정보보호론

문 1. 공개키 인증서의 구조를 정의한 ITU-T 권고안은?
① X.25 ② X.121
③ X.400 ④ X.509

문 2. ㉠, ㉡에 들어갈 정보보안 위험의 처리 방식을 바르게 연결한 것은?

> (㉠)은(는) 사업 목적상 위험을 처리하는 데 들어가는 과도한 비용 또는 시간 때문에 일정 수준의 위험을 받아들이는 것으로, 그 위험이 조직에 발생시키는 결과에 대한 책임을 관리층이 지는 방식이다.
> (㉡)은(는) 위험에 대한 책임을 제3자와 공유하는 것으로, 보험을 들거나 다른 기관과의 계약을 통하여 잠재적 손실을 제3자에게 이전하거나 할당하는 방식이다.

	㉠	㉡
①	위험 회피	위험 전가
②	위험 회피	위험 감소
③	위험 수용	위험 전가
④	위험 수용	위험 감소

문 3. 다음에서 설명하는 컴퓨터 시스템의 평가 기준은?

> ○ 컴퓨터 시스템의 보안성을 평가하기 위해 미국 정부의 표준으로 채택된 기준이다.
> ○ Rainbow 시리즈라는 미 국방부 문서 중의 하나로 오렌지 북(Orange Book)으로 불린다.
> ○ 안전성과 신뢰성이 입증된 컴퓨터 시스템을 보급하기 위해 단계별 보안 평가 등급(D, C1, C2, B1, B2, B3, A1)을 분류하여 각 기관별 특성에 맞는 컴퓨터 시스템을 도입 및 운영하도록 권고하고 있다.

① TCSEC ② CC
③ CMVP ④ ITSEC

문 4. 유닉스 시스템 명령어에 대한 설명으로 옳지 않은 것은?
① grep – 파일 내 정규 표현식을 포함한 모든 행을 검색·출력하는 명령
② mesg – 모든 로그인 사용자에게 메시지를 전송하는 명령
③ chmod – 파일이나 디렉토리의 접근 권한을 변경하는 명령
④ man – 각종 명령의 사용법을 출력하는 명령

문 5. 「정보통신기반 보호법」상 주요정보통신기반시설을 관리하는 기관의 장이 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있는 기관에 해당하지 않는 것은?
① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조의 규정에 의한 한국인터넷진흥원
② 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업
③ 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조의 규정에 의한 한국전자통신연구원
④ 「국가정보화 기본법」 제14조의 규정에 의한 한국정보화진흥원

문 6. SHA-512 알고리즘의 처리 방식에 대한 설명으로 옳지 않은 것은?
① 최대 크기가 2^{128}비트 이하인 메시지를 입력받아 512비트 메시지 다이제스트를 출력한다.
② 필요한 길이의 패딩과 128비트 블록을 추가하여 처리하려는 메시지의 전체 크기가 1,024비트의 배수가 되게 한다.
③ 8개 소수의 제곱근에서 얻은 이진수로 초기화된 512비트 버퍼를 알고리즘의 중간 값과 최종 값을 저장하는 데 사용한다.
④ 블록 단위로 메시지를 처리하는 과정은 80라운드로 이루어지며, 규칙성을 제거하기 위해 각 라운드마다 서로 다른 암호 키를 사용한다.

문 7. 커버로스(Kerberos) 버전 4 인증 시스템에서 클라이언트가 응용 서버에게 제시하는 티켓에 포함되는 구성요소가 아닌 것은?
① 클라이언트 ID
② 클라이언트와 응용 서버 간의 세션키
③ 인증 서버의 네트워크 주소
④ 티켓의 유효시간

