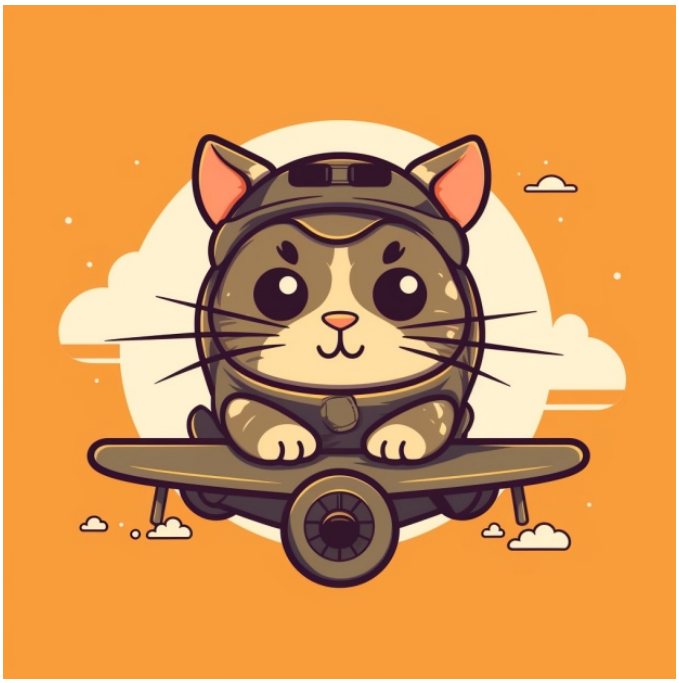
🥷

[취업폭격기 Zeromini 위클리 개념폭격 #15]

📕 과목 : 시스템네트워크보안

🔥 참고문제 : 2023년 경찰 경력채용 문제

🌝 문제 수정 버전 : V 1.0



1. **라우팅 (Routing)과 TTL (Time To Live)**
   문제: 라우팅 과정에서 TTL이 감소하는 원리와 그 목적에 대해 설명해주세요.
   해설: 라우팅 과정에서 패킷이 라우터를 거칠 때마다 TTL 값이 1씩 감소합니다. TTL이 0이 되면 해당 패킷은 폐기되어 무한 루프를 방지하며, 이는 네트워크 자원의 낭비를 방지하는데 중요한 역할을 합니다.
2. **패스워드 크래킹 도구**
   문제: 패스워드 크래킹에 사용되는 도구들 중 하나를 선택하고 그 도구의 작동 원리와 사용 방법에 대해 설명해주세요.

해설: 예를 들어, John the Ripper는 다양한 암호 해시 알고리즘을 지원하는 패스워드 크래킹 도구입니다. 먼저, 암호화된 패스워드의 해시를 획득한 후, 사전 공격이나 무작위 공격 등의 방법으로 가능한 모든 패스워드 후보를 해시화하고, 이를 원본 해시와 비교하여 일치하는 값을 찾습니다.

3. **방화벽 (Firewall)의 구축 형태**
   문제: 방화벽의 여러 구축 형태 중 하나를 선택하고 그 형태의 장단점에 대해 설명해주세요.
   해설: 예를 들어, 스크린드 서브넷 게이트웨이는 내부 네트워크와 외부 네트워크 사이에 DMZ라는 격리된 네트워크를 구성하여, 공격자가 내부 네트워크에 직접 접근하는 것을 방지합니다. 이 구조는 보안을 강화할 수 있지만, 구축과 관리가 복잡하고 비용이 더 들 수 있습니다.

4. **신뢰 플랫폼 모듈 (TPM)**
   문제: 신뢰 플랫폼 모듈 (TPM)이 무엇인지와 그 기능에 대해 설명해주세요.
   해설: TPM은 컴퓨터의 메인보드에 장착되는 마이크로칩으로, 시스템의 보안을 강화하는데 사용됩니다. TPM은 안전하게 키를 생성하고 저장할 수 있는 환경을 제공하며, 하드웨어 기반의 보안 기능을 지원하여 시스템의 무결성을 보호하고, 안전한 부팅 과정을 지원합니다.

5. **라우터와 HLEN (Header Length)**
   문제: 라우팅 과정에서 HLEN이 무엇을 나타내는지 설명해주세요.
   해설: HLEN은 IP 헤더의 길이를 나타내며, IP 패킷의 헤더 부분에서 찾을 수 있습니다. 이 값은 IP 헤더의 전체 길이를 나타내며, 라우터는 이 값을 사용하여 헤더와 데이터 부분을 구분합니다.

