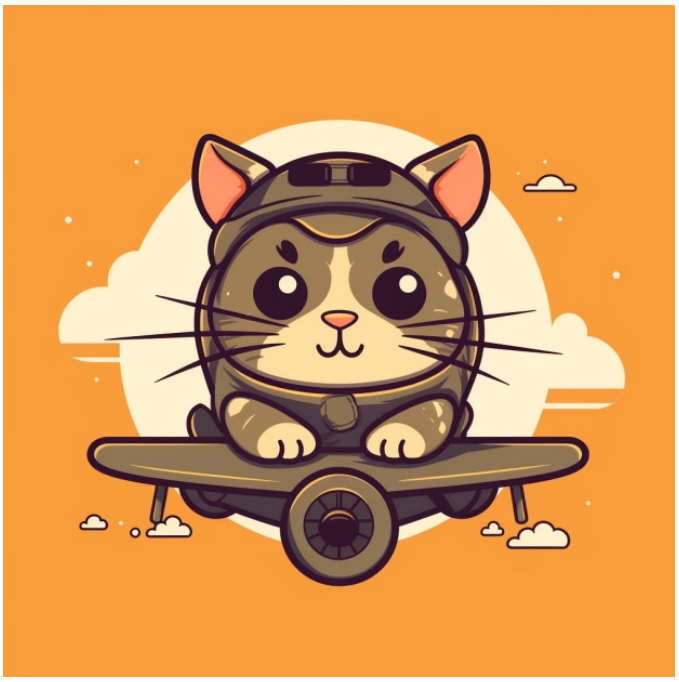
🥷

[취업폭격기 Zeromini 위클리 개념 폭격 #20]

📕 과목 : 정보보호론

🔥 참고문제 : 2023년 국가직 7급

🌝 문제 수정 버전 : V 1.0



1. **정보보호론**
   문제: 정보보호론에서 검증된 시스템 사용자가 시스템 자원에 접근할 수 있도록 허락하는 과정과 이 과정에서 중요한 4가지 단계를 설명하시오.
   해설: 정보보호론에서 시스템 사용자의 검증 후 자원 접근 허락 과정은 크게 4가지 단계로 나뉩니다. 첫째, Authentication은 사용자의 신원을 확인하는 과정입니다. 둘째, Authorization은 사용자에게 특정 자원에 대한 접근 권한을 부여하는 과정입니다. 셋째, Audit는 사용자의 접근 및 활동 로그를 기록하는 과정이며, 마지막으로 Accounting은 사용자의 활동을 기반으로 비용을 계산하거나 청구하는 과정입니다.

2. **위험 대처 방식**
   문제: 정보보호론에서 도출된 위험에 대한 보안 대책 마련을 위한 방식 중, 잠재적 위험을 자체적으로 감수하는 방식과 시스템 기능의 일부 사용 포기에 따른 불편함을 감수하는 방식에 해당하는 두 가지를 설명하시오.
   해설: 정보보호론에서 위험 대처 방식 중 잠재적 위험을 자체적으로 감수하는 방식은 '위험 수용'이라고 합니다. 이는 위험을 직접적으로 해결하거나 대응하지 않고 그대로 받아들이는 방식입니다. 또한, 시스템 기능의 일부 사용을 포기하여 불편함을 감수하는 방식은 '위험 회피'로, 특정 위험을 피하기 위해 관련 기능이나 서비스를 중단하거나 사용하지 않는 방식을 의미합니다.

3. **해시 충돌**
   문제: 해시 함수에서 입력값이 다르지만 출력값이 동일한 경우를 무엇이라고 하며, 이러한 현상이 발생하는 원인과 그로 인한 위험성에 대해 설명하시오.
   해설: 해시 함수에서 입력값이 다르지만 출력값이 동일한 경우를 '해시 충돌'이라고 합니다. 이러한 현상은 해시 함수의 출력 범위보다 입력 범위가 크기 때문에 발생합니다. 해시 충돌로 인한 위험성은 암호화된 데이터의 무결성이 손상될 수 있으며, 악의적인 공격자가 충돌을 이용해 정보를 변조하거나 접근할 수 있는 가능성이 있습니다.

