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 쉘(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