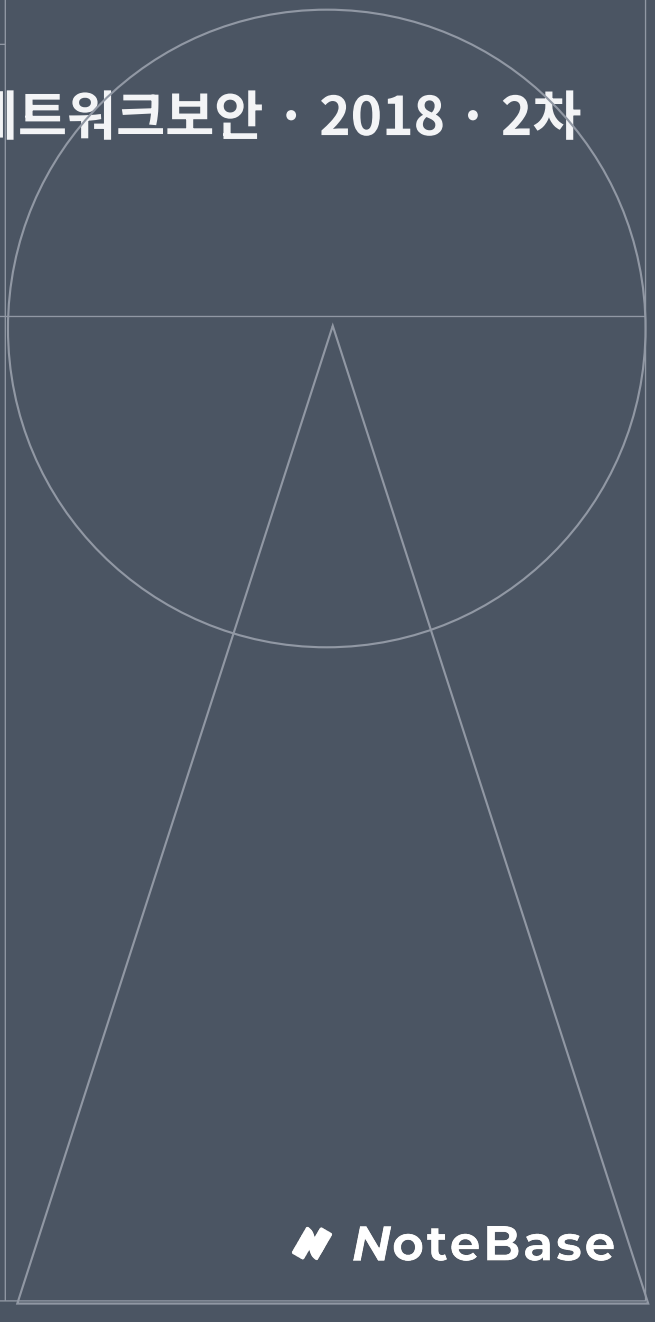
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2018 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2018 · 2차

공무원/해경/일반직 9급 · 네트워크보안 · 2018 · 2차

문 1. 다음은 OSI 7계층에 대한 설명 중 해당 계층끼리 올바르게 짝지어진 것은?

ㄱ. 경로설정, 데이터 교환 및 중계, 트래픽 제어, 패킷정보 전송
ㄴ. 정보형식(포맷), 코드 변환, 데이터 암호화, 데이터 압축, 구문검색, 문맥관리
ㄷ. 프로토콜 방식 PPP, PPTP, L2F, HDLC, SDLC 등

① ㄱ: Network Layer, ㄴ: Session Layer, ㄷ: Data link Layer
② ㄱ: Network Layer, ㄴ: Session Layer, ㄷ: Transport Layer
③ ㄱ: Session Layer, ㄴ: Network Layer, ㄷ: Data link Layer
④ ㄱ: Session Layer, ㄴ: Network Layer, ㄷ: Physical Layer

정답 1번

출제 포인트

OSI 7계층의 대표 기능과 프로토콜을 보고 해당 계층을 구별하는 문제이다. ㄱ은 경로 설정과 패킷 전달을 담당하는 네트워크 계층이고, ㄷ의 PPP·HDLC·SDLC는 데이터 링크 계층의 프로토콜이다.

핵심 개념

네트워크 계층: 여러 네트워크 사이에서 패킷의 경로를 정하고 전달하는 계층이다. 키워드는 라우팅·패킷·중계이다.
세션 계층: 통신 주체 사이의 대화 연결을 설정·유지·종료하고 동기화를 관리하는 계층이다.
표현 계층: 데이터의 표현 형식을 맞추며 코드 변환·암호화·압축을 담당하는 계층이다.
데이터 링크 계층: 인접 노드 사이의 프레임 전송과 오류·흐름 제어를 담당하며 PPP·HDLC·SDLC가 대표 프로토콜이다.

NoteBase

선지별 해설

① O(정답표 기준) — ㄱ의 경로 설정·패킷 중계는 Network Layer이고, ㄷ의 PPP·HDLC·SDLC는 Data Link Layer이므로 정답표는 ㄴ을 Session Layer로 연결한 ①을 정답으로 처리한다. 다만 ㄴ에 열거된 코드 변환·암호화·압축은 표준 OSI 분류상 Presentation Layer의 대표 기능이므로 이 부분은 주의가 필요하다.
② X — 틀린 표현은 'ㄷ: Transport Layer'이다. PPP·HDLC·SDLC는 전송 계층이 아니라 Data Link Layer의 프로토콜이다. 올바르게는 'ㄷ: Data Link Layer'이다.
③ X — 틀린 표현은 'ㄱ: Session Layer'와 'ㄴ: Network Layer'이다. 경로 설정과 패킷 중계는 Network Layer의 기능이므로 ㄱ은 Network Layer이다. 또한 ㄴ은 적어도 Network Layer가 아니며, 표준 분류에서는 Presentation Layer의 기능에 해당한다.
④ X — 틀린 표현은 'ㄱ: Session Layer', 'ㄴ: Network Layer', 'ㄷ: Physical Layer'이다. 올바르게는 ㄱ이 Network Layer이고 ㄷ이 Data Link Layer이며, ㄴ의 코드 변환·암호화·압축은 표준 분류상 Presentation Layer의 기능이다.

오답 포인트

ㄷ의 프로토콜을 전송 계층이나 물리 계층으로 착각하기 쉽다. PPP·HDLC·SDLC는 모두 프레임 단위 통신과 관련된 데이터 링크 계층 프로토콜이다. 또한 이 문항의 ㄴ에는 표현 계층의 대표 기능이 섞여 있는데도 선택지에는 Presentation Layer가 없고 정답표는 ①을 제시한다는 점이 실제 함정이다.

다시 나오면 이렇게 판단

'경로 설정·패킷'은 네트워크 계층, 'PPP·HDLC·SDLC·프레임'은 데이터 링크 계층으로 먼저 확정한다. '코드 변환·암호화·압축'은 표준 OSI 분류에서 표현 계층으로 판단하고, '대화 제어·동기화'는 세션 계층으로 구별한다.

암기 포인트

경로·패킷은 네트워크, 변환·암호화·압축은 표현, 대화·동기화는 세션, PPP·HDLC·SDLC는 데이터 링크이다.

NoteBase

문 2. IDS 공격탐지 방법 중 오용탐지에 대한 설명으로 가장 틀린 것은?

① 시그니처 기반으로 동작한다.

② 속도가 빠르며, 구현이 쉽다.

③ 이미 정립된 공격패턴을 미리 입력하고 매칭하여 침입을 판단한다.

④ 정상인지, 비정상인지 결정하는 임계치 설정이 어렵다.

정답 4번

출제 포인트

IDS의 오용탐지와 이상탐지를 구별하는 문제이다. 특히 알려진 공격 시그니처를 대조하는 방식과 정상 행위에서 벗어났는지를 임계치로 판단하는 방식을 구분해야 한다.

핵심 개념

오용탐지는 이미 알려진 공격의 특징이나 패턴을 시그니처로 등록하고, 관측된 활동과 일치하는지를 대조하여 침입을 탐지하는 방식이다. 구현이 비교적 쉽고 탐지 속도가 빠르지만, 알려지지 않은 새로운 공격에는 취약하다. 이상탐지는 정상 행위의 기준을 정한 뒤 그 기준에서 크게 벗어난 활동을 침입으로 판단하는 방식이다. 정상과 비정상을 나누는 임계치를 적절히 설정하기 어렵다는 특징이 있다.

