🥷

[취업폭격기 Zeromini 위클리 개념폭격 #5]

📕 과목 : 정보보호론

🔥 참고문제 : 2023년 공무원 지방직 9급 기출문제 (정보보호론)

🌝 문제 수정 버전 : V 1.0

1. **문제: 데이터의 위 · 변조를 방어하는 기술이 목표로 하는 것을 설명하시오.**
   해설: 데이터의 위 · 변조를 방어하는 기술은 무결성을 목표로 합니다. 무결성은 데이터가 원래의 상태에서 변경, 손상, 손실 없이 유지되는 것을 보장하는 것을 의미합니다.
2. **문제: UDP 헤더 포맷의 구성 요소를 설명하시오.**
   해설: UDP 헤더 포맷의 구성 요소에는 발신지 포트 번호, 목적지 포트 번호, 길이, 체크섬 등이 있습니다. 순서 번호는 TCP에서 사용되는 구성 요소로, UDP에서는 사용되지 않습니다.

3. **문제: 논리 폭탄에 대해 설명하시오.**
   해설: 논리 폭탄은 침입자에 의해 악성 소프트웨어에 삽입된 코드로서, 사전에 정의된 조건이 충족되기 전까지는 휴지 상태에 있다가 조건이 충족되면 의도한 동작이 트리거되도록 하는 것을 말합니다.

4. **문제: 대칭키 암호 알고리즘에 대해 설명하시오.**
   해설: 대칭키 암호 알고리즘은 암호화와 복호화에 같은 키를 사용하는 암호화 방식입니다. SEED, IDEA, LEA 등이 대표적인 대칭키 암호 알고리즘입니다. ECC는 비대칭키 암호 알고리즘에 속합니다.

5. **문제: 정보통신망 이용촉진 및 정보보호 등에 관한 법률에서 규정하고 있는 사항에 대해 설명하시오.**
   해설: 이 법률은 정보통신망의 표준화 및 인증, 정보통신망의 안정성 확보, 집적된 정보통신시설의 보호 등을 규정하고 있습니다. 고정형 영상정보처리기기의 설치 · 운영 제한은 개별적인 법률에 의해 규정됩니다.

6. **문제: CSRF 공격에 대해 설명하시오.**
   해설: CSRF(Cross-Site Request Forgery) 공격은 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격입니다. 특정 웹사이트가 사용자의 웹 브라우저를 신뢰하는 점을 노리고 사용자의 권한을 도용하려는 것입니다.

7. **문제: IPSec의 터널 모드를 이용한 VPN에 대해 설명하시오.**
   해설: IPSec의 터널 모드는 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 VPN 라우터 또는 IPSec 게이트웨이의 IP 주소를 넣는 방식입니다. 이 모드는 새로운 IP 헤더를 추가하기 때문에 전송 모드 대비 전체 패킷이 길어집니다.

8. **문제: 전자서명법 상 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정에 대해 설명하시오.**
   해설: 인정을 받으려는 전자서명인증사업자는 평가기관으로부터 평가를 먼저 받아야 하며, 평가 결과를 인정기관에 제출해야 합니다. 인정기관은 평가 결과와 인정을 받으려는 전자서명인증사업자가 법정 자격을 갖추었는지 여부를 확인하여 인정 여부를 결정합니다.

9. **문제: 위험 평가 접근방법에 대해 설명하시오.**
   해설: 위험 평가 접근방법에는 기준 접근법, 비정형 접근법, 상세 위험 분석, 복합 접근법 등이 있습니다. 이들 방법은 각각 다른 특징과 장단점을 가지며, 상황에 따라 적절하게 선택하여 사용해야 합니다.

10. **문제: ISMS-P 인증 기준의 세 영역 중 하나인 관리체계 수립 및 운영에 대해 설명하시오.**
    해설: 관리체계 수립 및 운영 영역에는 관리체계 기반 마련, 위험 관리, 관리체계 점검 및

개선 등이 포함됩니다. 이 영역은 정보보호 관리체계의 효과적인 운영을 위한 기반을 마련하고, 위험을 관리하며, 지속적인 개선을 위한 점검을 수행하는 것을 목표로 합니다.

