

※ 답안지에 표기한 답을 수정테이프 이외의 도구(수정액, 칼 등)를 사용하여 정정하였을 경우 그 문항은 무효로 처리함.

1. 무결성(Integrity)을 위협하는 보안 공격(Security Attack)으로 가장 적절하지 않은 것은?

- ① 변경(Modification) ② 트래픽 분석(Traffic Analysis)
③ 부인(Repudiation) ④ 가장(Masquerading)

2. 어떤 컴퓨터가 대칭키 암호화 연산을 초당 2^{32} 번 수행한다고 하자. 56비트 키를 전수조사 공격을 통해서 찾을 경우 소요 되는 시간과 128비트 키로 변경할 경우 전수조사 공격으로부터 안전한지 여부에 대하여 가장 적절한 것은?

- ① 약 3개월 소요, 키의 크기가 128비트이면 전수공격에 안전하지 않다.
② 약 6개월 소요, 키의 크기가 128비트이면 전수공격에 안전하지 않다.
③ 약 3개월 소요, 키의 크기가 128비트이면 전수공격에 안전하다고 말할 수 있다.
④ 약 6개월 소요, 키의 크기가 128비트이면 전수공격에 안전하다고 말할 수 있다.

3. 디지털 콘텐츠 보호에 활용되는 저작권 기술에 대한 설명으로 가장 적절하지 않은 것은?

- ① 디지털 워터마킹(Digital Watermarking)은 원본의 내용을 왜곡하지 않는 범위 내에서 혹은 사용자가 인식하지 못하도록 저작권 정보를 디지털 콘텐츠에 삽입하는 기술이다.
② 핑거프린팅(Fingerprinting)은 디지털 콘텐츠를 구매할 때 판매자의 정보를 삽입하여 불법 배포 발견 시 최초의 배포자를 추적할 수 있게 하는 기술이다.
③ DRM(Digital Rights Management)은 디지털 콘텐츠의 불법 복제와 유포를 막고 지적재산권 보유자의 이익과 권리를 보호해주는 기술과 서비스를 말한다.
④ DRM(Digital Rights Management) 구성요소 중 메타데이터(Metadata)는 콘텐츠 생명주기 범위 내에서 관리되어야 할 각종 데이터의 구조 및 정보를 의미한다.

4. 다음 암호화 알고리즘에 대한 설명으로 옳은 것은 모두 몇 개인가?

- 가. DES 알고리즘 : 64비트 평문을 64비트 암호문으로 암호화하며, 암호화와 복호화에 사용하는 키는 56비트이며 오류검출을 위해 8비트가 사용된다.
나. AES 알고리즘 : 128비트 암호화 블록으로 64, 128, 256비트의 다양한 키의 길이를 갖춘 알고리즘이다.
다. SEED 알고리즘 : 한국인터넷진흥원과 국내 암호 전문가들이 순수 국내 기술로 개발한 128비트 블록의 암호화 알고리즘이다.
라. RSA 알고리즘 : SSL 프로토콜을 가진 웹 브라우저, PGP 그리고 공개키 암호시스템에 사용된다.

- ① 1개 ② 2개 ③ 3개 ④ 4개

5. 다음 지문에서 설명하는 일방향 해시함수의 내용에 따른 인증 수행 방법으로 가장 적절한 것은?

일방향 해시함수를 사용하면 무결성을 확인할 수 있으나 송신자의 거짓 위장을 검출하지 못한다. 파일의 무결성을 조사함과 동시에 정당한 송신자의 것인가를 확인하는 인증을 필요로 한다.

- ① ECC(Elliptic Curve Cryptography)
② MDC(Modification Detection Code)
③ MAC(Message Authentication Code)
④ PGP(Pretty Good Privacy)

6. 다음 지문에서 설명하는 사회공학적인 해킹방법으로 가장 적절한 것은?

공격자는 피해자가 가지고 있는 가치 있는 정보를 포기하도록 유도하는 사회공학의 한 형태이다. 예를 들어, 공격자가 직원에게 전화를 걸어 CEO나 정보기술팀의 권한자로 가장하여 피해자에게 자신의 존재를 확신시키고, 피해자로부터 원하는 정보를 수집한다.

