[취업폭격기 Zeromini 위클리 개념폭격 #1]

📕 과목 : 정보보안 - 네트워크 보안

🔥 참고문제 : 2023년 공무원 9급 기출문제 (네트워크 보안 과목)

🌝 문제 수정 버전 : V 1.0

해당 문제는 샘플 버전이며 향후 지속적으로 업로드 드릴 예정입니다

1. 문제: HTTPS 통신에서 암호화되지 않는 요소는 무엇인가요?
   해설: HTTPS 통신에서는 대부분의 요소가 암호화되지만, 요청의 메타데이터 중 일부는 암호화되지 않습니다. 예를 들어, 요청의 URL, HTTP 메소드(GET, POST 등), 그리고 몇몇 HTTP 헤더는 암호화되지 않습니다.
2. 문제: 커버로스(Kerberos) 버전4의 특징 중 하나를 기술하시오.
   해설: 커버로스는 MIT에서 개발된 네트워크 인증 프로토콜로, 클라이언트와 서버 간의

안전한 인증을 제공합니다. 이 프로토콜은 신뢰할 수 있는 제3자인 키 분배 센터(KDC)를 사용하여 인증을 수행합니다.

3. 문제: 스니핑(sniffing) 공격에 대해 설명하시오.
   해설: 스니핑 공격은 네트워크 트래픽을 도청하여 중요한 정보를 획득하는 공격 방법입니다. 이는 주로 네트워크 상에서 전송되는 데이터를 가로채어, 중요한 정보(예: 로그인 정보, 개인 정보 등)를 빼내는 데 사용됩니다.

4. 문제: OpenFlow 프로토콜을 활용하는 네트워크 기술에 대해 설명하시오.
   해설: OpenFlow는 SDN(Software Defined Networking)의 핵심 프로토콜로, 네트워크의 제어 평면과 데이터 평면을 분리하여 네트워크를 프로그래밍 가능하게 만듭니다. 이를 통해 네트워크 운영자는 네트워크 트래픽의 흐름을 더욱 세밀하게 제어할 수 있습니다.

5. 문제: SSL/TLS 공격 유형에 대해 설명하시오.
   해설: SSL/TLS는 웹 통신의 보안을 위해 널리 사용되는 프로토콜입니다. 그러나 이러한 프로토콜도 다양한 공격 유형에 취약할 수 있습니다. 예를 들어, 중간자 공격(Man-in-the-Middle Attack)에서 공격자는 통신을 중계하면서 암호화된 데이터를 복호화하거나 조작할 수 있습니다. 또한, 다운그레이드 공격(Downgrade Attack)에서는 공격자가 클라이언트와 서버 사이의 통신을 덜 안전한 프로토콜로 변경하여 공격을 수행할 수 있습니다.

6. 문제: POP3 프로토콜의 주요 기능에 대해 설명하시오.
   해설: POP3(Post Office Protocol version 3)는 이메일 서버로부터 이메일을 다운로드하고, 이메일 클라이언트에서 이메일을 확인하는 데 사용되는 프로토콜입니다. 이 프로토콜은 이메일 서버와 클라이언트 간의 통신을 위한 명령과 응답으로 동작합니다.

7. 문제: IPv4 데이터그램 형식에 대해 설명하시오.
   해설: IPv4 데이터그램은 여러 필드로 구성되어 있습니다. 'Flags'는 단편화와 관련이 있는 필드이며, 'Time To Live'는 데이터그램이 방문할 수 있는 최대 라우터의 수를 나타내는 필드입니다. 'Total Length'는 헤더를 제외한 IP 데이터그램의 길이를 나타내는 필드이며, 'Protocol'은 IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 나타내는 필드입니다.

8. 문제: 네트워크 관리 기능 중 성능 관리에 대해 설명하시오.
   해설: 성능 관리는 네트워크의 효과적인 실행을 보장하기 위해 네트워크를 감시하고 제어하는 기능입니다. 이는 통계 정보를 수집하고, 시스템 상태 이력 기록을 유지하며, 시스템 성능을 측정하고, 지연 시간과 대역폭 사용률, 패킷 처리율 등을 단계별 또는 시간별로 관리합니다.

9. 문제: 공개키 기반 구조 X.509(PKIX) 모델에서 종단 개체(end entity)와 인증 기관(certificate authority) 간의 관리 기능에 대해 설명하시오.

해설: X.509(PKIX) 모델에서 종단 개체와 인증 기관 간의 관리 기능에는 등록, 키 쌍 복구, 키 쌍 갱신, 교차 인증 등이 있습니다. 등록은 인증 기관에 종단 개체를 등록하는 과정이며, 키 쌍 복구는 키 쌍이 손실된 경우 복구하는 과정입니다. 키 쌍 갱신은 키 쌍의 유효 기간이 만료되거나 보안 문제가 발생했을 때 새로운 키 쌍을 생성하는 과정이며, 교차 인증은 서로 다른 인증 기관이 서로를 인증하는 과정입니다.

