2021년도 일반직공무원 채용시험 문제지

- 정 보 보 호 (9급) -

성 명 :	응 시 번 호 :

응시자 유의사항 및 과목별 코드번호

※ **시험 과목 : 컴퓨터일반(15), 네트워크보안(28), 정보시스템보안(29)**

※ **시험이 시작되기 전까지 표지를 넘기지 마시오.**

해 양 경 찰 청

컴퓨터일반

1. 다음 중 해싱(Hashing)에 대한 설명으로 가장 옳지 않은 것은?
   ① 서로 다른 탐색키가 해시 함수를 통해 동일한 해시 주소로 사상될 수 있다.
   ② 충돌(Collision)이 발생하지 않는 해시 함수를 사용한다면 해싱의 탐색시간 복잡도는 O(1)이다.
   ③ 선형 조사법(Linear Probing)은 연결리스트(Linked List)를 사용하여 오버플로우 문제를 해결한다.
   ④ 폴딩함수(Folding Function)는 탐색키를 여러 부분으로 나누어 이들을 더하거나 배타적 논리합을 하여 해시 주소를 얻는다.

2. 후위표기법(Postfix Notation)으로 된 다음 식의 전위표기법(Prefix Notation)으로 옳은 것은?

ABC+D/-AE+BF*/+

   ① +-A/+BCD/+AE*BF
   ② -+A/BC+D/+AE*BF
   ③ +-A/+BCD/+*AEBF
   ④ +A-/+BCD/+AE*BF

3. 다음 <보기>의 고객계좌 테이블에서 잔고가 1,000,000원에서 3,000,000원 사이인 고객들의 등급을 '우대고객'으로 변경하고자 <보기>와 같은 SQL문을 작성하였다. ㉠과 ㉡에 순서대로 들어갈 내용으로 가장 옳은 것은?

<보 기>

```
UPDATE 고객계좌
(㉠) 등급 = '우대고객'
WHERE 잔고 (㉡) 1000000 AND 3000000
```

   ① SET, IN ② SET, BETWEEN
   ③ VALUES, IN ④ VALUES, BETWEEN

4. 다음 중 RISC와 CISC에 대한 설명 중 가장 옳지 않은 것은?
   ① RISC는 실행 빈도가 적은 하드웨어를 제거하여 자원 이용률을 높이는 장점이 있다.
   ② CISC는 고급 언어를 이용하여 알고리즘을 쉽게 표현 할 수 있는 장점이 있다.
   ③ RISC는 프로그램의 길이가 길어지므로 CISC보다 수행 속도가 느린 단점이 있다.
   ④ CISC는 복잡한 명령어군을 제공하므로 컴퓨터 설계 및 구현 시 많은 시간을 필요로 하는 단점이 있다.

5. IPv4 주소체계 기반의 어떤 네트워크 상에서 두 컴퓨터 A, B가 각각 192.168.0.1과 192.168.0.65의 주소를 사용할 때, 이 두 컴퓨터가 서로 다른 서브넷(Subnet) 상에 존재하기 위해 사용해야 하는 서브넷 마스크(Subnet Mask)로 가장 옳은 것은?
   ① 0.0.0.0 ② 255.255.255.0
   ③ 255.255.255.192 ④ 255.255.255.128

6. 다음 <보기> 중 잘 알려진 포트번호(Well-Known Port)와 TCP 프로토콜이 바르게 연결된 것을 모두 고른 것은?

<보기>

㉠ 21번 포트 : FTP ㉡ 67번 포트 : DHCP
㉢ 23번 포트 : SMTP ㉣ 80번 포트 : HTTP

   ① ㉠, ㉡ ② ㉠, ㉣ ③ ㉡, ㉢ ④ ㉡, ㉣

7. 다음 중 RAID 기술에 대한 설명으로 가장 옳지 않은 것은?
   ① RAID 1레벨은 미러링(Mirroring)을 지원한다.
   ② RAID 3레벨은 데이터를 블록 단위로 분산 저장하여 대용량의 읽기 중심 서버용으로 사용한다.
   ③ RAID 5레벨은 고정적인 패리티 디스크 대신 패리티가 모든 디스크에 분산되어 저장되므로 병목현상을 줄여준다.
   ④ RAID 6레벨은 두 개의 패리티 디스크를 사용하므로 두 개의 디스크 장애 시에도 데이터의 복구가 가능하다.

