정보시스템 보안

문 1. CPU에서 실행되는 머신 코드가 위치하는 시스템 메모리 영역은?
① 스택 ② 힙
③ 텍스트 ④ 데이터

문 2. 사용자와 운영체제 사이에서 중간자 역할을 수행하며, 명령어 해석 기능, 프로그래밍 기능, 사용자 환경 설정 기능을 제공하는 것은?
① 데몬 ② 커널
③ 프로세스 ④ 셸

문 3. (가)에 들어갈 용어로 옳은 것은?

> 보안 운영체제는 기존의 운영체제에 내재된 보안상의 결함으로 인한 각종 침해로부터 시스템을 보호하기 위하여 기존의 운영체제 내에 보안 기능을 통합시킨 [(가)]을/를 추가로 이식한 운영체제이다. 이를 통해 사용자의 모든 접근 행위가 안전하게 통제된다. 이것은 하드웨어, 운영체제 및 기타 시스템 요소 간의 보안 인터페이스를 제공한다.

① 보안 커널 ② 접근 제어
③ 신뢰 플랫폼 모듈 ④ 하이퍼바이저

문 4. 보안 모델의 하나인 만리장성(Chinese Wall) 모델에 대한 설명으로 옳은 것은?
① 높은 보안 수준에서 낮은 보안 수준으로 정보가 흐르는 것을 방지하기 위한 기밀성 보장 모델이다.
② 비즈니스 입장에서 직무 분리 개념을 적용하여 이해가 충돌하는 회사 간에 정보의 흐름이 일어나지 않도록 접근을 통제한다.
③ 무결성 중심의 상업적 모델로 내·외부의 일관성을 유지하고 비인가자에 의한 불법적인 수정을 방지한다.
④ 무결성을 위한 모델로 비인가자의 데이터 변형을 방지하기 위한 것이다.

문 5. 윈도시스템의 NTFS에서 폴더 및 파일 접근 권한에 대한 설명으로 옳은 것은?
① 그룹 A와 그룹 B에 속한 사용자가 그룹 A에서는 읽기 권한을 할당받고 그룹 B에서는 쓰기 권한을 할당받았다면, 사용자에게 읽기와 쓰기 권한이 모두 주어진다.
② 파일이 포함된 폴더 권한이 파일 권한보다 우선한다.
③ 권한을 중첩해서 적용할 수 있으며, 허용 설정이 거부 설정보다 우선한다.
④ 폴더 접근 권한은 그룹에게만 부여된다.

문 6. 다음에서 설명하는 전자우편 보안 기술은?

> ○ 종단 사용자에게 투명한 인증 기술을 제공하도록 설계되었다.
> ○ 전자우편 메시지는 전자우편 발신지 관리 도메인의 개인키에 의해 서명된다.
> ○ 서명은 메시지 내용 전체와 메시지 헤더의 일부를 대상으로 한다.
> ○ 수신 측의 MDA(Mail Delivery Agent)는 DNS를 통해 해당 공개키에 접근하여 서명을 검증할 수 있다.

① PGP ② PEM
③ MIME ④ DKIM

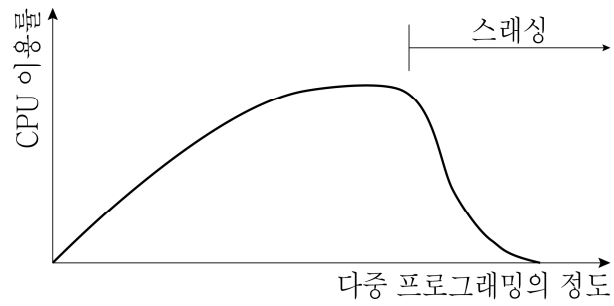
문 7. 다음에서 설명하는 윈도시스템 인증 구성 요소는?

> 사용자의 계정과 패스워드가 일치하는 경우 해당 사용자에게 고유의 SID(Security Identifier)를 부여하며, 파일이나 폴더에 대한 접근 허용 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

① SAM ② LSA
③ SRM ④ SPI

문 8. (가), (나)에 들어갈 용어를 바르게 연결한 것은?