선지별 해설

① O — 오용탐지는 알려진 공격의 특징을 시그니처로 저장하고 이를 현재 트래픽이나 행위와 비교하는 시그니처 기반 방식이다.
② O — 미리 정의된 패턴과의 일치 여부를 검사하므로 탐지 과정이 비교적 빠르고 구현도 비교적 쉽다.
③ O — 이미 정립된 공격 패턴을 사전에 입력한 뒤 관측된 활동과 매칭하여 침입 여부를 판단한다는 설명은 오용탐지의 핵심 원리이다.
④ X — 틀린 표현은 '정상인지, 비정상인지 결정하는 임계치 설정이 어렵다'이다. 이는 정상 행위에서 벗어난 정도를 기준으로 삼는 이상탐지의 특징이다. 오용탐지는 임계치보다 알려진 공격 시그니처와의 일치 여부를 중심으로 판단한다.

오답 포인트

④의 '임계치 설정'은 IDS 전반의 공통 특징이 아니라 이상탐지와 연결되는 표현이다. 오용탐지의 '패턴 매칭'과 이상탐지의 '정상 기준·임계치'를 뒤바꾼 것이 함정이다.

다시 나오면 이렇게 판단

선지에 '시그니처·알려진 공격·패턴 매칭'이 나오면 오용탐지로, '정상 행위·통계적 편차·임계치'가 나오면 이상탐지로 판단한다.

NoteBase

암기 포인트

오용탐지는 알려진 공격을 패턴으로 찾고, 이상탐지는 정상 기준에서 벗어난 행동을 찾는다.

NoteBase

문 3. Windows 시스템 명령창에서 netstat -an 명령을 수행한 결과의 일부이다. 구동 중인 서비스로 가장 옳지 않은 것은?

프로토콜	로컬주소	외부주소	상태
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:25	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING

① FTP

② Telnet

③ SMTP

④ HTTP

정답 2번

출제 포인트

netstat 결과의 로컬 TCP 포트 번호와 대표 서비스의 기본 포트를 대응시키는 문제이다. 자료에는 포트 21, 25, 80이 LISTENING 상태로 나타난다.

자료 읽는 순서

1. 프로토콜이 TCP이고 상태가 LISTENING인지 확인한다.
2. 로컬 주소 끝의 포트 번호 21, 25, 80을 읽는다.
3. 각 포트를 대표 서비스인 FTP, SMTP, HTTP와 대응시킨다.

핵심 근거

자료의 로컬 주소에는 0.0.0.0:21, 0.0.0.0:25, 0.0.0.0:80이 표시되어 있다. 각각 FTP, SMTP, HTTP의 대표 기본 포트이다. Telnet의 대표 기본 포트는 23인데 자료에는 포트 23이 없으므로 Telnet이 구동 중이라는 판단은 자료와 맞지 않는다.

NoteBase

선지별 해설

① O — FTP의 대표 기본 포트는 TCP 21이며, 자료의 첫 번째 행에 0.0.0.0:21이 LISTENING 상태로 표시되어 있다.
② X — Telnet의 대표 기본 포트는 TCP 23이지만 자료에는 포트 23이 없다. 틀린 표현은 ‘Telnet이 구동 중이다’이며, 올바르게는 ‘이 자료에서 Telnet 서비스의 구동은 확인되지 않는다’이다.
③ O — SMTP의 대표 기본 포트는 TCP 25이며, 자료의 두 번째 행에 0.0.0.0:25가 LISTENING 상태로 표시되어 있다.
④ O — HTTP의 대표 기본 포트는 TCP 80이며, 자료의 세 번째 행에 0.0.0.0:80이 LISTENING 상태로 표시되어 있다.

오답 포인트

선지에 제시된 서비스가 모두 널리 쓰이는 TCP 서비스라는 이유만으로 선택하면 안 된다. 이 문항에서는 실제 LISTENING 포트와 대조해야 하며, ② Telnet에 필요한 포트 23만 자료에 없다.

다시 나오면 이렇게 판단

netstat 표에서는 먼저 LISTENING 상태인 로컬 포트를 찾고, 포트 번호를 대표 서비스와 대응시킨다. 포트 21은 FTP, 23은 Telnet, 25는 SMTP, 80은 HTTP로 판단한다.

암기 포인트

21-FTP, 23-Telnet, 25-SMTP, 80-HTTP이다.

NoteBase

문 4. UDP 포트 스캐닝을 수행할 때 해당 포트에 서비스가 없을 경우 되돌아오는 메시지는 무엇인가?

① ICMP Unreachable

② UDP Unreachable

③ Reset

④ SYN+ACK

정답 1번

출제 포인트

UDP 포트 스캔에서 서비스가 없는 닫힌 포트가 반환하는 응답과 TCP 포트 스캔의 응답을 구별하는 문제이다.

핵심 개념

UDP는 연결 설정 과정이 없는 전송 계층 프로토콜이므로 TCP의 SYN, ACK, RST 같은 제어 플래그를 사용하지 않는다. UDP 데이터그램이 닫힌 포트에 도착하면 대상 호스트는 일반적으로 ICMP Destination Unreachable 중 Port Unreachable 메시지를 반환한다. 반면 TCP 스캔에서는 열린 포트가 SYN+ACK로, 닫힌 포트가 RST 계열 응답으로 반응한다.

선지별 해설

① O — UDP 데이터그램이 서비스가 없는 닫힌 포트에 도착하면 일반적으로 ICMP Destination Unreachable의 Port Unreachable 메시지가 돌아오므로 ICMP Unreachable이 맞다.
② X — 틀린 표현은 'UDP Unreachable'이다. UDP 자체에는 포트 도달 불가를 알리는 제어 메시지가 없으며, 올바르게는 'ICMP Port Unreachable'이다.
③ X — 틀린 표현은 'Reset'이다. Reset(RST)은 닫힌 TCP 포트에서 나타나는 TCP 응답이며, 닫힌 UDP 포트의 일반적인 응답은 ICMP Port Unreachable이다.
④ X — 틀린 표현은 'SYN+ACK'이다. SYN+ACK는 TCP SYN 스캔에서 열린 TCP 포트가 보내는 응답이며, UDP 포트 스캔의 닫힌 포트 응답은 ICMP Port Unreachable이다.

오답 포인트

③의 RST와 ④의 SYN+ACK는 모두 TCP 포트 스캔에서 사용하는 응답이다. UDP 스캔이라는 조건을 놓치면 TCP의 열린 포트·닫힌 포트 응답과 혼동하기 쉽다.

다시 나오면 이렇게 판단

먼저 전송 프로토콜이 UDP인지 TCP인지 구분한다. UDP의 닫힌 포트는 ICMP Port Unreachable, TCP의 열린 포트는 SYN+ACK, TCP의 닫힌 포트는 RST 계열 응답으로 판단한다.

NoteBase

암기 포인트

UDP 닫힘은 ICMP Port Unreachable, TCP 열림은 SYN+ACK, TCP 닫힘은 RST이다.

NoteBase

문 5. 다음에서 설명하는 보안 공격 기법은?

ㄱ. 두 프로세스가 자원을 서로 사용하려고 하는 것을 이용한 공격이다.
ㄴ. 시스템 프로그램과 공격 프로그램이 서로 자원을 차지하기 위한 상태에 이르게 하여 시스템 프로그램이 갖는 권한으로 파일에 접근을 가능하게 하는 공격방법을 말한다.

① Buffer Overflow 공격

② Format String 공격

③ MITB(Man–In–The–Browser) 공격

④ Race Condition 공격

정답 4번

출제 포인트

공유 자원을 두고 여러 프로세스가 경쟁할 때 실행 순서나 시간 차이를 악용하는 Race Condition 공격의 특징을 식별하는 문제이다.

핵심 개념

Race Condition 공격: 둘 이상의 프로세스가 같은 자원에 접근할 때 결과가 실행 순서나 시점에 따라 달라지는 경쟁 상태를 악용하는 공격이다. 특히 권한이 높은 시스템 프로그램의 검사 시점과 사용 시점 사이에 파일이나 자원의 상태를 바꾸어 그 권한으로 공격 대상에 접근하게 할 수 있다.
Buffer Overflow 공격은 버퍼의 허용 범위를 넘는 데이터를 입력해 인접 메모리를 덮어쓰는 공격이고, Format String 공격은 외부 입력을 서식 문자열로 잘못 사용하여 메모리를 읽거나 쓰는 공격이다. MITB 공격은 브라우저 내부의 악성코드가 사용자의 웹 통신이나 거래 내용을 가로채거나 변조하는 공격이다.

