

2023년도 제2차 해양경찰청 채용시험 문제지

- 관 제 정 보 보 호 (9 급) -



성 명 :

응 시 번 호 :

응시자 유의사항 및 과목별 코드번호

※ 시험 과목 : 컴퓨터일반(23), 네트워크보안(24),

정보시스템보안(38)

※ 시험이 시작되기 전까지 표지를 넘기지 마시오.

해 양 경 찰 청

컴퓨터일반

1. 다음 <보기>의 설명과 가장 관계있는 것은?

< 보 기 >

폰 노이만(Von Neumann)이 1945년에 “모든 프로그램과 데이터를 주기억장치에 저장한 다음, 이를 중앙처리장치가 명령에 따라 자동으로 실행하는 방식”을 제안하였다. 이는 오늘날의 모든 컴퓨터구조의 기본사상이 된 중요한 개념이 되었다.

- ① 프로그램 내장방식(Stored Programming) 컴퓨터
- ② 데이터 내장방식(Stored Data) 컴퓨터
- ③ 중앙처리장치 중심(Central Processing Unit Oriented) 컴퓨터
- ④ 중앙제어장치 중심(Control Unit Oriented) 컴퓨터

2. 다음 <보기>와 같이 이진수로 A와 B 값이 주어졌을 때, A XOR B = ?

< 보 기 >

A = 1011 1000, B = 1100 0000

- ① 1111 1000
- ② 1000 0000
- ③ 0111 1000
- ④ 0111 1111

3. 다음 중 컴퓨터 중앙처리장치와 기억장치 간의 통신을 위해 설치한 시스템 버스가 아닌 것은?

- ① 가속 버스 ② 데이터 버스
- ③ 주소 버스 ④ 제어 버스

4. 다음 중 CPU내 레지스터가 아닌 것은?

- ① MBR(Memory Buffer Register)
- ② MAR(Memory Address Register)
- ③ IR(Instruction Register)
- ④ DR(Disk Register)

5. 다음은 TCP/IP인터넷 프로토콜에서 사용되는 주소들이다. 거리가 가장 먼 것은?

- ① 포트(Port) 주소
- ② IP(Internet Protocol) 주소
- ③ MAC(Media Access Control) 주소
- ④ 상대(Relative) 주소

6. 다음 <보기>의 설명과 가장 가까운 RAID(Redundant Array of Independent Disks) 레벨은 무엇인가?

< 보 기 >

- 거울(Mirroring) 디스크라고 한다.
- 디스크 오류 시 실시간 데이터 복구가 가능하다.
- RAID 중 가장 구축 비용이 많이 든다.

- ① RAID 레벨 5 ② RAID 레벨 3
- ③ RAID 레벨 1 ④ RAID 레벨 0

7. 다음 <보기>의 설명과 가장 관계가 깊은 것은?

< 보 기 >

- 컴퓨터를 구성하는 장치 간의 속도의 차이 때문에 그대로 운영하면 저속의 장치에 성능이 종속되게 된다.
- 이러한 현상이 CPU와 주기억장치 사이에서도 발생한다. 즉, 주기억장치의 읽기/쓰기 속도가 CPU의 명령어 처리속도보다 현저히 느리기 때문에 고가의 초 고성능의 CPU를 사용해도 성능은 속도가 느린 주기억장치 읽기/쓰기 속도에 종속된다.
- 이러한 문제해결을 위해 두 장치 사이에 CPU 명령어 처리속도와 유사한 속도의 메모리를 장착하여 CPU가 이로부터 명령어나 데이터를 처리 하도록 하여 CPU 명령어 처리성능을 향상시켰다.

- ① 메모리 버퍼
- ② SSD(Solid State Disk) 버퍼
- ③ 캐시(Cache) 메모리
- ④ PC(Program Counter) 메모리

8. 다음 중 TCP/IP인터넷 프로토콜에서 흐름제어 및 오류제어 등을 통해서 종단간(End to End)에 신뢰할 수 있는 통신기능을 제공하는 계층은?

- ① 응용(Application) 계층
- ② 네트워크(Network) 계층
- ③ 전송(Transport) 계층
- ④ 데이터 링크(Link) 계층

9. 다음 중 TCP/UDP 포트(Port)를 기반으로 사용자의 요구를 여러 대의 서버로 부하를 분산하는 기능을 하는 스위치 장비는?

