

2017년도 일반직공무원 채용시험 문제지

- 정 보 보 호 -



성 명 :

응 시 번 호 :

응시자 유의사항

※ 시험이 시작되기 전까지 표지를 넘기지 마시오.

해 양 경 비 안 전 본 부

컴퓨터 일반

1. IPv6(Internet Protocol version 6)에 관한 설명으로 가장 적절하지 않은 것은?

- ① 16bit씩 8부분, 총 128bit로 구성된다.
- ② 각 부분은 세미콜론(;)으로 구분되며, 16진수로 표현한다.
- ③ IPv4에 있던 헤더 체크섬(checksum) 필드가 라우터의 처리 시간 감소를 위해서 제거되었다.
- ④ 기본 헤더 길이가 40byte로 고정되고, 확장 헤더는 추가적인 전송 기능이 필요할 때 사용된다.

2. 다음 중 디지털 콘텐츠의 제작 및 유통, 보안 등의 모든 과정을 관리할 수 있게 하는 기술 표준을 제시한 MPEG의 종류로 옳은 것은?

- ① MPEG-2
- ② MPEG-4
- ③ MPEG-7
- ④ MPEG-21

3. 다음 중 데이터 조작어(DML)에 해당하는 SQL 문은 무엇인가?

- ① COMMIT
- ② SELECT
- ③ DROP
- ④ CREATE

4. 객체 지향 소프트웨어 공학의 개념 중 상이한 클래스들이 동일한 메소드(Method)명을 이용할 수 있도록 하는 것은 무엇인가?

- ① 캡슐화(Encapsulation)
- ② 공용 인터페이스(Public Interface)
- ③ 상속(Inheritance)
- ④ 다형성(Polymorphism)

5. 분산처리시스템(Distributed Processing System)을 사용하는 데 있어 이점이라 할 수 없는 것은?

- ① 자원 공유
- ② 보안 강화
- ③ 확장성 용이
- ④ 연산속도 향상

6. 중위식(Infix)으로 표현된 다음의 연산식에 대한 전위식(Prefix) 표현은?

$$A = B * (C + D) - E$$

- ① $=A-*B+CDE$
- ② $=A-+*BCDE$
- ③ $ABCDE=*+-$
- ④ $ABCD+*E-=$

7. 데크(Deque)에 대한 옳은 설명으로만 짝지어진 것은?

가. 양끝에서 노드의 삽입과 삭제가 가능하다.
나. 하나의 포인터를 사용한다.
다. 선형구조이다.
라. 입력이 한쪽에서만 가능한 입력제한 데크를 Shelf라고 한다.

- ① 가, 나
- ② 가, 다
- ③ 나, 라
- ④ 다, 라

8. <보기>는 모듈화를 중심으로 한 소프트웨어 설계 방법에 대한 설명이다. 빈칸의 내용을 가장 올바르게 나열한 것은?

- <보기> —
- 결합도(coupling)와 응집도(cohesion)는 모듈의 (㉠)을 판단하는 기준이다.
 - 결합도란 모듈 (㉡)의 관련성을 의미하며, 응집도란 모듈 (㉢)의 관련성을 의미한다.
 - 좋은 설계를 위해서는 결합도는 (㉣), 응집도는 (㉤) 방향으로 설계해야 한다.

- | | ㉠ | ㉡ | ㉢ | ㉣ | ㉤ |
|-------|----|----|----|----|---|
| ① 독립성 | 사이 | 내부 | 작게 | 큰 | |
| ② 독립성 | 내부 | 사이 | 크게 | 작은 | |
| ③ 추상성 | 사이 | 내부 | 작게 | 큰 | |
| ④ 추상성 | 내부 | 사이 | 크게 | 작은 | |

9. 다음 중 값이 다른 하나는?

