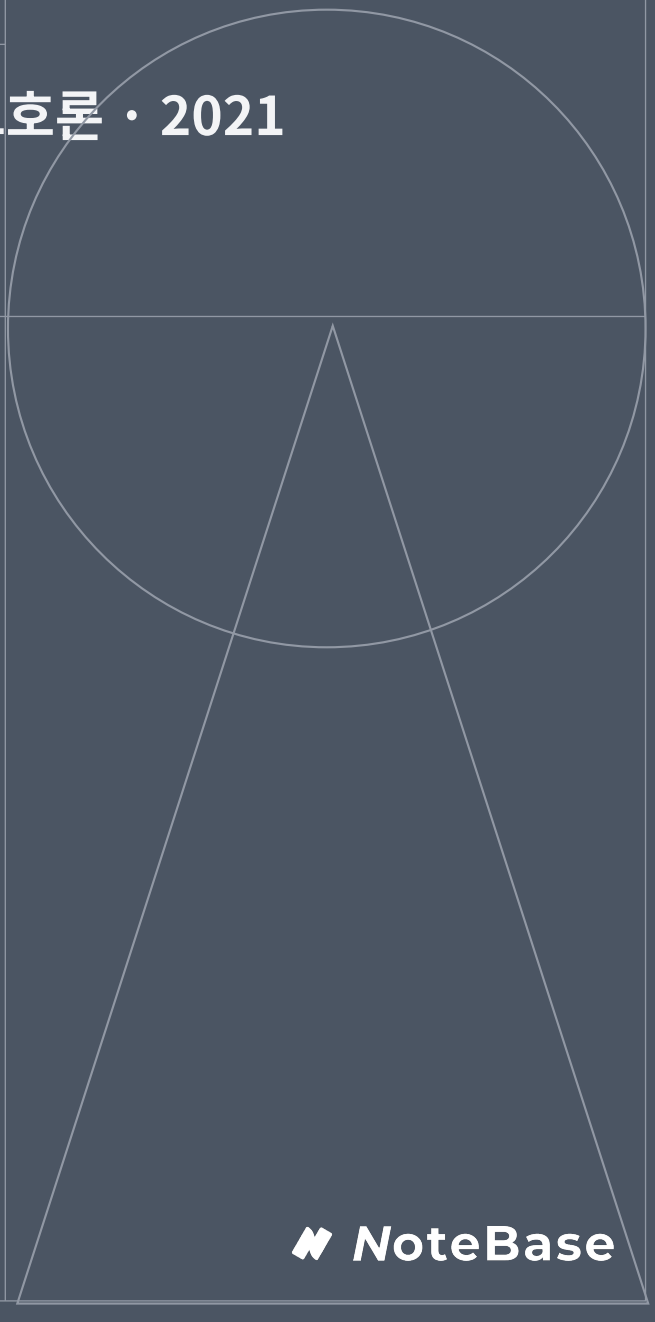
기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2021



NoteBase

기출OX 해설집

공무원/국회직/9급 · 정보보호론 · 2021

공무원/국회직/9급 · 정보보호론 · 2021

1. 선택된 폴더의 데이터를 완전 백업(Full Backup)한 후, 다음번 완전 백업(Full Backup)을 시행하기 전까지는 변경, 추가된 데이터만 백업하는 방식은?

   ① 일반 백업(Normal Backup)
   ② 매일 백업(Daily Backup)
   ③ 복사본 백업(Copy Backup)
   ④ 차등 백업(Differential Backup)
   ⑤ 증분 백업(Incremental Backup)

정답 5번

출제 포인트

이 문제는 완전 백업 이후 다음 완전 백업 전까지 변경되거나 새로 추가된 데이터만 저장하는 증분 백업의 개념을 묻는 문제이다.

핵심 개념

완전 백업은 선택한 데이터를 모두 백업하는 방식이다. 증분 백업은 직전 백업 이후 변경·추가된 데이터만 백업하고, 차등 백업은 마지막 완전 백업 이후 변경·추가된 데이터를 매번 모두 백업한다. 따라서 증분 백업은 회차별 백업량이 작지만 복구할 때 완전 백업본과 이후의 모든 증분 백업본이 필요하다.

NoteBase

선지별 해설

① X — 일반 백업(Normal Backup)은 선택한 데이터를 모두 백업하는 방식이므로 '변경·추가된 데이터만 백업'하는 방식이 아니다. 올바르게는 선택한 전체 데이터를 백업하는 방식이다.
② X — 매일 백업(Daily Backup)은 해당 날짜에 변경된 파일을 백업하는 방식으로, 마지막 완전 백업이나 직전 백업을 기준으로 변경분을 누적하는 방식이 아니다. 올바르게는 당일 변경된 데이터를 백업하는 방식이다.
③ X — 복사본 백업(Copy Backup)은 선택한 데이터를 복사하듯 백업하되 다른 백업 작업의 기준 상태에 영향을 주지 않는 방식이다. 올바르게는 선택한 데이터를 별도로 복사하여 백업하는 방식이다.
④ X — 차등 백업(Differential Backup)은 '직전 백업 이후의 변경분만'이 아니라 마지막 완전 백업 이후 변경·추가된 데이터를 매번 누적하여 백업한다. 올바르게는 마지막 완전 백업을 기준으로 한 모든 변경분을 백업하는 방식이다.
⑤ O — 증분 백업(Incremental Backup)은 완전 백업 후 직전 백업 이후 변경되거나 새로 추가된 데이터만 백업한다. 문제에서 묻는 방식에 해당한다.

오답 포인트

④ 차등 백업도 변경·추가된 데이터만 다루기 때문에 ⑤와 혼동하기 쉽다. 차등 백업의 기준은 항상 마지막 완전 백업이고, 증분 백업의 기준은 직전 백업이라는 점이 핵심이다.

다시 나오면 이렇게 판단

변경분의 기준 시점을 확인한다. '직전 백업 이후'이면 증분 백업, '마지막 완전 백업 이후의 변경분 전체'이면 차등 백업으로 판단한다.

암기 포인트

증분은 직전부터 조금씩, 차등은 완전 백업부터 누적한다.

NoteBase

2. 강화된 무선 네트워크 보안 기법으로서 기존 IEEE 802.11의 보안 취약성을 해결한 IEEE 802.11i 및 RSN 보안 기법에 해당하는 것은?

① ARIA
② AES
③ RC4
④ WPA2
⑤ EAP

정답 4번

출제 포인트

IEEE 802.11i의 RSN 보안 체계를 구현한 무선 LAN 보안 규격과, 그 체계 안에서 사용되는 암호 알고리즘·인증 방식의 역할을 구분하는 문제이다.

핵심 개념

IEEE 802.11i는 WEP의 취약점을 보완하기 위해 강한 인증, 키 관리, 암호화 및 무결성 보호를 규정한 무선 LAN 보안 표준이며, RSN은 이 표준이 정의한 보안 네트워크 체계이다.
WPA2는 IEEE 802.11i의 RSN 요구사항을 구현한 무선 LAN 보안 규격이다. WPA2에서 대표적으로 사용하는 보호 방식은 AES 기반의 CCMP이다.
AES는 암호 알고리즘이고, EAP는 인증 절차를 운반·확장하는 프레임워크이므로 WPA2라는 전체 보안 규격과 구분된다.

선지별 해설

① X — ARIA는 블록 암호 알고리즘이지만 IEEE 802.11i의 RSN을 구현한 무선 LAN 보안 규격은 아니다. 틀린 표현 'ARIA'는 'WPA2'로 고쳐야 한다.
② X — AES는 802.11i/WPA2의 CCMP에서 사용되는 핵심 블록 암호이지만, 그 자체가 RSN 전체를 구현한 보안 규격의 명칭은 아니다. 틀린 표현 'AES'는 전체 규격을 묻는 이 문항에서는 'WPA2'로 고쳐야 하며, 정확히는 AES-CCMP가 WPA2의 암호화·무결성 보호에 사용된다.
③ X — RC4는 WEP 및 WPA의 TKIP 계열에서 사용된 스트림 암호로, 802.11i의 강한 RSN 보안을 대표하는 규격이 아니다. 틀린 표현 'RC4'는 'WPA2'로 고쳐야 한다.
④ O — WPA2는 IEEE 802.11i의 RSN 보안 체계를 구현한 무선 LAN 보안 규격으로, WEP의 취약성을 보완하고 AES-CCMP를 중심으로 강한 기밀성과 무결성 보호를 제공한다.
⑤ X — EAP는 사용자·단말 인증 방식을 수용하는 인증 프레임워크이지 무선 구간의 암호화와 무결성까지 규정하는 RSN 보안 규격은 아니다. 틀린 표현 'EAP'는 'WPA2'로 고쳐야 한다.

오답 포인트

② AES가 WPA2의 핵심 암호라는 사실 때문에 AES를 정답으로 고르기 쉽다. 그러나 문제는 구성 알고리즘이 아니라 IEEE 802.11i 및 RSN에 해당하는 전체 보안 규격을 묻고 있으므로 WPA2를 선택해야 한다.

NoteBase

다시 나오면 이렇게 판단

선지가 전체 보안 규격인지 구성 기술인지 먼저 구분한다. IEEE 802.11i·RSN·WEP 취약점 보완이라는 단서가 함께 나오면 WPA2를 고르고, AES-CCMP는 암호화·무결성 보호 방식, EAP는 인증 프레임워크로 분류한다.

암기 포인트

802.11i·RSN은 WPA2, WPA2의 핵심 보호 방식은 AES-CCMP이다.

NoteBase

3. 아래 표에서 ㉠과 ㉡의 특징을 갖는 주요 악성코드를 옳게 짝지은 것은?

