정보보호론

1. TCP SYN flood 공격에 대해 가장 바르게 설명한 것은?
   ① 브로드캐스트 주소를 대상으로 공격
   ② TCP 프로토콜의 초기 연결설정 단계를 공격
   ③ TCP 패킷의 내용을 엿보는 공격
   ④ 통신과정에서 사용자의 권한 탈취를 위한 공격
   ⑤ TCP 패킷의 무결성을 깨뜨리는 공격

2. 다음 중 로봇프로그램과 사람을 구분하는 방법의 하나로 사람이 인식할 수 있는 문자나 그림을 활용하여 자동 회원 가입 및 게시글 포스팅을 방지하는데 사용하는 방법은?
   ① 해쉬함수 ② 캡차(CAPTCHA)
   ③ 전자서명 ④ 인증서
   ⑤ 암호문

3. Bell-LaPadula 보안 모델은 다음 중 어느 요소에 가장 많은 관심을 가지는 모델인가?
   ① 비밀성(Confidentiality)
   ② 무결성(Integrity)
   ③ 부인방지(Non-repudiation)
   ④ 가용성(Availability)
   ⑤ 인증(Authentication)

4. 네트워크의 OSI 3계층 주소(IP 주소)와 연관된 2계층 주소(MAC 주소)를 틀리게 알려주어서 정보를 가로채는 데에 활용되는 공격기법은?
   ① Smurf 공격 ② Teardrop 공격
   ③ DDoS 공격 ④ ARP Spoofing 공격
   ⑤ Phishing 공격

5. 다음 중 사이버 환경에서 사용자 인증의 수단으로 가장 적절하지 않은 것은?
   ① 패스워드 ② 지문
   ③ OTP(One Time Password) ④ 보안카드
   ⑤ 주민등록번호

6. 다음 중 소인수 분해 문제의 어려움에 기초한 암호 알고리즘은 무엇인가?
   ① Diffie-Hellman
   ② SHA-1
   ③ AES
   ④ DES
   ⑤ RSA

7. 인터넷 뱅킹 등에서 숫자를 화면에 무작위로 배치하여 마우스나 터치로 비밀번호를 입력하게 하는 가상 키보드의 사용목적으로 가장 적절한 것은?
   ① 키보드 오동작 방지
   ② 키보드 입력 탈취에 대한 대응
   ③ 데이터 입력 속도 개선
   ④ 비밀번호의 무결성 보장
   ⑤ 해당 서비스의 가용성 보장

8. 다음 NTFS 파일시스템에 대한 설명 중 옳지 않은 것은?
   ① 파티션에 대한 접근 권한 설정이 가능함
   ② 사용자별 디스크 사용공간 제어 가능
   ③ 기본 NTFS 보안 변경 시 사용자별 NTFS 보안 적용 가능
   ④ 미러(Mirror)와 파일 로그가 유지되어 비상 시 파일 복구 가능
   ⑤ 파일에 대한 압축과 암호화를 지원하지 않음

9. '정보통신망 이용촉진 및 정보보호 등에 관한 법률'은 정보통신망의 안전성을 확보하기 위한 목적으로 정보보호 최고책임자의 업무를 규정하고 있다. 다음 중 정보보호 최고책임자의 업무에 해당되지 않은 것은?
   ① 보안서버 적합성 검토
   ② 사전 정보보호대책 마련
   ③ 침해사고의 예방 및 대응
   ④ 정보보호 관리체계의 인증 심사
   ⑤ 정보보호 사전 보안성 검토

10. 다음 설명에 해당하는 정보보호 평가 기준은?

- 국제적으로 통용되는 제품 평가 기준
- 현재 ISO 표준으로 제정되어 있음
- 일반적인 소개와 일반 모델, 보안기능 요구사항, 보증 요구사항 등으로 구성되어 있음

① CC
② BS 7799
③ ITSEC
④ TCSEC
⑤ TNI

11. 웹 쿠키에 대한 설명으로 가장 옳지 않은 것은?

① 웹 서비스 사용자의 PC 저장소에 저장됨
② 웹 서비스의 세션을 유지하는데 사용될 수 있음
③ 서버에서 웹 서비스 사용자의 접근 기록을 추적할 수 있음
④ 쿠키는 Java Script 같은 웹 개발언어를 통해서는 접근이 불가함
⑤ 상태정보를 저장하지 않는 HTTP를 보완하기 위한 기술임

12. 다음은 '전자서명법'에서 공인인증기관의 업무수행에 관한 조항이다. 괄호 안에 들어갈 말은?