11. **문제: OTP 토큰이 속하는 인증 유형에 대해 설명하시오.**
    해설: OTP(One-Time Password) 토큰은 '가지고 있는 것'에 해당하는 인증 유형입니다. 이는 사용자가 물리적으로 소지하고 있는 장치나 카드 등을 이용하여 인증하는 방식을 의미합니다.

12. **문제: 서비스 거부 공격에 대해 설명하시오.**
    해설: 서비스 거부 공격(Denial of Service, DoS)은 공격 대상의 시스템이 정상적인 서비스를 제공하지 못하도록 고의적으로 과부하를 유발하는 공격입니다. 이는 네트워크 트래픽을 과도하게 증가시키거나, 시스템 자원을 과도하게 소모시키는 방법 등으로 이루어집니다.

13. **문제: 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제48조의4(침해사고의 원인 분석 등)의 내용을 설명하시오.**
    해설: 이 법률은 정보통신서비스 제공자 등 정보통신망을 운영하는 자가 침해사고가 발생하면 원인을 분석하고, 그 결과에 따라 피해의 확산 방지를 위한 사고대응, 복구 및 재발 방지에 필요한 조치를 하도록 규정하고 있습니다.

14. **문제: 전자상거래에서 소비자의 주문 정보와 지불 정보를 보호하기 위한 SET의 이중 서명에 대해 설명하시오.**
    해설: SET(Secure Electronic Transaction)의 이중 서명은 소비자의 주문 정보와 지불 정보를 독립적으로 암호화하여 전송하는 방식입니다. 이를 통해 상점은 주문 정보만, 금융 기관은 지불 정보만 확인할 수 있어, 소비자의 정보 보호를 도모합니다.

15. **문제: SHA-512 알고리즘의 수행 라운드 수와 처리하는 블록의 크기에 대해 설명하시오.**
    해설: SHA-512 알고리즘은 80라운드의 연산을 수행하며, 처리하는 블록의 크기는 1024비트입니다. 이 알고리즘은 입력된 메시지를 1024비트의 블록으로 나누어 각 블록을 80라운드의 연산을 통해 해시 값을 생성합니다.

16. **문제: 블록 암호 운용 모드에 대해 설명하시오.**
    해설: 블록 암호 운용 모드는블록 암호를 어떻게 운용할 것인지를 정의한 것입니다. 이에는 ECB(Electronic Codebook), CBC(Cipher Block Chaining), CFB(Cipher Feedback), OFB(Output Feedback), CTR(Counter) 등이 있습니다. 각 모드는 암호화의 특성과 보안 수준, 용도 등에 따라 적절하게 선택하여 사용합니다.

17. **문제: 트로이목마 바이러스에 대해 설명하시오.**
    해설: 트로이목마 바이러스는 사용자가 원하는 기능을 제공하면서, 그 뒤에 숨겨진 악성 코드를 실행하는 소프트웨어를 말합니다. 이는 사용자의 시스템을 공격하거나, 개인 정보를 도용하거나, 시스템의 제어권을 탈취하는 등의 행위를 수행합니다.

18. **문제: 공개키 기반구조(PKI)에 대해 설명하시오.**
    해설: 공개키 기반구조(PKI)는 디지털 인증서의 생성, 배포, 관리, 폐기 등을 관리하는 시스템입니다. 이는 공개키 암호화와 디지털 서명 기술을 이용하여 인터넷과 같은 네트워크 상에서 정보의 보안을 유지합니다.

19. **문제: 블루투스의 취약점에 대해 설명하시오.**
    해설: 블루투스는 인증 절차의 취약성, 암호화의 취약성, 주소 추적 등의 취약점을 가지고 있습니다. 이러한 취약점을 이용하면 공격자는 블루투스 장치를 통해 정보를 도용하거나, 장치를 제어하거나, 사용자의 위치를 추적하는 등의 공격을 수행할 수 있습니다.

20. **문제: 사회공학 공격에 대해 설명하시오.**
    해설: 사회공학 공격은 기술적인 방법보다는 사람의 심리나 행동을 이용하여 정보를 획득하거나 시스템에 침입하는 공격 방법을 말합니다. 이는 피싱, 스피어 피싱, 베이팅, 프리텍스팅 등 다양한 방법으로 이루어집니다.

