☑ 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. 처음 출제된 클라우드법, SMTP 명령어는 정보보안기사(알기사, 조현준 저 참조)에서 다루는 내용들입니다. 하지만, 이런 문제들도 기본을 통해 응용을 하면 충분히 해결 할 수 있습니다. 클라우드 관련 문제는 클라우드 개념과 공무원 기출문제를 응용해서 풀 수 있고, SMTP 명령어 문제는 지문에 답이 있었습니다. 향후 정보보호론은 범위는 넓어지고, 난이도는 계속 올라간다고 생각하시면 될 것 같습니다.

2. 난이도

전체적인 난이도는 전년도 지방직 시험과 비슷한 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) 위주의 이론정리를 하신 분들은 어렵게 느껴졌을 것으로 생각됩니다.

3. 향후 학습방향

지방직시험이기 때문에 지역마다 커트라인은 다를 것입니다. 하지만, 다음 시험을 위해서 본인의 위치를 냉철히 판단해보고 약점을 보완하셔야 합니다. 약간은 주관적일 수 있지만 이번 시험을 기준으로 85점 이상을 받으신 분들은 공부의 방향이 맞다고 보여집니다. 하지만, 60점이하로 받으신 분들은 공부방법을 다시 한번 생각해보세요. 사이에 있는 분들은 더 분발하시고요.

2020년 지방직,교육청 9급 정보보호론

-2020년 6월 13일 시행

1. ○△× 20.지방.9급

전자 서명(digital signature) 보안 메커니즘이 제공하는 보안 서비스가 아닌 것은?

① 근원 인증
② 메시지 기밀성
③ 메시지 무결성
④ 부인 방지

오답피하기 ② 전자서명은 비밀성(기밀성)은 제공하지 않는다.

정답 ②

이론: 110p 적중, 기출: 652번(심) 적중

※ 지문이나 문제의 유사도에 따라 적중 > 유사 > 응용으로 구분함.

2. ○△× 20.지방.9급

AES(Advanced Encryption Standard)에 대한 설명으로 옳은 것은?

① DES(Data Encryption Standard)를 대신하여 새로운 표준이 된 대칭 암호 알고리즘이다.
② Feistel 구조로 구성된다.
③ 주로 고성능의 플랫폼에서 동작하도록 복잡한 구조로 고안되었다.
④ 2001년에 국제표준화기구인 IEEE가 공표하였다.

◦ AES는 기존 DES, 3DES의 취약한 암호 강도를 극복하고자 미국 NIST에서 전세계 암호학자들에게 공모를 통하여 선정한 대칭 암호 알고리즘이다.
◦ AES는 알려진 블록 암호 알고리즘에 대한 모든 공격 방법으로부터 안전하도록 설계되었으며, 하드웨어나 소프트웨어 구현 시 속도나 코드 압축성 면에서 효율적이므로 스마트카드와 같은 응용에 적합하다는 장점이 있다.

오답피하기 ② AES는 SPN 구조로 구성된다. ③ AES는 스마트카드와 같은 응용에도 동작하도록 효율적으로 고안되었다. ④ 미국 NIST(National Institute of Standards and Technology)에서 공표하였다.

정답 ①②③④

이론: 53p 유사, 기출: 48번(기), 575번(심), 576번(심), 576번(심) 응용

3. ○△× 20.지방.9급

침입탐지시스템(IDS)에 대한 설명으로 옳지 않은 것은?

① 호스트 기반 IDS와 네트워크 기반 IDS로 구분한다.
② 오용 탐지 방법은 알려진 공격 행위의 실행 절차 및 특징 정보를 이용하여 침입 여부를 판단한다.
③ 비정상 행위 탐지 방법은 일정 기간 동안 사용자, 그룹, 프로토콜, 시스템 등을 관찰하여 생성한 프로파일이나 통계적 임계치를 이용하여 침입 여부를 판단한다.
④ IDS는 방화벽처럼 내부와 외부 네트워크 경계에 위치해야 한다.

