2018년 지방직 9급 정보보호론 총평

-지안학원 조현준 선생

1. 문제분석

(가) 출제 경향 분석

정보보호론이 공무원 시험과목으로 편입되고 올해로 5년차에 들어갑니다. 초창기에는 난이도 편차가 심해서 수험생들이 공부하기 어려웠는데 5년차에 들어가면서 출제 범위와 방향이 보이는 것 같습니다. 정보보안 관련 시험이 공무원 정보보호직, 해양경찰청, 경찰간부와 정보보안기사 시험 등이 있는데 이런 시험을 전산개발 정보보호론이 뒤따라가고 있습니다. 현재 출제 경향은 범위는 넓어지고 있고, 깊이는 점점 깊어지고 있습니다.

(나) 난이도 분석

전체적으로 올해 시행된 국가직 정보보호론보다는 쉬었고, 전년도 지방직 시험과는 비슷한 난이도 수준으로 판단됩니다. 이는 국가직 지안합격예측서비스와 지방직 설문조사(5월23일 시행) 결과 수험생 득점을 보면 제가 추정한 것과 비슷하게 객관적으로 나타나고 있습니다. 국가직에서는 85점~100점이 소수였는데, 이번 지방직은 85~100점이신 분들이 많이 늘었습니다.

2. 오프라인 수강생 설문조사

(가) 설문조사 주요 항목

1. 현재까지 시험을 준비한 기간?
2. 가채점 결과 본인의 점수?
3. 지안에듀 수강여부?(이론/기출/적중800제/모의고사)
4. 정보보호론 이론편/문제편 회독수?
5. 탑스팟 정보보호론으로 공부 안한 경우 교재와 학원?

(나) 설문조사 결과(온라인 제외)

동일 강의를 들어도 경쟁률이 높은 공무원시험을 모두가 합격할 수 없습니다. 개인마다 상황은 모두 다를 것입니다. 그래서 정보보호론에서 85 ~ 100점의 고득점을 받으신 분들의 공부방법만 안내드리고자 합니다. 설문결과 고득점자는 평균적으로 1년이상 공무원 시험준비를 하셨고, 지안에듀의 정규 커리큘럼(이론~모의고사)을 대다수 따라오신 분들였고, 교재 회독수는 평균 2~3회독 이상을 하신 분들였습니다. 회독수가 낮으면 상대적으로 점수가 낮았습니다. 그리고 이번 지방직 시험은 수업시간에 강조한 부분이 많이 출제되어 고득점자의 문제푸는 시간은 평균 6~7분정도였다고 합니다.

3. 탑스팟 정보보호론 적중률 분석

(가) 적중률(○○~○○%)

이번 시험은 수업시간에 나올 것을 예상한 내용들이 다른 시험에 비해서 많았던 것 같습니다. 그래서 수업을 충실히 듣고 정리하신 분들은 상대적으로 좋은 결과가 있었던 것 같습니다. 대다수가 이론서와 문제집에 있는 내용이고, 일부 몇 문제는 교재의 내용을 조합 응용해서 푸는 문제들였습니다. 적중률의 구체적인 수치는 주관적일 수 있기에 문항하다 출처를 표시해놨으니 참고 바랍니다.

4. 향후 학습방향

(가) 기본에 충실한 공부를 해라.

모든 공부나 시험이 그러하듯이 기본에 충실한 공부를 하셔야 합니다. 주춧돌을 올리고, 벽돌 하나하나씩 올려서 집을 완성해야 합니다. 많은 분들이 저한테 상담해올 때, 저는 단계적으로 공부할 것을 권합니다. 이론수업 → 기출 → 적중800제 → 모의고사 훈련 순서입니다. 순서를 무시하고 공부하면 항상 응용에 한계에 부딪치게 되어 점수가 낮게 나올 수 있어서 상대평가 시험을 보시는 분들에게 치명적일 수 있습니다. 그리고 얇은 책을 선호하지 마세요. 얇은 책은 이해하기 힘들고, 구멍이 많을 수가 있습니다. 국내에서 시행되는 모든 공개/비공개 빅데이터(BigData)를 가지고 수업·지도하면서 강조했던 내용을 다시 당부 드립니다.

(나) 이론서와 적중800제 회독수를 늘려라.

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.