6. **IPv6의 기본 헤더 길이**
   문제: IPv6의 기본 헤더 길이는 얼마인지 설명해주세요.
   해설: IPv6의 기본 헤더 길이는 40 바이트입니다. 이 헤더에는 여러 가지 필드가 포함되어 있으며, 이를 통해 패킷의 소스, 목적지, 트래픽 클래스 등의 정보를 전달합니다.

7. **패스워드 크래킹 도구 - RainbowCrack**
   문제: RainbowCrack 도구의 특징과 작동 원리에 대해 설명해주세요.
   해설: RainbowCrack은 미리 계산된 해시 값을 사용하여 패스워드를 빠르게 크래킹하는 도구입니다. 레인보우 테이블이라는 대규모 데이터를 사용하여 해시 함수의 출력을 빠르게 찾아내어, 시간 대비 효율적인 패스워드 크래킹을 가능하게 합니다.

8. **방화벽의 스크린드 서브넷 게이트웨이 구조**
   문제: 스크린드 서브넷 게이트웨이 구조의 방화벽은 어떤 특징을 가지고 있는지 설명해주세요.
   해설: 스크린드 서브넷 게이트웨이 구조는 DMZ라는 격리된 네트워크 영역을 형성하여 내부 네트워크를 외부로부터 보호합니다. 이 구조는 공격자가 내부 네트워크에 직접 접

근하는 것을 방지하며, 고도의 보안을 제공하지만 구축과 관리가 복잡하고 비용이 더 들 수 있습니다.

9. **레이스 컨디션 (Race Condition) 공격**
   문제: 레이스 컨디션 공격이 무엇인지와 이를 방지하기 위한 대응 방법에 대해 설명해주세요.
   해설: 레이스 컨디션 공격은 시스템의 자원에 대해 동시에 접근하려는 여러 프로세스나 스레드가 경쟁 상태에 놓이는 상황을 이용한 공격입니다. 이를 방지하기 위해서는 임시 파일 생성을 피하고, 비정상적인 링크를 검사하여 제거하는 등의 조치를 취해야 합니다.

10. **신뢰 플랫폼 모듈 (TPM)의 기능**
    문제: TPM이 시스템 부팅 과정에서 어떤 역할을 하는지 설명해주세요.
    해설: TPM은 시스템 부팅 과정에서 단계적으로 인증된 절차를 거쳐 부팅을 진행하게 합니다. 이를 통해 시스템이 안전한 상태에서 시작되도록 보장하며, 부팅 과정에서 발생할 수 있는 보안 위협을 최소화합니다.

11. **스푸핑 (Spoofing) 공격 - IP 스푸핑**
    문제: IP 스푸핑 공격이 무엇인지와 이 공격의 목적에 대해 설명해주세요.
    해설: IP 스푸핑 공격은 공격자가 다른 컴퓨터의 IP 주소를 사용하여 정보를 얻거나 접근하는 공격입니다. 이 공격의 목적은 보안 시스템을 우회하여 민감한 정보에 접근하거나, DDoS 공격의 일환으로 사용하는 것 등이 있습니다.

12. **UNIX 시스템의 로그 파일 - /etc/shadow**
    문제: UNIX 시스템의 /etc/shadow 파일에 대해 설명하고, 이 파일에서 사용자 패스워드의 해시 알고리즘을 어떻게 확인할 수 있는지 설명해주세요.
    해설: /etc/shadow 파일은 UNIX 시스템에서 사용자의 패스워드 정보를 암호화하여 저장하는 파일입니다. 이 파일에서 패스워드 해시 알고리즘은 패스워드 필드의 처음 부분에서 확인할 수 있으며, 예를 들어 "5"로 시작하는 경우 SHA-256 알고리즘을 사용한 것입니다.

13. **무선 LAN 프로토콜 - IEEE 802.11ac**
    문제: IEEE 802.11ac 프로토콜의 특징과 이 프로토콜이 지원하는 최대 전송 속도에 대해 설명해주세요.
    해설: IEEE 802.11ac는 Wi-Fi 5로도 불리며, 최대 6.9 Gbps의 데이터 전송 속도를 지원합니다. 이 프로토콜은 5 GHz 주파수 대역에서 높은 대역폭과 MIMO 기술을 사용하여 높은 데이터 전송 속도를 제공합니다.

