1. 본 자료는 전산직 수험생을 위하여 제작한 자료로 사이트(카페, 홈페이지 등)에 자유롭게 게시할 수 있습니다. 다만, 판매목적의 교재 등에는 절대 이용할 수 없습니다.

2. 무료 기출 동영상 제공 안내(정보보호직 포함) : 본 자료 외에 자세한 기출해설 강의를 아래 링크에 올려놨으니 이용바랍니다.
http://tech.zianedu.com/front/ProductVodView?a_lLinkCtgKey=0&a_lGKey=104348

3. 정보보호론 핵심이론 무료특강 안내 : 정보보호론 전 범위를 7강좌로 정리한 것으로 문제풀이 전에 보면 좋습니다.
http://tech.zianedu.com/front/ProductVodView?a_lLinkCtgKey=0&a_lGKey=104299

4. 기타 지안/탑스팟 가족이든 아니든 개인적으로 정보보호론 공부방법에 대해서 궁금한 내용이 있으신 분들은 kingsalt1102@naver.com으로 메일 보내시면 제가 아는 범위내에서 성심껏 답변드리도록 하겠습니다.

5. 기출해설 특강 후에 참석자에 대해 설문조사 결과 800제를 풀어보신 분들과 안 풀어보신 분들이 평균 15~20점 정도 점수 차이가 발생했습니다.

2016년 국가직 9급 정보보호론 총평

-지안학원 조상진 선생

1. 문제분석

(가) 전년도와 비슷한 난이도 수준

정보보보호론이 공무원 시험과목으로 편입되고 올해로 3년차에 들어갑니다. 어느 정도 문제가 공무원 스타일로 정형화가 되어가는 것 같습니다. 지금까지 16회(비공개 문제[교육청, 지방7급]-적중 800제 수록, 정보보호직 시험 포함)의 시험이 있었는데, 중간정도의 난이도로 보입니다. 전년도와는 비슷한 난이도 수준으로 판단되지만, 함정이 있는 문제들이 조금 있어서 점수가 낮게 나온 분들도 많을 것 같습니다.

(나) 행정자치부 주관 시험은 법규가 2문제

대다수 이공계 계통 수험생들이 어려워하는 파트가 법규입니다. 최근에 출제되는 정보보호론 시험에서 법규파트는 0~2개 문제 정도 출제되었습니다. 행정자치부/국회사무처/경기지방7급 2문제, 교육청 1문제, 서울시 0문제였습니다. 본인의 목표 시험이 무엇이냐에 따라 법규에 가중치를 적절히 두시기 바랍니다. 2016년 9급 시험의 2문제 중 하나는 대다수 수험생들이 자주 보는 망법의 동의사항 문제였고, 전자서명 관련 문제는 동형 모의고사에서 다룬 문제가 그대로 나왔습니다.

(다) 컴퓨터일반에 정보보호론에 다룬 문제들

컴퓨터일반에서 정보보호론에서 다룬 문제가 3문제 출제되었습니다. 라우팅, 네트워크 장비, TCP/IP였는데, 이런 문제들은 컴퓨터일반과 정보보호론의 교집합에 있다고 보시면 됩니다. 특히, 정보보호론에서는 네트워크 기반 공격을 이해하기 위해서 꼭 필요한 개념들입니다. 네트워크 기본 파트(TCP/IP ~ 라우팅, 네트워크 장비)도 잘 정리해주면 양쪽에 많은 도움이 될 것으로 판단됩니다.

2. 탑스팟 정보보호론 적중률 분석

(가) 적중률(95~99%)

20문제 모두 이론서에 있는 내용였습니다. 그리고 그것이 문제화되어 기출700제, 적중800제, 동형 모의고사에 있었는지 여부는 각 문제마다 출제된 페이지까지 명시해놨으니 확인 바랍니다. 특히, 이번에 처음으로 비공개로 진행된 적중800제가 점수 차이를 좌우하는 요인으로 작용했을 것 같은 생각이 해설 작업 하면서 들었습니다. 전체적으로 탑스팟 교재에서 95~99%정도의 적중률을 보였습니다.

3. 향후 학습방향

(가) 이론서와 적중800제 회독수를 늘려라.

