2015-국가직-정보보호론-사형-해설-곽후근

1. 다음에서 설명하는 공격방법은?

정보보안에서 사람의 심리적인 취약점을 악용하여 비밀 정보를 취득하거나 컴퓨터 접근권한 등을 얻으려고 하는 공격방법이다.

① 스푸핑 공격
② 사회공학적 공격
③ 세션 가로채기 공격
④ 사전 공격

정답 체크 :
(2) 사회공학적 : 컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여, 정상 보안 절차를 깨뜨리고 비기술적인 수단으로 정보를 얻는 행위이다. 실제로 조직 내에서 패스워드 점검 차원 등을 이유로 개인 패스워드를 물으면 상당수의 직원이 자신의 패스워드를 바로 알려주곤 한다.

오답 체크 :
(1) 스푸핑 : 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근 제어를 우회하는 공격 행위이다. 일례로, IP Spoofing 공격은 서버와 트러스트(Trust)로 관계를 맺고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다. IP Spoofing 이외에도 ARP, Port, Content(Payload), DNS Spoofing 등이 존재한다.
(3) 세션 가로채기 : TCP는 클라이언트와 서버간 통신을 할 때 패킷의 연속성을 보장하기 위해 클라이언트와 서버는 각각 시퀀스 넘버를 사용한다. 이 시퀀스 넘버가 잘못되면 이를 바로 잡기 위한 작업을 하는데, 세션 하이재킹은 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 위조해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어들어가는 방식이다.
(4) 사전 : 사전(dictionary file)에 있는 단어를 입력하여 암호를 알아내거나 해독하는 컴퓨터 공격법이다. 암호를 알아내기 위한 공격은 사전의 단어를 순차적으로 입력하는 것이다. 단어를 그대로 입력할 뿐 아니라, 대문자와 소문자를 뒤섞기도 하고, 단어에 숫자를 첨부하기도 하는 등의 처리도 병행하면서 공격을 할 수 있다. 사전 파일의 퀄리티에 따라 공격 성공 여부가 결정된다.

2. 능동적 보안 공격에 해당하는 것만을 모두 고른 것은?

ㄱ. 도청 ㄴ. 감시 ㄷ. 신분위장 ㄹ. 서비스 거부

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

정답 체크 :
(4)
(ㄷ) 신분위장 : 무결성(능동적/적극적/active)

(ㄹ) 서비스 거부 : 가용성(능동적/적극적/active)
오답 체크 :
(1), (2), (3)
(ㄱ), (ㄴ) 도청, 감시 : 기밀성(수동적/소극적/passive)

3. 다음에서 설명하는 재해복구시스템의 복구 방식은?

재해복구센터에 주 센터와 동일한 수준의 시스템을 대기 상태로 두어, 동기적 또는 비동기적 방식으로 실시간 복제를 통하여 최신의 데이터 상태를 유지하고 있다가, 재해 시 재해복구센터의 시스템을 활성화 상태로 전환하여 복구하는 방식이다.

① 핫 사이트(Hot Site)
② 미러 사이트(Mirror Site)
③ 웜 사이트(Warm Site)
④ 콜드 사이트(Cold Site)
정답 체크 :
(1) 핫 : 주 전산센터와 동일한 하드웨어, 소프트웨어 및 기타 부대 장비 등을 갖추어 놓고 관리되며, 이론적으로는 직원이나 운영자가 도보로 이동하여 최근 백업본으로부터 리스토어하여 매우 짧은 시간 안에 전체 운영을 시작하는 것이다. 즉, 사람이 없다.
오답 체크 :
(2) 미러 : 주 전산센터와 동일한 백업 센터를 두어 평시에 실시간으로 데이터를 백업하여 주 전산센터에 재해가 발생하면 즉시 업무를 대행하게 하는 백업 체제이다. 즉, 모든 게 다 갖춰져 있다.
(3) 웜 : Hot Site와 Cold Site의 절충안으로, Hot Site와 같이 전원이나 HVAC(Heating, Ventilation, Air Conditioning), 컴퓨터 등이 갖추어진 컴퓨터 설비를 구축하지만, 애플리케이션은 설치되거나 구성되어 있지 않다. 즉, 사람과 소프트웨어가 없다.
(4) 콜드 : 비상시 장비를 가져올 준비만 할 뿐 어떤 컴퓨터 하드웨어도 사이트에 존재하지 않는다. Cold Site는 전원과 HVAC는 설치되어 있고, 비상 사태 발생 시, 컴퓨터를 이동하여 복구 작업을 수행해야 한다. 즉, 사람과 소프트웨어, 하드웨어가 없다.

