2021-군무원-전산직-정보보호론-해설-곽후근

1. 응용 수준 취약점에 대한 설명으로 옳지 않은 것은?
① 버퍼오버플로우는 메모리나 버퍼의 블록 크기보다 더 많은 데이터를 넣음으로써 결함을 발생시키는 취약점이다.
② 크로스 사이트 스크립팅은 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입 할 수 있는 취약점이다. 주로 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다.
③ SSI 인젝션은 조작된 XPath(XML Path) 쿼리를 보냄으로써 비정상적인 데이터를 쿼리해 올수 있는 취약점이다.
④ SQL인젝션은 SQL문으로 해석될 수 있는 입력을 시도하여 데이터베이스에 접근할 수 있는 취약점이다.
정답 체크
(3) 해당 설명은 command 또는 code 인젝션이고, SSI 인젝션은 SSI에 악의적인 스크립트를 삽입하는 공격을 의미한다. 여기서, SSI는 Server Side Includes를 뜻하는데 이는 방문자 카운터, 홈페이지의 로고를 간단하게 수정하기 위해 사용되며, 형식은 HTML의 주석과 비슷하고 확장자명은 .shtml을 사용한다. 또한, HTML은 사용자의 브라우저에서 처리되는 반면에 SSI는 웹서버에서 처리되며 처리의 결과만이 사용자의 브라우저로 전송된다.
오답 체크
(1) 스택에는 복귀 주소(return address)가 저장되는데, 오버플로우가 발생하면 복귀 주소가 공격자가 원하는 주소로 바뀌어 공격자가 원하는 코드가 실행된다. (힙 버퍼 오버플로우도 가능)
(2) 웹사이트 관리자가 아닌 이가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 주로 여러 사용자가 보게 되는 전자 게시판에 악성 스크립트가 담긴 글을 올리는 형태로 이루어진다. 이 취약점은 웹 애플리케이션이 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 이 취약점으로 해커가 사용자의 정보(쿠키, 세션 등)를 탈취하거나, 자동으로 비정상적인 기능을 수행하게 할 수 있다. 주로 다른 웹사이트와 정보를 교환하는 식으로 작동하므로 사이트 간 스크립팅이라고 한다. (저장, 반사, DOM 등이 존재)
(4) 웹 주소창에 SQL 구문에 사용되는 문자 기호의 입력을 적절히 필터링하지 않아, 조작된 SQL 구문을 통해 DB에 무단 접근하여 자료를 유출/변조할 수 있는 취약점이다. 예를 들어 패스워드에 '1' or '1'='1'를 입력하면 or의 첫 번째 문장은 패스워드와 '1'을 비교해서 false가 되고 두 번째 문장은 true가 되기 때문에 전체적인 문장은 true(or는 두 문장 중 하나라도 true면 true가 됨)가 되어 패스워드 없이 로그인에 성공하게 된다.

2. 전자서명법에 대한 설명으로 옳지 않은 것은?
① "전자문서"란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
② 당사자 간의 약정에 따라 행해진 서명, 서명 날인 또는 기명날인 방식의 전자서명은 제3의 신뢰기관이 개입하지 않았으므로 전자서명법 상 효력을 가지지 않는다.
③ "인증서"란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
④ "전자서명생성정보"란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.
정답 체크

(2) 전자서명법 제3조(전자서명의 효력) 상 ② 법령의 규정 또는 당사자 간의 약정에 따라 서명, 서명날인 또는 기명날인의 방식으로 전자서명을 선택한 경우 그 전자서명은 서명, 서명날인 또는 기명날인으로서의 효력을 가진다.
오답 체크
(1) 전자서명법 제2조(정의) 상 “전자문서”란 정보처리시스템에 의하여 전자적 형태로 작성되어 송신 또는 수신되거나 저장된 정보를 말한다.
(3) 전자서명법 제2조(정의) 상 “인증서”란 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다.
(4) 전자서명법 제2조(정의) 상 “전자서명생성정보”란 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다.

3. RSA 암호알고리즘을 위해 두 개의 소수가 p=3, q=11일 경우, 공개키(n)과 암호화 공개키(e=7)에 대응되는 복호용 개인키(d)로 적절한 것은?
① n=33, d=3
② n=21, d=5
③ n=21, d=3
④ n=33, d=5
정답 체크
(1) n = pxq = 3x11 = 33
exd mod L = 1, 여기서 L은 오일러 피 함수로 (p-1)x(q-1)로 계산되어 20이 된다.
7xd mod 20 = 1이므로 d는 3이 된다.

