**rootkit端口复用取证工具**

本工具使用了rootkit内核级隐藏技术,具有很高的隐藏性和穿透连接功能。能隐藏运行在常见Linux系统，并在内核层做到连接劫持，可以复用对外的端口，去连接管理被控制的主机，通信行为隐藏于正常的流量之中。

本工具使用了bin合并技术，编译时把应用层程序加密融合于ko驱动文件中，安装时只有ko文件。ko驱动启动时会自动释放、隐藏应用层程序。

对chkrootkit、rkhunter、管理工具(ps,netstat等)都做了技术绕过与隐藏，也查看不到被隐藏的**网络、端口、进程、文件信息。**

为保证软件稳定性，各功能也经过压力测试。

支持:Linux Kernel 2.6/3.x/4.x 支持x32与x64系统。

支持版本:Redhat, CentOS, Debian, Fedora, Ubuntu等linux系统。

**技术特点：**

1。内核rootkit技术

采用rootkit内核技术,可以更深度的做到隐藏与保护，深度的利用开放的端口，去控制被控主机，隐藏于正常流量中。对常见的管理工具做了内核级的隐藏。

2。使用bin合并技术

bin合并技术，把应用层程序加密编译到ko文件中，使用时，自动解密释放并执行。

3。支持交互式pty shell

支持交互式pty shell,可以更方便的对主机进行远程操作。

4。内核级隐藏网络、端口、进程、文件

在内核级隐藏了网络连接,进程,端口,文件信息,也可以自定义隐藏的文件，进程。

5。通信加密处理

复用端口，连接成功后,网络的通信是经过数据加密的,保护通信的内容。

6。支持文件上传和下载

提供对本地及远程的文件，进行上传与下载操作。

7。代理功能

支持把本地的连接通过代理转发到被控主机网络，方便进行内部网络的操作。

**严禁不合规的使用，严禁对外传播。**