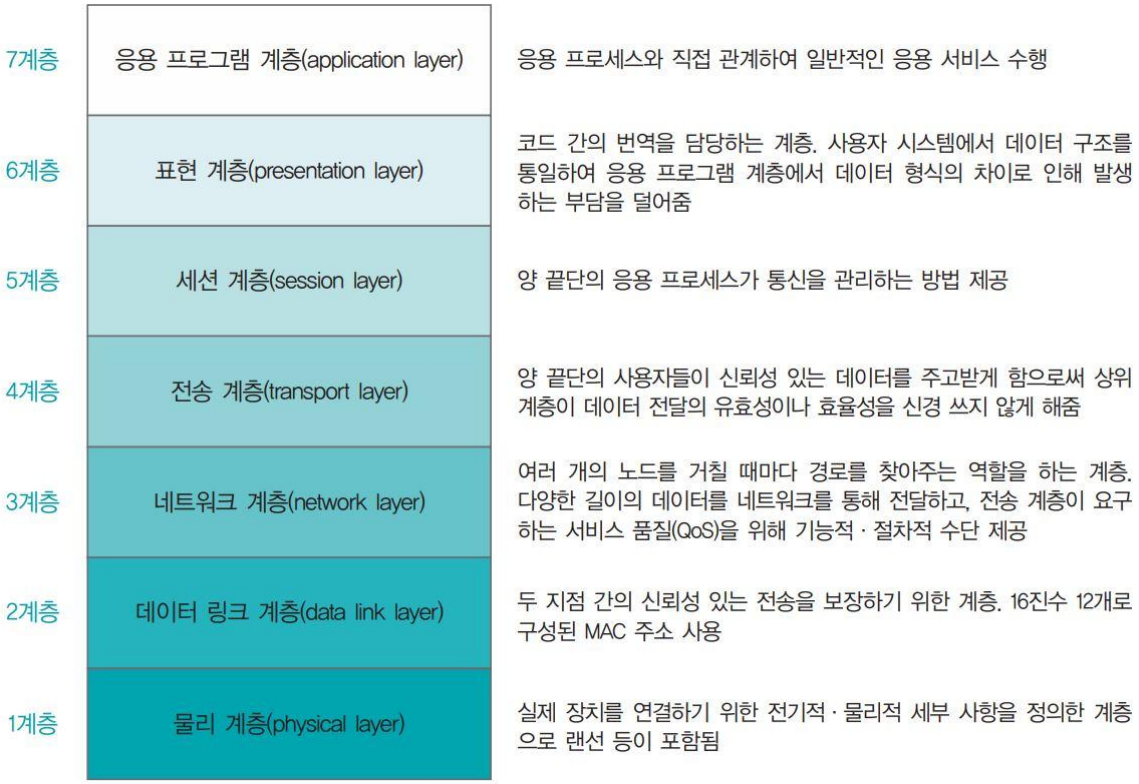
1. 네트워크의 이해

OSI 7계층의 이해

- 국제표준화기구(ISO)는 다양한 네트워크 간의 호환을 위해 만든 표준 네트워크 모델



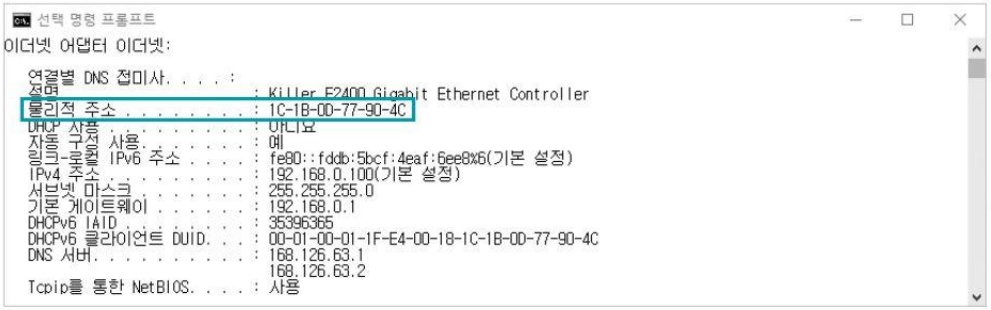
1. 네트워크의 이해

데이터 링크 계층 (2계층)

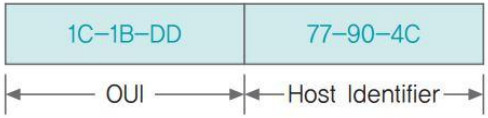
- 두 포인트 간의 신뢰성 있는 전송을 보장하기 위한 계층으로, CRC 기반의 오류 제어 및 흐름 제어가 필요
- 네트워크 위의 개체간에 데이터를 전달하며, 물리 계층에서 발생할 수 있는 오류를 찾아내고 수정하는 데 필요한 기능적·절차적 수단을 제공

MAC 주소

- 데이터 링크 계층에서는 상호 통신을 위해 MAC 주소를 할당 받음
  - MAC 주소는 윈도우 명령 창에서 ipconfig /all 명령을 실행하여 확인



  - MAC 주소는 총 12개의 16진수로 구성
  - 앞쪽의 6개 16진수는 네트워크 카드 를 만든 회사를 나타내는 것으로 OUIO
  - 뒤쪽의 6개 16 진수는 각 회사에서 임의로 붙이는 일종의 시리얼
  - 한 회사에서는 같은 시리얼의 네트워크 카드를 만들지 않기 때문에 같은 MAC 주소는 존재하지 않음

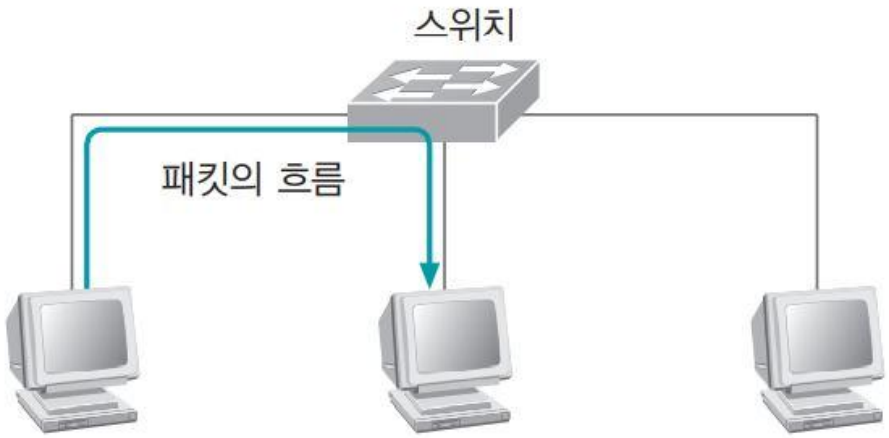


1. 네트워크의 이해

■ 데이터 링크 계층 (2계층)

▪ 데이터 링크 계층의 패킷 흐름

- 데이터 링크 계층의 대표적인 네트워크 장비는 스위치
- MAC 계층에서 동작하는 대표적인 프로토콜은 이더넷

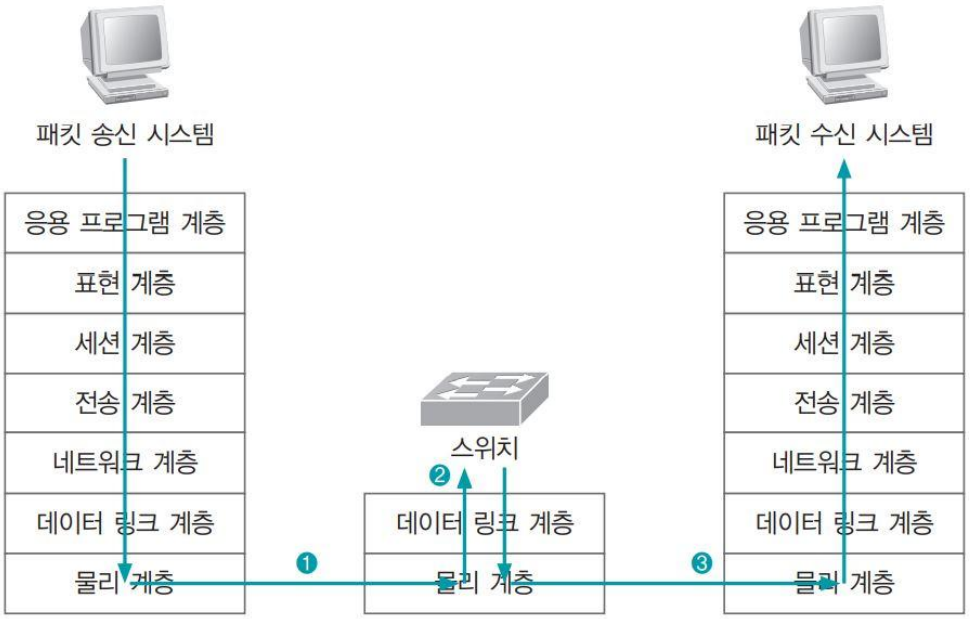


1. 네트워크의 이해

■ 데이터 링크 계층 (2계층)

▪ 데이터 링크 계층의 패킷 흐름

- 데이터 링크 계층의 패킷 흐름을 OSI 7계층에 따른 패킷 흐름



- ❶, ❷, ❸에서 흘러가는 패킷은 다음과 같은 구조

1. 네트워크의 이해

■ 데이터 링크 계층 (2계층)

▪ 스위치의 동작 원리

- 스위치의 포트가 4개이고 안방 컴퓨터와 연결된 케이블이 2번 포트에 꽂힐 경우 메모리의 정보

1번 포트	
2번 포트	안방 컴퓨터의 MAC 주소
3번 포트	
4번 포트	

- 작은방의 컴퓨터와 연결된 랜 케이블을 스위치의 3번 포트에 꽂힐 경우 메모리의 정보

1번 포트	
2번 포트	안방 컴퓨터의 MAC 주소
3번 포트	작은방 컴퓨터의 MAC 주소
4번 포트	

- 일반적으로 잘못 이해할 수 있는 스위치의 메모리 구조

1번 포트	
192.168.0.100	안방 컴퓨터의 MAC 주소
192.168.0.101	작은방 컴퓨터의 MAC 주소
4번 포트	

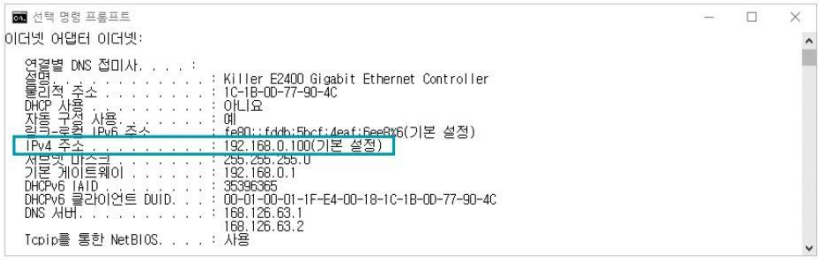
1. 네트워크의 이해

네트워크 계층 (3계층)

- 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할
- 다양한 길이의 데이터를 네트워크를 통해 전달
- 전달 과정에서 라우팅, 흐름 제어, 세그먼테이션, 오류 제어 등을 수행

IP주소

- 네트워크 계층에서 여러 개의 노드를 거쳐 경로를 찾기 위한 주소는 IP로 대표됨
- ipconfig /all 명령을 실행하여 IP 주소를 확인



- 확인한 IP 주소는 8비트의 수 4개로 되어 있음
- 그림 3-7의 IP주소를 이진법으로 바꿀 경우

11000000.10101000.00000000.01100100

1. 네트워크의 이해

■ 네트워크 계층 (3계층)

▪ IP주소의 클래스

- IP 주소는 A, B, C, D, E 클래스로 구분
  - A 클래스: 첫 번째 자리가 네트워크 주소, 나머지 세 자리는 호스트 주소
  - B 클래스: 두 번째 자리까지 네트워크 주소, 나머지 두 자리는 호스트 주소
  - C 클래스: 세 번째 자리까지 네트워크 주소, 나머지 한 자리는 호스트 주소

- A, B, C 클래스는 맨 앞부분의 2진수에 따라 구분

시작 주소	클래스	설명
0	A 클래스	• 00000000번부터 01111111(127)번까지의 네트워크 • A 클래스는 모두 2^7(128)개가 가능하고, 하나의 A 클래스 안에 256^3(16,777,216)개의 호스트가 존재할 수 있다.
10	B 클래스	• 10000000(128)번부터 10111111(191)번까지의 네트워크 • B 클래스는 $2^6 \times 256$(16,384)개가 가능하고, 하나의 B 클래스 안에 256^2(66,536)개의 호스트가 존재할 수 있다.
110	C 클래스	• 11000000(192)번부터 11011111(223)번까지의 네트워크 • C 클래스는 $2^5 \times 256^2$(2,097,152)개가 가능하고, 하나의 C 클래스 안에 256개의 호스트가 존재할 수 있다.
1110	D 클래스	• 11100000(224)번부터 1110111(239)번까지의 네트워크 • 멀티미디어 방송을 할 때 자동으로 부여된다.
E 클래스		• 11110000(240)번부터 1111111(255)번까지의 네트워크 • 테스트를 위한 주소 대역이며 사용하지 않는다.