- ① Quid Pro Quo ② Pretexting
③ Clickjacking ④ Dumpster Diving

7. 공개키 기반구조(PKI)의 구성요소에 대한 설명으로 가장 적절하지 않은 것은?

- ① 이용자 : 공개키 사용자는 메시지를 암호화해서 송신하거나 전자서명을 검증한다.
② 인증기관(CA) : 다른 인증기관(CA)과 상호인증을 제공한다.
③ 저장소 : 디렉터리를 관리하는 서버는 OCSP(Online Certificate Status Protocol)를 이용하여 X.500 디렉터리 서비스를 제공한다.
④ 인증기관(CA) : 인증서를 폐지하는 경우 인증기관은 인증서 폐지 목록(Certificate Revocation List, CRL)을 작성한다.

8. 다음 지문과 같은 특징을 갖는 접근통제 모델로 가장 적절한 것은?

- 무결성 중심의 상업 환경에 적합하게 설계된 모델
- 금융자산관리 및 회계분야에 주로 사용
- 체계화된 거래를 위한 접근통제 모델
- 인가자의 부적절한 정보 변조를 방지하는 직무분리를 반영

- ① BIBA 모델 ② BLP 모델
③ State Machine 모델 ④ Clark-Wilson 모델

9. 사용자 인증의 내용으로 가장 적절하지 않은 것은?

- ① 통합 인증 체계(Single Sign On, SSO)는 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보시스템에 재인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션이다.
② 일회용 패스워드(One-Time Password, OTP)의 비동기화 방식은 시간 혹은 계수기 메커니즘을 기반으로 한다.
③ 생체인증시스템 설계 시 고려 사항으로 무결성, 속도 및 처리량, 프라이버시, 위조 저항성 등이 있다.
④ 커beros(Kerberos)의 구성요소인 KDC(Key Distribution Center)는 키 분배 서버로 사전공격이 발생하고 있어도 알지 못한다.

10. 다음 지문의 리눅스 패스워드 규칙 설정 내용으로 가장 적절하지 않은 것은?

```
#cat /etc/security/pwquality.conf
minlen = 9
lcredit = -1
ucredit = -1
dcredit = -1
ocredit = -1

#cat /etc/login.defs
PASS_MAX_DAYS 90
PASS_MIN_DAYS 1
PASS_MIN_LEN 9
PASS_WARN_AGE 7
```

- ① 비밀번호는 최소 9자리 이상이어야 한다.
- ② 비밀번호는 최대 90일 변경주기를 가지고 있다.
- ③ 숫자, 소문자, 대문자는 각각 하나 이상을 포함해야 한다.
- ④ 특수문자를 사용하기 위해서는 별도의 설정값을 포함해야 한다.

11. 다음 중 버퍼 오버플로우(Buffer Overflow) 대응방법으로 가장 적절하지 않은 것은?

- ① DLP (Data Loss Prevention)
- ② ASLR (Address Space Layout Randomization)
- ③ Stack Guard
- ④ Stack Shield

12. 어떤 이미지에 작은 변화를 주어 딥러닝 네트워크가 판단할 때 결정경계(Decision Boundary)를 넘겨 잘못 인식하게 만드는 방법으로, AI 알고리즘에 내재되어 있는 취약점에 의해 발생할 수 있는 공격으로 가장 적절한 것은?

- ① Adversarial Attack ② Side Channel Attack
- ③ Bluekeep ④ Deepfake

13. 다음에서 커널의 기능으로 옳은 것을 모두 고른 것은?

```
㉠ 동기화(Synchronization)
㉡ 프로세스간 통신(Inter Process Communication)
㉢ POST(Power On Self Test)
㉣ 메시지 전달(Message Passing)
```

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

14. 유닉스/리눅스의 파일 시스템 구조 중 I-node 블록에 대한 설명으로 가장 적절하지 않은 것은?

- ① 각 파일이나 디렉터리에 대한 모든 정보를 저장한다.
- ② 모든 파일은 반드시 하나의 아이노드(I-node) 블록을 갖는다.
- ③ 전체 파일 시스템에 대한 정보를 저장한다.
- ④ 파일의 소유자, 유형, 접근권한, 접근시간, 크기, 링크 수, 저장된 블록 주소 등의 정보를 저장한다.

