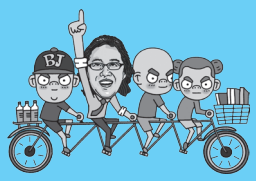
수험생의 마음으로 만든 책! 시나공 시리즈

2020 시나공

시험에 나오는 것만 공부한다!



2020년 2회 정보처리기사 실기 시험 100% 합격전략집

1일차 2일차 3일차 4일차 5일차 6일차 7일차 8일차 9일차 10일차
11일차 12일차 13일차 14일차 **15일차** 16일차 17일차 18일차 19일차 20일차

9장 소프트웨어 개발 보안 구축

2020년 2회 정보처리기사 실기 대비용 핵심요약

9장 | 소프트웨어 개발 보안 구축

2020 시나공 정보처리기사 필기 수록 내용

[핵심119] 소프트웨어 개발의 비용 산정 기법

- 소프트웨어 비용 산정은 소프트웨어의 개발 규모를 소요되는 인원, 자원, 기간 등으로 확인하여 실행 가능한 계획을 수립하기 위해 필요한 비용을 산정하는 것이다.
- 하향식 비용 산정 기법
  - 과거의 유사한 경험을 바탕으로 전문 지식이 많은 개발자들이 참여한 회의를 통해 비용을 산정하는 비과학적인 방법이다.
  - 종류

전문가 감정 기법	조직 내에 있는 경험이 많은 두 명 이상의 전문가에게 비용 산정을 의뢰하는 기법
델파이 기법	전문가 감정 기법의 주관적인 편견을 보완하기 위해 많은 전문가의 의견을 종합하여 산정하는 기법

- 상향식 비용 산정 기법
  - 프로젝트의 세부적인 작업 단위별로 비용을 산정한 후 집계하여 전체 비용을 산정하는 방법이다.
  - 종류

LOC(원시 코드 라인 수, source Line Of Code) 기법	• 소프트웨어 각 기능의 원시 코드 라인 수의 비관치, 낙관치, 기대치를 측정하여 예측치를 구하고 이를 이용하여 비용을 산정하는 기법이다. • 산정 공식 : – 노력(인월) = 개발 기간 × 투입 인원 = LOC / 1인당 월평균 생산 코드 라인 수 – 개발 비용 = 노력(인월) × 단위 비용 (1인당 월평균 인건비) – 개발 기간 = 노력(인월) / 투입 인원 – 생산성 = LOC / 노력(인월) 예 LOC 기법에 의하여 예측된 총 라인 수가 40,000라인, 개발에 참여할 프로그래머가 10명, 프로그래머들의 평균 생산성이 월간 400라인일 때 개발에 소요되는 기간은? • 노력(인월) = LOC/1인당 월평균 생산 코드 라인 수 = 40000/400 = 100명 • 개발 기간 = 노력(인월)/투입 인원 = 100/10 = 10개월
개발 단계별 인월수(Effort Per Task) 기법	LOC 기법을 보완하기 위한 기법으로, 각 기능을 구현시키는 데 필요한 노력을 생명 주기의 각 단계별로 산정한다.

2020년 1회 기사 실기

1. LOC 기법에 의하여 예측된 총 라인 수가 30,000라인, 개발에 참여할 프로그래머가 5명, 프로그래머들의 평균 생산성이 월간 300라인일 때 개발에 소요되는 기간을 쓰시오.

답

- 계산 공식 :
- 결과 :

2. 어떤 소프트웨어 개발을 위해 7명의 개발자가 5개월 동안 참여되었다. 그런데 그 중 5명은 5개월 동안 계속 참여했지만 2명은 2개월 동안만 부분적으로 참여했다. 이 소프트웨어 개발을 위한 인월(Man Month)은 얼마인지 쓰시오.

답 :

해설 2. 5명이 5개월 동안 개발한 것의 노력(인월)은 25이고, 2명이 2개월 동안 개발한 것의 노력은 4이므로 25 + 4 = 29입니다.

