

1과목 : 과목 구분 없음

1. 해시와 메시지 인증코드에 대한 <보기>의 설명에서 ㉠, ㉡에 들어갈 말을 순서대로 나열한 것은? (순서대로 ㉠, ㉡)

<보기>

해시와 메시지 인증코드는 공통적으로 메시지의 ( ㉠ )을 검증할 수 있지만, 메시지 인증코드만 ( ㉡ ) 인증에 활용될 수 있다.

- ① 무결성, 상호                      ② 무결성, 서명자  
③ 비밀성, 상호                      ④ 비밀성, 서명자
2. 바이러스의 종류 중에서 감염될 때마다 구현된 코드의 형태가 변형되는 것은?  
① Polymorphic Virus                      ② Signature Virus  
③ Generic Decryption Virus                      ④ Macro Virus
3. 침입탐지시스템(IDS)에 대한 설명으로 가장 옳지 않은 것은?  
① 오용탐지는 새로운 침입 유형에 대한 탐지가 가능하다.  
② 기술적 구성요소는 정보 수집, 정보 가공 및 축약, 침입 분석 및 탐지, 보고 및 조치 단계로 이루어진다.  
③ 하이브리드 기반 IDS는 호스트 기반 IDS와 네트워크 기반 IDS가 결합한 형태이다.  
④ IDS는 공격 대응 및 복구, 통계적인 상황 분석 보고 기능을 제공한다.
4. <보기>에서 블록암호 모드 중 초기 벡터(Initialization Vector)가 필요하지 않은 모드를 모두 고른 것은?

<보기>

㉠, CTR 모드    ㉡, CBC 모드    ㉢, ECB 모드

- ① ㉠                      ② ㉢  
③ ㉡, ㉢                      ④ ㉠, ㉡, ㉢
5. 스트림 암호(Stream Cipher)에 대한 설명으로 가장 옳지 않은 것은?  
① Key Stream Generator 출력값을 입력값(평문)과 AND 연산하여, 암호문을 얻는다.  
② 절대 안전도를 갖는 암호로 OTP(One-Time Pad)가 존재한다.  
③ LFSR(Linear Feedback Shift Register)로 스트림 암호를 구현할 수 있다.  
④ Trivium은 현대적 스트림 암호로 알려져 있다.
6. <보기>에서 설명하는 DRM 구성요소는?

<보기>

DRM의 보호 범위에서 유통되는 콘텐츠의 배포 단위로서 암호화된 콘텐츠 메타 데이터, 전자서명 등의 정보로 구성되어 있다. 또한, MPEG-21 DID 규격을 따른다.

- ① 식별자                      ② 클리어링 하우스  
③ 애플리케이션                      ④ 시큐어 컨테이너

7. 이더넷(Ethernet)상에서 전달되는 모든 패킷(Packet)을 분석하여 사용자의 계정과 암호를 알아내는 것은?  
① Nessus                      ② SAINT  
③ Sniffing                      ④ IPS
8. 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화되어 있는 파일은?  
① /etc/group                      ② /etc/passwd  
③ /etc/shadow                      ④ /etc/login.defs
9. 타원곡선 암호에 대한 설명으로 가장 옳지 않은 것은?  
① 타원곡선 암호의 단점은 보안성 향상을 위하여 키 길이가 길어진다는 것이다.  
② 타원곡선에서 정의된 연산은 덧셈이다.  
③ 타원곡선을 이용하여 디피-헬먼(Diffie-Hellman) 키 교환을 수행할 수 있다.  
④ 타원곡선은 공개키 암호에 사용된다.
10. 영지식 증명(Zero-Knowledge Proof)에 대한 설명으로 가장 옳지 않은 것은?  
① 영지식 증명은 증명자(Prover)가 자신의 비밀 정보를 노출하지 않고 자신의 신분을 증명하는 기법을 의미한다.  
② 영지식 증명에서 증명자 인증 수단으로 X.509 기반의 공개키 인증서를 사용할 수 있다.  
③ 최근 블록체인상에서 영지식 증명을 사용하여 사용자의 프라이버시를 보호하고자 하며, 이러한 기술로 zk-SNARK가 있다.  
④ 영지식 증명은 완전성(Completeness), 건실성(Soundness), 영지식성(Zero-Knowledgeness) 특성을 가져야 한다.
11. 「개인정보 보호법」상 주민등록번호의 처리에 대한 설명으로 가장 옳지 않은 것은?  
① 개인정보처리자는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다.  
② 행정안전부장관은 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있으나, 개인정보처리자가 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.  
③ 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.  
④ 개인정보처리자로부터 주민등록번호를 제공받은 자는 개인정보 보호 위원회의 심의·의결을 거쳐 제공받은 주민등록번호를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다.
12. <보기>의 설명에 해당되는 공격 유형으로 가장 적합한 것은?

<보기>

SYN 패킷을 조작하여 출발지 IP 주소와 목적지 IP 주소를 일치시켜서 공격 대상에 보낸다. 이때 조작된 IP 주소는 공격 대상의 주소이다.

- ① Smurf Attack                      ② Land Attack

- ③ Teardrop Attack      ④ Ping of Death Attack

13. TLS 및 DTLS 보안 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

- ① TLS 프로토콜에서는 인증서(Certificate)를 사용하여 인증을 수행할 수 있다.  
 ② DTLS 프로토콜은 MQTT 응용 계층 프로토콜의 보안에 사용될 수 있다.  
 ③ TLS 프로토콜은 Handshake · Change Cipher Spec · Alert 프로토콜과 Record 프로토콜 등으로 구성되어 있다.  
 ④ TCP 계층 보안을 위해 TLS가 사용되며, UDP 계층 보안을 위해 DTLS가 사용된다.

