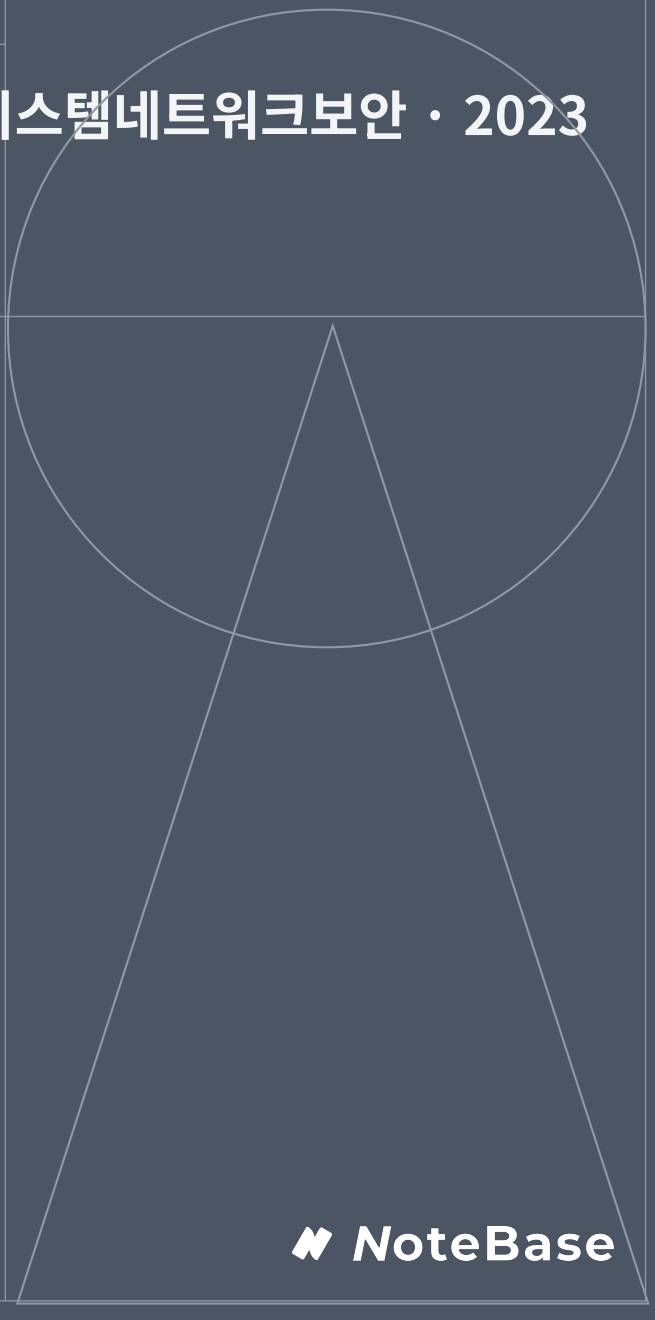
기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2023



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2023

공무원/경찰/공채(경위) · 시스템네트워크보안 · 2023

문 1. 다음에 설명하는 보안 솔루션의 유형으로 가장 적절한 것은?

· 해커에게 쉽게 노출된다.
· 시스템의 모든 구성 요소를 갖추고 있다.
· 통과하는 모든 패킷을 감시한다.
· 취약점을 갖고 있는 시스템이다.

① 침입탐지시스템
② 허니팟
③ 방화벽
④ 침입차단시스템

정답 2번

간단한 해설

허니팟은 공격자가 접근하도록 유도하는 시스템을 마련하고 그 안에서 일어나는 공격을 관찰하는 보안 기법이다. 취약한 대상으로 보이게 노출하고 트래픽과 행위를 기록한다는 점이 핵심 단서이다.

NoteBase

대응 관계 해설

허니팟은 공격자가 실제 목표로 오인하도록 마련한 **유인용 시스템**이다. 공격을 유도한 뒤 접근 기록과 행위를 관찰하여 공격 방식에 관한 정보를 얻는다.

'해커에게 쉽게 노출된다': 공격자가 발견하고 접근할 만한 대상으로 보이게 구성한다. 중요한 업무 시스템 대신 유인용 시스템에 관심을 돌리게 하는 목적과 연결된다.

'시스템의 모든 구성 요소를 갖추고 있다': 실제 시스템처럼 상호작용할 환경을 제공한다는 단서이다. 실제 운영체제와 서비스를 제공하는 고상호작용 허니팟이 이런 형태에 가깝다. 모든 허니팟이 완전한 시스템이어야 하는 것은 아니며, 일부 서비스만 모방하는 형태도 있다.

'통과하는 모든 패킷을 감시한다': 허니팟과 오가는 트래픽을 기록·분석하여 공격자의 접속과 공격 진행 과정을 관찰한다. 허니팟이 조직 전체 네트워크의 모든 통신을 자동으로 볼 수 있다는 뜻은 아니다.

'취약점을 갖고 있는 시스템이다': 제시된 환경에서는 공격 가능한 약점이 있는 유인 대상을 두어 침입 시도와 후속 행위를 관찰한다. 관찰용 취약 환경이 실제 업무 시스템이나 다른 시스템에 피해를 확산시키지 않도록 격리와 통제가 필요하다.

침입탐지시스템은 침입 징후를 탐지·분석하는 데, 방화벽과 침입차단시스템은 보안 정책에 따라 접근이나 통신을 통제하는 데 중심을 둔다. **취약한 유인 대상을 노출하고 그 대상에 대한 공격을 관찰**한다는 단서를 함께 만족하는 것은 허니팟이므로 ②에 해당한다.

NoteBase

문 2. IPSec 터널 모드에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. IP 헤더를 보호하지 않는다.
나. IP 헤더를 포함한 패킷 전체를 보호한다.
다. 두 개의 라우터 간, 호스트와 라우터 간, 또는 라우터와 호스트 간에 사용한다.
라. 전송층에서 네트워크층으로 전달되는 모든 패킷을 보호한다.

① 가, 다
② 가, 라
③ 나, 다
④ 나, 라

정답 3번

간단한 해설

터널 모드는 **원래 IP 헤더를 포함한 IP 패킷 전체**를 캡슐화해 보호한다. 새 외부 IP 헤더로 터널 끝점 사이를 전달하므로 보안 게이트웨이 간이나 호스트와 게이트웨이 간 연결에 사용할 수 있다.

NoteBase

보기별 해설

터널 모드는 원래 IP 패킷을 통째로 새 IP 패킷 안에 넣는 방식이다. 원래 헤더는 내부 IP 헤더가 되고, 새 외부 IP 헤더는 터널 양 끝점 사이의 전달에 사용된다.

가. X: 터널 모드는 **원래 IP 헤더도 보호 대상에 포함**한다. IP 헤더를 보호하지 않고 그 뒤의 데이터를 보호한다는 설명은 ESP 전송 모드의 보호 범위에 해당한다. AH 전송 모드는 일부 IP 헤더 필드도 인증하므로 모든 전송 모드에 이를 그대로 일반화하지 않는다.

나. O: 터널 안에 담긴 **원래 IP 헤더와 데이터 전체**가 보호 대상이다. 새로 붙인 외부 IP 헤더까지 동일하게 보호한다는 뜻은 아니다. ESP는 외부 IP 헤더를 보호하지 않고, AH는 외부 헤더 중 보호 가능한 부분에도 인증을 적용한다.

다. O: 보안 게이트웨이 역할의 라우터끼리 연결하거나 호스트와 라우터를 연결할 때 터널 모드를 사용할 수 있다. 원래 통신 당사자의 주소를 내부 헤더에 유지하면서 터널 끝점의 주소를 외부 헤더에 넣는다. 호스트 간에도 사용할 수 있으므로 제시된 연결에만 한정되는 것은 아니다.

라. X: 이 문항에서 전송층이 넘긴 데이터를 보호 대상으로 설명하는 부분은 전송 모드와 대비되는 표현이다. 터널 모드의 구별점은 상위 계층 데이터에 그치지 않고 **원래 IP 헤더까지 포함해 보호**한다는 데 있다. 터널 모드도 내부의 전송층 데이터를 보호하며, 어느 모드든 실제 보호 여부는 보안 정책에 따라 정해지므로 모든 트래픽을 무조건 보호한다는 뜻은 아니다.

따라서 터널 모드에 대한 설명으로 고르는 보기는 나, 다이며 ③에 해당한다.

NoteBase

문 3. 버퍼 오버플로(buffer overflow) 공격 대응책에 대한 설명으로 가장 적절한 것은?

① ASLR: 스택에서 실행 권한을 제거함으로써 스택에 로드된 공격자의 공격코드를 실행할 수 없도록 한다.

② Non-Executable Stack: 메모리 공격을 방어하기 위해 스택, 힙, 라이브러리 등의 데이터 영역 주소를 난수화 한다.

③ Stack Guard: 스택에 있는 복귀 주소를 실행 가능한 임의의 주소(libc 영역의 주소)로 돌려 원하는 함수를 수행한다.

④ Stack Shield: 함수를 호출할 때는 복귀 주소를 Global RET Stack이라는 특수 스택에 저장하고 함수를 종료할 때는 Global RET Stack에 저장된 복귀 주소 값과 스택의 복귀 주소 값을 비교하여 일치하지 않으면 프로그램을 종료시킨다.

정답 4번

간단한 해설

Stack Shield의 검사 모드는 **별도로 보관한 복귀 주소와 스택의 복귀 주소를 비교**하여 변조를 탐지한다. 두 주소가 다르면 프로그램을 종료한다.

선지별 해설

① X: 스택의 실행 권한을 제거하여 스택에 저장된 데이터를 명령으로 실행하지 못하게 하는 것은 **실행 불가능 스택**의 설명이다. ASLR은 스택·힙·공유 라이브러리 등의 배치 주소를 무작위화하여 공격자가 필요한 주소를 예측하기 어렵게 하는 기법이다. 실행 권한 제어와 주소 배치의 난수화를 혼동하면 안 된다.

② X: 주소를 난수화하는 기법은 **ASLR**이다. Non-Executable Stack은 스택에 실행 권한을 주지 않는 방식이며, 그 자체로 스택이나 힙의 주소를 바꾸는 것은 아니다. 두 기법은 서로 다른 방어 기능이므로 함께 적용할 수 있다.

③ X: 복귀 주소를 기존 라이브러리 코드 쪽으로 바꾸어 함수를 실행시키는 것은 **return-to-libc 공격**의 개념이다. Stack Guard의 대표적 방식은 복귀 주소 앞에 카나리 값을 두고 함수 복귀 전에 값이 변했는지 검사하여 변조를 탐지하는 것이다. 공격 기법과 이를 막기 위한 보호 기법을 바꾸어 설명했다.

④ O: Stack Shield는 복귀 주소의 사본을 별도 영역에 보관하여 보호한다. 제시문은 사본과 일반 스택의 복귀 주소를 비교해 다르면 종료하는 **검사 모드**에 해당한다. 이 모드는 실제로 존재하며, 카나리의 변화를 검사하는 Stack Guard와 구별된다. 다만 Stack Shield의 모든 동작 모드가 비교 후 종료하는 것은 아니다. 기본 복원 방식은 보관한 주소를 원래 스택에 다시 써서 복귀에 사용한다.

NoteBase

문 4. tcpdump에 대한 설명으로 가장 적절하지 않은 것은?

① Lawrence Berkley Nation Lab의 Network Research Group에서 만들었다.

② 리눅스에서 가장 기본이 되는 spoofing 도구이다.

③ 네트워크 상태를 확인하기 위해 패킷을 캡처하여 분석할 때 사용한다.

④ libpcap 라이브러리를 사용하여 패킷을 캡처한다.

정답 2번

간단한 해설

tcpdump는 네트워크를 지나는 **패킷을 캡처하고 내용을 분석하는 도구**이다. 주소나 신원 정보를 위조하는 spoofing과는 기능이 다르므로, spoofing 도구라고 한 설명이 적절하지 않다.

선지별 해설

① O: 개발 주체를 로런스 버클리 국립연구소의 Network Research Group으로 설명한 취지는 맞다. tcpdump는 이 연구 그룹에서 처음 개발되었다. 선지의 'Lawrence Berkley Nation Lab'은 기관 영문 표기의 오기가 있으며, 정확한 기관명은 Lawrence Berkeley National Laboratory이다.

② X: tcpdump는 **스니핑(sniffing) 및 패킷 분석**에 사용하는 명령행 도구이다. 스니핑은 관찰 가능한 네트워크 트래픽을 수집·확인하는 것이고, 스푸핑(spoofing)은 주소나 신원 등의 정보를 위조하여 다른 대상처럼 보이게 하는 것이다. 따라서 패킷을 캡처하는 tcpdump의 기본 기능을 spoofing으로 분류하면 안 된다.

③ O: tcpdump는 인터페이스에서 수집한 패킷의 주소·포트·프로토콜 등 정보를 표시하거나 파일에 저장하여 네트워크 통신 상태를 분석하는 데 사용한다. 예를 들어 통신 요청과 응답이 관찰되는지, 특정 연결에 어떤 패킷이 오가는지를 확인할 수 있다. 실제 관찰 범위는 캡처 지점과 권한·설정에 따라 달라진다.

④ O: tcpdump는 **libpcap의 패킷 캡처 기능**을 이용한다. libpcap이 운영체제별 캡처 기능에 접근하는 공통 인터페이스를 제공하고, tcpdump는 이렇게 얻은 패킷을 필터 조건에 따라 수집·해석하여 표시한다.

NoteBase

문 5. 다음은 웹 취약점 보완을 위한 특수 문자 필터링에 대한 특수 문자이다. XSS 취약점 공격에 사용되지 않는 특수 문자를 모두 고른 것으로 가장 적절한 것은?

가. < 나. = 다. ; 라. & 마. ? 바. *

① 가, 나, 다

② 가, 라, 마

③ 나, 다, 바

④ 나, 마, 바

정답 3번

간단한 해설

이 문항은 **HTML·URL에서 쓰는 문자**와 **SQL 구문에서 쓰는 문자**를 구분하는 분류 문제이다. 다만 '사용되지 않는'은 이 문항의 분류에 한정되며 실제 XSS 공격 코드에 해당 문자가 전혀 등장하지 않는다는 뜻은 아니다.

