흑 국 일 몽

독해의 기본

오 르 비
후 국 일
김 민 수

[2018학년도 6월 모의평가 30~34번]

DNS(도메인 네임 시스템) 스푸핑은 인터넷 사용자가 어떤 사이트에 접속하려 할 때 사용자를 위조 사이트로 접속시키는 행위를 말한다. 이는 도메인 네임을 IP 주소로 변환해 주는 과정에서 이루어진다.

인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신하기 위해서 각 컴퓨터들은 IP(인터넷 프로토콜)에 따라 ㉠ 만들어지는 고유 IP 주소를 가져야 한다. 프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어나 하드웨어로 구현된다. 현재 주로 사용하는 IP 주소는 '***.126.63.1'처럼 점으로 구분된 4개의 필드에 숫자를 사용하여 ㉡ 나타낸다. 이 주소를 중복 지정하거나 임의로 지정해서는 안 되고 공인 IP 주소를 부여받아야 한다.

공인 IP 주소에는 동일한 번호를 지속적으로 사용하는 고정 IP 주소와 번호가 변경되기도 하는 유동 IP 주소가 있다. 유동 IP 주소는 DHCP라는 프로토콜에 의해 부여된다. 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. 한편, 인터넷에 직접 접속은 안 되고 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP 주소도 있다.

인터넷은 공인 IP 주소를 기반으로 동작하지만 우리가 인터넷을 사용할 때는 IP 주소 대신 사용하기 쉽게 'www.***.***' 등과 같이 문자로 ㉢ 이루어진 도메인 네임을 이용한다. 따라서 도메인 네임을 IP 주소로 변환해 주는 DNS가 필요하며 DNS를 운영하는 장치를 네임서버라고 한다. 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 IP 주소를 직접 기록해 놓아야 한다. 인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영하고 있다.

㉮ 사용자가 어떤 사이트에 정상적으로 접속하는 과정을 살펴보자. 웹 사이트에 접속하려고 하는 컴퓨터를 클라이언트라 한다. 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. 네임서버는 해당 IP 주소가 자신의 목록에 있으면 클라이언트에 이 IP 주소를 알려 주는 응답 패킷을 보낸다. 응답 패킷에는 어느 질의 패킷에 대한 응답인지가 적혀 있다. 만일 해당 IP 주소가 목록에 없으면 네임서버는 다른 네임서버의 IP 주소를 알려 주는 응답 패킷을 보내고, 클라이언트는 다시 그 네임서버에 질의 패킷을 보내는 단계로 돌아가 같은 과정을 반복한다. 클라이언트는 이렇게 ㉣ 알아낸 IP 주소로 사이트를 찾아간다. 네임서버와 클라이언트는 UDP라는 프로토콜에 ㉤ 맞추어 패킷을 주고받는다. UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 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.

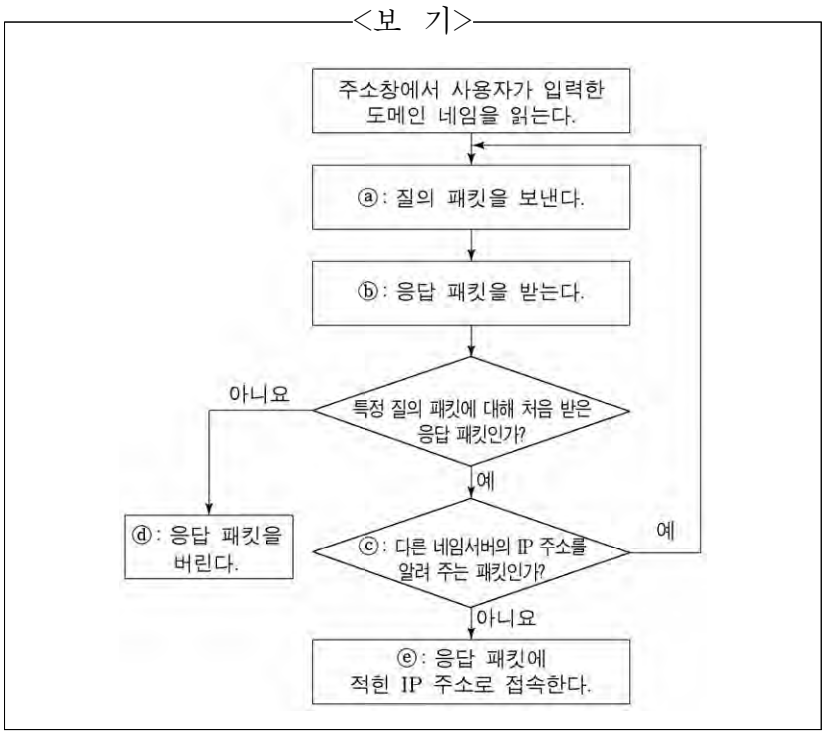
㉯ DNS 스푸핑이 이루어지는 과정을 알아보자. 악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다. 클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트의 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다. 공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다.

