정보시스템보안

1. OECD(경제협력개발기구) 개인정보보안 8원칙 중 정보 정확성 원칙의 구성 요소가 아닌 것은?
   ① 정확성
   ② 책임성
   ③ 완전성
   ④ 최신성

2. 정보보호에 대한 설명과 용어가 바르게 짝지어진 것은?

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자신의 잠재적인 속성으로 위협의 이용 대상이 되는 것
ㄹ. 정보자산에 피해를 주는 주체

	ㄱ	ㄴ	ㄷ	ㄹ
①	위협	취약점	위험	위협원
②	위협	위험	취약점	자산
③	취약점	위험	위협	노출
④	위협	위험	취약점	위협원

3. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳지 않는 것은?
   ① 커버로스는 시스템을 통해 패스워드를 평문 형태로 전송한다.
   ② 커버로스는 네트워크 응용 프로그램이 상대방의 신분을 식별할 수 있게 한다.
   ③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션을 통신한다.
   ④ Needham-Schroeder 프로토콜을 기반으로 만들어졌다.

4. UNIX 시스템에서 각 사용자가 로그인할 때마다 시스템에 의해 자동으로 실행되어야 하는 내용(PATH 변수, 프롬프트 지정 등)을 정의해 놓은 파일은?
   ① /etc/inittab
   ② /etc/inetd.conf
   ③ /etc/profile
   ④ /etc/rc.local

5. 다음 중 SSL 프로토콜에 대한 설명으로 옳지 않은 것은?
   ① SSL이 적용되었다는 표시로 HTTPS라고 사용한다.
   ② 보안성과 무결성을 유지하기 위해 마지막에는 HMAC을 붙인다.
   ③ SSL/TLS를 시작하기 위한 최초의 교신은 암호화와 MAC 없이 시작한다.
   ④ 110번 포트를 주로 사용한다.

6. 다음 서버 보안용 취약점 점검 도구에 대한 설명으로 가장 올바르지 못한 것은?
   ① nmap - 실시간 트래픽 분석과 패킷 로깅이 가능하다.
   ② SATAN - 네트워크를 통해 리모트 시스템의 보안정도를 조사하고 그 자료를 데이터베이스에 저장한다.
   ③ Nessus - 유닉스 플랫폼에서 동작하며 클라이언트-서버 구조로 클라이언트의 취약점을 점검한다.
   ④ SAINT - 유닉스 플랫폼에서 동작하는 네트워크 취약점을 분석한다.

7. 다음은 정보보호의 목표와 개념에 관한 설명으로 가장 거리가 먼 것은?
   ① 정보보호는 정보처리 영역에 있어서 가용성, 기밀성, 무결성을 보장하는 데 있다.
   ② 가용성이란 승인 또는 허가받은 사람의 경우 언제든지 접근과 이용을 보장 받는 것이다.
   ③ 최근에는 정보보호영역에서 부인방지, 책임성, 진정성, 신뢰성의 중요성이 날로 커지고 있다.
   ④ 기밀성이란 승인 또는 허가 받지 아니한 사람이나 프로세스에 의한 데이터의 변경 또는 훼손을 방지하는 것이다.

8. 다음 보기의 암호 알고리즘 중 키의 길이와 라운드 수가 가장 적은 것을 고르시오?

보기) DES IDEA Rijndael SEED

   ① 키의 길이 : DES, 라운드 수 : Rijndael
   ② 키의 길이 : IDEA, 라운드 수 : DES
   ③ 키의 길이 : DES, 라운드 수 : SEED
   ④ 키의 길이 : DES, 라운드 수 : IDEA

9. 다음 중 디바이스 인증기술의 장점이 아닌 것은?
① 책임추적성
② 상호 연동성
③ 보안성
④ 경제성

10. 다음 중 윈도우 운영체제의 IIS FTP 서버 설정에서 지정할 사항으로 가장 부적절한 것은?
① 운영 포트 변경 및 연결 시간의 제한
② Active/Passive 모드 지원여부
③ 보안계정 사용 및 익명 연결 허용 여부
④ 가상 디렉터리의 사용

11. 다음 중 위험관리에 관련된 용어와 그 의미의 연결이 가장 거리가 먼 것은?
① 잔여위험 – 위험처리를 수행하기 이전에 잔여하는 위험
② 위험수준 – 결과와 가능성의 조합으로 표현되는 위험의 크기
③ 통 제 – 위험을 변경시키기 위한 대책
④ 위험분석 – 위험의 본질을 이해하고 위험수준을 결정하는 과정

12. 다음 중 NTFS 파일 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 이론적인 최대 NTFS 파일 크기는 16EB이다.
② 기본 NTFS 보안을 변경하면 사용자마다 각기 다른 NTFS 보안을 설정할 수 없다.
③ NTFS 구조는 크게 VBR 영역, MTF 영역, Data 영역으로 나눈다.
④ 실제 최대 NTFS 파일 크기는 16TB이다.

