2015-지방직-정보보호론-A형-해설-곽후근

1. 인터넷 보안 프로토콜에 해당하지 않는 것은 ?
① SSL
② HTTPS
③ S/MIME
④ TCSEC
정답 체크 :
(4) TCSEC : 1983년에 미국에서 제정되었고, 표지가 오렌지색이라 오렌지북이라 불린다. 보안등급은 크게는 A, B, C, D 4단계, 세부적으론 A1, B3, B2, B1, C2, C1, D 총 7단계로 나뉜다. 4가지 요구사항은 정책(Security Policy), 책임성(Accountability), 보증(Assurance), 문서(Documentation)이다. 정보보호 시스템의 평가 기준에 사용되며, TNI, TDI, CSSI 등 시스템 분류에 따라 적용 기준이 다르다.
오답 체크 :
(1) SSL : 웹 브라우저와 웹 서버 간에 데이터를 안전하게 주고받기 위한 업계 표준 프로토콜이다. 웹 제품뿐만 아니라 파일 전송 규약(FTP) 등 다른 TCP/IP 애플리케이션에 적용할 수 있다.
(2) HTTPS : HTTP의 보안이 강화된 버전이다(443 포트). HTTPS는 통신의 인증과 암호화를 위해 넷스케이프 커뮤니케이션즈 코퍼레이션이 개발했으며, 전자 상거래에서 널리 쓰인다.
(3) S/MIME : 안전한 전자메일 전송을 위한 산업체 표준 규약이다. 기존 MIME 형식의 전자메일 서비스에 암호 및 보안 서비스가 추가된 구조이다.

2. 데이터 소유자가 다른 사용자의 식별자에 기초하여 자신의 의지대로 데이터에 대한 접근 권한을 부여하는 것은?
① 강제적 접근 제어(MAC)
② 임의적 접근 제어(DAC)
③ 규칙 기반 접근 제어(Rule-based AC)
④ 역할 기반 접근 제어(RBAC)
정답 체크 :
(2) DAC : 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
오답 체크 :
(1) MAC : 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(3) Rule-based AC : 규칙에 기반한 접근 제어이다. 여기서 규칙이란 “어떤 데이터는 3:00부터 6:00까지만 접근이 허용된다“와 같은 것을 의미한다.
(4) RBAC : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.

3. 생체 인증 기법에 대한 설명으로 옳지 않은 것은?
① 정적인 신체적 특성 또는 동적인 행위적 특성을 이용할 수 있다.
② 인증 정보를 망각하거나 분실할 우려가 거의 없다.
③ 지식 기반이나 소유 기반의 인증 기법에 비해 일반적으로 인식 오류 발생 가능성이 매우 낮다.
④ 인증 시스템 구축 비용이 비교적 많이 든다.
정답 체크 :
(3) 인식 오류 : 계속 개선되고는 있으나 지식 기반이나 소유 기반에 비해 인식 오류 발생 가능성이 높다.
오답 체크 :
(1) 정적 또는 동적 : 정적은 신체적 특징을 의미하고 얼굴, 홍채, 정맥, 지문, 망막, 손모양 등을 들 수 있다. 동적은 행동적 특징을 나타내고 음성, 걸음걸이, 서명 등을 들 수 있다.
(2) 망각 또는 분실 : 열쇠나 비밀번호처럼 타인의 도용이나 복제에 의해 이용될 수 없을 뿐만 아니라, 변경되거나 분실한 위험성이 없어 보안 분야에서 많이 활용한다.
(4) 구축 비용 : 홍채 인식이나 정맥 인식은 시스템을 구축하는 비용이 고가이고, 다른 인식도 지식 기반이나 소지 기반에 비해 구축비용이 비교적 많이 든다.

4. 시스템 침투를 위한 일반적인 해킹 과정 중 마지막 순서에 해당 하는 것은?
① 공격
② 로그 기록 등의 흔적 삭제
③ 취약점 분석
④ 정보 수집
정답 체크 :
(2)
해킹 과정의 순서를 테이블로 정리하면 다음과 같다.