> 그림과 같이 다중 프로그램의 정도에 따른 CPU 이용률은 처음에는 비례해서 증가하지만 다중 프로그래밍의 정도가 어느 정도 이상으로 커지면 스래싱(thrashing)이 일어나게 되어 CPU 이용률은 급격히 떨어진다. 스래싱은 [(가)] 페이지 교체 알고리즘을 사용하면 제한할 수 있다. 또한 이 현상을 방지하기 위해서는 각 프로세스에게 할당되는 최소한의 [(나)] 개수를 보장해야 한다.



(가)	(나)
① 전역	프레임
② 전역	페이지
③ 지역	프레임
④ 지역	페이지

문 9. S/MIME에 대한 설명으로 옳지 않은 것은?
① 서명된 데이터(signed data)의 디지털 서명은 메시지 다이제스트를 서명자의 개인키로 암호화한 것으로, 서명과 함께 메시지 내용은 base64로 부호화된다.
② 서명과 봉인된 데이터(signed and enveloped data)는 서명만 하거나 암호화만 한 개체들이 중첩된 것으로, 암호화한 데이터를 서명하거나 서명한 데이터를 암호화할 수 있다.
③ 디지털 서명만을 base64로 부호화한 클리어 서명 데이터(clear-signed data)의 경우, S/MIME 기능을 갖추지 않은 수신자도 서명을 검증하고 메시지의 내용을 볼 수 있도록 지원한다.
④ X.509의 버전 3을 따르는 공개키 인증서를 사용한다.

문 10. HTTP 버전 1.1에서 정의된 요청 메시지의 메소드에 대한 설명으로 옳은 것은?
① GET이 요청하는 웹페이지의 위치는 헤더 라인 안에 명시된다.
② 서버가 보내온 쿠키를 저장했다가 반환하는 GET의 경우, 쿠키 정보는 메시지 몸체(body)에 포함된다.
③ HEAD는 서버로부터 웹페이지 자체가 아닌 웹페이지에 대한 일부 정보를 요청하기 위한 것이다.
④ PUT은 요구 메시지가 서버에 의해 제대로 처리되는가를 검사하기 위한 에코 반환 용도로 사용된다.

문 11. 리눅스 시스템의 /etc/shadow 파일 내용에서 패스워드의 최종 변경일에 해당하는 것은?

root : 6L9~중략~ruKuT0 : 15917 : 0 : 99999 : 7 : 5 : 16070 :

① 15917 ② 99999
③ 7 ④ 16070

문 12. PKI에 대한 설명으로 옳지 않은 것은?

① 인증기관(CA), 등록기관(RA), 키 분배 센터(KDC)로 구성된다.
② 이용자는 공개키를 이용하기 전에 CA의 인증서 폐기 목록(CRL)을 조사해서 해당 인증서의 유효성을 확인할 필요가 있다.
③ CA의 공개키에 대해 다른 CA가 디지털 서명을 하는 것으로 그 CA의 공개키를 검증할 수 있다.
④ CA의 개인키가 노출된 경우에는 그 사실을 CRL을 사용해서 이용자에게 통지할 필요가 있다.

문 13. 인증을 받은 사용자가 여러 정보 시스템에 재인증 절차 없이 반복해서 접근할 수 있도록 해주는 것은?

① OTP ② SSO
③ Challenge & Response ④ CAPTCHA

문 14. 공격 대상이 되는 서버에서 먼저 공격자 PC로 연결하게 하여 방화벽 보안 정책을 우회하는 공격은?

① 리버스 텔넷 ② 쿠키 변조
③ 명령 삽입 ④ 파일 업로드

문 15. (가) ~ (다) 안에 들어갈 용어를 바르게 연결한 것은?