4. **메시지 인증 코드(MAC)**
   문제: 메시지 인증 코드(MAC)의 정의와 그것을 사용하기 위한 필요한 조건, 그리고 MAC의 주요 기능에 대해 설명하시오.
   해설: 메시지 인증 코드(MAC)는 메시지의 무결성과 인증을 보장하기 위한 코드입니다. MAC을 사용하기 위해서는 송·수신자 간의 공유된 비밀키가 필요합니다. MAC의 주요 기능은 메시지와 함께 전달되어 메시지의 무결성을 검증하며, 수신자는 MAC을 통해 메시지가 송신자로부터 전송된 것을 확인할 수 있습니다.

5. **디지털 서명**
   문제: 디지털 서명의 기본 원리와 그것을 사용하여 메시지의 무결성과 발신자의 인증을 어떻게 보장하는지 설명하시오.
   해설: 디지털 서명은 공개키 암호화를 기반으로 한 기술로, 발신자의 개인키로 메시지의 해시 값을 암호화하여 생성됩니다. 수신자는 발신자의 공개키로 서명을 복호화하여 메시지의 무결성을 검증하며, 서명이 올바르게 복호화되면 발신자의 인증도 동시에 확인됩니다.

6. **대칭키와 비대칭키**
   문제: 대칭키와 비대칭키 암호화의 주요 차이점과 각각의 장단점에 대해 설명하시오.
   해설: 대칭키 암호화는 동일한 키로 암호화와 복호화를 수행하는 방식이며, 처리 속도가 빠르다는 장점이 있지만 키 배포 문제가 있습니다. 비대칭키 암호화는 공개키와 개인키 두 개의 키를 사용하며, 키 배포 문제는 해결되었지만 대칭키에 비해 처리 속도가 느립니다.

7. **인증 프로토콜**
   문제: 인증 프로토콜 중 하나인 Kerberos의 기본 원리와 그것이 제공하는 보안 서비스에 대해 설명하시오.
   해설: Kerberos는 대칭키 기반의 인증 프로토콜로, 중앙 인증 서버를 통해 사용자와 서비스 서버 간의 인증을 제공합니다. 사용자는 인증 서버에 로그인 요청을 하고, 성공 시 티켓을 받아 서비스 서버에 접근합니다. Kerberos는 데이터의 기밀성, 무결성 및 인증을 보장합니다.

8. **방화벽**
   문제: 방화벽의 기본적인 역할과 패킷 필터링 방식, 프록시 방식의 방화벽의 차이점에 대해 설명하시오.
   해설: 방화벽은 내부 네트워크와 외부 네트워크 간의 통신을 제어하여 보안을 유지하는 역할을 합니다. 패킷 필터링 방식은 패킷의 헤더 정보를 기반으로 통신을 허용하거나 차단하는 반면, 프록시 방식은 요청을 대신 전송하며 내용을 검사하여 통신을 제어합니다.

9. **악성 코드**
   문제: 악성 코드의 정의와 대표적인 예시 3가지, 그리고 이를 방어하기 위한 기본적인 방법에 대해 설명하시오.
   해설: 악성 코드는 사용자의 동의 없이 비정상적인 동작을 수행하는 프로그램을 의미합니다. 대표적으로 바이러스, 웜, 트로이 목마 등이 있습니다. 악성 코드 방어 방법으로는 정기적인 백신 업데이트, 첨부 파일이나 링크의 신중한 열람, OS 및 소프트웨어의 패치 관리가 있습니다.

10. **피싱 공격**
    문제: 피싱 공격의 정의와 그것을 수행하는 주요 방법, 그리고 사용자가 피싱 공격을 예방하기 위한 조치에 대해 설명하시오.
    해설: 피싱 공격은 가짜 웹사이트나 이메일을 통해 사용자의 개인 정보를 획득하는 공격 방식입니다. 주로 이메일이나 메시지를 통해 사용자를 속여 가짜 사이트로 유도합니다. 사용자는 URL 주소를 항상 확인하고, 의심스러운 이메일이나 메시지에는 클릭하지 않는 등의 조치를 통해 피싱 공격을 예방할 수 있습니다.

