정보시스템 보안

〔강평 및 해설 : 임재선 교수〕

총 평

전반적인 난이도는 전년도와 비교해 평이하다고 볼 수 있다. 특이할 점은 시스템 보안 분야뿐만 아니라 애플리케이션 보안에서 많이 출제되었고 네트워크 보안과 정보보안 관리에서도 출제가 되었다는 것이다. 분야별로 정리하면 애플리케이션 보안 : 8문제, 네트워크 보안 3문제, 시스템 보안 : 5문제, 정보보안 관리 : 2문제, 보안과 암호 : 1문제가 출제되었다.

과목은 시스템 보안이지만 애플리케이션 보안과 네트워크 보안도 같이 공부해야 고득점을 얻을 수 있을 것이다.

특이할 점은 정보보안 관리 분야에서 국제/국가 표준 및 인증체계를 묻는 문제와 ISMS-P를 묻는 문제가 출제되었다는 것이다.

기존 ISMS와 PIMS를 통합하고 일원화하여 ISMS-P가 나왔는데 시사 문제로 출제를 한 것 같고, 애플리케이션 보안에서는 이메일과 관련된 보안 프로토콜을 묻는 문제가 3문제가 출제되어 이메일 관련 보안이슈를 중대하게 보고 있음을 알 수 있다.

정보시스템 보안은 시스템 보안 분야만 집중적으로 하기보다는 학습의 범위를 넓혀 애플리케이션과 네트워크 보안 분야를 함께 공부하는 것이 빠른 합격의 길이라 생각한다.

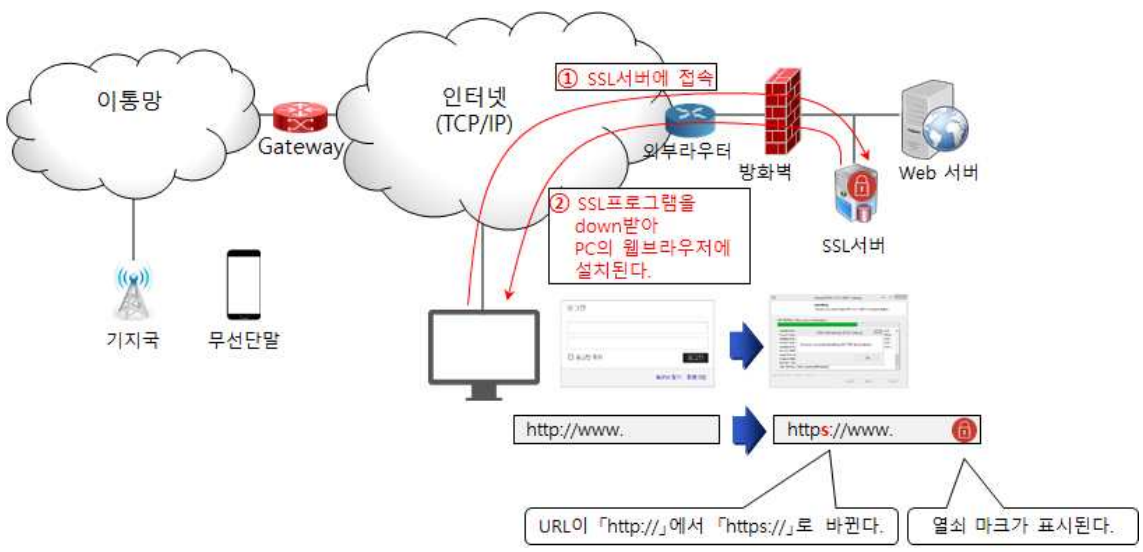
문 1. 다음 중 HTTPS를 구성하기 위해 필요한 프로토콜만을 모두 고르면?

ㄱ. TCP ㄴ. SSL
ㄷ. SOAP ㄹ. SET

① ㄱ, ㄴ
② ㄱ, ㄹ
③ ㄴ, ㄷ
④ ㄷ, ㄹ

해설

HTTPS는 본질적으로 HTTP와 동일한 프로토콜이나 보안 전송 방식인 SSL을 사용하여 네트워크를 통한 모든 데이터의 무결성과 프라이버시를 보호 받는다. https는 SSL로 암호화 한다.
SSL은 웹브라우저와 웹서버 간에 안전한 정보 전송을 위해 사용되는 암호화 방법이다.



정답 1

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

해설

국제웹보안표준기구 OWASP(The Open Web Application Security Project)는 오픈소스 웹 애플리케이션 보안 프로젝트로 국제 웹보안 표준기구이며, 웹에 대한 정보 노출, 악성파일 및 스크립트 보안 취약점 등을 연구하며, 10대 웹 애플리케이션 취약점을 정기적으로 발표하는 비영리 단체이다.
국제웹보안표준기구 OWASP(The Open Web Application Security Project)에서는 해마다 웹 관련 상위 10개의 주요 취약점을 발표하고 있다.