오답피하기 ④ HIDS의 경우에는 특별한 위치는 없으며, 보통 중요한 시스템에 설치한다. NIDS는 목적에 따라 여러 곳에 설치할 수 있다. 방화벽과 같이 외부와 내부의 경계선에 존재해야 하는 것이 아니라 네트워크의 어느 부분에나 설치할 수 있다.

정답 ④

이론: 447p 적중, 최고수준800제: 247번 응용

4. ○△× 20.지방.9급

RSA 암호 알고리즘에서 두 소수, p = 17, q = 23과 키 값 e = 3을 선택한 경우, 평문 m = 8에 대한 암호문 c로 옳은 것은?

① 121
② 160
③ 391
④ 512

RSA 암호화/복호화
◦ 암호화
평문: m
암호문: $c = m^e \bmod n$
◦ 복호화
암호문: c
평문: $m = c^d \bmod n$

오답피하기 ① $c = 8^3 \bmod 391 (391 = 17 \times 23,\ n = p \times q)$
$c = 512 \bmod 391 = 121$

정답 ①

이론: 79p 적중, 기출: 72번(기), 615번(심) 유사, 최고수준800제: 742번 적중

5. ○△× 20.지방.9급

IEEE 802.11i RSN(Robust Security Network)에 대한 설명으로 옳은 것은?

① TKIP는 확장형 인증 프레임워크이다.
② CCMP는 데이터 기밀성 보장을 위해 AES를 CTR 블록 암호 운용 모드로 이용한다.
③ EAP는 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다.
④ 802.1X는 무결성 보장을 위해 CBC—MAC를 이용한다.

◦ CCMP는 AES 블록 암호를 사용한 데이터의 비밀성과 무결성을 보장하기 위한 규칙을 정의하고 있다. TKIP이 RC4를 사용한 암호를 사용하는 반면, CCMP는 이미 전문가들의 많은 검토를 통해 안전성이 입증된 AES를 기반으로 한다.

오답피하기 ① EAP는 확장형 인증 프레임워크이다. ③ TKIP은 WEP로 구현된 하드웨어의 펌웨어 업데이트를 위해 사용한다. ④ 802.1x는 포트 기반 네트워크 접근제어 기능을 제공한다.

정답 ②

이론: 369p 적중, 기출: 264번(기,심) 적중, 최고수준800제: 767번 적중

6. ○△× 20.지방.9급

CC(Common Criteria) 인증 평가 단계를 순서대로 바르게 나열한 것은?

보기
가. PP(Protection Profile) 평가
나. ST(Security Target) 평가
다. TOE(Target Of Evaluation) 평가

① 가→나→다
② 가→다→나
③ 나→가→다
④ 다→나→가

오답피하기 ① CC의 평가과정은 PP Evaluation, ST Evaluation, TOE Evaluation의 3단계로 수행된다. PP(보호 프로파일) Evaluation은 PP의 완전성, 일치성 그리고 기술성을 평가하며, ST(보안목표명세서) Evaluation은 ST가 PP의 요구사항을 충족하는지에 대하여 평가하고, TOE(평가목표시스템) Evaluation은 TOE가 ST의 요구사항을 충족하는지에 대하여 평가한다.

정답 ①

이론: 645p 응용, 모의고사: 13회 3번 적중

7. ○△× 20.지방.9급

SQL 삽입 공격에 대한 설명으로 옳지 않은 것은?

① 사용자 요청이 웹 서버의 애플리케이션을 거쳐 데이터베이스에 전달되고 그 결과가 반환되는 구조에서 주로 발생한다.
② 공격이 성공하면 데이터베이스에 무단 접근하여 자료를 유출하거나 변조시키는 결과가 초래될 수 있다.
③ 사용자의 입력값으로 웹 사이트의 SQL 질의가 완성되는 약점을 이용한 것이다.
④ 자바스크립트와 같은 CSS(Client Side Script) 기반 언어로 사용자 입력을 필터링하는 방법으로 공격에 대응하는 것이 바람직하다.