4. Diffie-Hellman 키 공유 프로토콜에서, 공개 정보인 소수 p=11, 원시원소 g=7 인 경우, 갑이 자신의 비밀키(x)를 5로, 을이 자신의 비밀키 (y)를 3으로 선택했을 경우, 갑과 을이 공유하는 세션키로 옳은 것은?
① 10
② 7
③ 8
④ 5
정답 체크
(1) 세션키는 g^{xy} mod p로 계산된다.
7^{3x5} mod 11 = 7^{15} mod 11 = $7^3x7^3x7^3x7^3x7^3$ mod 11 = (7^3 mod 11) x (7^3 mod 11) x (7^3 mod 11) x (7^3 mod 11) x (7^3 mod 11) mod 11 = 2x2x2x2x2 mod 11 = 32 mod 11 = 10

5. 정보보호의 3대 요소로 옳지 않은 것은?
① 비인가자, 불법 침입자의 접근 제어를 통해 비밀 정보가 누출되지 않도록 보장하는 기밀 성
② 메시지의 송수신이나 교환 후, 또는 통신이나 처리가 실행된 후에 그 사실을 증명함으로써 사실 부인을 방지하는 부인 방지
③ 인가된 사용자가 적시, 적소에 필요 정보에 접근할 수 있고 사용 가능하도록 보장하는 가용성
④ 불법 사용자에 의해 정보 및 소프트웨어가 변경, 삭제, 생성되는 것으로부터 보호하여 원래 상태

를 보존 유지하는 무결성
정답 체크
(2) 부인 방지는 정보보호의 3대 요소가 아닌 6대 요소에 속한다.
오답 체크
(1), (3), (4) 정보보호의 3대 요소(CIA)는 기밀성, 무결성, 가용성이다.

6. 우리나라가 개발해 국제표준화한 암호 알고리즘 만으로 짝지은 것은?
① 블록 암호 알고리즘(SEED) - 서명 알고리즘(KCDSA)
② 블록 암호 알고리즘(AES) - 서명 알고리즘(RSA)
③ 블록 암호 알고리즘(triple DES) - 서명 알고리즘(DSA)
④ 블록 암호 알고리즘(ARIA) - 서명 알고리즘(ECDSA)
정답 체크
(1) SEED는 KISA(한국인터넷진흥원)와 국내암호 전문가가 만들었고, KCDSA는 KISA가 만들었다.
오답 체크
(2) AES는 미국(NIST)에서 만들고 내부에 사용된 Rijndael은 벨기에에서 만들었다. 그리고 RSA는 미국(MIT)에서 만들었다.
(3) 3DES는 미국(NIST)에서 만들고, DSA는 미국(NIST)에서 만들었다.
(4) ARIA는 한국(학계, 연구소, 정부 기관)에서 만들고, ECDSA는 ECC에 기반한 전자서명으로 ECC는 미국(워싱턴대학교, IBM)에서 만들어졌다.

7. 일어날 수 있는 모든 가능한 경우에 대하여 조사하는 형태의 공격으로 적절한 것은?
① 전수 조사 공격
② 중간자 공격
③ 생일 공격
④ 사전 공격
정답 체크
(1) 가능한 모든 조합을 이용(대입)해서 공격하는 것을 의미한다. 패스워드를 공격할 때 사용한다.
오답 체크
(2) 통신을 연결하는 두 사람 사이에 중간자가 침입하여, 두 사람은 상대방에게 연결했다고 생각하지만 실제로는 두 사람은 중간자에게 연결되어 있으며 중간자가 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달한다. 스니핑 등에 사용된다.
(3) 어떤 모임에서 사람의 수가 증가할수록 생일이 같을 확률이 증가함을 의미한다. 해시를 공격할 때 사용된다.
(4) 사전 파일을 이용하여 패스워드를 크래킹한다.

8. 정보 보호 제품 평가 인증 제도에 대한 설명으로 옳지 않은 것은?
① 정보보호제품의 보증수준을 정하기 위한 공통평가기준에서 미리 정의된 보증등급으로, EAL1, EAL2, EAL3, EAL4, EAL5, EAL6의 6개의 보증 등급으로 구분된다. EAL1은 최고의 평가보증등급이고, EAL6은 최저의 평가보증등급이다.
② 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.

