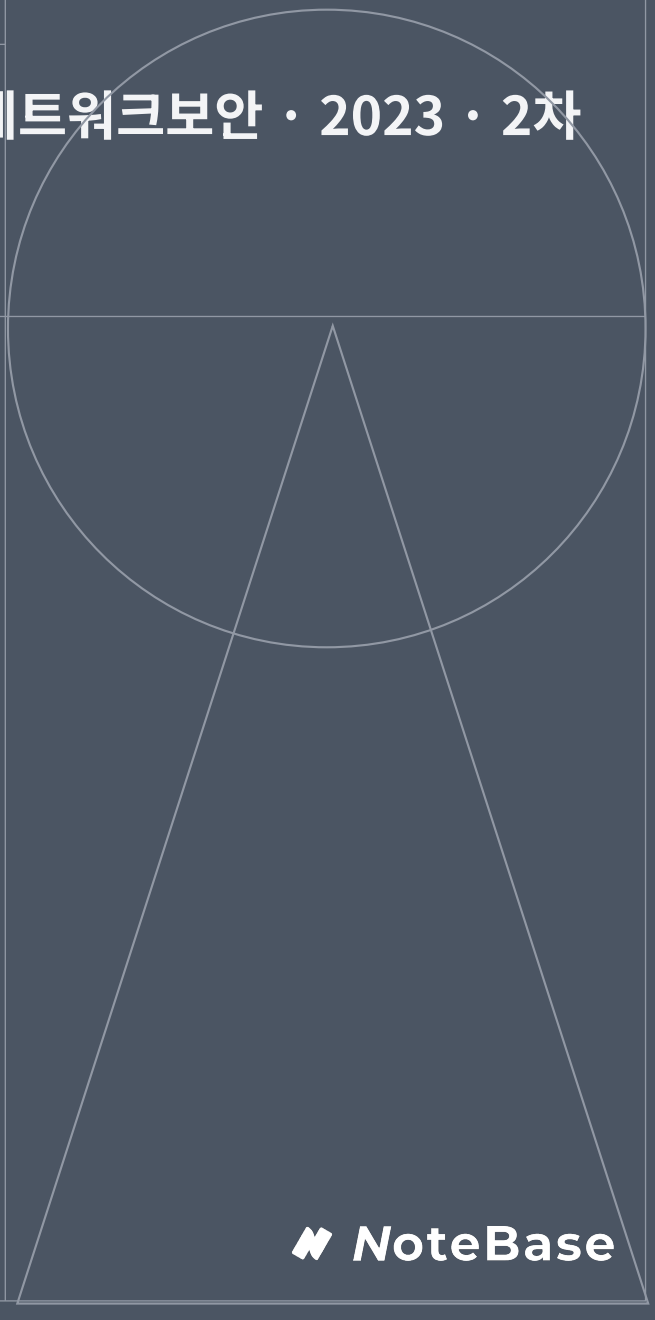
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2023 · 2차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2023 · 2차

공무원/해경/일반직 9급 · 네트워크보안 · 2023 · 2차

문 1. 다음 중 무선 AP(Access Point)에 전송데이터의 암호화 방식이나 인증절차가 설정되지 않은 경우 보안 강화책이 아닌 것은?

① WEP(Wired Equivalent Privacy) 설정한다.

② WAP2(Wi-Fi Protected Access v2) 설정한다.

③ Rogue AP로 대체한다.

④ 무선 AP에 SSID값을 'NULL'로 설정한다.

정답 3번

출제 포인트

암호화와 인증이 설정되지 않은 무선 AP의 보안을 강화하는 조치와, 오히려 새로운 위협을 만드는 행위를 구별하는 문제이다.

핵심 개념

무선 AP 보안 강화는 전송 데이터의 기밀성을 보호하는 암호화, 접속자를 확인하는 인증, 네트워크 노출을 줄이는 설정 등을 적용하는 것이다. Rogue AP는 관리자의 승인 없이 설치되거나 공격자가 정상 AP처럼 위장한 비인가 AP로, 보안 대책이 아니라 침입·도청·피싱의 통로가 된다.

NoteBase

선지별 해설

① O

WEP를 설정하면 암호화가 전혀 없는 상태보다는 전송 데이터 보호 기능이 추가되므로 문항의 맥락에서는 보안 강화 조치에 해당한다. 다만 WEP는 취약점이 알려진 오래된 방식이므로 실제 환경에서는 WPA2 또는 WPA3를 사용해야 한다.

② O

선지의 ‘WAP2’는 문맥상 ‘WPA2’를 뜻한다. WPA2는 무선 통신의 암호화와 인증 기능을 제공하므로 보안 강화 조치에 해당한다. 올바른 표기는 WPA2(Wi-Fi Protected Access 2)이다.

③ X

틀린 부분은 ‘Rogue AP로 대체한다’이다. Rogue AP는 신뢰할 수 없는 비인가 AP이므로 정상 AP를 이것으로 대체하면 보안이 강화되는 것이 아니라 공격자가 통신을 가로채거나 사용자를 위조 네트워크로 유도할 위험이 커진다. 올바르게는 Rogue AP를 탐지·차단하고, 인증 및 강한 암호화가 설정된 정상 AP를 사용해야 한다.

④ O

SSID 값을 NULL로 설정하여 네트워크 이름의 노출을 줄이는 것은 이 문항에서 제시한 보안 강화 조치이다. 다만 SSID 은닉만으로는 암호화나 인증을 대신할 수 없으므로 WPA2·WPA3 같은 보안 설정과 함께 사용해야 한다.

오답 포인트

①의 WEP와 ④의 SSID 은닉은 현재 기준으로 강력한 보안 수단은 아니지만, ③의 Rogue AP처럼 그 자체가 비인가 접속점이라는 위협 요소는 아니다. 이 문항은 ‘가장 좋은 보안 방식’을 묻는 것이 아니라 ‘보안 강화책이 아닌 것’을 묻는다.

다시 나오면 이렇게 판단

각 조치가 암호화·인증·노출 감소처럼 방어 기능을 추가하는지, 아니면 비인가 장비나 위장 접속점처럼 공격 경로를 만드는지를 구분한다. Rogue AP의 설치나 대체는 언제나 강화책이 아니라 탐지·차단 대상이다.

암기 포인트

WPA2·WPA3는 보호 설정, Rogue AP는 탐지·차단 대상이다.

NoteBase

문 2. 다음 중 무선 LAN보안에 AES 128비트를 사용하여 최상의 암호수준을 제공하는 것은?

① WEP(Wired Equivalent Privacy)

② EAP(Extensible Authentication Protocol)

③ WPA2(Wi-Fi Protected Access v2)

④ WPA(Wi-Fi Protected Access)

정답 3번

출제 포인트

무선 LAN 보안 방식별 역할과 암호화 알고리즘을 구분하고, AES 128비트를 사용하는 방식을 찾는 문제이다.

핵심 개념

WEP는 RC4 기반의 초기 무선 LAN 보안 방식이고, WPA는 WEP의 취약점을 보완하기 위해 TKIP와 RC4를 사용하는 과도기적 방식이다. WPA2는 AES 기반의 CCMP를 채택하여 이들보다 강한 기밀성과 무결성을 제공한다. EAP는 특정 암호 알고리즘이 아니라 인증 방법을 운반하고 협상하기 위한 인증 프레임워크이다.

선지별 해설

① X — WEP는 AES 128비트를 사용하는 방식이 아니라 RC4 스트림 암호를 사용하는 초기 보안 방식이다. 올바르게는 'WEP는 RC4 기반이며 보안 취약성이 크다'이다.
② X — EAP는 AES 128비트 암호화를 제공하는 무선 LAN 암호 방식이 아니라 여러 인증 방식을 지원하는 인증 프레임워크이다. 올바르게는 'EAP는 사용자·단말 인증을 위한 확장 가능한 인증 프로토콜 체계이다'이다.
③ O — WPA2는 AES 128비트 기반의 CCMP를 사용하여 보기 중 가장 높은 암호 수준을 제공한다.
④ X — WPA는 주로 TKIP와 RC4를 사용하므로 AES 128비트 기반의 최상 암호 수준에 해당하지 않는다. 올바르게는 'WPA는 TKIP·RC4 기반의 과도기적 보안 방식이고, AES·CCMP 기반 방식은 WPA2이다'이다.

오답 포인트

EAP를 암호화 방식으로 오해하거나 WPA와 WPA2를 같은 수준으로 보는 것이 함정이다. 이 문제에서는 인증 체계인 EAP와 암호화 방식인 WEP·WPA·WPA2를 먼저 구분해야 한다.