8. 다음 중 인터럽트 우선순위를 결정하는 Polling방식에 대한 설명으로 가장 옳지 않은 것은?
   ① 많은 인터럽트 발생 시 처리시간 및 반응시간이 매우 빠르다.
   ② S/W적으로 CPU가 각 장치 하나하나를 차례로 조사하는 방식이다.
   ③ 조사 순위가 우선순위가 된다.
   ④ 모든 인터럽트를 위한 공통의 서비스 루틴을 갖고 있다.

9. 운영체제는 일괄처리(Batch), 대화식(Interactive), 실시간(Real-Time) 시스템 그리고 일괄처리와 대화식이 결합된 혼합 시스템(Hybrid System) 등으로 분류될 수 있다. 이와 같은 분류 근거로 가장 옳은 것은?
   ① 응답 시간과 데이터 입력 방식
   ② 데이터 보호의 필요성 여부
   ③ 버퍼링(Buffering) 기능 수행 여부
   ④ 고급 프로그램 언어의 사용 여부

10. 다음 <보기>의 JAVA 프로그램 실행 결과로 가장 옳은 것은?

< 보기 >

```
class Test {
        public static void main(String[] args) {
                int a = 101;
                System.out.println((a>>3) << 2);
        }
}
```

① 0 ② 48 ③ 404 ④ 600

11. 다음 중 Flynn의 병렬컴퓨터 분류방식에 대한 설명으로 가장 옳지 않은 것은?

① SISD : 명령어와 데이터를 순서대로 처리하는 단일프로세서 시스템이다.
② SIMD : 단일 명령어 스트림을 처리하며 배열 프로세서라고도 한다.
③ MISD : 여러 개의 프로세서를 갖는 구조로 밀결합 시스템(tightly-coupled system)과 소결합 시스템(loosely-coupled system)으로 분류한다.
④ MIMD : 여러 개의 프로세서들이 서로 다른 명령어와 데이터를 처리하는 진정한 의미의 병렬 프로세서이다.

12. 다음 표는 각 프로세스의 제출시간과 CPU 수행시간을 나타낸 것이다. HRN(Highest Response-ratio Next) 스케줄링 기법을 사용하였을 때, 우선순위가 가장 높은 프로세스는 무엇인가?

프로세스	제출시간	CPU 수행시간
P1	15	5
P2	8	4
P3	12	3
P4	10	2

① P1 ② P2 ③ P3 ④ P4

13. 다음 정수 리스트를 퀵 정렬 알고리즘으로 오름차순 정렬할 때, 리스트를 처음 분할한 직후 분할된 두 리스트의 상태로 가장 옳은 것은? (단, 제어키는 5로 한다.)

(5 2 6 4 7 3 8 1)

① (1 2 3 4), (6 7 8)
② (2 4 3 1), (6 7 8)
③ (3 1 2 4), (7 6 8)
④ (3 2 1 4), (7 8 6)

14. 다음 중 소프트웨어 프로토타이핑(Prototyping)에 대한 설명으로 가장 옳지 않은 것은?

① 개발자가 구축할 소프트웨어의 모델을 사전에 만드는 공정으로서 요구사항을 효과적으로 유도, 수집한다.
② 프로토타입은 기능적으로 제품의 하위 기능을 담당하는 작동 가능한 모형이다.
③ 프로토타이핑에 의해 만들어진 프로토타입은 폐기될 수 있고, 재사용될 수도 있다.
④ 적용사례가 많고, 가장 오래됐으며 널리 사용되는 방법으로 결과물이 명확하므로 가시성이 매우 좋다.

