

## 정보보호론

1. 다음에서 설명하는 디지털 포렌식의 기본 원칙은?

증거는 절차를 통해 삭제 또는 손상된 파일이 복구되는 과정을 거칠 수 있다. 이 증거를 법정에 제출하려면 같은 환경에서 같은 결과가 나와야 한다.

- ① 재현의 원칙  
② 신속성의 원칙  
③ 무결성의 원칙  
④ 연계 보관성의 원칙

2. RSA 공개키 암호에서 공개키를 ( $n = 11 \times 13$ ,  $e = 7$ )로 설정하였을 때, 공개키에 대응하는 개인키  $d$ 값은?

- ① 41  
② 87  
③ 97  
④ 103

3. AES의 암호화 과정에서 마지막 라운드에 포함되지 않는 연산은?

- ① SubBytes  
② ShiftRows  
③ MixColumns  
④ AddRoundKey

4. 다음 설명에 해당하는 공격 기법은?

브라우저로 전달되는 데이터에 악성 스크립트가 포함되어 사용자의 브라우저에서 실행되면서 해킹이 수행된다. 일반적인 공격 목적은 웹 사용자의 정보를 추출하는 것이다.

- ① XSS(Cross Site Scripting)  
② 리버스 텔넷(Reverse Telnet)  
③ 디렉터리 리스팅(Directory Listing)  
④ SQL(Structured Query Language) Injection

5. 리눅스 시스템 명령어와 기능의 설명 중 옳지 않은 것은?

- ① mv - 파일의 이름 변경과 이동  
② chmod - 파일의 사용 권한 변경  
③ rm - 파일 및 디렉터리 목록 보기  
④ umask - 생성하는 디렉터리의 기본 권한 설정

6. 윈도 명령 프롬프트 창에서 명령어 (가)를 실행한 화면의 일부이다. 이에 대한 설명으로 옳지 않은 것은? (단, 게이트웨이의 IP 주소는 172.21.70.1이고, 공격자의 IP 주소는 172.21.70.227이다)

C:\Users\windows> (가)

Interface: 172.21.70.180 --- 0xb

Internet Address	Physical Address	Type
172.21.70.1	18-67-e0-4d-40-5c	dynamic
172.21.70.2	00-0c-db-58-27-2d	dynamic
172.21.70.227	18-67-e0-4d-40-5c	dynamic
172.21.70.253	00-0e-5e-fc-16-c4	dynamic

- ① 명령어 (가)는 arp -a이다.  
② 게이트웨이의 ARP 테이블을 보여주는 화면이다.  
③ 공격 대상의 IP 주소는 172.21.70.180임을 나타낸다.  
④ 게이트웨이의 MAC 주소와 공격자의 MAC 주소가 같은 상태이다.

7. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증에 대한 설명으로 옳지 않은 것은?

- ① 인증심사의 종류는 예비심사, 최초심사, 사후심사, 갱신심사가 있다.  
② 정보보호 관리체계 인증은 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 것이다.  
③ 정보보호 및 개인정보보호 관리체계 인증기준은 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리 단계별 요구사항의 세 부분으로 구성되어 있다.  
④ 최초심사를 통해 인증을 취득하면 3년의 유효기간이 부여되며, 유효기간 중 매년 1회 이상 사후심사를 신청하여야 한다.

8. 블록암호 운영 모드 중 암호화 과정에서 초기벡터(IV)를 사용하지 않는 것은?

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

9. TLS(Transport Layer Security) 1.3 프로토콜에 대한 설명으로 옳은 것만을 모두 고르면? (단, 세션 재개(resumption)와 PSK(Pre-Shared Key) 방식은 고려하지 않는다)

- ㄱ. Handshake 프로토콜 이전에 클라이언트와 서버가 사용할 암호 알고리즘을 결정한다.  
ㄴ. Handshake 프로토콜에서 서버를 인증하려면 클라이언트는 서버의 인증서를 이용한다.  
ㄷ. Record 프로토콜에서 사용할 대칭키는 Handshake 프로토콜의 키교환으로부터 생성된다.  
ㄹ. Record 프로토콜에서 메시지 단편화, 암호화, 메시지인증 코드 추가 등이 수행된다.

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

10. 다음과 같은 특성을 갖추고 있는 보안 모델은?

- 최초의 수학적 모델이다.
- 강제적 접근 통제 방식으로 접근을 통제하며, 시스템 내부에 있는 정보의 기밀성을 보호한다.
- 주체는 주체보다 같거나 낮은 보안 수준의 객체만 읽을 수 있고, 주체보다 같거나 높은 보안 수준의 객체만 쓸 수 있다.

