2014년

9급(국가직,지방직,교육청,서울시) 총평

-지안학원 조상진 선생

1. 문제분석

(가) 첫 년도 시험으로 출제범위를 제시

정보보호론이 2014년도 첫 시행되었습니다. 아직 국가직 7급시험과 국회사무처 시험이 남아 있지만, 7월부터 공부를 시작하시는 분들을 위하여 간단히 적어보도록 하겠습니다. 출제 범위에서 특이한 점은 (1)법규 문제가 안행부에서 주관하는 시험(국가직, 지방직)에서는 3문제씩 출제되었고, 개인정보보호법 문제가 교육청과 서울시 시험에서 1문제씩 출제되었습니다. (2) 최신 보안 경향을 묻는 몇 문제가 출제되었습니다. (3)시험 범위는 [대학교재+실무 법률+최신 보안 경향 파악]으로 정해지는 것 같습니다. 암호학 비중은 예상보다 낮았습니다.

(나) 영역별 출제 검토(80문항)

영역별로 출제된 내용을 검토해보면 다음과 같습니다.

1. 정보보호 개요(7문항, 8.8%)
2. 암호학(16문항, 20%)
3. 접근통제(10문항, 12.5%)
4. 시스템 보안(4문항, 5.0%)
5. 네트워크 보안(18문항, 22.5%)
6. 어플리케이션 보안(9문항, 11.3%)
7. 정보보호 관리(16문항, 20%)

자세한 내용은 엑셀 파일로 첨부했으니 참고바랍니다. 특이한 점은 정보보호관리 영역의 출제 비율이 출제기관에 따라 현격하게 차이가 나네요.

(다) 난이도 검토

첫 회 시험으로 몇 문제를 빼고 난이도가 높게 출제되지는 안았지만, 범위를 넓게 잡아서 출제를 하다보니 수험생들이 이 부분에서 상당히 부담을 느꼈을 것 같습니다. 어느 분들은 탑스팟 교재가 두껍다고 하는데, 몇 년 뒤에서는 지금 교재도 너무 얇다고 하는 날이 오지 않을까 하는 생각도 드네요. 왜냐하면 실무 법률과 정보보안기사 등에서나 출제되는 최신 경향을 묻는 문제가 계속 나올 것이기 때문입니다. 서울시 시험의 경우는 수강생 중에서 100점 받으신 분들도 몇 분 있는 것을 보면 첫 회 난이도는 평이했다고 볼 수 있습니다.

(다) 법규 문제 검토

개인정보보호법은 4개 시험에서 모두 출제가 되었습니다. 이 부분은 반드시 정확히 정리해야 할듯합니다. 그리고 법률이 개정되는 부분도 반드시 숙지하셔야 하고요. 나머지는 시험에서 정보통신망법과 정보통신기반보호법이 출제되었습니다. 법규는 암기하는 것이 아닙니다. 모르는 분들은 법규를 가장 힘들어 할 수 있는데, 가장 점수따기 쉬운 곳이기도 합니다.

2. 정보보호론 vs 정보보안기사

(가) 시험 후 수험생들이 생소하다고 한 문제들

1.스텃스넷(국가직 출제) : 정보보안기사 2회 기출되었고 교재에 수록됨. 2.CMVP(지방직 출제) : 정보보안기사 1회에서 출제되어 탑스팟 교재에 이론과 문제 수록. 3.블루스나핑(지방직 출제) : CISA/CISSP 시험에서 중요하게 다루었던 내용으로 교재에 수록. 4.리눅스 로그(교육청 출제) : 정보보안기사에서 가장 많이 출제된 문제임. 5.각종 법규 문제 : 정보보안기사 5개 법률에서 다룸. 6.PIMS(지방직 출제) : KISA(정보보안기사 출제기관) 주관 인증제도를 출제.

(나) 정보보안기사 문제들

위에 서술한 것은 제가 기억나는 것만 간단히 적어본 것이고요. 대다수 문제가 이미 SIS 문제나 정보보안기사에서 기출된 문제들입니다. 특히 최근에 기출된 문제들이 바로 공무원 시험에서 반영된 것을 보고서 많이 놀랐습니다. 현재 정보보안기사/산업기사는 한 회차에 180 문제가 출제되는데, 공무원 시험과 유사 문제들이 60~70%를 차지하고 있습니다. 난이도는 공무원 시험보다 높은 경우가 많고, 새로운 경향의 문제들이 계속 나오고 있습니다.

