정보보호론

문 1. Biba 보안 모델에 대한 설명으로 옳은 것은?

① 이해가 상충되는 회사들 간의 정보 흐름이 일어나지 않도록 고안되었다.
② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.
③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.
④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

문 2. IT 재해복구체계 수립 시, 업무영향분석(BIA: Business Impact Analysis) 과정에서 고려하는 항목이 아닌 것은?

① MTD(Maximum Tolerable Downtime)
② MTU(Maximum Transfer Unit)
③ RTO(Recovery Time Objective)
④ RPO(Recovery Point Objective)

문 3. 다음에서 설명하는 위험 분석 접근 방법은?

> ○ 정형화되고 구조화된 프로세스를 사용하는 대신, 분석가 개인의 지식 및 경험을 활용한다.
> ○ 비교적 비용대비 효과가 우수하며 중·소규모 조직에 적합하다.
> ○ 개인적인 경험에 의존하므로 정당성이나 일관성이 부족할 수 있다.

① 기준선 접근(Baseline Approach)
② 상세 위험 분석(Detailed Risk Analysis)
③ 비형식적 접근(Informal Approach)
④ 복합 접근(Combined Approach)

문 4. 다음 수식에 의해 산출되는 것은?

$$H[(K^{+} \oplus opad) \,||\, H[(K^{+} \oplus ipad) \,||\, M]]$$

H: 해시 함수 K^{+}: 비밀키 K에 0을 덧붙인 것
M: 메시지 ipad, opad: 특정 상수
⊕: XOR ||: 연결(concatenation)

① GMAC
② HMAC
③ CMAC
④ 전자 서명

문 5. 「정보보호 및 개인정보보호 관리체계(ISMS-P)의 인증 등에 관한 고시」상의 인증심사 기준 중, '개인정보 처리 단계별 요구사항'에 포함되지 않는 것은?

① 사용자 계정 관리
② 이용자 단말기 접근 보호
③ 영상정보처리기기 설치·운영
④ 개인정보처리방침 공개

문 6. 다음 리눅스 /etc/shadow 파일 항목에 대한 설명으로 옳지 않은 것은?

```
abcd:$1$qPZPGTVz$RDqazm48WaMXw3Mvy4OQb1:
17562:0:99999:7:3::
```

① 계정명은 abcd이다.
② 계정 패스워드의 해시값 계산에 사용된 해시 함수는 MD-5이다.
③ 솔트(salt)값은 qPZPGTVz이다.
④ 계정 패스워드의 유효기간은 7일이다.

문 7. 「개인정보 보호법」상 개인정보처리자가 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당하지 않는 것은?

① 정보주체로부터 별도의 동의를 받은 경우
② 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
③ 범죄의 예방을 위하여 필요한 경우
④ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우

문 8. 「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 그에 대한 설명으로 옳지 않은 것은?

① 인증 수행 제한 – 인증 반복시도 제한 및 인증실패 등에 대한 인증제한 기능 설계
② 암호키 관리 – 암호키 생성, 분배, 접근, 파기 등 안전하게 암호키 생명주기를 관리할 수 있는 방법 설계
③ 예외 처리 – 보안기능 동작을 위해 사용되는 입력값과 함수의 외부입력값 및 수행결과에 대한 처리방법 설계
④ 시스템 자원 접근 및 명령어 수행 입력값 검증 – 시스템 자원접근 및 명령어 수행을 위해 사용되는 입력값에 대한 유효성 검증방법과 유효하지 않은 값에 대한 처리방법 설계

문 9. 두 소수, $p = 13$, $q = 11$을 사용하는 RSA 시스템에서 키값 (e, d)로 사용할 수 있는 쌍은?

① (7, 11)
② (7, 23)
③ (13, 37)
④ (13, 47)

문 10. 암호 화폐인 비트코인이 채택한 블록체인의 블록 헤더에 포함되는 구성 요소가 아닌 것은?

① 이전 블록의 헤더를 두 번 연속 해시한 값
② 해당 블록에 포함된 모든 트랜잭션의 해시로부터 추출된 merkle root 해시값
③ 작업증명(proof of work) 조건을 만족하는 nonce 값
④ 블록 생성자(miner)의 계정

문 11. 다음에서 설명하는 해시 함수(H)의 특성은?

> 주어진 메시지 x에 대해, $H(y) = H(x)$를 만족하면서 $y \neq x$인 y를 찾는 것이 계산상 매우 어려워야 한다.

① 의사난수성(Pseudo-randomness)
② 역상 저항성(Pre-image Resistance)
③ 약한 충돌 저항성(Weak Collision Resistance)
④ 강한 충돌 저항성(Strong Collision Resistance)

문 12. ㉠ ~ ㉢에 들어갈 윈도우 운영체제 보안 컴포넌트를 모두 바르게 제시한 것은?

