2019년 국가직 7급 정보보호론

-2019년 8월 17일 시행

☑ 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

1. ○△× 19.국가.7급

Biba 보안 모델에 대한 설명으로 옳은 것은?

① 이해가 상충되는 회사들 간의 정보 흐름이 일어나지 않도록 고안되었다.
② 자신의 보안 수준보다 낮거나 같은 수준의 객체만 읽을 수 있다.
③ 자신의 보안 수준보다 높거나 같은 수준의 객체에만 쓸 수 있다.
④ 자신의 무결성 수준보다 높거나 같은 수준의 객체만 읽을 수 있다.

비바 무결성 모델(Biba Integrity Model)

- 단순 무결성(simple integrity): 객체의 무결성 수준이 주체의 무결성 수준보다 우세할 때만, 즉 $I(S) \leq I(O)$, 주체는 객체를 읽을 수 있다.
- 무결성 제한(integrity confinement, star integrity): 주체의 무결성 수준이 객체의 무결성 수준보다 우세할 때만, 즉 $I(S) \geq I(O)$, 주체는 객체를 변경할 수 있다.

오답피하기 ① 만리장성 모델에 대한 설명이다. ② 자신의 보안 수준보다 높거나 같은 수준의 객체만 읽을 수 있다. ③ 자신의 보안 수준보다 낮거나 같은 수준의 객체에만 쓸 수 있다.

정답 ④

2. ○△× 19.국가.7급

IT 재해복구체계 수립 시, 업무영향분석(BIA: Business Impact Analysis) 과정에서 고려하는 항목이 아닌 것은?

① MTD(Maximum Tolerable Downtime)
② MTU(Maximum Transfer Unit)
③ RTO(Recovery Time Objective)
④ RPO(Recovery Point Objective)

- RPO(Recovery Point Objective): 재해로 인하여 중단된 서비스를 복구하였을 때 유실을 감내할 수 있는 데이터의 손실 허용 시점
- RTO(Recovery Time Objective): 재해 후 시스템, 응용, 기능들이 반드시 복구 완료되어야 하는 시간
- MTD(Maximum Tolerable Downtime): 치명적인 손실 없이 조직이 운영을 중단하고 견딜 수 있는 최대 시간

오답피하기 ② MTU(Maximum Transfer Unit)는 네트워크를 통해 전송할 수 있는 최대 데이터량으로 BIA와는 무관하다.

정답 ②

3. ○△× 19.국가.7급

다음에서 설명하는 위험 분석 접근 방법은?

보기

- ○ 정형화되고 구조화된 프로세스를 사용하는 대신 분석가 개인의 지식 및 경험을 활용한다.
- ○ 비교적 비용대비 효과가 우수하며 중소규모 조직에 적합하다.
- ○ 개인적인 경험에 의존하므로 정당성이나 일관성이 부족할 수 있다.

① 기준선 접근(Baseline Approach)
② 상세 위험 분석(Detailed Risk Analysis)
③ 비형식적 접근(Informal Approach)
④ 복합 접근(Combined Approach)

오답피하기 ③ 비정형화된 접근법(Informal Approach, 비형식화된 접근법)은 조직 IT 자산에 대한 위험을 분석하기 위해 정형화되고 구조화된 위험 평가 프로세스를 사용하는 대신 위험을 분석하는 개인의 지식과 전문성을 활용하여 실용적인 위험 분석을 실시한다. 이 접근은 중소규모의 조직에 일반적으로 추천되는데 이런 조직에서는 IT 시스템이 조직의 업무 목표를 달성하는데 필수적이지 않아 위험 분석에 따르는 추가 비용이 정당화되기 어렵다.

정답 ③

4. ○△× 19.국가.7급

다음 수식에 의해 산출되는 것은?

