정보보호론

문 1. 컴퓨터 시스템 및 네트워크 자산에 대한 위협 중에서 기밀성 침해에 해당하는 것은?
① 장비가 불능 상태가 되어 서비스가 제공되지 않음
② 통계적 방법으로 데이터 내용이 분석됨
③ 새로운 파일이 허위로 만들어짐
④ 메시지가 재정렬됨

문 2. 공개키기반구조(PKI)에서 관리나 보안상의 문제로 폐기된 인증서들의 목록은?
① Online Certificate Status Protocol
② Secure Socket Layer
③ Certificate Revocation List
④ Certification Authority

문 3. AES 알고리즘의 블록크기와 키길이에 대한 설명으로 옳은 것은?
① 블록크기는 64비트이고 키길이는 56비트이다.
② 블록크기는 128비트이고 키길이는 56비트이다.
③ 블록크기는 64비트이고 키길이는 128/192/256비트이다.
④ 블록크기는 128비트이고 키길이는 128/192/256비트이다.

문 4. 우리나라 국가 표준으로 지정되었으며 경량 환경 및 하드웨어 구현에서의 효율성 향상을 위해 개발된 128비트 블록암호 알고리즘은?
① IDEA
② 3DES
③ HMAC
④ ARIA

문 5. '정보시스템과 네트워크의 보호를 위한 OECD 가이드라인' (2002)에서 제시한 원리(principle) 중 "참여자들은 정보시스템과 네트워크 보안의 필요성과 그 안전성을 향상하기 위하여 할 수 있는 사항을 알고 있어야 한다."에 해당하는 것은?
① 인식(Awareness)
② 책임(Responsibility)
③ 윤리(Ethics)
④ 재평가(Reassessment)

문 6. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신서비스 제공자등이 이용자 개인정보의 국외 이전을 위한 동의 절차에서 이용자에게 고지해야 할 사항에 해당하지 않는 것은?
① 이전되는 개인정보 항목
② 개인정보가 이전되는 국가, 이전일시 및 이전방법
③ 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간
④ 개인정보를 이전하는 자의 성명(법인인 경우는 명칭 및 정보관리책임자의 연락처)

문 7. IPSec에서 두 컴퓨터 간의 보안 연결 설정을 위해 사용되는 것은?
① Authentication Header
② Encapsulating Security Payload
③ Internet Key Exchange
④ Extensible Authentication Protocol

문 8. 다음 설명에 해당하는 것은?

> PC나 스마트폰을 해킹하여 특정 프로그램이나 기기 자체를 사용하지 못하도록 하는 악성코드로서 인터넷 사용자의 컴퓨터에 설치되어 내부 문서나 스프레드시트, 이미지 파일 등을 암호화하여 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구한다.

① Web Shell
② Ransomware
③ Honeypot
④ Stuxnet

문 9. 「개인정보 보호법 시행령」상 개인정보처리자가 하여야 하는 안전성 확보 조치에 해당하지 않는 것은?
① 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행
② 개인정보가 정보주체의 요구를 받아 삭제되더라도 이를 복구 또는 재생할 수 있는 내부 방안 마련
③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

문 10. 공개키 암호시스템에 대한 설명 중 ㉠~㉢에 들어갈 말로 옳게 짝지어진 것은?

> ○ (㉠)의 안전성은 유한체의 이산대수 계산의 어려움에 기반을 둔다.
> ○ (㉡)의 안전성은 타원곡선군의 이산대수 계산의 어려움에 기반을 둔다.
> ○ (㉢)의 안전성은 소인수분해의 어려움에 기반을 둔다.

	㉠	㉡	㉢
①	ElGamal 암호시스템	DSS	RSA 암호시스템
②	Knapsack 암호시스템	ECC	RSA 암호시스템
③	Knapsack 암호시스템	DSS	Rabin 암호시스템
④	ElGamal 암호시스템	ECC	Rabin 암호시스템

문 11. 가상사설망에서 사용되는 프로토콜이 아닌 것은?
① L2F
② PPTP
③ TFTP
④ L2TP

문 12. 메모리 영역에 비정상적인 데이터나 비트를 채워 시스템의 정상적인 동작을 방해하는 공격 방식은?

① Spoofing
② Buffer overflow
③ Sniffing
④ Scanning

문 13. 시스템과 관련한 보안기능 중 적절한 권한을 가진 사용자를 식별하기 위한 인증 관리로 옳은 것은?

① 세션 관리
② 로그 관리
③ 취약점 관리
④ 계정 관리

문 14. 무선랜을 보호하기 위한 기술이 아닌 것은?

① WiFi Protected Access Enterprise
② WiFi Rogue Access Points
③ WiFi Protected Access
④ Wired Equivalent Privacy

문 15. 다음 정보통신 관계 법률의 목적에 대한 설명으로 옳지 않은 것은?

① 「정보통신기반 보호법」은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운영하도록 하여 국가의 안전과 국민 생활의 안정을 보장하는 것을 목적으로 한다.
② 「전자서명법」은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다.
③ 「통신비밀보호법」은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.
④ 「정보통신산업 진흥법」은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

문 16. 위험분석 및 평가방법론 중 성격이 다른 것은?

① 확률 분포법
② 시나리오법
③ 순위결정법
④ 델파이법

문 17. 보안 침해 사고에 대한 설명으로 옳은 것은?

① 크라임웨어는 온라인상에서 해당 소프트웨어를 실행하는 사용자가 알지 못하게 불법적인 행동 및 동작을 하도록 만들어진 프로그램을 말한다.
② 스니핑은 적극적 공격으로 백도어 등의 프로그램을 사용하여 네트워크상의 남의 패킷 정보를 도청하는 해킹 유형의 하나이다.
③ 파밍은 정상적으로 사용자들이 접속하는 도메인 이름과 철자가 유사한 도메인 이름을 사용하여 위장 홈페이지를 만든 뒤 사용자로 하여금 위장된 사이트로 접속하도록 한 후 개인정보를 빼내는 공격 기법이다.
④ 피싱은 해당 사이트가 공식적으로 운영하고 있던 도메인 자체를 탈취하는 공격 기법이다.

문 18. 다음 설명에 해당하는 것은?

> ○ 응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다.
> ○ 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한 구역을 가리킨다.

① Whitebox
② Sandbox
③ Middlebox
④ Bluebox

문 19. 각 주체가 각 객체에 접근할 때마다 관리자에 의해 사전에 규정된 규칙과 비교하여 그 규칙을 만족하는 주체에게만 접근 권한을 부여하는 기법은?

① Mandatory Access Control
② Discretionary Access Control
③ Role Based Access Control
④ Reference Monitor

문 20. 임의로 발생시킨 데이터를 프로그램의 입력으로 사용하여 소프트웨어의 안전성 및 취약성 등을 검사하는 방법은?

① Reverse Engineering
② Canonicalization
③ Fuzzing
④ Software Prototyping