출제기준(필기)

직무 분야	정보통신	중직무분야	정보기술	자격종목	정보보안산업기사	적용기간	2019. 1. 1. ~ 2022.12.31.
○직무내용 : 보안에 관련한 시스템과 응용 서버, 네트워크 장비 및 보안장비에 대한 전문지식과 운용기술을 갖추고 시스템/네트워크/어플리케이션 분야별 기초 보안업무를 수행							
필기검정방법	객관식		문제수	80문		시험시간	2시간

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
시스템 보안	20문	1.클라이언트 보안	1. 클라이언트 보안 관리	1. 운영체제 이해 및 관리 2. 인증·접근통제의 이해 및 관리 3. 파일시스템 이해 및 관리 4. 공격기술의 이해 및 대응관리 5. 최신 유·무선 단말기의 보안(공격기술 및 대응기술, 보안이슈 등) 이해 및 관리
		2. 서버 보안	1. 서버 보안 관리	1. 운영체제 이해(레지스터, 웹 브라우저, 보안도구 등) 2. 인증·접근통제 이해 및 관리 3. 파일시스템 이해 및 관리 4. 공격 및 대응기술 이해 및 관리 5. 백업기술 이해 및 관리
네트워크 보안	20문	1. 네트워크 일반	1. 네트워크 개념 이해	1. 네트워크의 개요(OSI 7 Layers 및 TCP, UDP, IP, ICMP 등 네트워크 프로토콜) 2. 네트워크의 종류별 동작 원리 및 특징(Ethernet, LAN, Intranet, Extranet, Internet, CAN, PAN, HAN, SDN 등) 3. 네트워크 주소의 개요 (IPv4, IPv6 Addressing, Subnetting, CIDR, VLSM, 데이터 캡슐화, Multicast, Broadcast 등) 4. 네트워크 주소의 종류별 동작원리 및 특징(공인주소, 사설주소, 정적주소, 동적주소, NAT 등) 5. 포트(Port)의 개요

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
			2. 네트워크의 활용	1. 네트워크 장비별 원리 및 특징 (NIC, Router, Bridge, Switch, Hub, Repeater, Gateway, VLAN 등) 2. 네트워크 공유(Share)의 동작원리와 특징(Netbios, Netbeui, P2P 등) 3. 유·무선 네트워크 서비스의 개요와 종류별 특징 4. 네트워크 도구(ping, arp, rarp, traceroute, netstat, tcpdump 등)의 이해 및 활용
		2. 네트워크 기반 공격기술의 이해 및 대응	1. 서비스 거부(DoS) 공격	1. 서비스 거부(DoS) 공격 유형별 동작원리 및 특징 2. 각종 서비스 거부(DoS) 공격에 대한 대응 방법
			2. 분산 서비스 거부(DDoS) 공격	1. 분산 서비스 거부(DDoS) 공격 유형별 동작원리 및 특징 2. 각종 분산 서비스 거부(DDoS) 공격에 대한 대응 방법
			3. 스캐닝	1. 포트 및 취약점 스캐닝의 동작원리와 특징 2. 포트 및 취약점 스캐닝의 대응 방법
			4. 스푸핑 공격	1. 스푸핑 공격의 동작원리 및 특징(Spoofing) 2. 스푸핑 공격의 대응 방법
			5. 스니핑 공격	1. 스니핑 공격의 동작원리 및 특징 (Sniffing, Session Hijacking 등) 2. 스니핑 공격의 대응 방법
			6. 원격접속 공격	1. 원격접속 공격의 동작원리 및 특징 (Trojan, Exploit 등) 2. 원격접속 공격의 대응 방법