정답 3

문 3. 다음 중 데이터 기밀성을 보장할 수 있는 프로토콜은?
① IP
② UDP
③ Telnet
④ SSH

해설

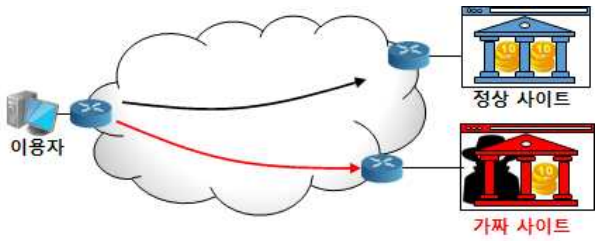
SSH(Secure Shell)는 네트워크 보안 도구 중 하나로 원격접속을 안전하게 할 수 있게 해주는 프로토콜이다.

정답 4

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)

해설

피싱(Phishing)은 개인정보(Private Data)와 낚시(Fishing)의 합성어로, 개인정보를 낚는다는 의미를 가지고 있다.
유명기관을 사칭하거나 개인정보 및 금융정보를 불법적으로 수집하여 금전적인 이익을 노리는 사기 수법이다.
피싱의 대표적인 증상은 클릭 시 이상한 사이트로 유도(URL이 틀리다)된다는 것이다.



정답 1

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

해설

PGP(Pretty Good Privacy)는 인터넷에서 전자우편을 사용할 때 보내고자 하는 내용을 암호 알고리즘을 이용하여 암호화해서 해당 키(Key)가 있어야만 내용을 볼 수 있도록 하는 것으로 기밀성, 무결성, 인증, 송신 부인방지 등의 기능을 지원하는 이메일 보안 기술이다.

정답 1

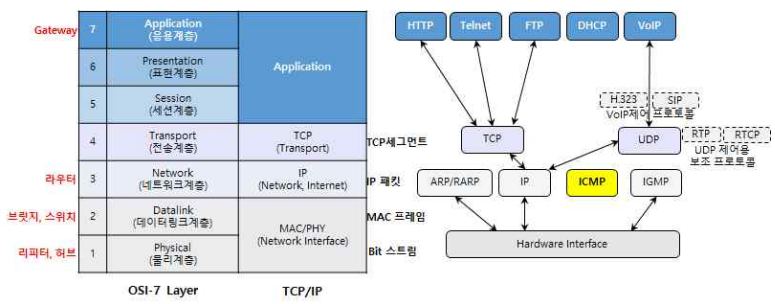
문 6. 다음 프로토콜 중 계층이 다른 것은?

① ICMP
② POP3
③ TFTP
④ SNMP

해설

ICMP(Internet Control Message Protocol)는 인터넷상의 노드 간에 에러 사항이나 통신 제어를 위한 메시지를 보고하게 할 목적으로 만들어진 3계층 프로토콜이다

POP3, TFTP, SNMP는 응용계층 프로토콜이다.



정답 1

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

① APT
② DDL
③ UTMP
④ TCPWrapper

해설

TCP 래퍼(TCP Wrapper)는 유닉스 계열의 운영체제에서 네트워크 연결에 대한 접근제어 도구이다.

정답 4

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

해설

① cmd는 윈도우 환경에서 사용할 수 있는 도스 명령 프롬프트이다.

정답 1

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)

해설

DAC(Discretionary Access Control: 임의적 접근통제)
정보의 소유자가 접근제어 설정, 대부분 OS에서 채택, 사용자별로 접근권리를 이전할 수 있다.
전통적인 UNIX 운영체계의 기본 접근제어 방식에 적용되었다.
데이터 소유자(Owner)가 다른 사용자의 식별자(ID)에 기초하여 자신의 의지대로 데이터에 대한 접근권한을 부여한다.

정답 2

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

해설

1) 스택(Stack)영역은 프로그램 실행 중 함수 호출 시 생성되는 매개 변수가 저장되었다가 함수가 종료되면 시스템에 반환되는 영역이다.
2) 스택가드(Stack Guard): 함수 진입시 스택에 SFP(Saved Frame Pointer)와 RET를 저장할 때 공격자에 의해 값이 변경되는 것을 막기 위해 스택 변수 공간과 SFP에 특정값을 저장

Terminator canaries : canary 값으로 NULL, CR, LF, Oxff 값의 조합이 사용되어, 공격자 공격시, 종료문자로 구성된 canary 값에 접근을 할 수 없음
Random canary : 프로그램을 실행할 때마다 랜덤한 canary 값을 삽입하여 공격자가 값을 예측하지 못하도록 함
Null canary(0x00000000) : 메모리상의 공격을 막기위해 canary 값을 NULL로 구성함. 공격자는 공격코드상에 NULL 값을 삽입할 수 없으므고 canary 값에 접근이 불가능.

