:: F.T.Z 복구 매뉴얼 ::

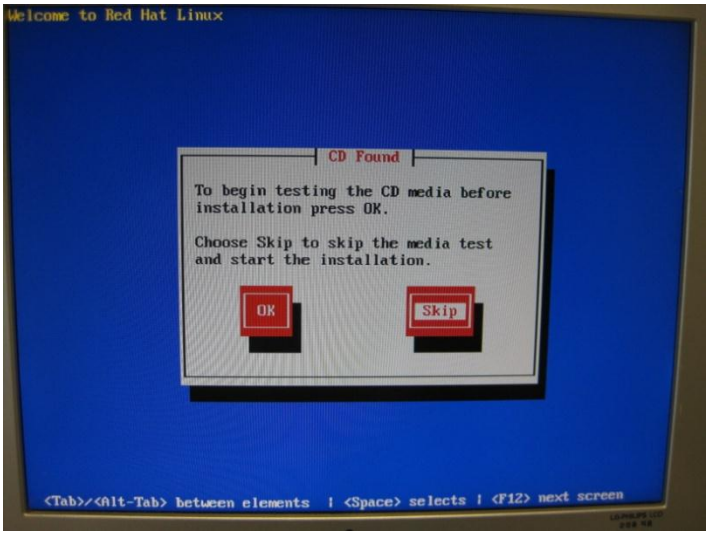
Redhat 9.0 설치

F.T.Z는 Redhat 9.0 리눅스 운영체제를 기반으로 구성되어 있습니다.
Redhat 9.0은 비교적 낮은 버전의 배포본에 속하는데, 이처럼 낮은 버전을 이용하는 이유는 최신 리눅스 배포본들의 경우 Buffer Overflow 등 취약점 공격에 대한 보안 장치가 뛰어나서 초보들이 쉽게 공략하기 힘들기 때문입니다. 반면 Redhat 9.0은 Buffer Overflow 등의 취약점 공격 연습을 하기에 적합한 환경을 가지고 있습니다.

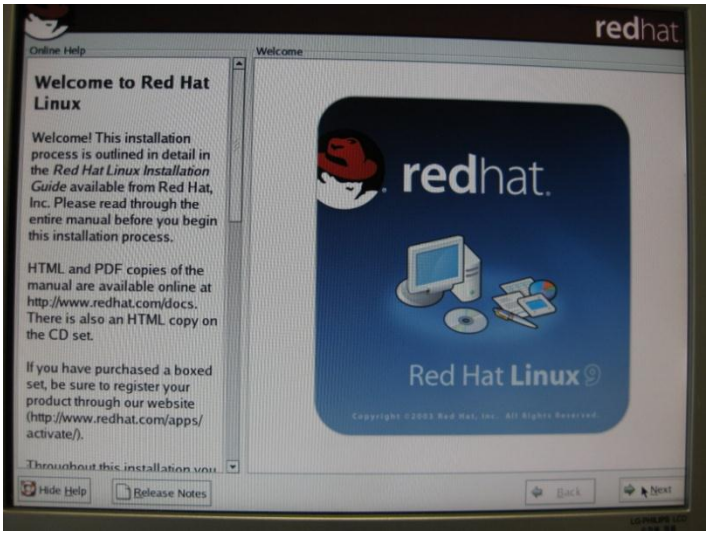
그럼 이제부터 Redhat 9.0을 설치해 보겠습니다.
다음과 같이 Redhat 9.0 CD 1~3번을 준비합니다.

이제 CD1을 넣고 부팅을 합니다.
(만약 CD 부팅이 되지 않는다면 CMOS 셋업에서 CD 부팅을 활성화 시켜주십시오.)

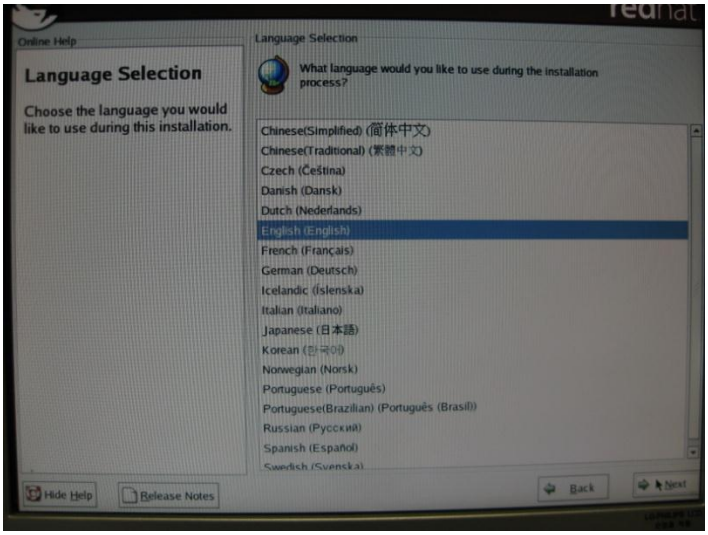
CD 무결성 체크는 SKIP을 해도 좋습니다.



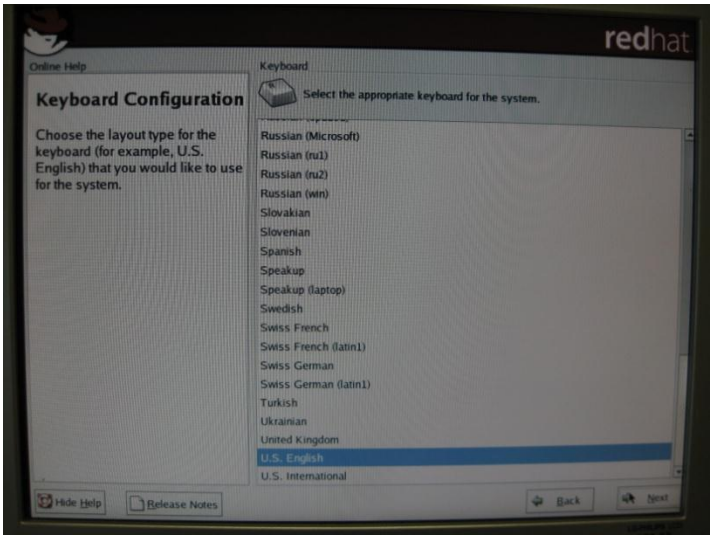
Next 버튼을 누릅니다.