5. 지안 공무원학원 향후 수업 안내

(가) 서울시 대비 모의고사반(4주)

지방직 대비과정과 동일하게 법규문제를 제일 앞에 배치하여, 수험생에게 두려움을 없애도록 할 예정입니다. 매주 첫 시간은 기출 해설 강의가 있을 예정이고, 2018년 3월 31일 시행된 정보보안기사 문제를 포함하여 모의고사반을 진행할 예정입니다.

(나) 국가직 7급, 군무원, 경찰간부(4주)

최신 감리사, 공무원, 정보보안기사 문제를 포함하여 모의고사식으로 진행할 예정입니다. 참고로 군무원시험은 프로그래밍언어론에서 정보보호론으로 대체후 시행되는 첫 시험입니다. 3과목(국어, 컴일, 정보)만 필기시험을 치루므로 전공 특히 정보보호론의 중요성은 아무리 강조해도 지나치지 않습니다. 가급적 공무원 정보보호론과 정보보안기사까지 정리할 것을 추천드립니다.

(다) 2019년 개정판

- 개정판 강의 : 2018년 9월 ~

2018년 지방직 9급 정보보호론

-2018년 5월 19일 시행

1. 18.지방.9급

정보보호의 3대 요소 중 가용성에 대한 설명으로 옳은 것은?

① 권한이 없는 사람은 정보자산에 대한 수정이 허락되지 않음을 의미한다.
② 권한이 없는 사람은 정보자산에 대한 접근이 허락되지 않음을 의미한다.
③ 정보를 암호화하여 저장하면 가용성이 보장된다.
④ DoS(Denial of Service) 공격은 가용성을 위협한다.

가용성(Availability)
- 시스템이 지체 없이 동작하도록 하고, 합법적 사용자가 서비스 사용을 거절당하지 않도록 하는 것이다.
- 가용성을 확보하기 위해서는 데이터의 백업, 중복성의 유지, 물리적 위협요소로부터의 보호 등의 보안 기술을 적용해야 한다.
- 시스템 가용성은 장비 혹은 소프트웨어 실패에 의해 영향을 받을 수 있다. 중대한 시스템을 신속하게 교체할 수 있도록 백업 장비가 사용되어야 하며, 시스템을 다시 가동시키기 위해 필요한 조치를 취할 수 있는 능력을 갖추어야 한다. 환경적 논점(예를 들면 열, 추위, 습도, 정전기, 그리고 오염 물질 등)은 시스템 가용성에 영향을 줄 수 있다.

오답피하기 ① 무결성 ② 기밀성 ③ 정보를 암호화하여 저장하면 기밀성이 보장된다.

정답 ④

이론서 32p 적중

2. 18.지방.9급

ISO/IEC 27001에서 제시된 정보보안관리를 위한 PDCA 모델에서 ISMS의 지속적 개선을 위해 시정 및 예방 조치를 하는 단계는?

① Plan
② Do
③ Check
④ Act

- 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 ISMS의 지속적 개선을 위해 시정 및 예방 조치를 하는 단계는 처리(Act) 단계이다.

정답 ④

이론서 645p 적중

3. 18.지방.9급

보안 관리 대상에 대한 설명으로 ㉠ ~ ㉢에 들어갈 용어는?

보기
- ㅇ (㉠) – 시스템과 네트워크의 접근 및 사용 등에 관한 중요 내용이 기록되는 것을 말한다.
- ㅇ (㉡) – 사용자와 시스템 또는 두 시스템 간의 활성화된 접속을 말한다.
- ㅇ (㉢) – 자산에 손실을 초래할 수 있는 원치 않는 사건의 잠재적 원인이나 행위자를 말한다.

	㉠	㉡	㉢
①	로그	세션	위험
②	로그	세션	위협
③	백업	쿠키	위험
④	백업	쿠키	위협

- 로그(log) : 시스템 사용에 관련된 전체의 기록, 즉 입출력내용, 프로그램 사용 내용, 자료변경내용, 시작시간, 종료시간 등의 기록이다.
- 세션(Session) : 단말 영역과 서버 영역 간 논리적 연결 방법으로, 이용자 연결 정보는 서버 영역에 남겨두고, 세션 정보만을 단말 영역에 남기는 기술이다.
- 위협 : 자산이 가진 고유의 취약점을 이용하여 자산에 직접적인 피해를 줄 수 있는 요소로서, 자산이 가진 취약점을 통해서만 자산에 피해를 줄 수 있다.

