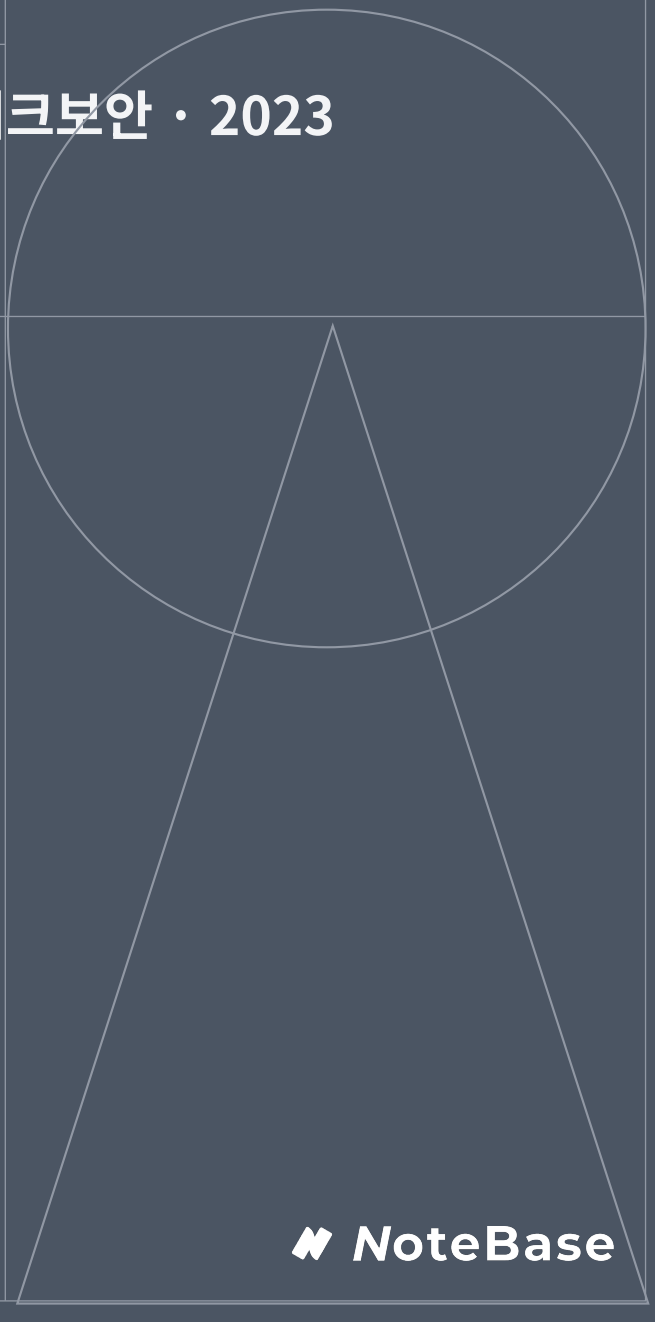
기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2023



NoteBase

기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2023

공무원/군무원/9급 · 네트워크보안 · 2023

1. 다음 중 같은 네트워크에서의 통신에서 악의적 사용자가 MAC 주소와 IP 주소의 맵핑 정보를 속이고자 할 때 악용되는 프로토콜로 옳은 것은?
① ARP ② SMTP
③ IP ④ ICMP

정답 1번

출제 포인트

같은 네트워크에서 IP 주소와 MAC 주소의 대응 정보를 관리하는 프로토콜과 ARP 스푸핑의 대상을 구별하는 문제이다.

핵심 개념

ARP는 같은 네트워크에서 목적지 IP 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 공격자가 거짓 ARP 응답을 보내 ARP 캐시에 잘못된 IP-MAC 대응 관계를 저장하게 만드는 공격을 ARP 스푸핑 또는 ARP 캐시 포이즈닝이라고 한다.
SMTP는 전자우편 전송, IP는 패킷의 주소 지정과 전달, ICMP는 오류 및 제어 메시지 전달에 사용된다.

선지별 해설

① O — ARP는 같은 네트워크에서 IP 주소를 MAC 주소로 대응시키며, 이 매핑 정보를 거짓으로 속이는 공격이 ARP 스푸핑이다.
② X — SMTP는 전자우편을 전송하는 프로토콜이므로 IP-MAC 매핑 정보를 속이는 대상이 아니다. 틀린 표현인 'SMTP'는 'ARP'로 고쳐야 한다.
③ X — IP는 논리 주소를 이용해 패킷을 전달하는 네트워크 계층 프로토콜이며, IP 주소와 MAC 주소의 매핑을 조회하는 프로토콜은 아니다. 틀린 표현인 'IP'는 'ARP'로 고쳐야 한다.
④ X — ICMP는 IP 통신 과정의 오류 보고와 진단·제어 메시지 전달에 사용되며, IP-MAC 매핑 정보를 관리하지 않는다. 틀린 표현인 'ICMP'는 'ARP'로 고쳐야 한다.

NoteBase

오답 포인트

문제에 IP 주소가 등장한다는 이유로 ③ IP를 고르기 쉽다. 그러나 공격 대상은 IP 패킷 자체가 아니라 같은 네트워크의 ARP 캐시에 저장되는 IP 주소와 MAC 주소의 대응 관계이다.

다시 나오면 이렇게 판단

‘같은 네트워크’, ‘IP 주소와 MAC 주소의 매핑’, ‘매핑 정보 위조’가 함께 제시되면 ARP 스푸핑으로 판단한다. 전자우편 전송은 SMTP, 패킷 주소 지정·전달은 IP, 오류·진단 메시지는 ICMP로 구별한다.

암기 포인트

IP-MAC 대응은 ARP, 그 대응 관계를 속이면 ARP 스푸핑이다.

NoteBase

2. IP 주소와 도메인 정보의 연관 정보를 위변조하는 공격을 탐지하고자 한다. IP 주소와 도메인 정보의 연관관계를 확인하기 위해 사용되는 명령어로 가장 적절한 것은?

① ping ② nslookup
③ arp ④ traceroute

정답 2번

출제 포인트

IP 주소와 도메인 이름의 대응 관계를 조회하는 DNS 질의 명령어를 구별하는 문제이다.

핵심 개념

nslookup은 DNS 서버에 질의하여 도메인 이름에 대응하는 IP 주소를 확인하거나, 역방향 조회를 통해 IP 주소에 대응하는 도메인 이름을 확인하는 명령어이다.
ping은 호스트의 통신 가능 여부, arp는 같은 네트워크 구간의 IP 주소와 MAC 주소 대응, traceroute는 목적지까지 거치는 경로를 확인하는 데 사용한다.

선지별 해설

① X — ping은 ICMP 메시지로 대상 호스트의 응답 여부와 왕복 시간을 확인한다. IP 주소와 도메인 정보의 연관관계를 조회하는 명령어라는 표현이 틀렸으며, 올바르게는 네트워크 연결 상태와 도달 가능성을 확인하는 명령어이다.
② O — nslookup은 DNS에 질의하여 도메인 이름과 IP 주소의 대응 관계를 확인할 수 있으므로 DNS 정보 위·변조 여부를 점검하는 데 가장 적절하다.
③ X — arp는 주로 동일한 로컬 네트워크에서 IP 주소와 MAC 주소의 대응 정보를 확인한다. IP 주소와 도메인 이름의 관계를 확인한다는 표현이 틀렸으며, 올바르게는 ARP 캐시의 IP-MAC 주소 매핑을 확인하는 명령어이다.
④ X — traceroute는 목적지까지 패킷이 거치는 라우터와 홉별 지연을 확인한다. IP 주소와 도메인 이름의 관계를 조회한다는 표현이 틀렸으며, 올바르게는 네트워크 전달 경로를 추적하는 명령어이다.

오답 포인트

모든 선지가 IP 주소를 다루는 네트워크 명령어이지만 확인 대상이 서로 다르다. 특히 arp의 IP-MAC 매핑과 nslookup의 도메인-IP 매핑을 혼동하기 쉽다.

다시 나오면 이렇게 판단

문제의 관계 대상을 먼저 확인한다. 도메인-IP는 nslookup, IP-MAC은 arp, 연결 여부는 ping, 전달 경로는 traceroute로 판단한다.

NoteBase

암기 포인트

이름-DNS는 nslookup, 이웃의 IP-MAC은 arp, 응답은 ping, 경로는 traceroute이다.

NoteBase

3. 보안관리자로서 특정 컴퓨터 내의 유입 및 유출 네트워크 트래픽 정보를 분석하고자 한다. 이러한 목적을 달성하기 위해 활용 가능한 소프트웨어로 적절하지 않은 것은?

① netstat ② nmap
③ wireshark ④ OllyDbg

정답 4번

출제 포인트

특정 컴퓨터의 유입·유출 네트워크 트래픽을 파악하는 도구와 실행 파일을 분석하는 디버거를 구분하는 문제이다.

핵심 개념

netstat은 현재 네트워크 연결, 수신 대기 포트, 라우팅 정보 등을 확인하는 명령어이다.
nmap은 호스트와 포트를 탐색하여 네트워크 서비스와 노출 상태를 조사하는 스캐닝 도구이다.
Wireshark는 패킷을 캡처하고 프로토콜별로 내용을 분석하는 네트워크 분석 도구이다.
OllyDbg는 실행 파일의 코드를 추적하며 동작을 분석하는 디버거로, 네트워크 트래픽 분석이 주된 용도가 아니다.

선지별 해설

① O — netstat은 특정 컴퓨터의 현재 연결과 수신 대기 포트 등을 보여 주므로 유입·유출 통신 상태를 확인하는 데 활용할 수 있다.
② O — nmap은 대상 호스트의 열린 포트와 서비스 등을 탐색하므로 네트워크 접근 상태를 조사하는 데 활용할 수 있다.
③ O — Wireshark는 송수신 패킷을 캡처하고 프로토콜과 필드 단위로 분석하므로 트래픽 분석 목적에 직접 적합하다.
④ X — OllyDbg를 네트워크 트래픽 분석 도구로 본 부분이 틀렸다. 올바르게는 OllyDbg는 실행 파일을 단계별로 추적하여 프로그램 동작을 분석하는 디버거이며, 패킷 기반 네트워크 트래픽 분석에는 Wireshark와 같은 도구를 사용한다.