- ① L1 스위치 ② L2 스위치
- ③ L3 스위치 ④ L4 스위치

10. 다음 <보기>에서 설명하는 기술을 운영체제에서 무슨 기술이라 하는가?

< 보 기 >

- 다중프로그래밍 OS 환경에서 사용자들이 실행을 요구한 프로세스들을 직접 주기억장치에 적재전략을 사용하면 주기억장치에 적재공간이 없을 경우 사용자가 요청한 프로세스들은 적재공간이 확보될 때까지 중지상태(Pending)가 된다. 이의 해결을 위해 직접 주기억장치에 적재하지 않고 특정한 디스크 영역에 적재시킨 다음, 주기억장치에 적재할 여유 공간이 있을 때 이로부터 적재하는 간접적재 방법을 사용한다.
- 또한, 주기억장치에서 실행 중인 특정 프로세스가 출력을 할 때 프린터에 직접하면 이 프로세스가 끝날 때까지 다른 프로세스가 그 프린터에 출력을 할 수 없게 되어 그 프로세스는 중지상태(Pending)가 된다. 이의 해결을 위해 프린터에 직접 프린트하지 않고 특정한 디스크 영역에 출력을 한 다음, 그곳에 출력이 완료된 출력물에 대해서만 연속적으로 프린터에 출력하도록 하여 문제점을 해결한다.

- ① SPOOL(Simultaneous Peripheral Operation OnLine) 기술
- ② 세마포아(Semaphore) 기술
- ③ 다중쓰레드(Multi Thread) 기술
- ④ 가상메모리(Virtual Memory) 기술

11. 다음은 파일시스템과 데이터베이스시스템을 설명한 것이다. 틀린 설명은?

- ① 데이터베이스시스템에서는 데이터의 구조가 변경되어도 변경항목과 관련이 없는 프로그램들은 변경할 필요가 없다.
- ② 데이터베이스시스템에서는 전체적인 개념적 스키마에서 프로그래머에게 필요한 논리스키마(혹은 서브스키마)만을 제공하기 때문에 보안이 강화된다.
- ③ 파일시스템은 파일을 구성하는 레코드(Record)에 필드가 추가되거나 삭제되면 이 파일을 사용하는 모든 프로그램이 이를 반영하여 변경되어야 한다.
- ④ 파일시스템은 파일단위로 임계구역(Critical Region)이 설정되기 때문에 파일의 동시공유(Concurrent Sharing) 및 다중접근(Multi Access)이 용이하다.

12. 다음 중 스래싱(Thrashing)에 대한 설명으로 가장 옳은 것은?

- ① 두 개 이상의 작업이 서로 상대방의 작업이 끝나기만을 기다리고 있기 때문에 결과적으로 아무것도 완료되지 못하는 현상을 의미한다.
- ② CPU 버스트가 짧은 프로세스에게 우선순위를 항상 부여한다면, 상대적으로 CPU 버스트가 긴 프로세스가 계속해서 지연되는 것을 의미한다.
- ③ CPU가 프로그램을 실행하고 있을 때 입출력 하드웨어 등의 장치나 예외 상황이 발생하여 처리가 필요한 경우 CPU에게 알려 처리할 수 있도록 하는 것을 의미한다.
- ④ 페이지 부재가 너무 자주 일어나 프로세스 실행에 보내는 시간보다 페이지 교체에 더 많은 시간을 소비하는 현상을 의미한다.

13. 다음 <보기>는 학생이라는 개체의 속성을 나타내고 있다. 데이터베이스 구축시 “성명”을 기본키로 사용하기 곤란한 이유로 가장 타당한 것은?

< 보 기 >

학생(성명, 학번, 전공, 주소, 우편번호)

- ① 동일한 성명을 가진 학생이 두 명 이상 존재할 수 있다.
- ② 성명은 기억하기 어렵다.
- ③ 성명을 정렬하는데 많은 시간이 소요된다.
- ④ 성명은 기억 공간을 많이 필요로 한다.