14. 무선 통신 보안 기술에 대한 설명으로 가장 옳지 않은 것은?

- ① 무선 네트워크 보안 기술에 사용되는 WPA2 기술은 AES/CCMP를 사용한다.  
 ② 무선 네트워크에서는 인증 및 인가, 과금을 위해 RADIUS 프로토콜을 사용할 수 있다.  
 ③ 무선 AP의 SSID값 노출과 MAC 주소 기반 필터링 기법은 공격의 원인이 된다.  
 ④ 무선 네트워크 보안 기술인 WEP(Wired Equivalent Privacy) 기술은 유선 네트워크 수준의 보안성을 제공하므로 기존의 보안 취약성 문제를 극복했다.

15. 서비스 거부 공격(DoS)에 대한 설명으로 가장 옳지 않은 것은?

- ① 공격자가 임의로 자신의 IP 주소를 속여서 다량으로 서버에 보낸다.  
 ② 대상 포트 번호를 확인하여 17, 135, 137번, UDP 포트 스캔이 아니면, UDP Flooding 공격으로 간주한다.  
 ③ 헤더가 조작된 일련의 IP 패킷 조각들을 전송한다.  
 ④ 신뢰 관계에 있는 두 시스템 사이에 공격자의 호스트를 마치 하나의 신뢰 관계에 있는 호스트인 것처럼 속인다.

16. 윈도우 운영체제에서의 레지스트리(Registry)에 대한 설명으로 가장 옳은 것은?

- ① 레지스트리 변화를 분석함으로써 악성코드를 탐지할 수 있다.  
 ② 레지스트리는 운영체제가 관리하므로 사용자가 직접조작할 수 없다.  
 ③ 레지스트리 편집기를 열었을 때 보이는 다섯 개의 키를 하이브(Hive)라고 부른다.  
 ④ HKEY\_CURRENT\_CONFIG는 시스템에 로그인하고 있는 사용자와 관련된 시스템 정보를 저장한다.

17. 침입차단시스템에 대한 설명으로 가장 옳은 것은?

- ① 스크린드 서브넷 구조(Screened Subnet Architecture)는 DMZ와 같은 완충 지역을 포함하며 구축 비용이 저렴하다.  
 ② 스크리닝 라우터 구조(Screening Router Architecture)는 패킷을 필터링하도록 구성되므로 구조가 간단하고 인증 기능도 제공할 수 있다.  
 ③ 이중 네트워크 호스트 구조(Dual-homed Host Architecture)는 내부 네트워크를 숨기지만, 베스천 호스트가 손상되면 내부 네트워크를 보호할 수 없다.  
 ④ 스크린드 호스트 게이트웨이 구조(Screened Host Gateway Architecture)는 서비스 속도가 느리지만, 베스천 호스트에 대한 침입이 있어도 내부 네트워크를 보호

할 수 있다.

18. 최근 알려진 Meltdown 보안 취약점에 대한 설명으로 가장 옳은 것은?

- ① CPU가 사용하는 소비 전력 패턴을 사용하여 중요한 키 값이 유출되는 보안 취약점이다.  
 ② CPU의 특정 명령어가 실행될 때 소요되는 시간을 측정하여 해당 명령어와 주요한 키 값이 유출될 수 있는 보안 취약점이다.  
 ③ SSL 설정 시 CPU 실행에 영향을 미쳐 CPU 과열로 인해 오류를 유발하는 보안 취약점이다.  
 ④ CPU를 고속화하기 위해 사용된 비순차적 명령어 처리(Out-of-Order Execution) 기술을 악용한 보안 취약점이다.

19. <보기>는 TCSEC(Trusted Computer System Evaluation Criteria)에 의하여 보안 등급을 평가할 때 만족해야 할 요건들에 대한 설명이다. 보안 등급이 높은 것부터 순서대로 나열된 것은?

〈보기〉

ㄱ. 강제적 접근 제어가 구현되어야 한다.  
 ㄴ. 정형화된 보안 정책을 일정하게 유지하여야 한다.  
 ㄷ. 사용자가 자신의 파일에 대한 접근 권한을 설정할 수 있어야 한다.

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

20. 정보보호 및 개인정보보호 관리체계인증(ISMS-P)에 대한 설명으로 가장 옳지 않은 것은?

- ① 정보보호 관리체계 인증만 선택적으로 받을 수 있다.  
 ② 개인정보 제공 시뿐만 아니라 파기 시의 보호조치도 포함한다.  
 ③ 위험 관리 분야의 인증기준은 보호대책 요구사항 영역에서 규정한다.  
 ④ 관리체계 수립 및 운영 영역은 Plan, Do, Check, Act의 사이클에 따라 지속적이고 반복적으로 실행 되는지 평가한다.

전자문제집 CBT PC 버전 : [www.comcbt.com](http://www.comcbt.com)

전자문제집 CBT 모바일 버전 : [m.comcbt.com](http://m.comcbt.com)

기출문제 및 해설집 다운로드 : [www.comcbt.com/x](http://www.comcbt.com/x)

전자문제집 CBT란?

종이 문제집이 아닌 인터넷으로 문제를 풀고 자동으로 채점하며 모의고사, 오답 노트, 해설까지 제공하는 무료 기출문제 학습 프로그램으로 실제 시험에서 사용하는 OMR 형식의 CBT를 제공합니다.

PC 버전 및 모바일 버전 완벽 연동  
 교사용/학생용 관리기능도 제공합니다.

오답 및 오탈자가 수정된 최신 자료와 해설은 전자문제집 CBT에서 확인하세요.

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