🥷

[취업폭격기 Zeromini 위클리 개념 폭격 #23]

📕 과목 : 네트워크보안

🔥 참고문제 : 2022년 군무원 7급

🌝 문제 수정 버전 : V 1.0

1.Active Contents Attack
문제: 메일 서비스 공격 유형 중 하나인 Active Contents Attack은 무엇입니까?
해설: Active Contents Attack은 이메일을 통해 악성 스크립트나 콘텐츠를 전송하여 사용자의 컴퓨터를 감염시키는 공격 유형입니다. 이메일 클라이언트나 웹 브라우저의 HTML 취약점을 이용하여 사용자의 시스템에 무단으로 접근하거나 개인 정보를 탈취할 수 있습니다. 이러한 공격을 방지하기 위해서는 이메일의 출처를 확인하고, 신뢰할 수 없는 소스의 콘텐츠는 열지 않아야 합니다.

2.Trojan Horse Attack
문제: 사용자의 시스템에 심각한 피해를 줄 수 있는 Trojan Horse Attack은 무엇입니까?
해설: Trojan Horse Attack은 사용자가 정상적인 소프트웨어로 위장한 악성 프로그램을 실행시키게 함으로써 시스템에 백도어를 설치하거나 데이터를 손상시키는 공격입니다. 이 공격은 사용자의 동의 없이 시스템에 접근하여 민감한 정보를 도용하거나 추가적인 악성 소프트웨어를 설치할 수 있어 매우 위험합니다.

3.SendMail 버퍼 오버플로
문제: SendMail 서비스를 대상으로 하는 버퍼 오버플로 공격은 무엇입니까?
해설: SendMail 버퍼 오버플로 공격은 공격자가 SendMail의 버퍼 오버플로 취약점을 이용하여 임의의 코드를 실행시키는 기법입니다. 과도한 양의 데이터를 전송하여 시스템의 메모리를 침범하고, 이를 통해 시스템 제어권을 획득할 수 있습니다. 이러한 취약점을 방지하기 위해 정기적인 소프트웨어 업데이트와 취약점 패치가 필수적입니다.

4.Buffer Overflow Attack
문제: 시스템의 메모리를 침범하여 임의의 명령을 실행할 수 있게 하는 Buffer Overflow Attack은 무엇입니까?
해설: Buffer Overflow Attack은 공격자가 프로그램의 버퍼에 예상치 못한 방식으로 데이터를 삽입하여 메모리를 침범하고, 시스템의 제어를 넘겨받아 악의적인 명령을 실행하는 공격입니다. 이는 프로그램의 입력값 검증 미흡으로 발생하며, 시스템의 보안을 심각하게 위협합니다. 개발자는 소프트웨어를 설계할 때 버퍼 오버플로를 방지하는 코딩 기법을 적용해야 합니다.

5.네트워크 기반 IPS(NIPS)
문제: 네트워크 트래픽을 모니터링하고 유해 트래픽을 차단하는 네트워크 기반 IPS(NIPS)는 무엇입니까?
해설: 네트워크 기반 IPS(NIPS)는 네트워크의 데이터 흐름을 지속적으로 감시하며, 알려진 공격 패턴이나 이상 행위를 탐지하면 즉각적으로 차단하는 보안 시스템입니다. NIPS는 네트워크의 중요 지점에 설치되어 전체 네트워크를 보호하는 역할을 하며, 보안 정책에 따라 자동으로 대응할 수 있습니다.

6.호스트 기반 IPS(HIPS)
문제: 개별 호스트의 보안을 강화하기 위해 설치되는 호스트 기반 IPS(HIPS)는 무엇입니까?
해설: 호스트 기반 IPS(HIPS)는 개별 컴퓨터나 서버에 직접 설치되어 해당 시스템의 파일과 네트워크 트래픽을 모니터링합니다. HIPS는 시스템에 침입하려는 악성 행위를 실시간으로 탐지하고 차단하며, 시스템의 취약점을 보호하는 데 중요한 역할을 합니다.

