정보보호론

1. 데이터의 위·변조를 방어하는 기술이 목표로 하는 것은?

① 기밀성

② 무결성

③ 가용성

④ 책임추적성

2. UDP 헤더 포맷의 구성 요소가 아닌 것은?

① 순서 번호

② 발신지 포트 번호

③ 목적지 포트 번호

④ 체크섬

3. 논리 폭탄에 대한 설명으로 옳은 것은?

① 사용자 동의 없이 설치되어 컴퓨터 내의 금융 정보, 신상 정보 등을 수집·전송하기 위한 것이다.

② 침입자에 의해 악성 소프트웨어에 삽입된 코드로서, 사전에 정의된 조건이 충족되기 전까지는 휴지 상태에 있다가 조건이 충족되면 의도한 동작이 트리거되도록 한다.

③ 사용자가 키보드로 PC에 입력하는 내용을 몰래 가로채어 기록한다.

④ 공격자가 언제든지 시스템에 관리자 권한으로 접근할 수 있도록 비밀 통로를 지속적으로 유지시켜 주는 일련의 프로그램 집합이다.

4. 대칭키 암호 알고리즘이 아닌 것은?

① SEED

② ECC

③ IDEA

④ LEA

5. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 사항이 아닌 것은?

① 정보통신망의 표준화 및 인증

② 정보통신망의 안정성 확보

③ 고정형 영상정보처리기기의 설치·운영 제한

④ 집적된 정보통신시설의 보호

6. CSRF 공격에 대한 설명으로 옳지 않은 것은?

① 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위를 특정 웹사이트에 요청하게 하는 공격이다.

② 특정 웹사이트가 사용자의 웹 브라우저를 신뢰하는 점을 노리고 사용자의 권한을 도용하려는 것이다.

③ 사용자에게 전달된 데이터의 악성 스크립트가 사용자 브라우저에서 실행되면서 해킹을 하는 것으로, 이 악성 스크립트는 공격자가 웹 서버에 구현된 애플리케이션의 취약점을 이용하여 서버 측 또는 URL에 미리 삽입해 놓은 것이다.

④ 웹 애플리케이션의 요청 내에 세션별·사용자별로 구별 가능한 임의의 토큰을 추가하도록 하여 서버가 정상적인 요청과 비정상적인 요청을 판별하는 방법으로 공격에 대응할 수 있다.

7. IPSec의 터널 모드를 이용한 VPN에 대한 설명으로 옳지 않은 것은?

① 인터넷상에서 양측 호스트의 IP 주소를 숨기고 새로운 IP 헤더에 VPN 라우터 또는 IPSec 게이트웨이의 IP 주소를 넣는다.

② IPSec의 터널 모드는 새로운 IP 헤더를 추가하기 때문에 전송 모드 대비 전체 패킷이 길어진다.

③ ESP는 원래 IP 패킷 전부와 원래 IP 패킷 앞뒤로 붙는 ESP 헤더와 트레일러를 모두 암호화한다.

④ ESP 인증 데이터는 패킷의 끝에 추가되며, ESP 터널 모드의 경우 인증은 목적지 VPN 라우터 또는 IPSec 게이트웨이에서 이루어진다.

8. 「전자서명법」상 전자서명인증사업자에 대한 전자서명인증업무 운영기준 준수사실의 인정(이하 “인정”이라 한다)에 대한 설명으로 옳지 않은 것은?

① 인정을 받으려는 전자서명인증사업자는 국가기관, 지방자치단체 또는 공공기관이어야 한다.

② 인정을 받으려는 전자서명인증사업자는 평가기관으로부터 평가를 먼저 받아야 한다.

③ 평가기관은 평가를 신청한 전자서명인증사업자의 운영기준 준수 여부에 대한 평가를 하고, 그 결과를 인정기관에 제출하여야 한다.

④ 인정기관은 평가 결과를 제출받은 경우 그 평가 결과와 인정을 받으려는 전자서명인증사업자가 법정 자격을 갖추었는지 여부를 확인하여 인정 여부를 결정하여야 한다.

9. 위험 평가 접근방법에 대한 설명으로 옳지 않은 것은?

① 기준(baseline) 접근법은 기준 문서, 실무 규약, 업계 최신 실무를 이용하여 시스템에 대한 가장 기본적이고 일반적인 수준에서의 보안 통제 사항을 구현하는 것을 목표로 한다.

② 비정형(informal) 접근법은 구조적인 방법론에 기반하지 않고 전문가의 지식과 경험에 따라 위험을 분석하는 것으로, 비교적 신속하고 저비용으로 진행할 수 있으나 특정 전문가의 견해 및 편견에 따라 왜곡될 우려가 있다.

③ 상세(detailed) 위험 분석은 정형화되고 구조화된 프로세스를 사용하여 상세한 위험 평가를 수행하는 것으로, 많은 시간과 비용이 드는 단점이 있는 반면에 위험에 따른 손실과 보안 대책의 비용 간의 적절한 균형을 이룰 수 있는 장점이 있다.

④ 복합(combined) 접근법은 상세 위험 분석을 제외한 기준 접근법과 비정형 접근법 두 가지를 조합한 것으로 저비용으로 빠른 시간 내에 필요한 통제 수단을 선택해야 하는 상황에서 제한적으로 활용된다.

