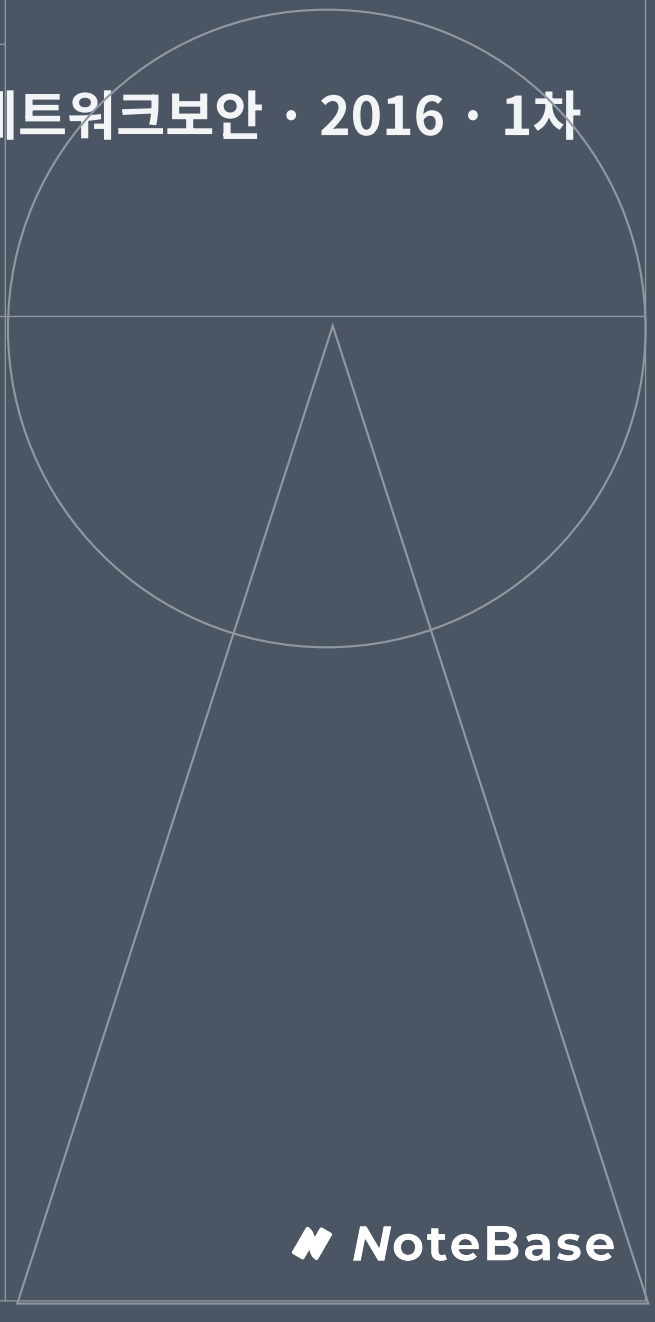
기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2016 · 1차



NoteBase

기출OX 해설집

공무원/해경/일반직 9급 · 네트워크보안 · 2016 · 1차

공무원/해경/일반직 9급 · 네트워크보안 · 2016 · 1차

문 1. 다음 중 물리계층 프로토콜과 관계가 가장 먼 것은?

① RS-232C

② i430

③ X.25

④ RS-449

정답 3번

출제 포인트

OSI 물리 계층의 인터페이스 표준과 네트워크 계층의 패킷 교환 프로토콜을 구별하는 문제이다.

핵심 개념

물리 계층은 전송 매체를 통해 비트를 보내기 위한 기계적·전기적·기능적·절차적 인터페이스를 다룬다. RS-232C, I.430, RS-449는 이러한 물리 인터페이스와 직접 관련된다. 반면 X.25는 공중 패킷 교환망에서 단말과 망 사이의 통신을 규정하는 프로토콜 체계이며, 핵심인 패킷 계층은 OSI 네트워크 계층에 대응한다.

선지별 해설

① X — RS-232C는 단말 장치와 통신 장치 사이의 직렬 통신 인터페이스에 관한 표준으로, 전기적 신호와 접속 기능 등을 규정하므로 물리 계층과 직접 관련된다. '물리 계층과 관계가 가장 멀다'가 아니라 '물리 계층의 직렬 인터페이스 표준'으로 고쳐야 한다.

② X — i430은 통상 I.430을 뜻하며, ISDN 기본 속도 접속의 사용자-망 인터페이스에서 계층 1 특성을 규정하므로 물리 계층과 직접 관련된다. '물리 계층과 관계가 가장 멀다'가 아니라 'ISDN 기본 속도 접속의 물리 계층 규격'으로 고쳐야 한다.

③ O — X.25는 패킷 교환망의 단말-망 인터페이스를 규정하고, 그 중심인 패킷 계층 프로토콜이 OSI 네트워크 계층에 대응한다. 따라서 나머지 물리 인터페이스 표준들보다 물리 계층과의 관계가 가장 멀다.

④ X — RS-449는 직렬 데이터 통신 인터페이스의 기계적·기능적 특성을 규정하고 전기적 특성은 RS-422·RS-423 계열과 연계되는 물리 계층 관련 표준이다. '물리 계층과 관계가 가장 멀다'가 아니라 '물리 계층의 직렬 인터페이스 표준'으로 고쳐야 한다.

NoteBase

오답 포인트

X.25 체계에도 하위 계층 규격이 포함될 수 있다는 점 때문에 혼동하기 쉽다. 그러나 선지 중 RS-232C, I.430, RS-449는 물리 인터페이스 자체를 직접 규정하는 반면, X.25를 대표하는 패킷 계층 기능은 네트워크 계층에 해당한다는 차이가 핵심이다.

다시 나오면 이렇게 판단

커넥터, 신호, 전기적 특성, 직렬 인터페이스, 계층 1이라는 단서가 있으면 물리 계층으로 판단한다. 패킷의 설정·전달과 논리적 경로를 다루면 네트워크 계층으로 판단한다.

암기 포인트

RS-232C·I.430·RS-449는 물리 인터페이스, X.25의 핵심은 네트워크 계층의 패킷 전달이다.

NoteBase

문 2. 다음 지문에서 설명하고 있는 것은 무엇인가?

침입차단시스템(Firewall), 침입탐지시스템(IDS), 가상 사설망(VPN) 등 서로 다른 보안제품에서 발생하는 정보를 한 곳에서 모으는 역할을 하는 보안관제시스템

① ESM
② NMS
③ TMS
④ IPS

정답 1번

출제 포인트

서로 다른 보안제품에서 발생한 정보를 중앙에 모아 통합적으로 관리·분석하는 보안관제시스템이 ESM임을 구별하는 문제이다.

핵심 개념

ESM(Enterprise Security Management)은 방화벽, IDS, VPN 등 여러 보안제품의 로그와 이벤트를 중앙에서 수집하고 연계·분석하여 보안 상태를 통합 관리하는 시스템이다.
NMS는 네트워크 장비의 상태·성능·장애를 관리하고, TMS는 네트워크 트래픽에서 위협을 탐지·분석하며, IPS는 침입 행위를 탐지한 뒤 차단한다.

선지별 해설

① O — ESM은 서로 다른 보안제품에서 발생한 정보를 한곳에 모아 통합 관제하는 시스템이므로 지문의 설명과 일치한다.
② X — NMS라고 본 부분이 틀렸다. NMS(Network Management System)는 라우터·스위치 등 네트워크 장비의 상태, 성능, 구성 및 장애를 감시·관리하는 시스템이다. 지문처럼 여러 보안제품의 정보를 통합 관리하는 것은 ESM이다.
③ X — TMS라고 본 부분이 틀렸다. TMS(Threat Management System)는 네트워크 트래픽과 위협 정보를 수집·분석하여 공격 징후와 유해 트래픽을 탐지하는 시스템이다. 이 문항에서 여러 종류의 보안제품 정보를 중앙에 통합하는 시스템은 ESM이다.
④ X — IPS라고 본 부분이 틀렸다. IPS(Intrusion Prevention System)는 네트워크상의 침입이나 악성 트래픽을 탐지하고 실시간으로 차단하는 시스템이다. 여러 보안제품의 정보를 한곳에 모아 관제하는 시스템은 ESM이다.