다시 나오면 이렇게 판단

'AES 128비트' 또는 'CCMP'가 제시되면 WPA2를, 'TKIP·RC4'가 제시되면 WPA를, '초기 방식·RC4·취약성'이 제시되면 WEP를 연결한다. EAP는 암호화 알고리즘이 아니라 인증 프레임워크로 판단한다.

NoteBase

암기 포인트

WEP는 RC4, WPA는 TKIP·RC4, WPA2는 AES·CCMP, EAP는 인증이다.

NoteBase

문 3. 다음 중 기기 인증기술 중에서 보안수준은 하위수준이지만, 접속이 가장 용이하고, 추가적인 프로토콜이 필요치 않고, 접속지연이 최소인 것은?

① ID/PW기반 인증기술

② MAC(Media Access Control)주소 인증기술

③ Challenge/Response 인증기술

④ PKI(Public Key Infrastructure)기반 기기 인증서를 활용한 인증기술

정답 2번

출제 포인트

기기 인증 방식별로 보안수준, 인증 절차의 복잡성, 접속 편의성, 접속지연을 비교하는 문제이다.

핵심 개념

MAC 주소 인증은 단말의 네트워크 인터페이스에 설정된 MAC 주소를 식별값으로 사용한다. 별도의 사용자 입력이나 복잡한 인증 교환 없이 접속을 허용할 수 있어 간편하고 지연이 작지만, MAC 주소를 알아내거나 위조할 수 있으므로 보안수준은 낮다.
ID/PW 인증은 사용자가 자격증명을 제시하고 서버가 이를 확인하는 방식이다. Challenge/Response 인증은 서버가 보낸 임의의 도전값에 대해 단말이 비밀정보를 이용한 응답값을 생성하는 방식이며, PKI 기반 인증은 공개키 인증서와 개인키를 이용해 기기의 신원을 검증하는 방식이다.

NoteBase

선지별 해설

① X
ID/PW 기반 인증은 자격증명의 입력·전송·검증 절차가 필요하므로, 별도의 인증 절차 없이 접속지연이 최소인 방식에 해당하지 않는다. 틀린 부분은 이 방식이 문제의 모든 조건을 충족한다고 보는 것이다. 올바르게는 사용자 인증정보를 확인하는 기본 인증 방식이라고 해야 한다.

② O
MAC 주소 인증은 접속 과정에서 확인 가능한 MAC 주소를 등록 목록과 대조하므로 접속이 간편하고 추가적인 복잡한 인증 프로토콜이 필요하지 않아 지연이 작다. 다만 MAC 주소는 노출되거나 위조될 수 있어 보안수준이 낮다.

③ X
Challenge/Response 인증은 도전값 전달, 응답값 계산, 응답 검증의 추가 교환이 필요하므로 접속지연이 최소인 방식이 아니다. 틀린 부분은 '추가적인 프로토콜이 필요치 않고, 접속지연이 최소'라는 조건과의 결합이다. 올바르게는 재전송 공격에 대한 저항성을 높이는 대신 추가 인증 절차가 필요한 방식이라고 해야 한다.

④ X
PKI 기반 기기 인증은 인증서와 개인키를 이용해 신원을 강하게 검증하지만, 인증서 검증과 암호 연산 등의 절차가 필요하므로 보안수준이 하위이고 접속지연이 최소인 방식이 아니다. 틀린 부분은 '보안수준은 하위수준'이라는 조건과의 결합이다. 올바르게는 높은 보안성을 제공하는 대신 구축·운영과 인증 처리의 부담이 상대적으로 큰 방식이라고 해야 한다.

오답 포인트

'접속이 용이하다'는 표현만 보고 익숙한 ID/PW 방식을 고르기 쉽다. 그러나 이 문항의 결정적 단서는 낮은 보안수준, 추가 프로토콜 불필요, 최소 접속지연이 동시에 제시되었다는 점이며, 이는 주소 대조만으로 허용하는 MAC 주소 인증에 해당한다.

다시 나오면 이렇게 판단

인증 방식 비교에서는 먼저 추가 메시지 교환과 암호 연산의 유무를 확인한다. 단순 식별자 대조는 빠르고 편하지만 위조에 취약하고, Challenge/Response나 PKI처럼 암호학적 검증을 수행하는 방식은 보안성이 높아지는 대신 절차와 처리 부담이 늘어난다.

암기 포인트

MAC 주소 인증은 빠르고 간편하지만 위조에 취약하고, Challenge/Response와 PKI는 절차가 늘어나는 대신 보안성이 높다.

NoteBase

문 4. 다음은 무선 AP(Access Point)가 태생적으로 보안에 취약하기 때문에 신규로 설치 시 고려할 사항을 나열한 것이다. 틀린 것은?

① AP 기본계정의 패스워드를 재설정한다.

② 누구나 접근이 가능한 장소에 설치한다.

③ DHCP(Dynamic Host Configuration Protocol)에 의한 IP주소 할당을 중지한다.

④ AP에 접속이 가능한 무선 랜카드 MAC주소를 기록하여 이를 반영하여 접속을 통제한다.

정답 2번

출제 포인트

무선 AP를 신규 설치할 때 논리적 접근 통제뿐 아니라 장비 자체에 대한 물리적 접근도 제한해야 한다는 점을 묻는 문제이다.

핵심 개념

무선 AP 보안 강화는 기본 인증정보 변경, 불필요한 자동 주소 할당 제한, 허용 단말 통제와 같은 논리적 조치와 AP의 도난·변조·초기화 등을 막는 물리적 보호를 함께 적용하는 것이다.

선지별 해설

① O

AP의 출고 시 기본 계정과 패스워드는 널리 알려져 있거나 추측하기 쉬우므로, 설치 직후 기본 패스워드를 강한 패스워드로 변경하는 것은 적절하다.

② X

틀린 부분은 '누구나 접근이 가능한 장소'이다. 누구나 장비에 손댈 수 있으면 AP의 설정을 변경하거나 초기화하고 케이블을 조작할 수 있으므로, AP는 출입이 통제되고 물리적으로 보호되는 장소에 설치해야 한다.

③ O

DHCP에 의한 자동 IP 주소 할당을 중지하면 임의의 단말이 접속 후 곧바로 네트워크 설정을 받는 것을 제한할 수 있다. 이는 단독 보안 수단은 아니지만, 허가된 단말에 고정된 네트워크 설정을 부여하는 방식과 함께 사용할 수 있는 강화 조치이다.

④ O

허용할 무선 랜카드의 MAC 주소를 등록하고 그 목록을 기준으로 접속을 통제하는 MAC 필터링은 미등록 단말의 접속을 제한하는 방법이다. 다만 MAC 주소는 위조될 수 있으므로 암호화와 강한 인증을 함께 적용해야 한다.

NoteBase

오답 포인트

AP를 개방된 곳에 두면 전파 전달이나 관리가 편리해 보일 수 있지만, 이 문항은 설치 편의가 아니라 보안을 묻는다. ②의 '누구나 접근이 가능한'이라는 표현은 물리적 보안 원칙과 정반대이다.

다시 나오면 이렇게 판단

AP 보안 선지는 계정·주소 할당·단말 허용 같은 논리적 통제와 출입·장비 보호 같은 물리적 통제로 나누어 판단한다. 접근이나 설정 변경을 불특정 다수에게 허용하는 내용은 보안 강화 조치가 아니다.

암기 포인트

기본 비밀번호는 변경하고, 자동 접속은 제한하며, 허용 단말만 접속시키고, AP 장비는 물리적으로 보호한다.

NoteBase

문 5. 다음 중 응용계층에서 동작되는 보안프로토콜이 아닌 것은?

① S/MIME(Secure/Multipurpose Internet Mail Extensions)

② SSH(Secure SHell)

③ SSL(Secure Socket Layer)

④ S-HTTP(Secure Hyper Text Transper Protocol)

정답 3번

출제 포인트

전자우편·원격 접속·웹처럼 특정 응용 서비스에 적용되는 보안 프로토콜과, TCP 위에서 응용 데이터의 보안 통신 경로를 제공하는 프로토콜을 구분하는 문제이다.

