정 보 보 호 론 (7급)

(과목코드 : 141)

2024년 군무원 채용시험　　응시번호 :　　성명 :

1. DoS(Denial of Service) 공격의 일종이 아닌 것은?
   ① Cross-site scripting
   ② TearDrop
   ③ UDP flooding
   ④ Slowloris

2. 인증서(digital certificate)에 포함된 정보가 아닌 것은?
   ① 인증서 소유자의 id 또는 이름
   ② 인증서 소유자의 private key
   ③ CA(Certificate Authority)의 정보
   ④ 유효기간

3. 전자 서명(digital signature)에 대한 설명 중 가장 적절하지 않은 것은?
   ① 서명하려는 문서에 대하여 같은 해시값을 갖는 문서를 찾아내면 서명을 위조할 수 있다.
   ② 전자 서명을 이용하여 문서의 무결성을 보장할 수 있다.
   ③ 서명하려는 문서의 해시값을 생성하여 서명한다.
   ④ 전자 서명(digital signature) 값은 서명자 public key로 암호화한 값이다.

4. 다음 용어 설명 중 가장 적절하지 않은 것은?
   ① repudiation: 메시지를 전송하였다는 것을 부인하지 못하도록 하는 기능
   ② confidentiality: 허가되지 않은 사용자가 열람하지 못하도록 하는 기능
   ③ integrity: 허가되지 않은 사용자가 수정하지 못하도록 하는 기능
   ④ authentication: 사용자를 확인하는 기능

5. 악성코드 분석에 대한 설명 중 가장 적절하지 않은 것은?
   ① 악성코드 분석 방법은 크게 정적 분석 방법과 동적 분석 방법으로 나눌 수 있다.
   ② 정적 분석 방법은 악성코드를 실행하지 않고 실행 파일을 분석하는 방법이다.
   ③ 패킹 기술이 적용된 악성코드는 동적 분석을 할 수 없다.
   ④ anti-VM 기술을 이용하여 동적 분석을 방해할 수 있다.

6. 침입탐지시스템(IDS)에 대한 설명 중 가장 적절하지 않은 것은?
   ① Host IDS, Network IDS 등이 있다.
   ② signature 기반 탐지 방법으로는 알려지지 않은 새로운 공격을 탐지하기 어렵다.
   ③ 공격임에도 불구하고 공격으로 탐지 못한 것을 false positive라고 한다.
   ④ anomaly detection 방법은 정상 사용자를 공격으로 오인하는 경우가 signature 기반 탐지 방법보다 많다.

7. 다음 <보기>에서 국제표준인 ISO 31000:2018의 위험관리 프로세스 중 위험평가(risk assessment)에 해당하는 활동으로 묶은 것은?

<보기>
가. 위험분석(risk analisys)
나. 위험수준평가(risk evaluation)
다. 위험처리(risk treatment)
라. 위험모니터링(risk monitoring)

① 가, 나　　② 다, 라
③ 가, 다　　④ 나, 라

8. SYN flooding 공격에 대한 설명 중 가장 적절하지 않은 것은?
① 공격자가 다수의 SYN 패킷을 피해자 컴퓨터에 보낸다.
② SYN 패킷을 받은 피해자 컴퓨터는 응답으로 ACK 패킷을 보낸다.
③ 피해 컴퓨터는 TCP 연결 설정을 위하여 SYN 패킷의 일부 정보를 유지해야 한다.
④ SYN flooding 공격은 DDoS 공격으로도 사용된다.

9. 다음 <보기>의 보안관제 기술을 발전 단계 순서대로 나열한 것은?

