정 보 보 호 론 (7급)

(과목코드 : 141)

2022년 군무원 채용시험 응시번호 : 성명 :

1. 다음 중 버퍼오버플로우 공격으로부터 가장 안전한 C언어 함수에 해당하는 것은?
   ① strcpy
   ② gets
   ③ sprintf
   ④ scanf_s

2. 다음 중 한국에서 개발한 암호화 알고리즘이 아닌 것은?
   ① AES
   ② ARIA
   ③ SEED
   ④ LEA

3. OSI 7계층은 다양한 네트워크 간의 호환을 위해 만든 표준 네트워크 모델이다. 다음 중 OSI 7계층에서 네트워크 계층에 대한 설명으로 가장 옳은 것은?
   ① 양 끝단의 응용 프로세스가 통신을 관리하는 방법을 제공한다.
   ② 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해준다.
   ③ 두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층으로 16진수 12개로 구성된 MAC 주소를 사용한다.
   ④ 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층으로 라우터를 통한 패킷 포워딩을 담당한다.

4. 다음은 TCP의 연결 설정 과정(3-way handshaking)을 무작위로 나열한 것이다. 이를 가장 올바른 순서로 나열한 것은?

   A: 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고, 클라이언트에 연결을 해도 좋다는 의미로 SYN+ACK 패킷을 보낸다.
   B: 두 시스템이 통신을 하기 전 클라이언트는 포트가 닫힌 Closed 상태이고 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태이다.
   C: 클라이언트가 통신을 하려고 하면 임의의 포트 번호가 클라이언트 프로그램에 할당되고, 클라이언트는 서버에 연결하고 싶다는 의사 표시인 SYN Sent 상태가 된다.
   D: 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보낸다.

   ① A→C→B→D
   ② B→C→A→D
   ③ C→D→A→B
   ④ C→D→B→A

5. 다음은 모바일 기기 상에서의 보안 관련 기술에 대한 설명이다. 해당 기술과 가장 가까운 것은?

   - 응용 프로그램이 실행될 때 가상 머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 의미한다.
   - 사용자 앱은 기본적으로 앱 간에 데이터를 주고받을 수 없고 시스템 파일에도 접근할 수 없다.
   - 앱 간 문서, 음악, 사진 등의 전송은 시스템 API에서 그 기능을 제공할 때만 가능하다.

   ① 샌드박스
   ② 멀티태스킹 금지
   ③ 원격 로그인 금지
   ④ 응용 프로그램 서명

6. 다음은 WEP(Wired Equivalent Privacy)를 이용한 암호화 세션 생성을 무작위로 나열한 것이다. 이를 가장 올바른 순서로 나열한 것은?

A: 사용하려는 무선 랜 서비스의 SSID 값을 알아내어 무선 랜 AP에 연결 요청 메시지를 전송한다.
B: 인증용 문자열(Challenge)을 받은 사용자는 자신이 가진 공유키로 WEP 암호화를 적용하여 암호문을 만든 다음 AP에 전송한다.
C: 사용자의 연결 요청 메시지를 받은 AP는 임의의 문장을 생성하여 원본을 저장하고 연결요청 응답 메시지를 이용하여 암호화 되지 않은 인증용 문자열(Challenge)을 전송한다.
D: 사용자가 공유키로 만든 암호문을 전송받은 AP는 자신이 가진 공유키로 암호문을 복호화한다. 그리고 복호화 된 문장과 자신이 저장하고 있던 원본 문장을 비교하여 같으면 사용자가 자신과 같은 공유키를 가진 그룹원이라고 인식해 연결 허용메시지를 전송한다.

① A→C→B→D
② B→C→A→D
③ C→A→B→D
④ C→B→A→D

7. 다음 중 인텔의 80x86 CPU의 범용 레지스터에 대한 설명으로 옳지 않은 것은?

① EAX(누산기): 산술 연산에 사용하며 함수의 결과 값을 저장한다.
② EBX(베이스 레지스터): 특정 주소를 저장하며 주소 지정을 확대하기 위한 인덱스로 사용한다.
③ ECX(카운터 레지스터): 반복적으로 실행되는 특정 명령에 사용한다. 루프의 반복 횟수나 좌우 방향 시프트 비트 수를 기억한다.
④ EDX(데이터 레지스터): 연산 결과 및 시스템 상태와 관련된 여러 가지 플래그 값을 저장한다.