핵심 개념

응용계층 보안 프로토콜은 전자우편, 원격 접속, 웹 등 특정 응용 서비스의 메시지나 기능을 보호한다. S/MIME은 전자우편, SSH는 원격 접속, S-HTTP는 HTTP 통신을 보호하는 응용계층 프로토콜이다. 반면 SSL은 TCP와 응용계층 프로토콜 사이에서 암호화·무결성·서버 인증 등을 제공하는 보안 프로토콜로, 이 문항의 계층 분류에서는 응용계층 보안 프로토콜에 해당하지 않는다.

선지별 해설

① O — S/MIME은 MIME 형식의 전자우편에 전자서명과 암호화 기능을 제공하므로 응용계층의 전자우편 보안 프로토콜이다.
② O — SSH는 원격 로그인과 명령 실행, 파일 전송 등을 안전하게 제공하는 응용계층 프로토콜이다.
③ X — SSL은 특정 응용 서비스 자체의 프로토콜이 아니라 TCP 위에서 응용 프로토콜에 보안 채널을 제공한다. 따라서 '응용계층에서 동작되는 보안 프로토콜'이라는 분류가 틀렸으며, 올바르게는 전송계층과 응용계층 사이에서 보안 기능을 제공하는 프로토콜로 분류한다.
④ O — S-HTTP는 HTTP 메시지의 보안을 목적으로 설계된 응용계층 보안 프로토콜이다. 선지의 'Secure Hyper Text Transper Protocol'은 철자가 잘못된 표기이며, 올바른 명칭은 'Secure Hypertext Transfer Protocol'이다.

오답 포인트

SSL이 웹 브라우저와 웹 서버의 통신에 널리 쓰이므로 웹 응용계층 프로토콜로 착각하기 쉽다. 그러나 SSL은 HTTP에만 종속되지 않고 TCP를 사용하는 여러 응용 프로토콜 아래에서 공통 보안 채널을 제공한다는 점이 핵심이다.

NoteBase

다시 나오면 이렇게 판단

프로토콜이 전자우편·원격 접속·HTTP처럼 특정 응용 서비스를 직접 보호하는지, 아니면 TCP 위에서 여러 응용 프로토콜에 공통 보안 통로를 제공하는지를 기준으로 구분한다. 전자는 응용계층 보안 프로토콜이고, 후자의 대표가 SSL이다.

암기 포인트

S/MIME은 메일, SSH는 원격 접속, S-HTTP는 HTTP, SSL은 TCP 위의 공통 보안 채널이다.

NoteBase

문 6. VPN(Virtual Private Network)은 인터넷에 보안채널(Secure Channel)을 만들어 공용인터넷을 사설망처럼 사용하는 기술이다. 통신프로토콜 3계층(네트워크계층)에 보안프로토콜을 추가하여 VPN을 구현하는 기술은?

① IPSec(Internet Protocol Security)

② SSL(Secure Socket Layer)

③ DNSsec(DNS Security)

④ S-HTTP(Secure Hyper Text Transper Protocol)

정답 1번

출제 포인트

VPN 보안 기술이 동작하는 계층과 보호 대상을 구분하는 문제이다. 네트워크 계층에서 IP 패킷 자체를 보호하는 기술은 IPSec이다.

핵심 개념

IPSec: IP 패킷에 인증·무결성 및 기밀성 보호를 제공하는 네트워크 계층 보안 프로토콜 모음이다. 터널 모드를 이용해 VPN을 구현할 수 있다.
SSL: TCP를 이용하는 응용 프로토콜에 보안 통신 기능을 제공하는 기술로, IP 패킷 자체를 네트워크 계층에서 보호하는 방식은 아니다.
DNSSEC: 전자서명을 통해 DNS 응답 데이터의 출처 인증과 무결성을 검증하는 기술이다.
S-HTTP: 개별 HTTP 메시지를 보호하는 응용 계층 방식이다.

선지별 해설

① O — IPSec은 네트워크 계층에서 IP 패킷을 보호하며, 터널 모드로 VPN의 보안 터널을 구성할 수 있다.
② X — 틀린 부분은 SSL을 네트워크 계층 VPN 구현 기술로 본 점이다. SSL은 TCP 위에서 응용 통신을 보호하며, 올바르게는 네트워크 계층에서 VPN을 구현하는 기술이 IPSec이다.
③ X — 틀린 부분은 DNSsec을 VPN용 보안채널 기술로 본 점이다. DNSSEC은 DNS 데이터의 출처 인증과 무결성을 전자서명으로 검증하며, 올바르게는 IP 패킷 기반 VPN 보안채널에는 IPSec을 사용한다.
④ X — 틀린 부분은 S-HTTP를 네트워크 계층 보안프로토콜로 본 점이다. S-HTTP는 개별 HTTP 메시지를 보호하는 응용 계층 방식이며, 올바르게는 네트워크 계층에서 IP 패킷을 보호하는 기술이 IPSec이다.

오답 포인트

②의 SSL도 보안 통신과 VPN에 활용될 수 있어 혼동하기 쉽다. 그러나 이 문항의 결정어는 '3계층(네트워크계층)'이며, 계층 기준으로 보면 IPSec이 정답이다. DNSSEC은 DNS 데이터 검증, S-HTTP는 HTTP 메시지 보호가 목적이다.

NoteBase

다시 나오면 이렇게 판단

문제에서 보호 대상과 동작 계층을 먼저 확인한다. IP 패킷·네트워크 계층·터널 모드가 제시되면 IPSec, DNS 응답의 서명 검증이면 DNSSEC, HTTP 메시지 보호이면 S-HTTP로 판단한다.

암기 포인트

IP 계층 VPN은 IPSec, DNS 서명 검증은 DNSSEC, HTTP 메시지 보호는 S-HTTP이다.

NoteBase

문 7. 다음 중 산재되어 있는 수많은 컴퓨터를 동원하여 동일 시간에 특정 컴퓨터에 트래픽 폭탄을 보내어 특정 컴퓨터가 정상적인 작동을 못하게 하는 공격은?

① APT(Advanced Persistence Threat) 공격
② DOS(Denial Of Service) 공격
③ IP Spoofing 공격
④ DDOS(Distributed Denial Of Service) 공격

정답 4번

출제 포인트

다수의 분산된 컴퓨터가 동시에 한 대상을 공격한다는 단서로 DoS와 DDoS를 구별하는 문제이다.

핵심 개념

DDoS(Distributed Denial of Service)는 여러 공격원에서 동시에 대량의 트래픽이나 요청을 보내 대상 시스템의 자원을 소진시키는 분산 서비스 거부 공격이다.
DoS는 대상의 서비스 가용성을 떨어뜨리는 공격이며, 시험에서는 한 공격원에 의한 DoS와 다수의 분산된 공격원에 의한 DDoS를 구별한다.
APT(Advanced Persistent Threat)는 특정 대상을 장기간 은밀하게 침투하는 지능형 지속 위협이고, IP 스푸핑은 패킷의 출발지 IP 주소를 위조하는 기법이다.

선지별 해설

① X - 틀린 표현은 'APT 공격'이다. APT는 특정 조직이나 시스템을 장기간 은밀하게 노리는 표적형 공격이며, 다수의 컴퓨터가 동시에 트래픽을 집중시키는 공격은 DDoS이다. 또한 APT의 정식 영문은 Advanced Persistent Threat이다.
② X - 틀린 표현은 'DOS 공격'이다. 일반적인 DoS는 한 공격원 또는 비분산 방식으로 대상의 서비스를 마비시키는 공격을 가리킨다. 문제처럼 산재한 다수의 컴퓨터를 동시에 동원하는 경우에는 DDoS 공격이라고 해야 한다.
③ X - 틀린 표현은 'IP Spoofing 공격'이다. IP 스푸핑은 패킷의 출발지 IP 주소를 다른 주소로 위조하는 기법이다. 다수의 공격원이 트래픽을 집중시켜 서비스를 마비시키는 공격은 DDoS이다.
④ O - DDoS 공격은 악성코드에 감염된 다수의 컴퓨터 등 분산된 공격원을 동원하여 특정 시스템에 트래픽이나 요청을 동시에 집중시키고 정상적인 서비스 제공을 방해한다. 문제의 설명과 일치한다.

오답 포인트

서비스를 마비시킨다는 결과만 보면 DoS를 고르기 쉽다. 그러나 '산재되어 있는 수많은 컴퓨터'와 '동일 시간'이 핵심 단서이므로 분산형인 DDoS로 판단한다.