정답 1. 계산 공식 : (30,000 / 300) / 5 = 20, 결과 : 20개월 2. 29

2020 시나공 정보처리기사 필기 수록 내용

[핵심120] 서비스 거부 공격

- 표적이 되는 서버의 자원을 고갈시킬 목적으로 다수의 공격자 또는 시스템에서 대량의 데이터를 한 곳의 서버에 집중적으로 전송함으로써, 표적이 되는 서버의 정상적인 기능을 방해하는 것이다.
- 서비스 거부 공격의 유형

Ping of Death (죽음의 핑)	Ping 명령을 전송할 때 패킷의 크기를 인터넷 프로토콜 허용 범위(65,536 바이트) 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법
Smurfing(스머핑)	IP나 ICMP의 특성을 악용하여 엄청난 양의 데이터를 한 사이트에 집중적으로 보냄으로써 네트워크 또는 시스템의 상태를 불능으로 만드는 공격 방법

SYN Flooding	TCP(Transmission Control Protocol)는 신뢰성 있는 전송을 위해 3-way-handshake를 거친 후에 데이터를 전송하게 되는데, SYN Flooding은 공격자가 가상의 클라이언트로 위장하여 3-way-handshake 과정을 의도적으로 중단시킴으로써 공격 대상인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법
TearDrop	데이터의 송 · 수신 과정에서 패킷의 크기가 커 여러 개로 분할되어 전송될 때 분할 순서를 알 수 있도록 Fragment Offset 값을 함께 전송하는데, TearDrop은 이 Offset 값을 변경시켜 수신 측에서 패킷을 재조립할 때 오류로 인한 과부하를 발생시킴으로써 시스템이 다운되도록 하는 공격 방법
Land	패킷을 전송할 때 송신 IP 주소와 수신 IP 주소를 모두 공격 대상의 IP 주소로 하여 공격 대상에게 전송하는 것으로, 이 패킷을 받은 공격 대상은 송신 IP 주소가 자신이므로 자신에게 응답을 수행하게 되는데, 이러한 패킷이 계속해서 전송될 경우 자신에 대해 무한히 응답하게 하는 공격
DDoS(Distributed Denial of Service, 분산 서비스 거부) 공격	여러 곳에 분산된 공격 지점에서 한 곳의 서버에 대해 분산 서비스 공격을 수행하는 것으로, 네트워크에서 취약점이 있는 호스트들을 탐색한 후 이들 호스트들에 분산 서비스 공격용 툴을 설치하여 에이전트(Agent)로 만든 후 DDoS 공격에 이용함

2020년 1회 기사 실기

1. 다음은 네트워크 공격에 대한 패킷 로그를 표현한 것이다. 아래의 패킷 로그와 같이 공격자가 패킷의 출발지 주소(Address) 또는 포트(Port)를 임의로 변경하여 송신측 IP 주소 또는 포트를 동일하게 함으로써 송신 IP 주소가 자신이므로 자신에게 응답을 수행하게 되는데, 이러한 패킷을 계속 전송하면 자신에 대해 무한히 응답하게 되므로 컴퓨터의 실행 속도를 느리게 하거나 동작을 마비시켜 서비스 거부 상태에 빠지도록 하는 네트워크 공격이 무엇인지 쓰시오.

```
source : 192.168.1.200
destination : 192.168.1.200
protocol : 6
src port : 21845
dst port : 21845
```

답 :

2020년 1, 2회 기사 필기

2. IP나 ICMP의 특성을 악용하여 특정 사이트에 집중적으로 데이터를 보내 네트워크 또는 시스템의 상태를 불능으로 만드는 공격 방법을 쓰시오.

답 :

정답 1. Land 2. Smurfing

2020 시나공 정보처리기사 필기 수록 내용

[핵심 121] 네트워크 침해 공격 관련 용어

스미싱 (Smishing)	각종 행사 안내, 경품 안내 등의 문자 메시지(SMS)를 이용해 사용자의 개인 신용정보를 빼내는 수법
스피어 피싱 (Spear Phishing)	사회 공학의 한 기법으로, 특정 대상을 선정한 후 그 대상에게 일반적인 이메일로 위장한 메일을 지속적으로 발송하여, 발송 메일의 본문 링크나 첨부된 파일을 클릭하도록 유도해 사용자의 개인 정보를 탈취 함
APT(Advanced Persistent Threats, 지능형 지속 위협)	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 공격
무작위 대입 공격 (Brute Force Attack)	암호화된 문서의 암호키를 찾아내기 위해 적용 가능한 모든 값을 대입하여 공격하는 방식
큐싱(Qshing)	QR코드(Quick Response Code)를 통해 악성 앱의 다운로드를 유도하거나 악성 프로그램을 설치하도록 하는 금융사기 기법의 하나로, QR코드와 개인정보 및 금융정보를 낚는다(Fishing)는 의미의 합성 신조어

SQL 삽입(Injection) 공격	전문 스캐너 프로그램 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작하는 일련의 공격 방식

1. 다음은 네트워크 침해 공격과 관련된 용어 설명이다. 괄호(①~④)에 들어갈 가장 알맞은 용어를 쓰시오.

