정보보호론

Ⓐ

(1번~20번)

(9급)

1. 정보보호의 목적 중 '기밀성'을 보장하기 위한 방법만을 묶은 것은?
   ① 데이터 백업 및 암호화
   ② 데이터 백업 및 데이터 복원
   ③ 데이터 복원 및 바이러스 검사
   ④ 접근통제 및 암호화
   ⑤ 접근통제 및 바이러스 검사

2. 다음 중 정보보호의 요소들에 대한 설명으로 옳은 것은?
   ① 부인방지(non-repudiation)란 정보가 비인가된 방식으로 변조되는 것을 방지하는 것을 의미한다.
   ② 무결성(integrity)이란 특정한 작업 또는 행위에 대해 책임소재를 확인 가능함을 의미한다.
   ③ 인증성(authenticity)이란 인가된 사용자가 필요 시 정보를 접근하고 변경하는 것이 가능함을 의미한다.
   ④ 가용성(availability)이란 정보나 해당 정보의 주체가 진짜임을 의미한다.
   ⑤ 기밀성(confidentiality)이란 정보의 비인가된 유출이 불가능함을 의미한다.

3. 다음 중 가장 안전한 패스워드는 어떤 것인가?
   ① 75481235
   ② abcd1234
   ③ korea2034
   ④ honggildong
   ⑤ do@ssud23

4. 다음 중 kerberos 인증 프로토콜에 대한 설명으로 옳지 않은 것은?
   ① Needham-Schroeder 프로토콜을 기반으로 만들어졌다.
   ② 대칭키 암호 알고리듬(Algorithm)을 이용한다.
   ③ 중앙 서버의 개입 없이 분산 형태로 인증을 수행한다.
   ④ 티켓 안에는 자원 활용을 위한 키와 정보가 포함되어 있다.
   ⑤ TGT를 이용해 자원 사용을 위한 티켓을 획득한다.

5. 다음 중 공개키 암호(public key cryptosystem)에 대한 설명으로 옳은 것은?
   ① 대표적인 암호로 AES, DES 등이 있다.
   ② 대표적인 암호로 RSA가 있다.
   ③ 일반적으로 같은 양의 데이터를 암호화하기 위한 연산이 대칭키 암호(symmetric key cryptosystem)보다 현저히 빠르다.
   ④ 대칭키 암호(symmetric key cryptosystem)보다 수백 년 앞서 고안된 개념이다.
   ⑤ 일반적으로 같은 양의 데이터를 암호화한 암호문(ciphertext)이 대칭키 암호(symmetric key cryptosystem) 보다 현저히 짧다.

6. 다음에서 설명하고 있는 기술은?

> "이것은 디지털 컨텐츠의 저작권을 보호하기 위한 기술로 DVD와 다운로드된 음원, 유료 소프트웨어 등에 적용된다. 이는 주로 컨텐츠의 불법적인 복제나 허가받지 않은 기기에서의 컨텐츠 소비를 방지한다."

   ① DRM
   ② IPS
   ③ GPL
   ④ VPN
   ⑤ DOM

7. 다음 중 공격자가 통신 프로토콜에 직접 개입하지 않고 감청(eavesdropping) 또는 감시(monitoring)만을 수행하는 수동적 공격(passive attack)으로 분류될 수 있는 것은?
   ① 가장(masquerade)
   ② 재사용(replay)
   ③ 서비스 거부(denial of service)
   ④ 메시지 변조(modification of message)
   ⑤ 트래픽 분석(traffic analysis)

8. 다음의 블록 암호 모드 중 각 평문 블록을 이전 암호문 블록과 XOR한 후 암호화되어 안전성을 높이는 모드는?
   ① ECB 모드
   ② CBC 모드
   ③ CTR 모드
   ④ OFB 모드
   ⑤ CFB 모드

9. PKI에 관한 다음의 설명 중 옳지 않은 것은?
   ① PKI란 public key infrastructure의 약어로 공개키 암호 알고리듬(Algorithm)을 적용하고 인증서를 관리하기 위한 기반시스템이다.
   ② 주로 X.509인증서를 사용하고 있다.
   ③ 인증서를 발급하는 역할을 하는 기관을 CA라 한다.
   ④ 인증서는 대상과 공개키를 묶어주는 역할을 하며 변조를 막기 위해 대상의 서명이 추가된다.
   ⑤ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

10. DES에 대한 다음의 설명 중 옳지 않은 것은?
   ① 1970년대에 표준화된 블록 암호 알고리듬(Algorithm)이다.
   ② 한 블록의 크기는 64비트이다.
   ③ 한번의 암호화를 위해 10라운드를 거친다.
   ④ 내부적으로는 56비트의 키를 사용한다.
   ⑤ Feistel 암호 방식을 따른다.

11. 방화벽(Firewall)에 대한 설명으로 옳지 않은 것은?
① 허가되지 않은 외부의 공격에 대비해 시스템을 보호하기 위한 하드웨어와 소프트웨어를 말한다.
② IP 필터링을 통하여 내부 네트워크로 들어오는 IP를 차단할 수 있다.
③ 방화벽을 구축해도 내부에서 일어나는 정보유출은 막을 수 없다.
④ 방화벽을 구축하면 침입자의 모든 공격을 완벽하게 대처할 수 있다.
⑤ 방화벽은 일반적으로 라우터 또는 컴퓨터가 된다.

