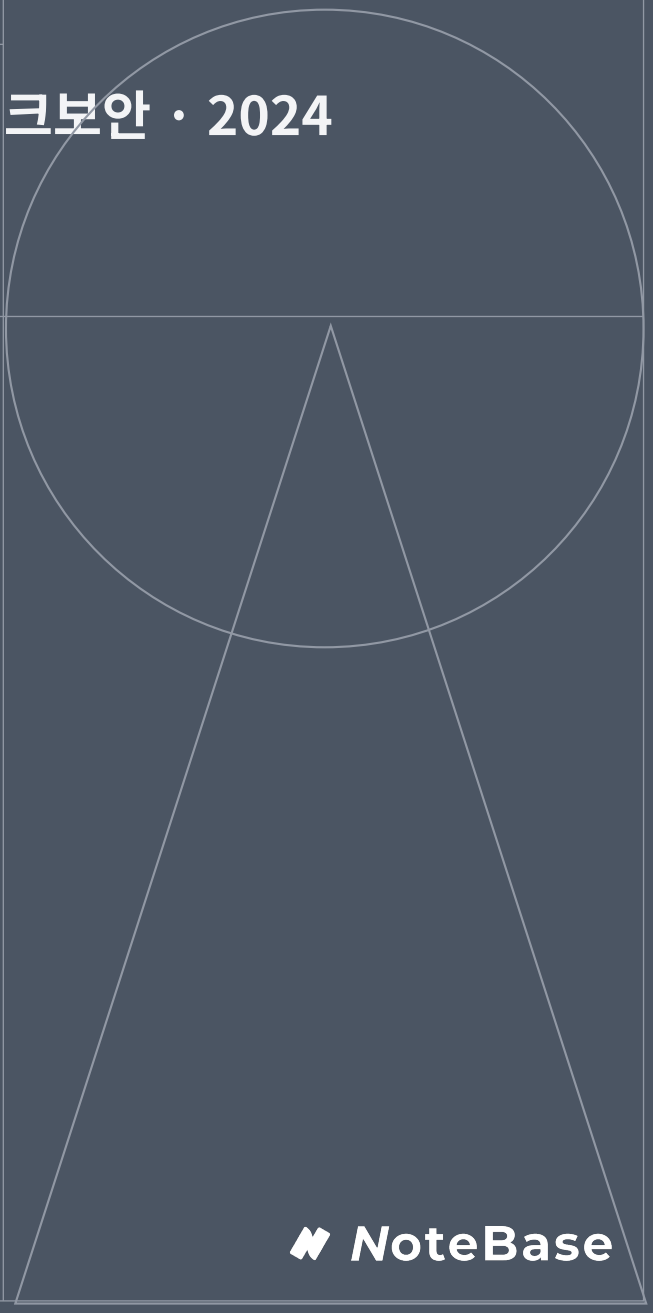
기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2024



NoteBase

기출OX 해설집

공무원/군무원/9급 · 네트워크보안 · 2024

공무원/군무원/9급 · 네트워크보안 · 2024

1. DDoS 공격의 형태로는 대역폭 공격, 자원 소진 공격, 웹/DB 부하 공격 등의 형태가 있다. 다음 중 네트워크 대역폭을 대상으로 하는 DDoS 공격의 특징으로 가장 적절한 것은?
   ① 대상 서버에 과부하 발생
   ② 높은 connection
   ③ 높은 pps(packet per second)
   ④ 높은 bps(bit per second)

정답 4번

출제 포인트

이 문제는 DDoS 공격을 어떤 자원의 처리 한계를 소진시키는지에 따라 구분하고, 네트워크 대역폭 공격의 대표 지표를 찾는 문제이다.

핵심 개념

대역폭 공격: 대량의 트래픽을 보내 회선의 전송 용량을 소진하는 공격이다. 핵심 지표는 초당 전송 비트 수인 *bps*이다.
자원 소진 공격: 연결 상태, 세션, 메모리, CPU 같은 시스템 자원을 고갈시키는 공격이다. 높은 connection 수가 대표적인 단서이다.
패킷 처리량 공격: 아주 많은 패킷을 보내 라우터·방화벽·서버 등의 패킷 처리 능력을 압박하는 공격이다. 핵심 지표는 초당 패킷 수인 *pps*이다.
웹/DB 부하 공격: 정상 요청처럼 보이는 다수의 응용 계층 요청으로 웹 서버나 DB의 처리 부하를 높이는 공격이다.

NoteBase

선지별 해설

① X — '대상 서버에 과부하 발생'은 서버의 CPU·메모리나 웹/DB 처리 자원을 소진시키는 공격의 설명에 가깝다. 대역폭 공격은 올바르게는 대상 측으로 향하는 회선의 전송 용량에 과부하를 일으킨다고 표현한다.
② X — '높은 connection'은 다수의 연결 또는 연결 상태를 유지시켜 세션·메모리 등의 자원을 고갈시키는 자원 소진 공격의 단서이다. 대역폭 공격의 대표 지표는 올바르게는 높은 *bps*이다.
③ X — '높은 *pps*'는 작은 패킷을 매우 많이 보내 네트워크 장비나 서버의 패킷 처리 한계를 압박하는 공격의 단서이다. 대역폭 소진 여부를 직접 나타내는 지표는 올바르게는 높은 *bps*이다.
④ O — 높은 *bps*는 초당 전송되는 비트량이 크다는 뜻이므로, 대량 트래픽으로 네트워크 회선 용량을 소진시키는 대역폭 DDoS 공격의 가장 직접적인 특징이다.

오답 포인트

대역폭 공격도 결과적으로 서비스 장애나 서버 접근 불능을 일으키므로 ①처럼 보일 수 있다. 그러나 문항은 결과가 아니라 공격이 직접 소진시키는 자원과 측정 지표를 묻는다. 또한 *pps*는 패킷 개수, *bps*는 전송 비트량이므로 서로 구분해야 한다.

다시 나오면 이렇게 판단

공격 유형별 병목 자원을 먼저 찾는다. 회선 용량은 *bps*, 패킷 처리 능력은 *pps*, 연결·세션 자원은 connection, 응용 프로그램 처리는 웹/DB 요청 부하로 판단한다.

암기 포인트

대역폭은 *bps*, 패킷 폭주는 *pps*, 상태 자원 소진은 connection으로 기억한다.

NoteBase

2. 다음에서 설명하는 네트워크 보안 솔루션은?

> - 네트워크에 접근하는 접속 단말의 보안성을 강제화할 수 있는 보안 인프라
> - 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC나 노트북, 모바일 단말기 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 시스템 전체를 보호하는 솔루션

① IPS(Intrusion Prevention System)
② SIEM(Security Information & Event Management)
③ NAC(Network Access Control)
④ SSL(Secure Sockets Layer)

정답 3번

출제 포인트

접속 단말의 신원과 보안 상태를 점검하여 네트워크 접속을 허용·차단하는 NAC의 기능을 묻는 문제이다.

핵심 개념

NAC(Network Access Control)는 사용자·단말의 신원과 보안 정책 준수 여부를 확인한 뒤 네트워크 접속을 허용, 제한 또는 격리하는 보안 솔루션이다. 허가되지 않았거나 악성코드에 감염된 단말의 접속을 원천적으로 통제한다.
IPS는 침입·공격 트래픽의 탐지와 차단, SIEM은 보안 로그와 이벤트의 통합 수집·분석, SSL은 통신 구간의 암호화와 인증이 핵심이다.

NoteBase

선지별 해설

① X
IPS는 네트워크를 통과하는 공격 패턴이나 이상 트래픽을 탐지하여 차단하는 침입방지시스템이다. 틀린 표현은 'IPS'이며, 제시문의 접속 단말 보안 상태 점검과 접속 통제 기능에 해당하는 올바른 용어는 NAC이다.

② X
SIEM은 여러 보안 장비와 시스템의 로그·이벤트를 통합 수집하고 상관분석하여 위협을 탐지·관리하는 솔루션이다. 틀린 표현은 'SIEM'이며, 감염·미허가 단말의 네트워크 접속을 차단하는 올바른 용어는 NAC이다.

③ O
NAC는 네트워크에 접속하려는 단말의 사용자·기기 정보와 보안 상태를 검사하고, 정책을 충족하지 못한 단말의 접속을 차단하거나 격리한다. 제시문의 두 특징에 모두 부합한다.

④ X
SSL은 통신 당사자 인증, 데이터 암호화, 무결성 보호를 제공하는 보안 프로토콜이다. 틀린 표현은 'SSL'이며, 단말의 보안 상태를 기준으로 네트워크 접속 자체를 허용·차단하는 올바른 용어는 NAC이다.

오답 포인트

'차단'이라는 말만 보고 공격 트래픽을 차단하는 IPS를 고르기 쉽다. 그러나 제시문의 판단 대상은 패킷이나 공격 행위가 아니라 네트워크에 접속하려는 단말이며, 감염 여부와 보안 정책 준수 상태에 따라 접속 자체를 통제한다는 점이 핵심이다.

다시 나오면 이렇게 판단

단말의 보안 상태를 검사하고 접속을 허용·차단·격리하면 NAC, 공격 트래픽을 탐지·차단하면 IPS, 로그와 이벤트를 통합 분석하면 SIEM, 통신 내용을 암호화하면 SSL로 판단한다.

암기 포인트

NAC는 단말의 네트워크 입장 통제, IPS는 공격 통제, SIEM은 로그 통합 분석, SSL은 통신 암호화이다.

NoteBase

3. 다음은 어떤 공격에 대한 대응방안인가?

- 비동기화 상태 탐지 - ACK Storm 탐지 - SSH와 같이 암호화된 연결 사용

① ARP 스푸핑
② TCP 세션 하이재킹
③ DRDoS 공격
④ SYN Flooding 공격

정답 2번

출제 포인트

TCP 세션 하이재킹의 징후와 대응방안을 다른 네트워크 공격의 방어기법과 구별하는 문제이다.

핵심 개념

TCP 세션 하이재킹은 공격자가 이미 성립된 TCP 연결의 순서번호 등 세션 정보를 악용하여 통신을 가로채거나 정상 통신자로 위장하는 공격이다. 공격 개입으로 양 끝의 순서번호가 어긋나는 비동기화 상태나 ACK 패킷이 반복되는 ACK Storm이 나타날 수 있으므로 이를 탐지하고, SSH처럼 내용을 암호화하는 연결을 사용하여 세션 탈취의 실효성을 낮춘다.