30. 윗글의 '프로토콜'에 대한 설명으로 적절하지 않은 것은?

① 컴퓨터 사이의 통신을 위한 규약으로서 저마다 정해진 기능이 있다.
② IP에 따르면 현재 주로 사용하는 IP 주소는 4개의 필드에 적힌 숫자로 구성된다.
③ DHCP를 이용하는 컴퓨터는 IP 주소를 요청해야 IP 주소를 부여받을 수 있다.
④ DHCP를 이용하는 컴퓨터에는 네임서버의 IP 주소를 사용자가 기록해야 한다.
⑤ UDP는 패킷 전송 속도를 높이기 위해 패킷이 목적지에 제대로 도착했는지 확인하지 않는다.

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

<보 기>



① ㉮: ⓐ가 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 측은 동일하다.
③ ㉮: ⓒ는 ⓐ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.

32. 윗글을 바탕으로 알 수 있는 것은?

① DNS는 도메인 네임을 사설 IP 주소로 변환한다.
② 동일한 내부 네트워크에 연결된 컴퓨터들의 사설 IP 주소는 서로 달라야 한다.
③ 유동 IP 주소 방식의 컴퓨터들에는 동시에 동일한 공인 IP 주소를 할당할 수 있다.
④ 고정 IP 주소 방식의 컴퓨터들에는 동시에 동일한 공인 IP 주소를 부여할 수 있다.
⑤ IP 주소가 서로 다른 컴퓨터들은 각각에 기록되어 있는 네임서버의 IP 주소도 서로 달라야 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 도메인 네임만 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.

34. 문맥상 ㉠~㉤과 바꿔 쓰기에 가장 적절한 것은?

① ㉠: 제조(製造)되는
② ㉡: 표시(標示)한다
③ ㉢: 발생(發生)된
④ ㉣: 인정(認定)한
⑤ ㉤: 비교(比較)해

DNS(도메인 네임 시스템) 스푸핑은 인터넷 사용자가 어떤 사이트에 접속하려 할 때 사용자를 위조 사이트로 접속시키는 행위를 말한다. 이는 도메인 네임을 IP 주소로 변환해 주는 과정에서 이루어진다.

인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신하기 위해서 각 컴퓨터들은 IP(인터넷 프로토콜)에 따라 ㉠ 만들어지는 고유 IP 주소를 가져야 한다. 프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어나 하드웨어로 구현된다. 현재 주로 사용하는 IP 주소는 '***.126.63.1'처럼 점으로 구분된 4개의 필드에 숫자를 사용하여 ㉡ 나타낸다. 이 주소를 중복 지정하거나 임의로 지정해서는 안 되고 공인 IP 주소를 부여받아야 한다.

공인 IP 주소에는 동일한 번호를 지속적으로 사용하는 고정 IP 주소와 번호가 변경되기도 하는 유동 IP 주소가 있다. 유동 IP 주소는 DHCP라는 프로토콜에 의해 부여된다. 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. 한편, 인터넷에 직접 접속은 안 되고 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP 주소도 있다.

인터넷은 공인 IP 주소를 기반으로 동작하지만 우리가 인터넷을 사용할 때는 IP 주소 대신 사용하기 쉽게 'www.***.***' 등과 같이 문자로 ㉢ 이루어진 도메인 네임을 이용한다. 따라서 도메인 네임을 IP 주소로 변환해 주는 DNS가 필요하며 DNS를 운영하는 장치를 네임서버라고 한다. 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 IP 주소를 직접 기록해 놓아야 한다. 인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영하고 있다.

