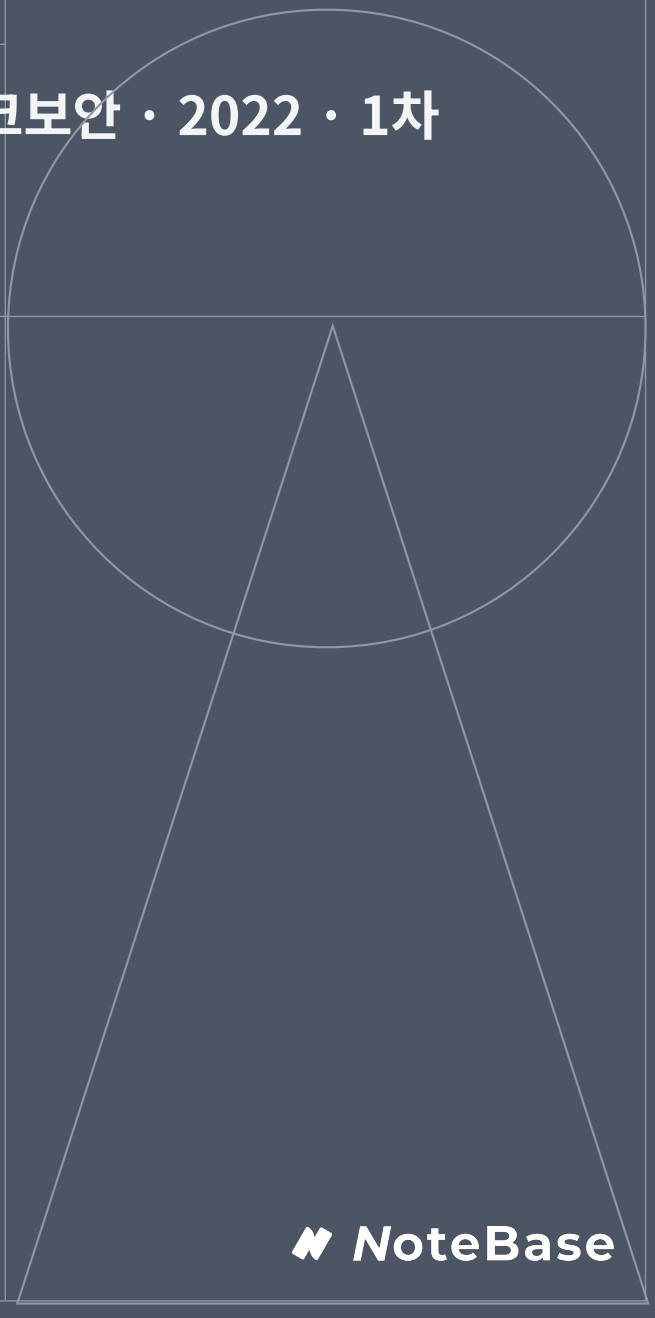
기출OX 해설집

공무원/해경/순경 · 네트워크보안 · 2022 · 1차



NoteBase

기출OX 해설집

공무원/해경/순경 · 네트워크보안 · 2022 · 1차

공무원/해경/순경 · 네트워크보안 · 2022 · 1차

문 1. 다음 중 SSL(Secure Socket Layer) 프로토콜에 대한 설명으로 가장 옳지 않은 것은?

① ChangeCipherSpec - Handshake 프로토콜에 의해 협상된 암호규격과 암호키를 이용하여 추후의 레코드 계층의 메시지를 보호할 것을 지시한다.

② Handshake - 서버와 클라이언트 간 상호인증 기능을 수행하고, 암호화 알고리즘과 이에 따른 키 교환 시 사용된다.

③ Alert - 내부적 및 외부적 보안 연관을 생성하기 위해 설계된 프로토콜이며, Peer가 IP 패킷을 송신할 필요가 있을 때, 트래픽의 유형에 해당하는 SA가 있는지를 알아보기 위해 보안 정책 데이터베이스를 조회한다.

④ Record - 상위계층으로부터(Handshake 프로토콜, ChangeCipherSpec 프로토콜, Alert 프로토콜 또는 응용계층) 수신하는 메시지를 전달하며 메시지는 단편화되거나 선택적으로 압축된다.

정답 3번

출제 포인트

SSL을 구성하는 ChangeCipherSpec, Handshake, Alert, Record 프로토콜의 역할을 구별하는 문제이다.

핵심 개념

Handshake는 통신 상대의 인증, 암호 알고리즘 협상, 키 교환에 필요한 정보를 처리한다.
ChangeCipherSpec은 협상된 암호 규격과 키를 이후 레코드에 적용하도록 알린다. Alert는 오류·경고와 연결 종료 상태를 전달한다. Record는 상위 프로토콜의 메시지를 단편화하고 필요하면 압축한 뒤 무결성 보호와 암호화를 적용하여 운반한다.

NoteBase

선지별 해설

① O — ChangeCipherSpec은 Handshake에서 협상한 암호 규격과 키를 현재 연결 상태에 적용하여 이후 Record 메시지를 보호하도록 전환을 알리는 프로토콜이다.
② O — Handshake는 서버 인증과 선택적인 클라이언트 인증을 수행하고, 사용할 암호 알고리즘과 키 교환 정보를 협상한다. 따라서 서버와 클라이언트의 상호 인증 및 키 교환과 관련된 설명은 타당하다.
③ X — 틀린 부분은 Alert가 보안 연관(SA)을 생성하고 보안 정책 데이터베이스를 조회한다는 표현이다. 이는 IPsec의 SA 및 보안 정책 처리에 관한 설명이다. Alert는 SSL 통신 중 발생한 경고·치명적 오류와 연결 종료 등의 상태를 상대방에게 알리는 프로토콜이다.
④ O — Record는 Handshake, ChangeCipherSpec, Alert 및 응용계층에서 받은 데이터를 운반하며, 이를 단편화하고 선택적으로 압축한 뒤 보호하여 전송한다.

오답 포인트

③은 '보안'이라는 공통 표현을 이용해 SSL의 Alert와 IPsec의 SA·보안 정책 데이터베이스를 섞었다. SA 생성과 정책 데이터베이스 조회는 Alert의 기능이 아니다.

다시 나오면 이렇게 판단

협상·인증·키 교환은 Handshake, 협상 결과의 적용 전환은 ChangeCipherSpec, 오류 통지는 Alert, 실제 데이터의 분할·보호·운반은 Record로 구분한다. SA나 보안 정책 데이터베이스가 나오면 SSL이 아니라 IPsec 문맥인지 확인한다.

암기 포인트

Handshake는 협상, ChangeCipherSpec은 전환, Alert는 경고, Record는 운반이다.

NoteBase

문 2. 다음 중 망 내 교환 장비들이 오류 상황에 대한 보고를 할 수 있게 하고, 예상하지 못한 상황이 발생한 경우 이를 알릴 수 있도록 지원하는 프로토콜은 무엇인가?

① ICMP

② ARP

③ RARP

④ IGMP

정답 1번

출제 포인트

이 문제는 TCP/IP 계층에서 오류 상황과 예외 상태를 알리는 프로토콜을 다른 주소 변환·멀티캐스트 관리 프로토콜과 구별하는 문제이다.

핵심 개념

ICMP: IP 패킷을 처리하거나 전달하는 과정에서 발생한 오류와 제어 정보를 송신 측에 알리는 프로토콜이다. 목적지 도달 불가, 시간 초과 등의 메시지가 대표적이다.
ARP는 IPv4 주소에 대응하는 MAC 주소를 알아내고, RARP는 MAC 주소로부터 IPv4 주소를 알아내는 과거의 역방향 주소 변환 프로토콜이며, IGMP는 IPv4 멀티캐스트 그룹의 가입 상태를 관리한다.