㉠	㉡
컴퓨터 취약점을 이용하여 네트워크 통한 감염 및 실행	컴퓨터 사용 시 자동으로 광고를 표시하는 악성코드
자기복제: O	자기복제: X
독립적인 프로그램: O	독립적인 프로그램: X

	㉠	㉡
①	웜	애드웨어
②	트로이 목마	애드웨어
③	애드웨어	바이러스
④	바이러스	트로이 목마
⑤	웜	트로이 목마

정답 1번

출제 포인트

자기복제 여부, 독립 실행 여부, 대표 행위를 기준으로 웜·바이러스·트로이 목마·애드웨어를 구별하는 문제이다.

핵심 개념

웜: 운영체제나 소프트웨어의 취약점을 이용해 네트워크로 스스로 전파되는 독립형 악성코드이다. 자기복제를 하며 다른 프로그램에 기생하지 않고 실행된다.
애드웨어: 컴퓨터 사용 중 광고를 자동으로 표시하는 소프트웨어이다. 이 문제의 분류에서는 자기복제와 독립적인 프로그램이라는 특징이 없다.
바이러스: 다른 파일이나 프로그램에 붙어 실행되고 복제되는 악성코드이므로 독립 실행형이 아니다.
트로이 목마: 정상적이거나 유용한 프로그램처럼 위장해 사용자의 실행을 유도하는 악성코드이며 자기복제를 하지 않는다.
따라서 네트워크 전파·자기복제·독립 실행은 웜, 자동 광고 표시·자기복제 없음·독립 프로그램 아님은 애드웨어에 해당한다.

NoteBase

선지별 해설

① O — ㉠은 네트워크로 감염·실행되며 자기복제하고 독립적으로 작동하므로 웜이다. ㉡은 광고를 자동 표시하고 자기복제하지 않으므로 애드웨어이다.
② X — ㉡의 애드웨어는 맞지만, ㉠의 '트로이 목마'가 틀렸다. 트로이 목마는 자기복제를 하지 않으므로, ㉠은 웜으로 고쳐야 한다.
③ X — ㉠의 '애드웨어'와 ㉡의 '바이러스'가 모두 틀렸다. ㉠은 네트워크 자기전파형인 웜이고, ㉡은 자동 광고 표시형인 애드웨어이다.
④ X — ㉠의 '바이러스'와 ㉡의 '트로이 목마'가 모두 틀렸다. 바이러스는 다른 파일이나 프로그램에 기생하므로 독립적인 프로그램이라는 ㉠의 특징과 맞지 않는다. ㉠은 웜, ㉡은 애드웨어로 고쳐야 한다.
⑤ X — ㉠의 웜은 맞지만, ㉡의 '트로이 목마'가 틀렸다. 광고를 자동으로 표시하는 ㉡은 애드웨어이다.

오답 포인트

'자기복제'만 보고 바이러스를 고르면 ④에 빠지기 쉽다. ㉠에는 자기복제뿐 아니라 네트워크를 통한 감염과 독립 실행도 제시되어 있으므로 바이러스가 아니라 웜이다. 또한 ㉡의 결정적 표현은 '광고를 표시'이므로 트로이 목마가 아니라 애드웨어이다.

다시 나오면 이렇게 판단

먼저 대표 행위를 확인하고 실행 형태를 함께 대조한다. 네트워크로 스스로 퍼지고 독립 실행하면 웜, 다른 파일에 기생해 복제되면 바이러스, 정상 프로그램처럼 위장하되 자기복제가 없으면 트로이 목마, 광고를 자동 표시하면 애드웨어로 판단한다.

암기 포인트

웜은 '혼자 복제해 네트워크 전파', 바이러스는 '숙주에 기생', 트로이 목마는 '위장', 애드웨어는 '광고'이다.

NoteBase

4. 암호 알고리즘에 대한 설명으로 옳지 않은 것은?

① Adaptive Chosen-plaintext Attack은 Ciphertext-only Attack보다 공격자 입장에서 더 높은 자유도를 갖는다.

② Differential Cryptanalysis는 평문과 암호문 간의 차분 정보를 사용하는 암호 공격 기법이다.

③ Side-channel Attack은 소비 전력이나 실행 시간 등 암호의 구현상 특성을 활용하는 공격 기법이다.

④ Birthday Attack은 공개키 암호 알고리즘의 암호 안전도를 측정하는 데 사용된다.

⑤ 해시함수는 Collision Resistance를 가져야 한다.

정답 4번

출제 포인트

암호 공격 기법마다 공격자가 이용하는 정보와 평가 대상이 무엇인지 구별하는 문제이다.

핵심 개념

Adaptive Chosen-plaintext Attack은 공격자가 이전 암호화 결과를 바탕으로 다음 평문을 선택해 암호문을 얻는 공격이다. Differential Cryptanalysis는 평문 쌍의 차이가 암호문 쌍의 차이에 미치는 확률적 관계를 분석한다. Side-channel Attack은 알고리즘의 수학적 구조가 아니라 실행 시간, 소비 전력 등 구현 과정에서 새는 정보를 이용한다. Birthday Attack은 생일 역설을 이용해 해시값의 충돌을 찾는 공격으로, 해시함수의 충돌 내성과 관련된다.

NoteBase

선지별 해설

① O — Adaptive Chosen-plaintext Attack에서는 공격자가 평문을 선택해 그 암호문을 얻고, 앞선 결과에 따라 다음 질의를 조정할 수 있다. 암호문만 관찰하는 Ciphertext-only Attack보다 공격자가 활용할 수 있는 정보와 자유도가 크다.
② O — Differential Cryptanalysis는 선택한 평문 쌍의 차분과 그에 대응하는 암호문 쌍의 차분 사이의 관계를 이용하는 공격 기법이다. 선지의 '평문과 암호문 간의 차분 정보'는 이러한 평문 차분과 암호문 차분의 대응 관계를 뜻한다.
③ O — Side-channel Attack은 암호 구현이 작동할 때 드러나는 소비 전력, 실행 시간 등의 물리적 부가 정보를 이용한다.
④ X — 틀린 표현은 '공개키 암호 알고리즘의 암호 안전도를 측정'한다는 부분이다. Birthday Attack은 해시함수에서 같은 해시값을 만드는 서로 다른 입력, 즉 충돌을 찾는 데 이용되며 해시함수의 충돌 내성을 평가하는 공격으로 고쳐야 한다.
⑤ O — 암호학적 해시함수는 서로 다른 두 입력이 같은 해시값을 갖는 충돌을 현실적으로 찾기 어려운 Collision Resistance를 갖추어야 한다.

오답 포인트

④의 '암호 안전도를 측정'이라는 표현만 보고 일반적인 암호 공격으로 받아들이기 쉽다. Birthday Attack의 핵심 대상은 공개키 암호가 아니라 해시함수의 충돌이며, 이는 ⑤의 Collision Resistance와 직접 연결된다.

다시 나오면 이렇게 판단

공격 기법을 공격자가 이용하는 정보로 구분한다. 암호문만 이용하면 Ciphertext-only, 선택한 평문과 암호문을 이용하면 Chosen-plaintext, 전력·시간을 이용하면 Side-channel, 같은 해시값을 만드는 두 입력을 찾으면 Birthday Attack이다.

암기 포인트

적응형 선택평문은 질의를 조정하고, 차분 공격은 평문·암호문 차분을 비교하며, 부채널은 전력·시간을 보고, 생일 공격은 해시 충돌을 찾는다.

NoteBase

5. 양자내성암호(Post-Quantum Cryptography)에 대한 설명으로 옳지 않은 것은?

① 양자컴퓨터의 실현 가능성이 높아짐에 따라 기존 대칭키 암호를 대체하는 목적으로 만들어지고 있다.

② RSA는 양자내성암호로 볼 수 없다.

③ 양자내성암호의 종류로는 격자 기반 암호, 코드 기반 암호, 해시기반 암호 등이 있다.

④ 양자내성암호는 알고리즘의 종류에 따라 키 교환 목적, 전자서명 목적으로 사용된다.

⑤ 양자내성암호는 NIST에 의해 표준화가 진행되고 있다.

정답 1번

출제 포인트

양자내성암호가 대체하려는 기존 암호의 범위와 주요 기반 문제, 용도 및 표준화 현황을 구별하는 문제이다.

핵심 개념

양자내성암호(PQC)는 양자컴퓨터로도 풀기 어렵다고 평가되는 수학적 문제에 기반한 공개키 암호이다. 주된 목적은 양자 알고리즘에 취약한 RSA·타원곡선암호 등 기존 공개키 암호의 기능을 대체하는 것이며, 대표 계열에는 격자 기반·코드 기반·해시 기반 암호 등이 있다. 대칭키 암호는 양자컴퓨터의 영향이 전혀 없는 것은 아니지만, 충분한 키 길이를 사용해 대응할 수 있으므로 PQC의 직접적인 대체 대상이라는 표현은 부정확하다.

NoteBase

선지별 해설

① X
틀린 표현은 '기존 대칭키 암호를 대체'한다는 부분이다. 양자내성암호는 주로 쇼어 알고리즘에 취약한 RSA·타원곡선암호 등 기존 공개키 암호를 대체하기 위해 개발된다. 올바르게는 '기존 공개키 암호를 대체하는 목적으로 만들어지고 있다'이다.

② O
RSA는 큰 정수의 소인수분해 난이도에 안전성을 두지만, 충분한 규모의 양자컴퓨터에서는 쇼어 알고리즘으로 효율적으로 공격할 수 있으므로 양자내성암호가 아니다.

③ O
양자내성암호의 대표적인 설계 계열에는 격자 기반 암호, 코드 기반 암호, 해시 기반 암호 등이 있다. 서로 다른 난제에 기반하여 양자 공격에 대한 안전성을 확보하려는 방식이다.