㉮ 사용자가 어떤 사이트에 정상적으로 접속하는 과정을 살펴보자. 웹 사이트에 접속하려고 하는 컴퓨터를 클라이언트라 한다. 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. 네임서버는 해당 IP 주소가 자신의 목록에 있으면 클라이언트에 이 IP 주소를 알려 주는 응답 패킷을 보낸다. 응답 패킷에는 어느 질의 패킷에 대한 응답인지가 적혀 있다. 만일 해당 IP 주소가 목록에 없으면 네임서버는 다른 네임서버의 IP 주소를 알려 주는 응답 패킷을 보내고, 클라이언트는 다시 그 네임서버에 질의 패킷을 보내는 단계로 돌아가 같은 과정을 반복한다. 클라이언트는 이렇게 ㉣ 알아낸 IP 주소로 사이트를 찾아간다. 네임서버와 클라이언트는 UDP라는 프로토콜에 ㉤ 맞추어 패킷을 주고받는다. UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 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.

㉯ DNS 스푸핑이 이루어지는 과정을 알아보자. 악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다. 클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트의 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다. 공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다.

-전체 구조 잡기

1문단 - 도메인 네임을 IP주소로 변환해주는 과정에서 발생하는 DNS스푸핑

2문단 - 컴퓨터가 인터넷에서 서로를 식별, 통신하기 위해 [고유 IP 주소]가 필요함

3문단 - 고유 IP주소의 종류와 각각의 특징

4문단 - [도메인 네임 -> IP주소]로 변환해주는 DNS와 네임서버

5문단 - 정상적인 사이트 접속 과정 -> 그 과정에서 UDP의 역할과 허점 -> 그러한 허점을 이용한 DNS스푸핑

6문단 - UDP의 허점을 이용한 DNS스푸핑이 발생하는 과정

<1문단>

① 첫 문장에서 DNS 스푸핑에 대해서 정의하고, 그러한 DNS 스푸핑이 [도메인 네임 -> IP주소]와 같은 변환 과정에서 이루어진 다고 제시하고 있죠. 2문장 밖에 안 되지만, 모두 중요한 정보였고, 이 글의 큰 방향을 모두 제시해주었어요. 이 글의 소재는 [DNS 스푸핑]이 될 것이고, 조금 더 구체적으로는 [도메인 네임 -> IP 주소로의 변환]과정에서 그러한 DNS 스푸핑이 발생하는 과정에 대해서 설명할 가능성이 매우 높은 글이 되겠죠. 그리고 그에 앞서 우리가 모르는 개념인 [IP주소, 도메인 네임]등에 대해서 먼저 설명해줄 가능성이 높구요. 이렇게 [과정&원리]와 관련된 글들은 1문단에서 전반적이고, 대략적인 과정을 제시한 후 그러한 과정에 대해서 구체화하는 경우가 많아요. 그러한 과정에서 필요한 선행 개념들에 대해서 먼저 설명을 해주구요. 글을 못 읽는 친구들은 그러한 정보가 왜 나오는지를 모르면서 그냥 읽죠. 그리고 어렵다고 말을 해요. 여러분은 이런 글을 읽을 때 명확하게 방향을 잡고, 그러한 개념이 결국에는 핵심 과정을 설명하기 위해 온다는 것을 잊으면 안돼요

②즉 다시한 번 정리하면 이 글은 앞으로 [도메인 네임, IP주소]등과 같은 개념을 우리가 모르기 때문에 우선 다음 문단에서는 그러한 개념들에 대해서 차근 차근 깔아주고, 그를 바탕으로 [도메인 네임 -> IP주소로 변환해주는 과정]을 알려주고, [그 과정에서 DNS스푸핑이 어떻게 일어나는지]에 대해서 설명해주는 구조로 이루어졌을 가능성이 큰 글이네요. 이렇게 방향성을 안 잡고 읽으면 2문단부터 도대체 왜 공인 IP, 프로토콜, 등등이 나오는 지 모르면서 "그냥" 읽게 되겠죠.

