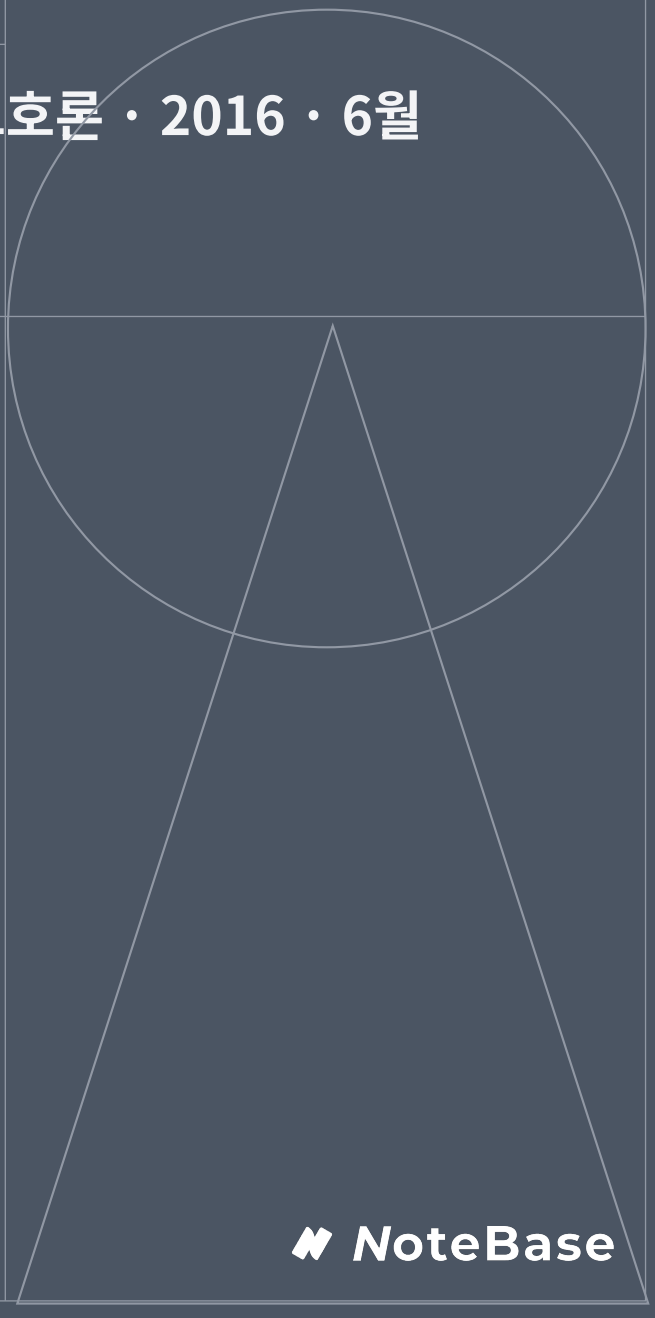
기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2016 · 6월



NoteBase

기출OX 해설집

공무원/서울시/9급 · 정보보호론 · 2016 · 6월

공무원/서울시/9급 · 정보보호론 · 2016 · 6월

문 1. 다음 중 X.509 v3 표준 인증서에 포함되지 않는 것은?

① 인증서의 버전(Version)

② 서명 알고리즘 식별자(Signature Algorithm ID)

③ 유효기간(Validity Period)

④ 디렉토리 서비스 이름(Directory Service Name)

정답 4번

간단한 해설

디렉토리 서비스 이름은 X.509 v3 인증서의 표준 구성 필드가 아니다. 인증서에 들어가는 이름 정보인 발급자(Issuer)와 주체(Subject)는 각각 인증서를 발급한 기관과 인증 대상의 이름을 나타낸다.

선지별 해설

① O: 인증서의 버전(Version)은 **인증서 형식의 버전**을 나타내는 필드이다. v3 인증서에는 v3 형식을 식별하는 버전 정보가 포함되며, v3에서는 확장 필드를 사용할 수 있다.

② O: 서명 알고리즘 식별자(Signature Algorithm ID)는 인증기관이 **인증서에 전자서명할 때 사용한 알고리즘**을 나타낸다. 서명값 자체와는 구별되며, 검증자는 이 정보를 이용해 어떤 알고리즘으로 서명을 검증할지 알 수 있다.

③ O: 유효기간(Validity Period)은 인증서의 **유효 시작 시각(notBefore)과 종료 시각(notAfter)**을 담는다. 인증서 검증 시 현재 시각이 이 구간에 포함되는지 확인한다. 다만 기간 안에 있더라도 폐지된 인증서는 유효한 것으로 인정되지 않으므로 유효기간과 폐지 여부는 별도로 확인한다.

④ X: 디렉토리 서비스 이름(Directory Service Name)은 **표준 인증서의 구성 필드가 아니다**. 인증서의 이름 필드에는 발급자를 나타내는 Issuer와 인증 대상인 주체를 나타내는 Subject가 있다. 이러한 이름 정보와 디렉토리 서비스 자체의 이름을 구별해야 한다.

NoteBase

문 2. 다음 중 성격이 다른 공격 유형은?

① Session Hijacking Attack

② Targa Attack

③ Ping of Death Attack

④ Smurf Attack

정답 1번

간단한 해설

세션 하이재킹은 정상 사용자의 **세션을 가로채 권한을 도용**하는 공격이다. 나머지 공격은 시스템이나 네트워크의 정상 이용을 방해하는 **서비스 거부(DoS)** 공격에 속한다.

선지별 해설

서비스 거부(DoS) 공격은 정상 사용자가 시스템이나 네트워크 서비스를 이용하지 못하게 하여 가용성을 해친다. 각 공격의 주된 목적과 효과를 이 기준으로 비교한다.