NoteBase

오답 포인트

보안 관련 정보를 수집한다는 공통점만 보고 TMS를 고르기 쉽다. 그러나 지문의 핵심 표현은 '서로 다른 보안제품'과 '한 곳에서 모으는'이며, 이는 개별 위협 탐지보다 여러 보안솔루션의 중앙 통합관리를 뜻한다.

다시 나오면 이렇게 판단

여러 보안제품의 로그·이벤트를 중앙에서 통합하면 ESM, 네트워크 장비의 상태·장애를 관리하면 NMS, 트래픽 위협을 분석하면 TMS, 침입 트래픽을 직접 차단하면 IPS로 판단한다.

암기 포인트

ESM은 보안제품 통합관제, NMS는 네트워크 관리, TMS는 위협 분석, IPS는 침입 차단이다.

NoteBase

문 3. 다음에서 허니팟(honeypot)이 갖는 고유 특징에 대한 설명으로 옳지 않은 것은?

① 공격자의 행동 패턴에 대한 유용한 정보를 수집할 수 있다.

② 중요한 시스템을 보호하기 위해서 잠재적 공격자를 유혹한다.

③ 시스템을 관찰하고 침입을 방지할 수 있는 규칙이 적용된다.

④ 대응책을 강구하기에 충분한 시간 동안 공격자가 머물게 한다.

정답 3번

출제 포인트

허니팟의 유인·관찰 기능과 침입방지시스템의 탐지·차단 기능을 구별하는 문제이다.

핵심 개념

허니팟은 공격자가 접근하도록 의도적으로 마련한 미끼 시스템 또는 자원으로, 공격을 유인하고 공격자의 행위와 기법에 관한 정보를 수집한다. 허니팟은 실제 중요 시스템을 직접 보호하는 차단 장비가 아니라 관찰과 분석을 위한 기만 수단이다. 반면 침입방지시스템(IPS)은 트래픽이나 행위를 탐지 규칙과 정책에 따라 검사하고 악성 활동을 차단한다.

선지별 해설

① O — 허니팟에 대한 접근과 활동은 공격자의 행동 패턴, 사용 도구, 공격 기법을 분석하는 자료가 되므로 옳다.
② O — 공격자를 실제 중요 시스템이 아닌 미끼 시스템으로 유인하여 중요 자원에 대한 위험을 줄이는 것이 허니팟의 목적 중 하나이므로 옳다.
③ X — 틀린 부분은 '침입을 방지할 수 있는 규칙이 적용된다'이다. 규칙이나 정책을 이용해 침입을 탐지하고 차단하는 것은 침입방지시스템(IPS)의 기능이다. 허니팟은 공격자를 유인한 뒤 그 활동을 관찰하고 정보를 수집하는 시스템이라고 고쳐야 한다.
④ O — 공격자가 허니팟 안에서 활동하도록 붙잡아 두면 공격을 분석하고 실제 시스템을 방어할 대응책을 마련할 시간을 확보할 수 있으므로 옳다.

오답 포인트

③의 '시스템을 관찰한다'는 표현만 보면 허니팟처럼 보이지만, '규칙을 적용하여 침입을 방지한다'는 부분은 IPS의 능동적 차단 기능이다. 허니팟의 핵심은 직접 차단이 아니라 유인·관찰·정보 수집이다.

다시 나오면 이렇게 판단

미끼 환경으로 공격자를 끌어들여 행동을 기록하고 분석하면 허니팟이고, 규칙이나 정책으로 침입을 탐지하여 실제로 차단하면 IPS로 판단한다.

NoteBase

암기 포인트

허니팟은 유인·관찰·수집, IPS는 탐지·차단이다.

NoteBase

문 4. 서비스 거부 공격 방법이 아닌 것은?

① ARP spoofing

② Smurf

③ SYN flooding

④ UDP flooding

정답 1번

출제 포인트

서비스 거부 공격은 대량의 트래픽이나 불완전한 연결을 유발하여 대상 시스템의 대역폭·연결 자원·처리 능력을 고갈시키는 공격이다. 이 문제는 서비스 가용성을 떨어뜨리는 공격과 ARP 주소 대응 관계를 조작하는 공격을 구별하는 문제이다.

핵심 개념

ARP spoofing은 위조된 ARP 정보를 보내 IP 주소와 MAC 주소의 대응 관계를 변조하는 공격이며, 주된 목적은 공격자가 통신 경로에 끼어드는 중간자 공격이나 트래픽 도청·변조이다.
Smurf는 출발지 IP 주소를 피해자의 주소로 위조한 ICMP Echo Request를 브로드캐스트하여 다수의 응답이 피해자에게 몰리게 하는 증폭형 서비스 거부 공격이다.
SYN flooding은 TCP 3-way handshake를 끝내지 않은 반개방 연결을 대량으로 만들어 서버의 연결 자원을 소진시키는 서비스 거부 공격이다.
UDP flooding은 대량의 UDP 패킷을 전송하여 대상의 대역폭과 처리 자원을 소진시키는 서비스 거부 공격이다.

선지별 해설

① X — ARP spoofing을 서비스 거부 공격 방법으로 분류하는 것은 틀리다. 올바르게는 위조된 ARP 정보로 IP 주소와 MAC 주소의 대응 관계를 변조하여 통신을 가로채거나 조작하는 공격이다. 따라서 문제에서 묻는 '서비스 거부 공격 방법이 아닌 것'에 해당한다.
② O — Smurf 공격은 피해자의 IP 주소로 출발지를 위조한 ICMP 요청을 브로드캐스트하고, 여러 호스트의 응답을 피해자에게 집중시켜 트래픽을 증폭하는 서비스 거부 공격이다.
③ O — SYN flooding은 다수의 SYN 패킷을 보낸 뒤 연결을 완성하지 않아 서버의 반개방 연결 큐와 자원을 고갈시키는 서비스 거부 공격이다.
④ O — UDP flooding은 대량의 UDP 패킷으로 네트워크 대역폭과 대상 시스템의 패킷 처리 자원을 소진시키는 서비스 거부 공격이다.

NoteBase

오답 포인트

ARP spoofing도 통신 장애를 일으킬 수 있어 서비스 거부 공격처럼 보일 수 있다는 점이 함정이다. 그러나 공격의 대표적인 분류 기준은 직접적인 자원 고갈이 아니라 ARP 캐시의 주소 대응 관계 조작이며, Smurf·SYN flooding·UDP flooding은 모두 대상의 가용성을 떨어뜨리는 전형적인 서비스 거부 공격이다.

다시 나오면 이렇게 판단

공격이 대량의 응답·패킷·반개방 연결로 자원을 고갈시키는지 먼저 확인한다. 자원 고갈이 핵심이면 서비스 거부 공격으로, IP 주소와 MAC 주소의 대응 관계를 속여 통신 경로를 가로채는 것이 핵심이면 ARP spoofing으로 판단한다.

암기 포인트

Smurf는 ICMP 증폭, SYN flooding은 반개방 연결, UDP flooding은 UDP 대량 전송, ARP spoofing은 IP–MAC 대응 관계 변조이다.

NoteBase

문 5. 스니핑(sniffing)을 방지하기 위한 대책으로 올바르지 못한 것은?

① 스위치 포트에 접근 제한을 설정한다.

