2018년 교육청 9급 정보보호론 총평

-지안학원 조현준 선생

1. 문제분석

(가) 출제 경향 분석

교육청 정보보보호론이 공무원 시험과목으로 편입되고 올해로 5년차에 들어갑니다. 처음 3년간은 문제가 비공개(적중 800제 수록)였고, 최근 2년전부터 공개하기 시작했습니다. 행정안전부에 출제하는 문제스타일과 수능을 출제하는 한국교육과정평가원의 문제 스타일이 확실히 차이가 있는 같습니다. 향후 교육청 시험을 대비하시는 분들은 이런 문제 유형에 익숙하셔야할 것 같습니다.

(나) 난이도 분석

전년도 교육청 문제보다는 많이 어려웠고, 2018년에 시행된 국가직, 지방직보다 어려운 편였습니다. 일부 한 두 문제는 정보보안기사를 뛰어넘는 문제도 있었고, 정교하게 다듬어진 함정 문제들도 많았습니다. 오프라인 학원 설문조사 결과 고득점자도 소수였습니다. 정보보호론은 난이도가 높을수록 수험생간 점수편차가 매우 큽니다. 이번 시험에서 최근 교재로 정보보호론을 제대로 정리하신 분들은 합격 효자과목의 역할을 톡톡히 하겠지만, 대다수 수험생들이 점수가 잘 안 나왔을 것 같습니다.

2. 탑스팟 정보보호론 적중률 분석

(가) 적중률(○○~○○%)

시험의 난이도가 높을수록 이론서의 확실한 개념정리가 중요합니다. 문제집도 기출문제집보다는 난이도가 높은 적중 800제가 보다 높은 비율로 적중한 것 같습니다. 대다수 문제가 이론서와 문제집에 있는 내용였습니다. 하지만, S-Box 계산 문제는 개념만 이론교재에 있었는데, 실제 계산법이 나와서 많은 분들이 틀렸을 것 같습니다. 디피-헬만의 원시근을 구하는 문제도 많은 응용을 요하는 문제였습니다. 일부 문제는 이론서와 적중800제 지문과 유사한 것도 있었지만, 전체적으로 이론서와 적중800제의 내용을 조합 응용해서 푸는 문제들이 많아서 응용력이 약한 분들은 체감 난이도가 높았을 것 같습니다. 적중률의 구체적인 수치는 주관적일 수 있기에 문항하다 출처를 표시해놨으니 참고 바랍니다.

3. 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 → 적중 800제 → 모의고사 훈련 순서입니다. 순서를 무시하고 공부하면 항상 응용에 한계에 부딪치게 되어 점수가 낮게 나올 수 있어서 상대평가 시험을 보시는 분들에게 치명적일 수 있습니다. 목표로 하는 시험의 남은 시간을 체크하여 만약 부족하다고 생각되시면 어느 부분부터 보완할 지 잘 판단하여 진행하시길 바랍니다. 정보보호론은 어느 정도 시간투자를 하면 비전공자도 합격 전략과목으로 만들 수 있는 과목입니다.

(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.

4. 지안 공무원학원 향후 수업 안내

(가) 서울시 대비 모의고사반(4주)

지방직, 교육청 대비과정과 동일하게 법규문제를 제일 앞에 배치하여, 수험생에게 두려움을 없애도록 할 예정입니다. 매주 첫 시간은 기출 해설 강의가 있을 예정이고, 2018년 3월31일 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 ~

※ 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.

2018년 교육청 9급 정보보호론

-2018년 5월 19일 시행

1.

다음 설명을 모두 만족하는 정보보호의 목표는?

보기

- ㅇ 인터넷을 통해 전송되는 데이터 암호화
- ㅇ 데이터베이스와 저장 장치에 저장되는 데이터 암호화
- ㅇ 인가된 사용자들만이 정보를 볼 수 있도록 암호화

① 가용성
② 기밀성
③ 무결성
④ 신뢰성

오답피하기 ② 기밀성은 정보의 소유자가 원하는 대로 정보의 비밀이 유지되어야 함을 말한다. 정보는 소유자의 인가를 받은 사람만이 접근할 수 있어야 한다. 기밀성 보장을 위해서 접근통제와 암호화 메커니즘을 적용한다.

정답 ②

이론서 32p 적중, 기출 3번 적중

2.

다음은 신문기사의 일부이다. 빈칸 ㉠에 공통으로 들어갈 용어로 옳은 것은?

㉠ 은(는) 하나의 PC로 제어되는 대규모 온라인 기기 모음이며, 악성 소프트웨어를 이용해 빼앗은 다수의 좀비 컴퓨터로 구성되는 네트워크라고 볼 수 있다. 일반적으로 PC, 공유기, 스마트 폰, 웹캠, 태블릿 등을 악성코드에 감염시켜 사용한다. ㉠ 은(는) 특정 온라인 서버를 표적으로 다운시키거나 대규모 스팸 캠페인을 전달하는 DDoS 공격에 사용할 수 있다. 또한 사용자는 자신의 기기에 있는 악성코드를 인식하지 못하기 때문에 사생활 침해 사기에 개인 정보를 쉽게 도용당할 수 있다.