<보기>
가. ESM(Enterprise Security Management)
나. SOAR(Security Ochestration, Automation and Response)
다. SIEM(Security Information and Event Management)

① 가-나-다 ② 가-다-나
③ 다-가-나 ④ 다-나-가

10. 개인정보파일의 가명정보 처리에서 데이터 자체의 식별 위험성 요소와 가장 거리가 먼 것은?
① 식별 가능정보
② 특이정보
③ 재식별시 영향도
④ 활용 형태

11. MAC(Message Authentication Code)에 대한 설명 중 가장 적절하지 않은 것은?
① 대칭키 암호화 방법을 이용하여 MAC을 생성할 수 있다.
② 암호화 알고리즘을 사용하지 않고 MAC을 생성할 수 있다.
③ MAC을 통하여 무결성과 기밀성을 보장할 수 있다.
④ MAC 생성을 위하여 해시 알고리즘이 사용된다.

12. 제로트러스트(Zero Trust)의 기본적인 원리에 해당하는 설명 중 가장 적절하지 않은 것은?
① 모든 종류의 접근에 대해 명시적인 신뢰를 확인 후 접근을 허용한다.
② 다양한 자원에 접근을 허용하기 위하여 분산된 보안정책으로 관리한다.
③ 물리적 경계가 아닌 소프트웨어 정의 경계와 같은 방식으로 경계를 설정한다.
④ 접근 주체와 리소스의 상태에 대한 신뢰성을 지속적으로 검증하고 제어한다.

13. Unix/Linux의 파일 및 디렉터리의 접근 제어 방법에 대한 설명 중 가장 적절하지 않은 것은?
① 디렉터리에 있는 파일 목록을 나열하기 위해서는 읽기 권한이 있어야 한다.
② 파일의 실행 권한(x)에 setuid bit를 설정할 수 있다.
③ 사용자를 owner, group, public으로 나누어서 읽기, 쓰기, 실행 권한을 부여한다.
④ 파일을 삭제하기 위해서는 파일에 대한 쓰기 권한이 있어야 한다.

14. 다음 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 하위 문서(고시, 지침, 기준)에 해당하지 않는 것은?
①「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」
②「집적정보 통신시설 보호지침」
③「주요정보통신기반시설 취약점 분석·평가 기준」
④「본인확인기관 지정 등에 관한 기준」

15. ASLR(Address Space Layout Randomization) 기법에 대한 설명 중 가장 적절하지 않은 것은?
① 가상 메모리의 메모리 공간 배치를 프로세스마다 다르게 설정하는 기법이다.
② return address를 변경하는 공격에 대하여 공격자가 원하는 메모리 주소를 찾기 어렵게 만든다.
③ 최신 운영체제에서는 대부분 지원된다.
④ 같은 실행 파일의 경우에는 메모리 공간 배치가 동일하게 된다.

16. 대칭키 암호화 알고리즘에 대한 설명 중 가장 적절하지 않은 것은?
① 일반적으로 비대칭키 암호화 알고리즘에 비하여 암호화/복호화 속도가 빠르다.
② 비대칭키 암호화 방법에 비하여 키 분배 및 관리가 어렵다.
③ 대칭키 암호화 알고리즘의 예로는 AES, ECC 등이 있다.
④ 암호화와 복호화를 위하여 같은 키를 사용한다.

17. 생성형 AI에서 제공하는 API(Application Programming Interface)를 이용할 때 발생할 수 있는 보안 위협으로 가장 적절한 것은?
① 보안시스템을 회피하는 복잡한 악성코드의 작성이 가능하다.
② 과도한 훈련 데이터를 암기하여 내부정보를 유출할 수 있다.
③ 연결된 서비스의 취약점을 이용하여 시스템 내부에 접근할 수 있다.
④ 악의적인 목적으로 제어할 수 없는 프롬프트를 주입할 수 있다.