$\Rightarrow 2^{24} = 16{,}777{,}216$

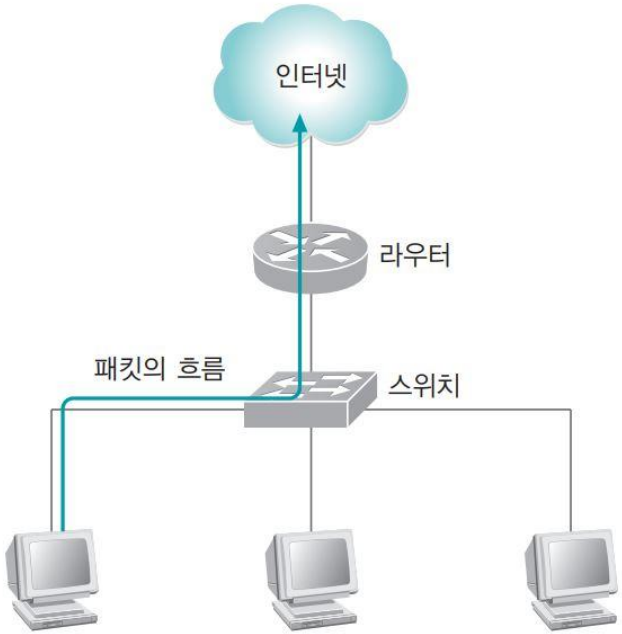
$\Rightarrow 2^{14} = 16{,}384$

$\Rightarrow 2^{21} = 2{,}097{,}152$

1. 네트워크의 이해

■ 네트워크 계층 (3계층)

- 네트워크 계층의 동작
  - 네트워크 계층과 관련된 대표적인 네트워크 장비는 라우터

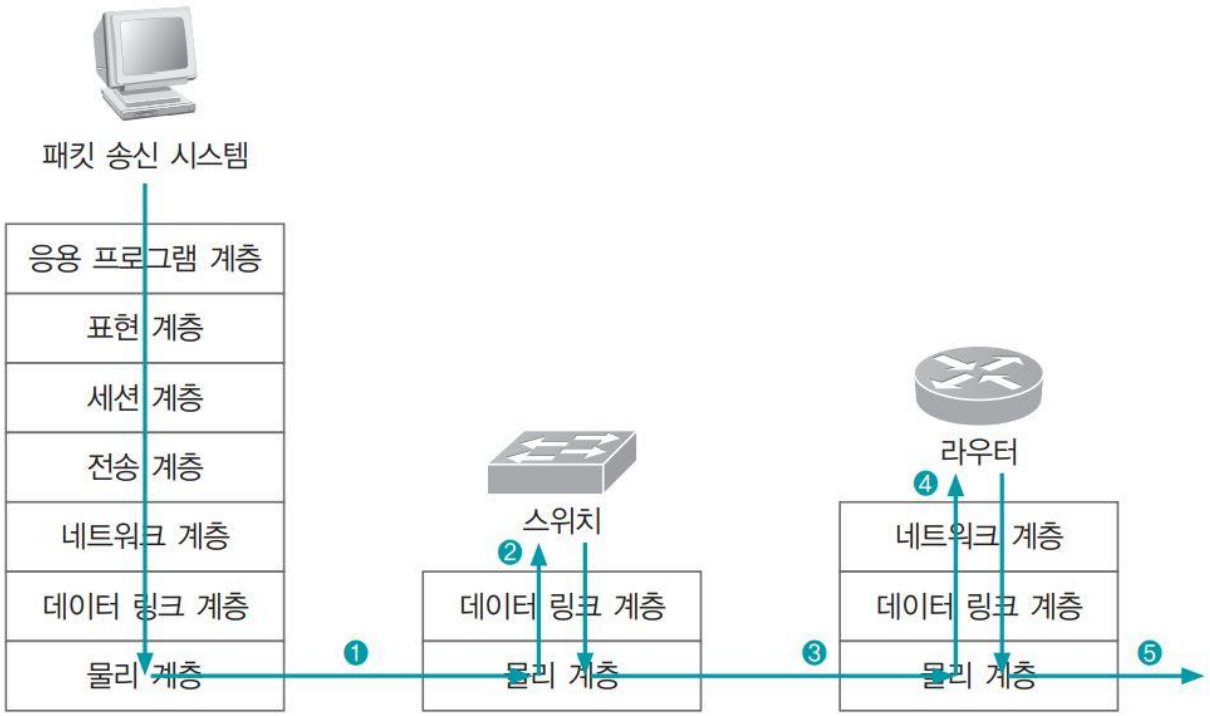


1. 네트워크의 이해

■ 네트워크 계층 (3계층)

▪ 네트워크 계층의 동작

- 데이터 링크 계층과 네트워크 계층의 패킷 흐름을 OSI 7계층에 따른 패킷 흐름으로 나타냄



1. 네트워크의 이해

■ 네트워크 계층 (3계층)

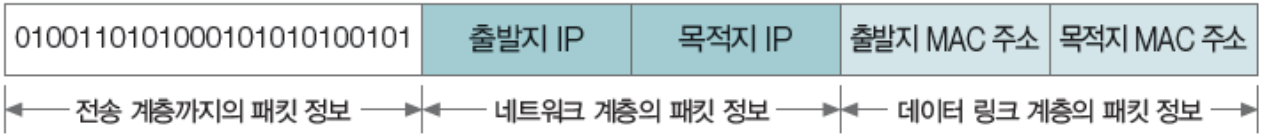
▪ 네트워크 계층의 패킷 전달 구조

- 시스템에서 생성된 패킷이 어떤 프로세스로 인터넷으로 나가는지 살펴보기 위한 예

• 패킷 송신 시스템의 IP: 172.16.0.100
• 라우터 랜 쪽 포트의 IP(게이트웨이): 172.16.0.1
• 패킷 송신 시스템의 MAC 주소: AA-AA
• 라우터 랜 쪽 포트의 MAC 주소(게이트웨이): BB-BB
• 라우터 인터넷 쪽 포트의 MAC 주소: CC-CC
• 스위치의 메모리에 존재하는 MAC 주소 테이블

1번 포트	BB-BB(라우터 케이블 연결 포트)
2번 포트	AA-AA(컴퓨터 연결 포트)
3번 포트	
4번 포트	

- 인터넷으로 보내는 패킷의 기본 구조

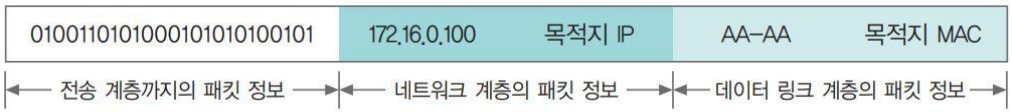


1. 네트워크의 이해

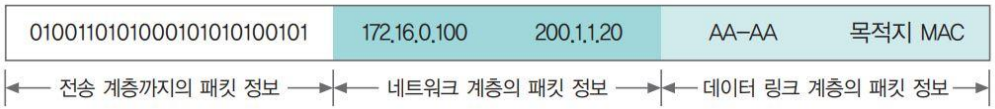
■ 네트워크 계층 (3계층)

▪ 네트워크 계층의 패킷 전달 구조

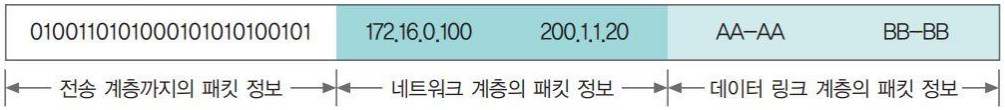
- 출발지의 IP와 MAC 주소가 기록됨



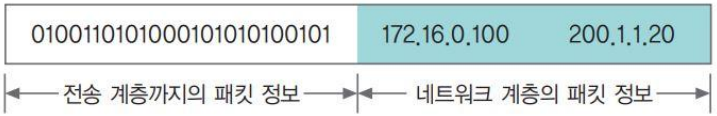
- 목적지 IP 주소 입력



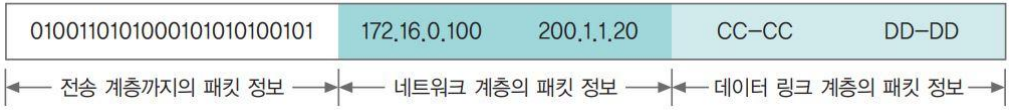
- 목적지 MAC 주소에는 랜을 벗어나기 위한 가장 일차적인 목적지, 즉 게이트웨이의 MAC 주소 입력
  - ARP 프로토콜 이용



- 라우터에서 사용한 데이터 링크 계층 정보를 벗겨냄



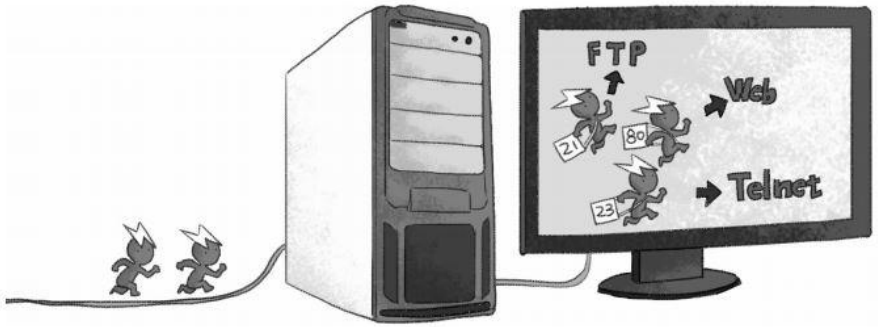
- 다음 라우터까지의 데이터 링크 계층 정보를 패킷에 덧씌움



1. 네트워크의 이해

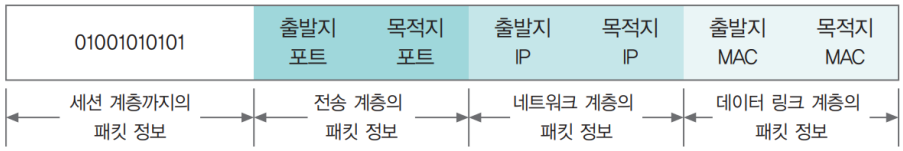
전송 계층 (4계층)

- 양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받을 수 있게 함
- 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌
- 시퀀스 넘버 기반의 오류 제어 방식을 사용하여 특정 연결의 유효성을 제어
- 가장 잘 알려진 전송 프로토콜은 TCP로 MCA주소와 IP주소처럼 TCP에도 포트라는 주소가 있음



포트

- 시스템에 도착한 후 패킷이 찾아갈 응용 프로그램으로 통하는 통로 번호
- 시스템에서 구동되는 응용 프로그램은 네트워킹을 하기 위해 자신에게 해당되는 패킷을 식별 할 때 사용
- 포트의 패킷 구조



1. 네트워크의 이해

■ 전송 계층 (4계층)

▪ 출발지 포트 결정

- 출발지 포트는 보통 1,025~ 65,535번 중에서 사용하지 않는 임의의 포트를 응용 프로그램별로 할당하여 사용

- 예시) 웹 서버에 접속할 경우
  - 웹 서버의 서비스 포트

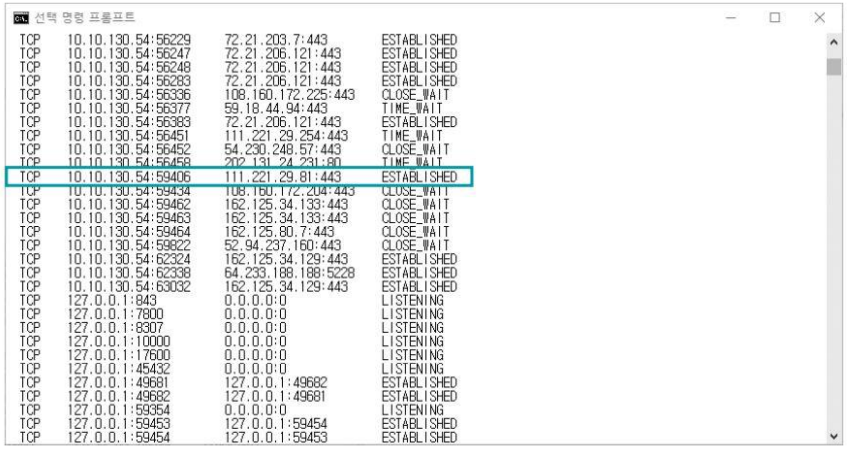
  - 출발지 포트로 할당된 3000번 대의 임의 포드

1. 네트워크의 이해

전송 계층 (4계층)

연결 상태 정보

- 네트워크 계층과 전송 계층의 정보는 netstat -an 명령으로 쉽게 확인할 수 있음

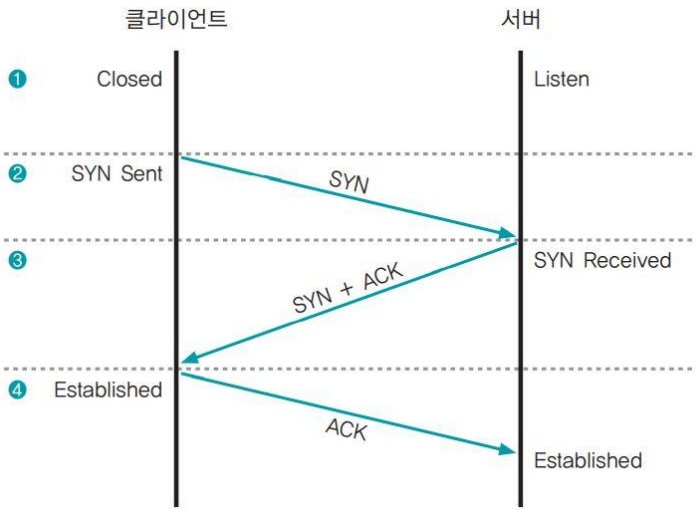


- 연결 상태 정보는 ESTABLISHED로 확인됨
- TCP는 패킷을 주고받기 전에 미리 연결을 맺어 가상 경로를 설정
- 연결을 설정하는 과정과 연결을 종료하는 과정이 존재
- 연결 설정 과정은 '3-way 핸드셰이킹' 이라고 함

