# 2017-국가직(추가)-정보보호론-나형-해설-곽후근

1. AES(Advanced Encryption Standard)에 대한 설명으로 옳지 않은 것은?
① 128, 192, 256비트 길이의 키를 사용할 수 있다.
② Feistel 구조를 사용한다.
③ 128비트 크기의 블록 대칭키 암호 알고리즘이다.
④ 미국 NIST(National Institute of Standards and Technology)의 공모에서 Rijndael이 AES로 채택되었다.
정답 체크)
(2) Feistel 구조는 DES에서 사용하고, AES는 SPN 구조를 사용한다.
오답 체크)
(1) 128/192/256비트 키를 사용하고, 이는 라운드 수(10/12/14)와 연관을 가진다.
(3) AES의 블록 크기는 128비트이다.
(4) 최종 후보는 MARS, RC6, Rijndael, Serpent, Twofish이다.

2. 다음 설명에 해당하는 악성 소프트웨어를 옳게 짝지은 것은?

| |
|---|
| ㄱ. 시스템 및 응용 소프트웨어의 취약점을 악용하거나 전자우편 또는 공유 폴더를 이용하며, 네트워크를 통해서 컴퓨터에서 컴퓨터로 빠르게 전파된다.<br>ㄴ. 사용자 컴퓨터 내에서 자신 또는 자신의 변형을 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다.<br>ㄷ. 겉으로 보기에는 유용해 보이지만 정상적인 프로그램 속에 숨어있는 악성 소프트웨어로, 사용자가 프로그램을 실행할 때 동작한다. |

| | ㄱ | ㄴ | ㄷ |
|---|---|---|---|
| ① | 웜 | 바이러스 | 트로이목마 |
| ② | 바이러스 | 웜 | 봇 |
| ③ | 바이러스 | 웜 | 트로이목마 |
| ④ | 웜 | 바이러스 | 봇 |

정답 체크)
(1)
웜 : 인터넷 또는 네트워크를 통해서 컴퓨터에서 컴퓨터로 전파되는 악성 프로그램이다. 윈도우의 취약점 또는 응용 프로그램의 취약점을 이용하거나 이메일이나 공유 폴더를 통해 전파되며, 최근에는 공유 프로그램(P2P)을 이용하여 전파되기도 한다. 바이러스와 달리 스스로 전파되는 특성이 있다.
바이러스 : 사용자 컴퓨터(네트워크로 공유된 컴퓨터 포함) 내에서 사용자 몰래 프로그램이나 실행 가능한 부분을 변형해 자신 또는 자신의 변형을 복사하는 프로그램이다. 가장 큰 특성은 복제와 감염이다. 다른 네트워크의 컴퓨터로 스스로 전파되지는 않는다.
트로이목마 : 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 형태이다.
오답 체크)
(2), (3), (4)
봇 : DDoS에서 전파되는 악성코드를 봇(Bot)이라고 한다.

3. 메일 수신 서버 또는 웹 메일 서버로부터 전자우편 메시지를 자신의 컴퓨터 단말 장치로 전송받는 데 사용되는 프로토콜이 아닌 것은?
① IMAP(Internet Mail Access Protocol)
② RTP(Realtime Transport Protocol)
③ POP(Post Office Protocol)
④ HTTP(HyperText Transfer Protocol)
정답 체크)
(2) 실시간으로 음성이나 동화상을 송수신하기 위한 전송 계층 통신 규약이다. RFC 1889에 RTCP(RTP control protocol)와 함께 규정되어 있다. 자원 예약 프로토콜(RSVP)과는 달리 라우터 등의 통신망 기기에 의지하지 않고 단말 간에 실행되는 것이 특징이다. RTP는 보통 사용자 데이터그램 프로토콜(UDP)의 상위 통신 규약으로 이용된다.
오답 체크)
(1) 메일 클라이언트가 메일 서버로부터 메일을 받을 때 사용하는데, 메일 서버에 메일 사본을 저장한다.
(3) 메일 클라이언트가 메일 서버로부터 메일을 받을 때 사용하는데, 메일 서버에 메일 사본을 저장하지 않는다.
(4) 별도의 메일 클라이언트와 메일 서버를 사용하지 않고, 웹 브라우저와 웹 서버를 이용해서 메일을 전송하고 확인하는 방식이다(예 : 네이버 메일 또는 구글 메일).