선지별 해설

① X — 틀린 표현은 'ARP 스푸핑'이다. ARP 스푸핑은 위조 ARP 메시지로 IP 주소와 공격자의 MAC 주소를 잘못 대응시키는 공격이며, 정적 ARP 등록이나 동적 ARP 검사 등으로 대응한다. 제시된 대응방안의 공격명은 올바르게는 'TCP 세션 하이재킹'이다.
② O — TCP 세션 하이재킹은 기존 TCP 연결에 공격자가 끼어드는 공격이므로, 세션 비동기화와 ACK Storm을 탐지하고 SSH 같은 암호화 연결을 사용하는 것이 대응방안에 해당한다.
③ X — 틀린 표현은 'DRDoS 공격'이다. DRDoS는 위조된 출발지 주소를 이용해 여러 반사 서버의 대량 응답을 피해자에게 보내는 공격이며, 출발지 주소 검증, 반사 서버의 요청 제한, 비정상 트래픽 차단 등으로 대응한다. 제시된 대응방안의 공격명은 올바르게는 'TCP 세션 하이재킹'이다.
④ X — 틀린 표현은 'SYN Flooding 공격'이다. SYN Flooding은 TCP 연결 설정의 반개방 상태를 대량으로 만들어 서버 자원을 고갈시키는 공격이며, SYN Cookie, 연결 대기 큐 조정, 타임아웃 단축, 요청률 제한 등으로 대응한다. 제시된 대응방안의 공격명은 올바르게는 'TCP 세션 하이재킹'이다.

NoteBase

오답 포인트

ACK가 보인다는 이유로 ④ SYN Flooding을 고르기 쉽지만, SYN Flooding의 핵심 징후는 연결 설정 단계의 SYN 요청과 반개방 연결 누적이다. 비동기화와 ACK Storm은 이미 성립된 TCP 세션에 공격자가 개입하는 세션 하이재킹의 단서이다.

다시 나오면 이렇게 판단

‘기존 세션’, ‘순서번호 불일치·비동기화’, ‘ACK Storm’, ‘암호화 연결’이 함께 제시되면 TCP 세션 하이재킹으로 판단한다. ‘ARP 정보 위조’는 ARP 스푸핑, ‘반사 서버의 대량 응답’은 DRDoS, ‘반개방 연결 누적’은 SYN Flooding으로 구별한다.

암기 포인트

세션 하이재킹은 비동기화·ACK Storm을 탐지하고 SSH로 통신을 암호화한다.

NoteBase

4. 다음 중 내부에 서버가 존재할 경우에 설정하여 사용하는 NAT는?
① Normal NAT
② Reverse NAT
③ Redirect NAT
④ Exclude NAT

정답 2번

출제 포인트

내부 서버를 외부에서 접근할 수 있게 할 때 사용하는 NAT 유형을 구별하는 문제이다.

핵심 개념

Normal NAT: 내부 호스트가 외부로 통신할 때 내부 주소를 외부 주소로 변환하는 방식이다.
Reverse NAT: 외부에서 공인 주소로 들어온 접속을 내부 서버의 사설 주소로 변환하여 전달하는 방식이다.
Redirect NAT: 특정 목적지로 향하는 트래픽을 방화벽 자신이나 별도의 지정 지점으로 돌리는 방식이다.
Exclude NAT: 지정한 트래픽을 주소 변환 대상에서 제외하는 방식이다.
내부 서버를 외부에 제공한다는 조건에서는 외부에서 내부로 들어오는 연결의 목적지 주소를 변환해야 하므로 Reverse NAT를 사용한다.

선지별 해설

① X — Normal NAT는 주로 내부 호스트가 외부로 나갈 때 출발지 주소를 변환하는 방식이므로 내부 서버에 대한 외부 접속 설정과 맞지 않는다. 틀린 표현은 ‘Normal NAT’이며, 올바르게는 ‘Reverse NAT’이다.
② O — Reverse NAT는 외부에서 공인 주소로 들어온 요청의 목적지 주소를 내부 서버 주소로 변환하여 내부 서버에 전달하므로 문제의 조건에 맞는다.
③ X — Redirect NAT는 트래픽을 방화벽 자신이나 지정한 다른 처리 지점으로 돌릴 때 사용하므로 내부 서버의 외부 공개를 뜻하는 유형이 아니다. 틀린 표현은 ‘Redirect NAT’이며, 올바르게는 ‘Reverse NAT’이다.
④ X — Exclude NAT는 특정 트래픽에 NAT를 적용하지 않도록 제외하는 방식이므로 외부 요청을 내부 서버 주소로 변환하지 않는다. 틀린 표현은 ‘Exclude NAT’이며, 올바르게는 ‘Reverse NAT’이다.

오답 포인트

‘내부에 있는 장비’라는 말만 보고 내부에서 외부로 나가는 Normal NAT를 고르기 쉽다. 그러나 이 문항의 핵심은 장비의 위치가 아니라 외부 사용자의 접속이 내부 서버로 들어오는 통신 방향이다.

NoteBase

다시 나오면 이렇게 판단

내부 사용자가 외부로 나가면 Normal NAT, 외부 사용자가 내부 서버로 들어오면 Reverse NAT로 판단한다. NAT를 적용하지 않는 예외는 Exclude NAT, 트래픽의 처리 지점을 돌리는 것은 Redirect NAT이다.

암기 포인트

밖으로 나가면 Normal, 밖에서 내부 서버로 들어오면 Reverse이다.

NoteBase

5. 다음과 같은 특징을 갖는 네트워크 공격 기법으로 가장 적절한 것은?

> - 주로 CGI를 기반으로 하는 웹서버(apache 등) 대상의 공격을 수행
> - 리눅스 계열 OS에서 주로 사용하는 GNU Bash에서 공격자가 원격으로 악의적인 시스템 명령을 실행

① 쉘 쇼크
② 워터링 홀
③ 하트 블리드
④ DNS 포이즈닝

정답 1번

출제 포인트

CGI 기반 웹서버와 GNU Bash를 매개로 공격자가 원격에서 악의적인 명령을 실행하는 취약점이 셸쇼크임을 식별하는 문제이다.

핵심 개념

셸쇼크는 GNU Bash가 환경변수에 덧붙은 명령을 잘못 처리하여 임의 명령 실행을 허용하는 취약점이다. 웹서버가 CGI를 통해 요청 정보를 환경변수로 Bash에 전달할 때 원격 공격에 악용될 수 있다.
워터링 홀은 공격 대상자가 자주 방문하는 웹사이트를 미리 침해하여 감염시키는 공격이다. 하트블리드는 OpenSSL의 Heartbeat 처리 오류로 서버나 클라이언트의 메모리 정보가 노출되는 취약점이다. DNS 포이즈닝은 DNS 정보나 캐시를 변조하여 사용자를 공격자가 의도한 주소로 유도하는 공격이다.

선지별 해설

① O — 셸쇼크는 GNU Bash의 명령 처리 취약점이며, CGI 기반 웹서버를 통해 전달된 값으로 원격 명령이 실행될 수 있다는 제시문의 특징과 일치한다.
② X — 틀린 부분은 '워터링 홀'이다. 워터링 홀은 공격 대상 집단이 자주 방문하는 웹사이트를 감염시켜 악성코드를 유포하는 공격이며, 제시문의 공격은 셸쇼크이다.
③ X — 틀린 부분은 '하트블리드'이다. 하트블리드는 OpenSSL의 Heartbeat 확장 기능에서 경계 검사가 제대로 이루어지지 않아 메모리 내용이 노출되는 취약점이며, 제시문의 공격은 셸쇼크이다.
④ X — 틀린 부분은 'DNS 포이즈닝'이다. DNS 포이즈닝은 DNS 응답이나 캐시 정보를 변조하여 도메인 이름이 잘못된 IP 주소로 연결되게 하는 공격이며, 제시문의 공격은 셸쇼크이다.

NoteBase

오답 포인트

웹서비스를 매개로 한다는 공통점만 보고 워터링 홀이나 DNS 포이즈닝을 고르기 쉽다. 그러나 제시문의 결정적 표현은 ‘CGI’, ‘GNU Bash’, ‘원격 명령 실행’이며, 이 세 단서는 셸쇼크를 가리킨다.

다시 나오면 이렇게 판단

공격 대상과 결과를 함께 확인한다. Bash·환경변수·CGI·원격 명령 실행이면 셸쇼크, OpenSSL·Heartbeat·메모리 노출이면 하트블리드, 자주 방문하는 사이트의 선제 감염이면 워터링 홀, DNS 주소 정보 변조이면 DNS 포이즈닝으로 판단한다.

암기 포인트

Bash에 명령이 덧붙으면 셸쇼크, Heartbeat에서 메모리가 새면 하트블리드이다.

NoteBase

6. traceroute는 패킷이 목적지까지 도달하는 동안 거쳐가는 라우터의 IP를 확인하는 도구이다. traceroute를 실행하여 패킷이 목적지 시스템에 도달하였을 때 출발지에서 확인할 수 있는 정보는?
① ICMP Echo Reply
② ICMP Time Exceeded
③ ICMP Port Unreachable
④ ICMP Information Reply

정답 3번

출제 포인트

일반적인 UDP 기반 traceroute에서 중간 라우터를 확인할 때의 ICMP 응답과 패킷이 목적지에 도달했을 때의 ICMP 응답을 구분하는 문제이다.

핵심 개념

traceroute는 TTL을 1부터 차례로 증가시킨 탐사 패킷을 보내 경로상의 라우터를 확인하는 도구이다.
중간 라우터에서는 TTL이 0이 되므로 ICMP Time Exceeded가 돌아오고, 일반적인 UDP 기반 traceroute의 패킷이 목적지의 사용하지 않는 UDP 포트에 도달하면 ICMP Port Unreachable이 돌아온다. 이 응답으로 출발지는 목적지 도달을 확인한다.

선지별 해설

① X — ICMP Echo Reply는 ICMP Echo Request에 대한 응답으로, ping이나 ICMP 탐사 방식에서 사용된다. 틀린 표현은 'ICMP Echo Reply'이며, 일반적인 UDP 기반 traceroute가 목적지에 도달했을 때의 응답은 'ICMP Port Unreachable'이다.
② X — ICMP Time Exceeded는 탐사 패킷의 TTL이 중간 라우터에서 만료되었음을 나타내며, 각 홉의 라우터를 확인하는 데 사용된다. 틀린 표현은 목적지 도달 시 'ICMP Time Exceeded'를 확인한다는 것이며, 올바르게는 목적지에서 'ICMP Port Unreachable'을 확인한다.
③ O — 일반적인 traceroute는 목적지의 사용하지 않는 UDP 포트로 탐사 패킷을 보낸다. 패킷이 목적지에 도달하면 해당 포트에서 수신할 프로세스가 없으므로 목적지가 ICMP Port Unreachable을 보내고, 출발지는 이를 통해 추적이 완료되었음을 안다.
④ X — ICMP Information Reply는 ICMP Information Request에 대한 응답이며 traceroute의 목적지 도달 확인에 사용되지 않는다. 틀린 표현은 'ICMP Information Reply'이며, 올바른 응답은 'ICMP Port Unreachable'이다.