1. 네트워크의 이해

■ 전송 계층 (4계층)

- TCP의 연결 과정 (3-way 핸드셰이킹)



❶ 두 시스템이 통신을 하기 전에 클라이언트는 포트가 닫힌 Closed 상태
서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태

❷ 클라이언트가 처음 통신을 하려면 임의의 포트 번호가 클라이언트 프로그램에 할당
클라이언트는 서버에 연결하고 싶다는 의사 표시로 SYN Sent 상태가 됨

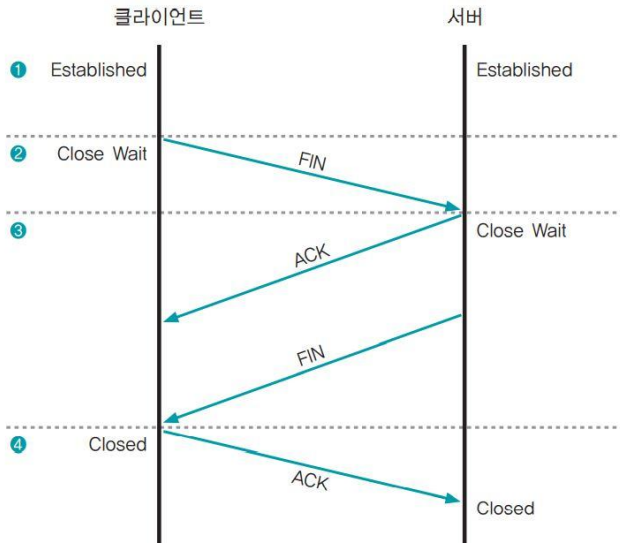
❸ 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 됨
클라이언트에 연결을 해도 좋다는 의미로 SYN + ACK 패킷을 보냄

❹ 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보냄

1. 네트워크의 이해

■ 전송 계층 (4계층)

- TCP 연결 해제 과정



❶ 통신 중에는 클라이언트와 서버 모두 Established 상태

❷ 통신을 끊으려는 클라이언트가 서버에 FIN 패킷을 보내고 클라이언트는 Close Wait 상태가 됨

❸ 서버는 클라이언트의 연결 종료 요청을 확인하고 응답으로 클라이언트에 ACK 패킷을 보내면 서버도 클라이언트의 연결을 종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 됨

❹ 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버에 보냄

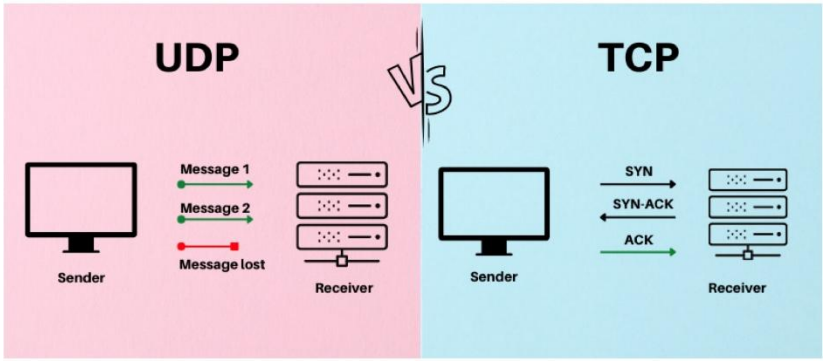
1. 네트워크의 이해

전송 계층 (4계층)

- TCP
  - 연결 지향형 프로토콜
    - 수신 측이 데이터를 흘려버리지 않도록 하는 데이터 흐름 제어
    - 전송 중 에러가 발생하면 자동으로 재전송하는 에러 제어 기능
  - 이를 통해 데이터의 확실한 전송을 보장 하지만 과정이 완전하지 않아 해커들에게 많은 공격을 받음

- UDP
  - TCP와 달리 데이터의 신뢰성 있는 전송을 보장하지 않음
  - 특정한 경우 전송 경로 확립을 위한 번잡함을 생략하고 시간을 절약할 수 있어 UDP가 더 효과적
    - 신뢰성이 매우 높은 회선을 사용하는 경우, 데이터의 확실한 전송을 요구하지 않는 경우, 한 번에 많은 상대에게 메시지를 전송하는 경우

항목	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
연결 방식	연결형 (Connection-oriented)	비연결형 (Connectionless)
신뢰성	높음	낮음
순서 보장	보장함	보장하지 않음
오류 검출 및 재전송	있음	없음
속도	상대적으로 느림	상대적으로 빠름
헤더 크기	큼 (20 바이트)	작음 (8 바이트)
오버헤드	높음	낮음
사용 사례	웹 페이지, 이메일, 파일 전송 등	스트리밍, 온라인 게임, VoIP 등



1. 네트워크의 이해

- **세션 계층(5계층)**
  - 양끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공
  - 동시 송수신 방식, 반이중 방식, 전이중 방식의 통신과 함께 체크 포인팅, 유휴, 종료, 다시 시작의 과정을 수행
- **표현 계층(6계층)**
  - 코드 간의 번역을 담당
  - ASN.1 방식
    - 사용자 시스템에서 데이터 구조를 하나의 통일된 형식으로 표현하여 응용 계층의 데이터 형식 차이로 인한 부담을 덜어 줌
    - 응용 프로그램 계층 간의 서로 다른 표현을 인식하기 위해 정보를 정의하고 데이터의 압축과 암호화 기능을 수행
- **응용 프로그램 계층(7계층)**
  - 사용자나 응용 프로그램 사이에 데이터 교환이 가능하게 하는 계층
  - 응용 프로세스와 직접 관계하여 일반적인 응용 서비스를 수행
  - HTTP, FTP, 터미널 서비스, 메일 프로그램, 디렉터리 서비스 등을 제공

2. 서비스 거부 공격: DoS와 DDoS

- **서비스 거부 공격(Denial of Service; DOS)**
  - 다른 해킹에 비해 비교적 간단한 것으로 일종의 훼방
    - 예를 들면 깡패가 노점상의 장사를 방해하는 것
    - 집기를 부수거나 식재료의 공급을 끊거나 나쁜 재료를 음식에 몰래 섞는 것

2. 서비스 거부 공격: DoS와 DDoS

- **서비스 거부 공격(DoS)**
  - 취약점 공격 형
    - 공격 대상이 반복적인 재요청과 수정을 계속하게 함으로써 시스템 자원을 고갈시키는 방법
    - 시스템의 패킷 재전송과 재조합에 과부하기 걸리도록 순서 번호를 속임
      - 보잉크(Boink)/봉크(Bonk)/티어드롭(Teardrop) 공격, 랜드(Land) 공격
  - 자원 고갈 공격 형
    - 네트워크 대역폭이나 시스템의 CPU, 세션 등의 자원을 소모시키는 형태
      - 랜드 공격, 죽음의 핑 공격(Ping of Death), SYN 플러딩(Flooding) 공격, HTTP GET 플러딩 공격
      - HTTP CC 공격, 동적 HTTP Request 플러딩 공격, 슬로 HTTP 헤더 DoS(슬로로리스) 공격, 슬로 HTTP POST 공격
      - 스머프 공격, 메일 폭탄 공격

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- 보잉크/봉크/티어드롭 공격
  - 프로토콜의 오류 제어 로직(재전송 요청 등)을 악용하여 시스템 자원을 고갈시키는 방식
  - TCP 프로토콜이 제공하는 오류 제거 기능
    - 패킷의 순서가 올바른지 확인
    - 중간에 손실된 패킷이 없는지 확인
    - 손실된 패킷의 재전송을 요구
  - TCP는 데이터 전송 시 신뢰를 확보하기 위해 패킷 전송에 문제가 있으면 반복적으로 재요청과 수정을 함
  - 보잉크, 봉크, 티어드롭은 공격 대상이 반복적인 재요청과 수정을 계속하게 함으로써 시스템 자원을 고갈시킴

보잉크, 봉크 공격

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- 보잉크/봉크/티어드롭 공격
  - 시퀀스 넘버가 조작된 패킷의 흐름은 공격 대상에게 절대로 풀 수 없는 퍼즐을 던져주는 것과 같음
  - 이런 취약점은 패치 관리를 통해 과부하가 걸리거나 계속 반복되는 패킷을 무시하고 버리도록 처리

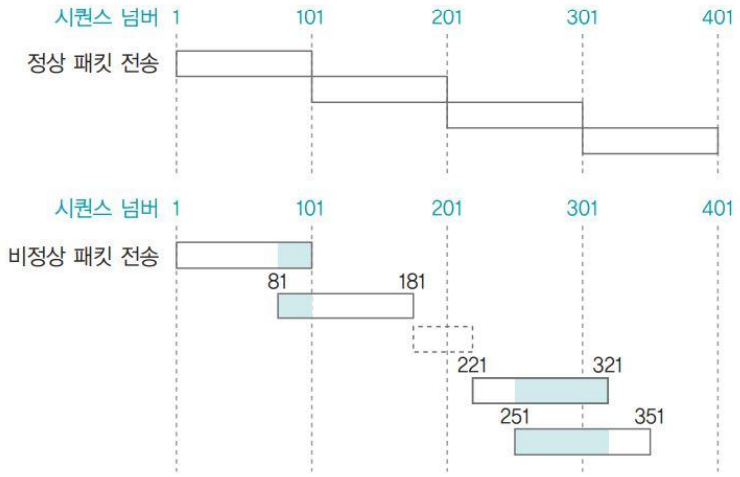
- Bonk : 처음 패킷을 1번으로 보낸 후 두 번째와 세 번째 패킷의 시퀀스 넘버를 모 두 1번으로 조작해서 보냄.
- Boink : 공격자는 hping3와 같은 도구를 사용하여 패킷을 생성하고, 특정 IP 주소로 패킷을 전송할 때, 패킷의 시퀀스 번호를 조작하여 비정상적인 순서로 전송
- Teardrop : 시퀀스 넘버를 일정하게 바꾸는 것을 넘어 중첩과 빈 공간을 만들어 시퀀스 넘버가 좀 더 복잡해지도록 섞음. **공격자는 패킷의 조각 순서와 길이를 조작**

➔ 전혀 맞지 않는 시퀀스 넘버 때문에 공격 대상이 패킷화된 데이터를 재조합 하는 데 혼란이 생겨 CPU에 과부하가 걸리게 됨

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- Teardrop

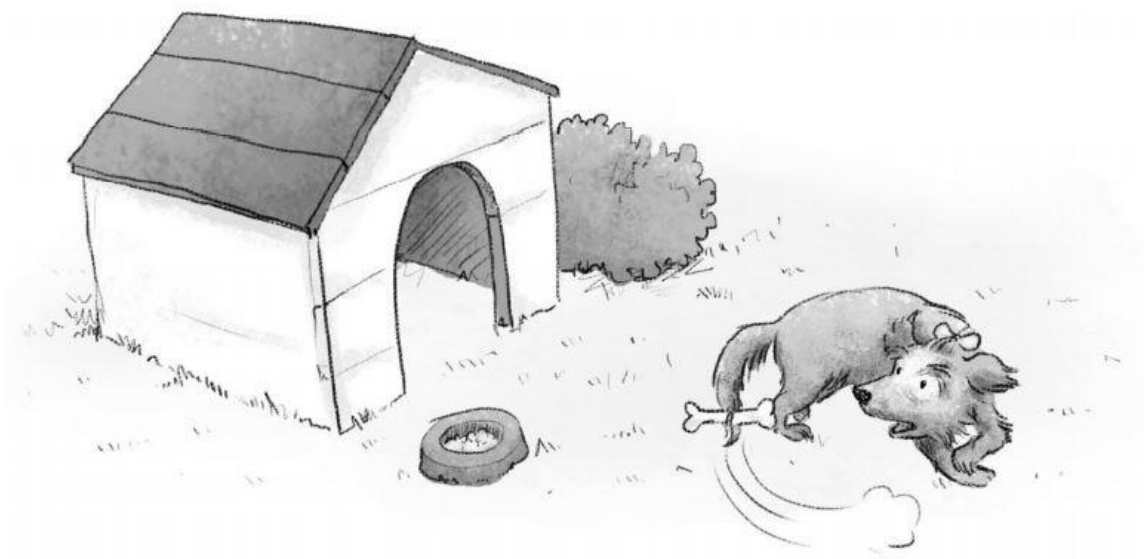


패킷 번호	정상 패킷의 시퀀스 넘버	공격을 위한 패킷의 시퀀스 넘버
1	1~101	1~101
2	101~201	81~181
3	201~301	221~321
4	301~401	251~351