4. 컴퓨터 보안의 형식 모델에 대한 설명으로 옳은 것은?
① Bell-LaPadular 모델은 다중 수준 보안에서 높은 수준의 주체가 낮은 수준의 주체에게 정보를 전달하는 것을 다루기 위한 것이다.
② Biba 모델은 데이터 무결성을 위한 것으로, 사용자 자신과 같거나 자신보다 낮은 무결성 수준의 데이터에만 쓸 수 있고, 자신과 같거나 자신보다 높은 무결성 수준의 데이터만 읽을 수 있도록 한 것이다.
③ Bell-LaPadular 모델은 이해 충돌이 발생할 수 있는 상업용 응용프로그램을 위해 개발되었으며, 강제적 접근 개념을 배제하고 임의적 접근 개념을 이용한 것이다.
④ Clark-Wilson 모델은 강력한 기밀성 모델을 제안하며, 데이터 및 데이터를 조작하는 트랜잭션에 높은 수준의 기밀성을 제공한다.
정답 체크)
(2) Biba 모델은 No Read Down, No Write Up 특성을 가진다.
오답 체크)
(1) BLP 모델의 보안 정책은 정보가 높은 레벨에서 낮은 레벨로 흐르는 것을 방지한다.
(3) 이해 충돌은 만리장성 모델에서 사용하는 개념이고, BLP 모델은 MAC 개념을 이용한다.
(4) Clark-Wilson 모델은 무결성 모델이다.

5. 개인정보 보호법 제24조의2(주민등록번호 처리의 제한)에서 개인정보처리자가 주민등록번호를 처리할 수 있도록 허용하는 경우는?
① 정보주체에게 별도로 동의를 받은 경우
② 시민단체에서 주민등록번호 처리를 요구한 경우
③ 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경

우
④ 개인정보처리자가 주민등록번호 처리가 불가피하다고 판단한 경우
정답 체크)
(3) 제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.
- 1. 법률 · 대통령령 · 국회규칙 · 대법원규칙 · 헌법재판소규칙 · 중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
- 2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
- 3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 행정안전부령으로 정하는 경우
오답 체크)
(1) 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.
- 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
- 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
(2), (4) 다른 경우에도 해당 법률 규정은 존재하지 않는다.

6. TCP 표준을 준수하는 서버의 열린 포트와 닫힌 포트를 판별하기 위한 TCP FIN, TCP N ULL, TCP Xmas 포트 스캔 공격 시, 대상 포트가 닫힌 경우 세 가지 공격에 대하여 동일하게 서버가 응답하는 것은?
① SYN/ACK
② RST/ACK
③ RST
④ 응답 없음
정답 체크)
(3) 대상 포트가 닫힌 경우 RST 패킷을 보낸다.
오답 체크)
① TCP Half Open에서 열린 경우의 응답이다.
② TCP Half Open에서 닫힌 경우의 응답이다.
④ 대상 포트가 열린 경우 어떤 응답도 하지 않는다.

7. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?
① 신용 카드를 이용한 인터넷 상의 전자결제를 안전하게 할 수 있게 하는 기술이다.
② 대칭키 암호화 방식과 공개키 암호화 방식이 모두 사용된다.
③ 신용 카드 정보를 판매자가 알 수 있도록 단일 서명 방식을 사용한다.
④ 신용조회 네트워크와 인터넷 사이에 설치된 지불 게이트웨이가 지불 명령을 처리한다.
정답 체크)
(3) 이중 서명 방식을 사용한다. 구매 정보와 결제 정보의 해시 값에 각각 서명하고, 이 둘을 묶은

해시 값에 다시 서명한다.
오답 체크)
(1) 자상거래 당사자들에게 신뢰성과 안전성을 제공하기 위하여 인증, 비밀성 등의 보안 기능과 지불 기능을 제공하는 전자상거래 전용 프로토콜이다.
(2) 하이브리드 암호화 방식을 사용한다. 메시지를 대칭키로 암호화하고, 대칭키를 공개키로 암호화한다.
(4) 지불 게이트웨이(payment gateway)를 가진다.