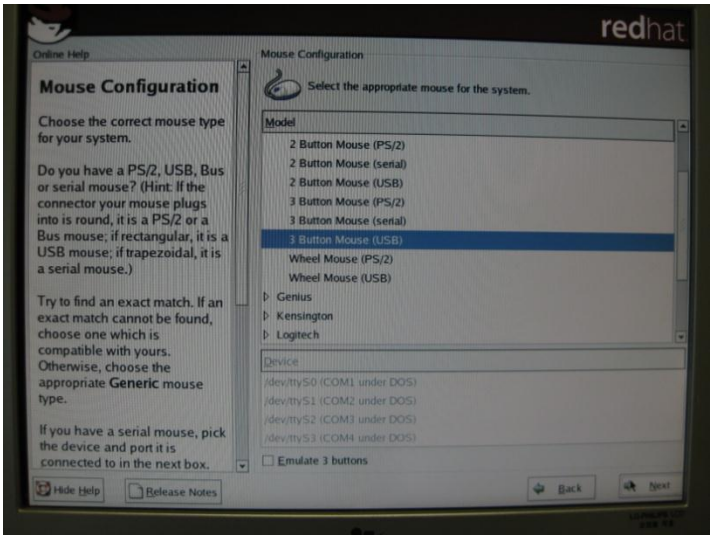
Next 버튼을 누릅니다.



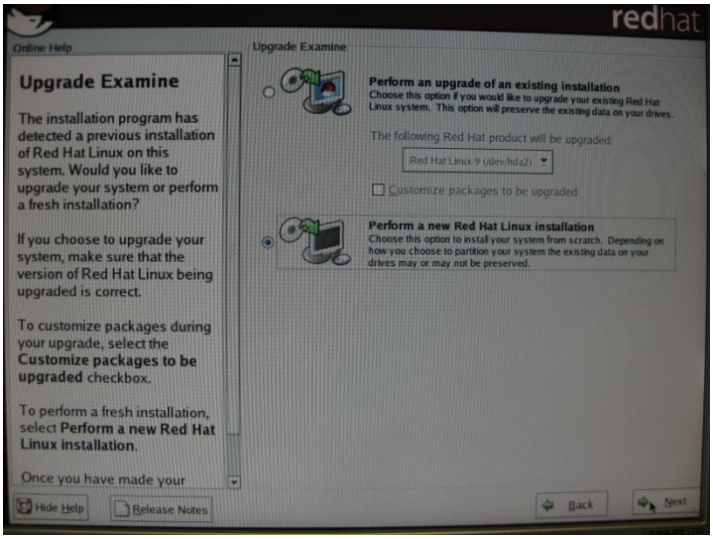
Next 버튼을 누릅니다.



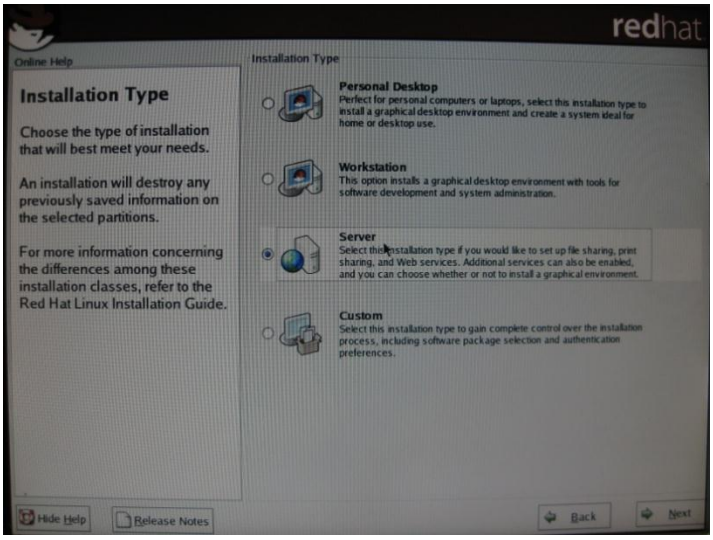
Next 버튼을 누릅니다.



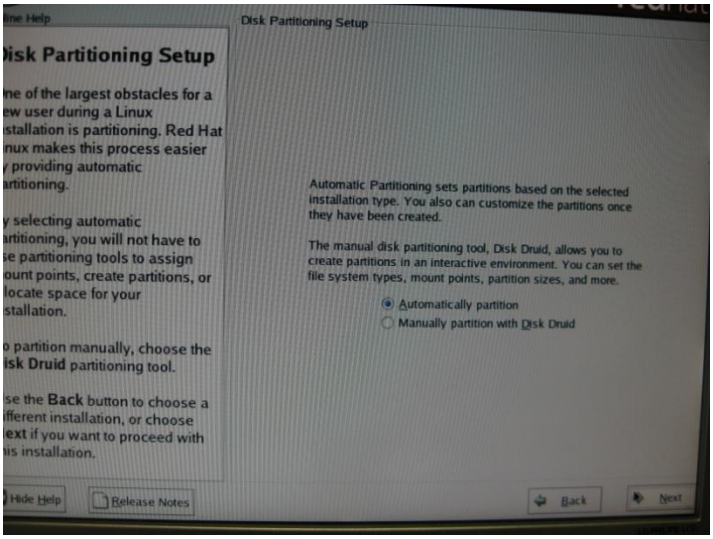
Perform a new Red Hat Linux installation을 선택합니다.