② 전자메일을 이용할 때에는 IPSec 기술을 사용하여 암호화 한다.

③ 원격 접속 프로그램으로는 telnet 대신 ssh 프로토콜을 이용한다.

④ VPN을 이용하여 네트워크 구간을 암호화 한다.

정답 2번

출제 포인트

스니핑 방지 대책을 접근 통제와 통신 내용 암호화로 구분하고, 보호 대상에 맞는 보안 기술을 선택할 수 있는지를 묻는 문제이다.

핵심 개념

스니핑은 네트워크를 흐르는 패킷을 가로채 그 내용을 엿보는 행위이다. 접근 통제는 공격자의 네트워크 진입과 패킷 수집 기회를 줄이고, 암호화는 패킷이 수집되더라도 내용을 알아보기 어렵게 한다. 전자메일 자체의 암호화에는 대표적으로 PGP나 S/MIME을 사용하며, IPsec은 IP 계층에서 IP 패킷을 보호하는 기술이다.

선지별 해설

① O — 스위치 포트에 접근 제한을 설정하면 허가되지 않은 단말의 접속이나 포트 악용을 줄여 스니핑 기회를 제한할 수 있다.
② X — 틀린 부분은 전자메일을 이용할 때 'IPSec 기술을 사용하여 암호화한다'는 표현이다. IPsec은 IP 계층의 통신을 보호하는 기술이며, 전자메일 메시지 자체를 암호화하는 대표 기술은 PGP나 S/MIME이다. 따라서 '전자메일을 이용할 때에는 PGP 또는 S/MIME을 사용하여 메일 내용을 암호화한다'로 고쳐야 한다.
③ O — Telnet은 통신 내용을 평문으로 전송하지만 SSH는 접속 구간을 암호화하므로 원격 접속 정보와 전송 내용을 스니핑으로부터 보호할 수 있다.
④ O — VPN은 공용 네트워크를 지나는 통신 구간에 암호화된 터널을 형성하므로 패킷이 가로채지더라도 내용을 노출하기 어렵게 한다.

오답 포인트

②의 함정은 IPsec도 암호화 기술이라는 사실만 보고 보호 대상을 구분하지 않는 데 있다. IPsec은 IP 패킷과 네트워크 구간을 보호하고, PGP와 S/MIME은 전자메일 메시지 자체를 보호한다.

다시 나오면 이렇게 판단

보안 기술의 이름만 확인하지 않고 보호 계층과 대상을 대응시킨다. 원격 접속은 SSH, 네트워크 구간은 VPN·IPsec, 전자메일 메시지는 PGP·S/MIME으로 구분한다.

NoteBase

암기 포인트

메일은 PGP·S/MIME, IP 구간은 IPsec, 원격 접속은 SSH이다.

NoteBase

문 6. 안드로이드 보안에 대한 설명으로 옳지 않은 것은?

① 리눅스 운영체제와 유사한 보안 취약점을 갖는다.

② 개방형 운영체제로서의 보안정책을 적용한다.

③ 응용프로그램에 대한 전자서명은 개발자가 한다.

④ 응용프로그램 간 데이터 통신을 엄격하게 통제한다.

정답 4번

출제 포인트

안드로이드의 리눅스 기반 구조, 개방형 플랫폼, 응용프로그램 서명, 응용프로그램 간 통신 방식을 구분하는 문제이다.

핵심 개념

안드로이드는 리눅스 커널을 기반으로 하며, 각 응용프로그램을 서로 다른 사용자 ID와 샌드박스로 분리한다. 응용프로그램은 개발자가 서명하고, 서로의 데이터에 임의로 접근할 수는 없지만 Intent, Binder, ContentProvider 같은 통신 수단을 통해 필요한 정보를 주고받을 수 있다. 이때 접근 제한은 권한과 구성요소의 공개 설정에 따라 이루어진다.

선지별 해설

① O — 안드로이드는 리눅스 커널을 기반으로 하므로 커널과 시스템 구성요소에서 리눅스 계열과 공통되거나 유사한 보안 취약점이 나타날 수 있다.
② O — 안드로이드는 소스와 플랫폼 구조가 공개된 개방형 운영체제이며, 이러한 환경에서 샌드박스·권한·서명 등의 보안정책을 적용한다.
③ O — 안드로이드 응용프로그램은 개발자가 자신의 개인키로 전자서명한다. 이 서명은 개발자 식별과 동일 개발자의 업데이트 여부 등을 판단하는 기반이 된다.
④ X — 틀린 표현은 '응용프로그램 간 데이터 통신을 엄격하게 통제한다'이다. 안드로이드는 응용프로그램을 샌드박스로 격리하지만 앱 간 통신 자체를 일률적으로 엄격히 차단하지는 않는다. 올바르게는 응용프로그램 간 통신을 허용하되, 권한과 구성요소의 공개 여부 등에 따라 접근을 통제한다고 해야 한다.

오답 포인트

④의 '엄격하게 통제한다'를 샌드박스와 혼동하기 쉽다. 샌드박스는 다른 앱의 파일과 실행 영역에 대한 임의 접근을 제한하는 장치이지, 앱 간 통신을 전면적으로 막는 장치가 아니다.

NoteBase

다시 나오면 이렇게 판단

안드로이드 보안 선지는 '기본 격리'와 '허용된 통신'을 나누어 판단한다. 앱은 사용자 ID와 샌드박스로 기본 격리되지만, 앱 간 통신은 권한과 구성요소 설정을 조건으로 허용된다.

암기 포인트

안드로이드는 리눅스 기반·개발자 서명·앱별 샌드박스이며, 앱 간 통신은 전면 차단이 아니라 권한 기반 허용이다.

NoteBase

문 7. <보기>의 설명에 해당하는 네트워크 장비는?

<보기>
· OSI계층 모델의 네트워크 계층에서 동작하는 장비이다.
· 송신측과 수신측 간의 가장 빠르고 신뢰성 있는 경로를 설정·관리하며, 데이터를 전달하는 역할을 한다.
· 주로 같은 프로토콜을 사용하는 네트워크간의 최적경로 설정을 위해 패킷이 지나가야 할 정보를 테이블에 저장하여 지정된 경로를 통해 전송한다.

① 게이트웨이(gateway)
② 브리지(bridge)
③ 리피터(repeater)
④ 라우터(router)

정답 4번

출제 포인트

OSI 계층과 데이터 전달 기능을 근거로 네트워크 장비를 구별하는 문제이다. 네트워크 계층, 최적 경로 설정, 라우팅 테이블이라는 단서가 라우터를 가리킨다.

핵심 개념

라우터는 OSI 네트워크 계층에서 목적지 IP 주소와 라우팅 테이블을 바탕으로 패킷의 전달 경로를 선택하고 서로 다른 네트워크 사이로 패킷을 전달하는 장비이다.
리피터는 물리 계층에서 신호를 재생하고, 브리지는 데이터 링크 계층에서 MAC 주소를 기준으로 프레임을 전달하며, 게이트웨이는 서로 다른 프로토콜이나 시스템 사이에서 변환·중계한다.

선지별 해설

① X — 게이트웨이는 서로 다른 프로토콜이나 시스템을 연결하면서 필요한 변환을 수행하는 장비이다. 틀린 대응은 '네트워크 계층에서 최적 경로를 설정하는 장비가 게이트웨이'라는 부분이며, 올바르게는 라우터이다.
② X — 브리지는 데이터 링크 계층에서 MAC 주소를 기준으로 네트워크 세그먼트 사이의 프레임을 전달하거나 걸러 낸다. 틀린 대응은 '네트워크 계층에서 라우팅 테이블로 경로를 정하는 장비가 브리지'라는 부분이며, 올바르게는 라우터이다.
③ X — 리피터는 물리 계층에서 약해지거나 왜곡된 신호를 재생해 전송 거리를 연장한다. 틀린 대응은 '패킷의 최적 경로를 설정하는 장비가 리피터'라는 부분이며, 올바르게는 라우터이다.
④ O — 라우터는 네트워크 계층에서 동작하며, 라우팅 테이블을 이용해 목적지까지의 경로를 선택하고 패킷을 전달한다. 보기의 세 단서와 모두 일치한다.