출제 포인트

XSS 관련 특수 문자의 역할을 구분하고, 정답표가 적용한 문자 분류에 맞는 조합을 판단한다.

핵심 개념

XSS는 신뢰할 수 없는 입력이 웹 페이지에서 악성 스크립트로 해석되어 사용자의 브라우저에서 실행되는 취약점이다. SQL 삽입은 입력이 데이터베이스 질의의 일부로 해석되어 질의를 변조하는 취약점이다.
가 '<': HTML 태그를 시작하는 문자이다.
라 '&': HTML 문자 참조를 시작하며, URL의 질의 매개변수를 구분할 때도 쓰인다.
마 '?': URL에서 질의 문자열의 시작을 나타낸다. 악성 입력을 URL의 매개변수로 전달하는 반사형 XSS와 연결해 이해할 수 있다. '?' 자체가 스크립트를 실행시키는 것은 아니다.
나 '=': SQL의 동등 비교에 쓰인다.
다 ';': SQL 명령문의 종료·구분에 쓰인다.
바 '*': SQL에서 모든 열을 지정하거나 곱셈 연산에 쓰인다.
이 문항의 정답표는 가·라·마를 XSS 관련 문자로, 나·다·바를 그 밖의 문자로 분류한다. 이는 문자의 대표적인 용도를 나눈 것으로, SQL 문자와 XSS 문자가 서로 배타적인 집합이라는 뜻은 아니다.

NoteBase

선지별 해설

① X
가 '<'는 태그를 시작하므로 이 문항에서 제외할 문자이다. 나·다는 유지하되 가를 바 '*'로 바꾸어 나·다·바로 고친다.

② X
가 '<', 라 '&', 마 '?'는 정답표의 분류에서 XSS 관련 쪽에 놓인 문자이다. 요구된 조합과 반대이므로 나 '=', 다 ';', 바 '*'의 조합으로 고친다.

③ O
나 '='는 SQL의 비교 연산, 다 ';'는 명령문 종료·구분, 바 '*'는 모든 열 지정이나 곱셈에 쓰인다. 이 문항의 분류에서 XSS 관련 쪽에 놓이지 않은 문자들을 모두 모은 조합이다. 실제 공격 코드에서 이 문자들을 사용할 수 없다는 뜻은 아니다.

④ X
나·바는 맞지만 마 '?'가 포함되고 다 ';'가 빠졌다. 마를 다로 바꾸어 나·다·바로 고친다.

오답 포인트

'사용되지 않는'을 문자 자체의 절대적인 안전성으로 받아들이면 안 된다. 실제로 '='는 HTML 속성의 값 지정에도, ';'는 JavaScript 문장이나 HTML 문자 참조에도 쓰이고, '*'는 JavaScript 연산에도 쓰인다. 정답표의 단순 분류와 실제 공격 구문에서의 사용 가능성을 구분해야 한다.

다시 나오면 이렇게 판단

문자가 어느 문법에서 어떤 역할을 하는지 먼저 확인한다. 이 문항은 HTML·URL 관련 문자와 SQL 관련 문자의 대표적인 용도를 구분해 조합을 비교한다. 실제 XSS 방어는 몇몇 문자를 일괄 삭제하는 것만으로 판단하지 않고, 입력이 들어가는 HTML·JavaScript·URL 문맥에 맞는 인코딩과 검증을 적용한다.

암기 포인트

이 문항의 분류: 태그·문자 참조·질의 시작은 <, &, ? / SQL 비교·명령 종료·전체 열은 =, ;, *. 문자 자체의 안전성을 뜻하는 분류는 아니다.

NoteBase

문 6. 포맷 스트링에 대한 설명으로 가장 적절하지 않은 것은?

① %d: 정수형 10진수 상수

② %s: 문자열

③ %f: 실수형 상수

④ %x: 8진수 양의 정수

정답 4번

간단한 해설

'%x'는 부호 없는 정수를 **16진수**로 표시하는 지정자이다. **8진수**로 표시할 때는 '%o'를 사용한다.

선지별 해설

포맷 스트링은 값의 자료형과 표시 방식을 지정하는 문자열이다. 여기서는 C의 printf 계열에서 길이 수식자 없이 사용하는 기본 변환 지정자를 기준으로 한다.

① O: '%d'는 int 값을 부호 있는 10진수로 출력한다. 정수형 10진수 상수도 출력할 수 있으며, 상수뿐 아니라 정수형 변수나 식의 값에도 사용한다.

② O: '%s'는 문자열을 출력하는 지정자이다. 기본적으로 전달된 문자 배열에서 널 문자 앞까지의 내용을 출력하므로, 문자 하나를 출력하는 '%c'와 구별된다.

③ O: '%f'는 실수 값을 소수점 표기를 이용한 10진수로 출력한다. printf에서는 double 형식의 인수를 사용하며, float 인수도 호출 시 double로 승격된다. 실수형 상수 외에 실수형 변수의 값도 출력할 수 있다.

④ X: '%x'는 부호 없는 정수를 **16진수**로 출력하며, 10~15에 해당하는 숫자는 a~f로 나타낸다. **8진수 출력은 '%o'**에 해당한다. 또한 부호 없는 정수에는 0도 포함되므로 양의 정수만을 뜻하지 않는다.

따라서 '%x'를 8진수와 연결한 ④가 가장 적절하지 않다.

NoteBase

문 7. 침입탐지시스템(IDS)의 기능으로 가장 적절하지 않은 것은?

① 정보 수집

② 정보 가공 및 축약

③ 침입 방지 및 분석

④ 보고 및 조치

정답 3번

간단한 해설

IDS의 핵심은 수집한 정보에서 **침입 징후를 탐지하고 분석**하는 것이다. 탐지한 공격을 중단시키는 침입 방지 기능은 IPS와 구별되는 지점이며, IDS의 보고·대응 지원과 혼동하지 않아야 한다.

선지별 해설

침입탐지시스템(IDS)의 기본 기능은 감시 자료의 수집, 분석 가능한 형태로의 가공, 침입 징후의 탐지·분석, 결과 보고와 대응 지원으로 정리할 수 있다. 아래 O/X는 각 표현이 이러한 기본 기능 분류에 적합한지를 뜻한다.

① O: 정보 수집은 네트워크 트래픽, 호스트의 감사 기록, 로그인·프로세스 활동 등에서 탐지에 필요한 자료를 확보하는 기능이다. 수집 대상은 네트워크 기반인지 호스트 기반인지에 따라 달라진다.

② O: 정보 가공 및 축약은 수집된 자료를 일관된 형식으로 정리하고 필요한 특징을 추출하거나 관련 사건을 요약하는 기능이다. 많은 원시 자료를 **탐지·분석에 사용할 정보**로 만드는 과정이다.

③ X: 이 단계의 기본 기능은 **침입 탐지 및 분석**이다. 공격 징후를 찾아 침입 가능성을 판단하는 IDS와, 탐지한 공격을 중단시키는 방지 기능을 갖춘 IPS를 구별해야 한다. '분석' 자체는 IDS 기능이지만 이를 '침입 방지'와 묶어 탐지 단계 대신 제시한 표현은 적절하지 않다.

④ O: 보고 및 조치는 탐지 결과를 기록하고 관리자에게 경보·보고를 전달하며, 설정된 대응 절차가 이루어지도록 지원하는 기능이다. 일부 시스템은 다른 보안 장비와 연계해 대응을 요청할 수 있다. 이런 대응 연계가 가능하다는 것과 모든 IDS가 통신 경로에서 공격을 직접 차단하는 IPS라는 것은 다르다.

NoteBase

문 8. 침입탐지시스템(IDS)의 오용 탐지 기법에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. 행위 또는 통계 기반 기법이다.
나. 미리 정의한 rule에 매칭한다.
다. false positive가 낮다.
라. 알려지지 않은 공격에 대응할 수 있다.
마. 대량의 자료를 분석하는 데 부적합하다.
바. false negative가 낮다.

① 가, 다, 라
② 가, 라, 바
③ 나, 다, 라
④ 나, 다, 마

정답 4번

간단한 해설

오용 탐지는 **미리 정의한 공격 규칙**과 대조하므로 알려진 공격에 대한 오탐은 낮은 편이지만, 규칙에 없는 공격을 놓칠 수 있다. 자료와 규칙이 많아지면 반복 대조의 처리 부담도 커진다.

NoteBase

보기별 해설

오용 탐지는 알려진 공격을 규칙이나 시그니처로 정의하고 관찰한 사건과 대조하는 방식이다. 정상 상태의 통계적 특성에서 벗어나는지를 보는 이상 탐지와 판단 기준이 다르다.

가. X: 행위·통계 기반의 정상 프로파일을 만들고 이탈 여부를 판단하는 것은 **이상 탐지**의 대표적인 방식이다. 오용 탐지는 정상 범위가 아니라 이미 알려진 공격 패턴을 기준으로 판단한다.

나. O: 오용 탐지는 패킷·로그 등에서 관찰한 정보를 **미리 정의한 공격 규칙에 매칭**한다. 따라서 알려진 공격의 특징이 규칙에 표현되어 있어야 탐지할 수 있다.

다. O: false positive는 정상 활동을 공격으로 잘못 판단하는 **오탐**이다. 알려진 공격의 구체적인 패턴을 비교하므로, 정상 행동의 변화를 이상으로 의심하는 방식에 비해 오탐이 낮은 편이다. 다만 규칙이 부정확하거나 적용 환경에 맞지 않으면 오탐이 발생할 수 있으며, 오탐이 없다는 뜻은 아니다.

라. X: 기존 규칙에 포착되는 특징이 없는 **미지의 공격을 탐지하는 데 한계**가 있다. 알려지지 않은 공격까지 대응할 수 있다는 일반적 장점은 정상 행동과의 차이를 보는 이상 탐지에 해당한다. 새 공격에 대응하려면 오용 탐지의 규칙 갱신이나 다른 탐지 방식과의 결합이 필요하다.

마. O: 전통적인 규칙 대조 방식의 처리 부담을 지적한 설명이다. 자료가 많고 공격 규칙도 많아지면 다수의 규칙과 반복 비교하는 데 필요한 연산이 증가하여, 대량 자료의 실시간 분석에 병목이 생길 수 있다. 따라서 **대량의 자료·규칙을 대조하는 처리 부담**이 단점이다. 모든 시그니처 기반 제품이 대량 자료를 처리할 수 없다는 절대적 뜻은 아니며, 최적화·병렬화·하드웨어 구성에 따라 처리 능력은 달라진다.

바. X: false negative는 실제 공격을 정상으로 판단하여 놓치는 **미탐**이다. 오용 탐지는 규칙에 없는 공격이나 기존 규칙을 우회한 공격을 놓칠 수 있으므로, 알려진 공격에 대한 낮은 오탐을 전체 공격에 대한 낮은 미탐과 동일시할 수 없다.

옳은 보기는 나, 다, 마이므로 ④의 조합과 일치한다.

NoteBase

문 9. 일반적인 유닉스 또는 리눅스 주요 로그에 대한 설명으로 가장 적절하지 않은 것은?

① btmp: 시스템에 현재 로그인한 사용자에 대한 상태 정보를 기록한다.

② syslog: 사용자 인증과 관련된 로그 및 커널, 데몬에서 생성된 모든 로그를 포함하여 기록한다.

③ history: 사용자별로 수행한 명령을 기록한다.

④ secure: telnet, ftp 등 인증과정을 거치는 모든 로그를 기록한다.

정답 1번

간단한 해설

'btmp'는 **실패한 로그인 시도**를 기록한다. 현재 로그인한 사용자의 상태를 확인하는 기록은 **'utmp'**이다.

선지별 해설

로그의 용도와 실제 저장 설정은 구별해야 한다. 이 문항은 전통적인 유닉스·리눅스 로그의 대표적 역할을 묻고 있으며, 파일 이름과 수집 범위는 운영체제·배포판·설정에 따라 달라질 수 있다.

① X: 'btmp'는 로그인에 실패한 내역을 기록하며, 보통 'lastb'로 조회한다. **현재 접속 중인 사용자 정보는 'utmp'**에 해당한다. 과거 로그인·로그아웃 이력을 누적하는 'wtmp'와도 구별된다.

② O: 'syslog'는 인증, 커널, 데몬 등 여러 출처의 메시지를 수집·분류하는 시스템 로깅 체계이다. 선지의 '모든 로그'는 특정 종류에 한정되지 않는 통합 수집 역할을 가리킨다. 실제로 모든 메시지가 하나의 'syslog' 파일에 자동 저장된다는 뜻은 아니며, **기록 대상과 저장 위치는 설정에 의해 결정**된다.

③ O: 셸의 'history'는 사용자가 입력한 명령의 이력을 관리한다. 예를 들어 Bash는 사용자별 이력을 '.bash_history' 파일에 저장할 수 있다. 다만 저장 설정이나 제외 규칙의 영향을 받으므로 모든 프로세스의 활동을 빠짐없이 기록하는 감사 로그와는 다르다.

④ O: 'secure'는 전통적으로 **인증·보안 관련 메시지**를 모으는 로그이다. telnet·ftp 등 서비스의 인증 성공·실패나 계정 접근 관련 기록이 여기에 해당할 수 있다. 이는 인증과 관련된 로그의 용도에 관한 설명으로, 해당 서비스의 모든 통신 내용까지 기록한다는 뜻은 아니다. 실제 기록 여부와 파일 이름은 서비스 및 로깅 설정에 따라 달라진다.

따라서 로그의 역할을 잘못 연결한 것은 ①이다.

NoteBase

문 10. 다음은 CSRF 공격 단계를 나열한 것이다. 순서가 가장 적절한 것은?

가. 사용자가 CSRF 스크립트가 포함된 게시글을 열람한다.
나. 공격자가 CSRF 취약점이 존재하는 임의의 웹 서버에 CSRF 스크립트가 포함된 게시글을 작성한다.
다. 사용자의 정상적인 요청에 의한 것이 아닌, 공격자가 의도한 동작을 수행한다.
라. 서버에서 CSRF 스크립트가 실행된다.

