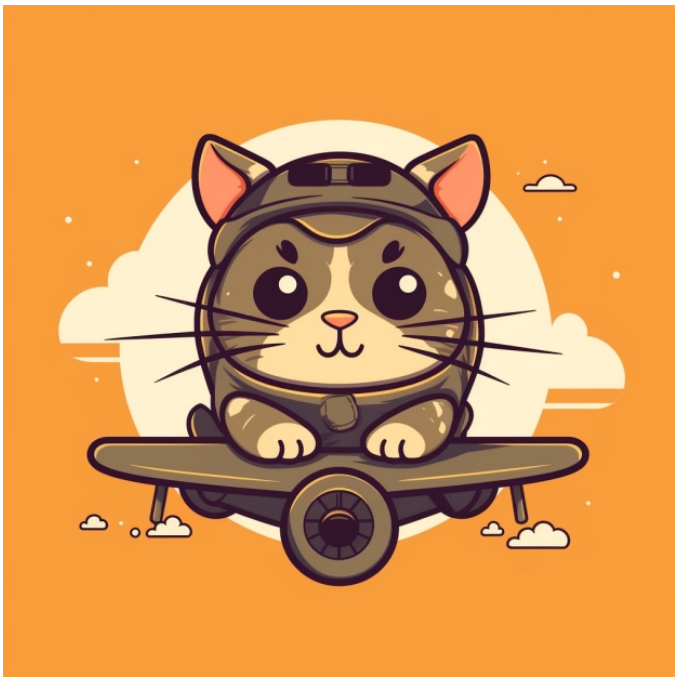
🥷

[취업폭격기 Zeromini 위클리 개념 폭격 #27]

📕 과목 : 정보보호론

🔥 참고문제 : 2021년 공무원 7급

🌝 문제 수정 버전 : V 1.0



1. **사용자 인증 기술**
   문제: 사용자 인증에 사용되는 기술 중 Smart Card와 Single Sign-On의 특징과 차이점을 설명하세요.
   해설: Smart Card는 물리적인 카드 형태의 보안 토큰으로, 사용자 인증에 필요한 정보를 저장합니다. 반면, Single Sign-On은 한 번의 로그인으로 여러 시스템에 접근할 수 있게 하는 기술로, 사용자 편의성을 높이고 관리 비용을 줄입니다. 두 기술은 보안 수준과 사용 편의성에서 차이를 보입니다.

2. **제로데이 공격**
   문제: 제로데이 공격의 개념과 이에 대응하기 위한 기본적인 보안 전략에 대해 설명하세요.
   해설: 제로데이 공격은 보안 취약점이 공개되기 전에 이루어지는 공격을 말합니다. 이러한 공격에 대응하기 위해서는 정기적인 시스템 업데이트와 패치 적용, 침입 탐지 시스템의 활용, 최소 권한 원칙의 적용 등이 필요합니다. 또한, 보안 인식 교육을 통해 사용자의 경각심을 높이는 것도 중요합니다.

3. **IPSec 프로토콜**
   문제: IPSec 프로토콜의 주요 기능과 이를 통해 달성하고자 하는 보안 목표에 대해 설명하세요.
   해설: IPSec 프로토콜은 인터넷 프로토콜 보안을 위해 설계된 프로토콜로, 데이터의 기밀성, 무결성, 인증을 제공합니다. 이는 Authentication Header와 Encapsulating Security Payload를 통해 이루어지며, VPN 구축에 주로 사용됩니다. IPSec은 네트워크 계층에서 작동하여 다양한 애플리케이션과 호환됩니다.

4. **악성코드의 유형**
   문제: 스파이웨어(Spyware)와 랜섬웨어(Ransomware)의 정의와 주요 차이점에 대해 설명하세요.
   해설: 스파이웨어는 사용자의 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성 소프트웨어입니다. 주로 개인정보나 금융정보를 목표로 합니다. 반면, 랜섬웨어는 사용자의 파일을 암호화하고 이를 해제하기 위해 금전을 요구하는 악성 소프트웨어입니다. 랜섬웨어는 데이터 접근을 차단하여 사용자에게 직접적인 피해를 입힙니다.

