# 2016년 국가직 9급 정보보호직 총평

-지안학원 조상진 선생

## 1. 문제분석

### (가) 전체적으로 평이한 수준

행정자치부 사전 예고대로 시스템보안부터 어플리케이션 보안파트가 정보시스템 보안 과목에 출제되었고, 네트워크 보안파트도 동일 범위였습니다. 3년전 정보보호론 첫해 시험과 같이 전체적으로 평이하게 출제된 것 같습니다. 많은 수험생들이 정보보호론이나 정보보안기사를 접해서 체감난이도는 더 낮았을 것 같습니다.

### (나) 정보보호론과 차이점

이론 위주의 시험과 다르게 운영체제 명령어를 알고 있는지, 툴에 대한 지식 등을 물어봄으로써 정보보호직만의 차별화로 가려는 시도가 보입니다. 정보보안기사와 같이 소스코드나 로그 문제가 1문제가 출제되었는데, 향후 실무형의 문제비율이 점차 들어날 것 같은 생각듭니다. 왜냐하면 정보보안기사 문제 스타일과 유사하고, 참조되는 대학교재도 동일한 것으로 봐서 약간 실무형쪽으로 진행되고, 이론도 정보보호론보다는 심화되어 들어갈 것으로 판단됩니다.

## 2. 탑스팟 정보보호직 적중률 분석

### (가) 정보시스템보안 적중률(91~95%)

컴퓨터기반 사회공학 기법과 버퍼오버플로우의 대응책 중 carnary(밀고자, 카나리아)는 교재에 언급은 되어 있지만, 약간 심화해서 출제된 것 같습니다. 나머지는 이론서(정보보호론, 정보보호직), 기출700제, 적중800제, 정보보호직 심화강의에서 대다수 다룬 내용입니다. 전체적으로 탑스팟 교재에서 91 ~ 95%정도의 적중률을 보였습니다.

### (나) 네트워크보안 적중률(95~99%)

대부분의 문제들이 이론서(정보보호론, 정보보호직), 기출700제, 적중800제, 정보보호직 심화강의에서 대다수 다룬 내용입니다. 전체적으로 탑스팟 교재에서 95 ~ 99%정도의 적중률을 보였습니다.

## 3. 향후 학습방향

### (가) 정보보호론에 먼저 깊게 공부하라.

정보보호직 시험이 올해 2번 시행되었습니다. 국민안전처 시험문제는 기출700제와 적중800제와 지문까지 동일한 문제들이 다수 출제되어 커트라인이 상당히 높았습니다. 이번에 시행된 행정자치부 시험도 정보보호론에서 조금 심화되어 들어가는 경향을 보이고 있습니다. 정보보호직을 제대로 준비하려면 먼저 정보보호론을 먼저 공부하시고, 정보보호직에 특화된 학습을 추가로 하면 좋은 성적을 거둘 수 있을 것 같습니다.

## 4. 지안 공무원학원 향후 수업 안내

### (가) 정보보호직 수업

정보보호론 기본/심화 학습 후에 2017년 선발인원이 결정되면 학원측과 상의 후에 개강하겠습니다. 정보보호직은 지안이 책임집니다.

### (나) 2017년 정보보호론 개정판

- 개정판 강의 : 2016년 9월 ~

# 2016년 국가직 9급
# 정보시스템 보안

–2016년 4월 9일 시행

## 1.

모바일 운영체제인 iOS와 안드로이드의 보안 체계에 대한 설명으로 옳지 않은 것은?

① iOS는 모든 앱에 대한 코드 무결성 점검을 수행하여 설치를 제한한다.
② iOS와 안드로이드 모두 프로그램의 실행 권한이 일반 사용자에게 있다.
③ iOS는 애플의 CA를 통하여 앱을 서명 및 배포하고, 안드로이드는 개발자가 서명 및 배포한다.
④ 보안 통제권이 iOS는 애플에 있고, 안드로이드는 개발자나 사용자에게 있다.