선지별 해설

① O — ICMP는 라우터나 호스트가 IP 패킷 처리 중 발생한 오류 또는 예외 상황을 알리는 제어 메시지를 전달한다. 따라서 지문의 설명에 해당한다.
② X — ARP라는 표현이 틀렸다. ARP는 오류 상황을 보고하는 프로토콜이 아니라 같은 네트워크에서 IPv4 주소에 대응하는 MAC 주소를 알아내는 프로토콜이다. 올바르게는 오류 및 제어 정보를 알리는 프로토콜이 ICMP이다.
③ X — RARP라는 표현이 틀렸다. RARP는 오류 상황을 보고하는 프로토콜이 아니라 MAC 주소를 바탕으로 IPv4 주소를 알아내기 위해 사용된 역방향 주소 변환 프로토콜이다. 올바르게는 오류 및 제어 정보를 알리는 프로토콜이 ICMP이다.
④ X — IGMP라는 표현이 틀렸다. IGMP는 오류 상황을 보고하는 프로토콜이 아니라 호스트와 라우터 사이에서 IPv4 멀티캐스트 그룹의 가입 상태를 관리하는 프로토콜이다. 올바르게는 오류 및 제어 정보를 알리는 프로토콜이 ICMP이다.

오답 포인트

네 프로토콜이 모두 TCP/IP 환경에서 사용되므로 이름만 보고 혼동하기 쉽다. 특히 ICMP는 오류를 직접 복구하는 프로토콜이 아니라 오류나 예외 상태를 메시지로 보고하는 프로토콜이라는 점이 핵심이다.

NoteBase

다시 나오면 이렇게 판단

문제의 기능어를 먼저 구분한다. 오류·도달 불가·시간 초과는 ICMP, IPv4 주소에서 MAC 주소 확인은 ARP, MAC 주소에서 IPv4 주소 확인은 RARP, 멀티캐스트 그룹 가입 관리는 IGMP로 판단한다.

암기 포인트

오류 보고는 ICMP, 주소 확인은 ARP·RARP, 멀티캐스트 그룹 관리는 IGMP이다.

NoteBase

문 3. 다음 <보기> 중 제시된 Well Known Port 번호에 해당하는 프로토콜을 순서대로 가장 적합하게 제시한 것은?

<보기>
㉠ 22번 포트 ㉡ 53번 포트 ㉢ 161번 포트

① ㉠ SSH ㉡ Gopher ㉢ NetBIOS
② ㉠ SSH ㉡ DNS ㉢ SNMP
③ ㉠ FTP ㉡ Gopher ㉢ SNMP
④ ㉠ FTP ㉡ DNS ㉢ NetBIOS

정답 2번

출제 포인트

Well Known Port 번호 22, 53, 161과 각각의 대표 프로토콜을 정확히 연결하는 문제이다.

핵심 개념

22번 포트는 원격 접속을 암호화하는 SSH, 53번 포트는 도메인 이름과 IP 주소를 질의·응답하는 DNS, 161번 포트는 네트워크 장비를 조회·관리하는 SNMP에 대응한다. 따라서 순서는 SSH-DNS-SNMP이다.

선지별 해설

① X
㉠ SSH는 22번 포트에 맞지만, ㉡ 53번 포트는 Gopher가 아니라 DNS이고 ㉢ 161번 포트는 NetBIOS가 아니라 SNMP이다. 올바르게 고치면 '㉠ SSH ㉡ DNS ㉢ SNMP'이다.

② O
22번은 SSH, 53번은 DNS, 161번은 SNMP이므로 세 항목이 모두 맞는다.

③ X
㉢ SNMP는 161번 포트에 맞지만, ㉠ 22번 포트는 FTP가 아니라 SSH이고 ㉡ 53번 포트는 Gopher가 아니라 DNS이다. 올바르게 고치면 '㉠ SSH ㉡ DNS ㉢ SNMP'이다.

④ X
㉡ DNS는 53번 포트에 맞지만, ㉠ 22번 포트는 FTP가 아니라 SSH이고 ㉢ 161번 포트는 NetBIOS가 아니라 SNMP이다. 올바르게 고치면 '㉠ SSH ㉡ DNS ㉢ SNMP'이다.

NoteBase

오답 포인트

각 선지에 정답 요소가 일부 섞여 있다는 점이 함정이다. 특히 ①은 SSH만, ③은 SNMP만, ④는 DNS만 맞으므로 한 항목만 확인해서는 안 되고 ㉠부터 ㉢까지 모두 대조해야 한다.

다시 나오면 이렇게 판단

포트 번호를 하나씩 고정 대응시킨다. 22→SSH, 53→DNS, 161→SNMP를 차례로 대입한 뒤 세 대응이 모두 일치하는 선지를 선택한다.

암기 포인트

22 SSH, 53 DNS, 161 SNMP이다. 함께 자주 나오는 오답용 포트는 FTP 21, Gopher 70, NetBIOS 137~139이다.

NoteBase

문 4. 다음 중 OSI 7계층 모델에서 동작하는 계층이 가장 다른 것은?

① L2TP

② PPTP

③ SYN 플러딩

④ ARP 스푸핑

정답 3번

출제 포인트

L2TP·PPTP·ARP 스푸핑과 SYN 플러딩이 주로 관련되는 OSI 계층을 구별하는 문제이다.

핵심 개념

L2TP와 PPTP는 데이터링크 계층의 프레임을 터널링하는 프로토콜이다. ARP 스푸핑은 IP 주소와 MAC 주소의 대응 관계를 조작하므로 데이터링크 계층 공격으로 분류한다. 반면 SYN 플러딩은 전송 계층 프로토콜인 TCP의 연결 설정 절차를 악용하는 공격이다.

선지별 해설

① X
L2TP는 이름 그대로 2계층 터널링 프로토콜이므로 데이터링크 계층과 관련된다. 따라서 나머지와 가장 다른 계층에 해당하지 않는다. 올바르게는 'L2TP는 데이터링크 계층의 터널링 프로토콜이다'라고 정리한다.

② X
PPTP는 PPP 프레임을 터널링하는 데이터링크 계층 관련 프로토콜이다. 따라서 가장 다른 계층에 해당하지 않는다. 올바르게는 'PPTP는 데이터링크 계층의 터널링 프로토콜이다'라고 정리한다.

③ O
SYN 플러딩은 TCP의 3방향 연결 설정에서 다수의 SYN 요청을 보내 반연결 상태를 누적시키는 공격이다. TCP는 전송 계층에서 동작하므로 다른 세 선지와 계층이 가장 다르다.

④ X
ARP 스푸핑은 거짓 ARP 정보를 보내 IP 주소와 MAC 주소의 대응 관계를 변조하는 공격으로, 시험에서는 데이터링크 계층 공격으로 분류한다. 따라서 가장 다른 계층에 해당하지 않는다. 올바르게는 'ARP 스푸핑은 데이터링크 계층과 관련된 공격이다'라고 정리한다.

오답 포인트

L2TP와 PPTP의 이름이 VPN 기술로 익숙하다는 이유만으로 네트워크 계층으로 오인하기 쉽다. 두 프로토콜은 2계층 프레임을 터널링하며, ③의 SYN 플러딩만 TCP 연결 설정을 공격하므로 전송 계층에 해당한다.

다시 나오면 이렇게 판단

프로토콜 이름보다 공격이나 기능이 직접 다루는 대상을 확인한다. 프레임·MAC·ARP·PPP는 데이터링크 계층, TCP·SYN·포트·연결 설정은 전송 계층의 신호이다.

암기 포인트

L2TP·PPTP·ARP는 2계층, TCP SYN 플러딩은 4계층이다.

