| 2과목 | 컴퓨터보안 (36~60) |
|---|---|
| 출제위원 : 방송대 김진욱 | |
| 출제범위 : 교재 1장~11장(멀티미디어 강의 1강~11강 포함) | |

**36. 정보보호에 대한 설명으로 바른 것은? (3점)**

① 정보를 여러 가지 위협으로부터 보호하기 위한 정책 및 기법
② 정보의 상태는 전달 중인 경우만 고려
③ 위협의 종류에는 허락된 접근과 허락된 수정이 있음
④ 컴퓨터 보안보다 좁은 개념임

**37. 다음 중 허락되지 않은 자가 정보의 내용을 알 수 없도록 하는 것을 의미하는 정보보호의 목표는? (3점)**

① 가용성(availability)
② 기밀성(confidentiality)
③ 인증(authentication)
④ 무결성(integrity)

**38. 정보를 보낸 사람이 나중에 정보를 보냈다는 것을 부인하지 못하도록 하는 것은? (3점)**

① 발신 부인방지
② 수신 부인방지
③ 발신 접근제어
④ 수신 접근제어

**39. 암호와 관련된 용어 설명이 바른 것은? (4점)**

① 평문(plaintext) - 코드화된 메시지
② 암호문(ciphertext) - 원래의 메시지
③ 복호화(decryption) - 암호문 → 다른 암호문
④ 암호화(encryption) - 평문 → 암호문

**40. 다음 중 치환법에 대한 설명으로 바른 것은? (4점)**

① 평문에 있는 문자들의 순서를 바꿈으로써 암호화함
② 대표적인 치환법으로 스파르타의 봉 암호가 있음
③ 시프트 암호는 스파르타의 봉 암호를 일반화함
④ 시프트 암호는 알파벳에 대해 26가지의 서로 다른 키 존재

**41. 다음 중 대칭키 암호에 대한 설명으로 바른 것은? (3점)**

① 암호화와 복호화에 두 개의 서로 다른 키를 사용함
② 공개키 암호에 비해 속도가 느림
③ 블록 암호와 스트림 암호로 나누어짐
④ 대표적인 알고리즘으로 RSA가 있음

**42. 다음 중 공개키 암호에 대한 설명으로 바르지 <u>않은</u> 것은? (3점)**

① 공개키와 개인키를 사용
② 누구나 공개키를 이용하여 암호화 가능
③ 오직 자신만 개인키를 이용하여 복호화 가능
④ 개인키로 암호화하면 개인키로 복호화 가능

**43. 스마트카드 등 사용자가 소유하고 있는 특정한 정보를 이용하는 사용자 인증 방식은? (2점)**

① 비밀번호 방식
② 생체인식 방식
③ 토큰 방식
④ 메시지 인증 방식

※ (44~47) 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)
자. 서비스 거부(DoS) 공격
차. 분산 서비스 거부(DDoS) 공격

**44. 시스템이나 사용자의 파일에 자신을 복제하고 그 컴퓨터 시스템 내에서 증식하거나 시스템을 파괴하는 악성코드는? (2점)**

① 가
② 나
③ 라
④ 아

**45. 사용자의 문서 파일 등을 암호화한 후 암호를 풀기 위해서는 비트코인 등을 송금하도록 유도하는 악성코드는? (2점)**

① 나
② 마
③ 바
④ 자

**46. 피해 호스트가 신뢰하는 호스트로 가장하여 정보를 수집하거나 가로채는 방식의 공격은? (2점)**

① 라
② 마
③ 바
④ 사

**47. 여러 대의 공격자를 분산적으로 배치해 동시에 대량의 데이터를 전송하여 특정 서비스나 자원의 가용성을 떨어트리는 결과를 초래하는 유형의 공격은? (2점)**

① 다
② 사
③ 아
④ 차

**48. ID와 패스워드가 될 가능성이 있는 단어를 미리 모아두고 이 단어를 대입하며 계정을 크랙하는 공격은? (2점)**

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

**49. 네트워크 보안 메커니즘의 하나로 IP 데이터그램의 무결성이나 기밀성을 보장할 수 있는 것은? (3점)**

① IPsec
② SSL
③ TLS
④ MAC

50. 침입탐지 시스템(IDS)의 분석 방법 설명이 바르게 짝지어진 것은? (3점)
① 시그니처 분석 - 알려진 공격에 대한 패턴을 활용하여 침입을 탐지
② 시그니처 분석 - 잘못된 경고 신호를 보낼 가능성이 높음
③ 통계적 분석 - 알려지지 않은 공격은 대처 불가
④ 무결성 분석 - 실시간 대응에 적합

51. 다음 설명에 가장 부합하는 보안 시스템은? (3점)

| |
|---|
| - 공중망을 이용하여 사설망처럼 직접 운용 관리하는 것<br>- 중요한 기반 기술로 터널링 기술이 있음 |

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

52. 메일 보안에 대한 설명으로 바르지 **않은** 것은? (3점)
① 일반적인 메일은 송수신자 주소와 내용까지 노출됨
② 일반적인 메일은 도청은 가능하지만 변조는 불가능
③ 메일 보안 기술로는 PGP, S/MIME이 있음
④ PGP는 기밀성, 인증, 무결성 등을 지원

53. 기수 64(Radix-64)는 데이터를 6 비트 단위로 나눠서 각 6 비트를 하나의 문자로 표현하는 방법이다. 만약 9 바이트의 데이터에 기수 64를 적용한다면 몇 개의 문자로 변환되는가? (단, 마지막 패드 문자는 고려하지 않는다고 가정) (4점)
① 9
② 12
③ 36
④ 54

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

55. 웹 보안에 대한 설명으로 바르지 **않은** 것은? (3점)
① 다양한 공격으로부터 웹 서비스를 지키기 위한 것
② 네트워크 부분은 SSL/TLS를 적용하여 해결 가능
③ 웹 클라이언트 부분은 백신으로만 해결 가능
④ 웹 서버 부분은 주기적인 취약점 점검 및 보안 패치 적용 필요

56. URL에 사용자 ID를 포함하도록 웹 서비스를 구성한 경우 이를 통한 공격을 일컫는 위협 요소는? (3점)
① SQL injection
② 크로스 사이트 스크립팅(XSS)
③ 접근제어 실패
④ 웹 클라이언트 공격

57. IEEE 802.11i 표준인 RSN (Robust Security Network)의 프로토콜이 **아닌** 것은? (2점)
① TKIP
② CCMP
③ WEP
④ EAP

58. 다음은 범죄 현장에서 발견된 것들이다. 이 중 디지털 증거와 가장 거리가 **먼** 것은? (3점)
① USB 메모리
② 종이사전
③ 디지털 액자
④ 블랙박스

59. 다음 중 메모리나 네트워크 상에서만 일시적으로 존재하고 작업이 끝나거나 전원이 꺼지면 사라지는 디지털 증거의 특성은? (3점)
① 비가시성
② 변조 가능성
③ 휘발성
④ 초국경성

60. 안티 포렌식에 대한 설명으로 바르지 **않은** 것은? (3점)
① 포렌식 기술을 위해 증거물을 온전하게 남기려는 활동
② 단순 포맷이 아닌 전문 제품으로 데이터를 완전 삭제
③ 메타 데이터를 변조하여 타임라인 분석 방어
④ 데이터를 암호화하여 증거로 사용되지 못하도록 방어