

정보시스템 보안

문 1. 다음 중 HTTPS를 구성하기 위해 필요한 프로토콜만을 모두 고르면?

| | |
|---------|--------|
| ㄱ. TCP | ㄴ. SSL |
| ㄷ. SOAP | ㄹ. SET |

- ① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

문 2. 웹에 관한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션의 취약점을 발표하는 기관은?

- ① IETF Web Security Working Group
② Web Application Security Working Group
③ Open Web Application Security Project
④ World Wide Web Consortium

문 3. 다음 중 데이터 기밀성을 보장할 수 있는 프로토콜은?

- ① IP
② UDP
③ Telnet
④ SSH

문 4. 이메일 등을 통해 진짜 사이트와 거의 동일하게 꾸민 가짜 사이트로 접속을 유도하여 개인정보를 탈취하는 공격 기법은?

- ① 피싱(Phishing)
② 이블 트윈 어택(Evil Twin Attack)
③ 언팩킹(Unpacking)
④ 사이버 폭력(Cyberbullying)

문 5. 다음은 전자우편의 암호화에 대한 설명이다. 괄호 안에 들어갈 용어는?

()은/는 IDEA 알고리즘과 RSA 알고리즘을 조합하여 만들었다. IDEA 알고리즘은 세션키 암호화, RSA 알고리즘은 사용자 인증을 위한 전자서명에 이용하였다. 이것의 장점으로는 구현이 쉽고, 특정 기관으로부터 인증서를 발급받지 않아도 된다는 것이다.

- ① PGP
② PEM
③ S/MIME
④ IMAP

문 6. 다음 프로토콜 중 계층이 다른 것은?

- ① ICMP
② POP3
③ TFTP
④ SNMP

문 7. 다음 중 유닉스 운영체제에서 네트워크 연결에 대한 접근제어 도구는?

- ① APT
② DDL
③ UTMP
④ TCPWrapper

문 8. 웹서비스를 대상으로 하는 다양한 코드 인젝션(Code Injection) 혹은 운영체제 명령어 인젝션(OS Command Injection) 공격 등으로부터 취약점을 갖는 PHP 함수가 아닌 것은?

- ① cmd
② system
③ eval
④ exec

문 9. 관리자는 자신이 소유하고 있는 특정 자원에 대한 자신의 권한을 다른 사람에게 위임할 수 있다. 이를 통해 사용자들에게 주어진 권한 이외에 모든 권한을 차단할 수 있는 접근 제어 모델은?

- ① 강제적 접근 제어(Mandatory Access Control)
② 임의 접근 제어(Discretionary Access Control)
③ 역할 기반 접근 제어(Role Based Access Control)
④ 속성 기반 접근 제어(Attribute Based Access Control)

문 10. 버퍼 오버플로우 공격 탐지 기법 중 스택 가드(Stack Guard)에 사용하는 기술은?

- ① Full Canary
② Buffer Canary
③ Stack Canary
④ Random Canary

문 11. 다음 설명에 해당하는 정보보안 제품 평가는?

- IT 제품의 보안성을 평가하기 위한 국제 표준
○ 여러 과정과 기준을 통해 각 시스템은 EAL로 보안 수준을 평가
○ 크게 3부분으로 구성되며, 제1부는 정보시스템의 보안 목적 및 요구 사항, 제2부는 보안 기능 요구 사항, 제3부는 보안 보증 요구 사항으로 구성

- ① TCSEC
② ITSEC
③ CC
④ ISO/IEC27001

문 12. 유닉스 파일 및 디렉토리 권한 변경 명령어와 그 기능을 연결한 것으로 옳지 않은 것은?

① chmod - 파일 및 디렉토리의 권한 변경

② chown - 파일 및 디렉토리의 소유자와 소유그룹 변경

③ chgrp - 파일 및 디렉토리의 소유그룹 변경

④ chmask - 파일 및 디렉토리 생성 시 부여되는 기본 권한 변경

문 13. OSI 각 계층 중 데이터 링크 계층에서 동작하는 프로토콜에 해당하지 않는 것은?

① L2F

② L2TP

③ PPTP

④ IPSec

문 14. SMTP에 대한 설명으로 옳지 않은 것은?

① SMTP는 실행 파일이나 2진 데이터를 텍스트 형태로 변환하여 전송한다.

② 송·수신 측이 직접 상대방을 상호 인증하는 방식을 통해 메시지를 전송한다.

③ SMTP 서버는 특정 크기 이상의 메일 메시지를 처리하지 못하고 거부한다.

④ 주로 TCP 포트 25번을 사용한다.

문 15. 윈도우즈 시스템 보안 아키텍처(Security Architecture)에 대한 설명으로 옳지 않은 것은?

① SRM(Security Reference Monitor)은 로컬 컴퓨터상에서 보안을 제어함으로써, 특권 컴포넌트들과 사용자 모드에서 동작하는 서브시스템에 보안 서비스를 제공한다.

② LSA(Local Security Authority)는 사용자 모드 프로세스에서 동작하며 윈도우즈에서 로컬 보안 정책을 집행한다.

③ SAM(Security Account Manager)은 윈도우즈 운영체제에서 로컬 주체 및 그룹에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스로 보안 토큰 발급과 저장 등을 수행한다.

④ AD(Active Directory) 서비스는 네트워크의 모든 정보를 디렉토리에 저장해 네트워크 자원을 손쉽게 찾고 접근하는 서비스를 제공한다.

문 16. ITU-T 권고안에서 정하고 있는 인증서 표준 규격은?

① RFC 822

② X.509

③ X.501

④ X.25

문 17. 다음 중 국내의 정보보호 및 개인정보보호 관리체계 인증제도에 해당하는 것은?

① P-ISMS

② ISMS-P

③ PDCA-K

④ ISMS-K

문 18. 윈도우즈 파일 시스템에 대한 설명으로 옳지 않은 것은?

① FAT16의 저장 가능 용량은 최대 2GB까지만 지원한다.

② FAT32 테이블의 기본 크기는 32비트이다.

③ NTFS는 윈도우 NT 버전에서 지원한다.

④ FAT32는 개별 폴더와 파일에 접근 제어를 설정할 수 있다.

문 19. SSL 레코드 프로토콜의 처리과정 기법에 해당하지 않는 것은?

① 압축(Compression)

② 메시지 인증 코드(Message Authentication Code)

③ 정규화(Normalization)

④ 단편화(Fragmentation)

문 20. 다음 설명에 해당하는 블루투스 공격 방식은?

블루투스 공격 장치를 검색하는 활동을 의미한다. 공격자는 블루투스의 서비스 발견 프로토콜(SDP)을 이용해 공격이 가능한 블루투스 장치의 종류(예, 전화 통화, 키보드 입력, 마우스 입력 등)를 검색하고 모델을 확인할 수 있다.

① 블루스나프(Bluesnarf)

② 블루버그(Bluebug)

③ 블루프린팅(Blueprinting)

④ 블루재킹(Bluejacking)