① Session Hijacking Attack: 정상 사용자와 서버 사이에 성립한 **세션을 가로채 사용자로 가장**하는 공격이다. 예를 들어 유효한 웹 세션 토큰을 탈취하여 사용하면, 공격자가 해당 사용자의 권한으로 서버에 접근할 수 있다. 핵심은 서비스 중단이 아니라 세션과 권한의 도용이다.

② Targa Attack: 비정상적인 IP 패킷을 이용하여 대상 시스템의 네트워크 처리 취약점을 공격한다. 취약한 시스템을 멈추거나 비정상 종료시켜 **서비스 이용을 방해**하므로 서비스 거부 공격에 속한다.

③ Ping of Death Attack: 조각난 패킷을 재조립했을 때 IPv4 패킷의 최대 크기인 65,535바이트를 넘도록 하는 등 비정상적인 ICMP 패킷으로 취약한 시스템에 장애를 일으킨다. **패킷 처리 과정의 취약점**을 이용해 정상 서비스를 방해하는 서비스 거부 공격이다.

④ Smurf Attack: 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내, 여러 호스트의 응답이 피해자에게 집중되도록 한다. **응답 트래픽을 증폭**하여 피해자의 네트워크나 시스템 자원을 소모시키는 서비스 거부 공격이다.

②·③·④는 정상적인 서비스 이용을 방해한다는 공통점이 있다. 이에 비해 ①은 정상 사용자의 세션과 권한을 도용하므로 공격의 성격이 다르다.

NoteBase

문 3. Stack에 할당된 Buffer overflow Attack에 대응할 수 있는 안전한 코딩(Secure Coding) 기술의 설명으로 옳지 않은 것은?

① 프로그램이 버퍼가 저장할 수 있는 것보다 많은 데이터를 입력하지 않는다.

② 프로그램은 할당된 버퍼 경계 밖의 메모리 영역은 참조하지 않으므로 버퍼 경계 안에서 발생될 수 있는 에러를 수정해 주면 된다.

③ gets()나 strcpy()와 같이 버퍼 오버플로우에 취약한 라이브러리 함수는 사용하지 않는다.

④ 입력에 대해서 경계 검사(Bounds Checking)를 수행해 준다.

정답 2번

간단한 해설

②의 '버퍼 경계 밖의 메모리 영역은 참조하지 않는다'는 전제가 잘못되었다. 버퍼 오버플로우는 **할당된 경계를 넘는 쓰기**로 주변 메모리를 훼손할 수 있으므로, 경계 안의 오류만 수정할 것이 아니라 **경계 밖 접근을 방지**해야 한다.

선지별 해설

① O: 버퍼에 기록할 데이터의 크기를 저장 가능한 용량 이내로 제한하면 초과 쓰기를 막을 수 있다. 문자열은 **끝을 표시하는 널 문자 공간까지** 확보해야 한다. 예를 들어 10바이트 버퍼에 1바이트 문자로 된 문자열을 저장한다면 문자 9개와 널 문자 1개를 담을 수 있다.

② X: C와 같은 언어에서는 배열이나 포인터를 통한 메모리 접근 시 버퍼 경계가 자동으로 검사된다고 보장할 수 없다. 따라서 잘못된 인덱스나 과도한 복사로 **할당된 버퍼 밖에도 접근할 수 있다**. 스택 버퍼를 넘겨 쓰면 주변 변수나 함수의 복귀 주소 등이 훼손될 수 있으므로, 버퍼 안의 오류만 수정하는 것이 아니라 입력 길이와 접근 범위를 검사해 경계 밖 접근을 막아야 한다.

③ O: gets()는 입력을 저장할 버퍼의 크기를 인수로 받지 않고, strcpy()도 목적지 버퍼의 크기를 확인하지 않은 채 문자열을 복사한다. 따라서 입력이나 원본 문자열이 목적지 용량보다 크면 버퍼 오버플로우가 발생할 수 있다. 이런 함수를 피하고 **목적지 용량에 맞게 읽기·복사 길이를 제한**하며, 문자열 종료를 위한 널 문자 공간도 확보해야 한다.

④ O: 경계 검사는 데이터를 저장하기 전에 입력 길이와 버퍼 용량을 비교하고, 접근할 인덱스가 유효한 범위에 있는지 확인하는 것이다. **쓰기 전에 범위 초과를 확인**하여 초과 입력을 거부하거나 허용 범위만 처리하면 버퍼 밖 메모리가 덮어써지는 것을 방지할 수 있다.

NoteBase

문 4. 전자화폐(Electronic Cash)에 대한 설명으로 옳지 않은 것은?

① 전자화폐의 지불 과정에서 물품 구입 내용과 사용자 식별 정보가 어느 누구에 의해서도 연계되어서는 안된다.

② 전자화폐는 다른 사람에게 즉시 이전할 수 있어야 한다.

③ 일정한 가치를 가지는 전자화폐는 그 가치만큼 자유롭게 분산이용이 가능해야 한다.

④ 대금 지불 시 전자화폐의 유효성 확인은 은행이 개입하여 즉시 이루어져야 한다.

정답 4번

간단한 해설

전자화폐의 **오프라인 결제**는 지불할 때 은행에 접속하지 않고 거래하는 방식이다. 따라서 은행이 개입하여 즉시 유효성을 확인해야 한다는 것은 전자화폐의 필수 요건이 아니다.

선지별 해설

① O: **익명성 또는 추적 불가능성**에 관한 설명이다. 정상적으로 전자화폐를 사용하는 사람의 구매 내역과 신원을 연결할 수 없도록 하여, 은행이나 판매자 등이 사용자의 소비 활동을 추적하지 못하게 한다.

② O: **양도성**에 관한 설명이다. 전자화폐를 받은 사람이 이를 은행에 입금하여 다시 발급받는 절차 없이 다른 사람에게 즉시 지급할 수 있어야 한다는 뜻이다.