NoteBase

오답 포인트

②의 ICMP Time Exceeded는 traceroute에서 자주 보이지만 목적지 도달 신호가 아니라 중간 홉의 TTL 만료 신호이다. 문제의 '목적지 시스템에 도달하였을 때'라는 조건에서는 ③의 ICMP Port Unreachable을 선택해야 한다.

다시 나오면 이렇게 판단

UDP 기반 traceroute에서는 '중간 라우터 + TTL 만료'이면 ICMP Time Exceeded, '목적지 + 닫힌 UDP 포트 도달'이면 ICMP Port Unreachable로 판단한다.

암기 포인트

중간 홉은 Time Exceeded, 최종 목적지는 Port Unreachable이다.

NoteBase

7. 다음 중 FIN, NULL, XMAS 스캔의 공통점으로 가장 적절한 것은?
   ① TCP의 플래그 중 일부만 설정하여 패킷을 전송한다.
   ② 정상적인 3-Way Handshaking을 통한 세션이 수립되지 않으므로 시스템에 로그가 남지 않는다.
   ③ UDP 프로토콜을 이용하면 동일한 정보를 수신하여 닫힌 포트를 확인할 수 있다.
   ④ 포트가 열려있는 경우 ACK 패킷을 수신함으로써 열려있는 포트를 확인하는 방식으로 스캔을 수행한다.

정답 2번

출제 포인트

FIN, NULL, XMAS 스캔이 TCP 플래그를 비정상적으로 조합하여 정상적인 3-Way Handshaking 없이 포트 상태를 탐지한다는 공통점을 묻는 문제이다.

핵심 개념

FIN 스캔은 FIN 플래그만 설정하고, NULL 스캔은 모든 TCP 플래그를 0으로 두며, XMAS 스캔은 FIN·PSH·URG 플래그를 설정한다. 세 방식 모두 SYN을 이용한 정상 연결 절차를 완료하지 않는 스텔스 스캔이다. 일반적인 TCP 동작에서는 닫힌 포트가 RST로 응답하고 열린 포트는 응답하지 않는 차이를 이용한다.

NoteBase

선지별 해설

① X
틀린 표현은 ‘TCP의 플래그 중 일부만 설정’이 세 스캔 모두의 공통점이라는 부분이다. FIN과 XMAS 스캔은 특정 플래그를 설정하지만 NULL 스캔은 모든 TCP 플래그를 0으로 설정한다. 올바르게는 ‘세 방식은 서로 다른 비정상적 TCP 플래그 조합을 사용한다’이다.

② O
세 방식 모두 정상적인 3-Way Handshaking으로 TCP 세션을 수립하지 않으므로 정상 연결 세션을 기준으로 하는 시스템·서비스 로그를 회피하려는 스텔스 스캔에 해당한다. 따라서 세 방식의 공통점으로 가장 적절하다.

③ X
틀린 표현은 ‘UDP 프로토콜을 이용’한다는 부분이다. FIN, NULL, XMAS 스캔은 모두 TCP 플래그를 이용하는 TCP 스캔이다. 올바르게는 ‘일반적으로 닫힌 TCP 포트의 RST 응답과 열린 포트의 무응답을 구분하여 포트 상태를 판단한다’이다.

④ X
틀린 표현은 ‘포트가 열려 있는 경우 ACK 패킷을 수신’한다는 부분이다. 일반적인 FIN·NULL·XMAS 스캔에서는 열린 포트가 응답하지 않고 닫힌 포트가 RST 패킷을 보낸다. 올바르게는 ‘무응답이면 열린 포트 또는 필터링된 포트로, RST 응답이면 닫힌 포트로 판단한다’이다.

오답 포인트

①은 FIN과 XMAS의 특징만 보면 그럴듯하지만, NULL은 설정된 플래그가 하나도 없다는 점에서 공통점이 아니다. 또한 ACK 응답 여부로 열린 포트를 찾는 방식과 FIN·NULL·XMAS 스캔의 RST·무응답 판별 방식을 혼동하기 쉽다.

다시 나오면 이렇게 판단

먼저 SYN-SYN/ACK-ACK의 정상 연결을 만드는지 확인한다. FIN·NULL·XMAS는 정상 세션을 만들지 않으며, 개별 플래그 조합은 서로 다르지만 닫힌 포트의 RST와 열린 포트의 무응답을 이용한다는 공통 기준으로 판단한다.

암기 포인트

FIN은 FIN만, NULL은 플래그 0개, XMAS는 FIN·PSH·URG이며, 셋 모두 정상 핸드셰이크 없이 RST와 무응답을 본다.

NoteBase

8. DSniff는 한국계 미국인 송덕준 교수가 개발한 패키지이다. DSniff의 도구 중 하나인 macof를 이용하면 스위치의 MAC 테이블에서 오버플로우를 발생시킬 수 있다. 이 현상을 이용하여 수행할 수 있는 공격에 대한 설명으로 가장 적절한 것은?
   ① 스위치에서 임의의 코드를 수행하여 다양한 네트워크 공격을 수행할 수 있다.
   ② Fail safe가 적용되어 네트워크 패킷을 모두 차단함으로써 네트워크 통신을 마비시키는 서비스 거부 공격이 가능하다.
   ③ MAC 주소와 IP 주소를 정적으로 연결하는 static 설정이 불가능하여 arp 스푸핑이 가능하다.
   ④ 스위치가 허브처럼 동작하여 모든 패킷을 모든 포트에 전송하게 되므로 스니핑이 가능하다.

정답 4번

출제 포인트

macof가 다수의 위조 출발지 MAC 주소로 스위치의 MAC 테이블을 가득 채운 뒤 프레임 플러딩을 유발하는 원리를 묻는 문제이다.

핵심 개념

MAC 테이블 오버플로우: 스위치의 MAC 주소 학습 테이블을 대량의 위조 항목으로 채워 정상적인 포트 식별을 어렵게 만드는 공격이다.
스위치는 목적지 MAC 주소에 대응하는 포트를 알 수 없는 프레임을 여러 포트로 플러딩한다. 공격자는 이 허브와 비슷한 전달 상태를 이용해 원래 자신의 포트로 오지 않을 트래픽을 스니핑할 수 있다.

NoteBase

선지별 해설

① X
틀린 표현은 '스위치에서 임의의 코드를 수행'한다는 부분이다. macof는 스위치에서 코드를 실행하는 도구가 아니라, 위조한 출발지 MAC 주소를 포함한 프레임을 대량 전송하여 MAC 테이블 오버플로우를 유발하는 도구이다.

② X
틀린 표현은 'Fail safe가 적용되어 네트워크 패킷을 모두 차단'한다는 부분이다. 이 공격의 핵심은 패킷 전면 차단이 아니라, 테이블이 넘친 스위치가 목적지 포트를 특정하지 못하는 프레임을 여러 포트로 플러딩하는 현상이다. 따라서 설명의 주된 결과는 서비스 거부가 아니라 트래픽 스니핑 가능성의 증가이다.

③ X
틀린 표현은 'MAC 주소와 IP 주소를 정적으로 연결하는 설정이 불가능하여 ARP 스푸핑이 가능'하다는 부분이다. 정적 MAC 항목, 포트 보안, 정적 ARP 항목 등은 설정할 수 있으며, macof가 직접 노리는 대상은 ARP 캐시가 아니라 스위치의 MAC 테이블이다. 올바르게는 macof가 다수의 위조 MAC 주소를 학습시켜 MAC 테이블 오버플로우를 일으킨다고 해야 한다.

④ O
MAC 테이블이 오버플로우되어 정상적인 목적지 포트 식별이 어려워지면 스위치는 해당 프레임을 여러 포트로 플러딩하여 허브와 비슷하게 동작할 수 있다. 공격자는 자신의 포트로 복제되어 들어오는 다른 호스트의 프레임을 수집함으로써 스니핑을 시도할 수 있다.

오답 포인트

②의 '모두 차단'과 ④의 '모든 포트로 전송'을 혼동하기 쉽다. macof의 핵심 결과는 스위치 내부 코드 실행이나 ARP 캐시 변조가 아니라, MAC 테이블 학습 기능을 교란하여 플러딩을 유발하는 것이다.

다시 나오면 이렇게 판단

도구가 대량의 위조 MAC 주소를 생성한다는 단서가 보이면 'MAC 테이블 고갈 → 목적지 포트 식별 실패 → 프레임 플러딩 → 스니핑 가능'의 흐름으로 판단한다. ARP 캐시의 IP-MAC 대응 관계를 거짓으로 바꾸는 ARP 스푸핑과 구별한다.

암기 포인트

macof는 MAC 테이블을 넘치게 하고, 넘친 스위치는 허브처럼 플러딩한다.

NoteBase

9. TLS는 취약한 SSL을 보강하여 암호화 통신을 지원한다. 이때 협상된 보안 파라미터를 이용하여 암·복호화 및 무결성 검증 등을 수행하는 과정을 Record라 한다. 다음 중 발신측에서 수행하는 Record 프로토콜의 절차를 올바른 순서로 나열한 것은?

㉠단편화	㉡암호화	㉢MAC 적용
㉣Record 헤더 추가		㉤압축

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

정답 2번

출제 포인트

이 문제는 TLS Record 프로토콜이 송신할 데이터를 일정 크기로 나눈 뒤 압축·무결성 보호·기밀성 보호를 거쳐 레코드로 만드는 순서를 묻는 문제이다.

올바른 순서

ㄱ 단편화 → ㅁ 압축 → ㄷ MAC 적용 → ㄴ 암호화 → ㄹ Record 헤더 추가

1. 단편화 — 상위 계층의 데이터를 처리 가능한 블록으로 나눈다.
2. 압축 — 단편화된 블록을 협상된 방식에 따라 압축한다.
3. MAC 적용 — 압축된 데이터에 MAC을 덧붙여 무결성과 인증을 검증할 수 있게 한다.
4. 암호화 — 데이터와 MAC을 함께 암호화하여 기밀성을 보호한다.
5. Record 헤더 추가 — 암호화된 결과 앞에 Record 헤더를 붙여 전송할 레코드를 완성한다.

MAC이 보호할 대상은 압축 후의 데이터이고, 암호화는 데이터와 MAC을 함께 감싸야 하므로 MAC 적용이 암호화보다 먼저 수행된다. Record 헤더는 최종 전송 단위를 구성하는 단계이므로 마지막에 추가된다.

NoteBase

선지별 해설

① X — Record 헤더를 처음에 추가하고 압축을 MAC·암호화 뒤에 둔 순서가 틀렸다. 올바르게는 단편화 → 압축 → MAC 적용 → 암호화 → Record 헤더 추가이다.