- ① 16진수 : FF
- ② 10진수 : 256
- ③ 8진수 : 377
- ④ 2진수 : 11111111

10. Unix 명령(\$ ls -l)의 실행 결과에 대한 설명으로 가장 옳은 것은?

```
-rwxr--r-- aaa bbb 98 Aug 7 19:16 ccc
```

- ① 파일 aaa에 대한 소유자는 bbb이다.
- ② 파일 bbb에 대한 소유자는 aaa이다.
- ③ 파일 ccc에 대한 소유자는 aaa이다.
- ④ 파일 aaa에 대한 소유자는 ccc이다.

11. 다음은 OSI 7계층 중 어떤 계층을 설명한 것인가?

- 정보의 순차적 전송을 위한 프레임 번호 부여
- 연속적인 프레임 전송 시 수신 여부의 확인
- 정보 전송 시 컴퓨터에서 처리가 용이하도록 프레임 단위로 전송

- ① 세션 계층(Session Layer)
- ② 데이터 링크 계층(Data Link Layer)
- ③ 네트워크 계층(Network Layer)
- ④ 트랜스포트 계층(Transport Layer)

12. 다음 C언어로 작성된 함수의 매개변수 값으로 5를 주었을 때 반환되는 값은?

```
int f(int n){
    if(n==1) return 1;
    else return (n + f(n-1));
}
```

- ① 14
- ② 11
- ③ 15
- ④ 21

13. 다음은 페이지(Page) 교체 정책에 대한 설명이다. 해당하는 교체 정책과 가장 옳게 연결된 것은?

- ① LRU : 가장 먼저 주기억장치에 들어온 페이지를 교체한다.
- ② LFU : 최근에 사용되지 않은 페이지를 교체한다.
- ③ NUR : 각 페이지 당 2개의 하드웨어 비트(참조 비트와 변형 비트)가 필요하다.
- ④ FIFO : 페이지 당 참조 횟수에 대한 계수기를 가지며 그 값이 가장 작은 페이지가 교체된다.

14. 마이크로프로세서는 명령어의 구성방식에 따라 CISC와 RISC로 구분된다. 두 방식의 일반적인 비교 설명으로 옳은 것은 모두 몇 개인가?

- 가. RISC 방식은 CISC 방식보다 처리속도의 향상을 도모할 수 있다.
- 나. CISC 방식의 프로세서는 RISC 방식의 프로세서보다 전력 소모가 적은 편이다.
- 다. RISC 방식의 프로세서는 CISC 방식의 프로세서보다 내부구조가 단순하다.
- 라. CISC 방식은 RISC 방식보다 단순하고 축약된 형태의 명령어를 갖고 있다.

- ① 1개
- ② 2개
- ③ 3개
- ④ 4개

15. 다음 지문은 Windows의 실행 창에 입력할 수 있는 명령어들을 나열한 것이다. 명령어별 수행할 수 있는 기능을 순서대로 나열한 것은?

```
dxdiag - msconfig - regedit - mstsc
```

- ① 컴퓨터 사양 확인 - 시작 프로그램 편집 - 레지스트리 편집 - 원격 데스크톱 실행
- ② 원격 데스크톱 실행 - 작업관리자 편집 - 레지스트리 편집 - 시스템 셋다운 설정
- ③ 컴퓨터 사양 확인 - 작업관리자 편집 - 레지스트리 편집 - 원격 데스크톱 실행
- ④ 원격 데스크톱 실행 - 시작 프로그램 편집 - 레지스트리 편집 - 시스템 셋다운 설정

16. 데이터베이스 관리 시스템(DataBase Management System)에 대한 설명으로 가장 옳지 않은 것은?

- ① 응용프로그램에 대한 데이터의 독립성이 보장된다.
- ② 데이터가 중복 저장되는 것을 방지하여 데이터의 일관성을 유지한다.
- ③ 데이터베이스의 구성과 저장, 접근 방법, 유지 및 관리를 위한 시스템 소프트웨어이다.
- ④ 고속/고용량의 메모리나 CPU 등이 요구되지 않으므로 시스템 운영비를 감소시킬 수 있다.

17. 프로세스(Process)와 스레드(Thread)에 대한 설명으로 가장 옳지 않은 것은?

