정보보호론

1. 적극적(active) 공격에 해당하는 것만을 모두 고르면?

ㄱ. 위장(masquerade)
ㄴ. 변조(modification)
ㄷ. 도청(eavesdropping)
ㄹ. 트래픽 분석(traffic analysis)

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄹ ④ ㄷ, ㄹ

2. 전자서명이 제공하는 보안 요소가 아닌 것은?
① 메시지 무결성
② 서명자 인증
③ 서명 부인 방지
④ 메시지 기밀성

3. 흔히 'Orange Book'으로 불리며, 미국에서 제정된 보안 표준으로 효과적인 정보보호 시스템 평가의 기준 개발과 이러한 기준에 맞게 개발된 제품들을 평가하는 데 초점을 두고 있는 정보 보안 평가 기준은?
① CC ② PIMS
③ ITSEC ④ TCSEC

4. 다음에서 설명하는 보안 모델은?

○ 상업 환경에서의 데이터의 무결성에 중점을 둔 것이다.
○ 정형화된 트랜잭션의 처리 과정에서 직무를 분리하도록 한다.
○ 제약을 받는(constrained) 데이터 항목에 대해 무결성 검증 절차를 거치도록 한다.

① Bell-LaPadula
② Biba
③ Clark-Wilson
④ Lattice

5. 다음에서 설명하는 정보보호의 목표에 해당하는 것은?

○ 정당한 사용자가 정보시스템의 데이터 또는 자원을 필요로 하는 시점에 사용할 수 있는 성질이다.
○ 확보 방법으로 데이터 백업, 중복성 유지 등이 있다.
○ 위협 요소로는 서비스 거부 공격, 지진, 홍수 등이 있다.

① 기밀성 ② 가용성
③ 무결성 ④ 책임추적성

6. 「개인정보 보호법」에서 규정하고 있는 개인정보에 해당하지 않는 것은?
① 성명
② 주민등록번호
③ 영상 등을 통하여 개인을 알아볼 수 있는 정보
④ 사망자에 대한 정보

7. 다음에서 설명하는 기술은?

○ 공인 IP 주소가 내부 사설 IP 주소보다 부족한 경우에 적용 가능한 방식이다.
○ 내부 사설 IP 주소나 내부 네트워크 대역을 공인 IP로 자동 매핑하는 기능을 제공한다.
○ 내부 IP 주소를 외부로부터 보호해 주는 기능을 제공하기도 한다.

① ARP
② IPS
③ NAT
④ VLAN

8. 다음과 같은 과정으로 진행되는 공격은?

1. 공개키 암호 방법을 사용하는 A와 B의 통신에 C가 개입한다.
2. C는 A의 공개키를 가로채어 B에게 C의 공개키를 A의 공개키처럼 전송한다.
3. B는 C의 공개키로 메시지를 암호화하여 A에게 전송한다.
4. C는 B가 보낸 메시지를 가로채어 C의 개인키로 복호화한다.
5. C는 복호화한 메시지를 단계 2에서 가로챈 A의 공개키로 암호화하여 A에게 B가 보낸 것처럼 전송한다.
6. A는 자신의 개인키로 메시지를 복호화한다.

① Smurf
② 중간자(MITM)
③ Sniffing
④ Slowloris

9. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

공개키 암호 방식으로 송신자가 수신자에게 보낼 평문을 암호화할 때는 [(가)]를 사용하고, 송신자가 평문을 전자서명하여 수신자에게 보낼 때는 [(나)]를 사용한다.

(가)	(나)
① 송신자의 공개키	송신자의 공개키
② 수신자의 공개키	송신자의 공개키
③ 송신자의 공개키	송신자의 개인키
④ 수신자의 공개키	송신자의 개인키

10. 「개인정보 보호법」 제3조(개인정보 보호 원칙)상 개인정보 보호 원칙으로 옳지 않은 것은?
① 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 가명처리가 가능한 경우에는 가명에 의하여, 가명처리로 목적을 달성할 수 없는 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

11. 스택 오버플로(stack overflow) 공격에 대응하는 방법으로 옳지 않은 것은?

① 스택에 저장할 수 있는 데이터의 최대 길이를 지정해야 하는 함수를 사용한다.
② 스택에서 코드가 실행되는 것을 허용한다.
③ 스택 영역을 임의의 메모리 주소에 할당하여 스택 영역의 주소에 대한 추측을 어렵게 한다.
④ 함수의 종료 연산을 수행하기 전에 카나리(canary) 값의 변경 여부를 검사한다.

