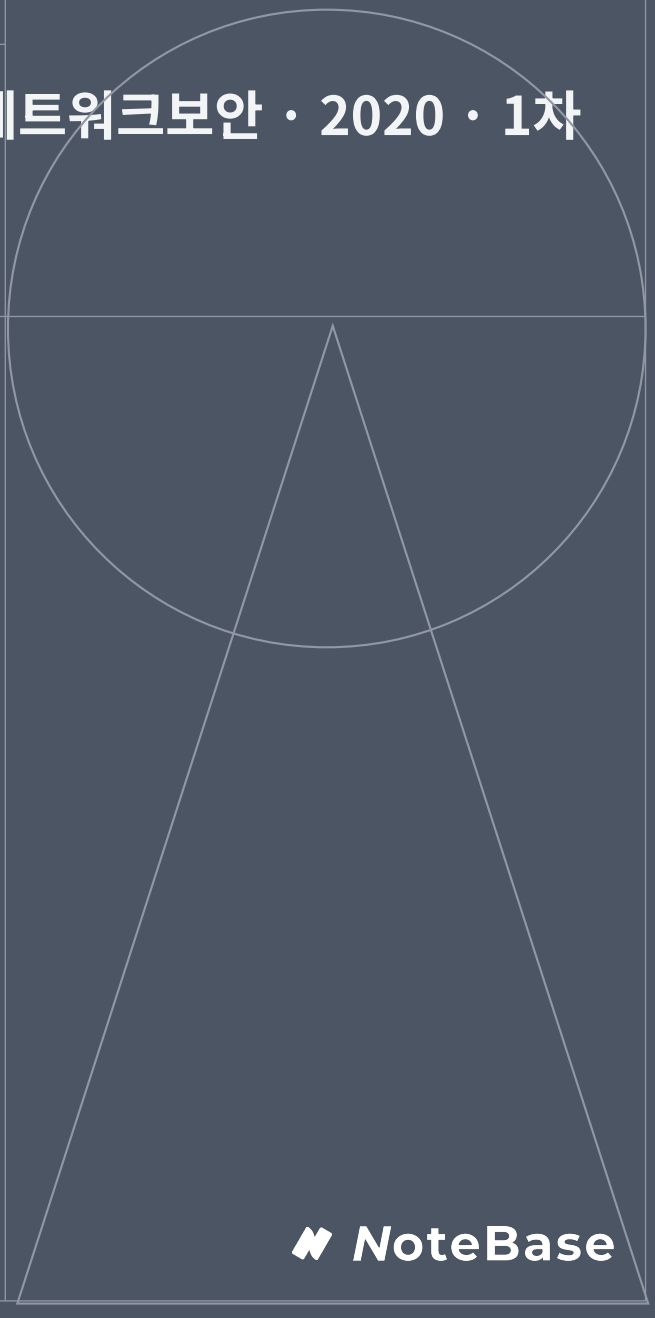
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2020 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2020 · 1차

공무원/해경/일반직 9급 · 네트워크보안 · 2020 · 1차

문 1. 다음 중 스니핑(Sniffing) 공격에 대처하는 방법으로 가장 올바른 것은?

① 전용 네트워크 망에서만 통신을 수행한다.

② SSL, SSH를 사용한다.

③ VLAN 기능을 활성화한다.

④ 데이터 전송시에 패킷마다 다른 경로를 사용한다.

정답 2번

출제 포인트

스니핑 공격으로 패킷이 가로채지더라도 통신 내용을 알아볼 수 없게 하는 직접적인 대응 방법을 묻는 문제이다.

핵심 개념

스니핑은 네트워크를 지나는 패킷을 엿보아 계정 정보나 통신 내용을 수집하는 공격이다. SSL/TLS나 SSH처럼 통신 내용을 암호화하는 프로토콜을 사용하면 공격자가 패킷을 가로채더라도 평문 내용을 해독하기 어렵다.

선지별 해설

① X — 틀린 표현은 '전용 네트워크 망에서만 통신을 수행한다'이다. 전용망은 외부 접근 가능성을 줄일 수 있지만 내부의 비인가 장비나 침해된 호스트가 패킷을 수집하는 것까지 막지는 못한다. 올바르게는 통신 경로의 종류와 별개로 중요한 데이터를 암호화하여 전송해야 한다.
② O — SSL/TLS는 응용 서비스의 통신 내용을 암호화하고, SSH는 원격 접속 세션을 암호화한다. 따라서 스니핑으로 패킷이 노출되더라도 평문 정보의 유출을 막는 직접적인 대응책이다.
③ X — 틀린 표현은 'VLAN 기능을 활성화한다'만으로 스니핑에 대처할 수 있다는 점이다. VLAN은 네트워크를 논리적으로 분리하여 패킷이 퍼지는 범위를 줄이지만 데이터 자체를 암호화하지는 않는다. 올바르게는 VLAN 분리와 별도로 SSL/TLS, SSH 등의 암호화 통신을 적용해야 한다.
④ X — 틀린 표현은 '패킷마다 다른 경로를 사용한다'이다. 경로를 분산해도 각 경로에서 패킷이 가로채질 수 있고, 패킷 내용도 보호되지 않는다. 올바르게는 전송 경로를 바꾸는 것이 아니라 패킷의 내용을 암호화해야 한다.

NoteBase

오답 포인트

전용망과 VLAN은 접근 범위나 브로드캐스트 영역을 줄이는 보조적 통제이지만 기밀성을 직접 제공하지 않는다.
이 문항의 함정은 네트워크 분리와 데이터 암호화를 같은 수준의 스니핑 방어로 보는 데 있다.

다시 나오면 이렇게 판단

스니핑 대책을 고를 때는 패킷을 가로채는 행위 자체보다 가로챈 내용을 읽지 못하게 하는지를 판단한다.
선택지에 SSL/TLS, SSH, VPN 등 암호화 통신이 있으면 직접적인 기밀성 대책으로 본다.

암기 포인트

스니핑 대응의 핵심은 경로 변경이 아니라 통신 내용의 암호화이다.

NoteBase

문 2. 다음 중 NAT(Network Address Translation)를 사용하는 가장 근본적인 이유로 올바른 것은?

① IP 주소 부족 문제를 해결

② 데이터 암호화

③ 네트워크 세그먼테이션

④ 네트워크 전송 속도 향상

정답 1번

출제 포인트

NAT의 핵심 목적과 암호화·망 분리·전송 성능의 기능을 구별하는 문제이다.

핵심 개념

NAT는 사설 IP 주소와 공인 IP 주소를 변환하는 기술이다. 여러 내부 단말이 소수의 공인 IPv4 주소를 공유하게 하므로 공인 IPv4 주소 부족 문제를 완화한다.

선지별 해설

① O — NAT를 사용하면 내부의 여러 사설 IP 주소를 하나 또는 소수의 공인 IP 주소로 변환하여 외부와 통신할 수 있으므로, 가장 근본적인 사용 이유는 IP 주소 부족 문제의 완화이다.
② X — 틀린 표현은 '데이터 암호화'이다. NAT는 주소를 변환할 뿐 데이터의 내용을 암호화하지 않는다. 데이터 암호화는 TLS, IPsec 등 암호화 프로토콜이 담당한다.
③ X — 틀린 표현은 '네트워크 세그먼테이션'이다. NAT의 주된 기능은 주소 변환이며, 네트워크 세그먼테이션은 서브넷, VLAN, 방화벽 정책 등으로 네트워크를 구획하는 것이다.
④ X — 틀린 표현은 '네트워크 전송 속도 향상'이다. NAT는 패킷의 주소와 필요하면 포트 정보를 변환하는 기술이지 전송 속도를 높이는 기술이 아니다.