② O — 단편화한 데이터를 압축하고 MAC을 적용한 뒤 암호화하며, 마지막에 Record 헤더를 추가하는 정확한 송신 순서이다.

③ X — 압축을 암호화 뒤에 둔 부분이 틀렸다. 압축은 MAC 적용과 암호화보다 먼저 수행해야 하므로 올바르게는 단편화 → 압축 → MAC 적용 → 암호화 → Record 헤더 추가이다.

④ X — 암호화를 압축과 MAC 적용보다 먼저 둔 부분이 틀렸다. MAC을 적용한 결과까지 함께 암호화해야 하므로 올바르게는 단편화 → 압축 → MAC 적용 → 암호화 → Record 헤더 추가이다.

오답 포인트

MAC 적용과 암호화의 순서를 바꾸기 쉽다는 점이 핵심 함정이다. 송신측에서는 먼저 MAC을 붙이고 그 결과를 암호화한다. 또한 Record 헤더 추가를 최초 단계로 오해하기 쉽지만, 제시된 절차에서는 암호화까지 끝난 결과에 헤더를 붙여 레코드를 완성한다.

다시 나오면 이렇게 판단

TLS Record 송신 절차는 데이터 준비인 단편화·압축, 보호 정보 생성인 MAC 적용, 기밀성 보호인 암호화, 전송 형식 완성인 Record 헤더 추가의 순서로 판단한다. 앞 단계의 결과가 뒤 단계의 입력이 되는지를 확인하면 된다.

암기 포인트

단-압-MAC-암-헤: 단편화 → 압축 → MAC 적용 → 암호화 → 헤더 추가이다.

NoteBase

10. SSL/TLS는 주로 RSA의 보안성을 다운그레이드 시키는 방식의 취약점들이 발견되었다. 이러한 SSL/TLS 대상의 공격 방식과 가장 거리가 먼 취약점은?
① 프리크(freak)
② 로그포제이(Log4j)
③ 로그잼(logjam)
④ 푸들(POODLE)

정답 2번

출제 포인트

SSL/TLS의 약한 암호군 또는 구형 프로토콜로 연결을 낮추는 공격과, 응용 프로그램 라이브러리 자체의 취약점을 구별하는 문제이다.

핵심 개념

SSL/TLS 다운그레이드 공격은 중간자 공격자가 통신 당사자에게 수출용 저강도 암호군이나 구형 프로토콜을 사용하게 하여 암호화된 연결을 약화하는 공격이다.
FREAK는 수출용 RSA, Logjam은 수출용 Diffie-Hellman, POODLE은 SSL 3.0 폴백과 CBC 패딩이라는 SSL/TLS 계층의 약점을 이용한다.
Log4j 취약점은 Java 로깅 라이브러리의 JNDI 조회 기능을 악용하는 응용 프로그램 계층의 취약점으로, SSL/TLS 다운그레이드 공격이 아니다.

NoteBase

선지별 해설

① X — FREAK는 취약한 SSL/TLS 연결을 수출용 RSA 암호군으로 낮춘 뒤 짧은 RSA 키를 깨는 공격이므로 SSL/TLS 및 RSA 보안 저하와 직접 관련된다. ‘SSL/TLS 공격과 거리가 먼 취약점’이라는 판단은 틀리며, 올바르게는 ‘수출용 RSA를 이용한 SSL/TLS 다운그레이드 공격’이다.
② O — Log4j 취약점은 Java 로깅 라이브러리에서 공격자가 통제하는 JNDI 조회 등이 처리될 때 원격 코드 실행으로 이어질 수 있는 취약점이다. SSL/TLS의 암호 협상이나 프로토콜 폴백을 약화하는 공격이 아니므로 가장 거리가 멀다.
③ X — Logjam은 TLS 연결을 수출용 저강도 Diffie-Hellman 암호군으로 낮추어 키 교환을 공격한다. RSA 자체를 겨냥하지는 않지만 SSL/TLS 다운그레이드 공격에는 해당한다. ‘SSL/TLS 공격과 거리가 먼 취약점’이라는 판단은 틀리며, 올바르게는 ‘수출용 Diffie-Hellman을 이용한 TLS 다운그레이드 공격’이다.
④ X — POODLE은 통신을 구형 SSL 3.0으로 폴백시킨 뒤 CBC 패딩 오라클을 이용하여 암호문 정보를 복구하는 공격이다. ‘SSL/TLS 공격과 거리가 먼 취약점’이라는 판단은 틀리며, 올바르게는 ‘SSL 3.0 폴백과 CBC 패딩 약점을 이용한 공격’이다.

오답 포인트

문두의 RSA라는 표현만 보고 Diffie-Hellman을 공격하는 Logjam을 고르기 쉽다. 그러나 질문은 개별 알고리즘이 아니라 SSL/TLS 대상 공격과 가장 거리가 먼 취약점을 묻는다. Logjam은 RSA 공격은 아니어도 TLS 다운그레이드 공격이고, Log4j만 로깅 라이브러리 취약점이다.

다시 나오면 이렇게 판단

먼저 공격 대상 계층을 구분한다. 약한 암호군 협상·프로토콜 폴백·패딩 문제이면 SSL/TLS 공격으로, 로깅 라이브러리의 입력 처리·JNDI 조회 문제이면 Log4j 계열의 응용 프로그램 취약점으로 판단한다.

암기 포인트

FREAK=RSA 수출 암호, Logjam=DH 수출 암호, POODLE=SSL 3.0 패딩, Log4j=Java 로깅 라이브러리이다.

NoteBase

11. 악성코드는 기능과 목적에 따라 다양한 형태로 분류할 수 있다. 다음 중 지정된 외부 주소에 접속 후 추가로 악성코드를 다운로드하여 실행하지만, 다운로드 자체는 악의적인 것이 아니기 때문에 백신 우회용으로 활용할 수 있는 악성코드는?
① 루트킷(Rootkit)
② 다운로더(Downloader)
③ 트로이 목마(Trojan Horse)
④ 드롭퍼(Dropper)

정답 2번

출제 포인트

이 문제는 외부 주소에서 추가 악성코드를 내려받아 실행하는 다운로더와 루트킷·트로이 목마·드롭퍼의 기능 차이를 묻는 문제이다.

핵심 개념

다운로더는 외부 서버에 접속해 추가 악성코드를 다운로드하고 실행하거나 설치하는 악성코드이다. 초기 파일에 최종 악성 페이로드를 직접 담지 않을 수 있어 파일 자체만 검사할 때 탐지를 피하는 데 이용될 수 있다.
루트킷은 악성 행위나 침입 흔적을 숨기고 시스템에 은밀하게 접근할 수 있게 한다. 트로이 목마는 정상 프로그램처럼 위장해 사용자의 실행을 유도한다. 드롭퍼는 내부에 포함한 악성 페이로드를 시스템에 풀어 설치하거나 실행한다.
결정적인 구분은 추가 악성코드를 외부에서 받으면 다운로더, 파일 내부에 품고 있다가 풀어 놓으면 드롭퍼라는 점이다.

선지별 해설

① X — 루트킷은 악성코드나 침입자의 존재 및 활동 흔적을 숨기는 데 중점을 둔다. 외부 주소에서 추가 악성코드를 내려받아 실행하는 유형이라는 표현은 틀리며, 올바르게는 다운로더이다.
② O — 다운로더는 지정된 외부 주소에 접속해 추가 악성코드를 다운로드하고 실행한다. 최종 악성 페이로드를 초기 파일에 직접 포함하지 않을 수 있다는 점도 문제의 설명과 일치한다.
③ X — 트로이 목마는 유용하거나 정상적인 프로그램처럼 위장하여 사용자가 실행하도록 유도하는 악성코드이다. 외부에서 추가 악성코드를 내려받는 기능으로 특정한 표현은 틀리며, 올바르게는 다운로더이다.
④ X — 드롭퍼는 자신이 내부에 포함하고 있던 악성 페이로드를 대상 시스템에 풀어 놓고 설치하거나 실행한다. 외부 주소에서 추가 악성코드를 다운로드하는 유형이라는 표현은 틀리며, 올바르게는 다운로더이다.

NoteBase

오답 포인트

② 다운로더와 ④ 드롭퍼는 모두 다른 악성코드를 실행하게 만들 수 있어 혼동하기 쉽다. 이 문항의 핵심 표현은 ‘지정된 외부 주소에 접속 후 추가로 다운로드’이다. 외부에서 가져오면 다운로더이고, 자기 내부의 페이로드를 풀어 놓으면 드롭퍼이다.

다시 나오면 이렇게 판단

악성 페이로드의 출처를 먼저 확인한다. 외부 서버에서 추가 파일을 받으면 다운로더, 내부에 포함된 파일을 추출하면 드롭퍼, 정상 프로그램으로 위장하면 트로이 목마, 존재와 흔적을 숨기면 루트킷으로 판단한다.

암기 포인트

외부에서 받는 것은 다운로더, 안에 든 것을 푸는 것은 드롭퍼이다.

NoteBase

12. 네트워크 기반의 침입탐지 시스템에 대한 설명 중 가장 적절한 것은?
① Snort, Suricata는 네트워크 기반의 침입탐지에 활용할 수 있다.
② 개별 시스템에 설치되어 공격의 결과를 상세하게 파악할 수 있다.
③ 공격을 탐지하면 즉시 차단이 가능하다.
④ 실행 중인 파일, 프로세스, 레지스트리 등을 모니터링한다.

정답 1번

출제 포인트

네트워크 기반 침입탐지시스템(NIDS), 호스트 기반 침입탐지시스템(HIDS), 네트워크 기반 침입방지시스템(NIPS)의 감시 대상과 대응 방식 차이를 묻는 문제이다.

핵심 개념

NIDS는 네트워크 구간의 패킷과 트래픽을 감시하여 침입 징후를 탐지하고 경보하는 시스템이다.
HIDS는 개별 호스트에 설치되어 파일, 프로세스, 시스템 로그, 레지스트리 등 호스트 내부의 변화를 감시한다.
NIPS는 네트워크 트래픽을 탐지할 뿐 아니라 악성 트래픽을 실시간으로 차단하는 시스템이다.
핵심 구분은 NIDS는 네트워크 트래픽의 탐지, HIDS는 개별 호스트 내부의 감시, NIPS는 네트워크 공격의 탐지와 차단이라는 점이다.