10. ISMS-P 인증 기준의 세 영역 중 하나인 관리체계 수립 및 운영에 해당하지 않는 것은?

① 관리체계 기반 마련

② 위험 관리

③ 관리체계 점검 및 개선

④ 정책, 조직, 자산 관리

11. OTP 토큰이 속하는 인증 유형은?

① 정적 생체정보

② 동적 생체정보

③ 가지고 있는 것

④ 알고 있는 것

12. 서비스 거부 공격에 해당하는 것은?

① 발신지 IP 주소와 목적지 IP 주소의 값을 똑같이 만든 패킷을 공격 대상에게 전송한다.

② 공격 대상에게 실제 DNS 서버보다 빨리 응답 패킷을 보내 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도한다.

③ LAN상에서 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 위조하여 둘 사이의 패킷이 공격자에게 전달되도록 한다.

④ 네트워크 계층에서 공격 시스템을 네트워크에 존재하는 또 다른 라우터라고 속임으로써 트래픽이 공격 시스템을 거쳐가도록 흐름을 바꾼다.

13. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의4 (침해사고의 원인 분석 등)의 내용으로 옳지 않은 것은?

① 정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 그 결과에 따라 피해의 확산 방지를 위하여 사고대응, 복구 및 재발 방지에 필요한 조치를 하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 침해사고가 발생하면 그 침해사고의 원인을 분석하고 피해 확산 방지, 사고대응, 복구 및 재발 방지를 위한 대책을 마련하여 해당 정보통신서비스 제공자에게 필요한 조치를 하도록 권고할 수 있다.

③ 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 발생한 침해사고의 원인 분석 및 대책 마련을 위하여 필요하면 정보통신서비스 제공자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

④ 과학기술정보통신부장관이나 민·관합동조사단은 관련 규정에 따라 정보통신서비스 제공자로부터 제출받은 침해사고 관련 자료와 조사를 통하여 알게 된 정보를 재발 방지 목적으로 필요한 경우 원인 분석이 끝난 후에도 보존할 수 있다.

14. 전자상거래에서 소비자의 주문 정보와 지불 정보를 보호하기 위한 SET의 이중 서명은 소비자에서 상점으로 그리고 상점에서 금융기관으로 전달된다. 금융기관에서 이중 서명을 검증하는데 필요하지 않은 것은?

① 소비자의 공개키

② 주문 정보의 해시

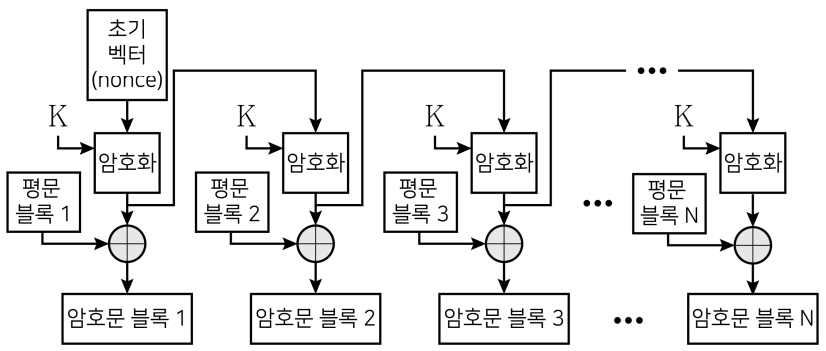
③ 상점의 공개키

④ 지불 정보

15. SHA-512 알고리즘의 수행 라운드 수와 처리하는 블록의 크기 (비트 수)를 바르게 짝 지은 것은?

	라운드 수	블록의 크기
①	64	512
②	64	1024
③	80	512
④	80	1024

16. 다음 그림과 같이 암호화를 수행하는 블록 암호 운용 모드는? (단, ⊕: XOR, K: 암호키)



① CBC

② CFB

③ OFB

④ ECB

17. 윈도우 최상위 레지스트리에 대한 설명으로 옳지 않은 것은?

① HKEY_LOCAL_MACHINE은 로컬 컴퓨터의 하드웨어와 소프트웨어의 설정을 저장한다.

② HKEY_CLASSES_ROOT는 파일 타입 정보와 관련된 속성을 저장하는 데 사용된다.

③ HKEY_CURRENT_USER는 현재 로그인한 사용자의 설정을 저장한다.

④ HKEY_CURRENT_CONFIG는 커널, 실행 중인 드라이버 또는 프로그램과 서비스에 의해 제공되는 성능 데이터를 실시간으로 제공한다.

18. SSH(Secure Shell)의 전송 계층 프로토콜에 의해 제공되는 서비스가 아닌 것은?

① 서버 인증

② 데이터 기밀성

③ 데이터 무결성

④ 논리 채널 다중화

19. 리눅스 배시 셸(Bash shell) 특수 문자와 그 기능에 대한 설명이 옳지 않은 것은?

	특수 문자	기능
①	~	작업 중인 사용자의 홈 디렉터리를 나타냄
②	" "	문자(" ") 안에 있는 모든 셸 특수 문자의 기능을 무시
③	;	한 행의 여러 개 명령을 구분하고 왼쪽부터 차례로 실행
④	|	왼쪽 명령의 결과를 오른쪽 명령의 입력으로 전달

20. ISMS-P 인증 기준 중 사고 예방 및 대응 분야의 점검 항목만을 모두 고르면?

ㄱ. 백업 및 복구 관리
ㄴ. 취약점 점검 및 조치
ㄷ. 이상행위 분석 및 모니터링
ㄹ. 재해 복구 시험 및 개선

① ㄱ, ㄴ

② ㄱ, ㄹ

③ ㄴ, ㄷ

④ ㄷ, ㄹ