③ O: **분할성**에 관한 설명이다. 전자화폐의 가치를 더 작은 금액으로 나누어 사용할 수 있어야 한다. 예를 들어 10,000원의 가치를 3,000원과 7,000원으로 나누어 쓰더라도 전체 가치는 10,000원으로 유지되어야 한다.

④ X: 전자화폐는 **지불 시 은행의 실시간 개입 없이도** 유효성을 확인하고 거래할 수 있는 오프라인 결제를 지원할 수 있다. 은행이 결제 때마다 개입하여 유효성과 이중 사용 여부를 확인하는 것은 온라인 방식의 특징이며, 모든 전자화폐에 반드시 요구되는 조건은 아니다.

NoteBase

문 5. Linux system의 바이너리 로그파일인 btmp(솔라리스의 경우는 loginlog 파일)를 통해 확인할 수 있는 공격은?

① Password Dictionary Attack
② SQL Injection Attack
③ Zero Day Attack
④ SYN Flooding Attack

정답 1번

간단한 해설

btmp와 loginlog는 **실패한 로그인 시도**를 기록한다. 비밀번호 사전 공격은 준비한 비밀번호 후보를 차례로 대입하므로, 반복되는 로그인 실패 기록에서 공격의 흔적을 확인할 수 있다.

공통 해설

btmp는 Linux에서 실패한 로그인 시도를 저장하는 바이너리 로그이며, lastb 명령으로 내용을 조회한다. Solaris의 loginlog도 실패한 로그인 시도를 기록한다. 두 로그를 해석하는 공통 기준은 **로그인 인증 실패의 반복 여부**이다.

비밀번호 사전 공격(Password Dictionary Attack)은 사전 단어나 자주 쓰이는 비밀번호 등으로 만든 **후보 목록을 차례로 대입**하여 비밀번호를 알아내는 공격이다. 이를 운영체제 로그인에 시도하면 일치하지 않는 후보 때문에 인증 실패가 반복될 수 있으므로, btmp나 loginlog가 공격 흔적을 조사하는 자료가 된다.

이 로그의 로그인 실패 기록은 SQL문 조작, 취약점의 공개 여부, TCP SYN 요청의 폭주를 직접 보여 주지 않으므로 SQL Injection, Zero Day, SYN Flooding의 핵심 특성을 입증하는 근거와는 구별된다. 다만 사용자의 입력 실수도 로그인 실패를 일으키므로, **실패 기록만으로 사전 공격을 확정할 수는 없다**.

NoteBase

문 6. 다음 바이러스 발전 단계에 따른 분류에 대한 설명으로 옳지 않은 것은?

① 원시형 바이러스는 가변 크기를 갖는 단순하고 분석하기 쉬운 바이러스이다.

② 암호화 바이러스는 바이러스 프로그램 전체 또는 일부를 암호화시켜 저장하는 바이러스이다.

③ 갑옷형 바이러스는 백신 개발을 지연시키기 위하여 다양한 암호화 기법을 사용하는 바이러스이다.

④ 매크로 바이러스는 매크로를 사용하는 프로그램 데이터를 감염시키는 바이러스이다.

정답 1번

간단한 해설

원시형 바이러스는 구조가 단순하고 분석하기 쉬우며, 바이러스 코드가 **고정된 크기**를 갖는다. ①의 '가변 크기'가 잘못된 표현이다.

선지별 해설

① X: 원시형 바이러스는 복잡한 암호화나 코드 변형 기법을 사용하지 않는 초기 형태로, 구조가 단순하고 분석하기 쉽다. 바이러스 코드가 **고정된 크기**를 가지므로 '가변 크기'를 '고정 크기'로 고쳐야 한다.

② O: 암호화 바이러스는 **바이러스 프로그램의 전체 또는 일부를 암호화**하여 저장한다. 바이러스 코드의 내용을 바로 알아보기 어렵게 만들어 백신의 탐지와 분석을 방해한다. 암호화한다고 해서 탐지나 치료가 불가능해지는 것은 아니다.

③ O: 갑옷형 바이러스는 다양한 암호화 기법 등으로 **분석을 어렵게 하여 백신 개발을 지연**시킨다. 메모리에 있는 코드도 암호화하거나 디버깅을 방해하는 코드를 넣는 방식으로 분석을 방해한다.

④ O: 매크로 바이러스는 문서 작성이나 표 계산 프로그램 등의 **매크로 기능을 이용해 문서·데이터 파일을 감염**시킨다. 매크로는 여러 작업을 자동으로 수행하는 명령들의 묶음이며, 감염된 문서에서 악성 매크로가 실행되면 다른 문서로 감염이 퍼질 수 있다.

NoteBase

문 7. 공개키 기반구조(Public Key Infrastructure, PKI)를 위한 요소 시스템으로 옳지 않은 것은?

① 인증서와 인증서 폐지 목록을 공개하기 위한 디렉토리

② 사용자 신원을 확인하는 등록기관

③ 인증서 발행업무를 효율적으로 수행하기 위한 인증기관 웹 서버

④ 인증서를 발행 받는 사용자(최종 개체)

정답 3번

간단한 해설

인증서를 발행하는 PKI의 핵심 주체는 **인증기관(CA)**이다. 웹 서버는 인증 업무를 위한 접속 창구로 활용될 수 있지만, 그 자체를 별도의 PKI 기본 구성요소로 보지는 않는다.

선지별 해설

① O: 디렉토리는 인증서와 인증서 폐지 목록(CRL)을 저장하고 공개하는 저장소 역할을 한다. 이용자는 이곳에서 **인증서와 폐지 정보**를 얻어 인증서 검증에 활용한다.

② O: 등록기관(RA)은 인증서를 신청한 **사용자의 신원을 확인**하고 등록 관련 업무를 처리한다. 인증기관을 대신해 이러한 업무를 수행할 수 있지만, 인증서에 서명하여 발행하는 주체는 인증기관(CA)이다.