④ O
양자내성 공개키 알고리즘은 기능에 따라 공유 비밀을 설정하는 키 설정·키 캡슐화와 전자서명에 사용된다. 문항의 '키 교환 목적'은 이러한 키 설정 기능을 가리키는 표현으로 볼 수 있다.

⑤ O
NIST는 양자내성암호 표준화 사업을 수행해 왔다. 2024년에 ML-KEM, ML-DSA, SLH-DSA 표준을 확정했으며, 추가 알고리즘에 대한 표준화도 계속 진행하고 있으므로 NIST에 의해 표준화가 진행된다는 설명은 타당하다.

오답 포인트

①은 '양자컴퓨터가 기존 암호를 위협한다'는 사실을 모든 암호가 같은 방식으로 대체된다는 뜻으로 바꾼 함정이다. PQC는 새로운 대칭키 암호의 명칭이 아니라, RSA·타원곡선암호와 같은 공개키 암호의 양자 취약성을 보완하는 공개키 암호 기술이다.

다시 나오면 이렇게 판단

대체 대상을 먼저 확인한다. RSA·타원곡선암호처럼 소인수분해나 이산로그에 기반한 공개키 암호가 대상이면 PQC의 취지에 맞고, 대칭키 암호 전체를 PQC가 대체한다고 하면 틀린 설명으로 판단한다. 이어서 기반 난제는 격자·코드·해시, 기능은 키 설정과 전자서명으로 구분한다.

암기 포인트

PQC는 '대칭키 대체'가 아니라 '양자에 취약한 공개키 암호 대체'이다. 대표 축은 격자·코드·해시, 대표 기능은 키 설정·전자서명이다.

NoteBase

6. 다음에서 설명하는 DoS 공격 유형은?

> 패킷을 전송할 때 출발지 IP주소와 목적지 IP주소의 값을 똑같이 만들어서 공격대상에게 보낸다. 이때 조작된 목적지 IP주소는 공격대상의 IP주소이다. 이렇게 목적지 주소가 조작된 패킷을 공격대상에게 보내면 시스템은 공격자가 보낸 SYN패킷의 출발지 주소를 참조하여 응답패킷을 보내는데, 이때 패킷이 네트워크 밖으로 나가지 않고 자신에게 다시 되돌아오며, 돌아온 패킷의 출발지 IP주소에는 또다시 자신의 IP주소가 기록되어 시스템을 마비시키는 공격의 종류이다.

① Ping of Death
② Land Attack
③ SYN Flooding Attack
④ Smurf Attack
⑤ Mail Bomb

정답 2번

출제 포인트

출발지 IP 주소와 목적지 IP 주소를 모두 공격 대상의 주소로 위조하여, 공격 대상이 자기 자신에게 응답하게 만드는 DoS 공격을 식별하는 문제이다.

핵심 개념

Land Attack은 조작한 패킷의 출발지 IP 주소와 목적지 IP 주소를 모두 공격 대상의 IP 주소로 설정하여, 공격 대상이 보낸 응답이 다시 자기 자신에게 돌아가도록 만드는 공격이다. 핵심 식별어는 '출발지 IP = 목적지 IP = 공격 대상 IP'이다.
Ping of Death는 비정상적으로 큰 ICMP 패킷을 이용하고, SYN Flooding은 다량의 연결 요청으로 반개방 연결을 누적시키며, Smurf Attack은 브로드캐스트망의 ICMP 응답을 피해자에게 집중시키고, Mail Bomb은 대량의 전자우편을 발송한다.

NoteBase

선지별 해설

① X — 틀린 표현은 'Ping of Death'이다. Ping of Death는 허용 범위를 넘는 비정상적으로 큰 ICMP 패킷을 전송하여 시스템 장애를 유발하는 공격이다. 제시문처럼 출발지와 목적지 IP 주소를 모두 피해자의 주소로 위조하는 공격은 Land Attack이다.
② O — Land Attack은 SYN 패킷의 출발지 IP 주소와 목적지 IP 주소를 모두 공격 대상의 IP 주소로 조작한다. 그 결과 공격 대상이 생성한 응답 패킷이 자기 자신에게 되돌아오므로 제시문의 설명과 일치한다.
③ X — 틀린 표현은 'SYN Flooding Attack'이다. SYN Flooding Attack은 다량의 SYN 패킷을 보내 서버에 반개방 연결을 누적시켜 연결 자원을 고갈시키는 공격이다. 제시된 주소 조작 방식은 Land Attack이다.
④ X — 틀린 표현은 'Smurf Attack'이다. Smurf Attack은 피해자의 IP 주소로 출발지를 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 여러 호스트의 응답이 피해자에게 집중되게 하는 증폭 공격이다. 출발지와 목적지를 모두 피해자 주소로 설정하는 공격은 Land Attack이다.
⑤ X — 틀린 표현은 'Mail Bomb'이다. Mail Bomb은 특정 수신자나 메일 서버에 대량의 전자우편을 보내 저장 공간이나 처리 자원을 고갈시키는 공격이다. 제시문의 패킷 주소 조작 공격은 Land Attack이다.

오답 포인트

제시문에 SYN 패킷이 등장한다는 이유만으로 ③ SYN Flooding Attack을 고르기 쉽다. 그러나 공격 유형은 패킷 종류보다 작동 방식으로 판단해야 한다. 다량의 SYN으로 반개방 연결을 쌓으면 SYN Flooding이고, 출발지와 목적지 IP를 모두 피해자 주소로 만들어 자기 자신에게 응답하게 하면 Land Attack이다.

다시 나오면 이렇게 판단

출발지 IP와 목적지 IP가 모두 피해자 자신의 IP인지 먼저 확인한다. 두 주소가 같고 피해자가 자기 자신에게 응답하는 구조이면 Land Attack으로 판단한다. 브로드캐스트를 통한 응답 증폭이면 Smurf Attack, 반개방 연결의 누적이면 SYN Flooding으로 구별한다.

암기 포인트

Land는 출발지도 피해자, 목적지도 피해자이다. SYN Flooding은 반개방 연결 누적, Smurf는 브로드캐스트 증폭이다.

NoteBase

7. OSI 7 Layer 중 계층별 프로토콜의 연결이 옳지 않은 것은?

	OSI 모델	프로토콜
①	응용계층	HTTP, FTP
②	표현계층	MPEG, Telnet
③	전송계층	TCP, UDP
④	네트워크계층	IP, ICMP
⑤	데이터링크계층	Ethernet

정답 2번

출제 포인트

OSI 7계층에서 대표 프로토콜과 데이터 형식이 어느 계층에 속하는지를 구분하는 문제이다.

핵심 개념

응용계층: 사용자의 네트워크 응용 서비스가 동작하는 계층이다. 대표 프로토콜은 HTTP, FTP, Telnet이다.
표현계층: 데이터의 표현 형식을 변환하고 인코딩·압축·암호화를 담당하는 계층이다. MPEG은 이 계층과 연결된다.
전송계층: 종단 간 데이터 전송을 담당하는 계층이다. 대표 프로토콜은 TCP, UDP이다.
네트워크계층: 논리 주소와 경로 선택을 담당하는 계층이다. 대표 프로토콜은 IP, ICMP이다.
데이터링크계층: 같은 네트워크 구간에서 프레임 단위 전송과 매체 접근을 담당하는 계층이다. Ethernet이 대표적이다.

선지별 해설

① O — HTTP와 FTP는 모두 사용자의 웹·파일 전송 서비스를 제공하는 응용계층 프로토콜이므로 연결이 옳다.
② X — 틀린 부분은 표현계층에 'MPEG, Telnet'을 함께 연결한 것이다. MPEG은 데이터 압축·표현과 관련되어 표현계층에 해당하지만, Telnet은 원격 접속 서비스를 제공하는 응용계층 프로토콜이다. 올바르게는 '표현계층-MPEG, 응용계층-Telnet'이다.
③ O — TCP와 UDP는 종단 간 전송을 담당하는 전송계층 프로토콜이므로 연결이 옳다.
④ O — IP는 논리 주소 지정과 패킷 전달을, ICMP는 네트워크 오류 및 상태 메시지 전달을 담당하므로 둘 다 네트워크계층에 해당한다.
⑤ O — Ethernet은 프레임 전송과 매체 접근 제어에 사용되는 대표적인 데이터링크계층 기술이므로 연결이 옳다.

NoteBase

오답 포인트

②는 MPEG이 표현계층에 속한다는 사실 때문에 전체 연결이 맞아 보이게 만든 선지이다. 한 선지에 두 항목이 제시되면 둘 다 해당 계층에 속하는지 각각 확인해야 하며, Telnet은 표현계층이 아니라 응용계층이다.

다시 나오면 이렇게 판단

프로토콜의 기능을 기준으로 계층을 판단한다. 사용자 서비스는 응용계층, 데이터 형식·압축은 표현계층, 종단 간 전송은 전송계층, 주소·경로 선택은 네트워크계층, 프레임·매체 접근은 데이터링크계층으로 구분한다.

암기 포인트

HTTP·FTP·Telnet은 응용, MPEG은 표현, TCP·UDP는 전송, IP·ICMP는 네트워크, Ethernet은 데이터링크이다.

NoteBase

8. IP주소에 대한 설명으로 옳지 않은 것은?

① IP주소는 TCP/IP 프로토콜로 접속된 네트워크에서 각 컴퓨터를 식별하는 데 사용하는 숫자이다.
② InterNIC에서 관리하는 IP주소는 네트워크와 호스트(노드)로 구성되어 있다.
③ IPv6는 IP주소 공간의 부족, 12개 필드로 구성된 IPv4 헤더 영역의 비효율적인 사용, 네트워크 프래그멘테이션 증가로 인한 스위칭의 비효율성 문제를 해결하기 위해 개발되었다.
④ IPv4 주소는 상위 4비트 값을 기초로 다섯 개의 클래스로 분류된다.
⑤ 클래스 D는 멀티캐스트용 주소이다.

