정보보호론

1. 보안 공격의 특성이 나머지 넷과 거리가 가장 먼 것은?

① Sniffing
② Snooping
③ Masquerade
④ Eavesdropping
⑤ Traffic Analysis

2. SQL 인젝션 공격이 발생할 가능성이 가장 높은 코드 구조는?

① 사용자 입력을 서버에서 세션으로 저장
② 사용자 입력을 파일로 저장한 후 비동기 처리
③ 사용자 입력을 인코딩 후 정적 HTML로 출력
④ 쿼리문 실행 전 입력값을 모두 소문자로 변환
⑤ 사용자 입력값을 문자열로 직접 연결해 SQL 쿼리를 구성

3. TCP/IP 프로토콜 계층의 응용 계층 보안 서비스로 옳지 않은 것은?

① PGP(Pretty Good Privacy)
② SET(Secure Electronic Transaction)
③ VPN(Virtual Private Network)
④ S/MIME(Secure Multi-Purpose Internet Mail Extensions)
⑤ Kerberos

4. SSL/TLS 서비스에 대한 설명으로 옳은 것은?

① 송신자와 수신자 간의 접근제어를 관리한다.
② 송신자의 인증 및 데이터 암호화를 지원한다.
③ 인증 헤더를 통하여 송신자를 인증할 수 있다.
④ 메시지를 여러 개의 단편으로 분할하고, 압축을 수행한다.
⑤ 전달되는 데이터가 전송 도중에 변경되지 않았음을 확인할 수 있다.

5. 「개인정보 보호법」에 따른 정보주체의 권리로 옳지 않은 것은?

① 개인정보 열람 청구권
② 개인정보 이전 요청권
③ 개인정보 삭제 요구권
④ 개인정보 처리 정지 요구권
⑤ 개인정보 처리에 관한 동의 철회권

6. 다음과 같은 해시값을 생성하는 알고리즘은? (단, 해시값은 16진수임)

f287a3e6d95e1616724ed8c2bc853903375990c4

① AES
② SHA-1
③ MD-5
④ SHA-2
⑤ SEED

7. 디지털 증거에 대한 무결성을 확보하기 위한 조치로 옳은 것은?

① 파일 압축
② 파일 암호화
③ 파일 변환
④ 해시값 계산 및 대조
⑤ 파일 분할

8. 다음에서 설명하는 공격 방법은?

○ 암호 설계 단계에서 고려하지 않은 전력 소모량, 전자파 누설, 열 등을 이용한 공격 방법으로 폴 코처(Paul Kocher)에 의하여 처음 제안되었다. ○ 타이밍 공격(timing attack), 전력분석 공격(power attack), 전자파 공격(electromagnetic emission attack) 등이 이 공격의 유형에 해당된다.

① 부채널 공격(side-channel attack)
② 선택 암호문 공격(chosen-ciphertext attack)
③ 전수조사 공격(brute-force attack)
④ 통계적 공격(statistical attack)
⑤ 암호문 단독 공격(ciphertext-only attack)

9. 다음에서 설명하는 프라이버시 강화 기술은?

> ○ 대규모 데이터에서 개별 주체들의 개인정보 노출을 최소화하는 동시에 개인정보를 활용할 수 있는 방법
>
> ○ 인공지능(AI) 학습에서 개인정보를 보호하기 위해 데이터를 계산하거나 결과를 산정하기 전에 데이터에 통계적 '노이즈'를 삽입하여 개인정보가 제3자에게 노출되지 않도록 익명성을 제공

① 동형 암호

② 연합 학습

③ 신뢰 실행 환경

④ 제로 지식 증명

⑤ 차분 프라이버시

10. 다크웹(Dark Web)에 대한 설명으로 옳지 않은 것은?

① 사용자와 서버의 익명성을 유지할 가능성이 높고, IP 주소 추적이 어렵다.

② 종단 간 암호화를 통해 통신 내용을 보호하여 보안성이 뛰어나다.

③ 중앙 서버 없이 분산된 노드들로 운영되는 구조이다.

④ 도메인은 일반적으로 .onion 확장자를 가지며, Tor 네트워크 전용으로 운영된다.

⑤ 고립된 폐쇄형 네트워크로 구성되어 있어, 물리적 인터넷 인프라를 사용하지 않고 자체적인 독립 인프라에서 운영된다.

11. 한국의 CSAP(Cloud Security Assurance Program) 제도에 대한 설명으로 옳지 않은 것은?

① 국내 공공기관이 클라우드 서비스를 제공하기 전에 해당 서비스의 보안성을 사전에 평가받도록 하는 제도이다.

② CSAP 인증은 서비스 유형(IaaS, PaaS, SaaS)에 따라 구분되며, 각 유형별로 요구되는 보안 기준이 상이하다.

③ 최초 인증 이후에도 정기적인 사후 심사를 통해 서비스 보안 상태를 지속적으로 검증한다.

④ 민간 기업은 공공시장 진출을 위해 CSAP 인증을 받을 수 있으며, 이를 통해 공공기관 대상 클라우드 서비스 공급이 가능해진다.

⑤ 개인정보나 민감정보를 처리하는 클라우드 서비스가 CSAP 인증을 받으려면 데이터의 물리적 위치에 대한 평가도 필요하다.

