Linux-admin mailing-list FAQ

Fyodor Yarochkin, <fygrave@usa.net> 외 Linux-admin 메일링 리스트 사용자들 v0.12, 1998년 11월 17일

번역: 권 순선 <cessi@kldp.linux-kr.org>, SGML 편집: 엄 기성 <jurist@sarang.net> v0.5, 1998년 11월 17일

번역자 주: 이 문서는 linux-admin 메일링 리스트의 FAQ입니다. 지금 읽고 계시는 이 문서는 원문의 최신 버전을 번역한 것은 아닙니다만 우선 현재 상태로도 꽤 많은 유용한 정보들이 포함되어 있습니다. 다음번에 이 문서를 올릴 때는 시간이 허락하는 한 최신 버전과 비교하여 바뀐 부분을 반영할 수 있도록 하겠습니다. 번역에 잘못된 점이나 고칠 점 등이 있으면 기탄없이 말씀해 주십시오. 이 번역 문서의 최신 버전은 <http://kldp.linux-kr.org>에서 읽으실 수 있습니다.

목 차

제 1 절 서문

이 글은 linux-admin 메일링리스트에서 자주 거론되는 질문과 답변들에 대한 FAQ(Frequently Asked Questions) 입니다. 이 문서는 다음 사이트에서 최신 버전을 읽으실 수 있습니다.

HTML버전 `<http://www.kalug.lug.net/linux-admin-FAQ/>`

미러 사이트

- `<http://linux.ibd.net/linux-admin-FAQ/>`
- `<http://spyjurenet.com/linux/>`
- `<http://beryte.com/linux/faq/>`
- `<http://www.miscellaneous.net/linux/>`
- `<http://www.cybernet.bg/linux/>`

이 FAQ는 여러분들이 리눅스/유닉스에 대해서 기본적인 내용을 어느 정도 숙지하고 있으며 시스템 관리와 관련된 사항들도 어느 정도 기초가 있다고 가정하고 있습니다. "리눅스가 뭐죠?", "리눅스를 어떻게 설치하죠?" 같은 질문은 ***RTFM(Read The *Fine* Manual")***이라고 적힌 간단한 답변만을 들을 수 있을 것입니다. 그런 질문에 대한 대답은 `<http://www.linux.org>`, `<http://sunsute.unc.edu/LDP>`등의 홈페이지를 참고하시기 바랍니다.

제 2 절 일반적인 정보

2.1 어떻게 이 메일링 리스트에 가입하고 탈퇴할 수 있습니까?

이 메일링 리스트는 `vger.rutgers.edu` 에 있는 `majordomo` 서버에서 운영되고 있습니다. 이 메일링 리스트에 가입/탈퇴하고 싶을때는 `majordomo@vger.rutgers.edu`로 메일을 보내시면 됩니다.

메일링 리스트에 가입하시려면 다음 내용을 메시지 본문에 적어서 보내세요.

```
subscribe linux-admin your@email.address
```

메일링 리스트에 탈퇴하시려면 다음 내용을 메시지 본문에 적어서 보내세요.

`unsubscribe linux-admin your@email.address`

메일을 보내실때 제목은 어떻게 붙여도 상관없습니다.

2.2 이 메일링 리스트는 무엇을 위한 것입니까?

이 메일링 리스트는 다른 linux-kernel, linux-net, linux-x11 등의 메일링 리스트와 약간 겹치는, 그런 사항들을 포함한 일반적인 모든 리눅스 관리와 관련된 사항들을 다룹니다.

2.3 더 자세한 정보를 얻고 싶을때는 어떻게 하나요?

인터넷에서 리눅스와 관련된 많은 리소스들을 찾아보실 수 있습니다. 처음 시작하기에 좋은 사이트들은 다음과 같습니다.

- <http://www.linux.org>
- <http://sunsite.unc.edu/mdw/linux.html>
- <http://www.linux.org/help/>
- <http://sunsite.unc.edu/mdw/FAQ/Linux-FAQ.html>
- <http://sunsite.unc.edu/LDP>
- <http://www.redhat.com>
- *Linux IP Masquerade Resource* <http://ipmasq.home.ml.org>

2.4 이 메일링 리스트의 메시지들이 어딘가에서 따로 저장되고 있나요?

예 그렇습니다. <http://www.reference.com>, <http://www.linuxhq.com/lnxlists/linux-admin/>에서 보실 수 있는데 다른 곳도 몇 군데 더 있을 겁니다.

이 메일링 리스트와 관련있는 사항들을 조금 다루고 있는 <http://linuxwww.db.erau.edu/mail_archives/>도 한번 뒤져 보십시오.

또한 리눅스와 관련된 메일링 리스트, 뉴스그룹 인덱스를 <http://www.linuxrx.com/Lists/Lists.perl>에서 찾아보실 수 있습니다. 이것은 제목을 기준으로 정렬되어 있고 내용을 찾아보기 쉽게 되어 있습니다. 현재 533개의 메일링리스트 정보가 있습니다.

또다른 곳: <http://www.findmail.com/list/linux-admin/>

2.5 저는 며칠동안 단 하나의 메시지도 받아보지 못했습니다. 메시지들이 모두 어디로 날아간 건가요?

몇 가지 이유로 인해 당신이 자동으로 메일링 리스트에서 탈퇴 처리되어버린 경우가 있을 수 있습니다. 물론 인터넷 네트워크 자체에 문제가 있었을 수도 있지요. 그럴때는 메일링리스트에서 탈퇴하신 다음 다시 가입하시면 됩니다. 메일링 리스트에 그런 문제에 관해서 메일을 보내는 것은 전혀 도움이 되지 않을 것입니다.

만약 당신이 메일링 리스트에서 탈퇴되었는지 살펴보기 위해서는 majordomo@vger.rutgers.edu에 본문을 다음과 같이 작성하여 메일을 보내 보세요.

`which [<address>]`

당신(만약 <address>를 명시했을 경우 해당 <address>사용자)이 어떤 메일링 리스트에 가입했는지 알려줄 것입니다.

가끔 메일링 리스트에 가입이 잘 안된다고 하는 분들이 있는데 그럴때는 가입을 일단 취소한 다음 다시 가입하면 됩니다.

제 3 절 리눅스 하드웨어 FAQ

3.1 64메가 이상의 메모리를 인식하게 하려면 어떻게 하나요?

커널이 64메가 이상의 메모리를 인식하게 하기 위해서는 부팅하고자 하는 부팅 이미지 이름(**label**)뒤에 **mem=XXXM**라는 내용을 추가시켜 주거나 혹은 이런 사항을 파라미터로 설정하여 계속 적용되도록 하면 됩니다.

/etc/lilo.conf 파일에

```
append="mem=XXXM"
```

을 추가해 주면 됩니다.(이렇게 **lilo.conf**에 내용을 추가하고 난 후에 `lilo`를 다시 실행시키는 것을 잊지 마세요.)

man bootparm의 내용중 일부를 한번 살펴보겠습니다.

```
'mem=...'
```

현재 설치되어 있는 메모리의 용량을 넘겨주는, PC 사양에 정의되어 있는 **BIOS**콜은 64메가까지만 보고할 수 있도록 설계되어 있습니다. 리눅스는 부팅할때 얼마만큼의 메모리가 장착되어 있는지 알아내기 위해 이 BIOS 콜을 이용합니다. 만약 여러분이 64메가 이상의 메모리를 설치했다면 이 부팅 관련 파라미터를 이용하여 리눅스 시스템에 얼마만큼의 메모리가 장착되어 있는지 알려줄 수 있습니다. 값은 십진수일 수도 있고 혹은 **16진수(0x 를 앞에 붙임)**일 수도 있으며 단위는 **k(1024)**혹은 **M(1048576)**을 사용할 수 있습니다. 리눅스 커널 개발자인 라이너스(Linus)는 'mem=' 파라미터에 관해 다음과 같이 언급했습니다.

커널은 당신이 지정하는 대로 'mem=xx' 파라미터를 받아들입니다. 그리고 만약 당신이 그 파라미터를 거짓으로 지정한 것이 드러나면 곧 시스템은 망가질 것입니다. 이 파라미터는 커널이 액세스할 수 있는 최상위 메모리 주소를 나타내므로 예를 들어 'mem=0x1000000' 은 당신이 16메가의 메모리를 가지고 있다는 것을 뜻하며 96메가의 메모리를 가지고 있다면 'mem=0x6000000' 이 됩니다.