14. 다음 중 소프트웨어 생명주기 모형 중 Boehm이 제시한 고전적 생명주기 모형으로서 선형 순차적 모델이라고 하며, 타당성 검토, 계획 요구사항 분석, 설계, 구현, 테스트, 유지보수의 단계를 통해 소프트웨어를 개발하는 모형은?

- ① 폭포수 모형
- ② 프로토타입 모형
- ③ 나선형 모형
- ④ RAD 모형

15. 다음 중 데이터베이스시스템에서 사용하는 데이터 언어가 아닌 것은?

- ① DDL(Data Description Language)
- ② DHL(Data Host Language)
- ③ DML(Data Manipulation Language)
- ④ DCL(Data Control Language)

16. 다음 <보기> 중 주문 테이블에서 결과 테이블을 나타내는 가장 적절한 SQL 구문은?

< 보 기 >

[주문 테이블]

주문번호	주문고객	주문제품	수량
A001	apple	P03	10
A002	melon	P01	5
A003	banana	P06	45
A004	carrot	P04	5
A005	apple	P03	35
A006	melon	P06	25
A007	banana	P06	20

[결과 테이블]

주문고객	주문제품	수량
apple	P03	35
apple	P03	10
carrot	P04	10
banana	P06	45
melon	P06	25
banana	P06	20

- ① SELECT 주문고객, 주문제품, 수량 FROM 주문 WHERE 수량 >= 10 ORDER BY 주문제품 ASC, 수량 DESC ;
- ② SELECT 주문고객, 주문제품, 수량 FROM 주문 WHERE 수량 > 10 ORDER BY 주문제품 DESC, 수량 ASC ;
- ③ SELECT 주문고객, 주문제품, 수량 FROM 주문 WHERE 수량 <= 10 ORDER BY 주문제품 DESC, 수량 ASC ;
- ④ SELECT 주문번호, 주문제품, 수량 FROM 주문 WHERE 수량 >= 10 ORDER BY 주문제품 ASC, 수량 DESC ;

17. 다음 중 일반적인 이동 통신 서비스보다 훨씬 작은 지역을 커버하는 초소형 기지국으로써 기존의 인터넷을 통해서 핵심망(코어망)과 접속되며, 전파가 닿기 힘든 실내 혹은 지하 공간에 설치해 이동통신 서비스를 제공하는 기술은?

- ① 블루투스(Bluetooth)
- ② 펌토셀(Femto Cell)
- ③ 빔 포밍(Beam Forming)
- ④ 와이파이(Wi-Fi)

18. 다음 <보기> 중 각 설명과 일치하는 데이터 구조로 가장 바르게 짝지어진 것은?

< 보 기 >

- ㉠ 먼저 추가된 항목이 먼저 제거된다.
- ㉡ 먼저 추가된 항목이 나중에 제거된다.
- ㉢ 항목이 추가된 순서에 상관없이 제거된다.

- | | | | |
|---|----|-------|-------|
| | ㉠ | ㉡ | ㉢ |
| ① | 큐 | 연결리스트 | 스택 |
| ② | 스택 | 연결리스트 | 큐 |
| ③ | 큐 | 스택 | 연결리스트 |
| ④ | 스택 | 큐 | 연결리스트 |

19. 다음 <보기>에서 설명하는 것은?

< 보 기 >

- 인터넷이나 네트워크 상에서 일정정도 이하의 지연시간이나 데이터 손실률 등의 보장을 일컫는 말이다.
- 데이터를 목적지까지 빠르게, 일정한 속도로, 신뢰성 있게 보내기 위해 대역폭, 우선순위 등 네트워크 자원을 할당해 주어진 네트워크 자원에 각종 응용프로그램의 송신 수요를 지능적으로 맞춰주는 여러 가지 기술을 총칭하는 용어이다.

- ① NTP
- ② QoS
- ③ RADIUS
- ④ SMTP

20. 다음 <보기>에서 설명하는 것은?

< 보 기 >

패킷 교환망인 인터넷을 이용하여 음성정보를 전달하는 전화 관련 기술로서 저렴한 전화서비스를 구현하는데 사용된다. 관련 표준 프로토콜로 ITU H.323과 IETF SIP(Session Initiation Protocol)가 있고, 게이트웨이를 이용하여 공중전화망(PSTN)과 연결할 수 있다.