정답 3번

출제 포인트

IP 주소의 역할과 IPv4의 클래스 구분, IPv6의 도입 배경 및 단순화된 헤더 구조를 구별하는 문제이다.

핵심 개념

IP 주소: TCP/IP 네트워크에서 인터페이스를 식별하고 패킷의 전달 경로를 정하는 논리 주소이다.
IPv4: 32비트 주소를 사용하며 전통적인 클래스 방식에서는 최상위 비트 패턴에 따라 A, B, C, D, E의 다섯 클래스로 구분한다.
IPv6: IPv4 주소 부족을 해결하기 위해 128비트 주소를 사용하고, 기본 헤더를 단순화하여 라우터의 패킷 처리 효율을 높인 방식이다. IPv6에서는 중간 라우터가 패킷을 단편화하지 않고 송신 호스트만 단편화를 수행한다.

선지별 해설

① O — IP 주소는 TCP/IP 기반 네트워크에서 통신 주체의 인터페이스를 식별하는 데 사용하는 숫자 형식의 논리 주소이다.
② O — 전통적인 IPv4 주소는 네트워크 부분과 해당 네트워크 안의 호스트(노드) 부분으로 구성된다. InterNIC은 인터넷 주소 자원의 등록·할당을 담당했던 기관이다.
③ X — 틀린 표현은 '네트워크 프래그멘테이션 증가로 인한 스위칭의 비효율성 문제'이다. IPv6의 핵심 도입 배경은 IPv4 주소 공간 부족의 해결과 헤더 단순화를 통한 라우팅 처리 효율 향상이다. 또한 IPv6에서는 중간 라우터가 단편화하지 않고 송신 호스트만 단편화하므로, 올바르게는 '주소 공간을 확대하고 기본 헤더를 단순화하며 라우터의 단편화 부담을 없애기 위해 개발되었다'라고 해야 한다.
④ O — 클래스 기반 IPv4 주소는 최상위 비트 패턴을 기준으로 A, B, C, D, E의 다섯 클래스로 분류된다.
⑤ O — 클래스 D 주소는 하나의 송신자가 여러 수신자에게 전송하는 멀티캐스트용 주소로 사용된다.

NoteBase

오답 포인트

③은 IPv6의 주소 공간 확대와 헤더 단순화라는 맞는 내용을 앞에 배치한 뒤, 단편화 문제를 '네트워크 프래그멘테이션 증가에 따른 스위칭 비효율'로 부정확하게 표현한 선지이다. IPv6에서 확인할 핵심은 중간 라우터가 단편화를 수행하지 않는다는 점이다.

다시 나오면 이렇게 판단

IPv6 도입 목적을 묻는 선지는 '128비트 주소 공간 확대, 기본 헤더 단순화, 라우터 단편화 금지'를 기준으로 판단한다. IPv4 클래스 문제는 A~C가 일반적인 유니캐스트 주소 범위, D가 멀티캐스트, E가 실험·예약용이라는 구분을 적용한다.

암기 포인트

IPv6는 주소는 크게, 헤더는 단순하게, 단편화는 송신 호스트에서만 수행한다. IPv4 클래스 D는 멀티캐스트이다.

NoteBase

9. RSA 암호 시스템에서 오일러 Totient 함수는 $\varnothing(n)=${n보다 작은 양의 정수 중에서 n과 서로소인 양의 정수의 개수}로 정의할 수 있다. p와 q가 각각 서로 다른 소수(Prime Number)라고 가정할 때, 옳지 않은 것은?

① $\varnothing(p)=p-1$

② $\varnothing(p \cdot q)=\varnothing(p)\varnothing(q)$

③ $a^{\varnothing(2\cdot p)} \not\equiv a^{\varnothing(p)} (\mathrm{mod}\, p)$: 만일 p가 2보다 큰 소수이고, a는 p에 의하여 나누어지지 않는 양의 정수일 때

④ $a^{\varnothing(n)} \equiv 1 (\mathrm{mod}\, n)$: 서로소인 a와 n에 대하여

⑤ $\varnothing(35)=24$

정답 3번

출제 포인트

오일러 피 함수의 소수에 대한 값과 곱셈적 성질, 오일러 정리를 정확히 적용할 수 있는지를 묻는 문제이다.

핵심 개념

오일러 피 함수 $\varphi(n)$는 1부터 n까지의 정수 중 n과 서로소인 양의 정수의 개수이다.
소수 p에 대해서는 $\varphi(p) = p - 1$이고, 서로소인 m, n에 대해서는 $\varphi(mn) = \varphi(m)\varphi(n)$이다.
또한 gcd(a, n) = 1이면 오일러 정리에 따라 a^(n)≡ 1±od n이다.

선지별 해설

① O — 소수 p보다 작은 양의 정수 1부터 $p - 1$까지는 모두 p와 서로소이므로 $\varphi(p) = p - 1$이다.
② O — 서로 다른 소수 p, q는 서로소이므로 피 함수의 곱셈적 성질에 따라 $\varphi(pq) = \varphi(p)\varphi(q)$이다.
③ X — 틀린 표현은 a^(2p)≡ a^(p)±od p이다. $p > 2$인 소수이면 2와 p가 서로소이므로
$\varphi(2p) = \varphi(2)\varphi(p) = 1 \cdot (p - 1) = p - 1 = \varphi(p)$이다. 따라서 올바르게는 a^(2p)≡ a^(p)±od p이다.
④ O — a와 n이 서로소이면 오일러 정리에 의해 a^(n)≡ 1±od n이다.
⑤ O — $35 = 5 \cdot 7$이고 5와 7은 서로 다른 소수이므로 $\varphi(35) = (5 - 1)(7 - 1) = 4 \cdot 6 = 24$이다.

오답 포인트

③의 함정은 지수 $\varphi(2p)$와 $\varphi(p)$가 달라 보이게 만든 데 있다. $p > 2$이면 2와 p가 서로소이고 $\varphi(2) = 1$이므로 두 지수는 모두 $p - 1$이다. 따라서 이 선지에서는 a에 오일러 정리를 적용하기 전에도 두 식의 지수가 같다는 사실만으로 합동임을 판단할 수 있다.

NoteBase

다시 나오면 이렇게 판단

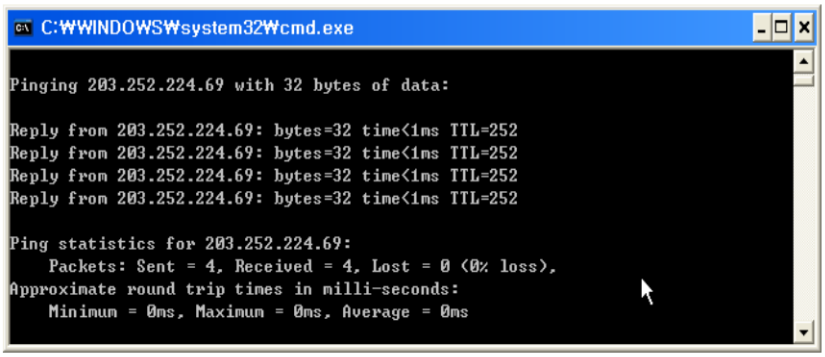
곱의 피 함수가 나오면 먼저 두 인수가 서로소인지 확인한다. 서로소이면 피 함수의 곱셈적 성질을 적용하고, 거듭제곱 합동식에서는 지수 자체가 같은지 먼저 비교한 뒤 오일러 정리의 서로소 조건을 확인한다.

암기 포인트

소수 p는 $\varphi(p) = p - 1, p > 2$이면 $\varphi(2p) = \varphi(p) = p - 1$이다.

NoteBase

10. 다음은 ping 명령을 실행한 것이다. TTL이 의미하는 것은?



① 해당 IP주소 서브넷의 대표 주소이다.
② 전송 속도를 보여주며, 단위는 ms이다.
③ 전송된 패킷의 바이트 크기이다.
④ 해당 패킷의 생명주기이다.
⑤ 발신 패킷과 수신 패킷 간의 손실률을 보여준다.

정답 4번

출제 포인트

ping 실행 결과에 표시되는 TTL, bytes, time, 패킷 손실률의 의미를 구분하는 문제이다.

핵심 개념

TTL(Time To Live)은 IP 패킷이 네트워크에서 무한히 순환하지 않도록 수명을 제한하는 값이다. 라우터를 한 번 거칠 때마다 일반적으로 1씩 감소하며, 0이 되면 패킷이 폐기된다. ping 응답의 TTL 값은 수신한 응답 패킷에 남아 있는 TTL을 나타낸다.
bytes는 응답한 ICMP 데이터의 크기이고, time은 왕복 응답 시간이며, 패킷 손실률은 Ping statistics의 Lost 항목에서 확인한다.

NoteBase

선지별 해설

① X
틀린 표현은 '해당 IP주소 서브넷의 대표 주소'이다. 화면의 203.252.224.69는 ping 대상이자 응답을 보낸 호스트의 IP 주소이며, 서브넷을 나타내는 네트워크 주소라는 뜻이 아니다.

② X
틀린 표현은 '전송 속도'이다. time<1ms는 패킷을 보내고 응답을 받기까지의 왕복 응답 시간이 1ms 미만이라는 뜻이며, 전송 속도를 뜻하지 않는다.

③ X
틀린 표현은 TTL이 '전송된 패킷의 바이트 크기'라는 설명이다. 바이트 크기는 bytes=32가 나타내는 ICMP 데이터 크기이고, TTL은 패킷의 남은 수명을 제한하는 값이다.

