

글은 읽고 이해하는 것 이것이 국어의 핵심이다

제대로 이해하고 거짓 정보와 알 수 없는 정보를 소거하면 된다

핵심은 올바른 독해! 평가원의 논리에 자연스럽게 반응하는 독해를 훈련하자

Step1: 개념/ 맥락/ 관점에 집중한 첫 문단 독해- 기본

개념	집중할 대상	
맥락	개념을 설명& 한정하는 앞 뒤 내용	
관점	복수의 개념이 등장할 때 견주어 구분하는 것 → A B 표시가 핵심 → 결국 공통점과 차이점 구분	'비해 반면 달리 지만 보다' '같은 테이블에 있는 두 개념'
구조	문단과 글 전체의 구조, 글의 전개 방식 떠올리기 →(6+2) 패턴+ 1	기존의 일반적 추상적 내용- 예시 배경지식- 화제 일반적 생각- 주장 등을 (6+2)패턴으로 재정립
주제	구조를 통해 드러나는 글의 핵심	

Step2: 사전 정보의 틀을 짜기(패턴 독해)

왜? 많은 정보 속에서도 집중할 부분을 확실하게 기억하기 위해

어떻게? 수능 국어의 6+2패턴을 사용

A-A'(개념어 형용사 구체화)	개념어	개념어란?
	형용사	얼마나 어떻게 형용사한가? 왜 형용사 한가?
P-S(문제- 해결)	문제	(기본 개념) 문제의 내용 해결책
Q-A(통념- 반박)	질문	(기본 개념) 답 근거
통념-반박	통념 (일반적/ 과거)	(기본 개념) 통념의 잘못된 부분 어떻게 반박
시간의 흐름	X시대	(기본 개념) Y시대 Z시대
대칭성	앞선 설명 구조	같은 설명 구조& 내용이 다름

과학 기술- 과정 원리	과학 기술 경제에서 현상.대상	(기본 개념) 대상의 구성요소
		대상이 만드는/ 작동하는 과정과 원리 활용하는 과정과 원리 측정하는 과정과 원리

특히 마지막 2가지는 정보량이 많고 어려운 요즘 국어의 핵심이다

과학 기술 경제 지문에서 쏟아지는 정보에 맞춰

많은 정보를 적고

이를 그림으로 표현하고 이해할 수 있어야 한다

Step3: 예측 참고 '개념 맥락 관점 중심으로 독해'.

예측을 참고해 개념 맥락 관점을 제대로 파악할 수 있어야 한다

이때 앞서 배운 6+2 패턴은 글 전체에서 등장하기에 반응할수록 좋다

점차 볼 수 있는 부분을 키워가자

Cf) 더 기초적인 독해력 키우기 방법

-어휘력을 키우자

환원: 복잡한 대상을 단일 레벨의 '기본요소로부터' 설명하는 것

-문장 간의 연결관계를 기억하자

수직적 관계	전제- 결론의 관계	A (따라서/ 결과적으로/ 이처럼/ 이런 점에서) B
		B (왜냐하면) A이기 때문
		B (예컨대/ 예를 들어) A
수평적 관계	전제- 전제/ 결론- 결론 관계	X(그리고/ 또한/ 게다가/ 더구나/ 그런데) Y
		동등한 사실들의 연결 (귀납 추리)
		결합 관계 (전제의 결합)
		동치 관계(즉, 다시 말하면)

이를 통해서 문단의 핵심을 파악하기

연결사를 조금 더 구체적으로 정리하자면

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

순접	앞 문장 이어서 서술	그리고 그리하여
대등	앞 문장과 동등 연결	또한 혹은 및
첨가	앞 문장에 새로운 설명 추가	더구나 게다가
예시	앞 문장에 구체적 예시	예컨대 예를 들어
인과	앞 뒤 문장 원인과 결과 관계	따라서 그러므로 왜냐하면
요약	앞 문장 내용 요약	결국 요컨대
전환	앞 문장과 새로운 화제	그런데 그렇다면 한편 다음으로
대조	앞 문장과 반대의 내용	하지만 그렇더라도 비해 달리

순접 대등 첨가는 수평적 예시 인과 요약은 수직적으로 기억!