(　　)은 인증업무의 안전성과 신뢰성 확보를 위하여 공인인증기관이 인증업무 수행에 있어 지켜야 할 구체적 사항을 전자서명인증업무지침으로 정하여 고시할 수 있다.

① 미래창조과학부 장관
② 개인정보보호위원장
③ 국가정보원장
④ 산업통상자원부 장관
⑤ 공정거래위원장

13. 커버로스(Kerberos)에 대한 설명 중 맞는 것은?

① 커버로스는 공개키 암호를 사용하기 때문에 확장성이 좋다.
② 커버로스 서버는 서버인증을 위해 X.509 인증서를 이용한다.
③ 커버로스 서버는 인증서버와 티켓발행서버로 구성된다.
④ 인증서버가 사용자에게 발급한 티켓은 재사용 할 수 없다.
⑤ 커버로스는 two party 인증 프로토콜로 사용 및 설치가 편리하다.

14. 다음은 공격자가 남긴 C 프로그램 파일과 실행 파일에 관한 정보이다. 제시된 정보로부터 유추할 수 있는 공격으로 가장 적합한 것은?

```
$ ls -l
total 20
-rwsr-xr-x 1 root root  12123 Sep 11 11:11 util
-rw-rw-r-- 1 root root     70 Sep 11 11:11 util.c
$ cat util.c
#include <stdlib.h>
void main()
{
    setuid(0);
    setgid(0);
    system("/bin/bash");
}
```

① Eavesdropping 공격
② Brute Force 공격
③ Scanning 공격
④ Backdoor 공격
⑤ 패스워드 유추 공격

15. 다음 중 공인인증서에 포함되지 않은 것은?

① 가입자의 이름
② 가입자의 전자서명 검증정보
③ 공인인증기관의 서명키
④ 공인인증서의 일련번호
⑤ 공인인증서의 유효기간

16. 사진이나 텍스트 메시지 속에 데이터를 잘 보이지 않게 은닉하는 기법으로서, 9.11 테러 당시 테러리스트들이 그들의 대화를 은닉하기 위해 사용한 기법은?

① 전자서명
② 대칭키 암호
③ 스테가노그라피(Steganography)
④ 영지식 증명
⑤ 공개키 암호

17. 다음은 정보보호의 3대 기본 목표 중 무엇에 대한 설명인가?

권한이 없는 사용자들은 컴퓨터 시스템 상의 데이터 또는 컴퓨터 시스템 간에 통신 회선을 통하여 전송되는 데이터의 내용을 볼 수 없게 하는 기능

① 비밀성(Confidentiality)
② 가용성(Availability)
③ 신뢰성(Reliability)
④ 무결성(Integrity)
⑤ 책임추적성(Accountability)

18. 다음 중 전자 상거래를 위한 신용카드 기반의 전자지불 프로토콜은?

① SSL(Secure Socket Layer)
② PGP(Pretty Good Privacy)
③ OTP(One Time Password)
④ SSO(Single Sign On)
⑤ SET(Secure Electronic Transaction)

19. 정보보호를 위해 사용되는 해쉬함수(Hash function)에 대한 설명 중 옳지 않은 것은?

① 주어진 해쉬값에 대응하는 입력값을 구하는 것이 계산적으로 어렵다.
② 무결성을 제공하는 메시지 인증코드(MAC) 및 전자서명에 사용된다.
③ 해쉬값의 충돌은 출력공간이 입력공간보다 크기 때문에 발생한다.
④ 동일한 해쉬값을 갖는 서로 다른 입력값들을 구하는 것이 계산적으로 어렵다.
⑤ 입력값의 길이가 가변이더라도 고정된 길이의 해쉬값을 출력한다.

20. 대칭키 암호에 대한 설명으로 옳지 않은 것은?

① 공개키 암호 방식보다 암호화 속도가 빠르다.
② 비밀키 길이가 길어질수록 암호화 속도는 빨라진다.
③ 대표적인 대칭키 암호 알고리즘으로 AES, SEED 등이 있다.
④ 송신자와 수신자가 동일한 비밀키를 공유해야 된다.
⑤ 비밀키 공유를 위해 공개키 암호 방식이 사용될 수 있다.