④ O
TTL은 패킷이 네트워크에서 계속 순환하는 것을 막기 위한 생명주기, 즉 홉 수 기반의 수명 제한 값이다. 라우터를 거칠 때마다 감소하고 0이 되면 패킷이 폐기된다.

⑤ X
틀린 표현은 TTL이 '발신 패킷과 수신 패킷 간의 손실률'을 보여 준다는 설명이다. 손실률은 Ping statistics의 Sent, Received, Lost 값으로 계산하며, 화면에서는 Lost=0 (0% loss)로 표시된다.

오답 포인트

TTL=252 옆에 bytes=32와 time<1ms가 함께 표시되어 각 항목의 의미를 혼동하기 쉽다. TTL은 수명 제한, bytes는 데이터 크기, time은 왕복 응답 시간, Lost는 손실률을 나타낸다.

다시 나오면 이렇게 판단

ping 결과에서는 항목명을 먼저 대응한다. TTL은 라우터를 지날 때 감소하는 패킷 수명 제한값, bytes는 데이터 크기, time은 왕복 응답 시간, Lost는 손실 패킷 수이다.

암기 포인트

TTL은 홉마다 감소하고 0이면 폐기된다.

NoteBase

11. 「개인정보보호법」상 민감정보에 해당하지 않는 것은?

① 건강 및 성생활에 관한 정보
② 사상, 신념 및 정치적 견해
③ 유전정보
④ 인종, 민족에 관한 정보
⑤ 사번, 학번, 법인등록번호, 사업자등록번호에 관한 정보

정답 5번

쟁점

이 문제는 개인정보 보호법상 민감정보의 범위에 관한 문제이다. 핵심은 사생활 침해 위험이 커 법령에서 민감정보로 정한 정보와 단순 식별·관리번호를 구별하는 것이다.

용어 풀이

민감정보는 사상·신념, 정치적 견해, 건강, 성생활 등 공개되거나 오용될 경우 정보주체의 사생활을 현저히 침해할 우려가 큰 개인정보이다.

핵심 구분

개인정보 보호법 제23조는 사상·신념, 정치적 견해, 건강, 성생활 등에 관한 정보를 민감정보로 규정한다. 같은 법 시행령 제18조는 유전자검사 등의 결과로 얻어진 유전정보와 인종·민족에 관한 정보 등을 민감정보에 포함한다. 반면 사번·학번·법인등록번호·사업자등록번호는 그 번호라는 이유만으로 민감정보가 되는 항목이 아니다. 개인을 알아볼 수 있게 하는 사번이나 학번은 개인정보가 될 수 있지만, 개인정보와 민감정보는 같은 개념이 아니다.

선지별 해설

① O — 건강 및 성생활에 관한 정보는 개인정보 보호법 제23조가 규정한 민감정보이다.
② O — 사상·신념 및 정치적 견해에 관한 정보는 개인의 내면적·정치적 성향을 드러내는 민감정보이다.
③ O — 유전자검사 등의 결과로 얻어진 유전정보는 개인정보 보호법 시행령 제18조가 규정한 민감정보이다.
④ O — 인종이나 민족에 관한 정보는 개인정보 보호법 시행령 제18조가 규정한 민감정보이다.
⑤ X — 사번·학번·법인등록번호·사업자등록번호에 관한 정보는 법령이 열거한 민감정보에 해당하지 않는다. 틀린 표현: 이러한 번호 정보가 민감정보라는 취지의 표현이다. 올바른 표현: 사번이나 학번은 개인 식별 가능성에 따라 개인정보가 될 수 있으나, 제시된 번호들은 그 자체로 민감정보에 해당하지 않는다.

NoteBase

오답 포인트

정보를 식별하는 번호는 모두 보호 수준이 높은 민감정보라고 생각하기 쉽다. 그러나 민감정보 여부는 단순히 개인을 식별할 수 있는지가 아니라 법령이 정한 정보 유형에 해당하는지를 기준으로 판단한다. ⑤의 번호 정보와 건강·사상·유전·인종 정보를 구별해야 한다.

다시 나오면 이렇게 판단

먼저 건강·성생활, 사상·신념·정치적 견해처럼 법률에 직접 규정된 항목인지 확인한다. 다음으로 유전정보, 범죄경력자료, 특정 개인 식별 목적의 생체인식정보, 인종·민족 정보처럼 시행령에 추가된 항목인지 확인한다. 여기에 해당하지 않는 단순 관리번호는 개인정보일 수 있어도 곧바로 민감정보로 판단하지 않는다.

암기 포인트

건강·사상·정치·유전·인종은 민감정보, 사번·학번 같은 관리번호는 민감정보가 아니다.

NoteBase

12. 다음과 관련된 디지털 포렌식의 기본 원칙은?

> ○ 적법한 절차를 따르지 않고 수집한 증거는 위법수집 증거에 해당되기 때문에 이를 사용할 수 없다.
> ○ 독수독과이론(Fruit of the Poisonous Tree) 또는 독과수이론

① 기밀성의 원칙
② 무결성의 원칙
③ 정당성의 원칙
④ 가용성의 원칙
⑤ 연계보관성의 원칙

정답 3번

출제 포인트

이 문제는 디지털 증거를 적법한 절차에 따라 수집해야 한다는 정당성의 원칙을 다른 포렌식 원칙과 구별하는 문제이다.

핵심 개념

정당성의 원칙은 디지털 증거의 수집·분석 과정이 법률과 적법한 절차에 따라 이루어져 증거능력을 갖추어야 한다는 원칙이다. 위법하게 수집한 증거와 그 증거에서 파생된 증거의 사용을 배제하는 독수독과이론은 이 원칙과 연결된다.
기밀성은 허가받지 않은 사람에게 정보가 공개되지 않도록 하는 성질이고, 무결성은 증거가 수집 이후 변경·훼손되지 않았음을 보장하는 성질이다. 가용성은 필요한 때 증거에 접근하여 사용할 수 있는 성질이며, 연계보관성은 증거의 수집·이송·보관·분석 전 과정과 취급자를 끊김 없이 기록하여 동일성과 관리 연속성을 입증하는 원칙이다.

NoteBase

선지별 해설

① X
틀린 표현은 '기밀성의 원칙'이다. 기밀성은 디지털 증거와 관련 정보가 권한 없는 사람에게 노출되지 않도록 보호하는 원칙이다. 제시문의 내용은 기밀성이 아니라 적법한 절차와 증거능력을 요구하는 정당성의 원칙이다.

② X
틀린 표현은 '무결성의 원칙'이다. 무결성은 해시값 확인 등으로 디지털 증거가 수집 당시부터 분석 시점까지 변경되거나 훼손되지 않았음을 보장하는 원칙이다. 제시문의 내용은 무결성이 아니라 정당성의 원칙이다.

③ O
정당성의 원칙은 디지털 증거를 적법한 절차에 따라 수집해야 하며, 위법하게 수집한 증거는 증거로 사용할 수 없다는 원칙이다. 위법수집증거와 그로부터 얻은 파생증거의 사용을 제한하는 독수독과이론도 정당성과 관련되므로 제시문에 부합한다.

④ X
틀린 표현은 '가용성의 원칙'이다. 가용성은 권한 있는 사용자가 필요한 때 디지털 증거나 정보에 접근하여 이용할 수 있도록 하는 성질이다. 제시문의 내용은 가용성이 아니라 정당성의 원칙이다.

⑤ X
틀린 표현은 '연계보관성의 원칙'이다. 연계보관성은 디지털 증거를 누가, 언제, 어디서, 어떤 방식으로 수집·이송·보관·분석했는지를 연속적으로 기록하여 증거의 동일성과 관리 이력을 입증하는 원칙이다. 제시문의 내용은 보관 이력의 연속성이 아니라 적법한 수집 절차를 강조하는 정당성의 원칙이다.

오답 포인트

'절차'라는 말만 보고 증거 취급 절차를 기록하는 연계보관성과 혼동하기 쉽다. 그러나 위법수집증거와 독수독과이론이 제시되면 판단 기준은 보관 이력이 아니라 수집의 적법성과 증거능력이므로 정당성이다.

다시 나오면 이렇게 판단

적법한 수집·영장·위법수집증거·증거능력은 정당성, 변경 방지·해시값은 무결성, 취급자와 이동 경로의 연속 기록은 연계보관성으로 구별한다.

암기 포인트

위법수집과 독수독과는 정당성, 변조 방지는 무결성, 취급 이력은 연계보관성이다.

NoteBase

13. SSL Record 프로토콜의 처리 순서가 올바른 것은?

① 압축 → 단편화 → 암호화 → MAC → 전송
② 압축 → 단편화 → MAC → 암호화 → 전송
③ MAC → 암호화 → 압축 → 단편화 → 전송
④ 암호화 → MAC → 단편화 → 압축 → 전송
⑤ 단편화 → 압축 → MAC → 암호화 → 전송

정답 5번

출제 포인트

이 문제는 SSL Record 프로토콜이 상위 계층의 데이터를 전송 가능한 레코드로 만드는 처리 순서를 묻는다.
핵심은 데이터를 먼저 단편화하고 압축한 뒤 MAC을 붙이며, 그 결과를 암호화하여 전송한다는 점이다.

올바른 순서

1. 단편화 — 상위 계층의 데이터를 처리 가능한 크기의 블록으로 나눈다.
2. 압축 — 단편화된 데이터를 필요에 따라 압축한다.
3. MAC — 압축된 데이터에 대한 메시지 인증 코드를 생성하여 붙인다.
4. 암호화 — 압축 데이터와 MAC을 함께 암호화한다.
5. 전송 — 처리된 SSL Record를 전송한다.