– 2017년 ○월 ○일자 –

① 웜(worm)
② 봇넷(botnet)
③ 루트킷(rootkit)
④ 랜섬웨어(ransomware)

◦ 웜(Worm) : 분산형 시스템, 네트워크에 상주하는 독립 프로그램 또는 실행 가능한 코드 모듈을 말한다. 웜은 가능한 많은 시스템 자원을 이용하기 위해 필요하다면 스스로 자기 자신을 복제한다.
◦ 루트킷(Rootkit) : 시스템 침입 후 침입 사실을 숨긴 채 차후의 침입을 위한 백도어, 트로이목마 설치, 그리고 원격접근, 내부 사용흔적 삭제, 관리자권한 획득 등 주로 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램들의 모음.
◦ 랜섬웨어(Ransomware) : 미국에서 발견된 스파이웨어 등의 신종 악성 프로그램. 컴퓨터 사용자의 문서를 볼모로 잡고 돈을 요구한다고 해서 '랜섬(ransom)'이란 수식어가 붙었다. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접촉해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하기도 한다.

오답피하기 ② 감염된 시스템의 CPU와 네트워크 자원을 공격자 자신의 용도로 사용하는 종류이다. 이렇게 감염된 시스템을 봇(robot에서 bot를 따옴), 좀비, 혹은 drone이라고 부르는데, 인터넷에 연결되어 있는 컴퓨터를 조용히 감염시켜 조종함으로써 봇의 제작자가 누구인지 알기 힘든 여러 가지 공격을 감행할 수 있게 된다. 보통 봇은 의심받지 않는 제3자에게 속해 있는 수백, 수천 개의 컴퓨터에 심어진다. 이 봇의 집합이 서로 협력하는 형태의 행동을 취할 수도 있는데, 이를 봇넷(botnet)이라고 한다.

정답 ②

이론서 633p 적중, 기출 499번 적중, 적중800제 330번 유사

3.

다음 스푸핑(spoofing) 공격에 대한 설명 (가)~(다)를 바르게 짝지은 것은?

보기

(가) 공격 대상이 잘못된 IP 주소로 웹 접속 유도
(나) 권한 획득을 위하여 다른 사용자의 IP 주소 강탈
(다) MAC 주소를 속여 클라이언트에서 서버로 가는 패킷이나 그 반대 패킷의 흐름을 왜곡

	(가)	(나)	(다)
①	IP 스푸핑	ARP 스푸핑	DNS 스푸핑
②	ARP 스푸핑	IP 스푸핑	DNS 스푸핑
③	ARP 스푸핑	DNS 스푸핑	IP 스푸핑
④	DNS 스푸핑	IP 스푸핑	ARP 스푸핑

◦ DNS(Domain Name System) 스푸핑은 실제 DNS 서버보다 빨리 공격 대상에게 DNS Response 패킷을 보내, 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격이다.
◦ IP 스푸핑은 공격자가 자신의 IP 주소가 아닌 신뢰관계를 가진 시스템의 주소로 위장하여 공격 대상 서버로부터 정보를 가로채는 방식이다. 신뢰관계에 있는 IP로 위장한 후 rlogin 등을 이용하여 공격대상 서버에 접속한다. 백도어 등을 설치하여 차후 공격 경로를 확보한다.
◦ ARP 스푸핑 공격은 ARP(Address Resolution Protocol)의 결과로 호스트의 주소 매칭 테이블에 위조된 MAC(Media Access Control)주소가 설정되도록 하는 공격이다.

오답피하기 ④ 스푸핑(Spoofing)은 타인의 시스템 자원에 접근할 목적으로 IP를 날조하여 정당한 사용자인 것처럼 보이게 하거나 승인받은 사용자인 체하여 시스템에 접근함으로써 추적을 피하는 고급 해킹 수법이다. 스푸핑의 종류에는 IP spoofing, ARP spoofing, DNS spoofing 등이 있다.

정답 ④

이론서 470p 적중, 적중800제 581번 적중

4.

리눅스 시스템에서 침해사고 분석 시 wtmp 로그파일에서 확인할 수 있는 정보로 〈보기〉에서 옳은 것만을 모두 고른 것은?

보기

ㄱ. 재부팅 시간 정보
ㄴ. 사용자의 로그인/로그아웃 정보
ㄷ. 로그인에 실패한 사용자의 IP 주소

① ㄱ
② ㄴ
③ ㄱ, ㄴ
④ ㄱ, ㄴ, ㄷ

wtmp(x) 파일

◦ wtmp(x) 파일에 로그를 남기는 wtmp 데몬은 /usr/include/utmp.h 파일의 구조체를 그대로 사용하며, utmp 데몬과 비슷한 역할을 한다. 즉 사용자의 로그인, 로그아웃, 시스템 재부팅 정보를 담는다.
◦ wtmp 데몬도 utmp 데몬처럼 wtmp(x) 파일에 텍스트가 아닌 바이너리 형태로 데이터를 저장한다. 로그의 내용은 last 명령어로 확인할 수 있다.

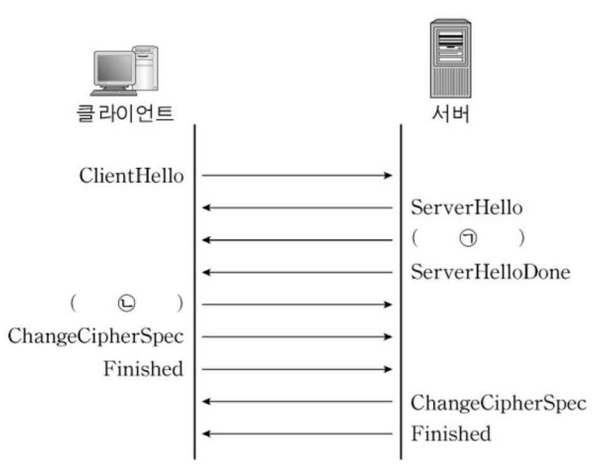
오답피하기 ③ 5번 이상 로그인 실패를 했을 경우에 로그인 실패 정보를 기록은 btmp이다.(솔라리스는 loginlog)

정답 ③

이론서 293p 적중, 기출 275번 유사

5.

