정보보호론

1. 사용자 A가 사용자 B에게 보낼 메시지에 대한 전자서명을 생성하는 데 필요한 키는?

① 사용자 A의 개인키
② 사용자 A의 공개키
③ 사용자 B의 개인키
④ 사용자 B의 공개키

2. 원본 파일에 숨기고자 하는 정보를 삽입하고 숨겨진 정보의 존재 여부를 알기 어렵게 하는 기술은?

① 퍼징(Fuzzing)
② 스캐닝(Scanning)
③ 크립토그래피(Cryptography)
④ 스테가노그래피(Steganography)

3. 다음에서 설명하는 공격 방법은?

> ○ 사람의 심리를 이용하여 보안 기술을 무력화시키고 정보를 얻는 공격 방법
> ○ 신뢰할 수 있는 사람으로 위장하여 다른 사람의 정보에 접근하는 공격 방법

① 재전송 공격(Replay Attack)
② 무차별 대입 공격(Brute-Force Attack)
③ 사회공학 공격(Social Engineering Attack)
④ 중간자 공격(Man-in-the-Middle Attack)

4. 블록 암호의 운영 모드 중 ECB 모드와 CBC 모드에 대한 설명으로 옳은 것은?

① ECB 모드는 블록의 변화가 다른 블록에 영향을 주지 않아 안전하다.
② ECB 모드는 암호화할 때, 같은 데이터 블록에 대해 같은 암호문 블록을 생성한다.
③ CBC 모드는 블록의 변화가 이전 블록에 영향을 주므로 패턴을 추적하기 어렵다.
④ CBC 모드는 암호화할 때, 이전 블록의 결과가 필요하지 않다.

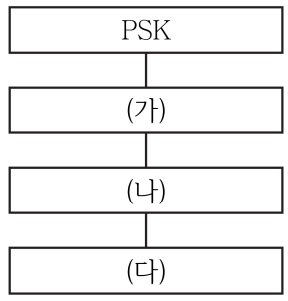
5. 컴퓨터 보안의 3요소가 아닌 것은?

① 무결성(Integrity)
② 확장성(Scalability)
③ 가용성(Availability)
④ 기밀성(Confidentiality)

6. 로컬에서 통신하고 있는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속여, 클라이언트와 서버 간에 이동하는 패킷이 공격자로 전송되도록 하는 공격 기법은?

① SYN 플러딩
② DNS 스푸핑
③ ARP 스푸핑
④ ICMP 리다이렉트 공격

7. IEEE 802.11i 키 관리의 쌍별 키 계층을 바르게 나열한 것은?



- TK(Temporal Key)
- PSK(Pre-Shared Key)
- PMK(Pairwise Master Key)
- PTK(Pairwise Transient Key)

	(가)	(나)	(다)
①	PMK	TK	PTK
②	PMK	PTK	TK
③	PTK	TK	PMK
④	PTK	PMK	TK

8. CC(Common Criteria)의 보증 요구사항(Assurance Requirements)에 해당하는 것은?

① 개발
② 암호 지원
③ 식별과 인증
④ 사용자 데이터 보호

9. 다음 /etc/passwd 파일 내용에 대한 설명으로 옳지 않은 것은?

> root(㉠) : x : 0(㉡) : 0 : root : /root(㉢) : /bin/bash(㉣)

① ㉠은 사용자 ID이다.
② ㉡은 UID 정보이다.
③ ㉢은 사용자 홈 디렉터리 경로이다.
④ ㉣은 패스워드가 암호화되어 /bin/bash 경로에 저장되어 있음을 의미한다.

10. 리눅스에서 설정된 umask 값이 027일 때, 생성된 디렉터리의 기본 접근 권한으로 옳은 것은?

① drw-r-----
② d---r--rw-
③ drwxr-x---
④ d---r-xrwx

11. 역공학을 위해 로우레벨 언어에서 하이레벨 언어로 변환할 목적을 가진 도구는?

① 디버거(Debugger)
② 디컴파일러(Decompiler)
③ 패커(Packer)
④ 어셈블러(Assembler)

12. 위험 평가 방법에 대한 설명으로 옳지 않은 것은?

① 정성적 위험 평가는 자산에 대한 화폐가치 식별이 어려운 경우 이용한다.
② 정량적 분석법에는 델파이법, 시나리오법, 순위결정법, 브레인스토밍 등이 있다.
③ 정성적 분석법은 위험 평가 과정과 측정기준이 주관적이어서 사람에 따라 결과가 달라질 수 있다.
④ 정량적 위험 평가 방법에 의하면 연간 기대 손실은 위협이 성공했을 경우의 예상 손실액에 그 위협의 연간 발생률을 곱한 값이다.

13. 「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)에 따라 개인정보처리자가 정해야 하는 '개인정보 처리방침'에 포함되는 사항이 아닌 것은?

① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
④ 개인정보처리자의 성명 또는 개인정보를 활용하는 부서의 명칭과 전화번호 등 연락처

14. 「개인정보 보호법」 제4조(정보주체의 권리)에 따른 정보주체의 권리가 아닌 것은?

① 개인정보의 처리에 관한 정보를 제공받을 권리
② 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
③ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리
④ 완전히 자동화된 개인정보 처리에 따른 결정을 승인하거나 그에 대한 회복 등을 요구할 권리

15. 증거물의 "획득 → 이송 → 분석 → 보관 → 법정 제출" 과정에 대한 추적성을 보장하기 위하여 준수해야 하는 원칙은?

① 연계 보관성의 원칙
② 정당성의 원칙
③ 재현의 원칙
④ 무결성의 원칙

16. 128비트 키를 이용한 AES 알고리즘 연산 수행에 필요한 내부 라운드 수는?

① 10 ② 12
③ 14 ④ 16

17. SSL에서 기밀성과 메시지 무결성을 제공하기 위해 단편화, 압축, MAC 첨부, 암호화를 수행하는 프로토콜은?

① 경고 프로토콜
② 레코드 프로토콜
③ 핸드셰이크 프로토콜
④ 암호 명세 변경 프로토콜

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에서 정보보호지침에 포함되어야 하는 사항으로 명시적으로 규정한 것이 아닌 것은?

① 정보통신망연결기기등의 정보보호를 위한 물리적 보호조치
② 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

19. 다음에서 설명하는 ISMS-P의 단계는?

> ○ 조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.
> ○ 관리체계 전 영역에 대한 정보서비스 및 개인정보 처리 현황을 분석하고 업무 절차와 흐름을 파악하여 문서화하며, 이를 주기적으로 검토하여 최신성을 유지하여야 한다.
> ○ 위험 평가 결과에 따라 식별된 위험을 처리하기 위하여 조직에 적합한 보호대책을 선정하고, 보호대책의 우선순위와 일정·담당자·예산 등을 포함한 이행계획을 수립하여 경영진의 승인을 받아야 한다.

① 위험 관리 ② 관리체계 운영
③ 관리체계 기반 마련 ④ 관리체계 점검 및 개선

20. 디지털 콘텐츠의 불법 복제와 유포를 막고 저작권 보유자의 이익과 권리를 보호해 주는 기술은?

① PGP(Pretty Good Privacy)
② IDS(Intrusion Detection System)
③ DRM(Digital Rights Management)
④ PIMS(Personal Information Management System)