① 가-나-다-라
② 가-나-라-다
③ 나-가-다-라
④ 나-가-라-다

정답 4번

간단한 해설

공격용 게시글이 먼저 준비되어야 사용자가 이를 열람할 수 있다. 열람으로 유발된 **위조 요청을 서버가 처리**한 뒤 공격자가 의도한 결과가 발생한다.

올바른 순서

나 → 가 → 라 → 다

나. 공격자가 CSRF 스크립트가 포함된 게시글을 작성한다. 사용자의 열람을 통해 위조 요청을 유발하려면, 먼저 **공격용 게시글이 준비**되어 있어야 한다.

가. 사용자가 준비된 게시글을 열람한다. 게시글의 스크립트가 사용자 브라우저에서 실행되면 공격자가 의도한 요청이 발생한다. 사용자가 대상 사이트에 로그인해 있고 요청에 세션 쿠키 등 인증정보가 함께 전송되는 경우, 서버는 이를 사용자의 요청으로 받아들일 수 있다.

라. 게시글 열람으로 유발된 요청이 서버에 전달되어 처리되는 단계이다. 원문의 '서버에서 CSRF 스크립트가 실행된다'는 표현은 엄밀하지 않다. 게시글의 **스크립트는 사용자 브라우저에서 실행**되며, 서버는 그 결과 발생한 **위조 요청을 처리**한다. 이 문항의 라는 서버 측 요청 처리 단계로 이해한다.

다. 서버가 위조 요청을 정상 요청으로 받아들이면, 사용자가 의도하지 않은 동작이 사용자의 권한으로 수행된다. 이것이 공격자가 노린 결과이므로, 해당 요청이 서버에 전달되어 처리되는 단계 뒤에 놓인다.

NoteBase

문 11. 응용계층 프로토콜과 잘 알려진 포트번호와의 연결이 가장 적절한 것은?

① HTTPS - 143

② POP3 - 25

③ TFTP - 21

④ DNS - 53

정답 4번

간단한 해설

DNS에는 **53번 포트**가 할당되어 있다. DNS는 이름 관련 정보를 조회하며 UDP와 TCP 모두에서 이 포트를 사용할 수 있다.

선지별 해설

잘 알려진 포트는 서비스에 통상 할당된 서버 측 포트이다. 이 문제는 이러한 기본 대응을 묻는 것이며, 특정 서버가 별도 포트로 설정되었는지를 묻는 것은 아니다.

① X: HTTPS의 기본 포트는 **443번**이다. HTTPS는 HTTP 통신을 암호화된 연결로 보호하며, 143번은 메일 서버의 메시지에 접근하고 관리하는 IMAP의 기본 포트이다.

② X: POP3의 기본 포트는 **110번**이다. POP3는 서버의 전자우편을 가져오는 데 사용하며, 25번은 전자우편 전송에 사용하는 SMTP의 기본 포트이다.

③ X: TFTP의 잘 알려진 포트는 **69번**이다. TFTP는 UDP 기반의 간단한 파일 전송 프로토콜로, 최초 읽기·쓰기 요청을 서버의 69번 포트로 보낸다. 이후 전송에는 정해진 전송 식별자에 해당하는 포트를 사용한다. 21번은 FTP의 제어 연결 포트이다.

④ O: DNS의 기본 포트는 **53번**이다. DNS는 도메인 이름에 대응하는 IP 주소 등 이름 관련 정보를 조회하며, 53번 포트에서 UDP와 TCP를 모두 사용할 수 있다.

따라서 프로토콜과 잘 알려진 포트번호가 바르게 연결된 것은 ④이다.

NoteBase

문 12. AAA 중 가장 일반적인 방법인 ID, 패스워드를 입력하여 자신의 신원(identity)을 시스템에 증명하는 과정으로 가장 적절한 것은?

① Audit Trail

② Authorization

③ Accounting

④ Authentication

정답 4번

간단한 해설

ID와 패스워드로 주장한 신원이 맞는지 확인하는 과정은 **Authentication(인증)**이다. 접근할 수 있는 자원을 정하는 인가, 이용 내역을 남기는 Accounting과 구별된다.

개념 구분

Authentication(인증)은 사용자가 주장하는 신원이 맞는지 확인하는 과정이다. ID는 어느 계정인지 식별하고, 패스워드는 해당 계정의 사용자임을 입증하는 근거로 사용된다. 따라서 **ID 제시는 식별, 패스워드 검증은 인증**으로 구별한다.

Authorization(인가)은 사용자가 어떤 자원에 접근하고 어떤 작업을 할 수 있는지 권한을 판단하는 과정이다. 예를 들어 로그인에 성공하더라도 관리자 전용 기능을 사용할 권한은 없을 수 있다.

Accounting(계정 활동·사용량 기록)은 접속 시간, 사용한 자원, 세션 등의 정보를 기록하여 이용 내역을 추적하는 기능이다. 과금에 활용될 수 있지만 금전 청구만을 뜻하지는 않는다.

Audit Trail(감사 추적 기록)은 누가 언제 어떤 작업을 했는지 사후에 재구성·확인할 수 있게 남긴 기록이다. Accounting과 관련될 수 있으나, 사용자의 신원을 검증하는 과정 자체는 아니다.

AAA는 Authentication, Authorization, Accounting을 가리킨다. 발문처럼 ID와 패스워드를 이용해 신원을 증명하는 과정은 Authentication이므로 ④에 해당한다.

NoteBase

문 13. 악성코드에 대한 설명으로 가장 적절하지 않은 것은?

① 런처: 자신 안에 존재하는 데이터로부터 새로운 파일을 생성하여 공격을 수행한다.

② 랜섬웨어: 사용자의 문서와 사진 등을 암호화시켜 일정 시간 안에 일정 금액을 지불하면 암호를 풀어주는 방식으로 사용자에게 금전적인 요구를 하는 악성코드를 말한다.

③ 익스플로잇: 운영체제나 특정 프로그램의 취약점을 이용하여 공격한다.

④ 봇: DDoS 공격 시 지정된 공격을 수행하도록 하는 악성코드이다.

정답 1번

간단한 해설

자신 안에 포함된 데이터를 풀어 악성 파일을 생성·설치하는 것은 **드로퍼(dropper)**의 대표적 기능이다. 런처(launcher)는 **다른 악성 프로그램을 실행시키는 역할**을 중심으로 구분한다.

선지별 해설

① X: 내부에 포함한 악성코드나 데이터를 파일로 만들어 설치하는 설명은 **드로퍼**에 해당한다. 런처는 다른 악성 프로그램이 실행되도록 구동하는 역할을 한다. 하나의 악성코드가 여러 기능을 함께 가질 수 있지만, 선지가 제시한 '내부 데이터로부터 새 파일 생성'이라는 분류 기준은 드로퍼의 특징이다.

② O: 랜섬웨어는 문서·사진 등을 암호화해 사용하지 못하게 한 뒤 복구를 대가로 금전을 요구하는 악성코드이다. 시간 제한을 두어 피해자를 압박할 수도 있다. 선지의 '지불하면 암호를 풀어주는 방식'은 공격자가 내세우는 거래 조건을 뜻하며, **돈을 지불해도 실제 복구가 보장되지는 않는다**.

③ O: 익스플로잇은 운영체제나 응용 프로그램의 **취약점을 이용하는 공격 코드 또는 기법**이다. 단순히 악성 파일을 실행하는 것과 달리, 소프트웨어의 보안 결함을 이용해 의도하지 않은 동작이나 권한 획득 등을 일으키는 데 초점이 있다.

④ O: 악성 봇은 감염된 기기에서 공격자의 명령을 받아 정해진 작업을 수행한다. 여러 봇을 묶은 봇넷이 동시에 트래픽을 보내면 DDoS 공격에 이용될 수 있다. 다만 봇의 기능이 DDoS에만 한정되는 것은 아니며, 스팸 발송이나 정보 탈취 등에 이용될 수도 있다.

따라서 드로퍼의 특징을 런처에 연결한 ①이 가장 적절하지 않다.

NoteBase

문 14. 어떤 기관의 호스트에 할당된 주소 200.107.16.17/22에 대한 설명으로 가장 적절하지 않은 것은?

① 해당 네트워크 내의 주소 개수는 1024개이다.

② 200.107.16.0/22은 네트워크 주소로서 IP 데이터그램을 목적지로 라우팅하는데 사용된다.

③ 200.107.18.255/22는 마지막 주소로서 해당 네트워크 내 브로드캐스트 주소이다.

④ CIDR을 지원하는 주소 지정 방식이다.

정답 3번

간단한 해설

/22 주소 블록에서 세 번째 옥텟은 16~19 범위에 속한다. 호스트 비트를 모두 1로 만든 브로드캐스트 주소는 **200.107.19.255**이며, 200.107.18.255가 아니다.

선지별 해설

IPv4 주소는 32비트이고 /22는 앞의 22비트가 네트워크 접두부임을 뜻한다. 따라서 호스트 부분은 32 − 22 = 10비트이다. 마스크는 255.255.252.0이며, 세 번째 옥텟의 주소 블록 간격은 256 − 252 = 4이다. 세 번째 옥텟이 16인 이 주소는 16~19 블록에 속하므로 전체 범위는 200.107.16.0~200.107.19.255이다.

① O: 호스트 부분 10비트로 표현할 수 있는 전체 주소 수는 2^{10} = 1,024개이다. 이는 네트워크 주소와 브로드캐스트 주소까지 포함한 수이다. 두 특수 주소를 제외한 통상적인 호스트 할당 가능 주소 수는 1,024 − 2 = 1,022개이므로, **전체 주소 수와 호스트 할당 가능 수**를 구별해야 한다.

② O: 주어진 주소와 /22 마스크를 비트 AND 연산하면 호스트 부분이 모두 0인 200.107.16.0이 된다. 200.107.16.0/22는 이 네트워크 전체를 식별하는 접두부이며, 라우터는 목적지 주소가 어떤 접두부에 속하는지 판단하여 경로를 선택한다. 이 주소를 일반 호스트 한 대에 할당한다는 뜻은 아니다.

③ X: 브로드캐스트 주소는 /22의 **호스트 부분 10비트를 모두 1**로 만든 200.107.19.255이다. 200.107.18.255는 이 블록의 마지막 주소가 아니다. 끝 옥텟이 255라는 사실만으로 브로드캐스트 주소라고 판단할 수 없으며, 세 번째 옥텟에 남아 있는 호스트 비트도 함께 확인해야 한다.

④ O: CIDR은 기존 주소 클래스의 고정 경계 대신 접두부 길이를 명시하여 주소 블록을 나타낸다. 따라서 /22를 붙여 네트워크와 호스트의 경계를 표현한 것은 **클래스 없는 주소 지정 방식**에 해당한다.

NoteBase

문 15. TCP 세그먼트(segment)의 순서 번호(sequence number)에 대한 설명으로 가장 적절한 것은?

① 클라이언트-서버 간 연결 설정 후에 임의의 초기 순서 번호가 할당된다.

② 순서 번호는 해당 세그먼트에 포함된 첫 번째 데이터 바이트의 번호로 정의된다.

③ 순서 번호는 0에서 $2^{16} - 1$의 범위에 있다.

④ 순서 번호의 구조적 문제로 SYN flooding 공격에 영향을 받기 쉽다.

정답 2번

간단한 해설

TCP는 데이터 스트림의 **바이트 단위로 순서 번호**를 부여한다. 일반 데이터 세그먼트의 순서 번호는 그 안에 담긴 첫 번째 데이터 바이트의 번호이며, 이 필드는 **32비트**이다.

선지별 해설

① X: 초기 순서 번호(ISN)는 **연결을 설정하는 과정에서** 각 송신 방향별로 선택되어 SYN과 SYN-ACK을 통해 상대에게 전달된다. 연결 설정이 끝난 뒤에 처음 할당하는 것이 아니다. 양 끝점은 서로 독립된 초기 순서 번호를 사용하여 각 방향의 바이트 스트림을 식별한다.

② O: SYN이 설정되지 않은 일반 데이터 세그먼트의 순서 번호는 **첫 번째 데이터 바이트의 번호**이다. 예를 들어 순서 번호가 1,000인 세그먼트가 데이터 100바이트를 담고 있다면 데이터의 번호는 1,000부터 1,099까지이고, 이어지는 새 데이터는 1,100부터 시작한다. 다만 SYN이 설정된 세그먼트의 순서 번호는 ISN이며, SYN도 번호 공간 하나를 사용하므로 첫 데이터 바이트는 ISN + 1이다.

③ X: TCP의 순서 번호 필드는 16비트가 아니라 **32비트**이다. 표현 범위는 0부터 $2^{32} - 1$까지이고, 번호 계산은 2^{32}를 법으로 순환한다. 선지의 $2^{16} - 1$은 순서 번호 필드의 크기를 잘못 적용한 것이다.

④ X: SYN flooding은 TCP 연결 설정 과정에서 **미완료 연결 상태가 자원을 점유**하는 점을 악용하는 공격이다. 서버가 SYN을 받고 응답한 뒤 최종 확인을 기다리는 반개방 연결이 다수 누적되면 정상 연결을 처리하기 어려워질 수 있다. 순서 번호의 예측 가능성은 세션 위조·가로채기와 관련된 별도의 쟁점이며, SYN flooding의 핵심 원인을 순서 번호의 구조적 문제로 설명하는 것은 적절하지 않다.

NoteBase

문 16. SSH-2(Secure Shell ver. 2) 프로토콜에 대한 옳은 설명을 모두 고른 것으로 가장 적절한 것은?

가. 클라이언트와 서버 간 보안성 있는 연결을 제공하는 범용 프로토콜이다.
나. SSH는 TCP 또는 UDP 위에 안전한 채널 형성을 위한 별도의 전송 프로토콜을 이용한다.
다. 클라이언트에 대한 인증만을 제공하며, 클라이언트와 서버 간 교환되는 메시지의 데이터 무결성을 보장한다.
라. 포트 포워딩(port forwarding)은 일종의 터널링 기능으로 FTP 응용 등에 보안 연결을 제공할 수 있다.

