정보시스템보안

1. 다음은 정보시스템에 대해 가용성(Availability)과 보안수준(Security Level)간의 관계를 설명한 것이다. 가장 적합한 설명은?
   ① 보안수준과 가용성간에는 아무런 관련이 없다.
   ② 보안수준을 높이면 가용성이 낮아진다.
   ③ 보안수준을 높이면 가용성도 높아진다.
   ④ 보안수준을 낮추면 가용성도 낮아진다.

2. 다음 중 조직내의 정보시스템을 안전하게 보호를 위해 마련해야 할 보호대책이 아닌 것은?
   ① 관리적 보호대책
   ② 기술적 보호대책
   ③ 소프트웨어공학적 보호대책
   ④ 물리적 보호대책

3. 다음 중 정보시스템에 대한 가장 대표적인 가용성(Availability) 공격은?
   ① 스니핑(Sniffing) 공격
   ② 변조(Modification) 공격
   ③ 위장(Masquerading) 공격
   ④ 분산서비스거부(Distributed Denial of Service) 공격

4. 다음 중 정보시스템 관리자를 속이거나 협박하여 정보시스템에 침입해서 불법적인 행위를 하는 공격은?
   ① 사회공학적공격(Social Enginnering Attack)
   ② 소프트웨어 공학적공격(SW Enginnering Attack)
   ③ 중간공격자 공격(Man In The Middle Attack)
   ④ 다중수준 보안공격(Multi Level Security Attack)

5. 다음 중 현재 시행중인 보안 관련 인증제와 가장 관계가 먼 것은?
   ① CC(Common Criteria) 인증제
   ② GS(Good SW)품질 인증제
   ③ KCMVP(Korea Cryptographic Module Verification Program) 인증제
   ④ ISMS(Information Security Management System) 인증제

6. 다음 중 하이브리드 암호시스템(Hybrid Cryptography System)에서 대칭키 암호알고리즘을 사용하는 가장 큰 이유는?
   ① 안전한 대칭키 분배용으로 활용
   ② 대량의 데이터에 대해 고속 암호화에 활용
   ③ 생성된 일회용 세션키 암호화에 활용
   ④ 고속의 공개키 암호시스템 보조용으로 활용

7. 다음 <보기> 설명에서 ㉠,㉡,㉢에 들어갈 용어를 순서대로 나열한 것은?

< 보기 >

저작물의 원본을 왜곡하지 않는 범위 내에서 저작권 정보를 삽입하는 기술을 (㉠)이라 하고, 디지털 콘텐츠를 판매할 때 구매자 정보를 삽입하여 불법 배포가 이루어질 경우 최초의 구매자를 추적하는 기술을 (㉡)이라 한다. 또한 디지털콘텐츠의 지적재산권이 안전하게 보호되도록 창작에서 소비까지 전 과정이 적법하게 이루어지도록 하는 기술을 (㉢)이라 한다.

   ① DRM(Digital Right Management), 워터마킹(Watermarking), 핑거프린팅(Fingerprinting)
   ② 핑거프린팅(Fingerprinting), DRM(Digital Right Management), 워터마킹(Watermarking)
   ③ 워터마킹(Watermarking), 핑거프린팅(Fingerprinting), DRM(Digital Right Management)
   ④ DRM(Digital Right Management), 핑거프린팅(Fingerprinting), 워터마킹(Watermarking)

8. 다음 중 대칭키 암호알고리즘과 가장 관련이 없는 것은?
   ① RSA(Rivest Shamir Adleman)
   ② ARIA(Academy Research Institute Agency)
   ③ SPN(Substitution Permutation Network)
   ④ AES(Advanced Encryption Standard)

9. 다음 중 대칭키 분배 방법 중에서 중간자공격(Man in The Middle Attack)에 가장 취약한 것은?
   ① 대칭키를 사전에 공유법
   ② Diffie-Hellman 키 분배 알고리즘에 의한 분배
   ③ 키 분배센터(KDC, Key Distribution Cenetr)에 의한 분배
   ④ PKI(Public Key Infrastructure)기반의 공개키 암호시스템을 활용한 분배

10. A가 B에게 공개키 암호시스템을 이용하여 메시지를 암호화하여 보내고 싶다. A는 어떻게 암호화해야 하는가?
① A의 공개키로 메시지를 암호화하여 B에게 보낸다.
② A의 개인키로 메시지를 암호화하여 B에게 보낸다.
③ B의 공개키로 메시지를 암호화하여 B에게 보낸다.
④ B의 개인키로 메시지를 암호화하여 B에게 보낸다.