오답피하기 ② 로그, 세션, 위협에 대한 용어설명으로 보안공부를 위해서 반드시 숙지해야 한다.

정답 ②

이론서 645p 응용

4. 18.지방.9급

유닉스 시스템에서 파일의 접근모드 변경에 사용되는 심볼릭 모드 명령어에 대한 설명으로 옳은 것은?

① chmod u-w: 소유자에게 쓰기 권한 추가
② chmod g+wx: 그룹, 기타 사용자에게 쓰기와 실행 권한 추가
③ chmod a+r: 소유자, 그룹, 기타 사용자에게 읽기 권한 추가
④ chmod o-w: 기타 사용자에게 쓰기 권한 추가

chmod 명령
- chmod 명령은 기존 파일 또는 디렉터리에 대한 접근권한을 변경할 때 사용한다.
- 접근권한을 기호로 기술하는 방법
  - 대상 : u(user), g(group), o(other), a(ll)
  - 연산자 : +(추가), -(제거), =(지정)

– 접근권한 : r(읽기), w(쓰기), x(실행)

오답피하기 ① chmod u-w: 소유자에게 쓰기 권한 제거, ② chmod g+wx: 그룹 사용자에게 쓰기와 실행 권한 추가, ④ chmod o-w: 기타 사용자에게 쓰기 권한 제거

정답 ③

기출문제집 255번 경간부 유사

5. 18.지방.9급

정보가 안전한 정도를 평가하는 TCSEC(Trusted Computer System Evaluation Criteria)의 보안등급 중에서 검증된 설계(Verified Design)를 의미하는 보안등급은?

① A 등급
② B 등급
③ C 등급
④ D 등급

TCSEC 단계

- D(Minimal Protection) : 보안 설정이 이루어지지 않은 단계이다.
- C1(Discretionary Security Protection) : 일반적인 로그인 과정이 존재하는 시스템이다. 사용자 간 침범이 차단되어 있고 모든 사용자가 자신이 생성한 파일에 대해 권한을 설정할 수 있으며, 특정 파일에 대해서만 접근이 가능하다. 초기의 유닉스 시스템이 C1 등급에 해당된다.
- C2(Controlled Access Protection) : 각 계정별 로그인이 가능하며 그룹 ID에 따라 통제가 가능한 시스템이다. 보안 감사가 가능하며 특정 사용자의 접근을 거부할 수 있다. 윈도우 NT 4.0과 현재 사용되는 대부분의 유닉스 시스템이 C2 등급에 해당된다.
- B1(Labeled Security) : 시스템 내에 보안 정책을 적용할 수 있고 각 데이터에 대해 보안 레벨 설정이 가능하다. 시스템 파일이나 시스템에 대한 권한을 설정할 수 있다.
- B2(Structured Protected) : 시스템에 정형화된 보안 정책이 존재하며 B1 등급의 기능을 모두 포함한다.
- B3(Security Domains) : 운영체제에서 보안에 불필요한 부분을 모두 제거하고, 모듈에 따른 분석 및 테스트가 가능하다.
- A1(Verified Design) : 수학적으로 완벽한 시스템이다. 현재까지 A1 등급을 받은 시스템은 없으므로 사실상 이상적인 시스템이다.

오답피하기 ① Verified Design은 A1 단계를 의미한다.

정답 ①

기출문제집 634번 기출해설 적중

6. 18.지방.9급

다음에서 설명하는 공격 기술은?

> 보기
> 암호 장비의 동작 과정 중에 획득 가능한 연산시간, 전력소모량, 전자기파 방사량 등의 정보를 활용하여 암호 알고리즘의 비밀 정보를 찾아내는 기술

① 차분 암호 분석 공격(Differential Cryptanalysis Attack)
② 중간자 공격(Man-In-The-Middle Attack)
③ 부채널 공격(Side-Channel Attack)
④ 재전송 공격(Replay Attack)

