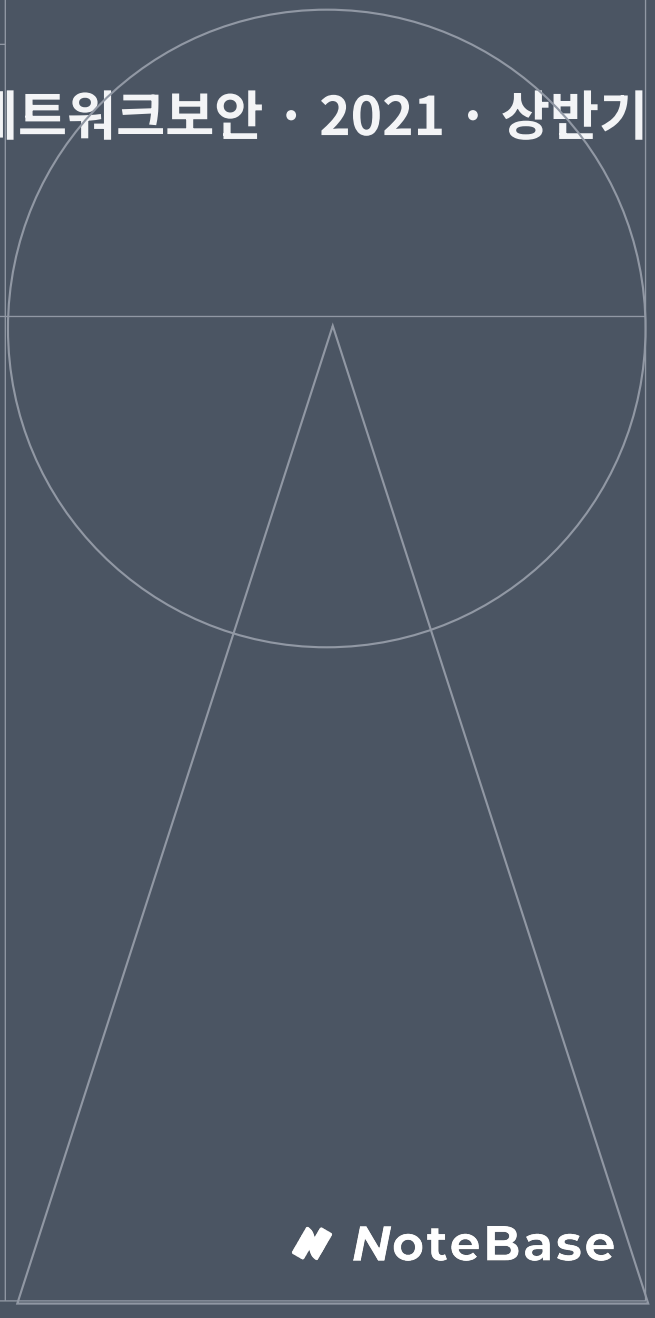
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2021 · 상반기



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2021 · 상반기

공무원/해경/일반직 9급 · 네트워크보안 · 2021 · 상반기

문 1. 다음 <보기>의 ㉠, ㉡, ㉢에 가장 적합한 것으로 짝지어진 것은?

<보기>
◯ 이더넷은 네트워크 인터페이스 카드에 설정된 _____㉠_____ 물리적 주소를 사용한다.
◯ 네트워크 계층의 주소는 _____㉡_____ 논리 주소를 사용한다.
◯ 전송계층의 주소는 _____㉢_____ 포트 주소를 사용한다.

① ㉠ 8Byte ㉡ 2Byte ㉢ 1Byte
② ㉠ 8Byte ㉡ 4Byte ㉢ 2Byte
③ ㉠ 6Byte ㉡ 2Byte ㉢ 1Byte
④ ㉠ 6Byte ㉡ 4Byte ㉢ 2Byte

정답 4번

출제 포인트

이 문제는 데이터 링크 계층의 MAC 주소, 네트워크 계층의 IPv4 주소, 전송 계층의 포트 주소가 각각 몇 바이트인지 구분하는 문제이다.

핵심 개념

MAC 주소: 이더넷에서 네트워크 인터페이스를 식별하는 48비트 물리적 주소로, 6Byte이다.
IPv4 주소: 네트워크 계층에서 호스트와 네트워크를 식별하는 32비트 논리 주소로, 4Byte이다.
포트 주소: 전송 계층에서 호스트 내부의 프로세스나 서비스를 식별하는 16비트 주소로, 2Byte이다.
따라서 ㉠ 6Byte, ㉡ 4Byte, ㉢ 2Byte이다.

NoteBase

선지별 해설

① X
㉠의 '8Byte', ㉡의 '2Byte', ㉢의 '1Byte'가 모두 틀렸다. 올바르게는 MAC 주소 6Byte, IPv4 주소 4Byte, 포트 주소 2Byte이다.

② X
㉡의 4Byte와 ㉢의 2Byte는 맞지만, ㉠의 '8Byte'가 틀렸다. 이더넷의 MAC 주소는 48비트이므로 올바르게는 6Byte이다.

③ X
㉠의 6Byte는 맞지만, ㉡의 '2Byte'와 ㉢의 '1Byte'가 틀렸다. 올바르게는 IPv4 주소가 4Byte이고 포트 주소가 2Byte이다.

④ O
MAC 주소 6Byte, IPv4 주소 4Byte, 포트 주소 2Byte를 계층별 주소 크기에 맞게 짝지었다.

오답 포인트

주소가 사용되는 계층과 주소의 크기를 뒤섞는 것이 함정이다. 특히 ③은 MAC 주소의 6Byte만 맞게 제시하고 IPv4 주소와 포트 주소의 크기를 각각 절반으로 줄여 놓았다.

다시 나오면 이렇게 판단

계층별 식별 대상을 먼저 연결한다. 데이터 링크 계층은 NIC의 MAC 주소, 네트워크 계층은 IPv4 주소, 전송 계층은 프로세스의 포트 주소이며, 크기는 차례로 6Byte, 4Byte, 2Byte이다.

암기 포인트

MAC·IPv4·포트의 주소 크기는 순서대로 6·4·2Byte이다.

NoteBase

문 2. 다음 <보기>는 라우터를 이용한 네트워크 보안 설정에 관련된 내용이다. 가장 옳은 내용을 모두 고르시오.

<보기>
㉠ egress 필터링은 라우터 내부에서 외부로 나가는 패킷의 소스 IP를 체크하여 필터링하는 것이다.
㉡ ingress 필터링은 standard 또는 extended access-list를 활용하여 라우터 내부로 유입되는 패킷의 소스 IP나 목적지 포트 등을 체크하여 허용하거나 거부하도록 필터링하는 것이다.
㉢ blackhole 필터링이란 인터페이스를 통해 들어오는 패킷의 소스 IP에 대해 라우팅 테이블을 확인하여 들어온 인터페이스로 다시 나가는지 확인하는 것이다.
㉣ unicast RPF는 access-list나 blackhole 필터링을 이용하여 일일이 IP나, IP대역을 지정하지 않고도 비정상 트래픽을 효율적으로 필터링할 수 있다.

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

정답 3번

출제 포인트

egress·ingress 필터링, blackhole 필터링, unicast RPF를 패킷의 방향과 검사 방식으로 구별하는 문제이다.

핵심 개념

egress 필터링: 내부에서 외부로 나가는 패킷을 검사하며, 내부망에서 허용될 수 없는 출발지 IP를 가진 위조 패킷의 외부 유출을 차단한다.
ingress 필터링: 외부에서 내부로 들어오는 패킷을 ACL 등의 조건으로 검사하여 허용하거나 거부한다.
blackhole 필터링: 특정 주소나 대역으로 향하는 트래픽을 폐기 경로로 보내 버리는 방식이다.
unicast RPF: 수신 패킷의 출발지 IP에 대한 역방향 경로를 라우팅 테이블에서 조회하여 패킷의 정상 여부를 검사한다. 엄격 모드에서는 그 역방향 경로의 인터페이스가 실제 수신 인터페이스와 일치하는지도 확인한다.
따라서 ㉠, ㉡, ㉣은 옳고 ㉢은 옳지 않다.

NoteBase

선지별 해설

① X — ㉠과 ㉡은 옳지만 ㉢은 blackhole 필터링이 아니라 엄격 모드 unicast RPF의 검사 방식을 설명한다. 또한 옳은 ㉣이 빠져 있다. 올바른 조합은 ㉠, ㉡, ㉣이다.
② X — ㉠과 ㉣뿐 아니라 ㉡도 옳다. ingress 필터링은 내부로 유입되는 패킷을 표준 또는 확장 ACL의 조건에 따라 허용하거나 거부한다. 올바른 조합은 ㉠, ㉡, ㉣이다.
③ O — ㉠은 외부로 나가는 패킷의 출발지 IP를 검사하는 egress 필터링, ㉡은 내부로 들어오는 패킷을 ACL로 통제하는 ingress 필터링에 해당한다. ㉣의 unicast RPF는 라우팅 정보를 이용해 출발지의 역방향 경로를 자동으로 검사하므로 ACL이나 blackhole 방식에서처럼 IP 또는 IP 대역을 일일이 열거하는 부담을 줄일 수 있다.
④ X — ㉢이 포함되어 있어 틀리다. ㉢의 '들어온 인터페이스로 다시 나가는지 확인'은 blackhole 필터링이 아니라 엄격 모드 unicast RPF의 설명이다. ㉢을 제외한 ㉠, ㉡, ㉣이 올바른 조합이다.

