정보보호론

문 1. 보안 공격 유형 중 소극적 공격으로 옳은 것은?
① 트래픽 분석(traffic analysis)
② 재전송(replaying)
③ 변조(modification)
④ 신분 위장(masquerading)

문 2. 암호학적 해시 함수가 가져야 할 특성으로 옳지 않은 것은?
① 서로 다른 두 입력 메시지에 대해 같은 해시값이 나올 가능성은 있으나, 계산적으로 같은 해시값을 갖는 서로 다른 두 입력 메시지를 찾는 것은 불가능해야 한다.
② 해시값을 이용하여 원래의 입력 메시지를 찾는 것은 계산상으로 불가능해야 한다.
③ 입력 메시지의 길이에 따라 출력되는 해시값의 길이는 비례해야 한다.
④ 입력 메시지와 그 해시값이 주어졌을 때, 이와 동일한 해시값을 갖는 다른 메시지를 찾는 것은 계산상으로 불가능해야 한다.

문 3. 다음 내용에 해당하는 공개키 기반 구조(PKI)의 구성요소로 옳은 것은?

> ○ 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다.
> ○ 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다.
> ○ 인증서 폐기 목록(certificate revocation list)을 작성한다.

① 사용자 ② 등록 기관
③ 인증 기관 ④ 디렉토리

문 4. ㉠과 ㉡에 들어갈 용어로 옳은 것은?

> (㉠)은(는) 디지털 콘텐츠를 구매할 때 구매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
> (㉡)은(는) 원본의 내용을 왜곡하지 않는 범위 내에서 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.

	㉠	㉡
①	크래커(Cracker)	커버로스(Kerberos)
②	크래커(Cracker)	워터마킹(Watermarking)
③	핑거프린팅(Fingerprinting)	커버로스(Kerberos)
④	핑거프린팅(Fingerprinting)	워터마킹(Watermarking)

문 5. 다음 내용에 해당하는 암호블록 운용 모드를 바르게 나열한 것은?

> ㄱ. 코드북(codebook)이라 하며, 가장 간단하게 평문을 동일한 크기의 평문블록으로 나누고 키로 암호화하여 암호블록을 생성한다.
> ㄴ. 현재의 평문블록과 바로 직전의 암호블록을 XOR한 후 그 결과를 키로 암호화하여 암호블록을 생성한다.
> ㄷ. 각 평문블록별로 증가하는 서로 다른 카운터 값을 키로 암호화하고 평문블록과 XOR하여 암호블록을 생성한다.

	ㄱ	ㄴ	ㄷ
①	CBC	ECB	OFB
②	CBC	ECB	CTR
③	ECB	CBC	OFB
④	ECB	CBC	CTR

문 6. 네트워크 공격에 대한 설명으로 옳지 않은 것은?
① Spoofing : 네트워크에서 송·수신되는 트래픽을 도청하는 공격이다.
② Session hijacking : 현재 연결 중인 세션을 가로채는 공격이다.
③ Teardrop : 네트워크 프로토콜 스택의 취약점을 이용한 공격 방법으로 시스템에서 패킷을 재조립할 때, 비정상 패킷이 정상 패킷의 재조립을 방해함으로써 네트워크를 마비시키는 공격이다.
④ Denial of Service : 시스템 및 네트워크의 취약점을 이용하여 사용 가능한 자원을 소비함으로써, 실제 해당 서비스를 사용하려고 요청하는 사용자들이 자원을 사용할 수 없도록 하는 공격이다.

문 7. 스택 버퍼 오버플로우 공격의 수행 절차를 순서대로 바르게 나열한 것은?

> ㄱ. 특정 함수의 호출이 완료되면 조작된 반환 주소인 공격 쉘 코드의 주소가 반환된다.
> ㄴ. 루트 권한으로 실행되는 프로그램 상에서 특정 함수의 스택 버퍼를 오버플로우시켜서 공격 쉘 코드가 저장되어 있는 버퍼의 주소로 반환 주소를 변경한다.
> ㄷ. 공격 쉘 코드를 버퍼에 저장한다.
> ㄹ. 공격 쉘 코드가 실행되어 루트 권한을 획득하게 된다.

