정보보호론

문 1. 사용자 인증에 사용되는 기술로 옳지 않은 것은?

① Smart Card
② Single Sign On
③ One Time Password
④ Supervisory Control And Data Acquisition

문 2. 제로 데이 공격에 대한 설명으로 옳은 것은?

① 서버의 성능을 크게 떨어뜨리거나 서버를 정지시키는 방법으로 서버의 정상적인 작동을 방해하는 공격 방법이다.
② 패스워드 사전 파일을 이용해 미리 지정한 아이디에 대입하여 접속계정을 알아내는 공격 방법이다.
③ 패치가 나오지 않은 시점에 이루어지는 공격 방법이다.
④ 버퍼에 일정 크기 이상의 데이터를 입력하여 프로그램을 공격하는 방법이다.

문 3. IPSec 프로토콜의 기능이 아닌 것은?

① Pretty Good Privacy
② Authentication Header
③ Internet Key Exchange
④ Encapsulating Security Payload

문 4. 다음 설명에 해당하는 악성코드는?

○ 사용자 동의 없이 설치되어 컴퓨터의 정보를 수집하고 전송하는 악성소프트웨어 ○ 신용카드와 같은 금융정보 및 주민등록번호와 같은 신상정보, 암호를 비롯한 각종 정보를 수집

① ransomware
② spyware
③ backdoor
④ dropper

문 5. 다음 설명에 해당하는 블루투스 공격을 옳게 짝지은 것은?

(가) 공격이 가능한 블루투스 장치들을 검색하고 모델을 확인하는 공격 (나) 블루투스 장치 내 저장된 데이터에 대한 접근을 허용하는 공격 (다) 블루투스 지원 장치에 대한 접근권한을 획득하는 공격

	(가)	(나)	(다)
①	bluesnarf	bluebug	blueprinting
②	bluesnarf	blueprinting	bluebug
③	blueprinting	bluebug	bluesnarf
④	blueprinting	bluesnarf	bluebug

문 6. 암호화에 대한 설명으로 옳은 것은?

① 대칭키 암호 방식은 암호화 키와 복호화 키가 다른 암호화 방법으로 암호화 키는 공개되고, 복호화 키는 공개되지 않는 구조로서 다수의 정보교환자 간의 통신에 적합하다.
② 공개키 암호에는 RSA, ElGamal 등이 있으며, 처리속도가 대칭키 알고리즘에 비해 매우 느린 단점이 있으나 키 전달이 편리하여 키교환 알고리즘으로 사용되며, 전자서명을 용이하게 구현할 수 있는 특징이 있다.
③ 블록 암호는 이진화된 평문과 키 이진수열을 배타적 논리합 이진 연산으로 결합하여 암호문을 생성하고, 블록 대칭 알고리즘에는 선형 쉬프트 레지스터 등이 있다.
④ 공개키 암호 방식은 암호화 키와 복호화 키가 동일한 암호화 방법으로 두 키가 동일하게 이용되며, 데이터를 변화하는 방법에 따라서 스트림암호와 블록암호로 나누어지고 기밀성용으로만 사용된다.

문 7. 해시에 대한 설명으로 옳지 않은 것은?

① 해시 알고리즘에는 MD5, SHA 등이 있다.
② 해시는 메시지의 무결성을 확인하기 위해서 사용한다.
③ 해시 알고리즘 SHA는 유럽 RIPE 프로젝트에 의해 개발된 해시함수이다.
④ 해시는 임의의 길이 메시지로부터 고정 길이의 해시값을 계산한다.

문 8. PPTP 프로토콜에 대한 설명으로 옳은 것은?

① 3계층인 네트워크 계층에서 동작한다.
② 마이크로소프트가 제안한 VPN 프로토콜로 PPP를 기반으로 한다.
③ 데이터를 스니핑한 뒤 해당 데이터를 다시 보내는 replay attack을 막을 수 있다.
④ 데이터가 전송 도중에 변조되었는지를 확인할 수 있도록 데이터 무결성을 검사한다.

