[30~34] 다음 글을 읽고 물음에 답하시오. -2018.06

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.

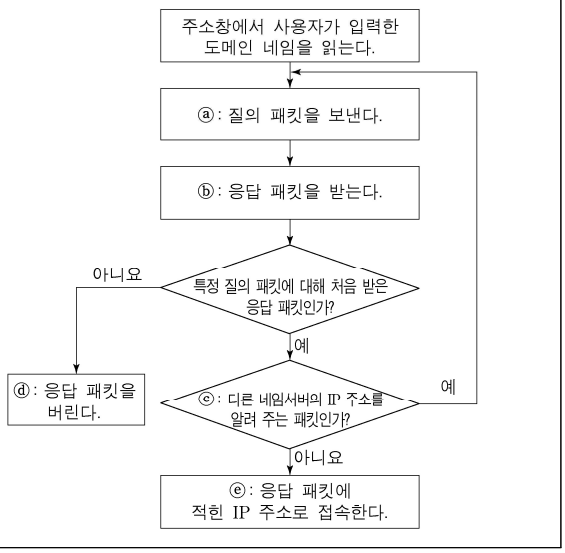
㉯ DNS 스푸핑이 이루어지는 과정을 알아보자. 악성 코드에 감염되어 DNS 스푸핑을 행하는 컴퓨터를 공격자라 한다. 클라이언트가 네임서버에 특정 IP 주소를 묻는 질의 패킷을 보낼 때, 공격자에도 패킷이 전달되고 공격자는 위조 사이트의 IP 주소가 적힌 응답 패킷을 클라이언트에 보낸다. 공격자가 보낸 응답 패킷이 네임서버가 보낸 응답 패킷보다 클라이언트에 먼저 도착하고 클라이언트는 공격자가 보낸 응답 패킷을 옳은 패킷으로 인식하여 위조 사이트로 연결된다.

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