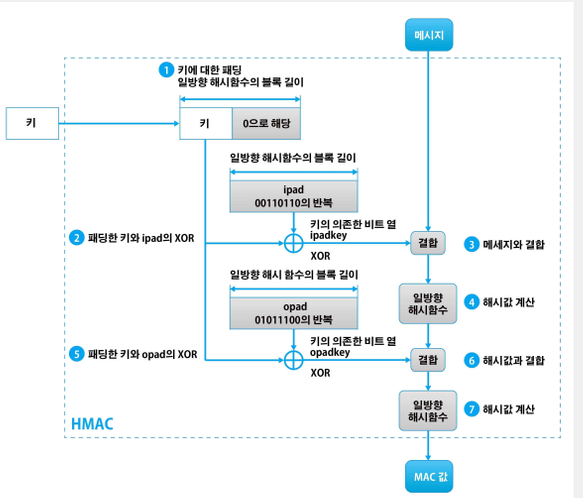
보기

$H[(K^{+} \oplus opad) \,||\, H[(K^{+} \oplus ipad) \,||\, M]]$

H: 해시 함수 K^{+}: 비밀키 K에 0을 덧붙인 것
M: 메시지 ipad, opad: 특정 상수
⊕: XOR ||: 연결(concatenation)

① GMAC
② HMAC
③ CMAC
④ 전자 서명

HMAC의 자세한 내용



오답피하기 ② HMAC은 SHA-1과 같은 일방향 해시함수를 이용하여 메시지 인증코드를 구성하는 방법이다. HMAC의 H는 Hash를 의미한다. 보기는 HMAC을 수식으로 표현한 것이다.

정답 ②

5. ○△× 19.국가.7급

「정보보호 및 개인정보보호 관리체계(ISMS-P)의 인증 등에 관한 고시」 상의 인증심사 기준 중 '개인정보 처리 단계별 요구사항'에 포함되지 않는 것은?

① 사용자 계정 관리
② 이용자 단말기 접근 보호
③ 영상정보처리기기 설치·운영
④ 개인정보처리방침 공개

ISMS-P 개인정보 처리 단계별 요구사항

분야	항목
개인정보 수집 시 보호조치	개인정보 수집 제한, 개인정보의 수집 동의, 주민등록번호 처리 제한, 민감정보 및 고유식별정보의 처리 제한, 간접수집 보호조치, 영상정보처리기기 설치·운영, 홍보 및 마케팅 목적 활용 시 조치
개인정보 보유 및 이용 시 보호조치	개인정보 현황관리, 개인정보 품질보장, 개인정보 표시제한 및 이용 시 보호조치, 이용자 단말기 접근 보호, 개인정보 목적 외 이용 및 제공
개인정보 제공 시 보호조치	개인정보 제3자 제공업무, 위탁에 따른 정보주체 고지, 영업의 양수 등에 따른 개인정보의 이전, 개인정보의 국외이전
개인정보 파기 시 보호조치	개인정보의 파기처리, 목적 달성 후 보유 시 조치, 휴면 이용자 관리
정보주체 권리 보호	개인정보처리방침 공개, 정보주체 권리보장, 이용내역 통지

오답피하기 ① 사용자 계정 관리는 ISMS-P의 개인정보 처리 단계별 요구사항에 포함되지 않는다.

정답 ①

6. ○△× 19.국가.7급

다음 리눅스 /etc/shadow 파일 항목에 대한 설명으로 옳지 않은 것은?

보기

abcd:1qPZPGTVz$RDqazm48WaMXw3Mvy4OQb1:17562:0:99999:7:3::

① 계정명은 abcd이다.
② 계정 패스워드의 해시값 계산에 사용된 해시 함수는 MD-5이다.
③ 솔트(salt)값은 qPZPGTVz이다.
④ 계정 패스워드의 유효기간은 7일이다.

/etc/shadow 파일 형식

[user_account]:[encrypted_password]:[last_change]:[minlife]:[maxlife]:[warn]:[inactive]:[expires]

❶ 사용자 계정(사용자 계정을 인덱스로 하여 /etc/passwd 파일과 사용자 정보를 서로 연계한다.)
❷ 암호화된 패스워드(복호화가 불가능하며, 사용자가 입력한 패스워드를 암호화하기 때문에 이 필드와 비교한다.)
- 형식: idsalt$encrypted_password
- id: 적용된 일방향 해시 알고리즘(1: MD5, 2: Blowfish, 5: SHA-256, 6: SHA-512 등)
- salt: 패스워드 암호화 강도를 높이기 위한 값으로 공격자의 사전공격에 대응할 수 있는 방법인 salt 값은 랜덤한 값으로 생성
- encrypted_password: 사용자가 지정한 패스워드에 salt 값을 추가해서 암호화된 패스워드(해시값)