15. 다음 중 OSI(Open System Interconnection) 7계층에 대한 설명으로 가장 옳지 않은 것은?

① 물리계층에서는 기계적·전기적·기능적·절차적 특징을 다루어 물리적 매체를 전송한다.
② 수신 측에서 패킷을 수신하게 되면, 상위 계층에서 하위 계층 순으로 처리된다.
③ 전송계층에서는 종점 간의 에러복구와 흐름제어를 담당한다.
④ 세션계층에서는 서로 협력하는 응용프로그램(Applications)들에 대하여 연결을 설정, 유지, 종료한다.

16. 다음 중 HTML5의 특징에 대한 설명으로 가장 옳지 않은 것은?

① 쌍방향 통신을 제공하여 실시간 채팅이나 온라인 게임을 만들 수 있다.
② 스마트폰의 일반 응용프로그램도 HTML5를 사용해 개발할 수 있다.
③ 디바이스에 접근할 수 없어서 개인정보 보호 및 보안을 철저히 유지할 수 있다.
④ 플러그인의 도움 없이 음악과 동영상 재생이 가능하다.

17. 다음 <보기>의 UML 다이어그램 중 시스템의 구조(structure)보다는 주로 동작(behavior)을 가장 잘 묘사하는 다이어그램들만 고른 것은?

< 보 기 >

㉠ 클래스 다이어그램(Class Diagram)
㉡ 상태 다이어그램(State Diagram)
㉢ 시퀀스 다이어그램(Sequence Diagram)
㉣ 패키지 다이어그램(Package Diagram)
㉤ 배치 다이어그램(Deployment Diagram)

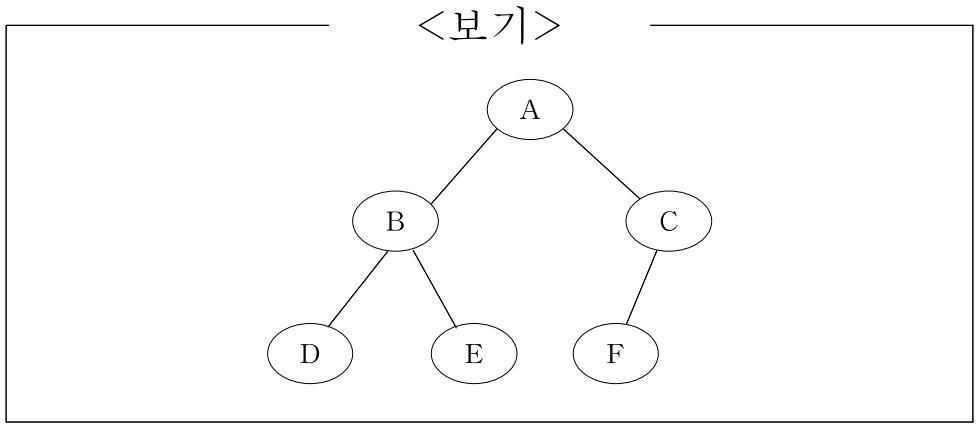
① ㉠, ㉣ ② ㉢, ㉣ ③ ㉡, ㉤ ④ ㉡, ㉢

18. 다음 중 파일 할당(File Allocation)에 대한 설명으로 가장 옳지 않은 것은?

① 파일에 대한 임의 접근(Random Access)은 연결 할당이 연속할당보다 성능이 우수하다.
② 연결 할당(Linked Allocation)은 파일에 할당된 모든 블록에 다음 블록의 위치를 나타내는 포인터가 포함된다.
③ 블록 단위의 색인 할당(Indexed Allocation)은 파일 내용을 저장하는 블록 외에 별도의 색인 블록(Index Block)이 필요하다.
④ 연속 할당(Contiguous Allocation)은 파일 생성 시 연속된 블록(Block)에 파일을 할당한다.

19. 다음 <보기>의 이진 트리의 내부 경로 길이(Length)와 외부 경로 길이(Length)로 가장 옳은 것은?

