정보보호론

문 1. 유닉스(Unix) 운영체제에서 사용자의 패스워드에 대한 해쉬 값이 저장되어 있는 파일은?

① /etc/shadow ② /etc/passwd
③ /etc/profile ④ /etc/group

문 2. 다음에서 설명하는 것은?

> 평문을 암호화하거나 암호화된 문장을 복호화하는 전기·기계 장치로 자판에 문장을 입력하면 회전자가 돌아가면서 암호화된 문장·복호화된 평문을 만들어낸다.

① 스키테일(Scytale) ② 아핀(Affine)
③ 에니그마(Enigma) ④ 비제니어(Vigenere)

문 3. RFC 2104 인터넷 표준에서 정의한 메시지 인증 코드를 생성하는 알고리즘은?

① Elliptic Curve Cryptography
② ElGamal
③ RC4
④ HMAC-SHA1

문 4. 다음에서 설명하는 디지털 포렌식(Digital Forensics)은?

> 자신에게 불리한 증거 자료를 사전에 차단하려는 활동이나 기술로 데이터 은닉, 데이터 암호화 등이 있다.

① 항포렌식(Anti Forensic)
② 임베디드 포렌식(Embedded Forensic)
③ 디스크 포렌식(Disk Forensic)
④ 시스템 포렌식(System Forensic)

문 5. 안전한 전자상거래를 구현하기 위해서 필요한 요건들에 대한 설명으로 옳은 것은?

① 무결성(Integrity) – 정보가 허가되지 않은 사용자(조직)에게 노출되지 않는 것을 보장하는 것을 의미한다.
② 인증(Authentication) – 각 개체 간에 전송되는 정보는 암호화에 의한 비밀 보장이 되어 권한이 없는 사용자에게 노출되지 않아야 하며 저장된 자료나 전송 자료를 인가받지 않은 상태에서는 내용을 확인할 수 없어야 한다.
③ 접근제어(Access Control) – 허가된 사용자가 허가된 방식으로 자원에 접근하도록 하는 것이다.
④ 부인봉쇄(Non-repudiation) – 어떠한 행위에 관하여 서명자나 서비스로부터 부인할 수 있도록 해주는 것을 의미한다.

문 6. 무선 인터넷 보안을 위한 알고리즘이나 표준이 아닌 것은?

① WEP ② WPA-PSK
③ 802.11i ④ X.509

문 7. 다음은 유닉스에서 /etc/passwd 파일의 구성을 나타낸 것이다. ㉠ ~ ㉣에 대한 설명으로 옳은 것은?

root : x : 0 : 0 : root : /root : /bin/bash
㉠㉡ ㉢ ㉣

① ㉠ – 사용자 소속 그룹 GID
② ㉡ – 사용자 UID
③ ㉢ – 사용자 계정 이름
④ ㉣ – 사용자 로그인 쉘

문 8. 「국가정보화 기본법」상 ㉠, ㉡에 들어갈 용어가 바르게 연결된 것은?

> ○ 정부는 국가정보화의 효율적, 체계적 추진을 위하여 (㉠)마다 국가정보화 기본계획을 수립하여야 한다.
> ○ 국가정보화 기본계획은 (㉡)이 국가와 지방자치단체의 부문계획을 종합하여 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제7조에 따른 정보통신 전략위원회의 심의를 거쳐 수립·확정한다.

㉠	㉡
① 3년	행정안전부장관
② 3년	과학기술정보통신부장관
③ 5년	과학기술정보통신부장관
④ 5년	행정안전부장관

문 9. 일정 크기의 평문 블록을 반으로 나누고 블록의 좌우를 서로 다른 규칙으로 계산하는 페이스텔(Feistel) 암호 원리를 따르는 알고리즘은?

① DES(Data Encryption Standard)
② AES(Advanced Encryption Standard)
③ RSA
④ Diffie-Hellman

문 10. IPSec 표준은 네트워크 상의 패킷을 보호하기 위하여 AH (Authentication Header)와 ESP(Encapsulating Security Payload)로 구성된다. AH와 ESP 프로토콜에 대한 설명으로 옳지 않은 것은?

① AH 프로토콜의 페이로드 데이터와 패딩 내용은 기밀성 범위에 속한다.
② AH 프로토콜은 메시지의 무결성을 검사하고 재연(Replay) 공격 방지 서비스를 제공한다.
③ ESP 프로토콜은 메시지 인증 및 암호화를 제공한다.
④ ESP는 전송 및 터널 모드를 지원한다.

문 11. 스마트폰 보안을 위한 사용자 지침으로 옳지 않은 것은?

① 관리자 권한으로 단말기 관리
② 스마트폰과 연결되는 PC에도 백신 프로그램 설치
③ 블루투스 기능은 필요 시에만 활성
④ 의심스러운 앱 애플리케이션 다운로드하지 않기

문 12. 다음에서 설명하는 것은?