18. 비밀번호 없이 본인의 스마트 기기를 통한 인증 후 온라인 서비스를 이용할 수 있는 FIDO 표준의 UAF(Universal Authentication Framework) 기능 중 플랫폼에서 적절한 인증 장치를 검색하는 기능은?
① 조회(Discovery)
② 확인(Check)
③ 처리(Process)
④ 상태(Status)

19. 공통평가기준(CC)에서 개발자가 설계 단계에서 개발방법론의 많은 변경 없이 기존 제품에 중간 수준의 보증을 제공하려고 할 때 가장 적합한 평가보증등급(EAL)은?
① EAL2 ② EAL3
③ EAL4 ④ EAL5

20. 개인정보영향평가의 수행 체계와 절차에 대한 설명 중 가장 적절한 것은?
① 개인정보보호위원회는 대상 공공기관의 사업에 적합한 영향평가 수행기관을 지정해준다.
② 영향평가 수행기관은 영향평가 수행 결과를 독립적으로 개인정보보호위원회에 제출한다.
③ 대상 공공기관은 영향평가 개선사항에 대한 이행확인서를 개인정보보호위원회에 제출한다.
④ 개인정보보호위원회는 모든 영향평가 수행 결과를 항상 심의하고 대상 공공기관에 의견을 통보한다.

21. format string 취약점에 대한 설명 중 가장 적절한 것은?
① 문자열이 잘못 정렬되었을 때 발생하는 취약점이다.
② strcpy() 함수에서 문자열을 복사할 때 발생할 수 있는 취약점이다.
③ printf() 함수에서 문자열을 출력할 때 발생할 수 있는 취약점이다.
④ 문자열을 초기화할 때 발생할 수 있는 취약점이다.

22. ROP(Return-Oriented Programming) 공격 방법에 대한 설명 중 가장 적절한 것은?
① return address를 조작하여 공격자가 입력한 코드를 실행하도록 하는 공격 방법이다.
② 함수가 return될 때, 공격자가 원하는 데이터를 전달하도록 하는 공격 방법이다.
③ 가상 메모리 영역 중 heap 영역에서 발생하는 공격 방법이다.
④ 바이너리 sequence 중에서 ret 명령어로 끝나도록 하는 sequence들을 모아서 원하는 공격을 한다.

23. strcpy() 함수와 strncpy() 함수에 대한 설명 중 가장 적절하지 않은 것은?
① strcpy() 함수는 buffer overflow를 유발시킬 수 있다.
② strncpy() 함수에서는 복사되는 문자열의 길이를 제한할 수 있다.
③ strncpy() 함수에서 문자열의 길이 제한 파라미터를 잘못 설정하면 buffer overflow가 발생할 수 있다.
④ strncpy() 함수에서는 문자열 끝에 '\0' 문자가 자동으로 추가된다.

24. IPSec의 ESP(Encasulating Security Payload)에 대한 설명으로 가장 적절한 것은?
① 트랜스포트 모드에서 원본 IP 헤더는 ESP의 인증 범위에서 제외된다.
② ESP는 IP 페이로드의 무결성을 제공하지만, 기밀성은 제공할 수 없다.
③ 터널 모드에서 새로 추가된 IP 헤더는 ESP의 인증 범위에 포함된다.
④ 터널 모드에서 원본 IP 헤더는 ESP의 암호화 범위에서 제외된다.

25. 사용자 인증 방법에서 id와 password를 이용하여 인증하는 방법에 대한 설명 중 가장 적절하지 않은 것은?
① Unix 계열의 운영체제에서는 사용자의 password 정보를 저장할 때, '사용자 아이디', 'salt 값' 그리고 'password 해시(hash)값'을 함께 저장한다.
② reactive password 검사 방법은 사용자가 password를 새로 설정할 때, 사용자가 설정한 password의 허용 여부를 검사하는 방법이다.
③ Bloom filter는 사용자가 설정하려는 password가 dictionary에 있는지 여부를 판단하기 위하여 사용할 수 있고, false negative는 0이다.
④ Linux에서는 password에 대한 정보를 안전하게 보관하기 위하여 /etc/shadow 파일에 저장하고 root 권한을 가진 사용자만 읽기/쓰기 권한을 허용한다.