(①)	QR코드(Quick Response Code)를 통해 악성 앱의 다운로드를 유도하거나 악성 프로그램을 설치하도록 하는 금융사기 기법이다.
(②)	각종 행사 안내, 경품 안내 등의 문자 메시지(SMS)를 이용해 사용자의 개인 신용 정보를 빼내는 수법이다.
(③)	전문 스캐너 프로그램 혹은 봇넷 등을 이용해 웹사이트를 무차별적으로 공격하는 과정에서 취약한 사이트가 발견되면 데이터베이스 등의 데이터를 조작하는 일련의 공격 방식이다.
(④)	사회 공학의 한 기법으로, 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 방식이다.

답
①:
②:
③:
④:

정답 1. ① 큐싱(Qshing) ② 스미싱(Smishing) ③ SQL 삽입(Injection) 공격 ④ 스피어 피싱(Spear Phishing)

2020 시나공 정보처리기사 필기 수록 내용

[핵심 122] 정보 보안 침해 공격 관련 용어

좀비(Zombie) PC	악성코드에 감염되어 다른 프로그램이나 컴퓨터를 조종하도록 만들어진 컴퓨터로, C&C(Command & Control) 서버의 제어를 받아 주로 DDoS 공격 등에 이용됨
C&C 서버	해커가 원격지에서 감염된 좀비 PC에 명령을 내리고 악성코드를 제어하기 위한 용도로 사용하는 서버를 말함
봇넷(Botnet)	악성 프로그램에 감염되어 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 말함
웜(Worm)	네트워크를 통해 연속적으로 자신을 복제하여 시스템의 부하를 높임으로써 결국 시스템을 다운시키는 바이러스의 일종으로, 분산 서비스 거부 공격, 버퍼 오버플로 공격, 슬래머 등이 웜 공격의 한 형태임
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 의미함
키로거 공격 (Key Logger Attack)	컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드, 계좌번호, 카드번호 등과 같은 개인의 중요한 정보를 몰래 빼가는 해킹 공격
랜섬웨어 (Ransomware)	인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 파일 등을 암호화해 사용자가 열지 못하게 하는 프로그램으로, 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 함
백도어 (Back Door, Trap Door)	• 시스템 설계자가 서비스 기술자나 유지 보수 프로그램 작성자(Programmer)의 액세스 편의를 위해 시스템 보안을 제거하여 만들어놓은 비밀 통로로, 컴퓨터 범죄에 악용되기도 함 • 백도어 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 없음

2020년 1, 2회 기사 필기

1. 컴퓨터 사용자의 키보드 움직임을 탐지해 ID, 패스워드 등 개인의 중요한 정보를 몰래 빼가는 해킹 공격을 무엇이라고 하는지 쓰시오.

답 :

2020년 1, 2회 기사 필기

2. 다음 설명의 정보 보안 침해 공격 관련 용어가 무엇인지 쓰시오.

> 인터넷 사용자의 컴퓨터에 침입해 내부 문서 파일 등을 암호화해 사용자가 열지 못하게 하는 공격으로, 암호 해독용 프로그램의 전달을 조건으로 사용자에게 돈을 요구하기도 한다.

답 :

2020년 1, 2회 기사 필기

3. 시스템 설계자가 서비스 기술자나 유지 보수 프로그램 작성자(Programmer)의 액세스 편의를 위해 시스템 보안을 제거하여 만들어놓은 비밀 통로를 백도어(Back Door)라고 한다. 백도어 탐지 방법 3가지를 쓰시오.

답 :

정답 1. 키로거 공격(Key Logger Attack) 2. 랜섬웨어(Ransomware) 3. 무결성 검사, 로그 분석, SetUID 파일 검사

1. 다음은 소프트웨어 개발 보안 관련 기관에 대한 설명이다. 괄호(①~②)에 들어갈 알맞은 기관을 쓰시오.

발주기관	소프트웨어 개발 보안의 계획을 수립한다.
(①)	소프트웨어 개발 보안 정책 및 가이드를 개발한다.
사업자	소프트웨어 개발 보안 관련 기술 수준 및 적용 계획을 명시한다.
(②)	소프트웨어 개발 보안 정책을 총괄한다.
감리법인	감리 계획을 수립하고 협의한다.