3. 2014 탑스팟 정보보호론 적중률 분석

(가) 국가직 적중률(95%)

정보통신기반보호법을 제외한 모든 문제가 탑스팟 교재에서 출제되어 95% 적중률을 보였습니다.

(나) 지방직 적중률(93~98%)

완전 일치하는 문제와 유사 지문이나 문제까지 했을 때 93~98% 적중률을 보였습니다. 지방직/서울시 특강에서 법규를 보완하여 적중도가 국가직과 비슷하였습니다.

(다) 교육청, 서울시 적중률(100%)

교육청 시험의 리눅스 로그부터 개인정보보호법까지 교재에 수록된 내용이었고, 수업시간에 강조한 내용들이 많이 출제 되었습니다. 100%의 적중률을 보였습니다. 해설에 페이지까지 있으니 확인 바랍니다.

(라) 높은 적중률 비결

어떤 분은 책이 두꺼워서 많이 적중되었다, 교재가 너무 어렵다, SIS 문제와 정보보안기사 문제는 볼 필요 없다고 들 합니다만 과연 그럴까요? 위 내용을 읽어 보신 분들은 직감하실 겁니다. 이 높은 적중률의 비결은 하나이며, 그것은 많은 기출문제 확보입니다. 현재 제가 가지고 있는 기출문제풀은 비공개 문제까지 2,000 문제 정도됩니다. 이를 토대로 이론서 집필을 했고요. 계속 업그레이드를 할 것입니다. 향후 몇 년간은 공무원 시험에서 이 테두리를 벗어나는 문제들은 드물지 않을까 나름 판단합니다.

4. 2015년 학습 전략

(가) 범위를 넓게 공부하라.

보안을 비유할 때 창과 방패에서 방패에 비유를 하곤합니다. 기술적으로 완벽하게 방어체제를 구축했다고 해도, 인간의 약한 심리를 이용하는 사회공학을 이용하여 공격에 성공합니다. 창의 기술이 발전하면 할수록 방패기술도 발전을 해야만 합니다. 그러기에 보안의 기술은 계속 업그레이드되고, 출제되는 문제들도 이를 따라갈 것입니다. 보안전문가가 갖추어야할 능력도 기술적 능력외에 관리적/물리적 기술까지도 요구하고 있으니, 출제범위가 넓은 것은 당연지사가 아닌가 생각이 듭니다.

(나) 기출문제를 정확히 파악하라.

모든 수험생의 목표는 시험에 합격하는 것입니다. 그러려면 내가 보는 시험이 어떤 문제가 출제되고 있는지 정확히 파악하는 것이 최단 기간 합격을 위한 필요충분조건입니다. 향후 몇 년간은 계속 새로운 문제들이 나올 수도 있습니다만, 현재까지 나온 문제들이 어디에 근거를 두고 출제가 되고 있는지를 정확히 알아야 합니다. 그리고 그와 유사한 문제들이 어디에서 출제가 되고 있는지도 정확히 알아야 합니다.

5. 탑스팟 교재 개정 및 강의 계획

(가) 교재 개정 계획

7급 시험까지 끝나면 어느 정도 출제 범위의 윤곽이 잡힙니다. 그러면 그에 맞게 교재를 개정할 예정입니다. 수험생들에게 보다 쉽게 효율적으로 공부할 수 있도록 많은 부분에서 개선이 이루어질 것입니다. 구체적인 개정 내용은 8월말에 안내해드리도록 하겠습니다.

(나) 향후 강의 계획

넓은 범위를 보다 효과적으로 이해시키기 위하여 그동안 지적되었던 개선 요구사항들을 모두 개선할 예정입니다. 예를 들어 판서하기 힘든 부분은 일정 부분 서브노트로 제공할 예정입니다. 그리고 철저하게 이해위주 수업으로 진행할 예정입니다.

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

서울시 9급 공개채용시험

–2014년 6월 28일 시행

1. 2014년 서울시 9급

정보보호의 목적 중 기밀성 을 보장하기 위한 방법만을 묶은 것은?

