS 오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성 코드는?
① 애드웨어
② 트로이 목마
③ 백도어
④ 매크로 바이러스

문 3. 데이터베이스 보안의 요구사항이 아닌 것은?
① 데이터 무결성 보장
② 기밀 데이터 관리 및 보호
③ 추론 보장
④ 사용자 인증

문 4. OSI 참조 모델의 제7계층의 트래픽을 감시하여 안전한 데이터만을 네트워크 중간에서 릴레이하는 유형의 방화벽은?
① 패킷 필터링(packet filtering) 방화벽
② 응용 계층 게이트웨이(application level gateway)
③ 스테이트풀 인스펙션(stateful inspection) 방화벽
④ 서킷 레벨 게이트웨이(circuit level gateway)

문 5. IPSec에 대한 설명으로 옳지 않은 것은?
① 네트워크 계층에서 패킷에 대한 보안을 제공하기 위한 프로토콜이다.
② 인터넷을 통해 지점들을 안전하게 연결하는 데 이용될 수 있다.
③ 전송 모드와 터널 모드를 지원한다.
④ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.

문 6. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?
① 네트워크 기반 인증 시스템으로 공개키 기반구조를 이용하여 사용자 인증을 수행한다.
② 인증 서버는 사용자를 인증하며 TGS(Ticket Granting Server)를 이용하기 위한 티켓을 제공한다.
③ TGS는 클라이언트가 서버로부터 서비스를 받을 수 있도록 티켓을 발급한다.
④ 인증 서버나 TGS로부터 받은 티켓은 클라이언트가 그 내용을 볼 수 없도록 암호화되어 있다.

문 7. 사용자 패스워드의 보안을 강화하기 위한 솔트(salt)에 대한 설명으로 옳지 않은 것은?
① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.
② 해시 연산 비용이 증가되어 오프라인 사전적 공격을 어렵게 한다.
③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.
④ 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.

문 8. 스택 버퍼 오버플로(overflow) 공격에 대응하기 위한 방어 수단에 해당하지 않는 것은?
① 문자열 조작 루틴과 같은 불안전한 표준 라이브러리 루틴을 안전한 것으로 교체한다.
② 함수의 진입과 종료 코드를 조사하고 함수의 스택 프레임에 손상이 있는지를 검사한다.
③ 한 사용자가 프로그램에 제공한 입력이 다른 사용자에게 출력될 수 있도록 한다.
④ 매 실행 시마다 각 프로세스 안의 스택이 다른 곳에 위치하도록 한다.

문 9. 디지털 증거의 법적 효력을 인정받기 위해 포렌식 과정에서 지켜야 하는 원칙이 아닌 것은?
① 정당성의 원칙
② 무결성의 원칙
③ 재현의 원칙
④ 연계추적불가능의 원칙

문 10. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 내용이 아닌 것은?
① 주요정보통신기반시설의 보호체계
② 정보통신망에서의 이용자 보호 등
③ 정보통신망의 안정성 확보 등
④ 개인정보의 보호

문 11. 인터넷 보안 프로토콜에 해당하지 않는 것은?
① SSL
② HTTPS
③ S/MIME
④ TCSEC

문 12. 데이터 소유자가 다른 사용자의 식별자에 기초하여 자신의 의지대로 데이터에 대한 접근 권한을 부여하는 것은?

① 강제적 접근 제어(MAC)
② 임의적 접근 제어(DAC)
③ 규칙 기반 접근 제어(Rule-based AC)
④ 역할 기반 접근 제어(RBAC)

문 13. 생체 인증 기법에 대한 설명으로 옳지 않은 것은?

① 정적인 신체적 특성 또는 동적인 행위적 특성을 이용할 수 있다.
② 인증 정보를 망각하거나 분실할 우려가 거의 없다.
③ 지식 기반이나 소유 기반의 인증 기법에 비해 일반적으로 인식 오류 발생 가능성이 매우 낮다.
④ 인증 시스템 구축 비용이 비교적 많이 든다.

문 14. 시스템 침투를 위한 일반적인 해킹 과정 중 마지막 순서에 해당하는 것은?

① 공격
② 로그 기록 등의 흔적 삭제
③ 취약점 분석
④ 정보 수집

문 15. 공개키를 사용하는 전자 서명에 대한 설명으로 옳지 않은 것은?

① 송신자는 자신의 개인키로 서명하고 수신자는 송신자의 공개키로 서명을 검증한다.
② 메시지의 무결성과 기밀성을 보장한다.
③ 신뢰할 수 있는 제3자를 이용하면 부인봉쇄를 할 수 있다.
④ 메시지로부터 얻은 일정 크기의 해시 값을 서명에 이용할 수 있다.

문 16. 침입탐지시스템(IDS)의 탐지 기법 중 하나인 비정상행위(anomaly) 탐지 기법의 설명으로 옳지 않은 것은?

① 이전에 알려지지 않은 방식의 공격도 탐지가 가능하다.
② 통계적 분석 방법, 예측 가능한 패턴 생성 방법, 신경망 모델을 이용하는 방법 등이 있다.
③ 새로운 공격 유형이 발견될 때마다 지속적으로 해당 시그니처(signature)를 갱신해 주어야 한다.
④ 정상행위를 가려내기 위한 명확한 기준을 설정하기 어렵다.

문 17. 보안 해시 함수가 가져야 하는 성질 중 하나인 강한 충돌 저항성(strong collision resistance)에 대한 설명으로 옳은 것은?

① 주어진 해시 값에 대해, 그 해시 값을 생성하는 입력 값을 찾는 것이 어렵다.
② 주어진 입력 값과 그 입력 값에 해당하는 해시 값에 대해, 동일한 해시 값을 생성하는 다른 입력 값을 찾는 것이 어렵다.
③ 같은 해시 값을 생성하는 임의의 서로 다른 두 개의 입력 값을 찾는 것이 어렵다.
④ 해시 함수의 출력은 의사 난수이어야 한다.

문 18. 「전자서명법」상 공인인증기관이 발급하는 공인인증서에 포함되어야 하는 사항이 아닌 것은?

① 가입자의 전자서명검증정보
② 공인인증기관의 전자서명생성정보
③ 공인인증서의 유효기간
④ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보

문 19. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인키로 선택하고, A는 B에게 $21(=7^3 \bmod 23)$을, B는 A에게 $3(=7^2 \bmod 23)$을 전송한다면, A와 B가 공유하게 되는 비밀키 값은? (단, 소수 23과 그 소수의 원시근 7을 사용한다)

① 4
② 5
③ 6
④ 7

문 20. ISO 27001의 ISMS(Information Security Management System) 요구사항에 대한 내용으로 옳지 않은 것은?

① 자산 관리 : 정보 보호 관련 사건 및 취약점에 대한 대응
② 보안 정책 : 보안 정책, 지침, 절차의 문서화
③ 인력 자원 보안 : 인력의 고용 전, 고용 중, 고용 만료 후 단계별 보안의 중요성 강조
④ 준거성 : 조직이 준수해야 할 정보 보호의 법적 요소