NoteBase

문 5. 다음 중 SNMP(Simple Network Management Protocol)에 대한 설명으로 가장 옳지 않은 것은?

① MIB는 객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다.

② 관리자는 GetRequest와 같은 메시지를 에이전트에 보내서 에이전트의 정보를 요구한다.

③ 에이전트는 비정상적인 상황을 관리자에게 경고하기 위하여 Trap 메시지를 관리자에 보냄으로써 관리 과정에 기여할 수 있다.

④ TCP/IP 프로토콜을 사용하는 네트워크에서 장치를 관리하기 위한 것으로, UDP 포트 161번과 162번을 사용한다.

정답 1번

출제 포인트

SNMP의 구성 요소인 SMI와 MIB의 역할, 관리자와 에이전트 사이의 메시지 흐름, 사용 포트를 구별하는 문제이다.

핵심 개념

SNMP는 TCP/IP 네트워크의 장치를 감시하고 관리하기 위한 응용 계층 프로토콜이다.
SMI(Structure of Management Information)는 관리 객체의 이름 지정, 자료형 정의, 부호화 방법 등 관리 정보의 표현 규칙을 정한다.
MIB(Management Information Base)는 SMI 규칙에 따라 정의된 관리 객체들을 계층적으로 모아 놓은 정보 구조이다.
관리자는 요청 메시지로 정보를 조회하고, 에이전트는 요청에 응답하거나 이상 상황을 알리는 Trap을 보낸다.

선지별 해설

① X — '객체의 이름을 붙이고 객체의 유형을 정의하며, 객체와 값을 부호화하는 등의 일반적인 규칙을 정의한다'는 것은 MIB가 아니라 SMI의 역할이다. 올바르게는 MIB가 SMI 규칙에 따라 정의된 관리 객체들의 집합이라고 해야 한다.
② O — 관리자는 GetRequest와 같은 요청 메시지를 에이전트에 보내 관리 객체의 값을 요구한다.
③ O — 에이전트는 장애나 임계값 초과 같은 비정상 상황을 관리자에게 자발적으로 알리기 위해 Trap 메시지를 보낼 수 있다.
④ O — SNMP는 TCP/IP 기반 네트워크 장치 관리에 사용되며, 일반적으로 에이전트의 요청 수신에는 UDP 161번, Trap 등 알림 수신에는 UDP 162번 포트를 사용한다.

NoteBase

오답 포인트

①은 MIB와 SMI의 역할을 바꾸어 놓았다. '관리 객체의 집합'은 MIB이고, 그 객체를 어떤 이름·자료형·부호화 방식으로 표현할지 정하는 '일반 규칙'은 SMI이다.

다시 나오면 이렇게 판단

이름 지정·자료형·부호화 규칙이 나오면 SMI, 실제 관리 객체의 계층적 집합이 나오면 MIB로 판단한다. 메시지 방향은 GetRequest가 관리자에서 에이전트로, Trap이 에이전트에서 관리자로 향한다.

암기 포인트

SMI는 표현 규칙, MIB는 객체 목록, Get은 관리자→에이전트, Trap은 에이전트→관리자, 포트는 161·162이다.

NoteBase

문 6. 취약한 웹 사이트에 로그인한 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 일으키도록 위조된 HTTP 요청을 웹 응용 프로그램에 전송하는 공격은 무엇인가?

① DoS 공격

② 취약한 인증 및 세션 공격

③ SQL 삽입 공격

④ CSRF 공격

정답 4번

출제 포인트

로그인된 사용자의 인증 상태를 악용하여 사용자가 원하지 않은 요청을 보내게 하는 CSRF의 특징을 다른 웹 공격과 구별하는 문제이다.

핵심 개념

CSRF(Cross-Site Request Forgery)는 공격자가 로그인된 사용자의 브라우저를 속여, 해당 사용자의 인증 정보가 실린 위조 요청을 취약한 웹 응용 프로그램에 보내게 하는 공격이다. 핵심은 공격자가 사용자의 권한을 직접 빼앗는 것이 아니라 사용자의 인증된 상태를 이용해 수정·삭제·등록 같은 행위를 대신 실행하게 한다는 점이다.

NoteBase

선지별 해설

① X
DoS 공격은 과도한 요청이나 자원 고갈을 일으켜 서비스의 정상 이용을 방해하는 가용성 공격이다. 틀린 표현은 ‘DoS 공격’이며, 제시된 공격은 로그인 사용자의 인증 상태를 악용해 위조 요청을 보내는 ‘CSRF 공격’이다.

② X
취약한 인증 및 세션 공격은 비밀번호, 세션 ID 등의 인증·세션 관리 결함을 이용해 계정을 탈취하거나 세션을 가장하는 공격이다. 틀린 표현은 ‘취약한 인증 및 세션 공격’이며, 사용자가 의도하지 않은 행위를 그 사용자의 권한으로 실행하게 하는 공격은 ‘CSRF 공격’이다.

③ X
SQL 삽입 공격은 입력값에 악의적인 SQL 구문을 넣어 데이터베이스 질의를 변조하는 공격이다. 틀린 표현은 ‘SQL 삽입 공격’이며, 문제처럼 인증된 사용자의 브라우저를 통해 위조된 HTTP 요청을 전송하게 하는 공격은 ‘CSRF 공격’이다.

④ O
CSRF 공격은 로그인된 사용자의 인증 정보가 요청에 함께 전송되는 점을 악용하여, 사용자의 의지와 무관한 수정·삭제·등록 등의 요청을 서버가 정상 요청처럼 처리하게 한다. 문제의 설명과 일치한다.

오답 포인트

‘인증된 사용자’라는 표현 때문에 ②를 고르기 쉽지만, 계정이나 세션 자체의 탈취가 핵심이 아니다. 이미 로그인된 사용자의 브라우저가 원치 않는 요청을 보내도록 속인다는 문구가 CSRF의 결정적 단서이다.

다시 나오면 이렇게 판단

로그인 상태에서 사용자의 의사와 무관한 요청이 실행되면 CSRF, SQL 질의문이 변조되면 SQL 삽입, 서비스 자원이 고갈되면 DoS, 인증 정보나 세션 자체가 탈취·가장되면 인증 및 세션 공격으로 판단한다.

암기 포인트

CSRF는 ‘로그인된 피해자의 권한으로 원치 않는 요청을 실행’하는 공격이다.

NoteBase

문 7. 다음 중 SMTP 클라이언트가 SMTP 서버의 특정 사용자를 확인함으로써 계정 존재 여부를 파악하는데 악용될 수 있는 명령어는 무엇인가?

① HELO

② MAIL FROM

③ RCPT TO

④ VRFY

정답 4번

출제 포인트

SMTP 명령 가운데 사용자나 메일함의 존재 여부를 확인하는 명령과 메일 전송 절차에 쓰이는 명령을 구별하는 문제이다.

핵심 개념

VRFY는 지정한 사용자가 SMTP 서버에서 유효한 수신자인지 확인하는 명령이다. 서버가 이 요청에 구체적으로 응답하면 공격자가 사용자 이름을 차례로 대입하여 유효한 계정을 수집하는 계정 열거에 악용할 수 있다.
HELO는 클라이언트 식별, MAIL FROM은 발신자 지정, RCPT TO는 수신자 지정에 사용된다.

선지별 해설

① X
HELO를 특정 사용자 확인 명령으로 본 점이 틀리다. HELO는 SMTP 세션을 시작하면서 클라이언트가 자신을 서버에 식별하는 명령이다. 사용자 계정의 존재 확인에는 VRFY가 해당한다.