오답 포인트

NAT가 내부 주소를 외부에 직접 드러내지 않는 효과 때문에 보안 기술로 오인하기 쉽다. 그러나 주소 은닉은 부수적 효과이며, NAT의 근본 목적은 공인 IPv4 주소의 절약이다.

다시 나오면 이렇게 판단

'사설 주소를 공인 주소로 변환한다'거나 '여러 단말이 공인 주소를 공유한다'는 내용이면 NAT의 주소 절약 기능으로 판단한다. 암호화, 망 분리, 속도 향상은 NAT의 본질적 기능이 아니다.

암기 포인트

NAT는 주소 변환, 핵심 목적은 공인 IPv4 주소 절약이다.

NoteBase

문 3. 다음 중 OSI 계층구조와 계층별로 사용되는 보안 프로토콜의 연결이 가장 옳지 않은 것은?

① 데이터링크 계층 - TLS

② 네트워크 계층 - IPSec

③ 전송계층 - SSL

④ 응용계층 - SSH

정답 1번

출제 포인트

OSI 계층별 보안 프로토콜의 대표적인 대응 관계를 구분하는 문제이다.

핵심 개념

TLS와 SSL은 TCP를 기반으로 통신 내용을 보호하며 통상 전송 계층 보안 프로토콜로 분류한다. IPSec은 IP 패킷을 보호하는 네트워크 계층 프로토콜이고, SSH는 원격 접속 등의 서비스를 제공하는 응용 계층 프로토콜이다. 데이터링크 계층의 대표적인 보안 프로토콜로는 MACsec이 있다.

선지별 해설

① X — TLS를 데이터링크 계층에 연결한 부분이 틀렸다. 올바르게는 '전송계층 - TLS'로 연결한다.
② O — IPSec은 IP 계층에서 패킷의 인증, 무결성 및 기밀성을 제공하므로 네트워크 계층에 해당한다.
③ O — SSL은 TCP 위에서 통신 데이터를 보호하는 프로토콜로, 통상 전송 계층 보안 프로토콜로 분류한다.
④ O — SSH는 안전한 원격 로그인과 명령 실행 등의 서비스를 제공하므로 응용 계층에 해당한다.

오답 포인트

TLS라는 이름에 '전송 계층'이 직접 드러나지 않아 데이터링크 계층 프로토콜로 잘못 연결하기 쉽다. ①의 잘못된 부분은 '데이터링크 계층'이며, TLS는 SSL과 함께 전송 계층 보안 프로토콜로 묶어 판단한다.

다시 나오면 이렇게 판단

보호 대상을 기준으로 구분한다. IP 패킷을 보호하면 네트워크 계층의 IPSec, TCP 기반 통신을 보호하면 전송 계층의 SSL·TLS, 원격 접속 서비스를 제공하면 응용 계층의 SSH로 판단한다.

암기 포인트

IPSec은 네트워크, SSL·TLS는 전송, SSH는 응용 계층이다.

NoteBase

문 4. 다음 중 UTM(Unified Threat Management)에 대한 설명으로 가장 옳지 않은 것은?

① 방화벽, VPN, IPS 등의 보안 기능을 하나로 통합하여 제공한다.

② 각각 다른 보안 정책을 수립하여 적용한다.

③ 보안 기능이 하나로 통합되어 구축시 비용이 절감된다.

④ 다양하고 복잡한 보안 위협에 대응하고 편의성이 향상된다.

정답 2번

출제 포인트

UTM이 여러 보안 기능과 정책 관리를 하나의 장비·체계로 통합한다는 점을 묻는 문제이다.

핵심 개념

UTM(Unified Threat Management, 통합 위협 관리)은 방화벽, VPN, 침입 방지 등 여러 보안 기능을 하나의 장비나 관리 체계에 통합하여 다양한 위협에 대응하는 방식이다. 핵심은 보안 기능뿐 아니라 정책의 설정과 운영도 통합·일원화한다는 점이다.

선지별 해설

① O — UTM은 방화벽, VPN, IPS 등 여러 보안 기능을 하나의 장비나 체계에 통합하여 제공한다.
② X — 틀린 표현은 '각각 다른 보안 정책을 수립하여 적용한다'이다. UTM은 기능별로 서로 다른 정책을 따로 운영하는 방식이 아니라, 여러 보안 기능에 대한 정책을 통합적으로 수립하고 중앙에서 일관되게 관리·적용한다.
③ O — 여러 보안 기능을 개별 장비로 각각 구축하는 대신 하나의 통합 장비로 구성할 수 있으므로 장비 도입과 구축·운영 비용을 줄일 수 있다.
④ O — 여러 종류의 보안 기능을 연계하여 복합적인 위협에 대응할 수 있고, 하나의 관리 체계에서 설정과 운영이 가능해 관리 편의성도 높아진다.

오답 포인트

②의 '각각 다른'이라는 표현이 함정이다. UTM에서 여러 보안 기능이 존재한다는 사실과 각 기능의 정책을 따로 관리한다는 것을 혼동하면 안 된다. UTM의 목적은 분산된 기능과 정책 관리를 통합하는 데 있다.

다시 나오면 이렇게 판단

UTM 선지에서는 '여러 보안 기능의 통합', '정책의 일원화', '중앙 관리', '비용과 관리 부담의 절감'을 핵심 특징으로 판단한다. 기능별로 정책을 분리하여 각각 운영한다는 설명은 UTM의 통합 취지에 어긋난다.

암기 포인트

UTM은 기능도 통합하고 정책 관리도 일원화한다.

NoteBase

문 5. 다음 중 LAN(Local Area Network) 관련 IEEE 802 표준에 대한 설명으로 가장 옳은 것은?

① IEEE 802.2는 Token Bus에 관한 규정이다.

② IEEE 802.3은 CSMA/CD에 관한 규정이다.

③ IEEE 802.5는 LLC 서브계층에 관한 규정이다.

④ IEEE 802.6은 Token Ring에 관한 규정이다.

정답 2번

출제 포인트

IEEE 802 계열의 번호와 각 LAN·MAN 기술의 대응 관계를 묻는 문제이다.

핵심 개념

IEEE 802.2는 데이터 링크 계층의 LLC 서브계층, IEEE 802.3은 이더넷의 CSMA/CD, IEEE 802.4는 Token Bus, IEEE 802.5는 Token Ring에 관한 표준이다. IEEE 802.6은 도시 규모의 MAN을 위한 DQDB에 관한 표준이다.

선지별 해설

① X
IEEE 802.2를 Token Bus와 연결한 부분이 틀렸다. IEEE 802.2는 LLC 서브계층에 관한 규정이며, Token Bus는 IEEE 802.4이다.

② O
IEEE 802.3은 이더넷의 매체 접근 방식인 CSMA/CD에 관한 규정이므로 옳다.

③ X
IEEE 802.5를 LLC 서브계층과 연결한 부분이 틀렸다. IEEE 802.5는 Token Ring에 관한 규정이며, LLC 서브계층은 IEEE 802.2이다.

④ X
IEEE 802.6을 Token Ring과 연결한 부분이 틀렸다. IEEE 802.6은 MAN의 DQDB에 관한 규정이며, Token Ring은 IEEE 802.5이다.

오답 포인트

선지는 IEEE 802.2, 802.5, 802.6의 대상을 서로 바꾸어 제시한다. 특히 LLC는 802.2, Token Ring은 802.5라는 대응 관계를 뒤바꾸지 않는 것이 핵심이다.