오답 포인트

㉢과 ㉣의 개념을 뒤섞는 것이 핵심 함정이다. '출발지 IP의 역방향 경로를 조회하고 수신 인터페이스와 대조한다'는 표현은 blackhole이 아니라 unicast RPF를 가리킨다.

다시 나오면 이렇게 판단

먼저 트래픽 방향을 본다. 내부에서 외부로 나가면 egress, 외부에서 내부로 들어오면 ingress이다. 다음으로 처리 방식을 본다. 폐기 경로로 보내면 blackhole이고, 출발지의 역방향 경로를 라우팅 테이블에서 확인하면 unicast RPF이다.

암기 포인트

나가는 것은 egress, 들어오는 것은 ingress, 버리는 경로는 blackhole, 출발지로 돌아가는 길을 확인하는 것은 RPF이다.

NoteBase

문 3. TCP는 흐름 제어를 다루기 위하여 슬라이딩 윈도우(Sliding Window)를 사용한다. 수신자 호스트 B는 8500 바이트의 버퍼를 갖고 있으며, 현재 버퍼에 3150 바이트의 처리되지 않은 데이터를 갖고 있다고 가정했을 때, 호스트 A를 위한 수신자 윈도우(rwnd) 값은?

① 3150

② 5350

③ 8500

④ 11650

정답 2번

출제 포인트

TCP 수신자 윈도우(rwnd)는 수신 버퍼에서 아직 사용할 수 있는 빈 공간을 나타낸다. 이 문제는 전체 버퍼 용량에서 처리되지 않아 버퍼를 차지한 데이터의 양을 빼서 rwnd를 구하는 문제이다.

조건 정리

주어진 값: 전체 수신 버퍼 용량은 8500byte, 처리되지 않은 데이터는 3150byte이다.
구해야 할 값: 호스트 B가 호스트 A에 알릴 수신자 윈도우(rwnd)이다.
주의할 조건: rwnd는 버퍼의 전체 크기나 이미 사용 중인 크기가 아니라 현재 남아 있는 빈 공간이다.

사용할 공식

rwnd=전체 수신 버퍼 용량-처리되지 않은 데이터의 양
수신자는 새 데이터를 더 받을 수 있는 범위만 송신자에게 알려야 하므로 전체 용량에서 현재 점유된 용량을 뺀다.

계산 과정

$rwnd = 8500 - 3150 = 5350byte$
따라서 호스트 A를 위한 수신자 윈도우 값은 5350byte이다.

선지 판단

① X — 3150byte는 아직 처리되지 않아 이미 버퍼를 차지한 데이터의 양이다. 틀린 값이며, 올바른 rwnd는 남은 공간인 5350byte이다.
② O — 전체 버퍼 8500byte에서 점유된 3150byte를 빼면 5350byte이므로 계산 결과와 일치한다.
③ X — 8500byte는 버퍼의 전체 용량이지 현재 수신 가능한 여유 공간이 아니다. 올바르게는 점유량을 뺀 5350byte가 rwnd이다.
④ X — 11650byte는 전체 용량과 점유량을 잘못 더한 값이다. rwnd는 두 값을 더하지 않고 $8500 - 3150 = 5350byte$로 계산한다.

NoteBase

오답 포인트

①의 3150을 현재 남은 공간으로 착각하거나 ③의 8500을 그대로 rwnd로 선택하기 쉽다. ④의 11650은 전체 용량과 이미 점유된 용량을 더해서 생기는 값이다. 핵심은 처리되지 않은 데이터가 버퍼를 이미 사용하고 있으므로 반드시 전체 용량에서 빼야 한다는 점이다.

다시 나오면 이렇게 판단

수신 버퍼의 전체 용량과 현재 점유량이 주어지면 먼저 rwnd가 남은 수신 가능 공간임을 확인하고, '전체 용량 – 점유량'으로 계산한다. 계산 결과가 0 이상이고 전체 버퍼 용량 이하인지 검산한다.

암기 포인트

TCP 수신자 윈도우(rwnd) = 전체 수신 버퍼 – 현재 점유된 데이터이다.

NoteBase

문 4. 다음 중 DDoS(Distributed Denial of Service) 공격과 툴에 대한 설명으로 가장 옳지 않은 것은?

① Teardrop은 두 번째 패킷의 Fragment Offset을 위조하여, 첫 번째 패킷 다음에 두 번째 패킷을 추가하지 않고 첫 번째 패킷의 TCP 헤더와 데이터 부분을 덮어쓰게 한다.

② Trinoo는 UDP Flood 서비스 거부 공격에 사용되는 툴이다.

③ Ghost Call은 IP Scan 이후 프리픽스로 호를 시도하여, Digest 인증을 해킹하는 공격을 의미하는 것이 아니라, 단순한 INVITE를 보내는 패턴 공격이다.

④ NetBot Attacker는 발신지와 수신지 IP를 동일하게 설정하여 라우터 및 서버의 성능장애나 시스템 다운을 유발시킨다.

정답 4번

출제 포인트

DDoS 공격 도구와 개별 서비스 거부 공격 기법의 특징을 정확히 대응시키는 문제이다.

핵심 개념

Teardrop은 IP 조각의 Fragment Offset을 조작해 조각들이 겹치도록 만드는 공격이다.
Trinoo는 여러 에이전트를 이용해 UDP Flood를 수행하는 분산 서비스 거부 공격 도구이다.
Ghost Call은 노출된 SIP 단말에 비정상적인 INVITE를 보내 원치 않는 착신을 발생시키는 공격 패턴이다.
발신지 IP와 수신지 IP를 피해 시스템의 주소로 동일하게 만든 패킷을 보내는 것은 LAND 공격의 특징이다.

선지별 해설

① O — Teardrop은 뒤 조각의 Fragment Offset을 비정상적으로 지정하여 앞 조각과 겹치게 한다. 이 때문에 재조립 과정에서 앞 조각의 TCP 헤더 또는 데이터 영역이 덮어써지는 형태가 나타날 수 있으므로 옳은 설명이다.
② O — Trinoo는 다수의 감염 호스트를 에이전트로 제어하여 표적에 UDP 패킷을 집중시키는 UDP Flood 계열의 DDoS 도구이므로 옳다.
③ O — Ghost Call은 SIP 단말을 탐색한 뒤 여러 번호나 프리픽스를 대상으로 단순 INVITE를 보내 전화가 울리게 하는 패턴이다. Digest 인증 정보를 해킹하는 공격 그 자체를 뜻하는 것은 아니므로 옳다.
④ X — 틀린 부분은 'NetBot Attacker는 발신지와 수신지 IP를 동일하게 설정한다'는 대응 관계이다. 발신지와 수신지 IP를 피해 시스템의 주소로 동일하게 위조하여 장애를 유발하는 것은 LAND 공격이다. NetBot Attacker는 좀비 PC를 제어하여 UDP·TCP·HTTP 등의 Flood 공격을 수행할 수 있는 DDoS 공격 도구로 고쳐야 한다.

NoteBase

오답 포인트

④는 장애나 시스템 다운이라는 결과만 보면 DDoS 도구의 설명처럼 보이지만, ‘발신지와 수신지 IP가 동일하다’는 고유한 단서는 LAND 공격을 가리킨다. 공격 결과가 아니라 패킷 구성 방식과 도구명을 대응시켜야 한다.

다시 나오면 이렇게 판단

선지에서 고유한 동작 단서를 먼저 찾는다. 조각 오프셋 중첩은 Teardrop, UDP Flood 도구는 Trinoo, SIP INVITE에 의한 유령 호출은 Ghost Call, 동일한 발신지·수신지 IP는 LAND 공격으로 구분한다.

암기 포인트

Teardrop은 조각 중첩, Trinoo는 UDP Flood, Ghost Call은 SIP INVITE, 같은 출발지·목적지 IP는 LAND이다.

NoteBase

문 5. ICMP(Internet Control Message Protocol) 프로토콜은 문제를 해결하는 기능과 전달할 수 없는 패킷에 대한 에러 정보를 알리기 위해 사용된다. 아래 대표적인 ICMP 메시지의 기능을 설명한 것 중 가장 옳지 않은 것은?

① Echo Request 메시지는 원하는 호스트로의 IP 연결을 확인하기 위해 사용된다.

② Destination Unreachable은 라우터나 목적호스트에 의해 보내지며 데이터그램이 전달되지 못한다는 것을 데이터를 보낸 호스트에 알려준다.

③ Source Quench는 데이터를 보내는 호스트에게 IP 데이터그램이 라우터의 집중현상에 의해 손실되고 있음을 알리기 위해 라우터가 보내는 메시지이다.