② X
MAIL FROM을 특정 사용자 확인 명령으로 본 점이 틀리다. MAIL FROM은 메일 전송 과정에서 반송 주소가 되는 봉투 발신자를 지정하는 명령이다. 사용자 계정의 존재 확인에는 VRFY가 해당한다.

③ X
RCPT TO를 특정 사용자 확인 명령으로 본 점이 틀리다. RCPT TO는 전송할 메일의 봉투 수신자를 지정하는 명령이다. 사용자 존재 여부를 직접 확인하도록 마련된 명령은 VRFY이다.

④ O
VRFY는 인수로 제시한 사용자가 서버에서 유효한 수신자인지 확인하는 명령이다. 서버의 응답을 이용해 실제 계정의 존재 여부를 알아내는 데 악용될 수 있으므로 옳다.

NoteBase

오답 포인트

③ RCPT TO도 수신자 주소를 다루므로 계정 확인 명령처럼 보이기 쉽다. 그러나 RCPT TO는 메일의 수신자를 지정하는 전송 절차의 명령이고, 사용자 확인 자체를 목적으로 하는 명령은 ④ VRFY이다.

다시 나오면 이렇게 판단

명령어의 동사 의미와 역할을 연결한다. verify에 해당하는 VRFY는 사용자 확인, hello에 해당하는 HELO는 클라이언트 인사·식별, FROM과 TO는 각각 봉투 발신자와 수신자 지정이다.

암기 포인트

계정 확인·열거는 VRFY, 발신자는 MAIL FROM, 수신자는 RCPT TO이다.

NoteBase

문 8. 다음 중 공공기관의 보안성 강화를 위한 망분리 기술에 대한 설명으로 가장 옳지 않은 것은?

① 물리적 망분리와 논리적 망분리 기법이 존재한다.

② 물리적 망분리가 되었다 하더라도 USB와 같은 저장 매체를 통한 악성 코드 침입이 가능하다.

③ 논리적 망분리 기법으로 SBC 및 CBC 기반의 망분리 기법이 존재한다.

④ 애플리케이션 가상화 및 데스크톱 가상화를 통해 물리적 망분리 실현이 가능하다.

정답 4번

출제 포인트

물리적 망분리와 논리적 망분리를 구분하고, 가상화 기술이 어느 방식에 해당하는지를 묻는 문제이다.

핵심 개념

물리적 망분리는 업무망과 인터넷망의 단말기·네트워크 장비·회선을 물리적으로 분리하는 방식이다. 논리적 망분리는 하나의 물리적 환경에서 가상화 기술 등으로 업무 영역과 인터넷 영역을 논리적으로 분리하는 방식이다. 애플리케이션 가상화와 데스크톱 가상화는 논리적 망분리에 활용된다.

선지별 해설

① O — 망분리 방식은 장비와 회선을 별도로 구성하는 물리적 망분리와, 가상화 등을 이용하는 논리적 망분리로 구분할 수 있다.
② O — 물리적으로 망을 분리해도 USB와 같은 이동식 저장 매체가 두 환경 사이에서 사용되면 악성 코드가 유입될 수 있으므로 저장 매체 통제가 별도로 필요하다.
③ O — 논리적 망분리에는 서버 자원을 이용하는 SBC(Server-Based Computing) 방식과 단말 내부의 가상화 환경을 이용하는 CBC(Client-Based Computing) 방식이 있다.
④ X — 틀린 표현은 '물리적 망분리 실현'이다. 애플리케이션 가상화 및 데스크톱 가상화는 가상화된 환경으로 두 영역을 나누므로, 올바르게는 '논리적 망분리 실현이 가능하다'이다.

오답 포인트

④는 가상화 기술로 사용 환경이 분리된다는 점을 실제 장비와 회선까지 물리적으로 분리하는 것으로 바꾸어 놓았다. 화면이나 작업 공간이 나뉘어 보여도 분리 수단이 가상화라면 논리적 망분리이다.

다시 나오면 이렇게 판단

단말기·장비·회선을 각각 두는지는 물리적 망분리로, 서버·클라이언트 가상화로 업무 영역과 인터넷 영역을 나누는지는 논리적 망분리로 판단한다.

NoteBase

암기 포인트

장비와 회선을 따로 두면 물리적 망분리, 가상화로 영역을 나누면 논리적 망분리이다.

NoteBase

문 9. 다음 중 정보통신망 등의 침해사고에 대응하기 위해 기업이나 기관의 업무 관할 지역 내에서 침해사고의 접수 및 처리 지원을 비롯해 예방, 피해 복구 등의 임무를 수행하는 조직으로 가장 옳은 것은?

① CISO

② CERT

③ CPPG

④ CPO

정답 2번

출제 포인트

침해사고를 접수하고 대응·예방·피해 복구를 지원하는 조직인 CERT와 정보보호·개인정보보호 분야의 직책 또는 자격을 구별하는 문제이다.

핵심 개념

CERT(Computer Emergency Response Team)는 침해사고의 신고·접수, 분석·대응, 예방 및 복구 지원을 담당하는 사고대응 조직이다.
CISO는 조직의 정보보호 업무를 총괄하는 최고정보보호책임자이고, CPO는 개인정보 보호 업무를 총괄하는 개인정보보호책임자이다. CPPG는 개인정보보호 관련 전문지식을 평가하는 개인정보관리사 자격이다.

선지별 해설

① X — CISO는 정보보호 정책과 업무를 총괄하는 책임자 직책이지, 침해사고의 접수·처리와 복구를 수행하는 대응 조직이 아니다. 틀린 표현은 'CISO'이며, 올바르게는 'CERT'이다.
② O — CERT는 정보통신망 침해사고를 접수하고 분석·대응하며, 사고 예방과 피해 복구를 지원하는 조직이다.
③ X — CPPG는 개인정보보호 분야의 전문 자격으로, 침해사고 대응 조직을 뜻하지 않는다. 틀린 표현은 'CPPG'이며, 올바르게는 'CERT'이다.
④ X — CPO는 개인정보 보호 업무를 총괄하는 책임자 직책이지, 침해사고 대응 조직이 아니다. 틀린 표현은 'CPO'이며, 올바르게는 'CERT'이다.

오답 포인트

CISO와 CPO도 보안·개인정보보호 업무에 관여하므로 CERT와 혼동하기 쉽다. 그러나 선지에서 '조직'인지 '책임자 직책'인지 '자격'인지를 구분해야 한다. 특히 침해사고의 접수·분석·대응·복구라는 표현은 CERT를 가리킨다.

NoteBase

다시 나오면 이렇게 판단

침해사고를 직접 접수하고 대응·복구하는 '팀 또는 조직'을 물으면 CERT로 판단한다. 정보보호 총괄 책임자는 CISO, 개인정보보호 총괄 책임자는 CPO, 개인정보보호 전문 자격은 CPPG로 구분한다.

암기 포인트

CERT는 사고대응팀, CISO·CPO는 책임자, CPPG는 자격이다.

NoteBase

문 10. 다음 중 HTTP 응답 메시지 상태 코드의 의미가 가장 옳지 않은 것은?

① 201 - Created

② 301 - Moved Permanently

③ 401 - Unauthorized

④ 501 - Bad Request

정답 4번

출제 포인트

HTTP 응답 상태 코드의 백의 자리별 분류와 각 코드의 구체적 의미를 구별하는 문제이다.

핵심 개념

HTTP 상태 코드는 서버가 요청을 처리한 결과를 세 자리 숫자로 나타낸 것이다. 200번대는 성공, 300번대는 리다이렉션, 400번대는 클라이언트 오류, 500번대는 서버 오류를 뜻한다.
400 Bad Request는 요청 문법이나 형식 등이 잘못되어 서버가 요청을 처리할 수 없음을 뜻하고, 501 Not Implemented는 서버가 요청을 수행하는 데 필요한 기능을 지원하지 않음을 뜻한다.

