☑ 만든이 : 지안에듀 조현준

- 성균관대학교 정보공학 전공
- CISA, CISSP, 정보보안기사

☑ 저서

- TopSpot 정보보호론 이론편/문제편
- 알기쉬운 정보보안기사 필기편/실기편(알기사)
- TopSpot 자료구조론 이론편/쪽집게 기출문제

☑ 무료 동영상 안내

- 지안에듀 홈페이지 이용(www.zianedu.com)
  - [빅데이터 3.2] 조현준 정보보호론 연도별 기출문제 풀이강의(전산 전직렬)
- 유튜브 자투리10분 기출20문항정리
  - 유튜브에서 조현준 정보보호론 검색

정보보호론 간단 총평

1. 출제경향 분석

시험범위는 계속 넓어져 정보보안기사를 따라가고 있습니다. 정보보호조치 문제는 정보보안기사에 출제되었던 문제를 약간 변형해서 출제된 것들도 있습니다.(알기사, 조현준 저 참조) Process Explorer 분석도구는 공무원 사이버 채용에서 나온 문제를 변형해서 출제된 문제입니다. 향후 정보보호론은 범위는 넓어지고, 난이도는 계속 올라간다고 생각하시면 될 것 같습니다.

2. 난이도

전체적인 난이도는 전년도 국가직 시험보다는 어려운 수준으로 판단됩니다. 문항에서 옳은 것을 고르라는 문제가 많아 시간이 걸리고, 실수가 좀 있을 것 같습니다. 기본에 충실하고 응용문제(800제, 모의고사 등)를 많이 푸신 분들은 고득점이 나왔을 것 같습니다. 하지만 쉬운 기출문제(시중 기출문제집이 어려운 문제는 빼는 경향이 있음) 위주로만 이론정리를 하신 분들은 어렵게 느껴졌을 것으로 생각됩니다.

3. 향후 학습방향

다음 시험을 위해서 본인의 위치를 냉철히 판단해보고 약점을 보완하셔야 합니다. 약간은 주관적일 수 있지만 이번 시험을 기준으로 80점 이상을 받으신 분들은 그 동안의 공부의 방향이 맞다고 보여집니다. 그러나 60점이하로 받으신 분들은 공부방법을 다시 한번 생각해 볼 필요가 있습니다.

1.

2020년 국가직 9급 정보보호론

-2020년 7월 11일 시행

1. ○△× 20.국가.9급

정보보호 위험관리에 대한 설명으로 옳지 않은 것은?

① 자산은 조직이 보호해야 할 대상으로 정보, 하드웨어, 소프트웨어, 시설 등이 해당한다.
② 위험은 자산에 손실이 발생할 가능성과 관련되어 있으나 이로 인한 부정적인 영향을 미칠 가능성과는 무관하다.
③ 취약점은 자산이 잠재적으로 가진 약점을 의미한다.
④ 정보보호대책은 위협에 대응하여 자산을 보호하기 위한 관리적, 기술적, 물리적 대책을 의미한다.

오답피하기 ② 위험(risk)이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 말한다. 위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 그들이 어떻게 위험의 규모에 영향을 미치는지를 분석하여야 한다.

정답 ②

이론: 618p 적중, 최고수준800제: 355번 유사

※ 지문이나 문제의 유사도에 따라 적중 > 유사 > 응용으로 구분함. 최고수준800제는 학원 내부교재임.

2. ○△× 20.국가.9급

공개키 암호화에 대한 설명으로 옳지 않은 것은?

① ECC(Elliptic Curve Cryptography)와 Rabin은 공개키 암호 방식이다.
② RSA는 소인수 분해의 어려움에 기초를 둔 알고리즘이다.
③ 전자서명 할 때는 서명하는 사용자의 공개키로 암호화한다.
④ ElGamal은 이산대수 문제의 어려움에 기초를 둔 알고리즘이다.

◦ 전자서명에서 서명자는 자신의 개인키를 이용하여 문서에 서명을 하게 되는데 이때 서명 알고리즘을 사용한다. 검증하는 사람은 역으로 서명자의 공개키를 이용하여 문서를 검증한다. 이때 검증 알고리즘을 이용한다.

오답피하기 ③ 전자서명을 할 때는 서명하는 사용자의 개인키로 암호화한다.

정답 ③

이론: 109p 적중, 기출: 102번(기) 적중

3. ○△× 20.국가.9급

X.509 인증서 형식 필드에 대한 설명으로 옳은 것은?