NoteBase

오답 포인트

여러 장비가 모두 네트워크를 연결한다는 공통점만 보면 게이트웨이나 브리지와 혼동하기 쉽다. 이 문항에서는 ‘네트워크 계층’, ‘최적 경로’, ‘라우팅 테이블’이 결정적인 표현이다.

다시 나오면 이렇게 판단

계층과 판단 기준을 함께 확인한다. 물리 계층의 신호 재생은 리피터, 데이터 링크 계층의 MAC 주소 기반 전달은 브리지, 네트워크 계층의 IP 주소·경로 선택은 라우터, 프로토콜 변환은 게이트웨이로 판단한다.

암기 포인트

신호는 리피터, MAC은 브리지, IP와 경로는 라우터, 프로토콜 변환은 게이트웨이이다.

NoteBase

문 8. 가설사설망(VPN)이 제공하는 보안 서비스에 해당하지 않는 것은?

① 패킷 필터링

② 데이터 암호화

③ 접근제어

④ 터널링

정답 1번

출제 포인트

VPN이 제공하는 보안 기능과 방화벽의 대표 기능을 구분하는 문제이다.

핵심 개념

VPN은 공중망에서 사설망처럼 안전하게 통신하도록 데이터를 캡슐화해 터널을 만들고, 암호화와 접근 통제를 적용하는 기술이다. 반면 패킷 필터링은 패킷의 출발지·목적지 주소, 포트, 프로토콜 등의 규칙에 따라 통과 여부를 결정하는 방화벽의 대표 기능이다.

선지별 해설

① O — 패킷 필터링은 방화벽이 통신 허용 여부를 판단하는 대표 기능이며, 이 문항에서 묻는 VPN 자체의 보안 서비스에는 해당하지 않는다.
② X — '데이터 암호화가 VPN 보안 서비스에 해당하지 않는다'는 판단이 틀리다. 실제로 VPN은 전송 데이터를 암호화하여 제3자가 내용을 알아보기 어렵게 하므로 기밀성을 제공한다.
③ X — '접근제어가 VPN 보안 서비스에 해당하지 않는다'는 판단이 틀리다. 실제로 VPN은 인증된 사용자나 장치에 대해 허용된 사설망 자원만 이용하게 하여 접근을 통제한다.
④ X — '터널링이 VPN 보안 서비스에 해당하지 않는다'는 판단이 틀리다. 실제로 VPN은 사설망 패킷을 다른 패킷 안에 캡슐화해 공중망을 통과하는 논리적 터널을 구성한다.

오답 포인트

VPN 장비와 방화벽이 함께 설치되는 경우가 많아 ①의 패킷 필터링을 VPN 고유 기능으로 혼동하기 쉽다. 이 문항에서는 통신 규칙에 따라 패킷을 거르는 기능과, 터널을 만들고 그 안의 통신을 보호하는 기능을 구분해야 한다.

다시 나오면 이렇게 판단

캡슐화·터널 생성, 암호화, 사용자·장치의 접근 통제는 VPN 쪽으로 분류하고, 주소·포트·프로토콜 규칙으로 패킷을 허용하거나 차단하는 기능은 패킷 필터링 방화벽 쪽으로 분류한다.

NoteBase

암기 포인트

VPN은 터널링·암호화·접근제어, 방화벽은 패킷 필터링이다.

NoteBase

문 9. 무선랜 보안 방식인 WEP(Wired Equivalent Privacy)은 일정한 양의 데이터를 분석하면 이로부터 키(key)를 추출할 수 있는 단점이 발견되었다. 802.11i에서 WEP보다 강화된 보안 방식인 WPA 및 WPA2를 제안하는데 개인용은 인증을 위해 어떤 방식을 사용하는지 고르시오.

① 802.11x

② AES(Advanced Encryption Standard)

③ TKIP(Temporary Key Integrity Protocol)

④ PSK(Pre-Shared Key)

정답 4번

출제 포인트

WPA·WPA2의 개인용 모드에서 사용하는 인증 방식과, 기업용 인증 및 암호화 기술을 구별하는 문제이다.

핵심 개념

WPA-Personal과 WPA2-Personal은 미리 공유한 비밀키를 사용하는 PSK 방식이다. 반면 기업용 모드는 보통 802.1X와 인증 서버를 이용한다. AES와 TKIP는 인증 방식이 아니라 무선 구간의 데이터를 보호하는 암호화 관련 기술이다.

선지별 해설

① X — 802.11x는 개인용 WPA·WPA2의 인증 방식이 아니다. 이 문맥에서 구별해야 할 802.1X는 인증 서버와 결합하여 주로 기업용 모드에서 사용하는 접근 인증 방식이며, 개인용은 PSK를 사용한다.
② X — AES는 암호화 알고리즘으로서 WPA2에서 주로 CCMP와 함께 데이터 기밀성과 무결성을 제공한다. 인증 방식이 아니며, 개인용 인증 방식으로 고치면 PSK이다.
③ X — TKIP는 WEP의 취약점을 보완하기 위해 WPA에 도입된 암호화·키 관리 프로토콜이다. 인증 방식이 아니며, 개인용 인증 방식으로 고치면 PSK이다.
④ O — PSK는 접속 장치와 무선 공유기가 사전에 같은 비밀키를 공유하여 인증에 사용하는 방식으로, WPA-Personal과 WPA2-Personal에 해당한다.

오답 포인트

AES와 TKIP가 WPA·WPA2에 실제로 사용된다는 점 때문에 이를 인증 방식으로 혼동하기 쉽다. 그러나 AES·TKIP는 암호화 관련 기술이고, 개인용과 기업용을 가르는 인증 방식은 각각 PSK와 802.1X이다.

다시 나오면 이렇게 판단

문제에서 개인용을 물으면 사전 공유키인 PSK를, 기업용을 물으면 인증 서버 기반의 802.1X를 연결한다.
AES·TKIP가 보이면 인증이 아니라 암호화 기술로 분류한다.

NoteBase

암기 포인트

개인용은 PSK, 기업용은 802.1X, 암호화는 TKIP·AES이다.

NoteBase

문 10. 회선 교환 방식은 정보전송의 필요성이 생겼을 때 상대방을 호출하여 물리적인 연결을 구성한 후 정보를 전송하는 방식을 말한다. 다음 중에서 회선 교환 방식의 특징이 아닌 것은?

① 항상 동일한 경로를 이용하여 전송한다.

② 대체적으로 Point-to-Point의 전송구조를 갖는다.

③ 경로 설정에 짧은 시간이 걸리며 전송지연이 거의 없다.

④ 고정적인 대역폭을 사용한다.

정답 3번

출제 포인트

회선 교환 방식이 통신 전에 전용 경로를 설정하고, 통신 중에는 그 경로와 대역폭을 계속 점유한다는 특징을 묻는 문제이다.

핵심 개념

회선 교환은 송신자와 수신자 사이에 전용 통신 경로를 먼저 설정한 뒤 정보를 연속적으로 전송하는 방식이다. 경로 설정에는 시간이 필요하지만, 설정이 끝난 뒤에는 동일한 경로와 예약된 대역폭을 사용하므로 전송이 안정적이고 지연 변화가 작다.

