정 보 보 호 론 (9급)

(과목코드 : 141)

2023년 군무원 채용시험　　응시번호 :　　성명 :

1. 정보보호의 기본 목표 중 아래에 대한 설명으로 가장 적절한 것은?

> - 허락된 사용자는 자산, 서비스를 적절하고 신뢰성 있게 이용할 수 있어야 한다.
> - 이것을 보존하기 위해 행해지는 활동으로는 백업, 시스템 및 네트워크 용량 증설, 침입 탐지 시스템 운용 등이 있다.

① 기밀성　② 무결성
③ 가용성　④ 인증성

2. 다음 중 자체적으로 실행되면서 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성코드는?
① 루트킷　② 바이러스
③ 웜　④ 트로이목마

3. 다음 중 강제적 접근 제어 모델에 대한 설명으로 가장 적절하지 않은 것은?
① 접근 권한이 시스템의 전체적인 보안 정책 및 관련 규칙에 따라 결정된다.
② 주체와 객체의 수가 증가함에 따라 규칙의 수도 기하급수적으로 증가하는 문제가 있다.
③ 시스템의 모든 주체와 객체가 보안 레이블을 반드시 갖는다.
④ 기밀문서가 엄격히 다루어지는 군이나 정보기관 등에 적합하다.

4. 다음 중 정상적인 프로그램으로 위장하여 사용자로 하여금 실행을 유도하는 악성 프로그램은?
① 트로이목마　② 백도어
③ 루트킷　④ 셸코드

5. 다음 중 이산대수 문제를 효율적으로 풀 수 있다면 깨지는 알고리즘은?
① AES　② RSA
③ Diffie-Hellman　④ SHA

6. 다음 중 인터넷과 같은 공중망에 터널을 형성하고 이를 통해 패킷을 캡슐화하여 전달함으로써 사설망과 같은 전용 회선처럼 사용할 수 있게 하는 기술에 해당하지 않는 것은?
① PPTP　② L2TP
③ ICMP　④ IPSec

7. 다음 위험 분석 중 가장 기본적이고 일반적인 수준에서 보안 통제 항목의 구현 여부를 조사하는 접근법은?
① 상세 접근법(Detailed Risk Analysis)
② 기준 접근법(Baseline Approach)
③ 비정형 접근법(Informal Approach)
④ 통합 접근법(Combined Approach)

8. 다음 대칭키 운영 모드 중 보안성이 가장 높은 방법으로, 각 블록은 이전 암호문과 XOR 연산 후에 암호화되며 한 블록에서 발생한 에러가 다음 블록들에 영향을 주기 때문에 병렬 처리가 불가능한 특징을 갖는 것은?
① ECB　② CBC
③ CFB　④ CTR

9. RSA 암호 시스템에서 밥이 앨리스의 공개키 (e, N) = (7, 143)을 취득하여 앨리스에게 평문 9를 암호화하여 보내고자 한다. 이때 전송되는 암호문은?
① $9^7 \bmod 143$　② $7^9 \bmod 143$
③ $143^7 \bmod 9$　④ $7^{143} \bmod 9$

10. SSL/TLS 프로토콜이 보안을 제공하는 계층은?
① 물리 계층　② 데이터링크 계층
③ 네트워크 계층　④ 전송 계층

11. 다음 중 커버로스(Kerberos)에 대한 설명으로 가장 적절하지 않은 것은?
① 신뢰받는 제3자인 키 배포 기관이 개입하여 각 구성원을 인증하고 구성원들 사이에 세션 키를 발급한다.
② 세션키는 공개키 알고리즘을 통해 구현된다.
③ 커버로스는 세션키를 기반으로 티켓 기반 인증 기법을 제공한다.
④ 티켓 발급 서버가 사용자에게 서비스를 받는 데 필요한 티켓을 발급한다.

12. 윈도우를 비롯한 시스템 내 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM에 대한 설명으로 가장 적절하지 않은 것은?
① 난수 발생, 키 생성 및 저장, 해시값 생성, 암호화 및 전자서명을 한다.
② TPM은 인증 키를 내장한 상태로 공장에서 출고된다.
③ 운영체제 부팅 과정에서 인증을 통해 신뢰성을 확보한다.
④ 명령어 처리 과정에서 운영체제에 의존한다.

13. ARP 스푸핑 공격으로 인한 피해를 막기 위한 방안으로 가장 적절하지 않은 것은?
① MAC 주소를 정적으로 바꾼다.
② ARP 캐시의 내용이 바뀌면 관리자에게 경고 메시지를 보낸다.
③ Snort와 같은 침입 탐지 시스템을 활용한다.
④ 방화벽을 이용하여 ARP 패킷에 대해 임계값을 설정한다.

14. 다음 중 802.11 무선 랜 보안이 제공하지 않는 것은?
① 전자서명 ② 인증
③ 키 교환 ④ 보호 데이터 전송

15. 다음 중 리버스 엔지니어링이 사용되는 분야에 해당하지 않는 것은?
① 취약점 분석 ② 악성코드 분석
③ 버그 수정 ④ 컴파일

16. 다음 중 XSS 공격이 수행되는 순서를 옳게 나열한 것은?

