출제기준(필기)

직무 분야	정보통신	중직무 분야	정보기술	자격 종목	정보보안산업기사	적용 기간	2013. 1. 1 ~ 2016. 12. 31

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

필기검정방법	객관식	문제수	80	시험시간	총 2시간

필기과목명	문제수	주요항목	세부항목	세세항목
시스템 보안	20문	1. 운영체제	1. 운영체제 개요	1. 운영체제의 주요기능 2. 운영체제의 구조 3. 운영체제의 기술발전 흐름
			2. 운영체제의 주요 구성 기술	1. 프로세스 관리 2. 기억장치 관리 3. 파일 시스템 관리 4. 분산 시스템
			3. 운영체제 사례별 특징과 주요 기능	1. 유닉스 2. 윈도우 3. 리눅스 4. 보안운영체제 특징
		2. 클라이언트 보안	1. 윈도우 보안	1. 설치 및 관리 2. 공유자료 관리 3. 바이러스와 백신
			2. 인터넷 활용 보안	1. 웹브라우저 보안 2. 메일 클라이언트 보안
			3. 공개 해킹도구에 대한 이해와 대응	1. 트로이목마 S/W 2. 크래킹 S/W 3. 키로그 S/W
			4. 도구활용 보안관리	1. 클라이언트용 보안도구 활용
		3. 서버보안	1. 인증과 접근통제	1. 계정과 패스워드 보호 2. 파일 시스템 보호 3. 시스템 파일 설정과 관리 4. 시스템 접근통제 기술
			2. 서버보안용 S/W 설치 및 운영	1. 시스템 취약점 점검 도구 2. 시스템 침입 탐지 시스템 3. 무결성 점검 도구

필기과목명	문제수	주요항목	세부항목	세세항목
네트워크 보안	20문	1. 네트워크 일반	1. OSI 7 layer	1. 각 레이어의 기능 및 역할 2. 레이어별 네트워크장비
			2. TCP / IP 일반	1. IPv4, IPv6 Addressing 2. 서브네팅 설계 및 활용 3. CIDR, LSM 4. 데이터 캡슐화 5. 포트주소 의미와 할당 원칙 6. IP, ARP, IGMP, ICMP, UDP, TCP등 각 프로토콜의 원리 및 이해 7. Broadcast 및 Multicast 이해
			3. Unix / Windows 네트워크 서비스	1. DNS, DHCP, SNMP, Telnet, FTP, SMTP 등 각종 서비스의 원리 및 이해 2. Workgroup 과 DOMAIN 3. 터미널서비스 등 각종 원격관리 서비스 4. 인터넷공유 및 NAT 원리, 활용
		2. 네트워크 활용	1. IP Routing	1. IP Routing
			2. 네트워크장비 이해	1. 랜카드, 허브, 스위치 및 브리지 2. 라우터 설정 명령어의 이해
			3. 네트워크기반 프로그램 활용	1. Ping, Traceroute 등 네트워크기반 프로그램의 활용 2. Netstat, Tcpdump등 활용
		3. 네트워크 기반 공격 이해	1. 서비스 거부(Dos) 공격	1. 각종 DoS 공격원리와 대처방법 2. SYN flooding, smurfing 등 각종 flooding 공격의 원리, 대처
			2. 분산서비스 거부 공격	1. DDoS 공격 원리 및 대처방법
			3. 네트워크 스캐닝	1. Remote finger printing 2. IP 스캔, 포트스캔
			4. IP spoofing, Session hijacking	1. IP spoofing 과 Session hijacking의 원리 및 실제
			5. 스니핑 및 암호화 프로토콜	1. 스니핑 공격 원리와 대처방법
			6. 원격접속 및 공격	1. 각종 공격의 인지 및 이해 2. Trojan, Exploit 등 식별, 대처

필기과목명	문제수	주요항목	세부항목	세세항목
		4. 네트워크 장비 활용 보안기술	1. 침입탐지시스템(IDS)의 이해	1. 원리, 종류, 작동방식, 특징, 단점 2. False Positive/Negative 이해
			2. 침입 차단시스템(Firewall)의 이해	1. 원리, 종류, 작동방식, 특징, 단점
			3. 라우터보안 설정	1. 라우터 자체 보안설정