③ 공통평가기준 1부는 정보보호시스템 보안성 평가의 원칙과 일반 개념을 정의하고 평가의 일반적인 모델을 설명하는 소개부분으로, IT 보안 목적을 표현하고 IT 보안요구사항을 선택 정의하며, 제품 및 시스템의 상위수준 명세를 작성하기 위한 구조를 소개한다.
④ "보호프로 파일" 이라 함은, 평가대상 범주를 위한 특정 소비자의 요구에 부합 하는 구현에 독립적인 보안요구사항의 집합을 말하며, "보안목표명세서"라 함은 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.
정답 체크
(1) 보증 등급은 7개이고, EAL1이 최저의 등급이고 EAL7이 최고의 등급이다.
오답 체크
(2) 예를 들어, 보안 장비(방화벽, IDS 등)에 적용할 수 있다.
(3) 공통평가기준에 대한 소개 부분으로, IT 보안성 평가의 원칙과 일반 개념을 정의하고 평가의 보편적인 모델을 제시한다.
(4) PP(Protection Profile)는 사용자 또는 개발자의 요구사항을 정의한다(전체 제품). ST(Security Target)는 개발자가 작성하며 제품 평가를 위한 상세 기능을 정의한다(개별 제품). PP는 기술적인 구현 가능성을 고려하지 않는데 반해, ST는 기술적 구현 가능성을 고려한다.

9. 정보 보안 시스템을 설 계 하거나 운영 할 때 고려하는 요소 중 하나인 가용성을 보존하기 위해 행해지는 활동으로 옳지 않은 것은?
① 백업
② 네트워크 증설
③ 침입 탐지 시스템 운용
④ 전자 서명
정답 체크
(4) 전자 서명으로 서명자 인증, 무결성, 부인 방지를 할 수 있지만 가용성을 제공하지는 않는다.
오답 체크
(1) 백업을 하면 문제가 생겼을 때 빠르게 복구할 수 있다(가용성 보존).
(2) 네트워크를 증설하면 대역폭으로 인한 문제를 해결할 수 있다(가용성 보존).
(3) 침입 탐지 시스템을 운용하면 오용 탐지와 이상 탐지를 통해 가용성에 문제가 되는 것을 탐지하여 해결할 수 있다.

10. 디지털 포렌식 원칙에 해당하지 않는 것은?
① 정당성의 원칙
② 재현의 원칙
③ 연계 보관성의 원칙
④ 무죄 추정의 원칙
정답 체크
(4) 해당 원칙은 디지털 포렌식 원칙에 해당하지 않는다.
오답 체크
(1) 모든 증거는 적법한 절차를 거쳐서 획득한 것이어야 함을 의미한다. 위법한 절차를 거쳐 획득한 증거는 증거 능력이 없다.
(2) 법정에 증거를 제출하려면 똑같은 환경에서 같은 결과가 나오도록 재현할 수 있어야 한다. 수행

할 때마다 다른 결과가 나온다면 증거로 제시할 수 없다.
(3) 증거는 획득되고 난 뒤 이송/분석/보관/법정 제출이라는 일련의 과정이 명확해야 하고, 이러한 과정에 대한 추적이 가능해야 함을 의미한다.

11. 개인정보보호법 제3조(개인정보보호원칙)에 명시된 내용으로 옳지 않은 것은?
① 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리 하여야하며, 그 목적 외의 용도로 활용하여서는 아니된다.
② 개인정보처리자는 정보주체의 동의를 받은 경우 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
③ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보 주체의 권리를 보장하여야 한다.
④ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
정답 체크
(2) 해당 내용은 개인정보 보호법 제3조(개인정보 보호 원칙)에 포함되지 않는다.
오답 체크
(1) 개인정보 보호법 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
(3) 개인정보 보호법 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
(4) 개인정보 보호법 제3조(개인정보 보호 원칙) 상 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