- ① 프로세스는 운영체제에서 작업의 기본 단위이다.
- ② 프로세스는 비동기적인 행위를 일으키는 주체이다.
- ③ 스레드는 프로세스에서 실행의 개념만을 분리한 것이다.
- ④ 하나의 스레드 내에는 여러 개의 프로세스가 존재할 수 있다.

18. RAID(Redundant Array of Inexpensive Disks)에 관한 설명으로 옳지 않은 것은?

- ① 데이터 복구의 용이성을 위해 사용한다.
- ② 다수의 디스크에 데이터를 분할하여 전송함으로써 전체적인 데이터 전송 속도 향상을 위해 사용한다.
- ③ 한 개의 데이터를 여러 디스크에 저장하여 데이터 안정성을 향상시키기 위해 사용한다.
- ④ 한 개의 대용량 디스크를 여러 개의 디스크처럼 나누어 사용함으로써 데이터 효율성을 향상시키기 위해 사용한다.

19. 다음 중 TCP(Transmission Control Protocol)에 대한 설명으로 가장 옳지 않은 것은?

- ① OSI 7 계층 모델에서 트랜스포트(Transport)계층에 해당한다.
- ② 다수의 기기에 대한 브로드캐스팅(Broadcasting)을 지원한다.
- ③ 연결지향형(Connection-oriented) 프로토콜이다.
- ④ 흐름 제어(Flow control) 기능이 지원된다.

20. 다음에서 설명하는 네트워크 장비로 옳은 것은?

- OSI 3계층에서 동작
- 동일한 전송 프로토콜을 사용하는 분리된 2개 이상의 네트워크를 연결

- ① 브리지(Bridge)
- ② 라우터(Router)
- ③ 리피터(Repeater)
- ④ 허브(Hub)

네트워크 보안

1. 다음에서 설명하고 있는 네트워크 공격은 무엇인가?

- ICMP의 echo 패킷을 이용하여 reply 패킷의 폭주를 통해 시스템을 마비시킨다.
- 공격자는 ping의 목표주소를 네트워크 브로드캐스트 주소로 할당하고 자신을 공격할 호스트로 위장한 후 echo 패킷을 전송한다.

- ① Teardrop 공격
- ② UDP flooding 공격
- ③ Smurf 공격
- ④ ICMP redirection 공격

2. 해커가 리눅스 서버에 침입 후 백도어를 설치하였다. 백도어와 연관된 포트가 열려있는지 확인하기 위해 사용할 수 있는 적절한 프로그램은 무엇인가?

- ① ps
- ② Nmap
- ③ nslookup
- ④ traceroute

3. VPN(Virtual Private Network)에 대한 설명으로 가장 옳지 않은 것은?

- ① 공중망을 사용하여 사설망과 같은 효과를 얻는다.
- ② 서로 다른 통신 프로토콜을 사용하여 네트워크 사이에서 데이터를 전송한다.
- ③ RSVP 프로토콜을 사용하여 터널을 만들고 암호화를 수행한다.
- ④ 터널링 기법은 IPsec, SSL 등의 방법을 사용한다.

4. 컴퓨터의 내부 자료를 탈취하는 수법으로 프로그램 개발 시에 내용을 볼 수 있는 부정루틴을 삽입하여 컴퓨터의 정비나 유지보수를 핑계 삼아 악의적인 행위를 하는 방법은 무엇인가?

- ① Trap Door
- ② TRINOO
- ③ Trojan Horse
- ④ Teardrop

5. 다음의 설명에 해당되는 시스템은 무엇인가?

기업 데이터 유출 방지를 의미하며 사용자가 사무실, 현장 및 집 어느 곳에서 업무 중이라도 사용자의 PC에서 기업 내 기밀 데이터가 외부로 반출되는 것을 항상 감시하고 기록하며, 정책에 따라 유출을 차단시키는 것을 주 기능으로 구현한 솔루션이다.

- ① DLP
- ② IDS
- ③ IDC
- ④ EIP

6. 다음에서 설명하는 것을 올바르게 짝지은 것은?

