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

36. 다음 중 정보보호의 핵심목표(CIA triad)에 포함되는 것은? (4점)

① 인증(authentication)
② 가용성(availability)
③ 부인방지(non-repudiation)
④ 접근제어(access control)

37. 다음 중 허락되지 않은 자가 정보를 함부로 수정할 수 없도록 하는 것을 의미하는 정보보호의 목표는? (3점)

① 부인방지(non-repudiation)
② 무결성(integrity)
③ 가용성(availability)
④ 기밀성(confidentiality)

38. 암호는 정보보호의 목표 중 무엇을 보장하기 위한 필수적인 기술인가? (3점)

① 기밀성(confidentiality)
② 가용성(availability)
③ 부인방지(non-repudiation)
④ 접근제어(access control)

39. 다음 중 전치법에 대한 설명으로 바른 것은? (4점)

① 평문의 문자들을 다른 문자로 치환함으로써 암호화함
② 대표적인 전치법으로 시저 암호가 있음
③ 스파르타의 봉 암호는 봉의 굵기가 키임
④ 시프트 암호는 시저 암호를 일반화함

40. 다음 암호에 대한 설명 중 <u>틀린</u> 것은? (3점)

① 대칭키 암호는 암호화와 복호화에 하나의 같은 키를 사용함
② 공개키 암호는 암호화와 복호화에 서로 다른 키를 사용함
③ 대칭키 암호는 암호화와 복호화 속도가 빠름
④ 공개키 암호는 키 분배의 문제가 있음

41. 다음 중 공개키 암호 알고리즘은? (2점)

① DES
② IDEA
③ RSA
④ AES

42. 비밀번호 방식의 사용자 인증을 이용하는 경우, 시스템에 저장된 비밀번호가 유출될 경우를 대비하여 비밀번호 대신 무엇을 시스템에 저장하는가? (2점)

① 개인키
② 공개키
③ 해시함수
④ 해시코드

※ (43~45) 다음 보기 중에서 아래 문제들의 해답을 고르시오.

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

43. 네트워크를 통해 스스로 감염되며 숙주가 필요 없는 악성코드는? (3점)

① 가 ② 나
③ 다 ④ 라

44. 정상적인 기능을 하는 프로그램으로 가장하여 프로그램 내에 숨어서 의도하지 않은 기능을 수행하는 악성코드는? (3점)

① 다 ② 라
③ 마 ④ 바

45. 공격대상 호스트들이나 네트워크에 대한 취약점을 발견하기 위한 사전 정보수집 활동은? (3점)

① 마 ② 바
③ 사 ④ 아

46. 서버의 침입 및 정보유출 단계에 대한 설명으로 바르지 <u>않은</u> 것은? (2점)

① 정보획득 단계 - 공격대상 시스템에 대한 정보를 획득
② 권한획득 단계 - 최종적으로 관리자 권한을 획득함
③ 공격 단계 - 관리자 권한을 이용해서 침입흔적을 지움
④ 재침입 단계 - 백도어를 설치함

47. 사람을 속여서 민감한 정보를 유출하게 하는 공격은? (3점)

① 버퍼 오버플로 공격
② 사전 공격
③ 사회공학적인 공격
④ 레이스 컨디션 공격

48. 강력한 로그인, 감시 기능이 있으며 프락시 서버를 활용하여 확장성이 우수하지만 속도가 빠르지 않은 방화벽의 구성 방식은? (2점)

① 패킷 필터링
② 서킷 게이트웨이
③ 애플리케이션 게이트웨이
④ 하이브리드 방식

49. 침입탐지 시스템의 구성과 설명이 바르게 짝지어지지 <u>않은</u> 것은? (3점)

① 모니터링부 - 정보수집
② 분석 및 조치부 - 분석 및 침입탐지
③ 관리부 - 보고 및 조치
④ 관리부 - 통제 및 관리, 보안정책 제공

50. 다음 설명에 해당하는 분석 방법은? (3점)

- 알려진 공격에 대한 패턴을 활용하여 침입을 탐지 - 패턴에 해당하지 않는 공격은 대처 불가

① 통계적 분석
② 시그니처 분석
③ 무결성 분석
④ 임의적 분석

51. 가상사설망(VPN)에 대한 설명으로 가장 바른 것은? (2점)
① 공중망을 이용하여 사설망처럼 직접 운용 관리하는 것
② 높은 비용으로 성능향상 제공
③ 방화벽 기반 VPN이 라우터 기반 VPN보다 보안성은 낮지만 성능이 좋음
④ 서비스 품질(QoS)은 제공하지 못함

52. PGP 보안 서비스와 사용되는 알고리즘이 바르게 짝지어진 것은? (3점)
① 인증 - RSA, SHA
② 기밀성 - DES, ECC
③ 압축 - AES
④ 전자우편 호환성 - 유니코드 변환

53. 기수 64(Radix-64)는 데이터를 6 비트 단위로 나눠서 각 6 비트를 하나의 문자로 표현하는 방법이다. 만약 6 바이트의 데이터에 기수 64를 적용한다면 몇 개의 문자로 변환되는가? (단, 마지막 패드 문자는 고려하지 않는다고 가정) (4점)
① 1 ② 3
③ 6 ④ 8

54. S/MIME의 메시지 구성에 대한 설명으로 바르지 <u>않은</u> 것은? (2점)
① 봉인된 데이터 - 암호화된 콘텐트 타입과 수신자를 위한 복호화된 콘텐트 암호키로 구성
② 서명된 데이터 - 콘텐트와 전자서명을 base64로 부호화
③ 클리어 서명 데이터 - 전자서명만 base64로 부호화
④ 서명 및 봉인된 데이터 - 암호화된 데이터는 서명될 수 있고 서명된 데이터나 클리어 서명 데이터는 암호화될 수 있음

55. 데이터베이스 쿼리에 추가적인 SQL을 삽입함으로써 악의적인 행위를 가능하게 하는 공격 방법은? (2점)
① SQL injection
② 크로스 사이트 스크립팅(XSS)
③ 접근제어 실패
④ 웹 서버 공격

56. 공격자가 악성 스크립트를 특정 게시판에 등록하여 사용자가 해당 게시판에 접속하여 이 게시물을 열면 자동으로 악성 스크립트가 실행되게 하는 공격은? (3점)
① SQL injection
② 저장된 크로스 사이트 스크립팅(XSS)
③ 반사된 크로스 사이트 스크립팅(XSS)
④ 접근제어 실패

57. 임시 키 무결성 프로토콜로 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용되는 것은? (3점)
① WEP
② TKIP
③ WPA
④ WPA2

58. 디지털 포렌식 절차가 가장 바르게 나열된 것은? (2점)
① 사전준비 → 조사분석 → 포장 및 이송 → 정밀검토 → 증거수집 → 보고서 작성
② 사전준비 → 증거수집 → 조사분석 → 정밀검토 → 보고서 작성 → 포장 및 이송
③ 포장 및 이송 → 사전준비 → 증거수집 → 조사분석 → 정밀검토 → 보고서 작성
④ 사전준비 → 증거수집 → 포장 및 이송 → 조사분석 → 정밀검토 → 보고서 작성

59. 다음 중 디지털 증거의 특성으로 바른 것은? (3점)
① 지역성
② 영구성
③ 대규모성
④ 가시성

60. 디지털 포렌식 절차 중 지켜져야 할 사항으로 바르지 <u>않은</u> 것은? (3점)
① 적법절차의 준수
② 원본의 안전한 보존
③ 증거의 무결성 확보
④ 분석결과의 비반복성