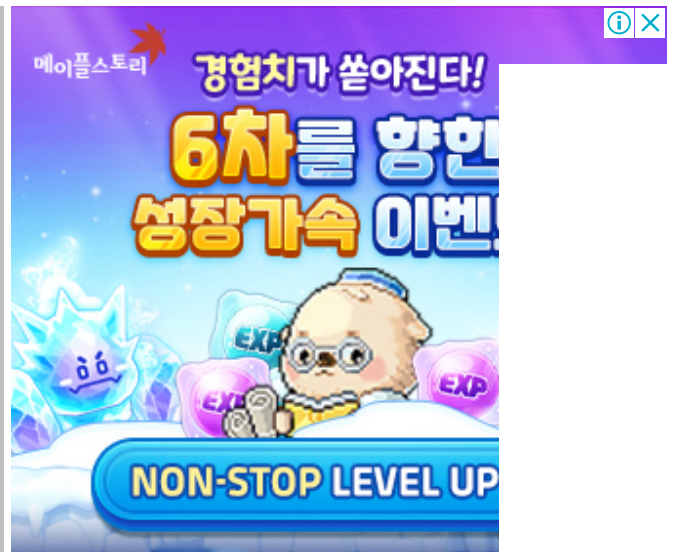


응시과목 : 정보처리기사 모의고사 202006~202204

과목	과 목 명	문항 수	맞힌 수	점 수	판정
1과목	소프트웨어 설계	0개	0개	0점	미응시
2과목	소프트웨어 개발	0개	0개	0점	미응시
3과목	데이터베이스 구축	0개	0개	0점	미응시
4과목	프로그래밍 언어 활용	0개	0개	0점	미응시
5과목	정보시스템 구축관리	20개	13개	65점	통과
전체 판정		20개	13개	65점	합격
합격을 진심으로 축하 드립니다.					



경과시간 : 00시간 09분 28초

틀린 문제의 내용은 아래와 같습니다. 다시 한번 풀어 보세요

5과목 : 정보시스템 구축관리

2021년08월14일 기출문제

81. 침입탐지 시스템(IDS : Intrusion Detection System)과 관련한 설명으로 틀린 것은?

1. 이상 탐지 기법(Anomaly Detection)은 Signature Base나 Knowledge Base라고도 불리며 이미 발견되고 정립된 공격 패턴을 입력해두었다가 탐지 및 차단한다.
2. HIDS(Host-Based Intrusion Detection)는 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고 어떤 작업을 했는지에 대한 기록을 남기고 추적한다.
3. NIDS(Network-Based Intrusion Detection System)로는 대표적으로 Snort가 있다.
4. 외부 인터넷에 서비스를 제공하는 서버가 위치하는 네트워크인 DMZ(Demilitarized Zone)에는 IDS가 설치될 수 있다.

입력한 답 : 4

정답 : [1]

정답률 : 44%

<문제 해설>

이상탐지(Anomaly Detection) -> Behavior, Statistical Detection로 불리며 평균적 시스템의 상태 기준으로 비정상적인 행위나 자원의 사용이 감지되면 이를 알려줌

오용탐지(Misuse Detection) -> Signature Base나 Knowledge Base로 불리며 미리 입력해둔 공격 패턴이 감지되면 이를 알려줌
[해설작성자 : 케인인님두판해요]

침입 탐지 시스템의 모델

- 오용탐지 : 잘 알려진 시스템의 취약점을 공격하는 패턴의 침입을 탐지 (새로운 공격 패턴을 막기 어려움)
- 이상탐지 : 잘 알려지지 않은 공격 탐지에 적합, 기존 패턴과 급격하게 다른 패턴을 발견하면 침입으로 판단

[해설작성자 : 눈딱감꼬낙하아아]

해설 추가(수정) 및 오류 신고

2020년08월22일 기출문제

83. 다음 빈칸에 알맞은 기술은

()은/는 웹에서 제공하는 정보 및 서비스를 이용하여 새로운 소프트웨어나 서비스, 데이터베이스 등을 만드는 기술이다.