❸ 마지막으로 패스워드를 변경한 날(1970년 1월1일부터 며칠이 지났는지 그 일수로 표기한다.)
❹ 최소 변경 일수(패스워드를 변경할 수 없는 기간의 일수를 지정한다.)
❺ 최대 변경 일수(현재 사용 중인 패스워드를 변경하지 않고 사용할 수 있는 기간의 일수를 지정한다.)
❻ 경고일수(max 필드에 지정한 일수가 며칠 남지 않았음을 알리는 필드로 로그인할 때마다 경고 메시지를 출력하는 용도로 사용한다.)
❼ 최대 비활성 일수(시스템에 로그인을 자주 하지 않는 사용자의 경우 사용자 계정을 비활성화시켜서 로그인이 되지 않도록 하는 기능이다.)
❽ 사용자 계정이 만료되는 날(1970년 1월 1일부터 며칠이 지났는지 그 일수로 표기한다.)

오답피하기 ④ 최대 변경 일수(Max Days)는 99999이고, 경고일수가 7일이다.

정답 ④

7. ○△× 19.국가.7급

「개인정보 보호법」상 개인정보처리자가 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 경우에 해당하지 않는 것은?

① 정보주체로부터 별도의 동의를 받은 경우
② 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
③ 범죄의 예방을 위하여 필요한 경우
④ 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

제18조(개인정보의 목적 외 이용 · 제공 제한)

① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.
② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 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
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의 · 의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형 및 감호, 보호처분의 집행을 위하여 필요한 경우

오답피하기 ③ 범죄의 예방이 아닌 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우가 해당된다.

정답 ③

8. ○△× 19.국가.7급

「전자정부 SW 개발·운영자를 위한 소프트웨어 개발보안 가이드」상 분석·설계 단계 보안요구항목과 그에 대한 설명으로 옳지 않은 것은?

① 인증 수행 제한 – 인증 반복시도 제한 및 인증실패 등에 대한 인증제한 기능 설계
② 암호키 관리 – 암호키 생성, 분배, 접근, 파기 등 안전하게 암호키 생명주기를 관리할 수 있는 방법 설계
③ 예외 처리 – 보안기능 동작을 위해 사용되는 입력값과 함수의 외부입력값 및 수행결과에 대한 처리방법 설계
④ 시스템 자원 접근 및 명령어 수행 입력값 검증 – 시스템 자원 접근 및 명령어 수행을 위해 사용되는 입력값에 대한 유효성 검증방법과 유효하지 않은 값에 대한 처리방법 설계

◦ 보안기능 동작에 사용되는 입력값 검증: 보안기능(인증, 인가, 권한부여 등) 동작을 위해 사용 되는 입력값과 함수(또는 메서드)의 외부입력값 및 수행결과에 대한 처리방법 설계
◦ 예외처리: 오류메시지에 중요정보(개인정보, 시스템 정보, 민감 정보 등)가 포함되어 출력되거나 에러 및 오류가 부적절하게 처리되어 의도치 않은 상황이 발생하는 것을 막기 위한 안전한 방안 설계

오답피하기 ③ 예외처리가 아닌 보안기능 동작에 사용되는 입력값 검증에 대한 설명이다.

정답 ③

9. ○△× 19.국가.7급

두 소수 p = 13, q = 11을 사용하는 RSA 시스템에서 키값 (e, d)로 사용할 수 있는 쌍은?

① (7, 11)
② (7, 23)
③ (13, 37)
④ (13, 47)

RSA 키 생성 알고리즘
◦ p와 q라고 하는 두 개의 서로 다른 $(p \neq q)$ 소수를 고른다.
◦ 두 수를 곱하여 $N = pq$를 찾는다.
◦ $\phi(N) = (p-1)(q-1)$를 구한다.
◦ $\phi(N)$보단 작고, $\phi(N)$과 서로소인 정수 e를 찾는다.
◦ 확장된 유클리드 호제법을 이용하여 $d \times e$를 $\phi(N)$로 나누었을 때 나머지가 1인 정수 d를 구한다. $(de \equiv 1 \pmod{\phi(N)})$

오답피하기 ③ 먼저 $\phi(N)$를 구하면 $\phi(N) = (13-1)(11-1) = 120$이 된다. 이때 $(de) \bmod 120 = 1$인 쌍을 찾으면 된다. (13, 17)은 $(13 \times 37 = 481) \bmod 120 = 1$을 만족한다.

정답 ③

10. ○△× 19.국가.7급

암호 화폐인 비트코인이 채택한 블록체인의 블록 헤더에 포함되는 구성 요소가 아닌 것은?

