

- 정보 보안의 3대 요소인 기밀성(confidentiality), 무결성(integrity), 가용성(availability)에 대한 설명으로 가장 옳지 않은 것은?
  - 기밀성은 인가된 사용자만 정보 자산에 접근할 수 있다는 것이다.
  - 무결성은 권한을 가진 사용자만 인가된 방법으로 정보를 변경할 수 있도록 하는 것이다.
  - 가용성은 인가된 사용자에게 제한된 시점에만 정보 자산에 대한 접근이 가능하도록 하는 것이다.
  - 기밀성의 대표적인 서비스로 방화벽, 암호 등이 있다.
- 블록암호의 운용 방식 중 ECB(Electric Code Book) 모드에 대한 설명으로 가장 옳지 않은 것은?
  - 긴 메시지를 블록 단위로 나누어 각각을 블록암호를 이용하여 암호화하는 방법이다.
  - 동일한 메시지 블록을 동일한 키로 암호화하면 동일한 암호문이 생성되기 때문에 보안 문제가 발생할 수 있다.
  - 메시지가 주어졌을 때 병렬 연산이 가능하다.
  - 메시지가 주어지기 전에 사전 계산이 가능하기 때문에, 이를 이용하여 효율을 높일 수 있다.
- 일방향 해시 함수에 대한 설명으로 가장 옳지 않은 것은?
  - MD4, MD5는 128비트 길이의 해시값을 출력하며 현재는 둘 다 안전하지 않다.
  - SHA-1은 180비트 길이의 해시값을 출력하며 강한 충돌 내성에 대한 취약점이 발견되어 안전하지 않다.
  - SHA-256, SHA-384, SHA-512는 각 256, 384, 512비트 길이의 해시값을 출력하며, 입력하는 메시지 길이는 SHA-256은  $2^{64}$ 비트 미만, SHA-384와 SHA-512는  $2^{128}$ 비트 미만으로 제한된다.
  - RIPMD-160은 160비트 길이의 해시값을 출력하며, RIPMD 함수를 수정하여 개발됐고, 비트코인에서 사용되기도 한다.
- RSA 암호 알고리즘에서 키 생성을 위해 두 개의 서로 다른 소수를 곱한 값인  $N=7 \times 11=77$ 이 주어졌다고 할 때, 공개키로 선택할 수 있는 가장 옳은 값은?
  - 3
  - 5
  - 7
  - 9
- 접근 제어 모델 중 하나인 비바(Biba) 모델에 대한 설명으로 가장 옳은 것은?
  - 임의적 접근 제어 모델(Discretionary Access Control)에 해당한다.
  - 수학적 보안 모델로 데이터의 기밀성에 초점을 맞춰 설계되었다.
  - 자신에게 허용된 보안 레벨보다 높은 보안 레벨의 문서에 대한 읽기가 허용되지 않는다.
  - 자신에게 허용된 보안 레벨보다 낮은 보안 레벨의 문서에 대한 쓰기가 허용된다.
- 버퍼 오버플로 공격에 대한 대응책 중 스택 실드에 대한 설명으로 가장 옳은 것은?
  - 스택에서 실행 권한을 제거하여 스택에 로드된 공격자의 공격 코드를 실행하지 못하도록 한다.
  - 컴파일러가 프로그램의 함수를 호출할 때 ret 앞에 canary값을 주입하고, 종료할 때 canary값의 변조 여부를 확인한다.
  - 함수를 호출할 때 ret값을 Global RET Stack이라는 특수 스택에 저장한 뒤, 함수를 종료할 때 Global RET Stack에 저장된 ret값과 스택의 ret값을 비교한다.
  - 스택, 힙, 라이브러리 등 데이터 영역의 주소를 난수화한다.
- 리눅스/유닉스 시스템에서 SetUID에 대한 설명으로 가장 옳지 않은 것은?
  - 시스템에 로그인한 계정은 일반적으로 시스템으로부터 처음 부여받은 RUID(Real UID)와 EUID(Effective UID)의 값이 동일하지만, SetUID 비트를 가진 프로그램을 실행하면 잠시 일치하지 않는 상태가 발생한다.
  - /usr/bin/passwd 파일에 SetUID가 설정되면 파일 소유주가 root이기 때문에, 이 파일이 실행되는 프로세스는 실행 시간 동안 root 권한을 갖는다.
  - 'find / -user root -perm /4000'과 같은 find 명령을 사용하면 SetUID가 설정된 파일들을 검색할 수 있다.
  - /usr/bin/passwd 파일에 SetUID가 설정되면 권한은 2755(rws r-x r-x)이다.

8. 디지털 서명에 대한 설명으로 가장 옳은 것은?