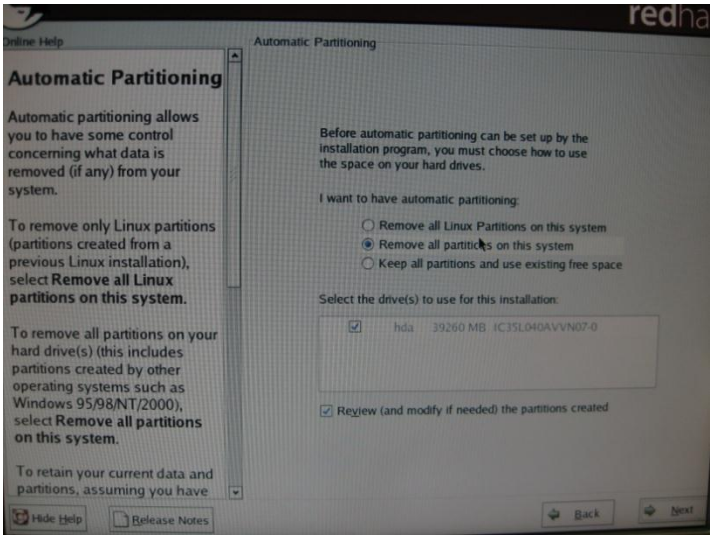
Installation Type으로 Server를 선택합니다.



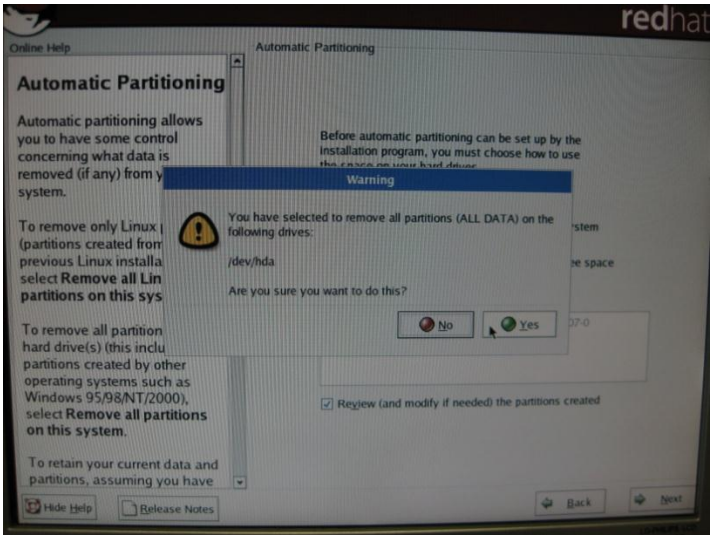
Automatically partition을 선택합니다.



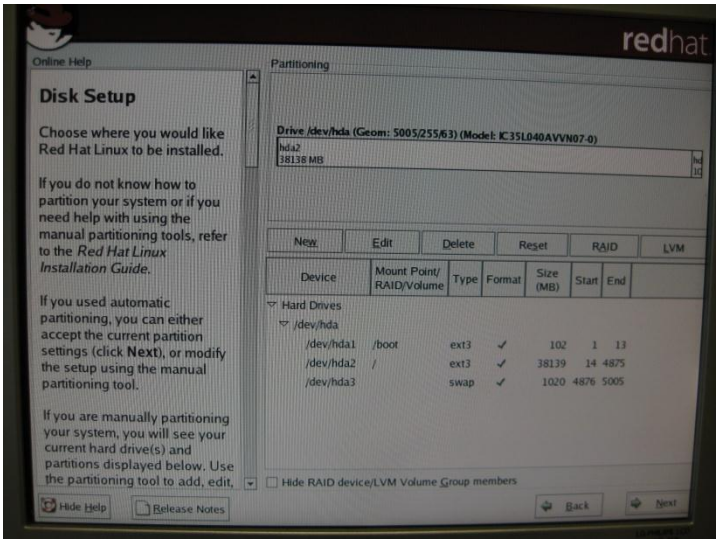
Remove all partitions on this system을 선택합니다.



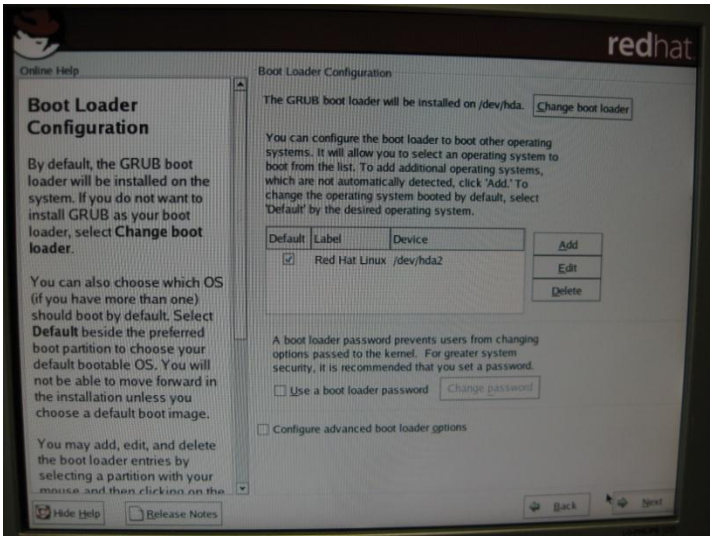
Yes를 선택합니다.



