2015년 국가직 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
②	④	①	③	①	④	④	①	①	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
③	③	④	②	②	④	③	②	①	②

문 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

답 ②

② 사회공학적 공격은 기술적인 방법이 아닌 사람들간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법을 일컫는다.
① 스푸핑(spoofing)공격은 네트워크 상에서 자신의 신분을 속이거나 다른 사용자로 위장해 공격 대상에 불법 접근하여 정보를 빼내는 것이다.
③ 세션 하이재킹(Session Hijacking) 공격은 시스템에 접근할 적법한 사용자 아이디와 패스워드를 모를 때, 이미 시스템에 접속되어 세션이 연결되어 있는 사용자의 세션을 가로채는 공격이다.
④ 사전 공격(Dictionary Attack)은 패스워드로 사용할 만한 문자열을 사전으로 만들어놓고 이를 하나씩 대입하여 일치 여부를 확인하는 방법이다

문 2. 능동적 보안 공격에 해당하는 것만을 모두 고른 것은?

> ㄱ. 도청 ㄴ. 감시
> ㄷ. 신분위장 ㄹ. 서비스 거부

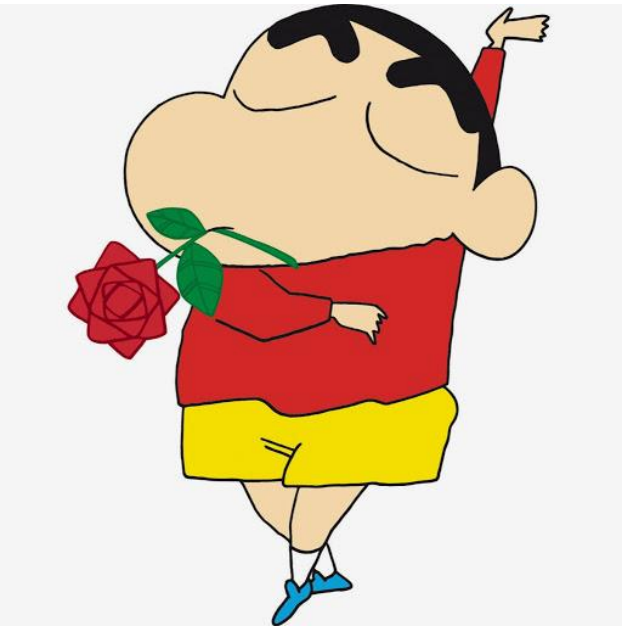
① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

답 ④

ㄷ 신분위장, ㄹ 서비스 거부 -> 적극적(능동적) 공격
ㄱ 도청 ㄴ 감시 -> 소극적(수동적) 공격

소극적 공격(수동적 공격)
- 도청(가로채기, interception)
- 트래픽 분석(traffic analysis)
- 메시지 내용 공개(release of message contents) 등

적극적 공격(능동적 공격)
- 차단(interruption)
- 변조(modification)
- 위조(fabrication)
- 신분 위장(masquerade)
- 서비스 거부 공격(Dos)
- 재전송 공격(replay attack) 등



문 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)

답 ①

① 주 센터와 동일한 수준을 유지하되, 평상시엔 대기 상태로 두는 것은 핫 사이트이다.
미러 사이트는 평상시에도 주 센터와 동시에 운영하는 방식이다.

재해복구시스템(DRS, Disaster Recovery System)은 데이터센터 등 기업 IT 인프라에 장애가 발생하여 제 기능을 수행하지 못하게 됐을 때, 이를 대체하거나 복구해 제 기능을 수행할 수 있도록 기능하는 시스템을 말한다.

