

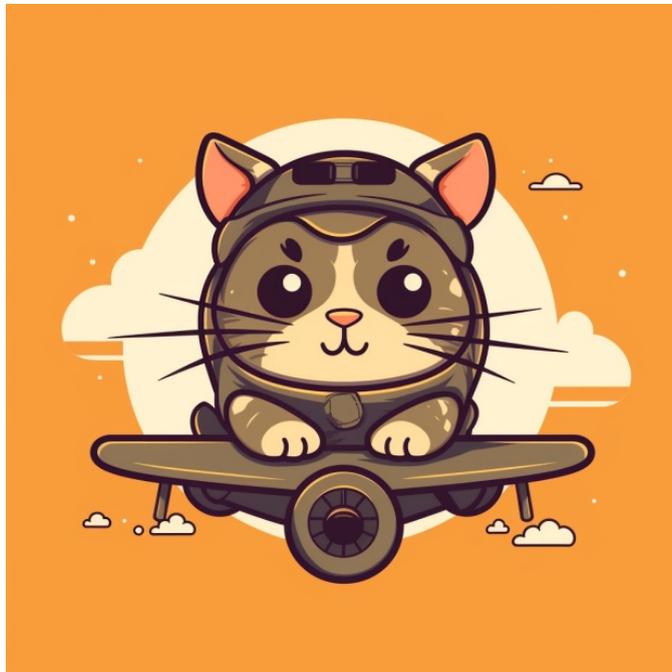


# [취업폭격기 Zeromini 위클리 개념 정밀 타격 #34] [빈칸넣기문제]

📖 과목 : 정보보호론

🔥 참고문제 : 2024년 경찰간부후보

😊 문제 수정 버전 : V 1.0



1. 문제: 정보보안에서 '\_\_\_\_\_ '는 데이터나 시스템에 대한 무단 접근, 사용, 공개, 파괴, 변경 또는 방해를 막는 과정입니다. 이는 기업이나 개인의 중요한 데이터를 보호하는데 필수적인 요소로, 다양한 보안 기술과 정책을 포함합니다. 예를 들어, 방화벽, 암호화, 접근 제어 등이 이에 해당합니다.  
답: 정보보안
2. 문제: '\_\_\_\_\_ ' 공격은 이메일, 문자 메시지 등을 통해 개인 정보를 빼내려는 사기 행위입니다. 이 방법은 종종 가짜 웹사이트나 이메일을 통해 사용자의 로그인 정보, 신용카드 번호 등을 획득하려고 시도합니다. 사용자의 주의 부족을 이용하는 이 공격 방식은

정보보안의 큰 위협 중 하나입니다.

답: 피싱

3. 문제: '\_\_\_\_\_ '은 데이터를 암호화하고 복호화하는 데 사용되는 문자열입니다. 이 키는 암호화 알고리즘과 함께 사용되어 데이터의 기밀성을 보장합니다. 키의 길이와 복잡성은 암호화의 강도를 결정하는 중요한 요소로, 보안성이 높은 시스템에서는 긴 키를 사용합니다.

답: 암호키

4. 문제: '\_\_\_\_\_ '은 컴퓨터 시스템의 취약점을 이용하여 무단으로 침입하는 사람을 말합니다. 이들은 보안 시스템을 우회하거나 취약점을 이용하여 불법적으로 정보에 접근하고, 때로는 데이터를 도용하거나 시스템을 파괴하기도 합니다. 이들로 인한 피해는 종종 심각한 수준에 이릅니다.

답: 해커

5. 문제: '\_\_\_\_\_ '은 인터넷상에서 사용자의 행동을 추적하고 데이터를 수집하는 소프트웨어 프로그램입니다. 이 프로그램은 사용자의 동의 없이 개인 정보를 수집하고, 때로는 광고 목적으로 사용됩니다. 사용자의 프라이버시 침해와 보안 위협이 되는 이 소프트웨어는 주의 깊게 관리해야 합니다.

답: 스파이웨어

6. 문제: '\_\_\_\_\_ '은 시스템이나 네트워크에 대한 무단 접근을 탐지하고 차단하는 장치 또는 소프트웨어입니다. 이는 네트워크 트래픽을 모니터링하여 의심스러운 활동이나 알려진 공격 패턴을 식별하고, 필요한 경우 경고를 발생시키거나 접근을 차단합니다. 네트워크 보안의 핵심 요소 중 하나입니다.

