2020-해경1차-정보시스템보안-해설-곽후근

1. 다음 중 스테가노그래피(Steganography)에 대한 설명으로 가장 옳지 않은 것은?
① 그림의 픽셀 중 일부를 저장하고 싶은 데이터로 대체하여 저장하는 방법으로 원본 그림과 대체된 그림을 육안으로 구별할 수 있다.
② 스테가노그래피는 민감한 정보의 존재 자체를 숨기는 기술이다.
③ 텍스트 · 이미지 파일 등과 같은 디지털화된 데이터에 비밀 이진(Binary) 정보가 은닉될 수 있다.
④ 9.11 테러 당시 테러리스트들이 대화를 은닉하기 위해 사용한 기법이다.
정답 체크
(1) 원본 그림과 대체된 그림을 육안으로 구별할 수 없다.
오답 체크
(2) 메시지의 내용을 읽지 못하게 하는 것이 아니라, 메시지의 존재 자체를 숨기는 기법이다. 메시지를 숨겨 넣는 방법을 알게 되면 메시지의 내용은 금방 노출된다.
(3) 전체 데이터에 일부분의 정보를 숨긴다. (디지털 데이터 2진 데이터이므로 비밀 이진 정보를 은닉한다.)
(4) 사진이나 텍스트 메시지 속에 데이터를 잘 보이지 않게 은닉하는 기법으로서, 9.11 테러 당시 테러리스트들이 그들의 대화를 은닉하기 위해 사용한 기법이다.

2. 다음 내용에 해당하는 공개키 기반 구조(PKI, Public Key Infrastructure)의 구성 요소로 옳은 것은?

· 사용자에 대한 공개키 인증서를 생성하고 이를 발급한다. · 필요 시 사용자 인증서에 대한 갱신 및 폐기 기능을 수행한다. · 인증서 폐기 목록(Certificate Revocation List)을 작성한다.

① 사용자
② 등록기관
③ 인증기관
④ 디렉토리
정답 체크
(3) 인증서의 관리를 행하는 기관으로, 키 쌍을 작성한다(이용자가 작성하는 경우도 있다). 그리고 공개 키 등록 때 본인을 인증하고, 인증서를 작성해서 발행하거나 인증서를 폐지한다.
오답 체크
(1) PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과 등록되어 있는 공개 키를 사용하고 싶어 하는 사람을 의미한다.
(2) 인증기관(CA)의 일 중 「공개키의 등록과 본인에 대한 인증」을 대행하는 기관이다.
(4) 인증서를 보존한다. PKI 이용자가 인증서를 입수할 수 있도록 한 데이터베이스이다. 인증서 저장소(repository)라고도 한다.

3. 웹에 관한 정보 노출, 보안 취약점, 악성 파일 및 스크립트 등을 연구하며, 10대(TOP 10) 웹 애플리케이션의 취약점을 발표하는 기관은?
① Open Web Application Security Project
② Web Application Security Working Group

③ IETF Web Security Working Group
④ World Wide Web Consortium
정답 체크
(1) 오픈소스 웹 애플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션의 취약점을 발표했다.
오답 체크
(2) 웹 어플리케이션의 보안을 개선하기 위해 보안과 정책 메커니즘을 개발하기 위해 조직되었다.
(3) 현재(2022년) 활동 중인 워킹 그룹이 아니다.
(4) 월드 와이드 웹을 위한 표준을 개발하고 장려하는 조직으로 팀 버너스 리를 중심으로 1994년 10월에 설립되었다. W3C는 회원기구, 정직원, 공공기관이 협력하여 웹 표준을 개발하는 국제 컨소시엄이다.

4. 다음은 어떤 공격에 대한 설명인가?

웹 사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로 사용자로 위장한 공격자가 웹 사이트에 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 크로스 사이트 스크립팅(Cross-Site Scripting : XSS)
정답 체크
(4) 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) HTTP 통신 시에 세션 관리를 위해 사용하는 세션 ID를 스니핑 등을 통해서 도용하는 기법이다.
(2) 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) 웹페이지상에서 HTML의 아이프레임(iframe, 프레임 안의 프레임) 태그를 사용한 눈속임 공격 방법이다. 공격자가 사용자로 하여금 알아차리지 못하게 공격자가 원하는 어떤 것을 클릭하도록 속이는 것이다.

