DNS 스푸핑 [18 6 30~34]

[핵심 흐름]
1문단에서 핵심흐름을 알려줬어. DNS스푸핑을 알기 위해서는 먼저 '도메인 네임'과 'IP주소'를 알아야 한다! 라고 우리한테 얘기해준 거야. 그러면 당연히 '도메인 네임'과 'IP주소'에 대해 궁금하고 찾아봤어야 해.
2~3문단이 IP주소에 대한 내용이고, 4문단이 도메인 네임에 대한 내용이야. 도메인 네임말고 IP주소를 먼저 언급한 이유는 도메인 네임에 대해 알려면 IP주소를 알고 있다는 것을 전제하기 때문이야.
이제 '도메인 네임'과 'IP주소'를 알았으니 본론으로 들어가야겠지. 5문단에서는 '정상적으로 접속하는 과정'을 설명해줘. 6문단에서는 우리가 궁금했던 DNS 스푸핑에 대해 설명하지. DNS스푸핑을 뒤에서 설명한 이유는 '정상'이 뭔지 알아야 '비정상'이 뭔지 알 수 있기 때문이야.

*30번
발문에 단서가 특별히 없어. '프로토콜'은 지문 전반적으로 대응되는 말이니까.
선택지로 가자.
[4%] 1: 프로토콜이 뭔지 묻고 있어. 통신 규약 얘기가 나오는 2문단으로 가면 되겠지?

[3%] 2: IP 주소의 특징을 묻고 있네. 2문단 하단 부분으로 가면 되겠지.

[9%] 3: DHCP를 단서로 잡아서 3문단 중간쯤으로 바로 갈 수 있어!. 3문단 중간쯤을 보면 DHCP는 주소를 할당해 주고, 사용하지 않으면 주소를 반환받는다고 했으니 옳은 선지!

[77%] v4: 1~3번보다 생각을 요하는 선지야! 3문단의 내용을 통해 'DHCP를 이용한다는 것'은 '유동 IP를 사용함'으로 이해할 수 있지. 4문단을 보면 <유동 IP을 사용할 때>는 네임서버에 IP주소를 자동으로 기록한다고 언급하고 있어. 사용자가 직접 기록해야 하는 건 <고정 IP를 사용할 때>지.

[5%] 5: UDP를 단서로 잡아서 5문단의 하단으로 가면 돼. UDP의 특징 중 하나가 '상대에게 패킷을 보내기만 할 뿐 도착 여부는 확인하지 않는다'는 점이지.

*31번
3점짜리라서 처음부터 이 문제에 집착한 학생들이 있었는데, 이런 문제는 처음 만났을 때 바로 풀면 안 되는 문제야. 시간을 잡아먹을 수밖에 없는 문제거든. 문학에서 3점짜리나 이 문제 3점이나 둘 다 어차피 3점이야. 그렇다면 시간을 덜 들일 수 있고 정답을 맞출 가능성이 높은 쪽을 선택하는 게 현명하겠지? 실전이라면 다른 문제들을 다 푼 다음에 시간이 남으면 이 문제를 보도록 하자.

자, 일단 '가'과정을 이해해볼까?
네가 naver에 접속한다고 하자. 그럼 여기서 넌 클라이언트고 네가 네임서버에 naver IP를 물어봤어. 그러면 네임서버의 응답은 두 가지 선택지밖에 없어.
1. naver IP를 알려준다. 2. 모르면 다른 데 가서 물어봐!! 라고 응답한다.(=타 네임서버 IP 응답)
2의 경우라면 넌 다시 다른 네임서버한테 "너 naver IP아니?"라고 물어보고 네임서버한테 둘 중 하나의 응답을 받겠지. 응 알어. 아니 몰라 딴 데 가봐.

이제 '나'의 과정을 보자.
원래 같으면 응답은 2가지 선택지밖에 없다는 것! 이해했지? 근데 여기에 1가지 선택지가 추가가 돼. [공격자]라는 놈이 응답하는 거지. 이놈은 가짜 naver IP를 너(클라이언트)에게 '가장 먼저'알려줘. UDP의 특성 중 하나가 '처음 도착한 응답을 신뢰'하는 건데, [공격자]놈의 응답이 가장 먼저 도착한 거지. 그래서 낚시 당하는 거고, 이게 DNS스푸핑!

선택지 보자!
[8%] 1: a가 두 번 동작했다는 게 무엇을 의미하니? 질의 패킷을 두 번 보냈다는 건 처음 질의 패킷을 보냈을 때는 naver IP를 못받았고, 두 번째에 받았다.를 의미해.
질의 내용은 똑같이 "너 naver 주소 아니?"
수신 측은 달라지겠지. 처음에 물어본 네임서버가

naver 모르니까 딴 데 가서 알아봐! 라고 할 테니.

[15%] 2: b가 두 번 동작했다는 게 뭘 의미하니? 1번과 유사하지? 다만 이번엔 주체가 '네임서버'로 바뀐 거야.
상황극으로 보면,
너(클라이언트) : 님 naver 주소 아심?
네임서버 A : ㄴㄴ 모름. B한테 물어보셈.
너(클라이언트) : A가 알려줘서 왔는데, B님 naver 주소 아심?
네임서버 B : ㅇㅇ 알려줄게.