답: 침입 탐지 시스템 (IDS)

7. 문제: '\_\_\_\_\_ '은 네트워크 보안에서 중요한 역할을 하는 장치로, 외부 네트워크로부터 내부 네트워크를 보호합니다. 이 장치는 불법적인 네트워크 트래픽을 차단하고, 정해진 규칙에 따라 트래픽을 필터링하여 내부 네트워크의 보안을 강화합니다.

답: 방화벽

8. 문제: '\_\_\_\_\_ '는 사용자가 웹사이트에 입력한 데이터를 검증하지 않고 그대로 사용할 때 발생하는 보안 취약점입니다. 이 취약점을 이용하면 공격자는 스크립트를 삽입하여 사용자의 브라우저에서 원치 않는 동작을 유발할 수 있습니다. 이로 인해 사용자의 세션 정보가 도난당하거나 악성 코드가 실행될 수 있습니다.

답: 크로스 사이트 스크립팅 (XSS)

9. 문제: '\_\_\_\_\_ '는 네트워크 상에서 데이터를 보낼 때, 제3자가 그 데이터를 도청할 수 없도록 하는 기술입니다. 이 기술은 데이터를 암호화하여 전송함으로써, 중간에 데이터를 가로채더라도 내용을 해독할 수 없게 합니다. 인터넷 뱅킹, 온라인 쇼핑 등에서 이 기술은 개인 정보와 금융 정보의 보안을 위해 필수적입니다.

답: 암호화

10. 문제: '\_\_\_\_\_ '는 컴퓨터 시스템이나 네트워크에 해를 끼치기 위해 고안된 악성 소프트웨어입니다. 이는 컴퓨터에 침투하여 데이터를 파괴하거나 시스템을 비정상적으로 만들 수 있습니다. 바이러스, 웜, 트로이 목마 등이 이에 속합니다.  
 답: 멀웨어
11. 문제: '\_\_\_\_\_ '는 인터넷 사용자가 웹사이트에 접속할 때, 그 사이트가 신뢰할 수 있는지 확인해주는 인증서입니다. 이 인증서는 웹사이트의 신원을 확인하고, SSL/TLS 암호화를 통해 안전한 통신을 보장합니다. 사용자는 이 인증서를 통해 웹사이트의 신뢰성을 판단할 수 있습니다.  
 답: SSL 인증서
12. 문제: '\_\_\_\_\_ '는 네트워크 보안에서 중요한 개념으로, 특정 네트워크 자원에 대한 접근을 제어하는 메커니즘입니다. 이는 사용자나 그룹별로 접근 권한을 설정하여, 민감한 정보가 무단으로 접근되거나 변경되는 것을 방지합니다. 파일 시스템, 데이터베이스, 네트워크 자원 등에서 이 메커니즘을 사용합니다.  
 답: 접근 제어
13. 문제: '\_\_\_\_\_ '는 네트워크 보안에서 사용되는 프로토콜로, 원격 사용자가 인터넷을 통해 안전하게 내부 네트워크에 접속할 수 있도록 해줍니다. 이 프로토콜은 데이터를 암호화하여 전송함으로써, 외부 네트워크를 통한 안전한 통신 경로를 제공합니다. 재택 근무나 원격 접속 시 자주 사용됩니다.  
 답: VPN (Virtual Private Network)
14. 문제: '\_\_\_\_\_ '는 정보보안에서 중요한 개념으로, 데이터나 시스템이 항상 사용 가능하고 접근 가능해야 함을 의미합니다. 이는 시스템의 다운타임을 최소화하고, 데이터가 필요할 때 언제든지 접근할 수 있도록 보장하는 것을 목표로 합니다. 예를 들어, 서버의 고가용성 구성이 이 개념을 지원합니다.  
 답: 가용성
15. 문제: '\_\_\_\_\_ '는 사용자의 신원을 확인하는 과정으로, 보안 시스템에서 매우 중요합니다. 이 과정을 통해 시스템은 사용자가 자신이 주장하는 사람임을 확인하고, 적절한 접근 권한을 부여합니다. 비밀번호, 지문 인식, 얼굴 인식 등이 이 과정에 사용됩니다.  
 답: 인증
16. 문제: '\_\_\_\_\_ '는 네트워크 보안에서 중요한 역할을 하는 장치로, 내부 네트워크와 외부 네트워크 사이에 위치하여 두 네트워크 간의 트래픽을 검사하고 필터링합니다. 이 장치는 불법적인 접근을 차단하고, 내부 네트워크의 보안을 강화하는 데 중요한 역할을 합니다.  
 답: 네트워크 게이트웨이
17. 문제: '\_\_\_\_\_ '는 데이터를 보호하기 위해 사용되는 암호화 방식 중 하나로, 같은 키를 암호화와 복호화에 모두 사용합니다. 이 방식은 키 관리가 상대적으로 간단하지만, 키가 노출되면 보안이 취약해질 수 있습니다. 대칭키 암호화의 예로는 AES, DES 등이 있

습니다.