-인식의 팁을 기억하자

글을 잘 읽기 위해서는 패턴을 통해서 글의 전반적인 연결관계를 파악하는 독해법도 중요하지만

실제 독해 과정에서 사용할 수 있는 다양한 인지적 팁을 알아두는 것 역시 필요하다

이러한 인지적 팁을 자주 활용하는 것을 중심으로 3가지만 기억하자

㉠어려운 말은 쉽게 내 말로 바꿔서 읽어보기

㉡예시는 조금만 바꿔 보면서 추상적인 내용을 이해하기

Ex) "다보탑은 경주에 있다." "다보탑은 개성에 있었을 것이다."는 한 세계에서 동시에 참이나 거짓이 될 수는 없지만 각 가능세계에는 참일 수 있다.

성수는 돈이 많다. 성수는 사업이 어려워서 돈을 많지 않다는 한 세계 안에서는 동시에 참일 수 없지만 성수는 돈이 많다가 참인 세계 또 실제와는 다르게 사업이 성공하지 못해 돈이 많지 않은 세계를 각각 설정할 수 있다

㉢어려운 글에서 따로 떨어져 있는 정보를 마구 연결하지 말고 따로따로 이해하기

Ex) 이로부터 콰인의 개별적인 가설뿐만 아니라 기존의 지식들과 여러 조건 등을 모두 포함하는 전체 지식이 경험을 통한 시험의 대상이 된다는 총체주의를 제안한다 (중략)

그런데 주변부 지식이 경험과 충돌하여 거짓으로 밝혀지면 전체 지식의 어느 부분을 수정해야 할지 고민하게 된다.

주변부 지식을 수정하면 전체 지식의 변화가 크지 않지만 중심부 지식을 수정하면 관련된 다른 지식이 많기 때문에 전체 지식도 크게 변화하게 된다. 그래서 대부분의 경우에는 주변부 지식을 수정하는 쪽을 선택하겠지만 실용적 필요 때문에 중심부 지식을 수정하는 경우도 있다.

그리하여 콰인은 중심부 지식과 주변부 지식이 원칙적으로 모두 수정의 대상이 될 수 있고, 지식의 변화도 더 이상 개별적 지식이 단순히 누적되는 과정이 아니라고 주장한다.

여기서는 가설+ 기존 지식+ 조건을 포함한 '전체 지식'이 경험을 통한 검증이라는 총체주의

이 총체주의에서 지식 분류(중심 주변)와 경험을 통한 검증에서 충돌할 때 어디를 어떻게 수정!

굳이 가설+ 기존지식+ 조건을 뒤로 가져와 기존 지식의 수정이 주변부인지 중심부인지 고민X

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

문제 풀이의 모든 것

문제 풀이의 핵심은 글과 연결한 내용 일치

우선 선지와 글을 연결해서 없는 정보 거짓인 정보를 거부하기

오답은 크게 글에 등장하지 않는 정보

글에 등장하는 내용과 정반대의 정보

글에 등장하는 복수의 개념을 마구잡이로 섞은 정보로 등장한다

간단한 문제 풀이라고 해도 유형별 팁을 정리해야 쉽고 빠르게 글을 분석할 수 있다

보기 문제의 경우 글의 핵심 개념과 연결되며

만약 중간에 식이 등장한다면 그 식을 깔끔하게 적어두기

ㄱ 에 대한 이해 문제의 경우에는

판단의 근거나 그 문단 혹은 앞과 뒤에 존재하며

주관식으로 먼저 판단의 근거를 미리 정리하는 것이 좋다

비판 문제는 강화 약화 없는 내용이 핵심으로

주장을 그대로 강화하는 서술

주장과 반대되는 약화 서술- 비판의 근거

마지막으로 선지에 가장 자주 나오는 서술자가 아예 말하지 않는 내용- 비판의 근거가 아님

만약 문제 풀이를 계속해서 틀린다면

주관식으로 문제를 푸는 것 역시 추천되는 방식이다

ㄱ 와 ㄴ 의 공통점과 차이점을 묻는 것이라면 우선 그 내용을 먼저 글에서 찾아

핵심 용어가 등장하는 선지부터 우선적으로 푸는 것이든

선지에서 반복되는 구절을 통해 EX) B가 움직이지 않는다면

이를 활용해서 미리 핵심 단어와 결과를 뽑고

이 선지부터 보는 것 모두 주관식 풀이의 답이 될 수 있다

1문단

DNS(도메인 네임 시스템) 스푸핑은 인터넷 사용자가 어떤 사이트에 접속하려 할 때 사용자를 위조 사이트로 접속시키는 행위를 말한다.