8. UNIX 시스템의 특수 접근 권한에 대한 설명으로 옳은 것은?
① getuid는 접근 권한을 출력하거나 변경한다.
② setgid는 파일 소유자의 권한을 지속적으로 사용자에게 부여한다.
③ setuid가 설정된 파일은 파일 사용자의 권한으로 실행된다.
④ sticky bit가 설정된 디렉터리에 있는 파일은 소유자 외 다른 일반 사용자에 의해 삭제되지 않는다.
정답 체크)
(4) 디렉토리 소유자나 파일 소유자 또는 슈퍼 유저가 아닌 사용자들은 파일을 삭제하거나 이름을 변경하지 못하도록 막는다. 파일 또는 디렉토리 생성은 누구나 할 수 있다(공유 모드).
오답 체크)
(1) 접근 권한을 출력하거나 변경하는 것이 아닌 현재 프로세스의 실제 유저 아이디를 얻어온다.
(2) 유효 그룹(EGID)를 사용자의 실제 그룹 ID(RGID)에서 파일 소유자의 그룹 ID로 변경한다. 소유자 권한이 아니 소유자의 그룹 권한을 부여한다.
(3) 실 사용자(프로그램을 실제 실행 중인 사용자)에서 프로그램 소유자의 ID로 유효 사용자(EUID)가 변경된다. 즉, 설정된 파일은 파일 소유자의 권한으로 실행된다.

9. 다음에 열거된 순서대로 진행되는 공격은?

| |
|---|
| ○ 취약점이 존재하는 웹 서버의 애플리케이션에 악성 코드를 삽입 |
| ○ 해당 웹 서비스 사용자가 공격자가 작성하여 저장한 악성 코드에 접근 |
| ○ 웹 서버는 사용자가 접근한 악성 코드가 포함된 게시판의 글을 사용자에게 전달 |
| ○ 사용자 브라우저에서 악성스크립트가 실행 |
| ○ 실행 결과가 공격자에게 전달되고 공격자는 공격을 종료 |

① 저장(stored) Cross-Site Scripting
② 반사(reflected) Cross-Site Scripting
③ 명령어 삽입(command injection)
④ SQL 삽입(injection)
정답 체크)
(1) 웹 사이트의 게시판, 사용자 프로필 및 코멘트 필드 등에 악성 스크립트를 삽입해 놓으면, 사용자가 사이트를 방문하여 저장되어 있는 페이지에 정보를 요청할 때, 서버는 악성 스크립트를 사용자에게 전달하여 사용자 브라우저에서 스크립트가 실행되면서 공격한다.
오답 체크)
(2) 웹 애플리케이션의 지정된 변수를 이용할 때 발생하는 취약점을 이용하는 것으로, 검색 결과, 에러 메시지 등 서버가 외부에서 입력받은 값을 받아 브라우저에게 응답할 때 전송하는 과정에서 입력

되는 변수의 위험한 문자를 사용자에게 그대로 돌려주면서 발생한다.
(3) 공격자의 코드를 프로그램에 추가하여 실행 순서를 공격자가 원하는 데로 바꾸는 공격 방법이다 (코드 삽이라고도 불림). SQL, LDAP, XML, NoSQL, SMTP 등에서 발생하고, 퍼징(fuzzing) 등을 이용하면 해당 취약점을 발견할 수 있다.
(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.