| 구분 | iOS | 안드로이드 |
|---|---|---|
| 운영체제 | Darwin UNIX에서 파생하여 발전한 OS X의 모바일 버전 | 리눅스 커널(2.6.25)을 기반으로 만들어진 모바일 운영체제 |
| 보안 통제권 | 애플 | 개발자 또는 사용자 |
| 프로그램 실행권한 | 관리자(root) | 일반 사용자 |
| 응용 프로그램에 대한 서명 | 애플이 자신의 CA를 통해 각 응용프로그램을 서명하여 배포 | 개발자가 서명 |
| 샌드박스 | 엄격하게 프로그램 간 데이터 통신 통제 | iOS에 비해 상대적으로 자유로운 형태의 어플리케이션의 실행이 가능 |
| 부팅 절차 | 암호화 로직으로 서명된 방식에 의한 안전한 부팅 절차 확보 | – |
| 소프트웨어 관리 | 단말 기기별 고유한 소프트웨어 설치 키 관리 | – |

오답피하기 ② 응용 프로그램의 실행권한은 iOS는 관리자(root)에 있고, 안드로이드는 개발자 또는 사용자에게 있다.

정답 ②

## 2.

시스템 접근을 허락받은 후에 그 시스템의 어떤 기능 또는 서비스를 이용할 수 있도록 필요한 권한을 부여하는 것은?

① 식별(identification)
② 인증(authentication)
③ 인가(authorization)
④ 평가(evaluation)

◦ 접근통제 절차는 식별, 인증, 인가로 구성되었으며, 대부분의 기업 및 조직 내 시스템은 이러한 3단계를 원칙으로 하여 시스템을 구성하고 있다.

오답피하기 ③ 인가는 권한부여라고도 하며, 인증된 주체에게 접근을 허용하고 특정 업무를 수행할 권리를 부여하는 과정이다.

정답 ③

## 3.

컴퓨터 기반 사회공학적 공격기법에 해당하지 않는 것은?

① 피싱(phishing)
② 파밍(pharming)
③ 스미싱(smishing)
④ 스푸핑(spoofing)

〈인간 기반 사회공학 기법〉
◦ 직접적인 접근
◦ 도청
◦ 어깨너머로 훔쳐보기
◦ 휴지통 뒤지기
〈컴퓨터 기반 사회공학 기법〉
◦ 시스템 분석
◦ 악성 소프트웨어 전송
◦ 인터넷을 이용한 사회공학 공격
◦ 피싱(Phishing)
◦ 파밍(Pharming)

오답피하기 ④ 스푸핑은 컴퓨터들이 통신하는 과정에 필요한 주소를 임의의 다른 값으로 변조하는 행위나 위조 지문을 악용하여 지문 인식 시스템을 속이고 통과하는 행위 등 다양한 형태를 가진다. 보기에서 컴퓨터 기반 사회공학적 공격과는 가장 거리가 멀다.

정답 ④

## 4.

다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?

보기

chmod 751 test.c

① -rwxr-x--x
② -rwxrw---x
③ -rwxr-x---
④ -rw-r-----

| 문자값 | 접근 권한 |
|---|---|
| r(4) | 파일에 대한 읽기 권한과 디렉터리 내에 있는 파일명을 읽을 수 있는 권한 |
| w(2) | 파일에 대한 쓰기 권한과 디렉터리 내에 파일을 생성하거나 삭제할 수 있는 권한 |
| x(1) | 파일에 대한 실행 권한과 디렉터리 내에서 탐색을 위해 이동할 수 있는 권한 |
| - | r, w, x에 대한 권한이 없는 경우 해당 자리를 대체 |

오답피하기 ① 접근권한이 751이므로 user는 rwx, group은 r-x, other는 - - x이 된다.

정답 ①

## 5.

FTP 보안에 대한 설명으로 옳지 않은 것은?

① 임의의 계정으로 로그인 시도를 반복적으로 수행하여 사용자 계정의 패스워드를 유추할 수 있는 취약점이 있다.
② 사용자 인증정보 유출 방지를 위한 보안 대책으로 SCP, SFTP, FTPS 등이 있다.
③ 익명 FTP는 모든 사용자에게 동일한 사용자 아이디와 유효한 사용자 이메일 주소를 패스워드로 요구한다.
④ FTP 보안 대책으로 반드시 서비스 사용이 필요하지 않은 경우 FTP 서비스 사용을 금지하는 것이 좋다.