주의. 주의. 주의: 어떤 시스템의 경우 최상위 메모리를 BIOS 캐싱 등의 용도로 사용하는 경우가 있기 때문에 96메가 전부에 접근하지 못할 수도 있습니다. 그 반대의 경우는 항상 성립합니다. 어떤 칩셋은 BIOS 가 커버하는 물리적인 메모리를 최상위 메모리 주소 다음 위치로 대응시키기 때문에 실제 최상위 메모리 주소는 96MB + 384kB 가 될 수도 있습니다. 만약 당신이 실제로 가지고 있는 메모리보다 더 많이 가지고 있다고 리눅스에게 알려주게 되면 좋지않은 일이 생길 것입니다.: 당장은 아니더라도 언젠가는 확실히 그런 일이 일어납니다.

번역자 주: 개발 커널 버전 2.1 대에서 64메가 이상의 메모리를 자동으로 인식하게 하는 기능이 추가되어 테스트되고 있으므로 안정 커널 버전 2.2 대에서는 자동으로 대용량의 메모리를 인식시킬 수 있을 것이다.

3.2 두 장 이상의 이더넷 카드를 사용하려면 어떻게 하나요?

커널이 두 장 이상의 이더넷 카드를 인식하게 하려면 'ether=IRQ,i/o addr,device' 파라미터를 부팅할때 넘겨 주어야 합니다. 예를 들면

```
boot:  linux ether=5,0x320,eth0
```

또는 *lilo.conf*에 다음과 같이 추가해 줍니다.

```
image=/boot/vmlinuz
        label=linux
        append="ether=5,0x320,eth0"
        root=/dev/hda2
        read-only
```

이것은 커널에 통채로 컴파일되어 들어가 있는 이더넷 카드인 경우에만 작동할 것입니다. 만약 드라이버가 모듈로 컴파일되어 있다면 이 파라미터를 */etc/modules.conf* 파일에 설정해 주어야 합니다. 예를 들면

```
alias eth0 3c509
options eth0 irq=10
```

3.3 무엇 때문에 GCC가 "exiting on signal 11" 메시지를 내보내게 합니까?

이 내용에 관해서는 <http://www.bitwizard.nl/sig11/>에서 좋은 참고 자료를 얻을 수 있습니다.

3.4 윈도우즈에서만 사용할 수 있는 WinModem/WinPrinter를 리눅스에서 사용하려면 어떻게 하나요?

모든 **Win***주변기기들은 우리들을 골치아프게 만들죠. WinModem 이나 WinPrinter 를 리눅스에서 사용할 수 있는 방법은 없습니다. Win- 디바이스들은 매우 단순화되어 있어 많은 작업들이 특별한 윈도우즈 드라이버를 통해 이루어지기 때문입니다.

불행히도 WinModem 이나 WinPrinter를 만들어 내는 회사들은 MS로부터 자사의 프로그래밍 관련 정보들을 유출시키지 말도록 압력을 받고 있기 때문에 리눅스 프로그래머들이 정보를 얻어낼 수가 없습니다.

어떤 사람이 윈도우즈와 WinPrinter 사이의 데이터 스트림을 리버스 엔지니어링을 통해 WinPrinter 중의 하나를 리눅스에서 사용할 수 있도록 했다고 하는데 저는 이에 관해서 더이상 아는바가 없군요.

제 4 절 리눅스 소프트웨어 FAQ

4.1 시스템의 시간을 맞추려면 어떻게 하나요?

xntp패키지를 <http://www.eecis.udel.edu/~ntp/>나 혹은 다른 리눅스 관련 웹사이트에서 구해서 사용하시기를 권장합니다.

4.2 패치를 적용하는 방법을 가르쳐 주십시오

소스코드가 있는 디렉토리로 이동합니다. 그리고

```
patch < patchfile
```

또는 패치 파일이 다른 디렉토리에 있을때

```
patch < /path/to/your/patchfile
```

4.3 보통 많이 사용하는 패키지의 최신 버전은 어디서 구할 수 있습니까?

- SunSite UNC `<ftp://sunsite.unc.edu/pub/Linux>`
- Linux Archive Search `<http://torgo.ml.org/las>`
- Linux Software Map (지금은 좀 구식이 된 듯한 느낌) `<http://www.boutell.com/lsm>`
- Linux Applications and Utilities Page `<http://www.xnet.com/~blatura/linapps.shtml>`
- Walnut Creek - 슬랙웨어 리눅스 공식 홈사이트 `<ftp://ftp.cdrom.com/pub/linux/>`

9.1(부록 A)에 더 많은 정보가 있습니다.

4.4 센드메일(sendmail)과 관련한 FAQ

4.4.1 센드메일을 이용한 버추얼 전자우편 호스팅 서비스를 구축하려 합니다. 그런데 'mail loops back to me'라는 에러 메시지가 생기는군요.

sendmail.cf의 w 클래스를 살펴보시고 양쪽의 도메인네임이 모두 지정되어 있는지 확인하세요.(***/etc/sendmail.cw***의 Fw/file/name 에 지정되어 있는 파일이나 혹은 ***/etc/sendmail.cf***파일의 Cwhostnames... 라인에 이 내용이 지정되어 있어야 합니다.)

더 많은 정보를 얻고 싶을땐 `<http://www.sendmail.org/virtual-hosting.html>`을 참고하세요.

4.4.2 인터넷에 연결되어 있지 않은 오프라인상에서 사용하기 위한 센드메일의 설정 방법은 어떻게 됩니까?

sendmail.cf 파일의 가장 상단에 다음과 같은 내용을 추가하시고

```
O HoldExpensive=True
```

각각의 메일러(`smtp`, `smtp8`, `esmtp`, `relay`)의 'F=' 섹션에 'e' 플래그를 추가하세요. 예를 들면

```
Msmtp, P=[IPC], F=mDFMuXe, S=11/31, R=21, E=\r\n, L=990,
             T=DNS/RFC822/SMTP,
             A=IPC $h
```

그리고 센드메일 데몬을 시작시키는 명령에'`-q15m`' 같은 옵션을 포함하지 않도록 고쳐 줍니다.(센드메일을 `-bd -os` 옵션으로 실행시키기를 권장합니다. 더 많은 정보를 얻기 위해서는 센드메일 관련 문서를 참고하세요.) 이런 방법으로 메일 큐에 쌓여 있는 메일들을 여러분이 인터넷에 접속될 때 내보낼 수가 있게 됩니다.:

```
sendmail -q
```

4.4.3 UUCP를 통해 연결되어 있는 시스템에서 센드메일을 사용하려면 어떻게 설정해야 하나요?

이것은 그다지 간단히 답변될 수 있는 성질의 것이 아니지만 이 작업을 어떻게 행할 수 있는지, 그리고 어디서 관련 정보를 얻을 수 있는지 한번 이야기해 보죠.

주의: 이 섹션에서는 제가 현재 사용하고 있는 **sendmail 8.8.8** 을 기준으로 이야기하겠습니다. 다른 버전의 센드메일에서는 조금 다르게 적용될 수도 있지만 아이디어 자체는 똑같습니다.

1단계: 센드메일 소스를 <ftp://ftp.sendmai.org>에서 받아 오세요. 여기 포함되어 있는 툴들과 템플리트를 이용해서 설정 파일을 생성해 내어야 하기 때문입니다. <ftp://ftp.redhat.com>에서 rpm 패키지를 얻어 오셔도 됩니다. 저는 여러분들이 이미 센드메일 바이너리를 컴파일해서 설치해 두었다고 가정하겠습니다. 이제 ***sendmail.cf*** 파일을 생성해 내어야 할 차례입니다. 이 작업을 하기 위해서 ***sendmail-X.X.X/cf/cf*** 디렉토리 아래의 템플리트를 이용합니다. ***uucpproto.mc***라는 파일을 사용합니다. 이것을 다른 파일 이름***(예를 들면 myuucp.mc)***으로 바꾸어 복사해 둡니다. 보통 여기에 약간의 수정만 가하면 됩니다. 운영체제 타입을 정하고 **SMART_HOST**(메일 릴레이를 담당할 시스템 이름)을 결정합니다. 이 파일을 에디터로 열어서 다음 항목들을 수정해 줍니다.

```
OSTYPE: 예)OSTYPE(linux)dnl
FEATURE(nodns)dnl 추가: DNS가 없을때
MAILER(smtp)dnl 추가: uucp-dom 메일러도 함께 사용하고 싶을때
define(‘SMART_HOST’, uucp:YOUR_UUCP_ISP)dnl 을 파일 맨 끝에 추가
```

이제 거의 다 됐습니다. 여러분이 수정한 파일은 다음과 같이 보이겠죠.

```
OSTYPE(linux)dnl
FEATURE(nodns)dnl
MAILER(local)dnl
MAILER(smtp)dnl
MAILER(uucp)dnl

define(‘SMART_HOST’,uucp:YOUR_UUCP_ISP)dnl
```

이제 ***sendmail.cf*** 파일을 다음과 같이 생성합니다.

```
m4 ../m4/cf.m4 myuucp.mc > /etc/sendmail.cf
```

이제 해주어야 할 일은 센드메일이 DNS를 통해서 호스트네임을 찾지 않도록 하는 것입니다. 제 경험에 의하면 **FEATURE(nodns)dnl** 만으로는 충분하지가 않았습니다. 이것이 제대로 작동되게 하려면 ***/etc/service.switch*** 파일을 다음과 같이 만들어 줍니다.

```
hosts           files
aliases         files
```

이제 uucp 시스템이 제대로 설정되었다면(uuchk 로 확인해보기 바랍니다.) 센드메일 데몬 프로세스를 `/usr/sbin/sendmail -bd -q 15m` 또는 그 비슷한 명령으로 시작할 수 있습니다.