선지별 해설

① O — 회선이 설정되면 통신이 끝날 때까지 송신자와 수신자 사이의 동일한 전용 경로를 이용한다.
② O — 두 통신 종단을 전용 회선으로 직접 연결하므로 대체로 Point-to-Point 전송 구조를 갖는다.
③ X — 틀린 표현은 '경로 설정에 짧은 시간이 걸리며'이다. 회선 교환은 정보를 보내기 전에 호출과 경로 설정 절차를 거치므로 연결 설정에 시간이 걸린다. 올바르게는 '경로 설정에는 시간이 걸리지만, 일단 연결된 뒤에는 전송지연이 작다'이다.
④ O — 통신이 지속되는 동안 설정된 회선의 대역폭을 전용으로 할당받아 고정적으로 사용한다.

오답 포인트

③은 연결 후의 작은 전송지연을 연결 전의 경로 설정 시간과 섞어 놓았다. 회선 교환은 데이터 전송 단계는 안정적이지만, 그 전에 별도의 연결 설정 시간이 필요하다.

다시 나오면 이렇게 판단

회선 교환의 과정을 '먼저 연결 설정, 그다음 전용 경로로 연속 전송'으로 나누어 판단한다. 설정 시간이 거의 없다는 표현은 회선 교환의 특징과 맞지 않는다.

NoteBase

암기 포인트

회선 교환은 설정은 느리고, 연결 후 전송은 일정하다.

NoteBase

문 11. CIDR을 지원하는 라우팅 프로토콜이 아닌 것은?

① RIPv1

② OSPF

③ BGP-4

④ IS-IS

정답 1번

출제 포인트

CIDR을 지원하려면 라우팅 정보에 네트워크 주소와 함께 접두사 길이(서브넷 마스크)를 전달할 수 있어야 한다는 점을 묻는 문제이다.

핵심 개념

CIDR은 기존의 클래스 A·B·C 경계와 관계없이 접두사 길이로 네트워크 범위를 표현하고 경로를 집약하는 방식이다.
클래스풀 라우팅 프로토콜은 경로 광고에 서브넷 마스크를 포함하지 않지만, 클래스리스 라우팅 프로토콜은 접두사 길이를 함께 전달하므로 CIDR과 VLSM을 지원할 수 있다.

선지별 해설

① O — RIPv1은 경로 갱신 정보에 서브넷 마스크를 포함하지 않는 클래스풀 라우팅 프로토콜이므로 CIDR을 지원하지 않는다. 따라서 문제의 정답이다.
② X — OSPF는 경로 정보에 네트워크 마스크를 포함하는 클래스리스 링크 상태 라우팅 프로토콜이므로 CIDR을 지원한다. 틀린 판단은 OSPF를 CIDR 미지원 프로토콜로 본 부분이며, 올바르게는 OSPF는 CIDR을 지원한다.
③ X — BGP-4는 도달 가능성 정보인 NLRI에 IP 접두사와 접두사 길이를 실어 전달하고 경로 집약을 지원하므로 CIDR을 지원한다. 틀린 판단은 BGP-4를 CIDR 미지원 프로토콜로 본 부분이며, 올바르게는 BGP-4는 CIDR을 지원한다.
④ X — IS-IS는 IP 경로를 접두사와 접두사 길이로 광고하는 클래스리스 링크 상태 라우팅 프로토콜이므로 CIDR을 지원한다. 틀린 판단은 IS-IS를 CIDR 미지원 프로토콜로 본 부분이며, 올바르게는 IS-IS는 CIDR을 지원한다.

오답 포인트

RIP이라는 이름만 보고 모든 RIP 버전을 같은 것으로 판단하는 것이 함정이다. RIPv1은 마스크를 보내지 않는 클래스풀 방식이지만, RIPv2는 마스크를 전달하는 클래스리스 방식이어서 CIDR을 지원한다.

NoteBase

다시 나오면 이렇게 판단

라우팅 갱신에 접두사 길이 또는 서브넷 마스크가 포함되는지를 확인한다. 포함되면 클래스리스 프로토콜로서 CIDR을 지원하고, 포함되지 않으면 클래스풀 프로토콜로서 CIDR을 지원하지 않는다.

암기 포인트

RIPv1은 클래스풀·CIDR 미지원, OSPF·BGP-4·IS-IS는 클래스리스·CIDR 지원이다.

NoteBase

문 12. 최근 많이 발생되는 공격 사례로 인터넷 사용자의 컴퓨터에 침입하여 내부 문서나, 사진파일, 스프레드시트 등 사용자의 파일들을 암호화하여 파일을 열지 못하도록 한 뒤 돈을 보내주면 암호화를 풀 수 있는 프로그램을 전송해 준다며 금품을 요구하는 악성프로그램을 뜻한다. 이러한 공격을 무엇이라고 하는가?

① 랜섬웨어(Ransomware)

② APT(Advanced Persistent Threat)

③ DDoS(Distributed Denial of Service)

④ 스미싱(Smishing)

정답 1번

출제 포인트

파일을 암호화해 사용할 수 없게 만든 뒤 복구를 조건으로 금품을 요구하는 악성프로그램이 랜섬웨어임을 구별하는 문제이다.

핵심 개념

랜섬웨어는 피해자의 파일이나 시스템을 암호화·잠금 처리하고 이를 풀어 주는 대가로 금전을 요구하는 악성프로그램이다. APT는 특정 대상을 장기간 은밀하게 공격하는 위협, DDoS는 다수의 시스템이 대량의 트래픽을 보내 서비스를 마비시키는 공격, 스미싱은 문자메시지의 링크 등을 이용해 악성 앱 설치나 정보 탈취를 유도하는 공격이다.

선지별 해설

① O — 랜섬웨어는 문서·사진·스프레드시트 등의 파일을 암호화하고 복구 프로그램이나 복호화 키 제공을 빌미로 금품을 요구한다. 제시된 설명과 정확히 일치한다.
② X — 틀린 표현은 'APT'이다. APT는 특정 조직이나 시스템을 표적으로 삼아 장기간 지속적이고 은밀하게 침투하는 공격이다. 제시된 악성프로그램은 랜섬웨어이다.
③ X — 틀린 표현은 'DDoS'이다. DDoS는 여러 공격원이 동시에 과도한 트래픽이나 요청을 보내 서버·네트워크의 정상 서비스를 방해하는 공격이다. 파일을 암호화해 금품을 요구하는 공격은 랜섬웨어이다.
④ X — 틀린 표현은 '스미싱'이다. 스미싱은 문자메시지와 피싱을 결합하여 악성 링크 접속, 악성 앱 설치 또는 개인정보·금융정보 탈취를 유도하는 공격이다. 제시된 악성프로그램은 랜섬웨어이다.

오답 포인트

'컴퓨터 침입'이라는 넓은 표현만 보고 APT를 고르기 쉽다. 그러나 이 문항의 결정적 단서는 '파일 암호화'와 '복구를 조건으로 한 금품 요구'이다.

NoteBase

다시 나오면 이렇게 판단

공격의 수단과 목적을 함께 확인한다. 파일 암호화·잠금 후 금품 요구는 랜섬웨어, 장기·표적·은밀한 침투는 APT, 대량 트래픽에 의한 서비스 마비는 DDoS, 문자메시지 링크를 통한 정보 탈취 유도는 스미싱으로 판단한다.

암기 포인트

암호화하고 돈을 요구하면 랜섬웨어이다.

NoteBase

문 13. 침입차단시스템 방식 중에 어플리케이션 게이트웨이방식 설명으로 옳지 않은 것은?

① 외부 네트워크와 내부 네트워크가 프록시 서버를 통해야만 연결이 된다.

② 내부 네트워크에 대한 경계선 방어 및 내부 네트워크에 대한 정보를 숨길 수 있다.

③ 패킷 필터링 방화벽보다 높은 보안성 설정이 가능하다.

