

# 정보보호론(7급)

(과목코드 : 141)

2023년 군무원 채용시험

응시번호 :

성명 :

1. 정보 보안의 중요한 3대 요소에 대한 사용 예로 방화벽, 암호, 패스워드 등과 가장 관련이 있는 것은?

- ① 가용성
- ② 기밀성
- ③ 무결성
- ④ 신뢰성

2. 다음에서 설명하는 용어로 가장 적절한 것은?

- 송신자와 수신자가 공유하고 있는 키와 메시지를 혼합해서 digest value를 계산한 값이다.
- 통신 중의 오류나 수정, 가장(disguise)을 검출할 수 있다.

- ① 해시 값
- ② 일회용 패드
- ③ 메시지 인증 코드
- ④ 일회용 패스워드

3. 백도어(backdoor)에 대한 설명으로 가장 거리가 먼 것은?

- ① 정상적인 인증을 거치지 않은 상태에서 관리자 권한으로 임의의 프로그램을 수행할 수 있다.
- ② 리눅스 시스템에서 공격자는 cron 데몬을 이용하여 백도어의 동작 시간을 원하는 대로 변경할 수 있다.
- ③ 윈도우 시스템에서는 SetUID를 이용하여 백도어를 생성하고 탐지할 수 있다.
- ④ 시스템 관리자는 MD5 해시 기법을 이용하여 시스템의 변경 내용을 확인하고 백도어를 탐지할 수 있다.

4. 유닉스의 로그 중 현재 로그인한 사용자의 아이디, 사용자 프로세스, 실행 레벨, 로그인 종류 등을 기록하는 것은?

- ① utmp
- ② wtmp
- ③ sulog
- ④ syslog

5. 윈도우 침해사고 정보 분석 방법에 대한 다음 설명으로 ( ) 안에 들어갈 용어로 가장 적절한 것은?

- ( )은(는) 시스템에 탐지되지 않도록 하는 코드와 프로그램의 집합으로 시스템 관리자 권한을 획득하기 위한 프로그램이라 할 수 있다.
- 일반적으로 윈도우 공격에 성공한 후 시스템에 다운로드된 악성 프로그램 파일 및 실행된 악성 네트워크, 프로세스 정보를 숨기기 위해 ( )을(를) 연동하고 있다.

- ① MAC
- ② 루트킷
- ③ 레지스트리
- ④ 자동실행 점검

6. 다음이 설명하는 보안 솔루션으로 가장 적절한 것은?

- 사용자 수준에서 정보가 유출되는 것을 막는 솔루션을 통칭하며, 사용자의 다양한 데이터 전송 인터페이스를 제어한다.

- ① DLP
- ② NAC
- ③ DRM
- ④ 스팸 필터 솔루션

7. 모바일 기기 보안에서 블루버그에 대한 설명으로 가장 적절하지 않은 것은?

- ① 블루투스 장비 간의 취약한 연결 관리를 악용한 공격이다.
- ② 블루투스의 취약점을 이용하여 장비의 임의 파일에 접근하는 공격이다.
- ③ 이 공격을 이용하여 지하철에서 타인의 전화기로 고액을 과금하도록 전화를 건 일도 있었다.
- ④ 블루투스 기기는 한 번 연결되면 이후에는 다시 연결하지 않아도 서로 연결되는데, 이러한 인증 취약점을 이용하여 공격하는 것이다.

8. 셸(shell)에 대한 설명으로 가장 적절하지 않은 것은?

- ① 윈도우에서 볼 수 있는 명령 창도 셸이라고 할 수 있다.
- ② 운영체제를 둘러싸고 있으면서 입력받는 명령어를 실행하는 명령어 해석기이다.
- ③ 셸의 종류는 C 셸, 본 셸, 콘 셸로 나뉘는데 이 중 C 셸이 유닉스 시스템에서 사용하는 기본 셸이다.
- ④ 관리자 권한을 얻더라도 시스템에 어떤 명령을 입력할 인터페이스가 없으면 무용지물이므로 획득한 관리자 권한을 이용할 수 있는 셸이 필요하다.