개념제시: DNS 스푸핑

DNS 스푸핑이라는 것은 우선 사용자가 있고 이 사용자가 특정 사이트에 접근하려 할 때 이 사용자를 위조 사이트로 가게 하는 것이군

이는 도메인 네임을 IP 주소로 변환해 주는 과정에서 이루어진다.

이 부분은 꼭 집중해야겠다. 이 글은 딱 봐도 과학 기술 경제 지문이고

따라서 뒤에서는 구성요소/ 작동과 조립의 과정 원리/ 활용의 과정과 원리/ 측정의 과정과 원리가 중요할 것이다

이런 흐름에서 등장한 도메인 네임을 IP 주소로 변환하는 과정이 등장했기에 이것은 DNS 스푸핑의 작동 과정에서 등장할 가능성이 높다

STEP2) 예측 독해

과학 기술 경제의 과정과 원리 지문

0. 도메인?

0. IP?

1. DNS 스푸핑 과정을 위한 구성 요소

2. DNS 스푸핑이 작동하는 과정과 원리

- 도메인→ IP

이제 이를 참고해서 다시 개념 맥락 관점을 중심으로 글을 읽어가야 한다

앞서 정리한 6+2 패턴에 반응하는 것을 점차 늘려가는 것이 좋다

사실 이 글은 그림이 '보기'에 등장한 글이다

따라서 구성 요소와 작동/조립의 과정원리가 등장할 때 이 그림을 반드시 활용해야 한다

인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신하기 위해서 각 컴퓨터들은 IP(인터넷 프로토콜)에 따라 만들어지는 고유 IP 주소를 가져야 한다.

서로를 알아보고 서로 통신하기 위해서는 고유 IP가 필요하구나 알아차리고 통신하기 위해서는 나만의 IP가 필요하구나

개념 제시: 고유 인터넷 프로토콜은 인터넷 프로토콜에 의해서 만들어진 그런데 프로토콜이 무엇인지에 대한 설명이 제대로 이어지고 있지 않음 아마 뒤에서 설명할 것이다

프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

어나 하드웨어로 구현된다.

글 중간에 등장한 A-A'(개념어 형용사에 대한 구체화)

개념 제시: 프로토콜은 서로 데이터를 주고받기 위해서 사용하는 일종의 규칙, 약속, 소프트웨어나 하드웨어를 통해 실현

현재 주로 사용하는 IP 주소는 '***.126.63.1'처럼 점으로 구분된 4개의 필드에 숫자를 사용하여 나타낸다.

현재 IP 주소는 즉 서로 데이터를 주고 받기 위한 규칙과 약속에 의해서 만들어진 IP 주소는 4개의 필드와 숫자로 나타나는구나

이 주소를 중복 지정하거나 임의로 지정해서는 안 되고 공인 IP 주소를 부여받아야 한다.

이 IP 주소는 공인 IP주소를 받아야 하는구나 서로를 알아보고 통신하기 위해서는 고유인 IP 주소가 필요하다고 했는데 이 IP 주소는 내가 임의로 지정하거나 중복해서는 안 되고 공인된 IP주소를 받아야 하는구나. 이렇게 주소를 받아야 이를 바탕으로 일정한 규칙에 따라 소통이 가능하겠구나

인식팁- 비슷한 용어를 구분하기

비슷한 용어가 등장할 때 이를 구분해서 읽어낼 수 있어야 제대로 된 독해가 가능하다

우선 고유 IP IP주소 IP등으로 유사한 개념이 등장하고 있다. 이럴 때 개념을 명확하게 이해하고 넘어가야 전체적인 시간을 줄일 수 있다. 프로토콜을 데이터를 주고 받는데 필요한 규칙과 약속이고 인터넷프로토콜은 인터넷 주소 차원에서 데이터를 주고 받는데 필요한 규칙과 약속 체계 자체를 말한다

IP는 표준 프로토콜로 인터넷에서 통신하고 메시지를 주고 받기 위한 규칙과 약속을 말한다. 개인적으로는 시스템으로 이해

IP 주소는 이 규칙과 약속에 의해 만들어지고 사용하는 '주소'를 말한다. 개인적으로는 시스템의 결과로 이해

공인 IP 주소에는 동일한 번호를 지속적으로 사용하는 고정 IP 주소와 번호가 변경되기도 하는 유동 IP 주소가 있다.

