2017년 국가직 생활안전분야 9급 정보보호론 풀이

by 호이호이꿀떡

정답 체크

01	02	03	04	05	06	07	08	09	10
②	①	②	②	③	③	③	④	①	③
11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
③	④	③	④	②	②	①	③	①	④

문 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.

답 ②

② AES 암호화는 SPN 구조이다.

◈ **AES**(Advanced Encryption Standard)
SPN구조
블록 128비트(16바이트)
키 길이 128비트 - 10라운드
키 길이 192비트 - 12라운드
키 길이 256비트 - 14라운드

문 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.
ㄴ. 사용자 컴퓨터 내에서 자신 또는 자신의 변형을 다른 실행 프로그램에 복제하여 그 프로그램을 감염시킨다.
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

답 ①

ㄱ. **웜**(Worm)
시스템에 직접적인 영향은 미치지 않는 악성 프로그램이다. 다른 파일에 기생하지 않고, 스스로 자가 복제하며 네트워크를 통해 전파되는 성질을 가졌다.
ㄴ. **바이러스**(Virus)
스스로를 복제하여 컴퓨터를 감염시켜 피해를 주는 악성 프로그램으로, 한 시스템에서 다른 시스템으로 전파되는 성질이 있다.
ㄷ. **트로이목마**(Trojan Horse)
정상적인 프로그램으로 가장한 악성 프로그램으로, 다른 시스템으로 전파되지는 않는다. 트로이목마는 보통 해커들이 대상 컴퓨터의 인증이나 백신을 우회하여 시스템 내부에 침투하기 위해 사용한다.

문 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

답 ②

② **RTP**(Real-time Transport Protocol, 실시간 전송 프로토콜)
IP 네트워크를 통해 오디오와 비디오를 전달하기 위한 표준화된 패킷 포맷을 정의한 프로토콜로, 스트리밍 미디어를 포함한 커뮤니케이션 및 엔터테인먼트 시스템에 널리 쓰이고 있다.

<오답 체크> ① **IMAP**(Internet Message Access Protocol, 인터넷 메시지 접속 프로토콜)
전자메일 수신 프로토콜, 읽어도 삭제되지 않음, 다운 여부 본인이 결정

③ **POP3**(Post Office Protocol)
전자메일 수신 프로토콜, 읽으면 자동 삭제 자동 다운

④ **HTTP**(HyperText Transfer Protocol)
HTTP는 클라이언트와 서버 사이에 이루어지는 요청/응답(request/response) 프로토콜로, WWW 상에서 정보를 어떻게 주고받을지 정의한 통신 규약이다. HTML을 기본으로 이미지, 동영상 등 거의 모든 데이터를 주고받는 데 쓰이며, TCP와 UDP를 사용하며, 80번 포트를 사용한다.
HTTP가 인터넷 표준 이메일 프로토콜은 아니다. 하지만, 웹 브라우저를 통해 자신의 메일함에 액세스하고, 인터넷 상에서 데이터를 주고받기 위해서는 HTTP 프로토콜이 사용되기 때문에 답이 되지 않는다.

문 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.

답 ②

② **Biba**(비바) 모델
무결성을 중시한 모델
높은 등급의 데이터에 쓸 수 없고, 낮은 등급의 데이터를 읽을 수 없다.
단순 무결성 속성 - NRD(No Read Down)
무결성 star(*) 속성 - NWU(No Write Up)

<오답 체크> ① **BLP**(Bell-Lapadula, 벨 라파듈라) 모델
기밀성을 중시한 모델, 높은 수준의 데이터가 낮은 수준으로 이동하여 유출되는 것을 방지하기 위한 모델이다.
따라서 높은 등급의 데이터를 못 읽고, 낮은 등급에 쓸 수 없다.
단순 보안 속성 – NRU(No Read Up)
Star(*) 속성 – NWD(No Write Down)

③ **Chineses Wall**(만리장성) 모델
서로 상충관계에 있는 객체간의 정보 접근을 통제하는 모델. 이익의 충돌이 많이 발생하는 금융, 회계, 투자, 광고 등의 분야에서 주로 사용된다.

④ **Clark-Wilson**(클락-윌슨) 모델은 기밀성이 아니라, 무결성 중심의 상업적 모델이다.
트랜잭션의 내·외부적 일관성 유지(Well-formed transaction), 직무 분리(Separation of duties), 프로그램을 통해서만 객체에 접근 가능의 특성을 가진다.

