리눅스 설치와 기본 사항

설치및 기본, 하드웨어는 나에게 오라! 노가다의 진수를 느껴보자!

박진우-reduck96@linux.uos.ac.kr 제 2회 리눅스 공동체 세미나 자료집

총 6단계로 나누어져 있는 'Everything 주제없음'은 초보자, 그러나 ls같은 명령은 알고 계시는 분들을 위해 만들어져 있습니다. 각 세부 명령은 자세히 쓰도록 노력하 겠습니다만, 일단 재미있게 만들기 위해 안내문을 작성하였습니다. 제가 세미나 당일 하는 내용은 여기 적혀있는 내용과는 다를것입니다. 즉, 세미나때는 제목처럼 주제가 없습니다. 모든 질문을 그 자리에서 풀수있는것은 풀어버리고 안 되는 것은 정리해서 답을 드리겠습니다. 이 글은 중급과정이라 할 수 있겠지요. 그러나 어려운 말은 안 하도록 하겠습니다.

목 차

제 1 절 준비물

1. 드라이버(십자모양 그리고 자석달린것), 롱노우즈쁘라이어, 니퍼
2. 뜨거운물,찬물
3. 사발면,커피,콜라,주스등등

자, 이제 CD를 넣고 컴퓨터를 켜볼까요?

제 2 절 리눅스? 다시 깔아볼까 아님 그냥 놔둘까?

이번에 나온 AlzzA 6.0은 glibc의 버젼이 놀라가면서 기존의 버전에서 만든 프로그램과 열받지만 호환되지 않습니다. 그렇다고 다시 갈아엎기에는 그동안 공들인 시간이 아깝고... 한 예로 리눅스를 무지무지 좋아하는 한 분이 알짜가 나오자마자 깔고 X의 그 환상적인 모습에 넋을 잃었습니다. 그러나 그것도 잠시... 그동안 만들었던 각종 프로그램들이 안돌아가고, 웹설정도 다시해야한다는 불안감에 쌓이게 되었죠. 그뒤로 한시간 뒤, 겨우 겨우 웹설정을 끝내고 끝내 건물 수위아저씨의 등쌀에 못이겨 집으로 돌아가면서 상심에 잠겼다는 전설같은(?) 이야기를 여러분들에게 전해드리지 않을수가 없네요. 이제 리눅스는 설치면에서는 Windog보다 탁월하게 잘 깔린다는것을 여러분들도 잘 아실것입니다. 그러나 자신의 환경에 맞는 설정을 하는것은 오랜 경험과 시간을 요구 합니다. 웹서버의 경우, /etc/httpd가 가장 문제가 되고요, 계정서비스및 메일 서비스 를 하는 사람의 경우는 /etc/passwd,/etc/group, /home이 중요하죠. oracle의 경우는 /home/oracle이 중요하고, postgres의 경우는 /var/lib/pgsql이 중요하죠. 아, 메일도 빼먹을수가 없겠지요? /var/spool/mail입니다. 자, 한번 정리해 볼까요? 새로 업데이트 되기전에 한번쯤 백업을 해두어야 할 디렉토리 입니다.

```
/etc
/usr/local
/usr/src/redhat
/var/spool
/var/log
/var/lib
/home
/root
```

위의 디렉토리 말고도 관리자가 특별히 특정한곳에 넣어 둘만한 파일이 있는지 한번 생각해 보세요. 예를 들어 야한 사진 등이요. 제가 아는 사람의 경우 이곳에 넣더군요.

```
/usr/X11R6/lib/X11/fonts/misc/pics
```

흠... 좀 힘들겠죠? 뭐, 더 길게 만들어서 넣어두는 경우도 있지만여... 너무 샛길로 빠졌군요. 여하튼 이러한 경우가 몇몇사람들에게 확실히 있었으니, 조심하시기 바랍니다. 자아, 한번 가정을 해보고 OS를 업그래이드 해봅시다.

```
의뢰인 : "저는 200명의 계정을 관리합니다. 메일과 home, 그리고 웹을
          관리하고 있습니다. 그리고 /usr/local쪽에 특수한 프로그램들이
          몇몇 있습니다. 특히 sogoban의 경우는 확실히 실행되어야
          합니다. 뭐냐구요? 바둑프로그램입니다."
```