선지별 해설

① O — Snort와 Suricata는 네트워크 패킷을 분석하는 침입탐지 엔진으로, 네트워크 기반 침입탐지에 활용할 수 있다.
② X — 틀린 표현은 '개별 시스템에 설치되어 공격의 결과를 상세하게 파악'한다는 부분이다. 이는 호스트 내부 정보를 감시하는 HIDS의 특징이며, NIDS는 네트워크 구간에 배치되어 패킷과 트래픽을 분석한다.
③ X — 틀린 표현은 '공격을 탐지하면 즉시 차단이 가능하다'는 부분이다. NIDS의 기본 기능은 공격 징후의 탐지·기록·경보이며, 탐지한 트래픽을 즉시 차단하는 기능은 NIPS의 특징이다.
④ X — 틀린 표현은 '실행 중인 파일, 프로세스, 레지스트리 등을 모니터링한다'는 부분이다. 이는 개별 호스트의 내부 상태를 감시하는 HIDS의 특징이며, NIDS는 네트워크 패킷과 트래픽을 모니터링한다.

NoteBase

오답 포인트

②와 ④는 HIDS의 호스트 내부 감시 기능을 NIDS의 특징처럼 제시한 선지이다. ③은 '탐지'와 '차단'을 혼동하게 하는 선지로, 즉시 차단이라는 표현은 NIDS가 아니라 NIPS를 가리킨다.

다시 나오면 이렇게 판단

감시 대상과 대응 동사를 함께 확인한다. 네트워크 패킷·트래픽을 탐지하면 NIDS, 개별 시스템의 파일·프로세스·레지스트리를 감시하면 HIDS, 악성 트래픽을 차단하면 NIPS로 판단한다.

암기 포인트

NIDS는 네트워크 탐지, HIDS는 호스트 내부 감시, NIPS는 네트워크 탐지와 차단이다.

NoteBase

13. TCP는 연결지향 프로토콜로 가상의 연결 통로를 설정하여 물리적인 전용회선과 같이 동작한다. 다음 중 TCP에서 신뢰성을 확보하기 위하여 적용하는 제어 기법으로 볼 수 없는 것은?

① 흐름 제어 ② 오류 제어
③ 혼잡 제어 ④ 경로 제어

정답 4번

출제 포인트

TCP가 연결의 신뢰성과 전송 상태를 관리하기 위해 사용하는 제어 기능과, 네트워크 계층이 담당하는 경로 선택 기능을 구별하는 문제이다.

핵심 개념

흐름 제어: 수신 측의 처리 능력을 넘지 않도록 송신량을 조절하는 기능이다. 핵심 키워드는 수신 윈도우이다.
오류 제어: 손상·유실·중복·순서 뒤바뀜을 확인하고 확인 응답과 재전송 등으로 데이터를 올바르게 전달하는 기능이다.
혼잡 제어: 네트워크의 혼잡 정도에 따라 송신 속도를 조절하는 기능이다. 핵심 키워드는 혼잡 윈도우이다.
경로 제어: 목적지까지 패킷이 이동할 경로를 선택하는 기능으로, TCP가 아니라 IP와 라우터가 동작하는 네트워크 계층의 영역이다.

NoteBase

선지별 해설

① X
흐름 제어는 수신 측이 감당할 수 있는 범위에 맞추어 송신량을 조절하는 TCP의 제어 기능이다. '흐름 제어'는 제외 대상이 아니라 TCP에 적용되는 제어 기법이다.

② X
오류 제어는 순서 번호, 확인 응답, 재전송 등을 이용해 데이터의 유실이나 순서 오류에 대응하는 TCP의 핵심 기능이다. '오류 제어'는 제외 대상이 아니라 TCP의 신뢰성 있는 전송을 위한 제어 기법이다.

③ X
혼잡 제어는 네트워크가 혼잡해지지 않도록 송신량을 조절하는 TCP의 제어 기능이다. '혼잡 제어'는 제외 대상이 아니라 TCP에 적용되는 제어 기법이다.

④ O
경로 제어는 목적지까지의 전달 경로를 결정하는 네트워크 계층의 기능이다. TCP는 종단 간 전송을 제어하지만 라우팅 경로를 결정하지 않으므로, 경로 제어는 TCP의 신뢰성 확보를 위한 제어 기법으로 볼 수 없다.

오답 포인트

'혼잡 제어'는 네트워크 전체 상태와 관련되므로 TCP 기능이 아니라고 착각하기 쉽다. 그러나 TCP는 혼잡 상태에 맞추어 송신량을 조절한다. 반면 '경로 제어'는 전송량 조절이 아니라 패킷이 이동할 길을 정하는 네트워크 계층의 기능이다.

다시 나오면 이렇게 판단

수신자의 처리 능력, 데이터의 오류·유실, 네트워크 혼잡에 따른 송신량 조절은 TCP의 기능으로 판단한다.
목적지까지의 경로 선택이나 패킷 전달은 IP·라우터가 담당하는 네트워크 계층의 기능으로 판단한다.

암기 포인트

TCP는 흐름·오류·혼잡을 제어하고, 경로는 네트워크 계층이 선택한다.

NoteBase

14. 다음 네트워크 프로토콜 중 가장 상위 계층에서 동작하는 것은?

① PPTP(Point-to-Point Tunneling Protocol)
② L2TP(Layer 2 Tunneling Protocol)
③ IPsec(Internet Protocol Security)
④ TLS(Transport Layer Security)

정답 4번

출제 포인트

PPTP·L2TP·IPsec·TLS가 동작하는 계층을 비교하여 가장 상위 계층의 프로토콜을 찾는 문제이다.

핵심 개념

PPTP와 L2TP는 데이터링크 계층의 프레임을 터널링하는 2계층 터널링 프로토콜이다.
IPsec은 IP 패킷을 보호하는 네트워크 계층 보안 프로토콜이다.
TLS는 전송계층 위에서 응용 데이터의 통신 보안을 제공하므로 이 선지들 가운데 가장 상위 계층에서 동작한다.
계층 순서는 데이터링크 계층 → 네트워크 계층 → 전송계층 및 그 상단의 순서로 높아진다.

선지별 해설

① X — PPTP는 PPP 프레임을 터널링하는 2계층 터널링 프로토콜이므로 가장 상위 계층에서 동작하지 않는다. 틀린 판단은 PPTP를 최상위로 보는 것이며, 올바르게는 데이터링크 계층의 터널링 프로토콜로 본다.
② X — L2TP는 이름 그대로 Layer 2, 즉 데이터링크 계층의 터널링 프로토콜이다. 틀린 판단은 L2TP를 최상위로 보는 것이며, 올바르게는 2계층 프로토콜로 본다.
③ X — IPsec은 IP 패킷 단위로 기밀성·무결성·인증 등을 제공하는 네트워크 계층 보안 프로토콜이다. 틀린 판단은 IPsec을 TLS보다 상위로 보는 것이며, 올바르게는 3계층 프로토콜로 본다.
④ O — TLS는 전송계층 위에서 응용 프로토콜의 데이터를 보호하므로 PPTP·L2TP·IPsec보다 상위 계층에서 동작한다.

오답 포인트

③ IPsec과 ④ TLS는 모두 보안 프로토콜이어서 용도를 기준으로만 보면 혼동하기 쉽다. 이 문제에서는 보안 강도나 터널링 여부가 아니라 보호하는 데이터 단위와 동작 계층을 비교해야 한다. IPsec은 IP 패킷을 다루는 3계층이고, TLS는 그보다 위에서 응용 데이터를 보호한다.

NoteBase

다시 나오면 이렇게 판단

프로토콜 이름과 처리 대상을 연결한다. Layer 2나 PPP 프레임이면 데이터링크 계층, IP 패킷이면 네트워크 계층, 응용 데이터의 종단 간 보안이면 TLS로 판단한다. 그런 다음 데이터링크 < 네트워크 < 전송계층 및 그 상단의 순서로 비교한다.

암기 포인트

PPTP·L2TP는 2계층, IPsec은 3계층, TLS는 그보다 위이다.

NoteBase

15. 다음 중 DDoS 공격을 방어하기 위한 기본적인 방법으로 가장 적절하지 않은 것은?
① 공격 트래픽의 소스 IP 주소 차단
② 방화벽 및 IDS/IPS 시스템을 이용한 필터링
③ 트래픽 분석을 통한 비정상적인 패턴 탐지
④ 유입되는 모든 트래픽을 허용하여 네트워크 자원을 최대한 활용

정답 4번

출제 포인트

DDoS 공격 방어는 공격 트래픽을 식별·차단하거나 유입량을 제한하여 서비스 자원의 고갈을 막는다는 원리를 묻는 문제이다.

핵심 개념

DDoS 공격은 다수의 공격원이 대량의 트래픽이나 요청을 동시에 보내 서버·회선 등의 자원을 고갈시키고 정상 이용자의 서비스를 방해하는 공격이다.
기본 방어는 출발지 차단, 방화벽·IDS/IPS 필터링, 비정상 패턴 탐지, 속도 제한 등으로 공격 트래픽을 줄이면서 정상 트래픽은 유지하는 방식이다.

선지별 해설

① O — 공격 트래픽의 소스 IP 주소를 식별하여 차단하면 해당 출발지에서 들어오는 공격 트래픽을 줄일 수 있으므로 기본적인 대응 방법에 해당한다. 다만 IP 위조나 다수의 분산된 공격원 때문에 이것만으로는 충분하지 않을 수 있다.

② O — 방화벽은 정책에 따라 트래픽을 차단하고, IDS/IPS는 공격 징후를 탐지하거나 차단하므로 DDoS 트래픽 필터링에 활용할 수 있다.

③ O — 평소와 다른 트래픽 급증, 비정상 요청 빈도 등의 패턴을 분석하면 공격 트래픽을 탐지하고 대응할 수 있다.

④ X — 틀린 표현은 '유입되는 모든 트래픽을 허용'이다. 모든 트래픽을 허용하면 공격 트래픽까지 내부 자원에 도달하여 대역폭과 서버 자원이 더 빨리 고갈된다. 올바르게는 비정상·악성 트래픽을 탐지하여 차단하거나 속도를 제한하고, 정상 트래픽에 필요한 자원을 확보해야 한다.

NoteBase

오답 포인트

④의 '네트워크 자원을 최대한 활용'이라는 표현만 보면 서비스 가용성을 높이는 방법처럼 보일 수 있다. 그러나 DDoS 방어의 목적은 모든 트래픽을 처리하는 것이 아니라 공격 트래픽을 걸러 자원을 보호하고 정상 이용자의 서비스를 유지하는 것이다.

다시 나오면 이렇게 판단

선지가 공격 트래픽을 탐지·차단·제한하여 자원 고갈을 막는 방식이면 적절한 방어로 판단한다. 반대로 출처와 정상 여부를 가리지 않고 트래픽을 모두 허용하거나 무제한 처리한다면 DDoS 공격을 키우는 방식으로 판단한다.

암기 포인트

DDoS 방어는 '모두 허용'이 아니라 '탐지·차단·제한으로 정상 서비스 보호'이다.

