정보관리론

1. 보안 관리 대상에 대한 <보기>의 설명에서 ( )에 들어갈 용어로 다음 중 가장 옳은 것은?

< 보 기 >

(㉠) : 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
(㉡) : 자산에 손실을 초래할 수 있는 원하지 않는 사건의 잠재적 원인이나 행위자를 말한다.
(㉢) : 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.

① ㉠ 로그 ㉡ 위험 ㉢ 쿠키
② ㉠ 로그 ㉡ 위협 ㉢ 세션
③ ㉠ 백업 ㉡ 위험 ㉢ 세션
④ ㉠ 백업 ㉡ 위협 ㉢ 쿠키

2. 다음 중 암호학적으로 안전한 의사(pseudo) 난수 생성기에 대한 설명으로 가장 옳지 않은 것은?
① 생성된 수열의 비트는 무작위로 발생한다.
② 생성된 수열의 어느 부분 수열도 다른 부분 수열로부터 추정될 수 있어야 한다.
③ 시드(seed)라고 불리는 입력 값은 외부에 알려지지 않도록 비밀로 하여야 한다.
④ 고정값 시드(seed)를 입력받아 결정적 알고리즘을 사용하여 출력 비트열을 생성한다.

3. 다음 중 중앙 집중형 인증 방식인 커버로스(Kerberos)에 대한 설명으로 가장 옳지 않은 것은?
① 신뢰받는 제3자인 키 배포기관이 구성원들 중간에 개입하는 방법이다.
② 커버로스는 세션키를 이용한 티켓 기반 인증 기법을 제공한다.
③ 인증 서버가 사용자에게 발급한 티켓(승인 티켓)은 유효기간 내에 재사용할 수 있다.
④ 분산 시스템 환경에서 SSO(Single Sign On) 시스템을 구축할 수 없다.

4. 다음 중 리눅스 시스템에서 패스워드 정책이 포함되고, 사용자 패스워드가 암호화 되어 있는 파일로 가장 옳은 것은?
① /etc/group
② /etc/passwd
③ /etc/shadow
④ /etc/login.defs

5. 다음 중 유닉스 로그파일에 대한 설명으로 가장 옳지 않은 것은?
① lastlog : 사용자들이 마지막으로 로그아웃한 정보를 가지고 있다.
② utmp : 현재 로그인한 사용자 정보를 가지고 있다.
③ wtmp : 로그인과 로그아웃, 시스템 부팅 정보를 가지고 있다.
④ sulog : su(switch user) 명령어를 실행한 정보를 가지고 있다.

6. 다음 중 hwp, pdf, doc 등의 문서를 암호화하여 외부 유출 시에도 기업 내부 정보를 보호하는 것으로 가장 옳은 것은?
① DRM ② CDR ③ NFV ④ EDR

7. 다음 중 개인정보영향평가 시 고려하여야 할 사항으로 가장 옳지 않은 것은?
① 처리하는 개인정보의 수
② 개인정보처리자의 인가 여부
③ 정보주체의 권리를 해할 가능성 및 그 위험 정도
④ 개인정보의 제3자 제공 여부

8. 다음 중 공개키 암호 시스템과 대칭키 암호 시스템의 장점을 조합한 하이브리드 암호 시스템에 대한 설명으로 가장 옳지 않은 것은?
① 하이브리드 암호 시스템은 대칭키 암호의 키 교환 문제가 존재한다.
② 암호화에 사용된 대칭키(세션키)를 상대방에게 전달할 때 상대방의 공개키를 사용한다.
③ 메시지 자체를 암호화 또는 복호화 할 때는 속도가 빠른 대칭키 암호 시스템을 사용한다.
④ 수신자는 암호화된 대칭키를 수신자의 개인키로 복호화 할 수 있다.

9. 다음 중 유닉스에서 파일의 속성을 검색하는 find 옵션으로 가장 옳지 않은 것은?
① mtime : 파일의 내용이 수정된 시간을 기준으로 검색한다.
② atime : 파일에 접근한 시간을 기준으로 검색한다.
③ ctime : 파일 속성, 권한, 크기가 변경된 시간을 기준으로 검색한다.
④ rtime : 파일 실행 일자를 기준으로 검색한다.

10. 다음의 ㉠ ~ ㉢에 해당되는 대칭키 암호 알고리즘을 가장 옳게 나열한 것은?

< 보 기 >

㉠ DES의 암호화 강도가 점점 약해지면서 이를 대체하기 위한 알고리즘으로 현재 미국 연방정부표준 블록 암호 알고리즘(NIST FIPS 197)으로 사용
㉡ 국내에서 민간 부분인 인터넷, 전자상거래, 무선 통신 등에서 민감 정보 및 프라이버시 보호를 위해 한국인터넷진흥원(KISA)이 주축이 되어 개발한 128/256 비트 암호키를 지원하며 IFTF 및 ISO/IEC 국제표준으로 채택된 바 있음
㉢ 전자정부 구현 등으로 다양한 환경에 적합한 암호화 알고리즘이 필요함에 따라 국가보안기술연구소 주도로 경량 환경 및 하드웨어의 효율성 향상을 위해 개발된 128비트 블록 암호 알고리즘으로 128/192/256 비트 암호화키를 지원