- ① 문서의 기밀성을 위한 기술이다.
- ② 문서의 크기가 크면 문서의 해시값에 서명한다.
- ③ 문서의 전송자가 누구인지는 알아낼 수 없다.
- ④ 공개키 방식일 경우, 공개키로 서명하고 비밀키로 검증한다.

9. 미국 NIST에서 추진 중인 양자내성암호(Post-Quantum Cryptography)에 대한 설명으로 옳은 것을 <보기>에서 모두 고른 것은?

<보기>

- ㄱ. 양자내성암호는 양자 컴퓨팅 환경에서 안전하게 암호 기술을 이용할 수 있도록 하는 새로운 공개키 암호이다.
- ㄴ. 1996년 그루버(Grover)는 양자 컴퓨팅을 이용한 연산으로 RSA 암호의 안전성 기반 문제인 인수분해 문제를 이론적으로 해독할 수 있는 알고리즘을 개발하였다.
- ㄷ. NIST는 양자내성암호화 알고리즘 표준으로 2022년에 FALCON, SPHINCS+, CRYSTALS-KYBER, CRYSTALS-DILITHIUM을 선정하였다.
- ㄹ. ECDSA는 양자 컴퓨팅을 이용한 연산으로도 해독이 불가능하여 안전하게 사용할 수 있다.

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

10. 스니핑(sniffing) 공격의 보안 대책과 이에 대한 설명으로 가장 옳지 않은 것은?

- ① Ping을 이용한 스니퍼 탐지 - 네트워크에 존재하지 않는 MAC 주소로 위장하여 스니퍼로 의심되는 호스트에 ping을 보냈을 때, ping에 대한 응답이 오는 경우 스니퍼로 탐지할 수 있다.
- ② ARP를 이용한 스니퍼 탐지 - 스니퍼로 의심되는 호스트에게 위조된 ARP Request를 보냈을 때, ARP Response가 오면 해당 호스트가 프러미스큐어스(promiscuous) 모드로 설정된 것이기 때문에 스니퍼로 탐지할 수 있다.
- ③ DNS를 이용한 스니퍼 탐지 - 스니핑 프로그램은 일반적으로 DNS에 대한 이름을 해석하기 위해 Reverse-DNS lookup을 수행하기 때문에, 의심되는 호스트에게 ping sweep을 보내고, 들어오는 Reverse-DNS lookup을 감시하여 스니퍼를 탐지한다.
- ④ 유인을 이용한 스니퍼 탐지 - MAC 주소와 IP 주소의 매칭 값을 저장하고 ARP 트래픽을 모니터링하여 이 매칭 값을 변하게 하는 패킷이 탐지되면, 위조된 ARP를 사용하는 스니퍼로 탐지한다.

11. SSH(Secure Shell)에 대한 설명으로 가장 옳은 것은?

- ① 서버에서는 기본적으로 80번 포트를 이용한다.
- ② 익명 계정을 이용하여 누구나 접속할 수 있다.
- ③ 포트 포워딩 기술을 이용하여 보안 수준이 낮은 환경에서도 안전하게 연결할 수 있다.
- ④ 원격 컴퓨터에 접속하기 위한 기술로, 보안 문제 때문에 SSH 대신 telnet을 사용할 것을 권장하고 있다.

12. 작업 증명(Proof of Work) 기반의 블록체인에서 블록을 블록체인 네트워크에 추가하는 행위는?

- ① 분산 원장(distributed ledger)
- ② 블로킹(blocking)
- ③ 트랜잭션(transaction)
- ④ 채굴(mining)

13. XSS(Cross Site Scripting) 공격에 대한 설명으로 가장 옳지 않은 것은?

- ① XSS 공격 유형 중 Stored XSS는 게시판 또는 자료실과 같이 사용자가 글을 저장하는 부분에 정상적인 평문이 아닌 스크립트 코드를 입력하는 기법이다.
- ② XSS 취약점을 확인할 수 있는 예제 코드는 `SELECT name FROM sysobjects WHERE xtype= 'U'`와 같다.
- ③ 크로스 사이트 요청 변조 공격인 CSRF 공격은 피해자가 인지하지 못하는 상태에서 피해자의 브라우저가 특정 사이트에 강제적으로 리퀘스트를 보내도록 하는 기법이다.
- ④ XSS 공격 유형 중 Reflected XSS는 웹 애플리케이션에 스크립트를 저장하는 것이 아니라 URL의 변수 부분처럼 스크립트 코드를 입력하는 동시에 결과가 바로 전해지는 공격 기법이다.

14. 시스템에 침투하기 위한 일반적인 웹 해킹 과정의 순서로 가장 옳은 것은?