NoteBase

다시 나오면 이렇게 판단

표준 번호를 핵심어와 직접 대응한다. 802.2는 LLC, 802.3은 CSMA/CD, 802.4는 Token Bus, 802.5는 Token Ring, 802.6은 MAN·DQDB이다.

암기 포인트

2-LLC, 3-CSMA/CD, 4-Bus, 5-Ring, 6-MAN·DQDB로 연결한다.

NoteBase

문 6. 다음 중 TCP Well-Known Port 번호와 서비스의 연결이 잘못된 것은?

① TCP 21 - FTP

② TCP 22 - SSH

③ TCP 25 - SNMP

④ TCP 80 - HTTP

정답 3번

출제 포인트

대표적인 TCP Well-Known Port 번호와 응용 계층 서비스의 연결 관계를 묻는 문제이다.

핵심 개념

Well-Known Port는 서버의 대표적인 서비스에 관례적으로 배정된 0~1023번 포트이다. FTP 제어 연결은 TCP 21번, SSH는 TCP 22번, SMTP는 TCP 25번, HTTP는 TCP 80번을 사용한다. SNMP는 일반적으로 관리 요청·응답에 UDP 161번, 트랩 통지에 UDP 162번을 사용한다.

선지별 해설

① O — FTP는 제어 연결에 TCP 21번 포트를 사용하므로 올바른 연결이다. 파일 전송용 데이터 연결에는 TCP 20번이 사용될 수 있다.
② O — SSH는 원격 로그인과 암호화된 통신을 위해 TCP 22번 포트를 사용하므로 올바른 연결이다.
③ X — 틀린 부분은 ‘TCP 25 - SNMP’이다. TCP 25번에 연결되는 서비스는 SMTP이며, SNMP는 일반적으로 UDP 161번을 사용한다. 따라서 올바르게는 ‘TCP 25 - SMTP’이다.
④ O — HTTP의 기본 포트는 TCP 80번이므로 올바른 연결이다.

오답 포인트

③은 25번 포트의 실제 서비스인 SMTP와 이름이 비슷하지 않은 SNMP를 연결하여 혼동을 유도한다. SNMP의 대표 포트는 UDP 161번이라는 점도 함께 구분해야 한다.

다시 나오면 이렇게 판단

먼저 자주 출제되는 기본 대응인 FTP-21, SSH-22, SMTP-25, HTTP-80을 확인한 뒤, SNMP는 UDP 161번이라는 별도 묶음으로 판별한다.

암기 포인트

FTP 21, SSH 22, SMTP 25, HTTP 80, SNMP는 UDP 161이다.

NoteBase

문 7. 다음 중 IPv6의 주소 유형으로 옳지 않는 것은?

① Unicast

② Anycast

③ Broadcast

④ Multicast

정답 3번

출제 포인트

IPv6가 사용하는 주소 유형과 IPv4의 브로드캐스트 방식이 IPv6에서 어떻게 대체되는지를 묻는 문제이다.

핵심 개념

유니캐스트(Unicast)는 하나의 송신자가 하나의 수신 인터페이스로 보내는 1대1 주소 방식이다.
애니캐스트(Anycast)는 여러 인터페이스에 같은 주소를 부여하고 라우팅상 가장 가까운 하나로 전달하는 방식이다.
멀티캐스트(Multicast)는 특정 그룹에 가입한 여러 수신자에게 전달하는 1대다 방식이다.
IPv6에는 브로드캐스트(Broadcast) 주소 유형이 없으며, 여러 노드에 전달해야 하는 기능은 멀티캐스트 등을 이용한다.

선지별 해설

① O — Unicast는 IPv6의 주소 유형이다. 하나의 인터페이스를 식별하며 해당 주소로 보낸 패킷은 그 인터페이스에 전달된다.
② O — Anycast는 IPv6의 주소 유형이다. 같은 애니캐스트 주소가 지정된 여러 인터페이스 가운데 라우팅 기준상 가장 가까운 하나에 패킷이 전달된다.
③ X — Broadcast는 IPv6의 주소 유형이 아니다. 틀린 표현은 ‘Broadcast’이며, 올바르게는 IPv6가 브로드캐스트 주소를 사용하지 않고 필요한 1대다 전달을 Multicast 등으로 처리한다고 해야 한다.
④ O — Multicast는 IPv6의 주소 유형이다. 특정 멀티캐스트 그룹에 속한 여러 인터페이스로 패킷을 전달한다.

오답 포인트

IPv4에서 익숙한 Broadcast를 IPv6에도 그대로 존재하는 주소 유형으로 생각하기 쉽다. IPv6의 대표 주소 유형은 Unicast, Anycast, Multicast이며 Broadcast는 제외된다.

다시 나오면 이렇게 판단

IPv6 주소 유형을 묻는 문제에서는 Unicast·Anycast·Multicast를 먼저 확인하고, Broadcast가 제시되면 IPv6에 없는 유형으로 판단한다.

NoteBase

암기 포인트

IPv6는 UAM(Unicast·Anycast·Multicast), Broadcast는 없다.

NoteBase

문 8. 다음 중 네트워크로 연결된 단말을 확인하는 것으로 무결성 검사, IP 주소와 MAC 주소로 접근제어를 하는 보안솔루션으로 가장 올바른 것은?

① IPS(Intrusion Prevention System)

② NAT(Network Address Translation)

③ NAC(Network Access Control)

④ DRM(Digital Rights Management)

정답 3번

출제 포인트

네트워크에 접속하는 단말을 식별하고 보안 상태를 점검한 뒤 IP 주소와 MAC 주소 등을 기준으로 접근을 허용하거나 차단하는 NAC의 기능을 묻는 문제이다.

핵심 개념

NAC(Network Access Control)는 네트워크에 접속하려는 단말을 식별하고 무결성·보안 상태를 검사하여 정책에 맞는 단말만 접근하도록 통제하는 솔루션이다.
IPS는 침입 탐지·차단, NAT는 주소 변환, DRM은 디지털 콘텐츠의 사용 권한 관리를 담당한다.

선지별 해설

① X — IPS는 네트워크 트래픽에서 공격이나 침입 징후를 탐지하고 차단하는 시스템이다. 단말의 무결성을 검사하고 IP 주소·MAC 주소를 바탕으로 접속을 통제하는 솔루션이라는 표현에는 맞지 않으며, 올바른 용어는 NAC이다.
② X — NAT는 사설 IP 주소와 공인 IP 주소 등을 서로 변환하는 기술이다. 단말의 보안 상태를 검사하여 네트워크 접근을 허용하거나 차단하는 기능을 뜻하지 않으며, 올바른 용어는 NAC이다.
③ O — NAC는 네트워크에 연결되는 단말을 확인하고 무결성 또는 보안 상태를 점검하며, IP 주소와 MAC 주소 등의 식별 정보를 이용해 접근을 통제한다. 문제의 설명과 일치한다.
④ X — DRM은 디지털 문서·음원·영상 등 콘텐츠의 이용 권한과 복제·배포를 통제하는 기술이다. 네트워크 접속 단말을 검사하고 접근을 제어하는 솔루션이 아니며, 올바른 용어는 NAC이다.

오답 포인트

①의 IPS도 네트워크 보안 장비이므로 혼동하기 쉽다. 그러나 공격 트래픽의 탐지·차단이 중심이면 IPS이고, 접속 단말의 식별·상태 점검·접근 통제가 중심이면 NAC이다.

NoteBase

다시 나오면 이렇게 판단

문제에서 단말 확인, 무결성 검사, 보안 정책 준수 여부, IP 주소·MAC 주소 기반 접속 통제가 함께 제시되면 NAC로 판단한다. 공격 패턴 차단은 IPS, 주소 변환은 NAT, 콘텐츠 권한 통제는 DRM으로 구분한다.