10. 정보보호 관련 법률에서 규정한 인증 제도에 대한 설명으로 옳지 않은 것은?
① 정보보호 관리체계 인증은 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 과학기술 정보통신부장관이 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호 조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 정해진 기준에 적합한지에 관하여 인증할 수 있도록 한 것이다.
② 개인정보보호 관리체계 인증은 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 상 방송통신위원회가 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립·운영하고 있는 자에 대하여 정해진 기준에 적합한지에 관하여 인증을 할 수 있도록 한 것이다.
③ 정보보호제품 평가·인증은 정보통신기반 보호법 상 행정안전부장관이 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호 시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있도록 한 것이다.
④ 개인정보보호 인증은 개인정보 보호법 상 행정안전부장관이 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 같은 법에 부합하는지 등에 관하여 인증할 수 있도록 한 것이다.
정답 체크)
(3) 국가정보화기본법 제38조(정보보호시스템에 관한 기준 고시 등) ① 과학기술정보통신부장관은 관계 기관의 장과 협의하여 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하여 고시하고, 정보보호시스템을 제조하거나 수입하는 자에게 그 기준을 지킬 것을 권고할 수 있다.
오답 체크)
(1) 정보통신망법 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.
(2) 정보통신망법 제47조의3(개인정보보호 관리체계의 인증) ① 방송통신위원회는 정보통신망에서 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위하여 필요한 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계(이하 "개인정보보호 관리체계"라 한다)를 수립 · 운영하고 있는 자에 대하여 제2항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.
(4) 개인정보 보호법 제32조의2(개인정보 보호 인증) ① 행정안전부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.

11. 보안의 3대 요소 중 가용성에 대한 직접적인 위협 행위는?

① 트래픽 분석(traffic analysis)
② 신분 위장(masquerading)
③ 패킷 범람(packet flooding)
④ 데이터 변조(modification)
정답 체크)
(3) 패킷 범람은 DoS(서비스 거부) 공격이고, DoS 공격은 가용성을 위협한다.
오답 체크)
(1) 트래픽 분석은 기밀성을 위협한다.
(2) 신분 위장은 무결성을 위협한다.
(4) 데이터 변조는 무결성을 위협한다.

12. Diffie-Hellman 키 교환 알고리즘에 대한 설명으로 옳은 것은?
① 두 사용자가 메시지 암호화에 사용할 공개키를 안전하게 교환하기 위한 것이다.
② 중간자(MITM) 공격에 안전하다.
③ 키를 교환하는 두 사용자 간의 상호 인증 기능을 제공한다.
④ 이산대수 문제를 푸는 것이 어렵다는 점을 활용한 것이다.
정답 체크)
(4) $g^x$ mod p, g, p를 알고 있는 상황에서 x를 구할 수 없다는 사실(이산대수 문제)에 기반한다.
오답 체크)
(1) 두 사용자가 메시지 암호화에 사용할 비밀키를 안전하게 교환하기 위한 것이다.
(2) Diffie-Hellman은 중간자 공격이 가능하다(상대방 난수의 진위를 파악할 수 없음).
(3) 키를 교환하는 것은 두 사용자 간의 기밀성 기능을 제공한다. (비밀키를 서로 공유했으므로 상호 인증이 안되는 것은 아니라 가장 맞는 답은 아니다)

13. 인증 기관에서 사용자에게 발급한 인증서의 생성 방법에 대한 설명으로 옳은 것은?
① 사용자의 공개키를 포함한 인증 정보를 인증 기관의 공개키로 암호화 한다.
② 사용자의 개인키를 포함한 인증 정보를 인증 기관의 개인키로 암호화 한다.
③ 사용자의 공개키를 포함한 인증 정보를 인증 기관이 자신의 개인키로 서명한다.
④ 사용자의 공개키를 포함한 인증 정보를 인증 기관의 독자적인 해시 함수로 해시한다.
정답 체크)
(3) 사용자(밥)의 공개키를 포함한 인증 정보를 인증 기관(트렌트)이 자신의 개인키로 서명한다.

14. 전송할 메시지에서 메시지 무결성 검증을 위한 고정 크기의 출력물을 만드는 방법으로 적합한 것만을 고른 것은?
① 난수 생성기, 코덱
② 메시지 인증 코드 생성기, 코덱
③ 의사 난수 생성기, 해시 함수
④ 메시지 인증 코드 생성기, 해시 함수
정답 체크)
(4) MAC(메시지 인증 코드)는 인증과 무결성을 제공한다. 그리고 해시 함수는 무결성을 제공한다.
오답 체크)

(1) 난수 생성기는 실제 난수를 생성하고, 대칭키(기밀성) 등에 이용되지만 잘 사용되지는 않는다(만들기가 어려움). 코덱은 압축을 하는데 사용한다(굳이 분류하자면 기밀성).
(2) 코덱은 압축을 하는데 사용한다(굳이 분류하자면 기밀성).
(3) 의사 난수 생성기는 소프트웨어적으로 의사 난수를 생성하고, 대칭키(기밀성) 등에 이용된다.