- Mirror Site(미러 사이트)
  원본 시스템과 동일한 데이터를 실시간으로 처리하여 **동시에 운영**되는 백업 사이트이다
- Hot Site(핫 사이트)
  원본 시스템과 동일한 장비와 데이터를 갖춘 백업 사이트지만, 평소엔 운영하지 않는다. 원본 시스템과 항상 동일한 데이터를 유지하기 때문에 백업은 실시간
- Warm Site(웜 사이트)
  핫 사이트와 콜드 사이트의 중간 단계로, 원본 시스템의 장비 일부를 백업 사이트에 설치하여 주요 업무에 대한 복구를 지원한다.
  하드웨어가 이미 연결이 되어 있으며, 직접 백업본을 갖출 수 있으나 완전하지 못할 수도 있다.
- Cold Site(콜드 사이트)
  평소에는 시스템을 사용할 수 있는 전기, 통신, 온도조절 시스템만 갖춰놓은 상태로, 재해 발생시 하드웨어와 소프트웨어를 설치하여 가동한다.
  백업 사이트 가운데 가장 값이 저렴하며, 데이터와 정보의 백업된 복사본을 거의 보유하고 있지 않다.

문 4. 정보보안의 기본 개념에 대한 설명으로 옳지 않은 것은?

① Kerckhoff 의 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.

답 ③

③ 대칭키 암호 알고리즘은 송수신자가 같은 키를 사용하는 방식으로, 비밀키를 공유해야 한다.
① 케르크호프스(Kerckhoff)의 원리는 키를 제외한 시스템의 다른 모든 내용이 알려지더라도 암호체계는 안전해야 한다는 것이다. 이 말을 클로드 섀넌(Claude Elwood Shannon)은 "적은 시스템을 알고 있다(The enemy knows the system)"라는 말로 표현했는데, 암호체계는 그 시스템이 적에게 파악되는 것을 가정하고 설계해야 한다는 말이다.
따라서 암호체계의 안전성은 오로지 키의 비밀성에만 의존해야 하며, 정보를 코딩하고 전송하는 방법이 모든 사람에게 알려지더라도 암호화 방식은 안전해야 한다는 얘기다.

문 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

답 ①

ㄱ. Certification Authority(CA, 인증기관)은 공개키 인증서와 인증서 폐기목록을 생성하고 발급한다.
ㄴ. 인증서는 해당 공개키가 위·변조되지 않았다는 사실을 인증해주는 것이다. 따라서 공개키와 그 소유자를 공식적으로 연결해준다고 할 수 있다.

ㄷ. 개인키는 사용자 본인만 가지고 있어야 한다. 따라서 인증서에는 개인키가 포함되지 않는다.
ㄹ. 인증서에는 인증기관의 서명이 첨부되어 있다. 인증서 이용자는 인증기관의 공개키로 이 서명을 검증하여, 인증서가 위·변조되지 않았다는 것을 확인할 수 있다.

문 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 유지보수 인력 등은 제외된다.

답 ④

④ 자산의 가치 평가 범위에는 유형 자산뿐 아니라, 데이터베이스, 계약서 등 무형 자산과 인력도 포함된다.

문 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.

답 ④

메시지 인증 코드(MAC: Message Authentication Code)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(송신자에 대한 인증)이 가능하다.

④ 메시지의 복제 여부는 확인할 수 없다.

① MAC 로 메시지의 출처 확인(송신지 인증)이 가능하다.
송신자 인증과 부인 방지는 다른 것이다.
송신자 인증(출처 인증)은 통신 당사자간 상대방의 신원을 확인할 수 있는 것을 의미한다. MAC 는 대칭키를 사용하기 때문에 네트워크 상의 상대방이 자신과 같은 비밀키를 가진 특정인이라는 걸 확인할 수 있다. 제 3 자에게 누가 송신자인지 증명할 수는 없다.
부인 방지는 제 3 자에게 누가 어떤 내용의 메시지를 보냈는지, 메시지의 전송 및 수신에 대한 사실 확인이 가능한 것을 의미한다.

문 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

답 ①

ㄷ과 ㄹ의 내용이 바뀌었다.
ㄷ. xferlog: FTP 파일 전송 내역을 기록
ㄹ. loginlog: 로그인할 때 5 번 이상 실패할 경우의 기록

문 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

답 ①

① SSL/TLS 는 암호화에 대칭키를 사용하기 때문에 부인 방지 서비스는 제공하지 못한다.

