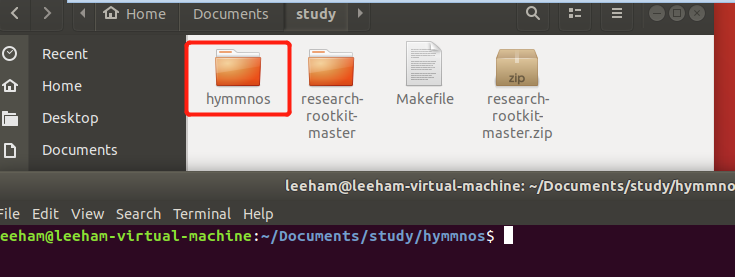
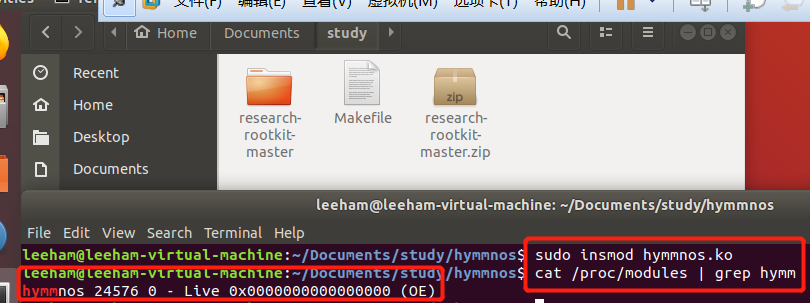
Rootkit测试文档

一．

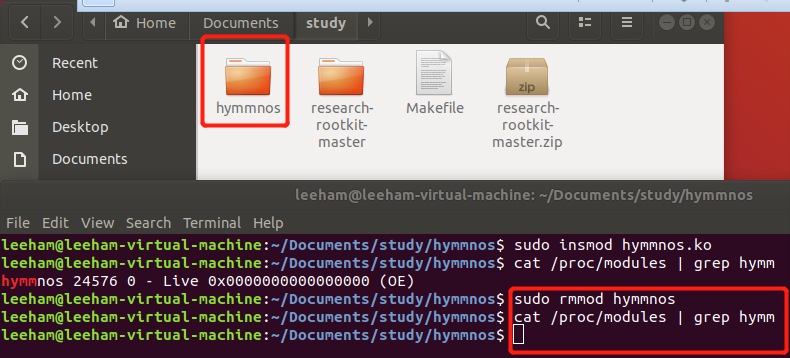
1.模块安装之前；文件夹存在



2.模块安装之后；文件夹隐藏



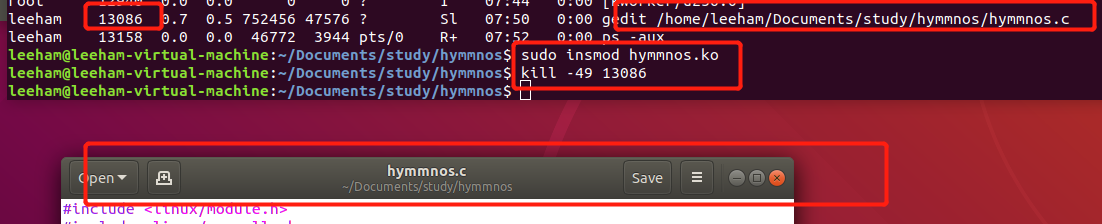
3.模块卸载时候；文件夹存在



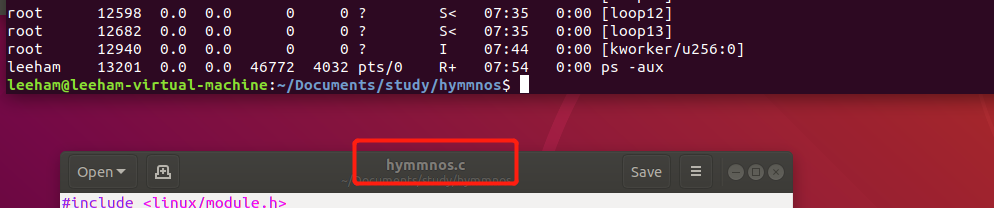
二．隐藏进程功能演示

**Kill -49 13086**

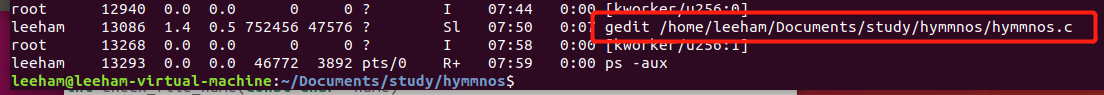
1.安装模块之前ps -aux；可以看到13086进程（这个是gedit hymmnos.c进程，图中可以看到）。安装模块之后可以看到该进程还存在



