정보보호론

1. 악성 코드(malware)에 대한 설명으로 옳지 않은 것은?
   ① 바이러스는 다른 프로그램에 자신을 복제하여 악의적 목적을 수행한다.
   ② 랜섬웨어는 사용자의 파일을 암호화하여 자료를 인질로 잡고 금전을 요구한다.
   ③ 웜은 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램이다.
   ④ 트로이목마는 정상적인 프로그램으로 위장하여 자기 복제를 통해 다른 시스템으로 확산한다.

2. 대칭키 암호 알고리즘에 대한 설명으로 옳지 않은 것은?
   ① 암호화/복호화 속도는 공개키 암호보다 빠르다.
   ② 키의 길이가 공개키 암호보다 상대적으로 짧다.
   ③ 공개키는 암호화에 사용하고 개인키는 복호화에 사용한다.
   ④ 사용자의 증가에 따라 관리해야 할 키의 수가 비례적으로 늘어난다.

3. (가) ~ (라)에 들어갈 용어를 바르게 연결한 것은?

구분	메시지 인증 코드	전자서명
송신자	(가)로 MAC값을 계산	(나)로 서명을 작성
수신자	(다)로 MAC값을 계산	(라)로 서명을 검증

	(가)	(나)	(다)	(라)
①	공유키	공개키	공유키	개인키
②	개인키	공유키	공개키	공유키
③	공유키	개인키	공유키	공개키
④	개인키	공유키	공유키	공개키

4. 디지털 포렌식에 대한 설명으로 옳지 않은 것은?
   ① 디지털 포렌식 과정에서 획득한 모든 증거는 법적 효력을 가진다.
   ② 수집된 증거가 결함이 없이 위·변조되지 않았음을 증명할 수 있어야 한다.
   ③ 동일한 조건과 동일한 상황이라면 디지털 포렌식의 분석 결과는 항상 같은 결과가 나와야 한다.
   ④ 증거를 획득한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정 및 각 과정의 담당자가 명확해야 하며 이에 대한 추적이 가능해야 한다.

5. 암호화 알고리즘에 대한 설명으로 옳은 것은?
   ① DES는 56비트 키를 사용하는 대칭키 암호 알고리즘이다.
   ② AES는 국내에서 개발된 블록 암호 알고리즘으로 국제 표준이 되었다.
   ③ SEED는 3개의 키값을 사용하고 DES의 3배인 168비트의 보안 강도를 제공한다.
   ④ RSA는 큰 소수의 곱을 인수분해하기 어렵다는 수학적 원리에 기반한 대칭키 암호 알고리즘이다.

6. 국내 국가보안기술연구소 주도로 개발된 암호화 알고리즘은?
   ① DES
   ② ARIA
   ③ RC5
   ④ IDEA

7. 사용자가 입력한 키보드 정보를 가로채는 방법은?
   ① 피싱(phishing)
   ② 파밍(pharming)
   ③ 스미싱(smishing)
   ④ 키로깅(keylogging)

8. 인증에 대한 설명으로 옳지 않은 것은?
   ① 패스워드는 길이가 길고 대소문자, 숫자, 특수문자를 조합할수록 무차별 대입 공격에 대한 안전성이 높아진다.
   ② 생체 인증은 신체적 특성을 이용하므로 원천적으로 복제가 불가능하여 별도의 보안 대책이 필요하지 않다.
   ③ SSO(Single Sign On)는 한 번의 인증으로 다수의 시스템에 접근할 수 있게 하는 인증 시스템이다.
   ④ OTP(One Time Password)는 한 번 생성되면 그 인증값이 임시적으로 한 번에 한해서만 유효하며, 시간 동기화, 이벤트 동기화, 챌린지·응답 등의 방식으로 생성된다.