④ Echo Reply는 데이터를 보내는 호스트에게 목적 IP 주소에 대한 좀 더 적합한 경로가 있음을 알리기 위해 라우터가 보내는 메시지이다.

정답 4번

출제 포인트

ICMP의 대표 메시지인 Echo Request·Echo Reply, Destination Unreachable, Source Quench, Redirect의 기능을 서로 구별하는 문제이다.

핵심 개념

ICMP는 IP 패킷 처리 과정에서 발생한 오류를 알리거나 진단 정보를 주고받는 제어 프로토콜이다.
Echo Request는 상대 호스트에 응답을 요청하고, Echo Reply는 그 요청에 응답한다.
Destination Unreachable은 데이터그램을 목적지까지 전달할 수 없음을 송신 호스트에 알린다.
Source Quench는 혼잡 때문에 송신 속도를 낮추도록 요구하려던 메시지이다. 다만 현재 표준에서는 폐기된 메시지이다.
Redirect는 동일 네트워크의 호스트에게 특정 목적지로 가는 더 적합한 다음 홉 경로를 알려 준다.

선지별 해설

① O — Echo Request는 대상 호스트에 ICMP 응답을 요청하여 IP 계층의 도달 가능성을 확인하는 데 사용된다.
② O — Destination Unreachable은 라우터 또는 목적지 호스트가 데이터그램을 전달할 수 없을 때 그 사실과 원인을 송신 호스트에 알리는 오류 메시지이다.
③ O — 고전적인 ICMP 기능 설명에서 Source Quench는 라우터의 혼잡으로 데이터그램이 손실될 때 송신 호스트에 송신량을 줄이도록 알리는 메시지이다. 다만 현재 표준에서는 생성과 처리가 폐기되었다.
④ X — 틀린 표현은 ‘Echo Reply’와 ‘좀 더 적합한 경로가 있음을 알린다’의 연결이다. Echo Reply는 Echo Request에 대한 응답이고, 더 적합한 경로를 알리는 메시지는 Redirect이다.

NoteBase

오답 포인트

④는 라우터가 더 좋은 경로를 알려 주는 Redirect의 기능을 Echo Reply의 기능으로 바꾸어 놓았다. Echo라는 이름 때문에 네트워크 상태 전반을 알려 주는 메시지로 오해하기 쉽지만, Echo Reply의 역할은 요청받은 에코에 응답하는 것으로 한정된다.

다시 나오면 이렇게 판단

메시지 이름의 동작을 먼저 대응시킨다. Echo Request와 Echo Reply는 요청·응답, Destination Unreachable은 전달 실패, Redirect는 더 적합한 경로 안내, Source Quench는 과거의 혼잡 통지에 해당한다.

암기 포인트

Echo는 요청·응답, Unreachable은 전달 실패, Redirect는 경로 변경, Source Quench는 과거의 혼잡 완화 메시지이다.

NoteBase

문 6. 다음 TCP(Transport Control Protocol) 프로토콜의 타이머에 대한 설명 중 가장 옳지 않은 것은?

① RTO 값은 해당 시간까지 Acknowledge가 전송되어 오지 않는 경우, 재전송하기 위한 설정값이다.

② RTO 값은 초기 RTT값을 기준으로 항상 고정되어 있다.

③ RTO 시간이 너무 클 경우 수신측의 중복 ACK에 대한 손실 세그먼트를 재전송 하는 Fast retransmission 현상이 발생한다.

④ TCP 세그먼트가 유실되어, 해당 세그먼트를 요구하는 Acknowledge가 계속 도착하더라도 RTO 시간이 Time-out되어야 재전송이 가능하다.

정답 2번

출제 포인트

TCP의 재전송 타임아웃(RTO)이 ACK와 RTT 측정값에 따라 어떻게 동작하는지, 그리고 타임아웃 재전송과 빠른 재전송을 구별하는 문제이다.

핵심 개념

RTO는 송신한 TCP 세그먼트의 ACK가 일정 시간 안에 오지 않을 때 재전송을 시작하기 위한 대기 시간이다. RTO는 최초 RTT에 고정되는 값이 아니라 측정된 RTT의 평활값과 변동성을 반영하여 갱신된다. 빠른 재전송은 재전송 타이머의 만료를 기다리지 않고 중복 ACK를 근거로 손실 세그먼트를 다시 보내는 별도의 손실 복구 방식이다.

선지별 해설

① O — RTO는 ACK가 정해진 시간 안에 도착하지 않았을 때 미확인 세그먼트를 재전송하기 위한 타이머 설정값이다.
② X — 틀린 표현은 '초기 RTT값을 기준으로 항상 고정'이다. 올바르게는 RTO가 측정된 RTT의 평활값과 RTT 변동성을 반영하여 동적으로 갱신된다.
③ O — RTO가 길면 타이머가 만료되기 전에 중복 ACK가 누적될 가능성이 있고, 송신자는 중복 ACK를 손실 신호로 삼아 빠른 재전송을 수행할 수 있다. 빠른 재전송은 RTO 만료를 기다리지 않는다.
④ O — 이 선지는 RTO 타이머에 의한 재전송 경로를 설명한 것으로, 해당 경로에서는 ACK로 확인되지 않은 세그먼트를 타이머 만료 시 재전송한다. 다만 중복 ACK가 빠른 재전송의 기준을 충족하면 RTO 만료 전에도 별도의 빠른 재전송이 이루어진다.

오답 포인트

②의 '항상 고정'이 핵심 함정이다. 초기값이 존재한다는 사실과 연결 중 계속 사용하는 RTO가 고정된다는 주장은 다르다. 또한 RTO 만료에 따른 재전송과 중복 ACK에 따른 빠른 재전송을 같은 조건으로 혼동하기 쉽다.

NoteBase

다시 나오면 이렇게 판단

RTO에 '항상', '고정'이라는 표현이 붙으면 먼저 의심한다. RTT 표본이 들어오면 RTO가 갱신되고, 충분한 중복 ACK가 들어오면 타이머 만료 전에도 빠른 재전송이 가능하다는 두 기준을 나누어 판단한다.

암기 포인트

RTO는 RTT에 따라 갱신되고, 중복 ACK는 타임아웃을 기다리지 않는 빠른 재전송의 신호이다.

NoteBase

문 7. 다음 <보기>는 TCP Session Hijacking의 공격 순서를 나열한 것이다. 순서가 가장 옳은 것은?

<보기>
㉠ 공격 목표를 정하고 공격 대상을 설정한다.
㉡ 시퀀스 넘버의 난이도 검사를 한다.
㉢ TCP/IP 스택 구현이나 원리를 예측하고, 이를 통하여 얻어진 데이터로부터 시퀀스 넘버를 추측한다.
㉣ 공격자가 세션을 설정하고자 하는 컴퓨터로부터 시퀀스 넘버의 추측이 끝나면 그 서버와 연결되어 있는 컴퓨터에게 DoS 공격 등을 통하여 사용자를 제거한다.
㉤ 공격 대상에 세션을 설정하여 현재 공격 목표와 연결되어있는 공격 대상의 세션을 설정한다.
㉥ 제거된 사용자로부터 추측한 시퀀스 넘버를 이용하여 Session Hijacking을 실시한다.

① ㉠-㉡-㉢-㉣-㉤-㉥
② ㉠-㉤-㉡-㉣-㉢-㉥
③ ㉠-㉢-㉣-㉡-㉤-㉥
④ ㉠-㉡-㉤-㉢-㉣-㉥

정답 3번

출제 포인트

TCP Session Hijacking에서 공격 대상을 정한 뒤 시퀀스 넘버를 추측·점검하고, 정상 사용자를 배제한 상태에서 공격 세션을 만든 다음 세션을 탈취하는 순서를 묻는 문제이다. Session Hijacking은 공격자가 통신 당사자 중 하나로 가장하여 이미 형성된 세션의 제어권을 빼앗는 공격이다.

올바른 순서

㉠ 공격 목표와 공격 대상을 정한다.
㉢ TCP/IP 스택의 구현이나 동작 원리를 예측하고, 얻은 데이터로 시퀀스 넘버를 추측한다.
㉣ 시퀀스 넘버 추측이 끝나면 정상 사용자를 DoS 공격 등으로 제거한다.
㉡ 추측한 시퀀스 넘버의 난이도를 검사한다.
㉤ 공격 대상에 위장된 세션을 설정한다.
㉥ 제거된 사용자의 시퀀스 넘버를 이용하여 Session Hijacking을 실시한다.

따라서 올바른 순서는 ㉠-㉢-㉣-㉡-㉤-㉥이다. 공격 목표 선정이 출발점이고, 시퀀스 넘버에 관한 준비와 정상 사용자 배제가 선행되어야 공격 세션 설정과 최종 세션 탈취가 가능하다.

