【정보보호론】

1. 다음에 설명하는 정보보호의 목표로 가장 적절한 것은?

> 정당한 방법으로 권한을 받은 사용자가 자원을 필요로 할 때, 아무런 방해 없이 자원에 접근하고 사용할 수 있음을 보장한다.

① 기밀성(confidentiality) ② 무결성(integrity)
③ 가용성(availability) ④ 신뢰성(reliability)

2. 다음 대칭키 암호화에서 키 K값으로 가장 적절한 것은?

> · 대칭키 암호화: 8비트 정보 P와 K의 배타적 논리합(XOR) 연산의 결과를 C라 함
> · P=00101100
> · C=10000110

① 11010010 ② 10101010
③ 01010101 ④ 10011001

3. 복호화 수식이 다음과 같을 때 블록 암호 운영모드로 가장 적절한 것은?
(단, P_i: i번째 평문, C_i: i번째 암호문, $D_K(C_i)$: 복호화)

$$P_i = D_K(C_i) \oplus C_{i-1}$$

① CBC(Cipher Block Chaining, 암호블록 연쇄) 모드
② CFB(Cipher FeedBack, 암호 피드백) 모드
③ ECB(Electronic CodeBook, 전자코드북) 모드
④ CTR(Counter, 카운터) 모드

4. 하이브리드 암호시스템에 대한 설명으로 가장 적절하지 **않은** 것은?

① 대칭키 암호시스템과 공개키 암호시스템의 장점을 조합하였다.
② 평문 메시지는 대칭키 암호로 암호화한다.
③ 암호화에서 사용하는 세션키는 의사난수 생성기를 이용하여 생성한다.
④ PGP(Pretty Good Privacy), SSL/TLS(Secure Socket Layer/Transport Layer Security), RSA에서 하이브리드 암호 시스템을 사용한다.

5. 메시지 인증 코드와 전자서명에 대한 설명으로 가장 적절하지 **않은** 것은?

① 메시지 인증 코드와 전자서명 모두 무결성을 확인할 수 있다.
② 메시지 인증 코드는 부인방지(non-repudiation) 기능을 제공한다.
③ 전자서명은 서명자를 인증하는 기능이 있다.
④ 메시지 인증 코드는 메시지와 비밀키를 사용한다.

6. 공개키 기반 구조(PKI: Public Key Infrastructure)에 대한 설명으로 가장 적절하지 **않은** 것은?

① 공개키 기반 구조의 구성요소로는 사용자(user), 등록기관(Registration Authority), 인증기관(Certification Authority), 저장소(repository) 등이 있다.
② 공개키 인증서를 발행하여 무결성, 인증, 부인방지를 보장한다.
③ 등록기관은 인증서와 인증서 취소 목록(Certificate Revocation List)을 발행하고, 공개키 등록 시 본인을 인증한다.
④ 저장소는 인증서를 보관해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 구성된 데이터베이스이다.

7. 다음 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

> (㉠) 공격은 소스 IP주소와 목적지 IP주소가 동일한 다량의 패킷을 특정 공격 대상 시스템으로 전송하면, 응답이 자기 자신에게 되돌아오도록 하여 시스템의 과부하를 유발한다.
> (㉡) 공격은 ICMP Echo 메시지를 큰 패킷으로 만들어, 공격 대상 시스템에 분할된 많은 양의 패킷을 도달시켜, 패킷 재결합으로 인한 시스템 과부하를 유발한다.
> (㉢) 공격은 ICMP 프로토콜과 브로드캐스팅 개념을 사용한 공격으로, 공격대상 호스트의 IP 주소를 source 주소로 갖는 ICMP Echo 요청 패킷을 directed 브로드캐스트 함으로써, 많은 양의 ICMP Echo 응답 패킷을 공격대상 호스트에 전송한다. 이는 공격대상 시스템의 자원을 고갈시킨다.

