정보시스템 보안

1. 보안 운영체제(Secure OS)에 대한 설명으로 옳지 않은 것은?
① 보안 커널은 접근 제어 및 감사 추적을 위한 메커니즘을 포함하고 있다.
② 패스워드의 설정 및 접근 허용의 변경 등과 같은 보안 관련 작업의 안전한 수행을 위해 안전한 경로(trusted path)를 제공한다.
③ TCB(Trusted Computing Base) 분할은 TCB를 계층화 구조로 구현하고, 각 계층은 고유의 보안 정책을 정의하기 때문에 기존의 TCB를 재사용할 수 없다.
④ 운영체제에 내재된 결함 때문에 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위해 보안 기능이 통합된 보안 커널을 추가로 이식한 운영체제이다.

2. 다음에서 설명하는 접근통제 모델은?

> ○ 정보 소유자가 정보의 보안 수준을 결정하고 그에 대한 접근 통제까지 설정하는 모델이다.
> ○ 중앙 집중화된 정보 관리가 어려워서 정보에 대한 엄격한 접근 통제는 거의 불가능하다.

① 비바(Biba)
② 임의적 접근통제(DAC)
③ 역할기반 접근통제(RBAC)
④ 벨 라파둘라(Bell-LaPadula)

3. 멀웨어(Malware)에 대한 설명으로 옳은 것은?
① 스파이웨어(Spyware)는 사용자 동의 없이 정보를 수집하여 전송한다.
② 트로이목마(Trojan Horse)는 시스템 자원을 암호화하여 금전을 요구하는 공격을 수행한다.
③ 바이러스(Virus)는 독립적으로 실행되며, 취약점을 이용하여 스스로 전파된다.
④ 웜(Worm)은 정상 프로그램이나 실행 가능한 부분에 자신 또는 자신의 변형을 복사하며, 다른 네트워크의 시스템으로 스스로 전파하지 못한다.

4. 다음에서 설명하는 공격은?

> ○ 공격자가 특정 대상을 목표로 다양한 공격 기술을 이용해 지속적으로 공격한다.
> ○ 이 공격의 사례는 제로데이 취약점을 활용한 Stuxnet이 있다.

① APT
② DDoS
③ Ransomware
④ Reverse Engineering

5. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?
① 이상탐지(Anomaly Detection)는 시그니처(Signature) 기반 탐지라고도 한다.
② 제로데이(Zero-day) 공격에 대한 탐지는 오용탐지에 비해 이상탐지가 효율적이다.
③ 오용탐지(Misuse Detection)는 알려진 공격의 패턴을 탐지하는 방법이다.
④ 이상탐지(Anomaly Detection)는 정상적이고 평균적인 상태를 크게 벗어나는 이벤트가 발생하는 것을 탐지하는 방법이다.

6. 다음에서 설명하는 도구는?

> 웹 브라우저와 웹 서버가 통신할 때, 중간에 위치하여 웹 브라우저의 요청 메시지를 받아 웹 서버로 전송하고, 웹 서버에서 받은 응답 메시지도 웹 브라우저로 전달하는 역할을 한다. 이것을 이용하면 웹 클라이언트와 웹 서버가 교환하는 모든 데이터를 중간에서 수정이 가능하다.

① 루트킷(rootkit)
② 웹 프록시(web proxy)
③ 애드웨어(adware)
④ 포트 스캐너(port scanner)

7. 다음과 관련된 공격은?

```
SELECT * FROM member
WHERE id = 'admin' and password = ''or''='';
```

① XSS
② CSRF
③ SQL Injection
④ Format String

8. 다음은 시스템의 보안 기능에 대한 설명이다. (가) ~ (다)에 들어갈 용어를 바르게 연결한 것은?

> ○ [(가)]는 사용자와 시스템 또는 두 시스템 간에 활성화된 접속을 관리하는 것이다.
> ○ [(나)]는 시스템 자체의 결함 때문에 발생하는 보안 문제를 체계적으로 관리하는 것이다.
> ○ [(다)]는 시스템 내부 또는 외부에서 시스템에 어떤 영향을 미쳤을 경우, 해당 사항을 기록하고 관리한다.

(가)	(나)	(다)
① 로그 관리	취약점 관리	계정 관리
② 로그 관리	취약점 관리	세션 관리
③ 세션 관리	권한 관리	로그 관리
④ 세션 관리	취약점 관리	로그 관리

9. 운영체제의 프로세스에 대한 설명으로 옳지 않은 것은?
① 프로세스는 실행 중인 프로그램이다.
② 프로세스의 상태는 준비(ready), 실행(running), 종료(terminated) 등이 있다.
③ 문맥 교환(context switch)은 한 프로세스 내에서 다른 메모리 공간을 사용해야 할 때 발생한다.
④ 프로세스를 관리하기 위한 정보는 프로세스 제어 블록(process control block)에 저장된다.

10. 다음은 리눅스의 파일 권한에 대한 설명이다. (가), (나)에 들어갈 내용을 바르게 연결한 것은?

> 소유자가 root인 어떤 파일의 권한이 '-rwsr-xr-x'로 설정되어 있다. 이 권한에서 's'는 [(가)] 설정을 의미한다. 이 파일의 권한을 숫자로 표현하면 [(나)]이다.