선지별 해설

① O — 201 Created는 요청이 성공적으로 처리되어 새로운 자원이 생성되었음을 뜻한다.
② O — 301 Moved Permanently는 요청한 자원이 새 위치로 영구 이동했음을 뜻한다.
③ O — 401 Unauthorized는 요청에 유효한 인증 자격 증명이 필요함을 뜻한다. 명칭은 Unauthorized이지만 핵심은 인증되지 않았거나 인증 정보가 유효하지 않다는 점이다.
④ X — 틀린 표현은 '501 - Bad Request'이다. Bad Request는 400이고, 501은 서버가 요청된 기능을 지원하지 않는다는 의미의 Not Implemented이다.

오답 포인트

④는 500번대이므로 막연히 서버가 요청을 잘못 받았다는 뜻으로 오인하기 쉽다. 그러나 Bad Request는 클라이언트가 보낸 요청 자체의 문제를 나타내는 400이고, 501은 서버의 기능 미구현을 나타낸다.

다시 나오면 이렇게 판단

먼저 백의 자리로 성공·리다이렉션·클라이언트 오류·서버 오류를 구분한 뒤, 자주 출제되는 개별 코드를 대조한다. 특히 400 Bad Request와 501 Not Implemented를 구별한다.

암기 포인트

201 생성, 301 영구 이동, 401 인증 필요, 501 기능 미구현이다. Bad Request는 400이다.

NoteBase

문 11. 다음 중 IP Spoofing 공격 활동으로 가장 옳지 않은 것은?

① SYN Flooding 공격

② slowloris 공격

③ RST를 이용한 접속 끊기

④ 순서번호 추측(Sequence number guessing)

정답 2번

출제 포인트

IP Spoofing을 이용하는 TCP 계층 공격과 응용 계층의 HTTP 서비스 거부 공격을 구별하는 문제이다.

핵심 개념

IP Spoofing은 패킷의 출발지 IP 주소를 다른 주소로 위조하여 송신자의 신원을 숨기거나 신뢰 관계를 악용하는 기법이다. TCP 공격에서는 위조한 출발지 주소와 순서번호를 이용해 연결을 방해하거나 세션을 가로챌 수 있다. 반면 slowloris는 HTTP 요청 헤더를 매우 느리게 전송하여 서버의 연결 자원을 오래 점유하는 응용 계층 서비스 거부 공격이다.

선지별 해설

① O — SYN Flooding은 다수의 SYN 패킷을 보내 서버에 반개방 연결을 쌓는 공격이며, 출발지 IP 주소를 위조하여 응답을 받지 않고 공격자를 숨기는 방식으로 수행될 수 있다.
② X — 틀린 부분은 ‘slowloris 공격’을 IP Spoofing 공격 활동으로 본 것이다. slowloris는 정상적인 TCP 연결을 맺은 뒤 불완전한 HTTP 요청을 천천히 보내 연결을 유지하는 응용 계층 서비스 거부 공격이며, IP Spoofing의 대표적 공격 활동이 아니다.
③ O — 공격자가 피해 호스트의 주소로 위조한 RST 패킷을 보내고 유효한 TCP 순서번호 범위를 맞히면 기존 TCP 접속을 강제로 종료할 수 있다.
④ O — TCP 순서번호 추측은 위조 패킷이 정상 세션의 패킷으로 받아들여지게 만드는 데 사용되며, IP Spoofing을 이용한 세션 가로채기나 접속 방해의 기반이 된다.

오답 포인트

네 선지가 모두 서비스 거부나 TCP 통신 방해와 관련되어 보여 혼동하기 쉽다. 핵심 함정은 ②의 slowloris도 네트워크 공격이라는 이유만으로 IP Spoofing 공격에 포함시키는 것이다. slowloris는 HTTP 연결을 실제로 오래 유지해야 하므로 출발지 IP 위조가 핵심인 공격과 구별된다.

NoteBase

다시 나오면 이렇게 판단

출발지 IP 주소 위조, 위조 TCP 패킷, 순서번호 추측이 핵심이면 IP Spoofing 관련 공격으로 판단한다. 정상 TCP 연결 후 HTTP 요청을 느리게 보내 서버 자원을 점유하는 방식이면 slowloris로 판단한다.

암기 포인트

IP Spoofing은 주소 위조와 TCP 패킷 조작, slowloris는 느린 HTTP 연결 점유이다.

NoteBase

문 12. 다음 중 ESM(통합보안솔루션)의 구성요소에 대한 설명으로 가장 옳지 않은 것은?

① 보안패치 : 최근 보안취약점이 발생한 시스템에 대해서 자동으로 패치를 수행한다.

② Manager : 수집된 로그정보를 통합하고 분석한다.

③ Console : 관리자는 ESM Console을 사용해서 모니터링하고 명령어를 실행한다.

④ Agent : 시스템에 설치되어서 각종 로그정보를 수집한다.

정답 1번

출제 포인트

ESM의 표준 구성요소인 Agent, Manager, Console의 역할을 구분하는 문제이다.

핵심 개념

ESM은 여러 보안 시스템에서 발생한 로그와 보안 이벤트를 한곳에 모아 통합 관리하는 시스템이다. Agent는 로그를 수집해 전달하고, Manager는 수집된 정보를 통합·저장·분석하며, Console은 관리자가 모니터링하고 관리 명령을 내리는 화면이다. 보안패치는 취약점을 보완하는 프로그램 또는 조치로서 ESM의 표준 구성요소 명칭이 아니다.

선지별 해설

① X — 틀린 표현은 '보안패치'를 ESM의 구성요소로 제시하고 자동 패치 수행을 그 역할이라고 한 부분이다. 올바르게는 ESM의 대표 구성요소를 Agent, Manager, Console로 구분하며, 자동 패치 배포는 패치 관리 시스템의 기능이다.
② O — Manager는 Agent가 보내 온 로그와 보안 이벤트를 통합하고 상관관계 등을 분석한다.
③ O — Console은 관리자가 ESM의 상황을 모니터링하고 필요한 관리 명령을 실행하는 사용자 인터페이스이다.
④ O — Agent는 관리 대상 시스템이나 보안 장비에 설치되어 각종 로그정보를 수집해 Manager로 전달한다.

오답 포인트

①의 '보안패치'는 보안과 관련된 기능이라는 이유만으로 ESM 구성요소처럼 보이게 한 함정이다. ESM은 보안 기능을 직접 모두 수행하는 제품이 아니라 여러 보안 장비의 정보를 수집·통합·분석·관리하는 체계이다.

다시 나오면 이렇게 판단

수집은 Agent, 통합·분석은 Manager, 관제·명령은 Console로 연결한다. 이 세 역할에 해당하지 않고 취약점 자체를 수정하거나 패치를 배포한다고 하면 ESM의 표준 구성요소와 구별한다.

NoteBase

암기 포인트

Agent는 수집, Manager는 통합·분석, Console은 관제·명령이다.

NoteBase

문 13. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
(㉠)는 웹 페이지에 입력되는 입력 값 검증 및 필터링 등을 수행하는 방화벽이다.
(㉡)는 모바일 단말에 대해서 소프트웨어 및 펌웨어를 관리하는 솔루션이다.
(㉢)는 네트워크 패킷을 탐지하고 대응까지 수행한다.

① ㉠ WAF(Web Application Firewall)
㉡ MDM
㉢ IPS

② ㉠ WAF(Web Application Firewall)
㉡ MAM
㉢ IDS

③ ㉠ Firewall
㉡ MDM
㉢ IDS

④ ㉠ Firewall
㉡ MAM
㉢ IPS

정답 1번

출제 포인트

웹 공격 방어 장비, 모바일 단말 관리 솔루션, 침입 탐지·방지 시스템을 기능에 따라 구별하는 문제이다.