15. 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 제52조에 의거하여 정부가 정보통신 망의 고도화(정보통신망의 구축·개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송 통신과 관련한 국제 협력·국외 진출 지원을 효율적으로 추진하기 위하여 설립한 기관 은?
① 방송통신위원회
② 한국인터넷진흥원
③ 한국정보화진흥원
④ 정보통신산업진흥원
정답 체크)
(2) 정보통신망법 제52조(한국인터넷진흥원) ① 정부는 정보통신망의 고도화(정보통신망의 구축 · 개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력 · 국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)을 설립한다.
오답 체크)
(1) 방통위법 제3조(위원회의 설치) ① 방송과 통신에 관한 규제와 이용자 보호 등의 업무를 수행하기 위하여 대통령 소속으로 방송통신위원회(이하 "위원회"라 한다)를 둔다.
(3) 국가정보화 기본법 제14조(한국정보화진흥원의 설립 등) ① 과학기술정보통신부장관과 행정안전부장관은 국가기관등의 국가정보화 추진과 관련된 정책의 개발과 건강한 정보문화 조성 및 정보격차 해소 등을 지원하기 위하여 한국정보화진흥원(이하 "정보화진흥원"이라 한다)을 설립한다.
(4) 정보통신산업 진흥법 제26조(정보통신산업진흥원의 설립 등) ① 정보통신산업을 효율적으로 지원하기 위하여 정보통신산업진흥원(이하 "산업진흥원"이라 한다)을 설립한다.

16. 쿠키에 대한 설명으로 옳지 않은 것은?
① 웹 사이트 접속 시 HTTP의 무상태성(statelessness)을 보완하기 위해 사용되는 정보이다.
② 사용자가 웹 사이트에 접속할 때 사용자 컴퓨터에서 생성되어 해당 웹 서버에 임시 파일로 전송·저장된다.
③ 보존 기간에 따라 임시(또는 세션) 쿠키와 영구(persistent) 쿠키로 분류 할 수 있다.
④ 사용자가 인식하지 못하는 사이에 사용자의 다양한 정보가 쿠키에 담겨 웹 서버로 전송 될 수 있기 때문에 개인정보에 대한 피해가 발생할 수 있다.
정답 체크)
(2) 사용자가 웹 사이트에 접속할 때 사용자 컴퓨터에서 생성되어 사용자 컴퓨터에 저장되는 파일이다.
오답 체크)
(1) 특정 사이트를 처음 방문하면 아이디와 비밀번호를 기록한 쿠키가 만들어지고 다음에 접속했을 때 별도 절차 없이 사이트에 빠르게 연결할 수 있다(무상태를 보완). 여기서, 무상태란 웹 사이트 방문 후 연결을 끊으면 어떤 정보도 남지 않음을 의미한다.
(3) 세션 쿠키(세션 유지용)는 웹 브라우저는 나가거나 컴퓨터를 종료하면 삭제되고, 영구 쿠키(사용자 상태 유지용)는 쿠키를 삭제하지 않는 한 유지된다.

(4) 쿠키에는 다양한 정보(ID/PW, 접근 기록 등)가 있고, 클라이언트가 서버에 접속할 때 쿠키를 전송하므로 서버에서 해당 쿠키를 볼 수 있다(개인정보에 대한 피해).

17. 동일 LAN 상에서 서버와 클라이언트의 IP 주소에 대한 2 계층 MAC 주소를 공격자의 MAC 주소로 속임으로써, 공격자가 서버와 클라이언트 간의 통신을 엿듣거나 통신 내용 또는 흐름을 왜곡 시킬 수 있다. 이러한 상황에서 발생한 공격과 거리가 먼 것은?
① IP 스푸핑(spoofing)
② ARP 스푸핑(spoofing)
③ 스니핑(sniffing)
④ MITM(Man-In-The-Middle)
정답 체크)
(1) 트러스트(Trust)로 접속하고 있는 클라이언트에 DoS 공격을 수행해 클라이언트가 사용하는 IP가 네트워크에 출현하지 못하도록 한 뒤, 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 이루어진다.
오답 체크)
(2) 문제의 설명은 ARP spoofing으로 근거리 통신망(LAN) 하에서 주소 결정 프로토콜(ARP) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 공격 기법이다. 즉, 공격자가 가짜 MAC 주소를 서버와 클라이언트에게 알려준다.
(3) ARP spoofing을 하는 이유는 sniffing을 하기 위해서이다.
(4) ARP spoofing은 전형적인 중간자 공격(MITM) 기법이다.