문 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 경우
④ 개인정보처리자가 주민등록번호 처리가 불가피하다고 판단한 경우

답 ③

「개인정보 보호법」 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

문 6. TCP 표준을 준수하는 서버의 열린 포트와 닫힌 포트를 판별하기 위한 TCP FIN, TCP NULL, 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

답 ③

③ **Stealth Scan**(스텔스 스캔)은 세션 연결을 완전히 성립하지 않은 상태로 공격 대상 시스템의 포트 활성화 여부를 스캔하는 것으로, 세션 연결이 성립되지 않은 상태이기 때문에 공격 대상 시스템에 로그가 남지 않는다. 따라서 공격 대상의 시스템 관리자는 어떤 IP를 가진 공격자가 자신의 시스템을 스캔했는지 확인할 수 없다.
스텔스 스캔의 종류에는 TCP FIN, Xmas Tree, NULL scan 등이 있다.
TCP FIN 스캔은 TCP flag의 FIN을 활성화 하여 대상 포트로 패킷을 전송하고, Xmas Tree 스캔은 TCP flag의 FIN, URG, PUSH을 활성화 하여 대상 포트로 패킷을 전송한다. NULL 스캔은 TCP flag를 모두 비활성화 하여 대상 포트로 패킷을 전송한다.
스텔스 스캔은 포트가 열려있을 때는 아무 응답이 오지 않고, 포트가 닫혀있을 때는 RST 패킷이 전송되어 온다.

<오답 체크> ①② TCP half 스캔에서의 응답이다.
TCP half 스캔의 시작은 일반 OPEN스캔과 같으나, 마지막에 서버의 활성화 여부만 확인한 뒤 바로 RST 패킷을 보내 즉시 세션을 끊는 스캔 방법이다.
공격자는 공격 대상 시스템에 SYN 패킷을 보내는데, 포트가 열려있을 경우 SYN/ACK 응답이 오며 공격자는 응답을 받자마자 RST 패킷을 보내 즉시 연결을 끊는다.
포트가 닫혀있을 경우에는 공격 대상 시스템으로부터 RST/ACK 응답이 온다.

문 7. SET(Secure Electronic Transaction)에 대한 설명으로 옳지 않은 것은?

① 신용카드를 이용한 인터넷상의 전자결제를 안전하게 할 수 있게 하는 기술이다.
② 대칭키 암호화 방식과 공개키 암호화 방식이 모두 사용된다.
③ 신용카드 정보를 판매자가 알 수 있도록 단일 서명 방식을 사용한다.
④ 신용조회 네트워크와 인터넷 사이에 설치된 지불 게이트웨이가 지불 명령을 처리한다.

답 ③

③ SET는 **이중 서명**(Dual Signature) 방식을 사용한다. 상품 주문정보와 결제정보를 각각 암호화하는 서명 방식으로, 은행에는 상품 주문정보를 숨기고, 상인에게는 결제정보를 숨기는 역할을 해준다.
고객이 결제 정보를 상인에게 보낼 때 주문정보는 상인의 공개키를 이용해 암호화하여 은행은 보지 못하게 하고, 지불정보는 은행의 공개키를 이용 암호화하여 상인이 보지 못하게 한다.

<오답 체크> ① SET는 비자와 마스터가 함께 개발한 전자 상거래 거래 프로토콜이다.
② SET은 하이브리드 암호화 방식을 지원한다. 메시지를 암호화하기 위해 세션키를 이용한 대칭키 암호화 알고리즘을 사용하며, 세션키를 분배하기 위해 RSA 공개키 암호화 알고리즘을 사용한다.
④ **지불 게이트웨이**(Payment Gateway), 지불 중계기관
가맹점 및 다양한 금융시스템의 거래 사이에서 중재자 역할을 하는 기관이다. 판매자로부터 카드정보 결제 요청을 받아 금융기관에 승인 및 결제를 요청한다.

문 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.

