정보보호론

문 1. 전자 서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은?
① 근원 인증
② 메시지 기밀성
③ 메시지 무결성
④ 부인 방지

문 2. AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은?
① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.
② Feistel 구조로 구성된다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.
④ 2001년에 국제표준화기구인 IEEE가 공표하였다.

문 3. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?
① 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.
② 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.
③ 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.
④ IDS는 방화벽처럼 내부와 외부 네트워크 경계에 위치해야 한다.

문 4. RSA 암호 알고리즘에서 두 소수, $p=17$, $q=23$과 키 값 $e=3$을 선택한 경우, 평문 $m=8$에 대한 암호문 c로 옳은 것은?
① 121 ② 160
③ 391 ④ 512

문 5. IEEE 802.11i RSN(Robust Security Network)에 대한 설명으로 옳은 것은?
① TKIP는 확장형 인증 프레임워크이다.
② CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.
③ EAP는 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다.
④ 802.1X는 무결성 보장을 위해 CBC-MAC를 이용한다.

문 6. CC(Common Criteria) 인증 평가 단계를 순서대로 바르게 나열한 것은?

가. PP(Protection Profile) 평가
나. ST(Security Target) 평가
다. TOE(Target Of Evaluation) 평가

① 가→나→다
② 가→다→나
③ 나→가→다
④ 다→나→가

문 7. SQL 삽입 공격에 대한 설명으로 옳지 않은 것은?
① 사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생한다.
② 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.
③ 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용한 것이다.
④ 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.

문 8. 유닉스/리눅스의 파일 접근 제어에 대한 설명으로 옳지 않은 것은?
① 접근 권한 유형으로 읽기, 쓰기, 실행이 있다.
② 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정할 수 있다.
③ 파일 접근 권한 변경은 파일에 대한 쓰기 권한이 있으면 가능하다.
④ SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.

문 9. IPSec에 대한 설명으로 옳지 않은 것은?
① 전송(transport) 모드에서는 전송 계층에서 온 데이터만을 보호하고 IP 헤더는 보호하지 않는다.
② 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.
③ 보안상 안전한 채널을 만들기 위한 보안 연관(Security Association)은 양방향으로 통신하는 호스트 쌍에 하나만 존재한다.
④ 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용한다.

문 10. 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 명시된 것으로 옳지 않은 것은?
① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.
② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
③ 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.
④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기할 수 있다.

문 11. 인증기관이 사용자의 공개키에 대한 인증을 수행하기 위해 X.509 형식의 인증서를 생성할 때 서명에 사용하는 키는?

① 인증기관의 공개키
② 인증기관의 개인키
③ 사용자의 개인키
④ 인증기관과 사용자 간의 세션키

문 12. 하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?

① 메시지는 대칭 암호 방식으로 암호화한다.
② 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성한다.
③ 생성된 세션키는 무결성 보장을 위하여 공개키 암호 방식으로 암호화한다.
④ 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다.

문 13. 해시함수의 충돌저항성을 위협하는 공격 방법은?

① 생일 공격
② 사전 공격
③ 레인보우 테이블 공격
④ 선택 평문 공격

문 14. 블록 암호 운용 모드에 대한 설명으로 옳지 않은 것은?

① CFB는 블록 암호화를 병렬로 처리할 수 없다.
② ECB는 IV(Initialization Vector)를 사용하지 않는다.
③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.
④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.

문 15. 「개인정보 보호법」상 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우
② 공공기관의 장이 허가한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 시설안전 및 화재 예방을 위하여 필요한 경우

문 16. SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는 데 악용될 수 있는 명령어는?

① HELO
② MAIL FROM
③ RCPT TO
④ VRFY

문 17. 다음 법 조문의 출처는?

> 제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

① 국가정보화 기본법
② 개인정보 보호법
③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률
④ 정보통신산업진흥법

문 18. 위조된 출발지 주소에서 과도한 양의 TCP SYN 패킷을 공격 대상 시스템으로 전송하는 서비스 거부 공격에 대응하기 위한 방안의 하나인, SYN 쿠키 기법에 대한 설명으로 옳은 것은?

① SYN 패킷이 오면 세부 정보를 TCP 연결 테이블에 기록한다.
② 요청된 연결의 중요 정보를 암호화하고 이를 SYN-ACK 패킷의 응답(acknowledgment) 번호로 하여 클라이언트에게 전송한다.
③ 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다.
④ TCP 연결 테이블에서 연결이 완성되지 않은 엔트리를 삭제하는 데까지의 대기 시간을 결정한다.

문 19. ISO/IEC 27001:2013 보안관리 항목을 PDCA 모델에 적용할 때, 점검(check)에 해당하는 항목은?

① 성과평가(performance evaluation)
② 개선(improvement)
③ 운영(operation)
④ 지원(support)

문 20. 다음에서 설명하는 블록체인 합의 알고리즘은?

> ○ 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생시킨다는 문제를 해결하기 위한 대안으로 등장하였다.
> ○ 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다.
> ○ 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.

① Paxos
② PoW(Proof of Work)
③ PoS(Proof of Stake)
④ PBFT(Practical Byzantine Fault Tolerance)