8. 아래에서 설명하는 전자우편 암호화와 가장 가까운 것은?

1991년에 IDEA 알고리즘과 RSA 알고리즘을 조합하여 만들어졌다. 세션 키를 암호화하기 위해 IDEA 알고리즘을 이용하고 사용자 인증을 위한 전자 서명에는 RSA 알고리즘을 이용한다. 특히 해당 기술을 사용하는 사람들 간의 신뢰 관계를 통해 공개키를 인증하는 기법을 사용하고 있다.

① S/MIME(Secure MIME)
② PGP(Pretty Good Privacy)
③ PEM(Privacy Enhanced Mail)
④ SSL(Secure Socket Layer)

9. 시스템 상에서 프로그램을 동작시키면 해당 프로그램을 동작하기 위한 가상의 공간이 메모리에 생성된다. 아래에서 설명하고 있는 메모리 구조와 가장 가까운 것은?

- 프로그램 로직이 동작하기 위한 인자(argument)와 프로세스 상태를 저장한다.
- 해당 영역은 레지스터의 임시 저장, 서브루틴 사용 시 복귀 주소 저장, 서브루틴에 인자 전달 등의 용도로 사용된다.
- 메모리의 상위 주소에서 하위 주소 방향으로 사용하며 후입선출(Last In First Out, LIFO) 원칙에 따라 나중에 저장된 값을 먼저 사용한다.

① 스택
② 힙
③ 레지스터
④ 버퍼

10. 다음 중 대칭키 암호화 기법이 아닌 것은?

① RC4
② ElGamal
③ LEA
④ ARIA

11. 다음은 XSS(Cross-Site Scripting) 공격 과정을 무작위로 나열한 것이다. 가장 올바른 순서로 나열한 것은?

> A: 웹 서버는 사용자가 접근한 XSS 코드가 포함된 게시판의 글을 사용자에게 전달한다.
> B: XSS 취약점이 존재하는 서버에 XSS 코드를 작성하여 저장한다. 일반적으로 공격자는 사용자가 이용하는 게시판을 공격한다.
> C: 공격자가 작성해놓은 XSS 코드에 해당 웹 서비스 사용자가 접근한다. 사용자는 공격자가 작성해놓은 XSS 코드에 접근한다는 것을 인지하지 못한다. 사용자는 어떤 게시판의 글을 읽는 과정에서 공격자의 XSS 코드에 접근하게 된다.
> D: 사용자의 시스템에서 XSS 코드가 실행되며 그 결과가 공격자에게 전달된다.

① C→A→B→D
② A→C→B→D
③ B→C→A→D
④ C→B→A→D

12. 아래에서 설명하는 보안 솔루션과 가장 관련이 있는 기술은?

> 문서 보안에 초점을 둔 기술로 문서의 열람, 편집, 인쇄에 접근 권한을 설정하여 통제한다. 특정한 형태의 문서만 통제하는 것이 아니라 MS워드나 HWP, TXT, PDF 파일 등 사무에 사용하는 대부분의 파일을 통제할 수 있다. 사내에서 사용하는 운영체제 커널에 해당 모듈을 삽입하는 형식으로 동작시킬 수 있다.

① VPN(Virtual Private Network)
② DRM(Digital Right Management)
③ DLP(Data Leak Prevention)
④ ASIC(Application Specific Integrated Circuit)

13. 다음은 OECD 개인 정보 보안 8원칙 중 일부를 나열한 것이다. 8원칙에 대한 설명으로 가장 옳지 않은 것은?

① 정보 정확성의 원칙(Data Quality Principle): 이용 목적상 필요한 범위 내에서 개인 정보의 정확성, 완전성, 최신성이 확보되어야 한다.
② 이용 제한의 원칙(Use Limitation Principle): 정보 주체의 동의가 있거나 법 규정이 있는 경우를 제외하고 목적 외에 이용하거나 공개할 수 없다.
③ 안전성 확보의 원칙(Security Safeguard Principle): 정보 주체의 개인 정보 열람•정정•삭제 청구권이 보장되어야 한다.
④ 책임의 원칙(Accountability Principle): 개인 정보 관리자에게 원칙 준수 의무 및 책임을 부과해야 한다.

