정보보호론

1. 전자서명의 활용 사례로 적합하지 않은 것은?

① 인증서 로그인을 통해 사용자의 신원을 증명한다.
② 다운로드하는 소프트웨어의 위변조 여부를 확인한다.
③ 이메일 내용이 중간 메일서버에 노출되지 않도록 한다.
④ 웹브라우저로 통신하는 서버의 사이트가 유효한지 검증한다.
⑤ 폐기된 인증서들을 모아서 인증서 폐기 목록(CRL)을 발행한다.

2. NAC(Network Access Control) 시스템의 기능이 아닌 것은?

① PC 및 네트워크 장치 통제
② 데이터 패킷 암호화
③ 접근 제어
④ 해킹, 웜, 유해 트래픽 탐지 및 차단
⑤ 접근 인증

3. X.509 인증서를 구성하는 필드에 대한 설명으로 옳지 않은 것은?

① Version: 현재 사용 중인 X.509의 버전 정보
② Serial number: 인증기관이 부여한 고유번호
③ Issuer name: 인증서를 발급한 인증기관 식별 정보
④ Subject name: 공개키의 소유자 정보
⑤ Signature: 공개키 소유자가 생성한 서명 정보

4. 다음 프로그램이 취약한 공격 유형은?

```
#define BUFSIZE 256
int main(int argc, char **argv) {
  char *buf;
  buf = (char *)malloc(sizeof(char)*BUFSIZE);
  strcpy(buf, argv[1]);
}
```

① 스택 버퍼 오버플로우 공격
② 힙 버퍼 오버플로우 공격
③ 포맷 스트링 공격
④ 정수 오버플로우 공격
⑤ 레이스 컨디션 공격

5. 대칭키 암호 운영모드로서 평문 블록 $(P_1, P_2, \ldots, P_n)$을 암호화하는 CBC(Cipher Block Chaining) 모드에 대한 설명으로 옳은 것만을 <보기>에서 모두 고르면?

<보 기>

ㄱ. 평문이 달라지면 초기벡터는 매번 새롭게 랜덤으로 생성된다.
ㄴ. 평문 블록이 동일하면 대응하는 암호문 블록도 동일하다.
ㄷ. P_2에 발생한 에러는 P_2블록 이후의 모든 암호화 과정에 파급된다.
ㄹ. 암호화 과정은 평문 블록 P_1부터 P_n까지 순차적으로 진행된다.
ㅁ. 암호화 및 복호화를 하는데 암호화 알고리즘만 있어도 된다.

① ㄱ, ㄴ, ㄹ
② ㄱ, ㄴ, ㅁ
③ ㄱ, ㄷ, ㄹ
④ ㄴ, ㄷ, ㄹ
⑤ ㄷ, ㄹ, ㅁ

6. TLS(Transport Layer Security) 프로토콜에서 TLS 세션을 처음 시작할 때 클라이언트와 서버 간에 안전한 연결을 위하여 상호 인증을 수행하고 암호 메커니즘의 정보를 교환하여 세션키를 생성하는 하부 프로토콜은?

① One Time Password 프로토콜
② Secure Electronic Transaction 프로토콜
③ Handshake 프로토콜
④ Document Object Model 프로토콜
⑤ Change Cipher Spec 프로토콜

7. 이메일 보안을 위하여 사용하는 PGP(Pretty Good Privacy)에 대한 설명으로 옳지 않은 것은?

① 송신 부인방지는 지원하지만 수신 부인방지는 미지원
② 기밀성 제공을 위하여 대칭키 방식과 공개키 방식 사용
③ 인증받을 메시지나 파일에 전자서명을 생성, 확인 작업을 수행
④ 이메일 어플리케이션에 플러그인 기능으로 확장 불가능
⑤ 공개키에는 RSA 버전과 Diffie-Hellman 버전이 존재

8. 리눅스 시스템에서 사용자 로그인 실패 정보가 저장되는 파일은?

① btmp
② extmp
③ wtmp
④ utmp
⑤ atmp

9. 최근 발생한 보안 위협에 대한 설명으로 옳은 것은?

① 블루킵(Bluekeep): 원격 데스크톱 서비스를 인증 없이 조작할 수 있는 취약점

② 다크웹(Dark Web): 피싱 메일을 통해 유포되며 금융정보 탈취를 시도하는 악성코드

③ 딥페이크(Deepfake): 특정 웹브라우저를 통해 익명성이 보장되는 인터넷 영역

④ 이모텟(Emotet): 한글로 작성된 메일 내부에 정상파일로 위장한 랜섬웨어

⑤ 소디노키비(Sodinokibi): 인공지능을 기반으로 실제처럼 조작한 음성, 영상 등을 통칭함

10. 암호화폐를 주고 받는 블록체인 네트워크에 대한 설명으로 옳지 않은 것은?

① 거래 내역들의 최상위 해시값은 머클 루트(Merkle Root)로서 블록 헤더에 포함된다.

② 채굴(Mining)은 주어진 난이도에 따라 해시값의 역상을 구하는 과정이다.

③ 공개키의 해시값이 암호화폐를 주고 받는 주소값으로 사용된다.

④ 블록체인 내의 원장을 수정하기 위해서는 개인키를 사용해야 한다.