1. Quantum Key Distribution
2. Digital Rights Management
3. Grayware
4. Mashup

입력한 답 : 3

정답 : [4] [정답감추기](#)

정답률 : 68%

<문제 해설>

Quantum Key Distribution -- 양자암호관련된거

Digital Rights Management -- DRM이라고도 하며, 저작권관리 관련 기술

Grayware -- 바이러스, 트로잔등 악성프로그램과는 다르게 사용자 동의를 받아 설치하는 프로그램

(ex 원격제어 프로그램, 애드웨어 등)

[해설작성자 : ㅋㅋ루뽕뽕]

해설 추가(수정) 및 오류 신고

2021년08월14일 기출문제

85. 정보 보안을 위한 접근 제어(Access Control)과 관련한 설명으로 틀린 것은?

1. 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것이다.
2. 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트로 볼 수 있다.
3. DBMS에 보안 정책을 적용하는 도구인 XDMCP를 통해 데이터베이스에 대한 접근제어를 수행할 수 있다.

4. 네트워크 장비에서 수행하는 IP에 대한 접근 제어로는 관리 인터페이스의 접근제어와 ACL(Access Control List) 등 있다.

입력한 답 : 4

정답 : [3] [정답감추기](#)

정답률 : 58%

<문제 해설>

1. 정보 보안에 대한 접근 제어의 기본 개념

2. 시스템 및 네트워크에 대한 제어 방법에 대해선 IP와 서비스 포트이며 예로는

Telnet port : 23 ssh port : 22

4. 네트워크 장비 라우터, L3 장비에서 ACL config 설정으로 Permit 와 deny 로 허용과 거부를 사용 할 수 있다.

[해설작성자 : OSPF_SAN]

X Display Manager Control Protocol(XDMCP) : 사용자 인증이 완료되면 X서버의 로그인 세션을 시작한다.

[해설작성자 : 눈딱감꼬낙하아아]

[해설 추가\(수정\) 및 오류 신고](#)

2020년08월22일 기출문제

87. 큰 숫자를 소인수 분해하기 어렵다는 기반 하에 1978년 MIT에 의해 제안된 공개키 암호화 알고리즘은?

1. DES
2. ARIA
3. SEED
4. RSA

입력한 답 : 2

정답 : [4] [정답감추기](#)

정답률 : 77%

<문제 해설>

1. DES는 1975년 IBM에서 개발함

2. ARIA는 국내에서 개발됨(SEED 이후 만들어짐)

3. SEED도 국내에서 개발됨

[해설작성자 : ㅋㅋ루뽕뽕]

[해설 추가\(수정\) 및 오류 신고](#)

2021년08월14일 기출문제

89. 비대칭 암호화 방식으로 소수를 활용한 암호화 알고리즘은?

1. DES
2. AES

3. SMT

4. RSA

입력한 답 : 1

정답 : [4] [정답감추기](#)

정답률 : 66%

<문제 해설>

대칭키 암호화 - 블록 암호화 방식 : DES, SEED, AES, ARIA

개인키 암호화 - 스트림 암호화 방식 : LFSR, RC4

공개키 암호화(비대칭 암호) : RSA

[해설작성자 : comcbt.com 이용자]

암호화 알고리즘은 크게 2가지로 나뉨.

1. 양방향 2. 단방향

1. 양방향은 1) 개인키와 2) 공개키로 나누어지며

1) 개인키는 또 다시 블록방식과 스트림방식으로 나누어짐.

블록방식은 DES, AES, SEED, ARIA 등이 있고 스트림 방식으론 LFSR과 RC4가 있음. 개인키는 다른말로 비대칭키라고 불리며, 암호화와 복호화때 사용하는 키가 다르며 장점으로는 속도가 빠르지만 관리해야할 키의 수가 많음($2n$ 개).

2) 공개키는 대표적으로 RSA가 있으며 소수 라는 키워드가 나오면 바로 RSA가 답임.