- ① 비바(Biba) 모델
- ② 만리장성(Chinese Wall) 모델
- ③ 클락-윌슨(Clark-Wilson) 모델
- ④ 벨-라파둘라(Bell-LaPadula) 모델

11. FIPS 202에서 명시된 SHA-3 표준에 대한 설명으로 옳지 않은 것은?

- ① KECCAK을 기반으로 한 해시함수 표준이다.
- ② SHAKE128, SHAKE256은 가변길이의 해시값을 출력한다.
- ③ SHA3-512는 256비트의 프리이미지 저항성을 갖는다.
- ④ SHA-2와 다른 스펀지(sponge) 구조를 이용한다.

12. 해시함수에 대한 설명으로 옳지 않은 것은?

- ① 무결성을 보장하는 HMAC은 두 단계의 해시 과정으로 안전성을 높인다.
- ② SHA-256을 생일공격으로 분석하려면 최소  $2^{256}$ 개의 해시값을 계산해야 한다.
- ③ DSA의 서명알고리즘은 메시지를 해시한 후 그 해시값을 이용하여 서명값을 생성한다.
- ④ 해시함수가 충돌저항성을 만족하면 제2 프리이미지 저항성도 만족한다.

13. 「개인정보 보호법」상 개인정보처리자가 준수해야 할 개인정보보호 원칙에 대한 설명으로 옳지 않은 것은?

- ① 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
- ② 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비공개 하여야 하며, 열람청구권 등 정보주체의 권리는 보장하여야 한다.
- ③ 개인정보의 처리 목적에 필요한 범위에서 적절하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
- ④ 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

14. 양자 컴퓨팅과 그에 대응하는 암호기법에 대한 설명으로 옳지 않은 것은?

- ① 양자 컴퓨팅은 양자 중첩과 양자 얽힘 등의 양자역학 특성을 이용한다.
- ② AES-256은 이상적인 양자 컴퓨팅하에서 256비트 안전성을 보장한다.
- ③ 이상적인 양자 컴퓨팅하에서 RSA 및 타원곡선암호(ECC)는 더 이상 안전하지 않다.
- ④ 미국 NIST는 양자 컴퓨팅에 대응하기 위해 양자내성암호(PQC, Post-Quantum Cryptography) 표준을 발표하였다.

15. A가 전자서명 및 공개키 암호기법을 이용하여, 메시지(M)를 안전하게 B에게 전송하는 과정이다. 동작 순서를 바르게 나열한 것은? (단, A는 B의 공개키를 알고 있다)

- (가) A의 서명키로 해시값을 전자서명한다.
- (나) A의 서명검증키와 암호문을 B에게 전송한다.
- (다) 메시지(M)의 해시값을 구한다.
- (라) B의 공개키를 이용한 하이브리드 방식으로 메시지(M)와 전자서명값을 암호화한다.

- ① (가) → (다) → (나) → (라)
- ② (가) → (라) → (다) → (나)
- ③ (다) → (가) → (라) → (나)
- ④ (다) → (라) → (나) → (가)

16. 정보보호시스템 공통평가기준(Common Criteria)의 등급별 EAL(Evaluation Assurance Level)의 목적에 대한 설명으로 옳지 않은 것은? (단, TOE(Target of Evaluation)는 평가대상이다)

- ① EAL1: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서를 이용하여 제한적인 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 기초적인 수준의 보증을 제공한다.
- ② EAL2: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서, TOE 구조의 기본적 설명을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.
- ③ EAL3: 보안 행동을 이해하기 위해 기능 및 인터페이스 명세, 설명서, TOE 설계의 아키텍처 설명을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.
- ④ EAL4: 보안 행동을 이해하기 위해 기능 및 완전한 인터페이스 명세, 설명서, TOE에 대한 설계 서술, 구현을 이용하여 완전한 보안목표명세서에 포함된 보안기능요구사항을 분석함으로써 보증을 제공한다.

17. 「개인정보 보호법 시행령」상 개인정보처리자가 정보주체의 동의 없이 개인정보를 이용 또는 제공하려는 경우 고려하여야 할 사항이 아닌 것은?

- ① 당초 수집 목적과 관련성이 있는지 여부
- ② 정보주체의 이익을 부당하게 침해하는지 여부
- ③ 개인정보 수집기관의 영업이익이 지속적으로 발생하는지 여부
- ④ 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

18. 다음의 사이버 공격 유형 (가) ~ (다)와 이에 대한 설명 A ~ C를 바르게 연결한 것은?

- (가) 스미싱(smishing)  
(나) 백도어(backdoor)  
(다) 키로깅(keylogging)

- A. 사용자가 키보드로 입력하는 정보를 몰래 가로채는 방법으로 트로이 목마 같은 악성코드와 결합하여 동작한다.  
B. 정상적인 사용자 인증 절차를 거치지 않고 응용 프로그램이나 시스템에 접근할 수 있는 보안 허점을 이용한다.  
C. 신뢰할 수 있는 사람이 보낸 문자메시지처럼 가장하여 링크 접속을 유도한 뒤 개인정보를 빼내는 수법이다.

