2014-서울시-정보보호론-A형-해설

대방고시 전산직/계리직, 하이클래스 군무원 곽후근(gobarian@gmail.com)

1. 정보보호의 목적 중 기밀성을 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
정답 체크 :
(4) 접근통제 및 암호화 : 접근통제는 인가된 사람만이 데이터에 접근하므로 기밀성에 해당되고, 암호화는 도청을 막아주므로 기밀성에 해당된다.
오답 체크 :
(1) 데이터 백업 및 암호화 : 데이터 백업은 인가된 사람이 언제나 데이터에 접근할 수 있으므로 가용성에 해당된다.
(2) 데이터 백업 및 데이터 복원 : 데이터 복원은 인가된 사람이 언제나 데이터에 접근할 수 있으므로 가용성에 해당된다.
(3) 데이터 복원 및 바이러스 검사 : 바이러스 검사는 데이터의 무결성을 검사한다.
(5) 접근 통제 및 바이러스 검사 : 바이러스 검사는 데이터의 무결성을 검사한다.

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.
정답 체크 :
(5) 기밀성 : 인가된 사람, 인가된 프로세스, 인가된 시스템만이 알 필요성에 근거하여 시스템에 접근해야 함을 의미한다.
오답 체크 :
(1) 부인방지 : 송신부인방지(어떤 메시지가 송신되었을 때 수신자는 그 메시지가 실제로 송신자라고 주장하는 주체에 의해 송신되었음을 확인한다). 수신부인방지(어떤 메시지가 수신되었을 때 송신자는 그 메시지가 실제로 수신자라고 주장하는 주체에 의해 수신되었음을 확인한다).
(2) 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질의 의미한다.
(3) 인증성 : 상대방의 신원을 확인시켜 준다. 사용자 인증(시스템 접근 통제)과 데이터 출처

인증(MAC)이 있다.
(4) 가용성 : 인가된 사용자가 자원이 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있어야 하는 성질을 의미한다.

3. 다음 중 가장 안전한 패스워드는 어떤 것인가?
① 75481235
② abcd1234
③ korea2034
④ honggildong
⑤ do@ssud23
정답 체크 : (이론이 아니라 실제 시간을 측정해본 결과 정답은 5번이 아니라 4번이다.)
(5) do@ssud23 : 소문자, 특수문자, 숫자로 구성(9문자) (크래킹에 16시간 걸림) (이론상으로는 3개의 문자를 섞은 9문자가 시간이 더 걸리는 것처럼 보이지만 실제로는 1개의 문자를 가진 11문자인 4번이 더 오래 걸린다. 2014 년도에 실제 검색 시간을 기반으로 이의 신청을 했어야 하는 것으로 보인다.)
오답 체크 :
(1) 75481235 : 숫자로 구성(9문자) (크래킹에 3밀리초 걸림)
(2) abcd1234 : 소문자, 숫자로 구성(8문자) (크래킹에 시간이 걸리지 않음)
(3) korea2034 : 소문자, 숫자로 구성(9문자) (크래킹에 42분 걸림)
(4) honggildong : 소문자(11문자) (크래킹에 하루 걸림) (실제로 5번보다 더 오래 걸린다)
Tip! : 패스워드는 글자 수와 어떤 문자들을 많이 섞었는지에 따라 보안의 강도가 정해진다. honggildong은 11문자이지만 소문자로만 되어있어 보안의 강도가 약하다. 크래킹에 걸리는 시간은 https://howsecureismypassword.net/에서 계산하였다.

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.
정답 체크 :
(3) 분산 형태 : 커버로스는 중앙 집중식 인증 서버를 이용한다.
오답 체크 :
(1) Needham-Schroeder : 대칭키 프로토콜과 공개키 프로토콜이 존재한다. 대칭키는 커버로스 프로토콜의 기반이 되고, 서버와 클라이언트 사이에 세션키를 생성한다. 공개키는 서버와 클라이언트 사이에서 상호 인증을 제공한다.
(2) 대칭키 : 커버로스는 MIT에서 개발한 비밀키(대칭키) 암호 기반 키 분배 및 사용자 인증 시스템이다.
(4) 티켓 : 클라이언트가 서버에 접속할 때 필요하다. 티켓에는 클라이언트와 서버의 세션키, 클라이언트 ID, 클라이언트 IP 주소, 서버의 ID, 타임스탬프, 유효기간이 있다.
(5) TGT : 티켓을 발급받는데 필요한 티켓이다. TGT에는 클라이언트와 TGS의 세션키, 클라

이언트 ID, 클라이언트 IP 주소, TGS ID, 타임스탬프, 유효기간이 있다.

