2022-군무원-정보보호론-해설-곽후근

1. 다음 중 개인정보의 자기결정권에 대한 설명으로 가장 옳은 것은?
① 개인정보를 수집하는 경우에, 처리목적 달성에 필요한 최소한의 개인정보만을 수집해야 하는 책임
② 특정개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 처리중지, 회수·파기해야 하는 의무
③ 개인정보가 분실·도난·유출·위조·변조·훼손되지 않도록 안전성 확보를 해야 하는 책임
④ 자신에 관한 정보가 언제, 어떻게, 어느 범위까지 수집, 이용, 공개될 수 있는지를 정보주체가 스스로 통제, 결정할 수 있는 권리
정답 체크
(4) 다른 지문은 개인정보 처리자가 수행하고, 해당 지문은 정보 주체가 수행한다.
오답 체크
(1), (2), (3) 개인정보처리자의 역할이다.

2. 다음 중 접근제어 원칙으로 옳지 않은 것은?
① 통신규약 ② 최소 권한 ③ 알 필요성 ④ 직무 분리
정답 체크
(1) 접근제어 원칙에 통신규약은 존재하지 않는다.
오답 체크
(2) 접근제어를 위해 최소한의 권한만을 주어야 함을 의미한다.
(3) 수정할 필요가 없다면 주체는 쓰기 권한을 받지 않게 한다.
(4) 접근제어를 위해 1명에게 너무 많은 권한을 주지 않음을 의미한다.
Tip! 이 외에도 고장시 안전초기화, 완전한 중재(모든 접근을 검사)를 포함한다.

3. 다음 중 대칭키와 비대칭키에 대한 설명으로 가장 옳은 것은?
① 대칭키: 빠른 처리 속도
비대칭키: 키 교환의 장점
② 대칭키: 암호화 및 복호화 키가 같음
비대칭키: 3개 이상의 키가 필요
③ 대칭키: 키 교환의 어려움
비대칭키: MD5(Message-Digest 5) 알고리즘
④ 대칭키: DES(Data Encryption Standard) 알고리즘
비대칭키: 개인키 및 공개키 모두 공개
정답 체크
(1) 대칭키는 수학적 연산을 하지 않아 속도가 빠르고, 비대칭키는 공개키는 공개하므로 키 교환에 유리하다.
오답 체크
(2) 비대칭키는 2개의 키가 필요하다.
(3) MD5는 해시 알고리즘이다.
(4) 개인키는 비밀로 한다.

4. 다음 중 랜섬웨어에 대한 설명으로 가장 옳지 않은 것은?

① 인질의 몸값을 나타내는 ‘ransom’과 ‘software’의 합성어
② 파일 암호화로 피해자는 파일의 읽기 및 실행 불가
③ 백업과 같은 사전 대비가 중요
④ 24시간 후 복호화는 가능하나 많은 양의 정보 손실 발생
정답 체크
(4) 24시간이 아니라 몸값(비트 코인)을 주고 복호화 키를 받으면 복호화가 가능하나 이마저도 많은 양의 정보 손실이 발생한다.
오답 체크
(1) ransom은 몸값을 나타낸다.
(2) 복호화를 하지 않으면 파일의 읽기 및 실행이 불가하다.
(3) 랜섬웨어 예방을 위해 파일을 주기적으로 백업해야 한다.

5. 다음 중 정보보호 서비스 개념으로만 묶인 것으로 가장 옳은 것은?
① 은닉성, 보안성, 다형성
② 가용성, 기밀성, 부인방지
③ 무결성, 효율성, 인증
④ 대응성, 보호성, 소유성
정답 체크
(2) 3대 서비스(기밀성, 무결성, 가용성), 6대 서비스(인증, 부인방지, 책임추적성)
오답 체크
(1), (3), (4) 서비스 개념에 은닉성, 보안성, 다형성, 효율성, 대응성, 보호성, 소유성은 존재하지 않는다.

6. 다음 중 문서의 무결성 비교를 위하여 사용되는 해시 값(함수)의 성질에 대한 설명으로 가장 옳지 않은 것은?
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.
정답 체크
(3) 해시 값 복호화는 불가능하다(일방향성). 그리고 해시와 대칭키는 무관하다.
오답 체크
(1) 입력을 가변이고 출력은 고정이다.
(2) 충돌저항성을 가진다.
(4) 일방향성을 가진다.

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 처리 하는 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
정답 체크
(2) 개인정보 보호법 제2조(정의) 1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
오답 체크
(1), (3) 개인정보처리자의 역할이다.
(4) 범위를 넘어설 수 없다.