올바른 흐름: 단편화 → 압축 → MAC → 암호화 → 전송

왜 이 순서인가: MAC은 압축된 데이터를 대상으로 계산되어야 하고, 암호화는 그 데이터와 MAC을 함께 보호해야 하므로 MAC이 암호화보다 먼저 수행된다.

NoteBase

선지별 해설

① X — '압축 → 단편화'와 '암호화 → MAC'의 선후관계가 모두 바뀌었다. 올바르게는 단편화 → 압축 → MAC → 암호화 → 전송이다.

② X — '압축 → 단편화'가 잘못되었다. 데이터를 먼저 단편화한 뒤 각 단편을 압축하므로 올바르게는 단편화 → 압축 → MAC → 암호화 → 전송이다.

③ X — MAC과 암호화를 단편화·압축보다 먼저 수행한 부분이 잘못되었다. MAC은 단편화와 압축을 마친 데이터에 붙이고 그 후 암호화하므로 올바르게는 단편화 → 압축 → MAC → 암호화 → 전송이다.

④ X — 암호화와 MAC을 단편화·압축보다 먼저 수행한 부분이 잘못되었고, '암호화 → MAC'의 순서도 바뀌었다. 올바르게는 단편화 → 압축 → MAC → 암호화 → 전송이다.

⑤ O — 단편화 → 압축 → MAC → 암호화 → 전송의 표준 처리 흐름과 일치한다.

오답 포인트

압축과 단편화의 순서를 뒤집거나, MAC을 암호화 뒤에 붙인다고 생각하기 쉽다. 이 문항에서는 '먼저 나누고, 압축한 데이터에 MAC을 붙인 다음, 데이터와 MAC을 함께 암호화한다'는 선후관계가 정답을 가른다.

다시 나오면 이렇게 판단

SSL Record의 송신 처리는 데이터 가공 단계인 단편화·압축, 무결성 단계인 MAC, 기밀성 단계인 암호화, 전송의 순서로 판단한다. 특히 MAC이 암호화보다 먼저인지 확인하면 선지를 빠르게 구별할 수 있다.

암기 포인트

단-압-맥-암-전: 단편화 → 압축 → MAC → 암호화 → 전송이다.

NoteBase

14. 인터넷 환경에서 많이 사용 중인 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① ISAKMP 프로토콜은 IPsec에서 보안 연관을 생성하기 위해 사용된다.

② IPsec은 IPv4와 IPv6에서 사용할 수 있는 보안 프로토콜이므로 상위계층 보안이 필요한 VPN을 제공하지 못한다.

③ IPsec에서 제공하는 Transport 모드는 두 엔드포인트 장치 간에 Point-to-point 연결을 제공한다.

④ IPsec은 데이터 보호를 위해 AH와 ESP 보안 프로토콜을 제공한다.

⑤ IPsec는 상호간 안전한 키 분배를 위해 Diffie-Hellman 키 분배 프로토콜을 사용할 수 있다.

정답 2번

출제 포인트

이 문제는 IPsec의 동작 계층, 보안 연관 설정, 운용 모드, 보안 프로토콜, 키 합의 방식을 구별하는 문제이다.

핵심 개념

IPsec은 IP 계층에서 패킷의 인증·무결성·기밀성 등을 제공하는 보안 체계이므로 IPv4와 IPv6에서 VPN을 구성할 수 있다.
ISAKMP는 보안 연관(SA)의 협상·설정·관리 절차를 위한 프레임워크이며, AH는 인증과 무결성을, ESP는 주로 기밀성과 함께 인증·무결성을 제공한다.
Transport 모드는 원래 IP 헤더를 유지한 채 주로 종단 호스트 사이의 상위 계층 데이터 부분을 보호하고, Tunnel 모드는 원래 IP 패킷 전체를 새 IP 패킷 안에 캡슐화하여 주로 보안 게이트웨이를 포함한 VPN에 사용한다.

NoteBase

선지별 해설

① O — ISAKMP는 IPsec에서 통신 당사자가 사용할 보안 연관(SA)을 협상하고 생성·관리하기 위한 절차와 메시지 형식을 제공한다.
② X — 틀린 표현은 '상위계층 보안이 필요한 VPN을 제공하지 못한다'이다. IPsec은 네트워크 계층에서 동작하므로 상위 계층 응용과 독립적으로 IP 패킷을 보호하며, Tunnel 모드 등을 이용해 VPN을 제공할 수 있다.
③ O — Transport 모드는 두 종단 호스트 사이에서 원래 IP 헤더를 유지하고 페이로드를 보호하므로 종단 간 point-to-point 보호에 적합하다.
④ O — IPsec은 AH와 ESP를 보안 프로토콜로 제공한다. AH는 데이터 출처 인증과 무결성을 제공하고, ESP는 암호화를 통한 기밀성을 중심으로 인증과 무결성도 제공할 수 있다.
⑤ O — IPsec의 키 관리 과정에서는 Diffie-Hellman 방식으로 통신 당사자가 안전하지 않은 네트워크에서도 공유 비밀을 합의할 수 있으며, 이를 세션 키 생성에 활용할 수 있다.

오답 포인트

②는 IPsec이 IP 계층에서 동작한다는 사실을 VPN 제공의 한계처럼 뒤집었다. 실제로는 특정 상위 계층 프로토콜에 의존하지 않고 IP 패킷을 보호할 수 있다는 점이 IPsec VPN의 핵심이다.

다시 나오면 이렇게 판단

IPsec 선지는 'IP 계층 보안과 VPN 가능', 'ISAKMP·IKE는 SA와 키 협상', 'Transport는 종단 간 페이로드 보호', 'Tunnel은 패킷 전체 캡슐화', 'AH는 인증·무결성, ESP는 기밀성 중심'의 기준으로 판단한다.

암기 포인트

IPsec은 IP 계층 VPN, AH는 인증, ESP는 암호화, ISAKMP·IKE는 협상이다.

NoteBase

15. Kerberos 보안 프로토콜에 대한 설명으로 옳지 않은 것은?

① 발급 받은 TGT(Ticket Granting Ticket)는 일회성으로 재사용이 불가능하다.

② Kerberos의 정상적인 동작을 위해서는 관련된 호스트의 시간 동기화가 필요하다.

③ Kerberos는 SSO(Single Sign On)와 상호 인증 기능을 제공한다.

④ Kerberos에 참여하는 인증서버는 클라이언트에 TGT(Ticket Granting Ticket)를 발급한다.

⑤ Kerberos는 대칭키 암호 기반의 인증 프로토콜로 신뢰할 수 있는 제3자를 필요로 한다.

정답 1번

출제 포인트

Kerberos의 티켓 재사용, 시간 동기화, SSO·상호 인증, 인증서버의 역할, 신뢰할 수 있는 제3자의 필요성을 구분하는 문제이다.

핵심 개념

Kerberos는 비밀키 암호와 신뢰할 수 있는 제3자인 KDC를 이용하여 네트워크상에서 사용자의 신원을 인증하는 프로토콜이다. 클라이언트는 인증서버로부터 TGT를 발급받아 유효기간 동안 보관하고, 이를 이용해 티켓 발급 서버에 여러 서비스 티켓을 요청할 수 있다. 티켓에는 유효시간이 포함되므로 참여 호스트 사이의 시간 동기화가 필요하다.

선지별 해설

① X — 틀린 표현은 'TGT는 일회성으로 재사용이 불가능하다'이다. TGT는 유효기간 동안 캐시에 보관하여 여러 서비스 티켓을 발급받는 데 재사용할 수 있다.

② O — Kerberos는 티켓과 인증자의 시간 정보를 검사하여 재전송 공격을 방지하므로 관련 호스트의 시간이 허용 범위 안에서 동기화되어야 한다.

③ O — 한 번 인증받은 뒤 TGT로 여러 서비스에 접근할 수 있어 SSO를 제공하며, 클라이언트와 서버가 서로의 정당성을 확인하는 상호 인증도 지원한다.

④ O — Kerberos의 인증서버는 사용자의 최초 인증을 수행하고 클라이언트에 TGT를 발급한다. 이후 클라이언트는 TGT를 제시하여 서비스 티켓을 요청한다.

⑤ O — Kerberos는 대칭키 암호를 사용하며, 각 주체와 비밀키를 공유하고 티켓을 발급하는 신뢰할 수 있는 제3자인 KDC가 필요하다.

NoteBase

오답 포인트

‘티켓은 재사용하면 안 된다’는 일반적인 보안 직관을 TGT에 그대로 적용하기 쉽다. Kerberos에서 재사용을 막는 대상은 탈취된 인증자의 재전송이며, 정상적인 TGT 자체는 유효기간 동안 반복하여 서비스 티켓을 요청하는 데 사용된다.

다시 나오면 이렇게 판단

TGT는 최초 인증의 결과로 받아 유효기간 동안 서비스 티켓 요청에 사용하고, 서비스 티켓은 특정 서비스 접근에 사용한다고 구분한다. 또한 시간 동기화, SSO·상호 인증, 인증서버의 TGT 발급, KDC에 대한 신뢰는 Kerberos의 정상적인 특징으로 판단한다.

암기 포인트

Kerberos는 ‘KDC를 신뢰하고, 시간을 맞추며, TGT를 유효기간 동안 재사용한다’로 정리된다.

NoteBase

16. <보기>에 해당하는 계층별 보안 프로토콜과 세부 프로토콜은?

<보 기>

이 프로토콜의 각 메시지는 2바이트로 되어 있으며, 첫 바이트는 발생한 메시지 오류의 심각성을 알려주기 위해 경고(warning) 또는 치명적(fatal) 값을 가진다. 만약 레벨이 치명적이라면, 계층 보안 프로토콜은 즉시 연결을 종결시킨다. 동일 세션상의 다른 연결들은 지속될 수 있지만, 이 세션에서 새로운 연결이 만들어질 수는 없다. 두 번째 바이트에는 구체적인 경보를 나타내는 코드가 들어있다.