스마트카드 공격 기법

공격기법	설명
소프트웨어 공격	◦ 애플리케이션, 알고리즘, 프로토콜 등에서 발견되는 취약점을 공격하는 기법
마이크로 프로빙 (Micro probing)	◦ 마이크로 프로세스 칩 표면에 직접 접근하여 보호요소를 제거하지 않고, 초음파 진동만을 사용 ◦ 카드의 ROM 칩에 직접 신호를 주어 조작이 가능
도청 기법	◦ 프로세서에서 방사되는 전자기파를 모니터링/도청하는 기법
장애 유발 기법	◦ 비정상 환경조건에서 프로세서가 오동작하도록 만드는 기술
부채널 공격 (Side-channel attack)	◦ 침입공격이 아니며 약점이나 문제점을 이용하지 않고 어떻게 동작하는지에 대한 중요한 정보를 알아내기 위해 사용 예) 차등전압분석(프로세스가 처리되는 과정에서 발생하는 전원을 검사), 전자기파분석(방사되는 주파수를 검사), 타이밍(특정 프로세스작업이 완료되기까지 소요시간 측정)

오답피하기 ③ 부채널 공격(Side-Channel Attack)은 공격 대상 통신기기가 작동하고 있을 때 사용하는 소비 전력 또는 발사되는 전자파 정보 등을 이용하여 통신 기기 내부에 있는 암호키와 같은 중요한 정보를 알아내는 공격이다.

정답 ③

2017년 이론서 203p 적중, 2018년 이론서 74p, 105p, 137p 응용

7. 18.지방.9급

DoS(Denial of Service) 공격의 대응 방법에 대한 설명으로 ㉠, ㉡에 들어갈 용어는?

> 보기
> ○ 다른 네트워크로부터 들어오는 IP broadcast 패킷을 허용하지 않으면 자신의 네트워크가 (㉠) 공격의 중간 매개지로 쓰이는 것을 막을 수 있다.
> ○ 다른 네트워크로부터 들어오는 패킷 중에 출발지 주소가 내부 IP 주소인 패킷을 차단하면 (㉡) 공격을 막을 수 있다.

	㉠	㉡
①	Smurf	Land
②	Smurf	Ping of Death
③	Ping of Death	Land
④	Ping of Death	Smurf

◦ 스머프 공격의 대응책은 중간매개지로 쓰이는 것을 막기 위해 라우터에서 다른 네트워크로부터 자신의 네트워크로 들어오는 IP directed broadcast 패킷을 막도록 설정한다. 또한 호스트는 IP broadcast address로 전송된 ICMP 패킷에 대해 응답하지 않도록 시스템을 설정할 수 있다.

◦ Land Attack의 탐지방법은 TCP 패킷의 소스 IP, 포트와 목적지 IP, 포트가 동일한지 확인한다(source 주소가 내부 IP인 패킷 차단).

오답피하기 ① 스머프 공격은 라우터나 호스트에서 Broadcast를 차단하고, Land Attack은 외부에서 들어오는 패킷 중에 출발지 주소가 내부 IP로 변경된 것을 탐지하여 차단하는 방법으로 대응할 수 있다.

정답 ①

이론서 445p, 447p 적중

8. 18.지방.9급

「전자서명법」상 용어의 정의로 옳지 않은 것은?

① '전자서명'이라 함은 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

② '인증서'라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.

③ '서명자'라 함은 전자서명검증정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

④ '전자서명생성정보'라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

오답피하기 ③ "서명자"라 함은 전자서명생성정보를 보유하고 자신이 직접 또는 타인을 대리하여 서명을 하는 자를 말한다.

정답 ③

이론서 734p 적중

9. 18.지방.9급

「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 구현 단계 보안약점을 연결한 것으로 옳지 않은 것은?

분석·설계 단계 보안요구항목	구현 단계 보안약점
① DBMS 조회 및 결과 검증	SQL 삽입
② 디렉터리 서비스 조회 및 결과 검증	LDAP 삽입
③ 웹서비스 요청 및 결과 검증	크로스사이트 스크립트
④ 보안기능 동작에 사용되는 입력값 검증	솔트 없이 일방향 해시함수 사용