① Issuer name – 인증서를 사용하는 주체의 이름과 유효기간 정보
② Subject name – 인증서를 발급한 인증기관의 식별 정보
③ Signature algorithm ID – 인증서 형식의 버전 정보
④ Serial number – 인증서 발급 시 부여된 고유번호 정보

오답피하기 ① 발행자 이름(Issuer name)은 인증서 발행자(통상적으로 인증기관)의 이름을 나타낸다. ② 주체 이름(Subject name)은 인증서에 대한 사용자(피발급자)의 이름을 나타낸다. ③ 서명 알고리즘 식별자(Signature Algorithm ID)는 인증기관이 인증서를 서명하기 위한 알고리즘과 알고리즘 식별자이다.

정답 ④

이론: 123p 적중, 기출: 115번(기) 응용, 최고수준800제: 63번 유사

4. ○△× 20.국가.9급

일방향 해시함수를 사용하여 비밀번호를 암호화할 때 salt라는 난수를 추가하는 이유는?

① 비밀번호 사전공격(Dictionary attack)에 취약한 문제를 해결할 수 있다.
② 암호화된 비밀번호 해시 값의 길이를 줄일 수 있다.
③ 비밀번호 암호화의 수행 시간을 줄일 수 있다.
④ 비밀번호의 복호화를 빠르게 수행할 수 있다.

오답피하기 ① 솔트는「소금」이라는 뜻이다. 요리에 소금을 뿌려 맛을 바꾸는 것처럼 솔트는 의사난수 생성기로 만들어지는 랜덤한 수로, 키(KEK)를 만들 때에 패스워드와 함께 일방향 해시함수에 입력된다. 솔트는 사전공격 또는 레인보 테이블을 이용한 공격을 막기 위해 존재한다. 사전공격이란 미리 키 후보를 계산해서 준비해두는 방법을 말한다.

정답 ①

이론: 129p 적중, 기출: 117번(기) 유사

5. ○△× 20.국가.9급

윈도우 운영체제에서 TPM(Trusted Platform Module)에 대한 설명으로 옳지 않은 것은?

① TPM의 공개키를 사용하여 플랫폼 설정정보에 서명함으로써 디지털 인증을 생성한다.
② TPM은 신뢰 컴퓨팅 그룹(Trusted Computing Group)에서 표준화된 개념이다.
③ TPM은 키 생성, 난수 발생, 암복호화 기능 등을 포함한 하드웨어 칩 형태로 구현할 수 있다.
④ TPM의 기본 서비스에는 인증된 부트(authenticated boot), 인증, 암호화가 있다.

신뢰 플랫폼 모듈(TPM)

◦ 신뢰 플랫폼 모듈(trusted platform module, TPM)은 신뢰 컴퓨팅 그룹(Trusted Computing Group)이라는 산업체 컨소시엄에 의해 표준화된 개념이다.
◦ TPM은 신뢰 컴퓨팅을 위한 하드웨어/소프트웨어 방법에서 핵심이 되는 하드웨어 모듈이다. 사실 지금 신뢰 컴퓨팅(trusted computing, TC)이란 용어는 이런 유형의 하드웨어/소프트웨어 방법을 말하기 위해 산업체에서 사용되고 있다.
◦ TC 방법은 개인용 컴퓨터의 마더보드, 스마트카드, 메인 프로세서에 결합된 TPM칩을 사용하며, TPM과 작업하도록 인증 또는 승인된 하드웨어/소프트웨어를 함께 사용한다.
◦ TPM은 시스템에 데이터를 전달하는 취약한 구성요소(저장 장치, 메모리, 오디오/비디오 하드웨어 등)와 공유하는 키를 생성한다. 키는 기계에서 사용되는 데이터를 암호화하기 위해 사용된다.
◦ 위에서 언급한 특징을 위해 TC는 세 개의 기본 서비스인 인증된 부트(authenticated boot), 인증(certification), 암호(encryption)를 제공한다.

오답피하기 ① 일단 TPM에 의해 설정이 완성되고 로그인되면, TPM은 다른 부분의 설정을 인증할 수 있다. TPM은 TPM의 사설키(private key)를 사용하여 설정 정보에 서명함으로써 디지털 인증을 만들 수 있다.(공개키 아님)

정답 ①

이론: 191p 적중, 기출: 159번(기), 400번(심) 응용, 최고수준800제: 108번 응용

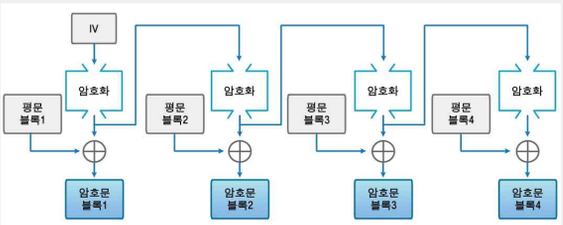
6. ○△× 20.국가.9급

키 k에 대한 블록 암호 알고리즘 E_k, 평문블록 M_i, Z_0는 초기벡터, $Z_i = E_k(Z_{j-1})$가 주어진 경우, 이때 $i = 1,2,\cdots,n$에 대해 암호블록 C_i를 $C_i = Z_i \oplus M_i$로 계산하는 운영모드는? (단, $\oplus$는 배타적 논리합이다)