그림은 SSL/TLS에서 상호인증을 요구하지 않는 경우의 핸드쉐이크(handshake) 과정이다. ㉠, ㉡에 들어갈 SSL/TLS 메시지를 바르게 짝지은 것은?



	㉠	㉡
①	ClientRequest	ClientHelloDone
②	ServerKeyExchange	ClientHelloDone
③	ClientKeyExchange	ServerKeyExchange
④	ServerKeyExchange	ClientKeyExchange

◦ SSL/TLS 핸드쉐이크 프로토콜은 크게 full 핸드쉐이크와 abbreviated 핸드쉐이크로 구분할 수 있다. full 핸드쉐이크의 경우 새로운 세션을 맺기 위해 사용되며 abbreviated 핸드쉐이크의 경우 이전에 생성되었던 세션을 재사용하기 위해 사용된다. abbreviated 핸드쉐이크는 공개키 연산을 수행하지 않으므로 full 핸드쉐이크에 비해 속도가 빠르다는 장점을 갖는다.
◦ 클라이언트가 처음 세션을 생성할 때(full handshake)는 empty를 전송하고 이미 생성된 세션이 상태를 재사용할 때(abbreviate Handshake)는 재사용하고자 하는 세션의 ID를 전송한다.

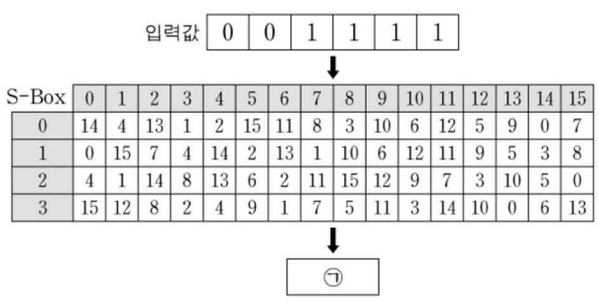
오답피하기 ④ 상호인증을 요구하지 않는 경우는 단축협상(abbreviate Handshake)으로 보기는 이 과정을 나타낸다.

정답 ④

이론서 579p 응용, 적중800제 291, 292번 유사

6.

그림은 DES(Data Encryption Standard)에서 S-Box를 통과하는 과정이다. 입력 값이 $001111_{(2)}$일 때 출력 비트 ㉠은?



① $0001_{(2)}$
② $0010_{(2)}$
③ $0110_{(2)}$
④ $0111_{(2)}$

S-박스

◦ S-박스는 실제로 섞어주는 역할을 수행한다. 즉, 혼돈(confusion)역할을 수행한다. DES는 각각 6비트 입력값과 4비트 출력값을 갖는 8개의 S-박스를 사용한다.
◦ 두 번째 연산으로부터 48비트 데이터는 8개의 6비트값으로 나누어지고, 각 6비트 값은 하나의 S-박스로 들어간다. 각 S-박스의 결과는 4비트 값이 된다. 이렇게 8개의 S-박스의 출력값이 결합되어 32비트가 된다.

오답피하기 ① 입력값 $001111_{(2)}$에서 1번, 6번자리 값(01 = 1)을 추출하여 행으로 잡고, 나머지 자리 값(0111 = 7)으로 열을 잡으면 1($0001_{(2)}$)이 선택된다.

정답 ①

이론서 79p 응용

7.

블록암호 운영모드 중 CTR(counter) 모드에 대한 설명으로 〈보기〉에서 옳은 것만을 모두 고른 것은?

보기

ㄱ. 운영모드에서 시프트 레지스터를 사용한다.
ㄴ. 패딩이 필요 없으며 평문 블록과 키 스트림을 XOR 연산하여 암호문을 생성한다.
ㄷ. 암호화는 각 블록에 독립적으로 적용되기 때문에, 블록 단위 에러 발생 시 해당 블록에 영향을 준다.

① ㄱ
② ㄱ, ㄴ
③ ㄴ, ㄷ
④ ㄱ, ㄴ, ㄷ

◦ CTR 모드는 OFB 모드와 마찬가지로 이전 암호문 블록과 독립적인 키 스트림을 생성하지만 피드백을 사용하지 않는다. 그리고 ECB 모드처럼 CTR 모드는 서로 독립적인 n비트 암호문 블록을 생성한다.
◦ CTR 모드의 오류 파급은 암호문의 한 비트 오류는 단지 대응되는 평문의 한 비트에만 영향을 준다.

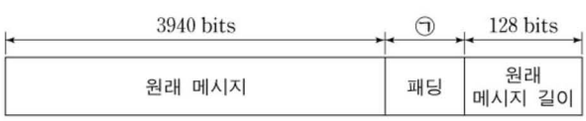
오답피하기 ③ 운영모드에서 시프트 레지스터를 사용하는 것은 CFB, OFB 모드이다. 나머지는 CTR 모드의 특징이다.