SSL(Secure Sockets Layer, 보안 소켓 레이어) 또는
TLS(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 데이터 무결성을 제공하는 보안 프로토콜
클라이언트와 서버 간 상호 인증과 기밀성과 무결성 서비스를 제공

※ SSL/TLS 암호화 알고리즘
- 키교환 알고리즘: RSA, Diffie-Hellman, ECDH, SRP, PSK
- 인증 알고리즘: RSA, DSA, ECDSA
- 대칭키 암호 알고리즘: RC4, 트리플 DES, AES, IDEA, DES, Camellia. 옛날 버전 SSL 에서는 RC2 가 쓰임.
- 해시함수 알고리즘: TLS 에서는 HMAC-MD5 또는 HMAC-SHA. SSL 에서는 MD5 와 SHA. 옛날 버전 SSL 에서는 MD2 와 MD4 가 쓰임

문 10. 다음에서 설명하는 스니퍼 탐지 방법에 이용되는 것은?

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

① ARP ② DNS
③ Decoy ④ ARP watch

답 ③

※ 스니핑(sniffing) 탐지 방법
- ping 을 이용한 탐지
  네트워크에 존재하지 않는 MAC 주소로 위조된 ping 을 보내 스니핑을 탐지하는 방법이다.
  ping 명령어는 해당 호스트가 접속 가능한지를 테스트하는 명령어인데, 존재하지 않는 MAC 주소이기 때문에 응답(reply)가 오지 않아야 정상이다.
  그런데 reply 가 온다면 무차별(promiscuous) 모드 상태로 모든 패킷을 들여다보는 스니퍼가 존재한다고 의심할 수 있다.
- ARP 를 이용한 탐지
  존재하지 않는 IP 주소로 위조된 ARP Request 를 보내 스니핑을 탐지하는 방법이다.
  네트워크에 존재하지 않는 IP 주소이기 때문에 ARP Response 가 오지 않아야 정상이다.
  그런데 ARP Response 가 온다면 무차별(promiscuous) 모드 상태로 모든 패킷을 들여다보는 스니퍼가 존재한다고 의심할 수 있다.
- DNS 를 이용한 탐지
  스니퍼들은 로그 파일의 가독성을 위해 IP 주소를 도메인 명으로 변환해주는 DNS inverse lookup 을 요청하는 경우가 많다. 해당 네트워크로 ping sweep 을 보내고 inverse lookup 을 감시하여 스니퍼를 탐지한다.
  존재하지 않는 IP 주소를 이
- Decoy(유인)를 이용한 탐지
  가짜 ID 와 패스워드를 노출시켜 해커를 유인하는 것이다. 해당 ID 와 패스워드로 접속을 시도하는 호스트는 스니퍼라고 의심할 수 있다.
- ARP watch 를 이용한 탐지
  ARP 테이블은 MAC 주소와 IP 주소의 매칭값을 저장해놓은 테이블인데, ARP watch 는 ARP 테이블을 비정상적인 방법으로 변경하려는 트래픽을 모니터링하는 툴이다.

문 11. 다음에 제시된 <보기 1>의 사용자 인증방법과 <보기 2>의 사용자 인증도구를 바르게 연결한 것은?

< 보 기 1 >

ㄱ. 지식 기반 인증
ㄴ. 소지 기반 인증
ㄷ. 생체 기반 인증

< 보 기 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

답 ③

A. OTP 토큰은 소지 기반 인증에 해당한다.
B. 패스워드는 지식 기반 인증에 해당한다.
C. 홍채는 생체 기반 인증에 해당한다.

※ 사용자 인증방법
- 지식 기반 인증: 패스워드(password), 아이핀(i-pin), 주민등록번호, 패스프레이즈(passphrase) 등
- 소지 기반 인증: 열쇠, 주민등록증, OTP 토큰(보안 토큰), 스마트 카드 등
- 생체 기반 인증: 지문, 홍채, 얼굴, 망막, 정맥 등
- 행동 기반 인증: 음성, 서명 동작, 키보드 동작 등
  (행동 기반 인증을 생체 기반 인증에 포함하기도 하고, 별개로 나누기도 한다.)

문 12. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 용어의 정의에 대한 설명으로 옳지 않은 것은?

