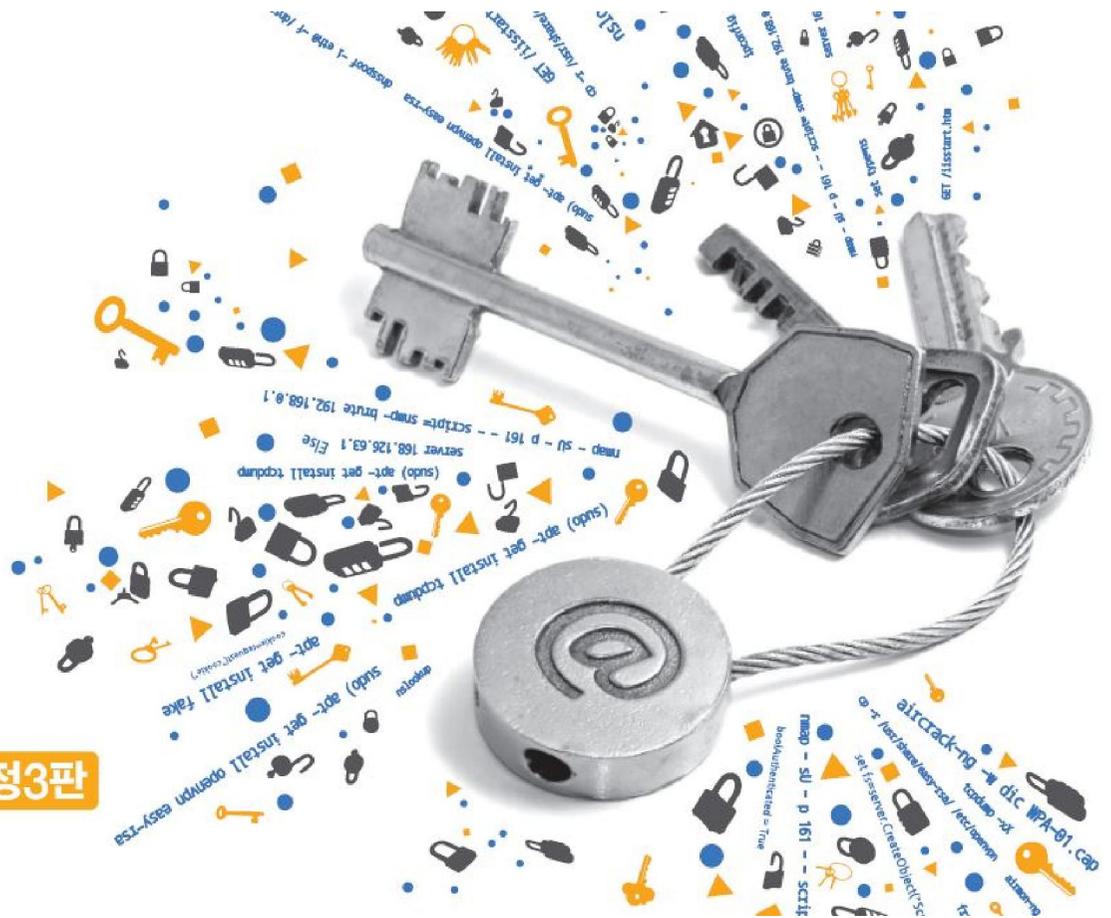




# 네트워크 해킹과 보안

정보 보안 개론과 실습

개정3판



## Chapter 06 스니핑

# 목차

- 01 스니핑 공격
- 02 스니핑 공격 툴
- 03 스니핑 환경에서의 스니핑
- 04 스니핑 공격의 대응책

# 학습목표

- 스니핑 공격을 이해하고 다양한 공격 툴을 실행할 수 있다.
- 스위칭 환경에서의 스니핑 공격을 이해하고 실행할 수 있다.
- 스니핑 공격에 대한 적절한 대책을 세울 수 있다.

# 1. 스니핑 공격

## 1.1 스니핑에 대한 이해

### ■ 스니핑

- sniff의 사전적 의미 : 코를 킁킁거리다
- 수동적(Passive) 공격 : 공격할 때 아무것도 하지 않아도 충분하기 때문

### ■ 스니핑의 개념

- 도청(Eavesdropping)과 엿듣기가 스니핑
- 전화선이나 UTP에 탭핑(Tapping)해서 전기 신호를 분석하여 정보를 찾아냄.
- 전기 신호(Emanation)을 템페스트(Tempest) 장비를 이용해 분석하는 일

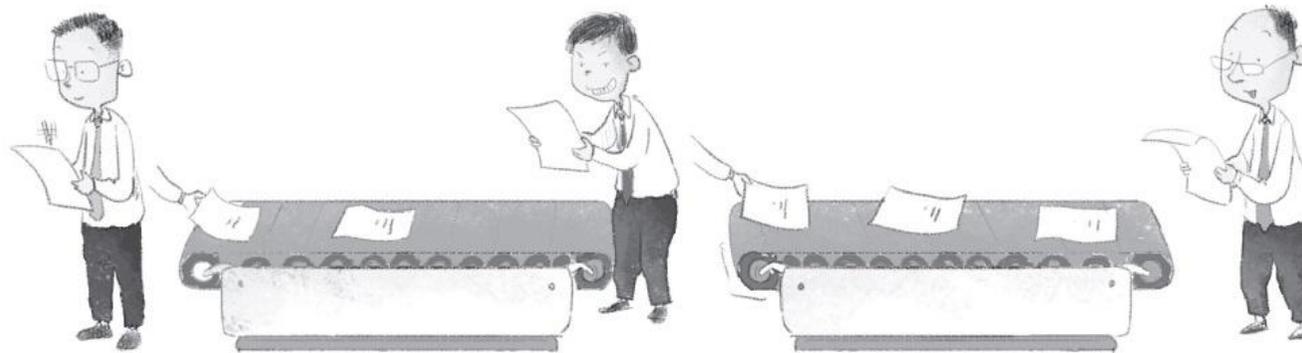


그림 6-1 스니핑의 개념

# 1. 스니핑 공격

## 1.1 스니핑에 대한 이해

---

### ■ 프러미스큐어스 모드(Promiscuous Mode)

- MAC 주소와 IP 주소에 관계없이 모든 패킷을 스니퍼에게 넘겨주는 것
- 리눅스나 유닉스 등의 운영체제에서는 랜 카드에 대한 모드 설정이 가능
- 윈도우에서는 스니핑을 위한 드라이버를 따로 설치
- 스니핑을 하려면 좋은 랜 카드가 필요

### ■ 바이패스 모드(Bypass Mode)

- 패킷에 대한 분석까지 하드웨어로 구현되어 있는 랜 카드
- 기가바이트(GByte) 단위의 백본 망에서 스니핑을 하기 위한 장비로 고가임.