필기과목명	문제수	주요항목	세부항목	세세항목
어플리케이션 보안	20문	1. 인터넷 응용 보안	1. FTP 보안	1. FTP 개념 2. FTP 서비스운영 3. FTP 공격유형 4. FTP 보안대책
			2. MAIL 보안	1. MAIL 개념 2. MAIL 서비스운영 3. MAIL 서비스공격유형
			3. Web 보안	1. WEB 개념 2. WEB 서비스운영 3. WEB 로그보안
			4. DNS 보안	1. DNS 개념 2. DNS 서비스운영 3. DNS 보안취약성
			5. DB 보안	1. DB 데이터보안 2. DB 관리자 권한보안 3. DBMS 운영보안
		2. 전자상거래 보안	1. 전자상거래 보안	1. 지불게이트웨이 2. SET 프로토콜 3. SSL 프로토콜 4. OTP
			2. 전자상거래 프로토콜	1. 전자지불 방식별 특징 2. 전자지불/화폐 프로토콜 3. 전자입찰 프로토콜 4. 전자투표 프로토콜

필기과목명	문제수	주요항목	세부항목	세세항목
정보보호 일반	20문	1. 보안요소 기술	1. 인증기술	1. 사용자 인증기술
				2. 메시지출처 인증기술
				3. 디바이스 인증기술
			2. 접근통제정책	1. 접근통제정책 구성요소
				2. 임의적 접근통제정책
				3. 강제적 접근통제정책
				4. 역할기반 접근통제정책
				5. 접근통제행렬과 AC
			3. 키분배 프로토콜	1. KDC 기반 키 분배
				2. Diffie-Hellman 프로토콜
				3. RSA 이용 키분배방법
			4. 전자서명과 공개키 기반 구조(PKI)	1. 전자인증서 구조
				2. 전자서명 보안서비스
				3. PKI 구성방식(계층, 네트워크)
				4. 전자서명 관련법규
		2. 암호학	1. 암호 알고리즘	1. 암호 관련용어
				2. 암호 공격방식
				3. 대칭키, 공개키 암호시스템 특징
				4. 대칭키, 공개키 암호시스템 활용
				5. 스트림암호
				6. 블록암호
				7. 블록암호 공격
				8. 인수분해 기반 공개키 암호 방식
			2. 해쉬함수와 응용	1. 해쉬함수 일반
				2. 전용 해쉬함수별 특징
				3. 메시지 인증 코드(MAC)
				4. 전자서명

출제기준(실기)

직무분야	정보통신	중직무분야	정보기술	자격종목	정보보안산업기사	적용기간	2013. 1. 1 ~ 2016. 12. 31

○ 직무내용 : 시스템과 응용 서버, 네트워크 장비 및 보안장비에 대한 전문지식과 운용기술을 갖추고 네트워크/어플리케이션 분야별 보안업무 분야의 기초적인 업무 수행

○ 수행준거 : 1. 운영체제, 네트워크 장비 및 보안장비의 보안관련 명령을 활용할 수 있다.
2. 보안요소기술들을 활용한 보안제품 및 솔루션 동작원리를 파악할 수 있다.
3. 보안정책 집행을 위해 운영체제, 네트워크 장비, 보안장비를 설정할 수 있다.
4. 시스템 로그 및 패킷 로그를 분석하여 침입상황을 식별할 수 있다.
5. 해킹 기술과 정보보호 대응기술에 대한 최신 경향을 파악할 수 있다.