NoteBase

선지별 해설

① X — �runs을 ㉢보다 먼저 둔 순서가 틀렸다. TCP/IP 스택의 특성을 예측하여 시퀀스 넘버를 추측하는 ㉢이 먼저이고, 올바르게는 ㉠-㉢-㉣-㉡-㉤-㉥이다.
② X — 시퀀스 넘버 추측과 정상 사용자 제거 전에 ㉤의 세션 설정을 배치한 점이 틀렸다. 올바르게는 ㉢과 ㉣ 및 ㉡을 거친 뒤 ㉤을 수행하므로 ㉠-㉢-㉣-㉡-㉤-㉥이다.
③ O — 공격 대상 선정, 시퀀스 넘버 추측, 정상 사용자 제거, 난이도 검사, 공격 세션 설정, 세션 탈취의 순서인 ㉠-㉢-㉣-㉡-㉤-㉥과 일치한다.
④ X — ㉤의 세션 설정을 시퀀스 넘버 추측 ㉢과 정상 사용자 제거 ㉣보다 먼저 둔 점이 틀렸다. 올바르게는 준비 단계인 ㉢-㉣-㉡ 뒤에 ㉤이 오므로 ㉠-㉢-㉣-㉡-㉤-㉥이다.

오답 포인트

㉡의 '난이도 검사'를 시퀀스 넘버 추측보다 앞선 단계로 오해하거나, ㉤의 세션 설정을 준비 단계보다 먼저 배치하기 쉽다. 이 문항에서는 ㉢-㉣-㉡이 모두 끝난 뒤 ㉤과 ㉥이 이어진다는 점이 핵심 함정이다.

다시 나오면 이렇게 판단

절차를 '대상 선정 → 시퀀스 넘버 관련 준비 → 정상 사용자 배제 → 공격 세션 설정 → 최종 탈취'로 묶어 판단한다. 특히 세션 설정과 탈취는 시퀀스 넘버 추측 및 정상 사용자 제거보다 뒤에 와야 한다.

암기 포인트

목표 선정-번호 추측-사용자 제거-난이도 검사-세션 설정-세션 탈취의 흐름으로 기억한다.

NoteBase

문 8. 다음 중 침입 방지 시스템에 대한 설명으로 가장 옳지 않은 것은?

① 침입 방지 시스템의 검사영역은 네트워크 계층과 전송계층의 IP/Port 정보를 기반으로 동작한다.

② 침입 방지 시스템의 검사영역은 방화벽이 검사할 수 없는 전송계층 상단의 어플리케이션 계층의 데이터까지도 검사가 가능하다.

③ 침입 경고 이전에 상대의 공격을 중단시키는데 목적을 두고 있다.

④ 안티 바이러스와 같은 시그니처 기반의 기술과 방화벽과 같은 네트워크 차단기능이 결합된 방식을 침입 방지 시스템이라 한다.

정답 1번

출제 포인트

침입 방지 시스템(IPS)이 단순히 IP 주소와 포트만 검사하는 장비인지, 애플리케이션 데이터까지 분석하여 공격을 능동적으로 차단하는 장비인지 구별하는 문제이다.

핵심 개념

침입 방지 시스템(IPS)은 네트워크 트래픽을 실시간으로 분석하여 침입 징후를 탐지하고 공격 트래픽을 자동으로 차단하는 보안 시스템이다. 전통적인 패킷 필터링 방화벽이 주로 IP 주소·포트 등 네트워크 계층과 전송계층 정보를 기준으로 통신을 통제하는 데 비해, IPS는 패킷의 애플리케이션 데이터까지 검사하여 알려진 공격 패턴 등을 식별할 수 있다.

NoteBase

선지별 해설

① X
틀린 표현은 '검사영역은 네트워크 계층과 전송계층의 IP/Port 정보를 기반으로 동작한다'이다. 이는 전통적인 패킷 필터링 방화벽의 주된 검사 방식에 가깝다. IPS는 IP 주소와 포트뿐 아니라 전송계층 상단의 애플리케이션 데이터와 공격 패턴도 분석한다.

② O
IPS는 패킷의 페이로드 등 애플리케이션 계층 데이터까지 심층 검사할 수 있으므로, 전통적인 방화벽보다 넓은 범위에서 공격 여부를 판단할 수 있다.

③ O
IPS는 침입을 탐지하여 경고하는 데 그치지 않고, 공격 패킷 폐기나 연결 차단 등의 방식으로 공격을 실시간으로 중단시키는 데 목적이 있다.

④ O
IPS는 안티바이러스처럼 알려진 공격 패턴을 대조하는 시그니처 기반 탐지 기술과 방화벽처럼 트래픽을 차단하는 능동 대응 기능을 결합한 시스템으로 설명할 수 있다.

오답 포인트

①은 방화벽의 IP/Port 기반 접근 통제 특징을 IPS의 검사영역으로 바꾸어 놓았다. IPS도 IP와 포트 정보를 활용하지만 검사영역이 거기에 한정되지 않는다는 점이 핵심이다.

다시 나오면 이렇게 판단

IP 주소·포트에 따른 허용과 차단이 중심이면 전통적인 방화벽, 애플리케이션 데이터와 공격 패턴을 분석한 뒤 즉시 차단하면 IPS로 판단한다. 탐지와 경고만 강조하면 IDS, 탐지 후 능동 차단까지 포함하면 IPS이다.

암기 포인트

방화벽은 접근 통제, IDS는 탐지·경고, IPS는 심층 탐지·즉시 차단이다.

NoteBase

문 9. 다음 중 무선 보안 강화 방안을 설명한 것 중 가장 옳지 않은 것은?

① SSID를 브로드캐스트 불가로 접속하면 누구도 접속할 수 없다.

② TKIP은 WEP을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다.

③ WEP는 RC4 스트림 암호화 기법을 사용하고 키 스트림을 정적 키를 사용한다.

④ IEEE 802.11i는 AES 암호화 기법을 사용한다.

정답 1번

출제 포인트

이 문제는 무선랜 보안 기술인 SSID 숨김, WEP, TKIP, IEEE 802.11i의 기능과 한계를 구분하는 문제이다.

핵심 개념

SSID 브로드캐스트 비활성화는 네트워크 이름을 비콘 프레임에 드러내지 않는 설정일 뿐 접속 자체를 차단하는 인증 수단은 아니다.
WEP는 RC4와 공유 정적 비밀키를 사용하는 초기 무선랜 보안 방식이고, TKIP은 기존 WEP 장비를 활용하면서 패킷별 키 혼합과 무결성 검사 등으로 보안을 보완한 과도기 방식이다.
IEEE 802.11i는 강한 무선랜 보안을 위해 AES 기반 CCMP를 채택한 표준이다.

선지별 해설

① X — 틀린 표현은 '누구도 접속할 수 없다'이다. SSID 브로드캐스트를 끄더라도 SSID를 알고 수동으로 설정한 사용자는 인증 정보가 맞으면 접속할 수 있으며, 무선 관리 프레임 분석으로 SSID가 드러날 수도 있다.
올바르게는 'SSID 브로드캐스트 비활성화는 네트워크 노출을 줄일 뿐 접속을 원천 차단하지 않는다'이다.
② O — TKIP은 WEP를 지원하던 기존 무선랜 장비를 펌웨어나 소프트웨어로 업그레이드해 적용할 수 있도록 고안되었으며, 패킷별 키 혼합과 메시지 무결성 검사 등으로 WEP보다 보안을 강화한다.
③ O — WEP는 RC4 스트림 암호를 사용하고 공유 비밀키를 정적으로 운용한다. 패킷마다 초기화 벡터를 결합하더라도 비밀키 자체가 고정되어 있어 키 재사용과 짧은 초기화 벡터가 취약점이 된다.
④ O — IEEE 802.11i의 핵심 보호 방식인 CCMP는 AES를 사용하여 기밀성과 무결성을 제공한다.

오답 포인트

①의 '브로드캐스트 불가'를 '접속 불가'로 바꿔 이해하기 쉽다. SSID 숨김은 검색 화면에서 덜 보이게 하는 설정이고, 실제 접속 통제는 WPA 계열의 인증과 암호화가 담당한다.

NoteBase

다시 나오면 이렇게 판단

무선 보안 선지는 ‘노출 억제’, ‘인증’, ‘암호화’를 구분해 판단한다. SSID 숨김은 노출 억제, WEP와 TKIP은 RC4 계열, IEEE 802.11i의 CCMP는 AES 계열로 연결한다.

암기 포인트

SSID 숨김은 접속 차단이 아니며, WEP는 RC4·정적 공유키, TKIP은 WEP 보완, 802.11i의 CCMP는 AES이다.

NoteBase

문 10. 다음 중 가상사설망(VPN) 구현에 사용되는 터널링 프로토콜(Tunneling Protocol)로 가장 옳은 것은?

① PPTP, IPSEC, MPLS

② PPTP, L2TF, WAP

③ IPSEC, SET, SSL

④ L2TF, WAP, IPSEC

정답 1번

출제 포인트

VPN 구현에 쓰이는 터널링·전달 기술과 무선 응용 규격, 전자상거래 보안 규격을 구별하는 문제이다. 각 선지에 나열된 세 항목이 모두 VPN 구현 기술에 해당해야 한다.