몇 개의 테스트 메시지들을 보내 보세요. 그리고 그 메시지들이 **YOUR_UUCP_ISP** 시스템의 ***uucp 디렉토리***에 제대로 쌓이는지 확인해 보고 만약 잘 안된다면 다시 앞으로 돌아가서 무엇이 잘못되었는지 확인해 보세요.(로그 파일이 매우 유용하게 쓰일 것입니다.)

이제 거의 다 됐습니다. 이제 해주어야 할 일은 시스템을 잘 설정해서 여러분의 ISP와 매 정해진 시간마다 이메일을 교환하도록 하는 것입니다. 몇 가지 방법이 있긴 하지만 저는 crontab 을 권장합니다.: 가장 간단한 방법은

```
0,15,30,45 * * * * /usr/sbin/uucico -S YOUR_UUCP_ISP
```

라는 줄을 crontab 에 추가해 주는 것입니다.(root 로긴한 상태에서 `crontab -e -u uucp` 라고 실행시키세요.) 이렇게 하면 매 15분마다 UUCP 쪽으로 접속을 할 것입니다.(crontab 과 비슷한 다른 방법에 대해서는 매뉴얼 페이지를 참고하세요.)

여기서 이야기한 것들은 충분한 설명이 되지 못합니다. 더 이상의 정보를 다음 웹사이트들을 통해서 얻을 수가 있으니 참고하세요.

- Sendmail+UUCP Mini HOWTO
- FreeBSD FAQ Section `<http://www.freebsd.org/FAQ/FAQ113.html##113>`
- Solaris 2 FAQ `<http://www.wins.uva.nl/pub/solaris/solaris2>`
- Sun managers Summaries `<http://www.latech.edu/sunman.html>`
- List of USENET FAQs `<http://www.cis.ohio-state.edu/hypertext/faq/usenet/unix-faq/top.html>`
- Sun World Online `<http://www.sun.com/sunworldonline/common/swol-siteindex.html>`
- Unix Guru Universe `<http://www.ugu.com>`
- Stokeley Consulting `<http://www.stokely.com>`

4.5 POP3 사용자들에게 'already being read' 라는 에러 메시지가 생깁니다.

*/var/tmp/.pop/<username>*을 지워 버리세요. 더 좋은 방법은 `pop3d` 배포본에 들어 있는 `rm_stale.sh` 스크립트를 `cron`등을 통해 주기적으로 실행하는 것입니다.

특정 리눅스 배포본, 특히 **슬랙웨어 3.3과 3.4**에서는 ***/var/tmp/.pop* 디렉토리**가 없는 것으로 밝혀져 이것 역시 에러 메시지의 원인이 되기도 합니다. 이 디렉토리가 제대로 소유자와 그룹 퍼미션이 설정되어 있는지 확인해 보세요.

4.6 서머타임에서도 제대로 동작하기 위해서 시간 설정을 어떻게 해 주어야 합니까?

1.
```
cd /usr/lib/zoneinfo
rm localtime posixrules posixtimes
ln -s /etc/localtime localtime
ln -s /etc/localtime posixrules
ln -s /etc/localtime posixtimes
```

2.
```
cd /etc
rm localtime
ln -s /usr/lib/zoneinfo/Europe/Copenhagen localtime
```

3.
```
/etc/rc.d/boot.local(Suse 5.1의 경우)을 수정해 다음과 같은 라인을
추가해 줍니다.

clock -a
echo "System time: $(date)"

/etc/init.d/local(Unifix 2.0)을 수정해 다음과 같은 라인을
    추가해 줍니다.
```

```
test -f /etc/adjtime || echo "0.0 0 0.0" >/etc/adjtime
clock -a
echo "System time: $(date)"

/etc/rc.d/rc.local(레드햇, 슬랙웨어, 데비안....)을 수정해 다음과
    같은 라인을 추가해 줍니다.

#test -f /etc/adjtime || echo "0.0 0 0.0" >/etc/adjtime
clock -a
echo "System time: $(date)"?
```

4. TZ 가 정의되어 있는 곳은 모두 바꾸어 주어야 합니다. TZ 가 정의되어 있어서는 안되는 것이죠.

```
cd /etc
find . -exec grep -ln TZ {} 2>/dev/null \;
TZ 가 정의되어 있는 곳에 #를 붙여 줍니다.

예를 들면
/etc/ENVIRONMENT        (unifix)
/etc/profile*           (suse, unifix)
/etc/login.defs         (suse, unifix)
```

5. 리부트(혹은 clock -a 를 수동으로 실행)

4.7 리눅스 시스템에서, 윈도우즈 시스템들과 공유하고 있는 리소스들에 접근하기 위해서는 어떻게 하나요?

FAQ 5.7(4.7)/5.8(4.8)을 참고하세요.

4.8 'ls' 를 칼라풀하게 만들려면 어떻게 해야 합니까?

다음 내용을 ***$HOME/.bashrc*** 파일에 추가합니다.

`alias ls = 'ls --color'`

만약 bash가 아닌 다른 쉘을 사용한다면 그 쉘의 rc 파일에 같은 내용을 넣어 주면 됩니다.

제 5 절 리눅스 시스템 관리 FAQ

5.1 root 의 패스워드를 잊어버렸습니다. 어떻게 로그인할 수 있습니까?

몇 가지 방법이 있죠. 가장 쉬운 방법은 시스템을 셧다운하고 쉘 프롬프트로 진입한 다음 루트 패스워드를 바꾸면 됩니다.

쉘 프롬프트로 진입하려면

```
boot: linux init=/bin/sh
```

루트 패스워드를 바꾸기 위해서는

```
bash# mount -o remount / -rw
bash# passwd root
```

주의: 루트 파티션을 수정하기 위해서는 루트 파티션을 읽기/쓰기 가능 모드로 마운트해야 합니다.

5.2 /etc/passwd 에 쉘 지정을 잘못하여 존재하지 않는 쉘을 지정하였습니다. 어떻게 로그인할 수 있습니까?

시스템을 셧다운하고 5.1(FAQ 4.1)에 나온 방법처럼 쉘 프롬프트로 진입한 뒤 쉘을 제대로 지정해 줍니다.

```
bash# chsh root
```

5.3 시스템 시작 스크립트에서 &를 붙이는 것을 잊어버렸습니다. 어떻게 이것을 백그라운드 모드로 전환해줄 수 있나요?

시스템을 셧다운하세요. 그리고 5.1(FAQ 4.1)에 나온 방법을 써서 쉘 프롬프트로 진입한 후 스크립트를 편집하세요.

5.4 싱글 유저 모드로 전환하려면 어떻게 합니까?

부트 이미지에 **single** 파라미터를 넘겨주면 됩니다.

```
boot: linux single
```

5.5 리눅스 시스템을 통해서 윈도우즈95 시스템이 인터넷을 사용하도록 해주는 IP masquerading 기능을 어떻게 설정합니까?

5.6 저는 (전화선을 통해) 한 개의 IP 어드레스만을 할당받아 사용하고 있습니다. 리눅스를 사용해서 두 대 이상의 컴퓨터가 인터넷을 동시에 사용할 수 있도록 설정하려면 어떻게 하나요?

이런 네트워킹 관련 문제에 대해서 리눅스는 최상의 솔루션을 제시해 줍니다. **IP_Masquerading** 기능이 현재 커널에 구현되어 있기 때문입니다. 여기 기술된 방법이 특별히 어렵진 않지만 이 FAQ의 범위를 벗어납니다. 이 문제에 관해 잘 설명해 둔 웹페이지들이 많이 있습니다. *IP Masquerade Resource* `<http://ipmasq.home.ml.org>`에서 정보를 찾으실 수도 있고 IP masquerading 기능을 통해서 작동하는 응용프로그램들에 대해서 알고 싶다면 *Masq Apps* `<http://dijon.nais.com/~nevo/masq>`을 방문해 보셔도 좋습니다.