5. **블루투스 공격**
   문제: 블루스나핑(Bluesnarfing)과 블루버깅(Bluebugging) 공격의 개념과 차이점에 대해 설명하세요.
   해설: 블루스나핑은 블루투스 장치의 보안 취약점을 이용하여 장치 내 저장된 데이터에 접근하는 공격입니다. 반면, 블루버깅은 블루투스 장치를 제어하여 통화나 메시지 전송 등을 조작하는 공격입니다. 블루스나핑은 주로 데이터 도난에, 블루버깅은 장치 제어에 초점을 맞춥니다.

6. **암호화 방식**
   문제: 대칭키 암호화와 공개키 암호화의 기본 원리와 각각의 장단점에 대해 설명하세요.
   해설: 대칭키 암호화는 암호화와 복호화에 같은 키를 사용하는 방식으로, 처리 속도가 빠르고 효율적입니다. 하지만 키 분배가 어렵다는 단점이 있습니다. 반면, 공개키 암호화는 암호화에는 공개키를, 복호화에는 비밀키를 사용하는 방식으로, 키 분배 문제를 해결했으나 대칭키 암호화에 비해 처리 속도가 느립니다.

7. **해시 함수**
   문제: 해시 함수의 역할과 MD5, SHA와 같은 해시 알고리즘의 특징에 대해 설명하세요.

해설: 해시 함수는 임의의 길이의 데이터를 고정된 길이의 해시값으로 변환하는 역할을 합니다. 이를 통해 데이터의 무결성 검증에 사용됩니다. MD5와 SHA는 대표적인 해시 알고리즘으로, 빠른 처리 속도와 충돌 방지 기능을 가지고 있으나, MD5는 보안 취약점이 발견되어 SHA가 더 널리 사용됩니다.

8. **PPTP 프로토콜**
   문제: PPTP(Point-to-Point Tunneling Protocol)의 주요 기능과 VPN 구축에서의 역할에 대해 설명하세요.
   해설: PPTP는 VPN을 구축하기 위한 프로토콜 중 하나로, 포인트 투 포인트 방식을 사용하여 가상 터널을 생성합니다. 이를 통해 원격 사용자가 사설 네트워크에 안전하게 접근할 수 있도록 합니다. PPTP는 구현이 간단하고 호환성이 좋지만, 보안성이 상대적으로 낮다는 단점이 있습니다.

9. **개인정보보호법**
   문제: 개인정보보호법상 정보주체의 권리 중 하나를 선택하여 그 내용과 중요성에 대해 설명하세요.
   해설: 개인정보보호법은 정보주체의 권리를 보장합니다. 예를 들어, 정보주체는 자신의 개인정보에 대한 접근, 정정, 삭제 요구권을 가집니다. 이는 개인의 사생활 보호와 자기 결정권을 강화하며, 개인정보의 오용이나 남용으로부터 보호하는 데 중요한 역할을 합니다.

10. **블록체인과 비트코인**
    문제: 블록체인 기술과 비트코인에서의 활용에 대해 간략히 설명하세요.
    해설: 블록체인은 분산된 데이터베이스로, 거래 기록을 블록에 연쇄적으로 저장하는 기술입니다. 비트코인은 이 블록체인 기술을 활용한 첫 번째 암호화폐로, 중앙 기관 없이 사용자 간 직접 거래를 가능하게 합니다. 블록체인의 투명성과 변경 불가능성은 비트코인의 신뢰성과 보안성을 보장합니다.

11. **OSI 7계층**
    문제: OSI 7계층 모델 중 하나를 선택하여 그 계층의 기능과 중요성에 대해 설명하세요.
    해설: OSI 7계층 모델의 각 계층은 네트워크 통신에서 특정 기능을 담당합니다. 예를 들어, 전송 계층(Transport Layer)은 데이터 전송의 신뢰성과 효율성을 보장합니다. 이 계층은 데이터의 분할, 전송, 재조립을 담당하며, 오류 검출 및 복구 기능을 제공하여 안정적인 데이터 전송을 지원합니다.

12. **VPN 기술**
    문제: VPN(Virtual Private Network)의 기본 원리와 기업에서의 활용 예를 설명하세요.
    해설: VPN은 공용 인터넷을 통해 가상의 사설 네트워크를 구축하는 기술입니다. 이를 통해 원격지 사용자가 회사의 내부 네트워크에 안전하게 접근할 수 있습니다. VPN은 데이터 암호화와 인증을 통해 보안을 강화하며, 기업은 원격 근무, 보안된 데이터 전송, 지사 간 네트워크 연결 등에 VPN을 활용합니다.