관점제시: 공인 IP 주소에는 고정IP VS 유동 IP .A B 표시- 공통점과 차이점 구분

인터넷에서 통신과 식별을 위해 필요한 공인 IP에는 같은 번호를 계속 쓰는 고정 IP와 주소가 바뀔 수 있는 유동 IP주소가

유동 IP 주소는 DHCP라는 프로토콜에 의해 부여된다.

그 중 유동 IP 주소 즉 변경되는 주소는 DHCP 프로토콜이라는 것에 의해서 부여되는구나. 앞서 본 가장 큰 개념인 포로토콜 즉 통신을 위한 규칙과 약속은 다양하게 나타날 수 있구나.

그리고 DHCP에 대한 구체화가 없기에 뒤에서는 이것에 대한 구체화가 일어나겠구나

DHCP는 IP 주소가 필요한 컴퓨터의 요청을 받아 주소를 할당해 주고, 컴퓨터가 IP 주소를 사용하지 않으면 주소를 반환받아 다른 컴퓨터가 그 주소를 사용할 수 있도록 해 준다.

DHCP 프로토콜 즉 DHCP 통신 규칙과 약속 체계는 식별과 통신을 위해서 IP 주소가 필요한 컴퓨터에서 IP 주소를 할당해주고 사용하지 않으면 이를 다시 가져와 다른 컴퓨터가 이 주소를 사용할 수 있도록 함

한편, 인터넷에 직접 접속은 안 되고 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP 주소도

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

있다.

새로운 내용 제시: 사실 IP는 Y로 앞선 개념과 구분이 필요함 즉 공인과의 관계!

앞선 고정과 유동이 모두 공인 IP 주소로 인터넷에서 서로를 알아보고 통신할 수 있는 규칙과 약속 체계에서

만들어진 주고였다면

사실 IP 주소는 인터넷이 아니라 내부 네트워크에서만 서로를 알아볼 수 있는 주소인 것

(자) 사실 IP주소를 가지고는 인터넷에 직접 접속은 안 되고 인터넷에서 직접 메시지를 주고 받는 것은 어려움

다만 사실 IP 주소의 경우 네트워크 안에서 서로를 식별하기 위한 프로토콜에 의한 주소이기에 네트워크 안에서는 서로식별이 가능하다

CF) 배경지식

현재 우리가 사용하는 것은 공인 IP와 공인 IP 주소

사실 IP와 사실 IP 주소 모두이다

집에서 사용하는 공유기를 생각하면 편하다

집에서 사용하는 컴퓨터 등은 공인 IP 주소가 아니라 사실 IP주소를 사용한다

공유기는 사실 IP주소와 공인 IP주소를 모두 가지고 있으며 우리가 인터넷을 통해 메시지를 전달하고자 하면

우선 사실 IP 주소를 통해 공유기로 또 이 공유기에서 공인 IP주소를 통해 인터넷을 통한 메시지 전달이 가능하다

기본적으로 사실 IP주소는 공인 IP가 사용하지 않는 부분을 사용한다.

서버의 경우에는 공인 IP 주소를 사용한다고 생각하자

인터넷 - (공유기) - 네트워크내 컴퓨터

-서버

인터넷은 공인 IP 주소를 기반으로 동작하지만 우리가 인터넷을 사용할 때는 IP 주소 대신 사용하기 쉽게 'www.***.***' 등과 같이 문자로 이루어진 도메인 네임을 이용한다.

개념제시: 도메인 이것은 공인 IP 주소 대신에 사용하는 것. 인터넷을 사용할 때 이를 사용할

여기서도 인터넷을 통한 사용이기에 기본적으로 공인 IP 주소를 전제한다고 볼 수 있다

계속해서 DNS 스푸핑이 작동되는 과정에서 필요한 기본 개념 구성 요소를 제시하고 있다

쭉쭉 읽으면서 필요한 정의 비교대조 상관관계 정리하기

따라서 도메인 네임을 IP 주소로 변환해 주는 DNS가 필요하며 DNS를 운영하는 장치를 네임서버라고 한다.

