

1. 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

2. 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.

3. 다음 중 메시지 인증 코드(MAC: Message Authentication 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.

4. 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

5. 스위칭 환경에서 스니핑(Sniffing)을 수행하기 위한 공격으로 옳지 않은 것은?

- ① ARP 스푸핑(Spoofing)
② ICMP 리다이렉트(Redirect)
③ 메일 폭탄(Mail Bomb)
④ 스위치 재밍(Switch Jamming)

6. 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)

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

- 각 계정별 로그인 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다.
- 보안검사가 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

8. 다음 중 백도어(BackDoor) 공격으로 옳지 않은 것은?

- ① 넷버스(Netbus)
② 백오리피스(Back Orifice)
③ 무차별(Brute Force) 공격
④ 루트킷(RootKit)

9. 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)

10. 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