14. **암호화 알고리즘 - AES**
    문제: AES 암호화 알고리즘이 무엇인지와 그 특징에 대해 설명해주세요.
    해설: AES는 Advanced Encryption Standard의 약자로, 블록 암호화 방식을 사용하는 대칭키 암호화 알고리즘입니다. 128, 192, 256비트의 키 길이를 지원하며, 높은 보안성과 빠른 처리 속도를 제공합니다.

15. **SQL 인젝션 공격**
    문제: SQL 인젝션 공격이 무엇인지와 이를 방지하기 위한 방법에 대해 설명해주세요.
    해설: SQL 인젝션 공격은 악의적인 SQL 쿼리를 웹 애플리케이션의 입력 필드에 삽입하여 데이터베이스를 조작하는 공격입니다. 이를 방지하기 위해서는 입력 검증, 파라미터화된 쿼리 사용, 최소 권한 원칙 적용 등의 방법을 사용해야 합니다.

16. **피싱 (Phishing) 공격**
    문제: 피싱 공격이 무엇인지와 이 공격의 주요 목적에 대해 설명해주세요.
    해설: 피싱 공격은 사기성 이메일이나 웹사이트를 통해 사용자의 개인 정보나 금융 정보를 획득하는 공격입니다. 이 공격의 주요 목적은 민감한 정보를 획득하여 금전적 이익을 얻거나, 추가적인 공격을 수행하는 것입니다.

17. **랜섬웨어 (Ransomware)**
    문제: 랜섬웨어가 무엇인지와 이러한 공격을 방지하기 위한 방법에 대해 설명해주세요.
    해설: 랜섬웨어는 악성 소프트웨어의 한 형태로, 사용자의 시스템이나 파일을 암호화하여 사용할 수 없게 만든 후, 복구를 위한 몸값을 요구하는 공격입니다. 정기적인 백업, 안전한 웹 브라우징 습관 유지, 알려진 보안 취약점을 해결하는 패치 관리 등을 통해 방지할 수 있습니다.

18. **브루트 포스 (Brute Force) 공격**
    문제: 브루트 포스 공격이 무엇인지와 이를 방지하기 위한 대응 방법에 대해 설명해주세요.
    해설: 브루트 포스 공격은 가능한 모든 조합을 시도하여 비밀번호를 찾아내는 공격 방법입니다. 이를 방지하기 위해서는 복잡한 비밀번호 사용, 2단계 인증 도입, 로그인 시도 횟수 제한 등의 방법을 사용할 수 있습니다.

19. **디지털 서명 (Digital Signature)**
    문제: 디지털 서명이 무엇인지와 그 기능에 대해 설명해주세요.
    해설: 디지털 서명은 전자 문서나 메시지의 진위를 검증하기 위한 암호화 기술입니다. 이 기술은 메시지의 해시를 생성하고, 그 해시를 개인 키로 암호화하여 서명을 생성합니다. 수신자는 공개 키를 사용하여 해시를 복호화하고, 메시지의 무결성과 발신자의 인증을 검증할 수 있습니다.

20. **무선 네트워크 보안 - WPA3**
    문제: WPA3 보안 프로토콜의 특징과 그로 인한 보안 강화 방법에 대해 설명해주세요.
    해설: WPA3는 Wi-Fi Protected Access 3의 약자로, 더 강화된 보안 기능을 제공하는 무선 네트워크 보안 프로토콜입니다. 이 프로토콜은 192비트 보안 암호화를 지원하며, 브루트 포스 공격에 대한 보호와 개선된 공개 네트워크 보안을 제공합니다.

21. **빅 데이터와 보안**
    문제: 빅 데이터 환경에서의 보안 취약점과 이를 해결하기 위한 방법에 대해 설명해주세요.

해설: 빅 데이터 환경은 대량의 데이터를 처리하고 저장하는데, 이로 인해 데이터 유출, 무단 접근 등의 보안 취약점이 발생할 수 있습니다. 이를 해결하기 위해 데이터 암호화, 접근 제어, 안전한 데이터 전송 방법의 도입 등이 필요합니다.

22. **클라우드 컴퓨팅과 멀티 테넌시**
    문제: 클라우드 컴퓨팅 환경에서 멀티 테넌시가 무엇인지와 이로 인한 보안 이슈에 대해 설명해주세요.
    해설: 멀티 테넌시는 여러 사용자나 그룹이 같은 클라우드 리소스를 공유하는 환경을 말합니다. 이로 인해 데이터 유출, 무단 접근 등의 보안 이슈가 발생할 수 있으며, 이를 방지하기 위해 강력한 접근 제어와 데이터 분리 기술이 필요합니다.

