

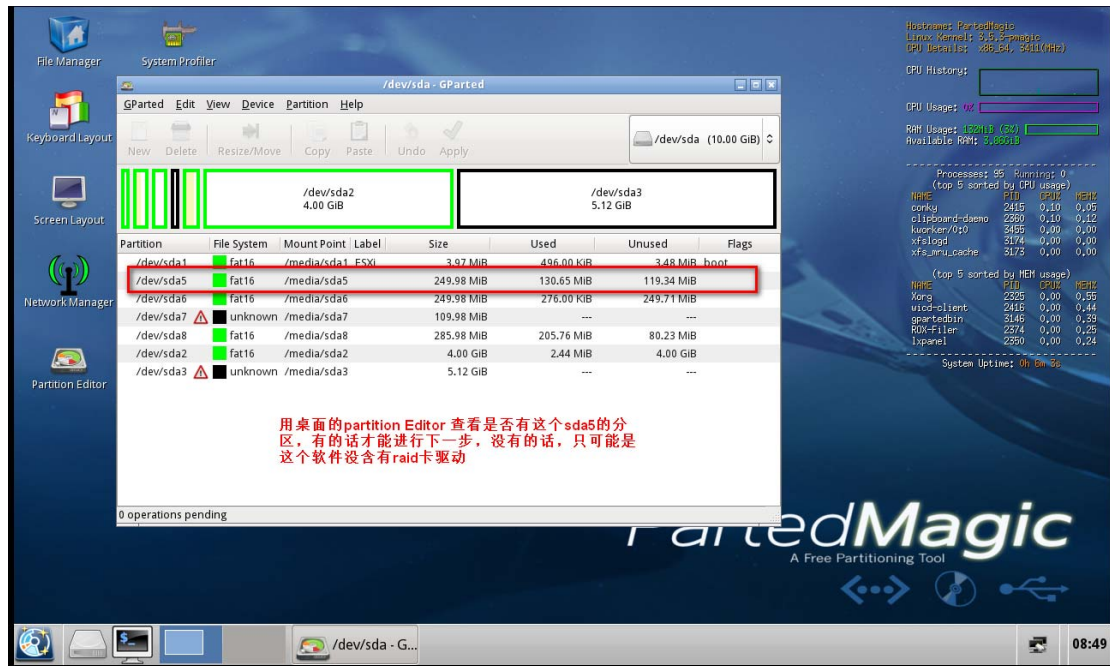
1. 破解密码要重启主机,所以首先迁移虚拟机到别的主机,之后重启服务器,用 parted magic 光盘 (PM) 启动服务器 , 具体您是量产 U 盘还是用光盘, 还是用光驱, 自己想法子! 下载 PM 地址如下

<http://sourceforge.net/projects/partedmagic/>

最新版本是 2013.5.1 日的,为啥要用这个盘启动呢? 其实用 liunx 安装盘进 rescue 模式也可以,但有个麻烦事,就是如果主机服务器的硬盘是用 RAID 卡管理的话,就要挂载 RAID 卡驱动,我想找驱动再找挂载方法很麻烦,这个 PM 盘带有很多 RAID 卡的驱动,咱就是偷懒了。

PM 盘主要用来调整分区的,或者把倒数据的,比如你系统挂了,可以直接接一个 USB 硬盘,直接把原来坏系统的硬盘里的东西倒腾出来,他识别文件系统非常多,一般 LINUX 和 WINDOWS 都可以

2. 启动后选择默认



3. 之后先进终端下图左下角那个

```
cd /
```

```
mkdir /mnt/sda5    #建立一个目录
```

```
mount /dev/sda5 /mnt/sda5  #挂载
```

```
cd /mnt/sda5
```