① 이전 블록의 헤더를 두 번 연속 해시한 값
② 해당 블록에 포함된 모든 트랜잭션의 해시로부터 추출된 merkle root 해시값
③ 작업증명(proof of work) 조건을 만족하는 nonce 값
④ 블록 생성자(miner)의 계정

블록의 헤더 구조

구분	설명
Version	블록 버전 숫자
Previous block hash	이전 블록헤더를 sha256 해시함수를 이용하여 2번 해싱한 해시값 sha256(sha256())
Merkle hash root	현재 블록에 포함된 거래정보의 거래 해시를 2진 트리 형태로 구성할 때 트리의 루트에 위치하는 해시값
Timestamp	블록의 생성시간, 1970년 1월 1일 이후의 초단위 시간
Bits	블록의 작업증명 알고리즘에 대한 난이도 목표
Nonce	특정 목표값보다 낮은 값을 구하기 위한 카운터

오답피하기 ④ 블록 생성자(miner)의 계정은 헤더에 포함되지 않는다.

정답 ④

11. ○△× 19.국가.7급

다음에서 설명하는 해시 함수(H)의 특성은?

보기
주어진 메시지 x에 대해, H(y) = H(x)를 만족하면서 y≠x인 y를 찾는 것이 계산상 매우 어려워야 한다.

① 의사난수성(Pseudo-randomness)
② 역상 저항성(Pre-image Resistance)
③ 약한 충돌 저항성(Weak Collision Resistance)
④ 강한 충돌 저항성(Strong Collision Resistance)

오답피하기 ③ 제2프리이미지 저항성(두 번째 역상 저항성, 약한 충돌 내성)은 주어진 입력값 x에 대해 h(x)=h(x'), x≠x'을 만족하는 다른 입력값 x'을 찾는 것이 계산적으로 불가능하다는 것이다.

정답 ③

12. ○△× 19.국가.7급

㉠ ~ ㉢에 들어갈 윈도우 운영체제 보안 컴포넌트를 모두 바르게 제시한 것은?

보기

(㉠)은 로컬 사용자에 관련된 보안 정보 및 계정 데이터를 저장하는 데이터베이스이다.
(㉡)은 커널 모드에서 수행되며 사용자나 프로세스가 어떤 객체를 열려고 시도하면 접근 권한을 확인한다.
(㉢)는 사용자 모드에서 수행되며, 로컬 보안 정책을 집행하는 책임이 있다.

	㉠	㉡	㉢
①	SAM	SRM	LSA
②	SRM	SAM	LSA
③	SAM	SRM	SID
④	SRM	SAM	SID

◦ LSA는 모든 계정의 로그인에 대한 검증을 하고 시스템 자원 및 파일 등에 대한 접근 권한을 검사한다.
◦ SAM은 사용자/그룹 계정 정보에 대한 데이터베이스를 관리한다. 그리고 사용자의 로그인 입력 정보와 SAM 데이터베이스 정보를 비교해 인증 여부를 결정한다.
◦ SRM은 사용자에게 SID(Security Identifier)를 부여한다. 또한 SRM은 SID에 기반하여 파일이나 디렉터리에 대한 접근(access)을 허용할지를 결정하고, 이에 대한 감사 메시지를 생성한다.

오답피하기 ① 윈도우의 인증과정에서 가장 중요한 구성 요소는 LSA, SAM, SRM이다. 보기는 각 구성 요소의 역할에 대한 설명이다.

정답 ①

13. ○△× 19.국가.7급

다음의 블록암호 운용모드 중 암호 과정에서는 암호화 함수 E를, 복호 과정에서는 E와 다른 복호화 함수 D를 필요로 하는 것만을 모두 고르면?

보기

ㄱ. ECB ㄴ. CBC ㄷ. CFB ㄹ. OFB

① ㄱ
② ㄱ, ㄴ
③ ㄷ, ㄹ
④ ㄱ, ㄴ, ㄹ

오답피하기 ② ECB, CBC 모드는 복호화 시 복호화 함수를 사용한다. 반면에 CFB, OFB, CTR 모드는 복호화 시 암호화 함수를 사용한다.

정답 ②

14. ○△× 19.국가.7급

「개인정보 보호법」상 '정보주체의 권리 보장'에 대한 설명으로 옳지 않은 것은?