IP masquerading 기능 대신 더 탄력적인 ipchains을 이용하실 수도 있습니다. 이것들은 **개발 버전 커널 2.1.102**에서부터 구현되어 왔는데 안정 커널 버전 2.0.33 에서 적용할 수 있는 패치도 있습니다. ipchains 홈페이지는 `<http://www.adelaide.net.au/~rustcorp/ipfwchains>`입니다.

5.7 리눅스 시스템에 있는 파일이나 프린터를 윈도우즈 시스템과 공유하려면 어떻게 합니까?

5.8 윈도우즈 시스템에 있는 파일이나 프린터를 리눅스 시스템과 공유하려면 어떻게 합니까?

SAMBA를 사용하십시오. *SMB-HOWTO* `<http://samba.anu.edu/au>`문서를 한번 읽어보시는것도 좋습니다. 프린터 설정에 관해서는 *Printing-HOWTO* `<http://sunsite.unc.edu/pub/Linux/docs/HOWTO/Printing-HOWTO>`도 같이 참고하세요.

5.9 부팅할때 "Can't find module XXXX-XXX" 라는 메시지가 계속 뜹니다. 별로 시스템이 문제를 일으키지는 않는데 어떻게 하면 좋을까요?

/etc/conf.modules 파일을 편집해서 다음과 같은 내용을 추가합니다.

```
alias module XXXX-XX           off
alias module XXXX-XX           off
```

주의: */etc/modules.conf* 파일이나 */etc/conf.modules* 파일이 없으면 만들어 주어야 합니다.

5.10 제 리눅스 시스템으로 telnet/FTP 접속을 시도하면 접속이 되지 않습니다.

5.10.1 제 리눅스 시스템으로 telnet/FTP 접속을 시도하는데 접속 시간이 너무 오래 걸립니다.

`reverse DNS`를 설정하시거나 */etc/hosts* 를 사용하세요.

5.11 root가 아닌 다른 사용자에 의해 제어되는 프로세스를 시스템이 부팅할때 시작하게 하려면 어떻게 합니까?

다음과 같은 라인을 */etc/rc.d/rc.local*에 추가합니다.

```
cd /path/to/program
su <username> -c <command>
cd
```

예를 들면 사용자 *'bob'* 소유의 프로세스 *'talker'*를 실행하려면

```
cd /home/bob
su bob -c ./talker &
cd
```

5.12 특정 사용자가 제 리눅스 시스템으로 telnet/FTP 를 통한 접속을 하지 못하게 하고 싶습니다.

텔넷 접속을 거부할 해당 사용자의 로긴 쉘을 */dev/null*로 바꾸어 버리면 됩니다. 만약 ftp 접속은 허용해 주려면 */etc/shells* 파일에 /dev/null 을 추가해 줍니다. 또는 여러분 자신의 스크립트를 만들어(로긴을 시켜주고 메시지를 뿌려주고......) 그것을 사용자의 쉘로 지정해 주면 됩니다.

특정 사용자가 ftp 서비스를 받지 못하게 하려면 그 사용자의 쉘을 ***/etc/shells에서 제거***하거나 혹은 그 사용자를 */etc/ftpusers*에 추가하면 됩니다.

TCP 래퍼 `<ftp://ftp.win.tue.nl/pub/security/index.html>`에 관해서도 살펴보셔야 합니다.

또한 **유저레벨 방화벽(ULF)**이라는 것도 있습니다.

5.13 저는 리눅스/윈도우즈95/윈도우즈NT를 모두 가지고 있습니다. 리눅스가 부팅할때 윈도우즈 쪽의 드라이브를 긴 파일 이름이 보존된 채로 마운트되게 하고 싶습니다. 어떻게 하면 됩니까?

`'msdos'`가 아닌`'vfat'`으로 마운트된 윈도우즈 드라이브는 긴 파일 이름을 그대로 사용할 수 있게 해 줍니다. */etc/fstab* 에 정의된 'msdos' 타입을 'vfat' 으로 바꾸어 주어야 합니다. vfat 이 자동으로 마운트되도록 하려

면 */proc* 이 vfat 관련 내용보다 앞에 위치해야 합니다. NTFS와 FAT 32 지원은 아직 베타 테스팅 중이라는 것을 명심하십시오. **따라서 FAT 16 드라이브만이 2.0 대의 커널에서 지원됩니다.**

```
Before:

/dev/hdc1       /               ext2    defaults        1 1
/dev/hda1       /c              msdos   defaults        0 0
/dev/hdc2       swap            swap    defaults        0 0
/dev/fd0        /mnt/floppy     ext2    noauto          0 0
/dev/cdrom      /mnt/cdrom      iso9660 noauto,ro       0 0
none            /proc           proc    defaults        0 0


After:

none            /proc           proc    defaults        0 0
/dev/hdc1       /               ext2    defaults        1 1
/dev/hda1       /c              vfat    defaults        0 0
/dev/hdc2       swap            swap    defaults        0 0
/dev/fd0        /mnt/floppy     ext2    noauto          0 0
/dev/cdrom      /mnt/cdrom      iso9660 noauto,ro       0 0
```

Win95 osr2 와 Win98(NT4 제외)는 "fat32"를 파일시스템으로 사용하도록 선택할 수 있습니다. 이것을 마운트하기 위해서는 fat32 지원이 커널에 포함되어 있어야 합니다. (커널 패치 작업 필요) 이 방법은 Win95 드라이브가 FAT16 으로 포맷되어야 제대로 적용할 수 있다고 알려져 있습니다. 커널 2.0.33 이전 버전에서는 패치를 따로 가해 주어야 하지만 2.0.34 에서는 vfat32 지원이 포함되어 있을 것입니다. vfat32 와 관련된 추가 정보는 <http://bmrc.berkeley.edu/people/chaffee/fat32.html>에서 구하실 수 있습니다.

5.14 동시에 로긴할 수 있는 횟수를 제한하려면 어떻게 하나요?

이것을 가능하게 해 주는 툴은 배포본에 포함되어 있지 않고 프로그램을 따로 구해야만 합니다. 현재로서는 두가지 선택이 있는데 clobberd와 idled가 바로 그것입니다. 둘 다 매우 자세한 부분까지 설정해줄 수 있고 특정 유저나 그룹에 대해 타임아웃(idle) 과 같은 파라미터를 제어할 수도 있습니다. 둘 다 <ftp://sunsite.unc.edu>등의 유명 리눅스 아카이브에서 구할 수 있습니다.

5.15 사용자의 유휴 시간(idle time)을 제한하려면 어떻게 합니까?

5.14(FAQ 4.14)와 동일.

5.16 "Shadow password"와 "Shadow suite" 가 무엇입니까?

몇몇 리눅스 배포본을 포함한 특정 유닉스 시스템에서는 암호화된 패스워드가 누구든지 읽을 수 있는(패스워드 파일은 그렇게 되어 있어야 합니다.) */etc/passwd*파일에 저장됩니다. 셰도우 패스워드 시스템에서는 암호화된 패스워드가 /etc/passwd 파일에서 지워지고 root 만이 읽을 수 있는 */etc/shadow*라는 파일에 따로 저장됩니다. 따라서 이렇게 해 두면 패스워드를 해킹하는 것이 더욱 어려워지게 됩니다.

제 6 절 리눅스 내부 구조 FAQ

6.1 좀비(zombie) 프로세스란 무엇입니까?

자식 프로세스(child process)가 종료하면 부모 프로세스(parent process)는 그것을 다시 거두어 들이게 되어 있습니다. 즉 자식 프로세스가 종료하면 그 상태를 리턴받아 체크한다는 뜻이죠.

좀비 프로세스는 부모 프로세스로가 거두어 들이지 못한 프로세스들입니다. 이것들은 메모리를 차지하지 않고 디스크 용량, IO, CPU 시간 또한 전혀 차지하지 않고 다만 이 프로세스들은 **프로세스 테이블의 용량만을 차지하고 있습니다**. 보통 이것은 별 문제가 되지는 않습니다만 프로세스를 거의 한계 용량에 다다를 정도로 많이 실행시키는 부하가 많이 걸리는 시스템의 경우, 혹은 자식 프로세스를 많이 만들어 내기만 하고 거의 거두어들이지 않는 그런 상황일 경우 문제가 될 수 있습니다.