1문단 정리
->도메인 네임을 IP주소로 변환해주는 과정에서 발생하는 DNS스푸핑

<2문단>

① 2문단의 첫 문장이 가장 핵심이었어요. 정리하면 인터넷에 연결된 컴퓨터들이 서로를 식별하고 통신을 하기 위해서는 컴퓨터들 이 각각 [IP가 만든 -> 고유 IP주소]를 가져야 한다는 거죠. 갑자기 IP주소 이야기를 왜 하는 건지를 파악했어야죠. 그렇죠. 이 글에서 중요한 건 [DNS스푸핑]이고 그러한 스푸핑은 [도메인 네임 -> IP주소로 변환]하는 과정에서 발생한다는 건데, 그걸 설명하기 위해 먼저 [IP주소]에 대해서 설명하고 있는 거죠. 두 번째 문장에서 [프로토콜]을 정의해주는데 이는 첫 문장에서 말한 프로토콜에 대해서 개념을 설명해주는 거죠. 그리고 나서 IP주소의 특징들을 설명한 뒤, [공인 IP주소]를 가져야 함을 언급하고 있어요.

② 복잡하지만 결국 큰 흐름을 파악하면 [컴퓨터 식별 통신을 위해 -> 고유 IP 주소 -> 공인 IP주소]를 가져야함을 언급하고 있는 거고 이 자체가 중요하다기 보단 이를 바탕으로 설명할 DNS스푸핑의 과정이 중요하겠죠.

2문단 정리
->컴퓨터가 인터넷에서 서로를 식별하기 위해서는 [고유한 IP 주소 -> 공인 IP주소]를 가져야 함.

<3문단>

① 3문단은 2문단과 같은 흐름이었어요. IP주소와 관련한 구체적인 설명이 이어지는 문단이었어요. [고정IP / 유동IP /사설 IP/ DHCP 프로토콜]등 많은 개념이 나오면서 여러분들은 당황해요. 당황하지 말고, 그러한 개념간의 관계를 묶어주고, 왜 그러한 개념이 제시가 되고 있는지를 의식적으로 파악해주세요.

② 결국 그러한 개념들은 분류하고 정리해주면 아래와 같죠.

[고유 IP주소] -> [사설 IP 주소 : 인터넷X]
-> [공인 IP 주소 : 인터넷O] -> [고정 IP 주소 : 동일한 번호 지속 사용]
-> [유동 IP 주소 : 번호가 변경되기도 함] -> [DHCP프로토콜에 의해 부여됨]

->결국 2~3문단에서 [프로토콜 -> 고유 IP]주소에 대해서 설명하고, 그것들의 종류와 특성에 대해 설명하고 있었고, 그 이유는 그러한 IP주소에 대한 개념이 1문단에서 제시한 체재인 [도메인 네임 -> IP주소의 변환 과정에서 -> DNS스푸핑이 발생]을 이해하는 필요한 선행개념이기 때문이겠죠. 세부정보에 매몰돼서 정작 중요한 큰 흐름을 놓치면 안 돼요. 3문단까지 해서 IP주소에 대한 설명이 끝났기 때문에 아마도 다음 문단에서는 [도메인 네임]과 관련한 설명이 등장할 가능성이 크겠죠.

3문단 정리
->고유 IP의 종류와 각각의 특징

<4문단>

① 인터넷은 -> 공인 IP주소를 기반으로 동작 -> 우리가 인터넷을 사용할 때는 [IP주소 대신 -> 사용하기 쉬운 도메인 네임 사용]한다고 하네요. 드디어 도메인 네임이 나왔어요. 그리고 왜 [스푸핑]이 [도메인 네임 -> IP주소]으로 변환하는 과정에서 일어난다고 했는지도 슬슬 드러나네요. 즉 우리가 인터넷이 공인 IP주소로 동작하는 것은 맞지만, 사용자가 사용할 때는 도메인 네임으로 사용하는데, 이걸 IP주소로 다시 바꾸는 과정에서 발생하는 게 1문단에서 말한 DNS스푸핑이 되겠네요. 그럼 다음 내용은 아마 조금 더 구체적으로 도메인 네임이 무엇인지, 어떻게 변환이 일어나는지 등에 대해서 설명해주겠죠. 그리고 그걸 바탕으로 [DNS 스푸핑]이 일어나는 과정을 설명하는 게 큰 흐름이구요.