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

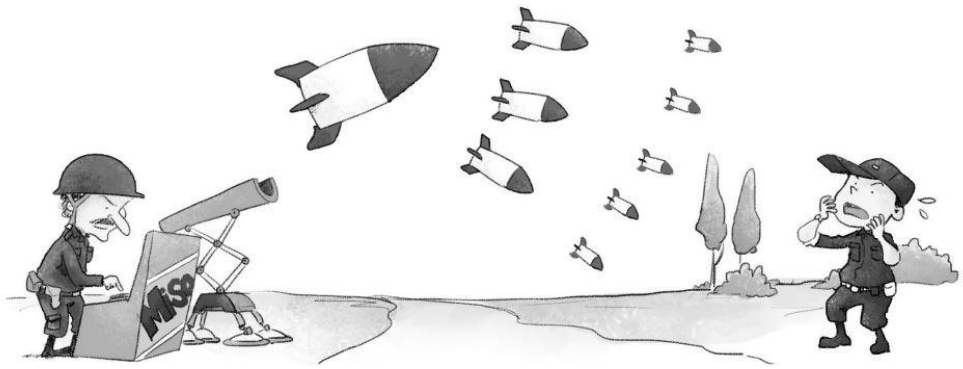
- 랜드(Land) 공격
  - 'land'를 영어사전에서 찾아보면 '땅', '착륙하다'라는 뜻 외에 '(나쁜 상태에) 빠지게 하다'라는 뜻
  - 패킷을 전송할 때 출발지 IP 주소와 목적지 IP 주소의 값을 똑같이 만들어서 공격 대상에게 보내는 것(조작된 IP 주소 값은 공격 대상의 IP 주소여야 함)
  - 이 공격법은 SYN 플러딩처럼 동시 사용자 수를 점유하고 CPU 부하를 올림.
  - Land 공격도 현재의 시스템에서는 대부분 효과가 없음
    - 현재의 시스템(라우터, 방화벽)은 출발지 주소와 목적지 주소를 확인하여 동일한 패 킷은 인식하고 버림



2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- 죽음의 핑 공격(Ping of Death)
  - NetBIOS 해킹과 함께 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격 방법
  - 네트워크의 연결 상태를 점검하는 ping 명령을 보낼 때 공격 대상에게 패킷을 최대한 길게(65,535 byte) 보내 패킷을 쪼갬(보통 Ping 요청은 32 또는 64byte)
  - **초당 수천 개의 큰 ICMP 에코 요청 패킷을 보내고** 대상 컴퓨터에서 조각을 다시 조립하려고 하면 CPU와 메모리 자원 소모가 증가하여 시스템의 성능이 저하되고, 결국 정상적인 서비스 요청을 처리할 수 없게 됨
  - 죽음의 핑 공격을 막으려면 ping이 내부 네트워크에 들어오지 못하도록 방화벽에서 ICMP를 차단
  - 방화벽, IDS/IPS 시스템에서 공격 패턴을 분석하여 감지
    - ICMP 패킷의 최대 크기를 제한하여 비정상적으로 큰 패킷을 차단
    - 반복적으로 들어오는 일정 수 이상의 ICMP 패킷을 필터링하게 설정(현재 대부분의 시스템)
  - 재조립 프로세스에서 패킷 재조립 후 ICMP 패킷의 최대 크기 제약 제한 정책 설정(보안 패치와 업데이터 등)

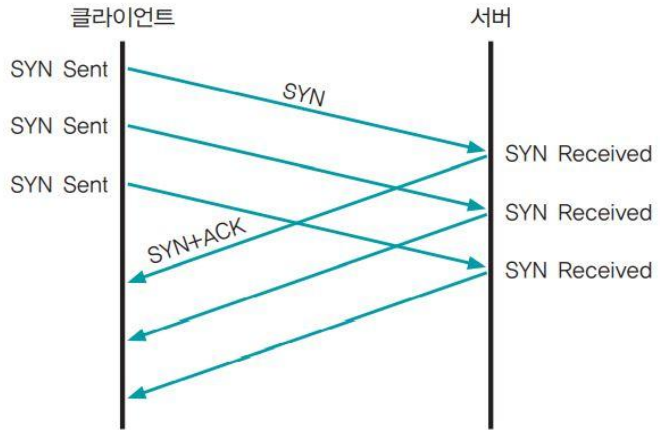


2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- SYN 플러딩(Flooding) 공격
  - **네트워크에서 서비스를 제공하는 시스템에는 동시 사용자 수 제한이 있는데 이를 이용한 공격을 말함**
  - 존재하지 않는 클라이언트가 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 함
    - TCP의 연결 과정인 3-way 핸드셰이킹의 문제점을 악용하는 것
  - 특정 웹 서버의 접속자가 폭주하여 서버 접속이 되지 않고 마비되는 경우도 이 공격을 받은 상황과 유사
    - 정상적인 인터넷 서비스의 경우, 어떤 사회적 이슈로 인하여 접속자가 폭주하여 서버가 접속되지 않고 마비되는 경우
  - 공격 대응책은 SYN Received의 대기 시간을 줄이는 것
  - IDS/IPS와 같은 보안 시스템으로 비정상적인 트래픽을 차단하거나 경고를 발생
    - 짧은 시간 안에 똑같은 형태의 패킷을 보내는 형태의 공격을 인지했을 경우 , 그에 해당하는 IP 주소 대역의 접속을 금지하거나 방화벽 또는 라우터에서 해당 접속을 금지시킴

기본 원리 : 클라이언트가 서버에 ACK 패킷을 보내지 않으면 → ACK 패킷을 수신할 때 까지 SYN Received 상태로 일정시간 기다림 → 공격자는 SYN 패킷을 수없이 만들어서 서버에 보내어 동시 접속자 수를 모두 SYN Received로 만듦.



SYN 플러딩 공격 시 3-웨이 핸드셰이킹

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- HTTP GET 플러딩 공격
  - 공격자가 대량의 HTTP GET 요청을 특정 웹 서버에 보내어 서버의 리소스를 소모시키고, 정상적인 사용자들이 웹 서비스에 접근하지 못하도록 하는 서비스 거부 공격
    - 웹 애플리케이션의 성능을 저하시킬 수 있으며, 심각한 경우 서버가 다운되거나 응답하지 않게 만듦
  - 공격 대상 시스템에 TCP 3-way 핸드셰이킹 과정으로 정상 접속한 뒤 HTTP의 GET 메소드로 특정 페이지를 무한대로 실행하는 공격
  - 공격 패킷을 수신하는 웹 서버는 정상적인 TCP 세션과 정상으로 보이는 HTTP GET을 지속적으로 요청하므로 시스템에 과부하가 걸림
    - 서버는 요청을 처리하기 위해 CPU, 메모리, 대역폭 등의 리소스를 소모
  - 웹 애플리케이션 방화벽(WAF)을 사용하여 **특징적인 요청(트래픽) 패턴을 탐지하고 차단**.
    - 특정 IP에서 오는 과도한 요청을 필터링
  - 특정 IP 주소에서 일정 시간 내에 허용되는 요청 수를 제한하여, 공격자가 대량의 요청을 보내는 것을 방지

```
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
www.wishfree.com/list.php?page=1&search=test
⋮
```

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- HTTP CC 공격
  - HTTP 1.1 버전의 CC 헤더 옵션은 자주 변경되는 데이터에 새로운 HTTP 요청 및 응답을 요구하기 위해 캐시 기능을 사용하지 않을 수 있음
  - 서비스 거부 공격에 이를 응용하려면 'Cache-Control: no-store, must-revalidate' 옵션을 사용
  - 이 옵션을 사용하면 웹 서버가 캐시를 사용하지 않고 응답해야 하므로 웹 서비스의 부하가 증가함

- 동적 HTTP 리퀘스트 플러딩 공격(Dynamic HTTP Request Flooding Attack)
  - 웹 방화벽 등에서 특징적인 HTTP 요청 패턴을 확인하여 방어하는 것을 우회하기 위한 공격
  - **지속적으로 요청 페이지를 변경하여 웹 페이지를 요청**

- 슬로 HTTP 헤더 DoS 공격 (Slowloris Attack)
  - 서버로 전달할 HTTP 메시지의 헤더 정보(GET, Host, User-Agent, Accept 등의 필드)를 한번에 전송하는 것이 아니라 각 필드를 매우 느리게, 또는 일부 필드만 전송한 후 일정 시간 동안 기다리는 방식으로 전송
  - 웹 서버가 헤더 정보를 완전히 수신할 때까지 연결을 유지하도록 하는 공격
  - 시스템 자원을 소비시켜 다른 클라이언트의 정상적인 서비스를 방해

- 슬로 HTTP POST 공격
  - 본문 데이터를 한 번에 전송하는 것이 아니라, 작은 조각으로 나누어 전송하고 각 조각 사이에 긴 지연을 두는 방식. 이로 인해 서버는 요청이 완료될 때까지 연결을 유지.
    - 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여, 서버가 해당 크기의 메시지가 전송될 때까지 커넥션을 유지하게 함.
  - 웹 서버와의 커넥션을 최대한 오래 유지하여 웹 서버가 정상적인 사용자의 접속을 받아들일 수 없게 하는 공격

2. 서비스 거부 공격: DoS와 DDoS

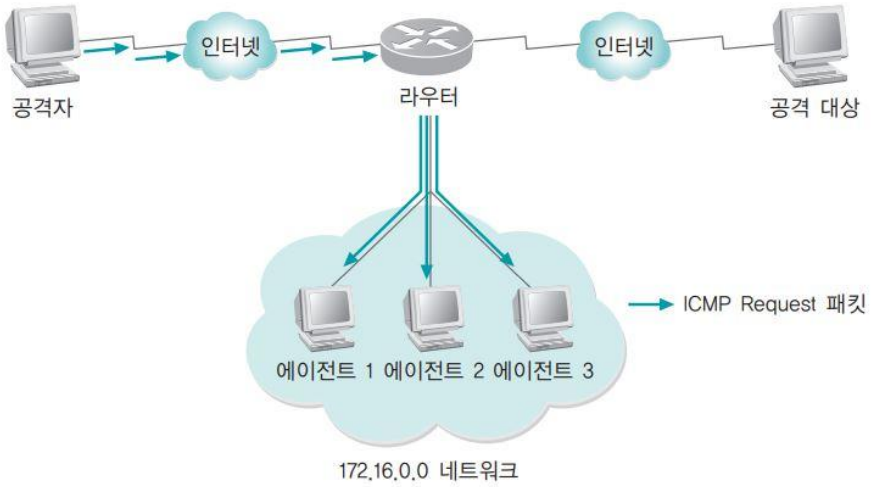
서비스 거부 공격(DoS)

- 스머프 공격(Smurf Attack)
  - **ICMP 패킷과 네트워크에 존재하는 임의의 시스템을 이용하여 패킷을 확장**함으로써 서비스 거부 공격을 수행
  - 다이렉트 브로드캐스트(Broadcast)를 악용하는 것으로 공격 방법이 간단
  - 스머프 공격 예시
    - 스머프 마을에서 거짓말쟁이 스머프가 확성기를 들고 "마을에 가가멜이 나타났어요. 가가멜이에요!"라고 소리침
    - 온 동네 스머프를 다 깨운 뒤 옆에 있던 멀뚱이 스머프에게 확성기를 쥐어 줌
    - 스머프들이 확인해보니 거짓말 이었는데, 모두 확성기를 가지고 있던 멀뚱이 스머프가 한 짓으로 생각함
    - 거짓말쟁이 스머프는 '공격자' / 멀뚱이 스머프는 '공격 대상'

2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

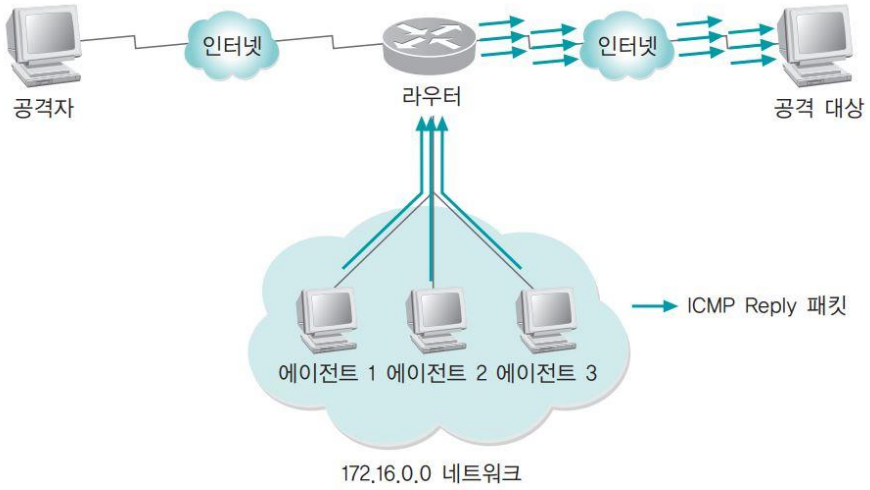
- 스머프 공격
  - 다이렉트 브로드캐스트(Direct Broadcast)
    - 기본적인 브로드캐스트는 목적지 IP 주소 255.255.255.255를 가지고 네트워크의 임의 시스템에 패킷을 보내는 것
    - 브로드캐스트는 기본적으로 네트워크 계층 장비인 라우터를 넘어가지 못함
    - 라우터를 넘어가서 브로드캐스트를 해야 하는 경우에는 클라이언트의 IP 주소 부분에 브로드캐스트 주소인 255를 채움
  - 공격자가 172.16.0.255로 다이렉트 브로드캐스트를 할 경우



2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- 스머프 공격
  - ICMP request를 받은 172.16.0.0 네트워크는 패킷의 위조된 시작 IP 주소로 ICMP reply를 재전송
  - 공격 대상은 수많은 ICMP reply를 받게 되고 수많은 패킷이 시스템을 과부하 상태로 만듦



  - 스머프 공격에 대한 대응책은 라우터에서 다이렉트 브로드캐스트를 막아서 대응함
  - 처음부터 다이렉트 브로드캐스트를 지원하지 않는 라우터도 있음

