2018년 서울시 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

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

1. 2009년 Moxie Marlinspike가 제안한 공격 방식이며, 중간자 공격을 통해 사용자와 서버 사이의 HTTPS 통신을 HTTP로 변경해서 비밀번호 등을 탈취하는 공격 방식으로 가장 옳은 것은?

① SSL stripping
② BEAST attack
③ CRIME attack
④ Heartbleed

답 ①

① **SSL stripping**(SSL 스트리핑)
공격 대상자와 서버가 최초 세션 연결할 때, 중간자 공격을 통해 HTTPS 통신을 HTTP 통신으로 변경해 트래픽 내용을 훔쳐보는 공격이다.
공격 대상자가 서버에 접속을 요청하면, 서버는 HTTPS를 사용하는 웹페이지의 링크를 전송한다. 이 때 공격자가 중간에서 응답을 가로채어 HTTPS의 링크를 HTTP로 변경한 뒤 공격대상에게 전송한다. 이렇게 함으로써 공격자는 공격대상과 HTTP 통신을 맺고, 서버와는 HTTPS 통신을 맺어 중간에서 트래픽을 훔쳐볼 수 있게 된다.

<오답 체크> ② **BEAST**(Browser Exploit Against SSL/TLS)
SSL 3.0의 취약점을 공격하는 것으로, HTTPS에서의 세션 쿠키를 해독하여 타깃의 세션을 하이재킹하는 공격이다.

③ **CRIME**(Compression Ration Info-Leak Mass Exploitation)
HTTPS 상에서 주고받는 데이터의 압축과정에서의 취약점을 이용하여 쿠키를 훔치는 공격이다.

④ **HeartBleed**(하트블리드) 공격
2014년 4월 OpenSSL 1.0.1 버전에서 발견된 매우 심각한 버그 OpenSSL을 구성하고 있는 TLS/DTLS의 HeartBeat 확장규격에서 발견된 취약점으로, 해당 취약점을 이용하면 서버와 클라이언트 사이에 주고받는 정보들을 탈취할 수 있다.

2. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

① 게시판 등의 웹페이지에 악의적인 코드 삽입이 가능하다는 취약점이 있다.
② 공격 코드를 삽입하는 부분에 따라 저장 XSS 방식과 반사 XSS 방식이 있다.
③ 악성코드가 실행되면서 서버의 정보를 유출하게 된다.
④ Javascript, VBScript, HTML 등이 사용될 수 있다.

답 ③

③ XSS 공격에서 악성코드는 서버가 아닌, 사용자의 브라우저에서 실행되어 사용자의 정보를 유출하게 된다.

◈ **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)는 웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
▷ **저장 XSS 공격**(Stroed XSS)은 웹 서버에 악성 스크립트를 영구적으로 저장해 놓는 공격 방법으로, 웹 사이트의 게시판, 사용자 프로필 및 댓글난 등에 악성 스크립트를 삽입해 놓는다. 사용자가 사이트를 방문하여 저장되어 있는 페이지에 접근하면, 서버에 있던 악성 스크립트를 사용자에게 전달되어 사용자 브라우저에서 실행되어 공격한다.
▷ **반사 XSS 공격**(Reflected XSS)은 사용자에게 악성 URL을 배포하여 사용자가 클릭하도록 유도하여 바로 사용자를 공격하는 방법이다. 공격자는 공격용 악성 URL을 생성한 뒤, 이 URL을 이메일 메세지나 거짓 정보 등 다양한 경로로 사용자들에게 배포한다. 사용자는 이 URL 링크를 클릭하는 순간 바로 악성 스크립트가 사용자의 브라우저에서 실행된다.

3. <보기>에서 설명하는 보안 목적으로 가장 옳은 것은?

〈 보 기 〉
정보가 허가되지 않은 방식으로 바뀌지 않는 성질

① 무결성(Integrity)
② 가용성(Availability)
③ 인가(Authorization)
④ 기밀성(Confidentiality)

답 ①

① 무결성(**Integrity**): 데이터가 위·변조되지 않아야 함

▷ 기밀성(Confidentiality): 비인가자에게는 메시지를 숨겨야 함
▷ 무결성(Integrity): 데이터가 위·변조되지 않아야 함
▷ 가용성(Availability): 권한이 있는 자는 서비스를 사용하여야 함
▷ 인증(authentication): 정당한 상대방인지, 진짜인지 가짜인지를 확인하는 것
▷ 인가(authorization): 특정한 프로그램이나 데이터에 대한 사용 권한이 있는지 확인하는 것

4.「개인정보 보호법」상 용어 정의로 가장 옳지 않은 것은?