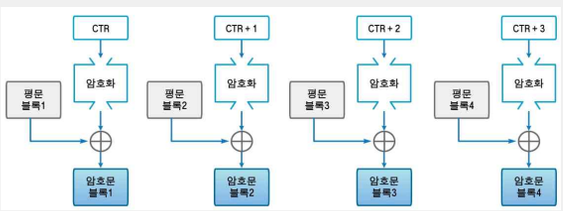
① CBC
② ECB
③ OFB
④ CTR

OFB 모드와 CTR 모드

◦ OFB 모드 암호화



◦ CTR 모드 암호화



오답피하기 ③ CTR 모드는 카운터를 암호화한 후 평문 블록과 암호화한다. OFB 모드는 초기화벡터를 암호화한 후 평문 블록과 암호화한다. 보기는 이를 수식으로 표현한 것이다.

정답 ③

이론: 64,66p 응용, 최고수준800제: 23번 유사, 모의고사: 2회 18번 유사

7. ○△× 20.국가.9급

정보보호 시스템 평가 기준에 대한 설명으로 옳은 것은?

① ITSEC의 레인보우 시리즈에는 레드 북으로 불리는 TNI(Trusted Network Interpretation)가 있다.
② ITSEC은 None부터 B2까지의 평가 등급으로 나눈다.
③ TCSEC의 EAL2 등급은 기능시험 결과를 의미한다.
④ TCSEC의 같은 등급에서는 뒤에 붙는 숫자가 클수록 보안 수준이 높다.

TCSEC

◦ TCSEC은 보증 수준을 계층적으로 나눈 분류 시스템을 제공한다.
  – A 검증된 보호(Verified protection)
  – B 강제적 보호(Mandatory protection)
  – C 임의적 보호(Discretionary protection)
  – D 최소 보호(Minimal security)
◦ 분류 A는 최고 수준의 보증을 나타내고, D는 최저 수준의 보증을 나타낸다.
◦ 각각의 분류 그룹은 시스템이 특정한 등급을 성취하기 위해 충족해야 하는 관련된 요구사항을 가지는 숫자로 표기된 등급을 가진다.
◦ 보다 높은 숫자를 가진 등급이 더 훌륭한 신뢰와 보증을 제공한다. 따라서 B2는 B1보다 높은 신뢰를 제공하고, C2는 C1보다 높은 신뢰를 제공한다.

오답피하기 ① ITSEC이 아닌 TCSEC의 레인보우 시리즈에는 레드 북으로 불리는 TNI(Trusted Network Interpretation)가 있다. ② ITSEC은 E0부터 E6까지의 평가 등급으로 나눈다. ③ CC의 EAL2 등급은 구조적 시험(Structurally tested)을 의미한다.

정답 ④

이론: 641p 적중, 기출: 32번(심) 유사, 최고수준800제: 362번 응용

8. ○△× 20.국가.9급

SSL(Secure Socket Layer)의 Handshake 프로토콜에서 클라이언트와 서버 간에 논리적 연결 수립을 위해 클라이언트가 최초로 전송하는 ClientHello 메시지에 포함되는 정보가 아닌 것은?

① 세션 ID
② 클라이언트 난수
③ 압축 방법 목록
④ 인증서 목록

➡ ClientHello 메시지 포함 정보
◦ 클라이언트를 지원할 수 있는 가장 높은 SSL 버전 번호
◦ 마스터 비밀을 생성하는 데 사용될 수 있는 32바이트 난수(클라이언트로부터)
◦ 세션을 나타내는 세션 ID
◦ 클라이언트를 지원할 수 있는 알고리즘 목록인 암호 그룹
◦ 클라이언트가 지원할 수 있는 압축 방법의 목록

오답피하기 ④ 인증서 목록은 ClientHello 메시지 포함 정보가 아니다.

정답 ④

이론: 534p 적중, 최고수준800제: 295번 적중

9. ○△× 20.국가.9급

「개인정보 보호법」상 기본계획에 대한 조항의 일부이다. ㉠, ㉡에 들어갈 내용을 바르게 연결한 것은?