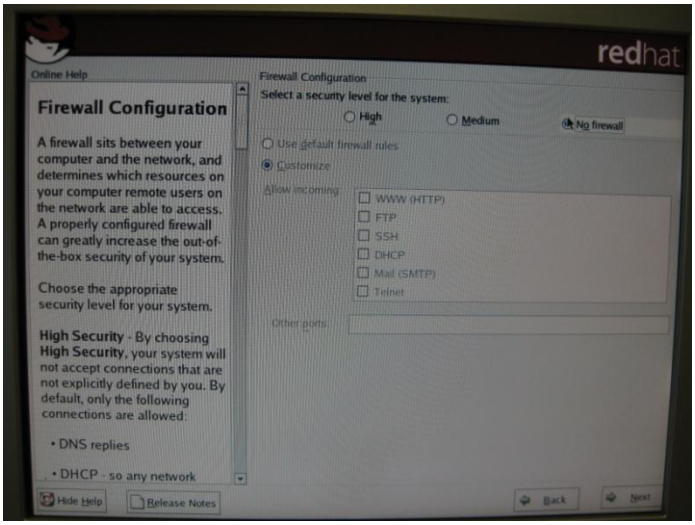
Next를 클릭합니다.



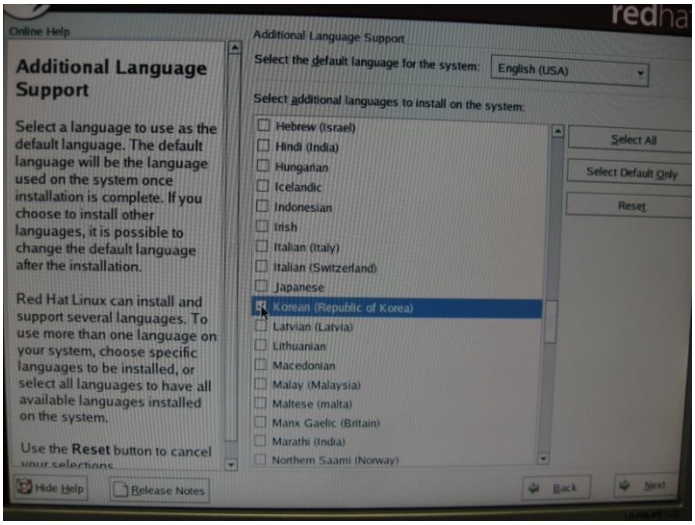
Next를 클릭합니다.



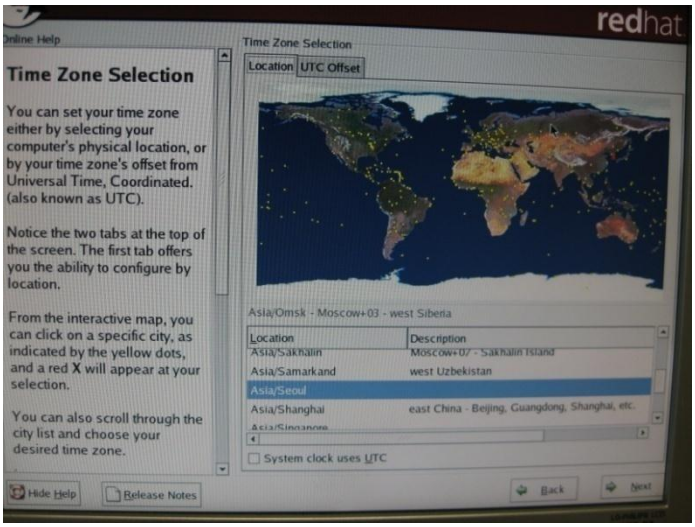
No firewall을 선택합니다. 방화벽을 켜 놓으면 외부에서의 접속이 안 되기 때문입니다.



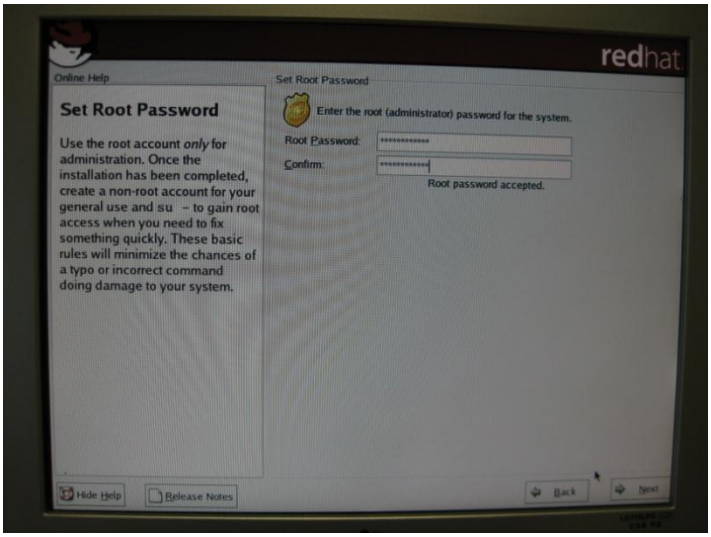
Korean 언어를 추가로 선택합니다.