실기검정방법	필답형	시험시간	2시간30분

실기과목명	주요항목	세부항목	세세항목
정보보안 실무	1. 시스템 및 네트워크 보안특성 파악	1. 운영체제별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 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. 운영체제별로 동작하는 악성코드의 종류 및 특징을 파악할 수 있다. 7. 운영체제에서 생성되는 로그 파일 관리가 적절히 설정되어 있는지 점검할 수 있다. 8. 보안 운영체제가 제공하는 보안서비스 ACL 강제적 접근 통제정책 설정방법을 파악할 수 있다.
		2. 프로토콜 특징 및 취약점 파악하기	1. OSI 7계층 및 TCP/IP 프로토콜 구성, 각 계층별 기능, 동작구조를 이해할 수 있다. 2. TCP/IP 각 계층에서 처리하는 PDU 구조 및 PDU 헤더별 필드 기능을 이해할 수 있다 3. ARP, RARP 프로토콜 동작절차와 취약점을 이해할 수 있다.

실기과목명	주요항목	세부항목	세세항목
			4. IP, ICMP, IGMP 및 각 Routing 프로토콜 동작절차 및 취약점을 이해할 수 있다. 5. TCP, UDP, SSL, IPSec 프로토콜의 동작절차와 취약점을 이해할 수 있다. 6. 서비스 거부 공격 및 DDos, DRDoS 공격 절차를 이해할 수 있다. 7. 무선 프로토콜 동작 구조 및 보안 취약점을 이해할 수 있다.
		3. 서비스별 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. FTP 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 3. MAIL 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 4. 웹 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 5. DNS 서비스 동작절차, 환경 설정 및 보안 취약점을 이해할 수 있다. 6. DB 보안 서비스, 환경 설정 및 보안 취약점을 이해할 수 있다. 7. 전자서명, 공개키 기반 구조 구성 및 보안 특성을 이해할 수 있다.
		4. 보안장비 및 네트워크 장비 보안특성 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. NIC, 허브, 스위치, 브리지 장비의 동작 절차를 이해할 수 있다. 3. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다. 4. 라우터 설정 절차 및 트래픽 통제 기능을 이해할 수 있다. 5. F/W, 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.
		5. 관리대상 시스템 및 네트워크 구조 파악하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 조직의 보안대상 관리시스템과 네트워크 장비를 파악할 수 있다. 3. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 정보를 파악할 수 있다.

실기과목명	주요항목	세부항목	세세항목
			4. SNMP를 이용한 원격관리기능 또는 스캐닝 도구를 이용하여 관리대상 시스템이 제공하는 서비스를 파악할 수 있다.
	2. 취약점 점검 및 보완	1. 운영체제 및 버전별 취약점 점검, 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 운영체제별 보안관리 매뉴얼이나 해당 운영체제 제조사 사이트를 게시된 보안 관리방법과 보안 취약점 정보를 수집할 수 있다. 3. 불필요한 계정이 존재하는지, 악성 코드가 설치되어 있는지 점검·보완할 수 있다. 4. 공유 폴더에 적절한 접근통제가 보안 목표에 적합한지 점검하며, 폴더가 불필요하게 공유되어 있지 않는지 점검·보완할 수 있다. 5. 운영체제별 보호 대상 객체(파일, 디렉터리) 권한 설정이 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다. 6. 운영체제별 이벤트 로그정보 생성과 관리가 보안목표에 따라 설정되어 있는지 점검·보완할 수 있다. 7. 운영체제 종류 및 버전 정보가 불필요하게 노출되어 있지 않은지 점검·보완할 수 있다. 8. 원격접속 및 원격관리 기능이 보안 목표에 따라 설정되어 있는지 점검·보완 할 수 있다.
		2. 서비스 및 버전별 취약점 점검, 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다 2. 조직에서 제공하지 않는 서비스가 동작하고 있는지 점검한 후 제거할 수 있다. 3. 파일서버, FTP 서버에 권한이 없는 사용자가 접근할 수 있게 설정되어 있는지, 각 사용자별로 접근할 수 있는 파일/ 디렉터리가 적절히 설정되어 있는지 점검할 수 있다. 4. 메일 서버 설정에서 스팸 메일 릴레이가 허용되어 있는지, 메일 송수신 프로토콜(SMTP, POP, IMAP) 보안 설정이 적절한지 점검할 수 있다.

