

## 정보보호론

### 1. 악성 코드(malware)에 대한 설명으로 옳지 않은 것은?

- ① 바이러스는 다른 프로그램에 자신을 복제하여 악의적 목적을 수행한다.
- ② 랜섬웨어는 사용자의 파일을 암호화하여 자료를 인질로 잡고 금전을 요구한다.
- ③ 웜은 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램이다.
- ④ 트로이목마는 정상적인 프로그램으로 위장하여 자기 복제를 통해 다른 시스템으로 확산한다.

### 2. 대칭키 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

- ① 암호화/복호화 속도는 공개키 암호보다 빠르다.
- ② 키의 길이가 공개키 암호보다 상대적으로 짧다.
- ③ 공개키는 암호화에 사용하고 개인키는 복호화에 사용한다.
- ④ 사용자의 증가에 따라 관리해야 할 키의 수가 비례적으로 늘어난다.

### 3. (가) ~ (라)에 들어갈 용어를 바르게 연결한 것은?

| 구분  | 메시지 인증 코드     | 전자서명        |
|-----|---------------|-------------|
| 송신자 | (가)로 MAC값을 계산 | (나)로 서명을 작성 |
| 수신자 | (다)로 MAC값을 계산 | (라)로 서명을 검증 |

- |       | (가) | (나) | (다) | (라) |
|-------|-----|-----|-----|-----|
| ① 공유키 | 공개키 | 공유키 | 개인키 |     |
| ② 개인키 | 공유키 | 공개키 | 공유키 |     |
| ③ 공유키 | 개인키 | 공유키 | 공개키 |     |
| ④ 개인키 | 공유키 | 공유키 | 공개키 |     |

### 4. 디지털 포렌식에 대한 설명으로 옳지 않은 것은?

- ① 디지털 포렌식 과정에서 획득한 모든 증거는 법적 효력을 가진다.
- ② 수집된 증거가 결함이 없이 위·변조되지 않았음을 증명할 수 있어야 한다.
- ③ 동일한 조건과 동일한 상황이라면 디지털 포렌식의 분석 결과는 항상 같은 결과가 나와야 한다.
- ④ 증거를 획득한 뒤에는 이송, 분석, 보관, 법정 제출이라는 일련의 과정 및 각 과정의 담당자가 명확해야 하며 이에 대한 추적이 가능해야 한다.

### 5. 암호화 알고리즘에 대한 설명으로 옳은 것은?

- ① DES는 56비트 키를 사용하는 대칭키 암호 알고리즘이다.
- ② AES는 국내에서 개발된 블록 암호 알고리즘으로 국제 표준이 되었다.
- ③ SEED는 3개의 키값을 사용하고 DES의 3배인 168비트의 보안 강도를 제공한다.
- ④ RSA는 큰 소수의 곱을 인수분해하기 어렵다는 수학적 원리에 기반한 대칭키 암호 알고리즘이다.

### 6. 국내 국가보안기술연구소 주도로 개발된 암호화 알고리즘은?

- ① DES
- ② ARIA
- ③ RC5
- ④ IDEA

### 7. 사용자가 입력한 키보드 정보를 가로채는 방법은?

- ① 피싱(phishing)
- ② 파밍(pharming)
- ③ 스미싱(smishing)
- ④ 키로깅(keylogging)

### 8. 인증에 대한 설명으로 옳지 않은 것은?

- ① 패스워드는 길이가 길고 대소문자, 숫자, 특수문자를 조합할수록 무차별 대입 공격에 대한 안전성이 높아진다.
- ② 생체 인증은 신체적 특성을 이용하므로 원천적으로 복제가 불가능하여 별도의 보안 대책이 필요하지 않다.
- ③ SSO(Single Sign On)는 한 번의 인증으로 다수의 시스템에 접근할 수 있게 하는 인증 시스템이다.
- ④ OTP(One Time Password)는 한 번 생성되면 그 인증값이 임시적으로 한 번에 한해서만 유효하며, 시간 동기화, 이벤트 동기화, 챌린지·응답 등의 방식으로 생성된다.

### 9. 공격자가 공격대상의 IP주소로 위장하여 브로드캐스팅 방식을 통해 ICMP echo request를 다수의 호스트에 전송하는 공격은?

- ① Smurf
- ② SYN Flooding
- ③ ARP Spoofing
- ④ ICMP Redirect

### 10. 허니팟(honeypot)에 대한 설명으로 옳지 않은 것은?

- ① 허니팟은 공격자에게 쉽게 노출되어야 한다.
- ② 허니팟은 쉽게 해킹이 가능한 것처럼 취약해 보이게 한다.
- ③ 허니넷(honeynet)은 여러 허니팟을 포함한 네트워크를 의미한다.
- ④ 허니팟은 시스템을 통과하는 패킷에 대해 일부분만을 샘플링하여 감시한다.

### 11. 정보시스템의 접근 제어(access control) 또는 로그 관리에 대한 설명으로 옳지 않은 것은?

- ① 인증(authentication)은 자신의 신원(identity)을 증명하기 위하여 행하는 과정이다.
- ② 감사 추적(audit trail)은 시스템의 위험을 평가하고 비용 대비 효과적인 대응책을 수립하는 과정이다.
- ③ 인가(authorization)는 인증된 주체에게 자원에 대한 접근 권한을 부여하거나 제한하는 과정이다.
- ④ 책임 추적성(accountability)은 시스템에 접근한 주체가 어떤 행동을 하였는지 기록하여 필요 시 그 행위자를 추적할 수 있게 한다.

- ① DNS Spoofing
- ② IP Spoofing
- ③ Switch Jamming
- ④ Teardrop

- ① 개인정보의 기술적·관리적 보호조치에 관한 사항
- ② 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항
- ③ 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
- ④ 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항