① 데이터 백업 및 암호화
② 데이터 백업 및 데이터 복원
③ 데이터 복원 및 바이러스 검사
④ 접근통제 및 암호화
⑤ 접근통제 및 바이러스 검사

정답 및 해설

◦ 기밀성 유지방법으로는 접근통제(access control), 암호화(encryption) 등이 있다. 이 중에서 암호화는 정보가 유출되더라도 변조되거나 위조되지 못하게 하는 기본적인 보안기술이다.

오답피하기 ④ 데이터 백업 및 데이터 복원은 가용성과 관련된 방법이며, 바이러스 검사는 무결성과 관련된 방법이다.

정답 ④

〈문제적중〉 이론서 10p 지문 동일 적중

2. 2014년 서울시 9급

다음 중 정보보호의 요소들에 대한 설명으로 옳은 것은?

① 부인방지(non-repudiation)란 정보가 비인가된 방식으로 변조되는 것을 방지하는 것을 의미한다.
② 무결성(integrity)이란 특정한 작업 또는 행위에 대해 책임소재를 확인 가능함을 의미한다.
③ 인증성(authenticity)이란 인가된 사용자가 필요 시 정보를 접근하고 변경하는 것이 가능함을 의미한다.
④ 가용성(availability)이란 정보나 해당 정보의 주체가 진짜임을 의미한다.
⑤ 기밀성(confidentiality)이란 정보의 비인가된 유출이 불가능함을 의미한다.

정답 및 해설

◦ 인증성(Authentication)은 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 객체의 자격이나 객체의 내용을 검증하는데 사용되는 성질이다.
◦ 부인방지(Non-repudiation)는 행위나 이벤트의 발생을 증명하여 나중에 그런 행위나 이벤트를 부인할 수 없도록 하는 것으로서, 정보보안의 방법에 의하여 데이터의 송수신가 송수신 사실을 부인하지 못하도록 방지하는데 사용된다.

오답피하기 ⑤ (1)은 무결성, (2)는 책임추적성, (3)는 가용성, (4)는 인증성에 대한 설명이다.

정답 ⑤

〈문제적중〉 이론서 10p 적중

3. 2014년 서울시 9급

다음 중 가장 안전한 패스워드는 어떤 것인가?

① 75481235
② abcd1234
③ korea2034
④ honggildong
⑤ do@ssud23

정답 및 해설

◦ 패스워드는 최소한 8자리이상의 문자와 4가지 유형의 문자(대/소문자, 숫자, 특수문자의 조합)로 구성하는 것이 좋다.

오답피하기 ⑤번은 소문자, 특수문자, 숫자의 조합의 9자리 패스워드로 보기 중에서 가장 안전한 패스워드로 볼 수 있다. 패스워드는 사전에 있는 단어, 이름, 예측 가능한 숫자나 단어는 피하는 것이 좋다.

정답 ⑤

〈문제적중〉 문제편 156페이지 10번 적중

4. 2014년 서울시 9급

다음 중 kerberos 인증 프로토콜에 대한 설명으로 옳지 않은 것은?

① Needham-Schroeder 프로토콜을 기반으로 만들어졌다.
② 대칭키 암호 알고리듬(Algorithm)을 이용한다.
③ 중앙 서버의 개입 없이 분산 형태로 인증을 수행한다.
④ 티켓 안에는 자원 활용을 위한 키와 정보가 포함되어 있다.
⑤ TGT를 이용해 자원 사용을 위한 티켓을 획득한다.

정답 및 해설

◦ 커버로스 (Kerberos)는 대칭 키 암호를 이용하는 TTP(Trusted Third-Party) 인증 프로토콜(Authentication Protocol). 클라이언트의 요청에 따라 인증 서버는 클라이언트의 패스워드를 기초로 티켓(TGT:Ticket-Granting Ticket)과 세션 키를 클라이언트에게 제공하고, 클라이언트는 애플리케이션 서버에 접근 시 일정 기간 내 사용자 인증용으로 이 티켓을 사용하는 방식. 버전 5의 규격은 RFC 1510에 규정되어 있다.

오답피하기 ③ 클라이언트는 인증기능을 가진 AS(Authentication Service)와 티켓을 발행하는 TGS(Ticket Granting Service)으로 구성된 KDC(Key Distribution Center)에 접속하므로 ③번은 옳지 않다.