③ X: 인증서 발행을 담당하는 기본 구성요소는 **인증기관(CA)**이다. CA는 인증서 주체와 공개키의 연결을 인증서에 담고 전자서명하여 발행한다. 웹 서버는 신청 접수나 안내 등의 업무에 활용될 수 있으나, '인증기관 웹 서버' 자체가 독립된 PKI 기본 구성요소에 해당하는 것은 아니다.

④ O: 사용자인 최종 개체는 **인증서를 발급받는 주체**에 해당한다. 개인뿐 아니라 서버나 장치 등도 최종 개체가 될 수 있으며, 인증서는 그 주체와 공개키의 연결을 증명하는 데 쓰인다.

NoteBase

문 8. 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보는 무엇인가?

① 수신 시스템이 처리할 수 있는 윈도우 크기

② 패킷을 송신하고 수신하는 프로세스의 포트 번호

③ 수신측에서 앞으로 받고자 하는 바이트의 순서 번호

④ 송신 시스템의 TCP 패킷의 생성 시간

정답 4번

간단한 해설

TCP 기본 헤더에는 **패킷의 생성 시각을 기록하는 필드가 없다**.

선지별 해설

① O: TCP 헤더의 **윈도우 크기(Window)** 필드는 수신 측이 추가로 받아들일 수 있는 데이터의 양을 바이트 단위로 알린다. 송신 측은 이를 이용해 전송량을 조절하므로, 수신 버퍼가 넘치지 않도록 하는 흐름 제어에 사용된다.

② O: TCP 헤더에는 **출발지 포트와 목적지 포트** 필드가 있다. 이 값으로 송신 측과 수신 측에서 통신에 사용하는 포트 번호를 확인할 수 있다. 포트 번호는 한 호스트 안에서 통신하는 응용 프로그램을 구분하는 데 쓰인다.

③ O: TCP 헤더의 **확인 응답 번호(Acknowledgment Number)**는 다음에 수신하기를 기대하는 바이트의 순서 번호이다. ACK 플래그가 설정되어 있을 때 유효하며, 예를 들어 이 값이 1001이면 1000번까지의 바이트를 연속해서 받았고 다음에는 1001번 바이트를 기대한다는 뜻이다.

④ X: 기본 TCP 헤더에는 **패킷의 생성 시각을 직접 기록하는 필드가 없다**. 따라서 기본 헤더 필드만 읽어 송신 시스템이 패킷을 생성한 시각을 알아낼 수는 없다. 선택적으로 사용하는 타임스탬프 옵션의 TSval은 송신 측 타이머 값이며, 실제 날짜·시각으로 표시한 패킷 생성 시각을 뜻하지 않는다.

NoteBase

문 9. 아래 <보기>의 지문은 신문에서 발췌한 기사이다. 빈칸에 들어갈 단어로 적절한 것은?

<보기>
취업준비생 김다정(28)씨는 지난 5월 7일 _____ 공격으로 취업을 위해 모아뒀던 학습 및 준비 자료가 모두 암호화돼 버렸다. 컴퓨터 화면에는 암호를 알려주는 대가로 100달러(약 11만 5000원)를 요구하는 문구가 떴지만, 결제해도 데이터를 되찾을 수 없다는 지인의 조언에 데이터복구 업체를 통해 일부 자료만 복구해 보기로 했다. 그런데 업체를 통해 데이터 일부를 복구한 지 하루 만인 지난 10일 또 다시 _____ 공격을 받아 컴퓨터가 먹통이 돼 버렸다.

① 하트블리드(Heart bleed)
② 랜섬웨어(Ransomware)
③ 백오리피스(Back Orifice)
④ 스턱스넷(Stuxnet)

정답 2번

간단한 해설

자료를 **암호화해 사용할 수 없게 만든 뒤 복구를 대가로 금전을 요구**하는 것은 랜섬웨어의 특징이다. 기사에서 자료가 암호화되고 암호를 알려주는 대가로 100달러를 요구한 것이 결정적인 단서이다.

공통 해설

랜섬웨어(Ransomware)는 피해자의 파일을 암호화하거나 시스템 접근을 막은 뒤, 이를 풀어 주는 대가로 금전을 요구하는 악성코드이다. 파일 암호화형은 자료를 읽을 수 없게 만들어 피해자가 복구 대가를 지급하도록 압박한다.

기사에서는 학습 및 준비 자료가 모두 암호화되었고, 화면에 암호를 알려주는 대가로 100달러를 요구하는 문구가 나타났다. 이처럼 **자료의 사용을 막고 복구를 조건으로 금전을 요구**하는 행위가 랜섬웨어에 해당하므로, 같은 공격을 가리키는 두 빈칸에는 모두 '랜섬웨어'가 들어간다. 단순히 컴퓨터가 먹통이 되었다는 사실보다 암호화와 금전 요구가 결합되어 있다는 점이 공격을 식별하는 기준이다.

NoteBase

문 10. 다음 중 Cipher Block Chaining 운용 모드의 암호화 수식을 제대로 설명한 것은? (단, P□는 i번째 평문 블록을, C□는 i번째 암호문 블록을 의미한다.)

① $C_i = E_k(P_i)$

② $C_i = E_k(P_i \oplus C_{i-1})$

③ $C_i = E_k(C_{i-1}) \oplus P_i$

④ $C_i = E_k(P_i) \oplus C_{i-1}$

정답 2번

간단한 해설

CBC는 **현재 평문 블록과 직전 암호문 블록을 먼저 XOR**하고, 그 결과를 키로 암호화한다. 따라서 XOR 연산은 암호화 함수의 괄호 안에 들어간다.