답: 대칭키 암호화

18. 문제: '\_\_\_\_\_ '는 데이터의 무결성을 보장하기 위해 사용되는 알고리즘으로, 데이터의 해시 값을 생성합니다. 이 해시 값은 데이터가 변경되지 않았음을 증명하는 데 사용되며, 데이터의 무결성 검증에 중요한 역할을 합니다. SHA-256, MD5 등이 이에 해당합니다.

답: 해시 함수

19. 문제: '\_\_\_\_\_ '는 공격자가 네트워크 서비스를 과부하 상태로 만들어 정상적인 서비스 이용을 방해하는 공격입니다. 이 공격은 대량의 트래픽을 일으켜 서버나 네트워크 자원을 소진시키며, 서비스의 가용성을 저하시킵니다. 이러한 공격을 방지하기 위해 다양한 보안 조치가 필요합니다.

답: DDoS (Distributed Denial of Service)

20. 문제: '\_\_\_\_\_ '는 개인이나 조직의 중요한 정보를 암호화한 후, 이를 해제하기 위해 금전을 요구하는 악성 소프트웨어입니다. 이 소프트웨어는 사용자의 파일을 인질로 삼아 금전적 이득을 취하려고 하며, 최근 몇 년간 큰 피해를 주고 있는 사이버 범죄 유형 중 하나입니다.

답: 랜섬웨어

21. 문제: '\_\_\_\_\_ '는 조직 내에서 정보보안 정책을 수립하고 관리하는 프로세스입니다. 이 과정은 조직의 보안 목표를 설정하고, 위험을 평가하며, 적절한 보안 조치를 구현하는 것을 포함합니다. 이는 조직의 정보 자산을 보호하고, 보안 위험을 관리하는 데 중요한 역할을 합니다.

답: 정보보안 거버넌스

22. 문제: '\_\_\_\_\_ '는 특정한 암호화 키를 생성하기 위해 사용자의 비밀번호와 결합되는 데이터 조각입니다. 이 방법은 같은 비밀번호라도 다른 키를 생성하게 하여, 암호화된 데이터의 보안을 강화합니다. 이는 특히 데이터베이스에 저장된 비밀번호의 보안을 강화하는 데 사용됩니다.

답: 솔트 (Salt)

23. 문제: '\_\_\_\_\_ '는 조직이나 개인이 인터넷을 통해 서비스를 제공할 때 발생할 수 있는 법적, 기술적, 운영적 위험을 관리하는 과정입니다. 이는 웹사이트의 보안, 사용자 데이터의 보호, 온라인 거래의 안전성 등을 포함합니다. 온라인 비즈니스에서 이 과정은 매우 중요하며, 다양한 보안 기술과 정책을 필요로 합니다.

답: 사이버 위험 관리

24. 문제: '\_\_\_\_\_ '는 조직의 컴퓨터 시스템, 네트워크, 데이터에 대한 물리적 및 전자적 보호를 제공하는 프로세스입니다. 이는 불법 접근, 사용, 공개, 파괴, 변경을 방지하기 위한 다양한 보안 조치를 포함합니다. 예를 들어, 데이터 센터의 물리적 보안, 네트워크 보

안, 애플리케이션 보안 등이 이에 해당합니다.

답: 정보보안 관리

25. 문제: '\_\_\_\_\_ '는 조직이나 개인이 정보보안 위험을 식별하고 평가하는 과정입니다. 이 과정은 잠재적인 보안 위협을 파악하고, 그 위협을 완화하기 위한 적절한 조치를 결정하는 데 도움을 줍니다. 위험 평가는 정보보안 관리의 핵심 요소 중 하나로, 지속적인 보안 강화를 위해 정기적으로 수행되어야 합니다.

답: 위험 평가

26. 문제: 정보보안에서 '\_\_\_\_\_ '는 자산에 대한 위협원의 공격 행동을 의미합니다. 이는 보안 위협을 이해하는 데 중요한 개념으로, 보안 체계를 구축할 때 고려해야 할 요소입니다. 예를 들어, 해커의 공격, 바이러스, 시스템의 취약점 등이 이에 해당합니다. 이러한 위협을 식별하고 평가하는 것은 정보보안 관리의 핵심적인 부분입니다.