12. 공개키 기반 구조에 대한 설명으로 옳지 않은 것은?
① X.509 국제표준에 기반하며, 정보의 기밀성, 무결성, 인증, 부인방지 등 신뢰 서비스를 제공하는데 이용된다.
② 공개키 인증서를 발행하는 인증기관, 실체의 신원을 확인하는 등록기관, 인증서 폐지 목록을 관리하는 보관소, 최종 실체 등으로 구성된다.
③ 기업 및 기관 단위에서 사용자들에게 특정 시스템 및 애플리케이션에 접근 할 수 있는 권한을 차등 부여해주는 관리 체계이다.
④ 공개키 인증서를 생성, 관리, 배포, 이용, 저장 및 폐지하기 위해 필요한 기능, 정책, 하드웨어, 소프트웨어 및 절차의 집합이다.
정답 체크
(3) 해당 설명은 굳이 분류하자면 접근 제어에 해당한다.
오답 체크
(1) X.509에 기반한다. 공개키에 CA(인증기관)가 서명함으로써 무결성, 인증, 부인방지를 제공하며, 해당 공개키로 암호화를 수행함으로 기밀성을 제공한다.
(2) 구성 요소는 이용자, 인증기관, 저장소로 구성된다.
(4) 공개키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택사양의 총칭이다.

13. 완성된 바이너리 형태의 소프트웨어를 역으로 분석하여 원래 소스 코드의 구조를 파악하는 리버

스 엔지니어링의 목적으로 옳지 않은 것은?
① 취약점 분석
② 악성 코드 분석
③ 디지털 포렌식
④ 컴파일 및 링킹
정답 체크
(4) 컴파일 및 링킹은 소스 코드를 바이너리 형태로 만드는 것으로 역공학이 아니라 공학(engineering)이다.
오답 체크
(1), (2) 역공학을 이용하면 취약점 분석 및 악성 코드 분석 등을 할 수 있다.
(3) 디지털 포렌식을 위해 역공학을 이용할 수 있다.

14. 정보통신기반 보호에 대한 설명으로 옳지 않은 것은?
① 중앙행정기관의 장은 소관분야의 정보통신기반시설 중 업무의 국가 사회적 중요성, 업무의 정보통신기반시설에 대한 의존도, 국가안전보장과 경제사회에 미치는 피해 규모 및 범위 등 을 고려하여 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.
② 주요정보통신기반시설 보호 계획에는 주요정보통신기반시설의 취약점 분석 · 평가, 침해사고에 대한 예방·백업·복구대책, 보호에 관하여 필요한 사항을 포함해야 한다.
③ 정보통신기반보호위원회는 주요정보통신기반 시설에 대하여 보호 지침을 제정하고 해당 분 야 관리기관의 장에게 이를 지키도록 권고 할 수 있다.
④ “정보통신기반시설”이라 함은 국가안전보장 · 행정 · 국방 · 치안 · 금융 · 통신 · 운송 · 에너지 등의 업무와 관련된 전자적 제어 · 관리시스템 및 정보통신망을 말한다.
정답 체크
(3) 정보통신기반 보호법 제10조(보호지침) 상 관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.
오답 체크
(1) 정보통신기반 보호법 제8조(주요정보통신기반시설의 지정 등) 상 중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다. 1. 해당 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성 2. 제1호에 따른 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도 3. 다른 정보통신기반시설과의 상호연계성 4. 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위 5. 침해사고의 발생가능성 또는 그 복구의 용이성
(2) 정보통신기반 보호법 제6조(주요정보통신기반시설보호계획의 수립 등) 상 주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다. 1. 주요정보통신기반시설의 취약점 분석 · 평가에 관한 사항 2. 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항 3. 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항
(4) 정보통신기반 보호법 제2조(정의) 상 “정보통신기반시설”이라 함은 국가안전보장 · 행정 · 국방 · 치안 · 금융 · 통신 · 운송 · 에너지 등의 업무와 관련된 전자적 제어 · 관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 말한다.

15. 암호화에 대한 설명으로 옳지 않은 것은?
① 순서보존 암호화(Order-preserving encryption)는 원본 정보의 순서와 암호값의 순서가 동일하게 유지되는 암호화 방식이다.
② 형태보존 암호화(Format-preserving encryption)는 원본 정보의 형태와 암호값의 형태가 동일하게 유지되는 암호화 방식이다.
③ 동형 암호화(Homomorphic encryption)는 암호화된 상태에서의 연산이 가능한 암호화 방식이다.
④ 일방향 암호화는 원문에 대한 암호화만 가능하며 추가 정보가 있으면 암호문에 대한 복호화가 가능하다.
정답 체크
(4) 여기서 일방향 암호화는 해시와 같은 단방향 암호화를 의미한다. 즉, 복호화가 불가능하다. 추가 정보라는 것은 해시에 걸리는 시간 등을 의미하고(부채널 공격), 이런 정보는 암호화/복호화가 가능한 곳에서는 사용 가능하나 일방향 암호화에서는 무용지물이다.
오답 체크
(1) 암호화 적용 시 암호 데이터가 원본 데이터와 동일 순서 정렬 기반 암호화 알고리즘이다.
(2) 평문과 암호문의 형태를 동일하게 유지한 채 암호화를 수행하는 암호화 알고리즘이다.
(3) 암호화된 데이터를 복호화 없이도 연산할 수 있는 암호 기술이다.