Foot Printing	가장 먼저 공격을 시도할 지역 혹은 사이트에 관한 정보를 수집하는 작업을 한다.
Scanning	스캐닝 작업은 공격을 시도할 표적들에 대해 진행 중인 서비스를 점검하는 단계다.
Enumeration	다음은 이전 단계를 통해 수집된 정보를 바탕으로 유효사용자 계정 수집 및 취약한 시스템의 자원공유를 정리 수집하는 단계라고 할 수 있다.
Gaining Access	다음 공격단계는 수집된 데이터를 통해 공격 목표에 접근을 시도해 접근권한을 취득하는 것이다.
Escalating Privilege	이 단계는 시스템 권한 상향을 조정하는 단계로 주로 Admin에 대한 정보 수집 및 탈취를 목적으로 하는 공격이다.
Pilfering	다음 단계는 서버의 접근 확보 후 신뢰된 시스템들에 대한 접근확보를 위해 필요한 정보 재수집 과정이다.
Covering Track	여기서는 공격 대상에 대한 제어 권한을 취득한 후 자취를 삭제하는 단계다.
Creating Backdoor	마지막 단계로 공격 대상에 대해서 후속침입이 용이하도록, 백도어(Backdoor)를 다양한 경로에 설치해 두는 일이다.

5. 공개키를 사용하는 전자 서명에 대한 설명으로 옳지 않은 것은?

① 송신자는 자신의 개인키로 서명하고 수신자는 송신자의 공개키로 서명을 검증한다.
② 메시지의 무결성과 기밀성을 보장한다.
③ 신뢰할 수 있는 제3자를 이용하면 부인봉쇄를 할 수 있다.
④ 메시지로부터 얻은 일정 크기의 해시 값을 서명에 이용할 수 있다.
정답 체크 :
(2) 무결성과 기밀성 : 무결성, 인증, 부인방지(봉쇄)는 보장하나 기밀성을 보장하지는 않는다. 기밀성을 보장하기 위해서는 별도의 암호화를 해야한다.
오답 체크 :
(1) 서명과 검증 : 송신자의 개인키로 서명하고 송신자의 공개키로 검증한다. 개인키 암호화라고도 한다.
(3) 제3자 : 신뢰할 수 있는 제3자(인증기관)를 이용하면 부인방지(봉쇄)를 할 수 있다.
(4) 해시 값 : 서명 시간을 단축하기 위해 메시지의 해시 값에 서명을 한다.

6. 침입탐지시스템(IDS)의 탐지 기법 중 하나인 비정상행위(anomaly) 탐지 기법의 설명으로 옳지 않은 것은?
① 이전에 알려지지 않은 방식의 공격도 탐지가 가능하다.
② 통계적 분석 방법, 예측 가능한 패턴 생성 방법, 신경망 모델을 이용하는 방법 등이 있다.
③ 새로운 공격 유형이 발견될 때마다 지속적으로 해당 시그니처(signature)를 갱신해 주어야 한다.
④ 정상행위를 가려내기 위한 명확한 기준을 설정하기 어렵다.
정답 체크 :
(3) 시그너처 : 시그너처는 비정상행위(anomaly)가 아니라 오용행위(misuse) 탐지 기법에 해당한다.
오답 체크 :
(1) 알려지지 않은 공격 : 초당 100개의 이상의 syn 패킷을 받지 않겠다고 하면 알려지지 않은 공격도 막을 수 있다.
(2) 방법 : 통계적 접근(과거의 통계 자료를 바탕으로 사용자의 행위를 관찰하여 프로파일을 작성하고 프로파일과 사용자 행위의 비교를 통해 비정상 정도를 측정), 예측 가능 패턴 생성(현재까지 발생한 사건들을 바탕으로 다음 사건을 예측), 신경망 방식(신경망을 이용하여 현재까지의 사용자의 행동이나 명령이 주어졌을 때 다음 행동이나 명령을 예측) 등이 존재한다.
(4) 명확한 기준 : 초당 100개의 이상의 syn 패킷을 받지 않겠다고 하면 정상 패킷도 막을 가능성이 존재한다. 즉, 명확한 기준을 잡기가 어렵다.