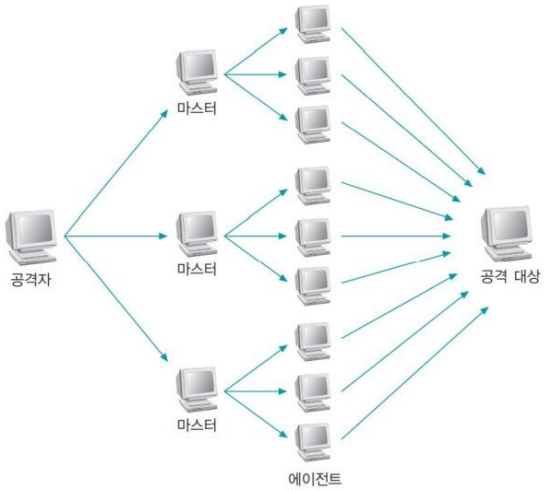
2. 서비스 거부 공격: DoS와 DDoS

서비스 거부 공격(DoS)

- 메일 폭탄 공격(Mail Bombing Attack)
  - 특정 이메일 주소로 대량의 이메일을 보내는 공격 방식
  - 해당 이메일 계정을 과부하 상태로 만들거나, 수신자의 이메일 시스템을 마비시킴
    - 메일 서버는 메일이 폭주하여 디스크 공간을 가득 채우면 메일을 받을 수 없으므로 각 사용자에게 일정한 양의 디스크 공간을 할당
  - 스팸 메일을 서비스 거부 공격으로 분류

분산 서비스 거부 공격(Distributed DoS; DDos)

- 분산 서비스 공격
  - 분산 서비스 거부 공격은 1999년 미네소타대학에서 처음 발생하여 야후, NBC, CNN 서버의 서비스를 중지
  - 아직까지 확실한 대책이 없으며 공격자의 위치와 구체적인 발원지를 파악하는 것도 거의 불가능
    - VPN이나 프록시 서버를 통해 공격을 수행하여 추적을 어렵게 만듦.
  - 분산 서비스의 기본 구성
    - 공격자(Attacker): 공격을 주도하는 해커 컴퓨터
    - 마스터(Master): 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리
    - 핸들러 프로그램(Handler Program): 마스터 시스템의 역할을 수행하는 프로그램
    - 에이전트(Agent): 직접 공격을 가하는 시스템
    - 데몬 프로그램(Demon Program): 에이전트 시스템의 역할을 수행하는 프로그램

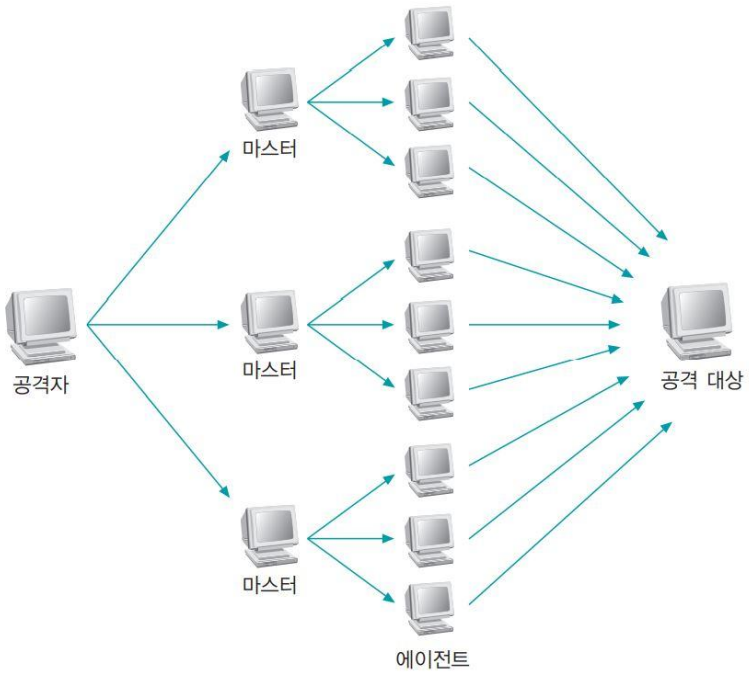


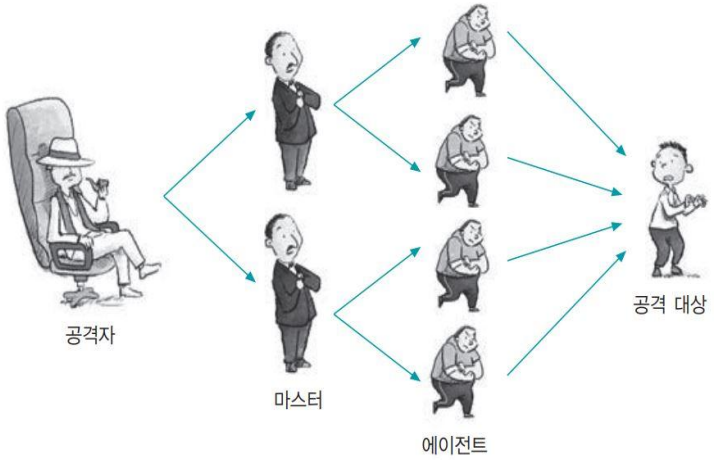
2. 서비스 거부 공격: DoS와 DDoS

분산 서비스 거부 공격(DDoS)

분산 서비스 공격

- 분산 서비스 거부 공격의 기본 구성
  - 구조는 폭력 조직과 비슷하여 공격자를 폭력 조직의 두목, 마스터를 행동대장, 에이전트를 졸개에 비유
  - 과거의 분산 서비스 거부 공격에서는 마스터와 에이전트가 중간자인 동시에 피해자





2. 서비스 거부 공격: DoS와 DDoS

■ 분산 서비스 거부 공격(DDoS)

▪ 분산 서비스 공격

- 최근에 발생하는 분산 서비스 공격 과정

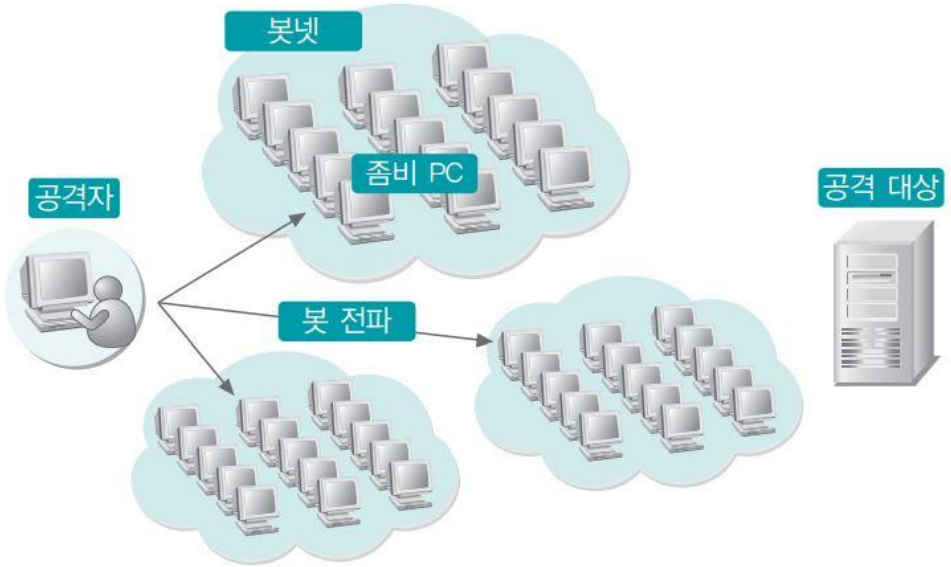
❶ PC에서 전파가 가능한 형태의 악성 코드를 작성

❷ 분산 서비스 거부 공격을 위해 사전에 공격 대상과 스케줄을 정한 뒤 이를 미리 작성한 악성 코드에 코딩

❸ 인터넷을 통해 악성 코드를 전파 (**봇(Bot): 분산 서비스 거부 공격에 사용되는 악성 코드**)

전파 과정에서는 별다른 공격 없이 잠복

악성 코드에 감염된 PC를 좀비 PC라고 하며, 좀비 PC끼리 형성된 네트워크를 봇넷(Botnet)이라고 함



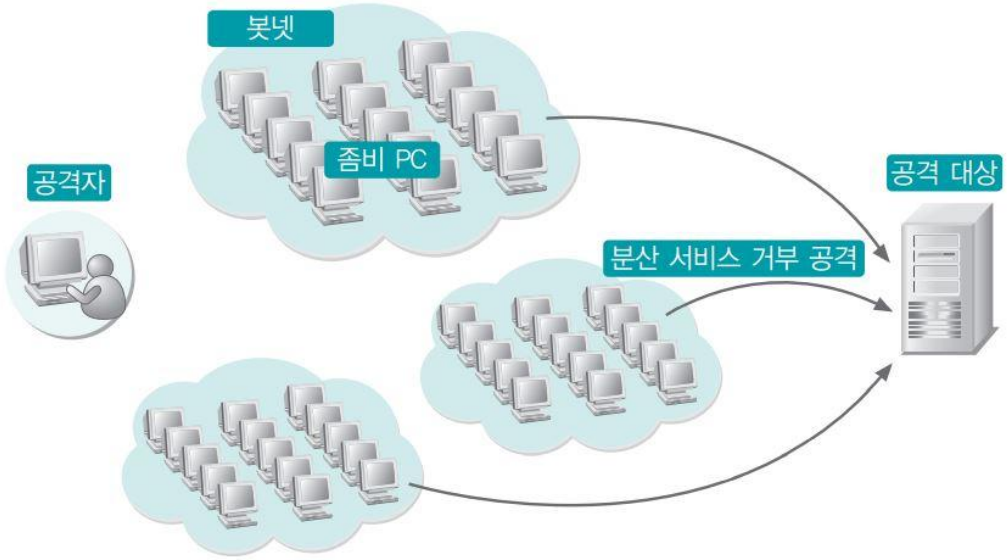
2. 서비스 거부 공격: DoS와 DDoS

■ 분산 서비스 거부 공격(DDoS)

- 분산 서비스 공격
  - 최근에 발생하는 분산 서비스 공격 과정

❹ 공격자가 명령을 내리거나 봇넷을 형성한 좀비 PC들이 정해진 공격 스케줄에 따라 일제히 공격 명령을 수행

이 공격은 HTTP 요청, TCP 연결, UDP 패킷 등 다양한 형태일 수 있음.



3. 스니핑 공격

스니핑(Sniffing) 공격

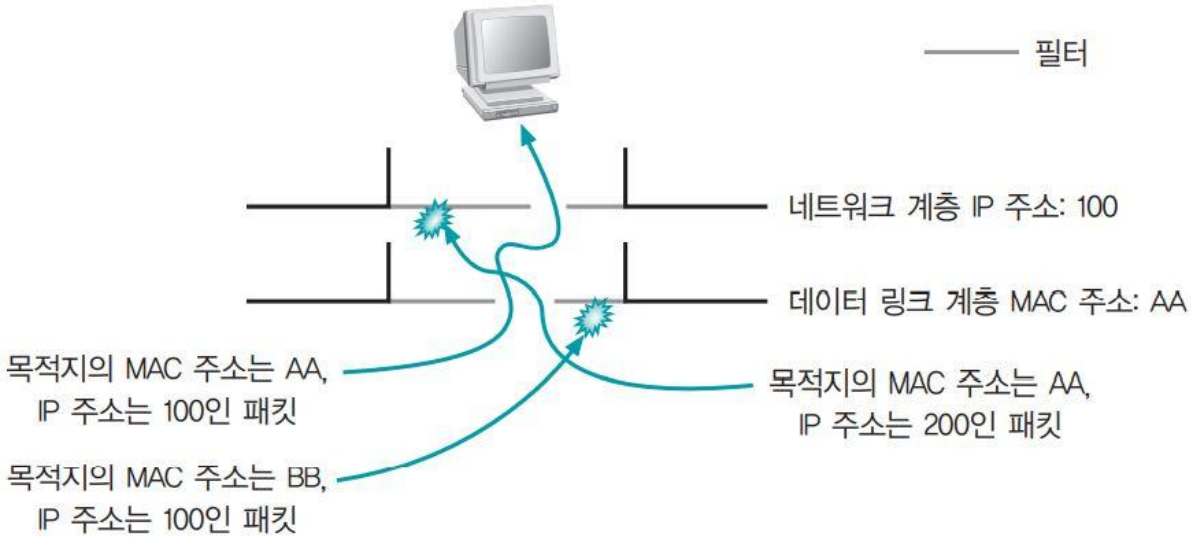
- 스니핑 공격의 개요
  - 코를 킁킁거리면서 음식을 찾는 동물처럼 데이터 속에서 정보를 찾는 것
  - 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문에 수동적 공격이라고도 함
    - 예) 다른 사람의 대화를 엿듣거나 도청하는 행위

3. 스니핑 공격

■ 스니핑 공격

▪ 스니핑 공격의 원리

- 네트워크 카드는 패킷의 IP 주소와 MAC 주소를 인식하고 자신의 버퍼에 저장할지를 결정
- 네트워크 카드에 인식된 데이터 링크 계층과 네트워크 계층의 정보가 자신의 것과 일치하지 않는 패킷은 무시

