정 보 보 호 론 (7급)

(과목코드 : 141)

2021년 군무원 채용시험　　응시번호 :　　성명 :

1. 정보보호의 요구사항으로서 가용성(availability)에 대한 설명으로 가장 옳지 않은 것은?
   ① 허락된 사용자가 정보 자산에 접근하려 할 때 방해받지 않도록 하는 것이다.
   ② 서비스거부(DoS) 공격은 가용성을 해치는 공격이다.
   ③ 가용성을 유지하려면 다수의 사용자에 대한 동시적 서비스가 이루어지게 해야 한다.
   ④ 가용성을 위한 네트워크 관리 대책은 현재의 인가 수준을 모든 사람에게 유지시키는 것이다.

2. 개인정보처리자의 정보보호 원칙에 대한 설명으로 가장 옳지 않은 것은?
   ① 개인정보에 관한 개발, 운용 및 정책에 관해서는 비공개 정책을 취해야 한다.
   ② 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 해야 한다.
   ③ 개인정보의 처리 목적에 필요한 범위에서 최소한의 개인정보만을 정당하게 수집해야 한다.
   ④ 개인정보를 수집하는 것을 원칙적으로 제한하여, 개인정보를 수집할 때는 정보 주체에게 동의를 구해야 한다.

3. 디지털 포렌식에서 연계 보관성의 원칙에 대한 설명으로 가장 옳은 것은?
   ① 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 한다.
   ② 법정에 증거를 제출하기 위해서는 똑같은 환경에서 같은 결과가 나와야 한다.
   ③ 수집된 정보는 각 단계를 거치는 과정에서 위조·변조되어서는 안 되며, 이런 사항을 매번 확인해야 한다.
   ④ 증거를 획득하고 이송·분석·보관·법정 제출하는 일련의 과정이 명확해야 하고 이런 과정에 대한 추적이 가능해야 한다.

4. 네트워크형 기반의 공개키 구조 시스템에 대한 설명으로 가장 옳지 않은 것은?
   ① 유연하며 실질적인 신뢰 관계에 적합하다.
   ② 루트 인증기관의 비밀키 노출 시 복구가 어렵다.
   ③ 사용자는 최소한 자신에게 인증서를 발행한 인증기관(CA)을 신뢰한다.
   ④ 사용자가 공개키 기반 구조의 다른 사용자들에게 서명검증을 보장하는 단일 인증 경로를 제공할 수 없다.

5. 침입탐지 유형에서 비정상행위 탐지 방법으로 가장 옳지 않은 것은?
   ① 신경망 방식
   ② 통계적 접근 방식
   ③ 상태 전이 분석 방식
   ④ 전문가 시스템 방식

6. 커버로스(kerberos) 인증 기술에 대한 설명으로 가장 옳지 않은 것은?
   ① 대칭키 암호화 체계를 사용한다.
   ② 각각의 부분들과 키 분배 센터와의 사이에 동등한 관계가 존재한다.
   ③ 클라이언트가 요구하는 통신망의 다른 객체들에게 그 클라이언트를 인증해 준다.
   ④ 인증을 위한 패스워드의 사용을 허용하지만 네트워크상에서 패스워드가 전송될 필요가 없다.

7. DoS(Denial of Service)의 공격유형으로 옳지 않은 것은?
   ① buffer overflow 공격
   ② smurf 공격
   ③ land 공격
   ④ TCP SYN flooding 공격

8. 다음은 특정 악성소프트웨어에 대한 설명이다. 적절한 악성소프트웨어로 옳은 것은?

> 공격자의 접근을 허용할 목적으로 컴퓨터에 자기 자신을 설치하는 악성코드로, 통상적으로 공격자가 보안접속 절차를 거치지 않고 컴퓨터에 접속해 로컬 시스템에서 명령어를 실행할 수 있게 한다.

① 좀비(zombie)
② 웜(worm)
③ 백도어(backdoor)
④ 플러더(flooders)

9. 다음에서 설명하는 데이터베이스 암호화 방식으로 가장 옳은 것은?