① 개인정보: 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
② 정보주체: 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람
③ 처리: 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위
④ 개인정보관리자: 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인

답 ④

④ '개인정보**처리자**'이다.

「개인정보 보호법」
제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. "**개인정보**"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "**처리**"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. "**정보주체**"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. "**개인정보파일**"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. "**개인정보처리자**"란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

5. Feistel 암호 방식에 대한 설명으로 가장 옳지 않은 것은?

① Feistel 암호 방식의 암호 강도는 평문 블록의 길이, 키의 길이, 라운드의 수에 의하여 결정된다.
② Feistel 암호 방식의 복호화 과정과 암호화 과정은 동일하다.
③ AES 암호 알고리즘은 Feistel 암호 방식을 사용한다.
④ Feistel 암호 방식은 대칭키 암호 알고리즘에서 사용된다.

답 ③

③ AES는 페이스텔이 아닌 SPN 구조를 사용한다.

◈ **DES**(Data Encryption Standard)
페이스텔(Feistel) **구조 16라운드**
블록 64**비트**
키 길이 56**비트 + 패리티** 8**비트 =** 64**비트**
◈ **AES**(Advanced Encryption Standard)
SPN**구조**
블록 128**비트**(16**바이트**)
키 길이 128**비트 –** 10**라운드**
키 길이 192**비트 –** 12**라운드**
키 길이 256**비트 –** 14**라운드**

<오답 체크> ② 이 선지가 약간 잘못된 부분이 있다.
페이스텔 방식에서 암호화 알고리즘과 복호화 알고리즘은 다르지 않지만, 문제에 나온 표현대로 '암호화 과정과 복호화 과정' 그 전체 과정은 반대이기 때문이다.
페이스텔 암호 방식에서 16라운드를 사용한다면, 각 라운드에 사용하는 라운드 키를 1번부터 16번으로 차례대로 사용한다. 반면 복호화 과정에서는 역순으로 16번부터 1번으로 사용해야 한다. 따라서 선지에 쓰인 대로 과정 자체가 동일하다는 표현은 논란의 여지가 있다. 하지만 문제에서 가장 옳지 않은 것으로 고르라고 했기 때문에, 확실하게 틀린 ③이 답이 된다.
④ 페이스텔 방식에서는 암호화와 복호화에 동일한 키를 사용하며, 대칭키 암호화 알고리즘인 DES, 3DES, blowfish, SEED 등에서 사용된다.

6. 디지털 서명에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

〈 보 기 〉
ㄱ. 디지털 서명은 부인방지를 위해 사용할 수 있다.
ㄴ. 디지털 서명 생성에는 개인키를 사용하고 디지털 서명 검증에는 공개키를 사용한다.
ㄷ. 해시 함수와 공개키 암호를 사용하여 생성된 디지털 서명은 기밀성, 인증, 무결성을 위해 사용할 수 있다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

답 ①

ㄱ. ◈ 전자서명의 특성
▷ 위조 불가(unforgeable)
▷ 서명자 인증(authentic)
▷ 부인 방지(non-repudiation)
▷ 변경 불가(unalterable)
▷ 재사용 불가(not reusable)
ㄴ. 전사 서명은 개인키로 암호화(생성)를 하고 공개키로 복호화(검증)를 한다
<오답 체크> ㄷ. 전자 서명은 무결성만 보장할 뿐, 기밀성은 보장하지 않는다. 공개키를 이용하여 누구나 복호화할 수 있으므로 기밀성은 보장할 수 없다.

7. 분산반사 서비스 거부(DRDoS) 공격의 특징으로 가장 옳지 않은 것은?

① TCP 프로토콜 및 라우팅 테이블 운영상의 취약성을 이용한다.
② 공격자의 추적이 매우 어려운 공격이다.
③ 악성 봇의 감염을 통한 공격이다.
④ 출발지 IP 주소를 위조하는 공격이다.