관리해야하는 키의 수가 적음

$n(n-1)/2$

그리고 단방향은 hash이며 대표적으로 Sha시리즈나 n nash, md4 md5 등이 있음. 매회 출제되는 영역이라서 계층별로 특징을 꼭 숙지해야됩니다.

[해설작성자 : 연상암기황제]

아래와 같은 오류 신고가 있었습니다.

여러분들의 많은 의견 부탁드립니다.

추후 여러분들의 의견을 반영하여 정답을 수정하도록 하겠습니다.

참고로 정답 변경은 오류 신고 5회 이상일 경우 수정합니다.

[오류 신고 내용]

암호 알고리즘 방식은 양방향과 일방향이 있다.

양방향에는 1) 대칭 키 암호 방식 2) 비대칭 키 암호 방식(= 공개키 암호 방식)이 있다.

일방향에는 해시함수 방식이 있다. ex) MDC, MAC

양방향

1) 대칭 키 암호 방식: 블록 암호 방식과 스트림 암호 방식이 있다. 장점으로는 계산 속도가 빠르고 단점으로는 키 분배 및 관리의 어려움이 있다. [$n(n-1)/2$ 개]

2) 비대칭 키 암호 방식: 공개키와 개인키가 존재한다. 장점으로는 관리해야 할 키의 개수가 적고 ($2n$ 개) 단점으로는 계산 속도가 느리다는 것이 있다. ex) RSA, 디피-헬만, ECC, Elgamal

연상암기황제님의 설명 중, 개인키는 다른 말로 비대칭 키라는 말과 암호화와 복호화 할 때 사용하는 키가 다르다는 것은 대칭 키 방식의 설명이 아닙니다. 공개키 암호 방식이 다른 말로 비대칭 키 암호 방식이며 비밀키가 다른 말로 대칭 키 입니다. 대칭 키 암호 방식은 암호화와 복호화에 같은 암호 키가 쓰입니다. 관리해야 할 키의 개수 또한 $2n$ 과 $n(n-1)/2$ 이 서로 바뀌었습니다.

[해설작성자 : CBT짱]

[해설 추가\(수정\) 및 오류 신고](#)

2022년04월24일 기출문제

97. 각 사용자 인증의 유형에 대한 설명으로 가장 적절하지 않은 것은?

1. 지식 : 주체는 '그가 알고 있는 것'을 보여주며 예시로는 패스워드, PIN 등이 있다.
2. 소유 : 주체는 '그가 가지고 있는 것'을 보여주며 예시로는 토큰, 스마트카드 등이 있다.
3. 존재 : 주체는 '그를 대체하는 것'을 보여주며 예시로는 패턴, QR 등이 있다.
4. 행위 : 주체는 '그가 하는 것'을 보여주며 예시로는 서명, 움직임, 음성 등이 있다.

입력한 답 : 1

정답 : [3] [정답감추기](#)

정답률 : 75%

<문제 해설>

1. 지식 - 본인이 알고 있는 것 (ex. 패스워드, PIN 등)
2. 소유 - 본인이 가지고 있는 것 (ex. 토큰, 스마트카드 등)
3. 존재 - 본인을 나타내는 것 (ex. 홍채, 지문 등)
4. 행위 - 본인이 하는 것 (ex. 서명, 움직임, 음성 등)

[해설작성자 : 지나가는 행인]

[해설 추가\(수정\) 및 오류 신고](#)

2020년09월26일 기출문제

98. NS(Nassi-Schneiderman) chart에 대한 설명으로 거리가 먼 것은?

1. 논리의 기술에 중점을 둔 도형식 표현 방법이다.
2. 연속, 선택 및 다중 선택, 반복 등의 제어논리 구조로 표현한다.
3. 주로 화살표를 사용하여 논리적인 제어구조로 흐름을 표현한다.
4. 조건이 복합되어 있는 곳의 처리를 시각적으로 명확히 식별하는데 적합하다.

