



链滴

CentOS_note_4

作者: [zhuhonglin](#)

原文链接: <https://ld246.com/article/1494639962128>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

系统启动

普通 pc 机系统启动的流程：

-

BIOS

-
-

MBR: Boot Code

-
-

GRUB

-
-

加载内核

-
-

执行 init

-
-

runlevel

-

BIOS

Basic Input Output System, 基本输入输出系统, 称之为 BIOS。保存在电脑的主板上。

BIOS, 第一负责检查硬件, 第二查找可启动的设备 (如硬盘, U 盘等)

>

可启动设备是指里面包含引导代码

<

MBR

MBR 不属于任何系统, 他其实是硬盘最开始的 512 个字节。

BIOS 启动其内含的引导代码。引导代码去加载 GRUB (一个更复杂的引导程序, 因为 MBR 只少量字节, 只能作为一个跳板或者中转站)

>

MBR 前 446 字节为引导代码, 后面第 447 到 512 个字节用来让 BIOS 识别自己。

<

GRUB

Linux 的主流引导程序。使用范围很广。

GRUB 相关文件保存在 centos 的 /boot/grub 目录中

转到这个目录下

会出现几个主要的文件, 如 stage1, stage2, grub.conf(启动配置)

内核

之后加载内核。

内核保存在 /boot/vmlinuz 字样的文件里。一同加载的还有一个驱动打包文件, 同一目录下 initramf 字样的文件。

>

Linux 的内核是精简的内核, 所以一些驱动都放在另一个文件里, 在需要的时候再动态加载, 从不会影响速度。

<

init

init 是操作系统上的第一个进程 (pid 是 1), 内核去运行他。并且一直存在这个进程, 直到系统关闭。

init 进程: 初始化系统, 挂载系统文件, 根据级别去启动服务

这里的级别就是下面的 runlevel, 他决定系统以什么级别运行, /etc/inittab 可以修改默认运行级别

<p>/etc/init 下也有很多初始配置文件</p>

<h3 id="runlevel">runlevel</h3>

<p>Linux 的运行级别。总共分为 7 个级别。</p>

<p>一般常用</p>

<p>级别 0: 关机</p>

<p>级别 3: 不使用图形界面</p>

<p>级别 5: 使用图形界面</p>

<p>级别 6: restart</p>

<h2 id="防止物理修改root密码">防止物理修改 root 密码</h2>

<p>之前说到系统启动的流程，实际上是可以在这个流程里，通过物理接触主机的方式，直接修改 root 密码，并且你不需要输入原来的密码。</p>

<p>步骤如下：</p>

<p>在启动时，使用上下键，使得系统停在 grub 的引导界面</p>

<p>使用 e 修改引导配置。</p>

<p>在引导内核的一行最后加入数字 1（效果就是 grub 告诉内核，你按照级别 1 去启动系统，级别 1 是一个单用户模式，自动进入 root）</p>

<p>进入系统后直接使用 passwd 直接修改密码就行</p>

<p>从这里可以看出，只要有人接近你的主机，就可以用物理的方式修改你的 root 密码，从而获得 root 权限。因此需要一个特殊的 grub 密码。</p>

<p>grub 密码是指，对之前的步骤 2 进行了修改，如果要进入修改引导配置，需要先输入 grub 密码，许可后才可以修改。</p>

<h3 id="配置grub密码">配置 grub 密码</h3>

<p>在 grub.conf 文件中，加入一行：</p>

password --md5 |aodf.....

<p>这个密码还是用 md5 方式加密的，更安全一点，最后那串东西是 md5 加密后的密码，当然也可以直接明文，password 后跟上密码。</p>

<blockquote>

<p>Linux 自带的 grub-md5-crypt 命令可以帮助生成 md5</p>

</blockquote>

<h2 id="总结">总结</h2>

<p>其实在 grub 密码配置这一段，已经涉及到了信息的保护，信息安全的保护很复杂，没有一个完的保护方案。</p>

<p>技术只能作为保护的一面，关键突破还在于人。即使是 grub 加密，仍然可以通过把硬盘偷走，载到别的 Linux 系统下进行修改从而获得信息这种物理的手法。</p>

<blockquote>

<p>大部分人都觉得自己的家是安全的，直到有一天忽然发现自己被锁在了门外，我们的看法才会在那间改变，才明白原来安全漏洞是那么明显</p>

</blockquote>

<blockquote>

<p>-- 《社会工程-安全体系中的人性漏洞》</p>

</blockquote>