정답 ③

〈문제적중〉 문제편 83페이지 38번 적중

5. 2014년 서울시 9급

다음 중 공개키 암호(public key cryptosystem)에 대한 설명으로 옳은 것은?

① 대표적인 암호로 AES, DES 등이 있다.
② 대표적인 암호로 RSA가 있다.
③ 일반적으로 같은 양의 데이터를 암호화하기 위한 연산이 대칭키 암호(symmetric key cryptosystem)보다 현저히 빠르다.
④ 대칭키 암호(symmetric key cryptosystem)보다 수백 년 앞서 고안된 개념이다.
⑤ 일반적으로 같은 양의 데이터를 암호화한 암호문(ciphertext)이 대칭키 암호(symmetric key cryptosystem) 보다 현저히 짧다.

정답 및 해설

◦ 대칭 암호알고리즘에서는 두 사용자 간에 비밀키를 공유하는 것이 가장 중요한 이슈이며, 비대칭 암호알고리즘에서는 다른 사용자의 공개키를 인증하는 것이 가장 중요한 이슈이다.
◦ 두 종류의 알고리즘 모두 유사한 용도로 사용할 수 있지만 비대칭 암호알고리즘이 대칭 암호알고리즘에 비해 상대적으로 많은 계산 비용이 소요되므로 주로 인증 목적으로 많이 사용된다.
◦ 비대칭 암호알고리즘은 다른 말로 공개키 암호알고리즘이라 하며, 암호화키와 복호화키가 서로 다르다. 비대칭 암호알고리즘은 Diffie와 Hellman이 1975년에 처음으로 제안하였으며, 대칭 암호알고리즘에 비해 상대적으로 역사가 짧다.

오답피하기 ② AES, DES는 대표적인 대칭키 알고리즘이고, RSA는 대표적인 비대칭키 알고리즘이다.

정답 ②

〈문제적중〉 문제편 26페이지 40번 적중

6. 2014년 서울시 9급

다음에서 설명하고 있는 기술은?

> 보기
> 이것은 디지털 컨텐츠의 저작권을 보호하기 위한 기술로 DVD와 다운로드된 음원, 유료 소프트웨어 등에 적용된다. 이는 주로 컨텐츠의 불법적인 복제나 허가받지 않은 기기에서의 컨텐츠 소비를 방지한다.

① DRM
② IPS
③ GPL
④ VPN
⑤ DOM

정답 및 해설

◦ GPL(General Public License) : 공개운영체계인 GNU 프로젝트로부터 제공되는 소프트웨어에 적용되는 라이센스. 사용자들이 소프트웨어를 자유롭게 공유하고 내용을 수정하도록 보증하는 것을 말한다. 따라서, 사람들은 GPL을 이용하여 소프트웨어의 배포판을 만들어 배포할 수 있고, 원한다면 그 배포판을 상업적으로 이용할 수도 있다. GPL의 가장 큰 특징은 GPL이 적용된 SW를 이용해 개량된 SW를 개발했을 경우, 개발한 SW의 소스코드 역시 공개해야 한다. 가장 널리(전체 공개SW의 70~80%) 적용되는 공개SW 라이선스로, 공개SW 세계의 헌법이라는 별칭까지 붙어있다. 자유SW재단의 리차드 스톨만이 만들었다.

◦ 문서 객체 모델(document object model, DOM) : 웹 브라우저를 통한 XML 문서의 상호 연동을 위한 객체 기반의 문서 모델.

오답피하기 ① 보기는 DRM에 대한 설명이다.

정 답 ①

〈문제적중〉 문제편 16페이지 12번, 17페이지 14번 적중

7. 2014년 서울시 9급

다음 중 공격자가 통신 프로토콜에 직접 개입하지 않고 감청(eavesdropping) 또는 감시(monitoring)만을 수행 하는 수동적 공격(passive attack)으로 분류될 수 있는 것은?

① 가장(masquerade)
② 재사용(replay)
③ 서비스 거부(denial of service)
④ 메시지 변조(modification of message)
⑤ 트래픽 분석(traffic analysis)

정답 및 해설

◦ 수동적 공격은 통신회선상의 정보를 무단으로 취득하는 행위인데, 통신회선에 제3자의 접속시도를 방지하는 방법과 데이터를 암호화하여 기밀성을 보장하는 방법으로 방어할 수 있다.