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.
정답 체크 :
(2) RSA : 대표적인 공개키 암호로, 이외에도 Elgamal, Rabin, ECC 등이 있다.
오답 체크 :
(1) AES, DES : 대표적인 대칭키 암호로, 이외에도 3-DES 등이 있다.
(3) 속도 : 공개키 암호는 두 키의 수학적 특성에 기반하기 때문에, 메시지를 암호화 및 복호화 하는 과정에 여러 단계의 산술 연산이 들어간다. 따라서 대칭키 암호에 비하여 속도가 매우 느리다는 단점을 지니고 있다.
(4) 년도 : 대칭키 암호는 고대(스키테일, 시저), 근대(제1, 2차 세계대전, Shannon, one-time pad), 현대(DES, 3-DES, AES)의 역사를 가진다. 공개키 암호는 1874년 윌리엄 스탠리 제본스가 인수 분해 문제를 거론했고, 1976년에 공개키의 시초가 된 디피-헬만 키 교환 방식이 발표되었다.
(5) 암호문의 길이 : 대칭키의 경우 블록 단위로 암호문이 생성(AES의 경우 128비트 평문이 128비트 암호문이 된다)되고 패딩만큼만 암호문의 길이가 증가한다. 공개키(RSA)의 경우 메시지를 N(예 : 1024bit)보다 작은 숫자로 변환 후 암호화를 수행하므로 암호문의 길이는 N보다 작다. 공개키도 패딩이 필요하다. 공개키의 암호문의 길이가 대칭키에 비해 현저히 짧지는 않다.

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 기기에 서의 컨텐츠 소비를 방지한다.

① DRM
② IPS
③ GPL
④ VPN
⑤ DOM
정답 체크 :
(1) DRM : 콘텐츠 제공자의 권리와 이익을 안전하게 보호하며 불법복제를 막고 사용료 부과와 결제대행 등 콘텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다.
오답 체크 :
(2) IPS : 수동적인 방어 개념의 침입 차단 시스템(Firewall)이나 침입 탐지 시스템(IDS)과 달

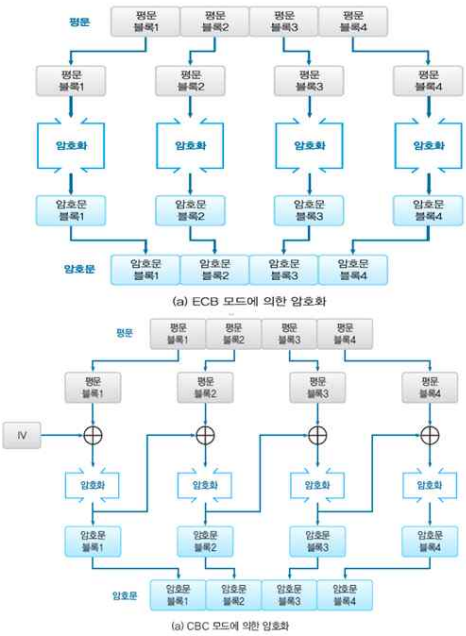
리 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다.
(3) GPL : 공개운영체계인 GNU 프로젝트로부터 제공되는 소프트웨어에 적용되는 라이센스. 사용자들이 소프트웨어를 자유롭게 공유하고 내용을 수정하도록 보증하는 것을 말한다.
(4) VPN : 인터넷망(public network)을 전용선(private network)처럼 사용할 수 있도록 특수 통신체계와 암호화기법을 제공하는 서비스로 기업 본사와 지사 또는 지사 간에 전용망을 설치한 것과 같은 효과를 거둘 수 있으며, 기존 사설망의 고비용 부담을 해소하기 위해 사용한다.
(5) DOM : 텍스트 파일로 만들어져 있는 웹 문서를 브라우저에 렌더링하려면 웹 문서를 브라우저가 이해할 수 있는 구조로 메모리에 올려야 한다. 브라우저의 렌더링 엔진은 웹 문서를 로드한 후, 파싱하여 웹 문서를 브라우저가 이해할 수 있는 구조로 구성하여 메모리에 적재하는데 이를 DOM이라 한다. 즉 모든 요소와 요소의 어트리뷰트, 텍스트를 각각의 객체로 만들고 이들 객체를 부자 관계를 표현할 수 있는 트리 구조로 구성한 것이 DOM이다. 이 DOM은 자바스크립트를 통해 동적으로 변경할 수 있으며 변경된 DOM은 렌더링에 반영된다.