문 9. 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)에서 제24조제1항에도 불구하고 개인정보처리자가 주민등록번호를 처리할 수 있는 경우가 아닌 것은?

① 수탁자가 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하는 경우
② 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
③ 제24조의2제1항제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 개인정보 보호위원회가 고시로 정하는 경우
④ 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우

문 10. 블록체인의 비트코인 블록헤더 구조에 대한 설명으로 옳지 않은 것은?

① Nonce는 4바이트로 구성된다.
② Timestamp는 블록을 생성한 시간이다.
③ Previous Block Hash는 32바이트로 구성된다.
④ Block Header는 5가지 필드로 구성하고 크기는 60바이트로 고정되어 있다.

문 11. OSI 7계층 중 각 층에 해당하는 프로토콜을 모두 옳게 짝지은 것은?

① Network – IP, NetBIOS, SMTP
② Transport – ICMP, SSL, FTP
③ Presentation – ASCII, JPEG, MPEG
④ Application – HTTP, PPP, IGMP

문 12. VPN에 대한 설명으로 옳은 것은?

① TCP, FTP는 VPN에서 사용하는 터널링 프로토콜이다.
② 공용 회선을 대신하여 저렴한 사설 임대 회선을 이용하는 공중 암호화망이다.
③ 사설 임대 회선에 터널을 형성하고 패킷을 캡슐화하지 않고 전달하는 방법을 사용한다.
④ 인터넷과 같은 공중 네트워크를 이용하여 사설망과 같은 전용선처럼 사용할 수 있는 보안 솔루션이다.

문 13. 정보보호 및 개인정보보호 관리체계 인증 기준에서 정하고 있는 보호대책 요구사항은?

① 인증 및 권한관리
② 관리체계 기반 마련
③ 정보주체 권리보호
④ 관리체계 점검 및 개선

문 14. 「개인정보 보호법」 제4조(정보주체의 권리)에서 정보주체가 자신의 개인정보 처리와 관련해서 가지는 권리로 옳지 않은 것은?

① 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
③ 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구할 권리
④ 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

문 15. 웹 해킹 공격에 대한 설명으로 옳지 않은 것은?

① Reverse Telnet은 특정 사용자를 대상으로 하지 않고 불특정 다수를 대상으로 로그인된 사용자가 자신의 의지와 무관하게 공격자가 의도한 행위를 하도록 한다.
② Cross Site Scripting은 악성스크립트를 게시판에 등록하는 글에 포함시켜, 이에 접근한 사용자 컴퓨터에서 실행하도록 한다.
③ File Upload는 첨부파일 업로드 기능을 이용해 해킹 프로그램을 업로드한 후, 웹서버의 권한 획득을 가능하도록 한다.
④ Directory Listing은 취약한 서버 설정으로 브라우징되는 디렉토리의 모든 파일이 인터넷 사용자에게 노출되어 파일의 열람을 가능하도록 한다.

문 16. NAC에 대한 설명으로 옳지 않은 것은?

① 사용자 식별과 인증을 수행한다.
② 단말 무결성 검증을 제공한다.
③ 해커를 유인해서 정보를 얻거나 잡으려고 설치한다.
④ 802.1x 방식, VLAN 방식 등으로 구현된다.

문 17. WTLS 레코드 프로토콜의 하위 프로토콜에 해당하는 것은?

① Handshake Protocol
② Change CipherSpec Protocol
③ Alert Protocol
④ Wireless Datagram Protocol

문 18. 보안 솔루션에 대한 설명으로 옳지 않은 것은?

① IPS는 유해 트래픽이나 다양한 유형의 공격을 사전에 탐지하고 자동화된 알고리즘에 의해 탐지된 공격을 차단하는 능동형 보안 기능을 제공한다.
② IDS는 전통적인 방화벽이 탐지할 수 없는 악의적인 네트워크 트래픽이나 컴퓨터 사용을 탐지하고 이를 알려 주는 역할만 한다는 점에서 공격 자체를 차단하는 방화벽과 차이가 있다.
③ DLP는 이미지 및 오디오 파일과 같은 다양한 디지털 매체를 통해 메시지를 숨겨 전송한다.
④ Firewall은 외부 네트워크에서 내부 네트워크로 유입되는 침입을 막는 역할을 한다.