공통 해설

CBC(Cipher Block Chaining)는 직전 암호문을 다음 평문 블록의 암호화에 연결하는 운용 모드이다. E_k는 키 k를 사용하는 블록 암호의 암호화 함수이고, ⊕는 두 비트가 다르면 1, 같으면 0을 내는 비트별 XOR 연산이다.

현재 평문 P_i와 직전 암호문 C_{i-1}을 XOR한 $P_i \oplus C_{i-1}$이 암호화 함수의 입력이 된다. 이를 암호화하여 현재 암호문을 얻으므로 관계식은 $C_i = E_k(P_i \oplus C_{i-1})$이다. 핵심은 **평문과 직전 암호문의 XOR 결과 전체를 암호화**한다는 점이다. 직전 암호문을 사용하지 않거나, 직전 암호문만 암호화한 뒤 평문과 XOR하거나, 평문을 암호화한 뒤 직전 암호문과 XOR하는 식은 이 관계와 다르다.

첫 블록에는 직전 암호문이 없으므로 초기화 벡터 IV를 사용한다. $C_0 = \text{IV}$로 두면 $C_1 = E_k(P_1 \oplus \text{IV})$이고, 이어서 $C_2 = E_k(P_2 \oplus C_1)$이 된다. 이처럼 앞서 생성한 암호문이 다음 블록의 암호화에 연결된다.

NoteBase

문 11. 공통평가기준(Common Criteria, CC)에 대한 설명 중 옳지 않은 것은?

① 보호프로파일(Protection Profile)과 보안목표명세서(Security Target) 중 제품군에 대한 요구사항 중심으로 기술되어 있는 것은 보안목표명세서(Security Target)이다.

② 평가대상에는 EAL 1에서 EAL 7까지 보증등급을 부여할 수 있다.

③ CC의 개발은 오렌지북이라는 기준서를 근간으로 하였다.

④ CC의 요구사항은 class, family, component로 분류한다.

정답 1번

간단한 해설

제품군에 공통으로 적용할 보안 요구사항을 구현 방식과 독립적으로 기술하는 문서는 **보호프로파일(PP)**이다. 보안목표명세서(ST)는 **특정 평가대상**의 보안 요구사항과 이를 충족하는 보안기능 등을 기술한다.

선지별 해설

① X: 보호프로파일(PP)은 특정 제품의 구현 방식에 종속되지 않고, 한 제품군이 충족해야 할 공통 보안 요구사항을 기술한다. 보안목표명세서(ST)는 식별된 특정 평가대상(TOE)의 보안목표·요구사항과 이를 충족하는 보안기능의 개요 등을 기술한다. 따라서 선지의 '제품군에 대한 요구사항 중심으로 기술되어 있는 것'은 보안목표명세서가 아니라 **보호프로파일**로 고쳐야 한다.

② O: CC는 평가대상의 보증 수준을 나타내는 **EAL1부터 EAL7까지 7개 평가보증등급**을 정의한다. 등급이 높아질수록 평가의 엄격성·범위·깊이가 증가하여, 명시된 보안 요구사항을 평가대상이 충족한다는 신뢰를 더 높게 제공한다.

③ O: 오렌지북은 미국의 신뢰 컴퓨터 시스템 평가기준(TCSEC)을 가리키며, **CC의 개발 기반 가운데 하나**이다. CC는 미국의 TCSEC, 유럽의 ITSEC, 캐나다의 CTCPEC 등 기존 평가기준을 통합하여 공통의 보안성 평가기준을 마련한 것이다.

④ O: CC의 보안 요구사항은 **클래스(class) → 패밀리(family) → 컴포넌트(component)**의 계층으로 분류한다. 클래스는 관련된 보안 주제를 크게 묶고, 그 안의 패밀리는 공통 목적을 가진 요구사항들을 묶는다. 컴포넌트는 패밀리 안에서 구체적인 요구사항을 제시하며, PP나 ST에 요구사항을 명시할 때 선택하는 단위가 된다.

NoteBase

문 12. <보기>에서 설명하는 암호화 알고리즘으로 옳은 것은?

<보기>
· Ron Rivest가 1987년에 RSA Security에 있으면서 설계한 스트림 암호이다.
· 바이트 단위로 작동되도록 만들어진 다양한 크기의 키를 사용한다.
· 사용되는 알고리즘은 랜덤 치환에 기초해서 만들어진다.
· 하나의 바이트를 출력하기 위해서 8번에서 16번의 기계연산이 필요하다.

① RC5
② SEED
③ SKIPJACK
④ RC4

정답 4번

간단한 해설

가변 길이 키와 순열을 이용해 바이트 단위의 키스트림을 생성하는 것은 RC4의 특징이다. 생성한 키스트림을 평문과 XOR하여 암호화한다.

공통 해설

RC4는 Ron Rivest가 1987년에 설계한 바이트 단위 스트림 암호이다. 스트림 암호는 키로부터 의사난수열인 키스트림을 만들고, 이를 평문과 차례로 XOR하여 암호문을 생성한다. RC4는 다양한 길이의 키를 지원하므로 보기의 설계자·설계 연도·가변 길이 키 조건에 부합한다.

RC4의 내부에는 0부터 255까지의 값이 하나씩 들어 있는 256바이트 배열이 있다. 키를 이용해 이 값들의 순서를 섞은 뒤, 배열의 두 값을 교환하고 배열을 참조하는 과정을 반복하여 키스트림을 한 바이트씩 출력한다. 보기의 '랜덤 치환'은 이처럼 **값의 순서를 바꾸는 순열**을 뜻한다. 출력 바이트당 8~16회의 기계연산이라는 설명은 이러한 간단한 연산 구조에 따른 소프트웨어 처리 효율을 나타낸다.