암기 포인트

NAC는 단말의 네트워크 출입 통제, IPS는 침입 차단, NAT는 주소 변환, DRM은 콘텐츠 권한 관리이다.

NoteBase

문 9. netstat -s 명령으로 프로토콜별 통계정보를 확인할 수 있다. 다음 중 이에 해당되지 않는 프로토콜은 무엇인가?

① MAC

② ICMP

③ TCP

④ UDP

정답 1번

출제 포인트

netstat -s가 제공하는 IP 계층·전송 계층의 프로토콜별 통계와 데이터 링크 계층의 MAC 정보를 구별하는 문제이다.

핵심 개념

netstat -s는 IP, ICMP, TCP, UDP 등 IP 프로토콜 스택의 프로토콜별 통계를 표시한다. 반면 MAC은 데이터 링크 계층에서 장치의 물리 주소 지정과 매체 접근 제어에 관한 개념이므로 이 명령의 프로토콜별 통계 항목에 해당하지 않는다.

선지별 해설

① O — MAC은 데이터 링크 계층의 매체 접근 제어 또는 물리 주소와 관련된 개념으로, netstat -s가 출력하는 프로토콜별 통계 대상에 해당하지 않는다. 따라서 문제에서 요구한 정답이다.
② X — 'ICMP는 해당되지 않는다'는 판단이 틀렸다. ICMP는 IP 네트워크의 오류 보고와 진단에 쓰이는 프로토콜이며, netstat -s로 ICMP 통계를 확인할 수 있다.
③ X — 'TCP는 해당되지 않는다'는 판단이 틀렸다. TCP는 연결 지향형 전송 계층 프로토콜이며, netstat -s로 연결·세그먼트 관련 TCP 통계를 확인할 수 있다.
④ X — 'UDP는 해당되지 않는다'는 판단이 틀렸다. UDP는 비연결형 전송 계층 프로토콜이며, netstat -s로 데이터그램 관련 UDP 통계를 확인할 수 있다.

오답 포인트

MAC도 네트워크 용어이므로 프로토콜 통계에 포함된다고 착각하기 쉽다. 그러나 이 문항의 구분 기준은 네트워크와 관련된 모든 개념인지가 아니라 netstat -s가 집계하는 IP 프로토콜 스택의 통계 대상인지이다.

다시 나오면 이렇게 판단

netstat -s의 대상은 IP, ICMP, TCP, UDP와 같은 프로토콜별 통계라고 판단한다. MAC처럼 데이터 링크 계층의 주소·매체 접근 개념은 분리한다.

NoteBase

암기 포인트

-s는 프로토콜 통계, MAC은 링크 계층이다.

NoteBase

문 10. 다음 중 허니팟(Honeypot)에 대한 설명으로 가장 옳지 않은 것은?

① 컴퓨터 시스템에 침입한 스팸, 바이러스, 크래커를 탐지하기 위하여 의도적으로 설치한 시스템이다.

② 실제 공격을 당한 것처럼 보이도록 만든 함정이다.

③ 공격자가 허니팟으로 접근할 수 없도록 차단해야 한다.

④ 침입자가 오래도록 머물게 해야 한다.

정답 3번

출제 포인트

허니팟이 공격자의 접근을 유도하여 침입 행위와 공격 기법을 관찰하는 함정 시스템이라는 점을 묻는 문제이다.

핵심 개념

허니팟은 실제 운영 시스템처럼 보이는 미끼 자원을 의도적으로 노출하여 공격자를 유인하고, 공격 과정과 도구 및 행위 정보를 수집하는 보안 시스템이다. 실제 중요 자산과는 격리하여 운영하되, 공격자가 접근하고 활동할 수 있어야 탐지와 분석이라는 목적을 달성할 수 있다.

선지별 해설

① O — 허니팟은 스팸 발송원, 악성코드, 크래커 등 잠재적 공격 주체나 위협의 접근을 유인하여 침입 시도와 행위를 탐지·분석하기 위해 의도적으로 설치하는 시스템이다.
② O — 실제 시스템이 공격받는 것처럼 보이게 만든 함정 또는 미끼라는 설명은 허니팟의 핵심 성격에 해당한다.
③ X — 틀린 표현은 '공격자가 허니팟으로 접근할 수 없도록 차단해야 한다'이다. 올바르게는 실제 운영망으로의 확산은 차단하되 공격자가 허니팟에는 접근하도록 유도해야 한다. 접근 자체를 막으면 공격 행위를 탐지하고 정보를 수집할 수 없다.
④ O — 공격자를 가능한 한 오래 머물게 하면 행동 패턴, 사용 도구, 공격 절차에 관한 정보를 더 많이 수집할 수 있으므로 허니팟의 운영 목적에 부합한다.

오답 포인트

일반 보안 시스템은 공격자의 접근을 차단하지만, 허니팟은 ③처럼 모든 접근을 막는 장치가 아니다. 공격자를 미끼 환경으로 유인하면서 실제 운영 시스템과 다른 자산으로의 이동만 통제한다는 점이 함정이다.

다시 나오면 이렇게 판단

허니팟 관련 선지는 '유인·접근·관찰·정보 수집'이면 옳은 방향이고, '허니팟 자체에 대한 접근 차단'이면 목적에 반하므로 틀린 방향이라고 판단한다.

NoteBase

암기 포인트

허니팟은 공격자를 막는 벽이 아니라 공격자를 끌어들여 관찰하는 미끼이다.

NoteBase

문 11. 다음 중 지능형 지속 공격(Advanced Persistent Threat, APT)에 대한 설명 중 가장 옳지 않은 것은?

① 사회 공학적 방법을 사용한다.

② 공격 대상이 명확하다.

③ 불분명한 목적과 동기를 가진 해커 집단이 주로 사용한다.

④ 가능한 방법을 총동원한다.

정답 3번

출제 포인트

지능형 지속 공격(APT)의 핵심 특징인 명확한 표적과 목적, 장기간의 은밀한 침투, 복합적인 공격 수단을 구별하는 문제이다.

핵심 개념

APT는 특정 조직이나 기관을 목표로 삼아, 명확한 목적을 달성할 때까지 장기간 은밀하게 침투를 지속하는 조직적 공격이다. 표적형 피싱 같은 사회 공학, 악성코드, 취약점 공격 등 여러 수단을 단계적으로 결합할 수 있다.

선지별 해설

① O — APT는 표적형 피싱이나 악성 첨부 파일처럼 사람의 신뢰와 행동을 악용하는 사회 공학적 방법을 초기 침투 수단으로 사용할 수 있다.
② O — APT는 불특정 다수를 무차별적으로 공격하기보다 특정 기관·기업·국가 등 공격 대상을 미리 정하는 표적 공격이다.
③ X — 틀린 표현은 '불분명한 목적과 동기'이다. APT 공격자는 정보 탈취, 기밀 수집, 시스템 교란 등 명확한 목적과 동기를 가지고 조직적·지속적으로 공격한다. 올바르게는 '명확한 목적과 동기를 가진 조직화된 공격 주체가 주로 사용한다'이다.
④ O — APT는 목적 달성을 위해 사회 공학, 악성코드, 취약점 악용 등 이용 가능한 여러 공격 방법을 복합적으로 동원한다.

오답 포인트

APT의 '지능형'이라는 말 때문에 정체와 목적까지 불분명하다고 오해하기 쉽다. 그러나 은밀한 것은 공격 과정과 침투 흔적이며, 표적과 목적은 오히려 명확하다는 점이 핵심이다.