개념제시: 도메인 네임 → DNS → IP주소

개념제시: 네임서버- DNS 를 운영하는 장치

도메인 네임을 이용하지만 인터넷에서 실제 서로를 알아보고 통신하기 위해서는 이를 위한 규칙과 약속의 체계에서 만들어진 공인 IP를 사용해야 할 것이다.

이를 위해서 도메인 네임을 IP 주소로 변환하는 것이 필요하며 이것이 DNS 이를 운영하는 장치가 네임서버인 것이다

컴퓨터에는 네임서버의 IP 주소가 기록되어 있어야 하는데, 유동 IP 주소를 할당받는 컴퓨터에는 IP 주소를 받을 때 네임서버의 IP 주소가 자동으로 기록되지만, 고정 IP 주소를 사용하는 컴퓨터에는 사용자가 네임서버의 IP주소를 직접 기록해 놓아야 한다.

내용이 길기에 적당하게 호흡을 끊으면서 글을 읽을 수 있어야 한다

너무 급하게만 읽지 말자

네임서버의 IP 주소가 필요한 네임서버를 말 그대로 '서버' 여기의 IP주소를 알아야 컴퓨터가

인터넷을 통해 서버에 접속이 가능할 것이다

관점 제시: 유동IP 주소를 받은 컴퓨터는 이미 네임서버 IP 주소를 알고

고정일 경우에는 이 서버의 IP를 직접 적어두어야 한다

인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영하고 있다.

통신사들은 이 서버를 공동으로 운영하고 있구나

㉔ 사용자가 어떤 사이트에 정상적으로 접속하는 과정을 살펴보자.

드디어 본격적인 과정과 원리가 등장하고 있다. 앞서 제시한 공인 IP 주소, 도메인, DNS,네임서버라는 구성 요소가 모이면서 DNS 스푸핑이 작동하는 과정과 원리가 등장할 것이다

다만 아직은 DNS 스푸핑이 아니라 어떤 사이트에 정상적으로 접속하는 과정과 원리가 등장하고 있다

웹 사이트에 접속하려고 하는 컴퓨터를 클라이언트라 한다.

개념제시: 클라이언트- 웹사이트에 접속하려는 컴퓨터

클라이언트가 있구나

사용자가 방문하고자 하는 사이트의 도메인 네임을 주소창에 직접 입력하거나 포털 사이트에서 그 사이트를 검색해 클릭하면 클라이언트는 기록되어 있는 네임서버에 도메인 네임에 해당하는 IP 주소를 물어보는 질의 패킷을 보낸다.

작동 원리가 계속되고 있다. 우선 접속하고자 하는 사이트의 도메인을 검색하거나 찾으면 이제 이 도메인에 해당하는 공인 IP 주소를 알아야 그 사이트에 접속하고 메시지를 보낼 수 있다. 이를 위해서 네임서버에 도메인 네임에 해당하는 IP 주소를 물어보는 질의 패킷을 보내는 것이다

이제 이 부분은 바로 이미지화가 필요하다

클라이언트- 도메인- 네임서버에 이 도메인의 IP를 묻는 질의 패킷

네임서버는 해당 IP 주소가 자신의 목록에 있으면 클라이언트에 이 IP 주소를 알려 주는 응답 패킷을 보낸다.

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

네임서버가 도메인에 해당하는 IP주소를(공인 IP주소) 알고 있다면 이 IP주소를 알려주는 응답패킷을 보낸다

응답 패킷에는 어느 질의 패킷에 대한 응답인지가 적혀 있다.

기본적으로 이 응답 패킷은 어떤 도메인 IP에 대한 답변인지가 적혀있다

만일 해당 IP주소가 목록에 없으면 네임서버는 다른 네임서버의 IP 주소를 알려 주는 응답 패킷을 보내고, 클라이언트는 다시 그 네임서버에 질의 패킷을 보내는 단계로 돌아가 같은 과정을 반복한다.

이 과정에서 네임 서버에 찾고자 하는 IP가 없다면 다른 '네임서버'의 IP 주소를 알려주게 되고 클라이언트는 이 네임서버의 IP 주소를 통해서 네임서버와 통신하고 찾고자 하는 도메인에 해당하는 IP를 찾게 된다

네임서버의 IP 주소를 알려준다는 것으로 클라이언트는 네임서버와 통신하는 것이고 통신을 통해서 찾고자 하는 도메인의 IP를 찾고자 하는 것이다

클라이언트는 이렇게 알아낸 IP 주소로 사이트를 찾아간다.