7.스위치 기반 IPS
문제: 네트워크 스위치에 통합되어 트래픽을 분석하는 스위치 기반 IPS는 무엇입니까?
해설: 스위치 기반 IPS는 네트워크 스위치에 내장되어 있는 침입 방지 기능으로, 스위치를 통과하는 모든 트래픽을 분석하고 악성 트래픽을 차단합니다. 이는 네트워크의 성능 저하를

최소화하면서 보안을 강화할 수 있는 방법이지만, 처리 능력이 한정되어 있어 대용량 트래픽 환경에서는 성능 제한이 있을 수 있습니다.

8.방화벽 기반 IPS
문제: 패킷 기반의 탐지 및 방어 기능을 제공하는 방화벽 기반 IPS는 무엇입니까?
해설: 방화벽 기반 IPS는 네트워크 방화벽에 통합된 침입 방지 기능으로, 네트워크를 통과하는 패킷을 검사하여 악의적인 트래픽을 식별하고 차단합니다. 이 시스템은 네트워크의 보안 정책을 기반으로 작동하며, 불필요하거나 위험한 트래픽을 효과적으로 필터링합니다.

9.라우터 필터링
문제: 네트워크 보안을 강화하는 데 사용되는 라우터 필터링은 무엇입니까?
해설: 라우터 필터링은 라우터에 구성된 액세스 리스트를 사용하여 네트워크로 들어오는 또는 나가는 트래픽을 제어하는 기술입니다. 이는 특정 IP 주소, 포트 번호, 프로토콜 유형 등을 기준으로 패킷을 허용하거나 거부함으로써 내부 네트워크를 외부 위협으로부터 보호합니다.

10.One-Time Password 생성 및 인증
문제: 보안성을 강화하기 위해 사용되는 One-Time Password의 생성 및 인증 방식은 무엇입니까?
해설: One-Time Password(OTP)는 사용자가 단 한 번만 사용할 수 있는 비밀번호로, 알고리즘에 기반하여 동적으로 생성됩니다. OTP는 시간 동기화 방식이나 이벤트 기반 방식으로 생성되며, 재사용 공격에 대한 보안을 강화하기 위해 사용됩니다. 사용자는 인증 시 OTP를 입력하여 자신의 정체성을 증명합니다.

11.세션 하이재킹 방어
문제: 세션 하이재킹을 방어하는 방법은 무엇입니까?
해설: 세션 하이재킹 방어에는 전송 데이터의 암호화, 재인증 시행, 취약점 패치, 그리고 ACK 패킷의 비율 조정 등이 있습니다. 이 중 데이터 암호화는 가장 기본적이며 효과적인 방법으로, 전송되는 데이터를 암호화하여 중간자 공격에 대한 위험을 줄입니다. 재인증은 세션 도중 정기적으로 사용자의 인증을 다시 확인하는 것을 의미하며, 시스템의 취약점을 해결하기 위한 패치 작업은 보안을 강화하는 데 필수적입니다.

12.이더넷 물리 주소
문제: 유효한 이더넷 물리 주소(MAC 주소)의 형식은 무엇입니까?
해설: 이더넷 물리 주소, 즉 MAC 주소는 6개의 2자리 16진수로 구성되며, 각각은 콜론(:) 또는 하이픈(-)으로 구분됩니다. 예를 들어, '00:0C:29:97:13:8C'는 유효한 MAC 주소 형식입니다. MAC 주소는 네트워크 상의 장비를 구별하기 위한 고유한 식별자로 사용됩니다.

13.IDS(Intrusion Detection System)
문제: HIDS와 NIDS의 차이점은 무엇입니까?
해설: HIDS(Host-based IDS)는 특정 호스트 시스템에서 발생하는 이벤트를 모니터링하여 침입을 탐지하는 반면, NIDS(Network-based IDS)는 네트워크 트래픽을 분석하여 침입을

탐지합니다. HIDS는 시스템 내부의 로그 파일, 시스템 호출 등을 분석하고, NIDS는 네트워크를 통과하는 패킷의 헤더와 페이로드를 분석하여 비정상적인 패턴을 찾아냅니다.

