정보보호론

문 1. 주민등록번호의 유출에 따른 피해를 막기 위하여 도입된 주민등록번호 대체수단(i-PIN)에 대한 설명으로 옳은 것은?
① 주민등록번호를 저장하지 않으므로 성인 인증에는 사용되지 못한다.
② 주민등록번호를 대신하여 본인임을 확인받을 수 있는 사이버 신원확인 정보체계이나 법률적인 근거는 마련되어 있지 않다.
③ i-PIN의 안전한 통합관리를 위하여 한국인터넷진흥원을 유일한 본인확인기관으로 운영한다.
④ 주민등록번호와 달리 i-PIN은 유출되어도 해지 및 신규 발급이 가능하여 피해를 줄일 수 있다.

문 2. 보안 공격에 대한 설명으로 옳지 않은 것은?
① 소극적 공격은 시스템의 정보를 알아내거나 악용하지만, 시스템 자원에 영향을 주지 않는다.
② 적극적 공격은 실제로 데이터를 변경하지 않기 때문에 탐지하기 매우 어렵다.
③ 소극적 공격의 유형에는 메시지 내용 공개, 트래픽 분석이 있다.
④ 적극적 공격의 유형에는 신분위장, 서비스 거부, 재전송이 있다.

문 3. 침입사고를 보고받고 상황 분석 및 상황에 대응하는 업무를 수행하는 팀은?
① CIDT(Computer Intrusion Detection Team)
② CSET(Computer Social Engineering Team)
③ CIPT(Computer Intrusion Prevention Team)
④ CERT(Computer Emergency Response Team)

문 4. 다음 ㉠ ~ ㉢에 들어갈 말을 바르게 나열한 것은?

> ○ 독립적으로 자기 복제를 실행하여 번식하는 빠른 전파력을 가진 컴퓨터 프로그램 또는 실행 가능한 코드는 (㉠)이다.
> ○ 스마트폰에 악성코드로 연결되는 주소가 포함된 메시지를 전송하여 악성코드를 유도하는 공격을 (㉡)이라 한다.
> ○ (㉢)은 인터넷 프로토콜 계층에서 동작하며, 모든 트래픽을 암호화하고 인증기능을 제공한다.

	㉠	㉡	㉢
①	바이러스(virus)	파밍(pharming)	SSL
②	파밍(pharming)	스미싱(smishing)	SSL
③	웜(worm)	파밍(pharming)	IPSec
④	웜(worm)	스미싱(smishing)	IPSec

문 5. 정보보호에 대한 위협요소, 위협을 막기 위한 보안서비스, 보안서비스 구현을 위한 암호학적인 메카니즘에 대한 각각의 연결로 옳지 않은 것은?
① 도청－기밀성－암호화
② 서비스거부－부인방지－접근제어
③ 변조－무결성－해시함수
④ 위조－인증－전자서명

문 6. 암·복호화할 때 동일한 키를 사용하는 암호화 알고리즘은?
① RSA ② KCDSA
③ SEED ④ ECC

문 7. SSL을 구성하는 프로토콜 중에서 상위계층에서 수신된 메시지를 전달하는 역할을 담당하며 클라이언트와 서버 간 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증 코드 생성 및 암호화 과정 등을 수행하는 프로토콜은?
① Handshake Protocol
② Alert Protocol
③ Record Protocol
④ Change Cipher Spec Protocol

문 8. 다음에서 설명하는 침입차단시스템(Firewall)의 유형은?

> ○ 종단－대－종단 TCP 연결을 허용하지 않는다.
> ○ 두 개(자신과 내부 호스트 사용자 간, 자신과 외부 호스트 TCP 사용자 간)의 TCP 연결을 설정한다.
> ○ 시스템 관리자가 내부 사용자를 신뢰할 경우 일반적으로 사용한다.
> ○ 이와 같은 유형의 구현 예로는 SOCKS가 있다.

① 회로 레벨 프록시(circuit-level proxy) 침입차단시스템
② 스테이트풀 패킷 검사(stateful packet inspection) 침입차단시스템
③ 응용 프록시(application proxy gateway) 침입차단시스템
④ 패킷 필터링(packet filtering) 침입차단시스템

문 9. 「개인정보의 안전성 확보조치 기준」상 개인정보처리시스템의 개인정보취급 및 처리자에 대한 접근권한 부여 내역과 기록 보관에 대한 기준으로 옳지 않은 것은?
① 개인정보처리자는 개인정보취급자가 개인정보시스템에 접속한 기록을 6개월 이상 보관·관리하여야 한다.
② 개인정보처리자는 개인정보취급자의 개인정보시스템에 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 1년간 보관하여야 한다.
③ 개인정보처리자는 개인정보의 유출, 변조, 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.
④ 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

문 10. <보기 1>의 ㄱ ~ ㄹ의 암호 공격 방식과 <보기 2>의 ⓐ ~ ⓓ에 대한 설명으로 옳지 않은 것은?

<보기 1>

> ㄱ. 암호문 단독 공격(Ciphertext Only Attack)
> ㄴ. 기지 평문 공격(Known Plaintext Attack)
> ㄷ. 선택 평문 공격(Chosen Plaintext Attack)
> ㄹ. 선택 암호문 공격(Chosen Ciphertext Attack)

<보기 2>

> ⓐ 암호문만을 가지고 평문이나 키를 찾아내는 방법으로 평문의 특성 등을 추정하여 해독하는 방법
> ⓑ 약간의 평문에 대응하는 암호문을 알고 있는 상태에서 암호문과 평문의 관계로부터 키나 평문을 추정하여 암호를 해독하는 방법
> ⓒ 해독자가 암호기에 접근할 수 있어, 평문을 선택하여 그 평문에 해당하는 암호문을 얻어 키나 평문을 추정하여 암호를 해독하는 방법
> ⓓ 해독자가 암호 복호기에 접근할 수 있어, 일부 평문에 대한 암호문을 얻어 암호를 해독하는 방법

① ㄱ－ⓐ ② ㄴ－ⓑ
③ ㄷ－ⓒ ④ ㄹ－ⓓ

문 11. 다음에서 설명하는 정보보호의 보안 서비스로 옳은 것은?