9. 공격자가 공격대상의 IP주소로 위장하여 브로드캐스팅 방식을 통해 ICMP echo request를 다수의 호스트에 전송하는 공격은?
   ① Smurf
   ② SYN Flooding
   ③ ARP Spoofing
   ④ ICMP Redirect

10. 허니팟(honeypot)에 대한 설명으로 옳지 않은 것은?
   ① 허니팟은 공격자에게 쉽게 노출되어야 한다.
   ② 허니팟은 쉽게 해킹이 가능한 것처럼 취약해 보이게 한다.
   ③ 허니넷(honeynet)은 여러 허니팟을 포함한 네트워크를 의미한다.
   ④ 허니팟은 시스템을 통과하는 패킷에 대해 일부분만을 샘플링하여 감시한다.

11. 정보시스템의 접근 제어(access control) 또는 로그 관리에 대한 설명으로 옳지 않은 것은?
   ① 인증(authentication)은 자신의 신원(identity)을 증명하기 위하여 행하는 과정이다.
   ② 감사 추적(audit trail)은 시스템의 위험을 평가하고 비용 대비 효과적인 대응책을 수립하는 과정이다.
   ③ 인가(authorization)는 인증된 주체에게 자원에 대한 접근 권한을 부여하거나 제한하는 과정이다.
   ④ 책임 추적성(accountability)은 시스템에 접근한 주체가 어떤 행동을 하였는지 기록하여 필요 시 그 행위자를 추적할 수 있게 한다.

12. 영국이 제정한 정보보호 관리체계 표준은?

① BS7799 ② FISMA

③ PIMS ④ NIST 800-53

13. 버퍼 오버플로 공격에 대한 설명으로 옳지 않은 것은?

① 버퍼에 정해진 크기 이상의 데이터를 입력하여 프로그램을 공격하는 행위이다.

② 버퍼 오버플로에 취약한 함수(strcpy(), strcat() 등)는 사용하지 않는 것이 좋다.

③ 메모리 공격을 방어하려고 주소 공간 배치를 난수화하는 기법을 스택 가드(stack guard)라 한다.

④ 세그멘테이션 폴트(segmentation fault)가 발생했을 때 버퍼 오버플로 공격을 의심할 수 있다.

14. 보안 요소 중 인가된 사용자에게만 정보에 접근할 수 있도록 허용하는 것은?

① 가용성(availability)

② 무결성(integrity)

③ 기밀성(confidentiality)

④ 부인방지(non-repudiation)

15. 정량적 위험 분석 방법에 해당하는 것은?

① 델파이법

② 시나리오법

③ 순위결정법

④ 과거자료 분석법

16. CSRF(Cross-Site Request Forgery) 공격에 대한 설명으로 옳은 것은?

① 쿠키를 변조한 후 불법적인 인증을 거쳐 권한을 획득하는 공격이다.

② 악성 URL을 보내서 클릭 시 피해자의 정보를 유출하는 공격이다.

③ 입력 값에 대한 유효성을 검증하지 않고 그대로 사용할 때 발생할 수 있는 데이터베이스 공격이다.

④ 로그인된 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 하는 공격이다.

17. 「개인정보 보호법」상 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 문서에 포함되어야 하는 내용이 아닌 것은?

① 개인정보의 기술적·관리적 보호조치에 관한 사항

② 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

③ 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항

④ 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항

18. 「개인정보 보호법」상 가명정보의 처리에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 없다.

② 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

③ 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

④ 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

19. 「개인정보 보호법」상 영업양도 등에 따른 개인정보의 이전 시 해당 정보주체에게 미리 알려야 하는 사항에 해당하지 않는 것은?

① 개인정보의 수집 출처

② 개인정보를 이전하려는 사실

③ 개인정보를 이전받는 자의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처

④ 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

20. 다음에서 설명하는 네트워크 공격 기술은?

> 신뢰 관계에 있는 두 개의 호스트 사이에서 하나의 시스템을 마비시킨 후 마치 자신이 신뢰관계에 있는 호스트인 것처럼 속이는 것이다.

① DNS Spoofing

② IP Spoofing

③ Switch Jamming

④ Teardrop