***** 수험자 유의사항 *****

1. 시험 문제지를 받는 즉시 응시하고자 하는 종목의 문제지가 맞는지를 확인하여야 합니다.
2. 시험 문제지 총면수·문제번호 순서·인쇄상태 등을 확인하고, 수험번호 및 성명을 답안지에 기재하여야 합니다.
3. 문제 및 답안(지), 채점기준은 일절 공개하지 않으며 자신이 작성한 답안, 문제 내용 등을 수험표 등에 이기(옮겨 적는 행위) 등은 관련 법 등에 의거 불이익 조치 될 수 있으니 유의하시기 바랍니다.
4. 수험자 인적사항 및 답안작성(계산식 포함)은 흑색 필기구만 사용하여야 하며 흑색을 제외한 유색 필기구 또는 연필류를 사용하였을 경우 그 문항은 0점 처리됩니다.
5. 답란(답안 기재란)에는 문제와 관련 없는 불필요한 낙서나 특이한 기록사항 등을 기재하여서는 안되며 부정의 목적으로 특이한 표식을 하였다고 판단될 경우에는 모든 문항이 0점 처리됩니다.
6. 답안을 정정할 때에는 반드시 정정부분을 두 줄(=)로 그어 표시하여야 하며, 두 줄로 긋지 않은 답안은 정정하지 않은 것으로 간주합니다. (수정테이프, 수정액 사용불가)
7. 답안의 한글 또는 영문의 오탈자는 오답으로 처리됩니다. 단, 답안에서 영문의 대·소문자 구분, 띄어쓰기는 여부에 관계 없이 채점합니다.
8. 계산 또는 디버깅 등 계산 연습이 필요한 경우는 <문 제> 아래의 연습란을 사용하시기 바라며, 연습란은 채점대상이 아닙니다.
9. 문제에서 요구한 가지 수(항수) 이상을 답란에 표기한 경우에는 답안기재 순으로 요구한 가지 수(항수)만 채점하고 한 항에 여러 가지를 기재하더라도 한 가지로 보며 그 중 정답과 오답이 함께 기재란에 있을 경우 오답으로 처리됩니다.
10. 한 문제에서 소문제로 파생되는 문제나, 가지수를 요구하는 문제는 대부분의 경우 부분채점을 적용합니다. 그러나 소문제로 파생되는 문제 내에서의 부분 배점은 적용하지 않습니다.
11. 답안은 문제의 마지막에 있는 답란에 작성하여야 합니다.
12. 부정 또는 불공정한 방법(시험문제 내용과 관련된 메모지사용 등)으로 시험을 치른 자는 부정행위자로 처리되어 당해 시험을 중지 또는 무효로 하고, 2년간 국가기술자격검정의 응시자격이 정지됩니다.
13. 시험위원이 시험 중 신분확인을 위하여 신분증과 수험표를 요구할 경우 반드시 제시하여야 합니다.
14. 시험 중에는 통신기기 및 전자기기(휴대용 전화기 등)를 지참하거나 사용할 수 없습니다.
15. 국가기술자격 시험문제는 일부 또는 전부가 저작권법상 보호되는 저작물이고, 저작권자는 한국산업인력공단입니다. 문제의 일부 또는 전부를 무단 복제, 배포, 출판, 전자출판 하는 등 저작권을 침해하는 일체의 행위를 금합니다.

※ 수험자 유의사항 미준수로 인한 채점상의 불이익은 수험자 본인에게 전적으로 책임이 있음

실무와 거리가 있어 실기 교재에서 다루지 않고 필기 교재에서만 다뤘던 내용을 문제 형태로 제공해 드리는 자료입니다. 문제의 내용뿐만 아니라 [병행학습]으로 제공되는 내용까지 빠짐없이 모두 학습하세요.