18. ISO 27001:2013의 통제 항목에 해당하지 않는 것은?
① 정보보호 정책(information security policy)
② 자산 관리(asset management)
③ 모니터링과 검토(monitoring and review)
④ 정보보호 사고관리(information security incident management)
정답 체크)
(3) 해당 항목은 ISO 27001:2013의 요구 사항에 해당한다(통제 항목이 아님).
오답 체크)
(1), (2), (4) ISO/IEC 27001:2013 개정판에서는 프로세스 부분인 PDCA가 삭제되고 기존 ISO/IEC 27001:2005의 통제항목 11개 영역 137개에서 통제항목 14개 영역 114개로 개정되었다.

19. RSA 암호 시스템에서 어떤 사용자의 공개키를 {e, n}이라 할 때, 평문 블록 M과 암호문 블록 C는 수식, $C = M^e \bmod n$을 만족한다. n을 두 소수 11과 13의 곱이라 할 때, e로 선택할 수 있는 것만을 모두 고른 것은?

| ㄱ. 9 | ㄴ. 1 7 | ㄷ. 19 | ㄹ . 127 |
|---|---|---|---|

① ㄴ, ㄷ
② ㄱ, ㄴ, ㄷ
③ ㄴ, ㄷ, ㄹ
④ ㄱ, ㄴ, ㄷ, ㄹ
정답 체크)

(1) 키 쌍을 생성하는 과정은 아래의 Tip을 참고한다.
n = p x q -〉 p = 11, q = 13
L = lcm(p-1, q-1) = lcm(10, 12) = 60(최신 버전) 또는 L = (p-1)x(q-1) = 10x12 = 120(처음 버전, 공무원 시험에서 계산되는 방식)
1 〈 E 〈 60 또는 120, gcd(E, L) = 1
(ㄴ) 17 -〉 조건에 만족
(ㄷ) 19 -〉 조건에 만족
오답 체크)
(2), (3), (4)
(ㄱ) 9 -〉 gcd(E, L) = 1이라는 조건에 만족하지 않음(3이라는 공약수가 존재)
(ㄹ) 127 -〉 1 〈 E 〈 60 또는 120이라는 조건에 만족하지 않음

20. 클라이언트와 서버 간의 파일 전송을 위한 FTP(File Transfer Protocol)에 대한 설명으로 옳지 않은 것은?
① TCP 포트 21은 제어 연결을 위해, TCP 포트 20은 데이터 연결을 위해 사용된다.
② 공개 파일 접근을 허용하는 사이트에서는 익명(anonymous) 로그인을 사용할 수 있으나, 익명 사용자에게는 보안상 제한적인 명령어만 사용하도록 한다.
③ 로그인 시 사용자 아이디와 패스워드를 사용하더라도 로그인 정보 도청이 가능하다.
④ FTP 대신에 TELNET를 사용함으로써 인증과 무결성의 보안 문제를 해결할 수 있다.
정답 체크)
(4) TELNET은 인증과 무결성 문제를 해결할 수 없고 파일 전송도 할 수 없다. TELNET 대신에 SSH를 사용해야 한다.
오답 체크)
(1) FTP는 다른 프로토콜과 다르게 2개의 포트를 사용한다. 하나는 제어용(21번 포트)이고, 나머지 하나는 데이터용(20번 포트)이다.
(2) 익명 로그인을 이용하여 FTP 임에도 불구하고 ID/PW를 사용하지 않아도 된다.
(3) FTP는 암호화가 안되어 있기 때문에 ID/PW에 대한 도청이 가능하다.