핵심 개념

PPTP는 PPP 프레임을 IP망을 통해 전달하도록 캡슐화하는 VPN 터널링 프로토콜이다. IPsec은 IP 계층에서 패킷의 기밀성·무결성·인증을 제공하며 터널 모드로 VPN을 구성할 수 있다. MPLS는 패킷에 붙인 레이블을 기준으로 경로를 설정·전달하여 통신사업자망의 VPN을 구현하는 데 활용된다. 반면 WAP은 무선 단말의 인터넷 서비스 이용을 위한 응용 규격이고, SET은 전자상거래의 카드 결제를 보호하기 위한 보안 규격이다. L2TF는 표준 VPN 터널링 프로토콜 명칭이 아니며, 혼동하기 쉬운 표준 명칭은 L2F 또는 L2TP이다.

선지별 해설

① O — PPTP는 PPP 기반 터널링, IPsec은 IP 계층의 터널 모드, MPLS는 레이블 경로를 이용한 사업자 VPN 구현에 각각 사용된다. 따라서 세 항목을 함께 제시한 조합이 옳다.
② X — PPTP만 적절하다. 틀린 표현은 'L2TF, WAP'이다. L2TF는 표준 프로토콜 명칭이 아니고 WAP은 무선 응용 규격이다. 올바르게는 L2F 또는 L2TP와 같은 실제 터널링 프로토콜 및 IPsec·MPLS와 같은 VPN 구현 기술로 고쳐야 한다.
③ X — 틀린 표현은 'SET'이다. SET은 신용카드 기반 전자상거래 결제를 보호하는 규격이므로 VPN 터널링 프로토콜이 아니다. SSL은 SSL VPN에 이용될 수 있고 IPsec도 VPN에 이용되지만, SET을 PPTP나 MPLS와 같은 VPN 구현 기술로 바꾸어야 세 항목이 성립한다.
④ X — 틀린 표현은 'L2TF, WAP'이다. L2TF는 표준 명칭이 아니며 WAP은 무선 인터넷 응용 규격이다. 올바르게는 L2F 또는 L2TP와 같은 실제 터널링 프로토콜과 PPTP·MPLS 같은 VPN 구현 기술로 고쳐야 한다.

NoteBase

오답 포인트

SSL에도 ‘SSL VPN’이라는 용례가 있어 ③이 그럴듯해 보이지만, SET은 결제 보안 규격이므로 조합 전체가 틀린다. 또한 L2TF를 실제 프로토콜인 L2F나 L2TP와 혼동하거나, WAP의 ‘무선 통신’ 이미지만 보고 VPN 기술로 판단하기 쉽다.

다시 나오면 이렇게 판단

각 약어의 사용 목적을 먼저 구분한다. 네트워크 패킷의 캡슐화·보호·레이블 경로 구성은 VPN 쪽이고, 무선 웹 접속 규격이나 전자결제 보호 규격은 VPN 터널링 쪽이 아니다. 조합형 선지는 한 항목이라도 범주가 다르면 전체를 X로 판단한다.

암기 포인트

PPTP·IPsec·MPLS는 VPN, WAP은 무선 응용, SET은 전자결제이다. L2TF가 아니라 L2F 또는 L2TP이다.

NoteBase

문 11. 다음 <보기>는 오용탐지(Misuse Detection)와 이상탐지(Anomaly Detection)에 대한 설명이다. 이상탐지에 해당되는 것을 모두 고른 것은?

<보기>
㉠ 통계적 분석방법 등을 활용하여 급격한 변화를 발견하면 침입으로 판단한다.
㉡ 미리 축적한 시그니처와 일치하면 침입으로 판단한다.
㉢ 제로데이 공격탐지에 적합하다.
㉣ 임계값을 설정하기 쉽기 때문에 오탐률이 낮다.

① ㉠, ㉢
② ㉠, ㉣
③ ㉡, ㉢
④ ㉡, ㉣

정답 1번

출제 포인트

이 문제는 알려진 공격 패턴을 기준으로 삼는 오용탐지와 정상 상태에서 벗어난 변화를 기준으로 삼는 이상탐지를 구별하는 문제이다.

핵심 개념

오용탐지는 미리 등록된 공격 시그니처와의 일치 여부로 침입을 찾는 방식이며, 알려진 공격 탐지에 강하다.
이상탐지는 정상적인 행위나 통계적 기준을 학습·설정한 뒤 그 기준에서 크게 벗어난 행위를 침입으로 판단하는 방식이며, 알려지지 않은 공격도 탐지할 수 있다.
이상탐지는 정상과 비정상을 가르는 임계값을 적절히 정하기 어려워 정상 행위를 공격으로 판단하는 오탐이 발생할 수 있다.

선지별 해설

① O — ㉠은 통계적 분석으로 급격한 변화를 찾으므로 이상탐지이고, ㉢도 알려진 시그니처가 없는 제로데이 공격을 탐지할 가능성이 있다는 이상탐지의 특징이다. 따라서 ㉠과 ㉢의 조합이 맞다.
② X — ㉠은 맞지만 ㉣의 '임계값을 설정하기 쉽기 때문에 오탐률이 낮다'가 틀리다. 실제로 이상탐지는 정상 범위의 임계값 설정이 어렵고 오탐이 발생하기 쉬우므로, ㉣이 아니라 ㉢이 포함된 '㉠, ㉢'이 옳다.
③ X — ㉡의 '미리 축적한 시그니처와 일치하면'은 이상탐지가 아니라 오용탐지의 기준이다. ㉡을 ㉠으로 바꾼 '㉠, ㉢'이 옳다.
④ X — ㉡은 오용탐지에 해당하고, ㉣은 이상탐지의 임계값 설정과 오탐률의 관계를 반대로 서술했다. 이상탐지에 해당하는 올바른 조합은 '㉠, ㉢'이다.

NoteBase

오답 포인트

㉣은 이상탐지에서 임계값을 사용한다는 사실에 그럴듯한 설명을 붙인 함정이다. 이상탐지는 임계값 설정이 쉽고 오탐률이 낮은 것이 아니라, 정상 행위의 범위가 다양하여 임계값 설정이 어렵고 오탐 가능성이 있다.

다시 나오면 이렇게 판단

‘시그니처·알려진 공격·패턴 일치’가 보이면 오용탐지로, ‘정상 기준·통계적 변화·행동 이탈·미지의 공격’이 보이면 이상탐지로 판단한다.

암기 포인트

오용탐지는 알려진 공격의 서명 대조, 이상탐지는 정상에서 벗어난 이상 징후 탐지이다.

NoteBase

문 12. 다음 중 가상 사설망(VPN)에 대한 설명으로 가장 옳지 않은 것은?

① 공중망을 이용하여 사설망과 같은 효과를 얻기 위한 기술로서, 별도의 전용선을 사용하는 사설망에 비해 구축비용이 저렴하다.

② 사용자들 간의 안전한 통신을 위하여 기밀성, 무결성, 사용자인증의 보안 기능을 제공한다.

③ 네크워크 종단점 사이에 가상터널이 형성되도록 하는 터널링 기능은 SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다.

④ 인터넷과 같은 공공 네트워크를 통해서 기업의 재택근무자나 이동중인 직원이 안전하게 회사 시스템에 접근할 수 있도록 해준다.

정답 3번

출제 포인트

가상 사설망(VPN)의 목적과 보안 기능을 이해하고, 터널링을 특정 계층이나 특정 프로토콜로만 구현해야 한다는 잘못된 설명을 구별하는 문제이다.

핵심 개념

VPN은 인터넷과 같은 공중망에 암호화된 논리적 통신 경로인 터널을 만들어 사설망처럼 안전하게 통신하는 기술이다. 전용선을 직접 구축하는 것보다 비용을 줄일 수 있으며, 기밀성·무결성·인증 등의 보안 기능을 제공한다. 터널링 방식은 하나로 고정되지 않고 계층과 용도에 따라 IPsec, L2TP, SSL/TLS 등 여러 프로토콜로 구현될 수 있다.

선지별 해설

① O — VPN은 공중망 위에 논리적인 사설 통신 경로를 구성하므로 별도의 전용선을 구축하는 방식보다 일반적으로 비용이 적게 든다.
② O — VPN은 암호화와 인증 및 무결성 검증을 이용해 통신 내용의 기밀성, 데이터의 무결성, 통신 주체의 인증을 제공한다.
③ X — 틀린 표현은 ‘SSH와 같은 OSI 모델 4계층의 보안 프로토콜로 구현해야 한다’이다. SSH는 TCP를 이용하는 상위 계층 프로토콜이지 OSI 4계층 프로토콜로 분류되지 않으며, VPN 터널링도 SSH로만 구현해야 하는 것이 아니다. 올바르게는 VPN 터널링은 IPsec, L2TP, SSL/TLS 등 목적과 방식에 맞는 여러 프로토콜로 구현할 수 있다.
④ O — 원격 접속 VPN은 재택근무자나 이동 중인 직원이 인터넷을 통해 회사 내부 시스템에 안전하게 접속하도록 한다.

NoteBase

오답 포인트

③은 ‘터널링’이라는 말 때문에 전송 계층의 기능으로 단정하게 하고, SSH를 OSI 4계층 프로토콜로 잘못 묶은 선지이다. VPN의 터널은 특정 계층이나 단일 프로토콜에 한정되지 않는다.