① ㄱ → ㄴ → ㄷ → ㄹ
② ㄱ → ㄷ → ㄴ → ㄹ
③ ㄷ → ㄴ → ㄱ → ㄹ
④ ㄷ → ㄱ → ㄴ → ㄹ

문 8. 접근통제(access control) 모델에 대한 설명으로 옳지 않은 것은?
① 임의적 접근통제는 정보 소유자가 정보의 보안 레벨을 결정하고 이에 대한 정보의 접근제어를 설정하는 모델이다.
② 강제적 접근통제는 중앙에서 정보를 수집하고 분류하여, 각각의 보안 레벨을 붙이고 이에 대해 정책적으로 접근제어를 설정하는 모델이다.
③ 역할 기반 접근통제는 사용자가 아닌 역할이나 임무에 권한을 부여하기 때문에 사용자가 자주 변경되는 환경에서 유용한 모델이다.
④ Bell-LaPadula 접근통제는 비밀노출 방지보다는 데이터의 무결성 유지에 중점을 두고 있는 모델이다.

문 9. 개인정보 보호법령상 개인정보 영향평가에 대한 설명으로 옳지 않은 것은?
① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 위험요인분석과 개선 사항 도출을 위한 평가를 하고, 그 결과를 행정자치부장관에게 제출하여야 한다.
② 개인정보 영향평가의 대상에 해당하는 개인정보파일은 공공기관이 구축·운용 또는 변경하려는 개인정보파일로서 50만명 이상의 정보주체에 관한 개인정보파일을 말한다.
③ 영향평가를 하는 경우에는 처리하는 개인정보의 수, 개인정보의 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험정도, 그 밖에 대통령령으로 정한 사항을 고려하여야 한다.
④ 행정자치부장관은 제출받은 영향평가 결과에 대하여 보호위원회의 심의·의결을 거쳐 의견을 제시할 수 있다.

문 10. 정보보호 시스템에서 사용된 보안 알고리즘 구현 과정에서 곱셈에 대한 역원이 사용된다. 잉여류 Z_{26}에서 법(modular) 26에 대한 7의 곱셈의 역원으로 옳은 것은?
① 11 ② 13
③ 15 ④ 17

문 11. 응용 계층 프로토콜에서 동작하는 서비스에 대한 설명으로 옳지 않은 것은?

① FTP : 파일전송 서비스를 제공한다.
② DNS : 도메인 이름과 IP 주소 간 변환 서비스를 제공한다.
③ POP3 : 메일 서버로 전송된 메일을 확인하는 서비스를 제공한다.
④ SNMP : 메일전송 서비스를 제공한다.

문 12. 「개인정보 보호법」상 용어 정의로 옳지 않은 것은?

① 개인정보 : 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)
② 정보주체 : 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인
③ 처리 : 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위
④ 개인정보파일 : 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

문 13. 다음 설명에 해당하는 OECD 개인정보보호 8원칙으로 옳은 것은?

> 개인정보는 이용 목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성이 확보되어야 한다.

① 이용 제한의 원칙(Use Limitation Principle)
② 정보 정확성의 원칙(Data Quality Principle)
③ 안전성 확보의 원칙(Security Safeguards Principle)
④ 목적 명시의 원칙(Purpose Specification Principle)

문 14. 현행 우리나라의 정보보호관리체계(ISMS) 인증에 대한 설명으로 옳지 않은 것은?