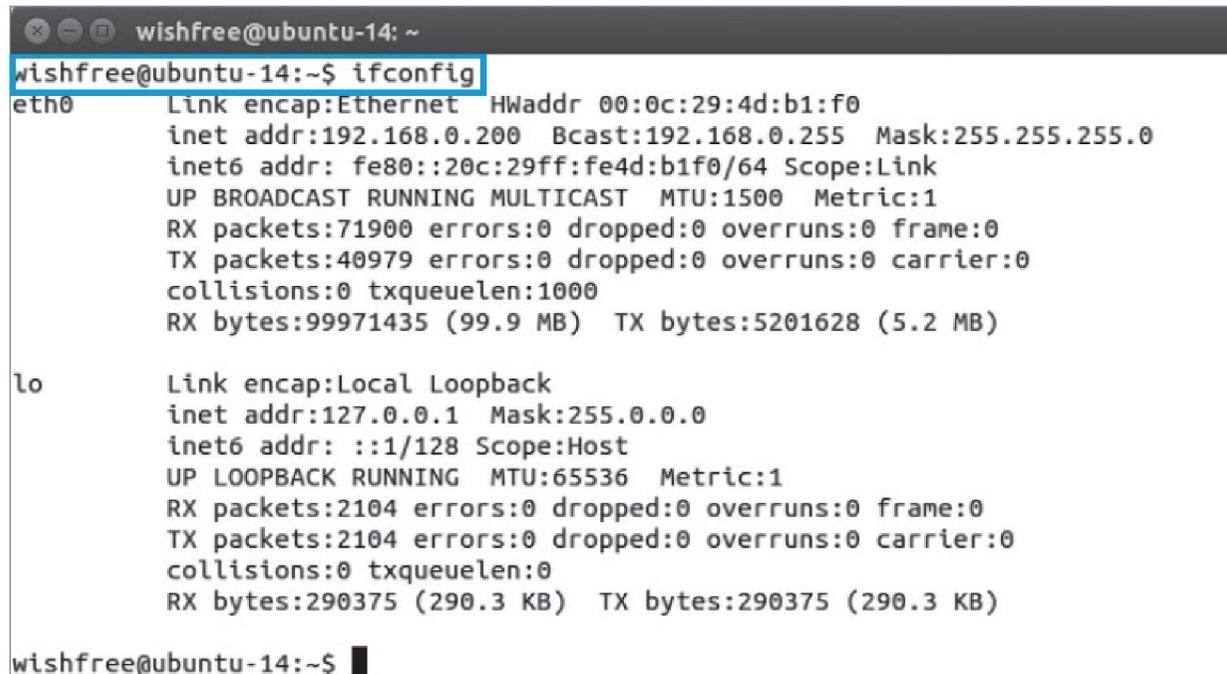
# 1. 스니핑 공격

## 실습 6-1 프리미엄스큐어스 모드 설정하기

실습환경 · 공격자 시스템 : 우분투 데스크탑 14

### ① 랜 카드 확인하기

ifconfig



```
wishfree@ubuntu-14: ~  
wishfree@ubuntu-14:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4d:b1:f0  
          inet addr:192.168.0.200  Bcast:192.168.0.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fe4d:b1f0/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:71900 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:40979 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:99971435 (99.9 MB)  TX bytes:5201628 (5.2 MB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:65536  Metric:1  
          RX packets:2104 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2104 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:290375 (290.3 KB)  TX bytes:290375 (290.3 KB)  
  
wishfree@ubuntu-14:~$
```

그림 6-2 네트워크 인터페이스 확인하기

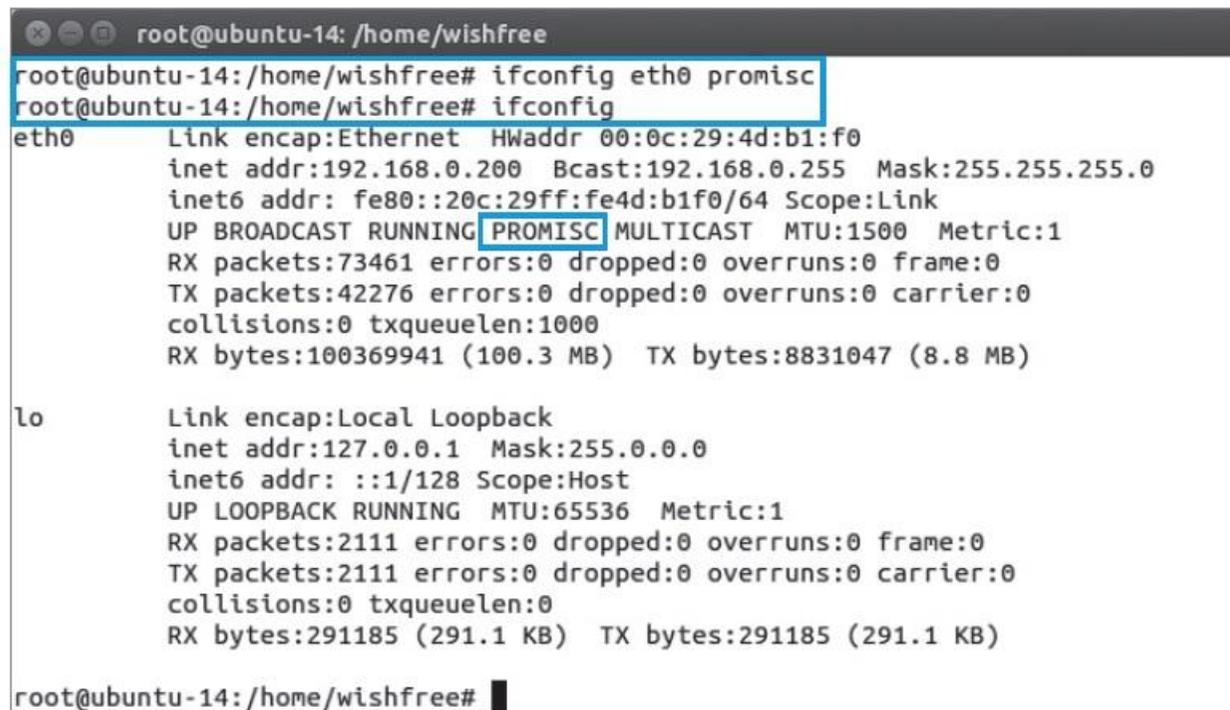
# 1. 스니핑 공격

## 실습 6-1 프러미스큐어스 모드 설정하기

### ② 프러미스큐어스 모드로 변경하기

```
ifconfig eth0 promisc
```

```
ifconfig
```



```
root@ubuntu-14: /home/wishfree
root@ubuntu-14:/home/wishfree# ifconfig eth0 promisc
root@ubuntu-14:/home/wishfree# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4d:b1:f0
          inet addr:192.168.0.200  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4d:b1f0/64 Scope:Link
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:73461 errors:0 dropped:0 overruns:0 frame:0
          TX packets:42276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:100369941 (100.3 MB)  TX bytes:8831047 (8.8 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:2111 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2111 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:291185 (291.1 KB)  TX bytes:291185 (291.1 KB)

root@ubuntu-14:/home/wishfree#
```

그림 6-3 프러미스큐어스 모드를 설정하고 확인하기

## 2. 스니핑 공격 툴

### 2.1 TCP Dump

---

#### ■ TCP Dump

- 리눅스에서 가장 기본이 되는, 하지만 강력한 스니핑 툴
- 처음에는 네트워크 관리를 위해 개발되었기 때문에 관리자 느낌이 강함.
- TCP Dump로 획득한 증거 자료는 법적 효력이 있음.

## 2. 스니핑 공격 툴

### 실습 6-2 TCP Dump로 계정과 패스워드 스니핑하기

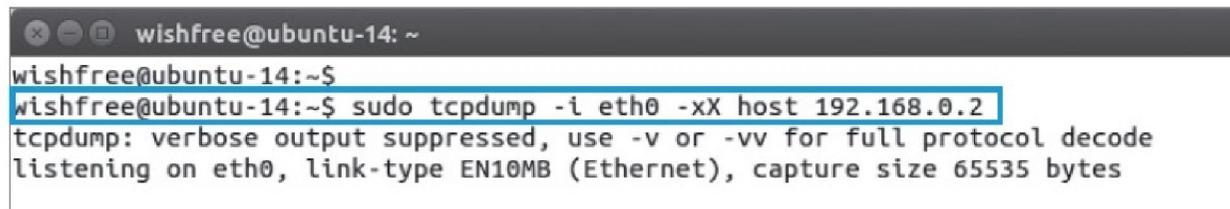
- 실습환경**
- 클라이언트 시스템 : 우분투 데스크탑 14
  - 텔넷 서버 시스템 : 우분투 서버 16
  - 필요 프로그램 : tcpdump

#### ① TCP Dump 설치하기

(sudo) apt- get install tcpdump

#### ② TCP Dump 실행하기

(sudo) tcpdump -i eth0 - xX host 192.168.0.2



```
wishfree@ubuntu-14: ~  
wishfree@ubuntu-14:~$  
wishfree@ubuntu-14:~$ sudo tcpdump -i eth0 -xX host 192.168.0.2  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```

그림 6-4 TCP Dump 설치 여부 확인

## 2. 스니핑 공격 툴

### 실습 6-2 TCP Dump로 계정과 패스워드 스니핑하기

#### ③ 텔넷 접속하기

telnet 192.168.0.2

```
wishfree@ubuntu-S-16: ~  
wishfree@ubuntu-14:~$  
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: Mon Jun  6 11:27:22 KST 2016 from localhost on pts/0  
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com/  
  
53 packages can be updated.  
0 updates are security updates.  
  