오답피하기 ④ 자바 스크립트와 같은 CSS(Client Side Script) 기반의 언어는 웹 프락시를 통해 웹 브라우저에 전달되기 때문에 웹 프락시를 통해 전달되는 과정에서 변조될 가능성이 있다. 따라서 CSS 기반의 언어로 필터링 할 경우 공격자가 필터링 로직만 파악하면 쉽게 필터링이 무력화된다. 즉, 필터링 로직은 ASP, JSP 등과 같은 SSS(Server Side Script)로 필터링을 수행해야 한다.

정답 ④

이론: 552p 응용, 기출: 173번(심) 적중

8. ○△× 20.지방.9급

유닉스/리눅스의 파일 접근 제어에 대한 설명으로 옳지 않은 것은?

① 접근 권한 유형으로 읽기, 쓰기, 실행이 있다.
② 파일에 대한 접근 권한은 소유자, 그룹, 다른 모든 사용자에 대해 각각 지정할 수 있다.
③ 파일 접근 권한 변경은 파일에 대한 쓰기 권한이 있으면 가능하다.
④ SetUID가 설정된 파일은 실행 시간 동안 그 파일의 소유자의 권한으로 실행된다.

오답피하기 ③ 파일의 소유주나 슈퍼 유저 root는 chmod 명령을 이용하여 기존 파일 또는 디렉터리에 대한 접근권한을 변경한다.

정답 ③

이론: 241p 적중, 기출: 188번(기), 189번(기) 유사

9. ○△× 20.지방.9급

IPSec에 대한 설명으로 옳지 않은 것은?

① 전송(transport) 모드에서는 전송 계층에서 온 데이터만을 보호하고 IP 헤더는 보호하지 않는다.

② 인증 헤더(Authentication Header) 프로토콜은 발신지 호스트를 인증하고 IP 패킷으로 전달되는 페이로드의 무결성을 보장하기 위해 설계되었다.

③ 보안상 안전한 채널을 만들기 위한 보안 연관(Security Association)은 양방향으로 통신하는 호스트 쌍에 하나만 존재한다.

④ 일반적으로 호스트는 보안 연관 매개변수들을 보안 연관 데이터베이스에 저장하여 사용한다.

◦ 보안 연계 서비스(Security Association, SA): 보안연계 서비스는 AH 프로토콜과 ESP 프로토콜을 이용하여 다양한 보안 서비스를 제공하기 위하여 보안 프로토콜 각각에 대한 보안 매개변수 집합(알고리즘 식별자, 모드, 키 등)을 정의하는 역할을 한다.

오답피하기 ③ SA는 송신자측과 수신자측의 트래픽 보안서비스를 제공하기 위해 상호 협상에 의해 생성되며 애플리케이션(application)마다 독립적으로 생성되고 관리된다. 그리고 SA가 단방향이기 때문에 양단간의 통신이 필요한 경우 각 방향에 대해 하나씩의 SA를 정의해야 한다.

정답 ③

이론: 486p 적중, 최고수준800제: 263번 유사

10. ○△× 20.지방.9급

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제25조(침해사고 등의 통지 등), 제26조(이용자 보호 등을 위한 정보 공개), 제27조(이용자 정보의 보호)에 명시된 것으로 옳지 않은 것은?

① 클라우드컴퓨팅서비스 제공자는 이용자 정보가 유출된 때에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.

② 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기할 수 있다.

◘ 제25조(침해사고 등의 통지 등)

① 클라우드컴퓨팅서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 지체 없이 그 사실을 해당 이용자에게 알려야 한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고가 발생한 때
2. 이용자 정보가 유출된 때
3. 사전예고 없이 대통령령으로 정하는 기간(당사자 간 계약으로 기간을 정하였을 경우에는 그 기간을 말한다) 이상 서비스 중단이 발생한 때

② 클라우드컴퓨팅서비스 제공자는 제1항제2호에 해당하는 경우에는 즉시 그 사실을 과학기술정보통신부장관에게 알려야 한다.