> - DBMS에 내장 또는 옵션으로 제공되는 암호화 기능을 이용하는 방식이다.
> - 응용 프로그램에 대한 수정이 없고 인덱스의 경우 DBMS 자체 인덱스 기능과 연동이 가능하다.
> - DB 내부에서 암·복호 처리를 하는 방식이다.

① TDE 방식
② API 방식
③ Plug-In 방식
④ Hybrid 방식

10. 침입차단 시스템에서 배스천 호스트(bastion host)에 대한 설명으로 가장 옳지 않은 것은?
① 침입차단 시스템의 주 서버로 사용된다.
② 보안 정책에 따라 사용자 계정 설정과 접근 권한 설정 기능 등을 수행한다.
③ 사용자의 접속내역과 사용내역을 기록하여 감사 추적을 위한 근거를 제시한다.
④ 내부 네트워크와 외부 네트워크 사이에서 프로토콜 및 데이터를 중계하는 역할을 수행한다.

11. AES의 내부 구조로 가장 옳지 않은 것은?
① S박스 계층(S-box layer)
② 확산 계층(diffusion layer)
③ 키 덧셈 계층(key addition layer)
④ 바이트 대치 계층(byte substitution layer)

12. 방화벽(Firewall)의 구축형태 중 Screening Router의 특징에 대한 설명으로 가장 옳지 않은 것은?
① 3계층과 4계층에서 실행되며 IP 주소와 포트에 대한 접근통제가 가능하다.
② 라우터에서 구현된 펌웨어의 수준으로는 제한점이 없고 복잡한 정책을 구현하기 쉽다.
③ 네트워크 수준의 IP 데이터그램에서는 출발지 주소 및 목적지 주소에 의한 스크린 기능이 있다.
④ TCP/UDP 수준의 패킷에서는 포트 번호에 의한 스크린, 프로토콜별 스크린 기능이 있다.

13. 네트워크 해킹 공격 중 land 공격의 대응책에 대한 설명으로 가장 옳은 것은?
① 타임아웃 시간을 줄인다.
② 일회용 패스워드 시스템을 사용한다.
③ 큰 패킷 전송을 제한하도록 설정된 ping 프로그램의 패치를 설치해야 한다.
④ 네트워크 내의 라우터가 내부 IP 주소를 발신지로 갖는 외부 패킷을 차단하도록 한다.

14. APT(Advanced Persistent Threat)에 대한 설명으로 가장 옳지 않은 것은?
① 정보를 수집한 후 공격 대상을 정한다.
② 기존에 알려지지 않았던 취약점을 다양하게 활용하여 이루어진다.
③ 공격자가 다양한 첨단 보안 위협을 이용해 특정 기업의 네트워크에 공격을 가한다.
④ 특정 조직 내부 직원의 컴퓨터를 장악한 후 그 컴퓨터를 통해 다른 컴퓨터나 서버의 중요 정보를 빼온다.

15. 정보통신기반 보호법에서 명시한 주요정보통신기반시설의 취약점을 분석·평가할 수 있는 기관으로 옳지 않은 것은?
① 한국인터넷진흥원
② 한국전자통신연구원
③ 정보통신기반 보호법 제16조의 규정에 의한 정보공유·분석센터
④ 정보보호산업의 진흥에 관한 법률 제23조에 따라 지정된 정보공유·분석센터

16. 다음은 SSL(Secure Socket Layer)의 프로토콜 스택에 대한 설명이다. 해당하는 SSL 프로토콜로 옳은 것은?

- 기밀성과 메시지 무결성 제공을 위하여 클라이언트와 서버 간의 약속된 절차에 따라 메시지에 대한 단편화, 압축, 메시지 인증코드 생성 및 암호화 과정 등을 수행한다. - 메시지 단편화 및 압축 시 상대와 합의한 알고리즘을 사용한다. - 압축한 단편과 메시지 인증코드를 합치고 그것을 대칭 암호화한다.

