[20v1]

정보보안산업기사

□ 교육 · 훈련목표

보안과 관련된 시스템과 응용 서버, 네트워크 장비 및 보안장비에 대한 전문지식과 운용기술을 갖추고 시스템, 네트워크, 애플리케이션 분야별 기초 보안업무를 실행할 수 있는 인력을 양성

□ 1차 시험

구 분	주 요 내 용	
시험방법 및 시험 시간	문제수 (40문제)	객관식 및 주관식 : 1시간 30분
문항수 및 시험문제 유형	객관식(30문항)	4지 택일형, 진위형(○/×), 연결형
	주관식(10문항)	단답형, 계산형
배점	100점(40%)	

□ 2차 시험

구 분	주 요 내 용			
시험방법	필답형 실기시험			
평가내용	필답형	· SW개발 보안 구축, 시스템 보안 구축, NW보안 구축, 네트워크 보안운영, 애플리케이션 보안운영, 시스템 보안 운영, 보안로그 분석 및 정보시스템을 진단할 수 있는 능력을 평가		
과제 및 시험시간	필답형(20문항)		1시간30분	1시간30분 (90분)
배점	필답형			계
	100점			100점(60%)

▣ 정보보안산업기사 외부평가문제 유형

□ 1차시험

진위형

1) 네트워크 장비 선정에 대한 다음 내용이 옳으면 ○표, 틀리면 ×표에 해당하는 번호를 선택하여 쓰시오. (　　)

> 다수의 네트워크 장비 관리자가 있을 때 관리자 계정별 접근 권한을 설정하는 기능을 제공하는 네트워크 장비를 선정하여야 한다.

① O　　② ×

2) 다음 SW개발 보안에 관한 설명이 옳으면 ○표, 틀리면 ×표에 해당하는 번호를 쓰시오. (　　)

> 소프트웨어 개발단계에서 해당 정보에 대해 적용되어야 하는 보안항목을 식별하는 작업이 우선적으로 수행되어야 한다.
> 기능에 대한 보안항목 식별은 입력데이터 검증 및 표현, 보안기능, 에러 처리, 세션통제 등으로 구분할 수 있다.

① O　　② ×

연결형

1) 다음의 각 공격 기법과 공격 대상을 올바르게 연결하시오.

① XSS	•	• ㉠ 데이터베이스 서버
② CSRF	•	• ㉡ 웹 클라이언트
③ SQL 인젝션	•	• ㉢ 웹 서버

2) 시스템 사용자가 로그인한 후 명령을 내리는 과정에 대한 동작은 Authentication, Authorization, Accounting으로 구분한다. 이를 Triple_A(AAA)라고 부르기도 한다. 각각의 요소와 설명을 올바르게 연결하시오.

① Authentication	•	• ㉠ 지문이나 패스워드 등을 통해 로그인이 허락된 사용자로 판명되어 로그인하는 과정이다. 즉 신원이 확인되어 인증받은 사람이 출입문에 들어가도록 허락하는 과정이다.
② Autorization	•	• ㉡ 자신의 신원을 시스템에 인증하는 과정으로, 아이디와 패스워드를 입력하는 과정이다.
③ Accounting	•	• ㉢ 로그인 이후 이용자의 행위에 대해 시스템이 이에 대한 기록을 남기는 활동이다. 즉 객체나 파일에 접근한 기록이다.

4지택일

1) 네트워크 장비에 관한 감사 데이터에 포함되어야 할 정보와 거리가 먼 것은? ( )

① 사건 발생 일시　② 사건 유형
③ 사건 대응 방안　④ 사건의 결과(성공 또는 실패)

2) 다음 Access_Log에 대한 분석이 잘못된 것은? ( )

192. 168. 137. 1 -- [06/JUN/2017:05:48:28 +0900] "GET/HTTP?1.1" 403 4609 "-"
"Mozilla/5.0(compitable; MSITE 9.0;Windos NT 6.1; WOW64; Trident/5.0)"

① 클라이언트 IP : 192.168.137.1
② HTTP 접근방법과 접근 URL : GET/HTTP/1.1
③ 실행코드 결과 : 4609
④ 클라이언트 웹브라우저 : Mozilla/5.0

단답형

1) 다음 설명에 해당하는 보안 솔루션을 가리키는 용어를 쓰시오.