*** System restart required ***  
wishfree@ubuntu-S-16:~$ █
```

그림 6-5 원격지 텔넷 서버로 로그인

## 2. 스니핑 공격 툴

### 실습 6-2 TCP Dump로 계정과 패스워드 스니핑하기

#### ④ 텔넷 패킷 분석하기

- 텔넷, FTP 등 초기 서비스들은 계정, 패스워드가 암호화되지 않은 평문으로 전달

```
wishfree@ubuntu-14: ~
02:01:18.001214 IP 192.168.0.2.telnet > 192.168.0.200.59604: Flags [P.], seq 76:
95, ack 114, win 227, options [nop,nop,TS val 301810306 ecr 464398], length 19
  ① 0x0000: 4510 0047 3f6f 4000 4006 7917 c0a8 0002  E..G?o@.@.y.....
    0x0010: c0a8 00c8 0017 e8d4 7ccd 7d69 f97b 3fe8  .....|.}.i.{?.
    0x0020: 8018 00e3 1a8b 0000 0101 080a 11fd 4282  .....B.
    0x0030: 0007 160e 7562 756e 7475 2d53 2d31 3620  ....ubuntu-S-16.
    0x0040: 6c6f 6769 6e3a 20                login:
02:01:18.001225 IP 192.168.0.200.59604 > 192.168.0.2.telnet: Flags [.], ack 95,
win 229, options [nop,nop,TS val 464398 ecr 301810306], length 0
  ② 0x0000: 4510 0034 297d 4000 4006 8f1c c0a8 00c8  E..4)}@.@.....
    0x0010: c0a8 0002 e8d4 0017 f97b 3fe8 7ccd 7d7c  .....{?.|.}|
    0x0020: 8010 00e5 8241 0000 0101 080a 0007 160e  ....A.....
    0x0030: 11fd 4282                ..B.
02:01:19.616113 IP 192.168.0.200.59604 > 192.168.0.2.telnet: Flags [P.], seq 114
:115, ack 95, win 229, options [nop,nop,TS val 464801 ecr 301810306], length 1
  ③ 0x0000: 4510 0035 297e 4000 4006 8f1a c0a8 00c8  E..5)~@.@.....
    0x0010: c0a8 0002 e8d4 0017 f97b 3fe8 7ccd 7d7c  .....{?.|.}|
    0x0020: 8018 00e5 8242 0000 0101 080a 0007 17a1  ....B.....
    0x0030: 11fd 4282 77                ..B.w
02:01:19.616325 IP 192.168.0.2.telnet > 192.168.0.200.59604: Flags [P.], seq 95:
96, ack 115, win 227, options [nop,nop,TS val 301810710 ecr 464801], length 1
  ④ 0x0000: 4510 0035 3f70 4000 4006 7928 c0a8 0002  E..5?p@.@.y(....
    0x0010: c0a8 00c8 0017 e8d4 7ccd 7d7c f97b 3fe9  .....|.}.i.{?.
    0x0020: 8018 00e3 f25f 0000 0101 080a 11fd 4416  ...._.....D.
    0x0030: 0007 17a1 77                ....w
```

그림 6-6 원격 텔넷 로그인 시 계정 Dump 1/2

## 2. 스니핑 공격 툴

### 실습 6-2 TCP Dump로 계정과 패스워드 스니핑하기

#### ④ 텔넷 패킷 분석하기

```
wishfree@ubuntu-14: ~
02:04:14.338463 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 115
:116, ack 96, win 229, options [nop,nop,TS val 508482 ecr 301854368], length 1
 0x0000: 4510 0035 fd10 4000 4006 bb87 c0a8 00c8 E..5..@.@.....
 0x0010: c0a8 0002 e8d6 0017 522e 3cbf 83fc c9de .....R.<.....
 0x0020: 8018 00e5 8242 0000 0101 080a 0007 c242 .....B.....B
 0x0030: 11fd eea0 69 .....i
02:04:14.338705 IP 192.168.0.2.telnet > 192.168.0.200.59606: Flags [P.], seq 96:
97, ack 116, win 227, options [nop,nop,TS val 301854390 ecr 508482], length 1
 0x0000: 4510 0035 24ca 4000 4006 93ce c0a8 0002 E..5$.@.@.....
 0x0010: c0a8 00c8 0017 e8d6 83fc c9de 522e 3cc0 .....R.<.
 0x0020: 8018 00e3 0201 0000 0101 080a 11fd eeb6 .....
 0x0030: 0007 c242 69 ...Bi
02:04:14.338722 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 115,
ack 97, win 229, options [nop,nop,TS val 508482 ecr 301854390], length 0
 0x0000: 4510 0034 fd11 4000 4006 bb87 c0a8 00c8 E..4..@.@.....
 0x0010: c0a8 0002 e8d6 0017 522e 3cc0 83fc c9df .....R.<.....
 0x0020: 8018 00e5 8241 0000 0101 080a 0007 c242 .....A.....B
 0x0030: 11fd eeb6 ....
02:04:14.440657 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 116
:117, ack 97, win 229, options [nop,nop,TS val 508507 ecr 301854390], length 1
 0x0000: 4510 0035 fd12 4000 4006 bb85 c0a8 00c8 E..5..@.@.....
 0x0010: c0a8 0002 e8d6 0017 522e 3cc0 83fc c9df .....R.<.....
 0x0020: 8018 00e5 8242 0000 0101 080a 0007 c25b .....B.....[
 0x0030: 11fd eeb6 73 .....s
02:04:14.440857 IP 192.168.0.2.telnet > 192.168.0.200.59606: Flags [P.], seq 97:
98, ack 117, win 227, options [nop,nop,TS val 301854416 ecr 508507], length 1
 0x0000: 4510 0035 24cb 4000 4006 93cd c0a8 0002 E..5$.@.@.....
 0x0010: c0a8 00c8 0017 e8d6 83fc c9df 522e 3cc1 .....R.<.
 0x0020: 8018 00e3 f7cb 0000 0101 080a 11fd eed0 .....
 0x0030: 0007 c25b 73 ...[s
02:04:14.440874 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 116,
ack 98, win 229, options [nop,nop,TS val 508507 ecr 301854416], length 0
 0x0000: 4510 0034 fd13 4000 4006 bb85 c0a8 00c8 E..4..@.@.....
 0x0010: c0a8 0002 e8d6 0017 522e 3cc1 83fc c9e0 .....R.<.....
 0x0020: 8018 00e5 8241 0000 0101 080a 0007 c25b .....A.....[
 0x0030: 11fd eed0 ....
```

그림 6-7 원격 텔넷 로그인 시 계정 Dump 2/2

## 2. 스니핑 공격 툴

### 실습 6-2 TCP Dump로 계정과 패스워드 스니핑하기

#### ④ 텔넷 패킷 분석하기