13. AES 알고리즘의 블록 크기와 키 길이에 대한 설명으로 가장 올바른 것은?
① 블록 크기는 128/192/256비트이고, 키 길이는 64비트이다.
② 블록 크기는 128비트이고, 키 길이는 56비트이다.
③ 블록 크기는 64비트이고, 키 길이는 128/192/256비트이다.
④ 블록 크기는 128비트이고, 키 길이는 128/192/256비트이다.

14. <보기 1>의 상황과 개인정보의 안전한 전달을 위해 제공되어야 할 <보기 2>의 정보보호서비스를 가장 바르게 연결한 것은?

<보기 1>

ㄱ. 甲은 송신하는 개인정보를 도청당하는 일이 없이 乙에게 전달하기 원한다.
ㄴ. 甲은 송신하는 개인정보가 조작당하는 일이 없이 乙에게 전달되기 원한다.
ㄷ. 甲은 통신 상대의 웹 서버가 乙의 진짜 서버라는 것을 확인하고 싶다.
ㄹ. 甲은 乙의 서버에 적절한 시간에 접속하여 정상적으로 요청된 내용을 수행하고 싶다.

<보기 2>

A. 무결성
B. 인증
C. 기밀성
D. 가용성

	ㄱ	ㄴ	ㄷ	ㄹ
①	B	A	C	D
②	A	D	C	B
③	C	A	B	D
④	B	A	D	C

15. 보기에서 설명하는 특징을 가진 보안 모델은?

ㄱ. 무결성 중심의 상업적 모델로 비인가자의 수정과 인가자의 부적절한 수정을 방지한다.
ㄴ. 정보의 특성에 따라 비밀 노출 방지보다 자료의 변조 방지가 더 중요할 때 적합하며 직무분리를 반영하였고, 접속에 대한 로그를 남긴다.
ㄷ. 군사적 보안 요구사항과 상용보안 요구사항 간의 차이점을 강조한다.
ㄹ. 무결성을 집행하기 위한 일반적인 메커니즘

① Clark – Wilson 모델
② Biba 모델
③ HRU(Harrison – Ruzzo – Ullman) 모델
④ BLP(Bell & La Padula) 모델

16. 기존에 알려진 침입 방법에 기초한 오용 침입탐지(Misuse Detection)의 특징이 아닌 것은?
① 알려진 공격법이나 보안정책을 위반하는 행위에 대한 패턴을 지식데이터베이스로부터 찾아서 특정 공격들과 시스템 취약점에 기초한 계산된 지식을 적용하여 탐지해 내는 방법으로 지식기반(Knowledge-Base)탐지라고도 한다.
② 비교적 탐지의 정확도가 높으나 알려진 공격에 대한 정보수집이 어려우며 새로운 취약성에 대한 최신 정보를 유지하기 어렵다.
③ 정상적인 혹은 유효한 행동 모델은 다양한 방법으로 수집된 참조 정보들로부터 생성되며 현재 활동과 행동 모델을 비교하여 탐지한다.
④ 오용 침입탐지 종류로는 전문가시스템(Expert System), 시그니처 분석(Signature Analysis), 상태전이분석(State Transition Analysis)등이 있다.

17. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 상 정보통신 서비스 제공자는 임원급의 정보보호 최고책임자를 지정할 수 있도록 정하고 있다. 이 법에서 정하고 있는 정보통신서비스 제공자의 정보보호 최고 책임자가 총괄하는 업무에 해당하지 않는 것은?
① 정보보호 관리체계 수립 및 관리·운영
② 정보보호 취약점 분석·평가 및 개선
③ 주요 정보통신 기반시설의 지정
④ 정보보호 사전 보안성 검토

18. 다음 중 윈도우 로그 종류와 설명이 가장 바르게 짝지어진 것은?
① 계정 관리 감사 – 사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.
② 정책 변경 감사 – 권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
③ 개체 액세스 감사 – 특정 파일이나 디렉터리, 레지스트리 키 등과 같은 객체에 대한 접근을 시도하거나 속성 변경 등을 탐지한다.
④ 로그인 이벤트 감사 – 시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

19. 위험분석 및 평가방법론 중 성격이 가장 다른 것은?
① 확률분포법
② 순위결정법
③ 과거자료 분석법
④ 수학공식 접근법

20. 다음 중 IPSec(Internet Protocol Security)에 대한 설명으로 가장 올바르지 못한 것은?
① 네트워크 계층에서 보안성을 제공해주는 표준화된 기술로 송수신자에게 인증 및 암호화 서비스를 제공한다.
② SA(Security Association)는 보안성 있는 데이터를 교환하기 위해 암호화, 키 교환 등에 대한 합의 사항들을 담고 있다.
③ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.
④ 보안서비스를 위하여 AH(Authentication Header)와 ESP(Encapsulating Security Payload)의 두 프로토콜을 사용한다.