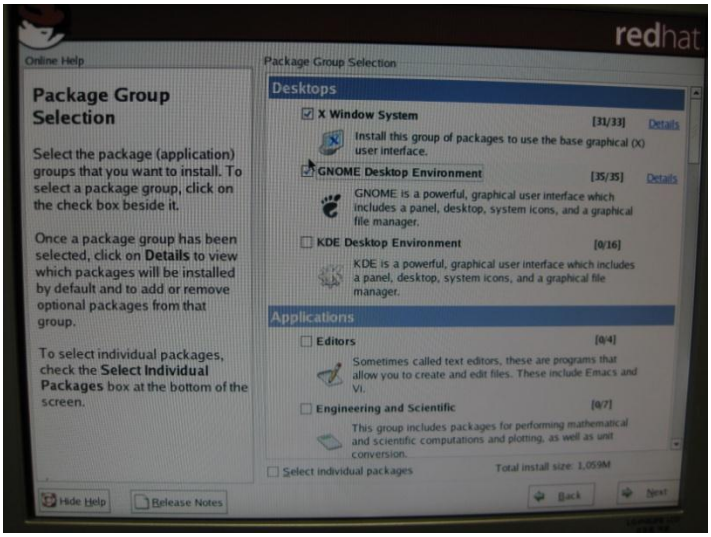
Time Zone은 Seoul을 선택합니다.



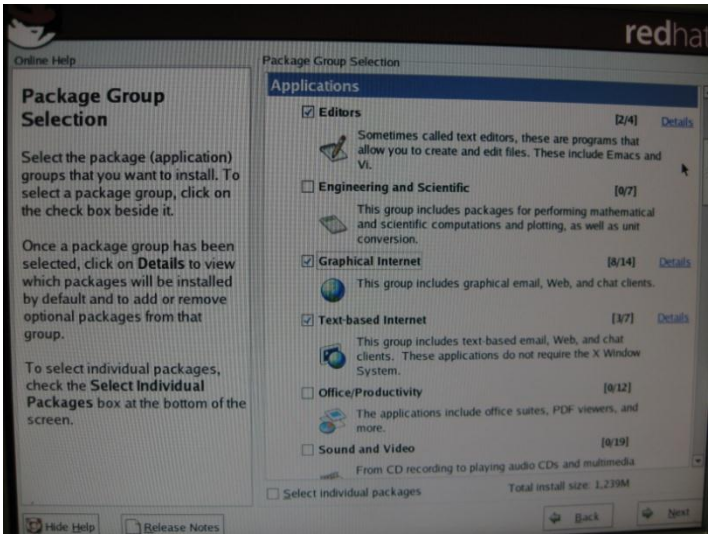
Root 암호를 설정합니다.



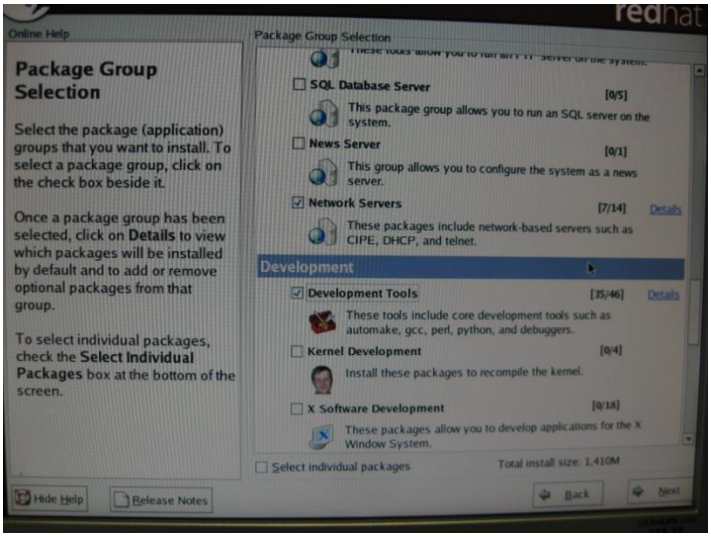
Desktops에 X Window System과 GNOME Desktop Environment를 선택해 줍니다.



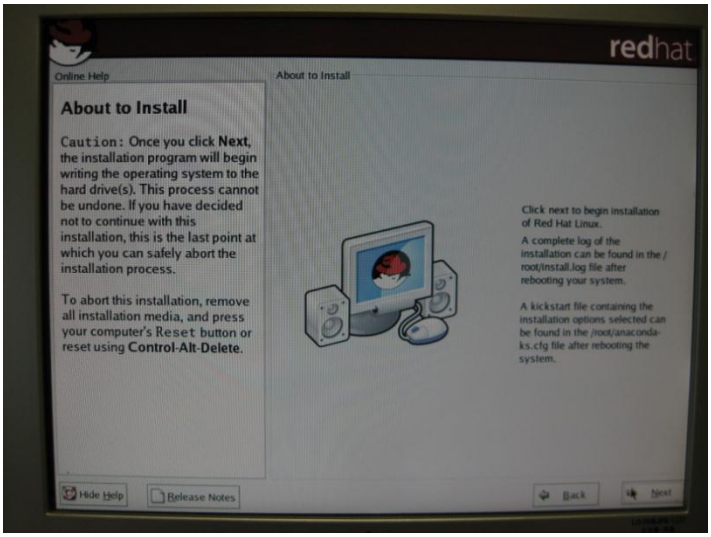
Applications에 Editors, Graphical Internet을 선택해 줍니다.



Development에 Development Tools를 선택해 준 후 Next 버튼을 클릭합니다.

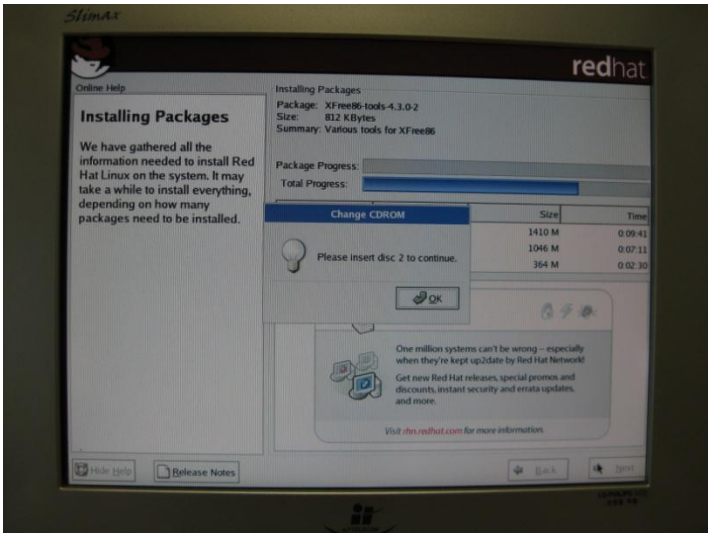


Next 버튼을 클릭합니다.