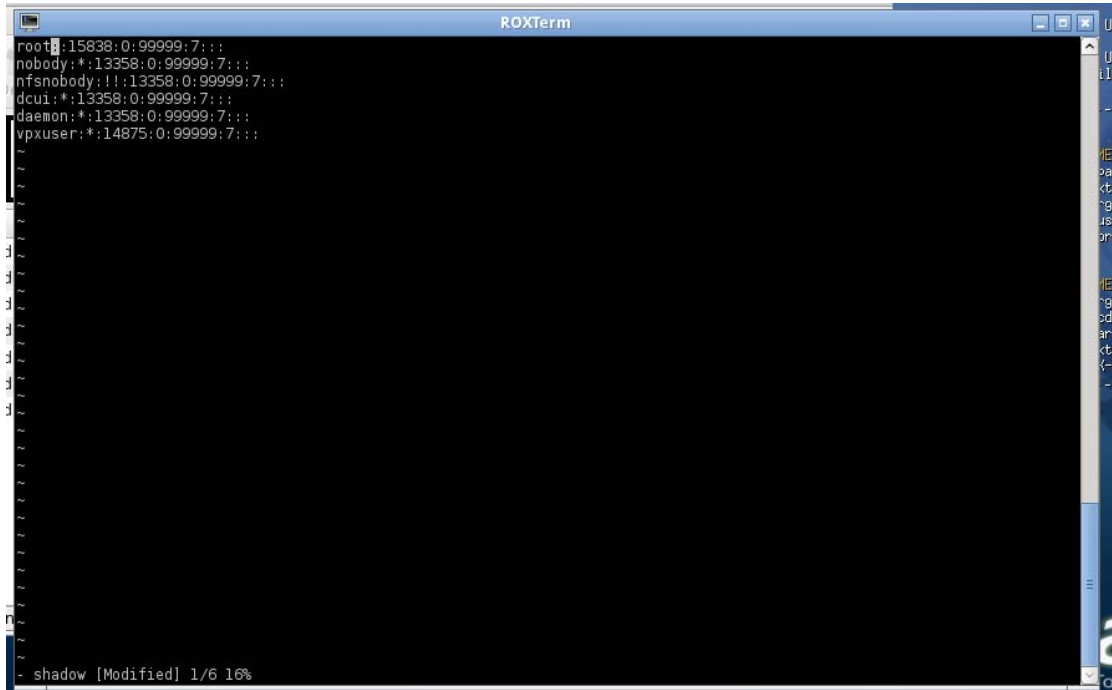
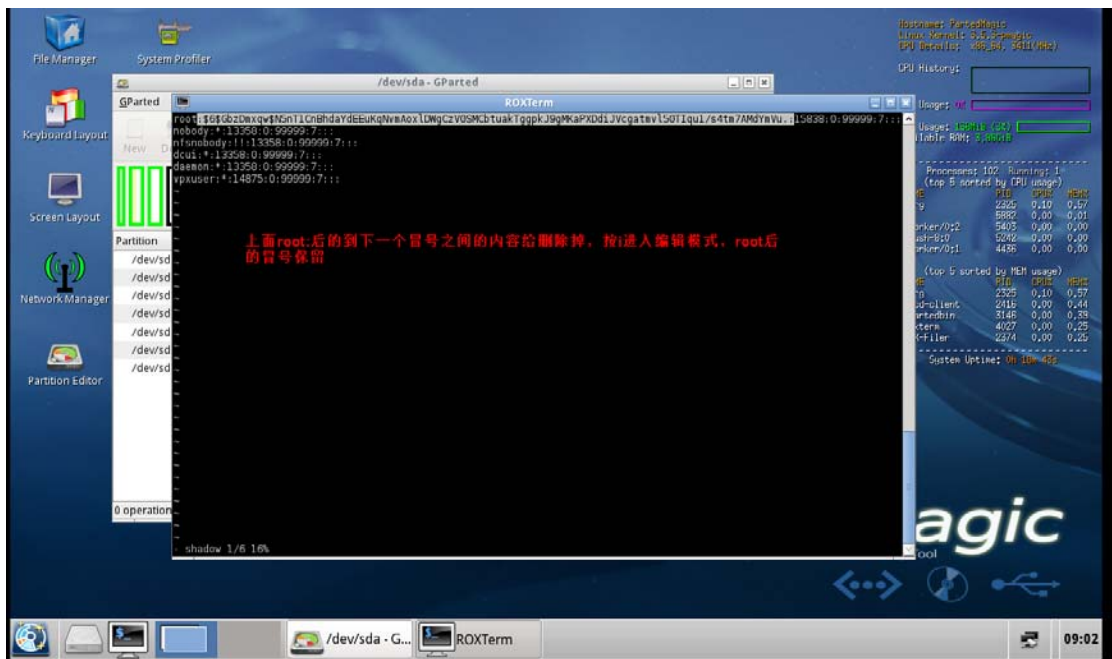
```
ls
```

确认下有 state.tgz 文件

```
tar zxvf state.tgz  #解压这个文件,得到 local.tgz
```

```
tar zxvf local.tgz  #解压 local.tgz 得到 etc 目录
```

```
vi /mnt/sda5/shadow
```



Esc

:wq 保存

rm -rf state.tgz local.tgz #删除之前的原文件, 如果不放心, 可以先 cp 到别的目录备份

tar zcpf local.tgz etc #压缩 etc

tar zcpf state.tgz local.tgz #压缩 local.tgz

cd /

umount /mnt/sda5 #卸载

4.之后拿出光盘重启, 看看密码还有没有?

Esxi 4.1, 5.0, 5.1U1 测试通过