23. **인증과 인가**
    문제: 인증과 인가의 차이점을 설명해주세요.
    해설: 인증(Authentication)은 사용자의 신원을 확인하는 과정이며, 인가(Authorization)는 인증된 사용자에게 특정 자원에 대한 접근 권한을 부여하는 과정입니다. 인증은 로그인 과정에서 이루어지며, 인가는 사용자가 특정 서비스나 데이터에 접근할 때 이루어집니다.

24. **보안 인증서**
    문제: 보안 인증서가 무엇인지와 그 역할에 대해 설명해주세요.
    해설: 보안 인증서는 웹사이트의 신원을 확인하고 안전한 연결을 제공하는데 사용되는 디지털 문서입니다. 이를 통해 사용자는 웹사이트가 신뢰할 수 있는 곳임을 알 수 있으며, 데이터가 암호화되어 안전하게 전송된다는 것을 보장받을 수 있습니다.

25. **루트킷(Rootkit)**
    문제: 루트킷이 무엇인지와 그로 인한 위험성에 대해 설명해주세요.
    해설: 루트킷은 시스템의 핵심 부분에 숨어 시스템을 제어하거나 모니터링하는 소프트웨어 도구입니다. 루트킷은 일반적으로 악성 목적으로 사용되며, 시스템의 보안을 심각하게 손상시킬 수 있습니다. 루트킷으로 인한 위험성은 데이터 유출, 시스템 손상 등이 있습니다.

26. **보안 정책(Security Policy)**
    문제: 보안 정책이 무엇인지와 그 중요성에 대해 설명해주세요.
    해설: 보안 정책은 조직이 정보 자산을 보호하기 위해 설정한 규칙과 절차의 집합입니다. 보안 정책은 조직의 보안 수준을 높이며, 데이터 유출이나 무단 접근과 같은 보안 위협으로부터 보호하기 위한 기준을 제시합니다.

27. **보안 인지 교육(Security Awareness Training)**
    문제: 보안 인지 교육의 목적과 중요성에 대해 설명해주세요.
    해설: 보안 인지 교육은 조직의 직원들에게 보안 위협을 인식하게 하고, 안전한 컴퓨팅 습관을 형성하게 하는 교육입니다. 이 교육은 직원들이 보안 위협을 피할 수 있는 방법을 배우게 하여, 조직의 보안 수준을 향상시키는데 중요합니다.

28. **사회 공학(Social Engineering)**
    문제: 사회 공학 공격이 무엇인지와 이러한 공격을 방지하기 위한 방법에 대해 설명해주세요.
    해설: 사회 공학 공격은 사람들의 심리를 이용하여 민감한 정보를 획득하는 공격 방법입니다. 이를 방지하기 위해서는 직원들에게 보안 교육을 제공하고, 민감한 정보를 공유하지 않도록 권장하는 등의 방법이 있습니다.

29. **보안 프로토콜 - HTTPS**
    문제: HTTPS 프로토콜이 무엇인지와 그 특징에 대해 설명해주세요.
    해설: HTTPS는 HTTP 프로토콜에 SSL/TLS 프로토콜을 추가하여 통신을 암호화하는 프로토콜입니다. 이 프로토콜은 데이터의 기밀성을 보장하며, 중간자 공격(Man-in-the-Middle Attack)을 방지하는데 효과적입니다.

30. **보안 취약점 평가 도구 - Nessus**
    문제: Nessus 도구가 무엇인지와 그 기능에 대해 설명해주세요.
    해설: Nessus는 네트워크를 스캔하여 보안 취약점을 찾아내는 도구입니다. 이 도구는 알려진 보안 취약점 데이터베이스를 기반으로 시스템을 분석하며, 발견된 취약점에 대한 보고서를 생성합니다.

31. **보안 테스트 - 펜 테스트 (Penetration Testing)**
    문제: 펜 테스트가 무엇인지와 이러한 테스트의 목적에 대해 설명해주세요.
    해설: 펜 테스트는 조직의 시스템이나 네트워크에 대해 의도적으로 공격을 시도하여 보안 취약점을 찾아내는 테스트입니다. 이 테스트의 목적은 보안 취약점을 식별하고, 이러한 취약점이 실제로 어떤 위험을 초래할 수 있는지 평가하는 것입니다.