자, 이제 우리들은 이 의뢰를 받고 업데이트해주는 노가다맨(?)이 되는 것입니다. 일단 판단을 합니다. 이 상황에서 과연 얼마만큼 효율적으로 할 수 있을것인지요. glibc의 버전이 바뀌므로 일단은 shared binary들을 백업할 생각은 버리자. 단, static binary들은 수단과 방법을 가리지 말고 살리자. 그리고 소스가 있다면 이것또한 수단과 방법을 가리지 말고 백업해야 한다. 다음은 각 계정에 해당되는 home을 백업하자. 그다음은 /etc의 설정파일들을 백업하자. 그냥 passwd와 group만 백업해서 나중에 통곡하는 일이 없도록 해놓자. etc만큼은 정말이지 확실히 통째로 백업해놓는것이 좋습니다. 자신도 모르는사이에 설정을 딱 해놓았을지 모르기때문이죠. 저도 한 2 3번 정도 당하니깐 나중에는 꼭 백업을 합니다. 다음은 메일 spool디렉토리입니다. 이것또한 중요하죠. 메일에 목메다는 사람들이 꼭 한두사람 있기때문에, 중요합니다. 자, 일단 다른 하드또는 DAT같은것으로 백업을 두세군데 해놓으셨다면 이제 마지막으로 점검을 해봅시다. 이때 좋은 방법으로는 이상하게 사용하면서도 잘 쓰는 사람을 초빙해서 물어보거나 사용하는것을 지켜보는 방법이 있습니다. 뭐, 지우거나 박살내는 것은 관리자 마음이니깐.... 책임질 수 있으면 이제 컴퓨터를 끄고 업데이트할 CD를 넣습니다. 자, 리눅스를 10분안에 깔고 다음 root넣고 복구할 준비를 합시다. 한가지 우리가 먼저 계획할것이 있습니다. 바로 복구시간이죠. 복구시간이 오래걸리면 재미가 없겠죠? 짧으면 짧을수록 좋습니다. 반복학습을 하시면 좋겠지만, 그렇게 하면 관리

직에서 내쫓길 위험성이 커지므로 한번 할때마다 목숨을 걸고 한다는 생각을 가지고 하세요. 저는 2시간을 드리겠습니다. 특정한 일없이 단순 업데이트의 경우, 2시간이면 충분합니다.

```
 !! 중요 !!
설치시 RedHat 5.2에서 RedHat 6.0으로 업데이트 할때는 update가 아닌
새로운 install을 권합니다.
```

설치끝나고 전원을 올렸으면 이제 백업했던 자료를 옮겨올 일이 남았습니다. 이제 passwd 파일과 group파일을 /etc로 복사합시다. 이때 주의할점! 만약 shadow를 작동시키고 하면 안됩니다. 그리고 이전에 있던 passwd도 shadow가 되어있지 않은 파일 이어야 합니다. 그렇지 않으면 당신은 엄청난 실수를 범한것입니다. 자 shadow 사용할때는 pwconv shadow 제거할대는 pwunconv 주의하세요. 그다음은 root 암호를 바꾸십시오.

```
passwd root
```

왜 그러냐구요? 이전의 암호를 옮겨왔기 때문에 설치하면서 만든 암호가 무효화되기 때문입니다. 다음으로 할 일은 home을 복사하고, 다음은 /var/spool/mail을 복사합시다. 자, 잘 되었는지 home디렉토리에 가서 ls -al 을 쳐봅시다. 각 디렉토리의 권한들이 각 유저들의 권한으로 되어 있습니까? 만약 그렇지 않고 root 권한으로 되어있다면? 당신은 또한번 크나큰 실수를 범한 것입니다. 백업할때 백업툴을 사용했다면 문제가 없을 것이고, tar를 사용해도 문제가 되지 않죠? cp를 사용하면? 이때는 옵션이 붙습니다. 간단하게 하는 방법!

```
cp -a /home /backup/
```