가. 공격자는 XSS 코드를 포함한 게시판의 글을 웹 서버에 저장한다.
나. 웹 사용자는 공격자가 작성해 놓은 XSS 코드를 포함한 게시판의 글에 접근한다.
다. XSS 코드를 포함한 게시판의 글이 웹 서버에서 사용자에게 전달된다.
라. 사용자 시스템에서 XSS 코드가 실행된다.
마. 공격 결과가 공격자에게 전달된다.

① 가-나-다-라-마
② 가-다-나-라-마
③ 가-나-라-다-마
④ 가-라-나-다-마

17. 두 사용자가 사전에 대칭키를 교환하지 않았다고 가정할 때, 다음 중 인증 및 키 교환 과정을 수행할 수 있는 방법으로 가장 적절하지 않은 것은?
① 공개키 암호
② 전자서명과 Diffie-Hellman의 조합
③ 공개키 암호와 Diffie-Hellman의 조합
④ 전자서명과 해시함수의 조합

18. 다음 중 대칭키 암호 알고리즘인 AES(Advanced Encryption Standard)에 대한 설명으로 가장 적절하지 않은 것은?
① 운영모드 중 CTR 모드로는 사용이 쉽지만 CBC 모드로는 사용이 어렵다.
② 메시지를 128비트열의 블록들로 나누는 메시지 패딩이 필요하다.
③ 보안 강도에 따라 128, 192, 256비트열의 키를 사용할 수 있다.
④ 각 보안 강도에 따라 AES 내부 라운드 함수의 동작 수가 달라진다.

19. 다음 중 이 권한이 설정되어 있는 파일을 사용자가 실행하면 일시적으로 사용자의 권한이 아닌 파일 소유자(특히 관리자)의 권한으로 실행되기 때문에 공격에 많이 사용되는 것은?
① SetUID ② SetGID
③ Sticky bit ④ UID

20. 다음 중 '정보보호시스템 공통평가기준'에 대한 설명으로 가장 적절하지 않은 것은?
① 보안목표명세서는 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.
② 보호프로파일은 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말한다.
③ 평가보증등급은 공통평가기준에서 미리 정의된 보증수준을 가지는 보증 컴포넌트로 이루어진 패키지를 말한다.
④ 클래스는 보호프로파일, 보안목표명세서에 포함될 수 있는 보안요구사항의 가장 작은 선택 단위로서 엘리먼트의 모음을 말한다.

21. 다음 중 클라이언트-서버 간 동작하는 TLS (Transport Layer Security) v1.2 프로토콜에 대한 설명 중 가장 적절하지 않은 것은?
① 서버는 암호 조합들(cipher suites)을 ClientHello 메시지로 전송한다.
② 서버인증 및 키 교환을 위해 Handshake 프로토콜을 수행한다.
③ 애플리케이션 층(Layer)의 데이터는 Record 프로토콜을 이용해서 암호화된다.
④ 서버가 전송한 인증서를 통해 클라이언트는 서버를 인증한다.

22. 다음 중 이메일 보안을 위한 PGP(Pretty Good Privacy)에 대한 설명으로 가장 적절하지 않은 것은?
① PGP는 Web of Trust 개념으로 신뢰된 인증기관 없이 인증한다.
② PGP의 공개키 암호 및 전자서명 기법은 X.509 형식을 따라야 한다.
③ 별도의 PGP 프로그램을 설치하고 기존의 이메일 시스템과 함께 사용한다.
④ 이메일 본문뿐만 아니라 첨부파일까지 비밀성 및 무결성을 보장할 수 있다.

23. 다음 중 사용자 인증서를 이용하여 인증서버에 로그인하는 경우에 대한 설명 중 가장 적절하지 않은 것은?
① 사용자 인증서는 인증서버도 신뢰하는 인증기관에서 발급받은 것이어야 한다.
② 인증서버는 사용자와 도전-응답 프로토콜을 수행해서 사용자를 인증한다.
③ 사용자 인증서에 대응하는 개인키는 인증서버에 보관하고 인증할 때마다 요청한다.
④ 사용자는 키보드 보안 및 개인 방화벽에 필요한 파일을 추가적으로 설치할 수 있다.

24. 다음 중 메시지 인증 코드(MAC: Message Authentication Code)와 전자서명을 비교한 설명으로 가장 적절하지 않은 것은?
① MAC와 전자서명 모두 메시지의 무결성을 보장하려는 경우 사용할 수 있다.
② MAC은 대칭키 환경에서 사용하고, 전자서명은 공개키 환경에서 사용한다.
③ 전자서명과는 다르게 MAC은 부인방지(Non-repudiation) 기능을 제공한다.
④ 대표적인 MAC 기법으로 CBC-MAC과 HMAC이 사용된다.

25. 다음 중 대칭키 암호에 대한 공격 모델 설명으로 가장 바르게 연결된 것은?
① Ciphertext-Only Attack: 선택한 암호문에 대응하는 평문을 획득하여 공격
② Known-Plaintext Attack: 전송되는 암호문만을 획득하여 공격
③ Chosen-Plaintext Attack: 선택한 평문에 대응하는 암호문을 획득하여 공격
④ Chosen-Ciphertext Attack: 알려진 평문에 대응하는 암호문을 획득하여 공격