14. 다음 중 양자 컴퓨팅과 관련한 설명으로 가장 옳지 않은 것은?

① 양자 컴퓨터에 Shor 알고리즘을 적용하면 현재 알려진 다수의 대칭키 암호화 알고리즘이 다항 시간 내에 공격 가능해지므로 안전하지 않게 된다.
② 양자 키 분배(quantum key distribution) 에서는 양자 물리학의 중첩과 얽힘의 성질을 이용하여 도청으로부터 안전한 키 분배 방식을 제공한다.
③ 양자 내성 암호(post-quantum cryptography)는 양자 컴퓨터가 등장하더라도 안전성을 보장하는 암호 알고리즘을 일컬으며, NIST에 의해 후보 알고리즘이 검토되고 있다.
④ 마이크로소프트에서는 양자 알고리즘을 개발하고 실행하기 위한 Q# 오픈 소스 프로그래밍 언어를 개발하였다.

15. 다음 중 부채널 분석(side-channel analysis)에 대한 설명으로 가장 옳지 않은 것은?

① 주로 구현상에서 발생하는 시간차, 전력 소모 등의 부가적인 정보로부터 민감한 정보를 유추하는 기법이다.

② 하드웨어에 대한 부채널 분석 뿐 아니라 소프트웨어 기반 부채널 분석 또한 가능하다.

③ 공통평가기준(Common Criteria, CC) 및 암호모듈평가체계(Cryptographic Module Validation Program, CMVP) 등에서 비침습 공격에 대한 평가가 이루어지며, 비침습 공격은 부채널 분석을 포함한다.

④ 알고리즘의 이론적 오류로 인한 정보 유출 취약점을 활용한다.

16. 다음 중 블록체인 기반 가상화폐에 대한 설명으로 가장 옳지 않은 것은?

① 중앙 집중화된 관리자나 제3의 중재자가 없다.

② 블록에는 하나의 거래 내역이 암호화되어 저장된다.

③ 거래장부에 해당하는 블록은 공개되어 분산 관리된다.

④ 분산된 모든 블록을 위조하는 어려움에 기반하여 가상화폐의 안전성이 보장된다.

17. 다음 중 위험분석 방법론의 성격이 가장 다른 것은?

① 전문가 집단을 구성하여 위험을 분석 및 평가하여 다양한 위협과 취약성을 토론을 통해 분석한다.

② 일정 조건 하에서 위협에 대한 발생 가능한 결과들을 추정한다.

③ 비교 우위 순위 결정표에 위험 항목들의 서술적 순위를 결정한다.

④ 위협의 발생 빈도를 계산하는 식을 이용하여 위험 순위를 결정한다.

18. 다음 중 암호학적 해시 함수(h)에 대한 설명으로 가장 옳지 않은 것은?

① 주어진 출력 y에 대하여 $h(x) = y$를 만족하는 x를 구하기 어렵다.

② 임의 메시지에 대하여 동일한 해시값을 가지는 메시지가 없다.

③ 동일한 해시값을 가지는 서로 다른 x와 x'을 구하기 어렵다.

④ 주어진 입력 x에 대하여 $h(x') = h(x)$, $x' \neq x$ 를 만족하는 x가 아닌 x'을 구하기 어렵다.

19. 다음 중 정보통신기반 보호법에 대한 설명으로 옳지 않은 것은?

① 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

② 주요정보통신기반시설을 관리하는 기관의 장은 취약점 분석·평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적·기술적 대책을 포함한 관리대책을 수립·시행하여야 한다.

③ 관리기관의 장은 침해사고가 발생하여 소관 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에는 관계 행정기관, 수사기관 또는 인터넷진흥원 중 하나의 기관에 반드시 그 사실을 통지하여야 한다.

