【정보보호론】

1. 정보보호의 주요 목적(3원칙)으로 가장 적절하지 **않은** 것은?
① 무결성(Integrity) ② 기밀성(Confidentiality)
③ 신뢰성(Reliability) ④ 가용성(Availability)

2. OECD 개인정보보호 8개 원칙 중 개인정보의 유출, 권한, 접근금지 등 합리적인 보안장치 설정과 개인정보의 물리적·조직적·기술적 안전 조치 확보와 관련한 원칙으로 가장 적절한 것은?
① 수집제한의 원칙(Collection Limitation Principle)
② 목적명시의 원칙(Purpose Specification Principle)
③ 이용제한의 원칙(Use Limitation Principle)
④ 안전성 확보의 원칙(Security Safeguards Principle)

3. 사용자 인증 방법 중에서 신분증, 주민등록증 등을 이용하여 인증하는 방법으로 가장 적절한 것은?
① 지식 기반 인증(What you know)
② 소유 기반 인증(What you have)
③ 커버로스 인증(Kerberos)
④ 생체 기반 인증(What you are)

4. 각 주체가 각 객체에 접근할 때마다 관리자에 의해 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 접근 권한을 부여하는 접근 통제 정책으로 가장 적절한 것은?
① 강제적 접근 통제(Mandatory Access Control)
② 임의적 접근 통제(Discretionary Access Control)
③ 역할기반 접근 통제(Role Based Access Control)
④ 최소 권한 정책(Least Privilege Policy)

5. 정보의 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 “검증된 설계(Verified Design)”를 의미하는 보안등급으로 가장 적절한 것은?
① A등급 ② B등급
③ C등급 ④ D등급

6. 윈도우즈(Windows) 운영체제에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 가장 적절하지 **않은** 것은?
① route : 라우팅 테이블의 정보 확인
② netstat : 연결 포트 등의 네트워크 상태 정보 확인
③ nslookup : 사용자 계정 정보 확인
④ ipconfig : 컴퓨터에 설치되어 있는 랜 카드에 대한 구성 상태를 확인

7. 다음 중 블록 암호 알고리즘으로 가장 적절하지 **않은** 것은?
① RC5 ② RC4
③ Blowfish ④ SEED

8. 다음 중 CFB(Cipher-FeedBack mode)의 복호화 수식으로 가장 적절한 것은?(단, P_i: i번째 평문, C_i: i번째 암호문, $E_K(P_i)$:암호화, $D_K(C_i)$:복호화)
① $P_i = D_K(C_i)$ ② $P_i = D_K(C_i) \oplus C_{i-1}$
③ $P_i = C_i \oplus E_K(C_{i-1})$ ④ $P_i = D_K(C_i \oplus C_{i-1})$

9. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인키로 선택하고, A는 B에게 21(=7^3 mod 23)을, B는 A에게 3(=7^2 mod 23)을 전송한다면, A와 B가 공유하게 되는 비밀키 값으로 가장 적절한 것은?(단, 사용자 A와 B는 소수 23과 그 소수의 원시근 7을 공유하여 사용한다.)
① 3 ② 4 ③ 5 ④ 6

10. 다음 중 공개키 암호 알고리즘에 대한 설명으로 가장 적절한 것은?
① ElGamal은 소인수 분해의 어려움을 이용한다.
② Diffie-Hellman의 알고리즘은 이산대수의 어려움을 이용한다.
③ RSA는 정보의 비밀성 보장을 위한 암호화에만 사용된다.
④ Rabin 암호 알고리즘은 이산대수의 어려움을 이용한다.

11. 암호학적 해시 함수가 가져야 할 특성으로 가장 적절하지 **않은** 것은?
① 서로 다른 두 입력 메시지에 대해 같은 해시 값이 나올 가능성은 있으나, 계산적으로 같은 해시 값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.
② 해시 값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.
③ 입력 메시지의 길이에 따라 출력되는 해시 값의 길이는 비례해야 한다.
④ 입력 메시지와 그 해시 값이 주어졌을 때, 이와 동일한 해시 값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.