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.
② 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있다.
③ 개인정보처리자는 정보주체가 열람 등 요구를 할 수 있는 구체적인 방법과 절차를 마련하고 이를 정보주체가 알 수 있도록 공개하여야 한다.
④ 개인정보처리자는 정보주체가 열람 등 요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

제36조(개인정보의 정정 · 삭제)
① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.
② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정 · 삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.
③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.
⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정 · 삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.
⑥ 제1항 · 제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

오답피하기 ② 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 개인정보 보호위원회의 심의를 거쳐 요구할 수 있는 것이 아니라 삭제를 요구할 수 없다.

정답 ②

15. ○△× 19.국가.7급

패스워드를 이용해서 원격 사용자를 인증하는 경우, 호스트는 비표(nonce)라는 일회성 임의 숫자 r를 생성하고 이와 함께 두 함수 h()와 f()를 사용자에게 제시한다. 사용자는 이에 대한 응답으로 f(r', h(P'))를 반환한다. 호스트는 r' = r, h(P') = h(사용자 패스워드)의 여부를 판단하여 인증을 완료한다. 이때 r을 사용하는 것은 어떤 공격에 대비하기 위한 것인가?

① 전사 공격(Brute-Force Attack)
② 트래픽 스니핑 공격(Traffic Sniffing Attack)
③ 패스워드 사전 공격(Password Dictionary Attack)
④ 재전송 공격(Replay Attack)

◦ 재전송 공격을 막을 수 있는 방법에는 순서번호, 타임스탬프, 비표(nonce), 시도응답 방법 등이 있다.

오답피하기 ④ 재전송 공격을 막기 위한 시도응답 방법에 대한 설명이다.

정답 ④

16. ○△× 19.국가.7급

HTTP 버전 1.1에 대한 설명으로 옳지 않은 것은?

① TCP를 전송 프로토콜로 사용한다.
② 요청 메시지의 첫 줄인 요청 라인에는 메소드, URL, HTTP 버전 필드가 포함된다.
③ 요청과 그에 대한 응답이 같은 연결로 보내지는 지속 연결(persistent connection)을 기본으로 하며, 분리된 별도의 연결을 이용하는 비지속 연결(non-persistent connection)도 지원한다.
④ HTTP 서버가 클라이언트에 대한 정보를 유지하는 상태(stateful) 프로토콜이다.

◦ HTTP 버전 1.0은 비영속적 연결(nonpersistent connection)을 사용하였으나, 버전 1.1은 영속적 연결(persistent connection)을 기본값으로 하는데 이는 사용자에 의해 변경될 수 있다.

오답피하기 ④ HTTP는 stateless 프로토콜이다.

정답 ④

17. ○△× 19.국가.7급

서버가 응용 메시지를 여러 개의 TCP 세그먼트로 나누어 클라이언트에게 전송하는 경우, TCP의 동작에 대한 설명으로 옳은 것은?

① 클라이언트와 서버 간의 TCP 연결 설정 후, 첫 번째 세그먼트의 순서 번호는 일반적으로 0부터 시작한다.
② 두 번째 세그먼트의 순서 번호는 첫 번째 세그먼트가 운반에 성공한 데이터의 바이트 수를 첫 번째 세그먼트의 순서 번호에 더한 것이다.
③ 일정량의 데이터를 포함한 세그먼트를 정상적으로 수신한 클라이언트는 수신한 세그먼트의 순서 번호에 1을 더한 값을 확인응답 번호로 하여 응답하고 다음 세그먼트를 기다린다.
④ 클라이언트가 FIN 세그먼트를 보내고 서버가 이에 대한 ACK 세그먼트를 보냄으로써 서버의 데이터 전송을 위한 연결이 완전히 종료된다.

◘ 순서 번호
◦ 첫 번째 세그먼트의 순서번호는 임의 번호인 ISN(초기 순서번호)이다.
◦ 어떤 다른 세그먼트의 순서번호는 이전 세그먼트 순서번호에 이전 세그먼트에 의해 운반된 바이트의 수를 합한 것이다.

◘ 확인 응답 번호
◦ 세그먼트 확인응답 영역의 값은 상대방이 수신하기를 기대하는 다음 바이트 번호로 정의된다. 확인응답 번호는 누적이 된다.

오답피하기 ① 첫 번째 세그먼트의 순서 번호는 일반적으로 임의 번호이다. ③ 수신한 세그먼트의 순서 번호와 수신한 데이터 크기에 1을 더한 값을 확인응답 번호로 하여 응답한다. ④ 3-way 연결 종료는 FIN - FIN+ACK - ACK 순서로 이루어지고, 4-way 연결 종료는 FIN - ACK - FIN -ACK 순서로 이루어진다.