다시 나오면 이렇게 판단

VPN 선지에서는 먼저 공중망 활용, 논리적 사설망, 암호화·무결성·인증, 원격 접속이라는 핵심 특징을 확인한다. 이어 ‘특정 계층에서만’, ‘특정 프로토콜로 반드시’처럼 구현 방식을 하나로 제한하는 표현이 있으면 그 프로토콜의 계층과 대체 방식을 함께 검토한다.

암기 포인트

VPN은 공중망 위의 안전한 가상 터널이며, 터널링은 특정 계층·특정 프로토콜 하나에 고정되지 않는다.

NoteBase

문 13. 다음 중 인터넷망에서 안전하게 정보를 전송하기 위하여 사용되고 있는 네트워크 계층 보안 프로토콜인 IPSec에 대한 설명으로 가장 옳지 않은 것은?

① DES-CBC, RC5, Blowfish 등을 이용한 메시지 암호화를 지원한다.

② 방화벽이나 게이트웨이 등에 구현한다.

③ IP 기반의 네트워크에서만 동작한다.

④ 암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능하다.

정답 4번

출제 포인트

IPSec의 동작 계층, 구현 위치, 암호 알고리즘의 선택 가능성을 구분하는 문제이다.

핵심 개념

IPSec은 IP 패킷을 네트워크 계층에서 보호하는 보안 프로토콜 모음이다. AH 또는 ESP로 인증·무결성·기밀성 등의 보안 서비스를 제공하며, 보안 연관(SA)을 설정할 때 사용할 암호·인증 알고리즘과 관련 매개변수를 협상할 수 있다.

선지별 해설

① O — IPSec의 ESP는 DES-CBC를 비롯하여 RC5, Blowfish 등 여러 암호 알고리즘을 사용한 데이터 암호화를 지원할 수 있다.
② O — IPSec은 종단 호스트뿐 아니라 방화벽이나 보안 게이트웨이에도 구현할 수 있다. 보안 게이트웨이 사이의 VPN에는 주로 터널 모드가 사용된다.
③ O — IPSec은 IP 계층의 패킷을 보호하므로 IPv4·IPv6와 같은 IP 기반 네트워크에서 동작한다.
④ X — 틀린 표현은 '암호화/인증방식이 지정되어 있어 신규 알고리즘 적용이 불가능하다'이다. 실제로 IPSec은 보안 연관을 통해 사용할 알고리즘을 선택·협상하는 확장 가능한 구조이므로, 규격과 구현이 지원하면 새로운 암호·인증 알고리즘을 적용할 수 있다.

오답 포인트

IPSec이 표준 프로토콜이라는 사실을 '한 가지 암호화·인증방식으로 고정된다'고 오해하기 쉽다. IPSec은 보안 처리의 틀을 정하지만 실제 알고리즘은 선택·협상할 수 있으므로 ④의 '신규 알고리즘 적용이 불가능하다'가 틀린 단정이다.

NoteBase

다시 나오면 이렇게 판단

IPSec 관련 선지는 ‘IP 계층에서 동작하는가’, ‘호스트와 보안 게이트웨이에 구현할 수 있는가’, ‘알고리즘을 선택·협상할 수 있는가’를 차례로 확인한다. 알고리즘이 하나로 고정되거나 새 알고리즘을 수용할 수 없다는 표현은 틀린 것으로 판단한다.

암기 포인트

IPSec은 IP 계층 보안이며, 구현 위치와 암호 알고리즘 선택에 유연성이 있다.

NoteBase

문 14. 다음 <보기>에서 설명하는 보안 시스템은?

<보기>
◯ 패킷을 버리거나 또는 의심이 가는 트래픽을 감지함으로써, 공격 트래픽을 방어하는 기능을 가지고 있다.
◯ 모든 트래픽을 수신하는 스위치의 포트를 모니터하고, 특정 트래픽을 막기 위하여 적합한 명령어를 라우터(Router)나 침입차단시스템(Firewall)에 전송할 수 있다.
◯ 호스트(Host) 기반의 이 보안 시스템은 공격을 감지하기 위하여 서명이나 비정상 감지기술을 사용한다.

① IDS
② IPS
③ DNS
④ VPN

정답 2번

출제 포인트

침입을 탐지하는 데 그치지 않고 패킷 폐기, 트래픽 차단 등 능동적인 방어까지 수행하는 보안 시스템을 구별하는 문제이다.

핵심 개념

IPS(Intrusion Prevention System, 침입방지시스템)는 서명 기반 또는 비정상 행위 기반 기법으로 공격을 탐지하고, 악성 패킷 폐기나 차단 명령 전송 등으로 공격을 능동적으로 막는 시스템이다.
IDS는 침입 징후를 탐지하여 기록하거나 경고하는 데 초점이 있고, IPS는 탐지 후 차단까지 수행한다.

선지별 해설

① X — IDS는 침입 징후를 탐지하고 관리자에게 알리는 데 초점을 둔다. 틀린 표현은 'IDS'이며, 패킷을 버리거나 차단 명령을 보내 공격을 방어하는 시스템은 IPS이다.
② O — IPS는 공격 트래픽을 탐지한 뒤 패킷을 폐기하거나 라우터·침입차단시스템에 차단 명령을 보내 침입을 예방한다. 호스트 기반 IPS도 서명 기반 탐지와 비정상 행위 탐지를 사용할 수 있다.
③ X — DNS는 도메인 이름과 IP 주소를 대응시키는 이름 해석 시스템이다. 틀린 표현은 'DNS'이며, 보기에서 설명한 능동적 침입 방어 시스템은 IPS이다.
④ X — VPN은 공용 네트워크에서 암호화된 터널을 구성하여 안전한 통신 경로를 제공하는 기술이다. 틀린 표현은 'VPN'이며, 공격 패킷의 탐지와 차단을 수행하는 시스템은 IPS이다.

NoteBase

오답 포인트

IDS와 IPS가 모두 서명 기반·비정상 행위 기반 탐지를 사용할 수 있다는 점이 함정이다. 보기의 '패킷을 버린다', '특정 트래픽을 막는 명령어를 전송한다'는 표현이 단순 탐지를 넘어 차단까지 수행하는 IPS의 결정적 단서이다.

다시 나오면 이렇게 판단

'탐지·기록·경고'가 중심이면 IDS로 판단하고, '패킷 폐기·연결 차단·차단 명령 전송'처럼 공격을 실제로 막는 동작이 제시되면 IPS로 판단한다.

암기 포인트

IDS는 탐지와 경고, IPS는 탐지와 차단이다.

NoteBase

문 15. 다음 중 네트워크 기반 공격기법에 대한 설명으로 가장 옳지 않은 것은?

① SYN Flooding 공격은 TCP 연결설정 과정의 취약점을 악용한 서비스 거부 공격이다.

② Zero Day 공격은 시그니처(Signature) 기반의 침입탐지시스템으로 방어하는 것이 일반적이다.

③ APT 공격은 공격대상을 지정하여 시스템의 특성을 파악한 후 지속적으로 공격한다.

④ Buffer Overflow 공격은 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하는 공격이다.

정답 2번

출제 포인트

SYN Flooding, Zero Day, APT, Buffer Overflow의 핵심 공격 원리를 구분하는 문제이다. 특히 알려진 공격 패턴을 찾는 시그니처 기반 탐지가 아직 알려지지 않은 취약점을 악용하는 Zero Day 공격에 적합한지 판단해야 한다.

핵심 개념

SYN Flooding은 TCP 연결 설정 과정에서 다수의 연결 요청을 보내 반쯤 열린 연결을 누적시키는 서비스 거부 공격이다.
Zero Day 공격은 취약점이 공개되거나 보안 패치·탐지 시그니처가 마련되기 전에 그 취약점을 악용하는 공격이다.
APT는 특정 대상을 정하고 장기간 은밀하게 침투·정찰·정보 탈취를 수행하는 지능형 지속 공격이다.
Buffer Overflow는 할당된 버퍼의 경계를 넘는 데이터를 입력하여 인접 메모리를 훼손하고 비정상 동작이나 임의 코드 실행을 유발할 수 있는 공격이다.

선지별 해설

① O — SYN Flooding은 TCP의 연결 설정 절차를 악용한다. 공격자가 대량의 SYN을 보내고 연결을 완성하지 않으면 서버에 반쯤 열린 연결이 쌓여 정상 사용자의 접속을 방해하므로 서비스 거부 공격에 해당한다.
② X — 틀린 표현은 '시그니처 기반의 침입탐지시스템으로 방어하는 것이 일반적'이라는 부분이다. Zero Day 공격은 아직 알려지지 않은 취약점과 공격 패턴을 이용하므로 기존 시그니처만으로 탐지하기 어렵다. 올바르게는 이상 행위·행위 기반 탐지, 최소 권한, 공격 표면 축소 등의 다층 방어로 위험을 줄이고, 취약점과 시그니처가 공개되면 신속히 패치하고 탐지 규칙을 갱신해야 한다.
③ O — APT는 불특정 다수를 일회성으로 공격하는 방식이 아니라 특정 조직이나 시스템을 표적으로 정하고, 대상의 특성을 파악한 뒤 장기간 지속적으로 침투하는 공격이다.
④ O — Buffer Overflow는 프로그램이 확보한 버퍼의 크기를 넘는 데이터를 입력하여 버퍼 경계를 벗어난 메모리 영역을 덮어쓰는 공격이다. 이로 인해 프로그램 충돌이나 임의 코드 실행이 발생할 수 있다.