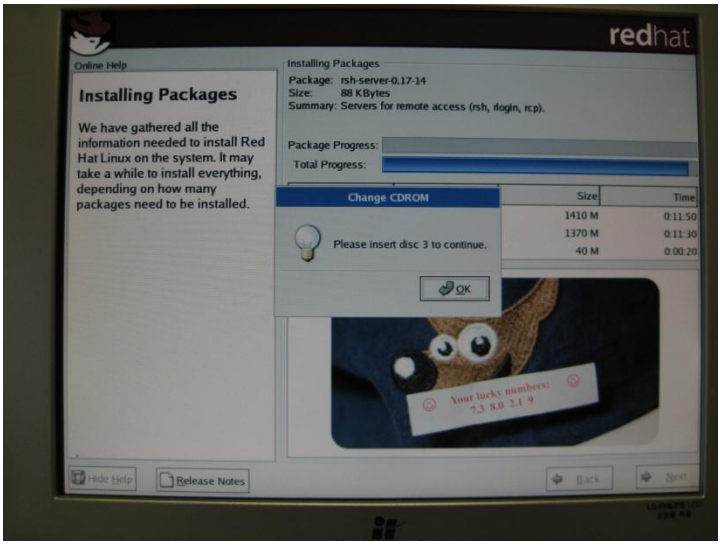


이제 하드디스크 포맷 및 설치가 시작됩니다.

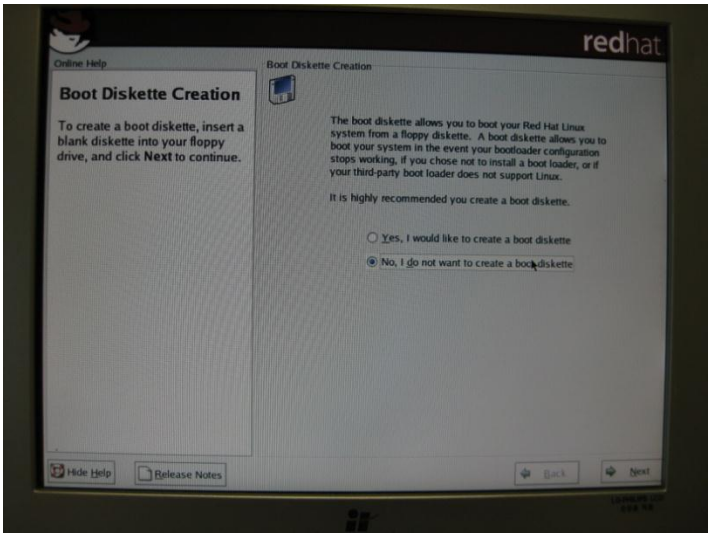
설치 도중 다음과 같은 화면이 나타나면 2번 CD를 넣어줍니다.



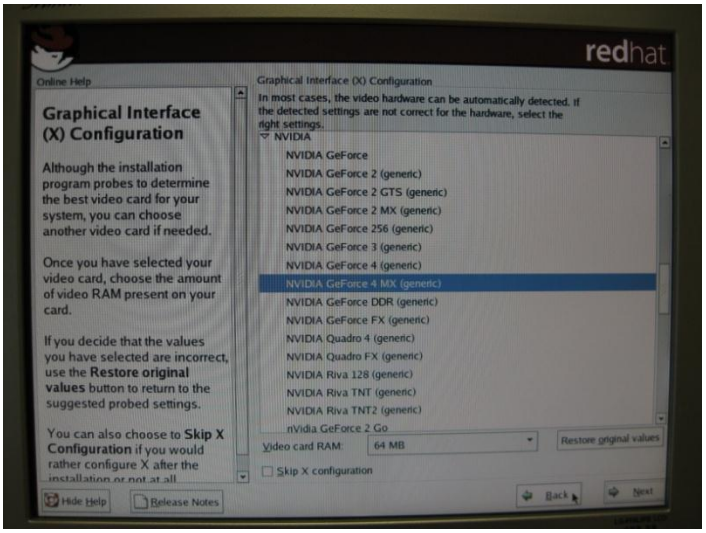
설치 도중 다음과 같은 화면이 나타나면 3번 CD를 넣어줍니다.



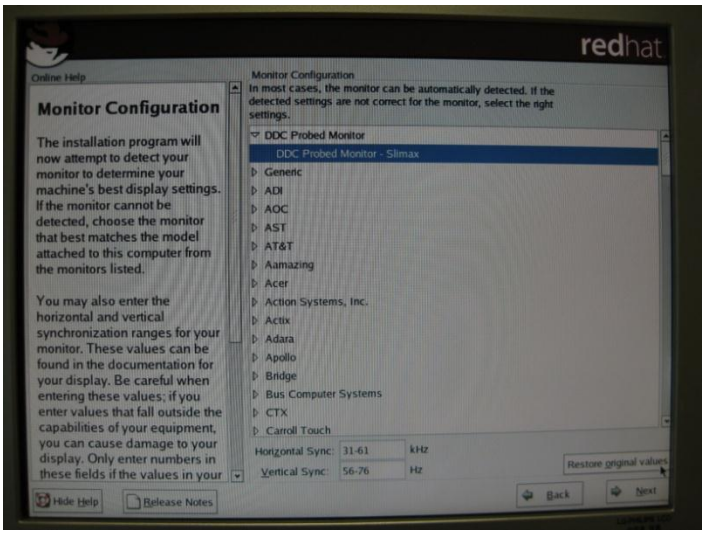
부팅 디스크를 따로 만들 필요는 없습니다.