오답피하기 ③ 익명 ftp는 아이디로 anonymous나 ftp를 사용한다. 그리고 패스워드로는 guest 또는 이메일 주소를 사용하곤 한다. 이때 입력하는 비밀번호는 실제 비밀번호가 아니며 누가 접속하고 있는지 서버가 로그에 기록하는데 쓰일 뿐으로 유효한이라는 표현은 적절치 않다고 볼 수 있다.

정답 ③

## 6.

SSL 프로토콜 스택에 포함되지 않는 것은?

① handshake 프로토콜
② alert 프로토콜
③ record 프로토콜
④ user authentication 프로토콜

◦ Record 프로토콜은 운반자이며, 응용 계층으로부터 오는 데이터뿐만 아니라 다른 3개의 프로토콜로부터 오는 메시지를 전송한다. Record 프로토콜에서 오는 메시지는 보통 TCP인 전송 계층의 페이로드이다.
◦ Handshake 프로토콜은 Record 프로토콜에 대한 보안 매개변수를 제공한다. 암호 집합을 설정하고 키와 보안 매개변수를 제공한다. 또한 필요하다면 클라이언트가 서버에 대해 그리고 서버가 클라이언트에 대해 인증된다.
◦ ChangeCipherSpec 프로토콜은 암호학적 비밀을 신속하게 보내는 데 사용된다. Alert 프로토콜은 비정상 조건을 알리는데 사용된다.

오답피하기 ④ SSL 프로토콜 스택에 user authentication 프로토콜은 없다.

정답 ④

## 7.

전자우편의 보안성 향상을 위해 개발된 것이 아닌 것은?

① SMTP
② PGP
③ S/MIME
④ PEM

◦

오답피하기 ① SMTP는 TCP/IP의 상위층 응용 프로토콜의 하나로, 컴퓨터 간에 전자 우편을 전송하기 위한 프로토콜이다. RFC 821에 규정

되어 있다. 2개의 전자 우편 시스템 간에 어떻게 대화하는지를 지정하고 전자 우편을 전송하기 위하여 교환하는 제어 메시지의 형식을 규정한다. 이는 단순한 전자우편 전송 프로토콜로 보안성 향상 프로토콜과는 거리가 멀다.

정답 ①

## 8.

일반적으로 이메일 형식으로 전달되며, 이메일 혹은 게시판 등에 거짓정보나 소문 등을 실어 사용자를 겁주거나 속이는 것은?

① 혹스(Hoax)
② 트로이 목마(Trojan horse)
③ 백도어(Backdoor)
④ 스파이웨어(Spyware)

◦ 조크 바이러스(Joke Virus) : 악의적인 목적이 없이 사용자의 심리적인 동요나 불안을 조장하는 가짜 바이러스이다. 웜 바이러스의 일종인 러브 바이러스의 변종이다. 가짜 바이러스라는 점에서 전자 우편이나 인터넷 메신저, 문자 메시지 등에 거짓 정보나 괴담 등을 실어 사용자들을 속이는 혹스와 비슷하다. 2000년을 전후하여 등장했는데, 해마다 만우절 무렵인 4월 전후에 많이 나타난다. 모니터 화면을 거꾸로 보여주거나, CD-ROM 드라이브가 저절로 열리거나, 하드 디스크 드라이브가 포맷하는 화면이 보이는 등 형태에 따라 여러 모습을 보인다. 가장 큰 특징은 공통적으로 악성바이러스 흉내를 낸다는 점이다.

오답피하기 ① 가짜 바이러스(virus hoax) : 컴퓨터 바이러스에 관하여 공신력 있는 기관을 사칭하거나 복잡한 기술 용어를 사용하여 사용자를 속이는 허위 정보이다. 전자 우편, 인터넷 메신저, 문자 메시지 등을 이용하여 거짓 정보 또는 유언비어, 괴담 등을 마치 사실인 것처럼 꾸며 사용자를 속인다.

정답 ①

## 9.

클라이언트 측에서 웹사이트에 접속할 때 발생하는 HTTP 에러코드와 이의 원인을 설명한 것으로 옳지 않은 것은?