전년도 많은 합격생들이 이론서와 1000제로 합격을 하였습니다. 올해는 1000제를 난이도별로 나누어서 단원별로 정리하여 기출700제와 적중800제(수록 문제들에 대한 안내는 탑스팟 카페에 있음)를 만들었습니다. 이론과 문제풀이의 적절한 병행이 고득점 비결입니다. 그리고 기출문제보다 한 단계 높은 문제들로 훈련을 하게 되면 실전에 가서 문제가 쉽게 느껴지는 것입니다. 남은 시간 문제집 2회독할 때 이론서를 1회독하면서 회독수를 늘려보세요. 특히 문제풀이 중간에 이론서를 한 번씩 읽어보면 이론서 내용이 더 잘 머릿속에 들어옵니다. 탑스팟 이론서는 국내외 보안시험(정보보안기사, 감리사, CISA, CISSP)을 분석 후에 대학교재를 토대로 공무원 시험에 맞게 최적화시킨 교재입니다.

4. 지안 공무원학원 향후 수업 안내

(가) 7급 대비 모의고사반(6주)

2016년 선행 정보보안기사 기출문제, 비공개 문제, 감리사 문제 등 난이도가 높은 문제 위주로 선별하여 모의고사식으로 진행합니다.

(나) 2017년 개정판

- 개정판 강의 : 2016년 9월 ~

2016년 국가직 9급
정보보호론

–2016년 4월 9일 시행

1.

사용자 인증에 사용되는 기술이 아닌 것은?

① Snort
② OTP(One Time Password)
③ SSO(Single Sign On)
④ 스마트 카드

◦ 일회용 패스워드(one-time password)는 오직 한 번만 사용되는 패스워드이다. 이런 패스워드에는 도청이나 도난이 무의미해진다.
◦ 통합 인증 체계(SSO)은 한 번의 시스템 인증을 통하여 접근하고자 하는 다양한 정보시스템에 재인증 절차 없이 접근할 수 있도록 하는 통합 로그인 솔루션이다.
◦ 스마트카드는 실질적으로 정보를 처리할 수 있다는 점에서 메모리 카드보다 발전된 기술이다. 마이크로 프로세스, 카드 운영체제, 보안 모듈, 메모리 등으로 구성되어 특정 업무를 처리할 수 있는 능력을 갖추고 있어야 한다.

오답피하기 ① Snort는 실시간 트래픽분석과 IP 네트워크에서의 패킷 처리를 담당하는 공개 소스 네트워크 침입방지시스템(IPS)이다.

정답 ①

이론서 194p, 적중 800제 500번 적중

2.

보안 요소에 대한 설명과 용어가 바르게 짝지어진 것은?

보기

ㄱ. 자산의 손실을 초래할 수 있는 원하지 않는 사건의 잠재적인 원인이나 행위자
ㄴ. 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성
ㄷ. 자산의 잠재적인 속성으로서 위협의 이용 대상이 되는 것

	ㄱ	ㄴ	ㄷ
①	위협	취약점	위험
②	위협	위험	취약점
③	취약점	위협	위험
④	위험	위협	취약점

◦ 위험(Risk) : 예상되는 위협에 의해 자산에 발생할 가능성이 있는 손실의 기대치. 자산의 가치 및 취약점과 위협 요소의 능력, 보호 대책의 효과 등에 의해 영향을 받는다.
◦ 취약점(Vulnerability) : 위협의 이용대상으로 관리적, 물리적, 기술적 약점이다.(정보보호 대책 미비)
◦ 위협(Threat) : 손실이나 손상의 원인이 될 가능성을 제공하는 환경의 집합이다. 보안에 해를 끼치는 행동이나 사건이다.

오답피하기 ② 보기는 위험관리에 나오는 용어에 대한 정의이다.

정답 ②

이론서 43p, 기출700제 596번, 적중800제 13번 적중

3.

공개키 암호 알고리즘에 대한 설명으로 옳은 것은?