12. 다음 중 TCP/IP 프로토콜 계층과 각 계층에서 구현되는 보안 기술의 연결이 가장 적절한 것은?
① 응용 계층 - Kerberos ② 전송 계층 - IPSec
③ 네트워크 계층 - SSL/TLS ④ 데이터링크 계층 - SET

13. 다음 중 TCP와 UDP에 대한 설명으로 가장 적절하지 **않은** 것은?

서비스	TCP	UDP
① 신뢰성	패킷이 그들의 목적지에 도달했는지 확인하며, 패킷이 도달할 때, ACK를 수신하기 때문에, 신뢰성 있는 프로토콜이다.	패킷이 목적지에 도달되는 것을 보장하지 않기 때문에, 신뢰성이 없는 프로토콜이다.
② 패킷 순서	패킷 내에 순서번호를 사용하지 않는다.	패킷 내에 순서번호를 사용하여, 각 패킷들이 순차적으로 수신되도록 한다.
③ 혼잡 제어	목적지 컴퓨터는 데이터의 처리가 어렵거나, 전송 속도가 느려질 경우 이를 송신지 컴퓨터에 통보한다.	목적지 컴퓨터는 송신지 컴퓨터로 흐름제어에 대한 통보를 하지 않는다.
④ 속도	UDP보다 느리다.	TCP보다 빠르다.

14. 다음은 SSL 프로토콜에 대한 내용이다. 이에 대해 가장 적절한 것은?

- 상위계층에서 수신된 메시지를 전달하는 역할을 담당 - 데이터 분할, 압축, 메시지 인증 및 암호화 기능을 수행

① Alert Protocol ② Handshake Protocol
③ Record Protocol ④ Change Cipher Spec Protocol

15. ㉠, ㉡, ㉢에 들어갈 내용이 바르게 연결된 것은?

(㉠)은(는) 메시지 압축과 변조된 종단 간 연결로를 제공하고, 인증서를 이용해 서버와 클라이언트의 인증을 하는데 사용된다. (㉡)은(는) 인터넷과 같은 공개된 통신망에서 전자상거래를 하기 위한 “지불시스템에 대한 기술표준”으로 S/W와 H/W를 포함한다. (㉢)은(는) 인터넷상에서 VPN(Virtual Private Network)을 구현하는데 사용될 수 있도록 개발된 Protocol이다.

	㉠	㉡	㉢
①	SSL	SET	IPSec
②	SET	SSL	IPSec
③	SET	IPSec	SSL
④	SSL	IPSec	SET

16. 다음 중 PGP(Pretty Good Privacy)에 대한 설명으로 가장 적절하지 **않은** 것은?

① E-mail의 보안과 파일 암호화에 사용된다.
② 전자 서명, 기밀성, 압축, 단편화와 재조립 등의 기능이 있다.
③ E-mail 응용 프로그램에 플러그인도 가능하다.
④ 자신의 공개키를 전달하려면 인증기관의 서명이 필요하다.

17. 다음 설명에 해당하는 블루투스(Bluetooth) 공격 방법으로 가장 적절한 것은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격 방법은 블루투스 장치끼리 인증없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여, 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나, 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf) ② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug) ④ 블루재킹(BlueJacking)

18. 다음 설명에 해당하는 공격 방법으로 가장 적절한 것은?

웹 사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로, 사용자로 위장한 공격자가 웹 사이트에 프로그램 코드를 삽입하여, 나중에 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다.

① 세션 탈취(Session Hijacking)
② 제로 데이(Zero-Day) 공격
③ 패킷 스니핑(Packet Sniffing) 공격
④ XSS(Cross-Site Scripting)

19. 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류를 발생하게 하는 공격으로 가장 적절한 것은?

① 스푸핑(Spoofing)
② 스니핑(Sniffing)
③ 버퍼 오버플로(Buffer Overflow)
④ 스캐닝(Scanning)

20. 다음 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 ㉠, ㉡에 들어갈 용어로 가장 적절한 것은?

제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다. 1. 제23조의3에 따라 (㉠)으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 (㉡)가 고시하는 경우

	㉠	㉡
①	개인정보처리기관	방송통신위원회
②	개인정보처리기관	개인정보보호위원회
③	본인확인기관	개인정보보호위원회
④	본인확인기관	방송통신위원회