보기

제9조(기본계획) ①보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 (㉠)년마다 개인정보 보호 기본계획(이하 "기본계획"이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.
②기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. (㉡)
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

	㉠	㉡
①	1	개인정보 보호 자율규제의 활성화
②	3	개인정보 보호 자율규제의 활성화
③	1	개인정보 활용·폐지를 위한 계획
④	3	개인정보 활용·폐지를 위한 계획

➡ 제9조(기본계획)
① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획을 관계 중앙행정기관의 장과 협의하여 수립한다.
② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.
1. 개인정보 보호의 기본목표와 추진방향
2. 개인정보 보호와 관련된 제도 및 법령의 개선
3. 개인정보 침해 방지를 위한 대책
4. 개인정보 보호 자율규제의 활성화
5. 개인정보 보호 교육·홍보의 활성화
6. 개인정보 보호를 위한 전문인력의 양성
7. 그 밖에 개인정보 보호를 위하여 필요한 사항

오답피하기 ② 기본계획은 개인정보보호의 기본목표와 추진방향을 큰 틀에서 제시하고, 이를 달성하기 위한 법·제도의 개선방안, 개인정보 침해 방지대책, 개인정보보호 자율규제의 활성화방안, 개인정보 보호 교육·홍보방안, 전문인력 양성 및 기타 개인정보보호를 위하여 필요한 사항 등에 관한 중기적 관점의 계획을 포함하여야 한다.

정답 ②

이론: 675p 응용, 모의고사: 11회2번 응용, 강의: 강조

10. ○△× 20.국가.9급

소수 p = 13, 원시근 g = 2, 사용자 A와 B의 개인키가 각각 3, 2일 때, Diffie-Hellman 키 교환 알고리즘을 사용하여 계산한 공유 비밀키는?

① 6
② 8
③ 12
④ 16

◦ Diffie-Hellman 알고리즘에 의해 비밀키를 구하면 수식은 다음과 같다.

오답피하기 ③ Diffie-Hellman 알고리즘에 의해 비밀키를 구하면 다음과 같다.

$2^{2\times 3} \bmod 13 = 2^6 \bmod 13 = 64 \bmod 13 = 12$

정답 ③

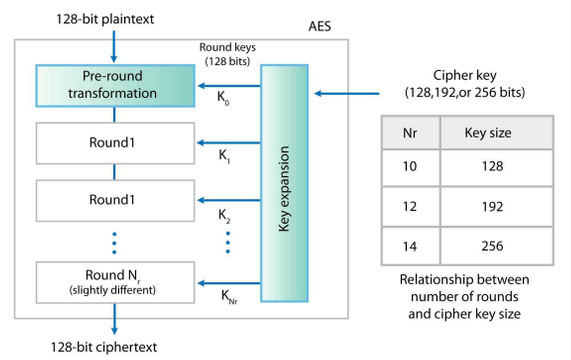
이론: 73p 응용, 기출: 605번(심) 적중

11. ○△× 20.국가.9급

NIST의 AES(Advanced Encryption Standard) 표준에 따른 암호화 시 암호키(cipher key) 길이가 256비트일 때 필요한 라운드 수는?

① 8
② 10
③ 12
④ 14

AES 암호의 구조도



오답피하기 ④ AES 알고리즘은 라운드 수에 따라서 키 길이가 다르다. (10라운드, 128비트), (12라운드, 192비트), (14라운드, 256비트)

정답 ④

이론: 53p 적중, 기출: 575번, 577번 유사

12. ○△× 20.국가.9급

IPsec의 ESP(Encapsulating Security Payload)에 대한 설명으로 옳지 않은 것은?

① 인증 기능을 포함한다.
② ESP는 암호화를 통해 기밀성을 제공한다.
③ 전송 모드의 ESP는 IP 헤더를 보호하지 않으며, 전송계층으로부터 전달된 정보만을 보호한다.
④ 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 공개키를 사용한다.

◦ 전송 모드(transport mode)는 호스트와 호스트 간의 전송 경로를 보호하는 방법으로서 계층 간의 캡슐화 과정을 통하여 상위 계층의 TPDU(Transport Protocol Data Unit) 데이터(TCP 및 응용 계층의 데이터)에 대하여 암호화 데이터 및 인증용 데이터를 생성하는 방법이다.
◦ Authentication Data : IP패킷에 대한 무결성을 조사하기 위한 값(Integrity Check Value)을 포함하는 필드로 MD5, SHA-1 등과 같은 해시함수를 사용해 MAC(Message Authentication Code)을 생성하여 포함한다.

오답피하기 ④ 터널 모드의 ESP는 Authentication Data를 생성하기 위해 해시 함수와 대칭키를 사용한다.(MAC을 생성하기 위해 해시함수와 대칭키가 필요함)

정답 ④

이론: 484p 유사, 최고수준800제: 634번 응용

13. ○△× 20.국가.9급

네트워크나 컴퓨터 시스템의 자원 고갈을 통해 시스템 성능을 저하시키는 공격에 해당하는 것만을 모두 고르면?