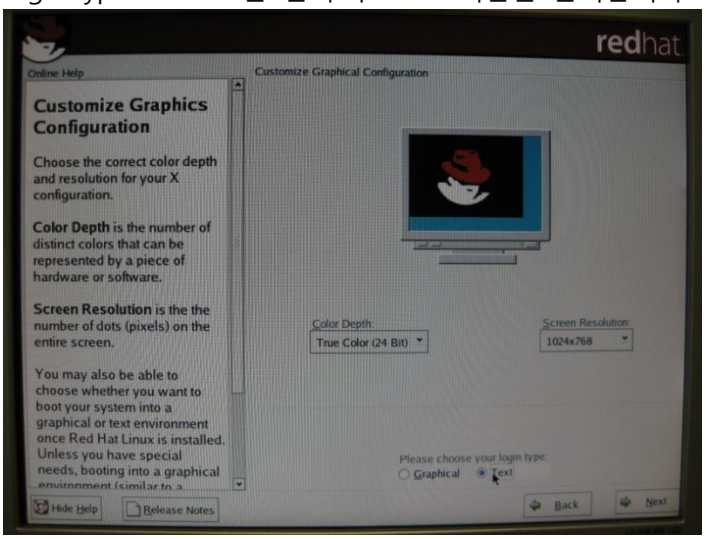
Next 버튼을 클릭합니다.



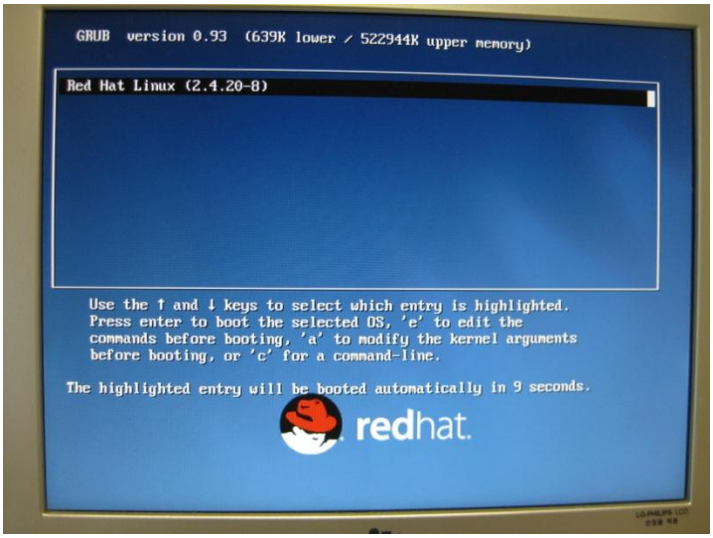
Next 버튼을 클릭합니다.



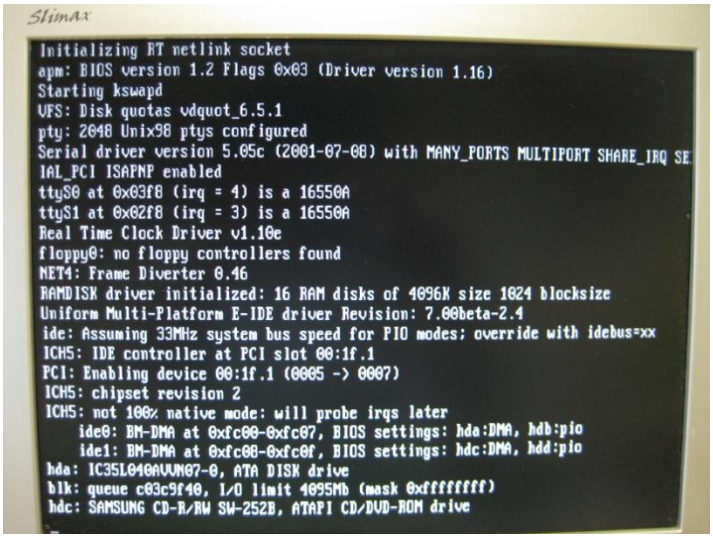
Login type으로 Text를 선택 후 Next 버튼을 클릭합니다.



이제 CD를 제거한 후, 재부팅을 하면 다음과 같이 boot loader가 나타납니다.



엔터를 치면 리눅스 부팅이 시작됩니다.



축하합니다. 리눅스 설치가 완료되었습니다.

:: F.T.Z 관련 파일 설치 ::

이제 다음의 절차에 따라 F.T.Z 관련 파일들을 설치합니다.

1. CD롬 마운트

1. F.T.Z 복구 CD를 시디롬에 넣습니다.
2. 다음과 같은 명령으로 마운트 시킵니다.

```
# mount /dev/cdrom /mnt/cdrom
```

* 사용을 마친 후엔 umount /dev/cdrom 명령으로 언마운트 시켜줍니다.

2. Trainer 1~10, Level 1~20 사용자 추가

```
# cat /mnt/cdrom/USER_INFO/passwd >> /etc/passwd
# cat /mnt/cdrom/USER_INFO/shadow >> /etc/shadow
# cat /mnt/cdrom/USER_INFO/group >> /etc/group
```

* >>(더블 리다이렉션)을 사용하면 기존 내용 뒤에 새로운 내용을 추가할 수 있습니다.