답 ③

▶ **DRDoS** 공격(Distributed Reflect DoS, 분산 반사 서비스 거부 공격)
패킷의 출발지 IP 주소를 공격 대상의 IP주소로 스푸핑한 TCP-SYN 패킷을 브로드캐스트로 다수의 시스템에 전송한다. 패킷을 받은 각 단말들은 이에 응답 패킷을 보내게 되는데, TCP-SYN 패킷의 출발지 IP 주소가 공격 대상의 IP 주소로 위조된 상태이기 때문에 응답 패킷은 공격 대상으로 향하게 된다. 이를 통해 각 단말들이 보내는 응답 패킷들이 공격 대상으로 몰리게 만들어 시스템 자원을 고갈시켜 서비스를 마비시키게 된다.

③ 악성 봇이 필요한 공격은 DDoS 공격이다.
DRDoS 공격은 악성 봇을 감염시킬 필요가 없다.

<오답 체크> ② DRDoS 공격 패킷은 공격자를 통해 들어오는 게 아니고 공격자의 패킷에 응답한 단말들을 통해 들어오는 것이기 때문에, 공격자를 추적하기가 매우 어렵다.

8. 침입탐지시스템의 비정상행위 탐지 방법에 대한 설명으로 가장 옳지 않은 것은?

① 정상적인 행동을 기준으로 하여 여기서 벗어나는 것을 비정상으로 판단한다.
② 정량적인 분석, 통계적인 분석 등을 사용한다.
③ 오탐률이 높으며 수집된 다양한 정보를 분석하는 데 많은 학습 시간이 소요된다.
④ 알려진 공격에 대한 정보 수집이 어려우며, 새로운 취약성 정보를 패턴화하여 지식데이터베이스로 유지 및 관리하기가 쉽지 않다.

답 ④

④ 비정상행위(이상) 탐지 기법은 정상 패턴을 DB에 등록해두고 정상에서 벗어나는 행위를 탐지하는 방법이다.
아직 공격에 악용되지는 않았지만 시스템에 존재하는 취약성 정보를 분석하여, 알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지가 가능하다.

<오답 체크> ① 비정상행위 탐지 기법은 이미 발견된 공격이 아닌, 예상 되는 공격 또한 포함하여 진단하기 때문에, 오탐율이 높고 어디까지 공격으로 판단할지에 대한 임계치의 설정이 어렵다.

◈ **오용 탐지**(Misuse Detection)
= 시그니처 기반(Signature Base)
= 지식 기반(Knowledge Base)
이미 발견되고 정립된 공격 패턴을 미리 입력해 두고 그에 해당하는 패턴을 탐지
오탐율이 낮고 비교적 효율적이나 알려진 공격 이외는 탐지 불가능
전문가 시스템(Expert System)의 지식 DB를 이용한 IDS
Zero Day attack(제로 데이 공격)에 취약

◈ **이상 탐지**(Anomaly Detection IDS)
= 행위 기반(Behavior)
= 통계적 탐지(Statistical Detection)
정상 패턴을 DB에 등록해두고, 정상에서 벗어나는 행위를 탐지(임계치 설정)
알려지지 않은 공격인 제로 데이 공격(zero day attack) 탐지 가능
오탐율 높고, 임계치 설정이 어려움

9. 메모리 변조 공격을 방지하기 위한 기술 중 하나로, 프로세스의 중요 데이터 영역의 주소를 임의로 재배치하여 공격자가 공격 대상 주소를 예측하기 어렵게 하는 방식으로 가장 옳은 것은?

① canary
② ASLR
③ no-execute
④ Buffer overflow

답 ②

② **ASLR**(Address Space Layout Randomization)
메모리상의 공격을 어렵게 하기 위해 스택이나 힙, 라이브러리 등의 주소를 랜덤으로 프로세스 주소 공간에 배치함으로써 실행할 때 마다 데이터의 주소가 바뀌게 하는 방법이다.

<오답 체크> ① **Stack Guard**(스택 가드) 또는 카나리(**canary**)
메모리의 특정한 위치(ret 앞)에 카나리(canary)라는 특정한 값을 집어넣어, 프로그램 실행 시 카나리 값을 검증하여 변조되었을 경우 스택 영역이 변조되었다고 판단하여 프로그램을 종료하는 방법이다.

③ **NX**(Non-Executable Stack)
= **DEP**(Deta Execution Pretection)
가장 기초적인 오버플로우 방어 기법으로, 스택에서 코드가 실행되지 않도록 설정하는 것이다.(**NX-bit** 설정)

④ 버퍼 오버플로우(buffer overflow)란 메모리 변조 공격을 방지하는 기술이 아니고, 프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터가 입력되어 메모리를 정상적으로 처리하지 못하게 되는 현상을 말한다. 이것을 악용하는 것이 버퍼 오버플로우 공격이다.