32. **물리적 보안**
    문제: 물리적 보안이 무엇인지와 그 중요성에 대해 설명해주세요.
    해설: 물리적 보안은 건물, 서버실 등 물리적 자산을 보호하기 위한 보안 조치를 의미합니다. 이러한 보안은 무단 접근, 도난, 화재 등의 위험으로부터 조직의 물리적 자산을 보호하는데 중요합니다.

33. **보안 인증 기준 - ISO 27001**
    문제: ISO 27001 인증이 무엇인지와 그 특징에 대해 설명해주세요.
    해설: ISO 27001은 정보 보안 관리 시스템(ISMS)에 대한 국제 표준입니다. 이 인증은 조직이 정보 보안 관리에 관한 국제 표준을 준수하고 있음을 보증하며, 데이터 보호와 정보 보안을 강화하는데 중요한 역할을 합니다.

34. **보안 위협 - 제로 데이 공격 (Zero-Day Attack)**
    문제: 제로 데이 공격이 무엇인지와 이러한 공격을 방지하기 위한 방법에 대해 설명해주세요.
    해설: 제로 데이 공격은 보안 취약점이 공개되기 전에 이루어지는 공격입니다. 이를 방

지하기 위해서는 정기적인 시스템 업데이트와 패치 관리, 안전한 프로그래밍 기법의 적용 등이 필요합니다.

35. **보안 프레임워크 - NIST Cybersecurity Framework**
    문제: NIST Cybersecurity Framework가 무엇인지와 그 목적에 대해 설명해주세요.
    해설: NIST Cybersecurity Framework는 미국 국립 표준 기술 연구소(NIST)에서 개발한 사이버 보안 프레임워크로, 조직이 사이버 위협에 대응하기 위한 기준을 제시합니다. 이 프레임워크의 목적은 조직의 사이버 보안 수준을 향상시키고 위협에 대응하는 능력을 개선하는 것입니다.

36. **보안 이벤트 관리 - SIEM**
    문제: SIEM(Security Information and Event Management) 시스템이 무엇인지와 그 기능에 대해 설명해주세요.
    해설: SIEM 시스템은 보안 정보 및 이벤트 관리를 담당하는 솔루션으로, 보안 로그 및 이벤트 데이터를 수집, 정규화, 분석하여 보안 위협을 식별하고 대응합니다. 이 시스템은 조직의 보안 상태를 모니터링하고, 위협에 빠르게 대응하기 위한 통합된 뷰를 제공합니다.

37. **보안 컴플라이언스**
    문제: 보안 컴플라이언스가 무엇인지와 그 중요성에 대해 설명해주세요.
    해설: 보안 컴플라이언스는 조직이 법률, 규정, 정책 등에 따라 정보 보안 요구 사항을 충족시키는 것을 의미합니다. 이는 조직이 법적 책임을 이행하고, 고객의 신뢰를 얻으며, 데이터 보호를 강화하는데 중요합니다.

38. **보안 위협 인텔리전스**
    문제: 보안 위협 인텔리전스가 무엇인지와 그 역할에 대해 설명해주세요.
    해설: 보안 위협 인텔리전스는 현재와 미래의 보안 위협에 대한 정보를 수집, 분석하는 프로세스입니다. 이를 통해 조직은 보안 위협을 미리 인지하고, 적절한 대응 전략을 수립하여 보안 사고를 예방하거나 미연에 방지할 수 있습니다.

39. **보안 평가 도구 - OWASP ZAP**
    문제: OWASP ZAP 도구가 무엇인지와 그 주요 기능에 대해 설명해주세요.
    해설: OWASP ZAP(Zed Attack Proxy)은 웹 애플리케이션의 보안 취약점을 찾기 위한 오픈 소스 보안 테스트 도구입니다. 이 도구는 자동 스캐너와 다양한 테스트 도구를 제공하여, 개발자와 테스터가 웹 애플리케이션의 보안 취약점을 찾고 해결할 수 있게 돕습니다.

40. **보안 개념 - 디지털 포렌식**
    문제: 디지털 포렌식이 무엇인지와 그 중요성에 대해 설명해주세요.
    해설: 디지털 포렌식은 범죄 현장에서 디지털 증거를 수집, 분석하는 과학적 방법론입니다. 이 분야는 법적 문제 해결과 범죄 수사에서 중요한 역할을 하며, 정확하고 신뢰할 수 있는 증거 제시를 통해 법적 절차를 지원합니다.