이것은 대부분 소프트웨어의 버그이며 시스템 크래쉬의 원인이 될 수도 있습니다. 부모 프로세스가 종료될 때 아직 거두어들이지 못한 자식 프로세스들은 모두 init 프로세스에 의해 거두어들여지게 되는데 이 과정은 시스템 로드가 많이 걸려있는 상황에선 오랜 시간이 걸릴 수도 있습니다. 많은 좀비 프로세스들이 매우 나쁜 영향을 미칠 수 있습니다. 왜냐하면 그 프로세스들은 여러분이 그 프로세스를 깨끗이 끝내기 위해서 실행해야 할 명령을 제대로 실행되지 못하게 할 수도 있기 때문입니다. **만약 그런 일이 생긴다면 셧다운만이 유일한 해결책입니다.**

또는 `ulimit`을 이용해서 위험한 작업을 수행할 때에는 미리 한계를 지워 줄 수도 있습니다.

6.2 커널을 새로 컴파일하고 부팅했더니 "kernel panic - no root device" 라는 메시지가 뜹니다. 뭐가 잘못된 건가요?

커널 컴파일시에 루트 디바이스를 제대로 설정했는지 확인하세요. 여러분이 `ramdisk`를 사용하지 않는다면 이 디바이스 드라이버는 모듈로 설정될 수가 없습니다.(이 경우에 모듈은 아직 마운트되지 않은 루트 디바이스에 위치하고 있기 때문입니다.)

`rdev`명령으로 루트 디바이스를 지정해줄 수도 있습니다.

여러분의 예전 커널로도 부팅할 수 있도록 lilo.conf 에 설정해 두고 문제가 생길 경우 예전 커널로 부팅하도록 해두기를 강력히 권장합니다.

제 7 절 리눅스 보안 FAQ

7.1 리눅스 시스템 보안의 기본 사항은 무엇입니까?

좋은 질문입니다. 시스템 보안은 모든 시스템 관리자들에게 아주 중요한 문제죠. 몇 가지 살펴보자면

로그 파일들을 잘 읽어보라: `syslog`메시지들, ***/var/adm* 디렉토리의 *.log 파일들**

패치를 제때 적용하라: 새로운 버전이 공개되면 업그레이드하고 패치한다.

보안 관련 소프트웨어를 사용하라: TCP 래퍼, COPS, Tripwire 등을 사용한다.

보안 관련 메일링리스트에 가입.

특히 UNIX 보안 관련 메일링 리스트 (예: `bugtraq@netspace.org`또는 `linux-security@redhat.com`)

7.2 무작위/안전한 패스워드를 만들려면 어떻게 합니까?

```
head -c 6 /dev/random | mmencode
```

또는 `mkpasswd`

7.3 리눅스의 보안 상태는 어떤가요? 누군가 리눅스는 버그가 많고 보안에 약하다고 얘기하던데......

UNIX 시스템의 보안은 항상 시스템 관리자가 얼마나 열심히 하느냐에 달려 있습니다. 더욱 많은 서비스를 제공할수록 보안 문제가 야기될 확률이 높아지죠.

SCO 나 다른 비슷한 운영체제들은 더욱 사용자들을 편리하게 하기 위해 운영체제 자체의 내부 동작과 연관되어 있는 많은 서비스들을 제공하기 때문에 보안에 더욱 약하다고 할 수 있습니다. 리눅스 자체는 매우 안정적이고 보안에 강하지만 여러 다른 배포본으로 제공되기 때문에 예를 들면 레드햇과 슬랙웨어를 서로 좋아하는 사용자들이 어느 배포본이 더 보안이 잘 되어 있는지에 관해 논쟁을 벌이기도 했죠.

리눅스를 설치할 때는 최소한의 프로그램만을 설치하고 차츰 필요한 프로그램을 조금씩 추가해 나가면서 응용 프로그램이 야기할 수 있는 보안 문제의 가능성을 최소한으로 줄여 볼 수 있습니다. 리눅스는 제대로 구현된다면 아주 강력한 보안 기능을 제공해 줍니다. 만약 명백한 문제가 있다면 수천명의 자원봉사자들이 즉각 그것을 해결 방법과 함께 지적해 주고 있습니다.

몇몇 상용 프로그램들과 같은 대형 조직들은 그런 문제를 해결할 사람들이 제한된 팀으로 구성되어 있기 때문에 자기들이 발견한 것에 대해 다른 사람들에게 알리는 것을 꺼려하는 경우가 많습니다. 또한 그런 문제점을 해결할 수 있는 패치나 업그레이드 버전을 내놓는 일이 상당히 오랜 시간을 요할 수도 있습니다. 그렇습니다. 그런 수정 사항은 곧 이용할 수 있게 되긴 하지만 많은 상용 프로그램의 관리자들은 자신들이 좀더 잘 설계되고 제작된 프로페셔널 소프트웨어를 사용하고 있다고 잘못 생각하면서 최초 배포본에 포함되어 있는 내용만을 사용하는 경향이 있습니다. **실수는 어느 프로그래밍 레벨에서도 일어날 수 있습니다.**

그렇지만 수천명의 사람들이 읽어볼 수 있는 소스코드가 있다면 이런 실수들은 좀더 빨리 발견될 수 있습니다. 물론 소스코드를 이리저리 조작해 보는 사람들도 그만큼 많아질 것입니다. 지금 약 700만 카피 정도의 리눅스가 이용되고 있으니 누군가 그런 보안 문제를 야기해낼 가능성도 그만큼 크죠.

Michael - The Web Administrator(`wwwadmin@wizard.ca`)

7.4 스팸메일을 추적하려면 어떻게 하나요?

인터넷이 발전함에 따라 많은 사람들이 스팸메일 때문에 고생하고 있습니다. 간단히 이 문제에 대해서 살펴보죠.

여기 스팸 추적과 관련한 간단한 예가 있습니다. (D. J. Vanecek(`djv@bedford.net`) 제공)

```
이 스팸은 스팸 헤더에 적힌 시간에 수신되었습니다. 추적은 간단합니다.

| From sales@canus.net  Sat Jun 27 02:42:41 1998
| Return-Path: <sales@canus.net>
| Received:  XXXXXXXXXXXXXXXXXXXXX CENSORED XXXXXXXXXXXXXXXXXXX

이것은 무시하세요.

| From: sales@canus.net
| Received: from CENSORED XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
|       by castor.loco.net (fetchmail-4.3.8 POP3)
|       for <djv/castor.loco.net> (single-drop); Sat, 27 Jun 1998 02:42:41 EDT pop을 통해서 메일을 수신했다는 것을 나타냅니다.
| Received: from server ([199.174.152.215]) by XXXXXXXXXXXXXXXXXXXXXXXXXXXX
|       with SMTP (IPAD 1.52/64) id 4950800 ; Sat, 27 Jun 1998 02:39:13 EST
```

이 헤더는 중요한 정보를 담고 있습니다. 이것은 내가 이용하는 ISP 측에서 스패머로부터 메일을 받고 있거나 혹은 스팸메일을 중계해주는 서버로부터 메일을 받고 있다는 것을 나타냅니다. 여기서는 그것이 어느 서버인지 알 수는 없습니다. **ISP 에서는 IPAD를 사용하고 있습니다.**따라서 우리는 메일 수신 시간이 제대로 되어 있다고 확신할 수가 없게 되었습니다.(중요)

```
| Date: Sat, 27 Jun 1998 01:00:59
```

여기서의 날짜는 옳을 수도 있고 그렇지 않을 수도 있습니다. 이 정보는 스팸메일을 추적하는 것과는 아무 상관이 없을지도 모릅니다. 왜냐면 이 정보는 주로 스패머의 시스템에서 생성되기 때문에 믿을 수가 없죠.

```
| Subject: Need A Loan?
| Message-Id: <199806270639.4950800@XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX>
| Apparently-To: XXXXXXXXXXXXXXXXXXXXXXX (me, correct email was here)
```

To: 헤더가 없는 것으로 봐서 한꺼번에 많은 메일을 날리는 것으로 해석할 수 있습니다.

```
| Status: RO
|
|    Are You in Debt?
|
|    If you are then we can help!
|    Qualifying is now at your fingertips and there are no
|    long distance calls to make or travel plans to arrange.
|
|    We are American Capital Corporation, and as you may have seen in our ad,
|    you can be loaned up to 125% of the value of  your home or up to $100,000.00
|    even if you have NO equity in your home!
|    There are NO up-front or advanced fees of any kind!
|    You can be approved WITHIN 24 hours and
|    have your cash in one weeks time!
|
|    We will provide you with a FREE loan evaluation, without obligation.
|    All you need do is go to our website and answer a short questionnaire.
|    One of our registered lenders will assess your information and give you
|    a personal call within 48 hours telling you how we can help you!
|
|    You are never under any obligation to use our services, but they are
|    there for you!
|
|    For complete information, please visit our website at:
|                     http://www.canus.net/amcap/129.html
```