이러면 됩니다. 꼭 계정에 대한 권한이 제대로 살아 있는지 확인하십시오. 다음은 의뢰자님께서 /usr/local쪽의 복구를 의뢰하셨으니, 어디 봅시다. 일단 static binary의 경우는 그냥 전에 있던 자리에 놓으셔도 됩니다. 참, PATH가 바뀌어 있다구요?

```
/etc/profile
```

이것을 전에 있던 파일과 비교해서 바꾸어 주시기 바랍니다. PATH를 손봐주시면 됩니다. 자, /etc의 파일들과 현재 설치된 파일들을 비교해가면서 바꾸어 봅시다. 다음은 /etc/httpd/conf를 손봅시다. php를 사용할경우 꼭 풀어주어야 할 옵션이 있습니다.

```
# Extra Modules
#LoadModule php_module         modules/mod_php.so
LoadModule php3_module        modules/libphp3.so
#LoadModule perl_module        modules/libperl.so

그리고
# Extra Modules
#AddModule mod_php.c
AddModule mod_php3.c
#AddModule mod_perl.c

그리고
AddType application/x-httpd-php3 .php3
AddType application/x-httpd-php3-source .phps
#AddType application/x-httpd-php .phtml
```

이렇게 생긴것의 앞의 #(주석처리)를 제거하시고

```
/etc/rc.d/init.d/httpd restart
```

해주시면 끝입니다. 웹이야 /home/httpd/html 에 있으면 그냥 쓰면 되니까 문제될 것은 없을 것입니다. 특수한 경우는 이전의 설정파일을 보고 비교하시면 됩니다. apache의 설정은 버전이 업되면서 크게 바뀐점이 없기 때문에, 그냥 사용하셔도 별무리는 없을 것입니다. 다음은 바둑프로그램... 요건 소스가 마침 공개되어 있기 때문에, 그냥 컴파일로 문제를 해결했습니다. 자 이제 남은 일은 뭘까요? 보안 설정? 요건 다음에 하기로 하구요, 긴급 복구는 여기서 끝내겠습니다.

제 3 절 우잉? 소스? Oh, NO! 일단 컴파일부터!

리눅스의 강점은 뭐니뭐니해도 공개된 소스가 아닐까 합니다. 이 부분은 타의 추종을 불허하죠. 그만큼 리눅스를 다루는 부분에서 컴파일은 장난감처럼 여겨야 합니다. 일단 어떤 복잡한 소스를 하나 예를 들어서 프로그램을 컴파일 해봅시다.

3.1 소스 구하기

보통 SRPM내지 tar.gz로 되어있는 것을 구하게 되실 것입니다. 자아 저도 어떤 파일을 붙잡고 여러분들과 같이 가지고 놀아야겠죠? procps-2.0.2-korea_patch.tgz 이 파일은 ftp://monster.uos.ac.kr/pub/misc/procps-2.0.2-korea_patch.tgz 에 준비시켜 놓았습니다. 우리는 이 파일에서 top부분의 안내문이 한글로 나오게 하는 것이 목적입니다.

```
** 주의 ! : 이 소스는 알짜 6.0 또는 RedHat 6.0 또는 파워,액셀
            리눅스에서 하는 것을 기본으로 합니다. 만약 RedHat 5.2또는
            알짜 5.2라면, 일단 procps를 (위의 파일) 모두 설치하신
            다음에 ldconfig를 실행시키시고 난 뒤에 시작하셔야
            됩니다. 왜냐구요? 그냥하면 libProc.ld를 찾느라고 난리를
            치기 때문입니다.
```

일단 이 파일을 적당한 곳에 두고 압축을 풉시다.

```
tar zxvf procps-2.0.2-korea_patch.tgz
```

자, 다 풀리셨습니까? 이제 procps-2.0.2 디렉토리로 들어갑시다. 들어가면 top.c 가보이시죠? 요것이 우리들의 목표입니다. 그러나... 이렇게 찾아 들어가면 안돼요!! 제일 먼저 보아야할 파일이 있습니다.

```
README
INSTALL
```