NoteBase

16. 제로트러스트 보안 모델에서 최소 권한 원칙에 대한 설명으로 가장 적절한 것은?

① 사용자에게 네트워크에 접근할 최소한의 권한만 부여해야 한다.

② 관리자만이 네트워크 자원에 접근할 수 있도록 해야 한다.

③ 사용자는 네트워크에 접근할 때마다 새로운 권한을 요청해야 한다.

④ 모든 네트워크 트래픽을 검증해야 한다.

정답 1번

출제 포인트

제로 트러스트 보안 모델의 최소 권한 원칙이 사용자에게 필요한 범위의 권한만 부여하는 원칙임을 이해하는지 묻는 문제이다.

핵심 개념

제로 트러스트는 사용자나 기기를 위치만으로 신뢰하지 않고 접근할 때마다 신원, 기기 상태, 요청 맥락 등을 확인하여 접근을 통제하는 보안 모델이다.
최소 권한은 사용자·기기·프로세스가 업무 수행에 필요한 자원에 필요한 수준과 기간만큼만 접근하도록 권한을 제한하는 원칙이다. 핵심은 '관리자에게 권한 집중'이나 '매번 새 권한 발급'이 아니라 '필요 최소한의 권한 부여'이다.

선지별 해설

① O — 사용자에게 네트워크 접근에 필요한 최소한의 권한만 부여한다는 설명은 최소 권한 원칙에 정확히 부합한다.
② X — 틀린 표현은 '관리자만이 네트워크 자원에 접근'하도록 한다는 부분이다. 최소 권한은 접근 주체를 관리자만으로 제한하는 원칙이 아니라, 각 사용자에게 직무 수행에 필요한 자원과 권한만 부여하는 원칙이다.
③ X — 틀린 표현은 네트워크에 접근할 때마다 '새로운 권한을 요청'해야 한다는 부분이다. 제로 트러스트에서는 접근 요청마다 인증·인가 조건을 지속적으로 검증하지만, 최소 권한 자체는 필요한 범위와 기간으로 권한을 제한하는 원칙이다.
④ X — 틀린 표현은 '모든 네트워크 트래픽을 검증'하는 것이 최소 권한 원칙이라는 부분이다. 트래픽 검사와 지속적 검증은 제로 트러스트의 다른 통제 요소가 될 수 있으나, 최소 권한은 접근 주체가 필요한 자원에 필요한 수준으로만 접근하도록 권한을 제한하는 원칙이다.

NoteBase

오답 포인트

③의 '접근할 때마다'와 ④의 '검증'은 제로 트러스트의 지속적 검증을 떠올리게 하지만, 문제는 제로 트러스트 전체가 아니라 최소 권한 원칙을 묻는다. 최소 권한의 판단 기준은 검증 횟수나 트래픽 검사 여부가 아니라 부여되는 권한의 범위와 수준이다.

다시 나오면 이렇게 판단

선지에서 '업무에 필요한 자원만', '필요한 수준만', '필요한 기간만'처럼 권한의 범위를 줄이는 표현을 찾으면 최소 권한으로 판단한다. '아무도 신뢰하지 않음', '매 요청 검증', '트래픽 감시'는 제로 트러스트의 관련 요소일 수 있지만 최소 권한의 직접적인 정의와는 구별한다.

암기 포인트

최소 권한은 필요한 사람에게, 필요한 자원만, 필요한 수준과 기간만 부여하는 원칙이다.

NoteBase

17. TCP 연결설정을 위한 3-Way Handshaking 과정에서 Half-Open 연결 시도가 가능하다는 취약점을 이용한 공격 방식을 나타낸 것으로 가장 적절한 것은?
① 스머프 공격
② ARP 스푸핑
③ SYN Flooding 공격
④ 핑 오브 데스

정답 3번

출제 포인트

TCP 3-Way Handshaking을 끝까지 완료하지 않아 Half-Open 연결을 대량으로 남기는 공격을 구별하는 문제이다.

핵심 개념

SYN Flooding은 다수의 SYN을 보낸 뒤 마지막 ACK를 보내지 않아 서버의 연결 대기 자원을 소진시키는 서비스 거부 공격이다. 핵심 키워드는 ‘TCP 연결 설정’, ‘마지막 ACK 미전송’, ‘Half-Open’이다.
스머프 공격은 피해자의 IP 주소로 출발지를 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수의 응답이 피해자에게 몰리게 하는 증폭 공격이다.
ARP 스푸핑은 위조된 ARP 정보를 보내 ARP 캐시의 IP 주소와 MAC 주소 대응 관계를 변조하는 공격이다.
핑 오브 데스는 비정상적으로 큰 IP 패킷을 조각화해 보내고 재조립 과정에서 시스템 장애를 유발하는 공격이다.

NoteBase

선지별 해설

① X
스머프 공격은 ICMP Echo와 브로드캐스트를 이용한 증폭 공격이므로 TCP의 Half-Open 연결을 만드는 공격이 아니다. 틀린 표현은 ‘스머프 공격’이며, Half-Open 취약점을 이용하는 공격으로는 ‘SYN Flooding 공격’이 맞다.

② X
ARP 스푸핑은 위조된 ARP 메시지로 ARP 캐시의 IP-MAC 대응 관계를 변조하는 공격이므로 TCP 3-Way Handshaking과 직접 관련되지 않는다. 틀린 표현은 ‘ARP 스푸핑’이며, Half-Open 연결을 대량으로 만드는 공격으로는 ‘SYN Flooding 공격’이 맞다.

③ O
SYN Flooding은 공격자가 SYN을 대량 전송한 뒤 서버의 SYN-ACK에 대한 마지막 ACK를 보내지 않는 방식이다. 이로 인해 서버에 Half-Open 연결이 누적되어 연결 대기 자원이 고갈된다.

④ X
핑 오브 데스는 비정상적으로 큰 IP 패킷의 조각화와 재조립 과정에서 시스템 오류나 장애를 유발하는 공격이므로 Half-Open 연결을 이용하지 않는다. 틀린 표현은 ‘핑 오브 데스’이며, TCP 연결 설정을 미완료 상태로 남기는 공격으로는 ‘SYN Flooding 공격’이 맞다.

오답 포인트

①과 ④도 네트워크 서비스 거부 공격이라는 공통점이 있어 혼동하기 쉽다. 그러나 문제의 결정적 단서는 ‘3-Way Handshaking’과 ‘Half-Open’이며, 이는 서버가 SYN-ACK를 보낸 뒤 마지막 ACK를 받지 못한 상태를 뜻한다.

다시 나오면 이렇게 판단

‘SYN → SYN-ACK → ACK’ 중 마지막 ACK가 오지 않아 연결이 미완료 상태로 쌓이면 SYN Flooding으로 판단한다. ICMP 브로드캐스트 증폭은 스머프, ARP 캐시 변조는 ARP 스푸핑, 비정상적으로 큰 패킷의 재조립 장애는 핑 오브 데스로 구별한다.

암기 포인트

Half-Open은 SYN Flooding, ICMP 증폭은 스머프, IP-MAC 변조는 ARP 스푸핑, 거대 패킷은 핑 오브 데스이다.

NoteBase

18. OSI 참조 모델에서 라우터가 동작하는 계층은?
① 응용 계층
② 데이터링크 계층
③ 세션 계층
④ 네트워크 계층

정답 4번

출제 포인트

이 문제는 라우터의 핵심 기능과 OSI 참조 모델의 계층을 연결할 수 있는지를 묻는 문제이다.

핵심 개념

라우터는 서로 다른 네트워크 사이에서 IP 주소를 바탕으로 패킷의 전달 경로를 결정하고 다음 네트워크로 전달하는 장비이다. 따라서 OSI 참조 모델의 네트워크 계층에서 동작한다.
응용 계층은 사용자 응용 프로그램에 네트워크 서비스를 제공하고, 세션 계층은 통신 세션을 설정·관리·종료하며, 데이터링크 계층은 인접한 노드 사이의 프레임 전송을 담당한다.

선지별 해설

① X — 응용 계층은 사용자 응용 프로그램에 네트워크 서비스를 제공하는 계층이므로 라우터의 기본 동작 계층이 아니다. 틀린 표현은 '응용 계층'이며, 올바르게는 '네트워크 계층'이다.
② X — 데이터링크 계층은 MAC 주소와 프레임을 이용해 같은 링크에서 인접한 노드 사이의 전송을 담당하므로 라우터의 기본 동작 계층이 아니다. 틀린 표현은 '데이터링크 계층'이며, 올바르게는 '네트워크 계층'이다.
③ X — 세션 계층은 응용 프로그램 사이의 통신 세션을 설정·관리·종료하는 계층이므로 라우터의 기본 동작 계층이 아니다. 틀린 표현은 '세션 계층'이며, 올바르게는 '네트워크 계층'이다.
④ O — 네트워크 계층은 IP 주소를 이용한 논리적 주소 지정과 경로 선택을 담당하며, 라우터는 이 계층에서 패킷을 전달한다.

오답 포인트

라우터에도 네트워크 인터페이스가 있으므로 데이터링크 계층과 혼동하기 쉽다. 그러나 장비를 분류할 때는 핵심 판단 기능을 본다. 라우터의 핵심은 MAC 주소에 따른 프레임 전달이 아니라 IP 주소에 따른 경로 선택과 패킷 전달이다.

다시 나오면 이렇게 판단

장비가 어떤 주소와 데이터 단위를 기준으로 전달하는지 확인한다. MAC 주소와 프레임이면 데이터링크 계층, IP 주소와 패킷이면 네트워크 계층으로 판단한다.

NoteBase

암기 포인트

라우터는 IP·패킷·경로 선택, 즉 네트워크 계층이다.

NoteBase

19. 쿠키와 세션의 차이점을 가장 잘 설명한 것은?
① 쿠키는 파일로 저장되는 경우 탈취, 변조, 스니핑 등의 공격에 취약하다.
② 세션은 서버에서 데이터를 참조하므로 속도가 빠르다.
③ 쿠키는 브라우저를 종료하면 삭제된다.
④ 쿠키는 서버의 메모리에 저장된다.

정답 1번

출제 포인트

쿠키와 세션이 사용자 상태정보를 어디에 저장하고 어떻게 식별하는지를 구분하는 문제이다.

핵심 개념

쿠키: 웹사이트가 보낸 작은 데이터를 브라우저가 클라이언트 측에 보관하고 이후 요청에 실어 보내는 방식이다. 키워드는 클라이언트 저장이다.
세션: 사용자별 상태정보를 서버 측에 보관하고, 클라이언트가 전달하는 세션 식별자로 해당 정보를 찾는 방식이다. 키워드는 서버 저장이다.
핵심 대비는 '쿠키는 클라이언트 측, 세션은 서버 측'이다.

