

## 정보보호론

### 1. 정보보호에 대한 설명으로 옳지 않은 것은?

- ① 정보자산을 여러 가지 위협으로부터 보호하는 것이다.
- ② 정보보호의 범위에는 사이버안전이 포함될 수 없다.
- ③ 정보의 가용성과 보안 측면에서 정보보호는 정보의 활용과 정보의 통제 사이에서 균형 감각을 갖는 행위이다.
- ④ 정보보호의 대상이 되는 자산에는 소프트웨어, 하드웨어, 데이터, 인적자원이 포함될 수 있다.

### 2. 포트 스캔에 대한 설명으로 옳지 않은 것은?

- ① 분석 대상 시스템에 어떤 서비스가 제공되고 있는지 확인하기 위한 정보수집 방법이다.
- ② 포트 번호는 0 ~ 65,535까지이며, 이 중 0 ~ 1,023은 잘 알려진 포트(well-known port)라고 한다.
- ③ Nmap은 오픈소스 기반 포트 스캔 도구이다.
- ④ TCP 포트 스캔 시 닫혀 있는 포트로부터 ICMP port Unreachable 패킷이 수신된다.

### 3. (가), (나)에 해당하는 정보보호 서비스를 바르게 연결한 것은?

메일 내용에 암호를 적용함으로써 (가) 을 제공할 수 있고,  
메일에 전자서명을 적용함으로써 (나) 을/를 제공할 수 있다.

(가) (나)

- ① 기밀성 가용성
- ② 기밀성 부인방지
- ③ 가용성 기밀성
- ④ 가용성 인증

### 4. (가)에 들어갈 용어는?

- (가) 은/는 1989년에 처음 등장한 것으로 알려져 있고 이후 2006년경에 GPCode라는 (가) 이/가 등장하였다.
- 최근의 (가) 은/는 공격자의 개인키를 모르면서 사실상 풀 수 없는 암호 알고리즘을 사용한다.

- ① 워
- ② 바이러스
- ③ 랜섬웨어
- ④ DDoS

### 5. (가), (나)에 해당하는 악성코드를 바르게 연결한 것은?

(가) DDoS 공격 시 지정된 공격을 수행하도록 하는 악성코드  
(나) 사용자의 동의 없이 설치되어 사용자 또는 컴퓨터의 정보를 수집하여 전송하는 악성코드

(가) (나)

- ① 봇 스파이웨어
- ② 봇 애드웨어
- ③ 루트킷 스파이웨어
- ④ 루트킷 애드웨어

### 6. VPN에서 사용하는 프로토콜이 아닌 것은?

- ① IGMP
- ② IPSec
- ③ L2TP
- ④ PPTP

### 7. (가)에 들어갈 용어는?

윈도우 운영체제에서 SAM이 사용자의 로그인 입력 정보(사용자 계정과 패스워드)와 SAM 데이터베이스 정보의 일치 여부를 확인하여 SRM에게 알리면 인증된 사용자에게 고유한 (가) 가 부여된다. 또 SRM은 (가) 를 기반으로 파일이나 디렉토리에 접근을 허용할지 여부를 결정하고 이에 대한 감사 메시지를 생성한다.

- ① GID
- ② SID
- ③ SetUID
- ④ SSID

### 8. 위험 처리 방법에 대한 설명으로 옳은 것은?

- ① 위험 수용: 위험에 처한 자산의 구조나 사용을 변경한다.
- ② 위험 감소: 위험을 발생시키는 행위나 시스템을 수행하지 않는다.
- ③ 위험 전가: 위험에 대응하여 보험을 들거나 다른 기관과 계약을 맺는다.
- ④ 위험 회피: 현재의 위험을 받아들이고 잠재적 손실 비용을 감수한다.

### 9. 공개키 암호 알고리즘이 아닌 것은?

- ① RSA
- ② 타원곡선암호
- ③ 배낭암호
- ④ A5/1

### 10. 다음에서 설명하는 보안 솔루션은?

- 조직 내 중요한 자료가 외부로 유출되는 것을 막는다.
- 사용자의 다양한 데이터 전송 수단인 USB 메모리 등과 같은 이동식 저장 매체, 이메일과 같은 네트워크 등을 제어한다.

- ① DRM
- ② DLP
- ③ IPS
- ④ SIEM

### 11. 다음 문제가 모두 해결된 블록암호 운용 모드는?

- 평문 블록이 동일하면 암호문 블록이 같아지는 문제
- 암호문 블록에 오류가 발생하면 다음 블록의 복호화에 오류가 전파되는 문제

- ① ECB(Electronic CodeBook)
- ② OFB(Output FeedBack)
- ③ CFB(Cipher FeedBack)
- ④ CBC(Cipher Block Chaining)

12. 다음에서 설명하는 블루투스 취약점 공격은?

블루투스 장비 간의 취약한 연결 관리를 악용한 공격으로, 공격 장치와 공격 대상 장치를 연결하여 공격 대상 장치에서 임의의 동작을 실행한다. 블루투스 기기가 한 번 연결된 이후에는 다시 연결하지 않아도 자동으로 연결되는 인증 취약점을 이용한 공격이다.

- ① 블루버그(bluebug)                      ② 블루재킹(bluejacking)
- ③ 블루프린팅(blueprinting)              ④ 블루스나프(bluesnarf)

13. 유럽의 GDPR(General Data Protection Regulation)에 따른 정보 주체의 권리가 아닌 것은?

