

# 2022년도 제1차 경찰공무원 채용시험 문제지

## - 정보통신\_전산(순경) -



성명 :

응시번호 :

### 응시자 유의사항 및 과목별 코드번호

※ 시험 과목 : 컴퓨터일반(15), 네트워크보안(28),  
정보관리론(17)

※ 시험이 시작되기 전까지 표지를 넘기지 마시오.

# 해양경찰청

## 컴퓨터일반

1. 클라우드 컴퓨팅 서비스 모델과 이에 대한 설명이 가장 옳게 짝지어진 것은?

< 보기 >

- ㉠ 응용소프트웨어 개발에 필요한 개발 요소들과 실행 환경을 제공하는 서비스 모델로, 사용자는 원하는 응용소프트웨어를 개발할 수 있으나 운영체제나 하드웨어에 대한 제어는 서비스 제공자에 의해 제한된다.
- ㉡ 응용소프트웨어 및 관련 데이터는 클라우드에 호스팅 되고 사용자는 웹 브라우저 등의 클라이언트를 통해 접속하여 응용소프트웨어를 사용할 수 있다.
- ㉢ 사용자 필요에 따라 가상화된 서버, 스토리지, 네트워크 등의 인프라 자원을 제공한다.

- ① ㉠ - SaaS, ㉡ - PaaS, ㉢ - IaaS  
 ② ㉠ - PaaS, ㉡ - IaaS, ㉢ - SaaS  
 ③ ㉠ - PaaS, ㉡ - SaaS, ㉢ - IaaS  
 ④ ㉠ - IaaS, ㉡ - SaaS, ㉢ - PaaS

2. 전자계산기의 중앙처리장치(CPU)는 4가지 단계를 반복적으로 거치면서 동작을 행한다. 4가지 단계에 가장 속하지 않는 것은?

- ① Fetch Cycle                      ② Interrupt Cycle  
 ③ Branch Cycle                    ④ Execute Cycle

3. ARP(Address Resolution Protocol)에 대한 설명으로 가장 옳은 것은?

- ① 호스트의 MAC주소에 해당하는 IP주소를 구할 수 있다.
- ② ARP 요청은 해당 네트워크상의 모든 호스트와 라우터에게 유니캐스트(unicast)된다.
- ③ ARP 응답은 ARP 요청을 전송한 요청자와 모든 호스트에게 브로드캐스트(broadcast)된다.
- ④ ARP는 인증 기능이 없으므로 위조된 정보를 사용할 수 있다.

4. Access Time이 빠른 순서로 나열할 때 가장 옳은 것은?

< 보기 >

- ㉠ Cache Memory                      ㉡ Register  
 ㉢ Main Memory                      ㉣ Magnetic Disk

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

5. 비선점(Non-Preemptive) 스케줄링에 가장 해당하지 않는 것은?

- ① SRT(Shortest Remaining Time)  
 ② FCFS(First Come First Served)  
 ③ SJF(Shortest Job First)  
 ④ HRN(Highest Response ratio Next)

6. 다음에서 운영체제에 대한 설명으로 옳은 것만을 고른 것은?

< 보기 >

- ㉠ 운영체제는 중앙처리장치, 주기억장치, 보조 기억장치, 주변장치 등의 컴퓨터 자원을 할당 및 관리하는 시스템 소프트웨어이다.
- ㉡ 스푼링(spooling)은 CPU와 입출력 장치의 속도 차이를 줄이기 위해 주기억장치의 일부분을 버퍼처럼 사용하는 것이다.
- ㉢ 비선점(non-preemptive) 방식의 CPU 스케줄링 기법은 CPU를 사용하고 있는 현재의 프로세스가 종료된 후 다른 프로세스에 CPU를 할당하는데 대표적으로 RR(Round Robin) 스케줄링 기법이 있다.
- ㉣ 가상메모리(virtual memory)는 디스크와 같은 보조기억장치에 가상의 공간을 만들어 주기억 장치처럼 활용하도록 하여 실제 주기억장치의 물리적 공간보다 큰 주소 공간을 제공한다.

