【문 1】 ISMS-P(정보보호 및 개인정보보호 관리체계)에 관한 다음 설명 중 가장 옳지 않은 것은?

① ISMS-P는 정보보호와 개인정보보호 관리체계를 함께 심사하는 인증제도이다.
② 관리체계의 수립.운영 등 조직적.관리적 보호 활동이 주요 평가 대상이 된다.
③ 국내에서는 KISA가 제도 안내와 심사 관련 정보를 제공한다.
④ ISMS-P는 개별 보안 제품의 기능 안전성을 시험하는 제품 인증제도이다.

【문 2】 SSL과 TLS의 운용 및 보안성에 관한 다음 설명 중 가장 옳지 않은 것은?

① SSL 3.0은 역사적으로 통신의 기밀성, 변조 방지, 메시지 위조 방지를 목표로 설계된 프로토콜이었다.
② SSL 3.0은 더 이상 안전하다고 보기 어려우므로, 현대적 운용에서는 사용하지 않아야 한다.
③ TLS 1.3은 클라이언트와 서버 응용이 도청, 변조, 메시지 위조를 방지하도록 통신하기 위한 프로토콜이다.
④ 구형 시스템과의 호환성을 위해 TLS 접속 실패 시 SSL 3.0으로 자동 하향(fallback)하는 기능은 보안상 권장된다.

【문 3】 IPSec의 전송 모드와 프로토콜에 관한 다음 설명 중 가장 옳지 않은 것은?

① ESP(Encapsulating Security Payload)를 사용하는 전송 모드(Transport mode)에서는 종단점 중 적어도 하나가 암호화 종단점이면 사용할 수 있다.
② 인증 헤더(Authenticated Header)를 사용하는 터널 모드(Tunnel mode)에서는 데이터의 기밀성을 보장하지 못한다.
③ AH는 IP 헤더의 변경 불가능한(immutable) 필드까지 포함하여 무결성 검사를 수행하므로, NAT 환경을 통과할 때 문제가 발생할 수 있다.
④ 전송 모드(Transport mode)에서는 원본 IP 헤더는 그대로 유지되고, IP 페이로드(상위 계층 데이터)만 보호된다.

【문 4】 사이버 보안 모델에 관한 다음 설명 중 옳은 것을 모두 고른 것은?

ㄱ. Bell-LaPadula Model: 무결성 보호를 목적으로 하며, “No Read Down, No Write Up” 규칙을 따른다.
ㄴ. Biba Model: 기밀성 보호를 목적으로 하며, “No Read Up, No Write Down” 규칙을 따른다.
ㄷ. Clark-Wilson Model: 상업적 환경에서 무결성을 보장하기 위해 잘 정의된 트랜잭션과 직무 분리를 사용한다.
ㄹ. Chinese Wall Model: 이해 충돌(Conflict of Interest)을 방지하기 위해 경쟁사 정보 접근을 제한한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄷ, ㄹ

【문 5】 컴퓨터 보안 용어에 관한 다음 설명 중 가장 옳지 않은 것은?

① 공격자(Adversary): 공격하는 사람
② 위험(Risk): 특정 위협이 가져올 확률적으로 표현되는 예상되는 손실
③ 취약성(Vulnerability): 시스템 상의 오류나 약점
④ 위협(Threat): 시스템의 취약점을 악용하여 시도한 공격

【문 6】 다음은 인터넷 웜의 고전적인 전파 모델에 관한 설명이다. 감염 속도 dI(t)/dt를 가장 올바르게 표현한 것은?(단, 감염된 컴퓨터는 치료되지 않는다고 가정한다)

I(t): 시간 t동안 감염된 개체의 수
S(t): 시간 t동안 감염에 민감한 개체의 수(취약하지만 아직 감염되지 않은 컴퓨터의 수)
b: 감염률
N: 총 컴퓨터의 수, N = I(t) + S(t)

① bI(t)S(t)
② I(t)S(t)
③ bS(t)
④ I(t)S(t)/b

【문 7】 침입 탐지 시스템(Intrusion Detection System)에 관한 다음 설명 중 가장 옳지 않은 것은?

① 감사와 로깅할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않는다.
② NIDS는 네트워크를 통한 공격을 탐지하기 위한 장비다.
③ 네트워크를 통한 공격을 탐지할 뿐만 아니라 차단을 수행한다.
④ 설치 위치와 목적에 따라 HIDS와 NIDS로 나뉠 수 있다.