NoteBase

다시 나오면 이렇게 판단

공격원의 수와 분산 여부를 먼저 확인한다. 한 공격원 중심의 서비스 마비는 DoS, 여러 지역의 다수 공격원이 동시에 트래픽을 집중시키는 서비스 마비는 DDoS이다. 출발지 주소 위조가 핵심이면 IP 스푸핑, 장기간의 은밀한 표적 침투가 핵심이면 APT이다.

암기 포인트

다수·분산·동시 트래픽 폭탄은 DDoS이다.

NoteBase

문 8. 다음 <보기>의 설명과 가장 가까운 장비는?

<보기>
방화벽과 침입탐지시스템의 장점만을 결합하여 실시간 방어체제를 구축한 장비이다. 이 장비는 실시간으로 네트워크 트래픽을 모니터링하여 분석하고 해킹으로 판단되면 패킷이 내부로 유입되는 것을 사전에 차단한다.

① DDOS(Distributed Denial Of Services) 보안장비

② VPN(Virtual Private Network) 보안장비

③ IPS(Intrusion Prevention System) 보안장비

④ NAC(Network Access Control) 보안장비

정답 3번

출제 포인트

침입을 탐지하는 데 그치지 않고 악성 패킷을 실시간으로 차단하는 보안장비가 IPS임을 구별하는 문제이다.

핵심 개념

IPS는 네트워크 트래픽을 실시간으로 탐지·분석하고, 공격으로 판단된 패킷을 능동적으로 차단하는 침입방지시스템이다.
DDoS 보안장비는 대량의 비정상 트래픽으로 서비스를 마비시키는 분산 서비스 거부 공격을 탐지·완화한다.
VPN 장비는 암호화된 가상 통신 경로를 만들어 원격지 간 통신의 기밀성과 안전성을 확보한다.
NAC 장비는 단말의 사용자·보안 상태를 확인하여 네트워크 접속 허용 여부와 접근 범위를 통제한다.

선지별 해설

① X — DDoS 보안장비는 분산된 다수의 공격원에서 유입되는 대량 트래픽을 탐지하고 완화하는 데 특화된다. 틀린 부분은 장비를 'DDoS 보안장비'로 본 것이며, 보기의 '침입 탐지 후 패킷의 내부 유입을 사전에 차단'하는 장비는 IPS이다.
② X — VPN 보안장비는 공중망에서 암호화 터널을 구성하여 안전한 통신을 제공한다. 틀린 부분은 장비를 'VPN 보안장비'로 본 것이며, 보기처럼 공격 패킷을 탐지하여 차단하는 장비는 IPS이다.
③ O — IPS는 트래픽을 실시간으로 모니터링·분석하고 침입 또는 공격으로 판단된 패킷을 능동적으로 차단한다. 보기의 '방화벽과 침입탐지시스템의 장점 결합', '실시간 분석', '사전 차단'에 모두 부합한다.
④ X — NAC 보안장비는 사용자와 단말의 인증 및 보안 상태를 점검하여 네트워크 접속을 통제한다. 틀린 부분은 장비를 'NAC 보안장비'로 본 것이며, 이미 흐르는 트래픽에서 공격 패킷을 탐지·차단하는 보기의 장비는 IPS이다.

NoteBase

오답 포인트

DDoS 장비와 NAC도 유해한 트래픽이나 단말을 차단할 수 있어 혼동하기 쉽다. 그러나 보기의 결정적 표현은 ‘침입을 실시간으로 탐지·분석한 뒤 공격 패킷의 내부 유입을 사전에 차단’한다는 것이다. 이는 IDS의 탐지 기능에 능동적 차단 기능을 더한 IPS의 특징이다.

다시 나오면 이렇게 판단

탐지 후 공격 패킷을 즉시 차단하면 IPS, 암호화 터널이면 VPN, 대량 서비스 거부 트래픽 완화이면 DDoS 보안장비, 접속 단말의 인증·보안 상태에 따른 접근 통제이면 NAC로 판단한다.

암기 포인트

IPS는 침입을 탐지하고 막으며, VPN은 통신을 암호화하고, NAC는 접속을 통제한다.

NoteBase

문 9. 다음 중 방화벽으로 할 수 있는 것은?

① 악성코드 침입 차단

② 내부자 공격 차단

③ 방화벽을 우회하는 트래픽 차단

④ 외부자의 내부 네트워크에 대한 접근통제

정답 4번

출제 포인트

이 문제는 방화벽의 기본 기능과 방화벽만으로 막기 어려운 위협을 구분하는 문제이다.

핵심 개념

방화벽은 내부 네트워크와 외부 네트워크의 경계에서 통과하는 트래픽을 보안 정책에 따라 허용하거나 차단하는 접근통제 장치이다. 핵심 판단 기준은 해당 통신이 방화벽을 통과하는지, 그리고 설정된 규칙으로 통제할 수 있는지이다.

선지별 해설

① X — '악성코드 침입 차단'은 일반적인 방화벽의 기본 기능만으로 보장할 수 없다. 방화벽은 주소·포트·프로토콜 등의 규칙으로 통신을 통제하지만, 허용된 통신에 포함된 악성코드까지 반드시 식별하는 것은 아니다. 올바르게는 악성코드 탐지·차단에는 백신, 침입방지시스템 등 별도의 보안 기능이 필요하다.
② X — '내부자 공격 차단'은 방화벽의 기본 기능으로 보기 어렵다. 내부에서 발생하여 경계 방화벽을 통과하지 않는 공격은 방화벽이 관찰하거나 통제할 수 없다. 올바르게는 내부자 공격에는 내부망 접근통제, 권한 관리, 행위 감시 등의 대책이 필요하다.
③ X — '방화벽을 우회하는 트래픽 차단'은 불가능하다. 방화벽을 거치지 않는 통신은 방화벽의 검사 대상에 들어오지 않기 때문이다. 올바르게는 모든 외부 연결 경로가 방화벽을 통과하도록 네트워크를 구성해야 방화벽 정책으로 차단할 수 있다.
④ O — 외부자가 내부 네트워크에 접근하려는 트래픽이 방화벽을 통과하면, 방화벽은 설정된 보안 정책에 따라 해당 접근을 허용하거나 차단할 수 있다. 이는 방화벽의 대표적인 접근통제 기능이다.

오답 포인트

①의 '악성코드', ②의 '내부자', ③의 '우회'는 모두 방화벽의 통제 범위를 벗어날 수 있다는 점이 함정이다. 방화벽은 모든 보안 위협을 막는 장치가 아니라 자신을 통과하는 경계 트래픽을 정책에 따라 통제하는 장치이다.

NoteBase

다시 나오면 이렇게 판단

먼저 트래픽이 방화벽을 통과하는지 확인하고, 다음으로 주소·포트·프로토콜 등 방화벽 정책으로 허용과 차단을 결정할 수 있는지 판단한다. 방화벽을 거치지 않는 내부 공격이나 우회 통신은 기본 방화벽의 통제 대상으로 보지 않는다.

암기 포인트

방화벽은 경계를 통과하는 트래픽의 문지기이며, 내부 공격과 우회 트래픽까지 자동으로 막는 만능 장치는 아니다.

NoteBase

문 10. 다음 중 공격 대상시스템의 로그에 흔적을 남기지 않은 포트 스캔 기술은?

① ICMP Scan

② UDP Scan

③ TCP Scan

④ Stealth Scan

정답 4번

출제 포인트

포트 스캔 방식별 목적과 연결 처리 방식의 차이를 바탕으로, 대상 시스템의 일반적인 연결 로그에 흔적을 최소화하도록 설계된 스캔을 구별하는 문제이다.

핵심 개념

Stealth Scan은 정상적인 TCP 연결을 끝까지 완성하지 않거나 비정상적인 플래그 조합을 이용하여 스캔 사실이 일반적인 연결 로그에 남을 가능성을 줄이는 포트 스캔 기법이다. 대표적으로 TCP SYN 스캔, FIN 스캔, NULL 스캔, Xmas 스캔 등이 이에 해당한다.
ICMP Scan은 호스트의 동작 여부를 확인하고, UDP Scan은 UDP 포트의 상태를 조사하며, 일반적인 TCP Connect Scan은 TCP 3-way handshake를 완성하므로 연결 기록이 남기 쉽다.