(가)은/는 악의적인 프로그램을 건전한 프로그램 처럼 포장하여 일반 사용자들이 의심 없이 자신의 컴퓨터 안에서 이를 실행시키고 실행된 (가)은/는 특정 포트를 열어 공격자의 침입을 돕고 추가적으로 정보를 자동 유출하며 자신의 존재를 숨긴다.
(나)은/는 OS에서 버그를 이용하여 루트권한 획득 또는 특정 기능을 수행하기 위한 공격 코드 및 프로그램을 의미한다.

- ① (가) Exploit (나) Trojan
- ② (가) Trojan (나) Hoax
- ③ (가) Trojan (나) Exploit
- ④ (가) Exploit (나) Hoax

7. 다음에서 설명하는 것은 무엇인가?

무선네트워크 액세스포인트 이름을 의미하며 각 액세스포인트에 하나씩 할당되어 있다. 기본적으로 AP와 Client는 이것이 일치해야만 통신이 가능하게 되는데 액세스포인트가 자신들의 이것을 브로드캐스팅하기 때문에 보안에 취약할 수밖에 없다.

- ① SSID
- ② MAC
- ③ WEP
- ④ WPA

8. 이더넷 물리 주소가 될 수 있는 것은 다음 중 어떤 것인가?

- ① 01:02:01:2C:4B
- ② 07:01:02:01:2C:4B:2C
- ③ 07:01:02:01:2C:4B
- ④ 07:02:01:02:3B:4C:3C:2B

9. 아래의 하드웨어 장비 중 OSI 2계층에 해당하는 장비는 무엇인가?

리피터, 허브, 브리지, 라우터, 스위치, L4 스위치

- ① 리피터, 허브
- ② 브리지, 스위치
- ③ 라우터, 스위치
- ④ 스위치, L4 스위치

10. 다음 지문의 필터링 규칙을 설명한 것 중에서 가장 옳지 않은 것은?

가. iptables -A INPUT -s 201.1.1.1 -j DROP
나. iptables -A INPUT -p TCP -j ACCEPT
다. iptables -A INPUT -i eth0 -p TCP -dport 80 -j DROP
라. iptables -A INPUT -i eth0 -p TCP -dport 80 -j REJECT

- ① “가”번은 201.1.1.1에서 유입되는 모든 패킷을 DROP 시킨다.
- ② “나”번은 TCP 프로토콜을 사용하는 모든 서비스의 요청을 허용한다.
- ③ “다”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP 시킨다.
- ④ “라”번은 eth0으로 유입되는 TCP 프로토콜 80번의 모든 패킷을 DROP하고 송신자는 차단 여부를 확인할 수 없게 한다.

11. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?

- 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

12. 다음 중 IPsec(IP Security Protocol)에 대한 설명으로 가장 옳지 않은 것은?

- ① IPsec 정책 설정 과정에서 송·수신자의 IP주소를 입력한다.
- ② 전송(Transport) 모드에서는 IP헤더가 암호화된다.
- ③ 재전송 공격을 막기 위해 IP 패킷별로 순서번호를 부여한다.
- ④ IKE(Internet Key Exchange) 프로토콜로 세션키를 교환한다.

13. 다음 설명에 해당하는 블루투스 공격 방법은?

블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격 방법이다. 이 공격방법은 블루투스 장치끼리 인증 없이 정보를 간편하게 교환하기 위해 개발된 OPP(OBEX Push Profile) 기능을 사용하여, 공격자가 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청해 이를 열람하거나 취약한 장치의 파일에 접근하는 공격 방법이다.

- ① 블루스나프(BlueSnarf)
- ② 블루프린팅(BluePrinting)
- ③ 블루버그(BlueBug)
- ④ 블루재킹(BlueJacking)

14. 다음의 보기에서 설명하고 있는 접근제어(Access Control) 방법은 무엇인가?