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

7. UNIX 시스템에서 커널의 수행 기능에 해당하는 것으로 가장 옳지 않은 것은?

- ① 프로세스 관리                      ② 기억장치 관리  
 ③ 입출력 관리                      ④ 명령어 해독

8. 파이프라이닝(pipelining) 기법이 적용된 중앙처리 장치(CPU)에서의 파이프라인 해저드(pipeline hazard) 종류와 대응 방법을 바르게 짝지은 것만을 모두 고른 것은?

< 보 기 >

- ㉠ 데이터 해저드(data hazard)  
→ 데이터 전방 전달(data forwarding)  
㉡ 구조적 해저드(structural hazard)  
→ 부족한 자원의 추가  
㉢ 제어 해저드(control hazard)  
→ 분기 예측(branch prediction)

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

9. 유비쿼터스 컴퓨팅에 대한 설명으로 가장 옳지 않은 것은?

- ① 노매딕(nomadic) 컴퓨팅은 현실 세계와 가상 화면을 결합하여 보여주는 기술이다.  
② 감지 컴퓨팅은 컴퓨터가 센서 등을 이용하여 사용자의 행위 또는 주변 환경을 인식하여 필요 정보를 제공하는 기술이다.  
③ 퍼베이시브(pervasive) 컴퓨팅은 컴퓨터가 도처에 편재되도록 하는 기술이다.  
④ 웨어러블(wearable) 컴퓨팅은 컴퓨터 착용을 통해 컴퓨터를 인간 몸의 일부로 여길 수 있도록 하는 기술이다.

10. 캐시메모리의 매핑(mapping) 방법이 아닌 것은?

- ① direct mapping  
② indirect mapping  
③ associative mapping  
④ set-associative mapping

11. Unix에서 <보기>의 작업을 수행하는 명령어들을 나열한 것 중 가장 옳은 것은?

< 보 기 >

- ㉠ 디렉터리 내의 파일 목록 확인  
㉡ 현재 실행 중인 프로세스들의 정보를 확인  
㉢ 현재 실행 중인 특정 프로세스 종료  
㉣ 파일 또는 디렉터리의 디스크 사용량 확인

- ① ㉠ ls    ㉡ netstat    ㉢ bg    ㉣ wc  
② ㉠ dir    ㉡ ps            ㉢ bg    ㉣ wc  
③ ㉠ ls    ㉡ netstat    ㉢ kill    ㉣ du  
④ ㉠ ls    ㉡ ps            ㉢ kill    ㉣ du

12. 다음 중 <보기>의 Java 프로그램 실행 결과로 가장 옳은 것은?

< 보 기 >

```
class CodeRunner {
    public static void main(String[] args) {
        A obj = new C();
        obj.f();
        obj.g();
    }
}
class A {
    public void f() {System.out.print("1 ");}
    public static void g() {System.out.print("2 ");}
}
class B extends A {
    public void f() {System.out.print("3 ");}
}
class C extends B {
    public static void g() {System.out.print("4 ");}
}
```

- ① 3 2                      ② 3 1                      ③ 1 4                      ④ 1 2

13. 다음 중 <보기1>의 테이블 R에 대해 <보기2>의 SQL을 수행한 결과로 가장 옳은 것은?

<보기1>

A	B
3	1
2	4
3	2
2	5
3	3
1	5

<보기2>

```
SELECT SUM(B) FROM R
GROUP BY A
HAVING COUNT(B) = 2;
```

- ① 9                      ② 5                      ③ 6                      ④ 2

14. 다음 중 <보기>에서 설명하는 기술로 가장 옳은 것은?

< 보 기 >

- 클라이언트의 요구에 대한 응답 시간을 줄일 수 있다.
- 외부 인터넷과 연결된 트래픽을 줄일 수 있다.
- 최근 호출된 객체의 사본을 저장한다.