선지별 해설

① X — ‘Buffer Overflow 공격’이라는 명칭이 틀렸다. Buffer Overflow는 버퍼 용량을 초과한 입력으로 인접 메모리나 제어 정보를 덮어쓰는 공격이다. 제시문의 올바른 공격 명칭은 Race Condition 공격이다.
② X — ‘Format String 공격’이라는 명칭이 틀렸다. Format String 공격은 검증되지 않은 입력을 printf 계열 함수 등의 서식 문자열로 사용하여 메모리 내용을 노출하거나 변경하는 공격이다. 제시문의 올바른 공격 명칭은 Race Condition 공격이다.
③ X — ‘MITB(Man–In–The–Browser) 공격’이라는 명칭이 틀렸다. MITB는 브라우저에 침투한 악성코드가 사용자의 통신이나 거래 정보를 가로채고 변조하는 공격이다. 제시문의 올바른 공격 명칭은 Race Condition 공격이다.
④ O — 두 프로세스가 동일한 자원을 차지하려 경쟁하고, 시스템 프로그램의 권한을 이용해 파일에 접근한다는 설명은 실행 시점과 순서의 틈을 악용하는 Race Condition 공격에 해당한다.

NoteBase

오답 포인트

‘시스템 프로그램의 권한으로 파일에 접근한다’는 결과만 보고 메모리 공격으로 오인하기 쉽다. 그러나 제시문의 결정적 단서는 ‘두 프로세스’, ‘서로 자원을 차지’, ‘상태에 이르게 한다’이다. 이는 입력 길이나 서식 문자열이 아니라 자원 접근의 타이밍과 순서를 악용하는 공격을 가리킨다.

다시 나오면 이렇게 판단

공유 자원, 두 프로세스, 실행 순서, 시간 차이, 검사 시점과 사용 시점의 불일치가 보이면 Race Condition을 판단한다. 버퍼 크기 초과는 Buffer Overflow, 서식 지정자 악용은 Format String, 브라우저 내부의 거래 변조는 MITB로 구별한다.

암기 포인트

Race Condition은 자원 경쟁과 타이밍, Buffer Overflow는 용량 초과, Format String은 서식 지정자, MITB는 브라우저 내부 변조이다.

NoteBase

문 6. NIC(Network Interface Card)에 대한 설명으로 올바르지 않은 것은 무엇인가?

① 네트워크 정보를 전송하기 위해서 병렬구조로 데이터를 바꾼다.

② 빠른 전송을 위해서 데이터를 코딩 및 압축한다.

③ 목적지 장비의 NIC는 데이터를 수신하고 CPU로 데이터를 전달한다.

④ 네트워크 장비와 LAN 사이의 통신을 준비한다.

정답 1번

출제 포인트

NIC가 컴퓨터 내부의 데이터와 LAN에서 전송되는 신호 사이를 중계하면서 수행하는 데이터 변환·송수신 기능을 묻는 문제이다.

핵심 개념

NIC(Network Interface Card)는 컴퓨터를 네트워크에 연결하는 장치이다. 송신할 때에는 컴퓨터 내부의 병렬 데이터를 네트워크 전송에 적합한 직렬 데이터와 신호로 바꾸고, 수신할 때에는 이 과정을 반대로 수행하여 CPU가 처리할 수 있도록 전달한다. 또한 전송을 위한 코딩, 데이터 송수신 및 LAN 접속 제어를 담당한다.

선지별 해설

① X — 틀린 표현은 '병렬구조로 데이터를 바꾼다'이다. 컴퓨터 내부에서는 여러 비트를 병렬로 처리하지만, NIC는 네트워크로 송신할 데이터를 직렬 형태로 변환한다. 따라서 '직렬구조로 데이터를 바꾼다'가 올바른 표현이다.
② O — NIC는 전송 매체에서 보낼 수 있는 신호 형태가 되도록 데이터를 코딩하며, 데이터량을 줄이는 압축 처리를 통해 전송 효율을 높일 수 있다.
③ O — 목적지 NIC는 네트워크에서 들어온 신호를 수신·복원한 뒤 시스템이 처리할 수 있는 데이터로 바꾸어 CPU 측에 전달한다.
④ O — NIC는 네트워크 장비인 컴퓨터와 LAN 전송 매체 사이의 접속점으로서 데이터 링크를 설정하고 송수신을 준비한다.

오답 포인트

①은 컴퓨터 내부 버스의 병렬 처리와 네트워크 선로상의 직렬 전송을 뒤바꾼 선지이다. '전송 속도가 빠르다'는 인상만으로 병렬 전송이라고 판단하면 틀리기 쉽다.

다시 나오면 이렇게 판단

NIC의 방향별 기능을 구분한다. 송신 방향에서는 내부의 병렬 데이터가 네트워크용 직렬 데이터·신호로 변환되고, 수신 방향에서는 네트워크 신호가 시스템이 처리할 데이터로 복원된다.

NoteBase

암기 포인트

NIC는 컴퓨터와 LAN의 경계이며, 송신 시 병렬을 직렬로 바꾼다.

NoteBase

문 7. IDS 탐지기능에서 False Negative의 의미로 가장 올바른 것은 무엇인가?

① false(+)로 표현되고, 공격이 아닌데도 공격이라고 오판

② false(-)로 표현되고, 공격인데도 공격이 아니라고 오판

③ false(+)로 표현되고, 공격인데도 공격이 아니라고 오판

④ false(-)로 표현되고, 공격이 아닌데도 공격이라고 오판

정답 2번

출제 포인트

IDS의 탐지 결과에서 False Positive와 False Negative를 실제 공격 여부와 경보 발생 여부로 구분하는 문제이다.

핵심 개념

False Positive는 실제로 공격이 아닌데 IDS가 공격이라고 잘못 탐지하는 오경보이다. False Negative는 실제로 공격인데 IDS가 공격이 아니라고 판단하여 탐지하지 못하는 미탐이다. Positive와 Negative는 IDS가 내린 판정, True와 False는 그 판정의 정답 여부를 뜻한다.

선지별 해설

① X

False Positive의 설명이다. 틀린 부분은 False Negative를 묻는 문항에서 ‘false(+)’라고 한 것이다. 올바르게는 ‘false(+)는 공격이 아닌데도 공격이라고 오판하는 경우’이다.

② O

False Negative는 실제 공격이 존재하지만 IDS가 공격이 아니라고 판정하여 놓치는 경우이다. 따라서 false(-)이고, 공격인데도 공격이 아니라고 오판한다는 설명이 정확하다.

③ X

‘공격인데도 공격이 아니라고 오판’한다는 내용은 False Negative이지만, 이를 ‘false(+)’로 표시한 부분이 틀렸다. 올바르게는 ‘false(-)로 표현되고, 공격인데도 공격이 아니라고 오판’이다.

④ X

‘false(-)’ 표시는 False Negative에 해당하지만, ‘공격이 아닌데도 공격이라고 오판’한다는 설명은 False Positive이므로 틀렸다. 올바르게는 ‘false(-)로 표현되고, 공격인데도 공격이 아니라고 오판’이다.

NoteBase

오답 포인트

Positive와 Negative를 실제 공격의 유무로 해석하면 혼동하기 쉽다. 특히 ③은 False Negative의 상황을 정확히 설명하면서 기호만 false(+)로 바꾸었고, ④는 false(-) 기호에 False Positive의 상황을 결합한 선지이다.

다시 나오면 이렇게 판단

먼저 IDS의 판정을 본다. 경보를 냈으면 Positive, 경보를 내지 않았으면 Negative이다. 그 판정이 실제 상태와 다르면 False를 붙인다. 따라서 실제 공격을 놓친 경우는 False Negative이다.

암기 포인트

False Positive는 오경보, False Negative는 공격 미탐이다.

NoteBase

문 8. 다음은 어느 포렌식 도구에 대한 설명인가?

ㄱ. 유닉스 운영체제에서 실행되는 도구
ㄴ. Dan Farmer와 Wietse Venema가 개발
ㄷ. 라이브 시스템에서 현재 상태정보를 캡쳐하고 분석할 수 있는 뛰어난 도구
ㄹ. 법원에서 증거로 채택하기 위해 데이터를 모으는 것이 아니라 어떻게 시스템을 손상시켰는지 알아내도록 돕기 위한 것

① Encase
② TCT
③ FTK
④ Safeback

정답 2번

출제 포인트

이 문제는 개발자, 실행 환경, 분석 목적을 단서로 유닉스 포렌식 도구 TCT를 식별하는 문제이다.

핵심 개념

TCT(The Coroner's Toolkit)는 Dan Farmer와 Wietse Venema가 개발한 유닉스용 사고 분석 도구 모음이다. 라이브 시스템의 상태 정보를 수집·분석하여 침해자가 시스템을 어떻게 손상시켰는지 조사하는 데 초점이 있다.
EnCase와 FTK는 디지털 증거의 수집·분석을 지원하는 종합 포렌식 도구이고, SafeBack은 저장매체의 비트 단위 복제에 사용되는 이미징 도구이다.