7. 보안 해시 함수가 가져야 하는 성질 중 하나인 강한 충돌 저항성(strong collision resistance)에 대한 설명으로 옳은 것은?
① 주어진 해시 값에 대해, 그 해시 값을 생성하는 입력 값을 찾는 것이 어렵다.
② 주어진 입력 값과 그 입력 값에 해당하는 해시 값에 대해, 동일한 해시 값을 생성하는 다른 입력 값을 찾는 것이 어렵다.
③ 같은 해시 값을 생성하는 임의의 서로 다른 두 개의 입력 값을 찾는 것이 어렵다.
④ 해시 함수의 출력은 의사 난수이어야 한다.
정답 체크 :
(3) 강한 충돌 저항성 : 해시 값이 일치할 것 같은, 다른 2개의 메시지를 발견해 내는 것이 매우 곤

란한 성질을 의미한다.
오답 체크 :
(1) 주어진 해시 값 : 해시 함수의 일방향성을 의미한다.
(2) 주어진 입력 값과 그 입력 값에 해당하는 해시 값 : 약한 충돌 저항성을 의미한다.
(4) 해시 함수 : 해시 함수를 이용하여 의사 난수를 만들 수 있다.

8. 전자서명법 상 공인인증기관이 발급하는 공인인증서에 포함되어야 하는 사항이 아닌 것은?
① 가입자의 전자서명검증정보
② 공인인증기관의 전자서명생성정보
③ 공인인증서의 유효기간
④ 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보
정답 체크 :
(2) 공인인증기관의 전자서명생성정보 : 개인키(전자서명생성정보)는 개인(공인인증기관)이 가지고 있어야 하는 것으로 공인인증서에 있으면 안 되는 정보이다.
오답 체크 :
(1), (3), (4)
"전자서명법" 제15조(공인인증서의 발급) 상 공인인증기관이 발급하는 공인인증서에는 다음 각호의 사항이 포함되어야 한다. 1. 가입자의 이름(법인의 경우에는 명칭을 말한다), 2. 가입자의 전자서명검증정보, 3. 가입자와 공인인증기관이 이용하는 전자서명 방식, 4. 공인인증서의 일련번호, 5. 공인인증서의 유효기간, 6. 공인인증기관의 명칭 등 공인인증기관임을 확인할 수 있는 정보, 7. 공인인증서의 이용범위 또는 용도를 제한하는 경우 이에 관한 사항, 8. 가입자가 제3자를 위한 대리권 등을 갖는 경우 또는 직업상 자격등의 표시를 요청한 경우 이에 관한 사항, 9. 공인인증서임을 나타내는 표시

9. 사용자 A와 B가 Diffie-Hellman 키 교환 알고리즘을 이용하여 비밀키를 공유하고자 한다. A는 3을, B는 2를 각각의 개인키로 선택하고, A는 B에게 21(= 7^3 mod 23)을, B는 A에게 3(= 7^2 mod 23)을 전송한다면, A와 B가 공유하게 되는 비밀키 값은? (단, 소수 23과 그 소수의 원시근 7을 사용한다)
① 4
② 5
③ 6
④ 7
정답 체크 :
(1)
Diffie-Hellman 키 교환 순서는 다음과 같다. 앨리스는 밥에게 2개의 소수 P와 한 원시근 G를 송신한다. 앨리스는 난수 A를 준비하고, 밥은 난수 B를 준비한다. 앨리스는 밥에게 G^A mod P라는 수를 송신하고, 밥은 앨리스에게 G^B mod P라는 수를 송신한다. 앨리스는 밥이 보낸 수를 A제곱해서 mod P를 계산한다 : 앨리스가 계산한 키 = $(G^B \bmod P)^A \bmod P = G^{B\times A} \bmod P$. 밥은 앨리스가 보낸 수를 B제곱해서 mod P를 계산한다 : 밥이 계산한 키 = $(G^A \bmod P)^B \bmod P = G^{A\times B} \bmod P$. 앨리스가 계산한 키와 밥이 계산한 키는 동일하게 이것이 비밀키가 된다.
위의 설명대로 2가지 방식으로 비밀키가 계산된다.