- ① DNS server                      ② NAT server  
③ Router                              ④ Proxy server

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

- ① 라우터(router)는 데이터 전송을 위한 최선의 경로를 설정한다.
- ② 브리지(bridge)는 한 네트워크 세그먼트에서 들어온 데이터를 그의 물리적 주소에 관계없이 무조건 다른 세그먼트로 전달한다.
- ③ 스위치(switch)는 보안(security) 및 트래픽(traffic) 관리 기능도 제공할 수 있다.
- ④ 허브(hub)는 전달받은 신호를 그와 연결된 모든 노드들에 전달한다.

16. 시큐어 코딩(Secure Coding) 기법으로 가장 옳지 않은 것은?

- ① 화이트리스트 방식으로 허용된 확장자만 업로드를 허용한다.
- ② 입력 화면 폼(Form) 작성시 POST 방식보다 GET 방식을 사용한다.
- ③ 사용자로부터 입력받은 스크립트 관련 문자열을 필터링 하여 변환한다.
- ④ 인자화된 질의문(parameterized query)을 사용한다.

17. 다음 중 RAID(Redundant Array of Inexpensive Disks)에 대한 설명으로 가장 옳지 않은 것은?

- ① RAID-0은 디스크 스트라이핑(Disk Striping) 방식으로 중복 저장과 오류 검출 및 교정이 없는 방식이다.
- ② RAID-1은 디스크 미러링(Disk Mirroring) 방식으로 높은 신뢰도를 갖는다.
- ③ RAID-4는 데이터를 비트(bit) 단위로 여러 디스크에 분할하여 저장하는 방식이며, 별도의 패리티(parity) 디스크를 사용한다.
- ④ RAID-5는 별도의 패리티(parity) 디스크 대신 모든 디스크에 패리티(parity) 정보를 나누어 기록하는 방식이다.

18. 다음 중 소프트웨어 규모를 예측하기 위한 기능점수(function point)를 산정할 때 고려할 사항으로 가장 옳지 않은 것은?

- ① 원시 코드 라인 수(Line Of Code)
- ② 외부입력(External Input)
- ③ 외부조회(External inquiry)
- ④ 내부논리파일(Internal Logical File)

19. 다음 중 캐시기억장치 교체 알고리즘에 대한 설명으로 가장 옳지 않은 것은?

- ① LRU는 최근에 가장 오랫동안 사용되지 않았던 블록을 교체하는 방법이다.
- ② FIFO는 캐시에 적재된 후 가장 오래된 블록을 먼저 교체하는 방법이다.
- ③ LFU는 참조 횟수를 기록함으로써 가장 많이 참조된 블록을 교체하는 방법이다.
- ④ Random은 사용 횟수와 무관하게 임의로 블록을 교체하는 방법이다.

20. 다음 중 <보기>에서 설명하는 C프로그램의 실행 결과로 가장 옳은 것은?

— < 보 기 > —

```
#include <stdio.h>

int a = 10;
int b = 20;
int c = 30;

void func(void)
{
    static int a = 100;
    int b = 200;

    a++;
    b++;
    c = a;
}

int main(void)
{
    func();
    func();

    printf("a = %d, b = %d, c = %d\n", a, b, c);
}
```

- ① a = 10, b = 20, c = 30
- ② a = 10, b = 20, c = 102
- ③ a = 101, b = 201, c = 101
- ④ a = 102, b = 202, c = 102

## 네트워크보안

1. 다음 중 SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

- ① ChangeCipherSpec - Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.
- ② Handshake - 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.
- ③ Alert - 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터 베이스를 조회한다.
- ④ Record - 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용계층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

2. 다음 중 망 내 교환 장비들이 오류 상황에 대한 보고를 할 수 있게 하고, 예상하지 못한 상황이 발생한 경우 이를 알릴 수 있도록 지원하는 프로토콜은 무엇인가?

- ① ICMP      ② ARP      ③ RARP      ④ IGMP

3. 다음 <보기> 중 제시된 Well Known Port 번호에 해당하는 프로토콜을 순서대로 가장 적합하게 제시한 것은?