NoteBase

선지별 해설

① X
제시문의 '유닉스에서 실행', 'Dan Farmer와 Wietse Venema가 개발', '라이브 시스템 상태정보 분석'은 EnCase가 아니라 TCT의 특징이다. EnCase는 저장매체의 증거 수집과 분석에 활용되는 종합 디지털 포렌식 도구이다.

② O
TCT는 Dan Farmer와 Wietse Venema가 개발한 유닉스용 포렌식 도구 모음으로, 라이브 시스템의 상태를 수집·분석하여 침해 과정을 조사하는 데 사용된다. 제시된 단서와 모두 일치한다.

③ X
제시문의 개발자와 유닉스 라이브 시스템 분석이라는 표현은 FTK가 아니라 TCT를 가리킨다. FTK는 디지털 증거의 수집·검색·분석을 지원하는 종합 포렌식 도구이다.

④ X
제시문의 설명은 SafeBack이 아니라 TCT에 해당한다. SafeBack은 디스크 등 저장매체의 비트 단위 사본을 만드는 포렌식 이미징 도구이다.

오답 포인트

네 선지 모두 포렌식 분야의 도구이므로 용도만 막연히 보면 혼동하기 쉽다. 이 문항의 결정적 단서는 'Dan Farmer와 Wietse Venema', '유닉스', '라이브 시스템 상태정보'이며, 이 조합은 TCT에 해당한다.

다시 나오면 이렇게 판단

포렌식 도구 식별 문제에서는 개발자와 운영체제를 먼저 확인하고, 그다음 기능이 라이브 침해 분석인지 저장매체 이미징인지 종합 증거 분석인지 구분한다. Farmer·Venema와 유닉스 라이브 분석이 함께 나오면 TCT로 판단한다.

암기 포인트

TCT는 Farmer·Venema가 만든 유닉스 침해 분석 도구, SafeBack은 저장매체 이미징 도구이다.

NoteBase

문 9. 다음 중 동적 라우팅(Dynamic Routing)의 특징에 대한 설명이 아닌 것은?

① 대부분 라우터에서 사용되며 환경이 수시로 변화하는 환경에 적합

② 네트워크 환경 변경 혹은 트래픽이 변경되는 경우에 자동으로 경로변경

③ 패킷을 전달할 경로가 여러 개 있을 경우 가장 큰 효과가 있음

④ 환경 변화가 적거나 상호 연결 네트워크가 적은 형태에 적합

정답 4번

출제 포인트

이 문제는 네트워크 변화에 따라 경로를 자동으로 갱신하는 동적 라우팅과 관리자가 경로를 직접 설정하는 정적 라우팅의 특징을 구별하는 문제이다.

핵심 개념

동적 라우팅: 라우팅 프로토콜을 이용해 라우터들이 경로 정보를 교환하고, 네트워크 상태가 바뀌면 라우팅 테이블을 자동으로 갱신하는 방식이다. 변화가 잦거나 규모가 크고 대체 경로가 여러 개인 네트워크에 적합하다.
정적 라우팅: 관리자가 경로를 직접 설정하며, 네트워크 변화가 생겨도 경로가 자동으로 바뀌지 않는 방식이다. 구조가 단순하고 변화가 적은 소규모 네트워크에 적합하다.

선지별 해설

① O — 동적 라우팅은 라우팅 프로토콜을 통해 경로 정보를 자동으로 학습·갱신하므로, 경로와 상태가 자주 달라지는 환경에서 활용하기 적합하다.
② O — 링크 장애, 토폴로지 변경 또는 트래픽 상태 변화가 발생하면 라우팅 프로토콜이 새 경로를 계산하여 경로를 자동으로 변경할 수 있다.
③ O — 전달 가능한 경로가 여러 개이면 동적 라우팅이 경로 정보를 비교하여 더 적절한 경로를 선택하고, 기존 경로에 장애가 생겼을 때 대체 경로로 전환할 수 있어 효과가 크다.
④ X — 틀린 표현은 '환경 변화가 적거나 상호 연결 네트워크가 적은 형태에 적합'이다. 이는 관리 부담이 작고 구성이 단순한 정적 라우팅에 더 적합한 설명이다. 동적 라우팅은 변화가 잦거나 상호 연결이 복잡하고 대체 경로가 필요한 환경에 적합하다.

오답 포인트

④의 '환경 변화가 적다'와 '상호 연결 네트워크가 적다'는 표현이 핵심 함정이다. 단순하고 안정적인 환경에서는 경로를 자동 계산하는 동적 라우팅의 이점보다 설정이 단순한 정적 라우팅의 장점이 더 크다.

NoteBase

다시 나오면 이렇게 판단

‘자동 학습·자동 갱신·변화 대응·대체 경로’가 나오면 동적 라우팅으로 판단한다. ‘관리자가 직접 설정·변화가 적음·소규모·단순한 연결’이 나오면 정적 라우팅으로 판단한다.

암기 포인트

동적 라우팅은 변화에 자동 대응하고, 정적 라우팅은 단순하고 안정적인 환경에 적합하다.

NoteBase

문 10. 다음 중 FTP 서버에 대한 Bounce Attack의 설명으로 옳지 않은 것은?

① FTP 프로토콜 구조의 허점을 이용한 공격 방법이다.

② Active, Passive 모드를 임의로 변경할 수 있다.

③ FTP Bounce Attack을 이용하면 근원지(Source)를 알 수 없는 전자 메일(Fake Mail)을 보낼 수 있다.

④ FTP 클라이언트가 실행되는 호스트가 아닌 다른 호스트를 지정하더라도 서버는 충실하게 지정된 곳으로 정보를 보낸다.

정답 2번

출제 포인트

FTP Bounce Attack이 능동 모드의 PORT 명령을 악용한다는 점과, 능동·수동 모드 전환 자체를 공격 기능으로 보는 설명을 구별하는 문제이다.

핵심 개념

FTP Bounce Attack은 공격자가 FTP 서버에 제3의 호스트와 포트를 지정하는 PORT 명령을 보내, FTP 서버가 그 제3의 대상에 데이터 연결을 맺도록 악용하는 공격이다. 핵심은 능동 모드의 서버발 데이터 연결과 목적지 지정 기능이며, 능동 모드와 수동 모드를 임의로 바꾸는 공격이 아니다.

선지별 해설

① O — FTP의 제어 연결과 데이터 연결이 분리되고, 능동 모드에서 클라이언트가 PORT 명령으로 데이터 연결 목적지를 알려 주는 구조적 허점을 이용한다.
② X — 틀린 표현은 ‘Active, Passive 모드를 임의로 변경할 수 있다’이다. 올바르게는 FTP Bounce Attack은 Active 모드의 PORT 명령에 제3의 호스트와 포트를 지정하여 서버의 데이터 연결을 우회적으로 이용하는 공격이다.
③ O — FTP 서버가 지정된 다른 서버의 SMTP 포트로 연결하게 한 뒤 메일 전송 명령을 전달하면, 실제 공격자의 근원지를 감춘 Fake Mail 전송에 악용할 수 있다.
④ O — 취약한 FTP 서버는 PORT 명령에 FTP 클라이언트가 아닌 제3의 호스트가 지정되어도 그 주소로 데이터 연결을 시도하므로 Bounce Attack이 성립한다.

오답 포인트

②는 FTP에 Active 모드와 Passive 모드가 모두 존재한다는 사실을 공격 효과와 혼동하게 만든다. Bounce의 핵심은 모드의 임의 변경이 아니라 Active 모드에서 PORT 명령으로 데이터 연결의 목적지를 제3의 호스트로 지정하는 데 있다.

NoteBase

다시 나오면 이렇게 판단

FTP 서버가 PORT 명령에 따라 제3의 호스트로 연결하는 설명이면 Bounce Attack에 해당한다. 모드 자체를 마음대로 전환한다는 설명은 Bounce Attack의 기능이 아니므로 틀린 것으로 판단한다.

암기 포인트

FTP Bounce는 Active 모드의 PORT 명령을 악용한 제3자 연결이다.

NoteBase

문 11. 다음에서 설명하는 침입 차단 시스템(Firewall)의 유형은?

ㄱ. 종단-대-종단 TCP 연결을 허용하지 않는다.
ㄴ. 시스템 관리자가 내부 사용자를 신뢰할 경우 일반적으로 사용한다.
ㄷ. 두 개(자신과 내부 호스트 사용자 간, 자신과 외부 호스트 TCP 사용자 간)의 TCP 연결을 설정한다.
ㄹ. 내부 IP 주소를 숨길 수 있다.