① 401 Unauthorized : 특정 웹사이트에 접속하기 위해 정확한 사용자 아이디와 암호를 입력하여야 하는데, 잘못된 정보를 입력하였을 경우
② 403 Forbidden : 다른 요청이나 서버의 구성과 충돌이 발생할 경우
③ 404 Not Found : URL이나 링크가 변경되어 요청한 주소의 페이지가 없을 경우
④ 414 Request-URI Too Long : 요청에 사용된 URL이 서버가 감당할 수 없을 만큼 너무 길 경우

| | | |
|---|---|---|
| 400 | Bad request | 요청 메시지의 문법 오류 |
| 401 | Unauthorized | 요청 메시지에 적합한 인증 부족 |
| 403 | Forbidden | 클라이언트의 요청에 대해 접근을 차단하는 것을 나타냄 |
| 404 | Not found | 클라이언트가 서버에 요청한 자료가 존재하지 않음을 나타냄 |

오답피하기 ② 403 Forbidden은 클라이언트의 요청에 대해 접근을 차단하는 것을 나타낸다.

정답 ②

## 10.

다음에서 설명하는 윈도우 NTFS 파일시스템의 구조는?

보기

모든 파일 및 디렉터리에 대한 정보가 저장된다. 즉, 정보는 파일 내용들을 정의하는 속성들의 집합으로 구성된다.

① PBS
② MFT
③ 시스템 파일
④ 백업 수퍼 블록

◦ MBR(PBS) : 하드디스크의 맨 앞에 기록되어 있는 시스템 기동용 영역. PC에 전원을 인가하면 먼저 첫 번째 하드디스크의 MBR에 기록되어 있는 프로그램이 읽힌다. 이렇게 읽힌 MBR의 프로그램은 분할표(partition table)의 정보를 기점으로 기동하는 분할(partition)의 부트 섹터(boot sector : 분할의 맨 앞에 있는 OS 기동 프로그램이 기록된 부분)를 읽어서 이 섹터의 프로그램에 의해서 OS가 기동된다.

따라서 MBR의 정보가 파괴되면 PC는 기동 불능이 된다.

오답피하기 ② MFT는 볼륨이 존재하는 모든 파일과 디렉터리의 정보를 담고 있는 테이블이다. 그러므로 이 테이블을 분석하면 볼륨에 있는 모든 파일과 디렉터리에 대한 정보를 전부 알아낼 수 있다. MFT(Master File Table)은 파일시스템의 모든 파일들과 디렉터리에 대한 정보를 포함하고 있는 것으로 NTFS의 핵심이다.

정답 ②

## 11.

〈보기 1〉의 상황과 개인정보의 안전한 전달을 위해 제공되어야 할 〈보기 2〉의 정보보호서비스를 바르게 연결한 것은?

보기1

ㄱ. 갑은 송신하는 개인정보를 도청당하는 일이 없이 을에게 전달하기 원한다.
ㄴ. 갑은 송신하는 개인정보가 조작당하는 일이 없이 을에게 전달되기 원한다.
ㄷ. 갑은 통신 상대의 웹 서버가 진짜 을의 서버라는 것을 확인하고 싶다.
ㄹ. 갑은 을의 서버에 적절한 시간에 접속하여 정상적으로 요청된 내용을 수행하고 싶다.

보기

A. 기밀성 B. 무결성 C. 인증 D. 가용성

| | ㄱ | ㄴ | ㄷ | ㄹ |
|---|---|---|---|---|
| ① | A | B | C | D |
| ② | A | D | C | B |
| ③ | B | A | C | D |
| ④ | B | A | D | C |

◦ 기밀성 : 오직 인가된 사람만이 알 필요성에 근거하여 시스템에 접근해야 한다는 원칙
◦ 무결성 : 정보의 내용이 불법적으로 생성 또는 변경되거나 삭제되지 않도록 보호되어야 하는 성질
◦ 인증 : 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 성질
◦ 가용성 : 자원을 필요할 때 지체 없이 원하는 객체 또는 자원에 접근하여 사용할 수 있는 성질

오답피하기 ① 보기는 정보보호목표에 대한 각각의 정의이다.

정답 ①

## 12.

운영체제에서 제공하는 파일 및 디렉터리 관리에 대한 설명으로 옳지 않은 것은?

