정보보호론

1. SSS(Server Side Script) 언어에 해당하지 않는 것은?
① IIS ② PHP
③ ASP ④ JSP

2. 정보나 정보시스템을 누가, 언제, 어떤 방법을 통하여 사용했는지 추적할 수 있도록 하는 것은?
① 인증성 ② 가용성
③ 부인방지 ④ 책임추적성

3. 디지털포렌식의 원칙에 대한 설명으로 옳지 않은 것은?
① 연계성의 원칙: 수집된 증거가 위변조되지 않았음을 증명해야 한다.
② 정당성의 원칙: 법률에서 정하는 적법한 절차와 방식으로 증거가 입수되어야 하며 입수 경위에서 불법이 자행되었다면 그로 인해 수집된 2차적 증거는 모두 무효가 된다.
③ 재현의 원칙: 불법 해킹 용의자의 해킹 도구가 증거 능력을 가지기 위해서는 같은 상황의 피해 시스템에 도구를 적용할 경우 피해 상황과 일치하는 결과가 나와야 한다.
④ 신속성의 원칙: 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 수집되어야 한다.

4. 다음에서 설명하는 국내 인증 제도는?

> ○ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의한 정보보호 관리체계 인증과 「개인정보 보호법」에 의한 개인정보보호 관리체계 인증에 관한 사항을 통합하여 한국인터넷진흥원과 금융보안원에서 인증하고 있다.
> ○ 한국정보통신진흥협회, 한국정보통신기술협회, 개인정보보호협회에서 인증심사를 수행하고 있다.

① CC ② BS7799
③ TCSEC ④ ISMS-P

5. 「개인정보 보호법」 제28조의2(가명정보의 처리 등)의 내용으로서 (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

> 제1항 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 [(가)] 가명정보를 처리할 수 있다.
> 제2항 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함[(나)].

(가)	(나)
① 동의를 받아	할 수 있다
② 동의를 받아	해서는 아니 된다
③ 동의 없이	해서는 아니 된다
④ 동의 없이	할 수 있다

6. SSL을 구성하는 프로토콜에 대한 설명으로 옳은 것은?
① Handshake는 두 단계로 이루어진 메시지 교환 프로토콜로서 클라이언트와 서버 사이의 암호학적 비밀 확립에 필요한 정보를 교환하기 위한 것이다.
② 클라이언트와 서버는 각각 상대방에게 ChangeCipherSpec 메시지를 전달함으로써 메시지의 서명 및 암호화에 필요한 매개변수가 대기 상태에서 활성화되어 비로소 사용할 수 있게 된다.
③ 송신 측의 Record 프로토콜은 응용 계층 또는 상위 프로토콜의 메시지를 단편화, 암호화, 압축, 서명, 헤더 추가의 순서로 처리하여 전송 프로토콜에 전달한다.
④ Alert 프로토콜은 Record 프로토콜의 하위 프로토콜로서 처리 과정의 오류를 알리는 메시지를 전달한다.

7. 블록체인 기술의 하나인 하이퍼레저 패브릭에 대한 설명으로 옳지 않은 것은?
① 허가형 프라이빗 블록체인의 형태로 MSP(Membership Service Provider)라는 인증 관리 시스템에 등록된 사용자만 참여할 수 있다.
② 체인코드라는 스마트 컨트랙트를 통해서 분산 원장의 데이터를 읽고 쓸 수 있다.
③ 분산 원장은 원장의 현재 상태를 나타내는 월드 스테이트와 원장의 생성 시점부터 현재까지의 사용 기록을 저장하는 블록체인 두 가지로 구성된다.
④ 트랜잭션을 정해진 순서로 정렬하는 과정을 합의로 정의하고, 이를 위해 지분 증명 방식과 BFT(Byzantine Fault Tolerance) 알고리즘을 사용한다.

8. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3(본인확인기관의 지정 등)에 의거하여 다음의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 "본인확인업무"라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있는 기관은?

> 1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
> 2. 본인확인업무의 수행을 위한 기술적·재정적 능력
> 3. 본인확인업무 관련 설비규모의 적정성

① 과학기술정보통신부 ② 개인정보보호위원회
③ 방송통신위원회 ④ 금융위원회

9. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

> 악성 코드의 정적 분석은 파일을 [(가)]하여 상세한 동작을 분석하는 단계로 악성 코드 파일을 역공학 분석하여 그 구조, 핵심이 되는 명령 부분, 동작 방식 등을 알아내는 것을 목표로 한다. 이를 위하여 역공학 분석을 위한 [(나)]와/과 같은 도구를 활용한다.

