

정보보호론

문 1. 패스워드 공격에 해당하지 않는 것은?

- ① 사전 대입 공격
- ② 이블 트윈 공격
- ③ 무작위 대입 공격
- ④ 레인보우 테이블을 이용한 공격

문 2. 역할기반 접근제어(RBAC)에 대한 설명으로 옳은 것은?

- ① 정보의 소유자가 특정 사용자와 그룹에 특정 권한을 부여한다.
- ② 사용자에게 부여된 권한에 따라 사용자를 역할로 분류하여 각 사용자에게 하나의 역할만 할당되도록 한다.
- ③ 역할 및 역할이 수행할 권한을 정의하고, 사용자를 역할에 할당하는 방식이다.
- ④ 기밀문서가 엄격히 다루어져야 하는 군이나 정보기관 등에서의 중앙집중형 보안 관리에 적합하다.

문 3. 정보시스템의 침입자를 속이는 기법의 하나로, 가상의 정보시스템을 만들어 놓고 실제로 공격을 당하는 것처럼 보이게 하여 해커나 스파, 바이러스를 유인하여 침입자들의 정보를 수집하고 추적하는 역할을 수행하는 것은?

- ① Honeypot
- ② IPS
- ③ ESM
- ④ DRM

문 4. 공개키 기반구조(PKI)에 대한 설명으로 옳지 않은 것은?

- ① PKI는 인증기관, 등록기관, 저장소, 사용자 등으로 구성된다.
- ② 인증서의 폐지 여부를 확인하기 위해 인증기관은 인증서 폐지 목록(CRL)을 주기적으로 관리한다.
- ③ 유효기간 내의 인증서를 가지고 있다면, 사용자는 별도로 CRL을 조사할 필요가 없다.
- ④ 한 인증기관이 다른 인증기관의 공개키를 검증하는 것이 가능하므로, 사용자는 모든 인증기관의 공개키를 사전에 가지고 있을 필요가 없다.

문 5. HTTP 응답 메시지 상태코드의 의미가 옳지 않은 것은?

- ① 201 - Created
- ② 301 - Moved Permanently
- ③ 401 - Unauthorized
- ④ 501 - Bad Request

문 6. 괄호 안에 들어갈 용어를 바르게 연결한 것은?

IPSec의 (㉠)는 발신지 인증과 데이터 무결성 그리고 데이터 기밀성을 제공한다. 두 호스트 사이의 논리적 관계인 SA (Security Association)를 생성하기 위하여 (㉡) 프로토콜을 사용하여 보안상 안전한 채널을 확보한다.

- | | |
|-------|------|
| ㉠ | ㉡ |
| ① AH | OSPF |
| ② AH | IKE |
| ③ ESP | IKE |
| ④ ESP | OSPF |

문 7. 괄호 안에 들어갈 접근 권한을 바르게 연결한 것은?

리눅스 시스템에서 umask 값을 027로 설정할 경우, 이후 생성되는 일반 파일의 접근 권한은 (㉠)이고, 디렉터리 접근 권한은 (㉡)이다.

- | | |
|-------|-----|
| ㉠ | ㉡ |
| ① 640 | 750 |
| ② 750 | 640 |
| ③ 644 | 755 |
| ④ 755 | 644 |

문 8. ISMS-P에 대한 설명으로 옳지 않은 것은?

- ① 인증기준은 크게 3개 영역으로 나뉘며 총 102개의 인증기준으로 구성되어 있다.
- ② 관리체계 수립 및 운영 영역은 4개 분야 16개 인증기준으로 구성되어 있다.
- ③ 보호대책 요구사항 영역은 12개 분야 64개 인증기준으로 구성되어 있다.
- ④ 개인정보 처리단계별 요구사항 영역은 6개 분야 24개의 인증기준으로 구성되어 있다.

문 9. 「개인정보 보호법」상의 개인정보 보호위원회에 대한 조항의 일부이다. 괄호 안에 들어갈 용어를 바르게 연결한 것은?

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 (㉠) 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.
② 보호위원회는 「정부조직법」 제2조에 따른 (㉡)으로 본다.