문 8. 방화벽은 검사 대상이나 동작 방식에 따라 패킷 필터링, 상태 검사(stateful inspection), 응용 레벨 게이트웨이, 회선 레벨 게이트웨이로 분류할 수 있다. 상태 검사 방화벽에 대한 설명으로 옳은 것은?
① 트래픽 정보 수집이 어렵고, IP 스푸핑 공격에 대응하기 어렵다.
② 서비스별로 프록시 서버 데몬을 두어 사용자 인증과 접근 제어를 수행한다.
③ 패킷 필터링 기능을 사용하며 현재 연결 세션의 트래픽 상태와 미리 저장된 상태와의 비교를 통하여 접근을 제어한다.
④ 송·수신자 간의 직접적인 연결을 허용하지 않고, 송신자와 수신자 사이에서 프록시가 어떤 연결을 허용할지를 판단한다.

문 9. VPN의 터널링 기능을 제공하는 L2TP(Layer 2 Tunneling Protocol)에 대한 설명으로 옳지 않은 것은?
① 데이터 링크 계층에서 터널링을 지원한다.
② PPTP(Point-to-Point Tunneling Protocol)와 L2F(Layer 2 Forwarding Protocol)의 기능을 결합한 프로토콜이다.
③ 데이터의 보안성을 높이기 위하여 IPsec과 결합하여 사용할 수 있다.
④ 패킷 인증, 암호화, 키 관리 기능을 제공한다.

문 10. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보 유출등의 통지·신고에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

> 정보통신서비스 제공자등은 개인정보의 분실·도난·유출(이하 "유출등"이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 (㉠) 또는 (㉡)에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
> 1. 유출등이 된 개인정보 항목
> 2. 유출등이 발생한 시점
> 3. 이용자가 취할 수 있는 조치
> 4. 정보통신서비스 제공자등의 대응 조치
> 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

	㉠	㉡
①	과학기술정보통신부	한국인터넷진흥원
②	과학기술정보통신부	개인정보보호위원회
③	방송통신위원회	한국인터넷진흥원
④	방송통신위원회	개인정보보호위원회

문 11. 침입차단시스템이 제공하는 주요 보안 서비스가 아닌 것은?
① 접근 통제 ② 최대 권한 부여
③ 사용자 인증 ④ 감사 및 로그 기능

문 12. ㉠, ㉡에 들어갈 네트워크 보안 공격을 바르게 연결한 것은?

> (㉠)은(는) TCP 연결 설정을 위한 3-way handshaking 과정에서 half-open 연결 시도가 가능하다는 취약성을 이용하는 공격 방식이다.
> (㉡)은(는) 서버와 클라이언트가 TCP 통신을 하고 있을 때, RST 패킷을 보내고 시퀀스 넘버 등을 조작하여 연결을 가로채는 공격 방식이다.

㉠	㉡
① SYN 플러딩	IP 스푸핑
② SYN 플러딩	세션 하이재킹
③ ARP 스푸핑	IP 스푸핑
④ ARP 스푸핑	세션 하이재킹

문 13. 다음에서 설명하는 암호 알고리즘은?

> ○ Koblitz와 Miller가 제안한 것이다.
> ○ RSA보다 키의 길이를 작게 하면서도 대등한 보안성을 제공한다.
> ○ 전자서명이나 키 교환에 활용될 수 있다.
> ○ 메모리와 처리능력이 제한된 분야에 효율적이다.

① ElGamal
② ECC(Elliptic Curve Cryptography)
③ Rabin
④ WHIRLPOOL

문 14. ㉠, ㉡에 들어갈 웹 공격 기법을 바르게 연결한 것은?

> (㉠)은(는) 웹 해킹으로 서버 권한을 획득한 후, 해당 서버에서 공격자의 PC로 연결하고 공격자가 직접 명령을 입력하여 개인정보 전송 등의 악의적인 행위를 하는 공격이다. 이 기법은 방화벽의 내부에서 외부로 나가는 패킷에 대한 아웃바운드 필터링을 수행하지 않는 허점을 이용한다.
> (㉡)은(는) 공격자가 웹 서버의 게시판 등에 악성 스크립트를 삽입한 후, 사용자의 쿠키와 같은 개인정보를 특정 사이트로 전송하게 하거나 악성파일을 다운로드하여 실행하도록 유도하는 공격이다.

