정보보호론

문 1. 이미지 파일 또는 MP3 파일 등에 인지하지 못할 정도의 미세한 변화를 주어 정보를 숨기는 기술은?

① 스테가노그래피(Steganography)
② 워터마킹(Watermarking)
③ 핑거프린팅(Fingerprinting)
④ 암호(Cryptography)

문 2. 대표적인 공격 유형으로 방해(interrupt)와 가로채기(intercept), 위조(fabrication), 변조(modification) 공격이 있다. 이 중 가로채기 공격에서 송·수신되는 데이터를 보호하기 위한 정보보호 요소는?

① 기밀성(Confidentiality)
② 무결성(Integrity)
③ 인증(Authentication)
④ 부인방지(Non-Repudiation)

문 3. 다음은 공개키 암호 시스템을 이용하여 Alice가 Bob에게 암호문을 전달하고, 이를 복호화하는 과정에 대한 설명이다. ㉠ ~ ㉢에 들어갈 내용으로 옳은 것은?

ㄱ. Bob은 개인키와 공개키로 이루어진 한 쌍의 키를 생성한다.
ㄴ. Bob은 (㉠)를 Alice에게 전송한다.
ㄷ. Alice는 (㉡)를 사용하여 메시지를 암호화한다.
ㄹ. Alice는 생성된 암호문을 Bob에게 전송한다.
ㅁ. Bob은 (㉢)를 사용하여 암호문을 복호화한다.

	㉠	㉡	㉢
①	Bob의 공개키	Alice의 공개키	Alice의 개인키
②	Bob의 개인키	Bob의 공개키	Bob의 개인키
③	Bob의 개인키	Alice의 공개키	Alice의 개인키
④	Bob의 공개키	Bob의 공개키	Bob의 개인키

문 4. 해시 함수(Hash Function)의 특징에 대한 설명으로 옳지 않은 것은?

① 임의의 메시지를 입력받아, 고정된 길이의 해시 값으로 출력한다.
② 암호학적으로 안전한 해시 함수를 설계하기 위해서는 역상 저항성(preimage resistance) 및 충돌 저항성(collision resistance)의 기준을 충족해야 한다.
③ 일반적으로 데이터 암호화에 사용된다.
④ 종류에는 SHA-1, MD5, HAS-160 등이 있다.

문 5. RSA 암호화 알고리즘에 대한 설명으로 옳지 않은 것은?

① 비대칭키를 이용한 부인방지 기능을 포함한다.
② AES 암호화 알고리즘보다 수행 속도가 빠르다.
③ 키 분배 및 관리가 용이하다.
④ 전자서명 등 응용 범위가 매우 넓다.

문 6. 개인정보보호관리체계(PIMS)에 대한 설명으로 옳지 않은 것은?

① 내부 정보 유출을 방지하기 위해, 인증 과정에 외부 전문가는 포함되지 않는다.
② PIMS 인증 취득 기업이 사고 발생 시 과징금, 과태료가 경감된다.
③ 인증 심사 기준은 개인정보관리과정과 개인정보보호대책, 개인정보생명주기 등이 있다.
④ PIMS는 기업이 자율적으로 심사를 신청하는 자율 제도로 운영한다.

문 7. 영국, 독일, 네덜란드, 프랑스 등 유럽 국가에서 평가 제품의 상호 인정 및 정보보호 평가 기준의 상이함에서 오는 시간과 인력 낭비를 줄이기 위해 제정한 유럽형 보안 기준은?

① CC(Common Criteria)
② ITSEC(Information Technology Security Evaluation Criteria)
③ TCSEC(Trusted Computer System Evaluation Criteria)
④ ISO/IEC JTC 1

문 8. 보안 사고에 대한 설명으로 옳지 않은 것은?

① 파밍(pharming)은 신종 인터넷 사기 수법으로 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.
② 스파이웨어(spyware)는 사용자의 동의 없이 시스템에 설치되어, 금융 정보 및 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼내가는 악의적 프로그램을 말한다.
③ 피싱(phishing)은 금융기관 등의 웹 사이트에서 보낸 이메일(email)로 위장하여, 링크를 유도해 타인의 인증 번호나 신용카드 번호, 계좌 정보 등을 빼내는 공격 기법이다.
④ 스니핑(sniffing)은 백 도어(backdoor) 등의 프로그램을 사용하여, 원격에서 남의 패킷 정보를 도청하는 해킹 유형의 하나로 적극적 공격에 해당한다.

문 9. 공공 기관에서 「개인정보 보호법」에 의거하여 영상정보처리기기를 설치 및 운용하려고 할 때, 안내판에 기재해야 할 내용으로 옳지 않은 것은?

① 설치 장소
② 영상정보 저장 방식
③ 촬영 시간
④ 관리 책임자의 이름

문 10. 생일 역설(Birthday Paradox)에 대한 설명으로 옳지 않은 것은?