어떤 소스든지, 요 둘중에 한가지는 꼭 들어있습니다. 요기에 설치법이 다 나와 있습니다. 물론 영어이겠죠...(^^;) 여하튼 이 파일을 먼저 보시고 이제 top.c를 봅시다. 일단 저는 'CPU states'를 'CPU 상태'로 바꾸겠습니다. 1274번째 줄입니다.

```
        /* END EXPERIMENTAL CODE */
        printf("CPU 상태:"
            " %2ld.%ld%% user, %2ld.%ld%% system,"
            " %2ld.%ld%% nice, %2ld.%ld%% idle",
```

자, "CPU 상태" 라고 바꾸셨죠? 이제 저장을 하시고 컴파일을 합시다. 컴파일 할때는 make를 적절하게 사용합시다.

```
make top
```

이렇게 하면 top 프로그램부분만 컴파일하게 됩니다. 자, 이제 top이라고 실행가능한 파일이 생성되었죠? 여기서 top을 실행시켜 봅시다.

```
  3:22am  up 17 days, 20:35,  2 users,  load average: 0.00, 0.00, 0.00
59 processes: 58 sleeping, 1 running, 0 zombie, 0 stopped
CPU 상태:  0.0% user,  0.0% system,  0.0% nice,  2.4% idle
```

어때요? 한글로 나오죠? 이렇게 조금씩 바꾸어 나가면 자신도 모르는 사이에 한글 패키지를 만드는 패키저가 될 수 있습니다. 이제 다른 부분도 모두 바꿔볼까요?

```
  4:33am  up 17 days, 21:46,  2 users,  load average: 0.07, 0.04, 0.00
51 작업개수: 50 잠팅이개수, 1 뛈박질개수, 0 좀비(귀신), 0 멈춘갯수
CPU 상태:  0.0% user,  0.7% system,  0.0% nice, 99.2% idle
Mem:   95592K av,  90880K used,   4712K free,  91880K shrd,  18700K buff
Swap:  96384K av,   1412K used,  94972K free              46492K cached
Memory 정보 보여줄까 말까? off
```

저의 짧은 영어실력으로 바꾼 안내문들입니다. 만약 영어번역에 조예가 깊으신 분들은 이와같은 재미있는 일에 동참해 주시기 바랍니다. 제가 바꾼 top은 RPM으로 만들어서 ftp://monster.uos.ac.kr/pub/misc/ 안에 넣어두겠습니다.

```
procps-2.0.2-linux4reduck96.src.rpm                    소스 패키지
-----------------------------------------------
procps-2.0.2-linux4reduck96_Alzza52.i386.rpm
procps-X11-2.0.2-linux4reduck96_Alzza52.i386.rpm
-----------------------------------------------알짜 5.2용
```

이렇게 파일을 두겠습니다. 만약 알짜 6.0을 사용하실 경우, rpm –rebuild procps-2.0.2-linux4reduck96.src.rpm 라고 하시면 /usr/src/redhat/RPMS/i386 에 밑의 두 파일이 생성됩니다. 그것으로 rpm -Uhv proc*.rpm 하시면 됩니다. 많이많이 수정해서 자료실에 올려주세요 ^^;

제 4 절 리눅스박스 하나로 다수의 웹서비스를?

```
의뢰인 : 헤이, 나 야한 웹하나 만들게 컴하나 만들어주라!
처리인 : 그럼 돈줘. 잘 만들어줄께.
의뢰인 : 야, 나 돈 별로 없어.
처리인 : 그래? 그럼 밥한끼 사줘라.
의뢰인 : 장난하냐?
처리인 : 반말이냐?
의뢰인 : 퍽!
처리인 : 팍!
퍽퍽~~ 팍팍!!
```

과연 누가 잘못하고 있는 것일까요? 웹을 하나 띄우기 위해서 컴을 하나 마련한다? 그것도 별로 중요한 자료도 없는 야 한 사이트를 위해 새것을? 처리인은 어떤 생각 을 가지고 밥한끼에 해결한다고 헛소리를 했을까요? 과연 헛소리일까요? WindogNT를 이용해서 한다면 위의 방법을 쓸려면 밥한끼에 안된다는 것을 잘 아실 것입니

다. 하하! 밥 한끼에 몇백만원 하냐구요? 설마 단란주점이라고 생각하신 독자가 계신다면 그건 큰 오산입니다. 리눅서가 무슨 돈이 있다고 단란주점에 갑니까? 라면 하나면 끝나는데... Linux에서는 공짜로 한대의 하드웨어에서 복수의 웹서포팅을 할 수 있는 기능이 기본으로 들어가 있습니다.