정답 ②

18. ○△× 19.국가.7급

다음에서 설명하는 네트워크 기반 공격 방법은?

보기

○ TCP 헤더 정보를 보고 패킷을 걸러내는 방화벽을 우회하기 위한 공격 방법이다.
○ IP 단편 옵션을 이용하여 매우 작게 패킷을 나누어서 TCP 헤더 자체가 분리되도록 만든다.
○ 일부 패킷 필터는 첫 번째 단편만 검사하고 나머지 단편은 모두 통과시키기 때문에 이러한 공격 방법이 유효할 수 있다.

① Source Routing Attack
② Ping of Death
③ Trinoo
④ Tiny Fragment Attack

◦ 송신 경로 지정법(source routing): 중간에 반드시 거쳐서 가야 할 경로를 지정하고 이를 거쳐왔는지 확인하는 라우팅 방법이다. 여러 경로로 돌아온 확인 메시지 중에서 가장 상태가 좋은 경로를 찾고 이후에는 이 경로 정보를 데이터에 넣어 송신한다.
◦ 근원지 경로배정 공격: 발신자가 패킷의 근원지 경로 정보를 분석 당하지 않도록 보안기능이 있는 곳들을 피해가기 위해 패킷에 인터넷을 통과할 때 따라가야할 경로를 지정해 공격하는 방법이다.

오답피하기 ④ Tiny Fragment 공격은 IP헤더보다 작은 fragment를 만들어서 침입차단시스템(방화벽)을 우회하여 내부 시스템에 침입하는 공격기법으로 DoS 공격 기법이 아닌 우회 공격 기법이다.

정답 ④

19. ○△× 19.국가.7급

다음은 「정보보호산업의 진흥에 관한 법률」상 정보보호산업의 활성화를 위한 구매수요정보의 제공에 관한 조항의 일부이다. ㉠, ㉡에 들어갈 용어를 바르게 연결한 것은?

보기

「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 (㉠) 정보보호기술등에 대한 구매수요 정보를 (㉡)에게 제출하여야 한다.

㉠	㉡
① 매년	과학기술정보통신부장관
② 매년	행정안전부장관
③ 2년마다	과학기술정보통신부장관
④ 2년마다	행정안전부장관

제6조(구매수요정보의 제공)

① 「전자정부법」 제2조제2호에 따른 행정기관 또는 공공기관의 장은 소관 기관·시설의 정보보호 수준을 강화하기 위하여 매년 정보보호기술등에 대한 구매수요 정보를 과학기술정보통신부장관에게 제출하여야 한다.

② 과학기술정보통신부장관은 제1항에 따라 제출된 구매수요정보를 정보보호기업에 제공할 수 있다.

③ 과학기술정보통신부장관은 제2항에 따라 구매수요정보를 정보보호기업에 제공하는 경우 과학기술정보통신부 내에 별도의 심의위원회를 개최하여 국가안전 및 공공의 이익에 중대한 영향을 미치는 내용이 정보보호기업에 제공되지 아니하도록 하여야 한다.

④ 제1항 및 제2항에 따른 구매수요정보 제출 및 제공의 구체적인 횟수·시기·방법·절차 등에 필요한 사항은 대통령령으로 정한다.

오답피하기 ① 행정기관 또는 공공기관의 장은 매년 정보보호기술등에 대한 구매수요 정보를 과학기술정보통신부장관에게 제출하여야 하고, 과학기술정보통신부장관은 제출된 구매수요정보를 정보보호기업에 제공할 수 있다.

정답 ①

20. ○△× 19.국가.7급

IEEE 802.11i에서 정의한 무선 랜 데이터 보안 프로토콜로 메시지 무결성 코드(MIC)와 RC4 암호 알고리즘을 이용하여 메시지 무결성과 데이터 기밀성을 제공하는 것은?

① EAP
② WEP
③ CCMP
④ TKIP

오답피하기 ④ WPA는 TKIP 알고리즘을 사용한다. TKIP는 기본적으로 WEP와 같은 RC4 키 스트림 암호화 알고리즘을 사용한다. 보안 강화를 위해 MIC(또는 Michael)라는 8바이트의 메시지 무결성 코드를 추가했고, IV 생성에서 새로운 배열 규칙을 적용했다.

정답 ④

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