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
		3. 대응기술 및 응용	1. 보안 프로토콜 이해	1. 보안 프로토콜별 동작원리 및 특징(SSL, IPSec 등) 2. 보안 프로토콜 응용 사례
			2. 보안 솔루션 이해	1. 보안 솔루션의 종류별 동작원리 및 특징 (Firewall, IDS, IPS, VPN, ESM, UTM, NAC, 역추적시스템 등) 2. 보안 솔루션의 활용(Snort, 탐지툴, Pcap 등) 3. 로그 분석 이해 및 응용 4. 패킷 분석 이해 및 응용
어플리케이션 보안	20문	1. 인터넷 응용 보안	1. FTP 보안	1. FTP 개념 2. FTP 서비스 운영 3. FTP 공격 유형 4. FTP 보안방안
			2. 메일 보안	1. 메일 개념 2. 메일 서비스 운영 3. 메일 서비스 공격유형(스팸 메일, 악성 메일, 웜 등) 과 대책 4. 메일 보안 기술
			3. 웹 보안	1. 웹 개념 2. 웹 서비스 운영 3. 웹 서비스 장애 분석 및 대응 4. 웹 서비스공격 유형 5. 웹 보안 기술
			4. DNS 보안	1. DNS 개념 2. DNS 서비스 운영 3. DNS 공격유형 4. DNS 보안 기술
			5. DB 보안	1. DB 보안 개념 2. DB 공격 유형 3. DB 보안 기술
		2. 전자 상거래 보안	1. 전자상거래 보안 기술	1. 전자지불 수단별 보안요소 2. 전자상거래 보안 프로토콜 3. 전자상거래 인증기술 4. 무선플랫폼에서의 전자상거래 보안

필 기 과목명	출 제 문제수	주요항목	세부항목 (출제기준)	세세항목
정보보안 일반	20문	1. 보안요소 기술	1. 인증	1. 사용자 인증 방식 및 원리 2. 메시지에 대한 인증 방식 및 핵심 기술 3. 디바이스에 대한 인증 기술의 원리
			2. 접근통제	1. 접근통제 정책의 이해 및 구성 요소 2. 접근통제 정책의 특징 및 적용 범위 (임의적, 강제적, 역할 기반 등) 3. 접근통제 기법과 각 모델의 특징
			3. 키 분배 프로토콜	1. 대칭 키 기반 분배 방식의 원리 및 운영 2. 공개 키 기반 분배 방식의 원리 (Diffie-Hellman, RSA, ECC 등)
			4. 전자서명	1. 전자인증서 구조 및 주요 특징 2. 전자서명의 이해 (종류, 보안 요구조건, 특징, 서명 방식 등) 3. PKI 구성방식 및 관리(계층구조, 네트워크 구조, 복합형 구조 등) 4. CRL 사용 목적 및 구조 5. 전자서명을 이용한 최신 응용프로그램의 특징 및 이해
		2. 암호학	1. 암호 알고리즘	1. 암호 관련 용어 및 암호 시스템의 구성 2. 암호 공격의 유형별 특징 3. 대칭키 암호시스템 특징 및 활용 (종류, 구조, 운영 모드, 공격 기술 등) 4. 공개키 암호시스템의 특징 및 활용 (종류, 구조, 특징) 5. 암호 알고리즘을 이용한 최신 응용 기술
			2. 해시함수	1. 해시함수의 개요 및 요구사항 2. 해시함수별 특징 및 구조 3. 메시지 인증 코드(MAC)의 원리 및 구조
		3. 정보보호 및 개인정보보호 이해	1. 정보보호 및 개인정보보호 특성 이해	1. 정보보호 및 개인정보보호의 목적과 특징
			2. 정보보호 및 개인정보보호법 체계	1. 사이버 윤리(보안윤리 개념, 디지털 저작권 침해 및 보호기술, 유해정보유통, 사이버 폭력, 사이버 사기 등 범죄행위) 2. 정보보호 및 개인정보보호 법 체계의 이해

출제기준(실기)

직무 분야	정보통신	중직무 분야	정보기술	자격종목	정보보안산업기사	적용 기간	2019. 1. 1. ~ 2022.12.31.