① 패킷 필터링(Packet Filtering) 침입 차단 시스템
② 회로 레벨 프록시(Circuit - Level Proxy) 침입 차단 시스템
③ 응용 프록시(Application Proxy Gateway) 침입 차단 시스템
④ 스테이트풀 패킷 검사(Stateful Packet Inspection) 침입 차단 시스템

정답 2번

출제 포인트

종단 간 연결의 중계 방식과 검사 계층을 기준으로 패킷 필터링, 회로 레벨 프록시, 응용 프록시, 스테이트풀 패킷 검사를 구별하는 문제이다.

핵심 개념

회로 레벨 프록시는 전송 계층 수준에서 내부 호스트와 외부 호스트 사이의 연결을 대신 중계하는 방화벽이다. 클라이언트와 프록시 사이, 프록시와 외부 서버 사이에 각각 TCP 연결을 만들므로 직접적인 종단-대-종단 연결이 형성되지 않고 내부 IP 주소를 감출 수 있다. 응용 데이터의 내용까지 세밀하게 검사하는 응용 프록시와 달리, 회로 레벨 프록시는 연결 설정과 세션 중계에 초점을 둔다.

NoteBase

선지별 해설

① X — 패킷 필터링 침입 차단 시스템은 주로 출발지·목적지 IP 주소, 포트 번호, 프로토콜 등 패킷 헤더의 규칙으로 통과 여부를 결정한다. '두 개의 TCP 연결을 설정한다'는 설명이 맞지 않으며, 올바르게는 '각 패킷의 헤더 정보를 필터링한다'이다.
② O — 회로 레벨 프록시는 내부 사용자와 프록시, 프록시와 외부 호스트 사이에 두 개의 TCP 연결을 설정한다. 따라서 직접적인 종단-대-종단 TCP 연결을 허용하지 않고 내부 IP 주소를 숨길 수 있으며, 내부 사용자를 신뢰하는 환경에서 주로 사용한다.
③ X — 응용 프록시 침입 차단 시스템은 HTTP, FTP 등 특정 응용 서비스별로 동작하며 응용 계층의 명령과 데이터 내용을 검사·중계한다. 제시문의 결정적 표현인 '내부 사용자를 신뢰할 경우 일반적으로 사용한다'는 회로 레벨 프록시의 특성이다. 올바르게는 '특정 응용 서비스의 프로토콜과 데이터까지 검사하여 중계한다'이다.
④ X — 스테이트풀 패킷 검사 침입 차단 시스템은 연결 상태표를 유지하면서 패킷이 정상적인 세션에 속하는지를 판단한다. '자신을 기준으로 두 개의 TCP 연결을 설정한다'는 설명이 맞지 않으며, 올바르게는 '하나의 통신 세션에 속한 패킷의 연결 상태를 추적하여 허용 여부를 결정한다'이다.

오답 포인트

응용 프록시도 연결을 중계하고 내부 주소를 숨길 수 있어 ③이 매력적으로 보인다. 그러나 제시문은 응용 데이터 검사라는 단서 없이 내부 사용자를 신뢰하고 전송 계층의 두 연결만 중계한다고 했으므로 회로 레벨 프록시를 가리킨다.

다시 나오면 이렇게 판단

'두 개의 TCP 연결', '종단 간 직접 연결 차단', '내부 IP 은닉', '신뢰하는 내부 사용자'가 함께 나오면 회로 레벨 프록시로 판단한다. 응용 명령·데이터 검사가 강조되면 응용 프록시, 패킷 헤더 규칙이면 패킷 필터링, 연결 상태표 추적이면 스테이트풀 패킷 검사이다.

암기 포인트

회로 레벨 프록시는 TCP 연결을 둘로 나누어 세션을 중계하고, 응용 프록시는 응용 데이터까지 검사한다.

NoteBase

문 12. 다음 중 사용자 패스워드의 보안을 강화하기 위한 솔트(Salt)에 대한 설명으로 가장 옳지 않은 것은?

① 여러 사용자에 의해 중복 사용된 동일한 패스워드가 서로 다르게 저장되도록 한다.

② 솔트 값은 보안 강화를 위하여 암호화된 상태로 패스워드 파일에 저장되어야 한다.

③ 한 사용자가 동일한 패스워드를 두 개 이상의 시스템에 사용해도 그 사실을 알기 어렵게 한다.

④ 해시(Hash) 연산 비용이 증가되어 오프라인의 사전 공격을 어렵게 만든다.

정답 2번

출제 포인트

이 문제는 패스워드 해시에 솔트를 사용하는 목적과 솔트의 공개 가능성을 구분하는 문제이다.

핵심 개념

솔트는 각 패스워드에 덧붙여 해시하는 고유한 임의의 값이다. 같은 패스워드라도 솔트가 다르면 해시 결과가 달라지므로 해시의 재사용·비교와 미리 계산한 사전 또는 레인보 테이블의 활용을 어렵게 한다. 솔트는 비밀키가 아니므로 암호화할 필요가 없으며, 일반적으로 해시값과 함께 저장한다.

선지별 해설

① O — 사용자마다 서로 다른 솔트를 적용하면 같은 패스워드를 사용하더라도 입력값이 달라져 저장되는 해시값도 달라진다.
② X — 틀린 표현은 '솔트 값은 암호화된 상태로 저장되어야 한다'이다. 솔트의 보안 목적은 비밀 유지가 아니라 해시값의 고유화이므로, 올바르게는 솔트를 암호화하지 않고 패스워드 해시값과 함께 저장할 수 있다.
③ O — 시스템마다 서로 다른 솔트를 사용하면 동일한 패스워드에서도 서로 다른 해시값이 생성되므로, 저장된 해시값만 비교하여 패스워드 재사용 사실을 알아내기 어렵다.
④ O — 솔트는 미리 계산해 둔 사전·레인보 테이블의 재사용을 막고 각 솔트에 대해 후보 패스워드를 다시 해시하게 하므로 오프라인 사전 공격의 전체 연산 비용을 증가시킨다. 다만 한 번의 해시 자체를 느리게 만드는 기능은 반복 횟수나 전용 패스워드 해시 함수가 담당한다.

오답 포인트

암호화되지 않은 값은 모두 취약하다고 생각하면 ②를 놓치기 쉽다. 솔트는 공개되어도 되는 값이고, 공격자가 여러 계정이나 시스템에서 같은 해시를 재사용하지 못하게 만드는 데 목적이 있다. 또한 ④의 연산 비용 증가는 개별 해시 한 번의 속도가 아니라 공격 전체에서 반복해야 하는 계산량이 늘어난다는 뜻이다.

다시 나오면 이렇게 판단

솔트 관련 선지는 '비밀로 보관하는가'가 아니라 '사용자·패스워드마다 다르게 부여하여 같은 패스워드의 해시를 다르게 만드는가'를 기준으로 판단한다. 솔트의 핵심 효과는 사전 계산 결과의 재사용 차단이다.

NoteBase

암기 포인트

솔트는 숨기는 값이 아니라 섞는 값이다. 서로 다른 솔트는 같은 패스워드도 서로 다른 해시로 만든다.

NoteBase

문 13. <보기>의 설명에 해당하는 네트워크 보안 솔루션은?

ㄱ. 사용자 컴퓨터 및 네트워크 단말기가 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사하여 네트워크 접속을 통제하는 기술
ㄴ. 네트워크 접근제어 기술을 이용하여 내부 네트워크의 자원을 관리하고, 네트워크 내의 장애 및 사고 원인을 예방·탐지하고 제거하여 안정적인 네트워크 운영·관리가 가능

① 역추적 시스템
② NAC
③ UTM
④ ESM

정답 2번

출제 포인트

네트워크 접속 전에 단말의 보안정책 준수 여부를 검사하고 접속을 허용·차단하는 NAC의 특징을 다른 보안 솔루션과 구별하는 문제이다.

핵심 개념

NAC(Network Access Control)는 사용자와 단말이 네트워크에 접속하기 전에 보안 상태와 정책 준수 여부를 검사하고, 그 결과에 따라 접속을 허용·제한·격리하는 네트워크 접근제어 기술이다. 또한 접속 단말과 내부 네트워크 자원을 파악·관리하여 장애와 보안사고의 예방·탐지·대응을 지원한다.
역추적 시스템은 침해사고의 공격 근원지와 경로를 추적하는 기술이고, UTM은 여러 보안 기능을 하나의 장비나 체계에 통합한 솔루션이며, ESM은 여러 보안 장비의 로그와 이벤트를 통합하여 관제하는 시스템이다.