나중에 이 웹사이트를 방문하게 됩니다.

```
|
|    Our business is helping people. May we help you?
```

이 스팸메일이 어디로부터 날아왔는지 알아봅시다. 우리는 메일 헤더로부터 199.174.152.215 의 IP 어드레스를 가진 머신이 스팸메일을 날려보내는 데 사용되었음을 알 수 있었습니다. ping 메시지를 보내 보았지만 반응이 없었습니다.

nslookup을 사용해 보니

```
[djv@castor djv]$ fg -
nslookup
199.174.152.215
Server:  localhost
Address:  127.0.0.1
```

```
Name:    dd35-215.dub.compuserve.com
Address:  199.174.152.215

>
```

따라서 이 스패머는 컴퓨서브 "throwaway" 계정을 이용하고 있다는 사실을 알아 냈습니다. 이것은 IP 어드레스가 유동적으로 변하는 다이얼업 접속인것 같군요. traceroute을 이용해본 결과 접근이 되지 않는 걸로 봐서 스패머는 어디론가 도망쳤다고 볼 수 있습니다. 비슷한 사이트인 199.174.152.1 로 traceroute 을 적용해볼 결과

```
[djv@castor djv]$ traceroute 199.174.152.1
traceroute to 199.174.152.1 (199.174.152.1), 30 hops max, 40 byte packets
 3  bordercore4-hssi5-0-24.NorthRoyalton.mci.net (166.48.232.97)  159.816 ms 658.176 ms  730.623 ms
 4  core2.WillowSprings.mci.net (204.70.4.177)  159.222 ms  158.668 ms 149.832 ms
 5  borderx1-fddi-1.WillowSprings.mci.net (204.70.104.52)  239.834 ms  298.712 ms  330.386 ms
 6  compuserve.WillowSprings.mci.net (204.70.104.102)  169.325 ms  148.648 ms 149.875 ms
 7  core-fddi0.chi.compuserve.net (205.156.223.161)  239.890 ms  158.549 ms 149.933 ms
 8  atm1-06-core.dub.compuserve.net (205.156.223.113)  159.801 ms  148.613 ms 149.868 ms
 9  fddi0-ppp-2.dub.compuserve.net (205.156.223.72)  149.805 ms  148.702 ms 149.804 ms
10  dub-dial-10.compuserve.net (206.175.65.25)  149.789 ms  148.658 ms 149.977 ms
11  dd10-001.dub.compuserve.com (199.174.152.1)  399.829 ms  478.724 ms 400.485 ms
[djv@castor djv]$
```

이 결과는 이 스패머가 컴퓨서브 계정을 통해서 스팸을 뿌렸다는 우리의 믿음을 더욱 확고하게 해 줍니다.

그렇지만 이 스패머에 관한 다른 정보는 어디 있나요?

"canus.net" 은 누구입니까? 그쪽도 추적해 보아야 하나요?

"canus.net" 으로 traceroute 명령을 적용해본 결과

```
|  3  bordercore4-hssi5-0-24.NorthRoyalton.mci.net (166.48.232.97)  169.821 ms 138.943 ms  149.408 ms
|  4  core3.Atlanta.mci.net (204.70.4.9)  279.872 ms  358.830 ms  369.607 ms
|  5  ast-uunet-nap.Atlanta.mci.net (206.157.77.114)  159.785 ms  138.895 ms 159.844 ms
|  6  104.ATM2-0-0.XR1.ATL1.ALTER.NET (146.188.232.50)  139.872 ms  158.687 ms 139.946 ms
|  7  195.ATM5-0-0.GW1.MIA1.ALTER.NET (146.188.232.137)  179.745 ms  188.757 ms  199.900 ms
|  8  bs-miami-gw.customer.alter.net (157.130.65.222)  199.871 ms  208.626 ms 199.989 ms
|  9  207.203.0.160 (207.203.0.160)  199.758 ms  188.954 ms  209.890 ms
| 10  172.25.80.90 (172.25.80.90)  199.859 ms  199.436 ms  199.321 ms
| 11  205.152.190.251 (205.152.190.251)  189.876 ms  218.826 ms  229.904 ms
```

여기 마지막 부분에 적혀있는 호스트는 IP 어드레스로부터 도메인 네임으로의 변환이 불가능한 호스들이며 마지막 라인은 canus.net 의 IP 어드레스입니다. whois canus.net 을 실행해본 결과는 다음과 같습니다.

```
| Registrant:
| CanUS Net (CANUS2-DOM)
|    1 First ST West
|    Gander, NFL D3K J7P
|    CA
```

여기 적힌 바에 따르면 이 회사는 캐나다에 위치하고 있군요. 사업은 미국에서 하고 있으면서 왜 이렇게 멀리 떨어진 곳에 위치하고 있을까요?

```
|
```

```
|    Domain Name: CANUS.NET
|
|    Administrative Contact:
|       Franklin, Bob  (BF3584)  dehal@USA.NET
|       360-695-3850
|    Technical Contact, Zone Contact:
|       Franklin, Bob  (BF3585)  dontcomplaintome@USA.NET
```

전자우편 주소가 나와 있으니 좋은 단서가 될수 있습니다.

```
|       360-695-3850
|    Billing Contact:
|       Franklin, Bob  (BF3584)  dehal@USA.NET
|       360-695-3850
```

여기 전자우편 주소가 **USA.NET**이라는 사실에 주목해야 합니다. 그들은 자신들이 등록한 도메인의 전자우편 주소를 이용하지 않고 있으며 고정된 이메일 주소를 이용하지 않습니다. 여기 적혀있는 전화번호 또한 허위일 가능성이 매우 높죠. 여기 적혀있는 사람(Bob Franklin)이 스패머입니다.

이 사람은 모든 연락을 거부합니다. 전화도, 메일도, 다른 어떤 방법으로도 연락이 되지 않습니다. 스팸 메일을 뿌리는 사람들의 전형적인 특징이죠.

스팸메일을 뿌리고자 하는 나라가 아닌 다른 나라에 위치한다. 컴퓨서브나 아메리카 온라인(AOL), 스프린트넷 등의 대형 ISP 계정을 이용한다.

```
|
|    Record last updated on 19-Jun-98.
```

스팸메일을 위한 도메인이 매우 최근에 개설되었습니다. 겨우 일주일 전이군요. 아마도 이 도메인은 곧 없어져도 괜찮다고 이 스패머는 생각할 것입니다. 이것은 커다란 스팸메일을 뿌리는 사람들의 전형적인 습성입니다.

```
|    Record created on 19-Jun-98.
|    Database last updated on 26-Jun-98 04:01:02 EDT.
|
|    Domain servers in listed order:
|
|    NS1.NAMESERVER1.NET                205.152.190.208
|    NS2.NAMESERVER1.NET                205.152.190.209
```

누군가가 이 스패머에게 DNS 서비스를 제공하고 있습니다. 만약 이 서비스를 제공하는 곳이 믿을만한 곳이라면 그쪽으로 스팸메일을 보내고 있는 도메인에게 서비스를 제공하고 있다고 알려 주어야 합니다.

```
|
| The InterNIC Registration Services database contains ONLY
| non-military and non-US Government Domains and contacts.
| Other associated whois servers:
|    American Registry for Internet Numbers - whois.arin.net
|    European IP Address Allocations        - whois.ripe.net
|    Asia Pacific IP Address Allocations    - whois.apnic.net
|    US Military                            - whois.nic.mil
|    US Government                          - whois.nic.gov
```

이제 누가 이 스패머에게 DNS 서비스를 제공하고 있는지 알아보기 위해 whois 서비스를 이용합니다.

```
whois 205.152.190.
```

결과는 다음과 같습니다.

```
| [No name] (MORR-HST)          MORRISON.PHICOM.NET            205.152.190.130
| [No name] (DRAKE4-HST)                DRAKE.PHICOM.NET 205.152.190.131
| [No name] (NS19481-HST)               NS.DCSOUTHFLORIDA.COM 205.152.190.2
| [No name] (NS41802-HST)               NS1.NAMESERVER1.NET 205.152.190.208
| [No name] (NS42268-HST)               NS2.NAMESERVER1.NET 205.152.190.209
|
| To single out one record, look it up with "!xxx", where xxx is the
| handle, shown in parenthesis following the name, which comes first.
|
| The InterNIC Registration Services database contains ONLY
| non-military and non-US Government Domains and contacts.
| Other associated whois servers:
|    American Registry for Internet Numbers - whois.arin.net
|    European IP Address Allocations        - whois.ripe.net
|    Asia Pacific IP Address Allocations    - whois.apnic.net
|    US Military                            - whois.nic.mil
|    US Government                          - whois.nic.gov
|
```