핵심 개념

WAF(Web Application Firewall): 웹 애플리케이션으로 들어오는 요청을 검사하여 SQL 삽입, 크로스사이트 스크립팅 등 웹 공격을 차단하는 방화벽이다. 키워드는 웹 입력값 검증·필터링이다.
MDM(Mobile Device Management): 모바일 단말 자체를 대상으로 운영체제, 소프트웨어, 펌웨어, 보안 정책 등을 통합 관리하는 솔루션이다.
MAM(Mobile Application Management): 모바일 단말 전체가 아니라 업무용 애플리케이션과 그 데이터를 배포·통제·보호하는 솔루션이다.
IDS(Intrusion Detection System)는 침입 징후를 탐지하고 경보하는 시스템이고, IPS(Intrusion Prevention System)는 탐지에 더해 차단·대응까지 수행하는 시스템이다.

NoteBase

선지별 해설

① O — ㉠ WAF는 웹 입력값을 검증·필터링하고, ㉡ MDM은 모바일 단말의 소프트웨어와 펌웨어 등을 관리하며, ㉢ IPS는 침입을 탐지하고 차단·대응까지 수행한다. 세 대응이 모두 옳다.
② X — 틀린 표현은 ㉡ MAM과 ㉢ IDS이다. 올바르게는 단말의 소프트웨어·펌웨어를 관리하는 ㉡은 MDM이고, 탐지 후 대응까지 수행하는 ㉢은 IPS이다.
③ X — 틀린 표현은 ㉠ Firewall과 ㉢ IDS이다. 올바르게는 웹 페이지 입력값을 검증·필터링하는 ㉠은 WAF이고, 탐지와 대응을 함께 수행하는 ㉢은 IPS이다. ㉡ MDM은 옳다.
④ X — 틀린 표현은 ㉠ Firewall과 ㉡ MAM이다. 올바르게는 웹 애플리케이션의 입력값을 검사하는 ㉠은 WAF이고, 모바일 단말의 소프트웨어·펌웨어를 관리하는 ㉡은 MDM이다. ㉢ IPS는 옳다.

오답 포인트

일반 Firewall과 WAF, MDM과 MAM, IDS와 IPS의 범위를 바꾸어 놓은 것이 함정이다. 특히 '대응까지 수행한다'는 표현은 탐지만 하는 IDS가 아니라 차단 기능을 가진 IPS를 가리킨다.

다시 나오면 이렇게 판단

'웹 입력값 검증·필터링'은 WAF, '단말의 소프트웨어·펌웨어 관리'는 MDM, '탐지 후 차단·대응'은 IPS로 연결한다. 애플리케이션만 관리하면 MAM, 탐지·경보에 그치면 IDS로 판단한다.

암기 포인트

웹은 WAF, 단말은 MDM, 앱은 MAM, 탐지만 IDS, 탐지와 차단은 IPS이다.

NoteBase

문 14. 다음 중 Spoofing의 종류로 가장 옳지 않은 것은?

① ARP Spoofing

② IP Spoofing

③ DNS Spoofing

④ ULU Spoofing

정답 4번

출제 포인트

대표적인 네트워크 스푸핑 공격의 명칭과 공격 대상을 구별하는 문제이다. 스푸핑은 공격자가 주소나 이름 등의 식별 정보를 속여 신뢰할 수 있는 대상처럼 위장하는 공격이다.

핵심 개념

ARP Spoofing은 IP 주소와 MAC 주소의 대응 정보를 속이고, IP Spoofing은 IP 패킷의 출발지 주소를 속이며, DNS Spoofing은 도메인 이름에 대한 IP 주소 응답을 속이는 공격이다. 공격자가 위조하는 식별 정보가 무엇인지로 각 유형을 구분한다.

선지별 해설

① O — ARP Spoofing은 위조된 ARP 정보를 보내 피해자의 ARP 캐시에 잘못된 IP 주소와 MAC 주소의 대응 관계를 저장하게 하는 대표적인 스푸핑 공격이다.
② O — IP Spoofing은 IP 패킷의 출발지 IP 주소를 다른 주소로 위조하여 송신자의 신원을 속이는 공격이다.
③ O — DNS Spoofing은 위조된 DNS 응답이나 변조된 이름 해석 정보를 이용하여 사용자를 공격자가 의도한 IP 주소로 연결하는 공격이다.
④ X — ‘ULU Spoofing’은 통상적으로 분류되는 네트워크 스푸핑 공격 명칭이 아니다. 올바르게는 ‘ULU Spoofing은 대표적인 스푸핑 유형이 아니다’라고 해야 한다.

오답 포인트

영문 약어처럼 보인다는 이유만으로 ④의 ‘ULU’를 실제 프로토콜이나 주소 체계로 오인하기 쉽다. ①은 주소 대응 정보, ②는 출발지 IP 주소, ③은 도메인 이름 해석 정보를 각각 위조하는 실제 공격 유형이지만, ④는 이에 해당하지 않는다.

다시 나오면 이렇게 판단

스푸핑 명칭 앞부분이 실제 네트워크 식별 체계나 프로토콜을 가리키는지 확인한다. ARP는 IP 주소와 MAC 주소의 대응, IP는 패킷의 출발지 주소, DNS는 도메인 이름과 IP 주소의 대응을 속인다는 기준으로 판단한다.

NoteBase

암기 포인트

ARP는 주소 대응 위조, IP는 출발지 위조, DNS는 이름 해석 위조이다. ULU Spoofing은 표준적인 스푸핑 유형 명칭이 아니다.

NoteBase

문 15. 다음 <보기>는 VPN에 대한 설명이다. ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
· IPSEC VPN은 (㉠) 단위로 데이터를 암호화 한다.
· SSL VPN은 (㉡) 단위로 데이터를 암호화 한다.

① ㉠ 프레임 ㉡ 데이터
② ㉠ 데이터 ㉡ 프레임
③ ㉠ 패킷 ㉡ 메시지
④ ㉠ 메시지 ㉡ 메시지

정답 3번

출제 포인트

IPsec VPN과 SSL VPN이 보호하는 데이터의 단위를 계층별로 구분하는 문제이다.

핵심 개념

IPsec VPN: 네트워크 계층에서 IP 패킷을 보호하는 기술이다. 이 문제의 ㉠은 패킷이다.
SSL VPN: SSL/TLS를 이용하여 상위 계층에서 전달되는 메시지를 보호하는 기술이다. 이 문제의 ㉡은 메시지이다.
프레임은 데이터링크 계층의 전송 단위이므로 IPsec의 단위인 패킷과 구별해야 한다.

선지별 해설

① X — ㉠의 '프레임'과 ㉡의 '데이터'가 모두 틀리다. 올바르게는 IPsec VPN은 패킷 단위, SSL VPN은 메시지 단위로 데이터를 암호화한다고 구분한다.
② X — ㉠의 '데이터'와 ㉡의 '프레임'이 모두 틀리다. 올바르게는 ㉠은 패킷, ㉡은 메시지이다. 특히 프레임은 데이터링크 계층의 전송 단위이므로 SSL VPN의 암호화 단위가 아니다.
③ O — IPsec VPN은 네트워크 계층의 패킷 단위로 보호하고, SSL VPN은 상위 계층의 메시지 단위로 보호하므로 ㉠ 패킷, ㉡ 메시지가 맞다.
④ X — ㉡의 '메시지'는 맞지만 ㉠의 '메시지'가 틀리다. 올바르게는 IPsec VPN의 ㉠에는 패킷이 들어간다.