3. 원격 root 접속이 가능하도록 설정

```
# rm –rf /etc/securetty
```

* securetty 파일 안에 원격 root 접속을 금지하는 설정이 들어있기 때문입니다.

4. Trainer 1-10, Level 1~20 HOME 디렉토리, 파일 추가

```
# cd /home/
# cp –rf /mnt/cdrom/HOME/* .
# tar xvfzp home.gzip
# rm –rf home.gzip
```

* tar의 p 옵션을 통해 각종 권한 설정이 자동 복원됩니다.

5. 각종 문제 파일 설치

Level1 문제 파일 설치

```
# gcc –o /bin/ExecuteMe /mnt/cdrom/LEVELS/LEVEL1/ExcuteMe.c
# chown level2.level1 /bin/ExecuteMe
# chmod u+s /bin/ExecuteMe
# chmod o-rwx /bin/ExecuteMe
```

chattr +ai /bin/ExecuteMe

* chattr 명령은 다른 사용자들이 해당 명령을 변경할 수 없도록 방어해 줍니다.

Level2 문제 파일 설치

gcc –o /usr/bin/editor /mnt/cdrom/LEVELS/LEVEL2/editor.c
chown level3.level2 /usr/bin/editor
chmod u+s /usr/bin/editor
chmod o-rwx /usr/bin/editor
chattr +ai /usr/bin/editor

Level3 문제 파일 설치

gcc –o /bin/autodig /mnt/cdrom/LEVELS/LEVEL3/autodig.c
chown level4.level3 /bin/autodig
chmod u+s /bin/autodig
chmod o-rwx /bin/autodig
chattr +ai /bin/autodig

Level4 문제 파일 설치

cp /mnt/cdrom/LEVELS/LEVEL4/backdoor /etc/xinetd.d/
chown root.level4 /etc/xinetd.d/backdoor
chattr +ai /etc/xinetd.d/backdoor
cp /bin/ls /home/level4/tmp/backdoor
chown level4.level4 /home/level4/tmp/backdoor
/etc/init.d/xinetd restart
rm –rf /home/level4/tmp/backdoor

* backdoor 파일이 있어야 79번 포트(finger)가 열리게 됩니다.

Level5 문제 파일 설치

gcc –o /usr/bin/level5 /mnt/cdrom/LEVELS/LEVEL5/level5.c
chown level6.level5 /usr/bin/level5
chmod g-r /usr/bin/level5
chmod u+s /usr/bin/level5
chmod o-rwx /usr/bin/level5
chattr +ai /usr/bin/level5

Level6 문제 파일 설치

Level6의 문제 파일은 home.gzip의 압축을 풀 때 자동으로 설치됩니다.

Level7 문제 파일 설치

```
# gcc –o /bin/level7 /mnt/cdrom/LEVELS/LEVEL7/level7.c
# chown level8.level7 /bin/level7
# chmod g-r /bin/level7
# chmod u+s /bin/level7
# chmod o-rwx /bin/level7
# chattr +ai /bin/level7
```

Level8 문제 파일 설치

```
# cp /mnt/cdrom/LEVELS/LEVEL8/found.txt /etc/rc.d/found.txt
# chown root.level8 /etc/rc.d/found.txt
# chmod o-rwx /etc/rc.d/found.txt
# chattr +ai /etc/rc.d/found.txt
```

Level9 문제 파일 설치

```
# gcc –o /usr/bin/bof /mnt/cdrom/LEVELS/LEVEL9/bof.c
# chown level10.level9 /usr/bin/bof
# chmod g-r /usr/bin/bof
# chmod u+s /usr/bin/bof
# chmod o-rwx /usr/bin/bof
# chattr +ai /usr/bin/bof
```

Level10 문제 파일 설치

Level10의 문제 파일은 home.gzip의 압축을 풀 때 자동으로 설치됩니다.

실행만 해주시면 됩니다.

```
# /home/level10/program/level10
```

Level11~20 문제 파일 설치

Level11~20의 문제 파일은 home.gzip의 압축을 풀 때 자동으로 설치됩니다.

My-pass 프로그램 설치

```
# gcc –o /bin/my-pass /mnt/cdrom/ETC/my-pass.c
# chmod o-rw /bin/my-pass
```

Level4, Level10 재부팅 후 자동 실행

cp –rf /mnt/cdrom/ETC/rc.local /etc/rc.local

* /etc/rc.local 스크립트는 부팅 시 자동 실행됩니다.

매 10분마다 Level4, Level5 관련 파일 초기화

crontab /mnt/cdrom/ETC/cron_root

* cron_root의 내용을 기반으로 cron 설정을 재등록 합니다.

6. 서버 배너 변경

cp –rf /mnt/cdrom/ETC/issue.net /etc/issue.net

7. 한글 사용 가능하도록 변경

cp –rf /mnt/cdrom/ETC/.bashrc.txt /etc/skel/.bashrc

cp –rf /mnt/cdrom/ETC/bashrc /etc/bashrc

8. telnet 서비스 활성화

cp –rf /mnt/cdrom/ETC/telnet /etc/xinetd.d/telnet

/etc/init.d/xinetd restart

9. web 서비스 활성화

/etc/init.d/httpd start

* 재부팅 후엔 rc.local에 의해 httpd가 실행됩니다.

[참고]

CD 마운팅 후 /mnt/cdrom/AUTO_SCRIPT/auto_script.sh을 실행하면 위 과정을 자동으로 수행해 줍니다. 하지만 경험 축적을 위해 되도록이면 직접 실습을 해보실 것을 적극 권장합니다.

이로써 F.T.Z 설치가 완료되었습니다.

수고하셨습니다.!

문의 사항 : 010-2762-5002 멍멍