① 가, 나
② 가, 라
③ 나, 다
④ 다, 라

정답 2번

간단한 해설

SSH-2는 **서버 인증과 사용자 인증**을 구분해 제공하며, 통상 TCP와 같은 신뢰성 있는 데이터 스트림 위에서 동작한다. 포트 포워딩으로 다른 응용의 연결도 SSH 터널 안에서 보호할 수 있다.

NoteBase

보기별 해설

SSH-2는 안전하지 않은 네트워크에서 원격 로그인과 여러 네트워크 서비스를 안전하게 이용하도록 하는 프로토콜 체계이다. 전송 계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜이 역할을 나누어 수행한다.

가. O: 클라이언트와 서버 사이에 인증·기밀성·무결성을 제공하는 보안 연결을 구성한다. 원격 명령 실행뿐 아니라 다른 응용의 통신을 전달하는 데도 사용할 수 있어 보안 원격 접속을 위한 범용적인 기능을 제공한다.

나. X: SSH 전송 계층 프로토콜은 보통 TCP 연결 위에서 동작하며, **신뢰성 있는 데이터 스트림**을 전제로 한다. UDP 자체는 데이터의 순서와 전달을 보장하지 않으므로 TCP와 UDP 중 어느 것이든 그대로 이용한다는 설명은 부정확하다. TCP 외의 기반을 쓰더라도 이에 필요한 신뢰성 있는 스트림이 제공되어야 한다.

다. X: SSH는 클라이언트 측 사용자 인증뿐 아니라 **서버 인증도 제공**한다. 전송 계층 프로토콜이 서버 인증·기밀성·무결성을 제공하고, 그 위의 사용자 인증 프로토콜이 클라이언트 측 사용자를 서버에 인증한다. 메시지의 데이터 무결성을 보장한다는 부분은 맞지만 '클라이언트에 대한 인증만'이라는 제한이 틀렸다.

라. O: 포트 포워딩은 특정 TCP 연결의 데이터를 SSH 채널 안으로 전달하는 터널링 기능이다. 이를 이용하면 FTP 같은 응용의 통신도 SSH 터널 구간에서 보호할 수 있다. 다만 FTP는 제어 연결과 데이터 연결이 별도이므로 제어 포트 하나를 전달했다고 전체 파일 전송이 자동으로 보호되는 것은 아니다.

따라서 옳은 보기는 가, 라이며 ②에 해당한다.

NoteBase

문 17. Smurf 공격은 공격자로부터의 패킷을 증폭하는 중간의 경유 네트워크를 필요로 한다. 자신의 네트워크가 Smurf 공격에 이용당하지 않는 방법으로 가장 적절한 것은?

① ICMP echo request 패킷을 필터링한다.

② ICMP echo reply 패킷을 전송하지 않는다.

③ ping 요청에 응답하지 않는다.

④ 외부로부터 수신되는 브로드캐스트 패킷을 필터링한다.

정답 4번

간단한 해설

자기 네트워크가 Smurf 공격의 증폭 경유지가 되지 않으려면 **외부에서 들어오는 IP 지향성 브로드캐스트를 차단**하는 것이 핵심이다. 하나의 요청이 내부 여러 호스트에 전달되어 다수의 응답을 만들지 못하게 한다.

NoteBase

선지별 해설

Smurf 공격은 피해자의 IP 주소를 출발지로 위조한 ICMP echo request를 중간 네트워크의 브로드캐스트 주소로 보내고, 여러 호스트가 피해자에게 응답하게 하는 반사·증폭 공격이다. 이 문항은 피해자의 수신 차단보다 **자기 네트워크가 증폭 경유지로 이용되는 것을 막는 방법**을 비교한다.

① ICMP echo request 필터링: 요청을 차단하면 응답의 발생을 줄여 공격을 억제할 수 있다. 다만 요청 전체를 일괄 차단하면 정상적인 유니캐스트 ping도 제한될 수 있어, 증폭의 원인이 되는 외부 브로드캐스트를 겨냥하는 방법보다 차단 범위가 넓다.

② ICMP echo reply 미전송: 해당 네트워크의 호스트가 응답을 보내지 않으면 반사 트래픽 생성을 억제할 수 있다. 그러나 모든 echo reply를 막는 방식은 정상적인 응답까지 제한하며, 외부 요청이 내부의 여러 호스트로 전달되는 구조 자체를 제거하지는 않는다.

③ ping 요청에 무응답: 호스트가 echo request에 답하지 않도록 하면 그 호스트의 공격 가담을 막는 데 도움이 된다. 다만 네트워크 전체를 보호하려면 적용 대상의 범위를 관리해야 하며, 정상적인 도달 가능성 확인도 영향을 받을 수 있다.

④ 외부 브로드캐스트 패킷 필터링: 경계 라우터에서 외부로부터 들어온 IP 지향성 브로드캐스트가 내부 네트워크로 전달되지 않도록 한다. **한 요청이 다수 호스트의 응답으로 증폭되는 경로**를 차단하므로 중간 네트워크 악용을 직접 막는다. 여기서 브로드캐스트는 외부에서 내부 네트워크의 브로드캐스트 주소를 목적지로 보낸 경우를 가리킨다.

다른 방법들도 적용 범위에 따라 완화 효과가 있지만, 발문이 강조한 네트워크 단위의 증폭 경유지 악용을 가장 직접적으로 겨냥하는 것은 ④이다.

NoteBase

문 18. IPv6에 대한 설명으로 가장 적절하지 않은 것은?

① IPv6 헤더의 '페이로드 길이' 필드는 기본 헤더를 뺀 IPv6 데이터그램의 길이를 포함한다.

② IPv6 데이터그램의 단편화(fragmentation)는 발신지 호스트와 라우터에서 수행할 수 있다.

③ IPv6 헤더의 '홉 제한(hop limit)' 필드는 IPv4의 TTL에 대응된다.

④ 같은 자원의 사용, 같은 종류의 보안 등 동일한 특성을 공유하는 일련의 패킷들에 대한 처리를 지원한다.

정답 2번

간단한 해설

IPv6의 단편화는 **발신지 노드만 수행**하며, 전달 중인 라우터는 단편화하지 않는다. 라우터는 다음 링크의 MTU보다 큰 패킷을 폐기하고 'Packet Too Big' 메시지로 발신지에 알린다.

선지별 해설

① O: '페이로드 길이'는 40바이트의 IPv6 기본 헤더 뒤에 오는 부분의 바이트 수를 나타낸다. 따라서 **확장 헤더가 있으면 그 길이도 포함**하며, 상위 계층 데이터만의 길이를 뜻하지 않는다. IPv4의 전체 길이 필드가 기본 헤더까지 포함하는 것과 구별된다.

② X: IPv6에서는 **발신지 노드만 단편화**할 수 있다. 라우터가 전달할 패킷이 다음 링크의 MTU보다 크면 패킷을 폐기하고 ICMPv6 'Packet Too Big' 메시지를 보낸다. 발신지는 이 정보를 바탕으로 패킷 크기를 줄이거나 필요하면 단편 헤더를 이용해 단편화한다. 전달 중인 라우터가 단편화할 수 있는 IPv4 방식과 다르다.

③ O: '홉 제한'은 IPv4의 TTL에 대응하여 패킷이 네트워크에서 무한히 순환하는 것을 막는다. **패킷을 전달하는 노드를 지날 때마다 1씩 감소**하며, 라우터는 값이 0이 되어 더 전달할 수 없는 패킷을 폐기한다. 이름 그대로 남은 전달 홉 수를 제한하는 필드이다.

④ O: IPv6의 '흐름 레이블(Flow Label)'은 일련의 패킷을 같은 흐름으로 식별하여 일관되게 처리할 수 있도록 지원한다. 같은 특성을 공유하는 패킷을 흐름 단위로 구분하는 데 활용할 수 있다는 뜻이다. 다만 레이블 자체가 자원 예약이나 암호화·보안 수준을 자동 보장하는 것은 아니며, 실제 처리는 네트워크의 정책과 기능에 달려 있다.

따라서 라우터도 단편화를 수행한다고 한 ②가 가장 적절하지 않다.

NoteBase

문 19. 다음 <보기 1>의 보안을 위한 프로토콜과 <보기 2>의 설명을 순서대로 나열한 것으로 가장 적절한 것은?

<보기 1>
가. IPSec 나. VPN 다. PGP 라. IEEE 802.1X

<보기 2>
㉠ 포트 기반으로 네트워크에의 접근을 통제하기 위한 프로토콜이며 LAN에서 주로 사용한다.
㉡ IP 데이터그램 단위의 암호화/인증을 제공하며 응용의 변경없이 이용할 수 있다.
㉢ 인터넷을 이용한 가상의 사설망으로 보안을 제공하기 위한 암호와 특별한 프로토콜을 사용하는 컴퓨터들의 집합이다.
㉣ 전자우편에 프라이버시(privacy), 무결성, 인증을 제공하기 위한 프로토콜로서 안전한 전자우편 메시지 생성에 사용할 수 있다.

① 가: ㉡, 나: ㉠, 다: ㉣, 라: ㉢
② 가: ㉡, 나: ㉢, 다: ㉣, 라: ㉠
③ 가: ㉢, 나: ㉣, 다: ㉠, 라: ㉠
④ 가: ㉢, 나: ㉠, 다: ㉣, 라: ㉡

정답 2번

간단한 해설

IPSec은 **IP 데이터그램을 보호하는 기술**이고, VPN은 **공중망 위에 논리적인 사설 연결을 구성**하는 개념이다. VPN을 구현할 때 IPSec을 이용할 수 있지만 두 용어의 설명 대상은 다르다.

NoteBase

대응 관계 해설

가. IPSec → ㉡: IPSec은 **IP 계층에서 데이터그램을 보호**하는 보안 체계이다. 암호화에 의한 기밀성과 인증·무결성 보호 등을 제공하며, 응용 프로그램마다 별도의 보안 기능을 구현하지 않고도 적용할 수 있다. 다만 실제 제공 서비스는 사용하는 프로토콜과 설정에 따라 달라지므로 모든 IPSec 통신이 반드시 암호화되는 것은 아니다.

나. VPN → ㉢: VPN은 인터넷과 같은 공중망 위에서 **논리적인 사설 연결**을 구성하는 방식이다. 제시된 설명은 암호화와 터널링 등의 기술로 외부망에서도 보호된 통신을 제공하는 보안 VPN을 뜻한다. IPSec은 이를 구현하는 데 사용할 수 있는 기술 중 하나이므로, VPN이라는 네트워크 구성 개념과 IPSec이라는 보호 기술을 구별한다.

다. PGP → ㉣: PGP는 전자우편 등의 메시지에 암호화와 전자서명을 적용하여 보호한다. **암호화는 내용의 기밀성**을, **전자서명은 무결성과 발신자 인증**을 제공하는 데 사용된다. 따라서 안전한 전자우편 메시지를 만든다는 설명에 대응한다.

라. IEEE 802.1X → ㉠: IEEE 802.1X는 LAN의 **포트 기반 네트워크 접근 통제**를 위한 표준이다. 접속하려는 장치나 사용자의 인증·권한 확인에 따라 네트워크 이용을 허용하는 방식이다. 여기서 포트는 TCP·UDP 서비스 번호를 뜻하는 것이 아니라 LAN 접속을 통제하는 접근 지점이다.

가·나·다·라의 대응은 ㉡·㉢·㉣·㉠이므로 선택지 ②와 일치한다.

NoteBase

문 20. 패킷의 발신지 IP 주소를 공격대상의 IP 주소로 변경하여 전송하는 공격들을 모두 고른 것으로 가장 적절한 것은?

가. LAND 공격
나. Smurf 공격
다. DNS spoofing 공격
라. TCP 세션 하이재킹

① 가, 나
② 가, 나, 다
③ 가, 나, 라
④ 가, 다, 라

정답 3번

간단한 해설

LAND와 Smurf는 **피해자의 IP 주소를 발신지로 위조**하며, TCP 세션 하이재킹도 정상 통신 당사자를 사칭할 때 그 주소를 사용한다. DNS spoofing의 핵심은 피해자의 발신지 주소 사용이 아니라 **거짓 DNS 정보를 믿게 하는 것**이다.

NoteBase

보기별 해설

가. O: LAND 공격은 패킷의 발신지 IP 주소와 목적지 IP 주소를 모두 **공격대상 호스트의 주소**로 설정하는 형태이다. 전통적인 LAND 패킷은 발신지·목적지 포트도 같게 만들어, 취약한 시스템이 자신에게서 온 것처럼 보이는 요청을 처리하도록 한다. 따라서 발신지 IP 주소를 피해자의 주소로 위조한다는 조건에 해당한다.

나. O: Smurf 공격은 ICMP Echo Request의 발신지 IP 주소를 **피해자 주소로 위조**하고, 이를 응답이 증폭될 수 있는 네트워크의 브로드캐스트 주소로 보낸다. 요청을 받은 여러 호스트의 응답이 위조된 발신지인 피해자에게 모이면서 통신 자원을 소모시킨다. 여기서 요청 패킷의 발신지는 피해자이고, 목적지는 증폭에 이용되는 네트워크의 브로드캐스트 주소이다.

다. X: DNS spoofing은 **DNS 응답이나 이름-주소 대응 정보를 위조**하여 잘못된 주소를 믿게 하는 공격이다. 응답 패킷의 발신지를 위조하는 방식에서는 정상 DNS 서버처럼 가장할 수 있으나, 피해 클라이언트 자신의 IP 주소를 발신지로 설정하는 것이 이 공격의 핵심 조건은 아니다. 피해자 주소를 발신지로 넣는 DNS 반사·증폭 공격과도 구별해야 한다.

라. O: TCP 세션 하이재킹은 이미 형성된 연결의 정상 통신 상대인 것처럼 패킷을 주입하여 세션을 가로채는 공격이다. 정상 클라이언트를 사칭해 서버로 보내는 패킷은 **가로채기 대상 클라이언트의 IP 주소를 발신지**로 사용하며, 해당 연결에 맞는 포트와 순서 번호 등의 조건도 충족해야 한다. IP 주소만 바꾼다고 가로채기가 성립하는 것은 아니지만, 이처럼 피해 통신 당사자의 주소를 사칭하는 형태가 발문의 조건에 해당한다.