답
① :
② :

정답 1. ① 한국인터넷진흥원(KISA) ② 행정안전부

[핵심123] 소프트웨어 개발 보안

- 소프트웨어 개발 과정에서 발생할 수 있는 보안 취약점을 최소화하여 보안 위협으로부터 안전한 소프트웨어를 개발하기 위한 일련의 보안 활동을 의미한다.
- 소프트웨어 개발 보안은 데이터의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 유지하는 것을 목표로 한다.
- 소프트웨어 개발 보안 관련 기관

행정안전부	소프트웨어 개발 보안 정책을 총괄한다.
한국인터넷진흥원(KISA)	소프트웨어 개발 보안 정책 및 가이드를 개발한다.
발주기관	소프트웨어 개발 보안의 계획을 수립한다.
사업자	소프트웨어 개발 보안 관련 기술 수준 및 적용 계획을 명시한다.
감리법인	감리 계획을 수립하고 협의한다.

[핵심124] 소프트웨어 개발 보안 활동 관련 법령

개인정보 보호법	개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호한다.
정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망의 이용 촉진 및 정보통신 서비스를 이용하는 이용자들의 개인정보를 보호한다.
신용정보의 이용 및 보호에 관한 법률	개인 신용정보의 효율적 이용과 체계적인 관리를 통해 정보의 오남용을 방지한다.
위치정보의 보호 및 이용 등에 관한 법률	개인 위치정보의 안전한 이용 환경을 조성하여 정보의 유출이나 오남용을 방지한다.
표준 개인정보 보호 지침	개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부사항을 규정한다.

개인정보의 안전성 확보 조치 기준	개인정보 처리자가 개인정보를 처리하는데 있어 개인정보가 분실, 도난, 유출, 위조, 변조, 훼손되지 않도록 안전성 확보에 필요한 기술적, 관리적, 물리적 안전조치에 관한 최소한의 기준을 규정한다.
개인정보 영향평가에 관한 고시	개인정보 영향평가를 위한 평가기관의 지정, 영향평가의 절차 등에 관한 세부기준을 규정한다.

1. 소프트웨어 개발 보안 활동 관련 법령 중 개인정보 보호법이 무엇인지 간략히 서술하시오.

답 :

정답 1. 개인정보 보호법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하는 법령이다.

[핵심125] Secure SDLC

- 보안상 안전한 소프트웨어를 개발하기 위해 SDLC에 보안 강화를 위한 프로세스를 포함한 것을 의미한다.
- SDLC(Software Development Life Cycle, 소프트웨어 개발 생명주기) : 소프트웨어 개발 방법론의 바탕이 되는 것으로, 소프트웨어를 개발하기 위해 정의하고 운용, 유지보수 등의 전 과정을 각 단계별로 나눈 것
- Secure SDLC는 요구사항 분석, 설계, 구현, 테스트, 유지 보수 등 SDLC 전체 단계에 걸쳐 수행되어야 할 보안 활동을 제시한다.

단계	보안 활동
요구사항 분석 단계	• 보안 항목에 해당하는 요구사항을 식별하는 작업을 수행한다. • 전산화되는 정보가 가지고 있는 보안 수준을 보안 요소별로 등급을 구분하여 분류한다.
설계 단계	식별된 보안 요구사항들을 소프트웨어 설계서에 반영하고, 보안 설계서를 작성한다.
구현 단계	• 표준 코딩 정의서 및 소프트웨어 개발 보안 가이드를 준수하며, 설계서에 따라 보안 요구사항들을 구현한다. • 시큐어 코딩(Secure Coding) : 소프트웨어의 구현 단계에서 발생할 수 있는 보안 취약점들을 최소화하기 위해 보안 요소들을 고려하며 코딩하는 것
테스트 단계	설계 단계에서 작성한 보안 설계서를 바탕으로 보안 사항들이 정확히 반영되고 동작되는지 점검한다.
유지 보수 단계	이전 과정을 모두 수행하였음에도 발생할 수 있는 보안 사고들을 식별하고, 사고 발생 시 이를 해결하고 보안 패치를 실시한다.

1. 다음에 제시된 내용은 Secure SDLC의 수행 과정 중 어느 단계에서의 보안 활동인지 쓰시오.

> • 표준 코딩 정의서 및 소프트웨어 개발 보안 가이드를 준수하며, 설계서에 따라 보안 요구사항들을 구현한다.
> • 개발 과정 중에는 지속적인 단위 테스트를 통해 소프트웨어에 발생할 수 있는 보안 취약점을 최소화해야 한다.

답 :

2. 다음은 무엇에 대한 설명인지 가장 적합한 용어를 쓰시오.

> • 소프트웨어의 구현 단계에서 발생할 수 있는 보안 취약점들을 최소화하기 위해 보안 요소들을 고려하며 코딩하는 것을 의미한다.
> • 보안 취약점을 사전에 대응하여 안정성과 신뢰성을 확보하기 위해 사용된다.

답 :

정답 1. 구현 단계 2. 시큐어 코딩(Secure Coding)