15. 무선 랜 통신 암호화에 대한 설명으로 가장 적절하지 않은 것은?

- ① WEP는 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용되기 시작했다.
- ② WPA-PSK는 802.11i 보안 표준의 일부분으로 WEP 방식의 보안 문제점을 해결하기 위해 만들어졌다.
- ③ WEP는 RC4 암호화 알고리즘을 기본으로 사용한다.
- ④ WPA-1은 CCMP 암호화방식을 사용하여 WEP 방식의 취약점을 해결하기 위해 제정된 표준이다.

16. 블록체인(Blockchain) 기반 기술에 대한 설명으로 가장 적절하지 않은 것은?

- ① 분산 네트워크의 경우 블록체인 정보는 네트워크에 참여하는 노드들이 가지고 있으며 동일한 거래 내역이 분산 저장되어 관리된다.
- ② 암호 기술의 경우 개인 간 거래 시 생성되는 전자서명을 검증하여 거래내역이 변경되지 않았음을 입증하는데 ECDSA 전자서명 알고리즘을 이용한다.
- ③ 이중 거래 방지의 경우 악의적인 목적으로 동시에 두 곳 이상의 계좌로 송금하는 행위를 방지하기 위해서 총 통화량과 The Longest Chain Wins 메커니즘을 이용한다.
- ④ 비트코인, 모네로 등의 채굴은 대부분 지분증명(PoS, Proof of Staking) 방식을 사용한다.

17. 다음 지문은 VLAN(Virtual LAN)에 대한 설명이다. 빈칸에 들어갈 내용을 순서대로 나열한 것은?

VLAN이란 (㉠) 트래픽을 제한하여 불필요한 트래픽을 차단하기 위한 (㉡) LAN이다. 스위치는 허브처럼 한 포트에서 발생한 데이터를 모든 포트에 전달하지 않기 때문에 스위치에 흐르는 데이터를 분석하려면 허브와는 달리 (㉢) 기능을 사용해야 한다.

- ① ㉠ 멀티캐스팅 ㉡ 논리적인 ㉢ 포트미러링
- ② ㉠ 브로드캐스팅 ㉡ 논리적인 ㉢ 포트미러링
- ③ ㉠ 멀티캐스팅 ㉡ 물리적인 ㉢ 포트필터링
- ④ ㉠ 브로드캐스팅 ㉡ 물리적인 ㉢ 포트필터링

18. APT(Advanced Persistent Threat) 침투 기법 중 드라이브-바이-다운로드(Drive-By-Download) 공격의 내용으로 가장 적절한 것은?

- ① 특정 기관의 구체적인 개인 또는 그룹을 목표로 진행되는 목표 지향적인 피싱공격이다.
- ② 공격자는 공격 대상이 주로 방문하는 웹사이트에 대한 정보를 사전에 파악한 후(사회공학적 기법) 제로데이 취약점을 이용해 해당 사이트에 악성코드를 심어두는 공격이다.
- ③ 다중 확산 메커니즘과 페이로드를 포함한 악성 소프트웨어로 목표를 오염시키는 공격이다.
- ④ 공격자는 사전에 USB 메모리에 악성코드를 삽입, 특정 타겟/조직의 이동 동선 상에 이를 방치한 후 누군가 이를 가져가서 내부 PC에 연결하는 순간 감염되게 하는 공격이다.

19. 다음 지문에서 설명하는 내용으로 가장 적절한 것은?

고객 신용정보를 훔치기 위해 POS에 침입하는 공격이다. POS 시스템의 메모리를 검사하여 악용을 목적으로 신용카드번호 및 개인식별번호와 같은 민감 개인정보를 수집한다.

- ① Free-Riding Attack ② RAM-Scraping Attack
- ③ Ransomware ④ Side Channel Attack

20. 다음 클라우드 컴퓨팅의 컨테이너 기술 중 ()안에 들어갈 내용으로 가장 적절한 것은?

단일 시스템에서 여러 운영체제가 동시에 실행될 수 있도록 하는 가상화와 달리 컨테이너는 리눅스 커널의 기능인 (㉠)와(과) (㉡)을(를) 통해 서로 다른 애플리케이션 프로세스별로 공간을 격리한다.