후보 중 RC4는 **바이트 단위 키스트림을 생성하는 스트림 암호**이고, RC5·SEED·SKIPJACK은 일정한 크기의 데이터 블록을 변환하는 블록 암호이다. 따라서 보기에서 설명하는 암호의 종류와 동작 방식은 RC4에 대응한다.

NoteBase

문 13. 다음 중 Spoofing 공격에 대한 설명으로 옳지 않은 것은?

① ARP Spoofing : MAC주소를 속임으로써 통신 흐름을 왜곡시킨다.

② IP Spoofing : 다른이가 쓰는 IP를 강탈해 특정 권한을 획득한다.

③ DNS Spoofing : 공격대상이 잘못된 IP주소로 웹 접속을 하도록 유도하는 공격이다.

④ ICMP Redirect : 공격자가 클라이언트의 IP주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근한다.

정답 4번

간단한 해설

ICMP Redirect 공격은 거짓 경로 변경 메시지로 **패킷의 전송 경로를 바꾸는** 공격이다. ④처럼 정상 클라이언트로 위장해 비밀번호 없이 접근하는 것은 서버의 **IP 기반 신뢰 관계**를 악용하는 IP Spoofing의 사례이다.

선지별 해설

① O: ARP는 같은 네트워크에서 IP주소에 대응하는 MAC주소를 알아내는 프로토콜이다. ARP Spoofing은 거짓 ARP 메시지로 피해자의 **IP주소와 MAC주소의 대응 정보**를 오염시킨다. 예를 들어 게이트웨이의 IP주소에 공격자의 MAC주소가 연결되면, 게이트웨이로 보낼 프레임이 공격자에게 전달되어 통신 흐름이 왜곡된다.

② O: IP Spoofing은 패킷의 **출발지 IP주소를 위조**하여 다른 호스트가 보낸 것처럼 가장하는 공격이다. 서버가 특정 IP주소를 신뢰하여 접근 권한을 부여하는 환경에서는 이를 악용해 권한을 얻을 수 있다. 선지의 'IP를 강탈'은 다른 호스트의 IP주소를 사칭한다는 취지이며, IP주소를 아는 것만으로 모든 서버의 인증을 통과하는 것은 아니다.

③ O: DNS는 도메인 이름을 IP주소로 변환하는 데 사용된다. DNS Spoofing은 **거짓 DNS 응답** 등을 통해 공격자가 지정한 IP주소를 정상적인 변환 결과로 받아들이게 한다. 따라서 사용자가 올바른 도메인 이름을 입력하더라도 엉뚱한 서버로 웹 접속이 유도될 수 있다.

④ X: ICMP Redirect는 라우터가 호스트에 더 적절한 다음 경유지인 게이트웨이를 알려 주어 경로 정보를 갱신하게 하는 기능이다. 이를 악용한 공격은 라우터를 사칭한 거짓 메시지로 **공격자가 원하는 경로로 패킷을 보내게** 한다. 정상 클라이언트의 IP주소를 사칭하여 비밀번호 없이 서버에 접근하는 설명은 IP 기반 신뢰 관계를 악용하는 IP Spoofing에 해당한다.

NoteBase

문 14. 다음 중 ISMS(Information Security Management System)의 각 단계에 대한 설명으로 옳은 것은?

① 계획 : ISMS 모니터링과 검토

② 조치 : ISMS 관리와 개선

③ 수행 : ISMS 수립

④ 점검 : ISMS 구현과 운영

정답 2번

간단한 해설

조치(Act)는 점검 결과를 바탕으로 시정·예방조치를 취하여 ISMS를 **유지·관리하고 개선**하는 단계이다. 운영 성과를 확인하는 점검(Check)과 달리, 확인된 문제를 바로잡아 지속적으로 개선한다.

선지별 해설

ISMS는 조직의 정보보호를 체계적으로 관리하기 위한 정보보호 관리체계이다. 이 문항의 PDCA 모형은 계획(Plan)·수행(Do)·점검(Check)·조치(Act)를 반복하여 관리체계를 지속적으로 개선한다.

① X: 'ISMS 모니터링과 검토'는 **점검(Check)** 단계의 활동이다. 계획(Plan) 단계에서는 정보보호 정책과 목표, 위험을 관리하기 위한 절차 등을 정하여 ISMS를 수립한다.

② O: 조치(Act) 단계에서는 내부감사와 경영진 검토 등의 결과를 바탕으로 **시정·예방조치**를 취한다. 이를 통해 ISMS를 유지·관리하고 지속적으로 개선하므로, 'ISMS 관리와 개선'이라는 연결이 성립한다.

③ X: 'ISMS 수립'은 **계획(Plan)** 단계의 활동이다. 수행(Do) 단계에서는 수립한 정책과 절차에 따라 보호대책을 실제로 구현하고 ISMS를 운영한다.

④ X: 'ISMS 구현과 운영'은 **수행(Do)** 단계의 활동이다. 점검(Check) 단계에서는 운영 중인 ISMS의 성과를 정책과 목표에 비추어 모니터링하고 검토하여, 보호대책이 의도대로 작동하는지 평가한다.

NoteBase

문 15. 중앙집중식 인증 방식인 커버로스(Kerberos)에 대한 다음 설명 중 옳은 것은 무엇인가?

① TGT(Ticket Granting Ticket)는 클라이언트가 서비스를 받을 때마다 발급 받아야 한다.

② 커버로스는 독립성을 증가시키기 위해 키 교환에는 관여하지 않아 별도의 프로토콜을 도입해야 한다.

③ 커버로스 방식에서는 대칭키 암호화 방식을 사용하여 세션 통신을 한다.

④ 공격자가 서비스 티켓을 가로채어 사용하는 공격에는 취약한 방식이다.

정답 3번

간단한 해설

커버로스는 클라이언트와 서비스 서버가 공유하는 **대칭 세션키**를 분배하여 인증하고, 이 키로 세션 통신을 보호할 수 있다. 서비스 티켓만 가로채더라도 세션키로 만든 인증자가 없으면 정상 사용자로 인증받을 수 없다.