◈ **버퍼 오버플로우**(buffer overflow) 공격
프로그램에 미리 할당된 버퍼보다 더 많은 양의 데이터를 집어넣어, 다른 메모리 영역을 침범하여 데이터를 변조시키는 공격이다.

10. 퍼징(fuzzing)에 대한 설명으로 가장 옳은 것은?

① 사용자를 속여서 사용자의 비밀정보를 획득하는 방법이다.
② 실행코드를 난독화하여 안전하게 보호하는 방법이다.
③ 소프트웨어 테스팅 방법 중 하나로 난수를 발생시켜서 대상 시스템에 대한 결함이 발생하는 입력을 주입하는 방법이다.
④ 소스 코드를 분석하는 정적 분석 방법이다.

답 ③

③ Fuzzing(퍼징)은 컴퓨터 프로그램에 유효한, 예상치 않은 또는 무작위 데이터를 입력하여, 프로그램의 충돌이나 빌트인 코드 검증의 실패, 잠재적인 메모리 누수 발견 등 소프트웨어의 버그를 찾아내는 방법이다.

▷ Generation Fuzzer: 새로운 데이터를 입력하는 방식
▷ Mutation Fuzzer: 기존 데이터를 변형하여 입력하는 방식

<오답 체크> ① 사회공학적 공격은 기술적인 방법이 아닌 사람들간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법을 일컫는다.

② **난독화**(Obfuscation)
프로그래밍 언어로 작성된 코드에 대해 읽기 어렵게 만드는 작업으로, 코드의 가독성을 낮춰 역공학에 대한 대비하는 방법이다.
난독화를 적용하는 범위에 따라 소스 코드 난독화와 바이너리 난독화로 나눌 수 있다.
난독화 방법으로는
ⅰ 필요 이상으로 복잡하거나 아무 의미 없는 코드를 작성하는 방법
ⅱ 관련이 없는 여러 함수들을 뒤섞는 방법
ⅲ 데이터를 알아보기 힘들게 인코딩하는 방법 등이 있다.

④ **정적 프로그램 분석**(Static program analysis)
실제 프로그램의 실행 없이 컴퓨터 소프트웨어를 분석하는 것을 말한다. 대부분의 경우는 소스 코드를 분석하며, 가끔은 목적 프로그램 형태를 분석한다.

11. 보안 측면에서 민감한 암호 연산을 하드웨어로 이동함으로써 시스템 보안을 향상시키고자 나온 개념으로, TCG 컨소시엄에 의해 작성된 표준은?

① TPM
② TLS
③ TTP
④ TGT

답 ①

① **TPM**(Trusted Platform Module, 신뢰할 수 있는 플랫폼 모듈)
암호화 키를 포함하여 외부의 공격이나 내부의 다른 요인에 의해 하드웨어의 변경이나 손상을 방지하는 등의 보안관련 기능을 제공하는 기술이다.
TPM을 통해 암호화를 할 경우, 하드 디스크 자체가 암호화되기 때문에 디스크를 떼어내 다른 PC에 연결하더라도 데이터를 볼 수 없다. 이렇게 하드웨어 자체를 암호화하는 것을 '암호 연산을 하드웨어로 이동'시켰다는 형이상학적 문장으로 표현한 것이다.

<오답 체크> ② **SSL**(Secure Sockets Layer, 보안 소켓 레이어) 또는
TLS(Transport Layer Security, 전송 계층 보안)
응용 계층과 전송 계층 사이에서 통신 과정에서 종단간 보안과 클라이언트와 서버 간 상호 인증, 기밀성, 무결성 서비스를 제공하는 보안 프로토콜
인터넷 전자상거래를 위해 넷스케이프사가 개발한 것으로, 웹 브라우저와 웹 서버 간의 전자상거래 정보를 안전하게 전송하기 위한 프로토콜이다. SSL 3.0버전이 TLS 1.0버전이 된다.