오답 포인트

'데이터'라는 포괄적 표현과 계층별 전송 단위인 프레임·패킷·메시지를 혼동하기 쉽다. 특히 ④는 SSL VPN의 메시지는 맞지만 IPsec까지 메시지로 바꾸어 놓은 선지이다.

NoteBase

다시 나오면 이렇게 판단

VPN 기술이 동작하는 계층을 먼저 찾는다. IP 계층에서 동작하는 IPsec은 패킷, SSL/TLS를 이용해 상위 계층 통신을 보호하는 SSL VPN은 메시지로 연결한다.

암기 포인트

IPsec은 IP 패킷, SSL VPN은 메시지이다.

NoteBase

문 16. 다음 <보기>는 VLAN(Virtual Local Area Network)에 대한 설명이다. 다음 중 ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
VLAN은 여러 개의 구별되는 (㉠) 도메인을 만들기 위해서 단일 2계층 네트워크를 (㉡)으로 분할하고 한 포트에서 보이는 모든 네트워크 패킷 혹은 전체 VLAN의 모든 패킷들을 다른 모니터링 포트로 복제하는 (㉢) 기능을 제공한다.

① ㉠ 유니캐스트 ㉡ 물리적 ㉢ 허브 미러링
② ㉠ 브로드캐스트 ㉡ 논리적 ㉢ 포트 미러링
③ ㉠ 유니캐스트 ㉡ 논리적 ㉢ 포트 미러링
④ ㉠ 브로드캐스트 ㉡ 물리적 ㉢ 허브 미러링

정답 2번

출제 포인트

VLAN이 만드는 도메인의 종류, 네트워크를 나누는 방식, 트래픽 복제 기능의 명칭을 구별하는 문제이다.

핵심 개념

VLAN: 하나의 물리적 2계층 네트워크를 논리적으로 분할하여 여러 개의 브로드캐스트 도메인을 구성하는 기술이다.
포트 미러링: 특정 포트에서 보이는 패킷이나 특정 VLAN의 패킷을 별도의 모니터링 포트로 복제하는 기능이다.

NoteBase

선지별 해설

① X
㉠의 '유니캐스트', ㉡의 '물리적', ㉢의 '허브 미러링'이 모두 틀렸다. VLAN은 브로드캐스트 도메인을 만들기 위해 네트워크를 논리적으로 분할하며, 패킷을 모니터링 포트로 복제하는 기능은 포트 미러링이다.

② O
VLAN은 여러 브로드캐스트 도메인을 만들도록 2계층 네트워크를 논리적으로 분할하고, 포트 미러링으로 패킷을 모니터링 포트에 복제한다. 따라서 ㉠ 브로드캐스트, ㉡ 논리적, ㉢ 포트 미러링이 모두 맞다.

③ X
㉠의 '유니캐스트'가 틀렸다. ㉡ '논리적'과 ㉢ '포트 미러링'은 맞지만, VLAN이 구분하는 것은 유니캐스트 도메인이 아니라 브로드캐스트 도메인이다.

④ X
㉡의 '물리적'과 ㉢의 '허브 미러링'이 틀렸다. ㉠ '브로드캐스트'는 맞지만, VLAN은 네트워크를 논리적으로 분할하고 패킷 복제 기능은 포트 미러링이라고 한다.

오답 포인트

VLAN이 스위치의 물리적 연결을 바꾸는 기술이라고 오해하거나, 패킷 복제 기능을 장비 이름인 허브와 연결하면 틀리기 쉽다. 핵심 표현은 '브로드캐스트 도메인', '논리적 분할', '포트 미러링'이다.

다시 나오면 이렇게 판단

VLAN 설명에서는 먼저 '브로드캐스트 도메인을 논리적으로 분리한다'를 확인하고, 감시용 포트로 트래픽을 복제한다는 표현이 나오면 '포트 미러링'으로 판단한다.

암기 포인트

VLAN은 브로드캐스트 도메인의 논리적 분할, 감시용 복제는 포트 미러링이다.

NoteBase

문 17. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
ANTI APT 솔루션에서 악성코드를 동적으로 분석하기 위해서 악성코드를 실행한 후에 행위 로그를 분석한다. 이때 악성코드 분석은 ( ) 환경에서 수행되어야 한다.

① SCADA

② Sandbox

③ Cloud

④ CRM

정답 2번

출제 포인트

악성코드를 실제로 실행해 행위를 관찰하는 동적 분석에 적합한 격리 환경을 묻는 문제이다.

핵심 개념

Sandbox는 의심스러운 프로그램을 실제 운영 환경과 분리된 통제 환경에서 실행하여 파일 변경, 프로세스 생성, 네트워크 통신 등의 행위를 관찰하는 기술이다. ANTI APT 솔루션은 이 격리 환경을 이용해 악성코드가 실제 시스템에 피해를 주지 않도록 하면서 행위 로그를 분석한다.

선지별 해설

① X — SCADA는 전력·수도·공장 같은 산업 제어 설비를 원격 감시하고 제어하는 시스템이므로 악성코드 동적 분석을 위한 격리 실행 환경이 아니다. 틀린 표현은 'SCADA'이며, 올바르게는 'Sandbox'이다.
② O — Sandbox는 악성코드를 격리된 환경에서 실행하고 그 행위 로그를 수집·분석할 수 있으므로 빈칸에 알맞다.
③ X — Cloud는 인터넷을 통해 서버·저장공간·응용 서비스 등의 컴퓨팅 자원을 제공하는 환경을 뜻하며, 그 자체가 악성코드 분석용 격리 환경을 의미하지 않는다. 틀린 표현은 'Cloud'이며, 올바르게는 'Sandbox'이다.
④ X — CRM은 고객 정보와 영업·마케팅 활동을 관리하는 고객관계관리 시스템이므로 악성코드를 실행해 분석하는 환경이 아니다. 틀린 표현은 'CRM'이며, 올바르게는 'Sandbox'이다.

오답 포인트

③의 Cloud도 원격 컴퓨팅 환경을 제공할 수 있어 혼동하기 쉽지만, 문제의 핵심은 원격성이나 자원 제공이 아니라 악성코드를 안전하게 실행하기 위한 격리와 행위 관찰이다.

NoteBase

다시 나오면 이렇게 판단

‘의심 파일을 실행한 뒤 행위 로그를 분석한다’는 표현이 나오면 실제 시스템과 분리된 실행 환경인지 확인한다. 격리 실행과 동적 행위 분석이 함께 제시되면 Sandbox로 판단한다.

암기 포인트

Sandbox는 격리 실행·행위 관찰, SCADA는 산업 제어, Cloud는 컴퓨팅 자원 제공, CRM은 고객관계관리이다.

NoteBase

문 18. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
Tcpdump는 네트워크에서 전송되는 패킷을 스니핑하는 도구이다. 전송되는 패킷을 특정 포트로 (㉠), 스니핑 모드를 (㉡)(으)로 설정해야 한다.

① ㉠ 포트 미러링 ㉡ 정규 모드
② ㉠ 무차별 모드 ㉡ 포트 미러링
③ ㉠ 포트 미러링 ㉡ 무차별 모드
④ ㉠ 무차별 모드 ㉡ 정규 모드

정답 3번

출제 포인트

스위치 환경에서 분석 대상 트래픽을 수집 포트로 복제하는 기능과, 네트워크 인터페이스가 수신 프레임을 받아들이는 모드를 구분하는 문제이다.

핵심 개념

포트 미러링은 스위치가 특정 포트나 VLAN의 트래픽을 패킷 분석기가 연결된 포트로 복제해 보내는 기능이다.
무차별 모드는 네트워크 인터페이스가 자신의 주소로 온 프레임뿐 아니라 인터페이스에 도달한 다른 프레임도 수신하도록 하는 모드이다.
정규 모드에서는 일반적으로 자신의 MAC 주소로 온 프레임과 브로드캐스트·관련 멀티캐스트 프레임만 처리한다.