○직무내용 : 보안에 관련한 시스템과 응용 서버, 네트워크 장비 및 보안장비에 대한 전문지식과 운용기술을 갖추고 시스템/네트워크/어플리케이션 분야별 기초 보안업무를 수행

○수행준거 : 1. 보안정책 운영을 위해 운영체제별, 프로토콜별, 서비스별, 보안장비 및 네트워크 장비별 보안 특성을 파악하고 설정 및 점검 등을 수행할 수 있다.
2. 운영체제, 서비스, 보안장비 및 네트워크 장비 등의 취약점 점검을 통해 원인파악, 보완 및 이력사항을 관리할 수 있다.
3. 시스템 로그 및 패킷 로그를 분석하여 침입 원인을 파악하고 보완할 수 있다.

실기 검정방법	필답형	시험시간	2시간30분

실 기 과목명	주요 항목	세부 항목	세세항목
정보보안실무	1. 시스템 및 네트워크 보안특성 파악	1. 운영체제별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도를 파악할 수 있다. 2. IT환경을 구성하고 있는 개인용 PC 또는 서버에 설치된 운영체제 및 버전정보를 파악할 수 있다. 3. 운영체제 및 버전별로 제공되는 보안서비스, 보안정책 설정, 보안 취약점들을 파악할 수 있다. 4. 내부 사용자와 네트워크 사용자에게 공유되는 객체들의 정보를 수집하고 보안목표에 따라 보안정책이 적절히 설정되었는지 점검할 수 있다. 5. 운영체제별로 동작하는 악성코드의 종류 및 특징을 파악할 수 있다. 6. 운영체제에서 생성되는 로그파일 관리가 되고 있는지 점검할 수 있다. 7. 보안 운영체제(SecureOS)가 제공하는 보안서비스를 이해하고, 접근 통제정책 등을 적용할 수 있다.
		2. 프로토콜별 보안특성 파악하기	1. OSI 7계층과 TCP/IP 프로토콜의 구성 그리고 각 계층별 기능, 동작 구조를 이해할 수 있다. 2. TCP/IP 각 계층에서 처리하는 PDU 구조 및 PDU 헤더별 필드 기능을 이해할 수 있다. 3. IP, ARP, RARP, ICMP 그리고 각 Routing 프로토콜 동작절차 및 취약점을 이해할 수 있다. 4. TCP, UDP, SSL, IPSec 프로토콜의 동작절차와 취약점을 이해할 수 있다. 5. 서비스 거부 공격 및 DDoS, DRDoS 공격 절차를 이해할 수 있다. 6. 무선 프로토콜 동작 구조 및 보안 취약점을 이해할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
		3. 서비스별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 파악할 수 있다. 2. FTP 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 3. 메일 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 4. 웹 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 5. DNS 서비스 동작절차와 환경 설정, 보안 취약점을 이해할 수 있다. 6. DB 서비스와 환경 설정, 보안 취약점을 이해할 수 있다. 7. 전자서명, 공개키 기반 구조 구성과 보안 특성을 이해할 수 있다.
		4. 보안장비 및 네트워크 장비별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 파악할 수 있다. 2. NIC, Hub, Switch, Bridge 장비의 역할과 동작을 이해할 수 있다. 3. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다. 4. Router 설정 절차 및 트래픽 통제 기능을 이해할 수 있다. 5. Firewall, IDS, IPS 보안 장비의 보안 서비스 및 설정 방법을 이해할 수 있다. 6. NAT 종류 및 동작 절차를 이해할 수 있다. 7. VPN 구현 방법 및 동작 절차를 이해할 수 있다. 8. 조직의 보안대상 관리시스템과 네트워크 장비를 파악할 수 있다. 9. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 등의 네트워크 정보를 파악할 수 있다. 10. SNMP를 이용한 원격관리기능과 스캐닝 도구를 이용한 관리대상시스템의 제공 서비스를 파악할 수 있다.
	2. 취약점 점검 및 보완	1. 운영체제 및 버전별 취약점 점검, 보완하기	1. 불필요한 계정 존재 및 악성코드 설치여부에 대하여 점검·보완할 수 있다. 2. 운영체제별 보호 대상 객체(파일, 폴더) 권한 설정이 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다. 3. 운영체제별 이벤트 로그정보 생성과 관리가 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다. 4. 운영체제 종류 및 버전 정보가 불필요하게 노출되어 있는지 점검.보완할 수 있다. 5. 원격접속 및 원격관리 기능이 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
			6. 운영체제의 패치관리 또는 패치관리 시스템이 적절히 설정되어 있는지 점검·보완할 수 있다. 7. 보안운영체제(SecureOS)를 적절히 설정하고 운영할 수 있다.
		2. 서비스 버전별 취약점 점검, 보완하기	1. 조직에서 제공하지 않는 서비스가 동작하고 있는지 점검한 후 제거 할 수 있다. 2. 파일서버, FTP서버에 권한이 없는 사용자가 접근할 수 있게 설정되어 있는지, 각 사용자별로 접근할 수 있는 파일/폴더가 적절히 설정되어 있는지 점검할 수 있다. 3. 공유폴더에 적절한 접근통제가 보안목표에 적합한지 점검하며, 폴더가 불필요하게 공유되어 있는지 점검·보완할 수 있다. 4. 메일 서버 설정에서 스팸메일 릴레이가 허용되어 있는지, 메일 송수신 프로토콜(SMTP, POP, IMAP) 보안 설정이 적절한지 점검할 수 있다. 5. 웹 서버 설정에서 다양한 공격 유형들에 대비하여 보안 설정이 적절한지 점검할 수 있다. 6. DNS 서버 설정에서 불필요한 명령어 수행이 허가되어 있지 않은지, DNS 보안 조치가 적절히 설정되어 있는지 점검할 수 있다. 7. DB 서버 설정에서 중요 정보가 암호화되어 저장되고 있는지, DB객체(테이블, 칼럼, 뷰 등)별 접근통제가 적절히 설정되어 있는지 점검할 수 있다.
		3. 보안장비 및 네트워크 장비 취약점 점검, 보완하기	1. Switch, Router 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다. 2. 침입차단시스템(Firewall) 장비 및 Router의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 3. 침입탐지시스템(IDS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 4. 침입방지시스템(IPS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 5. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 6. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다. 7. WAF 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 8. AntiDDoS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.