사용될 Application

1. Linux (당연하겠죠?)
2. Apache (기본으로 들어가있겠죠?)

이미 여러분들은 할 수 있는 도구를 다 가지고 있습니다. 다만 사용을 안해서 그렇죠. Linux에서 IP Alias기능을 사용하여 한개의 machine이 복수의 IP를 가지도록 합시다. 알짜 또는 RedHat Linux에서는 IP Alias기능이 커널 단위에서 선택되어져 있기 때문에 커널을 다시 컴파일 할 필요는 없습니다. 하고 싶으시다구여? 그럼 하십시요. 저보고 하라구요? 좀 기다리세요. 아직도 정리중이에요... 다 정리한다음, 통신망 강좌란에 올릴께요. 여하튼 지금은 중요한것이 이것이 아니죠... 일단 Alias를 사용해 봅시다. 여러분들이 만약 X-Window상태라면 다음의 툴을 띄워주시기 바랍니다.

```
netcfg
```

이거 말고도 여러 가지 툴들이 있지만, 저는 이것으로 하겠습니다. 자, 네모난 상자에 메뉴가 몇개 뜨죠? 아하 자신의 컴퓨터의 네트워크 설정을 하는 툴킷이네요. 자세히 보시면 여러분들이 수정할 수 있는 부분이 몇가지 있을것입니다. 수정하고 싶으신 분은 지금 바꾸시고 'Save'키를 눌러주시기 바랍니다. 이제 박스의 윗부분을 잘 봅시다. 'Interfaces'라는 키가 있지요? 누르십시오. 그러면 밑의 키에 'Alias'가 보일 것입니다. 자아 일단 alias를 활성화시킬 네트워크 카드를 선택합시다. 여러분의 컴퓨터가 특수한 목적에 사용되지 않는한, eth0 만이 여러분을 반길것입니다. 'lo'는 뭔데 취급도 안하냐구요? 그것은 자기 자신을 뜻합니다. 뭐, 잊으셔도 상관없습니다. 일단 'eth0'를 선택하신 후, 'Alias'키를 누릅시다. 그러면 메뉴가 하나 더뜨죠? 보면 뻔 하죠? 바로 IP를 넣어달라는 것입니다. C-Class까지는 먼저 차지한것과 같아야 합니다만, d-class를 바꿈으로서 이 machine은 복수의 IP를 가지게 되는 것입니다. c,d-class가 뭐냐구요? 한가지 예를 들겠습니다.

```
 IP : 203.249.231.199
요런 IP가 있다고 합시다.
203부분 : A-Class
249부분 : B-Class
231부분 : C-Class
199부분 : D-Class
```

즉, A.B.C.D 라고 생각하시면 됩니다. 간단하죠? 자, 이제 'Done'을 선택하시고 Save를 하시고, Active시키면 그때부터 여러분이 입력한 주소가 활성화됩니다. 자, 이제 웹서버에서 설정하는 것만 남았네요.

```
** 주의 **
여기서는 한가지 상황을 설정해 놓고 이야기를 이끌어가겠습니다.
Alias한 IP  : 203.249.231.199
        URL : nuclear_bumb.babo.net
이 서버의 원래 URL과 IP
        IP  : 203.249.231.50
        URL : mungchungi.babo.net
```

자아 /etc/httpd/conf 에 놀러가볼까요? 알짜를 사용하신다면, 씨께서 한꺼번에 뭉쳐놓고 한글로 설명해놓은 설정들을 볼 수 있을 것입니다. 우리는, 여기서 제일 맨 끝으로 가야 합니다.

```
#
# 가상 호스트 예제:
# 거의 모든 아파치 지시자가 VirtualHost 컨테이너에 올 수 있다.
#
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error_log
#    CustomLog logs/host.some_domain.com-access_log common
#
```

