# 정보시스템 보안

문 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.

문 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)

문 3. 컴퓨터 기반 사회공학적 공격기법에 해당하지 않는 것은?
① 피싱(phishing)
② 파밍(pharming)
③ 스미싱(smishing)
④ 스푸핑(spoofing)

문 4. 다음의 명령어를 실행한 파일의 접근 권한으로 옳은 것은?

| chmod 751 test.c |
|---|

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

문 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.

문 6. SSL 프로토콜 스택에 포함되지 않는 것은?
① handshake 프로토콜
② alert 프로토콜
③ record 프로토콜
④ user authentication 프로토콜

문 7. 전자우편의 보안성 향상을 위해 개발된 것이 아닌 것은?
① SMTP
② PGP
③ S/MIME
④ PEM

문 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)

문 9. 클라이언트 측에서 웹사이트에 접속할 때 발생하는 HTTP 에러 코드와 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

문 10. 다음에서 설명하는 윈도우 NTFS 파일시스템의 구조는?

| 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

문 11. <보기 1>의 상황과 개인정보의 안전한 전달을 위해 제공되어야 할 <보기 2>의 정보보호서비스를 바르게 연결한 것은?

<보기 1>

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 2>

| | |
|---|---|
| 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 |

문 12. 운영체제에서 제공하는 파일 및 디렉터리 관리에 대한 설명으로 옳지 않은 것은?

① 윈도우즈 NT 계열의 운영체제는 파일과 디렉터리에 대한 접근 제어를 통제하기 위하여 NTFS를 사용한다.
② 윈도우즈 NTFS는 모든 권한, 수정, 읽기 및 실행, 폴더내용 보기, 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.

문 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.

문 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.

문 15. 괄호 안에 들어갈 웹의 취약점은?

> (　　)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

문 16. 다음은 스택 버퍼 오버플로우 공격을 효과적으로 방어하기 위한 스택 보호 메커니즘을 서술한 것이다. ㉠ ~ ㉢에 들어갈 말을 바르게 연결한 것은?

> 스택가드(stackguard)는 가장 잘 알려진 보호 메커니즘 중 하나이다. 이것은 GCC 컴파일러의 확장 버전으로 추가의 함수 진입과 종료 코드를 삽입한다. 추가되는 함수 진입 코드는 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 |

문 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.

문 18. 트립와이어(tripwire)에 대한 설명으로 옳지 않은 것은?

① 파일의 무결성을 검사하는 도구이며, 해쉬 알고리즘을 이용하여 시스템에 존재하는 파일에 관한 정보를 데이터베이스화 한다.
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.

문 19. 괄호 안에 들어갈 말로 옳은 것은?

> 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)

문 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.