	㉠	㉡	㉢
①	LAND	ICMP Flooding	Ping of Death
②	LAND	Ping of Death	ICMP Flooding
③	Ping of Death	ICMP Flooding	LAND
④	Ping of Death	LAND	ICMP Flooding

8. 다음 TCP/IP 프로토콜의 계층별 역할에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

> (㉠) 계층에서는 송수신지 사이의 패킷을 전달한다. 이를 위해 IP 주소 지정, 패킷화, 단편화가 제공된다.
> (㉡) 계층에서는 근거리 통신망(LAN)에서 전송 매체에 데이터(프레임)를 송수신하는 역할을 담당한다.
> (㉢) 계층에서는 종단간 통신 서비스 제공을 담당한다. TCP와 UDP가 대표적인 프로토콜이다.

	㉠	㉡	㉢
①	네트워크	데이터링크	전송
②	네트워크	전송	데이터링크
③	전송	데이터링크	네트워크
④	전송	네트워크	데이터링크

9. 다음 사이버 공격 유형에 대한 설명 중 ㉠~㉢에 들어갈 내용으로 가장 적절하게 연결된 것은?

> (㉠)은 공격자가 도메인을 탈취하여 사용자가 정확한 URL 주소를 입력해도 가짜 사이트로 연결되도록 하는 방법이다.
> (㉡)은 이메일 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 신용정보 등의 기밀을 부정하게 얻으려는 사회공학기법을 사용한다.
> (㉢)은 문자메시지를 신뢰할 수 있는 사람이 보낸 것처럼 가장하여, 링크 접속을 유도한 뒤 개인정보를 빼내는 방법이다.

	㉠	㉡	㉢
①	스미싱(Smishing)	피싱(Phishing)	파밍(Pharming)
②	스미싱(Smishing)	파밍(Pharming)	피싱(Phishing)
③	파밍(Pharming)	피싱(Phishing)	스미싱(Smishing)
④	파밍(Pharming)	스미싱(Smishing)	피싱(Phishing)

10. 소인수분해의 어려움을 기반으로 한 RSA 암호 알고리즘에서 개인키 d는 7, 합성수 n은 33, 평문 값이 5일 때, 이를 암호화한 암호문의 값으로 가장 적절한 것은?

① 12 ② 13 ③ 21 ④ 26

11. IEEE 802.11i에서 데이터를 보호하기 위해서 AES 알고리즘을 사용한 암호화 운영모드와 메시지 인증기법으로 가장 적절하게 짝지은 것은?

① CBC 모드, HMAC 인증　② CBC 모드, CBC-MAC 인증
③ CTR 모드, HMAC 인증　④ CTR 모드, CBC-MAC 인증

12. 이메일 보안 S/MIME에 대한 설명 중 가장 적절한 것은?

① 동봉된 데이터(enveloped data)는 암호화된 내용과 서명자의 공개키로 구성된다.
② 서명된 데이터(signed data)는 메시지 다이제스트 값을 서명자의 공개키로 암호화한 후, 그 값을 Base64로 부호화한다.
③ 명문-서명 데이터(clear-signed data)는 내용과 내용에 대한 전자서명으로 구성되며, 전자서명만 Base64로 부호화한다.
④ 서명되고 동봉된 데이터(signed and enveloped data)에서 서명만 되거나 암호화된 개체는 중첩될 수 없다.

13. 웹사이트와 브라우저에 대한 공격 유형에 관한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

> (㉠) 공격법의 한 예로는 URL에 인자 형태로 악성 스크립트를 포함시킨 메일을 사용자에게 보낸 후, 사용자가 URL을 클릭하면 서버로부터 반송된 오류 메시지에 포함된 악성 스크립트가 실행되는 방법이 있다.
> (㉡) 공격법의 한 예로는 로그인 상태인 사용자의 세션 쿠키와 다른 인증정보를 취약한 웹 애플리케이션에 자동으로 포함시키고, 공격자가 의도한 HTTP 요청을 사용자가 보낸 것처럼 자동으로 보내는 방법이 있다.

	㉠	㉡
①	Reflected XSS	CSRF
②	SQL 인젝션	Reflected XSS
③	CSRF	SQL 인젝션
④	Reflected XSS	S-HTTP

14. 다음에 설명하는 서명기법을 사용하는 응용보안 프로토콜로 가장 적절한 것은?