다시 나오면 이렇게 판단

APT 선지에서는 '특정 표적', '명확한 목적', '장기간 지속', '은밀한 침투', '복합 수단'이 함께 나타나는지 확인한다. '불특정 대상'이나 '불분명한 목적'이라는 표현은 APT의 표적성과 목적성에 어긋난다.

NoteBase

암기 포인트

APT는 표적과 목적은 명확하고, 침투는 은밀하며, 공격은 지속적·복합적이다.

NoteBase

문 12. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳은 것은?

① 망분리 기술로 USB와 같은 저장매체를 통한 악성코드 침입이 불가능하다.

② 물리적 망분리 기법에는 SBC 및 CBC 기반의 망분리 기법이 존재한다.

③ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

④ 논리적 망분리는 VDI(Virtual Desktop Infrastructure)와 OS 커널 분리로 분류 될 수 있다.

정답 4번

출제 포인트

이 문제는 물리적 망분리와 논리적 망분리를 구현 방식에 따라 구분할 수 있는지를 묻는 문제이다.

핵심 개념

물리적 망분리는 업무망과 인터넷망에 별도의 단말기와 네트워크 장비를 두어 물리적으로 분리하는 방식이다.
논리적 망분리는 가상화 등의 기술로 하나의 물리적 환경 안에서 업무 영역과 인터넷 영역을 논리적으로 분리하는 방식이다.
SBC(Server Based Computing)는 서버에서 업무 환경을 실행하는 방식이고, CBC(Client Based Computing)는 사용자 단말에서 격리된 환경을 구성하는 방식이다. 이들은 논리적 망분리의 구현 방식에 해당한다.

선지별 해설

① X — '저장매체를 통한 악성코드 침입이 불가능하다'는 표현이 틀리다. 망을 분리하더라도 허가되지 않은 USB 사용이나 저장매체 관리 부실이 있으면 악성코드가 유입될 수 있다. 올바르게는 망분리가 침입 경로를 줄이지만 저장매체 보안 통제도 함께 적용해야 한다.
② X — '물리적 망분리 기법에는 SBC 및 CBC 기반의 기법이 존재한다'는 분류가 틀리다. SBC와 CBC는 가상화 또는 격리 환경을 이용하는 논리적 망분리 방식이다. 올바르게는 물리적 망분리는 업무망과 인터넷망에 별도의 단말기와 네트워크를 두는 방식이다.
③ X — '애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리를 실현한다'는 표현이 틀리다. 애플리케이션 가상화와 데스크톱 가상화는 물리적 자원을 공유하면서 실행 환경을 분리하므로 논리적 망분리를 구현한다.
④ O — 논리적 망분리는 서버 기반의 VDI(Virtual Desktop Infrastructure) 방식과 클라이언트 기반의 OS 커널 분리 방식으로 구현할 수 있다. 따라서 논리적 망분리의 대표적인 구현 방식을 올바르게 설명한 선지이다.

오답 포인트

②와 ③은 가상화 기술을 물리적 망분리로 바꾸어 표현한 함정이다. 또한 ①의 '불가능하다'처럼 보안 위험을 완전히 제거한다고 단정하는 표현도 주의해야 한다.

NoteBase

다시 나오면 이렇게 판단

별도의 단말기와 네트워크 장비를 사용하면 물리적 망분리이고, VDI·애플리케이션 가상화·OS 커널 분리처럼 가상화나 격리 기술을 사용하면 논리적 망분리로 판단한다.

암기 포인트

별도 장비는 물리적 망분리, VDI·SBC·CBC·OS 커널 분리는 논리적 망분리이다.

NoteBase

문 13. 다음 중 DMZ(dimilitarized zone)에 대한 설명으로 가장 옳은 것은?

① 외부 네트워크에서는 DMZ에 접근할 수 없다.

② DMZ내에는 외부 인터넷에 서비스를 제공하기 위해 매우 높은 보안 수준을 요구하므로 주로 내부 접속용 데이터베이스 서버가 위치하고 있다.

③ 내부 사용자가 DMZ에 접속하기 위해서는 외부 방화벽을 거쳐야 한다.

④ DMZ는 보안 조치가 취해진 네트워크 영역으로 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다.

정답 4번

출제 포인트

DMZ의 위치와 역할, 외부·내부 네트워크에서 DMZ로 접속할 때 거치는 방화벽을 구분하는 문제이다.

핵심 개념

DMZ는 인터넷과 같은 신뢰할 수 없는 외부 네트워크와 보호해야 할 내부 네트워크 사이에 두는 별도의 완충 네트워크 영역이다. 외부에 공개할 웹·메일·DNS 서버 등을 DMZ에 배치하고, 내부망과는 방화벽으로 분리하여 공개 서버가 공격받더라도 내부망으로 피해가 확산되는 것을 제한한다. 전형적인 이중 방화벽 구조에서는 외부 네트워크－외부 방화벽－DMZ－내부 방화벽－내부 네트워크의 순서로 구성된다.

NoteBase

선지별 해설

① X
틀린 표현은 '외부 네트워크에서는 DMZ에 접근할 수 없다'이다. DMZ는 외부 이용자에게 서비스를 제공하는 공개 서버를 두는 영역이므로, 허용된 서비스와 포트에 한하여 외부 네트워크에서 외부 방화벽을 거쳐 접근할 수 있다.

② X
틀린 표현은 '주로 내부 접속용 데이터베이스 서버가 위치하고 있다'이다. DMZ에는 주로 외부 공개용 웹·메일·DNS 서버 등을 배치한다. 중요 데이터가 저장된 내부 접속용 데이터베이스 서버는 일반적으로 DMZ가 아니라 내부 네트워크에 두고 접근을 엄격히 통제한다.

③ X
틀린 표현은 '외부 방화벽을 거쳐야 한다'이다. 전형적인 이중 방화벽 구조에서 내부 사용자가 DMZ에 접속할 때에는 내부 네트워크와 DMZ 사이의 내부 방화벽을 거친다. 외부 방화벽은 외부 네트워크와 DMZ 사이에 위치한다.

④ O
DMZ는 보안 통제가 적용되는 별도 네트워크 영역이며, 이중 방화벽 구조에서는 내부 방화벽과 외부 방화벽 사이에 위치할 수 있다. 따라서 옳은 설명이다.

오답 포인트

DMZ의 보안 수준이 높다는 점을 '외부에서 전혀 접근할 수 없는 내부 서버 영역'으로 오해하기 쉽다. DMZ는 외부 접근을 모두 차단하는 곳이 아니라, 공개가 필요한 서비스만 제한적으로 허용하면서 내부망과 분리하는 완충 영역이다.

다시 나오면 이렇게 판단

외부 공개용 서버는 DMZ, 중요 내부 서버는 내부망으로 구분한다. 이중 방화벽 구조에서는 외부망과 DMZ 사이가 외부 방화벽이고, DMZ와 내부망 사이가 내부 방화벽이다.

암기 포인트

DMZ는 외부에 열어 둔 공개 서비스와 내부망 사이의 완충지대이다.

NoteBase

문 14. 다음에서 설명하고 있는 공격은?

이 공격은 할당된 메모리 경계에 대한 검사를 하지 않은 프로그램의 취약점을 이용해서 공격자가 원하는 데이터를 덮어 쓰는 방식이다. 만약 실행 코드가 덮어 써진다면 공격자가 원하는 방향으로 프로그램이 동작하게 할 수 있다.

① Buffer Overflow 공격

② SQL Injection 공격

③ IP Spoofing 공격

④ Format String 공격

정답 1번

출제 포인트

할당된 메모리 영역의 경계를 넘어 데이터를 기록하여 인접한 데이터나 실행 흐름을 변조하는 공격을 식별하는 문제이다.