문제 1 **표적이 되는 서버의 자원을 고갈시킬 목적으로 다수의 공격자 또는 시스템에서 대량의 데이터를 한 곳의 서버에 집중적으로 전송함으로써, 표적이 되는 서버의 정상적인 기능을 방해하는 공격 기법을 쓰시오.**

답 : 서비스 거부(DoS; Denial of Service) 공격

문제 2 **다음 설명에 해당하는 서비스 거부(DoS) 공격 기법을 한글 또는 영문(Fullname 또는 약어)으로 쓰시오.**

- Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위(65,536 바이트) 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법이다.
- 공격에 사용되는 큰 패킷은 수백 개의 패킷으로 분할되어 전송되는데, 공격 대상은 분할된 대량의 패킷을 수신함으로써 분할되어 전송된 패킷을 재조립해야 하는 부담과 분할되어 전송된 각각의 패킷들의 메시지에 대한 응답을 처리하느라 시스템이 다운되게 된다.`

답 : Ping of Death(죽음의 핑)

문제 3 **다음 설명에 해당하는 서비스 거부(DoS) 공격 기법을 한글 또는 영문(Fullname 또는 약어)으로 쓰시오.**

- IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법이다.
- 공격자는 송신 주소를 공격 대상지의 IP 주소로 위장하고 해당 네트워크 라우터의 브로드캐스트 주소를 수신지로 하여 패킷을 전송하면, 라우터의 브로드캐스트 주소로 수신된 패킷은 해당 네트워크 내의 모든 컴퓨터로 전송된다.
- 해당 네트워크 내의 모든 컴퓨터는 수신된 패킷에 대한 응답 메시지를 송신 주소인 공격 대상지로 집중적으로 전송하게 되는데, 이로 인해 공격 대상지는 네트워크 과부하로 인해 정상적인 서비스를 수행할 수 없게 된다.

답 : SMURFING(스머핑)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 4 공격자가 가상의 클라이언트로 위장하여 TCP가 신뢰성 있는 전송을 위해 사용하는 3-wayhandshake 과정을 의도적으로 중단시킴으로써 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 서비스 거부(DoS) 공격 기법을 영문(Fullname 또는 약어)으로 쓰시오.

답 : SYN Flooding

문제 5 데이터의 송·수신 과정에서 패킷의 크기가 커 여러 개로 분할되어 전송될 때 분할 순서를 저장하는 Fragment Offset 값을 변경시켜 수신 측에서 패킷을 재조립할 때 오류로 인한 과부하를 발생시킴으로써 시스템이 다운되도록 하는 서비스 거부(DoS) 공격 기법을 영문(Fullname 또는 약어)으로 쓰시오.

답 : TearDrop

문제 6 패킷을 전송할 때 송신 IP 주소와 수신 IP 주소를 모두 공격 대상의 IP 주소로 하여 공격 대상에게 전송함으로써 이 패킷을 받은 공격 대상은 송신 IP 주소가 자신이므로 자신에게 응답을 수행하게 되는데, 이러한 패킷이 계속해서 전송될 경우 자신에 대해 무한히 응답하게 하는 서비스 거부(DoS) 공격 기법을 영문(Fullname 또는 약어)으로 쓰시오.

답 : Land

문제 7 서비스 거부(DoS) 공격 기법에 대한 다음 설명에 해당하는 용어를 한글 또는 영문(Fullname 또는 약어)으로 쓰시오.

- 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 서비스 거부 공격(DoS)을 수행하는 것으로, 네트워크에서 취약점이 있는 호스트들을 탐색한 후 이들 호스트들에 공격용 툴을 설치하여 에이전트(Agent)로 만든 후 공격에 이용한다.
- 공격의 범위를 확대하기 위해 일부 호스트에 다수의 에이전트를 관리할 수 있는 핸들러(Handler) 프로그램을 설치하여 마스터(Master)로 지정한 후 공격에 이용하기도 한다.