13. **정보보호 관리체계 인증기준**
    문제: 정보보호 관리체계 인증기준 중 하나를 선택하여 그 기준의 내용과 중요성에 대해 설명하세요.
    해설: 정보보호 관리체계 인증기준 중 '인증 및 권한 관리'는 사용자 인증과 접근 권한을 체계적으로 관리하는 것을 말합니다. 이는 불법 접근을 방지하고 정보 자산을 보호하는 데 중요합니다. 조직은 강력한 인증 메커니즘과 역할 기반 접근 제어를 통해 정보 보안을 강화할 수 있습니다.

14. **웹 해킹 공격**
    문제: 크로스 사이트 스크립팅(Cross-Site Scripting, XSS) 공격의 원리와 예방 방법에 대해 설명하세요.
    해설: XSS 공격은 악성 스크립트를 웹 페이지에 삽입하여 사용자의 브라우저에서 실행되게 하는 공격입니다. 이를 통해 사용자의 세션 정보를 탈취할 수 있습니다. 예방 방법으로는 사용자 입력에 대한 검증과 적절한 코딩 기법, 콘텐츠 보안 정책(CSP)의 적용 등이 있습니다.

15. **NAC(Network Access Control)**
    문제: NAC의 주요 기능과 기업 네트워크에서의 역할에 대해 설명하세요.
    해설: NAC는 네트워크 접근 제어를 위한 기술로, 사용자 및 장치의 식별, 인증, 접근 정책 적용을 담당합니다. 기업 네트워크에서 NAC는 불법 접근을 방지하고, 네트워크 자원의 보안을 강화하는 역할을 합니다. 또한, 네트워크 상태 모니터링과 보안 정책의 일관된 적용을 가능하게 합니다.

16. **WTLS 레코드 프로토콜**
    문제: WTLS(Wireless Transport Layer Security) 레코드 프로토콜의 주요 기능과 무선 환경에서의 중요성에 대해 설명하세요.
    해설: WTLS는 무선 환경에서 데이터의 기밀성과 무결성을 보장하는 프로토콜입니다. 이는 SSL/TLS의 무선 버전으로, 데이터 암호화, 인증, 메시지 무결성 검증 등을 제공합니다. 무선 네트워크의 제한된 대역폭과 높은 오류율을 고려하여 최적화되었으며, 무선 인터넷 트랜잭션의 보안을 강화하는 데 중요한 역할을 합니다.

17. **보안 솔루션**
    문제: IPS(Intrusion Prevention System)와 IDS(Intrusion Detection System)의 차이점과 각각의 역할에 대해 설명하세요.
    해설: IPS는 네트워크에 침입을 시도하는 악의적인 트래픽을 실시간으로 탐지하고 차단하는 시스템입니다. 반면, IDS는 침입을 탐지하고 알림을 제공하지만, 자동으로 차단하지는 않습니다. IPS는 능동적인 보안 조치를 제공하는 반면, IDS는 보안 위협을 모니터링하고 분석하는 데 중점을 둡니다.

18. **CERT(Computer Emergency Response Team)**
    문제: CERT의 주요 역할과 사이버 보안에서의 중요성에 대해 설명하세요.

해설: CERT는 컴퓨터 보안 사고에 대응하는 전문 팀으로, 사이버 공격의 탐지, 분석, 대응을 담당합니다. 이들은 보안 취약점 정보를 제공하고, 대규모 사이버 공격에 대한 경고 및 대응 방안을 조정합니다. CERT는 조직의 사이버 보안 체계를 강화하고, 신속한 사고 대응을 통해 피해를 최소화하는 데 중요한 역할을 합니다.

19. **정보보안 거버넌스**
    문제: 정보보안 거버넌스의 주요 구성 요소 중 하나를 선택하여 그 중요성과 구현 방법에 대해 설명하세요.
    해설: 정보보안 거버넌스의 핵심 요소 중 '전략적 연계'는 조직의 전략과 정보보안 전략을 일치시키는 것을 의미합니다. 이를 통해 조직의 목표와 보안 목표가 상호 보완적으로 작동하도록 합니다. 구현을 위해서는 경영진의 참여, 보안 정책의 명확한 정의, 전사적인 보안 인식 제고가 필요합니다.