선지별 해설

① O — 쿠키는 브라우저 등 클라이언트 측에 저장되므로 쿠키 값이 탈취되거나 변조될 위험이 있다. 또한 HTTPS로 보호되지 않은 통신에서는 전송 중 스니핑 위험도 생길 수 있으므로 네 선지 중 차이를 가장 잘 설명한다.
② X — 틀린 표현은 '서버에서 데이터를 참조하므로 속도가 빠르다'이다. 서버에서 상태정보를 조회한다는 사실만으로 쿠키보다 빠르다고 할 수 없으며, 조회와 관리에 추가 비용이 들 수도 있다. 올바르게는 '세션은 상태정보를 서버에 저장하고 클라이언트가 세션 식별자를 전달한다'이다.
③ X — 틀린 표현은 '브라우저를 종료하면 삭제된다'이다. 만료 시점이 지정된 영속 쿠키는 브라우저를 종료해도 남을 수 있다. 올바르게는 '브라우저 종료 시 삭제되는 세션 쿠키도 있지만, 쿠키의 만료 설정에 따라 종료 후에도 유지될 수 있다'이다.
④ X — 틀린 표현은 '서버의 메모리에 저장된다'이다. 쿠키는 클라이언트의 브라우저에 저장된다. 올바르게는 '서버 측에 저장되는 것은 세션의 상태정보이고, 쿠키는 클라이언트 측에 저장된다'이다.

NoteBase

오답 포인트

③은 '세션 쿠키'의 성질을 모든 쿠키의 성질로 확대하고, ④는 쿠키와 세션의 저장 위치를 뒤바꾼 선지이다. ②의 서버 참조 여부는 저장 위치의 차이이지 속도 우위를 보장하는 근거가 아니다.

다시 나오면 이렇게 판단

먼저 상태정보의 저장 위치를 확인한다. 클라이언트·브라우저에 저장되면 쿠키, 서버에 저장되고 식별자로 조회하면 세션으로 판단한다. 브라우저 종료 시 삭제 여부는 쿠키의 만료 방식에 따라 따로 판단한다.

암기 포인트

쿠키는 클라이언트 저장, 세션은 서버 저장이다.

NoteBase

20. SSL/TLS를 구성하는 프로토콜이 아닌 것은?
① Handshake Protocol
② Change Cipher Spec Protocol
③ Authorization Protocol
④ Record Protocol

정답 3번

출제 포인트

SSL/TLS를 구성하는 하위 프로토콜과 구성 요소가 아닌 명칭을 구별하는 문제이다.

핵심 개념

SSL/TLS는 데이터를 일정한 형식으로 캡슐화하여 전달하는 Record Protocol을 기반으로 하며, 그 위에서 Handshake Protocol, Change Cipher Spec Protocol, Alert Protocol 등이 동작한다.
Handshake Protocol: 통신 상대를 인증하고 암호 알고리즘과 키 생성에 필요한 정보를 협상한다.
Change Cipher Spec Protocol: 이후의 통신부터 협상된 암호 사양을 적용한다는 전환을 알린다.
Alert Protocol: 경고나 오류 및 연결 종료 상태를 상대에게 알린다.
Record Protocol: 상위 계층의 데이터를 분할·캡슐화하고 무결성 보호와 암호화를 적용하여 전송한다.

선지별 해설

① O — Handshake Protocol은 SSL/TLS의 구성 프로토콜로서 인증, 암호 알고리즘 선택, 키 관련 정보의 협상을 담당한다.
② O — Change Cipher Spec Protocol은 협상된 암호 사양을 이후 레코드부터 사용한다는 사실을 알리는 구성 프로토콜이다.
③ X — 틀린 표현은 'Authorization Protocol'이다. SSL/TLS의 구성 프로토콜에는 이 명칭이 없으며, 올바르게는 경고·오류·연결 종료를 알리는 'Alert Protocol'이다.
④ O — Record Protocol은 SSL/TLS의 기본 전송 단위인 레코드를 만들고 데이터의 무결성 보호와 암호화를 담당하는 구성 프로토콜이다.

오답 포인트

③의 Authorization은 보안 분야에서 자주 쓰이는 '권한 부여' 용어라 그럴듯해 보이지만, SSL/TLS의 프로토콜 명칭은 아니다. Authentication은 Handshake 과정에서 수행되지만 Authorization Protocol이라는 별도 구성 프로토콜은 없다.

NoteBase

다시 나오면 이렇게 판단

SSL/TLS 구성 프로토콜을 묻는 문제에서는 Record를 기반으로 Handshake, Change Cipher Spec, Alert가 동작한다는 구조를 확인한다. 인증과 권한 부여의 일반 용어를 실제 프로토콜 이름과 구별한다.

암기 포인트

SSL/TLS 구성은 ‘Record 위에 Handshake·Change Cipher Spec·Alert’이며, Authorization Protocol은 없다.

NoteBase

21. 다음 중 ㉠, ㉡에 들어갈 도구 이름으로 가장 적절한 것은?

> (㉠)은(는) 네트워크 검색 및 보안 점검을 위해 제작된 오픈소스 도구로서 여러 가지 네트워크 스캐닝 관련 스크립트를 포함하고 있다.
>
> (㉡)은(는) 네트워크 연결을 통해 TCP연결, UDP 패킷 전송, 임의 TCP 및 UDP 포트청취 등을 수행할 수 있어 포트 포워딩, 데이터전송, 네트워크 디버깅 등에 활용할 수 있다.

① ㉠: netcat ㉡: nmap
② ㉠: netcat ㉡: Hydra
③ ㉠: Burp Suite ㉡: netcat
④ ㉠: Burp Suite ㉡: Hydra

정답 1번

출제 포인트

네트워크 도구의 대표 기능을 근거로 nmap과 netcat을 구별하는 문제이다.

핵심 개념

nmap: 호스트·서비스·포트 등을 탐색하고 보안 점검에 사용하는 오픈소스 네트워크 스캐닝 도구이며, 스크립트 엔진을 통해 다양한 점검 기능을 수행한다.
netcat: TCP 또는 UDP 연결을 만들거나 특정 포트에서 연결을 기다리며 데이터를 송수신하는 범용 네트워크 도구이다.
Burp Suite: 웹 애플리케이션의 HTTP·HTTPS 통신을 가로채고 분석하여 보안 취약점을 점검하는 도구이다.
Hydra: 여러 네트워크 서비스의 로그인 인증 정보를 반복 대입하여 점검하는 도구이다.

NoteBase

선지별 해설

① O — ㉠은 네트워크 탐색·보안 점검과 스크립트 기반 스캐닝을 수행하는 nmap이고, ㉡은 TCP·UDP 연결, 포트 수신, 데이터 송수신 등에 쓰는 netcat이므로 두 대응이 모두 옳다.
② X — ㉠을 netcat, ㉡을 Hydra로 대응한 부분이 모두 틀렸다. 올바르게는 ㉠ nmap, ㉡ netcat이다.
③ X — ㉠을 Burp Suite로 대응한 부분이 틀렸다. Burp Suite는 주로 웹 애플리케이션 통신 분석과 취약점 점검에 사용하며, ㉠은 nmap이다. ㉡을 netcat으로 대응한 부분은 옳으므로 전체 조합은 ㉠ nmap, ㉡ netcat으로 고쳐야 한다.
④ X — ㉠을 Burp Suite, ㉡을 Hydra로 대응한 부분이 모두 틀렸다. Hydra는 로그인 인증 정보 대입 점검 도구이며, 올바른 조합은 ㉠ nmap, ㉡ netcat이다.

오답 포인트

㉠의 '보안 점검'이라는 표현만 보고 웹 보안 도구인 Burp Suite를 고르거나, ㉡의 '네트워크 연결'만 보고 인증 점검 도구인 Hydra를 고르는 것이 함정이다. '네트워크 스캐닝 스크립트'는 nmap, 'TCP·UDP 연결과 포트 수신'은 netcat을 가리킨다.

다시 나오면 이렇게 판단

도구의 대표 동작을 먼저 찾는다. 호스트·포트 탐색과 스크립트 기반 점검이면 nmap, TCP·UDP 연결을 직접 만들거나 포트에서 수신하며 데이터를 전달하면 netcat으로 판단한다. 웹 통신 가로채기는 Burp Suite, 로그인 인증 정보 반복 대입은 Hydra로 구별한다.

암기 포인트

nmap은 스캔, netcat은 연결·송수신, Burp Suite는 웹, Hydra는 로그인 인증 점검이다.

NoteBase

22. TCP 연결설정을 위한 3-Way Handshaking 과정에서 주고받는 메시지의 종류와 순서가 올바른 것은?

① FIN → SYN → SYN ACK
② SYN ACK → ACK → SYN
③ SYN → SYN ACK → FIN
④ SYN → SYN ACK → ACK

정답 4번

출제 포인트

TCP 연결 설정에 사용하는 3-Way Handshaking에서 SYN, SYN ACK, ACK가 오가는 순서를 묻는 문제이다.

올바른 순서

1. SYN — 연결을 시작하는 측이 상대에게 연결 설정과 초기 순서 번호의 동기화를 요청한다.
2. SYN ACK — 상대가 요청을 확인하면서 자신의 연결 설정 요청도 함께 보낸다.
3. ACK — 처음 요청한 측이 상대의 응답을 확인하여 연결 설정을 완료한다.

왜 이 순서인가: 상대는 먼저 SYN을 받아야 SYN ACK로 응답할 수 있고, 요청 측은 그 SYN ACK를 받은 뒤 ACK를 보내야 양쪽의 연결 설정 의사가 확인되기 때문이다.

선지별 해설

① X — FIN은 이미 설정된 연결을 종료할 때 사용하는 제어 메시지이므로 연결 설정의 첫 단계가 될 수 없다. 틀린 순서 'FIN → SYN → SYN ACK'는 올바르게 'SYN → SYN ACK → ACK'가 된다.

② X — 연결 설정은 요청 측의 SYN으로 시작해야 하므로 SYN ACK가 먼저 올 수 없고, 마지막 단계 뒤에 SYN을 다시 보내지도 않는다. 틀린 순서 'SYN ACK → ACK → SYN'은 올바르게 'SYN → SYN ACK → ACK'가 된다.

③ X — 첫 두 단계인 SYN과 SYN ACK는 맞지만, 마지막의 FIN은 연결 종료 메시지이다. 틀린 표현 'FIN'은 올바르게 'ACK'가 되어 'SYN → SYN ACK → ACK' 순서가 된다.

④ O — 요청 측의 SYN, 응답 측의 SYN ACK, 요청 측의 ACK 순서로 양쪽의 연결 설정 의사와 초기 순서 번호를 확인하므로 올바르다.