선지별 해설

① X — ICMP Scan은 ICMP Echo 요청·응답 등을 이용해 대상 호스트가 활성 상태인지 확인하는 기법이다. 포트 연결 로그를 피하기 위한 스텔스 포트 스캔을 뜻하지 않는다. 틀린 선택이며, 올바른 답은 Stealth Scan이다.
② X — UDP Scan은 UDP 데이터그램을 보내고 ICMP Port Unreachable 응답의 유무 등을 이용해 UDP 포트 상태를 판단한다. 로그 흔적을 최소화하는 방식 자체를 가리키는 명칭이 아니다. 틀린 선택이며, 올바른 답은 Stealth Scan이다.
③ X — 일반적인 TCP Connect Scan은 TCP 3-way handshake를 완성해 실제 연결을 성립시키므로 대상 시스템의 연결 로그에 기록되기 쉽다. 흔적을 줄이려면 연결을 완성하지 않는 TCP SYN 방식 등의 Stealth Scan을 사용한다.
④ O — Stealth Scan은 완전한 TCP 연결을 만들지 않거나 특수한 TCP 플래그를 사용해 대상 시스템의 일반적인 로그에 스캔 흔적이 남는 것을 줄이도록 설계된 기법이다. 따라서 문제의 설명에 해당한다.

NoteBase

오답 포인트

③의 TCP Scan과 ④의 Stealth Scan을 완전히 별개의 계층으로 생각하면 혼동하기 쉽다. Stealth Scan에는 TCP SYN 스캔처럼 TCP를 이용하는 방식도 있지만, 핵심은 TCP 사용 여부가 아니라 정상 연결을 끝까지 완성하여 로그를 남기기 쉬운지 여부이다.

다시 나오면 이렇게 판단

호스트 생존 확인이면 ICMP, UDP 포트 확인이면 UDP, 정상 TCP 연결 완성이면 TCP Connect, 연결을 완성하지 않거나 특수 플래그로 탐지를 줄이면 Stealth Scan으로 판단한다.

암기 포인트

Stealth는 완전한 연결을 피하여 흔적을 줄이고, TCP Connect는 연결을 완성하여 흔적이 남기 쉽다.

NoteBase

문 11. 다음 중 공격자가 공격대상자에게 자신을 노출시키지 않고 제3의 사용자인 것처럼 MAC주소, IP주소, E-Mail 주소, DNS 이름 등을 속여서 공격하는 것을 통칭하여 무엇이라 하는가?

① 스니핑(Sniffing) 공격
② 스푸핑(Spoofing) 공격
③ 하이재킹(Hijacking) 공격
④ 인터셉트(Intercept) 공격

정답 2번

출제 포인트

MAC 주소, IP 주소, E-Mail 주소, DNS 이름 등 식별 정보를 위조하여 다른 사용자나 시스템인 것처럼 가장하는 공격의 명칭을 묻는 문제이다.

핵심 개념

스푸핑은 통신 주체의 식별 정보를 위조하여 신뢰할 수 있는 대상인 것처럼 가장하는 공격이다. 스니핑은 통신 내용을 몰래 엿보는 공격이고, 하이재킹은 이미 성립된 세션이나 연결의 제어권을 탈취하는 공격이다.
인터셉트는 전송 중인 정보를 가로채는 행위를 뜻하며, 여러 식별 정보를 속이는 공격의 통칭은 스푸핑이다.

선지별 해설

① X — 스니핑은 네트워크 패킷이나 통신 내용을 몰래 수집·도청하는 공격이다. 틀린 표현은 '스니핑 공격'이며, 식별 정보를 위조하여 제3자인 것처럼 가장하는 공격은 '스푸핑 공격'이다.
② O — 스푸핑은 MAC 주소, IP 주소, E-Mail 주소, DNS 이름 등의 정보를 위조하여 다른 사용자나 시스템으로 가장하는 공격을 통칭한다.
③ X — 하이재킹은 정상적으로 형성된 세션이나 연결을 가로채 그 제어권을 탈취하는 공격이다. 틀린 표현은 '하이재킹 공격'이며, 주소나 이름을 속여 신원을 가장하는 공격은 '스푸핑 공격'이다.
④ X — 인터셉트는 전송 중인 통신이나 정보를 중간에서 가로채는 행위에 초점이 있다. 틀린 표현은 '인터셉트 공격'이며, MAC·IP·E-Mail·DNS 등의 식별 정보를 위조하는 공격의 통칭은 '스푸핑 공격'이다.

오답 포인트

'노출시키지 않고'와 '가로챈다'는 인상 때문에 스니핑·하이재킹·인터셉트를 고르기 쉽다. 그러나 이 문항의 결정적 표현은 '주소와 이름 등을 속여서 제3의 사용자인 것처럼 가장한다'는 부분이다.

다시 나오면 이렇게 판단

식별 정보 위조·신원 가장이면 스푸핑, 통신 내용 엿보기이면 스니핑, 성립된 세션의 제어권 탈취이면 하이재킹, 전송 중 정보 가로채기이면 인터셉트로 구분한다.

NoteBase

암기 포인트

스푸핑은 신원을 속이고, 스니핑은 내용을 엿보며, 하이재킹은 세션을 빼앗는다.

NoteBase

문 12. 다음 중 조직내 다수의 IT시스템과 보안시스템에서 발생하는 모든 로그들을 실시간으로 수집하여 종합적인 분석을 통해 이상징후를 파악하고 대응을 위해 마련한 장비는?

① SIEM(Security Information Event Management) 장비

② NAC(Network Access Control) 장비

③ MDM(Mobile Device Management) 장비

④ SAC(System Access Control) 장비

정답 1번

출제 포인트

여러 IT 시스템과 보안 장비의 로그를 실시간으로 통합 수집하고 상관분석하여 이상징후를 탐지·대응하는 SIEM의 기능을 묻는 문제이다.

핵심 개념

SIEM은 여러 정보시스템과 보안시스템에서 발생한 로그와 보안 이벤트를 중앙에서 수집·통합하고, 이들 사이의 연관성을 분석하여 침해 징후를 탐지하고 대응을 지원하는 체계이다. NAC는 네트워크 접속 통제, MDM은 모바일 기기 관리, SAC는 시스템 접속 통제가 중심이다.

선지별 해설

① O — SIEM 장비는 다수의 IT 시스템과 보안시스템에서 발생하는 로그를 실시간으로 통합 수집하고 상관분석하여 이상징후를 찾아내므로 문제의 설명에 해당한다.
② X — 틀린 부분은 NAC 장비를 로그 통합분석 장비로 본 것이다. NAC는 단말의 보안 상태나 사용자 정책 등을 확인하여 네트워크 접속을 허용·차단하는 장비이다.
③ X — 틀린 부분은 MDM 장비를 로그 통합분석 장비로 본 것이다. MDM은 스마트폰·태블릿 같은 모바일 기기의 설정, 보안 정책, 애플리케이션 및 원격 잠금·삭제 등을 중앙에서 관리하는 체계이다.
④ X — 틀린 부분은 SAC 장비를 로그 통합분석 장비로 본 것이다. SAC는 서버 등 개별 시스템에 대한 사용자 접속과 권한을 통제하는 장비이다.

오답 포인트

②~④도 모두 접근 또는 보안 관리 장비이지만, 문제의 핵심 표현은 '모든 로그의 실시간 수집'과 '종합적인 분석'이다. 이 두 기능은 접속 자체를 통제하는 NAC·SAC나 단말을 관리하는 MDM이 아니라 SIEM을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

‘여러 장비의 로그를 중앙 수집·상관분석하여 이상징후를 탐지한다’면 SIEM, ‘네트워크에 들어오는 단말을 검사·통제한다’면 NAC, ‘모바일 기기를 중앙 관리한다’면 MDM, ‘서버 등 시스템 접속과 권한을 통제한다’면 SAC로 판단한다.

암기 포인트

SIEM은 로그 통합분석, NAC는 네트워크 접속, MDM은 모바일 기기, SAC는 시스템 접속을 관리한다.

NoteBase

문 13. 리눅스 운영체제가 탑재된 컴퓨터에 랜카드를 설치한 다음, 리눅스운영체제를 통해서 랜카드를 'Promiscuous' 모드로 동작하도록 설정하였다. 설정 결과 랜카드 동작을 가장 잘 설명한 것은?

① 랜카드에 도착된 프레임내의 IP주소와 MAC주소가 랜카드가 장착된 컴퓨터의 IP주소와 MAC주소가 동일한 것만 컴퓨터로 받아들인다.

② 랜카드에 도착된 프레임내의 IP주소와 랜카드가 장착된 컴퓨터의 IP주소가 동일한 것만 컴퓨터로 받아들인다.

③ 랜카드에 도착된 프레임내의 MAC주소와 랜카드가 장착된 컴퓨터의 MAC주소가 동일한 것만 컴퓨터로 받아들인다.