- ① ㉠ cgroup ㉡ namespace
- ② ㉠ cgroup ㉡ dmesg
- ③ ㉠ pacct ㉡ dmesg
- ④ ㉠ wtmp ㉡ namespace

21. 레지스트리와 관련된 내용으로 가장 적절하지 않은 것은?

- ① 레지스트리는 윈도우 운영체제의 하위 레벨 시스템 설정을 저장하는 데이터베이스로 다섯 가지의 루트키가 존재한다.
- ② 서브키 중 SAM은 윈도우 OS에서 사용자의 암호를 LM 또는 NTLM 해시 형식으로 저장하는 곳이다.
- ③ 루트키 중 HKLM키에 포함된 데이터는 시스템의 사용자 활동이나 사용자 계정에 대한 수정 여부를 확인할 수 있다.
- ④ 사고 대응자가 시스템에 연결된 USB를 발견하려면 System 레지스트리 하이브를 이용해야 한다.

22. 침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상사설망(VPN) 등 서로 다른 보안제품에서 발생하는 보안이벤트 정보를 한 곳으로 모으는 역할을 수행하는 보안관제시스템으로 가장 적절한 것은?

- ① ESM ② NMS ③ TMS ④ UTM

23. 호스트가 네트워크를 통해서 다른 장비로 데이터를 전송할 때 프로토콜 정보와 함께 데이터가 캡슐화(Encapsulation)된다고 정의한다. 다음 OSI 참조모델 전송층부터 물리층 사이의 각 계층에서 캡슐화되는 순서로 가장 적절한 것은?

- ① BIT → FRAME → PACKET → SEGMENT
- ② PACKET → FRAME → BIT → SEGMENT
- ③ SEGMENT → PACKET → BIT → FRAME
- ④ SEGMENT → PACKET → FRAME → BIT

24. IP 패킷 필드의 내용으로 가장 적절하지 않은 것은?

- ① HL : 이 필드 값에 4를 곱한 값이 실제 헤더의 바이트 길이이다.
- ② Flag(DF) : DF 값이 1이면 단편화되지 않았음을 의미한다.
- ③ Flag(MF) : MF 값이 0이면 마지막 단편이거나 유일한 단편임을 의미한다.
- ④ Protocol : IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 정의하며 ICMP, IGMP, TCP, UDP, SIP가 있다.

25. 다음 버퍼오버플로우(Buffer Overflow) 공격의 대응책 중 하나인 안전한 코딩 기법들에서 사용을 자제해야 하는 함수는 모두 몇 개인가?

가. strcpy()	나. gets()
다. vsnprintf()	라. scanf()
마. fgets()	바. strcat()

- ① 3개 ② 4개 ③ 5개 ④ 6개

26. OSI 7계층 중 데이터의 압축과 암호화 기능을 수행하는 계층으로 가장 적절한 것은?

- ① 3계층(Network Layer) ② 4계층(Transport Layer)
- ③ 5계층(Session Layer) ④ 6계층(Presentation Layer)

27. 침입탐지시스템(IDS) 중 NIDS의 내용으로 가장 적절하지 않은 것은?

- ① 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고, 어떤 작업을 했는지에 대한 기록을 남기고 추적한다.
- ② 감사와 로깅을 할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않는다.
- ③ IP 주소를 소유하지 않기 때문에 해커의 직접적인 공격은 거의 완벽하게 방어할 수 있고 존재 사실도 숨길 수 있다.
- ④ 네트워크에서 하나의 독립된 시스템으로 운영되며, 스위칭 환경에서 NIDS를 설치하려면 다른 부가 장비가 필요하다.

28. 네트워크 기반 공격 중 BONK 공격에 대한 내용으로 가장 적절한 것은?

- ① ICMP 패킷을 일반 패킷보다 훨씬 큰 크기로 보내어 네트워크를 통해 공격 대상에 전달되는 동안 패킷 하나가 ICMP 패킷 여러 개로 분할되게 하여 공격 대상 시스템에 과부하를 일으키는 공격이다.
- ② TCP의 구조적인 문제를 이용하는 공격으로, SYN 패킷만을 보내어 각 서버의 동시 가용 사용자 수를 점유하여 다른 사용자가 서버를 사용할 수 없게 만드는 공격이다.
- ③ 패킷을 프래그먼트하여 전송할 때 패킷을 조작하여 결과적으로 공격 대상 시스템의 부하를 증가시키는 공격이다.
- ④ 출발지 주소와 도착지 주소가 같은 TCP 패킷을 공격 대상 시스템에 보내 가용 사용자 수를 점유하여 시스템 부하를 증가시키는 공격이다.