- ① IPTV
- ② VoIP
- ③ IPv6
- ④ IPSec

네트워크보안

- 다음 중 무선 AP(Access Point)에 전송데이터의 암호화 방식이나 인증절차가 설정되지 않은 경우 보안 강화책이 아닌 것은?
 - WEP(Wired Equivalent Privacy) 설정한다.
 - WAP2(Wi-Fi Protected Access v2) 설정한다.
 - Rogue AP로 대체한다.
 - 무선 AP에 SSID값을 'NULL'로 설정한다.
- 다음 중 무선 LAN보안에 AES 128비트를 사용하여 최상의 암호수준을 제공하는 것은?
 - WEP(Wired Equivalent Privacy)
 - EAP(Extensible Authentication Protocol)
 - WPA2(Wi-Fi Protected Access v2)
 - WPA(Wi-Fi Protected Access)
- 다음 중 기기 인증기술 중에서 보안수준은 하위수준이지만, 접속이 가장 용이하고, 추가적인 프로토콜이 필요치 않고, 접속지연이 최소인 것은?
 - ID/PW기반 인증기술
 - MAC(Media Access Control)주소 인증기술
 - Challenge/Response 인증기술
 - PKI(Public Key Infrastructure)기반 기기 인증서를 활용한 인증기술
- 다음은 무선 AP(Access Point)가 태생적으로 보안에 취약하기 때문에 신규로 설치 시 고려할 사항을 나열한 것이다. 틀린 것은?
 - AP 기본계정의 패스워드를 재설정한다.
 - 누구나 접근이 가능한 장소에 설치한다.
 - DHCP(Dynamic Host Configuration Protocol)에 의한 IP주소 할당을 중지한다.
 - AP에 접속이 가능한 무선 랜카드 MAC주소를 기록하여 이를 반영하여 접속을 통제한다.
- 다음 중 응용계층에서 동작되는 보안프로토콜이 아닌 것은?
 - S/MIME(Secure/Multipurpose Internet Mail Extensions)
 - SSH(Secure SHell)
 - SSL(Secure Socket Layer)
 - S-HTTP(Secure Hyper Text Transper Protocol)

- VPN(Virtual Private Network)은 인터넷에 보안채널(Secure Channel)을 만들어 공용인터넷을 사설망처럼 사용하는 기술이다. 통신프로토콜 3계층(네트워크계층)에 보안프로토콜을 추가하여 VPN을 구현하는 기술은?
 - IPSec(Internet Protocol Security)
 - SSL(Secure Socket Layer)
 - DNSsec(DNS Security)
 - S-HTTP(Secure Hyper Text Transper Protocol)
- 다음 중 산재되어 있는 수많은 컴퓨터를 동원하여 동일 시간에 특정 컴퓨터에 트래픽 폭탄을 보내어 특정 컴퓨터가 정상적인 작동을 못하게 하는 공격은?
 - APT(Advanced Persistence Threat) 공격
 - DOS(Denial Of Service) 공격
 - IP Spoofing 공격
 - DDOS(Distributed Denial Of Service) 공격
- 다음 <보기>의 설명과 가장 가까운 장비는?

— < 보 기 > —

방화벽과 침입탐지시스템의 장점만을 결합하여 실시간 방어체제를 구축한 장비이다. 이 장비는 실시간으로 네트워크 트래픽을 모니터링하여 분석하고 해킹으로 판단되면 패킷이 내부로 유입되는 것을 사전에 차단한다.

- DDOS(Distributed Denial Of Services) 보안장비
 - VPN(Virtual Private Network) 보안장비
 - IPS(Intrusion Prevention System) 보안장비
 - NAC(Network Access Control) 보안장비
- 다음 중 방화벽으로 할 수 있는 것은?
 - 악성코드 침입 차단
 - 내부자 공격 차단
 - 방화벽을 우회하는 트래픽 차단
 - 외부자의 내부 네트워크에 대한 접근통제
 - 다음 중 공격 대상시스템의 로그에 흔적을 남기지 않은 포트 스캔 기술은?
 - ICMP Scan
 - UDP Scan
 - TCP Scan
 - Stealth Scan

11. 다음 중 공격자가 공격대상자에게 자신을 노출시키지 않고 제3의 사용자인 것처럼 MAC주소, IP주소, E-Mail 주소, DNS 이름 등을 속여서 공격하는 것을 통칭하여 무엇이라 하는가?