답 ④

④ 스티키 비트(Sticky Bit)가 설정된 디렉터리에는 누구나 접근 가능하고 파일을 생성할 수 있지만,(파일은 생성한 사람이 소유자가 된다) 파일을 삭제하거나 변경하는 건 소유자나 관리자만 가능하다. 즉, 다른 사람은 자신의 소유가 아닌 파일은 삭제할 수 없으므로, 공유 디렉터리로 쓰고자 할 때 설정한다.

<오답 체크> ① geteuid()는 현재 프로세스의 유효 유저 아이디(effective user ID)를 출력하는 명령어이다.
접근 권한은 파일의 정보를 보여주는 'stat' 명령어를 통해 확인할 수 있고, 접근 권한을 변경하는 명령어는 'chmod' 명령어이다.
②③ 파일에 setuid(Set UserID)가 설정되어 있으면, 사용자는 해당 파일을 실행하는 동안 그 파일의 소유자(user)의 권한을 가지게 된다.
만약 프로그램의 소유자가 관리자라면 프로그램 사용자는 소유자인 관리자 권한을 얻게 되고, 악의를 가진 사용자는 이렇게 획득한 관리자 권한을 통해 여러 악의적인 동작을 수행할 수 있다.
이와 유사하게 setgid(Set GroupID) 설정은, 해당 파일을 실행하는 동안 사용자는 그 파일의 그룹(group)의 권한을 가지게 된다.

문 9. 다음에 열거된 순서대로 진행되는 공격은?

○ 취약점이 존재하는 웹 서버의 애플리케이션에 악성 코드를 삽입
○ 해당 웹 서비스 사용자가 공격자가 작성하여 저장한 악성코드에 접근
○ 웹 서버는 사용자가 접근한 악성코드가 포함된 게시판의 글을 사용자에게 전달
○ 사용자 브라우저에서 악성 스크립트가 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)

답 ①

① **XSS**(Cross-site Scripting, 크로스 사이트 스크립팅)는 웹 사이트에 악성 스크립트를 삽입한 뒤 다른 사용자의 접근을 유도하여, 사용자의 클라이언트에서 악성 프로그램이 실행되도록 하여 개인정보를 유출시키는 공격이다.
XSS 공격은 저장 XSS 공격과 반사 XSS 공격이 있다.
저장 XSS 공격(Stroed XSS)은 웹 서버에 악성 스크립트를 영구적으로 저장해 놓는 공격 방법으로, 웹 사이트의 게시판, 사용자 프로필 및 코멘트 필드 등에 악성 스크립트를 삽입해 놓는다. 사용자가 사이트를 방문하여 저장되어 있는 페이지에 접근하면, 서버에 있던 악성 스크립트를 사용자에게 전달되어 사용자 브라우저에서 실행되어 공격한다.
② **반사 XSS 공격**(Reflected XSS)은 사용자에게 악성 URL을 배포하여 사용자가 클릭하도록 유도하여 바로 사용자를 공격하는 방법이다. 공격자는 공격용 악성 URL을 생성한 뒤, 이 URL을 이메일 메세지나 거짓 정보 등 다양한 경로로 사용자들에게 배포한다. 사용자가 이 URL 링크를 클릭하는 순간 바로 악성 스크립트가 사용자의 브라우저에서 실행된다.
③ **명령어 삽입**(Command Injection)
시스템 명령어를 호출하는 애플리케이션의 인자 값을 조작하여 의도하지 않은 시스템 명령어를 실행시키는 공격 기법입니다.
④ **SQL 삽입**(SQL 인젝션, SQL injection)
클라이언트의 입력값을 조작하여 관리자가 예상하지 못한 명령을 실행하거나, 정당한 권한을 획득하지 않고 부정한 방법으로 데이터베이스에 접근하는 공격이다.

문 10. 정보보호 관련 법률에서 규정한 인증 제도에 대한 설명으로 옳지 않은 것은?

① 정보보호 관리체계 인증은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 과학기술정보통신부장관이 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 이용촉진 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.

답 ③

③ 정보보호제품을 평가·인증하고 기준을 정하고 고시하는 자는 행정안전부 장관이 아니라, 과학기술정보통신부 장관이다.