해당하는 보기는 가, 나, 라이므로 ③의 조합과 일치한다.

NoteBase

문 21. 버퍼 오버플로(buffer overflow)에 취약한 함수들을 모두 고른 것으로 가장 적절한 것은?
가. fscanf() 나. gets() 다. strncat() 라. snprintf()

① 가, 나
② 가, 라
③ 나, 다
④ 다, 라

정답 1번

간단한 해설

gets()는 입력 길이 제한 인자가 없고, fscanf()의 문자열 입력도 **필드 폭을 제한하지 않으면** 버퍼를 넘길 수 있다. strncat()와 snprintf()는 길이 제한 인자를 제공하지만 **실제 버퍼에 맞게 지정해야** 오버플로를 방지할 수 있다.

보기별 해설

이 문항은 대표적인 무제한 문자열 입력 함수와 명시적인 길이 제한 인자를 받는 함수를 비교한다. 아래 O/X는 이 비교에서 취약 입력 함수로 분류되는지를 나타낸다. 실제 버퍼 오버플로 발생 여부는 호출 방법과 버퍼 크기에 달려 있으므로 함수 이름만으로 항상 안전하거나 항상 위험하다고 단정할 수는 없다.

가. O: fscanf()에서 %s나 %[변환을 **필드 폭 제한 없이** 사용하면 입력 길이에 따라 저장 버퍼를 넘길 수 있다. 버퍼 크기를 별도 인자로 전달하는 방식은 아니다. 다만 문자열 저장 시 널 종료 문자 공간을 남긴 적절한 최대 필드 폭을 지정하면 입력 길이를 제한할 수 있다.

나. O: gets()는 한 줄을 읽으면서 목적지 버퍼의 크기를 전달받지 않는다. **입력 길이를 제한할 인자가 없으므로** 버퍼보다 긴 입력에 의해 오버플로가 발생할 수 있다.

다. X: strncat()는 추가할 문자 수의 상한을 인자로 받아 길이를 제한할 수 있는 함수이다. 그러나 그 값은 목적지 버퍼의 전체 크기가 아니다. 유효하게 널 종료된 목적지 문자열을 전제로, **남은 공간에서 종료 문자 1바이트를 뺀 범위** 안에서 추가량을 정해야 한다. 이 계산이 잘못되면 strncat()도 버퍼를 넘길 수 있다.

라. X: snprintf()는 저장할 최대 크기를 인자로 받는다. 0보다 큰 올바른 크기를 지정하면 널 종료 문자를 포함하여 그 범위 안에 출력한다. 지정 크기가 실제 버퍼 크기를 넘지 않아야 하며, 출력이 잘렸는지도 반환값으로 확인해야 한다.

따라서 명시적 길이 제한 인터페이스와 대비되는 대표적인 취약 입력 함수는 가·나로 묶이며, 이 비교 관점에서 ①에 해당한다.

NoteBase

문 22. 쿠키(cookies)에 관한 설명으로 가장 적절하지 않은 것은?

① 웹 서버는 클라이언트에 대한 정보를 기억할 목적으로 클라이언트로 전송하는 HTTP 응답 메시지의 'Set-Cookie' 헤더에 쿠키를 포함할 수 있다.

② 클라이언트가 웹 서버로부터 쿠키를 받으면, 브라우저는 도메인 서버 이름으로 정렬되는 쿠키 디렉터리에 쿠키를 저장한다.

③ 만료 날짜가 있어 일정 기간이 지나면 자동으로 삭제된다.

④ 쿠키는 XSS, CSRF, HTTP GET flooding 등의 공격에 악용될 수 있다.

정답 4번

간단한 해설

HTTP GET flooding은 **대량의 GET 요청으로 서버 자원을 소진**시키는 공격이며 **쿠키 악용이 필수인 공격은 아니다**. 쿠키 탈취나 자동 전송을 이용하는 XSS·CSRF와 공격 원리를 구분한다.

출제 포인트

쿠키의 전달·저장·만료 특성과 쿠키를 악용하는 공격의 원리를 구분하는 문제이다.

핵심 개념

쿠키는 서버가 브라우저에 저장하도록 보내는 작은 데이터로, 이후 요청에서 사용자를 식별하거나 상태를 이어 가는 데 쓰인다. 서버는 응답의 Set-Cookie 헤더로 쿠키를 설정하고 브라우저는 전송 조건에 맞는 쿠키를 요청의 Cookie 헤더에 담는다. 로그인 상태를 식별하는 쿠키가 대표적인 예이다.
XSS는 웹 페이지에 삽입된 악성 스크립트가 사용자 브라우저에서 실행되는 공격이고 CSRF는 로그인한 사용자가 의도하지 않은 요청을 보내도록 유도하는 공격이다. HTTP GET flooding은 GET 요청을 대량으로 보내 서비스를 방해하는 공격이다.

NoteBase

선지별 해설

① O: 서버는 HTTP 응답의 Set-Cookie 헤더로 쿠키를 브라우저에 전달할 수 있다. 브라우저가 이후 요청에 쿠키를 보내면 서버는 이를 이용해 사용자를 식별하거나 이전 상태를 이어 간다.
② O: 브라우저는 받은 쿠키를 저장하고 해당 서버의 도메인과 연결해 관리한다. 이 문항의 '도메인 서버 이름으로 정렬되는 쿠키 디렉터리'는 이러한 도메인별 관리를 설명한 표현이다. 다만 실제 저장 위치와 파일·데이터베이스 구조는 브라우저 구현에 따라 다르며 특정 디렉터리 구조가 HTTP 표준의 필수 요건은 아니다.
③ O: 만료 시각이나 유효기간을 설정한 쿠키는 그 기간이 끝나면 브라우저의 쿠키 저장소에서 제거된다. Expires는 만료 시각을, Max-Age는 유효기간을 지정한다. 이 설명은 만료를 설정한 쿠키에 해당하며 두 속성이 없는 세션 쿠키까지 모두 정해진 만료 날짜를 갖는 것은 아니다.
④ X: XSS로 스크립트에서 접근 가능한 쿠키를 탈취하거나 CSRF로 브라우저의 인증 쿠키 자동 전송을 악용할 수 있다는 부분은 적절하다. 그러나 HTTP GET flooding까지 같은 원리의 쿠키 악용 공격으로 묶은 부분은 적절하지 않다. 이를 'HTTP GET flooding은 대량의 GET 요청으로 서버 자원을 소진시키는 서비스 거부 공격이며 쿠키 없이도 성립한다'로 고친다. 공격 요청에 쿠키가 포함될 수 있다는 사실과 쿠키 악용이 공격의 핵심이라는 설명은 구별한다.

오답 포인트

④의 XSS·CSRF가 쿠키와 관련 있다는 이유로 뒤에 붙은 HTTP GET flooding까지 함께 받아들이기 쉽다. 요청에 쿠키가 실릴 가능성만으로 모든 HTTP 공격을 쿠키 악용 공격으로 분류할 수는 없다.

다시 나오면 이렇게 판단

공격이 무엇을 이용해 피해를 만드는지 확인한다. XSS는 악성 스크립트 실행, CSRF는 사용자 인증 상태를 이용한 요청 위조, GET flooding은 대량 요청에 따른 자원 소진으로 구분한다. 쿠키의 만료 설명에서는 만료 속성이 설정되었는지도 함께 확인한다.

암기 포인트

응답은 Set-Cookie, 요청은 Cookie이다. XSS는 스크립트, CSRF는 인증된 요청, GET flooding은 요청 폭주이다.

NoteBase

문 23. 다음 용어에 대한 설명 중 가장 적절하지 않은 것은?

① PCB(Process Control Block): 특정 프로세스에 대한 정보를 보관하는 일종의 테이블로서 부모와 자식 프로세스는 PCB를 공유한다.

② 샌드박스(sandbox): 기본적으로 시스템과 다른 애플리케이션에 접근하는 것을 통제하기 위해 사용한다.

③ SetGID: SetGID가 설정된 파일을 실행하면 해당 파일이 실행되는 동안 파일을 소유한 그룹의 권한으로 실행된다.

④ HKEY_CURRENT_USER: 윈도우 운영체제의 레지스트리의 하나로서 윈도우가 설치된 컴퓨터 환경 설정에 대한 정보를 저장한다.

정답 1번

간단한 해설

부모와 자식은 서로 다른 프로세스이므로 **각자의 PCB**를 가진다. 자식이 부모의 속성을 일부 상속하거나 자원을 공유할 수 있다는 사실은 PCB 자체를 공유한다는 뜻이 아니다.

선지별 해설

① X: PCB는 운영체제가 각 프로세스의 식별자, 실행 상태, CPU 문맥, 스케줄링 정보 등을 관리하는 자료구조이다. 부모와 자식은 서로 다른 식별자와 실행 상태를 가지므로 **PCB도 각각 따로 존재**한다. 프로세스 생성 과정에서 정보를 복사·상속하거나 열린 파일 같은 일부 자원을 공유하는 것과 PCB 공유는 구별해야 한다.

② O: 샌드박스는 프로그램을 제한된 환경에서 실행하여 파일·장치·네트워크 등 시스템 자원과 다른 프로그램에 대한 접근을 통제하는 방식이다. 프로그램에 허용된 권한과 자원을 제한하여 문제가 생겨도 영향이 밖으로 확산되는 것을 줄인다. 모든 접근을 없애는 것이 아니라 **정해진 정책에 따라 허용 범위를 제한**한다.

③ O: 실행 파일의 SetGID가 적용되면 실행 프로세스의 **유효 그룹 ID**가 그 파일의 소유 그룹으로 설정되어 해당 그룹 권한을 사용한다. 사용자의 실제 그룹 자체가 바뀌는 것은 아니다. 이 설명은 SetGID 실행이 허용되는 일반적인 경우이며, 보안 설정에 따라 해당 비트가 무시될 수 있다.

④ O: HKEY_CURRENT_USER는 컴퓨터 사용 환경 중 **현재 사용자의 설정**을 저장하는 레지스트리 키이다. 사용자별 환경 변수, 화면 색상, 프린터, 응용 프로그램의 개인 설정 등이 해당한다. 선지의 '컴퓨터 환경 설정'은 이 사용자별 환경의 범위로 이해해야 하며, 컴퓨터 전체에 공통으로 적용되는 하드웨어·소프트웨어 설정은 HKEY_LOCAL_MACHINE과 구별된다.

따라서 부모와 자식이 PCB를 공유한다고 한 ①이 가장 적절하지 않다.

NoteBase

문 24. 다음 취약점을 갖는 응용 프로토콜과 그 취약점을 이용한 공격을 연결한 것으로 가장 적절한 것은?

제어 명령 전달을 위한 연결과 데이터 전달을 위한 연결이 분리되어 있는 응용 프로토콜이며 파일 전송을 요청한 클라이언트와 실제 파일을 수신하는 클라이언트가 다를 수 있는 취약점이 존재한다.

① HTTP - Anonymous 공격

② FTP - Bounce 공격

③ FTP - Redirect 공격

④ TFTP - Hijacking 공격

정답 2번

간단한 해설

제어 연결과 데이터 연결이 분리되는 프로토콜은 **FTP**이다. 데이터 연결의 목적지를 제3자로 지정할 수 있는 기능을 악용하여 FTP 서버를 중계 지점으로 쓰는 것이 **Bounce 공격**이다.

대응 관계 해설

프로토콜의 대응: **제어 연결과 데이터 연결을 분리**하여 사용하는 것은 FTP이다. 제어 연결은 로그인·파일 전송 요청 등 명령과 응답을 주고받고, 별도의 데이터 연결은 파일 내용이나 목록을 전달한다. 따라서 명령을 보낸 상대와 데이터 연결의 상대가 달라질 수 있다는 단서가 FTP의 제3자 전송 기능과 연결된다.

공격의 대응: **FTP 서버를 경유해 제3자에게 연결하게 하는 공격**이 Bounce 공격이다. 데이터 연결의 목적지를 제어 연결의 상대와 다르게 지정할 수 있고 서버가 이를 제한하지 않으면, 공격자가 FTP 서버를 중계 지점으로 악용할 수 있다. 이 문제는 제3자 전송 자체를 항상 악성이라고 보는 것이 아니라, 그 기능의 부적절한 허용을 이용하는 취약점을 묻는다.

다른 연결의 구별: HTTP는 이 지문의 FTP식 제어·데이터 연결 분리 구조에 해당하지 않는다. 익명 접근인 anonymous와 경로·목적지 재지정을 가리키는 redirect라는 명칭만으로는 제시된 제3자 전송 악용을 특정할 수 없다. TFTP는 UDP를 사용하는 단순 파일 전송 프로토콜로 FTP와 같은 별도 제어·데이터 TCP 연결을 두지 않으며, hijacking은 기존 통신을 가로채는 공격을 가리킨다.

따라서 응용 프로토콜과 공격의 연결은 FTP - Bounce 공격이며 ②와 일치한다.

NoteBase

문 25. 웹 서버의 보안을 강화하기 위한 조치로 가장 적절하지 않은 것은?

① Acunetix와 같은 스캐너를 이용하여 웹 서버의 보안취약점을 점검하고 대응한다.

② 웹 서버 관리자는 최소 권한을 갖도록 설정한다.

③ 웹 서버는 사용자가 입력하는 입력 값에 대한 유효성을 검증할 필요가 있다.

④ VPN에 웹 서버를 배치하여 외부의 공격을 최대한 차단한다.

정답 4번

간단한 해설

VPN은 **인증된 사용자와의 통신을 보호**하는 기술이지 웹 서버의 취약점 공격을 일괄 차단하는 기술은 아니다.
일반적인 공개 웹 서버는 내부망과 분리된 **DMZ에 배치하고 접근을 통제**한다.

출제 포인트

웹 서버 보안 조치의 목적을 구분하고 VPN의 통신 보호 기능을 서버 배치와 공격 차단 기능으로 혼동하지 않는지를 묻는다.