4. 정보보안의 기본 개념에 대한 설명으로 옳지 않은 것은?
① Kerckhoff의 원리에 따라 암호 알고리즘은 비공개로 할 필요가 없다.
② 보안의 세 가지 주요 목표에는 기밀성, 무결성, 가용성이 있다.
③ 대칭키 암호 알고리즘은 송수신자 간의 비밀키를 공유하지 않아도 된다.
④ 가용성은 인가된 사용자에게 서비스가 잘 제공되도록 보장하는 것이다.
정답 체크 :
(3) 대칭키 : 암호화키(비밀키, 비공개)와 복호화키(비밀키, 비공개)가 동일한 암호를 의미한다. 속도가 빠르나 키 배송 문제가 있다. 즉, 송수신자 간의 비밀키를 공유해야 한다.
오답 체크 :
(1) Kerckhoff : 커크호프는 암호 시스템의 안전성에 대해 "키 이외에 암호 시스템의 모든 것이 공개되어도 안전해야 한다"고 했다. 즉, 암호 분야에서는 어떤 암호 알고리즘이 많은 암호학자들에 의해 장기간 세부적으로 수행된 분석에서도 잘 견디어낼 때까지는 그 알고리즘을 안전하다고 인정하지 않는다.
(2) 세 가지 주요 목표 : 3가지 주요 목표에는 CIA(기밀성(비밀성), 무결성, 가용성)이 포함되고, 나

머지 목표에는 인증, 부인방지, 책임추적성, 신뢰성 등이 포함된다.
(4) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.

5. 공개키 기반 구조(PKI : Public Key Infrastructure)의 인증서에 대한 설명으로 옳은 것만을 모두 고른 것은?

ㄱ. 인증기관은 인증서 및 인증서 취소목록 등을 관리한다.
ㄴ. 인증기관이 발행한 인증서는 공개키와 공개키의 소유자를 공식적으로 연결해 준다.
ㄷ. 인증서에는 소유자 정보, 공개키, 개인키, 발행일, 유효 기간 등의 정보가 담겨 있다.
ㄹ. 공인인증서는 인증기관의 전자서명 없이 사용자의 전자 서명만으로 공개키를 공증한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
정답 체크 :
(1)
(ㄱ) 인증서 및 인증서 취소목록 : 인증기관(CA)는 인증서의 관리를 행하는 기관으로 키 쌍을 작성하거나 공개키 등록 때 본인을 인증한다. 그리고 인증서를 작성해서 발행하고 인증서를 폐지한다.
(ㄴ) 공개키와 공개키의 소유자를 연결 : 공개키 이용자가 해당 공개키를 기반으로 메시지를 암호화해서 공개키 소유자에 보내면, 공개키 소유자는 자신의 개인키로 암호화된 메시지를 복호화한다.
오답 체크 :
(2), (3), (4)
(ㄷ) 개인키 : 개인키는 공개키로 암호화된 메시지를 복호화하기 위해 개인이 사용하는 것으로 절대 인증서에 있으면 안되는 정보이다.
(ㄹ) 공증 : 공증은 신뢰할 만한 사람이나 기관이 해야 하는 것으로 사용자의 전자서명은 신뢰할 수 없다. 그러므로 인증기관의 전자서명이 필요하다.