클라이언트는 네임서버를 통해서 알아낸 도메인의 IP주소를(공인 IP) 찾아서 그 사이트로 찾아가는구나

네임서버와 클라이언트는 UDP라는 프로토콜에 맞추어 패킷을 주고받는다.

앞서 정리했듯 클라이언트는 네임서버와 통신을 통해서 도메인의 IP를 찾는 것으로 이들의 통신 과정 역시 프로토콜에 의해서 이루어지고 이때 프로토콜은 UDP라는 프로토콜이다

UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대방에게 패킷을 보내기만 할 뿐 도착 여부는 확인하지 않으며, 특정 질의 패킷에 대해 처음 도착한 응답 패킷을 신뢰하고 다음에 도착한 패킷은 확인하지 않고 버린다. DNS 스푸핑은 UDP의 이런 허점들을 이용한다.

UDP의 특징이 제시되고 있다. UDP의 경우에는 도착여부를 확인하지 않고 처음 도착한 응답패킷 쉽게 처음도착한 IP 주소 정보를 찾고자 하는 도메인의 IP로 생각한다. DNS 스푸핑은 이 부분의 허점을 활용하는구나

바로 이점이 DNS 스푸핑 개념의 핵심적 과정과 원리이구나

위 부분 특히 네임서버의 IP주소를 통해서 네임서버와 통신하는 것. 이를 통해서 도메인의 해당하는 IP 주소를 찾는 것. 다시 도메인에 해당하는 이 IP 주소로 접속하는 것. 이렇게 과정과 원리를 명확하게 정리할 수 있어야 한다

④ DNS 스푸핑이 이루어지는 과정을 알아보자.

드디어 본격적인 DNS 스푸핑이 이루어지는 과정과 원리를 봐야 하구나. 앞에서 제시한 구성요소가 사용될 것이며

정상적 상태의 구조가 그대로 등장할 수 있다.

즉 계속해서 그림을 활용해야 한다!

악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다.

개념: 공격자- 악성코드 감염.DNS 스푸핑을 행하는 컴퓨터

클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트에 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다.