9. 바이러스를 세대별로 분류할 때, 5세대인 매크로 바이러스에 대한 설명으로 가장 거리가 먼 것은?

- ① 문서 내용에 깨진 글자나 이상한 문구가 포함 되어 있다.
- ② 프로그램이 실행될 때마다 바이러스 코드 자체를 변경하여 식별자를 구분하기 어렵게 한다.
- ③ 엑셀이나 워드 작업 중 비주얼 베이직 편집기의 디버그 모드가 실행된다.
- ④ 문서가 정상적으로 열리지 않거나 암호가 설정되어 있다.

10. 다음이 설명하는 디지털 포렌식의 기본 원칙으로 가장 적절한 것은?

증거를 획득한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정이 명확해야 하며 이러한 과정을 추적할 수 있어야 한다.

- ① 무결성의 원칙
- ② 신속성의 원칙
- ③ 정당성의 원칙
- ④ 연계 보관성의 원칙

11. 다음 중 ‘클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률’에서 클라우드컴퓨팅 서비스의 보안 인증에 대한 설명으로 가장 적절하지 않은 것은?

- ① 보안인증의 유효기간은 인증 서비스 등을 고려하여 대통령령이 정하는 5년 내의 범위로 한다.
- ② 클라우드컴퓨팅서비스 제공자는 보안인증을 받은 클라우드컴퓨팅서비스에 대해 보안인증을 표시할 수 있다.
- ③ 누구든지 보안인증을 받지 아니한 클라우드 컴퓨팅서비스에 대하여 보안인증 표시를 하여서는 아니 된다.
- ④ 클라우드컴퓨팅서비스가 보안인증기준에 적합하지 아니하게 된 경우 인증 평가기관은 보안인증을 취소할 수 있다.

12. 웹의 취약점 보완에서 XSS 취약점 공격에 포함되는 특수 문자와 가장 거리가 먼 것은?

- ① <
- ② &
- ③ \*
- ④ ?

13. 서비스 거부 공격 중 프로토콜의 오류 제어 로직을 악용하여 시스템 자원을 고갈시키는 방식과 가장 거리가 먼 것은?
- ① 퐁크 공격
  - ② 랜드 공격
  - ③ 보잉크 공격
  - ④ 티어드롭 공격
14. 데이터 형태에 대한 불명확한 정의로 인해 발생하는 문제와 가장 관계가 있는 것은?
- ① 포맷 스트링 공격
  - ② 웹 프록시 공격
  - ③ 메모리 해킹 공격
  - ④ 버퍼 오버플로 공격
15. 암호화 통신에서 4계층인 전송 계층과 5계층인 세션 계층 사이의 암호화 프로토콜로 가장 적절한 것은?
- ① SSL(Secure Socket Layer)
  - ② SLIP(Serial Line Internet Protocol)
  - ③ IPSec(Internet Protocol Security Protocol)
  - ④ PPTP(Point-to-Point Tunneling Protocol)
16. 무선 네트워크 암호화에 대한 설명으로 가장 거리가 먼 것은?
- ① WEP는 최대 128비트의 암호화 키를 제공한다.
  - ② WPA-1(TKIP)은 무선 단말기와 무선 AP 사이의 공유 비밀키를 동적으로 생성하여 패킷을 암호화 한다.
  - ③ EAP를 사용하여 암호화하는 경우, 무선 네트워크 사용자와 RADIUS 서버 간 아이디와 패스워드를 통한 사용자 인증을 수행한다.
  - ④ 802.1x/EAP는 무선 랜 세션별로 재사용 가능한 암호화 키를 사용하여 암호화의 효율성을 높인다.

17. TLS에 대한 설명으로 거리가 가장 먼 것은?
- ① TLS로 통신을 수행할 때의 URL은 https://로 시작된다.
  - ② TLS에서는 통신 상대를 인증하기 위해 전자 서명을 이용한다.
  - ③ TLS 레코드 프로토콜에서는 메시지 인증 코드와 공개키 암호가 사용된다.
  - ④ TLS 핸드셰이크 프로토콜에서는 일방향 해시 함수와 공개키 암호가 사용된다.

18. 다음 접근제어 행렬(ACM: Access Control Matrix)에 대한 설명으로 가장 거리가 먼 것은?