③ **TTP**(Trusted Third Party, 제3 신뢰 기관)
사용자들로부터 신뢰를 얻어, 사용자 인증, 부인 방지, 키 관리 등을 중재, 인증, 증명, 관리 등을 하는 기관을 의미한다.
ISO/IEC JTC 1/SC 27에서 TTP의 이용과 관리 지침을 기술 보고(Technical Report)로 채택할 예정으로 검토를 진행하고 있다. TTP의 기능에는 증명서 관리, 증거 관리, 키 관리, 타임 스탬프 등이 포함되어 있다.

④ TGT(티켓 승인 티켓, $Ticket_{TGS}$)는 커버로스(Kerberos)에서 사용자가 서비스 승인 티켓($Ticket_V$)을 획득하기 위해 TGS에 제시하는 티켓이다. TGT는 인증 서버가 발급하고 TGS가 검증해야 하므로, 인증 서버와 TGS의 대칭키로 암호화되어 있다.

12. 사회 공학적 공격 방법에 해당하지 않는 것은?

① 피싱
② 파밍
③ 스미싱
④ 생일 공격

답 ④

④ **생일 공격**(birthday attack)
해시 함수의 출력 해시값이 같은 서로 다른 임의의 두 메시지를 찾아내는(해시 충돌) 암호해독 공격으로, 생일 문제의 확률적 계산 이론을 기반으로 한다.
생일 문제에 따르면 해시 함수의 입력값을 다양하게 할수록 해시값이 같은 두 입력값을 발견할 확률은 빠르게 증가한다. 따라서 모든 값을 대입하지 않고도 해시 충돌을 찾아낼 확률을 충분히 크게 만들 수 있다.
생일은 365일 중 하루이기 때문에, 언뜻 생각하기엔 100명 정도는 모여야 생일이 같은 두 사람이 있을 것 같은데, 실제로는 23명만 모여도 생일이 같은 두 사람이 있을 확률은 50%를 넘고, 57명이 모이면 생일이 같은 두 사람이 있을 확률은 99%가 넘어간다.

<오답 체크> ① **피싱**(phishing)
인터넷 사용자에게 가짜 도메인을 알려주어, 가짜 사이트로 접속을 유도하는 공격이다.

② **파밍**(pharming)
사용자가 자신의 웹 브라우저에서 올바른 도메인을 입력해도 가짜 웹 페이지에 접속하게 하여 개인정보를 훔치는 것이다.

③ **스미싱**(Smishing)
문자 메시지(SMS)와 피싱(Phishing)의 합성어로, 스마트폰 사용자에게 가짜 사이트 주소 링크를 문자 메시지(SMS)로 보내 스마트폰 정보나 소액결제를 유도하는 공격이다.

13. 접근 제어 방식 중, 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용되는 방식은?

① 접근 제어 행렬(Access Control Matrix)
② 접근 가능 목록(Capability List)
③ 접근 제어 목록(Access Control List)
④ 방화벽(Firewall)

답 ②

② **CL**(Capability List, 접근가능 목록)
한 주체의 객체들에 대한 접근 권한을 명시한 리스트

<오답 체크> ① **ACM**(Access Control Matrix, 접근통제 매트릭스)
은 ACL과 CL의 결합으로, 주체들과 객체들의 접근 권한을 행렬(매트릭스) 형태로 작성한 표이다.

③ **ACL**(Access Control List, 접근통제 목록)
한 객체에 대한 주체들의 접근 권한을 명시한 리스트

④ **방화벽**(Firewall)
외부 공격으로부터 내부 시스템을 보호하기 위해 외부 네트워크와 내부 네트워크 사이에 설치된 하드웨어나 소프트웨어 장치를 의미한다.

14. WPA2를 공격하기 위한 방식으로, WPA2의 4-way 핸드셰이크(handshake) 과정에서 메시지를 조작하고 재전송하여 정보를 획득하는 공격 방식으로 가장 옳은 것은?

① KRACK
② Ping of Death
③ Smurf
④ Slowloris

답 ①

① KRACK(Key Reinstallation Attack, 키 재설정 공격)
WPA2의 키 관리 취약점을 공격하는 것
클라이언트가 WPA2 보안이 설정된 와이파이 네트워크에 접속할 때 수행하는 4-웨이 인증 핸드셰이크의 세 번째 단계를 대상으로 한다. 세 번째 단계에서 암호화 키는 여러 번 전송될 수 있는데, 만약 공격자가 이 전송 데이터를 특정한 방법으로 모아서 재생하면 와이파이 보안 암호화가 깨질 수 있다.