11. **인트루전 디텍션 시스템(IDS)**
    문제: 인트루전 디텍션 시스템(IDS)의 정의와 그것의 주요 기능, 그리고 네트워크 기반 IDS와 호스트 기반 IDS의 차이점에 대해 설명하시오.
    해설: IDS는 네트워크나 시스템에 대한 무단 접근이나 공격을 탐지하는 시스템입니다. 주요 기능은 무단 접근 탐지, 로그 기록, 경보 발생 등이 있습니다. 네트워크 기반 IDS는 네트워크 트래픽을 모니터링하여 공격을 탐지하는 반면, 호스트 기반 IDS는 특정 호스트의 로그나 시스템 활동을 모니터링하여 공격을 탐지합니다.

12. **DDoS 공격**
    문제: DDoS 공격의 정의와 이러한 공격의 주요 특징, 그리고 DDoS 공격을 방어하기

위한 기본적인 방법에 대해 설명하시오.
해설: DDoS 공격은 여러 대의 컴퓨터를 이용하여 특정 서버나 네트워크에 대량의 트래픽을 발생시켜 서비스를 마비시키는 공격입니다. 주요 특징은 대량의 트래픽 발생, 여러 지점에서 동시에 공격 등이 있습니다. DDoS 공격 방어 방법으로는 트래픽 필터링, 대역폭 확장, 공격 트래픽 차단 등이 있습니다.

13. **VPN**
문제: VPN의 정의와 그것을 사용하는 주요 목적, 그리고 VPN의 작동 원리에 대해 설명하시오.
해설: VPN은 Virtual Private Network의 약자로, 공용 네트워크를 통해 가상의 사설 네트워크 연결을 제공하는 기술입니다. 주요 목적은 원격 접속 보안, 데이터 암호화, 지역 제한 우회 등이 있습니다. VPN은 암호화된 터널을 통해 데이터를 전송하여 네트워크 통신의 보안을 강화합니다.

14. **물리적 보안**
문제: 정보보호의 관점에서 물리적 보안의 중요성과 주요 물리적 보안 조치에 대해 설명하시오.
해설: 물리적 보안은 정보 자산이 저장된 물리적 공간을 보호하는 것을 의미하며, 해커의 무단 접근, 자연재해 등으로부터 정보 자산을 보호하는데 중요합니다. 주요 물리적 보안 조치로는 보안 경비, CCTV 설치, 출입 통제 시스템, 방화 및 방수 조치 등이 있습니다.

15. **사회공학 공격**
문제: 사회공학 공격의 정의와 대표적인 예시 3가지, 그리고 이러한 공격을 예방하기 위한 조치에 대해 설명하시오.
해설: 사회공학 공격은 사람의 심리나 행동을 이용하여 정보를 획득하는 공격 방식입니다. 대표적으로 가짜 전화, 피싱 이메일, 가짜 직원 신분 등이 있습니다. 공격 예방 조치로는 개인 정보 보호 교육, 의심스러운 요청에 대한 확인, 정보 접근 권한 제한 등이 있습니다.

16. **데이터 유출 방지(DLP)**
문제: 데이터 유출 방지(DLP) 시스템의 주요 목적과 그것이 기업에 어떠한 가치를 제공하는지, 그리고 DLP의 기본적인 작동 원리에 대해 설명하시오.
해설: DLP는 기업의 중요 데이터가 외부로 누출되는 것을 방지하는 시스템입니다. 이는 기업의 지적 재산권 보호, 비즈니스 비밀 유지, 규제 준수 등의 가치를 제공합니다. DLP는 데이터의 패턴, 키워드, 지문 등을 기반으로 민감한 데이터의 이동을 감지하고 제어합니다.

17. **암호화 알고리즘**
문제: 대표적인 암호화 알고리즘인 AES와 RSA의 주요 차이점과 각각의 알고리즘이 사용되는 주요한 상황에 대해 설명하시오.
해설: AES는 대칭키 암호화 알고리즘으로, 빠른 처리 속도를 가지며 주로 데이터의 암

호화에 사용됩니다. RSA는 비대칭키 암호화 알고리즘으로, 공개키와 개인키를 사용하며 주로 디지털 서명이나 키 교환에 사용됩니다.