16. 온라인상 본인확인서비스에 대한 설명 중 옳지 않은 것은?
① “연계 정보”라 함은 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위해 본인확인기관이 이용자의 주민등록번호와 본인확인기관 간 공유 비밀정보를 이용하여 생성한 정보를 말한다.
② “중복가입확인정보”라 함은 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는 데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관 간 공유비밀정보를 이용하여 생성한 정보를 말한다.
③ “공유비밀정보”라 함은 본인확인기관이 특정 이용자에 대해 동일한 중복가입확인정보와 연계 정보를 생성하기 위해 공유하는 정보를 말한다.
④ 전자서명법에 따른 “전자서명인증사업자”는 “정보통신망 이용 촉진 및 정보보호 등에 관한 법률”에 근거해 지정되는 본인확인기관으로 간주된다.
정답 체크
(4) 본인확인기관 지정 등에 관한 기준 제2조(정의) 상 "본인확인기관"이라 함은 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하는 자로서 법 제23조의3제1항에 따라 방송통신위원회로부터 본인확인기관의 지정을 받은 자를 말한다.
오답 체크
(1) 본인확인기관 지정 등에 관한 기준 제2조(정의) 상 "연계정보"라 함은 정보통신서비스 제공자의 온·오프라인 서비스 연계를 위해 본인확인기관이 이용자의 주민등록번호와 본인확인기관간 공유 비밀정보를 이용하여 생성한 정보를 말한다.
(2) 본인확인기관 지정 등에 관한 기준 제2조(정의) 상 "중복가입확인정보"라 함은 웹사이트에 가입하고자 하는 이용자의 중복가입 여부를 확인하는 데 사용되는 정보로서 본인확인기관이 이용자의 주민등록번호, 웹사이트 식별번호 및 본인확인기관간 공유비밀정보를 이용하여 생성한 정보를 말한다.
(3) 본인확인기관 지정 등에 관한 기준 제2조(정의) 상 "공유비밀정보"라 함은 본인확인기관이 특정 이용자에 대해 동일한 중복가입확인정보와 연계정보를 생성하기 위해 공유하는 정보를 말한다.

17. 인터넷과 같은 공중망에 터널을 형성하고 이를 통해 패킷을 캡슐화해서 전달함으로써 사설망과 같은 전용 회선처럼 사용할 수 있게 하는 기술로 적절한 것은?
① 가상 사설망
② 접근 제어
③ 회선 관리
④ 세션 관리
정답 체크
(1) VPN은 공중망과 사설망의 장점을 결합한 기술이다.
오답 체크
(2) 어떻게 하면 사용자들이 자신의 권한에 맞는 정보만 접근할 수 있도록 통제할 수 있을까에 대한 것을 다룬다.
(3) 클라이언트 입장에서의 세션 관리는 사용자가 활동을 수행해서 세션을 유지하고, 서버 입장에서의 세션 관리는 지속적인 인증을 수행한다.
(4) 전용 회선 관리 등을 의미한다.

18. ARP Spoofing 공격에 대한 설명으로 옳지 않은 것은?
① ARP(Address Resolution Protocol)이 인증을 하지 않기 때문에 발생한다.
② 근거리 네트워크 환경에서 발생한다.
③ ARP 테이블 변경을 동적으로 관리함으로 예방할 수 있다.
④ 중간자 공격 기법을 통해 이루어진다.
정답 체크
(3) ARP 테이블 변경을 정적으로 관리함으로 예방할 수 있다.
오답 체크
(1) ARP를 통한 MAC이 정상적인 상대방인지 공격자인지 알 수 없다.
(2) ARP를 이용하므로 LAN 환경(브로드캐스팅 도메인)에서 발생한다.
(4) 해당 공격은 MITM(중간자 공격)의 한 종류이다.