정답 ③

이론서 96p 적중, 이론서 93~96p 응용, 모의고사 15회 18번 적중

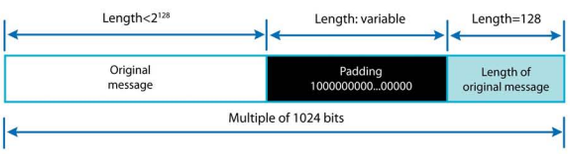
8.

해시함수 SHA-512를 이용하여 해시값을 구하려고 한다. 원래 메시지가 3940 비트일 때, 그림에서 ㉠ 패딩의 비트 수는?



① 24
② 28
③ 32
④ 36

SHA-512의 패딩과 길이 필드



◦ 길이 필드를 추가하기 전에 원래의 메시지가 1024비트의 배수가 되도록 패딩을 할 필요가 있다. 일단 128비트는 길이 필드로 확보를 해야 한다.
◦ 패딩으로 추가되는 비트의 형태는 첫 번째 비트가 1이고 그 뒤에 이어지는 비트들은 모두 0이다.

오답피하기 ② SHA-512는 1024bits 블록 단위로 암호화를 수행한다. (3940 + x + 128) mod 1024 = 0 되는 x는 280이다.

정답 ②

이론서 130p 적중, 적중800제 43, 44번 응용

9.

데이터베이스 서버와 어플리케이션 서버로 분리하여 운용할 경우, 데이터베이스 암호화 방식 중 암·복호화가 데이터베이스 서버에서 수행되는 방식으로 〈보기〉에서 옳은 것만을 모두 고른 것은?

보기

ㄱ. API 방식
ㄴ. 플러그-인 방식
ㄷ. 필터(filter) 방식
ㄹ. TDE(Transparent Data Encryption) 방식

① ㄱ, ㄴ
② ㄱ, ㄷ
③ ㄴ, ㄹ
④ ㄴ, ㄷ, ㄹ

DB 암호화 방식

◦ API 방식은 암 · 복호화 모듈을 애플리케이션 서버 내에 설치하고 이곳에서 암 · 복호화를 수행하는 구조로 애플리케이션의 수정을 동반한다.
◦ Plug-In 방식은 암 · 복호화 모듈을 DB 서버 내에 설치하고 이곳에서 암 · 복호화를 수행하는 구조로, 적용성이 뛰어나지만 암 복호화 시 DB 서버의 CPU를 사용하기 때문에 부하가 발생할 수 있다.
◦ 필터 방식은 독립된 프로세스로 구동하여 어플리케이션과 DBMS 중간에서 암복호화 처리를 하는 방식으로 API 방식과 동일하게 어플리케이션 서버에서 암 복호화 처리를 하는 방식이다.
◦ TDE 방식은 DBMS에 추가 기능으로 제공되는 암호화 기능을 이용하여 DB 내부에서 데이터 파일 저장 시 암호화하고, 파일에 저장된 내용을 메모리 영역으로 가져올 때 DBMS에 의해 자동으로 복호화되는 방식으로서, DBMS(Oracle 11g, MS SQL 등) 종류 및 버전에 따라 기능 지원 여부가 다르다.

오답피하기 ③ 플러그인 방식과 TDE 방식은 DB 서버에서 암·복호화가 수행되고, API 방식은 애플리케이션 서버에서 필터 방식은 애플케이션과 DBMS 중간에서 암·복호화가 수행된다.

정답 ③

적중800제 320번 적중

10.

다음의 개인정보보호법 제17조 ①항에 따라 개인정보처리자가 정보주체의 개인정보를 수집한 목적범위안에서 제3자에게 제공할 수 있는 경우로 〈보기〉에서 옳은 것만을 모두 고른 것은?

보기

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

보기

ㄱ. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

ㄴ. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

ㄷ. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우

① ㄱ

② ㄷ

③ ㄴ, ㄷ

④ ㄱ, ㄴ, ㄷ

개인정보의 수집·이용기준과 제공기준의 비교

기준	수집·이용(제15조)	제공(제17조)
1. 정보주체의 동의를 받은 경우	수집·이용 가능	제공 가능
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	수집·이용 가능	수집목적 범위 안에서 제공 가능
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우	수집·이용 가능	수집목적 범위 안에서 제공 가능
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우	수집·이용 가능	제공 불가(정보주체 동의 필요)
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	수집·이용 가능	수집목적 범위 안에서 제공 가능
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우.	수집·이용 가능	제공 불가(정보주체 동의 필요)

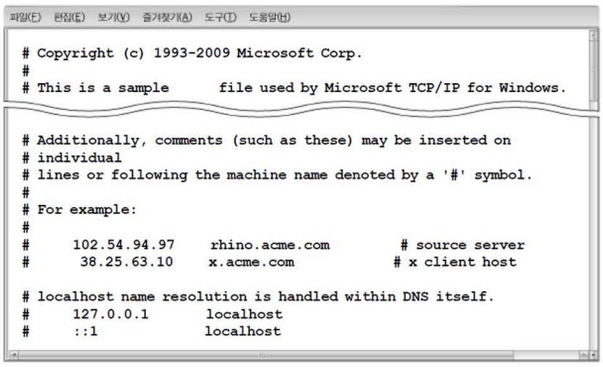
오답피하기 ③ 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우와 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우는 제15조 수집·이용에서는 적용되나 제17조에서는 정보주체의 동의 없이는 제공 불가하다.