(가)	(나)
① 패킹	OllyDbg
② 패킹	Regshot
③ 디스어셈블링	Regshot
④ 디스어셈블링	OllyDbg

10. 프로그램 입력 값에 대한 검증 누락, 부적절한 검증 또는 데이터의 잘못된 형식 지정으로 인해 발생할 수 있는 보안 공격이 아닌 것은?
① HTTP GET 플러딩 ② SQL 삽입
③ 크로스사이트 스크립트 ④ 버퍼 오버플로우

11. 정보의 무결성에 중점을 둔 보안 모델은?
① Biba ② Bell-LaPadula
③ Chinese Wall ④ Lattice

12. 허니팟에 대한 설명으로 옳지 않은 것은?
① 공격자가 중요한 시스템에 접근하지 못하도록 실제 시스템처럼 보이는 곳으로 유인한다.
② 공격자의 행동 패턴에 관한 정보를 수집한다.
③ 허니팟은 방화벽의 내부망에는 설치할 수 없다.
④ 공격자가 가능한 한 오랫동안 허니팟에서 시간을 보내도록 하고 그사이 관리자는 필요한 대응을 준비한다.

13. 다음에 설명하는 위험 분석 방법은?

○ 구조적인 방법론에 기반하지 않고 분석가의 경험이나 지식을 사용하여 위험 분석을 수행한다. ○ 중소 규모의 조직에는 적합할 수 있으나 분석가의 개인적 경험에 지나치게 의존한다는 단점이 있다.

① 기준선 접근법
② 비정형 접근법
③ 상세 위험 분석
④ 복합 접근법

14. RSA를 적용하여 7의 암호문 11과 35의 암호문 42가 주어져 있을 때, 알고리즘의 수학적 특성을 이용하여 계산한 245(=7 * 35)의 암호문은? (단, RSA 공개 모듈 n = 247, 공개 지수 e = 5)
① 2 ② 215
③ 239 ④ 462

15. 사용자 A가 사전에 비밀키를 공유하고 있지 않은 사용자 B에게 기밀성 보장이 요구되는 문서 M을 보내기 위한 메시지로 옳은 것은?

KpuX: 사용자 X의 공개키 KprX: 사용자 X의 개인키 KS: 세션키 H(): 해시 함수 E(): 암호화 ||: 연결(concatenation) 연산자

① M || E_{KprA}(H(M))
② E_{KprA}(M || H(M))
③ E_{KS}(M) || E_{KpuB}(KS)
④ E_{KS}(M) || E_{KprA}(KS)

16. 보안 서비스와 이를 제공하기 위한 보안 기술을 잘못 연결한 것은?
① 데이터 무결성 – 암호학적 해시
② 신원 인증 – 인증서
③ 부인방지 – 메시지 인증 코드
④ 메시지 인증 – 전자 서명

17. 웹 서버와 클라이언트 간의 쿠키 처리 과정으로 옳지 않은 것은?
① HTTP 요청 메시지의 헤더 라인을 통한 쿠키 전달
② HTTP 응답 메시지의 상태 라인을 통한 쿠키 전달
③ 클라이언트 브라우저의 쿠키 디렉터리에 쿠키 저장
④ 웹 서버가 클라이언트에 관해 수집한 정보로부터 쿠키를 생성

18. 「개인정보 보호법」 제15조(개인정보의 수집·이용)에서 개인정보처리자가 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있는 경우에 해당하지 않는 것은?
① 정보주체의 동의를 받은 경우
② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
③ 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
④ 공공기관과의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

19. 함수 P에서 호출한 함수 Q가 자신의 작업을 마치고 다시 함수 P로 돌아가는 과정에서의 스택 버퍼 운용 과정을 순서대로 바르게 나열한 것은?

(가) 스택에 저장되어 있는 복귀 주소(return address)를 pop한다. (나) 스택 포인터를 프레임 포인터의 값으로 복원시킨다. (다) 이전 프레임 포인터 값을 pop하여 스택 프레임 포인터를 P의 스택 프레임으로 설정한다. (라) P가 실행했던 함수 호출(function call) 인스트럭션 다음의 인스트럭션을 실행한다.

① (가) → (나) → (다) → (라)
② (가) → (다) → (라) → (나)
③ (나) → (가) → (라) → (다)
④ (나) → (다) → (가) → (라)

20. 무선 네트워크 보안에 대한 설명으로 옳은 것은?
① 이전에 사용했던 WEP의 보안상 약점을 보강하기 위해서 IETF에서 WPA, WPA2, WPA3를 정의하였다.
② WPA는 TKIP 프로토콜을 채택하여 보안을 강화하였으나 여전히 WEP와 동일한 메시지 무결성 확인 방식을 사용하는 약점이 있다.
③ WPA2는 무선 LAN 보안 표준인 IEEE 802.1X의 보안 요건을 충족하기 위하여 CCM 모드의 AES 블록 암호 방식을 채택하고 있다.
④ WPA-개인 모드에서는 PSK로부터 유도된 암호화 키를 사용하는 반면에, WPA-엔터프라이즈 모드에서는 인증 및 암호화를 강화하기 위해 RADIUS 인증 서버를 두고 EAP 표준을 이용한다.