④ 하나의 프록시 데몬이 존재한다.

정답 4번

출제 포인트

애플리케이션 게이트웨이 방식의 프록시 중계 구조와 서비스별 프록시 운용 특성을 구별하는 문제이다.

핵심 개념

애플리케이션 게이트웨이는 응용 계층에서 동작하는 프록시가 내부 호스트를 대신해 외부와 통신하도록 하는 방화벽 방식이다. 내부와 외부 사이의 직접 연결을 차단하고 응용 서비스별 통신 내용을 세밀하게 검사할 수 있다. 패킷 필터링 방화벽은 주로 패킷 헤더의 주소, 포트, 프로토콜 등을 기준으로 통과 여부를 판단하지만, 애플리케이션 게이트웨이는 서비스마다 해당 응용 프로토콜을 처리하는 프록시가 필요하다.

선지별 해설

① O — 외부 네트워크와 내부 네트워크는 직접 연결되지 않고 프록시가 각각의 연결을 중계한다. 따라서 허용된 통신은 프록시 서버를 거쳐 이루어진다.
② O — 프록시가 외부와 대신 통신하므로 내부 호스트의 주소와 네트워크 구조를 외부에 직접 노출하지 않으며, 네트워크 경계에서 접근을 통제할 수 있다.
③ O — 응용 계층에서 프로토콜과 명령 수준의 검사가 가능하므로 주소·포트 중심의 패킷 필터링보다 세밀하고 높은 수준의 보안 정책을 설정할 수 있다.
④ X — 틀린 표현은 '하나의 프록시 데몬'이다. 애플리케이션 게이트웨이는 하나의 범용 프록시 데몬만 두는 것이 아니라 HTTP, FTP 등 지원할 응용 서비스별로 별도의 프록시 기능 또는 프록시 데몬을 운용한다.

오답 포인트

프록시 서버가 한 대라는 사실과 프록시 데몬이 하나라는 설명을 혼동하기 쉽다. 한 장비에서 여러 프록시가 실행될 수 있으며, 핵심은 장비 수가 아니라 응용 서비스별 프록시가 필요하다는 점이다.

다시 나오면 이렇게 판단

애플리케이션 게이트웨이는 '응용 계층 검사, 내부·외부 직접 연결 차단, 내부 정보 은닉, 서비스별 프록시'로 판단한다. '하나의 범용 프록시가 모든 응용 서비스를 처리한다'는 표현은 틀린 설명이다.

NoteBase

암기 포인트

애플리케이션 게이트웨이 = 직접 연결 차단 + 응용 서비스별 프록시.

NoteBase

문 14. 다음 설명에 해당하는 컴퓨터 바이러스는?

산업 소프트웨어와 공정 설비를 공격 목표로 하는 극도로 정교한 군사적 수준의 사이버 무기로 지칭된다. 공정 설비와 연결된 프로그램이 논리제어장치(Programmable Logic Controller)의 코드를 악의적으로 변경하여 제어권을 획득한다. 네트워크와 이동저장매체인 USB를 통해 전파되며, SCADA(Supervisory Control and Data Acquisition) 시스템이 공격 목표이다.

① 오토런 바이러스(Autorun virus)

② 백도어(Backdoor)

③ 스턱스넷(Stuxnet)

④ 봇넷(Botnet)

정답 3번

출제 포인트

산업제어시스템을 겨냥하여 PLC 코드를 변조하고 USB와 네트워크로 전파되는 악성코드를 식별하는 문제이다.

핵심 개념

스턱스넷은 SCADA 등 산업제어시스템을 공격하고 PLC의 제어 코드를 악의적으로 변경하여 실제 공정 설비의 동작을 교란하도록 설계된 정교한 악성코드이다.
오토런 바이러스는 이동식 저장매체의 자동 실행 기능을 악용해 전파되고, 백도어는 정상적인 인증 절차를 우회하는 비밀 접근 통로이며, 봇넷은 공격자의 명령을 받는 감염 기기들의 네트워크이다.

선지별 해설

① X — 오토런 바이러스는 주로 이동식 저장매체의 자동 실행 기능을 악용해 전파되는 악성코드이다. 틀린 부분은 산업 소프트웨어와 PLC 코드를 변조해 SCADA를 공격하는 악성코드를 오토런 바이러스로 본 점이다. 올바르게는 스턱스넷이다.
② X — 백도어는 공격자가 정상적인 인증이나 보안 절차를 우회하여 시스템에 접근하도록 만든 비밀 통로이다. 틀린 부분은 PLC 코드 변조와 산업 공정 교란을 백도어의 고유한 설명으로 본 점이다. 올바르게는 스턱스넷이다.
③ O — 스턱스넷은 네트워크와 USB 등을 통해 전파되며, SCADA 환경과 PLC를 겨냥해 제어 코드를 변조하고 산업 공정을 교란하는 악성코드이다. 지문의 핵심 특징과 일치한다.
④ X — 봇넷은 악성코드에 감염되어 공격자의 명령·제어 아래 놓인 다수의 기기로 구성된 네트워크이다. 틀린 부분은 특정 산업제어시스템의 PLC 코드를 변조하는 악성코드를 봇넷으로 본 점이다. 올바르게는 스턱스넷이다.

NoteBase

오답 포인트

지문에 USB 전파가 제시되어 ① 오토런 바이러스를 고르기 쉽다. 그러나 정답을 가르는 표현은 USB 자체가 아니라 'SCADA 공격', 'PLC 코드의 악의적 변경', '산업 공정 설비의 제어권 획득'이며, 이 특징들은 스턱스넷을 가리킨다.

다시 나오면 이렇게 판단

악성코드 식별 문제에서는 전파 수단보다 공격 대상과 수행 행위를 먼저 확인한다. SCADA·PLC·산업 공정 제어가 함께 나오면 스턱스넷으로 판단한다.

암기 포인트

스턱스넷은 USB·네트워크로 침투하여 SCADA의 PLC 코드를 변조하는 산업제어시스템 공격 악성코드이다.

NoteBase

문 15. TCP와 UDP를 비교한 것 중 잘못된 것은 ?

① UDP는 비연결형 서비스이고, TCP는 연결형 서비스이다.

② TCP는 수신순서가 데이터의 송신순서와 동일하지만, UDP는 송신순서와 다를 수 있다.

③ TCP는 바이트 스트림 단위로, UDP는 블록단위로 비트정보를 전송한다.

④ TCP와 UDP는 오류제어와 흐름제어 기능을 수행한다.

정답 4번

출제 포인트

TCP와 UDP의 연결 방식, 데이터 전달 단위, 순서 보장, 오류제어 및 흐름제어의 차이를 묻는 문제이다.

핵심 개념

TCP는 연결을 설정한 뒤 신뢰성 있게 바이트 스트림을 전달하는 전송계층 프로토콜이다. 순서 제어, 재전송을 통한 오류제어, 흐름제어를 제공한다.
UDP는 연결 설정 없이 데이터그램 단위로 전송하는 전송계층 프로토콜이다. 메시지 경계는 유지하지만 도착 순서, 재전송, 흐름제어를 보장하지 않는다. UDP 체크섬은 오류를 검출할 수 있으나 손실되거나 손상된 데이터그램을 복구하는 오류제어 기능은 아니다.