19. 공개된 네트워크 환경에서 통신하는 두 당사자가 공유키를 만드는데 사용되는 Diffie-Hellman 알고리즘에 대한 설명으로 옳지 않은 것은?
① 비밀키 알고리즘의 일종이다.
② 안전을 위해 일반적으로 1024비트 이상의 큰 소수를 사용해야 한다.
③ 상대방에 대한 인증을 제공하지 않기 때문에 중간자 공격이 가능하다.
④ 안전을 위해 충분히 안전한 난수 생성 알고리즘을 사용해야 한다.
정답 체크
(1) 공개키 알고리즘의 일종이다.
오답 체크
(2) 1024비트 이상의 큰 소수를 사용한다.
(3) Diffie-Hellman은 중간자 공격에 약하다.
(4) 사용되는 난수를 위해 안전한 난수 생성 알고리즘을 사용한다.

20. 미국 국방부에 의해 개발된 컴퓨터 보안 평가 방법론인 TCSEC에 대한 설명으로 옳지 않은 것은?
① 가장 낮은 평가 수준은 D이고 가장 높은 수준은 A이다.
② 운영체제에 중점을 두어 평가하기 때문에 방화벽 등에 적용하기 어렵다.
③ 기밀성, 무결성, 가용성에 대한 요구 사항을 균형적으로 다루고 있다.
④ 평가 수준별로 기능 요구 사항과 보증 요구 사항을 포함한다.
정답 체크
(3) 기밀성에만 초점을 맞춘다.
오답 체크
(1) 가장 낮은 등급은 D이고, 가장 높은 등급은 A이다.
(2) 운영체제(윈도우즈, 유닉스 등)에 중점을 둔 평가체계로, 운영체제를 대상으로 보안 요소를 가감하여 등급을 매긴다고 할 수 있다. 방화벽이나 보안 장비에 적용하는 것은 CC이다.
(4) 기능 요구와 보증 요구는 CC로 이어진다.

21. 개인정보 가명처리에 대한 설명으로 옳지 않은 것은?
① 가명정보는 개인 정보를 가명 처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보이다.
② 가명정보는 처리(제공) 환경에 따라 가명정보 처리자 내부에서 활용(자체활용 또는 내부 제공·결합)하는 경우와 제3자에게 제공하는 경우로 구분할 수 있다.
③ 가명정보처리자는 가명정보 또는 추가정보의 안전한 관리를 위하여 기술적 안전조치와 관리적 안전조치를 취해야 하며, 물리적 안전조치를 취하지 않아도 무방하다.
④ 가명정보는 개인정보처리자의 정당한 처리 범위 내에서 통계 작성, 과학적 연구, 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 처리할 수 있다.
정답 체크
(3) 개인정보 보호법 제28조의4(가명정보에 대한 안전조치의무 등) 상 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
오답 체크
(1) 개인정보 보호법 제2조(정의) 상 가명정보란 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보이다.
(2) 개인정보보호위원회가 배포한 “가명정보 처리 가이드라인” 상 가명정보는 처리(제공) 환경에 따라 가명정보 처리자 내부에서 활용(자체활용 또는 내부 제공·결합)하는 경우와 제3자에게 제공하는 경우로 구분할 수 있다.
(4) 개인정보 보호법 제28조의2(가명정보의 처리 등) 상 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

22. 접근 권한이 시스템 전체적으로 보안 정책 및 관련 규칙에 따라 결정되기 보다는 자원의 소유자에 의해 결정되는 접근 제어 모델에 해당하는 것으로 옳은 것은?
① 강제적 접근 제어
② 임의적 접근 제어

③ 역할 기반 접근 제어
④ 규칙 기반 접근 제어
정답 체크
(2) 객체에 대한 소유권(ownership)에 기초해서 소유권을 가진 주체가 객체에 대한 권한의 전부 혹은 일부를 다른 주체에게 부여한다. 유닉스 혹은 관계형 데이터베이스(RDBMS)에서 사용한다.
오답 체크
(1) 주체와 객체에 적절한 보안 등급(레이블)을 부여하고, 접근 제어시 이 등급을 비교함으로써 접근의 허용 여부를 판단하게 된다. 군사 환경과 같은 엄격한 보안이 요구되는 분야에 적합하다.
(3) 기업 환경에서는 사용자가 기업 내에서 어떤 역할(Role)을 수행하고 있는가에 따라 권한이 정해진다. 이를 모델화한 것이 역할 기반 접근 제어이다.
(4) 규칙에 기반한 접근 제어이다. 여기서 규칙이란 “어떤 데이터는 3:00부터 6:00까지만 접근이 허용된다”와 같은 것을 의미한다.