18. **보안 인증서**
    문제: 보안 인증서의 역할과 그것을 발급하는 기관의 이름, 그리고 인증서의 주요 구성 요소에 대해 설명하시오.
    해설: 보안 인증서는 웹사이트의 신원을 확인하고 통신의 암호화를 보장하는 역할을 합니다. 이를 발급하는 기관을 CA(Certificate Authority)라고 합니다. 인증서의 주요 구성 요소로는 발급자, 수신자, 유효 기간, 공개키 정보 등이 포함됩니다.

19. **백도어**
    문제: 백도어의 정의와 그것이 시스템에 어떠한 위험성을 가지는지, 그리고 백도어를 방지하기 위한 주요한 조치에 대해 설명하시오.
    해설: 백도어는 시스템에 숨겨진 접근 경로를 의미하며, 이를 통해 공격자가 시스템에 무단으로 접근할 수 있습니다. 이는 데이터 유출, 시스템 파괴 등의 위험성을 가집니다. 백도어 방지 조치로는 정기적인 시스템 검사, 보안 패치 적용, 불필요한 서비스의 중단 등이 있습니다.

20. **휴대폰 보안**
    문제: 스마트폰의 보안 위협 요소 중 대표적인 것 3가지와 이를 방어하기 위한 기본적인 조치에 대해 설명하시오.
    해설: 스마트폰의 보안 위협 요소로는 악성 앱 설치, 무선 네트워크 공격, 물리적 접근 등이 있습니다. 방어 조치로는 앱의 정기적인 업데이트, 알려지지 않은 출처의 앱 설치 제한, 스마트폰 잠금 설정 등이 있습니다.

21. **보안 정책**
    문제: 기업의 보안 정책의 중요성과 그것을 수립할 때 고려해야 할 주요한 요소 3가지에 대해 설명하시오.
    해설: 보안 정책은 기업의 정보 자산을 보호하기 위한 기본 원칙과 지침을 제시합니다. 수립 시 고려해야 할 요소로는 기업의 비즈니스 목표, 현재의 보안 위협, 사용하는 기술 및 자원 등이 있습니다.

22. **멀티 팩터 인증**
    문제: 멀티 팩터 인증의 정의와 그것이 제공하는 보안의 이점, 그리고 대표적인 멀티 팩터 인증 방법 3가지에 대해 설명하시오.
    해설: 멀티 팩터 인증은 두 개 이상의 인증 방법을 조합하여 사용자의 신원을 확인하는 방식입니다. 이로 인해 단일 인증 방식보다 높은 보안성을 제공합니다. 대표적인 방법으로는 비밀번호 입력, 스마트카드 사용, 생체 인식 등이 있습니다.

23. **가상화 보안**
    문제: 가상화 기술에서의 보안 위협 요소 중 대표적인 것 3가지와 이를 방어하기 위한 기본적인 조치에 대해 설명하시오.

해설: 가상화 기술의 보안 위협 요소로는 하이퍼바이저 취약점, 가상 머신 간의 공격, 가상 네트워크 공격 등이 있습니다. 방어 조치로는 하이퍼바이저의 정기적인 업데이트, 가상 머신 간의 격리, 가상 네트워크의 보안 설정 최적화 등이 있습니다.

24. **IoT 보안**
    문제: IoT(Internet of Things)에서의 주요 보안 위협 요소와 이러한 위협에 대응하기 위한 기본적인 보안 조치에 대해 설명하시오.
    해설: IoT의 보안 위협 요소로는 물리적 접근, 기기의 취약점 공격, 네트워크 공격 등이 있습니다. 대응 조치로는 기기의 펌웨어 업데이트, 네트워크 트래픽 모니터링, 기기에 대한 접근 제어 설정 등이 있습니다.