오답 포인트

OllyDbg도 보안 분석에 쓰인다는 점 때문에 네트워크 분석 도구로 오인하기 쉽다. 그러나 이 문항은 보안 도구인지가 아니라 유입·유출 네트워크 트래픽을 분석하는 도구인지를 묻는다.

NoteBase

다시 나오면 이렇게 판단

도구가 연결·포트·패킷을 다루면 네트워크 관찰·분석 도구로 판단하고, 명령어 실행을 추적하거나 메모리·레지스터·실행 코드를 다루면 프로그램 디버깅 도구로 판단한다.

암기 포인트

netstat은 연결 상태, nmap은 포트 탐색, Wireshark는 패킷 분석, OllyDbg는 실행 파일 디버깅이다.

NoteBase

4. 다음 중 TCP 3-Way 핸드셰이크 절차가 갖는 특성을 이용하여 정상 사용자의 접속에 영향을 미치는 공격 기법에 해당하는 것은?
① Ping of Death
② HTTP Get Flooding
③ SYN Flooding
④ 스머핑(Smurfing) 공격

정답 3번

출제 포인트

TCP 3-Way 핸드셰이크의 미완료 연결을 악용하여 정상 사용자의 접속을 방해하는 공격을 구별하는 문제이다.

핵심 개념

SYN Flooding은 공격자가 다수의 SYN 패킷을 보내고 마지막 ACK를 완료하지 않아 서버에 반개방 연결을 쌓는 서비스 거부 공격이다. 서버의 연결 대기 자원이 소진되면 정상 사용자의 새 TCP 접속이 어려워진다.
Ping of Death는 비정상적으로 큰 ICMP 패킷을 이용하는 공격이고, HTTP GET Flooding은 다량의 HTTP GET 요청으로 웹 서버 자원을 소모시키는 공격이며, Smurf 공격은 출발지 IP를 피해자로 위조한 ICMP 요청을 브로드캐스트 주소로 보내 응답을 피해자에게 집중시키는 증폭 공격이다.

선지별 해설

① X — Ping of Death는 TCP 3-Way 핸드셰이크를 악용하는 공격이 아니다. 틀린 표현은 'Ping of Death'이며, 비정상적으로 큰 ICMP 패킷으로 시스템 장애를 유발하는 공격으로 고쳐야 한다.
② X — HTTP GET Flooding은 애플리케이션 계층에서 다량의 HTTP GET 요청을 보내 웹 서버 자원을 소모시킨다. 틀린 표현은 'HTTP Get Flooding'이며, 핸드셰이크의 반개방 연결을 악용하는 공격은 SYN Flooding으로 고쳐야 한다.
③ O — SYN Flooding은 SYN을 대량 전송한 뒤 마지막 ACK를 보내지 않아 서버의 반개방 연결 대기열과 관련 자원을 소진시킨다. 그 결과 정상 사용자의 TCP 접속이 방해된다.
④ X — Smurf 공격은 TCP 3-Way 핸드셰이크가 아니라 ICMP와 IP 스푸핑 및 브로드캐스트를 이용한 증폭 공격이다. 틀린 표현은 '스머핑(Smurfing) 공격'이며, 제시된 특징에 해당하는 공격은 SYN Flooding으로 고쳐야 한다.

오답 포인트

여러 서비스 거부 공격이 모두 서버 접속을 방해한다는 공통점만 보고 고르면 혼동하기 쉽다. 이 문항의 결정적 표현은 'TCP 3-Way 핸드셰이크'이며, SYN을 보낸 뒤 마지막 ACK를 완료하지 않는 공격은 SYN Flooding이다.

NoteBase

다시 나오면 이렇게 판단

TCP 연결 설정, SYN, 반개방 연결, 연결 대기열 고갈이 제시되면 SYN Flooding으로 판단한다. ICMP 대형 패킷은 Ping of Death, HTTP GET 요청의 대량 전송은 HTTP GET Flooding, ICMP 브로드캐스트 증폭은 Smurf 공격으로 구분한다.

암기 포인트

SYN은 연결을 시작하고 ACK는 연결을 완성한다. SYN만 쌓아 연결을 미완성 상태로 만드는 공격이 SYN Flooding이다.

NoteBase

5. 네트워크 인터페이스 카드에 무작위 모드(promiscuous mode)로 설정된 컴퓨터 단말장치가 네트워크 상에서 발견되었다. 해당 장치를 이용해 이루어질 가능성이 있는 공격으로 가장 적절한 것은?

① 스니핑 ② IP 스푸핑
③ Ping of Death ④ HTTP CC 공격

정답 1번

출제 포인트

네트워크 인터페이스 카드가 무작위 모드로 동작할 때 가능한 공격을 식별하는 문제이다.

핵심 개념

스니핑은 네트워크를 지나는 패킷을 몰래 수집하여 내용을 엿보는 수동적 공격이다. 무작위 모드는 네트워크 인터페이스 카드가 자기 주소로 온 프레임뿐 아니라 관찰 가능한 다른 프레임도 받아들이게 하므로 패킷 수집에 이용될 수 있다.
IP 스푸핑은 출발지 IP 주소를 위조하는 공격이고, Ping of Death는 비정상적으로 큰 IP 패킷이 재조립되도록 조작하여 시스템 장애를 유발하는 공격이며, HTTP CC 공격은 다수의 HTTP 요청으로 웹 서버 자원을 소모시키는 서비스 거부 공격이다.

선지별 해설

① O — 스니핑은 네트워크상의 패킷을 가로채 수집하는 공격이다. 네트워크 인터페이스 카드를 무작위 모드로 설정하면 관찰 가능한 다른 장치의 프레임까지 수신할 수 있으므로 해당 장치가 스니핑에 이용될 가능성이 있다.
② X — 틀린 표현은 'IP 스푸핑'이다. IP 스푸핑은 패킷의 출발지 IP 주소를 다른 주소로 위조하는 공격이며, 무작위 모드를 이용한 패킷 수집은 스니핑이다.
③ X — 틀린 표현은 'Ping of Death'이다. Ping of Death는 재조립 후 허용 크기를 넘도록 조작한 IP 패킷을 보내 시스템 오류나 장애를 유발하는 공격이며, 무작위 모드를 이용한 패킷 수집은 스니핑이다.
④ X — 틀린 표현은 'HTTP CC 공격'이다. HTTP CC 공격은 반복적이거나 대량의 HTTP 요청으로 웹 서버의 자원을 소모시키는 서비스 거부 공격이며, 무작위 모드를 이용한 패킷 수집은 스니핑이다.

오답 포인트

모두 네트워크 공격이라는 공통점만 보고 ②~④를 고르면 안 된다. 이 문제의 결정적 단서는 '네트워크 인터페이스 카드'와 '무작위 모드'이며, 이는 주소 위조나 비정상 패킷 전송, HTTP 요청 폭주가 아니라 패킷 수집과 연결된다.

NoteBase

다시 나오면 이렇게 판단

무작위 모드, 패킷 캡처, 트래픽 도청이 제시되면 스니핑으로 판단한다. 출발지 IP 위조는 IP 스푸핑, 비정상적으로 큰 패킷에 의한 장애는 Ping of Death, HTTP 요청 폭주는 HTTP CC 공격으로 구분한다.

암기 포인트

무작위 모드 → 패킷 수집 → 스니핑이다.

NoteBase

6. 네트워크 OSI 모델 7계층에서 응용 프로그램의 데이터 포맷에 관여하여 데이터의 암호화 및 복호화를 책임지는 영역으로 옳은 것은?
① 네트워크 계층 ② 전송 계층
③ 세션 계층 ④ 표현 계층

정답 4번

출제 포인트

OSI 7계층에서 데이터 표현 형식의 변환과 암호화·복호화를 담당하는 계층을 구별하는 문제이다.

핵심 개념

표현 계층은 응용 프로그램이 주고받는 데이터의 표현 형식을 맞추는 계층으로, 인코딩·형식 변환·압축·해제·암호화·복호화를 담당한다.
네트워크 계층은 경로 선택과 논리 주소 지정, 전송 계층은 종단 간 전송과 신뢰성 제어, 세션 계층은 통신 세션의 설정·유지·종료를 담당한다.

선지별 해설

① X — 네트워크 계층은 논리 주소를 바탕으로 경로를 선택하고 패킷을 전달하는 계층이다. 틀린 표현은 '네트워크 계층'이며, 데이터 형식과 암호화·복호화를 담당하는 계층은 표현 계층이다.
② X — 전송 계층은 종단 간 데이터 전송, 분할·재조립, 흐름·오류 제어 등을 담당한다. 틀린 표현은 '전송 계층'이며, 암호화·복호화는 표현 계층의 기능이다.
③ X — 세션 계층은 응용 프로그램 사이의 통신 세션을 설정·유지·종료하고 대화를 동기화한다. 틀린 표현은 '세션 계층'이며, 데이터 표현 형식의 변환은 표현 계층이 담당한다.
④ O — 표현 계층은 응용 프로그램의 데이터 형식을 변환하며 암호화와 복호화를 담당하므로 옳다.

오답 포인트

'응용 프로그램'이라는 말만 보고 응용 계층 주변의 기능을 막연히 고르면 안 된다. 문제의 결정적 단서는 '데이터 포맷'과 '암호화 및 복호화'이며, 이는 표현 계층의 대표 기능이다.

다시 나오면 이렇게 판단

형식 변환·인코딩·압축·암호화가 나오면 표현 계층, 세션의 연결 관리가 나오면 세션 계층, 종단 간 신뢰성 제어가 나오면 전송 계층, 주소와 경로 선택이 나오면 네트워크 계층으로 판단한다.

암기 포인트

표현 계층은 데이터의 표현을 바꾸는 계층이며, 변환·압축·암호화를 함께 묶어 기억한다.