우잉? 척보면 탁 알아야 하는데... 뭔가 의미가 있지요? 자, 앞의 #를 빼고 하나하나 설정해 봅시다.

```
<VirtualHost nuclear_bumb.babo.net>
    ServerAdmin nuclear@nuclear_bumb.babo.net
    DocumentRoot /home/nuclear/web_start
    ServerName nuclear_bumb.babo.net
    ErrorLog logs/nuclear_bumb.babo.net-error_log
    CustomLog logs/nuclear_bumb.babo.net-access_log common
```

우잉? 갑자기 쉬워진다는 느낌이 들죠? 이렇게 복수의 것을 만들면 끝! 아, httpd 리스타트(/etc/rc.d/init.d/httpd restart) 한다는것 잊지 마세요. 자아, 이제 얻어터진 의뢰자는 /home/nuclear/web_start에 웹소스를 넣기만 하면 끝입니다. 얻어터져도 싸죠?

제 5 절 tcpwraper는 시체가 아니다!

tcp_wraper... 요거 사용하는 사람 별로 없을것이라 생각됩니다. 요것이 무엇이냐! 바로 관리자가 선택적으로 접속하는 호스트를 막는 툴이다 이겁니다. 자, 필요한 파일들을 볼까요?

```
/etc/hosts.allow
/etc/hosts.deny
```

그리고 서비스로 하나 만들 것이 있죠. 파일이름은 host_check로 할께요.

```
#!/bin/sh

 ################################  변수정의부문

 # 메일 수신자
 mailto=reduck96

 # 화면출력 여부, 메일전송 여부
 dsp=$1; msg=$2

 # 접속자 정보 등
 a=$3; c=$4; d=$5; h=$6; n=$7; p=$8; s=$9; u=$10
```

```
# 현재 시간
time=`date`

# 접속시도자 소속 서버의 finger 정보
finger=`/usr/bin/finger -l @$h 2> /dev/null`


################################ 화면 출력부문

if [ $dsp = Y ]
   then

/bin/echo "
                     ===================================\n\
                          접속이 허용되지 않습니다.     \n\
                     ===================================\n\
\n\
              Access Time            : $time\n\
              Client host address    : $a\n\
              Client information     : $c\n\
              Client host name(or IP) : $h\n\
              Client host name       : $n\n\
              Client user name       : $u\n\n
"

fi


################################ 메일 송신부문

if [ $msg = Y ]
   then

/bin/echo "
                       ================================\n\
                             접속 거부자 상세정보      \n\
                       ================================\n\
\n\
        Access Time                    : $time\n\
        Access client host address     : $a\n\
        Access client information      : $c\n\
        The daemon process name        : $d\n\
        Access client host name(or IP) : $h\n\
        Access client host name        : $n\n\
        The daemon process id          : $p\n\
        Server information             : $s\n\
        Access client user name        : $u\n\
\n\
--------------------------------------------------------\n\
                       Access client finger information                   \n\
```

```
 -------------------------------------------------------\n\
 $finger\n\
 --------------------------------------------------------\n\
 \n\n" | \
      /bin/mail -s "tcp_wrapper report [$d]" $mailto

 fi
```

이렇게 host_check 파일을 만든뒤, /etc/에 넣어둡시다. 참, 이거 잊지 마세요.

```
chmod a+rx /etc/host_check
```

요렇게 실행할 수 있게 만들어 놓아야 되요. 자아, 이제 나머지 hosts.allow와 hosts.deny를 작살내봅시다. hosts.allow의 내용입니다.

```
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
in.telnetd : \
    127.0.0.1 \
    203.249.111. \
    133.207. \
    203.249.107.174 \
    nec.co.jp \
: rfc931: ALLOW
```

그리고, hosts.deny의 내용입니다.

```
#
# hosts.deny    This file describes the names of the hosts which are
#               *not* allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
# The portmap line is redundant, but it is left to remind you that
# the new secure portmap uses hosts.deny and hosts.allow.  In particular
# you should know that NFS uses portmap!
ALL : ALL EXCEPT LOCAL :\
 twist ( /etc/host_check Y Y %a %c %d %h %n %p %s %u ) &
```

