정보보안산업기사 필기 출제기준

직무 분야	정보통신(21)- 정보기술(211)	자격 종목	정보보안산업기사	적용 기간	2023. 1. 1.~ 2026. 12. 31.
○직무내용 : 서버, 네트워크 장비, 응용S/W, 보안시스템 등에 대한 보안기술을 이해하고 활용하는 직무					
필기 검정방법	객관식	문제수	80	시험시간	2시간

과목명	문제수	주요항목	세부항목	세세항목
시스템 보안	20	1. 정보 시스템의 범위 및 이해	1. 단말 및 서버 시스템	1. 단말 시스템(PC, 모바일, 프린터, IoT/IIoT 등)
				2. 시스템 서버 (DB, DNS, E-mail, WEB/WAS, 파일서버, Cloud, 보안제품 등)
			2. 운영체제	1. 단말 운영체제 (Window, Linux, Android, iOS, Embeded OS 등)
				2. 서버 운영체제(Windows, Linux, Unix 등)
			3. 시스템 정보	1. 시스템 환경정보, 인증정보, 시스템/감사 로그
		2. 시스템 보안위협 및 공격기법	1. 시스템 보안위협	1. 보안설정, 권한설정, 내부자 위협 등 관리적 보안위협
				2. 보안취약점에 의한 도청, 정보 유출·변조, 비인가 접근 등 기술적 보안위협
			2. 시스템 공격기법	1. APT 공격, 알려진 취약점, 취약점 스캐너, SQL Injection, Buffer overflow 등 시스템 공격 기법 정의 및 특징
		3. 시스템 보안위협 및 공격에 대한 예방과 대응	1. 시스템 보안대응기술	1. 보안설정, 인증강화, 보안패치, 클라우드 보안 등 관리적 보안
				2. 시스템 파일 위·변조 방지, 유출방지, 접근통제, 접근제어, 로그분석, 이벤트 분석 등 기술적 보안
			2. 시스템 분석 도구	1. 시스템 보안취약점 분석 도구(Nmap, Kali Linux, etc. 등) 기능
				2. 시스템 보안취약점 분석 도구(Nmap, Kali Linux, etc. 등) 특징

네트워크 보안	20	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 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)
			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. 유무선 네트워크 서비스의 개요와 종류별 특징
				4. 네트워크 도구(ping, arp, rarp, traceroute, netstat, tcpdump 등)의 이해
		2. 네트워크 기반 공격 기술의 이해 및 대응	1. 서비스 거부(DoS), 분산 서비스 거부(DDoS) 공격	1. 서비스 거부(DoS) 공격 유형별 동작원리 및 특징
				2. 각종 서비스 거부(DoS) 공격에 대한 대응 방법
				3. 분산 서비스 거부(DDoS) 공격 유형별 동작 원리 및 특징
				4. 각종 분산 서비스 거부(DDoS) 공격에 대한 대응 방법
			2. 스캐닝	1. 포트 및 취약점 스캐닝의 동작원리와 특징
				2. 포트 및 취약점 스캐닝의 대응 방법
			3. 스푸핑 공격	1. 스푸핑 공격의 동작원리 및 특징 (Spoofing)

				2. 스푸핑 공격의 대응 방법
			4. 스니핑 공격	1. 스니핑 공격의 동작원리 및 특징 (Sniffing, Session Hijacking 등)
				2. 스니핑 공격의 대응 방법
		3. 네트워크 보안 기술	1. 보안 프로토콜 이해	1. 보안 프로토콜별 동작원리 및 특징
				2. 보안 프로토콜 응용 사례
			2. 네트워크 보안기술 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
				4. 패킷 분석 이해
				5. 역추적 이해
				6. 악성코드 분석 도구의 이해
어플리케이션보안	20	1. 인터넷 응용 보안	1. FTP 보안	1. FTP 개념
				2. FTP 서비스 운영
				3. FTP 공격 유형
				4. FTP 보안기술
			2. 메일 보안	1. 메일 개념
				2. 메일 서비스 운영
				3. 메일 서비스 공격유형(스팸 메일, 악성 메일, 웜 등)
				4. 메일 보안 기술
			3. Web/App 보안	1. Web/App 개념

				2. Web/App 운영
				3. Web/App 장애 분석
				4. Web/App 공격 유형
				5. Web/App 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. 어플리케이션 보안 취약점	1. 어플리케이션 보안 취약점 대응	1. 어플리케이션 보안취약점 유형
				2. 어플리케이션 보안 취약점 대응 기술
정보보안 일반	20	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
				2. 접근통제 정책의 특징