정답 ③

이론서 743p 적중, 모의고사 19회 1번 부연 설명

11.

그림은 DNS 보다 우선 적용되는 파일로, 해커는 이 파일을 변조하여 파밍(pharming)에 사용할 수 있다. 이 파일명으로 옳은 것은?



```
파일(F)  편집(E)  보기(V)  즐겨찾기(A)  도구(T)  도움말(H)

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample      file used by Microsoft TCP/IP for Windows.

# Additionally, comments (such as these) may be inserted on
# individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com             # x client host

# localhost name resolution is handled within DNS itself.
#      127.0.0.1       localhost
#      ::1             localhost
```

① hosts
② networks
③ protocol
④ services

/etc/hosts 파일

◦ 호스트 파일은 호스트이름과 IP 주소를 대응하기 위해 사용한다. UNIX, Linux 시스템에서는 /etc/hosts에 위치하는 평문 텍스트 파일이다. 악성 프로그램이 hosts 파일을 얻게 되면 트래픽을 의도된 목적지로 우회시킬 수 있다. 침입을 방지하는 가장 효과적인 기법은 이 파일을 읽기 전용으로 설정하는 것이다.

오답피하기 ① 일반적으로 호스트 이름에 대한 IP 주소를 얻기 위해서는 캐시 → hosts 파일 → DNS 서버 순서로 질의한다. hosts 파일을 변조하여 공격자가 원하는 사이트로 이동토록 하는 공격이 파밍 공격이다.

정답 ①

이론서 605p 적중, 적중800제 300번 유사, 모의고사 8회 5번 적중

12.

다음 설명을 모두 만족하는 공개키 기반구조(PKI)의 구성요소는?

보기

- LDAP을 이용하여 X.500 디렉터리 서비스 제공
- 인증서와 사용자 관련 정보, 상호 인증서 쌍, CRL 등을 저장하고 검색하는 데이터베이스

① 사용자(user)
② 저장소(repository)
③ 등록기관(registration authority)
④ 인증기관(certification authority)

저장소(Repository, Directory)

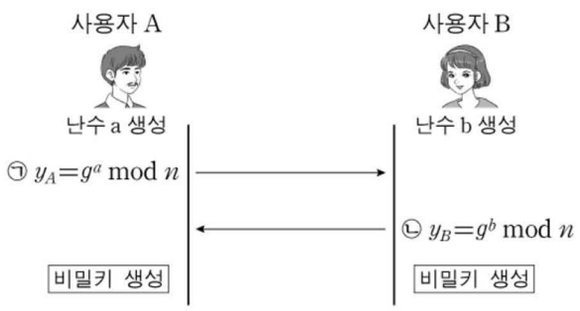
◦ 사용자의 인증서를 저장하는 저장소의 역할을 하는 일종의 데이터베이스라고 할 수 있다. 인증기관은 발급한 인증서를 발급과 동시에 디렉터리에 저장하며, 사용자는 자신이 원하는 상대방의 인증서를 이곳에서 검색할 수 있다.
◦ 또한 사용자의 정보는 이곳에서 포괄적으로 관리되며 디렉터리는 상황에 따라 적절한 접근 제한을 제공한다.
◦ 현재 디렉터리 표준형식으로는 ITU-T에서 정의한 X.500 표준형식과 이것을 간략화시킨 LDAP(Lightweight Directory Access Protocol) 등이 있다.
◦ 인증서는 신뢰받는 인증기관이 만들고 CA나 사용자가 디렉터리에 올린다. 디렉터리 서버 자체는 공개키 작성이나 인증 기능에 대해서는 관여하지 않는다. 오직 사용자가 인증서를 쉽게 찾을 수 있도록 잘 정리해놓을 뿐이다.

오답피하기 ② 저장소는 사용자의 인증서를 저장하는 일종의 데이터베이스이다. 인증기관은 발급한 인증서를 발급과 동시에 디렉터리에 저장하며, 사용자는 자신이 원하는 상대방의 인증서를 이곳에서 검색할 수 있다.

정답 ②

이론서 154p 적중, 적중800제 783번 유사

그림은 Diffie-Hellman의 키 교환 방법이다. 다음 그림을 보고 물음에 답하시오.



13.

위 그림의 식 ㉠, ㉡에서 n이 7일 때, g로 사용할 수 있는 것은?

① 2　② 3
③ 4　④ 7

원시근(primitive root)

◦ 법 p에 대한 원시근 a의 정의

$$\{a, a^2, a^3, \cdots, a^{p-3}, a^{p-2}, a^{p-1}\} = \{1, 2, \cdots, p-2, p-1\} \pmod p$$

◦ 법 p에 대한 원시근은 a로 거듭제곱하여 modular 연산을 하면 모든 원소들이 만들어 진다.

오답피하기 ② 3^6 mod 7 = 1, 3^2 mod 7 = 2, 3^1 mod 7 = 3, 3^4 mod 7 = 4, 3^5 mod 7 = 5, 3^3 mod 7 = 6 → 모든 원소는 3에 대한 임의의 a 거듭제곱으로 생성되므로 3은 법 7의 원시근이 된다.