< 보 기 >

- ㉠ 22번 포트      ㉡ 53번 포트      ㉢ 161번 포트

- |         |          |           |
|---------|----------|-----------|
| ① ㉠ SSH | ㉡ Gopher | ㉢ NetBIOS |
| ② ㉠ SSH | ㉡ DNS    | ㉢ SNMP    |
| ③ ㉠ FTP | ㉡ Gopher | ㉢ SNMP    |
| ④ ㉠ FTP | ㉡ DNS    | ㉢ NetBIOS |

4. 다음 중 OSI 7계층 모델에서 동작하는 계층이 가장 다른 것은?

- |           |           |
|-----------|-----------|
| ① L2TP    | ② PPTP    |
| ③ SYN 플러딩 | ④ ARP 스푸핑 |

5. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?

- ① MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.
- ② 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.
- ③ 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.
- ④ TCP/IP 프로토콜을 사용하는 네트워크에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

6. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은 무엇인가?

- ① DoS 공격
- ② 취약한 인증 및 세션 공격
- ③ SQL 삽입 공격
- ④ CSRF 공격

7. 다음 중 SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는데 악용될 수 있는 명령어는 무엇인가?

- |           |             |
|-----------|-------------|
| ① HELO    | ② MAIL FROM |
| ③ RCPT TO | ④ VRFY      |

8. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳지 않은 것은?

- ① 물리적 망분리와 논리적 망분리 기법이 존재한다.
- ② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.
- ③ 논리적 망분리 기법으로 SBC 및 CBC 기반의 망분리 기법이 존재한다.
- ④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

9. 다음 중 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직으로 가장 옳은 것은?

- ① CISO      ② CERT      ③ CPPG      ④ CPO

10. 다음 중 HTTP 응답 메시지 상태 코드의 의미가 가장 옳지 않은 것은?

- ① 201 - Created  
 ② 301 - Moved Permanently  
 ③ 401 - Unauthorized  
 ④ 501 - Bad Request

11. 다음 중 IP Spoofing 공격 활동으로 가장 옳지 않은 것은?

- ① SYN Flooding 공격  
 ② slowloris 공격  
 ③ RST를 이용한 접속 끊기  
 ④ 순서번호 추측(Sequence number guessing)

12. 다음 중 ESM(통합보안솔루션)의 구성요소에 대한 설명으로 가장 옳지 않은 것은?

- ① 보안패치 : 최근 보안취약점이 발생한 시스템에 대해서 자동으로 패치를 수행한다.  
 ② Manager : 수집된 로그정보를 통합하고 분석한다.  
 ③ Console : 관리자는 ESM Console을 사용해서 모니터링하고 명령어를 실행한다.  
 ④ Agent : 시스템에 설치되어서 각종 로그정보를 수집한다.

13. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

( ㉠ )는 웹 페이지에 입력되는 입력 값 검증 및 필터링 등을 수행하는 방화벽이다.  
 ( ㉡ )는 모바일 단말에 대해서 소프트웨어 및 펌웨어를 관리하는 솔루션이다.  
 ( ㉢ )는 네트워크 패킷을 탐지하고 대응까지 수행한다.

- ① ㉠ WAF(Web Application Firewall)  
     ㉡ MDM           ㉢ IPS  
 ② ㉠ WAF(Web Application Firewall)  
     ㉡ MAM           ㉢ IDS  
 ③ ㉠ Firewall  
     ㉡ MDM           ㉢ IDS  
 ④ ㉠ Firewall  
     ㉡ MAM           ㉢ IPS

14. 다음 중 Spoofing의 종류로 가장 옳지 않은 것은?

- ① ARP Spoofing                      ② IP Spoofing  
 ③ DNS Spoofing                      ④ ULU Spoofing

15. 다음 <보기>는 VPN에 대한 설명이다. ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

- IPSEC VPN은 ( ㉠ ) 단위로 데이터를 암호화 한다.
- SSL VPN은 ( ㉡ ) 단위로 데이터를 암호화 한다.