① 윈도우즈 NT 계열의 운영체제는 파일과 디렉터리에 대한 접근제어를 통제하기 위하여 NTFS를 사용한다.
② 윈도우즈 NTFS는 모든 권한, 수정, 읽기 및 실행, 폴더 내용보기, 읽기, 쓰기와 같은 6가지 권한을 설정하여 운영한다.
③ 유닉스 계열은 파일이나 디렉터리 등의 자원에 대한 접근 제어를 위해 소유권과 접근 권한을 할당한다.
④ 유닉스 계열에서는 'etc/passwd' 파일이나 'shadow' 파일의 읽기 및 쓰기 권한을 일반 사용자에게 부여해도 안전하다.

오답피하기 ④ /etc/passwd는 사용자 계정정보를 가지고 있고, /etc/shadow는 /etc/passwd 파일 노출 시 보안성을 높이기 위해 사용자 암호만을 별도로 저장하는 파일로 시스템관리에 중요한 파일이다. 일반 사용자에게 읽기 및 쓰기 권한을 부여하는 것은 적절치 않다.

정답 ④

## 13.

패스워드 공격에 대한 설명으로 옳지 않은 것은?

① 사용자의 패스워드는 암호화하여 저장하는 것이 안전하다.
② 패스워드를 알아내기 위하여 사용자의 신원이나 주변 정보로 패스워드를 알아내는 사회공학적 방법이 있다.
③ Brute force 공격은 사용자가 패스워드를 입력할 때 가로채는 공격이다.
④ Crypt() 함수를 이용하여 패스워드를 추측할 수 있다.

◦ crypt()는 시스템에서 사용할 수 있는 다양한 알고리즘을 사용하여

암호화한 문자열을 반환한다. 일방향 암화방법의 경우 충돌을 이용하여 패스워드를 추측할 수도 있다.

오답피하기 ③ 무차별 공격(Brute-force Attack)은 성공할 때까지 가능한 모든 조합의 경우의 수를 시도해 원하는 공격을 시도하는 해킹 방법이다. 이 경우 정확한 패스워드가 드러날 때까지 가능한 모든 문자의 나열을 시도하는 툴이 사용된다.

정답 ③

## 14.

보안이 취약한 웹 게시판이 저장 XSS 공격을 받았다고 가정했을 때, 이를 해결하기 위한 방법으로 가장 적절한 것은?

① 가상 사설망을 통해서만 사용자 게시판에 접근하도록 한다.
② 접근 권한을 설정하여 허가된 사용자만 글을 올릴 수 있게 한다.
③ 사용자 게시글 속에 있는 악성 스크립트 코드를 찾아서 제거한다.
④ SSL을 사용하여 사용자가 게시글을 올릴 수 있게 한다.

◦ XSS(Cross Site Scripting)는 공격자에 의해 작성된 스크립트가 다른 사용자에게 전달되는 것이다. 다른 사용자의 웹 브라우저 내에서 적절한 검증 없이 실행되기 때문에 사용자의 세션을 탈취하거나, 웹 사이트를 변조하거나 혹은 악의적인 사이트로 사용자를 이동시킬 수 있다.

오답피하기 ③ XSS 공격을 받았다고 판단되는 상황에서는 빨리 악성 스크립트 코드를 찾아서 제거하는 방법이 적절하다.

정답 ③

## 15.

괄호 안에 들어갈 웹의 취약점은?

보기

( )는(은) 불특정 다수를 대상으로 로그인된 사용자가 자신의 의도와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록, 송금) 등을 하게 만드는 공격이다.

① 명령 삽입 취약점
② XSS 취약점
③ 디렉터리 리스팅 취약점
④ CSRF 취약점

오답피하기 ④ 사이트 간 요청 위조(CSRF[XSRF], Cross Site Request Forgery)는 특정 웹사이트에 대해 사용자가 인지하지 못한 상황에서 사용자의 의도와는 무관하게 공격자가 의도한 행위(수정,삭제,등록 등)를 요청하게 하는 공격을 말한다. 웹 어플리케이션 사용자로부터 받은 요청에 대해서 사용자가 의도한 대로 작성되고 전송된 것인지 확인하지 않은 경우 발생 가능하고, 특히 해당 사용자가 관리자인 경우 사용자 권한관리, 게시물 삭제, 사용자 등록 등 관리자 권한으로만 수행 가능한 기능을 공격자의 의도대로 실행시킬 수 있게 된다.