NoteBase

오답 포인트

③은 앞의 두 메시지가 맞아 보이지만 마지막에 연결 종료용 FIN을 섞은 선지이다. 연결 설정은 ACK로 끝나며, FIN은 연결 종료 절차에서 사용된다는 구분이 핵심이다.

다시 나오면 이렇게 판단

TCP 연결 설정 절차는 '연결 요청(SYN) → 요청 수락과 동기화 응답(SYN ACK) → 응답 확인(ACK)'의 의존관계로 판단한다. FIN이 포함되면 연결 설정이 아니라 연결 종료와 관련된 절차로 구분한다.

암기 포인트

연결 설정은 'SYN → SYN ACK → ACK', 연결 종료 신호는 FIN이다.

NoteBase

23. 진짜처럼 꾸며진 가짜 와이파이로 접근을 유도한 뒤 사용자 신상정보를 훔치는 공격기법을 나타내는 용어는?
① 사회공학공격기법
② 딥페이크(Deep Fake)
③ 이블 트윈(Evil twin)
④ APT 공격

정답 3번

출제 포인트

진짜 무선 액세스 포인트와 비슷하게 꾸민 가짜 와이파이로 접속을 유도해 정보를 탈취하는 이블 트윈 공격의 정의를 묻는 문제이다.

핵심 개념

이블 트윈(Evil twin)은 정상 와이파이와 같거나 비슷한 네트워크 이름을 내세운 악성 액세스 포인트로 사용자의 접속을 유도한 뒤 통신 내용이나 인증정보 등 개인정보를 가로채는 무선 네트워크 공격이다. 핵심 단서는 '진짜처럼 꾸민 가짜 와이파이'이다.

선지별 해설

① X — 사회공학공격기법은 사람의 심리나 신뢰를 이용하여 정보를 얻거나 행동을 유도하는 넓은 공격 범주이다. 틀린 표현은 '사회공학공격기법'이며, 제시된 가짜 와이파이 공격의 구체적인 명칭은 이블 트윈이다.
② X — 딥페이크(Deep Fake)는 인공지능을 이용해 얼굴·음성·영상 등을 실제처럼 합성하거나 변조하는 기술이다. 틀린 표현은 '딥페이크'이며, 가짜 와이파이를 만들어 접속을 유도하는 공격은 이블 트윈이다.
③ O — 이블 트윈(Evil twin)은 정상 와이파이처럼 보이는 악성 액세스 포인트를 설치하여 사용자의 접속과 정보 탈취를 노리는 공격이므로 제시된 설명과 일치한다.
④ X — APT 공격은 특정 조직이나 기관을 장기간 지속적으로 노리는 지능형 표적 공격이다. 틀린 표현은 'APT 공격'이며, 진짜처럼 꾸민 가짜 와이파이로 사용자를 유인하는 공격은 이블 트윈이다.

오답 포인트

①은 사람을 속인다는 점에서 넓게 연관될 수 있지만, 문항은 '가짜 와이파이'라는 구체적 수법의 명칭을 묻는다. ②의 가짜 콘텐츠, ④의 장기 표적 침투와 구분해야 한다.

NoteBase

다시 나오면 이렇게 판단

정상 와이파이와 비슷한 이름의 가짜 액세스 포인트, 접속 유도, 통신·인증정보 탈취가 함께 제시되면 이블 트윈으로 판단한다.

암기 포인트

진짜 와이파이의 사악한 쌍둥이 가짜 AP는 이블 트윈이다.

NoteBase

24. 다음 중 SSL Handshake를 하는데 주고받는 메시지의 순서가 올바른 것은?

㉠: Client Hello
㉡: Change Cipher Spec Finished
㉢: Server Key Exchange
㉣: Client Key Exchange
㉤: Server Hello
㉥: Certificate

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

정답 3번

출제 포인트

SSL Handshake에서 클라이언트와 서버가 협상하고 인증 및 키 교환을 거쳐 암호 통신을 시작하는 메시지의 선후관계를 묻는 문제이다.

올바른 순서

1. Client Hello(ㄱ) — 클라이언트가 지원 가능한 암호 방식 등의 협상 정보를 제시한다.
2. Server Hello(ㅁ) — 서버가 사용할 암호 방식 등의 협상 결과를 알린다.
3. Certificate(ㅂ) — 서버가 자신의 인증서를 보내 신원과 공개키 정보를 제공한다.
4. Server Key Exchange(ㄷ) — 서버가 키 교환에 필요한 추가 정보를 보낸다.
5. Client Key Exchange(ㄹ) — 클라이언트가 공유 비밀을 만드는 데 필요한 키 교환 정보를 보낸다.
6. Change Cipher Spec·Finished(ㄴ) — 협상한 암호 사양을 적용하고 핸드셰이크가 정상적으로 끝났음을 확인한다.

왜 이 순서인가: 서버의 협상 결과와 인증·키 교환 정보가 먼저 제공되어야 클라이언트가 그에 맞는 키 교환 정보를 만들 수 있고, 키가 마련된 뒤에야 암호 사양을 적용하고 Finished 메시지로 완료를 확인할 수 있기 때문이다.

NoteBase

선지별 해설

① X — ㄱ 다음에 곧바로 ㄷ을 배치하고 ㅁ과 ㅂ을 맨 뒤에 둔 점이 틀렸다. Server Hello와 Certificate가 Server Key Exchange보다 먼저 와야 한다. 올바르게는 ㄱ → ㅁ → ㅂ → ㄷ → ㄹ → ㄴ이다.

② X — ㅂ을 Client Hello보다 앞에 배치한 점이 틀렸다. 핸드셰이크는 클라이언트의 Client Hello로 시작하고, 서버는 Server Hello 이후 Certificate를 보낸다. 올바르게는 ㄱ → ㅁ → ㅂ → ㄷ → ㄹ → ㄴ이다.

③ O — Client Hello 이후 Server Hello, Certificate, Server Key Exchange가 이어지고, 그다음 Client Key Exchange와 Change Cipher Spec·Finished가 오는 올바른 순서이다.

④ X — Server Hello를 Client Hello보다 앞에 두고, Certificate를 Server Key Exchange 뒤에 둔 점이 틀렸다. 서버는 Client Hello를 받은 뒤 Server Hello를 보내며, Certificate는 Server Key Exchange보다 먼저 온다. 올바르게는 ㄱ → ㅁ → ㅂ → ㄷ → ㄹ → ㄴ이다.

오답 포인트

서버가 보내는 Server Hello, Certificate, Server Key Exchange의 내부 순서와 전체 시작 메시지를 뒤섞는 것이 함정이다. 특히 Server Hello는 Client Hello에 대한 응답이므로 먼저 올 수 없고, Change Cipher Spec·Finished는 키 교환이 끝난 뒤의 마무리 단계이다.

다시 나오면 이렇게 판단

절차형 문항에서는 '클라이언트의 협상 제안 → 서버의 협상 응답 → 서버 인증과 키 교환 정보 → 클라이언트 키 교환 → 암호 적용과 완료 확인'의 의존관계로 판단한다.

암기 포인트

클라 인사 → 서버 인사·인증·키 정보 → 클라이언트 키 교환 → 암호 적용·완료의 흐름으로 기억한다.

NoteBase

25. ㉠, ㉡에 들어갈 단어로 가장 적절한 것은?

> (㉠)은(는) 방화벽 정책 설정 시 (㉡) 패킷에 대해서는 차단 정책을 두지 않은 허점을 이용하는 공격 방식으로 서버에서 공격자의 컴퓨터로 접속하도록 하여 시스템의 보안정책을 우회한다.

① ㉠: 리버스 텔넷
㉡: 아웃바운드
② ㉠: 원격 데스크톱 프로토콜 공격
㉡: 아웃바운드
③ ㉠: 리버스 텔넷
㉡: 인바운드
④ ㉠: 원격 데스크톱 프로토콜 공격
㉡: 인바운드

정답 1번

출제 포인트

이 문제는 방화벽의 아웃바운드 허용 정책을 악용하는 리버스 텔넷의 동작 방향을 묻는 문제이다.

핵심 개념

리버스 텔넷: 외부 공격자가 내부 서버에 직접 접속하는 대신, 내부 서버가 공격자의 컴퓨터로 역접속하게 만들어 방화벽 정책을 우회하는 공격 방식이다.
아웃바운드 패킷: 내부 네트워크에서 외부 네트워크로 나가는 패킷이다.
인바운드 패킷: 외부 네트워크에서 내부 네트워크로 들어오는 패킷이다.
핵심 대비는 외부에서 내부로 직접 들어오면 인바운드이고, 내부 서버가 외부 공격자에게 접속하면 아웃바운드라는 점이다.

NoteBase

선지별 해설

① O — 리버스 텔넷은 내부 서버가 공격자의 컴퓨터로 역접속하게 하며, 방화벽이 아웃바운드 패킷을 엄격히 차단하지 않는 허점을 이용한다. 따라서 ㉠은 리버스 텔넷, ㉡은 아웃바운드가 맞다.
② X — 틀린 표현은 ㉠의 '원격 데스크톱 프로토콜 공격'이다. 원격 데스크톱 프로토콜 공격은 RDP 서비스의 취약한 인증이나 취약점을 노리는 공격을 뜻하며, 제시문의 역접속 방식은 리버스 텔넷이다. 올바르게는 '㉠ 리버스 텔넷, ㉡ 아웃바운드'이다.
③ X — 틀린 표현은 ㉡의 '인바운드'이다. 제시문에서는 내부 서버가 외부의 공격자 컴퓨터로 접속하므로 패킷 방향은 아웃바운드이다. 올바르게는 '㉠ 리버스 텔넷, ㉡ 아웃바운드'이다.
④ X — ㉠의 '원격 데스크톱 프로토콜 공격'과 ㉡의 '인바운드'가 모두 틀렸다. 제시문은 내부 서버가 외부 공격자에게 역접속하는 리버스 텔넷이며, 이때 이용되는 방향은 아웃바운드이다. 올바르게는 '㉠ 리버스 텔넷, ㉡ 아웃바운드'이다.

오답 포인트

'서버에 침투하는 공격'이라는 인상만으로 인바운드를 고르기 쉽다. 그러나 패킷 방향은 공격자의 위치가 아니라 실제 접속을 시작한 쪽을 기준으로 판단한다. 제시문처럼 내부 서버가 외부 공격자에게 접속하면 아웃바운드이다.

다시 나오면 이렇게 판단

접속을 누가 시작하고 패킷이 어느 방향으로 이동하는지를 먼저 확인한다. 외부 공격자에서 내부 서버로 직접 접속하면 인바운드이고, 내부 서버가 외부 공격자에게 역접속하면 리버스 방식이면서 아웃바운드이다.

암기 포인트

리버스 텔넷은 서버가 공격자에게 거꾸로 접속하며, 그 방향은 아웃바운드이다.

NoteBase