⑤ 이중 지불을 방지하기 위해 송신자는 자신의 주소값에 대응하는 전자서명을 생성한다.

11. 대칭키 암호에 대한 설명으로 옳지 않은 것은?

① 부인방지 기능을 제공한다.

② 비대칭키 암호에 비해 속도가 빠르다.

③ 송신자와 수신자가 동일한 비밀키를 사용한다.

④ IDEA는 대칭키 암호 알고리즘이다.

⑤ RC4는 스트림 암호 알고리즘이다.

12. OSI 7계층 중 2계층 암호화 프로토콜로 짝지어진 것은?

① PPTP - SSL

② PPTP - IPSec

③ L2TP - IPSec

④ L2TP - SSL

⑤ PPTP - L2TP

13. 다음 설명에서 제시하는 접근 제어 정책은?

> 주체 또는 소속 그룹의 아이디(ID)에 근거하여 객체에 대한 접근 제한을 설정한다. 객체별로 세분화된 접근 제어가 가능하고, 유연한 접근 제어 서비스를 제공할 수 있어 다양한 환경에서 폭넓게 사용되고 있다.

① 강제적 접근 제어(Mandatory Access Control)

② 규칙 기반 접근 제어(Rule Based Access Control)

③ 역할 기반 접근 제어(Role Based Access Control)

④ 임의적 접근 제어(Discretionary Access Control)

⑤ 래티스 기반 접근 제어(Lattice Based Access Control)

14. 전자서명 알고리즘 중 하나인 ECDSA(Elliptic Curve Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?

① 타원곡선 상에서 이산대수 문제가 어렵다는 사실에 안전성의 근거를 두고 있다.

② 서명할 메시지를 해싱(Hashing)한 후 그 해시값을 ECDSA 서명 알고리즘에 입력한다.

③ 동일한 비도에서 RSA 전자서명보다 공개키 길이가 짧고 복호화가 빠르다는 장점을 갖는다.

④ 블록체인 환경에서 거래의 진위 여부를 검증하기 위해 사용된다.

⑤ 서명 생성 시 사용되는 난수는 메시지에 관계없이 동일하게 사용해야 안전하다.

15. Bob이 Alice의 공개키를 인증하는 과정이다. 순서대로 나열한 것은?

> ㄱ. Alice는 자신의 공개키와 인증서를 Bob에게 전송한다.
> ㄴ. Alice는 자신의 공개키를 인증기관에 보낸다.
> ㄷ. Bob은 인증기관의 공개키로 Alice의 인증서를 검증한다.
> ㄹ. Alice는 자신의 공개키와 개인키를 생성한다.
> ㅁ. 인증기관은 Alice의 공개키에 대응하는 인증서를 발급한다.

① ㄹ - ㄱ - ㄴ - ㄷ - ㅁ

② ㄹ - ㄴ - ㄷ - ㄱ - ㅁ

③ ㄹ - ㄴ - ㅁ - ㄱ - ㄷ

④ ㅁ - ㄹ - ㄱ - ㄷ - ㄴ

⑤ ㅁ - ㄹ - ㄷ - ㄱ - ㄴ

16. OWASP(Open Web Application Security Project) 2020에서 발표된 10가지 보안 위협에 속하지 않는 것은?

① Abuse of Cloud Computing
② Injection
③ XML External Entities
④ Broken Authentication
⑤ Sensitive Data Exposure

17. IPsec 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① IPsec 설정 시 송·수신자가 상대방의 IP 주소를 입력해야 한다.
② 전송모드는 원래의 IP 헤더에 새로운 IP 헤더를 추가한다.
③ ESP 프로토콜은 IP 패킷을 암호화하고 무결성까지 보장할 수 있다.
④ IKE 프로토콜은 인증된 Diffie-Hellman 키 교환 방식을 사용한다.
⑤ VPN(Virtual Private Network)을 구성하는 한 가지 방법이다.

18. 리눅스 서버에 저장된 first 파일의 접근 권한을 다음과 같이 설정하기 위한 명령어는?

rwsr—r—	1	test	test	8980	4월 18	14:18	first

① chmod 1644 first
② chmod 1744 first
③ chmod 2744 first
④ chmod 4644 first
⑤ chmod 4744 first

19. 2020년 8월 5일 개정된 「개인정보 보호법」에 대한 설명으로 옳지 않은 것은?

① 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부 등을 고려하여 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 없도록 함
② 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정개인을 알아볼 수 없도록 처리하는 것을 가명처리로 정의함
③ 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있도록 함
④ 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행하도록 함
⑤ 개인정보처리자는 가명정보를 처리하는 경우 해당 정보가 분실, 도난, 유출, 위조, 변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적 및 물리적 조치를 하도록 함

20. 다음 설명에서 제시하는 공격 유형은?

> 게시판의 글에 원본과 함께 악성 코드를 삽입하여 글을 읽을 경우 악성코드가 실행되도록 하여 클라이언트의 정보를 유출하는 공격기법이다. 웹 페이지가 사용자로부터 입력 받은 데이터를 필터링하지 않고 그대로 동적으로 생성된 웹 페이지에 포함하여 사용자에게 재전송할 때 발생한다.

① SQL Injection
② XSS(Cross Site Scripting)
③ 파일 업로드 취약점
④ CSRF(Cross Site Request Forgery)
⑤ 쿠키/세션 위조