① 정보통신서비스 : 전기통신사업법 제 2 조제 6 호에 따른 전기 통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것

② 정보통신망 : 전기통신사업법 제 2 조제 2 호에 따른 전기통신 설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용 기술을 활용하여 정보를 수집.가공.저장.검색.송신 또는 수신하는 정보통신체제

③ 통신과금서비스이용자: 정보보호제품을 개발.생산 또는 유통 하는 사람이나 정보보호에 관한 컨설팅 등과 관련된 사람

④ 침해사고: 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태

답 ③

③ 통신과금서비스이용자란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입·이용하는 자를 말한다.

③번의 설명은 제 2 조 8 항 '정보보호산업'에 대한 정의였는데, 현재 개정 법률안에는 해당 조항이 삭제되어 없다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제 2 조(정의)

1. "**정보통신망**"이란 「전기통신사업법」 제 2 조제 2 호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "**정보통신서비스**"란 「전기통신사업법」 제 2 조제 6 호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
3. "정보통신서비스 제공자"란 「전기통신사업법」 제 2 조제 8 호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
5. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.
6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
7. "**침해사고**"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.
8. 삭제
9. "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다.
10. "통신과금서비스"란 정보통신서비스로서 다음 각 목의 업무를 말한다.

가. 타인이 판매·제공하는 재화 또는 용역(이하 "재화등"이라 한다)의 대가를 자신이 제공하는 전기통신역무의 요금과 함께 청구·징수하는 업무

나. 타인이 판매·제공하는 재화등의 대가가 가목의 업무를 제공하는 자의 전기통신역무의 요금과 함께 청구·징수되도록 거래정보를 전자적으로 송수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 업무

11. "통신과금서비스제공자"란 제 53 조에 따라 등록을 하고 통신과금서비스를 제공하는 자를 말한다.
12. "**통신과금서비스이용자**"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입·이용하는 자를 말한다.
13. "전자적 전송매체"란 정보통신망을 통하여 부호·문자·음성·화상 또는 영상 등을 수신자에게 전자문서 등의 전자적 형태로 전송하는 매체를 말한다.

② 이 법에서 사용하는 용어의 뜻은 제 1 항에서 정하는 것 외에는 「국가정보화 기본법」에서 정하는 바에 따른다.

문 13. 안드로이드 보안에 대한 설명으로 옳지 않은 것은?

① 리눅스 운영체제와 유사한 보안 취약점을 갖는다.
② 개방형 운영체제로서의 보안정책을 적용한다.
③ 응용프로그램에 대한 서명은 개발자가 한다.
④ 응용프로그램 간 데이터 통신을 엄격하게 통제한다.

답 ④

④ 안드로이드는 리눅스 기반의 모바일 기기 운영체제로 개발과 배포가 자유로운 오픈 소스 플랫폼과 오픈 마켓이 특징이며, iOS 에 비해 데이터 간 통신에도 자율성을 중시하는 편이다.
반면 그 때문에 iOS 에 비해 보안이 취약하다.
① 안드로이드의 리눅스 기반이며, 리눅스와 유사한 보안 취약점을 가진다.
② 구글은 안드로이드의 모든 소스 코드를 오픈 소스 라이선스인 아파치 v2 라이선스로 배포하고 있어 기업이나 사용자는 각자 안드로이드 프로그램을 독자적으로 개발을 해서 탑재할 수 있다.
③ 안드로이드 환경에서 어플리케이션(응용 프로그램)에 대한 서명은 개발자가 하며, iOS 에서는 애플이 중앙집중 방식으로 관리하고 서명한다.

문 14. 개인정보 보호 인증(PIPL) 제도에 대한 설명으로 옳은 것은?

① 물리적 안전성 확보조치 심사영역에는 악성 소프트웨어 통제 심사항목이 있다.
② 인증절차는 인증심사 준비단계, 심사단계, 인증단계로 구성 되며, 인증유지관리를 위한 유지관리 단계가 있다.
③ 개인정보 보호를 위해 관리계획 수립과 조직구축은 정보주체 권리보장 심사영역에 속한다.
④ 인증을 신청할 수 있는 기관은 공공기관에 한정한다.