<보기>



① 5, 20 ② 5, 22 ③ 8, 20 ④ 8, 22

20. 다음 중 소프트웨어 테스트에 대한 설명으로 가장 옳지 않은 것은?

① 스트레스 테스트(Stress Test)는 비정상적으로 과도한 분량 또는 빈도로 자원을 요청할 때의 영향을 감사한다.
② 시스템 테스트(System Test)는 모듈들이 통합된 후 넓이 우선 방식 또는 깊이 우선 방식을 사용하여 테스트한다.
③ 단위 테스트(Unit Test)는 개별적인 모듈에 대한 테스트이며 테스트 드라이버(Test Driver)와 테스트 스텁(Test Stub)을 사용할 수 있다.
④ 인수 테스트(Acceptance Test)는 인수 전에 사용자의 요구사항이 만족되었는지 테스트한다.

네트워크보안

1. 다음 <보기>의 ㉠, ㉡, ㉢에 가장 적합한 것으로 짝지어진 것은?

< 보기 >

○ 이더넷은 네트워크 인터페이스 카드에 설정된 ㉠ 물리적 주소를 사용한다.
○ 네트워크 계층의 주소는 ㉡ 논리 주소를 사용한다.
○ 전송계층의 주소는 ㉢ 포트 주소를 사용한다.

① ㉠ 8Byte ㉡ 2Byte ㉢ 1Byte
② ㉠ 8Byte ㉡ 4Byte ㉢ 2Byte
③ ㉠ 6Byte ㉡ 2Byte ㉢ 1Byte
④ ㉠ 6Byte ㉡ 4Byte ㉢ 2Byte

2. 다음 <보기>는 라우터를 이용한 네트워크 보안 설정에 관련된 내용이다. 가장 옳은 내용을 모두 고르시오.

< 보기 >

㉠ egress 필터링은 라우터 내부에서 외부로 나가는 패킷의 소스 IP를 체크하여 필터링하는 것이다.
㉡ ingress 필터링은 standard 또는 extended access-list를 활용하여 라우터 내부로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것이다.
㉢ blackhole 필터링이란 인터페이스를 통해 들어오는 패킷의 소스 IP에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다.
㉣ unicast RPF는 access-list나 blackhole 필터링을 이용하여 일일이 IP나, IP대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

① ㉠, ㉡, ㉢ ② ㉠, ㉣
③ ㉠, ㉡, ㉣ ④ ㉠, ㉡, ㉢, ㉣

3. TCP는 흐름 제어를 다루기 위하여 슬라이딩 윈도우(Sliding Window)를 사용한다. 수신자 호스트 B는 8500 바이트의 버퍼를 갖고 있으며, 현재 버퍼에 3150 바이트의 처리되지 않은 데이터를 갖고 있다고 가정했을 때, 호스트 A를 위한 수신자 윈도우(rwnd) 값은?

① 3150
② 5350
③ 8500
④ 11650

4. 다음 중 DDoS(Distributed Denial of Service) 공격과 툴에 대한 설명으로 가장 옳지 않은 것은?

① Teardrop은 두 번째 패킷의 Fragment Offset을 위조하여, 첫 번째 패킷 다음에 두 번째 패킷을 추가하지 않고 첫 번째 패킷의 TCP 헤더와 데이터 부분을 덮어쓰게 한다.
② Trinoo는 UDP Flood 서비스 거부 공격에 사용되는 툴이다.
③ Ghost Call은 IP Scan 이후 프리픽스로 호를 시도하여, Digest 인증을 해킹하는 공격을 의미하는 것이 아니라, 단순한 INVITE를 보내는 패턴 공격이다.
④ NetBot Attacker는 발신지와 수신지 IP를 동일하게 설정하여 라우터 및 서버의 성능장애나 시스템 다운을 유발시킨다.

5. ICMP(Internet Control Message Protocol) 프로토콜은 문제를 해결하는 기능과 전달할 수 없는 패킷에 대한 에러 정보를 알리기 위해 사용된다. 아래 대표적인 ICMP 메시지의 기능을 설명한 것 중 가장 옳지 않은 것은?