```
wishfree@ubuntu-14: ~
02:04:15.543554 IP 192.168.0.2.telnet > 192.168.0.200.59606: Flags [P.], seq 105
:115, ack 124, win 227, options [nop,nop,TS val 301854691 ecr 508782], length 10
①  0x0000:  4510 003e 24d2 4000 4006 93bd c0a8 0002  E..>$.@.@.....
    0x0010:  c0a8 00c8 0017 e8d6 83fc c9e7 522e 3cc8  .....R.<.
    0x0020:  8018 00e3 80c5 0000 0101 080a 11fd efe3  .....
    0x0030:  0007 c36e 5061 7373 776f 7264 3a20      ...nPassword:.
02:04:15.543576 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [.], ack 115,
win 229, options [nop,nop,TS val 508783 ecr 301854691], length 0
    0x0000:  4510 0034 fd20 4000 4006 bb78 c0a8 00c8  E..4..@.@..X...
    0x0010:  c0a8 0002 e8d6 0017 522e 3cc8 83fc c9f1  .....R.<.....
    0x0020:  8010 00e5 8241 0000 0101 080a 0007 c36f  ....A.....o
    0x0030:  11fd efe3                                ....
02:04:19.156734 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 124
:125, ack 115, win 229, options [nop,nop,TS val 509686 ecr 301854691], length 1
②  0x0000:  4510 0035 fd21 4000 4006 bb76 c0a8 00c8  E..5.!@.@..v...
    0x0010:  c0a8 0002 e8d6 0017 522e 3cc8 83fc c9f1  .....R.<.....
    0x0020:  8018 00e5 8242 0000 0101 080a 0007 c6f6  ....B.....
    0x0030:  11fd efe3 64                             ....d
02:04:19.196496 IP 192.168.0.2.telnet > 192.168.0.200.59606: Flags [.], ack 125,
win 227, options [nop,nop,TS val 301855605 ecr 509686], length 0
③  0x0000:  4510 0034 24d3 4000 4006 93c6 c0a8 0002  E..4$.@.@.....
    0x0010:  c0a8 00c8 0017 e8d6 83fc c9f1 522e 3cc9  .....R.<.
    0x0020:  8010 00e3 617b 0000 0101 080a 11fd f375  ....a{.....u
    0x0030:  0007 c6f6                                ....
02:04:19.365676 IP 192.168.0.200.59606 > 192.168.0.2.telnet: Flags [P.], seq 125
:126, ack 115, win 229, options [nop,nop,TS val 509739 ecr 301855605], length 1
④  0x0000:  4510 0035 fd22 4000 4006 bb75 c0a8 00c8  E..5."@.@..u...
    0x0010:  c0a8 0002 e8d6 0017 522e 3cc9 83fc c9f1  .....R.<.....
    0x0020:  8018 00e5 8242 0000 0101 080a 0007 c72b  ....B.....+
    0x0030:  11fd f375 69                             ...ui
02:04:19.365822 IP 192.168.0.2.telnet > 192.168.0.200.59606: Flags [.], ack 126,
win 227, options [nop,nop,TS val 301855647 ecr 509739], length 0
    0x0000:  4510 0034 24d4 4000 4006 93c5 c0a8 0002  E..4$.@.@.....
    0x0010:  c0a8 00c8 0017 e8d6 83fc c9f1 522e 3cca  .....R.<.
    0x0020:  8010 00e3 611b 0000 0101 080a 11fd f39f  ....a.....
    0x0030:  0007 c72b                                ...+
```

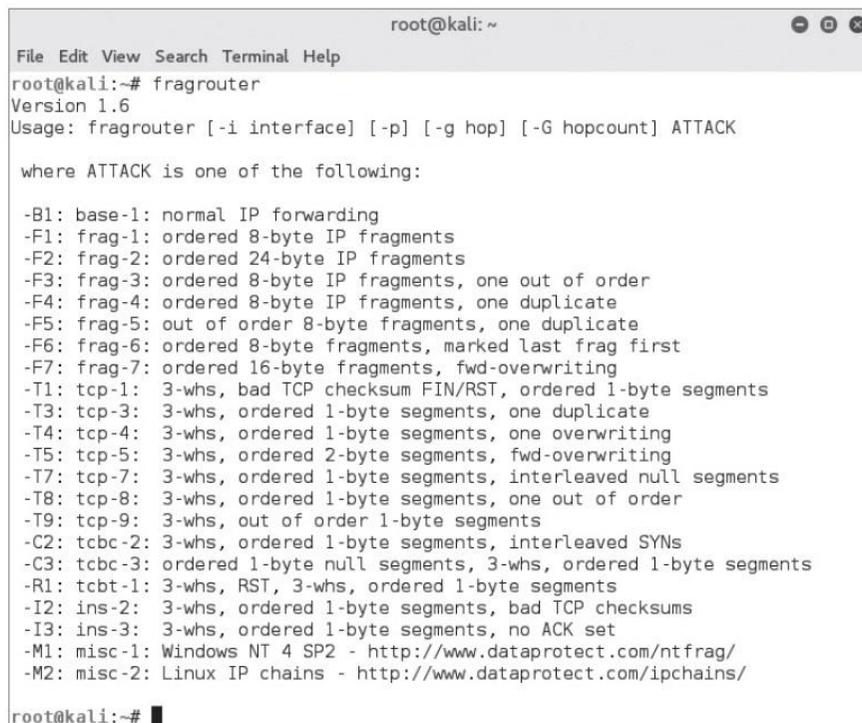
그림 6-8 원격 텔넷 로그인 시 패스워드 Dump

## 2. 스니핑 공격 툴

### 2.2 fragrouter

#### ■ Fragrouter(프래그라우터)

- 스니핑을 보조해주는 툴로, 받은 패킷을 전달하는 역할
- 스니핑을 하거나 세션을 가로챘을 때 공격자에게 온 패킷을 정상적으로 전달하려면 패킷 릴레이가 반드시 필요함.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# fragrouter  
Version 1.6  
Usage: fragrouter [-i interface] [-p] [-g hop] [-G hopcount] ATTACK  
  
where ATTACK is one of the following:  
  
-B1: base-1: normal IP forwarding  
-F1: frag-1: ordered 8-byte IP fragments  
-F2: frag-2: ordered 24-byte IP fragments  
-F3: frag-3: ordered 8-byte IP fragments, one out of order  
-F4: frag-4: ordered 8-byte IP fragments, one duplicate  
-F5: frag-5: out of order 8-byte fragments, one duplicate  
-F6: frag-6: ordered 8-byte fragments, marked last frag first  
-F7: frag-7: ordered 16-byte fragments, fwd-overwriting  
-T1: tcp-1: 3-whs, bad TCP checksum FIN/RST, ordered 1-byte segments  
-T3: tcp-3: 3-whs, ordered 1-byte segments, one duplicate  
-T4: tcp-4: 3-whs, ordered 1-byte segments, one overwriting  
-T5: tcp-5: 3-whs, ordered 2-byte segments, fwd-overwriting  
-T7: tcp-7: 3-whs, ordered 1-byte segments, interleaved null segments  
-T8: tcp-8: 3-whs, ordered 1-byte segments, one out of order  
-T9: tcp-9: 3-whs, out of order 1-byte segments  
-C2: tcbc-2: 3-whs, ordered 1-byte segments, interleaved SYNs  
-C3: tcbc-3: ordered 1-byte null segments, 3-whs, ordered 1-byte segments  
-R1: tcbt-1: 3-whs, RST, 3-whs, ordered 1-byte segments  
-I2: ins-2: 3-whs, ordered 1-byte segments, bad TCP checksums  
-I3: ins-3: 3-whs, ordered 1-byte segments, no ACK set  
-M1: misc-1: Windows NT 4 SP2 - http://www.dataprotect.com/ntfrag/  
-M2: misc-2: Linux IP chains - http://www.dataprotect.com/ipchains/  
root@kali:~#
```

그림 6-9 fragrouter 실행 옵션 확인

## 2. 스니핑 공격 툴

### 2.3 DSniff

#### ■ DSniff(디스니프)

- 스니핑을 위한 다양한 툴이 패키지처럼 만들어진 것
- 한국계 미국인으로 해커이자 정보보호기술 전문가인 미국 미시건 대학교의 송덕준 교수가 개발
- 알트보어(Altvore)와 함께 대표적인 스니핑 툴로 알려져 있음.
- 암호화된 계정과 패스워드까지 읽어낼 수 있음.
- dsniff가 읽어낼 수 있는 패킷

ftp, telnet, http, pop, nntp, imap, snmp, ldap, rlogin, rip, ospf, pptp, ms-chap, nfs, yp/nis+, socks, x11, cvs, IRC, ATM, ICQ, PostageSQL, Citrix ICA, Symantec pcAnywhere, MS SQL, auth, info

## 2. 스니핑 공격 툴

### 2.3 DSniff

#### ■ DSniff(디스니프)

표 6-1 DSniff에 포함되어 있는 툴

툴	기능
filesnarf	NFS 트래픽에서 스니핑한 파일을 현재 디렉토리에 저장한다.
macof	스위치 환경에서 스위치를 허브와 같이 작동시키기 위하여 임의의 MAC 주소로 스위치의 MAC 테이블을 오버플로우(overflow)시킨다.
mailsnarf	SNMP와 POP 트래픽을 스니핑하여 이메일을 볼 수 있게 한다. 스니핑한 이메일은 mail 클라이언트로 볼 수 있다.
msgsnarf	AOL 메신저, ICQ 2000, IRC, Yahoo 메신저 등의 채팅 메시지를 선택하여 스니핑한다.
tcpkill	특정 인터페이스를 통해 탐지할 수 있는 TCP 세션을 모두 끊는다.
tcprnic	ICMP source quench 메시지를 보내 특정 TCP 연결을 느리게 만든다. 속도가 빠른 네트워크에서 스니핑을 할 때 유용하다.
arp spoof	ARP 스푸핑 공격을 실행한다.
dns spoof	DNS 스푸핑 공격을 실행한다.
urlsnarf	CLF(Common Log Format)에서 HTTP 트래픽을 스니핑하여 선택된 URL을 알려준다.