12. 다음은 무엇에 대한 설명인가?

> "이것은 네트워크 상의 트랜잭션에 대한 상태 정보를 포함하는 일종의 토큰으로 주로 웹서버가 웹브라우저로 전송하여 클라이언트 쪽에 저장하고 나서 사용자가 해당 사이트를 재방문할 경우 웹브라우저가 웹서버에 재전송하는 형태로 많이 이용된다. 그러나 이는 원하지 않는 보안 상의 취약점을 야기할 수 있으므로 사용자가 이것을 주기적으로 삭제해 주는 것이 바람직하다."

① 애플릿(applet)
② URL(Uniform Resource Locator)
③ 공개키 인증서(public key certificate)
④ DOI(Digital Object Identifier)
⑤ 쿠키(Cookie)

13. 다음은 어떤 공격에 대한 설명인가?

> "웹사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로 사용자로 위장한 공격자가 웹사이트에 프로그램 코드를 삽입하여 나중에 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다."

① HTTP 세션 탈취(session hijacking)
② 피싱(phishing)
③ 클릭 탈취(click jacking)
④ 사이트 간 스크립팅(Cross-site scripting : XSS)
⑤ 파밍(pharming)

14. 다음 중 IPsec에 대한 설명으로 옳지 않은 것은?
① IPsec은 network layer에서 동작한다.
② Tunnel mode에서는 기존 패킷 앞에 IPsec 헤더 정보가 추가된다.
③ IKE 프로토콜은 SA를 협의하기 위해 사용된다.
④ AH 프로토콜은 메시지에 대한 인증과 무결성을 제공하기 위해 사용된다.
⑤ ESP 헤더는 메시지의 기밀성을 제공하기 위해 사용된다.

15. DDoS(Distributed Denial of Service)에 대한 설명으로 옳지 않은 것은?
① '좀비PC'가 되지 않기 위해서는 신뢰할 수 없는 기관의 프로그램은 설치하지 않는 것이 좋다.
② DDoS공격은 특정 서버에 침입하여 자료를 훔쳐가거나 위조시키기 위한 것이다.
③ '좀비PC'가 되면 자신도 모르게 특정사이트를 공격하는 수단으로 이용될 수 있다.
④ 공격을 당하는 서버에는 서비스가 중지될 수 있는 큰 문제가 발생한다.
⑤ '좀비PC'는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.

16. 다음의 접근 제어 모델 중 대상 기반의 접근 제어가 아니라 특정한 역할들을 정의하고 각 역할에 따라 접근 권한을 지정하고 제어하는 방식은?
① ACL ② DAC ③ RBAC
④ MAC ⑤ Capability

17. IDS에 관한 다음의 설명 중 옳지 않은 것은?
① IDS를 이용하면 공격 시도를 사전에 차단할 수 있다.
② 기존 공격의 패턴을 이용해 공격을 감지하기 위해 signature 기반 감지 방식을 사용한다.
③ 알려지지 않았지만 비정상적인 공격 행위를 감지해서 경고하기 위해 anomaly 기반 감지 방식을 사용한다.
④ DoS 공격, 패킷 조작 등의 공격을 감지하기 위해서는 network IDS를 사용한다.
⑤ IDS는 방화벽과 상호보완적으로 사용될 수 있다.

18. 다음 중 사용자 인증(user authentication)에 대한 설명으로 옳은 것은?
① 인터넷 뱅킹에 활용되는 OTP 단말(One Time Password Token)은 지식 기반 인증(authentication by what the entity knows)의 일종이다.
② 패스워드에 대한 사전 공격(dictionary attack)을 막기 위해 전통적으로 salt가 사용되어 왔다.
③ 통장 비밀번호로 흔히 사용되는 4자리 PIN(Personal Identification Number)은 소유 기반 인증(authentication by what the entity has)의 일종이다.
④ 지식 기반 인증(authentication by what the entity knows)의 가장 큰 문제는 오인식(False Acceptance), 오거부(False Rejection)가 존재한다는 것이다.
⑤ 건물 출입시 사용되는 ID 카드는 사람의 신체 또는 행위 특성을 활용하는 바이오 인식(biometric verification)의 일종이다.

19. 다음에서 설명하고 있는 공격은?

> "이 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어쓰는 방식이다. 만약 실행 코드가 덮어써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다."

① Buffer overflow 공격
② SQL injection 공격
③ IP spoofing 공격
④ Format String 공격
⑤ Privilege escalation 공격

20. 다음 중 개인정보 보호법에 대한 설명으로 맞는 것은?
① 개인정보 보호위원회의 위원은 대통령이 임명한다.
② 정보주체란 개인정보를 생성 및 처리하는 자를 의미한다.
③ 개인정보는 어떠한 경우에도 제3자에게 제공되거나 공유되어서는 안된다.
④ 개인정보의 처리 목적이 달성된 이후에는 개인정보를 1년간 보관하여야 한다.
⑤ 보호 대상이 되는 개인정보는 주민등록번호 등을 포함하여 생존 및 사망한 개인을 식별할 수 있는 정보를 의미한다.