- 주체(사용자)의 객체(정보)에 대한 접근이 주체의 비밀취급인가 레이블과 각 객체에 부여된 민감도 레이블에 따라 접근 허용 여부를 결정하는 방식
- 중앙집중적 관리가 가능하고, 기밀성이 매우 중요한 조직에서 사용
- 다단계 보안 모델이라고 부르기도 함

- ① 임의적 접근제어
- ② 강제적 접근제어
- ③ 역할기반 접근제어
- ④ 자율적 접근제어

15. 침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는데 적합한 기법은 무엇인가?

- ① 규칙 기반의 오용 탐지
- ② 통계적 분석에 의한 이상 탐지
- ③ 전문가 시스템을 이용한 오용 탐지
- ④ 시그니처 기반(Signature based) 탐지

16. VPN(Virtual Private Network)에서 “터널링”이라는 용어가 의미하는 내용에 가장 부합하는 것은?

- ① 선택사항으로서 작동 시 네트워크 성능을 향상시킬 수 있는 기능이다.
- ② 가상회선을 생성하고 유지할 목적으로 상이한 프로토콜의 패킷 안에 패킷을 캡슐화하는 기능이다.
- ③ 네트워크상 해커를 탐지하기 위해 시스템 관리자가 사용하는 기능이다.
- ④ 네트워크 침입이 탐지되면 바로 차단 조치를 취해 비정상 행위를 통제하는 기능이다.

17. 침해대응 과정에서 다음의 패킷로그를 기준으로 검토해 보았다. 어떤 공격 기법인가?

- Source IP : 203.234.212.10
 - Destination IP : 203.234.212.10
 - Protocol : 6
 - Source Port : 21845
 - Destination Port : 21845

- ① Land Attack
- ② Syn flooding Attack
- ③ Smurf Attack
- ④ Ping of Death Attack

18. ESM(Enterprise Security Management)에 대한 설명으로 가장 올바른 것은 무엇인가?

- ① 개별 솔루션 간의 별도 연동작업이 추가적으로 요구되지 않는다.
- ② Agent에서 읽어온 로그를 분석 없이 Manager가 수신 받고 콘솔로 표출한다.
- ③ 각 종 로그를 통합적으로 관리하여 통합 보안관제 서비스를 제공한다.
- ④ 이기종의 보안시스템을 통합하여 관리할 수 없다.

19. 특정 기관에서 사용자가 누구인가는 확인하지 않고, 그 기관이 인가한 장비이면 기관 네트워크에 접근이 가능하도록 하는 정책을 수행하고자 할 때, 적용할 수 있는 장비 인증기술로 적절한 것은?

- ① ID/PW 기반 인증기술
- ② MAC 주소 값 인증기술
- ③ SSID 인증기술
- ④ WEP 인증기술

20. 다음에서 설명하는 보안 장비는 무엇인가?

- 엔드포인트(Endpoint)가 처음 내부망 네트워크에 접근을 시도할 때 내부망에 피해가 없도록 엔드포인트에 일련의 보안정책을 적용하는 보안 솔루션이다.
 - 내부 백신 설치여부, 컴퓨터 이름 등을 바탕으로 제한한다.

- ① IDS(Intrusion Detection System)
- ② IPS(Intrusion Prevention System)
- ③ NAC(Network Access Control)
- ④ NFS(Network File System)

정보시스템보안

1. 다음 지문은 데이터베이스에서 키의 유형에 대한 설명이다. 지문에 적합한 키는 무엇인가?

- 여러개의 후보키 중에서 기본키로 선정되고 남은 나머지 키를 지칭
- 기본키를 <학번>으로 선정했다면, <이름, 학과>를 지칭

- ① Candidate Key
- ② Primary Key
- ③ Alternate Key
- ④ Foreign Key

2. 다음 설명하는 키 교환 알고리즘은 무엇인가?

1976년 미국 스탠퍼드 대학의 연구원이 개발한 것으로 공개키는 한 개의 정수와 한 개의 소수로 구성되어 있으며, 통신 직전에 통신 상대방과 공유하도록 해두고, 다른 비밀키 전용의 숫자를 통신 상대방 양쪽에서 각각 갖도록 해서, 이들과 공개키의 수치를 사용하여 공통 암호키용 수치를 산출한다.

