작성자: **saint**

Overview
BackTrack 는 LILO 를 부트로더로 사용한다. BactTrack 을 기본 환경 설정 그대로 설치하면 부팅할 수 없는 경우가 있는데, 이것은 실린더 크기가 1024 보다 큰 하드디스크에 설치하면 LILO 가 OS 를 정상적으로 읽어올 수 없기 때문이다. 요즘 나오는 LILO 는 이 문제를 해결했다고 하는데(lba32 옵션을 사용하면 된다고 한다), 불행히도 BackTrack 에 탑재된 LILO 는 그리 똑똑하지 못하다. 이런 이유로, 본문에서는 GRUB 을 부트로더로 이용하여 BackTrack 을 설치하는 방법을 다룬다.

BackTrack?
BackTrack 은 보안도구(뒤집어생각하면 해킹도구)를 정보보호 프레임워크에 따라 구성해서 패키지로 만든 리눅스 배포본이다. Slackware 를 Live CD 형태로 만든 Salx 에 기반하고 있어서 CD ROM 만 있으면 어디서든 리눅스 환경을 이용할 수 있다. 현재 최신 버전은 2.0 이다. BackTrack 은 이전에 있던 두가지 리눅스 배포본이 하나로 합쳐진 결과물이다. Auditor's Security Collection 과 WHAX 가 그것이다. 물론, 이 두가지 리눅스도 BackTrack 과 동일한 목적으로 만들어진 배포본이다.

BackTrack 를 자세히 알고 싶거나 CD 이미지를 다운로드하고 싶다면 http://www.remote-exploit.org/backtrack.html 를 방문해보기 바란다.

Contents

본문 닫기

1. 실행한 환경
내가 BackTrack 을 설치한 시스템은 노트북이다.

Fujitsu 7010AM
- CPU: Centrino 1.1GHz ULV
- Memory: 512MB
- Storage: 60GB
- Network: Intel wireless 2200, Realtek xxxx (뭔지 잘 모르겠다 =_=;a)
- Grphic: Intel 855GME (1280*768)

2. TrackBack2 부팅

TrackBack2 Live CD 를 드라이브에 넣고 부팅한다. boot: 프롬프트가 나타나면 그냥 엔터 키를 누른다.
리눅스 커널을 올리고 initrd 가 실행되면서 시스템이 준비되면 썰렁한 로그인 화면이 나타난다.
여기서 root 계정으로 로그인한다. 로그인 화면에 출력된 메시지를 보면 root 의 패스워드는 toor 라고 친절하게 설명해주고 있다.

부팅하기 전에 유동 IP 를 받을 수 있는 환경이라면, 노트북을 반드시 네트워크에 연결한다. 왜냐면, GRUB 을 인터넷에서 다운받아 사용할 것이기 때문이다... (BackTrack2 Live CD 는 GRUB 이 포함되어 있지 않다...)
DHCP 환경이 아니라면 부팅 후 "startx" 명령어를 입력하여 KDE 환경에서 IP 를 구성해준다. (필자는 명령어로 IP 구성하는 법을 모르고 있다... =_=;a)

3. Partition 구성

saint 는 디스크를 세개의 파티션으로 나누어 쓰려고 한다. 파티션을 나누는 이유는 각 파티션마다 별도의 파일 시스템 디렉토리를 구성해서 필요하면 언제든 갈아엎을 수 있도록 하고, 데이터를 안전하게 보관하고 싶어서다. (OS 를 운영하자면 이건 기본이 아닐까 싶다...)

본격적인 파티션 나누기 작업을 할까한다...

```
# fdisk /dev/hda

The number of cylinders for this disk is set to 7296.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versionsl of LILO)
2) booting and partitioning software from other OSs
     (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): p                                    #하드디스크 파티션을 조회

Disk /dev/hdb: 60.0 GB, 60011642880 bytes
255 heads, 63 sectors/track, 7296 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id System

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
```

```
p
Partition number (1-4): 1
First cylinder (1-7296, default 1):<Enter>
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-7296, default 7296): +64M

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (10-7296, default 10):<Enter>
Using default value 10
Last cylinder or +size or +sizeM or +sizeK (10-7296, default 7296): +1024M

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 3
First cylinder (135-7296, default 10):<Enter>
Using default value 135
Last cylinder or +size or +sizeM or +sizeK (135-7296, default 7296): +25648M

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 4
First cylinder (3254-7296, default 3254):<Enter>
Using default value 3254
Last cylinder or +size or +sizeM or +sizeK (3254-7296, default 7296):<Enter>

Command (m for help): a
Partition number (1-4): 1

Command (m for help): t
Partition number (1-4): 2
Hex code (type L to list codes): 82

Command (m for help): p

Disk /dev/hdb: 60.0 GB, 60011642880 bytes
255 heads, 63 sectors/track, 7296 cylinders
```

```
Units = cylinders of 16065 * 512 = 8225280 bytes

           Device  Boot      Start         End      Blocks   Id  Syste
m
/device/hda1   *           1           9       72261   83  Linu
x
/device/hda2               10         134     1004062+  82  Linux
swap
/device/hda3              135        3253    25053367+  83  Linux
/device/hda4             3254        7296    32475397+  83  Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.

WARNNING: Re-reading the partition table failed with error 16: Device or resource
busy.
The kernel still uses the old table.
The new table will be used at the next reboot.
Syncing disk.
# reboot
```