보기
ㄱ. Ping of Death 공격
ㄴ. Smurf 공격
ㄷ. Heartbleed 공격
ㄹ. Sniffing 공격

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄷ
④ ㄴ, ㄹ

◦ 하트블리드(Heartbleed)는 2014년 4월에 발견된 오픈 소스 암호화 라이브러리인 OpenSSL의 소프트웨어 버그이다. 발표에 따르면, 인증기관에서 인증받은 안전한 웹 서버의 약 17%(약 50만대)가 이 공격으로 개인키와 세션 쿠키 및 암호를 도난당할 수 있는 상태이다. 오픈 SSL은 인터넷을 통해 데이터를 송수신할 때 원본 내용을 암호화할 수 있게 해주는 방법(프로토콜)이다. 이슈가 된 하트블리드는 오픈 SSL에서 클라이언트(PC)와 웹 서버 간 암호화 통신이 제대로 이뤄지는지 확인하기 위해 사용되는 프로토콜인 '하트비트(HeartBeat)'에서 발견된 취약점이다.

오답피하기 ① Ping of Death 공격은 핑(Ping)을 이용하여 ICMP 패킷을 정상적인 크기(65,535 bytes)보다 아주 크게 만들어 공격하는 것이고, Smurf 공격은 공격대상자가 스푸핑된 소스 IP로부터 ICMP reply를 동시에 수신하는 현상을 갖는 DoS 공격의 사례이다.

정답 ①

이론: 405~408p 적중, 기출: 285번~288번 유사

14. ○△× 20.국가.9급

다음 설명에 해당하는 위험분석 및 평가 방법을 옳게 짝 지은 것은?

보기
ㄱ. 전문가 집단의 토론을 통해 정보시스템의 취약성과 위협요소를 추정하여 평가하기 때문에 시간과 비용을 절약할 수 있지만, 정확도가 낮다.
ㄴ. 이미 발생한 사건이 앞으로 발생한다는 가정하에 수집된 자료를 통해 위험 발생 가능성을 예측하며, 자료가 많을수록 분석의 정확도가 높아진다.
ㄷ. 어떤 사건도 기대하는 대로 발생하지 않는다는 사실에 근거하여 일정 조건에서 위협에 대해 발생 가능한 결과들을 예측하며, 적은 정보를 가지고 전반적인 가능성을 추론할 수 있다.

	ㄱ	ㄴ	ㄷ
①	순위 결정법	과거자료 분석법	기준선 접근법
②	순위 결정법	점수법	기준선 접근법
③	델파이법	과거자료 분석법	시나리오법
④	델파이법	점수법	시나리오법

오답피하기 ③ 정성적 위험분석 및 평가 방법 중 델파이법과 시나리오법, 정량적 위험분석 및 평가 방법 중 과거자료 분석법에 대한 설명이다.

정답 ③

이론: 628p 적중, 기출: 16번(심) 유사

15. ○△× 20.국가.9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제19조(국내대리인 지정 대상자의 범위)에 명시된 자가 아닌 것은?

① 전년도(법인인 경우에는 전(前) 사업연도를 말한다) 매출액이 1,000억 원 이상인 자
② 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억 원 이상인 자
③ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상인 자
④ 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품·서류 등을 제출하도록 요구받은 자

◘ 제32조의5(국내대리인의 지정)
① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 대리하는 자를 서면으로 지정하여야 한다.
② 국내대리인은 국내에 주소 또는 영업소가 있는 자로 한다.
③ 제1항에 따라 국내대리인을 지정한 때에는 다음 각 호의 사항 모두를 인터넷 사이트 등에 공개하여야 한다.
1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명)
2. 국내대리인의 주소(법인의 경우에는 영업소 소재지), 전화번호 및 전자우편 주소

◘ 시행령 제19조(국내대리인 지정 대상자의 범위)
① 법 제32조의5제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 전년도[법인인 경우에는 전(前) 사업연도를 말한다] 매출액이 1조원 이상인 자
2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
3. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 자
4. 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제64조제1항에 따라 방송통신위원회로부터 관계 물품·서류 등을 제출하도록 요구받은 자

오답피하기 ① 전년도[법인인 경우에는 전(前) 사업연도를 말한다] 매출액이 1,000억원이 아닌 1조원 이상인 자가 해당한다.

정답 ①

이론: 713p 응용, 최고수준800제: 388번 응용, 강의: 강조

16. ○△× 20.국가.9급

다음 설명에 해당하는 악성코드 분석도구를 옳게 짝 지은 것은?

보기
ㄱ. 가상화 기술 기반으로 악성코드의 비정상 행위를 유발하는 실험과정에서 발생할 수 있는 분석시스템으로의 침해를 방지하여 통제된 환경과 분석 기능을 제공한다.
ㄴ. 악성코드의 행위를 추출하기 위해 실제로 해당 코드를 실행함으로써 발생하는 비정상 행위 혹은 시스템 동작 환경의 변화를 살펴볼 수 있는 동적 분석 기능을 제공한다.