- | | |
|--------|--------------|
| ㉠ | ㉡ |
| ① 대통령 | 중앙행정기관의 보조기관 |
| ② 대통령 | 중앙행정기관 |
| ③ 국무총리 | 중앙행정기관의 보조기관 |
| ④ 국무총리 | 중앙행정기관 |

문 10. 타원 곡선 암호에 대한 설명으로 옳은 것만을 모두 고른 것은?

ㄱ. 타원 곡선은 함수 $y^2 = x^3 + ax + b$ 의 형태로 $4a^3 + 27b^2 \neq 0$ 의 조건을 만족해야 한다.
ㄴ. 임의의 평문과 암호문은 타원 곡선상의 점으로 표현되며, 곡선상의 모든 점들이 암호에 사용될 수 있다.
ㄷ. 타원 곡선상의 서로 다른 두 점, P와 Q의 합의 연산 (P + Q)은 P와 Q를 연결하는 직선과 교차하는 곡선상의 점이다.
ㄹ. 타원 곡선 암호는, k와 P로부터 Q = kP를 만족하는 Q를 구하는 것은 비교적 쉽지만, 주어진 Q와 P로 k를 결정하는 것은 매우 어렵다는 점을 이용한 것이다. 여기서, P와 Q는 타원 곡선상의 점들이고 k는 일정 조건을 만족하는 값이다.

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

문 11. 버퍼 오버플로우 공격에 대한 설명으로 옳지 않은 것은?

- ① 스택 오버플로우와 힙 오버플로우 공격 등이 있다.
- ② 버퍼에 일정한 크기 이상의 데이터를 입력하여 프로그램을 공격한다.
- ③ 취약한 C함수로는 strcpy(), strcat(), gets() 등이 있다.
- ④ 대응 방법의 하나인 스택 가드는 스택에서 권한을 제거해 스택에 로드된 공격자의 공격 코드가 실행될 수 없도록 한다.

문 12. 공인인증기관의 지정 등 공인인증서 관련 사항을 규정한 법은?

- ① 전자정부법
- ② 전자서명법
- ③ 신용정보의 이용 및 보호에 관한 법률
- ④ 정보통신망 이용촉진 및 정보보호 등에 관한 법률

문 13. 상해 위험 분석 방법에 대한 설명으로 옳은 것은?

- ① 시스템에 대해 보호의 기준 수준을 정하고, 목표를 달성하기 위하여 일련의 보호 대책을 선택한다.
- ② 모든 시스템에 적절한 기준 보안 대책을 이행하고, 상위 수준의 위험 평가를 통하여 중요하고 위험이 높은 시스템을 식별하고 평가한다.
- ③ 숙달된 전문가의 경험에 따라서 효율적으로 위험 분석을 수행한다.
- ④ 정형화되고 구조화된 프로세스를 사용하여 모든 중요한 위험을 식별하고 그 영향을 고려한다.

문 14. 설치된 백도어를 탐지하는 방법의 하나는 현재 동작 중인 프로세스를 확인하는 것이다. 다음 설명에 해당하는 윈도우 프로세스를 바르게 나열한 것은?

- ㄱ. 시스템에 대한 백업이나 업데이트에 관련된 작업의 스케줄러 프로세스
 ㄴ. DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스
 ㄷ. 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스

- | ㄱ | ㄴ | ㄷ |
|-------------|-------------|-------------|
| ① smss.exe | svchost.exe | csrss.exe |
| ② smss.exe | csrss.exe | svchost.exe |
| ③ mtask.exe | svchost.exe | csrss.exe |
| ④ mtask.exe | csrss.exe | svchost.exe |

문 15. 다음은 아래 범례를 사용하여 사용자 A가 사용자 B에게 메시지 M을 전송하기 위한 프로토콜을 순서대로 나타낸 것이다.

ID_U : U의 아이디, KU_U : U의 공개키, KR_U : U의 개인키
 $E(K, M)$: 메시지 M을 키 K로 암호화하는 함수
 $D(K, C)$: 암호문 C를 키 K로 복호화하는 함수

$B \rightarrow A: ID_B, KU_B$
 $A \rightarrow B: ID_A, C$ [단, $C = E(KU_B, M)$]
 $B: M = D(KR_B, C)$

위의 프로토콜에 대하여 다음과 같은 순서로 공격이 가능하다. 이 공격에 대한 설명으로 옳지 않은 것은?