29. Google Dork에 대한 설명으로 가장 적절하지 않은 것은?

- ① Google Dork은 구글을 이용한 해킹을 말한다.
- ② 구글검색엔진에서 “cache: police.ac.kr”로 검색할 경우, 해당 도메인의 캐시된 정보를 보여준다.
- ③ 구글검색엔진에서 “inurl: admin”로 검색할 경우, URL에 admin 단어가 들어가 있는 웹페이지를 보여준다.
- ④ 구글검색엔진에서 “site: police.ac.kr”로 검색할 경우, 서브도메인을 제외한 모든 도메인 리스트를 보여준다.

30. 다음은 디지털 포렌식에 있어서 전자적 증거의 분석 기술에 대한 설명이다. 아래의 설명으로 가장 적절한 것은?

저장매체 또는 하드디스크 이미지의 내부구조와 파일시스템을 확인하고 파일시스템 내부에 존재하는 파일에 대응되는 응용 프로그램 구동 없이 쉽고 빠르게 분석할 수 있는 기법이다. 복제한 이미지를 사용자가 수동으로 마운팅하여 열람할 필요가 없어 분석 시간을 줄일 수 있다. 대표적인 도구로는 EnCase, FTK, FinalForensic 등이 있다.

- ① 디스크 브라우징(Disk Browsing) 기술
- ② 데이터 뷰잉(Data Viewing) 기술
- ③ 검색 기술
- ④ Time Line 분석

31. 다음 지문에서 ㉠에 들어갈 내용으로 가장 적절한 것은?

스위치는 하나의 포트에서 여러 MAC 주소를 학습할 수 있도록 구현되어 있다. MAC 주소 테이블이 가득 차서 더 이상 MAC 주소를 학습할 수 없을 때, 그 뒤에 들어오는 모든 Frame들은 Flooding 되면서 마치 허브처럼 동작 될 수 있다. 위와 같은 공격기법을 MAC Flooding 공격이라고 한다. 이때 (㉠)를 설정하면 하나의 포트에 학습할 MAC 주소를 제한할 수 있어, 이런 공격을 방어할 수 있다. MIMT(중간자공격)에 있어서도 이 기능을 사용하면, MAC 주소를 변형하여 다른 디바이스 통신 사이에 끼어드는 ARP Spoofing도 허가된 MAC 주소로만 접속하게 제한할 수 있다.

- ① 포트시큐리티 ② 포트포워딩
- ③ 포트필터링 ④ 포트미러링

32. SQL Injection 공격에 대한 설명으로 가장 적절하지 않은 것은?

- ① 공격자가 입력값을 조작하여 원하는 SQL 구문을 실행하는 기법이다.
- ② 잠재적인 SQL 구문의 구조를 확인한 후에 적절히 실행되는 문자들의 결합을 찾을 때까지 입력값을 조작하는 방법으로 공격이 수행된다.
- ③ 공격자가 SQL 기반 게시판 등에 게시글과 함께 공격코드를 삽입하여 공격코드를 실행하도록 한 후 클라이언트의 정보를 유출하는 공격기법도 있다.
- ④ 부적절한 입력값을 전달하여 에러를 발생시켜 SQL 구문을 확인하고 이에 대한 취약점을 공격하는 기법이다.

33. 재해복구 시스템 유형별 내용으로 가장 적절하지 않은 것은?

- ① 미러 사이트 : 주 센터와 동일한 수준의 정보기술 지원을 원격지에 구축하고, 실시간 동시 서비스를 제공
- ② 핫 사이트 : 중요성이 높은 정보기술 지원만 부분적으로 재해 복구센터에 보유하고 서비스 제공 데이터는 동기적 또는 비 동기적 방식의 실시간 미러링을 통하여 최신상태 유지
- ③ 웜 사이트 : 데이터를 주기적(수 시간~1일)으로 백업하고 구축 및 유지비용이 핫 사이트에 비해 저렴
- ④ 콜드 사이트 : 데이터만 원격지에 보관하고 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보

34. 소프트웨어 안전(safety)에 대한 내용으로 가장 적절하지 않은 것은?

