정보보호론

문 1. 공격자가 자신이 전송하는 패킷에 다른 호스트의 IP 주소를 담아서 전송하는 공격은?

① 패킷 스니핑(Packet Sniffing)
② 스미싱(Smishing)
③ 버퍼 오버플로우(Buffer Overflow)
④ 스푸핑(Spoofing)

문 2. 정보보호의 주요 목적에 대한 설명으로 옳지 않은 것은?

① 기밀성(confidentiality)은 인가된 사용자만이 데이터에 접근할 수 있도록 제한하는 것을 말한다.
② 가용성(availability)은 필요할 때 데이터에 접근할 수 있는 능력을 말한다.
③ 무결성(integrity)은 식별, 인증 및 인가 과정을 성공적으로 수행했거나 수행 중일 때 발생하는 활동을 말한다.
④ 책임성(accountability)은 제재, 부인방지, 오류제한, 침입탐지 및 방지, 사후처리 등을 지원하는 것을 말한다.

문 3. 네트워크 각 계층별 보안 프로토콜로 옳지 않은 것은?

① 네트워크 계층(network layer) : IPSec
② 네트워크 계층(network layer) : FTP
③ 응용 프로그램 계층(application layer) : SSH
④ 응용 프로그램 계층(application layer) : S/MIME

문 4. 방화벽(firewall)에 대한 설명으로 옳지 않은 것은?

① 패킷 필터링 방화벽은 패킷의 출발지 및 목적지 IP 주소, 서비스의 포트 번호 등을 이용한 접속제어를 수행한다.
② 패킷 필터링 기법은 응용 계층(application layer)에서 동작하며, WWW와 같은 서비스를 보호한다.
③ NAT 기능을 이용하여 IP 주소 자원을 효율적으로 사용함과 동시에 보안성을 높일 수 있다.
④ 방화벽 하드웨어 및 소프트웨어 자체의 결함에 의해 보안상 취약점을 가질 수 있다.

문 5. 해시 함수(hash function)에 대한 설명으로 옳지 않은 것은?

① 임의 길이의 문자열을 고정된 길이의 문자열로 출력하는 함수이다.
② 대표적인 해시 함수는 MD5, SHA-1, HAS-160 등이 있다.
③ 해시 함수는 메시지 인증과 메시지 부인방지 서비스에 이용된다.
④ 해시 함수의 충돌 회피성은 동일한 출력을 산출하는 서로 다른 두 입력을 계산적으로 찾기 가능한 성질을 나타낸다.

문 6. 「정보통신기반 보호법」에 대한 설명으로 옳지 않은 것은?

① 주요정보통신기반시설을 관리하는 기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 한국인터넷진흥원에 그 사실을 통지하여야 한다.
② "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터 바이러스, 서비스 거부 또는 고출력 전자기파 등에 의한 공격행위를 말한다.
③ 관리기관의 장은 소관분야의 정보통신기반시설 중 전자적 침해행위로부터의 보호가 필요하다고 인정되는 시설을 주요정보통신기반시설로 지정할 수 있다.
④ 주요정보통신기반시설의 취약점 분석·평가 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

문 7. 「개인정보 보호법」상 공공기관에서의 영상정보처리기기 설치 및 운영에 대한 설명으로 옳지 않은 것은?

① 공공기관의 사무실에서 민원인의 폭언·폭행 방지를 위해 영상정보처리기기를 설치 및 녹음하는 것이 가능하다.
② 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 안 된다.
③ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다.
④ 「개인정보 보호법」에서 정하는 사유를 제외하고는 공개된 장소에 영상정보처리기기를 설치하는 것은 금지되어 있다.

문 8. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① 정보보호 측면에서 정보보호 기능이 있는 IT 제품의 안전성을 보증·평가하는 기준이다.
② 국제공통평가기준은 소개 및 일반모델, 보안기능요구사항, 보증요구사항 등으로 구성되고, 보증 등급은 5개이다.
③ 보안기능요구사항과 보증요구사항의 구조는 클래스로 구성된다.
④ 상호인정협정(CCRA : Common Criteria Recognition Arrangement)은 정보보호제품의 평가인증 결과를 가입 국가 간 상호 인정하는 협정으로서 미국, 영국, 프랑스 등을 중심으로 시작되었다.

문 9. 위험관리 요소에 대한 설명으로 옳지 않은 것은?

① 위험은 위협 정도, 취약성 정도, 자산 가치 등의 함수관계로 산정할 수 있다.
② 취약성은 자산의 약점(weakness) 또는 보호대책의 결핍으로 정의할 수 있다.
③ 위험 회피로 조직은 편리한 기능이나 유용한 기능 등을 상실할 수 있다.
④ 위험관리는 위협 식별, 취약점 식별, 자산 식별 등의 순서로 이루어진다.

문 10. 다음 설명에 해당하는 컴퓨터 바이러스는?

> 산업 소프트웨어와 공정 설비를 공격 목표로 하는 극도로 정교한 군사적 수준의 사이버 무기로 지칭된다. 공정 설비와 연결된 프로그램이 논리제어장치(Programmable Logic Controller)의 코드를 악의적으로 변경하여 제어권을 획득한다. 네트워크와 이동저장매체인 USB를 통해 전파되며, SCADA (Supervisory Control and Data Acquisition) 시스템이 공격 목표이다.