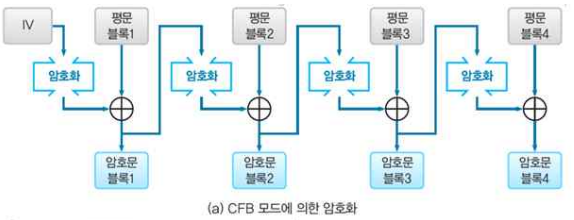
7. 다음 중 공격자가 통신 프로토콜에 직접 개입하지 않고 감 청(eavesdropping) 또는 감시(monitoring)만을 수행하는 수동적 공격(passive attack)으로 분류될 수 있는 것은?
① 가장(masquerade)
② 재사용(replay)
③ 서비스 거부(denial of service)
④ 메시지 변조(modification of message)
⑤ 트래픽 분석(traffic analysis)
정답 체크 :
(5) 트래픽 분석 : 기밀성을 해치는 소극적 공격이다.
오답 체크 :
(1) 가장 : 무결성을 해치는 적극적 공격이다.
(2) 재사용 : 무결성을 해치는 적극적 공격이다.
(3) 서비스 거부 : 가용성을 해치는 적극적 공격이다.
(4) 메시지 변조 : 무결성을 해치는 적극적 공격이다.
Tip! : 다음은 공격 방법, 적극적/소극적, 기밀성/무결성/가용성 관점에서 정리한 표이다.

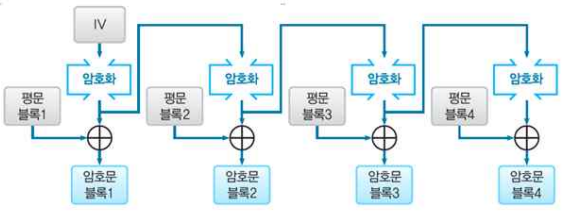
Attacks	*Passive/Active*	*Threatening*
Snooping (Sniffing) Traffic analysis	Passive	Confidentiality
Modification Masquerading (Spoofing) Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

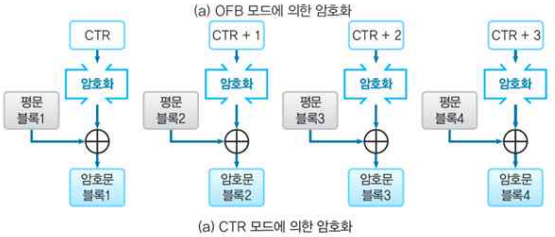
8. 다음의 블록 암호 모드 중 각 평문 블록을 이전 암호문 블록과 XOR한 후 암호화되어 안전성을 높이는 모드는?

① ECB 모드
② CBC 모드
③ CTR 모드
④ OFB 모드
⑤ CFB 모드
정답 체크 :
(2) CBC : 이전 단계의 암호문 블록과 현재 단계의 평문 블록을 XOR해서 암호문 블록을 만든다.
오답 체크 :
(1) ECB : 개별적으로 평문 블록을 암호화해서 암호문 블록으로 만든다.
(3) CTR : 개별적으로 카운터를 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
(4) OFB : 이전 단계의 출력 블록(평문 블록과 XOR해서 암호문 블록을 만들기 전 단계)을 암호화한 후 평문 블록과 XOR해서 암호문 블록을 만든다.
(5) CFB : 이전 단계의 암호문 블록을 암호화한 후 현재 단계의 평문 블록과 XOR해서 암호문 블록을 만든다.
이들을 그림으로 나타내면 다음과 같다.