바른 국어 다른 결과 서성수T/ Q&A 카톡: thets

클라이언트는 아까 네임서버의 도메인에 해당하는 IP를 묻는다고 했는데

이 물음은 그대로 공격자에게도 나간다

공격자는 찾고자 하는 도메인과는 다른 도메인의 IP 주소를 보내는 것

실제 설명의 길이가 확 줄어들었다. 이는 앞서 본 정상적인 작동의 설명의 틀을 그대로 활용할라는 것이다

클라이언트- 공격자- 위조 사이트의 IP주소 제공- 접속

-네임서버 -도메인의 IP 주소- 수용되지 않음

공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다

핵심인 먼저 도착했기에 UDP 프로토콜의 특징상 이를 응답 패킷이라고 생각하고 이제 위조 사이트로 연결되는 것이다

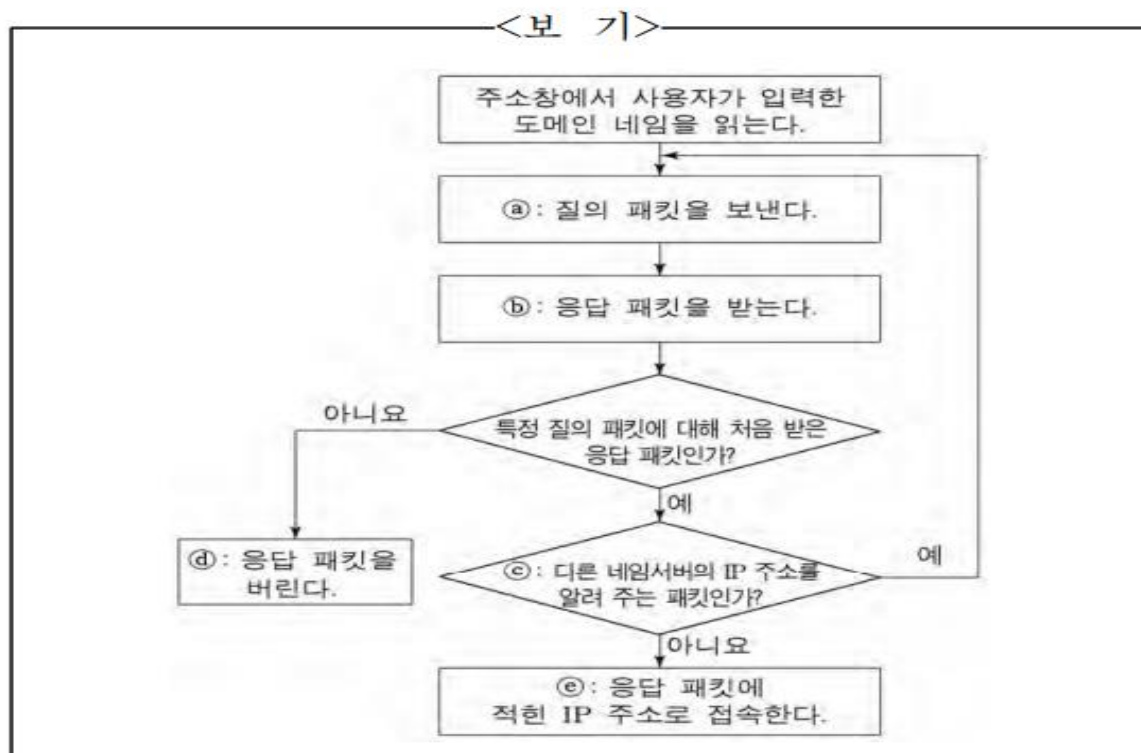
CF) 사실 네임서버의 IP 주소로 소통하는데 어떻게 공격자에게도 이 패킷이 나갔을까?

실제로는 인터넷상에 이 패킷을 뿌리는 형태라고 함

CF) 보기 문제로 등장했던 과정과 원리

파본 검사의 과정에서 이 과정과 원리를 반드시 파악했어야 하며

이 위에 글을 읽을 수 있어야 한다



33. 윗글과 <보기>를 참고할 때, DNS 스푸핑을 피하기 위한 방법으로 적절한 것은?

<보 기>

DNS가 고안되기 전에는 특정 컴퓨터의 사용자가 'hosts'라는 파일에 모든 도메인 네임과 그에 해당하는 IP 주소를 적어 놓았고, 클라이언트들은 이 파일을 복사하여 사용하였다. 네임서버를 사용하는 현재에도 여전히 클라이언트는 질의 패킷을 보내기 전에 hosts 파일의 내용을 확인한다. 클라이언트가 이 파일에서 원하는 도메인 네임의 IP 주소를 찾으면 그 주소로 바로 접속하고, IP 주소를 찾지 못했을 때 클라이언트는 네임서버에 질의 패킷을 보낸다.

- ① 클라이언트에서 사용자가 hosts 파일을 찾아 삭제하면 되겠군.
- ② 클라이언트의 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.
- ③ 클라이언트에 hosts 파일이 없더라도 사용자가 주소창에 도메인네임만 입력하면 되겠군.
- ④ 네임서버의 도메인 네임과 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.
- ⑤ 접속하려는 사이트의 도메인 네임과 IP 주소를 사용자가 클라이언트의 hosts 파일에 적어 놓으면 되겠군.

