정보보호론

(9급) **(1번~20번)** **Ⓑ**

1. 다음의 지문은 무엇을 설명한 것인가?

> 안전한 소프트웨어 개발을 위해 소스코드 등에 존재할 수 있는 잠재적인 보안 취약점을 제거하고, 보안을 고려하여 기능을 설계 및 구현하는 등 소프트웨어 개발 과정에서 지켜야 할 보안 활동이다.

① 시큐어코딩(Secure Coding)
② 스캐빈징(Scavenging)
③ 웨어하우스(Warehouse)
④ 살라미(Salami)

2. 다음은 TCSEC 보안등급 중 하나를 설명한 것이다. 이에 해당하는 것은?

> • 각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다.
> • 보안감사가 가능하며 특정 사용자의 접근을 거부할 수 있다.
> • 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 이에 해당한다.

① C1
② C2
③ B1
④ B2

3. 다음 중 백도어(BackDoor) 공격으로 옳지 않은 것은?
① 넷버스(Netbus)
② 백오리피스(Back Orifice)
③ 무차별(Brute Force) 공격
④ 루트킷(RootKit)

4. 다음 지문에서 설명하는 방화벽으로 옳은 것은?

> ㄱ. 다단계 보안을 제공하기 때문에 강력한 보안을 제공한다.
> ㄴ. DMZ(DeMilitarization Zone)라는 완충 지역 개념을 이용한다.
> ㄷ. 설치와 관리가 어렵고 서비스 속도가 느리다는 단점이 있다.

① 베스천 호스트(Bastion host)
② 듀얼 홈드 게이트웨이(Dual homed gateway)
③ 패킷 필터링(Packet filtering)
④ 스크린드 서브넷 게이트웨이(Screened subnet gateway)

5. 포렌식의 기본 원칙 중 증거는 획득되고, 이송/분석/보관/법정 제출의 과정이 명확해야 함을 말하는 원칙은?
① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 신속성의 원칙

6. 다음의 지문은 무엇을 설명한 것인가?

> ㄱ. 전자금융거래에서 사용되는 단말기 정보, 접속 정보, 거래 내용 등을 종합적으로 분석하여 의심 거래를 탐지하고 이상금융거래를 차단하는 시스템이다.
> ㄴ. 보안 프로그램에서 방지하지 못하는 전자금융사기에 대한 이상거래를 탐지하여 조치를 할 수 있도록 지원하는 시스템이다.

① MDM
② FDS
③ MDC
④ RPO

7. 다음 중 APT(Advanced Persistent Threat) 공격에 대한 설명 중 옳지 않은 것은?
① 사회 공학적 방법을 사용한다.
② 공격대상이 명확하다.
③ 가능한 방법을 총동원한다.
④ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.

8. 다음 중 메시지 인증 코드(MAC : Message Authentification Code)에 대한 설명 중 옳은 것은?
① 메시지 무결성을 제공하지는 못한다.
② 비대칭키를 이용한다.
③ MAC는 가변 크기의 인증 태그를 생성한다.
④ 부인 방지를 제공하지 않는다.

9. 다음 중 데이터베이스 관리자(Database Administrator)가 부여할 수 있는 SQL기반 접근권한 관리 명령어로 옳지 않은 것은?
① REVOKE
② GRANT
③ DENY
④ DROP

10. 스위칭 환경에서 스니핑(Sniffing)을 수행하기 위한 공격으로 옳지 않은 것은?
① ARP 스푸핑(Spoofing)
② ICMP 리다이렉트(Redirect)
③ 메일 봄(Mail Bomb)
④ 스위치 재밍(Switch Jamming)

11. 정부는 사이버테러를 없애기 위하여 2012년 8월 정보통신망법 시행령 개정으로 100만 명 이상 이용자의 개인정보를 보유했거나 전년도 정보통신서비스 매출이 100억 원 이상인 정보통신서비스 사업자의 경우 '망분리'를 도입할 것을 법으로 의무화했다. 다음 중 망분리 기술로 옳지 않은 것은?

① DMZ
② OS 커널분리
③ VDI
④ 가상화기술

12. 다음 지문에서 설명하는 것은?

> • 국내의 학계, 연구소, 정부 기관이 공동으로 개발한 블록 암호이다.
> • 경량 환경 및 하드웨어 구현을 위해 최적화된 Involutional SPN 구조를 갖는 범용 블록 암호 알고리즘이다.