	File A	File B	Program 1
Alice	-	own	-
Bob	read	write	execute
Sam	-	read	read write execute
Program 1	read	write	-

- ① 임의 접근제어 모델로 주체와 객체를 알고 있으면 바로 권한 확인이 가능하다.
  - ② Bob의 권한 목록(capability list)은 (File A, read), (File B, write), (Program 1, execute)이다.
  - ③ File A에 대한 접근제어 목록(access control list)은 (Alice, -), (Bob, read), (Sam, -), (Program 1, read)이다.
  - ④ Sam은 File B에 대해 read 권한만을 가지고 있다.
19. 다음 중 ARP 스푸핑 공격에 대한 보안 대책으로 가장 적절한 것은?
- ① 시스템의 IP 주소에 대한 Reverse-DNS lookup을 수행한다.
  - ② arp -s 명령을 이용하여 IP 주소와 MAC 주소를 static 상태로 변경한다.
  - ③ 서버와 클라이언트의 트러스트(trust) 관계를 사용하지 않는다.
  - ④ 호스트 파일에 중요 사이트의 IP 주소를 적어 관리한다.

20. 보안 수준에 따른 정책의 분류에 대한 설명으로 가장 적절한 것은?

- ① Standards: 소프트웨어나 하드웨어 사용 등 일반적으로 지켜야 할 보안 사항을 기술한 문서
- ② Baselines: 각각의 절차에 대한 세부 내용을 담고 있는 매뉴얼 수준의 문서
- ③ Guidelines: 조직에서 지켜야 할 가장 기본적인 보안 수준을 기술한 문서
- ④ Procedures: 특정 상황에 대한 충고나 방향 등을 제시한 문서

21. 다음 중 ISMS-P 인증에 대한 설명으로 가장 적절한 것은?

- ① 금융보안원(FSEC)은 법정 인증기관이다.
- ② 최초 인증 심사를 통해 인증을 취득하면 3년의 유효기간이 부여된다.
- ③ 인증을 취득한 이후 인증 유효기간 중 매년 2회 이상 사후 심사를 시행한다.
- ④ 인증범위로 정보서비스의 운영 및 보호에 필요한 조직, 물리적 위치, 정보자산으로 국한한다.

22. 전치 암호(transposition cipher) 및 치환 암호(substitution cipher)에 대한 설명으로 가장 거리가 먼 것은?

- ① 모든 전치 암호는 치환 암호이다.
- ② 전치 암호의 경우 평문에 사용된 문자와 암호문에 사용된 문자가 일대일 대응 규칙을 갖는다.
- ③ 다중 치환 암호의 경우 빈도 분석을 통해 암호문을 해석할 수 있다.
- ④ 비장느르 암호(Vigenere cipher)는 평문에 등장하는 문자의 빈도와 암호문에 등장하는 문자의 빈도를 다르게 만들 수 있다.

23. 다음이 설명하는 암호 알고리즘으로 가장 적절한 것은?

- 이산대수 문제에 기반을 두며, 역제곱의 역연산이 어렵다는 것에 기반한다.
- 암호화, 전자서명, 키 분배 등에 사용한다.
- 임베디드 시스템과 같은 경량 응용 분야에 적합하다.

- ① Diffie-Hellman
- ② RSA
- ③ ECC
- ④ ElGamal

24. 서비스 거부 공격 중 스머프 공격에 대한 설명으로 가장 적절하지 않은 것은?

- ① 네트워크를 공격할 때 많이 사용한다.
- ② 다이렉트 브로드캐스트를 악용하는 것으로 공격 방법이 간단하다.
- ③ ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용하여 패킷을 확장함으로써 서비스 거부 공격을 수행한다.
- ④ 패킷의 시퀀스 넘버와 길이를 조작하여 패킷 간의 데이터 부분이 겹치거나 빠진 상태로 전송하는 공격 방법이다.

25. 데이터베이스의 권한 관리에서 이미 부여된 데이터베이스 객체의 권한을 취소하는 명령어는?

- ① DENY
- ② DROP
- ③ GRANT
- ④ REVOKE