开题报告：资源恶意占用及文件加密程序

组长：左子萱 组员：林嘉豪 徐濛 陆赟杰

Motivation：

通过浏览网络，发现漏洞 CVE-2019-13272 能够对 Ubuntu18.04.1 Linux Version4.15.0-29-generic 实现提权操作。本组意图进行提权后执行相关脚本实现一些功能。

Survey：

https://github.com/bcoles/kernel-exploits/blob/master/CVE-2019-13272

漏洞介绍：在 5.1.17 之前的 Linux 内核中，kernel / ptrace.c 中的 ptrace_link 错误地处理了想要创建 ptrace 关系的进程的凭据记录，这允许本地用户通过利用父子的某些方案来获取 root 访问权限　进程关系，父进程删除权限并调用 execve（可能允许攻击者控制）

上述链接是基于 CVE-2019-13272 漏洞进行提权操作的代码，同时列出了对该漏洞的基本介绍。本组期望理解其提权原理，并使用该提权代码得到 root 权限进行后续操作。

https://blog.csdn.net/zxh2075/article/details/80630296?tdsourcetag=s_pcqq_aiomsg

上述链接是对于 AES 加密算法的介绍，在本次题目中，本组期望基于 AES 实现对文件的加密和解密操作。

https://blog.csdn.net/ycdhqzhiai/article/details/81014028

这篇 blog 介绍了 AES 加密算法实现，使用了 crypto++库对文件进行加密。

https://www.freebuf.com/articles/system/54263.html

介绍了 linux 内核模块的基本编写与隐藏以及系统调用挂钩技术，附有一个简单文件监视工具的代码

https://www.tldp.org/LDP/lkmpg/2.6/lkmpg.pdf

linux 内核模块编写教程，比较详细

同时希望能够进行恶意占用 CPU/内存资源，对此尝试以下两种操作：

1） https://blog.csdn.net/luckywang1103/article/details/79202751?tdsourcetag=s_pcqq_aiomsg

该链接文章介绍了一种 linux 控制 CPU 占用率的方法，能够是 CPU 占用率固定在某个值。

2） https://baijiahao.baidu.com/s?id=1593967383279172915&wfr=spider&for=pc&tdsourcetag=s_pcqq_aiomsg&qq-pf-to=pcqq.group

为了使系统资源利用更有效，尝试利用挖矿来实现 CPU/内存的占用。

Target：

包装成一个可执行文件，运行时会获得系统的 root 权限，然后进行挖矿环境的

部署，后台执行挖矿脚本，占用 CPU/内存资源降计算机性能，若检测到该进程被关闭，则运行加密脚本加密用户目录下所有文件。