실기과목명	주요항목	세부항목	세세항목
			5. 웹 서버 설정에서 다양한 공격 유형들(XSS, SQL Injection, 관리자 접근권한설정 등)과 관리자 접근권한 공격으로부터 적절히 보호되고 있는지 점검할 수 있다. 6. DNS 서버 설정에서 불필요한 명령어 수행이 허가되어 있지 않은지, DNS 보안조치(DNSSEC 등)가 적절히 설정되어 있는지 점검할 수 있다. 7. DB 서버 설정에서 중요 정보가 암호화되어 저장되고 있는지, DB 객체(테이블, 칼럼, 뷰 등)별 접근통제가 적절히 설정되어 있는지 점검할 수 있다.
		3. 보안장비 및 네트워크 장비 취약점 점검 보완하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 스위치, 라우터 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다. 3. F/W 장비 및 라우터의 보안 설정(IP별 통제, Port별 통제, 사용자 ID 별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 4. IDS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 5. IPS 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 6. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다. 7. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다.
		4. 취약점 점검 및 보완사항 이력관리하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 3. 조직에서 사용 중인 주요 서비스에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 4. 유·무선 네트워크 장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다. 5. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다.

실기과목명	주요항목	세부항목	세세항목
	3. 관제 및 대응	1. 운영체제별 로그정보 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 운영체제 및 버전별로 생성되는 로그정보 저장위치를 파악하고 로그 내용을 분석할 수 있다. 3. 운영체제에서 제공되는 로그정보 관리도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다. 4. 조직의 보안목표에 따라 운영체제별 로그정보가 적절히 생성되며 관리되고 있는지 점검할 수 있다.
		2. 서비스별 로그정보 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도를 수집할 수 있다. 2. 주요 서비스(FTP, MAIL, WWW, DNS, 보완 DB 등) 및 버전별로 생성되는 로그정보 저장위치를 파악하고 로그 내용을 분석할 수 있다. 3. 주요 서비스별로 제공되는 로그정보 관리도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다. 4. 조직의 보안목표에 따라 주요 서비스별 로그정보가 적절히 생성되며 관리되고 있는지 점검할 수 있다.
		3. 보안장비 및 네트워크 장비 로그정보 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 유·무선 네트워크 장비(스위치, 라우터, 무선접속 AP 등)별로 생성되는 로그정보 저장위치를 파악하고 로그내용을 분석할 수 있다. 3. 주요 보안장비(F/W, IDS, IPS) 별로 생성되는 로그정보 저장위치를 파악하고 로그 내용을 분석할 수 있다. 4. 유·무선 네트워크 장비별로 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다. 5. 주요 보안장비별로 제공되는 로그정보 관리 도구를 이용하여 로그정보의 생성수준, 로그정보 구성요소, 로그정보 저장위치 및 저장공간 등을 설정할 수 있다.

실기과목명	주요항목	세부항목	세세항목
			6. 조직의 보안목표에 따라 네트워크 장비/ 보안장비별 로그정보가 적절히 생성되며 관리되고 있는지 점검할 수 있다.
		4. 로그정보 통합 및 연관성 점검하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 보안로그 정보를 통합할 수 있다. 3. 시간대별로 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부를 점검할 수 있다. 4. IP 주소를 기준으로 통합 보안로그를 검색하여 내·외부 공격 시도 및 침투 여부를 점검 할 수 있다. 5. 통합 보안로그를 점검하여 관리자 계정의 불법 접근 및 변경 여부를 점검할 수 있다.
		5. 데이터 백업, 증거 수집 및 침입자 추적하기	1. 조직의 보안목표 문서와 IT환경 설계도, 네트워크 구성도를 수집할 수 있다. 2. 통합 보안로그 분석과정에서 침입 시도 또는 침입이 발견된 경우 침입 대상 시스템 및 장비의 주요 정보 및 보안 설정 정보를 백업할 수 있다. 3. 침입대상 시스템을 대상으로 삭제 또는 변경된 파일에 대한 복구 작업을 수행할 수 있다. 4. 침입자로 의심되는 사용자 및 발신지 IP를 이용하여 통합 보안로그에서 침입자의 침입경로를 추적할 수 있다.