9. PKI에 관한 다음의 설명 중 옳지 않은 것은?
① PKI란 public key infrastructure의 약어로 공개키 암호 알고리듬(Algorithm)을 적용하고 인증서를 관리하기 위 한 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.

정답 체크 :
(4) 대상의 서명 : 변조를 막기 위해 대상의 서명이 아닌 CA(인증기관)의 서명이 추가된다.
오답 체크 :
(1) PKI : 공개키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택사양의 총칭이다.
(2) X.509 : 암호학에서 공개키 인증서와 인증알고리즘의 표준 가운데에서 공개 키 기반(PKI)의 ITU-T 표준이다. X.500 표준안의 일환으로 시작되었다. 인증기관 고유 식별자와 주체고유식별자가 추가된 v2가 발표되었으며, 확장 기능(Extension)을 이용해 데이터를 추가할 수 있는 v3가 발표되어 현재 쓰이고 있다.
(3) CA : 인증서의 발행과 폐지는 인증기관(CA)에서 수행한다.
(5) OCSP : 인증서 폐지 및 효력 정지 상태를 파악해 사용자가 실시간으로 인증서를 검증할 수 있는 프로토콜이다.

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.
정답 체크 :
(3) 10라운드 : 16라운드를 거친다.
오답 체크 :
(1) 1970년대 : 1972년(미국 NBS(NIST)에서 필요성 절감), 1974년(IBM에서 루시퍼 알고리즘 제안), 1975년(DES 발표)
(2) 64비트 블록 : 키 길이가 64비트이다. 56비트의 키에 패리티 비트가 8비트 붙는다.
(4) 56비트의 키 : 해당 키 길이로 인해 보안 강도가 낮다.
(5) Feistel 암호 : 암호화 방식이 특정 계산 함수의 반복으로 이루어진다. 이 때, 각 과정에 사용되는 함수는 라운드 함수(round function)이라고 부른다. 예를 들어, 블로피시, SEED 등이 페이스텔 구조를 가진다.

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.
정답 체크 :
(4) 모든 공격 : 어떤 네트워크 보안 장비(Firewall, IDS, IPS, DPI)도 침입자의 모든 공격을 완벽하게 대처할 수 없다. 왜냐하면 대부분의 장비가 기존에 알려진 공격을 막고, 알려지지 않는 공격을 막을 수 있다고 하더라도 정상적인 패킷을 막을 수 있는 가능성이 존재한다. 그러므로 침입자의 모든 공격을 완벽하게 막는 것은 불가능하다. 미래에 인공지능과 빅데이터가

완벽하게 활성화되면 가능할지도 모른다.
오답 체크 :
(1) 하드웨어와 소프트웨어 : 컴퓨터에 소프트웨어적으로 동작할 수도 있고(예 : MS 윈도우 방화벽), 하드웨어적으로 장비를 만들어 동작할 수도 있다.
(2) IP 필터링 : 기본적으로 IP와 Port를 기반으로 필터링을 수행한다.
(3) 내부 정보유출 : 방화벽은 외부 네트워크와 내부 네트워크 사이에서 동작하므로 내부에서 발생하는 정보유출을 막을 수 없다.
(5) 라우터 또는 컴퓨터 : 컴퓨터는 소프트웨어 방화벽에 사용되고, 라우터는 예전에 사용되던 방식이다. 현재는 독립적인 방화벽 장비로서 네트워크에서 동작한다.