## 2. 스니핑 공격 툴

### 실습 6-3 Dsniff로 다양한 스니핑 공격하기

- 실습환경**
- 클라이언트 시스템 : 칼리 리눅스
  - FTP, 텔넷 서버 시스템 : 우분투 서버 16
  - 필요 프로그램 : dsniff 패키지

#### ① dsniff 설치하기

- 칼리 리눅스는 dsniff가 기본적으로 설치되어 있어 추가로 설치할 필요가 없음.
- 설치가 되어 있지 않은 경우 apt-get으로 설치  
`apt- get install dsniff`

## 2. 스니핑 공격 툴

### 실습 6-3 DSniff로 다양한 스니핑 공격하기

#### ② dsniff를 이용한 FTP와 텔넷의 패스워드 스니핑

- 클라이언트에서 dsniff를 실행하고 다른 터미널에서 서버에 FTP와 텔넷을 이용해 로그인하면 아이디와 패스워드가 잡힘(텔넷은 입력한 명령어도 확인 가능)

dsniff

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# dsniff  
dsniff: listening on eth0  
-----  
08/14/16 10:21:34 tcp kali.54226 -> 192.168.0.223 (telnet)  
wishfree  
dideodlf  
ls  
exit  
-----  
08/14/16 10:21:45 tcp kali.38802 -> 192.168.0.221 (ftp)  
USER wishfree  
PASS dideodlf
```

그림 6-10 dsniff 실행하기

## 2. 스니핑 공격 툴

### 실습 6-3 DSniff로 다양한 스니핑 공격하기

#### ③ urlsnarf를 이용한 웹 세션 스니핑

- 인터넷 사용자가 접속한 서버와 접속 후 입력한 내용 등의 정보를 볼 수 있음.

urlsnarf



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# urlsnarf  
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]  
kali - - [14/Aug/2016:10:51:09 -0700] "POST http://ocsp.digicert.com/ HTTP/1.1"  
- - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 I  
ceweasel/43.0.4"  
kali - - [14/Aug/2016:10:51:09 -0700] "POST http://ocsp.digicert.com/ HTTP/1.1"  
- - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 I  
ceweasel/43.0.4"  
kali - - [14/Aug/2016:10:51:17 -0700] "GET http://www.google.co.kr/ HTTP/1.1" -  
- "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 I  
ceweasel/43.0.4"  
kali - - [14/Aug/2016:10:51:17 -0700] "POST http://clients1.google.com/ocsp HTTP  
/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/4  
3.0 Iceweasel/43.0.4"  
kali - - [14/Aug/2016:10:51:18 -0700] "POST http://clients1.google.com/ocsp HTTP  
/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/4  
3.0 Iceweasel/43.0.4"  
kali - - [14/Aug/2016:10:51:18 -0700] "POST http://clients1.google.com/ocsp HTTP  
/1.1" - - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/4  
3.0 Iceweasel/43.0.4"
```

그림 6-11 urlsnarf 실행하기

## 3. 스위칭 환경에서의 스니핑

### 3.1 스위칭 환경과 스니핑

---

#### ■ 스위칭 환경과 스니핑

- 스위치는 각 장비의 MAC 주소를 확인하여 포트에 할당
  - 자신에게 향하지 않은 패킷 외에는 받아볼 수 없어 스니핑을 막게 됨.
- 스위치가 스니핑을 막기 위해 만들어진 장비는 아니지만 결과적으로는 저지하는 치명적인 장비가 됨.

### 3. 스위칭 환경에서의 스니핑

#### 3.2 ARP 리다이렉트와 ARP 스푸핑

##### ■ ARP 리다이렉트

- 공격자가 자신을 라우터라고 속이는 것
- 기본적으로 2계층 공격으로, 랜에서 공격
- 공격자 자신은 원래 라우터의 MAC 주소를 알고 있어야 하며, 받은 모든 패킷은 다시 라우터로 릴레이해줘야 함.
- ARP 스푸핑은 호스트 대 호스트 공격, ARP 리다이렉트는 랜의 모든 호스트 대 라우터라는 점 외에는 큰 차이가 없음.

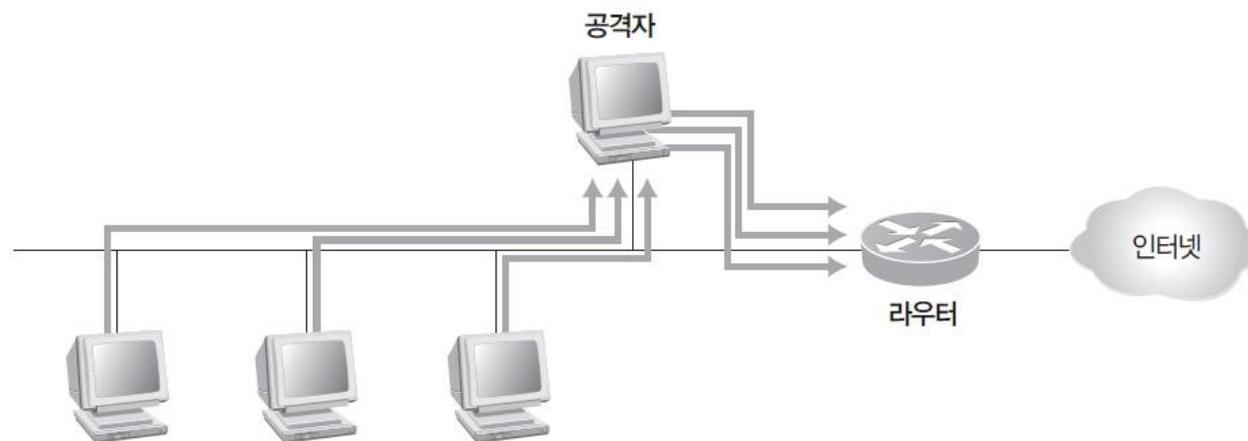


그림 6-12 ARP 리다이렉트의 개념도

### 3. 스위칭 환경에서의 스니핑

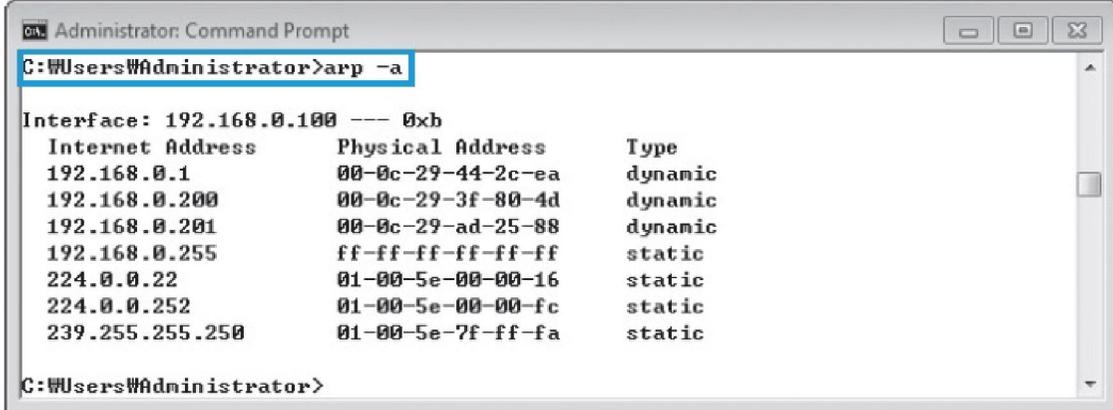
#### 실습 6-4 ARP 리다이렉트 공격하기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
  - 공격 대상 시스템 : 윈도우 7
  - 필요 프로그램 : fragrouter, dsniff 패키지

#### ① 공격 전에 공격 대상 시스템의 상태 정보 확인하기

- 공격 전에 MAC 주소 테이블 확인

arp -a



```
Administrator: Command Prompt
C:\Users\Administrator>arp -a

Interface: 192.168.0.100 --- 0xb
Internet Address      Physical Address      Type
192.168.0.1           00-0c-29-44-2c-ea     dynamic
192.168.0.200         00-0c-29-3f-80-4d     dynamic
192.168.0.201         00-0c-29-ad-25-88     dynamic
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:\Users\Administrator>
```