「국가정보화 기본법」
제38조(정보보호시스템에 관한 기준 고시 등) ① **과학기술정보통신부장관**은 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 **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」**
제47조(정보보호 관리체계의 인증) ① **과학기술정보통신부장관**은 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 **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」**
제47조의3(개인정보보호 관리체계의 인증) ① **방송통신위원회**는 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」**
제12조(개인정보 보호지침) ① **행정안전부장관**은 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 "표준지침"이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

문 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)

답 ③

③ 패킷 범람(packet flooding)은 목표 대상 서버에 많은 패킷을 보내 서버를 작동불능 상태에 빠뜨리기 때문에 가용성을 침해하는 행위에 해당한다.
<오답 체크> ① 트래픽 분석(traffic analysis)은 공개하지 않은 정보가 외부로 알려지기 때문에 기밀성 침해에 해당한다.
② 신분 위장(masquerading)은 불법적으로 시스템 접근 권한을 획득하여 정보를 탈취할 경우 기밀성 침해에 해당하고, 정보를 변경할 경우 무결성 침해에 해당하지만, 가용성 침해와는 직접적인 관련이 없다.
④ 데이터 변조(modification)는 공격자 임의대로 데이터를 변경하는 것이므로 무결성 침해에 해당한다.

문 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.

답 ④

④ 디피 헬만 키 교환(Diffie–Hellman key exchange) 알고리즘은 두 송수신자 간 공통의 비밀키(대칭키)를 생성하기 위한 방법으로, 이산대수의 어려움에 기반한 알고리즘이다.
<오답 체크> ① 공개키가 아니라 비밀키(대칭키)를 안전하게 교환하기 위한 것이다.
②③ 통신 상대방을 인증하지 않기 때문에 중간자(MITM) 공격에 취약하다.

문 13. 인증기관에서 사용자에게 발급한 인증서의 생성 방법에 대한 설명으로 옳은 것은?

① 사용자의 공개키를 포함한 인증 정보를 인증기관의 공개키로 암호화한다.
② 사용자의 개인키를 포함한 인증 정보를 인증기관의 개인키로 암호화한다.
③ 사용자의 공개키를 포함한 인증 정보를 인증기관이 자신의 개인키로 서명한다.
④ 사용자의 공개키를 포함한 인증 정보를 인증기관의 독자적인 해시 함수로 해시한다.

답 ③

③ 인증서에는 사용자의 공개키가 포함되어 있다. 개인키는 절대 유출해서는 안 되는 정보이기 때문에 인증서에 포함되지 않는다.
또한 인증서는 인증기관의 개인키로 생성한 서명이 첨부되어 있다. 인증서 이용자는 인증기관의 공개키로 이 서명을 검증하여, 인증서가 위·변조되지 않았다는 것을 확인할 수 있다.

문 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

답 ④

④ 해시 함수(Hash function)는 무결성 검증을 위해 사용하며, 메시지 인증 코드(MAC, Message Authentication Code)는 대칭키를 사용하는 해시값으로, 무결성과 출처 인증(발신지에 대한 인증)이 가능하다.
대부분의 메시지 인증 코드와 해시 함수는 가변 길이의 입력을 받아 고정 길이의 값을 출력한다.

<오답 체크> ①③ 난수(random number)는 무작위로 추출된 문자열을 의미한다. 정보보호론에서 난수는 주로 일회용 세션키나 비밀번호의 솔트(salt)값을 생성하는 데 쓰이므로 기밀성을 보장하기 위해 사용된다고 볼 수 있다.
하지만 보통의 컴퓨터는 진정한 난수를 생성할 수 없으며, 난수보다 의사난수가 더 유용한 경우가 많기 때문에 주로 의사난수를 사용한다.
의사 난수(psudeo random number)는 진정한 의미에서의 난수는 아니지만 그 결과값을 추측하는 건 매우 어렵기 때문에 어느 정도 난수로 취급할 수 있는 문자열을 말한다.

② 코덱(codec)
음성이나 영상 등 데이터 스트림이나 신호를 다른 형식으로 변환(인코딩이나 디코딩, 혹은 둘 다)할 수 있는 하드웨어나 소프트웨어 기술, 알고리즘을 말한다.

문 15. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 의거하여 정부가 정보통신망의 고도화(정보통신망의 구축· 개선 및 관리에 관한 사항을 제외한다)와 안전한 이용 촉진 및 방송 통신과 관련한 국제협력· 국외진출 지원을 효율적으로 추진하기 위하여 설립한 기관은?

