StegBrute：如何在CTF中快速进行隐写爆破

原创

黄一113530 于 2022-01-24 19:31:57 发布 373 收藏 1

分类专栏： 安全 文章标签： rust 开发语言 后端

本文链接：https://blog.csdn.net/weixin_43977912/article/details/122673638

StegBrute

StegBrute是一款功能强大的隐写术暴力破解工具，该工具基于Rust开发，并且引入了线程机制以提升其性能，可以帮助广大研究人员在CTF比赛中迅速对隐写内容进行暴力破解。

工具依赖

StegBrute的运行必须依赖于Steghide，因此，我们在使用StegBrute之前需要先安装并运行Steghide：

apt-get install -y steghide

如果你使用的并不是基于Debian的发行版系统的话，请直接点击【这里】访问Stetghide站点并下载最新版本。

工具安装&配置&运行

StegBrute提供了多种安装方式，具体如下。

Cargo安装

广大研究人员可以通过cargo（Rust包管理器）来安装StegBrute。如果你的设备上还没有安装cargo的话，你可以通过apt来安装，或直接下载配置Rust环境：

cargo install stegbrute

注意：这种安装方式适用于各种平台。

基于Debian的发行版系统

如果你使用的是uBuntu、Kali或其他基于Debian的发行版操作系统，你可以直接点击【这里】下载该工具预编译好的.deb文件来进行工具安装，下载完成后解压文件并运行即可：

wget https://github.com/R4yGM/stegbrute/releases/download/0.1.1/stegbrute_0.1.1_amd64.deb &&

dpkg --install stegbrute_0.1.1_amd64.deb

Docker安装

提醒：如果你还没有在自己的设备上安装Docker的话，请参考这篇【指引文档】。

首先，我们需要从【Docker库】中下载Docker镜像，大小仅为4.93MB。如果你没有下载该镜像的话，你还可以使用下列命令将该项目源码克隆至本地，然后运行命令来构建镜像以及Dockerfile：

git clone https://github.com/R4yGM/stegbrute.git

docker pull r4yan/stegbrute:latest

你还可以通过替换“latest”为不同的StegBrute版本号来下载不同版本的StegBrute镜像，比如说：

docker pull r4yan/stegbrute:0.1.0

如果上述工作你都懒得做的话，你可以直接点击【这里】下载/拷贝StegBrute的Dockerfile，然后利用Dockerfile构建工具镜像文件。

在启动容器之前，我们还需要创建一个卷来与容器共享文件：

docker volume create --name stegbrute_data

然后，将你需要使用（即使用StegBurte进行爆破）的文件拷贝到这个卷中的文件夹内，假设路径为“/var/lib/docker/volumes/stegbrute_data/_data”，则需要运行的命令如下：

cp wordlist.txt /var/lib/docker/volumes/stegbrute_data/_data && cp file.jpg /var/lib/docker/volumes/stegbrute_data/_data

现在，我们就可以使用下列命令运行StegBrute了：

docker run -v stegbrute_data:/stegbrute_data -it --rm --name stegbrute r4yan/stegbrute:latest

在使用过程中，还需要用你要提供给StegBrute的内容替换上述命令中的参数。

重要：请及时将处理结果存储在卷内，而不要存储在容器中，因为这些结果会被删除！你可以在运行命令后面添加下列选项来实现结果自动保存：

-x /

$$-extract-\ file\ /\ \mathrm{VOLUME\_NAME/results.txt}$$

项目地址

StegBrute：https://github.com/R4yGM/stegbrute