입력한 답 : 4

정답 : [3] [정답감추기](#)

정답률 : 66%

<문제 해설>

직사각형을 포개어가는 것으로 나타낸다.

[해설작성자 : 냐옹맨]

논리의 기술에 중점을 둔 도형을 이용한 표현 방법이다.

그리기가 어렵다. (전문성이 있어야 잘 그린다)

순차, 선택, 반복으로 표현한다.

임의의 제어 이동이 어렵다.

goto구조가 어렵다.

그래픽 설계 도구이다.

상자 도표라고도 한다

프로그램으로 구현이 쉽다.

조건이 복합되어 있는 곳의 처리를 명확히 식별하기에 적합하다.

if문이 여러개일 때 가능

[해설작성자 : comcbt.com 이용자]

여기까지가 틀린 문제 입니다.

42세 이하인 경우 이 게임을 플레이하지 마

sponsored by: RAID: Shadow Legends

다음에는 꼭 만점 받으세요 ^__^*

로그인 기능을 이용하지 않고 계십니다. 문제풀 기록을 남기시려면 본인의 이름이나 닉네임을 적으세요.

기록을 남겨 두시면 차후에 틀린문제만 다시 볼수 있는 오답노트 기능 및 본인의 틀린문제를 이용한 인공지능 모의고사가 지원됩니다.

이름을 남겨 두시면 이후 CBT 작동시 자동으로 이름을 인식 합니다.(접속중에 한함)

한글 15자 영문 30자 까지 입력가능합니다. 총 30Byte(한글 2Byte, 영문 1Byte, 공백문자 자동 제거됩니다.)

인터넷 익스플로러 6.0 사용자의 경우 일부 컴퓨터에서 정상 작동하지 않을 수 있습니다.

익스플로러 - [도구]-[인터넷옵션]의 [고급] 탭에 URL를 항상 UTF-8로 보냄을 설정(체크) 하시고 사용하세요.

이름 : 바이트 입력하였습니다.

아래 내용부터는 맞으신 문제입니다.

해설을 알고 계시다면 해설 추가 기능을 이용하여 다른분들과 함께 해설을 나누었으면 합니다.
여러분들께서 작성하신 해설 하나 하나가 모여서 전자문제집 CBT의 해설이 이루어 집니다.

해설작성후 해설은 바로 보이지 않으며 관리자의 간단한 검사 및 승인후 보이기 시작합니다.

해설 작성시 그림파일로 설명하고자 하실경우

www.comcbt.com/xe/freeb에 작성후 주소를 남겨주시면 됩니다.

5과목 : 정보시스템 구축관리

2020년06월06일 기출문제

82. 메모리상에서 프로그램의 복귀 주소와 변수사이에 특정 값을 저장해 두었다가 그 값이 변경되었을 경우 오버플로우 상태로 가정하여 프로그램 실행을 중단하는 기술은?

1. 모드체크
2. 리커버리 통제
3. 시스로그
4. 스택가드

정답 : [4] [정답보기](#)

정답률 : 77%

<문제 해설>

Stack Protection : Stack Overflow를 탐지하고 보안을 강화시키는 기법

Stack Guard : Stack 상에 일정한 주소번지에 프로그램이 선언한 canary를 심어 두어, 스택의 변조 된 경우에, canary를 체크하여 프로그램이 비정상적으로 종료 시키는 기법

Stack Shield : 함수의 리턴주소를 복사하여 실제 리턴주소를 참조하지 않고 함수를 리턴해주는 기법

Syslog : 시스템에서 로그메시지를 처리하기 위해서 제공

Recovery Control : 부적절한 사건/상황으로 인해 발생한 피해를 극복, 장애/혼란을 정돈하고 정상상태로 회복

+ 카나리(Canary 또는 Canaries) : buffer와 SFP 사이에 buffer overflow를 탐지하기 위한 특정 값(canary value)을 삽입하는 기법

+ Canary 종류 : terminator, random, random XOR (스택가드는 canary 세 가지 모두를 지원)

+ ProPolice 종류 : terminator와 random

+ StackGuard와 ProPolice는 (함수 포인터들을 오버플로우하는) 자동으로 할당된 구조체들에서 오버플로우를 방어하지 못한다.