④ 랜카드에 도착한 모든 프레임을 컴퓨터로 받아들인다.

정답 4번

출제 포인트

무차별 모드(promiscuous mode)로 설정된 랜카드가 목적지 주소에 따른 수신 필터링 없이 도착한 프레임을 운영체제에 전달한다는 점을 묻는 문제이다.

핵심 개념

일반 모드: 랜카드는 보통 자신의 MAC 주소로 온 프레임과 수신 대상인 브로드캐스트·멀티캐스트 프레임을 받아들인다.
무차별 모드: 랜카드는 목적지 MAC 주소가 자신의 주소인지와 관계없이 도착한 모든 프레임을 운영체제에 전달한다. 패킷 분석이나 네트워크 감시에 사용된다.

선지별 해설

① X — 'IP 주소와 MAC 주소가 모두 동일한 것만' 받아들인다는 부분이 틀렸다. 무차별 모드에서는 두 주소의 일치 여부로 프레임을 제한하지 않고, 랜카드에 도착한 모든 프레임을 운영체제에 전달한다.
② X — 'IP 주소가 동일한 것만' 받아들인다는 부분이 틀렸다. 랜카드의 기본 수신 필터링 기준은 프레임의 목적지 MAC 주소이며, 무차별 모드에서는 그 MAC 주소 필터링도 해제하여 도착한 모든 프레임을 전달한다.
③ X — 'MAC 주소가 동일한 것만' 받아들인다는 부분이 틀렸다. 이는 무차별 모드의 동작이 아니며, 올바르게는 목적지 MAC 주소가 자신의 주소와 달라도 도착한 프레임을 운영체제에 전달한다. 일반 모드도 자신의 MAC 주소와 일치하는 프레임뿐 아니라 브로드캐스트 및 수신 대상으로 설정된 멀티캐스트 프레임을 받을 수 있다.
④ O — 무차별 모드는 랜카드에 도착한 모든 프레임을 목적지 MAC 주소와 관계없이 운영체제에 전달하므로 가장 정확한 설명이다.

NoteBase

오답 포인트

③은 일반적인 랜카드의 MAC 주소 필터링과 무차별 모드를 뒤바꾼 함정이다. 또한 일반 모드도 브로드캐스트·멀티캐스트 프레임을 수신할 수 있으므로 '자신의 MAC 주소와 동일한 것만'이라는 표현은 엄밀하지 않다.

다시 나오면 이렇게 판단

promiscuous라는 말이 보이면 목적지 MAC 주소가 내 주소인지 검사해 걸러 내는 기능을 해제하고, 랜카드에 도착한 프레임을 운영체제에 넘기는 모드로 판단한다.

암기 포인트

무차별 모드는 '내 MAC만'이 아니라 '도착한 프레임 전부'이다.

NoteBase

문 14. 다음 중 사설 네트워크 용도로 사용되는 사설 IPv4 주소에 해당하는 것은?

① 10.10.20.300

② 168.10.40.11

③ 172.16.10.20

④ 192.10.20.30

정답 3번

출제 포인트

사설 IPv4 주소의 세 가지 예약 범위와 IPv4 주소의 유효 조건을 구분하는 문제이다.

핵심 개념

사설 IPv4 주소는 내부 네트워크에서 사용하도록 예약된 주소이다. 범위는 10.0.0.0~10.255.255.255, 172.16.0.0~172.31.255.255, 192.168.0.0~192.168.255.255이다. 또한 IPv4 주소의 각 옥텟은 0~255여야 한다.

선지별 해설

① X

10.10.20.300은 마지막 옥텟 300이 255를 초과하므로 유효한 IPv4 주소가 아니다. 틀린 부분은 '300'이며, 예를 들어 10.10.20.30이라면 10.0.0.0~10.255.255.255 범위의 사설 주소가 된다.

② X

168.10.40.11은 세 사설 주소 범위 어디에도 포함되지 않는다. 틀린 부분은 '168.10'이며, 사설 주소가 되려면 첫 옥텟이 10이거나, 앞부분이 172.16~172.31 또는 192.168이어야 한다.

③ O

172.16.10.20은 172.16.0.0~172.31.255.255 범위에 포함되므로 사설 IPv4 주소이다.

④ X

192.10.20.30은 192.168.0.0~192.168.255.255 범위에 포함되지 않는다. 틀린 부분은 '192.10'이며, 예를 들어 192.168.20.30이라면 사설 주소가 된다.

오답 포인트

①은 첫 옥텟이 10이라 사설 주소처럼 보이지만 300 때문에 주소 자체가 무효이다. ④는 192로 시작한다는 사실만 보고 고르기 쉽지만, 사설 범위는 192 전체가 아니라 192.168로 시작하는 범위이다.

NoteBase

다시 나오면 이렇게 판단

먼저 각 옥텟이 0~255인지 확인한 뒤, 유효한 주소가 10.*, 172.16~172.31.*, 192.168.* 중 하나에 포함되는지 판단한다.

암기 포인트

사설 IPv4의 시작 범위는 10, 172.16~31, 192.168이다.

NoteBase

문 15. 다음 중 조직내 네트워크에 기기/사용자 인증절차를 통해 네트워크에 접근을 통제하고, 네트워크에 접속되는 기기들의 백신관리 및 패치관리, 자산관리를 점검을 통해 무결성 유무에 따라 네트워크 접속 허용유무를 결정하고, 해킹, 웜 유해트래픽 탐지 및 차단하는 등의 기능을 하는 네트워크 보안장비는?

① SAC(System Access Control) 장비

② AAC(Account Access Control) 장비

③ NAC(Network Access Control) 장비

④ ESM(Enterprise Security Management) 장비

정답 3번

출제 포인트

기기·사용자의 네트워크 접속을 인증하고, 단말의 보안 상태를 점검하여 접속 허용 여부를 결정하는 NAC의 기능을 식별하는 문제이다.

핵심 개념

NAC(Network Access Control)는 네트워크에 접속하려는 사용자와 기기를 식별·인증하고, 백신·보안 패치 등 단말의 보안 상태가 정책을 충족하는지 검사한 뒤 접속 허용, 격리 또는 차단을 수행하는 기술이다.
NAC는 접속 전후의 접근 통제와 단말 무결성 점검이 핵심이고, ESM은 여러 보안 시스템의 로그와 이벤트를 중앙에서 통합 관리하는 것이 핵심이다.

선지별 해설

① X — SAC(System Access Control)는 시스템 자원에 대한 접근 통제를 가리키는 표현으로, 제시된 네트워크 접속 인증·단말 보안 상태 점검 기능을 대표하는 장비명이 아니다. 틀린 표현은 ‘SAC 장비’이며, 올바르게는 ‘NAC 장비’이다.
② X — AAC(Account Access Control)는 계정의 접근 권한 통제를 뜻하는 표현으로, 네트워크에 연결되는 기기의 백신·패치 상태를 검사하여 접속 여부를 정하는 장비가 아니다. 틀린 표현은 ‘AAC 장비’이며, 올바르게는 ‘NAC 장비’이다.
③ O — NAC(Network Access Control)는 사용자·기기를 인증하고 단말의 보안 상태와 정책 준수 여부를 점검하여 네트워크 접속을 허용·격리·차단한다. 문제의 설명과 일치한다.
④ X — ESM(Enterprise Security Management)은 방화벽·침입탐지시스템 등 여러 보안 시스템의 로그와 보안 이벤트를 통합 수집·분석·관리하는 체계이다. 개별 단말의 상태를 검사해 네트워크 접속 자체를 허용하는 장비가 아니다. 틀린 표현은 ‘ESM 장비’이며, 올바르게는 ‘NAC 장비’이다.

NoteBase

오답 포인트

‘접근 통제’라는 공통 표현만 보고 SAC나 AAC를 고르기 쉽다. 그러나 사용자·기기 인증, 백신·패치 점검, 무결성 또는 정책 준수 여부에 따른 접속 허용·격리·차단이 함께 제시되면 NAC이다. ESM의 핵심은 접속 승인보다 보안 로그와 이벤트의 중앙 통합 관리이다.

다시 나오면 이렇게 판단

문제에서 ‘네트워크 접속 단말 인증 → 단말 보안 상태 점검 → 정책에 따른 허용·격리·차단’의 흐름이 나타나는지 확인한다. 이 흐름이면 NAC로 판단하고, 여러 보안 장비의 로그·이벤트 통합 분석이 중심이면 ESM으로 판단한다.