- ① 스니핑(Sniffing) 공격
- ② 스푸핑(Spoofing) 공격
- ③ 하이재킹(Hijacking) 공격
- ④ 인터셉트(Intercept) 공격

12. 다음 중 조직내 다수의 IT시스템과 보안시스템에서 발생하는 모든 로그들을 실시간으로 수집하여 종합적인 분석을 통해 이상징후를 파악하고 대응을 위해 마련한 장비는?

- ① SIEM(Security Information Event Management) 장비
- ② NAC(Network Access Control) 장비
- ③ MDM(Mobile Device Management) 장비
- ④ SAC(System Access Control) 장비

13. 리눅스 운영체제가 탑재된 컴퓨터에 랜카드를 설치한 다음, 리눅스운영체제를 통해서 랜카드를 'Promiscuous' 모드로 동작하도록 설정하였다. 설정 결과 랜카드 동작을 가장 잘 설명한 것은?

- ① 랜카드에 도착된 프레임내의 IP주소와 MAC주소가 랜카드가 장착된 컴퓨터의 IP주소와 MAC주소가 동일한 것만 컴퓨터로 받아들인다.
- ② 랜카드에 도착된 프레임내의 IP주소와 랜카드가 장착된 컴퓨터의 IP주소가 동일한 것만 컴퓨터로 받아들인다.
- ③ 랜카드에 도착된 프레임내의 MAC주소와 랜카드가 장착된 컴퓨터의 MAC주소가 동일한 것만 컴퓨터로 받아들인다.
- ④ 랜카드에 도착한 모든 프레임을 컴퓨터로 받아들인다.

14. 다음 중 사실 네트워크 용도로 사용되는 사실 IPv4 주소에 해당하는 것은?

- ① 10.10.20.300
- ② 168.10.40.11
- ③ 172.16.10.20
- ④ 192.10.20.30

15. 다음 중 조직내 네트워크에 기기/사용자 인증절차를 통해 네트워크에 접근을 통제하고, 네트워크에 접속되는 기기들의 백신관리 및 패치관리, 자산관리를 점검을 통해 무결성 유무에 따라 네트워크 접속 허용유무를 결정하고, 해킹, 웹 유해트래픽 탐지 및 차단하는 등의 기능을 하는 네트워크 보안장비는?

- ① SAC(System Access Control) 장비
- ② AAC(Account Access Control) 장비
- ③ NAC(Network Access Control) 장비
- ④ ESM(Enterprise Security Management) 장비

16. 다음 중 이더넷 물리 주소(MAC)가 될 수 있는 것은?

- ① 00:0C:29:97:13:8C:48:A0
- ② 00:0C:29:97:13:8C:48
- ③ 00:0C:29:97:13:8C
- ④ 00:0C:29:97:13

17. 다음 중 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격 기법은?

- ① 스위치 재밍
- ② IP 스푸핑
- ③ DNS 스푸핑
- ④ ARP 스푸핑

18. 다음 <보기>의 내용은 DDoS 공격 직후가 발생하였을 경우 긴급 대응 절차를 나열한 것이다. 순서를 올바르게 나열하고 있는 것은?

< 보 기 >

ㄱ. 모니터링
 ㄴ. 상세분석
 ㄷ. 공격탐지
 ㄹ. 초동조치
 ㅁ. 차단조치

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

19. 다음 중 침입차단시스템(Firewall)에서 아래와 같이 주소에 의한 패킷 필터링 규칙을 적용 시 필터링 된 패킷의 결과가 가장 옳바르지 않은 것은?
(단, 적용순서는 A, B, C 순)

규칙	출발지주소	목적지 주소	동작
A	10.12.99.0/24	165.15.0.0/16	Deny
B	10.12.0.0/8	165.15.6.0/24	Allow
C	any	any	Deny

- ① 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.
- ② 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.
- ③ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.
- ④ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.

20. 다음 중 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로 TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?