- |   | (가) | (나) | (다) |
|---|-----|-----|-----|
| ① | A   | B   | C   |
| ② | B   | C   | A   |
| ③ | C   | A   | B   |
| ④ | C   | B   | A   |

19. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하는 자에 대한 금지행위가 아닌 것은?

- ① 광고성 정보 수신자의 수신거부 또는 수신동의의 철회를 회피·방해하는 행위
- ② 영리목적의 광고성 정보를 전송할 목적으로 전화번호 또는 전자우편주소를 자동으로 등록하는 행위
- ③ 광고성 정보 전송자의 신원이나 광고 전송 출처를 감추기 위한 각종 행위
- ④ 수신자가 수신거부나 수신동의의 철회를 할 때 발생하는 전화요금 등의 금전적 비용을 수신자가 부담하지 않도록 하는 행위

20. 국가사이버안보센터가 24시간 365일 국내 사이버 위협 수준을 평가하고 발령하는 사이버 위기 경보단계에 대한 설명으로 옳지 않은 것은?

- ① 정상: 워·바이러스, 해킹기법 등에 의한 피해발생 가능성이 증가
- ② 심각: 국가적 차원의 평가와 조치가 필요하다고 판단되는 사고가 발생
- ③ 주의: 다수기관의 정보통신망 및 정보시스템에 장애가 발생
- ④ 경계: 복수분야에서 광범위한 피해가 발생하는 등 대규모 피해로 확대될 가능성이 높아 다수기관의 공조대응이 필요

21. 리눅스 시스템의 로그 파일에 대한 설명으로 옳지 않은 것은?

- ① history: 텔넷이나 FTP, 원격 접속 등 인증과정을 거치는 로그를 저장한다.
- ② wtmp: 사용자의 로그인과 로그아웃한 정보 등을 저장한다.
- ③ lastlog: 사용자 이름, 포트, 마지막 로그인 시간 등을 저장한다.
- ④ utmp: 현재 로그인한 사용자 이름, 로그인한 디바이스 등을 저장한다.

22. 침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?

- ① 시그니처 기반(Signature-based) 침입탐지시스템은 신종 공격이나 변형된 공격을 능동적으로 탐지할 확률이 높은 장점이 있다.
- ② 비정상 기반(Anomaly-based) 침입탐지시스템은 정상적인 행위에 대한 모델을 만들어 놓고 그 모델에서 벗어나면 비정상으로 판단한다.
- ③ 호스트 기반(Host-based) 침입탐지시스템은 호스트에서 실행 중인 시스템 및 응용 프로그램의 로그를 이용하여 호스트 시스템에 가해지는 공격을 탐지한다.
- ④ 네트워크 기반(Network-based) 침입탐지시스템은 네트워크에서 전송되는 트래픽을 수집하고 정제한 후 분석하여 공격을 탐지한다.

23. 랜섬웨어(ransomware)에 대한 설명으로 옳지 않은 것은?

- ① 공격자는 사용자의 컴퓨터를 장악하거나 데이터를 암호화한 후 정상적인 작동을 조건으로 대가를 요구한다.
- ② 암호화된 파일을 풀어 주는 대가로 비트코인(Bitcoin) 등 가상자산을 요구하는 공격으로 진화하고 있다.
- ③ 랜섬웨어 중 하나인 워너크라이(WannaCry)는 리눅스의 원격 접속 프로토콜의 취약점을 활용하였다.
- ④ 랜섬웨어를 제작하여 공급·판매하는 방식인 RaaS(Ransomware as a Service)가 등장하였다.

24. IPSec 터널모드에 대한 설명으로 옳지 않은 것은?

- ① 양측 호스트가 속한 라우터 또는 게이트웨이 간에 IPSec 터널링을 설정한다.
- ② 호스트가 생성한 전송계층의 세그먼트를 페이로드(payload)로 취급하고 IP 헤더를 추가한다.
- ③ ESP와 결합하면, 터널링 구간에서 양측 호스트의 IP 주소는 외부 공격자에게 숨겨진다.
- ④ SA(Security Association) 생성, 키교환 및 상호인증을 위해 IKE 프로토콜을 사용한다.

25. 「개인정보 보호법 시행령」상 개인정보보호위원회가 개인정보처리자에게 자료의 제출을 요구할 수 있는 사항에 해당하지 않는 것은?

- ① 개인정보처리자가 처리하는 이동형 영상정보처리기의 설치·운영에 관한 사항
- ② 개인정보 보호책임자에게 부과된 과태료에 관한 사항
- ③ 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항
- ④ 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항