① 오토런 바이러스(Autorun virus)
② 백도어(Backdoor)
③ 스턱스넷(Stuxnet)
④ 봇넷(Botnet)

문 11. 서비스 거부(DoS : Denial of Service) 공격 또는 분산 서비스 거부(DDoS : Distributed DoS) 공격에 대한 설명으로 옳지 않은 것은?

① TCP SYN이 DoS 공격에 활용된다.
② CPU, 메모리 등 시스템 자원에 과다한 부하를 가중시킨다.
③ 불특정 형태의 에이전트 역할을 수행하는 데몬 프로그램을 변조하거나 파괴한다.
④ 네트워크 대역폭을 고갈시켜 접속을 차단시킨다.

문 12. 보안 프로토콜인 IPSec(IP Security)의 프로토콜 구조로 옳지 않은 것은?

① Change Cipher Spec
② Encapsulating Security Payload
③ Security Association
④ Authentication Header

문 13. DRM(Digital Right Management)에 대한 설명으로 옳지 않은 것은?

① 디지털 컨텐츠의 불법 복제와 유포를 막고, 저작권 보유자의 이익과 권리를 보호해 주는 기술과 서비스를 말한다.
② DRM은 파일을 저장할 때, 암호화를 사용한다.
③ DRM 탬퍼 방지(tamper resistance) 기술은 라이센스 생성 및 발급관리를 처리한다.
④ DRM은 온라인 음악서비스, 인터넷 동영상 서비스, 전자책, CD/DVD 등의 분야에서 불법 복제 방지 기술로 활용된다.

문 14. 다음 설명에 해당하는 접근제어 모델은?

> 조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다. 사용자가 적절한 직무에 할당되고, 직무에 적합한 접근 권한이 할당된 경우에만 접근할 수 있다.

① 강제적 접근제어(Mandatory Access Control)
② 규칙 기반 접근제어(Rule-Based Access Control)
③ 역할 기반 접근제어(Role-Based Access Control)
④ 임의적 접근제어(Discretionary Access Control)

문 15. 공개키 암호에 대한 설명으로 옳지 않은 것은?

① 공개키 인증서를 공개키 디렉토리에 저장하여 공개한다.
② 사용자가 증가할수록 필요한 비밀키의 개수가 증가하는 암호 방식의 단점을 해결할 수 있다.
③ 일반적으로 대칭키 암호방식보다 암호화 속도가 느리다.
④ n명의 사용자로 구성된 시스템에서는 $\frac{n(n-1)}{2}$개의 키가 요구된다.

문 16. 웹 서버 보안에 대한 설명으로 옳지 않은 것은?

① 웹 애플리케이션은 SQL 삽입공격에 안전하다.
② 악성 파일 업로드를 방지하기 위하여 필요한 파일 확장자만 업로드를 허용한다.
③ 웹 애플리케이션의 취약점을 방지하기 위하여 사용자의 입력 값을 검증한다.
④ 공격자에게 정보 노출을 막기 위하여 웹 사이트의 맞춤형 오류 페이지를 생성한다.

문 17. 「개인정보 보호법」상 개인정보 유출 시 개인정보처리자가 정보주체에게 알려야 할 사항으로 옳은 것만을 모두 고르면?

> ㄱ. 유출된 개인정보의 위탁기관 현황
> ㄴ. 유출된 시점과 그 경위
> ㄷ. 개인정보처리자의 개인정보 보관·폐기 기간
> ㄹ. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

① ㄱ, ㄴ
② ㄷ, ㄹ
③ ㄱ, ㄷ
④ ㄴ, ㄹ

문 18. PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① PGP는 전자우편용 보안 프로토콜이다.
② 공개키 암호 알고리즘을 사용하지 않고, 대칭키 암호화 알고리즘으로 메시지를 암호화한다.
③ PGP는 데이터를 압축해서 암호화한다.
④ 필 짐머만(Philip Zimmermann)이 개발하였다.

문 19. 컴퓨터 바이러스에 대한 설명으로 옳지 않은 것은?

① 트랩도어(Trapdoor)는 정상적인 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.
② 웜(Worm)은 네트워크 등의 연결을 통하여 자신의 복제품을 전파한다.
③ 트로이목마(Trojan Horse)는 정상적인 프로그램으로 가장한 악성프로그램이다.
④ 루트킷(Rootkit)은 감염된 시스템에서 활성화되어 다른 시스템을 공격하는 프로그램이다.

문 20. 「정보보호 관리체계 인증 등에 관한 고시」에 의거한 정보보호 관리체계(ISMS)에 대한 설명으로 옳지 않은 것은?

① 정보보호관리과정은 정보보호정책 수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현 등 4단계 활동을 말한다.
② 인증기관이 조직의 정보보호 활동을 객관적으로 심사하고, 인증한다.
③ 정보보호 관리체계는 조직의 정보 자산을 평가하는 것으로 물리적 보안을 포함한다.
④ 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위하여 관리적·기술적 수단과 절차 및 과정을 관리, 운용하는 체계이다.