정답 ②

기출 84번 응용, 적중800제 738번 응용

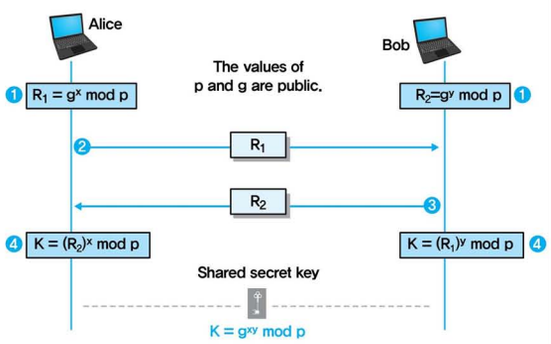
14.

위 그림에서 사용자 A, B가 생성하는 비밀키 값과 동일한 값을 구하는 식은? (단, mod는 나머지를 구하는 연산자이고, $\phi(n)$는 오일러의 Totient 함수이다.)

보기

① $g^{a \times b} \bmod n$
② $g^{a+b} \bmod n$
③ $g^{a \times b} \bmod \phi(n)$
④ $g^{a+b} \bmod \phi(n)$

◦ Diffie-Hellman 방법



오답피하기 ① 사용자 A와 B가 각각 개인키 a와 b를 가지고 공동 비밀키를 생성하면 $g^{ab} \bmod n$이 된다.

정답 ①

이론서 104p 적중, 적중800제 738번 적중

15.

그림은 리눅스에서 ls - l 명령을 실행한 결과이다. change 파일에 대한 설명으로 옳은 것은?

```
File  Edit  View  Search  Terminal  Help
$ ls -l
total 56
-rwsr-xr-x 1 test test    20 May  5 19:46 change
drwxr-xr-x 2 test test  4096 May  3 21:52 Desktop
drwxr-xr-x 2 test test  4096 May  3 21:52 documents
drwxr-xr-x 2 test test  4096 May  3 21:52 Downloads
-rw-r--r-x 1 test test  8980 May  3 21:45 examples.desktop
-rw-r--r-x 1 test test   189 May  5 20:34 fmtstr.c
-rw-r--r-x 1 test test   206 May  5 19:25 list.txt
```

① change 파일은 setGID 비트가 설정되어 있다.
② change 파일의 접근 권한을 8진수로 표현하면 754이다.
③ test 외의 사용자는 change 파일에 대해 쓰기 권한을 가진다.
④ change 파일은 test 외의 사용자가 실행할 때 유효 사용자 ID(effective UID)는 test가 된다.

SetUID, SetGID

◦ 계정이 누구인가를 식별하는 UID, GID를 각각 RUID(Real UID), RGID(Real GID)라고도 부른다. 하지만 특이하게 유닉스에서는 어떤 권한을 가지고 있는가에 대한 UID, GID가 별도로 존재한다. 이를 EUID(Effective UID), EGID(Effective GID)라고 한다.

◦ 최초로 로그인할 때는 RUID와 EUID, RGID와 EGID가 각각 같은 값을 갖는다. 일반적인 프로그램을 실행할 때도 이 값은 동일하며, SetUID 비트를 가진 프로그램을 실행했을 때만 프로세스 안에서 잠시 일치하지 않는 상태가 발생한다.

오답피하기 ① change 파일은 setUID 비트가 설정되어 있다. ② change 파일의 접근 권한을 8진수로 표현하면 4755이다. ③ test 외의 사용자는 change 파일에 대해 읽기, 실행 권한을 가진다.

정답 ④

이론서 279p 적중, 적중800제 648번 적중, 모의고사 15회 12번 적중

16.

AES(Advanced Encryption Standard) 알고리즘에서 사용되는 함수들이다. 암호화 과정의 마지막 라운드에서 수행되는 함수를 〈보기〉에서 옳은 것만을 모두 골라, 호출 순서대로 바르게 나열한 것은?

보기

ㄱ. SubBytes( ) /* 바이트 치환 */
ㄴ. ShiftRows( ) /* 행 이동 */
ㄷ. MixColumns( ) /* 열 혼합 */
ㄹ. AddRoundKey( ) /* 라운드 키 더하기 */

① ㄱ - ㄷ
② ㄱ - ㄴ - ㄹ
③ ㄴ - ㄱ - ㄹ
④ ㄹ - ㄱ - ㄴ - ㄷ

◦ AES 암호화 과정의 각 라운드는 비 선형성을 갖는 S-Box를 적용하여 바이트 단위로 치환을 수행하는 SubBytes( ) 연산, 행 단위로 순환 시프트(Cyclic shift)를 수행하는 ShiftRows( ) 연산, 높은 확산(diffusion)을 제공하기 위해 열 단위로 혼합(mixing)하는 MixColumns( ) 연산과 마지막으로 라운드 키와 state를 EX-OR하는 AddRoundKey( ) 연산으로 구성된다.

◦ 암호화의 마지막 라운드에서는 MixColumns( ) 연산을 수행하지 않는다는 특징이 있다.

오답피하기 ② AES의 마지막 라운드는 MixColumns( )을 제외하고, SubBytes( ), ShiftRows( ), AddRoundKey( ) 순서로 수행한다.

정답 ②

이론서 84p 적중, 적중800제 724번 유사

17.

네트워크 기반 침입탐지시스템(Intrusion Detection System)의 특징에 대한 설명으로 〈보기〉에서 옳은 것만을 모두 고른 것은?

보기

ㄱ. 어플리케이션 서버에 설치되어 관리가 간단하다.
ㄴ. 네트워크상의 패킷을 분석하여 침입을 탐지한다.
ㄷ. 방화벽 내부의 내부 네트워크와 방화벽 외부의 DMZ에 모두 배치 가능하다.