① Diffie-Hellman 키 교환 방식은 중간자(man-in-the-middle) 공격에 강하고 실용적이다.
② RSA 암호 알고리즘은 적절한 시간 내에 인수가 큰 정수의 소인수분해가 어렵다는 점을 이용한 것이다.
③ 타원곡선 암호 알고리즘은 타원곡선 대수문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하

기 위해서 더 긴 길이의 키를 필요로 한다.

④ ElGamal 암호 알고리즘은 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용한 것이다.

◦ ② RSA는 인수분해 문제해결의 높은 난이도를 이용한 가장 대표적인 공개키 암호 알고리즘으로 암호화뿐만 아니라 디지털서명의 용도로도 사용된다.

오답피하기 ① Diffie-Hellman 키 교환 방식은 인증단계가 없기 때문에 중간자(man-in-the-middle) 공격에 취약하다.

③ 타원곡선 암호 알고리즘은 타원곡선 대수문제에 기초를 두고 있으며, RSA 알고리즘과 동일한 안전성을 제공하기 위해서 더 짧은 길이의 키를 필요로 한다.

④ ElGamal 암호 알고리즘은 이산대수 문제에 근거한다. 많은 큰 수들의 집합에서 선택된 수들의 합을 구하는 것은 쉽지만, 주어진 합으로부터 선택된 수들의 집합을 찾기 어렵다는 점을 이용하는 것은 배낭 문제에 대한 설명이다.

정답 ②

이론서 123p, 기출700제 71번, 79번, 적중800제 103번 적중

4.

ISO/IEC 27001의 보안 위험 관리를 위한 PDCA 모델에 대한 설명으로 옳지 않은 것은?

① IT기술과 위험 환경의 변화에 대응하기 위하여 반복되어야 하는 순환적 프로세스이다.

② Plan 단계에서는 보안 정책, 목적, 프로세스 및 절차를 수립한다.

③ Do 단계에서는 수립된 프로세스 및 절차를 구현하고 운영한다.

④ Act 단계에서는 성과를 측정하고 평가한다.

◦ ISO 27001은 영국의 BSI(British Standards Institute)에서 제정한 BS 7799를 기반으로 구성되어 있는, 일종의 보안 인증이자 보안 프레임워크이다. 어떤 조직이 ISO 27001 인증을 획득했다고 하면 이는 ISO 27001에서 제시한 프레임워크에 따라 회사의 위험을 관리하고, 이를 개선해나가는 체계를 갖추었다는 의미이다.

◦ 보안 위험관리 PDCA 모델

- 계획(plan) : 보안 정책, 목적 프로세스 및 절차의 수립
- 실행(do) : 위험 처리 계획의 이행
- 점검(check) : 위험 처리 계획을 모니터링하고 유지 보수
- 처리(act) : 사건, 검토 또는 인지된 변화에 대응하여 정보 보안 위험 관리를 유지보수하고 개선

오답피하기 ④ 성과를 측정하고 평가하는 단계는 점검(Check) 단계이다.

정답 ④

이론서 673p, 적중800제 672번 문제 해설 적중

5.

메시지의 무결성을 검증하는 데 사용되는 해시와 메시지 인증코드(MAC)의 차이점에 대한 설명으로 옳은 것은?

① MAC는 메시지와 송수신자만이 공유하는 비밀키를 입력받아 생성되는 반면에, 해시는 비밀키 없이 메시지로부터 만들어진다.

② 해시의 크기는 메시지 크기와 무관하게 일정하지만, MAC는 메시지와 크기가 같아야 한다.

③ 메시지 무결성 검증 시, 해시는 암호화되어 원본 메시지와 함께 수신자에게 전달되는 반면에, MAC의 경우에는 MAC로부터 원본 메시지 복호화가 가능하므로 MAC만 전송하는 것이 일반적이다.

④ 송수신자만이 공유하는 비밀키가 있는 경우, MAC를 이용하여 메시지 무결성을 검증할 수 있으나 해시를 이용한 메시지 무결성 검증은 불가능하다.

◦ 메시지 인증코드는 임의 길이의 메시지와 송신자 및 수신자가 공유하는 키라는 2개의 입력을 기초로 해서 고정 비트길이의 출력을 계산하는 함수이다. 이 출력을 MAC값이라 부른다.