2.但是此时使用ps -aux看不到13086进程；但实际上该进程还在运行。只是隐藏了。

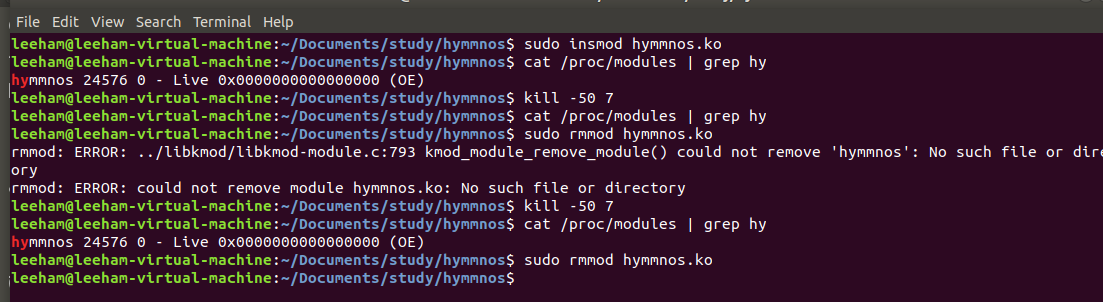


3.卸载模块之后。



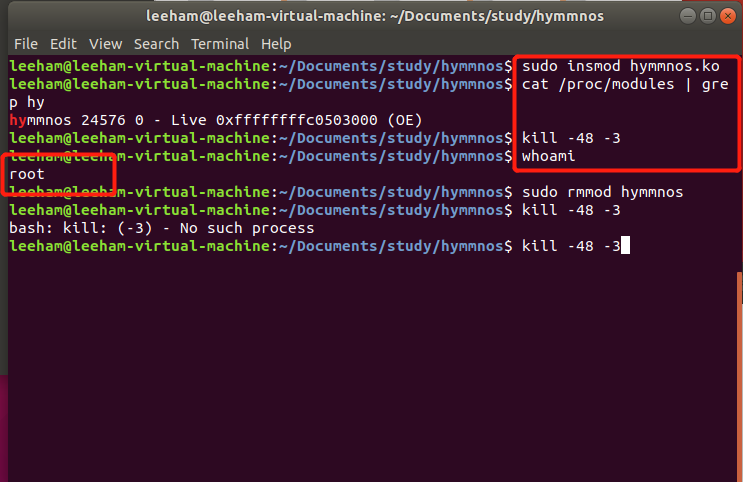
三．

测试**kill -50**的功能；将模块隐藏或显示；隐藏时显示；显示时隐藏

****

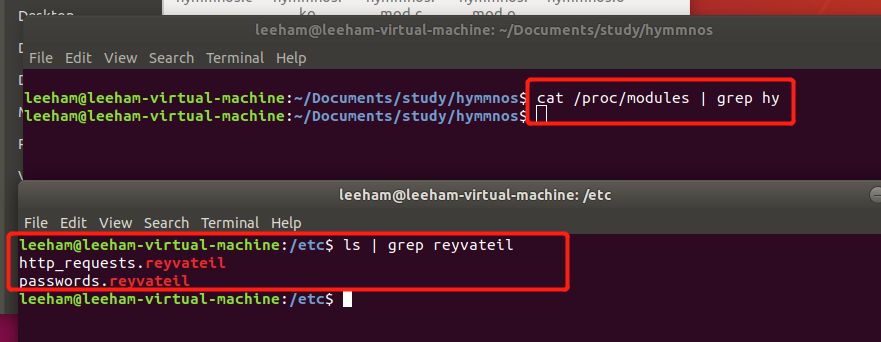
四．

测试**kill -48** ;获取root权限；使用whoami查看是否测试成功

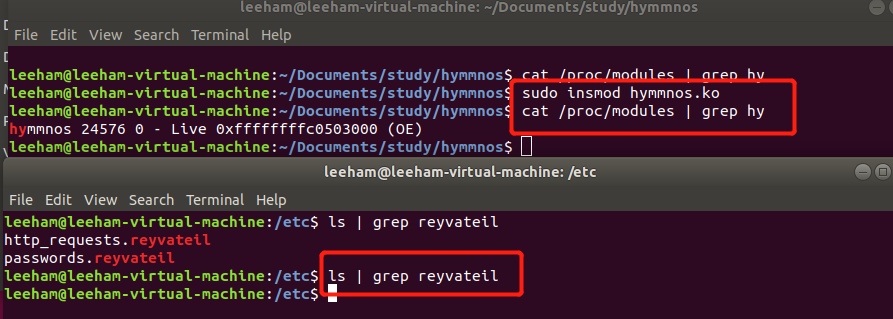


五．测试隐藏文件

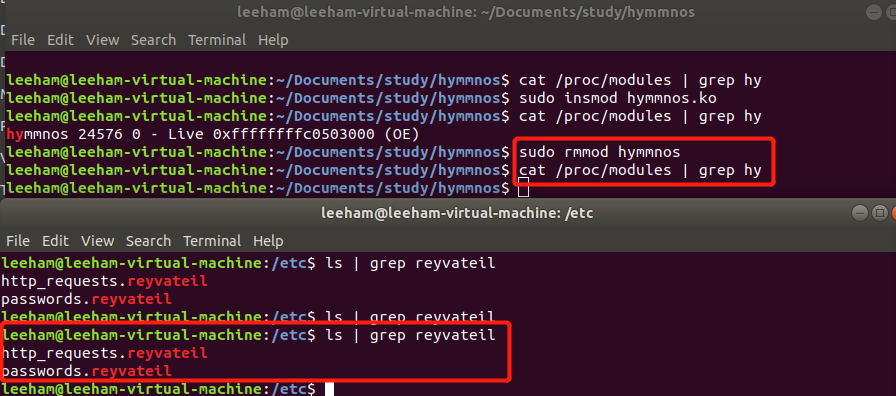
1. 未加载模块时的文件存在



2. 加载模块之后，文件被隐藏



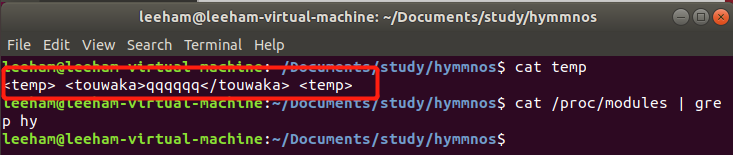