정답 4

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

해설

③ CC(Common Criteria: 공통평가기준) : 정보보호 제품의 평가 기준을 규정한 국제 표준(ISO 15408)으로, 국제사회에서 널리 이용할 수 있는 IT 보안성 평가를 위한 기준개발 결과물이다.

정답 3

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

해설

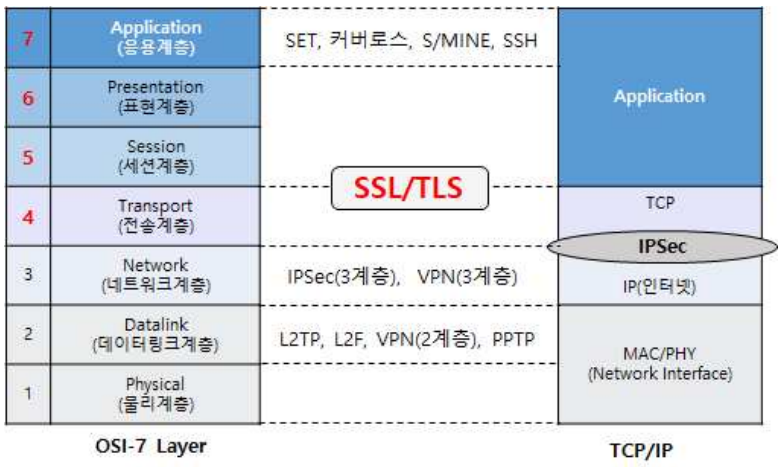
④ 파일 및 디렉토리 생성 시 부여되는 기본 권한 변경하는 명령어는 umask이다.

정답 4

문 13. OSI 각 계층 중 데이터 링크 계층에서 동작하는 프로토콜에 해당하지 않는 것은?
① L2F
② L2TP
③ PPTP
④ IPSec

해설

④ IPsec은 네트워크에서 IP에 보안성을 제공해 주는 프로토콜로 3계층에서 동작한다.



정답 4

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.

해설

SMTP는 간이 우편 전송 프로토콜(Simple Mail Transfer Protocol)의 약자. 이메일 전송에 사용되는 네트워크 프로토콜이다. 인증기능은 S/MIME 프로토콜을 이용한다.

정답 2

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

해설

③ 보안 계정 관리자(SAM: Security Account Manager)는 윈도우 XP, 윈도우 비스타, 그리고 윈도우 7에서 사용자의 비밀번호를 저장하는 데이터베이스 파일이다. SAM(보안 계정 관리자)은 사용자/그룹 계정 정보에 대한 데이터베이스를 관리한다.

정답 3

문 16. ITU-T 권고안에서 정하고 있는 인증서 표준 규격은?

① RFC 822
② X.509
③ X.501
④ X.25

해설

② X.509 : PKI(공개키 기반 구조)방식에서 공개키(RSA) 기반의 인증 시스템 표준이다.

정답 2

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

① P-ISMS
② ISMS-P
③ PDCA-K
④ ISMS-K

해설

② ISMS(Information Security Management System: 정보보호관리체계) 인증제도
정보보호관리체계(ISMS: Information Security Management System)는 정보 자산의 비밀을 유지하고 결함이 없게 하며 언제든 사용할 수 있게 한 보호 절차와 과정으로, 정보통신망의 안정성과 신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 인증 기준에 적합한지에 관하여 인증을 부여하는 제도이다.

정답 2

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.

해설

④ FAT32
총 32비트, 즉 232개의 클러스터를 가질 수 있으며, 호환성이 좋은 편이라 리눅스나 다른 운영체제에 정보를 옮길 때 유용하게 쓰인다.
호환성이 좋아 리눅스나 다른 운영체제에 정보를 옮길 때 종종 사용된다. 그러나 접근제어를 할 수 없어 보안과는 거리가 먼 파일 시스템이다.

정답 4

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)

해설

SSL의 레코드 프로토콜에서 응용메시지를 처리하는 동작순서는 '단편화 →압축 →MAC 첨부→암호화→SSL 레코드 헤더 붙이기'의 과정을 거친다.
정규화란 관계형 데이터베이스(테이블간에 관계를 맺을 수 있는 상황)에서 중복을 최소화 하기 위해서 데이터를 구조화 하는 작업.

정답 3

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)

해설

③ 블루프린팅(BluePrinting) 블루투스 공격장치의 검색 활동을 의미한다.

정답 3