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
정답 체크
(2) 방화벽 접근 제어를 위해 IPtables가 사용되고, 일반 PC의 접근 제어를 위해 TCP Wrapper가 사용된다.
오답 체크
(1) IPLogger는 리다이렉션 링크를 통해 IP와 약간의 기기정보를 알아내는 서비스이다. Wireshark는 tcpdump(CLI)의 GUI 버전이다.
(3) Scanner는 IP 또는 포트를 스캐닝하고, Sniffer는 도청하는 것을 의미한다.
(4) Portmap은 RPC에서 클라이언트가 프로그램 번호와 버전 번호를 서버의 포트 번호로 맵핑하는데 사용된다. Snort는 오픈 소스 IDS/IPS를 의미한다.

9. 다음 중 인증시스템의 주요 기능인 인증을 제공 하는 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
정답 체크
(3) 인증을 위해 인공 지능은 통상적으로 사용하지 않는다(나중에는 가능).
오답 체크
(1) 패스워드는 지식 기반이다.
(2) 홍채는 신체 기반이다.
(4) 공인(공동) 인증서는 소지 기반이다.

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
정답 체크
(1) 블록체인의 전체 노드 중 50%를 초과하는 해시 연산력을 확보한 뒤, 거래 정보를 조작함으로써 이익을 얻으려는 해킹 공격을 말한다.
오답 체크
(2), (3), (4) 통상적으로 사용하는 용어가 아니다.

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.
정답 체크
(2) 암호형에 대한 설명이고, 은폐형은 잠복기와 은폐 특성을 가진다.
오답 체크
(1) 부트 파이러스와 파일 바이러스가 존재한다.
(3) Mutation 프로그램을 이용하여 바이러스 코드를 변경한다.
(4) 워드, 엑셀, 파워포인트에서 발생한다(누구라도 쉽게 제작).

12. 다음 중 포렌식으로 증거를 획득할 때 지켜야할 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.
정답 체크
(4) 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 한다.
오답 체크
(1) 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 하고, 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(2) 컴퓨터 내부의 정보는 휘발성을 가진 것이 많기 때문에 신속하게 이뤄져야 한다.
(3) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 한다.

13. RSA 공개키 암호에서 2개의 소수 p=3와 q=7가 주어지고 복호화 키(d) 5로 고정했을때, 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
정답 체크
(3) N = 3x7 = 21, L(오일러 피 함수) = 2x6 = 12
e는 L과 서로소의 관계를 가져야 하므로 5여야 한다. (여기서 답이 나옴)

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.
정답 체크
(4) AES는 보안상 안전하므로 Weak Key(특정한 조작을 통해 쉽게 복호화가 가능한 키)가 존재하지 않는다.
오답 체크
(1) 128비트 블록 단위로 암호호/복호화가 이루어진다.
(2) 128/192/256비트 키를 가지며, 각 키에 따라 10/12/14 라운드를 가진다.
(3) DES는 Feistel 구조(별도의 복호화기가 필요 없음)이고, AES는 SPN 구조(별도의 복호화기가 필요함)이다.

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)
정답 체크
(3) 영지식 특성에 유일성은 존재하지 않는다.
오답 체크
(1) 어떤 문장이 참이면, 정직한 증명자는 정직한 검증자에게 이 사실을 납득시킬 수 있어야 한다.
(2) 어떤 문장이 거짓이면, 어떠한 부정직한 증명자라도 정직한 검증자에게 이 문장이 사실이라고 납득시킬 수 없어야 한다.
(4) 어떤 문장이 참이면, 검증자는 문장의 참 거짓 이외에는 아무것도 알 수 없어야 한다.

16. 다음 중 개인정보 보호법에 위배 되지 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 인터넷 상에 유통되는 개인정보를 활용하여 본인의 대리 인증 목적으로 활용하였다.
정답 체크
(2) 2가지가 위배되지 않는 것으로 본다. 하나는 아버지(친족)이고, 또 하나는 살아있지 않다는 것이다.
오답 체크
(1) 제3자의 개인정보를 이용하면 안된다.
(3) 상사의 ID와 패스워를 이용하면 안된다.
(4) 인터넷 상에 유통되는 개인정보를 이용하면 안된다.

17. 공격자가 존재하는 공개된 채널을 통해 보안 통신을 원하는 갑과 을에만 비밀정보를 생성하는 Diffie Hellman 키 공유 방식에서 공개변수로 소수 p = 11, 생성원 g = 3이 주어졌다. 갑과 을의 개인키가 각각 2와 3일 때 공유하는 비밀 값은?
① 4
② 6
③ 8
④ 10
정답 체크
답이 없음
비밀 값 = g^{ab} mod p = 3^6 mod 11 = 729 mod 11 = 3

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.
정답 체크
(3) 전사 공격을 의미하고 정채널(부채널의 반대 개념으로 지어낸 말) 공격이다.
오답 체크
(1) 소용 시간이나 전력 소모는 부가적인 정보를 의미한다.
(2) 무선 신호 수집 등은 부가적인 정보를 의미한다.
(4) 오동작을 통해 부가적인 정보를 얻어낸다.