A의 비밀키 : $3^3 \bmod 23 = 27 \bmod 23 = 4$
B의 비밀키 : $21^2 \bmod 23 = 441 \bmod 23 = 4$
Tip! : 2가지 방식 중에 계산량이 작은 것으로 구하는 것이 좋다.

10. ISO 27001의 ISMS(Information Security Management System) 요구사항에 대한 내용으로 옳지 않은 것은?
① 자산 관리 : 정보 보호 관련 사건 및 취약점에 대한 대응
② 보안 정책 : 보안 정책, 지침, 절차의 문서화
③ 인력 자원 보안 : 인력의 고용 전, 고용 중, 고용 만료 후 단계별 보안의 중요성 강조
④ 준거성 : 조직이 준수해야 할 정보 보호의 법적 요소
정답 체크 :
(1) 자산 관리 : 해당 설명은 정보호보 사고관리를 나타내고, 자산 관리는 자산에 대한 책임과 정보 분류를 포함한다.
오답 체크 :
(2) 보안 정책 : 정보보호 정책의 문서화와 검토를 포함한다.
(3) 인력 자원 보안 : 고용 전, 고용 중, 고용의 종료 또는 변경을 포함한다.
(4) 준거성 : 법적 요구사항의 준수, 보안 정책과 표준 및 기술적 준수, 정보시스템 감사 고려사항을 포함한다.
ISO/IEC 27001을 하나의 표로 정리하면 다음과 같다.

통제분야	통제항목	통제분야	통제항목
1. 보안 정책	정보보호 정책	7. 접근 통제	접근통제를 위한 사업요건
2. 정보보호 조직	내부 조직		사용자 접근 관리
	외부자		사용자 책임
3. 자산관리	자산에 대한 책임		네트워크 접근 통제
	정보 분류		운영 시스템 접근 통제
4. 인적보안	고용 전		응용 및 정보 접근 통제
	고용 중		모바일 컴퓨팅과 원격근무
	고용의 종료 또는 변경	8. 정보시스템 획득, 개발 및 유지보수	정보시스템의 보안요건
5. 물리 및 환경 보안	물리적 출입통제		응용 내의 정확한 처리
	시설 및 방비 유지보수		암호 통제
6. 통신 및 운영 관리	운영절차와 책임		시스템 파일의 보안
	제3자 서비스 제공 관리		개발 및 지원 프로세스의 보호
	시스템 계획 및 인수		기술적 취약성 관리
	악성코드 및 모바일코드 보호	9. 정보보호 사고관리	정보보호 사고 및 약점의 보고
	백업		정보보호 사고 관리 및 개선
	네트워크 보안 관리	10. 사업지속성 관리	사업지속성관리의 정보보호 측면
	매체 관리	11. 준수	법적 요구사항의 준수
	정보의 교환		보안 정책과 표준 및 기술적 준수
	전자거래 서비스		정보시스템 감사 고려사항
	모니터링		

11. 서비스 거부 공격 방법이 아닌 것은?

① ARP spoofing

② Smurf

③ SYN flooding

④ UDP flooding

정답 체크 :

(1) ARP spoofing : 무결성 침해 공격이다. 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다.

오답 체크 :

(2) Smurf : 가용성 침해 공격이다. 희생자의 스푸핑된 원본 IP를 가진 수많은 인터넷 제어 메시지 프로토콜(ICMP) 패킷들이 IP 브로드캐스트 주소를 사용하여 컴퓨터 네트워크로 브로드캐스트하는 분산 서비스 거부 공격이다. 네트워크의 대부분의 장치들은 기본적으로 원본 IP 주소에 응답을 보냄으로써 이에 응답한다. 원본 IP 주소를 컴퓨터는 대량의 ICMP 패킷을 받게 되므로 서비스 거부 상태에 빠지게 된다.