[해설 추가\(수정\) 및 오류 신고](#)

2020년06월06일 기출문제

84. IP 또는 ICMP의 특성을 악용하여 특정 사이트에 집중적으로 데이터를 보내 네트워크 또는 시스템의 상태를 불능으로 만드는 공격 방법은?

1. TearDrop
2. Smishing
3. Qshing
4. Smurfing

정답 : [4] [정답보기](#)

정답률 : 69%

<문제 해설>

서비스 공격 유형

DoS (서비스 거부) : 표적이 되는 서버의 자원을 고갈시킬 목적으로 다수 공격자 or 시스템에서 대량의 데이터를 한 곳에 집중적으로 전송함

Ping of Death (죽음의 핑) : Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용범위 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격

Smurfing : IP나 ICMP의 특성을 악용 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크를 불능 상태로 만드는 공격 방법.

SYN Flooding : TCP는 신뢰성 있는 전송을 위해 3-way-handshake를 거친 후 데이터를 전송하는데 SYN은 공격자가 가상의 클라이언트로 위장 3WH을 의도적으로 중단, 서버

가 대기상태에 놓여 정상 서비스를 못하게 하는 공격 방법

TearDrop : Offset 값을 변경시켜 수신 측에서 패킷을 재조립할 때 오류로 인한 과부하를 발생 시킴

Land : 패킷을 전송할 때 송 수신 IP주소를 모두 공격대상 IP주소로 하여 공격대상에게 전송하는 것, 공격대상은 송신IP주소가 자신이기 때문에 자신에게 무한히 응답하게 되는 공격

DDoS(분산 서비스 거부) : 여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행

[해설작성자 : 거상 주작섭]

해설 추가(수정) 및 오류 신고

2022년03월05일 기출문제

86. 소프트웨어 생명주기 모델 중 V 모델과 관련한 설명으로 틀린 것은?

1. 요구 분석 및 설계단계를 거치지 않으며 항상 통합 테스트를 중심으로 V 형태를 이룬다.
2. Perry에 의해 제안되었으며 세부적인 테스트 과정으로 구성되어 신뢰도 높은 시스템을 개발하는데 효과적이다.
3. 개발 작업과 검증 작업 사이의 관계를 명확히 드러내 놓은 폭포수 모델의 변형이라고 볼 수 있다.
4. 폭포수 모델이 산출물 중심이라면 V 모델은 작업과 결과의 검증에 초점을 둔다.

정답 : [1] [정답보기](#)

정답률 : 66%

<문제 해설>

V 모델(V-model)은 소프트웨어 개발 프로세스로 폭포수 모델의 확장된 형태 중 하나로 볼 수 있다. 아래 방향으로 선행적으로 내려가면서 진행되는 폭포수 모델과 달리, 이 프로세스는 오른쪽 그림과 같이 코딩 단계에서 위쪽으로 꺾여서 알파벳 V자 모양으로 진행된다

검증(Verification)단계

1. 요구사항 분석
2. 시스템 설계
3. 아키텍처 설계
4. 모듈 설계

[해설작성자 : 58]

해설 추가(수정) 및 오류 신고

2022년04월24일 기출문제

88. 물리적 위협으로 인한 문제에 해당하지 않는 것은?

1. 화재, 홍수 등 천재지변으로 인한 위협
2. 하드웨어 파손, 고장으로 인한 장애
3. 방화, 테러로 인한 하드웨어와 기록장치를 물리적으로 파괴하는 행위

4. 방화벽 설정의 잘못된 조작으로 인한 네트워크, 서버 보안 위협

정답 : [4] [정답보기](#)

정답률 : 82%

<문제 해설>

방화벽 설정의 잘못된 조작으로 인한 네트워크, 서버 보안 위협 - 기술적
[해설작성자 : 너굴맨]

[해설 추가\(수정\) 및 오류 신고](#)

2021년08월14일 기출문제

90. 다음에서 설명하는 IT 스토리지 기술은?