㉠	㉡
① 디렉토리 리스팅	포맷 스트링
② 디렉토리 리스팅	XSS
③ 리버스 텔넷	포맷 스트링
④ 리버스 텔넷	XSS

문 15. IEEE 802.11i에서 정의된 CCMP(Counter Mode with Cipher Block Chaining MAC Protocol)에 대한 설명으로 옳지 않은 것은?
① 기존의 WEP(Wired Equivalent Privacy) 보안 구현 장치에서 소프트웨어적으로 동작할 수 있도록 고안되었다.
② CBC(Cipher Block Chaining)-MAC를 사용하여 메시지 무결성을 제공한다.
③ AES(Advanced Encryption Standard)의 CTR 블록 암호 모드를 사용한다.
④ WPA2(Wi-Fi Protected Access 2)에서 사용하는 보안 기술이다.

문 16. 전자우편 보안을 위한 PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?
① 전자우편 메시지의 인증과 기밀성 제공을 위한 것으로 필 짐머만(Phil Zimmermann)이 고안하였다.
② 메시지 발송 시 메시지에 대한 서명, 압축, 암호화 순으로 처리할 수 있다.
③ 임의의 사용자는 여러 개의 공개·개인키 쌍을 가질 수 있도록 하고 있다.
④ 메시지 암호화를 위한 일회용 세션키를 사용하지 않기 때문에 공유 비밀키를 교환하기 위한 절차가 필요하다.

문 17. 스트림 암호에 대한 설명으로 옳은 것은?
① 대표적인 스트림 암호 방식인 RC4는 다양한 키 길이를 갖도록 설계된 바이트 기반의 알고리즘이다.
② 안전성은 키열(key stream)을 생성하는 의사 난수 생성기의 안전성에 반비례한다.
③ 블록 암호와 달리 구현이 어렵고 속도가 느린 단점이 있다.
④ 키열의 반복 주기가 짧을수록 암호문을 해독하기가 더 어려워진다.

문 18. 「개인정보의 안전성 확보조치 기준」상 개인정보처리자가 개인정보를 암호화할 때 준수해야 할 사항으로 옳지 않은 것은?
① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.
② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.
③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ: Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.
④ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어를 사용하여서는 아니 된다.

문 19. RSA 암호 알고리즘에 대한 설명으로 옳지 않은 것은?
① 대표적인 비대칭 암호 알고리즘으로, 널리 사용되고 있다.
② 공개키 $\{e,n\}$이 주어지면 지수 및 모듈러 연산을 통해 n과 무관한 임의 크기의 평문 블록을 하나의 암호문 블록으로 암호화할 수 있다.
③ 공개키 $\{e,n\}$의 n을 소인수분해할 수 있으면 개인키 $\{d,n\}$의 d를 알아낼 수 있다.
④ 일반적으로 키의 길이가 길수록 안전성은 높아지지만 알고리즘 수행시간은 길어진다.

문 20. 중간 시스템(reflector)을 이용해서 서비스 거부(DoS)를 발생시키는 반사(reflection) DDoS 공격에 대한 설명으로 옳지 않은 것은?
① 공격 대상의 주소를 시작 주소로 갖는 패킷을 중간 시스템에 보낸다.
② 중간 시스템으로 네트워크 연결이 좋은 고용량의 네트워크 서버나 라우터가 이용될 수도 있다.
③ 사전에 중간 시스템 내부에 공격자의 명령 수행을 위한 비정상 프로그램이 작동하도록 해야 한다.
④ 중간 시스템이 요청 메시지에 대해서 큰 응답 메시지를 생성하는 서비스를 이용하면 공격 대상 시스템에 더 많은 피해를 줄 수 있다.