20. **정보통신기반보호법**
    문제: 정보통신기반보호법의 주요 목적과 이를 통해 달성하고자 하는 보안 목표에 대해 설명하세요.
    해설: 정보통신기반보호법은 국가의 중요 정보통신 기반 시설을 보호하기 위해 제정되었습니다. 이 법은 중요 시설의 식별, 보호, 침해사고 대응 체계 구축을 목표로 합니다. 이를 통해 국가 안보와 공공의 안전을 보장하며, 사이버 공격으로 인한 피해를 최소화하고자 합니다.

21. **TCSEC(Trusted Computer System Evaluation Criteria)**
    문제: TCSEC의 등급 체계 중 하나를 선택하여 그 등급의 특징과 보안 평가에서의 역할에 대해 설명하세요.
    해설: TCSEC의 등급 중 'B1'은 '레이블된 보안 보호'를 제공합니다. 이 등급은 각 데이터에 보안 레이블을 부여하고, 사용자의 접근 권한을 체계적으로 관리합니다. B1 등급의 시스템은 중간 수준의 보안 요구사항을 충족하며, 보안 평가에서 데이터 분류와 접근 제어의 적절성을 검증합니다.

22. **본인확인기관 지정**
    문제: 본인확인기관의 역할과 온라인 환경에서의 중요성에 대해 설명하세요.
    해설: 본인확인기관은 온라인 서비스에서 사용자의 신원을 확인하는 역할을 합니다. 이는 온라인 거래의 신뢰성을 높이고, 사기나 부정 사용을 방지하는 데 중요합니다. 본인확인기관은 신원 확인 절차의 안전성과 정확성을 보장하며, 사용자의 개인정보 보호에도 기여합니다.

23. **RADIUS 프로토콜**
    문제: RADIUS(Remote Authentication Dial-In User Service) 프로토콜의 주요 기능과 네트워크 보안에서의 역할에 대해 설명하세요.
    해설: RADIUS는 네트워크 접근 제어와 계정 관리를 위한 프로토콜입니다. 이는 사용자 인증, 권한 부여, 계정 정보 기록을 중앙화된 방식으로 관리합니다. RADIUS는 VPN, 무

선 네트워크 등에서 사용자 인증을 강화하며, 네트워크 자원의 보안을 효과적으로 관리합니다.

24. **정보보호 및 개인정보보호 관리체계 인증**
    문제: 정보보호 및 개인정보보호 관리체계 인증의 목적과 조직에 미치는 영향에 대해 설명하세요.
    해설: 이 인증은 조직의 정보보호 및 개인정보보호 관리 체계의 적합성을 평가하고 인증하는 것을 목적으로 합니다. 이를 통해 조직은 정보보호 관리의 표준화와 체계화를 달성하며, 신뢰성과 법적 준수를 강화할 수 있습니다. 또한, 고객과 이해관계자에게 보안에 대한 신뢰를 제공합니다.

25. **사이버 보안 인시던트 대응**
    문제: 사이버 보안 인시던트 대응 계획의 주요 구성 요소와 그 중요성에 대해 설명하세요.
    해설: 사이버 보안 인시던트 대응 계획은 인시던트 발생 시 신속하고 효과적으로 대응하기 위한 지침을 제공합니다. 주요 구성 요소로는 인시던트 식별 및 평가, 대응 절차, 통신 계획, 복구 및 후속 조치가 있습니다. 이 계획은 사이버 위협으로부터 조직의 자산을 보호하고, 인시던트의 영향을 최소화하는 데 중요한 역할을 합니다.

26. **데이터 암호화 표준**
    문제: AES(Advanced Encryption Standard) 암호화 알고리즘의 특징과 사용되는 분야에 대해 설명하세요.
    해설: AES는 대칭키 암호화 방식의 표준 알고리즘으로, 높은 보안성과 효율성을 제공합니다. AES는 128, 192, 256비트의 키 길이를 지원하며, 블록 암호화 방식을 사용합니다. 이 알고리즘은 정부 및 금융 기관의 데이터 보호, 무선 네트워크 보안, 파일 암호화 등 다양한 분야에서 널리 사용됩니다.