- 가상화를 적용하며 필요한 공간만큼 나눠 사용할 수 있도록 하며 서버 가상화와 유사함
- 컴퓨팅 소프트웨어로 규정하는 데이터 스토리지 체계이며, 일정 조직 내 여러 스토리지를 하나처럼 관리하고 운용하는 컴퓨터 이용 환경
- 스토리지 자원을 효율적으로 나누어 쓰는 방법으로 이해할 수 있음

1. Software Defined Storage
2. Distribution Oriented Storage
3. Network Architected Storage
4. Systematic Network Storage

정답 : [1] [정답보기](#)

정답률 : 53%

<문제 해설>

두번째 단락의 '컴퓨팅 소프트웨어로(Software) 규정하는(Defined) 데이터 스토리지 체계이며,'

=> Software Defined Storage

[해설작성자 : 3.14]

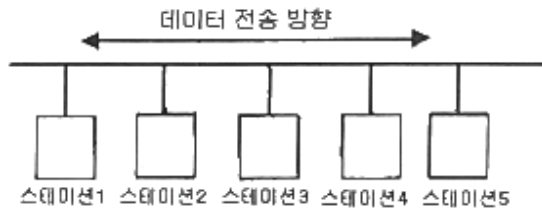
- 소프트웨어 정의 스토리지 (Software-defined storage) (SDS) : 스토리지에 가상화를 적용, 소프트웨어로 전체 스토리지 자원을 관리하여 하나의 저장장치처럼 사용할 수 있도록 하는 기법

[해설작성자 : 눈딱감꼬낙하아아]

[해설 추가\(수정\) 및 오류 신고](#)

2021년03월07일 기출문제

91. 다음 LAN의 네트워크 토폴로지는 어떤 형인가?



1. 그물형
2. 십자형
3. 버스형
4. 링형

정답 : [3] [정답보기](#)

정답률 : 87%

<문제 해설>

버스 스테이션 그래서 버스형 골랐어요.
 버스가 정거장 들리듯이 데이터가 전송됨
 [해설작성자 : comcbt.com 이용자]

[해설 추가\(수정\) 및 오류 신고](#)

2021년05월15일 기출문제

92. PC, TV, 휴대폰에서 원하는 콘텐츠를 끊임없이 자유롭게 이용할 수 있는 서비스는?

1. Memristor
2. MEMS
3. SNMP
4. N-Screen

정답 : [4] [정답보기](#)

정답률 : 72%

<문제 해설>

* 하드웨어 관련 신기술

1. Memristor : memory + register. 전원 공급이 끊어져도 다시 전원이 공급되면 이 전 상태 복원
2. MEMS : 센서, 액추에이터 등 기계구조를 다양한 기술로 미세 가공 후 전기기계적 동작 가능케 한 초미세장치
3. SNMP : 하드웨어 신기술 아님. 간이 망 관리 프로토콜
4. N-Screen : N개의 서로 다른 단말기에서 동일콘텐츠를 자유롭게 이용 가능한 서비스

[해설작성자 : 78]

[해설 추가\(수정\) 및 오류 신고](#)

2022년04월24일 기출문제

93. 대칭 암호 알고리즘과 비대칭 암호 알고리즘에 대한 설명으로 틀린 것은?

1. 대칭 암호 알고리즘은 비교적 실행 속도가 빠르기 때문에 다양한 암호의 핵심 함수로 사용될 수 있다.
2. 대칭 암호 알고리즘은 비밀키 전달을 위한 키 교환이 필요하지 않아 암호화 및 복호화의 속도가 빠르다.
3. 비대칭 암호 알고리즘은 자신만이 보관하는 비밀키를 이용하여 인증, 전자서명 등에 적용이 가능하다.
4. 대표적인 대칭키 암호 알고리즘으로는 AES, IDEA 등이 있다.