선지별 해설

① X: TGT는 서비스 티켓을 발급받기 위해 티켓 발급 서버(TGS)에 제시하는 티켓이다. 최초 인증으로 받은 TGT는 **유효기간 안에서 재사용**할 수 있으므로 서비스를 이용할 때마다 새로 발급받을 필요가 없다. 다른 서비스를 이용하려면 기존 TGT로 해당 서비스의 티켓을 요청한다.

② X: 커버로스의 키 분배 센터(KDC)는 인증뿐 아니라 **세션키 분배에도 관여**한다. 클라이언트와 서비스 서버가 같은 세션키를 안전하게 얻도록 티켓과 암호화된 응답을 제공하므로, 키 교환에 관여하지 않아 별도 프로토콜이 필요하다는 설명은 잘못이다.

③ O: 커버로스는 **공유 비밀키를 사용하는 대칭키 방식**을 기반으로 한다. 클라이언트는 암호화된 응답에서, 서비스 서버는 자신의 비밀키로 복호화한 티켓에서 세션키를 얻는다. 이렇게 공유한 세션키로 인증하며, 세션 데이터의 암호화에도 사용할 수 있다. 다만 커버로스로 인증했다는 사실만으로 모든 응용 데이터가 자동 암호화되는 것은 아니다.

④ X: 커버로스는 서비스 티켓과 함께 **세션키로 암호화한 인증자**를 요구하여 티켓의 부정 사용을 막는다. 인증자에는 시각 정보가 포함되며, 서버는 허용 시간차와 이미 사용된 인증자를 확인해 재전송을 탐지한다. 따라서 티켓만 가로채어 사용하는 공격에 그대로 취약하다는 설명은 잘못이다. 다만 티켓과 세션키가 함께 탈취되면 위장이 가능하므로 세션키 보호도 필요하다.

NoteBase

문 16. 다음 중 시스템 내부의 트로이목마 프로그램을 감지하기 위한 도구로 가장 적절한 것은?

① Saint

② Snort

③ Nmap

④ Tripwire

정답 4번

간단한 해설

Tripwire는 **파일 무결성 검사**로 시스템 파일의 변조를 감지한다. 정상 파일이 트로이목마가 포함된 파일로 바뀌면, 미리 저장한 정상 상태와의 차이를 찾아낼 수 있다.

공통 해설

Tripwire는 시스템 파일의 현재 상태를 미리 저장한 정상 상태와 비교하는 파일 무결성 검사 도구이다. 신뢰할 수 있는 정상 상태에서 검사 대상 파일의 해시값과 권한 등 기준 정보를 저장하고, 이후 검사에서 달라진 내용을 알린다. 해시값은 파일 내용으로부터 계산하는 값이므로, 정상 프로그램이 트로이목마가 포함된 파일로 교체되면 **기준 해시값과의 차이**로 변조를 감지할 수 있다. 이처럼 시스템 내부 파일의 변조를 찾아내는 도구가 Tripwire이다.

비교 기준은 **감염되지 않은 정상 상태**에서 만들어 두어야 한다. 또한 정상적인 프로그램 업데이트도 파일을 바꾸므로, 변경이 발견되었다는 사실만으로 트로이목마 감염이 확정되는 것은 아니다. 탐지된 변경이 승인된 작업인지 확인해야 한다.

NoteBase

문 17. ROT13 암호로 “info”를 암호화한 결과는?

① jvxv

② foin

③ vasb

④ klmd

정답 3번

간단한 해설

ROT13은 각 영문자를 알파벳 순서에서 **13칸 뒤의 문자**로 바꾸며, z를 넘으면 a부터 이어 센다. 'info'의 각 문자를 바꾸면 **'vasb'**가 된다.

계산 과정

ROT13은 영문 알파벳 26자를 원형으로 이어 놓고 각 문자를 13칸 뒤의 문자로 치환하는 방식이다. a를 1번째, z를 26번째로 두면 원래 위치에 13을 더하고, **26을 초과하면 26을 빼서** 변환할 문자의 위치를 구한다.

i → v: i는 9번째 문자이므로 9 + 13 = 22이다. 22번째 문자인 v로 바뀐다.

n → a: n은 14번째 문자이므로 14 + 13 = 27이다. 26을 넘으므로 27 − 26 = 1로 돌아가며, 첫 번째 문자인 a로 바뀐다.

f → s: f는 6번째 문자이므로 6 + 13 = 19이다. 19번째 문자인 s로 바뀐다.

o → b: o는 15번째 문자이므로 15 + 13 = 28이다. 26을 넘으므로 28 − 26 = 2로 돌아가며, 두 번째 문자인 b로 바뀐다.

원래 문자 순서를 유지하여 변환 결과를 이어 붙이면 암호문은 'vasb'이며, ③의 문자열과 일치한다.

NoteBase

문 18. 무선랜에서의 인증 방식에 대한 설명 중 옳지 않은 것은?

① WPA 방식은 48비트 길이의 초기벡터(IV)를 사용한다.

② WPA2 방식은 AES 암호화 알고리즘을 사용하여 좀 더 강력한 보안을 제공한다.

③ WEP 방식은 DES 암호화 방식을 이용한다.

④ WEP 방식은 공격에 취약하며 보안성이 약하다.

정답 3번

간단한 해설

WEP는 DES가 아니라 **RC4 스트림 암호**를 사용한다. RC4가 생성한 키 스트림과 평문을 XOR하여 데이터를 암호화한다.

선지별 해설

① O: WPA의 TKIP는 **48비트 초기벡터(IV)**를 사용한다. IV는 암호화에 사용하는 초기값이며, WEP의 24비트 IV보다 값의 범위가 넓어 같은 값이 반복되는 문제를 줄인다.