5. 다음 중 Windows에서 제공하는 기본 방화벽 설명으로 가장 옳지 않은 것은?
① 연결 보안 규칙의 종류에는 격리, 인증 예외, 서버 간, 터널, 사용자 지정 등이 있다.
② 바이러스 및 웜 뿐만 아니라 스팸이나 원하지 않은 메일의 수신도 차단 할 수 있다.
③ 해커나 악성 소프트웨어가 네트워크나 인터넷을 통해 사용자 컴퓨터에 액세스하지 못하도록 방지

하는 기능이다.
④ 새로운 프로그램을 차단할 때 알림을 표시할 수 있도록 설정할 수 있다.
정답 체크
(2) 바이러스 및 웜은 백신에서 차단하고, 스팸 메일은 스팸 메일 필터링 장비(외부에 따라 존재하거나 메일에서 지원)에서 차단한다.
오답 체크
(1) 격리는 도메인에 가입된 컴퓨터를 도메인 외부에 있는 컴퓨터로부터 격리할 수 있는 규칙을 만들 때 사용한다. 인증 예외는 다른 연결 보안 규칙에 관계없이 지정한 컴퓨터가 인증을 수행하지 않아도 되는 규칙을 만들 수 있다. 서버 간은 데이터베이스 서버와 다른 컴퓨터 간의 트래픽이나 인트라넷 컴퓨터와 다른 서버 간의 트래픽을 인증할 수 있다. 터널은 전송 모드 대신 터널 모드를 사용하여 두 컴퓨터 간의 보안을 설정한다. 그리고 사용자 지정은 특별 설정이 필요한 규칙을 만들 때 사용한다.
(3) inbound(외부에서 컴퓨터로 들어오는 것)와 outbound(컴퓨터에서 외부로 나가는 것) 정책을 적용할 수 있다.
(4) 사용 경험을 반추해보면 새로운 프로그램을 시작할 때 항상 사용자의 허락을 받음을 알 수 있다.

6.「 개인정보 보호법 」상 다음 업무를 수행하는 자는?

· 개인정보 보호 계획의 수립 및 시행 · 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선 · 개인정보 처리와 관련한 불만의 처리 및 피해 구제 · 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축 · 개인정보보호 교육 계획의 수립 및 시행 · 개인정보 파일의 보호 및 관리·감독

① 개인정보 담당자
② 개인정보 보호책임자
③ 개인정보 취급자
④ 개인정보 처리자
정답 체크
(2) 개인정보 보호법 제31조(개인정보 보호책임자의 지정) ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.
② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.
1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용 · 남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리 · 감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무
오답 체크
(1) 조직에서 개인정보를 담당하는 자로 통상적으로 사용되는 용어는 아니다.

(3) 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘 · 감독을 받아 개인정보를 처리하는 자이다(개인정보보호법 제28조).
(4) 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

7. 사용자 인증을 위한 접근방법으로는 사용자가 알고 있는 것, 사용자가 가지고 있는 것, 사용자 자신의 특성을 이용하는 것 등이 있다. OTP(One Time Password)에 대한 설명으로 가장 옳지 않은 것은?
① 질의응답 방식은 사용자가 직접 질의 값을 입력 하면 응답 값인 OTP가 생성되어 보안성이 높다.
② OTP는 일반적으로 OTP 토큰을 이용하므로 소유에 의한 인증 기법이다.
③ 일반적으로 사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다.
④ 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.
정답 체크
(3) 소유 기반 인증은 생체 기반 인증에 비해 식별 오류 발생 가능성이 낮다.
오답 체크
(1) 입력값이 매번 임의의 값이 된다는 측면에서는 안전성을 갖추고 있으나, 네트워크 모니터링(스니핑)에 의해 전송되는 값들이 노출될 경우 매우 취약해진다는 단점이 있다. 또 서버와 클라이언트 사이의 통신 횟수도 비교적 많이 요구된다.
(2) OTP 토큰은 OTP 기기를 의미하고 소유 기반이다(소지하고 있음).
(4) OTP는 4가지 방식(S/KEY 방식, 시간 동기화 방식, 이벤트 동기화 방식, 도전-응답 방식)이 존재하고, 각 방식에 따라 사용자나 인증 서버에 부담이 발생할 수 있다.

8. 다음 중 유닉스계열의 시스템에서 핵심부분인 커널 (Kernel)에 대한 설명으로 가장 옳지 않은 것은?
① 유닉스 시스템의 구성은 커널(Kernel), 셸(Shell), 파일시스템(File System)으로 구성되며, 커널은 프로세스, 메모리, 입출력 관리 등을 수행한다.
② 커널(Kernel)은 데몬(Daemon) 프로세스를 실행 하고 관리한다.
③ 유닉스계열의 시스템이 부팅될 때 가장 먼저 읽혀지는 핵심 부분으로 보조기억장치에 상주한다.
④ 커널(Kernel)은 셸(Shell)과 상호 연관되어 작업을 수행한다.
정답 체크
(3) 주기억장치에 상주한다.
오답 체크
(1) 커널은 자원을 관리하고, 셸은 인터페이스 역할을 수행한다.
(2) 여기서 데몬은 항상 실행중인 프로세스를 의미한다.
(4) 사용자가 쉘의 통해 커널에 명령을 내리며, 커널은 쉘을 통해 사용자에게 결과를 반환한다.