NoteBase

선지별 해설

① X — 역추적 시스템은 공격 패킷이나 로그 등을 분석하여 공격의 발신지와 이동 경로를 추적한다. 틀린 부분은 접속 전 정책 준수 여부를 검사하여 접근을 통제하는 기능으로 본 점이며, 올바르게는 이러한 기능은 NAC에 해당한다.
② O — NAC는 단말이 네트워크에 접근하기 전에 보안정책 준수 여부를 검사하고, 검사 결과에 따라 접속을 허용하거나 차단·격리한다. 제시문의 '접근 전 검사', '접속 통제', '내부 네트워크 자원 관리'가 모두 NAC의 핵심 기능에 해당한다.
③ X — UTM(Unified Threat Management)은 방화벽, 침입 탐지·방지, 가상사설망, 악성코드 차단 등 여러 보안 기능을 통합하여 제공한다. 틀린 부분은 UTM을 단말의 접속 전 보안상태 검사와 접근제어 기술로 본 점이며, 올바르게는 제시문의 기술은 NAC이다.
④ X — ESM(Enterprise Security Management)은 여러 보안 장비와 시스템에서 발생한 로그·이벤트를 모아 상관분석하고 중앙에서 통합 관제한다. 틀린 부분은 ESM을 네트워크 접속 자체를 허용·차단하는 기술로 본 점이며, 올바르게는 제시문의 기술은 NAC이다.

오답 포인트

'네트워크 내의 장애 및 사고 원인을 예방·탐지'라는 표현만 보면 통합 보안 솔루션인 UTM이나 통합 관제 시스템인 ESM으로 오인하기 쉽다. 그러나 '단말기가 네트워크에 접근하기 전에', '보안정책 준수 여부 검사', '접속 통제'가 NAC를 결정하는 표현이다.

다시 나오면 이렇게 판단

접속 전에 단말의 보안 상태를 점검하고 허용·차단·격리하면 NAC, 여러 보안 기능을 한 체계에 묶으면 UTM, 여러 장비의 로그와 이벤트를 통합 관제하면 ESM, 공격의 출발지와 경로를 찾아가면 역추적 시스템으로 판단한다.

암기 포인트

NAC는 '접속 전 검사와 접근 통제', UTM은 '보안 기능 통합', ESM은 '로그·이벤트 통합 관제', 역추적은 '공격 근원지 추적'이다.

NoteBase

문 14. 다음 중 비밀키 시스템에 대한 설명으로 맞는 것은 몇 개 인가?

ㄱ. 암호화 키와 복호화 키가 다름
ㄴ. 암호화 과정이 복잡하여 속도가 느림
ㄷ. 디지털 서명이 어려움
ㄹ. 평문을 암호화하는데 가장 많이 사용됨
ㅁ. RSA, PGP 암호 알고리즘이 가장 대표적임

① 2
② 3
③ 4
④ 5

정답 1번

출제 포인트

비밀키 시스템의 키 구조, 처리 속도, 디지털 서명 가능성, 주된 용도와 대표 알고리즘을 구분하여 옳은 설명의 개수를 판단하는 문제이다.

핵심 개념

비밀키 시스템은 송신자와 수신자가 같은 비밀키를 공유하여 암호화와 복호화를 수행하는 방식이다. 공개키 시스템보다 연산이 단순하고 빠르므로 대량의 평문을 암호화하는 데 주로 사용되지만, 같은 키를 공유하므로 누가 메시지를 만들었는지 제3자에게 입증하는 디지털 서명에는 적합하지 않다.
ㄱ X: 암호화 키와 복호화 키는 서로 다르지 않고 같다.
ㄴ X: 암호화 과정은 공개키 방식보다 단순하여 처리 속도가 빠르다.
ㄷ O: 동일한 비밀키를 양쪽이 공유하므로 서명자를 고유하게 증명하기 어려워 디지털 서명에 적합하지 않다.
ㄹ O: 처리 속도가 빠르므로 평문이나 대용량 데이터를 실제로 암호화하는 데 널리 사용된다.
ㅁ X: RSA는 대표적인 공개키 알고리즘이며, PGP는 비밀키와 공개키 방식을 함께 사용하는 혼합형 시스템이다. 대표적인 비밀키 알고리즘으로는 DES, 3DES, AES 등이 있다.
따라서 옳은 설명은 ㄷ과 ㄹ의 2개이다.

선지별 해설

① O: 옳은 설명은 ㄷ과 ㄹ, 모두 2개이므로 맞다.
② X: ‘3개’가 틀린 표현이다. 옳은 설명은 2개이다.
③ X: ‘4개’가 틀린 표현이다. 옳은 설명은 2개이다.
④ X: ‘5개’가 틀린 표현이다. 옳은 설명은 2개이다.

NoteBase

오답 포인트

ㄱ의 '키가 다름'은 공개키 시스템의 특징이고, ㄴ의 '속도가 느림'도 공개키 시스템의 일반적 특징이다. 또한 PGP를 하나의 비밀키 암호 알고리즘으로 오인하면 ㅁ까지 맞다고 세기 쉽지만, PGP는 공개키와 비밀키 암호를 결합해 사용하는 시스템이다.

다시 나오면 이렇게 판단

비밀키 방식은 '같은 키, 빠른 속도, 대량 데이터 암호화'로 판단하고, 공개키 방식은 '서로 다른 키, 상대적으로 느린 속도, 키 교환과 디지털 서명'으로 판단한다. 각 진술을 먼저 O/X로 확정한 뒤 O의 개수를 선택지와 대응한다.

암기 포인트

비밀키는 같은 키로 빠르게 본문을 암호화하고, 공개키는 서로 다른 키로 키 교환과 서명을 담당한다.

NoteBase

문 15. 다음 중 세션 하이재킹(Session Hijacking)에 대한 설명으로 틀린 것은?

① TCP의 취약점을 이용한 능동적 공격 방법이다.

② Telnet, FTP 등 TCP를 사용한 모든 세션의 갈취가 가능하다.

③ TCP의 Sequence Number를 이용한 공격이다.

④ TCP의 취약점을 이용하여 클라이언트와 서버 양쪽 모두 데이터 전송을 못하게 하는 공격이다.

정답 4번

출제 포인트

TCP 세션 하이재킹의 목적과 공격 원리를 서비스 거부 공격과 구별하는 문제이다.

핵심 개념

세션 하이재킹은 이미 인증되어 통신 중인 정상 세션을 공격자가 가로채 정상 사용자로 가장하는 능동적 공격이다. TCP 세션에서는 현재 시퀀스 번호를 알아내거나 예측하여 정상 패킷처럼 보이는 패킷을 삽입하고, 기존 연결의 동기 상태를 교란한 뒤 세션을 장악한다. 핵심 목적은 통신 자체를 양쪽 모두에게 불가능하게 만드는 것이 아니라 인증된 연결을 탈취하여 공격자가 그 연결을 이용하는 데 있다.

선지별 해설

① O — TCP 연결의 상태 관리와 패킷 식별 방식을 악용하여 이미 성립한 세션에 공격자가 개입하므로 능동적 공격에 해당한다.
② O — Telnet과 FTP처럼 TCP 기반으로 세션을 유지하는 서비스는 세션 하이재킹의 공격 대상이 될 수 있다. 여기서 '갈취가 가능하다'는 TCP를 사용하는 모든 세션이 반드시 탈취된다는 뜻이 아니라, 필요한 세션 정보와 공격 조건이 갖추어지면 해당 종류의 세션을 탈취할 수 있다는 의미이다.
③ O — TCP 세션 하이재킹에서는 수신 측이 정상 데이터로 받아들이도록 적절한 Sequence Number를 가진 위조 패킷을 삽입하는 것이 핵심이다.
④ X — 틀린 부분은 '클라이언트와 서버 양쪽 모두 데이터 전송을 못하게 하는 공격'이라는 표현이다. 이는 통신 가용성을 떨어뜨리는 서비스 거부 공격의 설명에 가깝다. 올바르게는 정상 클라이언트의 세션 동기를 깨뜨리고 공격자가 클라이언트를 가장하여 서버와의 기존 세션을 탈취하는 공격이다.

오답 포인트

세션을 교란하는 과정에서 정상 클라이언트의 통신이 끊길 수 있다는 점을 '양쪽 모두 전송 불가'로 확대하면 ④를 맞는 설명으로 오인하게 된다. 세션 하이재킹의 결과는 단순한 통신 마비가 아니라 공격자의 세션 장악이다.

NoteBase

다시 나오면 이렇게 판단

공격 설명에서 '인증된 연결 탈취·사용자 가장·Sequence Number 조작'이 나타나면 세션 하이재킹으로 판단한다. '서비스를 이용하지 못하게 함·양쪽 통신 마비'가 중심이면 서비스 거부 공격과 구별한다.