(3) SYN flooding : 가용성 침해 공격이다. 클라이언트가 SYN 패킷을 보내고 서버는 이에 응답해서 SYN+ACK 패킷을 보낸다. 서버는 클라이언트가 ACK 패킷을 보내올 때까지 SYN Received 상태로 일정 시간을 기다려야 하고, 그동안 공격자는 가상의 클라이언트로 위조한 SYN 패킷을 수없이 만들어 서버에 보냄으로써 서버의 가용 동시 접속자 수를 모두 SYN Received 상태로 만들 수 있다.
(4) UDP flooding : 가용성 침해 공격이다. 대량의 UDP 패킷을 위조된 소스 주소와 함께 공격 대상 호스트의 임의의 포트로 전송한다. 호스트는 이러한 데이터그램과 연계된 애플리케이션을 점검하고 아무 것도 발견하지 못하곤 "도달할 수 없는 목적지(Destination Unreachable)" 패킷으로 응답한다. 공격자는 호스트가 압도당해 더 이상 합법적인 사용자에게 응답할 수 없을 때까지 더 많은 패킷을 보낸다.

12. MS 오피스와 같은 응용 프로그램의 문서 파일에 삽입되어 스크립트 형태의 실행 환경을 악용하는 악성 코드는?
① 애드웨어
② 트로이 목마
③ 백도어
④ 매크로 바이러스
정답 체크 :
(4) 매크로 바이러스 : 엑셀 또는 워드와 같은 문서 파일의 매크로 기능을 이용하기 때문에 워드나 엑셀 파일을 열 때 감염된다. 누구나 바이러스를 만들어 배포하는 계기가 되었다.
오답 체크 :
(1) 애드웨어 : 특정 소프트웨어를 실행할 때 또는 설치 후 자동적으로 광고가 표시되는 프로그램을 말한다. 프리웨어인 경우 불가피하게 광고 수익으로 운영되는 경우가 많으므로, 애드웨어라고 반드시 악성 소프트웨어에 속하는 것은 아니다.
(2) 트로이 목마 : 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.
(3) 백도어 : 운영체제나 프로그램을 생성할 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로로 트랩도어(Trapdoor) 혹은 Administrative hook이라고도 불린다.

13. 데이터베이스 보안의 요구사항이 아닌 것은?
① 데이터 무결성 보장
② 기밀 데이터 관리 및 보호
③ 추론 보장
④ 사용자 인증
정답 체크 :
(3) 추론 : 추론(inference)은 보통의 일반적인 데이터로부터 기밀 정보를 획득할 수 있는 가능성을 의미한다. 그러므로 데이터베이스에서는 추론을 방지하여야 한다.
오답 체크 :
(1) 무결성 : 데이터의 내용을 수정할 수 있는 인가되지 않은 접근, 저장 데이터를 손상시킬 수 있는 시스템의 오류, 고장 등으로부터 DB를 보호하여야 한다. 이러한 유형의 보호는 적절한 시스템 통제, 다양한 백업 및 복구 절차, 임시적인 보안 절차 등을 통하여 DBMS가 수행한다. 특히 시스템 고

장 시, DB는 더 이상 일관성을 유지하지 못할 수도 있다.
(2) 기밀 데이터 : 중요 데이터에 대한 기밀성을 보호(암호화)하고 인가된 사용자에 대해서만 접근을 허용해야 한다.
(4) 인증 : DBMS의 사용자 인증은 운영체제에서 수행하는 사용자 인증보다 더욱 엄격하여야 한다. 전형적으로 DBMS는 운영체제상의 응용 프로그램으로써 실행된다. 이는 운영체제와 DBMS 사이에 신뢰할 수 있는 경로(trusted path)가 없음을 의미한다. 따라서 DBMS는 사용자 인증을 포함한 각종 데이터를 운영체제로 부터 수신할 때, 신뢰할 수 있는지의 여부를 점검하여야 한다.