암기 포인트

NAC는 단말을 검사해 네트워크 출입을 통제하고, ESM은 보안 이벤트를 한곳에서 통합 관리한다.

NoteBase

문 16. 다음 중 이더넷 물리 주소(MAC)가 될 수 있는 것은?

① 00:0C:29:97:13:8C:48:A0

② 00:0C:29:97:13:8C:48

③ 00:0C:29:97:13:8C

④ 00:0C:29:97:13

정답 3번

출제 포인트

이 문제는 이더넷 MAC 주소의 길이와 16진수 표기 형식을 묻는다.

핵심 개념

이더넷에서 사용하는 MAC-48 주소는 48비트, 즉 6바이트로 구성된다. 일반적인 표기에서는 1바이트를 두 자리 16진수로 나타내므로, 두 자리씩 묶인 6개의 옥텟이 콜론으로 구분되어야 한다. 따라서 전체 16진수 자릿수는 12자리이다.

선지별 해설

① X
00:0C:29:97:13:8C:48:A0는 두 자리 16진수 묶음이 8개이므로 8바이트, 64비트이다. 틀린 부분은 묶음이 8개라는 점이며, 이더넷 MAC-48 주소라면 두 자리 묶음이 6개여야 한다.

② X
00:0C:29:97:13:8C:48은 묶음이 7개이므로 7바이트, 56비트이다. 틀린 부분은 묶음이 7개라는 점이며, 올바른 MAC-48 형식은 묶음 6개이다.

③ O
00:0C:29:97:13:8C는 두 자리 16진수 묶음이 정확히 6개이므로 6바이트, 48비트의 이더넷 MAC 주소 형식에 맞는다. 각 자리도 0~9와 A~F 범위의 유효한 16진수 문자로 이루어져 있다.

④ X
00:0C:29:97:13은 묶음이 5개이므로 5바이트, 40비트에 불과하다. 틀린 부분은 마지막 1바이트가 부족하다는 점이며, 올바른 MAC-48 형식은 두 자리 묶음 6개이다.

NoteBase

오답 포인트

모든 선지가 콜론과 두 자리 16진수 묶음을 사용하므로 겉모양만 보면 비슷하다. 핵심 함정은 16진수 문자의 적법성보다 콜론으로 구분된 묶음의 개수를 세는 데 있다. ①의 8개 묶음은 64비트 표기이고, 이 문제에서 요구한 이더넷 MAC-48과 길이가 다르다.

다시 나오면 이렇게 판단

각 묶음이 두 자리 16진수인지 확인한 다음 묶음의 수를 센다. 두 자리 묶음 6개이면 6바이트, 48비트이므로 이더넷 MAC-48의 기본 형식에 맞는다.

암기 포인트

MAC-48은 48비트 = 6바이트 = 두 자리 16진수 6묶음이다.

NoteBase

문 17. 다음 중 근거리 통신망에서 공격대상의 MAC 주소를 공격자의 컴퓨터 MAC 주소로 변경하여 공격대상이 전송하는 모든 데이터를 가로챌 수 있는 공격 기법은?

① 스위치 재밍
② IP 스푸핑
③ DNS 스푸핑
④ ARP 스푸핑

정답 4번

출제 포인트

근거리 통신망에서 IP 주소와 MAC 주소의 대응 관계를 위조하여 통신을 가로채는 공격 기법을 구별하는 문제이다.

핵심 개념

ARP 스푸핑은 위조된 ARP 메시지로 피해자의 ARP 캐시를 오염시켜 특정 IP 주소가 공격자의 MAC 주소에 대응하는 것처럼 만드는 공격이다. 그 결과 피해자의 프레임이 공격자에게 전달되어 중간자 공격이나 도청이 가능해진다.
스위치 재밍은 스위치의 MAC 주소 테이블을 넘치게 하는 공격이고, IP 스푸핑은 IP 패킷의 출발지 IP 주소를 위조하는 공격이며, DNS 스푸핑은 도메인 이름에 대한 IP 주소 응답을 위조하는 공격이다.

선지별 해설

① X — '스위치 재밍'이라는 공격 기법명이 틀렸다. 스위치 재밍은 다수의 위조 MAC 주소를 보내 스위치의 MAC 주소 테이블을 포화시키는 공격이다. 문제처럼 IP 주소와 공격자의 MAC 주소가 대응하도록 ARP 정보를 위조하는 기법은 ARP 스푸핑이다.
② X — 'IP 스푸핑'이라는 공격 기법명이 틀렸다. IP 스푸핑은 패킷의 출발지 IP 주소를 다른 주소로 위조하는 기법이다. 근거리 통신망에서 ARP 캐시의 IP–MAC 대응 관계를 공격자 MAC 주소로 변조하는 기법은 ARP 스푸핑이다.
③ X — 'DNS 스푸핑'이라는 공격 기법명이 틀렸다. DNS 스푸핑은 위조된 DNS 응답 등을 이용해 도메인 이름을 공격자가 의도한 IP 주소로 연결하는 기법이다. 문제의 MAC 주소 대응 관계를 위조하는 기법은 ARP 스푸핑이다.
④ O — ARP 스푸핑은 위조된 ARP 메시지로 피해자의 ARP 캐시에 잘못된 IP–MAC 대응 정보를 저장시킨다. 피해자의 트래픽이 공격자의 MAC 주소로 향하게 되므로 공격자가 데이터를 가로챌 수 있다.

오답 포인트

스위치 재밍도 근거리 통신망에서 트래픽 도청을 유발할 수 있어 혼동하기 쉽다. 그러나 '특정 IP에 대응하는 MAC 주소를 공격자 MAC 주소로 바꾼다'는 단서는 ARP 캐시 오염을 뜻하므로 ARP 스푸핑을 가리킨다.

NoteBase

다시 나오면 이렇게 판단

위조 대상을 확인한다. IP–MAC 대응 관계이면 ARP 스푸핑, 출발지 IP이면 IP 스푸핑, 도메인–IP 대응 관계이면 DNS 스푸핑, 스위치 MAC 주소 테이블의 포화이면 스위치 재밍이다.

암기 포인트

ARP는 IP를 MAC으로 찾는 절차이므로, IP–MAC 대응 관계를 속이면 ARP 스푸핑이다.

NoteBase

문 18. 다음 <보기>의 내용은 DDoS 공격 직후가 발생하였을 경우 긴급 대응 절차를 나열한 것이다. 순서를 올바르게 나열하고 있는 것은?

<보기>
ㄱ. 모니터링
ㄴ. 상세분석
ㄷ. 공격탐지
ㄹ. 초동조치
ㅁ. 차단조치

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

정답 3번

출제 포인트

DDoS 공격 발생 직후의 긴급 대응 절차에서 상황을 관찰하고 공격을 확인한 뒤, 초기에 대응하고 상세히 분석하여 차단하는 선후관계를 묻는 문제이다.

올바른 순서

1. 모니터링(ㄱ) — 네트워크와 서비스 상태를 관찰하여 이상 징후를 확인하는 단계이다.
2. 공격탐지(ㄷ) — 관찰된 이상 징후가 DDoS 공격인지 식별하는 단계이다.
3. 초동조치(ㄹ) — 공격이 탐지되면 피해 확산을 줄이기 위한 초기 대응을 시행하는 단계이다.
4. 상세분석(ㄴ) — 공격의 유형·경로·특성을 구체적으로 파악하는 단계이다.
5. 차단조치(ㅁ) — 분석한 공격 특성에 맞추어 악성 트래픽을 차단하는 단계이다.

따라서 올바른 순서는 ㄱ → ㄷ → ㄹ → ㄴ → ㅁ이다. 모니터링 결과가 공격탐지의 근거가 되고, 상세분석 결과가 적절한 차단조치의 근거가 된다.

NoteBase

선지별 해설

① X — ㄹ(초동조치)을 ㄱ(모니터링)보다 먼저 둔 것이 틀렸다. 공격 징후를 모니터링하고 공격을 탐지한 뒤 초동조치를 시행해야 한다. 올바르게는 ㄱ → ㄷ → ㄹ → ㄴ → ㅁ이다.

② X — ㄹ(초동조치)로 시작하고 ㄱ(모니터링)을 그 뒤에 둔 것이 틀렸다. 모니터링과 공격탐지가 초동조치에 선행해야 한다. 올바르게는 ㄱ → ㄷ → ㄹ → ㄴ → ㅁ이다.

