1과목 : 과목 구분 없음

1. 겉으로는 유용한 프로그램으로 보이지만 사용자가 의도하지 않은 악성 루틴이 숨어 있어서 사용자가 실행시키면 동작하는 악성 소프트웨어는?

① 키로거 ❷ 트로이목마
③ 애드웨어 ④ 랜섬웨어

2. 능동적 공격에 해당하는 것만을 모두 고르면?

ㄱ. 도청	ㄴ. 서비스 거부
ㄷ. 트래픽 분석	ㄹ. 메시지 변조

① ㄱ, ㄷ ② ㄴ, ㄷ
❸ ㄴ, ㄹ ④ ㄷ, ㄹ

3. 분산 서비스 거부(DDoS) 공격에 대한 설명으로 옳지 않은 것은?

❶ 하나의 공격 지점에서 대규모 공격 패킷을 발생시켜서 여러 사이트를 동시에 공격하는 방법이다.
② 가용성에 대한 공격이다.
③ 봇넷이 주로 활용된다.
④ 네트워크 대역폭이나 컴퓨터 시스템 자원을 공격 대상으로 한다.

4. 부인방지 서비스를 제공하기 위한 전자서명에 대한 설명으로 옳지 않은 것은?

① 서명할 문서에 의존하는 비트 패턴이어야 한다.
② 다른 문서에 사용된 서명을 재사용하는 것이 불가능해야 한다.
❸ 전송자(서명자)와 수신자(검증자)가 공유한 비밀 정보를 이용하여 서명하여야 한다.
④ 서명한 문서의 내용을 임의로 변조하는 것이 불가능해야 한다.

5. 다음은 IT 보안 관리를 위한 국제 표준(ISO/IEC 13335)의 위험 분석 방법에 대한 설명이다. ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

(㉠)은 가능한 빠른 시간 내에 적정 수준의 보호를 제공한 후 시간을 두고 중요 시스템에 대한 보호 수단을 조사하고 조정하는 것을 목표로 한다. 이 방법은 모든 시스템에 대하여 (㉡)에서 제시하는 권고 사항을 구현하는 것으로 시작한다. 중요 시스템을 대상으로 위험에 즉각적으로 대응하기 위하여 비정형 접근법이 적용될 수 있다. 그리고 (㉢)에 의한 단계별 프로세스를 적절하게 수행한다. 결과적으로 시간이 흐름에 따라 비용 대비 효과적인 보안 통제가 선택되도록 할 수 있다.

	㉠	㉡	㉢
①	상세 위험 분석	기준선 접근법	복합 접근법
②	상세 위험 분석	복합 접근법	기준선 접근법
③	복합 접근법	기준선 접근법	상세 위험 분석
④	복합 접근법	상세 위험 분석	기준선 접근법

① ① ② ②
❸ ③ ④ ④

6. 다음에서 설명하는 크로스사이트 스크립팅(XSS) 공격의 유형은?

공격자는 XSS 코드를 포함한 URL을 사용자에게 보낸다. 사용자가 그 URL을 요청하고 해당 웹 서버가 사용자 요청에 응답한다. 이때 XSS 코드를 포함한 스크립트가 웹 서버로부터 사용자에게 전달되고 사용자 측에서 스크립트가 실행된다.

① 세컨드 오더 XSS ② DOM 기반 XSS
③ 저장 XSS ❹ 반사 XSS

7. SHA 알고리즘에서 사용하는 블록 크기와 출력되는 해시의 길이를 바르게 연결한 것은?

	알고리즘	블록 크기	해시 길이
①	SHA-1	256비트	160비트
②	SHA-256	512비트	256비트
③	SHA-384	1024비트	256비트
④	SHA-512	512비트	512비트

① ① ❷ ②
③ ③ ④ ④

8. 데이터베이스 접근 권한 관리를 위한 DCL(Data Control Language)에 속하는 명령으로 그 설명이 옳은 것은?

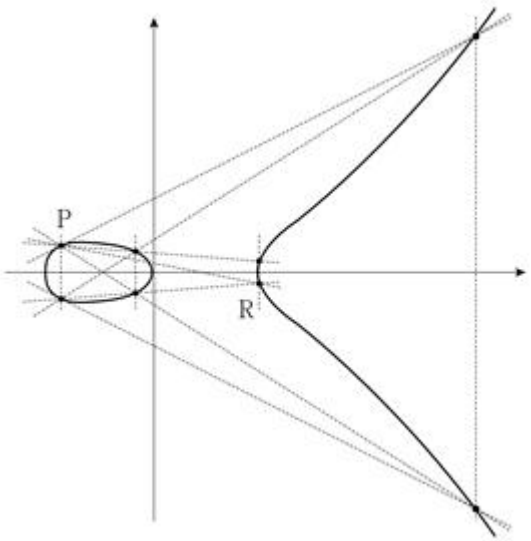
① GRANT : 사용자가 테이블이나 뷰의 내용을 읽고 선택한다.

❷ REVOKE : 이미 부여된 데이터베이스 객체의 권한을 취소한다.

③ DROP : 데이터베이스 객체를 삭제한다.

④ DENY : 기존 데이터베이스 객체를 다시 정의한다.

9. 타원곡선 암호시스템(ECC)은 타원곡선 이산대수의 어려움을 이용한다. 그림과 같이 실수 위에 정의된 타원곡선과 타원곡선 상의 두 점 P와 R이 주어진 경우, R = kP를 만족하는 정수 k의 값은? (단, 점선은 타원곡선의 접선, 점을 연결하는 직선 또는 수직선을 나타낸다)



① 2 ② 3

❸ 4 ④ 5

10. 「개인정보 보호법」상 가명정보의 처리에 관한 특례에 대한 사항으로 옳지 않은 것은?

① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

❷ 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 내부적으로 해당 정보를 처리 보관하되, 제3자에게 제공해서는 아니 된다.

③ 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

④ 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 개인정보 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.

11. 시스템 내 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 이벤트를 선택·수집하여 로그로 저장하고 이를 다른 시스템에 전송할 수 있도록 해 주는 유닉스의 범용 로깅 메커니즘은?

① utmp ❷ syslog

③ history ④ pacct

12. 공개키 암호시스템에 대한 설명으로 옳은 것만을 모두 고르면?

> ㄱ. 한 쌍의 공개키와 개인키 중에서 개인키만 비밀로 보관하면 된다.
> ㄴ. 동일한 안전성을 가정할 때 ECC는 RSA보다 더 짧은 길이의 키를 필요로 한다.
> ㄷ. 키의 분배와 관리가 대칭키 암호시스템에 비하여 어렵다.
> ㄹ. 일반적으로 암호화 및 복호화 처리 속도가 대칭키 암호시스템에 비하여 빠르다.

❶ ㄱ, ㄴ ② ㄱ, ㄹ

③ ㄴ, ㄷ ④ ㄷ, ㄹ

13. 이메일의 보안을 강화하기 위한 기술이 아닌 것은?

❶ IMAP ② S/MIME

③ PEM ④ PGP

14. 국제 정보보호 표준(ISO 27001:2013 Annex)은 14개 통제 영역에 대하여 114개 통제 항목을 정의하고 있다. 통제 영역의 하나인 물리적 및 환경적 보안에 속하는 통제 항목에 대한 설명에 해당하지 않는 것은?

① 보안 구역은 인가된 인력만의 접근을 보장하기 위하여 적절한 출입 통제로 보호한다.

② 자연 재해, 악의적인 공격 또는 사고에 대비한 물리적 보호를 설계하고 적용한다.

③ 데이터를 전송하거나 정보 서비스를 지원하는 전력 및 통신 배선을 도청, 간섭, 파손으로부터 보호한다.

❹ 정보보호에 영향을 주는 조직, 업무 프로세스, 정보 처리 시설, 시스템의 변경을 통제한다.

15. 대칭키 암호시스템에 대한 암호 분석 방법과 암호 분석가에게 필수적으로 제공되는 모든 정보를 연결한 것으로 옳지 않은 것은?

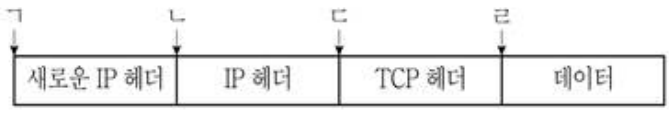
① 암호단독(ciphertext only) 공격－암호 알고리즘, 해독할 암호문

❷ 기지 평문(known plaintext) 공격－암호 알고리즘, 해독할 암호문, 임의의 평문

③ 선택 평문(chosen plaintext) 공격－암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 평문과 해독할 암호문에 사용된 키로 생성한 해당 암호문

④ 선택 암호문(chosen ciphertext) 공격－암호 알고리즘, 해독할 암호문, 암호 분석가에 의해 선택된 암호문과 해독할 암호문에 사용된 키로 복호화한 해당 평문

16. IPv4 패킷에 대하여 터널 모드의 IPSec AH(Authentication Header) 프로토콜을 적용하여 산출된 인증 헤더가 들어갈 위치로 옳은 것은?



① ㄱ ❷ ㄴ

③ ㄷ ④ ㄹ

17. 정보보호 관련 법률과 소관 행정기관을 잘못 짝 지은 것은?

①「전자정부법」－행정안전부

② 「신용정보의 이용 및 보호에 관한 법률」 – 금융위원회
❸ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 – 개인정보보호위원회
④ 「정보통신기반 보호법」 – 과학기술정보통신부

18. 침입탐지시스템의 비정상(anomaly) 탐지 기법에 대한 설명으로 옳지 않은 것은?

① 상대적으로 급격한 변화나 발생 확률이 낮은 행위를 탐지한다.
② 정상 행위를 예측하기 어렵고 오탐률이 높지만 알려지지 않은 공격에도 대응할 수 있다.
③ 수집된 다양한 정보로부터 생성한 프로파일이나 통계적 임계치를 이용한다.
❹ 상태전이 분석과 패턴 매칭 방식이 주로 사용된다.

19. 「전자서명법」상 과학기술정보통신부장관이 정하여 고시하는 전자서명인증업무 운영기준에 포함되어 있는 사항이 아닌 것은?

❶ 전자서명 관련 기술의 연구·개발·활용 및 표준화
② 전자서명 및 전자문서의 위조·변조 방지대책
③ 전자서명인증서비스의 가입·이용 절차 및 가입자 확인 방법
④ 전자서명인증업무의 휴지·폐지 절차

20. 안드로이드 보안 체계에 대한 설명으로 옳지 않은 것은?

① 모든 응용 프로그램은 일반 사용자 권한으로 실행된다.
② 기본적으로 안드로이드는 일반 계정으로 동작하는데 이를 루트로 바꾸면 일반 계정의 제한을 벗어나 기기에 대한 완전한 통제권을 가질 수 있다.
③ 응용 프로그램은 샌드박스 프로세스 내부에서 실행되며, 기본적으로 시스템과 다른 응용 프로그램으로의 접근이 통제된다.
❹ 설치되는 응용 프로그램은 구글의 인증 기관에 의해 서명·배포된다.

1	2	3	4	5	6	7	8	9	10
②	③	①	③	③	④	②	②	③	②
11	12	13	14	15	16	17	18	19	20
②	①	①	④	②	②	③	④	①	④