6. 위험 분석에 대한 설명으로 옳지 않은 것은?
① 자산의 식별된 위험을 처리하는 방안으로는 위험 수용, 위험 회피, 위험 전가 등이 있다.
② 자산의 가치 평가를 위해 자산구입비용, 자산유지보수비용 등을 고려할 수 있다.
③ 자산의 적절한 보호를 위해 소유자와 책임소재를 지정함으로써 자산의 책임추적성을 보장받을 수 있다.
④ 자산의 가치 평가 범위에 데이터베이스, 계약서, 시스템 유지 보수 인력 등은 제외된다.
정답 체크 :
(4) 데이터베이스, 계약서, 시스템 유지 보수 인력 : 자산은 유형/무형의 자산 모두를 포함한다(아래의 테이블 참조).
오답 체크 :
(1) 위험 처리 방안 : 위험 수용(위험의 잠재 손실 비용을 감수하는 것), 위험 감소(위험을 감소시킬 대책을 마련하는 것), 위험 회피(위험이 존재하는 사업, 프로세스를 진행하지 않는 것), 위험 전가(보험이나 외주 등으로 잠재적 위험을 제 3자에게 전가하는 방법)가 있다.
(2) 가치 평가 : 자산구입비용은 당연히 필요한 것이고, 유지보수로 인해 해당 자산의 경제적 효익이

증가했다면(에를 들어, 새로운 PC 설치 혹은 프로젝터 수리) 자산에 포함한다.
(3) 소유자와 책임소재를 지정 : 자산의 관리 정책 수립 과정에서 자산 관리를 위한 “책임자/소유자의 역할 정의 및 권한 부여”를 수행한다.

7. 메시지 인증 코드(MAC : Message Authentication Code)를 이용한 메시지 인증 방법에 대한 설명으로 옳지 않은 것은?
① 메시지의 출처를 확신할 수 있다.
② 메시지와 비밀키를 입력받아 메시지 인증 코드를 생성한다.
③ 메시지의 무결성을 증명할 수 있다.
④ 메시지의 복제 여부를 판별할 수 있다.
오답 체크 :
(4) 복제 여부 : 복제 여부는 워터마킹이나 핑거프린팅 등으로 알 수 있다.
정답 체크 :
(1) 출처 : 메시지 인증 코드는 비밀키를 이용하므로 메시지의 출처(인증)를 알 수 있다. (해당 비밀키는 상대방만 가지고 있다)
(2) 비밀키 : 메시지 인증 코드에는 비밀키가 필요하다(해시와의 차이점).
(3) 무결성 : 메시지 인증 코드는 수신자가 MAC 값을 비교하므로 통신 중 내용 변경 유무(무결성)를 알 수 있다.

8. 유닉스(Unix)의 로그 파일과 기록되는 내용을 바르게 연결한 것은?

ㄱ. history – 명령창에 실행했던 명령 내역
ㄴ. sulog – su 명령어 사용 내역
ㄷ. xferlog – 실패한 로그인 시도 내역
ㄹ. loginlog – FTP 파일 전송 내역

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ
정답 체크 :
(1)
(ㄱ) history : 유닉스에서는 실행 명령에 대한 기록이 .sh_history, .csh_history, .bash_history 같이 ‘[셸의 종류]_history 파일’형식으로 각 계정의 홈 디렉터리에 저장된다.
(ㄴ) sulog : su(switch user)는 권한 변경에 대한 로그이다.
오답 체크 :
(2), (3), (4)
(ㄷ) xferlog : FTP 파일 전송 내역이다.
(ㄹ) loginlog : 실패한 로그인 시도 내역이다.

9. 전송계층 보안 프로토콜인 TLS(Transport Layer Security)가 제공하는 보안 서비스에 해당하지 않는 것은?
① 메시지 부인 방지

② 클라이언트와 서버 간의 상호 인증
③ 메시지 무결성
④ 메시지 기밀성
정답 체크 :
(1) 부인 방지 : TLS에 기밀성, 무결성, 인증 기능은 있지만 부인 방지 기능은 없다.
오답 체크 :
(2) 인증 : 인증서(공개키에 디지털 서명을 붙임)를 상호 교환하여 상호 인증을 수행한다.
(3) 무결성 : 메시지 인증 코드를 이용한다. 메시지 인증 코드는 일방향 해시 함수를 이용한다.
(4) 기밀성 : 대칭키 암호를 이용한다. 대칭키는 의사난수 생성기를 이용하고 비밀키의 공유는 공개키 암호 또는 Diffie-Hellman 키 교환을 이용한다.

10. 다음에서 설명하는 스니퍼 탐지 방법에 이용되는 것은?