정답 ④

## 16.

다음은 스택 버퍼 오버플로우 공격을 효과적으로 방어하기 위한 스택 보호 메커니즘을 서술한 것이다. ㉠ ~ ㉢에 들어갈 말을 바르게 연결한 것은?

보기

스택가드(stackguard)는 가장 잘 알려진 보호 메커니즘 중 하나이다. 이것은 GCC 컴파일러의 확장 버전으로 추가의 함수 진입과 종료 코드를 삽입한다. 추가되는 함수 진입코드는 지역변수를 위한 공간을 할당하기 전에 이전 ( ㉠ ) 주소 앞에 ( ㉡ ) 값을 기록한다. 추가되는 함수 종료 코드는 이전 ( ㉠ )를 복원하고 제어를 ( ㉢ )로 이동하는 보통의 함수 종료 연산을 수행하기 전에 ( ㉡ ) 값이 변경되었는지를 검사한다. 전통적인 스택 버퍼 오버플로우 시도는 이전 ( ㉠ )와 ( ㉢ )를 변경하기 위해 ( ㉡ ) 값을 바꾸어야 하는데, 만약 변경되었다면 프로그램을 종료하게 된다.

| | ㉠ | ㉡ | ㉢ |
|---|---|---|---|
| ① | 스택포인터 | 반환주소 | 카나리아(canary) |
| ② | 스택포인터 | 카나리아(canary) | 반환주소 |
| ③ | 프레임 포인터 | 카나리아(canary) | 반환주소 |
| ④ | 프레임 포인터 | 반환주소 | 스택포인터 |

◦ Stackguard는 가장 잘 알려진 보호 메커니즘 중 하나이다. 이것은 GCC 컴파일러의 확장 버전으로 추가적인 함수 진입과 종료 코드를 삽입한다.
◦ 즉 컴파일러가 프로그램의 함수 호출(프롤로그) 시에 ret 앞에 carnary(밀고자) 값을 주입하고, 종료(return, 에필로그) 시에 carnary 값이 변조되었는 지의 여부를 확인하여 버퍼오버플로우 공격을 탐지한다.

오답피하기 ③ 스택가드는 상위메모리[ret(return address), sftp(stack frame pointer), carnary, 버퍼]하위메모리 순서로 배치하여 carnary의 변경유무를 이용하여 방어하는 기법이다.

정답 ③

## 17.

응용 보안에 대한 설명으로 옳지 않은 것은?

① HTTPS는 웹 브라우저와 웹 서버 간의 안전한 통신을 구현하기 위해 HTTP와 SSL을 결합한 것이다.
② SET는 웹 보안을 위하여 메시지 기밀성은 제공되지만, 메시지 무결성은 제공되지 않는다.
③ 공개키기반구조(PKI)는 전자서명, 전자상거래 등이 안전하게 구현되기 위하여 구축되어야 할 기반 기술이다.
④ 스팸메일의 문제점은 인터넷망을 통해 무차별로 전송되어 원하지 않는 사람이 읽거나 처리하는 데 많은 시간과 비용을 낭비하게 된다는 것이다.

오답피하기 ② SET은 블록암호 알고리즘, 해시함수, 공개키(서명)알고리즘을 이용하여 기밀성, 무결성, 인증, 부인방지 서비스를 제공한다.

정답 ②

## 18.

트립와이어(tripwire)에 대한 설명으로 옳지 않은 것은?

① 파일의 무결성을 검사하는 도구이며, 해쉬 알고리즘을 이용하여 시스템에 존재하는 파일에 관한 정보를 데이터베이스화한다.
② 해커의 침입으로 인한 시스템 파일이나 디렉터리의 변경을 쉽게 검출할 수 있도록 도와준다.
③ 데이터베이스에 저장된 해쉬 결과 값과 현재 파일의 해쉬 결과 값을 비교하여 무결성 여부를 판단한다.
④ 트립와이어의 데이터베이스에는 파일의 해쉬 결과 값이 저장되어 있어서 물리적 보안 대책이 필요 없다.

