이 경 호 / 김 현 진 / 여 승 철

# ARP 스푸핑 진단 프로그램

# CONTENTS

## 1) ARP(Address Resolution Protocal)란?

어떤 장치의 IP 주소를 이용해서 그 장치의 MAC 주소를 얻는 데 사용하는 프로토콜.

'Request' 기능 : 특정 IP 주소에 대응되는 MAC 주소가 무엇인지 조회하는 용도로 사용

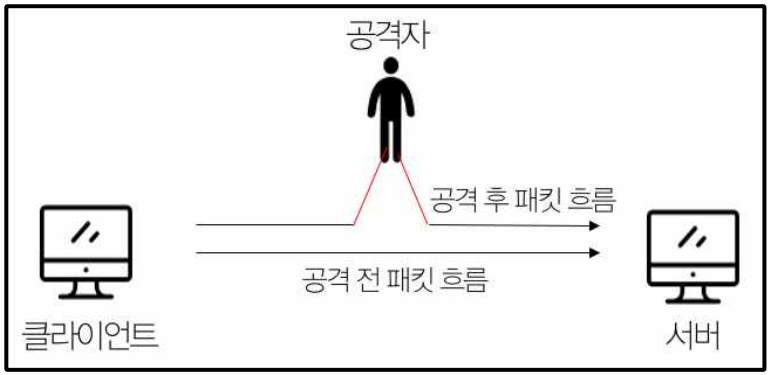
브로드캐스트로 전달되어 동일한 네트워크에 존재하는 모든 장치가

해당 메시지 확인가능

'Reply' 기능 : ARP Request 에 대응되는 장치가 송신자에게 자신의 MAC 주소

정보를 전달하는 메시지이며, Request와는 다르게 유니캐스트로 전달

## 2) ARP 스푸핑이란?




**" 스푸핑 " 이란 속임을 이용한 공격 으로**

**클라이언트의 IP 에 대한 MAC 주소를 공격자의 MAC 주소로 속여서**

**클라이언트에서 서버로 가는 패킷이나, 서버에서 클라이언트로 가는**

**패킷이 공격자에게 향하는 중간자 공격 기법.**

ARP에 Reply 패킷으로 받은 MAC 주소가 진짜인지 아닌지를 검증하는 인증 시스템이 없다는 취약점을 이용한 공격!

## 3) ARP 스푸핑 대표적인 증상

1, 특정 시스템의 ARP 트래픽 증가

2, 네트워크 속도 저하 (종단간의 통신을 가로채어 재전송하는 시스템 때문)

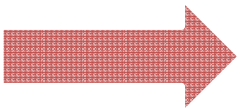
3, ARP 테이블에서 실제 게이트웨이와 동일한 MAC 주소를 사용하는 다른 시스템이 발견될 수 있음

4, promiscuous 모드 상태이다.

# 역할분담

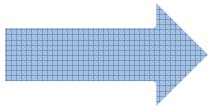
이경호 : MAC 주소의 중복 찾아내기

여승철 : Promiscuous 상태 확인하기



ARP 스푸핑 진단

김현진 : 진단된 ARP 스푸핑 MAC 주소 정적으로 설정하기



ARP 스푸핑 방어

# 1) MAC (media access Control) 주소란?

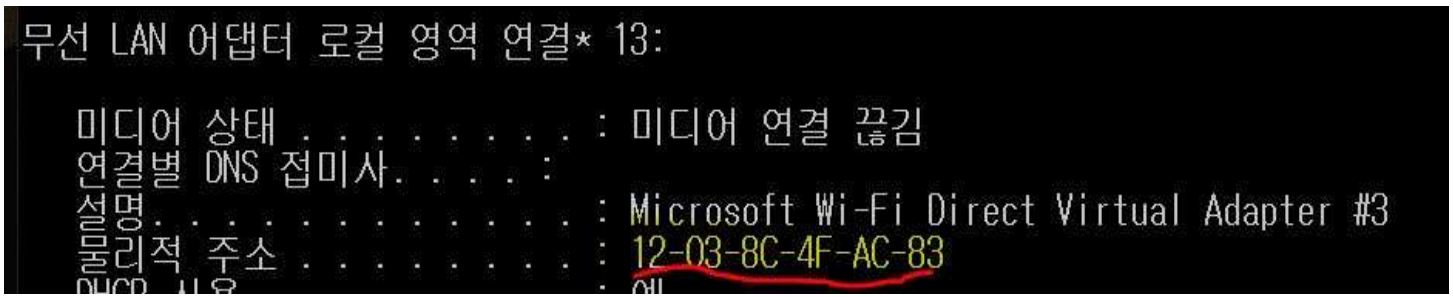
**데이터링크 계층에서 사용하는 네트워크로**

**인터페이스에서 할당된 고유 식별자로 네트워크상에서 "주민등록번호"라고 불린다.**

**총 48비트(6바이트)로 구성되어 있고 8비트(1바이트)단위로 끊어서**

**총 6개의 자리로 구분한다.**

ipconfig/all 명령어 사용



## 2) MAC 주소 통신

Unicast : 목적지 주소를 하나만 적어서 특정한 PC에게만 보내는 방식

1대1 통신 / MAC주소의 첫번째 bit(LSB - 최하위 bit) 가 0인 경우

Multicast : 도메인 안에 있는 모든 PC 들에게 한번에 전송하는 방식

MAC 주소의 첫번째 bit 가 1인 경우

Broadcast : MAC 주소의 모든 bit 가 1인 경우를 말한다.

