정보시스템보안

1. 다음 중 디지털 포렌식의 기본 원칙에 대한 설명으로 가장 옳지 않은 것은?
   ① 정당성의 원칙 : 모든 증거는 적법한 절차를 거쳐 획득하여야 하며, 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
   ② 재현의 원칙 : 증거는 어떤 절차를 통해 정제될 수 없으며 똑같은 환경에서 같은 결과가 한번만 나오면 된다.
   ③ 신속성의 원칙 : 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 가능한 빠르게 획득해야 한다.
   ④ 연계 보관성의 원칙 : 증거는 획득 후 이송/분석/보관/법정 제출의 과정이 명확해야 하며, 이러한 과정에 대한 추적이 가능해야 한다.

2. 다음 중 정보자산에 대한 위험분석에서 사용하는 ALE, SLE, ARO 사이의 관계로 가장 옳은 것은?
   ① ALE=SLE+ARO
   ② SLE=ALE+ARO
   ③ ALE=SLE×ARO
   ④ SLE=ARO×ALE

3. 다음 중 대칭키 암호에 대한 설명으로 가장 옳지 않은 것은?
   ① DES, AES는 대칭키 암호 알고리즘에 속한다.
   ② AES는 SPN(Substitution-Permutation Network) 기반 대칭키 암호이다.
   ③ AES는 128bit 라운드 키를 사용한다.
   ④ 대칭키 암호는 두 개의 키 값(비밀키, 공개키)이 서로 대칭적으로 존재해야 한다.

4. 다음 중 Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?
   ① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
   ② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
   ③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
   ④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

5. 다음 중 KDC(Key Distribution Center) 없이 양쪽 통신 주체가 대칭 세션 키를 생성할 수 있는 프로토콜로 가장 옳은 것은?
   ① Otway-Rees 프로토콜
   ② Needham-Schroeder 프로토콜
   ③ Kerberos 프로토콜
   ④ Diffie-Hellman 프로토콜

6. 정부는 사이버테러를 없애기 위하여 2020년 8월 「개인정보 보호법」 개정으로 100만 명 이상 이용자의 개인정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 망분리를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 가장 옳지 않은 것은?
   ① DMZ
   ② OS 커널분리
   ③ VDI
   ④ 가상화기술

7. 다음 중 유닉스/리눅스 시스템의 로그 파일에 기록되는 정보에 대한 설명으로 가장 옳지 않은 것은?
   ① secure - telnet이나 ftp 등 인증과정을 거치는 모든 로그를 저장
   ② loginlog - 성공한 로그인에 대한 내용
   ③ pacct - 시스템에 로그인한 모든 사용자가 수행한 프로그램 정보
   ④ btmp - 5번 이상 실패한 로그인 시도 정보

8. 다음 <보기> 중 리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 가장 옳은 것을 모두 고른 것은?

< 보 기 >

㉠ 재부팅 시간 정보
㉡ 사용자의 로그인/로그아웃 정보
㉢ 로그인에 실패한 사용자의 IP주소

① ㉠
② ㉠, ㉡
③ ㉡
④ ㉠, ㉡, ㉢

9. 다음 중 스트림 암호에 대한 설명으로 가장 옳지 않은 것은?
① 통상 한 번에 1비트씩 암호화 및 복호화를 하기 때문에 하드웨어적인 shift register 방식을 많이 사용한다.
② 짧은 주기와 높은 선형 복잡도가 요구되며 주로 LFSR을 이용한다.
③ 스트림 암호는 데이터의 흐름을 순차적으로 처리해 가기 때문에 내부상태를 가지고 있다.
④ 블록 암호화 방식보다 매우 빠르지만 암호화 강도는 약하다.

10. 다음은 정보보호 관리 체계(ISMS, Information Security Management System) 5단계 과정을 수립하려고 한다. 가장 옳은 순서는?
① 경영 조직 → 위험 관리 → 정책 수립 및 범위 설정 → 구현 → 사후관리
② 정책 수립 및 범위 설정 → 경영 조직 → 위험 관리 → 구현 → 사후관리
③ 정책 수립 및 범위 설정 → 경영 조직 → 구현 → 위험 관리 → 사후관리
④ 경영 조직 → 정책 수립 및 범위 설정 → 위험 관리 → 구현 → 사후관리

11. 다음 <보기>의 ㉠, ㉡에 들어갈 웹 공격 기법으로 가장 옳은 것은?