NoteBase

7. 사용자 윈도우즈 PC 환경에서 hosts 파일에 대한 임의적 수정이 일어났음을 알게 되었다. 해당 파일의 수정으로 인해서 일어날 수 있는 공격 기법으로 가장 적절한 것은?
① 스머핑 공격 ② DNS 스푸핑
③ ARP 스푸핑 ④ IP 스푸핑

정답 2번

출제 포인트

hosts 파일 변조로 도메인 이름이 공격자가 지정한 IP 주소로 해석되는 공격과, 네트워크 계층별 스푸핑 공격의 차이를 구별하는 문제이다.

핵심 개념

DNS 스푸핑: 도메인 이름에 대응하는 IP 주소 정보를 거짓으로 조작하여 사용자를 공격자가 의도한 서버로 유도하는 공격이다. hosts 파일은 운영체제가 이름 해석에 사용하는 로컬 도메인-IP 매핑 정보이므로, 이를 변조하는 행위는 이름 해석 결과를 속이는 DNS 스푸핑에 해당한다.
스머핑 공격: 출발지 IP 주소를 피해자 주소로 위조한 ICMP 요청을 브로드캐스트망에 보내 다수의 응답이 피해자에게 집중되게 하는 증폭형 서비스 거부 공격이다.
ARP 스푸핑: 위조된 ARP 정보를 보내 특정 IP 주소와 공격자의 MAC 주소가 연결되도록 속이는 근거리 통신망 공격이다.
IP 스푸핑: IP 패킷의 출발지 IP 주소를 다른 주소로 위조하는 공격이다.

선지별 해설

① X — '스머핑 공격'은 틀린 표현이다. 스머핑 공격은 위조한 출발지 IP 주소와 ICMP 브로드캐스트를 이용해 응답 트래픽을 피해자에게 증폭시키는 서비스 거부 공격이며, hosts 파일의 이름 해석 정보를 변조하는 공격이 아니다. 올바르게는 hosts 파일 변조로 도메인-IP 매핑을 속이는 DNS 스푸핑이다.
② O — hosts 파일에 거짓 도메인-IP 매핑을 넣으면 사용자가 정상 도메인을 입력해도 공격자가 지정한 IP 주소로 접속할 수 있다. 이름 해석 결과를 조작한다는 점에서 DNS 스푸핑이 가장 적절하다.
③ X — 'ARP 스푸핑'은 틀린 표현이다. ARP 스푸핑은 근거리 통신망에서 거짓 ARP 정보를 이용해 IP 주소와 MAC 주소의 대응 관계를 조작하는 공격이며, hosts 파일의 도메인-IP 대응 관계를 변조하는 공격이 아니다. 올바르게는 DNS 스푸핑이다.
④ X — 'IP 스푸핑'은 틀린 표현이다. IP 스푸핑은 전송되는 IP 패킷의 출발지 IP 주소를 위조하는 공격이며, hosts 파일을 수정하여 이름 해석 목적지를 바꾸는 공격이 아니다. 올바르게는 DNS 스푸핑이다.

NoteBase

오답 포인트

hosts 파일에 IP 주소가 적혀 있다는 이유로 ④ IP 스푸핑을 고르기 쉽다. 그러나 판단 기준은 'IP가 등장하는가'가 아니라 '무엇의 대응 관계를 속이는가'이다. hosts 파일 변조는 도메인 이름과 IP 주소의 대응 관계를 속이므로 ② DNS 스푸핑이다.

다시 나오면 이렇게 판단

조작 대상을 먼저 확인한다. 도메인-IP 이름 해석은 DNS 스푸핑, IP-MAC 대응은 ARP 스푸핑, 패킷의 출발지 IP 위조는 IP 스푸핑, ICMP 브로드캐스트 응답 증폭은 스머핑 공격으로 판단한다.

암기 포인트

hosts 변조는 이름을 거짓 IP로 연결하므로 DNS 스푸핑이다. DNS는 도메인-IP, ARP는 IP-MAC, IP 스푸핑은 출발지 IP 위조이다.

NoteBase

8. 스푸핑 된 근원지 주소 A를 이용하여 TCP SYN Flooding 공격이 주소 B로 진행된 경우, TCP SYN을 발송하지 않은 주소 A 시스템은 갑작스럽게 주소 B로부터 SYN/ACK 패킷을 수신하게 된다. 이런 상황에서 주소 A 시스템이 주소 B로 전송하는 메시지의 TCP 메시지 플래그에 해당하는 것은?

① FIN ② RST
③ ACK ④ PSH

정답 2번

출제 포인트

스푸핑된 SYN 때문에 요청하지 않은 SYN/ACK를 받은 시스템이 TCP 연결을 거부할 때 사용하는 제어 플래그를 묻는 문제이다.

핵심 개념

RST: 존재하지 않거나 유효하지 않은 TCP 연결을 즉시 거부·초기화하는 플래그이다. 주소 A는 SYN을 보낸 적이 없어 주소 B와의 연결 상태가 없으므로, 갑자기 도착한 SYN/ACK에 RST로 응답한다.
FIN: 정상적으로 설정된 연결을 종료할 때 사용한다.
ACK: 수신한 세그먼트나 연결 요청을 확인할 때 사용한다.
PSH: 수신 데이터를 버퍼에 오래 두지 않고 응용 프로그램에 신속히 전달하도록 요구한다.

NoteBase

선지별 해설

① FIN — X
FIN은 정상적으로 성립한 TCP 연결을 순차적으로 종료할 때 사용하는 플래그이다. 틀린 표현은 'FIN'이며, 연결 상태가 없는 주소 A가 예상하지 못한 SYN/ACK를 거부할 때는 RST를 전송한다.

② RST — O
주소 A는 SYN을 전송하지 않았으므로 주소 B와의 연결 상태가 존재하지 않는다. 따라서 예상하지 못한 SYN/ACK에 대해 연결이 유효하지 않음을 알리는 RST를 전송한다.

③ ACK — X
ACK는 상대가 보낸 세그먼트를 정상적으로 수신했음을 확인하는 플래그이므로, 이를 보내면 SYN/ACK를 정상적인 연결 절차의 일부로 받아들이는 의미가 된다. 틀린 표현은 'ACK'이며, 요청하지 않은 SYN/ACK에는 RST로 연결을 거부한다.

④ PSH — X
PSH는 이미 연결된 TCP 통신에서 데이터를 응용 프로그램에 신속히 전달하도록 요구하는 플래그이며, 비정상 연결 요청을 거부하는 기능이 아니다. 틀린 표현은 'PSH'이며, 이 상황에 해당하는 플래그는 RST이다.

오답 포인트

SYN/ACK에 보통 ACK로 응답한다는 3-way handshake 절차만 떠올리기 쉽다. 그러나 주소 A는 최초 SYN을 보낸 적이 없으므로 정상 연결 절차가 아니며, ACK가 아니라 RST로 거부한다.

다시 나오면 이렇게 판단

먼저 수신 시스템에 해당 TCP 연결 상태가 실제로 존재하는지 판단한다. 정상 연결의 종료이면 FIN, 정상 수신 확인이면 ACK, 데이터의 즉시 전달 요구이면 PSH, 존재하지 않거나 비정상인 연결의 거부·초기화이면 RST이다.

암기 포인트

보낸 적 없는 SYN에 대한 SYN/ACK는 ACK가 아니라 RST로 거부한다.

NoteBase

9. TCP 세션 하이재킹이 성공하기 위해서 공격자가 알고 있어야 하는 정보로 가장 적절하지 않은 것은?
① 세션을 구성하는 IP 주소
② 세션을 구성하는 포트 번호
③ 세션 내에서 주고받아지는 패킷의 적절한 일련번호
④ 세션 내의 패킷을 주고받는 시간

정답 4번

출제 포인트

TCP 세션 하이재킹에 필요한 세션 식별 정보와 패킷 삽입에 필요한 TCP 상태 정보를 구별하는 문제이다.

핵심 개념

TCP 세션 하이재킹은 공격자가 이미 형성된 TCP 연결의 통신 주체인 것처럼 위장하여 패킷을 삽입하거나 세션을 가로채는 공격이다.
TCP 연결은 출발지 IP 주소, 목적지 IP 주소, 출발지 포트 번호, 목적지 포트 번호의 조합으로 식별된다. 여기에 현재 통신 흐름에 맞는 시퀀스 번호 등의 TCP 상태 정보가 있어야 수신 측이 위조 패킷을 정상 패킷으로 받아들일 수 있다. 반면 패킷을 주고받은 시간 자체는 세션을 식별하거나 유효한 패킷을 만드는 핵심 정보가 아니다.

선지별 해설

① O — 세션을 구성하는 양 끝점의 IP 주소는 TCP 연결의 통신 주체를 식별하고 출발지 주소를 위조하는 데 필요한 핵심 정보이다.
② O — 출발지와 목적지의 포트 번호는 어떤 응용 프로그램 사이의 TCP 연결인지 식별하는 핵심 정보이다.
③ O — 세션에서 사용 중인 적절한 시퀀스 번호를 알아야 수신 측의 TCP 수신 범위에 맞는 위조 패킷을 삽입할 수 있다.
④ X — 틀린 표현은 '패킷을 주고받는 시간'이 공격자가 반드시 알아야 할 정보라는 부분이다. 올바르게는 패킷 송수신 시간 자체가 아니라 세션의 현재 TCP 상태와 유효한 시퀀스 번호 등의 정보를 파악해야 한다.

오답 포인트

④의 '시간'을 패킷 삽입 시점과 혼동하기 쉽다. 공격 시점을 잡는 것은 도움이 될 수 있지만, 패킷의 송수신 시간 자체는 IP 주소·포트 번호·시퀀스 번호처럼 세션을 식별하거나 위조 패킷의 유효성을 결정하는 필수 정보가 아니다.

NoteBase

다시 나오면 이렇게 판단

TCP 세션 하이재킹의 필요 정보를 묻는 경우 먼저 연결 식별 정보인 양쪽 IP 주소와 포트 번호를 확인하고, 다음으로 패킷 수용 여부를 좌우하는 시퀀스 번호 등 TCP 상태 정보를 확인한다. 단순한 송수신 시간은 이 두 범주에 속하지 않는다.

암기 포인트

TCP 하이재킹의 핵심은 '누구와 연결되었는가'인 IP 주소·포트 번호와 '어느 순서인가'인 시퀀스 번호이다.