보안약점과 보안요구항목과 연관 관계

보안요구항목	보안약점
입력 데이터 검증 및 표현	
DBMS 조회 및 결과 검증	◦ SQL 삽입
XML 조회 및 결과 검증	◦ XQuery 삽입 ◦ XPath 삽입
디렉터리 서비스 조회 및 결과 검증	◦ LDAP 삽입
시스템 자원 접근 및 명령어 수행 / 입력값 검증	◦ 경로조작 및 자원삽입 ◦ 운영체제 명령어 삽입
웹 서비스 요청 및 결과 검증	◦ 크로스사이트 스크립트
웹 기반 중요기능 수행 요청 유효성 검증	◦ 크로스사이트 요청 위조
HTTP프로토콜 유효성 검증	◦ 신뢰되지 않은 URL 주소로 자동접속 연결 ◦ HTTP 응답분할
허용된 범위내 메모리 접근	◦ 포맷스트링 삽입 ◦ 메모리 버퍼 오버플로우
보안기능 동작에 사용되는 입력값 검증	◦ 보안기능 결정에 사용되는 부적절한 입력값 ◦ 정수형 오버플로우 ◦ Null Pointer 역참조
업로드·다운로드 파일 검증	◦ 위험한 형식 파일 업로드 ◦ 무결성 검사 없는 코드 다운로드
보안 기능	
인증대상 및 방식	◦ 적절한 인증 없는 중요기능 허용 ◦ DNS lookup에 의존한 보안결정
인증수행 제한	◦ 반복된 인증시도 제한기능 부재
비밀번호 관리	◦ 하드코드된 비밀번호 ◦ 취약한 비밀번호 허용
중요자원 접근통제	◦ 부적절한 인가 ◦ 중요한 자원에 대한 잘못된 권한 설정
암호키 관리	◦ 하드코드된 암호화 키 ◦ 주석문 안에 포함된 시스템 주요 정보
암호연산	◦ 취약한 암호화 알고리즘 사용 ◦ 충분하지 않은 키 길이 사용 ◦ 적절하지 않은 난수 값 사용 ◦ 솔트없이 일방향 해시함수 사용
중요정보 저장	◦ 중요정보 평문저장 ◦ 사용자 하드디스크에 저장되는 쿠키를 통한 정보노출
중요정보 전송	◦ 중요정보 평문전송
에러 처리	
예외처리	◦ 오류메시지를 통한 정보노출 ◦ 시스템 데이터 정보노출
세션 통제	
세션통제	◦ 잘못된 세션에 의한 데이터 정보노출

오답피하기 ④ 솔트없이 일방향 해시함수 사용은 보안 기능의 암호연산과 관련된 보안 약점이다.

정답 ④

이론서 163p 응용

10. 18.지방.9급

개인정보 보호법령상 영업양도 등에 따른 개인정보의 이전 제한에 대한 내용으로 옳지 않은 것은?

① 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다.

② 영업양수자등이 과실 없이 서면 등의 방법으로 개인정보를 이전받은 사실 등을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 10일 이상 게재하여야 한다.

③ 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 개인정보를 이전하려는 사실 등을 서면 등의 방법에 따라 해당 정보주체에게 알려야 한다.

④ 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 서면 등의 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 「개인정보 보호법」 제27조 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

➡ 제27조(영업양도 등에 따른 개인정보의 이전 제한)

① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

➡ 영업양도 등에 따른 개인정보 이전의 통지(시행령 제29조)

1. 서면 등의 방법
2. 서면으로 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다(다만, 인터넷 홈페이지를 운영하지 아니하는 영업양도자 등의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시).

오답피하기 ② 10일이상이 아닌 30일이상 인터넷 홈페이지에 게재하여야 한다.

정답 ②

이론서 750p 적중

11. 18.지방.9급

대칭키 암호 알고리즘에 대한 설명으로 옳은 것만을 모두 고르면?

보기

ㄱ. AES는 128/192/256 비트 키 길이를 지원한다.
ㄴ. DES는 16라운드 Feistel 구조를 가진다.
ㄷ. ARIA는 128/192/256 비트 키 길이를 지원한다.
ㄹ. SEED는 16라운드 SPN(Substitution Permutation Network) 구조를 가진다.

① ㄱ, ㄹ
② ㄴ, ㄷ
③ ㄱ, ㄴ, ㄷ
④ ㄱ, ㄴ, ㄹ

오답피하기 ③ SEED는 1999년 한국정보진흥원(현 한국인터넷진흥원)과 국내 암호전문가들이 함께 개발한 알고리즘으로 16라운드 Feistel 구조를 가진다. 나머지 문항은 자주 출제되는 내용으로 암기하여야 한다.

정답 ③

이론서 86p 적중

12. 18.지방.9급

다음에서 설명하는 프로토콜은?

보기

○ 무선랜 통신을 암호화하는 프로토콜로서 IEEE 802.11 표준에 정의되었다.
○ 암호화를 위해 RC4 알고리즘을 사용한다.