> 기관 내부의 중요 데이터를 외부로 전송하는 행위가 탐지된 경우 전송자가 전송하지 않았음을 주장하지 못하도록 확실한 증거를 제시할 수 있는 보안 서비스이다.

① 무결성
② 접근제어
③ 기밀성
④ 부인방지

문 12. 「개인정보 보호법」 제33조에 따라 개인정보 영향평가를 하는 경우에 고려하여야 할 사항에 해당하지 않는 것은?

① 처리하는 개인정보의 수
② 개인정보의 제3자 제공 여부
③ 개인정보 보호 계획의 수립 및 시행 여부
④ 정보주체의 권리를 해할 가능성 및 그 위험 정도

문 13. 다음에서 설명하는 보안시스템은?

> ○ 패킷을 버리거나 또는 의심이 가는 트래픽을 감지함으로써 공격 트래픽을 방어하는 기능을 갖고 있다.
> ○ 모든 트래픽을 수신하는 스위치의 포트들을 모니터하고 특정 트래픽을 막기 위해 적합한 명령어를 라우터(Router)나 침입차단시스템(Firewall)에 보낼 수 있다.
> ○ 호스트(Host) 기반의 이 보안시스템은 공격을 감지하기 위해 서명이나 비정상 감지기술을 사용한다.

① IDS(Intrusion Detection System)
② IPS(Intrusion Prevention System)
③ DNS(Domain Name System)
④ VPN(Virtual Private Network)

문 14. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자 등이 개인정보를 취급할 때 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령이 정하는 기준에 따라 기술적·관리적 조치로 옳지 않은 것은?

① 개인정보를 안전하게 취급하기 위한 내부관리 계획의 수립·시행
② 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
③ 접속기록의 위조·변조 방지를 위한 조치
④ 법률에 근거하여 파기한 개인정보를 안전하게 복구하기 위한 조치

문 15. 블록 암호 알고리즘의 운영 모드로 옳지 않은 것은?

① ECB(Electronic Codebook)
② CBC(Cipher Block Chaining)
③ CFB(Cipher Feedback)
④ ECC(Error Correction Code)

문 16. 다음 내용에 해당하는 접근제어 모델을 바르게 나열한 것은?

> ㄱ. 권한을 직접 사용자에게 부여하는 대신 역할에 권한을 부여하고, 사용자들에게 적절한 역할을 할당하는 접근제어 모델.
> ㄴ. 한 사람이 모든 권한을 가지는 것을 방지하는 것으로서 정보의 입력·처리·확인 등을 여러 사람이 나누어 각 부분별로 관리하도록 하여 자료의 무결성을 보장하는 접근제어 모델.
> ㄷ. 군대의 보안등급처럼 그 정보의 기밀성에 따라 상하 관계가 구분된 정보를 보호하기 위한 접근제어 모델.

	ㄱ	ㄴ	ㄷ
①	역할기반 접근제어 모델	클락 윌슨 모델	벨-라파듈라 모델
②	임의적 접근제어 모델	클락 윌슨 모델	비바 모델
③	역할기반 접근제어 모델	만리장성 모델	비바 모델
④	임의적 접근제어 모델	만리장성 모델	벨-라파듈라 모델

문 17. 기존에 알려진 취약성에 대한 공격 패턴 정보를 미리 입력해 두었다가 이에 해당하는 패턴을 탐지하는 기법의 시스템은?

① 이상 탐지 기반의 침입탐지시스템
② 오용 탐지 기반의 침입탐지시스템
③ 비특성 통계 분석 기반의 침입탐지시스템
④ 허니팟 기반의 침입탐지시스템

문 18. 다음 공개키 기반 구조(PKI)에 대한 설명으로 옳은 것만을 모두 고른 것은?

> ㄱ. 사용자는 인증서를 발급받기 위하여 모든 인증기관의 승인을 얻어야 한다.
> ㄴ. 누구나 다른 사용자 및 인증기관의 공개키를 열람할 수 있다.
> ㄷ. 인증기관은 인증서에 대한 생성뿐만 아니라 갱신과 폐기도 가능하다.
> ㄹ. 인증서 폐기목록은 보안상 인증기관 및 등록기관에서만 접근 가능하다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

문 19. 허니팟(Honeypot)에 대한 설명으로 옳지 않은 것은?

① 공격자를 유인하기 위한 시스템이므로 쉽게 노출되지 않는 곳에 두어야 한다.
② 공격자를 중요한 시스템에 접근하지 못하게 유인한다.
③ 공격자의 행동패턴에 관한 정보를 수집한다.
④ 공격자가 가능한 오랫동안 허니팟에 머물도록 하고 그 사이에 관리자는 필요한 대응을 준비한다.

문 20. 해킹기법과 그 대응책에 대한 설명으로 옳지 않은 것은?

① Buffer Overflow 공격 : 프로그래밍 시 경곗값 검사를 적용하고 최신 운영체제로 패치
② Format String Bug 공격 : 데이터 형태(포맷 스트링)에 대한 명확한 정의
③ Denial of Service 공격 : MAC 주솟값을 고정으로 설정
④ SYN Flooding 공격 : SYN Received의 대기시간을 축소