핵심 개념

VPN은 공용망을 통해 사설망에 안전하게 접속하도록 인증과 암호화된 통신 경로를 제공하는 가상사설망이다.
DMZ는 외부에 공개하는 서버를 내부망과 분리해 두는 네트워크 구역이다.
VPN은 접속과 전송 과정의 보호에, DMZ는 공개 서버와 내부망의 분리에 초점을 둔다. DMZ도 배치만으로 안전해지는 것은 아니며 방화벽의 접근 통제와 서버 자체의 보안 설정이 필요하다.

NoteBase

선지별 해설

① O: Acunetix는 웹 애플리케이션의 보안취약점을 탐지하는 스캐너이다. 점검으로 발견한 취약점을 수정하고 보안 설정을 보완하면 공격 가능성을 줄일 수 있다. 스캔 결과를 확인하는 데 그치지 않고 대응하는 것이 필요하다.
② O: 최소 권한 원칙은 업무에 필요한 권한만 부여하는 것이다. 웹 서버 관리자에게 관리 업무에 필요한 권한만 주면 계정이 탈취되거나 관리자가 실수했을 때 피해 범위를 줄일 수 있다. 최소 권한은 관리 권한을 없앤다는 뜻이 아니다.
③ O: 사용자 입력은 신뢰할 수 없으므로 서버에서 허용된 형식, 길이, 범위에 맞는지 검증해야 한다. 브라우저에서만 검사하면 공격자가 이를 우회할 수 있다. 입력 검증은 필요한 방어 조치이며 그 자체로 모든 웹 공격을 막는 것은 아니다.
④ X: 'VPN에 웹 서버를 배치하여 외부의 공격을 최대한 차단한다'는 VPN의 기능과 공개 웹 서버의 배치 원칙을 혼동한 설명이다. 일반적인 공개 웹 서버는 DMZ에 배치하고 방화벽으로 필요한 통신만 허용하도록 고친다. VPN은 관리자 원격 접속이나 내부용 웹 서비스의 제한된 접속에 사용할 수 있지만 웹 서버의 취약점을 제거하거나 허용된 접속을 통한 공격까지 자동으로 차단하지는 않는다.

오답 포인트

④의 '외부의 공격을 최대한 차단한다' 때문에 VPN을 웹 공격 차단 장치로 생각하기 쉽다. 암호화된 경로로 들어오는 요청에도 악성 입력이 포함될 수 있으므로 통신 경로가 안전하다는 사실과 서버가 공격에 안전하다는 사실을 구분한다.

다시 나오면 이렇게 판단

선지의 보안 기술이 무엇을 보호하는지 먼저 확인한다. 취약점 점검은 결함 발견, 최소 권한은 피해 범위 제한, 입력 검증은 부적절한 입력 거부, DMZ는 공개 서버와 내부망 분리, VPN은 인증된 접속과 통신 보호에 대응한다.

암기 포인트

공개 서버의 분리는 DMZ, 안전한 사설망 접속은 VPN이다.

NoteBase

문 26. 다음에 설명하는 사회공학적기법으로 가장 적절한 것은?

· 사용자가 웹브라우저에 정확한 웹페이지 주소를 입력하였으나 가짜 웹페이지로 유도되어 진짜 사이트로 오인한다.
· 사용자가 특별한 의심없이 진짜 사이트로 생각하고 입력하는 모든 개인정보 등은 쉽게 유출될 수 있다.

① 보이스 피싱
② 메신저 피싱
③ 스미싱
④ 파밍

정답 4번

간단한 해설

정확한 주소를 입력해도 가짜 사이트로 유도되어 개인정보를 빼앗기는 것이 파밍이다. 사용자가 주소를 잘못 입력한 것이 아니라 접속 대상이 바뀌었다는 점이 핵심이다.

공통 해설

파밍은 사용자가 정상적인 웹사이트 주소를 입력했는데도 가짜 사이트로 접속하도록 유도하여 개인정보 등을 탈취하는 기법이다. 사용자는 원래 사이트에 접속했다고 믿지만, 가짜 사이트에 입력한 정보는 공격자에게 넘어갈 수 있다.

지문의 '정확한 웹페이지 주소를 입력하였으나 가짜 웹페이지로 유도'된다는 설명이 **파밍을 식별하는 기준**이다. 전화나 메신저·문자메시지로 사용자를 속였다는 설명이 아니라, 정상 주소를 입력한 뒤 가짜 사이트에 접속하여 정보를 입력한다는 상황이므로 파밍에 해당한다.

NoteBase

문 27. SSL에 관한 설명으로 가장 적절하지 않은 것은?

① SSL은 IPSec과는 달리 HTTP에만 적용 가능하여 HTTPS 프로토콜의 구현에 사용된다.

② SSL은 Handshake, Change Cipher Spec, Alert, Record 프로토콜 등으로 구성된다.

③ SSL Handshake 프로토콜은 RSA 공개키 암호 알고리즘을 사용한다.

④ SSL Record 프로토콜은 TCP 위에서 동작하며 응용 데이터를 암호화한다.

정답 1번

간단한 해설

SSL은 **응용 프로토콜에 독립적**이므로 HTTP 이외의 통신에도 적용할 수 있다. HTTPS는 SSL 계열 보안을 HTTP에 적용한 사용 형태이지, SSL의 유일한 적용 대상은 아니다.

선지별 해설

SSL은 응용 프로토콜과 TCP 같은 신뢰성 있는 전송 프로토콜 사이에서 통신을 보호하는 구조이다. Handshake는 인증·알고리즘·키 설정을 담당하고, Record는 협상된 방식으로 실제 데이터를 보호한다.

① X: SSL은 **HTTP에만 한정되지 않는다**. HTTP에 적용한 대표적인 사용 형태가 HTTPS이며, 다른 응용 프로토콜의 통신에도 적용할 수 있다. IPSec이 IP 계층을 보호한다는 차이를 SSL의 HTTP 전용성으로 바꾸어 설명하면 안 된다.

② O: 전통적인 SSL 구조에는 Handshake, Change Cipher Spec, Alert, Record 프로토콜이 있다. Handshake는 보안 매개변수를 협상하고, Change Cipher Spec은 이후 레코드에 새 설정을 적용함을 알리며, Alert는 오류·종료 등을 통지한다. 이들 메시지와 응용 데이터는 Record를 통해 운반된다.

③ O: SSL Handshake에서 **RSA 방식이 선택된 경우** RSA 공개키 암호를 인증과 키 교환에 이용한다. 예를 들어 클라이언트는 공유 비밀을 만드는 데 쓸 값을 서버의 공개키로 암호화해 보낼 수 있다. 다만 SSL이 RSA만 지원하거나 모든 연결에서 반드시 RSA를 사용한다는 뜻은 아니며, 다른 키 교환 방식도 지원한다.

④ O: SSL Record는 TCP와 같은 신뢰성 있는 전송 서비스 위에서 동작한다. 응용 데이터를 레코드 단위로 처리하고, 암호화가 협상된 연결에서는 **대칭키 암호**로 데이터를 암호화하며 무결성도 보호한다. 이는 Handshake에서 수행하는 공개키 기반 설정 과정과 구별된다.

NoteBase

문 28. 리눅스 보안에 관한 설명으로 가장 적절하지 않은 것은?

① nmap은 로컬 호스트나 원격의 서버가 사용 중인 포트와 운영 체제를 스캔할 수 있다.

② 시스템 관리자는 날짜가 오래된 로그 파일을 백업 후 삭제할 필요가 있다.

③ nmap은 네트워크 주소를 지정하여 특정 네트워크 전체를 스캔할 수 없다.

④ 일반 사용자 계정에서의 로그 파일에 대한 접근은 보안상 제한하는 것이 바람직하다.

정답 3번

간단한 해설

nmap은 단일 호스트뿐 아니라 **CIDR 표기나 IP 주소 범위로 지정한 네트워크**도 스캔할 수 있다. 따라서 네트워크 전체를 대상으로 지정할 수 없다는 설명이 잘못되었다.

선지별 해설

① O: nmap은 호스트의 포트 상태를 조사하고, 네트워크 응답의 특징을 분석하여 운영체제를 추정하는 기능을 제공한다. 원격 서버도 검사 대상이 될 수 있다. 다만 방화벽·권한·응답 상태 등에 영향을 받으므로 모든 포트나 운영체제를 항상 정확히 알아내는 것은 아니다.

② O: 로그가 계속 쌓이면 저장 공간이 부족해질 수 있으므로 관리자는 로그 순환 정책에 따라 오래된 로그를 백업·보관하고 정리할 필요가 있다. 이때 **보존기간과 사고 조사상 필요를 충족한 기록**을 대상으로 해야 하며, 단지 날짜가 오래되었다는 이유로 필요한 증거를 무조건 삭제한다는 뜻은 아니다.

③ X: nmap은 **네트워크 대역 전체를 대상으로 지정**할 수 있다. CIDR 방식의 네트워크 주소와 접두사 길이, IP 주소 범위, 호스트 목록 등을 지원하므로 여러 호스트를 연속해서 검사할 수 있다. 대역을 지정할 수 있다는 기능과, 그 대역의 모든 호스트가 실제 응답하여 식별된다는 보장은 구별된다.

④ O: 로그에는 사용자 활동이나 시스템 구성 등 민감한 정보가 포함될 수 있으므로 일반 사용자에게 필요한 범위를 넘는 접근 권한을 주지 않는 것이 바람직하다. 특히 임의 수정·삭제를 막아 **로그의 무결성**을 보호해야 하며, 읽기 권한도 로그의 민감도와 업무상 필요에 따라 제한한다.

따라서 nmap의 네트워크 대역 스캔 기능을 부정한 ③이 가장 적절하지 않다.

NoteBase

문 29. SSO(Single Sign On)에 관한 설명으로 가장 적절하지 않은 것은?

① 사용자가 한 번의 인증으로 인터넷 및 인트라넷 간 응용 프로그램을 별도의 인증 없이 이용할 수 있다.

② 사용자는 먼저 인증 서버에 접속하여 인증을 받은 후 응용 서버에 서비스를 요청한다.

③ 인증 서버에서 응용 서버로 사용자 인증정보를 전달할 때 보안 취약점이 발생할 수 있다.

④ 중앙집중관리를 통한 효율적인 관리가 가능하다.

정답 2번

간단한 해설

응용 서버에서 시작하는 SSO에서는 **서비스 요청이 먼저**이고 인증이 필요하면 인증 서버로 이동한다. 인증 서버에 먼저 접속한다는 순서를 SSO의 공통 절차로 볼 수는 없다.

출제 포인트

SSO의 인증 공유 기능과 서비스 요청·인증 처리의 순서를 구분하는 문제이다.

핵심 개념

SSO는 한 번 인증한 결과를 연동된 여러 응용 프로그램에서 이용해 반복 로그인을 줄이는 방식이다. 인증 서버는 사용자 신원을 확인하고 응용 서버는 그 인증 결과를 확인하여 서비스를 제공한다.
응용 서버에서 시작하는 방식에서는 서비스 요청 → 인증 서버로 이동 → 사용자 인증 → 응용 서버의 인증 결과 확인 순서로 진행된다. 이미 유효한 인증 상태라면 다시 로그인하지 않아도 된다.

NoteBase

선지별 해설

① O: SSO에 연동된 인터넷·인트라넷 응용 프로그램은 한 번의 로그인으로 이용할 수 있다. '별도의 인증 없이'는 사용자가 매번 로그인 정보를 다시 입력하지 않는다는 의미이며 응용 서버의 인증 결과 확인까지 생략한다는 뜻은 아니다.

② X: '먼저 인증 서버에 접속하여 인증을 받은 후 응용 서버에 서비스를 요청한다'는 순서를 SSO의 공통 절차로 제시한 부분이 부적절하다. 응용 서버에서 시작하는 방식에서는 사용자가 먼저 응용 서버에 서비스를 요청하고 인증이 필요하면 인증 서버로 이동해 인증받는다. 따라서 이 방식의 순서는 '응용 서버에 서비스 요청 → 인증 서버에서 인증 → 응용 서버가 인증 결과를 확인하여 서비스 제공'으로 고친다. 다만 인증 서버에서 시작하는 방식도 있으므로 선지의 순서 자체가 모든 구현에서 불가능한 것은 아니다.

③ O: 인증 서버의 인증정보를 응용 서버로 전달할 때 보호가 부족하면 탈취나 위조 등의 보안 취약점이 발생할 수 있다. SSO를 사용해도 인증정보 전달 과정의 보안은 필요하다.

④ O: 인증을 중앙에서 관리하면 여러 응용 프로그램의 사용자 인증과 인증 정책을 일관되게 관리할 수 있어 관리 효율이 높아진다.

오답 포인트

②에서 인증이 서비스 이용에 필요하다는 사실과, 인증 서버 접속이 최초 서비스 요청보다 반드시 앞선다는 설명을 혼동하기 쉽다. 서비스 요청은 인증보다 먼저 발생할 수 있고 실제 서비스 제공은 인증 결과를 확인한 뒤 이루어진다.

다시 나오면 이렇게 판단

한 번의 인증 결과를 여러 연동 서비스가 이용하는지 확인한다. 접속 순서를 묻는 선지는 응용 서버에서 시작하는지, 인증 서버에서 시작하는지에 따라 판단한다.

암기 포인트

SSO는 인증 결과 공유이다. 응용 서버에서 시작하면 서비스 요청 → 인증 → 서비스 제공 순서이다.

NoteBase

문 30. 다음 용어에 대한 설명 중 가장 적절하지 않은 것은?

① TCB(Trusted Computing Base): 컴퓨터 시스템의 신뢰성, 안전성, 효율성을 높이기 위해 시스템을 종합적으로 분석/평가하는 솔루션이다.

② DLP(Data Loss Prevention): 조직 내의 중요한 자료가 외부로 빠져나가는 것을 탐지하여 차단하는 보안 솔루션이다.

③ NAC(Network Access Control): 단말기가 조직 내부 네트워크에 접속을 시도할 때 사용자 인증을 수행하고 백신 설치와 관련한 무결성을 점검한다.

