# Linux主机防护系统技术手册(v1.0)

目录

[Linux主机防护系统技术手册(v1.0) 1](#_Toc482624781)

[第一章、 软件简介 3](#_Toc482624782)

[1.1、介绍 3](#_Toc482624783)

[1.2、防护系统能为您提供什么保护 3](#_Toc482624784)

[1.3、运行环境 3](#_Toc482624785)

[1.4、部署方式 3](#_Toc482624786)

[第二章、 软件功能 4](#_Toc482624787)

[2.1、安全管理员账户功能 4](#_Toc482624788)

[2.2、审计员账户功能 9](#_Toc482624789)

[第三章、 技术特色 11](#_Toc482624790)

[第四章、 后续计划 12](#_Toc482624791)

1. 软件简介

1.1、介绍

Linux主机防护系统是为企业级用户提供的，全方位的Linux操作系统保护软件，能有效防止病毒威胁，V2.0版本将支持二级部署和集中管理，同时符合等级保护要求，采用三权分立的设计，让管理账户和审计账户分离。

1.2、防护系统能为您提供什么保护

本系统可以实现多种保护，举例如下（实际保护不仅限于以下例子）：

1. 近期爆发的全球敲诈勒索蠕虫病毒Wannacry，一旦中招，系统中的图片和文档被加密，只能通过支付比特币来获取解密密钥来解密文件。使用本系统，只要配置策略，例如：限制对\*.doc、\*.jpg等的写操作，即可拦截该病毒对图片和文档的加密或修改，避免被勒索。
2. 系统部署重要服务时候，时间的准确性很重要，如果系统时间被修改，会导致系统服务同步出现异常甚至奔溃，使用本系统可以拦截系统时间修改。
3. 部分恶意病毒会破坏系统启动文件，导致系统无法正常启动，要求用户付费或者付出一定代价才能恢复，甚至即便付费也无法恢复。使用本系统可以保护系统启动文件不被破坏。
4. USB和CDROM也是病毒传播重要途径，本系统可以拦截USB和CDROM的加载，防止病毒自动传播。
5. 部分病毒会修改系统的动态库文件，以达到截获和修改应用数据的目的，本系统可以保护系统的库文件不被修改。
6. 一般主机的最后一道防线是ROOT权限，当系统被入侵之并获取ROOT权限后，主机就完全沦陷了，入侵者可以对主机做任何想做的操作，而本系统最大的优点在于：即便入侵者获取ROOT权限，依然不能为所欲为，依然会受到本系统设定权限的限制，因为本系统工作在操作系统的更底层，入侵者即便获取ROOT权限依然无法绕过本系统的拦截。
7. 本系统可以提供的保护不仅限于以上几种，上面只是一小部分常见场景的举例。

1.3、运行环境

运行环境为Linux操作系统，目前支持的操作系统为：

|  |  |  |
| --- | --- | --- |
| 操作系统 | 软件版本 | 备注 |
| CentOS\_6.4 x86\X64 | v1.0 | 支持 |
| CentOS\_6.5 x86\x64 | v1.0 | 支持 |
| 其他Linux系统 | v1.0 | 支持，但需要单独编译内核，额外耗时1周 |

1.4、部署方式

部署方式有两种：单机版，集中管理版本。

1.4.1、单机版部署

V1.0目前只有单机版，所以只支持单机部署，用来保护单台主机。

1.4.2、集中部署

V2.0版本将支持二级部署和集中管理，可以对批量机器进行管理和保护。

1. 软件功能

2.1、安全管理员账户功能

2.1.1、登录安全验证

登录采用密码认证，管理员和审计员账户分离，独自验证。



2.1.2、首页总揽

主界面展示了系统的基本状态和信息。采用图像化展示，美观，且直观。可以方便的看到系统的安全事件概况。



2.1.3、基础防护

用来配置系统的安全项，采用开关方式来配置，不需要用户懂技术就可以很方便的进行配置，这里的保护包括了对系统配置文件、系统库文件、系统程序文件、系统启动文件等的保护，还包括对网络操作的FTP、Telnet、POP/SMTP、HTTP访问的拦截。

基础防护不仅限于以下几项，再后续的版本中将增加更丰富的配置项，例如：对图片和文档的保护，以阻住敲诈者病毒加密用户的图片和文档。

同时还支持“监视模式”和“防护模式”，方便您随时切换，以适应不同的环境。



2.1.3.1、防护模式

模式有两种：

a）、监听模式

对触犯安全防护规则的操作，只进行日志记录，不会做拦截操作。

b）、防护模式

对触犯安全防护规则的操作，进行日志记录，并且拦截操作。

2.1.3.2、禁止修改系统配置

开启后，会对Linux系统的etc目录进行保护，防止恶意程序修改、删除该目录下的文件。很多病毒都会修改系统目录下的文件，而此项开启后，则可以拦截病毒对系统配置目录的操作。

2.1.3.3、禁止修改系统库文件

开启后，会对系统的动态库和静态库文件进行保护，防止恶意程序破坏，某些病毒，比如键盘记录者会替换系统的特殊库文件，拦截和记录用户的键盘操作记录，而开启此项，则可以起到拦截恶意操作保护系统的目的。