① ARIA
② CAST
③ IDEA
④ LOKI

13. 리눅스 커널 보안 설정 방법으로 옳지 않은 것은?

① 핑(ping) 요청을 응답하지 않게 설정한다.
② 싱크 어택(SYNC Attack) 공격을 막기 위해 백로그 큐를 줄인다.
③ IP 스푸핑된 패킷을 로그에 기록한다.
④ 연결 종료 시간을 줄인다.

14. 다음 중 XSS(Cross-Site Scripting) 공격에서 불가능한 공격은?

① 서버에 대한 서비스 거부(Denial of Service) 공격
② 쿠키를 이용한 사용자 컴퓨터 파일 삭제
③ 공격대상에 대한 쿠키 정보 획득
④ 공격대상에 대한 피싱 공격

15. "「전자서명법」 제15조(공인인증서발급) 공인인증기관은 공인인증서를 발급받고자 하는 자에게 공인인증서를 발급한다."라는 조문에서 공인인증서에 포함되지 않는 것은?

① 가입자의 전자서명검증정보
② 가입자와 공인인증기관이 이용하는 전자서명 방식
③ 공인인증서의 재발급 고유번호
④ 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항

16. 다음 <보기>가 설명하는 접근제어방식은?

<보기>

> 주체나 그것이 속해 있는 그룹의 신원에 근거하여 객체에 대한 접근을 제한하는 방법으로 자원의 소유자 혹은 관리자가 보안관리자의 개입 없이 자율적 판단에 따라 접근 권한을 다른 사용자에게 부여하는 기법이다.

① RBAC
② DAC
③ MAC
④ LBAC

17. 다음은 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명이다. 이들 중 옳지 않은 것은?

① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원
② 방화벽이나 게이트웨이 등에 구현
③ IP 기반의 네트워크에서만 동작
④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능함

18. 다음의 지문은 RSA 알고리즘의 키생성 적용 순서를 설명한 것이다. ( )를 바르게 채운 것은?

> ㄱ. 두 개의 큰 소수, p와 q를 생성한다. ($p \neq q$)
> ㄴ. 두 소수를 곱하여, $n = p \cdot q$를 계산한다.
> ㄷ. (㉮)을 계산한다.
> ㄹ. $1 < A < \phi(n)$이면서 A, $\phi(n)$이 서로소가 되는 A를 선택한다. $A \cdot B$를 $\phi(n)$으로 나눈 나머지가 1임을 만족하는 B를 계산한다.
> ㅁ. 공개키로 (㉯), 개인키로 (㉰)를 각각 이용한다.

	㉮	㉯	㉰
①	$\phi(n)=(p-1)(q-1)$	$(n,\ A)$	$(n,\ B)$
②	$\phi(n)=(p+1)(q+1)$	$(n,\ B)$	$(n,\ A)$
③	$\phi(n)=(p-1)(q-1)$	$(n,\ B)$	$(n,\ A)$
④	$\phi(n)=(p+1)(q+1)$	$(n,\ A)$	$(n,\ B)$

19. 스파이웨어 주요 증상으로 옳지 않은 것은?

① 웹브라우저의 홈페이지 설정이나 검색 설정을 변경, 또는 시스템 설정을 변경한다.
② 컴퓨터 키보드 입력내용이나 화면표시내용을 수집, 전송한다.
③ 운영체제나 다른 프로그램의 보안설정을 높게 변경한다.
④ 원치 않는 프로그램을 다운로드하여 설치하게 한다.

20. 다음 설명에 해당하는 취약점 점검도구는?

> 어느 한 시점에서 시스템에 존재하는 특정경로 혹은 모든 파일에 관한 정보를 DB화해서 저장한 후 차후 삭제, 수정 혹은 생성된 파일에 관한 정보를 알려주는 툴이다. 이 툴은 MD5, SHA 등의 다양한 해시 함수를 제공하고 파일들에 대한 DB를 만들어 이를 통해 해커들에 의한 파일들의 변조여부를 판별하므로 관리자들이 유용하게 사용할 수 있다.

① Tripwire
② COPS(Computer Oracle and Password System)
③ Nipper
④ MBSA(Microsoft Baseline Security Analyzer)