선지별 해설

① O — UDP는 연결 설정 과정이 없는 비연결형 서비스이고, TCP는 통신 전에 연결을 설정하는 연결형 서비스이다.
② O — TCP는 순서번호를 이용해 수신 측에 송신 순서대로 바이트를 전달한다. UDP는 데이터그램의 도착 순서를 보장하거나 순서를 복구하지 않으므로 송신 순서와 다르게 전달될 수 있다.
③ O — TCP는 메시지 경계를 구분하지 않는 바이트 스트림 방식이고, UDP는 하나의 메시지 경계를 유지하는 데이터그램, 즉 블록 단위 방식이다.
④ X — 틀린 부분은 'TCP와 UDP는 오류제어와 흐름제어 기능을 수행한다'이다. 올바르게는 TCP가 재전송 등의 오류제어와 수신 능력에 맞춘 흐름제어를 수행하고, UDP는 이러한 오류제어와 흐름제어를 제공하지 않는다.

오답 포인트

UDP에 체크섬 필드가 있다는 사실을 UDP도 오류제어를 수행한다는 뜻으로 오해하기 쉽다. 체크섬은 전송 오류를 검출하는 수단이며, UDP 자체에는 재전송이나 순서 복구 같은 오류 복구와 흐름제어 기능이 없다.

다시 나오면 이렇게 판단

연결 설정·신뢰성·순서 보장·재전송·흐름제어가 제시되면 TCP의 특성으로 판단한다.
비연결·데이터그램·메시지 경계 유지·순서와 전달 비보장이 제시되면 UDP의 특성으로 판단한다.

NoteBase

암기 포인트

TCP는 연결형 바이트 스트림과 신뢰성 제어, UDP는 비연결형 데이터그램과 최소 기능이다.

NoteBase

문 16. 이더넷(Ethernet) MAC(Media Access Control) Address를 정의하는 표준 Format은 몇 비트인가?

① 8bit

② 16bit

③ 48bit

④ 64bit

정답 3번

출제 포인트

이 문제는 이더넷 MAC 주소의 표준 길이가 48비트라는 점을 묻는다.

핵심 개념

이더넷 MAC 주소는 네트워크 인터페이스를 식별하는 데이터 링크 계층의 주소이며, 표준 길이는 48비트, 즉 6옥텟이다. 일반적으로 각 옥텟을 두 자리 16진수로 나타내어 모두 12개의 16진수 문자로 표현한다.

선지별 해설

① X — 8bit는 1옥텟에 불과하다. 틀린 표현은 '8bit'이며, 이더넷 MAC 주소의 표준 길이는 48bit이다.
② X — 16bit는 2옥텟으로 MAC 주소 전체 길이가 아니다. 틀린 표현은 '16bit'이며, 올바른 값은 48bit이다.
③ O — 48bit는 6옥텟이며, 이더넷에서 사용하는 표준 MAC 주소의 길이이다.
④ X — 64bit는 표준 이더넷 MAC 주소의 길이가 아니다. 틀린 표현은 '64bit'이며, 올바른 값은 48bit이다.

오답 포인트

주소를 16진수로 표기한다는 사실과 주소 길이를 혼동하면 16bit를 고르기 쉽다. 16진수는 표기 방식이고, MAC 주소 자체의 길이는 48비트이다.

다시 나오면 이렇게 판단

MAC 주소의 길이를 물으면 '6옥텟 × 옥텟당 8비트 = 48비트'의 관계로 판단한다.

암기 포인트

MAC 주소는 48비트, 6옥텟, 16진수 12자리이다.

NoteBase

문 17. 다음 지문은 무엇에 대한 설명인가?

패킷이 목적지까지 도달하는 동안 거치는 라우터 IP를 확인하는 도구이다. 이 도구는 udp와 icmp, ip의 ttl값을 이용한다. 명령어에 대한 결과에서 응답시간이 *로 표시되는 경우 침입차단시스템 등의 접근통제리스트에 의해 패킷이 차단되었음을 확인할 수 있다.

① traceroute

② ping

③ netstat

④ route

정답 1번

출제 포인트

목적지까지 거치는 라우터를 TTL과 ICMP 응답으로 추적하는 명령어를 구별하는 문제이다.

핵심 개념

traceroute는 TTL을 점차 증가시킨 탐사 패킷을 보내고, 중간 라우터가 반환하는 ICMP Time Exceeded 응답을 이용하여 목적지까지의 홉을 확인하는 도구이다. Unix 계열에서는 일반적으로 UDP 탐사 패킷을 사용하며 구현에 따라 ICMP 등을 사용할 수 있다. 응답이 *로 표시되면 제한 시간 안에 응답을 받지 못했다는 뜻이며, 방화벽·침입차단시스템의 필터링이나 패킷 손실 등이 원인일 수 있다.
ping은 목적지의 도달 가능성과 왕복 시간을 확인하고, netstat은 호스트의 네트워크 연결·포트·통계 정보를 확인하며, route는 라우팅 테이블을 조회하거나 설정한다.

선지별 해설

① O — traceroute는 TTL 값을 단계적으로 늘려 각 홉에서 돌아오는 ICMP 응답을 수집하므로, 목적지까지 거치는 라우터의 IP와 응답 시간을 확인한다. 지문의 설명과 일치한다.
② X — ping이라는 표현이 틀렸다. ping은 주로 ICMP Echo Request와 Echo Reply를 이용하여 특정 목적지의 도달 가능성과 왕복 시간을 확인하는 도구이다. 경로상의 라우터를 홉별로 추적하는 도구는 traceroute이다.
③ X — netstat이라는 표현이 틀렸다. netstat은 현재 네트워크 연결, 수신 대기 포트, 인터페이스 또는 프로토콜 통계 등을 확인하는 도구이다. TTL을 증가시키며 중간 라우터의 IP를 추적하는 도구는 traceroute이다.
④ X — route라는 표현이 틀렸다. route는 호스트의 라우팅 테이블을 조회하거나 경로 항목을 추가·삭제하는 도구이다. 패킷이 실제로 거치는 라우터를 차례로 확인하는 도구는 traceroute이다.

NoteBase

오답 포인트

ping도 ICMP와 응답 시간을 사용하므로 혼동하기 쉽다. 그러나 목적지 하나의 도달 여부와 왕복 시간을 확인하면 ping이고, TTL을 증가시키며 중간 홉을 하나씩 드러내면 traceroute이다. 또한 * 표시는 응답 시간 초과를 뜻하므로 접근통제에 의한 차단 가능성을 시사하지만, 그 자체만으로 차단 원인을 단정하지는 못한다.

다시 나오면 이렇게 판단

문제에서 '거치는 라우터', '홉', 'TTL 증가', 'ICMP Time Exceeded'가 함께 제시되면 traceroute로 판단한다. '목적지 도달 여부·왕복 시간'은 ping, '연결·포트 현황'은 netstat, '라우팅 테이블 관리'는 route로 구별한다.

암기 포인트

경로의 홉 추적은 traceroute, 목적지 생존 확인은 ping이다.

NoteBase

문 18. 다음 중 침입탐지시스템(IDS)의 주요기능이 아닌 것은?

① 데이터 수집(Raw Data Collection)

② 데이터 축약과 필터링(Data Reduction and Filtering)

③ 침입분석 및 탐지(Analysis and Intrusion Detection)

④ 역추적(Back Trace)

정답 4번

출제 포인트

침입탐지시스템(IDS)의 핵심 처리 단계와 별도의 보안 기능인 역추적을 구분하는 문제이다.

핵심 개념

침입탐지시스템은 네트워크 트래픽이나 시스템 활동을 수집하고, 분석에 필요한 정보로 축약·필터링한 뒤, 공격 징후나 보안정책 위반을 탐지하는 시스템이다.
주요 처리 흐름은 데이터 수집 → 데이터 축약·필터링 → 침입 분석·탐지이다. 역추적은 공격이 거쳐 온 경로나 실제 근원지를 추적하는 별도의 대응·조사 기능이다.