① 방송통신위원회
② 한국인터넷진흥원
③ 한국정보화진흥원
④ 정보통신산업진흥원

답 ②

② **「정보통신망 이용촉진 및 정보보호 등에 관한 법률」**
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.

문 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 분류할 수 있다.
④ 사용자가 인식하지 못하는 사이에 사용자의 다양한 정보가 쿠키에 담겨 웹 서버로 전송될 수 있기 때문에 개인정보에 대한 피해가 발생할 수 있다.

답 ②

② 쿠키(Cookie)는 사용자의 하드디스크에 저장된다.(임시 세션 쿠키의 경우 브라우저의 메모리 공간에 저장된다.)

<오답 체크> ① 무상태성(statelessness)란 클라이언트와 서버의 이전 통신 정보가 현재 통신까지 이어지지 않는 특성을 의미한다. 표준 프로토콜인 http는 웹 서버로 들어온 요청에 응답 데이터를 전송하고 나면 그 연결을 끊어버리기 때문에 무상태성의 특성을 갖게 된다.
쿠키를 사용해 사용자의 기본 설정 등의 정보를 저장하여 접속자의 상태를 지속적으로 추적·관리하는 게 가능해진다.

③ **Session Cookie**(세션 쿠키)는 브라우저 프로세스가 실행되고 있을 때까지만 유효한 쿠키로, 현재 연결중인 웹 사이트의 인증 정보를 유지하기 위한 것이다. 메모리 공간에 상주해있다가, 사용자가 브라우저를 종료하면 쿠키는 삭제된다.
Persistent Cookie(영구 쿠키)는 사용자가 웹 사이트 방문했을 때 설정한 정보(팝업창 표시 등)와 인증 정보(ID, Password 등)을 기억해두었다가, 나중에 재방문 시에 빠른 서비스를 제공하기 위한 것으로, 사용자의 하드 디스크에 저장해둔다.

④ 쿠키에는 인터넷 사용자의 개인 정보들이 포함되어 있고 네트워크를 통해 서버로 전송되기 때문에, 공격자에 의해 쿠키를 탈취당할 경우 개인정보가 유출되어 피해를 입을 수 있다.

문 17. 동일 LAN 상에서 서버와 클라이언트의 IP 주소에 대한 2계층 MAC 주소를 공격자의 MAC 주소로 속임으로써, 공격자가 서버와 클라이언트 간의 통신을 엿듣거나 통신 내용 또는 흐름을 왜곡시킬 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)

답 ①

① **IP Spoofing**(IP 스푸핑)은 공격자가 자신의 IP를 다른 사람의 IP로 속여 다른 사람 행세를 하는 것이다. 단말 사이가 IP 주소 기반의 트러스트 관계일 경우 인증 절차를 생략한다는 취약점을 이용한 공격으로, 서비스 거부 공격이나 세션 차단 등의 공격에 사용된다.

<오답 체크> ②③ **ARP Spoofing**(ARP 스푸핑)
공격자가 자신의 MAC 주소를 공격 대상의 MAC 주소로 바꾸어 마치 자신이 공격 대상인 척 속이는 공격으로, 공격 대상자로 보내지는 패킷을 가로채 스니핑을 하는 것이 목적이다.
공격자는 클라이언트와 서버 사이의 패킷을 읽고 확인한 후 정상적인 목적지로 향하도록 다시 돌려보내 연결이 유지되도록 한다.

④ **MITM**(Man-In-The-Middle, 중간자 개입) 공격은 연결하는 두 송수신자 사이에 중간자가 침입하여 한쪽에서 전달된 정보를 도청한 뒤 이를 다른 쪽에 전달하는 공격이다.
ARP 스푸핑을 통한 스니핑을 이용해 중간자 공격이 가능하다.

문 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 사고 관리(information security incident management

답 ③

▶ ISO 27001 영국의 정보보호 관리체계인 BS7799를 국제 표준으로 사용하기 위해 개정한 것으로, 정보보호 경영체계는 비즈니스 목표를 달성하기 위해 조직의 정보보안을 수립하고, 구현하고, 운영하고, 모니터링 및 검토, 유지하고, 지속적인 개선을 위한 요구사항을 규정하고 있다. 14개 통제 영역, 114개 통제 항목으로 구성되어 있다.
③ 모니터링 및 검토가 ISO 27001:2013의 기능에 들어있기는 한데, 통제 항목으로 규정되더 있지는 않다.