③ 과학기술정보통신부장관은 제2항에 따른 통지를 받거나 해당 사실을 알게 되면 피해 확산 및 재발의 방지와 복구 등을 위하여 필요한 조치를 할 수 있다.

④ 제1항부터 제3항까지의 규정에 따른 통지 및 조치에 필요한 사항은 대통령령으로 정한다.

◘ 제26조(이용자 보호 등을 위한 정보 공개)

① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

② 정보통신서비스를 이용하는 자는 정보통신서비스 제공자에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.

③ 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 제1항 및 제2항에 따른 정보를 공개하도록 권고할 수 있다.

④ 과학기술정보통신부장관이 제3항에 따라 정보를 공개하도록 권고하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다.

◘ 제27조(이용자 정보의 보호)

① 클라우드컴퓨팅서비스 제공자는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없이 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 수 없다. 클라우드컴퓨팅서비스 제공자로부터 이용자 정보를 제공받은 제3자도 또한 같다.

② 클라우드컴퓨팅서비스 제공자는 이용자 정보를 제3자에게 제공하거나 서비스 제공 목적 외의 용도로 이용할 경우에는 다음 각 호의 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 이용자 정보를 제공받는 자
2. 이용자 정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 이용자 정보의 항목
4. 이용자 정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.

④ 클라우드컴퓨팅서비스 제공자는 사업을 종료하려는 경우에는 그 이용자에게 사업 종료 사실을 알리고 사업 종료일 전까지 이용자 정보를 반환하여야 하며 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다. 다만, 이용자가 사업 종료일 전까지 반환받지 아니하거나 반환을 원하지 아니하는 등의 이유로 사실상 반환이 불가능한 경우에는 이용자 정보를 파기하여야 한다.

⑤ 제3항 및 제4항에도 불구하고 클라우드컴퓨팅서비스 제공자와 이용자 간의 계약으로 특별히 다르게 정한 경우에는 그에 따른다.

⑥ 제3항 및 제4항에 따른 이용자 정보의 반환 및 파기의 방법 · 시기, 계약 종료 및 사업 종료 사실의 통지 방법 등에 필요한 사항은 대통령령으로 정한다.

오답피하기 ④ 클라우드컴퓨팅서비스 제공자는 이용자와의 계약이 종료되었을 때에는 이용자에게 이용자 정보를 반환하여야 하고 클라우드컴퓨팅서비스 제공자가 보유하고 있는 이용자 정보를 파기하여야 한다.(임의규정이 아니라 강행 규정임)

정답 ④

기출: 104번(심) 응용, 강의: 스킬 반복 강조

11. ○△× 20.지방.9급

인증기관이 사용자의 공개키에 대한 인증을 수행하기 위해 X.509 형식의 인증서를 생성할 때 서명에 사용하는 키는?

① 인증기관의 공개키
② 인증기관의 개인키
③ 사용자의 개인키
④ 인증기관과 사용자 간의 세션키

오답피하기 ② 공개키 인증서에는 이름이나 소속, 메일 주소 등의 개인정보 및 그 사람의 공개키가 기재되고, 인증기관(CA)의 개인키로 전자서명 되어있다.

정답 ②

이론: 122p 적중, 기출: 666번(심) 적중

12. ○△× 20.지방.9급

하이브리드 암호 시스템에 대한 설명으로 옳지 않은 것은?

① 메시지는 대칭 암호 방식으로 암호화한다.
② 일반적으로 대칭 암호에 사용하는 세션키는 의사 난수 생성기로 생성한다.
③ 생성된 세션키는 무결성 보장을 위하여 공개키 암호 방식으로 암호화한다.
④ 메시지 송신자와 수신자가 사전에 공유하고 있는 비밀키가 없어도 사용할 수 있다.