① ㄱ
② ㄴ
③ ㄱ, ㄷ
④ ㄴ, ㄷ

네트워크 기반 IDS(Network-based IDS)

◦ 네트워크에서의 패킷 헤더, 데이터 및 트래픽 양, 응용프로그램 로그 등을 분석하여 침입 여부를 판단한다. 즉, 시스템의 감사 자료가 아닌 네트워크를 통해 전송되는 패킷 정보를 수집 분석하여 침입을 탐지하는 시스템이다.

◦ N-IDS의 장점
- 네트워크 기반의 침입 탐지 시스템은 트래픽을 감시할 수 있는 몇몇 위치에만 설치하므로 초기 구축 비용이 저렴하다.
- 운영체제에 독립적이므로 구현 및 관리가 쉽다.
- 캡처된 트래픽에 대해서는 침입자가 흔적을 제거하기 어렵다.
- 네트워크 레벨 에이전트를 설치함으로써 데이터 소스에 영향을 미치지 않는다.
- 네트워크 레벨 에이전트는 SYN flood나 패킷 폭풍(packet storm) 등과 같은 네트워크 공격을 모니터링하고 탐지할 수 있다.

오답피하기 ④ 어플리케이션 서버에 설치하는 것은 호스트 기반 IDS의 특징이다.

정답 ④

이론서 483p 적중, 적중800제 228, 229, 238번 유사

18.

다음 설명을 모두 만족하는 OTP(One-Time Password) 생성 방식은?

보기

o 해시체인 방식으로 계산된다.
o 생성된 일회용 패스워드의 사용 횟수가 제한된다.
o 검증 시 계산량이 적기 때문에 스마트카드와 같은 응용에 적합하다.

① S/KEY 방식
② 시간 동기화 방식
③ 이벤트 동기화 방식
④ Challenge-Response 방식

◦ 시간 동기화 방식 : OTP를 생성하기 위해 사용하는 입력 값으로 시각을 사용하는 방식이다. 클라이언트는 현재 시각을 입력값으로 OTP를 생성해 서버로 전송하고, 서버 역시 같은 방식으로 OTP를 생성하여 클라이언트가 전송한 값의 유효성을 검사한다.

◦ 이벤트 동기화 방식 : 서버와 클라이언트가 카운트 값을 동일하게 증가시켜 가며, 해당 카운트 값을 입력값으로 OTP를 생성해 인증하는 방식이다.

◦ 챌린지·응답 방식 : 서버에서 난수 생성 등을 통해 임의의 수를 생성하고 클라이언트에 그 값을 전송하면, 클라이언트가 그 값으로 OTP를 생성해 응답한 값으로 인증하는 방식이다.

오답피하기 ① S/KEY 방식은 벨 통신 연구소에서 개발한 OTP 생성 방식으로, 유닉스 계열 운영체제에서 인증에 사용되고 있다. 해시 체인에 기반하고 있는 이 알고리즘은, 해시 함수의 역연산을 하기 어렵다는 점에 착안하여 만들어졌다.

정답 ①

이론서 187p 적중, 적중800제 680번 적중, 모의고사 11회 15번 적중

19.

그림은 무선 AP(Access Point)를 설정한 결과 화면의 일부이다. ㉠~㉢에 대한 설명으로 옳지 않은 것은?

① ㉠의 'home'은 관리자가 변경할 수 없다.
② ㉡을 '사용함'으로 설정하였기 때문에, 클라이언트의 무선 네트워크 연결 목록에서 'home'을 볼 수 있다.
③ 무선 네트워크 연결 목록에서 'home'을 볼 수 없게하여 접속시도를 줄이려면, ㉡을 '사용하지 않음'으로 설정을 변경한다.
④ ㉢을 'WPA2PSK'로 설정하였기 때문에, '암호화 방법'으로 AES를 사용할 수 있다.

SSID 노출

◦ 기본적으로 무선랜에서 사용되는 기본적인 인증방식은 개방형 인증 방식, 즉 별도의 인증절차 없이 무선 AP와의 연결이 이루어지는 방식이다.

◦ 무선 AP에 별도의 무선 전송데이터의 암호화 방식이나, 인증절차가 설정되어 있지 않은 경우에는 무선 전송데이터의 모니터링을 통해 SSID 값을 획득하고, 획득한 SSID 값을 무선 단말기에 설정하는 것만으로 무선랜으로의 불

법적인 접속이 가능하게 된다.

◦ SSID는 안정적인 보안 메커니즘으로 고려되어서는 안 된다. 이는 많은 AP들이 SSID를 브로드캐스트하며, 공격자들에 의해 쉽게 스니핑되어 사용될 수 있기 때문이다.

오답피하기 ① SSID는 무선 랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로써 서비스 받고 있는 무선랜을 식별하거나 확인하기 위해 사용하는 것으로 관리자는 변경할 수 있다.

정답 ①

이론서 400p 적중, 기출 362번 유사, 적중800제 554번 유사

20.

그림은 C 언어 소스코드의 일부이다. 이 소스코드 ㉠~㉣에서 오버플로우 취약점을 가진 행은?