27. **네트워크 보안 프로토콜**
    문제: SSL(Secure Sockets Layer)과 TLS(Transport Layer Security) 프로토콜의 주요 기능과 차이점에 대해 설명하세요.
    해설: SSL과 TLS는 데이터 전송 시 기밀성과 무결성을 보장하는 보안 프로토콜입니다. SSL은 초기의 프로토콜이며, TLS는 SSL의 후속 버전으로 더 강화된 보안 기능을 제공합니다. 두 프로토콜은 암호화된 연결을 통해 인터넷 통신의 보안을 강화하지만, TLS는 보안 알고리즘과 프로토콜의 효율성 면에서 개선된 점이 있습니다.

28. **사이버 위협 인텔리전스**
    문제: 사이버 위협 인텔리전스의 개념과 조직에 미치는 영향에 대해 설명하세요.
    해설: 사이버 위협 인텔리전스는 사이버 공격의 동향, 전술, 기술을 분석하여 조직의 보안을 강화하는 정보입니다. 이를 통해 조직은 잠재적 위협을 사전에 파악하고, 적절한 보안 대책을 수립할 수 있습니다. 위협 인텔리전스는 조직의 사이버 보안 체계를 예방적으로 강화하는 데 중요한 역할을 합니다.

29. **클라우드 보안**
    문제: 클라우드 컴퓨팅 환경에서의 보안 과제와 해결 방안에 대해 설명하세요.
    해설: 클라우드 컴퓨팅 환경은 데이터의 중앙화, 다중 사용자 접근, 원격 서비스 제공 등으로 인해 특유의 보안 과제를 가집니다. 이러한 과제에 대응하기 위해 데이터 암호화, 접근 제어, 보안 인증, 네트워크 보안 강화 등의 방안이 필요합니다. 또한, 클라우드 서비스 제공업체와의 보안 협력도 중요합니다.

30. **모바일 보안**
    문제: 모바일 기기와 애플리케이션의 보안 위협과 이에 대한 예방 조치에 대해 설명하세요.
    해설: 모바일 기기와 애플리케이션은 악성 소프트웨어, 데이터 유출, 무단 접근 등 다양한 보안 위협에 노출되어 있습니다. 이를 예방하기 위해서는 강력한 암호화, 정기적인 소프트웨어 업데이트, 안전한 애플리케이션 사용, 다중 인증 방식의 적용 등이 필요합니다. 사용자 교육과 보안 인식 제고도 중요한 요소입니다.

31. **사이버 공격 유형**
    문제: 피싱(Phishing) 공격의 주요 특징과 이를 방지하기 위한 조직의 대응 방법에 대해 설명하세요.
    해설: 피싱은 가짜 웹사이트나 이메일을 통해 사용자의 개인정보를 탈취하는 사이버 공격입니다. 이를 방지하기 위해 조직은 직원들에게 피싱 이메일의 식별 방법을 교육하고, 정기적인 보안 훈련을 실시해야 합니다. 또한, 이메일 필터링 시스템과 다중 인증 방식을 도입하여 보안을 강화할 수 있습니다.

32. **사이버 보안 법률 및 규정**
    문제: GDPR(General Data Protection Regulation)의 주요 내용과 이 규정이 기업에 미치는 영향에 대해 설명하세요.
    해설: GDPR은 유럽연합의 개인정보 보호 규정으로, 개인 데이터의 처리와 이전에 대한 엄격한 규제를 제공합니다. 이 규정은 기업에게 사용자의 동의를 필수로 하고, 데이터 침해 시 신속한 보고를 요구합니다. GDPR 준수는 글로벌 비즈니스에서 신뢰성을 높이고 법적 위험을 줄이는 데 중요합니다.

33. **사이버 보안 기술**
    문제: 머신 러닝을 활용한 사이버 보안의 장점과 이를 적용할 때 고려해야 할 사항에 대해 설명하세요.
    해설: 머신 러닝은 대규모 데이터 분석을 통해 사이버 위협을 식별하고 예측하는 데 사용됩니다. 이 기술은 빠른 위협 탐지와 자동화된 대응을 가능하게 합니다. 하지만, 효과적인 적용을 위해서는 충분한 훈련 데이터와 지속적인 모델 업데이트가 필요하며, 오진의 가능성도 고려해야 합니다.