4. 디스크 포맷하고 마운트하기

이젠 디스크를 포맷하고 마운트해서 BackTrack 을 설치할 준비를 한다.

```
# mkfs.ext3 /dev/hda1                    # /dev/hda1 을 ext3 파일
시스템으로 포맷한다.
# mkfs.ext3 /dev/hda3                    # /dev/hda3 을 ext3 파일
시스템으로 포맷한다.
# mkfs.ext3 /dev/hda4                    # /dev/hda4 를 ext3 파일
시스템으로 포맷한다.
```

아마도 파티션은 마운트되어 있지 않을 것이다. 마운트 포인트를 만들고 파일 시스템을 해당 디렉토리에 마운트한다.

```
# cd /mnt
# mkdir {hda1,hda3,hda4}                 #중괄호를 이용하면 여러개의
디렉토리를 동시에 만든다.
# mount /dev/hda1 /mnt/hda1              #포맷된 파일 시스템 /dev/hda1 을
/mnt/hda1 에 마운트한다.
# mount /dev/hda1 /mnt/hda3              #포맷된 파일 시스템 /dev/hda3 을
/mnt/hda3 에 마운트한다.
# mount /dev/hda1 /mnt/hda4              #포맷된 파일 시스템 /dev/hda4 를
/mnt/hda4 에 마운트한다.
```

5. 콘솔화면에서 TrackBack 설치하기

콘솔화면에서 TrackBack 을 설치한다...라기보다는 복사라고 생각하자.

```
# cp --preserve -R /{bin,dev,etc,home,lib,root,sbin,usr,var,opt,pentest} /mnt/hda3 # xcopy
# mkdir /mnt/hda3/{boot,mnt,proc,sys,tmp} # /boot, /home 은 마운트 디렉토리로 사용한다.
# cp /boot/vmlinuz /mnt/hda1/                                    # /mnt/hda1 에 커널을 복사한다.
```

6. GRUB 설치하기

GRUB 을 설치한다. GRUB 을 설치할 때 사용되는 명령어 installpkg 는 slackware 배포본에서 사용하는 패키지 관리 명령어다.

```
# wget ftp://ftp.slackware.com/pub/slackware/slackware-current/extra/grub/grub-0.97-i486-2.tgz
# installpkg grub-0.97-i486-2.tgz
# grub-install --root-directory=/mnt/hda3 /dev/hda3
# cd /mnt/hda1; mkdir grub; mv /mnt/hda3/boot/grub/* /mnt/hda1/grub/
```

GRUB 을 설치하고 나면 /dev/hda3/boot/에 GRUB 설치 파일이 만들어진다. 이것들을 모두 /mnt/hda1 에 옮겨놓는다.

7. GRUB 부트에 필요한 menu.lst 파일 만들기

vi 편집기를 이용해 GRUB 에서 부팅시 읽어들일 부트 메뉴 파일을 작성하고 저장한다.

```
# vi /mnt/hda/hda1/grub/menu.lst
default 0
timeout 3
hiddenmenu

title        Back|Track v2.0
root         (hd0,0)
kernel /vmlinuz root=/dev/hda3 ro vga=791
boot
```

8. fstab 파일 수정

fstab 파일을 수정해서 /dev/hda1 를 /boot 에, /dev/hda4 를 /home 에 마운트하도록 한다.

```
/dev/hda1       /boot          ext3          defaults          0          0
/dev/hda2       swap           swap       defaults          0          0
/dev/hda3       /                 ext3          defaults          0          0
/dev/hda4       /home       ext3          defaults          0          0
```

9. 시스템 시작

다 끝났다. 이제 "reboot" 명령을 입력하여 시스템을 재시작한다. 별 다른 문제 없이 부팅에 성공한다면 OK. 문제가 있다면? 그땐 OTL... 몰라!!!