NoteBase

10. Linux 환경에서 상태기반 방화벽을 구축하고자 할 때 활용하게 되는 nf_conntrack의 상태 중 FTP 서비스의 제어를 위한 연결설정과 데이터 전송을 위한 연결설정 사이의 상태에 해당하는 것은?

① NEW ② INVALID
③ ESTABLISHED ④ RELATED

정답 4번

출제 포인트

이 문제는 nf_conntrack이 분류하는 연결 추적 상태 가운데, 기존 FTP 제어 연결과 새 FTP 데이터 연결의 관계를 묻는다.

핵심 개념

NEW: 새 연결을 시작하는 패킷이거나 아직 양방향 통신이 확인되지 않은 연결 상태이다.
INVALID: 패킷을 정상적인 연결로 식별하거나 추적할 수 없는 상태이다.
ESTABLISHED: 양방향 패킷이 확인되어 이미 성립한 연결 상태이다.
RELATED: 새로 생성된 연결이 이미 존재하는 다른 연결과 관련된 상태이다. FTP에서는 제어 연결과 데이터 연결이 별도로 만들어지므로, 데이터 연결은 기존 제어 연결에 대한 RELATED로 처리된다.

선지별 해설

① X — NEW는 새 연결이 시작되었지만 기존의 다른 연결과의 관련성이 상태의 핵심이 아닌 경우를 나타낸다. 이 문항의 FTP 데이터 연결은 기존 제어 연결에서 파생되므로, NEW가 아니라 RELATED가 올바르다.
② X — INVALID는 연결 추적 정보가 없거나 패킷을 정상적인 연결에 귀속시킬 수 없는 상태이다. 정상적인 FTP 제어 연결과 데이터 연결의 관계는 INVALID가 아니라 RELATED이다.
③ X — ESTABLISHED는 해당 연결 자체에서 양방향 통신이 확인되어 성립한 상태이다. 기존 제어 연결과 새 데이터 연결 사이의 관계를 나타내는 상태는 ESTABLISHED가 아니라 RELATED이다.
④ O — RELATED는 새 연결이 이미 추적 중인 기존 연결과 관련되어 있음을 뜻한다. FTP 데이터 연결은 FTP 제어 연결과 연관되어 생성되므로 이에 해당한다.

오답 포인트

FTP 데이터 연결도 새로 생성된다는 점만 보고 ① NEW를 고르기 쉽다. 그러나 이 문항은 데이터 연결 하나의 시작 여부가 아니라, 그 연결이 기존 제어 연결과 맺는 관계를 묻고 있으므로 RELATED가 핵심이다.

NoteBase

다시 나오면 이렇게 판단

패킷이 새 연결의 시작인지, 해당 연결이 이미 양방향으로 성립했는지, 또는 기존의 다른 연결에서 파생되었는지를 구분한다. 기존 연결과 연관되어 새 연결이 생기는 FTP 데이터 연결 같은 사례는 RELATED로 판단한다.

암기 포인트

FTP 제어 연결과 데이터 연결은 별도이며, 데이터 연결은 제어 연결에 RELATED이다.

NoteBase

11. 다음 중 응용계층 방화벽에 대한 설명으로 가장 적절하지 않은 것은?
① 응용계층에서의 메시지 내용을 기반으로 필터링할 수 있다.
② 내부 시스템이 외부 시스템에 직접적으로 연결되는 것을 방지한다.
③ 내부의 민감정보가 외부로 유출되는 것을 막는 데에 활용한다.
④ 여러 응용 프로토콜에 대해 하나의 응용계층 방화벽으로 보호할 수 있다.

정답 4번

출제 포인트

응용계층 방화벽이 응용계층의 메시지 내용을 검사하고 응용 프로토콜별로 중계·통제한다는 특징을 묻는 문제이다.

핵심 개념

응용계층 방화벽은 내부 사용자와 외부 서버 사이에서 프록시처럼 통신을 중계하며, HTTP·FTP 등 응용 프로토콜의 명령과 메시지 내용을 검사하는 방화벽이다. 패킷의 주소와 포트뿐 아니라 응용 데이터까지 확인할 수 있어 세밀한 필터링이 가능하지만, 응용 프로토콜마다 그 구조와 명령이 다르므로 일반적으로 프로토콜별 처리 기능이 필요하다.

선지별 해설

① O — 응용계층 방화벽은 응용 메시지의 명령, 요청, 콘텐츠 등 메시지 내용을 기준으로 허용 또는 차단할 수 있다.

② O — 프록시가 내부 시스템과 외부 시스템 사이에서 연결을 각각 종단하고 중계하므로 두 시스템이 직접 연결되는 것을 방지한다.

③ O — 응용 데이터의 내용을 검사해 보안 정책에 어긋나는 민감정보의 외부 전송을 탐지·차단하는 데 활용할 수 있다.

④ X — 틀린 표현은 '여러 응용 프로토콜에 대해 하나의 응용계층 방화벽으로 보호할 수 있다'이다. 응용 프로토콜마다 메시지 형식과 명령 체계가 다르므로, 올바르게는 각 응용 프로토콜에 맞는 프록시 또는 검사·중계 기능이 필요하다고 표현해야 한다.

NoteBase

오답 포인트

④의 '하나의 방화벽'이라는 표현이 핵심 함정이다. 한 장비에 여러 프로토콜용 기능을 함께 탑재할 수 있다는 사실과, 하나의 공통 응용계층 처리 기능이 여러 프로토콜을 동일하게 보호한다는 주장은 다르다. 응용계층 방화벽은 프로토콜별 동작을 이해해야 하므로 전용 처리 기능이 필요하다.

다시 나오면 이렇게 판단

메시지 내용 검사, 프록시 중계, 직접 연결 차단은 응용계층 방화벽의 특징으로 판단한다. 반면 서로 다른 응용 프로토콜을 하나의 공통 처리 기능으로 모두 보호한다는 표현은 프로토콜별 구조 차이를 무시한 것이므로 틀린 것으로 판단한다.

암기 포인트

응용계층 방화벽은 '내용까지 검사, 프록시로 중계, 프로토콜별로 처리'한다.

NoteBase

12. 다음 중 네트워크 진단 도구인 traceroute에 대한 설명으로 가장 적절하지 않은 것은?
① 송신지와 목적지 사이에 L3 라우터 상태를 확인하기 위해 사용한다.
② 중계노드 수, IP 주소, 응답시간을 확인할 수 있다.
③ 4개의 UDP 패킷의 TTL을 하나씩 증가시키면서 순차적으로 전송한다.
④ 운영체제에 따라 traceroute는 ICMP, TCP를 선택적으로 사용할 수 있다.

정답 3번

출제 포인트

이 문제는 traceroute가 TTL과 ICMP 응답을 이용해 경로상의 라우터를 확인하는 원리와 일반적인 probe 전송 방식을 묻는 문제이다.

핵심 개념

traceroute는 TTL을 1부터 차례로 늘린 probe 패킷을 보내고, 각 라우터가 반환하는 ICMP Time Exceeded 메시지를 이용해 목적지까지의 경로를 추적하는 도구이다. 전통적인 UDP 기반 traceroute는 일반적으로 각 TTL 값마다 3개의 probe 패킷을 전송한다. 구현과 옵션에 따라 UDP뿐 아니라 ICMP Echo 또는 TCP 방식도 사용할 수 있다.

NoteBase

선지별 해설

① O
송신지와 목적지 사이에서 TTL이 만료될 때 응답하는 L3 라우터를 순서대로 확인하므로, 경로상의 라우터와 응답 여부를 진단하는 데 사용한다.

② O
각 hop의 응답을 통해 중계 노드 수, 응답한 인터페이스의 IP 주소, 각 probe의 왕복 응답시간을 확인할 수 있다.

③ X
틀린 표현은 '4개의 UDP 패킷'이다. 전통적인 UDP 기반 traceroute는 일반적으로 동일한 TTL 값으로 3개의 probe 패킷을 보낸 뒤 TTL을 하나씩 증가시킨다. 올바르게는 '각 TTL 값마다 일반적으로 3개의 UDP probe 패킷을 전송하고, TTL을 1씩 증가시켜 다음 hop을 확인한다'이다.

④ O
운영체제의 구현과 실행 옵션에 따라 ICMP Echo 방식이나 TCP 방식의 probe를 선택할 수 있다. 전통적인 Unix 계열 구현에서는 UDP 방식도 널리 사용한다.

오답 포인트

③은 'TTL을 하나씩 증가시킨다'는 부분은 맞지만 probe의 개수를 4개라고 바꾸어 놓았다. TTL 증가 규칙과 TTL별 기본 probe 수를 분리해서 판단해야 한다.

다시 나오면 이렇게 판단

traceroute 선지는 'TTL을 1부터 증가', '중간 라우터의 ICMP Time Exceeded 응답', 'TTL별 일반적인 probe 3개'의 세 기준으로 판단한다. 패킷 종류는 구현과 옵션에 따라 UDP·ICMP·TCP가 가능하다는 점을 함께 확인한다.

암기 포인트

TTL은 1씩 증가하고, 기본 probe는 hop마다 3개이다.

NoteBase

13. 다음 중 스위칭 환경에서 수행할 수 있는 스니핑 공격에 해당하는 것을 모두 고르면?

㉠ Teardrop Attack
㉡ TCP SYN Flooding Attack
㉢ ARP 스푸핑
㉣ ICMP 리다이렉트
㉤ 스위치 재밍

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

정답 3번

출제 포인트

스위칭 환경에서 트래픽을 공격자 쪽으로 우회시키거나 스위치가 프레임을 여러 포트로 플러딩하게 만들어 스니핑할 수 있는 공격을 구별하는 문제이다.

핵심 개념

ARP 스푸핑은 위조 ARP 정보를 보내 공격자의 MAC 주소를 다른 호스트나 게이트웨이의 주소처럼 믿게 하여 중간자 위치에서 패킷을 가로챌 수 있게 하는 공격이다.
ICMP 리다이렉트는 조작된 경로 변경 정보를 전달하여 피해자의 패킷 경로를 공격자 쪽으로 우회시킬 수 있는 공격이다.
스위치 재밍은 다수의 위조 MAC 주소로 스위치의 MAC 주소 테이블을 넘치게 하여 프레임 플러딩을 유도하고 다른 포트의 트래픽을 엿볼 수 있게 하는 공격이다.
반면 Teardrop Attack과 TCP SYN Flooding Attack은 서비스 거부 공격이며, 스니핑 기법이 아니다.