③ O — ㄱ(모니터링) → ㄷ(공격탐지) → ㄹ(초동조치) → ㄴ(상세분석) → ㅁ(차단조치)의 순서로, 관찰·식별·초기 대응·분석·차단의 흐름과 일치한다.

④ X — ㄱ(모니터링)을 마지막에 둔 것이 틀렸다. 모니터링은 공격탐지에 필요한 이상 징후를 먼저 확인하는 출발 단계이다. 올바르게는 ㄱ → ㄷ → ㄹ → ㄴ → ㅁ이다.

오답 포인트

초동조치와 차단조치를 모두 즉각적인 대응으로 보아 앞쪽에 배치하기 쉽다. 그러나 초동조치는 공격탐지 직후의 초기 대응이고, 최종 차단조치는 상세분석으로 공격 특성을 파악한 뒤 이루어진다는 점이 핵심이다.

다시 나오면 이렇게 판단

절차형 문제에서는 관찰 → 식별 → 초기 대응 → 원인·특성 분석 → 분석 결과에 따른 조치의 의존관계를 확인한다. 앞 단계의 결과가 뒤 단계의 판단 근거가 되는지를 보면 순서를 정할 수 있다.

암기 포인트

모니터링 → 탐지 → 초동조치 → 상세분석 → 차단조치, 즉 '모·탐·초·상·차'의 순서이다.

NoteBase

문 19. 다음 중 침입차단시스템(Firewall)에서 아래와 같이 주소에 의한 패킷 필터링 규칙을 적용 시 필터링 된 패킷의 결과가 가장 올바르지 않은 것은? (단, 적용순서는 A, B, C 순)

규칙	출발지주소	목적지 주소	동작
A	10.12.99.0/24	165.15.0.0/16	Deny
B	10.12.0.0/8	165.15.6.0/24	Allow
C	any	any	Deny

① 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.

② 출발지 주소가 10.12.99.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.

③ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.6.1인 패킷은 허용된다.

④ 출발지 주소가 10.12.1.1, 목적지 주소가 165.15.1.1인 패킷은 거부된다.

정답 2번

출제 포인트

출발지·목적지 주소가 여러 규칙에 동시에 일치할 때 A, B, C 순으로 검사하여 처음 일치한 규칙의 동작을 적용할 수 있는지를 묻는 문제이다.

자료 읽는 순서

1. 규칙 A의 출발지와 목적지 조건을 모두 확인한다.
2. A에 일치하지 않을 때만 규칙 B를 확인한다.
3. A와 B에 모두 일치하지 않으면 규칙 C의 기본 거부를 적용한다.

CIDR에서 /24는 앞의 24비트, /16은 앞의 16비트, /8은 앞의 8비트가 같은 주소 범위를 뜻한다.

핵심 근거

규칙 A는 출발지가 10.12.99.0/24이고 목적지가 165.15.0.0/16인 패킷을 거부한다. 따라서 목적지가 165.15.6.1이더라도 출발지가 10.12.99.1이면 A에 먼저 일치하여 거부된다. 규칙 B는 A에 일치하지 않은 패킷 중 출발지가 10.0.0.0/8 범위이고 목적지가 165.15.6.0/24 범위인 패킷을 허용한다. 나머지는 규칙 C에 따라 거부된다.

NoteBase

선지별 해설

① O — 10.12.99.1은 A의 10.12.99.0/24에, 165.15.1.1은 A의 165.15.0.0/16에 포함되므로 A가 먼저 적용되어 거부된다.
② X — 10.12.99.1과 165.15.6.1은 규칙 B의 조건에도 들어가지만, 그보다 먼저 규칙 A의 두 주소 조건에 모두 일치한다. 틀린 표현은 '허용된다'이며, 올바르게는 규칙 A에 따라 '거부된다'이다.
③ O — 10.12.1.1은 A의 10.12.99.0/24에 포함되지 않으므로 A를 통과한다. 이어서 출발지는 B의 /8 범위에, 목적지 165.15.6.1은 B의 165.15.6.0/24에 포함되므로 허용된다.
④ O — 10.12.1.1은 A의 출발지 조건에 맞지 않고, 165.15.1.1은 B의 목적지 165.15.6.0/24에 포함되지 않는다. A와 B에 모두 일치하지 않으므로 C의 기본 거부가 적용된다.

오답 포인트

②에서 목적지 165.15.6.1만 보고 허용 규칙 B를 바로 적용하기 쉽다. 그러나 이 패킷은 규칙 A에도 일치하며, 적용 순서가 A가 먼저이므로 B까지 내려가지 않는다. 또한 10.12.0.0/8의 /8은 첫 번째 옥텟만 비교하므로 10.12.1.1과 10.12.99.1이 모두 그 범위에 포함된다는 점도 주의한다.

다시 나오면 이렇게 판단

각 패킷마다 규칙을 위에서부터 하나씩 대조하고, 출발지와 목적지 조건이 모두 맞는 최초 규칙에서 판단을 끝낸다. 더 구체적인 프리픽스가 있더라도 먼저 배치된 규칙에 일치하면 뒤 규칙은 적용되지 않는다.

암기 포인트

패킷 필터링은 '위에서부터, 출발지와 목적지를 함께, 최초 일치에서 종료'로 정리한다.

NoteBase

문 20. 다음 중 네트워크상의 호스트를 발견하고 그 호스트가 제공하는 서비스와 사용하는 운영체제 등을 탐지할 목적으로 고든 라이언에 의해 개발된 네트워크 스캐닝 유틸리티로 TCP Xmas 스캔과 같은 스텔스 포트 스캐닝에 활용되는 것은?

① Ping
② netstat
③ nmap
④ nbstat

정답 3번

출제 포인트

이 문제는 호스트 발견, 포트·서비스 조사, 운영체제 추정, 스텔스 스캔 기능을 함께 제공하는 네트워크 도구를 구별하는 문제이다.

핵심 개념

Nmap(Network Mapper)은 고든 라이언이 개발한 네트워크 탐색·보안 점검 도구이다. 호스트 발견, 포트 상태 확인, 서비스와 버전 식별, 운영체제 추정 등을 수행하며 TCP Xmas 스캔도 지원한다.
Ping은 ICMP 등을 이용한 도달 가능성 확인, netstat은 주로 현재 시스템의 연결·대기 포트·통계 확인, nbtstat은 Windows의 NetBIOS over TCP/IP 정보 확인에 쓰인다.

선지별 해설

① X — Ping은 주로 대상 호스트의 도달 가능성과 응답 시간을 확인하는 도구이다. 호스트의 서비스·운영체제를 종합 탐지하고 TCP Xmas 스캔을 수행하는 도구라는 표현은 틀리며, 올바르게는 Nmap이다.
② X — netstat은 주로 실행 중인 시스템의 네트워크 연결, 대기 중인 포트, 라우팅 정보 및 프로토콜 통계를 확인한다. 원격 호스트를 탐색하는 종합 스캐너라는 표현은 틀리며, 올바르게는 Nmap이다.
③ O — Nmap은 호스트 발견과 포트 스캔, 서비스·버전 식별, 운영체제 추정을 지원한다. TCP 세그먼트의 FIN·PSH·URG 플래그를 설정하는 Xmas 스캔도 제공하므로 문제의 설명과 일치한다.
④ X — 선지의 nbstat은 문제에서 설명한 네트워크 스캐닝 도구가 아니다. 유사한 Windows 명령의 올바른 이름은 nbtstat이며, 이는 NetBIOS over TCP/IP의 이름 테이블·캐시·세션 정보를 확인하는 도구이다. 문제의 기능에 해당하는 도구는 Nmap이다.

오답 포인트

Ping과 netstat도 네트워크 점검에 사용되므로 혼동하기 쉽다. 그러나 '서비스와 운영체제 탐지'와 'TCP Xmas 스캔'이 함께 제시되면 단순 연결 확인 도구가 아니라 Nmap을 가리킨다. 또한 ④의 nbstat은 일반적인 Windows 명령인 nbtstat과 철자가 다르다.

NoteBase

다시 나오면 이렇게 판단

도구의 대표 기능을 묶어서 판단한다. 도달 가능성·응답 시간은 Ping, 현재 연결·대기 포트 확인은 netstat, NetBIOS 정보 확인은 nbtstat, 원격 호스트 발견·포트 스캔·서비스 및 운영체제 탐지는 Nmap이다.

암기 포인트

Nmap은 Network Mapper이며, 호스트 발견·포트·서비스·운영체제·스텔스 스캔을 한 묶음으로 기억한다.

NoteBase