

정 보 보 호 론 (9 급)

(과목코드 : 141)

2022년 군무원 채용시험

응시번호 :

성명 :

- | | |
|---|---|
| <p>1. 다음 중 개인정보의 자기결정권에 대한 설명으로 가장 옳은 것은?</p> <ul style="list-style-type: none">① 개인정보를 수집하는 경우에, 처리목적 달성에 필요한 최소한의 개인정보만을 수집해야 하는 책임② 특정개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 처리중지, 회수·파기해야 하는 의무③ 개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보를 해야 하는 책임④ 자신에 관한 정보가 언제, 어떻게, 어느 범위까지 수집, 이용, 공개될 수 있는지를 정보주체가 스스로 통제, 결정할 수 있는 권리 <p>2. 다음 중 접근제어 원칙으로 옳지 않은 것은?</p> <ul style="list-style-type: none">① 통신규약② 최소 권한③ 알 필요성④ 직무 분리 <p>3. 다음 중 대칭키와 비대칭키에 대한 설명으로 가장 옳은 것은?</p> <ul style="list-style-type: none">① 대칭키: 빠른 처리 속도 비대칭키: 키 교환의 장점② 대칭키: 암호화 및 복호화 키가 같음 비대칭키: 3개 이상의 키가 필요③ 대칭키: 키 교환의 어려움 비대칭키: MD5(Message-Digest 5) 알고리즘④ 대칭키: DES(Data Encryption Standard) 알고리즘 비대칭키: 개인키 및 공개키 모두 공개 | <p>4. 다음 중 랜섬웨어에 대한 설명으로 가장 옳지 않은 것은?</p> <ul style="list-style-type: none">① 인질의 몸값을 나타내는 'ransom'과 'software'의 합성어② 파일 암호화로 피해자는 파일의 읽기 및 실행 불가③ 백업과 같은 사전대비가 중요④ 24시간 후 복호화는 가능하나 많은 양의 정보 손실 발생 <p>5. 다음 중 정보보호 서비스 개념으로만 묶인 것으로 가장 옳은 것은?</p> <ul style="list-style-type: none">① 은닉성, 보안성, 다형성② 가용성, 기밀성, 부인방지③ 무결성, 효율성, 인증④ 대응성, 보호성, 소유성 <p>6. 다음 중 문서의 무결성 비교를 위하여 사용되는 해시 값(함수)의 성질에 대한 설명으로 가장 옳지 않은 것은?</p> <ul style="list-style-type: none">① 입력되는 가변의 데이터에 대해서 고정 길이의 해시 값이 발생한다.② 입력되는 데이터가 다르면 해시 값도 다르다.③ 해시 값 복호화를 위해서는 대칭키 알고리즘만 가능하다.④ 해시 값으로부터 원래의 데이터 복구가 불가능하다. |
|---|---|

7. 다음 중 개인정보의 가명처리에 대한 설명으로 가장 옳은 것은?

- ① 개인정보의 정당한 사용을 위하여 개인정보 소유자에게 권한을 위임받아 안전성 확보를 위한 행위를 처리하는 것
- ② 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것
- ③ 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 것
- ④ 개인정보의 수집 및 이용 목적의 범위를 넘어 정보를 제공받는 자의 이익을 위하여 위해 업무를 처리하는 것

8. 다음 중 리눅스에서 제공하는 방화벽 메커니즘과 호스트기반 접근 제어 시스템의 조합으로 옳은 것은?

- ① IPLogger, Wireshark
- ② IPtables, TCP Wrapper
- ③ Scanner, Sniffer
- ④ Portmap, Snort

9. 다음 중 인증시스템의 주요 기능인 인증을 제공하는 인증 수단과 예제로 가장 옳지 않은 것은?

- ① 알고 있는 것: 패스워드
- ② 자신의 신체: 홍채
- ③ 문제 및 계산: 인공 지능
- ④ 가지고 있는 것: 공인(공동) 인증서

10. 다음 중 블록체인 네트워크의 합의 알고리즘에 대한 공격으로 가장 옳은 것은?

- ① 51% 공격
- ② 코인 Flooding 공격
- ③ 지갑 파밍 공격
- ④ 2:8 공격

11. 다음 중 컴퓨터 바이러스에 대한 설명으로 가장 옳지 않은 것은?

