정보보호론

문 1. 다음에서 설명하는 공격방법은?

> 정보보안에서 사람의 심리적인 취약점을 악용하여 비밀정보를 취득하거나 컴퓨터 접근권한 등을 얻으려고 하는 공격방법이다.

① 스푸핑 공격
② 사회공학적 공격
③ 세션 가로채기 공격
④ 사전 공격

문 2. 능동적 보안 공격에 해당하는 것만을 모두 고른 것은?

> ㄱ. 도청 ㄴ. 감시
> ㄷ. 신분위장 ㄹ. 서비스 거부

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

문 3. 다음에서 설명하는 재해복구시스템의 복구 방식은?

> 재해복구센터에 주 센터와 동일한 수준의 시스템을 대기 상태로 두어, 동기적 또는 비동기적 방식으로 실시간 복제를 통하여 최신의 데이터 상태를 유지하고 있다가, 재해 시 재해복구센터의 시스템을 활성화 상태로 전환하여 복구하는 방식이다.

① 핫 사이트(Hot Site)
② 미러 사이트(Mirror Site)
③ 웜 사이트(Warm Site)
④ 콜드 사이트(Cold Site)

문 4. 정보보안의 기본 개념에 대한 설명으로 옳지 않은 것은?

① Kerckhoff의 원리에 따라 암호 알고리즘은 비공개로 할 필요가 없다.
② 보안의 세 가지 주요 목표에는 기밀성, 무결성, 가용성이 있다.
③ 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하지 않아도 된다.
④ 가용성은 인가된 사용자에게 서비스가 잘 제공되도록 보장하는 것이다.

문 5. 공개키 기반 구조(PKI : Public Key Infrastructure)의 인증서에 대한 설명으로 옳은 것만을 모두 고른 것은?

> ㄱ. 인증기관은 인증서 및 인증서 취소목록 등을 관리한다.
> ㄴ. 인증기관이 발행한 인증서는 공개키와 공개키의 소유자를 공식적으로 연결해 준다.
> ㄷ. 인증서에는 소유자 정보, 공개키, 개인키, 발행일, 유효기간 등의 정보가 담겨 있다.
> ㄹ. 공인인증서는 인증기관의 전자서명 없이 사용자의 전자서명만으로 공개키를 공증한다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

문 6. 위험 분석에 대한 설명으로 옳지 않은 것은?

① 자산의 식별된 위험을 처리하는 방안으로는 위험 수용, 위험 회피, 위험 전가 등이 있다.
② 자산의 가치 평가를 위해 자산구입비용, 자산유지보수비용 등을 고려할 수 있다.
③ 자산의 적절한 보호를 위해 소유자와 책임소재를 지정함으로써 자산의 책임추적성을 보장받을 수 있다.
④ 자산의 가치 평가 범위에 데이터베이스, 계약서, 시스템 유지보수 인력 등은 제외된다.

문 7. 메시지 인증 코드(MAC : Message Authentication Code)를 이용한 메시지 인증 방법에 대한 설명으로 옳지 않은 것은?

① 메시지의 출처를 확신할 수 있다.
② 메시지와 비밀키를 입력받아 메시지 인증 코드를 생성한다.
③ 메시지의 무결성을 증명할 수 있다.
④ 메시지의 복제 여부를 판별할 수 있다.

문 8. 유닉스(Unix)의 로그 파일과 기록되는 내용을 바르게 연결한 것은?

> ㄱ. history – 명령창에 실행했던 명령 내역
> ㄴ. sulog – su 명령어 사용 내역
> ㄷ. xferlog – 실패한 로그인 시도 내역
> ㄹ. loginlog – FTP 파일 전송 내역

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

문 9. 전송계층 보안 프로토콜인 TLS(Transport Layer Security)가 제공하는 보안 서비스에 해당하지 않는 것은?

① 메시지 부인 방지
② 클라이언트와 서버 간의 상호 인증
③ 메시지 무결성
④ 메시지 기밀성

문 10. 다음에서 설명하는 스니퍼 탐지 방법에 이용되는 것은?

