정보보안기사 실기 출제기준

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

○ **직무내용** : 서버, 네트워크 장비, 응용S/W, 보안시스템 등에 대한 보안기술과 활용을 통해 보안서비스를 제공하는 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.
4. 조직의 정보자산을 식별하고 내·외부 위협요인을 분석·평가하여 적절한 정보보호대책 선정 및 이행계획을 수립할 수 있다.

실기 검정방법	필답형	시험시간	3시간

과목명	주요항목	세부항목	세세항목
정보보안 실무	1. 시스템 및 네트워크 보안 특성 파악	1. 운영체제별 보안특성 파악하기	1. IT환경을 구성하고 있는 개인용 단말 시스템 또는 서버에 설치된 운영체제 환경 및 특징을 파악할 수 있다.
			2. 서비스별 운영체제 및 버전을 파악할 수 있다.
			3. 운영체제별 식별 및 인증, 접근통제, 보안업데이트 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.

과목명	주요항목	세부항목	세세항목
			4. TCP, UDP, SSL/TLS, IPSec 프로토콜의 동작절차와 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.
			6. 전자서명, 공개키 기반 구조 구성과 보안 특성을 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.

과목명	주요항목	세부항목	세세항목
			5. VLAN 보안 서비스 및 설정 방법을 이해할 수 있다.
			6. Router 설정 절차 및 트래픽 통제 기능을 이해할 수 있다.
			7. Firewall, IPS/IDS, WAF, VPN 등 보안 장비별 특성과 설정 방법을 이해할 수 있다.
			8. NAT 종류 및 동작 절차를 이해할 수 있다.
	2. 취약점 점검 및 보완	1. 운영체제 보안설정 점검과 보완하기	1. 불필요한 계정 존재 및 악성코드 설치 여부에 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.

과목명	주요항목	세부항목	세세항목
			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.
			7. Anti-DDoS(DDOS 대응장비) 보안 설정이 보안목표에 따라 적절히 설정되어 있는지 점검할 수 있다.

과목명	주요항목	세부항목	세세항목
			8. Anti-APT(APT 대응솔루션) 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 로그정보의 생성 수준, 구성요소 등을 설정 할 수 있다.
		2. 로그분석 및 대응	1. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별, 시간대별로 보안 로그 정보를 통합·분석할 수 있다.
			2. 통합 보안로그를 정렬하여 내·외부 공격 시도 및 침투 여부 등 관련 정보를 수집 및 분석할 수 있다.
			3. 시스템별, 주요 서비스별, 유·무선 네트워크 장비별, 보안장비별 비정상 접근과 변경 여부를 확인 및 분석할 수 있다.

과목명	주요항목	세부항목	세세항목
			4. 업무 연속성을 위한 정보 및 보안 설정 정보를 백업 및 복구 등으로 대응할 수 있다.
	4. 위험분석 및 정보보호 대책 수립	1. IT 자산 위협 분석하기	1. 조직의 IT환경의 시스템 및 네트워크 구성도 등 정보자산 현황을 파악할 수 있다.
			2. IT환경을 구성하는 서버, 어플리케이션, DBMS, WEB/WAS, PC 등으로부터의 위협 요인을 식별할 수 있다.
			3. 조직의 네트워크를 구성하는 네트워크 장비, 보안 장비로부터의 위협요인을 식별할 수 있다.
			4. 정보보호 및 개인정보보호 관련 법적 준거성 위험을 식별할 수 있다.
		2. 조직의 정보자산 위협 및 취약점 분석 정리하기	1. 조직의 H/W자산(PC, 서버, 네트워크 및 보안장비)에 대한 중요도, 내·외부위협 및 취약점분석 내용을 정리할 수 있다.
			2. 조직의 S/W자산(운영체제, 상용 및 자가개발패키지)에 대한 중요도, 내외부 위협 및 취약점분석 내용을 정리할 수 있다.
			3. 조직의 정보자산(기업정보 및 고객정보)에 대한 중요도, 내·외부 위협 및 취약점 분석 내용을 정리할 수 있다.
		3. 위험평가하기	1. 식별된 위험을 기반으로 위험도를 산정할 수 있다.
			2. 조직에서 수용 가능한 목표 위험수준을 정하고 그 수준을 초과하는 위험을 식별할 수 있다.
		4. 정보보호대책 선정 및 이행계획 수립하기	1. 식별된 위험에 대한 처리 전략(위험감소, 위험회피, 위험전가, 위험수용 등)을 수립하고 위험처리를 위한 정보보호대책을 파악할 수 있다.
			2. 정보보호대책의 우선순위를 정한 후에 일정, 예산 등을 포함하여 정보보호 대책 이행계획을 수립할 수 있다.