그림 6-13 ARP 공격 전 클라이언트의 ARP 테이블

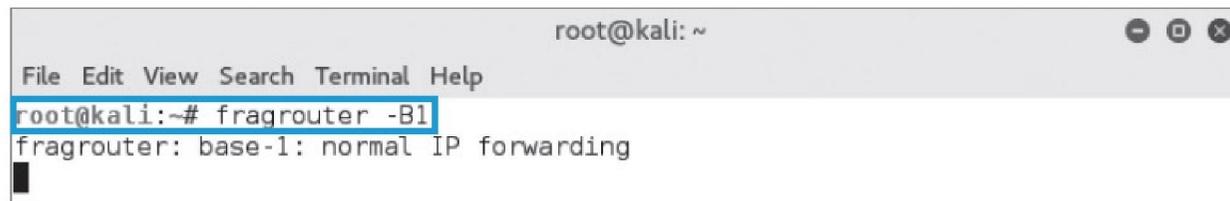
### 3. 스위칭 환경에서의 스니핑

#### 실습 6-4 ARP 리다이렉트 공격하기

#### ② ARP 리다이렉트 공격 수행하기

- 패킷이 오면 세션이 끊어지지 않게 패킷을 원래 목적지로 전달하기 위해 먼저 릴레이 툴로 fragrouter 실행

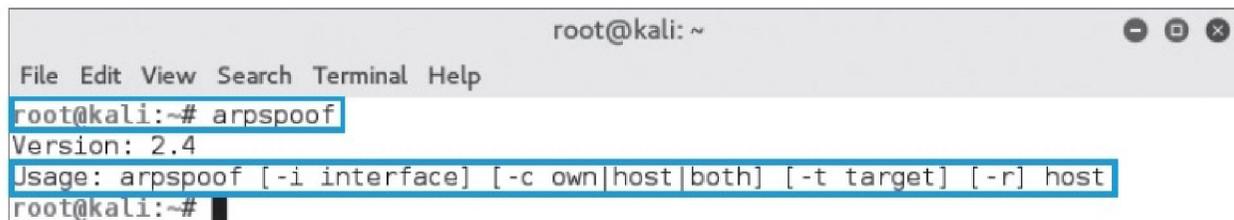
fragrouter - B1



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

그림 6-14 fragrouter 실행

- ARP 리다이렉트 공격을 수행하기 위해서 arpspoof를 사용



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof  
Version: 2.4  
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host  
root@kali:~#
```

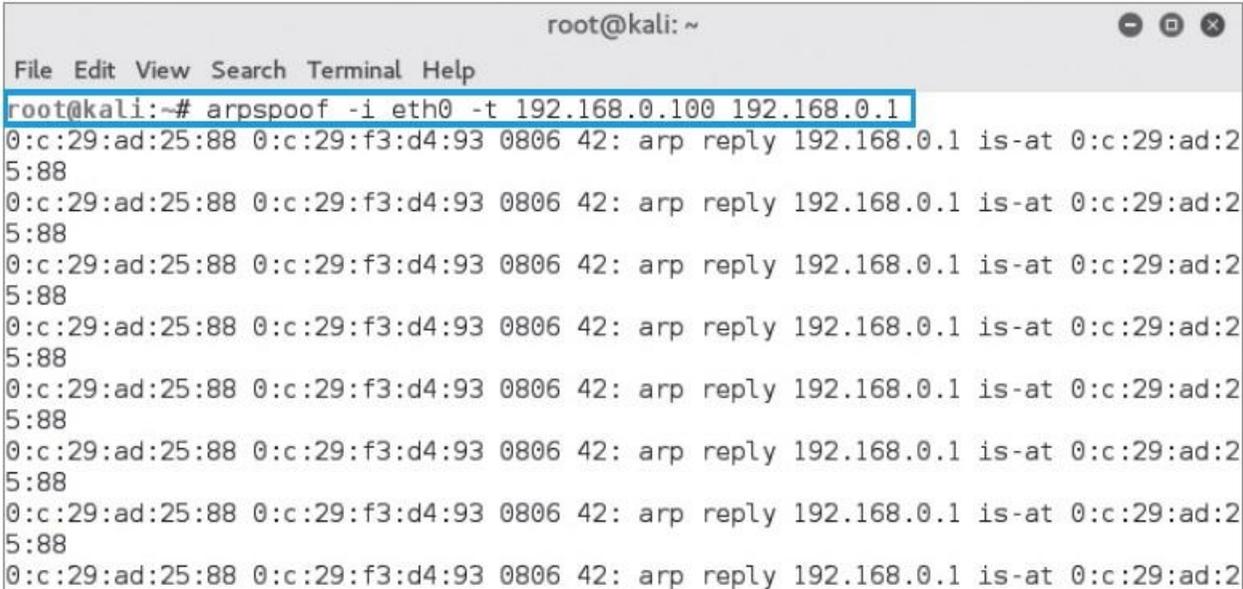
그림 6-15 arpspoof 실행

### 3. 스위칭 환경에서의 스니핑

#### 실습 6-4 ARP 리다이렉트 공격하기

#### ② ARP 리다이렉트 공격 수행하기

```
arpspoof -i eth0 -t 192.168.0.100 192.168.0.1
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# arpspoof -i eth0 -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  
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  
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
```

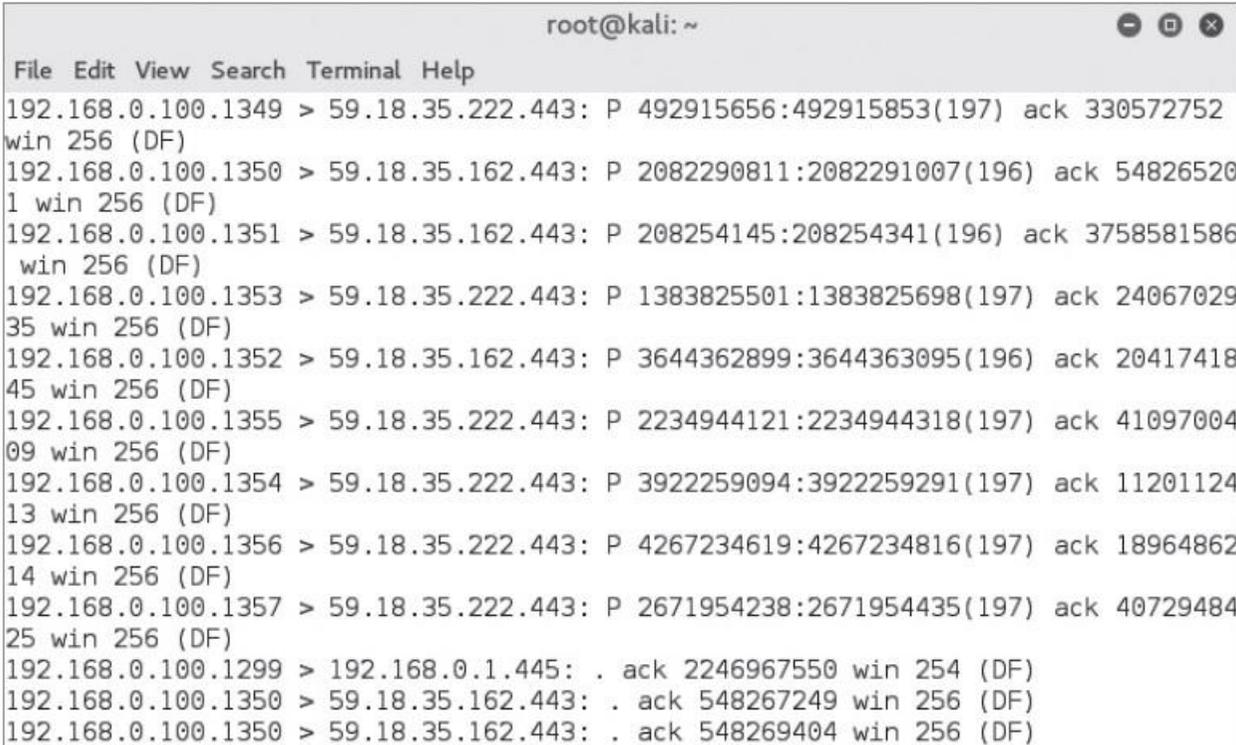
그림 6-16 ARP 리다이렉트 공격 실행하기

### 3. 스위칭 환경에서의 스니핑

#### 실습 6-4 ARP 리다이렉트 공격하기

#### ② ARP 리다이렉트 공격 수행하기

- 패킷이 공격자 시스템을 통과한 것을 fragrouter를 실행한 창에서 확인