② 사용의 편의때문에 인터넷을 사용할 때는 도메인 네임을 사용하는데, 그러한 [도메인 네임]을 다시 [IP주소]로 바꿔주기 위해서 [DNS]가 필요하고, 그러한 DNS를 운영하는 장치가 [네임서버]가 되고, 컴퓨터에는 네임서버의 주소가 기록되어 있어야 함.
->여기서부터 머리가 아파요. 다 새로운 정보같으니까요. 관계를 맺어주세요. 즉 [컴퓨터에는 네임서버의 IP주소가 기록 되어있어야 함 -> 그 네임서버가 DNS운영 -> 네임서버의 주소가 기록되어 있어야 그러한 네임서버를 통해 도메인 네임을 다시 IP주소로 바꿀 수 있나보다] 와 같이요:)

1) 유동 IP를 할당 받는 컴퓨터 -> 자동으로 네임서버의 해당 주소가 기록됨.
2) 고정 IP를 할당 받는 컴퓨터 -> 사용자가 직접 네임서버의 해당 주소를 기록해야 함.
->그런데 인터넷 통신사는 가입자들이 공동으로 사용할 수 있는 네임서버를 운영한다네요. ㅇㅇ.

->그냥 컴퓨터에는 네임서버의 주소가 기록되어있어야 하는구나가 아니라, 왜 그런지를 자꾸 생각해야 돼요. 왜 그럴까요? 그렇죠. 인터넷은 IP주소를 기반으로 동작해요. 그런데 우리가 인터넷을 사용할 때는 편의를 위해서 도메인 네임을 사용하죠. 따라서 실제 인터넷 동작을 위해서는 이러한 도메인 네임을 다시 IP주소로 바꿔줘야 하고, 그러한 변환을 해주는 게 DNS, 그 운영자가 네임서버인 거잖아요. 따라서 그러한 네임서버의 주소가 컴퓨터에 있어야 그 네임서버를 통해, [도메인 네임 -> IP주소]의 변환이 일어날 수 있고, 그러한 IP주소를 바탕으로 인터넷이 동작되겠죠.

③ 4문단까지해서 1문단에서 말한 제재를 살펴보기 위한 선행 개념들은 다 설명해주었어요. 즉 인터넷 사용자가 사이트에 접속할려고 할 때 위조사이트에 접속하게 하는 게 DNS스푸핑이었죠. 그런데 그러한 스푸핑의 과정은 [도메인 네임 -> IP주소]]로의 변환 과정에서 일어난다고 했어요. 그래서 2~3문단에서 먼저 IP주소가 무엇인지, 왜 필요한지에 대해서 설명해주었고, 4문단에서 그러한 IP주소 대신 편의를 위해 도메인 네임이 사용된다고 하죠. 그렇기 때문에 실제 인터넷이 동작하기 위해서는 [도메인 네임 -> IP주소]의 변환이 필요하게 되고, 그러한 과정을 도와주는 친구들이 DNS, 네임서버구요. 그리고 이러한 과정에서 발생하는 게 DNS스푸핑인 거죠.:) 어때요. 이해하니까 정보량이 확 줄지 않나요?

4문단 정리
->[도메인 네임 -> IP주소]로 변환해주는 DNS와 네임서버

<5문단>

① 5문은 2~4문단에서의 설명한 개념을 바탕으로 [사용자가 어떤 사이트에 정상적으로 접속하는 과정]에 대해서 먼저 설명하네요.
->다만 단순히 정상적으로 접속하는 과정 자체를 이해하는 것도 중요하지만, 더욱 중요한 건 그 과정에 대한 이해를 통해 [DNS스푸핑이 발생하는 것]에 대해서 말하려고 한다는 것을 놓치지 않는 거죠.