- ① 원시형: 단순하게 자기복제 기능과 데이터 파괴 기능만을 가지고 있다.
- ② 은폐형: 바이러스 코드를 암호화하여 코드를 은닉한 바이러스이다.
- ③ 다형성: 프로그램이 실행될 때마다 바이러스 코드를 변경한다.
- ④ 매크로: 주로 오피스 프로그램의 매크로 기능을 통해 감염된다.

12. 다음 중 포렌식으로 증거를 획득할 때 지켜야 할 기본 원칙에 대한 설명으로 가장 옳지 않은 것은?

- ① 정당성의 원칙: 모든 증거는 적법한 절차를 거쳐서 얻은 것이어야 한다.
- ② 신속성의 원칙: 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속해야 한다.
- ③ 연계 보관성의 원칙: 증거를 획득한 뒤에는 이송, 분석, 보관, 법정제출이라는 일련의 과정이 명확해야 한다.
- ④ 무결성의 원칙: 수집된 증거는 경찰 및 검찰이 관여한 경우에만 변경 가능하다.

13 RSA 공개키 암호에서 2개의 소수 $p=3$ 와 $q=7$ 가 주어지고 복호화 키(d) 5로 고정했을 때, 암호화 키(e)값과 메시지 2에 대한 암호문 값(C)은?

- ① $e = 3$, $C = 5$
- ② $e = 4$, $C = 7$
- ③ $e = 5$, $C = 11$
- ④ $e = 6$, $C = 15$

14. 미국 NIST가 표준으로 제정한 AES(Advanced Encryption Standard) 암호의 특징으로 가장 옳지 않은 것은?

- ① 평문과 암호문의 크기가 128비트인 블록 암호이다.
- ② 키는 128비트, 192비트, 256비트 중 선택하여 사용한다.
- ③ Substitution-and-Permutation Network 형태의 암호 체계이다.
- ④ Weak Key가 존재한다.

15. 다음 중 내부자 공격 등을 방지하는 영지식 증명 기법의 조건에 가장 해당하지 않는 성질은?

- ① 완전성(completeness)
- ② 정당성(soundness)
- ③ 유일성(uniqueness)
- ④ 영지식성(zero knowledge)

16. 다음 중 개인정보 보호법에 위배되지 않는 것은?

- ① 지인으로부터 수신한 제3자의 개인정보를 이용하여 주식 투자에 사용하였다.
- ② 돌아가신 아버님이 생전에 좋아하시던 곳이나 취미를 알기 위하여 관련 정보를 수집하였다.
- ③ 상사의 책상 위에 기록되어있는 상사의 ID와 패스워드를 이용하여 상사가 사용하는 컴퓨터를 접근하였다.
- ④ 인터넷상에 유통되는 개인정보를 활용하여 본인의 대리 인증 목적으로 활용하였다

17. 공격자가 존재하는 공개된 채널을 통해 보안 통신을 원하는 갑과 을에만 비밀정보를 생성하는 Diffie Hellman 키 공유 방식에서 공개변수로 소수 $p=11$, 생성원 $g=3$ 이 주어졌다. 갑과 을의 개인키가 각각 2와 3일 때 공유하는 비밀 값은?

- ① 4
- ② 6
- ③ 8
- ④ 10

18. 다음 중 부채널 공격에 해당하지 않는 것은?

- ① 공격 대상 장비에서 암호 연산에 소요되는 시간이나 전력 소모 정보를 관찰하여 비밀 정보를 유추한다.
- ② 공격 대상 장비에서 방사되는 전자파 정보 등과 같은 무선 신호를 수집하여 비밀정보를 유추한다.
- ③ 비밀 정보가 가질 수 있는 모든 가용 공간에서 가능한 값을 모두 대입하여 탐색해 비밀 정보를 유추한다.
- ④ 정상적인 동작을 하고 있는 공격 대상 장비에 인위적으로 오동작을 발생하도록 하여 비밀 정보를 추출한다.

19. 분산 반사 서비스 거부 공격(DRDoS, Distributed Reflection Denial of Service)의 설명으로 가장 옳지 않은 것은?