선지별 해설

① X — ㉠과 ㉡을 스니핑 공격에 포함한 부분이 틀렸다. ㉠ Teardrop Attack은 비정상적으로 겹치는 IP 조각을 이용하는 서비스 거부 공격이고, ㉡ TCP SYN Flooding Attack은 반개방 연결을 누적시키는 서비스 거부 공격이다. 올바른 조합은 ㉢, ㉣, ㉤이다.
② X — ㉡을 포함한 부분이 틀렸다. TCP SYN Flooding Attack은 서버의 연결 자원을 고갈시키는 서비스 거부 공격이므로 제외해야 하며, 올바른 조합은 ㉢, ㉣, ㉤이다.
③ O — ㉢ ARP 스푸핑과 ㉣ ICMP 리다이렉트는 패킷 경로를 공격자 쪽으로 바꿀 수 있고, ㉤ 스위치 재밍은 MAC 주소 테이블의 한계를 이용해 프레임 플러딩을 유도하므로 모두 스위칭 환경의 스니핑에 이용될 수 있다.
④ X — ㉢ ARP 스푸핑을 빠뜨린 부분이 틀렸다. ARP 스푸핑도 공격자를 통신 경로에 끼워 넣어 패킷을 가로채는 데 이용할 수 있으므로, 올바른 조합은 ㉢, ㉣, ㉤이다.

NoteBase

오답 포인트

네트워크 공격이라는 공통점만 보고 ㉠ Teardrop Attack이나 ㉡ TCP SYN Flooding Attack까지 고르면 틀린다. 두 공격의 목적은 서비스 자원 고갈이나 시스템 장애이고, ㉢·㉣·㉤은 트래픽의 경로나 스위치의 전달 방식을 바꾸어 패킷 관찰을 가능하게 한다는 차이가 있다.

다시 나오면 이렇게 판단

각 공격이 단순히 서비스를 마비시키는지, 아니면 트래픽을 공격자에게 우회시키거나 프레임을 다른 포트까지 퍼뜨려 패킷 관찰을 가능하게 하는지를 기준으로 판단한다. 전자는 서비스 거부 공격이고 후자는 스니핑에 이용되는 공격이다.

암기 포인트

스위칭 스니핑은 ARP로 경로 위조, ICMP로 경로 변경, 스위치 재밍으로 프레임 플러딩이다. Teardrop과 SYN Flooding은 서비스 거부 공격이다.

NoteBase

14. 포트 스캔을 통해 얻을 수 있는 정보 중 가장 적절하지 않은 것은?
① 시스템의 논리 주소
② 시스템의 동작 여부
③ 시스템의 제공 서비스
④ 방화벽의 필터링 규칙

정답 1번

출제 포인트

포트 스캔의 대상이 되는 정보와 스캔 응답을 통해 확인하거나 추론할 수 있는 정보를 구별하는 문제이다.

핵심 개념

포트 스캔은 대상 시스템의 논리 주소에 여러 포트 요청을 보내고 응답 상태를 분석하여 포트의 열림·닫힘·필터링 여부를 파악하는 기법이다. 열린 포트에서는 제공 서비스를 추정할 수 있고, 응답 유무와 형태에서는 시스템의 동작 여부 및 방화벽의 필터링 동작을 추론할 수 있다. 반면 대상 시스템의 논리 주소는 일반적으로 스캔을 수행하기 전에 지정하는 입력 정보이다.

선지별 해설

① O — 시스템의 논리 주소는 포트 스캔 요청을 보낼 대상 주소로 먼저 알고 있거나 별도의 호스트 탐색으로 찾아야 한다. 따라서 포트 스캔 결과로 얻는 정보라고 보기 가장 어렵다.

② X — 포트 요청에 대한 응답이 있거나 열린 포트가 확인되면 대상 시스템이 동작 중임을 확인하거나 추정할 수 있다. 틀린 표현은 '얻을 수 없는 정보'로 본 부분이며, 올바르게는 시스템의 동작 여부는 포트 스캔 응답으로 확인·추정할 수 있는 정보이다.

③ X — 열린 포트와 배너 등의 응답을 분석하면 웹, 메일, 원격 접속 등 시스템이 제공하는 서비스를 확인하거나 추정할 수 있다. 틀린 표현은 '얻을 수 없는 정보'로 본 부분이며, 올바르게는 시스템의 제공 서비스는 포트 스캔으로 파악할 수 있는 대표적 정보이다.

④ X — 포트가 filtered로 나타나거나 응답이 차단되는 양상을 분석하면 방화벽이 어떤 트래픽을 허용·차단하는지 추론할 수 있다. 틀린 표현은 '얻을 수 없는 정보'로 본 부분이며, 올바르게는 방화벽의 전체 규칙 원문을 직접 알아내는 것은 아니지만 필터링 동작이나 규칙의 일부를 추론할 수 있다.

NoteBase

오답 포인트

④의 '필터링 규칙'을 방화벽 설정 파일 전체를 직접 획득한다는 뜻으로 넓게 해석하면 혼동하기 쉽다. 이 문항에서는 포트별 응답 상태를 통해 허용·차단 동작을 추론할 수 있다는 의미이다. 반대로 ①의 논리 주소는 스캔 결과가 아니라 스캔 대상을 정할 때 필요한 정보라는 점이 핵심이다.

다시 나오면 이렇게 판단

포트 스캔 문항에서는 먼저 '대상을 지정하기 위한 입력 정보'와 '포트 응답에서 얻는 결과 정보'를 구분한다. IP와 같은 논리 주소는 입력 정보이고, 동작 여부·열린 포트·제공 서비스·필터링 상태는 응답에서 확인하거나 추론하는 결과 정보이다.

암기 포인트

논리 주소는 스캔 대상, 포트 상태·서비스·필터링 동작은 스캔 결과이다.

NoteBase

15. 다음 중 포트 스캐닝 결과에 대한 신뢰도가 가장 낮은 스캐닝 방법으로 옳은 것은?
① TCP ACK scan ② UDP scan
③ ICMP Sweep ④ TCP SYN scan

정답 2번

출제 포인트

TCP·UDP·ICMP 기반 스캔에서 응답이 없을 때 그 원인을 얼마나 명확하게 판별할 수 있는지를 묻는 문제이다.

핵심 개념

TCP 스캔은 SYN/ACK 또는 RST 같은 응답을 이용하므로 상태 판별 기준이 비교적 분명하다.
UDP 스캔은 비연결형 방식이며 열린 포트가 응답하지 않는 경우가 많다. 응답이 없더라도 포트가 열려 있는지, 방화벽에서 차단한 것인지, 패킷이 유실된 것인지 구별하기 어려워 결과의 신뢰도가 가장 낮다.
ICMP Sweep은 포트 상태가 아니라 여러 호스트의 동작 여부를 확인하는 호스트 탐색 방식이다.

선지별 해설

① X
- '신뢰도가 가장 낮다'는 표현이 틀리다. TCP ACK scan은 ACK 패킷에 대한 RST 또는 무응답·ICMP 오류를 바탕으로 주로 방화벽의 필터링 여부를 판단한다. 열린 포트를 직접 식별하는 방식은 아니지만, UDP scan처럼 열린 포트의 무응답 때문에 판별이 특히 불명확한 방식은 아니다. 올바르게는 '필터링 여부와 방화벽 규칙을 파악하는 데 사용하는 스캔'이다.

② O
- UDP scan은 열린 포트가 아무 응답도 보내지 않을 수 있다. 이때 무응답이 열린 포트, 필터링, 패킷 유실 중 무엇 때문인지 구별하기 어려우므로 포트 스캐닝 결과의 신뢰도가 가장 낮다.

③ X
- '포트 스캐닝 결과의 신뢰도가 가장 낮은 방법'이라는 분류가 틀리다. ICMP Sweep은 ICMP Echo 요청 등에 대한 응답으로 활성 호스트를 찾는 방식이며, 개별 TCP·UDP 포트의 개방 여부를 판별하는 포트 스캔이 아니다. 올바르게는 '네트워크에서 동작 중인 호스트를 탐색하는 방식'이다.

④ X
- '신뢰도가 가장 낮다'는 표현이 틀리다. TCP SYN scan은 SYN/ACK이면 열린 포트, RST이면 닫힌 포트로 판단할 수 있어 응답 기준이 비교적 명확하다. 올바르게는 'TCP 응답 플래그를 이용하여 포트 상태를 비교적 신뢰성 있게 판별하는 방식'이다.

NoteBase

오답 포인트

ACK scan이 열린 포트를 직접 확인하지 못한다는 사실만 보고 ①을 고르기 쉽다. 그러나 이 문항의 핵심은 무응답의 의미가 가장 모호한 방식이며, 열린 UDP 포트도 흔히 응답하지 않는다는 점 때문에 ②가 정답이다. 또한 ICMP Sweep은 애초에 호스트 탐색 방식이라는 점을 구분해야 한다.

다시 나오면 이렇게 판단

응답이 없는 경우 그 원인을 구별할 수 있는지를 기준으로 판단한다. TCP는 SYN/ACK·RST 등 명시적 응답이 있지만, UDP는 열린 포트도 무응답일 수 있으므로 'UDP=무응답의 의미가 모호함=낮은 신뢰도'로 연결한다.

암기 포인트

TCP는 플래그로 판별하고, UDP는 무응답이 모호하며, ICMP Sweep은 호스트를 찾는다.

NoteBase

16. 다음 중 무선랜 보안 기술 규격인 WPA-Personal의 PSK 인증에 대한 설명으로 가장 적절하지 않은 것은?
① 인증서버가 설치되지 않은 환경에서 동작 가능
② AP와 단말기의 인증 과정 중 3-way handshake 수행
③ AP와 단말기가 사전에 공유된 키(PSK)와 802.1x에 규정된 EAPoL-Key 프레임을 활용하여 인증 수행
④ 인증 후 공유키로부터 256비트 길이의 임시 암호키(PMK) 생성

정답 2번

출제 포인트

WPA-Personal의 PSK 인증 구조와 AP·단말기 사이에서 수행되는 키 설정 절차의 명칭을 묻는 문제이다.