정답 : [2] [정답보기](#)

정답률 : 49%

<문제 해설>

대칭 암호화 알고리즘은 키 교환이 필요하기 때문에 키를 교환하는 중 키가 탈취될 수 있다는 문제가 있다.
공개 암호화 방식에 비해 속도가 빠르다.
[해설작성자 : 코봉이]

[해설 추가\(수정\) 및 오류 신고](#)

2021년05월15일 기출문제

94. IPSec(IP Security)에 대한 설명으로 틀린 것은?

1. 암호화 수행시 일방향 암호화만 지원한다.
2. ESP는 발신지 인증, 데이터 무결성, 기밀성 모두를 보장한다.
3. 운영 모드는 Tunnel 모드와 Transport 모드로 분류된다.
4. AH는 발신지 호스트를 인증하고, IP 패킷의 무결성을 보장한다.

정답 : [1] [정답보기](#)

정답률 : 70%

<문제 해설>

일방향 암호화는 해시암호화
[해설작성자 : comcbt.com 이용자]

IPSec : IP계층(3계층)에서 무결성과 인증 보장하는 인증헤더와 기밀성 보장하는 암호화 이용해 양 종단 구간에 보안 서비스 제공하는 터널링 프로토콜

* IPSec의 세부프로토콜

- IKE(Internet Key Exchange) : 보안 관련 설정들을 생성, 협상 및 관리하는 프로토콜(udp500번 포트 사용)
- ESP(Encapsulating Security Payload) : 메시지 인증코드, 암호화 이용해 "인증(무결성)", "발신지인증", "기밀성" 제공 프로토콜
- AH(Authentication Header) : 기밀성 제외한 메시지 인증코드 이용한 "인증(무결성)", "발신지인증" 제공 프로토콜

[해설작성자 : 빨리 집가야쥐...]

[해설 추가\(수정\) 및 오류 신고](#)

2022년03월05일 기출문제

95. DES는 몇 비트의 암호화 알고리즘인가?

- 1. 8
- 2. 24
- 3. 64
- 4. 132

정답 : [3] [정답보기](#)

정답률 : 76%

<문제 해설>

DES의 키는 7비트마다 오류 검출을 위한 정보가 1비트씩 들어가기 때문에 실질적으로는 56비트이다.

추가적으로 AES는 암호화 알고리즘은 AES-128, AES-192, AES-256로 나뉘어지며 숫자는 비트수이다.

[해설작성자 : 구구구구]

[해설 추가\(수정\) 및 오류 신고](#)

2020년08월22일 기출문제

96. 전자 칩과 같은 소프트웨어 부품, 즉 블록(모듈)을 만들어서 끼워 맞추는 방법으로 소프트웨어를 완성시키는 재사용 방법은?

- 1. 합성 중심
- 2. 생성 중심
- 3. 분리 중심
- 4. 구조 중심

정답 : [1] [정답보기](#)

정답률 : 72%

<문제 해설>

합성 중심(Composition-Based) : 전자 칩과 같은 소프트웨어 부품, 즉 블록(모듈)을 만들어서 끼워 맞추어 소프트웨어를 완성시키는 방법으로, 블록 구성 방법이라고도 한다.

생성 중심(Generation-Based) : 추상화 형태로 쓰여진 명세를 구체화하여 프로그램을 만드는 방법으로, 패턴 구성 방법이라고도 한다.

[해설 추가\(수정\) 및 오류 신고](#)

2021년05월15일 기출문제

99. 서로 다른 네트워크 대역에 있는 호스트들 상호간에 통신할 수 있도록 해주는 네트워크 장비는?