NoteBase

오답 포인트

②의 함정은 침입탐지시스템이 모든 공격을 같은 방식으로 탐지한다고 보는 데 있다. 시그니처 기반 탐지는 이미 알려진 패턴에는 효과적이지만, 아직 시그니처가 없는 Zero Day 공격에는 한계가 있다.

다시 나오면 이렇게 판단

공격 이름마다 핵심 단서를 연결한다. SYN Flooding은 TCP 연결 설정과 반쪽 연결, Zero Day는 미공개 취약점과 기존 시그니처의 한계, APT는 특정 표적과 장기·지속성, Buffer Overflow는 버퍼 경계 초과와 메모리 훼손으로 판단한다.

암기 포인트

SYN은 연결 고갈, Zero Day는 기존 시그니처 부재, APT는 표적형 장기 침투, Buffer Overflow는 버퍼 경계 초과이다.

NoteBase

문 16. 다음 <보기>는 보안 공격 유형을 나열한 것이다. 소극적 공격을 모두 고른 것은?

<보기>
㉠ 신분위장(Masquerade)
㉡ 재전송(Replay)
㉢ 패킷 분석(Analysis of Packet)
㉣ 메시지 수정(Modification of Message)
㉤ 스니핑(Sniffing)
㉥ 서비스 거부(Denial of Service)

① ㉠, ㉢, ㉤
② ㉠, ㉣
③ ㉢, ㉤
④ ㉢, ㉣, ㉥

정답 3번

출제 포인트

이 문제는 보안 공격을 소극적 공격과 적극적 공격으로 구분할 수 있는지를 묻는다.

핵심 개념

소극적 공격은 통신 내용을 몰래 관찰하거나 수집하지만 데이터나 시스템 상태를 직접 바꾸지 않는 공격이다. 패킷 분석과 스니핑이 이에 해당한다.
적극적 공격은 데이터의 변경·삽입·재전송이나 서비스 방해처럼 통신 또는 시스템 상태에 변화를 일으키는 공격이다. 신분위장, 재전송, 메시지 수정, 서비스 거부가 이에 해당한다.

NoteBase

선지별 해설

① X
ⓒ 패킷 분석과 ⓓ 스니핑은 소극적 공격이지만, ㉠ 신분위장은 공격자가 다른 사용자인 것처럼 가장하여 인증이나 통신에 개입하는 적극적 공격이다. 틀린 구성은 ㉠을 포함한 것이며, 올바른 소극적 공격의 조합은 ⓒ, ⓓ이다.

② X
㉠ 신분위장과 ㉣ 메시지 수정은 모두 적극적 공격이다. 신분위장은 거짓 신원을 사용하고, 메시지 수정은 전송 내용을 변경한다. 올바른 소극적 공격의 조합은 ⓒ, ⓓ이다.

③ O
ⓒ 패킷 분석과 ⓓ 스니핑은 전송 중인 패킷이나 통신 내용을 몰래 관찰·수집하는 공격으로, 데이터 자체를 변경하지 않는 소극적 공격이다.

④ X
ⓒ 패킷 분석만 소극적 공격이다. ㉣ 메시지 수정은 전송 내용을 바꾸고, ㉤ 서비스 거부는 정상적인 서비스 이용을 방해하므로 적극적 공격이다. 틀린 구성은 ㉣과 ㉤을 포함한 것이며, 올바른 소극적 공격의 조합은 ⓒ, ⓓ이다.

오답 포인트

공격자가 정보를 얻는다는 결과만 보고 신분위장이나 재전송까지 소극적 공격으로 오인하기 쉽다. 분류 기준은 공격 목적이 아니라 데이터·통신·서비스 상태에 직접 변화를 일으키는지 여부이다.

다시 나오면 이렇게 판단

엿보기·도청·관찰처럼 정보만 수집하면 소극적 공격으로 판단한다. 위장·재전송·변조·서비스 방해처럼 통신이나 시스템 상태를 바꾸면 적극적 공격으로 판단한다.

암기 포인트

패킷 분석·스니핑은 소극적 공격, 신분위장·재전송·메시지 수정·서비스 거부는 적극적 공격이다.

NoteBase

문 17. 다음 중 공격자가 인터넷을 통해 전송되는 데이터의 TCP Header에서 검출할 수 없는 정보로 가장 옳은 것은?

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

출제 포인트

TCP 헤더에 실제로 들어 있는 필드와 헤더만으로 알 수 없는 정보를 구분하는 문제이다.

핵심 개념

TCP 헤더는 송신지·목적지 포트 번호, 순서 번호, 확인응답 번호, 윈도우 크기 등 연결과 신뢰성 있는 전송에 필요한 제어 정보를 담는다. 그러나 일반적인 TCP 헤더에는 패킷의 생성 시각을 직접 나타내는 필드가 없다. TCP 타임스탬프 옵션이 사용되더라도 그 값은 왕복 시간 측정과 오래된 중복 세그먼트 판별 등에 쓰이는 시계 값이지, 패킷의 정확한 생성 시간을 뜻하지 않는다.

선지별 해설

① O — TCP 헤더의 Window Size 필드는 수신측이 추가로 받을 수 있는 데이터의 양, 즉 수신 윈도우를 알린다. 따라서 공격자는 헤더를 관찰하여 수신 시스템이 광고한 윈도우 크기를 검출할 수 있다.
② O — TCP 헤더에는 Source Port와 Destination Port 필드가 있으므로 송신 프로세스와 수신 프로세스의 포트 번호를 검출할 수 있다.
③ O — TCP 헤더의 Acknowledgment Number 필드는 ACK가 유효할 때 수신측이 다음에 받기를 기대하는 바이트의 순서 번호를 나타낸다. 따라서 해당 정보를 헤더에서 검출할 수 있다.
④ X — 틀린 표현은 ‘TCP 패킷의 생성 시간’이다. 일반적인 TCP 헤더에는 패킷 생성 시간을 직접 기록하는 필드가 없으므로 헤더만으로 이를 검출할 수 없다. 올바르게는 ‘송신 시스템의 TCP 패킷 생성 시간은 일반적인 TCP 헤더에서 직접 알 수 없다’이다.

오답 포인트

TCP의 선택적 Timestamp 옵션을 ‘패킷 생성 시간’으로 오해하기 쉽다. 이 옵션의 타임스탬프 값은 전송 제어를 위한 값이며, 송신 시스템의 실제 패킷 생성 시각을 직접 표시하는 정보가 아니다.

NoteBase

다시 나오면 이렇게 판단

포트 번호, 순서·확인응답 번호, 윈도우 크기는 TCP의 전송 제어에 필요한 표준 헤더 정보로 판단한다. 실제 생성 시각처럼 TCP 전송 제어와 직접 관계없는 정보는 별도의 표준 필드가 있는지 확인한다.

암기 포인트

TCP 헤더에는 포트·순서·ACK·윈도우가 있고, 패킷 생성 시간은 없다.

NoteBase

문 18. 다음 중 ACL 적용 규칙에 해당하지 않는 것으로 가장 옳은 것은?

① Named ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.

② ACL의 마지막에는 deny any가 생략되어 있다.

③ ACL은 먼저 입력한 순서대로 수행된다.

④ Numbered ACL은 순서대로 입력되므로 중간에 삽입이나 삭제가 불가능하다.

정답 1번

출제 포인트

이 문제는 ACL의 위에서 아래로 진행되는 최초 일치 처리, 마지막의 묵시적 거부, 그리고 Named ACL과 Numbered ACL의 편집 방식 차이를 묻는 문제이다.

핵심 개념

ACL(Access Control List)은 패킷의 허용 또는 거부 조건을 위에서 아래로 검사하는 규칙 목록이다. 패킷이 어떤 항목과 일치하면 그 항목의 permit 또는 deny를 적용하고 검사를 끝내므로 항목의 순서가 중요하다. 어느 항목에도 일치하지 않으면 맨 마지막에 생략된 묵시적 deny any가 적용된다.
Named ACL은 이름으로 식별하며 순서 번호를 이용해 특정 항목을 삽입하거나 삭제할 수 있다. Numbered ACL은 번호로 ACL을 식별하며, 이 문항이 전제하는 기본 편집 방식에서는 중간 항목만 삽입하거나 삭제하기 어렵고 ACL을 다시 구성한다.

NoteBase

선지별 해설

① X
틀린 표현은 ‘Named ACL은 중간에 삽입이나 삭제가 불가능하다’이다. Named ACL은 순서 번호를 이용해 원하는 위치에 항목을 삽입하거나 특정 항목을 삭제할 수 있다. 따라서 ACL 적용 규칙에 해당하지 않는 것은 ①이다.