오답피하기 ② 해시나 MAC은 메시지 크기와 무관하게 일정하다. ③ 해시나 MAC은 원본과 함께 해시 또는 MAC을 전송한다. ④ 해시마 MAC은 무결성 검증이 가능하다.

정답 ①

이론서 148p, 기출700제 97번, 적중800제 134번 적중

6.

DMZ(demilitarized zone)에 대한 설명으로 옳은 것만을 고른 것은?

보기

ㄱ. 외부 네트워크에서는 DMZ에 접근할 수 없다.
ㄴ. DMZ 내에는 웹 서버, DNS 서버, 메일 서버 등이 위치할 수 있다.
ㄷ. 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.
ㄹ. DMZ는 보안 조치가 취해진 네트워크 영역으로, 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

① ㄱ, ㄷ ② ㄴ, ㄷ
③ ㄴ, ㄹ ④ ㄱ, ㄹ

◦ 스크린드 서브넷 구조(Screened Subnet Architecture)는 스크리닝 라우터들 사이에 듀얼홈드 게이트웨이가 위치하는 구조로 인터넷과 내부 네트워크 사이에 DMZ(Demilitarized Zone)라는 네트워크 완충 지역 역할을 하는 서브넷을 운영하는 방식이다.
◦ 외부에서 접속할 수 있어야 하며 보호되어야 할 시스템은 주로 DMZ 네트워크에 배치한다. 보통 DMZ 안에 있는 시스템은 회사의 웹사이트, 이메일 서버 또는 DNS 서버와 같이 반드시 외부로 연결할 수 있어야 한다.(중요한 정보들이 있는 DB 서버 등과 같은 시스템들은 내부 네트워크에 설치)

오답피하기 ③ ㄱ. 외부 네트워크에서는 DMZ에 접근할 수 있어야 한다. ㄷ. 내부 사용자가 DMZ에 접속하기 위해서는 내부 방화벽을 거쳐야 한다.

정답 ③

이론서 525p, 적중800제 519, 520번 적중

7.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 상 정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 이용자들에게 알리고 동의를 받아야 하는 내용이 아닌 것은?

① 개인정보의 수집·이용 목적
② 수집하는 개인정보의 항목
③ 개인정보의 보유·이용 기간
④ 개인정보 처리의 위탁기관명

◦ 제22조(개인정보의 수집·이용 동의 등)
① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.
1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간
② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.
1. 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

오답피하기 ④ 개인정보 처리의 위탁기관명은 동의사항에 포함되지 않는다.

정답 ④

이론서 750p, 적중800제 735번 적중

8.

임의접근제어(DAC)에 대한 설명으로 옳지 않은 것은?

① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 둔다.
② 주체 또는 주체가 소속되어 있는 그룹의 식별자(ID)를 근거로 객체에 대한 접근을 승인하거나 제한한다.
③ 소유권을 가진 주체가 객체에 대한 권한의 일부 또는 전부를 자신의 의지에 따라 다른 주체에게 부여한다.
④ 전통적인 UNIX 파일 접근제어에 적용되었다.

오답피하기 ① 사용자에게 주어진 역할에 따라 어떤 접근이 허용되는지를 말해주는 규칙들에 기반을 두는 것은 RBAC에 대한 설명이다.

정답 ①

이론서 224p, 기출700제 183, 184번, 적중800제 231번, 232번 적중

9.

식별된 위험에 대처하기 위한 정보보안 위험 관리의 위험 처리 방안 중, 불편이나 기능 저하를 감수하고라도, 위험을 발생시키는 행위나 시스템 사용을 하지 않도록 조치하는 방안은?

① 위험 회피
② 위험 감소
③ 위험 수용
④ 위험 전가

오답피하기 ① 위험 회피(Risk avoidance)는 위험이 존재하는 프로세스나 사업을 수행하지 않고 포기하는 것이다. 자산 매각이나 설계변경 등 다른 대안을 선택하여 해당 위험이 실현되지 않도록 하는 것이다. 이것은 보통 편리함의 상실이나 조직에 유용한 기능을 수행할 수 있는 능력의 상실을 초래할 수 있다.

정답 ①

이론서 688p, 기출700제 606번, 적중800제 686번 적중

10.