2.1.3.4、禁止修改系统程序文件

开启后，会对bin目录下的系统可执行文件进行保护，防止恶意程序修改和替换系统可执行文件。

2.1.3.5、禁止修改系统启动文件

开启后，会对boot目录进行保护，防止恶意程序破坏启动文件。有部分敲诈者病毒会对系统启动文件进行修改，阻止系统启动，从而敲诈用户，而开启此项，则可以避免此类病毒的危害。

2.1.3.6、禁止FTP访问

开启后，会拦截系统的FTP访问。

2.1.3.7、禁止Telnet访问

开启后，会拦截系统的Telnet访问。

2.1.3.8、禁止POP/SMTP访问

开启后，会拦截系统的POP/SMTP访问。

2.1.3.9、禁止HTTP访问

开启后，会拦截系统的HTTP访问请求。

2.1.4、特殊资源

特殊资源配置项，采用开关方式来配置，不需要用户懂技术就可以很方便的进行配置，这里包括了：禁止修改系统时间、禁止关机和重启、禁用光驱、禁用USB存储设备等。



2.1.4.1、防护模式

模式有两种：

a）、监听模式

对触犯安全防护规则的操作，只进行日志记录，不会做拦截操作。

b）、防护模式

对触犯安全防护规则的操作，进行日志记录，并且拦截操作。

2.1.4.2、禁止修改系统时间

开启后，系统时间将做为一个资源被保护，不可修改，一些恶意的攻击会修改主机的时间，导致主机上应用出现紊乱甚至崩溃，而此项保护开启后可以拦截此类攻击。

2.1.4.3、禁止关机和重启

开启后，系统将无法关机或者重启，在主机端可以有效的防止恶意关机导致服务异常。

2.1.4.4、禁用光驱

开启后，光驱将无法正常加载，可以防止攻击者使用CD携带恶意程序现场对主机进行破坏。

2.1.4.5、禁用USB存储设备

开启后，USB存储设备将无法正常加载，可以防止攻击者使用CD携带恶意程序现场对主机进行破坏。

2.1.5、高级配置

高级配置功能，是提供给专业人员使用的，用来做一些更为复杂的规则和策略使用的，将在v2.0之后考虑是否开放此功能，对于普通用户，不提倡使用，因为高级策略的配置，需要用户理解软件的原理和策略的模型，并且错误的策略会对系统带来一定的风险，故不对普通用户开放此功能，这里也不做详细说明，如有特殊需求可以单独提供配置说明。



2.1.6、系统设置

2.1.6.1、设置登录密码和授权码

修改登录密码后点击提交会返回是否修改成功，失败则提示错误原因。

软件授权：

我们会根据每个机器码生成一个注册码，用户将注册码复制粘贴后，点击注册，即可看到注册状态。未注册的用户，是无法正常使用软件的功能的。



2.1.6.2、设置白名单

在白名单里的程序，其所有操作都会被放行，此项用来过滤一些特程序以及做系统调优。



2.1.6.3、自保护

自保护是对防护系统自身的保护，防止有恶意软件去停止或者修改防护系统，开启后系统将不可卸载和停止，如果需要卸载防护系统，需要先停止自保护。



2.2、审计员账户功能

2.2.1、登录安全验证

登录采用密码认证，管理员和审计员账户分离，独自验证。



2.2.2、首页概览

与管理员账户首页一致，主界面展示了系统的基本状态和信息。采用图像化展示，美观，且直观。可以方便的看到系统的安全事件概况。



2.2.3、安全事件

用来查看发生的安全事件，很详细的记录了每个安全事件的信息，包括：用户名称，哪个进程对哪个对象进行了何种操作，被软件的哪个模块所拦截，当前的保护模式是什么，最终的操作结果是放行还是拦截，以及操作发生的精确时间。同时事件查看还支持按时间段的模糊查询，可以通过选择时间段，输入关键字，筛选符合条件的事件。



2.2.4、运行事件

记录和查询软件的操作和运行记录。例如哪个用户登录了管理界面，并且进行了哪些操作。同时事件查看还支持按时间段的模糊查询，可以通过选择时间段，输入关键字，筛选符合条件的事件



2.2.5、系统设置

2.2.5.1、设置登录密码

修改当前审计管理员的登录密码，点击提交会返回是否修改成功，失败则提示错误原因。



1. 技术特色

Linux主机防护系统是在系统内核层，对系统的各种操作进行拦截过滤，是更深层、更全面的拦截和防护方案。尤其对系统已经被黑客攻破、root权限已经泄漏的情况下，可以防止黑客进一步破坏系统，或者窃取重要数据。

1. 后续计划

|  |  |  |
| --- | --- | --- |
| 版本 | 功能 | 备注 |
| V1.0 | 基础保护功能 | 已完成 |
| V2.0 | 1. 增加集中管理 2. 批量部署 | 计划中 |
| V3.0 | 1. 扩展基础保护项 2. 针对不同应用设计不同的策略套餐 |  |