<오답 체크> ② **Ping of Death**
icmp 패킷을 정상보다 매우 크게 만들어 공격하는 DoS 공격이다.
크게 조작된 icmp 패킷은 라우터를 통과하는 동안 매우 작은 패킷으로 조각화(fragment)되어 공격 대상에 도달하는데, 공격 대상은 조각화된 패킷을 모두 처리하느라 과부하가 걸리게 된다.

③ **Smurf**(ICMP flooding) 공격
출발지 IP주소를 공격대상의 IP주소로 위장하여 ICMP Echo 메시지를 브로드캐스트함으로써, 공격대상으로 많은 양의 ICMP Echo 응답 패킷이 몰리게 만들어 시스템 자원이 고갈되도록 만드는 공격이다.

④ **Slowloris** 공격
공격자가 공격 대상 서버로 접속하여 정상 세션을 맺은 후, 완전하지 않은 헤더값을 꾸준히 보내 connection을 계속 유지하게 만들어 다른 사용자가 서버를 이용하지 못하게 하는 공격이다.
정상 헤더라면 '0d0a'값이 들어있어 헤더의 전송이 완료되었음을 알리는데, 비정상 헤더에는 '0d'의 값만 들어있어, 서버는 헤더의 전송이 완료되지 않은 것으로 판단하여 계속 connection을 유지하게 된다.

15. 오일러 함수 Φ( )를 이용해 정수 n = 15에 대한 Φ(n)을 구한 값으로 옳은 것은? (단, 여기서 오일러 함수 Φ( )는 RSA 암호 알고리즘에 사용되는 함수이다.)

① 1
② 5
③ 8
④ 14

답 ③

RSA 암호 알고리즘 키 생성 과정에서 n은 두 소수인 p와 q의 곱이며, Φ(n)는 p-1과 q-1의 곱이다.
n = p × q // Φ(n) = (p – 1) × (q – 1)
n을 두 소수로 인수분해하면, 3 × 5 가 되며,
따라서 Φ(n) = (3 – 1) × (5 – 1) = 2 × 4 = **8** 이 된다.

◈ RSA 알고리즘 공개키와 개인키 생성 순서
○ 단계 1: 두 소수 p, q를 선정한다.
○ 단계 2: n = p × q를 계산한다.
○ 단계 3: Φ(n) = (p – 1) × (q – 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
○ 단계 4: Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
○ 단계 5: e × d mod Φ(n) = 1의 관계를 갖는 d를 계산한다.
(단, mod는 나머지를 구하는 연산자이다.)
○ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

$$\text{암호문} = (\text{평문})^{e} \bmod n$$
$$\text{평문} = (\text{암호문})^{d} \bmod n$$

16. 능동적 공격으로 가장 옳지 않은 것은?

① 재전송
② 트래픽 분석
③ 신분위장
④ 메시지 변조

답 ②

② 트래픽 분석은 수동적 공격(소극적 공격)에 해당한다.

✠ **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

17. 무선랜 보안에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

〈 보 기 〉
ㄱ. WEP는 RC4 암호 알고리즘을 사용한다.
ㄴ. WPA는 AES 암호 알고리즘을 사용한다.
ㄷ. WPA2는 EAP 인증 프로토콜을 사용한다.

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

답 ②

ㄱ. **WEP** 방식
암호화를 위해 RC4 사용하며(암호키 계속 사용)
암호화와 인증에 동일한 키를 사용
ㄷ. **WPA2** 방식
AES-CCMP 사용
EAP를 통한 사용자 인증
<오답 체크> ㄴ. **WPA** 방식
RC4-TKIP를 통한 암호화(암호키 주기적인 변경)
48비트 길이의 초기벡터(IV) 사용
EAP를 통한 사용자 인증

18. BLP(Bell & La Padula) 모델에 대한 설명으로 가장 옳지 않은 것은?

① 다단계 등급 보안(Multi Level Security) 정책에 근간을 둔 모델이다.
② 기밀성을 강조한 모델이다.
③ 수학적 모델이다.
④ 상업용 보안구조 요구사항을 충족하는 범용 모델이다.