○ 스니핑 공격을 하는 공격자의 주요 목적은 사용자 ID와 패스워드의 획득에 있다. ○ 보안 관리자는 이점을 이용해 가짜 ID와 패스워드를 네트워크에 계속 보내고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지한다.

① ARP
② DNS
③ Decoy
④ ARP watch
정답 체크 :
(3) Decoy : 스니핑 공격을 하는 공격자의 주요 목적은 ID와 패스워드의 획득에 있다. 가짜 ID와 패스워드를 네트워크에 계속 뿌리고, 공격자가 이 ID와 패스워드를 이용하여 접속을 시도할 때 스니퍼를 탐지한다(유인).
오답 체크 :
(1) ARP : 위조된 ARP Request를 보냈을 때 ARP Response가 오면 프러미스큐어스 모드(스니핑 모드)로 설정되어 있는 것이다.
(2) DNS : 일반적으로 스니핑 프로그램은 사용자의 편의를 위해, 스니핑한 시스템의 IP 주소에 DNS에 대한 이름 해석 과정(Inverse-DNS lookup)을 수행이다(로깅). 테스트 대상 네트워크로 Ping Sweep(여러 대상에 대한 연속적인 ping)을 보내고, 들어오는 Inverse-DNS lookup을 감시하여 스니퍼를 탐지한다.
(4) ARP watch : MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여, 이를 변하게 하는 패킷이 탐지되면 관리자(network administrator)에게 메일로 알려주는 툴이다.

11. 다음에 제시된 〈보기 1〉의 사용자 인증방법과 〈보기 2〉의 사용자 인증도구를 바르게 연결한 것은?

〈보기 1〉 ㄱ. 지식 기반 인증 ㄴ. 소지 기반 인증 ㄷ. 생체 기반 인증

〈보기 2〉
A. OTP 토큰
B. 패스워드
C. 홍채

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	A	C
④	B	C	A

정답 체크 :
(3)
(ㄱ) 지식 기반 인증 : 패스워드, PIN(Personal Identification Number) 등
(ㄴ) 소지 기반 인증 : 스마트 키, 스마트 카드, 신분증, 인터넷 뱅킹 카드와 OTP(One Time Password), 공인 인증서 등
(ㄷ) 생체 기반 인증 : 지문, 손 모양, 망막, 홍채, 서명, 키보드, 목소리, 얼굴 등

12. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 용어의 정의에 대한 설명으로 옳지 않은 것은?
① 정보통신서비스 : 전기통신사업법 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것
② 정보통신망 : 전기통신사업법 제2조제2호에 따른 전기통신 설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용 기술을 활용하여 정보를 수집·가공·저 장·검색·송신 또는 수신하는 정보통신체제
③ 통신과금서비스이용자 : 정보보호제품을 개발·생산 또는 유통하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람
④ 침해사고: 해킹, 컴퓨터바이러스, 논리 폭탄, 메일 폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태
정답 체크 :
(3)
통신과금서비스이용자 : 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입·이용하는 자
정보보호산업(“정보보호산업의 진흥에 관한 법률”) : 정보보호를 위한 기술(이하 "정보보호기술"이라 한다) 및 정보보호기술이 적용된 제품(이하 "정보보호제품"이라 한다)을 개발·생산 또는 유통하거나 이에 관련한 서비스(이하 "정보보호서비스"라 한다)를 제공하는 산업

13. 안드로이드 보안에 대한 설명으로 옳지 않은 것은?
① 리눅스 운영체제와 유사한 보안 취약점을 갖는다.
② 개방형 운영체제로서의 보안정책을 적용한다.
③ 응용 프로그램에 대한 서명은 개발자가 한다.
④ 응용 프로그램 간 데이터 통신을 엄격하게 통제한다.
오답 체크 :

(4) 엄격 통제 : 애플이 응용프로그램 간 데이터 통신을 엄격하게 통제하고 안드로이드는 상대적으로 응용프로그램 간 통신과 데이터 전달이 자유롭다.
정답 체크 :
(1) 보안 취약점 : 안드로이드는 리눅스를 기반으로 하기 때문에 리눅스 운영체제와 유사한 보안 취약점을 갖는다.
(2) 보안정책 : 사용자의 선택에 따라 보안 수준을 선택할 수 있다.
(3) 서명 : 안드로이드는 개발자가 서명하고 iOS는 애플이 서명한다.