◦ 능동적 공격은 통신회선상의 정보를 변조, 위조하는 행위인데 암호화와 함께 데이터의 무결성을 확인하는 방법을 사용하여 방어할 수 있다.

오답피하기 ⑤ 가장, 재사용, 서비스 거부, 메시지 변조는 능동적 공격에 해당된다.

정 답 ⑤

〈문제적중〉 문제편 232페이지 1, 2번 적중

8. 2014년 서울시 9급

다음의 블록 암호 모드 중 각 평문 블록을 이전 암호문 블록과 XOR한 후 암호화되어 안전성을 높이는 모드는?

① ECB 모드
② CBC 모드
③ CTR 모드
④ OFB 모드
⑤ CFB 모드

정답 및 해설

◦ CBC 모드는 암호 블록 연쇄모드(Cipher Block Chaining mode)의 약자이다. 암호문 블록을 마치 체인처럼 연결시키기 때문에 붙여진 이름이다.

오답피하기 ② CBC 모드에서는 1단계 전에 수행되어 결과로 출력된 암호문 블록에 평문 블록을 XOR하고 나서 암호화를 수행한다. 따라서 생성되는 각각의 암호문 블록은 단지 현재 평문 블록뿐만 아니라 그 이전의 평문 블록들의 영향도 받게 된다.

정 답 ②

〈문제적중〉 문제편 30페이지 48번 적중

9. 2014년 서울시 9급

PKI에 관한 다음의 설명 중 옳지 않은 것은?

① PKI란 public key infrastructure의 약어로 공개키 암호 알고리듬(Algorithm)을 적용하고 인증서를 관리하기 위한 기반시스템이다.
② 주로 X.509인증서를 사용하고 있다.
③ 인증서를 발급하는 역할을 하는 기관을 CA라 한다.
④ 인증서는 대상과 공개키를 묶어주는 역할을 하며 변조를 막기 위해 대상의 서명이 추가된다.
⑤ 인증서의 폐기 여부를 확인하기 위해 사용되는 프로토콜은 OCSP이다.

정답 및 해설

◦ 한 쌍의 공개키/개인키와 특정 사람/기관을 연결시켜 주는, 즉 해당키가 특정인의 것이라는 것을 보증해주는 것으로서 전자서명에 사용된 개인키와 상응하는 공개키를 제공하여 그 공개키가 특정인의 것이라는 것을 확신할 수 있는 증거로서의 기능을 수행한다.

오답피하기 ④ 인증서에 포함되어 있는 공개키에는 인증기관이 자신의 개인키로 서명한 전자서명이 붙어 있어서 바꿔치기 하는 것을 불가능하게 만든다.

정답 ④

〈문제적중〉 이론서 147페이지 적중

10. 2014년 서울시 9급

DES에 대한 다음의 설명 중 옳지 않은 것은?

① 1970년대에 표준화된 블록 암호 알고리듬(Algorithm)이다.
② 한 블록의 크기는 64비트이다.
③ 한번의 암호화를 위해 10라운드를 거친다.
④ 내부적으로는 56비트의 키를 사용한다.
⑤ Feistel 암호 방식을 따른다.

정답 및 해설

◦ DES(data encryption standard)는 미국 정부의 상무부 표준국(NBS: 현재는 NIST로 개편됨)이 1977년에 IBM사의 제안을 바탕으로 제정한 데이터 암호화 표준 규격으로, 연방 정부의 연방 정보 처리 표준 46(FIPS publication 46)으로 채택된 것. 데이터 암호화 표준(DES)은 비밀 키 방식의 일종으로 64비트의 키를 사용하여 64비트의 평문을 전자(轉字)와 환자(換字)를 조합하여 암호화하는 방식이다.

오답피하기 ③ 한번의 암호화를 위해 16라운드를 거친다.

정답 ③

〈문제적중〉 이론서 69페이지 적중

11. 2014년 서울시 9급

방화벽(Firewall)에 대한 설명으로 옳지 않은 것은?