< 보 기 >

(㉠)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

12. 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec(IP Security Protocol)에 대한 설명 중 가장 옳지 않은 것은?
① 네트워크 계층의 보안을 위하여 인증 헤더(AH, Authentication Header) 프로토콜과 ESP(Encapsulating Security Payload) 프로토콜을 사용하여 보안연계(SA, Security Association) 서비스를 제공한다.
② 강력한 암호화와 인증 방식을 가지며, 두 컴퓨터 사이의 터널화 된 통신을 가능하도록 한다.
③ 비연결 무결성은 메시지가 위·변조되지 않았음을 보장해준다.
④ ESP 프로토콜은 암호화를 지원하지 않으며 AH 프로토콜만 암호화를 지원한다.

13. 다음 <보기>의 접근 제어 정책으로 가장 옳은 것은 무엇인가?

< 보 기 >

○ 한 주체가 어느 한 객체를 읽고 그 내용을 다른 어느 한 객체로 복사하는 경우에 처음의 객체에 내포된 접근 통제 정보가 복사된 객체로 전달되지 않는다.
○ 특정 객체에 대해 특정 주체가 다른 주체에 대해 임의적으로 접근 제어가 가능하여 매우 유연한 접근 제어 서비스를 제공할 수 있다.

① Access Control List
② RBAC
③ DAC
④ MAC

14. 다음 <보기>에서 설명하는 블록암호 운용 모드는?

< 보 기 >

○ 암·복호화 모두 병렬 처리가 가능하다.
○ 블록 암호 알고리즘의 암호화 로직만 사용한다.
○ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① CTR
② CFB
③ CBC
④ ECB

15. 다음 <보기>에서 설명하는 기법으로 가장 옳은 것은?

< 보 기 >

높은 등급의 인가를 가진 주체가 낮은 등급의 인가를 가진 주체에게 정보를 보내는 방법으로 비밀정보를 다른 사람이 알지 못하게 전달하는 방법이다.

① 터널링
② 은닉채널
③ 송신채널
④ 이중채널

16. 다음 <보기>는 사이버 침해사고 대응절차에 대한 설명이다. 침해사고 대응 1단계부터 6단계까지 순서를 가장 옳게 나열한 것은?

< 보 기 >

㉠ 침해사고의 인식 및 신고
㉡ 긴급조치
㉢ 침해사고 결과 분석 및 보고서 작성
㉣ 분석
㉤ 재발방지 조치
㉥ 침해사고 분석 및 대응 결과 승인

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

17. 다음 중 커버로스(Kerberose)에 대한 설명으로 가장 옳지 않은 것은?

① 커버로스는 모든 사용자의 패스워드를 알고 있고, 중앙집중식 데이터베이스에 그 패스워드를 저장하고 있는 인증 서버를 이용한다.
② 커버로스는 사용자에게 동일한 계정 정보로 여러가지 서비스를 받을 수 있게 한다.
③ 커버로스는 패스워드 사전공격(Dictionary Attack)에 강하다.
④ 대칭키를 사용하여 도청으로부터 보호한다.

18. 암호 해독자가 일정량의 평문 P에 대응하는 암호문 C를 알고 있는 상태에서 해독하는 방법이며, 암호문 C와 평문 P의 관계로부터 키 K나 평문 P를 추정하여 해독하는 공격방법은 무엇인가?

① KPA
② CPA
③ COA
④ CCA

19. 다음 중 위험(Risk)에 대한 정의 및 구성요소에 대한 내용으로 가장 옳지 않은 것은?

① 위험이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 말한다.
② 위험은 자산, 위협, 취약성으로 표현한다.
③ 위험은 손실을 끼치는 사건 발생 가능성에는 비례하나 발생 손실의 정도에 반비례한다.
④ 위협 주체가 취약점을 활용할 수 있는 가능성과 그와 관련된 비즈니스 영향을 가리킨다.

20. 다음 중 위험분석 방법에 대한 설명으로 가장 옳지 않은 것은?

① 과거자료 분석법 : 과거 자료가 많을수록 분석의 정확도가 높아진다. 과거에 일어났던 사건이 미래에도 일어난다는 가정이 필요하며 과거의 사건 중 발생 빈도가 낮은 자료에 대해서는 적용이 어렵다.
② 확률분포법 : 미지의 사건을 추정하는데 사용되는 방법이다. 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다. (정확성이 낮다)
③ 시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법이다.
④ 순위 결정법 : 시스템에 관한 전문적인 지식을 갖춘 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다.