① alert protocol
② record protocol
③ handshake protocol
④ change cipher spec protocol

17. 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)에 명시된 개인정보 처리방침의 필수 항목으로 옳지 않은 것은?
① 개인정보의 처리 목적
② 개인정보의 처리 및 보유 기간
③ 개인정보의 제3자 제공에 관한 사항
④ 정보주체의 권리·의무 및 그 행사방법에 관한 사항

18. 이메일 보안을 위해 사용되는 보안 기술로만 묶인 것으로 가장 옳은 것은?
① SET, S/MIME
② PEM, PGP
③ S/MIME, IDS
④ PGP, SSO

19. 다음에서 설명하는 데이터베이스 접근통제 방법으로 가장 옳은 것은?

- 데이터베이스 서버에 접근제어를 설치하는 방식이다. - 데이터베이스에 직접 접근하는 전용 클라이언트를 포함해 모든 접근 루트를 제어할 수 있다. - 데이터베이스 서버에 트래픽을 발생시켜 서버의 성능 저하가 우려된다.

① 에이전트 방법
② 게이트웨이 방법
③ 스니핑 방법
④ 하이브리드 방법

20. 사용자의 X.509 인증서 생성 시, 인증기관이 사용자 인증서 내의 사용자 공개키에 대한 신뢰성을 제공하기 위해 서명에 사용하는 키는?
① 사용자의 개인키
② 사용자의 공개키
③ 인증기관의 개인키
④ 인증기관의 공개키

21. ARIA 암호 알고리즘에 대한 설명으로 가장 옳지 않은 것은?
① 128비트 블록 암호 알고리즘이다.
② 페이스텔 암호(feistel cipher) 구조를 따른다.
③ 키의 길이는 128, 192, 256 비트를 지원한다.
④ 키의 길이로 128 비트를 사용하면 라운드 수는 12이다.

22. 개인정보보호법에 명시된 개인정보 보호책임자의 수행업무에 대한 설명으로 옳지 않은 것은?

① 개인정보 처리와 관련한 불만의 처리 및 피해 구제

② 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선

③ 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 취득

④ 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축

23. 접근 통제 보안 모델에서 비바(biba) 모델에 대한 설명으로 가장 적절한 것은?

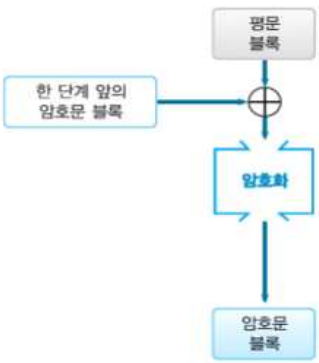
① 허가되지 않은 방식의 접근을 방지한다.

② 시스템 내의 활동에 관계없이 시스템이 스스로를 보호하고 불안정한 상태가 되지 않도록 한다.

③ 무결성에 초점을 두고 비인가자들의 데이터 변형 방지만 취급한다.

④ 한 보안 수준에서 실행된 명령과 활동은 타 보안 수준의 주체와 객체에 영향을 주지 않음을 보장한다.

24. 다음 그림이 나타내는 블록암호 운영모드로 옳은 것은?



① ECB(Electronic CodeBook)

② CFB(Cipher FeedBack)

③ CBC(Cipher Block Chaining)

④ CTR(Counter)

25. 다음은 특정 무선 네트워크 보안 프로토콜에 대한 설명이다. 적절한 무선 네트워크 보안 프로토콜로 옳은 것은?

- WEP 방식의 보안 취약점을 해결하기 위한 대안으로 만들어진 프로토콜이다. - WEP 보다 훨씬 강화된 암호화 세션을 제공한다. - AP에 접속하는 사용자마다 같은 암호화키를 사용한다는 점이 보안상 미흡하다.

① EAP ② TKIP

③ IEEE 802.11i ④ WPA-PSK