답 ②

① 물리적 안전성 확보조치 심사영역은 하드웨어 및 주변기기에 대한 심사항목이며, 악성 소프트웨어 통제는 기술적 안전성 확보조치 심사영역이다.
③ 관리계획 수립과 조직구축은 보호관리체계의 수립 심사영역에 해당한다.
④ 개인정보 보호 인증(PIPL)은 공공기관은 물론, 개인정보를 처리하는 민간기업, 법인, 단체 및 중소기업과, 소상공인까지 인증받을 수 있다.

문 15. 해킹에 대한 설명으로 옳지 않은 것은?

① SYN Flooding 은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.
② Zero Day 공격은 시그니처(signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.
③ APT 는 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.
④ Buffer Overflow 는 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

답 ②

② **Zero Day**(제로데이) 공격은 운영체제나 소프트웨어의 보안 취약점에 대한 업데이트 패치가 나오기 전에, 그 취약점을 이용하여 공격하는 방법이다.

오용 탐지(Misuse Detection)는 이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지하는 방법으로, 알려진 공격 이외는 탐지 불가능

이상 탐지(Anomaly Detection IDS)는 정상 패턴을 DB 에 등록해두고, 정상에서 벗어나는 행위를 탐지하는 방법으로, 알려지지 않은 공격도 탐지 가능

① **SYN Flooding** 공격
TCP 3-way handshaking 을 이용한 DoS 공격으로, 공격 대상 서버에 무수히 많은 SYN 패킷을 보낸 뒤, 서버로부터 오는 SYN+ACK 패킷을 무시하여, 서버가 SYN Received 상태로 끊임없이 기다리게 만드는 공격이다.

③ **APT**(Advanced Persistent Threats, 지능형 지속 공격)
개인이나 단체, 국가, 또는 사업체나 정치 단체를 표적으로 삼아, 목적을 달성하기 위해 오랜 시간 동안 정보를 수집하고 다각도로 연구하여 고급 기술을 동원해 공격하는 기법을 말한다.

④ **Buffer Overflow**(버퍼 오버플로우) 공격
프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.
오버 플로우가 발생하는 데이터 영역에 따라, 힙 오버플로우(heap overflow) 공격과 스택 기반 오버플로우(stack overflow)로 나뉜다.

문 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

답 ④

④ SQL 삽입(SQL injection)은 클라이언트의 입력값을 조작하여 서버의 데이터베이스를 공격하는 것이다.

① 취약한 직접 객체 참조 (Insecure Direct Object Reference)
파일, 디렉터리, 데이터베이스 키와 같은 내부적으로 처리되는 오브젝트가 노출되는 경우 다운로드 취약점 등을 이용하여 시스템 파일 등 권한이 없는 데이터에 접근하는 취약점 등을 의미한다.

② 크로스사이트 요청 변조(CSRF, Cross-site request forgery)
로그인 된 피해자의 취약한 웹 애플리케이션에 피해자의 세션 쿠키와 기타 다른 인증정보를 자동으로 포함하여 위조된 HTTP 요청을 강제로 보내도록 하는 것이다.

③ 크로스 사이트 스크립팅(XSS, Cross-site Scripting)
웹 사이트에 악성 스크립트를 삽입하여, 다른 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.

문 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.

답 ③

시도-응답(Challenge-Response) 인증 방식은 재전송 공격에 취약한 기존의 패스워드 인증 방식을 보완한 일회성 인증 방식이다.

문제처럼 대칭키 암호를 이용하여 시도-응답 인증방식을 사용할 경우, 우선 사용자가 인증을 원할 경우 서버에선 사용자에게 일회성 Challenge(시도 값)를 보낸다. 사용자는 이를 대칭키(비밀키)로 암호화하여 서버에 Response(응답)한다. 서버는 해당 응답을 복호화해서 Challenge 를 비교해 사용자를 인증한다.

③ 시도-응답 인증 방식은 동기화가 필요 없다.
동기화가 필요한 인증 방식은 타임스탬프(timestamp) 방식이다.

문 18. 국제공통평가기준(Common Criteria)에 대한 설명으로 옳지 않은 것은?