하이브리드 암호 시스템(hybrid cryptosystem)

- 하이브리드 암호 시스템은 대칭키 암호와 공개키 암호의 장점을 살릴 수 있도록 조합한 방법이다. 일반적으로 서로 다른 2개의 방식을 조합하는 것을 하이브리드라고 한다.
- 하이브리드 암호 시스템에서는 먼저 메시지를 고속의 대칭키 암호로 암호화한다. 그렇게 하면 메시지가 암호문으로 변환되기 때문에 메시지의 기밀성을 지킬 수 있게 된다.
- 그 다음에 대칭키 암호의 키 기밀성을 지키기 위해서 이 부분에 공개키 암호를 사용한다. 즉, 메시지를 암호화할 때 사용한 대칭키 암호키를 공개키 암호로 암호화한다.

오답피하기 ③ 생성된 세션키는 무결성이 아닌 기밀성 보장을 위하여 공개키 암호 방식으로 암호화한다.

정답 ③

이론: 84p 적중, 기출: 626번(심), 628번(심) 유사

13. ○△× 20.지방.9급

해시함수의 충돌저항성을 위협하는 공격 방법은?

① 생일 공격
② 사전 공격
③ 레인보우 테이블 공격
④ 선택 평문 공격

- 레인보 테이블(rainbow table)은 해시 함수를 사용하여 변환 가능한 모든 해시값을 저장한 표이다. 보통 해시 함수를 이용하여 저장된 비밀번호에서 원래의 비밀번호를 추출해 내는 데 사용된다.

오답피하기 ① 생일 공격(birthday attack)은 일방향 해시함수의 강한 충돌 내성(충돌저항성)을 깨고자 하는 공격이다.

정답 ①

이론: 95p 적중, 최고수준800제: 760번 응용

14. ○△× 20.지방.9급

블록 암호 운용 모드에 대한 설명으로 옳지 않은 것은?

① CFB는 블록 암호화를 병렬로 처리할 수 없다.
② ECB는 IV(Initialization Vector)를 사용하지 않는다.
③ CBC는 암호문 블록에 오류가 발생한 경우 복호화 시 해당 블록만 영향을 받는다.
④ CTR는 평문 블록마다 서로 다른 카운터 값을 사용하여 암호문 블록을 생성한다.

- CFB 모드는 복호화는 병렬처리가 가능하나 암호화는 병렬처리가 불가능하다.

오답피하기 ③ 복호화할 때 CBC 모드의 암호문 블록이 1개 파손된 경우, 암호문 블록의 길이가 바뀌지 않았다면 평문 블록에 미치는 영향은 2개 블록에 머문다. 반면 평문 블록의 한 비트 오류는 출력되는 모든 암호문에 영향을 미친다.

정답 ③

이론: 60p 적중, 최고수준800제: 26번 적중

15. ○△× 20.지방.9급

「개인정보 보호법」상 공개된 장소에 영상정보처리기기를 설치·운영할 수 있는 경우가 아닌 것은?

① 범죄의 예방 및 수사를 위하여 필요한 경우
② 공공기관의 장이 허가한 경우
③ 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
④ 시설안전 및 화재 예방을 위하여 필요한 경우

제25조(영상정보처리기기의 설치·운영 제한)

① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

오답피하기 ② 공공기관의 장이 허가한 경우는 영상정보처리기기를 설치 및 운영할 수 없다.

정답 ②

이론: 682p 적중, 기출: 466번(기) 적중

16. ○△× 20.지방.9급

SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는 데 악용될 수 있는 명령어는?