23. 윈도우를 비롯한 시스템에서 하드웨어 레벨에서 보안을 향상시키는 방안으로 TPM(Trusted Platform Module)이 있다. TPM에 대한 설명으로 옳지 않은 것은?
① 암·복호화 및 전자서명 기능 제공
② 부팅 과정에서 인증을 통해 신뢰성 제공
③ 디바이스 및 플랫폼 인증
④ 운영체제에 의존하여 명령어가 동작함
정답 체크
(4) TPM은 독립된 하드웨어 모듈로서 운영체제가 들어가 있지 않다.
오답 체크
(1) 암호화, 복호하, 전자서명 엔진이 들어있다.
(2) 부팅 단계에서부터 시스템의 무결성 검증에 이용된다.
(3) 디바이스 및 플랫폼 인증과 원격 검증에서 사용된다.

24. 블록체인 합의 알고리즘에 대한 설명으로 옳지 않은 것은?
① 분산 시스템에서 합의란 네트워크에 존재하는 독립적인 참여자들이 동일한 블록체인 원장을 유지할 수 있도록 원장에 포함할 블록을 결정하는 방식이다.
② 분산 원장 시스템에서는 다양한 합의 알고리즘들이 사용될 수 있으며, 예로는 작업 증명 (PoW: Proof of Work), 지분증명(PoS : Proof of Stake), 위임 지분증명(DPoS : Delegated Proof of Stake) 등이 존재한다.
③ 지분 증명은 블록을 생성하는 노드가 작업(예: 특정 조건을 충족해야 하는 해시 연산 등 높은 비용/자원이 필요한 작업)을 통해 스스로의 신뢰성을 증명하는 합의 방식이다.
④ 분산 원장 시스템 내의 모든 노드가 일관성 있는 분산 원장을 보유할 수 있도록 통신을 통해 새로운 기록의 공유, 검증 및 추가에 대한 전체의 동의를 이끌어 내는 알고리즘이다.
정답 체크
(3) 해당 설명은 작업 증명이고, 지분 증명은 채굴기 없이 본인이 소유한 코인의 지분으로 채굴되는 방식이다. 해당 코인을 가지고 있는 소유자가 현재 보유하고 있는 자산(stake) 양에 비례하여 블록을 생성할 권한을 더 많이 부여되는 방식이다. 참여에 대한 보상은 이자와 같은 방식으로 코인이 지급되며, 일정 수 이상의 코인을 보관하고 있는 지갑을 블록체인 네트워크에 연결시켜놓기만 하면 보

상을 받을 수 있다.
오답 체크
(1), (4) 합의란 다수의 참여자들이 통일된 의사결정을 하기 위해 사용하는 알고리즘을 말한다.
(2) 위임 지분증명은 암호화폐 소유자들이 각자의 지분율에 비례하여 투표권을 행사하여 자신의 대표자를 선정하고, 이 대표자들끼리 합의하여 의사결정을 내리는 합의 알고리즘이다.

25. 유닉스나 리눅스 파일 설정 권한 중에서 일반 사용자가 실행 시 일시적으로 관리자(root)의 권한으로 실행되도록 함으로써 시스템의 보안에 허점을 초래할 수 있는 것으로 옳은 것은?
① SetGID
② SetUID
③ Sticky Bit
④ touch
정답 체크
(2) 8진수로 4000으로 표현한다. 사용자가 실행 파일의 사용자 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.
오답 체크
(1) 8진수로 2000으로 표현한다. 사용자가 실행 파일의 그룹 권한을 가지도록 한다. 사용자가 어떤 일을 수행하기 위해 일시적으로 권한 상승을 하기 위해 사용한다.
(3) 8진수로 1000으로 표현한다. 디렉토리에 sticky bit가 설정되면 디렉토리 안의 파일들은 파일 소유자, 디렉토리 소유자 또는 관리자(root)만이 수정하거나 삭제할 수 있다.
(4) 파일의 접근이나 타임스탬프의 형식을 변경하는 데 사용되는 표준 유닉스 프로그램이다. 또한 이것은 새로운 빈 파일을 만드는 데 사용된다.