- ① 개인정보의 처리에 대한 차단/제한을 요구할 권리
- ② 개인정보를 본인 또는 다른 사업자에게 전송하도록 요구할 권리
- ③ 개인정보의 삭제를 요구할 권리
- ④ 프로파일링 등 자동으로 이루어지는 모든 의사결정에 대해 거부할 권리

14. 안티 리버싱 기법에 해당하는 것만을 모두 고르면?

ㄱ. 난독화  
ㄴ. 스택 실드  
ㄷ. 안티 디버깅  
ㄹ. 카나리아

- ① ㄱ, ㄷ                                              ② ㄱ, ㄹ
- ③ ㄴ, ㄷ                                              ④ ㄴ, ㄹ

15. 「개인정보 보호법」상 개인정보의 파기에 대한 설명으로 옳지 않은 것은?

- ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성, 가명정보의 처리 기간 경과 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
- ② 개인정보처리자가 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
- ③ 개인정보처리자가 개인정보를 파기하지 아니하고 다른 법령에 따라 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
- ④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 총리령으로 정한다.

16. 다중문자 암호 방식에 해당하는 것만을 모두 고르면?

ㄱ. 비즈네르(Vigenère) 암호  
ㄴ. 시저(Caesar) 암호  
ㄷ. 플레이페어(Playfair) 암호  
ㄹ. 아핀(Affine) 암호

- ① ㄱ, ㄷ                                              ② ㄱ, ㄹ
- ③ ㄴ, ㄷ                                              ④ ㄴ, ㄹ

17. 「개인정보 보호법」상 개인정보처리자가 개인정보의 제3자 제공과 관련하여 정보주체에게 동의를 받을 때 정보주체에게 알려야 하는 사항이 아닌 것은?

- ① 개인정보를 제공받는 자의 개인정보 이용 목적
- ② 동의에 따른 이익이 있는 경우에는 그 이익의 내용
- ③ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

18. 다음 표를 이용하여 24비트 입력 ‘01000001 01000010 01000011’에 Base64 부호화를 적용할 때, 출력되는 문자열은?

| Index | Binary | Char | Index | Binary | Char | Index | Binary | Char | Index | Binary | Char |
|-------|--------|------|-------|--------|------|-------|--------|------|-------|--------|------|
| 0     | 000000 | A    | 16    | 010000 | Q    | 32    | 100000 | g    | 48    | 110000 | w    |
| 1     | 000001 | B    | 17    | 010001 | R    | 33    | 100001 | h    | 49    | 110001 | x    |
| 2     | 000010 | C    | 18    | 010010 | S    | 34    | 100010 | i    | 50    | 110010 | y    |
| 3     | 000011 | D    | 19    | 010011 | T    | 35    | 100011 | j    | 51    | 110011 | z    |
| 4     | 000100 | E    | 20    | 010100 | U    | 36    | 100100 | k    | 52    | 110100 | 0    |
| 5     | 000101 | F    | 21    | 010101 | V    | 37    | 100101 | l    | 53    | 110101 | 1    |
| 6     | 000110 | G    | 22    | 010110 | W    | 38    | 100110 | m    | 54    | 110110 | 2    |
| 7     | 000111 | H    | 23    | 010111 | X    | 39    | 100111 | n    | 55    | 110111 | 3    |
| 8     | 001000 | I    | 24    | 011000 | Y    | 40    | 101000 | o    | 56    | 111000 | 4    |
| 9     | 001001 | J    | 25    | 011001 | Z    | 41    | 101001 | p    | 57    | 111001 | 5    |
| 10    | 001010 | K    | 26    | 011010 | a    | 42    | 101010 | q    | 58    | 111010 | 6    |
| 11    | 001011 | L    | 27    | 011011 | b    | 43    | 101011 | r    | 59    | 111011 | 7    |
| 12    | 001100 | M    | 28    | 011100 | c    | 44    | 101100 | s    | 60    | 111100 | 8    |
| 13    | 001101 | N    | 29    | 011101 | d    | 45    | 101101 | t    | 61    | 111101 | 9    |
| 14    | 001110 | O    | 30    | 011110 | e    | 46    | 101110 | u    | 62    | 111110 | +    |
| 15    | 001111 | P    | 31    | 011111 | f    | 47    | 101111 | v    | 63    | 111111 | /    |

- ① YWJj
- ② Q0JB
- ③ QUJD
- ④ Y2Jh

19. 개인정보 가명 처리 세부기술에 대한 설명으로 옳지 않은 것은?

- ① 총계 처리는 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리한다.
- ② 일반 라운딩은 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법으로, 일반적으로 세세한 정보보다는 전체 통계 정보가 필요한 경우 많이 사용한다.
- ③ 로컬 일반화는 전체 정보집합물 중 특정 열 항목(들)에서 특이한 값을 가지거나 분포상의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는 방법이다.
- ④ 순서보존 암호화는 원문에 대한 암호화의 적용만 가능하고 암호문에 대한 복호화 적용이 불가능한 암호화 기법이다.

20. S/MIME에서 사용하는 암호 알고리즘과 기능을 옳게 짝지은 것은?

- ① DSS – 전자서명
- ② ElGamal – 메시지 인증
- ③ AES – 전자서명과 세션키 암호화
- ④ RSA – 메시지 암호화