답 : DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 8 **컴퓨터 보안에 있어서, 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 시스템 침입 수단을 가리키는 용어를 쓰시오.**

답 : 사회 공학(Social Engineering)

문제 9 **다음은 네트워크 침해 공격 기법의 종류에 대한 설명이다. 괄호(①~③)에 들어갈 알맞은 종류를 쓰시오.**

(①)	각종 행사 안내, 경품 안내 등의 문자 메시지(SMS)를 이용해 사용자의 개인 신용정보를 빼내는 공격 기법이다.
스피어 피싱 (Spear Phishing)	특정 대상을 선정한 후 그 대상에게 일반적인 이메일로 위장한 메일을 지속적으로 발송하여, 발송 메일의 본문 링크나 첨부된 파일을 클릭하도록 유도해 사용자의 개인 정보를 탈취하는 공격 기법이다.
(②)	다양한 IT 기술과 방식들을 이용해 조직적으로 특정 기업이나 조직 네트워크에 침투해 활동 거점을 마련한 뒤 때를 기다리면서 보안을 무력화시키고 정보를 수집한 다음 외부로 빼돌리는 형태의 공격이다.
무작위 대입 공격 (Brute Force Attack)	암호화된 문서의 암호키를 찾아내기 위해 적용 가능한 모든 값을 대입하여 공격하는 방식이다.
큐싱(Qshing)	QR 코드를 통해 악성 앱의 다운로드를 유도하거나 악성 프로그램을 설치하도록 하는 금융사기 기법의 하나로, QR 코드와 개인정보 및 금융정보를 '낚는다(Fishing)'는 의미의 합성 신조어이다.
SQL 삽입(Injection) 공격	• 입력란에 SQL을 삽입하여 무단으로 DB를 조회하거나 조작하는 공격 기법이다. • 예를 들어 전문 스캐너 프로그램 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작한다.
(③)	• 웹페이지에 악의적인 스크립트를 삽입하여 방문자들의 정보를 탈취하거나, 비정상적인 기능 수행을 유발하는 공격 기법이다. • 사용자가 특정 게시물이나 이메일의 링크를 클릭하면 악성 스크립트가 실행되어 페이지가 깨지거나, 사용자의 컴퓨터에 있는 로그인 정보나 개인 정보, 내부 자료 등이 해커에게 전달된다.

답

- ① : 스미싱(Smishing)
- ② : APT(Advanced Persistent Threats,지능형 지속 위협)
- ③ : 크로스 사이트 스크립팅(XSS; Cross Site Scripting)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 10 다음은 정보 보안 침해 공격과 관련된 용어에 대한 설명이다. 괄호(①~③)에 들어갈 알맞은 용어를 한글 또는 영문(Fullname 또는 약어)으로 쓰시오.

좀비(Zombie) PC	악성코드에 감염되어 다른 프로그램이나 컴퓨터를 조종하도록 만들어진 컴퓨터로, C&C(Command & Control) 서버의 제어를 받아 주로 DDoS 공격 등에 이용된다.
C&C 서버	해커가 원격지에서 감염된 좀비 PC에 명령을 내리고 악성코드를 제어하기 위한 용도로 사용하는 서버를 말한다.
봇넷(Botnet)	악성 프로그램에 감염되어 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 말한다.
(①)	• 네트워크를 통해 연속적으로 자신을 복제하여 시스템의 부하를 높임으로써 결국 시스템을 다운시키는 바이러스의 일종이다. • 대표적으로 분산 서비스 거부 공격, 버퍼 오버플로 공격, 슬래머 등이 있다.
제로 데이 공격 (Zero Day Attack)	보안 취약점이 발견되었을 때 발견된 취약점의 존재 자체가 널리 공표되기도 전에 해당 취약점을 통하여 이루어지는 보안 공격으로, 공격의 신속성을 의미한다.
키로거 공격 (Key Logger Attack)	컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드, 계좌번호, 카드번호 등과 같은 개인의 중요한 정보를 몰래 빼가는 해킹 공격이다.
(②)	인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 파일 등을 암호화해 사용자가 열지 못하게 하는 프로그램으로, 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 한다.
(③)	• 시스템 설계자가 서비스 기술자나 유지 보수 프로그램 작성자(Programmer)의 액세스 편의를 위해 시스템 보안을 제거하여 만들어놓은 비밀 통로로, 컴퓨터 범죄에 악용되기도 한다. • 탐지 방법 : 무결성 검사, 로그 분석, SetUID 파일 검사
트로이 목마 (Trojan Horse)	정상적인 기능을 하는 프로그램으로 위장하여 프로그램 내에 숨어 있다가 해당 프로그램이 동작할 때 활성화되어 부작용을 일으키는 것으로, 자기 복제 능력은 없다.