14. OSI 참조 모델의 제7계층의 트래픽을 감시하여 안전한 데이터만을 네트워크 중간에서 릴레이하는 유형의 방화벽은?
① 패킷 필터링(packet filtering) 방화벽
② 응용 계층 게이트웨이(application level gateway)
③ 스테이트풀 인스펙션(stateful inspection) 방화벽
④ 서킷 레벨 게이트웨이(circuit level gateway)
정답 체크 :
(2) 응용 계층 : 7계층에서 동작한다.
오답 체크 :
(1) 패킷 필터링 : 4계층에서 동작한다.
(3) 스테이트풀 인스펙션 : 여러 계층의 상태(스테이트)가 존재한다. 3계층에서는 IP 상태를 유지하고, 4계층에서는 TCP와 UDP의 상태를 유지한다. 그리고 7계층에서는 데이터의 상태를 유지한다(출제자가 의도한 상태는 아님). 동작 방식에서도 지문의 유형과 다르다(여러 개의 패킷을 모아서 문제가 없는지를 판단한다). 즉, 가장 맞는 답은 아니다.
(4) 서킷 레벨 게이트웨이 : 5계층에서 7계층 사이에서 동작한다.

15. IPSec에 대한 설명으로 옳지 않은 것은?
① 네트워크 계층에서 패킷에 대한 보안을 제공하기 위한 프로토콜이다.
② 인터넷을 통해 지점들을 안전하게 연결하는 데 이용될 수 있다.
③ 전송 모드와 터널 모드를 지원한다.
④ AH(Authentication Header)는 인증 부분과 암호화 부분 모두를 포함한다.
정답 체크 :
(4) AH : AH는 인증 부분을 포함하고, ESP가 암호화 부분을 포함한다.
오답 체크 :
(1) 네트워크 계층 : IP 계층을 보호하기 위해 OSI 3계층(network layer)에서 동작한다.
(2) 안전하게 연결 : VPN에서 사용된다.
(3) 모드 : 전송 모드(네트워크 계층 상위 계층인 전송, 응용 계층의 데이터에 대한 보호를 목적으로 하며, IP 패킷의 원본(payload)에 필드를 추가함으로서 구현)와 터널 모드(IP 헤더를 포함한 전체 IP 패킷에 대한 보호, 즉 네트워크, 전송, 응용 계층의 전체 데이터에 대한 보호를 목적)를 지원한다.

16. 커버로스(Kerberos)에 대한 설명으로 옳지 않은 것은?
① 네트워크 기반 인증 시스템으로 공개키 기반구조를 이용하여 사용자 인증을 수행한다.

② 인증 서버는 사용자를 인증하며 TGS(Ticket Granting Server)를 이용하기 위한 티켓을 제공한다.
③ TGS는 클라이언트가 서버로부터 서비스를 받을 수 있도록 티켓을 발급한다.
④ 인증 서버나 TGS로부터 받은 티켓은 클라이언트가 그 내용을 볼 수 없도록 암호화되어 있다.
정답 체크 :
(1) 사용자 인증 : 대칭키를 이용한 Authenticator(인증자)를 이용하여 사용자 인증을 수행한다. 커버로스 구조 안에서 공개키가 사용될 여지는 있지만 해당 지문은 가장 틀린 답에 해당된다.
오답 체크 :
(2) AS, TGS : AS는 사용자가 TGS에 사용하기 위한 TGT를 발급한다.
(3) TGS : TGS는 사용자가 서버에 사용하기 위한 Ticket을 발급한다.
(4) 암호화 : TGT는 AS와 TGS 사이의 비밀키로 암호화되어 있고, Ticket은 TGS와 서버 사이의 비밀키로 암호화되어 있어 사용자가 그 내용을 볼 수 없다.