함수 P가 함수 Q를 호출하기 위해, P는 Q에 전달할 인수를 스택에 넣는다. Q를 호출하는 call 명령어를 수행하면 [(가)]가 스택에 저장된다. Q는 [(나)]를 스택에 넣는다. 프레임 포인터 레지스터 값을 현재의 포인터 값으로 설정하고, 스택 포인터를 아래로 움직여 [(다)]를 저장할 공간을 할당하고, Q의 코드를 수행한다. 컴파일러의 최적화 기능에 따라 실제 배치는 차이가 있을 수 있으나, 저장된 [(가)]와 [(나)]에 겹쳐 쓰기는 스택 버퍼 오버플로 공격의 핵심이다.

	(가)	(나)	(다)
①	반환 주소	P의 스택 프레임 포인터	지역 변수
②	반환 주소	Q의 스택 프레임 포인터	지역 변수
③	P의 스택 프레임 포인터	지역 변수	반환 주소
④	Q의 스택 프레임 포인터	지역 변수	반환 주소

문 16. FTP에 대한 설명으로 옳지 않은 것은?

① 데이터 연결 시 평문으로 데이터를 전송한다.
② 데이터 연결은 송·수신 모두 지정된 포트 20번을 통해서만 가능하다.
③ 사용자 계정의 패스워드는 암호화되지 않은 상태로 전달된다.
④ FTP를 이용하여 클라이언트는 서버의 파일을 읽고 서버에 파일을 저장할 수 있을 뿐만 아니라 서버의 파일 목록을 볼 수도 있다.

문 17. SQL 뷰에 대한 설명으로 옳지 않은 것은?

① 사용자가 뷰를 통해서만 데이터에 접근하게 함으로써 기본 테이블에 대한 보안성을 높일 수 있다.
② 뷰가 정의된 기본 테이블이 확장되거나 뷰가 속해 있는 데이터베이스에 테이블이 늘어난다고 하더라도 기존의 뷰를 사용하는 프로그램이나 사용자는 영향을 받지 않는다.
③ 필요한 데이터만 뷰로 정의해서 처리할 수 있기 때문에 사용자 권한 관리가 용이하다.
④ 대부분의 경우 삽입, 삭제, 갱신 연산에 많은 제한이 따르며 질의문이 복잡해지는 단점이 있다.

문 18. 리눅스에서 제공하는 특수 권한에 대한 설명으로 옳지 않은 것은?

① 숫자로 나타내면 접근 권한의 맨 앞자리에 Set-UID는 4, Set-GID는 2, Sticky-Bit는 1로 표현된다.
② Set-UID를 설정하면 소유자 실행 권한 자리에, Set-GID를 설정하면 그룹 실행 권한 자리에 s 혹은 S가 표시된다.
③ Sticky-Bit는 공유를 목적으로 파일에 설정하는 특수 권한으로, 설정 시 소유자 실행 권한 자리에 t 혹은 T가 표시된다.
④ Set-UID가 설정된 파일이 실행되는 동안에는 파일을 실행한 사용자의 권한이 아니라 파일 소유자의 권한이 적용된다.

문 19. 다음에서 설명하는 웹 취약점 점검 방법과 해당 취약점을 바르게 연결한 것은?

(가) "../"를 이용해서 임의의 경로가 포함된 값으로 웹페이지 파라미터를 변조한 후 해당 경로의 파일 내용이 표시되는지 확인
(나) 사용자 입력값을 전달받는 게시판, 자료실 등에 <script>alert()</script>와 같은 스크립트를 입력한 후 실행 여부 확인
(다) 인증 후 정상적으로 세션이 발행된 페이지의 정보를 취득하고 일정 시간 후에 재전송했을 때 정상 처리가 되는지 확인

	(가)	(나)	(다)
①	경로 추적	CSRF	불충분한 인증 및 인가
②	경로 추적	XSS	불충분한 세션 관리
③	디렉터리 인덱싱	XSS	불충분한 인증 및 인가
④	디렉터리 인덱싱	CSRF	불충분한 세션 관리

문 20. 보안 요구 조건을 명세화하고 평가 기준을 정의하기 위한 ISO 표준인 공통 기준(CC)에서는 요구 조건을 기능적 요구 조건과 보증 요구 조건으로 나누고 있다. 기능적 요구 조건에 해당하지 않는 것은?

① 식별과 인증 ② 암호 지원
③ 보안 감사 ④ 취약점 평가