	ㄱ	ㄴ
①	Sandbox	Process Explorer
②	Sandbox	Burp Suite
③	Blackbox	IDA Pro
④	Blackbox	OllyDBG

◦ Paros와 Burp suite는 웹 취약점 스캐너이다.
◦ IDA(Interactive DisAssembler) Pro는 컴퓨터 소프트웨어용 디스어셈블러이다. 디스어셈블러는 기계어 코드로부터 어셈블리어 소스 코드를 생성한다.
◦ OllyDbg(만든이인 Oleh Yuschuk의 이름을 딴)는 바이너리 코드 분석을 위한 x86 디버거로서, 소스 코드가 없을 때 유용하게 사용된다.

오답피하기 ① Sandbox는 응용 프로그램이 실행될 때 일종의 가상머신 안에서 실행되는 것처럼 원래의 운영체제와 완전히 독립되어 실행되는 형태를 말한다. 컴퓨터 메모리에서 애플리케이션 호스트 시스템에 해를 끼치지 않고 작동하는 것이 허락된 보호받는 제한 구역을 가리킨다. Process Explorer는 프로세스를 관리할 수 있는 프로그램이다. 현재 실행중인 프로세스를 파악하여 해당 프로세스의 우선권을 변경, 정지, 강제 종료 등을 할 수 있도록 지원한다. 프로세스를 관리하는 Process Explorer가 악성코드 분석 시에도 유용하게 사용되곤 한다.

정답 ①

이론: 601p 응용, 기출: 317p(14번) 응용

17. ○△× 20.국가.9급

윈도우 운영체제의 계정 관리에 대한 설명으로 옳은 것은?

① 'net accounts guest /active:no' 명령은 guest 계정을 비활성화한다.
② 'net user' 명령은 시스템 내 사용자 계정정보를 나열한다.
③ 'net usergroup' 명령은 시스템 내 사용자 그룹정보를 표시한다.
④ 컴퓨터/도메인에 모든 접근권한을 가진 관리자 그룹인 'Admin'이 기본적으로 존재한다.

◦ net accounts: 사용자 계정 데이터베이스를 업데이트하고 모든 계정에 대해 암호와 로그온 요청을 수정한다. net accounts 명령을 매개 변수 없이 입력하면 암호, 로그온 제한 및 도메인 정보에 대한 현재 설정을 표시할 수 있다.

오답피하기 ① guest 계정을 비활성화 하기 위해서는 'net user guest /active:no', 활성화 하기 위해서는 'net user guest /active:yes' 명령을 사용한다. ③ 윈도우에서 그룹 관리 명령어는 net localgroup과 net group이 있다. net localgroup은 로컬 컴퓨터 그룹에 사용하고, net group은 도메인 그룹에 사용한다. ④ 컴퓨터/도메인에 모든 접근권한을 가진 관리자 그룹인 'Administrators'이 기본적으로 존재한다.

정답 ②

기출: 427번 응용

18. ○△× 20.국가.9급

커버로스(Kerberos) 프로토콜에 대한 설명으로 옳지 않은 것은?

① 양방향 인증방식의 문제점을 보완하여 신뢰하는 제3자 인증 서비스를 제공한다.
② 사용자의 패스워드를 추측하거나 캡처하지 못하도록 일회용 패스워드를 제공한다.
③ 버전 5에서는 이전 버전과 달리 DES가 아닌 다른 암호 알고리즘을 사용할 수 있다.
④ 클라이언트는 사용자의 식별정보를 평문으로 인증 서버(Authentication Server)에 전송한다.

오답피하기 ② 커버로스는 대칭키 암호를 사용하고 점대점(end-to-end) 보안을 제공한다. 비록 인증을 위해 패스워드의 사용을 허용하지만, 특별히 네트워크를 통해 패스워드를 전송해야 할 필요를 제거하기 위해 설계되었다. 대부분의 커버로스 구현은 일회용 패스워드가 아닌 공유된 비밀키를 가지고 동작한다.

정답 ②

이론: 156p 응용, 기출: 520번~523번(심) 유사

19. ○△× 20.국가.9급

임의적 접근 통제(Discretionary Access Control) 모델에 대한 설명으로 옳은 것은?

① 주체가 소유권을 가진 객체의 접근 권한을 다른 사용자에게 부여할 수 있으며, 사용자 신원에 따라 객체의 접근을 제한한다.
② 주체와 객체가 어떻게 상호 작용하는지를 중앙 관리자가 관리하며, 사용자 역할을 기반으로 객체의 접근을 제한한다.
③ 주체와 객체에 각각 부여된 서로 다른 수준의 계층적인 구조의 보안등급을 비교하여 객체의 접근을 제한한다.
④ 주체가 접근할 수 있는 상위와 하위의 경계를 설정하여 해당 범위 내 임의 객체의 접근을 제한한다.