답

- ① : 웜(Worm)
- ② : 랜섬웨어(Ransomware)
- ③ : 백도어(Back Door) 또는 트랩도어(Trap Door)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 11 데이터를 송·수신하는 두 컴퓨터 사이, 종단 간, 즉 TCP/IP 계층과 애플리케이션 계층(HTTP, TELNET, FTP 등) 사이에 위치하여 인증, 암호화, 무결성을 보장하는 업계 표준 프로토콜을 영문(Fullname 또는 약어)으로 쓰시오.

답 : SSL(Secure Socket Layer)

문제 12 정부의 '개인정보의 기술적·관리적 보호조치 기준'에 따라 SSL 인증서 또는 암호화 응용 프로그램을 설치하여 전송 정보를 암호화하여 송·수신 하는 서버를 가리키는 용어를 쓰시오.

답 : 보안 서버

문제 13 다음은 인증(Authentication)에 대한 설명이다. 괄호(①, ②)에 들어갈 알맞은 용어를 쓰시오.

- 인증은 다중 사용자 컴퓨터 시스템이나 네트워크 시스템에서 로그인을 요청한 사용자의 정보를 확인하고 접근 권한을 검증하는 보안 절차이다.
- 인증에는 네트워크를 통해 컴퓨터에 접속하는 사용자의 등록 여부를 확인하는 것과 전송된 메시지의 위·변조 여부를 확인하는 것이 있다.
- 인증의 주요 유형은 다음과 같다.

(①)	• 사용자가 기억하고 있는 정보를 기반으로 인증을 수행하는 것이다. • 관리 비용이 저렴하나, 사용자가 인증 정보를 기억하지 못하면 본인이라도 인증받지 못한다. [예] 고정된 패스워드, 패스 프레이즈, 아이핀(i-PIN) 등
소유 기반 인증 (Something You Have)	• 사용자가 소유하고 있는 것을 기반으로 인증을 수행하는 것이다. • 소유물이 쉽게 도용될 수 있으므로 (①) 방식이나 (②) 방식과 함께 사용된다. [예] 신분증, 메모리 카드, 스마트 카드, OTP(One Time Password) 등
(②)	• 사용자의 고유한 생체 정보를 기반으로 인증을 수행하는 것이다. • 사용이 쉽고 도난의 위험도 적으며 위조가 어렵다. [예] 지문, 홍채/망막, 얼굴, 음성, 정맥 등
행위 기반 인증 (Something You Do)	사용자의 행동 정보를 이용해 인증 수행하는 것이다. [예] 서명, 동작
위치 기반 인증 (Somewhere You Are)	인증을 시도하는 위치의 적절성을 통해 인증을 수행하는 것이다. [예] 콜백, GPS나 IP 주소를 이용한 위치 기반 인증

답

- ① : 지식 기반 인증(Something You Know)
- ② : 생체 기반 인증(Something You Are)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 14 상대방이 전화로 인증을 요청한 경우, 전화를 끊고 걸려온 번호로 다시 전화를 걸어 해당 전화번호가 유효한지 확인하는 방법을 가리키는 용어를 쓰시오.

답 : 콜백(Call Back)

문제 15 보안 아키텍처(Security Architecture)에 대한 다음 설명에서 괄호(①~③)에 들어갈 알맞은 용어를 쓰시오.

- 보안 아키텍처란 정보 시스템의 (①), (②), (③)을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조를 말한다.
- 보안 아키텍처를 통해 관리적, 물리적, 기술적 보안 개념의 수립, 보안 관리 능력의 향상, 일관된 보안 수준의 유지를 기대할 수 있다.
- 보안 아키텍처는 보안 수준에 변화가 생겨도 기본 보안 아키텍처의 수정 없이 지원할 수 있어야 한다.
- 보안 아키텍처는 보안 요구사항의 변화나 추가를 수용할 수 있어야 한다.