17. 사용자 패스워드의 보안을 강화하기 위한 솔트(salt)에 대한 설명으로 옳지 않은 것은?
① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.
② 해시 연산 비용이 증가되어 오프라인 사전적 공격을 어렵게 한다.
③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.
④ 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.
정답 체크 :
(4) 암호화된 상태 : 시스템이 패스워드와 어떤 것을 합해 해시를 구한 것인지 알 수 없기 때문에 패스워드 파일에 저장 시 암호화를 하지 않고 간단한 인코딩을 통해 해시 결과 값 앞이나 뒤에 붙인다.
오답 체크 :
(1) 여러 사용자, 동일한 패스워드 : 동일한 패스워드에 다른 솔트를 사용하므로 서로 다르게 저장된다.
(2) 오프라인 사전적 공격 : 오프라인 사전적 공격이란 공격자가 시스템 비밀번호 파일을 얻어, 흔히 사용되는 비밀번호의 해시 값과 비교하는 것이다. 솔트를 사용하면 흔히 사용되는 비밀번호의 해시 값이 바뀌므로 공격을 어렵게 한다.
(3) 한 사용자, 동일한 패스워드 : 동일한 패스워드에 다른 솔트를 사용하므로 서로 다르게 저장된다.

18. 스택 버퍼오버플로(overflow) 공격에 대응하기 위한 방어 수단에 해당하지 않는 것은?
① 문자열 조작 루틴과 같은 불안전한 표준 라이브러리 루틴을 안전한 것으로 교체한다.
② 함수의 진입과 종료 코드를 조사하고 함수의 스택 프레임에 손상이 있는지를 검사한다.
③ 한 사용자가 프로그램에 제공한 입력이 다른 사용자에게 출력될 수 있도록 한다.
④ 매 실행 시마다 각 프로세스 안의 스택이 다른 곳에 위치하도록 한다.
정답 체크 :
(3) 입력과 출력 : 입력이 출력 버퍼의 크기를 초과하면 버퍼 오버플로우가 발생한다. 즉, 방어가 아니라 공격이 발생한다.
오답 체크 :
(1) 문자열 조작 루틴 : 예를 들면, strcpy(입력 문자열의 크기를 검사하지 않음)는 strncpy(입력

문자열의 크기를 검사함)로 교체해야 한다.
(2) 함수의 진입과 종료 코드 : 스택 가드(컴파일러가 프로그램의 함수 호출 시에 복귀 주소 앞에 canary(밀고자) 값을 주입하고, 종료 시에 canary 값 변조 여부 확인)와 스택 쉴드(함수 호출 시 복귀 주소를 특수 스택에 저장하고 함수 종료 시 특수 스택에 저장된 복귀 주소 값과 스택의 복귀 주소 값을 비교) 방법에 해당한다.
(4) 다른 곳에 위치 : ASLR(메모리 공격을 방어하기 위해 주소 공간배치를 난수화하는 기법) 방법에 해당된다.

19. 디지털 증거의 법적 효력을 인정받기 위해 포렌식 과정에서 지켜야 하는 원칙이 아닌 것은?
① 정당성의 원칙
② 무결성의 원칙
③ 재현의 원칙
④ 연계추적불가능의 원칙
정답 체크 :
(4) 연계추적불가능 : 연계추적불가능이 아니라 연계보관성이다. 연계보관성은 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.
오답 체크 :
(1) 정당성 : 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(2) 무결성 : 수집된 정보는 연계 보관성을 만족시켜야 하고, 각 단계를 거치는 과정에서 위조 및 변조되어서는 안 되며, 이러한 사항을 매번 확인해야 함을 의미한다.
(3) 재현 : 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 함을 의미한다.

20. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률에서 규정하고 있는 내용이 아닌 것은?
① 주요정보통신기반시설의 보호체계
② 정보통신망에서의 이용자 보호 등
③ 정보통신망의 안정성 확보 등
④ 개인정보의 보호
정답 체크 :
(1)
“정보통신기반 보호법”에서 규정하고 있는 내용은 주요정보통신기반시설의 보호체계, 주요정보통신기반시설의 지정 및 취약점 분석, 주요정보통신기반시설의 보호 및 침해사고의 대응, 기술지원 및 민간협력 등이다.
오답 체크 :
(2), (3), (4)
“정보통신망 이용촉진 및 정보보호 등에 관한 법률”에서 규정하고 있는 내용은 정보통신망의 이용촉진(기술 개발, 표준화), 전자문서중계자를 통한 전자문서의 활용, 개인정보의 보호(개인정보의 수집, 이용 동의), 정보통신망에서의 이용자 보호 정보통신망의 안정성 확보 등이다.