(가)	(나)
① SetUID	2755
② SetUID	4755
③ SetGID	2755
④ SetGID	4755

11. 리눅스의 보안 관리에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. 원격에서 root 계정으로 접속하는 것을 관리자가 제한한다.
ㄴ. /etc/passwd 파일의 소유자와 권한 설정을 확인한다.
ㄷ. 소유자가 없는 파일과 디렉터리를 관리자가 삭제하거나 소유자를 변경한다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

12. 리눅스의 파일 및 디렉터리 권한에 대한 설명으로 옳지 않은 것은?

① '-rw-r-xr-x'을 숫자로 표현하면 655이다.
② 'drw-r-xr-x'에서 'd'는 디렉터리를 의미한다.
③ 'chmod u-w' 명령은 소유자의 쓰기 권한을 제거한다.
④ 'chown -R' 명령은 소유한 모든 하위 파일의 권한을 변경한다.

13. 리눅스의 로그에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. lastlog는 가장 최근 로그인 정보의 기록으로 lastlog 명령어로 확인한다.
ㄴ. btmp는 실패한 로그인 정보를 기록한 바이너리 파일로 lastb 명령어로 확인한다.
ㄷ. boot.log는 부팅 시 동작하는 데몬 관련 정보를 기록한다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

14. 버퍼 오버플로 공격에 대한 설명으로 옳지 않은 것은?

① realpath()는 버퍼 오버플로에 취약한 함수이다.
② 데이터 타입(data type)에 대한 불명확한 정의로 인해 발생한다.
③ 할당된 버퍼 한계를 벗어나서 인근 메모리 위치에 데이터를 덮어쓰는 것이다.
④ 대응 방법은 스택가드, 스택쉴드, ASLR 등이 있다.

15. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?

① RSA 암호 알고리즘을 사용한다.
② 이중 서명 프로토콜을 사용한다.
③ 상점은 고객의 지불 정보(카드 번호 등)를 알 수 없다.
④ 은행은 고객의 주문 정보를 알 수 있다.

16. 구글 검색 명령어(Google search operator)에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. "site:"는 특정 사이트를 선택하여 검색한다.
ㄴ. "url:"은 페이지의 URL에 검색하려는 문자가 포함된 사이트를 검색한다.
ㄷ. "title:"은 페이지의 제목에 검색하려는 문자가 포함된 사이트를 검색한다.
ㄹ. "filetype:"은 특정 파일타입만 검색한다.

① ㄱ, ㄴ ② ㄱ, ㄹ
③ ㄴ, ㄷ ④ ㄷ, ㄹ

17. 시스템 관리에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. OWASP-ZAP는 웹 취약점 점검 시 사용하는 도구이다.
ㄴ. 데이터베이스 REVOKE문은 허가된 권한을 취소하는 명령어이다.
ㄷ. 리눅스 chage는 사용자 계정의 패스워드 에이징(aging) 정보를 변경하는 명령어이다.

① ㄱ, ㄴ ② ㄱ, ㄷ
③ ㄴ, ㄷ ④ ㄱ, ㄴ, ㄷ

18. PGP와 S/MIME에 대한 설명으로 옳은 것만을 모두 고르면?

ㄱ. PGP에서 전자 서명을 위해 DSS 또는 RSA를 사용한다.
ㄴ. PGP에서 타임스탬프, KeyID, 공개키, 암호화된 개인키, 인증서, 사용자 ID는 개인키 링에 포함되어 있다.
ㄷ. S/MIME에서 봉인된 데이터(enveloped data)는 메시지의 비밀성을 제공하기 위해 사용된다.
ㄹ. S/MIME에서 키 관리는 X.509와 PGP에서 사용되는 키 관리의 조합 방법을 사용한다.

① ㄱ, ㄷ ② ㄱ, ㄹ
③ ㄱ, ㄷ, ㄹ ④ ㄴ, ㄷ, ㄹ

19. 다음은 HTTP 버전 1.1에서 정의된 요청 메서드에 대한 설명이다. (가) ~ (라)에 들어갈 내용을 바르게 연결한 것은?

○ 게시판 등에서 파일 업로드는 [(가)] 방식으로 할 수 있다. 이는 [(나)] 방식과 달리 보내려는 데이터가 URL을 통해 노출되지 않기 때문에 최소한의 보안성은 갖추고 있다.
○ 일반적으로 게시판의 목록이나 글 보기 화면은 접근 자유도를 부여하기 위해 [(다)] 방식을 사용하고, 게시글을 저장・수정・삭제하거나 대용량 데이터를 전송할 때는 [(라)] 방식을 사용한다.

	(가)	(나)	(다)	(라)
①	POST	GET	GET	POST
②	POST	GET	POST	GET
③	GET	POST	GET	POST
④	GET	POST	POST	GET

20. 다음은 리눅스의 /etc/shadow 파일 구조이다. 각 항목에 대한 설명으로 옳은 것만을 모두 고르면?

anthony:6L9~중략~ruKuT0:18365:(가):(나):(다):(라)::

ㄱ. (가) 값이 0이면 패스워드를 즉시 변경할 수 있다.
ㄴ. (나)는 패스워드를 변경하지 않고 사용 가능한 최대 일수이다.
ㄷ. (다)는 패스워드가 만료되기 전에 경고를 시작하는 일수이다.
ㄹ. (라)는 사용자 계정이 만료되는 날이다.

① ㄱ, ㄴ ② ㄱ, ㄹ
③ ㄱ, ㄴ, ㄷ ④ ㄴ, ㄷ, ㄹ