Bell-LaPadula 보안 모델의 *-속성(star property)이 규정하고 있는 것은?

① 자신과 같거나 낮은 보안 수준의 객체만 읽을 수 있다.
② 자신과 같거나 낮은 보안 수준의 객체에만 쓸 수 있다.
③ 자신과 같거나 높은 보안 수준의 객체만 읽을 수 있다.
④ 자신과 같거나 높은 보안 수준의 객체에만 쓸 수 있다.

◦ No read up : 주체는 같거나 낮은 보안 수준의 객체만 읽을 수 있다. 단순 보안 속성(ss-property, simple security property)으로 불린다.
◦ No write down : 주체는 같거나 높은 보안 수준의 객체에만 쓸 수 있다. *속성(*-property, star property)으로 불린다.

오답피하기 ④ BLP 모델은 *-속성(star property)은 No write down으로 주체는 같거나 높은 보안 수준의 객체에만 쓸 수 있다.

정답 ④

이론서 230p, 적중800제 247번, 248번 적중

11.

버퍼 오버플로우에 대한 설명으로 옳지 않은 것은?

① 프로세스 간의 자원 경쟁을 유발하여 권한을 획득하는 기법으로 활용된다.
② C 프로그래밍 언어에서 배열에 기록되는 입력 데이터의 크기를 검사하지 않으면 발생할 수 있다.
③ 버퍼에 할당된 메모리의 경계를 침범해서 데이터 오류가 발생하게 되는 상황이다.
④ 버퍼 오버플로우 공격의 대응책 중 하나는 스택이나 힙에 삽입된 코드가 실행되지 않도록 하는 것이다.

◦ 버퍼오버플로우의 실행가능 주소 공간의 보호 기법에는 스택과 힙을 실행불능으로 만듦으로써 기존 프로그램을 위한 여러 가지 유형의 버퍼 오버플로우 공격에 대한 방어를 제공한다. 따라서 최신 운영체제들은 이 기법을 표준으로 포함하고 있다.

오답피하기 ① Race Condition 공격에 대한 설명이다.

정답 ①

이론서 343p, 기출700제 288번, 적중800제 339번 적중

12.

침입탐지시스템(IDS)에서 알려지지 않은 공격을 탐지하는 데 적합한 기법은?

① 규칙 기반의 오용 탐지
② 통계적 분석에 의한 이상(anomaly) 탐지
③ 전문가 시스템을 이용한 오용 탐지
④ 시그니처 기반(signature based) 탐지

오답피하기 ② 알려지지 않은 공격 즉, Zero Day 공격을 방어하는 것은 일반적으로 통계적 분석에 의한 이상 탐지를 이용한다.

정답 ②

이론서 502p, 기출700제 424번, 425번

13.

전자서명법 상 공인인증기관이 발급한 공인인증서의 효력 소멸 또는 폐지의 사유에 해당하지 않는 것은?

① 공인인증서의 유효기간이 경과한 경우
② 가입자의 전자서명검증정보가 유출된 경우
③ 공인인증기관이 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
④ 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우

제16조(공인인증서의 효력의 소멸 등)
① 공인인증기관이 발급한 공인인증서는 다음 각호의 1에 해당하는 사유가 발생한 경우에는 그 사유가 발생한 때에 그 효력이 소멸된다.
1. 공인인증서의 유효기간이 경과한 경우
2. 제12조제1항의 규정에 의하여 공인인증기관의 지정이 취소된 경우
3. 제17조의 규정에 의하여 공인인증서의 효력이 정지된 경우
4. 제18조의 규정에 의하여 공인인증서가 폐지된 경우

제18조(공인인증서의 폐지)
① 공인인증기관은 공인인증서에 관하여 다음 각호의 1에 해당하는 사유가 발생한 경우에는 당해 공인인증서를 폐지하여야 한다.
1. 가입자 또는 그 대리인이 공인인증서의 폐지를 신청한 경우
2. 가입자가 사위 기타 부정한 방법으로 공인인증서를 발급받은 사실을 인지한 경우
3. 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
4. 가입자의 전자서명생성정보가 분실·훼손 또는 도난·유출된 사실을 인지한 경우

오답피하기 ② 가입자의 전자서명검증정보가 아닌 전자서명생성정보가 유출된 경우가 해당된다.