## 1) Promiscuous Mode 란?

일반적으로 NIC (Network Interface Card)는 자신의 것이 아닌 다른 MAC 주소로 보내진 ethernet frame 을 확인하지 않고 폐기하게 된다.

그러나 다른 호스트의 주소로 전송되는 ethernet frame 을 폐기하지 않고 상위계층으로 전달하는 모드를 Promiscuous 모드라고 한다.

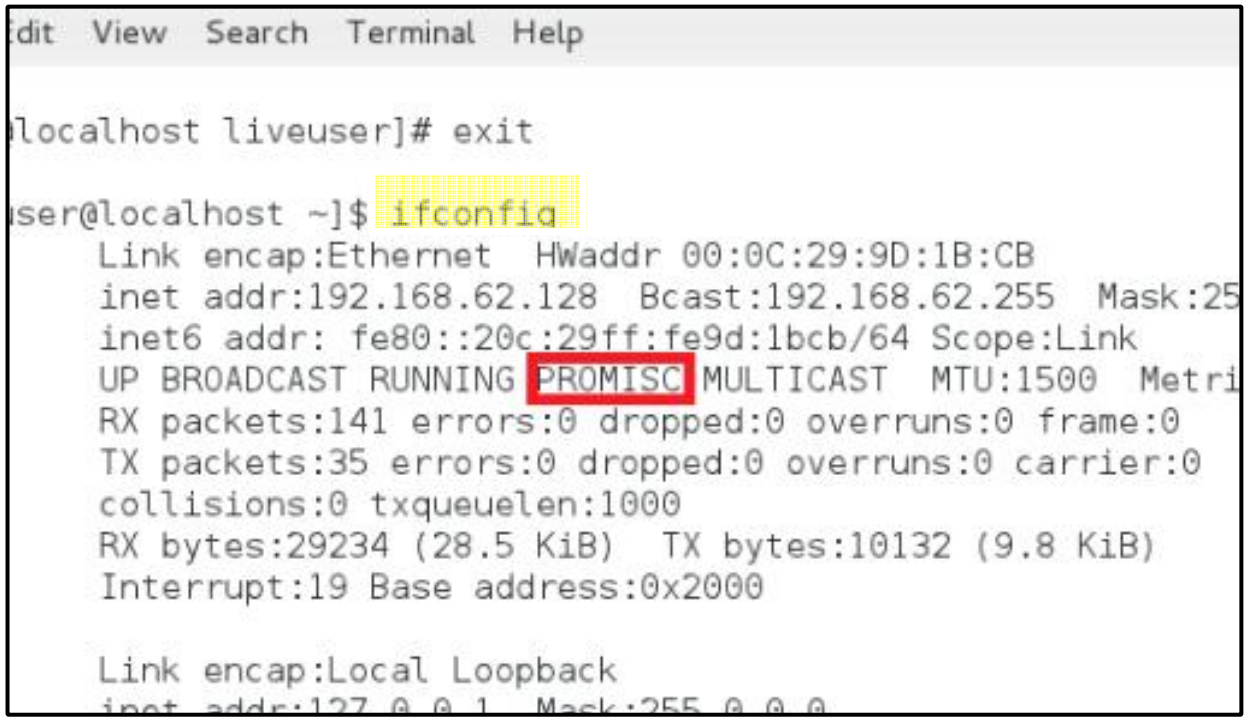
## 2) Promiscuous Mode인지 점검해야 하는 이유는 ?

Promiscuous Mode 가 실행되어 있으면 스니핑 툴이 몰래 설치 되어있을 수 있으므로 해제하는 것이 좋다.

또한 공격자 입장에서 피해자의 NIC 이 Promiscuous Mode 라면 스니핑/스푸핑 공격이 훨씬 수월해 질 수 있다.

