【문 1】 대표적인 블록암호인 DES, Triple DES, AES에 관한 다음 설명 중 가장 옳지 않은 것은?

① DES는 Feistel 구조를 기반으로 설계되었으며, AES는 Substitution Permutation Network 구조를 기반으로 설계가 되었다.
② Triple DES는 DES의 암호화 과정을 각각 다른 암호화 키로 3회 수행하는데, 효율을 높이기 위해 첫 번째와 두 번째 암호화 키를 동일하게 사용하도록 권장하고 있다.
③ AES의 암호화 과정은 마지막 라운드를 제외한 모든 라운드가 동일한 함수로 설계되었다.
④ AES는 안전성의 정도에 따라 키의 길이가 128, 192, 256비트를 가질 수 있으며, 키의 길이에 따라 실행하는 라운드 수가 각각 10, 12, 14라운드로 다르다.

【문 2】 네트워크 서비스 거부 공격 기법에 관한 다음 설명 중 가장 옳지 않은 것은?

① Slowloris 공격은 HTTP 헤더 정보를 비정상적으로 조작하여 웹서버가 온전한 헤더 정보가 올 때까지 기다리게 하는 공격이다.
② Mail Bomb은 사용자에게 할당된 디스크 공간 이상의 메일을 보내어 더 이상 메일을 받을 수 없게 하는 공격이다.
③ Teardrop 공격은 UDP와 TCP 패킷의 시퀀스 넘버를 조작하여 공격 시스템에 과부하를 일으키는 공격이다.
④ Land 공격은 패킷 전송 출발지 IP 주소와 목적지 IP 주소의 값을 다르게 설정하여 공격 대상에게 패킷을 보내는 공격이다.

【문 3】 NAC(Network Access Control) 시스템에 관한 다음 설명 중 가장 옳지 않은 것은?

① 네트워크에 접근하는 접속 단말의 보안성을 검증하여 보안성을 강제화하고 접속을 통제할 수 있는 보안 인프라이다.
② 사용 단말이 내부 네트워크에 접근하기 전에 보안 정책을 준수했는지 여부를 검사해 네트워크 접속을 통제하는 보안 솔루션이다.
③ NAC은 접근제어, 인증, 무결성 체크, 유해 트래픽 탐지 및 차단 기능을 제공한다.
④ NAC의 접근 제어 및 인증 기능은 장치에 부여된 고유한 장치명을 기반으로 수행되며, 등록된 장치명만 네트워크에 접속할 수 있게 허용한다.

【문 4】 UTM(Unified Threat Management)과 ESM(Enterprise Security Management)에 관한 다음 설명 중 가장 옳지 않은 것은?

① UTM은 단일장비로 다양한 보안 기능을 하나의 장비로 통합하여 제공할 수 있다.
② UTM은 장애 발생 시 다른 보안 기능에 영향을 주지 않는다.
③ ESM은 기업과 기관의 보안 정책을 반영하고 다양한 보안 시스템을 관제, 운영, 관리함으로써 조직의 보안 목적을 효율적으로 실현하는 시스템이다.
④ ESM은 통합보안관제를 위해 구축된 다양한 보안 솔루션과 보안 장비에서 발생하는 로그와 보안 이벤트를 취합하고 이들 간에 상호 연관 분석을 함으로써 실시간 보안 위협을 파악하고 대응한다.

【문 5】 크로스사이트 스크립트 공격과정을 순서대로 바르게 나열한 것은?

ㄱ. 일반 사용자 PC의 보안 취약점이 외부에 전달된다.
ㄴ. 일반 사용자가 웹서버에 접속하여 웹서버에 저장된 악성코드를 내려받는다.
ㄷ. XSS 취약점이 있는 웹 서버에 악성코드를 업로드한다.
ㄹ. 공격자는 추가적인 보안 공격을 시작한다.
ㅁ. 일반 사용자의 PC에서 악성코드가 실행된다.

① ㄷ - ㄱ - ㄴ - ㅁ - ㄹ
② ㄷ - ㄴ - ㅁ - ㄱ - ㄹ
③ ㄷ - ㄴ - ㄱ - ㅁ - ㄹ
④ ㄷ - ㅁ - ㄱ - ㄴ - ㄹ

【문 6】 정보보호제품 평가·인증 제도에 관한 다음 설명 중 가장 옳지 않은 것은?

① 정보보호제품 평가 인증제도는 지능정보화 기본법 제58조(정보보호시스템에 관한 기준 고시 등)에 근거한다
② 공통평가기준(Common Criteria, CC)는 보증의 요구를 구조화하기 위해 가장 엄격한 보증 증거인 EAL 1부터 가장 엄격하지 않은 보증 증거인 EAL 7까지 7개의 평가 보증 수준으로 보증 등급을 정의하고 있다.
③ 보호 프로파일(PP)은 정보 제품이 갖추어야 할 공통적인 보안 요구사항을 모아 놓은 것이다.
④ IT보안인증사무국은 정보보호제품 평가·인증제도에 지정된 CC 인증기관이다.