◦ 파일무결성 점검도구는 정상적인 상태의 디렉터리 및 파일 정보를 백업하고 있다가 점검 수행 시점에서의 정보와 백업한 정보를 비교하여 변경된 사항을 점검하는 도구이다.
◦ tripwire : MD5, SHA, CRC-32 등의 다양한 해시 함수를 지원하고, 파일들에 대한 데이터베이스를 만들어 이를 통해 공격자들에 의한 파일들의 변조여부를 판별한다.

오답피하기 ④ 트립와이어의 데이터베이스는 물리적 보안대책이 필요하다.

정답 ④

## 19.

괄호 안에 들어갈 말로 옳은 것은?

보기

운영체제의 구조는 이중 모드(dual mode)로 되어있는데, 이는 사용자 모드(user mode)와 커널 모드(kernel mode, 또는 운영체제 실행 모드)이다. 이 중 사용자 모드는 특권 명령어를 사용할 수 없으며, 이러한 경우에 사용자 프로세스는 운영체제에게 도움을 요청하게 되는데, 이를 ( )(이)라 한다. 즉, ( )는(은) 실행 중인 프로그램과 운영체제 사이에 인터페이스를 제공하는 것이다.

① 시스템 관리(system management)
② 시스템 호출(system call)
③ 프로세스 관리(process management)
④ 스케줄링(scheduling)

오답피하기 ② 이중모드에서 사용자 모드는 특권 명령어를 사용할 수 없으며, 이런 경우에 사용자 프로세스는 운영체제에게 도움을 요청하게 되는데 이를 시스템 호출이라 한다. 즉, 시스템 호출은 실행 중인 프로그램과 운영체제 사이에 인터페이스를 제공하는 것이다.

정답 ②

## 20.

코드 보안과 관련된 설명으로 옳지 않은 것은?

① 버퍼 오버플로우 공격은 데이터 길이에 대한 불명확한 정의를 이용한 공격이다.
② gets()는 버퍼 오버플로우 공격에 취약하지 않은 함수이다.
③ 포맷 스트링 공격은 데이터 형태에 대한 불명확한 정의로 발생한다.
④ 버퍼 오버플로우 공격 방어 방법으로는 공격에 취약한 함수를 사용하지 않거나 최신 운영체제를 사용하는 것 등이 있다.

◦ 사용 자제를 권장하는 함수들
strcat(), strcpy(), gets(), scanf(), sscanf(), vscanf(), vsscanf(), sprintf(), vsprintf(),gethostbyname()
◦ 사용을 권장하는 함수들
strncat(), strncpy(), fgets(), fscanf(), vfscanf(), snprintf(), vsnprintf()

오답피하기 ② 버퍼오버플로우 공격에서 gets()는 사용 자제가 요구되는 함수이다.

정답 ②

# 2016년 국가직 9급
# 네트워크 보안

–2016년 4월 9일 시행

## 1.

㉠ ~ ㉢에 들어갈 용어를 바르게 연결한 것은?

보기
◦ OSI 7계층에서 ( ㉠ )은 물리 계층으로부터 제공되는 물리적 특성을 이용하여 인접한 두 장치 간에 데이터 송수신을 수행한다.
◦ ( ㉠ )은 ( ㉡ )와 ( ㉢ )라는 두 개의 부계층으로 나뉜다.

| | ㉠ | ㉡ | ㉢ |
|---|---|---|---|
| ① | 데이터링크 계층 | 논리링크제어 | 오류제어 |
| ② | 데이터링크 계층 | 논리링크제어 | 매체접근제어 |
| ③ | 네트워크 계층 | 흐름제어 | 오류제어 |
| ④ | 네트워크 계층 | 흐름제어 | 매체접근제어 |

오답피하기 ② 데이터링크 계층은 논리적 연결제어를 담당하는 LLC(Logical Link Control sub layer, DLC(Data Link Control))와 장비와 장비 간의 물리적인 접속을 담당하는 MAC(Media Access Control)의 두 sub 계층으로 나뉘어진다.

정답 ②