정보보호론

문 1. 정보시스템의 접근제어 보안 모델로 옳지 않은 것은?
① Bell LaPadula 모델 ② Biba 모델
③ Clark-Wilson 모델 ④ Spiral 모델

문 2. 정보보안에 대한 설명으로 옳은 것은?
① 부인 방지는 송신자나 수신자가 메시지를 주고받은 사실을 부인하지 못하도록 방지하는 것을 의미한다.
② 정보보호의 3대 목표는 기밀성, 무결성, 접근제어이다.
③ 공개키 암호 시스템은 암호화 키와 복호화 키가 동일하다.
④ 보안공격 유형 중 소극적 공격은 적극적 공격보다 탐지하기 매우 쉽다.

문 3. 비대칭키 암호화 알고리즘으로만 묶은 것은?
① RSA, ElGamal ② DES, AES
③ RC5, Skipjack ④ 3DES, ECC

문 4. 전자우편 서비스의 보안 기술로 옳지 않은 것은?
① PGP(Pretty Good Privacy)
② S/MIME(Secure/Multipurpose Internet Mail Extension)
③ SET(Secure Electronic Transaction)
④ PEM(Privacy Enhanced Mail)

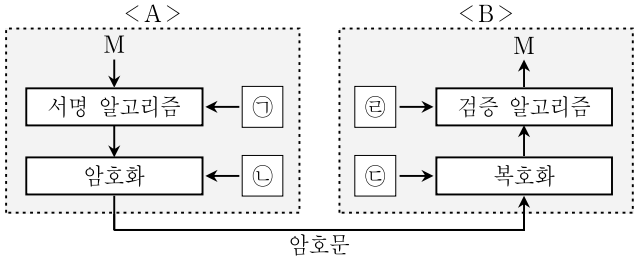
문 5. 서비스 거부(Denial of Service) 공격기법으로 옳지 않은 것은?
① SYN Flooding 공격 ② Teardrop 공격
③ Zero Day 공격 ④ Ping Flooding 공격

문 6. 해시(Hash) 함수에 대한 설명으로 옳은 것으로만 묶은 것은?

ㄱ. 입력데이터의 길이가 달라도 동일한 해시함수에서 나온 해시 결과값 길이는 동일하다.
ㄴ. 일방향 함수를 사용해서 해시함수를 구성할 수 있다.
ㄷ. 최대 128비트까지 해시함수의 입력으로 지원한다.
ㄹ. SHA-256의 해시 결과값 길이는 512비트이다.

① ㄱ, ㄴ ② ㄴ, ㄷ
③ ㄷ, ㄹ ④ ㄱ, ㄹ

문 7. A가 B에게 공개키 알고리즘을 사용하여 서명과 기밀성을 적용한 메시지(M)를 전송하는 그림이다. ㉠~㉣에 들어갈 용어로 옳은 것은?



㉠	㉡	㉢	㉣
① A의 공개키	B의 공개키	A의 개인키	B의 개인키
② A의 개인키	B의 개인키	A의 공개키	B의 공개키
③ A의 개인키	B의 공개키	B의 개인키	A의 공개키
④ A의 공개키	A의 개인키	B의 공개키	B의 개인키

문 8. 다음에서 설명하는 패스워드 크래킹(Cracking) 공격 방법은?

○ 사용자가 설정하는 대부분의 패스워드에 특정 패턴이 있음을 착안한 방법으로 패스워드로 사용할 만한 것을 사전으로 만들어놓고 이를 하나씩 대입하여 일치 여부를 확인하는 방법이다.
○ 패스워드에 부가적인 정보(salt)를 덧붙인 후 암호화하여 저장함으로써 이 공격에 대한 내성을 향상시킬 수 있다.

① Dictionary 공격
② Flooding 공격
③ Rainbow Table을 이용한 공격
④ Brute Force 공격

문 9. 다음에서 설명하는 보안 공격 기법은?

○ 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.
○ 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

① Buffer Overflow 공격
② Format String 공격
③ MITB(Man-In-The-Browser) 공격
④ Race Condition 공격

문 10. 다음의 내부에서 외부 네트워크 망으로 가는 방화벽 패킷 필터링 규칙에 대한 <보기>의 설명으로 옳은 것으로만 묶은 것은? (단, 방화벽을 기준으로 192.168.1.11은 내부 네트워크에 위치한 서버이고, 10.10.10.21은 외부 네트워크에 위치한 서버이다)

No.	From	Service	To	Action
1	192.168.1.11	25	10.10.10.21	Allow
2	Any	21	10.10.10.21	Allow
3	Any	80	Any	Allow
4	192.168.1.11	143	10.10.10.21	Allow

<보 기>

ㄱ. 내부 서버(192.168.1.11)에서 외부 서버(10.10.10.21)로 가는 Telnet 패킷을 허용한다.
ㄴ. 내부 Any IP대역에서 외부 서버(10.10.10.21)로 가는 FTP 패킷을 허용한다.
ㄷ. 내부 Any IP대역에서 외부 Any IP대역으로 가는 패킷 중 80번 포트를 목적지로 하는 패킷을 허용한다.
ㄹ. 내부 서버(192.168.1.11)에서 외부 서버(10.10.10.21)로 가는 POP3 패킷을 허용한다.