> ○ 스니핑 공격을 하는 공격자의 주요 목적은 사용자 ID와 패스워드의 획득에 있다.
> ○ 보안 관리자는 이 점을 이용해 가짜 ID와 패스워드를 네트워크에 계속 보내고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지한다.

① ARP ② DNS
③ Decoy ④ ARP watch

문 11. 다음에 제시된 <보기 1>의 사용자 인증방법과 <보기 2>의 사용자 인증도구를 바르게 연결한 것은?

<보기 1>

> ㄱ. 지식 기반 인증 ㄴ. 소지 기반 인증 ㄷ. 생체 기반 인증

<보기 2>

> A. OTP 토큰 B. 패스워드 C. 홍채

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

문 12. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 용어의 정의에 대한 설명으로 옳지 않은 것은?

① 정보통신서비스 : 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것

② 정보통신망 : 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제

③ 통신과금서비스이용자 : 정보보호제품을 개발·생산 또는 유통하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람

④ 침해사고 : 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태

문 13. 안드로이드 보안에 대한 설명으로 옳지 않은 것은?

① 리눅스 운영체제와 유사한 보안 취약점을 갖는다.

② 개방형 운영체제로서의 보안정책을 적용한다.

③ 응용프로그램에 대한 서명은 개발자가 한다.

④ 응용프로그램 간 데이터 통신을 엄격하게 통제한다.

문 14. 개인정보 보호 인증(PIPL) 제도에 대한 설명으로 옳은 것은?

① 물리적 안전성 확보조치 심사영역에는 악성 소프트웨어 통제 심사항목이 있다.

② 인증절차는 인증심사 준비단계, 심사단계, 인증단계로 구성되며, 인증유지관리를 위한 유지관리 단계가 있다.

③ 개인정보 보호를 위해 관리계획 수립과 조직구축은 정보주체 권리보장 심사영역에 속한다.

④ 인증을 신청할 수 있는 기관은 공공기관에 한정한다.

문 15. 해킹에 대한 설명으로 옳지 않은 것은?

① SYN Flooding은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.

② Zero Day 공격은 시그니처(signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.

③ APT는 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.

④ Buffer Overflow는 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

문 16. 다음에서 설명하는 웹 서비스 공격은?

> 공격자가 사용자의 명령어나 질의어에 특정한 코드를 삽입하여 DB 인증을 우회하거나 데이터를 조작한다.

① 직접 객체 참조

② Cross Site Request Forgery

③ Cross Site Scripting

④ SQL Injection

문 17. 사용자와 인증 서버 간 대칭키 암호를 이용한 시도 – 응답(Challenge-Response) 인증방식에 대한 설명으로 옳지 않은 것은?

① 재전송 공격으로부터 안전하게 사용자를 인증하는 기법이다.

② 인증 서버는 사용자 인증을 위해 사용자의 비밀키를 가지고 있다.

③ 사용자 시간과 인증 서버의 시간이 반드시 동기화되어야 한다.

④ Response값은 사용자의 비밀키를 사용하여 인증 서버에서 전달받은 Challenge값을 암호화한 값이다.

문 18. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.

② 보호 프로파일(Protection Profiles)은 특정 제품이나 시스템에만 종속되어 적용하는 보안기능 수단과 보증수단을 기술한 문서이다.

③ 평가 보증 등급(EAL : Evaluation Assurance Level)에서 가장 엄격한 보증(formally verified) 등급은 EAL7이다.

④ 보안 요구조건을 명세화하고 평가기준을 정의하기 위한 ISO/IEC 15408 표준이다.

문 19. 「개인정보 보호법」상 주민등록번호 처리에 대한 설명으로 옳지 않은 것은?

① 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인인 개인정보처리자는 개인정보 보호위원회의 심의·의결을 거쳐 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.

② 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 유출된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 주민등록번호가 유출되지 아니하도록 개인정보처리자가 「개인정보 보호법」에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 개인정보처리자는 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

문 20. 다음에서 설명하는 윈도우 인증 구성요소는?

> ○ 사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다.
> ○ SID에 기반을 두어 파일이나 디렉터리에 대한 접근의 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)

② SRM(Security Reference Monitor)

③ SAM(Security Account Manager)

④ IPSec(IP Security)