답 ④

④ 상업적인 관점에서의 보안 요구사항을 강조하는 모델로는 클락-윌슨 모델과 만리장성 모델 등이 있다.
✠ **클락-윌슨**(Clark-Wilson) 모델
무결성 중심의 상업적 모델
• 트랜잭션의 내·외부적 일관성 유지(Well-formed transaction)
• 효율적인 업무 처리를 위한 직무 분리(Separation of duties)
• 접근 주체가 권한을 가지고 직접 접근하는 게 아니라 프로그램을 통해서 접근
✠ **Chineses Wall**(만리장성) 모델
서로 상충관계에 있는 객체간의 정보 접근을 통제하는 모델. 이익의 충돌이 많이 발생하는 금융, 회계, 투자, 광고 등의 분야에서 주로 사용된다.
<오답 체크> ② **벨 라파듈라**(BLP, Bell-LaPadula) 모델
기밀성을 중시한 모델, 최초의 수학적 모델
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star(*) 속성 – NWD(No Write Down)

19. <보기>와 관련된 데이터베이스 보안 요구 사항으로 가장 옳은 것은?

> 〈 보 기 〉
> 서로 다른 트랜잭션이 동일한 데이터 항목에 동시적으로 접근하여도 데이터의 일관성이 손상되지 않도록 하기 위해서는 로킹(locking) 기법 등과 같은 병행 수행 제어 기법 등이 사용되어야 한다.

① 데이터 기밀성
② 추론 방지
③ 의미적 무결성
④ 운영적 무결성

답 ④

④ 데이터의 운영적 무결성 보장
트랜잭션의 병행처리 동안에 데이터베이스 내의 데이터에 대한 논리적인 일관성을 유지하는 것 (이런 요구사항은 DBMS의 병행수행관리자에 의하여 보장됨)
▷ 로킹기법 : 고유 가능한 데이터에 대한 접근을 상호배타적으로 통제하는 병행수행제어기법으로 데이터의 논리적 일관성 보장

<오답 체크> ① 데이터 기밀성(confidentiality)
부적절하게 데이터가 노출되는 것을 방지하는 것
② 추론방지(inference control)
사용자가 겉에 보이는 일반적 데이터로부터 숨겨둔 비밀정보를 획득하는 추론이 불가능하도록 보호하는 것
③ 데이터의 의미적 무결성 보장
데이터베이스는 데이터에 대한 허용값을 통제함으로써 변경 데이터의 논리적 일관성을 유지하는 것

20. RSA에 대한 설명으로 가장 옳지 않은 것은?

① AES에 비하여 암, 복호화 속도가 느리다.
② 키 길이가 길어지면 암호화 및 복호화 속도도 느려진다.
③ 키 생성에 사용되는 서로 다른 두 소수(p, q)의 길이가 길어질수록 개인키의 안전성은 향상된다.
④ 중간자(man-in-the-middle) 공격으로부터 안전하기 위해서는 2,048비트 이상의 공개키를 사용하면 된다.

답 ④

④ RSA 암호화 알고리즘에서 키의 길이란 키 생성에 사용되는 큰 두 소수 p와 q의 곱 N의 길이를 의미한다.
수 년 전부터 마이크로소프트, 구글 등 IT 선두 기업들은 자사의 서비스에서 2048비트의 RSA키를 사용하고 있다.

◈ RSA 알고리즘 공개키와 개인키 생성 순서
○ 단계 1: 두 소수 p, q를 선정한다.
○ 단계 2: n = p × q를 계산한다.
○ 단계 3: Φ(n) = (p – 1) × (q – 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
○ 단계 4: Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
○ 단계 5: e × d mod Φ(n) = 1의 관계를 갖는 d를 계산한다.
(단, mod는 나머지를 구하는 연산자이다.)
○ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

$$\text{암호문} = (\text{평문})^{e} \bmod n$$
$$\text{평문} = (\text{암호문})^{d} \bmod n$$

<오답 체크> ① AES는 대칭키 암호화 알고리즘이며, RSA는 공개키 암호화 알고리즘이다. 암·복호화 속도는 대칭키 방식이 훨씬 빠르다.
②③ 키 길이는 p와 q의 곱인 N의 길이를 말하는데, p와 q가 길어질수록 N의 길이도 당연히 길어진다. 키의 길이가 길어질수록 키를 해독하는 시간은 기하급수적으로 늘어나 안전성이 향상된다. 하지만 무작정 키의 길이만 늘리다 보면, 암·복호화를 처리하는 시간이 늘어나 효율성이 떨어지게 된다. 보통 전문가들은 키 길이를 두 배로 늘리면 복호화 처리 시간이 6~7배 더 걸린다고 말한다.