① ㄱ, ㄴ ② ㄴ, ㄷ
③ ㄷ, ㄹ ④ ㄱ, ㄹ

문 11. 전자서명이 제공하는 기능으로 옳지 않은 것은?
① 부인 방지(Non Repudiation)
② 변경 불가(Unalterable)
③ 서명자 인증(Authentication)
④ 재사용 가능(Reusable)

문 12. 위험 관리 과정에 대한 설명으로 ㉠, ㉡에 들어갈 용어로 옳은 것은?

> (가) (㉠)단계는 조직의 업무와 연관된 정보, 정보시스템을 포함한 정보자산을 식별하고, 해당 자산의 보안성이 상실되었을 때의 결과가 조직에 미칠 수 있는 영향을 고려하여 가치를 평가한다.
> (나) (㉡)단계는 식별된 자산, 위협 및 취약점을 기준으로 위험도를 산출하여 기존의 보호대책을 파악하고, 자산별 위협, 취약점 및 위험도를 정리하여 위험을 평가한다.

	㉠	㉡
①	가치평가 및 분석	취약점 분석 및 평가
②	위험 평가	가치평가 및 분석
③	자산식별 및 평가	취약점 분석 및 평가
④	자산식별 및 평가	위험 평가

문 13. 다음의 사이버 공격 유형과 그에 대한 <보기>의 설명을 바르게 연결한 것은?

> ㄱ. 피싱(Phishing) ㄴ. 파밍(Pharming) ㄷ. 스미싱(Smishing)

<보 기>

> A. 공격자가 도메인을 탈취하여 사용자가 정확한 사이트 주소를 입력해도 가짜 사이트로 연결되도록 하는 방법이다.
> B. 이메일 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여 신용정보 등의 기밀을 부정하게 얻으려는 사회공학기법이다.
> C. 문자메시지로 신뢰할 수 있는 사람이 보낸 것처럼 가장하여, 링크 접속을 유도한 뒤 개인정보를 빼내는 방법이다.

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

문 14. 「개인정보 보호법」상 정보주체가 자신의 개인정보 처리와 관련하여 갖는 권리로 옳지 않은 것은?

① 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
② 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
④ 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에 개인정보보호위원회에 개인정보 침해요인평가를 요청할 권리

문 15. 재해복구시스템의 복구 수준별 유형에 대한 설명으로 옳은 것은?

① Mirror site는 Cold site에 비해 구축 비용이 저렴하고, 복구에 긴 시간이 소요된다.
② Hot site는 Cold site에 비해 구축 비용이 높고, 데이터의 업데이트가 많은 경우에 적합하다.
③ Cold site는 Mirror site에 비해 높은 구축 비용이 필요하다.
④ Warm site는 Mirror site에 비해 전체 데이터 복구 소요 시간이 빠르다.

문 16. 무선랜의 보안 대응책으로 옳지 않은 것은?

① AP에 접근이 가능한 기기의 MAC 주소를 등록하고, 등록된 기기의 MAC 주소만 AP 접속을 허용한다.
② AP에 기본 계정의 패스워드를 재설정한다.
③ AP에 대한 DHCP를 활성화하여 AP 검색 시 SSID가 검색되도록 설정한다.
④ 802.1x와 RADIUS 서버를 이용해 무선 사용자를 인증한다.

문 17. 다음의 OSI 7계층과 이에 대응하는 계층에서 동작하는 <보기>의 보안 프로토콜을 바르게 연결한 것은?

> ㄱ. 2계층 ㄴ. 3계층 ㄷ. 4계층

<보 기>

> A. SSL/TLS B. L2TP C. IPSec

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	C	A
④	B	A	C

문 18. 「개인정보의 기술적·관리적 보호조치 기준」상 정보통신서비스 제공자 등이 준수해야 하는 사항으로 옳지 않은 것은?

① 이용자의 비밀번호 작성규칙은 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성하도록 수립한다.
② 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취한다.
③ 개인정보처리시스템에 개인정보취급자의 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관한다.
④ 개인정보처리시스템에 주민번호, 계좌번호를 저장할 때 안전한 암호알고리듬으로 암호화한다.

문 19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 ㉠, ㉡에 들어갈 용어로 옳은 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	개인정보보호위원회
②	개인정보처리기관	방송통신위원회
③	본인확인기관	개인정보보호위원회
④	본인확인기관	방송통신위원회

문 20. 다음에서 설명하는 국제공통평가기준(CC)의 구성요소는?

> ○ 정보제품이 갖추어야 할 공통적인 보안 요구사항을 모아 놓은 것이다.
> ○ 구현에 독립적인 보안 요구사항의 집합이다.

① 평가보증등급(EAL) ② 보호프로파일(PP)
③ 보안목표명세서(ST) ④ 평가대상(TOE)