④ Salt: 패스워드의 해시에 사용하는 난수의 일종으로 운영체제별로 다양한 알고리즘이 존재한다.

정답 1번

간단한 해설

TCB는 시스템을 분석·평가하는 솔루션의 이름이 아니다. 시스템의 **보안 정책을 집행하는 하드웨어·펌웨어·소프트웨어 보호 기구의 집합**을 뜻한다.

선지별 해설

① X: TCB(Trusted Computing Base)는 **보안 정책 집행을 책임지는 신뢰 기반**이다. 접근 제어처럼 시스템 보안이 의존하는 하드웨어·펌웨어·소프트웨어 구성요소와 보호 기구가 함께 포함된다. 성능이나 효율성까지 종합적으로 분석·평가하는 별도 솔루션을 뜻하지 않으므로, 선지는 평가 도구와 보호 기구의 집합을 혼동했다.

② O: DLP(Data Loss Prevention)는 중요 정보의 부적절한 외부 전송·공유 등을 식별하여 **정보 유출을 예방·통제**하는 솔루션이다. 자료의 내용과 정책을 대조하여 경고·차단 등의 조치를 할 수 있다. 모든 자료의 이동을 무조건 막는다는 의미가 아니라 조직이 보호하도록 정한 정보와 반출 조건을 관리하는 것이다.

③ O: NAC(Network Access Control)는 네트워크 접속을 시도하는 사용자·단말의 인증 결과와 **단말의 보안 상태**를 바탕으로 접근을 허용하거나 제한한다. 백신 설치·동작·업데이트 상태와 보안 패치 등의 점검은 이러한 보안 상태 검사에 해당한다. 기준에 미달하는 단말은 접속을 제한하거나 격리하여 보완하도록 할 수 있다.

④ O: 솔트(salt)는 패스워드를 해시할 때 함께 입력하는 **무작위성이 있는 추가 값**이다. 계정별로 서로 다른 솔트를 사용하면 같은 패스워드라도 저장되는 해시가 달라지게 하여, 미리 계산한 해시 표를 여러 계정에 재사용하는 공격을 어렵게 한다. 솔트 자체가 해시 알고리즘은 아니며, 이를 이용하는 패스워드 해싱 알고리즘과 저장 방식은 운영체제·구현에 따라 다를 수 있다. 솔트는 일반적으로 해시와 함께 저장하며 비밀 암호키처럼 숨겨야 하는 값은 아니다.

NoteBase

문 31. 윈도우 운영체제에서의 네트워크 관리 명령어에 대한 설명으로 가장 적절하지 않은 것은?

① ipconfig /flushdns: dns 캐시 정보를 삭제한다.

② netstat -r: 로컬 호스트의 라우팅 테이블을 보여준다.

③ ping -f 사이트 주소: ‘Ctrl+c’로 중지할 때까지 사이트 주소에 ping을 실행한다.

④ tracert 사이트 주소: 최종 수신지에 도달하기까지 중간에 경유하는 라우터 경로 및 응답 시간을 보여준다.

정답 3번

간단한 해설

Windows의 ping에서 계속 요청을 보내는 옵션은 **'-t'**이다. '-f'는 **IPv4 패킷의 단편화 금지**를 지정하는 옵션이다.

선지별 해설

① O: 'ipconfig /flushdns'는 **로컬 컴퓨터의 DNS 해석 캐시**를 비우고 초기화한다. 이전 이름 조회의 결과가 남아 생긴 문제를 점검할 때 사용하며, DNS 서버의 원본 레코드를 삭제하는 명령은 아니다.

② O: 'netstat -r'는 로컬 호스트의 IP 라우팅 테이블을 표시한다. 목적지 네트워크로 보낼 패킷이 사용할 게이트웨이와 인터페이스 등의 정보를 확인할 수 있으며, 'route print'와 같은 용도의 조회이다.

③ X: Windows에서 사용자가 중지할 때까지 ICMP 에코 요청을 계속 보내는 옵션은 **'-t'**이다. 따라서 'ping -t 사이트 주소'가 제시된 동작에 해당하고 Ctrl+C로 종료한다. **'-f'는 IPv4 패킷의 단편화 금지(DF) 비트**를 설정하는 옵션이며, 경로 MTU 문제를 점검하는 데 사용한다.

④ O: 'tracert'는 TTL 값을 단계적으로 늘린 탐색 메시지와 각 홉의 응답을 이용해 목적지까지의 경로를 확인한다. 표시되는 시간은 해당 홉까지 다녀오는 왕복 응답 시간이며, 인접한 두 라우터 사이만의 지연 시간이 아니다. 일부 라우터가 응답하지 않으면 '*'가 나타날 수 있어 모든 홉이 반드시 표시되는 것은 아니다.

따라서 반복 실행 옵션과 단편화 금지 옵션을 혼동한 ③이 가장 적절하지 않다.

NoteBase

문 32. 다음 윈도우XP 운영체제 부팅에 대한 설명으로 가장 적절한 것은?

· 기본 파일 시스템 정보가 들어있다.
· 저장 매체의 첫 번째 섹터(LBA)에 위치하는 512 바이트 영역이다.
· 부팅 가능한 파티션이 없으면 미리 정의된 오류 메시지를 출력한다.
· 운영 체제를 부팅할 때 저장 매체의 첫 번째 섹터를 호출하면 해당 부트 코드를 수행한다.
· 부트 코드의 주 역할은 파티션 테이블에서 부팅 가능한 파티션을 찾아 해당 파티션의 부트 섹터를 호출한다.

① CMOS 로딩
② MBR 로딩
③ POST 실행
④ WBM(Window Boot Manager) 실행

정답 2번

간단한 해설

저장 매체의 **첫 번째 512바이트 영역**에 있고, 파티션 테이블에서 **부팅 가능한 파티션을 찾아 그 부트 섹터로 제어를 넘기는 것**은 MBR의 역할이다.

NoteBase

구성 요소별 해설

지문은 Windows XP의 전통적인 BIOS·MBR 방식 부팅을 설명한다. MBR은 디스크 앞부분에 있는 마스터 부트 레코드로, 부트 코드와 파티션 테이블 등을 포함한다.

기본 정보: MBR의 파티션 테이블에는 파티션의 위치·크기·유형과 활성 여부 등이 기록된다. 지문의 '기본 파일 시스템 정보'는 이러한 파티션 식별 정보를 중심으로 이해한다. **파일 시스템의 세부 구조를 담는 볼륨 부트 섹터와 MBR은 구별**된다.

위치와 크기: 지문에서 제시한 512바이트 영역은 저장 매체의 첫 번째 논리 섹터, 즉 **LBA 0의 MBR**이다. CMOS 설정 저장 영역이나 운영체제의 일반 실행 파일을 가리키는 것이 아니다.

부팅 실패 처리: 파티션 정보를 확인해도 정상적으로 부팅할 대상을 찾지 못하면 다음 부트 단계로 진행할 수 없다. 지문의 오류 메시지 설명은 이 초기 부팅 실패 처리를 가리키며, 구체적인 메시지와 처리 방식은 BIOS와 부트 코드 구현에 따라 달라질 수 있다.

부트 코드 실행: BIOS가 부팅 장치의 첫 섹터를 메모리로 읽어 들이고 그 안의 MBR 부트 코드에 제어를 넘기면, MBR 코드가 실행된다. MBR 로딩은 단순한 설정 조회가 아니라 다음 부트 단계를 준비하는 코드의 로딩·실행과 연결된다.

파티션 부트 섹터 호출: MBR 코드는 파티션 테이블에서 활성 파티션을 찾아 **그 파티션의 부트 섹터를 읽고 실행**한다. 이 과정이 디스크 전체의 첫 섹터인 MBR과 각 파티션의 첫 섹터인 볼륨 부트 레코드의 관계를 보여 준다.

CMOS는 부팅 장치 순서 등 하드웨어 설정과 관련되고, POST는 전원 인가 후 하드웨어를 점검하는 과정이다. Windows Boot Manager는 이후 Windows 계열의 부트 관리 구성 요소이며, 전통적인 Windows XP 부팅에서는 NTLDR가 사용된다. 따라서 제시된 특징의 조합에 해당하는 것은 ② MBR 로딩이다.

NoteBase

문 33. 윈도우 운영체제에서 백도어가 이용하는 csrss.exe 프로세스에 대한 설명으로 가장 적절한 것은?

① 작업표시줄, 바탕화면 등 사용자 셸을 지원하는 프로세스이다.

② 시스템 백업이나 업데이트 등을 작업하는 스케줄러 프로세스이다.

③ winlogin 서비스에 필요한 인증 프로세스이다.

④ 윈도우 콘솔을 관장하고 스레드를 생성 및 삭제하며 32비트 가상 MS-DOS 모드를 지원하는 프로세스이다.

정답 4번

간단한 해설

csrss.exe는 구형 Win32 하위 시스템에서 **콘솔과 스레드 관련 기능을 지원**하는 핵심 프로세스이다. 사용자 셸, 작업 스케줄러, 로그인 인증의 역할과 구별해야 한다.

NoteBase

개념 구분

csrss.exe는 Client/Server Runtime Subsystem의 사용자 모드 프로세스이다. 구형 Windows의 Win32 하위 시스템에서 **콘솔 처리와 스레드 생성·삭제 지원** 등의 역할을 맡았으며, DOS 가상 실행 환경을 지원하는 일부 기능에도 관여했다.

④의 가상 MS-DOS 지원은 실행 환경과 담당 프로세스를 나누어 이해해야 한다. 32비트 Windows에서 DOS 실행 환경의 기반이 되는 프로세스는 ntvdm.exe이며, 16비트 Windows 응용과 16비트·32비트 DOS 응용을 지원한다. CSRSS가 이 환경의 일부를 지원한다는 것과 CSRSS 자체가 DOS 실행기라는 것은 다르다.

역할은 Windows 버전에 따라 달라진다. 예를 들어 Windows 7부터 콘솔 호스트 기능은 CSRSS에서 분리되어 conhost.exe가 맡게 되었다. 따라서 구형 하위 시스템의 역할 설명을 모든 최신 Windows에 그대로 적용해서는 안 된다.

다른 선택지와의 구분: ① X: 작업표시줄·바탕화면 등 사용자 셸은 주로 explorer.exe의 역할이다.

② X: 예약된 작업을 실행하는 작업 스케줄러의 기능이다.

③ X: 로그인 인증은 주로 LSASS와 인증 구성 요소의 역할이며, CSRSS의 대표 기능을 설명한 것이 아니다.

발문의 백도어 이용은 정상 프로세스 이름을 사칭하거나 정상 구성 요소를 악용할 수 있다는 보안 맥락이다. **정상 csrss.exe 자체가 곧 백도어라는 뜻은 아니다**.

④ O: 이처럼 프로세스의 역할을 구별하면 구형 Win32 하위 시스템의 콘솔·스레드 및 가상 실행 환경 지원을 설명한 ④가 CSRSS와 연결된다.

NoteBase

문 34. 어셈블리 명령어에 대한 설명으로 가장 적절하지 않은 것은?

① CMP: 산술 연산 명령이며 데이터의 두 값을 비교할 때 사용한다.

② JMP: 제어 전송 명령이고 점프 명령(분기)이며 프로그램 실행 주소 또는 레이블로 이동할 때 사용한다.

③ LEA: 데이터 전송 명령이며 스택에서 데이터를 삭제할 때 사용한다.

④ STC: 프로세서 제어 명령이고 피연산자 없이 사용하며 EFLAGS 레지스터의 CF 값을 설정할 때 사용한다.

정답 3번

간단한 해설

LEA는 주소 지정식의 **유효 주소를 계산하여 레지스터에 저장**하는 명령이다. 이를 스택에서 데이터를 꺼내는 명령으로 설명한 것이 적절하지 않다.

선지별 해설

① (O) **CMP는 두 피연산자를 비교**하는 산술 명령이다. 내부적으로 첫 번째 값에서 두 번째 값을 뺀 것처럼 플래그를 갱신하지만, 뺄셈 결과를 피연산자에 저장하지는 않는다. 이후 조건 분기 명령은 이 플래그를 이용하여 두 값의 관계를 판단할 수 있다.

② (O) **JMP는 무조건 분기**를 수행하는 제어 전송 명령이다. 지정된 주소나 레이블에 해당하는 위치로 실행 흐름을 옮긴다. 조건에 따라 분기 여부를 결정하는 조건 분기 명령과 구별된다.

③ (X) **LEA는 유효 주소 계산**에 사용되는 데이터 전송 명령이다. 메모리 주소 지정식으로 계산한 주소 값을 목적 레지스터에 저장하며, 그 주소의 메모리 내용을 읽어 오는 명령도 아니다. 스택의 맨 위 데이터를 꺼내고 스택 포인터를 조정하는 동작은 POP에 해당한다. POP 역시 메모리의 비트를 지운다는 뜻은 아니므로, 선지의 '삭제'는 스택에서 논리적으로 제거한다는 의미로 구별해야 한다.

④ (O) **STC는 캐리 플래그 CF를 1로 설정**하는 프로세서 제어 명령이다. 명시적인 피연산자 없이 실행되어 EFLAGS 레지스터의 CF를 설정한다. CF를 0으로 지우는 CLC와 구별된다.

NoteBase

문 35. 랜섬웨어에 대한 설명으로 가장 적절한 것은?

① CryptoLocker: 감염되면 파일 확장자가 .locker로 변경되며 바탕화면과 텍스트 파일로 복구 관련 메시지를 출력한다.

② CryptXXX: 정상 rundll32.exe를 svchost.exe 이름으로 복사한다.

③ Locky: 윈도우 운영체제의 SMB(Server Message Block)를 이용하여 악성코드를 감염시킨다.

④ WannaCry: 실행 파일이 아닌 동적 링크 라이브러리(DLL) 형태로 유포한다.

정답 2번

간단한 해설

CryptXXX는 **rundll32.exe를 svchost.exe라는 이름으로 복사**한 뒤 악성 DLL을 실행하는 방식이 확인되었다. 파일 이름은 svchost.exe이지만 실제 실행에 이용되는 프로그램은 rundll32.exe이다.