답: 위협

27. 문제: '\_\_\_\_\_ '는 정보보안에서 자산이 가지고 있는 속성이거나 보안 대책의 미비점을 의미합니다. 이는 보안 위협을 평가하고 관리하는 데 중요한 요소로, 적절한 보안 대책을 수립하는 데 필수적입니다. 예를 들어, 암호화되지 않은 데이터, 업데이트되지 않은 소프트웨어 등이 이에 해당할 수 있습니다. 이러한 취약점을 파악하고 강화하는 것은 보안 사고를 예방하는 데 중요합니다.

답: 취약점

28. 문제: RSA 암호화 방식에서 두 소수  $(p)$ 와  $(q)$ 를 사용하여  $(n = p \times q)$ 를 구성하고, 암호화 키가  $(e)$ 일 때, 복호화 키  $(d)$ 는 법(modulus)  $(\phi(n))$ 에서  $(e)$ 의 '\_\_\_\_\_ '입니다. 예를 들어,  $(p = 5)$ ,  $(q = 11)$ 이고  $(e = 7)$ 일 때,  $(d)$ 의 값은 특정 계산을 통해 구할 수 있습니다. RSA는 공개키 암호화 방식의 대표적인 예로, 안전한 통신을 위해 널리 사용됩니다.

답: 승산역원

29. 문제: '\_\_\_\_\_ '는 정보보안에서 암호화 모드 중 하나로, 동일한 키에 의한 동일한 평문 블록은 항상 동일한 암호문을 출력합니다. 이 모드의 특징은 동일한 평문 블록이 암호화될 때마다 같은 암호문 블록이 생성된다는 것입니다. 이러한 특성 때문에 특정 패턴의 평문이 반복될 경우 보안 취약점이 될 수 있습니다.

답: ECB 모드

30. 문제: '\_\_\_\_\_ '는 공개키 암호방식을 이용하여 전자서명을 생성하고 검증할 때 사용되는 키입니다. 송신자가 전자서명을 생성하고 수신자에게 전자서명을 전송하는 경우, 수신자가 전자서명을 검증할 때 사용하는 이 키는 보안 통신에서 중요한 역할을 합니다. 이 키를 통해 수신자는 송신자의 신원을 확인하고, 메시지의 무결성을 검증할 수 있습니다.

답: 송신자의 공개키

31. 문제: '\_\_\_\_\_ '는 정보보안에서 사용되는 해시 알고리즘의 한 종류로, 160비트의 해시 값을 출력합니다. 이 알고리즘은 데이터의 무결성을 확인하는 데 사용되며, 데이터가 변경되지 않았음을 증명하는 데 중요한 역할을 합니다. 해시 알고리즘은 데이터의 원본 내용을 알 수 없게 하면서도, 데이터의 변경 여부를 확인할 수 있는 방법을 제공합니다.  
 답: SHA-1
32. 문제: '\_\_\_\_\_ '는 공개키 암호방식 중 하나로, 전자서명, 암호화, 키 교환에 사용될 수 있는 기법입니다. 이 기법은 소인수분해의 어려움을 이용하며, 일반적으로 암호문의 길이가 평문의 길이보다 짧습니다. 이 암호방식은 안전한 디지털 통신을 위해 중요하며, 다양한 보안 애플리케이션에서 활용됩니다.  
 답: ElGamal 암호방식
33. 문제: '\_\_\_\_\_ '는 타원곡선암호시스템(ECC)에서 사용되는 방정식의 형태로, 이는 암호학에서 중요한 역할을 합니다. 이 방정식은 타원곡선상의 점들을 정의하며, 이 점들을 사용하여 암호화 및 복호화 과정을 수행합니다. ECC는 고전 암호방식에 비해 더 작은 키 크기로 높은 보안 수준을 제공합니다.  
 답:  $y^2 = x^3 + ax + b$
34. 문제: '\_\_\_\_\_ '는 메시지 인증 코드(MAC)의 한 형태로, 일방향 해시 함수를 이용하여 메시지의 인증 코드를 생성합니다. 이 기법은 메시지의 무결성과 인증을 동시에 제공하며, 네트워크 보안에서 중요한 역할을 합니다. 이를 통해 전송된 메시지가 변경되지 않았음을 확인하고, 메시지의 출처를 검증할 수 있습니다.  
 답: HMAC
35. 문제: '\_\_\_\_\_ '는 전자지불시스템에서 중요한 정보보호 요구사항 중 하나로, 거래하는 전자화폐는 위조가 불가능해야 합니다. 이 요구사항은 전자화폐 시스템의 신뢰성을 보장하며, 사용자가 안전하게 전자화폐를 사용할 수 있도록 합니다. 전자화폐의 위조 방지는 전자상거래의 보안과 직결되는 중요한 요소입니다.  
 답: 위조 불가능성