```
root@kali: ~  
File Edit View Search Terminal Help  
192.168.0.100.1349 > 59.18.35.222.443: P 492915656:492915853(197) ack 330572752  
win 256 (DF)  
192.168.0.100.1350 > 59.18.35.162.443: P 2082290811:2082291007(196) ack 54826520  
1 win 256 (DF)  
192.168.0.100.1351 > 59.18.35.162.443: P 208254145:208254341(196) ack 3758581586  
win 256 (DF)  
192.168.0.100.1353 > 59.18.35.222.443: P 1383825501:1383825698(197) ack 24067029  
35 win 256 (DF)  
192.168.0.100.1352 > 59.18.35.162.443: P 3644362899:3644363095(196) ack 20417418  
45 win 256 (DF)  
192.168.0.100.1355 > 59.18.35.222.443: P 2234944121:2234944318(197) ack 41097004  
09 win 256 (DF)  
192.168.0.100.1354 > 59.18.35.222.443: P 3922259094:3922259291(197) ack 11201124  
13 win 256 (DF)  
192.168.0.100.1356 > 59.18.35.222.443: P 4267234619:4267234816(197) ack 18964862  
14 win 256 (DF)  
192.168.0.100.1357 > 59.18.35.222.443: P 2671954238:2671954435(197) ack 40729484  
25 win 256 (DF)  
192.168.0.100.1299 > 192.168.0.1.445: . ack 2246967550 win 254 (DF)  
192.168.0.100.1350 > 59.18.35.162.443: . ack 548267249 win 256 (DF)  
192.168.0.100.1350 > 59.18.35.162.443: . ack 548269404 win 256 (DF)
```

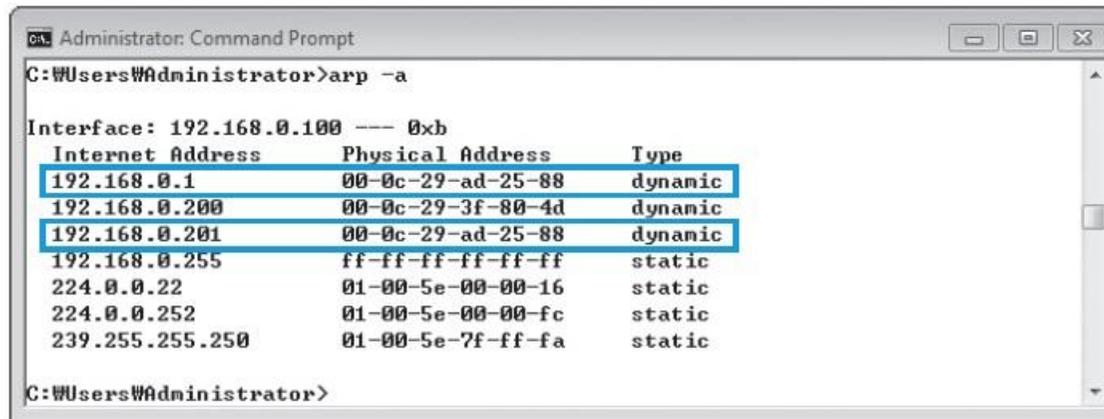
그림 6-17 fragrouter 실행 결과

### 3. 스위칭 환경에서의 스니핑

#### 실습 6-4 ARP 리다이렉트 공격하기

### ③ ARP 리다이렉트 공격 수행의 결과 확인

arp -a



```
Administrator: Command Prompt
C:\Users\Administrator>arp -a

Interface: 192.168.0.100 --- 0xb
Internet Address      Physical Address      Type
192.168.0.1           00-0c-29-ad-25-88    dynamic
192.168.0.200         00-0c-29-3f-80-4d    dynamic
192.168.0.201         00-0c-29-ad-25-88    dynamic
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:\Users\Administrator>
```

그림 6-18 ARP 공격 후 클라이언트의 ARP 테이블

## 3. 스위칭 환경에서의 스니핑

### 3.3 ICMP 리다이렉트

#### ■ ICMP 리다이렉트

- 공격 대상에게 패킷을 보낸 후 라우터 A에 다시 릴레이시켜 스니핑함.
- 3계층에서 패킷을 주고받기 때문에 랜이 아니더라도 공격이 가능
- 최근에는 운영체제에서 ICMP 리다이렉트를 기본적으로 차단함.

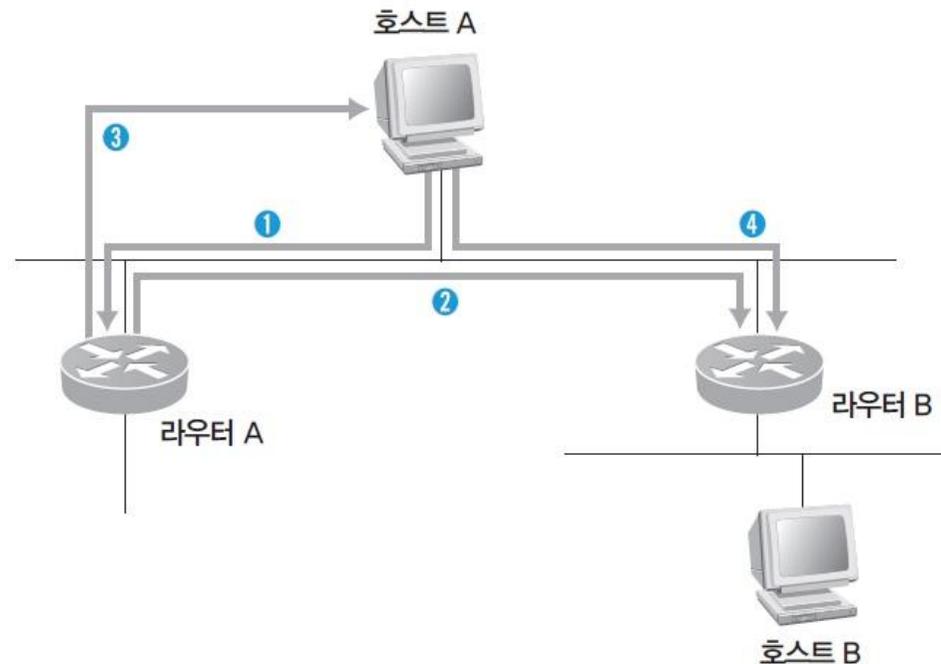


그림 6-19 ICMP 리다이렉트의 개념도

## 3. 스위칭 환경에서의 스니핑

### 3.4 스위치 재밍

---

#### ■ 스위치 재밍(Switch Jamming)

- 스위치를 직접 공격
- MAC 테이블을 위한 캐시 공간에 버퍼 오버플로우 공격을 실시
- 일부 고가의 스위치는 MAC 테이블의 캐시와 연산 장치가 사용하는 캐시가 독립적으로 나뉘어 있어 스위치 재밍 공격이 통하지 않음.

### 3. 스위칭 환경에서의 스니핑

#### 실습 6-5 macof로 스위치 재밍시키기

- 실습환경**
- 공격자 시스템 : 칼리 리눅스
  - 공격 대상 시스템 : 스위치
  - 필요 프로그램 : macof(dsniff를 설치하면 자동으로 설치)

#### ① macof 사용법 확인하기

macof /?



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# macof /?  
Version: 2.4  
Usage: macof [-s src] [-d dst] [-e tha] [-x sport] [-y dport]  
           [-i interface] [-n times]  
root@kali:~#
```

