1. 블록암호 알고리즘 중 보안강도가 가장 높은 것은?
① DES ② AES-192
③ 3TDEA ④ HIGHT

2. ISO/IEC 27001 통제 항목 및 통제 내용에 대한 설명으로 가장 옳지 않은 것은?
① 운영관리 영역은 정보보호 정책, 정보보호 조직 구성 등을 통제한다.
② 인적자원 보호 영역은 내부 조직, 외부 기업, 고용 전, 고용 기간, 고용 변경 및 종료 등을 통제한다.
③ 접근통제 영역은 접근통제 요구사항, 사용자 접근관리, 사용자 책임, 네트워크 접근, 운영시스템 접근 등을 통제한다.
④ 통신 보안 영역은 네트워크 정보보호 관리, 매체 취급, 정보교환, 전자상거래서비스, 모니터링 등을 통제한다.

3. XSS(Cross-Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?
① XSS 공격은 쿠키에 저장된 DBMS의 SQL 구문의 취약점을 공격하는 기법이다.
② Stored XSS는 게시판 또는 자료실과 같이 사용자가 글을 저장하는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 기법이다.
③ Reflected XSS는 웹 애플리케이션에 스크립트를 저장하는 것이 아니라 URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법이다.
④ CSRF 공격은 피해자가 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 리퀘스트를 보내도록 하는 기법이다.

4. 다양한 NAC(Network Access Control) 구현 방식에 대한 설명으로 가장 옳지 않은 것은?
① 802.1x 방식은 802.1x 프로토콜과 RADIUS 서버를 이용하는 것으로, 실질적인 접근 허용이나 차단은 스위치에서 수행하고 신규 클라이언트에 대한 인증 요청은 실제로 인증을 수행하는 RADIUS 서버로 전달한다.
② VLAN 방식은 인가받지 않은 사용자라면 VLAN으로 미리 분리된 망 중에서 통신이 되지 않는 VLAN 망에 신규 클라이언트를 할당한다.
③ ARP 방식은 신규 클라이언트가 적법한 사용자라면 NAC가 게이트웨이의 정상적인 MAC 주소를 알려주고, 그렇지 않은 사용자라면 비정상적인 MAC 주소를 전송하여 네트워크에 대한 접근을 막는다.
④ 소프트웨어 에이전트 설치 방식은 네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치하는 동시에 해당 클라이언트에서 차단 정책을 설정한다.

5. 버퍼 오버플로우 공격을 고려할 때 가장 안전한 C언어 함수는?
① snprintf( ) ② strcpy( )
③ strcat( ) ④ gets( )

6. 생체기반 인증에 대한 설명으로 가장 옳지 않은 것은?
① FRR은 오거부율을 말하며 시스템에 등록된 사용자 본인의 생체정보를 본인이 아닌 것으로 잘못 판단하여 인증을 거부하는 오류율이다.
② EER은 오인식률과 오거부율이 같아지는 비율을 말하며, EER이 높을수록 인증의 정확도가 높아진다.
③ 생체인식을 위해 이용되는 생체정보를 선택함에 있어서 고려해야 하는 요소인 보편성은 시스템을 이용하는 모든 사람들이 인증하는 데 사용되는 생체정보를 지니고 있어야 함을 의미한다.
④ FAR은 오인식률을 말하며, 시스템이 본인의 것이 아닌 다른 사람의 생체인식 정보를 본인의 것으로 잘못 판단하여 인증을 수락하는 오류율이다.

7. 접근통제 모델에 대한 설명으로 가장 옳은 것은?
① Bell-LaPadula 모델에서 낮은 보안 수준의 권한을 가진 사람이 자신의 권한보다 높은 보안 수준을 가진 문서에 대해 쓰기가 불가능하다.
② Bell-LaPadula 모델은 보다 신뢰할 수 있는 정보, 즉 정보의 무결성을 높이는 데 목적이 있는 경우 사용된다.
③ Biba 모델에서는 낮은 무결성 수준의 권한을 가진 사람이 자신의 권한보다 높은 무결성 수준의 문서에 대해 읽기가 불가능하다.
④ Biba 모델에서는 높은 무결성 수준의 권한을 가진 사람이 자신의 권한보다 낮은 무결성 수준의 문서에 대해 쓰기가 가능하다.