보기

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#define BUFSIZE 10
int main(int argc, char **argv)
 {
    char *dest = NULL ;  ———————— ㉠
    dest = (char *)malloc(BUFSIZE);  ———— ㉡
    strcpy(dest, argv[1]);  ———————— ㉢
    free(dest);
    return 0 ;  ———————————— ㉣
 }
```

① ㉠　② ㉡

③ ㉢　④ ㉣

오답피하기 ③ 버퍼 오버플로우 공격의 대응책으로 프로그래머는 코드를 검사하고 불안전한 코딩 구조를 안전한 방법으로 재작성할 필요가 있다. 예를 들어 사용을 자제해야할 strcpy() 함수 대신 사용을 권장하는 strncpy() 함수를 사용하면 피해를 최소화할 수 있다.

정답 ③

이론서 300p 적중, 기출 298번 유사, 적중800제 670번 적중

2018년 빅데이터 기반 합격 커리큘럼 [정보보호론]

전산개발, 정보보호직, 경찰간부

※ 공무원 시험일정과 학원사정에 의해 변경될 수 있음.

구분		2017.09~2017.10	2017.11~2017.12	2018.01~2018.02	2018.03~2018.04	2018.05~2018.06	2018.07~2018.08
전산개발	이론 1.0	기본+심화 1.1	용어+요약 1.2 + 1.3	속성이론 1.4			
	기출+적중 3.0		4년간 기출총정리 + α 3.1	적중 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	정보시스템보안 + 네트워크보안 7.2			
교재		2018 탑스팟 이론서	4년간 기출총정리 + α	· 2018 탑스팟 이론서/ 적중 800제 · 정보보호직은 자체 교재	프린트물	프린트물	프린트물
문제난이도		중 ~ 중상	중 ~ 중상	중상 ~ 상	중상 ~ 상	중상 ~ 상	상
비고		· 이론서2권-전2권 구성 · 주3회 이론 수업 · 매주 복습 퀴즈 진행	· 연도별 기출문제 풀이 3.2 -교재 프린트 제공, 동영상 진행 · 4년간 기출총정리 + α(문제편/ 정답·해설편/용어·요약집) -전3권 구성 · 정보보안기사는 12월 개강	· 적중 800제(제본, 수강생 제공) 는 고득점 합격을 목표로 함 · 정보보호직 수업은 정보보호론에 포함되지 않는 과정만 진행	모의고사식 실전 훈련	· 모의고사식 실전 훈련 · 최신 정보보안기사 기출문제 포함 모의고사 진행	· 모의고사식 실전 훈련 · 국회사무처 등 시험대비 겸함
추천과정	전산개발(9급)	이론 1.1 + 1.2 + 1.3 → 기출 3.1, 3.2 中 택1 → 적중 800제 3.3 → 9급 대비 모의고사 5.1 + 5.2					
	전산개발(7급)	이론 1.1 + 1.2 + 1.3 → 기출 3.1 3.2 中 택1 → 적중 800제 3.3 → 9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3					
	정보보호직	이론 1.1 + 1.2 + 1.3 → 기출 3.1, 3.2 中 택1 → 적중 800제 3.3 → 정보보호직 강좌 7.1, 7.2 中 택1					
	경찰간부	이론 1.1 + 1.2 + 1.3 → 기출 3.1, 3.2 中 택1 → 적중 800제 3.3 → 정보보호직 강좌 7.1, 7.2 中 택1→ 9급 대비 모의고사 5.1 + 5.2 → 7급 대비 모의고사 5.3					

빅데이터 1.0 / 이론

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

빅데이터 3.0 / 기출+적중

- 3.1 4년간 기출총정리 + α
- 3.2 연도별 기출문제 풀이
- 3.3 적중 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)
- 7.2 정보시스템보안, 네트워크보안(학원 내부교재)

기타 무료 강의

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

전산직 공채 총정리(2017년, 2018년)

※ 상기 내용은 공개채용만 해당됨

시험 종류			2017년				2018년				시험과목	비고
구분	직류	급수	인원	접수기간	시험일	필기 합격선	인원	접수기간	시험일	필기 합격선		
해경	정보보호	9급	2	2.8 ~ 2.22	3.11	90점~	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	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	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		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		국,영,한,컴일,정보	거주지 제한 있음
서울시	전산개발	7급					3	3.12~3.16	6.23		국,영,한,정보,자구,DB,소공	거주지 제한 없음, 영어는 공인시험 대체 아님
서울시	전산개발	9급	7	3.13~3.17	6.24	86	13	3.12~3.16	6.23		국,영,한,컴일,정보	거주지 제한 없음
군무원	국방부	7급					2	6.7~6.12	8.11		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		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		국,컴일,정보	상동
군무원	해군	9급	8	4.24~4.28	7.1	67	9	6.7~6.12	8.11		국,컴일,정보	상동
군무원	공군	9급	2	4.24~4.28	7.1	66	3	6.7~6.12	8.11		국,컴일,정보	상동
국회사무처	전산개발	9급	1	5.8~5.15	7.22	80	1	5.21~5.25	8.25		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		국,한,정보,자구,DB,소공	2017년부터 영어는 공인시험으로 대체
해경	전산	순경	14	7.31~8.11	9.2	-					실기시험(서술, 약술)	실기시험→서류전형→면접→최종합격
지방직(경기)	전산개발	7급	2	6.26~6.29	9.23	81.42	3	7.16~7.20	10.13		국,영,한,정보,자구,DB,소공	영어는 공인시험 대체 아님
경찰간부	사이버	간부	5	8.14~8.23	9.23	332.5(1차) 463(2차)	5	8.7~8.16	9.15		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)**