② O
ACL의 끝에는 명시하지 않아도 모든 나머지 패킷을 거부하는 묵시적 deny any가 존재한다. 따라서 필요한 트래픽을 허용하려면 그보다 앞에 permit 항목이 있어야 한다.

③ O
ACL 항목은 입력되어 있는 순서대로 위에서 아래로 검사한다. 패킷이 처음 일치한 항목의 동작을 적용하면 이후 항목은 검사하지 않는다.

④ O
이 문항이 전제하는 기본 Numbered ACL 편집 방식에서는 항목이 입력 순서대로 배치되므로 중간 항목만 삽입하거나 삭제하기 어렵다. 원하는 순서로 바꾸려면 ACL을 삭제한 뒤 다시 작성하는 방식이 사용된다.

오답 포인트

①과 ④는 문장 구조가 거의 같지만 ACL의 종류가 다르다. ‘중간 삽입·삭제가 불가능하다’는 기본 Numbered ACL의 제약으로 제시된 것이며, 순서 번호로 항목을 편집할 수 있는 Named ACL에 그대로 적용하면 틀린다. 또한 ③의 ‘먼저 입력한 순서’는 먼저 일치한 항목에서 처리가 끝난다는 뜻까지 함께 판단해야 한다.

다시 나오면 이렇게 판단

ACL 문제에서는 먼저 ‘위에서 아래로 검사하여 최초 일치에서 종료’와 ‘마지막의 묵시적 deny any’를 확인한다. 편집 방식 문제에서는 Named ACL은 순서 번호에 따른 항목 삽입·삭제가 가능하고, 기본 Numbered ACL은 중간 편집이 어렵다는 차이로 판단한다.

암기 포인트

ACL은 위→아래, 최초 일치에서 종료, 끝에는 deny any이다. Named ACL은 중간 편집이 가능하다.

NoteBase

문 19. 다음 <보기>의 VPN에 대한 설명 중 가장 옳은 것을 모두 고른 것은?

<보기>
㉠ 터널링 기술은 VPN의 기본이 되는 기술로서 터미널이 형성되는 양 호스트 사이에 전송되는 패킷을 추가 헤더 값으로 캡슐화하는 기술이다.
㉡ 데이터 암호화 기술은 터널이 형성된 한 쪽 호스트에서 데이터를 암호화해서 보내면 반대편 호스트에서 암호화 데이터를 복호화하여 원본 데이터를 확인하게 된다.
㉢ VPN은 데이터의 출처 즉, 출발지 IP가 확실한지에 대한 인증기술을 제공하고, 내부 자원에 대해서 허가 받지 않은 사용자의 접속을 차단하는 접근제어 기능을 제공한다.
㉣ VPN 구현에 가장 널리 사용되는 터널링 프로토콜에는 PPP, SSL, SSH 등이 있다.

① ㉠
② ㉠, ㉡
③ ㉠, ㉡, ㉢
④ ㉠, ㉡, ㉢, ㉣

정답 3번

출제 포인트

VPN의 핵심 기능인 터널링·암호화·인증·접근제어와 대표적인 터널링 프로토콜을 구별하는 문제이다.

핵심 개념

VPN은 공용 네트워크 위에 논리적인 사설 통신 경로를 구성하여 데이터를 안전하게 전달하는 기술이다.
㉠ 터널링은 원래 패킷을 다른 프로토콜의 패킷 안에 넣고 추가 헤더를 붙여 전송하는 캡슐화 기술이므로 옳다.
㉡ 송신 측에서 암호화한 데이터를 수신 측에서 복호화하면 통신 내용의 기밀성을 확보할 수 있으므로 옳다.
㉢ VPN은 통신 상대나 데이터 출처를 확인하는 인증과, 허가되지 않은 사용자의 내부 자원 접근을 제한하는 접근제어를 제공할 수 있으므로 옳다.
㉣ PPP·SSL·SSH를 대표적인 VPN 터널링 프로토콜이라고 한 부분은 옳지 않다. 대표적인 VPN 터널링 관련 프로토콜로는 PPTP, L2TP, IPsec 등이 있다.

NoteBase

선지별 해설

① X — ㉠만 고른 선지이지만 ㉡의 암호화·복호화 설명과 ㉢의 인증·접근제어 설명도 옳다. 올바르게는 ㉠, ㉡, ㉢을 모두 골라야 한다.
② X — ㉠과 ㉡만 고른 선지이지만 ㉢도 VPN의 보안 기능을 바르게 설명한다. 올바르게는 ㉢까지 포함해야 한다.
③ O — ㉠의 캡슐화, ㉡의 암호화·복호화, ㉢의 인증·접근제어는 모두 VPN의 원리와 기능에 부합하고, 잘못된 ㉣은 제외하였다.
④ X — 틀린 부분은 ㉣까지 포함한 것이다. PPP·SSL·SSH를 대표적인 VPN 터널링 프로토콜로 묶는 것은 부정확하며, 올바르게는 ㉣을 제외하고 ㉠, ㉡, ㉢만 선택해야 한다.

오답 포인트

㉣은 SSL과 SSH도 암호화 통신에 쓰인다는 점을 이용해 모두 대표적인 VPN 터널링 프로토콜인 것처럼 보이게 한다. 그러나 PPP는 링크 계층 통신 프로토콜이며, 대표적인 VPN 터널링 관련 프로토콜은 PPTP·L2TP·IPsec 등으로 구분한다.

다시 나오면 이렇게 판단

VPN 설명은 기능과 프로토콜을 나누어 판단한다. 패킷 캡슐화는 터널링, 내용 보호는 암호화, 상대·출처 확인은 인증, 내부 자원 사용 제한은 접근제어에 해당한다. 프로토콜 나열에서는 PPTP·L2TP·IPsec 같은 대표 항목인지 확인한다.

암기 포인트

VPN의 핵심은 터널링·암호화·인증·접근제어이며, 대표 프로토콜은 PPTP·L2TP·IPsec이다.

NoteBase

문 20. 다음 중 무선랜 구축 시 보안을 위한 고려사항으로 가장 옳지 않은 것은?

① SSID(Service Set IDentifier)를 숨김모드로 사용

② 무선 단말기의 MAC(Media Access Control)주소 인증 수행

③ 관리자용 초기 ID/Password 변경

④ 보안성이 우수한 WEP(Wired Equivalent Privacy) 사용

정답 4번

출제 포인트

무선랜 보안 대책의 기능과 한계를 구분하고, 취약한 구식 암호화 방식인 WEP를 안전한 방식으로 잘못 평가한 선지를 찾는 문제이다.

핵심 개념

무선랜 보안은 네트워크 식별 정보의 노출을 줄이고, 접속 단말을 통제하며, 관리자 계정을 보호하고, 강한 암호화·인증 방식을 적용하는 것이다. SSID 숨김과 MAC 주소 인증은 우회될 수 있으므로 보조 대책에 해당하고, 실제 통신 보호에는 WPA2의 AES 기반 방식이나 WPA3처럼 강한 보안 방식을 사용한다. WEP는 취약한 암호화 방식이므로 사용하지 않는다.

선지별 해설

① O — SSID를 숨김모드로 설정하면 주변 단말의 일반적인 네트워크 검색 목록에 이름이 쉽게 나타나지 않아 무선랜 노출을 줄이는 보조 대책이 된다. 다만 SSID를 완전히 은폐하는 강한 보안 수단은 아니다.
② O — 허용한 무선 단말기의 MAC 주소만 접속하도록 인증·필터링하면 비인가 단말의 접근을 제한하는 보조 대책이 된다. 다만 MAC 주소는 위조될 수 있으므로 암호화와 함께 사용해야 한다.
③ O — 제조사가 설정한 관리자용 초기 ID와 비밀번호는 널리 알려져 있거나 추측하기 쉬우므로 반드시 변경해야 한다. 이는 무선 공유기나 액세스 포인트의 관리 권한 탈취를 막는 기본 조치이다.
④ X — 틀린 표현은 '보안성이 우수한 WEP'이다. WEP는 암호화 키를 알아낼 수 있는 구조적 취약점이 있어 보안성이 낮다. 올바르게는 WEP를 사용하지 않고 WPA2의 AES 기반 방식이나 WPA3처럼 강한 무선랜 보안 방식을 사용해야 한다.

오답 포인트

①과 ②는 단독으로는 우회 가능한 약한 대책이지만, 무선랜 구축 시 고려할 수 있는 보조 보안 조치이다. 반면 ④는 취약한 WEP를 '보안성이 우수하다'고 평가했으므로 명백히 옳지 않다.

NoteBase

다시 나오면 이렇게 판단

SSID 숨김·MAC 주소 인증은 접근 노출과 접속 대상을 줄이는 보조 대책으로 판단하고, 통신 암호화 방식은 WEP인지 WPA2·WPA3인지 확인한다. WEP를 안전하거나 권장되는 방식이라고 설명하면 틀린 선지이다.

암기 포인트

SSID 숨김·MAC 필터링은 보조 수단, 초기 관리자 비밀번호는 변경, WEP는 취약하므로 사용하지 않는다.

NoteBase