실 기 과목명	주요 항목	세부 항목	세세항목
			9. AntiAPT 또는 Sandbox 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
		4. 취약점 점검 및 보완 사항 이력 관리하기	1. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 2. 조직에서 사용중인 주요 서비스에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 3. 네트워크 장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완사항을 기록할 수 있다. 4. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안 취약점 및 보완사항을 기록할 수 있다.
	3. 관제 및 대응	1. 관제하기	1. 조직의 보안목표에 따라 운영체제 및 버전별, 서비스별(FTP, 메일, WWW, DNS, DB 등) 보안 등 생성되는 로그 정보를 파악하고 로그 내용을 모니터링 및 통제할 수 있다. 2. 주요 보안장비(Firewall, IDS, IPS 등), 네트워크 장비(Switch, Router, 무선접속AP 등) 등에서 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성 수준, 구성요소 등을 설정 할 수 있다. 3. 최신 공격 및 대응기술에 대해 이해하고 모니터링 및 통제할 수 있다.
		2. 대응하기	1. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별, 시간대별로 보안 로그정보를 수집 및 식별할 수 있다. 2. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 비정상 접근 및 변경 여부를 확인할 수 있다. 3. 업무 연속성을 위한 정보 및 보안 설정 정보를 백업 및 복구할 수 있다. 4. 최신 공격 및 대응기술에 대해 이해하고, 기본적인 초기대응을 할 수 있다.