핵심 개념

WPA-Personal은 별도의 인증 서버 없이 AP와 단말기가 미리 공유한 비밀값인 PSK를 바탕으로 인증과 암호화용 키 설정을 수행하는 방식이다. AP와 단말기는 EAPOL-Key 프레임을 주고받는 4-way handshake를 통해 서로 PMK를 보유하고 있음을 확인하고 실제 통신에 사용할 세션 키를 만든다. PMK는 256비트 길이의 상위 키 자료이며, 실제 데이터 암호화에는 handshake에서 파생된 임시 키가 사용된다.

선지별 해설

① O — WPA-Personal은 인증 서버를 사용하는 Enterprise 방식과 달리 PSK를 이용하므로 별도의 인증 서버가 설치되지 않은 환경에서도 동작할 수 있다.

② X — 틀린 표현은 '3-way handshake'이다. AP와 단말기의 키 확인 및 세션 키 설정 과정은 3-way가 아니라 4-way handshake로 수행된다.

③ O — AP와 단말기는 사전에 공유한 PSK를 기반으로 하며, 인증·키 설정 과정에서 IEEE 802.1X에 규정된 EAPOL-Key 프레임을 주고받는다.

④ O — 공유된 PSK로부터 256비트 길이의 PMK가 마련되며, 이 PMK가 이후 4-way handshake에서 임시 세션 키를 파생하는 기반이 된다.

NoteBase

오답 포인트

②의 '3-way'는 TCP의 연결 설정 절차인 3-way handshake와 혼동하도록 만든 표현이다. WPA-Personal의 키 설정 절차는 4개의 메시지를 주고받는 4-way handshake이다. 또한 EAPOL-Key라는 명칭 때문에 반드시 별도의 EAP 인증 서버가 필요하다고 오해하기 쉽지만, WPA-Personal은 PSK를 사용하므로 인증 서버가 필수는 아니다.

다시 나오면 이렇게 판단

Personal과 Enterprise를 먼저 구분한다. Personal은 PSK·인증 서버 불필요, Enterprise는 802.1X/EAP·인증 서버 사용으로 판단한다. 이어 WPA의 동적 키 설정 절차가 나오면 4-way handshake인지 확인한다.

암기 포인트

WPA-Personal은 PSK, 인증 서버 불필요, EAPOL-Key 기반 4-way handshake로 연결한다.

NoteBase

17. 다음 중 ICMP 패킷의 크기를 기준 크기보다 크게 증가시키고, 더 많은 조각으로 단편화하여 공격 대상에게 전송하는 공격으로 가장 적절한 것은?

① Ping of Death ② SMURF Attack
③ DDoS ④ Teardrop Attack

정답 1번

출제 포인트

비정상적으로 큰 ICMP 패킷을 여러 조각으로 단편화해 전송하는 공격과 다른 서비스 거부 공격을 구별하는 문제이다.

핵심 개념

Ping of Death는 허용 범위를 넘는 크기의 IP 패킷을 주로 ICMP 조각들로 나누어 보내고, 대상이 이를 재조립하는 과정에서 오류나 시스템 장애를 일으키게 하는 공격이다.
SMURF Attack은 출발지 주소를 피해자의 주소로 위조한 ICMP 요청을 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 집중되게 하는 증폭 공격이다.
DDoS는 다수의 감염된 시스템이 동시에 한 대상을 공격하여 서비스 자원을 고갈시키는 분산 서비스 거부 공격이다.
Teardrop Attack은 서로 겹치거나 모순되는 단편화 오프셋을 가진 IP 조각을 보내 재조립 오류를 유발하는 공격이다.

선지별 해설

① O — Ping of Death는 기준을 초과할 정도로 큰 패킷을 여러 ICMP 조각으로 전송하여 재조립 과정에서 장애를 유발하므로 제시된 설명에 해당한다.
② X — 틀린 부분은 큰 ICMP 패킷을 더 많은 조각으로 나누는 공격을 SMURF Attack으로 본 것이다. 올바르게는 SMURF Attack은 피해자의 IP 주소로 출발지를 위조한 ICMP 요청을 브로드캐스트하여 다수의 응답을 피해자에게 집중시키는 공격이다.
③ X — 틀린 부분은 제시된 구체적 공격 방식을 포괄적 범주인 DDoS로 본 것이다. 올바르게는 DDoS는 여러 공격원이 동시에 트래픽이나 요청을 보내 대상의 서비스를 마비시키는 분산 서비스 거부 공격이며, 제시된 방식은 Ping of Death이다.
④ X — 틀린 부분은 패킷 크기 초과와 다수 단편 전송을 Teardrop Attack의 식별 기준으로 본 것이다. 올바르게는 Teardrop Attack은 겹치거나 잘못된 단편화 오프셋을 이용해 IP 조각의 재조립 오류를 유발하는 공격이다.

NoteBase

오답 포인트

①과 ④는 모두 IP 단편의 재조립 과정과 관련되어 혼동하기 쉽다. 그러나 문제의 'ICMP 패킷의 크기를 기준 크기보다 크게 증가'는 Ping of Death의 단서이고, '조각의 오프셋이 겹치거나 비정상적'이라는 단서가 있어야 Teardrop Attack으로 판단한다.

다시 나오면 이렇게 판단

초대형 ICMP 패킷과 단편화가 함께 나오면 Ping of Death, 위조된 출발지와 브로드캐스트 응답 증폭이면 SMURF Attack, 다수 공격원의 동시 공격이면 DDoS, 중첩되거나 비정상적인 단편 오프셋이면 Teardrop Attack으로 구별한다.

암기 포인트

큰 ICMP는 Ping, 방송 증폭은 SMURF, 다수 공격원은 DDoS, 겹친 조각은 Teardrop이다.

NoteBase

18. 공격자가 발신지 주소를 공격 대상의 IP로, 목적지 주소를 직접 브로드캐스트 주소(Directed Broadcast Address)로 설정한 Ping 메시지를 통해 증폭 네트워크(Amplifier network)의 시스템들이 공격 대상에게 Ping 응답 메시지를 동시에 전송하도록 만드는 공격으로 가장 적절한 것은?
① Land Attack
② TCP SYN Flooding Attack
③ SMURF Attack
④ DDoS

정답 3번

출제 포인트

출발지 IP 주소를 피해자의 주소로 위조하고 목적지를 직접 브로드캐스트 주소로 지정한 ICMP Ping을 이용해 다수의 응답을 피해자에게 집중시키는 공격을 식별하는 문제이다.

핵심 개념

SMURF 공격은 피해자의 IP 주소로 출발지를 위조한 ICMP Echo Request를 증폭 네트워크의 브로드캐스트 주소로 보내고, 그 네트워크의 여러 시스템이 ICMP Echo Reply를 피해자에게 동시에 보내게 하는 반사·증폭 공격이다.
Land 공격은 출발지와 목적지의 IP 주소를 동일한 대상 주소로 조작하는 공격이고, TCP SYN Flooding은 다량의 SYN 요청으로 반개방 연결을 누적시키는 공격이다. DDoS는 여러 공격원이 분산되어 대상을 공격하는 넓은 범주의 공격이다.

선지별 해설

① X — Land Attack은 패킷의 출발지 IP 주소와 목적지 IP 주소를 동일한 피해자 주소로 설정해 피해자가 자기 자신에게 응답하도록 만드는 공격이다. 틀린 표현은 직접 브로드캐스트 주소를 이용해 여러 시스템의 Ping 응답을 집중시킨다는 부분이며, 올바르게는 출발지와 목적지를 같은 피해자 주소로 조작하는 공격이다.
② X — TCP SYN Flooding Attack은 다량의 TCP SYN 요청을 보내 서버의 반개방 연결과 자원을 고갈시키는 공격이다. 틀린 표현은 브로드캐스트된 Ping에 대한 응답을 증폭에 이용한다는 부분이며, 올바르게는 TCP 연결 설정 과정의 SYN 요청을 악용하는 공격이다.
③ O — SMURF Attack은 피해자 IP로 출발지를 위조한 ICMP Ping을 직접 브로드캐스트 주소로 전송하여 증폭 네트워크의 여러 시스템이 피해자에게 동시에 응답하게 한다. 제시된 공격 절차와 정확히 일치한다.
④ X — DDoS는 여러 분산된 공격원이 동시에 트래픽을 보내 대상을 마비시키는 일반적인 공격 범주이다. 이 문항의 구체적 단서는 분산 공격원 자체가 아니라 출발지 위조, 직접 브로드캐스트, ICMP 응답 증폭이므로 가장 적절한 명칭은 DDoS가 아니라 SMURF Attack이다.

NoteBase

오답 포인트

④ DDoS도 다수의 시스템이 트래픽을 보낸다는 점에서 비슷해 보이지만, 문항은 공격의 넓은 범주가 아니라 구체적인 기법을 묻는다. '피해자 IP로 출발지 위조 + 브로드캐스트 Ping + 다수의 Echo Reply'라는 조합이 SMURF 공격의 결정적 단서이다.

다시 나오면 이렇게 판단

ICMP Ping, 출발지 주소 위조, 브로드캐스트 주소, 여러 호스트의 응답이 한 피해자에게 집중된다는 단서가 함께 나오면 SMURF 공격으로 판단한다. SYN과 반개방 연결이 핵심이면 TCP SYN Flooding, 출발지와 목적지 주소가 같으면 Land 공격으로 구분한다.

암기 포인트

SMURF = 피해자 주소로 위조한 브로드캐스트 Ping → 여러 응답이 피해자에게 증폭·집중된다.

NoteBase

19. 이더넷에서 사용되는 매체 접근 방식 중 호스트가 채널의 상태를 감지하여 충돌을 회피하는 방식으로 옳은 것은?