① ㉠ AES ㉡ SEED ㉢ ARIA
② ㉠ AES ㉡ ARIA ㉢ SEED
③ ㉠ ARIA ㉡ SEED ㉢ AES
④ ㉠ ARIA ㉡ AES ㉢ SEED

11. 서버 관리자가 사용할 수 있는 보안용 소프트웨어 중 그 용도가 가장 다른 것은?
① AWstats ② Nessus
③ Acunetix ④ Nmap

12. 리눅스 서버 관리자 A씨는 피해 시스템을 점검하던 중 다음과 같은 시스템 바이너리 파일들이 변조된 것을 확인하였다. 공격자의 입장에서 파일을 변조한 이유가 가장 옳지 않게 연결된 것은?
① ps, top : 특정 프로세스 정보를 숨김
② w, who : 특정 사용자의 정보를 숨김
③ ls, du : 특정 파일이나 디렉토리를 숨김
④ ifconfig : 특정 IP에서의 접속을 숨김

13. 다음은 FTP(File Transfer Protocol) 서비스에 대한 내용을 설명한 것이다. 가장 옳지 않은 것은?
① 전송계층 프로토콜로 TCP를 사용하고 있으며, 클라이언트 서버 모델로 구성되어 있다.
② IETF에 따라 RFC 959로 정의된다.
③ 기본적으로 액티브 모드(Active mode)와 패시브 모드(Passive mode)를 지원한다.
④ 제어 연결은 21 포트를, 데이터 연결은 512 이후 포트를 사용한다.

14. 다음 중 블록 암호 알고리즘의 종류가 아닌 것은?
① RC5 ② DES ③ MD5 ④ IDEA

15. 다음은 윈도우 부팅 순서이다. 가장 옳게 나열한 것은?

< 보 기 >

㉠ MBR - 부팅 매체에 대한 기본적인 파일 시스템 정보가 들어 있는 MBR 정보를 읽는다.
㉡ POST - 하드웨어 자체가 시스템에 문제가 없는지 기본적인 사항을 체크하는 과정
㉢ NTLDR - 하드디스크의 부팅 파티션에 있는 프로그램으로 윈도우가 부팅될 수 있도록 간단한 파일시스템을 실행하며 boot.ini 파일의 내용을 읽는다.
㉣ NTDETECT.com - 설치된 하드웨어를 검사한다.
㉤ ntoskrnl.exe - HAL.dll을 로드한다.
㉥ CMOS - 사용자가 설정한 기본 사항을 읽어 시스템에 적용한다.

① ㉥ - ㉢ - ㉣ - ㉠ - ㉤ - ㉡
② ㉡ - ㉥ - ㉢ - ㉣ - ㉠ - ㉤
③ ㉡ - ㉥ - ㉠ - ㉢ - ㉣ - ㉤
④ ㉥ - ㉠ - ㉤ - ㉡ - ㉢ - ㉣

16. '사이버위기경보'의 등급 중 복수 정보통신서비스 제공자(ISP) 망에 장애 또는 마비가 발생하였을 경우, 발령하는 경보의 단계는 무엇인가?

① 심각 단계 ② 경계 단계
③ 주의 단계 ④ 관심 단계

17. 다음 중 전자우편 보안기술 PGP의 기능으로 가장 옳지 않은 것은?

① 전자서명 ② 암호화
③ 생체인증 ④ 무결성

18. 다음의 접근통제 모델(Access Control Model) 중 무결성을 보장하기 위한 모델을 모두 고른 것은?

< 보 기 >

㉠ 벨라파듈라(Bell-LaPadula) 모델
㉡ 비바(Biba) 모델
㉢ 클락 윌슨(Clark-Wilson) 모델

① ㉠ ② ㉡ ③ ㉠ ㉡ ④ ㉡ ㉢

19. 다음에서 설명하는 키의 종류는 무엇인가?

< 보 기 >

㉠ 반복적으로 사용하는 대표키로 안전한 보관이 필요하다.
㉡ 한번만 사용하는 키로 사용이 종료되면 폐기되는 키이다.
㉢ 비대칭 암호시스템에서 전자서명용 검증키이고, 평문데이터의 암호화용으로 사용한다.

① ㉠ 대칭키 ㉡ 세션키 ㉢ 개인키
② ㉠ 세션키 ㉡ 대칭키 ㉢ 공개키
③ ㉠ 마스터키 ㉡ 세션키 ㉢ 공개키
④ ㉠ 세션키 ㉡ 마스터키 ㉢ 개인키

20. 해킹 수단과 그 공격 방법에 대한 설명으로 가장 옳지 않은 것은?

① Ransomware : 파일을 암호화한 후 복호화를 조건으로 금전을 요구함
② Rootkit : 스택에 할당된 버퍼보다 큰 코드를 삽입하여 오동작을 일으킴
③ SQL Injection : 데이터베이스에 질의어를 변조하여 공격함
④ Cross-site Scripting : 웹 페이지에 악성 스크립트를 삽입하여 정보를 획득함