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 운영하는 시스템을 공격 에이전트로 활용한다.

④ UDP 프로토콜을 사용하는 DNS, NTP, SNMP 등의 서비스는 반사와 증폭 공격 형태를 나타낸다.
정답 체크
(2) IP 근원지가 공격 대상으로 바뀌므로 추적이 어렵다.
오답 체크
(1) DRDoS에 사용되는 반사 서버는 응답을 하도록 되어 있다. 예를 들어, TCP를 보내면 이에 대해 응답하고, ICMP를 보내면 이에 대해 응답한다.
(3) TCP 서비스(3-way 핸드쉐이크)를 이용한다.
(4) UDP Protocol 기반의 서비스를 이용하여, 반사(Reflection)와 증폭(Amplification) 공격 형태로 나타난다. 출발지 IP를 Spoofing하고, UDP 기반 서버에 대규모 요청을 전송하여 반사를 시도한다. 이때 반사된 응답은 증폭되어 공격 대상에게 전달된다.

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 발견 되었다.
② 다양한 제품에 패키지 형태로 내장된 프로그램이라 발견하기가 대단히 어렵다.
③ 제품 패치 이후에도 내부 중요 시스템에 전반적인 비정상 프로세스 여부 등 다양한 관점에서 점검이 필요하다.
④ 사용자가 많은 공개 소프트웨어는 검증된 것으로 인식하고 자유롭게 사용한다.
정답 체크
(4) Log4j는 사용자가 많은 공개 소프트웨어로서 안전하다고 인식되었으나 이번 일을 계기로 믿을 수 없다는 것이 판명되었다.
오답 체크
(1) CVE-2021-44832, CVE-2021-45105 등이 계속적으로 발견되었다.
(2) 자바 기반 로깅 유틸리티 패키지이다.
(3) 패치를 해도 계속적인 감염이 있을 수 있다.

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)
정답 체크
(1) 유무선 공유기(집)나 커피숍에서 많이 사용하는 방식이다.
오답 체크
(2) ping 등에서 제어 메시지를 전달한다.
(3) IPTV 등에서 사용자가 라우터에게 자신이 속한 멀티캐스트 그룹을 알릴 때 사용한다.
(4) IP 주소에 대한 MAC 주소를 알려준다(arp request와 reply에서 MAC 브로드캐스트와 유니캐스트를 사용).

22. 유닉스 시스템에서 사용자의 계정 정보 등의 기본 정보가 평문 형태로 저장되어 있는 파일로 옳

은 것은?
① /etc/passwd
② /etc/shadow
③ /etc/group
④ /etc/services
정답 체크
(1) 사용자 계정 정보가 들어간다.
오답 체크
(2) 암호화된 패스워드가 들어간다.
(3) 그룹 정보가 들어간다.
(4) 데몬 이름, 포트 번호, 프로토콜 정보가 저장되어 있다.

23. 다음 중 국가에서 중소기업에 제공하는 '정보 보안 지원 서비스'에 대한 설명으로 가장 옳지 않은 것은?
① 휘슬(웹셸 탐지도구): 홈페이지 게시판 등을 통해 공격자가 업로드한 웹셸(해킹 도구)을 탐지 하는 전용 도구로 웹셸 뿐만 아니라 악성 코드 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 사이버 대피소: 피해 웹 사이트로 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 웹 사이트의 보안을 강화할 수 있다.
정답 체크
(4) 해당 설명은 웹 취약점 점검 도구를 통해 가능하고, 정보보호 관리체계는 정보보호에 관한 경영시스템(PDCA)이며 조직의 의사결정시스템, 내부통제시스템이다.
오답 체크
(1) 웹셸은 서버에서 실행되어 공격자가 명령을 내릴 수 있는 셸을 의미한다.
(2) 웹 방화벽은 웹에 특화된 방화벽을 의미한다.
(3) 허니팟의 기능을 의미한다.

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

(1) 개인정보보호에 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

정답 체크

(4) 제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.
제7조의2(보호위원회의 구성 등) ① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

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 역 할에 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
정답 체크
(3) ㄱ, ㄹ은 RBAC를 나타낸다.
오답 체크
(1), (2), (4) ㄴ : MAC에 대한 설명이다. ㄷ : ACL에 대한 설명이다.