- ① 기능 동작 오류, 데이터 처리 오류, 소스코드 오류에 대한 장애 관련 위험원을 식별해야 한다.
- ② 소프트웨어가 동작하는 시스템으로 인해 인명피해, 시스템, 재산 등에 손실을 줄 수 있는 소프트웨어 위험요소를 확인 및 관련하여 위험이 수용 가능한 수준 이하로 유지하는 것이 소프트웨어 안전 진단의 목표이다.
- ③ 국내 소프트웨어 안전의 법적 근거는 준비 중이며, 안전진단 범위는 항공기, 기차 및 원자력 시스템들이고, 향후 자율주행차, 드론 등이 포함된다.
- ④ 미국, 유럽은 항공우주, 국방, 철도, 원자력에 대한 소프트웨어 안전을 위한 규정이 존재한다.

35. 데이터베이스 암호화 방법의 내용으로 가장 적절하지 않은 것은?

- ① Hybrid 방식은 Plug-In 방식의 단점인 배치 업무의 성능 저하를 보완하기 위해 API 방식을 이용하는 구성이다.
- ② Plug-In 방식은 암호·복호화 모듈을 DB 서버 내에 설치하고 이곳에서 암호·복호화를 수행하는 구조이다.
- ③ API 방식은 암호·복호화 모듈을 애플리케이션 서버 내에 설치하고 이곳에서 암호·복호화를 수행하는 구조로 애플리케이션의 수정을 동반한다.
- ④ 파일 암호화 방식은 DBMS에 추가 기능으로 제공되는 암호화 기능을 이용하여 DB 내부에서 데이터 파일 저장 시 암호화한다.

36. 「개인정보 보호법」상 개인정보 유출 시 개인정보처리자가 정보주체에게 알려야 할 사항으로 다음 보기에 가장 적절한 것은?

제34조(개인정보 유출 통지 등)
 ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.
 1. 유출된 (㉠)
 2. (㉡)과 그 경위
 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해 구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

- ① ㉠ 개인정보의 위탁 현황 ㉡ 개인정보 보관 기간
- ② ㉠ 정보저장매체 ㉡ 개인정보의 위탁 현황
- ③ ㉠ 개인정보의 항목 ㉡ 유출된 시점
- ④ ㉠ 정보저장매체 ㉡ 개인정보 보관 기간

37. 정보보호 관리체계(ISMS)에서는 정보보호 정책과 목적에 부합하도록 위험분석을 통해 위험을 허용 가능한 수준으로 관리한다. 이때 위험처리 방식으로 가장 적절하지 않은 것은?

- ① 수용 ② 삭제 ③ 회피 ④ 전가

38. 인터넷 뱅킹 시스템의 위험요소로 바르게 연결되지 않은 것은?
- ① 클라이언트 보안에서의 위협요소 - Virus, Trojan Horse
 - ② 서버보안에서의 위협요소 - Unix/NT Security Holes, Improper Administration
 - ③ 거래처리 보안에서의 위협요소 - Poor Programming, Weak Authentication
 - ④ 내부적인 보안에서의 위협요소 - Virus & Trojan Horse, Unix/NT Security Holes, Improper Administration

39. 운영체제에서 보안에 불필요한 부분을 모두 제거하여 모듈에 따른 분석 및 테스트가 가능한 TCSEC의 단계별 보안수준으로 가장 적절한 것은?
- ① B1 ② B2 ③ B3 ④ C1

40. 다음 「정보통신기반 보호법」 제9조(취약점의 분석·평가)에서 () 안에 들어갈 내용으로 가장 적절한 것은?

(㉠)은(는) 관계중앙행정기관의 장 및 (㉡)과(와) 협의하여 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.

- | | |
|-----------------|-----------|
| ① ㉠ 행정안전부장관 | ㉡ 국가정보원장 |
| ② ㉠ 방송통신위원장 | ㉡ 행정안전부장관 |
| ③ ㉠ 한국인터넷진흥원장 | ㉡ 행정안전부장관 |
| ④ ㉠ 과학기술정보통신부장관 | ㉡ 국가정보원장 |