① Token Ring ② CSMA/CA
③ CSMA/CD ④ Token Bus

정답 3번

출제 포인트

이더넷의 매체 접근 제어 방식과 토큰 패싱 방식의 차이를 묻는 문제이다.

핵심 개념

CSMA/CD는 공유형 반이중 이더넷에서 전송 전에 반송파를 감지하고, 전송 중 충돌이 발생하면 이를 검출하여 전송을 중단한 뒤 임의 시간 후 재전송하는 방식이다.
CSMA/CA는 충돌을 직접 검출하기 어려운 무선 LAN에서 충돌 가능성을 미리 줄이는 방식이다.
Token Ring과 Token Bus는 토큰을 가진 장치만 전송하도록 하는 토큰 패싱 방식이다.

선지별 해설

① X — Token Ring은 링을 따라 전달되는 토큰을 획득한 장치가 전송하는 방식이다. 틀린 표현은 이더넷에서 채널 상태를 감지하는 방식으로 본 부분이며, 올바르게는 토큰 링 네트워크의 토큰 패싱 방식이다.
② X — CSMA/CA는 충돌을 감지하는 방식이 아니라 전송 전 대기와 확인 절차 등으로 충돌 가능성을 줄이는 방식이며 주로 무선 LAN에서 사용된다. 틀린 표현은 이를 전통적인 공유형 이더넷의 방식으로 본 부분이며, 올바르게는 이더넷은 CSMA/CD를 사용한다.
③ O — CSMA/CD는 전송 전에 채널 사용 여부를 감지하고, 전송 중 충돌이 발생하면 이를 검출하여 재전송을 조정하는 전통적인 공유형 이더넷의 매체 접근 방식이다.
④ X — Token Bus는 버스형 물리 구조에서 논리적 링을 구성하고 토큰을 순서대로 전달하는 방식이다. 틀린 표현은 이를 이더넷의 채널 감지 방식으로 본 부분이며, 올바르게는 토큰을 이용하는 매체 접근 방식이다.

오답 포인트

문장의 '충돌을 회피'만 보면 ② CSMA/CA를 고르기 쉽다. 그러나 이더넷이라는 조건이 결정적이며, 전통적인 공유형 반이중 이더넷은 채널을 감지하고 충돌을 검출하는 CSMA/CD를 사용한다.

다시 나오면 이렇게 판단

이더넷과 충돌 검출이 연결되면 CSMA/CD, 무선 LAN과 충돌 회피가 연결되면 CSMA/CA로 구분한다. 토큰을 가진 장치만 전송한다면 Token Ring 또는 Token Bus 계열로 판단한다.

NoteBase

암기 포인트

유선 이더넷은 CD, 무선 LAN은 CA, 토큰 방식은 순번 전송이다.

NoteBase

20. 다음 IDS의 탐지 유형 중 지식기반 탐지 기법에 해당하지 않는 것은?
① 전문가 시스템(Expert System)
② 시그니처 분석(Signature-based Detection)
③ 페트리넷(Petri-nets)
④ 통계적 분석

정답 4번

출제 포인트

IDS의 지식기반 탐지와 행위기반 탐지를 구분하는 문제이다. 지식기반 탐지에 해당하지 않는 기법을 찾아야 한다.

핵심 개념

지식기반 탐지는 이미 알려진 공격의 규칙·패턴·상태 모델을 지식으로 저장해 두고 현재 활동과 대조하는 방식이다. 전문가 시스템, 시그니처 분석, 페트리넷 등이 이에 해당한다.
행위기반 탐지는 정상적인 사용 행위의 기준을 만들고 그 기준에서 벗어나는 이상 징후를 탐지하는 방식이다. 통계적 분석은 관측값과 정상 행위의 통계적 기준을 비교하므로 행위기반 탐지에 해당한다.

선지별 해설

① X — 전문가 시스템은 전문가의 지식을 규칙 형태로 구성하여 침입 여부를 판단하므로 지식기반 탐지 기법이다. '지식기반 탐지에 해당하지 않는다'가 틀린 판단이며, 올바르게는 '전문가 시스템은 지식기반 탐지 기법이다'이다.
② X — 시그니처 분석은 알려진 공격의 고유 패턴과 현재 활동을 대조하므로 지식기반 탐지 기법이다. '지식기반 탐지에 해당하지 않는다'가 틀린 판단이며, 올바르게는 '시그니처 분석은 지식기반 탐지 기법이다'이다.
③ X — 페트리넷은 시스템의 상태와 상태 전이를 모델링하여 알려진 침입 과정을 표현하고 탐지하는 지식기반 기법이다. '지식기반 탐지에 해당하지 않는다'가 틀린 판단이며, 올바르게는 '페트리넷은 지식기반 탐지 기법이다'이다.
④ O — 통계적 분석은 정상 행위의 통계적 특성을 기준으로 편차나 이상을 찾는 행위기반 탐지 기법이므로 지식기반 탐지에 해당하지 않는다.

오답 포인트

④의 '분석'이라는 표현만 보고 저장된 지식을 분석하는 방식으로 오해하기 쉽다. 구분의 핵심은 분석 여부가 아니라 알려진 공격 지식과 대조하는지, 정상 행위의 통계적 기준에서 벗어났는지를 판단하는지에 있다.

NoteBase

다시 나오면 이렇게 판단

규칙·시그니처·공격 상태 모델처럼 알려진 공격 정보를 기준으로 삼으면 지식기반 탐지로 판단한다. 정상 프로파일·평균·분산·임계값·편차처럼 정상 행위의 통계적 기준을 사용하면 행위기반 탐지로 판단한다.

암기 포인트

알려진 공격 지식은 전문가 시스템·시그니처·페트리넷, 정상 행위의 편차는 통계적 분석이다.

NoteBase

21. 다음 무선랜 보안 기법 중 짧은 길이의 IV 값으로 인해 공격자가 쉽게 암호키를 예측하는 것이 가능한 기법에 해당하는 것은?

① WEP ② WPA-1
③ WPA-2 ④ 802.1x/EAP

정답 1번

출제 포인트

무선랜 보안 방식 가운데 짧은 IV를 사용하여 IV 재사용과 키스트림 분석에 취약한 방식을 구별하는 문제이다.

핵심 개념

WEP는 RC4 기반 암호화에서 24비트 IV와 공유 비밀키를 결합해 패킷별 키를 만드는 초기 무선랜 보안 방식이다. IV 공간이 작아 같은 IV가 반복되기 쉽고, 공격자는 반복된 키스트림과 다수의 패킷을 분석하여 암호화 키를 알아낼 수 있다.
WPA-1은 WEP의 취약점을 보완하기 위해 TKIP의 키 혼합과 더 긴 IV를 사용한다. WPA-2는 주로 AES-CCMP를 사용하는 보안 규격이다. 802.1X/EAP는 사용자·단말 인증과 키 전달을 위한 접근 제어 체계이지, 짧은 IV를 사용하는 암호화 기법이 아니다.

선지별 해설

① O — WEP는 24비트의 짧은 IV를 사용하므로 IV가 재사용되기 쉽다. 공격자는 반복된 IV와 패킷을 수집·분석하여 키스트림을 추론하고 암호화 키를 알아낼 수 있으므로 문제의 설명에 해당한다.
② X — WPA-1은 TKIP를 통해 키 혼합을 강화하고 WEP보다 긴 IV를 사용하므로 '짧은 IV로 암호화 키를 쉽게 예측할 수 있는 기법'이라는 설명에 해당하지 않는다. 틀린 표현 'WPA-1'은 'WEP'로 고쳐야 한다.
③ X — WPA-2는 주로 AES-CCMP를 사용하며, WEP의 짧은 IV 재사용 취약점을 가리키는 기법이 아니다. 틀린 표현 'WPA-2'는 'WEP'로 고쳐야 한다.
④ X — 802.1X/EAP는 네트워크 접속 인증을 수행하는 체계로서 암호화용 IV 길이로 구분되는 암호화 기법이 아니다. 틀린 표현 '802.1X/EAP'는 'WEP'로 고쳐야 한다.

오답 포인트

WEP, WPA-1, WPA-2를 모두 무선랜 보안 규격이라는 이유로 혼동하기 쉽다. 이 문항의 결정적 표현은 '짧은 길이의 IV'이며, 이는 24비트 IV의 재사용 문제가 있는 WEP를 지칭한다. 또한 802.1X/EAP는 암호화 방식이 아니라 인증 체계라는 점을 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

무선랜 보안 문제에서 ‘24비트 IV’, ‘IV 재사용’, ‘RC4 키스트림 분석’이 제시되면 WEP로 판단한다. ‘TKIP’는 WPA-1, ‘AES-CCMP’는 WPA-2, ‘포트 기반 접근 제어·인증’은 802.1X/EAP로 연결한다.

암기 포인트

짧은 24비트 IV와 재사용 취약점은 WEP이다.

NoteBase

22. 다음 중 세션 하이재킹에 대한 설명으로 가장 적절하지 않은 것은?
① 인증 과정을 마치고 생성된 정상 세션의 연결을 가로채는 공격이다.
② 인증 과정에 포함된 절차를 모두 우회하는 것이 가능하다.
③ TCP의 취약점을 이용한 공격이다.
④ TCP로 연결된 송신자와 수신자의 세션을 차단하는 것이 목적이다.

정답 4번

출제 포인트

세션 하이재킹이 이미 인증된 정상 세션의 통신 권한을 탈취하는 공격이라는 점과 단순한 세션 차단 공격의 차이를 묻는 문제이다.

핵심 개념

세션 하이재킹: 공격자가 이미 성립된 정상 세션을 가로채 정당한 사용자처럼 통신하거나 권한을 사용하는 공격이다. 핵심은 세션의 '차단'이 아니라 세션 제어권의 '탈취'이다.
TCP 세션 하이재킹: TCP의 순서 번호 예측, 패킷 위조 등 TCP 통신의 취약점을 이용해 기존 연결에 끼어들어 세션을 장악하는 방식이다.