◈ ISO 27001:2013의 14개 통제 영역

통제 영역	항목수	내용
정보보안 정책 (Information security policies)	2	정보보호에 대한 경영방침과 지원사항을 제공하기 위함
정보보안 조직 (organizing information security)	7	조직 내에서 보호를 효과적으로 관리하기 위해서는 보호에 대한 책임을 배정
인원 보안 (Human resource policity)	6	사람에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 위험을 감소
자산 관리 (Asset management)	10	조직의 자산에 대한 적절한 보호책 유지
접근 통제 (Access control)	13	정보에 대한 접근통제를 하기 위함
암호화 (Cryptography)	2	기밀성, 인증 또는 정보의 무결성을 보호하기 위해 암호화의 적절하고 효과적인 사용을 보장
물리적 환경적 보안 (Physocal & environmental security)	15	비인가된 접근, 손상과 사업장에 대한 영향을 방지하기 위함
운영 보안 (Operation security)	15	정보처리 설비의 정확하고 안전한 운영을 보장하기 위함
통신 보안 (Communication security)	7	네트워크 및 지원 정보처리 시설의 안전한 통신을 보장하기 위함
시스템 취득, 개발, 유지보수 (System acquisition, development & maintenance)	13	정보시스템 내에 보안이 ㅜ립되었음을 보장하기 위함
협력업체(공급자) 관리 (Supplier relationships)	5	협력업체(공급자)에게 접근가능한 조직 내 정보보호 보장과 협력업체와의 계약에 따라 정보보안 및 서비스 제공에 합의된 수준을 유지하기 위함
보안사고 관리 (Information security incident management)	7	보안사고에 대한 대응 절차의 수립 및 이행을 보장
사업연속성 관리의 정보보안 측면 (Information security aspects of business continuity management)	4	사업활동에의 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요 사업 활동을 보호하기 위함
준거성 (Compliance)	8	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보보흉구사항의 불일치를 방지하기 위함

문 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. 17	ㄷ. 19	ㄹ. 127

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

답 ①

n = p × q 일 때,
오일러의 Totient 함수는 Φ(n) = (p – 1) × (q – 1) 가 된다.
따라서 Φ(n)은 (11 – 1) × (13 – 1) = 120 이다.
e는 Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 정수이므로, 17과 19가 가능하다.
9는 120과 공약수 1, 3을 가지므로 서로소 관계가 아니고, 127은 120보다 크므로 안 된다.

◈ RSA 알고리즘 공개키와 개인키 생성 순서
○ 단계 1: 두 소수 p, q를 선정한다.
○ 단계 2: n = p × q를 계산한다.
○ 단계 3: Φ(n) = (p – 1) × (q – 1)을 계산한다.
(단, Φ(n)은 오일러의 Totient 함수이다.)
○ 단계 4: Φ(n)보다 작고, Φ(n)과 서로소의 관계를 갖는 임의의 e 값을 선택한다.
○ 단계 5: e × d mod Φ(n) = 1의 관계를 갖는 d를 계산한다.
(단, mod는 나머지를 구하는 연산자이다.)
○ 단계 6: (e, n)을 공개키로 하고, (d, n)을 개인키로 한다.

암호문 = $(\text{평문})^e \bmod n$

평문 = $(\text{암호문})^d \bmod n$

문 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.

답 ④

④ TELNET(텔넷)은 원격 접속 프로토콜이며, FTP와 마찬가지로 암호화를 하지 않기 때문에 보안에 취약하다. FTP와 TELNET의 보안 문제를 해결하기 위해서는 SSH(Secure Shell) 등의 보안 프로토콜을 사용한다.
<오답 체크> ② 익명 FTP 사용자는 보통 로그인, 제한적으로 디렉터리 내의 콘텐츠 정열, 디렉토리에서 파일 검색 등의 제한적인 조작만 가능하다. 일반적으로 FTP 서버로 파일을 전송하는 건 허용되지 않는다.
③ FTP 프로토콜은 암호화를 하지 않기 때문에 사용자 인증 정보가 노출될 수 있다. 따라서 보안을 위해서는 TLS 프로토콜과 결합한 FTPS, SSH 프로토콜과 결합한 SFTP를 사용한다.