◘ Lattice-Based Model
◦ 역할에 할당된 민감도 레벨에 의해 결정된다.(주체 및 객체에게 보안클래스 부여, 정보흐름 통제)
◦ 주체와 객체의 관계에 의거하여 접근할 수 있는 Upper bound와 Lower bound를 설정하여 접근을 제어하는 것이다.
◦ 예를 들어, 핵무기와 관련된 임무를 수행하고 있는 사람은 이와 관련된 상, 하위 정보로만 접근통제한다.

오답피하기 ②, ③ MAC에 대한 설명이고, ④ Lattice-Based Model에 대한 설명이다.

정답 ①

이론: 162p 적중, 기출: 142번(기) 적중

20. ○△× 20.국가.9급

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제45조(정보통신망의 안정성 확보 등)에 정보보호조치에 관한 지침에 포함되어야 할 보호조치로 명시되지 않은 것은?

① 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
② 사전 정보보호대책 마련 및 보안조치 설계·구현 등을 위한 기술적 보호조치
③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
④ 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치

◘ 제45조(정보통신망의 안정성 확보 등)
① 다음 각 호의 어느 하나에 해당하는 자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.
1. 정보통신서비스 제공자
2. 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 대통령령으로 정하는 기기·설비·장비를 제조하거나 수입하는 자
② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침을 정하여 고시하고 제1항 각 호의 어느 하나에 해당하는 자에게 이를 지키도록 권고할 수 있다.
③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.
1. 정당한 권한이 없는 자가 정보통신망에 접근·침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치·운영 등 기술적·물리적 보호조치
2. 정보의 불법 유출·위조·변조·삭제 등을 방지하기 위한 기술적 보호조치
3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치
4. 정보통신망의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치
5. 정보통신망연결기기등의 정보보호를 위한 기술적 보호조치
④ 과학기술정보통신부장관은 관계 중앙행정기관의 장에게 소관 분야의 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준에 정보보호지침의 내용을 반영할 것을 요청할 수 있다.

오답피하기 ② 정보보호지침에 사전 정보보호대책 마련 및 보안조치 설계·구현 등을 위한 기술적 보호조치는 없다.

정답 ②

이론: 711p 적중, 모의고사: 15회 1번 적중

[전산직 공채 총정리 (3년간)]

시험종류			2017년				2018년				2019년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8~2.22	3.11	90~	3	3.5 ~ 3.15	4.14	70점후	-				컴일,네트워크보안,시스템보안	필기 합격선이 2016년, 2017년 모두 90점이상 공무원기출+정보보안기사필기 문제집에서 다수 출제
해경	전산	7급					1	3.5 ~ 3.15	4.14	-	-				서류전형	
국가직	전산개발	9급	35	2.1 ~ 2.6	4.8	84	50	2.20 ~ 2.23	4.7	73	83	2.20~2.23	4.6	83	국,영,한,컴일,정보	전산개발, 정보보호직 동시 접수 불가
국가직	정보보호	9급	7	2.1 ~ 2.6	4.8	83	5	2.20 ~ 2.23	4.7	69	8	2.20~2.23	4.6	75	국,영,한,네트워크보안,시스템보안	전산개발, 정보보호직 동시 접수 불가
지방직	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.12 ~ 3.16	5.19	시도별	시도별	4.8~4.12	6.15	시도별	국,영,한,컴일,정보	지방직, 교육청 동시 접수 가능, 동시 응시는 불가
교육청	전산개발	9급	시도별	4.17~4.21	6.17	시도별	시도별	3.26 ~ 3.30	5.19	시도별	시도별	4.15~4.19	6.15	시도별	국,영,한,컴일,정보	거주지 제한 있음, 2019년부터 지방직과 시험지 동일
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12 ~ 3.16	6.23	88	18	3.12~3.18	6.15	76	국,영,한,컴일,정보	거주지 제한 없음, 2019년부터 지방직 시험일자와 동일
군무원	국방부	7급					2	6.7 ~ 6.12	8.11	77	14	4.12~4.17	6.22	74	국,자구,DB,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	국방부	9급	11	4.17~4.21	7.1	72	13	6.7 ~ 6.12	8.11	77.33	8	4.12~4.17	6.22	78.67	국,컴일,정보	영어와 한국사는 공인시험으로 대체 2018년부터 프로그래밍언어론→정보보호론 교체
군무원	육군	9급	24	4.24~4.28	7.1	68	18	6.7 ~ 6.12	8.11	74.67	56	4.12~4.17	6.22	77.33	국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7 ~ 6.12	8.11	73.33	19	4.12~4.17	6.22	73.33	국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7 ~ 6.12	8.11	73.33	21	4.12~4.17	6.22	76	국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25	83	3	5.20~5.24	8.24		국,영,한,컴일,정보	객관식 5지 선다형 출제
국가직	전산개발	7급	26	6.5~6.9	8.26	75.83	29	7.14~7.17	8.18	74.16	30	7.14~7.17	8.17		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-	10	7.11~7.30	8.11	-	10	5.24~6.3	7.2		실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격, 경력채용
경찰	사이버(보안)	경장					135	7.20~7.31	9.1	시도별	79	7.12~7.22	8.10		필기(2): 정보보호론,시스템네트워크보안 선택(1): 정보보호관리및법규,디지털포렌식개론, 데이터베이스론	객관식 과목별 20문항, 경력채용 필기시험(50%)→신체,적성,체력(25%)→면접(25%)
지방직(서울)	전산개발	7급					3	3.12~3.16	6.23	80	4	8.6~8.9	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 없음
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13	76.42	2	8.5~8.7	10.12		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님, 거주지 제한 있음
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15	312.5(1차) 463.5(2차)	5	8.20~8.29	10.5		필수 : 정보보호론(객), 시스템네트워크보안㈜ 선택 : DB, 통신이론, 소공 중 택1	정보보호론은 전 범위에서 출제 시스템네트워크보안은 해당 범위에서만 서술식으로 출제
국가직(추가)	전산개발	9급	10	8.14~8.17	10.21	80									국,영,한,컴일,정보	2017년 하반기 추가 채용
지방직(추가)	전산개발	9급	시도별	10.20~10.26	12.16	시도별									국,영,한,컴일,정보	2017년 하반기 추가 채용