- ① ㉠ 프레임                      ㉡ 데이터  
 ② ㉠ 데이터                      ㉡ 프레임  
 ③ ㉠ 패킷                        ㉡ 메시지  
 ④ ㉠ 메시지                      ㉡ 메시지

16. 다음 <보기>는 VLAN(Virtual Local Area Network)에 대한 설명이다. 다음 중 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

VLAN은 여러 개의 구별되는 ( ㉠ ) 도메인을 만들기 위해서 단일 2계층 네트워크를 ( ㉡ )으로 분할하고 한 포트에서 보이는 모든 네트워크 패킷 혹은 전체 VLAN의 모든 패킷들을 다른 모니터링 포트로 복제하는 ( ㉢ ) 기능을 제공한다.

- ① ㉠ 유니캐스트            ㉡ 물리적    ㉢ 허브 미러링  
 ② ㉠ 브로드캐스트    ㉡ 논리적    ㉢ 포트 미러링  
 ③ ㉠ 유니캐스트            ㉡ 논리적    ㉢ 포트 미러링  
 ④ ㉠ 브로드캐스트    ㉡ 물리적    ㉢ 허브 미러링

17. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

< 보 기 >

ANTI APT 솔루션에서 악성코드를 동적으로 분석하기 위해서 악성코드를 실행한 후에 행위 로그를 분석한다. 이때 악성코드 분석은 ( ) 환경에서 수행되어야 한다.

- ① SCADA                              ② Sandbox  
 ③ Cloud                                ④ CRM

18. 다음 중 <보기>의 설명에서 (    )에 들어갈 설명으로 가장 옳은 것은?

— < 보 기 > —  
Tcpdump는 네트워크에서 전송되는 패킷을 스니핑하는 도구이다. 전송되는 패킷을 특정 포트로 ( ㉠ ), 스니핑 모드를 ( ㉡ )(으)로 설정해야 한다.

- |            |          |
|------------|----------|
| ① ㉠ 포트 미러링 | ㉡ 정규 모드  |
| ② ㉠ 무차별 모드 | ㉡ 포트 미러링 |
| ③ ㉠ 포트 미러링 | ㉡ 무차별 모드 |
| ④ ㉠ 무차별 모드 | ㉡ 정규 모드  |

19. 다음 중 <보기>의 설명에서 (    )에 들어갈 설명으로 가장 옳은 것은?

— < 보 기 > —  
IPv6는 ( ㉠ )비트의 주소 공간을 가지며 헤더는 총 ( ㉡ )개의 필드를 가지고 있다. 그리고 암호화와 ( ㉢ )기능을 지원한다.

- |         |     |      |
|---------|-----|------|
| ① ㉠ 128 | ㉡ 8 | ㉢ 인증 |
| ② ㉠ 32  | ㉡ 4 | ㉢ 인증 |
| ③ ㉠ 32  | ㉡ 8 | ㉢ 인가 |
| ④ ㉠ 128 | ㉡ 4 | ㉢ 인가 |

20. 다음 중 리눅스 시스템의 네트워크 관리 도구 및 서비스에 대한 설명으로 가장 옳지 않은 것은?

- ① ifconfig - 네트워크 인터페이스의 IP 주소 설정
- ② traceroute - 최종 목적지 컴퓨터까지 중간에 걸치는 여러 개의 라우터에 대한 경로 및 응답 속도를 표시
- ③ fping - 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력
- ④ tcpdump - 네트워크 모니터링 및 패킷 분석을 위해 사용되는 도구로, 패킷 필터 기능을 통해서, 특정 침입자의 침입 경로에 따라 원하는 트래픽만을 감시

## 정보관리론

1. 보안 관리 대상에 대한 <보기>의 설명에서 ( )에 들어갈 용어로 다음 중 가장 옳은 것은?

< 보 기 >

- ( ㉠ ) : 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.  
 ( ㉡ ) : 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인이나 행위자를 말한다.  
 ( ㉢ ) : 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.

- |        |      |      |
|--------|------|------|
| ① ㉠ 로그 | ㉡ 위험 | ㉢ 쿠키 |
| ② ㉠ 로그 | ㉡ 위험 | ㉢ 세션 |
| ③ ㉠ 백업 | ㉡ 위험 | ㉢ 세션 |
| ④ ㉠ 백업 | ㉡ 위험 | ㉢ 쿠키 |

2. 다음 중 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 가장 옳지 않은 것은?