① 허가되지 않은 외부의 공격에 대비해 시스템을 보호하기 위한 하드웨어와 소프트웨어를 말한다.
② IP 필터링을 통하여 내부 네트워크로 들어오는 IP를 차단할 수 있다.
③ 방화벽을 구축해도 내부에서 일어나는 정보유출은 막을 수 없다.
④ 방화벽을 구축하면 침입자의 모든 공격을 완벽하게 대처할 수 있다.
⑤ 방화벽은 일반적으로 라우터 또는 컴퓨터가 된다.

정답 및 해설

◦ 방화벽은 외부망에서 내부망으로 접근하는 입구나 주요 서버 앞단에 위치하여 허가되지 않은 사용자가 내부 네트워크의 정보에 접근하는 것을 방지하고, 허가된 사용자들을 방해하지 않고 내부 네트워크에 접근하는 것을 보장해주는 역할을 하는 S/W 및 H/W로 구성된다.

오답피하기 ④ 방화벽을 구축한다 해도, 모뎀을 통한 접속이나 사회공학적인 접근 등에 대한 완벽한 대처는 불가능하다.

정답 ④

〈문제적중〉 이론편 571페이지 적중

12. 2014년 서울시 9급

다음은 무엇에 대한 설명인가?

보기

이것은 네트워크 상의 트랜잭션에 대한 상태 정보를 포함하는 일종의 토큰으로 주로 웹서버가 웹브라우저로 전송하여 클라이언트 쪽에 저장하고 나서 사용자가 해당 사이트를 재방문할 경우 웹브라우저가 웹서버에 재전송하는 형태로 많이 이용된다. 그러나 이는 원하지 않는 보안 상의 취약점을 야기할 수 있으므로 사용자가 이것을 주기적으로 삭제해 주는 것이 바람직하다.

① 애플릿(applet)
② URL(Uniform Resource Locator)
③ 공개키 인증서(public key certificate)
④ DOI(Digital Object Identifier)
⑤ 쿠키(Cookie)

정답 및 해설

◦ 자바 애플릿(Java applet)은 자바(Java) 언어로 작성된 작은 소프트웨어. 애플릿이라고도 한다. 크기가 작아서 네트워크에서의 전송에 적합하고, 월드 와이드 웹(WWW)을 써서 배포할 수 있다. 자바 애플릿은 사전에 컴파일하여 웹 서버에 등록해 둔다. 웹에서 사용하는 표준 데이터 형식인 하이퍼텍스트 생성 언어(HTML)로 작성한 문서에 애플릿이라는 꼬리표를 써서 자바 애플릿을 지정한다. 자바 애플릿을 동작시키는 데는 자바 가상 머신을 내장한 웹 브라우저가 필요하다. 브라우저는 불러내 온 문서 속에 애플릿이라는 꼬리표가 있으면, 지정된 자바 애플릿을 웹 서버로부터 내려받기하여 실행한다.
◦ 디지털 객체 식별자(digital object identifier, DOI)는 인터넷 주소가 변경되더라도 사용자가 그 문서의 새로운 주소로 다시 찾아갈 수 있도록, 웹 파일이나 인터넷 문서에 영구적으로 부여된 식별자. 즉 서적에 매겨진 국제 표준 도서 번호(ISBN)와 같이 모든 디지털 객체에 부여되는 고유 식별 번호다.

오답피하기 ⑤ 보기는 쿠키에 대한 설명이다.

정답 ⑤

〈문제적중〉 문제편 137페이지 39번 적중

13. 2014년 서울시 9급

다음은 어떤 공격에 대한 설명인가?

보기

웹사이트에서 입력을 엄밀하게 검증하지 않는 취약점을 이용하는 공격으로 사용자로 위장한 공격자가 웹사이트에 프로그램 코드를 삽입하여 나중에 이 사이트를 방문하는 다른 사용자의 웹 브라우저에서 해당 코드가 실행되도록 한다.

① HTTP 세션 탈취(session hijacking)
② 피싱(phishing)
③ 클릭 탈취(click jacking)
④ 사이트 간 스크립팅(Cross-site scripting : XSS)
⑤ 파밍(pharming)

정답 및 해설

◦ 클릭잭킹 (Clickjacking)은 마우스 클릭(Click)과 하이잭킹(Hijacking)을 더한 말로, 아이프레임(Iframe) 태그를 쓴 눈속임 공격 방법. 공격자가 사용자로 하여금 알아차리지 못하게 하고 어떤 것을 클릭하도록 속이는 것으로, 어떤 웹 페이지 혹은 버튼을 클릭하지만 실제로는 다른 페이지의 콘텐츠를 클릭하게 되는 것이다. 대처 방법은 스크립트 기능과 플러그 인(plug in) 기능을 무효화하거나 아이프레임을 활성화하지 않는 방법이 있다.