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)
정답 체크 :
(5) 쿠키 : 고객이 특정 홈페이지를 접속할 때 생성되는 정보를 담은 임시 파일로 크기는 4KB 이하로 작다. 쿠키는 애초 인터넷 사용자들의 홈페이지 접속을 돕기 위해 만들어졌다. 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다.
오답 체크 :
(1) 애플릿 : 웹 상에서는 자바와 같이 객체지향 프로그래밍 언어를 써서 웹 페이지와 함께 사용자에게 보낼 수 있도록 작게 만든 프로그램을 애플릿이라고 부른다. 자바 애플릿은 애니메이션이나, 간단한 계산 그리고 사용자가 서버에 별도의 요청을 하지 않고서도 수행할 수 있는 단순한 작업들을 수행할 수 있다.
(2) URL : 다양한 서비스(HTTP, FTP, 이메일, Telnet 등)를 제공하는 수많은 서버들로부터 필요한 정보를 획득하기 위해 이들의 위치를 표시하는 체계가 필요한데 이를 위해 URL이 사용된다. (URL의 상위 개념으로 URI가 있다.)
(3) 공개키 인증서 : 전자 서명의 검증에 필요한 공개키(전자서명법에는 전자서명검증정보로 표기)에 소유자 정보를 추가하여 만든 일종의 전자 신분증(증명서)이다. 공인 인증서, 공개키 증명서, 디지털 증명서, 전자 증명서 등으로도 불린다. 공인인증서는 개인키(전자서명법에는 전자서명생성정보로 표기)와 한 쌍으로 존재한다.
(4) DOI : 책이나 잡지 등에 매겨진 국제표준도서번호(ISBN)와 같이 모든 디지털 콘텐츠에 부여되는 고유 식별번호로 디지털 콘텐츠(객체) 식별자라 한다.

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)
정답 체크 :
(4) 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.
오답 체크 :
(1) Session hijacking : 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.
(2) Phishing : Private data(개인 정보)와 fishing(낚는다)의 합성어이다. 불특정 다수에게 메일을 발송해 위장된 홈페이지로 접속하도록 한 뒤 인터넷 이용자들의 금융정보와 같은 개인정보를 빼내는 사기기법을 말한다.
(3) Click jacking : 웹페이지상에서 HTML의 아이프레임(iframe) 태그를 사용한 눈속임 공격 방법이다. 공격자가 사용자로 하여금 알아차리지 못하게 공격자가 원하는 어떤 것을 클릭하도록 속이는 것이다. 사용자가 어떤 웹 페이지 혹은 버튼을 클릭하지만 실제로는 다른 페이지의 콘텐츠를 클릭하게 되는 것이다.
(5) Pharming : Phishing(개인 정보)과 farming(대규모 피해)의 합성어이다. DNS Spoofing과 같이 인터넷 주소창에 방문하고자 하는 사이트의 URL을 입력하였을 때 가짜 사이트(fake site)로 이동시키는 공격 기법이다.

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.
정답 체크 : (문제 오류로서 모두 정답이다.)
(1) IPsec : OSI 3계층(network layer)에서 동작한다.
(2) Tunnel mode : IP 헤더를 포함한 전체 IP 패킷에 대한 보호, 즉 네트워크, 전송, 응용

계층의 전체 데이터에 대한 보호를 목적으로 한다.
(3) IKE : 인터넷 표준 암호키 교환 프로토콜이다. 송신 측에서 수신 측이 생성한 암호키를 상대방에게 안전하게 송신하기 위한 방법이다.
(4) AH : IPSec에서 인증과 무결성을 제공하기 위해서 사용된다.
(5) ESP : IPSec에서 기밀성(암호화)을 제공하기 위해서 사용한다.

15. DDoS(Distributed Denial of Service)에 대한 설명으로 옳지 않은 것은?
① 좀비 PC가 되지 않기 위해서는 신뢰할 수 없는 기관의 프로그램은 설치하지 않는 것이 좋다.
② DDoS공격은 특정 서버에 침입하여 자료를 훔쳐가거나 위조시키기 위한 것이다.
③ 좀비 PC가 되면 자신도 모르게 특정사이트를 공격하는 수단으로 이용될 수 있다.
④ 공격을 당하는 서버에는 서비스가 중지될 수 있는 큰 문제가 발생한다.
⑤ 좀비 PC는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.
정답 체크 :
(2) DDoS 공격 : 해당 설명은 해킹에 해당된다. 해킹은 IP Spoofing 등을 이용한다.
오답 체크 :
(1) 좀비 PC(프로그램 설치) : DDoS에서 봇(Bot, 악성 코드)에 감염된 컴퓨터를 말한다.
(3) 좀비 PC(특정 사이트 공격) : 공격자가 마스터를 통해 좀비 PC를 제어하여 특정 사이트를 공격한다.
(4) 서비스 중지 : DDoS 공격의 목적이 서버를 무력화해서 Denial of Service 상태를 만드는 것이다.
(5) 좀비 PC(하드디스크 손상) : 하드디스크와 데이터를 파괴해 정상적으로 부팅할 수 없게 만든다.

