2과목	컴 퓨 터 보 안 (36~60)
출제위원 : 방송대 김진욱	
출제범위 : 교재 1장~11장(멀티미디어 강의 1강~11강 포함)	

36. 다음 중 정보보호의 핵심목표(CIA triad)에 포함되지 **않는** 것은? (2점)
① 기밀성(confidentiality)
② 무결성(integrity)
③ 가용성(availability)
④ 접근제어(access control)

37. 다음 중 허락된 자가 정보에 접근하고자 할 때 이것이 방해 받지 않도록 하는 정보보호의 목표는? (3점)
① 기밀성(confidentiality)
② 무결성(integrity)
③ 가용성(availability)
④ 접근제어(access control)

38. 암호와 관련된 설명으로 바른 것은? (4점)
① 두 사람이 안전하지 않은 채널을 통해 정보를 주고받더라도 제3자는 이 정보의 내용을 알 수 없도록 하는 것
② 평문이란 코드화된 메시지를 의미함
③ 평문을 암호문으로 변환하는 과정을 복호화라 함
④ 키는 암호화에는 중요하지만 복호화에는 중요하지 않음

39. 스파르타의 봉 암호로 평문 '12345678'을 암호화할 때 **만들어질 수 없는** 암호문은? (4점)
① 13572468
② 12348765
③ 14725836
④ 15263748

40. 다음 중 대칭키 암호 알고리즘은? (2점)
① RSA
② AES
③ ECC
④ ElGamal

41. 다음 중 공개키 암호에 대한 설명으로 바른 것은? (3점)
① 암호화와 복호화에 하나의 같은 키를 사용함
② 대칭키 암호에 비해 속도가 빠름
③ 누구나 공개키를 이용하여 암호화를 할 수 있음
④ 블록 암호와 스트림 암호로 나누어짐

42. 다음 중 메시지 인증에 대한 설명으로 **잘못된** 것은? (3점)
① 메시지의 내용이 전송 도중 불법적으로 변경되지 않고 정확하고 완전하게 수신되었는지 확인하는 것
② 메시지에 대한 무결성을 확인
③ HMAC은 공개키 암호에 기반을 둠
④ CMAC은 블록 암호에 기반을 둠

43. 지문, 홍채, 음성 등 개개인의 고유한 정보를 이용하는 사용자 인증 방식은? (2점)
① 비밀번호 방식
② 생체인식 방식
③ 토큰 방식
④ 2단계 인증

※ (44~46) 다음 보기 중에서 아래 문제들의 해답을 고르시오.

가. 바이러스(Virus)
나. 트로이 목마(Trojan Horse)
다. 백도어(Backdoor)
라. 랜섬웨어(Ransomware)
마. 스캐닝(Scanning)
바. 스푸핑(Spoofing)
사. 스니핑(Sniffing)

44. 공격자가 시스템에 침입한 후 이후에도 손쉽게 피해 시스템에 대한 접근권한을 획득하기 위한 용도로 설치하는 악성코드는? (3점)
① 가 ② 다
③ 라 ④ 마

45. 사용자의 중요한 정보를 인질로 삼아 금전을 요구하는 악성코드는? (3점)
① 가 ② 다
③ 라 ④ 바

46. 네트워크상의 데이터를 도청하는 행위를 일컫는 사이버 공격 방식은? (3점)
① 가 ② 나
③ 라 ④ 사

47. 과도한 데이터를 입력하여 프로그램의 복귀주소를 조작함으로써 공격자가 원하는 코드를 실행하는 공격은? (2점)
① 버퍼 오버플로 공격
② 사전 공격
③ 사회공학적인 공격
④ 스푸핑

48. 네트워크 보안에서 공격의 방식과 그에 대한 설명이 **잘못** 짝지어진 것은? (2점)
① 능동적 공격 - 암호화로 방어
② 수동적 공격 - 통신 회선상의 데이터를 암호화하여 방어
③ 능동적 공격 - 통신 회선상의 정보를 변조, 위조하는 행위
④ 수동적 공격 - 수신 측에서 데이터에 대한 무결성을 확인하여 방어

49. 네트워크 보안의 목표와 거리가 **먼** 것은? (3점)
① 기밀성 ② 가용성
③ 부인방지 ④ 다양성

50. 다음 설명에 가장 부합하는 보안 시스템은? (3점)

- 외부 네트워크와 내부 네트워크 사이에 위치시켜 두 네트워크 사이를 오가는 트래픽의 종류와 양을 제어 - 정상적인 사용자에 대해서만 접근을 가능하게 해주고 불법적이고 인증되지 않은 사용자의 접근을 차단시키는 시스템

① 침입차단 시스템(방화벽)
② 침입탐지 시스템(IDS)
③ 침입방지 시스템(IPS)
④ 가상사설망(VPN)

51. 침입차단 시스템의 구축 형태 중 중립적인 네트워크인 비무장지대(DMZ)를 구축하는 것은? (2점)

① 스크리닝 라우터
② 베스천 호스트
③ 스크린 호스트 게이트웨이
④ 스크린 서브넷 게이트웨이

52. 다음 설명에 해당하는 분석 방법은? (3점)

- 지금까지 알려지지 않은 공격을 검출할 수 있음 - 잘못된 경고 신호를 보낼 가능성이 높음

① 통계적 분석
② 시그니처 분석
③ 무결성 분석
④ 임의적 분석

53. 다음 설명에 해당하는 가상사설망의 기반 기술은? (2점)

- 특정 사용자들 간에 전용망처럼 사용할 수 있게 하는 것 - 인터넷 상의 가상정보 흐름 통로를 이용

① 터널링 기술
② 키 관리 기술
③ VPN 관리 기술
④ 멀티캐스트 기술

54. PGP에서 사용되는 키의 종류가 **아닌** 것은? (2점)

① 세션키 ② 공개키
③ 개인키 ④ 평문구문

55. S/MIME의 보안 서비스와 알고리즘이 **잘못** 짝지어진 것은? (3점)

① 메시지 암호화 - RSA
② 전자서명 - RSA
③ 세션키 분배 - RSA
④ 해시함수 - SHA-256

56. 메일이나 웹페이지에 추가적인 악성 스크립트를 포함시켜 웹 클라이언트가 이를 열면 자동으로 악성 스크립트가 실행되게 하는 공격은? (4점)

① SQL injection
② 크로스 사이트 스크립팅(XSS)
③ 접근제어 실패
④ 웹 서버 공격

57. 접근제어에 대한 공격을 방어하는 방법으로 가장 올바른 것은? (3점)

① 관리자 페이지에 대한 링크를 만들지 않음
② 관리자 페이지 자체에 접근권한을 설정
③ URL에 사용자 ID를 포함
④ 디렉터리 목록 보여주는 기능 활성화

58. 무선 LAN 환경에서 기밀성을 제공하기 위한 알고리즘이지만 현재는 취약성이 드러나 사용하지 **않는** 것은? (3점)

① WEP
② RSN
③ EAP
④ WPA2

59. 다음 중 디지털 증거를 찾을 수 **없는** 것은? (3점)

① 외장하드
② 블랙박스
③ 진주목걸이
④ 스마트폰

60. 다음 중 디지털 증거의 특성으로 바른 것은? (3점)

① 가시성
② 소규모성
③ 휘발성
④ 지역성