① Echo Request 메시지는 원하는 호스트로의 IP 연결을 확인하기 위해 사용된다.
② Destination Unreachable은 라우터나 목적호스트에 의해 보내지며 데이터그램이 전달되지 못한다는 것을 데이터를 보낸 호스트에 알려준다.
③ Source Quench는 데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지이다.
④ Echo Reply는 데이터를 보내는 호스트에게 목적 IP 주소에 대한 좀 더 적합한 경로가 있음을 알리기 위해 라우터가 보내는 메시지이다.

6. 다음 TCP(Transport Control Protocol) 프로토콜의 타이머에 대한 설명 중 가장 옳지 않은 것은?

① RTO 값은 해당 시간까지 Acknowledge가 전송되어 오지 않는 경우, 재전송하기 위한 설정값이다.
② RTO 값은 초기 RTT값을 기준으로 항상 고정되어 있다.
③ RTO 시간이 너무 클 경우 수신측의 중복 ACK에 대한 손실 세그먼트를 재전송 하는 Fast retransmission 현상이 발생한다.
④ TCP 세그먼트가 유실되어, 해당 세그먼트를 요구하는 Acknowledge가 계속 도착하더라도 RTO 시간이 Time-out되어야 재전송이 가능하다.

7. 다음 <보기>는 TCP Session Hijacking의 공격 순서를 나열한 것이다. 순서가 가장 옳은 것은?

< 보기 >

㉠ 공격 목표를 정하고 공격 대상을 설정한다.
㉡ 시퀀스 넘버의 난이도 검사를 한다.
㉢ TCP/IP 스택 구현이나 원리를 예측하고, 이를 통하여 얻어진 데이터로부터 시퀀스 넘버를 추측한다.
㉣ 공격자가 세션을 설정하고자 하는 컴퓨터로부터 시퀀스 넘버의 추측이 끝나면 그 서버와 연결되어 있는 컴퓨터에게 DoS 공격 등을 통하여 사용자를 제거한다.
㉤ 공격 대상에 세션을 설정하여 현재 공격 목표와 연결되어있는 공격 대상의 세션을 설정한다.
㉥ 제거된 사용자로부터 추측한 시퀀스 넘버를 이용하여 Session Hijacking을 실시한다.

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

8. 다음 중 침입 방지 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 침입 방지 시스템의 검사영역은 네트워크 계층과 전송계층의 IP/Port 정보를 기반으로 동작한다.
② 침입 방지 시스템의 검사영역은 방화벽이 검사할 수 없는 전송계층 상단의 어플리케이션 계층의 데이터까지도 검사가 가능하다.
③ 침입 경고 이전에 상대의 공격을 중단시키는데 목적을 두고 있다.
④ 안티 바이러스와 같은 시그니처 기반의 기술과 방화벽과 같은 네트워크 차단기능이 결합된 방식을 침입 방지 시스템이라 한다.

9. 다음 중 무선 보안 강화 방안을 설명한 것 중 가장 옳지 않은 것은?

① SSID를 브로드캐스트 불가로 접속하면 누구도 접속할 수 없다.
② TKIP은 WEP을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다.
③ WEP는 RC4 스트림 암호화 기법을 사용하고 키 스트림을 정적 키를 사용한다.
④ IEEE 802.11i는 AES 암호화 기법을 사용한다.

10. 다음 중 가상사설망(VPN) 구현에 사용되는 터널링 프로토콜(Tunneling Protocol)로 가장 옳은 것은?

① PPTP, IPSEC, MPLS
② PPTP, L2TF, WAP
③ IPSEC, SET, SSL
④ L2TF, WAP, IPSEC

11. 다음 <보기>는 오용탐지(Misuse Detection)와 이상탐지(Anomaly Detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고른 것은?