정답 ②

이론서 775p, 2016년 국가직 모의고사 7회 15번, 8회 15번 적중

14.

가상사설망(VPN)에 대한 설명으로 옳지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축 비용이 저렴하다.
② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자 인증의 보안 기능을 제공한다.
③ 네트워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.
④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동 중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

◦ 공중 네트워크를 이용하여 사설 네트워크가 요구하는 서비스를 제공할 수 있도록 네트워크를 구성한 것이기 때문에 가상 사설 네트워크라고 한다.
◦ 즉, 인터넷과 같은 공중 네트워크를 마치 전용회선처럼 사용할 수 있게 해주는 기술 혹은 네트워크를 통칭한다.
◦ 공중망을 경유하여 데이터가 전송되더라도 외부인으로부터 안전하게 보호되도록 주소 및 라우터 체계의 비공개, 데이터 암호화, 사용자 인증 및 사용자 액세스 권한 제한 등의 기능을 제공한다.

오답피하기 ③ SSH는 TELNET과 같이 TCP를 하부 전송 프로토콜로 사용하나 더 안전하고 TELNET 보다 더 많은 서비스를 제공한다. 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해주는 4계층 프로토콜이 아닌 응용 프로그램 또는 프로토콜을 가리킨다.

정답 ③

이론서 456p, 적중800제 415번 적중

15.

ISO/IEC 27002 보안 통제의 범주에 대한 설명으로 옳지 않은 것은?

① 보안 정책 : 비즈니스 요구사항, 관련 법률 및 규정을 준수하여 관리 방향 및 정보 보안 지원을 제공
② 인적 자원 보안 : 조직 내의 정보 보안 및 외부자에 의해 사용되는 정보 및 자원 관리
③ 자산 관리 : 조직의 자산에 대한 적절한 보호를 성취하고 관리하며, 정보가 적절히 분류될 수 있도록 보장
④ 비즈니스 연속성 관리 : 비즈니스 활동에 대한 방해에 대처하고, 중대한 비즈니스 프로세스를 정보 시스템 실

패 또는 재난으로부터 보호하며, 정보 시스템의 시의 적절한 재개를 보장

◦ 인적 자원 보안(ISO 27002) : 고용 전, 고용 중, 고용 종료 및 직무 변경
◦ 외부자 보안(KISA-ISMS) : 계약 및 서비스수준협약 보안관리, 외부자 보안 실행관리
◦ 인적보안(KISA-ISMS) : 책임할당 및 규정화, 비밀유지, 적격심사 및 주요 직무 담당자 관리

오답피하기 ② ISO 27002는 27001의 요구사항에 대한 실무규약으로 인적자원 보안이란 고용 전, 고용 중, 고용 종료 및 직무 변경에 대한 내용을 통제한다.

정답 ②

이론서 674p, 679p, 737p 적중

16.

OWASP(The Open Web Application Security Project)에서 발표한 2013년도 10대 웹 애플리케이션 보안 위험 중 발생 빈도가 높은 상위 3개에 속하지 않는 것은?

① Injection
② Cross-Site Scripting
③ Unvalidated Redirects and Forwards
④ Broken Authentication and Session Management

A1-Injection(인젝션취약점)
A2-Broken Authentication and Session Management (취약한 인증과 세션관리)
A3-XSS(크로스사이트 스크립팅)
A4-Insecure Direct Object References (안전하지 않은 직접 객체 참조)
A5-Security Misconfiguration(보안상 잘못된 구성)
A6-Sensitive Data Exposure(민감한 데이터 노출)
A7-Missing Function Level Access Control (미약한 접근통제 기능수준)
A8-CSRF(크로스사이트 요청변조)
A9-Using Components with Known Vulnerabilities (알려진 취약 컴포넌트 이용)
A10-Unvalidated Redirects and Forwards (검증되지 않은 리다이렉트,포워드)

오답피하기 ④ Unvalidated Redirects and Forwards(검증되지 않은 리다이렉트,포워드)는 2013년 발표한 OWASP의 10위이다.