10. 문제: 스미싱 공격을 예방하는 방법에 대해 설명하시오.
    해설: 스미싱은 SMS 메시지를 통해 사용자를 속여 악성 웹사이트로 유도하거나 악성 앱을 설치하게 하는 공격입니다. 이를 예방하기 위해서는 보호되지 않은 무선 공유기의 사용을 피하고, 알 수 없는 출처의 앱 설치를 허용하지 않아야 합니다. 또한, 모바일 백신을 설치하여 스마트폰의 보안 상태를 주기적으로 점검하고, 스마트폰 운영체제를 항상 최신 버전으로 업데이트하여 보안상 취약점이 없도록 관리해야 합니다.

11. 문제: Firewall의 주요 기능에 대해 설명하시오.
    해설: Firewall은 네트워크의 보안을 유지하기 위해 사용되는 장치 또는 소프트웨어로, 사전에 정의된 규칙에 따라 네트워크 트래픽을 허용하거나 차단합니다. 이는 네트워크 내부와 외부 간의 통신을 제어하여, 외부로부터의 불필요하거나 위험한 접근을 차단하고, 내부 네트워크의 정보를 보호하는 역할을 합니다.

12. 문제: IEEE 802.11i RSN의 동작 단계에 대해 설명하시오.
    해설: IEEE 802.11i RSN(Robust Security Network)의 동작 단계는 다음과 같습니다. 먼저, 탐색(discovery) 단계에서는 클라이언트와 액세스 포인트 간의 통신이 가능한지 확인합니다. 다음으로, 인증(authentication) 단계에서는 클라이언트와 액세스 포인트 간의 신원을 확인합니다. 그 후, 키 생성 및 분배(key generation and distribution) 단계에서는 암호화된 통신을 위한 키를 생성하고 분배합니다. 마지막으로, 안전 데이터 전송(protected data transfer) 단계에서는 생성된 키를 사용하여 데이터를 안전하게 전송합니다.

13. 문제: SNMP에서 관리 대상 장치 내부 객체들에 대한 정보 저장소를 나타내는 용어는 무엇인가요?
    해설: SNMP(Simple Network Management Protocol)에서 관리 대상 장치 내부 객체들에 대한 정보를 저장하는 저장소를 MIB(Management Information Base)라고 합니다. MIB는 네트워크 장치의상태, 구성, 성능 등에 대한 정보를 포함하며, SNMP를 통해 이 정보를 조회하거나 변경할 수 있습니다.

14. 문제: 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알림으로써 패킷의 흐름을 바꾸는 공격은 무엇인가요?
    해설: 이러한 공격 방식은 ICMP 리다이렉트 공격이라고 합니다. 공격자는 ICMP 리다이렉트 메시지를 사용하여 트래픽을 자신에게로 유도하게 만듭니다. 이를 통해 공격자는 네트워크 트래픽을 도청하거나 조작할 수 있습니다.

15. 문제: 시저 암호에 대해 설명하고, 평문 "STUDY"를 시저 암호를 사용하여 암호화하는 방법을 설명하시오.
    해설: 시저 암호는 가장 간단한 형태의 치환 암호 중 하나로, 각 문자를 알파벳 순서로 일정한 수만큼 이동시켜 암호화합니다. 예를 들어, 시저 암호 치환식 C = (P + 3) mod 26을 사용하여 평문 "STUDY"를 암호화하면, 각 문자를 알파벳 순서로 3칸 이동시키므로 암호문은 "VWXGB"가 됩니다.

16. 문제: SSL Handshake 프로토콜의 '서버 인증과 키 교환' 단계에서 인증서 메시지가 사용되지 않는 기법은 무엇인가요?
    해설: SSL Handshake 프로토콜의 '서버 인증과 키 교환' 단계에서 인증서 메시지가 사용되지 않는 기법은 Anonymous DH 기법입니다. 이 기법은 서버의 인증서를 사용하지 않으므로, 서버의 신원을 확인할 수 없어 중간자 공격에 취약합니다.

17. 문제: 전자 서명에 대해 설명하시오.
    해설: 전자 서명은 디지털 데이터에 첨부되어, 데이터의 무결성과 송신자의 신원을 확인할 수 있게 하는 기술입니다. 전자 서명은 송신자의 개인 키를 사용하여 생성되며, 수신자는 송신자의 공개 키를 사용하여 전자 서명을 검증할 수 있습니다. 이를 통해 데이터가 송신자에 의해 생성되었으며, 전송 중에 변경되지 않았음을 확인할 수 있습니다.

18. 문제: 네트워크 보안에서 IDS(Intrusion Detection System)와 IPS(Intrusion Prevention System)의 차이점에 대해 설명하시오.
    해설: IDS는 네트워크 내의 비정상적인 행동이나 알려진 공격 패턴을 감지하는 시스템입니다. IDS는 이러한 활동을 감지하고 경고를 발생시키지만, 공격을 차단하거나 막는 기능은 없습니다. 반면에, IPS는 IDS의 기능에 더해, 비정상적인 행동이나 알려진 공격을 실시간으로 차단하는 기능을 가지고 있습니다.

