정보보호론

1. 사용자 A가 사용자 B에게 보내는 메시지 M의 해시값을 A와 B가 공유하는 비밀키로 암호화하고 이를 M과 함께 보냄으로써 보장하려는 것은?
   ① 무결성
   ② 기밀성
   ③ 가용성
   ④ 부인방지

2. 서비스 거부 공격에 해당하지 않는 것은?
   ① Smurf 공격
   ② Slowloris 공격
   ③ Pharming 공격
   ④ HTTP GET 플러딩 공격

3. (가)와 (나)에 들어갈 용어를 바르게 연결한 것은?

traceroute 명령어는 (가) 시스템에서 사용되며 (나) 기반으로 구현된다.

(가)	(나)
① Windows	IGMP
② Windows	TCP
③ Linux	HTTP
④ Linux	ICMP

4. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?
   ① 대칭키 암호와 공개키 암호의 장점을 조합한 방법이다.
   ② 메시지의 기밀성과 세션키의 기밀성을 제공한다.
   ③ 송신자의 공개키를 이용하여 메시지를 암호화한다.
   ④ 수신자의 공개키를 이용하여 세션키를 암호화한다.

5. 암호학적 해시 함수 H에 대한 설명으로 옳은 것은?
   ① 임의의 크기의 데이터 블록 x에 대해서 가변적 길이의 해시값 H(x)를 생성한다.
   ② 주어진 h로부터 h = H(x)인 x를 찾는 것은 계산적으로 불가능하다.
   ③ 임의의 크기의 데이터 블록 x에 대해 H(x)를 구하는 계산은 어려운 연산이 포함되어 계산이 비효율적이다.
   ④ H(x) = H(y)를 만족하는 서로 다른 x, y는 존재하지 않는다.

6. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?
   ① 네트워크를 이용한 인증 프로토콜이다.
   ② 세션키를 분배하는 데 사용될 수 있다.
   ③ 세션키를 이용하여 데이터의 기밀성을 제공할 수 있다.
   ④ 버전 5에서는 비표(nonce)를 사용하지 않기 때문에 재생(replay) 공격에 취약하다.

7. 포트 스캔 방식 중에서 포트가 열린 서버로부터 SYN+ACK 패킷을 받으면 로그를 남기지 않기 위하여 RST 패킷을 보내 즉시 연결을 끊는 스캔 방식은?
   ① TCP Half Open 스캔
   ② UDP 스캔
   ③ NULL 스캔
   ④ X-MAS 스캔

8. 패스워드를 저장할 때 솔트(salt)를 사용함으로써 얻을 수 있는 이점이 아닌 것은?
   ① 시스템 내에 같은 패스워드를 쓰는 사용자가 복수로 존재한다는 것을 발견하지 못하게 한다.
   ② 오프라인 사전(dictionary) 공격을 어렵게 한다.
   ③ 사용자가 같은 패스워드를 여러 시스템에서 중복해서 사용하여도 그 사실을 발견하기 어렵게 한다.
   ④ 패스워드 파일에 솔트가 암호화된 상태로 저장되므로 인증 처리 시간을 단축시킨다.

9. 다음에서 설명하는 보안 공격은?

사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생하는 것으로, 공격자가 악의적으로 질의에 포함시킨 특수 문자를 제대로 필터링하지 않으면 데이터베이스 자료가 무단으로 유출·변조될 수 있다.

   ① 버퍼 오버플로우
   ② SQL 삽입
   ③ XSS
   ④ CSRF

10. 「개인정보 보호법 시행령」에서 규정한 민감정보에 해당하지 않는 것은? (단, 공공기관이 관련 규정에 따라 해당 정보를 처리하는 경우는 제외한다)
    ① 유전자검사 등의 결과로 얻어진 유전정보
    ② 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
    ③ 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아보지 못하도록 일정한 기술적 수단을 통해 생성한 정보
    ④ 인종이나 민족에 관한 정보

11. DNS 스푸핑 공격에 대한 설명으로 옳지 않은 것은?
    ① 위조된(spoofed) DNS 응답을 보내 공격자가 의도한 웹 사이트로 사용자의 접속을 유도하는 공격이다.
    ② 일반적으로 DNS 질의는 TCP 패킷이므로 공격자는 로컬 DNS 서버가 인터넷의 DNS 서버로부터 응답을 얻기 위해 설정한 TCP 세션을 하이재킹해야 한다.
    ③ 위조된 응답이 일반적으로 로컬 DNS 서버에 의해 캐시되므로 손상이 지속될 수 있는데 이를 DNS 캐시 포이즈닝이라고 한다.
    ④ 디지털 서명으로 DNS 데이터의 진위 여부를 확인하는 DNSSEC는 DNS 캐시 포이즈닝에 대처하도록 설계되었다.

12. (가)와 (나)에 들어갈 내용을 바르게 연결한 것은?