8. MAC(Message Authentication Code)에 대한 설명으로 가장 옳지 않은 것은?
① 전송할 데이터가 변조되었는지 검증할 수 있도록 덧붙이는 코드이다.
② MAC을 통해 데이터의 기밀성을 보장할 수 있다.
③ 해시함수를 이용해 MAC을 구성하는 것이 HMAC(Hashed MAC)이다.
④ MAC이 사용되는 사례로는 IPSec, SSL/TLS 등이 있다.

9. 리눅스 및 유닉스 계열의 운영체제에서 디렉터리 탐색 공격을 위해 사용되는 etc 디렉터리에 있는 passwd 파일을 다운로드하는 경로명으로 가장 옳은 것은?

① ../root/bin/passwd ② ../etc/passwd
③ ../etc/sbin/passwd ④ /home/passwd

10. 악성코드의 특징과 사례에 대한 설명으로 가장 옳지 않은 것은?

① 좀비 악성코드에 감염되면 외부 명령에 의해 DDoS 공격에 사용되기도 한다.
② 다형성 바이러스는 응용 프로그램에 의해 해석되는 매크로나 스크립팅 코드를 사용하며 주로 문서에 포함된다.
③ 바이러스, 웜, 좀비 악성코드는 자가 복제를 하는 특징이 있다.
④ Drive-by-Download 악성코드는 사용자가 이것을 심어 놓은 웹사이트를 방문할 때 자신도 모르게 다운로드 된다.

11. 공개키 암호 알고리즘인 RSA에 대한 설명으로 가장 옳지 않은 것은? (단, N은 서로 다른 두 개의 소수를 곱한 값이다.)

① 공개키 암호 알고리즘은 암호화 키와 복호화 키를 사용하며, RSA는 디지털 서명에 사용할 수 있다.
② RSA의 암호문은 평문을 E제곱해서 mod N을 취하여 만들 수 있으며 여기서 E와 N으로 이뤄진 쌍이 공개키다.
③ RSA의 평문은 암호문을 D제곱해서 mod N을 취하여 만들 수 있으며 여기서 D와 N으로 이뤄진 쌍이 개인키다.
④ 큰 수의 소인수 분해를 고속으로 할 수 있는 방법이 발견되면 RSA를 해독할 수 있으며, 중간자 공격을 사용해도 RSA를 해독할 수 있다.

12. 무선 랜 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① 802.11b는 와이파이라고 하며 WEP 방식의 보안 기능을 사용한다.
② 802.11g는 802.11b에 802.11a의 속도 성능을 추가한 프로토콜이다.
③ 802.11n은 여러 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술로, 대역폭 손실을 최소화하며 최대 속도는 400Mbps이다.
④ 802.11ad는 60GHz 대역을 사용해 데이터를 전송하는 방식으로 대용량의 데이터 등 높은 비트레이트 동영상 스트리밍에 적합하다.

13. 〈보기〉의 설명에 가장 적합한 용어는?

〈보기〉

- DDoS와 같은 서비스 거부 공격의 대응 방법으로 사용된다.
- 특정 IP 주소로부터의 패킷들을 드롭시키는 방법을 적용한다.

① IP spoofing
② Security patches
③ Port scanning
④ Blackholing

14. IKE(Internet Key Exchange) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① IPSec의 구성 요소 중 하나로 SA(Security Association)를 성립하는 데 필요한 데이터들을 안전하게 전달하기 위해 사용된다.
② ISAKMP를 토대로 만들어진 IPSec 전용의 키 교환 프로토콜이다.
③ IKEv2와 IKEv1은 서로 호환된다.
④ Diffie-Hellman 키 교환 프로토콜이 IKE에서 사용된다.