오답피하기 ④ 크로스 사이트 스크립팅 취약점(Cross Site Scripting Vulnerability, CSS, XSS)은 게시물에 실행코드와 태그의 업로드가 규제되지 않는 경우 이를 악용하여 열람한 타 사용자의 PC로 부터 정보를 유출할 수 있는 보안 취약점으로 보기는 이에 대한 설명이다.

정답 ④

〈문제적중〉 문제편 348페이지 43번 적중

14. 2014년 서울시 9급

다음 중 IPsec에 대한 설명으로 옳지 않은 것은?

① IPsec은 network layer에서 동작한다.

② Tunnel mode에서는 기존 패킷 앞에 IPsec 헤더 정보가 추가된다.
③ IKE 프로토콜은 SA를 협의하기 위해 사용된다.
④ AH 프로토콜은 메시지에 대한 인증과 무결성을 제공하기 위해 사용된다.
⑤ ESP 헤더는 메시지의 기밀성을 제공하기 위해 사용된다.

정답 및 해설

◦ 전송모드는 두 대의 호스트 간 종단 대 종단 통신에 사용되어 상위계층 프로토콜에 대한 암호화와 선택적 인증을 제공하는데 IP header를 제외한 IP payload가 보호되므로 전송되는 패킷의 트래픽 분석에는 노출된다.
◦ 터널모드는 한쪽 또는 양쪽 종단이 IPSec이 실행되는 방화벽이나 라우터 같은 보안 게이트웨이일 때 사용되어 전체 IP 패킷에 대한 보호를 제공한다.
◦ 즉, 안쪽 IP헤더는 source와 destination 주소를 가지고 바깥 IP 헤더는 보안 게이트웨이 주소를 가짐으로써 트래픽 분석에 의한 공격을 방지할 수 있다.

정 답 가답안 ②

〈이의제기〉 논란이 있을 수 있는 문제로 여겨짐.
〈문제적중〉 문제편 300페이지 21번 적중

15. 2014년 서울시 9급

DDoS(Distributed Denial of Service)에 대한 설명으로 옳지 않은 것은?

① 좀비PC 가 되지 않기 위해서는 신뢰할 수 없는 기관의 프로그램은 설치하지 않는 것이 좋다.
② DDoS공격은 특정 서버에 침입하여 자료를 훔쳐가거나 위조시키기 위한 것이다.
③ 좀비PC 가 되면 자신도 모르게 특정사이트를 공격하는 수단으로 이용될 수 있다.
④ 공격을 당하는 서버에는 서비스가 중지될 수 있는 큰 문제가 발생한다.
⑤ 좀비PC 는 악성코드의 흔적을 지우기 위해 스스로 하드디스크를 손상시킬 수도 있다.

정답 및 해설

오답피하기 ② DDoS 공격은 정보보안 목표의 가용성과 가장 밀접하게 관련되어 있다.

정 답 ②

〈문제적중〉 문제편 243페이지 31번 적중

16. 2014년 서울시 9급

다음의 접근 제어 모델 중 대상 기반의 접근 제어가 아니라 특정한 역할들을 정의하고 각 역할에 따라 접근 권한을 지정하고 제어하는 방식은?

① ACL
② DAC
③ RBAC
④ MAC
⑤ Capability

정답 및 해설

오답피하기 ③ RBAC은 1970년대 다중 사용자, 다중 프로그래밍 환경에서의 보안처리 요구를 만족시키기 위해 제안된 방식으로 사용자의 역할에 기반을 두고 접근을 통제하는 모델이다.

정 답 ③

〈문제적중〉 문제편 86페이지 3번 적중

17. 2014년 서울시 9급

IDS에 관한 다음의 설명 중 옳지 않은 것은?