1. L2 스위치
2. HIPO
3. 라우터
4. RAD.

정답 : [3] [정답보기](#)

정답률 : 82%

<문제 해설>

라우터 : 브리지와 같이 LAN과 LAN의 연결 기능에 데이터 전송의 최적 경로를 선택할 수 있는 기능이 추가된 것으로, 서로 다른 LAN이나 LAN과 WAN의 연결도 수행한다.
[해설작성자 : 코코누나]

라우터는 3계층(네트워크)까지의 프로토콜 구조가 다른 네트워크 간의 연결을 위해 프로토콜 변환 기능을 수행한다.
[해설작성자 : 만히]

[해설 추가\(수정\) 및 오류 신고](#)

2020년06월06일 기출문제

100. 시스템 내의 정보는 오직 인가된 사용자만 수정할 수 있는 보안 요소는?

1. 기밀성
2. 부인방지
3. 가용성
4. 무결성

정답 : [4] [정답보기](#)

정답률 : 44%

<문제 해설>

아래와 같은 오류 신고가 있었습니다.
여러분들의 많은 의견 부탁드립니다.
추후 여러분들의 의견을 반영하여 정답을 수정하도록 하겠습니다.
참고로 정답 변경은 오류 신고 5회 이상일 경우 수정합니다.

[오류 신고 내용]

답이 1번인 듯합니다.

오직 인가된 사용자만이 수정할 수 있는 보안요소----->기밀성
인가된 사용자가 언제든지 사용가능----->가용성
전송 전 데이터와 전송 후 데이터가 동일함(수정, 삭제, 변조 등을 차단)--->무결성
[해설작성자 : 통신마왕(부경대 정보통신공학과 레전설)]

[오류신고 반론]

정답 4번 맞는 것 같아요 접근가능한게 기밀성이고 수정은 무결성이 맞습니다
[해설작성자 : ㅇㅇ]

[관리자 입니다.]

가답안 및 확정답안 확인결과

가답안 4번, 확정답안 4번으로 중복답안 인정되지 않은것으로 확인 됩니다.

논란의 여지는 있겠지만. 확정답안은 4번 이었습니다.
문제가 좀 매끄럽지 못하기는 하네요.
차후에 동일한 문제가 출제된다면 아마도 정답은 4번일겁니다.
한번 답으로 정해진게 다음에 출제되었을때 답을 바꾸는 경우는 아주 드뭅니다.
참고 하시고 열공하세요.]

[오류신고 반론]

잘못 알고 계십니다.

기밀성은 오직 인가된 사용자만이 내용을 확인 할 수 있는 것입니다. 기밀문서가 비
공개문서지 수정문서라고 생각하는 사람은 없겠죠?

무결성은 그 기밀성 내에서 인가된 사용자만이 내용을 수정할 수 있는 것이구요.

가용성은 인가된 사용자가 언제든지 사용가능한 것입니다.

[해설작성자 : 거상 주작성]

[오류신고 반론]

※최종결론

기밀성 - 열람

무결성 - 수정

가용성 - 사용

따라서 정답 4번. 무결성

해설 추가(수정) 및 오류 신고

다음에는 꼭 만점 받으세요 ^__^*

**로그인 기능을 이용하지 않고 계십니다. 문제풀 기록을 남기시려면 본인의 이름이나 닉네임을 적으
세요.**

기록을 남겨 두시면 차후에 틀린문제만 다시 볼수 있는 오답노트 기능 및 본인의 틀린문제를 이용한
인공지능 모의고사가 지원됩니다.

이름을 남겨 두시면 이후 CBT 작동시 자동으로 이름을 인식 합니다.(접속중에 한함)

한글 15자 영문 30자 까지 입력가능합니다. 총 30Byte(한글 2Byte, 영문 1Byte, 공백문자 자동 제거되
니다.)

인터넷 익스플로러 6.0 사용자의 경우 일부 컴퓨터에서 정상 작동하지 않을 수 있습니다.

익스플로러 - [도구]-[인터넷옵션]의 [고급] 탭에 URL를 항상 UTF-8로 보냄을 설정(체크) 하시고 사용
하세요.

이름 : 바이트 입력하였습니다.