16. 다음의 접근 제어 모델 중 대상 기반의 접근 제어가 아니라 특정한 역할들을 정의하고 각 역할에 따라 접근 권한을 지정 하고 제어하는 방식은?
① ACL
② DAC
③ RBAC
④ MAC
⑤ Capability
정답 체크 :
(3) RBAC : 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
오답 체크 :
(1) ACL : 주체의 관점에서 객체들에 대한 권한을 다루거나 객체의 관점에서 주체들의 권한을 다룬다.
(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.
(4) MAC : 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교

함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(5) Capability (List) : 주체의 관점에서 한 주체가 접근 가능한 객체와 권한을 명시한 목록으로 안드로이드 플랫폼과 분산 시스템 환경에서 많이 사용한다.

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.
정답 체크 :
(1) IDS(사전 차단) : IDS는 탐지 기능만 있고, 사전 차단 기능은 IPS 혹은 DPI에 있다.
오답 체크 :
(2) signature 기반 감지 방식 : 패킷의 페이로드(payload, 7계층 정보)를 시그너처(웜이나 바이러스가 가지는 특정 문자열)와 비교하여 일치하면 해당 패킷을 폐기한다.
(3) anomaly 기반 감지 방식 : 비정상적인 패킷을 차단하다. 예를 들어, 초당 100개의 syn 패킷을 받기로 설정하면 초과하는 패킷은 비정상 패킷이므로 해당 패킷은 버린다.
(4) network IDS : 네트워크상에서 오고 가는 패킷들을 검사할 수 있으므로 네트워크 관련 공격(DoS 공격 등)을 감지할 수 있다.
(5) 상호보완적 : 방화벽에서 1차로 차단하고 나머지를 IDS에서 차단하는 방식으로 동작한다. 현재는 모든 네트워크 보안 기술을 하나의 장비에 넣는다.

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.
정답 체크 :
(2) salt : 패스워드에 salt를 추가하면 같은 패스워드라도 다르게 표현할 수 있다. 그러므로 salt는 사전 공격(사전 파일에 주어진 패스워드를 차례대로 공격)에 강하다.
오답 체크 :
(1) OTP : OTP는 사람이 소지하고 다니므로 소유 기반 인증의 일종이다.
(3) PIN : PIN은 사람이 기억해야 하므로 지식 기반 인증의 일종이다.

(4) 오인식, 오거부 : 바이오 인식(지문 인식, 얼굴 인식, 홍채 인식 등)에서 발생한다.
(5) ID 카드 : ID 카드는 사람이 소지하고 다니므로 소유 기반 인증의 일종이다.

19. 다음에서 설명하고 있는 공격은?

이 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어 쓰는 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
정답 체크 :
(1) Buffer overflow : 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다.
오답 체크 :
(2) 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.
(3) IP spoofing : 트러스트(Trust)로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다.
(4) Format string : printf() 사용된 %s와 같은 문자열을 가리켜 포맷 스트링이라 한다. 포맷 스트링을 조작하면 임의의 메모리 주소의 쓰기 혹은 복귀 주소를 변경할 수 있다.
(5) Privilege escalation : 권한 상승은 SetUID가 설정된 파일 등을 이용해서 일반 사용자로부터 보호된 리소스에 접근할 수 있는 권한을 얻기 위한 행동이다.

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 공유 되어서는 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.
정답 체크 :
(1) 개인정보 보호위원회의 위원 : "개인정보 보호법" 제7조(개인정보 보호위원회) 상 위원은 다음 각 호의 어느 하나에 해당하는 사람을 대통령이 임명하거나 위촉한다. 1. 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람, 2. 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람, 3. 그 밖에 개인정보에 관한 학식과 경험이 풍부한

사람

오답 체크 :

(2) 정보주체 : 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

(3) 개인정보의 제3자 제공 : "개인정보 보호법" 제17조(개인정보의 제공) 상 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우, 2. 제15조제1항제2호(법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우)·제3호(공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우) 및 제5호(정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우)에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

(4) 1년간 보관 : 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

(5) 보호 대상이 되는 개인 정보 : 개인 정보란 살아 있는 개인에 관한 정보를 의미한다.