② O: WPA2는 **AES 기반의 CCMP**를 사용하여 데이터의 기밀성과 무결성을 보호한다. RC4 기반의 WEP·WPA보다 강화된 암호화와 무결성 보호를 제공한다.

③ X: WEP가 사용하는 암호 알고리즘은 DES가 아니라 **RC4**이다. RC4는 키 스트림을 생성하고 이를 평문과 XOR하는 스트림 암호이다. DES는 데이터를 일정한 크기의 블록으로 나누어 암호화하는 블록 암호이므로 WEP의 암호 알고리즘과 구별해야 한다.

④ O: WEP는 **짧은 IV와 RC4 사용 방식의 취약점** 때문에 수집한 무선 패킷을 분석하여 키를 복구하는 공격에 취약하다. 또한 무결성 검사에 사용하는 CRC-32는 공격자의 의도적인 데이터 변조를 안전하게 막는 암호학적 메시지 인증 수단이 아니므로 보안성이 약하다.

NoteBase

문 19. 다음 중 ISO 27001의 통제 영역별 주요 내용으로 옳은 것은?

① 정보보안 조직: 정보보호에 대한 경영진의 방향성 및 지원을 제공

② 인적 자원 보안: 정보에 대한 접근을 통제

③ 정보보안 사고 관리: 사업장의 비인가된 접근 및 방해 요인을 예방

④ 통신 및 운영 관리: 정보처리시설의 정확하고 안전한 운영을 보장

정답 4번

간단한 해설

통신 및 운영 관리는 정보처리시설이 **정확하고 안전하게 운영**되도록 운영 절차와 책임, 시스템 변경 등을 관리하는 영역이다.

선지별 해설

이 문항의 '통신 및 운영 관리'는 ISO/IEC 27001:2005의 통제 영역 명칭이다.

① X: 정보보호에 대한 경영진의 방향성과 지원을 제공하는 것은 **정보보안 정책**의 목적이다. 정보보안 조직은 보안 역할과 책임을 명확히 정하고 관련 활동을 조정하여 조직 내 정보보안을 관리하는 영역이다.

② X: 정보에 대한 접근을 통제하는 것은 **접근 통제** 영역의 목적이다. 인적 자원 보안은 구성원의 보안 책임, 교육·훈련, 퇴직이나 직무 변경 시 조치 등을 통해 사람으로 인한 보안 위험을 줄이는 영역이다.

③ X: 사업장의 비인가된 물리적 접근과 손상·방해를 예방하는 것은 **물리적 및 환경적 보안** 영역의 목적이다. 정보보안 사고 관리는 보안 사건과 취약점을 신속히 보고하고, 정해진 책임과 절차에 따라 사고에 일관되고 효과적으로 대응하도록 하는 영역이다.

④ O: 통신 및 운영 관리는 정보처리시설의 정확하고 안전한 운영을 보장하는 영역이다. **운영 절차의 문서화, 변경 관리, 직무 분리** 등을 통해 운영 오류나 비인가 변경·오용의 위험을 줄인다.

NoteBase

문 20. 「개인정보보호법」에 따르면 주민등록번호를 처리하기 위해서는 법에서 정하는 바에 따라야 하는데, 그에 대한 내용 중 옳지 않은 것은?

① 주민등록번호 처리는 원칙적으로 금지되고 예외적인 경우에만 허용한다.

② 주민등록번호는 암호화 조치를 통해 보관해야 한다.

③ 개인정보처리자는 법령에서 주민등록번호의 처리를 허용한 경우에도 주민등록번호를 사용하지 않는 인터넷 회원 가입 방법을 정보주체에게 제공해야 한다.

④ 기 보유한 주민등록번호는 수집 시 동의 받은 보유기간까지만 보유하고 이후에는 즉시 폐기해야 한다.

정답 4번

간단한 해설

④의 '동의받은 보유기간까지만 보유'는 주민등록번호의 특별한 처리 제한을 놓친 설명이다. 법정 예외에 해당하지 않는 기존 주민등록번호는 동의받은 기간이 남아 있어도 개정법 **시행일부터 2년 이내에 파기**해야 했다.

선지별 해설

① O: 개인정보 보호법 제24조의2제1항은 주민등록번호 처리를 원칙적으로 금지한다. 구체적인 법령상 처리 근거가 있거나 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위하여 명백히 필요한 경우 등 법에서 정한 예외에 해당해야 한다. **정보주체의 동의만으로는 처리할 수 없다.**

② O: 제24조의2제2항에 따라 개인정보처리자는 주민등록번호를 **암호화하여 안전하게 보관**해야 한다. 이는 적법하게 보유하는 주민등록번호에도 적용되는 보호 의무이며, 암호화했다고 해서 법적 근거 없는 보유가 허용되는 것은 아니다.

③ O: 제24조의2제3항에 따라 법에서 정한 예외 사유로 주민등록번호를 처리하는 경우에도 인터넷 홈페이지의 회원 가입 단계에서는 **주민등록번호 없이 가입할 수 있는 방법**을 제공해야 한다. 주민등록번호의 처리 허용과 회원 가입 시 대체 방법 제공 의무는 별개의 문제이다.

④ X: 이미 수집한 주민등록번호라고 하여 동의받은 보유기간까지 계속 보유할 수 있는 것은 아니다. 법률 제11990호 개정법 부칙 제2조는 법정 예외에 해당하지 않는 기존 주민등록번호를 **법 시행일부터 2년 이내에 파기**하도록 정했다. 이 법은 2014년 8월 7일 시행되었으므로 파기 기한은 2016년 8월 6일까지였다. 다만, 제24조의2제1항의 예외 사유에 해당하는 주민등록번호는 이 경과조치에 따른 일괄 파기 대상에서 제외된다.

NoteBase