19. 문제: 네트워크 보안에서 사용되는 암호화 기술 중 대칭키 암호화와 비대칭키 암호화의 차이점에 대해 설명하시오.
    해설: 대칭키 암호화는 암호화와 복호화에 같은 키를 사용하는 암호화 방식입니다. 이 방식은 계산이 빠르다는 장점이 있지만, 키를 안전하게 공유하는 것이 어렵다는 단점이 있습니다. 반면에, 비대칭키 암호화는 암호화와 복호화에 서로 다른 키(공개키와 개인키)를 사용하는 암호화 방식입니다. 이 방식은 키 공유 문제를 해결하지만, 대칭키 암호화에 비해 계산이 느리다는 단점이 있습니다.

20. 문제: 네트워크 보안에서 사용되는 '포트 스캐닝'에 대해 설명하시오.
    해설: 포트 스캐닝은 네트워크에 연결된 컴퓨터의 특정 포트가 열려 있는지 확인하는 과정입니다. 이는 공격자가 시스템의 취약점을 찾아내는 데 사용될 수 있습니다. 열려 있는 포트를 통해 공격자는 시스템에 접근하거나 서비스를 중단시키는 등의 공격을 시도할 수 있습니다.

21. 문제: 네트워크 보안에서 '피싱' 공격에 대해 설명하시오.
    해설: 피싱은 사용자를 속여 개인 정보를 획득하는 공격 방법입니다. 공격자는 보통 이

메일이나 웹사이트를 통해 사용자에게 가짜 메시지를 보내고, 이를 통해 사용자의 개인 정보(예: 로그인 정보, 신용카드 정보 등)를 획득합니다.

22. 문제: 네트워크 보안에서 '인증'의 의미에 대해 설명하시오.
해설: 인증은 사용자, 시스템, 또는 서비스의 신원을 확인하는 과정입니다. 이는 사용자가 자신이 주장하는 사람이 맞는지, 또는 시스템이나 서비스가 신뢰할 수 있는지를 확인하기 위해 사용됩니다. 인증은 일반적으로 사용자 이름과 비밀번호, 디지털 인증서, 바이오메트릭 데이터 등을 사용하여 수행됩니다.

23. 문제: 네트워크 보안에서 '암호화'의 의미에 대해 설명하시오.
해설: 암호화는 정보를 안전하게 보호하기 위해 데이터를 읽을 수 없는 형태로 변환하는 과정입니다. 암호화된 데이터는 적절한 키를 가진 사람만이 복호화하여 원래의 형태로 되돌릴 수 있습니다. 암호화는 데이터를 보호하고, 데이터의 무결성을 유지하며, 데이터의 출처를 확인하는 데 사용됩니다.

24. 문제: 네트워크 보안에서 '방화벽'의 역할에 대해 설명하시오.
해설: 방화벽은 네트워크의 보안을 유지하기 위해 사용되는 장치 또는 소프트웨어로, 사전에 정의된 규칙에 따라 네트워크 트래픽을 허용하거나 차단합니다. 이는 네트워크 내부와 외부 간의 통신을 제어하여, 외부로부터의 불필요하거나 위험한 접근을 차단하고, 내부 네트워크의 정보를 보호하는 역할을 합니다.

25. 문제: 네트워크 보안에서 '무결성'의 의미에 대해 설명하시오.
해설: 무결성은 데이터가 원래의 상태에서 변경되지 않았음을 보장하는 보안 원칙입니다. 이는 데이터가 전송, 저장, 검색 과정에서 실수나 고의적인 조작으로부터 보호되어야 함을 의미합니다.

26. 문제: 네트워크 보안에서 '가용성'의 의미에 대해 설명하시오.
해설: 가용성은 필요한 시점에 시스템과 데이터에 접근할 수 있음을 보장하는 보안 원칙입니다. 이는 시스템이 항상 작동하며, 필요한 데이터에 접근할 수 있어야 함을 의미합니다.

27. 문제: 네트워크 보안에서 '비밀성'의 의미에 대해 설명하시오.
해설: 비밀성은 데이터가 인가된 사용자만이 접근할 수 있도록 보장하는 보안 원칙입니다. 이는 데이터가 암호화되어 인가되지 않은 사용자에게는 읽을 수 없는 형태로 보호되어야 함을 의미합니다.

28. 문제: 네트워크 보안에서 '공격자'의 의미에 대해 설명하시오.
해설: 공격자는 네트워크나 시스템에 대해 불법적이거나 악의적인 행동을 수행하는 개인이나 그룹을 의미합니다. 공격자는 보통 시스템의 취약점을 이용하여 정보를 훔치거나, 시스템을 손상시키거나, 서비스를 중단시키는 등의 행동을 수행합니다.

29. 문제: 네트워크 보안에서 '디지털 인증서'의 역할에 대해 설명하시오.
해설: 디지털 인증서는 인터넷에서 통신하는 개체의 신원을 인증하는 데 사용되는 파일

입니다. 디지털 인증서는 개체의 이름, 공개 키, 인증서를 발행한 기관, 그리고 인증서의 유효 기간 등의 정보를 포함하며, 이 정보는 디지털 서명으로 보호됩니다.