25. **클라우드 보안**
    문제: 클라우드 서비스에서의 보안 위협 요소 중 대표적인 것 3가지와 클라우드 보안을 강화하기 위한 주요한 방법에 대해 설명하시오.
    해설: 클라우드 서비스의 보안 위협 요소로는 데이터 유출, 계정 무단 접근, 서비스 거부 공격(DDoS) 등이 있습니다. 보안 강화 방법으로는 데이터 암호화, 멀티 팩터 인증 적용, 정기적인 보안 검사 및 모니터링 등이 있습니다.

26. **보안 인식 교육**
    문제: 보안 인식 교육의 중요성과 그것을 통해 기대할 수 있는 주요한 효과 3가지에 대해 설명하시오.
    해설: 보안 인식 교육은 사용자들에게 보안 위협에 대한 인식을 높이는 활동입니다. 이를 통해 사회공학 공격에 대한 저항력 향상, 보안 정책 준수율 증가, 보안 사고 발생 위험 감소 등의 효과를 기대할 수 있습니다.

27. **비밀번호 정책**
    문제: 효과적인 비밀번호 정책의 중요성과 그것을 수립할 때 고려해야 할 주요한 요소 3가지에 대해 설명하시오.
    해설: 효과적인 비밀번호 정책은 시스템과 데이터의 보안을 강화하는 데 중요합니다. 수립 시 고려해야 할 요소로는 최소 문자 수, 복잡성 요구 사항(대문자, 숫자, 특수 문자 포함), 정기적인 변경 주기 등이 있습니다.

28. **무선 네트워크 보안**
    문제: 무선 네트워크에서의 주요 보안 위협 요소와 이러한 위협에 대응하기 위한 기본적인 보안 조치에 대해 설명하시오.
    해설: 무선 네트워크의 보안 위협 요소로는 무단 접근, 중간자 공격, 패킷 스니핑 등이 있습니다. 대응 조치로는 WPA3와 같은 강력한 암호화 표준 사용, SSID 숨김, MAC 주소 필터링 등이 있습니다.

29. **보안 프레임워크**
    문제: 보안 프레임워크의 정의와 그것을 도입하는 기업에게 제공하는 주요한 가치에 대해 설명하시오.

해설: 보안 프레임워크는 정보 보안 관리와 관련된 정책, 지침, 표준, 절차의 체계적인 구조입니다. 이를 도입함으로써 기업은 보안 위협에 대한 효과적인 대응, 규제 준수, 보안 리스크 관리의 효율화 등의 가치를 얻을 수 있습니다.

30. **보안 로그 관리**
    문제: 보안 로그 관리의 중요성과 로그를 효과적으로 관리하기 위한 주요한 방법 3가지에 대해 설명하시오.
    해설: 보안 로그 관리는 보안 사고의 탐지, 분석, 대응에 필수적입니다. 효과적인 로그 관리 방법으로는 로그의 중앙 집중화, 정기적인 로그 검토, 로그의 보관 및 백업 등이 있습니다.

31. **보안 표준 및 규제**
    문제: 정보 보안 표준 및 규제의 중요성과 그것이 기업에게 제공하는 주요한 가치에 대해 설명하시오.
    해설: 정보 보안 표준 및 규제는 정보 보안의 최소한의 기준을 제시하며, 이를 준수함으로써 기업은 보안 위협으로부터의 보호, 고객의 신뢰 향상, 법적 책임 회피 등의 가치를 얻을 수 있습니다.

32. **보안 평가 및 테스트**
    문제: 시스템의 보안 평가 및 테스트의 중요성과 이를 수행하기 위한 주요한 방법 2가지에 대해 설명하시오.
    해설: 보안 평가 및 테스트는 시스템의 취약점을 발견하고 대응하는 데 중요합니다. 주요한 방법으로는 침투 테스트와 취약점 평가가 있습니다.

33. **보안 인증 및 인가**
    문제: 정보 보안에서 인증(Authentication)과 인가(Authorization)의 차이점과 각각의 중요성에 대해 설명하시오.
    해설: 인증은 사용자의 신원을 확인하는 과정을 의미하며, 인가는 해당 사용자에게 특정 자원에 대한 접근 권한을 부여하는 과정을 의미합니다. 인증은 시스템에 올바른 사용자만이 접근하도록 보장하며, 인가는 사용자가 접근할 수 있는 자원의 범위를 제한하여 보안을 강화합니다.