> 사용자의 신용카드 번호와 같은 지불정보는 은행의 공개키로 암호화하여 상점에 숨기고, 주문정보는 상점의 공개키로 암호화하여 은행이 알지 못하도록 하는 서명기법

① PGP(Pretty Good Privacy)
② SET(Secure Electronic Transaction)
③ IPsec(IP Security)
④ Bitcoin

15. 웹 보안을 위한 TLS 프로토콜의 핸드셰이크 과정에서 클라이언트와 서버가 Cipher Suite로 TLS_RSA_WITH_AES_128_CBC_SHA256을 채택하였다. 다음 설명 중 가장 적절하지 **<u>않은</u>** 것은?

① RSA 알고리즘을 이용하여 상호 인증을 수행한다.
② 레코드 프로토콜에서 데이터를 암호화할 때, 128비트 키 AES 알고리즘을 CBC 모드로 사용한다.
③ 사용 중인 AES 알고리즘은 암호명세변경(ChangeCipherSpec) 프로토콜을 통해 변경할 수 있다.
④ 레코드 프로토콜에서 메시지 인증 값은 해시함수 SHA256을 CBC-MAC 방식으로 사용하여 만든다.

16. 운영체제의 이중 모드에 대한 설명 중 ㉠과 ㉡에 들어갈 용어로 가장 적절하게 연결된 것은?

> 운영체제의 구조는 이중 모드(dual mode)로 되어 있는데, 이는 사용자 모드(user mode)와 커널 모드(kernel mode)이다. 이 중 사용자 모드에서 하드웨어 자원을 사용하려고 하면 (㉠)가(이) 발생해서 운영체제에 도움을 요청한다.
> 또한, 사용자 모드로 실행 중인 프로그램에서 포인터를 사용하여 커널 주소 영역 메모리를 접근하려 하면 (㉡)를(을) 발생시켜 커널 영역을 보호한다.

	㉠	㉡
①	시스템 호출	교착상태
②	예외	스케줄링
③	시스템 호출	예외
④	교착상태	시스템 호출

17. 보안 운영체제의 설계 원리와 이에 대한 설명으로 가장 적절하지 **<u>않은</u>** 것은?

① 최소권한: 각각의 사용자와 프로그램은 가능한 최소한의 권한을 사용하여 시스템 자원을 사용하여야 한다.
② 허용에 근거한 접근: 접근 검토에 대한 기본 값은 접근 허용이며, 설계자는 접근을 차단하여야 하는 항목의 식별에 주의하여야 한다.
③ 완전한 조정: 직접적인 접근 시도와 접근 통제 메커니즘을 우회하려는 접근 시도를 완전히 검사하여야 한다.
④ 권한분리: 객체에 대한 권한은 두 개 이상의 조건에 의존하여야 한다.

18. BLP(Bell-LaPadula) 보안모델이 가지고 있는 특성과 규칙에 대한 설명으로 가장 적절하지 **<u>않은</u>** 것은?

① 정보의 불법적인 파괴나 변조를 방지하기 보다 비밀정보의 허가없는 접근을 방지하는 것이 목표이다.
② 강제적 정책에 의한 접근통제를 원할 때에 대한 통제 규칙을 정의한다.
③ 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 높으면 주체는 객체에 쓰기를 할 수 없다.
④ 주체가 객체를 읽기 위해서는 주체의 비밀 취급 허가 수준이 객체의 보안 분류 수준보다 낮아야 한다.

19. 다음과 같은 사례를 방지하기 위한 데이터베이스 보안통제로 가장 적절한 것은?

> 낮은 비밀 취급 등급자가 레코드 입력 시, 오류를 통하여 자신보다 높은 비밀 취급 등급자가 있다는 사실을 알게 되는 사례

① 접근 통제　② 추론 통제
③ 흐름 통제　④ 무결성 통제

20. 소프트웨어 개발과정에서 소스코드에 존재하는 버퍼 오버플로우에 취약한 함수, 하드 코드된 패스워드 등 잠재적인 취약점을 제거하고, 보안을 고려하여 기능을 구현할 때 지켜야 할 보안활동으로 가장 적절한 것은?

① 안전한 코딩(secure coding)
② 위험분석(risk analysis)
③ 모의 침투(penetration test)
④ 디지털 포렌식(digital forensics)