- ① DES
- ② Diffie-Hellman
- ③ AES
- ④ SEED

3. 다음 중 대칭키(비밀키) 암호화 기반의 알고리즘이 아닌 것은?

- ① DES(Data Encryption Standard)
- ② ECC(Elliptic Curve Cryptosystem)
- ③ IDEA(International Data Encryption Algorithm)
- ④ AES(Advanced Encryption Standard)

4. 다음 중 세마포어에 대한 설명으로 가장 옳지 않은 것은?

- ① 여러 개의 프로세스가 동시에 그 값을 수정하지 못한다.
- ② 상호배제 문제를 해결하기 위해 사용된다.
- ③ 세마포어에 대한 연산은 처리 중에 인터럽트 되어야 한다.
- ④ 다익스트라(E.J. Dijkstra)가 제안한 방법이다.

5. 다음은 윈도우 부팅 순서이다. 올바르게 나열된 것은?

- 가. MBR - 부팅 매체에 대한 기본적인 파일시스템 정보를 읽는다.
- 나. POST - 하드웨어 자체의 시스템에 문제가 없는지 체크한다.
- 다. NTLDR - 하드디스크 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며, BOOT.INI 파일의 내용을 읽는다.
- 라. NTDETECT.COM - 설치된 하드웨어를 검사한다.
- 마. NTOSKRNL.EXE - HAL.dll을 로드한다.
- 바. CMOS - 사용자가 설정한 기본사항을 읽어 시스템에 적용한다.

- ① 바-다-라-가-마-나
- ② 나-바-가-다-라-마
- ③ 나-바-다-라-가-마
- ④ 바-가-마-나-다-라

6. 다음 괄호 안에 공통으로 들어갈 적당한 단어는?

()은/는 하드웨어 특성으로부터 프로그램들을 격리시키고, 하드웨어와 직접적으로 상호 작동함으로써 프로그램들에게 일관된 서비스를 제공한다. ()의 기본개념은 프로세스와 파일의 관리이다. 그밖에 입출력장치 관리, 메모리 관리 및 시스템 호출 인터페이스 등이다.

- ① 유틸리티(Utilities)
- ② 커널(Kernel)
- ③ 셸(Shell)
- ④ 데몬(Daemon)

7. 다음 중 오버플로우에 대한 설명 중 가장 옳지 않은 것은?

- ① 버퍼에 저장된 프로세스 간의 자원 경쟁을 통해 권한을 획득하여 공격하는 방법이다.
- ② 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복귀주소를 조작하는 기법을 사용한다.
- ③ 스택 오버플로우와 힙 오버플로우 공격이 있다.
- ④ 버퍼 오버플로우가 발생하면 저장된 데이터는 인접한 변수 영역 및 포인터 영역까지 침범함으로 해커가 원하는 특정코드를 실행하도록 할 수 있다.

8. 다음 중 개인 식별 방법이 아닌 것은?

- ① 사용자의 공개키를 이용하는 방법
- ② 사용자의 고유의 물리적 특성을 이용하는 방법
- ③ 사용자가 알고 있는 정보를 이용하는 방법
- ④ 사용자가 소지하고 있는 것을 이용하는 방법

9. 게시판에 악성 스크립트를 삽입해서 쿠키, 개인정보 전송, 악성코드 다운로드 등을 수행할 수 있는 공격기법은 무엇인가?

- ① Web Shell
- ② XSS
- ③ 쿠키/세션 위조
- ④ SQL Injection

10. 다음 지문 중 괄호에 들어갈 포트번호를 적절하게 나열하고 있는 것은?

- SMTP는 전자우편을 보내는 데 사용되는 기본 프로토콜로서 TCP (㉠)번 포트를 사용한다.
- POP3 데몬 포트는 TCP (㉡)번을 사용해 메일 서버에서 전자우편을 내려 받는다.