< 보기 >

㉠ 통계적 분석방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다.
㉡ 미리 축적한 시그니처와 일치하면 침입으로 판단한다.
㉢ 제로데이 공격탐지에 적합하다.
㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

① ㉠, ㉢ ② ㉠, ㉣ ③ ㉡, ㉢ ④ ㉡, ㉣

12. 다음 중 가상 사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.
② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자인증의 보안 기능을 제공한다.
③ 네크워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.
④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

13. 다음 중 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명으로 가장 옳지 않은 것은?

① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원한다.
② 방화벽이나 게이트웨이 등에 구현한다.
③ IP 기반의 네트워크에서만 동작한다.
④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능하다.

14. 다음 <보기>에서 설명하는 보안 시스템은?

< 보기 >

○ 패킷을 버리거나 또는 의심이 가는 트래픽을 감지함으로써, 공격 트래픽을 방어하는 기능을 가지고 있다.
○ 모든 트래픽을 수신하는 스위치의 포트를 모니터하고, 특정 트래픽을 막기 위하여 적합한 명령어를 라우터(Router)나 침입차단시스템(Firewall)에 전송할 수 있다.
○ 호스트(Host) 기반의 이 보안 시스템은 공격을 감지하기 위하여 서명이나 비정상 감지기술을 사용한다.

① IDS ② IPS ③ DNS ④ VPN

15. 다음 중 네트워크 기반 공격기법에 대한 설명으로 가장 옳지 않은 것은?

① SYN Flooding 공격은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.
② Zero Day 공격은 시그니처(Signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.
③ APT 공격은 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.
④ Buffer Overflow 공격은 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

16. 다음 <보기>는 보안 공격 유형을 나열한 것이다. 소극적 공격을 모두 고른 것은?

< 보기 >

㉠ 신분위장(Masquerade)
㉡ 재전송(Replay)
㉢ 패킷 분석(Analysis of Packet)
㉣ 메시지 수정(Modification of Message)
㉤ 스니핑(Sniffing)
㉥ 서비스 거부(Denial of Service)

① ㉠, ㉢, ㉤ ② ㉠, ㉣
③ ㉢, ㉤ ④ ㉢, ㉣, ㉥

17. 다음 중 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보로 가장 옳은 것은?

① 수신 시스템이 처리할 수 있는 윈도우 크기
② 패킷을 송신하고 수신하는 프로세스의 포트 번호
③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
④ 송신 시스템의 TCP 패킷의 생성 시간

18. 다음 중 ACL 적용 규칙에 해당하지 않는 것으로 가장 옳은 것은?

① Named ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.
② ACL의 마지막에는 deny any가 생략되어 있다.
③ ACL은 먼저 입력한 순서대로 수행된다.
④ Numbered ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.

19. 다음 <보기>의 VPN에 대한 설명 중 가장 옳은 것을 모두 고른 것은?

< 보기 >

㉠ 터널링 기술은 VPN의 기본이 되는 기술로서 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 캡슐화하는 기술이다.
㉡ 데이터 암호화 기술은 터널이 형성된 한 쪽 호스트에서 데이터를 암호화해서 보내면 반대편 호스트에서 암호화 데이터를 복호화하여 원본 데이터를 확인하게 된다.
㉢ VPN은 데이터의 출처 즉, 출발지 IP가 확실한지에 대한 인증기술을 제공하고, 내부 자원에 대해서 허가 받지 않은 사용자의 접속을 차단하는 접근제어 기능을 제공한다.
㉣ VPN 구현에 가장 널리 사용되는 터널링 프로토콜에는 PPP, SSL, SSH 등이 있다.

① ㉠
② ㉠, ㉡
③ ㉠, ㉡, ㉢
④ ㉠, ㉡, ㉢, ㉣

20. 다음 중 무선랜 구축 시 보안을 위한 고려사항으로 가장 옳지 않은 것은?

① SSID(Service Set IDentifier)를 숨김모드로 사용
② 무선 단말기의 MAC(Media Access Control)주소 인증 수행
③ 관리자용 초기 ID/Password 변경
④ 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

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.