34. **보안 위험 관리**
    문제: 보안 위험 관리의 중요성과 위험 관리 과정에서 고려해야 할 주요한 요소 3가지에 대해 설명하시오.
    해설: 보안 위험 관리는 잠재적인 보안 위협을 식별, 평가, 대응하는 과정입니다. 이를 통해 기업은 보안 사고의 발생 확률과 영향을 최소화할 수 있습니다. 고려해야 할 주요 요소로는 위험 평가, 위험 우선 순위 설정, 대응 전략 수립 등이 있습니다.

35. **보안 인사이드트 위협**
    문제: 보안 인사이드트(내부자) 위협의 정의와 이러한 위협에 대응하기 위한 기본적인 조치에 대해 설명하시오.

해설: 인사이드트 위협은 조직 내부의 사람들로부터 발생하는 보안 위협을 의미합니다. 이를 대응하기 위한 조치로는 직원 교육, 데이터 접근 권한 제한, 사용자 활동 모니터링, 정기적인 보안 감사 등이 있습니다.

36. **모바일 디바이스 관리(MDM)**
    문제: 모바일 디바이스 관리(MDM)의 정의와 그것이 기업에게 제공하는 주요한 가치에 대해 설명하시오.
    해설: MDM은 기업 내에서 사용되는 모바일 디바이스의 설정, 관리, 보안을 중앙에서 통합적으로 관리하는 솔루션을 의미합니다. 이를 통해 기업은 모바일 디바이스의 보안 위협을 최소화하고, 디바이스 사용 정책을 효과적으로 적용할 수 있습니다.

37. **보안 인프라 구축**
    문제: 효과적인 보안 인프라 구축의 중요성과 구축 시 고려해야 할 주요한 요소 3가지에 대해 설명하시오.
    해설: 효과적인 보안 인프라는 기업의 정보 자산을 보호하고, 보안 위협에 대응하는 데 필수적입니다. 구축 시 고려해야 할 주요 요소로는 현재의 보안 위협 분석, 기업의 비즈니스 요구 사항, 보안 솔루션의 확장성 및 유연성 등이 있습니다.

38. **사이버 보안 인력 양성**
    문제: 사이버 보안 인력 양성의 중요성과 그것을 위해 기업이나 교육 기관에서 취해야 할 주요한 조치에 대해 설명하시오.
    해설: 사이버 보안 인력은 다양한 사이버 위협에 대응하고, 기업의 정보 자산을 보호하는 데 중요한 역할을 합니다. 인력 양성을 위해 기업이나 교육 기관에서는 전문 교육 프로그램 운영, 실무 경험 제공, 연구 및 개발 지원 등의 조치를 취해야 합니다.

39. **피싱 공격**
    문제: 피싱 공격의 정의와 이러한 공격의 주요 특징, 그리고 피싱 공격을 방어하기 위한 기본적인 방법에 대해 설명하시오.
    해설: 피싱 공격은 가짜 웹사이트나 이메일을 통해 사용자의 개인 정보나 자격증명 정보를 획득하는 공격 방식입니다. 주요 특징은 실제와 유사한 가짜 페이지 제작, 긴급성을 강조하는 메시지 등이 있습니다. 방어 방법으로는 이메일의 발신자와 URL을 항상 확인, 의심스러운 이메일은 열지 않기, 개인 정보 제공을 요구하는 이메일에 대해 신중하게 대응하기 등이 있습니다.

40. **보안 프로토콜**
    문제: SSL/TLS 프로토콜의 주요 기능과 그것이 웹 통신에서 어떠한 보안성을 제공하는지에 대해 설명하시오.
    해설: SSL/TLS 프로토콜은 웹 통신의 보안을 강화하기 위한 프로토콜입니다. 주요 기능은 데이터 암호화, 통신 당사자 간의 신원 인증, 데이터 무결성 보장 등이 있습니다. 이를 통해 중간자 공격, 데이터 변조, 무단 접근 등의 보안 위협으로부터 웹 통신을 보호합니다.