① 해시 함수(hash function)는 충돌 메시지 쌍을 찾아내는 데 사용된다.
② 특정 장소에서 23명 이상이 있으면, 그중에서 2명 이상의 사람이 생일이 같을 확률은 0.5보다 크다.
③ 블록 암호 알고리즘의 안전성을 분석하는 데 이용된다.
④ 0부터 N − 1까지의 균일 분포를 갖는 수 중에서 임의로 한 개의 수를 선택한다면, $(N)^{1/2}$번의 시도 후에 동일한 수가 반복해서 선택될 확률은 0.5를 넘는다는 이론과 부합한다.

문 11. 자산의 위협과 취약성을 분석하여, 보안 위험의 내용과 정도를 결정하는 과정은?
① 위험 분석
② 보안 관리
③ 위험 관리
④ 보안 분석

문 12. 정보보호관리체계(ISMS) 인증과 관련하여 정보보호 관리과정 수행 절차를 순서대로 올바르게 나열한 것은?

ㄱ. 관리체계 범위 설정	ㄴ. 위험 관리
ㄷ. 정보보호 정책 수립	ㄹ. 사후 관리
ㅁ. 구현	

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

문 13. 다음은 개인정보의 수집 이용에 대한 사항이다. 동의를 받아야 할 항목만을 모두 고른 것은?

ㄱ. 개인정보의 수집·이용 목적
ㄴ. 수집하는 개인정보의 항목
ㄷ. 개인정보의 보유 및 이용 기간
ㄹ. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

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

문 14. 패스워드(Password)에 사용될 수 있는 문자열의 범위를 정하고, 그 범위 내에서 생성 가능한 패스워드를 활용하는 공격은?
① 레인보 테이블(Rainbow Table)을 이용한 공격
② 사전 공격(Dictionary Attack)
③ 무작위 대입 공격(Brute-Force Attack)
④ 차분 공격(Differential Attack)

문 15. 다음의 공격 유형과 그 대응 조치를 올바르게 연결한 것은?

<공격 유형>
1. Sendmail Daemon에 대해 알려진 패턴의 원격 버퍼 오버플로(Buffer Overflow) 공격
2. 계정 도용(Account Theft)
3. 해커가 임의로 파일을 삭제
4. XSS(Cross Site Scripting)

<대응 조치>
ㄱ. WAF(Web Application Firewall)
ㄴ. OTP(One Time Password)
ㄷ. IPS(Intrusion Prevention System)
ㄹ. 디스크 포렌식(Disk Forensics)에 의한 자료 복원

① 1－ㄱ, 2－ㄴ, 3－ㄹ, 4－ㄷ
② 1－ㄷ, 2－ㄴ, 3－ㄹ, 4－ㄱ
③ 1－ㄴ, 2－ㄱ, 3－ㄹ, 4－ㄷ
④ 1－ㄷ, 2－ㄱ, 3－ㄴ, 4－ㄹ

문 16. 다음 설명에 해당하는 접근제어 정책은?

한 개체(entity)가 자신의 의지로 다른 개체의 자원에 접근할 수 있는 권한을 승인받을 수 있다.

① MAC(Mandatory Access Control)
② DAC(Discretionary Access Control)
③ ACL(Access Control List)
④ RBAC(Role Based Access Control)

문 17. 침입 탐지 시스템(Intrusion Detection System)에 대한 설명으로 옳지 않은 것은?
① 호스트 기반과 네트워크 기반으로 나눌 수 있다.
② 침입 탐지 기법은 크게 오용 탐지(misuse detection) 기법과 이상 탐지(anomaly detection) 기법으로 나눌 수 있다.
③ 데이터의 효과적인 필터링(filtering)과 축약(reduction)을 수행해야 한다.
④ 오용 탐지 기법에는 정량적인 분석과 통계적인 분석 등이 포함된다.

문 18. 다음 설명에 해당하는 것은?

○ 송신자 측에서는 전송할 이메일(email)에 대한 전자서명 생성에 사용되며, 수신자 측에서는 이메일에 포함된 전자서명의 확인 작업에 사용된다.
○ 비대칭 암호 기술을 사용한다.
○ 이메일 어플리케이션에 플러그인(plug-in) 방식으로 확장이 가능하다.
○ 최초 개발자는 '필 짐머만(Phil Zimmermann)'이다.

① PGP(Pretty Good Privacy)
② PKI(Public-Key Infrastructure)
③ MIME(Multipurpose Internet Mail Extensions)
④ IKE(Internet Key Exchange)

문 19. 네트워크 스캐닝 기법 중 TCP 패킷에 FIN, PSH, URG 플래그를 설정해서 패킷을 전송하는 것은?
① TCP SYN 스캐닝
② UDP 스캐닝
③ NULL 스캐닝
④ X-MAS tree 스캐닝

문 20. 서비스 거부 공격(DoS: Denial of Service)에 대한 설명으로 옳지 않은 것은?
① Smurf 공격은 공격 대상의 IP 주소를 근원지로 대량의 ICMP 응답 패킷을 전송하여, 서비스 거부를 유발시키는 공격이다.
② Syn Flooding 공격은 TCP 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약성을 이용한 공격이다.
③ Land 공격은 출발지와 목적지의 IP 주소를 상이하게 설정하여, IP 프로토콜 스택에 장애를 유발하는 공격이다.
④ Ping of Death 공격은 비정상적인 ICMP 패킷을 전송하여, 시스템의 성능을 저하시키는 공격이다.