【문 7】 윈도우 운영체제에서 사용하는 주요 그룹에 관한 다음 설명 중 가장 옳지 않은 것은?

① Administrators: 대표적인 관리자 그룹으로 윈도우 시스템의 모든 권한을 가지고 있으며, 사용 가능한 자원에 대한 권한을 설정할 수 있다.
② Power Users: 로컬 컴퓨터에서 Administrators 그룹이 가진 대부분의 권한을 가지며, 해당 컴퓨터 밖의 네트워크에서는 일반 사용자로 존재한다.
③ Users: 대부분의 사용자가 속하는 그룹으로, 네트워크를 통하여 서버나 다른 도메인 구성 요소에 로그인이 가능하다.
④ Guests: 윈도우 시스템에서 네트워크를 통하여 서버에 로그인할 수는 없으나, 서버로의 로컬 로그인은 가능하다.

【문 8】 네트워크 OSI(Open System Interconnection) 7계층에 관한 다음 설명 중 가장 적절한 것은?

① 데이터 링크 계층(Data Link Layer)은 실제 장치를 연결하기 위한 전기적·물리적 세부 사항을 정의한 계층이다.
② 네트워크 계층(Network Layer)은 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있게 해주는 계층이다.
③ 전송 계층(Transport Layer)은 여러 개의 노드를 거치는 경우 경로를 찾아주는 역할을 하는 계층이다.
④ 세션 계층(Session Layer)은 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공하는 계층이다.

【문 9】 다음은 보안 기능에 대한 설명이다. 가장 올바르게 짝지어진 것은?

ㄱ. 전송된 메시지가 변경 없이 전송되었는지 확인하는 보안 기능
ㄴ. 필요할 때 언제나 메시지를 보낼 수 있도록 보장하는 보안 기능
ㄷ. 전송되는 메시지가 외부에 유출되는 것을 방지하는 보안 기능

ㄱ	ㄴ	ㄷ
① 기밀성	가용성	무결성
② 가용성	무결성	기밀성
③ 무결성	기밀성	가용성
④ 무결성	가용성	기밀성

【문10】 다음 설명에 해당하는 이메일 암호화 방식은?

- 1991년 필립 짐머만에 의해 개발되었다.
- 사용자 간의 상호 인증을 통한 네트워크 구조를 통해 사용된다.
- 세션 키를 암호화하기 위하여 IDEA 알고리즘을 사용한다.
- 사용자 인증을 위한 서명으로 RSA 서명을 사용한다.

① S/MIME ② PGP ③ PEM ④ VPN

【문11】 암호학적 해시 함수에 관한 다음 설명 중 가장 옳지 않은 것은?

① 해시함수 h의 일방향성(One-wayness)은 임의의 값 y가 주어졌을 때, h(x)=y를 만족시키는 x값을 찾기 어려운 성질을 말한다.
② 해시함수 h의 충돌저항성(Collision resistance)은 h(x)=h(x′)을 만족하는 서로 다른 값 x, x′을 찾기 어려운 성질을 말한다.
③ 대표적인 해시함수로는 MD5와 SHA 계열 함수를 들 수 있는데, 이 중 SHA-3는 해시 결과값의 크기로 128, 256, 384 비트 중 하나로 설정할 수 있다.
④ 비트코인에 활용되는 해시함수인 SHA-256은 SHA-2계열 해시함수의 하나로 해시 결과값의 크기가 256비트이다.

【문12】 IPv4와 IPv6에 관한 다음 설명 중 가장 옳지 않은 것은?

① 기존 IPv4는 32비트 주소길이를 사용하고, IPv6는 64비트 주소 길이를 사용한다.
② IPv4는 IPSec 프로토콜을 별도로 설치해야 하지만, IPv6는 자체 지원한다.
③ IPv4는 네트워크 클래스 단위의 비순차적으로 주소를 할당하지만, IPv6는 네트워크 규모와 단말기수에 따라 순차적으로 주소를 할당한다.
④ IPv6는 헤더 내에 플로우 레이블(Flow Label) 필드를 이용하여 트래픽을 효과적으로 분류할 수 있는 기능을 제공한다.

【문13】 다음 중 개인정보처리자가 개인정보 보호법 제18조(개인정보의 목적 외 이용·제공 제한)에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당되지 않은 것은?

① 정보주체로부터 별도의 동의를 받은 경우
② 다른 법률에 특별한 규정이 있는 경우
③ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우
④ 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우

【문14】 VPN(Virtual Private Network)에 관한 다음 설명 중 가장 옳지 않은 것은?