"Phicom.net" 에서 이 스패머에게 DNS 서비스를 제공해 주고 있는것 같습니다. 여기는 또 어떤 곳인지 알아보기 위해 whois 서비스를 또 이용합니다.

```
whois phicom.net

| Registrant:
| Phicom, Inc (PHICOM-DOM)
|    1370 W. Flagler St  Suite C
|    Miami, Florida 33135
```

주소에 적힌 대로 플로리다주 마이애미에 위치한 임대 사무실에 있군요. 아마도 스패머는 이곳에 살고 있을 가능성이 매우 높습니다.

```
|
|    Domain Name: PHICOM.NET
|
|    Administrative Contact, Technical Contact, Zone Contact:
|       Dominguez, Alvio  (AD1820)  Alvio124@PHICOM.NET
|       305-642-2638 (FAX) 305-541-0608
|    Billing Contact:
|       Baptista, Daniel  (DB5797)  Daniel34@PHICOM.NET
|       305-642-2638 (FAX) 305-541-0608
|
|    Record last updated on 30-Apr-97.
|    Record created on 02-Apr-97.
|    Database last updated on 26-Jun-98 04:01:02 EDT.
```

이곳은 등록한지 일년이 넘었군요. 여기서는 스팸메일을 한번 뿌리고 치고 빠지기 식의 그런 행동은 하지 않을 것입니다.

```
|
|    Domain servers in listed order:
|
|    MORRISON.PHICOM.NET                205.152.190.130
|    DRAKE.PHICOM.NET           205.152.190.131
|
|
| The InterNIC Registration Services database contains ONLY
| non-military and non-US Government Domains and contacts.
| Other associated whois servers:
|    American Registry for Internet Numbers - whois.arin.net
|    European IP Address Allocations        - whois.ripe.net
|    Asia Pacific IP Address Allocations    - whois.apnic.net
|    US Military                            - whois.nic.mil
|    US Government                          - whois.nic.gov
```

이제 www.phicom.net 으로 lynx 웹브라우저를 이용해서 한번 접속해 보겠습니다. 홈페이지가 있을것 같은데 다음과 같은 내용의 홈페이지를 가지고 있군요.

```
|
|      [INLINE] 1380 W. Flagler St. Miami, FL 33135 1(888) 642-2NET (305)
|                                642-2638
```

NIC 에 등록된 정보와 일치합니다.

```
|
|                 You are the [INLINE] visitor to our site.
|
|    * World Wide Internet/Access  * U.S. Robotics X 2 technology * Local /
|      Wide / Global Area Networks * Hardware / Software Sales * Web Site
|    Hosting & Construction * Service Repair Center * IBM Business Partner
|                 * Hewlett Packard Warranty Service Center
|
|
|
```

여기는 합법적인 ISP 인것 같습니다. 하드웨어 관련 사업도 함께 하고 있군요. IBM이나 HP같은 대형 회사의 계열 회사라면 이곳이 스팸메일을 위한 도메인으로 활용되진 않을 가능성이 크죠. 따라서 이쪽에다 스패머에게 DNS 서비스를 제공하고 있는 것에 대해 알려 주어야 합니다.

스팸메일에 적혀있는 웹페이지는 어디일까요? 거기도 한번 방문해 봅시다. http://www.canus.net/amcap/129.html 이었죠. 거기로 가보겠습니다.

```
|                                  [INLINE]
|                              Mortgage Services
|
|
|
|                              Are you in debt?
|
|    If you are then we can help. Qualifying is now at your fingertips and
|    there are no long distance calls to make or travel plans to arrange.
|
|    As you may have seen in our ad you can be loaned up to 125% of the
```

```
|    value of your home or $100,000.00 even if you have NO equity in your
|    home. There are no up-front or advanced fees of any kind. You can be
|    approved within 24 hours and have your cash in one weeks time.
|
|    In order for us to provide you with a FREE loan evaluation we must ask
|    for the following so that a representative can contact you via the
|    telephone within 24-48 hours.
|         * indicates required fields
|        *Name    ____________________
|        *Address ____________________
|                  ____________________
|         *City   ____________________  *State ___  *Zip __________
|        *Home Phone       ____________________
|          Work Phone       ____________________
|         *Email Address   ____________________
|        Best Time to Call ____________________
|            Type of Home  [None Selected......]
| Estimated Value of Home  ____________________
| Current Debt Against
| Home(Loan Balance):      ____________________
| Type of Loan Requested   [None Selected.....]
| Amt. of Loan Requested   ____________________
| Total Household Income   ____________________
|        Credit Rating   [None Selected]
|
|    To send this information to American Capital, press the Submit button;
|         To clear this form and start again, press the Reset button.
```

그들은 여러분의 신상에 관한 자세한 정보를 요구하면서도 자신들에 대해서는 별로 밝히지 않고 있습니다. 조심해야 합니다.

```
|
| SubmitReset
|
|                              About our company:
|
|    We are a FREE national referral service for homeowners seeking to
|    consolidate their bills. We have a network of affiliated companies
|    that are regarded as the best and most respected mortgage banking
|    companies in the country. You can rest assured that you are in good
|    hands and will receive extraordinary service with our affiliated
|    companies, for we only allow in our association and work with the
|    absolute best companies in the nation.
|
|                             You may reach us at:
|
|                      American Capital Mortgage Services
|                                1-212-796-6549
|
|
|                        We do not promote SPAM or UBE.
|             Please be assured that we are doing everything we can
|               to ensure that our users do not abuse this policy.
|
```

이쪽으로 어떻게 접속할 수 있는지 알아보기 위해 traceroute 을 사용해 보겠습니다.

```
[djv@castor djv]$ traceroute www.canus.net
traceroute to www.canus.net (205.152.190.251), 30 hops max, 40 byte packets

 4  core3.Atlanta.mci.net (204.70.4.9)  209.895 ms  158.635 ms  199.880 ms
 5  ast-uunet-nap.Atlanta.mci.net (206.157.77.114)  199.820 ms  148.672 ms 139.873 ms
 6  104.ATM2-0-0.XR1.ATL1.ALTER.NET (146.188.232.50)  189.844 ms  168.612 ms 149.935 ms
 7  195.ATM5-0-0.GW1.MIA1.ALTER.NET (146.188.232.137)  209.791 ms  198.624 ms 199.881 ms
 8  bs-miami-gw.customer.alter.net (157.130.65.222)  199.831 ms  198.651 ms 199.884 ms
 9  207.203.0.160 (207.203.0.160)  209.834 ms  160.053 ms  199.343 ms
10  172.25.80.90 (172.25.80.90)  209.514 ms  209.896 ms  179.381 ms
11  205.152.190.251 (205.152.190.251)  209.781 ms  168.693 ms  199.847 ms

[djv@castor djv]$
```

205.152.190.251 는 phicom.net 아래에 있다는 것을 알게 되었습니다. 그러므로 phicom.net 은 DNS 서비스뿐만 아니라 실제 인터넷 접속까지 함께 제공하고 있는 셈이죠.

이제 거의 다 잡은 셈입니다.

우리는 이 스패머가 사용하고 있는 usa.net 과 컴퓨서브로 스패머가 있다는 사실을 알려줄 수 있고 스패머가 실제로 사용하고 있는 phicom.net 에도 같은 사실을 알려주는 등의 행동을 취할 수 있습니다.

usa.net 이나 컴퓨서브 에서는 스패머의 계정을 취소할 수 있습니다만 phicom.net 에서는 자신들이 스패머에게 이용당하고 있다는 사실조차 모르고 있을 가능성도 있습니다. 스패머들에 대해서 무지한 ISP 도 많이 있기 때문입니다.

스패머에게 스팸메일을 뿌리지 말라고 경고하는 것은 별 의미가 없고, 이쪽에서 할 수 있는 수동적인 조치는 phicom.net 으로부터 송신되는 모든 메일을 거부하도록 설정해 주는 것입니다. 그래서 나중에 phicom.net 으로부터 스패머의 웹사이트가 삭제되었다는 확실한 통지를 받은 후에 다시 메일을 원래대로 받을 수 있도록 설정하는 것 정도가 이쪽에서 할 수 있는 일의 전부입니다.

제 8 절 그외 FAQ

8.1 리눅스에서 가능한 가장 큰 파일의 크기는?