선지별 해설

① O — 인증을 마친 뒤 생성된 정상 세션의 연결을 공격자가 가로채는 것은 세션 하이재킹의 대표적 특징이다.
② O — 공격자는 이미 인증된 세션을 탈취하므로 최초 인증 과정에 포함된 절차를 다시 거치지 않고도 정당한 사용자처럼 접근할 수 있다.
③ O — TCP 세션 하이재킹은 순서 번호 예측이나 패킷 위조 등 TCP의 구조적 취약점을 이용할 수 있으므로 적절한 설명이다.
④ X — 틀린 표현은 '세션을 차단하는 것이 목적'이라는 부분이다. 올바르게는 TCP로 연결된 송신자와 수신자의 기존 세션에 개입하여 그 세션의 제어권을 탈취하는 것이 목적이다. 단순히 통신을 끊는 것은 서비스 거부 공격의 성격에 가깝다.

오답 포인트

④의 '차단'은 공격 과정에서 정상 사용자의 통신을 방해할 수 있다는 사실과 공격의 본래 목적을 뒤섞은 표현이다. 세션 하이재킹의 핵심 목적은 연결 종료가 아니라 인증이 끝난 세션을 빼앗아 사용하는 데 있다.

NoteBase

다시 나오면 이렇게 판단

세션 하이재킹 선지는 ‘인증 후 성립된 세션’, ‘세션 가로채기’, ‘정상 사용자 위장’, ‘제어권 탈취’를 기준으로 판단한다. 목적을 단순 차단이나 연결 종료라고 설명하면 서비스 거부 공격과 혼동한 것이므로 틀린 선지로 판단한다.

암기 포인트

세션 하이재킹은 세션을 끊는 공격이 아니라 인증된 세션을 빼앗는 공격이다.

NoteBase

23. 다음 중 Land Attack에 대한 대응책으로 가장 적절한 것은?
① egress filtering 적용
② TCP 패킷의 소스 IP가 내부 IP인 외부 패킷 차단
③ SYN 쿠키 기법 적용
④ TCP 패킷의 소스 IP가 외부 IP인 내부 패킷 차단

정답 2번

출제 포인트

LAND 공격의 패킷 위조 방식과 이를 차단하는 인그레스 필터링을 구별하는 문제이다.

핵심 개념

LAND 공격: 공격 대상의 IP 주소를 출발지와 목적지에 동일하게 넣은 위조 패킷을 보내 대상이 자기 자신에게 응답하도록 하여 자원을 소모시키는 서비스 거부 공격이다.
인그레스 필터링: 외부에서 내부로 들어오는 패킷의 출발지 주소가 내부망 주소로 위조되었는지 검사해 차단한다.
이그레스 필터링: 내부에서 외부로 나가는 패킷의 출발지 주소가 정상적인 내부망 주소인지 검사해 출발지 주소 위조를 막는다.

선지별 해설

① X — 이그레스 필터링은 내부망에서 외부로 나가는 패킷을 검사하므로, 외부에서 들어오는 LAND 공격 패킷을 막는 직접적인 대책이 아니다. 틀린 표현은 'egress filtering'이며, 올바르게는 외부 유입 패킷을 검사하는 'ingress filtering'을 적용한다.
② O — 외부에서 유입되었는데 출발지 IP가 내부 IP인 패킷은 내부 주소를 사칭한 위조 패킷이다. 인그레스 필터링으로 이를 차단하면 공격 대상의 내부 IP를 출발지로 위조하는 LAND 공격을 막을 수 있다.
③ X — SYN 쿠키는 TCP 연결 요청 정보를 서버에 저장하지 않고 검증하여 SYN Flood 공격에 대응하는 기법이다. 틀린 표현은 'SYN 쿠키 기법'이며, LAND 공격에는 외부에서 내부 IP를 출발지로 위조한 패킷을 차단하는 인그레스 필터링을 적용한다.
④ X — 외부에서 내부로 들어오는 정상 패킷은 출발지 IP가 외부 IP일 수 있으므로 이를 일괄 차단하면 정상 통신까지 막는다. 틀린 표현은 '소스 IP가 외부 IP인 내부 패킷 차단'이며, 올바르게는 '소스 IP가 내부 IP인 외부 유입 패킷 차단'이다.

NoteBase

오답 포인트

①의 egress와 ingress의 방향을 뒤바꾸거나, ③의 SYN Flood 대응 기법인 SYN 쿠키를 LAND 공격 대책으로 혼동하기 쉽다. 또한 ④처럼 외부 출발지 주소를 정상적인 외부 유입 패킷의 특징으로 보지 못하면 정상 트래픽을 차단하는 선지를 고르게 된다.

다시 나오면 이렇게 판단

외부에서 들어온 패킷이 내부 주소를 출발지로 사용하면 주소 위조로 판단하여 인그레스 필터링으로 차단한다. 내부에서 나가는 패킷의 출발지 주소를 검사하는 것은 이그레스 필터링이다.

암기 포인트

LAND는 출발지와 목적지가 피해자 자신, 외부에서 내부 주소를 사칭하면 인그레스 필터링이다.

NoteBase

24. 다음 중 IPsec의 AH(Authentication Header) 프로토콜과 가장 거리가 먼 것은?
① AH Header
② Next Header
③ Padding
④ SPI(Security Parameter Index)

정답 3번

출제 포인트

IPsec의 AH 헤더에 포함되거나 직접 관련된 요소와 ESP에서 주로 사용하는 요소를 구별하는 문제이다.

핵심 개념

AH(Authentication Header)는 IP 패킷의 무결성과 송신자 인증을 제공하는 IPsec 프로토콜이다. AH 헤더의 주요 필드는 Next Header, Payload Length, Reserved, SPI, Sequence Number, Authentication Data이다. 반면 표준 패킷 형식에서 독립된 Padding 필드는 ESP 트레일러에 포함되어 암호화 블록이나 필드 정렬에 사용된다.

선지별 해설

① X — 'AH Header가 AH 프로토콜과 거리가 멀다'는 판단이 틀리다. AH Header는 AH 프로토콜이 IP 패킷에 추가하는 인증용 헤더 자체이므로 AH와 직접 관련된다.
② X — 'Next Header가 AH와 거리가 멀다'는 판단이 틀리다. Next Header는 AH 다음에 오는 상위 계층 프로토콜 또는 헤더의 종류를 나타내는 AH 헤더 필드이다.
③ O — Padding은 이 문항에서 AH와 가장 거리가 먼 요소이다. 표준 IPsec 패킷 형식에서 독립된 Padding 필드는 AH의 기본 헤더 필드가 아니라 ESP 트레일러의 구성 요소이다.
④ X — 'SPI가 AH와 거리가 멀다'는 판단이 틀리다. SPI(Security Parameter Index)는 수신자가 해당 패킷에 적용할 보안 연관(SA)을 식별하도록 하는 AH 헤더 필드이다.

오답 포인트

③의 Padding을 AH의 Authentication Data 길이 정렬과 혼동하기 쉽다. 문항은 표준 헤더의 독립된 필드를 묻고 있으므로, Padding은 ESP 트레일러의 필드로 구분해야 한다.

다시 나오면 이렇게 판단

Next Header · SPI · Sequence Number · Authentication Data가 보이면 AH의 주요 필드로 판단하고, Padding · Pad Length · Next Header가 묶여 ESP 트레일러로 제시되면 ESP의 구성으로 판단한다.

NoteBase

암기 포인트

AH는 인증 헤더와 SPI, ESP 트레일러는 Padding이다.

NoteBase

25. 다음 중 암호화 통신과 인증을 제공하는 원격 접속 프로토콜로 가장 적절한 것은?

① SSH ② Rlogin

③ SNMP ④ Telnet

정답 1번

출제 포인트

암호화 통신과 사용자 인증을 제공하는 원격 접속 프로토콜을 구별하는 문제이다.

핵심 개념

SSH: 원격 시스템에 안전하게 접속하기 위한 프로토콜로, 통신 내용을 암호화하고 서버 및 사용자 인증 기능을 제공한다. 키워드는 암호화·인증·안전한 원격 접속이다.
Rlogin·Telnet: 원격 로그인 또는 터미널 접속에 쓰이지만 기본적으로 통신 내용을 평문으로 전송하므로 보안성이 낮다.
SNMP: 네트워크 장비의 상태를 조회하고 설정을 관리하기 위한 네트워크 관리 프로토콜이다. 일반적인 원격 터미널 접속 프로토콜이 아니다.

선지별 해설

① O — SSH는 원격 접속 과정에서 통신 내용을 암호화하고 인증을 제공하므로 문제의 조건에 가장 적절하다.
② X — Rlogin은 원격 로그인 프로토콜이지만 기본적으로 암호화되지 않은 평문 통신을 사용한다. 틀린 부분은 암호화 통신과 인증을 제공하는 프로토콜로 본 점이며, 올바르게는 보안 원격 접속에는 SSH를 사용한다.
③ X — SNMP는 네트워크 장비를 감시·관리하는 프로토콜이다. 틀린 부분은 SNMP를 원격 접속 프로토콜로 본 점이며, 올바르게는 암호화된 원격 접속에는 SSH가 적절하다.
④ X — Telnet은 원격 터미널 접속에 사용되지만 사용자 정보와 통신 내용이 기본적으로 평문으로 전송된다. 틀린 부분은 암호화 통신을 제공한다고 본 점이며, 올바르게는 암호화와 인증이 필요한 원격 접속에는 SSH를 사용한다.

오답 포인트

Rlogin과 Telnet도 원격 접속에 사용된다는 점 때문에 혼동하기 쉽다. 그러나 문제의 결정적 표현은 '암호화 통신과 인증'이며, 이 조건을 함께 충족하는 대표적인 원격 접속 프로토콜은 SSH이다. SNMP는 원격 로그인용이 아니라 장비 관리용이라는 점도 구분한다.

다시 나오면 이렇게 판단

원격 접속 선지에서는 먼저 용도를 확인한 뒤 통신 암호화 여부를 판단한다. 안전한 원격 로그인은 SSH, 평문 기반 원격 접속은 Telnet·Rlogin, 네트워크 장비 관리는 SNMP로 구분한다.

NoteBase

암기 포인트

SSH는 암호화 원격 접속, Telnet·Rlogin은 평문 원격 접속, SNMP는 네트워크 관리이다.

NoteBase