※ 만든이 : 지안에듀-조현준 선생(정보보호론, 자료구조론, 정보보안기사 담당), 최신 자료는 지안에듀(www.zianedu.com) 조현준 교수방 참조

2020년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

비전공자도 합격 전략 과목으로 만들수 있는 정보보호론!

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2019.09~2019.10	2019.11~2019.12	2020.01~2020.02	2020.03~2020.04	2020.05~2020.06	2020.07~2020.08
전산개발	이론 1.0	기본+심화	용어+요약 1.1 + 1.2	속성이론 1.4			
	기출+적중 3.0		핵심기출 700선 3.1	최고수준 800제 3.3			
	모의고사 5.0				국가직 9급 5.1	지방직 등 9급 5.2	국가직 7급 5.3
정보보호직+경간부 7.0			정보보안기사 필기 7.1				
교재		2020 탑스팟 이론서	핵심기출 700선	·2020 탑스팟 이론서/ 최고수준 800제	프린트물	프린트물	프린트물
문제난이도		중~중상	중~중상	중상~상	중상~상	중상~상	상
비고		·이론서2권-전2권 구성 ·주3회 이론수업 ·매주 복습 퀴즈 진행	·연도별 기출문제 풀이 3.2 -교재프린트 제공, 동영상 진행 ·핵심기출 700선 (문제편/정답·해설편/용어·요약집) -전3권 구성 ·정보보안기사는 11월 개강	·최고 수준 800제 (제본, 수강생 제공)는 고득점 합격을 목표로 함	·모의고사식 실전 훈련	·모의고사식 실전 훈련 ·최신 정보보안기사 기출문제 포함 모의고사 진행	·모의고사식 실전 훈련 ·국회사무처 등 시험대비 겸합 ·최종 마무리 정리

추천과정	
전산개발(9급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2
군무원(9급, 7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2
전산개발(7급)	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3
정보보호직	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1
사이버, 경찰간부	입문과정(무료B)→이론 1.1 + 1.2 + 1.3 →기출 3.1 , 3.2 ☒ 택1→최고수준 800제 3.3 →정보보안기사 필기 7.1 →9급 대비 모의고사 5.1 + 5.2 7급 대비 모의고사 5.3

빅데이터 1.0 / 이론

- 1.1 기본+심화 통합이론
- 1.2 핵심 용어 정리 200선(용어집)
- 1.3 핵심 요약집 정리
- 1.4 속성 이론

빅데이터 3.0 / 기출+적중

- 3.1 핵심기출 700선
- 3.2 연도별 기출문제 풀이
- 3.3 최고수준 800제(학원 내부교재)

빅데이터 5.0 / 모의고사

- 5.1 국가직 9급 대비 모의고사
- 5.2 지방직, 교육청, 서울시, 군무원 대비 모의고사
- 5.3 7급 대비 모의고사

빅데이터 7.0 / 정보보호직+경간부

- 7.1 정보보안기사 필기(알기사)

기타 무료 강의

- A 정보보호론 학습 전략
- B 정보보호론 기초 입문 과정
- C 계리직 대비 정보보호론