① HELO
② MAIL FROM
③ RCPT TO
④ VRFY

SMTP 명령어

명령 코드	명령	설명
HELO	인사(Hello)	SMTP 송신자가 SMTP 세션을 초기화하기 위해 SMTP 수신자에게 보내는 전통적인 명령이다.
EHLO	확장된 Hello (Extended Hello)	SMTP 확장 기능을 지원하는 SMTP 송신자가 SMTP 세션을 초기화하고 SMTP 수신자에게 지원하는 SMTP 확장의 목록을 보내달라고 요청하는 명령이다. 인자로는 송신자의 도메인 이름을 사용한다.
MAIL	메일 전송 시작 (Initiate Mail Transaction)	SMTP 송신자가 이메일 전송을 시작하기 위해 수신자로 보내는 명령이다.
RCPT	받는 사람 (Recipient)	현재 전송하고자 하는 이메일 메시지를 받는 사람의 주소 하나를 지정한다.
DATA	메일 메시지의 데이터	실제 메시지를 송신하기 위해 사용한다.
RSET	리셋(Reset)	메일 전송 중에 중단시킨다. MAIL 명령이나 RCPT 명령을 보내다가 오류가 발생하여 더 이상 전송을 계속 할 수 없을 때 SMTP 송신자가 사용할 수 있다.
VRFY	확인(Verify)	SMTP 수신자에게 편지함이 사용 가능한지를 확인하도록 요청한다.
EXPN	확장(Expand)	수신 호스트에게 인수로 보내진 메일링 리스트를 확장하여, 그 목록을 이루는 수신자들의 주소를 되돌려 주도록 요구한다.
HELP	도움말(Help)	인자를 명시하지 않으면 일반 도움말 정보를 요청하는 것을 의미한다. 인자를 사용하는 것은 해당 명령 코드에 관한 정보를 요청하는 것을 의미한다.
NOOP	무동작 (No Operation)	SMTP 수신자와의 통신 상태를 확인하는 것 외에는 아무런 역할을 하지 않는다.
QUIT	종료(Quit)	SMTP 세션을 종료한다.

오답피하기 ④ SMTP 수신자에게 편지함이 사용 가능한지를 확인하도록 요청할 때 VRFY 명령어를 사용한다.

정답 ④

최고수준800제: 280번 응용

17. ○△× 20.지방.9급

다음 법 조문의 출처는?

보기

제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

① 국가정보화 기본법
② 개인정보 보호법
③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률
④ 정보통신산업진흥법

오답피하기 ③ 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조에 근거하여 ISMS와 ISMS-P 인증제도를 시행한다.

정답 ③

이론: 713p 적중, 최고수준800제: 388번 응용

18. ○△× 20.지방.9급

위조된 출발지 주소에서 과도한 양의 TCP SYN 패킷을 공격 대상 시스템으로 전송하는 서비스 거부 공격에 대응하기 위한 방안의 하나인, SYN 쿠키 기법에 대한 설명으로 옳은 것은?

① SYN 패킷이 오면 세부 정보를 TCP 연결 테이블에 기록한다.
② 요청된 연결의 중요 정보를 암호화하고 이를 SYN-ACK 패킷의 응답(acknowledgment) 번호로 하여 클라이언트에게 전송한다.
③ 클라이언트가 SYN 쿠키가 포함된 ACK 패킷을 보내오면 서버는 세션을 다시 열고 통신을 시작한다.
④ TCP 연결 테이블에서 연결이 완성되지 않은 엔트리를 삭제하는 데까지의 대기 시간을 결정한다.

오답피하기 ③ SYN 쿠키 기법은 SYN 패킷을 수신한 서버가 시간정보, 클라이언트 IP 주소, 클라이언트 시작 순서번호, 비밀번호 등을 입력값으로 해시값(Hash Value)을 쿠키로 구한 다음, 이를 서버 시작 순서번호(ISN)로 하는 SYN+ACK 패킷을 클라이언트로 회신한다. 그리고 이에 대한 정상적인 ACK 패킷을 수신할 때까지 연결 테이블에 자료구조 설정을 미룬다. 서버가 사용한 쿠키는 시간정보, 비밀번호 등이 포함되어 재사용하거나 위조할 수 없는 값이므로 서버가 송신한 SYN+ACK 패킷을 정상적으로 수신하지 않은 공격자는 확인번호(ack no)를 추론할 수 없다. 때문에 ACK 패킷을 위조하여 서버에게 전송할 수가 없다. 따라서 위조 SYN 패킷을 수신한 서버는 결국 정상적인 ACK 패킷을 수신하지 않게 되어 위조 SYN 패킷에 의한 연결 테이블의 자원이 소진되는 현상을 방지할 수 있게 되는 것이다.