[정상적 사이트 접속 과정]

1) 클라이언트는 자신의 컴퓨터에 기록된 네임서버로 -> 접속할 사이트의 도메인 네임에 해당하는 IP주소를 묻는 질의 패킷을 보냄
2) 네임서버는 해당 IP주소가 목록에 있으면 해당 IP주소를 응답 패킷으로 알려주고 클라이언트는 그 주소로 접속
네임서버는 해당 IP주소가 목록에 없으면 다른 네임서버의 주소를 응답 패킷으로 알려주고 클라이언트는 그 네임서버와 다시 1)의 과정을 반복
3) 그러한 과정을 통해 클라이언트는 알아낸 IP주소로 접속

② ①과 같이 [클라이언트<->네임서버]가 질의, 응답 패킷을 주고 받게 해주는 프로토콜이 [UDP]가 되겠네요 그러한 UDP에 대해서 구체화해서 설명하죠. UDP를 왜 구체화해서 설명하죠? 그렇죠. 그러한 역할을 해주는 UDP를 설명하면서, 그러한 UDP에 허점이 있다는 것을 제시하고, 그러한 허점을 이용한 것이 DNS스푸핑임을 제시하고 있는 거죠. 따라서 여러분은 그러한 허점이 무엇인지 정확하게 파악하고, 다음 문단을 읽을 때에도 제시된 내용들을 활용해서 읽어주셨어야 이해가 수월하겠죠.

[UDP의 허점] -> [이러한 허점을 이용한 DNS스푸핑]

1) UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 패킷을 보내기만 할 뿐 도착여부는 확인하지 않음
2) 특정 질의 패킷에 [처음] 도착한 응답 패킷을 신뢰 -> [다음]에 도착한 패킷은 확인하지 않고 버림
3) 이러한 1~2)의 UDP의 허점을 이용해 -> DNS스푸핑의 발생

5문단 정리
->[사용자가 웹사이트의 정상적으로 작동하는 과정 = 클라이언트와 네임서버가 서로 질의&응답 패킷을 주고 받음] -> [그 과정에서의 UDP의 역할과 허점] -> [그러한 허점을 이용한 DNS스푸핑]

<6문단>

① 1문단에서 말한 DNS스푸핑이 이루어지는 과정에 대해서 설명해주는 문단이자, 가장 핵심이 되는 문단이네요. 그리고 이러한 DNS스푸핑의 발생 과정은 5문단에서 말한 UDP의 허점을 이용해서 발생한다는 내용이 오겠죠. 앞에 제시된 선행 개념과, 정상적으로 작동하는 과정, 그 과정에서의 UDP의 허점을 이해해두었다면 매우 수월하게 이해할 수 있는 문단이었죠. 그걸 위해서 미리 선행 개념을 제시해줬던 거니까요:)

[DNS 스푸핑의 과정]

1) 악성 코드에 감염되어 DSN 스푸핑을 행하는 컴퓨터 = 공격자
2) 정상 컴퓨터 = 클라이언트가 네임서버에 질의 패킷을 보낼 때, 공격자에게도 패킷이 전달 됨
3) 공격자는 위조 사이트의 IP주소가 적힌 응답 패킷을 클라이언트에게 보내고, 그 패킷이 네임서버가 보내는 패킷보다 먼저 클라이언트에게 도착함 .
4) 클라이언트는 그 먼저 도착한 위조 사이트의 IP주소를 통해 위조 사이트로 연결 됨

->3~4)과정에서 UDP의 허점을 이용하는 거죠. 즉 클라이언트는 먼저 도착한 IP주소를 신뢰하고, 뒤에 오는 네임서버의 패킷을 버리게 되는 거고, 그것을 이용한 게 DNS스푸핑이니까요:)

6문단 정리
->UDP의 허점을 이용한 DNS스푸핑의 과정

후국일몽 독해의 기본 정답&해설

[2018학년도 6월 모의평가 30~34번]

30번 : ④

->DHCP를 이용하는 컴퓨터는 유동 IP주소를 할당받는 컴퓨터이므로, IP주소를 받을 때 자동으로 네임서버의 IP주소가 기록된다고 했죠. 사용자가 직접 기록해야 하는 경우는 고정 IP주소를 사용하는 경우에 해당해요. 전형적인 [구분][비교] 문제에 해당하네요.