14.UTM과 ESM
문제: UTM(Unified Threat Management)과 ESM(Enterprise Security Management)의 기능은 무엇입니까?
해설: UTM은 여러 보안 기능을 하나의 장비로 통합하여 제공하는 반면, ESM은 조직의 보안 정책을 반영하여 다양한 보안 시스템을 통합 관리합니다. UTM은 방화벽, 안티바이러스, 스팸 필터링 등을 제공하고, ESM은 보안 이벤트의 로그를 수집하고 분석하여 조직의 보안을 강화합니다.

15.Fragment Overlap Attack
문제: Fragment Overlap Attack의 원리는 무엇입니까?
해설: Fragment Overlap Attack은 공격자가 IP 패킷의 조각을 조작하여 침입 탐지 시스템(IDS)을 우회하는 기법입니다. 공격자는 두 개의 패킷 조각을 생성하고, 첫 번째 패킷 조각으로 허용된 포트 번호를 포함시킨 후, 두 번째 패킷 조각으로 첫 번째 패킷의 일부를 덮어씌워 IDS가 두 번째 패킷 조각을 허용하도록 만듭니다.

16.SQL 인젝션 공격
문제: SQL 인젝션 공격이란 무엇입니까?
해설: SQL 인젝션 공격은 애플리케이션의 보안 취약점을 이용하여 데이터베이스에 악의적인 SQL 코드를 주입하고 실행하는 기법입니다. 이를 통해 공격자는 데이터베이스에서 데이터를 무단으로 조회, 수정, 삭제할 수 있으며, 심지어 데이터베이스 서버를 제어할 수도 있습니다. 이를 방지하기 위해 입력 값에 대한 검증과 파라미터화된 쿼리 사용이 필요합니다.

17.XSS(Cross-Site Scripting)
문제: XSS 공격의 유형에는 어떤 것들이 있습니까?
해설: XSS 공격에는 주로 세 가지 유형이 있습니다: 반사형(Reflected), 저장형(Stored), 그리고 DOM 기반(DOM-based) XSS입니다. 반사형은 사용자로부터 입력 받은 스크립트를 즉시 실행하는 것이고, 저장형은 악성 스크립트가 웹 서버에 저장되어 다른 사용자에게 전달되는 것입니다. DOM 기반은 클라이언트 측 스크립트 내에서 발생하며, 문서 객체 모델(DOM)을 조작합니다.

18.DDoS(Distributed Denial of Service)
문제: DDoS 공격이란 무엇이며, 어떻게 방어할 수 있습니까?
해설: DDoS 공격은 다수의 시스템을 이용하여 대상의 네트워크 자원을 과부하 상태로 만들어 정상적인 서비스 이용을 방해하는 공격입니다. 방어 방법으로는 트래픽 분산, 공격 트래픽 필터링, 대역폭 증가, 그리고 공격 징후를 조기에 탐지할 수 있는 시스템의 구축 등이 있습니다.

19.랜섬웨어
문제: 랜섬웨어의 작동 원리와 예방 방법은 무엇입니까?

해설: 랜섬웨어는 사용자의 시스템에 침입하여 데이터를 암호화하고, 이를 해제하기 위한 몸값을 요구하는 악성 프로그램입니다. 예방 방법으로는 정기적인 백업, 최신 보안 패치 적용, 이메일 첨부파일에 대한 주의, 그리고 안티바이러스 소프트웨어의 사용 등이 있습니다.

20.피싱 공격

문제: 피싱 공격의 목적과 이를 식별하는 방법은 무엇입니까?
해설: 피싱 공격의 주된 목적은 사용자의 개인정보나 금융정보를 불법적으로 획득하는 것입니다. 이를 식별하는 방법으로는 URL의 정확성 검증, SSL 인증서 확인, 이메일의 발신자 주소와 내용의 정확성 검토, 그리고 의심스러운 첨부파일이나 링크를 클릭하지 않는 것 등이 있습니다.

21.웹 취약점 스캐너

문제: 웹 취약점 스캐너의 기능은 무엇입니까?
해설: 웹 취약점 스캐너는 웹 애플리케이션의 보안 취약점을 자동으로 탐지하는 도구입니다. SQL 인젝션, XSS, CSRF 등의 취약점을 검사하며, 웹 애플리케이션의 보안 수준을 평가하고 강화하는 데 도움을 줍니다. 정기적인 스캔을 통해 새로운 취약점을 발견하고 적시에 대응할 수 있습니다.