12. 방화벽의 유형과 그 특징에 대한 설명으로 옳지 않은 것은?

① 패킷 필터링 방화벽은 IP 주소, 포트 번호, 프로토콜 등의 정보를 기반으로 트래픽을 허용하거나 차단한다.

② 상태 기반 방화벽은 각 연결의 상태 정보를 추적하여, 비정상적인 연결 요청이나 응답을 감지할 수 있다.

③ 애플리케이션 계층 방화벽은 HTTP, FTP 프로토콜의 내용을 분석할 수 있으며, 콘텐츠 수준의 보안 통제를 수행한다.

④ 프록시 방화벽은 물리 계층에서 작동하며, 패킷의 헤더 정보를 확인하여 빠르게 트래픽을 처리한다.

⑤ 차세대 방화벽은 전통적인 방화벽 기능 외에도 애플리케이션 제어, 사용자 식별, 침입 방지 등의 기능이 있다.

13. SSH(Secure Shell)에 대한 설명으로 옳지 않은 것은?

① 네트워크상에서 원격 접속을 제공하기 위해 설계된 프로토콜로, 대칭키와 비대칭키 암호화가 모두 사용된다.

② 기본적으로 22번 포트를 사용하며, 세션 동안 전달되는 데이터는 도청 및 중간자 공격으로부터 안전하다.

③ 클라이언트가 서버에 접속하면, 서버가 먼저 클라이언트의 공개키를 인증하고 세션이 시작된다.

④ 원격 터미널 접속 외에도 파일 전송, 포트 포워딩, 터널링 등의 기능도 지원한다.

⑤ 공개키 기반 또는 Kerberos 기반의 인증을 사용하기도 한다.

14. 은행 업무 환경에서의 접근 제어 방식(Access Control Model)에 대한 설명으로 옳은 것은?

① RBAC(Role-Based Access Control)는 조직 내 역할에 따라 접근 권한을 부여하므로, '여신 심사역' 역할을 가진 사용자는 자동으로 관련 시스템에 접근할 수 있다.

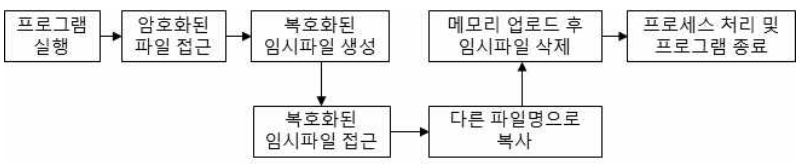
② DAC(Discretionary Access Control)는 자산 소유자가 권한을 자유롭게 부여할 수 있기 때문에, 보안 사고 발생 시 책임 소재가 명확해져 금융기관에서 자주 활용된다.

③ ABAC(Attribute-Based Access Control)는 특정 파일을 '중요 파일'로 분류하더라도 사용자 속성이 일치하지 않으면 누구든 접근이 가능하므로 보안성이 낮다.

④ RBAC는 개별 사용자마다 권한을 직접 지정하기 때문에, 사용자가 많을수록 관리가 어려워진다.

⑤ ABAC는 규칙이 아닌 사용자 개별 요청에 따라 접근이 결정되므로, 정책 자동화가 어렵다는 단점이 있다.

15. 다음 그림과 같이 수행하는 공격의 명칭은?



① 스니핑 공격
② 백도어 공격
③ 포맷 스트링 공격
④ 레이스 컨디션 공격
⑤ 버퍼 오버플로 공격

16. TCP/IP 응용계층의 보안 프로토콜에 해당하는 것만을 <보기>에서 모두 고르면?

< 보 기 >

ㄱ. S/MIME
ㄴ. L2TP
ㄷ. IPSec
ㄹ. SSH

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄴ, ㄹ
⑤ ㄷ, ㄹ

17. 802.1x/EAP에서 제공하는 기능으로 옳지 않은 것은?

① 디렉터리 리스팅
② 사용권한의 중앙관리
③ 인증서, 스마트카드 등 다양한 인증 제공
④ 세션별 암호화키 제공
⑤ 사용자 인증

18. 윈도우에서 제공하는 기본 프로세스 중 다음 설명에 해당하는 것은?

> 이 서비스는 DLL이 실행하는 프로세스에 대한 기본 프로세스로, 하나의 시스템상에서 동시에 여러 개가 수행될 수 있으며 백그라운드 서비스를 처리할 수 있다.

① winlogon.exe
② smss.exe
③ svchost.exe
④ spoolsv.exe
⑤ explorer.exe

19. 다음 SQL 쿼리문에 대한 설명으로 옳지 않은 것은?

```
SELECT * FROM user WHERE name = '' or ''='';
```

① SQL 인젝션 공격에 취약한 문장이다.
② WHERE절에서 user의 모든 레코드를 반환받을 가능성이 있다.
③ 위 SQL 쿼리문의 취약점 해결 방법으로 prepared statements를 사용하는 것이 좋다.
④ 입력값 검증을 위하여 블랙리스트 방식으로 유효한 값만 허용하는 것이 좋다.
⑤ JPA, Hibernate 등 ORM으로 데이터를 추상화하는 것이 좋다.

20. RSA 암호에서 암호문이 C=2, 공개키가 (e=3, n=33)일 때, 평문 M은?

① 8
② 10
③ 17
④ 19
⑤ 29