암기 포인트

세션 하이재킹은 연결을 끊는 공격이 아니라 Sequence Number를 맞춰 인증된 연결을 빼앗는 공격이다.

NoteBase

문 16. 다음 중 DNS 레코드에 대한 설명으로 가장 옳지 않은 것은?

① CNAME 레코드 : 여러 개의 호스트가 같은 IP 주소로 응답할 경우 설정이 용이하다.

② MX 레코드 : 메일 서버가 이메일을 전달하기 위해 DNS에서 읽어오는 레코드이다.

③ NS 레코드 : 역방향 영역 안에서 IP를 도메인 주소로 변경하기 위한 호스트 등록작업을 한다.

④ A 레코드 : 호스트는 각 영역별로 중복될 수는 있지만 같은 영역 안에 중복된 호스트가 있으면 안된다.

정답 3번

출제 포인트

DNS의 주요 자원 레코드인 CNAME, MX, NS, A, PTR의 역할을 구별하는 문제이다.

핵심 개념

A는 호스트 이름을 IPv4 주소에 대응시키고, CNAME은 별칭을 정규 이름에 대응시킨다. MX는 해당 도메인의 메일을 받을 서버를 지정하고, NS는 해당 DNS 영역을 담당하는 권한 있는 네임 서버를 지정한다. IP 주소를 호스트 이름으로 찾는 역방향 조회에는 PTR 레코드를 사용한다.

선지별 해설

① O — CNAME은 여러 별칭을 하나의 정규 호스트 이름에 연결할 수 있다. 정규 이름의 A 레코드만 관리하면 되므로 여러 이름이 같은 IP 주소를 가리키게 할 때 관리가 편리하다.
② O — MX는 도메인의 메일 수신 서버와 우선순위를 나타낸다. 송신 측 메일 서버는 DNS의 MX 레코드를 조회하여 메일을 전달할 서버를 결정한다.
③ X — 틀린 부분은 'NS 레코드'이다. NS는 영역을 담당하는 네임 서버를 지정한다. 역방향 영역에서 IP 주소를 도메인 이름에 대응시키는 호스트 등록에는 PTR 레코드를 사용한다.
④ O — 서로 다른 DNS 영역에서는 같은 상대 호스트 이름을 사용할 수 있는데, 영역 이름까지 붙인 전체 도메인 이름이 달라지기 때문이다. 같은 영역 안에서는 같은 이름을 별개의 호스트 이름으로 중복 등록하는 것이 아니라 하나의 DNS 이름으로 관리한다. 같은 이름에 여러 A 값을 둔 경우도 별도 이름의 중복이 아니라 하나의 RRset이다.

오답 포인트

③은 '영역을 담당하는 서버'를 나타내는 NS와 '역방향 주소 변환'을 담당하는 PTR을 바꾸어 놓았다. 정방향과 역방향의 대응 방향을 구분하지 않으면 NS를 역방향 레코드로 오인하기 쉽다.

다시 나오면 이렇게 판단

레코드 이름보다 대응 관계를 먼저 확인한다. 이름→IPv4는 A, 별칭→정규 이름은 CNAME, 도메인→메일 서버는 MX, 영역→권한 네임 서버는 NS, IP 주소→이름은 PTR이다.

NoteBase

암기 포인트

A는 주소, CNAME은 별칭, MX는 메일, NS는 네임 서버, PTR은 역방향 이름 조회이다.

NoteBase

문 17. 다음에서 설명하는 것은 무엇인가?

ㄱ. 초기에는 PPP(Point to Point Protocol)에서 사용하기 위해 개발되었으나, 현재는 무선랜 표준인 IEEE 802.1x에서 사용자 인증 방법으로 사용
ㄴ. 어떤 링크에도 접속이 가능한 단순한 캡슐화 개념의 프로토콜로 모든 링크에 적용될 수 있으며 다양한 인증 방법을 사용 할 수 있도록 설계됨
ㄷ. 네트워크 접근을 위한 인증 서버와 무선장비 사이에 상호 인정을 허용

① SSID
② WEP
③ EAP
④ MAC

정답 3번

출제 포인트

이 문제는 무선 LAN 인증에서 EAP의 역할을 SSID, WEP, MAC과 구별하는 문제이다.

핵심 개념

EAP(Extensible Authentication Protocol)는 하나의 인증 방식 자체가 아니라 여러 인증 방법을 실어 나를 수 있도록 만든 확장 가능한 인증 프레임워크이다. 처음에는 PPP 인증을 확장하기 위해 개발되었고, IEEE 802.1X 기반 네트워크 접근 인증에도 사용된다. 인증 과정에서는 무선 AP와 같은 인증자가 단말과 인증 서버 사이의 EAP 메시지를 중계하며, 선택한 EAP 방식에 따라 상호 인증도 지원할 수 있다.

NoteBase

선지별 해설

① SSID — X
SSID는 무선 LAN을 식별하는 네트워크 이름이다. 여러 인증 방법을 캡슐화하고 IEEE 802.1X 인증에 사용하는 프로토콜이라는 설명과 맞지 않는다. 틀린 개념인 SSID를 올바르게 고치면 EAP이다.

② WEP — X
WEP는 무선 LAN 통신의 기밀성을 위해 사용된 초기 보안 방식으로, 여러 인증 방법을 수용하는 확장형 인증 프레임워크가 아니다. 틀린 개념인 WEP를 올바르게 고치면 EAP이다.

③ EAP — O
EAP는 PPP용으로 출발한 확장형 인증 프로토콜이며 IEEE 802.1X에서 다양한 인증 방법을 운반하는 데 사용된다. 지문의 PPP, IEEE 802.1X, 다양한 인증 방법이라는 단서가 모두 EAP를 가리킨다.

④ MAC — X
MAC은 데이터 링크 계층에서 장치를 식별하는 주소 또는 매체 접근 제어를 뜻한다. MAC 주소를 이용한 접근 제한은 가능하지만, 지문처럼 다양한 인증 방법을 캡슐화하는 프로토콜은 아니다. 틀린 개념인 MAC을 올바르게 고치면 EAP이다.

오답 포인트

IEEE 802.1X가 무선 LAN 보안에 사용된다는 이유만으로 WEP를 고르기 쉽다. 그러나 WEP는 암호화 방식이고, EAP는 여러 인증 방식을 수용하여 인증 메시지를 교환하게 하는 프레임워크라는 차이가 핵심이다.

다시 나오면 이렇게 판단

PPP에서 출발, IEEE 802.1X에서 사용, 여러 인증 방법 지원이라는 단서가 함께 나오면 EAP로 판단한다.
네트워크 이름은 SSID, 초기 무선 암호화는 WEP, 장치 식별 주소는 MAC으로 구분한다.

암기 포인트

EAP는 인증 방법을 확장해 담는 틀, SSID는 이름, WEP는 암호화, MAC은 주소이다.

NoteBase

문 18. 다음에서 설명하고 있는 서비스 공격기법에 해당하는 것은?

ㄱ. TCP의 3-Way Handshake의 취약점을 이용한 공격
ㄴ. 출발지 IP주소를 존재하지 않는 IP주소로 변조한 후 다량의 SYN패킷을 전송하여 공격대상 시스템의 백로그 큐(Backlog Queue)를 가득 채워 시스템을 마비시키는 공격
ㄷ. 시스템은 백로그 큐의 모든 자원을 소모하여 정상적인 서비스 불가능

① Smurfing
② SYN Flooding
③ LAND Attack
④ Teardrop

정답 2번

출제 포인트

TCP 3-Way Handshake 과정에서 대량의 SYN 패킷으로 연결 대기 자원을 고갈시키는 SYN Flooding의 특징을 구별하는 문제이다.

핵심 개념

SYN Flooding은 위조한 출발지 IP 주소로 다량의 SYN 패킷을 보내 서버가 불완전한 연결 정보를 백로그 큐에 계속 유지하게 함으로써 정상적인 연결을 방해하는 서비스 거부 공격이다.
Smurfing은 브로드캐스트 주소와 위조된 피해자 IP 주소를 이용한 ICMP 증폭 공격이고, LAND Attack은 출발지와 목적지의 IP 주소 및 포트를 피해 시스템의 동일한 값으로 조작하는 공격이며, Teardrop은 비정상적으로 겹치는 IP 단편을 전송해 재조립 과정의 취약점을 악용하는 공격이다.