① AH(Authentication Header)
② SSH(Secure SHell)
③ WAP(Wireless Application Protocol)
④ WEP(Wired Equivalent Privacy)

➡ WEP(Wired Equivalent Privacy)

◦ 무선 데이터 암호화 방식으로 많이 사용되고 있는 WEP은 전송되는 MAC 프레임을 40비트의 WEP 공유 비밀 키와 임의로 선택되는 24비트의 Initialization Vector(IV)로 조합된 총 64비트의 키를 이용한 RC4 스트림 암호화방식으로 보호한다.

◦ 기본적으로 무선 클라이언트와 무선 AP는 동일한 패스워드 문장으로부터 4개의 고정된 장기 공유키를 생성한 후 이들 중에서 하나를 선택하여 암호 및 인증에 활용한다.

◦ 문제는 선택된 공유키의 KEY ID와 IV값을 평문으로 상대방에게 알려줘야 하기 때문에 WEP키가 추출될 수 있는 약점이 존재한다.

◦ WEP과 관련된 세 가지 핵심 결점은 정적 암호와 키의 사용, IV의 비효율적 사용, 그리고 패킷 무결성 보장의 부족이다.

오답피하기 ④ WEP는 대표적인 무선랜 통신 암호화 프로토콜로 RC4 알고리즘을 사용하며, 현재는 여러 취약점을 가지고 있는 안전하지 않은 프로토콜로 분류되고 있다.

정답 ④

이론서 400p 적중

13. 18.지방.9급

기밀성을 제공하는 암호 기술이 아닌 것은?

① RSA
② SHA-1
③ ECC
④ IDEA

◦ RSA, ECC는 비대칭키 알고리즘으로 기밀성, 인증, 부인방지 서비스 등을 제공하고, IDEA는 대칭키 알고리즘으로 기밀성 서비스를 제공한다.
오답피하기 ② SHA-1은 해시함수로 무결성 서비스를 주로 제공한다.
정답 ②

이론서 53p 적중

14. 18.지방.9급

SSL 프로토콜에 대한 설명으로 옳지 않은 것은?

① 전송계층과 네트워크계층 사이에서 동작한다.
② 인증, 기밀성, 무결성 서비스를 제공한다.
③ Handshake Protocol은 보안 속성 협상을 담당한다.
④ Record Protocol은 메시지 압축 및 암호화를 담당한다.

오답피하기 ① SSL 프로토콜은 전송계층과 응용계층 사이에서 동작한다.
정답 ①

적중800제 285번, 286번, 287번 적중

15. 18.지방.9급

DSA(Digital Signature Algorithm)에 대한 설명으로 옳지 않은 것은?

① 기밀성과 부인방지를 동시에 보장한다.
② NIST에서 발표한 전자서명 표준 알고리즘이다.
③ 전자서명의 생성 및 검증 과정에 해시함수가 사용된다.
④ 유한체상의 이산대수문제의 어려움에 그 안전성의 기반을 둔다.

◦ DSA(Digital Signature Algorithm)는 전자서명에 대한 미 연방 정부 표준 DSS이고 NIST가 제안하였다. ElGamal 서명 스킴보다 서명 길이가 320비트로 짧고, ElGamal에 대한 공격 중 일부가 적용되지 않는다는 것이다.
오답피하기 ① DSA(Digital Signature Algorithm)는 전자서명 알고리즘으로 기밀성 서비스를 제공하지 못한다.
정답 ①

이론서 143p 적중

16. 18.지방.9급

무의미한 코드를 삽입하고 프로그램 실행 순서를 섞는 등 악성코드 분석가의 작업을 방해하는 기술은?

① 디스어셈블(Disassemble)
② 난독화(Obfuscation)
③ 디버깅(Debugging)
④ 언패킹(Unpacking)

오답피하기 ② 코드 난독화(Code Obfuscation) : 프로그램을 바꾸는 방법의 일종으로, 코드를 읽기 어렵게 만들어 역공학을 통한 공격을 막는 기술을 의미한다. 난독화는 대상에 따라 크게 소스코드 난독화와 바이너리 난독화로 나눌 수 있다. 소스코드 난독화는 C/C++/자바 등의 프로그램의 소스코드를 알아보기 힘든 형태로 바꾸는 기술이고, 바이너리 난독화는 컴파일 후에 생성된 바이너리를 역공학을 통해 분석하기 힘들게 변조하는 기술이다.
정답 ②

기출문제집 588번 적중

17. 18.지방.9급

윈도우즈용 네트워크 및 시스템 관리 명령어에 대한 설명으로 옳은 것은?