> ○ 전달하려는 정보를 이미지 또는 문장 등의 파일에 인간이 감지할 수 없도록 숨겨서 전달하는 기술
> ○ 이미지 파일의 경우 원본 이미지와 대체 이미지의 차이를 육안으로 구별하기 어렵다.

① 인증서(Certificate)
② 스테가노그래피(Steganography)
③ 전자서명(Digital Signature)
④ 메시지 인증 코드(Message Authentication Code)

문 13. 조직의 정보자산을 보호하기 위하여 정보자산에 대한 위협과 취약성을 분석하여 비용 대비 적절한 보호 대책을 마련함으로써 위험을 감수할 수 있는 수준으로 유지하는 일련의 과정은?

① 업무 연속성 계획
② 위험관리
③ 정책과 절차
④ 탐지 및 복구 통제

문 14. 「개인정보 보호법」상 다음 업무를 수행하는 자는?

> 개인정보파일의 보호 및 관리·감독하는 임원(임원이 없는 경우에는 개인 정보를 담당하는 부서의 장)을 말한다.

① 수탁자
② 정보통신서비스 제공자
③ 개인정보취급자
④ 개인정보 보호책임자

문 15. XSS 공격에 대한 설명으로 옳은 것은?

① 자료실에 올라간 파일을 다운로드할 때 전용 다운로드 프로그램이 파일을 가져오는데, 이때 파일 이름을 필터링하지 않아서 취약점이 발생한다.
② 악성 스크립트를 웹 페이지의 파라미터 값에 추가하거나, 웹 게시판에 악성 스크립트를 포함시킨 글을 등록하여 이를 사용자의 웹 브라우저 내에서 적절한 검증 없이 실행되도록 한다.
③ 네트워크 통신을 조작하여 통신 내용을 도청하거나 조작하는 공격 기법이다.
④ 데이터베이스를 조작할 수 있는 스크립트를 웹 서버를 이용하여 데이터베이스로 전송한 후 데이터베이스의 반응을 이용하여 기밀 정보를 취득하는 공격 기법이다.

문 16. 영국, 독일, 네덜란드, 프랑스 등의 유럽 국가가 평가 제품의 상호 인정 및 정보보호평가 기준의 상이함에서 오는 시간과 인력 낭비를 줄이기 위해 제정한 유럽형 보안 기준은?

① CC(Common Criteria)
② TCSEC(Orange Book)
③ ISO/IEC JTC 1
④ ITSEC

문 17. 다음에서 설명하는 것은?

> 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위한 인증 업무이며, 공공기관, 민간기업, 법인, 단체 및 개인 등 모든 공공기관 및 민간 개인정보처리자를 대상으로 개인정보 보호 관리체계 구축 및 개인정보 보호 조치 사항을 이행하고 일정한 보호 수준을 갖춘 경우 인증마크를 부여하는 제도이다.

① SECU－STAR(Security Assessment for Readiness)
② PIPL(Personal Information Protection Level)
③ EAL(Evaluation Assurance Level)
④ ISMS(Information Security Management System)

문 18. 개인정보보호 관리체계(PIMS) 인증에 대한 설명으로 옳지 않은 것은?

① 한국인터넷진흥원이 PIMS 인증기관으로 지정되어 있다.
② PIMS 인증 후, 2년간의 유효 기간이 있다.
③ PIMS 인증 신청은 민간 기업 자율에 맡긴다.
④ PIMS 인증 취득 기업은 개인정보 사고 발생 시 과징금 및 과태료를 경감 받을 수 있다.

문 19. 다음은 침입 탐지 시스템의 탐지분석 기법에 대한 설명이다. ㉠~㉣에 들어갈 내용이 바르게 연결된 것은?

> 침입 탐지 시스템에서 (㉠)은 이미 발견되고 정립된 공격 패턴을 미리 입력해 두었다가 해당하는 패턴이 탐지되면 알려주는 것이다. 상대적으로 (㉡)가 높고, 새로운 공격을 탐지하기에는 부적합하다는 단점이 있다. (㉢)은 정상적이고 평균적인 상태를 기준으로 하여, 상대적으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 침입 탐지로 알려주는 것이다. 정량적인 분석, 통계적인 분석 등이 포함되며, 상대적으로 (㉣)가 높다.

	㉠	㉡	㉢	㉣
①	이상탐지기법	False Positive	오용탐지기법	False Negative
②	이상탐지기법	False Negative	오용탐지기법	False Positive
③	오용탐지기법	False Negative	이상탐지기법	False Positive
④	오용탐지기법	False Positive	이상탐지기법	False Negative

문 20. 위험 분석 방법 중 손실 크기를 화폐가치로 측정할 수 없어서 위험을 기술 변수로 표현하는 정성적 분석 방법이 아닌 것은?

① 델파이법
② 퍼지 행렬법
③ 순위 결정법
④ 과거자료 접근법