정답 ④

이론서 618p 적중

17.

전자우편의 보안 강화를 위한 S/MIME(Secure/Multipurpose Internet Mail Extension)에 대한 설명으로 옳은 것은?

① 메시지 다이제스트를 수신자의 공개키로 암호화하여 서명한다.
② 메시지를 대칭키로 암호화하고 이 대칭키를 발신자의 개인키로 암호화한 후 암호화된 메시지와 함께 보냄으로써 전자우편의 기밀성을 보장한다.
③ S/MIME를 이용하면 메시지가 항상 암호화되기 때문에 S/MIME 처리 능력이 없는 수신자는 전자우편 내용을 볼 수 없다.
④ 국제 표준 X.509 형식의 공개키 인증서를 사용한다.

〈S/MIME의 인증구조〉
◦ 송·수신 측이 직접 상대방을 상호 인증하는 방식
◦ 공인인증서를 맞교환하여 상호 인증하는 방식
◦ 인증계층상의 인증 기관(CA)들의 체인을 통해 상호 인증하는 방식

오답피하기 ① 메시지 다이제스트를 송신자의 개인키로 서명한다. ② 메시지를 대칭키로 암호화하고 이 대칭키를 수신자의 공개키로 암호화한 후 암호화된 메시지와 함께 보냄으로써 전자우편의 기밀성을 보장한다. ③ S/MIME의 다이제스트된 데이터 콘텐츠 유형은 메시지의 무결성을 제공하기 위해 사용되는데, 기밀성 서비스는 제공되지 않는다.

정답 ④

이론서 587p 적중

18.

국내 정보보호관리체계(ISMS)의 관리 과정 5단계 중 위험 관리 단계의 통제항목에 해당하지 않는 것은?

① 위험 관리 방법 및 계획 수립
② 정보보호 대책 선정 및 이행 계획 수립
③ 정보보호 대책의 효과적 구현
④ 위험 식별 및 평가

정보보호 정책수립 및 범위설정	정보보호정책의 수립
	범위 설정
경영진 책임 및 조직구성	경영진 참여
	정보보호 조직 구성 및 자원 할당
위험관리	위험관리 방법 및 계획 수립
	위험 식별 및 평가
	정보보호대책 선정 및 이행계획 수립
정보보호대책 구현	정보보호대책의 효과적 구현
	내부 공유 및 교육
사후관리	법적요구사항 준수 검토
	정보보호 관리체계 운영현황 관리
	내부감사

오답피하기 ③ 정보보호 대책의 효과적 구현은 정보보호대책 구현과정에 포함된다.

정답 ③

이론서 738p, 국가직 모의고사 수강생 문제 3주차 8번 적중

19.

공개키 기반 전자서명에서 메시지에 서명하지 않고 메시지의 해시값과 같은 메시지 다이제스트에 서명하는 이유는?

① 공개키 암호화에 따른 성능 저하를 극복하기 위한 것이다.
② 서명자의 공개키를 쉽게 찾을 수 있도록 하기 위한 것이다.
③ 서명 재사용을 위한 것이다.
④ 원본 메시지가 없어도 서명을 검증할 수 있도록 하기 위한 것이다.

오답피하기 ① 디지털서명 시스템에서 메시지는 일반적으로 매우 길지만 그래도 비대칭키 시스템을 사용해야만 한다. 이 경우에 비효율성 문제를 해결하기 위해 실제 메시지보다 훨씬 짧은 메시지 다이제스트에 서명을 하는 방법을 이용한다.

정답 ①

이론서 157p, 적중800제 147번 적중

20.

윈도우즈에서 지원하는 네트워크 관련 명령어와 주요 기능에 대한 설명으로 옳지 않은 것은?

① route :라우팅 테이블의 정보 확인
② netstat :연결 포트 등의 네트워크 상태 정보 확인
③ tracert :네트워크 목적지까지의 경로 정보 확인
④ nslookup :사용자 계정 정보 확인

오답피하기 ④ nslookup 명령어는 특정 도메인명에 대한 IP 주소를 조회할 때 사용하는 명령어이다.

정답 ④

이론서 460p~463p, 기출700제 358번, 적중800제 420번 적중