문 19. CERT에 대한 설명으로 옳은 것은?

① 컴퓨터 긴급 관리팀으로 불리며, 영국의 옥스포드대학에서 만들었다.
② 웜 사고에 대응하기 위해 만들어졌지만, 현재는 웜뿐만 아니라 해커의 침입에 대한 대응과 추적에 대한 업무까지 맡고 있다.
③ 정부에서만 CERT를 운영하고 있다.
④ CERT팀은 법률 대리인, 대외 언론 및 외부 기관 대응 전문가로만 구성된다.

문 20. 정보 보안 거버넌스의 구현 요건에 대한 설명으로 옳지 않은 것은?

① 전략적 연계: 정보 보안 사고의 잠재적 위험을 줄이려면 조직에 적합한 위험 관리 체계를 수립하고 지속적으로 관리해야 한다.

② 가치 전달: 정보 보안 투자의 효과를 높이기 위해서는 구성원들에게 정보 보안의 중요성과 가치를 교육하고 국제 표준을 기준으로 정보 보안 관리 체계를 갖추어 운영해야 한다.

③ 자원 관리: 정보 보안 지식과 자원을 효율적으로 관리하기 위해 중요한 정보 자산과 인프라를 포함하는 전사적 정보 보안 아키텍처를 확보해야 한다.

④ 성과 관리: 정보 보안 거버넌스의 효과적인 운영을 위한 척도로 모니터링이나 보고 및 성과 평가 체계를 운영해야 한다.

문 21. 「정보통신기반 보호법」 제8조제1항에서 규정하고 있는 주요정보통신기반시설 지정 기준에 해당하지 않는 것은?

① 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가 사회적 중요성

② 정보통신산업의 기반을 조성하기 위하여 산업입지의 조성 및 정보통신산업 기반시설의 지원

③ 다른 정보통신기반시설과의 상호연계성

④ 침해사고가 발생할 경우 국가안전 보장과 경제사회에 미치는 피해 규모 및 범위

문 22. TCSEC의 등급에 대한 설명으로 옳은 것은?

① C2 등급에서는 레이블된 정보보호(labeled security)를 평가한다.

② D 등급에서는 검증된 정보보호(verified design)를 평가한다.

③ A1 등급에서는 최소한의 보호(minimal protection)만 가능하다.

④ A1, B1, B2, B3, C1, C2, D 등급으로 구분된다.

문 23. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의3에 따라 본인확인기관 지정을 위한 심사 사항으로 옳지 않은 것은?

① 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획

② 이동통신사업자의 본인확인업무 수행과 관련하여 이용자의 주민등록번호를 수집·이용하기 위한 계획

③ 본인확인업무 관련 설비규모의 적정성

④ 본인확인업무의 수행을 위한 기술적·재정적 능력

문 24. RADIUS에 대한 설명으로 옳은 것은?

① 주로 서버/클라이언트 방식으로 동작한다.

② 분산형 접근 제어방식으로 인터넷을 이용하여 직접적으로 사용자를 인증하는 프로토콜이다.

③ 등록되지 않은 사용자를 인증한다.

④ 보안 강화를 위하여 TCP를 사용한다.

문 25. 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」에서 규정하고 있는 인증 기준에 대한 설명으로 옳지 않은 것은?

① 정보자산 식별: 조직의 업무 특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.

② 사용자 인증: 정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.

③ 원격접근 통제: 보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙으로 금지하고 재택근무·장애대응·원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인, 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속 단말 보안(백신, 패치 등) 등 보호대책을 수립·이행하여야 한다.

④ 사용자 계정 관리: 개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.