이것은 사용하고 있는 파일시스템의 종류에 따라 틀립니다. ext2 파일시스템은 **64기가**까지의 파일을 저장할 수 있습니다. 미닉스(minix)나 ext 파일 시스템은 2기가가 한계입니다.

ext2 의 inode 는 12개의 블럭과 직접 연결되어 있고 한개는 간접적으로, 한개와는 이중, 한개는 삼중으로 연결되어 있으며 각각의 ext2 zone은 256개까지의 zone 포인터를 가질 수 있다. 따라서

12*BLOCK_SIZE + 256*BLOCK_SIZE + 256*256*BLOCK_SIZE + 256*256*256*BLOCK_SIZE

BLOCK_SIZE 는 보통 4096 이다. (2048 이나 1024 일 수도 있다.).

제 9 절 부록

9.1 부록A 인터넷 상의 리눅스 관련 웹사이트

- 일반적인 정보
  - *Linux Home Site* <http://www.linux.org>

  - *Linux On Sunsite* <http://www.sunsite.unc.edu/pub/Linux>
  - *Suman Saraf's web site devoted to linux* <http://www.jimin.com/suman>
  - *Linux Resource Exchange* <http://www.linuxrx.com>
  - *Linux bizzare: How many firms* <http://www.m-tech.ab.ca/linux-biz/>

- organisations, institutions in the world use Linux
  - *Linux Resource Exchange* <http://www.linuxrx.com>
  - *Mailing Lists and Newsgroups related to linux* <http://www.linuxrx.com/Lists/Lists.perl>

- 리눅스 배포본
  - *RedHat site* <http://www.redhat.com>
  - *Debian site* <http://www.debian.org>
  - *Slackware site.* <http://www.slackware.org>

- 리눅스 정보 찾아보기
  - <http://www.linuxlinks.com/>
  - <http://www.redhat.com/linux-info/Software/>
  - <http://uiarchive.cso.uiuc.edu/SearchEngines/linux.cgi>

- 시스템 관리
  - <http://www.secretagent.com/doc/ldp/sag/index.html>
  - <http://www.samag.com/>
  - <http://www.solucorp.qc.ca/linuxconf/>

- 네트워킹
  - <http://www.wwonline.com/~achau/ipmasq/>
  - <http://www.landfield.com/faqs/by-newsgroup/comp/comp.os.linux.networking.html>
  - <ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO/PPP-HOWTO>
  - <http://www.dna.lth.se/~erics/diald.html>
  - <http://www.umr.edu/~mark/linux/ppp.html>
  - <http://www.netdoor.com/helpdesk/linux.html>
  - <http://dijon.nais.com/~nevo/masq/index.html>
  - <http://samba.anu.edu.au/samba/>

- 프로그래밍
  - <http://samba.anu.edu.au/samba/>
  - <http://virtual-mktg.com/tiwatson/>
  - <http://franz.ww.tu-berlin.de/msqlperl/index.html##80>
  - <ftp://ftp.dti.ad.jp/pub/lang/CPAN/doc/wwwman/libwww/lib/LWP.html>

- 메일
  - <http://www.infinet.com/~gnosis/mail.html>
  - <http://www.qmail.org/>
  - <http://www.best.com/~ariel/nospam/>

  - <http://locke.ccil.org/~esr/fetchmail/>

- 문서 자료
  - <http://www.redhat.com/linux-info/lg/issue23/lg_toc23.html>
  - <http://www.linuxresources.com/>
  - <http://www.tux.org/~balsa/linux/cyrix/>
  - <http://www.tiac.net/users/williams/lugnuts/>
  - <http://www.ssc.com/linux/linux.html>
  - <http://www.scripps.edu/~jsmith/jazip/>
  - <http://www.solucorp.qc.ca/linuxconf/features.html>
  - <http://www.secretagent.com/>
  - <http://bmrc.berkeley.edu/people/chaffee/fat32.html>
  - <http://sunsite.unc.edu/LDP/HOWTO/mini/Kerneld.html>
  - <http://www.ch4549.org/lust/>
  - <http://www.LinuxMall.com/mallidx.html>
  - <http://sunsite.unc.edu/LDP/>
  - <http://sunsite.unc.edu/mdw/linux.html>
  - <ftp://sunsite.unc.edu/pub/Linux/docs/faqs/>
  - <http://www.redhat.com/linux-info/lg/issue18/issue18.html>
  - <http://www.gamers.org/dEngine/xf3D/>
  - <http://sunsite.unc.edu/LDP/FAQ/Linux-FAQ.html>
  - <http://amelia.db.erau.edu/Excite/AT-LDPquery.html>
  - <http://amelia.db.erau.edu/ldp/HOWTO/mini/Offline-Mailing.html##toc3>

- X 윈도우
  - <http://www.xfree86.org/>
  - <http://www.PLiG.org/xwinman/>
  - <http://x.unicom.net/themes/>
  - <http://tnt.microimages.com/freestuf/mix.htm>

- 레드햇
  - <http://www.redhat.com/support/docs/rhl/manual/manual/>
  - <http://www.redhat.com/support/docs/rhl/intel/rh41-errata-intel.html##Install_fails_with_some_SCSI_adaptors>
  - <http://www.best.com/~aturner/RedHat-FAQ/>
  - <http://www.redhat.com/redhat/softdir/index.phtml>
  - <http://www.labs.redhat.com/>

- 응용프로그램
  - <http://www.roestock.demon.co.uk/isapnptools/>
  - <ftp://ftp.xemacs.org/pub/tux/robotti/>
  - <http://mc.blackdown.org/mc/>

- <http://argeas.argos.hol.gr/pub/unix/cooledit/>
- <http://www.xnet.com/~blatura/linapps.shtml>
- <http://www.uwsg.indiana.edu/hypermail/linux/kernel/9707.3/0201.html>
- <http://www.rootshell.com/>
- <http://www.geek-girl.com/bugtraq/archives.html>
- <http://webwatcher.org/>
- <http://citv.unl.edu/linux/LinuxPresentation.html>
- <http://terminus.terminator.net/ipmasq/>
- <http://darkrain.vup3d.com/>

9.2 부록B 이 FAQ에 공헌할 수 있는 방법

linux-admin@vger.rutgers.edu나 FAQ 편집자에게 직접 FAQ 에 포함되었으면 하는 질문과 답변을 함께 적어서 보내면 된다.

9.3 부록C 감사

9.3.1 부록C.1 FAQ 내용

- Glynn Clements (glynn@sensei.co.uk)
- Edmund Lau (edlau@ucf.ics.uci.edu)
- John Evans (evansj@hi-line.net)
- Richard Betel (mto@rim.net)
- Marin D (marin@iclub.techno-link.com)
- LUIS FELIPE BALBINOT (9510919@turing.unisinos.tche.br)
- Brian Schau (bsc@fleggaard.dk)
- Mullen, Patrick (Patrick.Mullen@GSC.GTE.Com)
- Dave Sutherland (dave@ibd.net)
- Michael Granzow (mg@medi.physik.uni-oldenburg.de)
- Ajay Gautam (ajay@avlinsun.avlin.stpn.soft.net)
- Nagib Hobeica (nag@beryte.com)
- Chris MacLeod (stick@physis.viper.net)
- Robert Towster (towster@technologist.com)
- Tethys (tethys@ml.com)
- Troy Bowman (troy@ns.lumpnet.ml.org)
- Richard Betel (mto@rim.net)
- Martin Humberto Hoz Salvador (mhoz@uanl.mx)
- Gustavo Courault (courault@santafe.com.ar)

- Mark Conway Wirt (mark@intrepid.net)
- Irfan Akber (iakber@super.net.pk)
- Dave J. Vanecek (djv@bedford.net)
- Suman_Saraf (ssaraf@hss.hns.com)
- Edmund Lau (edlau@ucf.ics.uci.edu)
- Chris McGee (CMMcGee@Pella.com)
- Kristian Soerensen (elof@image.dk)
- Rob Riggs (rob@devilsthumb.com)
- Dave Wreski(dave@nic.com)
- Azfar Kazmi (oup@iname.com)

9.3.2 부록C.2 FAQ 호스팅/미러링

- Mullen, Patrick (Patrick.Mullen@GSC.GTE.Com)
- Nagib Hobeica (nag@beryte.com)
- Chris MacLeod (stick@physis.viper.net)
- Dave Sutherland (dave@ibd.net)

FAQ 편집자에게 연락하고 싶을때는

- Fyodor Yarochkin `fygrave@usa.net`
- Fyodor Yarochkin `fygrave@freenet.bishkek.su`