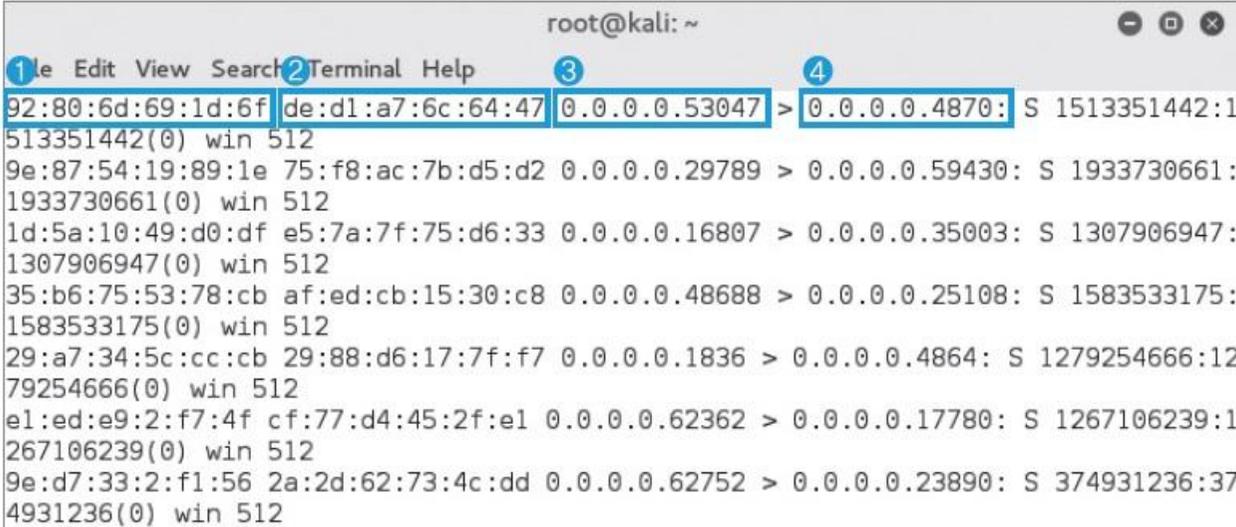
그림 6-20 macof의 사용법

### 3. 스위칭 환경에서의 스니핑

#### 실습 6-5 macof로 스위치 재밍시키기

##### ① macof 사용법 확인하기

macof



```
root@kali: ~  
1 le Edit View Search 2 Terminal Help 3 4  
92:80:6d:69:1d:6f de:d1:a7:6c:64:47 0.0.0.0.53047 > 0.0.0.0.4870: S 1513351442:1  
513351442(0) win 512  
9e:87:54:19:89:1e 75:f8:ac:7b:d5:d2 0.0.0.0.29789 > 0.0.0.0.59430: S 1933730661:  
1933730661(0) win 512  
1d:5a:10:49:d0:df e5:7a:7f:75:d6:33 0.0.0.0.16807 > 0.0.0.0.35003: S 1307906947:  
1307906947(0) win 512  
35:b6:75:53:78:cb af:ed:cb:15:30:c8 0.0.0.0.48688 > 0.0.0.0.25108: S 1583533175:  
1583533175(0) win 512  
29:a7:34:5c:cc:cb 29:88:d6:17:7f:f7 0.0.0.0.1836 > 0.0.0.0.4864: S 1279254666:12  
79254666(0) win 512  
e1:ed:e9:2:f7:4f cf:77:d4:45:2f:e1 0.0.0.0.62362 > 0.0.0.0.17780: S 1267106239:1  
267106239(0) win 512  
9e:d7:33:2:f1:56 2a:2d:62:73:4c:dd 0.0.0.0.62752 > 0.0.0.0.23890: S 374931236:37  
4931236(0) win 512
```

그림 6-21 macof 실행 결과

## 3. 스위칭 환경에서의 스니핑

### 3.5 SPAN 포트 태핑

#### ■ SPAN(Switch Port Analyzer)

- 각 포트에 전송되는 데이터를 미러링하는 포트에도 똑같이 보내주는 포트 미러링(Port Mirroring)을 이용한 것
- 주로 IDS를 설치할 때 많이 사용
- SPAN은 주로 시스코에서 사용하는 용어며, 다른 벤더에서는 'Port Roving'이라 부르기도 함.

#### ■ 태핑

- SPAN은 상당히 많은 문제점을 가져서 효과적인 모니터링을 하는데 어려움이 있는데, 이를 해결할 수 있는 것이 태핑
- 허브와 같이 포트를 모니터링하기 위한 장비
- Splitter(스플리터)라고 부르기도 함.

## 4. 스니핑 공격의 대응책

### 4.1 스니핑 대응책

#### ■ 능동적인 대응책 - 스니퍼 탐지

##### ① ping을 이용한 탐지

- 의심이 가는 호스트에 ping을 보낼 때 네트워크에 존재하지 않는 MAC 주소를 위장하여 보냄.
- 만약 ICMP Echo Reply를 받으면 해당 호스트가 스니핑을 하고 있는 것

##### ② ARP를 이용한 탐지

- 위조된 ARP Request를 스니퍼임을 확인하고자 하는 시스템에 보냄.
- 대상 시스템이 응답으로 ARP Response를 보내면 이를 통해 프러미스큐어스 모드로 동작 중인 스니퍼임을 확인

##### ③ DNS를 이용한 탐지

- 테스트 대상 네트워크로 Ping Sweep을 보내고 들어오는 Inverse-DNS lookup을 감시

##### ④ 유인을 이용한 탐지

- 가짜 계정과 패스워드를 뿌려 공격자가 이 가짜 정보로 접속을 시도하면, 접속을 시도하는 시스템을 탐지

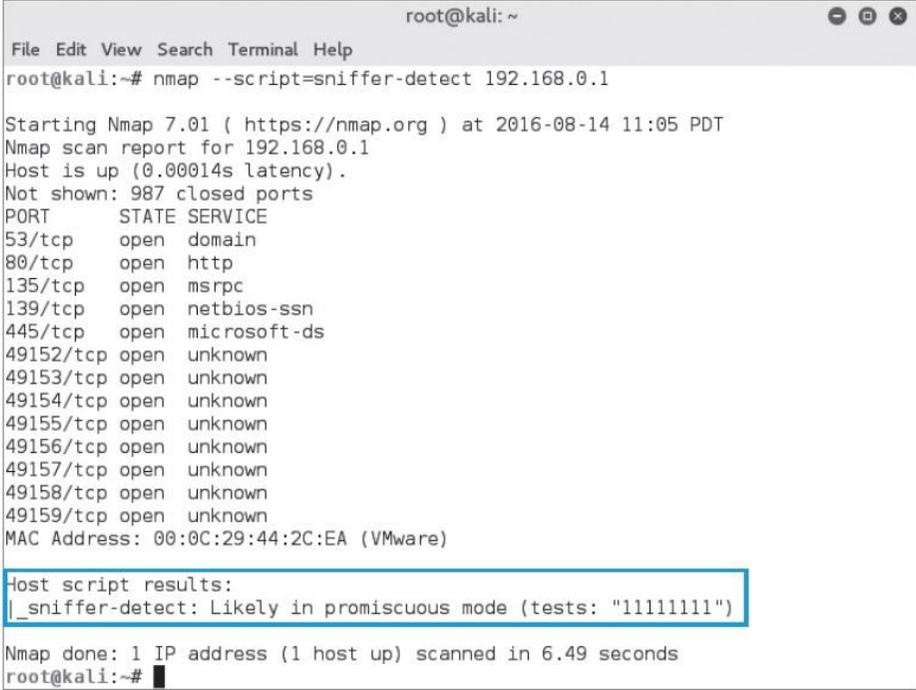
## 4. 스니핑 공격의 대응책

### 4.1 스니핑 대응책

#### ■ 능동적인 대응책 - 스니퍼 탐지

##### ⑤ ARP watch를 이용한 탐지

- 초기에 MAC 주소와 IP 주소의 매칭 값을 저장하고 ARP 트래픽을 모니터링하여 이를 변하게 하는 패킷이 탐지되면 관리자에게 메일로 알려줌.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap --script=sniffer-detect 192.168.0.1  
  
Starting Nmap 7.01 ( https://nmap.org ) at 2016-08-14 11:05 PDT  
Nmap scan report for 192.168.0.1  
Host is up (0.00014s latency).  
Not shown: 987 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
49152/tcp open  unknown  
49153/tcp open  unknown  
49154/tcp open  unknown  
49155/tcp open  unknown  
49156/tcp open  unknown  
49157/tcp open  unknown  
49158/tcp open  unknown  
49159/tcp open  unknown  
MAC Address: 00:0C:29:44:2C:EA (VMware)  
  
_host script results:  
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")  
  
Nmap done: 1 IP address (1 host up) scanned in 6.49 seconds  
root@kali:~#
```

그림 6-22 nmap을 이용한 스니퍼 탐지

## 4. 스니핑 공격의 대응책

### 4.1 스니핑 대응책

#### ■ 수동적인 대응책 - 암호화

##### ① SSL(Secure Socket Layer)

- 암호화된 웹 서핑을 가능하게 함.
- 40비트와 128비트 암호화키가 존재(현재 우리나라 금융 거래 사이트의 대부분은 40비트 암호화 방법을 사용)

##### ② PGP, PEM, S/MIME

- PGP, PEM, S/MIME 모두 이메일을 전송할 때 사용하는 암호화 방법
- PGP : 내용을 암호화하는 데에 IDEA, IDEA 키와 전자 서명을 암호화하는 데에 RSARivest, Shamir, Addleman 알고리즘 사용  
기본적으로 ' Web of Trust' 개념 사용
- PEM : 공개키 암호화 표준을 따르고, CA에서 키를 관리  
데이터 암호화에는 DES-EDE, 키를 위한 암호화 알고리즘에는 RSA, 전자 인증을 위한 해시 함수에는 MD2, MD5 사용
- S/MIME : 이메일 표준인 MIME 형식에 암호화 서비스만을 추가한 것  
PKCS를 기반으로 만들어져 있으며, 디지털 인증에 X.509를 사용

## 4. 스니핑 공격의 대응책

### 4.1 스니핑 대응책

#### ■ 수동적인 대응책 - 암호화

##### ③ SSH(Secure Shell)

- 텔넷과 같은 서비스 암호화를 위해 사용하는 것
- OpenSSL 라이브러리가 SSH를 지원
- SSH를 이용한 암호화 프로토콜은 계속 발전하고 있으며 텔넷보다는 훨씬 더 안전

##### ④ VPN(Virtual Private Network)

- 한 회선을 여러 회사가 공유하여 비용을 절감하려는 목적으로 개발
- 암호화된 트래픽 제공
- VPN을 제공하는 시스템이 해킹을 당할 경우 암호화되기 이전에 데이터가 스니핑이 될 수 있음.



# 감사합니다.

## 네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습

---