9. 다음 중 쿠키(Cookie)에 대한 설명으로 가장 옳지 않은 것은?
① 사용자가 웹 사이트에 접속할 때 사용자 컴퓨터에서 생성되어 해당 웹 서버에 임시 파일로 전송, 저장된다.
② 웹 사이트 접속 시 HTTP의 무상태성(Statelessness)을 보완하기 위해 사용되는 정보이다.
③ 보존기간에 따라 임시 쿠키와 영구 쿠키로 분류할 수 있다.

④ 사용자가 인식하지 못하는 사이에 사용자의 다양한 정보가 쿠키에 담겨 웹 서버로 전송될 수 있기 때문에 개인정보에 대한 피해가 발생 할 수 있다.

정답 체크

(1) 서버에 저장되지 않고 사용자 컴퓨터에 저장된다. 다만, 초기 접속에서 쿠키 정보가 서버에게 전송되는 것은 맞는 설명이다.

오답 체크

(2) 웹 서버는 사용자의 정보를 저장하지 않는다. 이를 보완하기 위해 쿠키(사용자 정보 저장)를 사용한다.

(3) 임시 쿠키는 세션 쿠키를 의미하고, 영구 쿠키는 4KB의 텍스트 파일을 의미한다.

(4) 쿠키에는 ID/PW, 방문 기록 등이 담겨 있으므로 개인정보에 대한 피해가 발생할 수 있다.

10. 다음 설명에 해당하는 접근통제(Access Control) 모델은?

조직의 사용자가 수행해야 하는 직무와 직무 권한 등급을 기준으로 객체에 대한 접근을 제어한다. 접근 권한은 직무에 허용된 연산을 기준으로 허용함으로 조직의 기능 변화에 따른 관리적 업무의 효율성을 높일 수 있다. 사용자가 적절한 직무에 할당되고, 직무에 적합한 접근 권한이 할당된 경우에만 접근 할 수 있다.

① Mandatory Access Control

② Role-Based Access Control

③ Discretionary Access Control

④ Access Control List

정답 체크

(2) 역할 기반 접근 제어로서 지문에서 직무는 역할에 해당한다.

오답 체크

(1) 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) 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) 주체의 관점에서 객체들에 대한 권한을 다루거나 객체의 관점에서 주체들의 권한을 다룬다.

11. 다음 중 윈도우 레지스트리 키 중에서 최근 열어본 파일의 목록을 기록하고 있는 것은?

① RUN ② RecentDocs

③ Docs ④ OfficeDocs

정답 체크

(2) MRU(most recently used) 문서의 목록을 기록한다.

오답 체크

(1) 윈도우가 부팅이 되면서 자동적으로 실행이 되는 프로그램으로 이 폴더에 어떠한 파일을 넣으면 자동적으로 실행이 된다.

(3), (4) 통상적으로 윈도우 레지스트리에 사용되는 키가 아니다.

12. 다음 중 윈도우 “원격 데스크톱 연결” 명령어로 가장 옳은 것은?

① vnc ② mstsc ③ teamviewer ④ ftp

정답 체크
(2) 윈도우에서 원격으로 컴퓨터를 제어할 때 사용한다.
오답 체크
(1) 컴퓨터 환경에서 원격으로 다른 컴퓨터를 제어하는 그래픽 데스크톱 공유 시스템이다.
(3) 컴퓨터 간 원격 제어, 데스크톱 공유, 파일 전송을 위한 컴퓨터 소프트웨어 패키지이다.
(4) 파일 전송 명령어이다.

13. 다음 중 비선점(Non-preemptive) 스케쥴링 방식으로 바르게 묶인 것은?
① FCFS, SJF
② FCFS, Round Robin
③ SJF, SRT
④ SJF, Round Robin
정답 체크
(1) 이외에도 HRRN, 우선순위(비선점) 등이 존재한다.
오답 체크
(2), (3), (4) 이외에도 우선순위(선점), MLQ, MLFQ 등이 존재한다.