핵심 개념

버퍼 오버플로 공격은 프로그램이 버퍼의 크기를 제대로 검사하지 않을 때 허용된 범위를 넘는 데이터를 써서 인접 메모리를 덮어쓰는 공격이다. 반환 주소와 같은 실행 흐름 관련 정보가 변조되면 공격자가 의도한 코드를 실행하게 만들 수 있다.
SQL Injection은 입력값에 악의적인 SQL 구문을 삽입하는 공격이고, IP Spoofing은 패킷의 출발지 IP 주소를 위조하는 공격이며, Format String 공격은 외부 입력을 서식 문자열로 부적절하게 사용하여 메모리 내용을 읽거나 쓰는 공격이다.

선지별 해설

① O — Buffer Overflow 공격은 경계 검사가 없는 버퍼에 용량을 초과한 데이터를 기록하여 인접 메모리를 덮어쓴다. 실행 흐름을 결정하는 메모리까지 변조할 수 있다는 지문의 설명과 일치한다.
② X — 틀린 부분은 'SQL Injection 공격'이다. SQL Injection은 데이터베이스 질의에 악의적인 SQL 구문을 삽입하여 질의를 변조하는 공격이다. 지문의 공격은 올바르게는 Buffer Overflow 공격이다.
③ X — 틀린 부분은 'IP Spoofing 공격'이다. IP Spoofing은 네트워크 패킷의 출발지 IP 주소를 다른 주소로 위조하는 공격이다. 지문의 공격은 올바르게는 Buffer Overflow 공격이다.
④ X — 틀린 부분은 'Format String 공격'이다. Format String 공격은 사용자 입력을 서식 문자열로 직접 처리할 때 서식 지정자를 악용하여 메모리를 노출하거나 변조하는 공격이다. 지문처럼 버퍼 용량을 넘어 데이터를 써서 경계를 침범하는 공격은 올바르게는 Buffer Overflow 공격이다.

NoteBase

오답 포인트

④의 Format String 공격도 메모리 변조로 이어질 수 있어 혼동하기 쉽다. 그러나 지문의 결정적 표현은 '할당된 메모리 경계에 대한 검사를 하지 않음'과 '데이터를 덮어 씀'이다. 이는 버퍼의 허용 범위를 넘겨 기록하는 Buffer Overflow의 전형적인 단서이다.

다시 나오면 이렇게 판단

공격의 대상과 수단을 구분한다. 버퍼 경계 초과 기록은 Buffer Overflow, SQL 구문 삽입은 SQL Injection, 출발지 IP 위조는 IP Spoofing, 서식 지정자 악용은 Format String 공격으로 판단한다.

암기 포인트

경계 밖 덮어쓰기 = Buffer Overflow이다.

NoteBase

문 15. 다음은 네트워크 서비스 거부 공격으로 인한 접속 마비에 대한 현상 및 대응요령을 설명한 것이다. 다음 중 가장 옳지 않은 것은?

① 리눅스 시스템의 경우 iptables를 이용한 패킷 필터링을 설정한다.

② 이상 트래픽에 의한 네트워크 속도 저하시 서비스 거부 공격을 의심하고, 트래픽을 분석한다.

③ 서비스 거부 공격시 라우터의 패킷 필터링 기능을 설정하여 대응한다.

④ 외부에서 들어오는 패킷의 발신자를 확인하여 공격자에게 역공격을 감행한다.

정답 4번

출제 포인트

서비스 거부 공격이 의심될 때 정상적인 방어·분석 조치와 부적절한 보복 행위를 구별하는 문제이다.

핵심 개념

서비스 거부 공격 대응은 비정상 트래픽을 탐지·분석하고, 방화벽·호스트·라우터의 필터링 기능으로 공격 트래픽을 차단하거나 제한하여 서비스 가용성을 회복하는 활동이다. 공격 근원지로 추정되는 대상을 다시 공격하는 행위는 방어 조치가 아니며, 발신 주소가 위조되었거나 중간 시스템이 악용되었을 수 있어 실제 공격자를 잘못 특정할 위험도 있다.

선지별 해설

① O — 리눅스의 iptables는 패킷의 출발지·목적지·포트·프로토콜 등의 조건에 따라 허용 또는 차단 규칙을 적용할 수 있으므로 공격 트래픽을 필터링하는 대응 수단이 된다.
② O — 갑작스러운 네트워크 속도 저하와 비정상적인 트래픽 증가는 서비스 거부 공격의 징후일 수 있다. 트래픽의 양상과 출발지, 대상 서비스 등을 분석하여 공격 여부와 차단 대상을 확인하는 것이 적절하다.
③ O — 라우터의 접근 제어 목록이나 패킷 필터링 기능을 이용하면 특정 주소·프로토콜·포트 등의 공격 트래픽을 상위 구간에서 제한할 수 있으므로 적절한 대응이다.
④ X — 틀린 표현은 '공격자에게 역공격을 감행한다'이다. 패킷에 표시된 발신 정보만으로 실제 공격자를 확정하기 어렵고, 역공격은 피해 확대나 무관한 제3자 시스템 공격으로 이어질 수 있다. 올바르게는 의심 트래픽을 분석한 뒤 필터링·차단하고, 필요한 경우 네트워크 운영자나 관계 기관과 협조하여 대응한다.

오답 포인트

④는 '발신자를 확인한다'는 분석 행위와 '역공격한다'는 부적절한 행위를 한 문장에 묶어 그럴듯하게 만든 선지이다. 발신 정보 확인은 대응에 활용할 수 있지만, 그 정보를 근거로 보복 공격을 하는 것은 정상적인 침해사고 대응이 아니다.

NoteBase

다시 나오면 이렇게 판단

탐지·분석·필터링·차단·운영자 협조는 방어적 대응으로 판단한다. 반대로 해킹, 역추적 후 공격, 보복처럼 상대 시스템에 피해를 주는 조치는 적절한 대응에서 제외한다.

암기 포인트

DoS 대응은 분석하고 막는 것이며, 되받아 공격하는 것이 아니다.

NoteBase

문 16. 다음 중 웹 보안을 제공하는 방법인 SSL의 설명으로 가장 옳지 않은 것은?

① TCP/IP 프로토콜의 네트워크 계층에서 보안기능을 수행하며 전송 계층이 있는 프로토콜의 안정성을 제공한다.

② 웹사이트 접속시 http:// 대신 https://를 사용하며, 서버와 클라이언트의 상호 인증 기능이 있다.

③ 넷스케이프에서 개발된 프로토콜로써 네트워크 통신 및 인터넷 사용자에게 안전한 정보를 교환하기 위한 보안 프로토콜이다.

④ 기밀성 제공을 위한 비밀키는 핸드쉐이크 프로토콜에 의해 생성된다.

정답 1번

출제 포인트

SSL의 동작 계층, 인증 기능, 개발 배경, 세션 키 생성 과정을 구분하는 문제이다.

핵심 개념

SSL은 응용 계층의 데이터를 보호하기 위해 신뢰성 있는 전송 프로토콜인 TCP 위에서 동작하는 보안 프로토콜이다. 핸드셰이크 과정에서 서버 인증과 선택적인 클라이언트 인증을 수행하고, 암호화 통신에 사용할 세션 비밀키를 협상·생성한다.