① ping – 원격 시스템에 대한 경로 및 물리 주소 정보를 제공한다.
② arp – IP 주소에서 물리 주소로의 변환 정보를 제공한다.
③ tracert – IP 주소, 물리 주소 및 네트워크 인터페이스 정보를 제공한다.
④ ipconfig – 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다.

◦ 동일 네트워크에 존재하는 호스트 A와 B의 IP 주소가 I_a와 I_b이고 물리 주소는 P_a와 P_b라고 가정할 때, 호스트 A의 네트워크 계층에서는 호스트 B로 패킷을 전송할 때 목적지 I_b에 해당하는 P_b를 찾는 과정을 수행하는데, 이때 사용되는 프로토콜이 ARP이다.
오답피하기 ① ping – 원격 시스템의 동작 여부 및 RTT(Round Trip Time) 정보를 제공한다. ③ tracert – 원격 시스템에 대한 경로 정보를 제공한다. ④ ipconfig – IP 주소, 물리 주소 및 네트워크 인터페이스 정보를 제공한다.
정답 ②

이론서 353p 적중

18. 18.지방.9급

정보자산에 대한 위험분석에서 사용하는 ALE(Annualized Loss Expectancy, 연간예상손실액), SLE(Single Loss Expectancy, 1회손실예상액), ARO(Annualized Rate of Occurrence, 연간발생빈도) 사이의 관계로 옳은 것은?

① ALE = SLE + ARO
② ALE = SLE × ARO
③ SLE = ALE + ARO
④ SLE = ALE × ARO

◦ 노출계수(exposure factor) : 어떤 자산에 대해 실현된 위험으로 인해 침해가 발생할 때 조직이 입게 되는 손실 비율(%)
◦ SLE : 한 번의 침해로 발생한 손실액
SLE = 자산가치 × 노출계수
◦ ARO : 연간 발생률은 1년 동안의 시간 단위에서 특정한 위협이 발생할 수 있는 빈도를 추정하는 값
◦ ALE
ALE = ARO × SLE

오답피하기 ② ALE(Annualized Loss Expectancy)는 정량적 위험분석 방법으로 1회손실예상액(SLE)와 연간발생빈도(AR))의 곱으로 표현된다.

정답 ②

이론서 662p 적중

19. 18.지방.9급

개인정보 보호법」상 개인정보 보호 원칙으로 옳지 않은 것은?

① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.
④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀로 하여야 한다.

개인정보 보호 원칙(제3조)

◦ 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다(수집제한의 원칙, 목적 명확화의 원칙).
◦ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다(이용제한의 원칙).
◦ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다(정보 정확성의 원칙)
◦ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다(안정성 확보의 원칙).
◦ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다(처리방침 공개의 원칙, 정보주체 참여의 원칙).
◦ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다(수집제한의 원칙).
◦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다(수집제한의 원칙).
◦ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다(책임의 원칙).

오답피하기 ④ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 비밀이 아닌 공개하여야 한다.

정답 ④

이론서 739p 적중

20. 18.지방.9급

다음에서 설명하는 블록암호 운용 모드는?

보기
○ 암복호화 모두 병렬 처리가 가능하다.
○ 블록 암호 알고리즘의 암호화 로직만 사용한다.
○ 암호문의 한 비트 오류는 복호화되는 평문의 한 비트에만 영향을 준다.

① ECB
② CBC
③ CFB
④ CTR

CTR 모드

장점	단점
• 패딩이 필요 없다. • 암·복호화의 사전 준비 가능. • 암·복호화가 같은 구조 • 비트 단위의 에러가 있는 암호문을 복호화하면 평문의 대응하는 비트만 에러가 난다. • 병렬 처리 가능(암·복호화 양쪽)	• 적극적 공격자가 암호문 블록의 비트를 반전시키면 대응하는 평문 블록의 비트가 반전된다.

오답피하기 ④ CTR 모드가 ATM(asynchronous transfer mode) 네트워크 보안과 IPSec(IP security)에 응용되면서 최근 들어 관심이 늘어나는 모드이다. 보기는 CTR 모드의 장점에 대한 설명이다.

정답 ④

이론서 98p 적중