- ① ㉠ 25 ㉡ 100
- ② ㉠ 25 ㉡ 110
- ③ ㉠ 80 ㉡ 100
- ④ ㉠ 143 ㉡ 110

11. 유닉스 파일시스템의 i-Node가 가지고 있지 않는 정보는 무엇인가?

- ① 파일 유형
- ② 파일 수정시각
- ③ 파일의 링크 수
- ④ 파일의 이름

12. MS오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성 코드는?

- ① 애드웨어
- ② 트로이 목마
- ③ 백도어
- ④ 매크로 바이러스

13. 다음 지문의 괄호 안에 들어갈 용어를 순서대로 나열한 것은?

공개키 알고리즘으로 정보화 서비스와 전자서명 서비스를 제공할 때 암호화에 사용하는 키는 수신자의 ()이고, 전자서명에서 서명 검증에 사용하는 키는 송신자의 ()이다.

- ① 개인키, 개인키
- ② 개인키, 공개키
- ③ 공개키, 개인키
- ④ 공개키, 공개키

14. 대칭키 암호 알고리즘과 공개키 암호 알고리즘에 대한 설명 중 가장 잘못된 것은?

- ① 대칭키 암호 알고리즘은 실행 속도가 빠르기 때문에 다양한 암호의 핵심함수로 사용된다.
- ② 공개키 암호 알고리즘은 자신만이 보관하는 비밀키를 이용하여 인증, 전자서명 등에 적용이 가능하다.
- ③ 대칭키 암호의 경우 키를 자주 변경해야 하는 불편함이 있다.
- ④ 대칭키 암호 알고리즘은 비밀키 공유를 위한 키 분배가 필요하지 않으면서도 암호화 및 복호화의 속도가 빠르다.

15. 다음 지문의 프로그램은 주로 어떤 용도로 사용되는가?

Nmap, Hping, PortQry

- ① 스캔 공격
- ② DoS 공격
- ③ Sniffing 공격
- ④ Session Hijacking 공격

16. 메시지에 대한 불법적인 공격자의 위협에는 수동적 공격과 능동적 공격이 있는데 다음 중 가장 올바르게 짝지어진 것은?

- ① 수동적 공격 - 삽입 공격
- ② 수동적 공격 - 재생 공격
- ③ 능동적 공격 - 메시지 변조
- ④ 능동적 공격 - 트래픽 분석

17. 다음 중 커버로스(Kerberos)에서 재전송 공격을 막기 위해 사용하는 것은 무엇인가?

- ① 인증정보
- ② 쿠키
- ③ 타임스탬프
- ④ 세션키

18. 다음에서 설명하는 것은 무엇인가?

재해복구센터에 주센터와 동일한 수준의 정보기술자원을 보유하는 대신 중요성이 높은 정보기술자원만 부분적으로 재해복구센터에 보유하는 방식이다. 구축 및 유지비용이 저렴하나 초기의 복구수준이 완전하지 않으며, 완전한 복구까지는 다소의 시일이 소요된다.

- ① 중복 사이트
- ② 핫(Hot) 사이트
- ③ 웜(Warm) 사이트
- ④ 콜드(Cold) 사이트

19. FTP 연결 방식과 관련된 다음 설명 중 가장 옳지 않은 것은?

- ① FTP 모드에는 active와 passive 모드가 있다.
- ② FTP 클라이언트에서 FTP 서버 방향으로 데이터 연결을 개시하는 것이 active 모드이다.
- ③ active 모드를 사용할지 passive 모드를 사용할지 결정하는 것은 FTP 클라이언트이다.
- ④ passive 모드에서 데이터 전송을 위해서는 서버와 클라이언트 모두 1024번 이후의 포트를 사용한다.

20. 침입을 당했을 때 로그파일을 비롯한 여러 파일의 환경설정이나 접근권한, 일부 파일이 변조나 삭제가 된다. 시스템이 변조되기 전에 헤더 값의 checksum을 저장하는 파일의 변조, 삭제 시 원래의 파일과 비교 대조할 수 있는 피해 분석 도구는?

- ① snort ② tcpdump
③ netstat ④ tripwire