【문 8】 접근통제(Access Control) 모델에 관한 다음 설명 중 가장 옳은 것은?

① DAC(Discretionary Access Control)에서는 시스템 관리자가 모든 권한을 강제로 부여한다.
② MAC(Mandatory Access Control)에서는 객체의 소유자가 자신의 재량으로 권한을 부여한다.
③ RBAC(Role-based Access Control)은 사용자의 역할에 권한을 부여하고, 사용자는 역할을 통해 권한을 획득한다.
④ ABAC(Attribute-based Access Control)은 역할만을 기준으로 접근을 결정한다.

【문 9】 정보의 무결성(Integrity)을 검증하기 위해 사용되는 해시 함수(H)의 특성 중 ‘제2역상 저항성(Second Preimage Resistance)’의 의미에 관한 다음 설명 중 가장 옳은 것은?

① 해시값(y=H(x))이 주어져 있을 때, 그 해시값을 출력하는 입력값(x)을 찾기 어렵다.
② 입력값(x)이 주어져 있을 때, 그 입력과 같은 해시값(H(y)=H(x))을 출력하는 다른 입력값(y)을 찾기 어렵다.
③ 입력의 작은 변화가 해시값을 크게 바꾼다.
④ 같은 해시값(H(y)=H(x))을 출력하는 두 개의 다른 입력값(x, y, x≠y)을 찾기 어렵다.

【문10】 대칭 암호화 구조에 관한 다음 설명 중 가장 옳지 않은 것은?
① 평문(plaintext): 암호화될 데이터이며, 암호화 알고리즘의 입력값이다.
② 암호화 알고리즘: 평문을 변화시켜 암호문을 만드는 알고리즘이다.
③ 복호화 알고리즘: 암호문을 평문으로 바꾸어주는 알고리즘이다.
④ 비밀 키: 암호화 키와 복호화 키는 반드시 다른 종류이어야 한다.

【문11】 <보기>와 같은 ASP 코드에 대해서, 다음 중 SQL Injection이 성공하는 user 입력이 아닌 것은?(단, DBMS는 Microsoft SQL Server를 기준으로 한다)

< 보 기 >

```
set ok = execute( "SELECT * FROM Users
     WHERE user=' "  &  form("user")  & "
  '
     AND   pwd=' " & form("pwd") & " '" );

if not ok.EOF
     login success
else  fail;
```

① ' or 1=1 --
② ' ; DROP TABLE Users --
③ ' ; exec xp_cmdshell 'net user badguy badpwd / ADD' --
④ ' pwd=1234 --

【문12】 다음 중 문제를 수론(number theory) 문제로 변환한 후 양자 컴퓨터를 사용하여 큰 정수를 효율적으로 인수분해하도록 설계된 알고리즘은?
① 그로버 알고리즘(Grover's Algorithm)
② 쇼어 알고리즘(Shor's Algorithm)
③ 야오 법칙(Yao's Principle)
④ 확장 유클리드 알고리즘(Extended Euclidean Algorithm)

【문13】 이상 탐지 기반 IDS와 시그니처 기반 IDS의 비교에 관한 다음 설명 중 가장 옳지 않은 것은?
① 시그니처 기반 IDS는 알려진 공격 패턴 DB와 일치하는 트래픽을 탐지한다.
② 이상 탐지 기반 IDS는 정상 행위의 기준선을 학습한 후 이를 벗어난 경우를 탐지한다.
③ 시그니처 기반 IDS는 제로데이 공격(미지의 공격) 탐지에 강점이 있다.
④ 이상 탐지 기반 IDS는 오탐(False Positive) 비율이 상대적으로 높다.

【문14】 방화벽 유형에 관한 다음 설명 중 가장 옳은 것은?
① 패킷 필터링 방화벽(Packet Filtering Firewall)은 응용 계층 데이터까지 검사하므로 성능 오버헤드가 크다.
② 상태 기반 검사 방화벽(Stateful Inspection Firewall)은 연결 상태 테이블을 유지하여 트래픽 흐름을 동적으로 추적한다.
③ 애플리케이션 레벨 게이트웨이(Application-level Gateway)는 IP 헤더만 검사하고 응용 데이터는 검사하지 않는다.
④ 회선 레벨 게이트웨이(Circuit-level Gateway)는 각 패킷의 내용을 상세히 분석한다.