① IPsec에서의 경보 프로토콜(Alert Protocol)
② SSL에서의 경보 프로토콜(Alert Protocol)
③ SSH에서의 경보 프로토콜(Alert Protocol)
④ S/MIME에서의 경보 프로토콜(Alert Protocol)
⑤ SSH에서의 연결 프로토콜(Connection Protocol)

정답 2번

출제 포인트

2바이트 메시지 중 첫 바이트에 경고 또는 치명적 수준을, 둘째 바이트에 구체적인 경보 코드를 담는 계층별 보안 프로토콜을 식별하는 문제이다.

핵심 개념

SSL 경보 프로토콜은 SSL 통신 중 발생한 오류나 상태를 상대에게 알리는 프로토콜이다. 경보 메시지는 2바이트로 구성되며, 첫 바이트는 경보 수준인 warning 또는 fatal을, 둘째 바이트는 구체적인 경보 설명 코드를 나타낸다. fatal 경보가 발생하면 해당 연결은 즉시 종료되고 그 세션에서는 새로운 연결을 만들 수 없다.
IPsec은 AH·ESP 등의 프로토콜로 IP 계층을 보호하고, SSH 연결 프로토콜은 SSH 위에서 여러 논리 채널을 관리한다. S/MIME은 전자우편 메시지의 보안을 제공한다. 따라서 제시문의 결정적 키워드는 '2바이트 경보 메시지', 'warning/fatal', 'fatal이면 연결 종료'이다.

NoteBase

선지별 해설

① X
'IPsec에서의 경보 프로토콜'이 틀린 표현이다. IPsec의 핵심 보안 프로토콜은 AH와 ESP이며, 제시문처럼 warning/fatal 수준을 전달하는 경보 프로토콜을 두지 않는다. 올바르게는 'SSL에서의 경보 프로토콜'이다.

② O
SSL의 경보 프로토콜은 2바이트 메시지로 경보 수준과 경보 설명을 전달한다. 첫 바이트의 fatal 수준에서 연결을 즉시 종료한다는 설명까지 제시문과 일치한다.

③ X
'SSH에서의 경보 프로토콜'이 틀린 표현이다. SSH는 전송 계층 프로토콜, 사용자 인증 프로토콜, 연결 프로토콜 등으로 구성되며, 제시된 2바이트 SSL 경보 메시지를 의미하지 않는다. 올바르게는 'SSL에서의 경보 프로토콜'이다.

④ X
'S/MIME에서의 경보 프로토콜'이 틀린 표현이다. S/MIME은 전자우편의 암호화와 전자서명을 제공하는 메시지 보안 방식이며, 제시된 warning/fatal 경보 메시지 구조에 해당하지 않는다. 올바르게는 'SSL에서의 경보 프로토콜'이다.

⑤ X
SSH에 연결 프로토콜이 존재하기는 하지만, 이는 SSH 전송 계층 위에서 여러 논리 채널을 설정하고 관리하는 프로토콜이다. 제시문의 warning/fatal 경보 처리와는 기능이 다르므로 'SSH에서의 연결 프로토콜'이 아니라 'SSL에서의 경보 프로토콜'로 고쳐야 한다.

오답 포인트

⑤의 'SSH 연결 프로토콜'은 실제로 존재하는 명칭이어서 혼동하기 쉽다. 그러나 프로토콜의 존재 여부가 아니라 제시된 메시지 형식과 동작을 기준으로 판단해야 한다. '수준 1바이트 + 설명 1바이트'와 fatal 시 연결 종료는 SSL 경보 프로토콜의 특징이다.

다시 나오면 이렇게 판단

경보 메시지에 warning과 fatal이 나오고 fatal에서 연결을 즉시 종료한다면 SSL 경보 프로토콜로 판단한다. SSH 연결 프로토콜은 경보 전달이 아니라 논리 채널 관리라는 기능 차이로 구별한다.

암기 포인트

SSL Alert는 2바이트이다. 첫째는 수준(warning/fatal), 둘째는 구체적 경보 코드이다.

NoteBase

17. 다음 네트워크 기반과 호스트 기반 IDS(침입탐지시스템)의 특징 중 옳지 않은 것만을 모두 고르면?

<네트워크 기반(Network-based)>

ㄱ. 전체 네트워크에 대한 침입탐지가 가능하다.
ㄴ. 탐지된 침입의 실제 공격 성공 여부를 네트워크단에서는 알지 못한다.
ㄷ. 기존 네트워크 환경을 크게 변경하여야만 설치가 가능하다.

<호스트 기반(Host-based)>

ㄹ. 네트워크 기반 IDS가 탐지 불가능한 로컬 시스템에 대한 공격을 탐지할 수 있다.
ㅁ. 모든 개별 호스트에 대한 설치 및 관리를 하기 때문에 네트워크 기반 IDS 보다 설치 및 관리가 쉽다.
ㅂ. 고부하·스위치 네트워크에서도 적용이 가능하며, 우회 가능성이 거의 없다.

① ㄱ, ㄹ
② ㄴ, ㅁ
③ ㄴ, ㅂ
④ ㄷ, ㅁ
⑤ ㄷ, ㅂ

정답 4번

출제 포인트

네트워크 기반 IDS와 호스트 기반 IDS의 탐지 범위, 설치·관리 방식, 운용 환경의 차이를 구별하는 문제이다.

핵심 개념

네트워크 기반 IDS(NIDS): 네트워크 구간의 패킷과 트래픽을 감시하여 여러 시스템에 대한 침입을 탐지한다. 넓은 범위를 한 번에 감시하지만, 공격이 개별 호스트에서 실제로 성공했는지까지는 판단하기 어렵다.
호스트 기반 IDS(HIDS): 개별 호스트에 설치되어 시스템 로그, 파일, 프로세스 등 호스트 내부의 활동을 감시한다. 로컬 공격을 탐지하고 스위치 네트워크나 네트워크 고부하의 영향을 비교적 덜 받지만, 호스트마다 설치하고 관리해야 한다.
따라서 ㄱ·ㄴ·ㄹ·ㅂ은 옳고, ㄷ·ㅁ은 옳지 않다.

NoteBase

선지별 해설

① X — ㄱ과 ㄹ은 모두 옳은 진술이므로 '옳지 않은 것'의 조합이 아니다. 올바른 조합은 ㄷ과 ㅁ이다.
② X — ㄴ은 옳고 ㅁ만 옳지 않으므로 틀린 진술만을 묶은 조합이 아니다. 올바른 조합은 ㄷ과 ㅁ이다.
③ X — ㄴ과 ㅂ은 모두 옳은 진술이므로 '옳지 않은 것'의 조합이 아니다. 올바른 조합은 ㄷ과 ㅁ이다.
④ O — ㄷ의 '기존 네트워크 환경을 크게 변경하여야만'은 틀리다. NIDS는 일반적으로 기존 네트워크 구조를 크게 바꾸지 않고 감시 지점에 설치할 수 있다. ㅁ의 '설치 및 관리가 쉽다'도 틀리다. HIDS는 모든 개별 호스트에 설치·관리해야 하므로 NIDS보다 관리 부담이 크다. 따라서 옳지 않은 진술은 ㄷ과 ㅁ이다.
⑤ X — ㄷ은 옳지 않지만 ㅂ은 옳으므로 틀린 진술만을 묶은 조합이 아니다. HIDS는 호스트 내부에서 감시하므로 고부하·스위치 네트워크에서도 적용할 수 있고, 이 문항의 비교 기준에서는 단순한 네트워크 수준의 우회 가능성이 낮다. 올바른 조합은 ㄷ과 ㅁ이다.

오답 포인트

'전체 네트워크를 감시하는 NIDS가 설치도 더 복잡할 것'이라고 생각하면 ㄷ을 놓치기 쉽다. 반대로 HIDS는 한 호스트를 자세히 감시하지만 모든 호스트에 에이전트를 설치하고 관리해야 하므로 관리가 더 쉽다는 ㅁ은 틀리다. 또한 문제의 부정형 문두에 따라 옳은 진술이 아니라 옳지 않은 진술 ㄷ · ㅁ의 조합을 골라야 한다.

다시 나오면 이렇게 판단

감시 범위를 먼저 구분한다. NIDS는 네트워크 구간을 넓게 감시하고 설치 대상이 적지만 호스트 내부의 공격 성공 여부를 알기 어렵다. HIDS는 개별 호스트 내부를 자세히 감시하지만 호스트별 설치·관리 부담이 크다. 그다음 문제의 문두가 '옳은 것'인지 '옳지 않은 것'인지 확인하여 조합한다.

암기 포인트

NIDS는 넓게·간편하게 설치, HIDS는 깊게·호스트마다 관리한다.

NoteBase

18. 재해복구시스템의 복구 수준별 유형을 비교한 설명으로 옳지 않은 것은?

① Mirror Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하고 Active-Active 상태로 운영한다.

② Hot Site는 주센터와 동일한 수준의 정보 기술 자원을 원격지에 구축하여 대기(Standby) 상태로 유지한다.

③ Warm Site는 중요성이 높은 정보기술 자원만 부분적으로 재해복구 센터에 보유한다.

④ Cold Site는 데이터만 원격지에 보관하고 이의 서비스를 위한 정보자원을 확보하지 않거나 장소 등 최소한으로만 확보한다.

⑤ 재해발생시 RTO(Recovery Time Objective)가 빠른 것은 Hot Site → Mirror Site → Warm Site → Cold Site 순서이다.

정답 5번

출제 포인트

재해복구 사이트를 정보기술 자원의 준비 수준과 운영 방식에 따라 구분하고, 그에 따른 복구목표시간(RTO)의 빠르기를 판단하는 문제이다.