① IDS를 이용하면 공격 시도를 사전에 차단할 수 있다.
② 기존 공격의 패턴을 이용해 공격을 감지하기 위해 signature 기반 감지 방식을 사용한다.
③ 알려지지 않았지만 비정상적인 공격 행위를 감지해서 경고 하기 위해 anomaly 기반 감지 방식을 사용한다.
④ DoS 공격, 패킷 조작 등의 공격을 감지하기 위해서는

network IDS를 사용한다.
⑤ IDS는 방화벽과 상호보완적으로 사용될 수 있다.

정답 및 해설

오답피하기 ① IDS(Intrusion Detection System)는 컴퓨터 또는 네트워크에서 발생하는 이벤트들을 모니터링(monitoring)하고, 침입 발생여부를 탐지(detection)하고, 대응(response)하는 자동화된 시스템으로 공격 시도를 사전에 차단하는 성격은 아니다.

정 답 ①

〈문제적중〉 이론편 562페이지 적중

18. 2014년 서울시 9급

다음 중 사용자 인증(user authentication)에 대한 설명으로 옳은 것은?

① 인터넷 뱅킹에 활용되는 OTP 단말(One Time Password Token)은 지식 기반 인증(authentication by what the entity knows)의 일종이다.
② 패스워드에 대한 사전 공격(dictionary attack)을 막기 위해 전통적으로 salt가 사용되어 왔다.
③ 통장 비밀번호로 흔히 사용되는 4자리 PIN(Personal Identification Number)은 소유 기반 인증(authentication by what the entity has)의 일종이다.
④ 지식 기반 인증(authentication by what the entity knows)의 가장 큰 문제는 오인식(False Acceptance), 오거부(False Rejection)가 존재한다는 것이다.
⑤ 건물 출입시 사용되는 ID 카드는 사람의 신체 또는 행위 특성을 활용하는 바이오 인식(biometric verification)의 일종이다.

정답 및 해설

오답피하기 ② (1)은 토큰을 이용한 Type Ⅱ에 대한 설명이고, (3)은 Type Ⅰ에 대한 설명이며, (4)는 Type Ⅲ에 대한 설명이다. (5)의 ID 카드는 Type Ⅱ에 대한 설명으로, 생체인증(바이오)와는 거리가 멀다.

정 답 ②

〈문제적중〉 이론편 198페이지 적중

19. 2014년 서울시 9급

다음에서 설명하고 있는 공격은?

보기
이 공격은 할당된 메모리 경계에 대한 검사를 하지 않는 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어쓰는 방식이다. 만약 실행 코드가 덮어써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.

① Buffer overflow 공격
② SQL injection 공격
③ IP spoofing 공격
④ Format String 공격
⑤ Privilege escalation 공격

정답 및 해설

◦ 권한상승공격(Privilege escalation 공격)이란 적절한 권한을 갖고 있지 않은 컴포넌트가 부당하게 권한을 획득해 접근해서는 안 될 자원에 접근 가능하게 되는 것을 말한다.

오답피하기 ① 버퍼오버플로우 공격은 해커가 데이터의 길이와 내용을 적절히 조정함으로써 버퍼 오버플로우를 일으키고 운영체제의 스택을 붕괴시켜 특정 코드가 실행되도록 하는 것이다.

정 답 ①

〈문제적중〉 문제편 385페이지 1번 적중

20. 2014년 서울시 9급

다음 중 개인정보 보호법에 대한 설명으로 맞는 것은?

① 개인정보 보호위원회의 위원은 대통령이 임명한다.
② 정보주체란 개인정보를 생성 및 처리하는 자를 의미한다.
③ 개인정보는 어떠한 경우에도 제3자에게 제공되거나 공유되어서는 안된다.
④ 개인정보의 처리 목적이 달성된 이후에는 개인정보를 1년간 보관하여야 한다.
⑤ 보호 대상이 되는 개인정보는 주민등록번호 등을 포함하여 생존 및 사망한 개인을 식별할 수 있는 정보를 의미한다.

정답 및 해설

◦ 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다.

오답피하기 ② "정보주체"란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
③ 개인정보는 정보주체의 동의를 받은 경우 등에서 제3자에게 제공할 수 있다.
④ 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다.
⑤ "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말하는 사망자의 정보는 해당 없다.

정답 ①

〈문제적중〉 이론편 831페이지 적중