선지별 해설

① X — ㉠의 포트 미러링은 맞지만 ㉡의 '정규 모드'가 틀린 표현이다. 스니핑을 위해서는 ㉡을 무차별 모드로 설정해야 한다.
② X — ㉠의 '무차별 모드'와 ㉡의 '포트 미러링'은 역할과 위치가 서로 바뀌었다. 올바르게는 ㉠이 포트 미러링이고 ㉡이 무차별 모드이다.
③ O — 스위치에서 분석할 패킷을 포트 미러링으로 수집 포트에 복제하고, Tcpdump가 사용하는 인터페이스를 무차별 모드로 동작시키는 조합이다.
④ X — ㉠의 '무차별 모드'와 ㉡의 '정규 모드'가 모두 틀린 표현이다. 올바르게는 전송 패킷을 특정 포트로 포트 미러링하고 스니핑 모드를 무차별 모드로 설정한다.

NoteBase

오답 포인트

포트 미러링과 무차별 모드는 모두 패킷 수집에 쓰이지만 적용 대상이 다르다. 포트 미러링은 스위치가 트래픽을 복제하는 기능이고, 무차별 모드는 수집 호스트의 네트워크 인터페이스가 프레임을 받아들이는 방식이다.

다시 나오면 이렇게 판단

문장에서 '특정 포트로 트래픽을 복제한다'는 표현은 포트 미러링, '인터페이스가 자기 주소 이외의 프레임도 수신한다'는 표현은 무차별 모드로 판단한다.

암기 포인트

스위치는 미러링, 수집 인터페이스는 무차별 모드이다.

NoteBase

문 19. 다음 중 <보기>의 설명에서 ( )에 들어갈 설명으로 가장 옳은 것은?

<보기>
IPv6는 (㉠)비트의 주소 공간을 가지며 헤더는 총 (㉡)개의 필드를 가지고 있다. 그리고 암호화와 (㉢)기능을 지원한다.

① ㉠ 128 ㉡ 8 ㉢ 인증
② ㉠ 32 ㉡ 4 ㉢ 인증
③ ㉠ 32 ㉡ 8 ㉢ 인가
④ ㉠ 128 ㉡ 4 ㉢ 인가

정답 1번

출제 포인트

IPv6의 주소 길이, 기본 헤더의 필드 수, IPsec이 제공하는 보안 기능을 정확히 연결하는 문제이다.

핵심 개념

IPv6는 IPv4를 대체하기 위해 설계된 인터넷 프로토콜로서 128비트 주소를 사용한다. IPv6 기본 헤더는 Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, Destination Address의 8개 필드로 구성된다. IPsec의 AH와 ESP를 통해 데이터 출처 인증·무결성 및 암호화에 의한 기밀성 같은 보안 기능을 지원한다. 여기서 인증은 통신 주체나 데이터의 출처를 확인하는 것이고, 인가는 인증된 주체에게 자원 접근 권한을 부여하는 것이다.

선지별 해설

① O — IPv6의 주소 공간은 128비트이고 기본 헤더는 8개 필드로 구성되며, IPsec을 통해 암호화와 인증 기능을 지원하므로 세 항목이 모두 맞는다.
② X — ‘32비트’와 ‘4개’가 틀린 표현이다. 올바르게는 ‘128비트의 주소 공간, 8개의 기본 헤더 필드, 인증’이다.
③ X — ‘32비트’와 ‘인가’가 틀린 표현이다. 올바르게는 ‘128비트의 주소 공간, 8개의 기본 헤더 필드, 인증’이다.
④ X — ‘4개’와 ‘인가’가 틀린 표현이다. 올바르게는 ‘128비트의 주소 공간, 8개의 기본 헤더 필드, 인증’이다.

오답 포인트

32비트는 IPv4의 주소 길이이므로 IPv6의 128비트와 혼동하면 안 된다. 또한 인증은 신원이나 데이터 출처를 확인하는 기능이고, 인가는 확인된 주체에게 권한을 부여하는 기능이므로 서로 바꾸어 쓸 수 없다.

NoteBase

다시 나오면 이렇게 판단

IPv6의 기본 묶음을 '128비트 주소, 기본 헤더 8개 필드, IPsec의 인증·암호화 지원'으로 먼저 확정한 뒤 각 빈칸을 대조한다.

암기 포인트

IPv6는 128-8-인증이다. 32비트는 IPv4이고, 인가는 권한 부여이다.

NoteBase

문 20. 다음 중 리눅스 시스템의 네트워크 관리 도구 및 서비스에 대한 설명으로 가장 옳지 않은 것은?

① ifconfig - 네트워크 인터페이스의 IP 주소 설정

② traceroute - 최종 목적지 컴퓨터까지 중간에 걸치는 여러 개의 라우터에 대한 경로 및 응답 속도를 표시

③ fping - 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력

④ tcpdump - 네트워크 모니터링 및 패킷 분석을 위해 사용되는 도구로, 패킷 필터 기능을 통해서, 특정 침입자의 침입 경로에 따라 원하는 트래픽만을 감시

정답 3번

출제 포인트

리눅스 네트워크 관리 명령어의 기능을 구별하는 문제이다. 특히 fping과 netstat의 역할을 바꾸어 놓은 표현을 판별해야 한다.

핵심 개념

ifconfig는 네트워크 인터페이스의 주소와 동작 상태를 확인하거나 설정하는 명령어이다. traceroute는 목적지까지 패킷이 거치는 홉과 각 홉의 응답 시간을 추적한다. fping은 ICMP Echo 요청을 이용하여 여러 호스트의 도달 가능 여부를 효율적으로 확인한다. netstat는 네트워크 연결 상태, 라우팅 테이블, 인터페이스 통계 등을 출력한다. tcpdump는 네트워크 인터페이스를 지나는 패킷을 수집하고 필터 조건에 따라 분석하는 도구이다.

선지별 해설

① O — ifconfig는 네트워크 인터페이스의 IP 주소, 넷마스크 등의 정보를 확인하고 설정하는 데 사용한다.
② O — traceroute는 목적지까지 거치는 라우터의 경로를 홉 단위로 보여 주며, 각 홉에서 측정된 응답 시간도 표시한다.
③ X — 틀린 부분은 ‘fping - 네트워크 연결 상태, 라우팅 테이블, 인터페이스 관련 통계 정보 출력’이다. 이 기능은 주로 netstat에 해당한다. 올바르게는 ‘fping은 ICMP Echo 요청을 이용하여 하나 이상의 호스트가 응답하는지 빠르게 확인하는 도구’이다.
④ O — tcpdump는 패킷을 수집·분석하며, 패킷 필터 표현식을 이용하여 호스트, 주소, 포트, 프로토콜 등 조건에 맞는 트래픽만 선택해 감시할 수 있다.

오답 포인트

③은 fping이라는 명령어 이름에 netstat의 기능을 붙인 선지이다. fping의 핵심은 호스트의 도달 가능 여부 확인이고, 연결·라우팅·인터페이스 통계 출력은 netstat의 대표 기능이다.

NoteBase

다시 나오면 이렇게 판단

명령어를 기능별로 대응시킨다. 인터페이스 설정은 ifconfig, 경로 추적은 traceroute, 다중 호스트 응답 확인은 fping, 연결·라우팅 통계는 netstat, 패킷 수집과 필터링은 tcpdump이다.

암기 포인트

fping은 호스트 응답 확인, netstat는 네트워크 상태·통계 확인이다.

NoteBase