선지별 해설

① X — 틀린 표현은 '네트워크 계층에서 보안기능을 수행'한다는 부분이다. SSL은 IP 계층에서 동작하는 네트워크 계층 보안 프로토콜이 아니라 TCP 위에서 응용 계층 데이터를 보호한다. 네트워크 계층 보안은 대표적으로 IPsec이 담당한다.
② O — HTTPS는 HTTP 통신을 SSL/TLS로 보호하는 방식이다. 서버 인증 기능이 있으며, 서버가 클라이언트 인증서를 요구하는 경우 클라이언트 인증도 수행할 수 있으므로 상호 인증 기능을 제공할 수 있다.
③ O — SSL은 넷스케이프가 개발한 보안 프로토콜이며, 인터넷 통신에서 암호화와 인증 등을 통해 정보를 안전하게 교환하도록 한다.
④ O — 핸드셰이크 프로토콜은 암호 방식과 관련 매개변수를 협상하고, 통신 당사자가 공유할 비밀값을 바탕으로 실제 데이터 암호화에 사용할 세션 비밀키를 생성하도록 한다.

오답 포인트

①의 'TCP/IP 프로토콜'이라는 표현 때문에 SSL을 네트워크 계층 보안으로 착각하기 쉽다. SSL은 TCP의 신뢰성 있는 전송 서비스를 이용하며, IP 계층 자체를 보호하는 프로토콜은 IPsec이다.

NoteBase

다시 나오면 이렇게 판단

보안 프로토콜의 위치를 묻는 경우 보호 대상과 하위 기반을 구분한다. SSL/TLS는 TCP 위에서 응용 데이터를 보호하고, IPsec은 네트워크 계층에서 IP 패킷을 보호한다.

암기 포인트

SSL/TLS는 TCP 위, IPsec은 IP 계층이다.

NoteBase

문 17. 다음 중 ㉠~㉢에 들어갈 용어를 바르게 연결한 것은?

· (㉠) 기법은 정상적인 활동 데이터베이스와 비교하여 침입을 구분한다.
· (㉡) 기법은 공격패턴, 시그니처 데이터베이스와 비교하여 침입을 구분한다.
· (㉢) IDS(Intrusion Detection System)는 네트워크 상의 모든 패킷을 캡처한 후 이를 분석하여 침입을 탐지하는 시스템이다.
※ 이상탐지 : Anomaly Detection, 오용탐지 : Misuse Detection

① ㉠: 이상탐지, ㉡: 오용탐지, ㉢: 네트워크 기반
② ㉠: 이상탐지, ㉡: 오용탐지, ㉢: 호스트 기반
③ ㉠: 오용탐지, ㉡: 이상탐지, ㉢: 네트워크 기반
④ ㉠: 오용탐지, ㉡: 이상탐지, ㉢: 호스트 기반

정답 1번

출제 포인트

침입 탐지 기법을 비교 대상에 따라 이상탐지와 오용탐지로 구분하고, IDS의 감시 위치에 따라 네트워크 기반과 호스트 기반을 구분하는 문제이다.

핵심 개념

이상탐지는 정상적인 활동의 기준이나 프로파일을 만들고, 현재 활동이 그 기준에서 벗어나는지를 탐지하는 기법이다.
오용탐지는 알려진 공격패턴이나 시그니처와 현재 활동을 대조하여 침입을 탐지하는 기법이다.
네트워크 기반 IDS는 네트워크 구간의 패킷을 수집·분석하고, 호스트 기반 IDS는 개별 호스트의 로그·파일·프로세스 등의 활동을 분석한다.

선지별 해설

① O — ㉠은 정상 활동 데이터베이스와 비교하므로 이상탐지, ㉡은 공격패턴·시그니처 데이터베이스와 비교하므로 오용탐지, ㉢은 네트워크상의 패킷을 캡처·분석하므로 네트워크 기반 IDS이다. 세 용어가 모두 바르게 연결되었다.
② X — 틀린 표현은 ㉢의 '호스트 기반'이다. 네트워크상의 모든 패킷을 캡처하여 분석하는 IDS는 네트워크 기반 IDS이다. 따라서 올바른 연결은 '㉠: 이상탐지, ㉡: 오용탐지, ㉢: 네트워크 기반'이다.
③ X — 틀린 표현은 ㉠의 '오용탐지'와 ㉡의 '이상탐지'이다. 정상 활동을 기준으로 비교하는 ㉠은 이상탐지이고, 공격패턴·시그니처를 기준으로 비교하는 ㉡은 오용탐지이다. ㉢의 네트워크 기반 연결만 옳다.
④ X — ㉠과 ㉡이 서로 뒤바뀌었고, ㉢의 '호스트 기반'도 틀렸다. 올바르게는 ㉠은 이상탐지, ㉡은 오용탐지, ㉢은 네트워크 기반 IDS이다.

NoteBase

오답 포인트

‘정상 활동’과 ‘공격패턴’이라는 비교 기준을 반대로 연결하거나, 패킷을 분석한다는 문구를 개별 컴퓨터 내부를 감시하는 호스트 기반 IDS로 착각하기 쉽다.

다시 나오면 이렇게 판단

정상 상태와의 편차를 찾으면 이상탐지, 알려진 공격 서명과 일치하는지를 찾으면 오용탐지로 판단한다.
네트워크 패킷을 감시하면 네트워크 기반, 개별 호스트 내부의 로그나 파일 변화를 감시하면 호스트 기반으로 판단한다.

암기 포인트

정상에서 벗어나면 이상탐지, 공격 서명과 맞으면 오용탐지, 패킷을 보면 네트워크 기반이다.

NoteBase

문 18. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 설명 중 가장 옳지 않은 것은?

① LISTENING : 연결을 위해 접속을 대기하고 있는 상태

② CLOSE_WAIT : 연결 종료 메시지를 수신하고 그에 대한 확인메시지를 보낸 상태

③ ESTABLISHED : 완전히 종료된 상태

④ TIME_WAIT : 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태

정답 3번

출제 포인트

TCP 연결 상태를 나타내는 LISTENING, CLOSE_WAIT, ESTABLISHED, TIME_WAIT의 의미를 구별하는 문제이다.

핵심 개념

LISTENING은 서버가 연결 요청을 기다리는 상태이고, ESTABLISHED는 양쪽 사이의 연결이 성립된 상태이다. CLOSE_WAIT는 상대방의 연결 종료 요청을 확인한 뒤 로컬 프로그램의 종료 처리를 기다리는 상태이며, TIME_WAIT는 연결 종료 후 지연된 패킷의 소멸과 마지막 확인 응답의 재전송 가능성에 대비해 일정 시간 기다리는 상태이다.

선지별 해설

① O — LISTENING은 서버 소켓이 클라이언트의 연결 요청을 받아들이기 위해 대기하는 상태이다.
② O — CLOSE_WAIT는 상대방의 연결 종료 메시지인 FIN을 받고 ACK를 보낸 뒤, 로컬 프로그램이 소켓을 닫기를 기다리는 상태이다.
③ X — 틀린 표현은 '완전히 종료된 상태'이다. ESTABLISHED는 TCP 연결이 정상적으로 성립되어 데이터를 송수신할 수 있는 상태이다. 완전히 종료된 상태가 아니다.
④ O — TIME_WAIT는 능동적으로 연결을 종료한 쪽이 연결 종료 후 일정 시간 대기하는 상태이다. 지연된 패킷이 사라지고 필요하면 마지막 ACK를 다시 보낸 뒤 동일한 연결 정보가 재사용되도록 하는 상태이므로, 연결 종료 후 다음 연결을 위한 대기 상태라는 설명은 타당하다.

오답 포인트

③의 ESTABLISHED를 연결 절차가 '끝났다'는 뜻으로 오해하기 쉽다. 여기서 established는 종료가 아니라 연결의 성립을 뜻한다. 또한 CLOSE_WAIT와 TIME_WAIT는 모두 종료 과정에서 보이지만, CLOSE_WAIT는 로컬 프로그램의 종료를 기다리고 TIME_WAIT는 네트워크상의 지연 패킷과 마지막 ACK 처리에 대비한다는 차이가 있다.