①[정의][구분][목/수]
->2문단 [프로토콜은 컴퓨터들이 연결되어 서로 데이터를 주고받기 위해 사용하는 통신 규약으로 소프트웨어나 하드웨어로 구현된다.]에서 규약이라는 것을 확인할 수 있고, [DHCP -> 유동 IP주소를 부여해줌], [UDP -> 네임서버와 클라이언트가 패킷을 주고 받게 해줌], [IP -> 고유 IP주소를 만들어줌] 등과 같이 저마다 정해진 기능이 있어요.
②[예시]
->2문단 [현재 주로 사용하는 ~4개의 필드에 숫자를 사용하여 나타낸다]에서 확인할 수 있네요.
③[인과][구분]
->유동 IP주소를 사용하는 경우에 해당해요. 3문단을 보면 [DHCP는 IP가 필요한 컴퓨터의 요청을 받아 주소를 받아 할당해 줌 -> 컴퓨터가 IP주소를 사용하지 않으면 주소를 반환받아 다른 컴퓨터가 그 주소를 사용할 수 있도록 함]이므로 적절하죠.
⑤[목/수]
->5문단 UDP는 패킷의 빠른 전송 속도를 확보하기 위해 상대에게 패킷을 보내기만 할 뿐 도착 여부는 확인하지 않는다고 했어요. 이러한 점을 악용한 것이 DNS스푸핑에 해당하는 거죠.

31번 : ③[인과]

->해당 문제와 같이 <보기>에 지문의 [인과]과정이 그림으로 제시된 경우에는 그림을 보면서 글을 읽는 것이 훨씬 이해하기 쉬운 경우가 많아요. <보기>는 5문단에서 설명하는 ㉮와 6문단에서 설명하는 ㉯의 과정에서 이루어지는 '클라이언트의 동작'을 나타낸 것이므로, 각각의 경우에 '클라이언트의 동작'이 어떻게 다른지를 비교해가면서 읽어주면 좋아겠죠.

ⓒ는 ⓐ에서 질의한 도메인 네임에 해당하는 IP주소를 네임서버가 찾았는지 여부를 확인하는 절차에 해당합니다. 확인 후 IP주소를 네임서버가 찾았을 경우엔 찾은 IP주소를 ⓑ에 질의 패킷으로 보내주고 '클라이언트'는 ⓔ와 같이 응답 패킷에 적힌 IP 주소로 접속하죠. 반면 질의 패킷을 받은 네임서버가 해당 IP주소를 찾지 못했다면, 다른 네임서버의 IP 주소를 알려줍니다. 그러면 '클라이언트'는 다시 응답 패킷에 적혀있는 다른 네임서버에 ⓐ와 같이 다시 질의 패킷을 보내고 다시 응답 패킷을 받는 거죠. 이러한 과정을 해당 도메인 네임의 IP주소를 찾을 때가지 반복하네요.

①,②구분][비교][인과]
->㉮의 정상적인 과정에 해당하죠. ⓐ가 두 번 동작했다는 것은 [클라이언트 A라는 네임서버에 질의 패킷을 보냄->근데 A에는 클라이언트가 질의한 도메인 네임에 해당하는 IP주소가 없음 -> B라는 다른 네임서버의 주소를 응답 패킷으로 보내줌 -> 그럼 클라이언트는 다시 B에 질의 패킷을 보냄 -> 이번엔 B에 해당 IP주소가 있음 -> 해당 주소로 접속]의 과정인 것이죠. 따라서 [두 질의 내용은 동일하고 패킷을 받는 수신 측은 A와B로 다르다.]라고 봐야겠죠.
ⓑ가 두 번인 경우도 마찬가지에요. 따라서 두 응답 내용은 서로 다르겠죠. 첫 번째는 [B라는 다른 네임 서버의 주소], 두 번째는 [질의한 도메인 네임에 해당하는 IP주소]이겠죠. 또한 ⓑ라는 응답 패킷을 보낸 송신 측 역시 A와 B라는 서로 다른 네임 서버겠죠.
④,⑤[구분][비교][인과]
->㉯와 같이 DNS 스푸핑이 이루어지는 과정이네요. 공격자가 보내 온 IP주소가 포함되어 있는 것은 버려지지 않는 처음으로 받은 응답 패킷에 해당할 것입니다. 즉 네임 서버로 부터 응답 패킷이 도착하기 전에 공격자가 먼저 응답 패킷을 클라이언트에게 보내고, 네임 서버가 보낸 응답 패킷은 첫 번째로 도착하지 못하므로, ⓓ와 같이 버려지겠죠. 따라서 ⓔ가 ㉮의 경우에는 질의한 도메인 네임으로 접속하겠지만, ㉯의 경우에는 첫 번째로 도착한 것은 공격자가 보낸 위조 사이트의 IP주소이므로 클라이언트는 위조IP에 접속하게 되겠죠.

