사이버보안 1과제 이론 출제 범위

시스템 보안, 네트워크 보안, 어플리케이션 보안, 정보보안 일반 각 부문에서 10문제씩 총 40문제를 출제합니다.

□ 출제 범위

시스템 보안	1) 유닉스 시스템 구성요소 및 역할 2) 유닉스 시스템 로그 파일의 종류와 특징 3) 윈도우 LSA, SAM, SRM 개념 4) IPtables 기초 문법 5) 아이노드의 개념과 특징 6) 윈도우 레지스트리 구조 7) 버퍼 오버플로 방지 대책 8) 버퍼 오버플로, 포맷 스트링, 레이스컨디션 공격의 개념과 특징 9) 윈도우 이벤트 로그의 종류와 특징 10) 악성 소프트웨어의 종류, 루트킷의 개념과 특징
네트워크 보안	11) TCP/IP 4 계층 구조, 각 계층별 특징 12) 네트워크 기반 공격기술의 이해와 대응 (DoS/DDoS 공격의 종류, ARP/IP/DNS 스푸핑) 13) TCP/UDP 프로토콜의 특징 14) 네트워크 기반 공격기술의 이해와 대응 (DoS/DDoS 공격의 종류, ARP/IP/DNS 스푸핑) 15) 세션 하이재킹 공격원리 16) 무선 암호화 프로토콜(WEP, WPA) 특징 17) 네트워크 도구의 이해와 활용(ping, traceroute, netstat, tcpdump로 제한) 18) IPsec 프로토콜 19) 각종 포트 스캐닝 기법 20) 보안 솔루션의 종류별 개념과 특징 (방화벽, IDS/IPS, UTM, ESM으로 제한)
어플리케이션 보안	21) 전자우편 보안 프로토콜(PGP, S/MIME) 22) FTP 모드와 익명(Anonymous) FTP의 개념 23) XSS(Cross Site Scripting), SQL Injection, CSRF(Cross-site Request Forgery), HTTP Get flooding 개념 24) 전자우편 보안 프로토콜(PGP, S/MIME) 25) SSL/TLS 프로토콜 특징 26) HTTP 주요 상태 코드 27) HTTP 요청 메소드 종류 28) DNSSEC의 개념과 특징 29) SSL/TLS 프로토콜 구조 30) 전자우편 시스템 구성요소
정보보안 일반	31) 접근 통제 정책 32, 33) 해시 함수의 개념과 특성 34) 대칭키/공개키 암호 알고리즘의 종류 35) 디피 헬만(Diffie-Hellman) 알고리즘 계산법 36, 37, 40) 대칭키 암호 시스템 공개키 암호 시스템 특징, 키 개수 계산법 38) Kerberos v4 개념 및 특징 39) 접근 통제 모델 - Biba