NoteBase

다시 나오면 이렇게 판단

상태 이름을 연결의 단계와 연결한다. LISTENING은 연결 요청 대기, ESTABLISHED는 연결 성립과 통신, CLOSE_WAIT는 상대의 종료 요청을 받은 뒤 로컬 종료 대기, TIME_WAIT는 종료 후 안전한 재사용을 위한 시간 대기이다.

암기 포인트

ESTABLISHED는 통신 중, CLOSE_WAIT는 내 프로그램의 종료 대기, TIME_WAIT는 종료 후 시간 대기이다.

NoteBase

문 19. 다음 중 ESM(Enterprise Security Management) 기능으로 가장 옳지 않은 것은?

① 트래픽 조절 : 네트워크상의 트래픽 조절을 통한 연구생산성과 안정적인 성능을 지원 및 중요 트래픽의 대역폭 우선순위를 조절하여 안정적이고 신뢰성 있는 통신을 제공

② 통합관리 : 다양한 시스템에서 발생되는 이벤트를 로그화하여 관리자가 필요로 하는 모든 정보(Error, Warning, Notice, Account)를 손쉽게 검색

③ 종합관제 : 통합 관리 기능을 수행하기 위한 인터페이스를 제공하여, 다양한 보안시스템(방화벽, IDS, Scanner)에서 보내온 데이터에 의한 공격 유형, 공격자 정보, 발생 일시, 적용 필터 등을 실시간 모니터링하여 종합적으로 관리

④ 운영관리 : 관리자 관리, 권한별 접근 관리, 실시간 연결 데이터 관리 등을 통해, 관리자가 시스템을 보다 더 체계적으로 운영할 수 있도록 지원

정답 1번

출제 포인트

ESM의 통합 보안관리 기능과 네트워크의 트래픽 품질 관리 기능을 구별하는 문제이다.

핵심 개념

ESM(Enterprise Security Management)은 방화벽, IDS, 취약점 스캐너 등 여러 보안시스템에서 발생한 이벤트와 로그를 한곳에 모아 분석·검색·모니터링하고, 관리와 대응을 지원하는 통합 보안관리 체계이다. 반면 트래픽의 대역폭과 우선순위를 조절하여 통신 품질을 보장하는 것은 QoS 또는 네트워크 트래픽 관리의 영역이다.

선지별 해설

① X — 틀린 부분은 '네트워크상의 트래픽 조절'과 '중요 트래픽의 대역폭 우선순위 조절'을 ESM 기능으로 본 것이다. 이는 패킷 전송 품질과 대역폭을 제어하는 QoS·트래픽 관리 기능이다. 올바르게는 ESM이 여러 보안장비의 이벤트와 로그를 통합 수집·분석하고 보안상황의 관제와 대응을 지원한다고 해야 한다.
② O — 여러 시스템에서 발생한 이벤트를 로그로 통합하여 오류, 경고, 알림, 계정 관련 정보 등을 검색하게 하는 것은 ESM의 로그 통합관리 기능에 해당한다.
③ O — 방화벽, IDS, 스캐너 등 이기종 보안시스템의 데이터를 연계하여 공격 유형, 공격자 정보, 발생 일시, 적용 필터 등을 실시간으로 모니터링하는 것은 ESM의 종합관제 기능에 해당한다.
④ O — 관리자와 권한별 접근을 관리하고 실시간 연결 데이터를 관리하는 기능은 ESM 자체의 안전하고 체계적인 운영을 지원하는 운영관리 기능에 해당한다.

NoteBase

오답 포인트

①은 '트래픽 조절'이라는 표현 때문에 보안관리 기능처럼 보이지만, 핵심은 보안 이벤트가 아니라 대역폭과 우선순위 제어이다. 보안 로그의 수집·분석·관제는 ESM이고, 통신 품질을 위한 대역폭 제어는 QoS이다.

다시 나오면 이렇게 판단

선지의 목적어를 확인한다. 이벤트·로그·경보·보안장비 연동·실시간 보안 모니터링이면 ESM이고, 대역폭·전송 우선순위·통신 품질 제어이면 QoS 또는 트래픽 관리이다.

암기 포인트

ESM은 보안 이벤트를 통합하고, QoS는 네트워크 트래픽을 조절한다.

NoteBase

문 20. 다음 중 무선랜의 보안을 강화하기 위한 대책으로 가장 안전하지 않은 것은?

① 무선랜 AP(Access Point) 접속시 데이터 암호화와 사용자 인증 기능을 제공하도록 한다.

② 무선랜 AP에 MAC(Media Access Control) 주소를 필터링하여 등록된 MAC 주소만 허용하는 정책을 설정한다.

③ 무선랜 AP에 보안을 위해 무지향성 안테나를 사용한다.

④ 무선랜 SSID(Service Set ID)를 숨김으로 설정하여 폐쇄시스템을 운영하면 SSID를 모르는 사용자의 접속시도가 현저하게 줄어든다.

정답 3번

출제 포인트

무선랜 보안 대책이 통신 내용 보호, 사용자 인증, 접속 통제, 전파 도달 범위 축소에 실제로 도움이 되는지를 구별하는 문제이다.

핵심 개념

무선랜 보안은 암호화와 인증을 기본으로 하고, MAC 주소 필터링·SSID 숨김·안테나 방향 및 송신 출력 조절 등을 보조 수단으로 사용한다. 무지향성 안테나는 전파를 여러 방향으로 넓게 방사하므로 보안을 위한 전파 노출 범위 제한에는 불리하다.

선지별 해설

① O — 데이터 암호화는 무선 구간에서 전송 내용이 노출되는 것을 막고, 사용자 인증은 허가된 이용자인지를 확인하므로 핵심적인 무선랜 보안 대책이다.
② O — 등록된 MAC 주소만 허용하면 미등록 단말의 접속을 제한할 수 있다. 다만 MAC 주소는 위조될 수 있으므로 암호화·인증과 함께 사용하는 보조 수단이다.
③ X — '보안을 위해 무지향성 안테나를 사용한다'는 표현이 틀렸다. 무지향성 안테나는 전파를 사방으로 넓게 보내 외부에서도 신호를 수신할 가능성을 키운다. 올바르게는 지향성 안테나를 사용하고 설치 위치와 송신 출력을 조절하여 전파가 필요한 구역 밖으로 퍼지는 범위를 줄이는 것이 보안에 유리하다.
④ O — SSID를 숨기면 일반적인 무선망 검색 화면에 네트워크 이름이 드러나지 않아 우발적이거나 단순한 접속 시도를 줄이는 보조 효과가 있다. 다만 SSID는 무선 패킷 분석으로 알아낼 수 있으므로 이것만으로 접속을 안전하게 차단할 수는 없다.

오답 포인트

③의 '무지향성'이 넓은 서비스 범위에는 유리하다는 점을 보안에도 유리하다고 착각하기 쉽다. 또한 ②의 MAC 필터링과 ④의 SSID 숨김은 우회 가능하지만, 보조 대책으로서의 효과가 전혀 없는 것은 아니다.

NoteBase

다시 나오면 이렇게 판단

무선랜 보안 선지는 먼저 암호화·인증·접속 통제 여부를 확인하고, 안테나 관련 선지는 전파가 필요한 공간 밖까지 퍼지는지를 판단한다. 전파 노출 범위를 넓히는 방식은 보안 강화책으로 보기 어렵다.

암기 포인트

무선랜은 암호화·인증이 기본이고, 전파는 필요한 구역 안으로 좁게 제한하는 것이 안전하다.

NoteBase