22.사이버 포렌식

문제: 사이버 포렌식의 주요 과정은 무엇입니까?
해설: 사이버 포렌식은 디지털 증거를 수집, 분석하여 범죄를 조사하는 과정입니다. 주요 단계로는 증거의 식별, 보존, 수집, 분석, 보고가 있으며, 이 과정을 통해 법적으로 유효한 증거를 확보하고 범죄 사실을 밝힐 수 있습니다.

23.암호화 알고리즘

문제: 대칭키 암호화와 비대칭키 암호화의 차이점은 무엇입니까?
해설: 대칭키 암호화는 같은 키를 이용해 데이터를 암호화하고 복호화하는 반면, 비대칭키 암호화는 공개키로 암호화하고 개인키로 복호화합니다. 대칭키는 속도가 빠르지만 키 관리가 어렵고, 비대칭키는 키 관리가 용이하지만 처리 속도가 느립니다.

24.무선 네트워크 보안

문제: WEP, WPA, WPA2의 차이점은 무엇입니까?
해설: WEP는 초기 무선 보안 프로토콜로 쉽게 해킹될 수 있습니다. WPA는 WEP의 취약점을 개선한 프로토콜이며, WPA2는 더 강화된 암호화와 보안을 제공합니다. WPA3는 최신 프로토콜로, 이전 버전보다 더 강력한 보안 기능을 갖추고 있습니다.

25.클라우드 보안

문제: 클라우드 서비스 모델(SaaS, PaaS, IaaS)의 보안 책임 분담은 어떻게 다릅니까?
해설: SaaS에서는 서비스 제공자가 대부분의 보안 책임을 담당합니다. PaaS에서는 개발자가 애플리케이션 수준의 보안을, 제공자는 플랫폼 수준의 보안을 담당합니다. IaaS에서는 사용자가 운영 체제 이상의 보안을, 제공자는 인프라 수준의 보안을 담당합니다.

26.사회공학 공격
문제: 사회공학 공격의 예시와 방어 방법은 무엇입니까?
해설: 사회공학 공격은 신뢰를 이용하여 정보를 얻는 방법으로, 피싱, 프리텍스팅, 베이트링 등이 있습니다. 방어 방법으로는 직원 교육, 정책 수립, 의심스러운 요청에 대한 검증 절차 마련 등이 있습니다.

27.모바일 보안 위협
문제: 모바일 기기에서 발생할 수 있는 보안 위협은 무엇입니까?
해설: 모바일 보안 위협에는 악성 앱 설치, 무단 데이터 접근, 네트워크 스누핑, 운영 체제의 취약점을 이용한 공격 등이 있습니다. 사용자는 앱의 권한을 주의 깊게 검토하고, 보안 패치를 적용하며, 안전하지 않은 네트워크 사용을 피해야 합니다.

28.IoT 보안
문제: IoT 장치의 보안 취약점과 이를 강화하는 방법은 무엇입니까?
해설: IoT 장치는 종종 업데이트 부족, 약한 기본 설정, 불안전한 인터페이스 등으로 인해 취약합니다. 보안을 강화하기 위해서는 정기적인 소프트웨어 업데이트, 강력한 암호화, 네트워크 분리, 보안 감사 등이 필요합니다.

29.가상화 보안
문제: 가상화 환경에서의 보안 고려 사항은 무엇입니까?
해설: 가상화 환경에서는 하이퍼바이저 보안, 가상 네트워크의 격리, 가상 머신 간의 안전한 데이터 이동, 가상 머신의 보안 설정과 패치 관리 등이 중요합니다. 가상 환경 특유의 취약점을 관리하고, 가상 머신을 정기적으로 모니터링해야 합니다.

30.애플리케이션 보안
문제: 애플리케이션 수준에서의 보안 강화 방법은 무엇입니까?
해설: 애플리케이션 수준의 보안 강화에는 코드 검토, 취약점 스캐닝, 안전한 코딩 관행, 인증 및 권한 부여 메커니즘의 강화, 그리고 데이터 보호를 위한 암호화 적용 등이 포함됩니다. 개발 단계부터 보안을 고려하고, 지속적인 보안 교육과 테스트를 실시하는 것이 중요합니다.