11. 다음 중 재전송 공격(Replay Attack)의 방어법이 아닌 것은?
① 초기벡터(IV, Initial Vector) 사용
② 타임스템프(Timestamp) 사용
③ 비표(Nonce) 사용
④ 순서번호(Sequence Number) 사용

12. 한번의 시스템 인증을 통해 재인증 절차 없이 정보시스템들에 대해 접근할 수 있는 통합 로그인 제품은?
① SSO(Single Sign On)
② SAC(Server Access Control)
③ RBAC(Role Base Access Control)
④ TSO(Trust Sign On)

13. 다음 중 컴퓨터에 침투하여 주요 파일을 암호화하고 컴퓨터 사용자에게 암호화된 파일의 복호화 키를 알려준다는 조건으로 금전 등을 요구하는 악성코드는?
① 웜(Worm)
② 매크로 바이러스(Mecro Virus)
③ 랜섬웨어(Ransomware)
④ 트로이목마(Trojan Horse)

14. 다음 중 PKI에 관한 설명 중 가장 옳지 않은 것은?
① PKI란 Public Key Infrastructure의 약어로 공개키 암호 알고리즘을 적용하고 인증서를 관리하기 위한 기반시스템이다.
② 주로 X.509 인증서를 사용하고 있다.
③ 인증서를 발급하는 역할을 하는 기관을 RA라 한다.
④ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

15. 다음 중 시스템 설계자가 서비스 기술자와 유지보수 기술자를 위하여 특정 컴퓨터에 접근을 편리하게 할 수 있도록 고의적으로 만든 악성코드는?
① 애드웨어(Adware)
② 백도어(Backdoor)
③ 매크로 바이러스(Macro Virus)
④ 웜(Worm)

16. 다음 중 패스워드를 저장할 때 해시를 이용하는데, 안전도를 높이기 위해 무작위 문자열을 추가한다. 이렇게 추가되는 문자열을 무엇이라 하는가?
① Nonce ② Plaintext
③ Salt ④ Cipher

17. 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려될 수 있으므로 기반시설을 지정하여야 한다. 다음 중 주요정보통신기반시설이 아닌 것은 무엇인가?
① 전력, 가스, 석유 등 에너지·수자원 시설
② 인터넷포털, 전자상거래 등 인터넷시설
③ 도로, 철도, 지하철, 공항, 항만 등 주요 교통시설
④ 방송중계, 국가지도통신망 시설

18. 다음 보기에서 설명하는 유닉스 시스템 명령어는?

< 보 기 >

시스템의 파일 또는 디렉토리(Directory)가 만들어질 때의 허가권(Permission)의 기본값을 정하기 위해서 사용한다. 해당 설정값은 모든 계정 사용자들에게 존재하는 값으로써 각 계정 사용자들이 생성하는 파일 또는 디렉토리(Directory)의 허가권(Permission)을 결정하기 위한 값이다.

① chmod
② umask
③ chown
④ touch

19. 다음 중 지능형 지속 위협(APT, Advanced Persistent Threat)에 대한 설명으로 가장 옳은 것은?

① 공격의 설계부터 침투까지 매우 빠른 시간 내에 이루어진다.
② 다른 형태의 공격들에 비해 대체로 공격자의 비용이 적게 든다.
③ 시스템관리자는 가능한 모든 공격을 고려해야 되기 때문에 방어가 매우 어렵다.
④ 하나의 타깃에 대해서 같은 방법으로 지속적으로 뚫을 때까지 공격하는 것이다.

20. 다음 중「개인정보보호법」제25조에 따라 공개된 장소에서의 영상정보처리기기 설치가 예외적으로 허용되는 경우가 아닌 것은?

① 법령에서 구체적으로 허용하고 있는 경우
② 범죄의 예방 및 수사를 위하여 필요한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 통계작성·과학적 연구·공익적 기록보전 등을 위하여 필요한 경우