① 국가마다 서로 다른 정보보호시스템 평가기준을 연동하고 평가결과를 상호인증하기 위해 제정된 평가기준이다.
② 보호 프로파일(Protection Profiles)은 특정 제품이나 시스템에만 종속되어 적용하는 보안기능 수단과 보증수단을 기술한 문서이다.
③ 평가 보증 등급(EAL : Evaluation Assurance Level)에서 가장 엄격한 보증(formally verified) 등급은 EAL7 이다.
④ 보안 요구조건을 명세화하고 평가기준을 정의하기 위한 ISO/IEC 15408 표준이다.

답 ②

② 보호 프로파일(PP)는 제품군에 대한 보안 요구사항을 정의한 것이고, 보안목표 명세서(ST)는 특정 제품에 대한 보안 명세를 정의한 것이다.

보호프로파일(PP, Protection Profile)
사용자나 개발자의 보안 요구사항을 표현하기 위해 CC 를 준용하여 작성된 것으로, 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구사항 집합
제품군에 대한 보안 요구사항을 정의한 것으로, 특정 제품의 기술적인 구현에 독립적이며, 여러 제품이나 시스템이 동일한 PP 를 적용할 수 있다.

보안목표명세서(ST, Security Target)
개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC 를 준용하여 작성한 것으로, 제품 평가를 위한 기초자료로 사용됨
특정 제품에 대한 보안 명세를 정의한 것이기 때문에 기술적인 구현에 종속적이며, 각 제품이나 시스템은 각각의 ST 를 적용한다.
ST 는 PP 를 포함한다.

문 19.「개인정보 보호법」상 주민등록번호 처리에 대한 설명으로 옳지 않은 것은?

① 주민등록번호를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, 개인인 개인정보처리자는 개인정보 보호위원회의 심의·의결을 거쳐 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공할 수 있다.

② 행정자치부장관은 개인정보처리자가 처리하는 주민등록번호가 유출된 경우에는 5 억원 이하의 과징금을 부과ㆍ징수할 수 있으나, 주민등록번호가 유출되지 아니하도록 개인정보처리자가「개인정보 보호법」에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 개인정보처리자는 주민등록번호가 분실ㆍ도난ㆍ유출ㆍ변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

답 ①

① (상당히 조잡한 문제)
주민등록번호(X) -> 개인정보(○)

제 18 조(개인정보의 목적 외 이용·제공 제한) 제 2 항의 5
개인정보를 목적 외의 용도로 이용하거나 이를 제 3 자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

② 제 34 조의 2(과징금의 부과 등) 제 1 항
행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5 억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제 24 조제 3 항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.

③ 제 24 조의 2(주민등록번호 처리의 제한)의 제 3 항
개인정보처리자는 제 1 항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 제 24 조의 2(주민등록번호 처리의 제한)의 제 2 항
개인정보처리자는 제 24 조제 3 항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.

문 20. 다음에서 설명하는 윈도우 인증 구성요소는?

> ○ 사용자의 계정과 패스워드가 일치하는 사용자에게 고유의 SID(Security Identifier)를 부여한다.
> ○ SID 에 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)

답 ②

② **SRM**(Security Reference Monitor)
인증된 사용자에게 **SID(Security ID)를 부여**
SID 를 기반으로 하여 파일이나 디렉터리에 대한 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성
① **LSA**(Local Security Authority)
모든 계정의 로그인에 대한 검증
시스템 자원(파일 등)에 대한 **접근 권한 검사**(로컬 및 원격 로그인 포함)
계정명과 SID(Security ID)를 매칭하여 SRM 이 생성한 감사 로그를 기록
보안 서브시스템(Security Subsystem)이라고도 함
③ **SAM**(Security Account Manager)
사용자/그룹 계정 정보에 대한 **데이터베이스 관리**
사용자 로그인 정보와 SAM 파일에 저장된 사용자 패스워드 정보를 비교해 인증 여부 결정
SAM 파일은 사용자, 그룹 계정 및 암호화된 패스워드 정보를 저장하고 있는 데이터베이스
④ IPSec(IP Security)은 IP 패킷을 암호화하고 인증하는 안전한 인터넷 프로토콜(IP) 통신을 위한 프로토콜로, 윈도우 인증 구성요소가 아니다.