- ① Ping
- ② netstat
- ③ nmap
- ④ nbstat

정보시스템보안

- 다음은 정보시스템에 대해 가용성(Availability)과 보안수준(Security Level)간의 관계를 설명한 것이다. 가장 적합한 설명은?
 - ① 보안수준과 가용성간에는 아무런 관련이 없다.
 - ② 보안수준을 높이면 가용성이 낮아진다.
 - ③ 보안수준을 높이면 가용성도 높아진다.
 - ④ 보안수준을 낮추면 가용성도 낮아진다.
- 다음 중 조직내의 정보시스템을 안전하게 보호를 위해 마련해야 할 보호대책이 아닌 것은?
 - ① 관리적 보호대책
 - ② 기술적 보호대책
 - ③ 소프트웨어공학적 보호대책
 - ④ 물리적 보호대책
- 다음 중 정보시스템에 대한 가장 대표적인 가용성(Availability) 공격은?
 - ① 스니핑(Sniffing) 공격
 - ② 변조(Modification) 공격
 - ③ 위장(Masquerading) 공격
 - ④ 분산서비스거부(Distributed Denial of Service) 공격
- 다음 중 정보시스템 관리자를 속이거나 협박하여 정보시스템에 침입해서 불법적인 행위를 하는 공격은?
 - ① 사회공학공격(Social Engineering Attack)
 - ② 소프트웨어 공학적공격(SW Enginnering Attack)
 - ③ 중간공격자 공격(Man In The Middle Attack)
 - ④ 다중수준 보안공격(Multi Level Security Attack)
- 다음 중 현재 시행중인 보안 관련 인증제와 가장 관계가 먼 것은?
 - ① CC(Common Criteria) 인증제
 - ② GS(Good SW)품질 인증제
 - ③ KCMVP(Korea Cryptographic Module Verification Program) 인증제
 - ④ ISMS(Information Security Management System) 인증제

- 다음 중 하이브리드 암호시스템(Hybrid Cryptography System)에서 대칭키 암호알고리즘을 사용하는 가장 큰 이유는?
 - ① 안전한 대칭키 분배용으로 활용
 - ② 대량의 데이터에 대해 고속 암호화에 활용
 - ③ 생성된 일회용 세션키 암호화에 활용
 - ④ 고속의 공개키 암호시스템 보조용으로 활용
- 다음 <보기> 설명에서 ㉠, ㉡, ㉢에 들어갈 용어를 순서대로 나열한 것은?

— < 보기 > —

저작물의 원본을 왜곡하지 않는 범위 내에서 저작권 정보를 삽입하는 기술을 (㉠)이라 하고, 디지털 콘텐츠를 판매할 때 구매자 정보를 삽입하여 불법 배포가 이루어질 경우 최초의 구매자를 추적하는 기술을 (㉡)이라 한다. 또한 디지털콘텐츠의 지적재산권이 안전하게 보호되도록 창작에서 소비까지 전 과정이 적법하게 이루어지도록 하는 기술을 (㉢)이라 한다.

- ① DRM(Digital Right Management), 워터마킹(Watermarking), 핑거프린팅(Fingerprinting)
 - ② 핑거프린팅(Fingerprinting), DRM(Digital Right Management), 워터마킹(Watermarking)
 - ③ 워터마킹(Watermarking), 핑거프린팅(Fingerprinting), DRM(Digital Right Management)
 - ④ DRM(Digital Right Management), 핑거프린팅(Fingerprinting), 워터마킹(Watermarking)
- 다음 중 대칭키 암호알고리즘과 가장 관련이 없는 것은?
 - ① RSA(Rivest Shamir Adleman)
 - ② ARIA(Academy Research Institute Agency)
 - ③ SPN(Substitution Permutation Network)
 - ④ AES(Advanced Encryption Standard)
 - 다음 중 대칭키 분배 방법 중에서 중간자공격(Man in The Middle Attack)에 가장 취약한 것은?
 - ① 대칭키를 사전에 공유법
 - ② Diffie-Hellman 키 분배 알고리즘에 의한 분배
 - ③ 키 분배센터(KDC, Key Distribution Cenetr)에 의한 분배
 - ④ PKI(Public Key Infrastructure)기반의 공개키 암호 시스템을 활용한 분배

10. A가 B에게 공개키 암호시스템을 이용하여 메시지를 암호화하여 보내고 싶다. A는 어떻게 암호화해야 하는가?

- ① A의 공개키로 메시지를 암호화하여 B에게 보낸다.
- ② A의 개인키로 메시지를 암호화하여 B에게 보낸다.
- ③ B의 공개키로 메시지를 암호화하여 B에게 보낸다.
- ④ B의 개인키로 메시지를 암호화하여 B에게 보낸다.