대충 보시면 아시겠죠? hosts.allow에는 허용할 컴의 ip내지 domain을 쓰면 됩니다. 그리고 hosts.deny는 수정할 것이 거의 없습니다. 단, 메일받는 사람의 ID는 바꾸어 주셔야 겠죠? reduck96 부분입니다. 이것이 우째 작동을 하느냐 궁금하시죠? 일단 허용되지 않는곳의 IP에서 telnet으로 접속을 시도합니다. 그러면 바로 host_check가 돌죠. 그리고 접속을 시도한 컴에게 finger를 시도해서 정보를 메일로 관리자에게 보냅니다. 물론 host_check를 특수한 프로그램으로 바꾸어 한다면 무지무지 재미있겠죠? 예를 들어 Tear_Drop이라든지, PING_DUMP같은 아주 성질 나쁜 것으로요. 요런 거 어디서 구하냐구요? 흐흐흐 이곳에 한번 가보세요. 재미있는 툴들이 많습니다.

`<http://www.rootshell.com>`

자, 세부 설정은 여러분들에게 숙제로 남기겠습니다. 잘 설정해서 사용하시기를... 참, telnet말고도 다른것도 막고싶다구요? 그럼 예제를 더 넣어드릴께요.

```
portmap rpc.nfsd rpc.mountd: \
    127.0.0.1 \
    203.249.111. \
: ALLOW
in.fingerd in.cfingerd : rfc931:DENY
in.timed ipop3d: ALL@ALL: rfc931: DENY
in.ntalkd in.talkd: ALL: rfc931: ALLOW
in.ftpd: ALL@ALL: rfc931: ALLOW
```

이정도면 되겠죠? 간단하죠? 사용할 대몬프로그램의 이름을 앞에 써주고 형식은 같으니 변형해서 사용하시면 됩니다. 요렇게 해서 걸린 IP들을 조사해보면, 대부분 sscan으로 휘집어 깐다는 것을 아실 수 있을 것입니다. 조심하세요. 저에게 sscan걸리면 전 바로 Vs 모드(보복모드)로 돌변하니까요.

제 6 절 Service : Hardware 될때까지 바꾸어라!

이제 마지막으로 hardware에 대해 논하겠습니다. 사실 4년전만 해도 linux는 하드웨어의 특성을 엄청 잘 탓었습니다. 그러나 펜티엄이 나오면서 왠만큼 특성을 타는 하드웨어가 줄어들기 시작했죠. 그러나 한가지 변하지 않는것이 있습니다. "국산 하드웨어는 잘 안된다... XX대기업 회사 제품은 리눅스 깔면 안깔린다 등등.." 그러나 시대가 흘러가면서 이러한 소문도 점차 줄어들기 시작했죠. 자 소문이야기는 그만하고, 하드웨어 이야기를 합시다.

6.1 PNP의 경우 잘생기는 현상

PNP...Plug and Pray...(장착하고 기도하라) 너무너무 괴롭히는 하드웨어입니다. 물론 요놈을 끌수 있으면 좋으련만... Linux와 Windows를 사용하시는 분들이시라면 요 PNP때문에 고생하는 분들이 꽤 계실것입니다. 급기야 하드웨어를 교체까지 하던지, 아니면 linux를 포기하게 되죠. 이중, 여러사람들에게 질문을 받게 되는데, 다 그런것은 아니고 아주 간단한 작업을 하면 이 문제는 해결됩니다. 바로 리눅스를 깔고나니 하드웨어, 특히 사운드카드와 랜카드가 먹통이 되는 현상이죠. 어쩔때는 작동되고, 어쩔때는 안되고... 이것은 바로 OS가 PNP를 누가 먼저 선점하느냐에 따라 변하는 괴현상입니다. 해결책은 의외로 간단합니다. 리부팅, 즉 웜부팅(Ctrl+Alt+Del)으로는 절때 꺼서는 안됩니다. 그리고 Windog에서 다시 시작으로 해도 안됩니다. 전원을 완전히 내려서 어떤 OS도 PNP를 선점하지 못하게 해야 합니다. 그리고나서 linux나 windog를 선택해주시면 문제가 해결됩니다.

6.2 isapnp를 이용하여 잡고싶어요

isapnp를 이용하여 하드웨어를 설정하는 방법이 있습니다. 사용방법은 다음과 같습니다.

```
pnpdump > /etc/isapnp.conf
```

편집기로 /etc/isapnp.conf 내용을 본다.