① VPN은 공중망을 경유하여 데이터가 전송되더라도 외부인으로부터 안전하게 보호되도록 주소 및 라우터 체계의 비공개, 데이터 암호화, 사용자 인증 및 사용자 엑세스 권한 제한 기능을 제공한다.
② SSL VPN은 종단간 보안이 가능하며 3계층 프로토콜이다.
③ VPN에서 사용되는 암호화 프로토콜에는 PPTP, L2TP, IPSec, SSL 등이 있다.
④ VPN은 IP 패킷이 공중망을 통과할 때 사용자 간에 전용망과 같은 보안 효과를 주기 위해 터널링 프로토콜을 통해 데이터를 캡슐화하여 전송한다.

【문15】 다음 설명 중 가장 옳지 않은 것은?

① 스니핑은 네트워크 상에서 주고받은 패킷 정보를 추출하여 사용자의 정보를 탈취하거나 통신 내용을 엿보는 공격이다.
② 서버 파밍은 여러 대의 컴퓨터를 이용해 대상 웹 서버에 과도한 트래픽을 보내 서버가 기능을 못하도록 만드는 공격이다.
③ 중간자공격은 통신 중인 두 객체 사이에 중간자가 데이터를 도청하고 조작한 후 다른 쪽으로 전달하는 공격이다.
④ 피싱은 신뢰할 수 있는 객체가 보낸 메시지로 가장하여 원래 사이트와 비슷한 사이트로 접속을 유도해 정보를 부정하게 얻는 공격이다.

【문16】 리눅스의 권한 설정에 관한 다음 설명 중 가장 옳지 않은 것은?

① 리눅스에서는 파일의 접근 권한에 대하여 파일을 만든 소유자 권한, 소유자가 속한 소유 그룹 권한으로만 나눠서 관리한다.
② 리눅스에서는 기본적으로 사용자 ID를 체크하여 실행 권한이 있으면 명령어를 수행한다.
③ 리눅스에서는 사용자 ID에게 실행 권한이 없으면 SetUID, SetGID, Sticky bit이 설정되어 있는지를 확인한다.
④ SetUID가 설정되어 있는 파일을 사용자가 실행하면 사용자의 권한이 아닌 소유자의 권한으로 실행한다.

【문17】 다음 중 해당 취약점에 대한 패치가 아직 나오지 않은 취약점을 이용한 공격은?

① 인젝션 공격
② 전수조사 공격
③ Slowloris 공격
④ 제로데이 공격

【문18】 다음 중 버퍼 오버플로 공격(Buffer Overflow Attack)에 취약한 함수와 가장 거리가 먼 것은?

① strcpy
② scanf
③ gets
④ printf

【문19】 다음 중 개인정보 보호법 시행령에서 정한 고유식별정보의 범위에 포함되지 않은 것은?

① 여권번호
② 운전면허번호
③ 이메일 주소
④ 외국인등록번호

【문20】 악성코드에 관한 다음 설명 중 가장 옳지 않은 것은?
① 트로이목마는 정상적인 프로그램으로 위장하여 사용자로 하여금 실행을 유도하는 악성 프로그램을 말한다.
② 바이러스는 프로그램 또는 문서에 삽입되어 감염되거나 동작한다.
③ 웜은 자체적으로 실행되면서 네트워크를 통해 자신을 복제하고 전파한다.
④ 루트킷은 바이러스나 웜과 결합하여 자동으로 설치되기 어렵다.

【문21】 보안 시스템 설계 시 참고하는 접근 제어 원칙 중 운영체제에서 사용하는 관리자 계정에 일반적으로 적용되지 않는 원칙은?
① 직무분리
② 고장 시 안전 초기화
③ 최소권한
④ 알 필요성

【문22】 SSL(Secure Socket Layer)에 관한 다음 설명 중 가장 옳지 않은 것은?
① 암호화된 웹서핑을 가능하게 한다.
② 서버 인증, 클라이언트 인증, 암호화된 세션 기능을 제공한다.
③ SSL을 지원하는 웹사이트는 https://로 시작한다.
④ 데이터링크 계층에서 동작하는 프로토콜이다.

【문23】 다음 중 ECC(Elliptic Curve Cryptosystem)와 RSA(Rivest Shamir Adleman) 암호 방식에 대한 설명으로 가장 옳지 않은 것은?
① ECC는 RSA에 비해 속도가 빠르다.
② RSA는 ECC에 비해 키 길이가 짧다.
③ ECC는 RSA 대비 소형 Mobile 환경에 적합하다.
④ ECC는 WPKI(무선) 기반 구조이고, RSA는 PKI(유선) 기반 구조이다.

【문24】 ARP 스푸핑 공격을 방지 하기 위한 방안으로 가장 옳지 않은 것은?
① 관리자가 수동으로 MAC 주소를 관리한다.
② ARP 캐쉬의 내용이 바뀌면 관리자에게 경고 메시지를 보내도록 설정한다.
③ 방화벽을 이용하여 ARP 패킷에 대해 임계값을 설정한다.
④ Snort와 같은 침입 탐지 시스템을 활용한다.

【문25】 IPSec 프로토콜이 보안을 제공하지 못하는 계층은?
① 응용
② 전송
③ 네트워크
④ 물리