14. 다음 중 리눅스 계정 관리 파일 /etc/shadow에서 확인할 수 있는 정보로 가장 관련 없는 것은?
① 사용자 계정 이름
② 암호화된 사용자 패스워드
③ 사용자 패스워드 최소 길이
④ 사용자 패스워드 만료일까지 남은 기간
정답 체크
(3) shadow에 사용자 패스워드 최소 길이는 확인할 수 없다.
오답 체크
(1), (2), (4) 이외에도 마지막으로 패스워드 변경한 날, 패스워드 최소 사용 기간, 패스워드 최대 사용 기간, 계정 사용 제한 등이 포함된다.

15. 다음 중 유닉스 시스템의 로그분석에 사용하는 로그 파일에 대한 설명으로 가장 옳지 않은 것은?
① wtmp : 사용자 로그인, 로그아웃 정보를 기록
② sulog : su(switch user) 명령어 사용 정보를 기록
③ utmp : 시스템에 현재 로그인한 사용자의 정보를 기록
④ btmp : 로그인에 성공한 정보를 기록
정답 체크
(4) 실패한 로그인에 대한 정보를 기록한다.
오답 체크
(1) 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보를 기록한다.
(2) 권한 변경에 대한 기록이다.
(3) 현재 시스템에 로그인한 사용자의 상태를 기록한다.

16. 다음 중 데이터베이스 보안 요구사항으로 가장 옳지 않은 것은?
① 데이터 무결성 보장
② 비밀 데이터 관리 및 보호
③ 추론 보장
④ 사용자 인증
정답 체크
(3) 추론을 방지한다. 추론(inference)은 보통의 일반적인 데이터로부터 기밀 정보를 획득할 수 있는 가능성을 의미한다.
오답 체크
(1) 데이터의 내용을 수정할 수 있는 인가되지 않은 접근, 저장 데이터를 손상시킬 수 있는 시스템의 오류, 고장 등으로부터 DB를 보호하여야 한다.
(2) 중요 데이터에 대한 기밀성을 보호하고 인가된 사용자에 대해서만 접근을 허용해야 한다.
(4) DBMS는 엄격한 사용자 인증을 필요로 한다. DBMS의 사용자 인증은 운영체제에서 수행하는 사용자 인증보다 더욱 엄격하여야 한다.

17. 해양경찰청은 4명이 사용할 수 있는 암호 시스템을 도입하려고 한다. 대칭키 암호 시스템과 공개키 암호 시스템 도입 시 필요한 키의 개수를 각각 구분하여 순서대로 나열한 것은?
① 2개, 4개
② 4개, 6개
③ 6개, 8개
④ 8개, 10개
정답 체크
(3) 대칭키 개수 = nx(n-1)/2 = 4x3/2 = 6
공개키 개수 = 2n = 2x4 = 8

18. 다음 중 전자서명(Digital Signature)이 제공하는 기능으로 가장 옳지 않은 것은?
① 부인 방지(Non Repudiation)
② 변경 불가(Unalterable)
③ 서명자 인증(Authentication)
④ 재사용 가능(Reusable)
정답 체크
(4) 재사용 불가능이다. 서명문의 해시값을 전자서명에 이용하므로 한 번 생성된 서명을 다른 문서의 서명으로 사용할 수 없다.
오답 체크
(1) 서명자가 나중에 서명한 사실을 부인할 수 없다.
(2) 서명된 문서는 내용을 변경할 수 없기 때문에 데이터가 변조되지 않았음을 보장하는 무결성을 만족한다.
(3) 서명문의 서명자를 확인할 수 있다.

19. 다음 중 능동적 보안 공격에 해당하는 것을 모두 고르면?

㉠ 신분위장 ㉡ 도청 ㉢ 메시지 변조 ㉣ 트래픽 분석 ㉤ 서비스 거부

① ㉠, ㉡, ㉢
② ㉠, ㉢, ㉤
③ ㉡, ㉢, ㉣
④ ㉢, ㉣, ㉤
정답 체크
(2) 신분위장, 메시지 변조는 무결성 공격이다. 서비스 거부는 가용성 공격이다.
오답 체크
(1), (3), (4) 도청, 트래픽 분석은 기밀성 공격이다.

20. 리눅스 운영체제에서 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은? (단, kcg.txt는 일반파일이다.)

```
chmod 761 kcg.txt
```

① -rwxr-x—x
② -rwxrw---x
③ -rwxr-x---
④ -rw-r-----
정답 체크
(2) rwx는 7(=4+2+1)이고, rw-는 6(=4+2)이고, --x는 1(=1)이다.
오답 체크
(1) chmod 751 kcg.txt이다.
(3) chmod 750 kcg.txt이다.
(4) chmod 640 kcg.txt이다.