> 하트블리드(Heartbleed)는 [(가)]를 구현한 공개 소프트웨어인 OpenSSL의 심각한 보안 취약점으로, 수신한 요청 메시지의 실제 [(나)]을/를 제대로 확인하지 않은 것에 기인한 것이다.

	(가)	(나)
①	SSH	길이
②	SSH	유형
③	TLS	길이
④	TLS	유형

13. 정보보호제품 평가·인증제도에 대한 설명으로 옳지 않은 것은?

① 정보보호제품 평가·인증제도는 「지능정보화 기본법」 제58조(정보보호시스템에 관한 기준 고시 등)에 근거한다.

② 인증기관은 국가보안기술연구소이다.

③ 「정보보호시스템 공통평가기준」은 최고의 평가보증등급인 EAL 1부터 최저의 평가보증등급인 EAL 7까지 보증등급을 정의하고 있다.

④ 보호 프로파일은 정보보호시스템이 사용될 환경에서 필요한 보안 기능 및 보증 요구사항을 공통평가기준에 근거하여 서술한 것이다.

14. 소켓은 통신의 한 종점을 추상화한 것으로, 통신 상대를 식별하기 위한 것이다. TCP 연결을 위한 소켓 정의에 사용되는 것은?

① MAC 주소, IP 주소

② IP 주소, Port 번호

③ Port 번호, URL

④ URL, MAC 주소

15. 개인정보 보호위원회의 「가명정보 처리 가이드라인」(2024. 2.)에 있는 정형데이터 가명처리 기술로 다음에서 설명하는 암호화 기법은?

> ○ 암호화된 상태에서의 연산이 가능한 암호화 방식으로 원래의 값을 암호화한 상태로 연산 처리를 하여 다양한 분석에 이용 가능한 기술이다.
> ○ 암호화된 상태의 연산값을 복호화하면 원래의 값을 연산한 것과 동일한 결과를 얻을 수 있는 4세대 암호화기법이다.

① 동형 암호화(homomorphic encryption)

② 다형성 암호화(polymorphic encryption)

③ 순서보존 암호화(order-preserving encryption)

④ 형태보존 암호화(format-preserving encryption)

16. 「개인정보 보호법」에서 규정하고 있는 사항이 아닌 것은?

① 개인정보의 수집·이용

② 위치정보사업자의 개인위치정보 제공

③ 고정형 영상정보처리기기의 설치·운영 제한

④ 개인정보 처리방침의 수립 및 공개

17. 다음은 「OECD 프라이버시 프레임워크」(2013)에서 제시한 개인정보 보호 원칙을 설명한 것이다. (가)와 (나)에 해당하는 것을 A ~ D에서 바르게 연결한 것은?

> (가) 개인 데이터의 수집에는 제한이 있어야 하고 그러한 정보는 적법하고 공정한 방법에 의해 얻어져야 하며, 정보주체의 적절한 인지 또는 동의가 있어야 한다.
> (나) 개인 데이터는 사용목적과 관계가 있어야 하고 그 목적에 필요한 한도 내에서 정확하고, 완전하며, 최신의 것이어야 한다.

> A. 수집 제한의 원칙(collection limitation principle)
> B. 목적 명확화의 원칙(purpose specification principle)
> C. 데이터 품질 원칙(data quality principle)
> D. 개인 참여의 원칙(individual participation principle)

	(가)	(나)
①	A	B
②	A	C
③	D	B
④	D	C

18. ISMS-P의 보호대책 요구사항 중 '외부자 보안' 인증 항목에 해당하지 않는 것은?

① 보호 구역 지정

② 외부자 현황 관리

③ 외부자 보안 이행 관리

④ 외부자 계약 변경 및 만료 시 보안

19. NIST 표준(FIPS 186)인 전자서명 표준(DSS)에 대한 설명으로 옳지 않은 것은?

① DSA(Digital Signature Algorithm)는 DSS에서 명세한 알고리즘으로 ElGamal과 Schnorr에 의해 제안된 기법을 기반으로 한다.

② 서명자는 공개키와 개인키의 쌍을 생성하고 검증에 필요한 매개변수들을 공개해야 한다.

③ 서명 과정을 거치고 나면 두 개의 요소로 이루어진 서명이 생성되는데 서명자는 이를 메시지와 함께 수신자(검증자)에게 보낸다.

④ 검증 과정에서 검증자는 서명으로부터 추출한 값과 수신한 메시지로부터 얻은 해시값을 비교하여 일치하는가를 확인함으로써 서명을 검증한다.

20. 「개인정보 보호법」 제31조(개인정보 보호책임자의 지정 등)에서 규정한 개인정보 보호책임자의 수행 업무가 아닌 것은?

① 개인정보 보호 계획의 수립 및 시행

② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

③ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

④ 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항