정보보호론

문 1. 보안 공격에 대한 설명으로 옳지 않은 것은?
① Land 공격 : UDP와 TCP 패킷의 순서번호를 조작하여 공격 시스템에 과부하가 발생한다.
② DDoS(Distributed Denial of Service) 공격 : 공격자, 마스터, 에이전트, 공격 대상으로 구성된 메커니즘을 통해 DoS 공격을 다수의 PC에서 대규모로 수행한다.
③ Trinoo 공격 : 1999년 미네소타대학교 사고의 주범이며 기본적으로 UDP 공격을 실시한다.
④ SYN Flooding 공격 : 각 서버의 동시 가용자 수를 SYN 패킷만 보내 점유하여 다른 사용자가 서버를 사용할 수 없게 만드는 공격이다.

문 2. 웹 브라우저와 웹 서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법은?
① PGP ② SSH
③ SSL ④ S/MIME

문 3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 정보통신서비스 제공자의 정보보호 최고책임자가 총괄하는 업무에 해당하지 않는 것은? (단, 이 법에 명시된 것으로 한정함)
① 정보보호관리체계 수립 및 관리·운영
② 주요정보통신기반시설의 지정
③ 정보보호 취약점 분석·평가 및 개선
④ 정보보호 사전 보안성 검토

문 4. 「개인정보 보호법」상 자신의 개인정보 처리와 관련한 정보주체의 권리에 대한 설명으로 옳지 않은 것은?
① 개인정보의 처리에 관한 정보를 제공받을 수 있다.
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 수 있다.
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 수 있다.
④ 개인정보에 대하여 열람을 할 수 있으나, 사본의 발급은 요구할 수 없다.

문 5. 침해사고가 발생하였을 경우 조직 내의 모든 사람들이 신속하게 대처하여 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 단계는?
① 보안탐지 단계 ② 대응 단계
③ 사후검토 단계 ④ 조사와 분석 단계

문 6. 다음 설명에 해당하는 블루투스 공격 방법은?

> 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격 방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP (OBEX Push Profile) 기능을 사용하여 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

① 블루스나프(BlueSnarf) ② 블루프린팅(BluePrinting)
③ 블루버그(BlueBug) ④ 블루재킹(BlueJacking)

문 7. 데이터베이스 보안 요구사항 중 비기밀 데이터에서 기밀 데이터를 얻어내는 것을 방지하는 요구사항은?
① 암호화
② 추론 방지
③ 무결성 보장
④ 접근통제

문 8. 가상사설망의 터널링 기능을 제공하는 프로토콜에 대한 설명으로 옳은 것은?
① IPSec은 OSI 3계층에서 동작하는 터널링 기술이다.
② PPTP는 OSI 1계층에서 동작하는 터널링 기술이다.
③ L2F는 OSI 3계층에서 동작하는 터널링 기술이다.
④ L2TP는 OSI 1계층에서 동작하는 터널링 기술이다.

문 9. 미국의 NIST와 캐나다의 CSE가 공동으로 개발한 평가체계로 암호모듈의 안전성을 검증하는 것은?
① CMVP
② COBIT
③ CMM
④ ITIL

문 10. MS Windows 운영체제 및 Internet Explorer의 보안 기능에 대한 설명으로 옳은 것은?
① Windows 7의 각 파일과 폴더는 사용자에 따라 권한이 부여되는데, 파일과 폴더에 공통적으로 부여할 수 있는 사용 권한은 모든 권한·수정·읽기·쓰기의 총 4가지이며, 폴더에는 폴더 내용 보기라는 권한을 더 추가할 수 있다.
② BitLocker 기능은 디스크 볼륨 전체를 암호화하여 데이터를 안전하게 보호하는 기능으로 Windows XP부터 탑재되었다.
③ Internet Explorer 10의 인터넷 옵션에서 개인정보 수준을 '낮음'으로 설정하는 것은 모든 쿠키를 허용함을 의미한다.
④ Windows 7 운영체제의 고급 보안이 포함된 Windows 방화벽은 인바운드 규칙과 아웃바운드 규칙을 모두 설정할 수 있다.