선지별 해설

랜섬웨어는 파일 등을 암호화해 사용할 수 없게 한 뒤 복구 대가를 요구하는 악성코드이다. 여기서는 각 계열의 알려진 대표 동작을 구별하며, 확장자와 유포 방식이 변종마다 달라질 수 있다는 점을 전제로 한다.

① X: CryptoLocker에 감염되면 파일 확장자가 일률적으로 '.locker'가 된다는 연결은 부정확하다. 국내에서 분석된 CryptoLocker 계열에는 원래 파일명에 **'.encrypted'를 덧붙이는 사례**가 있다. 복구 관련 메시지를 보여 주는 행위는 여러 랜섬웨어에서 나타나므로 그것만으로 계열을 특정할 수 없다.

② O: CryptXXX는 **정상 rundll32.exe를 svchost.exe라는 이름으로 복사**해 악성 DLL을 실행하는 방식이 확인되었다. svchost.exe라는 이름으로 보이는 파일이 실제로는 이름을 바꾼 rundll32.exe라는 점이 핵심이다. 정상 실행 파일을 악성 DLL 구동에 악용하는 경우이다.

③ X: SMB 취약점을 이용해 다른 컴퓨터로 확산한 대표적인 랜섬웨어는 **WannaCry**이다. Locky는 송장 등으로 위장한 이메일 첨부 문서의 악성 매크로나 스크립트를 통해 유입되는 방식으로 알려져 있다. 두 계열의 대표 감염 경로를 바꿔 연결했다.

④ X: 실행 파일 대신 DLL 형태로 유포되고 rundll32.exe를 이용해 동작한다는 설명은 이 문항에서는 **CryptXXX**의 특징에 해당한다. WannaCry는 실행 파일을 포함한 악성코드로 동작하며 SMB 취약점을 이용하는 웜 방식의 확산이 대표 특징이다. 내부에 DLL이 있다는 사실과 DLL 형태의 유포를 계열의 대표 특징으로 삼는 것은 구별된다.

따라서 랜섬웨어와 대표 동작을 바르게 연결한 것은 ②이다.

NoteBase

문 36. 보안 커널의 기능 중 참조 모니터(reference monitor)에 대한 설명으로 가장 적절하지 않은 것은?

① 프로세스와 파일의 정보 흐름을 감시하는 보안 모듈이다.

② 객체에 대한 접근통제 기능을 수행한다.

③ 액세스 권한을 변경하는 등 보안 관리기능을 수행할 때 신뢰할 수 있는 경로를 제공해야 한다.

④ 감사, 식별, 인증 및 보안 매개변수 설정 등과 같은 다른 보안 메커니즘과 데이터를 교환하면서 상호작용을 한다.

정답 3번

간단한 해설

참조 모니터는 **주체의 객체 접근을 보안 정책에 따라 중재**하는 기능이다. 사용자가 보안 관리 기능과 안전하게 통신하도록 하는 것은 **신뢰 경로(trusted path)**의 기능이다.

선지별 해설

참조 모니터는 프로세스 같은 주체가 파일 같은 객체에 접근할 때 권한을 검사하는 추상적 보안 개념이며, 이를 구현하는 핵심 구성 요소가 보안 커널이다. 모든 관련 접근을 거쳐야 하고, 임의 변경으로부터 보호되며, 정확성을 분석·검증할 수 있어야 한다.

① O: 프로세스가 파일을 읽거나 쓰는 등의 접근을 중재하여 보안 정책에 어긋나는 정보 흐름을 통제한다. 여기서 감시는 사건을 사후에 기록하는 데 그치지 않고, **접근 시점에 허용 여부를 검사**하는 역할을 포함한다.

② O: 참조 모니터의 핵심은 **객체에 대한 접근통제**이다. 요청한 주체와 대상 객체, 요청 연산, 적용되는 보안 정책을 확인하여 해당 접근을 허용하거나 거부한다.

③ X: 액세스 권한 변경 같은 보안 관리 작업에서 사용자와 시스템의 보안 기능 사이에 안전한 통신 수단을 제공하는 설명은 **신뢰 경로**에 해당한다. 신뢰되지 않는 프로그램이 그 경로를 가장하거나 개입하지 못하도록 하는 기능이다. 참조 모니터가 권한 변경 요청의 접근 권한을 검사할 수는 있지만, 그것과 사용자에게 신뢰할 수 있는 경로를 제공하는 기능은 구별된다.

④ O: 실제 접근통제 구현은 식별·인증으로 확인된 주체 정보와 설정된 보안 매개변수를 이용하고, 접근 결정이나 보안 사건을 감사 기능에 전달하는 등 다른 보안 기능과 연계된다. 이러한 데이터 교환이 참조 모니터가 인증·감사 기능 전체를 직접 수행한다는 뜻은 아니다.

따라서 참조 모니터의 기능과 신뢰 경로의 기능을 혼동한 ③이 가장 적절하지 않다.

NoteBase

문 37. 블루투스 보안 취약점에 대한 설명으로 가장 적절한 것은?

① blueprinting: 블루투스 장치가 서로 한 번 연결되면 그 이후에는 별다른 인증절차 없이 자동으로 서로 연결되는 인증 취약점을 악용한 것으로 10미터 이내의 거리에서 블루투스 기기에 전화 걸기, 불특정 번호로 SMS 보내기, 주소록 읽기 및 쓰기 등을 실행할 수 있다.

② bluejacking: 서비스 발견 프로토콜(SDP:Service Discovery Protocol)을 통해 블루투스 장치를 검색하고 모델을 확인한다.

③ bluebugging: 사용자들은 블루투스를 통해서 스팸 메시지들을 보낸다. 메시지들은 피해가 없는 광고와 스팸메시지 등이다.

④ bluesnarfing: 블루투스 장치끼리 인증없이 간편하게 정보를 교환하도록 개발된 OPP 기능을 사용하여 블루투스 장치에 있는 주소록 등의 내용을 요청하여 열람하거나 취약한 장치의 파일에 접근할 수 있다.

정답 4번

간단한 해설

블루스나핑(bluesnarfing)은 **취약한 블루투스 장치의 정보를 무단으로 읽어 오는 공격**이다. OPP의 잘못된 접근 통제 구현을 악용하면 주소록 등의 정보가 유출될 수 있다.

NoteBase

선지별 해설

블루투스 공격은 장치 식별, 원치 않는 메시지 전송, 기기 제어, 정보 탈취 중 어떤 행위를 하는지에 따라 구별한다.

① X: 전화 걸기, 문자 전송, 주소록 조작처럼 취약한 기기를 제어하는 것은 **블루버깅(bluebugging)**의 특징이다. 블루프린팅(blueprinting)은 장치의 서비스 정보 등을 분석하여 제조사나 모델을 식별하는 기법이다. 정상적인 페어링 후 저장된 키를 이용하는 재연결 자체가 곧 취약점인 것은 아니며, 공격 가능 거리도 모든 장치에서 10미터로 고정되는 것은 아니다.

② X: SDP로 제공 서비스의 특성을 조사하여 장치를 식별하는 것은 **블루프린팅**이다. 블루재킹(bluejacking)은 블루투스를 통해 상대방이 요청하지 않은 메시지나 명함 등을 보내는 행위이다.

③ X: 원치 않는 광고·스팸 메시지를 보내는 것은 **블루재킹**이다. 블루버깅은 취약점을 이용하여 기기에 명령을 실행시키거나 통화·메시지 등의 기능을 무단으로 제어하는 공격이다. 블루재킹 메시지가 직접 기기를 장악하지 않더라도 피싱이나 악성 행동을 유도할 수 있으므로 항상 무해하다고 일반화할 수는 없다.

④ O: 블루스나핑은 취약한 장치의 OPP·OBEX 처리 과정에서 발생하는 접근 통제 결함을 이용해 주소록 등 내부 정보를 무단으로 얻는 공격이다. 핵심은 **허용되지 않은 정보에 접근할 수 있는 잘못된 구현**이다. 인증 없이 객체를 주고받는 기능 자체만으로 모든 장치에서 정보 탈취가 가능한 것은 아니며, 올바르게 구현된 OPP와 취약한 장치를 구별해야 한다.

NoteBase

문 38. 윈도우 운영체제에서 ARP spoofing 공격을 막기 위하여 MAC 주소를 고정하는 네트워크 명령어로 가장 적절한 것은?

· IPv4 주소: 203.237.128.40
· MAC 주소: AA-BB-CC-DD-A0-B0

① route ADD 203.237.128.40 AA-BB-CC-DD-A0-B0
② route CHANGE 203.237.128.40 AA-BB-CC-DD-A0-B0
③ arp - d 203.237.128.40 AA-BB-CC-DD-A0-B0
④ arp - s 203.237.128.40 AA-BB-CC-DD-A0-B0

정답 4번

간단한 해설

Windows의 **'arp -s'**는 IPv4 주소와 MAC 주소의 대응을 정적 ARP 항목으로 등록한다. 올바른 대응을 고정하면 해당 항목이 거짓 ARP 정보로 바뀌는 것을 막는 데 도움이 된다.

핵심 풀이

ARP는 같은 링크에서 IPv4 주소에 대응하는 MAC 주소를 알아내는 데 사용된다. ARP 스푸핑은 거짓 대응 정보를 보내 통신 상대의 ARP 캐시를 오염시키는 공격이므로, 이 문제에서는 지정된 IP·MAC 대응을 **정적 항목으로 추가**하는 기능을 찾아야 한다.

주어진 IPv4 주소는 203.237.128.40이고 MAC 주소는 AA-BB-CC-DD-A0-B0이다. 이를 지정하는 명령의 표준 표기는 'arp -s 203.237.128.40 AA-BB-CC-DD-A0-B0'이다. '-s' 뒤에 IP 주소, 그다음에 연결할 MAC 주소를 둔다. 여기서 고정하는 것은 네트워크 카드 자체의 MAC 주소가 아니라 **ARP 캐시의 IP·MAC 대응 관계**이다.

'route ADD'는 IP 경로를 추가하고 'route CHANGE'는 기존 경로를 변경한다. 둘 다 라우팅 테이블을 다루므로 MAC 주소 대응을 고정하는 명령이 아니다. 'arp -d'는 지정된 ARP 항목을 삭제하는 옵션이므로 정적 등록과 다르다.

따라서 정적 ARP 항목을 추가하는 ④가 해당한다. 이 대응은 올바른 MAC 주소를 확인하여 설정해야 하며, 하나의 항목을 고정하는 것만으로 네트워크 전체의 모든 위조 공격이 차단되는 것은 아니다. 또한 'arp -s'의 항목은 TCP/IP가 재시작되면 제거될 수 있으므로 영구 보존과도 구별한다.

NoteBase

문 39. HTTP Response의 상태 코드 '301'에 대한 설명으로 가장 적절한 것은?

① bad request

② moved permanently

③ not modified

④ not implemented

정답 2번

간단한 해설

HTTP 301은 요청한 자원이 **새 URI로 영구 이동**했음을 나타낸다. 클라이언트가 이후 요청에 새 주소를 사용하도록 안내하는 상태 코드이다.

개념 구분

301 Moved Permanently: 요청한 자원에 **새로운 영구 URI가 부여되었음**을 나타내는 리다이렉션 상태 코드이다. 서버는 일반적으로 Location 헤더에 이동할 URI를 제시하며, 이후 요청에는 새 URI를 사용하도록 안내한다.

400 Bad Request: 요청 문법이나 메시지 형식 등 클라이언트 측 문제 때문에 서버가 요청을 처리할 수 없거나 처리하지 않는 경우이다. 자원이 이동했다는 의미가 아니다.

304 Not Modified: 조건부 GET 또는 HEAD 요청에서 검사한 표현이 변경되지 않아, 클라이언트가 저장한 표현을 재사용할 수 있음을 알린다. **주소의 영구 이동이 아니라 캐시 재검증**과 관련된다.

501 Not Implemented: 서버가 요청 수행에 필요한 기능을 지원하지 않는 경우이다. 예를 들어 서버가 요청 메서드를 인식하지 못하고 어느 자원에 대해서도 지원할 수 없는 상황이 해당한다.

따라서 301의 설명은 'moved permanently'인 선택지 ②와 일치한다.

NoteBase

문 40. 다음에 설명하는 구글검색엔진의 검색 파라미터를 제시한 것들로 가장 적절한 것은?

· 특정 도메인으로 지정한 사이트에서 검색하려는 문자열이 포함된 사이트를 찾는다.
· 페이지 제목에 검색하는 문자가 들어있는 사이트를 찾는다.
· 특정 파일 유형에 한해 검색하는 문자가 들어있는 사이트를 찾는다.

① cache, inurl, link

② cache, filetype, intitle

③ filetype, link, site

④ filetype, intitle, site

정답 4번

간단한 해설

검색 범위를 지정한 사이트로 제한하는 것은 **site**, 페이지 제목을 조건으로 삼는 것은 **intitle**, 파일 유형을 제한하는 것은 **filetype**이다. 세 연산자를 모두 포함한 묶음을 고르면 된다.

대응 관계 해설

첫째 설명 → **site**. 검색 결과를 지정한 도메인이나 사이트 범위로 제한한다. 검색어가 포함된 페이지를 인터넷 전체에서 찾는 대신, 지정한 사이트 안에서 찾는 조건이다.

둘째 설명 → **intitle**. 검색어가 페이지 제목에 들어 있는 결과를 찾는다. URL에 검색어가 들어 있는지를 제한하는 inurl과 구별된다.

셋째 설명 → **filetype**. 검색 대상을 PDF 등 지정한 파일 유형으로 제한한다. 제목에 포함된 단어나 사이트의 도메인이 아니라 결과 파일의 형식을 기준으로 삼는다.

세 설명에 대응하는 연산자는 **site, intitle, filetype**이다. 이 문제는 설명 순서대로 배열한 선지가 아니라 세 연산자를 모두 포함한 묶음을 고르는 문제이므로, filetype, intitle, site를 제시한 ④가 적합하다. ①은 이 세 연산자를 모두 빠뜨리고, ②는 site가 없으며, ③은 intitle이 없다.

NoteBase