32번 : ②[목수]

->3문단 [한편, 인터넷에 직접 접속은 안 되고, 내부 네트워크에서만 서로를 식별할 수 있는 사설 IP주소도 있다.]에서 확인할 수 있죠. 즉 서로를 식별하기 위해서는 서로의 IP주소가 달라야만 합니다. 따라서 적절해요:)

①[목수][구분]
->DNS는 도메인 네임을 공인 IP주소로 변환해주는 장치죠.
③[인과]
->유동 IP주소는 공인 IP주소의 한 종류에 속하는데, 이러한 주소는 중복 지정하거나, 임의로 지정해서는 안 된다. 특히 유동 IP주소의 경우에 DHCP가 IP 주소가 필요한 컴퓨터의 요청을 받아 주소를 할당해 주고, 사용하지 않으면 반환받은 후에 다른 컴퓨터가 사용하도록 해주기 때문에 동시에 다른 컴퓨터가 같은 주소를 사용할 수 없어요.
④[인과]
->고정 IP주소 역시 공인 IP주소의 한 종류에 속하는데 이러한 주소는 중복 지정하거나 임의로 지정해서는 안 되겠죠. 따라서 동시에 같은 주소가 중복되어 사용될 수 없어요.
⑤[인과][비교]

->고정IP & 유동IP를 사용하는 컴퓨터는 네임서버의 IP주소가 기록되는 방법만 각각 수동/자동으로 다를 뿐 기록되는 네임서버의 IP주소는 인터넷 통신사들이 사용자들이 공동으로 사용할 수 있는 동일한 주소를 이용하겠죠.

33번 : ⑤[인과]

->DNS 스푸핑을 피하는 방법을 알기 위해서는 먼저 DNS 스푸핑의 원리를 이해해야 하는 문제에요. [클라이언트<->네임서버]간의 질의&응답 패킷이 오가는 과정 중 [네임서버 -> 클라이언트]로의 응답 패킷이 가는 과정에서 공격자가 개입해 네임서버의 응답 패킷보다 먼저 공격자의 응답 패킷이 도달하게 하는 것이 DNS스푸핑의 원리죠. <보기>를 보면 [DNS 고안되기 전 -> 네임서버가 없었을 때 -> 클라이어트&네임서버의 질의&응답으로 IP주소에 접속하는 것이 아님 -> 클라이언트가 host라는 파일을 보고 직접 IP주소를 찾아서 접속]했던 것을 의미해요. DNS가 있는 현재에도 클라이언트는 먼저 host를 확인하고 거기에 해당하는 IP주소가 없으면 비로소 네임서버에 질의 패킷을 보내는 것이죠. 그렇다면, DNS 스푸핑을 피하는 가장 확실한 방법은 애초에 공격자가 개입할 수 없게 [클라이너트<->네임서버]간의 질의&응답을 안 하면 되겠죠. 따라서 ⑤과 같이 사용자가 클라이언트의 host파일에 적어 접속하려는 IP주소를 적어놓으면 클라이언트는 그 host파일에서 해당 주소를 확인하고 굳이 질의 패킷을 보내지 않고도, 해당 주소로 접속할 것이네요.

①[인과]
->host파일을 삭제하면 클라이언트는 네임서버에 질의 패킷을 보낼 수밖에 없어요.
②[인과]
->클라이언트의 IP주소가 아니라, 접속하려는 도메인 네임에 해당하는 IP주소가 필요한 것이죠.
③[인과]
->인터넷은 공인 IP주소를 동작하는 것이며, 단지 우리가 인터넷을 사용할 때는 사용의 편의를 위해 도메인 네임을 사용할 뿐이죠. 따라서 도메인 네임을 IP주소로 변환해주는 과정이 필요해요.
④[인과]
->네임서버의 도메인 네임과 IP주소가 아니라, 접속하려는 도메인 네임에 해당하는 IP주소가 필요해요.

34번 : ②

->나타낸다 : 보이지 아니하던 어떤 대상이 모습을 드러내다.
->표시한다 : 겉으로 드러내 보이다.