보기 문제 풀이의 핵심은 글의 개념과 연결하는 것

주관식으로 풀자면 글에서 제시한 개념은 공격자 컴퓨터와 통신하지 않는 것

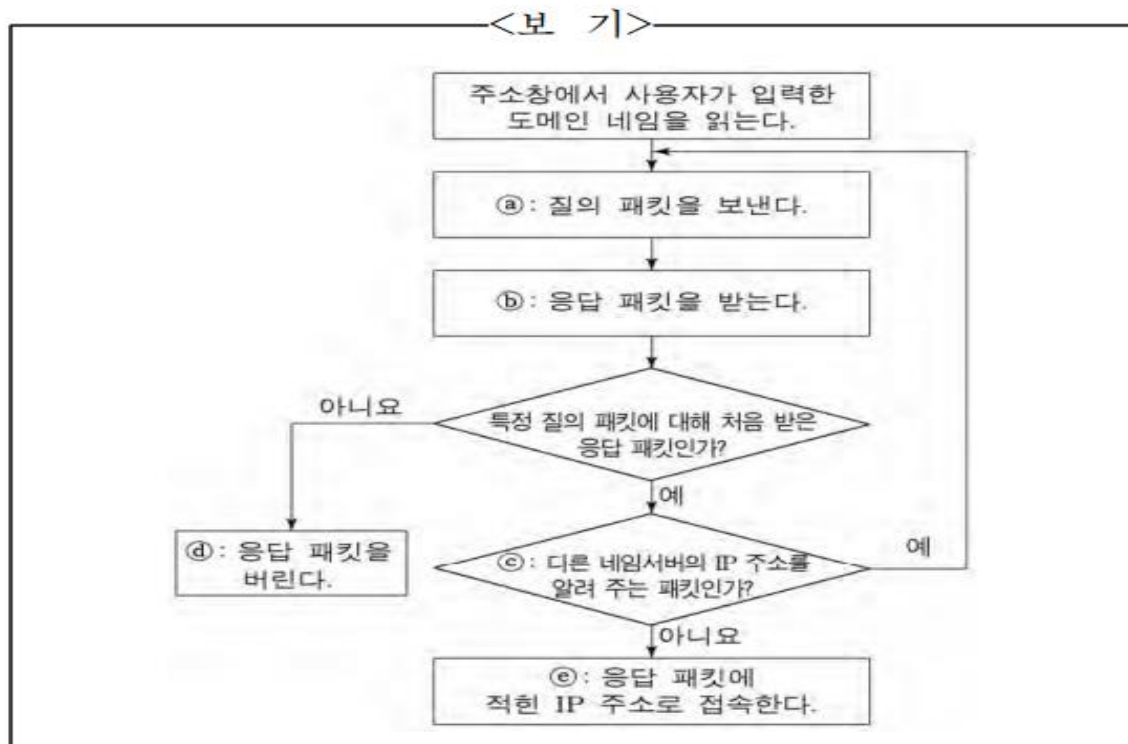
혹은 네임서버의 응답 패킷이 공격자가 알려주는 도메인의 IP 주소 보다 더 빠르면 되는 것

보기에 등장한 내용은 아예 클라이언트가 아예 질의 패킷을 보내기 전에 하는 것으로

여기서 DNS 스푸핑을 피하기 위해서는 아예 공격자와 통신하지 않는 방법

즉 호스트에 사용하는 도메인의 아이피 주소를 미리 적어두는 방법이다

31. <보기>는 ㉠ 또는 ㉡에서 이루어지는 클라이언트의 동작을 나타낸 것이다. 이에 대한 이해로 적절한 것은? [3점]



- ① ㉠ : ㉠이 두 번 동작했다면, 두 질의 내용이 동일하고 패킷을 받는 수신 측도 동일하다.
- ② ㉠ : ㉡가 두 번 동작했다면, 두 응답 내용이 서로 다르고 패킷을 보낸 송신 측도 동일하다.
- ③ ㉠ : ㉢은 ㉠에서 질의한 도메인 네임에 해당하는 IP 주소를 네임서버가 찾았는지 여부를 확인하는 절차이다.
- ④ ㉡ : ㉣의 응답 패킷에는 공격자가 보내 온 IP 주소가 포함되어 있다.
- ⑤ ㉡ : ㉤의 IP 주소는 ㉠에서 질의한 도메인 네임에 해당하는 IP 주소이다

핵심은 글의 개념과 연결하는 것 이미 정리한 도메인의 IP 주소를 찾아서 접속하는 과정과 원리

즉 그림과 이어지는 내용이다

우선 질의가 두 번 이루어진 것은 첫 네임서버에 도메인 네임이 없는 것으로 이때는 다른 네임서버의 IP 주소와 통신한다

응답이 두 번 있던 것도 마찬가지로 첫 네임서버에 도메인 네임이 없는 것으로 이때 보낸 송신 측 네임서버는 다르다

만약 다른 네임서버의 IP 주소가 아닌 도메인의 IP 주소를 알려준다면 이것은 그 값을 찾은 것이다

DNS 스푸핑에서는 응답자도 도메인의 IP 주소에 대한 요청을 받았고 이 값을 먼저 주기에 버려지는 응답패킷은 네임서버의 것

DNS 스푸핑에서 접속하는 IP 주소는 거짓된 정보이다