				3. 접근통제 기법
			3. 키 분배 프로토콜	1. 대칭 키 기반 분배 방식의 원리 및 운영
				2. 공개 키 기반 분배 방식의 원리
			4. 디지털서명	1. 인증서 구조 및 주요 특징
				2. 디지털서명의 이해 (종류, 보안 요구조건, 특징, 서명 방식 등)
				3. PKI 구성방식 및 관리(계층구조, 네트워크 구조, 복합형 구조, CRL, OCSP 등)
		2. 암호학	1. 암호 알고리즘	1. 암호 관련 용어 및 암호 시스템의 구성
				2. 암호 공격의 유형별 특징
				3. 대칭키 암호시스템 특징
				4. 공개키 암호시스템의 특징
			2. 해시함수	1. 해시함수의 개요 및 요구사항
				2. 해시함수별 특징 및 구조
				3. 메시지 인증 코드(MAC)의 원리 및 구조

정보보안산업기사 실기 출제기준

직무 분야	정보통신(21)- 정보기술(211)	자격 종목	정보보안산업기사	적용 기간	2023. 1. 1.~ 2026. 12. 31.

○ **직무내용 :** 서버, 네트워크 장비, 응용S/W, 보안시스템 등에 대한 보안기술을 이해하고 활용하는 직무

○ **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	2시간 30분

과목명	주요항목	세부항목	세세항목
정보보안 실무	1. 시스템 및 네트워크 보안특성 파악	1. 운영체제별 보안특성 파악하기	1. IT환경을 구성하고 있는 개인용 단말시스템 또는 서버에 설치된 운영체제 환경 및 특징을 파악할 수 있다.
			2. 서비스별 운영체제 및 버전을 파악할 수 있다.
			3. 운영체제별 식별 및 인증, 접근통제, 보안 업데이트 등 보안강화 방안을 파악할 수 있다.
			4. 운영체제에서 생성되는 로그파일관리가 되고 있는지 점검할 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/TLS, IPSec 프로토콜의 동작 절차와 취약점을 이해할 수 있다.
			5. 서비스 거부(DoS/DDoS 등) 공격 방식과 절차를 이해할 수 있다.
			6. 무선 프로토콜 동작 구조 및 보안 기법을 이해할 수있다.

		3. 서비스별 보안특성 파악하기	1. FTP 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다. 2. 메일 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다. 3. 웹 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다. 4. DNS 서비스 동작절차와 환경 설정, 보안 기법을 이해할 수 있다. 5. DB 서비스와 환경 설정, 보안 기법을 이해할 수 있다.
		4. 보안장비 및 네트워크 장비별 보안특성 파악하기	1. 조직의 보안대상 시스템과 네트워크 장비를 파악할 수 있다. 2. 네트워크 구성도를 분석하여 사용 중인 IP 주소, 서브넷 등의 네트워크 정보를 파악할 수 있다. 3. SNMP를 이용한 원격관리기능과 스캐닝 도구를 이용한 관리대상시스템의 제공 서비스를 파악할 수 있다. 4. 네트워크 장비의 역할과 동작을 이해할 수 있다. 5. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다. 6. Firewall, IPS/IDS, WAF, VPN 등 보안 장비별 특성과 설정 방법을 이해할 수 있다. 7. NAT 종류 및 동작 절차를 이해할 수 있다.
	2. 취약점 점검 및 보완	1. 운영체제 보안설정 점검과 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.
			6. 운영체제의 패치관리가 적절히 설정되어 있는지 점검·보완할 수 있다.
		2. 서비스 보안설정 점검과 보완하기	1. 비인가된 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. WEB/WAS 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. 네트워크 및 보안장비 설정 점검과 보완하기	1. 네트워크 장비의 관리자 계정 보안이 적절히 설정되어 있는지 점검할 수 있다.
			2. 침입차단시스템(Firewall) 장비의 보안 설정(IP별 통제, Port별 통제, 사용자 ID별 통제 등)이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			3. 침입탐지 및 방지 시스템(IDS/IPS) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
			4. NAT 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.

			5. 무선접속 장비가 보안목표에 따라 암호화 및 접근통제가 적절히 설정되어 있는지 확인할 수 있다.
			6. WAF 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.
		4. 취약점 점검이력과 보완 내용 관리하기	1. 운영체제별 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완 사항을 기록할 수 있다.
			2. 조직에서 사용 중인 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 보안취약점 및 보완사항을 기록할 수 있다.
			4. 보안장비에 대해 수행한 보안점검 내용과 방법(도구), 발견된 보안취약점 및 보완사항을 기록할 수 있다.
	3. 보안관제 및 대응	1. 정보수집 및 모니터링	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 로그 정보의 생성 수준, 구성요소 등을 설정 할 수 있다.
		2. 로그분석 및 대응	1. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별, 시간대별로 보안 로그정보를 이해할 수 있다.
			2. 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부 등 관련 정보를 수집 할 수 있다.
			3. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 비정상 접근과 변경 여부를 확인할 수 있다.
			4. 업무 연속성을 위한 정보 및 보안 설정 정보를 백업 및 복구를 할 수 있다.