선지별 해설

① O — 데이터 수집(Raw Data Collection)은 패킷, 로그, 시스템 이벤트 등 분석의 원재료를 확보하는 IDS의 기본 기능이다.
② O — 데이터 축약과 필터링(Data Reduction and Filtering)은 수집된 대량의 데이터에서 불필요한 정보를 제거하고 분석할 대상을 추리는 IDS의 주요 기능이다.
③ O — 침입분석 및 탐지(Analysis and Intrusion Detection)는 수집·정제된 데이터를 규칙이나 행위 특성과 비교하여 공격 징후를 식별하는 IDS의 핵심 기능이다.
④ X — 틀린 표현은 '역추적(Back Trace)이 IDS의 주요 기능'이라는 부분이다. 역추적은 공격 경로나 근원지를 거슬러 확인하는 대응·포렌식 성격의 기능이며, IDS의 기본 처리 단계는 데이터 수집, 축약·필터링, 침입 분석·탐지이다.

오답 포인트

IDS가 공격자의 출발지 정보나 관련 로그를 보여 줄 수 있다는 점 때문에 역추적까지 IDS의 고유한 주요 기능으로 보기 쉽다. 그러나 탐지는 공격 징후를 찾아내는 기능이고, 역추적은 탐지 후 공격 경로와 근원을 조사하는 기능이다.

NoteBase

다시 나오면 이렇게 판단

선지가 '수집 → 축약·필터링 → 분석·탐지'의 흐름에 속하는지 확인한다. 공격 경로를 거슬러 근원지를 찾는 내용이면 IDS의 기본 탐지 기능이 아니라 별도의 역추적·조사 기능으로 판단한다.

암기 포인트

IDS는 수집·정제·탐지, 역추적은 사후 경로 조사이다.

NoteBase

문 19. 다음 중 IPv6의 전달 방식 중 애니캐스트(AnyCast)에 대한 설명으로 가장 바른 것은?

① 하나의 호스트에서 다른 하나의 호스트에게 전달하는 방식

② 하나의 호스트에서 그룹 내의 가장 가까운 곳에 있는 수신자에게 전달하는 방식

③ 다중호스트를 여러 개의 호스트들에게 전달하는 방식

④ 하나의 호스트에서 모든 호스트들에게 전달하는 방식

정답 2번

출제 포인트

IPv6의 유니캐스트, 애니캐스트, 멀티캐스트를 수신 범위와 전달 대상의 선택 방식으로 구별하는 문제이다.

핵심 개념

애니캐스트는 동일한 애니캐스트 주소를 공유하는 여러 인터페이스 중 라우팅 기준상 가장 가까운 하나의 인터페이스로 패킷을 전달하는 방식이다.
유니캐스트는 하나의 송신자에서 특정한 하나의 수신자로 전달하고, 멀티캐스트는 하나의 송신자에서 특정 그룹의 여러 수신자로 전달한다. IPv6는 브로드캐스트를 사용하지 않는다.

선지별 해설

① X — '다른 하나의 호스트에게 전달'은 특정 수신자 하나를 지정하는 유니캐스트의 설명이다. 애니캐스트는 같은 주소를 가진 수신자 그룹 중 가장 가까운 하나에 전달하는 방식이다.
② O — 같은 애니캐스트 주소가 지정된 그룹 가운데 라우팅 기준상 가장 가까운 수신자 하나에게 전달하므로 애니캐스트에 대한 설명으로 가장 바르다.
③ X — '여러 개의 호스트들에게 전달'은 멀티캐스트에 해당하는 표현이다. 올바르게는 애니캐스트는 수신자 그룹 전체가 아니라 그중 가장 가까운 하나의 수신자에게 전달한다.
④ X — '모든 호스트들에게 전달'은 브로드캐스트의 설명이다. 올바르게는 IPv6에는 브로드캐스트가 없으며, 애니캐스트는 그룹 중 가장 가까운 하나의 수신자에게 전달한다.

오답 포인트

②의 '그룹 내'만 보고 멀티캐스트로 오해하기 쉽다. 애니캐스트는 그룹의 모든 구성원에게 보내는 것이 아니라 그중 가장 가까운 하나에게 보내는 방식이라는 점이 핵심이다.

다시 나오면 이렇게 판단

수신자가 특정 하나이면 유니캐스트, 특정 그룹의 전부이면 멀티캐스트, 같은 주소를 공유하는 그룹 중 가장 가까운 하나이면 애니캐스트로 판단한다. IPv6에서 모든 호스트 대상의 브로드캐스트는 사용하지 않는다.

NoteBase

암기 포인트

유니캐스트는 하나, 멀티캐스트는 그룹, 애니캐스트는 그룹 중 가장 가까운 하나이다.

NoteBase

문 20. 악성코드를 운반하는 페이로드(payload)의 네 가지 분류와 예가 잘못 연결된 것은?

① 시스템 파괴 - 논리폭탄, Stuxnet

② 공격 에이전트 - 랜섬웨어, 트랩 도어

③ 정보 유출 - 키로거, 피싱, 스파이웨어

④ 잠입 - 백도어, 루트킷

정답 2번

출제 포인트

악성코드의 페이로드를 수행 목적에 따라 시스템 파괴, 공격 에이전트, 정보 유출, 잠입으로 구분하고 각 유형의 대표 사례를 연결하는 문제이다.

핵심 개념

시스템 파괴는 시스템이나 데이터를 훼손하거나 사용하지 못하게 하는 기능이며,
논리폭탄·랜섬웨어·Stuxnet이 대표 사례이다.
공격 에이전트는 감염된 시스템을 원격 조종하여 다른 대상을 공격하게 하는 기능이며, 좀비와 봇이 대표 사례이다.
정보 유출은 자격 증명이나 개인정보 등을 빼내는 기능이며, 키로거·피싱·스파이웨어가 대표 사례이다.
잠입은 악성코드의 존재나 접근 통로를 숨기는 기능이며, 백도어(트랩 도어)와 루트킷이 대표 사례이다.

선지별 해설

① O — 논리폭탄은 특정 조건에서 파괴 기능을 실행하고, Stuxnet은 산업 제어 시스템을 교란·훼손하므로 시스템 파괴 유형에 해당한다.
② X — '공격 에이전트 - 랜섬웨어, 트랩 도어'의 연결이 잘못되었다. 공격 에이전트의 대표 사례는 감염된 컴퓨터를 외부 공격에 이용하는 좀비와 봇이다. 랜섬웨어는 시스템·데이터의 이용을 막는 시스템 파괴 유형이고, 트랩 도어는 은밀한 접근 통로를 두는 잠입 유형이다.
③ O — 키로거는 입력 정보를 기록하고, 피싱과 스파이웨어는 사용자의 자격 증명이나 개인정보 등을 탈취하므로 정보 유출 유형에 해당한다.
④ O — 백도어는 정상 인증 절차를 우회하는 비밀 접근 통로를 만들고, 루트킷은 악성코드의 파일·프로세스 등을 숨기므로 잠입 유형에 해당한다.

오답 포인트

랜섬웨어와 트랩 도어도 공격에 활용되므로 모두 '공격 에이전트'처럼 보일 수 있다. 그러나 이 분류는 공격에 쓰이는지보다 페이로드가 직접 수행하는 기능을 기준으로 하며, 다른 시스템을 공격하게 만드는 좀비·봇만 공격 에이전트에 해당한다.

NoteBase

다시 나오면 이렇게 판단

페이로드가 직접 하는 일을 기준으로 분류한다. 훼손·암호화는 시스템 파괴, 감염 호스트를 이용한 추가 공격은 공격 에이전트, 정보 수집은 정보 유출, 존재나 접근 통로 은폐는 잠입으로 판단한다.

암기 포인트

파괴는 논리폭탄·랜섬웨어·Stuxnet, 공격 대행은 좀비·봇, 유출은 키로거·피싱·스파이웨어, 잠입은 백도어·루트킷이다.

NoteBase