- ① 생성된 수열의 비트는 무작위로 발생한다.  
 ② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 있어야 한다.  
 ③ 시드(seed)라고 불리는 입력 값은 외부에 알려지지 않도록 비밀로 하여야 한다.  
 ④ 고정값 시드(seed)를 입력받아 결정적 알고리즘을 사용하여 출력 비트열을 생성한다.

3. 다음 중 중앙 집중형 인증 방식인 커버로스(Kerberos)에 대한 설명으로 가장 옳지 않은 것은?

- ① 신뢰받는 제3자인 키 배포기관이 구성원들 중간에 개입하는 방법이다.  
 ② 커버로스는 세션키를 이용한 티켓 기반 인증 기법을 제공한다.  
 ③ 인증 서버가 사용자에게 발급한 티켓(승인 티켓)은 유효기간 내에 재사용할 수 있다.  
 ④ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

4. 다음 중 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화 되어 있는 파일로 가장 옳은 것은?

- ① /etc/group  
 ② /etc/passwd  
 ③ /etc/shadow  
 ④ /etc/login.defs

5. 다음 중 유닉스 로그파일에 대한 설명으로 가장 옳지 않은 것은?

- ① lastlog : 사용자들이 마지막으로 로그아웃한 정보를 가지고 있다.  
 ② utmp : 현재 로그인한 사용자 정보를 가지고 있다.  
 ③ wtmp : 로그인과 로그아웃, 시스템 부팅 정보를 가지고 있다.  
 ④ sulog : su(switch user) 명령어를 실행한 정보를 가지고 있다.

6. 다음 중 hwp, pdf, doc 등의 문서를 암호화하여 외부 유출 시에도 기업 내부 정보를 보호하는 것으로 가장 옳은 것은?

- ① DRM      ② CDR      ③ NFV      ④ EDR

7. 다음 중 개인정보영향평가 시 고려하여야 할 사항으로 가장 옳지 않은 것은?

- ① 처리하는 개인정보의 수  
 ② 개인정보처리자의 인가 여부  
 ③ 정보주체의 권리를 해할 가능성 및 그 위험 정도  
 ④ 개인정보의 제3자 제공 여부

8. 다음 중 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?

- ① 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.  
 ② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.  
 ③ 메시지 자체를 암호화 또는 복호화 할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.  
 ④ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화 할 수 있다.



9. 다음 중 유닉스에서 파일의 속성을 검색하는 find 옵션으로 가장 옳지 않은 것은?

- ① mtime : 파일의 내용이 수정된 시간을 기준으로 검색한다.  
 ② atime : 파일에 접근한 시간을 기준으로 검색한다.  
 ③ ctime : 파일 속성, 권한, 크기가 변경된 시간을 기준으로 검색한다.  
 ④ rtime : 파일 실행 일자를 기준으로 검색한다.

10. 다음의 ㉠ ~ ㉣에 해당되는 대칭키 암호 알고리즘을 가장 옳게 나열한 것은?

< 보 기 >

- ㉠ DES의 암호화 강도가 점점 약해지면서 이를 대체하기 위한 알고리즘으로 현재 미국 연방정부표준 블록 암호 알고리즘(NIST FIPS 197)으로 사용  
 ㉡ 국내에서 민간 부분인 인터넷, 전자상거래, 무선 통신 등에서 민감 정보 및 프라이버시 보호를 위해 한국인터넷진흥원(KISA)이 주축이 되어 개발한 128/256 비트 암호키를 지원하며 IFTF 및 ISO/IEC 국제표준으로 채택된 바 있음  
 ㉢ 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안 기술연구소 주도로 경량 환경 및 하드웨어의 효율성 향상을 위해 개발된 128비트 블록 암호 알고리즘으로 128/192/256 비트 암호화키를 지원

- ① ㉠ AES      ㉡ SEED      ㉢ ARIA  
 ② ㉠ AES      ㉡ ARIA      ㉢ SEED  
 ③ ㉠ ARIA      ㉡ SEED      ㉢ AES  
 ④ ㉠ ARIA      ㉡ AES      ㉢ SEED

11. 서버 관리자가 사용할 수 있는 보안용 소프트웨어 중 그 용도가 가장 다른 것은?