03

# Promiscuous Mode인지 확인하는 방법

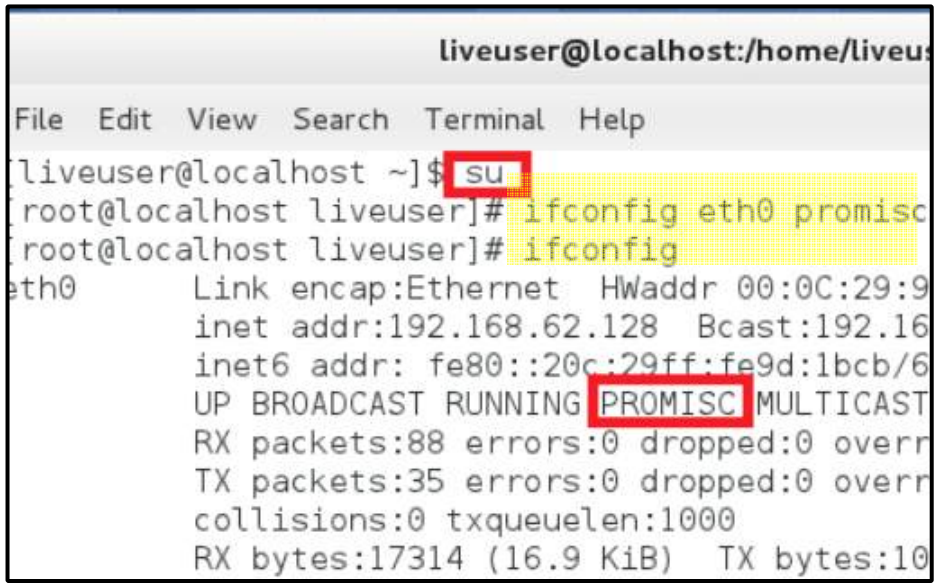



ifconfig 명령어 사용

03

# Promiscuous Mode 설정/해제 하는법

※root권한인 상태여야 확인 할 수 있다. (su명령어)




ifconfig eth0 promisc 명령어로 설정
ifconfig eth0 –promisc명령어로 설정을 해제

**su (switch user) 명령어**
현재 계정을 로그아웃없이 다른 권한으로 로그인 할 수 있는 명령어

## 1) ARP 스푸핑을 방지 할 수 있는 방법은 . . .

1, ARP 테이블에서 게이트웨이 주소를 정적으로 설정하여 MAC 주소가 변환되지 않도록 설정하는 방법

(재부팅시 초기화 되므로 설정을 반복해줘야하는 번거로움이 있음)

2, 스푸핑이 진단 된 네트워크를 끊는 방법

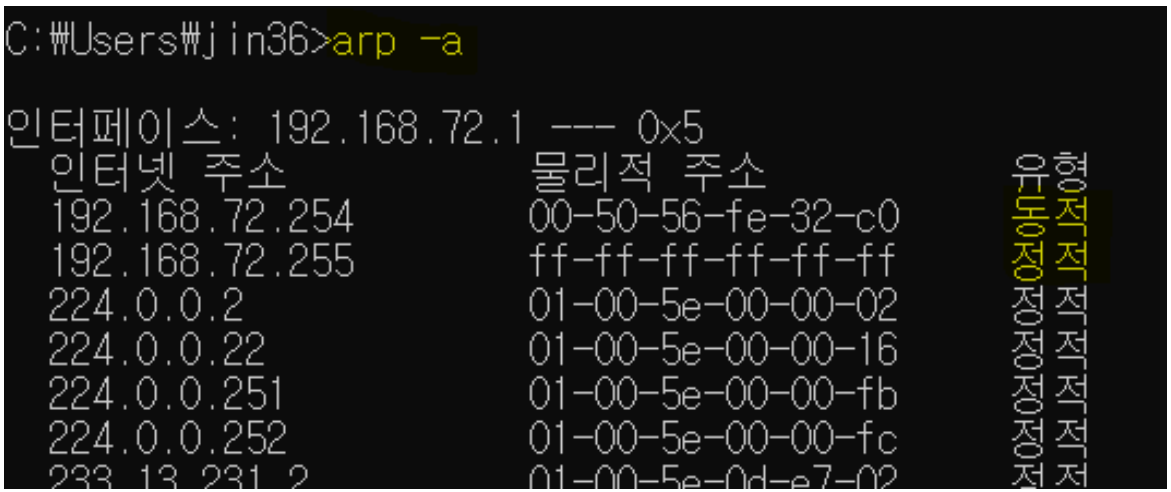
## ARP 테이블을 정적으로 설정하기

### < ARP 테이블 명령어 >

arp -a : IP 주소, MAC 주소, 정적인지 동적인지 유형을 볼 수 있음

arp -s IP 주소 MAC 주소 : 입력하여 정적으로 MAC 주소를 설정할 수 있음

arp -D (IP 주소) : P 주소 입력시 IP 주소 리스트 삭제 , * 적으면 전체 삭제




arp -a 명령어 입력한 상태

arp의 유형을 확인 할 수 있다.

## ARP 테이블을 정적으로 설정하기

< ARP 테이블 명령어 >

arp -a : IP 주소, MAC 주소, 정적인지 동적인지 유형을 볼 수 있음

arp -s IP 주소 MAC 주소 : 입력하여 정적으로 MAC 주소를 설정할 수 있음

arp -D (IP 주소) : P 주소 입력시 IP 주소 리스트 삭제 , * 적으면 전체 삭제

```
C:₩>arp -s 192.168.100.123 FF-FF-FF-FF-FF-FF

C:₩>arp -a

Interface: 192.168.100.222 --- 0x2
  Internet Address      Physical Address      Type
  192.168.100.50        00-40-ca-c4-40-ed     dynamic
  192.168.100.123       ff-ff-ff-ff-ff-ff     static
  192.168.100.254       00-10-5a-84-49-bd     dynamic
```

⇨ arp -s 명령어 입력한 상태

⇨ arp가 정적으로 설정되었다.

# THANK YOU