답

- ① : 무결성(Integrity)
- ② : 가용성(Availability)
- ③ : 기밀성(Confidentiality)

문제 16 보안 아키텍처(Security Architecture)에 대한 다음 설명에서 괄호에 들어갈 알맞은 용어를 쓰시오.

- 보안 아키텍처는 정보 시스템의 무결성(Integrity), 가용성(Availability), 기밀성(Confidentiality)을 확보하기 위해 보안 요소 및 보안 체계를 식별하고 이들 간의 관계를 정의한 구조를 말한다.
- 보안 아키텍처의 표준화된 모델은 ( )에서 정의하고 있다.
- ( )는 보안 아키텍처를 보안 계층(Security Layers), 보안 영역(Security Areas), 보안 요소(Security Elements)의 3개 레이어로 구분하여 설명하고 있다.

답 : ITU-T X.805

문제 17 데이터 처리 과정에서의 오류나 외부의 불법적인 침입을 파악하기 위해 정보 시스템 내·외부의 모든 활동을 기록하고 분석하는 것을 가리키는 용어를 쓰시오.

답 : 감사 추적(Audit Trails)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 18 **소프트웨어 개발 보안에 관한 다음 설명에서 괄호에 공통으로 들어갈 알맞은 용어를 쓰시오.**

• 보안 프레임워크(Security Framework)는 안전한 정보 시스템 환경을 유지하고 보안 수준을 향상시키기 위한 체계를 말한다. • ( )은 정보보안 관리를 위한 국제 표준으로, 일종의 보안 인증이자 가장 대표적인 보안 프레임워크이다. • ( )은 영국의 BSI(British Standards Institute)가 제정한 BS 7799를 기반으로 구성되어 있다. • ( )은 조직에 대한 정보보안 관리 규격이 정의되어 있어 실제 심사/인증용으로 사용된다.

답 : ISO 27001

문제 19 **다음 설명의 괄호에 공통으로 들어갈 용어를 쓰시오.**

• ( )은 시스템 사용에 대한 모든 내역을 기록해 놓은 것으로, 이 정보를 이용하면 시스템 침해 사고 발생 시 해킹 흔적이나 공격 기법을 파악할 수 있다. • ( ) 정보를 정기적으로 분석하면 시스템에 대한 침입 흔적이나 취약점을 확인할 수 있다. • 리눅스에서는 시스템의 모든 ( )를 var/log 디렉터리에서 기록하고 관리한다. • Windows 시스템에서는 이벤트 형식으로 시스템의 ( )를 관리한다.

답 : 로그(Log)

문제 20 **정보 보안에 대한 다음 설명에 해당하는 용어를 쓰시오.**

• 기업이나 조직 내부의 네트워크와 인터넷 간에 전송되는 정보를 선별하여 수용·거부·수정하는 기능을 가진 침입 차단 시스템이다. • 내부 네트워크에서 외부로 나가는 패킷은 그대로 통과시키고, 외부에서 내부 네트워크로 들어오는 패킷은 내용을 엄밀히 체크하여 인증된 패킷만 통과시키는 구조이다. • 해킹 등에 의한 외부로의 정보 유출을 막기 위해 사용한다.

답 : 방화벽

문제 21 **해커 침입 패턴에 대한 추적과 유해 정보 감시를 위해 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템으로, 오용 탐지(Misuse Detection), 이상 탐지(Anomaly Detection) 등의 기능을 수행하는 보안 솔루션을 쓰시오.**

답 : 침입 탐지 시스템(IDS; Intrusion Detection System)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 22 **정보 보안에 대한 다음 설명에 해당하는 보안 솔루션을 쓰시오.**

• 방화벽과 침입 탐지 시스템을 결합한 것이다. • 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등의 방어 조치를 취하는 보안 솔루션이다. • 침입 탐지 기능으로 패킷을 하나씩 검사한 후 비정상적인 패킷이 탐지되면 방화벽 기능으로 해당 패킷을 차단한다.