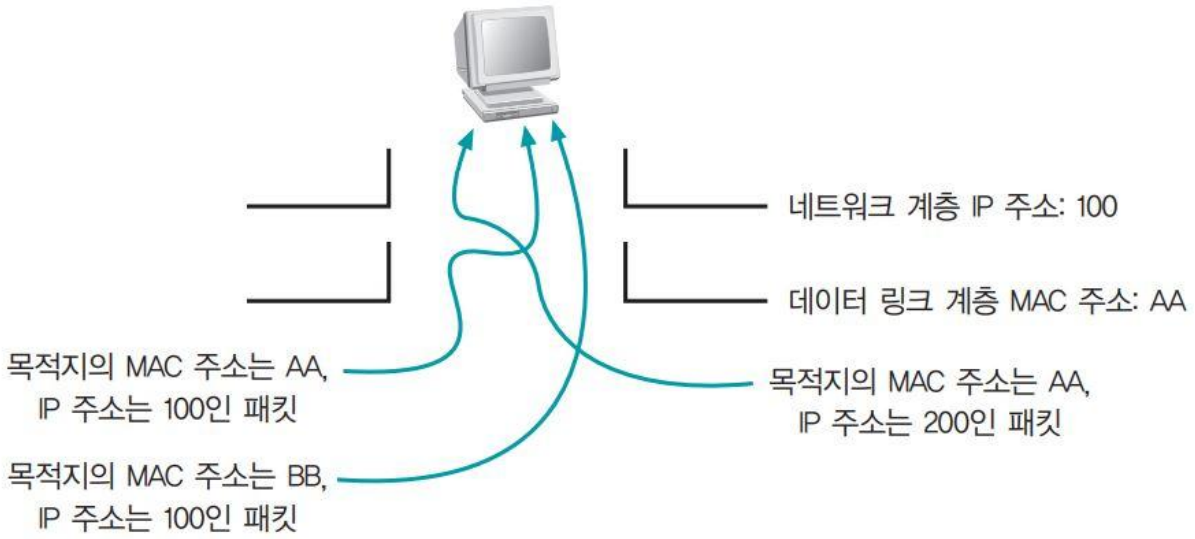


3. 스니핑 공격

스니핑 공격

스니핑 공격의 원리

- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하므로 필터링이 방해됨
- 랜 카드의 설정 사항을 간단히 조정하거나 스니핑을 위한 드라이버를 설치하여 프러미스큐어스 모드로 변경
  - 프러미스큐어스 모드: 데이터 링크 계층과 네트워크 계층의 필터링을 해제하는 랜 카드의 모드

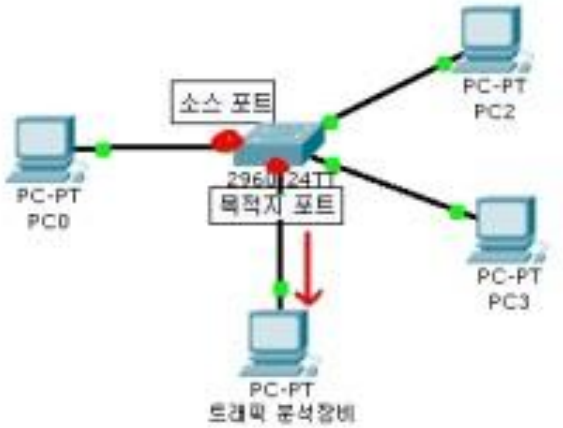


프러미스큐어스 모드 상태에서는 MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨준다.

3. 스니핑 공격

스니핑 공격의 종류

- 스위치 재밍(Switch Jamming) 공격
  - 스위치가 MAC 주소 테이블을 기반으로 패킷을 포트에 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격
  - 랜덤 형태로 생성한 MAC 주소를 가진 패킷을 스위치에 무한대로 보내 MAC 테이블의 저장 용량을 초과시킴.
  - 고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시(운영자 캐시로서 스위치의 관리 및 설정 등)가 독립적으로 나뉘어 있어 통하지 않음
- SPAN 포트 태핑(Port Tapping) 공격 = 포트 로빙
  - SPAN(Switched Port Analyzer)는 스위치의 포트 미러링 기능을 이용한 것
    - 포트 미러링이란 각 포트(스팬 소스 포트)에 전송되는 데이터를 미러링하는 포트(스팬 목적지 포트)에도 똑같이 보내는 것
    - 침입 탐지 시스템을 설치하거나 네트워크 모니터링을 할 때 또는 로그 시스템을 설치할 때 많이 사용
  - SPAN 포트는 기본적으로 네트워크 장비에서 간단한 설정으로 활성화되나, 포트 태핑은 하드웨어 장비(모니터링 장비 등)를 이용
    - 네트워크 분석기: **Wireshark, tcpdump와 같은 소프트웨어를 사용하는 PC 또는 서버.**
    - 전용 하드웨어: 패킷 캡처 및 분석을 위한 전용 장비(예: NetScout, SolarWinds 등).

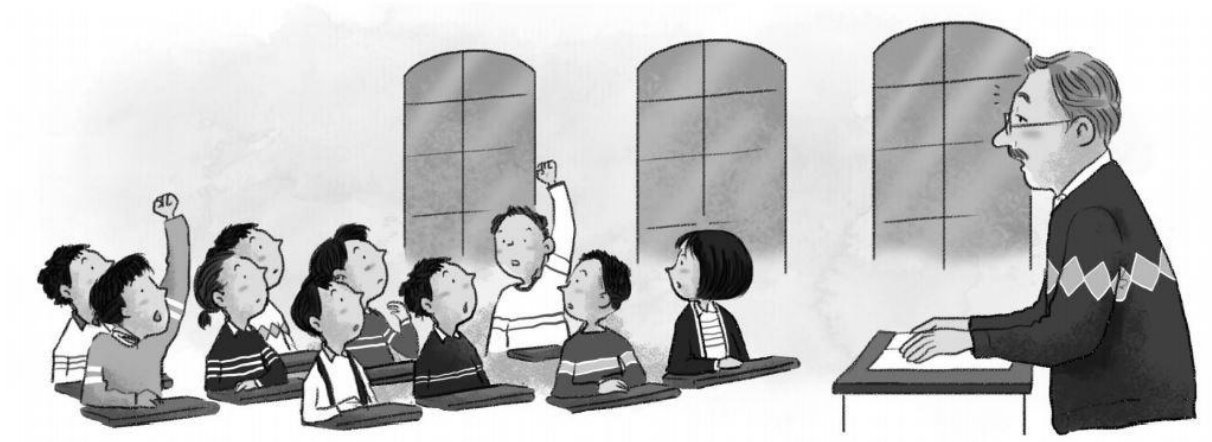


참고: https://m.blog.naver.com/goacts29/50041976755

3. 스니핑 공격

스니핑 공격의 탐지

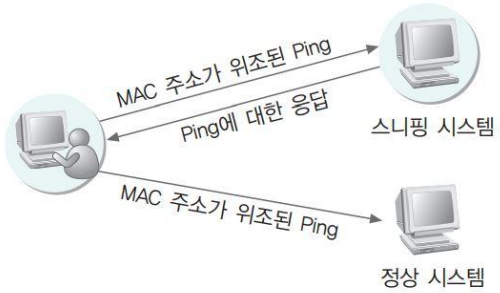
- 스니퍼(Sniffer)를 설치한 이후에는 네트워크에 별다른 이상 현상을 일으키지 않기 때문에 사용자가 인지하기 어려움
- 스니퍼를 쉽게 탐지하려면 스니퍼가 프러미스큐어스 모드에서 작동한다는 점을 이용해야 함
- 스니퍼 탐지의 예시 (강의실에서 교수가 출석을 부를 때)
  - 친구의 출석을 대신 해주기로 한 학생은 자신의 이름이 호명되지 않았는데도 목소리를 바꿔서 대답
  - 두 명이 동시에 대답한다면 프러미스큐어스 모드인 학생은 교수에게 들키게 됨



3. 스니핑 공격

■ 스니핑 공격의 탐지

- ping을 이용한 스니퍼 탐지
  - 대부분의 스니퍼는 일반 TCP/IP에서 동작하기 때문에 request를 받으면 response를 전달
  - 이를 이용하여 의심이 가는 호스트에 ping을 보내면 스니퍼를 탐지할 수 있음.
    - 네트워크에 존재하지 않는 MAC 주소를 위장해서 전송
    - 만약 ICMP echo reply를 받으면 해당 호스트가 스니핑을 하고 있는 것
      - 존재하지 않는 MAC 주소를 사용했으므로 스니핑을 하지 않는 호스트라면 Ping request를 볼 수 없는 것이 정상이기 때문임



- ARP를 이용한 스니퍼 탐지
  - 위조된 ARP request를 보냈을 때 ARP response오면 프러미스큐어스 모드로 설정되어 있는 것
  - 존재하지 않는 IP 주소를 사용했으므로, ARP response를 보낼 수가 없음.

- DNS를 이용한 스니퍼 탐지
  - 일반적인 스니핑 프로그램은 스니핑한 시스템의 IP 주소에 대한 DNS의 이름 해석 과정인 Reverse-DNS lookup을 수행
    - Reverse-DNS lookup: DNS 서버에 요청을 보내어 IP 주소에 대한 도메인 이름을 조회
  - 대상 네트워크로 ping sweep를 보내고 들어오는 네트워크 내의 활성 장치를 식별하고, Reverse-DNS lookup을 감시하면 스니퍼 탐지 가능
    - Ping sweep: 네트워크에서 여러 IP 주소에 대해 동시에 또는 순차적으로 ICMP Echo Request 패킷을 전송하여, 응답이 있는 IP 주소를 확인
    - 감시 방법: DNS 서버 로그, 네트워크 트래픽 모니터링(Wireshark 등), IDS/IPS 시스템 등을 이용한 DNS 트래픽을 모니터링

3. 스니핑 공격

스니핑 공격의 탐지

- 유인을 이용한 스니퍼 탐지
  - 스니핑 공격을 하는 공격자의 주요 목적은 아이디와 패스워드 획득
  - 보안 관리자는 이 점을 이용하여 가짜 아이디와 패스워드를 네트워크에 계속 뿌림
  - 공격자가 이 아이디와 패스워드로 접속을 시도할 때 스니퍼를 탐지

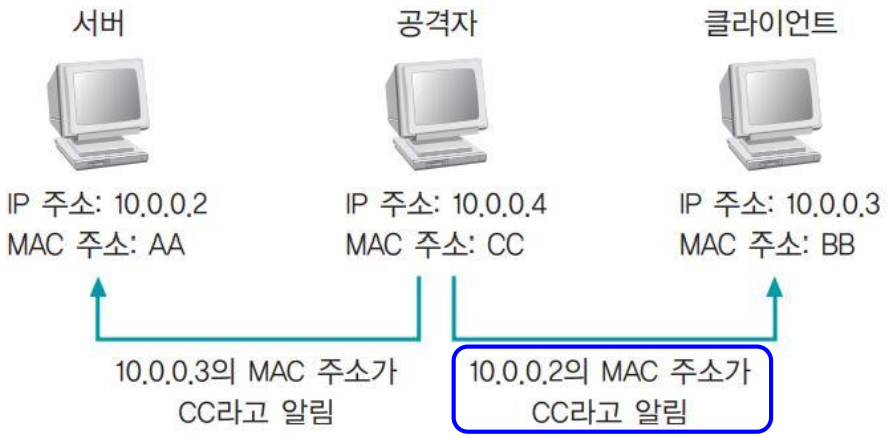
- ARP watch를 이용한 스니퍼 탐지
  - ARP watch: MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 네트워크에서 전송되는 ARP 트래픽을 모니터링하여 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려주는 툴
  - 특정 IP 주소에 대한 MAC 주소가 변경될 때마다 이를 감지
    - 정상적인 네트워크 환경에서는 IP 주소에 대한 MAC 주소가 자주 변경되지 않기 때문에, 이러한 변화는 의심스러운 활동으로 간주

4. 스푸핑 공격

ARP 스푸핑(Spoofing) 공격

- ARP 스푸핑의 개요
  - ARP 스푸핑은 MAC 주소를 속이는 것
    - 로컬에서 통신하는 서버와 클라이언트의 IP 주소에 대한 MAC 주소를 공격자의 MAC 주소로 속임
    - 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡

- ARP 스푸핑 과정



호스트 이름	IP 주소	MAC 주소
서버	10.0.0.2	AA
클라이언트	10.0.0.3	BB
공격자	10.0.0.4	CC

❶ 공격자는 서버의 클라이언트에 10.0.0.2에 해당하는 가짜 MAC 주소 CC를 알리고 서버에는 10.0.0.3에 해당하는 가짜 MAC 주소 CC를 알림

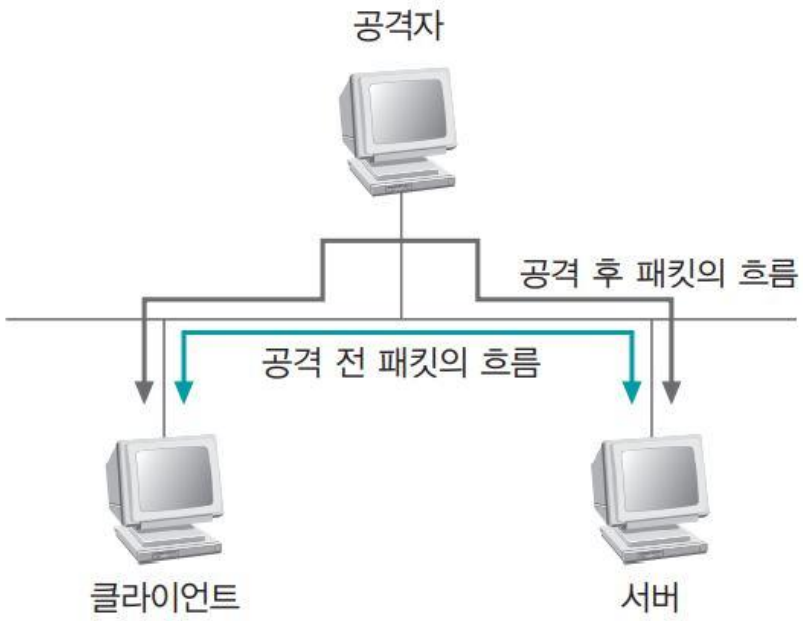
❷ 공격자가 서버와 클라이언트 컴퓨터에 서로 통신하는 상대방을 자기 자신으로 알렸기 때문에 서버와 클라이언트는 각각 공격자에게 패킷을 보냄