사실 이 부분을 보시면, 영어이기는 하지만 안내문이 나옵니다. 제가 시간이 나면 isapnp tool을 영어로 번역하여 패키지로 올려놓겠습니다. 흠... 일단 대충 보시면 아실것입니다. IRQ와 IO, DMA를 선택하는 것이지요. 앞의 #를 선택해서 제거해 주시면 끝입니다. 그리고 한가지... 꼭 "Y"를 지워달라는 말이 있죠? 요것을 꼭 해주시기 바랍니다. 이렇게 해서 저장을 하고 나와서 다음을 실행시켜 주세요.

```
isapnp /etc/isapnp.conf
```

그러면 준비 끝! 만약 에러가 나오면 다시 설정해 주세요. 이것은 많은 경험이 요구됩니다. 그리고 나서 module을 올려야 한다면 모듈을 올려주시면 문제 끝입니다. 자, 웬만큼 해결되었습니까?

6.3 하드웨어가 windog에서도 잘 안잡혀요.

요건 여러가지 원인이 있을수 있겠으나, 가장 많은 경우는 pci의 irq가 엉켜서 생기는 문제가 많습니다. 요건 linux에서도 생깁니다. 해결방법은 여러 가지가 있습니다.

```
 --> PCI카드를 전부 뽑아서 순서를 바꾸어서 다시 장착한다.
 --> BIOS에서 PCI부분의 정보를 reset한다.
 --> 보드의 건전지를 제거했다가 다시 붙인다.
 --> 보드 구입처에가서 보드를 바꾸어 달라고 한다.
```

기타 등등...

여러 가지가 있을 수 있습니다만, 가장 손쉬운 방법은 역시 PCI카드의 꼽는 위치를 바꾸는 것입니다. 그리고 나서 다시 BIOS에 들어가 설정해주고 windog나 linux로 가보세요. 잘 되는 경우가 엄청 많았습니다.

6.4 module을 올리고 싶어요. 어떻게 해요?

우와악! 이건 X-Window에서 하는 것이 사실 편하답니다. kernelcfg라는 프로그램이 있습니다. 이것으로 대충 눈짐작으로 추가할 수 있습니다. 그러나 상세한 정보를 원하신다면... 일단은 /usr/src/linux/Documentation에 가보세요. 자신의 하드웨어를 커널이 지원하는지 일단 알아봐야겠죠? 만약 있다면? 그럼 설치해야죠! 알짜의 경우 대부분의 하드웨어를 모듈로 만들어 놓았기때문에 다시 컴파일할 필요가 없습니다. 자, 다음의 명령을 익힙시다.

```
insmod : module을 install한다.
rmmod : module을 remove한다.
modprobe : module을 probe 한다.
lsmod : 현재 install되어 있는 modules를 보여준다.
```

module은 /lib/modules/2.2.xx/에 있습니다. 2.2.xx는 자신의 커널 버젼과 같으며, 이 복수개가 있다면 현재 설치되어 있는 커널이 무엇인지 수단과 방법을 가리지 말고 알아내야 합니다. 자신의 랜카드가 3c509라면... /lib/modules/2.2.xx/net/3c509.o 가 설치할 모듈 이네요.

```
insmod /lib/modules/2.2.xx/net/3c509
```

간단하죠? 만약 irq나 io를 옵션으로 붙여야 한다면? ne2000호환일때 그런 경우가 많죠. 이때는 /etc/conf.modules라는 파일을 만듭시다. 그리고 다음의 내용을 넣읍시다.

==> 자신의 ne2000카드의 IRQ가 5번이고, IO가 300번일때...

```
alias eth0 ne
options ne io=0x300 irq=5
```

이렇게 저장하시고 modprobe ne 라고 하시면 문제 끝! 쉽죠? 많은 경험들을 글로 표현하기란 정말 쉽지 않군요. 일반 서점에서 살 수 있는 딱딱한 교본으로 백날해도 안되는 경우가 많지요? 이렇게 경험을 부족하지만 글로 쓸 수 있게 기회를 준 여러분들께 이 글을 드립니다.