답 : 침입 방지 시스템(IPS; Intrusion Prevention System)

문제 23 **정보 보안에 대한 다음 설명에 해당하는 보안 솔루션을 쓰시오.**

• 내부 정보의 외부 유출을 방지하는 보안 솔루션이다. • 사내 직원이 사용하는 PC와 네트워크상의 모든 정보를 검색하고 메일, 메신저, 웹하드, 네트워크 프린터 등의 사용자 행위를 탐지·통제해 외부로의 유출을 사전에 막는다.

답 : 데이터 유출 방지(DLP; Data Leakage/Loss Prevention)

문제 24 **일반 방화벽이 탐지하지 못하는 SQL 삽입 공격, XSS 등의 웹 기반 공격을 방어할 목적으로 만들어진 웹 서버에 특화된 방화벽으로, 웹 관련 공격을 감시하고 공격이 웹 서버에 도달하기 전에 이를 차단해 주는 보안 솔루션을 쓰시오.**

답 : 웹 방화벽(Web Firewall)

문제 25 **정보 보안에 대한 다음 설명에 해당하는 보안 솔루션을 한글 또는 영문(Fullname 또는 약어)으로 쓰시오.**

• 인터넷 등 통신 사업자의 공중 네트워크와 암호화 기술을 이용하여 사용자가 마치 자신의 전용 회선을 사용하는 것처럼 해주는 보안 솔루션이다. • 암호화된 규격을 통해 인터넷망을 전용선의 사설망을 구축한 것처럼 이용하므로 비용 부담을 줄일 뿐만 아니라 원격지의 지사, 영업소, 이동 근무자가 지역적인 제한 없이 업무를 수행할 수 있다.

답 : VPN(Virtual Private Network, 가상 사설 통신망)

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.

문제 26 **정보 보안에 대한 다음 설명에 해당하는 보안 솔루션을 영문(Fullname 또는 약어)으로 쓰시오.**

• 네트워크에 접속하는 내부 PC의 MAC 주소를 IP 관리 시스템에 등록한 후 일관된 보안 관리 기능을 제공하는 보안 솔루션이다. • 내부 PC의 소프트웨어 사용 현황을 관리하여 불법적인 소프트웨어 설치를 방지한다. • 일괄적인 배포 관리 기능을 이용해 백신이나 보안 패치 등의 설치 및 업그레이드를 수행한다.

답 : NAC(Network Access Control)

문제 27 **정보 보안에 대한 다음 설명에 해당하는 보안 솔루션을 영문(Fullname 또는 약어)으로 쓰시오.**

• 다양한 장비에서 발생하는 로그 및 보안 이벤트를 통합하여 관리하는 보안 솔루션이다. • 방화벽, IDS, IPS, 웹 방화벽, VPN 등에서 발생한 로그 및 보안 이벤트를 통합하여 관리함으로써 비용 및 자원을 절약할 수 있다. • 보안 솔루션 간의 상호 연동을 통해 종합적인 보완 관리 체계를 수립할 수 있다.

답 : ESM(Enterprise Security Management)

문제 28 **다음은 '주요정보통신기반시설 취약점 분석·평가 기준' 행정규칙에 제시된 정보 통신 기반 시설에 대한 취약점 분석·평가에 대한 설명이다. 괄호에 공통으로 들어갈 알맞은 용어를 쓰시오.**

• 취약점 분석 및 평가를 위해서는 관리적, 물리적, ( ) 세부 점검 항목표를 작성해야 한다. • 관리적 점검은 정보보호 정책이나 지침 등 관련 문서 확인과 정보보호 담당자, 시스템 관리자, 사용자 등과의 면담을 통해 수행한다. • 물리적 점검은 전산실, 발전실 등 통제구역을 직접 찾아가 현장 점검 형태로 수행한다. • ( ) 점검은 점검 도구, 수동 점검, 모의 해킹 등을 통해 수행한다. • 파악된 취약점별로 위험 등급을 '상, 중, 하' 3단계로 표시한다. • 위험등급 '상'은 조기 개선, '중', '하'는 중기 또는 장기 개선으로 구분하여 개선 방향을 수립한다.

답 : 기술적

연 습 란

※ 다음 여백은 연습란으로 사용하시기 바랍니다.