14. 개인정보 보호인증(PIPL) 제도에 대한 설명으로 옳은 것은?
① 물리적 안전성 확보조치 심사 영역에는 악성 소프트웨어 통제 심사 항목이 있다.
② 인증절차는 인증심사 준비 단계, 심사 단계, 인증 단계로 구성되며, 인증유지관리를 위한 유지관리 단계가 있다.
③ 개인정보 보호를 위해 관리계획수립과 조직 구축은 정보주체 권리보장 심사 영역에 속한다.
④ 인증을 신청할 수 있는 기관은 공공기관에 한정한다.
정답 체크 :
(2) 인증절차 : 준비, 심사, 인증 단계로 구성된다.
오답 체크 :
(1) 물리적 안전성 확보조치 : CCTV의 설치 및 운영에 대한 보호조치 및 물리적 출입통제 등에 대한 보호조치 사항을 정한다.
(3) 정보주체 권리보장 : 정보주체의 권리보장을 위함 열람·정정·삭제, 처리정지 등의 요구에 대한 법적 요구사항 및 보호조치 사항을 정한다.
(4) 인증 신청 : 신청은 공공기관, 대기업, 중소기업, 소상공인 등이 할 수 있다.

15. 해킹에 대한 설명으로 옳지 않은 것은?
① SYN Flooding은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.
② Zero Day 공격은 시그니처(signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.
③ APT는 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.
④ Buffer Overflow는 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.
정답 체크 :
(2) Zero Day : 프로그램에 문제가 알려지고 난 후 보안패치가 나올 때까지 시간차를 이용해 공격하는 기법을 말한다. 알려지지 않은 공격이므로 보안 장비로 막을 수 없으나 IDS를 이용하고자 한다면 시그너처 기반의 오용 탐지가 아니라 이상 탐지로 방어를 해야 한다.
오답 체크 :
(1) SYN Flooding : 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.
(3) APT : 특정 기업 또는 기관의 핵심 정보통신 설비에 대한 중단 또는 핵심정보의 획득을 목적으로 공격자는 장기간 동안 공격 대상에 대해 IT인프라, 업무환경, 임직원 정보 등 다양한 정보를 수집하고, 이를 바탕으로 제로 데이 공격, 사회공학적 기법 등을 이용하여 공격 대상이 보유한 취약점을 수집·악용해 공격을 실행하는 것을 말한다.

(4) Buffer Overflow : 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다.

16. 다음에서 설명하는 웹 서비스 공격은?

공격자가 사용자의 명령어나 질의어에 특정한 코드를 삽입하여 DB 인증을 우회하거나 데이터를 조작한다.

① 직접 객체 참조
② Cross Site Request Forgery
③ Cross Site Scripting
④ SQL Injection
해설)
정답 체크 :
(4) SQL Injection : 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.
오답 체크 :
(1) 직접 객체 참조 : 파일, 디렉터리, 데이터베이스 키와 같이 내부적으로 구현된 객체에 대한 참조가 노출될 때 발생한다. 예를 들어, 디렉토리 탐색, 파일 업로드 제한 부재, 리버스 텔넷 등이 있다.
(2) CSRF : 웹 사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹 사이트에 요청하게 하는 공격이다. 즉, 일단 사용자가 웹 사이트에 로그인한 상태에서 CSRF 공격 코드가 삽입된 페이지를 열면, 이후에는 사용자의 행동과 관계없이 사용자의 웹 브라우저와 공격 대상 웹 사이트 간의 상호 작용이 이루어진다.
(3) XSS : 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다.

17. 사용자와 인증 서버 간 대칭키 암호를 이용한 시도-응답(Challenge-Response) 인증방식에 대한 설명으로 옳지 않은 것은?
① 재전송 공격으로부터 안전하게 사용자를 인증하는 기법이다.
② 인증 서버는 사용자 인증을 위해 사용자의 비밀키를 가지고 있다.
③ 사용자 시간과 인증 서버의 시간이 반드시 동기화되어야 한다.
④ Response 값은 사용자의 비밀키를 사용하여 인증 서버에서 전달받은 Challenge 값을 암호화한 값이다.
정답 체크 :
(3) 동기화 : 해당 방식은 타임스탬프 방식이 아니기 때문에 반드시 동기화되어야 할 필요가 없다.
오답 체크 :

(1) 재전송 공격 : 재전송은 보존해 준 정당한 값을 다시 송신하는 공격이므로 시도-응답 인증방식을 이용하면 재전송 공격을 막을 수 있다.
(2) 인증 서버 : 사용자가 암호화한 Challenge값을 복호화해야 하기 때문에 비밀키를 가지고 있어야 한다.
(4) 비밀키 : 사용자는 인증 서버로부터 받은 Challenge(난수)값을 암호화하여 Response값을 만든다.

18. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?
① 국가 마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.
② 보호프로파일(Protection Profiles)은 특정 제품이나 시스템에만 종속되어 적용하는 보안기능 수단과 보증 수단을 기술한 문서이다.
③ 평가보증등급(EAL : Evaluation Assurance Level)에서 가장 엄격한 보증(formally verified) 등급은 EAL7이다.
④ 보안 요구조건을 명세화하고 평가기준을 정의하기 위한 ISO/IEC 15408 표준이다.
정답 체크 :
(2) 보호 프로파일 : 사용자 또는 개발자의 요구사항을 정의한다. 특정 제품이나 시스템에만 종속되지 않는다.
오답 체크 :
(1) 평가기준 : 국제 표준화 기구(ISO)와 국제 전기 표준 회의(IEC)가 정한 최초의 정보 기술 보안에 관한 국제 표준이다.
(3) EAL : 7개의 보증 등급을 가진다. 보증 등급은 기능 시험(EAL-1), 구조 시험(EAL-2), 방법론적 시험과 점검(EAL-3), 방법론적 설계, 시험, 검토(EAL-4), 준정형적 설계 및 시험(EAL-5), 준정형적 검증된 설계 및 시험(EAL-6), 정형적 검증(EAL-7)로 나눠진다.
(4) ISO/IEC 15408 : 정보 보호 제품의 평가 기준을 규정한 국제 표준(ISO 15408). 공통평가기준(CC)은 선진 각국들이 정보 보호 제품에 서로 다른 평가 기준을 가지고 평가를 시행하여 시간과 비용 낭비 등이 초래되는 문제점을 없애기 위해 개발되었다.

19. 개인정보보호법 상 주민등록번호 처리에 대한 설명으로 옳지 않은 것은?
① 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인인 개인정보처리자는 개인정보보호위원회의 심의·의결을 거쳐 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.
② 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 유출된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 주민등록번호가 유출되지 아니하도록 개인정보처리자가 개인정보보호법에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주 민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여 야 한다.
④ 개인정보처리자는 주민등록번호가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.
정답 체크 :
(1)

“개인정보 보호법” 제24조의2(주민등록번호 처리의 제한) 상 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다. 1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우, 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우, 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우

20. 다음에서 설명하는 윈도우 인증 구성요소는?

○ 사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다. ○ SID에 기반을 두어 파일이나 디렉터리에 대한 접근의 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① LSA(Local Security Authority)
② SRM(Security Reference Monitor)
③ SAM(Security Account Manager)
④ IPSec(IP Security)

정답 체크 :
(2) SRM : SAM이 사용자의 계정과 패스워드 일치 여부를 확인하여 알리면 사용자에게 SID(Security Identifier) 부여, SID에 기반하여 파일이나 디렉터리에 대한 접근(access) 허용 여부 결정하고, 이에 대한 감사(audit) 메시지 생성한다.

오답 체크 :
(1) LSA : 모든 계정의 로그인에 대한 검증, 시스템 자원 및 파일 등에 대한 접근 권한 검사한다. 로컬, 원격 모두에 해당, 이름과 SID를 매칭하며, SRM이 생성한 감사(audit) 로그를 기록한다.
(3) SAM : 사용자/그룹 계정 정보에 대한 데이터베이스 관리, 사용자의 로그인 입력 정보와 SAM 데이터베이스 정보를 비교해 인증 여부 결정한다. 윈도우에서 패스워드 암호화하여 보관하는 파일의 이름과 동일하다.
(4) IPSec : 네트워크 계층(network layer)으로 ip 계층을 보호하기 위한 프로토콜이다.