34. **네트워크 보안 관리**
    문제: 방화벽(Firewall)의 기능과 네트워크 보안에서의 역할에 대해 설명하세요.

해설: 방화벽은 네트워크와 외부의 통신을 제어하여 무단 접근과 네트워크 공격을 차단하는 장치입니다. 이는 인바운드 및 아웃바운드 트래픽을 모니터링하고, 사전에 정의된 보안 규칙에 따라 트래픽을 허용하거나 차단합니다. 방화벽은 네트워크의 첫 번째 방어선으로서 중요한 역할을 합니다.

35. **데이터 보안**
    문제: 데이터 마스킹(Data Masking)의 개념과 데이터 보호에서의 중요성에 대해 설명하세요.
    해설: 데이터 마스킹은 중요한 데이터를 가리거나 변형하여 실제 데이터를 보호하는 기술입니다. 이는 테스트 환경이나 외부에 데이터를 제공할 때 실제 데이터의 노출을 방지합니다. 데이터 마스킹은 개인정보 보호와 데이터 유출 방지에 중요한 역할을 하며, 법적 준수를 지원합니다.

36. **사이버 보안 인식 및 교육**
    문제: 조직 내 사이버 보안 인식 향상을 위한 효과적인 교육 방법에 대해 설명하세요.
    해설: 사이버 보안 인식 교육은 직원들이 보안 위협을 인식하고 적절하게 대응할 수 있도록 하는 데 중요합니다. 효과적인 교육 방법으로는 실제 사례 기반의 학습, 정기적인 훈련 및 시뮬레이션, 인터랙티브한 교육 콘텐츠 제공, 보안 정책과 절차에 대한 명확한 안내가 있습니다.

37. **사이버 보안 정책**
    문제: 조직의 사이버 보안 정책 수립 시 고려해야 할 주요 요소에 대해 설명하세요.
    해설: 사이버 보안 정책은 조직의 보안 목표, 규정 준수 요구사항, 위험 관리 전략을 명확하게 정의해야 합니다. 정책 수립 시 조직의 자산, 기술 환경, 인력, 보안 위협 등을 고려해야 하며, 정책은 지속적으로 검토하고 업데이트되어야 합니다.

38. **사이버 보안 위험 관리**
    문제: 사이버 보안 위험 관리의 주요 과정과 조직에 미치는 영향에 대해 설명하세요.
    해설: 사이버 보안 위험 관리는 위험 식별, 평가, 완화, 모니터링의 과정을 포함합니다. 이 과정을 통해 조직은 잠재적인 보안 위협을 파악하고, 적절한 보안 조치를 취할 수 있습니다. 위험 관리는 조직의 자산 보호와 비즈니스 연속성을 유지하는 데 중요한 역할을 합니다.

39. **사이버 보안 감사**
    문제: 사이버 보안 감사의 목적과 감사 과정에서 수행되는 주요 활동에 대해 설명하세요.
    해설: 사이버 보안 감사는 조직의 보안 체계와 정책이 적절하게 운영되고 있는지 평가하는 과정입니다. 감사 활동에는 보안 정책의 적합성 검토, 보안 인프라와 시스템의 취약점 분석, 보안 사고 대응 절차의 효과성 평가 등이 포함됩니다. 이는 조직의 보안 수준을 향상시키고 규정 준수를 보장하는 데 중요합니다.

40. **사이버 보안 기술 동향**
    문제: 현재 사이버 보안 분야에서 주목받고 있는 기술 동향 중 하나를 선택하여 그 중요

성과 잠재적 영향에 대해 설명하세요.
해설: 인공지능(AI)과 머신 러닝은 사이버 보안에서 중요한 동향입니다. 이 기술들은 대량의 데이터 분석을 통해 사이버 위협을 식별하고 예측하는 데 사용됩니다. AI의 자동화된 위협 탐지와 대응은 보안 효율성을 크게 향상시키며, 미래의 사이버 보안 전략에 중요한 역할을 할 것으로 예상됩니다.