④ 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

20. 다음 중 유닉스 시스템에서의 파일 또는 디렉터리의 권한 관리에 대한 설명으로 가장 옳지 않은 것은?
① SetUID가 설정된 프로그램이 실행되면, 일반 사용자가 소유자 권한을 위임받아 특정 명령을 실행시킬 수 있다.
② 새롭게 생성되는 파일이나 디렉터리는 umask에 의해 결정되는 디폴트 권한으로 생성된다.
③ Sticky bit가 설정된 디렉터리는 해당 디렉터리 내의 파일을 임의대로 삭제할 수 없고, root와 소유자에게 삭제 변경 권한이 부여된다.
④ SetGID 명령은 chmod 명령에서 'chmod 1755 setgid_program'과 같이 1000번대 인자를 주어 설정할 수 있다.

21. 다음 중 국내 정보보호 관리체계 및 인증제도에 대한 설명으로 옳지 않은 것은?
① 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증을 받고자 하는 신청기관은 '관리체계 수립 및 운영', '보호대책 요구사항'의 2개 영역에서 80개의 인증기준을 적용받게 된다.
② 관리체계 수립 및 운영은 관리체계 기반마련, 위험관리, 관리체계 운영, 관리체계 점검 및 개선의 4개 분야 16개 인증기준으로 구성된다.
③ ISMS 인증은 의무 대상자가 아니더라도 자발적으로 신청하여 인증심사를 받을 수 있다.
④ 정보보호 관리체계를 유지하는 기업을 대상으로, 정보보호 수준을 측정하여 '우수', '최우수' 등급을 부여하는 정보보호 등급제 인증제도가 운영되고 있다.

22. 다음 중 접근 통제의 성격이 가장 다른 것은?
① 보안클래스를 보안의 중요도에 따라 비교 우위를 가려 이를 선행으로 나열하는 접근 통제이다.
② 주체의 책임과 역할을 기반으로 하는 접근 통제이다.
③ 주체와 객체의 등급을 비교하여 접근 권한을 부여하는 접근 통제이다.
④ 개인의 역할을 기반으로 하는 접근 통제이다.

23. 다음 중 신뢰 컴퓨팅 기반(Trusted Computing Base, TCB)에 대한 설명으로 가장 거리가 먼 것은?
① TCB의 각 계층은 고유의 보안 정책을 정의하고, 기존의 TCB를 재사용 또는 확장할 수 있다
② 운영 TCB는 기본적인 보호 환경을 구축하고, 신뢰성 있는 시스템에 필요한 부가적인 사용자 서비스를 제공한다.
③ 일반적으로 컴퓨터의 메인보드에 설치되어 하드웨어 버스를 사용하여 시스템의 다른 부분과 통신한다.
④ 보안 정책의 정확한 적용 능력은 오직 TCB 내의 메커니즘과 보안 정책 관련 정보의 입력에 따른다.

24. 다음 중 인공지능 보안에 대한 설명으로 가장 옳지 않은 것은?
① 학습 과정에 무작위 오류가 존재하는 노이즈를 고의적으로 추가함으로써 인공지능이 잘못된 판단을 하도록 하는 회피 공격(evasion attack)과 같은 데이터 변조 공격을 수행할 수 있다.
② 수많은 질의를 보내고 산출된 결과를 분석함으로써 인공지능에 사용된 데이터를 추출하는 전도 공격(inversion attack)이 존재한다.
③ 동일한 데이터를 반복 학습함으로써 편향된 성향을 가지도록 하는 재전송 공격(replay attack)이 존재한다.
④ 악의적 데이터를 주입함으로써 정상적인 서비스가 불가능하게 하는 중독공격(poison attack)과 같은 공격 기법이 존재한다.

25. 다음 중 트래픽 분석(traffic analysis)에 대한 설명으로 가장 옳은 것은?
① 사용자가 보낸 메시지 사본을 획득하여 나중에 그 메시지를 사용하기 위한 목적으로 이용하는 소극적 공격이다.
② 시스템의 서비스를 느리게 하거나 완전히 차단하는 적극적 공격이다.
③ 송수신되는 데이터를 가로채거나 획득 후 정보를 조작하는 적극적 공격이다.
④ 송수신되는 데이터 자체 외의 다른 정보를 유추하는 소극적 공격이다.