> (㉠)은 로컬 사용자에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스이다.
> (㉡)은 커널 모드에서 수행되며, 사용자나 프로세스가 어떤 객체를 열려고 시도하면, 접근 권한을 확인한다.
> (㉢)는 사용자 모드에서 수행되며, 로컬 보안 정책을 집행하는 책임이 있다.

	㉠	㉡	㉢
①	SAM	SRM	LSA
②	SRM	SAM	LSA
③	SAM	SRM	SID
④	SRM	SAM	SID

문 13. 다음의 블록암호 운용모드 중, 암호 과정에서는 암호화 함수 E를, 복호 과정에서는 E와 다른 복호화 함수 D를 필요로 하는 것만을 모두 고르면?

> ㄱ. ECB　　ㄴ. CBC　　ㄷ. CFB　　ㄹ. OFB

① ㄱ
② ㄱ, ㄴ
③ ㄷ, ㄹ
④ ㄱ, ㄴ, ㄹ

문 14. 「개인정보 보호법」상 '정보주체의 권리 보장'에 대한 설명으로 옳지 않은 것은?

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.
② 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있다.
③ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.
④ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

문 15. 패스워드를 이용해서 원격 사용자를 인증하는 경우, 호스트는 비표(nonce)라는 일회성 임의 숫자 r를 생성하고 이와 함께 두 함수 h()와 f()를 사용자에게 제시한다. 사용자는 이에 대한 응답으로 f(r′, h(P′))를 반환한다. 호스트는 $r' = r$, $h(P') = h$(사용자 패스워드)의 여부를 판단하여 인증을 완료한다. 이때, r를 사용하는 것은 어떤 공격에 대비하기 위한 것인가?

① 전사 공격(Brute-Force Attack)
② 트래픽 스니핑 공격(Traffic Sniffing Attack)
③ 패스워드 사전 공격(Password Dictionary Attack)
④ 재전송 공격(Replay Attack)

문 16. HTTP 버전 1.1에 대한 설명으로 옳지 않은 것은?

① TCP를 전송 프로토콜로 사용한다.
② 요청 메시지의 첫 줄인 요청 라인에는 메소드, URL, HTTP 버전 필드가 포함된다.
③ 요청과 그에 대한 응답이 같은 연결로 보내지는 지속 연결(persistent connection)을 기본으로 하며, 분리된 별도의 연결을 이용하는 비지속 연결(non-persistent connection)도 지원한다.
④ HTTP 서버가 클라이언트에 대한 정보를 유지하는 상태(stateful) 프로토콜이다.

문 17. 서버가 응용 메시지를 여러 개의 TCP 세그먼트로 나누어 클라이언트에게 전송하는 경우, TCP의 동작에 대한 설명으로 옳은 것은?

① 클라이언트와 서버 간의 TCP 연결 설정 후, 첫 번째 세그먼트의 순서 번호는 일반적으로 0부터 시작한다.
② 두 번째 세그먼트의 순서 번호는 첫 번째 세그먼트가 운반에 성공한 데이터의 바이트 수를 첫 번째 세그먼트의 순서 번호에 더한 것이다.
③ 일정량의 데이터를 포함한 세그먼트를 정상적으로 수신한 클라이언트는 수신한 세그먼트의 순서 번호에 1을 더한 값을 확인응답 번호로 하여 응답하고 다음 세그먼트를 기다린다.
④ 클라이언트가 FIN 세그먼트를 보내고 서버가 이에 대한 ACK 세그먼트를 보냄으로써 서버의 데이터 전송을 위한 연결이 완전히 종료된다.

문 18. 다음에서 설명하는 네트워크 기반 공격 방법은?

> ○ TCP 헤더 정보를 보고 패킷을 걸러내는 방화벽을 우회하기 위한 공격 방법이다.
> ○ IP 단편 옵션을 이용하여 매우 작게 패킷을 나누어서 TCP 헤더 자체가 분리되도록 만든다.
> ○ 일부 패킷 필터는 첫 번째 단편만 검사하고, 나머지 단편은 모두 통과시키기 때문에 이러한 공격 방법이 유효할 수 있다.

① Source Routing Attack
② Ping of Death
③ Trinoo
④ Tiny Fragment Attack

문 19. 다음은 「정보보호산업의 진흥에 관한 법률」상 정보보호산업의 활성화를 위한 구매수요정보의 제공에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

> 「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 (㉠) 정보보호기술등에 대한 구매수요 정보를 (㉡)에게 제출하여야 한다.

	㉠	㉡
①	매년	과학기술정보통신부장관
②	매년	행정안전부장관
③	2년마다	과학기술정보통신부장관
④	2년마다	행정안전부장관

문 20. IEEE 802.11i에서 정의한 무선 랜 데이터 보안 프로토콜로, 메시지 무결성 코드(MIC)와 RC4 암호 알고리즘을 이용하여 메시지 무결성과 데이터 기밀성을 제공하는 것은?

① EAP
② WEP
③ CCMP
④ TKIP