【문15】 SSH 프로토콜 구조에 관한 다음 설명 중 가장 옳지 않은 것은?
① SSH 사용자 인증 프로토콜은 클라이언트 사용자의 인증과 서버 호스트 키 검증을 담당하며, 서버 인증은 사용자 인증 단계에서 수행된다.
② SSH 사용자 인증 프로토콜은 전송 계층 위에서 동작하며 공개키, 패스워드, 호스트 기반 인증 등의 방법을 포함할 수 있다.
③ SSH 연결 프로토콜은 암호화된 터널 위에서 여러 논리 채널을 다중화하는 기능을 제공한다.
④ SSH 전송 계층 프로토콜은 일반적으로 TCP/IP 위에서 동작하며 서버 인증, 기밀성, 무결성을 제공한다.

【문16】 다음 중 능동적 공격(active attack)에 해당하지 않는 것은?
① 위장
② 가장
③ 메시지 위조
④ 트래픽 분석

【문17】 DoS 공격에 관한 다음 설명 중 가장 옳지 않은 것은?
① SIP Flood 공격은 IRC에 관한 공격 중 하나이다.
② Reflection 공격을 하려면 패킷 내 소스 IP 주소를 위조해야 한다.
③ Reflection 공격을 이용하면 DNS 서비스에 대한 DoS 공격이 가능하다.
④ DoS 공격은 가용성(Availability)을 떨어뜨리는 공격이다.

【문18】 다음 중 크로스사이트 스크립팅(XSS) 공격의 근본적인 원인으로 가장 옳은 것은?
① 취약한 암호화 알고리즘 사용
② 세션 타임아웃 미설정
③ 잘못된 접근통제 설정
④ 사용자 입력값의 불충분한 검증.이스케이핑

【문19】 다음 중 HTTPS가 HTTP와 비교하여 추가로 제공하는 핵심 기능으로 가장 옳은 것은?
① 더 빠른 데이터 전송 속도
② 전송 계층의 암호화 및 서버 인증
③ IP 주소 은닉
④ 바이러스 침투 방지

【문20】 다음 중 사용자 인증의 수단(factor)으로 가장 옳지 않은 것은?
① 지식 기반: Something you know (예: 비밀번호, PIN)
② 소유 기반: Something you have (예: 스마트카드, 토큰)
③ 생체 기반: Something you are (예: 지문, 홍채)
④ 신뢰 기반: Something you trust (예: 인증기관)

【문21】 비밀번호를 공격하는 방법에 관한 다음 설명 중 가장 옳은 것은?
① 오프라인 사전 공격은 암호화된 시스템 비밀번호 파일이 필요없다.
② 특정 계정 공격은 오프라인으로만 가능하다.
③ 잘 알려진 비밀번호를 공격하는 방법을 막기 위해서는 짧은 패스워드를 못 쓰게만 하면 된다.
④ 레인보우 테이블을 이용한 공격은 메모리가 충분할 때 효율적이다.

【문22】 다음 중 주요 서비스의 기본 포트번호로 옳지 않은 것은?
① SMTP: 21
② SSH: 22
③ remote desktop: 3389
④ HTTPS: 443

【문23】 다음 중 디지털 서명(Digital Signature)이 제공하는 보안 서비스가 아닌 것은?
① 기밀성(Confidentiality)
② 서명자 인증(Authentication)
③ 부인방지(Non-repudiation)
④ 무결성(Integrity)

【문24】 다음 중 항상 모든 가능한 평문이 모든 가능한 암호문으로 동일한 확률로 매핑되어 완벽한 비밀성을 보장하는 기법은?
① 디피-헬만 키 교환
② RSA
③ OTP (One-Time Pad)
④ 트리플 DES

【문25】 분산서비스거부(DDoS) 공격에 관한 다음 설명 중 가장 옳지 않은 것은?
① 정보보안의 3요소 중 가용성이 훼손된다.
② 일반 DoS와 달리 여러 호스트 또는 봇넷을 이용해 공격 트래픽을 분산.증폭시키는 경우가 많다.
③ UDP에서는 DDoS 공격이 성립하지 않는다.
④ 서버 메모리 증설만으로는 대역폭, CPU, 애플리케이션 처리량 등을 겨냥한 DDoS 공격을 충분히 방어하기 어렵다.