정보보호론

Ⓑ

(1번~20번)

(9급)

1. 다음 바이러스 발전 단계에 따른 분류에 대한 설명으로 옳지 않은 것은?
   ① 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.
   ② 암호화 바이러스는 바이러스 프로그램 전체 또는 일부를 암호화시켜 저장하는 바이러스이다.
   ③ 갑옷형 바이러스는 백신 개발을 지연시키기 위하여 다양한 암호화 기법을 사용하는 바이러스이다.
   ④ 매크로 바이러스는 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스이다.

2. 공개키 기반구조(Public Key Infrastructure, PKI)를 위한 요소 시스템으로 옳지 않은 것은?
   ① 인증서와 인증서 폐지 목록을 공개하기 위한 디렉토리
   ② 사용자 신원을 확인하는 등록기관
   ③ 인증서 발행업무를 효율적으로 수행하기 위한 인증기관 웹 서버
   ④ 인증서를 발행 받는 사용자(최종 개체)

3. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?
   ① 수신 시스템이 처리할 수 있는 윈도우 크기
   ② 패킷을 송신하고 수신하는 프로세스의 포트 번호
   ③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호
   ④ 송신 시스템의 TCP 패킷의 생성 시간

4. 아래 <보기>의 지문은 신문에서 발췌한 기사이다. 빈칸에 들어갈 단어로 적절한 것은?

<보기>

취업준비생 김다정(28)씨는 지난 5월 7일 [ ] 공격으로 취업을 위해 모아뒀던 학습 및 준비 자료가 모두 암호화돼 버렸다. 컴퓨터 화면에는 암호를 알려주는 대가로 100달러(약 11만 5000원)를 요구하는 문구가 떴지만, 결제해도 데이터를 되찾을 수 없다는 지인의 조언에 데이터복구 업체를 통해 일부 자료만 복구해 보기로 했다. 그런데 업체를 통해 데이터 일부를 복구한 지 하루 만인 지난 10일 또 다시 [ ] 공격을 받아 컴퓨터가 먹통이 돼 버렸다.

   ① 하트블리드(Heart bleed)
   ② 랜섬웨어(Ransomware)
   ③ 백오리피스(Back Orifice)
   ④ 스턱스넷(Stuxnet)

5. 다음 중 Cipher Block Chaining 운용 모드의 암호화 수식을 제대로 설명한 것은? (단, P_i는 i번째 평문 블록을, C_i는 i번째 암호문 블록을 의미한다.)
   ① $C_i=E_k(P_i)$
   ② $C_i=E_k(P_i \oplus C_{i-1})$
   ③ $C_i=E_k(C_{i-1}) \oplus P_i$
   ④ $C_i=E_k(P_i) \oplus C_{i-1}$

6. 다음 중 X.509 v3 표준 인증서에 포함되지 않는 것은?
   ① 인증서의 버전(Version)
   ② 서명 알고리즘 식별자(Signature Algorithm ID)
   ③ 유효기간(Validity Period)
   ④ 디렉토리 서비스 이름(Directory Service Name)

7. 다음 중 성격이 다른 공격 유형은?
   ① Session Hijacking Attack
   ② Targa Attack
   ③ Ping of Death Attack
   ④ Smurf Attack

8. Stack에 할당된 Buffer overflow Attack에 대응할 수 있는 안전한 코딩(Secure Coding) 기술의 설명으로 옳지 않은 것은?
   ① 프로그램이 버퍼가 저장할 수 있는 것보다 많은 데이터를 입력하지 않는다.
   ② 프로그램은 할당된 버퍼 경계 밖의 메모리 영역은 참조하지 않으므로 버퍼 경계 안에서 발생될 수 있는 에러를 수정해 주면 된다.
   ③ gets()나 strcpy()와 같이 버퍼 오버플로우에 취약한 라이브러리 함수는 사용하지 않는다.
   ④ 입력에 대해서 경계 검사(Bounds Checking)를 수행해 준다.

9. 전자화폐(Electronic Cash)에 대한 설명으로 옳지 않은 것은?
   ① 전자화폐의 지불 과정에서 물품 구입 내용과 사용자 식별 정보가 어느 누구에 의해서도 연계되어서는 안된다.
   ② 전자화폐는 다른 사람에게 즉시 이전할 수 있어야 한다.
   ③ 일정한 가치를 가지는 전자화폐는 그 가치만큼 자유롭게 분산이용이 가능해야 한다.
   ④ 대금 지불 시 전자화폐의 유효성 확인은 은행이 개입하여 즉시 이루어져야 한다.