21. **문제: 악성코드의 유형에 대해 설명하시오.**
    해설: 악성코드의 유형에는 바이러스, 웜, 트로이목마, 스파이웨어, 랜섬웨어 등이 있습니다. 이들은 각각 다른 특징과 동작 방식을 가지며, 사용자의 시스템을 공격하거나, 개인 정보를 도용하거나, 시스템의 제어권을 탈취하는 등의 행위를 수행합니다.

22. **문제: 네트워크 침입 탐지 시스템(NIDS)에 대해 설명하시오.**
    해설: 네트워크 침입 탐지 시스템(NIDS)은 네트워크 트래픽을 모니터링하며 악성 행동이나 의심스러운 패턴을 탐지하는 시스템입니다. 이는 공격을 실시간으로 탐지하고, 경고를 발생시키며, 필요한 경우 트래픽을 차단하는 역할을 수행합니다.

23. **문제: 블록체인의 작동 원리에 대해 설명하시오.**
    해설: 블록체인은 거래 정보를 블록에 담아 체인 형태로 연결하는 분산형 데이터베이스입니다. 각 블록은 이전 블록의 해시값을 포함하고 있어, 한번 기록된 정보는 변경이 불가능합니다. 이를 통해 데이터의 무결성과 안전성을 보장합니다.

24. **문제: 클라우드 컴퓨팅의 서비스 모델에 대해 설명하시오.**
    해설: 클라우드 컴퓨팅의 서비스 모델에는 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service) 등이 있습니다. 이들은 각각 인프라, 플랫폼, 소프트웨어를 서비스로 제공하며, 사용자는 필요한 서비스를 선택하여 사용할 수 있습니다.

25. **문제: 랜섬웨어의 작동 원리에 대해 설명하시오.**
    해설: 랜섬웨어는 사용자의 시스템에 침입하여 데이터를 암호화하는 악성코드입니다. 데이터를 암호화한 후, 복호화 키를 제공하기 위한 몸값을 요구하며, 이를 통해 금전적 이익을 취합니다.

26. **문제: 웹 쿠키의 기능과 보안 문제에 대해 설명하시오.**
    해설: 웹 쿠키는 웹사이트가 사용자의 브라우저에 저장하는 작은 텍스트 파일로, 사용자

의 세션 관리, 개인화 설정, 행동 추적 등의 기능을 수행합니다. 하지만 쿠키는 사용자의 개인 정보를 저장하고 전송하는 과정에서 보안 문제를 일으킬 수 있습니다.

27. **문제: SSL/TLS 프로토콜의 역할에 대해 설명하시오.**
    해설: SSL/TLS 프로토콜은 웹 브라우저와 서버 간의 통신을 암호화하여 정보의 안전성을 보장하는 역할을 합니다. 이를 통해 중간자 공격 등의 보안 위협으로부터 통신 내용을 보호합니다.

28. **문제: 사이버 보안의 3가지 주요 요소에 대해 설명하시오.**
    해설: 사이버 보안의 3가지 주요 요소는 기밀성, 무결성, 가용성입니다. 기밀성은 정보의 접근과 이용을 인가된 사용자만이 가능하게 하는 것, 무결성은 정보가 정확하고 완전하게 유지되는 것, 가용성은 정보와 시스템이 필요할 때 항상 사용 가능한 상태를 유지하는 것을 의미합니다.

29. **문제: 피싱 공격에 대해 설명하시오.**
    해설: 피싱 공격은 공격자가 가짜 웹사이트나 이메일 등을 통해 사용자로부터 개인 정보를 빼내는 공격입니다. 이는 보통 정상적인 기관이나 서비스로 위장하여 사용자의 신뢰를 이용합니다.

30. **문제: 웹 애플리케이션 방화벽(WAF)의 기능에 대해 설명하시오.**
    해설: 웹 애플리케이션 방화벽(WAF)은 웹 애플리케이션에 대한 공격을 탐지하고 차단하는 보안 솔루션입니다. SQL 인젝션, 크로스 사이트 스크립팅(XSS), 크로스 사이트 요청 위조(CSRF) 등의 공격을 방어하는 데 사용됩니다.