- ① 공격 대상 선정 → 정보 수집 → 취약점 분석 → 공격
- ② 정보 수집 → 공격 대상 선정 → 취약점 분석 → 공격
- ③ 공격 대상 선정 → 취약점 분석 → 공격 → 정보 수집
- ④ 취약점 분석 → 공격 대상 선정 → 정보 수집 → 공격

15. HTTPS(HTTP over Secure Socket Layer)에 대한 설명으로 가장 옳지 않은 것은?

- ① 요청 문서의 URL과 문서 내용, HTTP 헤더 내용, 폼 요소 내용은 암호화되지만 쿠키는 암호화되지 않는다.
- ② HTTPS 연결이 명시되면 포트번호는 기본적으로 443번이 사용되고 SSL이 호출된다.
- ③ HTTPS를 사용하는 웹 페이지의 URI는 http:// 대신 https://로 시작한다.
- ④ 1994년에 넷스케이프사에서 HTTPS를 개발하였다.

16. <보기>는 IPv4 패킷에 대해서 IPSec 터널 모드의 ESP(Encapsulation Security Payload) 프로토콜을 적용한 결과이다. (가)~(라)에 들어갈 항목들을 가장 옳게 짝지은 것은?

<보기>						
(가)	(나)	IP Header	TCP Header	Data	(다)	(라)

	(가)	(나)	(다)	(라)
①	New IP Header	ESP Header	ESP Trailer	ESP Authentication
②	ESP Header	New IP Header	ESP Authentication	ESP Trailer
③	New IP Header	ESP Header	ESP Authentication	ESP Trailer
④	ESP Header	New IP Header	ESP Trailer	ESP Authentication

17. 디지털 포렌식 수행 절차에 대한 설명으로 가장 옳지 않은 것은?

- ① 수사 준비 - 디지털 기기의 데이터 수집 및 분석을 위한 장비와 틀을 확보하고 적절한 법적 절차를 거쳐 피의자 또는 수사 대상에 접근한다.
- ② 증거물 획득 - 디지털 포렌식 수사 현장에서 증거를 획득하는 사람과 그 과정에서 위법 여부의 존재 유무를 감독하는 사람, 인증하는 사람의 참관하에 증거를 획득한다.
- ③ 분석 및 조사 - 현장에서 획득된 증거인 원본을 다양한 디지털 포렌식 도구를 사용하여 조사 및 분석한다.
- ④ 보고서 작성 - 분석에 사용한 증거 데이터, 분석 및 조사 과정에서 증거 수집을 위해 문서화한 무결성과 관련된 정보 등을 보고서로 작성한다.

18. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조의3에서 정의하고 있는 정보보호 최고책임자가 총괄하는 업무로 가장 옳지 않은 것은?

- ① 정보보호 실태와 관행의 정기적인 감사 및 개선
- ② 정보보호 위험의 식별 평가 및 정보보호 대책 마련
- ③ 개인정보 보호 교육 계획의 수립 및 시행
- ④ 정보보호 계획의 수립·시행 및 개선

19. 정보보호 및 개인정보보호 관리체계 인증 기준의 보호 대책 요구사항 분야와 항목이 바르게 짝지어진 것으로 옳지 않은 것은?

분야

항목

- |                    |                |
|--------------------|----------------|
| ① 정보시스템 도입 및 개발 보안 | 운영환경 이관        |
| ② 접근 통제            | 접근권한 검토        |
| ③ 시스템 및 서비스 보안관리   | 정보전송 보안        |
| ④ 시스템 및 서비스 운영관리   | 정보자산의 재사용 및 폐기 |

20. <보기>에서 CC(Common Criteria: 공통평가기준)에 대한 설명으로 옳은 것을 모두 고른 것은?

<보기>

- ㄱ. CC는 IT 제품의 보안성을 평가하기 위한 국제표준(ISO)으로 국가 간 평가결과를 상호인정하기 위해 미국, 유럽 등 여러 국가의 평가기준을 참조하여 개발한 단일화된 평가기준이다.
- ㄴ. CC는 적용범위가 IT 제품에만 한정되지 않으므로 TOE(Target of Evaluation)라는 용어를 사용하며, TOE의 예시로 응용 소프트웨어, 운영체제 + 운영소프트웨어, 스마트카드 IC칩 등이 있다.
- ㄷ. 보안목표명세서(Security Target)는 사용자의 보안 요구를 표현하기 위해 CC를 준용하여 작성된 것으로 보안기능을 포함한 IT 제품이 갖추어야 할 보안요구 사항 집합이다.
- ㄹ. 보호프로파일(Protection Profile)은 개발자가 특정 IT 제품의 보안기능을 표현하기 위해 CC를 준용하여 작성한 것으로 제품 평가를 위한 기초자료로 사용된다.

① ㄱ, ㄴ

② ㄱ, ㄷ

③ ㄴ, ㄹ

④ ㄷ, ㄹ