3. 卸载模块之后，隐藏的文件被显示



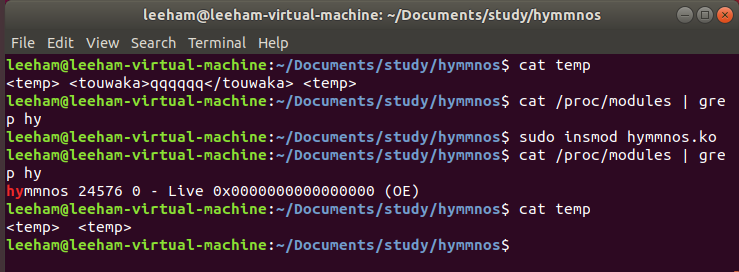
六．

使用**kill -51**命令可以隐藏或显示文件内容

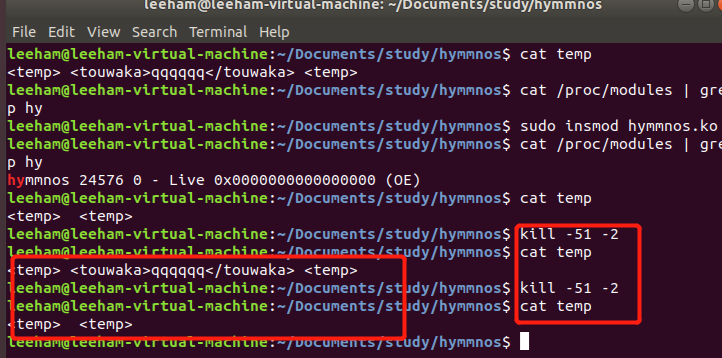
1. 首先在当前目录下新建一个文件，内容可定义如下（实际上只要包含<touwaka>标签就可以）；此时模块还没有有加载；并且内容是显示的。



2. 接着加载模块，此时文件内容中的<touwaka>标签中的内容被隐藏。

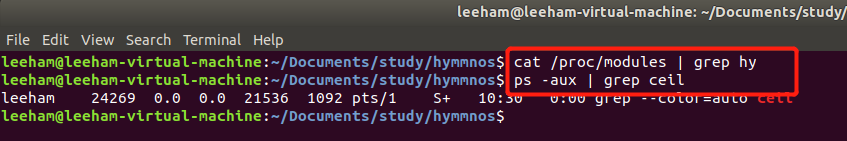


3. 分别使用kill -51命令可以隐藏或显示文件内容

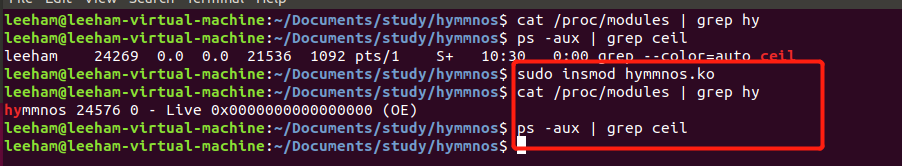


七．对包含指定字段的进程隐藏

1.加载模块之前，能看到含有“ceil”字段的进程



2. 加载模块之后看不到含有“ceil”字段的进程



3. 卸载之后又可以看到含有“ceil”字段进程