핵심 개념

Mirror Site: 주센터와 같은 수준의 정보기술 자원을 갖추고 양쪽을 Active-Active로 운영하는 사이트이다. 즉시 업무를 이어 갈 수 있어 RTO가 가장 짧다.
Hot Site: 주센터와 같은 수준의 자원을 갖추되 원격지는 대기(Standby) 상태로 유지하는 사이트이다.
Warm Site: 중요 자원만 일부 갖추어 재해 후 추가 준비와 복구가 필요한 사이트이다.
Cold Site: 데이터와 장소 등 최소 기반만 확보하고 서버 등 정보기술 자원은 거의 또는 전혀 준비하지 않는 사이트이다.
복구 속도는 일반적으로 Mirror Site가 가장 빠르고, Hot Site, Warm Site, Cold Site 순으로 느려진다.

NoteBase

선지별 해설

① O — Mirror Site는 주센터와 동등한 수준의 정보기술 자원을 원격지에 구축하고 Active-Active로 운영하므로 옳다.
② O — Hot Site는 주센터와 같은 수준의 정보기술 자원을 갖추고 원격지를 Standby 상태로 유지하므로 옳다.
③ O — Warm Site는 핵심 업무에 필요한 중요 자원을 부분적으로 보유하고, 재해 발생 후 나머지 환경을 준비하는 방식이므로 옳다.
④ O — Cold Site는 원격지에 데이터와 장소 등 최소한의 기반만 확보하고 서비스용 정보기술 자원은 미리 갖추지 않거나 최소한으로만 갖추므로 옳다.
⑤ X — 틀린 부분은 RTO가 빠른 순서에서 Hot Site를 Mirror Site보다 앞에 둔 것이다. Mirror Site는 이미 Active-Active로 운영되므로 Hot Site보다 더 빠르게 복구할 수 있다. 올바른 순서는 Mirror Site → Hot Site → Warm Site → Cold Site이다.

오답 포인트

⑤는 Hot Site도 주센터와 같은 수준의 자원을 갖춘다는 점을 이용한 함정이다. 자원 수준이 같더라도 Hot Site는 Standby이고 Mirror Site는 Active-Active이므로, 즉시 전환 가능한 Mirror Site의 RTO가 더 짧다.

다시 나오면 이렇게 판단

먼저 운영 상태를 확인한다. Active-Active이면 Mirror Site, 동일 자원의 Standby이면 Hot Site, 중요 자원만 일부 준비하면 Warm Site, 장소·데이터 등 최소 기반만 있으면 Cold Site로 판단한다. 준비 수준이 높고 추가 복구 작업이 적을수록 RTO가 짧다.

암기 포인트

복구 속도는 Mirror → Hot → Warm → Cold, 운영 상태는 Active-Active → Standby → 부분 준비 → 최소 준비이다.

NoteBase

19. 악성코드에 대한 설명으로 옳지 않은 것은?

① Backdoor는 비인가된 접근을 허용하는 것으로 공격자가 사용자 인증 과정 등의 정상 절차를 거치지 않고 프로그램이나 시스템에 접근하도록 지원한다.

② Rootkit은 보안 관리자나 보안 시스템의 탐지를 피하면서 시스템을 제어하기 위해 공격자가 설치하는 악성파일이다.

③ Ransomware는 사용자의 파일을 암호화하여 사용자가 실행하거나 읽을 수 없도록 한 뒤 자료복구 대가로 돈을 요구한다.

④ Launcher는 Downloader나 Dropper 등으로 생성된 파일을 실행하는 기능을 가지고 있다.

⑤ Exploit은 악성코드에 감염되지 않았는데도 악성코드를 탐지했다고 겁을 주어 자사의 안티바이러스 제품으로 제거해야 한다는 식으로 구매를 유도한다.

정답 5번

출제 포인트

Backdoor, Rootkit, Ransomware, Launcher, Exploit의 기능과 공격 목적을 구별하는 문제이다.

핵심 개념

Backdoor는 정상 인증 절차를 우회하여 시스템에 접근하게 하는 통로이다. Rootkit은 공격자의 존재나 악성 행위를 숨기면서 시스템을 제어하게 하는 악성 도구의 집합이다. Ransomware는 파일이나 시스템의 이용을 막고 복구 대가를 요구하는 악성코드이다. Launcher는 다른 악성 파일을 실행하는 역할을 한다. Exploit은 소프트웨어나 시스템의 취약점을 이용하여 비정상 동작이나 코드 실행을 일으키는 공격 코드 또는 기법이다.

선지별 해설

① O — Backdoor는 정상적인 인증·접근 통제 절차를 거치지 않고 프로그램이나 시스템에 접근할 수 있게 하는 비인가 통로이므로 옳다.

② O — Rootkit은 보안 관리자나 보안 도구의 탐지를 피하도록 자신의 존재와 활동을 숨기면서 공격자가 시스템을 제어하게 하므로 옳다.

③ O — Ransomware는 파일을 암호화하거나 시스템 접근을 막은 뒤 복구를 조건으로 금전을 요구하므로 옳다.

④ O — Launcher는 Downloader가 내려받거나 Dropper가 시스템에 생성한 악성 파일 등을 실행하는 기능을 하므로 옳다.

⑤ X — 틀린 표현은 '악성코드에 감염되지 않았는데도 감염 경고를 띄워 자사 안티바이러스 제품 구매를 유도한다'는 부분이다. 이는 허위 백신 또는 스케어웨어의 수법이다. Exploit은 올바르게는 소프트웨어나 시스템의 취약점을 이용하여 공격자가 의도한 비정상 동작이나 악성 코드 실행을 유발하는 코드 또는 기법이다.

NoteBase

오답 포인트

⑤는 보안 위협과 관련된 행위라는 점 때문에 Exploit처럼 보이게 만든 선지이다. 그러나 '취약점 이용'이 없고 '거짓 감염 경고와 제품 구매 유도'가 핵심이므로 허위 백신·스케어웨어에 해당한다.

다시 나오면 이렇게 판단

용어를 공격의 핵심 동작과 연결한다. 인증 우회는 Backdoor, 은폐와 제어는 Rootkit, 암호화·사용 제한과 금전 요구는 Ransomware, 다른 파일 실행은 Launcher, 취약점 이용은 Exploit으로 판단한다.

암기 포인트

Exploit은 취약점 이용, 스케어웨어는 거짓 경고와 구매 유도이다.

NoteBase

20. NAT(Network Address Translation)에 대한 설명으로 옳지 않은 것은?

① 사용자에게 투명성을 제공함으로써 처리 속도가 빠르다.
② 한정된 공인 IP주소 부족 문제의 해결이 가능하다.
③ 주소 변환 기능을 제공한다.
④ 외부 컴퓨터에서 사설 IP를 사용하는 호스트에 대한 접근이 어려워 보안 측면에서 장점을 제공한다.
⑤ 외부 컴퓨터에 네트워크 구조를 노출하지 않는 보안상의 이점을 제공한다.

정답 1번

출제 포인트

NAT의 주소 변환 기능과 공인 IP 주소 절약·내부망 은닉 효과를 알고, 이를 처리 속도 향상과 혼동하지 않는지를 묻는 문제이다.

핵심 개념

NAT(Network Address Translation)는 사설 네트워크의 내부 IP 주소와 외부에서 사용하는 공인 IP 주소를 변환하는 기술이다. 여러 내부 호스트가 제한된 공인 IP 주소를 공유하게 할 수 있고, 외부에 내부 주소와 네트워크 구조가 직접 드러나는 것을 줄인다. 다만 주소와 포트 정보를 변환하는 처리가 추가되므로 NAT 자체가 처리 속도를 빠르게 하는 기술은 아니다.

선지별 해설

① X - '투명성을 제공함으로써 처리 속도가 빠르다'는 부분이 틀리다. NAT는 주소 변환 처리를 추가하므로 그 자체가 처리 속도를 향상시키지 않으며, 종단 간 직접 연결의 투명성을 제한할 수도 있다. 올바르게는 'NAT는 주소 변환 기능을 제공하지만 처리 속도를 빠르게 하는 기능은 아니다'이다.
② O - 여러 사설 IP 호스트가 소수의 공인 IP 주소를 공유할 수 있으므로 한정된 공인 IP 주소의 부족 문제를 완화할 수 있다.
③ O - NAT의 핵심 기능은 패킷의 출발지 또는 목적지 IP 주소와 필요시 포트 정보를 변환하는 것이다.
④ O - 사설 IP 주소는 외부에서 직접 라우팅되지 않고 외부에서 내부 호스트로 임의의 연결을 시작하기도 어려우므로 보안 측면의 부수적 이점이 있다. 다만 NAT가 방화벽을 완전히 대신하는 것은 아니다.
⑤ O - 외부에는 변환된 공인 주소가 보이므로 내부 IP 주소 체계와 네트워크 구조가 직접 노출되는 것을 줄이는 보안상 이점이 있다.

NoteBase

오답 포인트

①의 '투명성'과 '처리 속도가 빠르다'를 자연스럽게 이어 붙인 표현이 함정이다. NAT의 대표 효과는 주소 변환, 공인 IP 주소 절약, 내부망 은닉이며 처리 속도 향상은 아니다.

다시 나오면 이렇게 판단

NAT 선지는 먼저 주소 변환·공인 IP 주소 절약·내부 주소 은닉에 해당하는지 확인한다. 처리 속도 향상이나 완전한 보안 제공처럼 NAT의 기본 목적을 넘어선 표현은 틀린 선지로 판단한다.

암기 포인트

NAT는 주소를 바꾸고 공인 IP를 아끼며 내부망을 숨기지만, 속도를 높이는 기술은 아니다.

NoteBase