$B \rightarrow X: ID_B, KU_B$
 $X \rightarrow A: ID_B, KU_X$
 $A \rightarrow X: ID_A, C'$ [단, $C' = E(KU_X, M)$]
 $X: M = D(KR_X, C')$
 $X \rightarrow B: ID_A, C$ [단, $C = E(KU_B, M)$]
 $B: M = D(KR_B, C)$

- ① A가 B의 공개키를 검증하지 못해서 발생하는 중간자 공격이다.
- ② 공격자 X가 A의 메시지를 가로채서 다시 보내는 재전송 공격이다.
- ③ 공개키 인증서를 사용하면 방지할 수 있다.
- ④ 디피-헬만 키 교환에서도 발생할 수 있다.

문 16. 다음은 FTP에서 데이터 연결을 생성하는 과정을 순서대로 설명한 것이다. 괄호 안에 들어갈 용어를 바르게 나열한 것은?

- (㉠)가 임시 포트로 (㉡) 연결 설정을 시도한다.
 ○ (㉢)는 이 포트 번호를 PORT 명령어를 사용하여 (㉣)에 전송한다.
 ○ (㉤)는 포트 번호를 수신한 후, 잘 알려진 포트 20과 임시 포트 번호를 사용하여 (㉥) 연결 설정을 시도한다.

- | ㉠ | ㉡ | ㉢ | ㉣ |
|---------|-----|-------|-----|
| ① 클라이언트 | 수동적 | 서버 | 능동적 |
| ② 클라이언트 | 능동적 | 서버 | 수동적 |
| ③ 서버 | 수동적 | 클라이언트 | 능동적 |
| ④ 서버 | 능동적 | 클라이언트 | 수동적 |

문 17. 안전한 소프트웨어 개발 방법론의 하나인 MS사의 SDL(Secure Development Lifecycle)의 소프트웨어 개발 프로세스 중 위험 모델링을 수행해야 하는 단계는?

- ① 계획·분석
- ② 설계
- ③ 구현
- ④ 시험·검증

문 18. 엔트로피에 대한 설명으로 옳은 것만을 모두 고른 것은?

- ㄱ. 한 비트가 가질 수 있는 엔트로피의 최댓값은 1이다.
 ㄴ. 블록 암호문의 엔트로피는 낮을수록 안전하다.
 ㄷ. 엔트로피는 정보량 또는 정보의 불확실도를 측정하는 수학적 개념이다.
 ㄹ. 어떤 확률변수가 가질 수 있는 모든 값의 발생 확률이 같을 경우, 엔트로피는 최솟값을 갖는다.

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

문 19. 사용자 B가 메시지 M과 함께 $H(M \text{ XOR } K_{AB})$ 를 MAC로 하여 사용자 A에게 보내고, A는 수신한 MAC와 M으로부터 산출한 MAC를 비교함으로써 보안을 강화한 경우에 대한 설명으로 옳지 않은 것은? (단, K_{AB} 는 A와 B의 공유 비밀키, H는 해시 함수)

- ① A는 메시지 M의 무결성을 확인할 수 있다.
- ② A는 메시지 M의 출처가 B라는 것을 확인할 수 있다.
- ③ A는 B가 메시지 M에 대하여 부인하지 못하도록 하는 부인 봉쇄를 보장받을 수 있다.
- ④ MAC에 시간이나 순서 정보가 포함되어 있지 않다면, 재전송 공격이 발생할 가능성이 있다.

문 20. 「정보통신기반 보호법」상의 정보통신기반보호위원회에 관한 사항으로 옳지 않은 것은?

- ① 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반 시설의 보호에 관한 사항을 심의하기 위하여 국무총리 소속하에 정보통신기반보호위원회(이하 “위원회”라 한다)를 둔다.
- ② 위원회의 위원은 위원장 1인을 포함한 25인 이내의 위원으로 구성한다.
- ③ 위원회의 위원장은 과학기술정보통신부장관이 되고, 위원회의 위원은 대통령령으로 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 사람으로 한다.
- ④ 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간 분야를 각각 담당하는 실무위원회를 둔다.