10. Linux system의 바이너리 로그파일인 btmp(솔라리스의 경우는 loginlog 파일)를 통해 확인할 수 있는 공격은?
   ① Password Dictionary Attack
   ② SQL Injection Attack
   ③ Zero Day Attack
   ④ SYN Flooding Attack

11. 다음 중 시스템 내부의 트로이목마 프로그램을 감지하기 위한 도구로 가장 적절한 것은?
① Saint
② Snort
③ Nmap
④ Tripwire

12. ROT13 암호로 “info”를 암호화한 결과는?
① jvxv
② foin
③ vasb
④ klmd

13. 무선랜에서의 인증 방식에 대한 설명 중 옳지 않은 것은?
① WPA 방식은 48비트 길이의 초기벡터(Ⅳ)를 사용한다.
② WPA2 방식은 AES 암호화 알고리즘을 사용하여 좀 더 강력한 보안을 제공한다.
③ WEP 방식은 DES 암호화 방식을 이용한다.
④ WEP 방식은 공격에 취약하며 보안성이 약하다.

14. 다음 중 ISO 27001의 통제 영역별 주요 내용으로 옳은 것은?
① 정보보안 조직 : 정보보호에 대한 경영진의 방향성 및 지원을 제공
② 인적 자원 보안 : 정보에 대한 접근을 통제
③ 정보보안 사고 관리 : 사업장의 비인가된 접근 및 방해 요인을 예방
④ 통신 및 운영 관리 : 정보처리시설의 정확하고 안전한 운영을 보장

15. 「개인정보보호법」에 따르면 주민등록번호를 처리하기 위해서는 법에서 정하는 바에 따라야 하는데, 그에 대한 내용 중 옳지 않은 것은?
① 주민등록번호 처리는 원칙적으로 금지되고 예외적인 경우에만 허용한다.
② 주민등록번호는 암호화 조치를 통해 보관해야 한다.
③ 개인정보처리자는 법령에서 주민등록번호의 처리를 허용한 경우에도 주민등록번호를 사용하지 않는 인터넷 회원가입 방법을 정보주체에게 제공해야 한다.
④ 기 보유한 주민등록번호는 수집 시 동의 받은 보유기간까지만 보유하고 이후에는 즉시 폐기해야 한다.

16. 공통평가기준(Common Criteria, CC)에 대한 설명 중 옳지 않은 것은?
① 보호프로파일(Protection Profile)과 보안목표명세서(Security Target) 중 제품군에 대한 요구사항 중심으로 기술되어 있는 것은 보안목표명세서(Security Target)이다.
② 평가대상에는 EAL 1에서 EAL 7까지 보증등급을 부여할 수 있다.
③ CC의 개발은 오렌지북이라는 기준서를 근간으로 하였다.
④ CC의 요구사항은 class, family, component로 분류한다.

17. <보기>에서 설명하는 암호화 알고리즘으로 옳은 것은?

<보기>
- Ron Rivest가 1987년에 RSA Security에 있으면서 설계한 스트림 암호이다.
- 바이트 단위로 작동되도록 만들어진 다양한 크기의 키를 사용한다.
- 사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.
- 하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.

① RC5 ② SEED
③ SKIPJACK ④ RC4

18. 다음 중 Spoofing 공격에 대한 설명으로 옳지 않은 것은?
① ARP Spoofing : MAC주소를 속임으로써 통신 흐름을 왜곡시킨다.
② IP Spoofing : 다른이가 쓰는 IP를 강탈해 특정 권한을 획득한다.
③ DNS Spoofing : 공격대상이 잘못된 IP주소로 웹 접속을 하도록 유도하는 공격이다.
④ ICMP Redirect : 공격자가 클라이언트의 IP주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근한다.

19. 다음 중 ISMS(Information Security Management System)의 각 단계에 대한 설명으로 옳은 것은?
① 계획 : ISMS 모니터링과 검토
② 조치 : ISMS 관리와 개선
③ 수행 : ISMS 수립
④ 점검 : ISMS 구현과 운영

20. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳은 것은 무엇인가?
① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.
② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.
③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션 통신을 한다.
④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.