두 응답 내용은 다른 거 맞아.
but 응답 패킷을 보낸 송신 측은 네임서버A와 B로 다르지.

[49%] v3: 선지는 'naver IP를 네임서버가 찾았는지 여부'를 묻고 있어. 그럼 경우는 두 가지뿐이지. 찾았다. 못 찾았다.
C는 같은 말을 다른 식으로 서술하고 있어.
'다른 네임서버의 IP를 알려주는가? (=naver IP를 네임서버가 못 찾았는지 여부)'
답 나왔네.

[11%] 4: '나'의 경우를 묻고 있어. DNS스푸핑 당하는 과정이지. d에 공격자가 보내 온 IP가 담겨 있다면 DNS스푸핑을 당하지 않는다는 얘기지?

[14%] 5: 마찬가지로 DNS스푸핑 당하는 과정인데, 만약 선지가 언급한 대로 응답패킷에 원하는 IP가 적혀져 있다면 DNS스푸핑을 당하지 않는다는 의미지.

*32번
발문에 단서가 없어. 선택지로 가자.

[9%] 1: 상당히 중요한 선지야. 평가원이 자주 사용하는 논리가 담겨있지.
DNS를 단서로 잡자. 4문단으로 가지지? 일단 도메인 네임을 IP주소로 바꿔주는 건 맞아.
자 그런데 4문단 내용을 잘 보면 '도메인 네임을 사용한다'의 '전제'가 있어. 뭘까?
그치. 바로 인터넷을 사용한다는 거야.
인터넷을 사용한다는 건 '공인 IP'를 사용한다는 것이고, '공인 IP'가 아닌 '사설 IP'는 인터넷에 접속할 수 없어.

[46%] v2: '사설 IP'를 단서로 잡아서 3문단 하단으로 가자. 거기를 보면, '내부 네트워크에서만 서로를 식별할 수 있는'이라는 말이 나오지. 식별이라는 말을 쉬운 말로 바꾸면 '구분할 수 있다'라고 이해할 수 있지? 그래서 사설 IP 주소는 서로 달라야 해.

[15%] 3: 유동 IP주소와 공인 IP 주소를 단서로 잡자. 그러면 2문단 하단으로 가지지. 중복 지정은 안 돼.

[15%] 4: 3번이랑 같은 의도의 선지야. 고정 IP주소는 공인 IP주소의 일종이야. 그러므로 공인 IP주소의 특징을 담고 있지. 중복 지정은 안 돼.

[13%] 5: IP주소가 서로 다르면, 네임서버도 달라야 해?
그런 이야기는 지문에 언급하지 않았지. 더욱이 4문단 마지막에 공동 네임서버 얘기가 나와.

*33번
발문에 단서 있니?
없다고?? ㅠㅠ

'DNS스푸핑을 피하기 위한 방법'을 물어봤잖아~
피할 방법을 알기 위해서는 우선 뭘 알아야 할까?
그렇지. DNS스푸핑이 뭔지 알아야 피할 방법을 생각할 수 있겠지!

자, 지문의 마지막 문단으로 가서 DNS스푸핑이 왜 일어나는지 살펴보자.
정상적인 과정에서는 클라이언트가 질의패킷 보내면 네임서버가 받아서 응답패킷을 보내는데, DNS스푸핑이 일어날 때는 질의패킷이 '공격자'에게도 전달돼. 그리고 공격자가 보낸 응답패킷이 클라이언트에게 가장 먼저 도착해서 문제가 발생하지.
자, 그러면 이 문제에 대한 솔루션은 어떻게 낼 수 있을까? <보기>를 보기 전에 생각해보자.
문제가 발생한 이유로 크게 두 가지를 생각해볼 수 있어. (UDP를 사용한다는 전제)

1. 질의패킷이 공격자에게도 갔다.
2. 공격자의 응답패킷이 가장 먼저 도착했다.

그러면 솔루션은 다음과 같겠지.
1. 질의패킷이 공격자에게 가지 못하게 한다. (근본적 해결책)
2. 공격자의 응답패킷보다 네임서버의 응답패킷이 먼저 도착하게 한다.

이 정도 생각하고 〈보기〉를 보자.
〈보기〉 내용은 'hosts'파일에 IP들을 적어놓는다는 내용이야. 그래서 네임서버에 질의패킷을 보내지 않고도 원하는 IP로 접속할 수 있다는 내용이네,
우리가 〈보기〉를 보기 전에 생각했던 1번 솔루션에 해당되는 내용이지?
자, 그러면 적절한 것을 골라야 하니까 적절한 선지에는 "hosts파일에 접속하고자 하는 IP가 담겨있다" 라는 말이 있어야 하겠네.
답 바로 나오니? **5번 [54%]**

2번과 4번은 함정 의도가 같은 선지야.
'문제가 발생한 이유'를 생각해보지 않은 친구들을 낚기 위한 선지지.