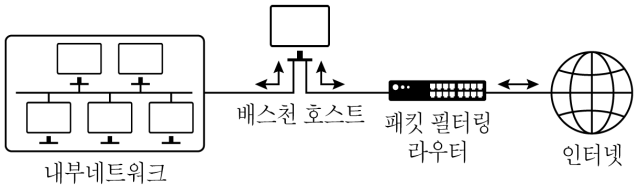
① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 근거를 두고 있다.
② 인증심사의 종류에는 최초심사, 사후심사, 갱신심사가 있다.
③ 인증에 유효기간은 정해져 있지 않다.
④ 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

문 15. 보안 서비스에 대한 설명을 바르게 나열한 것은?

> ㄱ. 메시지가 중간에서 복제·추가·수정되거나 순서가 바뀌거나 재전송됨이 없이 그대로 전송되는 것을 보장한다.
> ㄴ. 비인가된 접근으로부터 데이터를 보호하고 인가된 해당 개체에 적합한 접근 권한을 부여한다.
> ㄷ. 송·수신자 간에 전송된 메시지에 대해서, 송신자는 메시지 송신 사실을, 수신자는 메시지 수신 사실을 부인하지 못하도록 한다.

	ㄱ	ㄴ	ㄷ
①	데이터 무결성	부인봉쇄	인증
②	데이터 가용성	접근통제	인증
③	데이터 기밀성	인증	부인봉쇄
④	데이터 무결성	접근통제	부인봉쇄

문 16. 다음에 해당하는 방화벽의 구축 형태로 옳은 것은?



> ○ 인터넷에서 내부네트워크로 전송되는 패킷을 패킷 필터링 라우터에서 필터링함으로써 1차 방어를 수행한다.
> ○ 배스천 호스트에서는 필터링 된 패킷을 프록시와 같은 서비스를 통해 2차 방어 후 내부네트워크로 전달한다.

① 응용 레벨 게이트웨이(Application-level gateway)
② 회로 레벨 게이트웨이(Circuit-level gateway)
③ 듀얼 홈드 게이트웨이(Dual-homed gateway)
④ 스크린 호스트 게이트웨이(Screened host gateway)

문 17. SSH(Secure SHell)를 구성하고 있는 프로토콜 스택으로 옳지 않은 것은?

① SSH User Authentication Protocol
② SSH Session Layer Protocol
③ SSH Connection Protocol
④ SSH Transport Layer Protocol

문 18. 위험분석 방법에 대한 설명을 바르게 나열한 것은?

> ㄱ. 시스템에 관한 전문적인 지식을 가진 전문가 집단을 구성하고 토론을 통해 정보시스템이 직면한 다양한 위협과 취약성을 분석하는 방법이다.
> ㄴ. 자산의 가치 분석, 위협 분석, 취약점 분석을 수행하여 위험을 분석하는 방법이다.
> ㄷ. 표준화된 보호대책의 세트를 체크리스트 형태로 구현하여 이를 기반으로 보호대책을 식별하는 방법이다.

	ㄱ	ㄴ	ㄷ
①	시나리오법	기준선 접근법	상세 위험 분석 접근법
②	시나리오법	상세 위험 분석 접근법	기준선 접근법
③	델파이법	기준선 접근법	상세 위험 분석 접근법
④	델파이법	상세 위험 분석 접근법	기준선 접근법

문 19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 취급방침에 포함되어야 할 사항이 아닌 것은?

① 이용자 및 법정대리인의 권리와 그 행사 방법
② 개인정보에 대한 내부 관리 계획
③ 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
④ 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집 방법

문 20. 전자서명 방식에 대한 설명으로 옳지 않은 것은?

① 은닉 서명(blind signature)은 서명자가 특정 검증자를 지정하여 서명하고, 이 검증자만이 서명을 확인할 수 있는 방식이다.
② 부인방지 서명(undeniable signature)은 서명을 검증할 때 반드시 서명자의 도움이 있어야 검증이 가능한 방식이다.
③ 위임 서명(proxy signature)은 위임 서명자로 하여금 서명자를 대신해서 대리로 서명할 수 있도록 한 방식이다.
④ 다중 서명(multisignature)은 동일한 전자문서에 여러 사람이 서명하는 방식이다.