문 11. 정보보호의 주요 목표 중 하나인 인증성(Authenticity)을 보장하는 사례를 설명한 것으로 옳은 것은?
① 대학에서 개별 학생들의 성적이나 주민등록번호 등 민감한 정보는 안전하게 보호되어야 한다. 따라서 이러한 정보는 인가된 사람에게만 공개되어야 한다.
② 병원에서 특정 환자의 질병 관련 기록을 해당 기록에 관한 접근 권한이 있는 의사가 이용하고자 할 때 그 정보가 정확하며 오류 및 변조가 없었음이 보장되어야 한다.
③ 네트워크를 통해 데이터를 전송할 때는 데이터를 송신한 측이 정당한 송신자가 아닌 경우 수신자가 이 사실을 확인할 수 있어야 한다.
④ 회사의 웹 사이트는 그 회사에 대한 정보를 얻고자 하는 허가받은 고객들이 안정적으로 접근할 수 있어야 한다.

문 12. 시스템 계정 관리에서 보안성이 가장 좋은 패스워드 구성은?
① flowerabc ② P1234567#
③ flower777 ④ Fl66ower$

문 13. 다음은 「정보통신기반 보호법」의 일부이다. 본 조의 규정 목적으로 옳은 것은?

> 제12조(주요정보통신기반시설 침해행위 등의 금지) 누구든지 다음 각호의 1에 해당하는 행위를 하여서는 아니된다.
> … 중략 …
> 2. 주요정보통신기반시설에 대하여 데이터를 파괴하거나 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터 바이러스·논리폭탄 등의 프로그램을 투입하는 행위
> 제28조(벌칙)
> ① 제12조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.
> ② 제1항의 미수범은 처벌한다.

① 명예훼손 방지
② 개인정보 보호 침해 방지
③ 인터넷 사기 방지
④ 웜 피해 방지

문 14. 다음 설명에 해당하는 것은?

> 기업이 개인정보 보호 활동을 체계적·지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로서, 한국인터넷진흥원(KISA)에서 시행 중인 인증제도

① TCSEC ② CC
③ PIMS ④ ITSEC

문 15. 보안 공격 중 적극적 보안 공격의 종류가 아닌 것은?
① 신분위장(masquerade) : 하나의 실체가 다른 실체로 행세를 한다.
② 재전송(replay) : 데이터를 획득하여 비인가된 효과를 얻기 위하여 재전송한다.
③ 메시지 내용 공개(release of message contents) : 전화통화, 전자우편 메시지, 전송 파일 등에 기밀 정보가 포함되어 있으므로 공격자가 전송 내용을 탐지하지 못하도록 예방해야 한다.
④ 서비스 거부(denial of service) : 통신 설비가 정상적으로 사용 및 관리되지 못하게 방해한다.

문 16. 피싱(Phishing)에 대한 설명으로 옳지 않은 것은?
① Private Data와 Fishing의 합성어로서 유명 기관을 사칭하거나 개인 정보 및 금융 정보를 불법적으로 수집하여 금전적인 이익을 노리는 사기 수법이다.
② Wi-Fi 무선 네트워크에서 위장 AP를 이용하여 중간에 사용자의 정보를 가로채 사용자인 것처럼 속이는 수법이다.
③ 일반적으로 이메일을 사용하여 이루어지는 수법이다.
④ 방문한 사이트를 진짜 사이트로 착각하게 하여 아이디와 패스워드 등의 개인정보를 노출하게 하는 수법이다.

문 17. 국내 기관에서 주도적으로 개발한 암호 알고리즘은?
① IDEA
② ARIA
③ AES
④ Skipjack

문 18. 공개키 기반 구조(PKI, Public Key Infrastructure)에 대한 설명으로 옳지 않은 것은?
① 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보 보호 방식이다.
② 인증서의 폐지 여부는 인증서폐지목록(CRL)과 온라인 인증서 상태 프로토콜(OCSP) 확인을 통해서 이루어진다.
③ 인증서는 등록기관(RA)에 의해 발행된다.
④ 인증서는 버전, 일련번호, 서명, 발급자, 유효기간 등의 데이터 구조를 포함하고 있다.

문 19. 소인수분해 문제의 어려움에 기초하여 큰 안전성을 가지는 전자서명 알고리즘은?
① RSA
② ElGamal
③ KCDSA
④ ECDSA

문 20. 디지털 포렌식의 기본 원칙에 대한 설명으로 옳지 않은 것은?
① 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐서 획득되어야 한다.
② 신속성의 원칙 : 컴퓨터 내부의 정보 획득은 신속하게 이루어져야 한다.
③ 연계보관성의 원칙 : 증거자료는 같은 환경에서 같은 결과가 나오도록 재현이 가능해야 한다.
④ 무결성의 원칙 : 획득된 정보는 위·변조되지 않았음을 입증할 수 있어야 한다.