12. ISMS-P 인증을 위한 정보보호 보호대책 요구사항 중 '인증 및 권한관리' 항목에 해당하지 않는 것은?

① 비밀번호 관리
② 접근권한 검토
③ 정보시스템 보호
④ 특수 계정 및 권한관리

13. 정보보호 관련 법률과 소관 부처를 잘못 짝지은 것은?

①「개인정보 보호법」- 개인정보보호위원회
②「위치정보의 보호 및 이용 등에 관한 법률」- 과학기술정보통신부
③「공공기관의 정보공개에 관한 법률」- 행정안전부
④「전자서명법」- 과학기술정보통신부

14. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

> 공격자는 웹사이트에서 인증 과정을 거쳐 활성 세션을 가지고 있는 사용자로 하여금 공격자가 만든 악의적인 링크에 접근하게 유도한다. 이 링크를 클릭한 사용자는 자신도 인지하지 못한 채 공격자가 의도한 데이터를 HTTP 몸체(body)에 첨부하여 페이지 내용을 변경하도록 하는 HTTP [(가)] 요청을 웹사이트로 보내다. 이와 같은 방식의 공격을 [(나)]라고 한다.

(가)	(나)
① GET	XSS
② GET	CSRF
③ POST	XSS
④ POST	CSRF

15. S/MIME(RFC 8551)의 데이터 콘텐트 유형(data content type) 중 데이터의 기밀성만을 제공하는 것은?

① Signed-Data
② Enveloped-Data
③ Auth-Enveloped-Data
④ Compressed-Data

16. 리눅스 /etc/shadow 파일에 포함되지 않는 것은?

① 사용자 계정명
② 솔트(salt)
③ 대칭키 암호 알고리즘의 종류
④ 기준일(epoch)부터 패스워드가 최종 수정된 날까지의 일수

17. 소수 p를 선택하고, 위수가 p-1인 원시근을 사용하는 대신에 p-1의 소인수인 q를 위수로 갖는 원소를 이용해서 서명과 검증에 사용할 키를 생성하는 전자서명 구조는?

① RSA
② ElGamal
③ ECDSA
④ Schnorr

18. TLS 핸드셰이크 프로토콜의 목적에 해당하는 것만을 모두 고르면?

> ㄱ. 인증서 확인
> ㄴ. 세션을 활성 상태로 유지
> ㄷ. 세션키 생성 및 교환
> ㄹ. 응용 데이터 전송

① ㄱ, ㄷ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

19. 다음 수식으로 표현된 HMAC에 대한 설명으로 옳지 않은 것은? (단, K는 키, M은 메시지, H는 해시 함수, ⊕는 XOR, ||는 연결(concatenation)이다)

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

① HMAC 구조는 해시 함수 H로 MD5, SHA-1, SHA-512 등 가용한 것을 선택할 수 있도록 되어 있다.
② K는 HMAC를 주고받는 사용자가 공유하는 비밀키이다.
③ K^{+}는 K의 왼쪽에 0을 패딩해서 전체 비트 수가 해시 함수 출력의 크기와 같게 되도록 한 것이다.
④ ipad와 opad는 각각 16진수 36과 5C가 반복된 것으로, 해시 함수에 입력되는 블록의 크기와 같다.

20. 다음 수식으로 나타낸 블록 암호 운용 모드에 대한 설명으로 옳은 것은?

P_i: 평문 블록 C_i: 암호문 블록 E_K: 암호화 함수 K: 키 IV: 초기벡터	$C_1 = E_K(P_1 \oplus IV)$ $C_i = E_K(P_i \oplus C_{i-1}),\ i = 2, 3, ..., N$

① 복호화 함수를 D_K이라고 하면, 평문 블록 $P_1 = D_K(C_1) \oplus IV$이고, $P_i = D_K(C_i) \oplus C_{i-1},\ i = 2, 3, ..., N$이다.
② 송신자와 수신자가 공유하는 IV는 반드시 제3자에게 비밀로 해야 한다.
③ 암호문 블록 C_j $(j = 1, 2, ..., N)$의 전송 도중에 비트 오류가 발생하면, 복호화된 P_j부터 P_N까지의 모든 평문 블록에 영향을 미친다.
④ 여러 평문 블록에 대한 암호화 과정의 병렬처리가 가능하다.