31.보안 인시던트 대응
문제: 보안 인시던트 대응 계획에 포함되어야 하는 주요 요소는 무엇입니까?
해설: 보안 인시던트 대응 계획에는 인시던트 식별, 보고, 조사, 대응, 복구, 그리고 사후 분석과 개선이 포함되어야 합니다. 이 계획은 조직이 보안 사고 발생 시 신속하고 효과적으로 대처할 수 있도록 체계적인 절차를 마련하는 데 중요합니다.

32.데이터 유출 방지(DLP)
문제: 데이터 유출 방지(DLP) 시스템의 기능은 무엇입니까?
해설: DLP 시스템은 조직의 중요한 데이터가 무단으로 외부로 유출되는 것을 방지하는 기술입니다. 데이터의 이동을 모니터링하고, 민감한 정보가 포함된 문서의 전송을 제한하며, 데이터 유출 위험을 감지할 때 경고를 발생시킵니다.

33.멀웨어 분석
문제: 멀웨어 분석의 목적은 무엇입니까?
해설: 멀웨어 분석은 악성 코드의 행동, 기능, 그리고 퍼짐 방식을 이해하기 위해 수행됩니다. 이를 통해 보안 전문가는 멀웨어의 소스를 추적하고, 감염된 시스템을 정화하며, 향후 유사한 공격을 방지하기 위한 대책을 마련할 수 있습니다.

34.보안 감사
문제: 보안 감사의 중요성은 무엇입니까?
해설: 보안 감사는 조직의 보안 정책과 절차가 적절히 이행되고 있는지를 평가합니다. 이 과정을 통해 보안 취약점을 식별하고, 위험을 관리하며, 규정 준수 여부를 확인할 수 있습니다.

35.사이버 보안 교육
문제: 사이버 보안 교육의 중요성은 무엇입니까?
해설: 사이버 보안 교육은 직원들이 보안 위협을 인식하고, 올바른 보안 관행을 습득하며, 잠재적인 보안 사고를 예방하는 데 중요합니다. 지속적인 교육과 훈련은 조직의 전반적인 보안 수준을 향상시키는 데 기여합니다.

36.암호 관리
문제: 효과적인 암호 관리 정책에는 어떤 요소들이 포함되어야 합니까?
해설: 효과적인 암호 관리 정책에는 강력한 암호 생성 규칙, 정기적인 암호 변경, 암호의 다양성 및 비밀 유지, 그리고 암호 저장과 관리를 위한 안전한 방법이 포함되어야 합니다.

37.네트워크 모니터링
문제: 네트워크 모니터링의 목적은 무엇입니까?
해설: 네트워크 모니터링은 네트워크의 성능을 지속적으로 추적하고, 문제를 식별하며, 네트워크 자원의 최적화를 돕는 과정입니다. 이는 네트워크의 안정성과 효율성을 유지하는 데 필수적입니다.

38.가상 사설망(VPN)
문제: VPN이 제공하는 보안 이점은 무엇입니까?
해설: VPN은 인터넷을 통한 데이터 전송 시 암호화를 제공하여, 사용자의 데이터와 통신이 외부로부터 보호받을 수 있도록 합니다. 이는 특히 공공 Wi-Fi와 같은 불안전한 네트워크에서 중요합니다.

39.사이버 보안 정책
문제: 사이버 보안 정책의 구성 요소는 무엇입니까?
해설: 사이버 보안 정책은 조직의 정보 자산을 보호하기 위한 규칙과 절차를 정의합니다. 이에는 접근 제어, 데이터 분류, 사고 대응, 사용자 교육 및 훈련 등이 포함됩니다.

40.위험 평가
문제: 위험 평가의 목적은 무엇입니까?
해설: 위험 평가는 조직이 직면할 수 있는 보안 위험을 식별하고, 이에 대한 우선 순위를 정하

며, 적절한 위험 완화 전략을 수립하는 과정입니다. 이는 조직의 자산을 보호하고 비즈니스 연속성을 유지하는 데 중요한 역할을 합니다.