11. 다음 중 재전송 공격(Replay Attack)의 방어법이 아닌 것은?

- ① 초기벡터(IV, Initial Vector) 사용
- ② 타임스탬프(Timestamp) 사용
- ③ 비표(Nonce) 사용
- ④ 순서번호(Sequence Number) 사용

12. 한번의 시스템 인증을 통해 재인증 절차 없이 정보 시스템들에 대해 접근할 수 있는 통합 로그인 제품은?

- ① SSO(Single Sign On)
- ② SAC(Server Access Control)
- ③ RBAC(Role Base Access Control)
- ④ TSO(Trust Sign On)

13. 다음 중 컴퓨터에 침투하여 주요 파일을 암호화하고 컴퓨터 사용자에게 암호화된 파일의 복호화 키를 알려준다는 조건으로 금전 등을 요구하는 악성코드는?

- ① 웜(Worm)
- ② 매크로 바이러스(Macro Virus)
- ③ 랜섬웨어(Ransomware)
- ④ 트로이목마(Trojan Horse)

14. 다음 중 PKI에 관한 설명 중 가장 옳지 않은 것은?

- ① PKI란 Public Key Infrastructure의 약어로 공개키 암호 알고리즘을 적용하고 인증서를 관리하기 위한 기반시스템이다.
- ② 주로 X.509 인증서를 사용하고 있다.
- ③ 인증서를 발급하는 역할을 하는 기관을 RA라 한다.
- ④ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

15. 다음 중 시스템 설계자가 서비스 기술자와 유지보수 기술자를 위하여 특정 컴퓨터에 접근을 편리하게 할 수 있도록 고의적으로 만든 악성코드는?

- ① 애드웨어(Adware)
- ② 백도어(Backdoor)
- ③ 매크로 바이러스(Macro Virus)
- ④ 웜(Worm)

16. 다음 중 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 무작위 문자열을 추가한다. 이렇게 추가되는 문자열을 무엇이라 하는가?

- ① Nonce
- ② Plaintext
- ③ Salt
- ④ Cipher

17. 국가안전보장에 중대한 영향을 미치는 주요정보통신 기반시설에 대한 보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려될 수 있으므로 기반시설을 지정하여야 한다. 다음 중 주요정보통신 기반시설이 아닌 것은 무엇인가?

- ① 전력, 가스, 석유 등 에너지·수자원 시설
- ② 인터넷포털, 전자상거래 등 인터넷시설
- ③ 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설
- ④ 방송중계, 국가지도통신망 시설

18. 다음 보기에서 설명하는 유닉스 시스템 명령어는?

— < 보 기 > —

시스템의 파일 또는 디렉토리(Directory)가 만들어질 때의 허가권(Permission)의 기본값을 정하기 위해서 사용한다. 해당 설정값은 모든 계정 사용자들에게 존재하는 값으로써 각 계정 사용자들이 생성하는 파일 또는 디렉토리(Directory)의 허가권(Permission)을 결정하기 위한 값이다.

- ① chmod
- ② umask
- ③ chown
- ④ touch

19. 다음 중 지능형 지속 위협(APT, Advanced Persistent Threat)에 대한 설명으로 가장 옳은 것은?

- ① 공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.
- ② 다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.
- ③ 시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.
- ④ 하나의 타겟에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

20. 다음 중 「개인정보보호법」 제25조에 따라 공개된 장소에서의 영상정보처리기기 설치가 예외적으로 허용되는 경우가 아닌 것은?

- ① 법령에서 구체적으로 허용하고 있는 경우
- ② 범죄의 예방 및 수사를 위하여 필요한 경우
- ③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
- ④ 통계작성·과학적 연구·공익적 기록보존 등을 위하여 필요한 경우