- ① 서비스의 응답 특성을 이용한 새로운 형태의 서비스 거부 공격이다.
- ② 공격을 시도하는 IP 근원지를 추적하기가 용이하다.
- ③ 별도의 에이전트 설치 없이 프로토콜 상의 취약점을 이용하여 정상적인 서비스를 운영 하는 시스템을 공격 에이전트로 활용한다.
- ④ UDP 프로토콜을 사용하는 DNS, NTP, SNMP 등의 서비스는 반사와 증폭 공격 형태를 나타낸다.

20. Log4j 악성 코드에 대한 설명 및 대책 중 가장 옳지 않은 것은?

- ① 최초 제로데이 취약점(CVE-2021-44228)이 발견된 이후에도 다수의 추가 취약점이 발견되었다.
- ② 다양한 제품에 패키지 형태로 내장된 프로그램이라 발견하기가 대단히 어렵다.
- ③ 제품 패치 이후에도 내부 중요 시스템에 전 반적인 비정상 프로세스 여부 등 다양한 관 점에서 점검이 필요하다.
- ④ 사용자가 많은 공개 소프트웨어는 검증된 것으로 인식하고 자유롭게 사용한다.

21. 인터넷에 연결 시 노드가 사용하는 IP 주소를 자동으로 할당해 주는 프로토콜로 옳은 것은?

- ① DHCP(Dynamic Host Configuration Protocol)
- ② ICMP(Internet Control Message Protocol)
- ③ IGMP(Internet Group Management Protocol)
- ④ ARP(Address Resolution Protocol)

22. 유닉스 시스템에서 사용자의 계정 정보 등의 기본 정보가 평문 형태로 저장되어 있는 파일로 옳은 것은?

- ① /etc/passwd
- ② /etc/shadow
- ③ /etc/group
- ④ /etc/services

23. 다음 중 국가에서 중소기업에 제공하는 ‘정보 보안 지원 서비스’에 대한 설명으로 가장 옳지 않은 것은?

- ① 휘של(웹셸 탐지도구): 홈페이지 게시판 등을 통해 공격자가 업로드 한 웹셸(해킹 도구)을 탐지하는 전용 도구로 웹셸 뿐만 아니라 악성코드 은닉 사이트 탐지 기능도 가지고 있다.
- ② 캐슬(웹 방화벽): 웹 취약점을 악용한 공격을 사전 차단할 수 있는 웹 방화벽 프로그램으로, 주요 웹 취약점을 이용한 웹 해킹 공격을 차단한다.
- ③ 디도스 사이버대피소: 피해 웹사이트로 향하는 DDoS 트래픽을 대피소로 우회하여 분석, 차단함으로써 정상적으로 운영될 수 있도록 한다.
- ④ 정보보호 관리체계: SQL 인젝션, XSS 등의 웹 취약점을 원격으로 점검해 주는 서비스로 발견된 취약점을 보완하여 웹사이트의 보안을 강화할 수 있다.

24. 개인정보보호위원회에 관한 법률 조항 중 각 괄호에 해당하는 것은?

- (1) 개인 정보 보호에 관한 사무를 독립적으로 수행하기 위하여 (ㄱ) 소속으로 개인정보 보호위원회를 둔다.
- (2) 개인정보보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 (ㄴ) 명의 위원으로 구성한다.

(ㄱ) (ㄴ)

- | | |
|--------|---|
| ① 대통령 | 6 |
| ② 국무총리 | 6 |
| ③ 대통령 | 9 |
| ④ 국무총리 | 9 |

25. 다음 중 역할 기반 접근 제어(Role-Based Access Control)에 대한 설명으로 옳은 것은 몇 개인가?

- ㄱ. 다중 사용자 및 프로그래밍 환경에서의 접근 제어를 위하여 사용자의 역할에 기반을 두고 통제하는 방식으로 강제적 및 임의적 접근 제어를 보완한 방식이다.
- ㄴ. 접근대상 정보를 보안등급을 지정하여 분류한다.
- ㄷ. 접근 제어 목록을 이용하여 각 객체에 대한 권한을 명시한다.
- ㄹ. 사용자의 역할이 변경되면 이에 따른 접근 제어 권한을 변경한다.

- ① 0개
- ② 1개
- ③ 2개
- ④ 3개