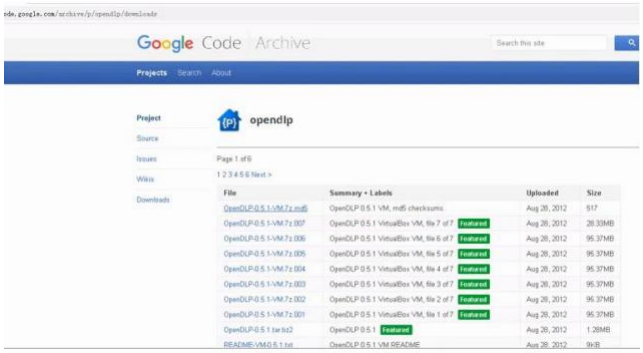
11 DLP

0x01 实验环境

数据防泄漏 DLP(Data Loss Prevention)就是该款工具的主要目的。该攻击可以全面扫描数据，无论数据是存在数据库中还是存放在文件系统里。Open DLP 会搜索与公司相关的敏感数据以发现数据的未授权复制和传输。这对防御恶意内部人或粗心大意的员工往外部发送数据很有用。该工具在 Windows 系统上运行良好，也支持 Linux,且可通过代理部署，或作为无代理工具使用。

下载地址：https://github.com/ezarko/opendlp 可以直接百度网盘下载：但这个环境搭建麻烦，现在主要靠 google 在维护，界面不好看。

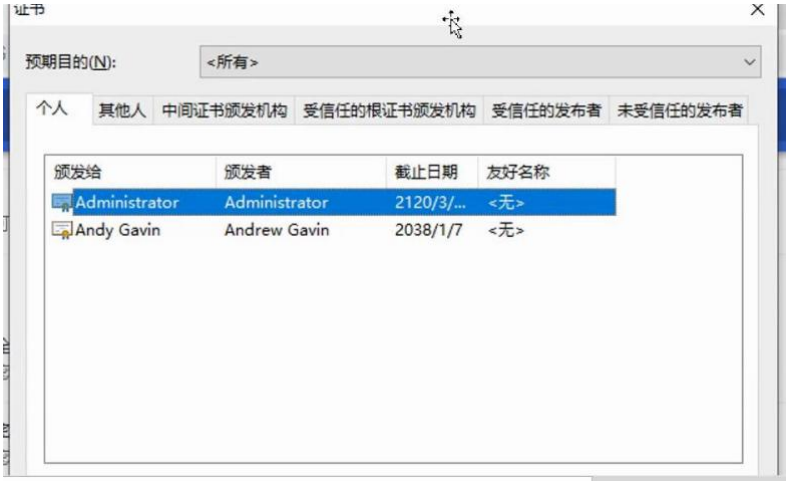


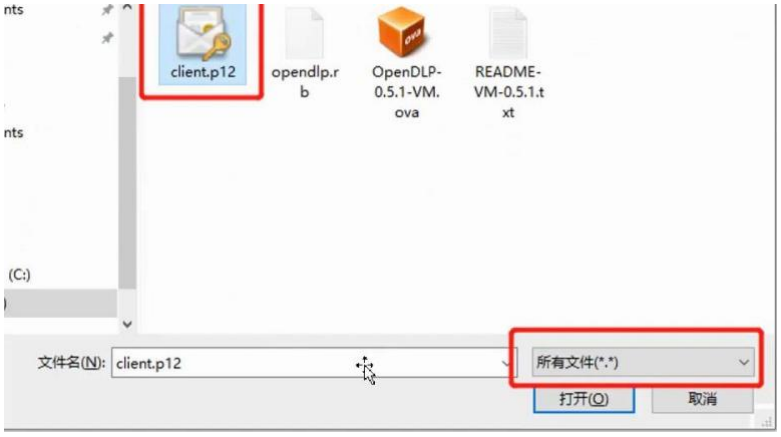
0x02 原理介绍

一个免费的，开源的，基于代理和无代理的，集中管理，可大规模分发的数据丢失防护工具。

0x03 实践操作

需要安装证书





登录

https://192.168.2.113/OpenDLP/index.html

username:dlpuser

password:QpenDLP

12 终端管理

这个东西更简单，统一的集中管理平台，管理终端，但这是个人谁都不愿意装，但领导特别喜欢的软件。。。。。

0×01 功能

0x02 厂商

360、奇安信、腾讯、北信源等。。。

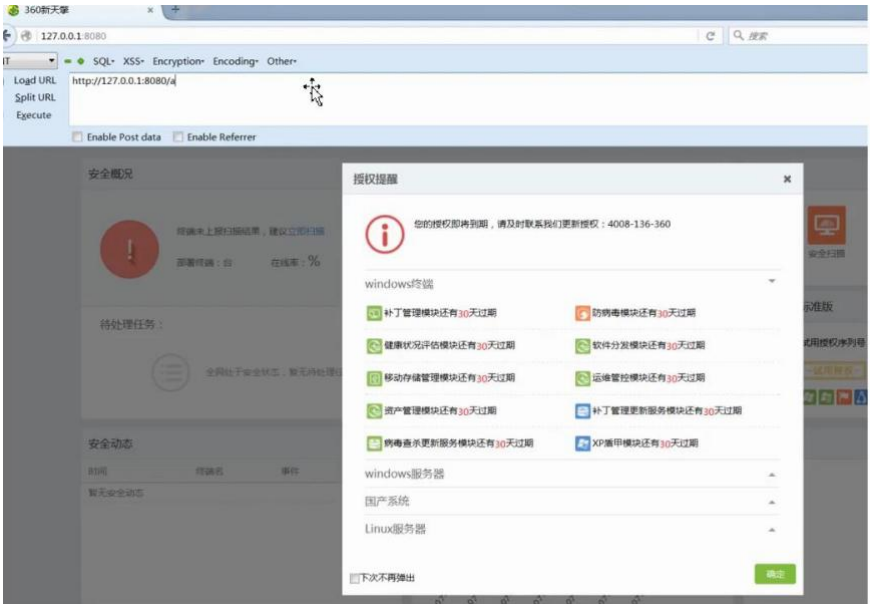
0x03 奇安信天擎试验

天擎 6.0 下载地址：

http://down.360safe.com/skylar6/360skylarsetup_f7f974da5bf38c6b24988c0f7e2f11c0_6.0.0.3100.exe

或者提供的云盘

下载的为试用版，30 天试用


360新天擎
127.0.0.1:8080
SQL- XSS- Encryption- Encoding- Other-
Load URL
Split URL
Execute
http://127.0.0.1:8080/a
Enable Post data
Enable Referrer
安全概况
待处理任务：
安全动态
授权提醒
您的授权即将到期，请及时联系我们更新授权：4008-136-360
windows终端
补丁管理模块还有30天过期
防病毒模块还有30天过期
健康状况评估模块还有30天过期
软件分发模块还有30天过期
移动存储管理模块还有30天过期
运维管控模块还有30天过期
资产管理模块还有30天过期
补丁管理更新服务模块还有30天过期
病毒查杀更新服务模块还有30天过期
XP盾甲模块还有30天过期
windows服务器
国产系统
Linux服务器
下次不再弹出
确定