❸ 공격자는 서버와 클라이언트로부터 받은 패킷을 읽은 후, 서버가 클라이언트에 보내려던 패킷은 클라이언트에 보내주고 클라이언트가 서버에게 보내려던 패킷은 서버에 보냄

4. 스푸핑 공격

ARP 스푸핑 공격

- ARP 스푸핑 공격 후 패킷의 흐름 변화



4. 스푸핑 공격

ARP 스푸핑 공격

ARP 테이블

- 윈도우에서는 arp -a 명령을 이용하여 현재 인지하고 있는 IP와 해당 IP를 가지고 있는 시스템의 MAC 주소 목록을 확인할 수 있음

arp –a 명령 실행 결과

- 위 예의 클라이언트(10.0.0.3)에서 ARP 스푸핑 공격을 당하기 전에 arp -a 명령을 실행한 결과

```
Internet Address Physical Address Type
10.0.0.2 AA Dynamic
```

- ARP 스푸핑을 당한 후 arp -a 명령을 실행하면 결과가 변경

```
Internet Address Physical Address Type
10.0.0.2 CC Dynamic
```

- APR 스푸핑의 대응책으로 arp –s [IP 주소] [MAC 주소]' 명령으로 MAC 주소 값을 고정

```
arp -s 10.0.0.2 AA
```

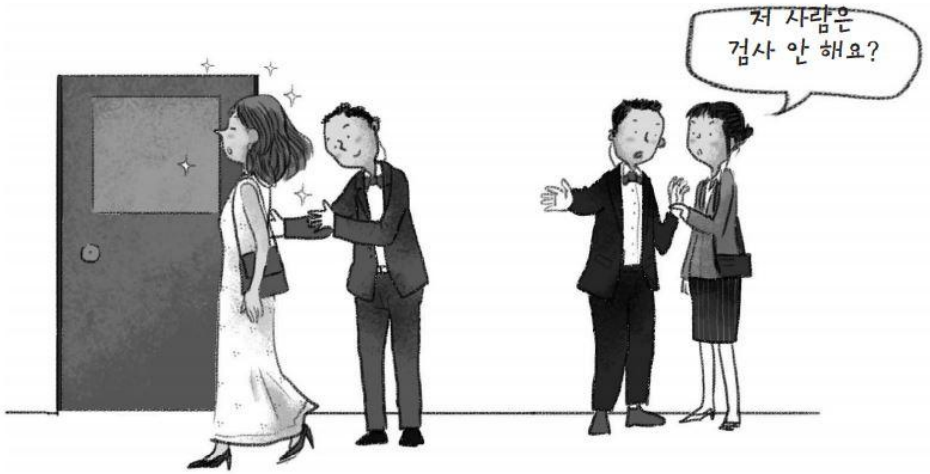
4. 스푸핑 공격

IP 스푸핑 공격

IP 스푸핑의 개요

- 쉽게 말해 IP 주소를 속이는 것으로, 다른 사용자의 IP를 강탈하여 어떤 권한을 획득
- 트러스트를 맺고 있는 서버와 클라이언트를 확인한 후 클라이언트에 서비스 거부 공격을 하여 연결을 끊음
- 클라이언트의 IP 주소를 확보하여 실제 클라이언트처럼 패스워드 없이 서버에 접근

- 트러스트 (신뢰 관계)
  - 클라이언트의 정보를 서버에 미리 기록함
  - 합당한 클라이언트가 서버에 접근하면 아이디와 패스워드의 입력없이 로그인을 허락하는 인증 법
  - 유닉스에서는 주로 트러스트 인증법을 사용하고 윈도우에서는 디렉터리를 사용



4. 스푸핑 공격

IP 스푸핑 공격

IP 스푸핑의 개요

- 트러스트 (신뢰 관계)
  - 트러스트를 설정하려면 유닉스에서는 **/etc/host.equiv** 파일에 클라이언트의 IP와 접속 가능한 아이디를 등록

```
❶ 200.200.200.200 root
❷ 201.201.201.201 +
```

❶ 200.200.200.200에서 root 계정이 로그인을 시도하면 패스워드 없이 로그인을 허락하라는 의미

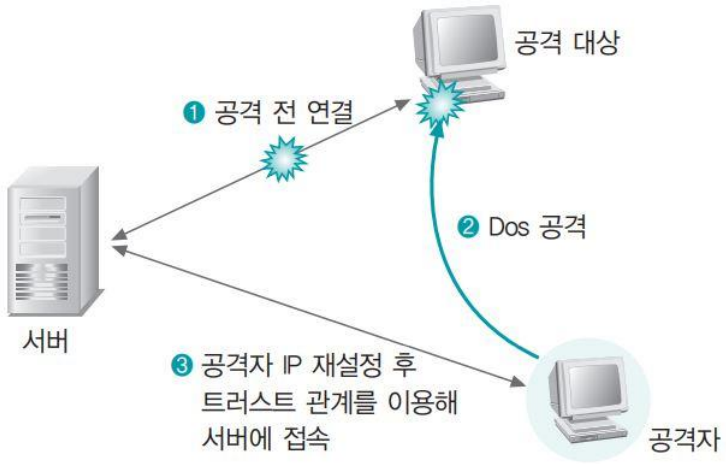
❷ 201.201.201.201에서는 어떤 계정이든 로그인을 허락하라는 것

- + 는 모든 계정을 의미
- ++라고 적힌 행이 있으면 IP와 아이디에 관계없이 모두 로그인을 허용

4. 스푸핑 공격

IP 스푸핑 공격

- IP 스푸핑의 서버 접근
  - 공격자가 해당 IP를 사용하여 접속하면 스니핑으로 패스워드를 알아낼 필요가 없음
    - 공격자는 제로 트러스트로 접속한 클라이언트에 서비스 거부 공격을 수행하여, 작동 불능 상태를 만듬.
      - 따라서 클라이언트의 IP의 네트워크 출연을 불가능 하게 만듬
    - 그 후 공격자 자신이 해당 IP로 설정을 변경한 후 서버에 접속하는 형태로 공격

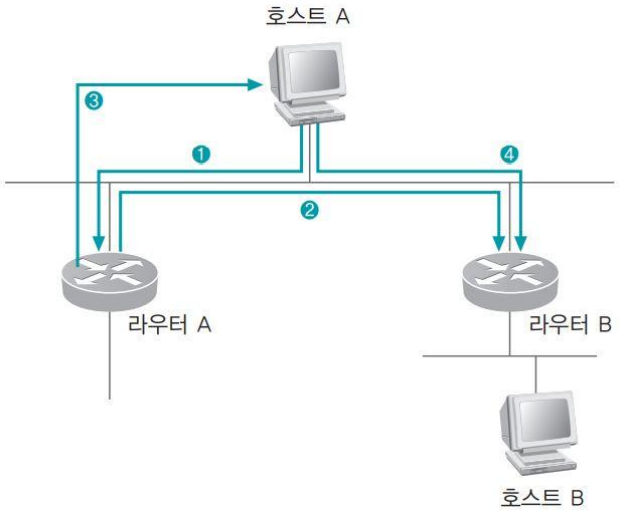


- IP 스푸핑 공격에 대한 대응책은 트러스트를 이용하지 않는 것

4. 스푸핑 공격

ICMP 리다이렉트(Redirect)

- 네트워크 계층에서 스니핑 시스템을 네트워크에 존재하는 또 다른 라우터라고 알려 패킷의 흐름을 바꾸는 공격
- ICMP 리다이렉트의 동작



❶ 호스트 A에 라우터 A가 기본으로 설정되어 있기 때문에 호스트 A가 원격의 호스트 B로 데이터를 보낼 때 패킷을 라우터 A로 전송

❷ 라우터 A는 호스트 B로 보내는 패킷을 수신, 그 후 라우팅 테이블을 검색하여 호스트 A가 자신보다 라우터 B를 이용하는 것이 더 효율적이라고 판단하여 해당 패킷을 라우터 B로 전송

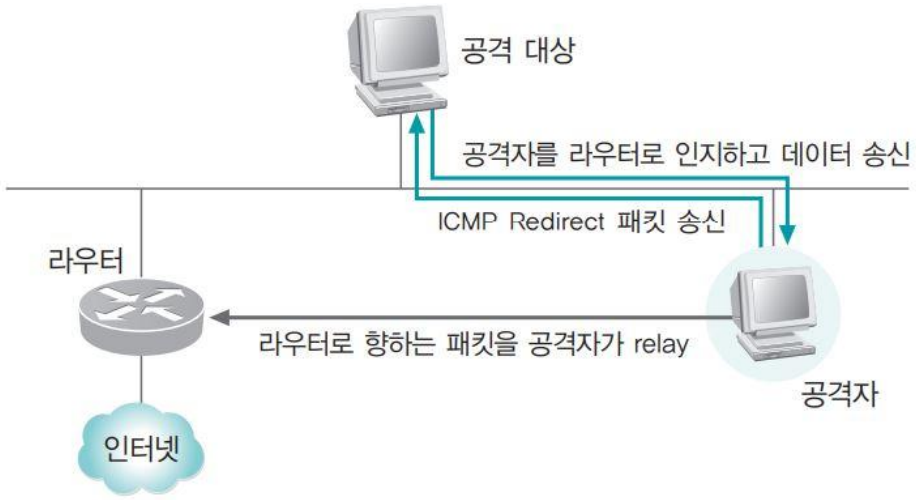
❸ 라우터 A는 호스트 B로 향하는 패킷을 호스트 A가 자신에게 다시 전달하지 않도록, 호스트 A에 **ICMP 리다이렉트 패킷**을 보내어 호스트 A가 호스트 B로 보내는 패킷이 라우터 B로 바로 향하게 함

❹ 호스트 A는 라우팅 테이블에 호스트 B에 대한 값을 추가하고 호스트 B로 보내는 패킷은 라우터 B로 전달

4. 스푸핑 공격

ICMP 리다이렉트

- ICMP 리다이렉트를 이용해 공격하면 공격자가 라우터 B가 됨
- ICMP 리다이렉트 패킷을 공격 대상에게 보낸 후 라우터 A에 다시 연결하면 모든 패킷을 스니핑할 수 있음
- ICMP 리다이렉트는 데이터 링크 계층의 공격이 아니기 때문에 잘 응용하면 로컬의 랜이 아니라도 공격이 가능

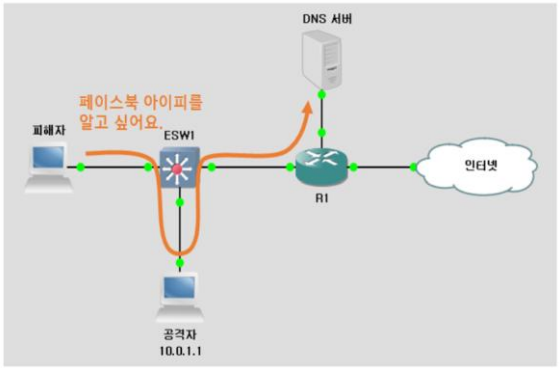


4. 스푸핑 공격

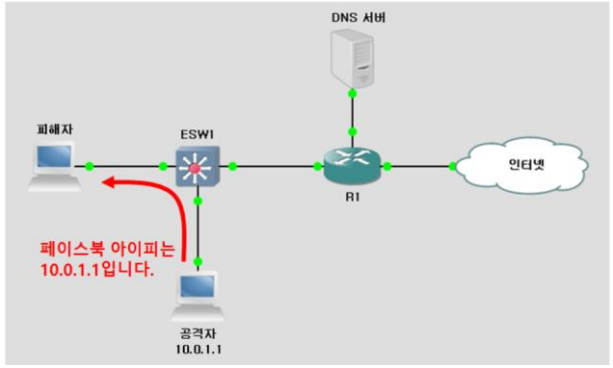
DNS 스푸핑 공격

- DNS 스푸핑
  - **실제 DNS 서버보다 빨리 공격 대상에게 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격**
    - 인터넷 익스플로러에 사이트 주소를 입력하고 Enter를 눌렀을 때 쇼핑몰이나 포르노 사이트가 뜨는 경우
  - DoS 공격이 되지만 이를 조금만 응용하면 웹 스푸핑이 됨
    - ① 자신의 웹 서버를 하나 만들고 공격 대상이 자주 가는 사이트를 하나 골라서 웹 크롤러를 이용해 해당 사이트를 긁어 옴
    - ② 아이디와 패스워드를 입력 받아 공격 사이트로 전달해주는 스크립트를 프로그래밍 함
    - ③ 공격 대상은 사이트 주소를 입력하고, 접속하던 사이트와 동일한 것을 보고 당연히 정상적으로 접속했다고 생각
    - ④ 자신의 아이디와 패스워드를 입력하여 해킹 당함