선지별 해설

① X — Smurfing은 피해자의 IP 주소로 출발지를 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 집중되게 하는 공격이다. 이 문항의 ‘TCP 3-Way Handshake와 백로그 큐 고갈’이라는 설명은 Smurfing이 아니라 SYN Flooding에 해당한다.
② O — SYN Flooding은 다량의 SYN 패킷으로 서버에 반쯤 열린 연결을 누적시켜 백로그 큐를 소진하고 정상적인 TCP 연결을 거부하게 한다. 제시문의 공격 과정과 정확히 일치한다.
③ X — LAND Attack은 패킷의 출발지와 목적지 IP 주소 및 포트를 모두 공격 대상의 동일한 값으로 설정하여 시스템이 자기 자신과 통신하도록 만드는 공격이다. ‘존재하지 않는 출발지 IP 주소와 다량의 SYN 패킷으로 백로그 큐를 채우는 공격’은 LAND Attack이 아니라 SYN Flooding이다.
④ X — Teardrop은 오프셋을 비정상적으로 조작한 중첩 IP 단편을 보내 수신 시스템의 단편 재조립 취약점을 악용하는 공격이다. ‘TCP 연결 대기 큐를 고갈시키는 공격’은 Teardrop이 아니라 SYN Flooding이다.

NoteBase

오답 포인트

SYN Flooding과 LAND Attack은 모두 조작된 SYN 패킷을 사용할 수 있어 혼동하기 쉽다. 그러나 '다량의 SYN', '반쯤 열린 연결', '백로그 큐 고갈'이 함께 나오면 SYN Flooding이고, 출발지와 목적지를 공격 대상의 동일한 주소와 포트로 맞추면 LAND Attack이다.

다시 나오면 이렇게 판단

공격에 사용된 프로토콜과 고갈되거나 오작동하는 지점을 확인한다. TCP 연결 요청과 백로그 큐는 SYN Flooding, ICMP 브로드캐스트 증폭은 Smurfing, 동일한 출발지·목적지는 LAND Attack, 비정상 IP 단편 재조립은 Teardrop으로 판단한다.

암기 포인트

SYN Flooding은 SYN을 쌓아 백로그 큐를 고갈시키는 공격이다.

NoteBase

문 19. 다음은 보안시스템들에 대한 설명이다. (가), (나)에 들어갈 용어로 알맞은 것은?

(가)은(는) 외부 침입에 대한 정보를 수집하고 분석하여 침입활동을 탐지해 이에 대응하도록 보안 담당자에게 통보하는 기능을 수행하는 네트워크 보안 시스템이다. (나)은(는) 침입을 탐지했을 경우에 이에 대한 대처까지 수행한다. 즉, (나)은(는) 예방적이고 사전에 조치를 취하는 기술이고, (가)은(는) 탐지적이고 사후에 조치를 취하는 기술이다.

① (가): IDS, (나): Firewall

② (가): IDS, (나): IPS

③ (가): Firewall, (나): IPS

④ (가): Firewall, (나): IDS

정답 2번

출제 포인트

침입을 탐지해 관리자에게 알리는 IDS와 침입을 탐지한 뒤 차단·방어 조치까지 수행하는 IPS의 차이를 묻는 문제이다.

핵심 개념

IDS(Intrusion Detection System)는 네트워크나 시스템의 침입 징후를 탐지·분석하고 관리자에게 경보하는 침입 탐지 시스템이다.
IPS(Intrusion Prevention System)는 침입 징후를 탐지할 뿐 아니라 의심 트래픽 차단 등 예방 조치까지 수행하는 침입 방지 시스템이다.
Firewall은 미리 정한 보안 정책에 따라 네트워크 트래픽의 통과 여부를 통제하는 방화벽이다.

NoteBase

선지별 해설

① X
(가)의 IDS는 맞지만, (나)의 Firewall이 틀렸다. 침입 탐지 후 대처까지 수행하는 (나)는 IPS이다.

② O
(가)는 침입 정보를 수집·분석해 탐지하고 관리자에게 통보하는 IDS이고, (나)는 탐지 후 차단 등 대처까지 수행하는 IPS이다.

③ X
(나)의 IPS는 맞지만, (가)의 Firewall이 틀렸다. 탐지적·사후 대응 중심으로 설명된 (가)는 IDS이다.

④ X
(가)와 (나)가 모두 틀렸다. (가)는 Firewall이 아니라 IDS이고, (나)는 IDS가 아니라 IPS이다. 올바른 연결은 (가): IDS, (나): IPS이다.

오답 포인트

Firewall도 네트워크 접근을 통제하므로 IPS와 혼동하기 쉽다. 그러나 이 문제의 결정적 표현은 '탐지하여 통보'와 '탐지 후 대처까지 수행'이다. 전자는 IDS, 후자는 IPS에 해당한다.

다시 나오면 이렇게 판단

설명에서 경보·통보까지만 하면 IDS, 탐지와 함께 차단·방어까지 하면 IPS로 판단한다. 미리 정한 정책에 따른 트래픽 허용·차단이 중심이면 Firewall로 구분한다.

암기 포인트

IDS는 Detect(탐지), IPS는 Prevent(방지), Firewall은 정책에 따른 통행 통제이다.

NoteBase

문 20. 다음에서 설명하고 있는 네트워크 공격 기법은 무엇인가?

ㄱ. 공격자는 출발지 IP로 스푸핑하여 SYN패킷을 공격 경유지 서버로 전송한다.
ㄴ. SYN패킷을 받은 경유지 서버는 스푸핑된 IP의 타깃 서버로 SYN/ACK를 전송한다.
ㄷ. 타깃 서버는 수많은 SYN/ACK를 받아 다운된다.

① DoS
② DDoS
③ DRDos
④ SYN Flooding

정답 3번

출제 포인트

출발지 IP를 피해자 주소로 위조하고 여러 경유지 서버의 응답이 피해자에게 향하게 하는 DRDoS의 반사·분산 구조를 묻는 문제이다.

핵심 개념

DoS는 한 공격 주체가 대상의 자원을 고갈시켜 서비스를 방해하는 공격이다.
DDoS는 다수의 공격원이 동시에 대상을 공격하는 분산 서비스 거부 공격이다.
DRDoS(Distributed Reflection DoS)는 피해자의 IP로 출발지를 위조한 요청을 여러 반사 서버에 보내고, 그 서버들의 응답이 피해자에게 집중되게 하는 분산 반사 서비스 거부 공격이다. 핵심 흐름은 공격자 → 여러 경유지 서버 → 피해자이다.
SYN Flooding은 대량의 SYN을 대상 서버에 보내 반개방 연결을 쌓이게 하여 연결 자원을 고갈시키는 공격이다.

선지별 해설

① X — DoS는 서비스 거부 공격의 포괄적 명칭이며, 단순 DoS만으로는 여러 경유지 서버의 응답을 피해자에게 반사시키는 제시문의 구조를 정확히 나타내지 못한다. 틀린 표현은 'DoS'이며, 올바르게는 'DRDoS'이다.
② X — DRDoS는 넓게 보면 DDoS의 한 유형이지만, 제시문은 출발지 IP 스푸핑과 경유지 서버의 응답 반사를 명시하므로 더 구체적인 공격 기법은 DRDoS이다. 틀린 표현은 'DDoS'이며, 올바르게는 'DRDoS'이다.
③ O — 공격자가 피해자 IP로 출발지를 위조해 여러 경유지 서버에 SYN을 보내고, 경유지 서버들이 SYN/ACK를 피해자에게 전송하게 한다. 다수의 반사 서버가 만든 응답이 피해자에게 집중되므로 DRDoS에 해당한다.
④ X — SYN Flooding은 보통 공격자가 대상 서버에 대량의 SYN을 보내 대상에 반개방 연결 상태를 누적시키는 공격이다. 제시문처럼 경유지 서버들이 스푸핑된 피해자 주소로 SYN/ACK를 보내게 하는 반사 구조 자체를 가리키는 명칭은 아니다. 틀린 표현은 'SYN Flooding'이며, 올바르게는 'DRDoS'이다.

NoteBase

오답 포인트

제시문에 SYN과 SYN/ACK가 등장하므로 ④ SYN Flooding을 고르기 쉽다. 그러나 판단 기준은 패킷 종류가 아니라 전송 구조이다. 피해자 IP로 출발지를 위조하고 여러 경유지 서버의 응답을 피해자에게 돌려보내면 '분산 반사'가 핵심이다.

다시 나오면 이렇게 판단

출발지 주소가 피해자 IP로 위조되었는지, 요청이 여러 제3의 서버로 전송되는지, 그 서버들의 응답이 피해자에게 집중되는지를 차례로 확인한다. 세 요소가 함께 나타나면 DRDoS로 판단한다.

암기 포인트

DRDoS는 'D(분산) + R(반사) + DoS'이다. 피해자 주소로 위조한 요청을 여러 반사 서버에 보내 응답을 피해자에게 집중시킨다.

NoteBase