- ① AWstats      ② Nessus  
 ③ Acunetix      ④ Nmap

12. 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 가장 옳지 않게 연결된 것은?

- ① ps, top : 특정 프로세스 정보를 숨김  
 ② w, who : 특정 사용자의 정보를 숨김  
 ③ ls, du : 특정 파일이나 디렉토리를 숨김  
 ④ ifconfig : 특정 IP에서의 접속을 숨김

13. 다음은 FTP(File Transfer Protocol) 서비스에 대한 내용을 설명한 것이다. 가장 옳지 않은 것은?

- ① 전송계층 프로토콜로 TCP를 사용하고 있으며, 클라이언트 서버 모델로 구성되어 있다.  
 ② IETF에 따라 RFC 959로 정의된다.  
 ③ 기본적으로 액티브 모드(Active mode)와 패시브 모드(Passive mode)를 지원한다.  
 ④ 제어 연결은 21 포트를, 데이터 연결은 512 이후 포트를 사용한다.

14. 다음 중 블록 암호 알고리즘의 종류가 아닌 것은?

- ① RC5      ② DES      ③ MD5      ④ IDEA

15. 다음은 윈도우 부팅 순서이다. 가장 옳게 나열한 것은?

< 보 기 >

- ㉠ MBR - 부팅 매체에 대한 기본적인 파일 시스템 정보가 들어 있는 MBR 정보를 읽는다.  
 ㉡ POST - 하드웨어 자체가 시스템에 문제가 없는지 기본적인 사항을 체크하는 과정  
 ㉢ NTLDR - 하드디스크의 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며 boot.ini 파일의 내용을 읽는다.  
 ㉣ NTDETECT.com - 설치된 하드웨어를 검사한다.  
 ㉤ ntoskrnl.exe - HAL.dll을 로드한다.  
 ㉥ CMOS - 사용자가 설정한 기본 사항을 읽어 시스템에 적용한다.

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

16. ‘사이버위기경보’의 등급 중 복수 정보통신서비스 제공자(ISP) 망에 장애 또는 마비가 발생하였을 경우, 발령하는 경보의 단계는 무엇인가?

- ① 심각 단계                      ② 경계 단계  
③ 주의 단계                      ④ 관심 단계

17. 다음 중 전자우편 보안기술 PGP의 기능으로 가장 옳지 않은 것은?

- ① 전자서명                      ② 암호화  
③ 생체인증                      ④ 무결성

18. 다음의 접근통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것은?

< 보 기 >

- ㉠ 벨라파둘라(Bell-LaPadula) 모델  
㉡ 비바(Biba) 모델  
㉢ 클락 윌슨(Clark-Wilson) 모델

- ① ㉠                      ② ㉡                      ③ ㉠ ㉡                      ④ ㉡ ㉢

19. 다음에서 설명하는 키의 종류는 무엇인가?

< 보 기 >

- ㉠ 반복적으로 사용하는 대표키로 안전한 보관이 필요하다.  
㉡ 한번만 사용하는 키로 사용이 종료되면 폐기되는 키이다.  
㉢ 비대칭 암호시스템에서 전자서명용 검증키이고, 평문데이터의 암호화용으로 사용한다.

- ① ㉠ 대칭키                      ㉡ 세션키                      ㉢ 개인키  
② ㉠ 세션키                      ㉡ 대칭키                      ㉢ 공개키  
③ ㉠ 마스터키                      ㉡ 세션키                      ㉢ 공개키  
④ ㉠ 세션키                      ㉡ 마스터키                      ㉢ 개인키

20. 해킹 수단과 그 공격 방법에 대한 설명으로 가장 옳지 않은 것은?

- ① Ransomware : 파일을 암호화한 후 복호화를 조건으로 금전을 요구함  
② Rootkit : 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴  
③ SQL Injection : 데이터베이스에 질의어를 변조하여 공격함  
④ Cross-site Scripting : 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함