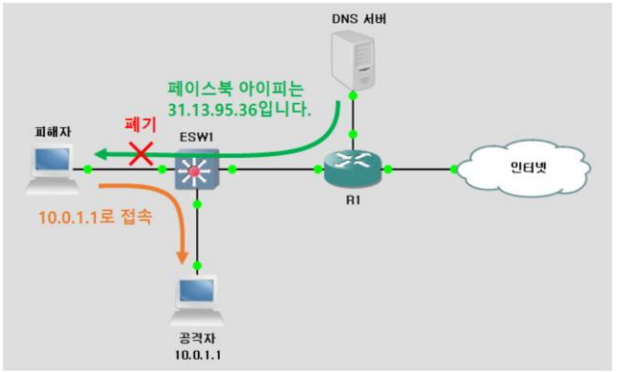
참고: https://blog.naver.com/kimdj217/221334628205



ARP 공격을 한 상황



DNS response

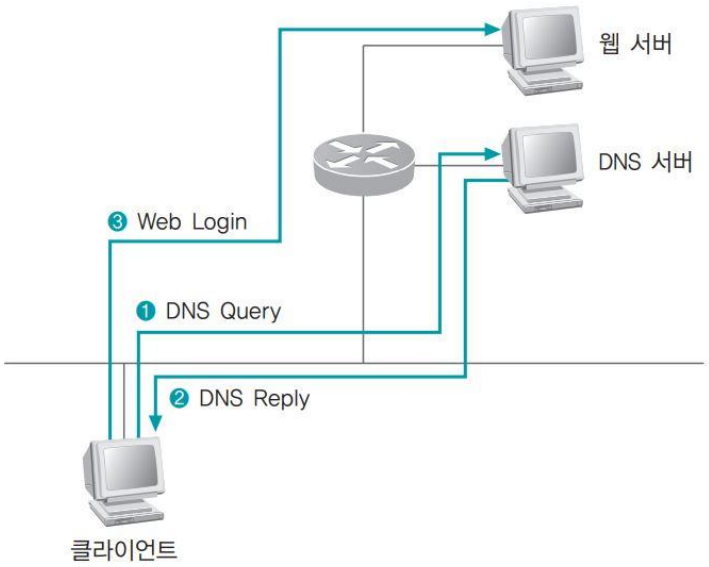


공격자 시스템으로 접속

4. 스푸핑 공격

DNS 스푸핑 공격

- 정상적인 DNS 스푸핑



❶ 클라이언트가 DNS 서버에 접속하고자 하는 IP 주소(www.wishfree.com과 같은 도메인 이름)를 물어봄
이 때 보내는 패킷은 DNS query

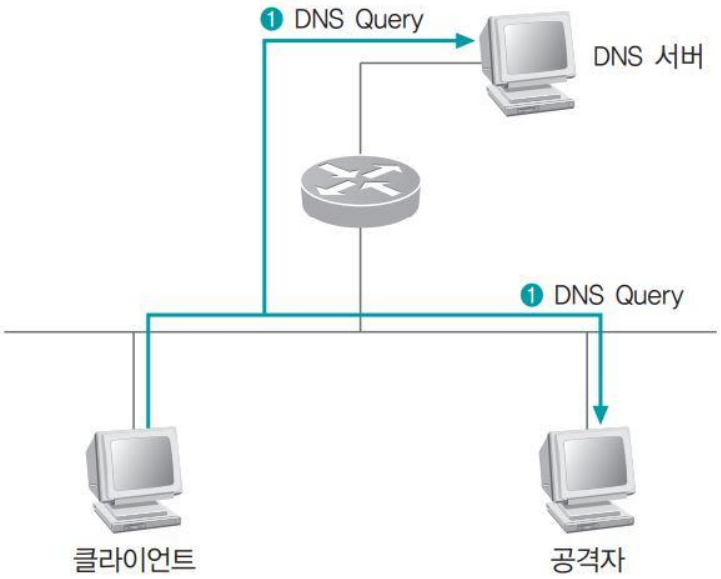
❷ DNS 서버가 해당 도메인 이름에 대한 IP 주소를 클라이언트에 전송.

❸ 클라이언트가 받은 IP 주소를 바탕으로 웹 서버를 찾아 감

4. 스푸핑 공격

DNS 스푸핑 공격

- DNS 스푸핑 공격: DNS Query



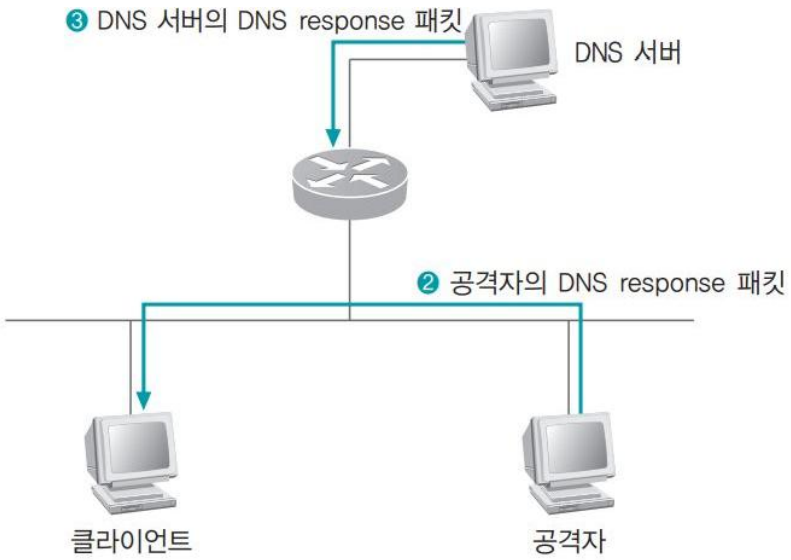
❶ 공격자는 클라이언트가 DNS 서버로 DNS query 패킷을 보내는 것을 확인

스위칭 환경인 경우에는 클라이언트가 DNS query 패킷을 보내면 이를 받아야 하므로 ARP 스푸핑과 같은 선행 작업이 필요. 만약 허브를 쓰고 있다면 모든 패킷이 자신에게도 전달되므로 클라이언트가 DNS query 패킷을 보내는 것을 자연스럽게 확인할 수 있음

4. 스푸핑 공격

DNS 스푸핑 공격

- DNS 스푸핑 공격: 공격자와 DNS 서버의 DNS response



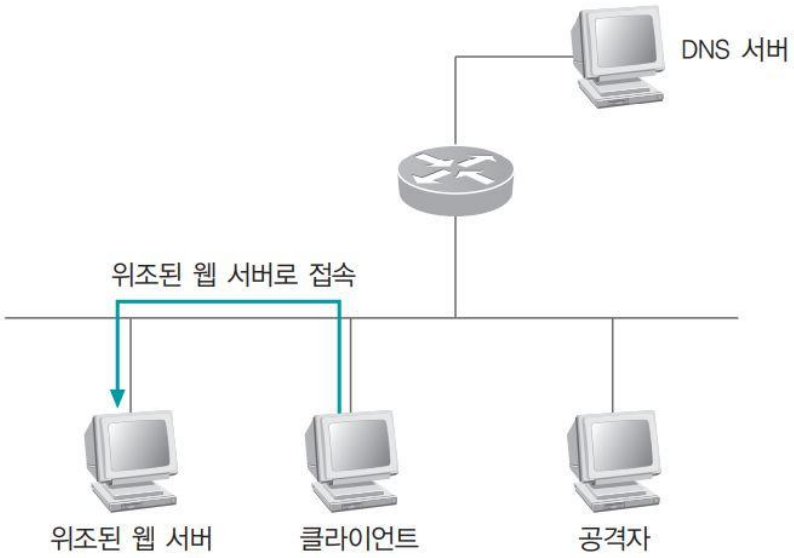
❷ 공격자는 로컬에 존재하므로 지리적으로 DNS 서버보다 가까우므로 DNS 서버가 올바른 DNS response 패킷을 보내주기 전에 클라이언트에 위조된 DNS response 패킷을 보낼 수 있음.

❸ 클라이언트는 공격자가 보낸 DNS response 패킷을 올바른 패킷으로 인식하고 웹에 접속함. 지리적으로 멀리 떨어진 DNS 서버가 보낸 DNS response 패킷은 버림

4. 스푸핑 공격

DNS 스푸핑 공격

- DNS 스푸핑 공격: 위조된 웹 서버로 접속하는 클라이언트
  - DNS 스푸핑 공격은 반드시 대상을 기다리고 있다가 공격을 수행해야 하는 것은 아님
  - 네트워크의 특정 URL에 거짓 IP 정보를 계속 브로드캐스팅하면 해당 패킷을 받은 클라이언트는 잘못된 IP로 들어감



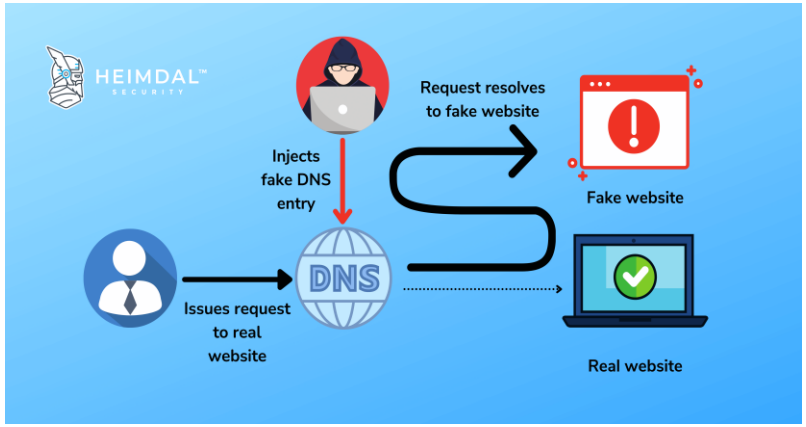
4. 스푸핑 공격

DNS 스푸핑 공격

- DNS 스푸핑 공격 대응책
  - DNS 스푸핑 공격을 막으려면 중요 서버에 대해 DNS query를 보내지 않으면 됨
    - 먼저 시스템 메모리의 정보를 확인하고 그 다음 hosts 파일에 등록된 정보를 확인
    - hosts 파일에는 URL과 IP 정보가 등록

```
127.0.0.1 localhost
200.200.200.123 www.wishfree.com
201.202.203.204 www.sysweaver.com
```

  - 중요 접속 서버의 URL에 대한 IP 를 hosts 파일에 등록해놓으면 되지만 하지만 모든 서버의 IP를 등록하는 것은 무리이므로 모든 서버에 대한 DNS 스푸핑을 막기는 어려움

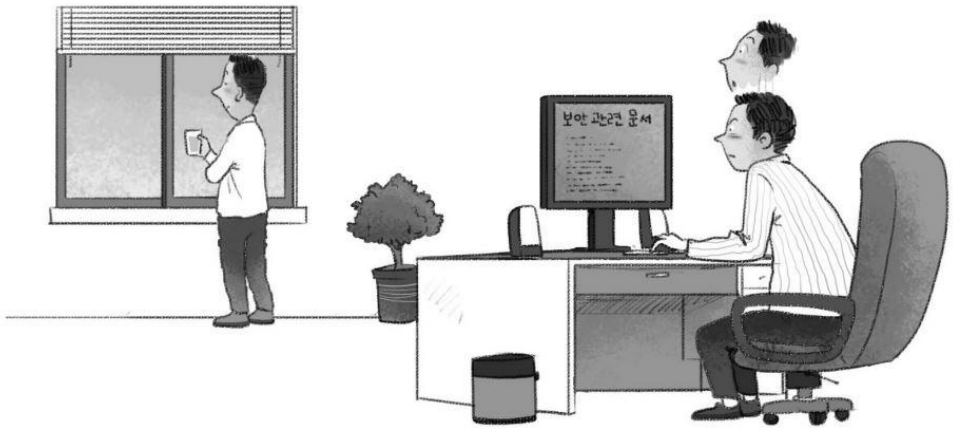


참고: https://heimdalsecurity.com/

5. 세션 하이재킹 공격

세션 하이재킹(Session Hijacking) 공격

- 세션 하이재킹 공격의 개요
  - 1995년에 케빈 미트닉이 시스템 관리자인 시모무라 쓰토무의 컴퓨터를 공격한 기술
  - 말 그대로 '세션 가로채기'를 의미
    - 세션: '사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태'
    - 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로채는 것
    - 가장 쉬운 세션 하이재킹은 누군가 작업을 하다가 잠시 자리를 비웠을 때 몰래 PC를 사용하여 원하는 작업을 하는 것
  - TCP 세션 하이재킹의 경우 공격자가 원하는 접속만 공격대상이 생성하면 네트워크 공격으로 세션을 빼앗을 수 있음



5. 세션 하이재킹 공격

세션 하이재킹 공격

- 공격자가 원하는 접속만 공격 대상이 생성하면 네트워크 공격으로 세션을 빼앗을 수 있음
- TCP 세션 하이재킹의 기본적인 단계
  - ① 클라이언트와 서버 사이의 패킷을 통제 : ARP 스푸핑 등을 통해 클라이언트와 서버 사이의 통신 패킷이 전부 공격자를 지나가게 함
  - ② 서버에 클라이언트 주소로 연결을 재설정하기 위한 RSTreset 패킷을 보냄: 서버는 패킷을 받아 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고 다시 TCP 3-웨이 핸드셰이킹을 수행
  - ③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음
- 예방 방법
  - MAC 주소를 고정하는 방법은 ARP 스푸핑을 막아주기 때문에 결과적으로 세션 하이재킹을 막을 수 있음
  - SSH와 같은 인증 수준이 높은 프로콜을 이용하여 서버에 접속해야 함