정답 ③

이론: 405p 적중, 강의: 심화 설명

19. ○△× 20.지방.9급

ISO/IEC 27001:2013 보안관리 항목을 PDCA 모델에 적용할 때, 점검(check)에 해당하는 항목은?

① 성과평가(performance evaluation)
② 개선(improvement)
③ 운영(operation)
④ 지원(support)

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 ① 성과평가(performance evaluation)는 모니터링 과정으로 4단계 중 점검(check) 단계에 해당한다.

정답 ①

이론: 609p 응용, 기출: 428번(기), 429번(기) 응용

20. ○△× 20.지방.9급

다음에서 설명하는 블록체인 합의 알고리즘은?

보기

- ○ 비트코인에서 사용하는 방식이 채굴 경쟁으로 과도한 자원 소비를 발생시킨다는 문제를 해결하기 위한 대안으로 등장하였다.
- ○ 채굴 성공 기회를 참여자에 따라 차등적으로 부여한다.
- ○ 다수결로 의사 결정을 해서 블록을 추가하는 방식이 아니므로 불특정 다수가 참여하는 환경에서 유효하다.

① Paxos
② PoW(Proof of Work)
③ PoS(Proof of Stake)
④ PBFT(Practical Byzantine Fault Tolerance)

블록체인 합의 알고리즘

◦ Paxos: 합의 알고리즘 중 하나입니다. 데이터베이스를 복제할 때는 동일한 서버를 하나 더 만들어 데이터를 복제하는 것이 일반적이다. Paxos의 특징은 과반수의 동의를 얻었다면 그 동의 내용이 나중에 변경되지 않는다. 리더를 중심으로 합의 형성을 수행하지만 Byzantine Fault 모델이 아니기 때문에 리더가 부정을 저지르는 경우 동기화되지 않는다.

◦ PBFT(Practical Byzantine Fault Tolerance): PBFT는 PoW나 PoS와 마찬가지로 Byzantine Fault 모델이지만 PoW와 PoS의 단점인 파이널리티의 불확실성과 성능 문제를 해결한 것이다.

◦ 작업증명(PoW, Proof of Work): 최초의 블록체인인 비트코인을 창시한 사토시 나카모토가 제안한 합의 알고리즘이다. 새로 만든 블록을 앞 블록에 연결하는데 필요한 해시를 만들고 해시 연결성을 검증하여 데이터가 중간에 위변조가 되지 않았음을 확인한다. 임의의 숫자를 조합해 번호형 자물쇠의 비밀번호를 알아내는 것과 비슷하다. 처음 비밀번호를 파악한 사람만이 가상통화로 보상을 받고 블록을 체인에 추가할 수 있다. 합의 시간이 오래 걸리고 전력을 많이 소비하는 단점이 있다. 비트코인이나 이더리움(후에 PoS로 전환), 제트캐시, 모네로 등의 채굴은 대부분 PoW 방식을 쓴다.

오답피하기 ③ 지분증명(PoS)은 작업증명(PoW)의 에너지 낭비 문제를 해결하기 위해 만들어진 합의 알고리즘이다. 컴퓨팅 파워가 아닌 자신이 가진 가상통화의 양, 즉 지분(stake)에 따라 블록을 생성하고 추가적으로 발행되는 코인을 받는다.

정답 ③

이론: 282p 적중, 기출: 493번(심) 응용

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

[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