내부망의 호스트(PC, 이동 단말 등)가 네트워크에 접근할 때 보안 정책에 따라 네트워크 접속을 통제하는 보안 솔루션

○

2) 다음은 정보시스템 진단에 있어 위험의 구성요소에 관한 설명이다. 해당하는 용어를 쓰시오.

자산의 잠재적 속성으로서 위협의 이용 대상으로 정의하며, 때로는 정보 보호 대책의 미비로 정의되기도 한다.

○

□ 2차 시험

과제수	과제명(작업명)	시험시간	비 고
제1과제	정보보안 운영 및 분석진단 등	1시간30분	·필답형
합 계		1시간30분 (90분)	

[제1과제 필답형]

다음 문제를 읽고 해당 답안을 보기에서 골라 쓰시오.

문제 1. 검증되지 않은 외부 입력 값에 의해 브라우저에서 악의적인 코드가 실행되는 보안약점은 무엇인지 쓰시오.

○

문제 2. SW를 실행하지 않고, 소스코드 보안약점을 분석하는 SW보안 테스트 종류는 무엇인지 쓰시오.

○

문제 3. 망 환경에서 사용자 간 또는 컴퓨터간의 대화를 위한 논리적 연결 혹은 컴퓨터의 프로세스들 사이에서 통신하기 위해 메시지를 교환하며 서로를 인식한 이후부터 통신을 마칠 때까지의 기간이 무엇인지 쓰시오.

○

문제 4. SunOS에서 루트(root) 계정의 원격 접속을 제한하는 파일은 무엇인지 경로를 포함하여 쓰시오.

○

문제 5. 스마트폰 문자 발송 메시지를 통해 악성 앱 설치를 유도하고 개인정보 혹은 금융정보를 탈취하는 침해 기법은 무엇인지 쓰시오.

○

문제 6. 시스템의 오용/악용으로부터 정보 시스템을 보호하기 위한 것으로써, 중요 내부 업무 처리를 수행하는 사용자의 PC나 노트북을 인터넷 접속이 되지 않도록 차단하는 기술은 무엇인지 쓰시오.

○

문제 7. OSI 7계층에서 통신에 사용할 프로토콜 타입을 결정하는 최상위 계층은 무엇인지 쓰시오.

○

문제 8. 목표물을 시스템 장애 상태로 만들어 다른 사람이 요청하는 서비스를 거부하도록 할 수 있는 네트워크 공격 유형은 무엇인지 쓰시오.

○

문제 9. 위험의 구성요소에 대한 설명이다. 괄호 안에 들어갈 단어는 무엇인지 모두 쓰시오.

위험(risk)은 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 말한다. 위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소와 그들이 어떻게 위험의 규모에 영향을 미치는지를 분석해야 한다. 위험을 구성 하는 요소는 ( ), ( ), ( ) 이다.

○

보기	1	CVE(Common Weakness Enumeration)	2	정적분석	3	동적분석
	4	크로스 사이트 스크립트(XSS)	5	세션(Session)	6	쿠키(Cookie)
	7	무작위 대입 공격(Brute Force Attack)	8	권한(Authority)	9	피싱(Pishing)
	10	FAR(False Acceptance Ratio)	11	망분리	12	사고 조사
	13	FRR(False Rejection Ratio)	14	위협(Threat)	15	정보규칙
	16	인증(Authentication)	17	위험 관리	18	사고 회피
	19	프리젠테이션 계층(Presentation Layer)	20	자산(Assert)	21	서비스 거부(DoS)
	22	애플리케이션 계층(Application Layer)	23	(^)	24	[^]
	25	정보보호 관리체계 인증(ISMS)	26	위험 회피	27	보안로그
	28	예방 대응(Prevention)	29	스미싱(Smishing)	30	SQL Injection
	31	취약성(Vulnerability)	32	/etc/securetty	33	기준선 접근법
	34	분산 서비스 거부(DDoS)	35	/etc/default/login	36	비정형 접근법
	37	크로스 사이트 요청위조(CSRF)	38	정보 보안 규정	39	XML Injection