15. 개인정보 보호법령상 개인정보의 안전성 확보 조치를 위한 개인정보처리자의 업무로 가장 옳지 않은 것은?

① 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
② 개인정보 유출 및 오용·남용 방지를 위한 내부통제 시스템의 구축
③ 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
④ 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치

16. 〈보기〉에서 설명하는 블록암호 운영 모드로 가장 옳은 것은?

〈보기〉

CTR과 CBC-MAC을 통합한 블록암호 모드로 기밀성과 인증, 무결성을 제공한다. 핵심적인 알고리즘의 구성 요소는 AES 암호 알고리즘, CTR 모드, CBC-MAC이다. NIST에 의해 IEEE 802.11 WiFi 보안 요구사항을 지원하기 위해 표준화되었다.

① CCM ② GCM
③ CFB ④ OFB

17. 〈보기〉는 정보보호 및 개인정보보호 관리체계(ISMS-P)의 개인정보 수집 제한에 대한 인증 기준이다. 이 기준에 대한 주요 확인사항으로 가장 옳지 않은 것은?

〈보기〉

개인정보는 서비스 제공을 위해 필요한 최소한의 정보를 적법하고 정당하게 수집하여야 하며, 필수정보 이외의 개인정보를 수집하는 경우에는 선택항목으로 구분하여 해당 정보를 제공하지 않는다는 이유로 서비스 제공을 거부하지 않아야 한다.

① 개인정보를 수집하는 경우 서비스 제공 또는 법령에 근거한 처리 등을 위해 필요한 범위 내에서 최소한의 정보만을 수집하고 있는가?

② 수집 목적에 필요한 최소한의 정보 외의 개인정보를 수집하는 경우 정보주체(이용자)가 해당 개인정보의 제공 여부를 선택할 수 있도록 하고 있는가?

③ 정보주체(이용자)가 수집 목적에 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 서비스 또는 재화의 제공을 거부하지 않도록 하고 있는가?

④ 법적 근거에 따라 정보주체(이용자)의 주민등록번호 수집이 가능한 경우에도 아이핀, 휴대폰 인증 등 주민등록번호를 대체하는 수단을 제공하고 있는가?

18. 블록암호 알고리즘을 구성하는 데 사용되는 페이스텔(Feistel) 구조와 SPN 구조에 대한 설명으로 가장 옳은 것은?

① 정상적으로 복호화 과정이 수행되기 위해서 페이스텔 구조의 라운드 함수는 가역적(invertible)이어야 한다.

② 페이스텔 구조를 사용하는 대표적인 블록암호 알고리즘으로 AES가 있다.

③ SPN 구조는 Shannon의 혼동(confusion)과 확산(diffusion) 이론을 바탕으로 한 구조이다.

④ SPN 구조의 암호화 과정은 최소 2라운드 반복 수행해야 전체 평문이 암호화된다.

19. 타원 곡선 암호(ECC: Elliptic Curve Cryptography)에 대한 설명으로 가장 옳은 것은?

① 사용되는 키의 길이가 RSA보다 짧다.

② 타원 곡선 위의 실숫값을 이용하여 계산하는 기술이다.

③ 데이터 암호화와 복호화에 사용되며, 디지털 서명에는 사용이 불가능하다.

④ 타원 곡선상의 점 G와 정수 x에 대하여, xG를 계산하는 데 시간이 오래 걸린다는 성질을 이용한다.

20. RAID level과 그 특성을 옳게 짝지은 것은?

	RAID 0	RAID 1	RAID 5
①	striping	mirroring	distributed parity
②	mirroring	striping	parity
③	parity	mirroring	multiple storage
④	mirroring	striping	fast mirroring